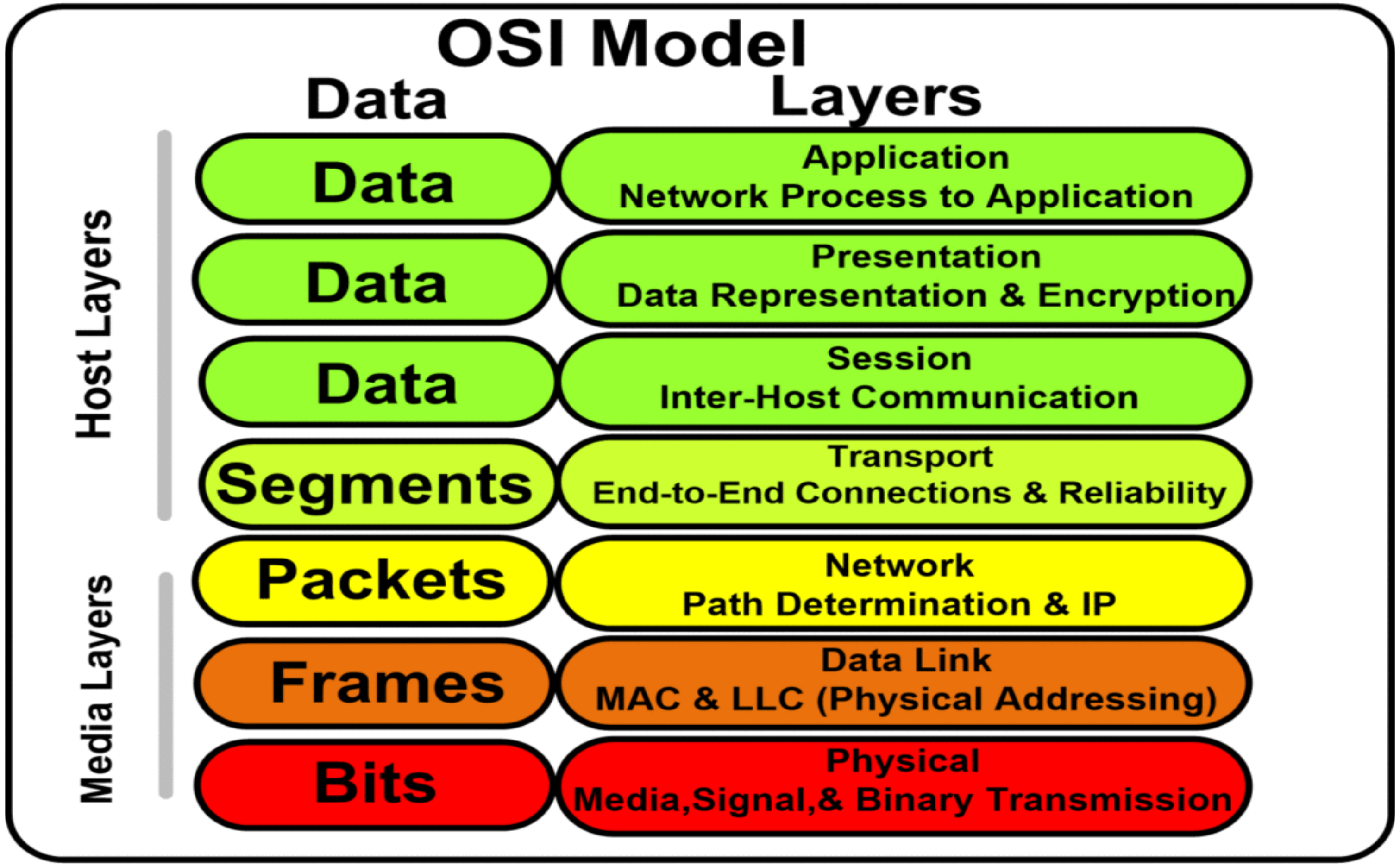
COMP3052 Computer Security

Session 08: Network Security



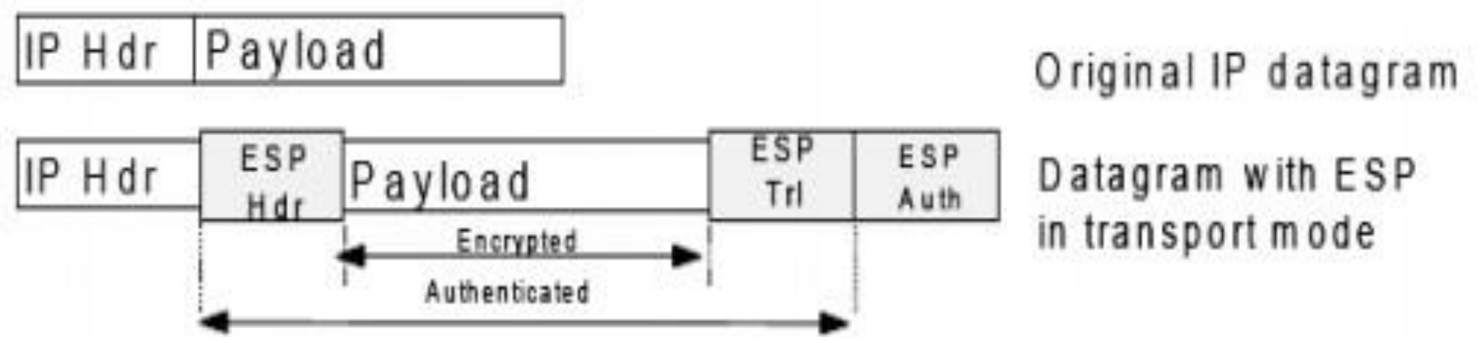
OSI Model

	Data	Layers
Host Layers	Data	Application Network Process to Application
	Data	Presentation Data Representation & Encryption
	Data	Session Inter-Host Communication
	Segments	Transport End-to-End Connections & Reliability
