

修士論文 2001年度(平成13年度)

広域ネットワークにおけるトラフィック特性を  
考慮した経路選択機構の構築

慶應義塾大学大学院 政策・メディア研究科  
安田 歩

# 修士論文要旨

## 広域ネットワークにおけるトラフィック 特性を考慮した経路選択機構の構築

インターネットの爆発的な普及と増加により、インターネットの利用者は急増し、ネットワークを流れるトラフィックの形態は多様化している。また、インターネットを構成する通信路も様々な種類のものが現れている。インターネット上で利用されるアプリケーションは、伝送帯域や伝送品質の保証、あるいは実時間性をネットワークに要求するようになってきている。一方、既存の経路制御プロトコルに基づいた経路制御機構では、ネットワークの特性や状態を考慮したり、アプリケーションからの要求を考慮したパケット転送は一部でしか実現されていない。

本研究では、様々なネットワークの特性を考慮し、アプリケーションからの要求やネットワーク管理者の要求をより柔軟にパケット転送に反映させるための機構を提案した。これに基づき、同一の宛先ノードに対して複数の経路を持つ2つのルータ間で、自由度の高い統合的なパケット転送を実現する経路選択機構を設計し、実装した。また、本機構で実装した機能を多数のルータに搭載することにより、インターネット上の任意の2地点間でポリシーに基づいた経路選択が可能となることを示した。

本研究で提案した手法に基づいて設計・実装した機構を、実ネットワーク上に構築し、評価を行なった。評価を行なったネットワークは、片方向通信路を含み、また、複数の受信専用局が存在するため、マルチキャスト通信を行なうにも適している。

この結果、本研究で提案した手法が、ネットワークの状態と利用者の要求を考慮した経路選択機構として有用であることを証明し、マルチキャスト通信を行なう際にも適していることを示した。

### キーワード

1. インターネット
2. 経路制御
3. 経路選択機構
4. Traffic Engineering
5. QoS

慶應義塾大学 政策・メディア研究科  
安田 歩

# Abstract of Master's Thesis

## Constructing Route Selection Apparatus Considering Traffic Feature in Widely Network

Explosive popularization and growth of the Internet has resulted in rapid increase of the Internet users, and diversification in forms of network traffic. Traffic-path infrastructures of which networks are composed are also getting more and more intricatated. On the other hand, software applications made for the use on the Internet are demanding higher qualities on genre like traffic bandwidth, traffic guarantee, and realtime communication to the networks. However, only some parts of the packet-transferring mechanism which considers network characteristics, network status, and the demands from the software applications are implemented by routing-control apparatuses depending on the existing routing protocols. This research proposes an architecture which reflects the demands from the applications and the demands from the network administrators flexibly by considering the various network characteristics. Based on this architecture, route selection apparatus, which implements flexible and integrative packet transfers between two routers having multiple routes, is designed and implemented. Additionally, this paper implies the availability of the route selection between discretional two routers on the Internet by running the functions implemented for this apparatus on number of routers. I have conducted the evaluation of the system designed and implemented according to the system proposed in this research by setting up the system on actual networks. Networks used in this evaluation suites the communication using Multicast since they include Uni-directional Link and has multiple Receive Only Station. As the result of the evaluation, system proposed in this research is proven to be effective as a network status and the user demands considered, route selection apparatus, and also showed suitable for communication using Multicast.

### Keywords

1. Internet
2. Routing
3. Route Selection Apparatus
4. Traffic Engineering
5. QoS

KEIO University Graduate School of Media and Governance  
Ayumu Yasuda

# 目次

<b>第 1 章</b>	<b>序論</b>	<b>1</b>
1.1	はじめに	1
1.2	研究背景	1
1.3	本研究の目的	2
1.4	本論文の構成	3
<b>第 2 章</b>	<b>経路制御の問題点</b>	<b>4</b>
2.1	既存の経路制御機構	4
2.1.1	RIP	4
2.1.2	OSPF	5
2.2	Traffic Engineering の必要性	5
2.3	関連研究：MPLS	5
2.3.1	MPLS の概要	6
2.3.2	MPLS を用いた Traffic Engineering	6
2.3.3	MPLS の問題点	8
2.4	Traffic Engineering を実現しているプロトコル	9
2.4.1	cisco のポリシールーティング	10
2.4.2	IGRP	10
2.4.3	OSPF の equal cost multi-path	11
2.4.4	SCTP	11
2.4.5	IDPR	12
2.5	既存の経路制御機構の問題点のまとめ	12
<b>第 3 章</b>	<b>経路選択機構の提案</b>	<b>13</b>
3.1	本機構で実現する目標	13
3.2	本機構で解決する問題	14
3.3	本機構で想定するネットワーク	14
3.4	対象とする利用者	16
3.4.1	エンドユーザからの利用	16
3.4.2	ネットワーク管理者からの利用	16
3.4.3	ポリシーの最終的な決定権	16
3.5	経路選択機構	17

3.5.1	経路選択機構の概念的な位置付け	17
3.5.2	経路選択機構の全体像	18
3.6	ポリシーの定義	18
3.7	既存のルータへの組み込み	19
3.8	広域性への対応	19
3.9	既存の Traffic Engineering との違い	21
3.10	source routing との違い	21
3.11	既存の経路制御機構との関わり	21
3.12	UDL との親和性	22
3.13	マルチキャストとの親和性	22
3.14	本機構の利用モデル	23
<b>第 4 章</b>	<b>設計</b>	<b>25</b>
4.1	基本設計方針	25
4.2	設計概要	25
4.2.1	経路選択機構の全体	25
4.2.2	処理の流れ	26
4.3	policy server	27
4.3.1	policy server の役割	27
4.3.2	ポリシーの正当性の審査	27
4.3.3	選択先経路の正当性の審査	28
4.4	route selector	28
4.4.1	route selector の役割	28
4.4.2	回線の状態の検知	28
4.5	end point	29
4.5.1	end point の役割	29
4.6	条件が衝突する際の制御	29
4.6.1	衝突が生じる例 1	29
4.6.2	衝突が生じる例 2	30
4.6.3	衝突を回避する手法	31
4.7	ルーティンググループの回避	32
4.8	経路選択の機能を必要としない場合	33
4.9	予想される問題点	33
<b>第 5 章</b>	<b>実装</b>	<b>34</b>
5.1	policy server の実装	34
5.2	route selector の実装	35
5.2.1	経路選択の処理の実装	35
5.2.2	パケット転送の処理の流れ	35
5.3	end point の実装	36

<b>第 6 章</b>	<b>評価</b>	<b>37</b>
6.1	評価手法	37
6.2	単一ルータによる経路選択との比較	37
6.2.1	システムの概要	37
6.2.2	設計・実装	38
6.3	単一ルータの経路選択による限界	39
6.4	単一ルータによる経路選択との比較	39
6.5	実ネットワークでの評価	40
6.5.1	AI3 Network の概要	40
6.5.2	衛星ネットワークの特性	40
6.5.3	評価環境の構築	41
6.5.4	経路選択の実験	42
6.6	評価のまとめ	42
<b>第 7 章</b>	<b>結論</b>	<b>44</b>
7.1	まとめ	44
7.2	今後の課題	45

## 目 次

1.1	2 地点間で使用される経路 . . . . .	2
2.1	L3 routing と L2 switching の比較 . . . . .	6
2.2	経路の決定方法の相違を述べるための前提ネットワーク . . . . .	7
2.3	MPLS ドメイン内のパス . . . . .	9
2.4	cisco のポリシールーティングの例 . . . . .	10
3.1	本研究が前提とするネットワークの例 . . . . .	15
3.2	経路選択機構の概念的な位置付け . . . . .	17
3.3	経路選択機構の構成 . . . . .	18
3.4	多数のルータによる経路選択機構の構築 . . . . .	20
3.5	本機構上でのマルチキャストの利用 . . . . .	23
3.6	VPN での使用例 . . . . .	24
4.1	本機構の処理の流れ . . . . .	26
4.2	ポリシーが衝突する例 1 . . . . .	30
4.3	ポリシーが衝突する例 2 . . . . .	30
4.4	各リンクのコストを考慮したネットワークトポロジ . . . . .	32
5.1	policy server . . . . .	34
5.2	sysctl で見たポリシーの設定例 . . . . .	35
6.1	単一のルータで経路選択を行なう場合のネットワークトポロジ . . . . .	38
6.2	AI3 Network の概念的トポロジ . . . . .	41
6.3	評価に関係する AI3 Network のトポロジ図 . . . . .	43

## 表 目 次

2.1	既存の経路制御機構のルータ A の経路表の例 . . . . .	7
2.2	既存の経路制御機構のルータ B の経路表の例 . . . . .	8
2.3	MPLS を用いたルータ A の経路表の例 . . . . .	8
2.4	MPLS を用いたルータ B の経路表の例 . . . . .	8
4.1	ポリシーが衝突する条件の例 1 . . . . .	29
4.2	ポリシーが衝突する条件の例 2-1 . . . . .	31
4.3	ポリシーが衝突する条件の例 2-2 . . . . .	31
4.4	条件が衝突した場合に優先される client . . . . .	31
6.1	経路を選択する機構の性能評価 . . . . .	40



# 第1章 序論

## 1.1 はじめに

本研究では、インターネット上の任意の2地点間を通るトラフィックの経路を自由に選択できる機構を実現する。これにより、ネットワークの帯域を有効に活用できる。また、トラフィックの特性に見合った経路を選択でき、効率の良い通信が可能となる。

## 1.2 研究背景

今日、インターネットの生活基盤としての役割が増し、その重要性が高まってきている。

インターネットを構成する回線の種類は増加し、それに合わせて回線が持つ特性も多様化してきている。一方、ネットワークを利用するユーザも増え、ユーザが用いるアプリケーションは、ネットワークに対して様々な要求を出すようになってきている。この要求には、実時間性を重視するもの、ネットワークの帯域容量を重視するものなどが挙げられる。

しかし、既存の経路制御機構では、ネットワーク管理者やユーザがネットワークの特性を考慮してトラフィック毎に適切な経路を選択することはできず、アプリケーションが利用する回線を自由に選択する機構は存在しない。

また、インターネット上には、バックアップのためだけに存在するネットワークなど、冗長なネットワークが数多くある。しかし、冗長なネットワークは定常状態ではトラフィックがほとんど流れていないなど、有効に利用されていない。その一方で、定常的に使用されているネットワークでは、トラフィックが増えて帯域を圧迫しているという問題が起きている。このように、現在のインターネットでは回線の利用が効率的でない。

現在のインターネットでは、パケットが通過する2地点間の経路は、経路制御プロトコルに基づく経路制御機構により決定されている。インターネット上で任意の2地点 A,B を結ぶ経路が複数存在する場合、一般的には地点 A から地点 B に向かうトラフィックは、図 1.1 に示すように経路制御プロトコルにより決定される一つの経路しか利用されない。

例外として、source routing や QoS routing などが挙げられる。しかしこれらは、現状ではユーザの要求を十分に満たしたり、ネットワークの無駄な

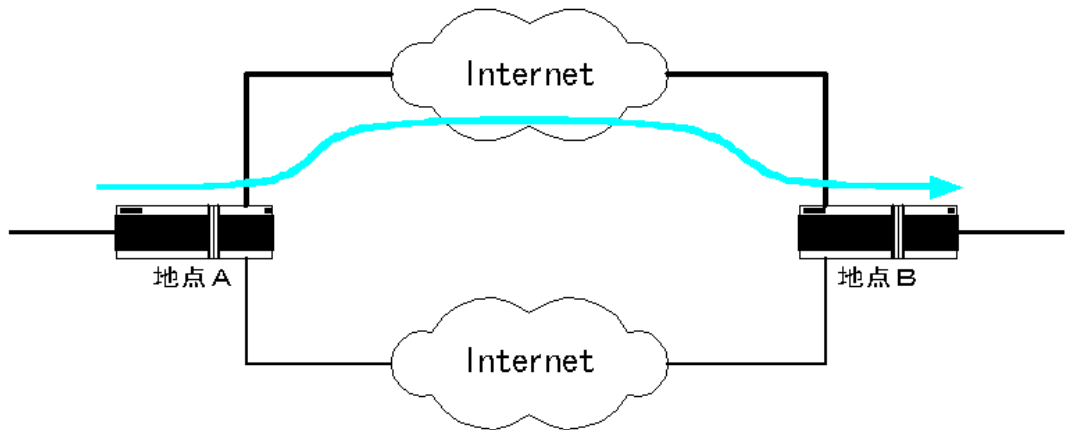


図 1.1: 2 地点間で使用される経路

冗長性を回避したりしている訳ではない。

### 1.3 本研究の目的

本研究では、次に述べる 2 つの事項を大きな目的とする。

#### ネットワーク帯域の有効活用

冗長な回線を有効に活用し、トラフィックと対比して帯域に余裕がないネットワークの負荷を減らす。

#### 経路選択の自由

ユーザやネットワーク管理者が、トラフィックの種類などの様々なポリシーにより、任意の 2 地点間を通過するトラフィックの経路を、自由に選択できるようにする。

これにより、現在あるネットワークを有効に活用し、アプリケーションの要求を満足させることが可能となる。

このことを実現するため、広域なネットワークにおいてトラフィック毎に通過する経路を選択できる統合的な経路選択機構を設計して構築し、評価を行なう。

## 1.4 本論文の構成

本論文は、本章を含めて7章から構成される。本章では、本研究の背景および目的を述べた。第2章では、現在実現されている経路制御機構の概要と問題点を明白にする。第3章で問題点の解決手法を示し、解決を実現するモデルを提案する。第4章で経路選択機構の設計を行ない、第5章で実装について述べる。第6章では本研究で実装した機構の性能評価を行なう。最後に、第7章で本研究の結論と、今後の課題について述べる。

## 第2章 経路制御の問題点

本章では、既存の経路制御プロトコルによる経路制御、および Traffic Engineering による経路制御について論じる。これを基に、既存の経路制御機構で実現されていない機能や問題点を明確にする。

