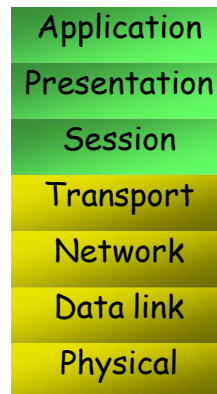


Chương 5 Tầng mạng

MẠNG MÁY TÍNH NÂNG CAO

Mục tiêu

- ❑ Thiết lập kết nối giữa 2 host để truyền dữ liệu từ host - host



Tầng mạng vs tầng vận chuyển

- ❑ *Tầng mạng*: cung cấp kết nối logic giữa các host
- ❑ *Tầng vận chuyển*: cung cấp kết nối logic giữa các tiến trình
 - Dựa trên, mở rộng dịch vụ của tầng mạng

Ví dụ:

A gửi B 1 bức thư qua đường bưu điện

- processes = A, B
- app messages = bức thư
- hosts = nhà của A, nhà của B
- transport protocol ???
- network-layer protocol???

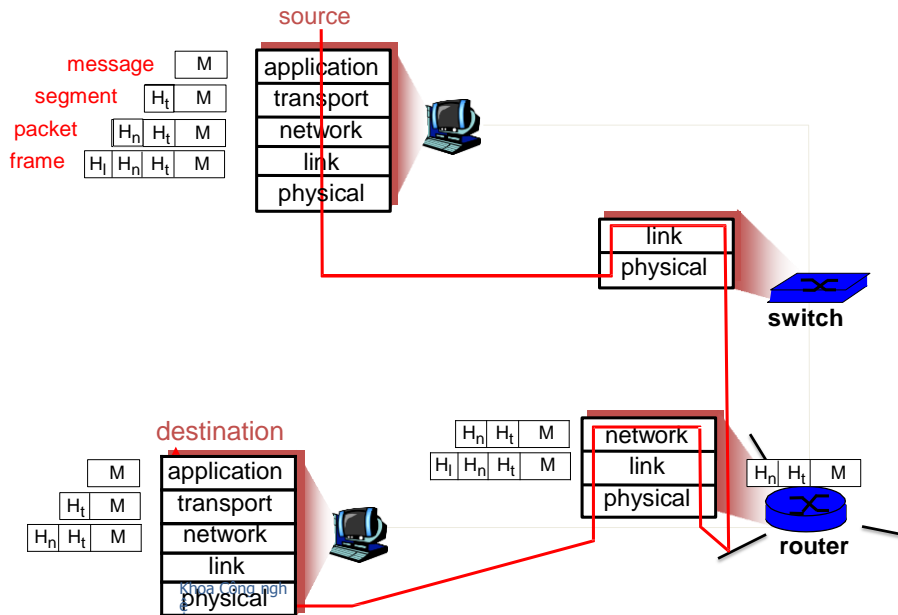
3

Nội dung

- ❑ Giới thiệu
- ❑ Định tuyến – chuyển tiếp
- ❑ Giao thức IP
- ❑ Giao thức ICMP
- ❑ Giao thức NAT

4

Nhắc lại



5

giới thiệu - 1

- ❑ Thực hiện chuyển các segment từ host gửi đến host nhận
- ❑ Tại host gửi:
 - Nhận các segment từ transport layer
 - Đóng gói thành các packet
- ❑ Tại host nhận:
 - Nhận các packet từ data link layer
 - Chuyển các segment lên transport layer
- ❑ Tại các router:
 - Dựa vào **thông tin đích đến** để chuyển các packet đến host nhận
 - Định tuyến: quyết định gói tin đi đường nào
 - Chuyển tiếp: chuyển gói tin từ interface nhận ra interface gửi

6

giới thiệu - 2

❑ Tầng mạng cung cấp 2 loại dịch vụ

- Hướng kết nối (Connection)
 - Virtual Circuit
 - Trước khi truyền dữ liệu, 2 host phải thiết lập kết nối
- Hướng không kết nối (Connectionless)
 - Datagram Network
 - Không cần thiết lập kết nối trước khi gửi

❑ Trong 1 kiến trúc mạng: chỉ hỗ trợ duy nhất 1 loại dịch vụ

7

Virtual circuit (VC) network - 1

❑ Thiết lập, quản lý, duy trì mỗi kết nối khi truyền dữ liệu

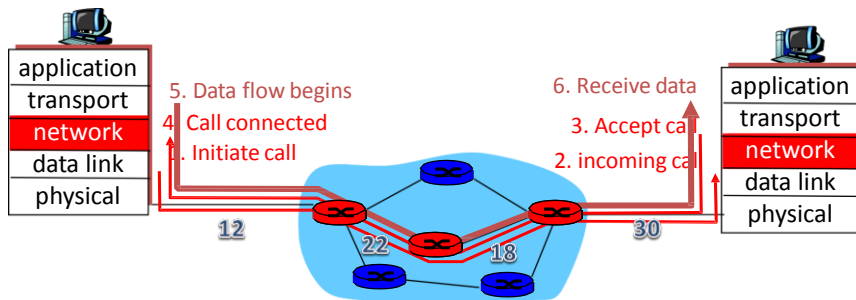
- 1 đường đi ảo khi truyền dữ liệu
 - Số hiệu VC (VC number)
 - Khác nhau trên mỗi link
- Mỗi gói tin có một virtual circuit identifier (VC ID)
- Các router duy trì trạng thái kết nối đi qua
 - bảng chuyển đổi VC ID
 - Thay thế thông tin VC ID của gói tin đi ngang qua router

❑ Thông tin định tuyến: Virtual Circuit number (VC ID)

❑ Dùng trong ATM, X.25, Frame-Relay,...

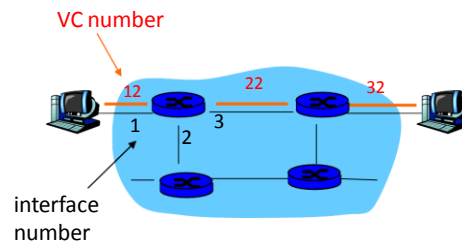
8

Virtual circuit (VC) network - 2



9

Virtual circuit network - 3



Cổng vào	VC# vào	Cổng ra	VC# ra
1	12	3	22
2	63	1	18
3	7	2	17
1	97	3	87
...

