Switch and Link-level Security

Kiravuo, et.al: A Survey of Ethernet LAN Security
IEEE Communication Surveys & Tutorials

DNS security

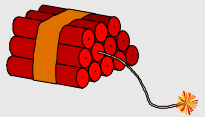
- Replies from DNS servers are not authenticated
  - Response can come from anyone
  - Tool to become a MITM
- DNSsec – used by the .se domain
  - All records are signed (certificates)
  - Everyone can verify authenticity
  - Future standard, not universally used yet
- DNS over HTTPS (DoH) RFC 8484
  - DNS request is encrypted using HTTPS
  - Prevents MITM to fake DNS replies
  - The name server must support it
  - Windows 10 can support DoH (off by default)
  - Many web browsers also support DoH if the system is not DoH enabled (in settings)
- DNS over TLS (DoT)
  - Competing standard…

TABLE I
TIMELINE OF THE MOST SIGNIFICANT EVENTS TO SECURE THE DNS PROTOCOL

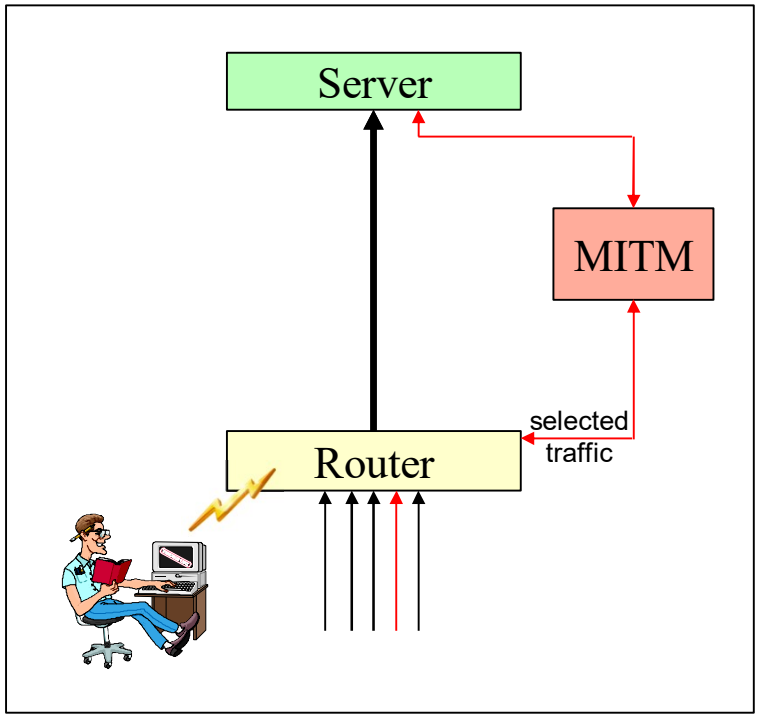
Month	Year	Event
Nov	1987	DNS current protocol defined (RFC 1034, 1035)
Oct	1990	Bellovin's system break-ins through DNS
Jan	1997	●DNSSEC first introduction (RFC 2065)
Sep	1999	SPKI/SDSI theory and requirements (RFC 2692, 2693)
Oct	2001	Zooko's triangle conjecture
Mar	2005	DNSSEC upgrades (RFC 4033, 4034, 4035)
Mar	2008	NSEC3 Auth. Denial of Existence (RFC 5011)
Jul	2008	Kaminsky's attack
Jun	2009	DNSCurve implementation by D.J. Bernstein
Dec	2011	DNSCrypt protocol first version
Jul	2012	Analysis about Internet censorship in China
Oct	2012	Namecoin/DotBit launch
Mar	2014	NSA surveillance and attack plans revealed
May	2014	Pervasive monitoring is an attack (RFC 7258)
Sep	2014	IETF DPRIVE Working Group established
Oct	2014	GNU name system
Aug	2015	●DNS privacy considerations (RFC 7626)
Mar	2016	QNAME minimization (RFC 7816)
May	2016	DNS-over-TLS (DoT) (RFC 7858)
Aug	2017	Stubby (DoT client) source repository released
Sep	2017	IETF DoH Working Group established
Oct	2017	Paged domain name system
Jun	2018	Oblivious DNS
Oct	2018	●DNS-over-HTTPS (DoH) (RFC 8484)
Jan	2019	Google launch a DoT service
Jun	2019	Google launches its Public DoH service
Feb	2020	●Firefox moves to DoH for all US users
Jan	2021	●Microsoft Windows 10 21H1 will include DoH
Mar	2021	NSA tips on encrypted DNS resolvers

https://ieeexplore.ieee.org/document/9520679

Routing protocol attacks



- RIP – routing information protocol:
  - Routers broadcast their routes regularly
  - Relatively easy to send false RIP packets
  - Hosts and routers will probably believe them
- OSPF requires passwords/keys to update routes
  - The most widely used routing protocol in larger networks (inside ISP/AS networks)
  - All messages should be authenticated (neighbor authentication)
  - Keys can be per link or for a larger area
- BGP – Border Gateway Protocol
  - Interconnects all ISP networks (AS) in the Internet
  - (next page)

