

シスコプログラミング勉強会

cisco 1600



開催期間：2001年10月から12月
週1回90分程度
参加者：中嶋、佐藤、土屋

コンピュータの作るネットワーク（インターネット）は、世界中どこにでも繋がっているように思われるかも知れないが、ルーターの動いていない状態では、そのコンピュータが属する同じネットワークアドレスを持った、そのネットワーク内部でしか通信が出来ない。その閉じた世界をインターネットに繋ぐのがルーターの役割である。

ルーターはネットワーク内の必要なパケットだけを上流に配送する。これは不要な負荷をネットワークにかけないという点においても、余分な情報を外に出さないというセキュリティ面においても重要である。

またその逆に上流から流れてくるパケットを選択し必要なものだけを適切に下流に流す。近接する互いのルーターは、最適経路でパケットを配送するために、経路情報を常に交換し内部にマップを作ってパケットを制御している。

かつては複数のネットワークインターフェースを持つコンピュータがその役割を担っていたが、OSの持つ脆弱性、あるいはパフォーマンスの点から、今日では専用のハードウェアが使われることが多くなった。その代表がアメリカ CISCO 社の製品で、矢上キャンパスでも多数使われている。

CISCO のプログラミングは不馴れなものには理解が難しいとされているが、勉強会を開いて理解を深めることにした。

ciscoのプログラム例

ここでは2つのイーサネット、1つのWAN用シリアルポートを持つciscoを仮想し、上流側のルーティングプロトコル OSPFをRIPに変換し内側に流す設定、およびアクセスリストを使って特定のマシンへのメール転送を制限している。

```
version 11.1
service password-encrypting
service udp-small-servers
service tcp-small-servers
!
hostname expr-router
!
enable secret 5 $1$XV31$Yizkg3/P9tkGglzBAC0bs/
!
interface Ethernet0
ip address 131.113.1.100 255.255.255.0
ip access-group 101 in
ip ospf authentication-key 1 23456789ABCDEFH
!
interface Ethernet1
ip address 131.113.100.200 255.255.255.128
!
interface Serial0
no ip address
encapsulation frame-relay ietf
bandwidth 128
frame-relay lmi-type ansi
!
router rip
 redistribute ospf 1 metric 3
 network 131.113.0.0
 distribute-list 20 in
!
ip classless
logging buffered
access-list 101 deny ip host any 101.113.100.150 smtp
access-list 101 deny ip host any 101.113.100.161 smtp
access-list 101 deny ip host any 101.113.100.172 smtp
access-list 101 deny ip host any 101.113.100.183 smtp
access-list 101 permit ip any any
access-list 20 deny any
!
!
line con 0
line vty 0 4
 password *****
!
login
```

ciscoの操作例

(ルーティングテーブルの表示)

```
RouterB#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 a
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

A --> R 10.0.0.0/8 [120/1] via 192.168.3.253, 00:00:24, FastEthernet0/1
R 192.168.1.0/24 [120/1] via 192.168.2.254, 00:00:20, FastEthernet0/0
C 192.168.2.0/24 is directly connected, FastEthernet0/0
B --> C 192.168.3.0/24 is directly connected, FastEthernet0/1
RouterB#
```

ここではCISCO内部に作成されたルーティングテーブルを表示させている。

Aでは目的地10.0.X.Xのネットワークへは、192.168.3.253のルータを経由することがRIPプロトコルによってテーブルに登録されたことを示す。

Bでは192.168.3.Xのネットワークはこのルータの100 Mイーサネットインタフェース0/1によって直接繋がっていることが分かる。

ルータ同士は、最適なルーティング経路を決定するため、常に互いに通信する。回線の速さ、目的地までの距離、混雑具合などを考慮し、最適ルートを決定し、ルータ内部にテーブルを作成する。回線状況は常に変わるので、それに応じて最適ルートも常に更新される。ルート決定のアルゴリズムには様々なものがあるが、理工学部では、OSPF、RIPなどが広く用いられている。

一つのネットワークドメイン
ドメイン内のパケットとR1、R2経由で下流から受け取ったパケットの内、上流へ流す必要のあるものだけを送出する。

このドメイン宛とR1、R2経由で流すべきパケットだけを選択して取り込む。下流へは最も適切なルータを選択する。

ルーター機能はUNIXマシンなどでも行うことができるが、専用ルータはセキュリティの高さ、機能の豊富さ、パフォーマンスの高さ、設定の容易さなどの点において勝っているため、現在では広く用いられるようになった。