Routers duy trì thông tin về trạng thái kết nối!

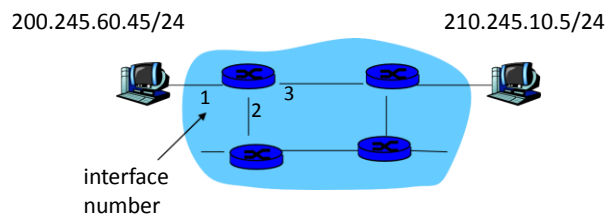
10

Datagram network - 1

- ❑ Không thiết lập kết nối trước khi truyền dữ liệu
 - Router không cần quản lý trạng thái kết nối
- ❑ Thông tin định tuyến: địa chỉ đích đến
 - Mỗi router duy trì một bảng định tuyến
- ❑ Dừng trong Internet

11

Datagram network - 2



Destination Network	Subnetmask	Out Interface	Next hop
210.245.10.0	255.255.255.0	3
210.245.15.0	255.255.255.0	1
210.245.15.192	255.255.255.192	2
...

12

Nội dung

- ☐ Giới thiệu
- ☒ Định tuyến – chuyển tiếp
- ☐ Giao thức IP
- ☐ Giao thức ICMP
- ☐ Giao thức NAT

13

Định tuyến - Chuyển tiếp

☒ Định tuyến:

- Quyết định “lộ trình” mà gói tin di chuyển từ host nguồn đến host đích đến
- Sử dụng thông tin toàn cục

☒ Chuyển tiếp:

- Di chuyển gói tin từ cổng vào đến cổng ra
- Sử dụng thông tin cục bộ

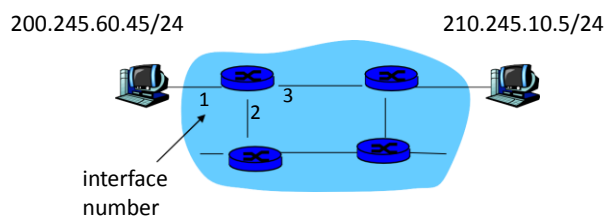
14

Định tuyến

- ❑ Được thực hiện bởi các bộ định tuyến.
 - VD: router
- ❑ Dùng bảng định tuyến (routing/forwarding table)
 - destination/subnetmask
 - Out interface
 - next hop
 - chi phí
 - Hop count
 - Delay
 - Bandwidth
 - ...

15

Ví dụ - định tuyến



Destination Network	Subnet mask	Next hop	Out Interface
210.245.10.0	255.255.255.0	192.168.3.2	3
210.245.15.0	255.255.255.0	192.168.1.2	1
210.245.15.192	255.255.255.192	192.168.2.2	2
...

16

Định tuyến

❑ Router định tuyến một gói tin như thế nào?

- Dùng địa chỉ đích đến và bảng định tuyến
- Thực hiện:
 - Tìm record thích hợp trong bảng định tuyến
 - Tính địa chỉ đường mạng giữa địa chỉ đích đến với subnetmask của từng record
 - So sánh destination network với địa chỉ đường mạng vừa tính
 - Gửi gói tin theo thông tin của record tìm được

❑ VD: R1 nhận gói tin có destination 210.245.10.5

- 255.255.255.192
 - Net: 210.245.10.0 → không có record thoả
- 255.255.255.0
 - Net: 210.245.10.0 → record số 1 thoả
 - gói tin chuyển ra interface số 3 và nơi nhận gói tin tiếp theo là 192.168.3.2

17

Bảng định tuyến

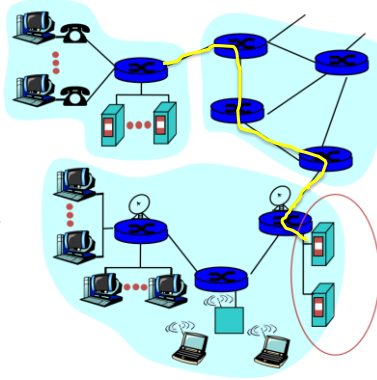
❑ Xây dựng bảng định tuyến:

- Tĩnh (static): con người tự thiết lập
- Động (dynamic): học
 - Distance Vector:
 - Gửi theo định kỳ
 - Gửi toàn bộ bảng định tuyến
 - VD: RIP, IGRP, ...
 - Link State:
 - Gửi khi có thay đổi
 - Gửi tình trạng kết nối
 - VD: OSPF, ISIS, ...

18

Static route

- ❑Biết: Sơ đồ mạng
- ❑Xây dựng:
 - Vẽ “đường đi” *tối ưu*
- ❑Khi có thay đổi:
 - Tự cập nhật bằng tay



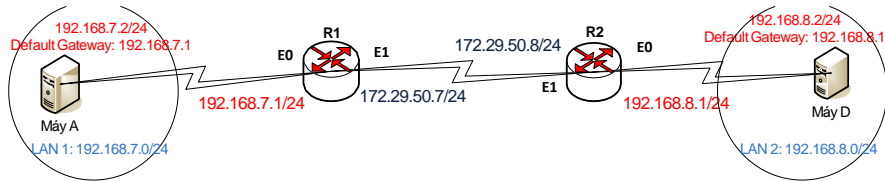
19

Dynamic route

- ❑Biết: không
- ❑Xây dựng:
 - Sử dụng các giao thức định tuyến
 - Thông qua các gói tin “thu thập” thông tin
 - Thành phần:
 - Gửi và nhận thông tin từ các router khác
 - Tính đường đi tối ưu
 - Phản ứng khi có thay đổi
- ❑Khi thay đổi
 - Cập nhật tự động

20

Static route - Ví dụ - 1



Yêu cầu: cấu hình thông tin định tuyến cho R1 và R2 để các máy trong LAN1 có thể liên lạc với các máy trong LAN2.

