
# Techniques for securing switches against attacks

Author: Jack Gates (1500763)

BSc (Honours) Ethical Hacking

Institution: University of Abertay, Dundee.

2017

# Contents

# Abstract

This Whitepaper will investigate common attacks against a switch and also techniques a person can perform in order to prevent them. It will demonstrate how these attacks will be performed by a hacker, and offer configuration techniques a person can undergo to mitigate them. There are several ways a malicious person can attack a switch and if it is not configured using sufficient methods then a user's security could be at risk. A variety of popular attacks will be discussed in this paper, along with the mitigation techniques necessary to circumvent them.

With the rapid growth of the internet, a lot of concern has been raised for network security. The reason the data-link layer is being investigated in this paper is because it is often overlooked in network security, although in actuality, this layer has several unique vulnerabilities that can be exploited by a malicious person. Attacking a networks data-link security is so popular among malicious hackers as the consequences can be very severe. The data-link layer should therefore be given just as much attention when it comes to security as any of the other network layers on the OSI model.

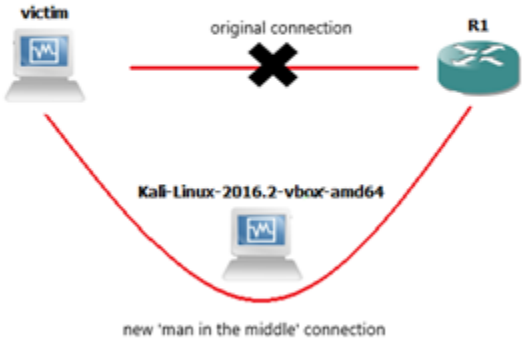
The purpose of this Investigation is to give a user insight into just how vulnerable the data-link layer of their network may be, and that switch security should not be overlooked. It will also educate them on the different kinds of attacks that can be launched against their data link layer, to allow them to test their security for themselves. This investigation will also teach a user the methods available for securing the data-link layer of their network against the attacks investigated.

# 1 Introduction

Networks have been growing rapidly in recent years. The data-link layer of a network, also known as Layer 2 of the OSI model, is where data transfers between adjacent network nodes happen. There are several ways in which a malicious person can abuse the data-link layer of a network, which is where the switches work. However, luckily most network switches offer a wide range of features that can keep a networks data-link layer secure. The best way to prevent a network from an attack is to first understand the most popular methods used for attacking a networks data-link layer and to configure a network in such a way that makes these attacks impossible. There are four popular attacks in particular that will be discussed, below is a brief summary of each, along with a description of the features that these attacks exploit.

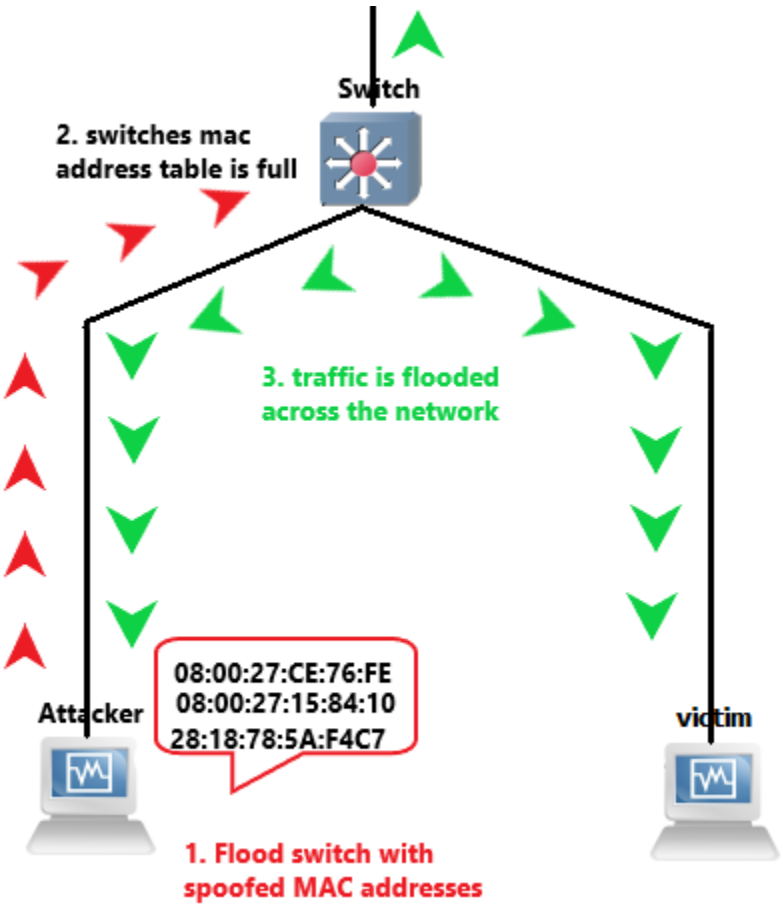
## *1.1* ARP flooding

The address resolution protocol (ARP) is a protocol that is used to map IP network addresses to the hardware (MAC) address that is recognised in the LAN. ARP spoofing can only work if it is on a LAN that uses the address resolution protocol. ARP spoofing is an attack in which a malicious user sends fake ARP messages over a LAN resulting in their MAC address being linked with the victims IP address. The malicious user can then start receiving the data that was intended for the victims IP address. Not only can they intercept this data, but they can also modify the data or stop the victim from receiving the data. This attack is also known as a 'man in the middle' attack as the attacker is secretly relaying packets between two parties on the network. This means that all the traffic going between the two parties will flow through the attacker. The new path that the packets will follow is illustrated below.



## *1.2* Mac address spoofing

Every network interface has a MAC address, which is used as a unique identifier. Whenever devices are communicating on a network the switch will receive the packet and look up the destination Media Access Control (MAC) address in what's called a MAC address table. However, if the MAC address does not match any of the addresses in the table, then the switch that received the packet will forward the frame onto every other port. A switches Mac address table can only store a limited amount of memory, and once it is full, the switch cannot save any more MAC addresses. MAC address flooding makes use of this limited size of memory and starts loading a switches MAC address table with fake sources of MAC addresses until it is full, thousands are generated and can keep the switch full for as long as the hacking tool is used. When it can no longer store any MAC addresses it will enter a fail-open mode, then the switch will start broadcasting all of its received packets to every port on the switch, including the attackers port.

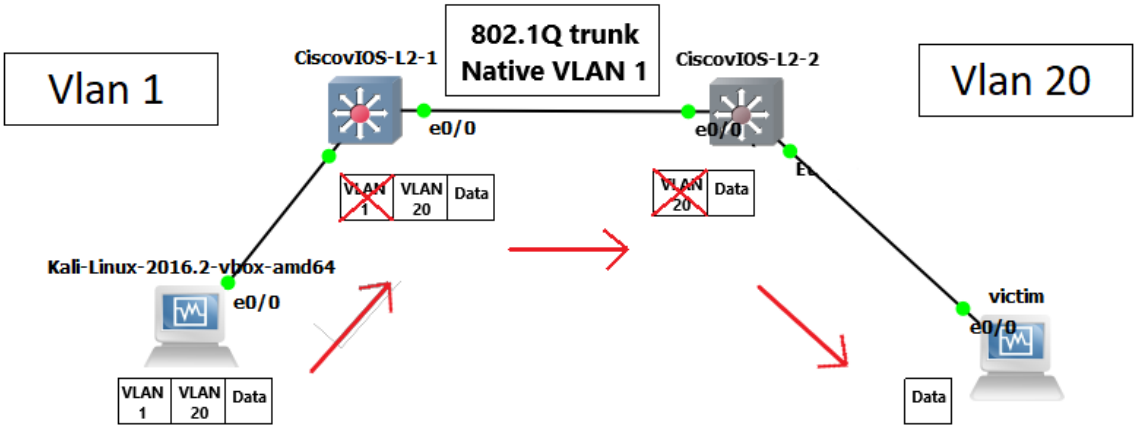



## *1.3* VLAN hopping

A VLAN (Virtual Local area network) is just a local network that maps devices together, but not based on geography, for example different departments or user types. VLAN hopping is when a malicious user on

a VLAN gains access to traffic on other VLANS that would normally not be accessible to them. There are two ways in which a VLAN hoping attack can occur and they both rely on poor switch port configuration.

Switch spoofing is when the malicious user configures a system to spoof itself as a switch so they must be capable of emulating 802.1Q and DTP messages. The attacker will trick the victim switch into thinking that another switch is attempting to form a trunk, and then can gain access to all the VLANs allowed on the trunk port. Double tagging is the other method of VLAN hopping – The attacker must be on the same VLAN as the trunks native. The attacker transmits data through one switch to another by sending frames with two 802.1Q tags, one of their own VLAN, and another for the VLAN they want to gain access to. The target switch will think that the frame was intended for them and send the frame along to the target host. The diagram below will show what will happen to the double tagged packet as it makes its way across the network.




