Ingress Port Map for 802.1Q

Norman Finn, Cisco Systems

1.0 Introduction

An Ingress Port Map is proposed, with a control element for each inbound Port. The control element specifies, for each VID, whether a frame received with that VID is to be filtered.

Whether this Ingress Port Map would be required or optional is a matter to be discussed at the interim meeting.

The justification for an Ingress Port Map is twofold:

1. In a large number of current VLAN installations, and perhaps in the majority of them, there is no dynamic component to the assignment of VLANs to ports. Moves, adds, and changes are either not important, or are handled by methods such as DHCP. In such installations, the easiest transition to 802.1Q is to maintain the semantics of the existing implementations, in which dynamic movement of VLANs via GVRP is unnecessary.
2. In existing large VLAN installations, security cannot be ignored. Whether dynamic VLANs are used or not, the Ingress Port Map provides an important security capability. Where dynamic VLANs are not important, as in many or most current installations, the Ingress Port Map provides all of the L2 security required by most users.

In short, it is claimed that a great many users and vendors would be well served by a model in which VLAN assignments are static, rather than dynamic. In this model, the Ingress Port Map is essential, and GVRP irrelevant. This contribution proposes, therefore, that we incorporate an Ingress Port Map into the next 802.1Q draft.

It is not the purpose of this document to suggest that there are no other models for VLAN operation, nor to remove anything from the current 802.1Q draft.

2.0 Static VLAN model

Figure 1 illustrates a portion of a typical static VLAN installation consisting of (from top to bottom) a routed backbone cloud, local routers, distribution switches, and edge switches. Each device has redundant connections to the devices at the next higher level, in order to enhance the reliability of the network. Note that the local routers are commonly connected to each other via switches (though dedicated links may be used), and that there may be switches in the routed backbone cloud, as well.

Let us assume that a VLAN is equated to an L3 addressing domain such as an IP subnet. If the routing algorithms are to be relied upon to efficiently direct packets, then the VLANs (subnets) must be localized in space. Sophisticated algorithms are in common use by routers for such purposes as bandwidth allocation, load sharing, and prioritization of traffic. Such algorithms can be defeated if a given VLAN (subnet) is allowed an arbitrary number of access points to the routers.