Tại router R1:

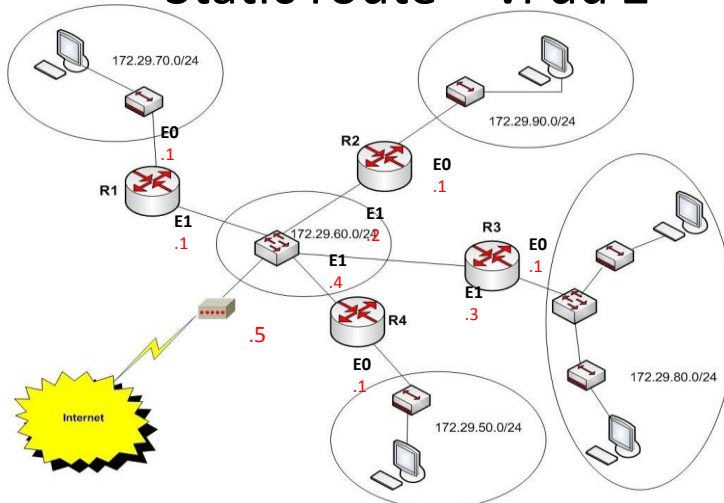
Destination network	Out interface	Next hop
192.168.8.0/24	E1	172.29.50.8

Tại router R2:

Destination network	Out interface	Next hop
192.168.7.0/24	E1	172.29.50.7

21

Static route – ví dụ 2



Yêu cầu: cấu hình thông tin định tuyến cho các router để tất cả các máy trong có thể liên lạc với nhau và có thể truy cập Internet.

22

Static route – ví dụ 2

Tại router R1:

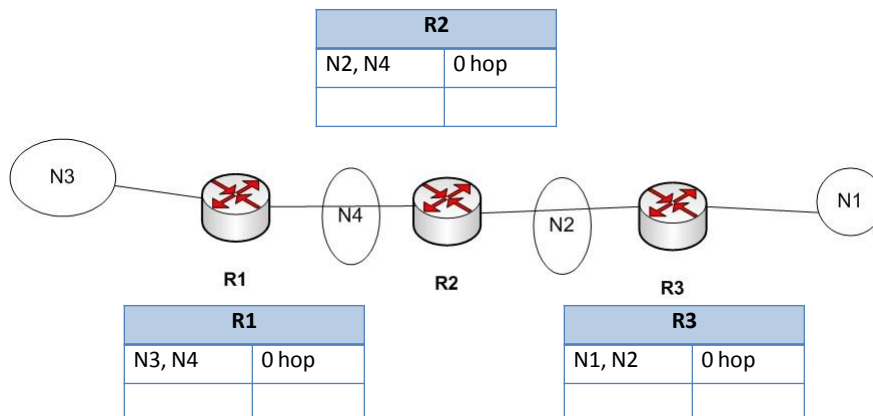
Destination network	Out interface	Next hop
172.29.90.0/24	E1	172.29.60.2
172.29.80.0/24	E1	172.29.60.3
172.29.50.0/24	E1	172.29.60.4
0.0.0.0/0	E1	172.29.60.5

Tại router R2:

Destination network	Out interface	Next hop
172.29.70.0/24	E1	172.29.60.1
172.29.80.0/24	E1	172.29.60.3
172.29.50.0/24	E1	172.29.60.4
0.0.0.0/0	E1	172.29.60.5

