Protecting the Network – LAN Security

INFO-6078 – Managing Enterprise Networks

FANSHAWE

Protecting the Network – LAN Security

- The network edge is often the main focus in attempts to protect the network from attack
- The LAN is often viewed as a safe zone of the network, a trait that is not always true
- Protocols used at the network edge usually contain better security features than those used internally, which make the LAN an attractive area of attack
- In particular, many protocols that operate in layer 2 lack security in their default state

Securing End User Devices

- Users can be categorized as one of the networks greatest threats, as a user that lacks security awareness can allow an attacker entry into the LAN
- Therefore, users devices are often the focus of phishing and malware campaigns
- An additional threat is presented to organizations that promote bring your own device (BYOD), as administrators tend to have less control over these devices
- Technologies used to secure end user devices include: host-based firewalls, Antivirus software, host intrusion detection systems (HIDS), email spam filtering services, whole disk encryption such as Microsoft Bitlocker and other methods

Email & Spam Data

July 2019

TOTAL GLOBAL EMAIL & SPAM VOLUME FOR JULY 2019

Average Daily Legitimate Email Volume

73.62 BILLION

Email Volume Change from Previous Month

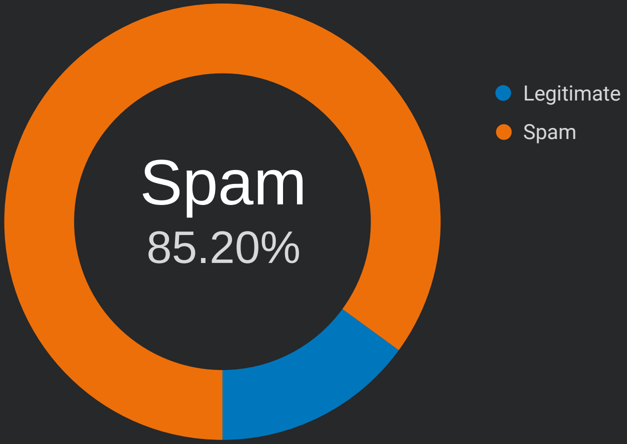
-8.4%

Average Daily Spam Volume

422.49 BILLION

Spam Volume Change from Previous Month

-8%



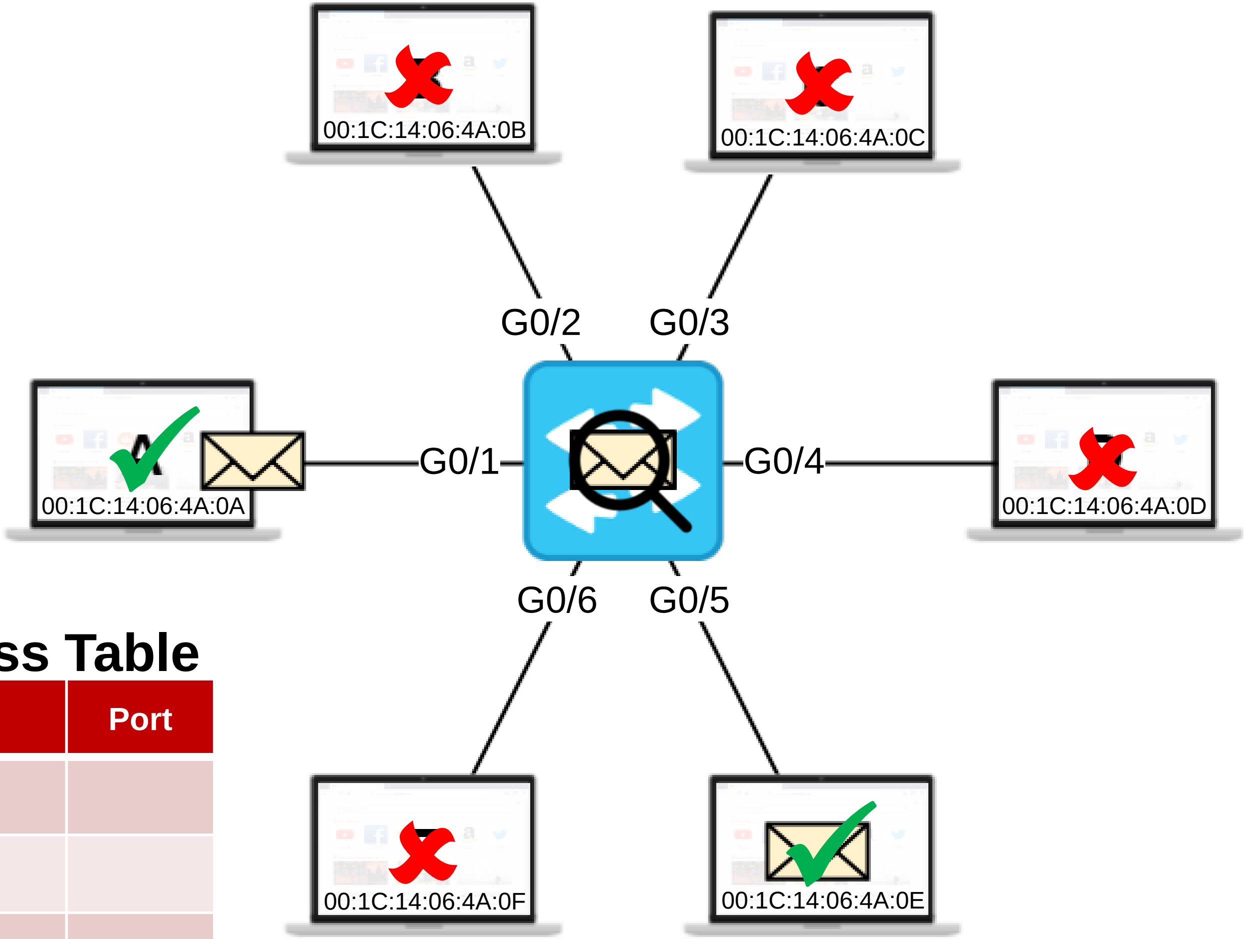
DAILY EMAIL VOLUME

EMAIL TYPE	AVERAGE DAILY VOLUME (BILLIONS)	PERCENTAGE OF GLOBAL TRAFFIC
Legitimate	71.94	14.97%
Spam	408.58	85.02%

Data Link Layer Security

- Network security is often configured from the network layer to the application layer of the OSI model
- The data link layer does not include any “built in” security features and is at significant threat of compromise
- If an attacker can capture or alter traffic at the data link layer, all other layers can be affected
- Securing the data link layer requires understanding the technologies that operate within and configuring them to increase security

Layer 2 Security – MAC Address Table (review)



MAC Address Table

MAC Address	Port

Unknown Unicast Flood

