L2 SECURITY

EN.600.444/644

Spring 2019

Dr. Seth James Nielson

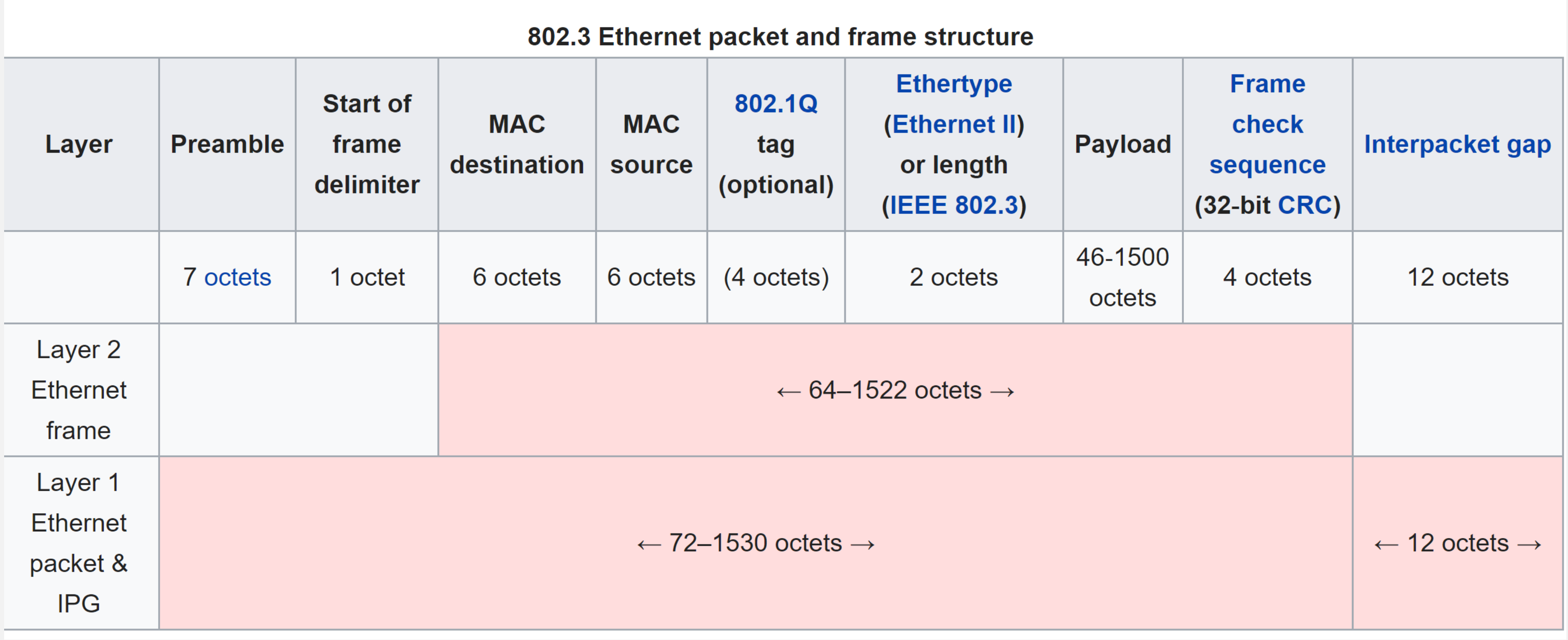
OVERVIEW OF ETHERNET

- Inspired by AlohaNet (a *wireless* protocol!)
- Originally, a shared medium with collision detect
- Modern ethernet (e.g., Gig Ether) has no collisions
- Technically, the messages are called “frames”
  - Actually have a layer 1 and layer 2 component!
  - Also include “ethertype” which says what kind of data