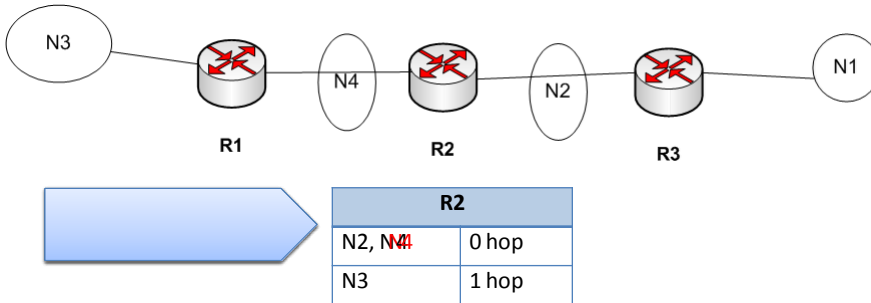
23

Dynamic route – ví dụ



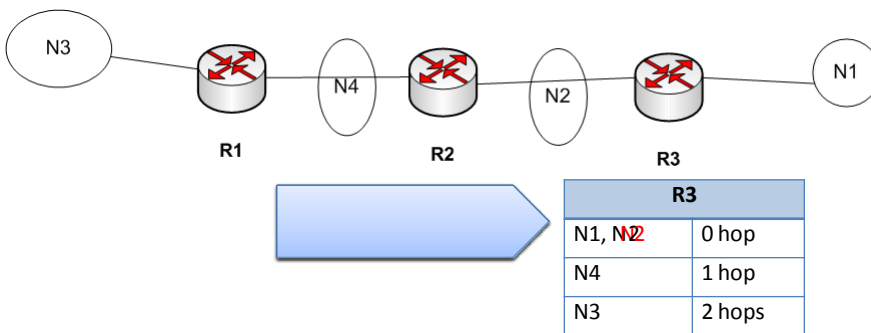
24

Dynamic route – ví dụ



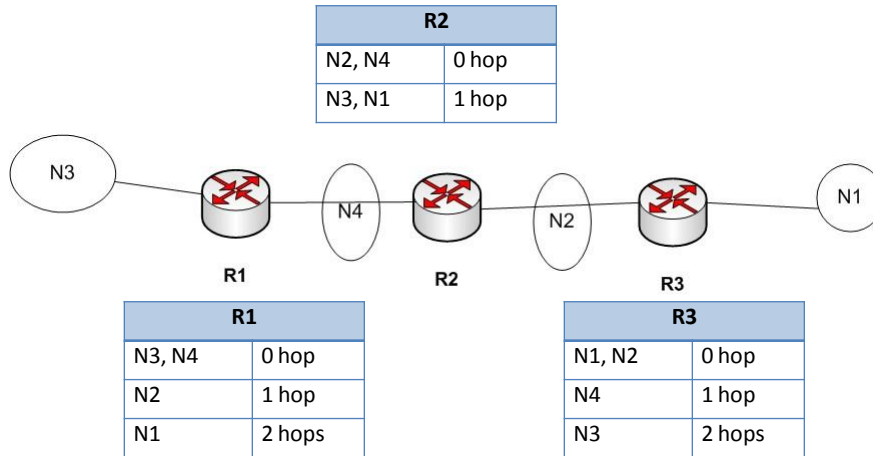
25

Dynamic route – ví dụ



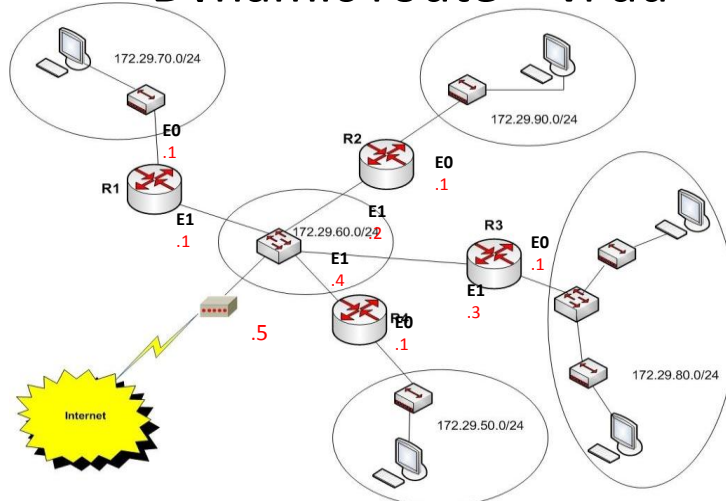
26

Dynamic route – ví dụ



27

Dynamic route – ví dụ



Yêu cầu: cấu hình thông tin định tuyến cho các router để tất cả các máy trong có thể liên lạc với nhau và có thể truy cập Internet

