A Survey of Ethernet LAN Security

Done and Presented by :

- Tarun Ayyagari - B180682CS
- Tarun Kansal - B180403CS
- Teres George - B180318CS
- Thanzeel Hassan - B180322CS
- Thummaluru Mohith Kumar - B180299CS
- Tushar Kumar Patni - B180122CS
- Umarul Farooque Kozhummal - B180455CS
- Vimal Rajesh - B180336CS
- Vishnu Sajith - B180474CS
- Yacha Venkata Rakesh - B180427CS
- Yadla Prasanth Babu - B180580CS

Table of Contents

I. INTRODUCTION

- Ethernet was designed to be flexible, decentralized and low cost.
- It is now switched, full duplex, collision free with standard speed of 1 Gbps.
- It is now the only form of wired LAN still used.
- Ethernet segments are increasing in size as it faster than using Routers.
- We will discuss about the security aspects of Ethernet and understand the benefits and shortcomings of Ethernet.
- The topics discussed in here are with context to wired Ethernet.

II. ETHERNET TODAY

A. Ethernet Frame

- Plain Ethernet is defined as full-duplex, twisted pair based ethernet connecting hosts joined by switches.
- Every node in a Ethernet segments communicates using frames.
- Frame Consists of:
  - Preamble
  - Destination Address
  - Source Address
  - Ethertype
  - Payload
  - CRC

Preamble	Destination address	Source address	Type or length	Payload	CRC
8	6	6	2	46-1500	4

Contd..

- Preamble is 8 bytes long and is used for synchronization with the receiver host.
- Destination and Source MAC addresses are are 6 bytes each and are hard coded into the NIC.
  - Frames can be sent to unicast, multicast or broadcast addresses.
- Ethertype field is 2 bytes long and is used to describe the length/type of payload.
- Payload is the actual data in the frame(usually higher layer data). Minimum size is 46 bytes.
- Cyclic Redundancy Check (CRC) is used to check the contents of the frame are not decayed.

B. Ethernet Switch

- Connects hosts together over an Ethernet network.
- Hosts are connected to ports on the Switch. The switch then forwards frames received on one to the port of the destination host.
- Switch maintains a Content Addressable Memory (CAM) which maintains hosts' MAC addresses and the port they are connected to.
- It fills the CAM using backward learning.
- Multiple hosts can have the same port assigned to them.

Contd...

- Switches can also connect to other switches. Called a trunk link.
- A switch has 3 layers:
  - Data Plane - forwards frames from one port to another.
  - Control Plane - Handles frames that need processing. Done by the CPU.
  - Management Plane- To configure the switch’s features.
- CAM can also store additional information based on the implementation.

C. Spanning Tree Protocol

- The IEEE 802.1D Spanning Tree Protocol (STP) is a method for avoiding loops in the LAN.
- Layer 2 protocol that runs on bridges and switches.
- When connected in a mesh topology, switches would receive the same frame over several links and have to decide which port to enter into the MAC address table.
- Sooner or later the individual MAC tables would form a loop together and frames would start to circulate within the network congesting it.
- STP creates a spanning tree as a solution to this problem.
- One of the switches is initially selected to act as a root node and broadcasts Bridge Protocol Data Units (BPDUs), which have a cost.

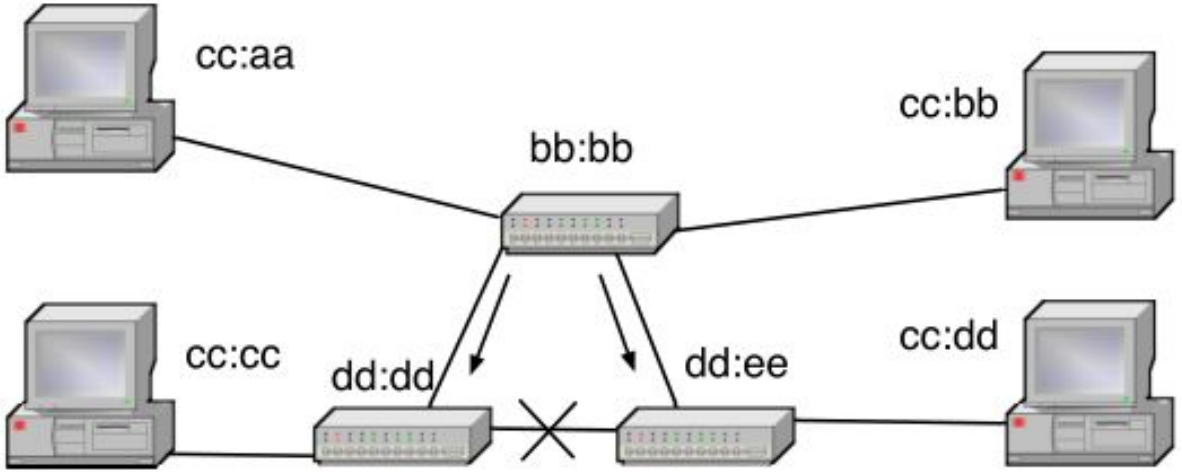


Fig. 3. Creating the spanning tree; switch bb:bb becomes the root switch.

- Each switch increments the cost and floods the frame out of the other ports.
- If a switch receives a BPDU from two ports, it blocks the port with the higher cost.
- If an active link between two hosts is lost, they (or one of them) send a Topology Change Notice (TCN) BPDU to the root switch, which broadcasts a TCN message to all switches, and the tree reconfigures.
- Several versions of STP exist : -
    - Rapid STP improves performance from the original.
    - Multiple STP supports separate spanning trees for each VLAN.
    - Vendors have developed their own versions for similar needs.

