Virtual LANs

Fulvio Risso

Politecnico di Torino
The problem: multiple LANs across a campus (1)

Why?

- Performance
  - A single LAN has too much broadcast traffic (not filtered by switches)
  - Flooded traffic (e.g. due to frequent STP reconfiguration)
- Privacy, Security
  - Do not want a station to leak some information out (e.g. MAC Flooding attack)
- Management
  - Smaller network, simple (and uniform) policies
The problem: multiple LANs across a campus (2)

- Different physical networks (full separation)
  - \( N \) networks = \( N \) links + \( N \) devices
  - Waste of resources
Virtual LANs (1)

Without VLAN

With VLAN
Virtual LANs (2)

- Single physical infrastructure
  - Same devices, same cabling
    - No switches with only a few ports used
    - No need to have multiple fibers (for different LANs) in the backbone

- Different LANs
  - Different broadcast domains
    - E.g., Ethernet frames cannot be propagated on another VLAN
    - No broadcast between LANs
    - No MAC flooding attacks
    - No ARP spoofing
  - Created through a proper (logic) separation on switches
  - Intra-switch or inter-switch
VLAN: switch architecture
VLAN: forwarding database

Real implementations: unique filtering database (usually made with a TCAM, which is unique across the network device)
Sending data from a VLAN to another

- L2 data cannot cross VLANs
  - An Ethernet station cannot send an L2 frame to another station in a different VLAN
  - VLANs are different broadcast domains

- An L3 device (router) is needed
  - L2 header is thrown away
  - Lookup at layer 3 (e.g., IP destination address)
  - A new L2 header is created
Associate frames to VLANs (1)

- Problem
  - How can we associate frames to VLANs?
- VLANs on a single switch
  - We can mark the switch ports
  - The received frame is associated to the VLAN the port belongs to
Associate frames to VLANs (2)

- VLAN on different switches
  - Problem: how to distinguish which VLAN a frame belongs to, as there is a single link between switches?
- Same problem for devices that belong to different VLANs
  - E.g., servers, routers

Note: the IDs in the frames are the MAC addresses of the involved stations
Associate frames to VLANs: tagging

- Required only on links that transport traffic of different VLANs
- Old method: Tunnelling
  - An Ethernet (Token Ring or FDDI) frame is encapsulated into another Ethernet frame
  - Proprietary solutions
    - E.g., ISL (Inter-Switch Link) by Cisco
- Frame Tagging
  - An additional header is added to the MAC header
    - Standardized by IEEE 802.1Q
    - 4 additional bytes added to the frame
    - Basically, VLAN-ID plus a bunch of other info
IEEE 802.1Q Tag Encoding (1)

VLAN in Ethernet encapsulation (default)

<table>
<thead>
<tr>
<th>MAC Dest.</th>
<th>MAC Source</th>
<th>Ether type</th>
<th>802.1Q</th>
<th>Data</th>
<th>FCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>8100</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Ethertype for VLAN tagging

VLAN in Ethernet with LLC SNAP

<table>
<thead>
<tr>
<th>MAC Dest.</th>
<th>MAC Source</th>
<th>Length</th>
<th>LLC SNAP</th>
<th>802.1Q</th>
<th>Data</th>
<th>(Pad)</th>
<th>FCS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>03</td>
<td>00-00-00</td>
<td>8100</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IEEE 802.1Q Tag Encoding (2)

- Can be encapsulated in either Ethernet (DIX) or any link layer using LLC SNAP
  - In both cases, it uses the Ethertype 0x8100
    - The frame has IEEE 802.1Q tag
    - Called TPID (Tag Protocol Identifier)
  - PCP (Priority Code Point)
    - Refers to IEEE 802.1p priority
  - CFI (Canonical Format Indicator)
    - “1”: MAC address in non-canonical format (e.g., Token Ring)
    - Usually set to “0” (e.g., Ethernet)
IEEE 802.1Q Tag Encoding (3)

- VID (VLAN Identifier)
  - Values 1-4094
  - Usually, “1” refers to the default VLAN
  - 0: the frame does not belong to any VLAN
    - Used in case the user just wants to set the priority for her traffic
  - 0xFFF: reserved
### VLANs and network switches

- **Two types of switches**
  - VLAN-Aware: handle tagged and untagged frames
  - VLAN-Unaware: do not accept tagged frames
    - May discard frames (if too big)
    - Low-end devices

