
LIGHTHOUSE LABS

Week 1 Day 3
Cyber Security Bootcamp

Network Overview

We are making time to answer questions! Please don't worry!

LIGHTHOUSE LABS

Today . . .

OSI & TCP/IP models, Encapsulation process

The Frame’s Journey

IPv4 addresses

IPv6 addresses

Wireshark overview

LIGHTHOUSE LABS

OSI Model vs TCP/IP Protocol Stack

OSI Model	Encapsulation (PDU)	TCP/IP Stack
Layer 7 - Application	Data	Application
Layer 6 - Presentation	Data	
Layer 5 - Session	Data	
Layer 4 - Transport	Segment	Transport
Layer 3 - Network	Packet	Internet
Layer 2 - Data Link	Frame	Network Access
Layer 1 - Physical	Bits	

OSI Model - Layer Particulars

OSI Model Layers	Details
Layer 7 - Application	Protocols connecting software to network processes
Layer 6 - Presentation	Data formatting and encryption
Layer 5 - Session	Establish, maintain, and tear down of connection between source and destination
Layer 4 - Transport	Segment data, sequence numbers, port numbers (type of data and protocol involved)
Layer 3 - Network	Routing, source and destination identification (IP addresses)
Layer 2 - Data Link	Local link addressing (MAC addresses)
Layer 1 - Physical	Equipment standards and physical details

The Frame’s Journey

IP addresses - logical, identify original source and final destination of the frame, do not change once frame is sent by the source device

MAC addresses - physical address, used for local link communications only, identify the next hop (router or computer) the frame is headed for, can not be used to identify a device in another network segment, change at each hop the frame stops at

The Frame's Journey

PC1	**Switch1**	**Router1**	**Router2**	**Switch2**	**PC2**
MAC = A IP = 1	MAC = B IP = 2	MAC = C IP = 3	MAC = D IP = 4	MAC = E IP = 5	MAC = F IP = 6
Outgoing Frame Addressing					
SM = A	SM = A	SM = C	SM = D	SM = D	SM = F
SIP = 1	SIP = 1	SIP = 1	SIP = 1	SIP = 1	SIP = 6
DM = C	DM = C	DM = D	DM = F	DM = F	DM = D
DIP = 6	DIP = 6	DIP = 6	DIP = 6	DIP = 6	DIP = 1
S=source, D=destination, M=MAC address, IP=IP address, all addresses are symbolic					

IP Addresses

IPv4

32 bit

Dotted-decimal notation

4 octets

Written in decimal number format

Each octet = 8 bits

Use subnet mask to id network vs host portions, can be written in full or slash notation

1 address per interface

Public and private address ranges

IPv6

128 bits

Hexidecimal format

Can be compressed

Uses prefix (slash notation) to id network portion

Can be subnetted, simpler than in IPv4

Each interface gets at least 2 addresses, Link-local, and Global

Wireshark

A good intro to working in Wireshark . . .

Try the Getting Started lab

https://gaia.cs.umass.edu/kurose_ross/wireshark.php

Thoughts, Comments . . .

?

LIGHTHOUSE LABS

Today's To Do . . .

Complete W1D2 scheduled activities if needed

Complete W1D3 activities, including 'Wireshark Analysis Practice' Task

Review before tomorrow's class:

- Network Segmentation
- Firewalls
- VPNs

LIGHTHOUSE LABS