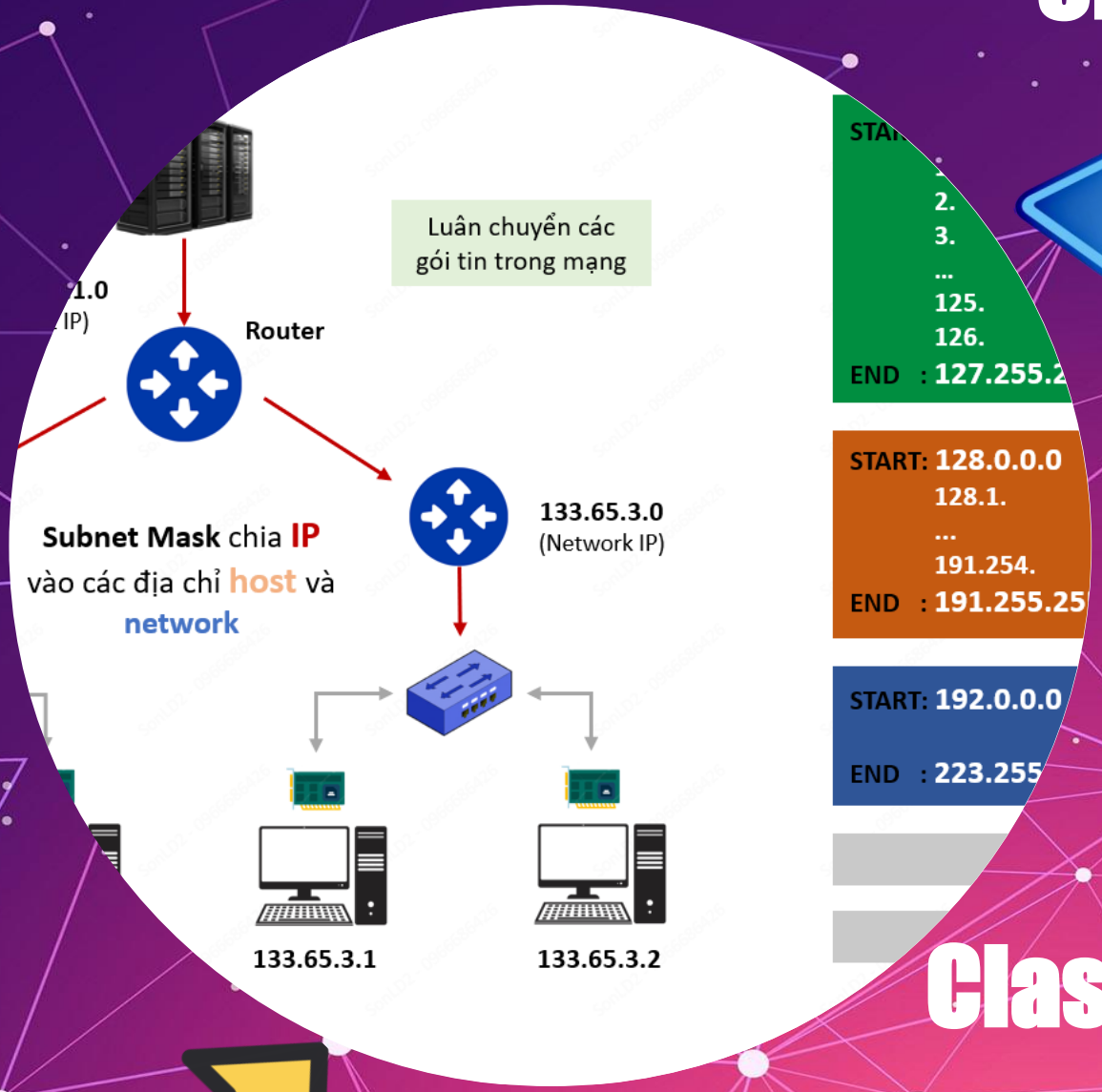
Class C

Class A

Basic Networking

# Subnet Mask



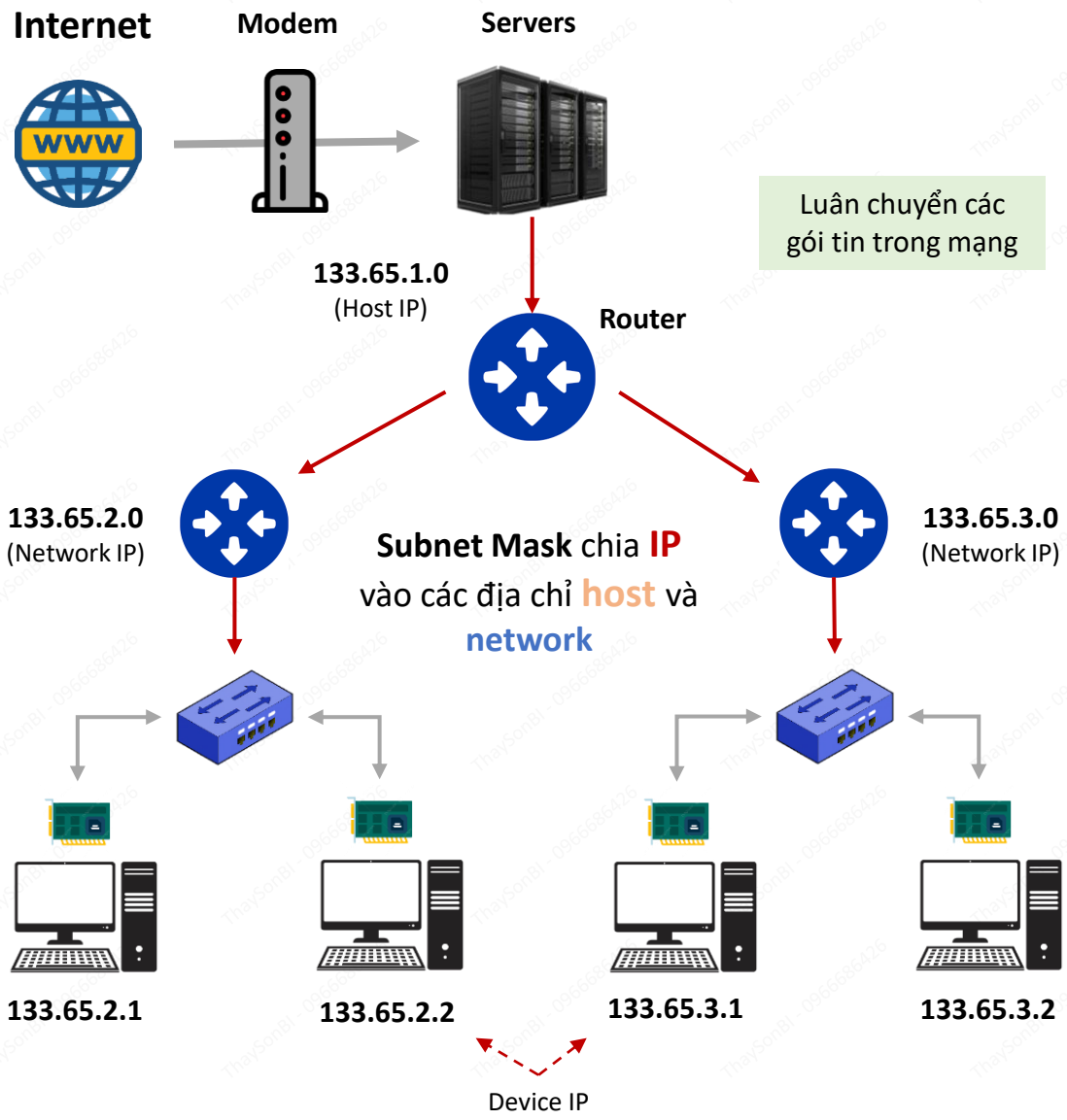

Class B

Class D, E

amazon web services™

Amazon Web Service - Training

# LAYER 3 – SUBNET MASK




**A**

START: 0.0.0.0
1.
2.
3.
...
125.
126.
END : 127.255.255.255

Network: 128
IPs per NW: 16,777,216

**B**

START: 128.0.0.0
128.1.
...
191.254.
END : 191.255.255.255

Network: 16,384
IPs per NW: 65,536

**C**

START: 192.0.0.0
END : 223.255.255.255

Network: 2,097,152
IPs per NW: 256

**Class D**

**Class E**

Basic Networking

# Layer 3 - CIDR

IPv4

Avoid Waste

Superneting

Popular

amazon web services™

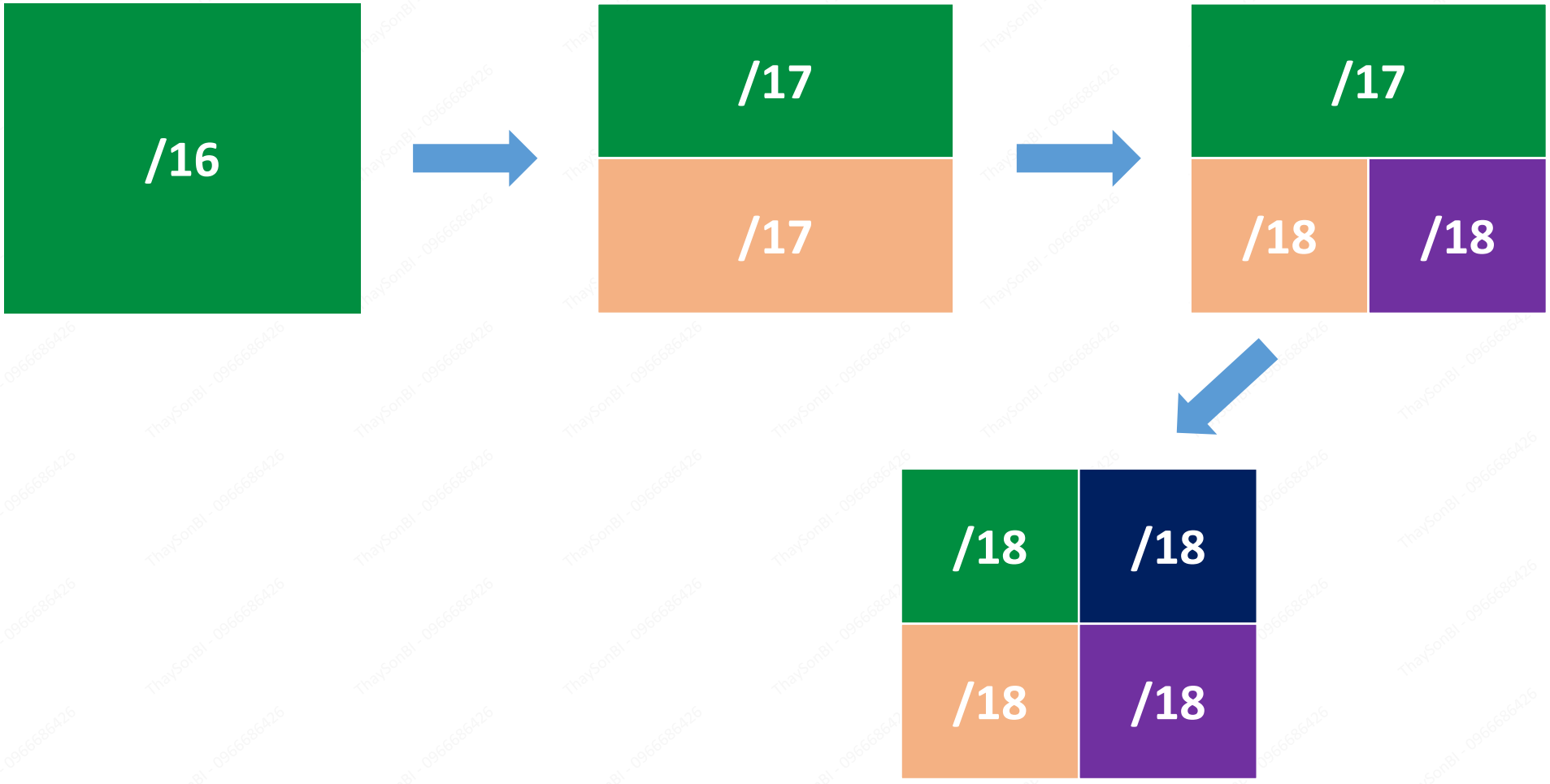
Amazon Web Service - Training

# LAYER 3 – CIDR


| Tiền tố | Số IPs | Ví dụ |
|---|---|---|
| /16 | 65536 | 192.168.0.0/16 → Start: 192.168.0.0 End: 192.168.255.255 |