Media Layers	Packets	Network Path Determination & IP
	Frames	Data Link MAC & LLC (Physical Addressing)
	Bits	Physical Media,Signal,& Binary Transmission

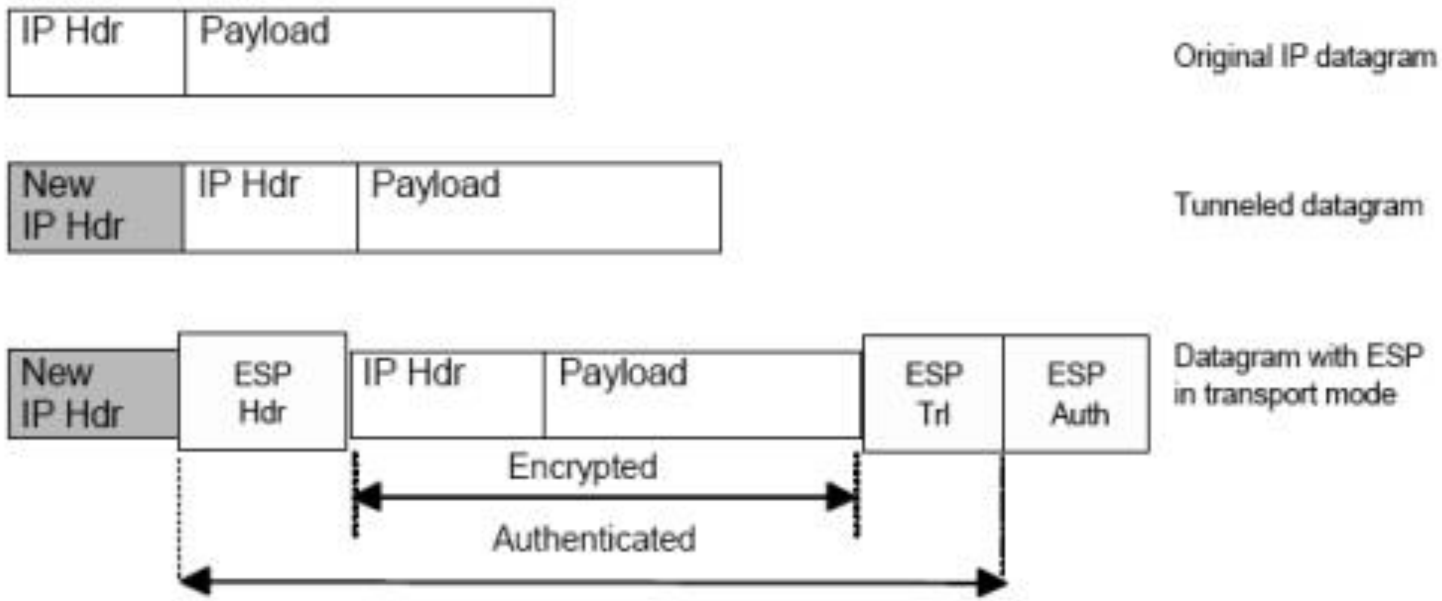
Reference: 7 Layers of OSI Model and Their Functions
https://electricala2z.com/cloud-computing/osi-model-layers-7-layers-osi-model/

