

CHƯƠNG 4

Kết nối Internet

Bùi Trọng Tùng
Bộ môn TT&MMT – Khoa CNTT
Trường Đại học BKHN

Cài đặt & Quản trị mạng - Bộ môn Truyền thông
& Mạng máy tính - CNTT - BKHN

1

Nội dung

1. Danh sách điều khiển truy cập
2. Mô hình kết nối tầng mạng – NAT
3. Mô hình kết nối tầng ứng dụng - Proxy

Cài đặt & Quản trị mạng - Bộ môn Truyền thông
& Mạng máy tính - CNTT - BKHN

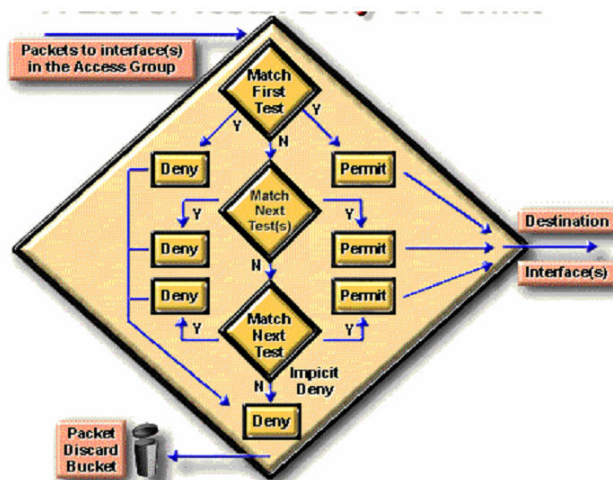
2

1. Danh sách điều khiển truy cập

1.1. Giới thiệu chung

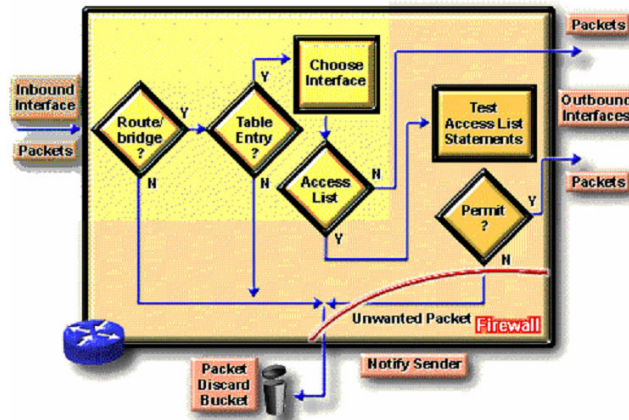
- ACL : Access Control List
- Đặc tả những điều kiện để router sẽ xử lý các gói tin vào ra mạng.
- Danh sách chuẩn(Standard ACL) : Kiểm tra địa chỉ nguồn của gói tin
 - ACL Number : 1-99, 1300-1999
- Danh sách mở rộng (Extended ACL) : Kiểm tra địa chỉ nguồn, địa chỉ đích, giao thức, cổng ứng dụng của gói tin
 - ACL Number : 100-199, 2000-2699

Nguyên tắc lọc gói



Nguyên tắc chuyển tiếp gói tin với ACL

1 ACL / 1 protocol / 1 interface



Cài đặt & Quản trị mạng - Bộ môn Truyền thông
& Mạng máy tính - CNTT - BKHN

5

1.2. Cài đặt ACL trên router

- Mặt nạ kiểm tra : 32 bit
 - Bit 0 : kiểm tra bit trong địa chỉ IP có vị trí tương ứng
 - Bit 1 : không kiểm tra bit trong địa chỉ IP có vị trí tương ứng

■ Ví dụ

128	64	32	16	8	4	2	1	Vị trí các bit trong byte và giá trị địa chỉ của nó
0	0	0	0	0	0	0	0	Mặt nạ kiểm tra tất cả các bit địa chỉ
0	0	1	1	1	1	1	1	Mặt nạ không kiểm tra 6 bits cuối cùng của địa chỉ
0	0	0	0	1	1	1	1	Mặt nạ không kiểm tra 4 bits cuối cùng của địa chỉ
1	1	1	1	1	1	0	0	Mặt nạ kiểm tra 2 bits cuối cùng của địa chỉ
1	1	1	1	1	1	1	1	Mặt nạ không kiểm tra địa chỉ

Cài đặt & Quản trị mạng - Bộ môn Truyền thông
& Mạng máy tính - CNTT - BKHN

6

Cài đặt ACL chuẩn

Router(config)# **access-list** *ACL-Number* {**deny** | **permit**}
 {*Source Source-Wildcard* | **host** *Source* | **any**}

ACL-Number	0-99
deny permit	Cấm Cho phép
Source	Địa chỉ IP tham chiếu
Source-Wildcard	Mặt nạ kiểm tra
host	Áp dụng với 1 địa chỉ IP chỉ định
any	Áp dụng với địa chỉ IP bất kì

#access-list 10 permit 172.16.0.1 0.0.31.254

#access-list 10 deny any

Cài đặt & Quản trị mạng - Bộ môn Truyền thông
& Mạng máy tính - CNTT - BKHN

7

Cài đặt ACL mở rộng

Router(config)#**access-list** *ACL-Number* {**deny** | **permit**}
 Protocol {*Source Source-Wildcard* | **host** *Source* | **any**}
 [*Operator Port*] {*Destination Destination-Wildcard* |
 host *Destination* | **any**} [*Operator Port*]

ACL-Number	100-199
Protocol	Giao thức cần kiểm tra
Operator	Toán tử : lt (<), gt (>), eq (=), neq (#), range
Port	Cổng ứng dụng cần kiểm tra