D. Layer 3 Adaptation Protocol

- IP version 4 (IPv4) uses two protocols to operate over Ethernet : -
  - Dynamic Host Configuration Protocol (DHCP) is used to request an IP address for a host.
  - When an IPv4 host without an IP address becomes active on an Ethernet segment it sends a request for DHCP servers using an Ethernet broadcast.
  - Upon receiving one or more unicast replies, the host selects one server and requests an IP address with a unicast message and, upon success, receives a lease for an IP address and additional information, such as the netmask and the gateway's (router's) IP address.

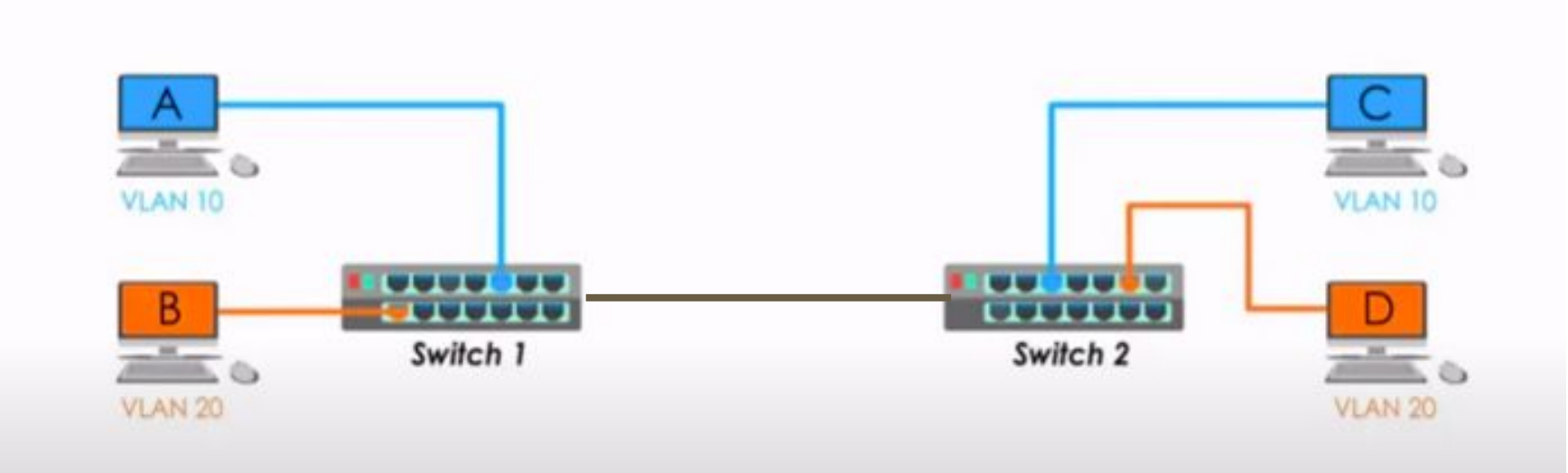
- Address Resolution Protocol (ARP) is needed for IP to operate on shared media like Ethernet, as the MAC addresses need to be mapped to corresponding IP addresses.
- When a host wishes to communicate with another host in the LAN, like the gateway, it sends a broadcast message requesting a MAC address that corresponds to the IP address in the message.
- The host, which has the IP address in use, responds with a unicast message.
- The recipient stores the IP and the MAC address pair in a table (the ARP cache) for some duration.

- IPv6 has similar functions.
  - Hosts are found with Neighbor Discovery Protocol, which uses Ethernet multicast.
  - Some hosts use Dynamic Host Configuration Protocol v6 (DHCPv6) instead
  - IPv6 routers are found by listening for multicast Router Advertisements, from which a host can create its own IPv6 address and use Neighbor Discovery to verify its uniqueness.

- Switches may also include other layer 3 functionalities.
  - IP multicast handling
  - IP routers require registration for a multicast group with IPv4 Internet Group Management Protocol (IGMP) or IPv6 Multicast Listener Discovery (MLD).
  - However, the multicast packets are typically sent to the Ethernet layer as broadcast frames, thus flooding the network.
  - A switch can snoop into the layer 3 registration messages and build a table of multicast listeners, thus forwarding multicast frames only to those ports where a listener is active.

E. Virtual LAN

- Virtual LANs or VLANs are used to separate a physical network into several logical networks.
- The reason why this concept was introduced was to increase efficiency by making the best use of the limited amount of size of the broadcasting domain.
- It is also used for security purposes.


A
VLAN 10
B
VLAN 20
Switch 1
Switch 2
C
VLAN 10
D
VLAN 20

Structuring of VLAN tag and identification

- To differentiate between the frames when transiting between the switches, the VLAN mechanism adds a four byte VLAN tag inside the Ethernet header, between the sender-MAC address and the ethertype fields.
- Then, it adds a second tag to create separate local and provider VLAN domains.
- In order to notify the cables that it is using VLAN, the tag's first two bytes contain the value 0x8100.
- The purpose of the other two bytes is to identify which particular VLAN this packet belongs to.

How it helps in security

- As said in the previous slide, the switch will process the frames transparently, because it has been identified that the first two bytes match the ethernet field.
- Now, since the other two bytes show where this packet belongs to, the switches can enforce more boundaries, meaning adding more security.
- This can be done by putting the tag as soon as the frame is sent from the host and can be removed before it reaches the destination.

F. Layer 2 control plane protocols

There are a lot of protocols that are linked to the ethernet.