1. Which of the following diagrams describes ESP in tunnel mode?

(A)



(B)

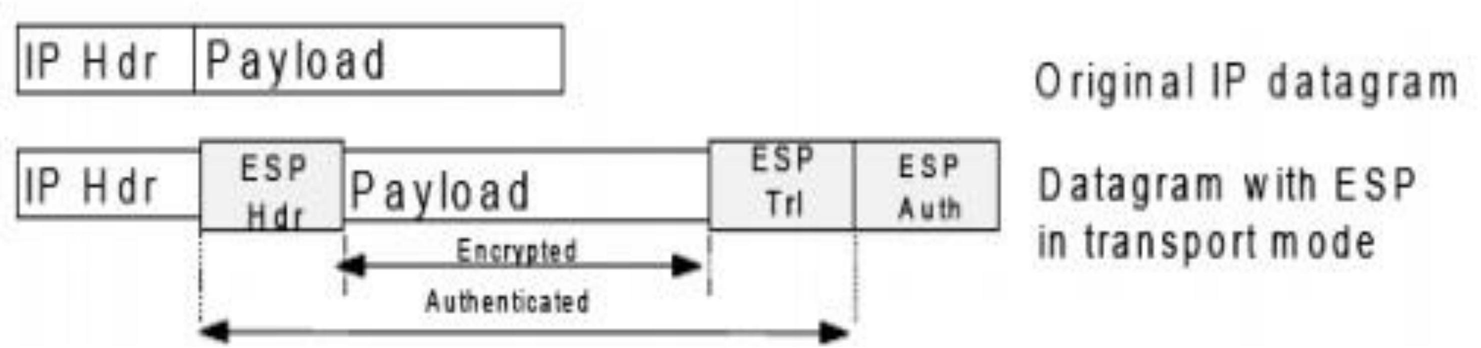


Reference: What is ESP in tunnel and transport mode and the difference between AH and ESP?

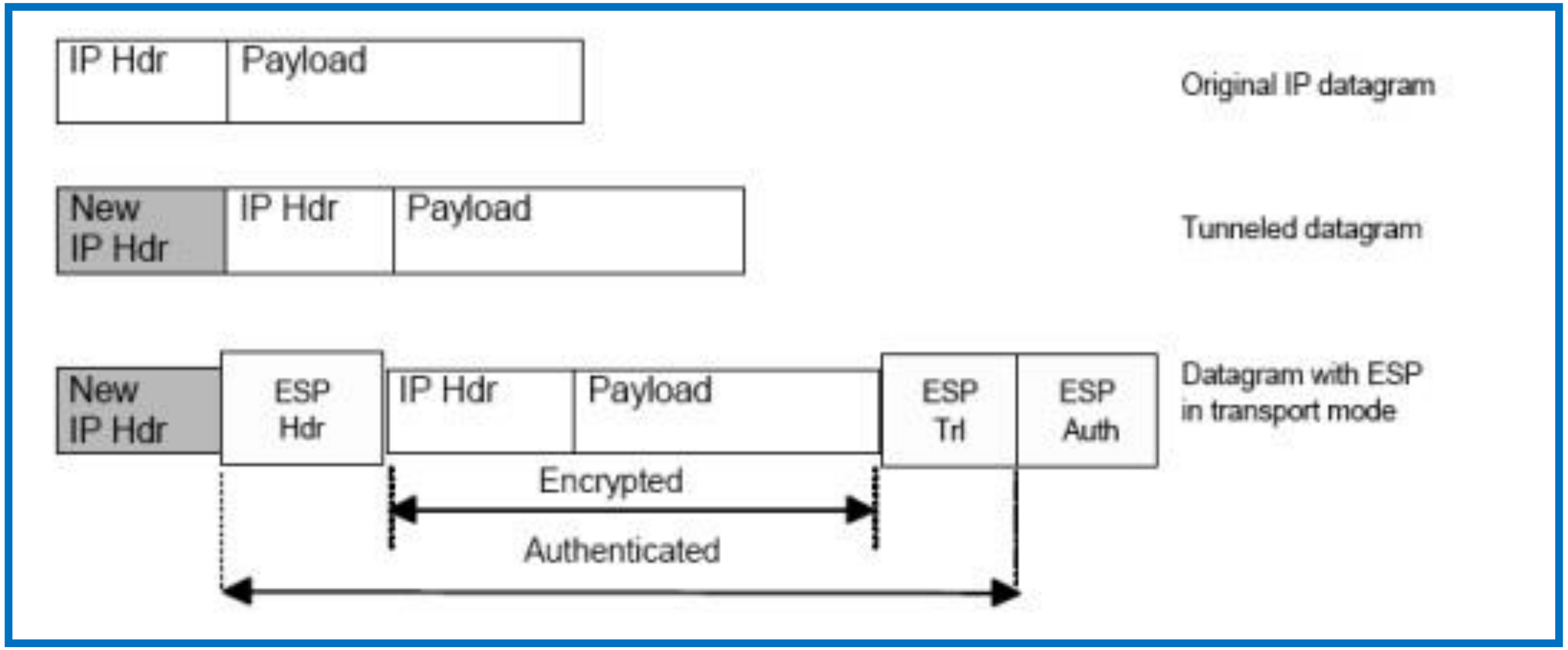
https://www.tutorialspoint.com/what-is-esp-in-tunnel-and-transport-mode-and-the-difference-between-ah-and-esp

