You like Networking?

By Chet Apichart & Taylor Swift

Sign in :3

https://da.gd/mSclJf

Agenda

01 Intro to Networking

02 Protocol Stacks

03 Ports & Services

04 Subnetting

05 Firewall

06 Blooket

07 Lab

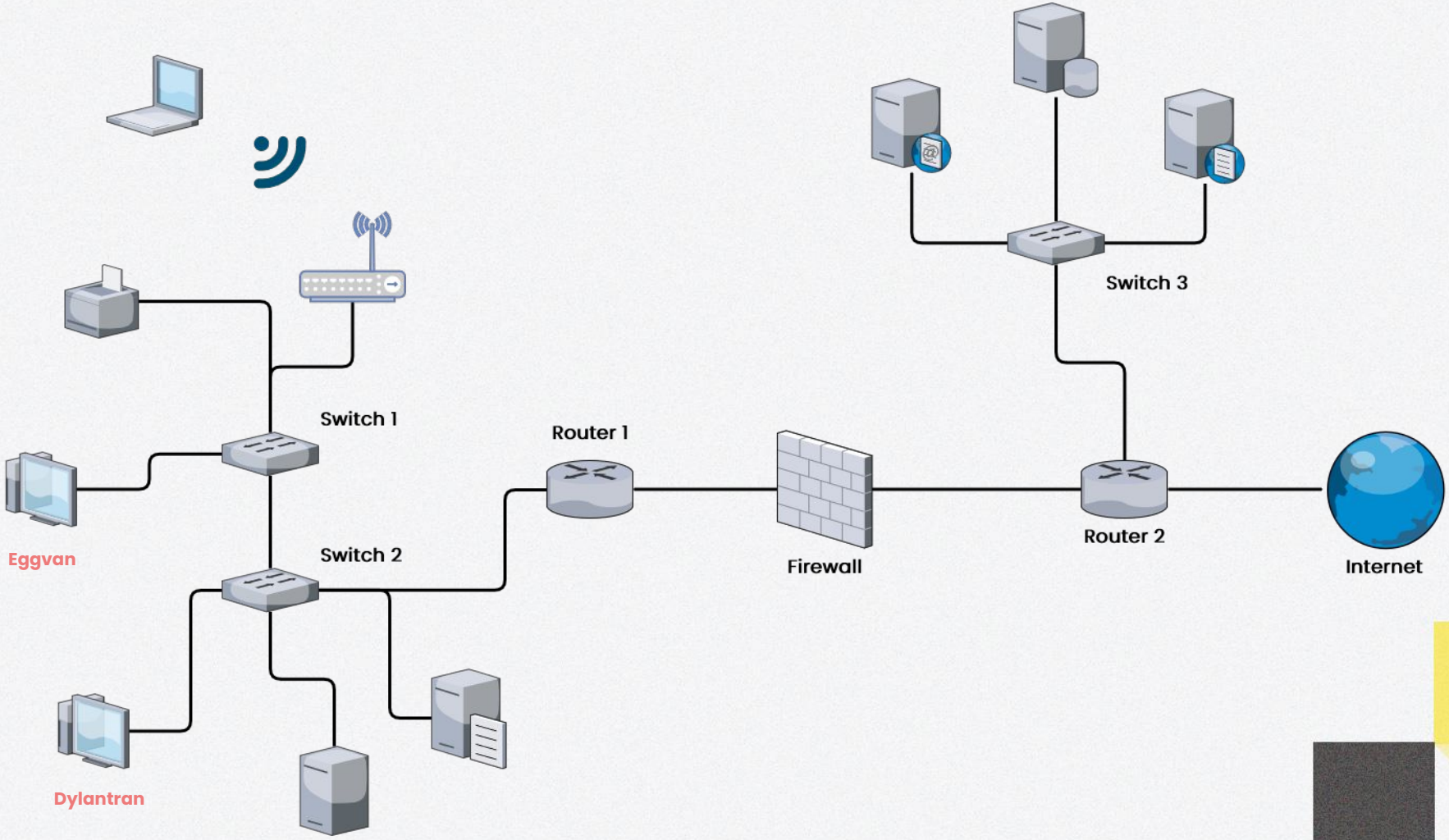
Disclaimers

- Do we expect you to be a networking expert after this talk?
  - No!
- Do we expect you to understand everything in this talk?
  - No!
- What are the expectations?
  - If you don't understand, **ASK!**
  - Learn stuff

