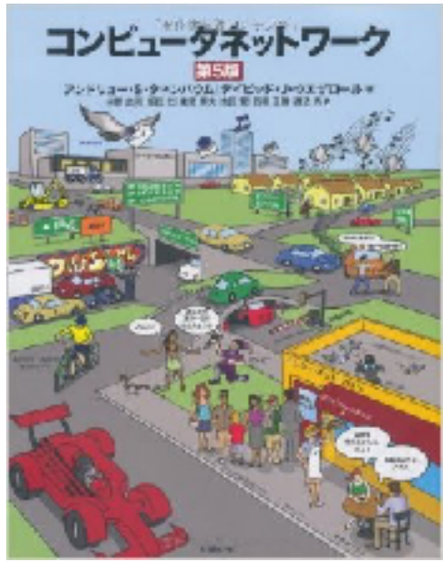
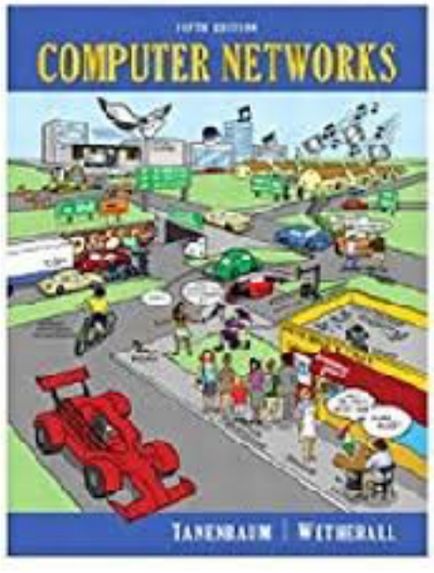
コンピュータネットワーク

開講クォーター: 1Q

曜日・時限: 火、金1-2限

講義室: S011





https://join.slack.com/t/titech-comp-network/signup

講義日程

		授業計画		課題
05/11	第９回	ネットワーク層１ ルーティング・輻輳制御	５章	ルーティングの種類を理解し 輻輳制御手法を説明できる
05/15	第１０回	ネットワーク層２ インターネットとサービス品質	５章	インターネットの制御プロトコルを理解し ネットワーク間の接続について説明できる
05/18	第１１回	トランスポート層１ トランスポート・プロトコルの要素	６章	誤り制御とフロー制御を理解し 輻輳制御について説明できる
05/22	第１２回	トランスポート層２ UDP と TCP	６章	TCP の信頼性を理解し TCP のコネクション管理を説明できる
05/25	第１３回	アプリケーション層 DNS, 電子メール, www	７章	DNS, 電子メール, www のしくみを理解し ストリーミング，P2P について説明できる
05/29	第１４回	ネットワークセキュリティ１ 対称鍵暗号，公開鍵暗号	８章	暗号アルゴリズムを理解し SHA-1,2 と RSA について説明できる
06/01	第１５回	ネットワークセキュリティ２ デジタル署名，認証プロトコル	８章	電子メール,Web のセキュリティ の脅威について把握できる

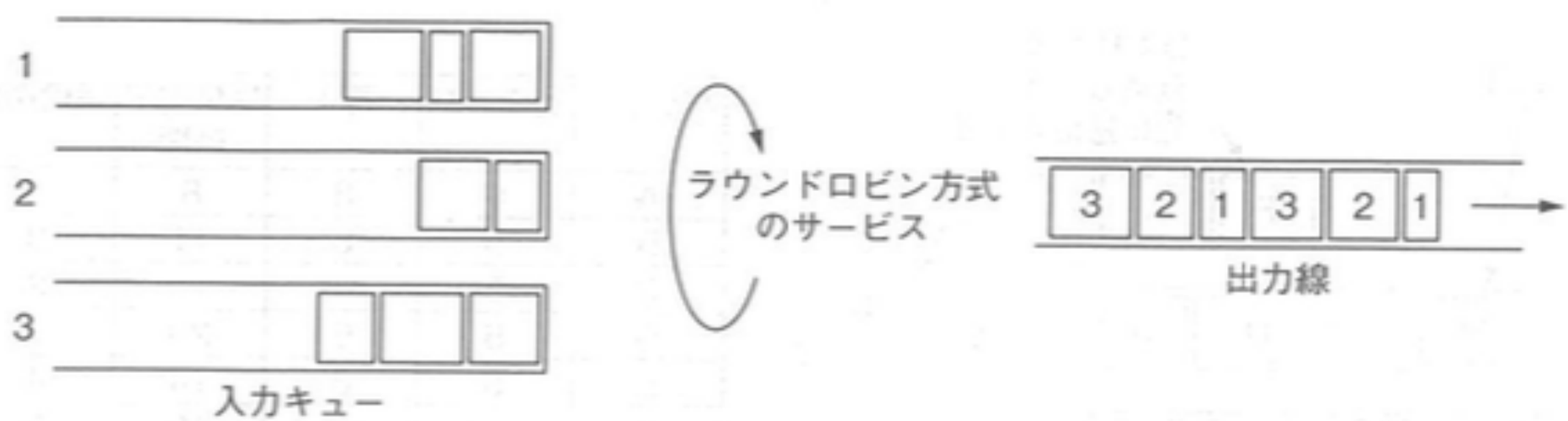
パケット・スケジューリング

<u>割り当てられるリソース</u>

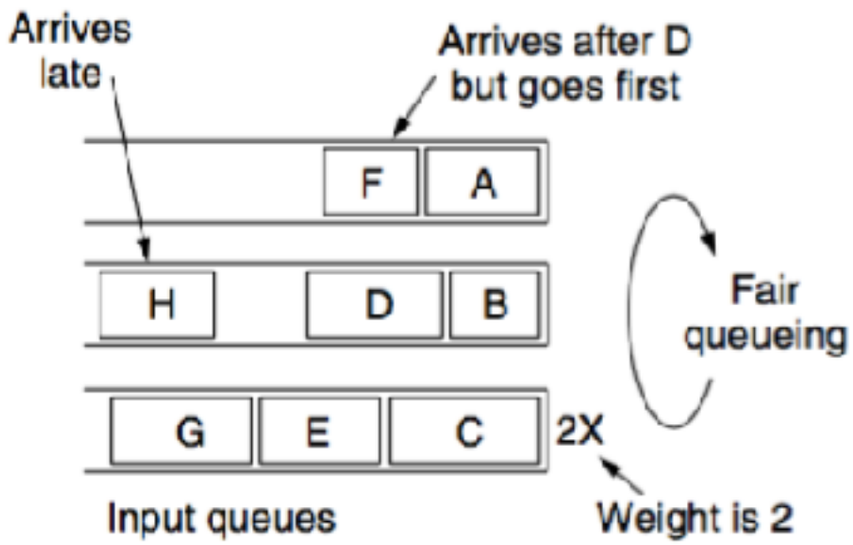
1. 帯域幅
2. バッファ・スペース
3. CPU サイクル

<u>スケジューリング・アルゴリズム</u>

1. 先入れ先出し(FIFO)
 - 一つのフローが簡単に他のフローに影響を与える
2. 公平キューイング(Fair queueing)
 - 大きいパケットを使うホストに大きい帯域幅を与える



Packet Scheduling



(a)

Packet	Arrival time	Length	Finish time	Output order
A	0	8	8	1
B	5	6	11	3
C	5	10	10	2
D	8	9	20	7
E	8	8	14	4
F	10	6	16	5
G	11	10	19	6
H	20	8	28	8

(b)

スケジューリング・アルゴリズム

3. 重み付け公平キューイング (WFQ)

到着時刻 :A

送信完了時刻 :F

パケット長 :L

フローの重み :W

$$F_i = \max(A_i, F_{i-1}) + L_i / W$$

- 送信完了時刻でソートしてキューに入れる

不足ラウンド・ロビン

- より効率的な実装が可能

許諾制御

QoS ルーティング

別経路を選択することによって十分な容量を確保し
新たなフローに対するQoSを保証する

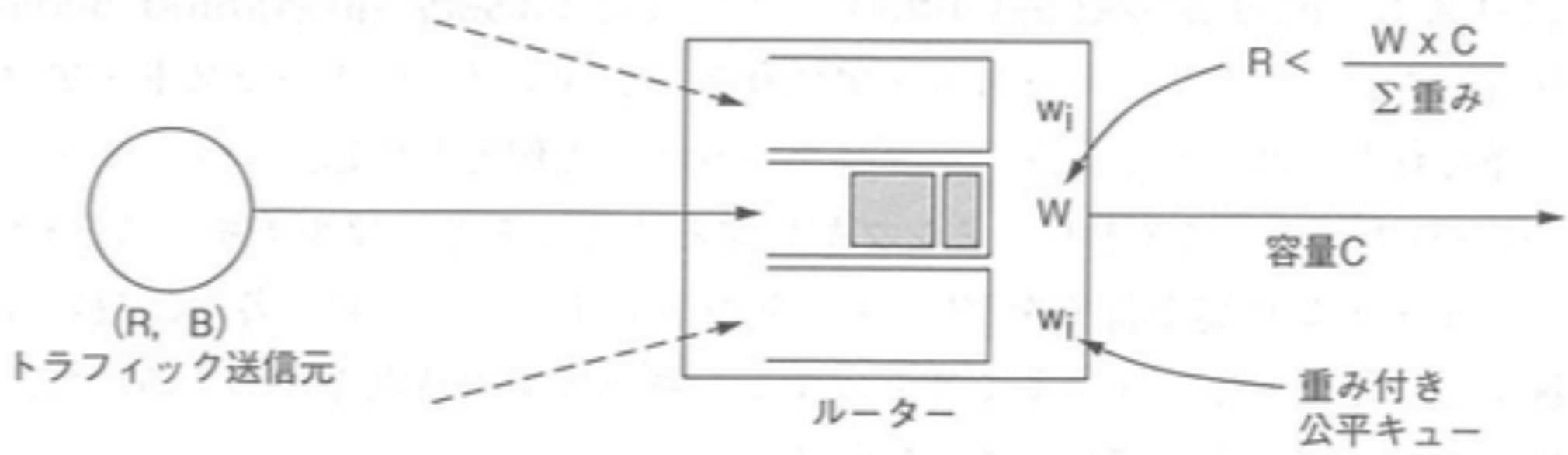
フローの仕様

パラメータ	単位
トークン・バケツ転送速度	バイト / 秒
トークン・バケツ長	バイト
ピーク時の転送速度	バイト / 秒
最小パケット長	バイト
最大パケット長	バイト