L2 COMMUNICATION

- Mac Addresses
- Broadcast support
- ARP – map MAC to IP address

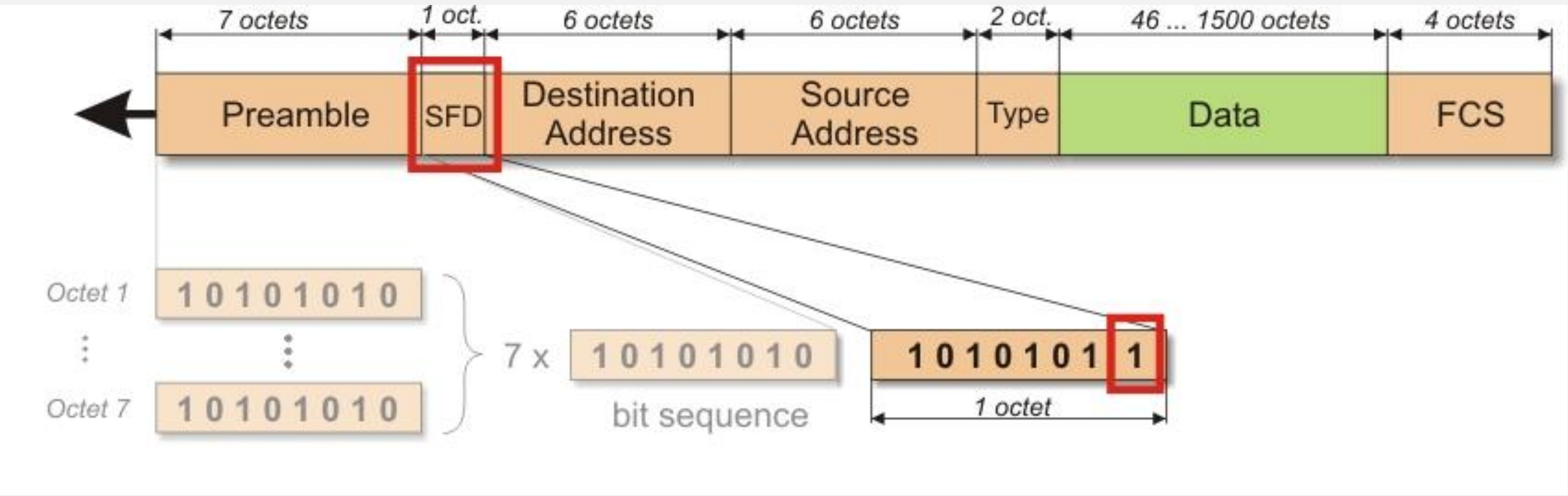
ETHERNET TYPE II FRAME



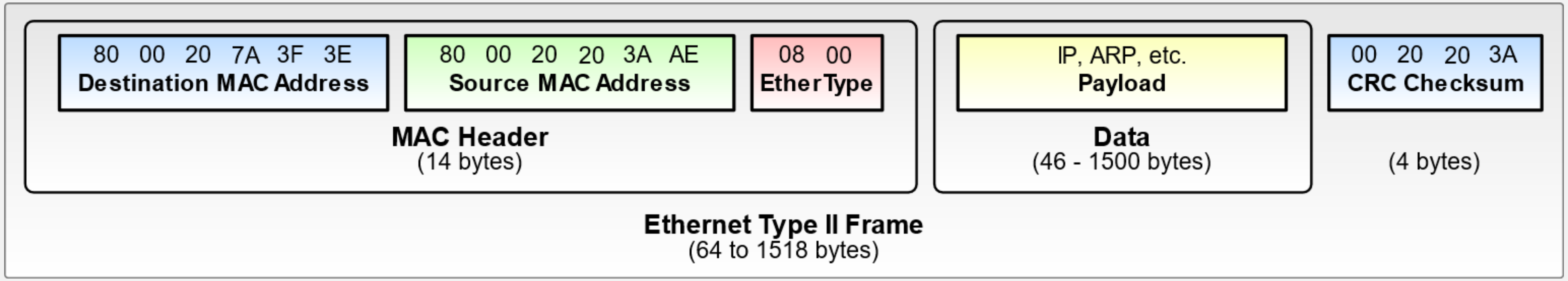
802.3 Ethernet packet and frame structure

Layer	Preamble	Start of frame delimiter	MAC destination	MAC source	802.1Q tag (optional)	Ethertype (Ethernet II) or length (IEEE 802.3)	Payload	Frame check sequence (32-bit CRC)	Interpacket gap
	7 octets	1 octet	6 octets	6 octets	(4 octets)	2 octets	46-1500 octets	4 octets	12 octets
Layer 2 Ethernet frame			← 64–1522 octets →						
Layer 1 Ethernet packet & IPG	← 72–1530 octets →								← 12 octets →

PREAMBLE


7 octets
1 oct.
6 octets
6 octets
2 oct.
46 ... 1500 octets
4 octets
Preamble
SFD
Destination Address
Source Address
Type
Data
FCS
Octet 1
1 0 1 0 1 0 1 0
Octet 7
1 0 1 0 1 0 1 0
7 x
1 0 1 0 1 0 1 0
bit sequence
1 0 1 0 1 0 1 1
1 octet

ETHERNET FRAME



80 00 20 7A 3F 3E
Destination MAC Address

80 00 20 20 3A AE
Source MAC Address

08 00
EtherType

MAC Header
(14 bytes)

