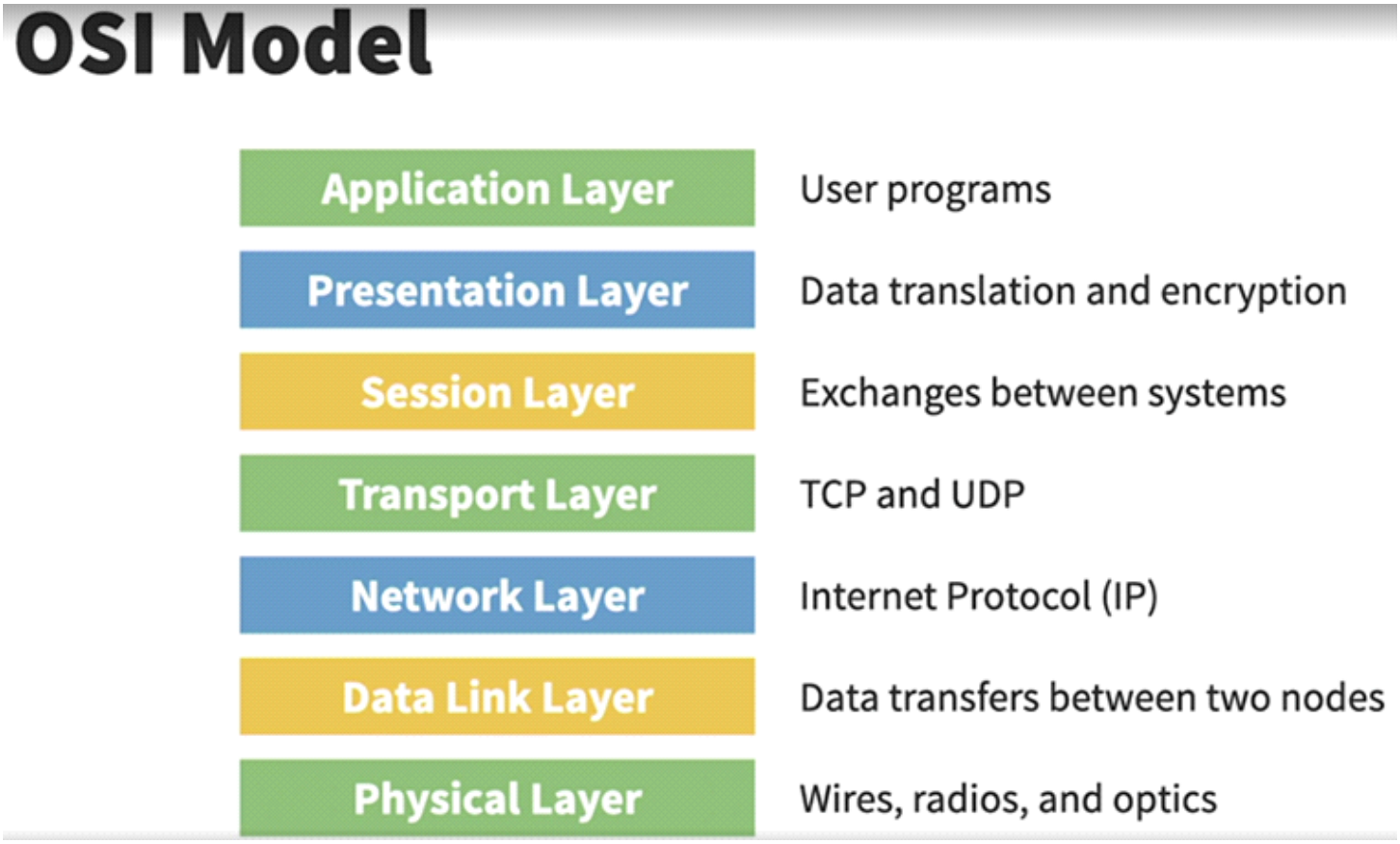
Review

Thursday, June 13, 2024 9:38 AM

Network

Tuesday, June 11, 2024 10:21 AM

TCP - connection oriented; 3-way handshake, reliable
UDP - quicker, connectionless, used for voice and video apps



0 - 1,023 : well-known ports
1,024 - 49,151 : registered ports
49,152 - 65,535 : dynamic ports

Common Ports:

Port 21 : FTP	Port 23 : Telnet	Port 53 : DNS	Port 3389 : RDP
Port 22 : SSH	Port 25 : SMTP	Port 137/138/139 : NetBIOS	Port 110 : POP
Port 143 : IMAP	Port 80 : HTTP	Port 443 : HTTPS	

Test Install

Tuesday, June 11, 2024 11:54 AM

nmap -V

nmap scanme.nmap.org

Scanning

Tuesday, June 11, 2024 11:58 AM

Port States in Nmap

State	Description
open	Accepting connection requests
closed	No service responding to requests
filtered	Blocked by a firewall
unfiltered	Accessible, but scanner was unable to determine whether open or closed

dig cmd to locate IP address of a URL
nmap x.x.x.x : example to perform scan on a single device
nmap x.x.x.x z.z.z.z c.c.c.c : example to scan multiple IPs
nmap 192.168.1.1,3,6 : shortened way to scan multiple Ips
nmap 192.168.1.1-6 : scan an IP range
nmap 192.168.1.0/29 : scan an entire subnet
nmap -6 : to scan IPV6 addresses

Host Discovery Flags

Flag	Purpose
-Pn	No host discovery
-PS	TCP SYN request
-PA	TCP ACK request
-PU	UDP request
-PE	ICMP echo request
-PR	ARP request

nmap -n : to disable reverse DNS resolution

TCP Scan Types

Flag	Description
-sS	TCP SYN Scan
-sT	TCP Connect Scan
-sN	TCP NULL Scan
-sF	TCP FIN Scan
-sX	TCP Xmas Scan
-sA	TCP ACK Scan
-sW	TCP Window Scan
-sM	TCP Maimon Scan

nmap -F : scans only top 100 ports
nmap -p : scan specific ports
Ex nmap -p 80,443
Ex nmap -p http,https

nmap -p- : scans all TCP ports

Nmap Timing Templates

Template	Description
-T5	Insane
-T4	Aggressive
-T3	Normal
-T2	Polite
-T1	Sneaky
-T0	Paranoid

nmap -O : to detect OS of target
nmap -sV : svc version running on an open port
nmap -A : remote OS detection; svc & version detection; traceroute; nmap scripting engine (NSE)

Output

Tuesday, June 11, 2024 1:51 PM

Nmap Output Formats

Flag	Description
-oN	Human-readable text file
-oX	Machine-readable XML file
-oG	Grepable text file

nmap -v : scan in verbose mode
nmap -vv : scan very verbosely