### 2.1 既存の経路制御機構

インターネットでは、ネットワークを構成する回線の種類が多様化し、ネットワークポロジも複雑になる一方である。

このようなネットワークの AS(Autonomous System) 内の経路制御には、RIP[1] や OSPF[2]、IS-IS[3] などの IGP(Interior Gateway Protocol) が用いられている。これらの経路制御プロトコルでは、ルータ同士が協調して経路表を生成してゆくことで、自律分散的に経路制御を行なっている。

しかし、これらの経路制御プロトコルに基づく経路制御機構は、あらゆるユーザの、あらゆる要求を完全に満たしている訳ではない。

現在インターネットで使用されている代表的な IGP である、RIP と OSPF の動作概要と、経路の選択に関する問題点について述べる。

#### 2.1.1 RIP

各ルータは、隣接しているルータと経路情報を交換する。RIP では接続しているネットワークに経路表をブロードキャストすることで経路情報の交換を行なっている。

RIP の問題点として、次のことが挙げられる。

- metric の最大値が 15 である
- ネットワークの負荷や帯域容量を考慮した経路選択が困難である
- ブロードキャストを多用する
  - ネットワークに負荷がかかる
  - ネットワーク全体に経路情報が伝達する収束時間が遅くなる
- 認証機構が存在しない

RIP では、ホップ数、つまり宛先ノードまでの間に経由するルータの数が少ない経路が、パケットが転送される経路として選択される。このため、経路の選択に関する問題として、ホップ数が少なければ回線のスループットが低い経路が選択されるということが挙げられる。

### 2.1.2 OSPF

各ルータは、自身が接続しているネットワークの情報を、ネットワーク全体に通知する。各ルータはこの情報を基にネットワークトポロジを構築し、経路表を作成する。

OSPF では、ホップ数ではなく実際の回線の速度に基づいてコストを計算し、よりスループットの大きい経路を選択する。回線速度とは、回線の帯域容量と遅延である。このため、経路制御に、信頼性などの回線の特性が考慮されることはない。意図的に経路を選択する場合には、管理者が手動でコストを設定しなければならない。

## 2.2 Traffic Engineering の必要性

Traffic Engineering とは、ネットワーク資源である帯域の利用率を最適な状態に維持し、ネットワークの転送能力を向上させることである。

この点においては、第 2.1 節で述べたように、経路制御プロトコルによって生成される経路表を用いた既存の経路制御機構は、充分ではない。

ユーザが使用するアプリケーションは多岐に渡り、ネットワーク内に存在する回線の種類や性質も多様化している。ネットワークが、ユーザの様々な要求を満たすためには、適切な回線を選択が必要となっている。

一方、広い帯域を有するネットワーク資源は非常に高価なものである。高価な回線を有効に活用し、ネットワークの運用コストを下げる為にも、最適な経路選択や、明示的なトラフィックの経路変更が必要となってきている。

Traffic Engineering を実現することにより、ネットワーク管理者は、定義されたドメイン内においてトラフィックのフローを管理でき、各回線のトラフィック量を制御することができる。

## 2.3 関連研究：MPLS

現在 Traffic Engineering を実現している技術の一つとして、MPLS(Multi Protocol Label Switching) について述べる。

### 2.3.1 MPLS の概要

経路制御プロトコルに基づいた経路制御では、パケットの宛先アドレスに基づき、ルータが経路を選択する。一方、MPLS では、パケットに付与されたラベルに基づき、ルータおよびスイッチが経路を選択する。

従来のパケット転送機構では、パケットの宛先アドレスを経路表で検索して、適切な next hop ルータおよびパケットが送出されるインターフェースを決定する。MPLS では、ラベルを用いて経路の選択を行なうことにより、ルータで経路制御の処理にかかるオーバーヘッドを削減し、高速な経路制御が実現できる。従来のパケット転送方式と、ラベルを用いたパケット転送方式の関係を、図 2.1 に示す。

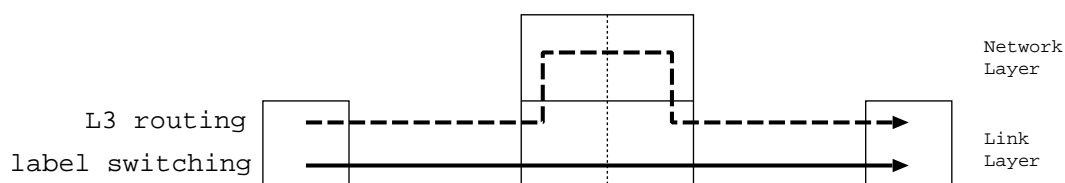


図 2.1: L3 routing と L2 switching の比較

実際には、ラベルは、MAC アドレスなどのデータリンク層のアドレスに対応しており、固定長で扱う。ネットワーク層で行なうパケット転送をホップバイホップ転送と呼ぶのに対し、ラベルスイッチによる転送を、カットスルー転送と呼ぶ。

図 2.2 を基に、従来の経路表を用いた経路の決定方法と、ラベルによる経路の決定方法の違いを述べる。ルータの側に表示している添字は、インターフェース名である。

ルータ A、ルータ B における、経路制御機構による経路表を簡単にしたものを表 2.1、表 2.2 に示す。既存の経路制御機構による経路制御では、宛先アドレスを経路表で検索する。この処理は、ネットワーク層で行なう。MPLS のラベルに基づく経路表を簡単にしたものを、表 2.3、表 2.4 に示す。

### 2.3.2 MPLS を用いた Traffic Engineering

MPLS を用いることによって、Traffic Engineering を実現できる。[4] MPLS を用いた Traffic Engineering の特徴を以下に挙げる。

- パケット転送にはラベルを使用
- 転送のポリシーは、IGP から注入

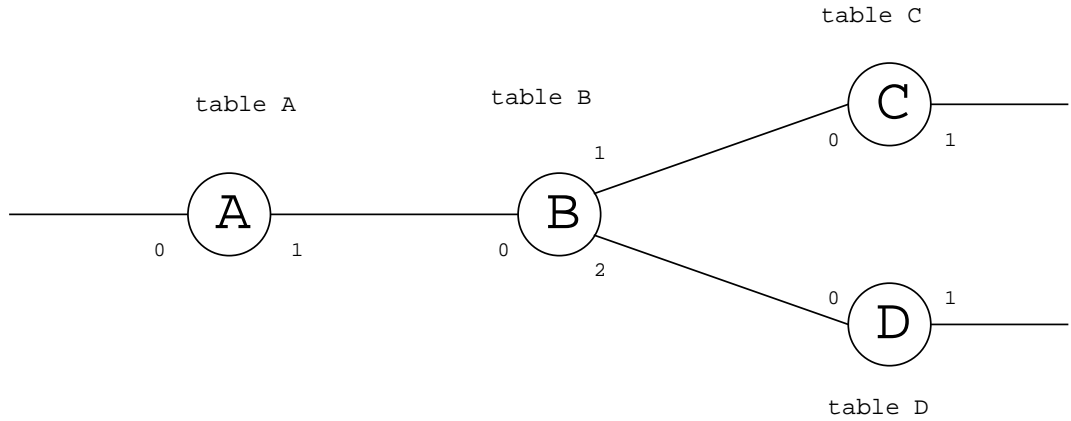


図 2.2: 経路の決定方法の相違を述べるための前提ネットワーク

表 2.1: 既存の経路制御機構のルータ A の経路表の例

destination	next hop	out I/F
10.1/16	B	1
10.2/16	B	1
10.3/16	B	1
10.4/16	B	1

- RSVP-extension を使用して、LSP(Label Switched Path) を確立
- パケットの転送経路には、LSP を利用

MPLS ドメインのエッジルータ間でパスを確立させ、明示的な経路制御が可能となる。

エッジルータ間のパスは、RSVP-extension[5][6] を使用して LSP を確立し、トンネルとして利用する。

図 2.3 は MPLS ドメイン内で、エッジルータ E1 から E2 までパスを確立させた図である。図中の実線が LSP である。E はエッジルータを、C はコアルータを表す。

また、MPLS を用いた Traffic Engineering では、ドメイン全体でポリシーを反映させる。

表 2.2: 既存の経路制御機構のルータ B の経路表の例

destination	next hop	out I/F
10.1/16	C	1
10.2/16	D	2
10.3/16	D	2
10.4/16	D	2

表 2.3: MPLS を用いたルータ A の経路表の例

in label	destination	next hop	out label
-	10.1/16	B	5
-	10.2/16	B	7
-	10.3/16	B	6
-	10.4/16	B	1

### 2.3.3 MPLS の問題点

ラベルスイッチで使用する LSP を設定するためには、次の 2 つの方式がある。[7]

- フロー・ドリブン
 

ある特定の packets がラベルスイッチルータ (LSR) を通過する時に、LSP が設定される。トラフィックが一定時間流れないと、LSP は解放される。フロー・ドリブンの場合、次の欠点が挙げられる。

  - LSP が生成される前に流れる packets は、ホップバイホップ転送

表 2.4: MPLS を用いたルータ B の経路表の例

in label	destination	next hop	out label
5	10.1/16	C	4
7	10.2/16	D	9
6	10.3/16	D	3
1	10.4/16	D	2



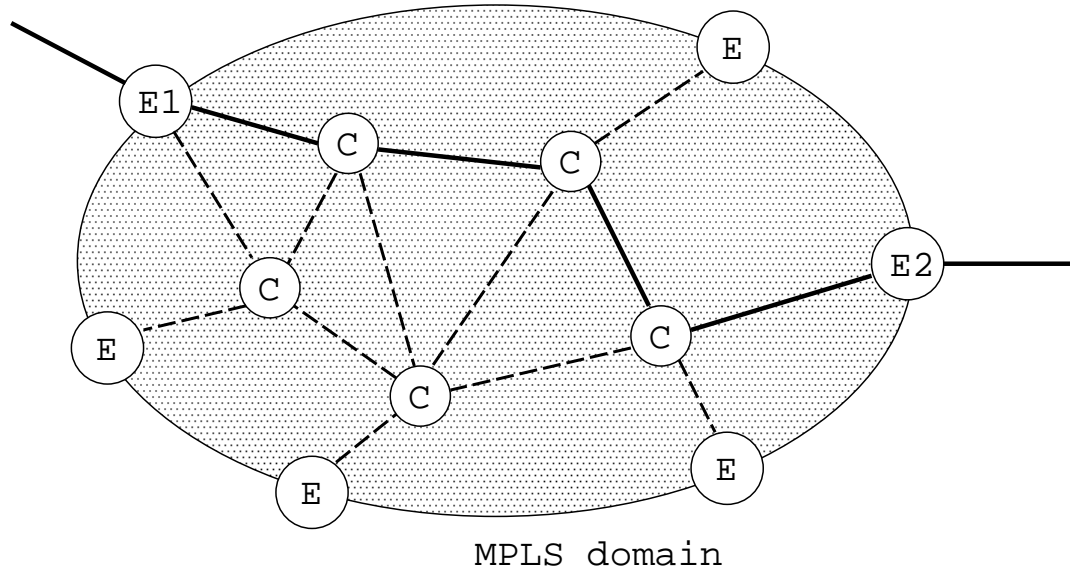


図 2.3: MPLS ドメイン内のパス

される

- フローの数が多くなると、ラベルが急増する
- トポロジ・ドリブン
  - 経路表に新たに経路エントリが加わった時に、LSP が設定される。経路表からそのエントリが削除された時、LSP は解放される。トポロジ・ドリブンの場合、次の欠点が挙げられる。
  - 経路エントリの数だけラベルが必要となる
  - フロー毎の制御ができない

## 2.4 Traffic Engineering を実現しているプロトコル

既存のプロトコルで、Traffic Engineering を実現しているものについて述べる。

### 2.4.1 cisco のポリシールーティング

cisco [8] のポリシールーティング [9] の機能は、パケットの送信元、あるいは送信元と宛先の組み合わせに基づいて経路制御をする。この例を図 2.4 に示す。

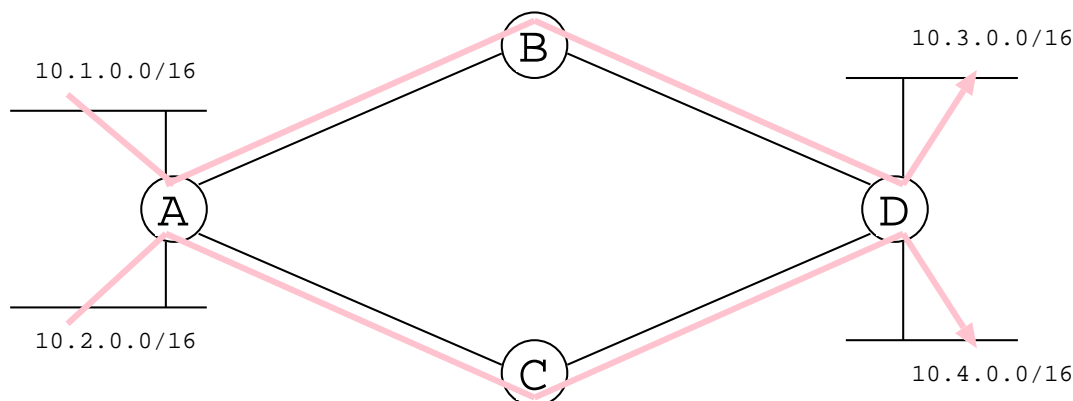


図 2.4: cisco のポリシールーティングの例

cisco のポリシールーティングを用いると、図 2.4 の場合、10.1.0.0/16 のネットワークから 10.3.0.0/16 のネットワークへ到達したい時はルータ B を経由させ、10.2.0.0/16 のネットワークから 10.4.0.0/16 のネットワークへ到達した時はルータ C を経由させるということが出来る。

