BAB 6

Konfigurasi NAT, ACL dan DHCP

Objektif :

1. Mahasiswa dapat memahami Konsep Dasar NAT
2. Mahasiswa dapat memahami Konsep Dasar DHCP
3. Mahasiswa dapat memahami Konsep Dasar ACL
4. Mahasiswa dapat memahami Konfigurasi NAT pada Router Cisco
5. Mahasiswa dapat memahami Konfigurasi DHCP pada Router Cisco
6. Mahasiswa dapat memahami Konfigurasi ACL pada Router Cisco

Konsep Dasar NAT (Network Address Translation)

NAT adalah suatu metode untuk menghubungkan lebih dari satu komputer ke jaringan internet dengan menggunakan satu alamat IP. Banyaknya penggunaan metode ini disebabkan karena ketersediaan alamat IP yang terbatas, kebutuhan akan keamanan (Security), kemudahan serta fleksibilitas dalam administrasi jaringan.

NAT merupakan salah satu protokol dalam suatu sistem jaringan, NAT memungkinkan suatu jaringan dengan IP atau internet protokol yang bersifat privat IP belum teregistrasi di jaringan internet untuk mengakses jalur internet, hal ini berarti suatu alamat IP dapat mengakses internet dengan menggunakan IP Privat atau bukan menggunakan IP Public, NAT biasanya dibenamkan dalam sebuah router, NAT juga sering digunakan untuk menggabungkan atau menghubungkan dua jaringan yang berbeda, dan mentranslate atau menterjemahkan IP Privat dalam jaringan internal ke dalam jaringan yang legal network sehingga memiliki hak untuk melakukan akses data dalam sebuah jaringan. Tujuan NAT adalah mengurangi keterbatasan IPv4 dan menyembunyikan skema network internal.

Terminologi NAT

Berikut ini adalah istilah-istilah penting NAT :

- **Inside Local Adress** : source address sebelum translasi (IP private)
- **Outside Local Address** : destination address sebelum translasi (IP private)
- **Inside Global Address** : inside host setelah translasi (IP public)
- **Outside Global Address** : outside destination host setelah translasi (IP public)

IP Private

Yaitu IP yang digunakan oleh organisasi secara internal dan tidak dapat dirutekan di Internet. Jadi selain dari range IP di bawah ini adalah IP Public.

Class	Range
A	10.0.0.0 – 10.255.255.255
B	172.16.0.0 – 172.31.255.255
C	192.168.0.0 – 192.168.255.255

Keuntungan NAT

Berikut ini adalah keuntungan menggunakan NAT :

- Menghemat alamat IP secara legal
- Mengurangi overlap pengalamatan
- Meningkatkan fleksibilitas ketika berkomunikasi ke internet
- Mengurangi penomoran kembali jika terjadi perubahan network

Kerugian NAT

Berikut ini adalah kerugian menggunakan NAT :

- Terdapat delay pada proses switching
- Tidak dapat melakukan trace end-to-end IP
- Terdapat beberapa aplikasi yang tidak berfungsi ketika implementasi NAT

Tipe NAT

Tipe NAT terdiri dari NAT Static, NAT Dynamic, dan PAT (Port Address Translation). Berikut ini adalah penjelasan mengenai :

