VLAN Hopping

Applied Network security (comp420 –001)

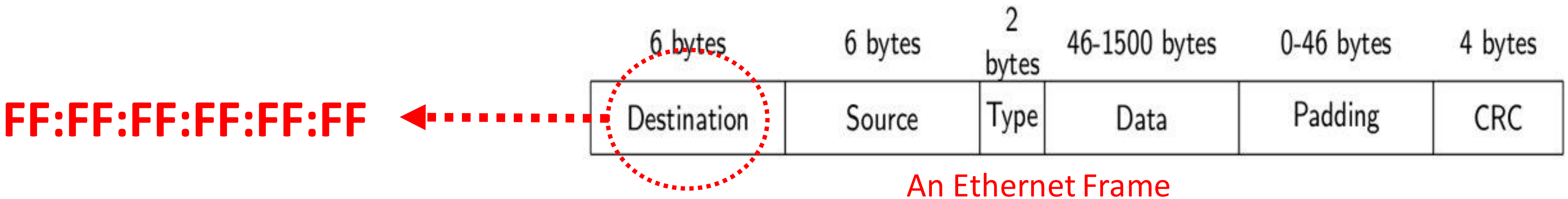
Department of Computer science

Fall 2020

What Is a Layer 2 (aka L2) Domain

Domain: A domain contains a group of computers that can be accessed and administered with a common set of rules.

Layer 2 (L2) Domain: In a Layer 2 network, broadcasting refers to sending traffic to all nodes on a network. Layer 2 broadcast traffic stays within a local area network (LAN) boundary; known as the **broadcast domain (aka L2 Domain)**. Layer 2 broadcast traffic is sent to all domain members using a MAC address of FF:FF:FF:FF:FF:FF.