| /17 | 32768 | 192.168.0.0/17 → Start: 192.168.0.0 End: 192.168.127.255 |
| /18 | 16384 | 192.168.0.0/18 → Start: 192.168.0.0 End: 192.168.63.255 |
| /19 | 8192 | 192.168.0.0/19 → Start: 192.168.0.0 End: 192.168.31.255 |
| /20 | 4096 | 192.168.0.0/20 → Start: 192.168.0.0 End: 192.168.15.255 |
| /21 | 2048 | 192.168.0.0/21 → Start: 192.168.0.0 End: 192.168.7.255 |
| /22 | 1024 | 192.168.0.0/22 → Start: 192.168.0.0 End: 192.168.3.255 |
| /23 | 512 | 192.168.0.0/23 → Start: 192.168.0.0 End: 192.168.1.255 |
| /24 | 256 | 192.168.0.0/24 → Start: 192.168.0.0 End: 192.168.0.255 |
| /25 | 128 | 192.168.0.0/25 → Start: 192.168.0.0 End: 192.168.0.127 |
| /26 | 64 | 192.168.0.0/26 → Start: 192.168.0.0 End: 192.168.0.63 |
| /27 | 32 | 192.168.0.0/27 → Start: 192.168.0.0 End: 192.168.0.31 |
| /28 | 16 | 192.168.0.0/28 → Start: 192.168.0.0 End: 192.168.0.15 |