a). NAT Static

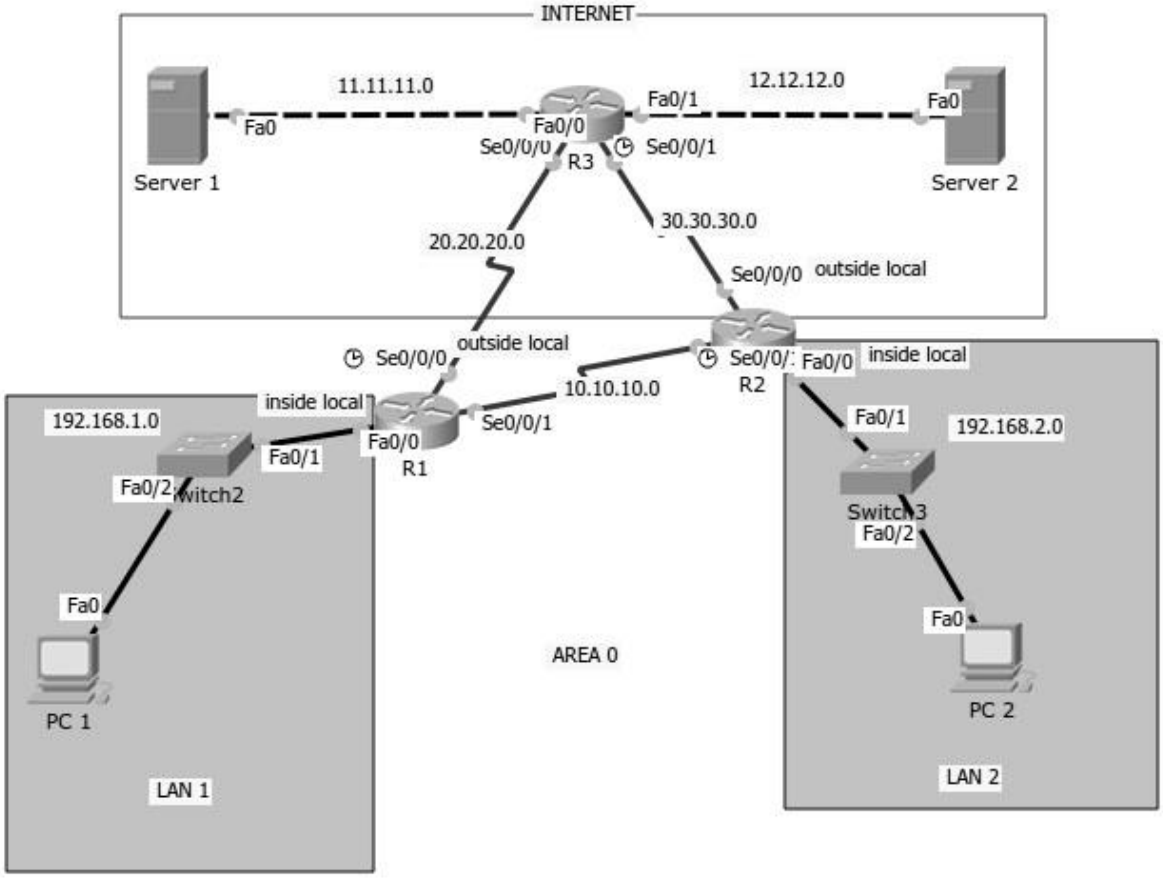
NAT Statis menggunakan table routing yang tetap, atau alokasi translasi alamat ip ditetapkan sesuai dengan alamat asal atau source ke alamat tujuan atau destination, sehingga tidak memungkinkan terjadinya pertukaran data dalam suatu alamat ip bila translasi alamat IPnya belum didaftarkan dalam table NAT. Berikut karakteristik NAT Static :

- Termasuk jenis *one-to-one* NAT, satu IP private ditranslate menjadi satu IP public
- Catatan : NAT static tiap host menggunakan IP public sendiri
- Bisa inisiasi komunikasi dari network outside global

Konfigurasi

Contoh topologi :

Untuk mempraktikkan konsep NAT Static ini, kita asumsikan bahwa semua area jaringan (kecuali jaringan LAN 1 dan LAN 2) menggunakan routing OSPF. Jaringan LAN 1 dan LAN 2 tidak diadvertise oleh OSPF sehingga masuk Network Private, sehingga untuk mengakses Internet dibutuhkan NAT. Agar jaringan LAN 1 dan LAN 2 tidak diadvertise oleh OSPF berarti kita tidak perlu memasukkan jaringan LAN 1 dan LAN 2 pada perintah OSPF di R1 maupun R2.



Tabel Addressing

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.1	255.255.255.0	N/A
	Se0/0/0	20.20.20.1	255.255.255.0	N/A
	Se0/0/1	10.10.10.1	255.255.255.0	N/A
R2	Fa0/0	192.168.2.1	255.255.255.0	N/A
	Se0/0/0	30.30.30.1	255.255.255.0	N/A
	Se0/0/1	10.10.10.2	255.255.255.0	N/A
R3	Fa0/0	11.11.11.1	255.255.255.0	N/A
	Fa0/1	12.12.12.1	255.255.255.0	N/A
	Se0/0/0	20.20.20.2	255.255.255.0	N/A
	Se0/0/1	30.30.30.2	255.255.255.0	N/A
Server 1	NIC	11.11.11.2	255.255.255.0	11.11.11.1
Server 1	NIC	12.12.12.2	255.255.255.0	12.12.12.1
PC 1	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC 2	NIC	192.168.2.2	255.255.255.0	129.168.2.1

Tampilan routing table R1

```
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

     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, Serial0/0/1
     11.0.0.0/24 is subnetted, 1 subnets
O       11.11.11.0 [110/65] via 20.20.20.2, 00:36:31, Serial0/0/0
     12.0.0.0/24 is subnetted, 1 subnets
O       12.12.12.0 [110/65] via 20.20.20.2, 00:36:31, Serial0/0/0
     20.0.0.0/24 is subnetted, 1 subnets
C       20.20.20.0 is directly connected, Serial0/0/0
     30.0.0.0/24 is subnetted, 1 subnets
O       30.30.30.0 [110/128] via 10.10.10.2, 00:36:21, Serial0/0/1
                   [110/128] via 20.20.20.2, 00:36:21, Serial0/0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
```