- The default behavior of a switch is to flood traffic to an unknown destination MAC out all ports in the VLAN, except the port that traffic was received on; this process is known as unknown unicast flooding
- Constant and consistent flooding has negative side effects for switches and the can degrade network performance
- Unicast flood mitigation can include alerting an administrator that a flood is occurring, filtering the flood traffic, disabling the port that is the source of the flood, or redirect the traffic to a single port.

MAC Table Overflow

- As switches often come pre-configured with a static amount of RAM, the number of MAC addresses a switch can store in the MAC address table is finite
- To reduce the number of layer 2 broadcasts, most network devices remember learned MAC addresses for 300 seconds before removing them from the table
- If an attacker bombards the switch with traffic that contains randomly generated, unique source MAC addresses before the existing entries timeout, no new entries will be accepted

MAC Table Overflow

- When the MAC Address table is full, the switch reverts to flooding all frames received out all ports associated with that VLAN including across trunk lines
- As long as the attack continues, the attacker can capture traffic destined for any port within the VLAN
- When the attack ceases, the entries in the MAC address table will eventually timeout, and switch operation will return to normal
- One tool used to mitigate MAC Table Overflows is port security

Port Security

- Port security describes a collection of features used to protect against layer 2 sniffing, denial of service, or address spoofing attacks
- Techniques such as MAC address limiting, DHCP protection, IP source guard, ARP spoofing protection and spanning tree protection improve security and stability of layer 2 networks

Port Security Events

- When a port security event occurs, the switch can take action to protect the networks
- Specific actions vary from vendor to vendor, but the following common actions exist:
  - **Drop** – Drop packets from restricted hosts, but do not generate an alert
  - **Drop & Log** – Drop packets from restricted hosts and generate an alert
  - **Shutdown** – Shutdown the port that experienced the security event

