Chapter 8: Securing Switched LANs

Chapter goals:
- Understand security vulnerabilities in switched LANs
- Learn how to secure switches
- Understand VLANs (Virtual LANs) and their security
Chapter Roadmap

- Securing Switched Ethernet LANs
  - Securing the MAC self-learning process
  - Securing DHCP and ARP
  - Securing the spanning tree protocol
- VLANs
  - Securing VLANs

Switched Ethernet – Reminder

- Switches build a spanning tree to avoid loops
  - Root bridge, root ports, forwarding/blocking ports
- Switches self-learn mapping between MAC addresses and ports, by looking at MAC source addresses
  - They build a CAM (Content Addressable Memory) forwarding table
  - When a MAC address is not in the table, the switch floods the received frame
- Switches are transparent to routers and hosts
  - A set of interconnected switches form a LAN
  - For IP, this LAN is a subnet
- IP addresses are mapped on MAC addresses by the ARP protocol
- Don’t confuse MAC forwarding tables and ARP tables!
  - In which devices do we find them?
  - What do they contain?
Chapter Roadmap

- Securing Switched Ethernet LANs
  - Securing the MAC self-learning process
  - Securing DHCP and ARP
  - Securing the spanning tree protocol
- VLANs
  - Securing VLANs

MAC spoofing attack

- MAC spoofing
  - B sends a frame with source MAC address C
- Switch « learns » that C is reachable via interface 2!
  - B can now see the frames destined for C
- Some switches will overwrite C’s entry
  - C cannot see frames any longer!
  - DoS attack!
MAC flooding attack

- B generates a large number of frames with spoofed MAC addresses (X, Y, …)
- Switch (CAM) table will overflow
  - Capacity of table may vary from a few thousands to more than 100,000 entries
- Older entries will be removed from table
  - Switch now floods frames on all interfaces for removed (unknown) MAC addresses
- Usually one table per switch, not one per VLAN
  - All VLANs impacted

Detecting/preventing MAC spoofing and flooding attacks

- MAC address activity notification
  - Many switches can be configured to warn about frequent MAC address changes
- Port security
  - Associate a few MAC addresses with every port (Why not just 1?)
  - Only for access ports, not inter-switch (trunk) ports
  - Can be static or dynamic
  - Violations are notified
- Unicast flooding protection
  - Limited flooding is normal
  - But continuous flooding is not!
    - Alert!
- DHCP snooping
  - See next slides
Chapter Roadmap

- Securing Switched Ethernet LANs
  - Securing the MAC self-learning process
  - Securing DHCP and ARP
  - Securing the spanning tree protocol
- VLANs
  - Securing VLANs

Attack against DHCP

- DHCP is not a datalink protocol (it runs over UDP), but solutions to DHCP attacks are also useful to thwart layer 2 attacks
- DHCP reminder:
  - Client discovers server(s): broadcast packet
  - DHCP server broadcasts an offer
  - Client broadcasts interest in (one) offer
  - DHCP server acks
- Client gets IP address and mask, but also default router and DNS servers!
  - A (quick) rogue DHCP server can easily redirect client to a fake router and/or fake DNS server
- Solution: DHCP snooping
  - Monitor and restrict DHCP operations on a (V)LAN
  - A host has no reason to send DHCP offers (nor ACKs)!
  - Don’t let DHCP offers enter the switch on “untrusted” ports
    - Need access control above layer 2!
- In addition:
  - DHCP snooping allows to learn IP-to-MAC bindings
    - Switch learns IP address assigned to client and knows client MAC address (present in request)
DHCP snooping to thwart IP/MAC spoofing attacks

IP spoofing
- Spoofed source IP is $IP_C$
- Source: B
- Dest: A
- A  B  IP packet
- B: attacker

MAC spoofing
- Spoofed MAC source: C
- Source IP is $IP_A$
- Dest: A
- A  C  IP packet
- B: attacker

- DHCP snooping: discard frames with invalid <IP, MAC> source address pairs

ARP spoofing/poisoning

- ARP reminder:
  - ARP request: MAC broadcast frame searching for an IP address
  - ARP reply: unicast
  - Gratuitous ARP:
    - Reply sent without prior request
    - Useful when MAC address changes