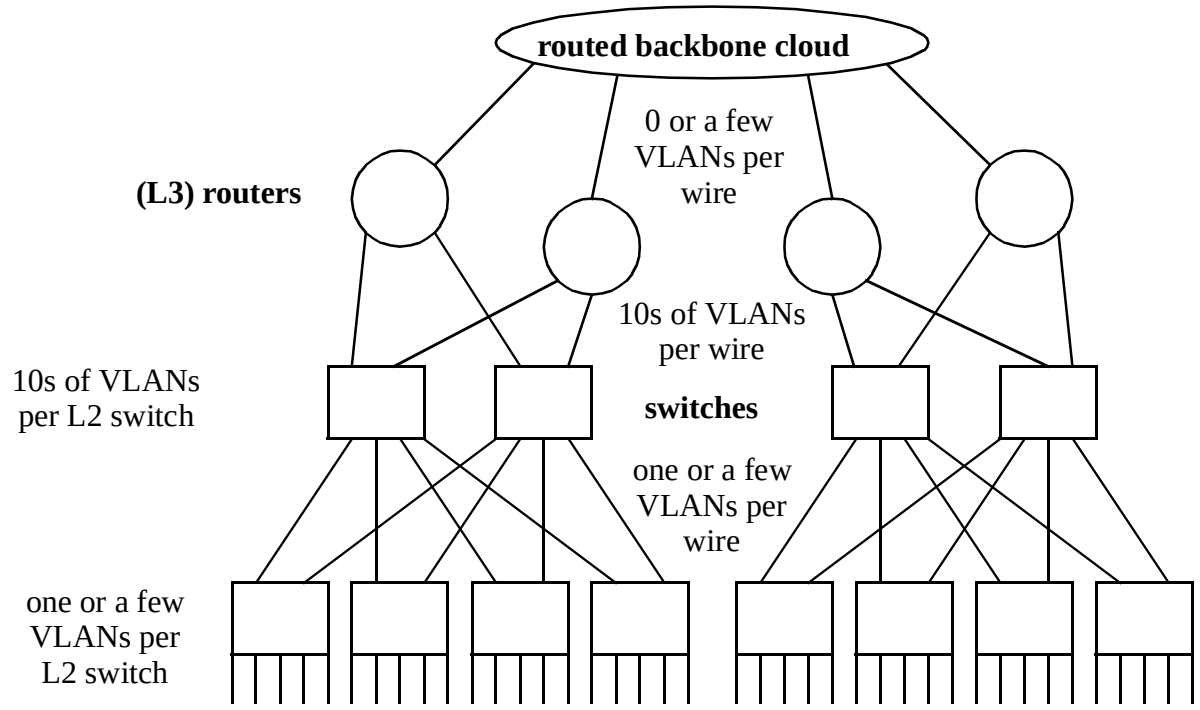

FIGURE 1. Static VLAN Model

The routers' algorithms can be made pointless if traffic must traverse a tortuous path through the switch cloud between the endstation and the router.

In such installations, the static assignment of VLANs to switch ports gives the routers the stability they need to perform their tasks. Problems such as the mobility of endstations are commonly solved using techniques such as RARP (reverse address resolution protocol) or DHCP (dynamic host configuration protocol), one or both of which are implemented in most desktop computers shipped, today.

The ingress port map enables the system administrator to specify which VLANs are allowed on any given port. This is typically one per access port, and more than one per trunk port. The question of which VLANs need to be supported/bridged by a given switch is then trivial to answer, and no dynamic protocols are required other than the spanning tree.

3.0 Security

Whether "security" in the broad sense is included in the 802.1Q PAR or not, it is clear that allowing endstation inject traffic for any VLAN is insecure. Since an ingress port map would often be implemented in hardware, and since its utility to security is fundamental, it is appropriate to include it in the first 802.1Q standard, rather than introducing it later.

In the absence of dynamic protocols such as GVRP, the combination of ingress and egress port maps provide the VLAN user with essentially the same level of L2 security currently provided by separate bridged LANs. Thus, it is compatible with the expectations of the higher-layer security techniques in common use.

4.0 Changes to 802.1Q/D6.5 to support ingress port maps

The text and specific suggestions in this document for altering the 802.1Q/D6.5 draft are meant to convey the details of the operation of the ingress port map. They are not meant to constrain the editors to any specific text. The editors may determine that an entirely different means for describing the ingress port map is more appropriate.

`In this contribution, suggested new text for the 802.1P/D7 document is shown in this font.`

4.1 Required or optional

Depending on whether the ingress port map is made optional or mandatory, it may need to be mentioned in sections 1.5.1 (if required) or 1.5.2 (if optional).

4.2 Relay function: filtering and relaying information

Section 3.1.2, “filtering and relaying information”, requires changes. Suggested text to be inserted after paragraph h):

`A bridge filters frames in order to prevent the injection of traffic for a given VLAN on a port on which that VLAN is disallowed. The function that supports the use and maintenance of information for this purpose is:`

`i) Explicit configuration of the Ingress Port Map, which specifies for each VID, the ports on which frames with that VID may be accepted.`

4.3 Model of operation

Section 3.3 needs a mention of the ingress port map. A new paragraph b) should be inserted ahead of the current paragraph b).

`b) The Ingress Port Map (reference here) which filters frames from disallowed VLANs;`

4.4 Ingress rules

The last paragraph of the Ingress rules (3.7) should state that frames pass to the Ingress Port Map after being classified to a specific VLAN.

4.5 Description of the Ingress Port Map

It would appear that the Ingress Port Map description should be a new section between 3.7 “Ingress rules” and 3.8 “The Forwarding Process”.