IP, ARP, etc.
Payload

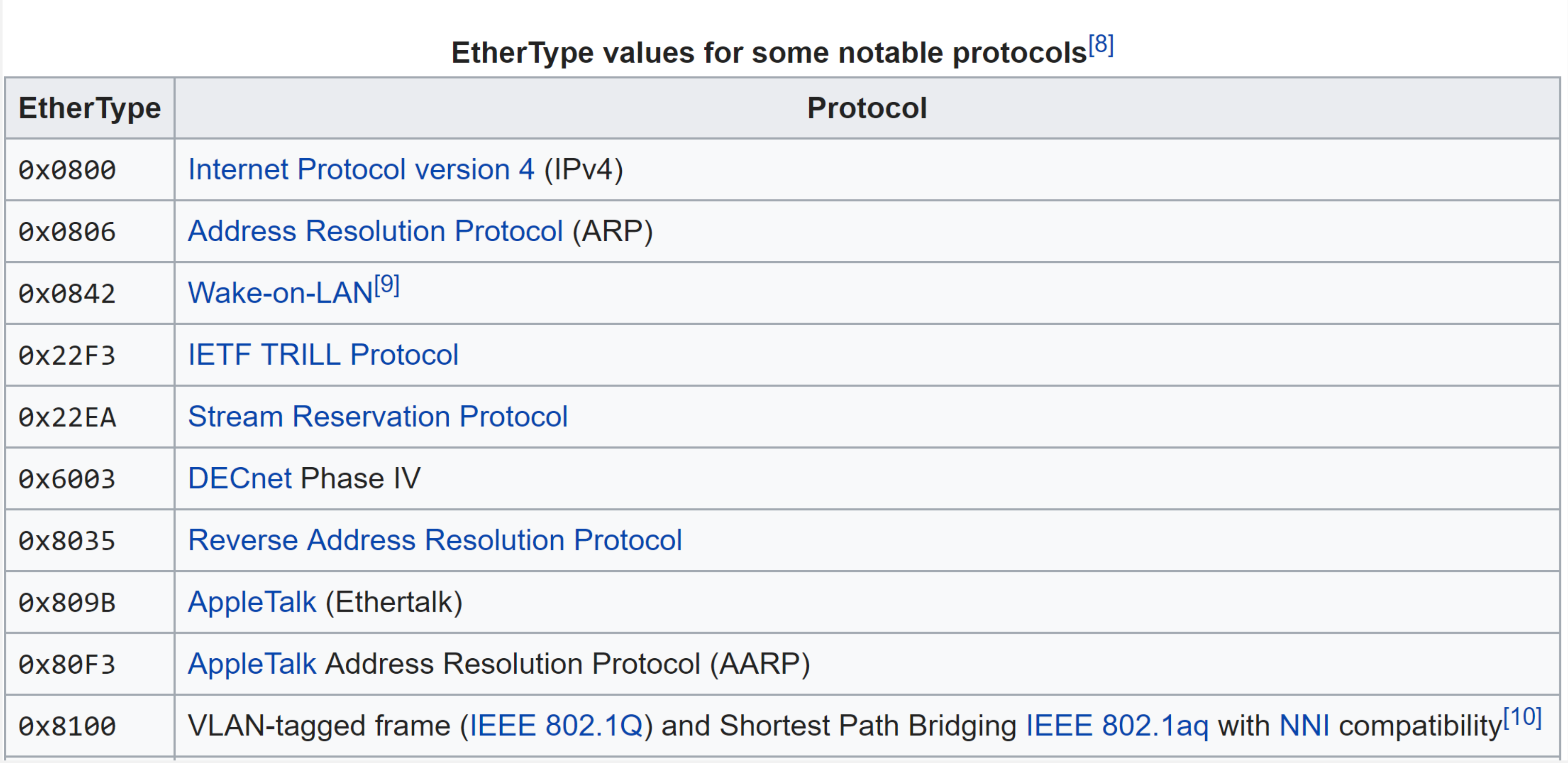
Data
(46 - 1500 bytes)

00 20 20 3A
CRC Checksum

(4 bytes)

Ethernet Type II Frame
(64 to 1518 bytes)