ポリシールーティングを実行する際、ポリシールーティングの対象となるトラフィックに対して、複数の next hop ルータを指定できる。これは、最初に指定した next hop ルータに到達性がない場合でも、その他のルータ経由で宛先に到達できるようにするためである。ポリシールーティングで指定した全てのルータに到達性がない場合は、経路表に従ったパケット転送をすることが可能である。

### 2.4.2 IGRP

IGRP(Interior Gateway Routing Protocol) は、cisco が独自に策定した経路制御プロトコルである。[10]

同じ宛先に対して 2 つの経路が存在する場合、この 2 つの経路の転送遅延を比較するために、複合メトリックを使用する。複合メトリックでは、次の値が考慮される。

- 回線が持つ遅延時間 (D)

- 帯域容量 (B)
- 信頼性 (R)
- 負荷 (L)

信頼性は、経路のエラーレートを表す。エラーレートとは、パケットが、指定された経路を辿って宛先まで届く確率であり、255 を 100% としている。負荷は、2 地点間で辿る経路の中で、最も帯域容量の小さく使用率が高くなる回線の負荷を表す。255 を 100% としている。

複合メトリック (M) の値は、次の計算式によって導き出される。各項の係数を、 $a_1$  から  $a_5$  で表す。

$$M = \left( \frac{a_1 B + a_2 B}{255 - L} + a_3 D \right) \times \frac{a_4}{R + a_5}$$

係数  $a_1$  から  $a_5$  に任意の値を入れることで、ネットワーク管理者は先に挙げた要素の値を調整できる。

### 2.4.3 OSPF の equal cost multi-path

OSPF では、同一の宛先ノードに対して複数の経路が存在する場合、コストが等しい全ての経路でトラフィックを均等に分割する。しかし、パケットの到着順序を重視する TCP では、同一のフローのパケットを複数の経路に分散させることは、パフォーマンスの低下を招く。このため、パケットの送信元アドレス、宛先アドレス、宛先ポート番号からハッシュコードを生成し、フローを識別してフロー毎に振り分けを行なう。ただし、既存の OSPF の実装では実現されていない。

### 2.4.4 SCTP

SCTP[11][12] は、トランスポート層のプロトコルの一つとして定義されている。

TCP とは異なり、コネクションの確立に four-way handshake を用いる。これにより blind attack に対して強固となり、信頼性のあるパケット転送が可能となる。

2 地点間で複数経路が存在する場合に、互いのネットワークアドレスとポート番号で、パスを確立する。同一の 2 者の間で同時に確立されるパスは、唯一つである。

また、SCTP では、一定の条件の下、宛先に到達できなかったパケットの再転送を別の回線で行なう。

#### 2.4.5 IDPR

IDPR(Inter-Domain Policy Routing)[13][14][15] は、AS間でポリシールーティングを行なうためのプロトコルである。

ネットワークマップを定義し、このマップに基づくポリシールートの計算を行なう。

また、OSPFのequal cost multi-pathと同等の機能をドメイン間のものとして有しているが、現時点で実装が存在せず、動作実績がない。

### 2.5 既存の経路制御機構の問題点のまとめ

これまで述べてきたように、既存の動的経路制御では、宛先までのホップ数や、回線のスループットに基づいた方法でしか経路を選択することができない。

また、これらの問題を解決しようとしているいくつかの、Traffic Engineeringを実現している機能でも、十分に解決できているとは言えない。

結果として現状では、トラフィック制御に対するネットワーク資源の最適化はされていない。このため、効率的な回線の利用が難しい。IGPを用いても自律的にネットワーク全体のパフォーマンスを向上させることは、現状では不可能である。

つまり、現時点では、エンドユーザが適切なQoS(Quality of Service)を享受することは難しいと言える。

## 第3章 経路選択機構の提案

本章では、既存のネットワーク資源を有効活用し、アプリケーションからネットワークへの要求を可能な限り満足させるために、経路選択機構を提案する。

### 3.1 本機構で実現する目標

本研究では、インターネット上に存在するあらゆる回線を有効かつ適切に活用して、ネットワーク上で次に挙げる項目を考慮した経路制御を実現する。また、アプリケーションが発生させる要求を考慮し、ユーザの要望に見合ったトラフィックの制御を行なう。

- 最短経路
- 回線の遅延
- 回線の輻輳状態
- 回線の帯域容量

ネットワークでの最短経路を意識した経路制御は、既存の経路制御機構で実現されている。本研究で実現する経路制御では、トラフィックが最短経路のパスを通ることには拘らない。最短経路を通ることよりも、ユーザからの要求や回線の特性、状態を考慮することを重視する。

回線が持つ特性として、遅延や信頼性が挙げられる。回線の持つ特性によって生じる遅延は、アプリケーションにとって重要な要素である。実時間性を重視する通信を行なうアプリケーションでは、遅延が重要である。一方、ファイル転送のような通信では、実時間性をそれほど必要としない。

本機構では、ネットワーク遅延のような回線の特性を考慮し、輻輳状態、帯域容量といった回線の状態に見合った経路をアプリケーションが選択できるようにする。

これにより、ネットワーク管理者およびエンドユーザにとっての QoS の実現が可能となる。

## 3.2 本機構で解決する問題

第2章で述べたように、従来の経路制御機構では送信元から宛先までの中間ルータの数や、回線のスループットから算出したメトリックに基づいた方法でしか、経路を選択することができない。

しかし、今日、ユーザからネットワークに対する要求は多様化してきている。その中で、前述した以外の様々なポリシーによる経路選択が実現されていないという問題が挙げられる。

既存の経路制御機構は、経路制御プロトコルに支配されている。このため、ネットワークの管理者やエンドユーザが、パケットが通る経路を柔軟に設定することができない。一部実現されてはいるものの、必要条件が厳しかったり、実現できる機能が限られていたりする。

本研究では、この問題点を解決するために、経路選択機構を提案する。

## 3.3 本機構で想定するネットワーク

本研究で提案する経路選択機構は、あらゆるネットワーク環境で使用できることを目標とする。本機構を構築するのに適したネットワークの環境および条件を述べる。

ここで、本研究が前提とするネットワークトポロジの具体例を図3.1に示す。

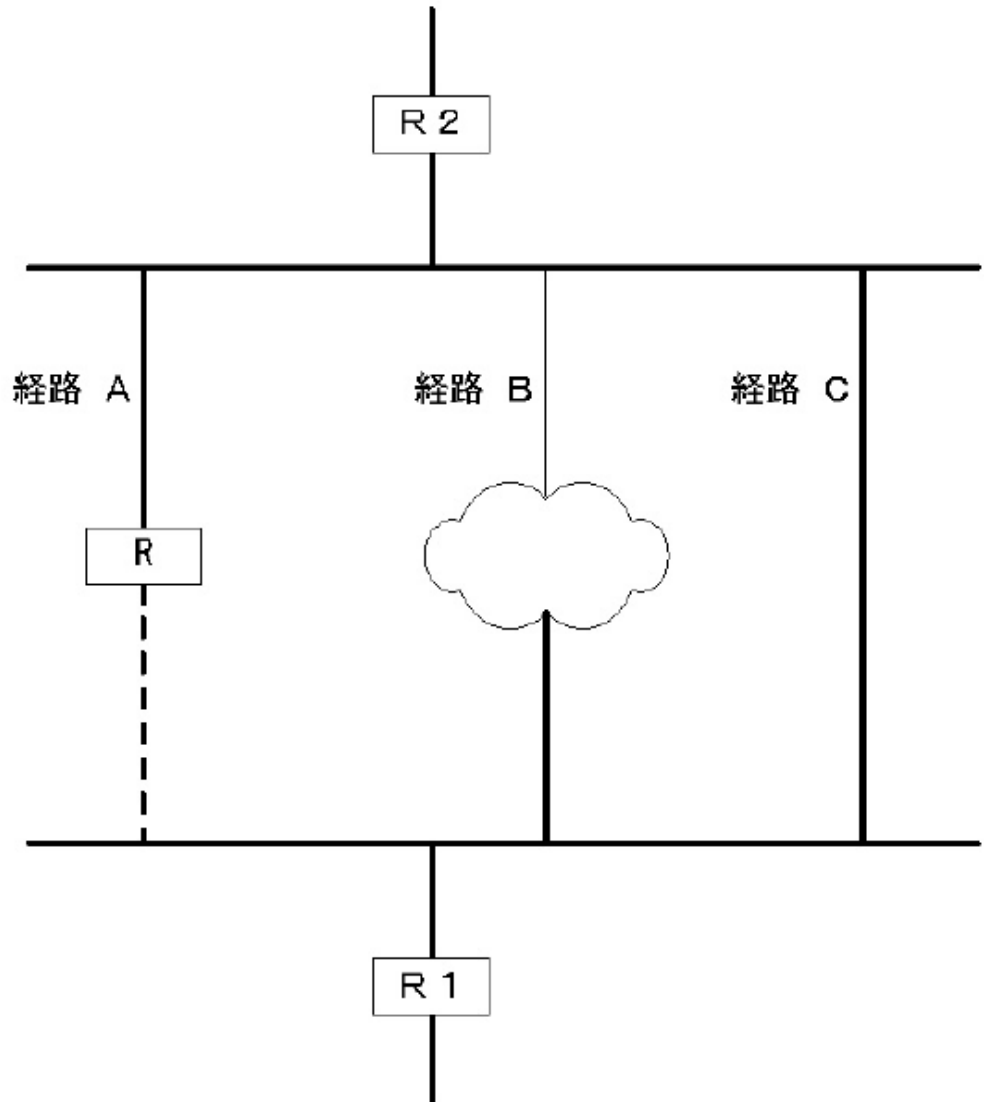


図 3.1: 本研究が前提とするネットワークの例

このネットワークが持つべき必要条件を、以下に挙げる。

- 2つのルータ間に複数の経路が存在する
- ネットワーク特性の異なる回線である

図 3.1 の例では、2つのルータ R1, R2 の間にネットワーク特性の異なる3つの経路 A,B,C が存在する。2つのルータ間に、いくつの経路が存在しても良い。また、経路 B の例のように、AS を跨ぐような経路でも問題ない。

## 3.4 対象とする利用者

本機構では、経路の選択を要求する者として、ネットワーク管理者とエンドユーザを想定する。ネットワーク管理者とは、トラフィックの振り分けを行なうルータの管理者を指す。エンドユーザは、2地点間での経路選択を要求するユーザのことである。

本論文では、このネットワーク管理者とエンドユーザを合わせて、client と呼ぶ。client が、経路選択機構に経路選択のポリシーを申請することができる。

### 3.4.1 エンドユーザからの利用

エンドユーザは、経路選択を行なう2地点を通るトラフィックを経路選択の対象として、本機構にポリシーを申請できる。このエンドユーザは、2地点間で経路の選択を行なう者であれば、ネットワーク上のどこに存在していても良い。

本機構を利用することにより、エンドユーザは経路選択の対象となるパケットと、選択先の経路を指定することができる。

### 3.4.2 ネットワーク管理者からの利用

ネットワークの管理者は、管理しているネットワークに流れるトラフィックの状態を常に把握し、注意している必要がある。

ネットワークを流れるトラフィックが帯域容量を超過した場合、現在のインターネットでは通信速度が極端に遅くなり、また帯域容量から溢れたトラフィックは到達性を失うという問題が起こる。管理するネットワークに、回線の物理的な障害が発生した時などのための冗長性が確保されている場合であっても、その冗長な回線が活用されることなくこの問題は生じる。

ネットワークの管理者は、2地点間を通過するパケットに対して任意に経路選択のポリシーを決定することができる。これにより、冗長的な部分の回線を利用し、トラフィックの流れを支配して前述の問題を防ぐことが可能となる。

また、ネットワーク管理者は、client の一つとしてエンドユーザと同じようにポリシーを申請することもできる。

### 3.4.3 ポリシの最終的な決定権

多数のユーザから要求された複数の条件が衝突した時には、誰かが衝突を回避するための制御を行なわなければならない。また、複数のユーザに対して優先度を付ける場合も、申請された要求全体を把握して判断する者が必要である。このため、あらゆるトラフィックの経路選択に関して最終的な決定



権を持つ者が存在しなければならない。

本機構では、この権利を経路選択を行なうネットワーク管理者に割り当てる。経路選択を行なうルータの管理者は、この権利を他に委譲することも可能である。

### 3.5 経路選択機構

#### 3.5.1 経路選択機構の概念的な位置付け

経路選択機構の概念的な位置付けを図 3.2 に示す。

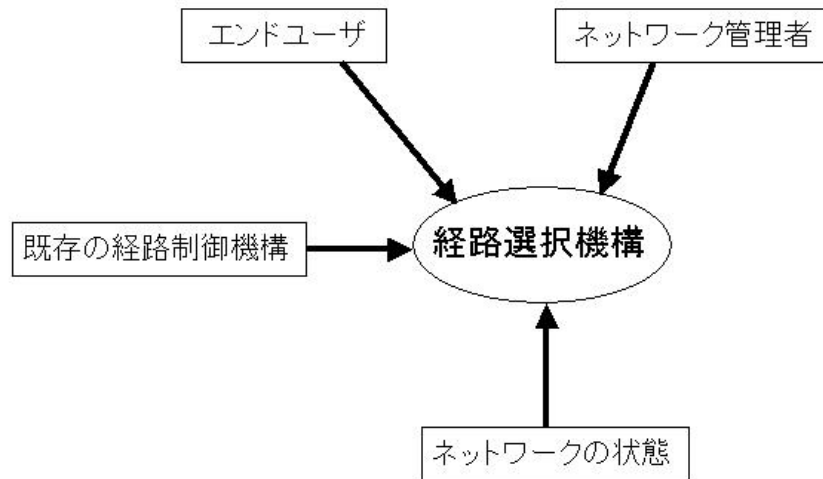


図 3.2: 経路選択機構の概念的な位置付け

エンドユーザは、本機構に対してトラフィックの経路選択を要求する。ネットワーク管理者は、本機構に対して経路選択を要求するとともに、経路選択を決定する最終的な権限を持つ。

