DATA LINK LAYER SECURITY PROBLEMS AND SOLUTIONS

Nasir Siddique, Mustafa Ali, Mubeen Zubair

Computer Network Engineering, 15 credits

Halmstad 2015-01-20
“Acknowledgements”

First of all we would like to present our hearty gratitude to ALLAH ALMIGHTY, who always blesses us and makes our path easy during the journey of our lives. We are also very thankful to Professor Tony Larsson and Malin Bornhager and Pererik Andreasson, who patiently helped us to complete this work smoothly. Indeed, their efforts and talent make it really easy to overcome the hurdles without any problem. Thank you for guiding us.

Also, thanks to our parents and their prayers, who always take our work into their consideration and remembered us during their supplication.

Finally, we would thank to everyone for their nice support and feedback.
Abstract
The Open Systems Interconnect Model (OSI) is a conceptual model of networking that categorizes network functions into seven layers. It is defined in this model that how layers communicate with each other. In this thesis, we address common Layer 2 attacks and their solutions. Layer 2 is considered a very weak link in a secure network. If the data is compromised at Layer 2, it cannot be detected at other layers because each layer works without the knowledge of other layers. We discuss Layer 2 weakness and vulnerability exploitation tools briefly. It is explained how an attacker can exploit network by using different attack tools. Our results show that these attacks are very productive if a network administrator does not implement proper security at Layer 2 in the OSI model. We propose solutions to secure Layer 2 devices and these solutions are implemented by using attack tools. Security configurations are deployed to combat against attacks and protect the integrity, confidentiality, and availability of the network traffic.
Contents

Abstract ........................................................................................................................................... 4

1 Introduction ..................................................................................................................................... 9
   1.1 Problem statement ..................................................................................................................... 9
   1.2 Goal of the Thesis .................................................................................................................... 10

2 Technical Background ..................................................................................................................... 12
   2.1 Open System Interconnection (OSI) ....................................................................................... 12
   2.2 Basic security areas .................................................................................................................. 13
       2.2.1 Confidentiality .................................................................................................................. 13
       2.2.2 Integrity ............................................................................................................................. 13
       2.2.3 Availability ....................................................................................................................... 13
   2.3 Layer 2 security concerns ........................................................................................................ 14
       2.3.1 Address Resolution Protocol (ARP) Poisoning ................................................................. 14
       2.3.2 Cisco Discovery Protocol (CDP) ..................................................................................... 16
       2.3.3 DHCP Starvation .............................................................................................................. 17
       2.3.4 VLAN spoofing .................................................................................................................. 17
       2.3.5 Content Address Memory (CAM) Table Overflow .......................................................... 17
       2.3.6 Spanning Tree Protocol (STP) Manipulation ..................................................................... 17

3 Experiments .................................................................................................................................... 19
   3.1 Case study 1: ARP Poisoning ................................................................................................. 19
   3.2 Case study 2: CDP Attack ....................................................................................................... 22
   3.3 Case study 3: DHCP Starvation .............................................................................................. 24
   3.4 Case study 4: VLAN Spoofing ............................................................................................... 25
   3.5 Case study 5: Cam Table Overflow ....................................................................................... 26
   3.6 Case study 6: STP Manipulation ............................................................................................. 28

4 Results .......................................................................................................................................... 31
   4.1 ARP Poisoning .......................................................................................................................... 31
   4.2 CDP Attack ............................................................................................................................ 32
   4.3 DHCP Starvation ..................................................................................................................... 32
   4.4 VLAN spoofing ....................................................................................................................... 32
   4.5 CAM Table Overflow ............................................................................................................. 33
   4.6 STP Manipulation ..................................................................................................................... 34

5 Conclusion ...................................................................................................................................... 36

6 Abbreviation ................................................................................................................................... 38
References ................................................................. 40
Appendix ............................................................................ 44
1 Introduction

Information security plays an important role in an organization. The Open Systems Interconnect Model (OSI) is a conceptual model of networking that categorize network functions into seven layers called physical layer, data link layer, network layer, transport layer, session layer, presentation layer and application layer. It is defined in this model how layers communicate with each other. Usually a network administrator does not concentrate on data link layer (layer 2 of OSI) security devices because it is very difficult for external hackers to connect to an organization’s LAN [1]. Packet filtering, access list, Intrusion Detection Systems (IDS), encryption techniques and firewall can be implemented to secure Layer 3 and upper layers. On the other hand, the data link layer lacks the fine-grain controls to stop data link layer attacks from occurring [2]. In most cases a network administrator gives very little attention to Layer 2 security and often this area is left untouched. Layer 2 attacks can result in damage to the network [3]. For example Cdp attack can cause run out of memory and a device can loss its functionality. The network administrator gives very little attention to secure Layer 2 devices, and due to this reason, it is very easy for attacks to be carried out on the network. The normal way an attacker uses to get from outside the network to do an attack on the network is a social engineering attack. Social engineering is the use of fraud and tricks to obtain confidential information. It is a non-technical type of intrusion that relies mainly on human interaction and usually comprises tricking other people to break normal security procedures. According to FBI/CSI computer crime and security survey in 2006, total losses caused by insider abuse of net access was 1,849,810 dollars. The survey showed that 32 percent of respondents think that their organizations have never had cyber losses by insiders. Another 39 percent of respondents said that greater than 20 percent of an organization’s cyber losses are caused by insiders. Seven percent of respondents believe that more than 80 percent of an organization’s cyber losses are caused by insiders. A significant number of respondents think that insiders account for a considerable portion of the losses [4].