## *1.4* CDP flooding attack

the CDP (Cisco discover protocol) is a protocol for a device that discovers other devices that are directly connected to it. It shares information between devices depending on the type of device, such as the IP address, the VLAN, and operating system versions. CDP messages are broadcast, by default every 60 seconds, out of each connected interface of a device. This packet is then received by the switch (or any other device that supports CDP). This protocol is used to simplify the configuration and connectivity of a network.

A CDP flooding attack is known as a Dos (denial of service) attack as they can freeze a switches operating system, and force it to drop traffic. It can also cause the switch to start forwarding traffic out of all of its ports, allowing the attacker to sniff for packets that could contain valuable information. This attack is done by flooding a devices CDP table with thousands of spoofed messages and causing it to run out of memory.

These attacks will be demonstrated throughout this investigation, to give a user a great understanding of how these attacks work, and to illustrate how simple they are to perform which will highlight the reasons for having a secure data-link layer. They will be easy to follow to allow a user to test these

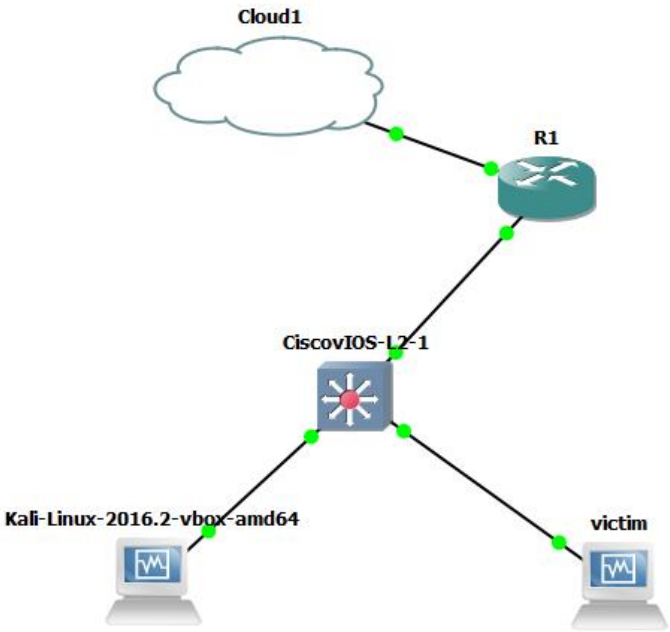
attacks on their network themselves for security purposes. This investigation will also exhibit the actions necessary to mitigate these attacks, which will give insight into how to keep the data-link layer secure. The mitigation tutorials will be short and concise, to provide the knowledge necessary to secure a network. Another aim of this report is to show that layer 2 security should not be overlooked in any organisational network. It should be noted that this report is not intended to show all possible switch security methods but simply highlight some of the most commonly referenced.

# 2 Procedures and Results

This section will cover the popular attacks that could put a networks data-link layer at risk. It will do this by demonstrating how the attack can happen through the aid of diagrams and screenshot, allowing a user to see a step-by-step view of the process. It will also offer an explanation of what is happening at each stage, which tools are being used, and how the user can replicate the attacks on their own network. After the attack has been demonstrated this section will give a brief description of what the consequences of the attack are.

At the end of each attack demonstration, there is a mitigation section underneath. This section will go into detail about how the attack can be prevented through the configuration of the network or the use of certain features. The mitigation techniques will be demonstrated using screenshots, and will also include an explanation of how that technique works. Below, four different kinds of popular attacks are demonstrated and there is a mitigation to go along with each attack.

## *2.1.1* Arp Flooding




On the network diagram above, we can see a configuration of a network, where the router (R1) is a DHCP server connected to the internet and a switch with two hosts. On this network, the data would normally be sent between the hosts – the attacker and our victim - and the router. With an ARP attack, the packets are instead sent to our attackers' machine who then relays them, to make the targets believe that they are talking to each other. The attacker can do this by scanning for the IP addresses of the victim and default gateway, then they send a fake ARP reply message to the default gateway, informing it that the attackers' MAC address should now be associated with the targets' IP address and also that the targets MAC address is associated with the attackers. Once the default gateway receives this message, all of the victims traffic will flow through the attackers' machine. The attacker can then eavesdrop on all of the packets being sent between them to obtain potentially valuable information. This path that the packets will follow is illustrated in the introduction, under section 1.1.

To perform an ARP attack, our malicious user will first need to scan the network so that they can gather the information they need in order to launch this attack. First, the IP route will be checked, so that they know the IP of the default gateway as well as the network interface being accessed by them. After That the attacker will also have to make sure that the data that is sent to him will pass through them and onto it's real destination, otherwise the victim will not be connected to the DHCP server and this attack will not work. The attacker does this by turning on IP forwarding using the second command. IP forwarding is the process used to determine which path a packet can be sent. It is set to '1' which means that it is enabled.

```
root@menmuir:~# ip route
default via 10.0.10.1 dev eth0
10.0.10.0/24 dev eth0 proto kernel scope link src 10.0.10.4
root@menmuir:~# echo 1 > /proc/sys/net/ipv4/ip_forward
```

At this stage the attacker will now have to scan for its victim. They can do this using a program like Nmap, to scan for all of the live hosts on the 10.0.10.0 network. They can do this by typing ‘nmap -sP’ and then the range of IP addresses to scan. ‘sP’ means ping scan the entire range and list hosts that respond. As seen in diagram 1.4, the attacker has found 3 live hosts on the network. They would already know their own address and the gateway address, so they can choose any other host that the scan has picked up, in this case address 10.0.10.5.

```
root@menmuir:~# nmap -sP 10.0.10.0-100

Starting Nmap 7.40 ( https://nmap.org ) at 2017-10-27 12:21 EDT
Nmap scan report for 10.0.10.1
Host is up (0.061s latency).
MAC Address: C2:01:24:44:00:01 (Unknown)
Nmap scan report for 10.0.10.5
Host is up (0.18s latency).
MAC Address: 08:00:27:21:27:37 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.10.4
Host is up.
Nmap done: 101 IP addresses (3 hosts up) scanned in 3.42 seconds
```

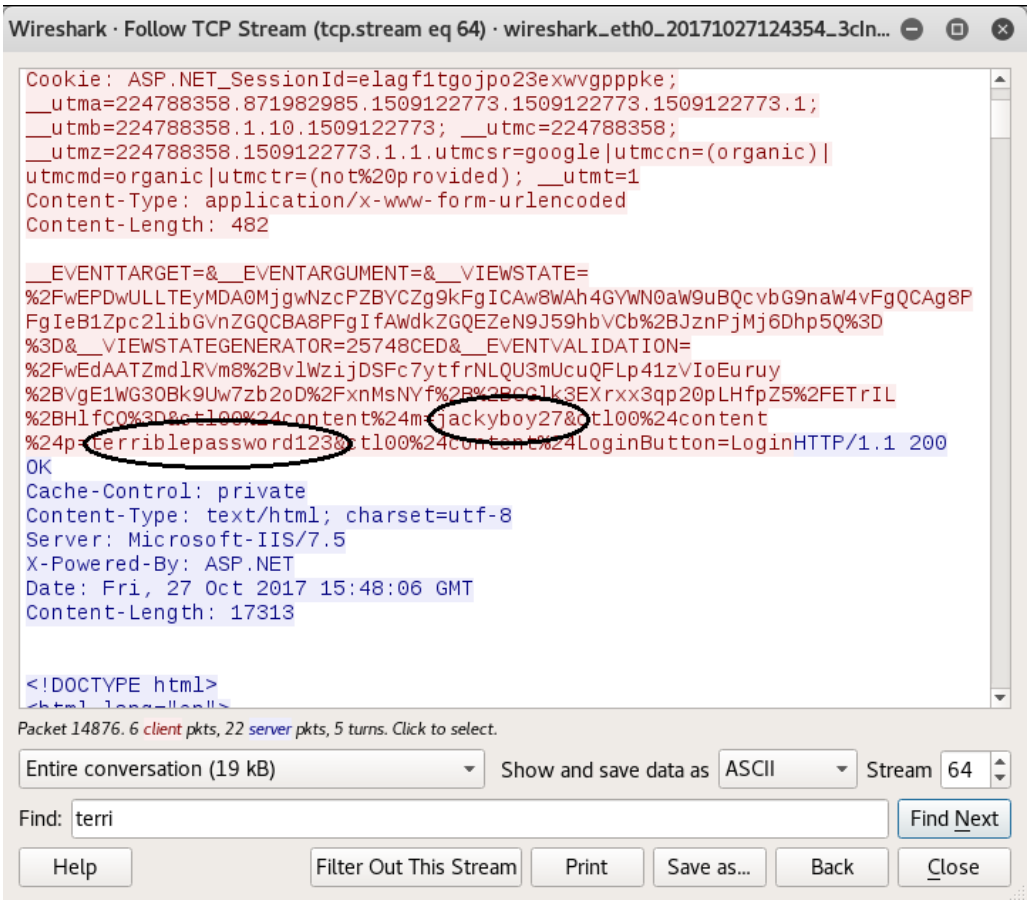
Now the attacker has all of the information that they need to perform an ARP flooding attack. With a tool like ‘arpspoof’ all they need is to type in one command to launch an attack. All the command needs is the data previously gathered using simple scanning techniques – the network interface, the default gateway, and the victims address. To enter the interface type ‘-i’ before the network interface being attacked (we are using ethernet 0), for the target type ‘-t’ and then target (our target is 10.0.10.5), and then type ‘-r’ and then the default gateway (10.0.10.1 is the gateway being used in this demonstration). After the command is executed, a spoofed ARP response is sent to the default gateway, and the attacker will then start receiving ARP replies that tell us that the attackers mac address is tied to both the gateway and the victim.

```
root@menmuir:~# arpspoof -i eth0 -t 10.0.10.5 -r 10.0.10.1
8:0:27:27:6:d4 8:0:27:21:27:37 0806 42: arp reply 10.0.10.1 is-at 8:0:27:27:6:
d4
8:0:27:27:6:d4 c2:1:24:44:0:1 0806 42: arp reply 10.0.10.5 is-at 8:0:27:27:6:d
4
8:0:27:27:6:d4 8:0:27:21:27:37 0806 42: arp reply 10.0.10.1 is-at 8:0:27:27:6:
d4
8:0:27:27:6:d4 c2:1:24:44:0:1 0806 42: arp reply 10.0.10.5 is-at 8:0:27:27:6:d
4
```