01

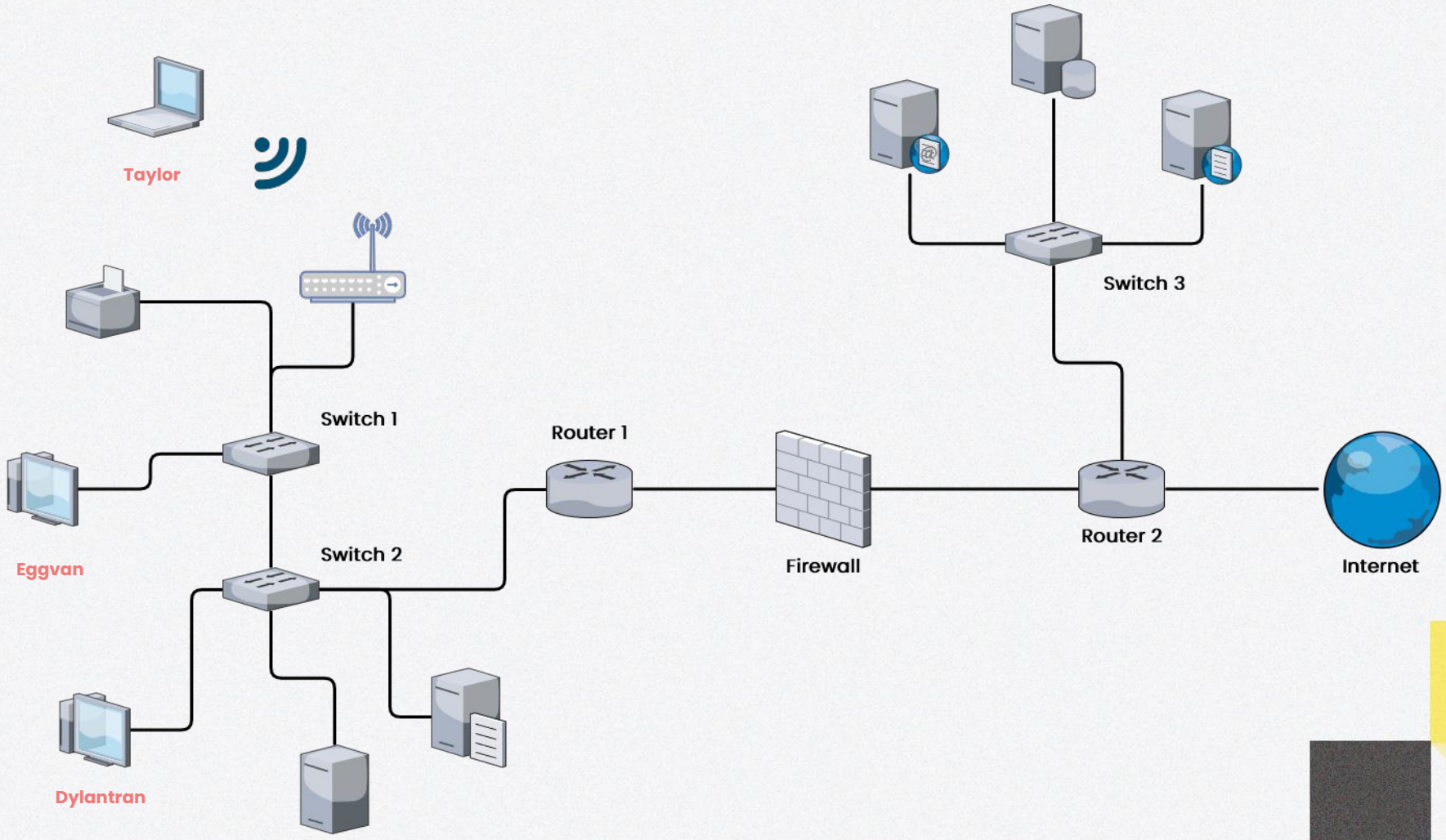
Intro to Networking

Networking is very cool, trust me


Switch 3
Switch 1
Router 1
Firewall
Router 2
Internet
Eggvan
Switch 2
Dylantran

Network Devices

- Can be anything on the network
  - Computers, phones, routers, switches, etc.
- Contains at least one **Network Interface Card,** or **NIC**
  - Wired
  - Wireless


Taylor
Switch 1
Eggvan
Switch 2
Dylantran
Router 1
Firewall
Switch 3
Router 2
Internet

Lingo

IP Addresses

Nodes

Gateways

End Devices

Router

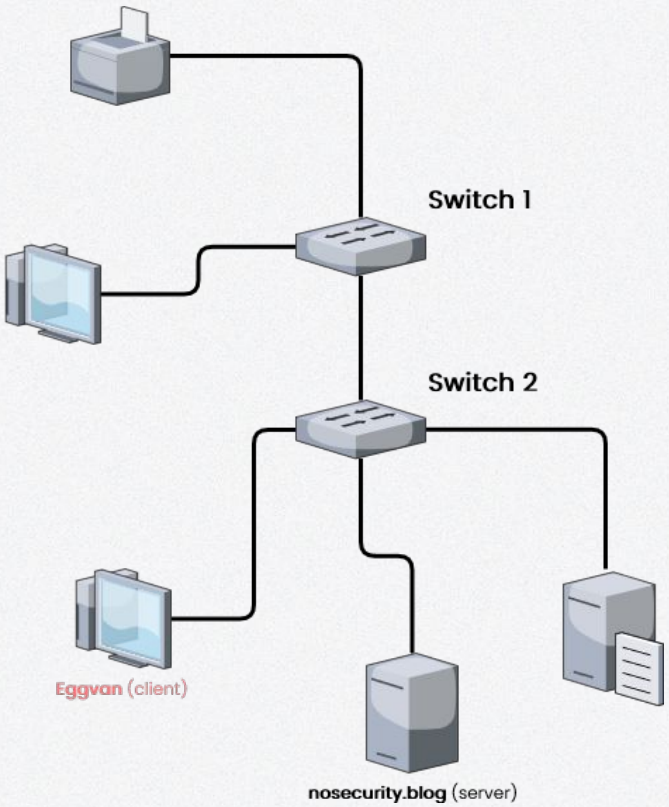
Firewall

Switch

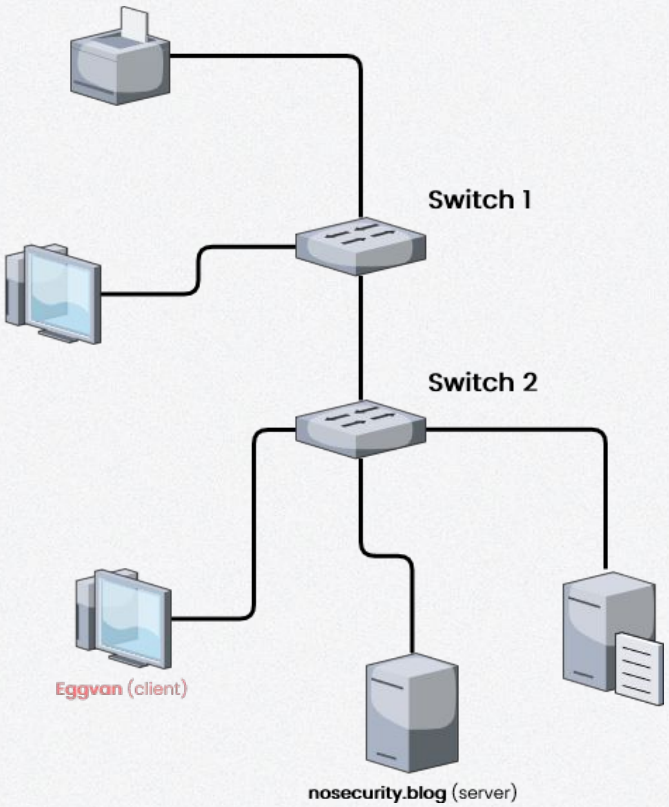
02

TCP/IP Model

Stacked



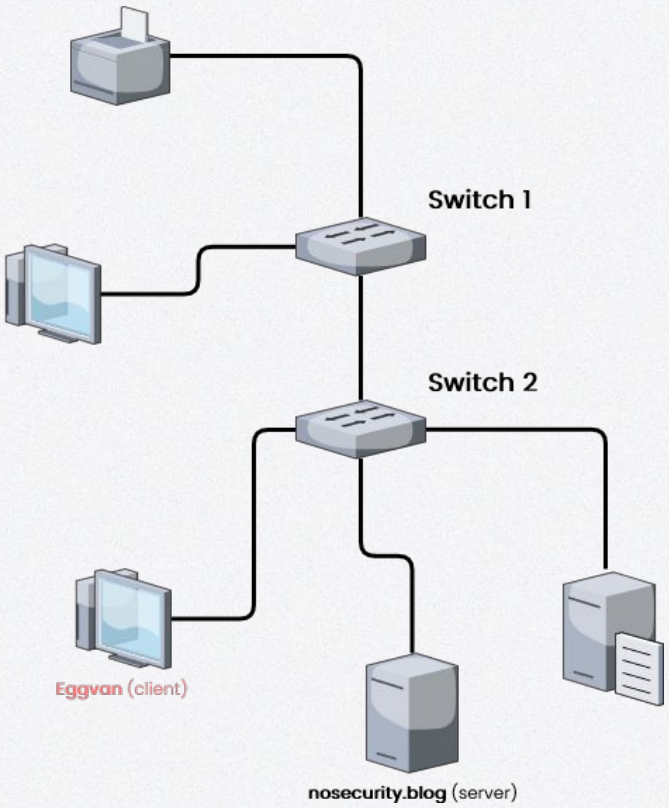
TCP/IP Model



TCP/IP Model

Application	Web Service/Application	

Eggvan's computer is requesting a service, or application (web, file, streaming, etc)