- Almost current products can handle VLAN tagging

- VLANs are no longer a “plug and play” technology
  - STP was
VLANs and network switches: link types (1)

- Access link
  - Receive and transmit Untagged frames
  - Default port configuration on switches
  - Usually used to connect end-stations to the network
    - PC do not need to change their frame format

- Trunk link
  - Receive and transmit Tagged frames
  - Must be configured explicitly on switches
    - Usually used in switch-to-switch connections and to connect servers/routers
  - Cannot have hubs on trunk ports
    - E.g. Ethernet hubs do not support frames > 1518 bytes
VLANs and network switches: link types (2)

- Hybrid link
  - Accepts both tagged and untagged frames
    - Differentiates frame according to the “type” field (0x8100 or not)
    - Some hosts may not be fully operational (e.g. Station A cannot understand tagged traffic directed to it)
  - Trunk links are usually also Hybrid links
  - May be used on ports on which both hosts and servers / routers / switches are connected
  - In any case, very uncommon nowadays
Tagging on trunk ports

- Different possibilities
  - Some switches tag the traffic belonging to all VLANs
  - Other leave the traffic belonging to VLAN 1 untagged

- Another reason of incompatibility between network devices of different vendors
Configuring VLANs on switches (1)

- VLAN creation

```
Switch# vlan database
Switch(vlan)#vlan 2 name Administration
  VLAN 2 added:
    Name: Administration

Switch(vlan)#exit
  APPLY completed.
  Exiting....
switch#
```
Configuring VLANs on switches (2)

- VLAN port association
  - Default behavior: a port is considered Access and associated to a default VLAN
  - The switch has a VLAN-unaware behavior

Switch# configure terminal
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch# show vlan brief

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>default</td>
<td>active</td>
<td>Fa0/2, Fa0/3, Fa0/4</td>
</tr>
<tr>
<td>2</td>
<td>Administration</td>
<td>active</td>
<td>Fa0/1</td>
</tr>
</tbody>
</table>
Configuring VLANs on switches (3)

