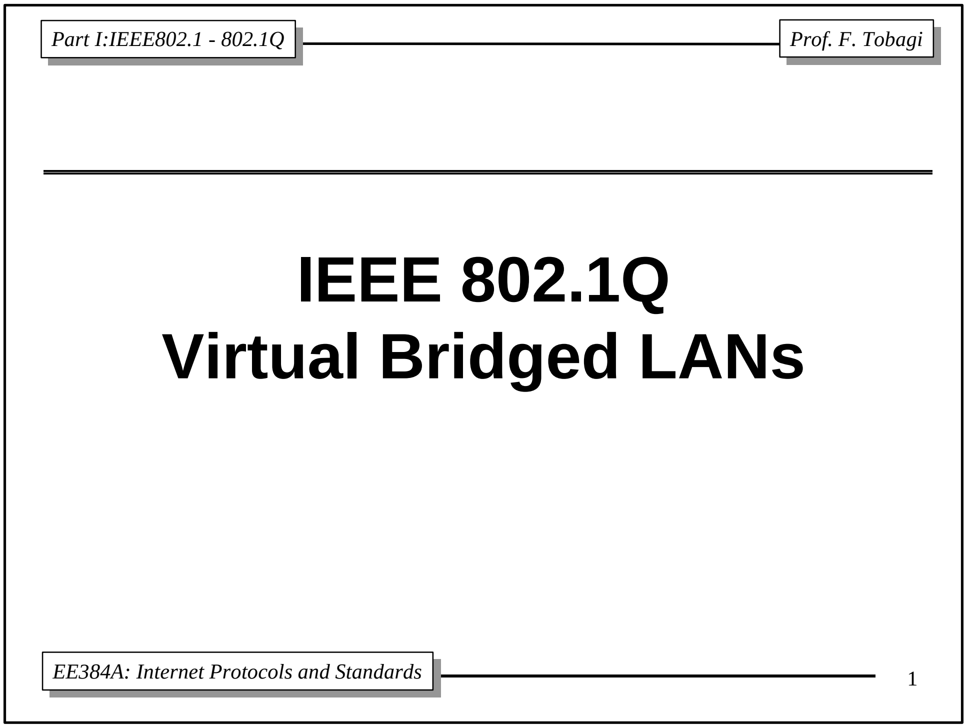
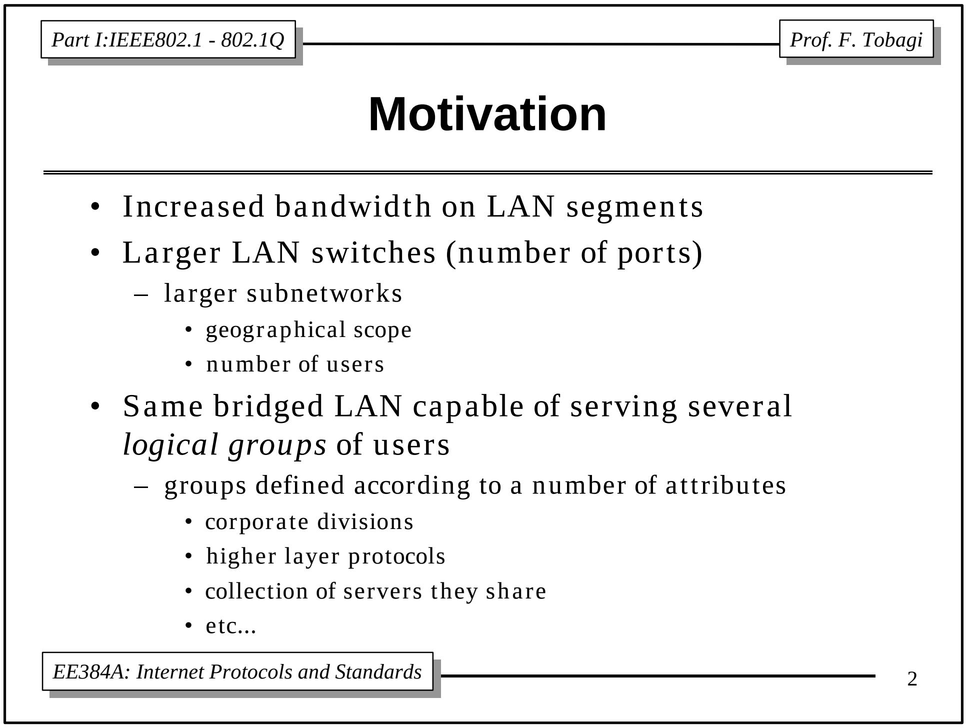
