



## Executive Summary

Blue Coat ProxySG appliances utilizing MACH5 WAN Optimization allow IT organizations to accelerate and secure the delivery of business applications for all users across the distributed enterprise - including those near Internet gateways, as well as in branch offices, data centers, and even individual end points. As part of the MACH5 WAN Optimization solution, ProxySG appliances support VLAN Tagging, which allows seamless deployment of ProxySG appliances in the path of VLAN-tagged traffic while also providing application-level control over VLAN connections.

## What is VLAN Tagging?

When VLANs span multiple switches, VLAN Tagging is required. A VLAN is a method of creating independent logical networks within a physical network. VLAN Tagging is the practice of inserting a VLAN ID into a packet header in order to identify which VLAN (Virtual Local Area Network) the packet belongs to. More specifically, switches use the VLAN ID to determine which port(s), or interface(s), to send a broadcast packet to. VLAN Tagging support allows administrators to deploy ProxySG appliances inline with switches that are routing VLAN traffic without the risk of losing VLAN ID information.

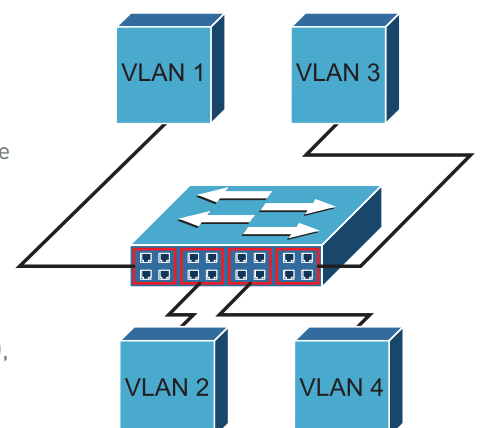
## Why should I enable VLAN Tagging support in my network?

VLAN Tagging support is specifically designed for networks where the ProxySG appliance is deployed in the path of VLAN-tagged traffic; common examples of this are a ProxySG appliance deployed between two switches, or between a switch and a router that is forwarding or bridging traffic. Without VLAN Tagging support, deployments in which an appliance is in the path of VLAN-tagged traffic often result in VLAN-tagged traffic being dropped, or passed through by a bridging configuration. This creates a problem if, for example, users located on different floors all belong to the same VLAN, but the switches on each floor are separated by a proxy that does not recognize VLAN-tagged packets. With VLAN Tagging support, administrators can deploy the ProxySG appliance inline with any VLAN-tagged traffic and take full advantage of the functionality of the ProxySG appliance on those connections.

## How does VLAN Tagging support work?

Before describing how VLAN Tagging works, you should first have a general understanding of VLANs. The purpose of VLANs is to group multiple physical network segments into individual broadcast domains, allowing you to have multiple virtual switches. The benefit of this grouping is that clients can be organized logically rather than being limited to a subnet per physical switch.

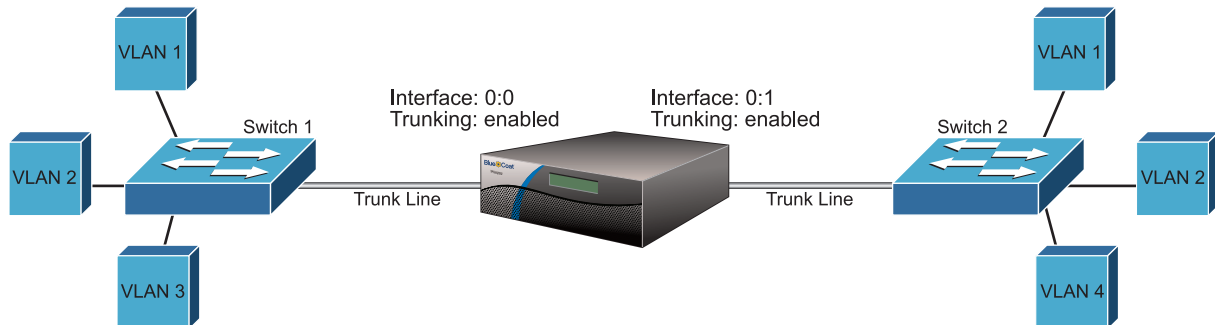
VLAN configuration occurs on the switch; the network administrator specifies which ports belong to which VLANs. This identification is called the native VLAN ID, also known as the PVID (Port VLAN Identifier). Switch ports can also be configured to be members of VLANs other than what is configured as their native VLAN





ID, however, a packet is only associated with one VLAN ID. At the packet level, VLAN identification is achieved by the switch tagging, or inserting, the VLAN ID into the packet header. VLAN tagging is only necessary, however, when VLANs span multiple switches; packets moving between switches are tagged so that the next switch inline knows the destination VLAN of the packet. When a packet is forwarded between switches, the forwarding switch determines which VLAN the packet belongs to inserts the VLAN ID into packet header. When the receiving switch is forwarded the tagged packet, it forwards the packet to the port(s) corresponding to that VLAN ID. If the VLAN ID of the packet is the same as the native VLAN ID of the port on which the packet is being forwarded, the tag is removed before the packet is forwarded. If the VLAN ID does not match, the packet is forwarded out of the interface, keeping the VLAN ID, or tag, intact. It is possible for connected switches to send and receive packets with no tag. This is only allowed, however, if the connecting interfaces are configured on the same native VLAN and traffic associated with that particular VLAN is being forwarded.

When VLANs span multiple switches, a trunk data link is required between the switches. With VLAN Tagging support, ProxySG appliances can be deployed inline between two switches on a trunk data link and perform VLAN trunking. By enabling VLAN trunking on the ProxySG appliance, all packets are accepted, regardless of their tag, and if configuration and policy allow, are passed from one interface to the other with the original VLAN tag preserved. If a packet arrives on one interface with a VLAN tag, the tag remains when it is forwarded out of another interface (assuming both interfaces are on the same native VLAN).



While VLAN trunking provides more deployment options for an administrator, the ProxySG appliance provides additional VLAN functionality. Specifically, ProxySG appliances can add or remove tags to ensure proper forwarding of packets in configurations in which trunk-enabled interfaces are on different native VLANs, or where one or more interfaces are configured with trunking disabled. If a packet arrives untagged and the destination interface has a different native VLAN configured than the interface on which it was received, the ProxySG appliance adds a tag to ensure that the VLAN is preserved. Similarly, if a tagged packet arrives and the VLAN ID matches the native VLAN of the destination interface, the ProxySG appliance removes the tag before forwarding the packet. This adding or stripping tags is the same functionality that a switch performs for a given interface port.