**IEEE 802.1Q**

***A. What (What is the IEEE 802.1Q)?***

IEEE 802.1Q is a networking standard that defines VLAN tagging. It allows multiple virtual LANs (VLANs) to share the same physical link. Think of it like creating separate, isolated networks within a larger network infrastructure. It adds a tag to Ethernet frames to identify which VLAN they belong to.

***B. Who (Who invented IEEE 802.1Q)?***

Primarily network engineers, network administrators, and IT professionals who design, implement, and manage networks. It's also relevant to vendors *(nhà cung câp)* of networking equipment (switches, routers, etc.) as they need to implement the standard.

***C. When (When the IEEE 802.1Q was established)?***

802.1Q was initially standardized in 1998 and has been revised and updated since then. It's used whenever VLANs are implemented in a network, which is common in enterprise networks, data centers, and even some home networks.

***D. Where (Where the IEEE 802.1Q was established)?***

802.1Q operates on Layer 2 (Data Link Layer) of the OSI model. It's implemented in network devices like switches and routers. It's relevant wherever Ethernet networks are used.

***E. Why (Why did the IEEE 802.1Q was established)?***

The primary reason for 802.1Q is to improve network efficiency, security, and manageability. VLANs allow you to segment a network, isolating traffic between different groups of users or devices. This enhances security (e.g., keeping guest Wi-Fi separate from the corporate network), improves performance (by reducing broadcast traffic in each VLAN), and simplifies network administration.

***F. How (How did the IEEE 802.1Q was established)?***

02.1Q achieves VLAN tagging by adding a 4-byte tag to the Ethernet frame header. This tag includes the VLAN ID (VID), which identifies the specific VLAN the frame belongs to. Switches that are 802.1Q-aware can then forward frames based on their VID, ensuring that traffic stays within the correct VLAN. This tagging allows multiple VLANs to share the same physical link, as the switches can distinguish between them based on the tags.

**\*What if WITHOUT IEEE 802.1Q:**

**- Big, messy network:** Everyone on the same "line," like a crowded room.

**- Slow traffic:** Lots of unnecessary chatter, like everyone talking at once.

**- Security holes:** Easy for anyone to eavesdrop or cause trouble.

**- Hard to manage:** Like trying to organize a huge, disorganized party.

**- Expensive:** Would need lots more equipment to try to separate things.

=> Basically, networks would be a lot less useful and much more problematic.

**IEEE 802.1Q ELEMENTS**

**I. The 802.1Q Tag (Thẻ 802.1Q)**

This is the heart of 802.1Q. It's a 4-byte field inserted into the Ethernet frame header. Think of it as ***a label that tells network devices*** which VLAN the frame belongs to. Here's what's inside:

**+ Tag Protocol Identifier (TPID: Định danh giao thức thẻ):** 2 bytes. This identifies the frame as an 802.1Q tagged frame. It's like saying, "Hey, I'm carrying VLAN information!"

**+ Tag Control Information (TCI: Thông tin điều khiển thẻ):** 2 bytes. This contains the actual VLAN information:

* **Priority Code Point (PCP: Điểm Mã Ưu Tiên):** 3 bits. Used for Quality of Service (QoS). It lets you prioritize certain types of traffic (like voice or video) to ensure they get through smoothly.
* **Drop Eligible Indicator (DEI: Chỉ báo Đủ điều kiện Loại bỏ):** 1 bit. A flag that indicates whether the frame can be dropped if there's congestion.
* **VLAN Identifier (VID: Định danh VLAN):** 12 bits. This is the actual VLAN number, ranging from 1 to 4094. It's what identifies which virtual network the frame belongs to.

**II. VLAN Trunking**

This is how 802.1Q allows multiple VLANs to share the same physical link.

* **Trunk Link:** A link (usually between switches) that carries traffic for multiple VLANs. It's like a multi-lane highway for network traffic.
* **Tagging and Untagging (Gắn thẻ và Gỡ thẻ):** When a frame enters a trunk link, the switch adds the 802.1Q tag. When it leaves the trunk link, the tag is removed. This ensures that frames are delivered to the correct VLAN.

**3. VLAN-Aware Devices**

These are the devices (primarily switches) that understand and can process 802.1Q tags.

**Switch Ports:** Switches have different types of ports:

**+ Access Ports (Cổng truy cập):** Connect to end devices (like computers). These ports are typically assigned to a single VLAN.

**+ Trunk Ports (Cổng Trunk):** Connect to other switches and carry traffic for multiple VLANs.

**+ Hybrid Ports (Cổng Hỗ Trợ):** Can act as both access and trunk ports.

**4. VLAN Configuration**

Network administrators need to configure VLANs on switches. This involves:

* **Creating VLANs:** Assigning a VID and name to each VLAN.
* **Assigning Ports to VLANs:** Specifying which ports belong to which VLANs.
* **Configuring Trunk Links:** Enabling trunking on the appropriate ports.

**5. Inter-VLAN Routing**

Since VLANs are isolated from each other, you need a way for devices in different VLANs to communicate. This is usually done with a router or a Layer 3 switch.

* **Router or Layer 3 Switch:** Acts as a gateway between VLANs, forwarding traffic between them.

**Key Concepts to Remember:**

* **Broadcast Domain (Miền Quảng Bá):** A network segment where all devices can hear each other's broadcasts. VLANs create separate broadcast domains. => Layer 2: Data Link Layer
* **Collision Domain (Miền Xung Đột):** A network segment where devices share the same transmission medium. VLANs can help reduce collision domains. => Layer 1 (Physical Layer)