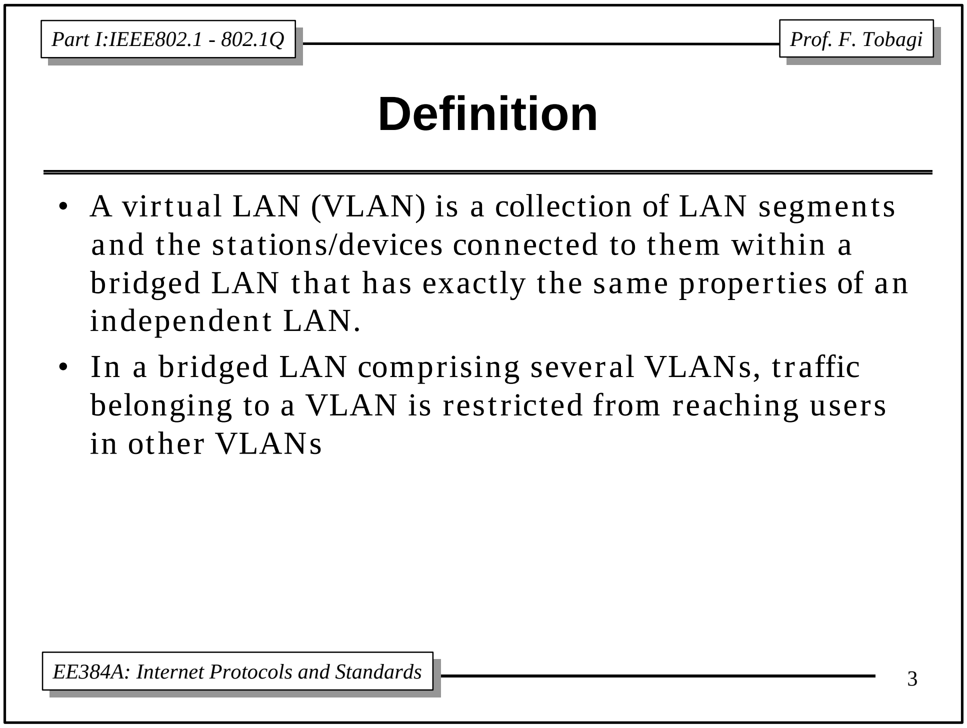