Now that the attack has been successfully launched, the attacker can eavesdrop on the packets using software like wireshark, which will allow him to see all of the packets being sent and received from the victim. A lot of packets will be sent to the attacker, so it would be a good idea for him to filter the packets, based on protocols for example. In this scenario the attacker decides that they want to look for http packets. They can see all the domains the victim has visited and can also find text that was input and sent from the target to a particular domain.

```
14969 197.298598343 86.54.42.236   10.0.10.5   TCP    1514 [TCP segment of a reassembled PDU
14970 197.298601728 86.54.42.236   10.0.10.5   TCP    1514 [TCP Retransmission] 80→54724 [A
14971 197.309470130 86.54.42.236   10.0.10.5   HTTP    363 HTTP/1.1 200 OK  (text/html)
14972 197.309491731 86.54.42.236   10.0.10.5   TCP     363 [TCP Retransmission] 80→54724 [P
14975 197.315601089 10.0.10.5      86.54.42.236 TCP     60 54724→80 [ACK] Seq=1185 Ack=1460
```

Investigating certain packets, such as http packets, could reveal sensitive data, such as log-in usernames and passwords.




Through just eavesdropping on the packets sent, the attacker now can access the victims account on the domain being used and the victim has no idea that the attack has happened. ARP spoofing is a very common attack on networks, and given the right circumstances can be a very harmful attack for the target. In this example, we only eavesdropped, but it is also possible for a hacker to alter the packets sent as a way to manipulate the victim. It is a pretty straight forward attack as all a hacker really needs is his machine to be within reception range of an unencrypted wireless access point, and a poorly configured network.

## *2.1.2* Arp Flooding Mitigation

To avoid being susceptible to an ARP spoofing attack, it is important to employ proper mitigation techniques. Layer 2 security features such as DHCP snooping, and dynamic ARP inspection (DAI) can be used to prevent this. DHCP snooping acts like a firewall between untrusted hosts and trusted DHCP servers. It drops DHCP traffic that it determines to be unacceptable. This includes DHCP messages from

a server that is not trusted. By default, all ports are untrusted and the user can configure which ports are trusted manually. Typically, the trusted ports are for DHCP servers or any relay agents for a DHCP server, and the untrusted ports are for the clients.

The other security feature that will be implemented is known as Dynamic Arp Inspection (DAI). This feature validates ARP packets within a network, it does this by evaluating an ARP packets MAC/IP address binding and compares it with the MAC/IP bindings contained in what is known as a binding table. if an ARP packets information is inconsistent with what is held in the binding table, then it is dropped. DAI intercepts all ARP requests and responses on ports that are not trusted.

Configuring these security features can be done in the configuration terminal of the switch. To set up DHCP snooping on the network, simply type 'ip dhcp snooping' in the configuration and to set up dynamic ARP inspection, type 'ip arp inspection vlan [VLAN id]'. The VLAN ID should be of the VLAN where DAI will be used which is our trunks native VLAN as all traffic on the trunk should be trusted.

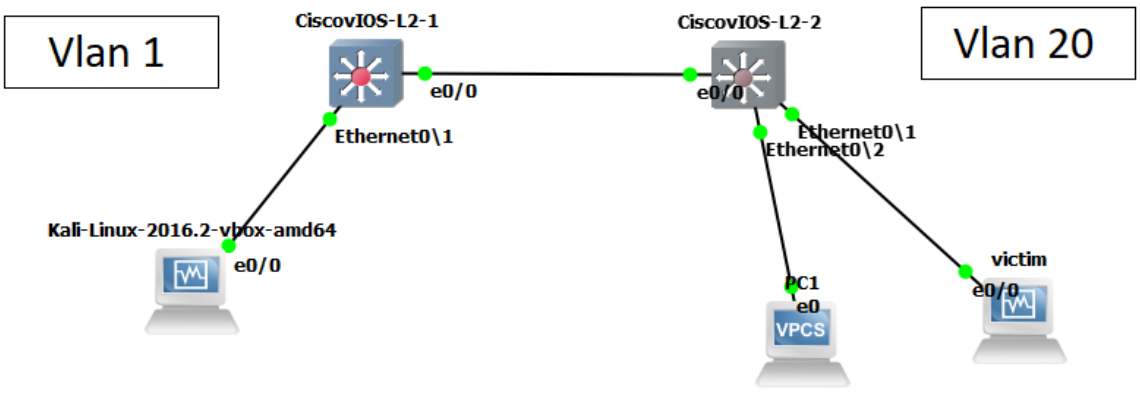
```
Switch(config)#ip dhcp snooping
Switch(config)#ip arp inspection vlan 1
Switch(config)#
```

To set up the trusted ports, the interface of the port to be configured must be accessed in the terminal, then each feature must be set to trust. This port is the port that leads to R1. To configure that port as a port that the DAI feature trusts type 'ip arp inspection trust' and to configure the port as a port that DHCP snooping trusts, type 'ip dhcp snooping trust'.

```
Switch(config)#int gigabitEthernet 0/2
Switch(config-if)#ip arp inspection trust
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#exit
```

## *2.2.1* VLAN Hopping

There are two different ways in which a malicious user can hop from one VLAN to another to access private data. The first method that will be covered is known as switch spoofing, which is when an attacker takes advantage of the Dynamic Trunk Protocol (DTP). If a network switch ports mode is set to Dynamic auto, then this means that the port is willing to convert the link into a trunk. An attacker can



turn their port into a trunk port if it is set to dynamic auto, which will allow them to see the traffic of all the VLANS on the network. Below is a simple network configuration with two VLANS, 1 and 20. The attacker is situated on VLAN 1, but wants to listen to traffic on VLAN 20.

