

032

TECHNICAL NOTE

Gary Macknofsky, Product Specialist, Transport and Datacom Business Unit

The terms VLAN and Q in Q are common in Ethernet technology. While both these notions are beneficial to Ethernet networking, it is important to understand the basics so as to better comprehend their advantages. This article defines these terms, describes their benefits and provides concrete examples of how Q in Q and VLANs are used.

What is Q in Q?

Q in Q is an informal industry term that refers to the doubling up of IEEE 802.1Q. More commonly though, Q in Q is also known as virtual local-area network (**VLAN**) *stacking* or *double-tagging*.

In the early days of networking, everything had to be physically connected to each other to be part of the same network. Unfortunately, sometimes in larger buildings with multiple floors, it became an expensive proposition to get people on the tenth floor connected to the same physical network as the people on the second floor. Imagine the cost to physically move everyone from one floor to the next just to get on the same physical local-area network (LAN)!

With the advent of IEEE 802.1Q, VLANs were born. These virtual networks offered a new networking solution that could offer QoS due to its priority scheme and cost-saving solutions for businesses. With VLANs, there was no longer a need to physically move around office employees to connect them to the same network as their counterparts on different floors.

With the help of a few Ethernet switches, the employees on the tenth floor could get all their traffic tagged with the same VLAN ID as the employees on the second floor. This method allowed them to be on the same network "virtually", and thus eliminate the expensive moving costs.

In short, a VLAN is a group of computers on one or more LANs that are configured so that they can talk to each other as if they were attached to the same wire. The real truth is that these computers are actually spread out on different LAN segments, as VLANs are based on logical connections instead of physical connections.

VLAN Benefits

1. **Better performance than a routed network** - A network that uses VLAN technology is a switched network and therefore will perform better than a routed network, mainly because of the routing overhead required. In a switched network, when using a shared link, the size of each VLAN can be decreased, which results in fewer collisions because each VLAN is an independent collision domain as far as the network layer is concerned. Furthermore, it is also possible to group a large LAN based on some logic to smaller VLANs and reduce broadcast traffic overall as each broadcast will be sent on to the relevant VLAN only.
2. **Easier network management** - Configuring large networks using VLAN technology is relatively easy. Even if the networks are spread across large geographic distances, an administrator is able to manage the entire global network from a single location; i.e., where the main switching is done. Additionally, a VLAN requires very little overhead if it uses ports, as this reduces the managerial burden even more for some networks.
3. **Physical-layer independence** - VLANs are not dependent on the physical topology and medium over which the network is connected. It is possible to use VLAN technology over a network consisting even of different physical mediums and, on the user

level, this will be completely transparent. In addition, the network can span across a large physical distance and even go through an ATM cloud while remaining transparent to the users of the same VLAN, which could be accessed from different countries around the globe.

4. **Better security** - VLANs provide inherent security to the network by delivering the frames only within the destined VLANs (when sending broadcasts) and to the specific recipient within the destined VLAN (when sending a regular frame). This makes it much harder to sniff the traffic across the switch as this would require locating the exact specific port, which allows for extra security. Furthermore, when dividing users by VLANs, it is possible to make the division according to a security policy and offer sensitive data only to users on a given VLAN without exposing the information to the entire network.
5. **Cost** - Using a network switched with VLANs is cheaper than creating a routed network with expensive routers as routers cost a lot more than switches in general.

Q in Q – Advantages and Example

Using Q in Q (i.e., VLAN stacking), a service provider can assign different service-provider (SP-VLANs) to different customer traffic. This guarantees a separation between each customer's traffic within the service provider network. Customers' VLANs are then moved transparently inside the service provider's network. The original customers' VLANs get encapsulated by the SP-VLAN, allowing transparent LAN service (TLS).

For example as shown in Figure 1, corporate headquarters A wants to send information to its branch office, which we will call branch office AA. Despite the fact that both locations are 1000 miles apart from each other, they do have one thing in common; that is, the same VLAN ID. Both A and AA use a VLAN ID of 100; this is called the *customer-edge VLAN* (CE-VLAN).

In order to get information from A to AA, traffic will have to be routed onto the carrier's backbone to transport the data from end to end. This normally would not be an issue; however, this situation actually poses a security risk. Unfortunately, the carrier has another customer, who we will call corporate headquarters as D and who is also trying to send data to his branch office, that we will call DD. Corporate headquarters D also uses the exact same VLAN ID of 100. Since both customers are using the same VLAN ID, the possibility of traffic being mixed together could make all transactions non-secure.

The easiest way for the carrier to ensure security to customers is to encapsulate the original VLAN from A and AA with a second VLAN ID of 32. This is known as the SP-VLAN. For D and DD, the service provider will use a second SP-VLAN of 48. The SP-VLAN is added on as the data enters the service provider's network and then removed as it exits.

With the help of the newly ratified IEEE 802.1ad, service providers now have the added ability to retain all of their customers' VLANs with all security issues resolved.