待ち時間による遅延

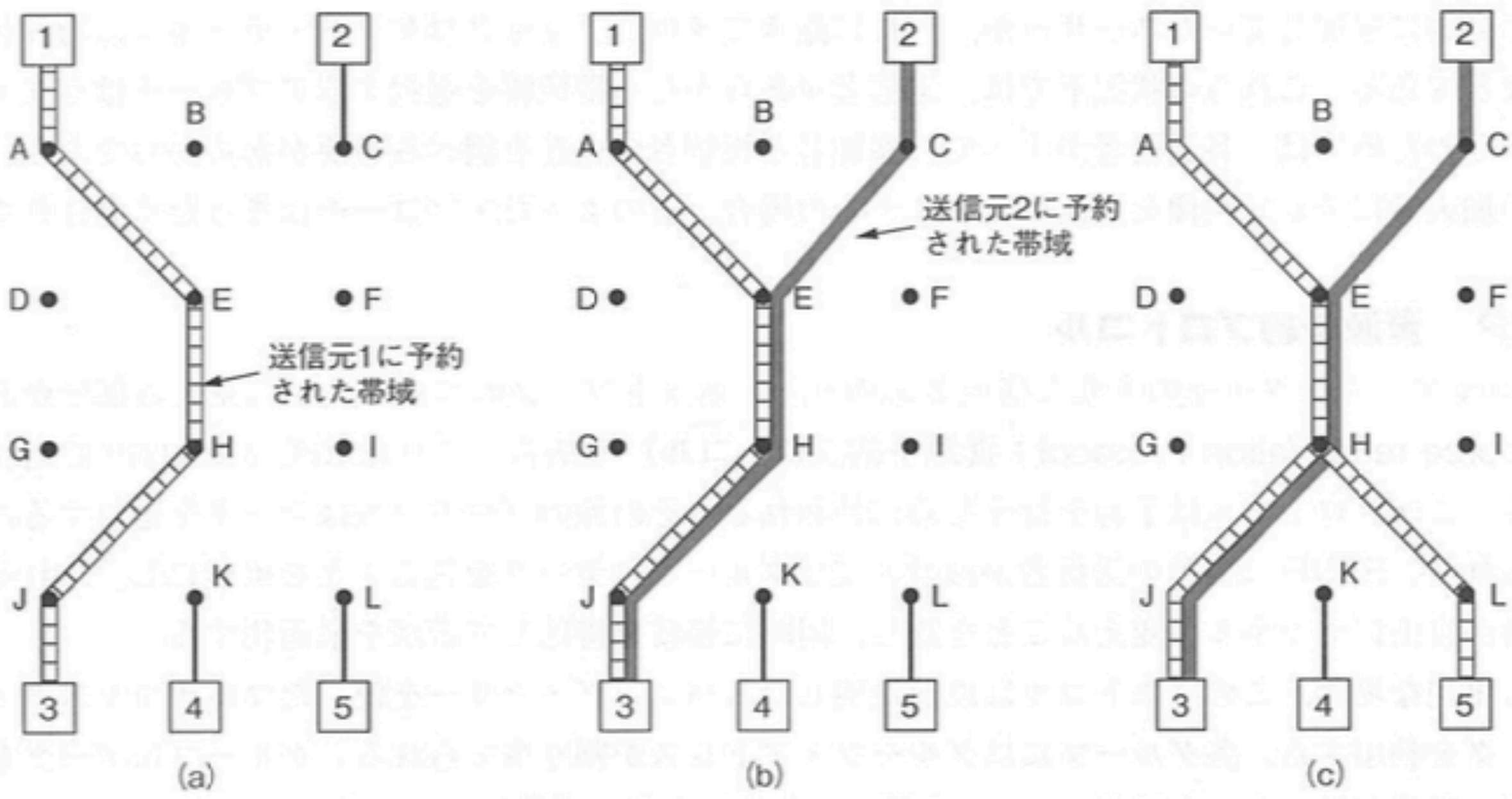
平均遅延 :T
平均到着率 :λ
平均サービス率 : μ
CPU利用率 : ρ=λ/μ

$$T = \frac{1}{\mu} \times \frac{1}{1-\lambda/\mu} = \frac{1}{\mu} \times \frac{1}{1-\rho}$$



統合サービス(IntServ)

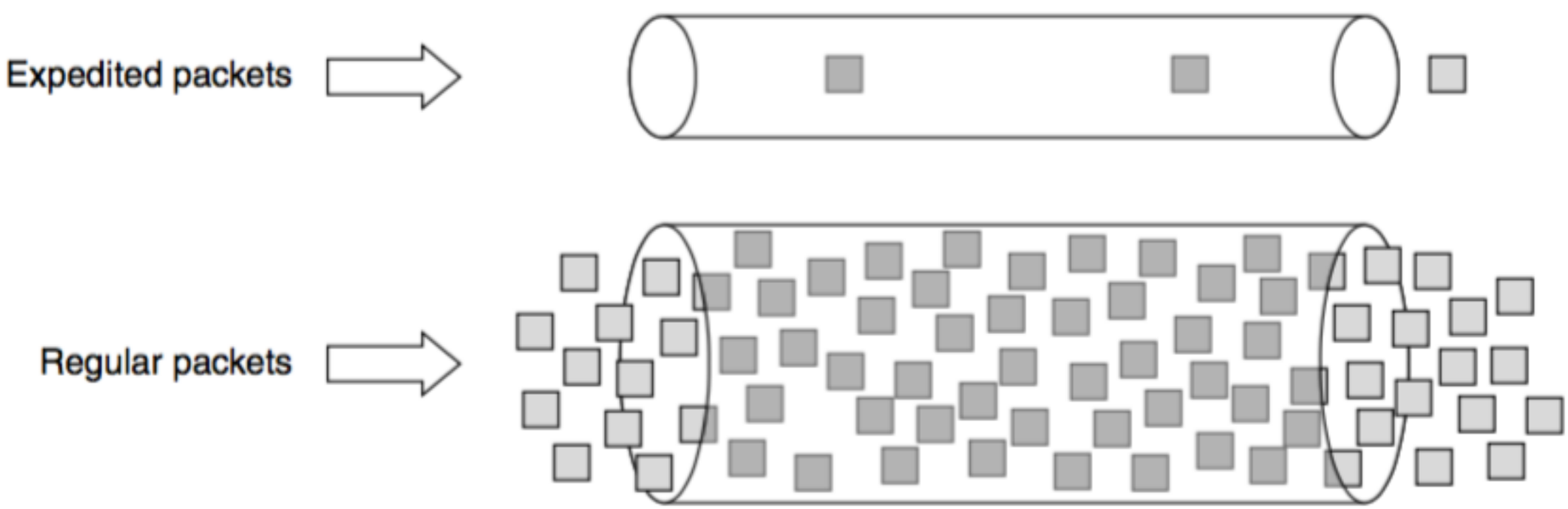
<u>資源予約プロトコル RSVP (The Resource reSerVation Protocol)</u>
受信効率を良くし、輻輳を排除するため、あるグループ内のどの受信者も予約メッセージをツリーの上流にいる送信者に逆方向経路転送アルゴリズムを用いて伝搬する



差別化サービス(DiffServ)

<u>優先転送(Expedited Forwarding)</u>

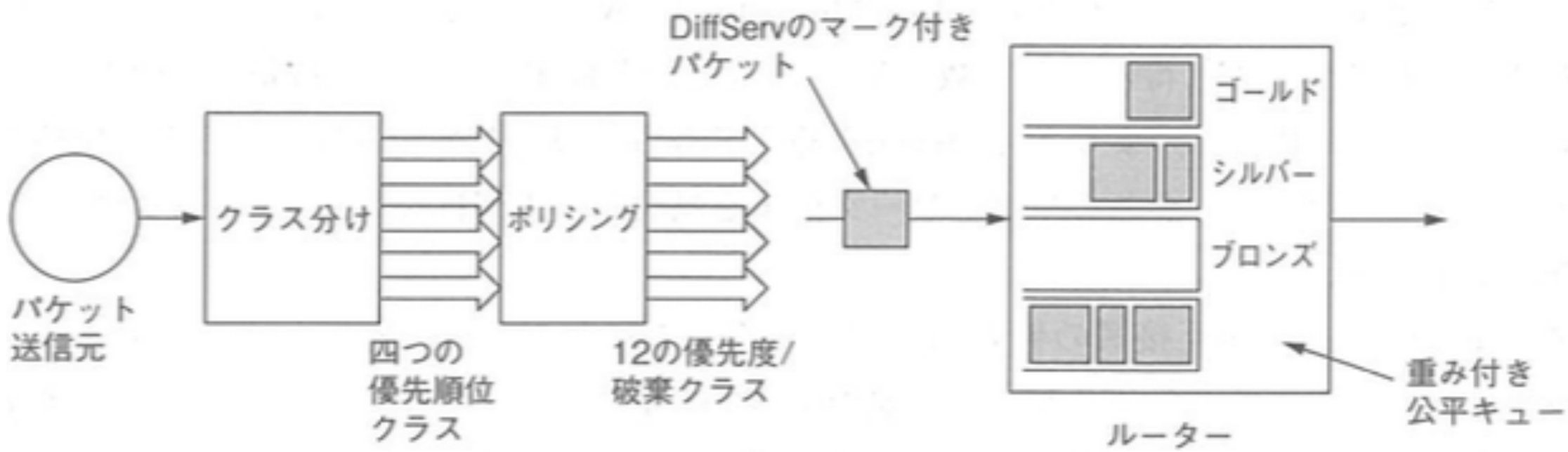
1. 大多数のトラフィックは通常クラスと考えられるが、ごく限られたパケットは優先クラスとされる
2. パケットは入口ルータで通常と優先に分けられ、それに応じたマークがつけられる
3. ルータは通常と優先パケットの２つのキューを持つ