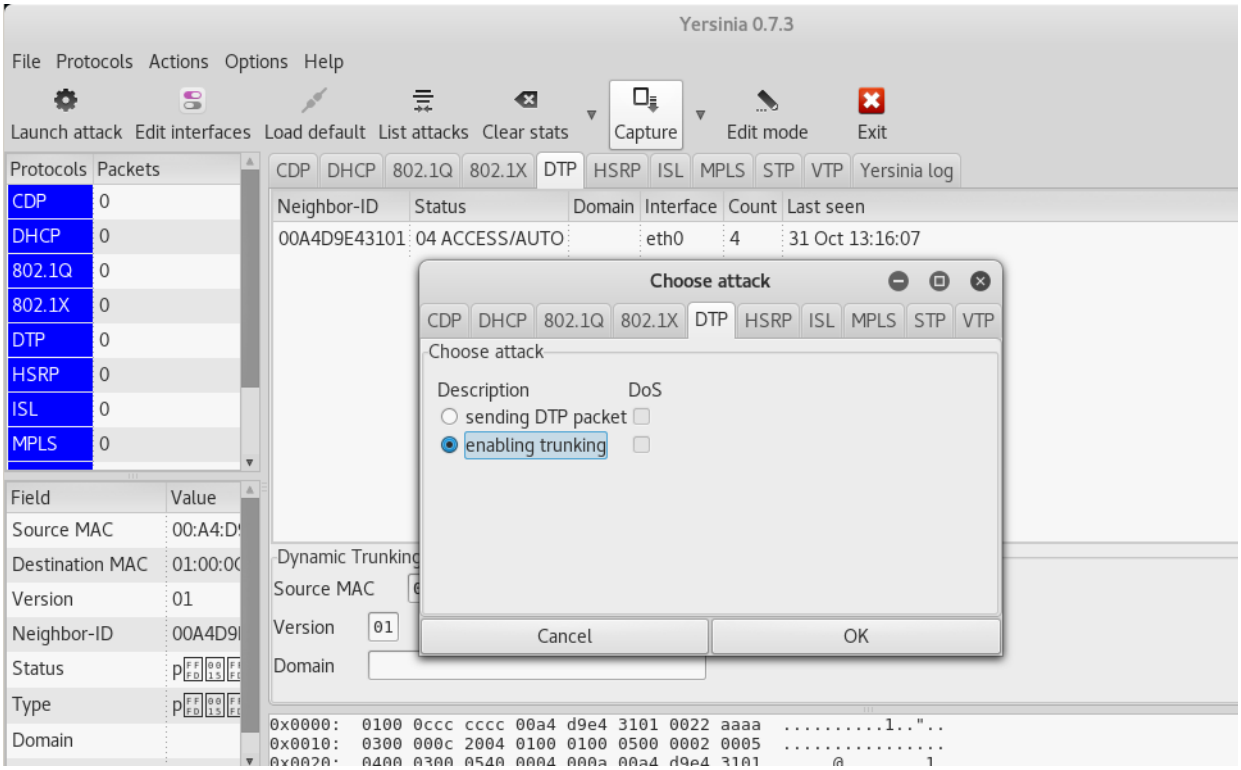
Going into the first switch, we can see that there is a trunk formed on port GigabitEthernet0/0. The trunk carries traffic for all of the VLANS across the network. In privileged execution mode we can see all the VLANS allowed on this trunk and active in the management domain. We can also see that trunking mode is automatic.

```
s1>
s1>en
s1#show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi0/0       auto             n-isl          trunking      1

Port        Vlans allowed on trunk
Gi0/0       1-4094

Port        Vlans allowed and active in management domain
Gi0/0       1,20

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/0       1,20
```

To launch the attack, the attacker will load up a program called Yersinia. Yersinia is a too which can take advantages of certain weaknesses in network protocols, in our case it takes advantage of poorly configured ports in order for us to set up the attackers' port as a trunk. To launch Yersinia, type in the following command.

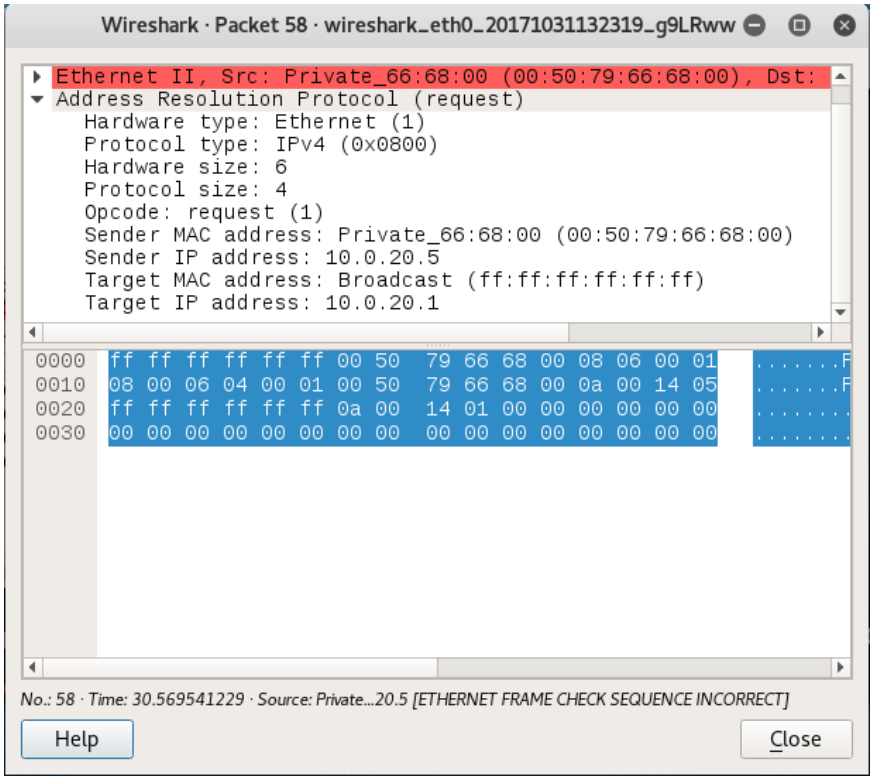
```
root@menmuir:~# yersinia -G
```

After the program has opened, the attacker can click the launch attack button on the top left side of the screen. They then select the DTP menu and click on "enabling trunking" and okay. Now if the interface trunk is checked again, it is apparent that there are two trunks.




```
s1#show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi0/0       auto             n-isl          trunking      1
Gi0/1       auto             n-802.1q       trunking      1

Port        Vlans allowed on trunk
Gi0/0       1-4094
Gi0/1       1-4094

Port        Vlans allowed and active in management domain
Gi0/0       1,20
Gi0/1       1,20

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/0       1,20
Gi0/1       none
```

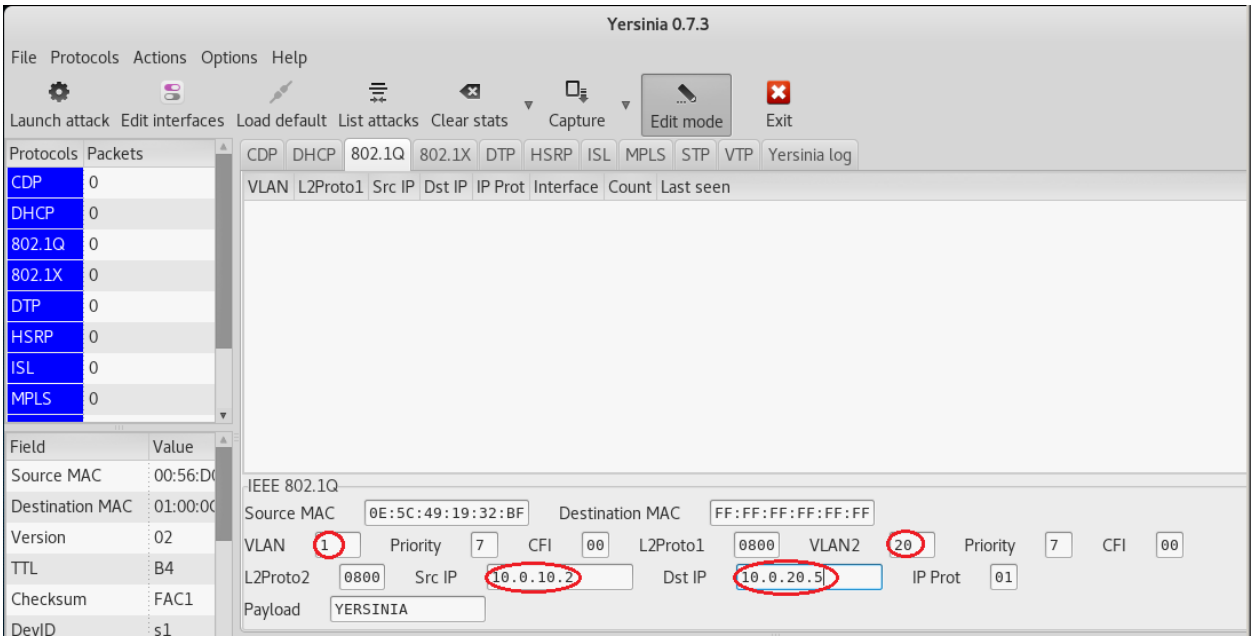
Now that the attacker has successfully set their port on the network to trunking, they can see the traffic on all the VLANS on the network, and will be able to view packets from the machines on VLAN 20 using packet sniffing software like wireshark. The attacker can now access private data being sent across the whole network on all of the different VLANS.