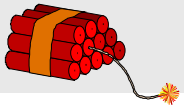


Securing BGP

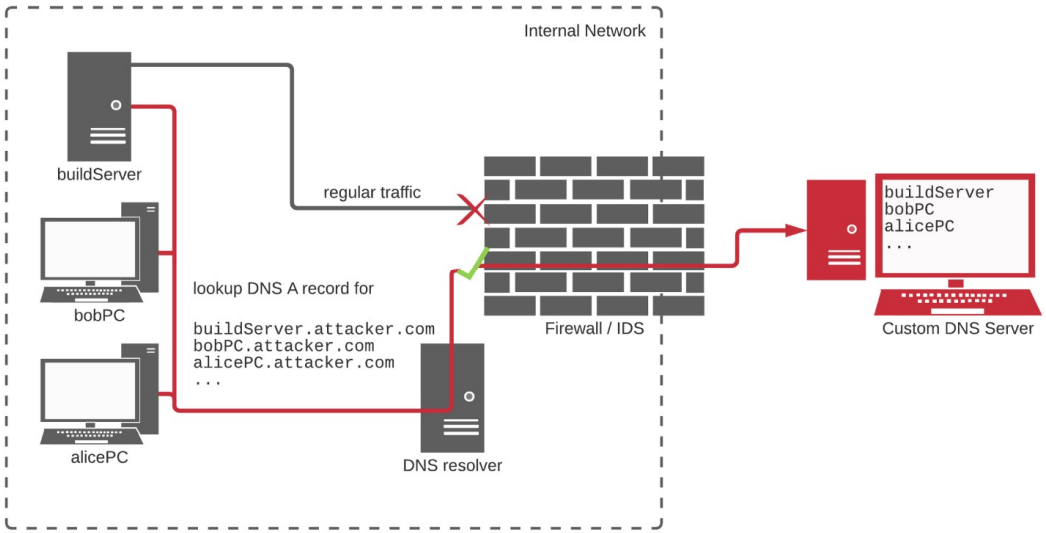
RFC 7454 – Best practices for operators:

- Use ACL lists: Routers should only talk to pre-defined IP addresses
  - TCP port 179
- Should use TCP Authentication Option (RFC 5925) or IPsec
  - A TCP option negotiated at connection time
  - Keys are delivered out-of-band and can be changed at any time
  - MD5 keyed hashes most common
- TTL security should be used
  - Send updates between routers with TTL=255 when possible
  - Neighboring routers know what to expect (e.g. 254)
- Always check that received route updates are valid
  - Origin validation
  - And know who is allowed to update what network paths

Using DNS to phone home



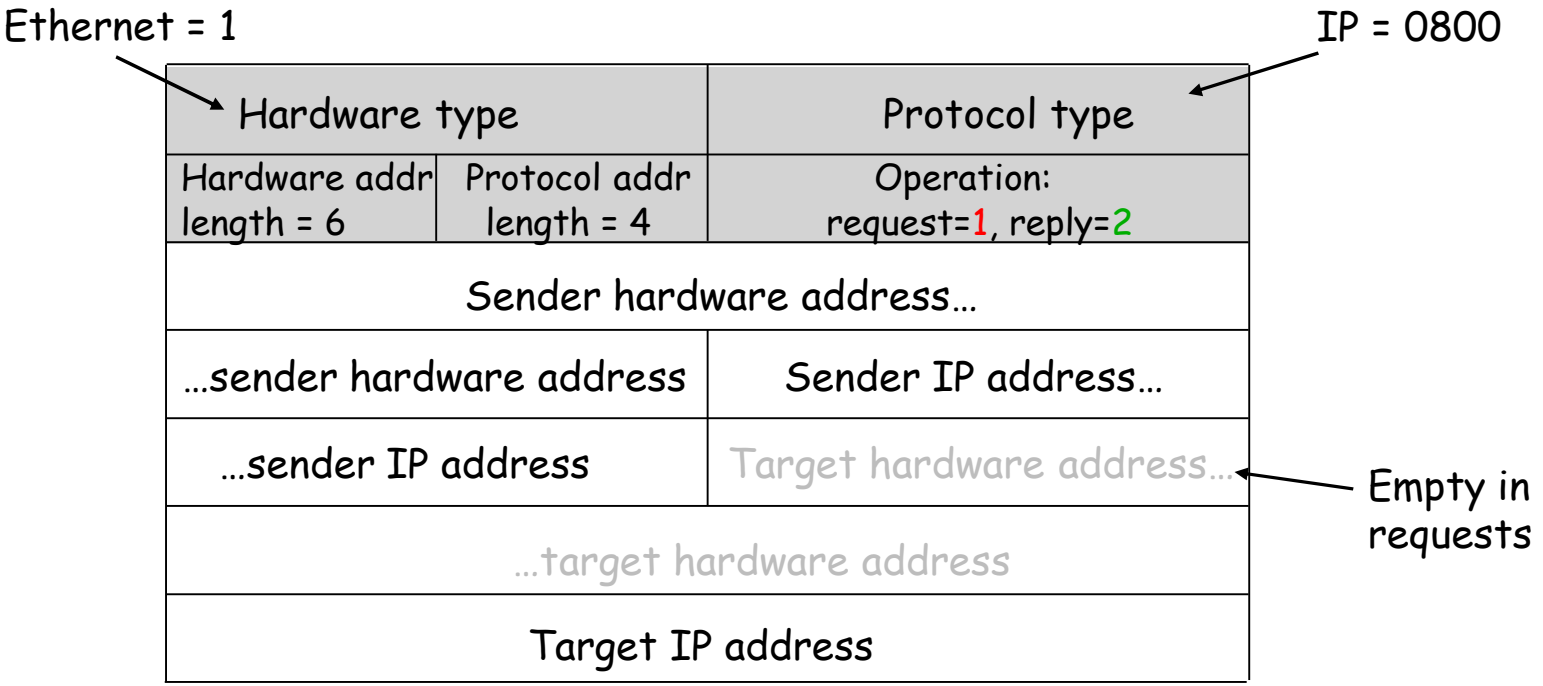
- A way for malware to phone home and tell that they are ready to receive commands, is to do a DNS lookup to a specific server
- Request can include name of internal server
- Reply can be a message for the malware