Layer 2 security has an important role in the network, because we transfer data in the network through Layer 2. If the data is compromised at Layer 2, then it is useless to implement high-level security in the upper layers. All layers of the OSI model work without the knowledge of each other [5].

If an attacker performs a successful security attack, then all sensitive information can be stolen from the network using different techniques. An attacker can use different attacking tools to perform Layer 2 attacks. These attacks can cause loss of integrity, data confidentiality, and availability. A network administrator should monitor the network to identify security holes. The most-common attacks on LAN network for example CAM table overflow, VLAN hopping, Spanning Tree Protocol (STP) manipulation, ARP cache poisoning, DHCP Starvation, Cisco Discovery Protocol (CDP) attacks.

1.1 Problem statement

The weakest connection in a secure network is considered Layer 2. Most of Layer 2 protocols are insecure because they do not provide a secure binding between the Internet Protocol (IP) and MAC Addresses [6]. When a network is developed, a network administrator concentrates more
on Layer 3 devices security such as routers as compared to Layer 2 devices such as switches because Layer 3 bridges different subnets to support end-to-end internet connectivity between nodes. Usually networks are connected to the Internet and external users also need to access the network. Most of the Layer 3 protocols like Internet Protocol (IP) have no built-in mechanism to cope with malicious hosts. Therefore Layer 3 devices are suspected to different types of attacks like session hijacking, Denial-of-Service (DoS) and IP Address Spoofing etc. It is very difficult for external hackers to connect to an organization’s LAN. An attacker needs a physical connection to exploit Layer 2 vulnerabilities. Social engineering can be used to gain access to the building or he/she can pretend to be an engineer requested on site to fix a technical problem [1]. In addition a user can also plug in an unauthorized switch which could permit other devices to connect to the network.

1.2 Goal of the Thesis
The main goal of this thesis is to test Layer 2 security attacks such as the ARP poisoning, DHCP starvation, VLAN spoofing, CDP, CAM table overflow and STP Manipulation. In addition, to understand how these attacks work and possible methods and techniques to mitigate them. Moreover, we will use different attacking tools to exploit layer 2 security and then we will implement the possible solutions to secure layer 2 devices.
2    Technical Background

2.1 Open System Interconnection (OSI)
The OSI layer model has seven layers and starts with the physical layer. The physical layer, layer one, is responsible for raw bits transmission over communication channels and it confirms that the sent and received bit number is not changed or missing [7]. Also, it is responsible for physical hardware connectivity [8].

The data link layer, layer two, provides a reliable communication across the physical layer to other locations like LAN or Wide Area Network (WAN), and deals with physical addressing like media access control (MAC) and logical link control [8]. The data link layer can help with error detection and errors in flow determination [8].

The network layer, layer three, deals with logical addresses and how data is routed from start to end [7]. Transit time and packet delays are also issues of the network layer. All the packets are assigned addresses. Assigned addresses help to send packets from one destination to another destination point [8].

The transport layer, layer four, works with data transport. First the transport layer accepts the data, and then it divides it into smaller parts. After updating the data, the data is sent to the network layer with confirmation that all data parts are correctly connected [7, 8]. The transport layer carries data from the source to the destination, and it deals with end to end connections, delivery of data, and reliability [8].

The session layer, layer five, communicates with applications and end users on different machines to establish connections [9, 8]. Generally, it is responsible for closing, opening, and managing sessions.

The presentation layer, layer six, is the operating system part. It changes incoming and outgoing data information to another format. Layer six handles transmitted information syntax and semantics [9, 8, 10]. A communication between computers with different internal data representations is possible when the data structures are exchanged and characterized by encoding and data formatting [7]. The application layer contains electronic mail protocols, FTP, and HTTP [10]. It determines how a user’s application should use the network and communicate with network services that interact with the user [10].

The application layer, layer seven, actually interacts with the operating system or applications. It is responsible for the data format and data display at the end user side. The application layer is also closely interacting with the presentation layer.
Table 1: OSI layer responsibilities

<table>
<thead>
<tr>
<th>Layer</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 (Application)</td>
<td>Message format at the human machine interface and the data display.</td>
</tr>
<tr>
<td>6 (Presentation)</td>
<td>Data encryption, data compression, data conversion.</td>
</tr>
<tr>
<td>5 (Session)</td>
<td>Session establishment, maintenance and management of a session.</td>
</tr>
<tr>
<td>4 (Transport)</td>
<td>Message traffic control, data acceptance, session multiplexing, message</td>
</tr>
<tr>
<td></td>
<td>segmentation, message acknowledgement.</td>
</tr>
<tr>
<td>3 (Network)</td>
<td>Routing, subnet traffic control, Logical-physical address mapping,</td>
</tr>
<tr>
<td></td>
<td>Frame fragmentation.</td>
</tr>
<tr>
<td>2 (Data Link)</td>
<td>Establish and terminates the logical between nodes, frame</td>
</tr>
<tr>
<td></td>
<td>acknowledgment, frame error checking, flow control.</td>
</tr>
<tr>
<td>1 (Physical)</td>
<td>Physical medium transmission bits over communication channels, data encoding,</td>
</tr>
<tr>
<td></td>
<td>physical hardware connectivity.</td>
</tr>
</tbody>
</table>

2.2 Basic security areas

There are three basic security areas, confidentiality, integrity, and availability. These are the basic pillars of the security and without these three concepts a secure network cannot be developed.