The other method of VLAN hopping that an attacker might choose, is known as double tagging. For this to work, the attacker's access VLAN must be the same as the trunks native VLAN. In this scenario, they are both set as VLAN 1. A double tagging attack takes advantage of the tag removal process that many types of switches perform as most switches remove only one tag. The attacker changes the packet to have two VLAN tags, one tag as his own VLAN (also the native VLAN) and the other tag is of the victim VLAN. When this packet reaches the switch, the switch can only see the tag on the outside, which belongs to the attacker, which it then removes. After this it is forwarded to the other ports belonging to native VLAN and will go across the trunk port. When it reaches the other switch, the second tag will be seen and the packet will be forwarded to the victim VLAN 20. If given the right circumstances, then this attack is pretty straight forward. As seen in the screenshot below, the attacker cannot reach the victim in VLAN 20.

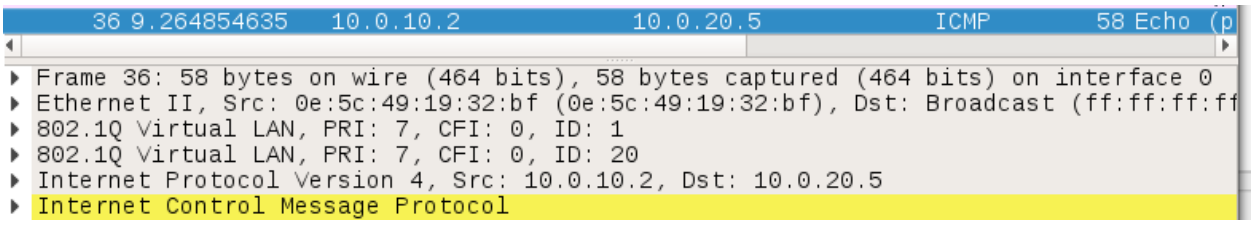
```
root@menmuir:~# ping 10.0.20.5
PING 10.0.20.5 (10.0.20.5) 56(84) bytes of data.
^C
--- 10.0.20.5 ping statistics ---
30 packets transmitted, 0 received, 100% packet loss, time 29691ms
```

First, the attacker will load up Yersinia, like in the previous attack. Then they will click on the “802.1Q” menu at the top and go into edit mode. After that, the attacker will fill in information in the text boxes at the bottom. They will put their own VLAN ID in the first VLAN box, and their own IP address in the “Src IP” box. The attacker will also put the victims VLAN in the VLAN2 box, and the victims IP in the “Dst IP” box. All these input boxes will be highlighted below.




After this the attacker will exit edit mode and click on the Launch attack button, at the top left-hand side. They will be presented with a menu and they are to click “Double tagging” and then okay.

The attacker has now launched an attack. They can now send and listen to traffic on the VLAN they were not previously allowed to access.



## *2.2.2* VLAN Hopping Mitigation

Avoiding a Double tagging attack is simple, all that is needed to be done is to change the native VLAN on all trunk ports to a VLAN that does not have any hosts assigned on it.

```
s1(config)#vlan 99
s1(config-vlan)#int gi0/0
*Nov  3 16:46:11.600: %IP-4-DUPADDR: Duplicate address 10.0.10.2 on Vlan1, sourced by 0056.d0e5.8000
s1(config-if)#no switchport trunk native vlan 1
s1(config-if)#switchport trunk native vlan 99
s1(config-if)#exit
s1(config)#exit
s1#
```

To prevent a switch spoofing attack, make sure that all ports that are not meant to be trunks are set to access mode. Access mode is a mode set on a port that can only have one VLAN configured on it. The dynamic trunking protocol should also be disabled. This means that ports will not automatically negotiate trunking. The key to preventing a switch spoofing attack is to not leave any of the access ports in “Dynamic auto”, “Dynamic desirable”, or “trunk” mode.

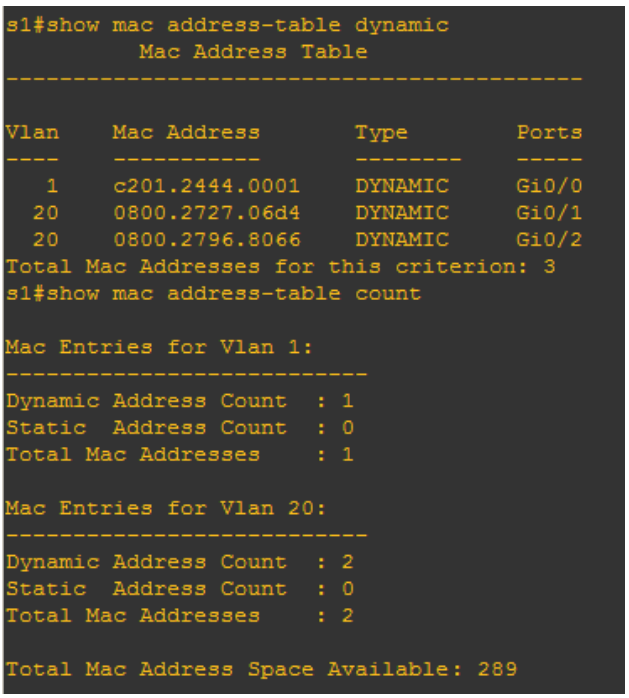
```
s1(config)#int gi0/1
s1(config-if)#switchport mode access
s1(config-if)#switchport nonegotiate
s1(config-if)#exit
s1(config)#exit
```

To make a network extra secure against these attacks, DTP could also be disabled on trunk ports.

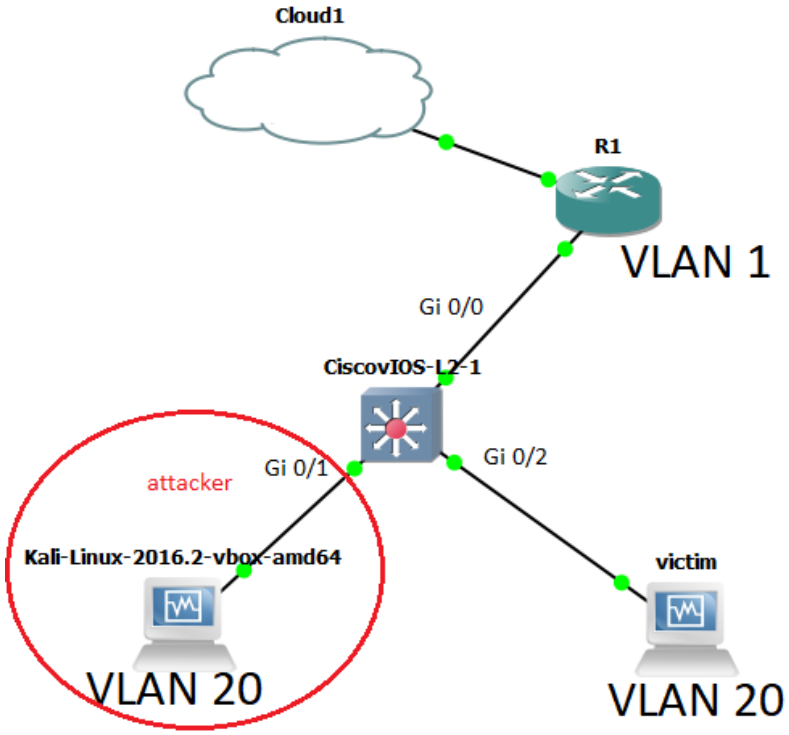
```
s1(config)#int gi0/3
s1(config-if)#switchport trunk encapsulation dot1q
s1(config-if)#switchport mode trunk
s1(config-if)#switchport nonegotiate
s1(config-if)#exit
s1(config)#
```

## *2.3.1* MAC address spoofing

Every MAC address of all the devices connected to the switch can be viewed, using the command “show mac address-table dynamic” in the privileged execution mode. As we can see, there are only 3 MAC addresses held in the table, and we can also see the ports that these addresses are from. To see how many remaining MAC address spaces are left, simply type “show mac address-table count” into the terminal.



This is what the network looks like.