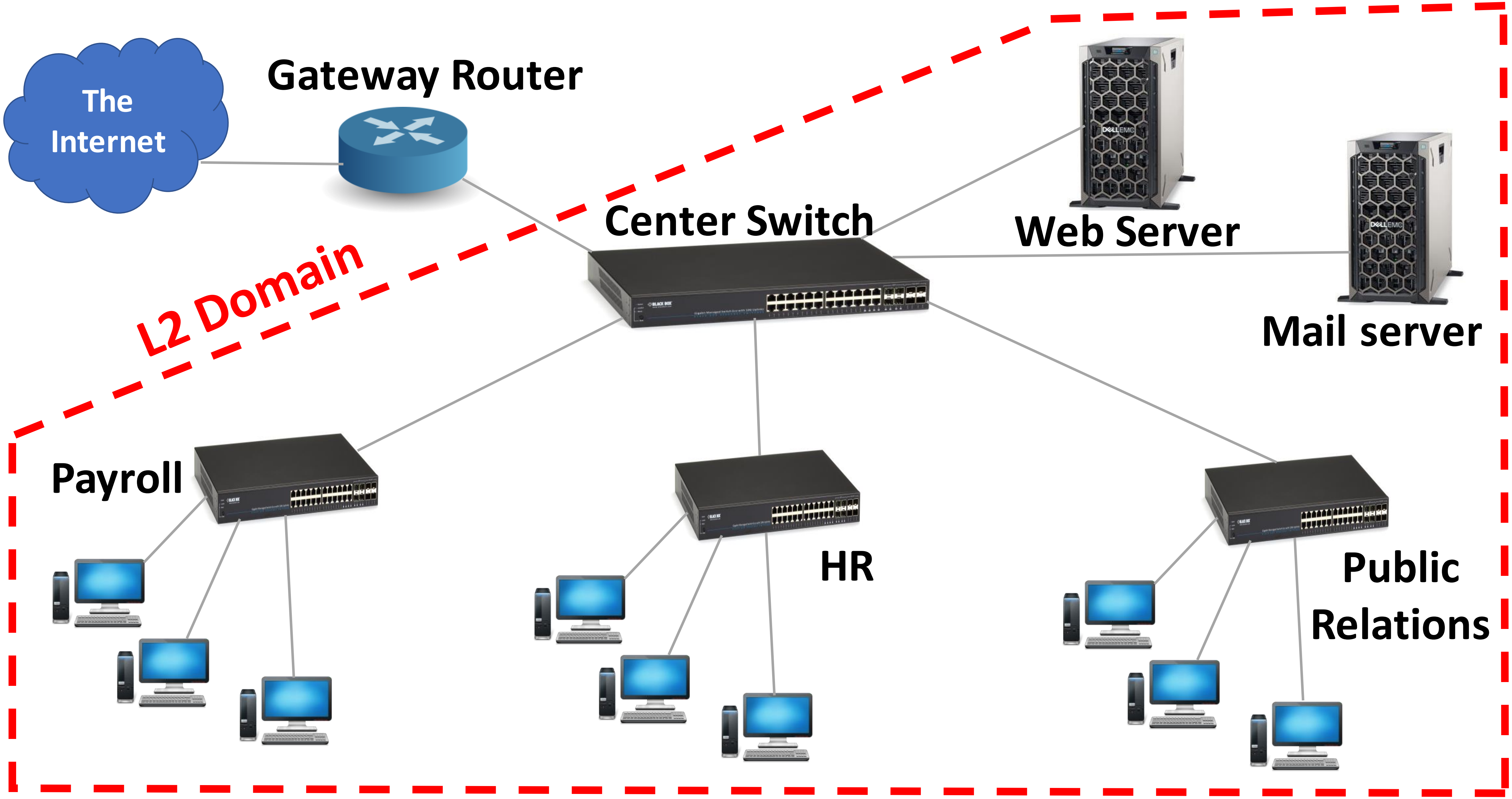


FF:FF:FF:FF:FF:FF

6 bytes	6 bytes	2 bytes	46-1500 bytes	0-46 bytes	4 bytes
Destination	Source	Type	Data	Padding	CRC

An Ethernet Frame

Hierarchical Switched LANs



Your Turn 1

Modern institutional LANs (an example illustrated in the previous slide) are often configured hierarchically, with each workgroup (department) having its own switch LAN connected to the switch LANs of other groups via a switch hierarchy.

- What drawbacks do you possibly identify in such a configuration? Briefly justify your answers.

Hierarchical Configuration Drawbacks

- Such a configuration has the following drawbacks:
  - **Lack of Traffic Isolation:**
    - Switch hierarchy localizes group traffic to within a single switch.
    - Broadcast traffic (frames carrying ARP or DHCP messages).
    - Frames whose destinations have not been learned by a switch yet.
    - Limiting the scope of such broadcast traffic can improve LAN performance & enhance group's security and privacy.
    - A router can be used instead of a switch, but routers do not support 'plug & play' and they are usually more expensive than a switch.
  - **Inefficient Use of Switches:**
    - LAN Traffic can be managed by just one switch if the switch provides desired traffic isolation.
  - **Managing Users:**
    - If users move between departments (workgroup), the physical cabling must be changed.

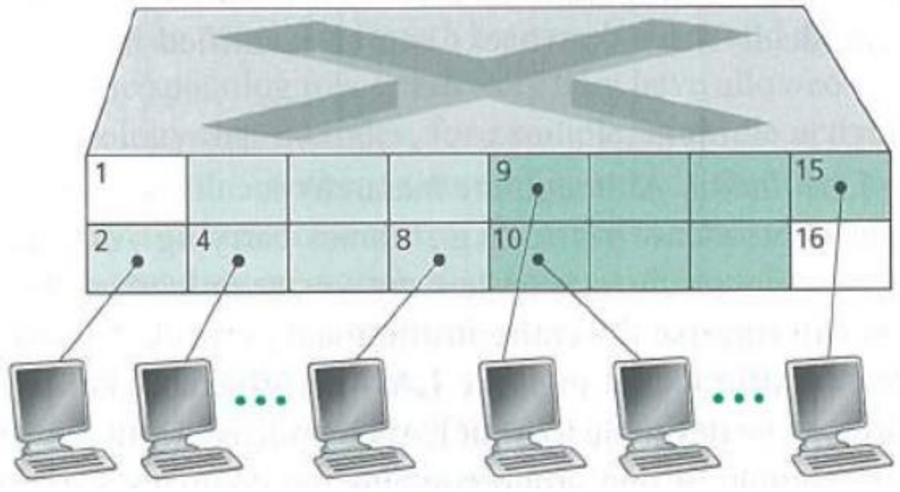
Each of these difficulties can be handled by a switch that supports Virtual Local Area Networks (VLANs).