差別化サービス(DiffServ)

<u>帯域保証転送 (Assured Forwarding)</u>

1. 4つの優先順位クラスがあり、各々が固有の資源を持つ
2. それぞれにパケット破棄クラスが3つあり、合計12クラス
3. 12クラスの分類情報がパケットに埋め込まれる
4. ルータはこの情報を元にクラス分けとポリシングを行う



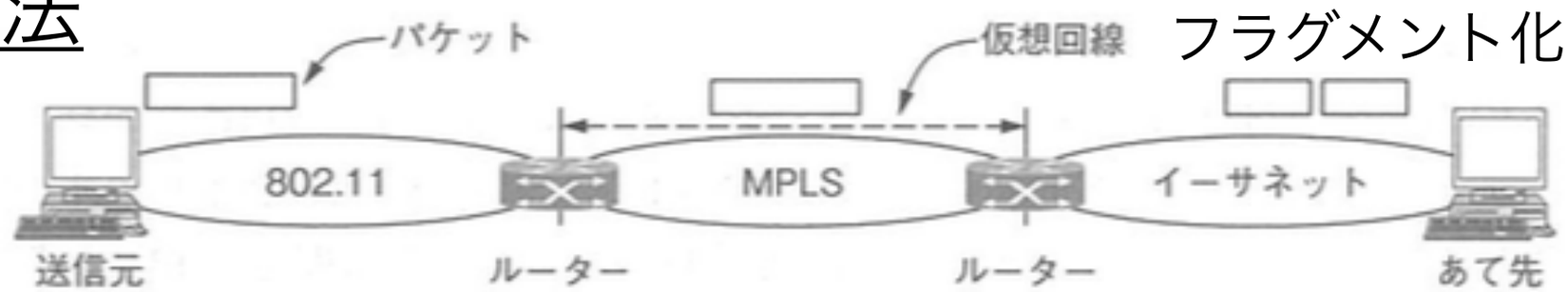
ネットワーク間接続

ネットワークの相違点

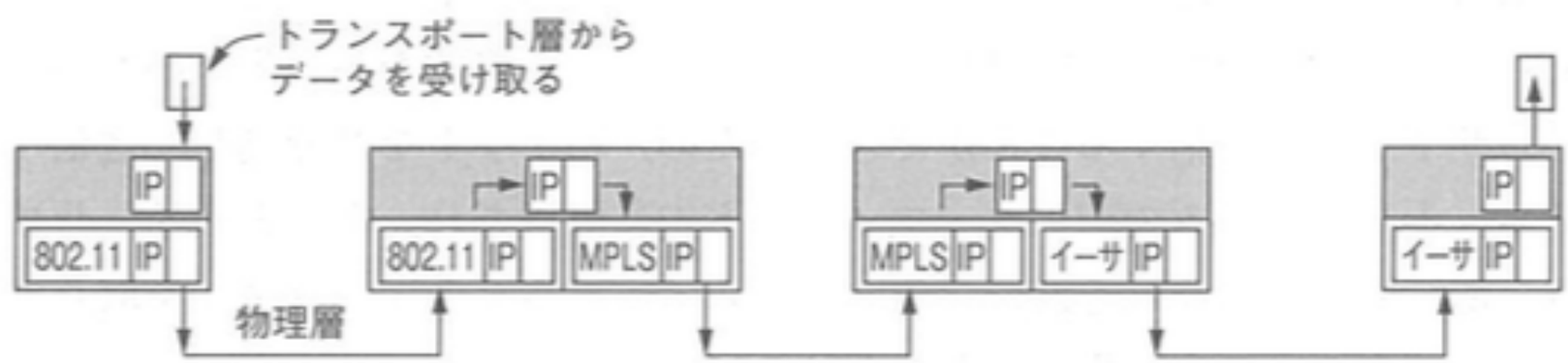
項目	いくつかの可能性
提供サービス	コネクション型，コネクションレス型
プロトコル	IP，IPX，SNA，ATM，MPLS，AppleTalk など
アドレスの付け方	フラット（802），階層的（IP）
マルチキャスト	あり，なし（ブロードキャストも同様）
パケット長	すべてのネットワークはそれぞれ固有の最大パケット長を有する
サービス品質	あり，なし，あるいはさまざまな種類がある
誤りの取り扱い	信頼性のある配送，到着順序が保証された配送，到着順序が保証されない配送
フロー制御	スライディング・ウインドウ，転送速度制御，その他，またはフロー制御なし
輻輳制御	穴開きバケツ，トークン・バケツなど
セキュリティ	プライバシーのためのルール，暗号化など
パラメータ	異なったタイムアウト，フロー仕様など
アカウント制御	接続時間，パケット数，バイト数による制御，あるいは制御なし

ネットワークの接続方法

フラグメント化

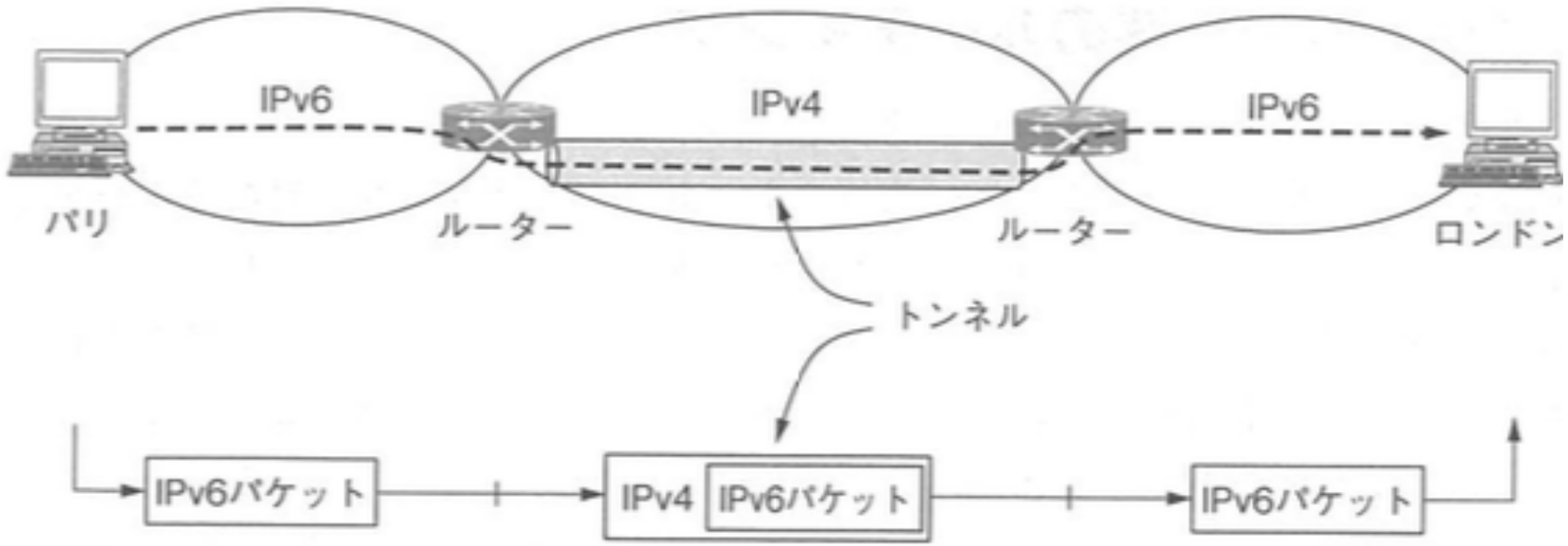


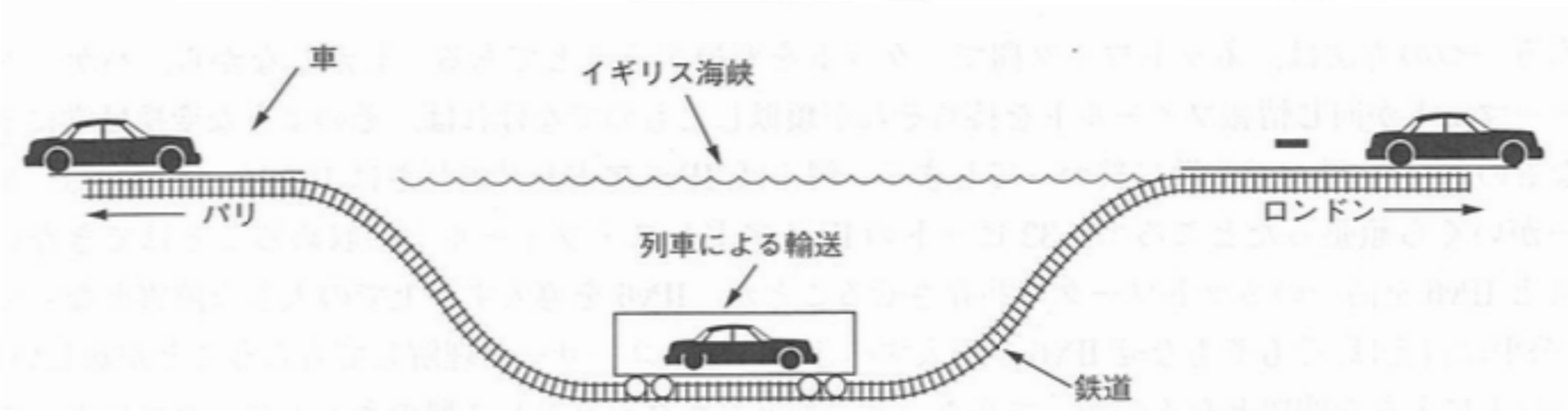
(a)