- Configuration of the trunk port

```
Switch(config)#interface FastEthernet 0/2
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan add 1,2 [or “all”]
Switch(config-if)#exit
Switch#`

Assigning VLANs

- Different types of problems

  - Associate stations to the proper VLAN
    - E.g. port-based VLANs

  - A station can be associated also to multiple VLANs
    - E.g., required in case of servers, routers

  - Define which VLANs are allowed on trunk links
Port-based VLANs (1)

- Most common choice in current networks
  - Each port can be configured as either access port or trunk port
  - Each access port is associated to a single VLAN
  - Each trunk port is associated to a group of allowed VLANs
- Default: all ports in Access mode, associated to VLAN 1

![Diagram showing VLAN A and VLAN B connected through access and trunk links](image-url)
Port-based VLANs (2)

- Completely transparent to the user
  - Association is done on the switch
  - Maximum compatibility, since there is no need to configure PCs
- Different VLAN (e.g., privileges) depending on the actual network socket we connect to
- No mobility
Port-based VLANs (3)

- Given the following network
  - All ports are configured in “access mode”
  - SW-1 is configured with the RED VLAN on all its ports
  - SW-2 is configured with the GREEN VLAN on all its ports

- Can host H1 communicate with host H4?

Yes, because values configured on access ports are not propagated outside the switch!
VLANs to end systems: Transparent assignment

- New criteria in transparent assignment
  - Per L3 protocol (802.1v; no longer useful)
  - Per MAC address
    - Configuration problems
      - Keep MAC database aligned (new host, host with new NIC card, ...)
    - Network administrator has full control on association user-VLAN
    - Allows seamless mobility

- Mainly historical
VLANs to end systems: Cooperative assignment

- Cooperative assignment ("anarchic" VLAN assignment)
  - User keep control of the VLAN assignment
    - User sets the VLAN on the network card
  - Requires a reconfiguration on all the PCs
  - Allows seamless mobility
    - User will attach always to the same VLAN anywhere in the campus
  - What about a user joining the wrong VLAN?
    - Negligence or bad will
  - Used mostly on devices than must be part of different VLANs
    - E.g. routers, servers
- New possibilities with 802.1x
VLANs to end systems: trunk interfaces (1)

- Allow users to set the VLAN-ID
  - Although the configuration on the switch is always needed
    - Trunk ports on switches must be configured with the list of allowed VLANs
- Two modes for configuring end-systems in trunk mode
  - Simple association of VLAN tagging to the incoming/outgoing traffic
  - Use virtual NICs
- Depends on the NIC driver / OS
- Warning: IP addresses associated to the interfaces (either real or virtual) must belong to different IP networks
VLANs to end systems: trunk interfaces (2)

- Simple association of VLAN tagging to the incoming/outgoing traffic
  - Incoming/outgoing traffic is generated with 802.1Q tagging
  - Only one VLAN-ID per NIC interface is allowed (and specified by configuration)
  - Allowed on almost all network cards (e.g., the ones we have in our PCs)
  - We may have multiple cards in case multiple VLANs are required
  - Barely used
VLANs to end systems: trunk interfaces (3)

- Use virtual NICs
  - Multiple virtual network interfaces are created
  - Each one with its L3 configuration (e.g. IP address) and VLAN-ID
    - Only one VLAN-ID is allowed per virtual card
    - A maximum of N VLANs are allowed (N = number of V-NICs)
  - Widely used; mostly on servers and routers
  - Explicit support required from the NIC driver and the Operating system
VLANs in the backbone (1)

- Necessity to know which VLANs are handled on a given link
  - The switch needs to create the proper number of filtering DB
    - In the example, how can SW-2 know that it will have to forward VLANs 1-3?
  - The problem relates to all switches (access/core) with trunk ports
- Three solutions
  - Manual configuration
  - Proprietary mechanisms
  - GVRP
VLANs in the backbone (2)

- Shall we configure all VLANs on all trunk links?
- Configuring proper VLANs in the backbone may improve network behavior
  - Unicast is filtered by the filtering database
  - Broadcast is sent on the entire network
    - A broadcast storm on one VLAN will impair all VLANs
    - Network isolation is not complete, even with VLANs
VLANs in the backbone: manual configuration

- Used in most networks
- Usually, VLANs are configured explicitly on each switch
  - Possible problems (related to STP) in case you want to optimize trunk ports and filter useless VLANs out
    - What about if the link between SW-1 and SW-2 is turned off?
    - Better to allow all VLANs on all links and avoid optimizations

```
SW-1
(Role bridge)