2.2.1 Confidentiality

The area of confidentiality focus on that information will be shared among the right persons. Implementation of this security mechanism guarantees that data and other valuable sources would not be exploited by an unauthorized person. It is crucial to protect information during transmission and processing to maintain the confidentiality. Strong encryption should be implemented to enforce confidentiality.

Security can be exploited with the help of scanning tools like Wireshark. Confidentiality can also be exploited due to human errors like missing configuration during implementation of the security measures or execution of malicious programs [11].

2.2.2 Integrity

Integrity assures the protection of information from changing, deleting, and adding from unauthorized persons. The information is printed as received (preserving data integrity), but its source is incorrect (corrupting origin integrity) [11]. It is important to restrict access to critical resources to maintain the integrity. Integrity consists of two mechanisms called prevention mechanisms and detection mechanisms.Detection mechanisms protect information from being modified or deleted by unauthorized persons. Detection mechanisms do not prevent the information from being violated by unauthorized persons. Detection mechanisms report to administrator if integrity is disturbed. Detection mechanisms monitor the activities to find problems in the network. They can also point out the specific area where integrity was violated within the network.

2.2.3 Availability

Availability means that the system delivers required data to the users when needed. Authorized persons should have access to authorized sources without any interruption. Availability can be
compromised by interruption attacks, such as Denial of Service (DoS) attacks. Availability ensures access to required information without any interruption.

Backup and redundancy should be provided if any interruption happens. Access channels should work properly to fetch required information. The security policy should be strong enough to maintain availability [11].

2.3 Layer 2 security concerns

2.3.1 Address Resolution Protocol (ARP) Poisoning
ARP was published in 1984 and is still in use [12]. This protocol works at Layer 2 but provide services to Layer 3. In a layer two switched network the communication is carried out on the basis of MAC addresses. ARP cache is used to map network addresses (IP) to corresponding physical addresses such as an Ethernet address [13, 14]. ARP is a stateless protocol. It cannot deal with malicious hosts due to lack of authentication. If host A wants to communicate with host B in the same Local Area Network (LAN), host A must know the MAC address of host B to corresponding to the network address (IP). Host A will lookup MAC address of host B in the ARP cache table. If the host B MAC address is not available in the ARP cache table, it will broadcast ARP Request to in the Area Network (LAN) with source’s IP, source’s MAC address and destination’s IP address. This request for the host B MAC address is illustrated below in the figure 2.3.1 [15].
As shown in the figure 2.3.2, only the host B will send back an ARP reply to host A with the IP address and MAC address. The rest of the hosts will ignore the request. Host A will store the MAC address of host B in its ARP cache table to reduce the amount of transactions. Host A will communicate with host B on the basis of the stored MAC address.
Due to lack of authentication, malicious hosts can poison the ARP cache by sending forged ARP request or reply. The developer of the ARP protocol did not define any authentication mechanism. Due to this reason, the ARP protocol also accepts fake request or reply and all these fake requests or replies will be stored in the cache table. A forged request or reply can also be used to redirect traffic to other hosts. In a LAN network, Man in Middle (MITM) and Denial of Services (DoS) attacks can be performed by poisoning the ARP cache of the victim host [16].

An attacker can poison the ARP cache to manipulate network traffic between two devices [17]. The attacker can spoof the IP addresses of two hosts and send all information in both directions by sitting between these two hosts. Victims do not know that their traffic is being intercepted by someone. It is called Man in the Middle Attack (MITM).

Denial of Service attack can also be performed by poisoning the ARP cache. The victim is poisoned by forging MAC addresses and sending all the traffic to the intruder host. The attacker disables the victim’s access to the internet [17].

2.3.2 Cisco Discovery Protocol (CDP)
CDP is used to get information from neighboring devices. Due to lack of authentication, an attacker can perform a CDP attack. The following information can be obtained if an attack is performed successfully.

- Internet Protocol
- Software Version
- Platform
- Capabilities
- Native VLAN

An attacker can also overflow CDP cache by using attack tools. CDP table can be overflowed due to lots of false information in the table.
2.3.3 DHCP Starvation
In LANs network, the Dynamic Host Configuration Protocol (DHCP) is used to dynamically or statically assign IP addresses to a computer for a fixed-time period. To acquire configuration information from a DHCP server, a DHCP client first sends a broadcast message with a DHCPDISCOVER packet in the local network. The DHCP server replies with a DHCPOFFER message if it has available IP addresses. The DHCP client accepts the offer and broadcast a DHCPREQUEST to the DHCP server. The DHCP server replies with a DHCPACK message after receiving this request. When the DHCP client receives the DHCPACK message, it checks whether the IP address is in use by sending an ARP message in local network. If an address is available, the client starts using the configuration information provided by the DHCP server.

The DHCP server can be attacked if it is not configured properly. In the DHCP starvation attack, an intruder requests for all available DHCP addresses. This can result in a denial of service attack and network outage. An intruder can plug in own rouge DHCP server and start providing IP addresses to the clients. An intruder can give a different default gateway with the DHCP responses. The new default gateway becomes an intruder’s machine and all traffic redirect to a malicious machine to intercept and analysing the network [18].