https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610

ARP – Address Resolution Protocol

ARP message format



ARP – Address Resolution Protocol

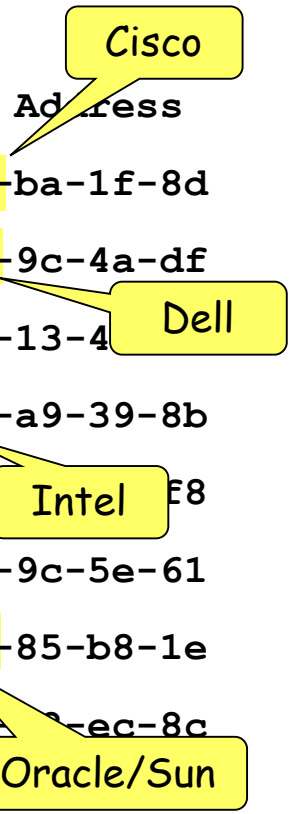
- RFC 826 – November 1982
  - No security!
- Questions are broadcasted on the network
  - "Who has IP address nnn.nnn.nnn.nnn"?
  - Both questions and replies are recorded by everyone
- Each node manages an ARP table (cache)
  - Displayed with "**arp -a**" command
- Entries can be static (i.e. manually configured) or dynamic
- Dynamic entries are the default, they have a TTL:
  - If used: max 10 minutes
  - If not used: 0,5 minutes
  - Windows: combines ARP with IPv6 neighbor discovery – more complex*
- Local attackers can scan hosts with ARP
  - Good: only works on the local subnet
  - Alternative to SYN/FIN/… and ICMP Echo scans
    ARP: "Who has IP address 10.17.221.100"?
- Or use IPv6 Neighbor discovery (required in IPv6)
- Or Windows LLTD (Link Layer Topology Discovery protocol) which returns MAC address, IPv4 and IPv6 addresses and host name

* https://support.microsoft.com/kb/949589/en-us

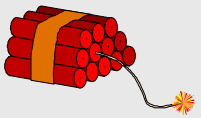
MAC addresses show hardware vendor

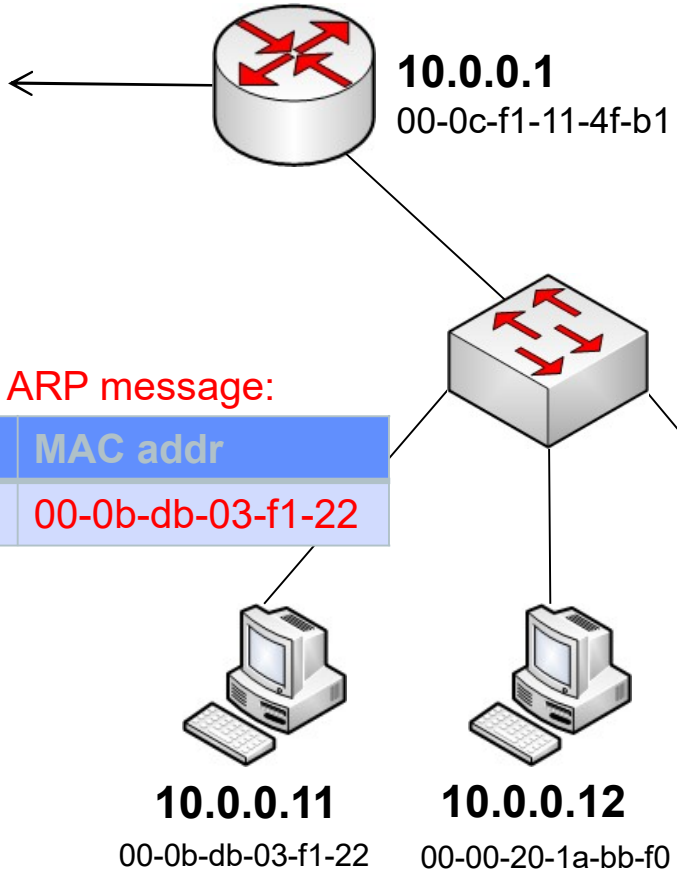
> arp -a

```
Interface: 129.16.20.103 --- 0x2
  Internet Address      Physical Address      Type
  129.16.1.4            6c-9c-ed-ba-1f-8d     dynamic
  129.16.20.125         00-0b-db-9c-4a-df     dynamic
  129.16.20.213         00-c0-9f-13-4         dynamic
  129.16.20.244         00-0c-f1-a9-39-8b     dynamic
  129.16.20.245         08-00-20              dynamic
  129.16.20.250         08-00-20-9c-5e-61     dynamic
  129.16.21.57          08-00-20-85-b8-1e     dynamic
  129.16.21.59          08-00-20-             dynamic
```



ARP cache poisoning – MITM problem!





Countermeasure: use static address translations for important servers and gateways:

arp -s 10.0.0.1 00-0c-f1-11-4f-b1

Internal ARP cache:

IP addr	MAC addr
10.0.0.12	00-00-20-1a-bb-f0
10.0.0.1	~~00-0c-f1-11-4f-b1~~ 00-0b-db-03-f1-22

Other countermeasures

- Create smaller subnets (smaller broadcast domains)
- Encrypt traffic (packets of no use to attackers)
  - Also makes life harder for IDS systems
- ARP alert / Dynamic ARP Inspection
  - IDS should check all ARP requests and replies (together with DHCP inspection)
  - Host-based or network based
- Antidote "patch" (Linux):
  - Try old MAC address first before new is accepted
  - When real destination machine is down or unknown, attack succeeds…
- Accept only the first reply (some Unix systems)
  - Ignores subsequent ARP requests/replies
  - Assumes the first entry was ok
  - But sooner or later entry times out...
- Secure ARP (S-ARP)
  - Work in progress where CA issues digitally signed ARP messages

Security functions in switches

Switch features at a glance

Netgear GS408 EPP
2,000 SEK

- Browser-based graphical user interface (GUI)
- 16 Gbps non-blocking fabric (bandwidth) with <2.7 µs latency
- 192KB packet buffer memory (dynamically shared across used ports)
- 4K Media Access Control (MAC) addresses
- Security
  - Broadcast, multicast and unknown unicast storm control (DoS prevention)
  - If broadcast traffic on any port exceeds the threshold, the switch temporarily blocks (discards) it
- Quality of Service (QoS)
  - Port-based rate limiting (ingress and egress)
  - 4 Priority queues with Weighted Round Robin (WRR) priority queuing
- 64 VLANs
  - IEEE 802.1Q VLAN tagging
  - Port-based VLANs (physical)

