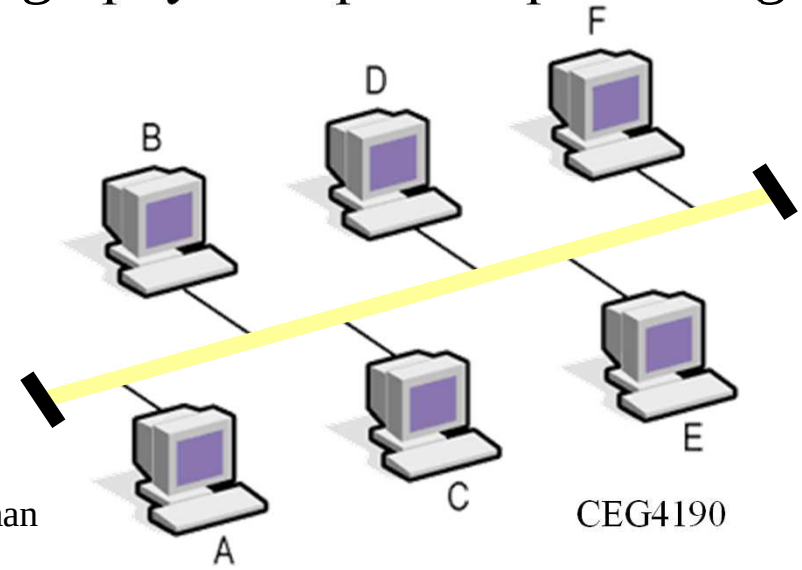
Lecture 10:

Virtual LANs (VLAN)
and
Virtual Private Networks (VPN)

Instructor: Hussein Al Osman

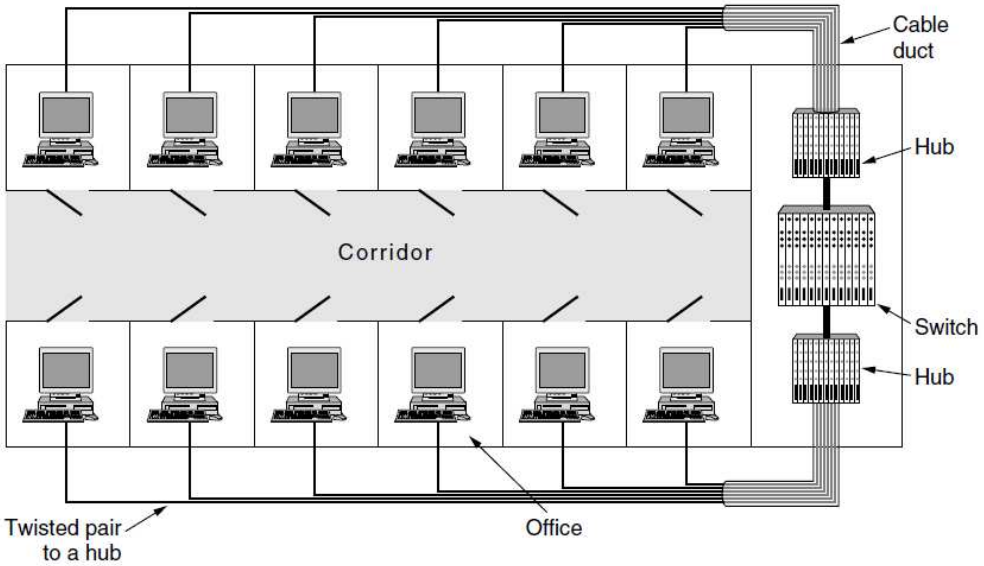
Local Area Networks

- Early days of local area networking: thick yellow cables snaked through the cable ducts of office buildings
  - Every computer they passed was plugged in
- No thought was given to which computer belonged on which LAN
  - People in adjacent offices were put on the same LAN
  - Geography trumped corporate organization charts



Local Area Networks

- With advent of twisted pair and hubs in the 1990s, buildings were rewired to rip out all the yellow wires and install twisted pairs from every office to central wiring closets



- If a company wants *k* LANs, it could buy *k* switches
- By carefully choosing which connectors to plug into which switches, the occupants of a LAN can be chosen in a way that makes organizational sense

Virtual Local Area Networks

- In many companies, organizational changes occur all the time
  - System administrators spend a lot of time pulling out plugs and pushing them back in somewhere else
- In some cases, the change cannot be made at all because the twisted pair from the user's machine is too far from the correct switch
- Therefore, network vendors began working on a way to rewire buildings entirely in software
  - Resulting concept is called a **VLAN (Virtual LAN)**
  - Standardized by the IEEE 802 committee and is now widely deployed in many organizations

Virtual LANs

- Description:
  - Group of devices on one or more physical LANs that are configured as if they are logically attached to the same wire
  - LAN's based on Logical instead of Physical connections
- Used to separate out users into logical groups of workers, regardless of actual physical location.

Virtual LANs

- Usage scenarios:
  - Say you want workers assigned to the same project to be grouped logically together for control of traffic but they are physically located in different physical areas
  - Say you want to divide up the broadcast domain in a large flat network without using a bunch of routers
- Must be supported by the switch: switches must have the ability to support more than one subnet