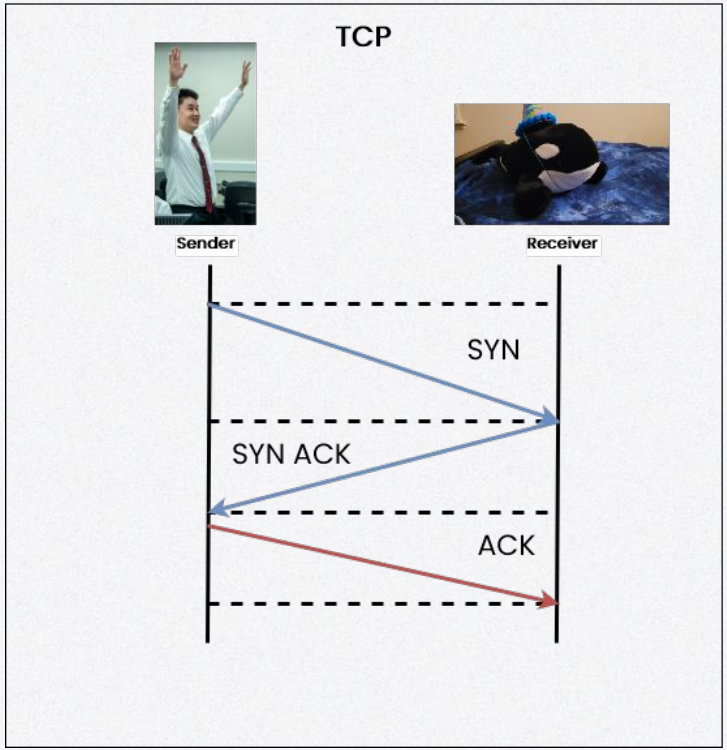


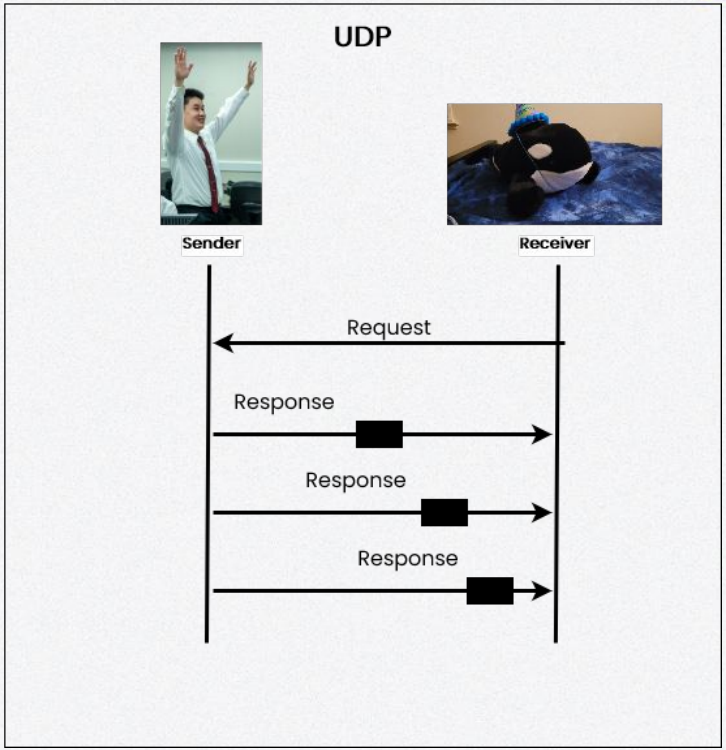
TCP/IP Model

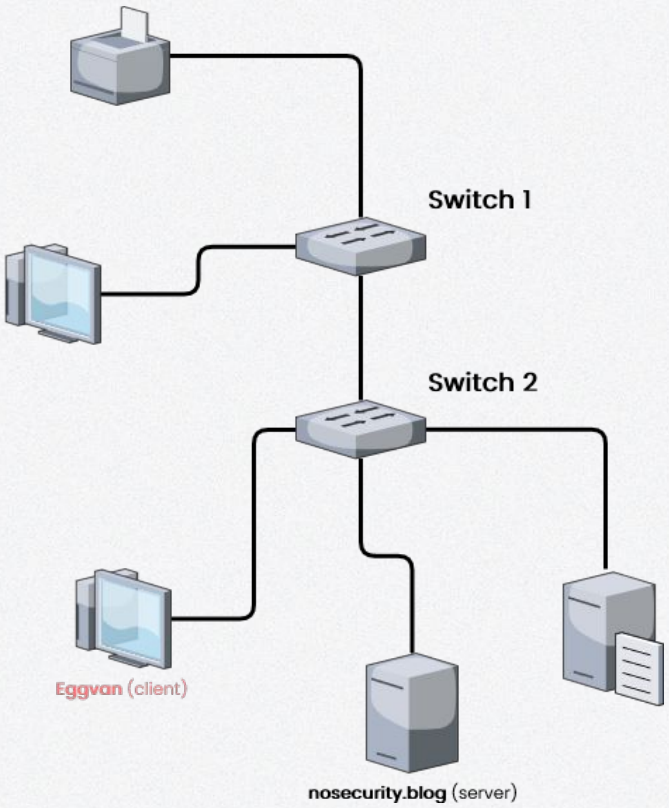
Application	Web Service/Application	
Transport	TCP Protocol	