Allowed VLANs: green, yellow

SW-2

Allowed VLANs: green, purple

SW-3
```
VLANs in the backbone: GVRP

- It propagates info about required VLANs on all the switches
- Prunes switches that are not interested by some VLANs from the tree of that VLAN
  - Can filter the broadcast traffic of some VLANs on some switches
- Handy (because automatic), but not widely used
- It inserts a new level of intelligence in switches
  - Configuration required
  - New software (i.e. bugs)
- Is it really needed (especially if you want to have a robust network)?
GVRP: GARP VLAN Registration Protocol

- A specialization of GARP: Generic Attribute Registration Protocol
- Used to register or unregister VLAN related attributes
  - A switch registers the VLANs it “knows” with the switch on the other side of a trunk link
  - Remote switch learns the VLANs whose packets should be forwarded on the trunk link
- Alternative to static definition of VLANs to be forwarded on a Trunk Link
- Switch using GVRP are said GVRP-Aware
- GVRP operates on the STP active topology
GARP: Generic Attribute Registration Protocol

- Registers or unregisters various types of attributes into an entity within a switch called GID

- GID (GARP Information Distribution)
  - Collection of state machines defining the current status of attribute registrations and declarations

- Attribute registration relates to a port receiving a GARP PDU with the corresponding declaration
  - Also a port set in Blocking state by STP

- GIP (GARP Information Propagation)
  - Entity in charge of propagating information among GARP Participants
    - Inside a single bridge
    - Among different bridges (based on LLC type 1)
# GVRP Packet Format

<table>
<thead>
<tr>
<th>DMAC</th>
<th>SMAC</th>
<th>Length</th>
<th>DSAP</th>
<th>SSAP</th>
<th>Control</th>
<th>GVRP PDU</th>
<th>FCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast 01-80-C2-00-00-21</td>
<td>Unicast Bridge address</td>
<td>XY 042H</td>
<td>042H</td>
<td>XID</td>
<td>GVRP PDU</td>
<td>FCS</td>
<td></td>
</tr>
</tbody>
</table>

## Attribute 1
- **Protocol Identifier**: 00-01
- **Attribute Type**: 00-01
- **Attribute Length**: 04
- **Attribute Event**: VLAN ID

## Attribute n
- **Attribute Length**: 04
- **Attribute Event**: VLAN ID

## List of Attributes
- 0 = LeaveALL
- 1 = JoinEmpty
- 2 = JoinIn
- 3 = Leave Empty
- 4 = LeaveIN
- 5 = Empty

### Control Byte
- Bit 7: 0 = LeaveALL
- Bit 6: 1 = JoinEmpty
- Bit 5: 2 = JoinIn
- Bit 4: 3 = Leave Empty
- Bit 3: 4 = LeaveIN
- Bit 2: 5 = Empty
- Bit 1: LeaveALL
- Bit 0: JoinEmpty
VLANs and Spanning Tree

- In theory, they are completely independent
  - First, Spanning Tree is computed in order to disable loops
  - Then, VLANs are propagated across the resulting topology
- Almost all vendors offer Per-VLAN Spanning Tree (PVST)
  - Most vendors can turn back to an unique STP via configuration
  - Cisco cannot (PVST is the only option)

Allowed VLANs: green, purple on all links
Per-VLAN Spanning Tree (PVST)

- Allows multiple spanning trees in the network
  - Network optimization
- Requires a per-VLAN configuration of ST parameters
  - Bridge priority, at least, for differentiating the root bridge among different VLANs (otherwise it will result the same tree for all VLANs)
  - Other parameters (Hello Time, Max Age, ...)
- Increase the load on the CPU of the switches
  - N instances of ST at the same time
- Interoperability problems between Cisco and other vendors
  - Broadcast storm if devices with/without PVSP are together in the same network
    - Some VLANs may not have a valid Spanning Tree
VLANs and network isolation

- Not complete
  - Frames do not cross the border of a VLAN
  - Links are shared, hence a problem on a VLAN may affect other VLANs
- VLANs do not protect from broadcast storms
  - A trunk link may be saturated by a broadcast storm on a VLAN
  - Other VLANS do not receive that broadcast but...
  - ... the trunk link is congested and it may be unable to transport the traffic of other VLANs
- Per-VLAN QoS may be required
Mixing VLAN-aware/unaware switches (1)

Problem: clients of servers S1 and S2 cannot exchange data to each other
Mixing VLAN-aware/unaware switches (2)

Problem: clients of servers S1 can no longer reach their server
Mixing VLAN-aware/unaware switches (3)

VLAN-unaware switches may be OK in the access side (e.g., in order to add new ports), provided that all clients belong to the same VLAN.
Relevant standards (1)

- **IEEE 802.1Q**
  - Defines VLAN-aware bridges
  - Per port based VLAN assignment
    - For both “access” and “trunk” ports
  - Unique spanning tree
  - Multiple filtering database identified by FID (Filtering Identifier)
    - Only one entry per MAC address can be present in each filtering database
    - A MAC Address may be present in different filtering databases
  - Defines the VLAN tag (User Priority, CFI, VLAN-ID), encapsulations
  - GVRP for propagating VLAN related information among switches
    - Based on the more general GARP defined in IEEE 802.1p
    - GARP = Generic Attribute Registration Protocol
    - GVRP = GARP VLAN Registration Protocol
Relevant standards (2)

- IEEE 802.3ac
  - Defines the new Ethernet frame format
    - Includes the VLAN tagging
    - Extends the maximum frame from 1518 to 1522 bytes

- IEEE 802.1p
  - Packet priority field, whose use is specified by IEEE 802.1p
Conclusions

- Pervasive technology
  - Network isolation useful in many cases (privacy, security, management, ...)
- Not complete isolation, though
  - Broadcast storm in one VLAN
  - QoS enforcement not always easy
- Many form of incompatibilities between different vendors
  - Better to select a single vendor for the entire L2 network
- L3 switch preferred
- Possibility to enforce L3 (or even L4/7) layer protection (e.g. firewall)

- Relevant standards:
  - IEEE 802.1p: format
  - IEEE 802.3ac: Frame extension
  - IEEE 802.1Q: VLAN