More expensive switches

Cisco 300 Series Switches

15,000 SEK

Security	
Secure Shell (SSH) Protocol	SSH secures Telnet traffic to and from the switch
Secure Sockets Layer (SSL)	SSL support: Encrypts all HTTPS traffic, allowing highly secure access to the browser-based management GUI in the switch
IEEE 802.1X (Authenticator role)	802.1X: RADIUS authentication and accounting, MD5 hash; guest VLAN; unauthenticated VLAN, single/multiple host mode and single/multiple sessions Supports time-based 802.1X Dynamic VLAN assignment
Layer 3 isolation*	Allow/disallow routing between IP subnets or directly connected IP networks
Layer 2 isolation Private VLAN Edge (PVE) with community VLAN	PVE (also known as protected ports) provides Layer 2 isolation between devices in the same VLAN, supports multiple uplinks
Port security	Locks MAC addresses to ports, and limits the number of learned MAC addresses
RADIUS/TACACS+	Supports RADIUS and TACACS authentication. Switch functions as a client
Storm control	Broadcast, multicast, and unknown unicast
DoS prevention	DoS attack prevention
Congestion avoidance	A TCP congestion avoidance algorithm is required to minimize and prevent global TCP loss synchronization.
ACLs	Support for up to 512 rules Drop or rate limit based on source and destination MAC, VLAN ID or IP address, protocol, port, differentiated services code point (DSCP)/IP precedence, TCP/ UDP source and destination ports, 802.1p priority, Ethernet type, Internet Control Message Protocol (ICMP) packets, IGMP packets, TCP flag

Managed Switches

- Managed switches have an IP address for remote management
- Configuration can be done via:
  - GUI using HTTPS
  - Telnet: login with username/password, uses cleartext…
  - SSH: encrypted traffic supported by most newer switches
- Password guessing attacks possible
- Cisco switches exchange information via CDP: ”Cisco Discovery Protocol”
  - Simplifies management
  - Broadcasts info on link level: IP address, version, platform, capabilities, VLAN, …
  - Disable CDP unless really needed!

Cisco Security Advisory

Cisco Nexus 9000 Series Fabric Switches Application Centric Infrastructure Mode Default SSH Key Vulnerability

Advisory ID:	cisco-sa-20190501-nexus9k-sshkey	CVE-2019-1804
First Published:	2019 May 1 16:00 GMT	CWE-310
Last Updated:	2019 May 2 17:09 GMT	
Version 1.1:	Interim	
Workarounds:	No workarounds available	
Cisco Bug IDs:	CSCvo80686	
CVSS Score:	Base 9.8	

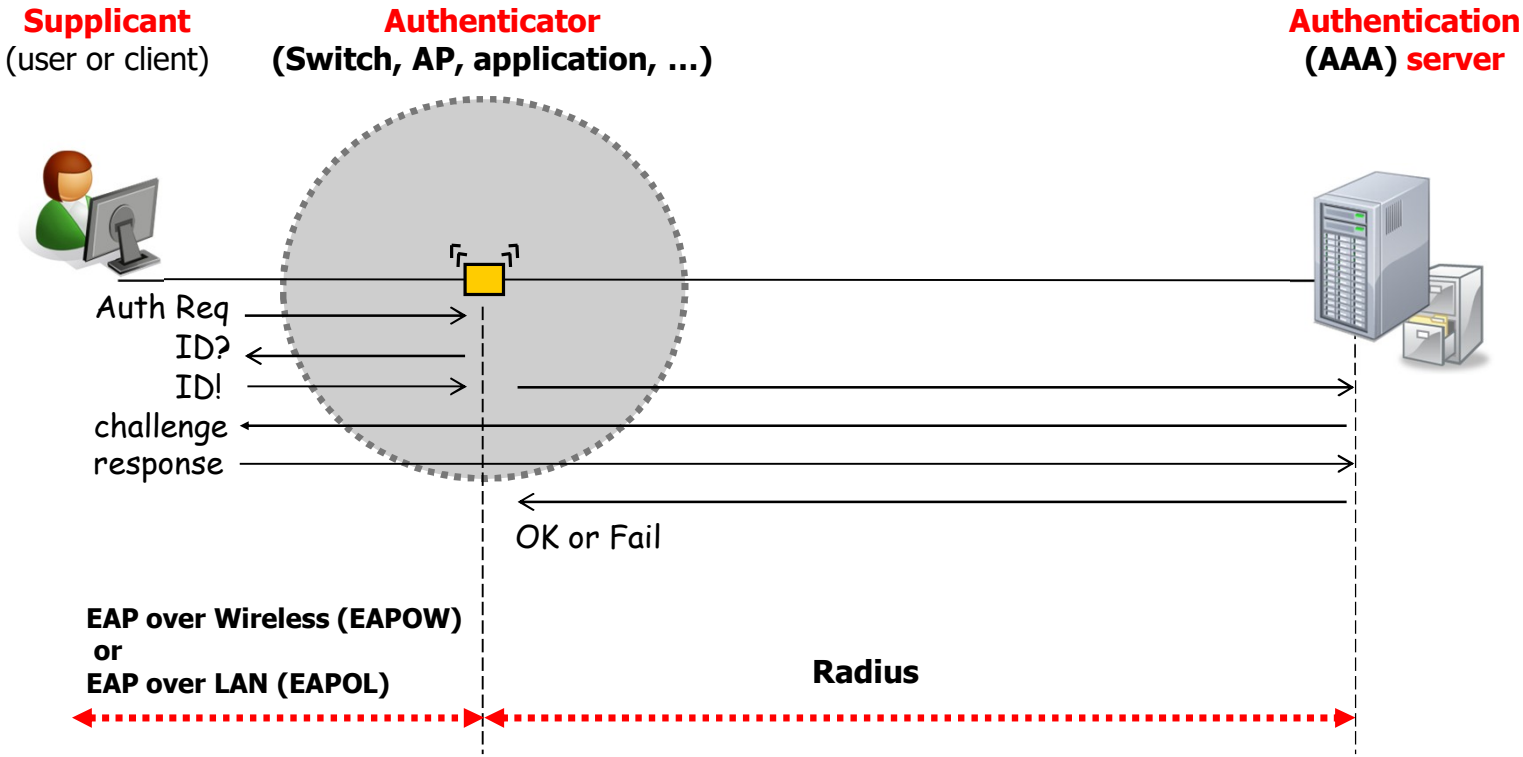
Summary

A vulnerability in the SSH key management for the Cisco Nexus 9000 Series Application Centric Infrastructure (ACI) Mode Switch Software could allow an unauthenticated, remote attacker to connect to the affected system with the privileges of the *root* user.