Cài đặt & Quản trị mạng - Bộ môn Truyền thông
& Mạng máy tính - CNTT - BKHN

8

Áp dụng ACL lên cổng giao tiếp

Router(config-if)#**ip access-group** *ACL-Number* {in | out}

2. NAT

2.1. Giới thiệu chung

- NAT : Network Address Translation
 - Chuyển đổi IP cục bộ sang IP công cộng
 - Và ngược lại
- PAT : Port Address Translation
 - NAT with overloading sử dụng thêm cổng ứng dụng
- Lợi ích:
 - Tiết kiệm địa chỉ IP công cộng
 - Che giấu địa chỉ riêng
 - Giảm chi phí cấu hình khi thay đổi ISP

Hoạt động của NAT/PAT

■ Các thuật ngữ

- Địa chỉ cục bộ bên trong (ILA)
- Địa chỉ công cộng bên trong (IGA)
- Địa chỉ cục bộ bên ngoài (OLA)
- Địa chỉ công cộng bên ngoài (OGA)

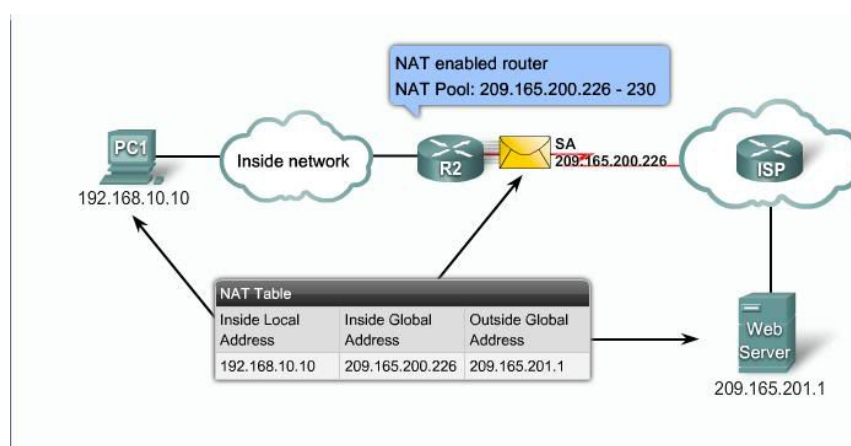
■ NAT Table

192.168.1.3	1.1.1.1	2.2.2.2
192.168.1.2	1.1.1.1	2.2.2.2

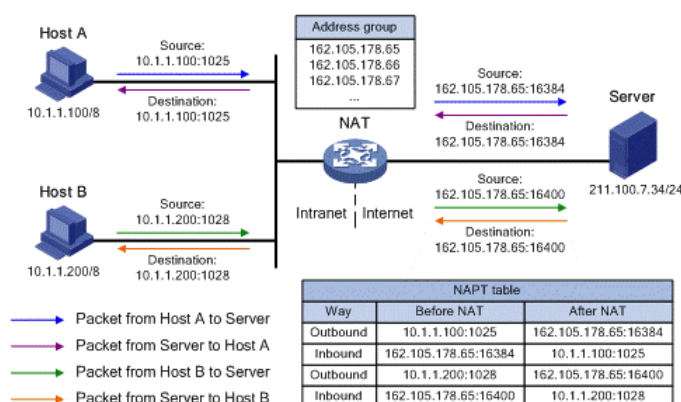
■ PAT Table

192.168.1.3 : 1000	1.1.1.1:2001
192.168.1.2 : 1000	1.1.1.1 : 2000

Hoạt động của NAT



Hoạt động của PAT



Cài đặt & Quản trị mạng - Bộ môn Truyền thông
& Mạng máy tính - CNTT - BKH

13

2.2. Cài đặt NAT trên router

■ Chuyển đổi tĩnh

Router (config) # ip nat inside source static *Local-IP Global-IP* //ánh xạ

Router (config) # interface *Interface-ID* //cổng vào

Router (config-if) # ip nat inside //đánh dấu cổng vào

Router (config-if) # exit

Router (config) # interface *Interface-ID* //cổng ra

Router (config-if) # ip nat outside

Cài đặt & Quản trị mạng - Bộ môn Truyền thông
& Mạng máy tính - CNTT - BKH

14

2.2. Cài đặt NAT trên router

■ Chuyển đổi động : n ILAs → 1 IGA

Router(config) # access-list *ACL-Number* permit *Source* *Source-wildcard*

// dải IP nội bộ được chuyển đổi

Router(config) # ip nat inside source list *ACL-Number* interface *Interface-ID*

// Ánh xạ

// Cổng vào

// Cổng ra

2.2. Cài đặt NAT trên router

■ Chuyển đổi động : n ILAs → n IGAs

Router (config) # ip nat pool *Name* *Start-IP* *End-IP* *NetMask*

//dải địa chỉ IGA

Router (config) # access-list *ACL-Number* permit *source*

Source-Wildcard

//dải địa chỉ ILA

Router (config) # ip nat inside source list *ACL-number* pool

Name // ánh xạ

// Cổng vào

// Cổng ra

2.2. Cài đặt PAT trên router

■ Chuyển đổi động : n ILAs → 1 IGA

Router(config) # access-list ACL-Number permit Source
Source-wildcard

// dải IP nội bộ được chuyển đổi

Router(config) # ip nat inside source list ACL-Number interface
Interface-ID overload

// Ánh xạ

// Cổng vào

// Cổng ra

2.2. Cài đặt PAT trên router

■ Chuyển đổi động : n ILAs → n IGAs

Router (config) # ip nat pool Name Start-IP End-IP NetMask
//dải địa chỉ IGA

Router (config) # access-list ACL-Number permit source
Source-Wildcard

//dải địa chỉ ILA

Router (config) # ip nat inside source list ACL-number pool
Name overload

// ánh xạ

// Cổng vào

// Cổng ra