LAN Technology

Virtual LAN Protocol

Arash Habibi Lashkari
PHD of Computer Science - Information Security
July 2010

Virtual LAN Protocol

Outlines:

VLAN: Virtual Local Area Network and the IEEE 802.1Q

IEEE 802.1P: LAN Layer 2 QoS/CoS protocol for Traffic Prioritization

Create a VLAN in Network Lab

PPTP: Point to Point Tunneling Protocol

L2TP: Level 2 Tunneling Protocol

IPSec: IP Security

GMRP: GARP Multicast Registration Protocol

GARP: Generic Attribute Registration Protocol

GVRP: GARP VLAN Registration Protocol

GMRP

GARP Multicast Registration Protocol

A mechanism that allows:

- End stations to dynamically register (and subsequently de-register) group membership information with the MAC bridges attached to the same LAN segment
- Bridges to disseminate that information across all bridges in the bridged LAN that support extended filtering services

Operation of GMRP depends upon the services provided by GARP (Generic Attribute Registration Protocol)

Result of Group Membership Information Registration and Propagation

- Frames sent to a particular group:
  - Can be received on all LAN segments to which registered GMRP participants are attached
- Bridges filter frames on ports which have not had group registration entries created by GMRP
  - Multicast frames are not transmitted on those LAN segments which:
    - Neither have registered GARP participants
    - Nor are in the path, through active topology, from source to registered members

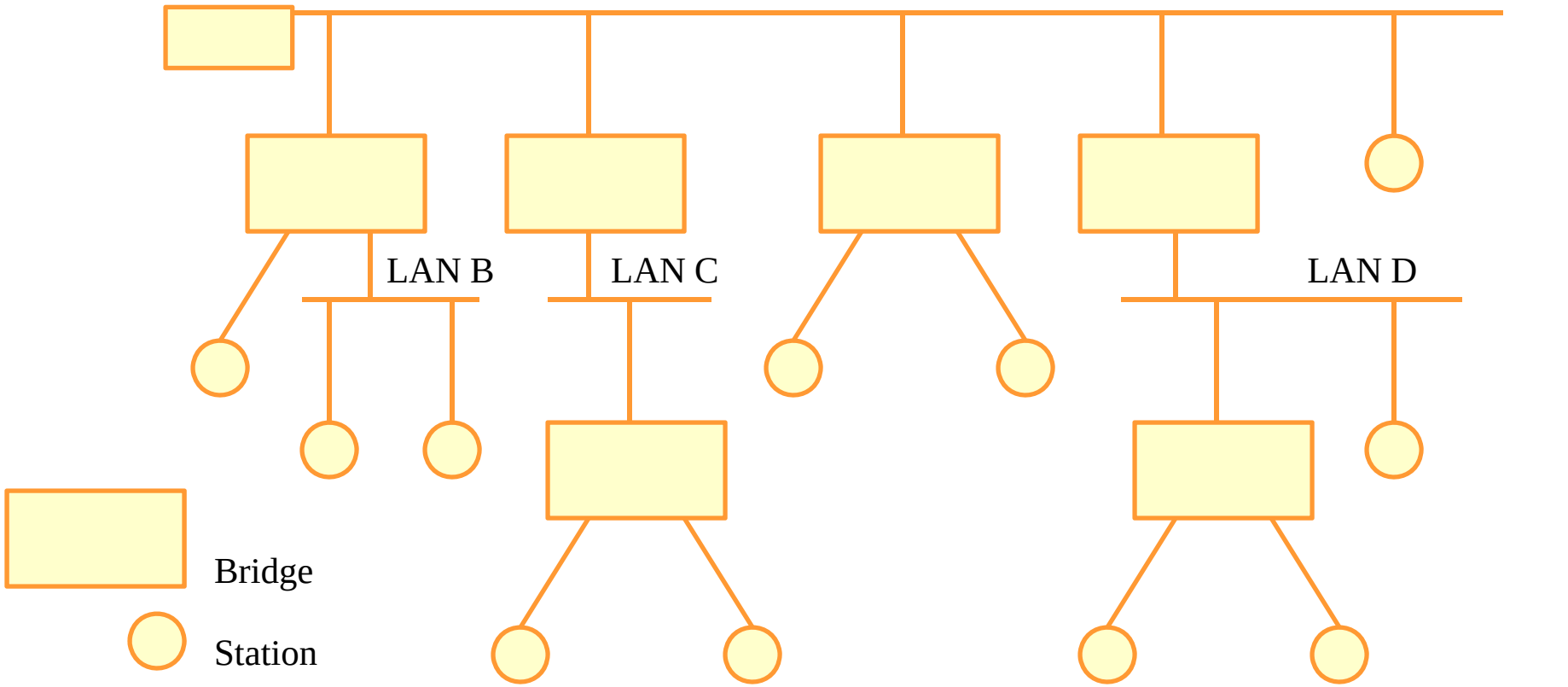
Open Host Group Concept

Any GMRP participants that wish to receive frames transmitted to a particular group or groups register their intention to do so by requesting membership to the concerned group(s)