TCP=Transmission Control Protocol, UDP=User Diagram Protocol

TCP vs UDP Communication



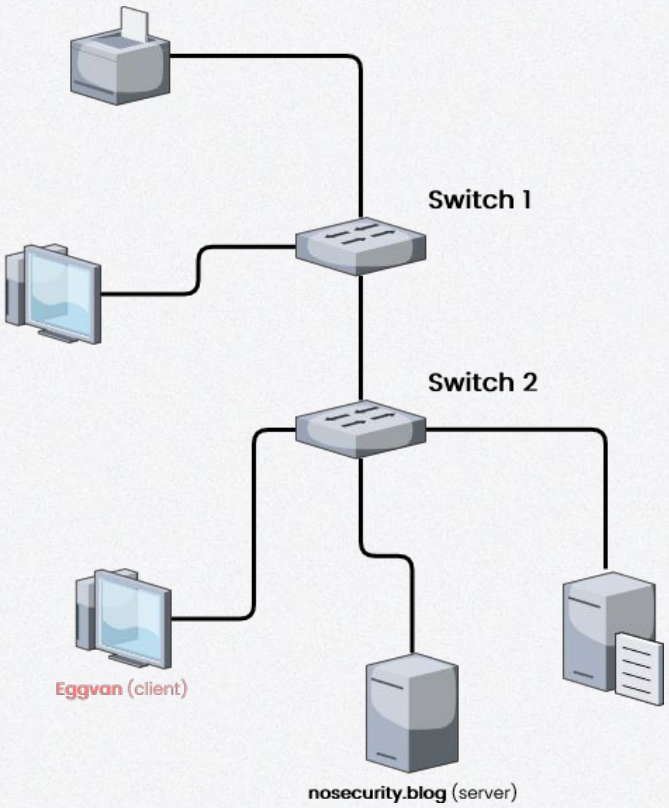




TCP/IP Model

Application	Web Service/Application	
Transport	TCP Protocol	
Network	IP Address	

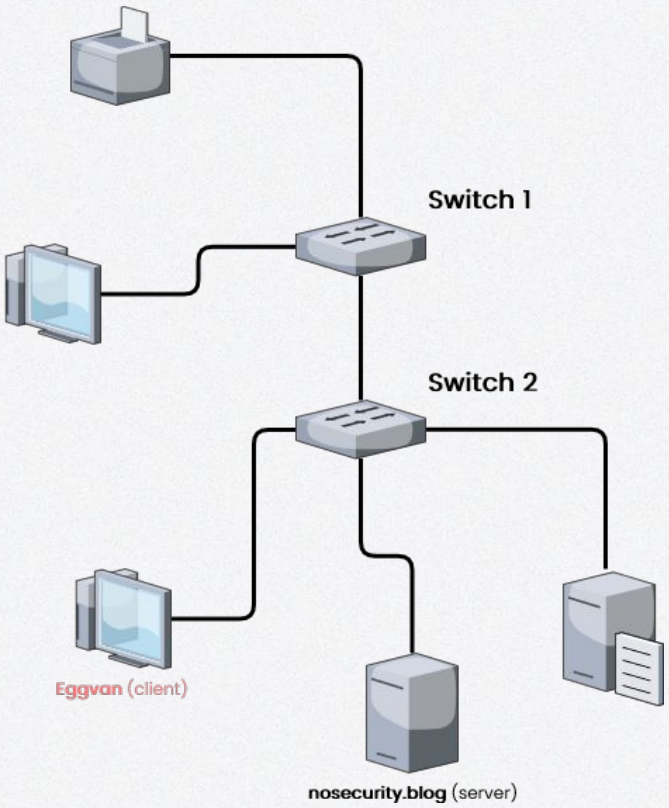
IP = Internet Protocol



TCP/IP Model

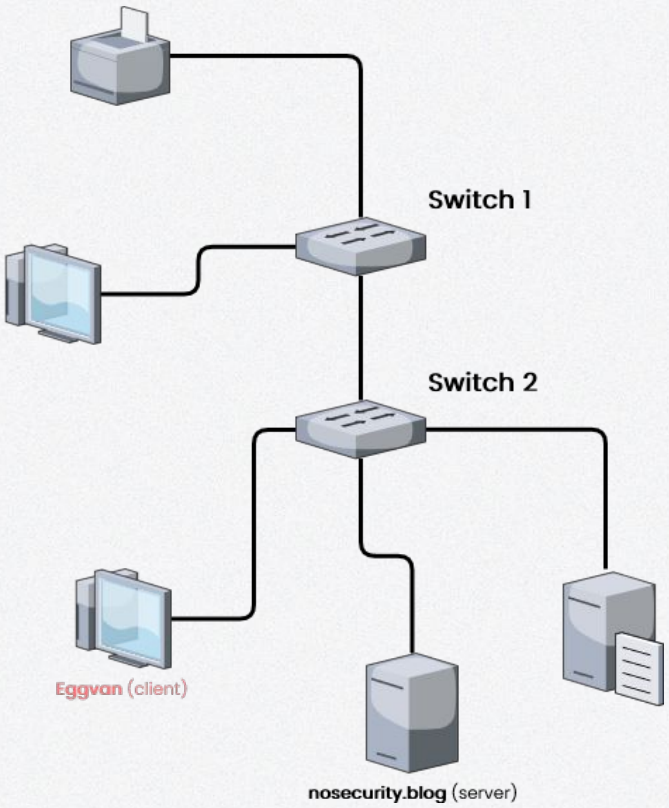
Application	Web Service/Application	
Transport	TCP Protocol	
Network	IP Address	
Data Link	MAC Address	

MAC = Media Access Control



TCP/IP Model

Application	Web Service/Application	
Transport	TCP Protocol	
Network	IP Address	
Data Link	MAC Address	
Physical	0's and 1's	



TCP/IP Model

Application	Web Service/Application	5
Transport	TCP Protocol	4
Network	IP Address	3
Data Link	MAC Address	2
Physical	0's and 1's	1

Troubleshooting Example

03

Ports and Services

wowww

TCP and UDP

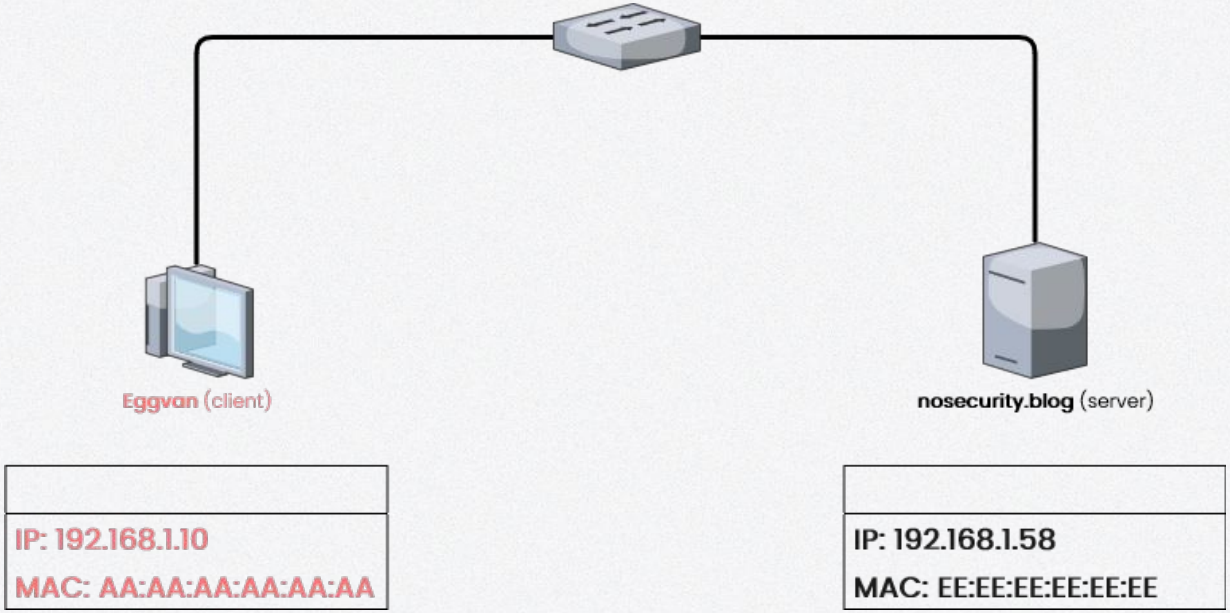
- Layer 4 protocols
- TCP - Slow but reliable
  - Synchronization
  - Flow control
  - TCP Handshake
- UDP - Fast but unreliable
  - No error-checking
  - No acknowledgements
  - Just send data

What are ports?

- Numbers that identify specific running services on a machine
- Common port numbers
  - TCP 20 and 21 - FTP
  - TCP 22 - SSH
  - TCP 25 - SMTP
  - UDP 53 - DNS
  - TCP 80 - HTTP
  - TCP 443 - HTTPS
  - etc.