Virtual Local Area Networks (VLANs)

- A VLAN is a subnetwork which can group together collections of devices on separate physical Local Area Networks (LANs).
- As its name suggests, a switch that supports VLANs allows multiple virtual LANs to be defined over a single physical LAN infrastructure. A VLAN can divide a physical LAN into small pieces of virtual LAN to contain broadcast traffic in a limited, reasonable range. In technical terms, it breaks the network into different broadcast domains.
- VLANs make it easy for network administrators to partition a single switched network to match the functional and security requirements of their systems without having to run new cables or make major changes in their current network infrastructure.
- There are different types of VLANs:
  - Port-based VLANs: Switch's ports (i.e. Interfaces) are divided into virtual groups.
  - MAC-based VLANs: Set of MAC addresses that belong to a VLAN.
  - Network-layer-protocol VLANS: VLANs based on IPv4, IPv6, etc.

Port-based VLAN

- A switch's ports (interfaces) are divided into groups by network administrator.
- Each group constitutes a VLAN, with the ports in each VLAN forming a broadcast domain.
  - Hosts in different VLANs cannot communicate with each other directly (isolation)
  - One switch is enough for Payroll and HR (efficient resources utilization)
  - Hosts can move between different VLANs with a simple reconfiguration of VLANs (easy network management)



Payroll (VLAN ports 2-8) HR(VLAN ports 9-15)