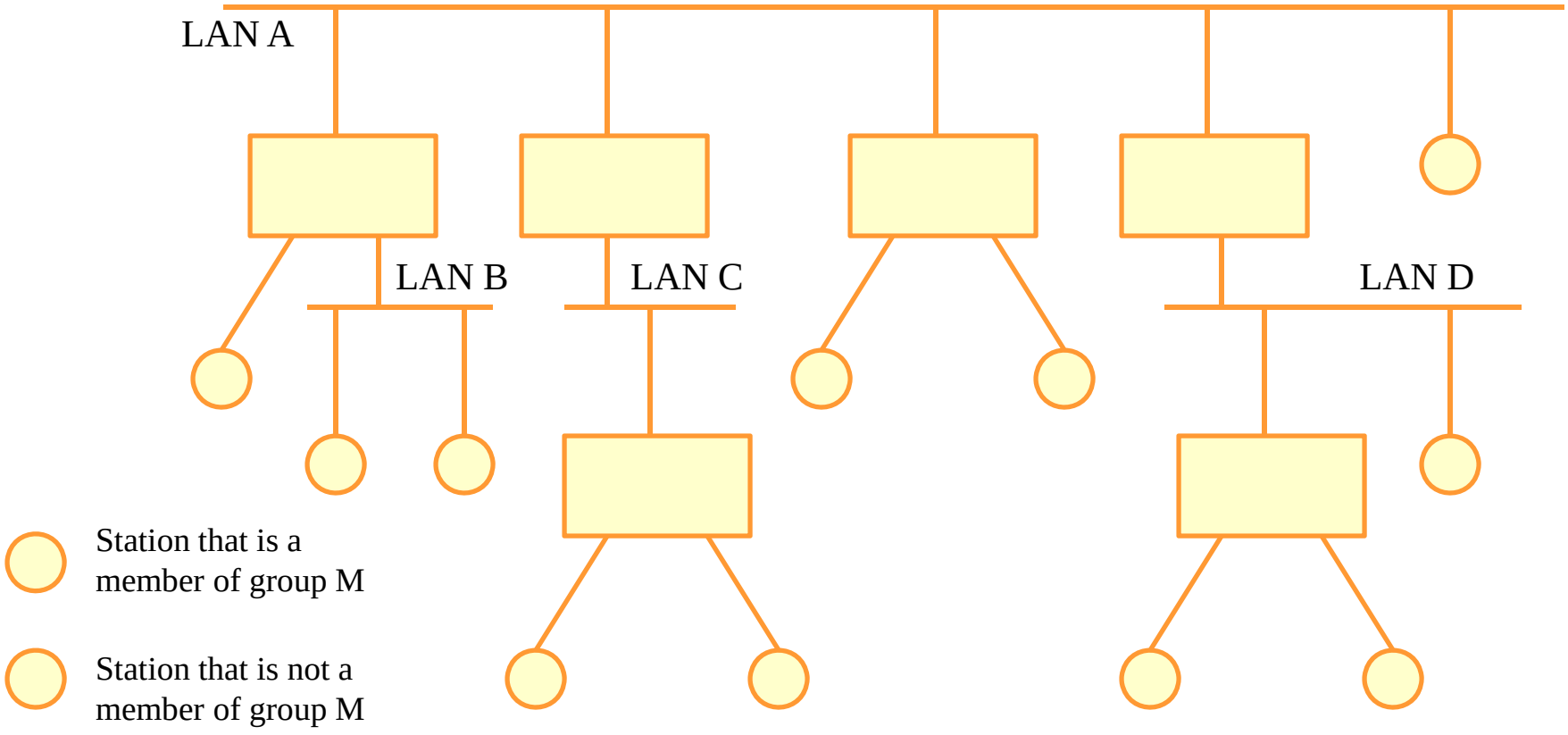
Any station that wishes to send frames to a particular group can do so from *any point of attachment* in the extended LAN

MAC service users that are sources of MAC frames for a group do not have to register as group members themselves unless they also wish to receive frames sent to that group by other sources