(b)

トンネリング





遠く離れた同種のネットワーク間を異なるネットワークを介して接続する場合によく利用される

ネットワーク間のルーティング

<u>パケットのフラグメント化</u>

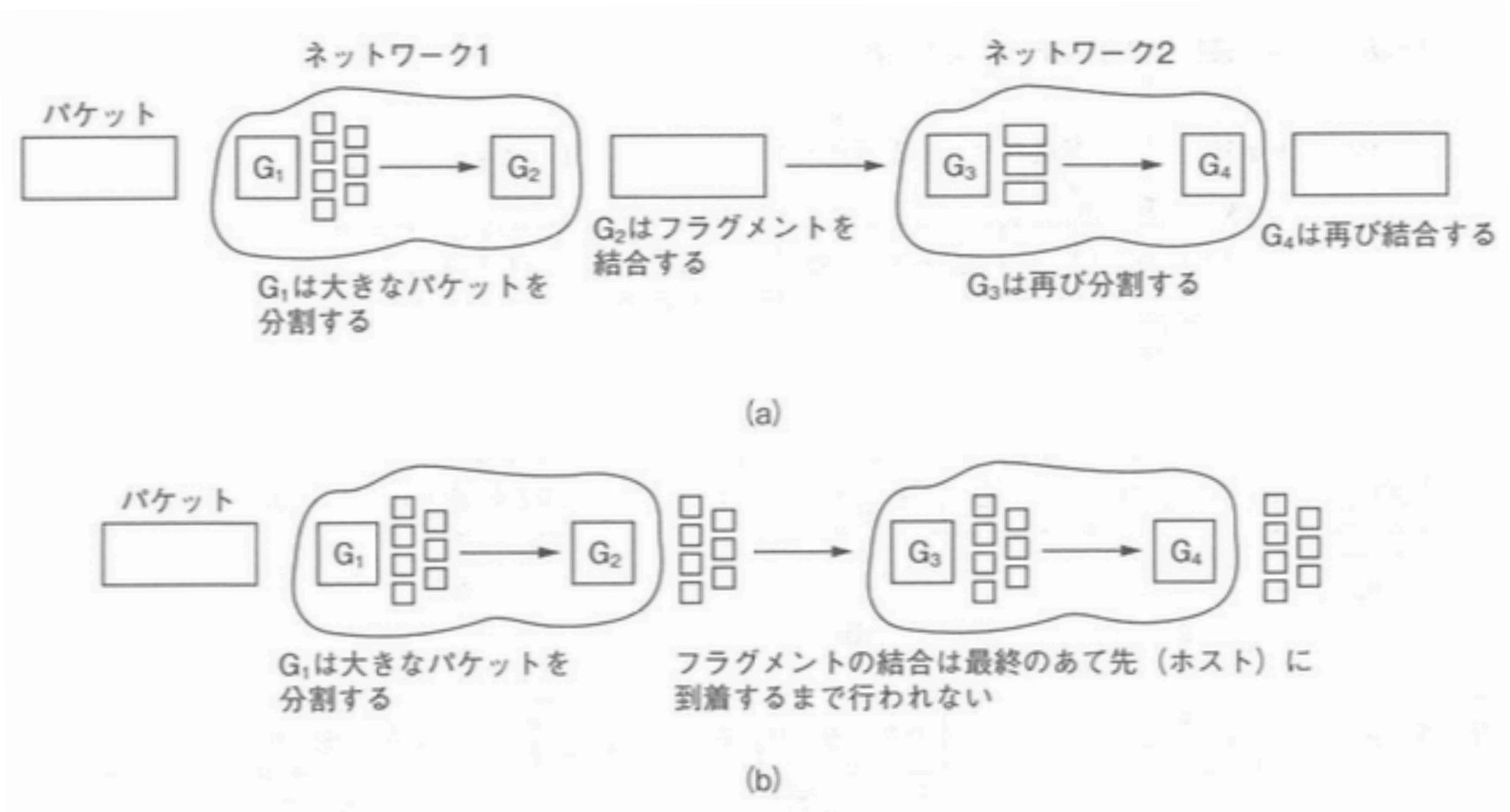
1. ハードウェア (例：イーサネット・フレームのサイズ)
2. OS (例：全てのバッファが512 Byte)
3. プロトコル (例：パケット長フィールドのビット数)
4. 国際標準への準拠.
5. 誤りによる再送の数を抑えるため
6. 一つのパケットがチャネルを占有しないようにするため

<u>MTU(Maximum Transmission Unit)</u>

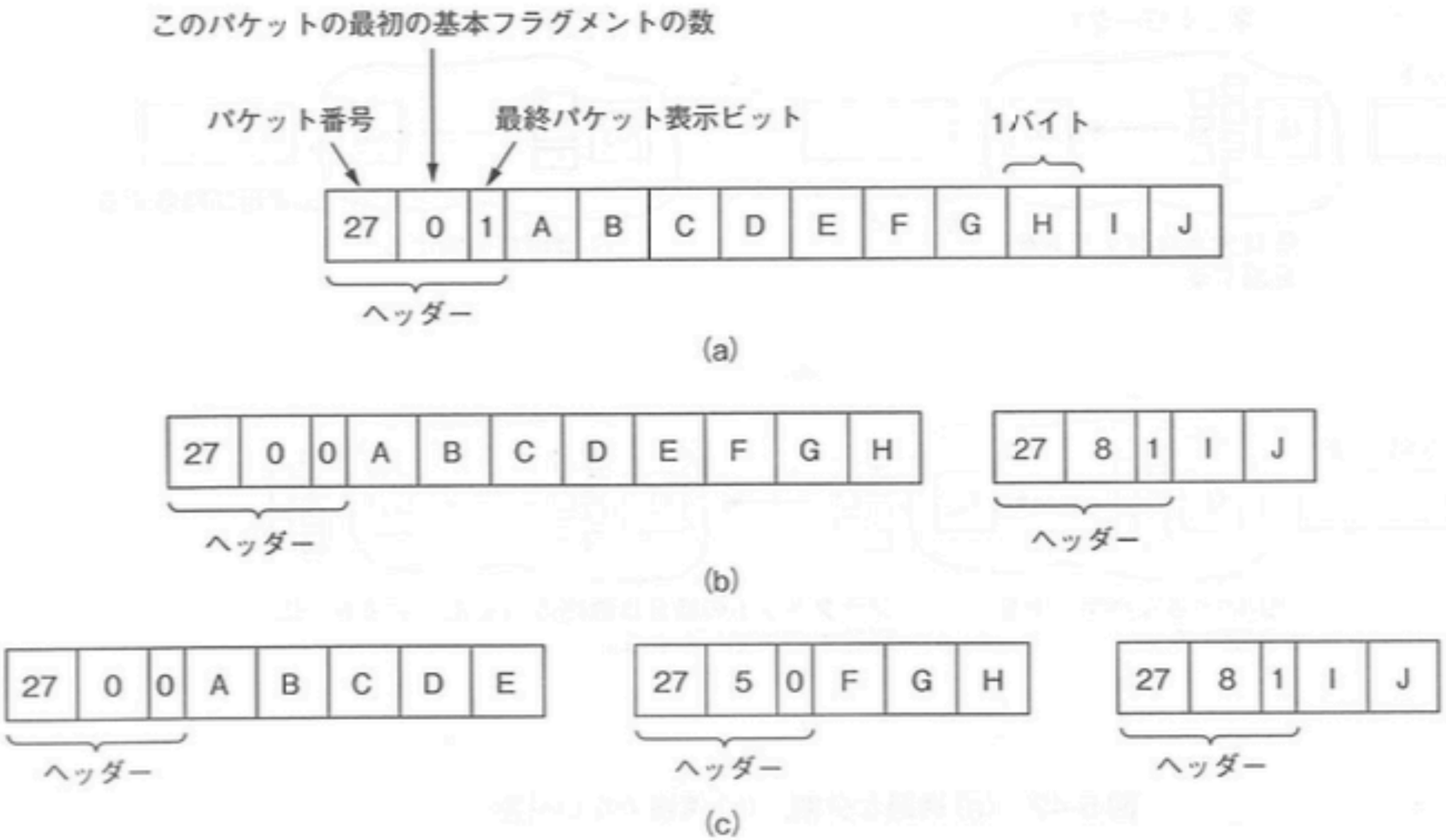
Ethernet : 1500 bytes
802.11 : 2272 bytes
IP : 65,515 bytes