- Hot Standby Router Protocol (HSRP) :

  * It is designed for multiple redundant routers to communicate on the active and standby roles.

  * The routers share a virtual MAC and IP address. The messages are sent using IP multicast and are authenticated with a clear text password.

  * This is a Cisco proprietary protocol and it was later replaced by a standardized protocol

  Called Virtual Router Redundancy Protocol.

- There are also many network discovery protocols in order to find out how a particular network is organized.
- IEEE Link Layer Discovery Protocol is becoming more popular.
- The reason is because such protocols report on the node’s connectivity, addresses and capabilities.
- Other similar protocols include Cisco Discovery Protocol and Microsoft’s Link Layer Topology Discovery.

- Link aggregation technologies and mechanisms are important because they help in combining multiple physical links into one and this would help in high traffic.
- This can be especially utilized in STPs.
- The protocol for such purposes is the Link Aggregation Control Protocol.
- These links can be aggregated and treated as one link.

III. Ethernet Threats

Ethernet Threats

- Aim
  - Gaining access to the target Ethernet segment
- Attacker
  - might be an insider with full access rights
  - may have taken control using a malware application or other methods
- Key Vulnerabilities
  - Self Configuring nature
  - MAC table learning methods, STP, ARP.

Motivation behind attacks

1. Learning about private network topology and traffic
2. Gaining control over switches, routers, or servers in the LAN
3. Eavesdropping
4. Manipulating information
5. Disrupting the availability of the network

Contd...

Few prominent methods used for attacking Ethernet Segments

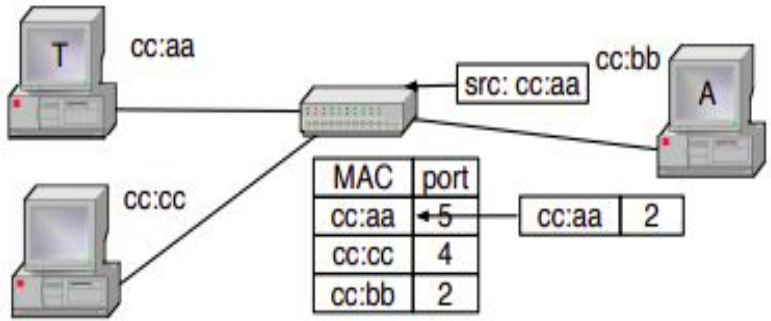
A. Traffic Confidentiality
B. Systems Security
C. Network and System Access
D. Denial of Service
E. Traffic Integrity

A. Traffic Confidentiality

- By analysing the traffic in the network, attacker can gain information about passwords and network topology info that can be used later.
- Original coaxial ethernet was easily eaves droppable bus, where every station received every frame.
- Modern Bridged Ethernet network filters the traffic and a host receives its own traffic , broadcasts and random frames flooded at the switches after the timeout.
- Passive eavesdropping is also possible.
- Attacker uses a software to generate enough frames with random addresses to overwrite the entire MAC table and make the switch flood all data frames to all ports for eavesdropping.

MAC Spoofing attack

- A frame with a forged sender address overwrites the correct entry in the MAC table and redirects traffic to the attacker.
- This is useful when the real owner of the MAC address is disables or offline.



B. Systems Security

Several threats are not tied to the architecture of Ethernet itself but to its implementation and use

- Configuration and Installation Issues
  - Faulty, Lacking or incorrect configuration of the network switches can enable an attacker to get access to more of the network's resources than intended like in VLAN hopping attack.
  - Even when using network management tools, vulnerabilities are usually invisible by their nature and hard to notice

Contd...

- Implementation Issues and Vendor Extensions
  - Attacker can analyze the particular implementation and find unforeseen features like higher level areas of the switch
- Architectural Issues
  - Architecture primarily focuses on message delivery and not on security
  - For instance, in the basic switch design where a frame to an unknown address is flooded out to all ports.
  - But the alternative for this should have been not deliver anything unless the authenticity of the receiver is established

Contd...

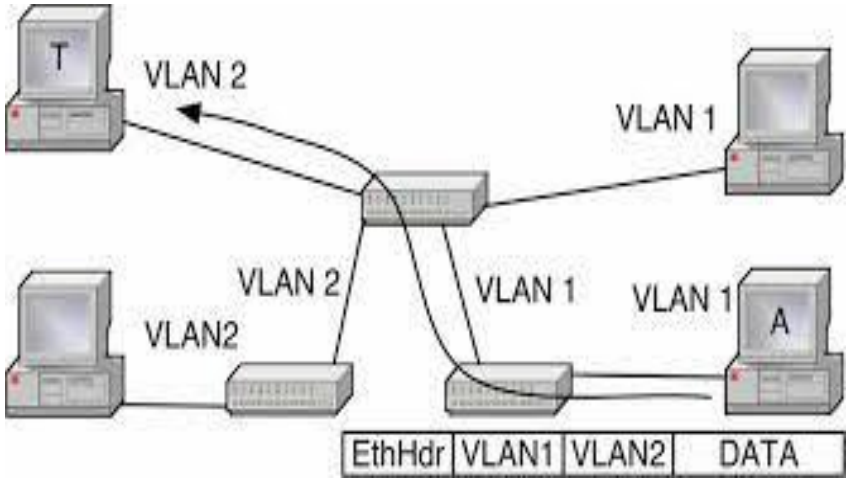
- Issues with Legacy Technology
  - Ethernet technology adds the equipment and software from various eras which makes modern solutions hard to deploy
  - Operating with legacy equipment might leave holes in the security perimeter
- Freely Available Software for Attacks and Exploits
  - Network Sniffers - Wireshark, Tcpdump
  - Packet crafting - Hping