Port Security Events

- If a port is shutdown due to a security event, it can be automatically recovered with event auto recovery
- Two type of auto recovery exist:
  - Timed – The port is automatically recovered after a preset timer expires
  - Inactivity – The port is automatically recovered after no activity is detected for a preset time
- Port security event logging refers to sending SNMP traps to a network management server when an event occurs

MAC Limiting

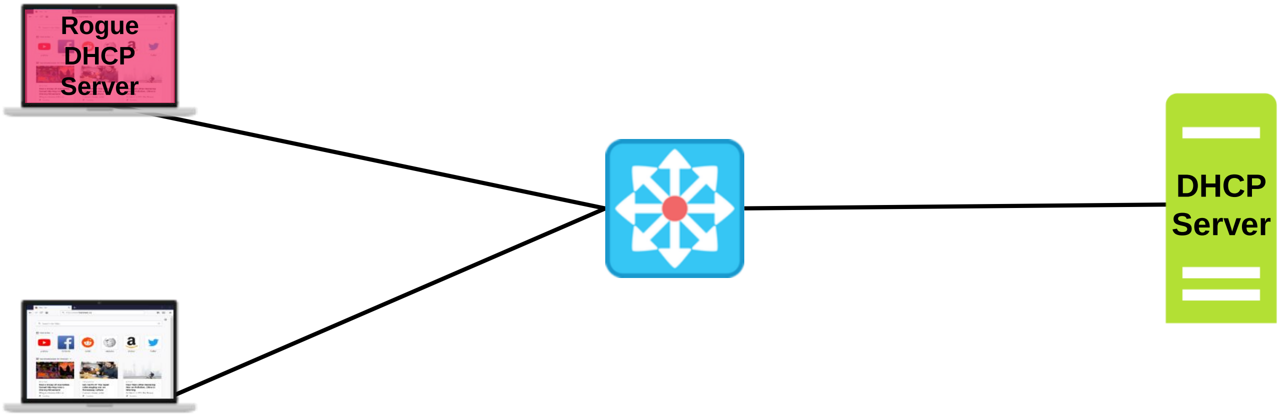
- MAC limiting protects against a MAC address table overflow attack by limiting the number of MAC addresses a switch can learn from an individual port
- MAC limiting is configured on a per-port basis
- A switch can learn about new MAC addresses in one of two ways:
  - **Manual** – An administrator manually configures the MAC addresses that are allowed to connect to the port
  - **Dynamic** – Known as sticky MAC learning, the switch learns MAC addresses automatically and adds the address to the switches configuration

MAC Move Limiting

- MAC move limiting is a variation of MAC limiting that tracks MAC addresses across ports
- If the same MAC address is detected on multiple ports within one second, a port security event is triggered
- MAC move limiting helps to protect against MAC address spoofing and switching loops
- MAC move limiting is configured on a per-VLAN basis

DHCP Attacks

- DHCP servers allows host device IP settings to be configured dynamically
- Using DHCP spoofing, an attacker introduces a rogue DHCP server, which can provide hosts with invalid DHCP information



DHCP Spoofing

- Using DHCP spoofing, an attacker with a rogue DHCP server can affect the integrity of the network in the following ways:
  - **Modify the default gateway**
    - The attacker sets his own computer as the default gateway, they can observe network traffic as it passes through their computer
    - This is a man-in-the-middle (MITM) attack
  - **Modify DNS settings**
    - The attacker modifies the location of the DNS server
    - This may create a MITM attack, but could also be used to direct network traffic to illegitimate web addresses
  - **Modify IP settings**
    - The attacker modifies other IP information related to the host
    - They can put the default gateway out-of-rage of the hosts subnet
    - This is a Denial-of-Service (DoS) attack

DHCP Starvation

- Another form of DHCP DoS attack is a DHCP starvation attack:
  1. An attacker determines the DHCP range (scope) a server is providing
  2. The attacker sends enough DHCP discover messages with spoofed MAC addresses to lease every possible address in the scope
  3. As the DHCP server responds to the requests, the attacker completes the DHCP process and takes all available addresses in the scope
- When all addresses are leased, no new hosts can join the network