Tampilan routing table R2

```
R2#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

     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, Serial0/0/1
     11.0.0.0/24 is subnetted, 1 subnets
O       11.11.11.0 [110/65] via 30.30.30.2, 00:44:27, Serial0/0/0
     12.0.0.0/24 is subnetted, 1 subnets
O       12.12.12.0 [110/65] via 30.30.30.2, 00:44:27, Serial0/0/0
     20.0.0.0/24 is subnetted, 1 subnets
O       20.20.20.0 [110/128] via 10.10.10.1, 00:44:27, Serial0/0/1
                   [110/128] via 30.30.30.2, 00:44:27, Serial0/0/0
     30.0.0.0/24 is subnetted, 1 subnets
C       30.30.30.0 is directly connected, Serial0/0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

Dari output kedua routing table di R1 dan R2, sudah tidak terlihat lagi route menuju masing-masing jaringan LAN 1 dan LAN 2.

Tabel NAT R1

Private IP	Public IP
192.168.1.2	20.20.20.20
192.168.1.3	20.20.20.30
192.168.1.4	20.20.20.40

Tabel NAT R2

Private IP	Public IP
192.168.2.2	30.30.30.20
192.168.2.3	30.30.30.30
192.168.2.4	30.30.30.40

Langkah sederhana Konfigurasi NAT Static:

1. Tentukan interface NAT inside
2. Tentukan interface NAT outside
3. Buat translasi NAT dari source Private IP ke destination Public IP

Konfigurasi NAT Static di R1

Perintah untuk mengkonfigurasi NAT Static. Contoh IP Private 192.168.1.2 akan di NAT menjadi IP Public 20.20.20.20

```
R1(config)#interface f0/0
R1(config-if)#ip nat inside
R1(config-if)#interface s0/0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#ip nat inside source static 192.168.1.2 20.20.20.20
```

Konfigurasi NAT Static di R2

Perintah untuk mengkonfigurasi NAT Static. Contoh IP Private 192.168.2.2 akan di NAT menjadi IP Public 30.30.30.20

```
R2(config)#interface f0/0
R2(config-if)#ip nat inside
R2(config-if)#interface s0/0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#ip nat inside source static 192.168.2.2 30.30.30.20
```

Verifikasi

Tes Ping dari PC 1 ke Server 1

```
PC1>ping 11.11.11.2
Pinging 11.11.11.2 with 32 bytes of data:
Reply from 11.11.11.2: bytes=32 time=1ms TTL=254
Reply from 11.11.11.2: bytes=32 time=0ms TTL=254
Reply from 11.11.11.2: bytes=32 time=1ms TTL=254
Reply from 11.11.11.2: bytes=32 time=0ms TTL=254
Ping statistics for 11.11.11.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Tes Ping dari PC 2 ke Server 2

```
PC1>ping 12.12.12.2
Pinging 12.12.12.2 with 32 bytes of data:
Reply from 12.12.12.2: bytes=32 time=1ms TTL=254
Reply from 12.12.12.2: bytes=32 time=0ms TTL=254
Reply from 12.12.12.2: bytes=32 time=1ms TTL=254
Reply from 12.12.12.2: bytes=32 time=0ms TTL=254
Ping statistics for 12.12.12.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Dari tampilan diatas dapat diketahui bahwa PC 1 dan PC 2 yang berada di Private Network dapatberkomunikasi dengan server yang berada di Internet.

Tampilan NAT table di R1

```
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 20.20.20.20:13    192.168.1.2:13     11.11.11.2:13      11.11.11.2:13
icmp 20.20.20.20:14    192.168.1.2:14     12.12.12.2:14      12.12.12.2:14
---  20.20.20.20       192.168.1.2        ---                ---
---  20.20.20.2        192.168.1.2        ---                ---
```

Tampilan NAT table di R1

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 30.30.30.20:31    192.168.2.2:31     11.11.11.2:31      11.11.11.2:31
icmp 30.30.30.20:32    192.168.2.2:32     12.12.12.2:32      12.12.12.2:32
---  30.30.30.20       192.168.2.2        ---                ---
```

b). NAT Dynamic

Konsep Dasar

- Termasuk tipe *many-to-many* NAT, IP private dalam jumlah banyak kemudian ditranslatemenjadi IP public yang banyak juga dengan menyediakan sebuah pool IP public
- Kita tidak perlu melakukan translate satu per satu, cukup sediakan IP public sesuai jumlah user yang akan terkoneksi ke Internet

Konfigurasi

Contoh topologi :

Topologi yang digunakan pada konfigurasi ini sama dengan topologi yang digunakan pada NAT static.