ネットワークの状態として、回線の輻輳や回線が持つ遅延も、本機構に影響

響する。このため、本機構の中で回線の状態を監視する必要がある。

本機構は、既存の経路制御機構の上に成り立つ。ポリシーによる経路選択を行わない場合は、従来の経路制御機構によってパケット転送を行なう。

### 3.5.2 経路選択機構の全体像

経路選択機構全体の構成を、図 3.3 に示す。

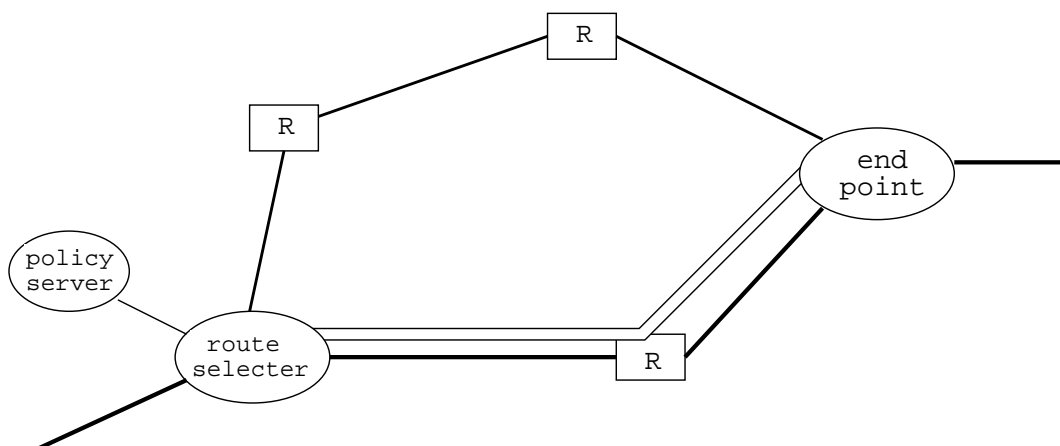


図 3.3: 経路選択機構の構成

適切な経路選択を行なうネットワーク上で、経路選択を行なうルータを route selector、route selector からのパスの宛先となるルータを end point と呼ぶ。また、エンドユーザからの要求を受け付け、route selector に経路選択のポリシーを注入するサーバを、policy server と呼ぶ。

経路選択機構は、これら 3つの機能を持つルータおよびサーバから構成される。

### 3.6 ポリシの定義

経路選択を行なうためには、経路選択の対象となるパケットを指定し、選択先の経路を明示する必要がある。この client から与えられる経路選択を行なうための条件を、本論文では「ポリシー」と定義する。本論文で扱うポリシーには、次の 5つがあり、これらの値をユーザが policy server に申請できる。

- パケットの送信元 IP アドレス
- パケットの宛先 IP アドレス

- 宛先ポート番号
- RFC1700[16] で定義されたプロトコル
- ロードバランス

RFC1700 で定義されたプロトコルとは、パケットの IP ヘッダに記述される TCP, UDP, ICMP などのプロトコルである。このプロトコルの一覧を、付録 1 で示す。

本論文では、ロードバランスを、隣接する 2 地点間のルータで複数の回線が存在する時、それぞれの回線の帯域容量に対するトラフィック量を監視し、複数の回線でトラフィック量のバランスを保ち回線状態を維持することと定義する。

アプリケーションからの要求や、ネットワークからの状態の報告について、本機構がいつでもこれらの要求を全て満たしてパケットの転送処理をできるとは限らない。よって、policy server では、経路選択を行なう際にトリガーとなるポリシーに対して、優先度の順位づけを行なう。

また本機構では、ポリシーそのものを追加することができる拡張性を持たせる。

### 3.7 既存のルータへの組み込み

経路選択機構を構築するには、route selector および end point となるルータに、それぞれの機能を組み込まなければならない。このため、経路選択を行なう route selector は当該ネットワークの管理者によってあらかじめ決定されている必要がある。また、end point は、ネットワークトポロジを把握した管理者により決定される。本機構を導入する際には、これらの事項に留意する必要がある。しかし、変更が必要なルータは route selector と end point の 2 つだけであり、2 地点の間に存在するルータなど他のルータには、機能を変更する必要がない。

### 3.8 広域性への対応

本機構は、route selector と end point の 2 つルータをネットワーク上の任意の 2 地点に導入することにより、2 地点間のネットワークの規模に関係なく、経路の選択が実現できる。route selector と end point との間は tunnel によって接続するため、中間のネットワークの規模、形態は問題とならない。

また、route selector と end point を多数設置することにより、広域のネットワークに対応したより汎用的な経路選択機構の構築が可能となる。この例を図 3.4 に示す。

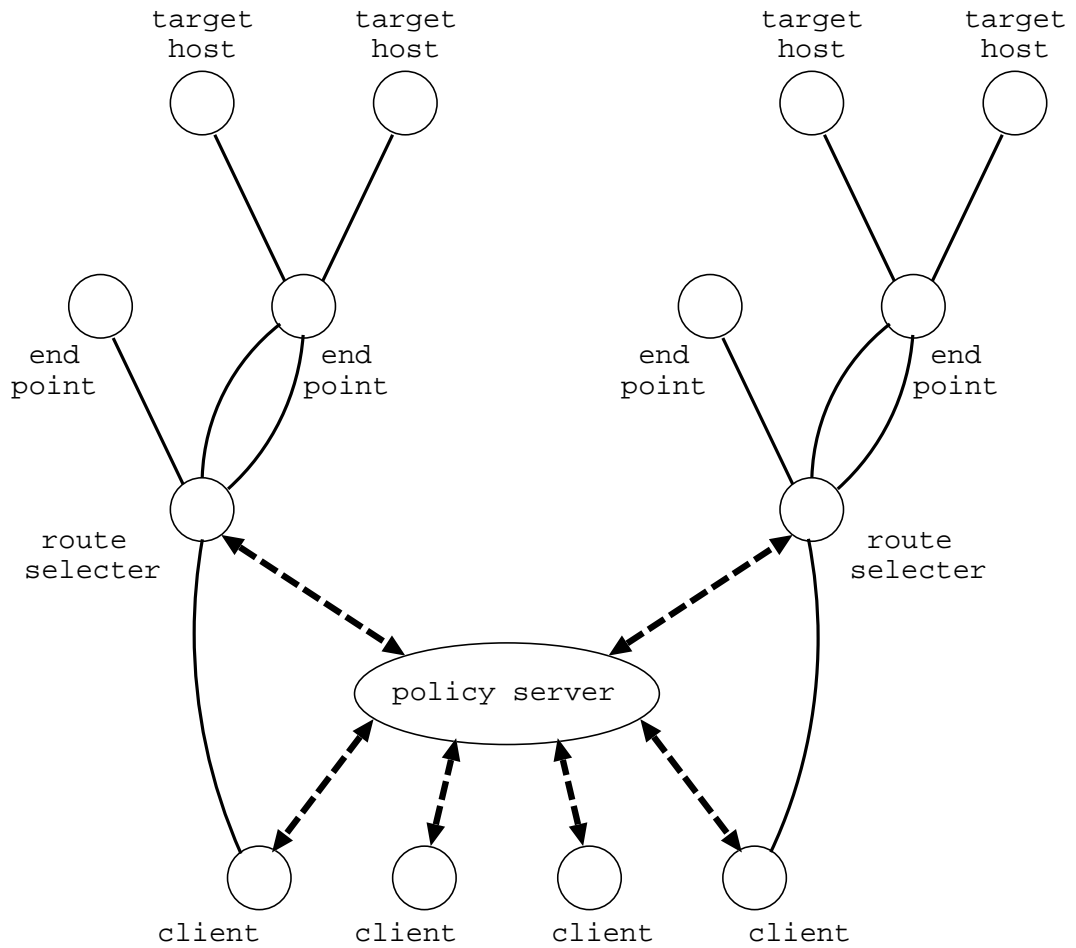


図 3.4: 多数のルータによる経路選択機構の構築

点線は policy server・各ルータ間のポリシーに関する情報交換を、実線はコネクションを表す。

本機構が数多くの client, route selector, end point で構成されるようになっても、一つあるいは少数の policy server で本機構の全てを制御できる。

ネットワーク上の全てのルータが route selector と end point の双方の機能を持てば、エンドユーザは任意の2地点間で経路を選択することが可能となる。

### 3.9 既存の Traffic Engineering との違い

MPLS や DiffServ などでは、特定のドメイン、ネットワーク内では Traffic Engineering を実現できない。例えば MPLS では、edge router に囲まれた MPLS domain 内でのみパスを張ることができる。これに対し、本機構では、インターネット上での任意の 2 地点間での適切な経路選択を実現する。

### 3.10 source routing との違い

source routing[17] とは、データの送信時に、宛先までどのルータを通過するかという経路情報を指定する経路制御の方法である。この方法は送信者がネットワークトポロジ全体を知っている必要がある。source routing には、次の 2 種類がある。

- strict source routing  
送信元で、宛先までの間にパケットが通過するルータの IP アドレスを全て正確に指定する方法。指定されたルータに到達できなければ、ICMP エラーを返す。
- loose source routing  
送信元で、宛先までの間にパケットが通過するルータの IP アドレスを 1 つ以上指定する。最初に指定されたルータまでは、任意のルータを通過することができる。

このように、source routing では、エンドユーザが宛先までの中継ノードを把握している必要があり、ホップバイホップ転送と比較して非実用的である。現に、strict source routing は RSVP を用いる場合に使用されることがある他は、現実には使用されることはほとんどない。また、source routing は元来トークンリングのために開発された機能であり、現状のインターネットの経路制御に適しているとは言えない。

### 3.11 既存の経路制御機構との関わり

経路制御機構とは、経路制御プロトコルに基づき、パケットの経路制御を行なう機構のことである。動的経路制御、静的経路制御とも、ネットワーク全体を通して、パケットが適切な経路を辿り、目的ノードへ到達させるための機構である。

経路選択機構は、経路制御機構とは異なる。経路選択の処理を行なう前に経路表を参照するものの、次ノードに向けたルータの出口となるインターフェース決定する際に、既存の経路制御機構のように経路表に依存することはない。

また、本機構は、経路選択を行なうルータである route selector と、tunnel の end point との間で完結する。

本機構と既存の経路制御機構の関係は、ルータ内で行なう処理の一つとして、既存の経路制御機構の不足した機能を本機構で補完する。

### 3.12 UDL との親和性

本研究で提案する機構は、片方向通信路 (UDL: Uni-Directional Link) を含むネットワーク上でも利用できる。UDL の代表的な例として、衛星回線が挙げられる。UDLR[18] を用いることにより、UDL も双方向通信路 (BDL: Bi-Directional Link) として使用することが可能になる。ここで、UDLR(Uni-Directional Link Routing) について述べる。

UDLR とは、広帯域の UDL を狭帯域の BDL と組み合わせることによって広帯域の BDL に見せかけるための技術である。一般的に、クライアントからサーバに対するトラフィック (上り) よりもサーバからクライアントへのトラフィック (下り) の方が圧倒的に多いことに着目する。上りに狭帯域の回線を使用し、下りに広い帯域の回線を使用することで、広帯域の UDL を有効に利用できる。

これにより、衛星回線のような広帯域で遅延の大きい片方向通信路を有効に活用することができる。

経路選択機構を導入する 2 地点間の経路として UDL と BDL の両方を用いる時、UDLR を利用することにより UDL と BDL との間で経路の選択ができる。

### 3.13 マルチキャストとの親和性

衛星回線の UDL を含むネットワークは、マルチキャストとの親和性が高い。衛星回線の受信専用局を多数設置することにより、マルチキャストの receiver は増加する。本研究ではこの点に着目し、経路選択機構がマルチキャストにも適応できるようにする。

図 3.5 に、UDL を含むネットワークでマルチキャストを使用する時のトポロジの例を示す。

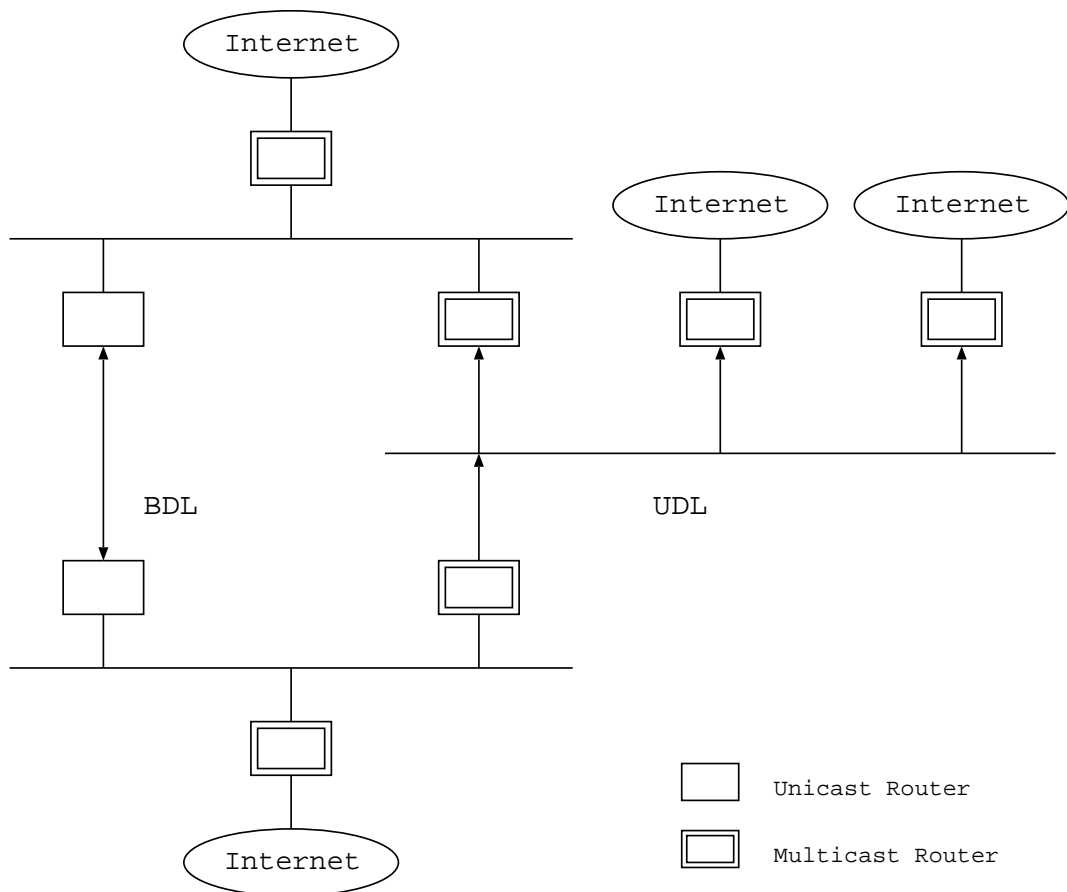


図 3.5: 本機構上でのマルチキャストの利用

図 3.5 に示すように、ユニキャストルータ、マルチキャストルータを配置する。マルチキャストのネットワークを構成する主要な要素として、衛星回線の UDL バックボーンを想定する。

