**VLAN hopping** is a [computer security exploit](https://en.wikipedia.org/wiki/Exploit_(computer_security)), a method of attacking networked resources on a [virtual LAN](https://en.wikipedia.org/wiki/Virtual_LAN) (VLAN). The basic concept behind all VLAN hopping attacks is for an attacking host on a VLAN to gain access to traffic on other VLANs that would normally not be accessible. There are two primary methods of VLAN hopping: **switch spoofing** and **double tagging**. Both attack vectors can be mitigated with proper switch port configuration.



**Contents**

* [1Switch spoofing](https://en.wikipedia.org/wiki/VLAN_hopping#Switch_spoofing)
  + [1.1Mitigation](https://en.wikipedia.org/wiki/VLAN_hopping#Mitigation)
* [2Double tagging](https://en.wikipedia.org/wiki/VLAN_hopping#Double_tagging)
  + [2.1Mitigation](https://en.wikipedia.org/wiki/VLAN_hopping#Mitigation_2)
  + [2.2Example](https://en.wikipedia.org/wiki/VLAN_hopping#Example)
* [3See also](https://en.wikipedia.org/wiki/VLAN_hopping#See_also)
* [4References](https://en.wikipedia.org/wiki/VLAN_hopping#References)

Switch spoofing[[edit](https://en.wikipedia.org/w/index.php?title=VLAN_hopping&action=edit&section=1)]

In a switch spoofing attack, an attacking host imitates a trunking switch[[1]](https://en.wikipedia.org/wiki/VLAN_hopping#cite_note-1) by speaking the tagging and trunking protocols (e.g. [Multiple VLAN Registration Protocol](https://en.wikipedia.org/wiki/Multiple_VLAN_Registration_Protocol), [IEEE 802.1Q](https://en.wikipedia.org/wiki/IEEE_802.1Q), [Dynamic Trunking Protocol](https://en.wikipedia.org/wiki/Dynamic_Trunking_Protocol)) used in maintaining a VLAN. Traffic for multiple VLANs is then accessible to the attacking host.

**Mitigation**[[edit](https://en.wikipedia.org/w/index.php?title=VLAN_hopping&action=edit&section=2)]

Switch spoofing can only be exploited when interfaces are set to negotiate a trunk. To prevent this attack on [Cisco IOS](https://en.wikipedia.org/wiki/Cisco_IOS), use one of the following methods:[[2]](https://en.wikipedia.org/wiki/VLAN_hopping#cite_note-Boyles,_2010-2):163

1. Ensure that ports are not set to negotiate trunks automatically by disabling [DTP](https://en.wikipedia.org/wiki/Dynamic_Trunking_Protocol#Switch_port_modes):

Switch (config-if)# switchport nonegotiate

2. Ensure that ports that are not meant to be trunks are explicitly configured as access ports

Switch (config-if)# switchport mode access

Double tagging[[edit](https://en.wikipedia.org/w/index.php?title=VLAN_hopping&action=edit&section=3)]

In a double tagging attack, an attacker connected to an [802.1Q](https://en.wikipedia.org/wiki/802.1Q)-enabled port prepends [two VLAN tags](https://en.wikipedia.org/wiki/IEEE_802.1Q#Double_tagging) to a frame that it transmits. The frame (externally tagged with VLAN ID that the attacker's port is really a member of) is forwarded without the first tag because it is the native VLAN of a trunk interface. The second tag is then visible to the second switch that the frame encounters. This second VLAN tag indicates that the frame is destined for a target host on a second switch. The frame is then sent to the target host as though it originated on the target VLAN, effectively bypassing the network mechanisms that logically isolate VLANs from one another.[[3]](https://en.wikipedia.org/wiki/VLAN_hopping#cite_note-3) However, possible replies are not forwarded to the attacking host (unidirectional flow).