Virtual LANs

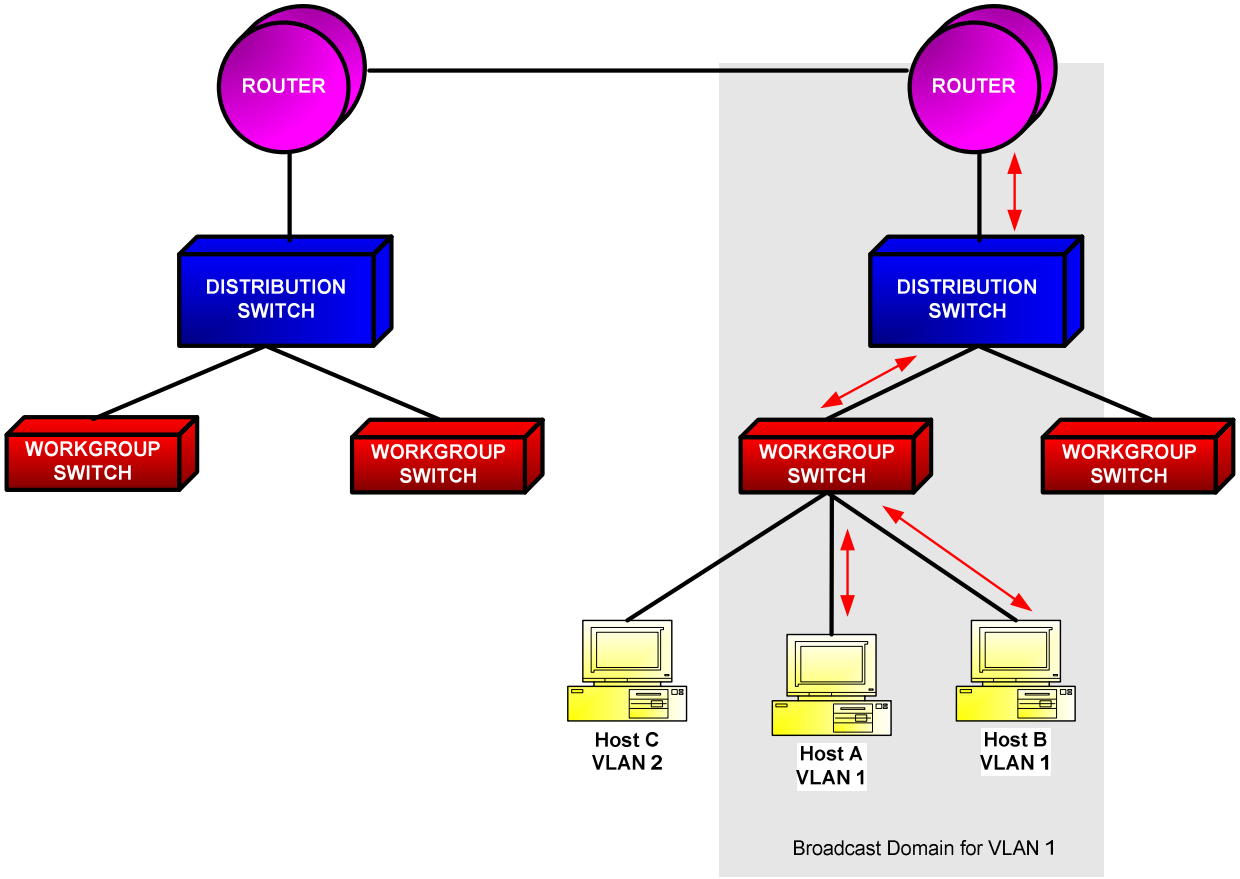
- To set up a VLAN-based network, the network designer/administrator decides:
  - How many VLANs there will be
  - Which computers will be on which VLAN
  - What the VLANs will be called
- Often the VLANs are (informally) named by colors
  - Since it is then possible to print color diagrams showing the physical layout of the machines, with the members of the red LAN in red, members of the green LAN in green, and so on

VLAN Levels

- At the User Level
- At the Wiring Closet Level
- AT the Distribution Switch Level

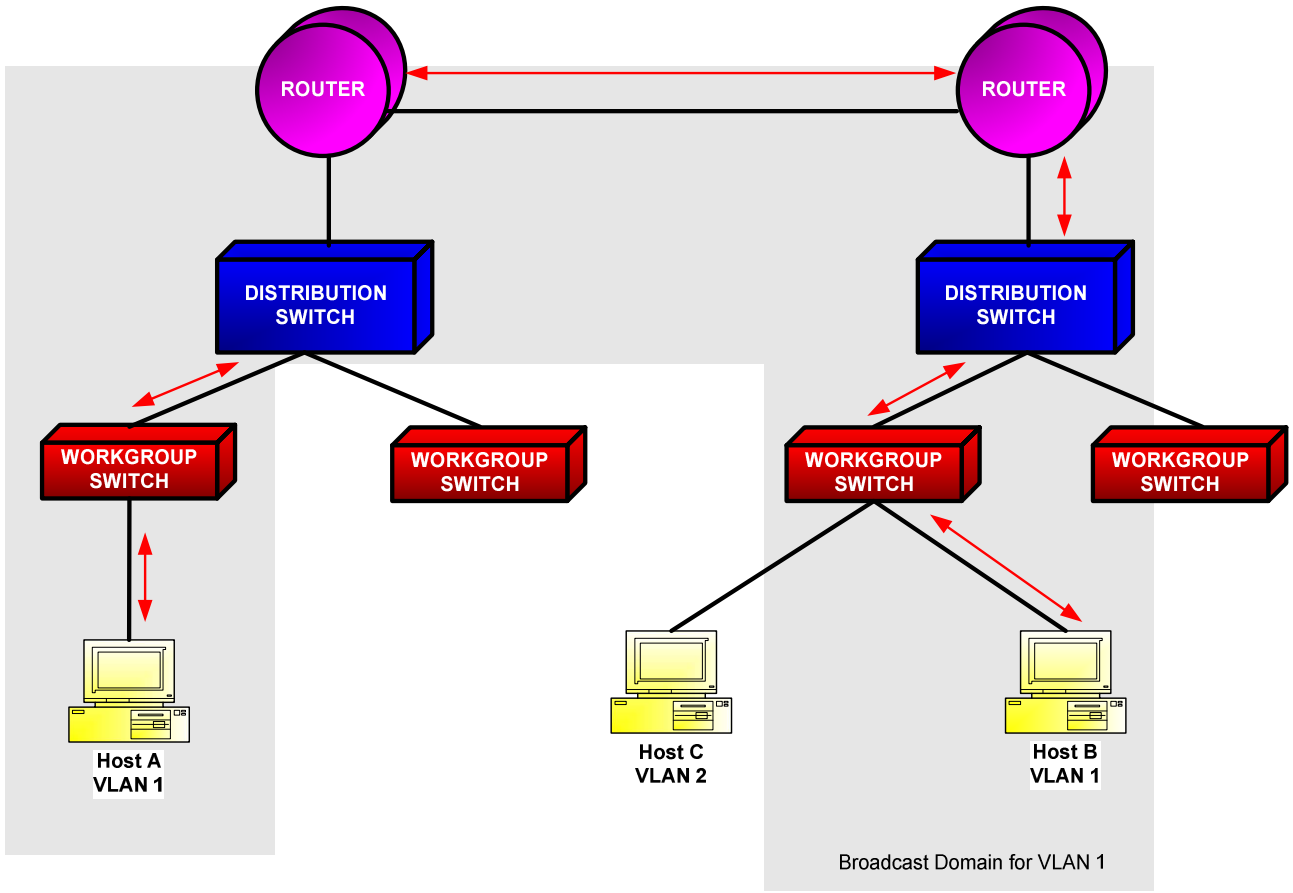
User Level VLAN

- Users belong to a specific VLAN regardless of where they attach to the network
- User can “roam” on the network
- Beneficial when traffic stays on the VLAN
- However, broadcast traffic will follow the user