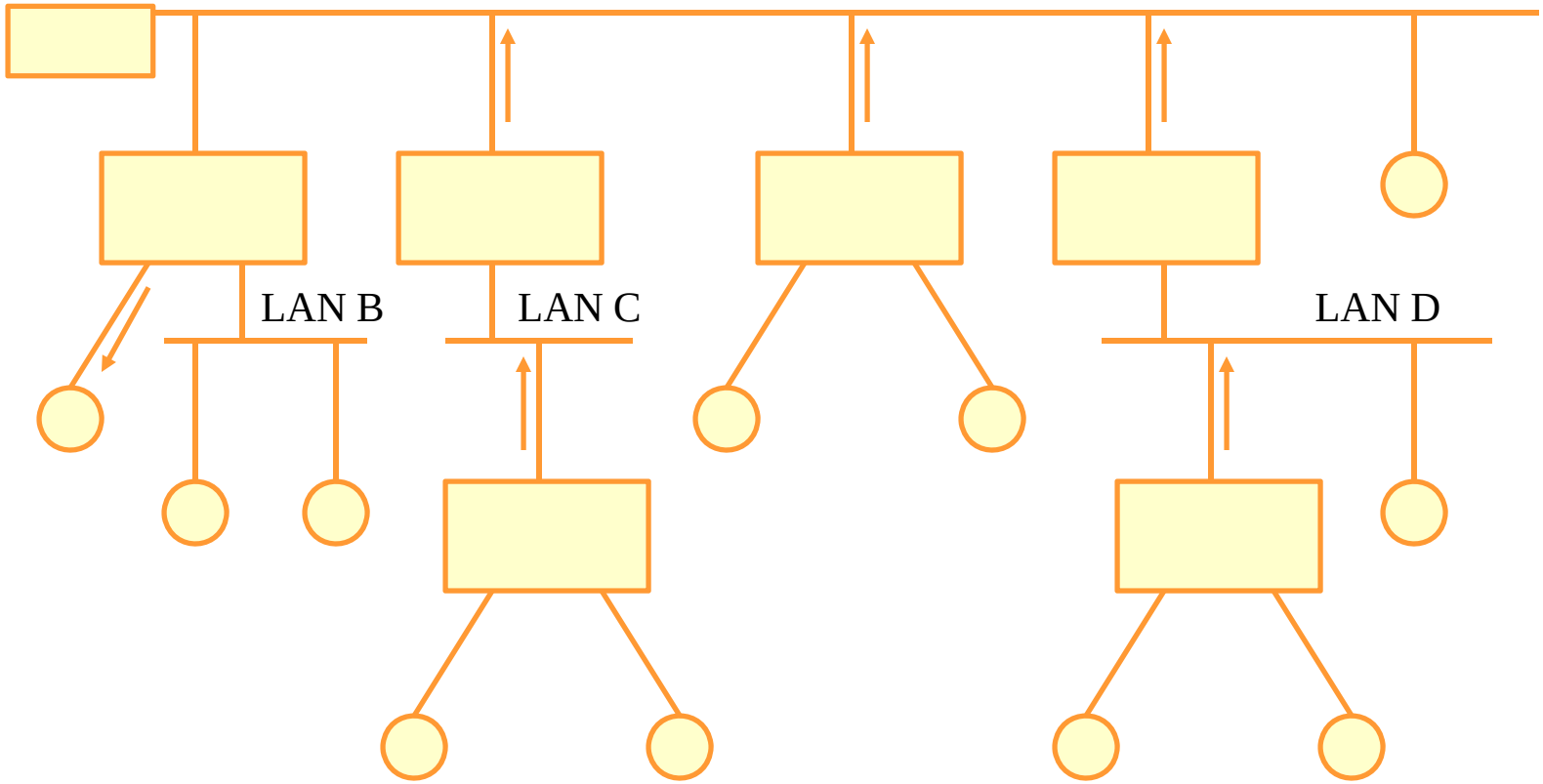
Example of an Active Topology



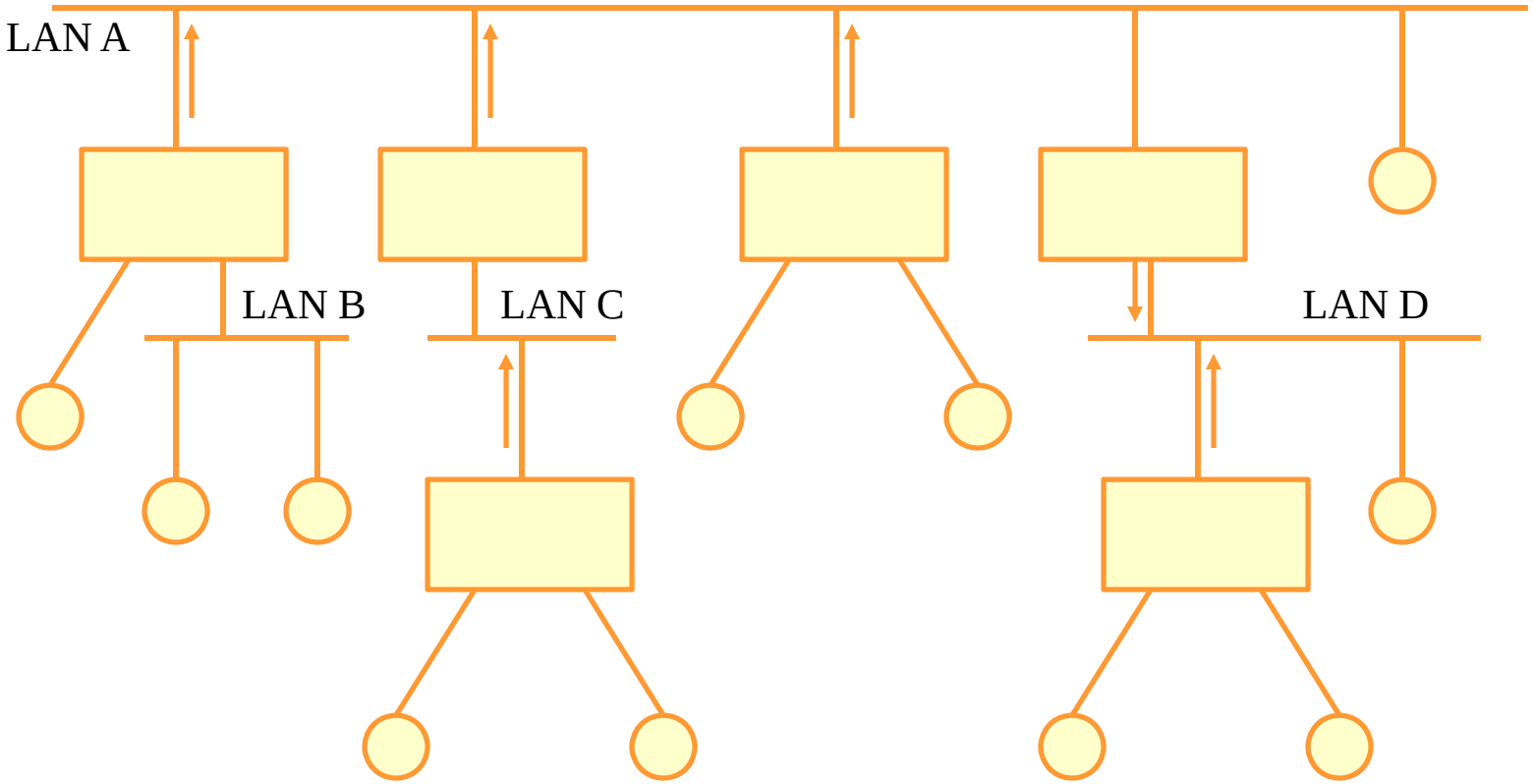
Active Topology with Group Members