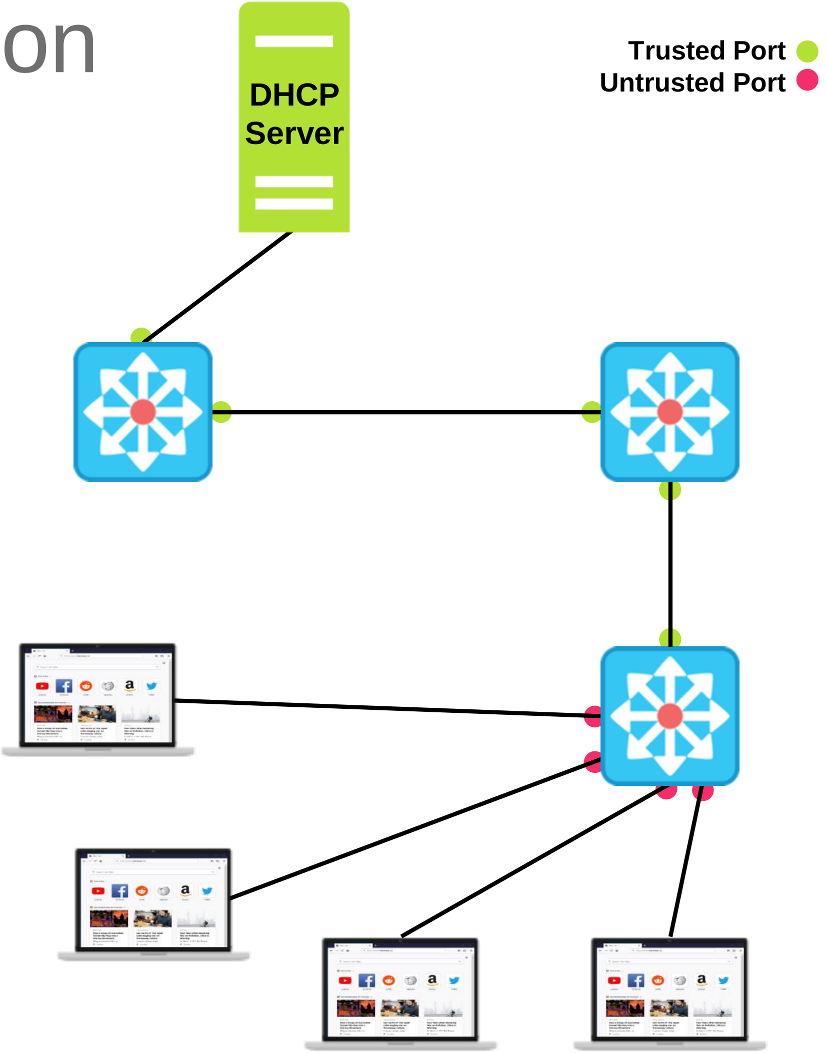
DHCP Snooping

- DHCP snooping is used to prevent DHCP attacks from affecting the network
- When DHCP snooping is enabled, the switch listens to DHCP messages and builds a DHCP snooping binding database containing MAC and IP addresses contained within
- This database is used to identify and filter DHCP messages from untrusted sources
- Additionally, only trusted ports may respond to DHCP requests
- With DHCP snooping enabled untrusted ports are rate-limited, helping to mitigate DHCP starvation attacks

DHCP Snooping Operation

DHCP snooping defines two port types:

- **Trusted Port**
  - A trusted DHCP server exists upstream to this port
  - Only trusted ports can process DHCP Offer and DHCP ACK messages
- **Untrusted Port**
  - Host devices are connected to untrusted ports
  - The default port configuration when snooping is enabled



Address Resolution Protocol (ARP) Attacks

- ARP is used by hosts to determine their MAC address, when only the host's IP is available
- ARP achieves this by utilizing a data link layer broadcast (ARP request), which the target host responds to in an ARP reply
- Hosts can also send an unsolicited ARP reply, called a gratuitous ARP, which preempts the ARP process and allows hosts to store the IP to MAC mapping in their ARP cache
- ARP is an insecure protocol, and allows an attacker to send gratuitous ARP messages with a spoofed MAC address and update the cache that points to a legitimate host