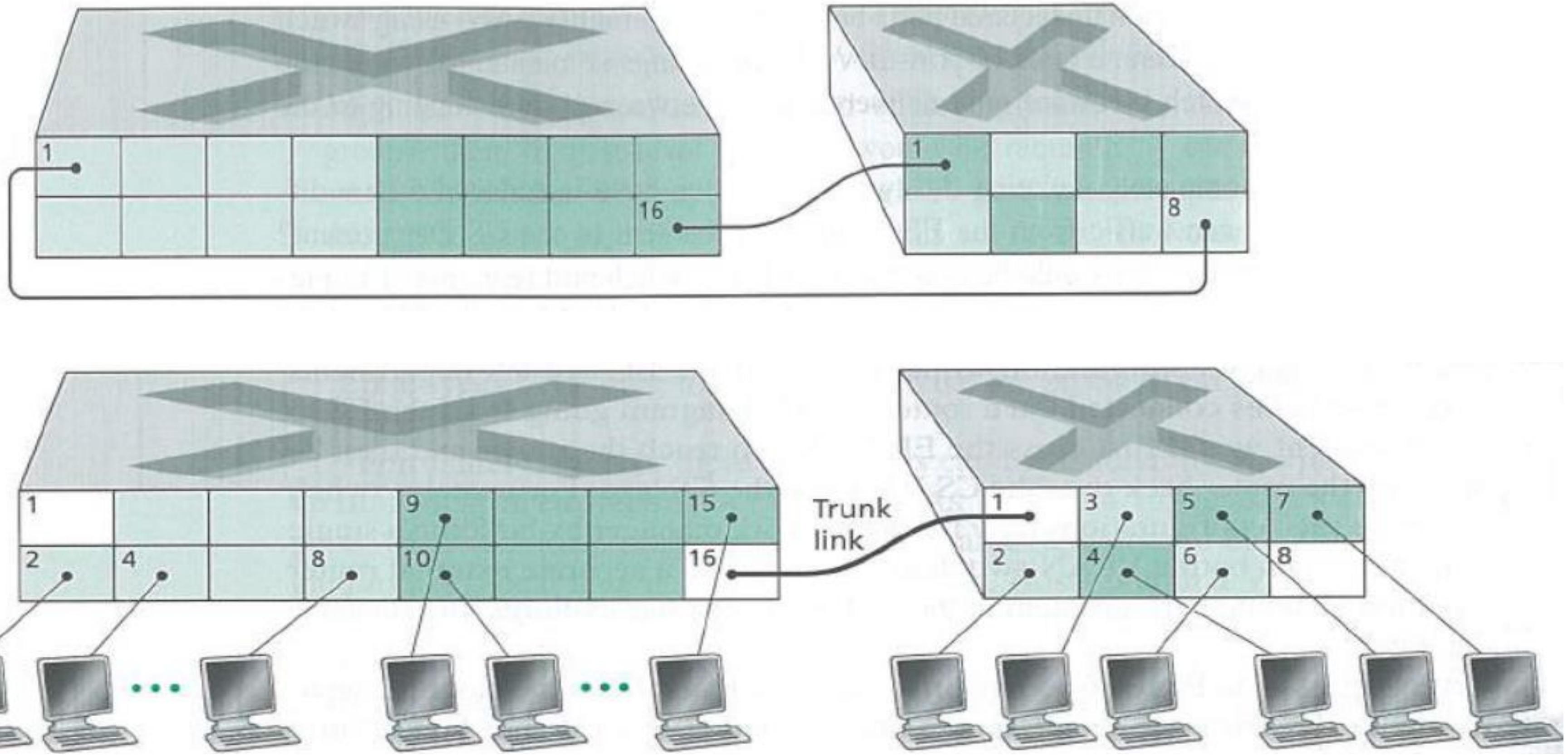
Your Turn 2

Assume payroll and HR departments do not have enough space and some of their employees need to move to a new building where they need network access and of course they need to be part of their VLAN. The new building has its own switch and required VLANs have been configured on the new switch in advance.

- How the new switch can be connected to the existing one? Discuss possible limitations of your proposed solution.

VLAN Trunk

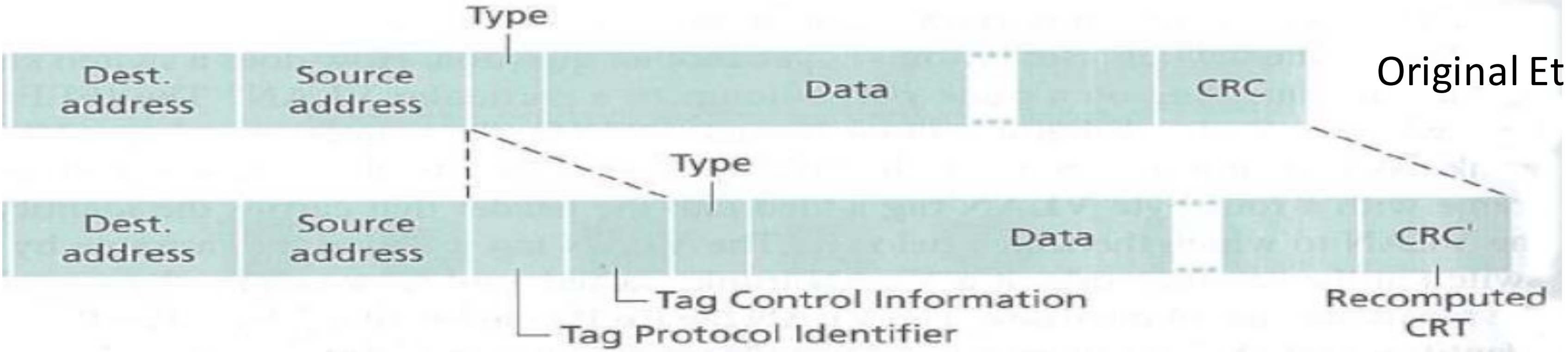
- A host can be assigned to any VLAN regardless of geographic location, if the switches are connected by trunk links.