IEEE 802.1Q
Virtual Bridged LANs



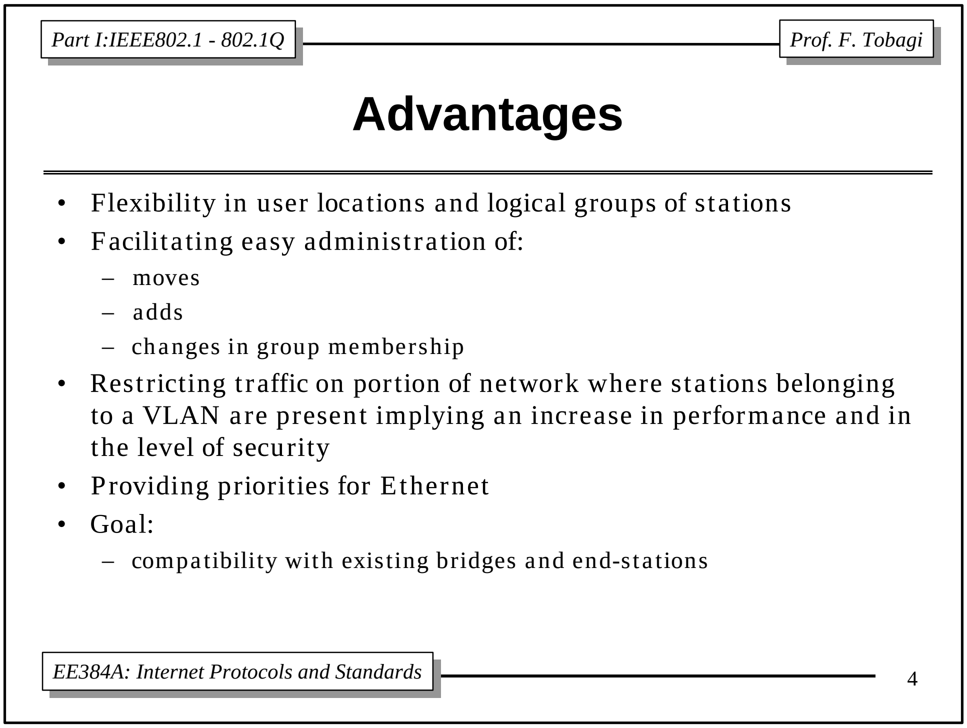
Motivation

- 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

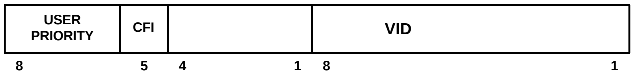
- A virtual LAN (VLAN) is a collection of LAN segments and the stations/devices connected to them within a bridged LAN that has exactly the same properties of an independent LAN.
- In a bridged LAN comprising several VLANs, traffic belonging to a VLAN is restricted from reaching users in other VLANs



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 implying an increase in performance and in the level of security
- Providing priorities for Ethernet
- Goal:
  - compatibility with existing bridges and end-stations

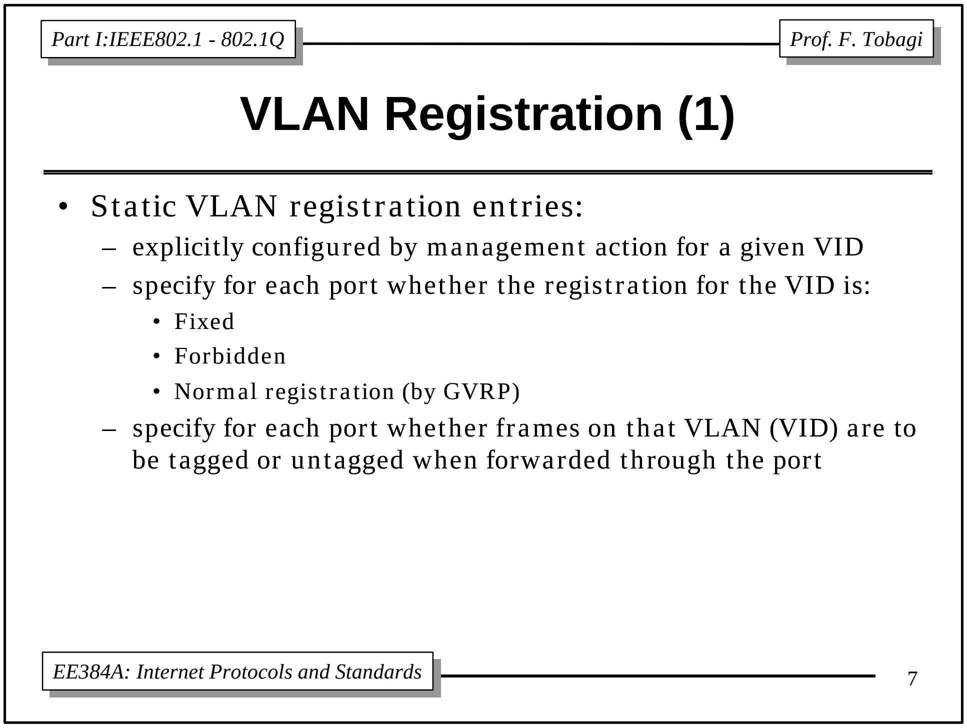
VLAN Tags



- Differentiation among traffic belonging to different VLANs is accomplished by the addition of VLAN tags (VLAN ID or VID) to frames
- Used by bridges to appropriately filter frames