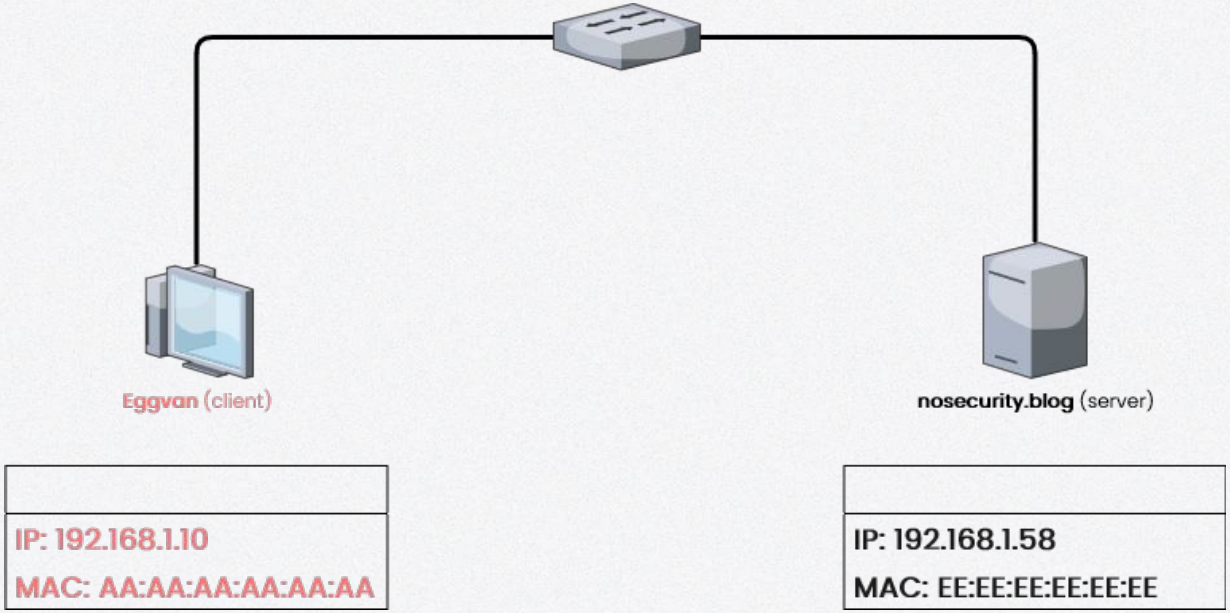
Walking thru a connection

- Snail mail
  - Sender's address
  - Recipient's address
- Networking does the same thing



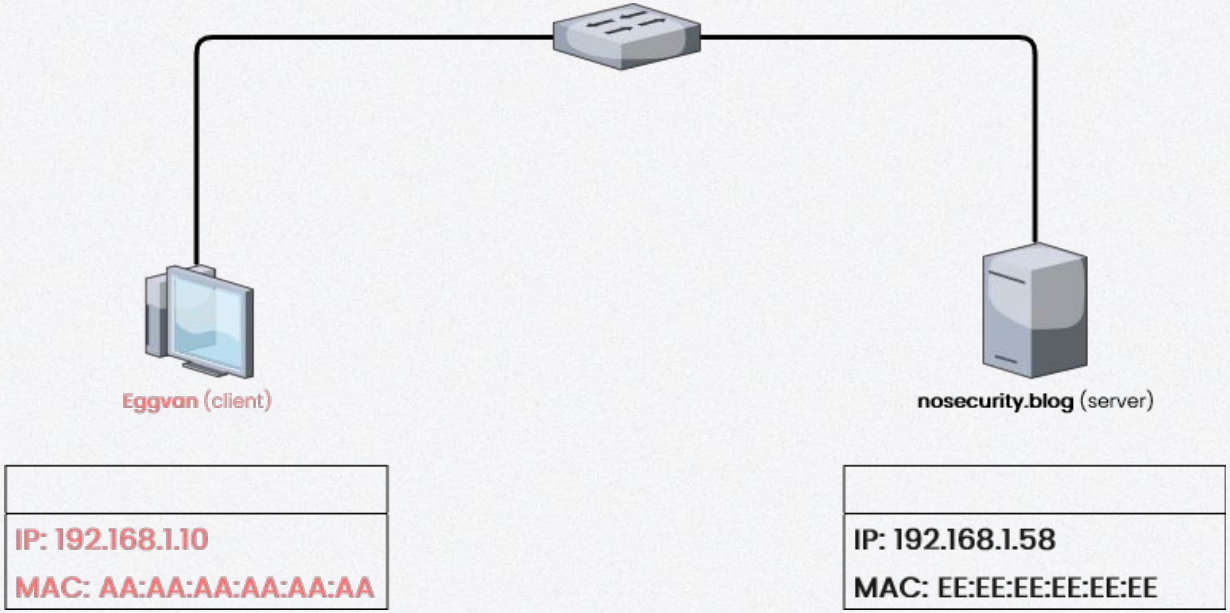
Source MAC	Destination MAC	Source IP	Destination IP	Source Port	Destination Port

Eggvan wants to visit the epic website nosecurity.blog



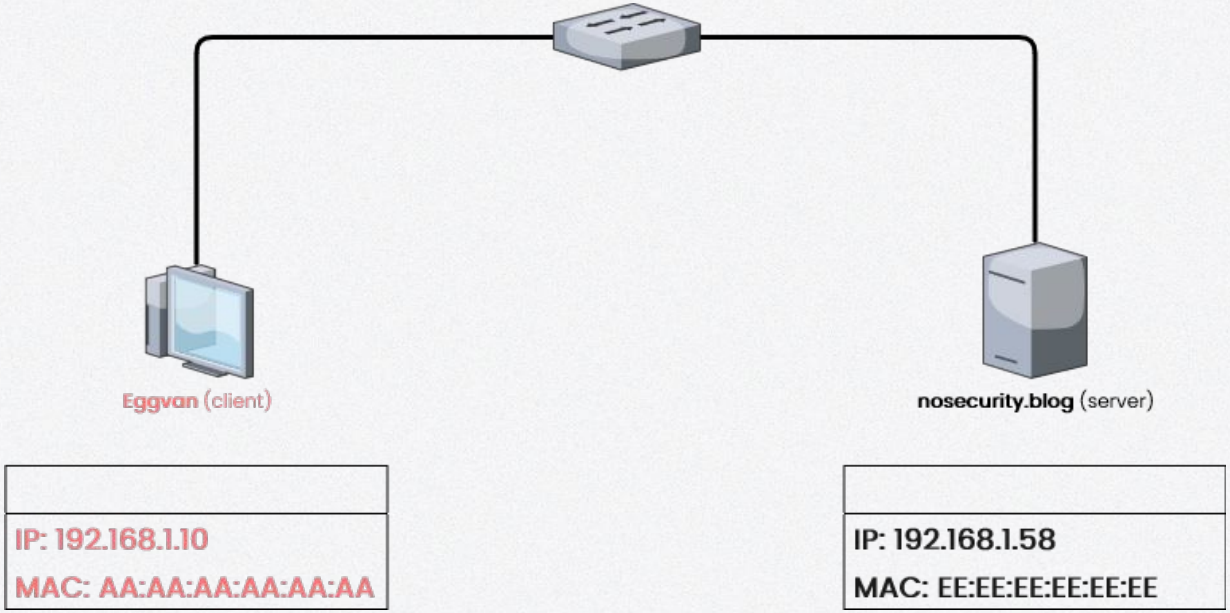
Source MAC	Destination MAC	Source IP	Destination IP	Source Port	Destination Port
AA:AA:AA:AA:AA:AA					