Payroll (VLAN ports 2-8) HR(VLAN ports 9-15) Payroll (VLAN ports 2,3,6) HR(VLAN ports 4,5,7)

VLAN Trunk

- VLAN trunking is a scalable approach to interconnecting VLAN switches.
- A trunk port is configured on each switch.
- Trunk ports belongs to all VLANs configured on a switch.
- Frames sent to any VLAN are forwarded over the trunk link to the other switch.
- How does a switch know that a frame arriving on a trunk port belongs to a particular VLAN?
  - Extended frame format, defined in IEEE 802.1Q, for frames crossing a VLAN trunk (4-byte VLAN tag).



Original Ethernet Frame

802.1Q tagged Ethernet VLAN Frame

VLAN Hopping

- The basic concept behind all VLAN hopping attacks is for an attacking host on a VLAN to gain access to traffic on other VLANs that would normally not be accessible.
- There are two primary methods of VLAN hopping:
  - **Switch spoofing**
  - **Double tagging**
- Both attack vectors can be mitigated with proper switch port configuration.
- On a switch, a port is either configured as an access port or a trunking port.
- An access port is typically used when connecting a host to a switch. With the implementation of VLANs, each access port is assigned to only one VLAN.
- A trunking port is used when connecting two switches or a switch and a router together. Trunking ports allow for traffic from multiple VLANs.

Switched Spoofing VLAN Attack

- A trunk port can be configured manually or created dynamically using Dynamic Trunking Protocol (DTP).
- DTP is a Cisco proprietary protocol where one use is to dynamically establish a trunk link between two switches.
- An attacker acts as a switch in order to trick a legitimate switch into creating a trunking link between them.
- The attacker will send DTP packets and tries to negotiate a trunk with a switch. Once the trunk link is established, the attacker then has access to traffic from any VLAN. This exploit is only successful when the legitimate switch is configured to automatically negotiate a trunk (i.e. using DTP).
- **Mitigation:**
  1. Ensure that ports are not set to negotiate trunks automatically by disabling DTP.
  2. Ensure that ports that are not meant to be trunks are explicitly configured as access ports.

Double Tagging

- **Native VLAN**
  - In some cases, an untagged frame will arrive on a tagged port. To handle this, tagged ports have a special VLAN configured on them called the untagged VLAN. This is also known as the ‘native VLAN’.
  - The switch assigns any untagged frame that arrives on a tagged port to the native VLAN. If a frame on the native VLAN leaves a trunk (tagged) port, the switch strips the VLAN tag out.
- The idea behind the double tagging attack is that the attacker is connected to an interface in access mode with the same VLAN as the native untagged VLAN on the trunk. The attacker sends a frame with two 802.1Q tags, the “inner” VLAN tag is the VLAN that we want to reach and the “outer” VLAN tag is the native VLAN. When the switch receives the frame, it will remove the first (native VLAN) 802.1Q tag and forwards the frame with the second 802.1Q tag on its trunk interface(s). The attacker has now “jumped” from the native VLAN to the victim’s VLAN.
- **Mitigation:**
  1. Assign an access VLAN other than VLAN 1 (i.e. the default VLAN) to every access port.
  2. Change the native VLAN on all trunk ports to an unused VLAN ID.

Your Turn 3

Consider a secure web server on a VLAN called VLAN2. Hosts on VLAN2 are allowed access to the web server; hosts from outside VLAN2 are blocked. An attacking host on a separate VLAN, called VLAN1(Native), creates a specially formed packet to attack the web server. It places a header tagging the packet as belonging to VLAN2 under the header tagging the packet as belonging to VLAN1. When the packet is sent, the switch sees the default VLAN1 header and removes it and forwards the packet. The next switch sees the VLAN2 header and puts the packet in VLAN2. The packet thus arrives at the target server as though it was sent from another host on VLAN2, ignoring any layer 3 filtering that might be in place.

- What type of VLAN hopping is that? How can you mitigate such attack?