- ARP spoofing/poisoning
  - Sends gratuitous ARP with wrong IP-to-MAC mapping: attacker’s MAC address (MAC$_B$) mapped to victim’s IP address ($IP_C$)
  - All traffic to $C$ is actually sent to $B$. Then $B$ can silently forward it to $C$ after sniffing: Man-in-the-Middle attack
  - Note: $B$ needs a second ARP spoofing attack to also sniff the return traffic

- Solutions:
  - Ignore gratuitous ARP
  - Use an IDS to track changes in IP-to-MAC mappings
  - Rely on DHCP snooping
Chapter Roadmap

- Securing Switched Ethernet LANs
  - Securing the MAC self-learning process
  - Securing DHCP and ARP
  - Securing the spanning tree protocol
- VLANs
  - Securing VLANs

Attacking the Spanning Tree Protocol

- Taking over the root bridge
  - Attacker sends BPDUs with smallest switch id
  - Becomes root bridge
  - If attacker is dual-homed, some traffic can be redirected to cross attacker’s device
- BPDU flooding
  - DoS attack

- Solution:
  - Distinguish trunk ports from access ports
  - Discard BPDUs on access ports
    - End stations are not supposed to send BPDUs!
**Chapter Roadmap**

- Securing Switched Ethernet LANs
  - Securing the MAC self-learning process
  - Securing DHCP and ARP
  - Securing the spanning tree protocol
- **VLANs**
  - Securing VLANs

**VLANs**

- Switches have been extended by adding virtualization (VLAN switch)
- A VLAN switch emulates multiple, independent switches
- We will review
  - The motivation for VLANs
  - Their technology
  - VLANs spanning multiple physical switches
  - The need for an extra field in the frame (VLAN tag)
  - Security in VLANs
**VLANs: motivation**

**Human resource management:**
- CS user moves office to EE area, while staying in the CS department. How to keep user connected to CS switch?
- CS user becomes part of EE department, but wants to keep his/her office. How to connect user to EE switch?

**Performance/security issues:**
- LAN = single broadcast domain
- Issue: all layer-2 broadcast traffic crosses entire LAN (e.g., ARP, DHCP, flooding due to unknown destination MAC address)

**Cost:**
- Many lowest level switches may have only few ports in use

---

**VLANs**

**Virtual Local Area Network**

Switch(es) supporting VLAN capabilities can be configured to define multiple virtual LANs over single physical LAN infrastructure

**Port-based VLAN:** switch ports grouped (by switch management software) so that single physical switch …

... operates as multiple virtual switches
Port-based VLAN

- traffic isolation:
  - frames to/from ports 1-8 can only reach ports 1-8
  - broadcast traffic remains on its VLAN

- dynamic membership:
  - ports can be dynamically assigned among VLANs
  - update done by software when user changes location

Address-based VLAN

- easier management:
  - VLANs are based on MAC addresses of endpoints, rather than switch port
  - user (i.e. MAC address) can move from one port to another without changing VLAN

- dynamic membership:
  - MAC addresses can be reassigned among VLANs

- VLANs can also be based on IP addresses of endpoints (e.g. IP prefix/subnet defining a VLAN)
VLANs: motivation

- VLANs address issues such as scalability, security, and network management.
- Network architects set up VLANs to provide network segmentation over a shared physical infrastructure:
  - Traffic cannot jump from one VLAN to another, and broadcast LAN frames stay on their VLAN.
- VLANs can be used to partition a network into several distinctive segments, e.g.:
  - Voice over IP
  - Network management
  - Storage area network (SAN)
  - Guest Internet access
  - Demilitarized zone (DMZ)
- A common infrastructure shared by VLANs can provide a measure of security with great flexibility for a comparatively low cost.
- Quality of service schemes can optimize traffic on inter-switch (trunk) links for real-time (e.g. VoIP) or low-latency requirements (e.g. SAN).

Forwarding between VLANs

- *forwarding between VLANs* always done via routing (just as with separate switches):
  - figure shows interconnection through a separate router.
- In practice, vendors sell combined switches plus routers (so-called layer 3 switches).