**CIDR** là IP address scheme (phương thức định vị địa chỉ IP) giúp cải thiện việc phân bổ địa chỉ IP trong mạng

# LAYER 3 – SUBNETING

Basic Networking

# Route Table & Route

Router

Hop

Destination

Interface

Amazon Web Service - Training

# LAYER 3 – ROUTE TABLE & ROUTE

**Router** định tuyến packet từ **SRC** đến **DST** (đóng gói packet ở L2)

**Package SRC 192.168.1.123** (Home)

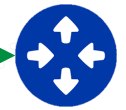
**Destination 55.127.1.45**

1

2

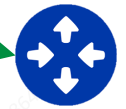
4

55.127.1.0/24



52.67.78.0/24

**Route** cho biết nơi nào sẽ gửi packet đến



52.67.78.0/24

**Router** có rất nhiều **route** (interface) trong **route table** để chọn lựa

**Router** sẽ so sánh **destination IP** với **route table** để tìm ra địa chỉ đích chính xác nằm ở đâu. Packet sẽ được gửi đến **Next Hop/Target**

3

| Destination | Next Hop / Target |
|---|---|
| **55.127.1.0/24** | **55.127.1.123** |
| 0.0.0.0/0 | 52.67.78.1 |
| 51.223.10.0/24 | 52.67.78.1 |

Basic Networking

# Traffic Routing

Hop

Router

Destination

Interface

amazon web services™

Amazon Web Service - Training

NETWORKING BASIC

# LAYER 3 – ROUTING

## Lam Network

(D2) **133.33.3.8**

Frame được gửi đến D2. D2 tạo ra packet **P2** chứa IP đích

**ARP*** tìm địa chỉ MAC của D2

**Subnet Mask** và **IP đích** xác nhận D1 và D2 nằm cùng mạng nội bộ

**F1** **P1**

(D1) **133.33.3.7**

**F2** **P2**

R1

1. **Subnet Mask** và **IP đích** cho biết **D3** không nằm trong mạng Lam (Local)
2. **ARP** tìm kiếm địa chỉ MAC của R1
3. **P2** chứa địa chỉ D3 được đóng gói cùng với frame **F2** sẽ chuyển từ D2 sang R1

## Cam Network

4. R1 xóa frame **F2** chỉ giữ lại **P2** và tìm kiếm địa chỉ IP đích của **D3**

**P2** → 5 → **F3** **P2**

R1 biết con đường để đến Xám Network (nơi chứa D3). Nó tạo ra frame F3 và dùng R2 lúc này là **"Next IP Hop"** để chuyển frame F3 đi. **P2** không thay đổi và nằm cùng khối frame F3 sẽ chuyển sang Xám Network

6. F3 gửi cho R2 địa chỉ MAC

**F3** **P2**

R2

## Xám Network

7. R2 xóa frame **F3**, giữ lại **P2**

**P2** → **F4** **P2**

8. R2 xác thực địa chỉ IP đích của P2 nằm trong cùng network với D3 và sử dụng ARP để lấy địa chỉ MAC của D3. Nó tạo ra frame F4 với địa chỉ MAC đích của D3 và khối đã đóng gói **P2**

9. F4 chuyển tới D3, **P2** hoàn thành chuyến đi của mình

**F4** **P2**

(D3) **119.18.35.60**

* **ARP** (Address Resolution Protocol) là giao thức mạng được dùng để **tìm ra địa chỉ phần cứng (địa chỉ MAC)** của thiết bị từ một địa chỉ IP nguồn

No Order

Break

Basic Networking

# Layer 3 - Problems


Miss

Latency

amazon web services™

Amazon Web Service - Training

# LAYER 3 – PROBLEMS

Source IP

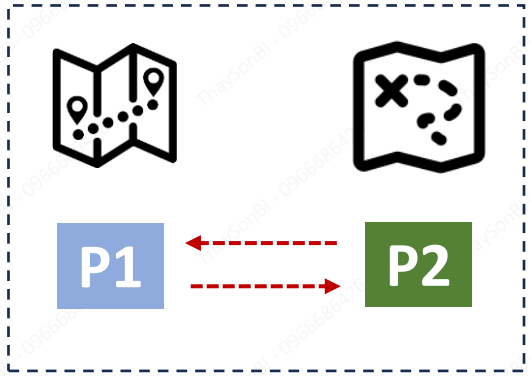
P5 P4 P3 P2 P1

Mỗi **packet** được định tuyến một cách **độc lập** với nhau

P3 P2 P1

Ở layer 3 packet **có source và destination** IP nhưng **không có phương thức** chia tách, cũng như **cơ chế kiểm soát** (thất thoát packet)

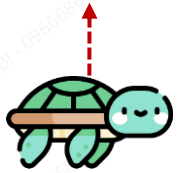
Các packet **đang định hướng** (routing) có thể **gây trễ** cho các packet **đang truyền đi**




Sự khác biệt về con đường có thể dẫn tới phá vỡ **thứ tự của packet** tại điểm đích. L3 **không có cơ chế sắp xếp**

Destination IP

P5 P4 X



Layer 3 **không đảm bảo** giao tiếp một cách hoàn toàn tin cậy. Packet có thể bị **mất** trên đường di chuyển

Basic Networking

# OSI Layer 4

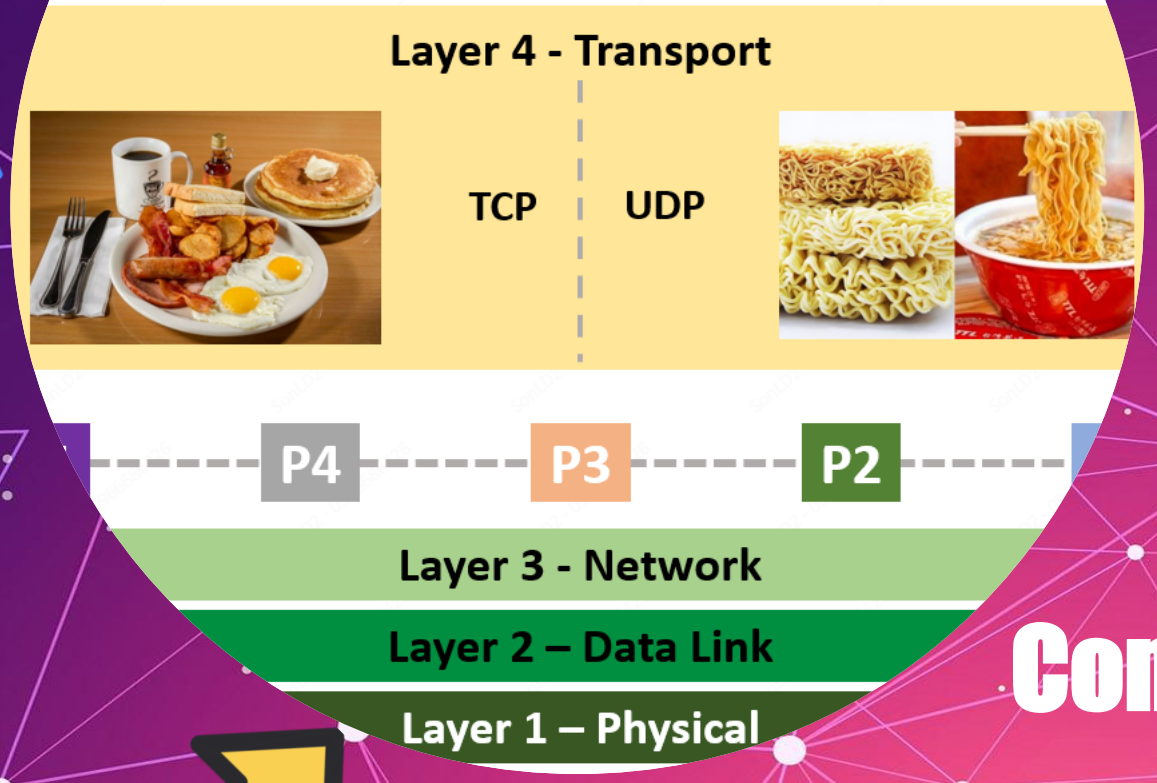
TCP

UDP

Transport

Compare

| Protocol | UDP |
| --- | --- |
| Định hướng kết nối | Giao thức kém kết nối |
| ụ trách nhiệm cung cấp dữ liệu | Chỉ thực hiện kiểm tra lỗi cơ bả |
| Truyền dữ liệu theo thứ tự | Truyền **KHÔNG** theo thứ tự, có lớp |
| Có thể gửi lại packet nếu lỗi | Không thể truyền lại các packet |
| Tốc độ chậm, khối lượng nặng | Tốc độ nhanh và hiệu quả |