衛星回線の UDL バックボーンを用いることにより、一つの送信ノードに対し、多数の受信専用ノードを接続できる。これは、他のデータリンクの通信路では実現が容易ではない、大きな特徴である。

### 3.14 本機構の利用モデル

単純に特定の 2 地点のルータの間での経路選択にとどまらず、本機構を用いた将来的な利用モデルとして、企業や大学などが地理的・ネットワークポロジ的に離れた 2 地点間を結ぶ VPN(Virtual Private Network) などでの

利用が挙げられる。ネットワークトポロジ的に離れた2地点では、間に複数の経路が存在する場合が多い。このような時に2地点間で複数のパスを持つVPNを構成している場合、トラフィック毎に適切な経路選択を行なうことにより、ネットワーク資源の有効活用を図ることが可能となる。

本機構をVPNで利用する例を、図3.6に示す。

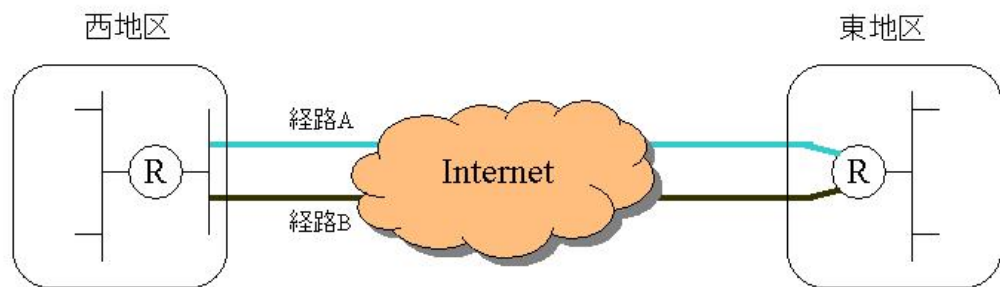


図 3.6: VPN での使用例

西地区と東地区の、距離的にもネットワークトポロジ的にも離れた2地点のネットワークをVPNで接続する。2つの地区は複数の経路で接続されている。ここでは、それぞれの地区のRが route selector, end point となる。Rには2地点を接続する複数の経路が収容される。

本機構を導入することによって、2つの経路A, Bの間での経路選択が可能となる。



## 第4章 設計

本章では、第3章で提案した経路選択機構の設計を行なう。

経路選択機構は、3つの主要なサーバおよびルータから構成される。経路選択機構全体の設計と、これら個々の設計について述べる。

### 4.1 基本設計方針

第3章で提案したモデルを、より汎用性のある機構として実現するため、以下の基本方針に基づいて設計する。

- 前提とするネットワークポロジ  
本機構は、第3.3節で述べたネットワークポロジを前提とする。設計も、このネットワークポロジを前提として行なう。
- 優先度の順位付け  
複数のポリシーを、同時にパケット転送に反映できない場合が考えられる。ポリシーに対して優先度を決定できるようにし、優先度に応じてパケット転送を行なうよう設計する。
- ネットワークに対する最小限の変更  
本機構では、route selector, end point となるルータにのみ変更を行なう。経路選択を行なう2地点間の途中のルータに対しての変更は、必要としないように設計する。
- 機構の拡張性  
将来的には、多数の route selector と end point で本機構が構築されてゆくことを想定する。

### 4.2 設計概要

#### 4.2.1 経路選択機構の全体

経路選択機構を担う大きな機能を次の3つに分割する。

- policy server

- route selector
- end point

それぞれは独立したルータおよびサーバであり、互いに協調して経路選択を実現する。

#### 4.2.2 処理の流れ

本機構全体での処理の流れを、図 4.1 に示す。

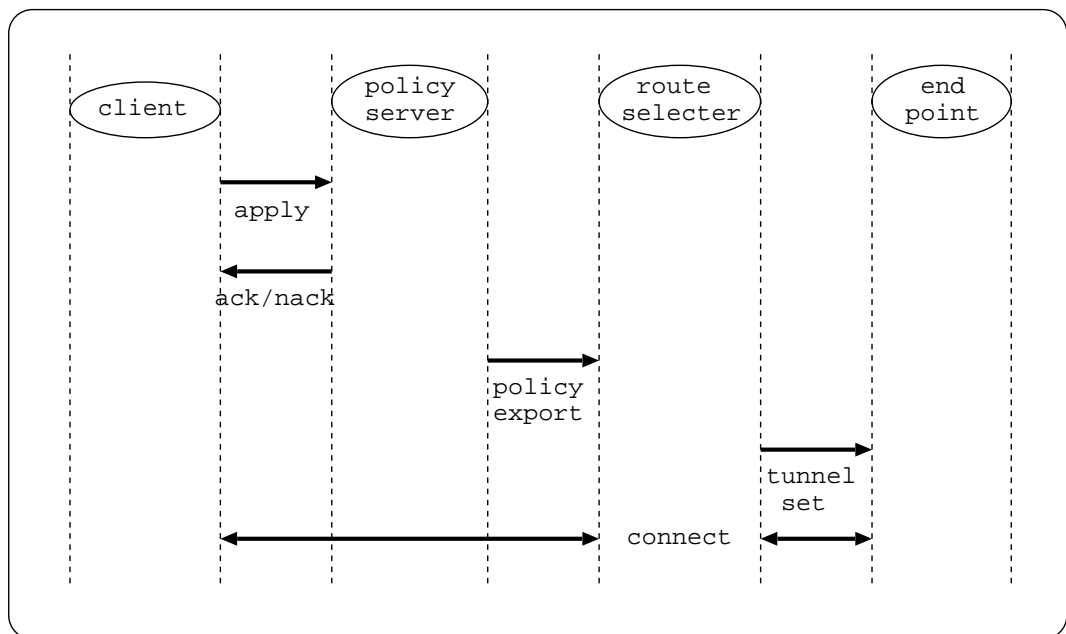


図 4.1: 本機構の処理の流れ

はじめに、client から policy server に、経路選択の対象となるパケットの条件と、経路を選択するためのポリシーを申請する。これに対し、policy server では、申請された内容が経路選択を実行するのに正しいかどうかを審査する。この審査の結果、route selector で経路選択を行なうのに問題ないと判断された場合、client に申請された内容が正しいことを返す。同時に、その内容を route selector に反映させる。申請された内容が route selector で経路選択を実行するのに適さないと判断された場合、その旨を client に返す。

policy server から経路選択のための条件およびポリシーを受け取った route selector は、end point との間に tunnel を確立させる。end point がこれを受けて、route selector との間で tunnel が確立される。

この結果、client から route selector を通り、end point までの経路が確立される。

経路選択機構全体での流れをまとめると、次のようになる。

1. client が、経路選択のポリシーを policy server に申請する
2. policy server が route selector に経路選択のポリシーを反映する
3. policy server と end point が協調して tunnel を確立させる
4. route selector で経路選択を実行する

## 4.3 policy server

### 4.3.1 policy server の役割

policy server では、client であるエンドユーザまたはネットワーク管理者が申請する、経路選択のためのポリシーと選択先の経路を、受け付ける。

経路選択の対象となるパケットの条件は、第 3.6 節で挙げたポリシーの各要素が該当する。選択先の経路には、tunnel の end point のルータを指定する。

policy server は、route selector となるルータのリストをあらかじめ保持しておく。また、end point になり得るルータのリストも保持する。

次に、policy server は、申請されたポリシーと選択先の経路が、正当なものかどうかを審査する。審査の結果が問題なければ、route selector にポリシーと選択先の経路を注入する。

### 4.3.2 ポリシーの正当性の審査

第 3.6 節で定義したポリシーについて、client から申請されたものが有効であるかどうかを次の事項について各々審査する。

#### 有効な値であるかどうか

指定された送信元 IP アドレスや宛先ポート番号などが、値として有効なものであるかどうかを審査する。無効な値が存在した場合、申請された条件が無効であることを client に返す。

#### 正当な client であるかどうか

経路選択の対象としたパケットの、送信元 IP アドレスまたは宛先 IP アドレスのいずれかは、申請した client 自身あるいは client が存在するネットワー

クのネットワークアドレスでなければならない。これは、他のネットワークの client になりすまして通信を阻害したりすることを防ぐためである。

### 4.3.3 選択先経路の正当性の審査

ここでは、選択された経路について、次の2つの事項を審査する。

#### 正当な end point であるかどうか

選択先の経路、すなわち end point が、policy server で保持しているリストにあるかどうかを審査する。リストに存在しない場合、client に経路選択が無効であることを返す。

#### 選択された経路に到達性があるかどうか

選択された経路が route selector より先で到達性を失っていた場合も、経路選択が無効であることを client に返す。

## 4.4 route selector

### 4.4.1 route selector の役割

route selector は、policy server からポリシーと選択先経路を受け入れる。その選択先経路に従い、end point との間に tunnel を確立する。経路選択の対象となるパケットは、tunnel を通じて end point に転送する。

route selector が選択する経路は、end point までの経路として次の2つがある。

- route selector の経路表が持つ経路
- end point との間に確立した tunnel

policy server から注入されたポリシーに従い経路選択を行なう場合、経路制御プロトコルによって生成された経路表に則らずにパケット転送を行なう。

route selector では経路表を検索した後に、経路選択の処理に移行する。

### 4.4.2 回線の状態の検知

選択された経路への回線が使用不能になっていた場合、パケットの転送経路として使用することができない。この時、選択された経路に向かうパケット

は、宛先に到達不能となる。このことを防ぐため、route selector では tunnel のインターフェースを監視し、回線が使用不能に陥った場合には、その旨を policy server に伝達する。

## 4.5 end point

### 4.5.1 end point の役割

宛先ノードへの適切な経路がなければ、その宛先ノードに対する end point になることはできない。このため、end point となるルータには、経路選択の対象となるパケットの宛先ノードへの適切な経路が経路表に存在している必要がある。適切な経路とは、client のノード、route selector、end point、宛先ノードの間でルーティングループを起こさずに、client から宛先ノードに到達できる経路のことを指す。

また、route selector からの要求により、route selector との間に tunnel を確立させる。

## 4.6 条件が衝突する際の制御

複数の client からそれぞれポリシーが申請された時、ポリシーの条件が衝突する可能性がある。ポリシーの条件が衝突する例を挙げ、これに対する解決方法を述べる。

### 4.6.1 衝突が生じる例 1

条件の衝突が生じる例を、図 4.2 を基にして述べる。

client A は、表 4.1 の条件を満たすフローに対して、route 2 を通るように policy server に申請する。

表 4.1: ポリシが衝突する条件の例 1

送信元 IP アドレス	target host
宛先 IP アドレス	client A,B が属するネットワークアドレス
宛先 port 番号	N

この後、client B から、表 4.1 と同じ条件を満たすフローに対して route 1 を通るような申請が行なわれた場合、先に client A が申請した条件と衝突

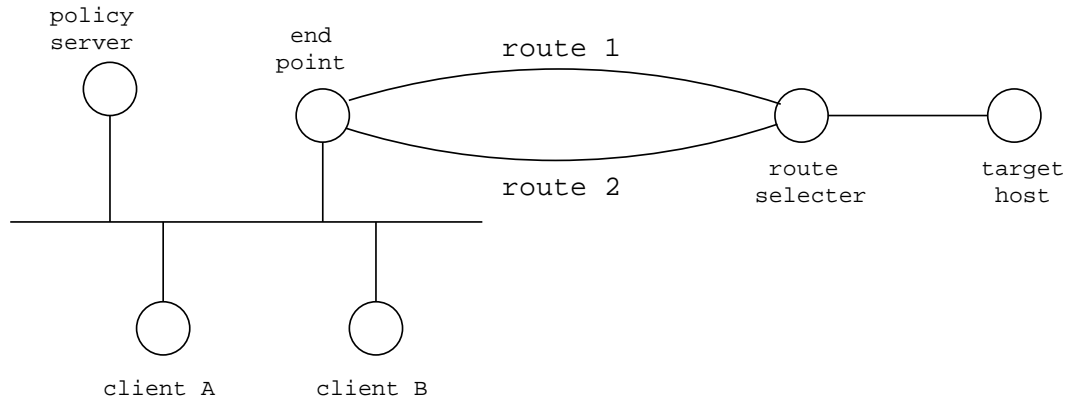


図 4.2: ポリシが衝突する例 1

する。

#### 4.6.2 衝突が生じる例 2

条件の衝突が生じるもう一つの例を、図 4.3 を基にして述べる。

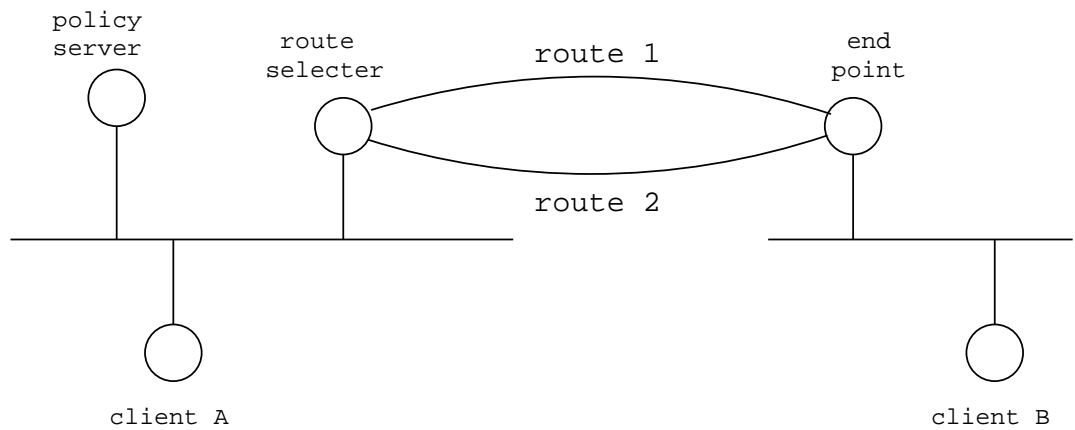


図 4.3: ポリシが衝突する例 2

client A は、表 4.2 の条件を満たすフローに対して、route 2 を通るように policy server に申請する。この後、client B から、表 4.3 の条件を満たすフローに対して route 1 を通るような申請がされた場合、client A が申請したポリシーの条件と衝突する。