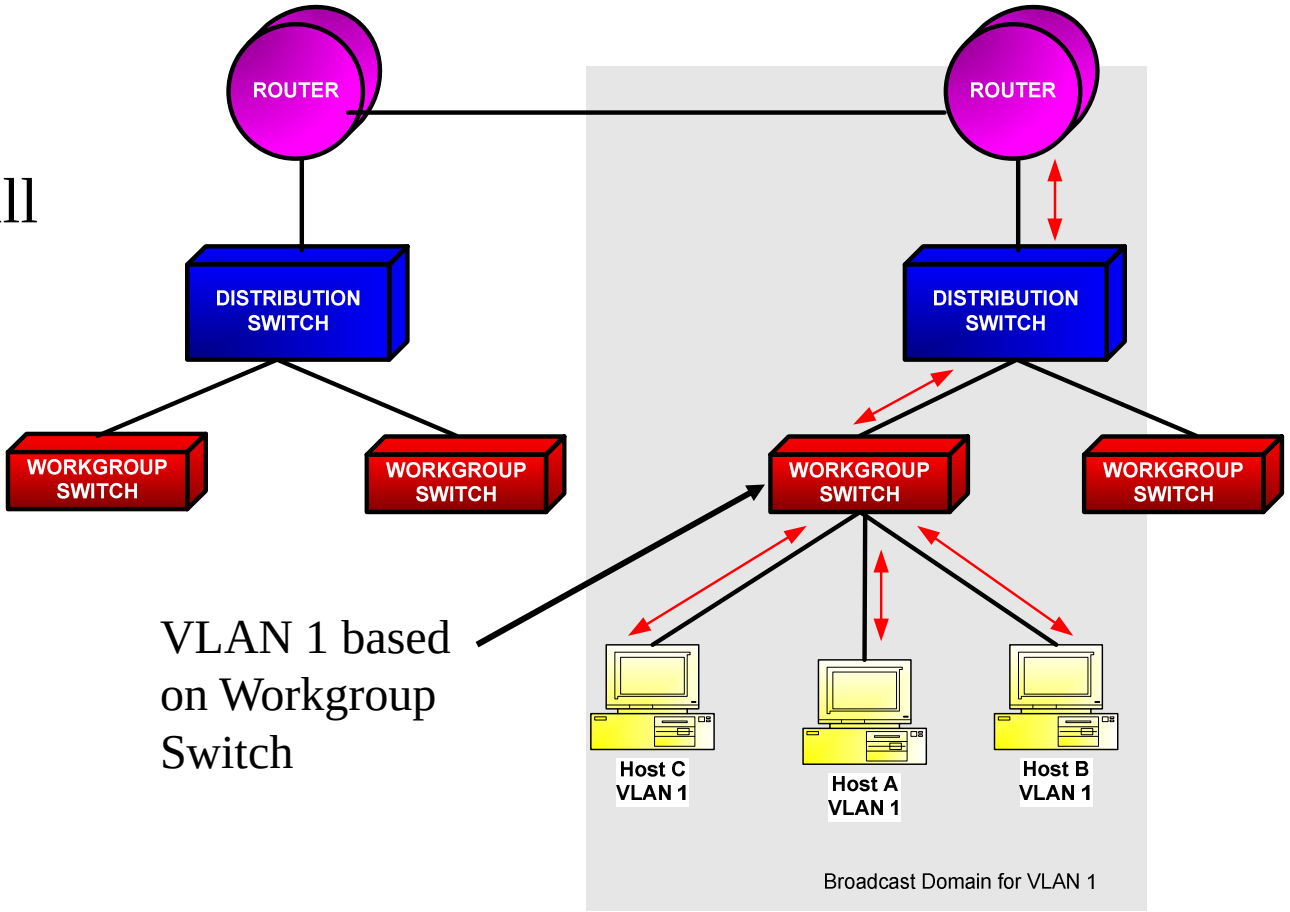
User Movement

If Host A moves to a different Workgroup Switch, the Broadcast Domain follows the movement of Host A.