The vulnerability is due to the presence of a default SSH key pair that is present in all devices. An attacker could exploit this vulnerability by opening an SSH connection via IPv6 to a targeted device using the extracted key materials. An exploit could allow the attacker to access the system with the privileges of the *root* user. This vulnerability is only exploitable over IPv6; IPv4 is not vulnerable.

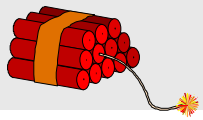
802.1x Port-based access control

Link-level feature



After User Authentication, the port is opened
All traffic is now allowed from this port (all MAC addresses)

MAC address flooding



- Many switches can learn MAC addresses
  - Stored in fast CAM (Content Addressable Memory): [MAC address ←→ Port#]
  - Separates traffic (performance and confidentiality)
  - When memory is full, it sends traffic to all interfaces (same as when learning)
- MAC Flooding: make switch drown in false ARP messages
  - Table is constantly full with garbage and all traffic is sent to all ports
- MAC Duplication: some switches allow address duplication and send the packets to all ports with that MAC address
- Some switches can set maximum number of MAC addresses per port
  - Only learns the first n addresses
  - "n"can even be 1 (cisco "Port Security" feature) – port shuts down if exceeded
  - Configurable timeout for when to forget entries (e.g. 300 sec)

Example

A switch with a limited number of MAC addresses per port:

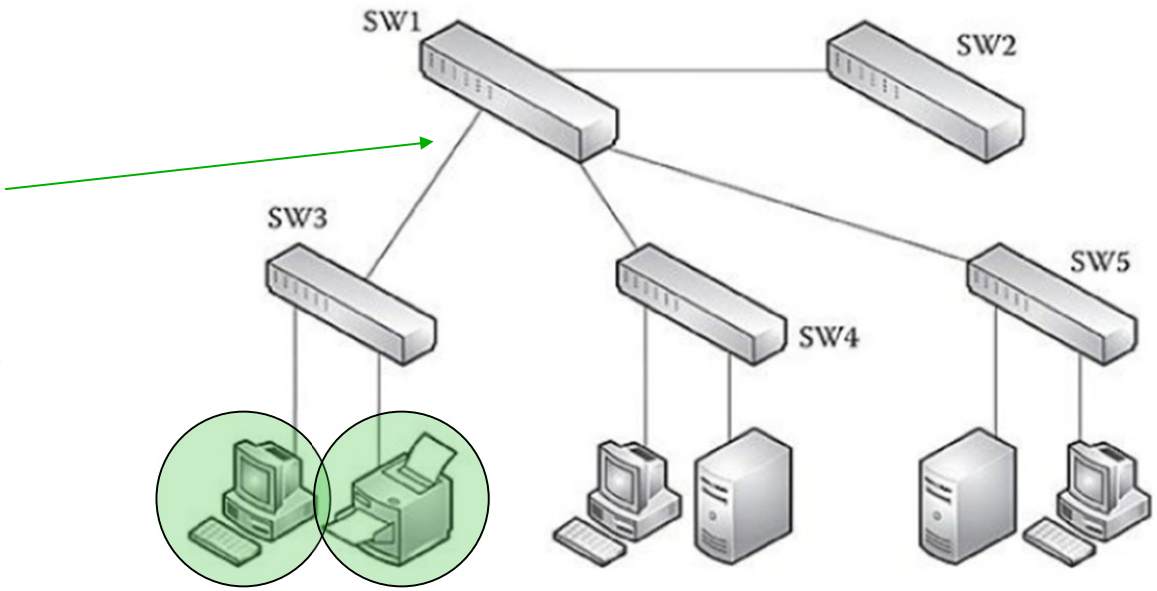
```
# show port-security interface fa 0/18

  Port Security : Enabled
  Port Status : Secure-up
  Violation Mode : Shutdown
  Aging Time : 0 mins
  Aging Type : Absolute
  SecureStatic Address Aging : Disabled
  Maximum MAC Addresses : 1
  Total MAC Addresses : 1
  Configured MAC Addresses : 0
  Sticky MAC Addresses : 0
  Last Source Address : 0004.00d5.285d
  Security Violation Count : 0

#
```

However, multiple MAC address per port common

- Switches are invisible
- SW1 will see two devices on each port
- SW3 sees four devices on one port

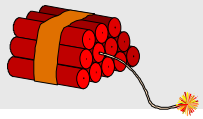


DHCP

- Dynamic Host Configuration Protocol
- Gives machines IP addresses, network masks and default routes
- Typical information sent in a reply:

```
subnet 239.252.197.0 netmask 255.255.255.0 {
   your_addr 239.252.197.22;
   default-lease-time 600 max-lease-time 7200;
   option subnet-mask 255.255.255.0;
   option broadcast-address 239.252.197.255;
   option routers 239.252.197.1;
   option domain-name-servers 239.252.197.2, … ;
   option domain-name "isc.org";
}
```

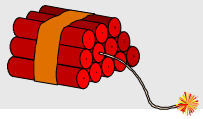
DHCP spoofing



- DHCP is unauthenticated
  - Replies can easily be spoofed – clients accept first reply it gets
  - Impossible to know if reply is authentic
- Easy to spoof DNS server or default gateway (router) and become a MITM
- The attacker must have access to the local network

- Some switches support ”trusted ports”
  - Only they are allowed to answer DHCP requests
  - A reply on another port closes that port
- Ports may be defined as “protected ports”
  - No traffic *between* protected ports → prevents clients to talk to each other
  - WLAN access points often offer this functionality, separates users from each other
  - Several switches (and APs) can cooperate

DHCP starvation



- Someone constantly requesting new addresses
  - Fakes MAC addresses and all available leases will be occupied
  - Clients cannot get an IP address

- Rate-limit DHCP requests
- Monitor MAC addresses and ports in requests and replies
  - Keep track of client requests (Cisco calls it “DHCP snooping”)
  - ARPwatch, open source program for Linux. Generates alarms.