Eggvan wants to visit the epic website nosecurity.blog



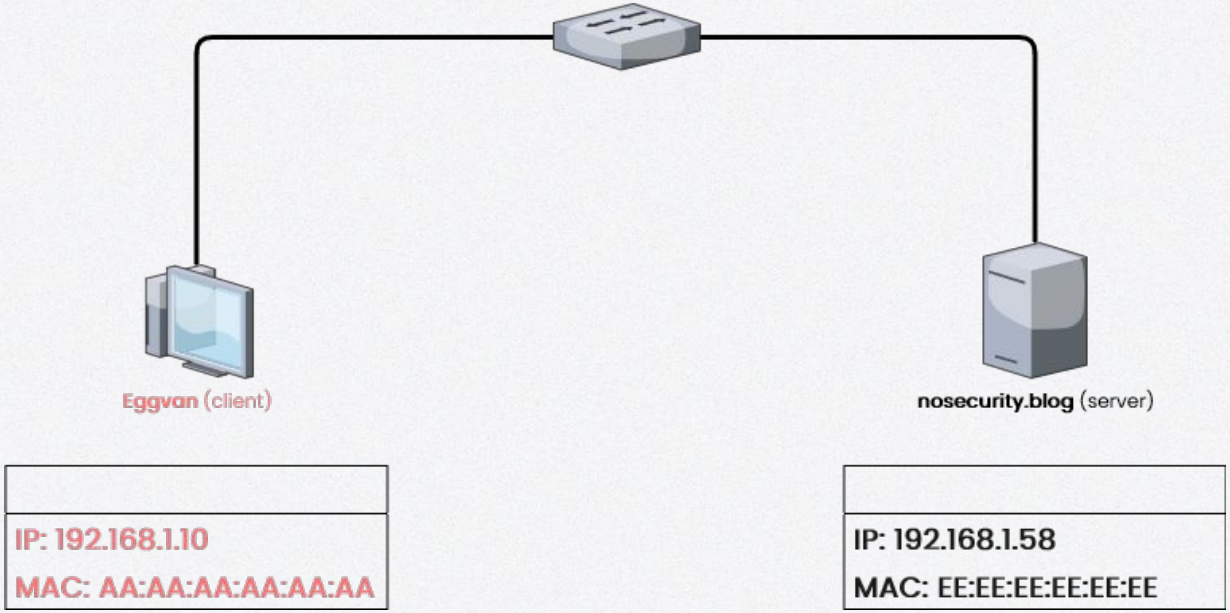
Source MAC	Destination MAC	Source IP	Destination IP	Source Port	Destination Port
AA:AA:AA:AA:AA:AA	EE:EE:EE:EE:EE:EE				

Eggvan wants to visit the epic website nosecurity.blog



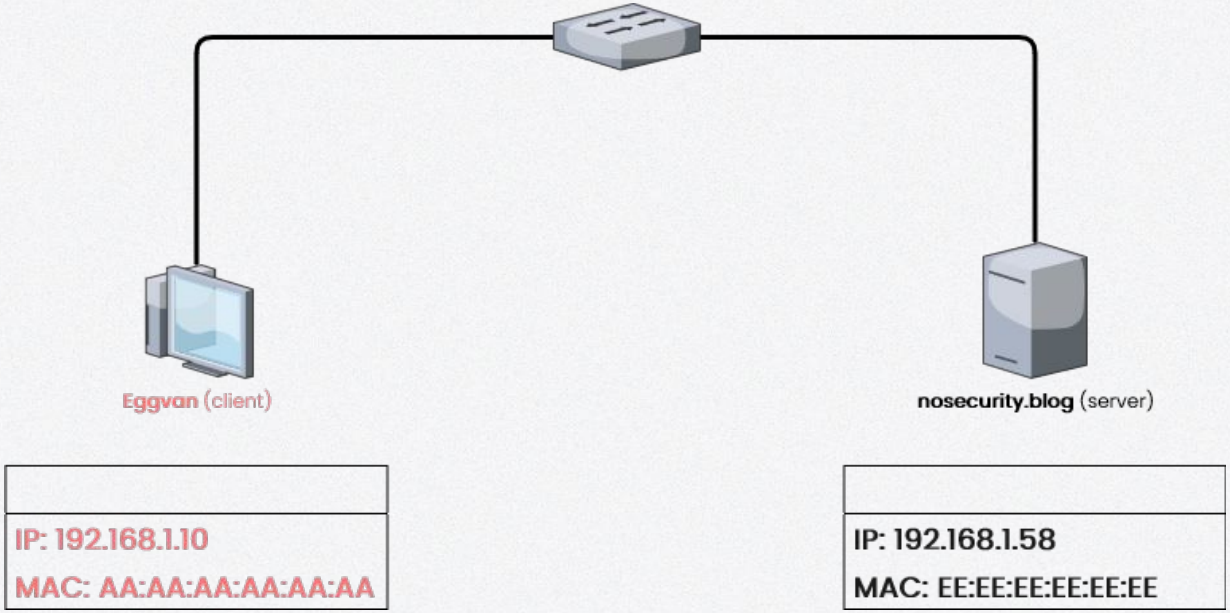
Source MAC	Destination MAC	Source IP	Destination IP	Source Port	Destination Port
AA:AA:AA:AA:AA:AA	EE:EE:EE:EE:EE:EE	192.168.1.10			

Eggvan wants to visit the epic website nosecurity.blog



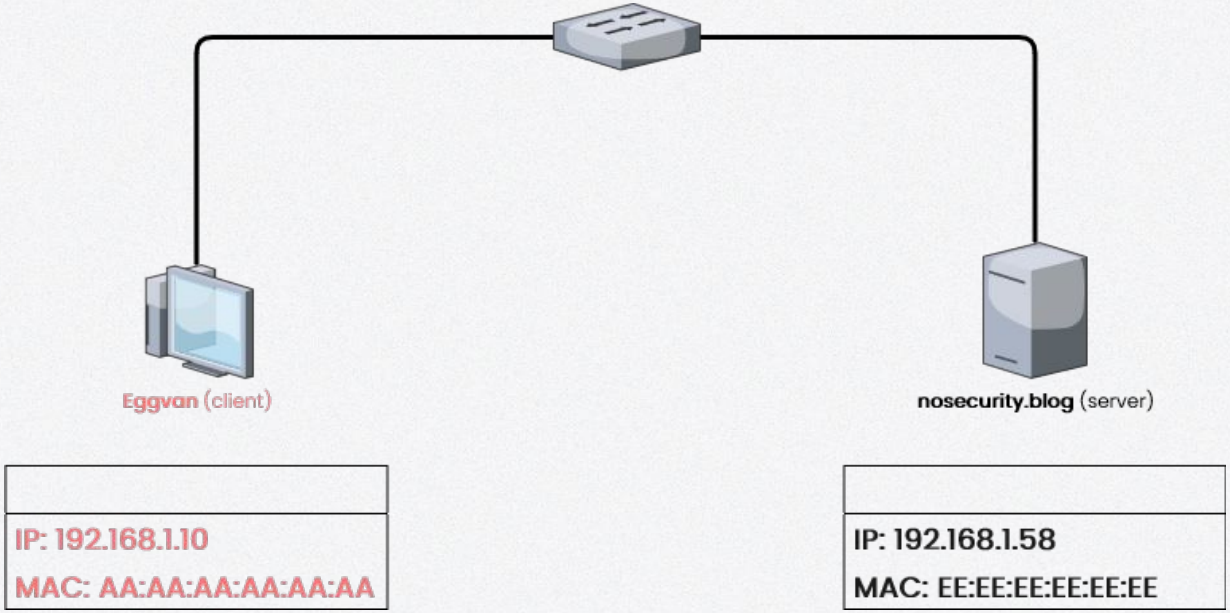
Source MAC	Destination MAC	Source IP	Destination IP	Source Port	Destination Port
AA:AA:AA:AA:AA:AA	EE:EE:EE:EE:EE:EE	192.168.1.10	192.168.1.58		