2.3.4 VLAN spoofing
VLAN spoofing can occur if the switch port is configured in trunking mode or in Dynamic Trunking Protocol. An intruder pretends to be a switch and establishes a trunk to the switch during this attack and gain access to all the VLANs by using the 802.1q trunk tagging on the trunk port. Then he can “hop” into any available VLAN on the trunk [19]. Usually the purpose of VLAN spoofing is to spread worms, Trojans and viruses on the network. In order to stop this attack, disable auto negotiation and do not use default VLANs on any port.

2.3.5 Content Address Memory (CAM) Table Overflow
A switch’s MAC address table holds network information such as MAC addresses available on each physical switch port. MAC address table is limited in size. It will overflow if adequate entries are entered before the old expires [20]. An attacker can fill the MAC address table by sending thousands of bogus entries. If the MAC address table is overflowing, then the switch started to act like a hub and traffic is flooded out to all ports.

2.3.6 Spanning Tree Protocol (STP) Manipulation
STP is used to keep the loop-free topology in the Layer 2 redundant network. Loops can create a broadcast storm. It is enabled by default on switches. A switch with the lowest configuration priority will be elected as Root Bridge among other switches. If the bridge id of all switches is same, then switch with lowest Mac address will elect as Root Bridge. Once a switch elects a Root Bridge, all the redundant paths to Root Bridge will be blocked and all the data will flow through the Root Bridge. An attacker will send bogus BPDUs request to become the Root Bridge because STP does not have any method to authenticate BPDUs messages [21].
3 Experiments
We developed six scenarios in order to perform attacks. Each scenario is investigated by using different attack tools called *Yersinia, IRPAS, Ettercap* and *Wireshark*. These tools are used for penetration testing. Cisco 2960 switches are used in order to implement configurations. Ubuntu (14.04 LTS) is installed on the attacker PC in order to perform attacks.

3.1 Case study 1: ARP Poisoning

![Diagram of ARP cache poisoning attack scenario](image)

Figure 3.1.1: ARP cache poisoning attack scenario

We demonstrated in the figure 3.1.1 how to perform an ARP cache poisoning attack. The attacker PC is directly connected to the switch. An attacker performs this attack by using an attack tool called *Ettercap* [22]. *Ettercap* is a sniffing tool that is normally used to perform a Man-in-Middle attack on Local Area Network. Man-in-Middle attacks can be performed by poisoning the ARP cache. The attacker PC has several network interfaces such as wifi and Ethernet and we connected by the cable so “eth0” is selected. Host scanning tasks performed by *Ettercap* on the local network and all the host will be listed. Select the targeted host which the attack should be performed and start sniffing on that device. On *Ettercap* menu, we start ARP poisoning.

At the same time a sniffing tool called *Wireshark* [23] is started to capture and analyze the packets.
We can see in figure 3.1.2 that an attacker sent his MAC address to both devices. The MAC address 00.0c:29:73:11:45 was being advertised for both the victim PC1 and the switch as shown in the figure 3.1.2. The purpose of advertising same MAC address is to redirect network traffic toward attacker machine. The attacker PC wanted to capture the communication between both devices and this was successfully accomplished.

The victim, PC1, opened a telnet connection and entered the password for telnet which has been captured as it could be seen in figure 3.1.3. The victim host entered password “cisco” on the switch. The attacker PC can see the password as shown in figure 3.1.3. The figure 3.1.3 also shows that a connection between two machines is established and communication between PC1 and switch is being captured.
The figure 3.1.4 shows the telnet session between the victim PC1 and the switch. An attacker can also inject packets in both targeted devices. He/she can see the sensitive information and can change the configuration by injecting packets. We can see the terminal connection in the figure 3.1.4, that is showing the running configuration. That proves that we got the right information and then we tempered one packet and sent it to the switch which is “I am on your PC dude!” in both devices as shown in figure C2 in the appendix C. As a result, figure 3.1.4 shows that packets have been injected successfully in both targeted devices.
3.2 **Case study 2: CDP Attack**

![CDP Attack scenario](image)

Figure 3.2.1: CDP Attack scenario

We demonstrated in the figure 3.2.1 how to perform a CDP attack. The attacker PC is directly connected to the switch. An attacker can perform this attack by using an attack tool called IPRPAS [24]. This tool was developed to attack routers and switches. The attacking tool IPRPAS is installed and started on the attacker machine in order to launch the attack as shown in the figure 3.2.2.

```
nasir@ubuntu:~$ cd
$ cd [-v] [-l <Interface> -n [0,1] ...]
Flood mode (-m 0):
- n <number> number of packets
- l <number> length of the device id
- c <char> character to fill in device id
- r randomize device id string

Spoof mode (-m 1):
- D <string> Device id
- P <string> Port id
- L <string> Platform
- S <string> Software
- F <string> IP address
- C <capabilities>
these are:
  R - Router, T - Trans Bridge, B - Source Route Bridge
  S - Switch, H - Host, I - IGMP, r - Repeater
```

Figure 3.2.2: CDP attack information

A flood attack and spoofing attack can be launched by using the IRPAS tool. To perform a spoofing attack, we can create a spoof entry by implementing following command.
Figure 3.2.3: CDP spoofing attack result

The figure 3.2.3 shows that an attacker sends incorrect information successfully. The CDP shows the incorrect neighbor’s information. CDP does not have any authentication method. This attack does not have any negative effect on the network, but it can confuse and disturb the network administrator.