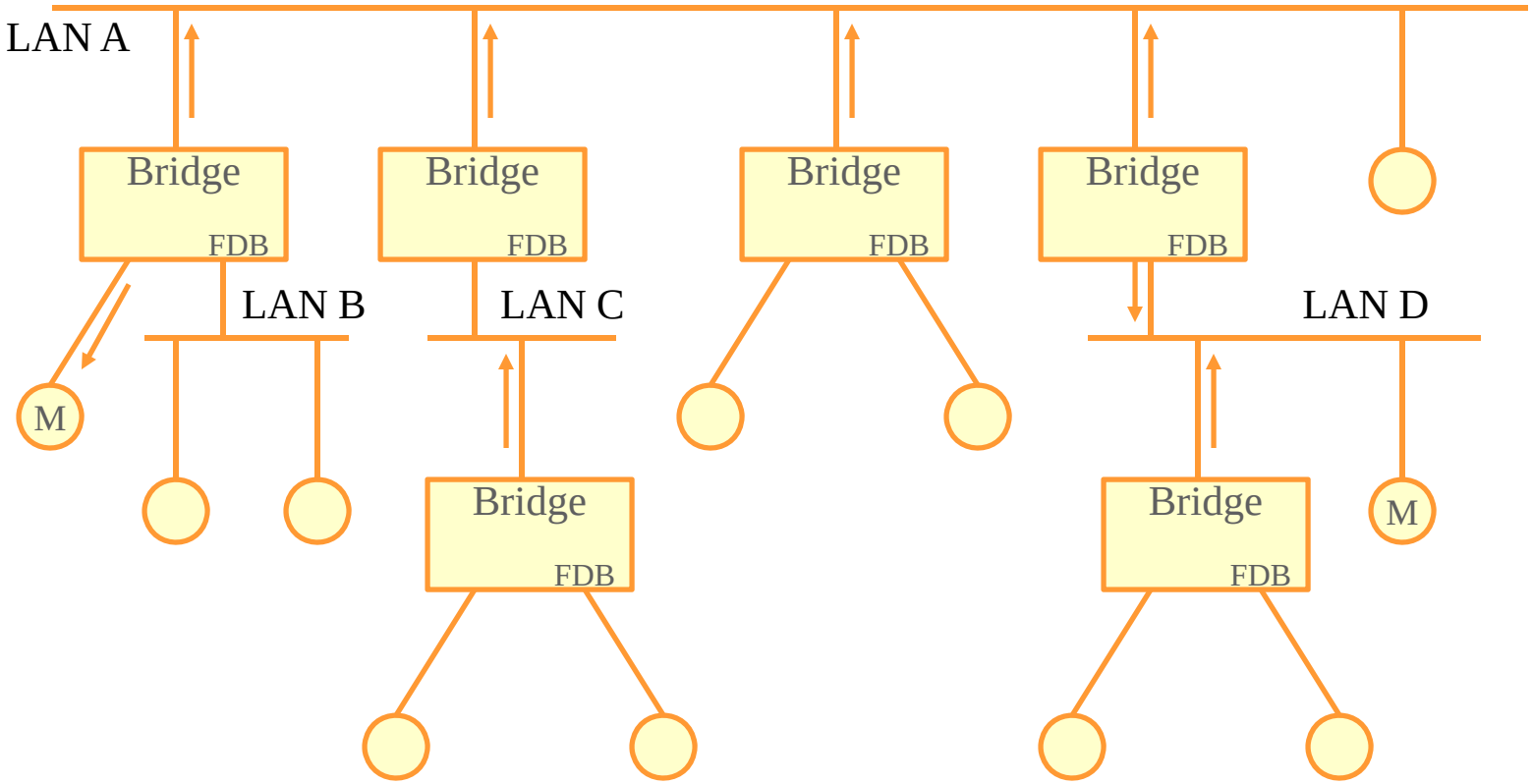
Example 1 with Active Topology



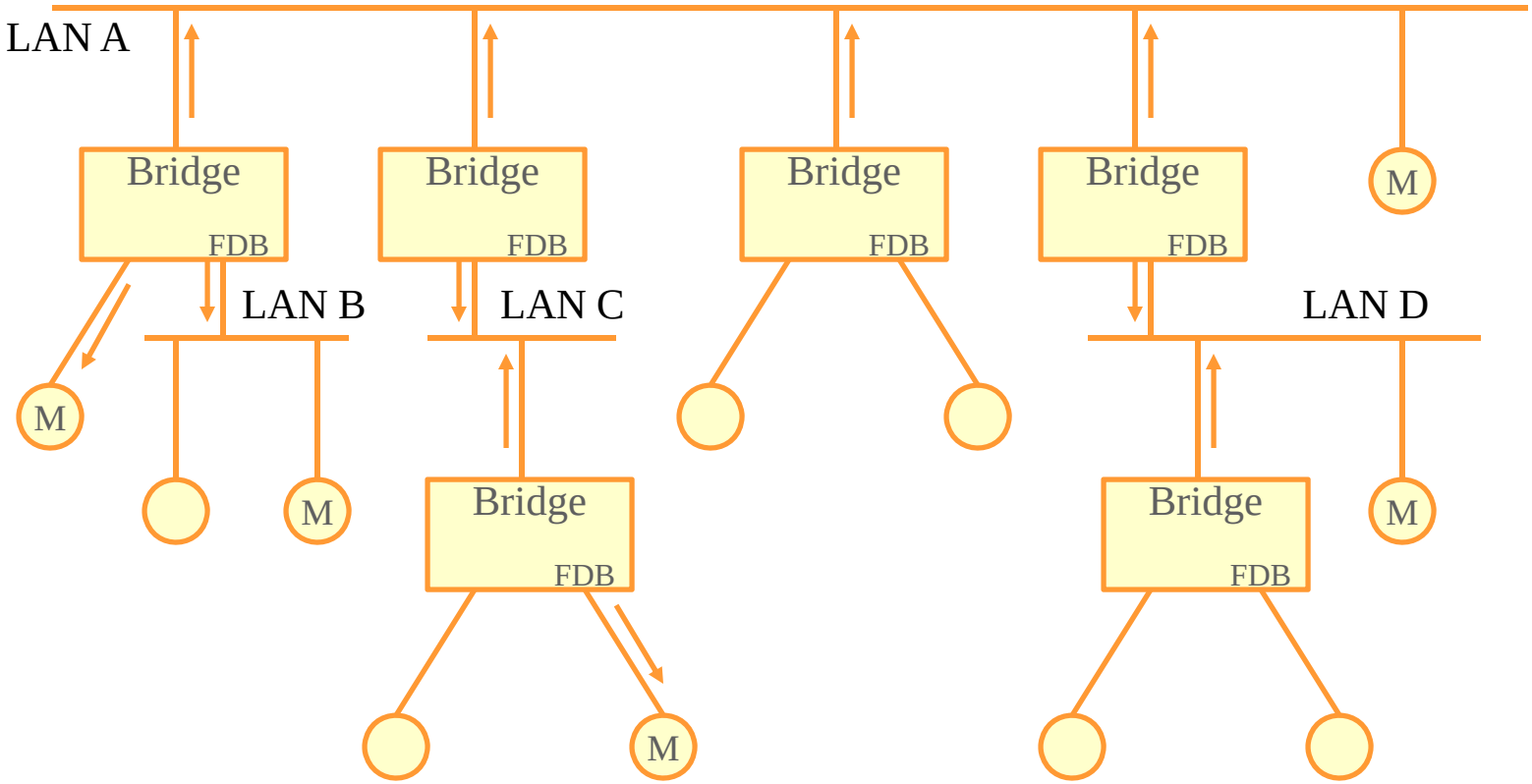