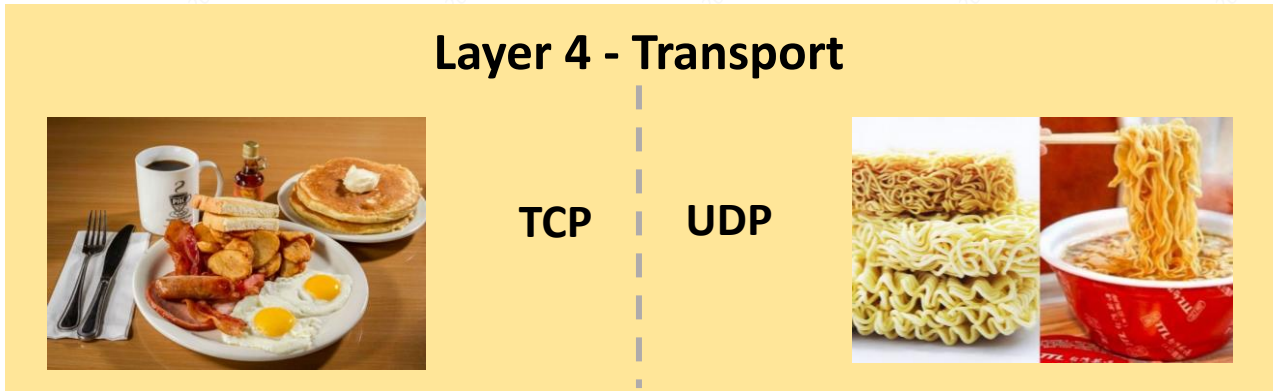

amazon web services™

Amazon Web Service - Training

# LAYER 4 – TRANSPORT

| TCP – Transmission Control Protocol | UDP – User Datagram Protocol |
|---|---|
| Định hướng kết nối | Giao thức kém kết nối |
| Hỗ trợ kiểm tra lỗi và chịu trách nhiệm cung cấp dữ liệu | Chỉ thực hiện kiểm tra lỗi cơ bản nhất qua checksum |
| Truyền dữ liệu theo thứ tự | Truyền **KHÔNG** theo thứ tự, có lớp ứng dụng sẽ sắp xếp |
| Có thể gửi lại packet nếu lỗi | Không thể truyền lại các packet |
| Tốc độ chậm, khối lượng nặng | Tốc độ nhanh và hiệu quả |