Figure 3.2.4: flood switch CDP table result

The result shows in figure 3.2.4 that the switch memory near about 38 MB has been filled up and the switch functionality crash due to memory of fragmentation.
3.3 Case study 3: DHCP Starvation

In this case study, we demonstrated how to perform attacks on a DHCP. The figure 3.3.1 has one Layer 3 router, one Layer 2 switch, and two connected computers. DHCP (Dynamic Host Control Protocol) is a protocol that assigns IPs automatically to the clients. The DHCP server is configured on the router for assigning IPs to clients. The DHCP server is not a secure protocol, and it has no security features. If the switch is not configured properly to protect against DHCP starvation attacks, an attacker can plug his attacker machine to a server and start performing the attack from his attacker machine. An attacker performed the DHCP starvation attack by using *Yersinia* tool [25]. *Yersinia* sends discovery packets frequently via spoofed a MAC address on a DHCP server. The DHCP server replies back with ACK packets until it consumes its complete range of IP addresses from its DHCP IP pool. All of these IP addresses are leased to the attacking machine. It can give benefits to the attacker for performing a man in the middle attack, or causing network outages.
3.4 **Case study 4: VLAN Spoofing**

We demonstrated in the figure 3.4.1 how to perform a VLAN spoofing attack on a Layer 2 switch and results are shown in the appendix B. The diagram has one Layer 2 switch and one connected attacker computer. A trunk port on switch carries all information of all VLAN. VTP (VLAN Trunking Protocol) automatically sending VLAN updates between the switch to switch, or switch to router. If the switch is not configured properly to protect against a VLAN spoofing attack, an attacker can plug his attacker machine in with a switch and start performing the attack from his attacker machine. An attacker performed this attack by using an attack tool “*Yersinia*” [25]. Cisco Catalyst switch ports are to default to auto mode for Trunking. It means that all ports are in “dynamic desirable” mode, and they will become trunk ports if they receive Dynamic Trunking Protocol (DTP) frames. An attacker can use *Yersinia* to send DTP frames on to the switch port, and the switch becomes a trunk port between attacker and switch. He can use this attack to sniff all the traffic on all VLANs. This type of attack can be used to discover the username and password credentials. He can also use this attack to wipe out all information about VTP and insert his information.
3.5 Case study 5: Cam Table Overflow

3.5.1: cam table overflows attack scenario

For the explanation of the CAM overflow attack, we performed a case study to get the security vulnerabilities. We demonstrated in the figure 3.5.1, how to perform a CAM table overflow attack on Layer 2 switch and the results are shown in the appendix E.

The figure 3.5.1 has one Layer 2 switch and two connected computers. The switch has a fixed size of the CAM table to store information of MAC addresses. The attacker PC is directly connected to the switch. The attacker in this case performed this attack by using an attack tool called “dsniff” [26]. This attack tool sends a huge number of bogus MAC addresses to fill the CAM table of the switch.

The figure 3.5.2 shows total number of available MAC Address space before the attack.

```
SW_2960#show mac address-table count

Mac Entries for Vlan 1:
-----------------------
Dynamic Address Count : 3
Static Address Count  : 0
Total Mac Addresses   : 3

Total Mac Address Space Available: 8044
```

Figure 3.5.2: cam table available space

The switch dynamically learns one MAC address of PC1 on Port1 and two MAC addresses on Port5. The two MAC addresses on Port 5 is the MAC address of the PC and the MAC address of
Ubuntu OS. The Ubuntu OS installed on VMware workstation. We launched the attack by writing command on the attacking machine terminal.

This attacking tool sends thousands of fake MAC addresses to fill the memory of the cam table as shown in the appendix E. In figure 3.5.3, the cam table filled with bogus MAC address entries.

![SW_2960#show mac address-table count](image)

Mac Entries for Vlan 1:

<table>
<thead>
<tr>
<th>Dynamic Address Count</th>
<th>8046</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static Address Count</td>
<td>0</td>
</tr>
<tr>
<td>Total Mac Addresses</td>
<td>8046</td>
</tr>
</tbody>
</table>

Total Mac Address Space Available: 0

Figure 3.5.3: cam table overflow result

The difference between hub and switch is that, a hub transfers a message across a network to any device that will listen, while a switch transfers a message directly between two devices that are already involved in a communication. By cam table attack, we can see that we make the switch run out of memory to learn new addresses. In this case the switch will act like a hub, which will flood the packets to all ports. At that moment anyone can capture the packets from the switch.
3.6 Case study 6: STP Manipulation

In the above scenario, we have a demonstration of STP attack. We can see how to perform attacks on a Cisco 2960 switch. We used an attack tool called Yersinia [25] to perform this attack. The attacker PC is directly connected to the switch. Before performing this attack, we manually changed the bridge id priority of switch 3. The default bridge id priority on Cisco switches is 32768. After we had assigned priority 24576 manually, switch 3 became the root bridge because of the low bridge id priority. The results are shown in figure D1 and D2 in the appendix D.

```
*Mar 2 06:29:09.799: STP: VLAN0001 heard root 24577-001e.f6d9.8e80 on Fa0/13
*Mar 2 06:29:09.799:  supersedes 24577-001e.f6da.8e80
*Mar 2 06:29:09.799: STP: VLAN0001 new root is 24577, 001e.f6d9.8e80 on port Fa0/13, cost 38
*Mar 2 06:29:09.807: STP: VLAN0001 Topology Change rcvd on Fa0/2
*Mar 2 06:29:09.807: STP: VLAN0001 sent Topology Change Notice on Fa0/13
```