Pool NAT R1

Private IP (ACL 1)	Public IP (POOL R1)
192.168.1.0 /24	20.20.20.10 - 20.20.20.20

Pool NAT R2

Private IP (ACL 1)	Public IP (POOL R2)
192.168.2.0 /24	30.30.30.10 – 30.30.30.20

Langkah sederhana setting NAT Dynamic:

1. Tentukan interface NAT inside
2. Tentukan interface NAT outside
3. Tentukan permit ACL Private Network
4. Tentukan pool Public IP
5. Buat translasi NAT dari source ACL ke destination pool Public IP

Setting NAT Dynamic di R1

Perintah untuk mensetting NAT Dynamic

```
R1(config)#interface f0/0
R1(config-if)#ip nat inside
R1(config-if)#
R1(config-if)#interface s0/0/0
R1(config-if)#ip nat outside
R1(config-if)#
R1(config-if)#exit
R1(config)#
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)#
R1(config)#ip nat pool POOLR1 20.20.20.10 20.20.20.20 netmask 255.255.255.0
R1(config)#
R1(config)#ip nat inside source list 1 pool POOLR1
```

Setting NAT Dynamic di R2

Perintah untuk mensetting NAT Dynamic

```
R2(config)#interface f0/0
R2(config-if)#ip nat inside
R2(config-if)#
R2(config-if)#interface s0/0/1
R2(config-if)#ip nat outside
R2(config-if)#
R2(config-if)#exit
R2(config)#
R2(config)#access-list 1 permit 192.168.2.0 0.0.0.255
R2(config)#
R2(config)#ip nat pool POOLR2 30.30.30.10 30.30.30.20 netmask 255.255.255.0
R2(config)#
R2(config)#ip nat inside source list 1 pool POOLR2
```

Verifikasi

Tes Ping dari PC 1 ke Server 1

```
PC1>ping 11.11.11.2
Pinging 11.11.11.2 with 32 bytes of data:
Reply from 11.11.11.2: bytes=32 time=1ms TTL=254
Reply from 11.11.11.2: bytes=32 time=0ms TTL=254
Reply from 11.11.11.2: bytes=32 time=1ms TTL=254
Reply from 11.11.11.2: bytes=32 time=0ms TTL=254
Ping statistics for 11.11.11.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Tes Ping dari PC 2 ke Server 2

```
PC1>ping 12.12.12.2
Pinging 12.12.12.2 with 32 bytes of data:
Reply from 12.12.12.2: bytes=32 time=1ms TTL=254
Reply from 12.12.12.2: bytes=32 time=0ms TTL=254
Reply from 12.12.12.2: bytes=32 time=1ms TTL=254
Reply from 12.12.12.2: bytes=32 time=0ms TTL=254
Ping statistics for 12.12.12.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Dari tampilan diatas dapat diketahui bahwa PC 1 dan PC 2 yang berada di Private Network dapatberkomunikasi dengan server yang berada di Internet.

Tampilan NAT table di R1

```
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 20.20.20.10:7     192.168.1.2:7      11.11.11.2:7       11.11.11.2:7
icmp 20.20.20.10:8     192.168.1.2:8      12.12.12.2:8       12.12.12.2:8
```

Tampilan NAT table di R2

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 30.30.30.10:24    192.168.2.2:24     11.11.11.2:24      11.11.11.2:24
icmp 30.30.30.10:25    192.168.2.2:25     12.12.12.2:25      12.12.12.2:25
```

Dari tampilan NAT tabel di R1dapat dilihat proses translasi dari host 192.168.1.2 menjadi 20.20.20.10 dengan tujuan host 11.11.11.2 dan 12.12.12.2. Dan R2 dari host 192.168.2.2 menjadi 30.30.30.10 dengan tujuan host 11.11.11.2 dan 12.12.12.2.

c). NAT Dynamic Overload (PAT)

Konsep Dasar

- Tipe NAT yang paling popular
- Termasuk tipe *many-to-one* NAT
- Dengan menyediakan satu IP public dapat mentranslate IP private yang banyak denganmenggunakan pembeda yaitu port
- Disebut juga sebagai NAT Dynamic Overload, Port Address Translation (PAT), atau NAT

Konfigurasi

Contoh topologi :

Topologi yang digunakan pada konfigurasi ini sama dengan topologi yang digunakan pada NAT static.

Pool NAT R1

Private IP (ACL 1)	Public IP (POOL R1)
192.168.1.0 /24	20.20.20.10

Pool NAT R2

Private IP (ACL 1)	Public IP (POOL R2)
192.168.2.0 /24	30.30.30.10

Langkah sederhana setting NAT Dynamic PAT:

1. Tentukan interface NAT inside
2. Tentukan interface NAT outside
3. Tentukan permit ACL Private Network
4. Tentukan pool Public IP (terdiri dari single Public IP)
5. Buat translasi NAT dari source ACL ke destination pool Public IP

Setting NAT Dynamic PAT di R1

Perintah untuk mensetting NAT Dynamic PAT.