表 4.2: ポリシが衝突する条件の例 2-1

送信元 IP アドレス	client A
宛先 IP アドレス	client B
送信元 port 番号	N

表 4.3: ポリシが衝突する条件の例 2-2

送信元 IP アドレス	client B
宛先 IP アドレス	client A
宛先 port 番号	N

#### 4.6.3 衝突を回避する手法

衝突するポリシの条件が、複数のエンドユーザから申請された場合、先に policy server に申請したエンドユーザの条件を優先させる。後から申請した者に対しては、policy server に申請された時点で、申請が無効であることを client に返す。

衝突するポリシの条件が管理者とエンドユーザからそれぞれ申請された場合、管理者のポリシが優先される。この時、エンドユーザのポリシに従って特定のフローに対して経路選択が行なわれている場合、このエンドユーザのポリシによる経路選択は強制的に終了する。

ポリシの条件が衝突した場合に優先される処理を、表 4.4 にまとめる。

表 4.4: 条件が衝突した場合に優先される client

client 1	client 2	優先される client
ネットワーク管理者	エンドユーザ	ネットワーク管理者
エンドユーザ	エンドユーザ	先にポリシを申請した client

## 4.7 ルーティンググループの回避

end point を決定する際には、各リンクのコストを考慮しなければならない。このことを考えるトポロジの例を、図 4.4 に示す。A から J はルータを表す。数字は、各リンクのコストである。この図 4.4 において、B を route selector とする。送信元ノードを A、宛先ノードを J とするパケットを考える。

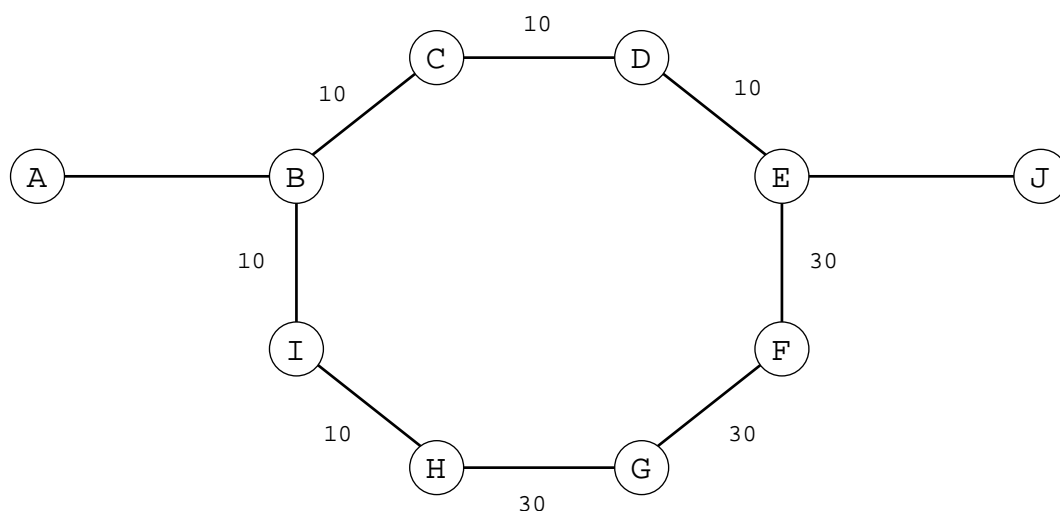


図 4.4: 各リンクのコストを考慮したネットワークトポロジ

B の経路表では、宛先 J に対する next hop は C である。B から、I-H-G-F-E を経由して J にパケットを到達させたいユーザがいる場合、route selector B で適切な経路選択を行なう必要がある。

この時、end point を H として、B と H の間に tunnel を張ることを考える。しかし、H から E への各リンクのコストの合計は、H-I-B-C-D-E と通る場合は合計 50、H-G-F-E と通る場合は合計 90 となる。よって、H が持つ経路表の E および J への next hop は I となる。この結果、H-G-F-E という経路は使用されることがなくなり、B-I-H 間で余計なトラフィックが発生し、route selector B で経路選択を行なった意味がなくなる。

B で経路選択を適用されたパケットが、B-I-H-G-F-E という経路を辿るためには、end point を G に設定するべきである。G-F-E ではコストの合計が 60、G-H-I-B-C-D-E ではコストの合計が 80 となり、policy server にポリシーを申請した、ユーザまたはネットワーク管理者の要求通りの経路を辿ることができる。



## 4.8 経路選択の機能を必要としない場合

経路選択機構による経路選択を必要としない時、本機構によって他の経路制御プロトコルの動作に影響を与えてはならない。本機構では、ポリシーによる経路選択を必要としない時、パケットに対して一切の処理を行なわない。

route selector でのパケット処理の流れとしては、経路表を検索した後に経路選択のための処理に移る。このため、route selector で経路選択の処理が何も行なわれなかった場合、経路表の検索結果がパケット転送に反映される。

## 4.9 予想される問題点

本機構では、route selector と end point の接続に tunnel を利用する。tunnel ではパケットをカプセル化するため、必然的にトラフィックが増大するという問題点が挙げられる。

## 第5章 実装

本章では、第4章で行なった設計に基づき、経路選択機構の実装を行なう。policy server, route selector, end point の各実装と、それぞれの接続部分の実装について述べる。

### 5.1 policy server の実装

policy server の内部を、図5.1のようにモジュールに分割した。

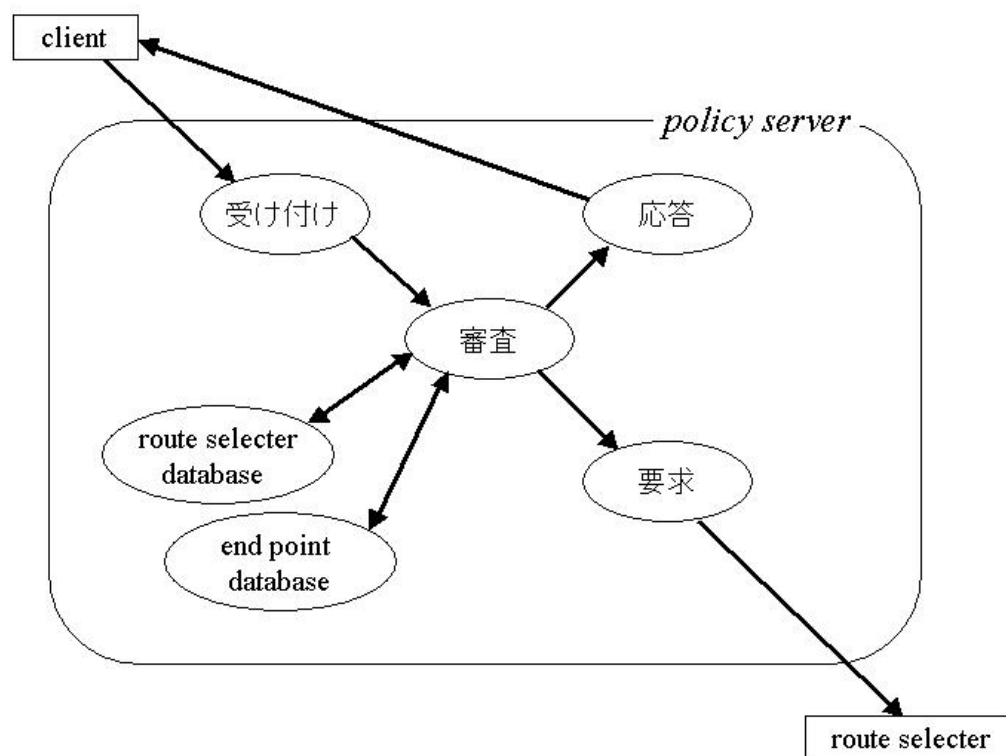


図 5.1: policy server

受け付けモジュールが client からの要求を受け付ける。その後、審査を行なうモジュールが、ポリシーと選択先経路の審査を行なう。この際、route selector と end point のデータベースを呼び出す。policy server は、内部で route selector となるルータと end point となるルータの IP アドレスをそれぞれデータベースで保持している。審査の結果問題なければ、route selector に client からの申請を注入する。問題があれば、client に返す。

## 5.2 route selector の実装

### 5.2.1 経路選択の処理の実装

カーネル内の、パケット転送の際に経路を決定するプログラムである、ip\_output.c に変更を加えることにより実装した。関連するヘッダファイルも変更した。OS は、FreeBSD 4.2-Release を対象にした。

ポリシーの変更は、カーネルに対して直接行なう。また、ネットワーク管理者は、sysctl を用いてポリシーの操作ができる。sysctl コマンドで見た、route selector の設定例を図 5.2.1 に示す。

```
route-selector# sysctl -a | grep orochi
root@route-selector.ai3.net:/usr/src/sys/compile/orochi
kern.hostname: route-selector.ai3.net
net.orochoi.tcp_port: 80
net.orochoi.udp_port: 0
net.orochoi.src_addr: 192.168.1.1
net.orochoi.dst_addr: 0.0.0.0
net.orochoi.ipproto: 6
net.orochoi.next_addr: 192.168.10.2
net.orochoi.if_name: fxp1
```

図 5.2: sysctl で見たポリシーの設定例

各要素の、デフォルト値は 0 である。ポリシーの条件が指定されていない場合、デフォルト値が入る。

### 5.2.2 パケット転送の処理の流れ

route selector 内部における、パケット転送の処理の流れについて説明する。

ネットワークインターフェースが、データリンク層からパケットを受信すると、キューイングを行なう。この後、受信したパケットが自ルータ宛のものか、他へ転送するべきものかを判断し、自ルータ宛ならトランスポート層

へ送る。転送するパケットであるなら、ポリシーによる経路選択の対象になっているかどうかを検索する。

経路表を検索し、経路選択のための処理が行われた後、送信のための処理として、パケットの終点アドレスを抽出して経路表を検索し、送信する tunnel のインターフェースを決定する。最後に、ネットワークインターフェースからデータリンク層にパケットを送る。

### 5.3 end point の実装

route selector と end point を繋ぐ tunnel には、既存の tunnel の実装を用いた。Trumpet 社が提案している DTCP(Dynamic Tunnel Configuration Protocol) は、TCP を用いて、tunnel のクライアント側からの接続要求によって、tunnel の受け側がクライアントに対して動的に tunnel を設定する。本機構の場合、route selector がクライアントであり、end point がサーバとなる。

end point では、tunnel の受け側となる DTCP サーバを組み込んだ。

## 第6章 評価

本論文で提案し、設計・実装した経路選択機構が有用である事を証明するため、評価を行なう。

### 6.1 評価手法

本研究で提案し、設計および実装を行なった経路選択機構を、次の2つの手法で評価する。

- 単一のルータによる経路選択との性能比較
- 本機構を実際のネットワークに導入し、性能を検証

はじめに、本機構と経路選択の機能を持つ単一のルータとを比較する。単一のルータでは実現できなかったことを、本機構によって実現したことを示す。次に、本機構を実際のネットワークに組み込み、本論文で設計および実装した機能が動作することを検証する。そして、広域ネットワークにおける経路選択機構の有効性を評価する。

### 6.2 単一ルータによる経路選択との比較

複数のルータで協調する統合的な経路選択機構と、単一で動作する経路選択ルータとを比較する。本機構の比較対象として、単一で動作する経路選択ルータを実装した。また、ベンダールータの中で経路選択やロードバランスの機能を持つ cisco 社のルータを取り上げる。

#### 6.2.1 システムの概要

単一のルータで動作する経路選択機構は、ある目的ノードに対し、複数の経路を持つルータが、特定のポリシーに基づきパケットを送出するインターフェースを選択し、送信する。この場合の経路選択は、一台のルータと、そのルータとの間に2つ以上の経路を持つノードが存在すれば、可能である。

