- **EEE 802.1q Identification Method**

Created by the IEEE as a standard method of frame tagging and vendor independent. IEEE 802.1q actually inserts a field into the frame to identify the VLAN. If you're trunking between a Cisco switched link and a different vendor switch, you've got to use 802.1q for the trunk to work. Unlike ISL, which encapsulates the frame with control information, 802.1q inserts an 802.1q field along with tag control information, as shown in Figure 3.5 below.

For the Cisco exam objectives, it's only the 12-bit VLAN ID that matters. This field identifies the VLAN and can be 212, minus 2 for the 0 and 4,095 reserved VLANs, which means an 802.1q tagged frame can carry information for 4,094 VLANs. It works like this: You first designate each port that's going to be a trunk with 802.1q encapsulation. The other ports must be assigned a specific VLAN ID in order for them to communicate. VLAN 1 is the default native VLAN, and when using 802.1q, all traffic for a native VLAN is untagged. The ports that populate the same trunk create a group with this native VLAN and each port gets tagged with an identification number reflecting that. Again the default is VLAN 1. The native VLAN allows the trunks to accept information that was received without any VLAN identification or frame tag

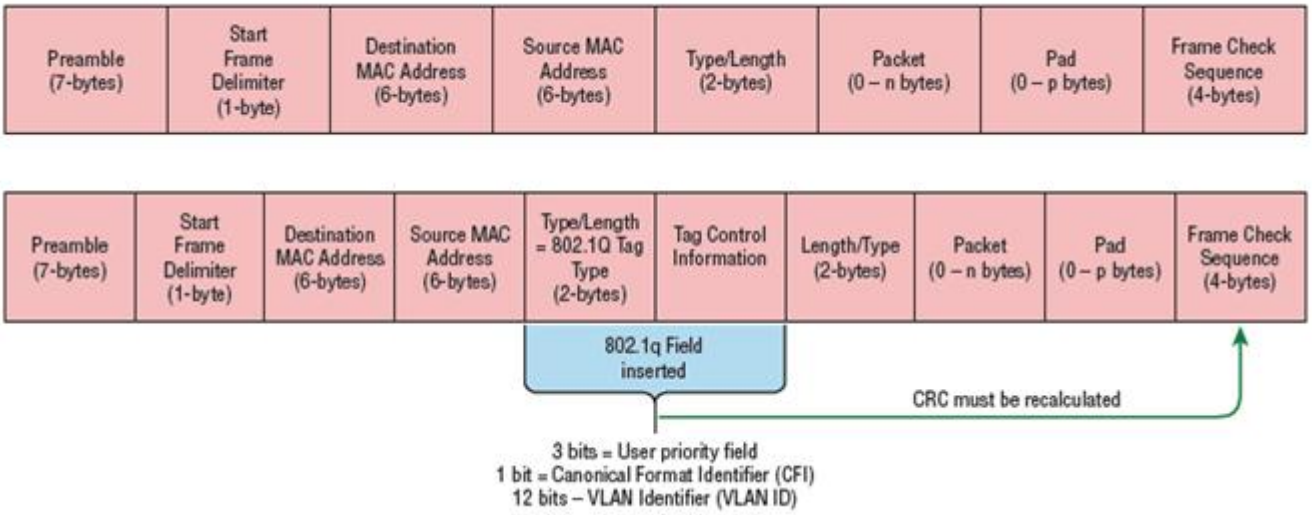

Figure 4: IEEE 802.1q encapsulation with and without the 802.1q tag (**source:** CCNA Routing and Switching, 2013)
Most 2960 model switches only support the IEEE 802.1q trunking protocol, but the 3560 will support both the ISL and IEEE methods

10. Creating And Configuring Vlans

It is easy to create and configure VLAN. One has to decide on the number of VLANs you want to create and establish which users you want in each VLAN, by that one brings an idea of VLAN models into the real world. To configure VLANs on a Cisco Catalyst switch via the Cisco IOS Command Line Interface (CLI), use the *global config vlan command.* Below is an example demonstrating how to configure VLANs on the S1 switch by creating three VLANs for three different departments—Sales, Marketing and Accounting again. Remember that VLAN 1 is the native and management VLAN by default:

```
S1(config)#vlan ?
  WORD        ISL VLAN IDs 1-4094
  access-map  Create vlan access-map or enter vlan access-map command mode
  dot1q       dot1q parameters
  filter      Apply a VLAN Map
  group       Create a vlan group
  internal    internal VLAN
S1(config)#vlan 2
S1(config-vlan)#name Sales
S1(config-vlan)#vlan 3
S1(config-vlan)#name Marketing
S1(config-vlan)#vlan 4
S1(config-vlan)#name Accounting
S1(config-vlan)#^Z
S1#
```

Figure 5: Creating VLAN in CLI (**source:** CCNA Routing and Switching, 2013)

From the output of *figure 5* above, we saw up to 1 to 4094 VLANs. But invariably only 1001 VLANs can be created, and you can't use, change, rename, or delete VLANs 1 or 1002 through 1005 because they're reserved. The VLAN numbers above 1005 are called extended VLANs and won't be saved in the database unless your switch is set to what is called VLAN Trunk Protocol (VTP) transparent mode. You won't see these VLAN numbers used too often in production. After you create the VLANs that you want, you can use the "*show vlan command*" to check them out. By default, all ports on the switch are in VLAN 1. To change the VLAN associated with a port, you need to go to each interface and specifically tell it which VLAN to be a part of. Once the VLANs are created, one can verify it with the show "*vlan command."*

11. Inter-VLAN Routing

The major problem in VLAN is; how can users from one VLAN (broadcast domain), use services offered by another VLAN. Each network has its own needs, though whether it's a large or small network, internal routing, in most cases, is essential. The ability to segment your network by creating VLANs, thus reducing network broadcasts and enhancing security is a technique used by most engineers. Popular setups include a separate broadcast domain for critical

services such as File Servers, Print servers, Domain Controllers and other servers.