ARP Poisoning Attack

- If the attacker was to claim his MAC address resolved to the IP address of the default gateway, hosts within the subnet would direct traffic destined to other networks to the attackers MAC address
- Likewise, if the attacker informed the router that it’s MAC address resolved to the IP of other hosts found within the network, the router would send traffic destined to the other hosts to the attacker
- Combining these two steps, the attacker has poisoned the ARP cache of the devices, and created a MITM attack, where all traffic destined to other hosts is relayed through the attacker

Dynamic ARP Inspection

- Dynamic ARP inspection can prevent ARP poisoning by filtering gratuitous ARP messages containing invalid MAC addresses
- Dynamic ARP inspection intercepts ARP requests and replies received on untrusted ports and verifies the addresses contained in the messages, by comparing them to the binding table created for DHCP snooping
- Consequently, dynamic ARP inspection can only occur on a network that has DHCP snooping enabled
- Invalid ARP replies are dropped and logged if logging is enabled
- Hosts configured with static addressing require ARP ACLs to participate in dynamic ARP inspection

Address Spoofing Attacks

- The method used to populate the MAC address table of a switch is vulnerable to MAC addressing spoofing
- If an attacker spoofs their MAC address to that of a known host, a switch can alter the MAC address table to direct traffic to the attacking host
- For a spoofing attack to be successful, the attacker will need to send a constant stream of traffic with the spoofed address towards the switch, or risk the original host from regaining the MAC to port mapping
- Additionally, IP address spoofing occurs when an attacker assumes an IP address that it was not assigned

IP Source Guard

- IP source guard inspects all traffic that passes through a port for valid addresses based on the binding table created for DHCP snooping
- IP source guard dynamically creates and maintains per-port VLAN ACLs, ensuring that hosts cannot communicate on the network until the DHCP process is complete and only valid source IP addresses, or source IP and MAC address are accepted from the port

VLAN Access Control List (VACL)

- Unlike IP ACLs, VACLs provide access control for traffic that has a source or destination address within a VLAN
- VACLs do not follow the same rules as IP ACLs, and are not defined by direction, all traffic in the VLAN is subject to the VLANs rules
- Actions for matched traffic include forward or drop

VLAN Hopping Attack

- VLAN hopping is a vulnerability of a poorly configured layer 2 network
- An attacker uses software to present it’s host as a switch, and exploit the Cisco proprietary Dynamic Trunking Protocol (DTP), that enables switches to automatically configure a trunk between two compatible devices
- Alternatively, an attacker can use a compatible switch to create a trunk link
- If the attacker can successfully create a trunk with the switch, they can access all VLANs configured on the switch

Improving VLAN Security

- The following steps help to improve VLAN security:
  - Disable trunking on all port that will connect to end device by setting the ports to access mode
  - Manually enable trunks on desired ports by statically configuring trunks
  - Disable DTP on all ports
  - Change the native VLAN from the default setting
  - Create a “black hole” VLAN and place all unused port in it
  - Shutdown all unused ports

802.1X Port-Based Network Access Control

- 802.1X provides a port-based authentication method for devices wanting to join the network and restricts access to unauthorized devices
- Until a device is authenticated, 802.1X restricts the network device to only exchange Extensible Authentication Protocol (EAP) over LAN aka EAPOL messages
- EAPOL operates within layer 2 and utilizes the EtherType value 0x888E
- A common implementation of 802.1X restricts users network access until their identity can be verified against a Microsoft Active Directory Domain