C. Network and System Access

- **Unauthorized Joins**
  - Can gain physical access, plugging in a switch between the existing computer and the wall socket
  - Removing the cable from a computer and plugging it into another computer, or plugging in a switch between the existing computer and the socket.
- **Unauthorized Expansion of the Network**
  - Ethernet's architecture allows users to expand the network by installing their own switches or wireless access points.
  - Automatically be allowed to join the network, unless the switches are configured to prevent it by limiting new MAC addresses

- **VLAN Join**
  - For VLAN management protocols on host ports, a host can act as a switch and join all VLANs.
  - Even if the switches are configured to not transmit VLAN management protocols, but they will still listen for these protocols
  - Attacker uses these hidden features to probe the switch
- **VLAN Hopping**
  - It can be achieved when a layer 3 device, such as an IP router, is serving several VLANs and is reachable through all of them.
  - In this the attacker can send a frame with the router's LAN port MAC address and the IP address of a host in another VLAN, thus using layer 3 to bypass layer 2 restrictions.
  - Depending on configuration, the router will receive the frame and forward it to the IP layer, inspect the IP address and resend it to the correct recipient on a VLAN other than the attacker's

- **VLAN Tagging**
  - In this Attacker can create Ethernet frames that have a VLAN tag and thus inject frames to VLANs to which they are not supposed to have access.
  - A type of this is Double Tagging in which attacker creates a frame which has the target host's MAC address as the recipient and contains a VLAN 1 tag followed by a VLAN 2 tag
  - The double tagging attack does not provide return traffic capability, but additional spoofing can do this, too



VLAN double tagging attack; Attacker A's frames reach target T.

- **Remote Access to the LAN**
  - Can be achieved by gaining higher layer access to a host on the segment.
  - To get a user at the target network to open a remote system administration service, which then connects to a host on the Internet and enables the attacker to access the Ethernet layer.
- **Topology and Vulnerability Discovery**
  - Attacker tries to map the network's topology and services in host to find the vulnerabilities for further attacks.
  - By sending ARP broadcast, attacker can gain the IP addresses that are in use and services or gateways to which other hosts connect to.
  - Potential vulnerabilities can be identified by the info requested from DHCP server, like info regarding host's software including operating systems, services, and versions.

- **Break-Ins**
  - These attacks typically target vulnerabilities on higher layer network software, like the TCP/IP stack and especially server applications.
  - The attacker can lead to the capture of a host or a switch, which can be used for further attacks. They can also target the Ethernet firmware in the NIC and software at the host and attempt to get control of the interface.
- **Switch Control**
  - By default switches have default or no passwords, and these passwords can be reset by gaining physical access to switch.
  - After gaining access to switch, traffic can be rerouted by switching links down, claiming the STP root by raising the priority of the switch or DoS selected links.
  - But switch's software limits the attackers ability to eavesdrop on the traffic or generate spoofed frames.
  - Workstation is needed for such attacks, along with the connected host the switch can be used to turn on the mirroring for eavesdropping and gain access to any VLAN in use

D. Denial of Service

1. Basically DoS attacks is not to gain access to data but to prevent its use.
2. This attack can be implemented on layer 1 by cutting links physically or by damaging the circuitry with electricity.However, layer 2 attacks can cause much more damage.
3. Depending on the switch design this may affect more than one port, as one chip serves several ports And Making the entire switch inoperable is less likely but possible.

- **Resource Exhaustion Attacks**
  - This attacks mainly target the control and management planes of a switch by sending frames that require additional processing and handling.
  - Unknown unicast flooding is a method for sending frames with a receiver address that does not exist in the network.
  - As CAM tables do not have this address, the frame is broadcast over all links which is the same attack as MAC flooding but the intention is to congest the network and success depends on being able to cause sufficient traffic while in MAC flooding is to allow normal traffic but make the switch broadcast it

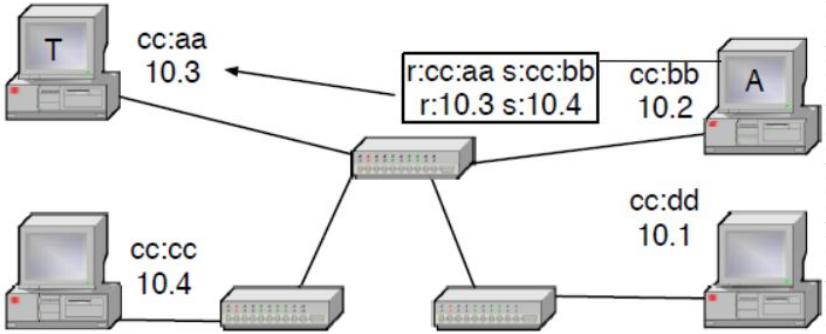
- **Protocol Based DoS**
  - STP that makes a tree out of a mesh network is designed to be self-configuring
  - In this Attacker that controls a node on the network can send STP messages and pretend to be a switch
  - Whole Switching network can be brought to halt by flooding it with STP TCNs or other STP control messages