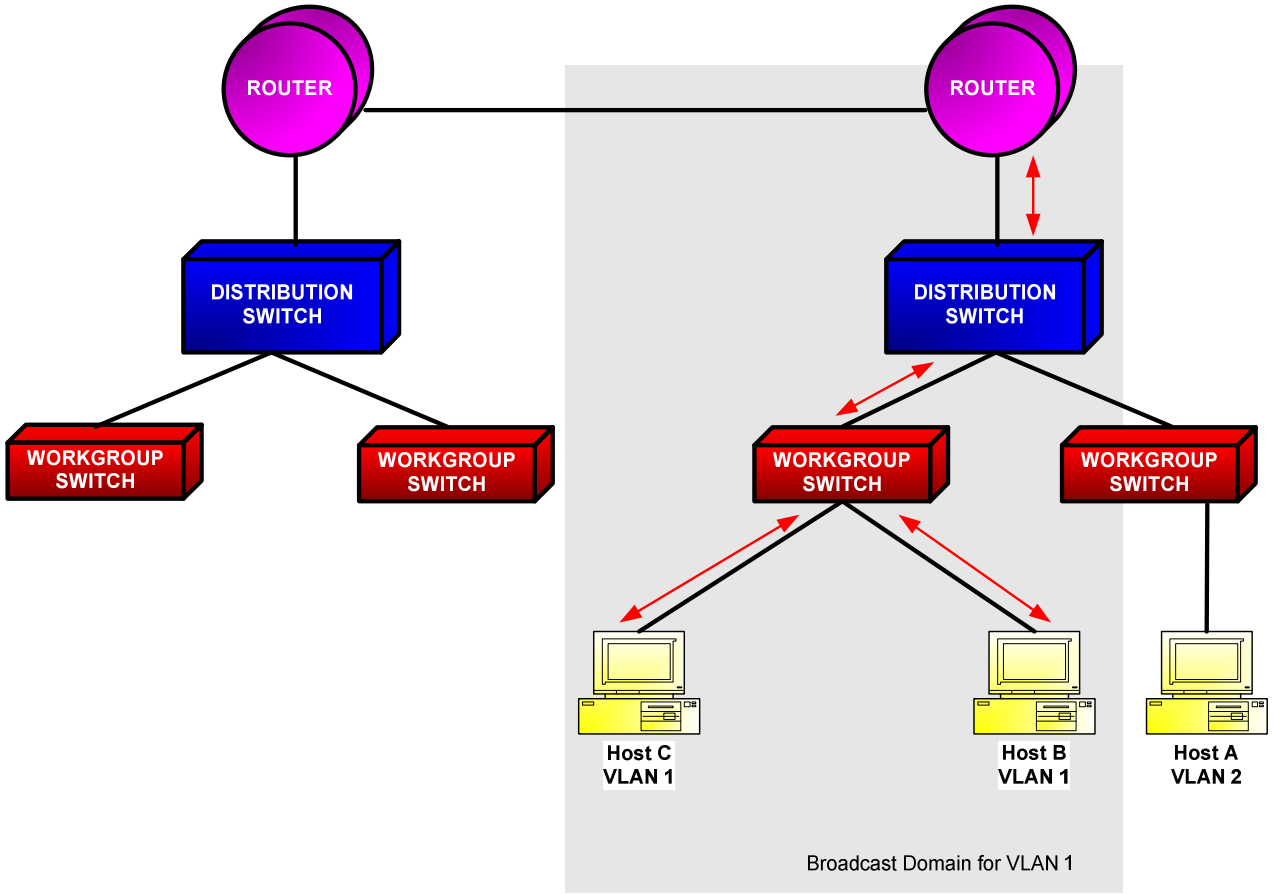
Wiring Closet VLAN

- People must be physically close together on same VLAN
- Broadcast traffic will not follow the user



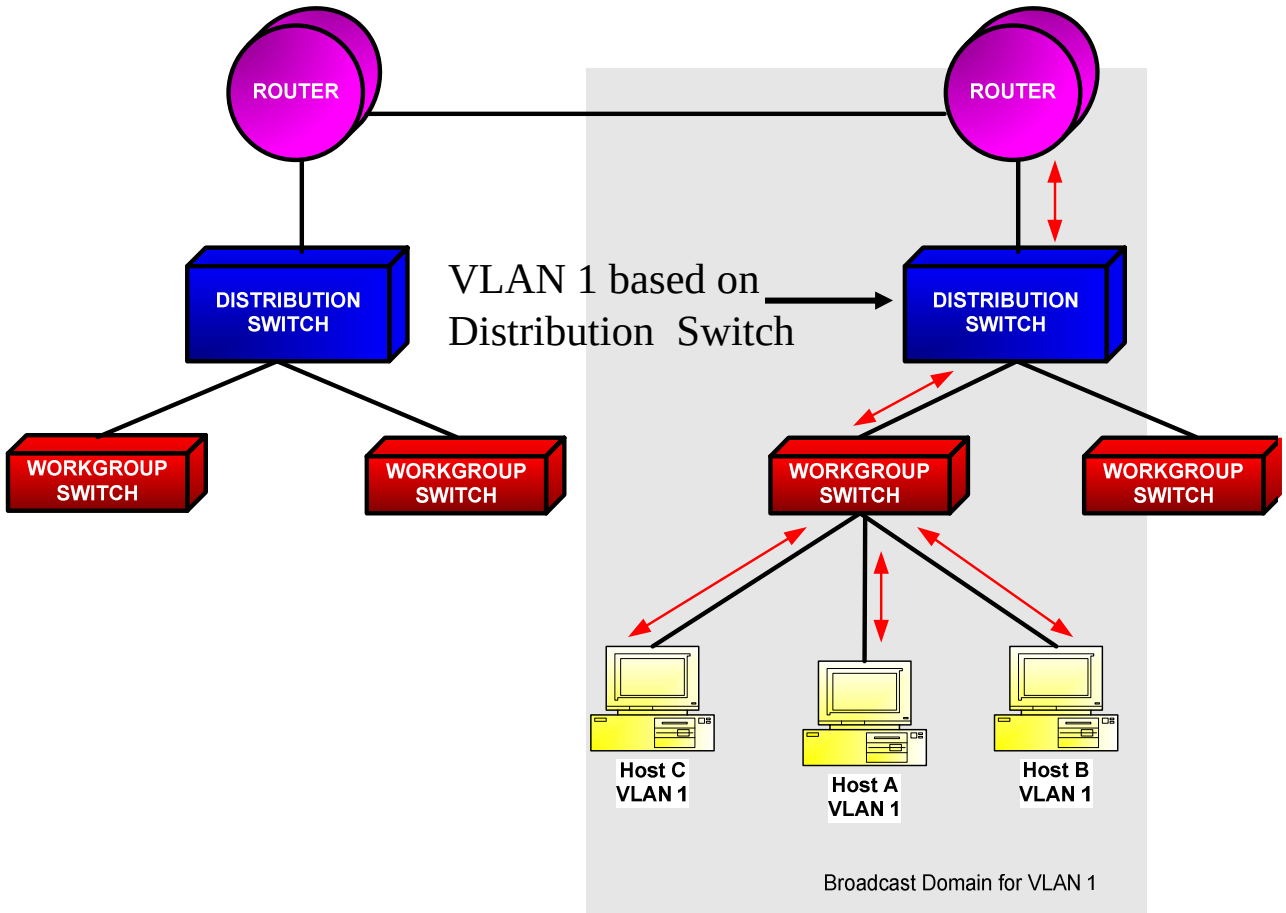
User Movement

If Host A moves to a different Workgroup Switch, it belongs to a new VLAN. Broadcast Domain stays with the switch, and does not follow Host A.