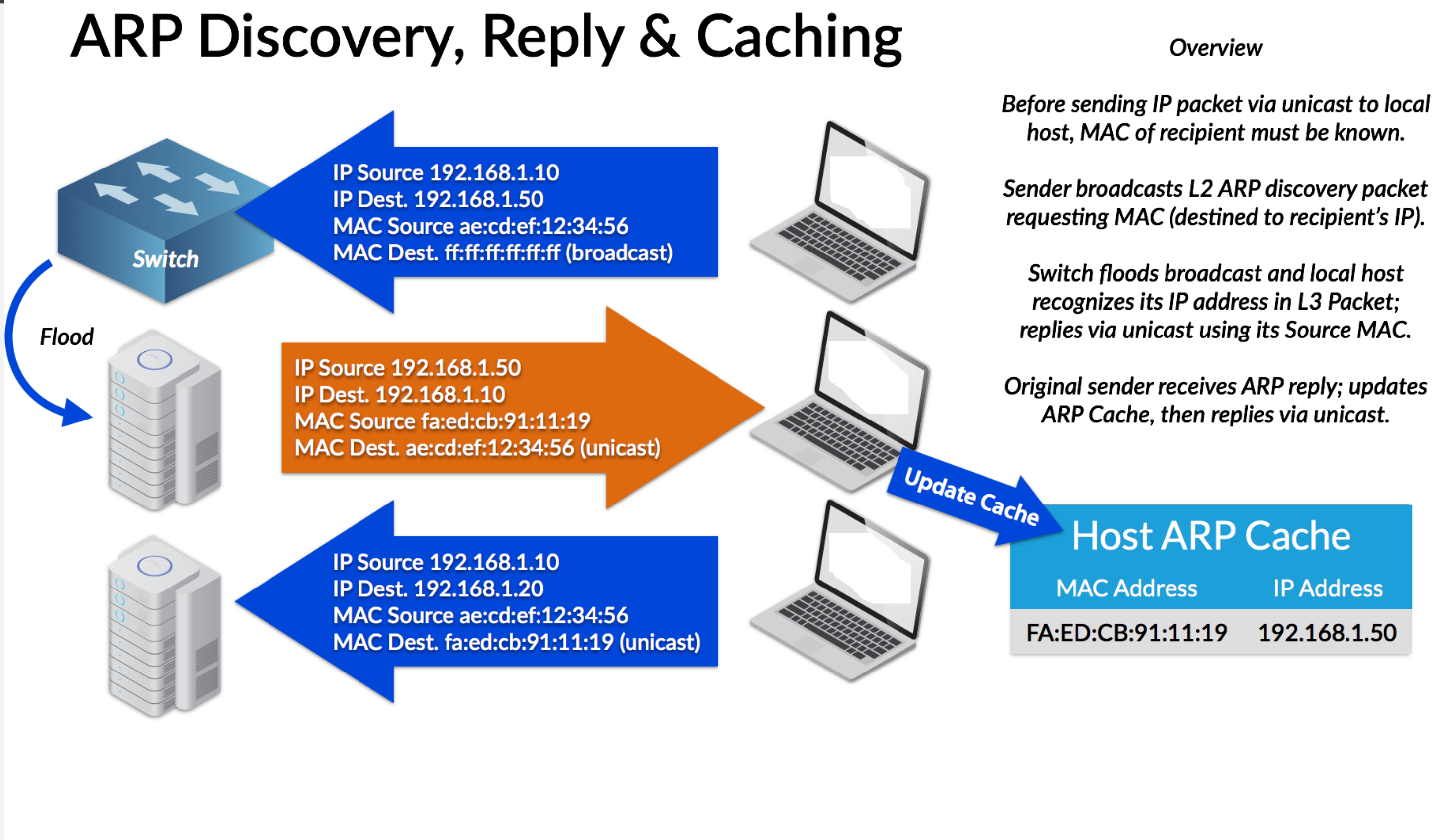
COMMON ETHERTYPE’S



EtherType values for some notable protocols[8]

EtherType	Protocol
0x0800	Internet Protocol version 4 (IPv4)
0x0806	Address Resolution Protocol (ARP)
0x0842	Wake-on-LAN[9]
0x22F3	IETF TRILL Protocol
0x22EA	Stream Reservation Protocol
0x6003	DECnet Phase IV
0x8035	Reverse Address Resolution Protocol
0x809B	AppleTalk (Ethertalk)
0x80F3	AppleTalk Address Resolution Protocol (AARP)
0x8100	VLAN-tagged frame (IEEE 802.1Q) and Shortest Path Bridging IEEE 802.1aq with NNI compatibility[10]

ADDRESS RESOLUTION PROTOCOL



ARP Discovery, Reply & Caching

IP Source 192.168.1.10
IP Dest. 192.168.1.50
MAC Source ae:cd:ef:12:34:56
MAC Dest. ff:ff:ff:ff:ff:ff (broadcast)

IP Source 192.168.1.50
IP Dest. 192.168.1.10
MAC Source fa:ed:cb:91:11:19
MAC Dest. ae:cd:ef:12:34:56 (unicast)

IP Source 192.168.1.10
IP Dest. 192.168.1.20
MAC Source ae:cd:ef:12:34:56
MAC Dest. fa:ed:cb:91:11:19 (unicast)

Overview

Before sending IP packet via unicast to local host, MAC of recipient must be known.