© From Computer Networking, by Kurose & Ross
VLANs spanning multiple switches

- how to interconnect multiple physical switches with devices on several VLANs?
- could connect the devices from the same VLAN through a dedicated link between the 2 switches
  - but would require one inter-switch link per VLAN!

VLANs spanning multiple switches

- trunk link/port: carries frames in VLANs defined over multiple physical switches
  - frames forwarded within VLAN between switches can’t be vanilla 802.1 frames (must carry VLAN ID info)
  - 802.1Q protocol adds/removes additional header fields for frames forwarded between trunk ports
IEEE 802.1Q VLAN frame format

- When the field following the 2 MAC addresses is 0x8100 (> 1500), it's a 802.1Q frame
- 3-bit priority field is used to provide QoS
- When a frame has no tag on a trunk link, there is a native/default VLAN id (= 1) which the frame is considered to be associated with

Assigning a VLAN id to a host

- If a host NIC sends an untagged frame, the frame will be associated with the VLAN corresponding to the incoming port (in port-based VLAN) or to the source MAC address (in address-based VLAN)
  - If the frame crosses a trunk link, the tag is added
    - unless the frame is associated with the native/default VLAN and the trunk port is configured to support the native VLAN
- A host NIC could also send tagged frames
  - e.g., an IP phone sending frames on the “VoIP VLAN”
  - VLAN ids can be assigned manually to hosts or assigned dynamically (e.g. thanks to IEEE 802.1x after host authentication with an AAA server)
Consider a Layer-2 VPN scenario
- Provider’s network creates one VLAN per customer
- Customer may still define multiple VLANs within customer’s multi-site network
- Customers’ VLAN frames carried through provider’s VLAN:
  - 802.1Q frames will be double tagged in the provider’s network
  - Outer VLAN id = Provider’s VLAN id
  - Inner VLAN id = Customer’s VLAN id

VLANs and spanning trees
- When several VLANs are deployed, it is possible to build one or several spanning trees:
  - Per-VLAN spanning tree (PVST)
  - Multiple spanning tree protocol (MSTP):
    - one spanning tree per group of VLANs
Chapter Roadmap

- Securing Switched Ethernet LANs
  - Securing the MAC self-learning process
  - Securing DHCP and ARP
  - Securing the spanning tree protocol
- VLANs
  - Securing VLANs

VLANs – A security plus

- Layer-2 broadcast frames remain on their VLAN
  - ARP, DHCP, …
- Frames cannot jump from one VLAN to another without passing through a layer-3 device
  - and high-end layer-3 switches can even perform firewall functions without using an external firewall device
- This traffic isolation is a security plus, unless there are misconfigurations and incorrect cabling
VLANs and firewalls

- The same physical switch could be used for the internal network and the DMZ, with a dedicated DMZ VLAN.
- But usually considered preferable to keep devices at different security levels isolated on physically separate switches.

VLANs – Trunk versus access ports

- Non trunk ports should be configured as access ports to avoid switch spoofing attacks.
  - In a switch spoofing attack, an attacking host imitates a trunking switch.
- On access ports the switch will discard:
  - Tagging and trunking protocols used to manage VLANs:
    - e.g., CISCO's Dynamic Trunking Protocol (DTP) used to negotiate trunking on a link and to configure the VLANs in a multi-switch network.
    - but also BPDUs for example.
- Also:
  - disable unused switch ports and create a VLAN to collect disabled switch ports.
VLAN hopping - Attacking the VLAN tag stack

VLAN hopping

- Frame hops from VLAN 1 to VLAN 2!
- Victim on VLAN 2 can receive killer packets from an attacker on VLAN 1 without crossing any router (and possible filter)!

Solutions

- Don't assign native VLAN to any access port
- Force all traffic on trunk to always carry a tag, even the native one
- Assign another unused number to the native VLAN

Summary

Securing Switched LANs

- Securing the MAC self-learning process
  - MAC spoofing
  - MAC flooding
- Securing DHCP and ARP
  - Rogue DHCP server
  - ARP spoofing/poisoning
- Securing the spanning tree protocol
- IEEE 802.1x can also be used with Switched LANs
  - was initially designed in this context

VLANs

- VLAN as a network segmentation mechanism
- A security plus

Securing VLANs

- Switch spoofing
- VLAN hopping