

H.O. #7
Winter 98-99

IEEE 802.1Q

Virtual Bridged Local Area Networks

IEEE 802.1Q/D9 Standard:

`ftp://p8021:-go_wildcats@p8021.hep.net/8021/q-drafts/q9/q-d9.pdf`

Recommended Reading: Chapters 1, 5, 6, 8 (sections 8.1 through 8.4; 8.6; 8.8; 8.10) and Chapter 9

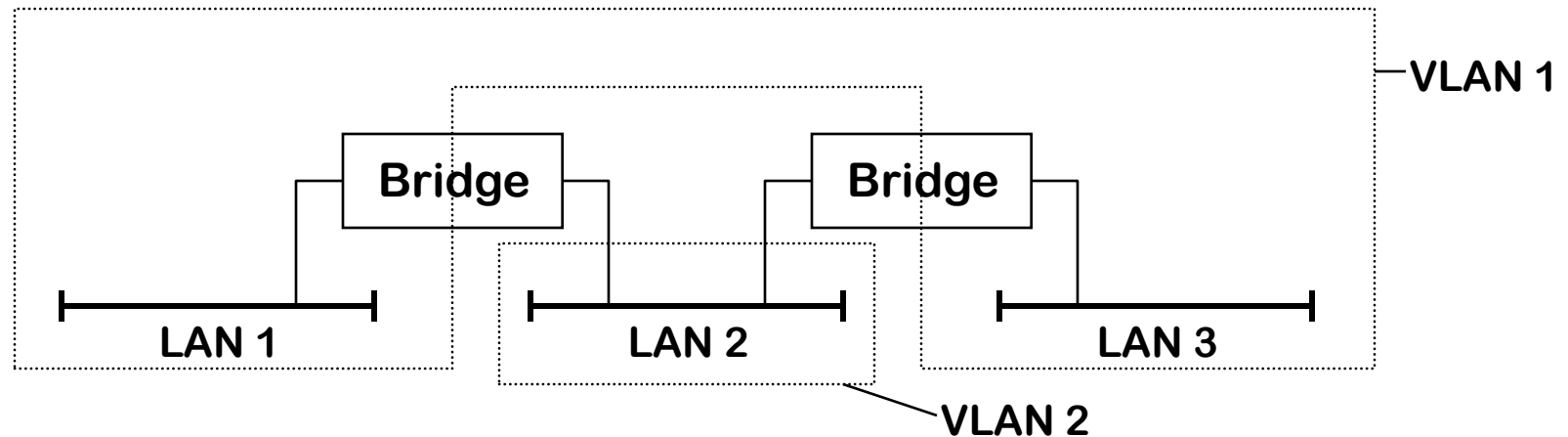
Motivation

- Increased bandwidth on LAN segments
- Larger LAN switches (number of ports)
 - larger subnetworks
 - geographical scope
 - number of users
- Same bridged LAN capable of serving several *logical groups* of users
 - groups defined according to a number of attributes
 - corporate divisions
 - higher layer protocols
 - collection of servers they share
 - etc...

Definition

- A virtual LAN (VLAN) is a collection of LAN segments and the stations/devices connected to them within a bridged LAN that has exactly the same properties of an independent LAN.
- In a bridged LAN comprising several VLANs, traffic belonging to a VLAN is restricted from reaching users in other VLANs

VLAN Example



- Stations in LAN1 and LAN3 can freely communicate and “believe” to be in the same LAN
- Stations in LAN2 cannot talk to stations on LAN1 or LAN3.
- LAN2 is still used to convey traffic between LAN1 and 3

Advantages

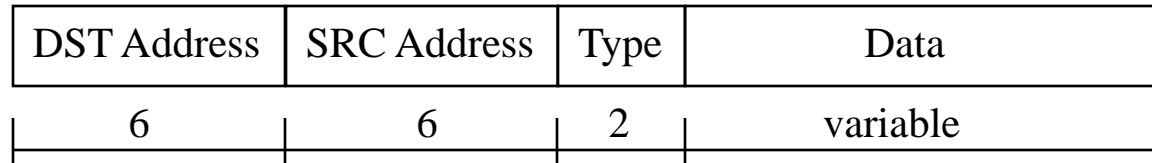
- Flexibility in user locations and logical groups of stations
- Facilitating easy administration of:
 - moves
 - adds
 - changes in group membership
- Restricting traffic on portion of network where stations belonging to a VLAN are present
- Goal:
 - compatibility with existing bridges and end-stations