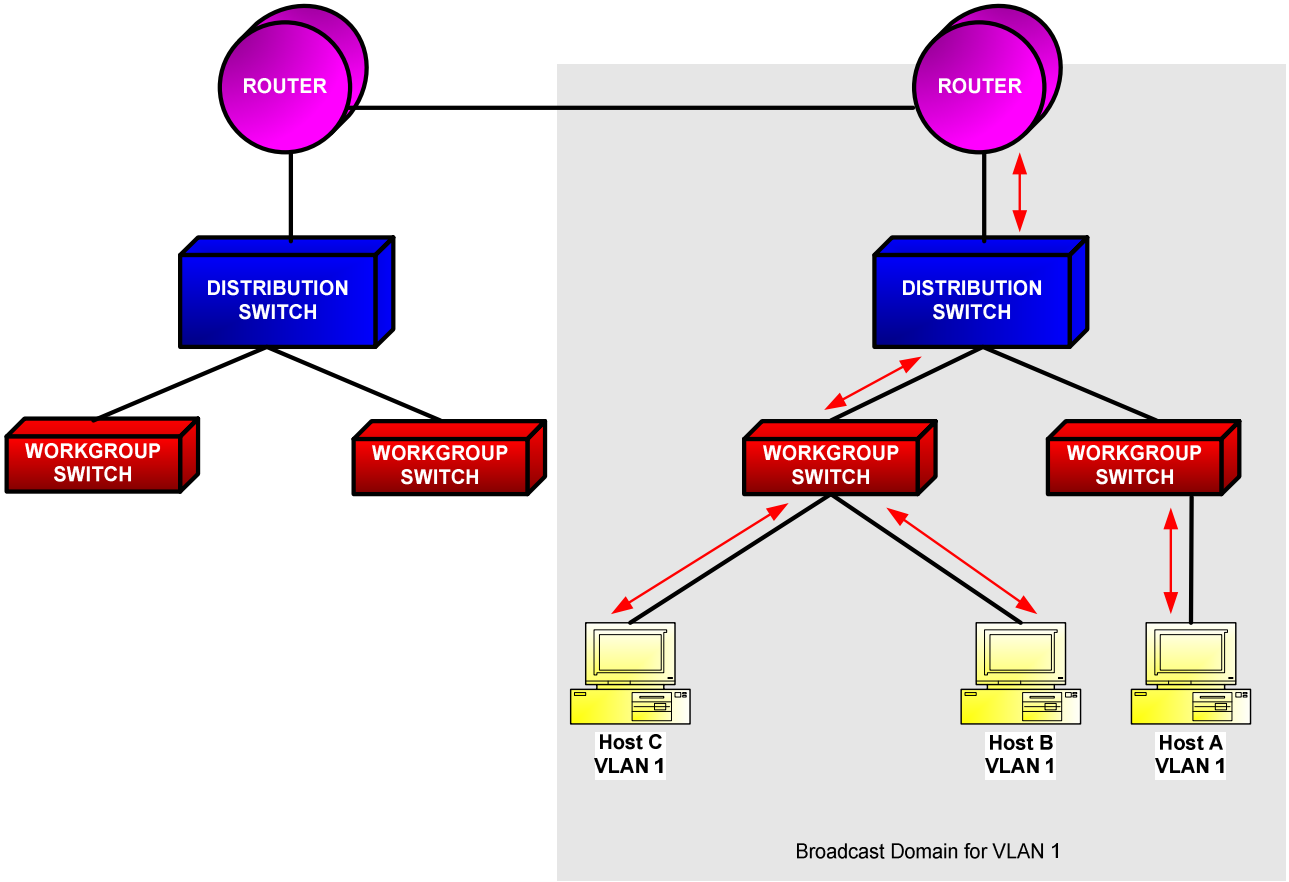
Distribution Switch VLAN

- Middle ground between User and Wiring Closet designs
- If users move but stay on the same distribution switch - Same VLAN
- If users move to different distribution switch, then it's a Different VLAN



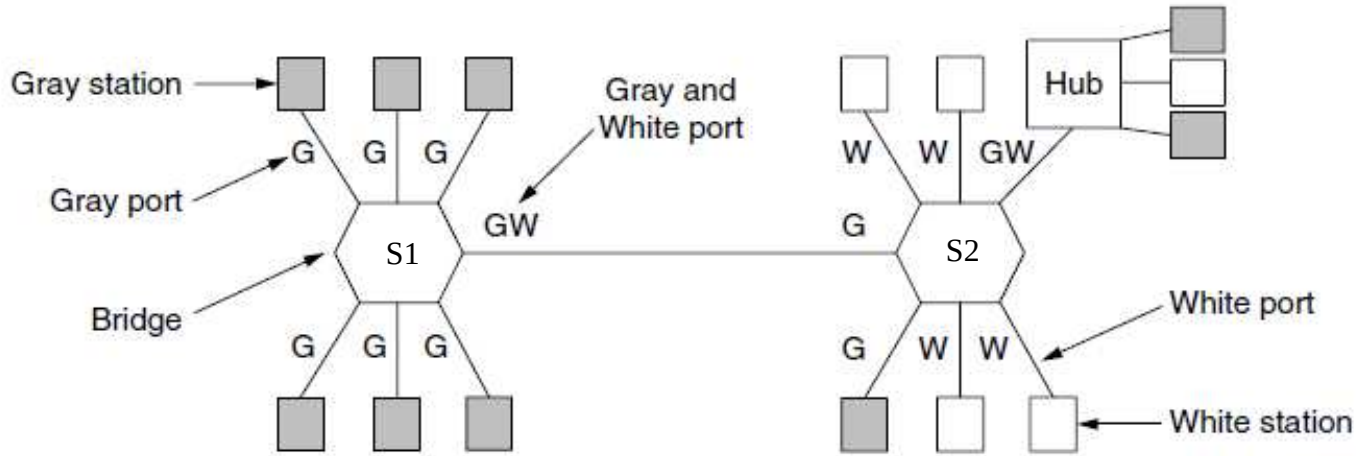
User Movement

If Host A moves to a different Distribution Switch, the Broadcast Domain follows Host A since it stays on the same distribution switch.