パケットのフラグメント化

<u>透過なフラグメント</u>
ネットワークごとにフラグメントを結合する
<u>透過でないフラグメント</u>
フラグメントを途中で結合しない



パケットのフラグメント化

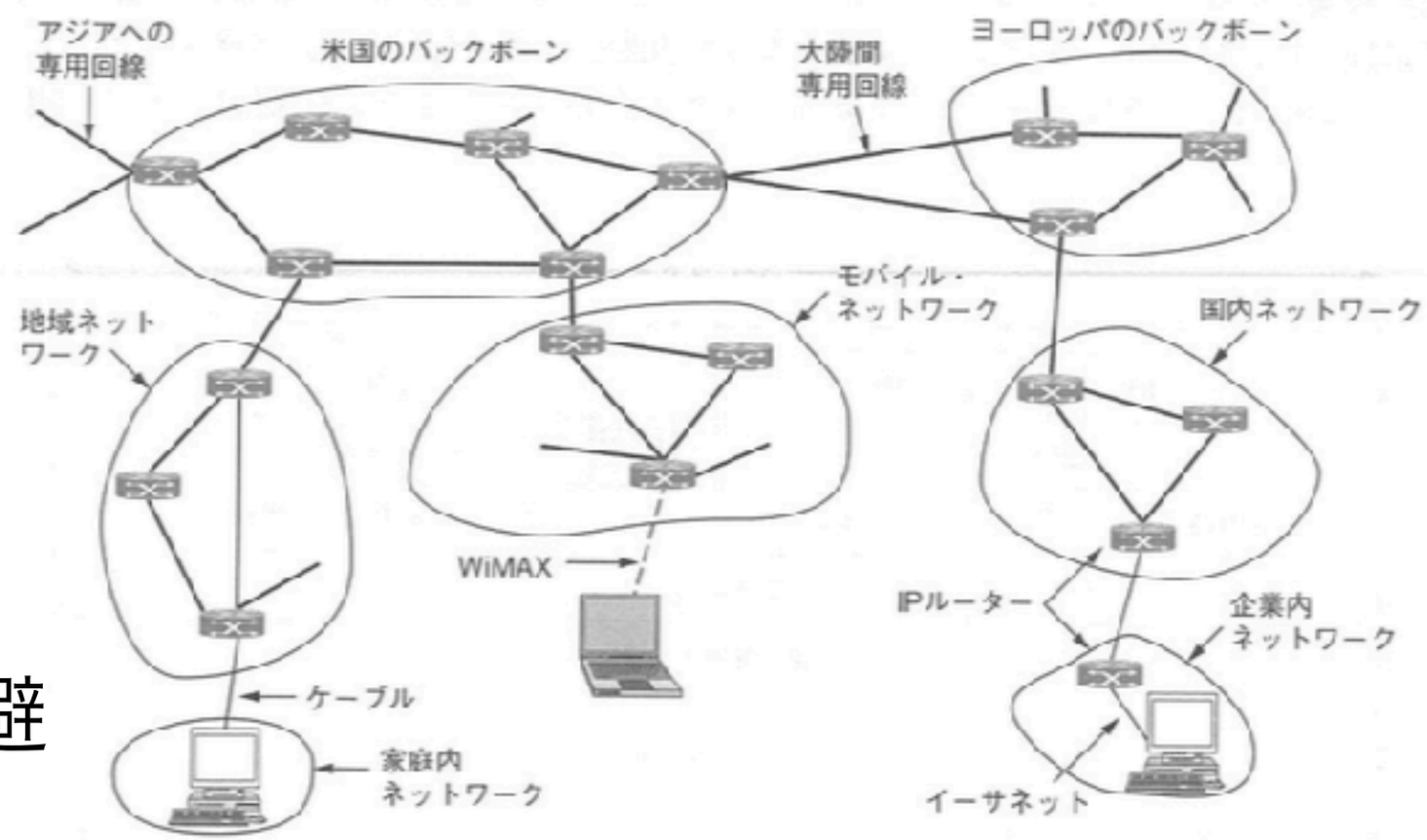


経路MTU探索

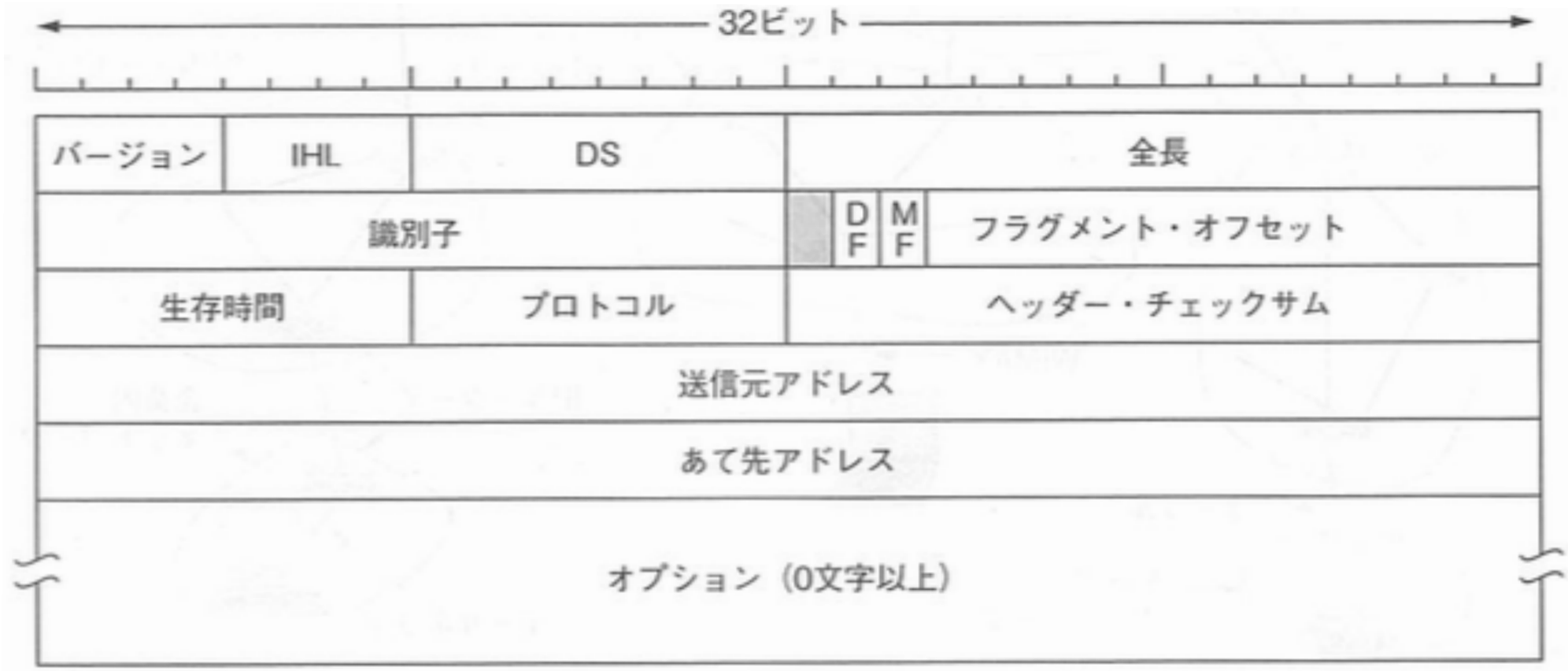
MTU(Maximum Transmission Unit)

インターネットにおけるネットワーク層

1. 動作の保証
2. 単純さの維持
3. 明確な選択
4. モジュール単位の開発
5. 異種性の容認
6. 静的なパラメータの回避
7. 良い設計を探す
8. 送信時の正確さ、受信時の耐性
9. スケーラビリティ
10. 性能とコストを考慮



The IP Version 4 Protocol



(課題6)

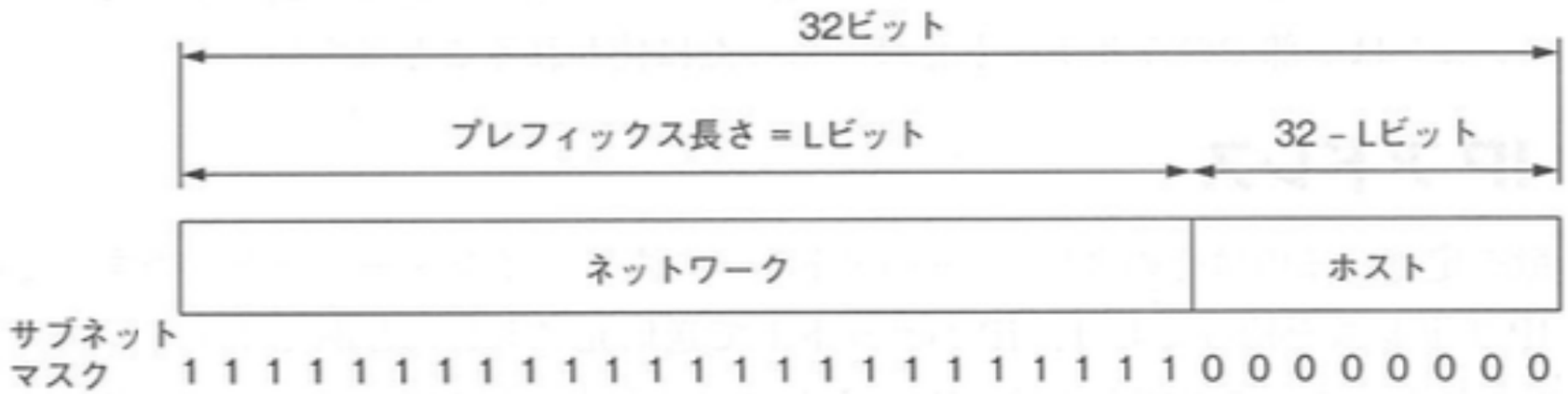
バージョン: IPv4 or IPv6
IHL: ヘッダの長さ (min 5, max 15)
DS: サービスクラス、輻輳の通知
全長: ヘッダ＋データ全体の長さ (max 65,535)
識別子: フラグメントがどのパケットに属するか
DF: Don’t fragment (MTUを求めるのにも使われる)
MF: More fragments
フラグメント・オフセット: フラグメントのパケット内のオフセット
生存時間: パケットの寿命(255秒)
プロトコル:TCP, UDPなど
ヘッダ・チェックサム: 16ビットごとに1の補数、到着時に0になるはず
オプション: 将来のバージョンで使うためのスペース