28

Dynamic route – ví dụ

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

    172.29.0.0/24 is subnetted, 5 subnets
O       172.29.50.0 [110/2] via 172.29.60.4, 00:00:15, FastEthernet0/0
C       172.29.60.0 is directly connected, FastEthernet0/0
C       172.29.70.0 is directly connected, FastEthernet0/1
O       172.29.80.0 [110/2] via 172.29.60.3, 00:00:15, FastEthernet0/0
O       172.29.90.0 [110/2] via 172.29.60.2, 00:00:46, FastEthernet0/0
```

29

Nội dung

- ☐ Giới thiệu
- ☐ Định tuyến – chuyển tiếp
- ☐ Giao thức IP
- ☐ Giao thức ICMP
- ☐ Giao thức NAT

30

Routed protocol - 1

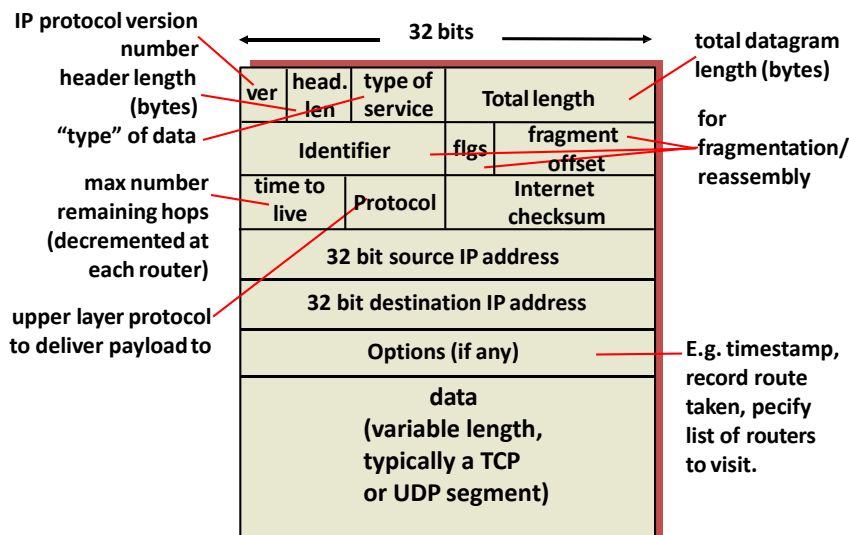
□ Giao thức được định tuyến (routed protocol):

- qui định cách thức đóng gói dữ liệu truyền trên đường truyền
- VD: IP (IPv4, IPv6), IPSec,....

Routing protocol	Routed protocol
Tạo bảng định tuyến	Đóng gói gói tin tại tầng mạng

31

Routed protocol - 2



32

Routed protocol - 3

- ❑ Version (4)
 - version của IP
- ❑ Header Length (4):
 - Chiều dài IP header (byte)
- ❑ Type of service (8)
 - Chứa định thông tin ưu tiên
 - Ít sử dụng
- ❑ Total length (16)
 - Tổng chiều dài của datagram (tính cả header) (byte)
- ❑ Identifier (16):
 - Khi một gói tin IP bị chia nhỏ ra thành nhiều đoạn, thì mỗi đoạn được gán cùng số ID
 - Dùng khi tổng hợp

33

Routed protocol - 4

- ❑ Flag (3)

	DF	MF
--	----	----

 - DF
 - Don't fragment, không chia nhỏ
 - MF
 - More fragment, còn gói tin nhỏ tiếp
 - Khi 1 gói tin bị chia nhỏ, tất cả các gói nhỏ (trừ gói tin cuối cùng), bit này được bật lên
- ❑ Fragment offset (13)
 - Vị trí gói nhỏ trong gói tin ban đầu
- ❑ Time to live – TTL (8)
 - Thời gian sống của gói tin (hop count)
 - Giảm mỗi khi gói tin đến 1 router mới
 - Khi hop count =0 thì gói tin bị loại bỏ

34

Routed protocol - 5

- ☐ Protocol (8)
 - Chỉ ra nghi thức nào ở tầng transport mà gói tin đang sử dụng
 - VD: TCP = 6, UDP = 17
- ☐ Internet (Header) checksum (16)
 - Kiểm tra tính đúng đắn nội dung của IP header
 - Không theo cách kiểm tra tuần tự
- ☐ Source and destination addr (32)
 - Địa chỉ IP của bên gửi và bên nhận
- ☐ Options (32)
 - Có thể dài đến 40 bytes
 - Dùng cho các tính năng mở rộng của IP
 - Vd: source routing, security, record route, ...
- ☐ Data:
 - Dữ liệu ở tầng transport gửi xuống

35

Nội dung

- ☐ Giới thiệu
- ☐ Định tuyến – chuyển tiếp
- ☐ Giao thức IP
- ☐ Giao thức ICMP
- ☐ NAT

36

Nội dung

- ☐ Giới thiệu
- ☐ Định tuyến – chuyển tiếp
- ☐ Giao thức IP
- ☐ Giao thức ICMP
- ☒ NAT

37

Định tuyến

- ☐ Định tuyến là quá trình chọn lựa các đường đi trên một mạng máy tính để gửi dữ liệu qua đó .
- ☐ Định tuyến chỉ ra đường đi tốt nhất từ nguồn đến đích của gói tin (packet) thông qua các node trung gian là các router .