```
R1(config)#interface f0/0
R1(config-if)#ip nat inside
R1(config-if)#
R1(config-if)#interface s0/0/0
R1(config-if)#ip nat outside
R1(config-if)#
R1(config-if)#exit
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)#
R1(config)#ip nat pool POOLR1 20.20.20.10 20.20.20.10 netmask 255.255.255.0
R1(config)#
R1(config)#ip nat inside source list 1 pool POOLR1 overload
```

Setting NAT Dynamic PAT di R2

Perintah untuk mensetting NAT Dynamic PAT.

```
R2(config)#interface f0/0
R2(config-if)#ip nat inside
R2(config-if)#
R2(config-if)#interface s0/0/1
R2(config-if)#ip nat outside
R2(config-if)#
R2(config-if)#exit
R2(config)#
R2(config)#access-list 1 permit 192.168.2.0 0.0.0.255
R2(config)#
R2(config)#ip nat pool POOLR2 30.30.30.10 30.30.30.10 netmask 255.255.255.0
R2(config)#
R2(config)#ip nat inside source list 1 pool POOLR2 overload
```

Verifikasi

Tes Ping dari PC 1 ke Server 1

```
PC1>ping 11.11.11.2
Pinging 11.11.11.2 with 32 bytes of data:
Reply from 11.11.11.2: bytes=32 time=1ms TTL=254
Reply from 11.11.11.2: bytes=32 time=0ms TTL=254
Reply from 11.11.11.2: bytes=32 time=1ms TTL=254
Reply from 11.11.11.2: bytes=32 time=0ms TTL=254
Ping statistics for 11.11.11.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Tes Ping dari PC 2 ke Server 2

```
PC1>ping 12.12.12.2
Pinging 12.12.12.2 with 32 bytes of data:
Reply from 12.12.12.2: bytes=32 time=1ms TTL=254
Reply from 12.12.12.2: bytes=32 time=0ms TTL=254
Reply from 12.12.12.2: bytes=32 time=1ms TTL=254
Reply from 12.12.12.2: bytes=32 time=0ms TTL=254
Ping statistics for 12.12.12.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Dari tampilan diatas dapat diketahui bahwa PC 1 dan PC 2 yang berada di Private Network dapat berkomunikasi dengan server yang berada di Internet.

Tampilan NAT table di R1

```
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 20.20.20.10:10    192.168.1.2:10     11.11.11.2:10      11.11.11.2:10
icmp 20.20.20.10:11    192.168.1.2:11     12.12.12.2:11      12.12.12.2:11
icmp 20.20.20.10:12    192.168.1.2:12     11.11.11.1:12      11.11.11.1:12
```

Tampilan NAT table di R1

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 30.30.30.10:28    192.168.2.2:28     11.11.11.2:28      11.11.11.2:28
icmp 30.30.30.10:29    192.168.2.2:29     12.12.12.2:29      12.12.12.2:29
icmp 30.30.30.10:30    192.168.2.2:30     11.11.11.1:30      11.11.11.1:30
```

Dari tampilan NAT tabel di R1 dapat dilihat proses translasi dari host 192.168.1.2 menjadi 20.20.20.10 dengan tujuan host 11.11.11.2 dan 12.12.12.2. Dengan menggunakan single-IP address Public, maka yang membedakan tiap sessionnya yaitu port. Dan begitu pun dengan tampilan NAT table di R2.

Konsep Dasar DHCP (Dynamic Host Configuration Protocol)

DHCP adalah protokol berbasiskan arsitektur client/server yang diaplikasikan untuk mempermudah pengalokasian IP Address pada suatu jaringan. Sebuah jaringan lokal yang tidak menggunakan DHCP diharuskan secara manual memberikan IP Address kepada semua komputer. Jika DHCP terpasang pada jaringan lokal, maka semua komputer yang terhubung ke jaringan akan memperoleh IP Address secara otomatis dari DHCP server. Selain IP Address banyak parameter jaringan yang dapat diberikan oleh DHCP, misalnya default gateway dan DNS server.

Proses pertukaran data antara DHCP Server dan DHCP klien

Konfigurasi

Contoh Topologi :

Topologi yang digunakan pada konfigurasi ini sama dengan topologi yang digunakan pada NAT static.