For the attack the hacker will be using a tool called ‘macof’ which specialises in flooding switches with mac addresses. In the command the attacker types ‘macof’ then specifies the network they are on (ethernet 0) by typing ‘i [network]’ as well as the destination typing ‘-d [destination IP]’, which is the IP address of the switch they will be flooding. After that has been typed in, the flooding will begin, and the attacker will start sending spoofed MAC addresses.

```
root@menmuir:~# macof -i eth0 -d 10.0.20.1
```

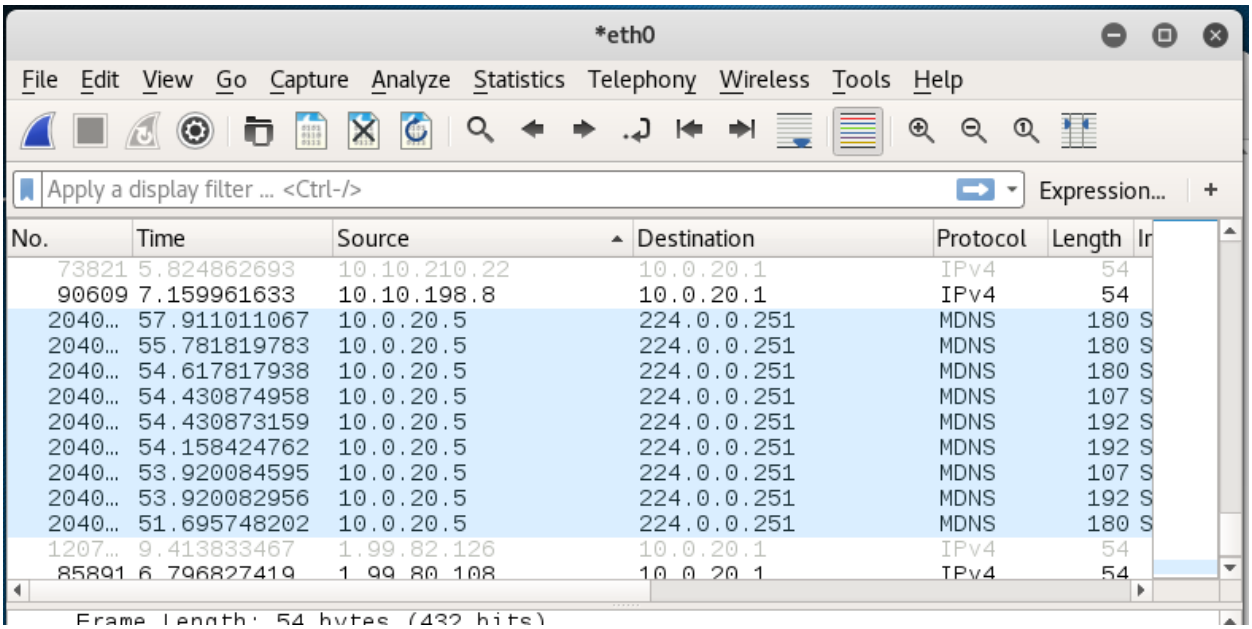
```
root@menmuir: ~
File  Edit  View  Search  Terminal  Help
29:81:ad:77:c4:67 51:70:b2:41:f6:2f 0.0.0.0.5399 > 10.0.20.1.42796: S 909256583:
909256583(0) win 512
da:9e:5c:64:5:5b e6:cb:6:12:f1:69 0.0.0.0.61912 > 10.0.20.1.64777: S 1192959358:
1192959358(0) win 512
68:26:f3:57:fe:49 51:72:65:50:22:4b 0.0.0.0.39726 > 10.0.20.1.55254: S 193814190
8:1938141908(0) win 512
c5:e7:6f:48:7f:c1 13:fe:41:69:d3:b7 0.0.0.0.53017 > 10.0.20.1.27095: S 209603311
7:2096033117(0) win 512
35:e1:b8:1d:78:91 16:40:b:1f:fb:fb 0.0.0.0.47654 > 10.0.20.1.23016: S 125761314:
125761314(0) win 512
5d:9:64:42:aa:fb 1c:85:32:35:2d:ad 0.0.0.0.33868 > 10.0.20.1.61412: S 556377086:
556377086(0) win 512
95:2b:7e:5f:ff:9c e:ff:e9:53:dd:f3 0.0.0.0.5240 > 10.0.20.1.56114: S 1250146948:
1250146948(0) win 512
12:27:3a:3:de:ee 6c:e1:ad:57:b4:ab 0.0.0.0.19091 > 10.0.20.1.35542: S 794180211:
794180211(0) win 512
de:ca:1e:7a:b1:c3 de:16:6:47:b2:9a 0.0.0.0.55694 > 10.0.20.1.54528: S 1152317425
:1152317425(0) win 512
93:38:ba:20:85:2c b6:ef:5:29:eb:85 0.0.0.0.13755 > 10.0.20.1.55523: S 1813102436
:1813102436(0) win 512
d5:3c:86:30:a8:86 7c:e5:7b:22:29:3c 0.0.0.0.63191 > 10.0.20.1.30019: S 190886166
7:1908861667(0) win 512
77:43:5f:7c:80:e7 d2:a8:9c:25:19:9f 0.0.0.0.37408 > 10.0.20.1.31997: S 159766322
2:1597663222(0) win 512
```

The MAC address table is now full as there is no more space available for addresses. Checking the table also allows us to determine where the attack is coming from. The attacker is from port Gi0/1 and is on VLAN 20.

```
Mac Entries for Vlan 1:
---------------------------
Dynamic Address Count   : 1
Static  Address Count   : 0
Total Mac Addresses     : 1

Mac Entries for Vlan 20:
---------------------------
Dynamic Address Count   : 291
Static  Address Count   : 0
Total Mac Addresses     : 291

Total Mac Address Space Available: 0
```

```
s1#show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    c201.2444.0001    DYNAMIC     Gi0/0
  20    0058.ea7e.674c    DYNAMIC     Gi0/1
  20    00d7.bd32.7b40    DYNAMIC     Gi0/1
  20    00f9.885c.4987    DYNAMIC     Gi0/1
  20    01dc.2d6c.7575    DYNAMIC     Gi0/1
  20    01e5.8949.0a6b    DYNAMIC     Gi0/1
  20    0208.a529.1e38    DYNAMIC     Gi0/1
  20    0361.f55a.93cb    DYNAMIC     Gi0/1
  20    0487.2609.7905    DYNAMIC     Gi0/1
  20    04c6.cb1f.d485    DYNAMIC     Gi0/1
  20    051a.4614.420e    DYNAMIC     Gi0/1
  20    05b7.f140.ecd8    DYNAMIC     Gi0/1
  20    05e1.6c71.a01d    DYNAMIC     Gi0/1
  20    0602.9b3f.3f29    DYNAMIC     Gi0/1
  20    0645.2422.9b9f    DYNAMIC     Gi0/1
  20    07ed.9625.2ebc    DYNAMIC     Gi0/1
```

The attacker can now view packets on the same VLAN as the switch has entered into a fail-open mode. This means that it is acting like a hub and is broadcasting messages to all network interfaces. If we use a program like wireshark, we can capture these packets and look through them for useful information.




## *2.3.2* MAC Address Spoofing Mitigation

A MAC address attack can be mitigated using switchport security and also secure MAC addresses. When secure MAC addresses are assigned to a port, that port will not forward packets with MAC addresses outside of the group of defined secure addresses. There are three ways in which secure MAC addresses can be learned. They can be typed in manually on the switch in what's known as static secure mac addresses. These are mainly configured when the mac addresses used are known and don't change often. To configure a static mac address, enter the interface and type in "switchport port-security mac-address [desired MAC address]".

The port can also be allowed to configure secure mac addresses dynamically with the MAC addresses of already connected devices. Dynamic secure MAC addresses are normally used when the connected hosts change often, so that the port is to be used by a specific number of hosts at a time. Lastly, the port can be configured with sticky secure MAC addresses. This is a bit of a hybrid of the two as they can be statically configured, and dynamically learned. The way to set up sticky learning on a device is to enter the switches interface and type "switchport port-security mac-address sticky".

The other way to secure a network against a MAC address attack is to set a security violation mode. This feature of switchport security will take action depending on what mode we set it in. We will set it in restrict mode, which means that when a violation occurs we will be notified of it and the traffic from unknown mac addresses will be dropped. A violation happens when the set number of maximum secure MAC addresses has been exceeded or when an address on one secure interface is seen in another interface. This is how security violation mode can be set up.