`Associated with each VID known to a VLAN Bridge is a vector of permission parameters, one for each Port on which frames may be`

received. For each {Port, VID} pair, the permission parameter may have either of two values:

a) Permit. Frames received on this VID are allowed.

b) Discard. Frames received on this VID are discarded.

All frames that are not discarded as a result of the application of the Ingress Port Map are submitted to the Forwarding Process and to the Learning Process.

Note that frames which are discarded by the Ingress Port Map do not affect the bridge's filtering database.

Use of this parameter, in conjunction with Static VLAN Registration Entries (reference here) allows a Bridge to be built in which some or all Ports can be restricted to carrying only certain VLANs. Since a Bridge cannot forward frames for VLANs which are not permitted on any of its Ports, this allows a Bridge to optimize its resources even in the absence of dynamic VLAN registration information. It also allows the Bridge to deny access to the VLAN to ports where the VID information encoded in Tagged traffic may be suspect, without discarding all Tagged traffic.

4.6 VLAN topology management

Section 6 of the 802.1Q/D6.5 document describes VLAN topology management strictly in terms of GARP/GMRP. This section should be retitled "Dynamic VLAN topology management", and a new section, "Static VLAN topology management" added. Either section 6 should be split in two, (6.1 and 6.2, static and dynamic, with the title of section 6 unchanged) or a new section 5 or section 7 should be added for the static version.

The gist of the contents of the "Static VLAN topology management" section are that a system administrator can manage the VLAN topology explicitly, via the Ingress Port Map and the Static VLAN Registration Entries, rather than using information provided by the GARP/GMRP protocols. Text for this section is not included in this present contribution.

4.7 Configuration management

In section 7.1.1 "Configuration management", point f) should be modified:

f) The ability to identify the VLANs in use, and through which Ports of the Bridge frames belonging to a given VLAN may be received and/or forwarded.

4.8 Managed objects

The list in section 7.2 "Managed objects" needs a new paragraph c) ahead of the existing paragraph c):

c) The Ingress Port Map of the MAC Relay Entity (reference here).

4.9 VLAN Bridge Management: Ingress Port Map

A new section 7.6 “Ingress Port Map” should be inserted ahead of the current section 7.6 “Forwarding process”.

f. 7.6 Ingress Port Map

f. The Ingress Port Map counters record the number of frames discarded by the Ingress Port Map, as well as recording the VID of the last-discarded frame. This information is the minimum required to detect and debug the misconfiguration and/or misuse of the network using the Ingress Port Map. Configuration data, defining which VLANs may be received on which Ports, is maintained by the Ingress Port Map.

f. The management operations that can be performed on the Ingress Port Map are Read Ingress Port Map, Set Ingress Port Map, and Read Ingress Port Map Counters.

f. 7.6.1.1 Read Ingress Port Map

f. 7.6.1.1.1 Purpose

f. To read the state of the Ingress Port Map for a given VID and Bridge Port.

f. 7.6.1.1.2 Inputs

f. Port Number.

f. VID--VLAN Identifier of the entry

f. 7.6.1.1.3 Outputs

f. Permit. Boolean True or False. If True, this VID may be received on this Port. If False, frames associated with this VID will be discarded when received.

f. 7.6.1.2 Set Ingress Port Map

f. 7.6.1.2.1 Purpose

f. To set the state of the Ingress Port Map for a given VID and Bridge Port.

f. 7.6.1.2.2 Inputs

f. Port Number.

f. VID--VLAN Identifier of the entry

f. Permit. Boolean True or False. If True, this VID may be received on this Port. If False, frames associated with this VID will be discarded when received.

f. 7.6.1.2.3 Outputs

f. None

f. 7.6.2 Read Ingress Port Map Counters

f. 7.6.2.1 Purpose

f. To read the state of the Ingress Port Map statistics.

f. 7.6.2.2 Inputs

f. Port Number.

f. 7.6.2.3 Outputs

f. Frames Discarded--count of frames discarded on this Port because the Ingress Port Map specified that the frame must be discarded.

f. Last VID Discarded--VID of the last frame discarded on this Port. 0 if the value of Frames Discarded is 0.