Login console ke R1 dan R2 untuk mempraktikkan konfigurasi DHCP

Untuk mensetting DHCP di R1, berikut ini perintah yang digunakan :

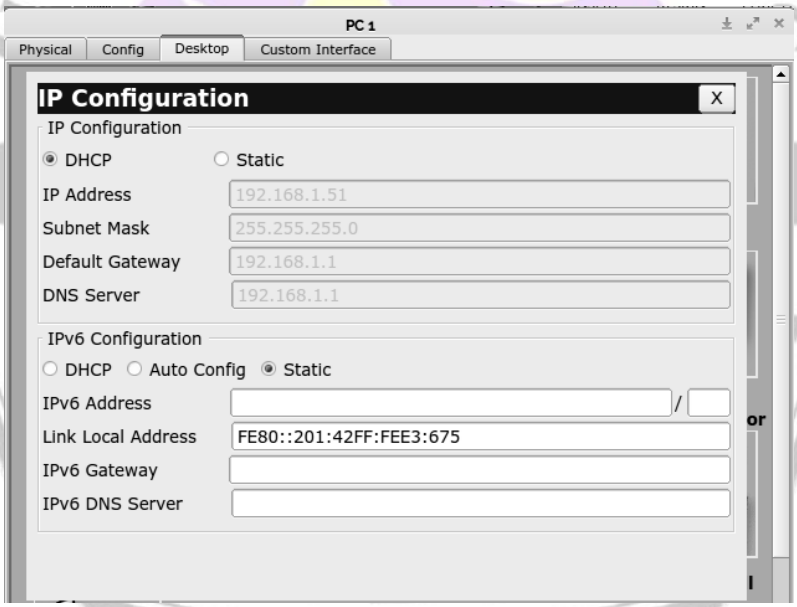
```
R1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.50
R1(config)#ip dhcp pool Pool_R1
R1(dhcp-config)#network 192.168.1.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.1.1
R1(dhcp-config)#dns-server 192.168.1.1
```

Keterangan:

excluded-address	: untuk menentukan IP yang tidak boleh di lease oleh DHCP, biasanyaberupa IP static untuk server / printer
pool	: tentukan nama pool DHCP, misal untuk network 192.168.1.0 namanya Pool_R1
network	: menentukan network DHCP
default-router	: menentukan default gateway untuk klien
dns-server	: menentukan dns server untuk klien

Verifikasi

Klik **PC 1** -> Pilih **Desktop** -> Pilih **IP Configuration** -> Pilih **DHCP**



Keamanan Menggunakan ACL

Dalam dunia jaringan cukup banyak *threats* (potensi serangan). Berbagai treats yang mengancam network security seperti contoh nya *viruses,worms,trojan horses, spyware, adware, hacker attacks,DoS,* dan masih banyak lainnnya.

Pada bab ini akan membahas tentang keamanan jaringan dengan menggunakan Cisco Access List(ACL). Cisco ACL merupakan sebuah metode yang digunakan untuk menyeleksi paket paket yang keluar masuk *network.* Ada beberapa tipe ACL, yaitu :

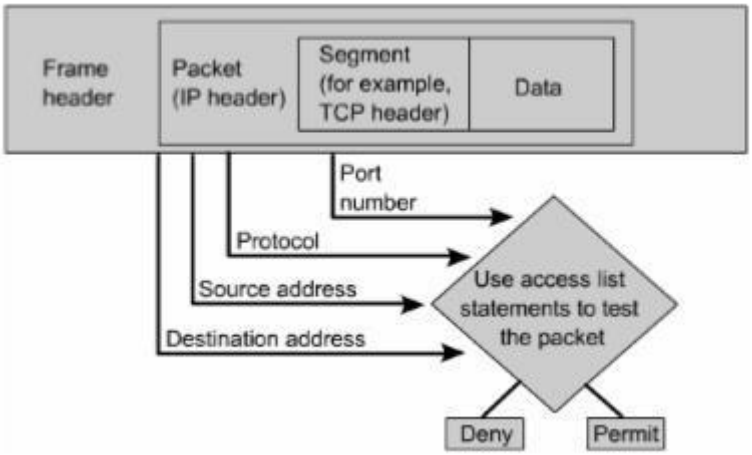
- Standard IP
- Extended IP
- IPX
- AppleTalk

Pada materi ini kita akan membahas ACL jenis *Standard* dan *Extended IP*.

Penjelasan Cisco Access List (ACL)

Untuk mem-filter trafik jaringan, ACL menentukan jika paket itu dilewatkan atau diblok pada interface router. Router ACL membuat keputusan berdasarkan alamat asal, alamat tujuan, protokol, dan nomor port.