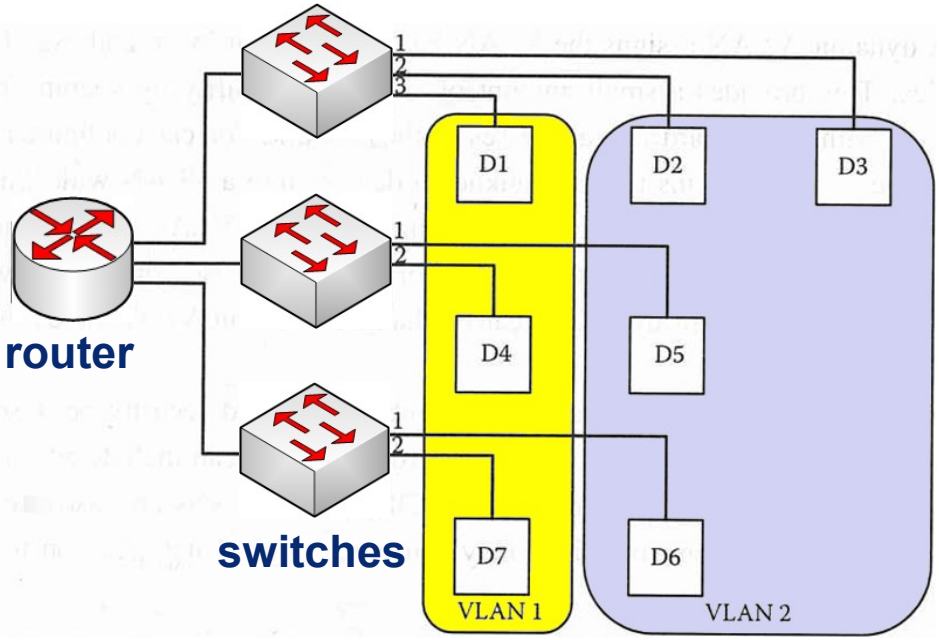
VLANs – Virtual LANs

802.1q

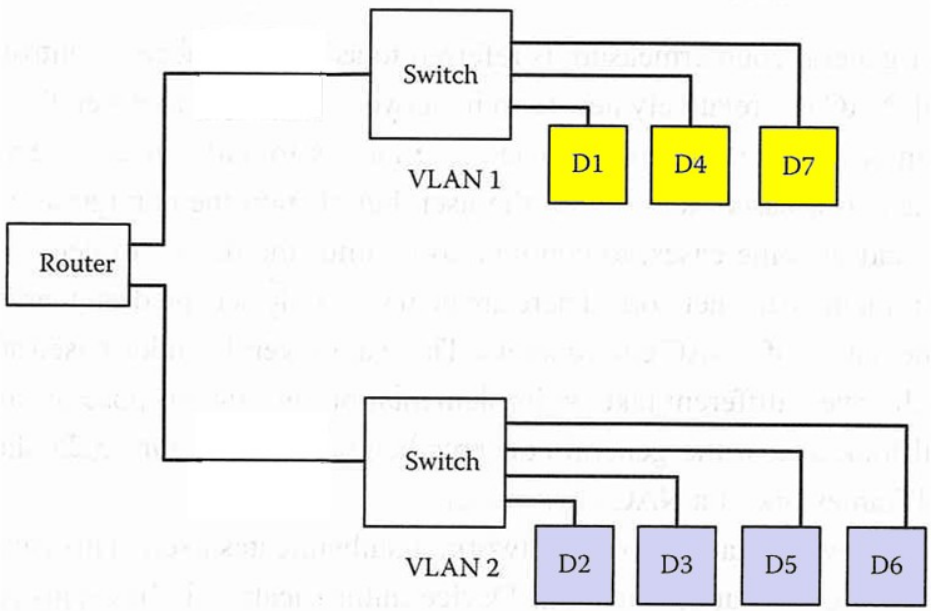
Link-level security: VLAN 802.1q

- Virtual LANs (VLANs) useful
  - Enables creation of workgroups of devices
  - Traffic within a VLAN is private (including broadcasts)
  - Supported by switches, routers and many operating systems
- Standard: IEEE 802.1q
  - Adds an extra 4-byte header to the Ethernet header
  - Contains 12-bit ID that identifies VLAN number (up to 4096)
- VLAN can be implemented in switches with or without tags
- With tags → switches "route" packets based on labels already present
  - All systems may add labels (firewalls, routers, servers, end systems, …)
  - One port can belong to several VLANs, switch can check acceptable values
- Untagged → switches make decision based on incoming port number
  - Port 1 to 4 form one VLAN, port 5 to 12 another, etc.