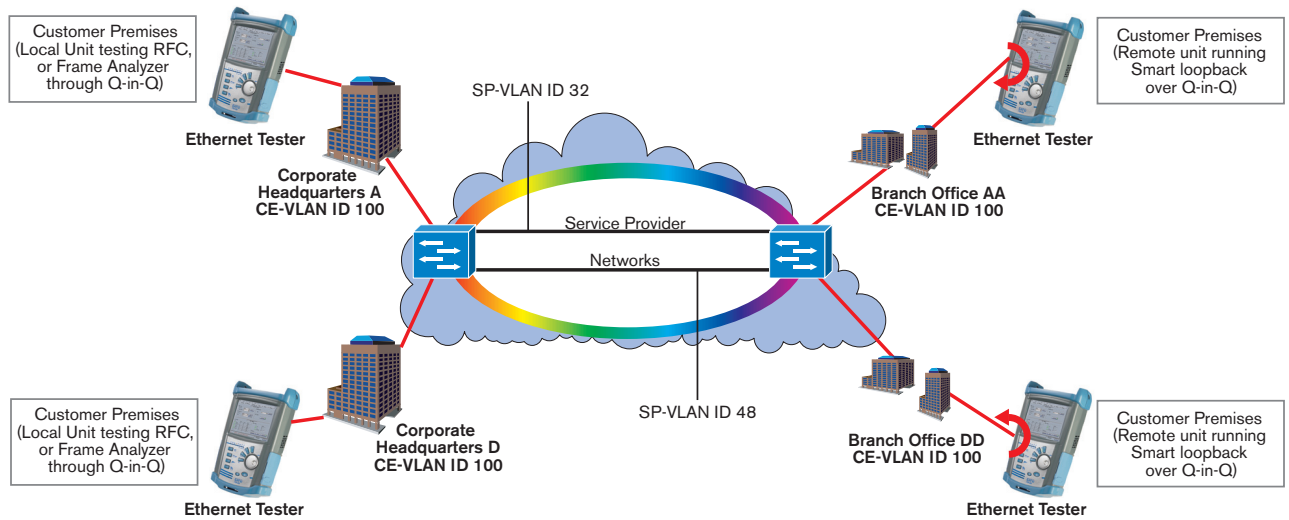


Figure 1: Q in Q example (802.1ad)

VLAN Tag in the Ethernet Frame

The VLAN tag is a two-byte tag used to identify the traffic circulating on the VLAN; it basically indicates the origin and destination of the frame transmission. The first three bits of the VLAN tag indicate the priority of the traffic that is included in the packet. This allows for some basic QoS assurance, which ensures that critical data can pass through the network quickly with as little delays as possible. The value of this field can be generated at the end station and updated on every switch (VLAN-aware) along the way as well.

The fourth bit is a canonical format indicator (CFI), which is used mainly for 802.3 source routing information.

The last 12 bits comprise the VLAN identifier (VID), which enable the creation of 4094 VLANs (VID=0 and 4096 are reserved).

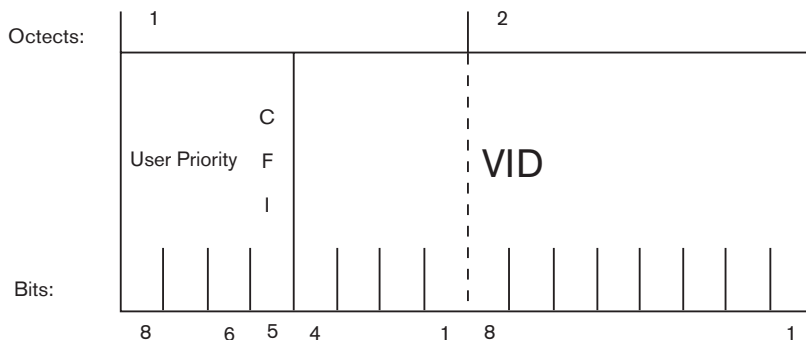


Figure 2: VLAN tag in Ethernet frame

An Ethernet frame with Q in Q looks like a VLAN-tagged frame, except that it has two tags instead of one. In Figure 3, shown below, you can see an original Ethernet frame, VLAN tagged frame and a VLAN stacked frame (Q in Q)