Eggvan wants to visit the epic website nosecurity.blog



Source MAC	Destination MAC	Source IP	Destination IP	Source Port	Destination Port
AA:AA:AA:AA:AA:AA	EE:EE:EE:EE:EE:EE	192.168.1.10	192.168.1.58		80

Eggvan wants to visit the epic website nosecurity.blog

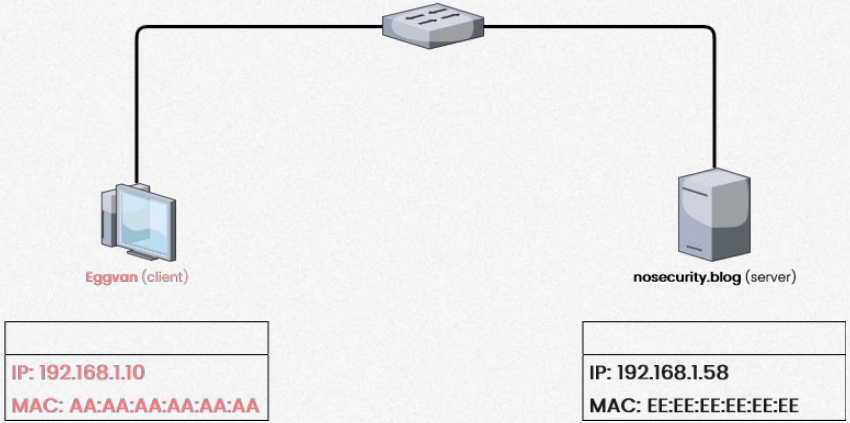


Source MAC	Destination MAC	Source IP	Destination IP	Source Port	Destination Port
AA:AA:AA:AA:AA:AA	EE:EE:EE:EE:EE:EE	192.168.1.10	192.168.1.58	**57361**	80

Eggvan wants to visit the epic website nosecurity.blog

What are sockets?

Each end of a connection, basically a pairing between an IP and a port.



192.168.1.10:57138 → 192.168.1.58:80

why

- Identify normal/abnormal traffic
  - Is it coming from scoring engine/orange team? Or is it red team?
- Troubleshooting services
  - Firewall issue? Service disabled?