ACL harus didefinisikan berdasarkan protokol, arah atau port. Untuk mengontrol aliran trafik pada interface, ACL harus didefinisikan setiap protokol pada interface. ACL kontrol trafik pada satu arah dalam interface. Dua ACL terpisah harus dibuat untuk mengontrol trafik inbound dan outbound. Setiap interface boleh memiliki banyak protokol dan arah yang sudah didefinisikan. Jika router mempunyai dua interface diberi IP, AppleTalkdan IPX, maka dibutuhkan 12 ACL. Minimal harus ada satu ACL setiap interface.



Cisco ACL memeriksa paket pada header upper-layer

Grup access list dalam Router

Berikut ini adalah fungsi dari ACL:

- Membatasi trafik jaringan dan meningkatkan unjuk kerja jaringan. Misalnya, ACL memblok trafik video, sehingga dapat menurunkan beban jaringan dan meningkatkan unjuk kerja jaringan.
- Mengatur aliran trafik. ACL mampu memblok update routing. Jika update tidak dibutuhkan karena kondisi jaringan, maka bandwidth dapat dihemat.
- Mampu membrikan dasar keamanan untuk akses ke jaringan. Misalnya, host A tidak diijinkan akses ke jaringan HRD dan host B diijinkan.
- Memutuskan jenis trafik mana yang akan dilewatkan atau diblok melalui interface router. Misalnya, trafik email dilayani, trafik telnet diblok.
- Mengontrol daerah-daerah dimana klien dapat mengakses jaringan.

- Memilih host-hots yang diijinkan atau diblok akses ke segmen jaringan. Misal, ACL mengijinkan atau memblok FTP atau HTTP.

Penerapan access list itu sendiri terbagi menjadi dua macam, antara lain:

- Standard Access List - yang akan melakukan penyeleksian paket berdasarkan alamat IP pengirim paket.
- Extended Access List - yang akan menyeleksi sebuah paket berdasarkan alat IP pengirim dan penerima, protokol, dan jenis port paket yang dikirim.

Ketika ACL dikonfigurasi pada sebuah router, maka ACL harus memiliki sebuah nomor identifikasi unik yang diberikan kepadanya. Nomor ini menandakan jenis access list yang dibuat dan harus berada pada range tertentu dari nomor yang valid untuk jenis daftar tersebut.

Jenis Access List	Range Nomor Pengenal
IP Standard	1-99
IP Extended	100-199
IPX Standard	800-899
IPX Extended	900-999
Apple Talk	600-699
IPX SAP Filter	1000-1099

Fungsi dari wildcard mask

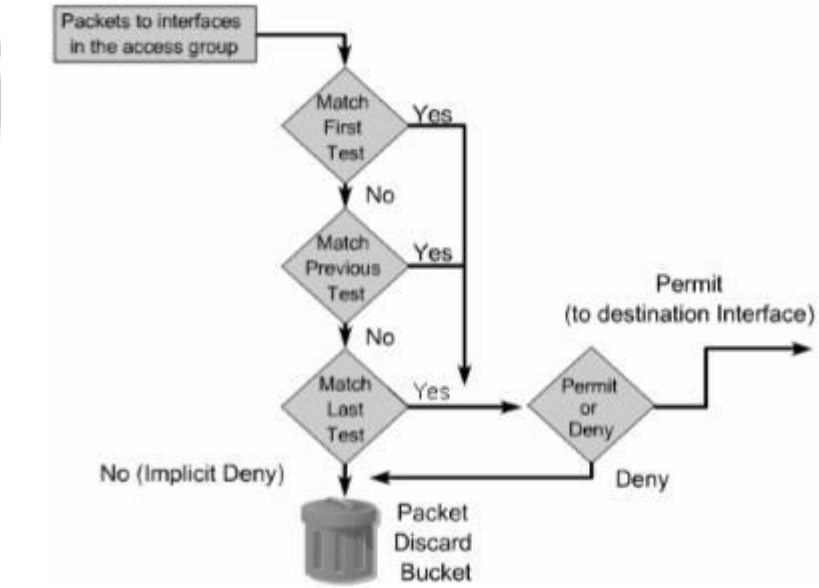
Wildcard mask panjangnya 32-bit yang dibagi menjadi empat octet. Wildcard mask adalah pasangan IP address. Angka 1 dan 0 pada mask digunakan untuk mengidentifikasikan bit-bit IP address. Wildcard mask mewakili proses yang cocok dengan ACL mask-bit. Wildcard mask tidak ada hubungannya dengan subnet mask.Wildcard mask dan subnet mask dibedakan oleh dua hal. Subnet mask menggunakan biner 1 dan 0 untuk mengidentifikasi jaringan, subnet

dan host. Wildcard mask menggunakan biner 1 atau 0 untuk memfilter IP address individual atau grup untuk diijinkan atau ditolak akses. Persamaannya hanya satu dua-duanya sama-sama 32-bit.

```
Router(config)#access-list 1 permit 0.0.0.0 255.255.255.255

Can be written as:
Router(config)#access-list 1 permit any

Router(config)#access-list 1 permit 172.30.16.29 0.0.0.0

Can be written as:
Router(config)#access-list 1 permit host 172.30.16.29
```