**Chậm**
nhưng
**Chắc Chắn**



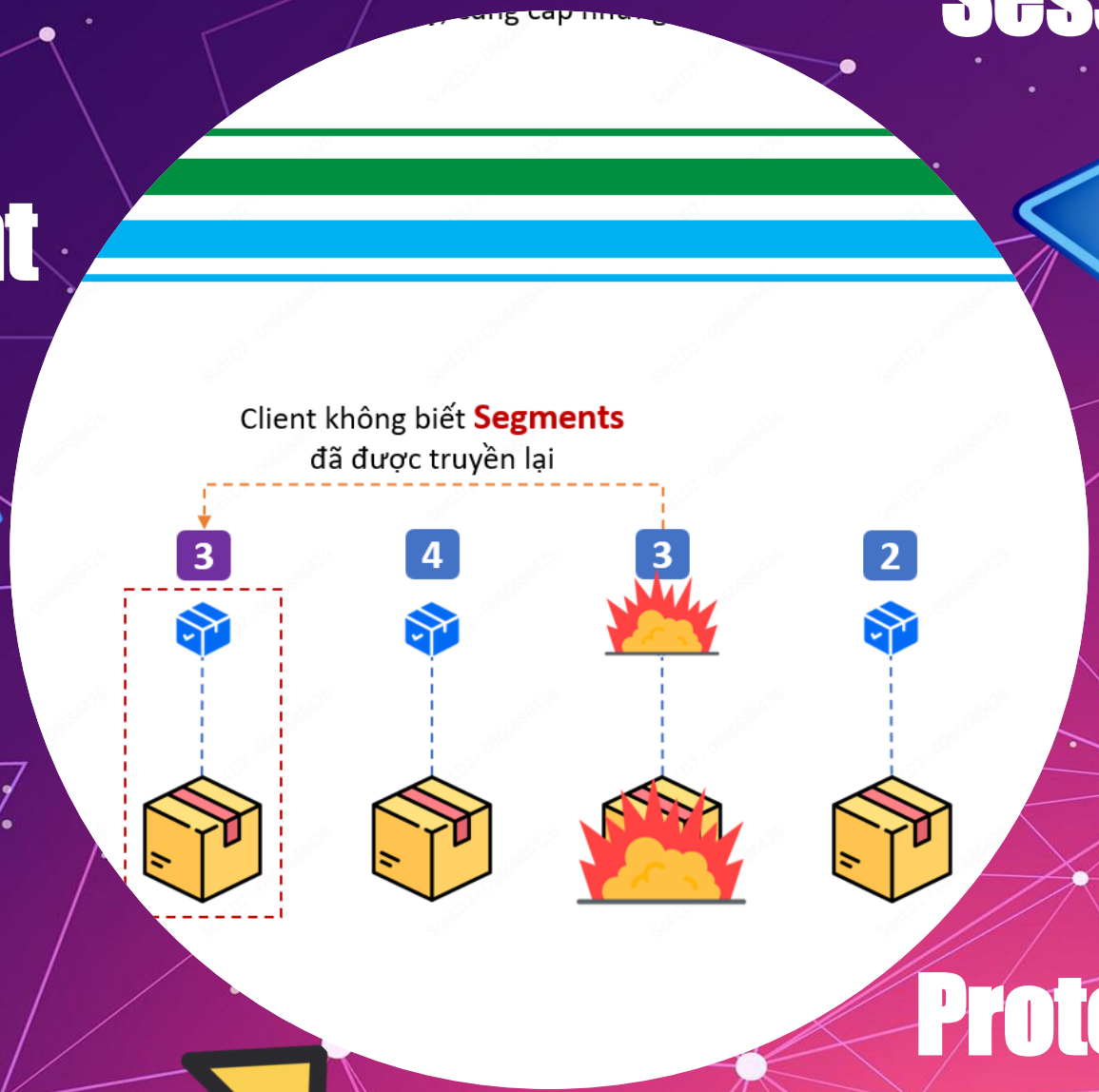

**Nhanh**
nhưng
**Chưa Chắc**

Session

Segment

Basic Networking

# Layer 4
# TCP



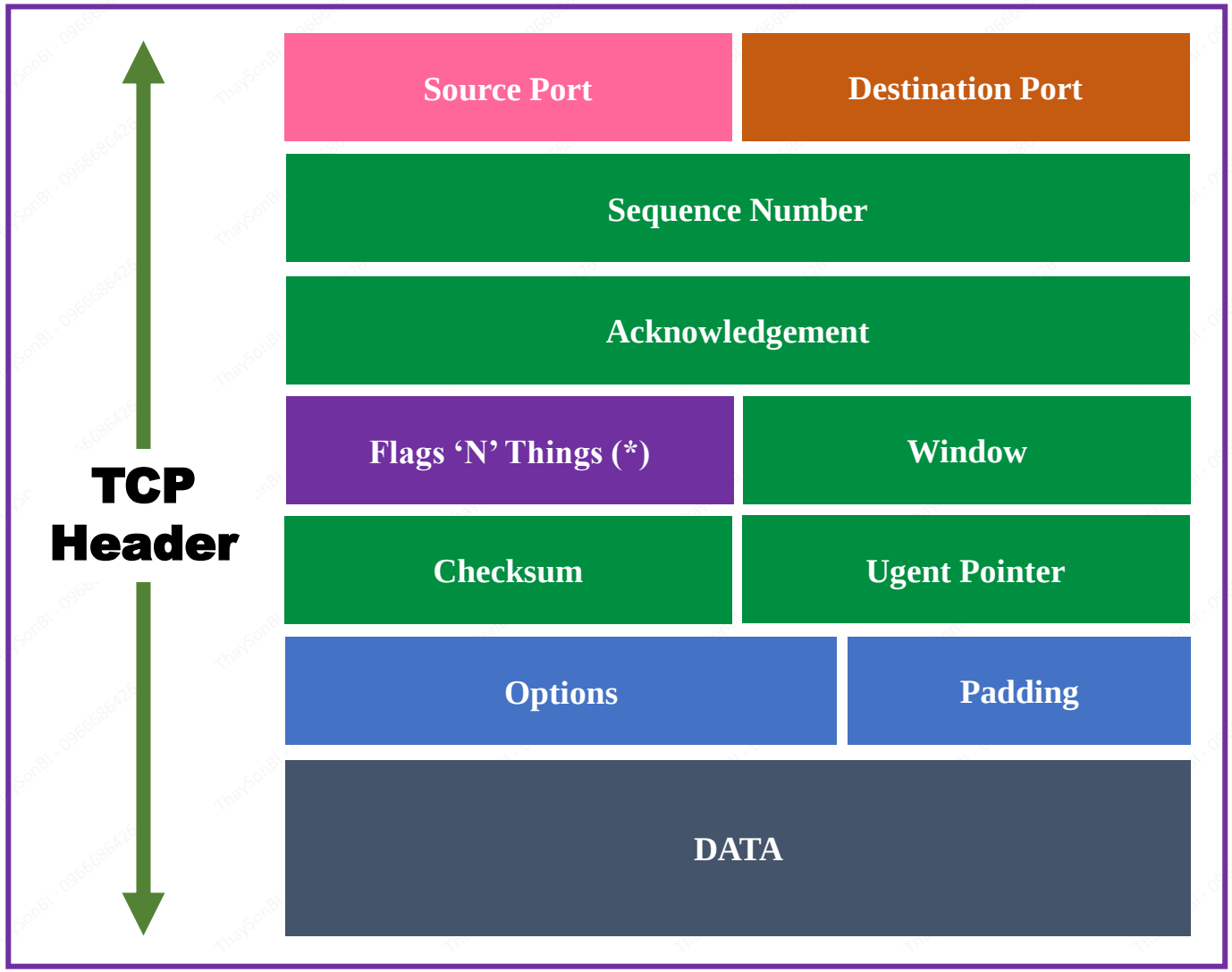

Protection

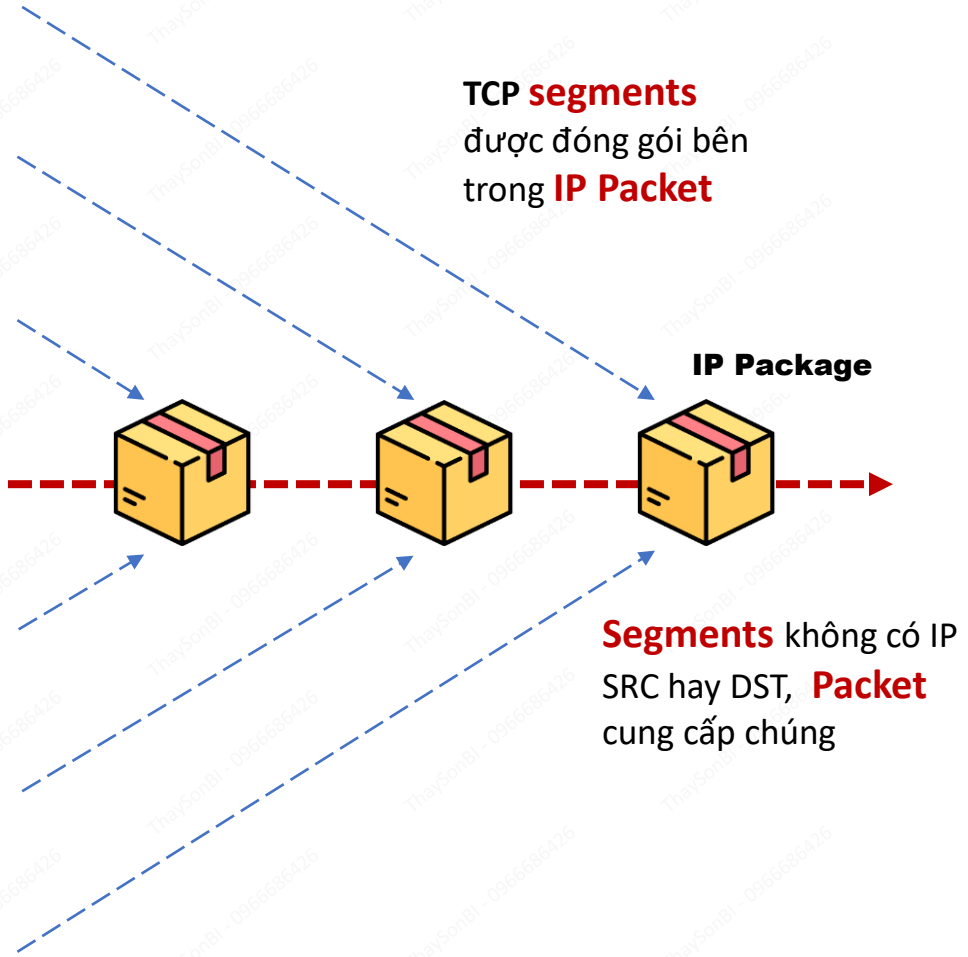
Slow

amazon web services™

Amazon Web Service - Training

# LAYER 4 – TCP SEGMENT




**TCP segments** được đóng gói bên trong **IP Packet**

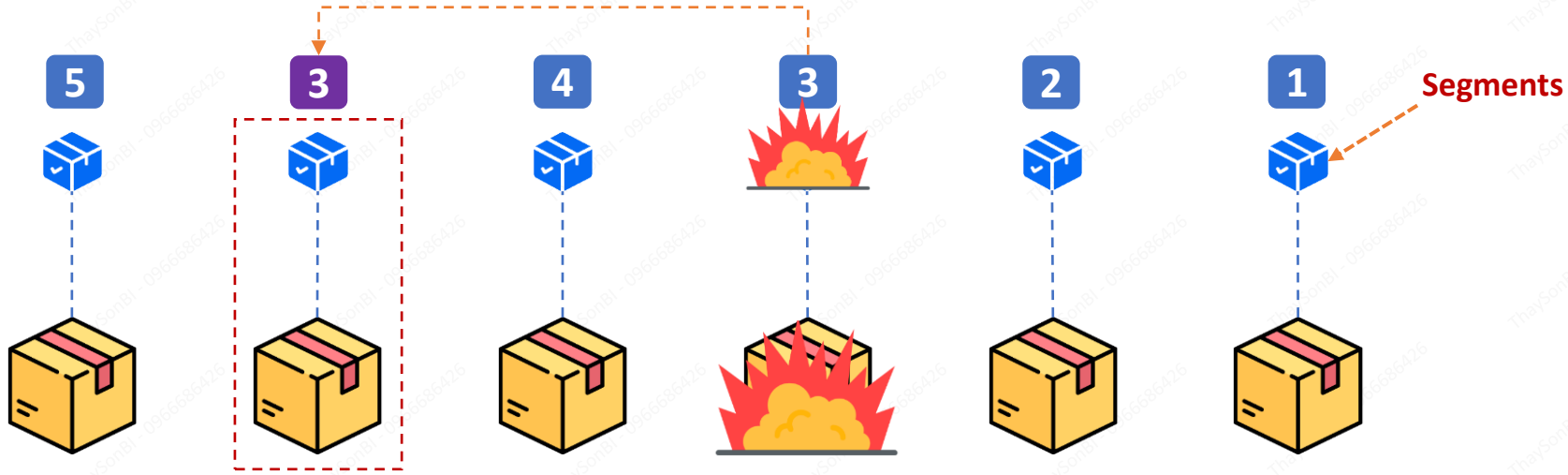
**Segments** không có IP SRC hay DST, **Packet** cung cấp chúng

# LAYER 4 – TCP WORKING

**TCP** là một giao thức mạng. Một kết nối được tạo ra giữa 2 thiết bị thông qua cổng ngẫu nhiên của Client và cổng được biết trước của Server. Kết nối này là **đáng tin cậy**, cung cấp những Segment được đóng gói trong IP Packet


**Segments** được gắn vào một connection để kiểm tra lỗi, sắp xếp thứ tự package và truyền lại khi có lỗi

**L3 Packet** không có giải pháp check lỗi, sắp xếp và kết hợp



# LAYER 4 – TCP 3 WAY HANDSHAKE

**Flags 'N' Things (*)**

| U | A | P | R | S | F |
|---|---|---|---|---|---|
| R | C | S | S | Y | I |
| G | K | H | T | N | N |

Những **Flag** này có thể được setup để thay đổi kết nối.
**Ví dụ: FIN** có thể dùng để đóng kết nối, **ACK** cho acknowledgements, **SYN** để đồng bộ số một cách tuần tự

**1** **SYN**

Gửi một segment with **SYN** sequence là '**cs**' số ngẫu nhiên

sequence = cs

**SYN-ACK** **2**

Tăng '**cs**' (= **cs +1**). Chọn một sequence ngẫu nhiên '**ss**'
Gửi segment – **SYN** & **ACK**
Với **sequence = ss**
Và **acknowledge = cs+1**

sequence = ss
acknowledge = cs+1

**3** **ACK**

Tăng **ss** (= **ss +1**).
Tăng **cs+1** (= **cs +2**).
Gửi segment **ACK**
Với **sequence = cs+2**
Và **acknowledge = ss+1**