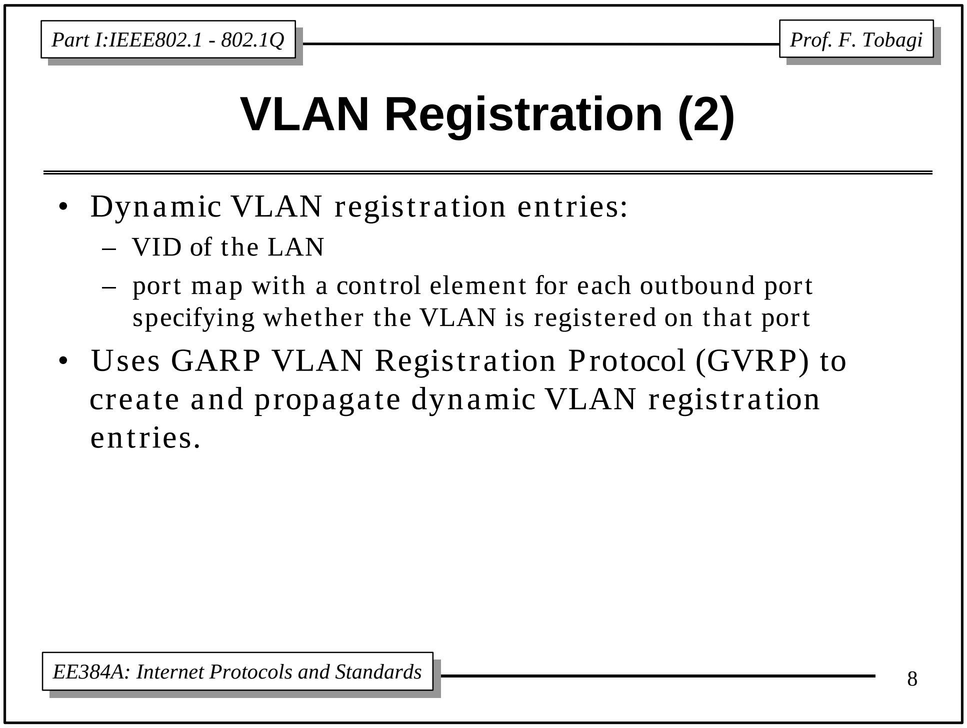
Tagged and Untagged Frames

- 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
  - specify for each port whether the registration for the VID is:
    - Fixed
    - Forbidden
    - Normal registration (by GVRP)
  - specify 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
- Uses GARP VLAN Registration Protocol (GVRP) to create and propagate dynamic VLAN registration entries.

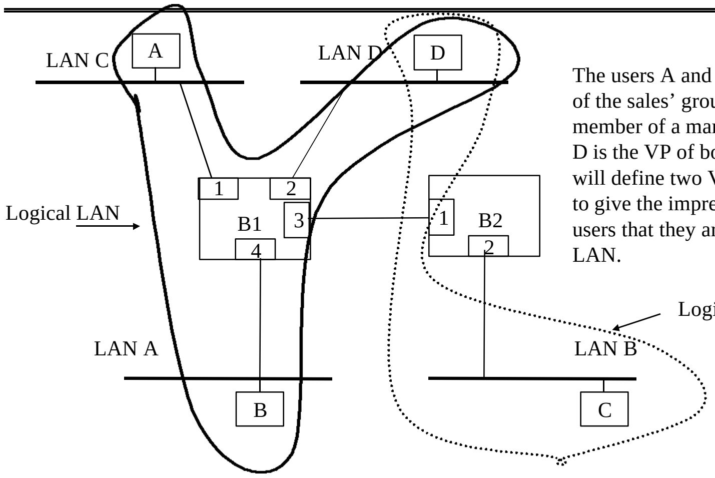
GVRP

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

Member Set and Untagged set for a VLAN

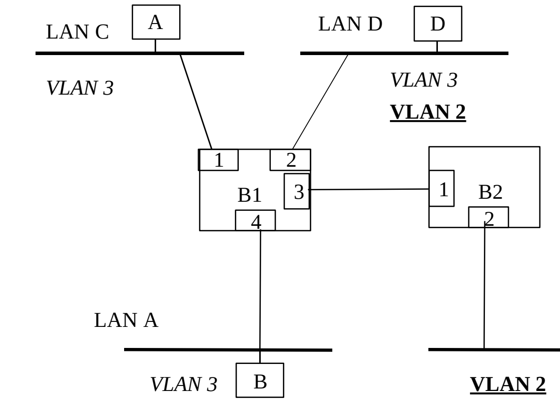
- The Member set consists of the set of Ports through which members of the VLAN can currently be reached.
- The untagged set consists of the set of ports through which frames that are transmitted shall be sent untagged

Example (1)



The users A and B are members of the sales' group, the user C is member of a marketing group and D is the VP of both groups. We will define two VLANs to be able to give the impression to these users that they are on the same LAN.

Example (2)



Using the information in the filtering database, the member set of the bridge B1 will be :
ports 1,2,4 for VLAN 3
ports 2,3 for VLAN 2
If the member of the VLAN 2 on the LAN B wanted to receive untagged frames, this should be specified and the port 2 of B2 will be in the Untagged set for VLAN 2

Ingress Rules

- Identify the VID associated 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)
- Default PVID = 1.
- If the Enable Ingress Filtering parameter is set, then frames are discarded if the Port is not in the member set.