Example 2 with Active Topology



Example 3 with Active Topology



Group Registration Entries in FDBs Resulting in a Directed Graph



Source Pruning

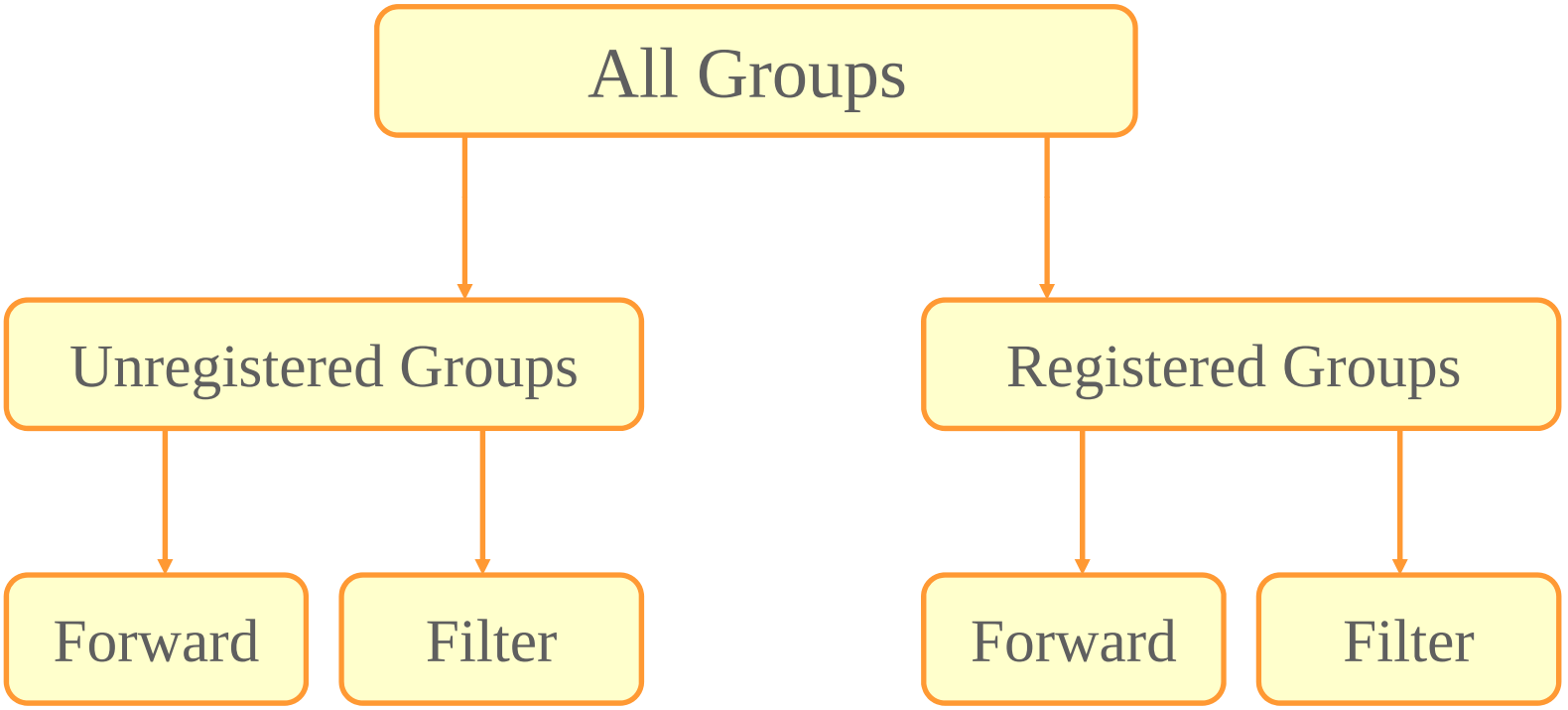
Should a station transmit a frame without knowing whether there is a recipient or not?