VLAN Example (1)

- Nine of the machines belong to the G (gray) VLAN and five belong to the W (white) VLAN
- Machines from the gray VLAN are spread across two switches, including two machines that connect to a switch via a hub



VLAN Example (2)

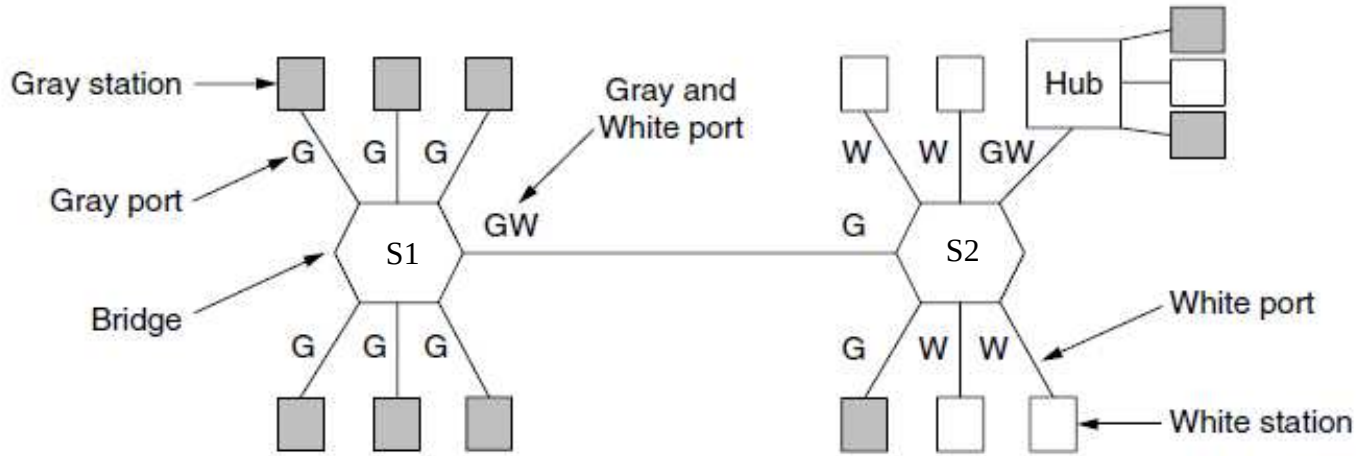
- To make the VLANs function correctly, configuration tables have to be set up in the switches
- These tables tell which VLANs are accessible via which ports
  - Note that a port may be labeled with multiple VLAN colors
- When a frame comes in from the gray VLAN, it must be forwarded on all the ports marked with a G **for**:
  - Ordinary (i.e., unicast) traffic where the switch has not learned the location of the destination
  - Broadcast traffic

VLAN Example (3)

- Suppose that one of the gray stations plugged into S1 sends a frame to a destination that has not been seen before by S1
  - S1 will receive the frame and flood the frame on all ports labeled G (except the incoming port)
  - The frame will be sent to the five other gray stations attached to S1 as well as over the link from S1 to S2
  - At switch S2, the frame is similarly forwarded on all ports labeled G
  - This sends the frame to one further station and the hub (which will transmit the frame to all of its stations)

VLAN Example (4)

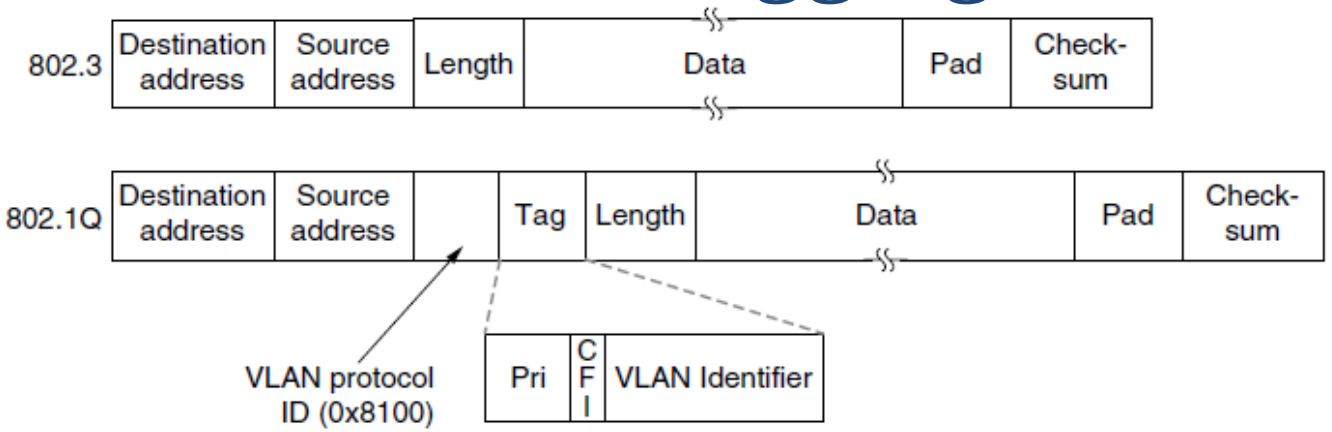
- S2 port that connects to S1 is not labeled W
- This means that a frame on the white VLAN will not be forwarded from S2 to bridge S1
- This behavior is correct because no stations on the white VLAN are connected to S1



VLAN Tagging

- To implement VLANs, switches need to know to which VLAN an incoming frame belongs
- Using last example, when S2 gets a frame from S1, it need to know whether to forward the frame on the gray or white VLAN
- If we were designing a new type of LAN, it would be easy enough to just add a VLAN field in the header
  - But what to do about Ethernet, which is the dominant LAN, and did not have any spare fields lying around for the VLAN identifier?
- The IEEE 802 committee changed the Ethernet header
- The new format was published in IEEE standard **802.1Q**, issued in 1998

VLAN Tagging



- What to do with computer and switches that only know the original format?
  - Nothing!! The first VLAN-aware switch to touch a frame adds VLAN fields and the last one down the road removes them
- Fields:
  - VLAN protocol ID: always has the value 0x8100
  - VLAN ID: 12 bits representing ID of VLAN
  - Other two fields have mostly nothing to do with VLANs (since we are changing header, we might as well add fields…)