Sender broadcasts L2 ARP discovery packet requesting MAC (destined to recipient's IP).

Switch floods broadcast and local host recognizes its IP address in L3 Packet; replies via unicast using its Source MAC.

Original sender receives ARP reply; updates ARP Cache, then replies via unicast.

Host ARP Cache

MAC Address	IP Address
FA:ED:CB:91:11:19	192.168.1.50

L2 THREAT: ARP POISONING

- Address Resolution Protocol
- ARP request broadcast asks for IP address
- Node responds saying, "That's me!"
- Other nodes record the message in "ARP Cache"
- False response is called "poisoning"

ATTACKS

- Man-in-the-Middle (MITM)
  - Intercept communications meant for another principal
  - Screw up SDN
- DoS – Change packets to mess with communications
  - Can also screw up SDN

DEFENSES

- Attacker must be connected to the local network
- Static ARP caches (small networks only)
- One-mac address per switch port
- MACsec
  - Complex key management problems
  - Does not stop a “legitimate” user from sending bad ARPs
  - Does make it auditable, however.

PORT STEALING

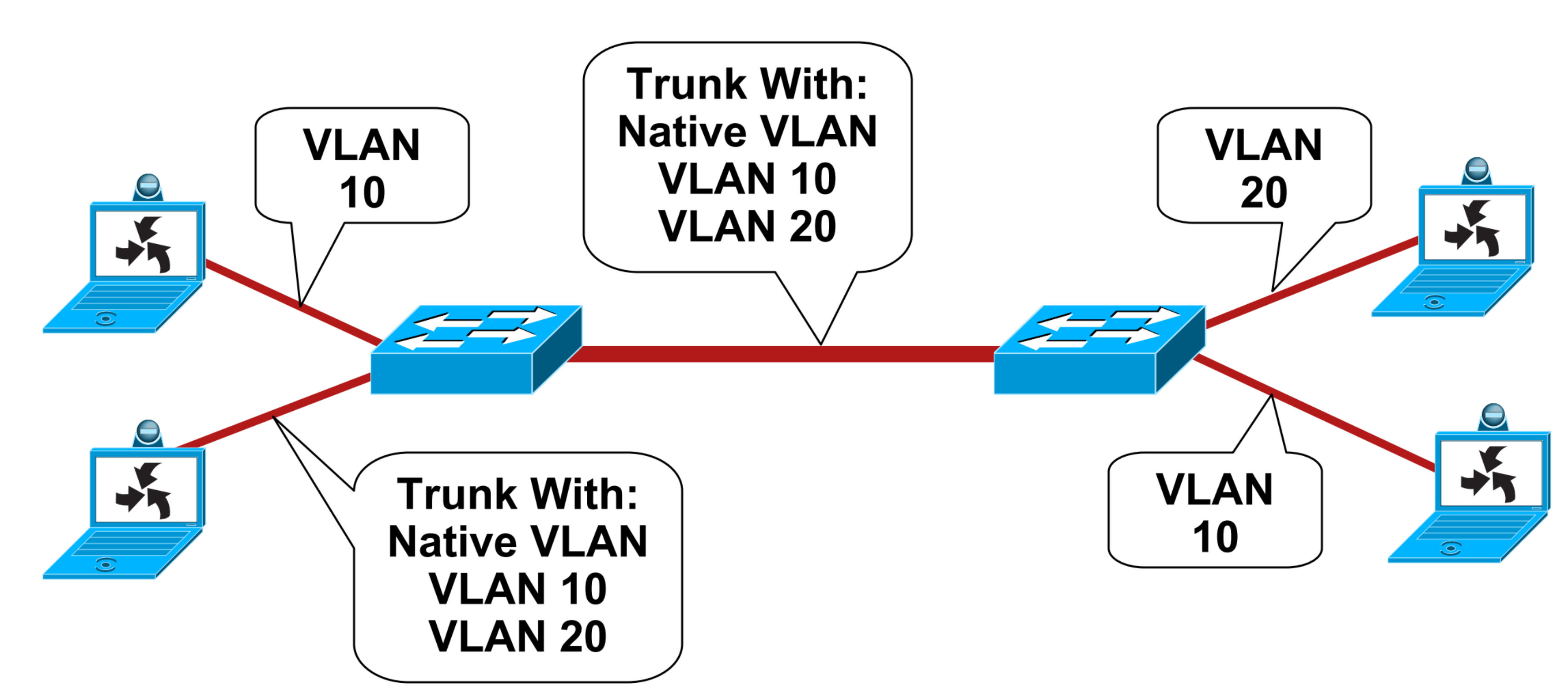
- Flood switches with ARP packets to change port mapping
- Ethernet, remember ,no longer does share media
- Instead, ports map to MAC addresses
- Attack:
  - Convince the switch that your computer owns target's port
  - After data is received, allow victim to take back port