sequence = cs +2
acknowledge = ss+1

**Kết nối được tạo**

**Client có thể gửi data**

**4**

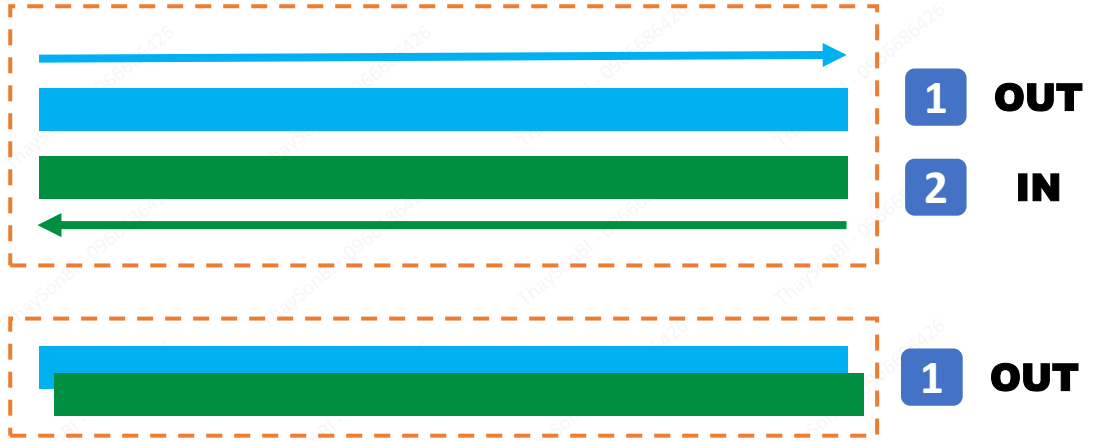
# LAYER 4 – SESSION & STATE


## Network ACL
## (AWS)

**Stateless** xem xét 2 thứ:

**Outbound…** (**LAPTOP-IP** & **tcp/23060**) ➔ (**SERVER-IP** & **tcp/443**)

**Response…** (**SERVER-IP** & **tcp/443**) ➔ (**LAPTOP-IP** & **tcp/23060**)




**Stateful** xem xét 1 thứ duy nhất:

**Outbound… LAPTOP-IP** & **tcp/23060** ➔ **SERVER-IP** & **tcp/443**

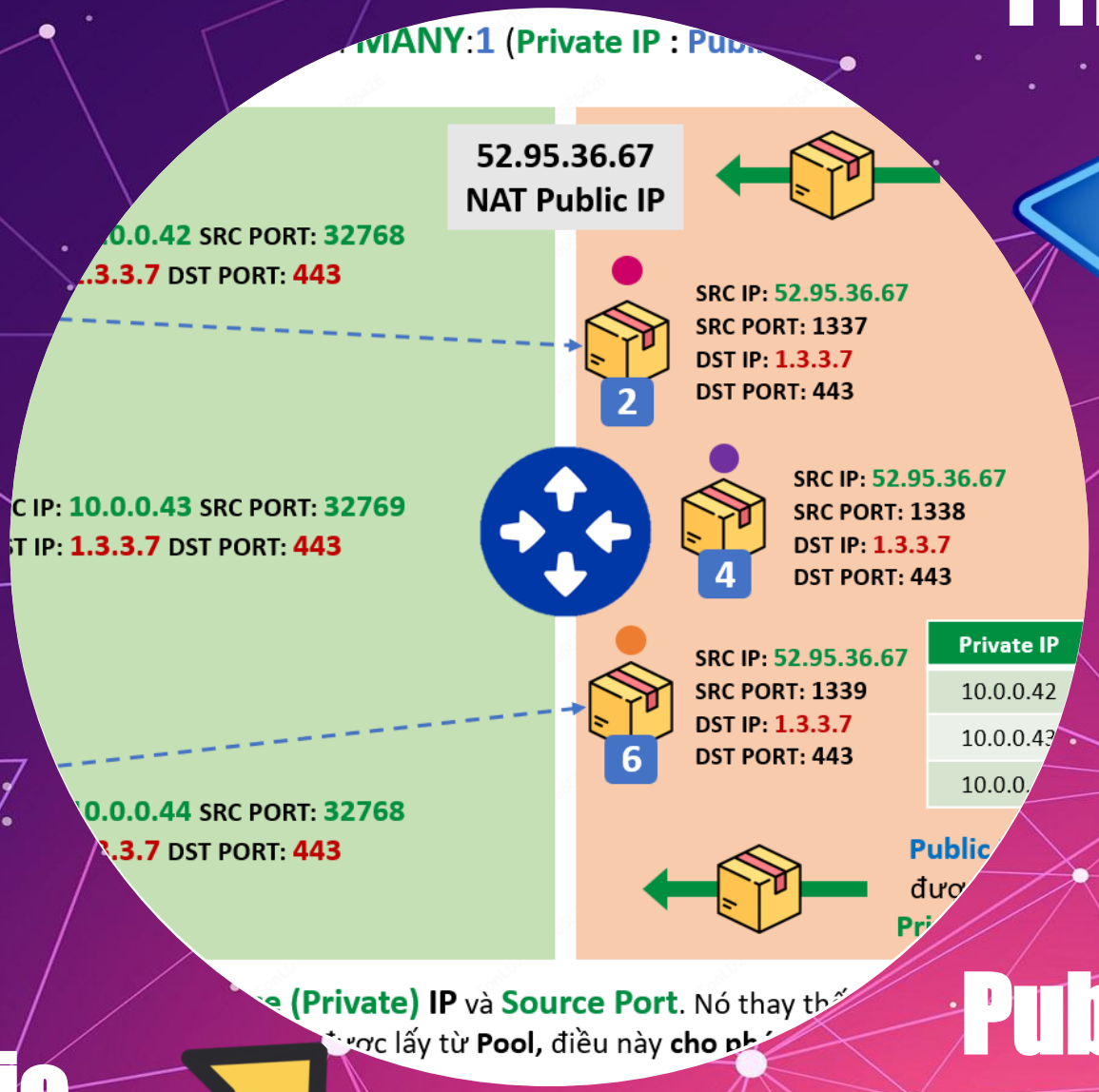
Coi việc chấp thuận **Outbound** đồng nghĩa với chấp thuận **Inbound Response**

Private

Static

Basic Networking

# What is NAT?




Public

Dynamic

amazon web services™

Amazon Web Service - Training

# NETWORK ADDRESS TRANSLATION (NAT)


**NAT** giúp hỗ trợ những thiếu hụt của **IP**

… cũng như cung cấp thêm những lợi ích về **bảo mật**

**NAT** dịch địa chỉ **bí mật** của IPv4 sang dạng **Public**

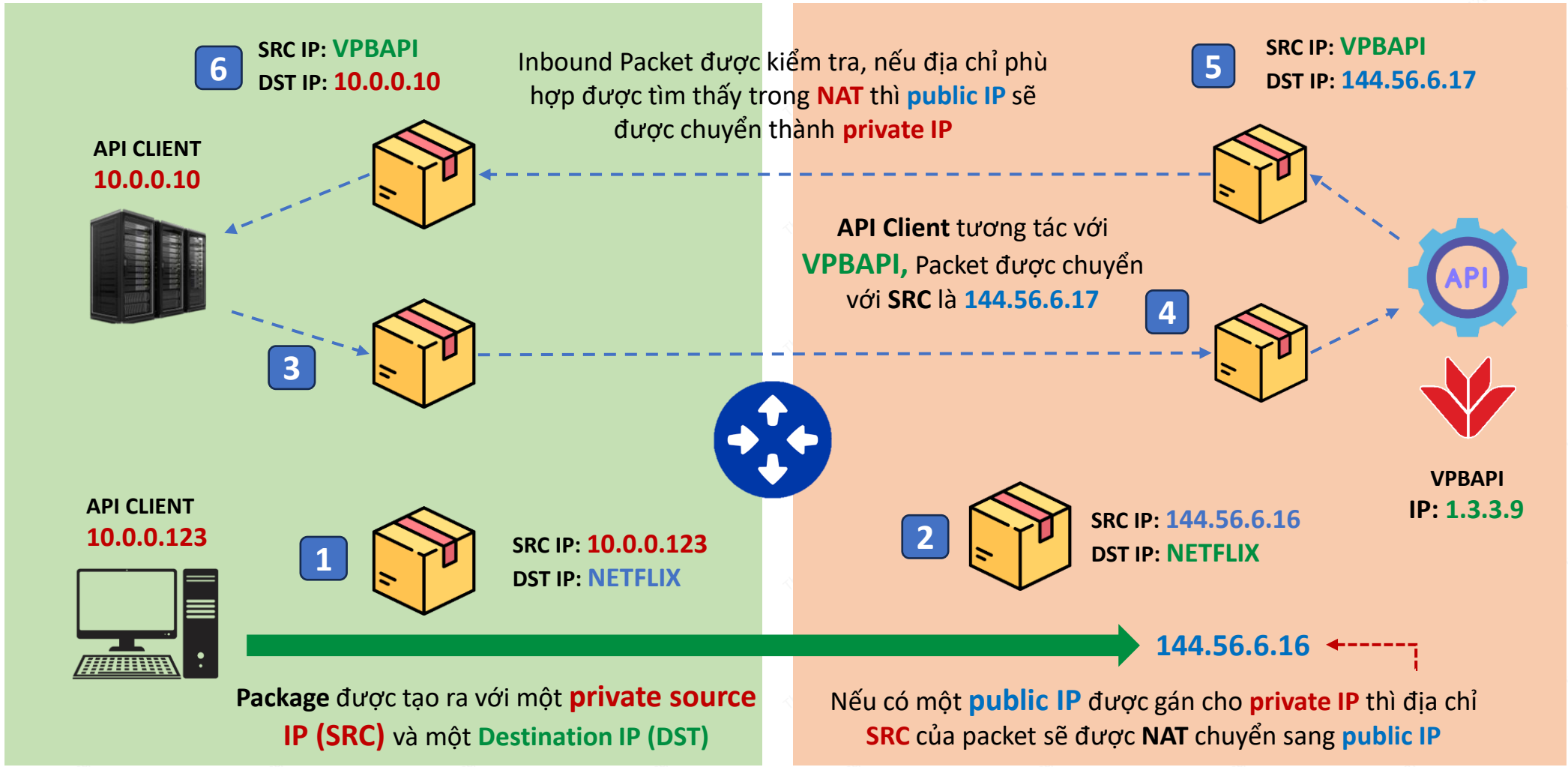
**Static NAT – 1 private** sang **1 địa chỉ (cố định) public** (IGW)