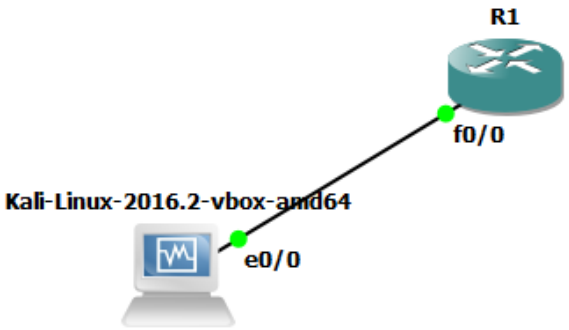
```
s1(config)#int range gigabitEthernet 0/1-2
s1(config-if-range)#switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled

s1(config-if-range)#switchport port-security violation restrict
s1(config-if-range)#switchport port-security maximum 10
s1(config-if-range)#switchport port-security
s1(config-if-range)#end
s1#
```

We have set our maximum secure MAC addresses to 10. Now if we perform our attack again, the results can be seen below. We will only receive the maximum number of secure MAC addresses from the same interface before traffic is dropped

```
s1#show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    c201.2444.0001    DYNAMIC     Gi0/0
  20    275b.5833.0455    DYNAMIC     Gi0/1
  20    7904.3547.b7c1    DYNAMIC     Gi0/1
  20    7b80.2735.a0ac    DYNAMIC     Gi0/1
  20    815d.fd0b.7a44    DYNAMIC     Gi0/1
  20    9173.d11c.c848    DYNAMIC     Gi0/1
  20    b177.aa29.ec89    DYNAMIC     Gi0/1
  20    b733.9415.7bde    DYNAMIC     Gi0/1
  20    dd19.e074.43f7    DYNAMIC     Gi0/1
  20    f398.5240.3199    DYNAMIC     Gi0/1
  20    f911.bb74.86a0    DYNAMIC     Gi0/1
Total Mac Addresses for this criterion: 11
```

## *2.4.1* CDP flooding attack

CDP (Cisco Discovery Protocol) packets are enabled by default on Cisco devices, and they are not encrypted, so an attacker can gain valuable information about the device from reading the packets. This is reason enough for most people to want to disable CDP throughout their network, however there is a worse way in which CDP can be abused which is known as CDP flooding. A CDP flooding attack is a type of DoS (Denial of service) attack as it can freeze the operating system on a switch or router, blocking anyone from managing it, as well as locking the CPU which will cause the switch to start dropping traffic on the network. The device crashed because there was a vulnerability in Cisco devices that Improper memory allocation for the CDP process, meaning it would run out of memory. This attack can also be used to sniff data throughout the network because when a switch is overwhelmed it will start forwarding packets to all of its ports, as seen on the MAC address spoofing attack. The hacker can perform this DoS attack by flooding the switch with thousands of spoofed CDP messages. A simple network will be used to demonstrate this, the router being used like a switch.



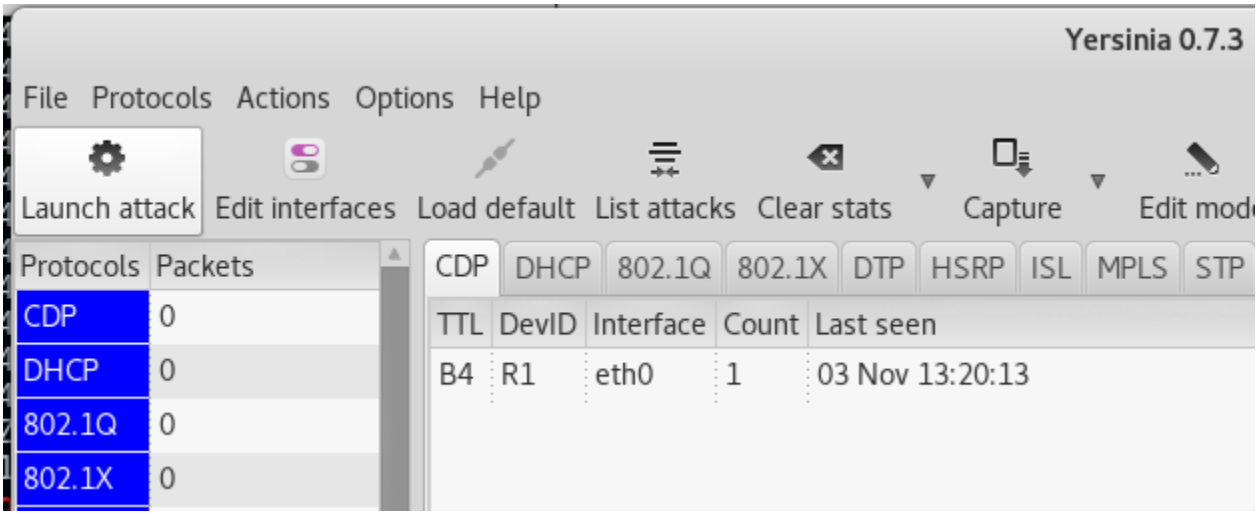
To see neighbouring devices, simply go into the router or switch and type “show cdp neighbours” in privileged execution mode. As seen below there are currently no CDP neighbours.

```
R1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
R1#
```

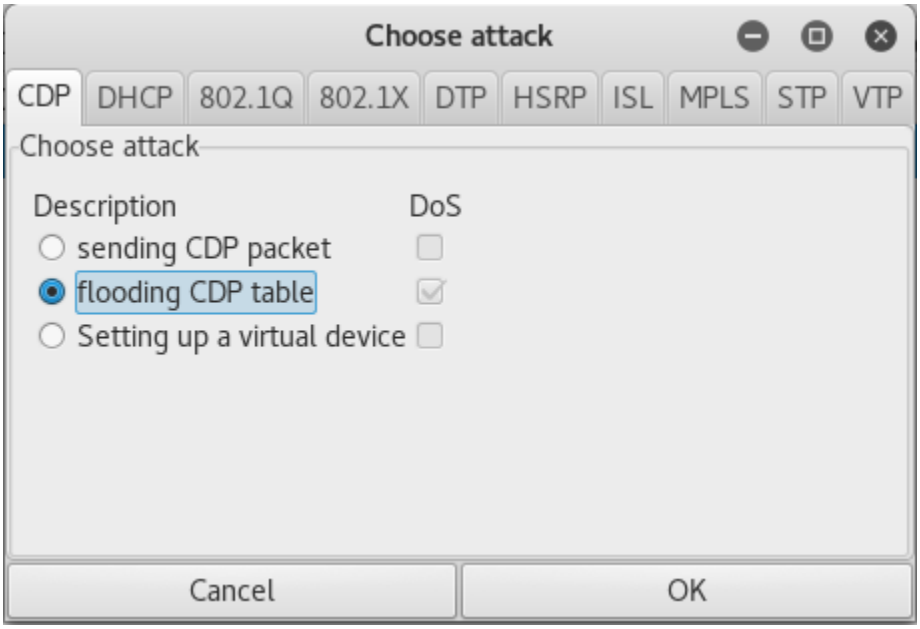
To test that the device is up and reachable from the hacker’s machine, they can ping it.

```
root@menmuir:~# ping 10.0.10.1
PING 10.0.10.1 (10.0.10.1) 56(84) bytes of data.
64 bytes from 10.0.10.1: icmp_seq=1 ttl=255 time=40.0 ms
64 bytes from 10.0.10.1: icmp_seq=2 ttl=255 time=2.98 ms
64 bytes from 10.0.10.1: icmp_seq=3 ttl=255 time=5.45 ms
```

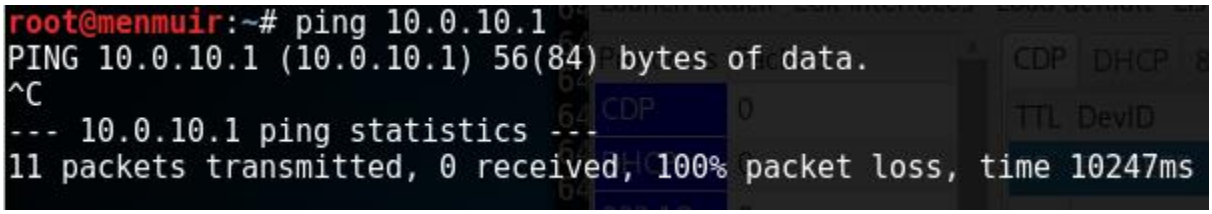
When the attacker is ready to perform the attack, they will load up Yersinia using “Yersinia -G” like in the previous VLAN hopping attacks. When the Yersinia menu loads up, they will select the CDP menu at the top, then click the “Launch attack” button in the top left corner.



Then they must select the “Flooding CDP table” option and click on okay to confirm their attack.

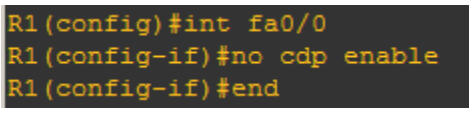



Now that the CDP table of the router is flooded with spoofed CDP messages, we can’t enter the router to check the CDP table as it has crashed and it will not load up. Also, when the attacker tries to ping the router again, it is unreachable, meaning that it has completely dropped traffic.




## *2.4.2* CDP Flooding Attack Mitigation

CDP may be useful for network managers, but at a potentially significant cost if it is not set up securely. The easiest way to prevent a CDP attack is to disable it on the entire switch.