E) Traffic Integrity

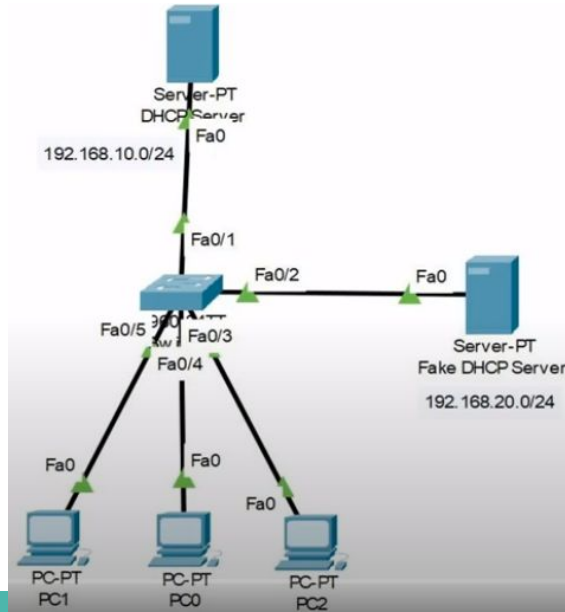
- Three main goals of Security are Confidentiality, Integrity and Availability (CIA).
- After confidentiality, the next step for an attacker is to modify traffic on the network thus compromising Integrity.
- Integrity has three goals to achieve data security.
  - Preventing the modification of information by unauthorized users
  - Preventing unauthorized or unintentional modification of information by authorized users.
  - Preserving internal and external consistency.
- For Instance, An attacker can imitate a bank's web server to a user, and imitate the user to the bank's server, and gain temporary control of the user's bank account.

E. 1) ARP and DHCP Poisoning

- ARP (Address Resolution Protocol) is a stateless protocol and most of the operating systems will accept ARP replies even when not requested.
- This enables attacker to capture traffic intended for another host just by sending an ARP spoof message to the sender with the intended receiver's IP address and the attacker's MAC address.
- Similarly, a host can detect broadcast DHCP (Dynamic Host Configuration Protocol) server requests and race the server to reply them first. On success the attacker can assign a gateway router that is different from the host's LAN and DNS servers to the target host, along with its IP address, and thus control all the host's traffic.



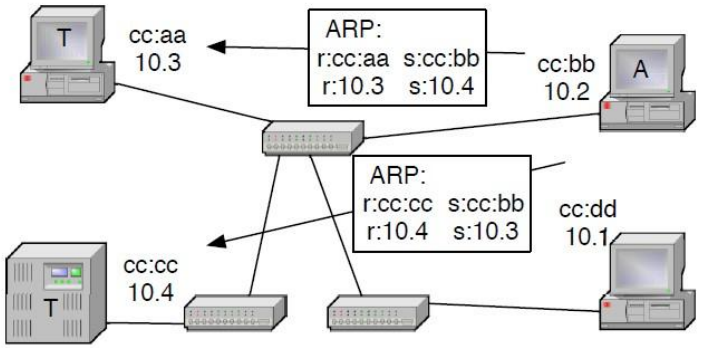
A modifies T's ARP table by sending an ARP spoof message that A is the one with IP address 10.4



Attacker sending host an IP address not in his LAN spoofing as DHCP server

E. 2) Man in the Middle

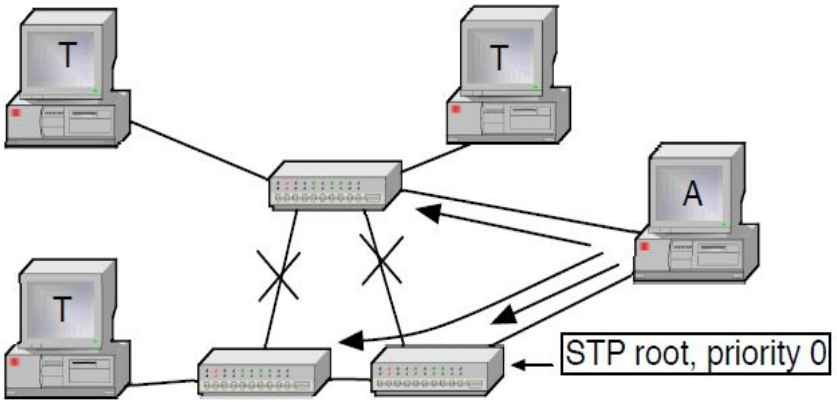
- If an attacker can direct traffic to pass through their node and that traffic is not protected by an integrity verification mechanism, the attacker can easily modify the traffic thus compromising integrity.
- MITM attacks are performed relatively easily on an Ethernet segment against higher layer protocols. IP being the most common higher layer protocol on Ethernets, above mentioned ARP and DHCP poisoning attacks can be deployed for eavesdropping or even traffic modification.
- MITM attack on the Ethernet layer itself is harder, but can be done using STP (Spanning Tree Protocol).



Double ARP spoofing attack by poisoning ARP caches of both targets A can intercept all traffic between the two hosts

E. 2) Man in the Middle

- If a host is connected to two switches it can act as the Root Bridge in the STP environment and create a tree topology, where part of the traffic goes through this host.
- A host sets its STP priority to lowest and becomes the root, splitting networks in two and gaining access to traffic between the two halves.
- This attack requires gaining a connection to two switches.
- Router redundancy protocols like HSRP (Hot Standby Router Protocol) or VRRP (Virtual Router Redundancy Protocol) may also be used to Masquerade as a router and gain access to the traffic.



STP root capture splits the network and leaves A in the middle for MITM

E. 3) Session Hijacking

- Ethernet is a stateless protocol, but many higher level protocols create a session. Once a session is created it is often assumed to be trusted and no further traffic verification is made.
- If an attacker can eavesdrop or somehow gain enough information about a session (IP addresses, TCP ports, sequence numbers, application data like HTTP authentication cookies), the attacker can easily re-create the session and act like one endpoint.
- One end point can be silenced with a DoS attack. With the correct timing, a session may be brought up to date with the correct application messages or by trusting TCP to discard packets that appear to be duplicates on basis of sequence number.