Figure 3.6.2: result after stp attack

In the above figure 3.6.2, Yersinia sent the same bridge id priority with a little lower MAC address to become Root Bridge. If the switches have had the same bridge id priority, then Root
Bridge is selected on the basis of the lowest MAC address. The attacker device on interface 13 became the root bridge, and the topology has been changed entirely. We can see this in figure D3 in appendix D. Now switch 3 is no longer a root bridge and the role of its ports has also been changed. The results can be seen in the appendix D.
4 Results

4.1 ARP Poisoning

In the case study one, we implemented Dynamic Arp Inspection (DAI) to mitigate this attack. We enabled the dhcp snooping before configuring it. After we configured DAI, we performed the attack again, and we got the result shown in figure 4.1.1.

![Figure 4.1.1: result after configure DAI](image)

The figure 4.1.1 shows that a host with the IP address 192.168.10.7 tried to send an ARP packet. The DAI intercepted the packet because it was received on an untrusted interface. The packet did not match against the IP-Mac binding table and for that reason it is dropped as shown in the figure 4.1.1.

DAI is a security feature that is used to validate ARP packets. By default, DAI and DHCP snooping is disabled on all VLANS [39]. DHCP snooping must be enabled before the implementation of DAI, since it needs the DHCP snooping database. DAI checks the APR packets which are received on untrusted ports. It intercepts ARP packets, and if the receiving packets do not match against the IP-Mac binding table, they will be dropped. It can also validate packets of a statics ACL created by a user. DAI gives priority to statics ACL over DHCP snooping binding database table. DAI checks ARP packets against the static ACL table and the DHCP snooping binding database [27].

Adding static ARP entries to the client hosts is another solution to stop ARP spoofing attack. This technique restrains an attacker from adding spoofed ARP entries. However, static ARP entries are very difficult to maintain, especially in large size networks.

Different Intrusion Detection Systems (IDS) like snort, arpcachewatch and DecaffeintID can be installed to detect ARP spoofing attacks. They can detect any change in the MAC addresses immediately. In addition, they alert the user by messaging if any changes in the MAC addresses are detected. These IDS can perform only detection and are not capable to prevent ARP spoofing attacks. The downside of this technique is that the attacker can achieve his/her goals in short time before the network administrator take action against the attack [34].

If we compare the above presented solutions, we can conclude that Dynamic ARP Inspection (DAI) and DHCP snooping combination is best technique of preventing a cam table overflow attack.
All the solutions discussed above are not limited to the Cisco switches. These can also be implemented in other switches vendors like HP, Juniper Networks [35], Netgear and Huawei etc.

4.2 CDP Attack
In the case study two, CDP attack can be mitigated by disabling CDP. The best practice is to disable CDP globally or for each interface. If CDP is used for troubleshooting or security operations, CDP should be enabled globally, each device in the local network should run CDP. However, it should be disabled on those interfaces on which the interfaces connected to the external network, for example internet service provider (ISP) [28].

CDP is a Cisco proprietary protocol and runs only on Cisco manufactured devices, therefore this attack can be performed only on Cisco devices.

Steve A. Rouiller and Sean Convey also provide the same solution against the CDP attack [31, 32].

4.3 DHCP Starvation
In the case study three, we implemented port security to stop unauthorized machines from connecting. Port security has one of the most important security functionalities in Cisco Layer 2 switches. It is used to minimize the DHCP Starvation attack by providing a limited number of MAC addresses that are allowed to communicate on a switch port [31]. We tested this port security on Cisco Layer 2 switches, and we got the best result to protect the switch against this DHCP starvation attack. If we bind the maximum number of the MAC addresses to the switch ports, the switch will not allow an attacker to plug his computer on this switch.

The same technique is also presented by Juniper Networks to mitigate DHCP Starvation attack [37]. DHCP snooping is another technique that can be implemented in order to mitigate DHCP attack. This technique can mitigate Rogue DHCP Server attack. In DHCP Rouge server attack an attacker user pretends itself as a DHCP server and reply to DHCP request with the invalid ip address. Port security is not useful to mitigate Rogue DHCP Server attack [31].

DHCP snooping monitors and controls DHCP messages received from untrusted devices like a host connected to the switch. It builds and maintains a DHCP snooping database table using information obtained from intercepted DHCP messages. A host with valid binding is granted access to the network [38].

Steve A. Roui (2008) and Bhaiji (2005), mentioned about mitigate this attack by implementing port security on all network switches such as restrict the number of MAC addresses on the port. These solutions are similar to our solutions [3, 32].

4.4 VLAN spoofing
In the case study four, we used the following techniques to mitigate the VLAN spoofing attack [32].

- Disabled all VLAN ports which are not used in our network.
- Disabled auto Trunking port.
• Switchport nonegotiate.

Steve A. Rouiller and Sean Convey also provide the same solution to protect from VLAN spoofing attack [31, 32].

4.5 CAM Table Overflow

In blackhat research report [31], a solution against cam table overflow attack called “port security” is presented. It is a common and primary solution against cam table overflow attack.