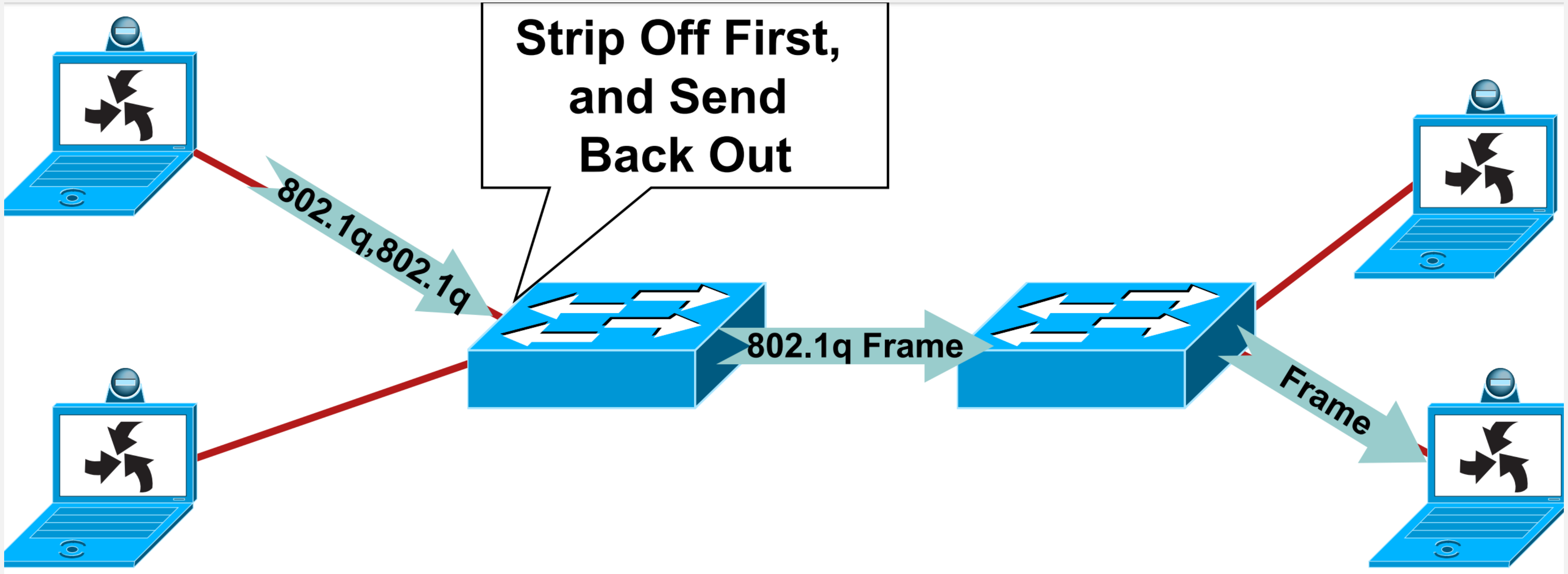
VLAN'S

- VLAN – Virtual LAN
- Typically uses a special TAG in the Ethernet frame
- May be on one or more physical LAN segments
- Creates a broadcast domain
- Traffic cannot move from one VLAN to another without routing

VLAN SECURITY

- Can reduce ARP attacks because ARP traffic is bounded
- However, has its own weaknesses and attacks
  - Abuse Dynamic Trunking Protocol to be part of all VLAN's
  - VLAN hopping using double tagging


VLAN 10
Trunk With: Native VLAN VLAN 10 VLAN 20
VLAN 20
Trunk With: Native VLAN VLAN 10 VLAN 20
VLAN 10