1. Which of the following diagrams describes ESP in tunnel mode?

(A)



(B)



Reference: What is ESP in tunnel and transport mode and the difference between AH and ESP?

https://www.tutorialspoint.com/what-is-esp-in-tunnel-and-transport-mode-and-the-difference-between-ah-and-esp

2. Which protocol is used to discover the destination address needed to be added to an Ethernet frame?

(A) ARP

(B) DNS

(C) DHCP

(D) HTTP

Reference: 7.2.3 Address Resolution Quiz Answers

https://itexamanswers.net/7-2-3-address-resolution-quiz-answers.html

3. Which protocol is used to discover the destination address needed to be added to an Ethernet frame?

(A) ARP
(B) DNS
(C) DHCP
(D) HTTP

Reference: 7.2.3 Address Resolution Quiz Answers
https://itexamanswers.net/7-2-3-address-resolution-quiz-answers.html

4. What is one function of the ARP protocol?

(A) Obtaining an IPv4 address automatically

(B) Mapping a domain name to its IP address

(C) Resolving an IPv4 address to a MAC address

(D) Maintaining a table of domain names with their resolved IP addresses

Reference: 7.2.3 Address Resolution Quiz Answers

https://itexamanswers.net/7-2-3-address-resolution-quiz-answers.html

3. What is one function of the ARP protocol?

(A) Obtaining an IPv4 address automatically

(B) Mapping a domain name to its IP address

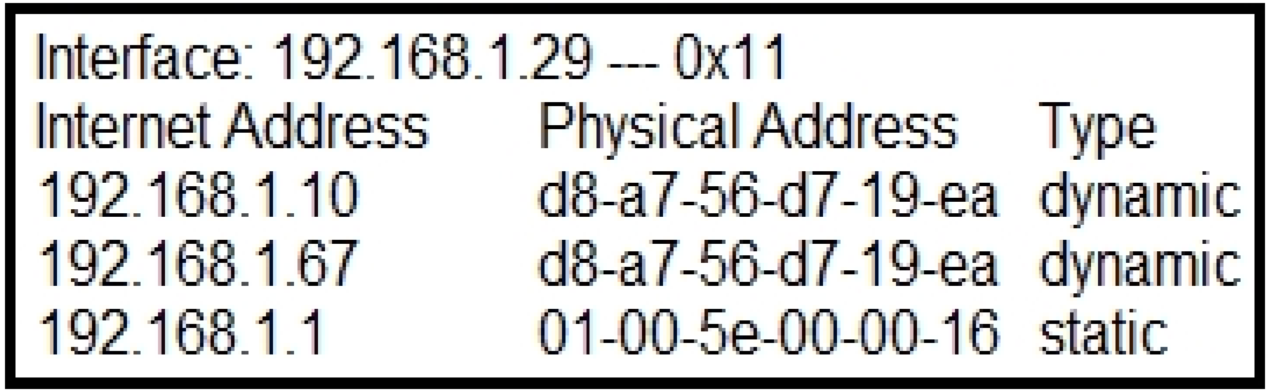
(C) Resolving an IPv4 address to a MAC address