![Figure 4.5.1: result after configuring port security](image)

After the port security was configured, we launched an attack and more than allowed MAC addresses were detected on port interface fa0/5 as shown in the figure 4.5.1. As the result of this, the port f0/5 in the figure 4.5.1 is moved into err-disable and shut down as shown in figure 4.5.1. More figures of the CAM overflow attack can be seen in the appendix E.

**Port Security** has one of the most-important security functionalities in Cisco Layer 2 switches. It is used to prevent the CAM table overflow attack by providing a limited number of MAC addresses that are allowed to communicate on a switch port. We can configure this type of secure MAC addresses:

- **Static secure MAC addresses**: These can statically configure all secure MAC addresses by using the switch port, port security MAC address interface configuration command. These MAC addresses will be stored in the address table, and add to the switch running configuration.

- **Dynamic secure MAC addresses**: We can allow the port to dynamically learn secure the MAC addresses of connecting devices and store only in address tables. If the port has a link-down status, all dynamically learned addresses are removed.

- **Sticky secure MAC addresses**: These can learn dynamically or configure manually and store in the running configuration of the address table. If we save these addresses in configuration files, then ports do not need to relearn them again, even if the switch restarts [29].

The same solution is also presented on SANS Institute InfoSec Reading Room research paper and the same result is achieved [32]. This technique can also be used in other switches for example Juniper, HP and Netgear [33].

**DHCP snooping** and **Dynamic ARP Inspection (DAI)** combination is a another method of preventing a cam table overflow attack. By using this technique multiple Layer 2 attacks can be mitigated [20].
4.6 STP Manipulation

In blackhat research report [31], two protection mechanisms against STP manipulation called *BPDU Guard* and *Root Guard* are presented. In case study six, we implemented root guard and Bridge Protocol Data Unit (BPDU) guard on access port fa0/13 and launched the attack. We got the following result shown in the below figure 4.6.1.

![Figure 4.6.1: result after applying security](image)

We can see in the figure 4.6.1 that BPDU guard detected Bridge Protocol Data Unit (BPDU) messages on access port fa0/13 and moved this port into errdisable state. It prevents host devices to participate in the STP process. Below it is explained, how root guard and BPDU guard works against STP manipulation.

Usually STP is enabled on a switch by default. The solution against STP manipulation is to disable STP. We do not propose this solution because if we disable STP in a redundant network, then broadcast storm can occur. In a redundant network a broadcast can circulate around the network and can consume all available bandwidth. Moreover, we cannot get redundant paths without looping.

Root guard is a security feature that is enabled on root ports. If root guard enabled ports receive greater BPDU messages, the bridge would move the sender port into non-consistent state. It ensures that root guard enabled ports are designated ports as Root Bridge ports are designated ports. It is shown in figure D1 in appendix D.

It is implemented on the ports that connect to host devices because attacks originate from host devices. BPDU guard will not allow devices behind BPDU guard enabled ports to take part in the STP process because end user devices do not need to take part in STP. The difference between root guard and BPDU guard is that a root guard enabled port receives BPDU messages until it gets superior BPDU, but a BPDU guard enabled port does not receive BPDU messages [30].

The same solutions are also implemented in SANS Institute InfoSec Reading Room research paper and the same results are achieved [32]. These solutions can also be implemented on switches from other vendors, for example Juniper, HP [36], Netgear and Dell.
5 Conclusion

Most of the Layer 2 protocols are insecure due to lack of authentication. If proper security is not implemented on Layer 2 devices, an attacker can exploit security holes by using different attack tools. In this thesis we suggested that performing attacks for learning and testing purpose is the best way in order to find vulnerabilities and then secure a network. Techniques and methods discussed in this thesis can help a network administrators during security testing. To mitigate CAM table overflow we used “port security” method, to mitigate ARP poisoning we used dynamic ARP inspection solution and moreover to overcome with STP manipulation we used root guard and BPDU guard in this thesis report. Furthermore, the effects of these attacks are presented in this thesis work. The solutions are tested with attacking tools Yersinia, dsniff, Ettercap, IPRPAS to get the results. Network attacks can be mitigated by deployment of the security configuration carefully. All the presented solutions are not limited to the cisco switches. These can be implemented in other switches vendors like HP, Juniper Networks, Netgear and Huawei etc. However, the configuration commands are little different on every switch vendor. In addition, CDP is a Cisco proprietary protocol and runs only on Cisco manufactured devices, therefore the CDP attack is workable only on cisco devices.
6 Abbreviation

IRPAS (Internetwork Routing Protocol Attack Suite)
STP (Spanning Tree Protocol)
VLAN (Virtual Local Area Network)
BPDU (Bridge Protocol Data Unit)
CDP (Cisco Discovery Protocol)
RARP (Reverse Address Resolution Protocol)
ARP (Address Resolution Protocol)
DHCP (Dynamic Host Configuration Protocol)
MAC (Media Access Control)
IP (Internet Protocol)
DNS (Domain Name Server)
DG (Default Gateway)
DAI (Dynamic Arp Inspection)
HTTP (Hyper Text Transfer Protocol)
7 References


[16] Debashis Roy, Katayoon Moazzami and Rachita Singh, “ARP Spoofing and Man in the Middle attack using Ettercap”, School of Computer Science, University of Windsor, Canada.