- ☐ Có 2 loại định tuyến : tĩnh và động

38

Định tuyến

- □ Định tuyến tĩnh: đường đi là cố định . Khi thay đổi trong mạng phải cấu hình lại . Phù hợp với mạng nhỏ . Rất khó triển khai trong mạng lớn.
- □ Định tuyến động: Có ưu thế trên mạng Internet ngày nay . Các đường đi đến đích có tính linh hoạt .

39

Các kiểu định tuyến động

- RIP (Routing information protocol)
- IGRP (Interior Gateway Routing Protocol)
- EIGRP (Enhanced IGRP)
- OSPF (Open Shortest Path First)
- IS-IS (Intermediate System-to-Intermediate System)
- BGP (Border Gateway) .

40

Định tuyến tĩnh

- Cấu hình các đường cố định cho router.
- Router cài đặt các đường đi này vào bảng định tuyến
- Các gói dữ liệu được định tuyến theo các đường cố định.

41

Định tuyến tĩnh

- Router (config)# ip route {destination network} {subnet mask} {nexthop ip address | outgoing interface} <administrative distance>.
- administrative distance (AD): độ tin cậy của một con đường
- AD càng thấp càng được tin cậy.
- Giá trị AD mặc định của tuyến đường tĩnh là 1.

42

Định tuyến tĩnh

- **Default Route:**
- Cú pháp: `ip route 0.0.0.0 0.0.0.0 {nexthop ip address | outgoing interface}`

Default route: gửi các packet đến các mạng đích mà không có trong bảng định tuyến.

43

Định tuyến động

- ☐ Router Information Protocol (RIP)
- ☐ Tìm đường đi tốt nhất trong mạng và duy trì chúng.
- ☐ Có rất nhiều cách để xây dựng lên bảng định tuyến một cách tự động.
- ☐ Thực hiện một số quy tắc đã định trước để xác định ra đường tốt nhất đến đích.

44

Routing Information Protocol (RIP)

- □ Đặc điểm:
- Là giao thức định tuyến theo Distance Vector.
- Thông tin định tuyến là số lượng hop.
- Nếu gói dữ liệu đến mạng đích có số lượng hop lớn hơn 15 thì gói dữ liệu đó sẽ bị hủy bỏ.
- Chu kỳ cập nhật mặc định là 30 giây.
-

45

Routing Information Protocol (RIP)

- □ Đặc điểm:
- RIPv1 sử dụng phổ biến
- Mọi router đều có hỗ trợ giao thức này.
- RIPv1 đơn giản và tính tương thích cao
- Chia tải ra tối đa là 6 đường có metric bằng nhau.

46

Routing Information Protocol (RIP)

- □ Một số giới hạn của RIPv1:
- Không gửi thông tin subnet mask
- Gửi quảng bá theo địa chỉ 255.255.255.255
- Không hỗ trợ xác minh thông tin nhận được
- Không hỗ trợ VLSM và CIDR

▪

47

Routing Information Protocol (RIP)

- □ RIPv2:
- RIPv2 được phát triển từ RIPv1
- Là một giao thức theo Distance Vector
- Sử dụng thời gian holddown để chống loop với thời gian mặc định là 180 giây.
- Sử dụng cơ chế split horizon để chống loop.
- Số hop tối đa là 15.
- Gửi thông tin định tuyến theo địa chỉ Multicast 224.0.0.9

48

Routing Information Protocol (RIP)

- □ RIPv2:
- RIPv2 được phát triển từ RIPv1
- Là một giao thức theo Distance Vector
- Sử dụng thời gian holddown để chống loop với thời gian mặc định là 180 giây.