**Mitigation**[[edit](https://en.wikipedia.org/w/index.php?title=VLAN_hopping&action=edit&section=4)]

Double Tagging can only be exploited on switch ports configured to use *native VLANs*.[[2]](https://en.wikipedia.org/wiki/VLAN_hopping#cite_note-Boyles,_2010-2):162 Trunk ports configured with a *native VLAN* don't apply a VLAN tag when sending these frames. This allows an attacker's fake VLAN tag to be read by the next switch.[[4]](https://en.wikipedia.org/wiki/VLAN_hopping#cite_note-4)

Double Tagging can be mitigated by any of the following actions (Incl. IOS example):

* Simply do not put any hosts on VLAN 1 (The default VLAN). i.e., assign an access VLAN other than VLAN 1 to every access port

Switch (config-if)# switchport access vlan 2

* Change the native VLAN on all trunk ports to an unused VLAN ID.

Switch (config-if)# switchport trunk native vlan 999

* Explicit tagging of the native VLAN on all trunk ports. *Must be configured on all switches in network autonomy.*

Switch(config)# vlan dot1q tag native

**Example**[[edit](https://en.wikipedia.org/w/index.php?title=VLAN_hopping&action=edit&section=5)]

As an example of a double tagging attack, consider a secure web server on a VLAN called VLAN2. Hosts on VLAN2 are allowed access to the web server; hosts from outside VLAN2 are blocked by layer 3 filters. An attacking host on a separate VLAN, called VLAN1(Native), creates a specially formed packet to attack the web server. It places a [header](https://en.wikipedia.org/wiki/Header_(computing)) tagging the packet as belonging to VLAN2 under the header tagging the packet as belonging to VLAN1. When the packet is sent, the switch sees the default VLAN1 header and removes it and forwards the packet. The next switch sees the VLAN2 header and puts the packet in VLAN2. The packet thus arrives at the target server as though it was sent from another host on VLAN2, ignoring any layer 3 filtering that might be in place.[[5]](https://en.wikipedia.org/wiki/VLAN_hopping#cite_note-5)

See also[[edit](https://en.wikipedia.org/w/index.php?title=VLAN_hopping&action=edit&section=6)]

* [Private VLAN](https://en.wikipedia.org/wiki/Private_VLAN)

References[[edit](https://en.wikipedia.org/w/index.php?title=VLAN_hopping&action=edit&section=7)]

* 1. [**^**](https://en.wikipedia.org/wiki/VLAN_hopping#cite_ref-1) *Rik Farrow (2003-03-17).*[*"VLAN Insecurity"*](http://rikfarrow.com/Network/net0103.html)*. Retrieved 2017-06-07.*
  2. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/VLAN_hopping#cite_ref-Boyles,_2010_2-0) [***b***](https://en.wikipedia.org/wiki/VLAN_hopping#cite_ref-Boyles,_2010_2-1) *Boyles, Tim (2010).*[*CCNA Security Study Guide: Exam 640-553*](https://dl.acm.org/citation.cfm?id=1841651)*. SYBEX Inc.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*9780470527672*](https://en.wikipedia.org/wiki/Special:BookSources/9780470527672)*.*
  3. [**^**](https://en.wikipedia.org/wiki/VLAN_hopping#cite_ref-3) *Rouiller, Steve A.*[*"Virtual LAN Security: weaknesses and countermeasures"*](https://www.sans.org/reading-room/whitepapers/networkdevs/virtual-lan-security-weaknesses-countermeasures-1090)*. SANS Institute InfoSec Reading Room. Retrieved 2017-06-07.*
  4. [**^**](https://en.wikipedia.org/wiki/VLAN_hopping#cite_ref-4) [*"What is Double tagging attack and how to prevent Double tagging attack"*](http://www.omnisecu.com/ccna-security/what-is-double-tagging-attack-how-to-prevent-double-tagging-attack.php)*. Retrieved 2017-10-15.*
  5. [**^**](https://en.wikipedia.org/wiki/VLAN_hopping#cite_ref-5) [*"Configuration Examples Related to VLAN Features"*](https://web.archive.org/web/20130128125232/http:/www.cisco.com/en/US/docs/switches/lan/catalyst2900xl_3500xl/catalyst1900_2820/version8.00.03/scg/AleakyV.html)*. Catalyst 2820 and 1900 Enterprise Edition Software Guide.*[*Cisco*](https://en.wikipedia.org/wiki/Cisco)*. Archived from*[*the original*](http://www.cisco.com/en/US/docs/switches/lan/catalyst2900xl_3500xl/catalyst1900_2820/version8.00.03/scg/AleakyV.html)*on 2013-01-28. Retrieved 2017-06-07.*