E. 4) Replay

- A message eavesdropped earlier can be sent again.
- As the message is not modified, it can be authenticated or encrypted using the same mechanism by the original sender without affecting the attack - the attacker just need to guess at the content of the message to consider whether its worth sending.
- Within the Ethernet domain useful messages to resend would be small, stateless control messages that fit within one frame is rare.
- Typical messages for targeting a resend attack could be routing notifications or SNMP (Simple Network Management Protocol) “set” or “trap” messages.

IV. EXISTING SECURITY SOLUTIONS

IV. Existing Security Solutions

- The security of Ethernet has been improved by standardization organizations, equipment vendors, and the research community.
- Ethernet's lack of security has been solved by defining any Ethernet segment as unsecure and requiring it to be placed inside a protected domain: behind a firewall in a secure building with trusted staff.
- A major problem is that a switch has no way of knowing if each of its ports is connected to: one computer (a host); a host with several virtual hosts (and virtual MAC addresses); a hub; a silent switch (that does not talk STP and other topology revealing protocols); a regular switch; or a switch that has other switches behind it.

A. Router Based Security

We start by presenting how replacing one central Ethernet switch with an IP router would affect security.

The IP router partitions the rest of the Ethernet network into several segments. Each new segment is a separate broadcast domain. ARP, STP, VLAN, and MAC address table based attacks are no longer possible between the segments. Inside the segments the same attacks remain feasible, unless each switch is replaced with a multiport router.

Replacing a switch with a router will incur some costs. Compared to an Ethernet switch an IP router provides a considerable amount of protection against other users connected to the same router.

Router over Ethernet Switch?

1. The traffic between segments becomes impossible to eavesdrop on from other segments.
2. The router blocks Ethernet's control plane protocols (ARP and STP) from transit between the segments.
3. An IP router requires configuration, such as address allocation and default route configuration. But this can be automated as in case of residential Broadband Connection.
4. The router also prohibits easy mobility.
5. A router also splits the broadcast domain. Auto discovery protocols are blocked (unless the router includes application layer support for these)

Conclusion or Outcome

Despite the cost overhead, IP router is definitely an upgrade over Ethernet Switch when in terms of the security it provides.

Compared to an Ethernet switch an IP router provides a considerable amount of protection against other users connected to the same router. An attacker may target the protocols and implementations on higher layers (IP, transport, and application). DoS is also possible. However, in general, most of the attacks like MITM attack, and DHCP attacks become infeasible.

B. Access control

An attacker needs access before being able to perform any attacks. Untrusted entities can be kept out by limiting access to the network or requiring authentication. Limiting the access capabilities of trusted entities reduces the threat potential even further.

Different Types of Access Control

1. Physical Protection of the Network
2. Segmentation and VLANs
3. Individual VLANs
4. Authentication Based Access Control
5. Access Control Lists
6. Control and Management Plane Overload Protection:
7. Centrally Managed LAN Security

1. Physical Protection of the Network

Network equipment can be located in locked cabinets and racks and wiring installed inside walls to prevent unauthorized access. However, access is needed for the network to be useful and physical protection is of limited value.

2. Segmentation and VLANs

- Limiting the size of an Ethernet segment limits the area vulnerable to attacks. A segmentation method external to Ethernet would be a higher layer device, such as a router or firewall.
- Inside Ethernet, VLAN mechanism provides a way to limit broadcasts and other traffic to specific segments. They are logically separated within the same physical installation and define security domains inside one network.
- VLAN based security depends on proper switch configuration and vendor documentations but the default settings of switches are not secure, leaving it vulnerable to VLAN hopping etc.

3. Individual VLANs

Each host on the Ethernet can also be placed into its own VLAN, using IEEE 802.1ad Q-in-Q double tagging or vendor provided Private VLAN (PVLAN) switch configuration.

- Q-in-Q is mainly a specification for extending the VLAN 14 bit identifier space by adding another VLAN tag.
- The PVLAN technique uses switch configuration to isolate hosts and only let their traffic pass to one “promiscuous” port, typically connected to a router and to the Internet

4. Authentication Based Access Control

Being able to authenticate the user or host connecting to a port at the switch is a step forward from plain physical access control.

IEEE 802.1X port authentication supports several types of authentication credentials, such as a user-name and password pair, or a certificate and corresponding private key.

When hosts are connected directly to an 802.1X capable switch, it provides protection from MAC spoofing and flooding attacks. However, ARP poisoning and other attacks remain possible

Ways Around 802.1X Authentication

- An attacker may place a hub or switch between the authenticated host and the authenticating switch. After authentication, the authenticated host can be disconnected without losing the electrical connection to the authenticating switch and another host, configured with same MAC address, be used in the network.
- Authentication can also be used between switches to form a trusted inner network. This can be used to prevent attacks where a host acts as a switch.

5. Access Control Lists (ACL)

Access Control Lists (ACLs) are not part of the Ethernet specification. Switch vendors have added various types of capabilities by themselves.

The Ethernet frame does not have many features:

For a simple Ethernet frame ACL the usable attributes are the sender’s or receiver’s MAC address or the Ethertype field. Access can be limited based on MAC addresses, but several service specific ACLs are commonly implemented.