VLAN Tags

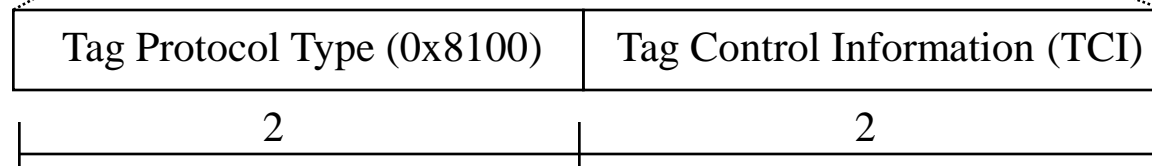
- Depending on the network topology, traffic between different physical parts of the same VLAN may need to be “tunneled” through segments not belonging to that VLAN.
- These “transit packets” must contain some additional information:
 - The VLAN they belong to (this is encoded as a 12-bit number, assigned by the network manager)
 - The frame priority (to convey priority information over LANs that do not support it)
 - Information about MAC addressing (for packets travelling between different kinds of LANs)

Inserting the VLAN tag (Ethernet)

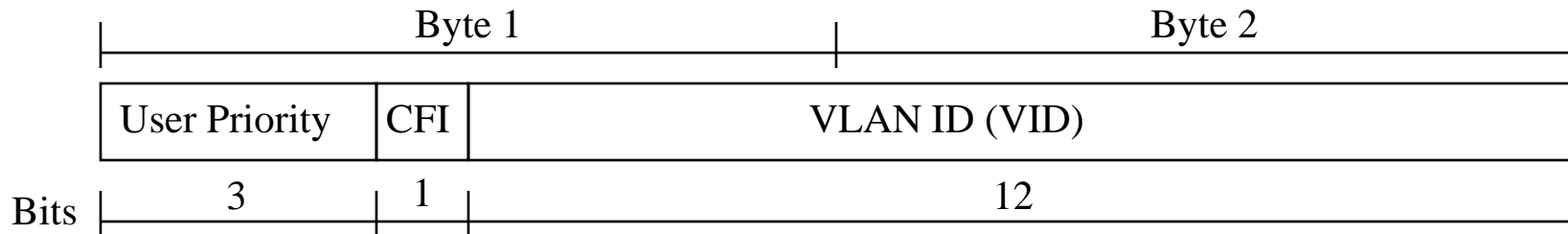
Original
Frame



Tagged
Frame



TCI Format



- **User Priority:** as defined in IEEE 802.1D
- **CFI (Canonical Format Indicator):** Specifies the bit ordering of the MAC addresses and the presence of source-routing data.
- **VID:** Identifies the VLAN. Values 0, 1 and 0xFFF are reserved.

Tagged and Untagged Frames

- Legacy stations and bridges (VLAN-unaware) do not handle tags
- Interoperation of VLAN-aware and VLAN-unaware devices requires the ability to handle mixtures of tagged and untagged frames

VLAN Registration (1)

- Static VLAN registration entries:
 - explicitly configured by management action for a given VID
 - specifying for each port whether the registration for the VID is:
 - Fixed
 - Forbidden
 - Normal registration (by GVRP)
 - specifying for each port whether frames on that VLAN (VID) are to be tagged or untagged when forwarded through the port

VLAN Registration (2)

- Dynamic VLAN registration entries:
 - VID of the LAN
 - port map with a control element for each outbound port specifying whether the VLAN is registered on that port
- Use of GARP VLAN Registration Protocol (GVRP) to create and propagate dynamic VLAN registration entries.

GVRP

- Operation of GVRP defines a single attribute type, the VID attribute type
- Value is a list of VIDs

Ingress Rules

- Identify the VID associate with a frame
 - If a VLAN tag exists, use the VID in the tag
 - If a VLAN tag exists with VID = 0 or if a VLAN tag does not exist, use a pre-assigned Port VID (PVID) (a VLAN tag with VID=0 is conveying priority info only, not VID info).
- Default PVID = 1
- If the Enable Ingress Filtering parameter is set, then frames are discarded if the Port is not in the member set (i.e., it is not part of the VLAN)

Egress Rules

- Determine whether or not a frame is forwarded on a port
 - takes into account VLAN info
- A frame is filtered if
 - The Port is not in the member set for the VID determined by the Ingress Rules
 - Port is in the untagged set and the bridge does not support the ability to translate from the canonical format to the format appropriate to the medium access method for the output port
- Untagged set - set of ports on which frames should be sent untagged

The Learning Process

- Deduce the port through which particular end stations can be reached
- Takes into account VID information (as determined by the Ingress Rules)
- If the Member Set for a VID is empty an entry is not created into the Filtering Database

Filtering Database

- Static and Dynamic entries
- FID (Filtering Identifier)
 - Identifies a set of VLANs amongst which shared VLAN learning takes place
 - A pair of FID's identifies two sets of VLANs between which independent learning takes place
 - Local significance to the bridge
- Allocation of VID's to FID's
- Member Set
- Untagged Set