If the network manager finds CDP useful and would rather use it on the network, then individual ports can just be disabled on devices that do not need it instead using the “no CDP enable” command on the interface. Not much more can be done to prevent CDP attacks other than being very selective about its use in a security sensitive environment.

# 3 Discussion

## *3.1* Overview

As shown through the procedures, it is really simple for a malicious person to exploit a networks' switches through the data-link layer. All the tools used to exploit the network are free and could be possessed by anyone, so it should be made abundantly clear that it is a very wise idea to configure a network with the security procedures demonstrated in this document. It takes very little time to configure a network with these security features, as they are just a few simple commands for the most part, so it will be worthwhile implementing them into any future networks managed. It must be noted that this paper only investigated a selection of the most common switch attacks. Following these tutorials will not lead to complete switch security, although network security will be improved to a great extent.

## *3.2* Findings

ARP spoofing can be a particularly damaging attack as the attacker can harm the victim in several ways. If they wanted to, they could listen to a person's traffic and act as a 'man in the middle', they could manipulate the data, or even disconnect the victim from the server entirely. The attack is easily avoided and mitigated using two security features. Dynamic ARP inspection and DHCP snooping work together to prevent attacks, such as ARP spoofing. DAI ensures that only valid ARP requests and responses are relayed. It does this by intercepting all ARP requests on ports that are configured as 'untrusted' and verifies that each of these intercepted packets has a valid IP-to-MAC address binding in the DHCP snooping table. Since the attackers' port had been set to untrusted, the ARP response sent to the switch in which they try to spoof their own MAC address with the victims IP address and vice versa, will now be dropped. This means that the attack will no longer work on the network. DHCP snooping should also be configured on the network as the DHCP snooping table is used by DAI. It also performs a range of activities that essentially make it a firewall between untrusted hosts and trusted DHCP servers, which will aid in switch security. These security features are easy to set up as demonstrated in the procedures, and will make the data-link layer of a network invulnerable to any ARP spoofing attacks if configured correctly.

The VLAN hoping attacks can come in two variations, and both can be detrimental to a person's network. The switch spoofing attack can allow a malicious user to view traffic on all VLANS throughout the network and view private data on a network. The double tagging attack is more specified, and allows an attacker to view traffic on a specified VLAN. The double tagging attack is very easily avoided, to prevent it the trunks native VLAN should not be left as the default number. Changing it to a number that is not used on any of the ports will make a network secure from double tagging attacks. To secure a network from a switch spoofing attack, the first thing a user would do, would be to make sure that all switchports that are not meant to be trunks are set into access mode. The second thing a user should do is turn of DTP (Dynamic Trunk Protocol) as this will make the ports non-negotiable and ports will not

negotiate trunking. Now when an attacker tries to perform a switch spoofing attack, it will not work as their switchport will not negotiate trunking.

The MAC address flooding attack is another harmful attack. It can allow the attacker to see all of the traffic going through a switch because it will be broadcasting packets to all the connected interfaces as its MAC address table is full. Using secure MAC address types will be beneficial in keeping a secure network. It is down to the preference of the user, although the size of the network will determine which choice of secure MAC address is more suitable for a network. A Static secure MAC address is suitable for a smaller network as it means there is no MAC addresses allowed on the network other than the ones configured by the network manager. Although a dynamic or sticky secure MAC address type is the preferred choice for slightly larger networks. This attack is also easily avoided using the port security feature available on most switches. Once this feature is enabled on a switch, it allows the user to configure it in a way that's optimal for their network. One of the configurations of this feature is the maximum number of secure MAC addresses received on a single port. This works as setting it to a relatively low number, in our case 10, prevents the switches MAC address table from being flooded by a single port. In the procedures, the violation mode configuration was also set to restrict, which is a sensible mode to have as it will not only drop traffic from the offending MAC addresses, but will also notify the network manager. With this feature activated, it is seen that in the procedures, when an attacker tries to perform a MAC address attack again, only the configured maximum number of MAC addresses will be stored in the switches MAC address table.

The last attack covered in this report was the CDP attack. This attack can be very damaging for a network as the attacker will use it to overload the switches memory and cause it to freeze, denying service to all the hosts supported by that switch. CDP can be seen as a useful feature for most networks, although if it is not needed, the best practice for preventing a CDP attack is to just disable it throughout the network. If a network manager is wanting to use the CDP feature then it should only be active on ports that the network manager trusts. With CDP deactivated on a port, simply will not be able to send any CDP packets to a switch, so the network is secure against the attack.

## *3.3* Future work

Layer 2 security could be investigated further, as there are more attacks than the ones mentioned in this paper. Future research could be put into other attack mitigations, such as for the spanning tree protocol attack, an attack in which a user impersonates the root bridge of a network allowing all traffic to pass through them. Another attack, known as the DHCP starvation attack, works by flooding a DHCP server with broadcasts of DHCP requests from spoofed MAC addresses. After enough spoofed addresses are sent the attacker can exhaust the available IP addresses in the DHCP server scope. Once the server can no longer respond to the hosts requests, then the attacker takes the servers place and becomes a rogue DHCP server and can capture sensitive user data on the network – similar to the 'man in the middle' attack performed in the ARP spoofing demonstration. Attacks such as these can have consequences as severe as the ones covered in this investigation and should be investigated more in future. Investigating more switch attacks, such as these, could potentially guarantee complete security of the data-link layer.

# 4 Conclusions

To conclude this investigation, Layer 2 security is easy to exploit and security should be implemented to keep data safe. This paper gave a brief summary of the different features that are common on networks and how these useful features could be vulnerable to attacks. Having a secure network is important as it is shown that there are many ways to attack a networks data-link layer, and this paper illustrates how easy it is to perform these attacks through the detailed demonstrations. All these attacks can be done with free and legal software that is accessible for anyone, which is a scary thought. Mitigating these attacks is very uncomplicated and was done using security features built into most devices, sensible port configuration, as well as sensible VLAN configuration. Through these mitigation tutorial, a secure network is easily achieved in which these common attacks will not be a threat.

# 5 References


King, J. and Lauerman, K. (updated 2016) '*ARP Poisoning (MAN-in-the-Middle) Attack and Mitigation Techniques*' [online] Accessible From: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/white_paper_c11_603839.html (Accessed 21 October 2017)

Cisco Product support (updated 2013) '*Catalyst 6500 Release 12.2SX Software Configuration Guide - DHCP Snooping [Cisco Catalyst 6500 Series Switches]*' [online] Accessible From: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoodhcp.html (Accessed 21 October 2017)

Cisco Networking Academy (2014) '*Cisco Networking Academy's Introduction to VLANs*' [online] Accessible From: http://www.ciscopress.com/articles/article.asp?p=2181837&seqNum=10 (Accessed 23 October 2017)

Nanayakkara, R. (2014) '*Double Tagging Attack (VLAN Hopping Attack)*' [online] Accessible From: https://cisconetworkengineer.wordpress.com/2014/02/03/double-tagging-attack-vlan-hopping-attack/ (Accessed 23 October 2017)

'*What is Switch spoofing attack and how to prevent Switch spoofing attack*' [online] Accessible From: http://www.omnisecu.com/ccna-security/what-is-switch-spoofing-attack-how-to-prevent-switch-spoofing-attack.php (Accessed 23 October 2017 )

Sankar, R. (2015) '*Yersinia*' [online] Accessible From: http://kalilinuxtutorials.com/yersinia/ (Accessed 24 October 2017)

Wilkins, S. (2011) '*Switchport Security Concepts and Configurations*' [online] Accessible From: http://www.ciscopress.com/articles/article.asp?p=1722561 (Accessed 25 October 2017)

Cisco Product Support [online] '*Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(20)EWA - Configuring Port Security [Cisco Catalyst 4500 Series Switches]*' Accessible From: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/20ewa/configuration/guide/conf/port_sec.html (Accessed 25 October 2017)

Sankar, R. (2015) '*macof*' [online] Accessible From: http://kalilinuxtutorials.com/macof/ (Accessed 25 October 2017)

Popeskic, V. '*CDP Attacks – Cisco Discovery Protocol Attack*' [online] Accessible From: https://howdoesinternetwork.com/2011/cdp-attack (Accessed 26 October 2017)

Popeskic, V. '*How to configure CDP – Cisco Discovery Protocol*' [online] Accessible From: https://howdoesinternetwork.com/2012/configure-cdp/ (Accessed 26 October 2017)

Cisco Product support '*Cisco Discovery Protocol Configuration Guide, Cisco IOS Release 15M&T*' [online] Accessible From: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cdp/configuration/15-mt/cdp-15-mt-book/nm-cdp-discover.html (Accessed 26 October 2017)