49

Routing Information Protocol (RIP)

- □ RIPv2:
- Sử dụng cơ chế split horizon để chống loop.
- Số hop tối đa là 15.
- Gửi thông tin định tuyến theo địa chỉ Multicast 224.0.0.9

50

Routing Information Protocol (RIP)

- □ Ưu điểm của RIPv2:
 - Cung cấp thêm nhiều thông tin định tuyến hơn.
 - Có cơ chế xác minh giữa các router khi cập nhật để bảo mật cho bảng định tuyến.
 - Có hỗ trợ VLSM (variable Length Subnet Masking-Subnet mask có chiều dài khác nhau).

51

Routing Information Protocol (RIP)

- □ Cấu hình mẫu:
 - Router(config)#router rip (dùng giao thức định tuyến RIP)
Router(config-router)#network địa_chỉ_ip (địa chỉ mạng muốn quảng bá bằng giao thức RIP)
Router(config-router)#version 2 (dùng RIP version 2, mặc định là version 1)

52

Giao thức Open Shortert Path First (OSPF)

- □ OSPF là giao thức định tuyến dạng Link-state
- □ Dựa trên chuẩn mở
- □ Được phát triển để thay thế phương thức RIP
- □ OSPF phù hợp với mạng lớn , có khả năng mở rộng

53

OSPF

- □ Ưu điểm của OSPF:
- Tốc độ hội tụ nhanh .
- Hỗ trợ mạng con (VLSM) .
- Có thể áp dụng cho mạng lớn .

54

OSPF

- □ Ưu điểm của OSPF:
- Chọn đường theo trạng thái đường link hiệu quả hơn distance vector
- Đường đi linh hoạt hơn
- Hỗ trợ xác thực (Authenticate)

55

SO SÁNH RIP & OSPF

- □ Hệ thống RIP: Mạng đích không được có quá 15 router
- □ Mạng dùng RIP nhỏ
- □ Khả năng mở rộng kém
- OSPF thì không bị giới hạn về kích thước , tăng khả năng mở rộng .

56

SO SÁNH RIP & OSPF

- ☐ Hệ thống OSPF : Có thể cấu hình theo nhiều vùng (area)
- ☐ Có thể giới hạn lưu thông trong từng vùng .
- ☐ Thay đổi vùng này không ảnh hưởng đến vùng khác
- ☐ Khả năng mở rộng cao

57

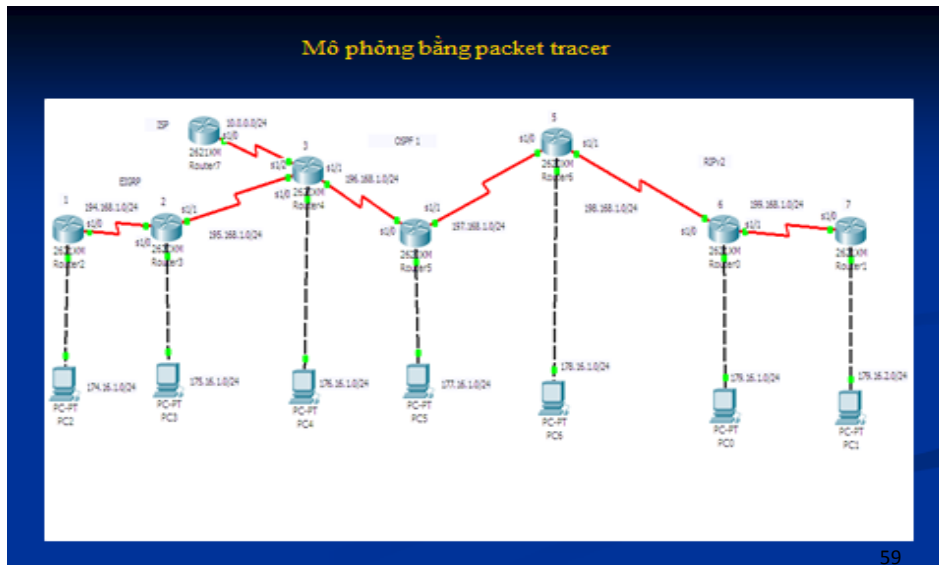
OSPF

- ☐ Cấu hình mẫu:

Router(config)# router ospf process ID
Router(config-router)# network
Network_number Wildcard_mask area_ID

58

Mô phỏng



59

Bảng so sánh

Giao thức	Administrative distance
Nối trực tiếp	0
Static route	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
ODR	160
External EIGRP	170
Internal BGP	200
Không xác định	255

60

Nhắc lại

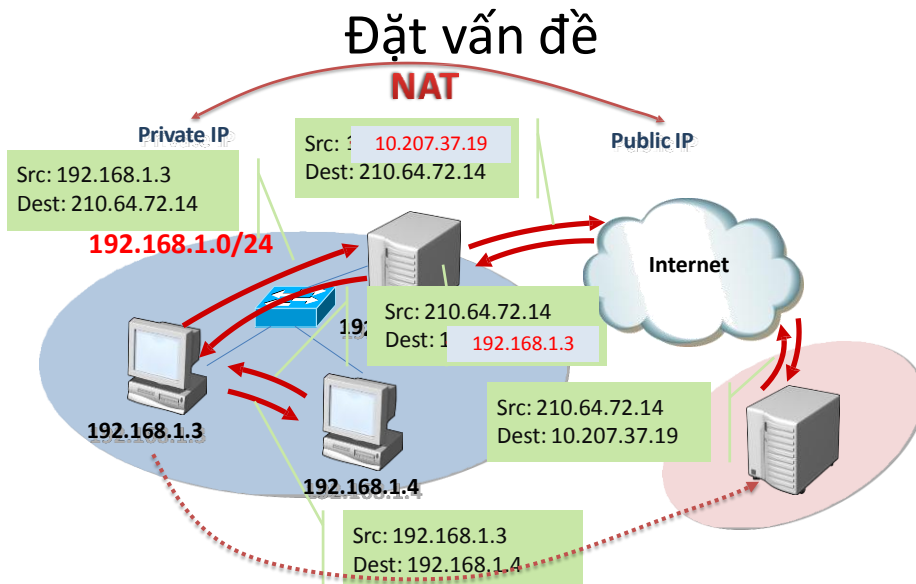
❑ Địa chỉ IP:

- Kích thước: 32 bits → không gian: 2^{32} địa chỉ
 - 0.x.x.x/8, 127.0.0.0/8, lớp D, lớp E; không dùng
 - Số lượng node trên Internet “khổng lồ”
- Giải quyết:
 - dùng địa chỉ private trong mạng LAN
 - Dùng địa chỉ public khi giao tiếp bên ngoài Internet

❑ Gửi dữ liệu giữa 2 host

- Địa chỉ host gửi
- Địa chỉ host nhận

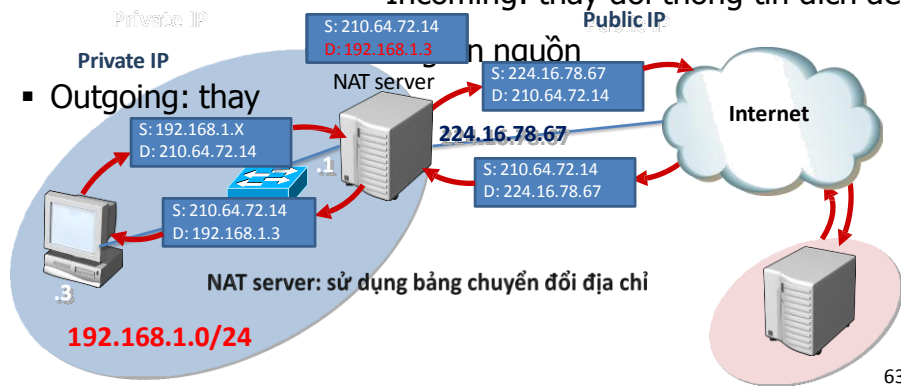
61



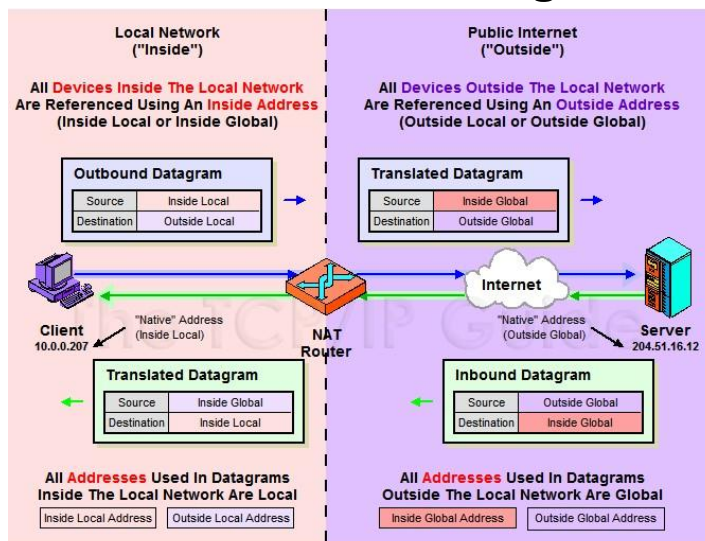
62

NAT – giới thiệu

- ❑ NAT = Network Address Translation
- ❑ RFC 1631, 1918, 2663
- ❑ Chức năng: “thay đổi” địa chỉ
 - Incoming: thay đổi thông tin đích đến