[22] “Ettercap” a tool for performing attack on the network

[23] “Wireshark” a tool used for network traffic analyses

[24] “IPRPAS” a tool for performing attack on the network

[25] “Yersinia”, a tool for performing attack on the network

[26] “CAM table overflow” by Song, D. “dsniff”


[33] “CAM Table Overflow” http://hakipedia.com/index.php/CAM_Table_Overflow


Appendix A  DHCP Starvation Attack
Appendix B VLAN Spoofing
<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Encapsulation</th>
<th>Status</th>
<th>Native vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/6</td>
<td>auto</td>
<td>802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>Vlans allowed on trunk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fa0/6</td>
<td>1,4894</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>Vlans allowed and active in management domain</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fa0/6</td>
<td>1.18.30</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>Vlans in spanning tree forwarding state and not pruned</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fa0/6</td>
<td>1.18.30</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
appendix C ARP cache poisoning

Figure C1: character injection
Figure C2: character injection
Appendix D STP

Sw3#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID  Address    Priority  Hello Time  Max Age  Forward Delay
  001e.f6da.8e80  24577       2 sec     20 sec     15 sec

  This bridge is the root

Bridge ID  Priority  Address    Hello Time  Max Age  Forward Delay
  24577      (priority 24576 sys-id-ext 1) 001e.f6da.8e80  2 sec    20 sec     15 sec

Aging Time 300 sec

<table>
<thead>
<tr>
<th>Interface</th>
<th>Role</th>
<th>Sts</th>
<th>Cost</th>
<th>Prio.Nbr</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/1</td>
<td>Desg</td>
<td>FWD</td>
<td>19</td>
<td></td>
<td>P2p</td>
</tr>
<tr>
<td>Fa0/2</td>
<td>Desg</td>
<td>FWD</td>
<td>19</td>
<td></td>
<td>P2p</td>
</tr>
</tbody>
</table>

Figure D1

Figure D2
Appendix E cam table overflow attack

Figure E1: attack launched by dsniff
Figure E2: mac addresses learned on port interface after attack

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Type</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>324b.d075.f965</td>
<td>DYNAMIC</td>
<td>Fa0/5</td>
</tr>
<tr>
<td>3253.c40d.a09b</td>
<td>DYNAMIC</td>
<td>Fa0/5</td>
</tr>
<tr>
<td>3269.166e.09ad</td>
<td>DYNAMIC</td>
<td>Fa0/5</td>
</tr>
<tr>
<td>3271.8c22.8665</td>
<td>DYNAMIC</td>
<td>Fa0/5</td>
</tr>
<tr>
<td>3274.9520.db4e</td>
<td>DYNAMIC</td>
<td>Fa0/5</td>
</tr>
<tr>
<td>3275.01d5.7dfe</td>
<td>DYNAMIC</td>
<td>Fa0/5</td>
</tr>
<tr>
<td>3278.5434.0e09</td>
<td>DYNAMIC</td>
<td>Fa0/5</td>
</tr>
<tr>
<td>3279.445b.a4b2</td>
<td>DYNAMIC</td>
<td>Fa0/5</td>
</tr>
<tr>
<td>327d.a372.8581</td>
<td>DYNAMIC</td>
<td>Fa0/5</td>
</tr>
<tr>
<td>3285.482c.092d</td>
<td>DYNAMIC</td>
<td>Fa0/5</td>
</tr>
<tr>
<td>3286.9026.e6e5</td>
<td>DYNAMIC</td>
<td>Fa0/5</td>
</tr>
<tr>
<td>3287.4e2d.829f</td>
<td>DYNAMIC</td>
<td>Fa0/5</td>
</tr>
<tr>
<td>3291.f15b.0609</td>
<td>DYNAMIC</td>
<td>Fa0/5</td>
</tr>
<tr>
<td>329f.0469.a85f</td>
<td>DYNAMIC</td>
<td>Fa0/5</td>
</tr>
<tr>
<td>32a0.3421.2796</td>
<td>DYNAMIC</td>
<td>Fa0/5</td>
</tr>
<tr>
<td>32aa.991b.f5d9</td>
<td>DYNAMIC</td>
<td>Fa0/5</td>
</tr>
<tr>
<td>32af.0007.19ab</td>
<td>DYNAMIC</td>
<td>Fa0/5</td>
</tr>
<tr>
<td>32b4.3c30.5e63</td>
<td>DYNAMIC</td>
<td>Fa0/5</td>
</tr>
<tr>
<td>32bc.8c75.30c2</td>
<td>DYNAMIC</td>
<td>Fa0/5</td>
</tr>
<tr>
<td>32bd.572e.1d8e</td>
<td>DYNAMIC</td>
<td>Fa0/5</td>
</tr>
<tr>
<td>32c1.613e.8a20</td>
<td>DYNAMIC</td>
<td>Fa0/5</td>
</tr>
<tr>
<td>32c4.bf40.9548</td>
<td>DYNAMIC</td>
<td>Fa0/5</td>
</tr>
<tr>
<td>32c4.d965.2e7e</td>
<td>DYNAMIC</td>
<td>Fa0/5</td>
</tr>
</tbody>
</table>

FastEthernet0/5 is down, line protocol is down (err-disabled)

Hardware is Fast Ethernet, address is 001d.7169.6105 (bia 001d.7169.6105)
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)

Figure E3: port shutdown because of security violation