The IP Version 4 Protocol オプション

オプション	説明
セキュリティ	データグラムをどのように秘密にするかが明記されている
ストリクト送信元ルーティング	従うべき完全な経路を指定する
ルーズ送信元ルーティング	必ず通らなければならないルーターのリストを与える
経路記録	各ルーターにその IP アドレスを記憶させる
タイムスタンプ	各ルーターにその IP アドレスとタイムラインスタンプを記憶させる

IP アドレス

(課題7)



128.208.0.0/24

ドット付き10進表記

ネットワーク部のサイズ

サブネット・マスク

255.255.255.0

上位ビットには可変長のネットワーク部があり、
下位ビットには残るビットのホスト部がある

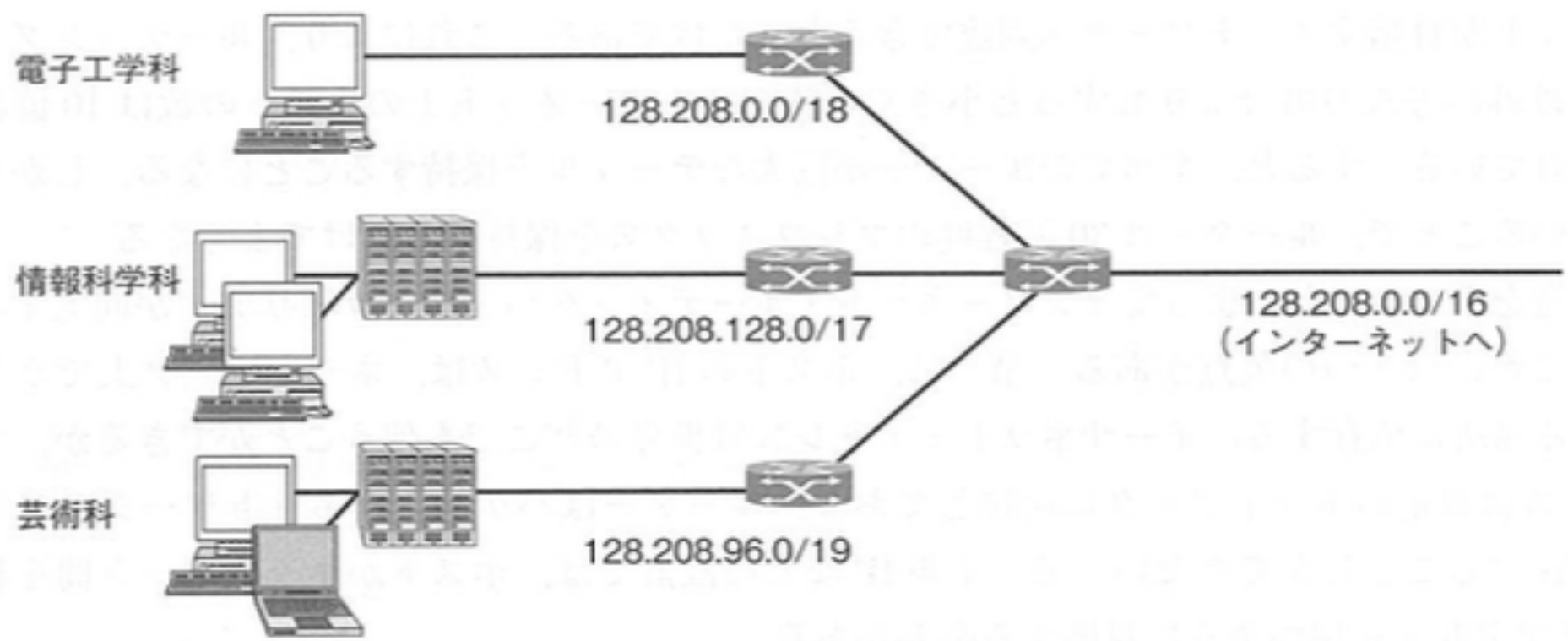
それぞれのネットワークが固有のアドレス・ブロックを持つ

階層構造を用いることでルータは30万程度のプレフィックスを保持するだけで済んでいる

サブネット

ネットワーク番号は、競合を防ぐために
ICANN (Internet Corporation for Assigned Names and Numbers)
によって管理されている

情報科学科：	10000000	11010000	1|xxxxxxx	xxxxxxxx
電子工学科：	10000000	11010000	00|xxxxxx	xxxxxxxx
芸術科：	10000000	11010000	011|xxxxx	xxxxxxxx



組織内でアドレス・ブロックをいくつかのサブネットに分割し
単一のネットワークとして振る舞うようにする
サブネット・マスクとの論理積を取るとホストのアドレスが
取り出せる

CIDR—Classless InterDomain Routing

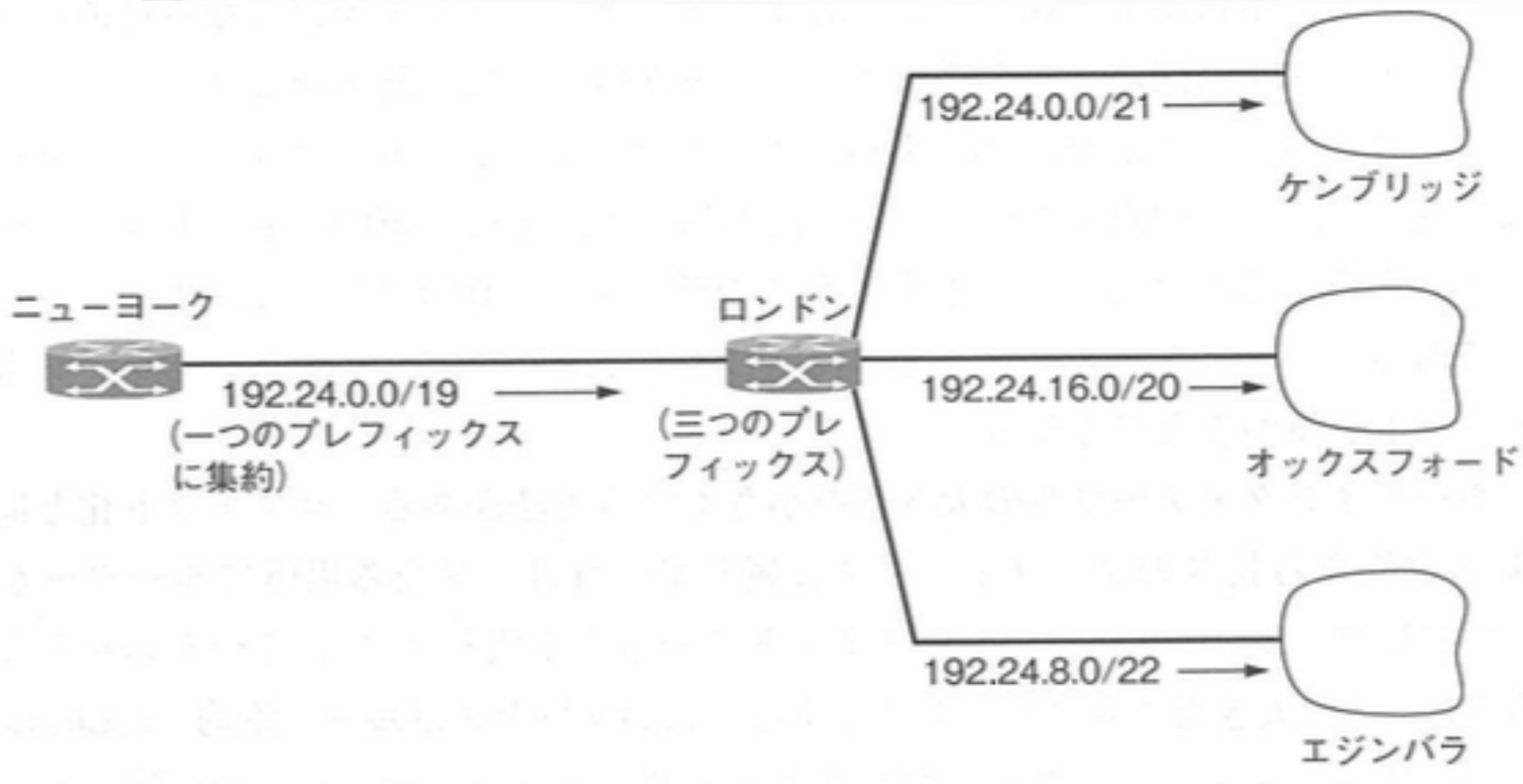
ISPのルータやバックボーンの中核ルータは全ての経路を知っている必要がある

(課題8)

<u>ルート集約</u>

小さなプレフィックスをまとめて一つのスーパーネットにする

大学	最初のアドレス	最後のアドレス	個数	表記
ケンブリッジ	194.24.0.0	194.24.7.255	2048	194.24.0.0/21
エジンバラ	194.24.8.0	194.24.11.255	1024	194.24.8.0/22
（利用可能）	194.24.12.0	194.24.15.255	1024	194.24.12/22
オックスフォード	194.24.16.0	194.24.31.255	4096	194.24.16.0/20

