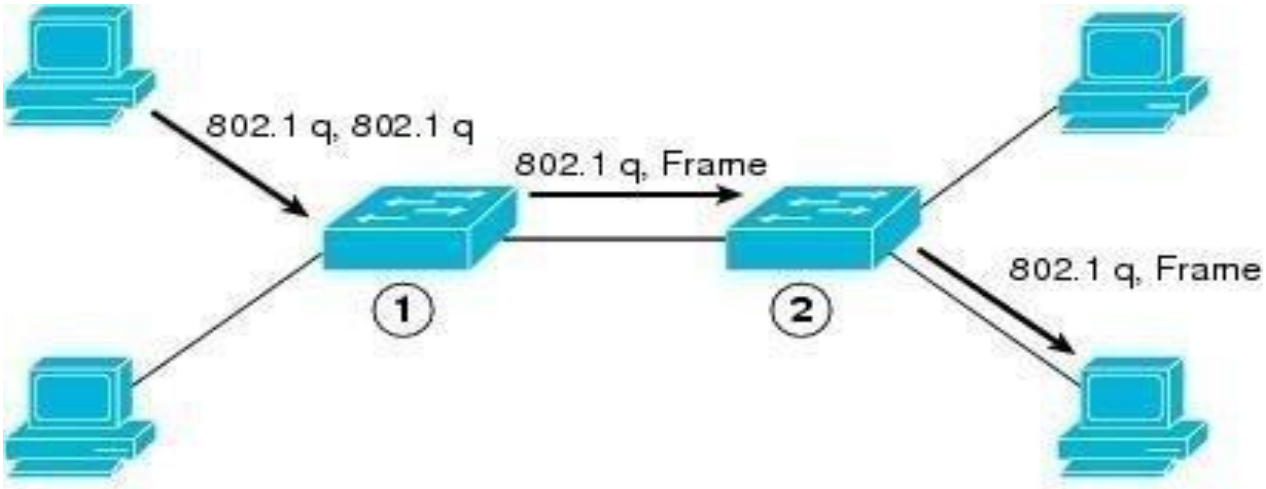
VLAN Hopping

VLAN Hopping is one of the primary VLAN based attacks used by hackers to infiltrate network security. VLAN hopping is used to attack a network by sending packets to a port which is generally not accessible. VLAN hopping attacks are mainly conducted in the Dynamic TrunkingProtocol and, in some cases; the attacks are targeted to the trunking encapsulation protocol (802.1q or ISL). The Dynamic Trunking Protocol is utilized for negotiating trunking on links between devices and the type of trunking encapsulation to be used.

Types of VLAN Hopping

Switch Spoofing

If a network switch is in place for autotrunking, the network attacker manages to configure a system that spoof or passes itself off as a switch. This means that the network attacker is capable of emulating either ISL or 802.1q signaling together with Dynamic Trunk Protocol (DTP) signaling. If successful, the hacker enters into a switch which gives every indication that it has a continuous need to trunk. This allows the attacking system to gain access all the VLANs allowed on the trunk port.



Double Tagging

In this form of VLAN hopping, the attacker tries to send data from one switch to another by sending frames with two 802.1Q headers – one for the victim switch and the other for the attacking switch. The victim switch accepts the frame because it thinks it is supposed to receive the incoming data. The target switch then forwards the frame to the destination based on the VLAN identifier in the second 802.1q header.

Consequences of VLAN Hopping

VLAN hopping can disable any security measures users may have in place on the device which maps routes between the VLAN's. Hackers use VLAN hopping to capture sensitive information such as bank account details and passwords from targeted network subscribers. VLAN hopping is also used by some attackers to corrupt, modify, or delete data from the end user's computer. Another intended use of VLAN hopping is to propagate viruses, worms, Trojan horses, and other malicious programs such as malware and Spyware.

Preventing VLAN Hopping

VLAN hopping can be prevented to some extend by turning off the autotrunking feature of all the switches which do not require trunking and by following specific recommendations from switch suppliers on VLAN security.

You should never use the default VLAN either because VLAN hopping is much more easily accomplished from the default VLAN. A good security measure is to assign all your used interfaces to some VLAN and never using any default VLAN, (typically VLAN 1) for anything.

Source: http://www.tech-faq.com/vlan-hopping.html