802.1X Port-Based Network Access Control

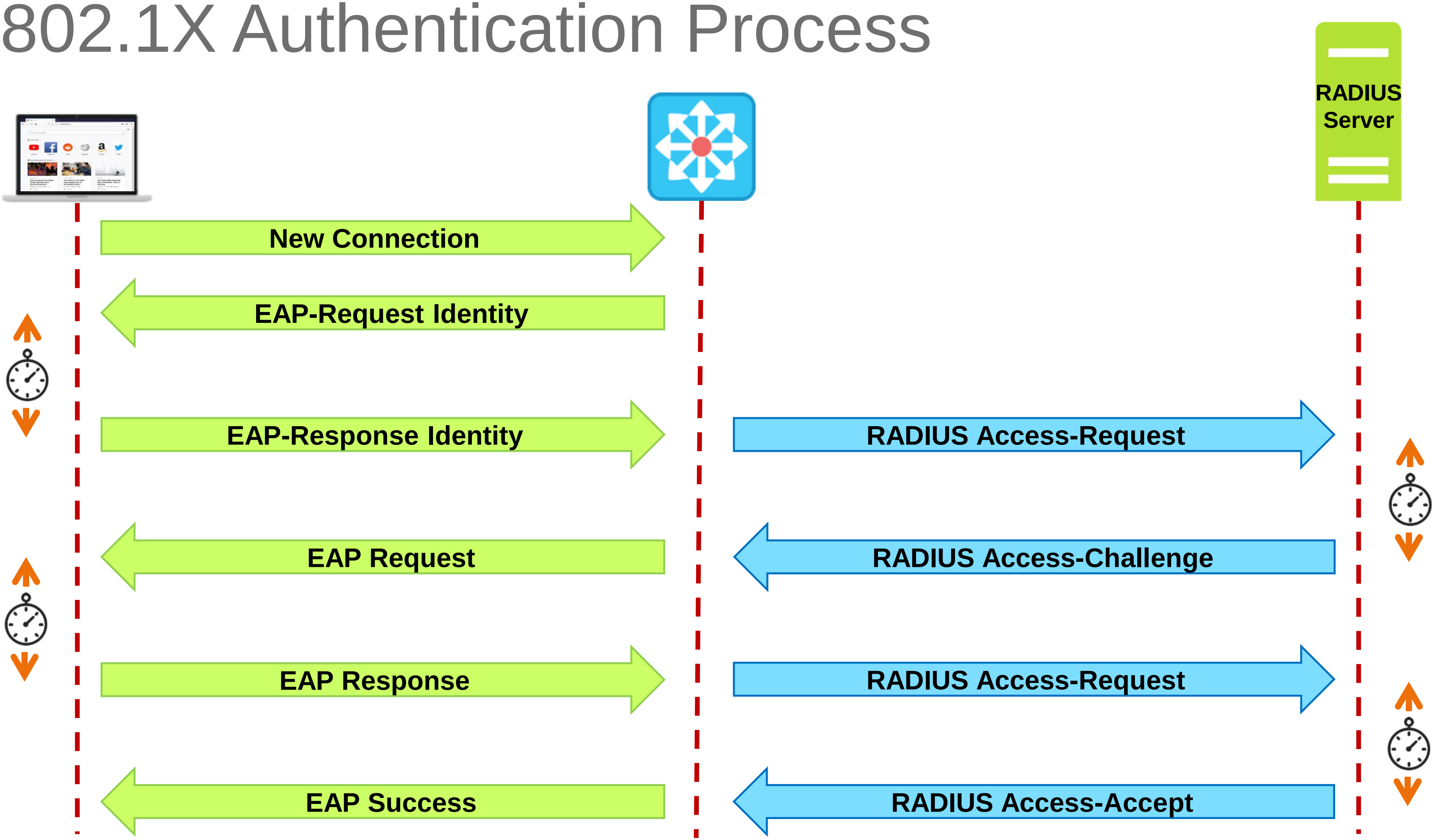
802.1X authentication involves three parties:

- **Supplicant**
  - A client device such as a laptop or phone
- **Authenticator**
  - An infrastructure device like a switch or access point
  - The authenticator restricts regular network access until the supplicant has been authenticated
  - Acts as a proxy exchanging authentication messages between the supplicant and the authentication server
- **Authentication Server**
  - Validates the identity of the supplicant and notifies the authenticator is access should be allowed

802.1X Port States

- When a device connects to an 802.1x controlled port, the port is in an unauthorized state, allowing only EAPOL messages to be forwarded
- Upon successful authentication, the port transitions into an authorized state, allowing all network traffic to flow
- If a client logs out, or the authenticator detects a change in port state, the port reverts to an unauthorized state

802.1X Authentication Process



References

- Email & Spam data based on Cisco Talos Website – Retrieved from: https://www.talosintelligence.com/reputation_center/email_rep