Service Specific Access Control Lists (ACL)

1. **Port Security:** Allows the administrator limit access to a port in a switch, based on the number of MAC addresses. Blocks MAC flooding. Port security may also be set to block a port from existing MAC addresses.
2. **Packet storm protection:** Limits the number of frames per time unit a switch will allow from a port. Prevents MAC flooding attacks if the limit is low enough but is more commonly used to guard against packet storms.
3. **BPDU guard:** Blocks all STP messages from a port and can be used to designate a port that will not form a part of the mesh network.

6. Control and Management Plane Overload Protection:

Control and management planes can be protected from overload by limiting the amount of traffic on these planes.

Control Plane Policing (CPP) achieves this by providing a set of filters, based on rate limiting methods and addresses to prevent the overloading of control plane functionalities.

The filters are configured to allow only a certain amount of control and management plane data packets to reach the CPU – everything else is blocked before reaching the CPU level.

Protects against intentional CPU exhaustion attacks, with the drawback that during an attack legitimate messages are also lost.

7. Centrally Managed LAN Security

Several approaches to collecting information from a LAN to a central point and using this to manage security have been presented by the research community in recent years.

- **SANE**
- **Ethane**
- **OpenFlow**

C. Secure Protocols

Access controls limit the availability of targets to attackers. The targets can also be made harder to reach by adding security features to protocols and protocol implementations.

1. Encryption and Integrity Verification
2. Securing Address Resolution Protocol
3. Control and Management Plane Logical Protection
4. Replay Protection

1. Encryption and Integrity Verification

- Cryptography can solve integrity and confidentiality requirements. IEEE 802.1AE MACsec forms encrypted connections between hosts and switches, protecting confidentiality and integrity of the content in the frames.
- Deployment requires software installation and configuring authentication for each participating network entity.
- MACsec uses 802.1X authentication information as its basis. MACsec provides protection against intruders to the network, preventing reading and modification of data frames.

2. Securing Address Resolution Protocol

- ARP creates a major vulnerability in the Ethernet architecture. Information gained by DHCP snooping can be used to prevent ARP spoofing attacks, by tying MAC addresses to their corresponding IP addresses and ports.
- S-ARP can be used, which adds an authentication field to ARP messages and provides a corresponding key management structure, that uses cryptographic name space binding, which extends MACsec's reach to endpoint to endpoint and multicast protection.

3. Control and Management Plane Logical Protection

Protecting the higher functions in a switch from misuse relies on controlling the access to the switch. Control plane functions have to be connected to the user plane and can be protected.

4. Replay Protection

The basic Ethernet frame has no protection against replay attacks, leaving it to higher layers. MACsec and many higher layer protocols include features to thwart replay.

D. Security Monitoring.

- Up until now we have seen security techniques that are proactive.
- Active participation from external systems or human interactions are not needed.
- To enhance the security of the network we need active technologies;
- Security Monitoring:
    1. Ethernet Firewall and Deep Packet Inspection.
    2. Intrusion Detection (IDS) and Intrusion Prevention Systems (IPS).
    3. Planning, Configuration and Administration.

1. Ethernet Firewall and Deep Packet Inspection.

- **Firewalls** are more complex cases of **Access Control Lists (ACLs).**
- Ethernet Firewall is not significant as current Firewall products can operate on all network layers.
- It is basically used to limit the traffic in the network segments.
- **How does a firewall work?**
  - Firewalls scan packets for malicious code or attack vectors that have already been identified as established threats.
  - Firewalls can also employ **deep packet inspection (DPI)** and application layer session recreation for inspection purposes.

Contd...

- **Deep Packet Inspection**: Analysing the contents of the packet at the application level, beyond the header.
- It is often used to baseline application behavior, analyze network usage, troubleshoot network performance, ensure that data is in the correct format, to check for malicious code, eavesdropping, and internet censorship.
- DPI can be used to protect the control management planes, of protocols like ARP and DHCP which are relevant to ethernet.
- Shallow Packet Inspection: Analysing the packet by just looking at the header.

2. Intrusion Detection and Prevention Systems.

- IDS and IPS uses DPI to identify network attacks, from a signature library of attacks.
- Access to the network is gained through:
  - Placing an IDS/IPS device between 2 endpoints.
  - Using port mirroring feature to monitor traffic from a switch. It copies traffic between selected ports to a listening port, where the monitoring device is located.
- It is also possible to have the monitoring devices in a separate network from the monitored/protected network.

Contd...

- The **MAC address notification** can send a Simple Network Management Protocol (**SNMP**) trap message when a host moves in the network.
- SNMP Management Information Base (**MIB**) definitions can be used for IDS purposes - Remote Network Monitoring MIB (**RMON**) and its switch extensions (**SMON**)
- Frames with known expected behaviour can be injected to the network and the results can be monitored to detect **ARP spoofing attacks**.

Firewall vs Intrusion Detection System.

Firewall

- Traditional network firewall uses a static set of rules to permit or deny network connections.
- It implicitly prevents intrusions, assuming an appropriate set of rules have been defined.
- Firewalls limit access between networks to prevent intrusion and do not signal an attack from inside the network.

Intrusion Detection System

- An IDS describes a suspected intrusion once it has taken place and signals an alarm.
- It also watches for attacks that originate from within a system.
- This is achieved by examining network communications, identifying heuristics and patterns of common computer attacks, and taking action to alert operators.

3. Planning, Configuration, and Administration.

- Good network administration practices play a very important role in the security aspects of an Ethernet network.
- Most of the above mentioned solutions require configuration and constant adjustments with respect to changes in the network topology.
- Administrator can configure the information about trunk networks into the switches.
- By limiting the control plane functionality and data flow, and by separating management information dedicated to a Virtual LAN enhances the security of the network.
- The duties of the network administrator include active network scanning, probing, and testing to detect vulnerabilities.