Strip Off First,
and Send
Back Out

802.1q,802.1q

802.1q Frame

Frame

VLAN SECURITY

- Don’t use VLAN -1 (Native)
- Dedicated VLAN ID per port,
- Disable DTP on “user facing” ports
- Disable unused ports, put them in unused VLAN

DHCP

- Request an IP address dynamically
- Sent over L2, of course, because no IP address yet

DHCP ATTACKS

- Gobbler: Request ALL DHCP ADDRESSES!
- MITM: Pretend to be DHCP server
  - Give false gateway, get control of routes

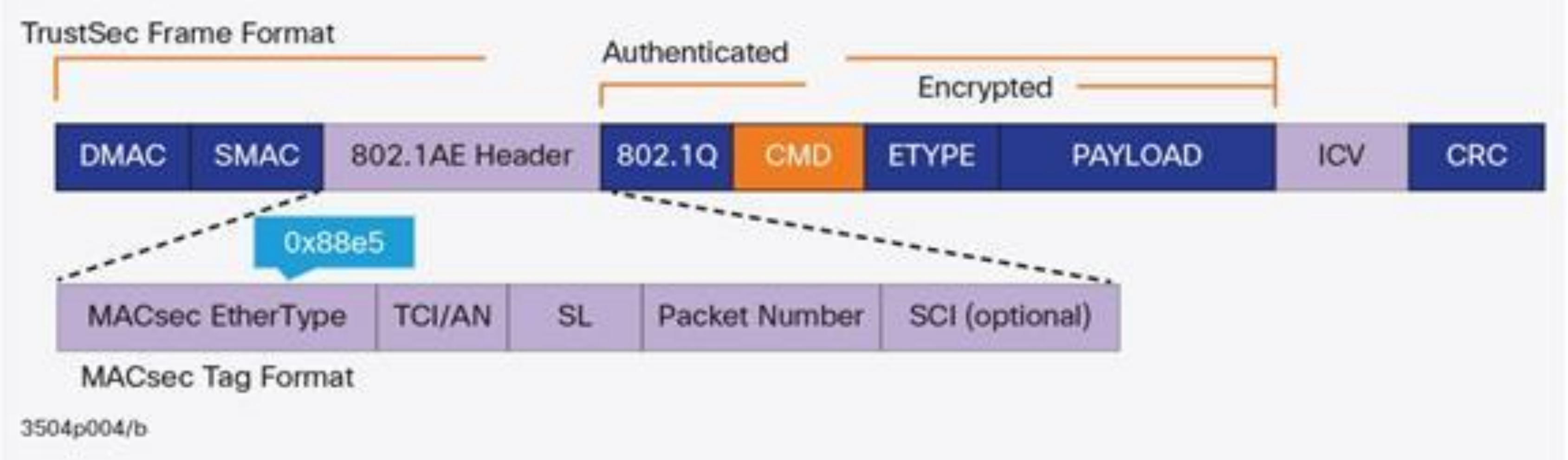
GENERAL CONCERNS FOR L2

- Who owns L2 security?
- Physical security of ports is often non-existant

LAYER 2 FIREWALL

- Can insert a firewall WITHOUT an IP address
- Must be used at a bridge point in the network
  - Sometimes this is done where a VPN connects
  - But can be used between any partition
- Firewall still inspects all the traffic (up to L7)
- Cannot be "targeted" (or even seen!) by attackers

MACSEC FRAME



MACSEC FRAME DETAILS

- EtherType – 0x88E5
- TCI – TAG control info, such as version number, features
- AN – Association Number, identifies security association
- SL – Short Length (if length is less than 48)
- Packet Number – Used for IV/prevent replay
- SCI – Secure Channel Identifier for optional station ID