Inter-VLAN routing is process of forwarding network traffic from one VLAN to another VLAN using a router. In the previous pages, we learned about how to configure VLANs on a network switch(s). To allow devices connected to the various VLANs to communicate with each other, you need to connect a router. In figure 2, for any host from EBSU Admin VLAN to send traffic to EBSU Database VLAN we deploy Inter-VLAN routing. Hosts in a VLAN live in their own broadcast domain and can communicate freely. VLANs create network partitioning and traffic separation at layer 2 of the OSI. Therefore, if you want hosts or any other IP-addressable device to communicate between VLANs, you must have a layer 3 device to provide routing services.

- **Inter-VLAN routing Implementation**

Using VLANs technology and protocols to segment a network can be useful to control broadcast traffic and implement security boundaries. However, allowing absolutely NO access between VLANs is never very beneficial. To fix this, we suppose to implement inter-VLAN routing. At the CCNA level, there are two ways we can make this happen namely:

a) Attach a unique router port to each VLAN
b) Implement a router on a stick.

12. Conclusion

Though there are some many problems facing network and data communication today but security has always been the most paramount challenge. Every efforts is always how to mitigate insecurity issues and ensure that information is communicated to appropriate destinations without compromise. This paper had adequately discussed the need of implementing Virtual Local Area Network (VLAN) and Inter-VLAN Routing technologies in Ebonyi State University Network. Going by the usual flat Local Area Network infrastructure where every users belong to one broadcast domain different series of network insecurities exist. In the case of an enterprise network having critical file servers, application servers, organisational databases and other confidential information, this would mean that all users would have equal access privileges to these resources. To effectively prevent such situations from operational network we need to restrict access at the network level by segmenting the existing network into different broadcast domains, hence, the need of Virtual Local Area Network (VLAN). In contrast to normally flat LAN architecture where every hosts are connected without segmentation; we break a large broadcast domain into different sizes of broadcast domains by creating Virtual Local Area Networks (VLANs). This VLAN architecture which is a logical grouping of network users and resources connected to administratively defined ports on a switch when deployed in Ebonyi State University Network would be of immense benefit as outlined in the work. In all, this work exhaustively x-rayed the benefits of VLAN and Inter-VLAN routing in managing and maintaining of Ebonyi State University Networks.

References

[1] Baker, R. H. (1995). *Network security*: How to plan for it and achieve it. New York: McGraw Hill, Inc.
[2] Chappell, L. A. and Hakes, D. E. (1994). *Novell's guide to NetWare LAN analysis*. 2nd ed. Alameda, CA: SYBEX Inc.
[3] Comer, D. E. (1995). *Internetworking with TCP/IP*, volume I: Principles, protocols, and architecture. 3rd ed. Upper Saddle River, NJ: Prentice Hall, Inc.
[4] Derfler, F. J. and Freed, L. (1996). *How Networks Work*. 2nd ed. Emeryville.
[5] Henry, P. D. and De Libero, G. (1996) *Strategic networking*: From LAN and WAN to Information superhighways. London: International Thomson Computer Press.
[6] Martin, J., Chapman, K. K., & Leben, J. (1994). *Local area networks: Architectures and implementations*. 2nd ed. New Jersey: P T R Prentice Hall, Inc.
[7] Passmore, D. and Freeman, J. (1998). *The virtual LAN technology report*. [online]. Available: http://www.3com.com/nsc/200374.html. (October 2, 1998)
[8] Roese, J. (1998) *Switched LANs: Implementation, operation, maintenance.* New York: McGraw-Hill, Inc.
[9] Roese, J. and Knapp, E. (1997). *SecureFast:* A comparative analysis of SecureFast and 802.1Q. Rochester, NH: Cabletron Systems, Inc.
[10] SecureFast services overview. (1998). Cabletron Systems product marketing white papers. Rochester, NH: Cabletron Systems, Inc.
[11] Tittel, E. and Robbins, M. (1994). *Network design essentials*. Cambridge, MA: AP Professional
[12] Virtual LAN communications. (1996). [online]. Available: http://cio.cisco.com/warp/public/614/13.html. (October 22, 1998)
[13] VLAN information. UC Davis Network 21. (1998). [online]. Available: http://net21.ucdavis.edu/newvlan.htm. (October 21, 1998)
[14] Institute of Electrical and Electronics Engineers (1998). IEEE P8021.Q, IEEE standards for local and metropolitan area networks: Virtual bridged networks. New York: Institute of Electrical and Electronics Engineers.
[15] CCNA Routing and Switching, 2013 cisco systems *Mega Guide, CCNA 640-802, www.preplogic.com*