Using VLANs

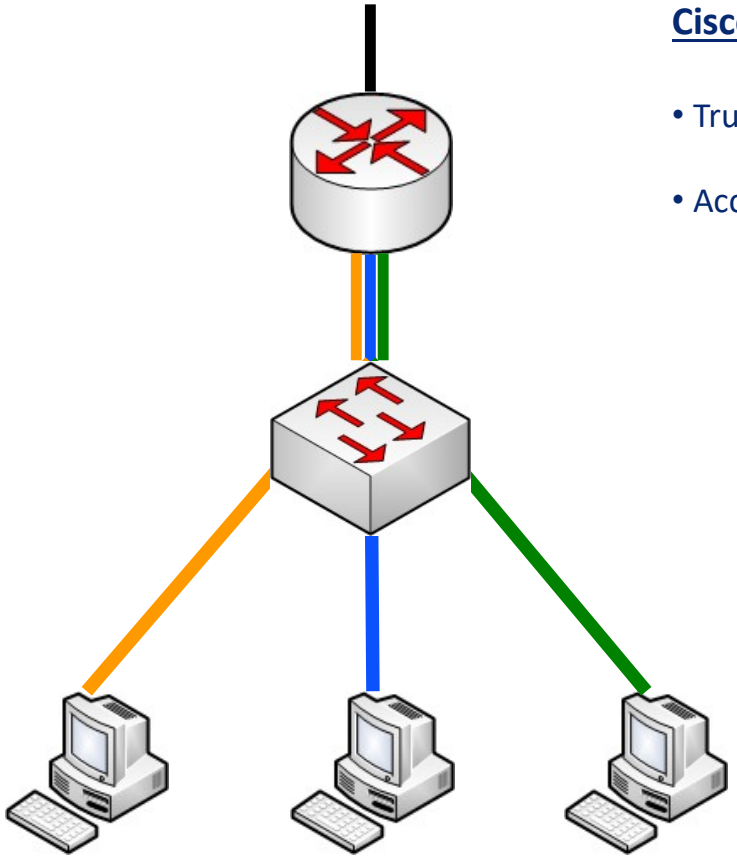


Physical network



Logical view

Coloring to show logical VLANs

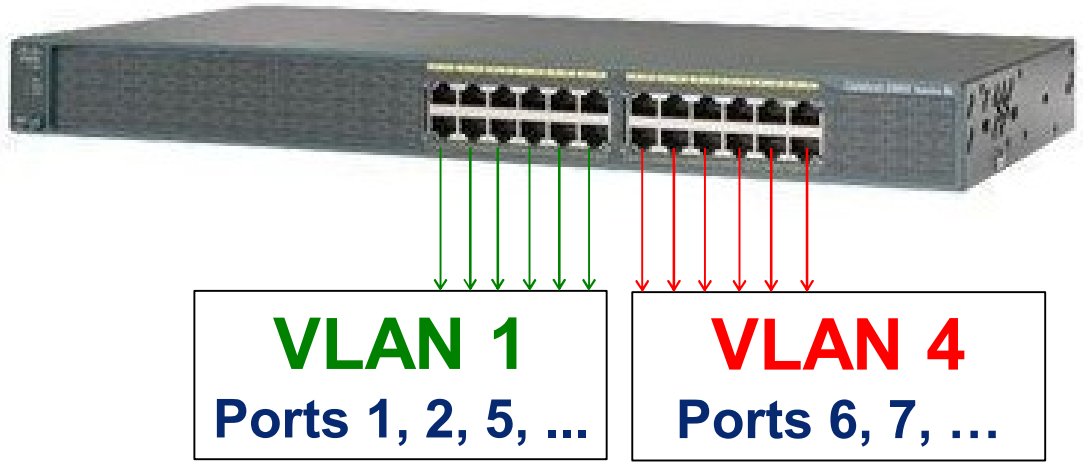


Cisco terminology:

- Trunk mode = multiple VLANs between devices
- Access mode = for end devices with only one VLAN