Virtual Private Networks

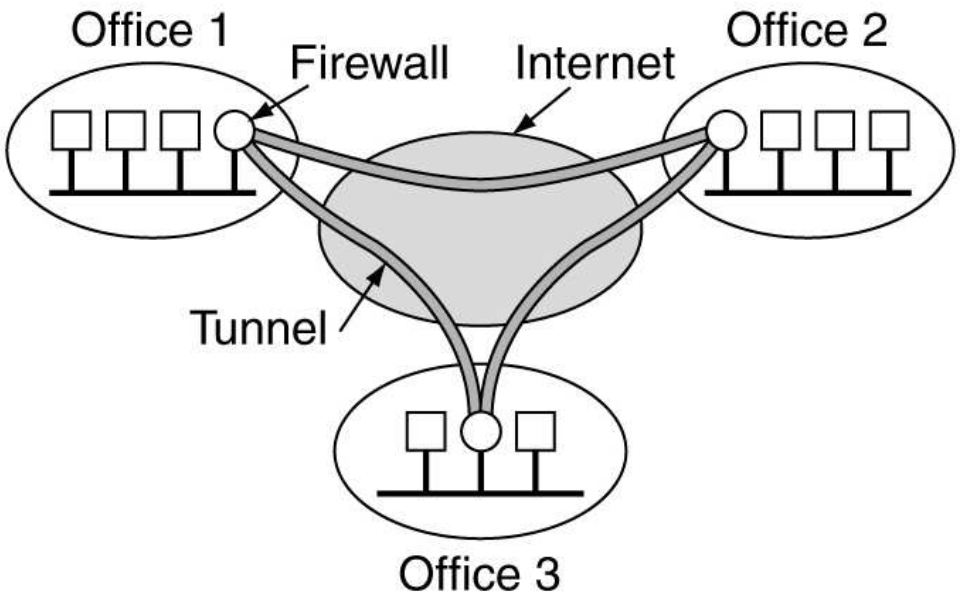
- VPN's enable an organization to use Public Networks such as the Internet, to provide a **Secure** connection among the organization's wide area network.
- Traditionally, businesses have relied on private 56-Kbps or T-1 leased lines to connect remote offices together
- Leased lines are expensive to install and maintain
  - For small companies, the cost is just too high
- Using the Internet as a backbone, a VPN can securely and cost effectively connect all of a companies offices, telecommuters, mobile workers, customers, partners and suppliers.

VPN Functionality

- A VPN needs to provide the following 4 critical functions:
  - Authentication – ensuring that the data originates at the source that it claims.
  - Access Control – restricting unauthorized users form the network.
  - Confidentiality – Preventing anyone from reading the data as it travels through the network
  - Data Integrity – Preventing anyone from tampering with the data as it traverses through the network

VPN Gateway and Tunnels

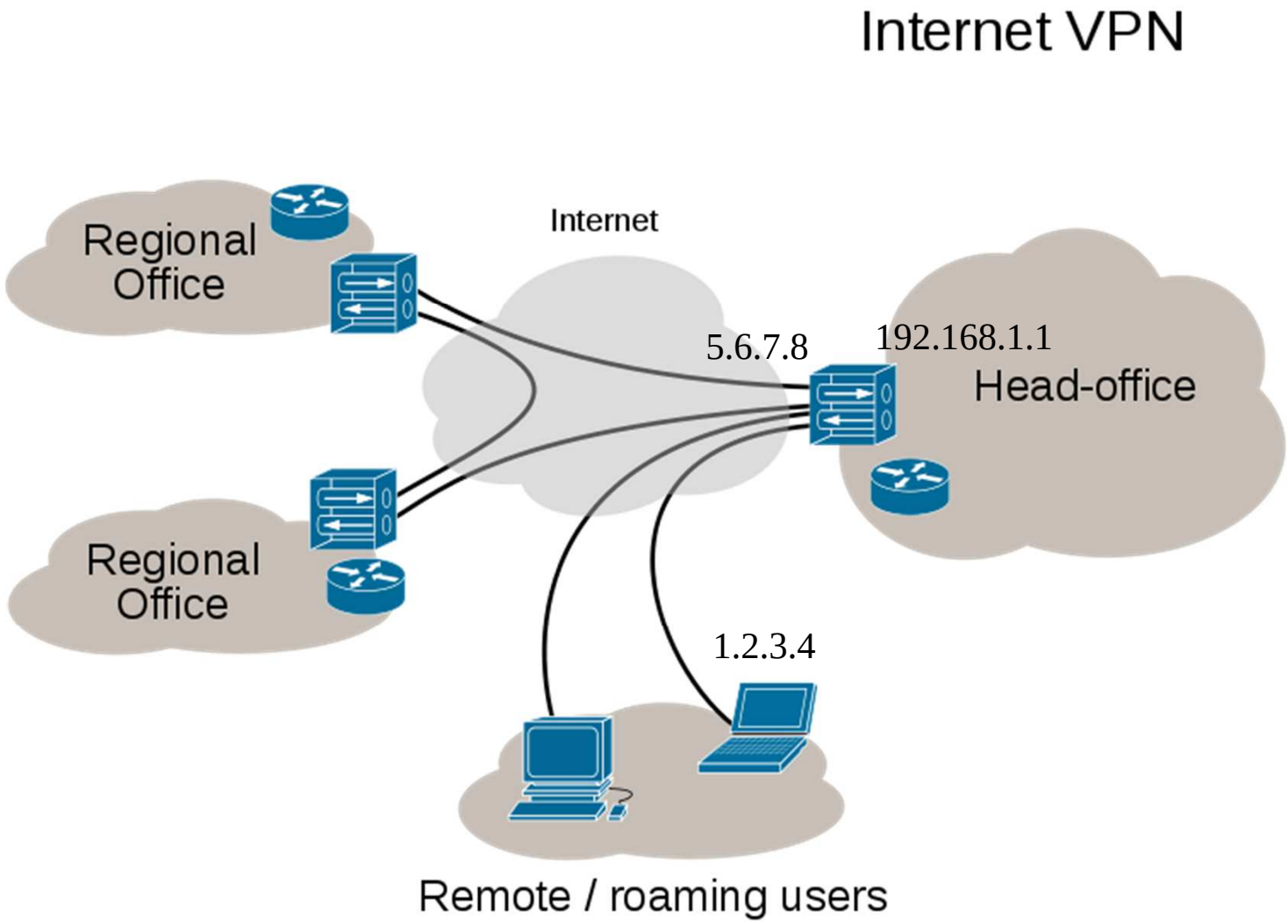
- A VPN gateway is a network device that provides encryption and authentication service to a multitude of hosts that connect to it.
- From the outside (Internet), all communications addressed to inside hosts flow through the gateway
- There are 2 types of end point VPN tunnels:
  - Computer to Gateway
    - For remote access: generally set up for a remote user to connect A corporate LAN.
  - Gateway to Gateway
    - This the typical Enterprise-to-enterprise configuration. The 2 gateways communicate with each other.