MACSEC ADVANTAGES

- Data decrypted at each hop
- Permits examination of data for security scanning

MACSEC KEY AGREEMENT

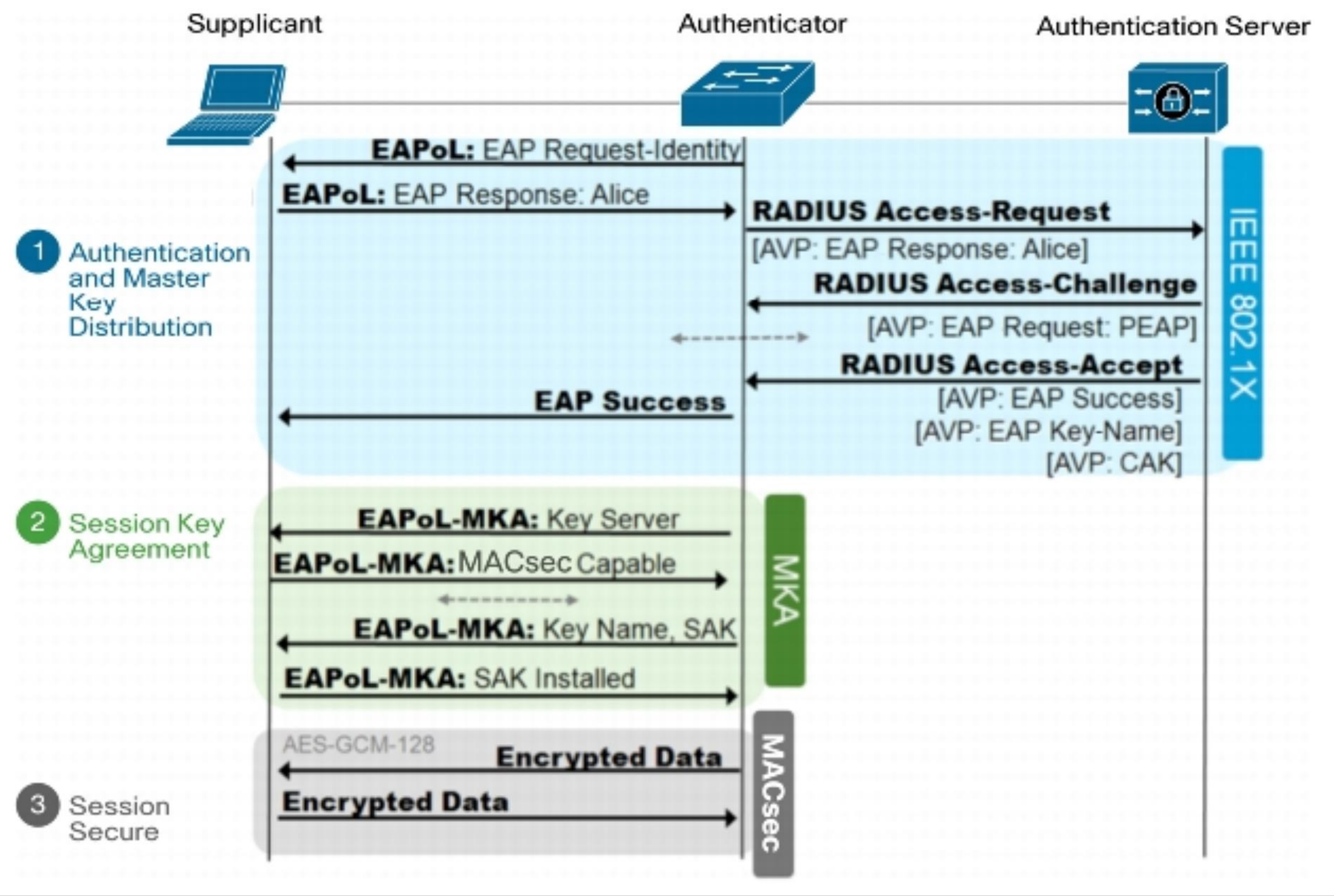
- Preshared Keys
- The master session key which is a product of a successful Extensible Authentication Protocol (EAP) authentication
- Key distributed from an MKA key server

MKA KEYS

- MACSec Key Agreement Protocol (MKA) – Discovery, Keys
- Connectivity Association Key (CAK) – Master key (shared)
  - Pre-shared
  - Or EAP
- Connectivity Associations (CA) – CA if share same CAK
- Secure Association Key (SAK) – Session Key
- Key Server – Elected peer that distributes SAK’s

EAP AUTH

Figure 5. High-Level IEEE 802.1X and MACsec Sequence


Supplicant
Authenticator
Authentication Server
1 Authentication and Master Key Distribution
2 Session Key Agreement
3 Session Secure
EAPoL: EAP Request-Identity
EAPoL: EAP Response: Alice
RADIUS Access-Request
[AVP: EAP Response: Alice]
RADIUS Access-Challenge
[AVP: EAP Request: PEAP]
RADIUS Access-Accept
[AVP: EAP Success]
[AVP: EAP Key-Name]
[AVP: CAK]
EAP Success
IEEE 802.1X
EAPoL-MKA: Key Server
EAPoL-MKA: MACsec Capable
EAPoL-MKA: Key Name, SAK
EAPoL-MKA: SAK Installed
MKA
AES-GCM-128
Encrypted Data
Encrypted Data
MACsec