These three computers cannot communicate directly on link level

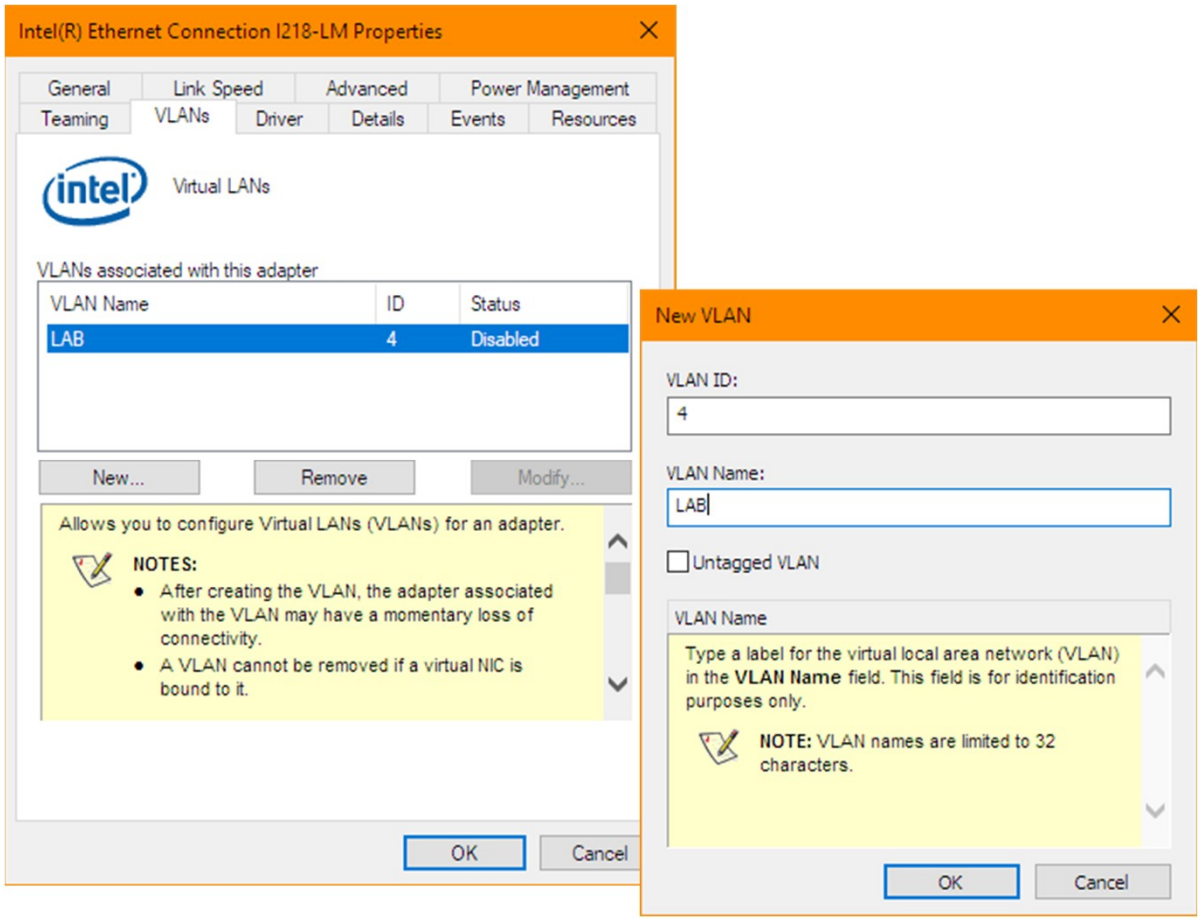
A switch configured for VLAN



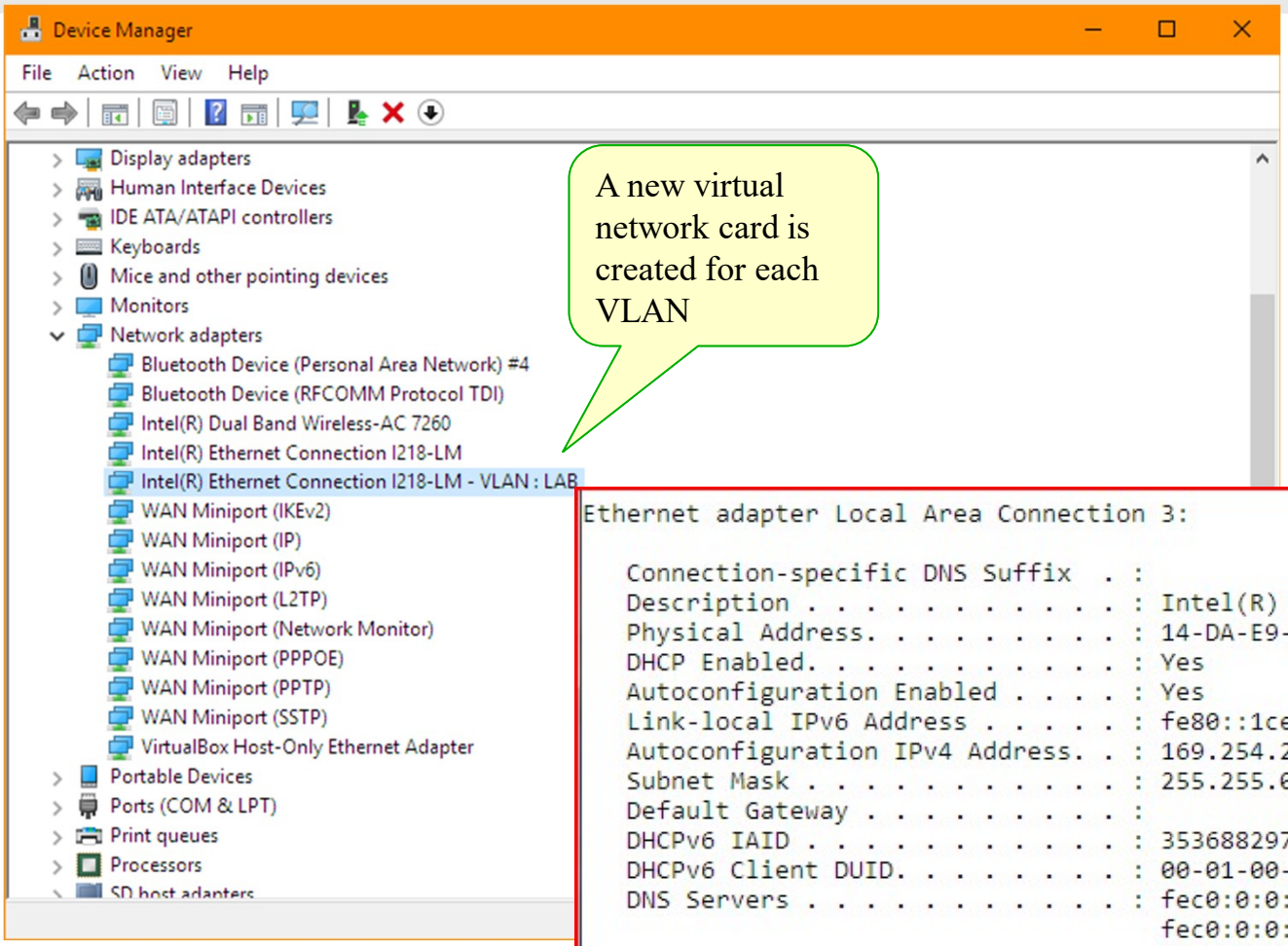

```
# show vlan

VLAN    Name                Status          Ports
---------------------------------------------------------------------------
1       default             active          Fa0/1, Fa0/2, Fa0/5, …
2       Sales               active          Fa0/3, Fa0/4
4       LAB                 active          Fa0/6, Fa0/7, …
```

Configuring a Windows client



Configuring a Windows client



A new virtual network card is created for each VLAN

```
Ethernet adapter Local Area Connection 3:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82579V Gigabit Network Connection - VLAN : LAB
   Physical Address. . . . . . . . . : 14-DA-E9-0F-7E-EC
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::1ce9:a950:313c:ed1a%21(Preferred)
   Autoconfiguration IPv4 Address. . : 169.254.237.26(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 353688297
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-12-78-E9-94-00-1E-8C-08-8A-AB
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Each “network card” has its own IP address

VLAN not designed for security

- VLAN technology was primarily designed for separation, not for security
  - Use it with caution
- No protection against:
  - Man in the middle attacks
    - Possible to change labels on the network (although the traffic must pass the attacker)
  - VLAN with tags trusts the end-point devices
    - Easy to change labels if desired
    - However: switches, routers or firewalls may not accept all tags from clients
  - No encryption → no confidentiality or data integrity
- A misconfigured or hacked switch or router may send traffic anywhere
- VLAN technology is still very useful in security work
  - Adds a layer that isolates traffic (multi-layer security)

Summary

- ARP cache poisoning
  - Use static MAC to IP address translations for sensitive hosts
- DHCP spoofing
  - Limit number of MAC addresses per port
  - Some support ”trusted ports” which only are allowed to answer
- DHCP starvation attacks
  - Limit rate of DHCP requests
  - Only allow DHCP replies from trusted ports
- MAC address flooding
  - Lock MAC addresses to specific ports (interfaces)
  - Some switches can set maximum number of MAC addresses per port
- Use of VLANs (802.1q) to create segments can reduce problems