(D) Maintaining a table of domain names with their resolved IP addresses

Reference: 7.2.3 Address Resolution Quiz Answers

https://itexamanswers.net/7-2-3-address-resolution-quiz-answers.html

4. Refer to the exhibit below. What is occurring in this network?



```
Interface: 192.168.1.29 --- 0x11
Internet Address      Physical Address    Type
192.168.1.10          d8-a7-56-d7-19-ea   dynamic
192.168.1.67          d8-a7-56-d7-19-ea   dynamic
192.168.1.1           01-00-5e-00-00-16   static
```

(A) ARP cache poisoning

(B) DNS cache poisoning

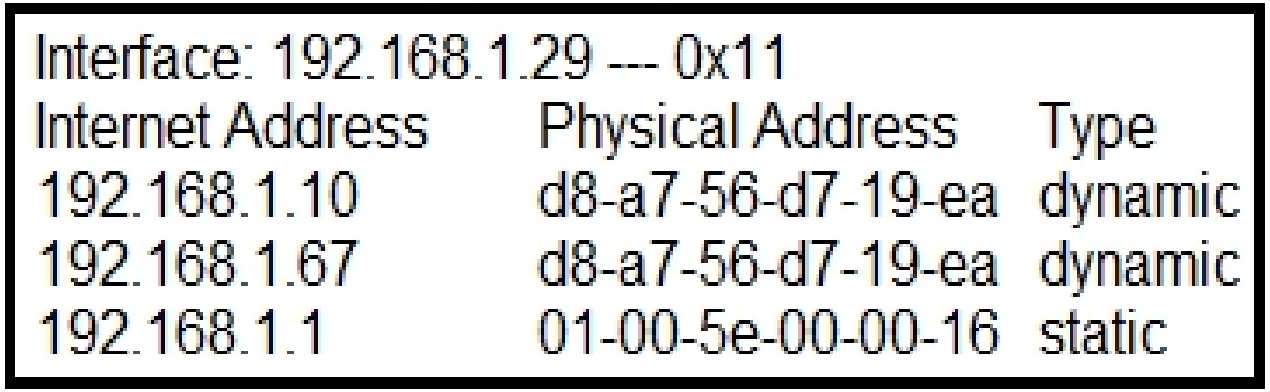
(C) MAC address table overflow

(D) MAC flooding attack

Reference: Exam Topics

https://www.examtopics.com/discussions/cisco/view/65956-exam-200-201-topic-1-question-63-discussion/

4. Refer to the exhibit below. What is occurring in this network?



```
Interface: 192.168.1.29 --- 0x11
Internet Address      Physical Address    Type
192.168.1.10          d8-a7-56-d7-19-ea   dynamic
192.168.1.67          d8-a7-56-d7-19-ea   dynamic
192.168.1.1           01-00-5e-00-00-16   static
```

(A) ARP cache poisoning

(B) DNS cache poisoning

(C) MAC address table overflow

(D) MAC flooding attack

ARP poisoning, is a Man in the Middle (MitM) attack that allows attackers to intercept communication between network devices. The attacker must have access to the network. They scan the network to determine the IP addresses of at least two devices. The attacker uses a spoofing tool such as Arpspoof or Driftnet, to send out forged ARP responses. The forged responses advertise that the correct MAC address for both IP addresses, belonging to the router and workstation, is the attacker's MAC address. This fools both router and workstation to connect to the attacker's machine, instead of to each other. The two devices update their ARP cache entries and from that point onwards, communicate with the attacker instead of directly with each other. The attacker is now secretly in the middle of all communications.

Reference: Exam Topics

https://www.examtopics.com/discussions/cisco/view/65956-exam-200-201-topic-1-question-63-discussion/

5. Which of the following threats commonly relies on DNS poisoning and spoofing to exploit an unknowing victim?

(A) Rainbow tables

(B) Brute force

(C) Man-in-the-middle

(D) Zero-day attacks

(E) Phishing

Reference: Exam Topics

https://www.examtopics.com/discussions/comptia/view/75105-exam-220-1002-topic-1-question-492-discussion/

5. Which of the following threats commonly relies on DNS poisoning and spoofing to exploit an unknowing victim?

(A) Rainbow tables
(B) Brute force
(C) Man-in-the-middle
(D) Zero-day attacks
(E) Phishing

DNS spoofing is a type of attack in which a malicious actor intercepts DNS request and returns the address that leads to its own server instead of the real address. Hackers can use DNS spoofing to launch a man-in-the-middle attack and direct the victim to a bogus site that looks like the real one.

Reference: Exam Topics

https://www.examtopics.com/discussions/comptia/view/75105-exam-220-1002-topic-1-question-492-discussion/