NAT – thuật ngữ



NAT – bảng chuyển đổi địa chỉ

- ❑ Dùng chuyển đổi global <-> local
 - Thông tin cục bộ bên trong (Inside local)
 - Thông tin toàn cục bên trong (Inside global)
- ❑ Thông tin trong bảng chuyển đổi
 - Static
 - dynamic

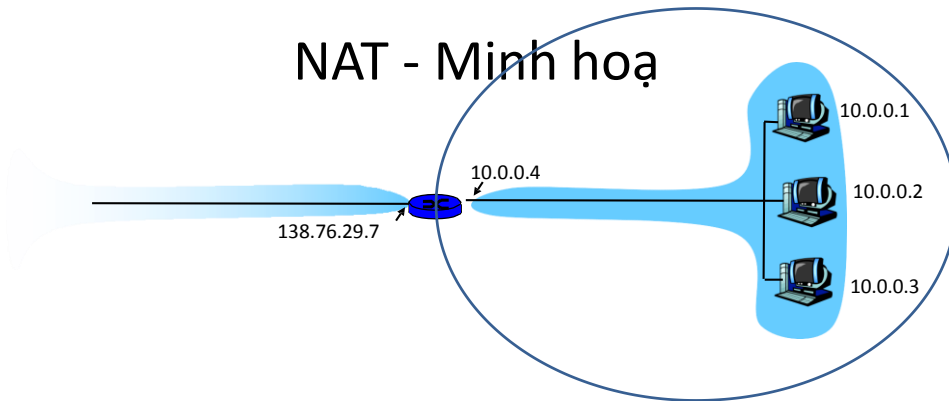
65

Nat – phân loại

- ❑ Static
 - Cố định: 1 local IP \Leftrightarrow 1 global IP
- ❑ Dynamic
 - n local IP \Leftrightarrow m global IP
 - NAT: chọn 1 global IP còn rảnh để NAT
- ❑ Overloading
 - n local IP \Leftrightarrow 1 global IP
 - NAT: <local IP, local port> \Leftrightarrow <global IP, global port>
- ❑ Overlapping
 - Cố định: <local IP, *port*> \Leftrightarrow <global IP, *port*>

66

NAT - Minh họa



□ Thứ tự gửi các gói tin như sau:

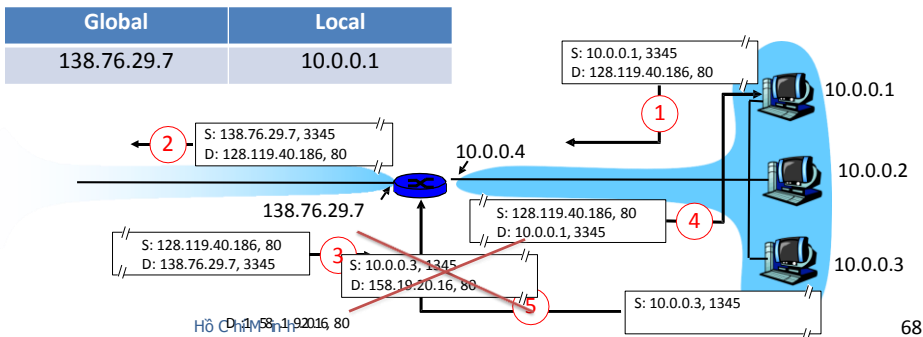
- Máy 10.0.0.1 gửi 1 gói tin đến 128.119.40.186, 80 từ ứng dụng 3345
- Ứng dụng <128.119.40.186, 80> gửi lại gói tin phản hồi
- Máy 10.0.0.3 gửi 1 gói tin đến 158.19.20.16, 80 từ ứng dụng 1234
- Ứng dụng <120.11.40.18, 3345> gửi gói tin truy cập dịch vụ web tại máy 10.0.0.1

67

Static NAT

□ Cấu hình **cố định**: 1 local IP \Leftrightarrow 1 global IP

- Số máy kết nối ra ngoài bằng với số địa chỉ IP global
- Bên ngoài (outside) có thể chủ động tạo kết nối với bên trong (inside)



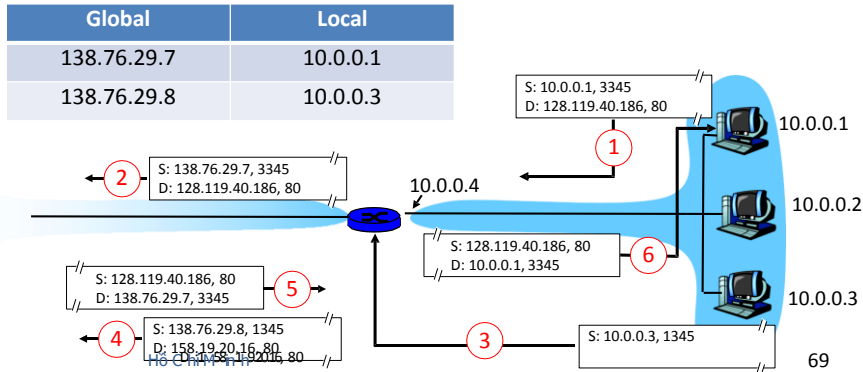
68

Dynamic NAT

□ Cấu hình: $n \text{ local IP} \Leftrightarrow m \text{ global IP}$

- Có m kết nối đồng thời
- Bên ngoài (outside) **không** thể chủ động tạo kết nối với bên trong (inside)

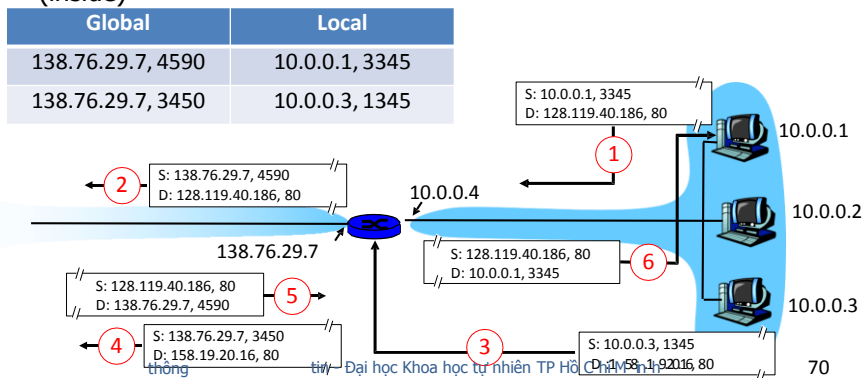
□ Ví dụ: $10.0.0.0/24 \Rightarrow 138.76.29.7$ và $138.76.29.8$



Overloading NAT

□ Cấu hình: $n \text{ local IP} \Leftrightarrow 1 \text{ global IP}$

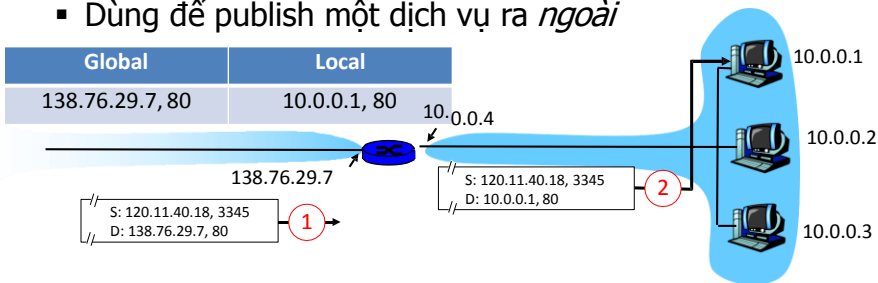
- NAT: $\langle \text{local IP, local port} \rangle \Leftrightarrow \langle \text{global IP, global port} \rangle$
- Có n kết nối đồng thời
- Bên ngoài (outside) **không** thể chủ động tạo kết nối với bên trong (inside)



Overlapping NAT

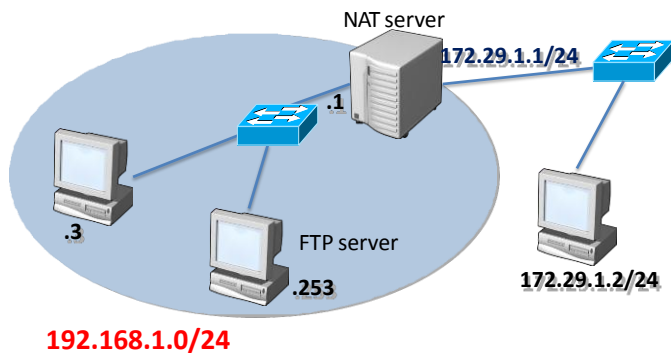
□ Cấu hình **cố định**: <local IP, port> ⇔ <global IP, port>

- Bên ngoài (outside) có thể chủ động tạo kết nối với bên trong (inside)
- Dùng để publish một dịch vụ ra *ngoài*



71

NAT – mô tả bài toán



□ Yêu cầu:

- Các máy tính trong LAN: 192.168.1.0/24 có thể truy cập ra ngoài bằng IP: 172.29.1.1
- Bên ngoài có thể truy cập dịch vụ FTP trên máy 192.168.3.253

72

NAT – Cấu hình Windows Server

- ❑ Chọn card public và private
 - Private: 192.168.1.1
 - Public: 172.29.1.1
- ❑ Chọn dịch vụ để publish (nếu có): Web
 - Local IP: 192.168.1.253
 - Incoming port: 80
 - Outgoing port: 80

73

Tài liệu tham khảo

- ❑ J.F Kurose and K.W. Ross về Computer Networking: A Top Down Approach