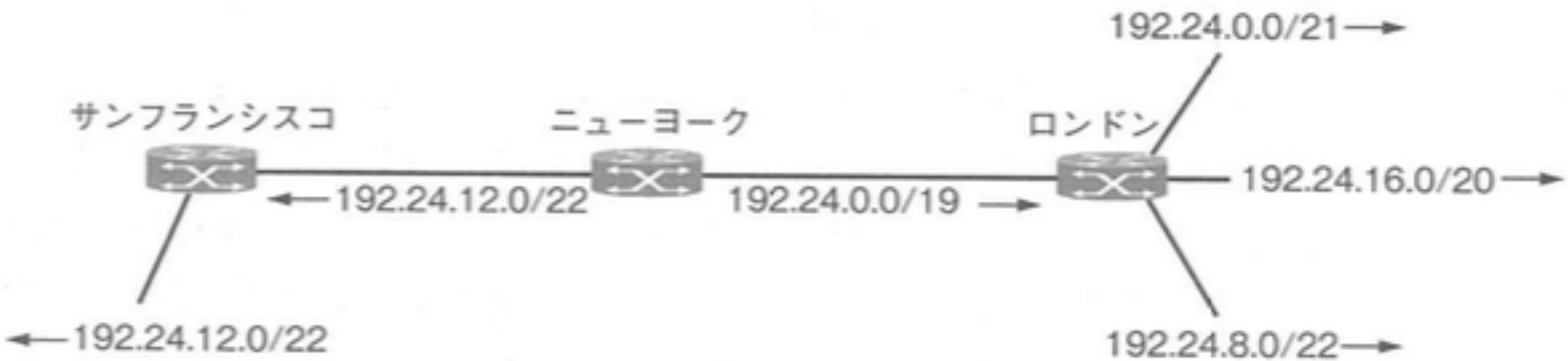


CIDR—Classless InterDomain Routing

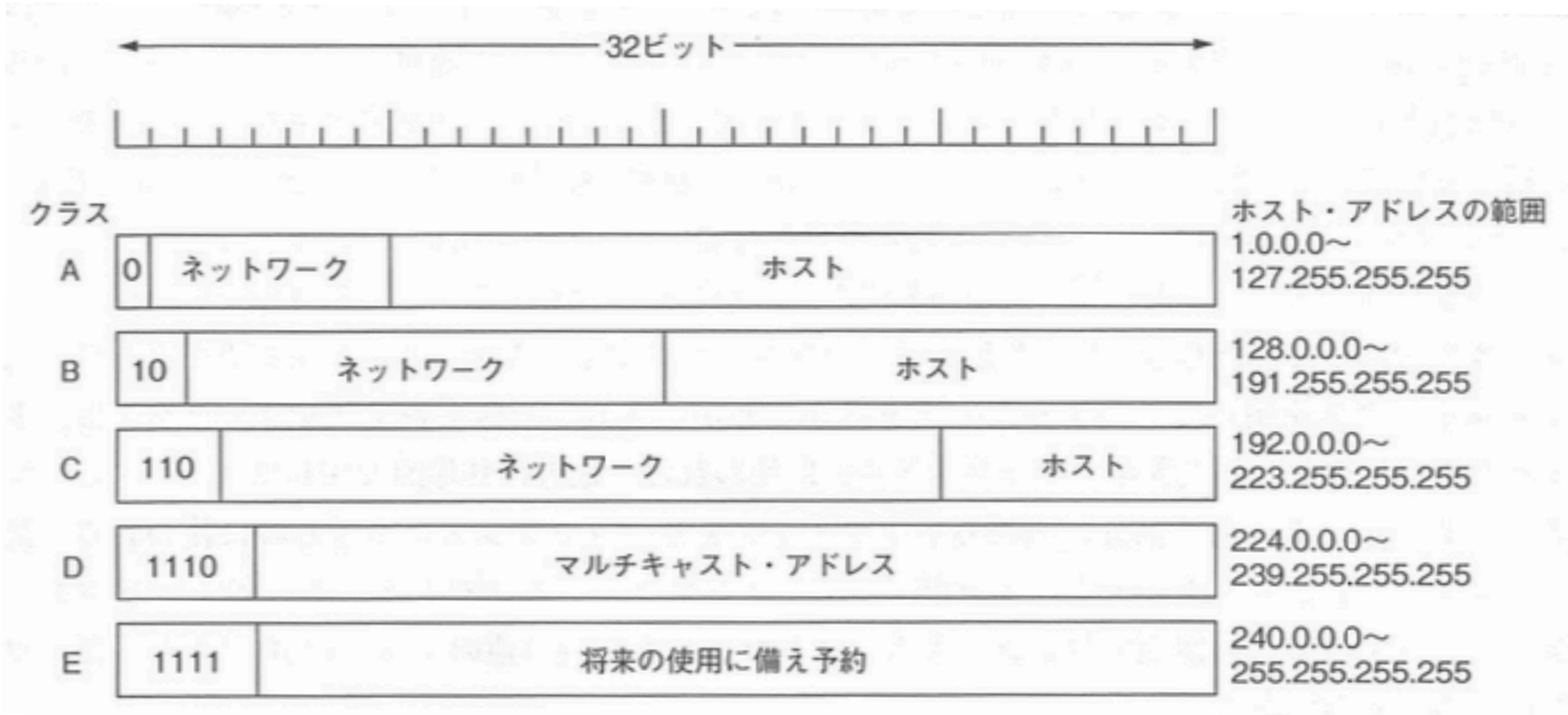
<u>最長マッチング・プレフィックス</u>

1. パケットが来るとルーティング・テーブルを検索し、あて先がプレフィックスの中にあるかどうかを調べる
2. 複数の項目がマッチする場合最も長いエントリを採用する

例えば/20のマスクと/24のマスクがマッチした場合、/24を選択する



クラスフル・アドレッシング



1993年以前

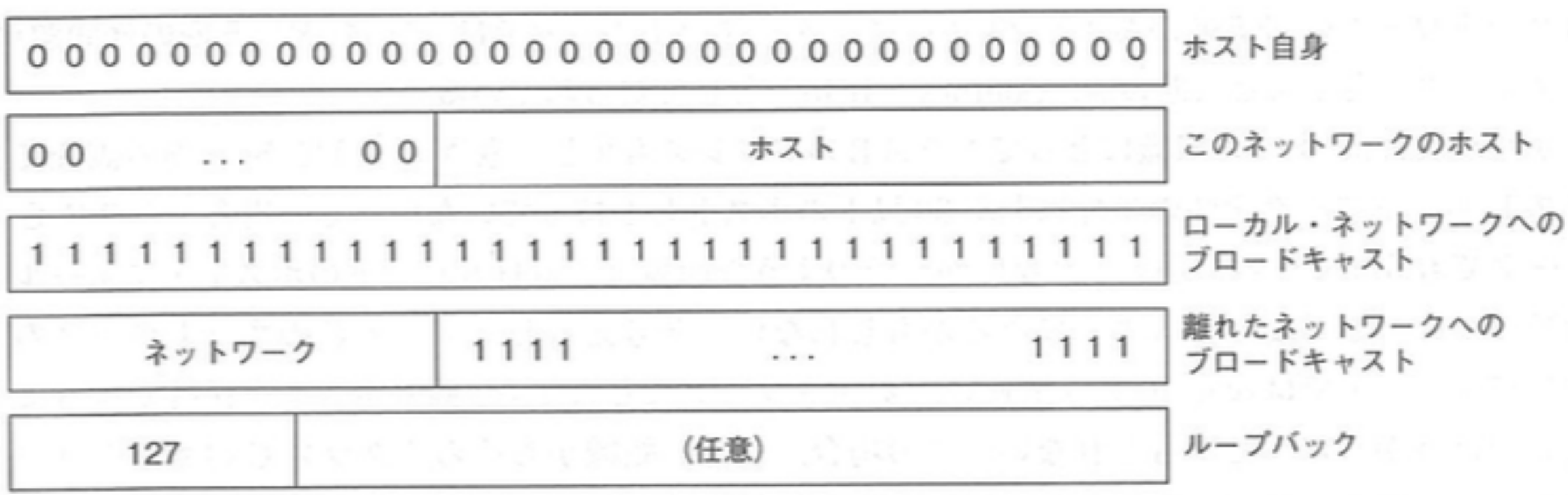
クラスごとにブロックの大きさは固定

A, B, Cのどのクラスに属するかを示すビットは現在は使われていない

クラスDはマルチキャストのために現在も使われている

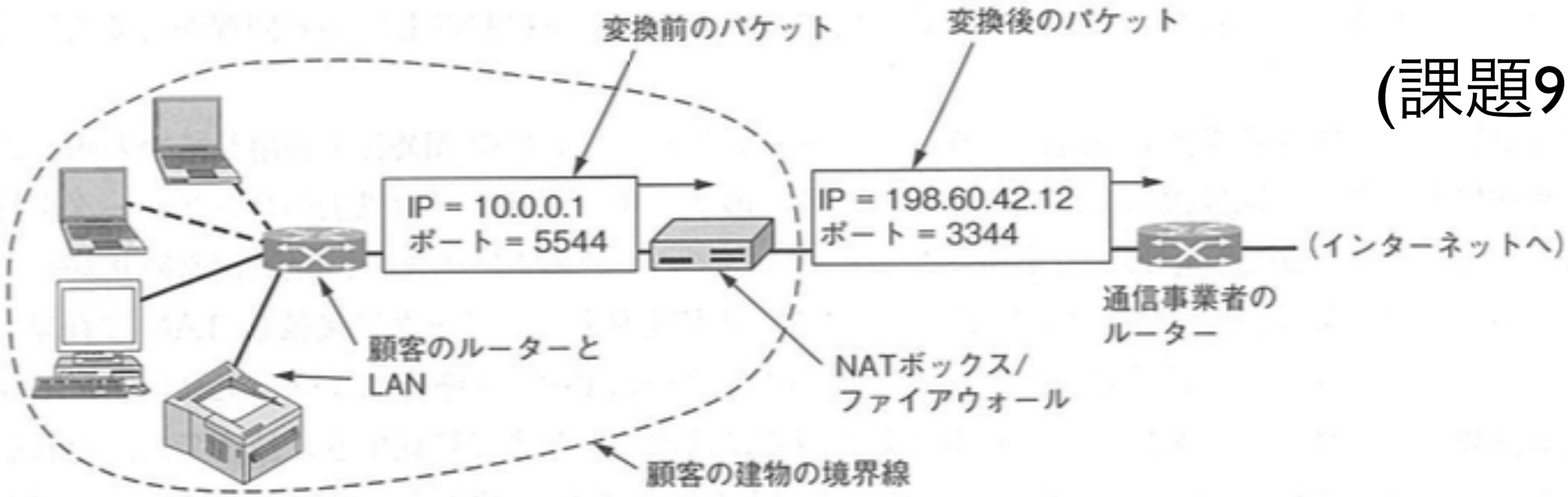
特別なIPアドレス

0.0.0.0: ホスト自身
255.255.255.255: 全てのホスト (broadcast)
127.xx.xx.xx: ループバック・テスト用



ネットワーク・アドレス変換NAT

(課題9)