V. RESEARCH DIRECTIONS

V. RESEARCH DIRECTIONS

- Ethernet is growing technology and security is most essential.
- Operators are running ethernet edge-to-edge and inter-operator Ethernet segment is quite possible.
- Cloud Computing shows that data centers are becoming larger and have an increasing no. of independent and potentially hostile tenants.
- Stuxnet brought out need for protecting legacy networks especially as many industrial SCADA (Supervisory Control And Data Acquisition) and automation networks contain old hardware and software that can't be easily upgraded.

So we shall look at potential / possible solutions

A) New and Existing Areas of use
B) Architectural Issues
C) New Vulnerabilities and Threats

A) New and Existing Areas of use

- Transition from Ethernet segment to VLAN technology, Improved security and traffic management yet not most secure separator.

1. CAM Table Overflow / MAC Attack
2. ARP attack
3. Switch Spoofing / VLAN Hopping
4. Double Tagging / Double Encapsulation
5. VLAN query protocol Attack
6 .Cisco Discovery Protocol (CDP) Attack
7. Multicast Brute-Force Attack
8. Random Frame-stress Attack
9. Private VLAN Attack
10. Spanning Tree Protocol (STP) Attacks

A) New and Existing Areas of use

- Legacy automation systems which use Ethernet for supervisory control and monitoring even for real-time needs.
- These are some decades back systems and legacy equipment might have also designed caring only the purpose not the security.
- These equipment could also be sensitive to various modern features like traffic volumes or large data frames.
- These systems are often connected to Ethernet directly or indirectly which requires protection from several present-day attacks.

B) Architectural Issues

- Key issue is with data plane (Forwarding Plane) and control plane as they are mixed which compromises the authenticity of the participants.
- Role of control plane is to take routing decisions and role of data plane is to forward frames based on control plane.

Several Possible solutions are

1) Software Defined Networking (SDA)
2) Removing Broadcast
3) Cryptographically Generated Addresses (CGA)

B. 1) Software Defined Networking

- SDN is based on the concept of separating data plane and control plane for traffic routing which makes it more powerful to customize networks on the fly.
- SDN provides new level of programmability and abstraction to Network Layer which helps in automating the networks.
- OpenFlow have potential to unify the switches which allows implementing a centralize command and control into a central node LAN as SANE and ethane have demonstrated.

B. 2) Removing Broadcasts

- Security would be considerably improved if the broadcasts could be removed from the Ethernet.
- Distributed Hash Tables (DHT) have been proposed as a replacement solution for locating a host.
- Re-engineering the control plane is an another solution.
- Motivation for removing broadcasts is usually to extend the size of the Ethernet segment, while avoiding moving to IP layer.

B. 3) Cryptographically Generated Addresses (CGA)

- It's an IPv6 address that has a host identifier computed from cryptographic hash function.
- Least significant 64 bits of the 128 bit IPv6 address are replaced with cryptographic hash of the public key. The messages are signed with corresponding private key. This doesn't require any PKI (Public Key Infrastructure). Valid CGA's can be generated by any sender.
- Ethernet addresses with 46 or 47 bits of significance could be created by hashing from public keys of a host.
- These addresses would be compatible with legacy equipment, but other hosts could verify the identity of an endpoint when needed.
- Participating equipment could use its public or private key pair to sign control layer frames, thus enabling switches to monitor the identities of hosts.

B. 3) Cryptographically Generated Addresses (CGA)

- CGA parameters consists of *modifier, subnetPrefix, collCount, publicKey, extFields.* An additional parameter *Sec* determines the strength of the CGA's against brute-force attacks.
- In order for an attacker to make a client believe it received a valid message from CGA's not owned by attackers, they must find a hash collision for the relevant bits by brute-force attack. Attacker can generate the same CGA as the target CGA only if they finds the set of all CGA parameters involved.
- It is very unlikely that 3-address collisions occur. collCount is limited to the range from 0 to 2 in order to prevent attacker trying all different values.

C. New Vulnerabilities and Threats

- Literature surveyed indicates that findings have been mostly found by a random process and reported as individual cases.
- Thus unrecorded weaknesses could exist in the current architecture and in the implementation of technologies.
- New technologies like TRILL (Transparent Interconnection of Lots of Links) and SDN (Software Defined Networking) improves existing security but introduces new vulnerabilities.
- Though TRILL problem statement states that they should not introduce new vulnerabilities their main focus of work is on path efficiency but not on security.
- SDN's have potential to be very complex systems and thus they have more room for vulnerabilities.

VI SUMMARY

Summary

- The major strengths of Ethernet are its simplicity and zero configurability.
- Ethernet can be secured to a reasonably high level by administering all switches, hosts, and users centrally and applying cryptographic methods, which means the loss of simplicity and zero configurability
- Existing solutions are granular and don’t provide protection against the misuse from authorized users
- A reasonable level of protection can be reached by administering the switches and maintaining separation of the switching nodes and leaf nodes which is equivalent to the protection we get by replacing the switches with the IP routers, except for ARP broadcasts which leave the system vulnerable to misuse

Contd...

- Another potential solution is to select a source of trust and leverage this to authenticate and authorize known entities.
- This could require changes to end nodes and protocols but could be done without human intervention and would save the zero-configurability aspect, while losing some of the simplicity.
- A third option would be to remove the ARP broadcasts, which would solve a major security issue while maintaining the desirable aspects of Ethernet.

Thank You