図 6.1 において、ホスト H1 から ホスト H2 に向かってパケットを送信する時を考える。

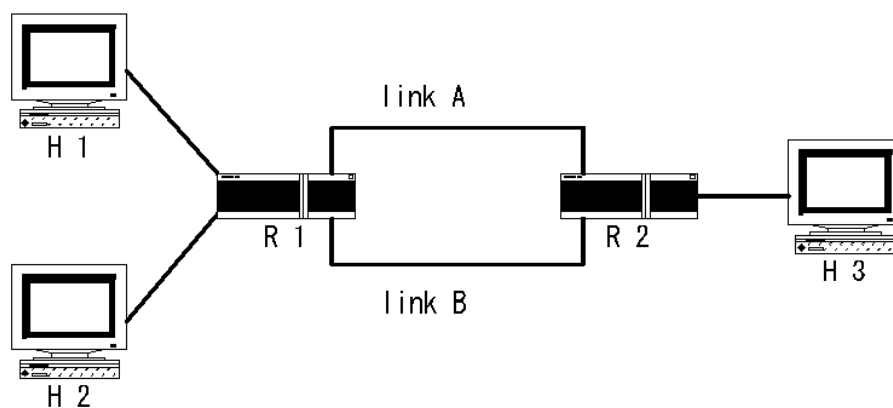


図 6.1: 単一のルータで経路選択を行なう場合のネットワークポロジ

経路途中のルータ R1 と R2 の間には、link A と link B の 2 つの経路が存在する。R1 では、経路上の次ノードとなる R2 へパケットを転送する。この時 R1 は、route A と route B のいずれか一方の経路を選択する。

R1 では、与えられたポリシーに基づき経路の選択を行なう。

### 6.2.2 設計・実装

この機構は、パケットの経路選択の仕組み全体を制御する制御部と、実際に経路選択を行なう振分部から構成される。制御部と振分部について、それぞれ概説する。

#### 制御部

各振分部を統括し、パケット転送の優先度づけを行なう。経路選択の対象となるパケットを受信した時、振分部を呼び出す。制御部が行なう処理を、実行する順に挙げる。

1. ユーザが記述したパケット転送を行なう条件の読み込み
2. ポリシの設定
3. 回線の状態を検知するモジュールを呼び出し
4. 要求に沿ったモジュールを呼び出し
5. モジュールから送信先インターフェイスの情報を取得

6. 優先度の順位づけ
7. 送信のための処理へ移行

#### 振分部

実際に経路選択を行なうための処理は、各振分部のモジュールが行なう。パケットに対する処理を行なうために基にする情報の特性の違いにより、モジュールは3つのタイプに分かれる。各モジュールの種類と処理を、以下に挙げる。

#### タイプA ユーザからの要求

- パケットの始点アドレス
- アプリケーション
- トランスポート層プロトコル

#### タイプB 回線の状態

- 回線の状態

#### タイプC ユーザからの要求、回線の状態の両方

- ロードバランス

経路選択にあたって、これらのポリシーは、複数組み合わせで指定することもできる。

### 6.3 単一ルータの経路選択による限界

単一のルータで経路選択を行なう場合、隣接する2地点間、あるいはそれに準ずるネットワークトポロジで複数経路が存在する場合しか実現できない。広域なネットワークでの任意の2地点間に存在する複数の経路を使い分けることは、現状では不可能である。

### 6.4 単一ルータによる経路選択との比較

経路選択機構と、単一ルータによる経路選択の機能および性能を比較する。経路選択が適用できる範囲の比較を、表 6.1 に示す。

表 6.1: 経路を選択する機構の性能評価

	同一 link	domain	どこでも
cisco	○	-	×
6.2.2 で行なった実装	○	×	×
MPLS	○	○	×
本機構	○	-	○

本機構では、経路選択のためのドメインを定義していないため、適用可能な範囲としての評価対象にはしていない。この結果、本機構が最も広範囲での経路選択が可能であることが分かった。

## 6.5 実ネットワークでの評価

次に、本研究で提案した機構が、実際のインターネットの上で有効であることを検証する。

実際に2地点間で性質の異なる複数の回線を持つ広域なネットワークとして、AI3 Network(Asia Internet Interconnection Initiatives) [19] 上に、本研究で実装した機構を組み込み、評価を行なった。

### 6.5.1 AI3 Network の概要

AI3 Network は、奈良と藤沢に衛星回線のハブ局を持ち、東南アジアの6ヶ国と接続している(2002年1月現在)。AI3 Network の概念的なトポロジを、図6.2に示す。

日本のハブ局からインターネットに接続し、各対地国は各々が下部組織を持つ。AI3 は一つのASであり、transit AS としての役割も果たす。

### 6.5.2 衛星ネットワークの特性

衛星回線は、一般の地上回線とは異なる性質を持つ。衛星回線が持つ優位性として、次のものを挙げる。

- 地理不偏性
- 広域同報性
- 耐災害性



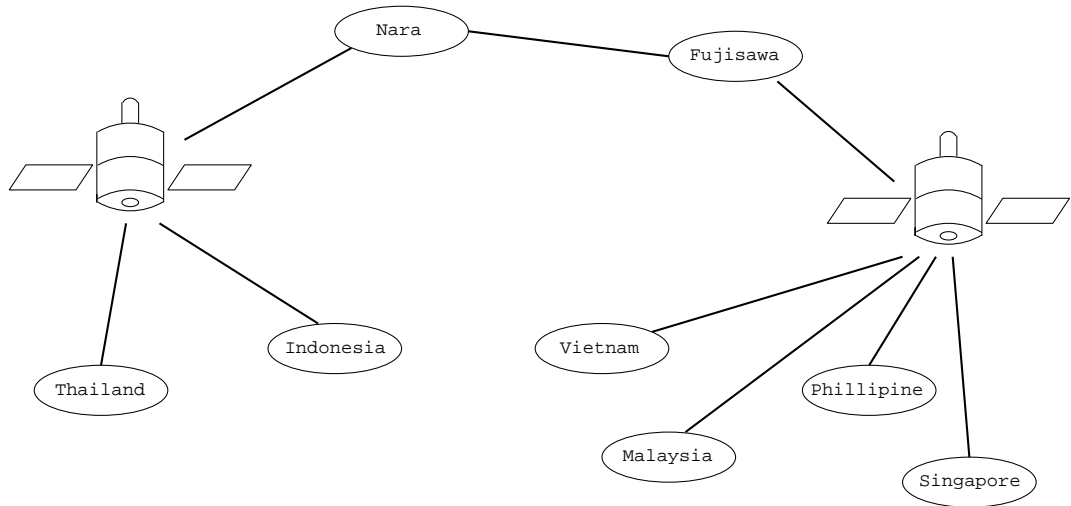


図 6.2: AI3 Network の概念的トポロジ

また、一方で、以下のような欠点がある。

- 片方向の通信で 250ms の伝送遅延が発生
- 降雨減衰による通信の遮断

衛星回線は、基本的に片方向通信路であるという大きな特徴がある。双方向での通信も、UDL の組み合わせによって実現される。これは、非対称なネットワークが容易に構築できることを意味する。

インフラストラクチャとしてのネットワークが整備されていない場所では、受信専用局を設置した方が地上回線を敷設するよりもコストが低い。UDLR を用いることで双方向の通信も可能となるため、インターネットの普及が遅れている地域での利用が見込まれる。

### 6.5.3 評価環境の構築

本研究の評価を行なうため、AI3 Network の再構築を行なった。評価に関わる部分のネットワークトポロジを、図 6.3 に示す。AI3 Network に、route selector, end point となるルータを新たに導入した。また、UDL のネットワークを追加した。元来の AI3 Network のトポロジ図と、本研究のために変更を行なった後の AI3 Network のトポロジ図を、付録 2 に載せる。

図 6.3 で、実線は地上回線、点線は衛星回線を、矢印は UDL であることを示す。R8 は、UDL の feeder(送信専用局)に接続されたルータ、R9 は receiver(受

信専用局)に接続されたルータである。R9 の他にも receiver は数多く存在し、AI3 Network に繋がっている。

衛星回線を用いた UDL では、一つの feeder に対して receiver を多数設置することが可能であり、同報型の回線として利用するのに適している。また、図 6.3 に示すように、BDL の衛星ルータと UDL の受信側の衛星ルータは同一のセグメントに存在することになる。

#### 6.5.4 経路選択の実験

図 6.3 において、R2 が新たに導入したルータであり、route selector の役割を果たす。また、R10 が宛先ノードとなる。R3-R4 は BDL の衛星回線、R8-R9 は R8 から R9 への UDL の衛星回線である。このトポロジで、R2 から R10 への経路は、R2-R3-R4-R10 を辿る経路と、R2-R5-R6-R7-R8-R9-R10 と辿る経路の 2 つが存在する。各ルータの経路表に基づくと、R2 から R10 への経路は R2-R3-R4-R10 となる。ここで、client が R2 から UDL を通り R10 へトラフィックを流したいとする。各ルータの経路表を見ると、R5 からは BDL を通り R10 に到達するが、R6 からは UDL を通り R10 に到達する。よって、R6 を end point に設定する。

この結果、R2 を route selector、R6 を end point として経路選択機構が構築された。R2 で、ポリシーによる適切な経路選択が実現できた。

## 6.6 評価のまとめ

単一で経路の選択を行なうルータとの比較により、本研究の経路選択機構の方が広域での経路選択を行なえることを示した。

また、実ネットワークに本機構を構築することで、実用性に関する評価を行なった。この結果、広域ネットワークで本機構が十分に実用に耐え得ることが証明された。

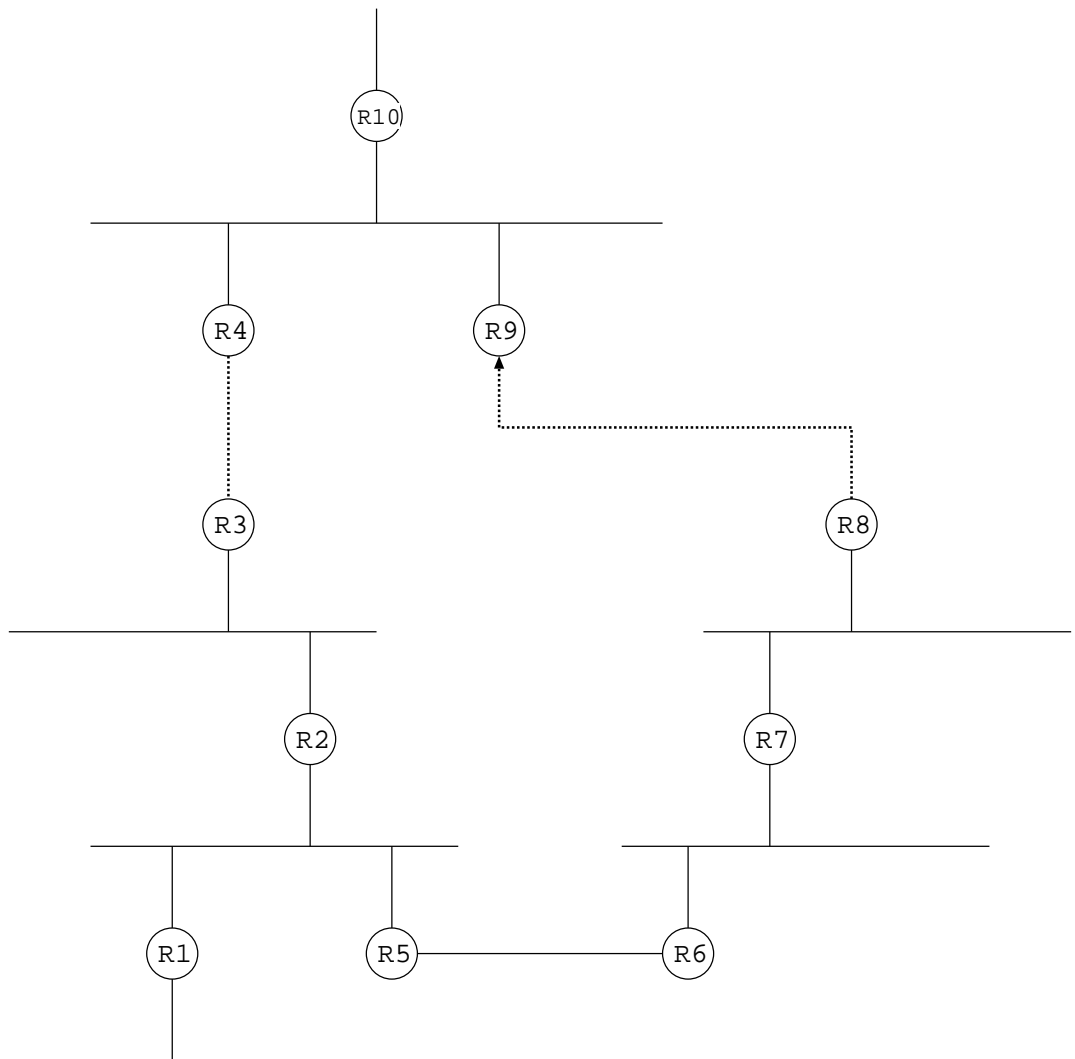


図 6.3: 評価に関する AI3 Network のトポロジ図

## 第7章 結論

本章では、本論文で述べてきた事項をまとめ、本研究の結論と今後の課題について述べる。

### 7.1 まとめ

本研究では、インターネットを構成する多数の回線を有効活用し、また、ネットワーク管理者やエンドユーザからのネットワークに対する要求を満足させることを目的とした。この目的を実現するため、経路選択機構を提案し設計した。経路選択機構では、policy server, route selector, end point の3つの機能を導入し、自由度の高い統合的な経路選択機構を実装した。これにより、ネットワーク管理者やエンドユーザが、様々なポリシーでパケットの転送経路を選択し設定することができるようになった。

route selector と end point の間に入るルータには実装の変更を加えることなく、従来の経路制御プロトコルに基づいた経路制御機構のままで、任意の2地点間の経路選択を実現した。

評価対象として、単一のルータで動作する経路選択ルータを実装した。経路選択機構の性能を、このルータと、ベンダールータで経路選択の機能を持つ cisco のルータとの間で比較した。

また、本研究で実装した経路選択機構を、ネットワーク内に Uni-Directional Link を含み、マルチキャスト通信にも適した AI3 Network の上に構築し、評価を行なった。

この結果、本研究で提案した経路選択機構は、単一で動作する経路選択ルータよりも柔軟性があり、拡張性があることが示された。また、実際のネットワーク上での評価により、広域ネットワークにも適応した、自由度を持った経路選択を実現した。