End stations use group membership information registered via GMRP to keep track of the set of groups for which active members exist

End stations may suppress the transmission of frames for which there are no valid recipients (or active members)

- Avoids unnecessary flooding of traffic on the LAN if there are no members that wish to receive such traffic

Default Group Filtering Behavior



Default Group Filtering Behavior

By default, there are three different group services

- Forward All groups
- Forward unregistered groups
- Filter unregistered groups

Each port may be assigned these default behaviors

Use of "Forward All Groups"

Frame is forwarded unless an explicit static filtering entry exists

To ensure that regions of the extended LAN that contain legacy devices can receive all multicast frames

- Can use static configuration to explicitly disallow certain multicast traffic

To allow successful operation of devices that require promiscuous reception

- Routers
- Network Monitors

Use of "Forward Unregistered Groups"

Group addresses which do not have dynamic FDB entries are forwarded

Group addresses which have dynamic FDB entries are forwarded or filtered based on the dynamic entry

Useful in circumstances where GMRP-aware devices distinguish between legacy multicast addresses for which they do not register and "new" multicast addresses for which they register

Must ensure that GMRP-aware end stations do not register for legacy multicast addresses

Use of "Filter Unregistered Groups"

Group addresses which do not have dynamic FDB entries are filtered

Group addresses which have dynamic FDB entries are forwarded or filtered based on the dynamic entry

Intended for operation with GMRP-aware end stations only

Type of Information Registered by GMRP

- Group membership information
  - Indicates that one or more GMRP participants that are members of a particular group (or groups), exist
  - Carries the group MAC address(es) information associated with the group(s)
  - Results in the creation or updating of group registration entries in the filtering database to indicate the port(s) on which the members of the group(s) have been registered
- Group service requirement information
  - Indicates that one or more GMRP participants require “forward all groups” or “forward unregistered groups” to be the default group filtering behavior (applied to a frame whose group address is not in the FDB)

The Extended FDB

The extended FDB contains information in the form of filtering entries that are either:

- Static entries
  - Explicitly configured by the management
- Dynamic entries
  - Automatically entered into the FDB by the normal operation of the bridge
- Group registration entries
  - Created, modified, and deleted by the operation of GMRP

GARP

- Objective:
  - Registration and dissemination of information of any generic attribute over a bridged LAN
  - End stations can issue/revoke declarations for the attribute values
- Attributes are opaque to GARP
  - It is up to the GARP application to define and interpret the generic attribute
  - Think of GMRP as an application which uses GARP!

GARP Control Messages

Two principal control messages

- Join Message
  - Sent by a user to register an attribute
- Leave Message
  - Sent by a user to de-register an attribute

There will be other messages derived from these two principal messages!

GARP: Design Principles

- Fully distributed protocol
- Simple
  - No explicit information about members
- Resilient against loss of a single control packet
  - A participant that wishes to make a declaration sends two join messages
- Scalable
  - Transmission of GARP control messages by participants is randomized over time
  - An applicant that sees a join message for the same attribute it intends to register considers it as if it were one of its own

GARP: Design Principles

- Soft State
  - No acknowledgments, no confirmation, no information about registered users
  - Registrations have to be refreshed continuously
    - Every 10s, the bridge issues a leave all message “threatening” to de-register all groups. Users still interested in keeping the registration alive send Join messages
- Resilient to failure of GARP participants
  - This is in case the GARP participants fail to see some GARP messages such as Join…
- Operates in homogeneous and heterogeneous LANs

GVRP: GARP VLAN Registration Protocol

The GARP (Generic Attribute Registration Protocol) VLAN Registration Protocol (GVRP) defines a GARP application that provides the 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports.

