VLAN Tag encoding and recognition

Re: Q-rev/D1.0 SA ballot comment I-65.

Mick Seaman
mickseaman@gmail.com

Note: This presentation discusses what is standardized, not proprietary solutions (whether arguably standards 'compatible' or not) or what changes might be desirable in networks using those solutions.

Overview

Simple cases first:

- C-VLAN Bridge Forwarding
  - — Forwarding between Ethernet interfaces
  - — Transparent bridging (now and for the future)
- Network configuration for VLAN traffic segregation
  - — Peer-to-peer, sub-layered architecture
  - — Ethernet-attached end-station behavior

Mixing it up:

- Tags and forwarding for different media

C-VLAN Bridge Forwarding—Steps

Assign each received frame to a VLAN:

- If the initial octets of the frame (following the MAC SA) are recognized as a VLAN Tag with non-zero VID, the assigned VLAN ID is the VID in the Tag.
  - Discard if Acceptable Frame Types is Admit Only Untagged and Priority-tagged frames
  - Remove the Tag
- If the initial octets of the frame (following the MAC SA) are recognized as a VLAN Tag with zero VID, the assigned VLAN ID is the PVID .
  - Discard if Acceptable Frame Types is Admit Only VLAN-tagged frames
  - Remove the TAG
- Otherwise frame’s VID is the PVID.
  - Discard if Acceptable Frame Types is Admit Only VLAN-tagged frames

Forward to other Ports (conditionally on DA and VLAN ID)

Conditionally tag transmitted frames:

- Prepend a VLAN Tag if the Port is not in the untagged set for the VID.
- Otherwise transmit the frame without adding a Tag

C-VLAN Bridge Forwarding—Summary

If the initial octets of a received frame comprise a recognized C-VLAN Tag:

- The Tag is removed on receipt, and a Tag may be added on transmit

If the initial octets of a received frame do not comprise a recognized C-VLAN Tag:

- A Tag can be added on transmit

Frame forwarding by a series of N simple C-VLAN Bridges:

- Initially untagged frames can be transmitted with zero or one prepended Tags
- Initially tagged frame can be transmitted with the same (possibly VID translated) Tag or with the removal of up to N consecutive C-VLAN Tags

Note: Interface stacks that intentionally add other tags, e.g. the MACsec SecTAG can hide C-VLAN Tags from the reception process. Nonsensical network configuration, e.g. random addition of S-VLAN Bridges can also restart the tagging process.

C-VLAN Bridge Forwarding—Ethernet examples

DA, SA precedes all octet sequences shown in these examples.

IPv4 frame, transmitted untagged or tagged by end station. Assigned to VLAN 1:

08-00 .. → 08-00 ..

08-00 .. → 81-00 00-01 08-00 ..

81-00 00-01 08-00 .. → 81-00 00-01 08-00 ..

81-00 00-01 08-00 .. → 08-00 ..

Adversary includes hidden VLAN Tag:

81-00 00-01 81-00 00-02 08-00 .. → 81-00 00-01 81-00 00-02 08-00 ..

81-00 00-01 81-00 00-02 08-00 .. → 81-00 00-02 08-00 .. !!

Adversary hides an extra VLAN Tag behind a CN-TAG:

81-00 00-01 22-E9 57-57 81-00 00-02 08-00 ..

→ 81-00 00-01 81-00 00-02 08-00 .. → 81-00 00-02 08-00 .. !!

All the above examples use VLAN VID 1 or VLAN VID 2, because a 0 in the VID field in a VLAN Tag indicates that the frame has not yet been assigned to a VLAN. In that case the VLAN Tag just carries priority and drop_eligible information.

Discarding illegitimate tags

Problem: Bridges will no longer be ‘transparent’ or cost-effective if they need to parse and reject frames with ‘unknown’ or stacked protocol identifiers.

Solution: Enforce peer-to-peer (sub-layered network architecture) relationships:

- Every interface stack entity that adds a Tag (of any type) has a peer (or peers) that removes that Tag.
- Discard any frame with an unexpected Tag (apparent presence of an unknown/unauthorized peer) as unknown protocol.
- Existing 802.1 protocols use ‘domain’ or ‘address scope’ concepts to bound network regions with legitimate peers, discarding data frames or control frames that might otherwise enter the domain e.g. by Reserved MAC address filtering.

Network config for VLAN traffic segregation

Example network uses 802.1X at exposed access interfaces:

- Bridge serving that interface adds C-VLAN Tag (with VID appropriate to accessing system authorization) or verifies frame already has that Tag, before transmitting into the protected network.
- Tag is not removed as it transits the protected, traffic segregated, network domain.
- Tag can be removed when frame leaves the traffic segregated network domain (the bridge that removes the Tag is a peer of the bridge that added it), but is not removed for 'efficiency' reasons within the domain.
  - Tag removal appropriate for transmission to a VLAN-unaware end station.
  - Exposes VLAN-aware end stations to a potentially 'hidden tag'. Protected network domain needs to ensure those end stations cannot return frames on an inappropriate VLAN.
- Tag not removed when delivering frames to a VLAN-aware end station. The protocol shim that recognizes the C-VLAN Tag is a protocol peer of the bridge that added it.
  - End station needs to treat any further C-VLAN Tag (or an inappropriately placed S-TAG, for example) as unrecognized protocol, and discard the frame.

Tags and forwarding for different media

Whatever the media type all Tags (all protocol identifers allocated by IEEE 802) in a frame, apart from the first, are Length/Type encoded (see 802.1Q-2018 G.3).

Alternative descriptions of C-VLAN Bridge forwarding:

1. Recognize VLAN Tag on receipt (remove if present), select VLAN for forwarding. Forward to selected transmission ports.
   If VLAN Tag on receipt but not on transmit, translate received initial protocol id encoding for transmit media type.
   If VLAN Tag not on receipt, but on transmit, translate received initial protocol id encoding to Length/Type.
   If VLAN Tag on transmit, add with encoding for transmit media type.
2. On receipt, translate initial protocol id encoding to Length/Type (media dependent support of the ISS).
   Recognize VLAN Tag EtherType, remove Tag if present, select VLAN for forwarding. Forward to selected transmission ports.
   Add VLAN Tag (if required), update assigned VID (if required).
   Translate initial protocol id encoding to type required by media (media dependent support of the ISS).