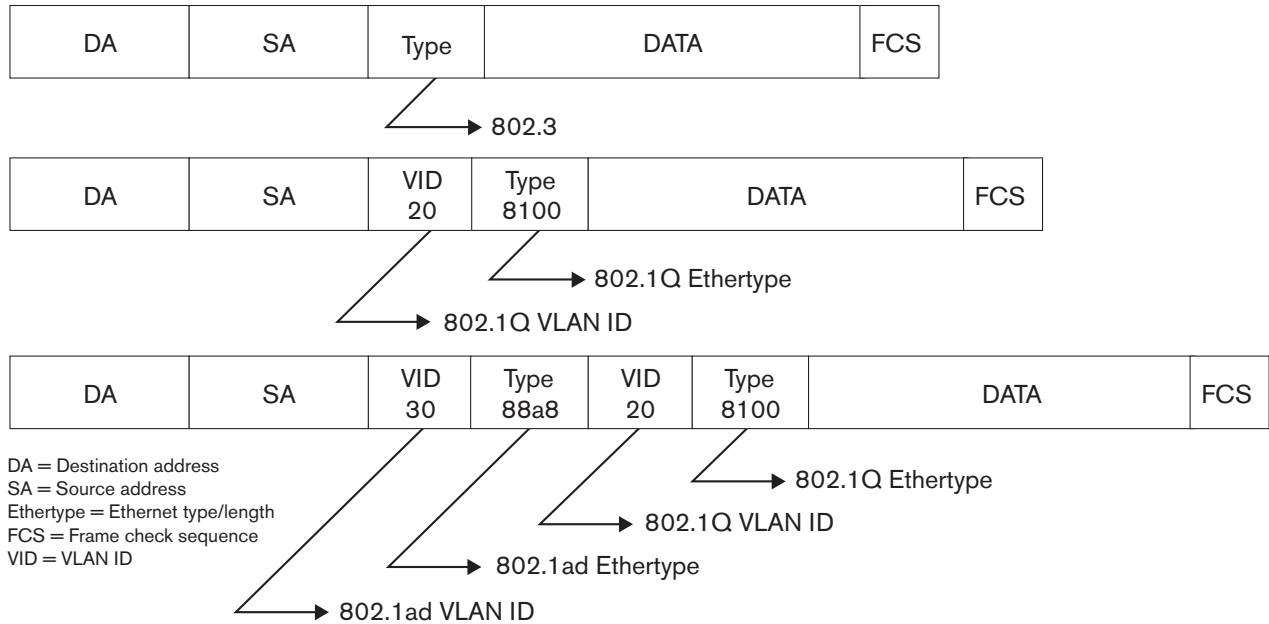


Figure 3: Ethernet, 802.1Q and 802.1ad frames

Additional Capability with the FTB-8510 Packet Blazer Ethernet Test Module

The FTB-8510 can perform RFC 2544 and frame analysis tests end to end, through three different VLAN tags and priorities. The traffic analysis feature can also filter on any of the three VLANs or their respective priority.

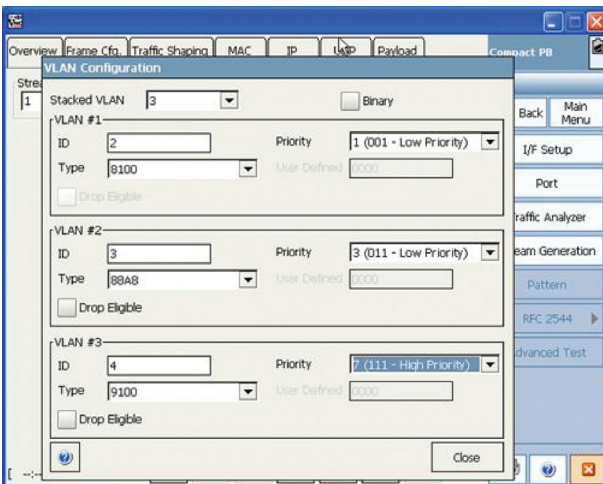


Figure 4: Q-in-Q feature on Packet Blazer

By default, the Packet Blazer selects an Ethertype of 8100 for the first VLAN and 88a8 for the second VLAN. These Ethernets have been standardized in IEEE 802.1Q for the first one, and IEEE 802.1ad for the second one. The Packet Blazer can also select Ethernets such as 9100, 9200, 9300 and user-defined types for any of the three VLANs.



EXFO Corporate Headquarters > 400 Godin Avenue, Quebec City (Quebec) G1M 2K2 CANADA | Tel.: 1 418 683-0211 | Fax: 1 418 683-2170 | info@EXFO.com

Toll-free: 1 800 663-3936 (USA and Canada) | www.EXFO.com

EXFO America	3701 Plano Parkway, Suite 160	Plano, TX 75075 USA	Tel.: 1 800 663-3936	Fax: 1 972 836-0164
EXFO Europe	Omega Enterprise Park, Electron Way	Chandlers Ford, Hampshire S053 4SE ENGLAND	Tel.: +44 2380 246810	Fax: +44 2380 246801
EXFO Asia	151 Chin Swee Road, #03-29 Manhattan House	SINGAPORE 169876	Tel.: +65 6333 8241	Fax: +65 6333 8242
EXFO China	No.88 Fuhua, First Road Central Tower, Room 801, Futian District	Shenzhen 518048, CHINA	Tel.: +86 (755) 8203 2300	Fax: +86 (755) 8203 2306
	Beijing New Century Hotel Office Tower, Room 1754-1755 No. 6 Southern Capital Gym Road	Beijing 100044 P. R. CHINA	Tel.: +86 (10) 6849 2738	Fax: +86 (10) 6849 2662

