If you're responsible for securing a corporate or private network, you need to be aware of the vulnerabilities that attackers will use. Security expert Sean Wilkins discusses seven common methods that can give attackers access, helping them to control or steal information from your network.

**Like this article? We recommend**

[CCNA Routing and Switching 200-120 Network Simulator](https://www.pearsonitcertification.com/store/ccna-routing-and-switching-200-120-network-simulator-9780789750884?w_ptgrevartcl=7+Popular+Layer+2+Attacks_2491767)  
  
[Learn More](https://www.pearsonitcertification.com/store/ccna-routing-and-switching-200-120-network-simulator-9780789750884?w_ptgrevartcl=7+Popular+Layer+2+Attacks_2491767) [Buy](https://www.pearsonitcertification.com/buy.aspx?isbn=9780789750884&w_ptgrevartcl=7+Popular+Layer+2+Attacks_2491767)

**Overview**

A large number of common threats need to be considered when securing a network, but a frequently overlooked area is the security of the LAN. When people think about security, often they’re thinking specifically of the layers above Layer 2, but there’s no reason to limit a security plan to these upper layers. A good security plan should account for *all* layers, from Layer 1 through Layer 7. This article takes a look at some of the most common Layer 2 attacks and how they operate.

**Spanning Tree Protocol (STP) Attacks**

The Spanning Tree Protocol (STP) is used on LAN-switched networks. Its primary function is removing potential loops within the network. Without STP, Layer 2 LANs simply would stop functioning, because the loops created within the network would flood the switches with traffic. The optimized operation and configuration of STP ensures that the LAN remains stable and that traffic takes the most optimized path through the network. If an attacker inserts a new STP device onto the network and attempts to alter the operation of STP, this attack has the potential to affect how traffic flows through the LAN, greatly affecting the usability and security of the traffic flowing through the network.

**Address Resolution Protocol (ARP) Attacks**

The Address Resolution Protocol (ARP) is used by all network devices that connect to an Ethernet network. Devices use ARP to find the Layer 2 Ethernet address (MAC) for a destination device, using only the target device’s known IP address. ARP by itself is inherently insecure because devices are told to trust the answers they receive. So if device A requests the MAC address of device B, and device C answers in place of device B, device A will send all traffic destined for device B to device C. If device C was attempting to run a transparent attack, it would then forward the traffic to device B while recording the data from the traffic; this is called a *man-in-the-middle* (MITM) attack.

**Media Access Control (MAC) Spoofing**

In a Media Access Control (MAC) spoofing attack, one device on a network uses the MAC address of another device. The goal of the attacker is to redirect all of the traffic for the targeted device to the attacking device. If you think about a telephone network, this attack is the equivalent of someone taking over your phone number and having future calls rerouted to them. This rerouting could be used to disguise one device as another for multiple purposes, including to act as that device (possibly a server), or to perform a [denial-of-service attack](file:///\\store\ccna-routing-and-switching-200-120-network-simulator-9780789750884) on that device.

**Content Addressable Memory (CAM) Table Overflows**

The Content Addressable Memory (CAM) tables, also called *MAC address tables*, on switches are used to track where to send traffic for specific learned MAC addresses. To grasp the true effect of this attack, you need to understand the basic operation of the CAM table and how it optimizes the forwarding behavior of the switch.

When a switch is turned on, it has a blank CAM table. It doesn’t know which devices are connected to which interfaces, and therefore it initially sends received traffic out to all interfaces (flooding). As the CAM table receives traffic in each interface, it creates entries for each of the MAC addresses it sees, linking each address with its specific interface.

Once the switch has an entry for a specific destination MAC address in its CAM table, it doesn’t forward the traffic out to all interfaces; instead, it sends the traffic for that address to its specific learned interface. Once all of the connected device MAC addresses are learned, almost no traffic will be flooded; traffic will be sent out to each destination’s learned interface. This result greatly optimizes the forwarding behavior of the switch, and it increases the amount of bandwidth available through the switch (assuming that it’s a busy switch).

Every switch limits the number of MAC addresses that the CAM address table can hold. If the table limit is reached, all traffic from unknown MAC addresses will be flooded. A CAM table overflow attack works by having a single device (or a few devices) spoof a large number of MAC addresses and send traffic through the switch. The switch’s CAM table will be filled, and all other traffic (typically the traffic from legitimate devices) will be flooded, causing the switch to become very busy and potentially overloaded. As a result, the network rapidly slows down and eventually becomes unusable.

**Cisco Discovery Protocol (CDP)/Link Layer Discovery Protocol (LLDP) Reconnaissance**

The Cisco Discovery Protocol (CDP) and the Link Layer Discovery Protocol (LLDP) are used for similar purposes. Both offer a way to see which types of devices are connected on a link, as well as some of the device configuration (IP address, software version, and so on). Typically this information is used by network engineers to improve troubleshooting efficiency on large networks. However, this information is also typically open to anyone who is “listening,” which means that an attacker just has to listen on the same link in order to obtain a large amount of information about the connected devices.

**Virtual LAN (VLAN) Hopping**

There are two types of virtual LAN (VLAN) hopping attacks, but the goal is the same—sending traffic to another VLAN:

* **Switch spoofing.** In this attack, the attacker attempts to connect a rogue switch into the network and then set up a trunk. If the attack is successful, traffic from multiple VLANs can be sent to and through the rogue switch, enabling the attacker to view and potentially manipulate the traffic. This attack relies on the default behavior of some switches that support dynamic trunking: If dynamic trunking is disabled, and all non-trunk interfaces are configured not to become trunked, this attack is mitigated.
* **Double tagging.** To understand double tagging, you need some VLAN basics. Virtual LANs provide security on LANs by isolating traffic into separate traffic *lanes*. Traffic from all VLANs (except for the native VLAN) is “tagged” with an IEEE 802.1q tag when the traffic is sent over trunks between switches. These tags can be nested, which means that traffic can have multiple attached tags. If a frame with two nested tags is received on a trunking interface, and the first tag (the outermost tag) is the same as the tag for the native VLAN for that interface, some switches will remove that outer tag and send the traffic along to the VLAN of the second tag. This design allows an attacker to send traffic from one VLAN into another VLAN (hopping), which is supposed to be impossible without a Layer 3 device.

**Dynamic Host Configuration Protocol (DHCP) Spoofing**

Similar to the other types of spoofing attacks, Dynamic Host Configuration Protocol (DHCP) spoofing involves an attacker pretending to be someone else; in this case, acting as the legitimate DHCP server. Since DHCP is used on most networks to provide addressing and other information to clients, losing control of this part of the network can be dangerous.

In DHCP spoofing attacks, the attacker places a rogue DHCP server on the network. As clients are turned on and request an address, the server with the fastest response is used. If the device receives a response from the rogue server first, the rogue server can assign any address as well as control which device it uses as a gateway. A well-designed attack can funnel traffic from local hosts to a rogue server that logs all traffic and then forwards the traffic out to the “correct” gateway; to the device, this action would be almost transparent. Thus, the attacker can steal information almost invisibly.

**Summary**

To secure the network, a security engineer must be aware of a wide variety of attack types. This article has examined only a few of the most common Layer 2 attacks. There are many more, and some attacks probably haven’t been used (or discovered) yet. The true work of the network security engineer is to learn where the next attack will originate and determine how to mitigate it—before the attack occurs, or as soon as it does.

I hope this article provides enough of a primer to fulfill your current needs. For further information about these types of attacks and how to mitigate them, check out the [*CCNA Security 210-260 Official Cert Guide*](https://store/ccna-security-210-260-official-cert-guide-9781587205668).