Common Ports

HTTP/HTTPS - 80/443

SSH - 22

Dylantran - 1337

FTP - 20/21

DNS - 53

mysql - 3306

Common Ports - pt. 2

RDP - 3389

LDAP - 389/636

SMB - 139/446

SMTP - 25

Common Ports - pt. 3

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-08 00:31 CDT
Nmap scan report for 172.16.25.33
Host is up (0.00038s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    nginx 1.10.1
2020/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
2022/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
2222/tcp open  http    nginx 1.10.1
```

Ports & Services Review

- TCP and UDP
- Ports - numbers that identify a running service/application
- Common ports
- Source and destination addresses/ports
    - **Ephemeral ports** on client-side
    - Sockets

04

Subnetting

"Time to dance 💃"

IPv4 Address and Subnet Mask

IPv4 address

192.168.1.100

255.255.255.0

Subnet Mask

Binary

192 . 168 . 1 . 100

11000000.10101000.00000001.01100100

Octet

255 . 255 . 255 . 0

11111111.11111111.11111111.00000000

Binary pt 2

192 . 168 . 1 . 100

$\underbrace{11000000}_{\text{Octet}}$.10101000.00000001.01100100

1	1	0	0	0	0	0	0
128	64	32	16	8	4	2	1

= 192

Network/Host bits

Network bits | Host bits

11000000.10101000.00000001 | 01100100

11111111.11111111.11111111 | 00000000

Identify Ranges

Network bits | Host bits

11000000.10101000.00000001 | 01100100

11111111.11111111.11111111 | 00000000

11000000.10101000.00000001.00000000

Network ID

192.168.1.0/24

CIDR

Block Size

Range of usable IPv4 addresses

11000000.10101000.00000001.11111111

Broadcast Address

192.168.1.255

Subnetting Calculator

https://www.calculator.net/ip-subnet-calculator.html

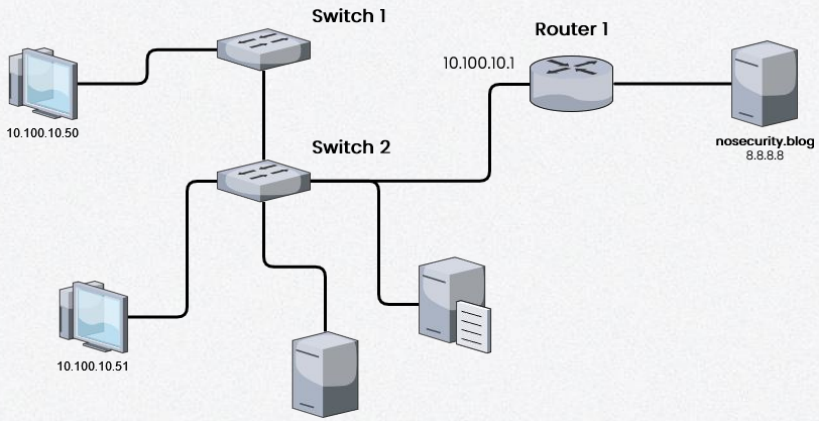
why

- Understand your network
  - Knowing your network is a huge advantage in cyber defense

Subnetting Review

- Subnet mask - divides an IP address into network bits and host bits
- Network bits - bits that belong to the network address
- Host bits - bits that belong to the host
- Block size - range of IP addresses
- Special addresses
  - Network ID/address - the first address in a block (host bits = 0)
  - Broadcast address - the last address in a block (host bits = 1)

Default Gateway



Process:

1. Host wants to view nosecurity.blog
2. Host does not know ip address of nosecurity.blog
3. Host asks it's DNS server (8.8.8.8)
4. Host notices that 8.8.8.8 is NOT on the same network as the host
5. Host sends it to Default Gateway
6. Default Gateway contacts DNS server
7. DNS Server responds with IP of nosecurity.blog

NAT

Problem

Not enough IP addresses

Solution

Translate Private ips to public

IPv4

32 bits each

Total range = 4.3 billion possible addresses

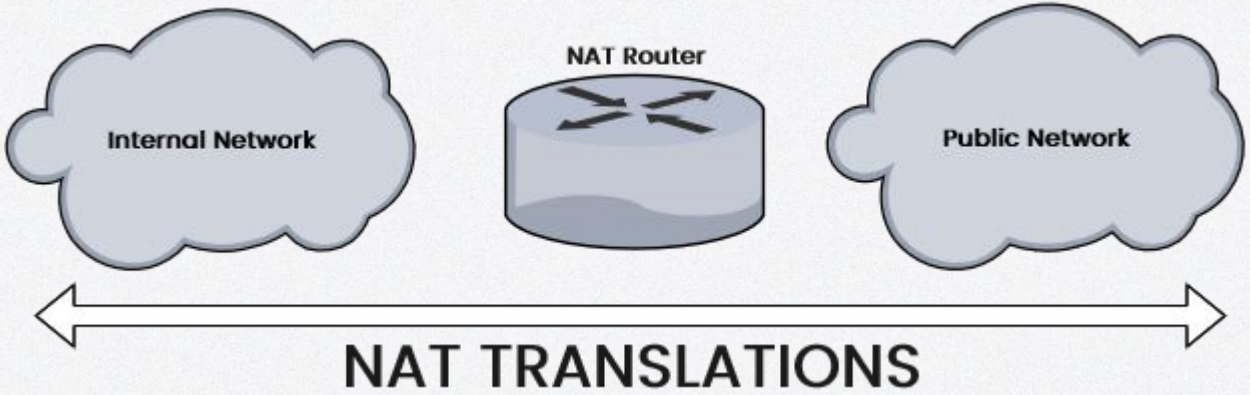
8.8.8.8

IPv6

128 bits each

Total range = 340 undecillion possible addresses

2001:db8::ff00:42:8329



- **Class A:** 10.0.0.0 - 10.255.255.255
- **Class B:** 172.16.0.0 - 172.31.255.255
- **Class C:** 192.168.0.0 - 192.168.255.255

05

Fyrwall

FIREWALL TIME BABEYY

Block IPs

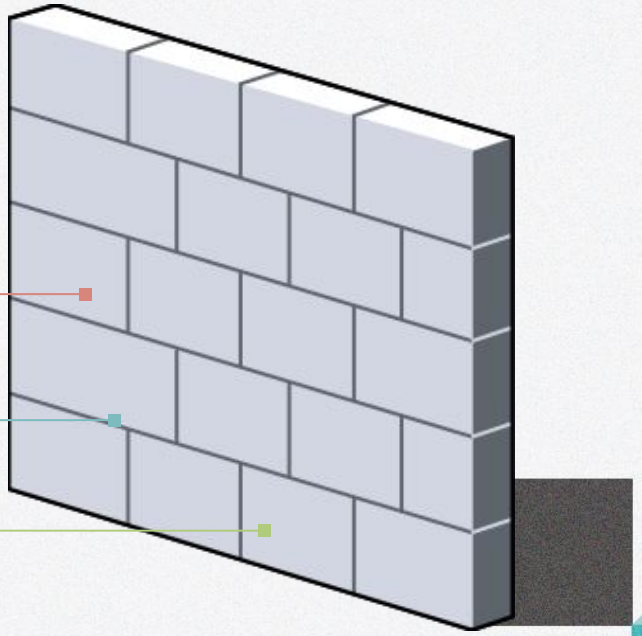
Can block a whole subnet or individual.

Block Ports

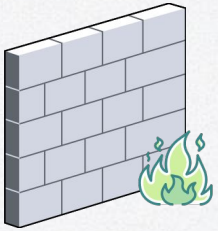
Block which ports the external network can access on the LAN

Filtering

Ingress and Egress filtering rules.

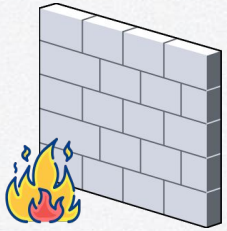


NGFW vs Traditional

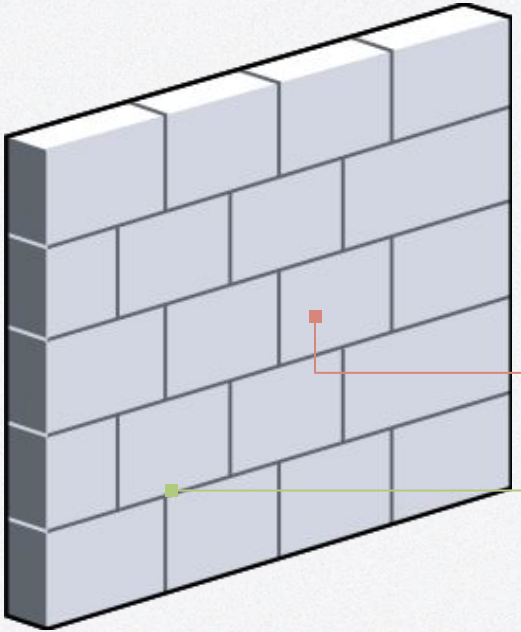


- Stateful Inspection on incoming and outgoing traffic
- Comprehensive application control and visibility
- L2-L7
- Easy to install, configure, integrate security tools, reducing administrative controls
- SSL traffic can be decrypted and inspected.
- IPS & IDS are integrated

- Stateful Inspection on incoming and outgoing traffic
- Partial application control and visibility only
- L2-L4 Only
- Managing security tools separately is $$$
- Cannot decrypt and inspect SSL traffic
- Integrated IPS and IDS are deployed separately in traditional firewalls



Stateless vs Stateful



Stateless

ACL. Looks at
Individual packets.

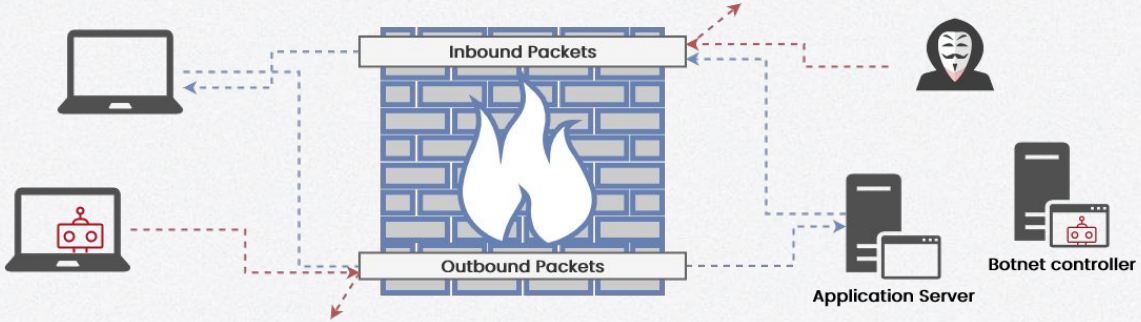
Stateful

Traffic patterns and flows.
Remembers connections.

FW Example

Inbound
- Only allow required services
- Allow certain subnets
- Allow certain ip addresses

Outbound
- Block everything going outbound (break internet)



FW Example 2

Floating WAN LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	21 /80 KiB	IPv4 *	172.16.109.39	*	*	*	*	none			

Add Add Delete Save Separator

FW Example 3

Floating WAN LAN

Rules (Drag to Change Order)

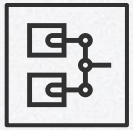
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0 /3.83 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
✗	0 /0 B	IPv4 *	*	*	*	*	*	none			
✓	3 /2.07 GiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Save Separator

Firewall Demo

Firewall Admin Roles

Secure



Filter

Monitor

06

Blooket

07

Lab

Lab Time babeyy

- Go to this document https://da.gd/ccdc3lab and follow instructions
- If you still need vpn: **https://da.gd/ccdcvpns -> pin 000000**
- **Once you finish Troubleshooting dm jacob**

Thanks!

Any questions? Questions are very cool. Please ask questions I am very lonely :((