Ada dua kata kunci di sini yaitu any dan host. Any berarti mengganti 0.0.0.0 untuk IP address dan 255.255.255.255 untuk wildcard mask. Host berarti mengganti 0.0.0.0 untuk mask. Mask ini membutuhkan semua bit dari alamat ACL dan alamat paket yang cocok. Opsi ini akan cocok hanya untuk satu alamat saja.

Cara kerja Cisco Access List



Keputusan dibuat berdasarkan pernyataan/statement cocok dalam daftar akses dan kemudian menerima atau menolak sesuai apa yang didefinisikan di

daftar pernyataan. Perintah dalam pernyataan ACL adalah sangat penting, kalau ditemukan pernyataan yang cocok dengan daftar akses, maka router akan melakukan perintah menerima atau menolak akses.

Pada saat frame masuk ke interface, router memeriksa apakah alamat layer 2 cocok atau apakah frame broadcast. Jika alamat frame diterima, maka informasi frame ditandai dan router memeriksa ACL pada interface inbound. Jika ada ACL, paket diperiksa lagi sesuai dengan daftar akses. Jika paket cocok dengan pernyataan, paket akan diterima atau ditolak. Jika paket diterima di interface, ia akan diperiksa sesuai dengan table routing untuk menentukan interface tujuan dan di-switch ke interface itu. Selanjutnya router memriksa apakah interface tujuan mempunyai ACL. Jika ya, paket diperiksa sesuai dengan daftar akses. Jika paket cocok dengan daftar akses, ia akan diterima atau ditolak. Tapi jika tidak ada ACL paket diterima dan paket dienkapsulasi di layer 2 dan di-forward keluar interface device berikutnya.

Konfigurasi Cisco Access List(ACL)

ACL terbagi dua jenis :

Standard ACL :

Diletakkan dekat dengan destination, nomor yang dipakai biasanya 1-99, tidak dapat memilih port atau traffic yang diatur, semua kena. Perintahnya :

Router(config)#access-list numberacl permit|deny sourcenetwork wildcardsourcenetwork

Terapkan pada interface :

Router(config)#interface interface number

Router(config-if)#ip access-group numberacl in|out

Pada akhir setiap ACL statement, letakkan perintah :

Router(config)#access-list numberacl permit any

Perhatikan :

- Host dengan wildcard 0.0.0.0 dapat digantikan dengan kata-kata "host",

Contoh :

IP tunggal

192.168.10.1 0.0.0.0

Dapat ditulis juga :

Host 192.168.10.1

- Seluruh network dengan pernyataan :

0.0.0.0 255.255.255.255

Dapat digantikan dengan kata :

any

Extended ACL :

Diletakkan dekat dengan source, nomor yang dipakai biasanya 100-199, dapat memilih protocol ataupun port yang diatur. Perintahnya :

Router(config)#access-list numberacl permit | deny protocol sourcenetwork wildcard sourcenetwork destinationnetwork wilcarddestinationnetwork eq | lt | gt | neq servicename/serviceport

Terapkan pada interface :

Router(config)#interface interface number

Router(config-if)#ip access-group numberacl in|out

Pada akhir ACL statement, pasang perintah :

Router(config)#access-list numberacl permit ip any any

Perintah-perintah show :

a) Melihat statement ACL :

Router(config)#show access-list

b) Melihat arah inbound atau outbound ACL :

Router(config)#show ip interface

c) Melihat ACL di running-config :

Router(config)#show run

Standard dari exteded ACL yang di pelajari merupakan numbered ACL, ada pula named ACL yang terdiri dari standard dan extended ACL

Contoh :

a) Named Standard ACL

Router(config)# ip access-list standard namedacl
Router(config-std-nacl)# permit | deny sourcenetw wildcardsourcenetw
Router(config)#interface interface numberint
Router(config)#ip access-group namedacl in|out

b) Named Extended ACL

Router(config)# ip access-list extended namedacl
Router(config-ext-nacl)# permit | deny protocol sourcenetw wildcardsourcenetw destinationnetw wildcarddestinationnetw eq | lt | gt | neq protocol/port Router(config)#ip access-group nameacl in|out

Selain access-list, juga terdapat access-class yang diterapkan pada line vty atau telnet line.