VPN Tunnel Example

- Remote host (IP address 1.2.3.4) wishes to connect to a server inside a company network
- Server has internal address 192.168.1.10 and is not reachable publicly
- Before the client can reach this server, it needs to go through a VPN server device that has public IP address 5.6.7.8 and an internal address of 192.168.1.1
- All data between the client and the server will need to be kept confidential

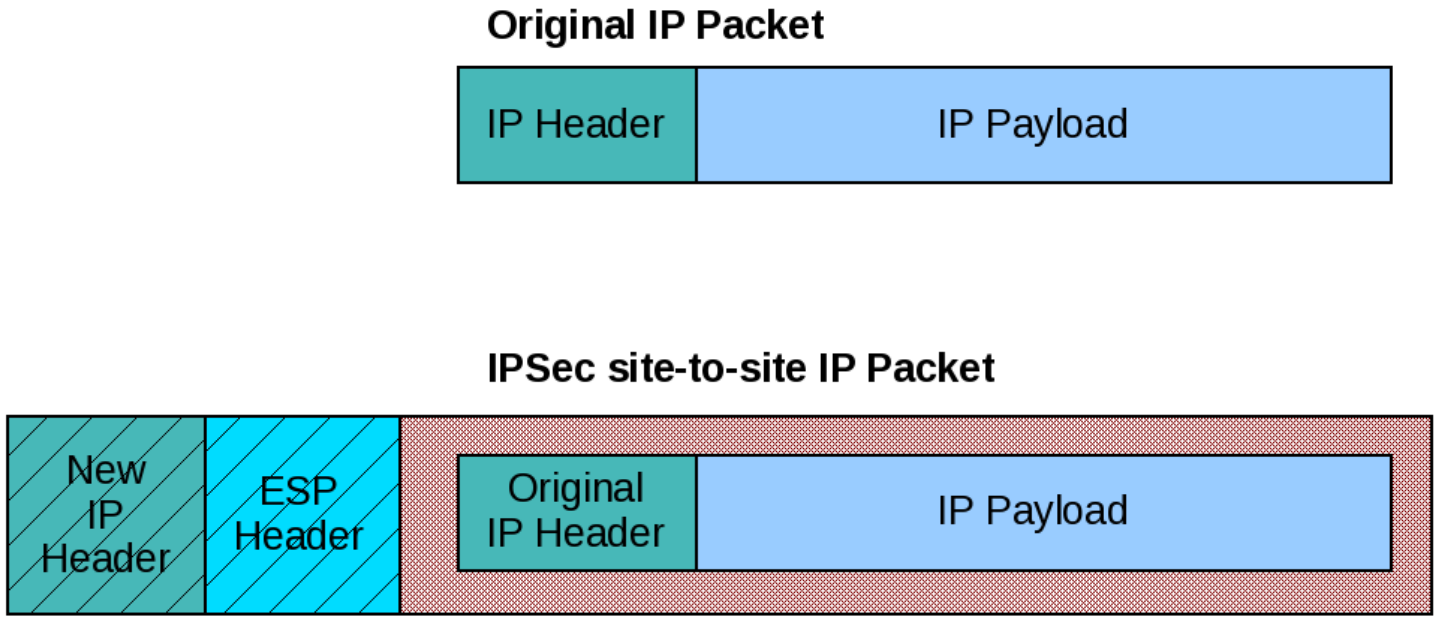
VPN Tunnel Example



VPN Tunnel Example

- The VPN client connects to a VPN server via an external network interface
- The VPN server assigns an IP address to the VPN client from the VPN server's subnet
  - Client gets internal IP address 192.168.1.50,
  - Client creates a virtual network interface through which it will send encrypted packets to the other tunnel endpoint
  - This interface also gets the address 192.168.1.50
- When the VPN client wishes to communicate with company server, it prepares a packet addressed to 192.168.1.10, encrypts it and encapsulates it in an IPSec packet

VPN Tunnel Example



VPN Tunnel Example

- This packet is then sent to the VPN server at IP address 5.6.7.8 over the public Internet
- The inner packet is encrypted so that even if someone intercepts the packet over the Internet, they cannot get any information from it
  - They can see that the remote host is communicating with a VPN server, but none of the contents of the communication.
  - The inner encrypted packet has source address 192.168.1.50 and destination address 192.168.1.10.
  - The outer packet has source address 1.2.3.4 and destination address 5.6.7.8

VPN Tunnel Example

- When the packet reaches the VPN server from the Internet, the VPN server:
  - Decapsulates the inner packet
  - Decrypts it
  - Finds the destination address to be 192.168.1.10
  - Forwards it to the intended server at 192.168.1.10

VPN Tunnel Example

- After some time, the VPN server receives a reply packet from 192.168.1.10, intended for 192.168.1.50
- The VPN server consults its routing table, and sees this packet is intended for a remote host that must go through VPN
- The VPN server encrypts this reply packet, encapsulates it in a VPN packet and sends it out over the Internet
- The inner encrypted packet has source address 192.168.1.10 and destination address 192.168.1.50
- The outer VPN packet has source address 5.6.7.8 and destination address 1.2.3.4
- The remote host receives the packet. The VPN client unencapsulates the inner packet, decrypts it, and passes it to the appropriate software at upper layers.

Thank You!