本研究により、広域ネットワークでの2地点間で、トラフィック特性を考慮した経路選択が実現できた。

## 7.2 今後の課題

本研究では、route selector と end point の接続の確立に tunnel を使用した。tunnel ではパケットのカプセル化を行なうため、必然的にトラフィックの流量が増加する。このため、数多くのルータに route selector および end point の機能を搭載し、経路選択がインターネット上のあらゆる2地点で実現できるようになった時、既存の経路制御機構に比べてネットワーク全体のパフォーマンスが低下することが考えられる。

tunnel を使用することがネットワーク全体の性能にどの程度影響を与えるのかを正確に予測することが必要となる。このためのシミュレーションを行ない、検証する。

また、client は適切な end point の位置をあらかじめ知っていなければならない。現状では、利用するネットワークのトポロジをある程度知っている者でないと、client にはなれない。あらゆるエンドユーザが利用できるように、改善の必要がある。

最後に、本機構が拡張されていった時、どの程度の数の client, route selector, end point に対して一台の policy server を設置すべきか、追求しなければならない。

## 謝辞

本研究を行なう機会を与えて下さり、御指導を頂きました慶應義塾大学環境情報学部教授の村井純博士に感謝致します。また、絶えず御助言と御指導を頂きました同学部の楠本博之博士と中村修博士、奈良先端科学技術大学院大学の山口英博士に深い感謝の意を表します。

本研究を進めるにあたり、貴重な御意見を頂きました JSAT 株式会社の泉山英孝氏、慶應義塾大学政策メディア研究科の西田視磨氏、小原泰弘氏、同大学環境情報学部の小柴晋氏、渡里雅史氏をはじめとする多くの研究室の皆様感謝します。また、本研究のネットワーク実験のため、強引な要求を飲んで無茶なオペレーションにつき合っていたいただいた AI3 Project のメンバーに、心より感謝します。

## 参考文献

- [1] G.Malkin. RIP Version 2. RFC 2453, IETF, November 1998.
- [2] J.Moy. OSPF Version 2. RFC 2328, IETF, April 1998.
- [3] R.Callon. Use of OSI IS-IS for Routing in TCP/IP and Dual Environments. RFC 1195, IETF, December 1990.
- [4] D.Awduche, J.Malcolm, J.Agobua, M.O'Dell, J.McManus. Requirements for Traffic Engineering Over MPLS. RFC2702, IETF, September 1999.
- [5] R.Braden, L.Zhang. Resource ReSerVation Protocol(RSVP). RFC 2209, IETF, September 1997.
- [6] E.Rosen, Y.Rekhter. BGP/MPLS VPNs. RFC 2547, IETF, March 1999.
- [7] 宇多仁. ラベルスイッチング技術を用いたネットワークにおけるファイヤウォールの実現. 修士論文, 北陸先端科学技術大学院大学, 1999.
- [8] <http://www.cisco.com/>
- [9] Bassam Halabi. Internet Routing Architectures. プレンティスホール出版, April 1998
- [10] C.Huitema, 前村昌紀. インターネットルーティング翔泳社, March 2001
- [11] R.Stewart, Q.Xie, K.Morneault, C.Sharp, H.Schwarzbauer, T.Taylor, I.Rytina, M.kalla, L.Zhang and V.Paxson. Stream Control Transmission Protocol RFC 2960, IETF, October 2000.
- [12] A.Jungmaier, E.P.Rathgeb, M.Schopp and M.Tuxen. SCTP - A Multi-link End-to-end Protocol for IP-based Networks.
- [13] M.Steenstrup. IDRP as a Proposed Standard. RFC1477, IETF. July 1993.

- [14] M.Steenstrup. An Architecture for Inter-Domain Policy Routing. RFC 1478, IETF, June 1993.
- [15] M.Steenstrup. Inter-Domain Policy Routing Protocol Specification: version 1. RFC1479, IETF, July 1993.
- [16] J.Reynolds, J.Postel ASSIGNED NUMBERS. RFC1700, IETF, October 1994.
- [17] D.Estrin, T.Li, Y.Rekhter, K.Varadhan and D.Zappala. Source Demand Routing. RFC1940, IETF, May 1996.
- [18] E.Duros, W.Dabbous, H.Izumiyama, N.Fujii and Y.Zhang. A Link-Layer Tunneling Mechanism for Unidirectional Links. RFC 3077, IETF, March 2001.
- [19] <http://www.ai3.net/>



# 付録 1

## RFC1700 で定義されているプロトコル一覧

### Assigned Internet Protocol Numbers

Decimal	Keyword	Protocol	References
-----	-----	-----	-----
0		Reserved	[JBP]
1	ICMP	Internet Control Message	[RFC792, JBP]
2	IGMP	Internet Group Management	[RFC1112, JBP]
3	GGP	Gateway-to-Gateway	[RFC823, MB]
4	IP	IP in IP (encapsulation)	[JBP]
5	ST	Stream	[RFC1190, IEN119, JWF]
6	TCP	Transmission Control	[RFC793, JBP]
7	UCL	UCL	[PK]
8	EGP	Exterior Gateway Protocol	[RFC888, DLM1]
9	IGP	any private interior gateway	[JBP]
10	BBN-RCC-MON	BBN RCC Monitoring	[SGC]
11	NVP-II	Network Voice Protocol	[RFC741, SC3]
12	PUP	PUP	[PUP, XEROX]
13	ARGUS	ARGUS	[RWS4]
14	EMCON	EMCON	[BN7]
15	XNET	Cross Net Debugger	[IEN158, JFH2]
16	CHAOS	Chaos	[NC3]
17	UDP	User Datagram	[RFC768, JBP]
18	MUX	Multiplexing	[IEN90, JBP]
19	DCN-MEAS	DCN Measurement Subsystems	[DLM1]
20	HMP	Host Monitoring	[RFC869, RH6]
21	PRM	Packet Radio Measurement	[ZSU]
22	XNS-IDP	XEROX NS IDP	[ETHERNET, XEROX]
23	TRUNK-1	Trunk-1	[BWB6]
24	TRUNK-2	Trunk-2	[BWB6]

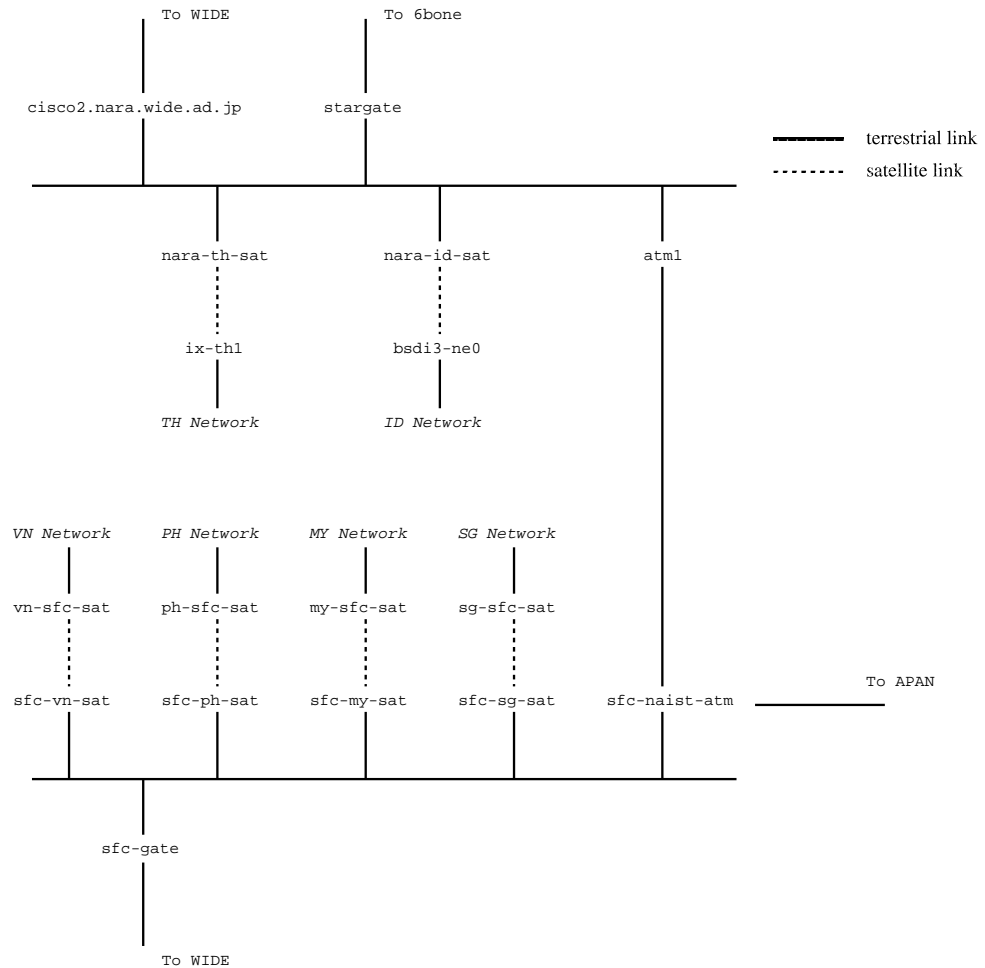
25	LEAF-1	Leaf-1	[BWB6]
26	LEAF-2	Leaf-2	[BWB6]
27	RDP	Reliable Data Protocol	[RFC908,RH6]
28	IRTP	Internet Reliable Transaction	[RFC938,TXM]
29	ISO-TP4	ISO Transport Protocol Class 4	[RFC905,RC77]
30	NETBLT	Bulk Data Transfer Protocol	[RFC969,DDC1]
31	MFE-NSP	MFE Network Services Protocol	[MFENET,BCH2]
32	MERIT-INP	MERIT Internodal Protocol	[HWB]
33	SEP	Sequential Exchange Protocol	[JC120]
34	3PC	Third Party Connect Protocol	[SAF3]
35	IDPR	Inter-Domain Policy Routing Protocol	[MXS1]
36	XTP	XTP	[GXC]
37	DDP	Datagram Delivery Protocol	[WXC]
38	IDPR-CMTP	IDPR Control Message Transport Proto	[MXS1]
39	TP++	TP++ Transport Protocol	[DXF]
40	IL	IL Transport Protocol	[DXP2]
41	SIP	Simple Internet Protocol	[SXD]
42	SDRP	Source Demand Routing Protocol	[DXE1]
43	SIP-SR	SIP Source Route	[SXD]
44	SIP-FRAG	SIP Fragment	[SXD]
45	IDRP	Inter-Domain Routing Protocol	[Sue Hares]
46	RSVP	Reservation Protocol	[Bob Braden]
47	GRE	General Routing Encapsulation	[Tony Li]
48	MHRP	Mobile Host Routing Protocol	[David Johnson]
49	BNA	BNA	[Gary Salamon]
50	SIPP-ESP	SIPP Encap Security Payload	[Steve Deering]
51	SIPP-AH	SIPP Authentication Header	[Steve Deering]
52	I-NLSP	Integrated Net Layer Security TUBA	[GLENN]
53	SWIPE	IP with Encryption	[JI6]
54	NHRP	NBMA Next Hop Resolution Protocol	
55-60		Unassigned	[JBP]
61		any host internal protocol	[JBP]
62	CFTP	CFTP	[CFTP,HCF2]
63		any local network	[JBP]
64	SAT-EXPAK	SATNET and Backroom EXPAK	[SHB]
65	KRYPTOLAN	Kryptolan	[PXL1]
66	RVD	MIT Remote Virtual Disk Protocol	[MBG]
67	IPPC	Internet Pluribus Packet Core	[SHB]
68		any distributed file system	[JBP]

69	SAT-MON	SATNET Monitoring	[SHB]
70	VISA	VISA Protocol	[GXT1]
71	IPCV	Internet Packet Core Utility	[SHB]
72	CPNX	Computer Protocol Network Executive	[DXM2]
73	CPHB	Computer Protocol Heart Beat	[DXM2]
74	WSN	Wang Span Network	[VXD]
75	PVP	Packet Video Protocol	[SC3]
76	BR-SAT-MON	Backroom SATNET Monitoring	[SHB]
77	SUN-ND	SUN ND PROTOCOL-Temporary	[WM3]
78	WB-MON	WIDEBAND Monitoring	[SHB]
79	WB-EXPAK	WIDEBAND EXPAK	[SHB]
80	ISO-IP	ISO Internet Protocol	[MTR]
81	VMTP	VMTP	[DRC3]
82	SECURE-VMTP	SECURE-VMTP	[DRC3]
83	VINES	VINES	[BXH]
84	TTP	TTP	[JXS]
85	NSFNET-IGP	NSFNET-IGP	[HWE]
86	DGP	Dissimilar Gateway Protocol	[DGP,ML109]
87	TCF	TCF	[GAL5]
88	IGRP	IGRP	[CISCO,GXS]
89	OSPFIGP	OSPFIGP	[RFC1583,JTM4]
90	Sprite-RPC	Sprite RPC Protocol	[SPRITE,BXW]
91	LARP	Locus Address Resolution Protocol	[BXH]
92	MTP	Multicast Transport Protocol	[SXA]
93	AX.25	AX.25 Frames	[BK29]
94	IPIP	IP-within-IP Encapsulation Protocol	[JI6]
95	MICP	Mobile Internetworking Control Pro.	[JI6]
96	SCC-SP	Semaphore Communications Sec. Pro.	[HXH]
97	ETHERIP	Ethernet-within-IP Encapsulation	[RXH1]
98	ENCAP	Encapsulation Header	[RFC1241,RXB3]
99		any private encryption scheme	[JBP]
100	GMTP	GMTP	[RXB5]
101-254		Unassigned	[JBP]
255		Reserved	[JBP]

## 付録 2

### 変更前の AI3 Network トポロジ図

AI3 Network Topology Map (2001.10.29, routers only)



## 変更後の AI3 Network トポロジ図

AI3 Network New Topology Map (Proposed, 2001.10.29, routers only)