GVRP is an application defined in the IEEE 802.1P standard that allows for the control of 802.1Q VLANs.

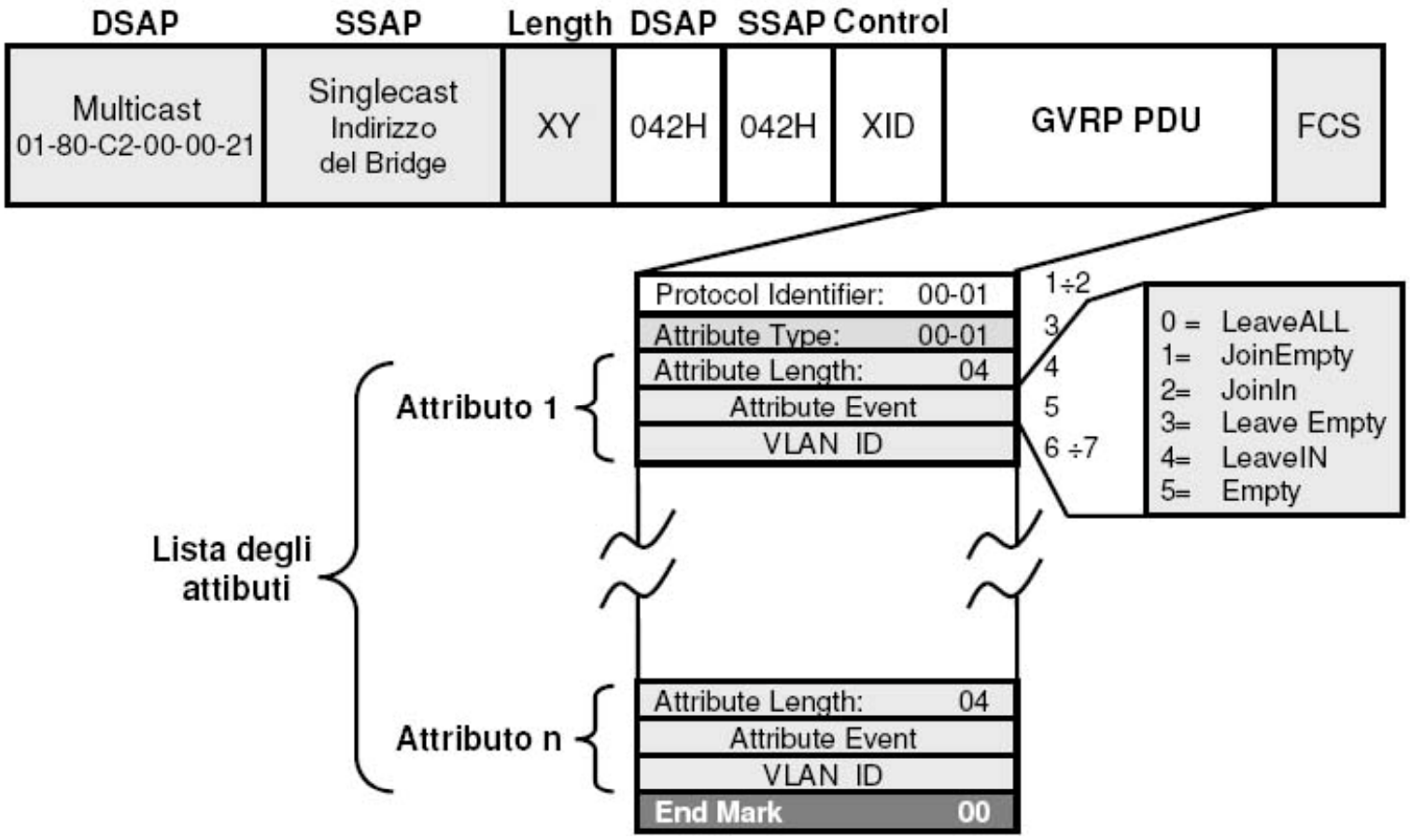
With GVRP, the switch can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs on switches connected through 8

GVRP allows the propagation of VLAN information from device to device.

With GVRP, a single switch is manually configured with all the desired VLANs for the network, and all other switches on the network learn those VLANs dynamically.

An endnode can be plugged into any switch and be connected to that endnode"s desired VLAN. For endnodes to make use of GVRP, they need GVRP-aware Network Interface Cards (NICs).

GVRP Packet Format



Questions