Egress Rules

- Determine whether or not a frame is forwarded on a port
  - take into account VLAN info
- A frame is filtered if
  - The transmission 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

The Learning Process

- Deduces 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 in the Filtering Database.
  - The reason for this is that, in any case, you would not forward a frame on this port since it is not in the member set for this VID.

Example (3)

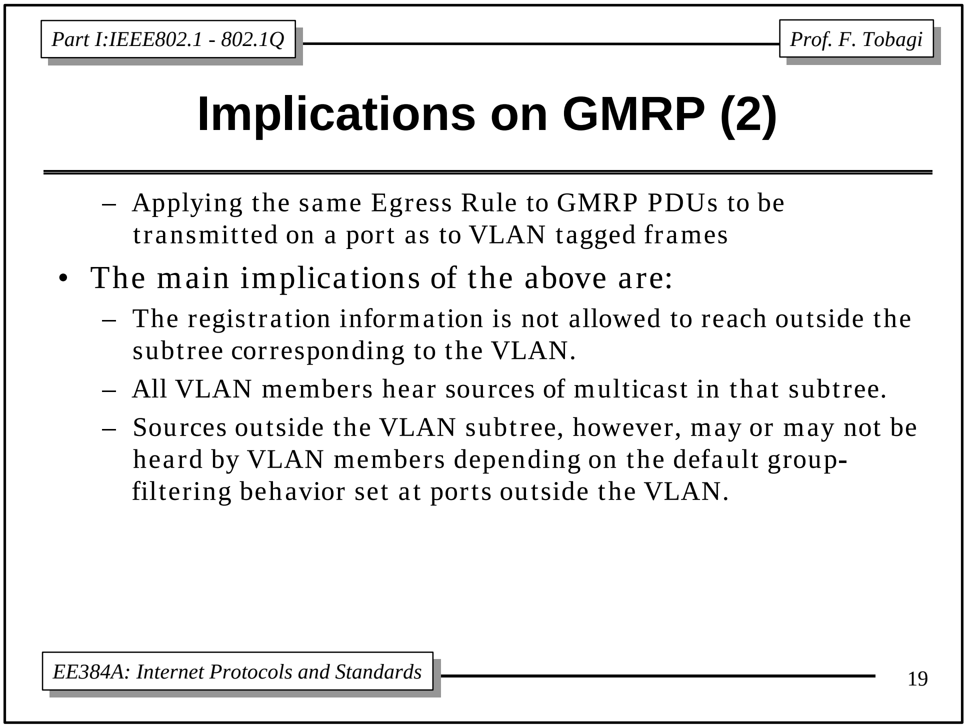
- In our example, it is easy to see that if D sends a message to C using VID = 2 in the Tag header then, the bridges B1 and B2 will have an entry in their filtering database for D saying that it is located respectively on ports 2 and 1.
- Nevertheless, as it has just been said, this entry is specific to this particular VID. So, if B sends a message to D using VID = 3 in the Tag header, the bridge B1 would not know where to forward the message and would send it to ports 1, 2 and 3 (assuming that there is no entry for this VLAN).
- To prevent these extra forwardings, it is possible to define a FID (a set of VID on which the learning process is shared). We would have FID = 2, 3 in our case. This way, the entry in the filtering database will be shared for both VLANs.

Filtering Database

- Static and Dynamic entries
- FID
  - Identifies a set of VLANs amongst which shared VLAN learning takes place
  - Two different FID’s identify two sets of VLANs between which independent learning takes place.
- Allocation of VID’s to FID’s
- Member Set
- Untagged Set

Implications on GMRP (1)

- In the absence of VLANs, GMRP data units are propagated throughout the entire spanning tree
  - This is referred to as the *Base Spanning Tree Context*.
- With VLANs, it is possible to allow GMRP registrations that are be made specific to a VLAN. This is simply accomplished by:
  - Considering that within each participant, there is an applicant and a registrar per VLAN, identified by the VID of the VLAN.
  - Tagging GMRP PDUs with the VID corresponding to the VLAN to which they apply.
  - Applying the same Ingress Rule to received GMRP PDUs as to VLAN tagged frames.



Implications on GMRP (2)

  - Applying the same Egress Rule to GMRP PDUs to be transmitted on a port as to VLAN tagged frames
- The main implications of the above are:
  - The registration information is not allowed to reach outside the subtree corresponding to the VLAN.
  - All VLAN members hear sources of multicast in that subtree.
  - Sources outside the VLAN subtree, however, may or may not be heard by VLAN members depending on the default group-filtering behavior set at ports outside the VLAN.