**Dynamic NAT – 1 private** sang **1 available Public**

Port Address Translation **(PAT) – many private** sang **1 Public** (NATGW)

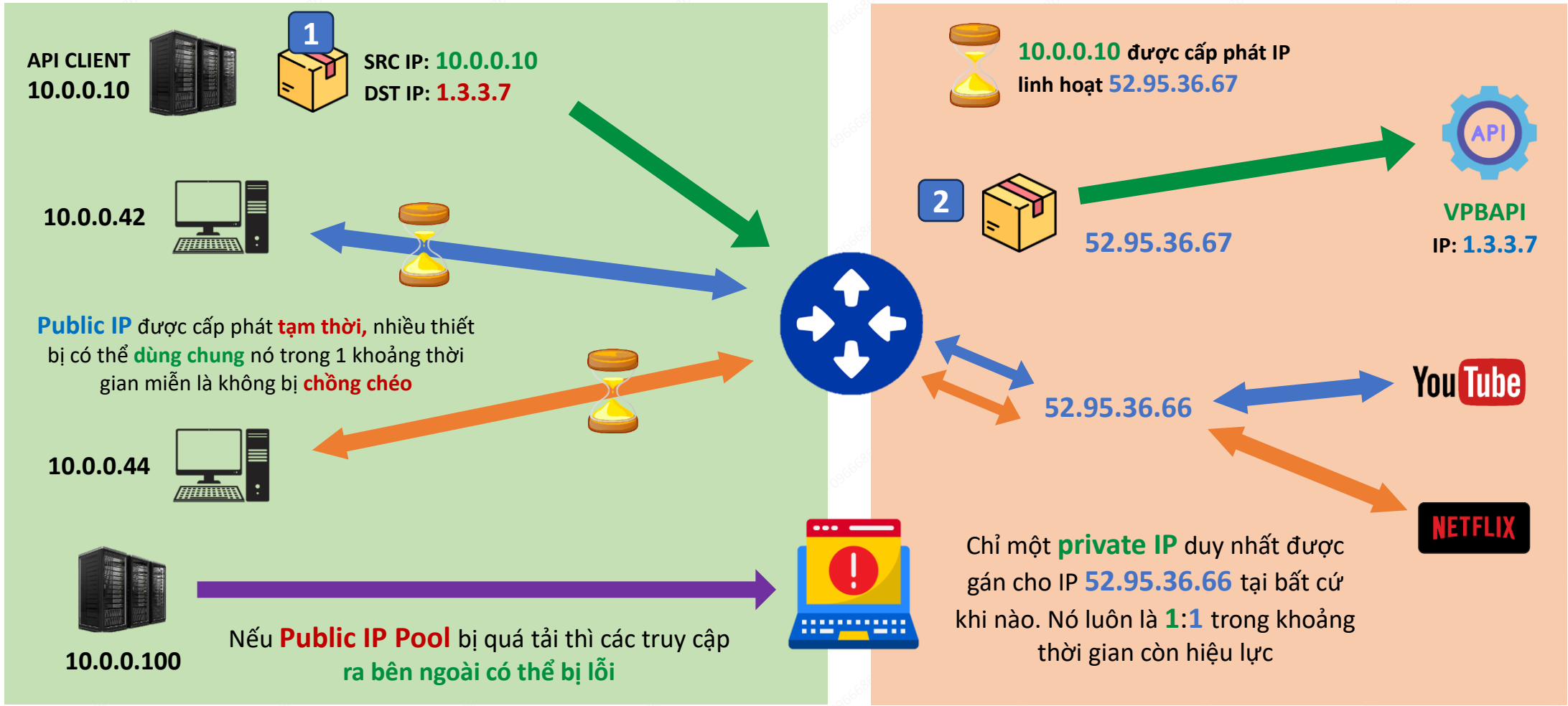
**Chỉ cho IPv4…**không sử dụng cho IPv6

# STATIC NAT


6
SRC IP: VPBAPI
DST IP: 10.0.0.10
Inbound Packet được kiểm tra, nếu địa chỉ phù hợp được tìm thấy trong NAT thì public IP sẽ được chuyển thành private IP
5
SRC IP: VPBAPI
DST IP: 144.56.6.17
API CLIENT
10.0.0.10
API Client tương tác với VPBAPI, Packet được chuyển với SRC là 144.56.6.17
4
3
API
VPBAPI
IP: 1.3.3.9
API CLIENT
10.0.0.123
1
SRC IP: 10.0.0.123
DST IP: NETFLIX
2
SRC IP: 144.56.6.16
DST IP: NETFLIX
144.56.6.16
Package được tạo ra với một private source IP (SRC) và một Destination IP (DST)
Nếu có một public IP được gán cho private IP thì địa chỉ SRC của packet sẽ được NAT chuyển sang public IP

NETWORKING BASIC

# DYNAMIC NAT




Router (NAT device) quản lý một NAT table, nó mapping Private IP : Public IP

Những Public IP được cấp phát tạm thời từ một Public IP Pool

NETWORKING BASIC

# PORT ADDRESS TRANSLATION (PAT)

Sau đây là kiến trúc áp dụng trên **AWS** để gán **MANY**:1 (**Private IP** : **Public IP**) thông qua **NAT Gateway** (**NATGW**)

**10.0.0.42**

1 — SRC IP: 10.0.0.42 SRC PORT: 32768
DST IP: 1.3.3.7 DST PORT: 443

**10.0.0.43**

3 — SRC IP: 10.0.0.43 SRC PORT: 32769
DST IP: 1.3.3.7 DST PORT: 443

**10.0.0.44**

5 — SRC IP: 10.0.0.44 SRC PORT: 32768
DST IP: 1.3.3.7 DST PORT: 443

**52.95.36.67**
**NAT Public IP**

2 — SRC IP: 52.95.36.67
SRC PORT: 1337
DST IP: 1.3.3.7
DST PORT: 443

4 — SRC IP: 52.95.36.67
SRC PORT: 1338
DST IP: 1.3.3.7
DST PORT: 443

6 — SRC IP: 52.95.36.67
SRC PORT: 1339
DST IP: 1.3.3.7
DST PORT: 443

Luồng trả về gồm **tcp/443** và **1.3.3.7** chứa source và **public IP** của thiết bị NAT cùng với **cổng đích**

API — **VPBAPI**
**IP: 1.3.3.7**
**tcp/443**

**NAT Table**

| Private IP | Private Port | Public IP | Public Port |
|---|---|---|---|
| 10.0.0.42 | 32768 | 52.95.36.67 | 1337 |
| 10.0.0.43 | 32769 | 52.95.36.67 | 1338 |
| 10.0.0.44 | 32768 | 52.95.36.67 | 1339 |

**Public Port** và **Public IP** được dịch trở lại thành **Private Port** và **Private IP**

Thiết bị NAT ghi nhớ **Source (Private) IP** và **Source Port**. Nó thay thế source IP bằng một **Public IP đơn** và 1 **Public Source Port** được lấy từ **Pool,** điều này **cho phép IP Overloading** (many to one)