パケットがNATボックスを通過すると送信元アドレス10.0.0.1がグローバルIPアドレス198.60.42.12に変換される

逆にISPからNATボックスにパケットが届くと、TCPヘッダの送信元ポートが参照されNATボックスから10.0.0.1の割り当てを受ける

IP Version 6

IPv4: 32-bit
IPv6: 128-bit

1. 非効率にアドレスを割り当てても、数十億台のホストに対応できること
2. ルーティング・テーブルのサイズを削減すること
3. ルータの処理を高速化するため、単純あプロトコルとすること
4. より良いセキュリティ（認証やプライバシー）を提供すること
5. リアルタイム・データなど、サービスの種類に注目したプロトコルとすること
6. スコープを指定できるようにし、マルチキャストを行いやすくすること
7. ホストがアドレスを変えることなくローミングを行えるようにすること
8. 将来の発展を見越したプロトコルとすること
9. 数年の間は、新しいプロトコルと古いプロトコルが共存できるようにすること

The Main IPv6 Header

(課題10)

バージョン: IPv4 or IPv6
DS: サービスクラス、輻輳の通知
フロー・ラベル: 同じように扱うべきパケットに印をつける
ペイロード長: ヘッダを除くデータの大きさ (max value 65,535)
次ヘッダ: ６種類ある拡張ヘッダのうちどれを用いるのか
ホップ制限: IPv4の生存期間は秒だったが、実際の使われ方はホップが多かった

拡張ヘッダ

拡張ヘッダー	内容
ホップ・バイ・ホップ・オプション	ルーターに対するさまざまな情報
あて先オプション	あて先に関する付加情報
ルーティング	訪問したルーターのルーズ・リスト
フラグメント化	データグラム・フラグメントの管理
認証	送信元の身元確認
暗号化されたセキュリティ・ペイロード	暗号化された内容についての情報

ホップ・バイ・ホップ・オプション

	タイプ	長さ	値
次ヘッダー	0	194	4
ジャンボ・ペイロード長			

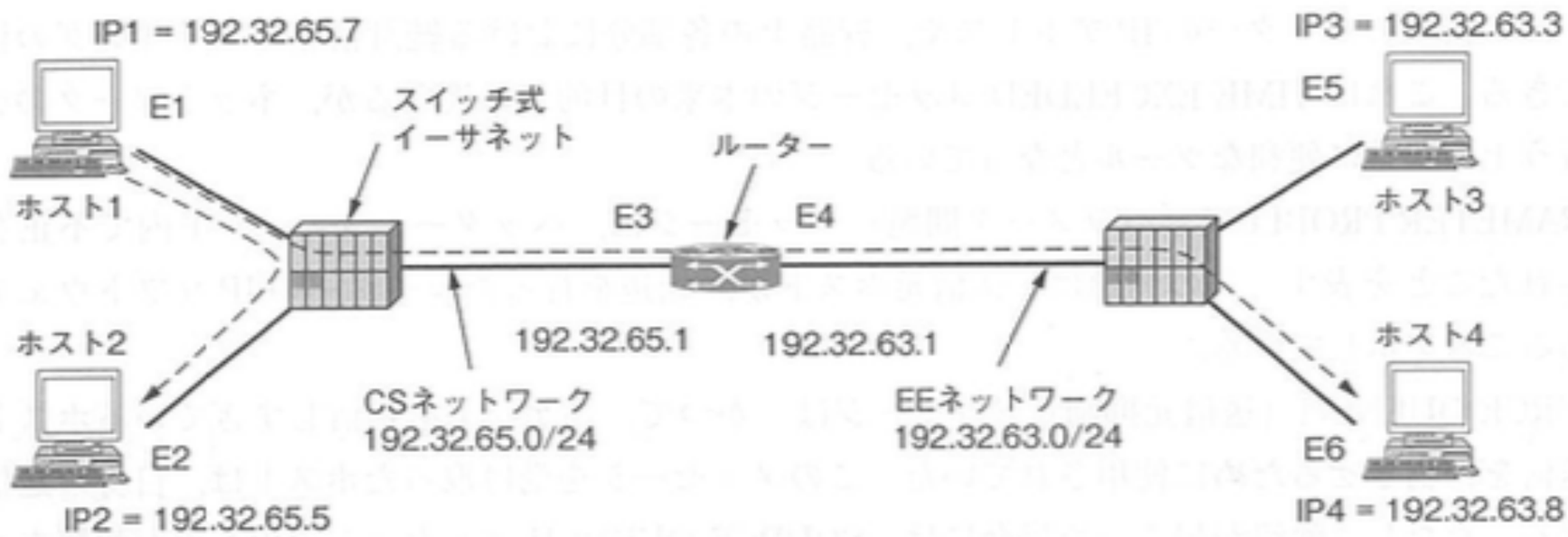
ルーティング

次ヘッダー	拡張ヘッダー長	ルーティング・タイプ	セグメント残数
タイプ固有のデータ			

インターネット制御プロトコル (IMCP)

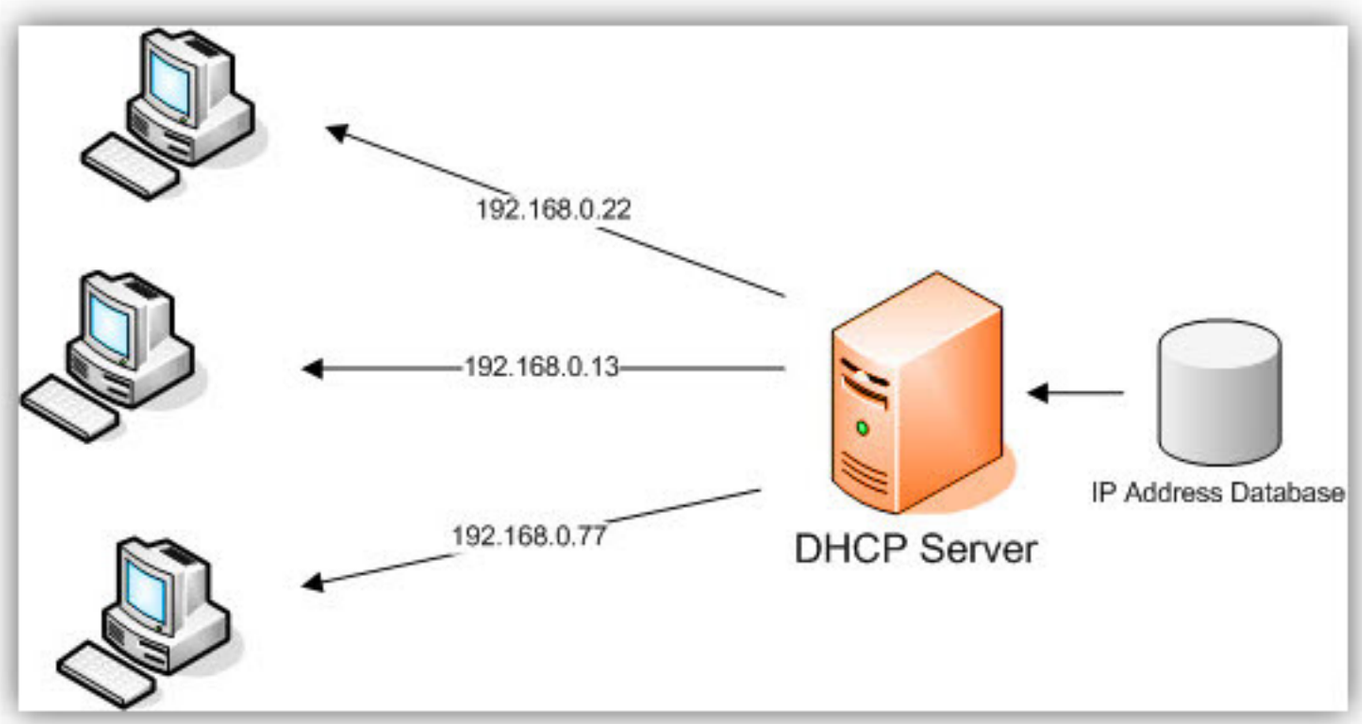
メッセージ・タイプ	説明
あて先到達不能	パケットが配送できない
時間超過	生存時間カウンタが0になった
パラメータ問題	間違ったヘッダー・フィールド
送信元制御	チョーク・パケット
リダイレクト	ルーターに地理情報を教える
エコーとエコー応答	マシンに生きているかどうか尋ねる
タイムスタンプ要求 / 応答	エコー要求と同じ（ただし，タイムスタンプが付加されている）
ルーター広告 / 要請	近隣のルーターを見つける

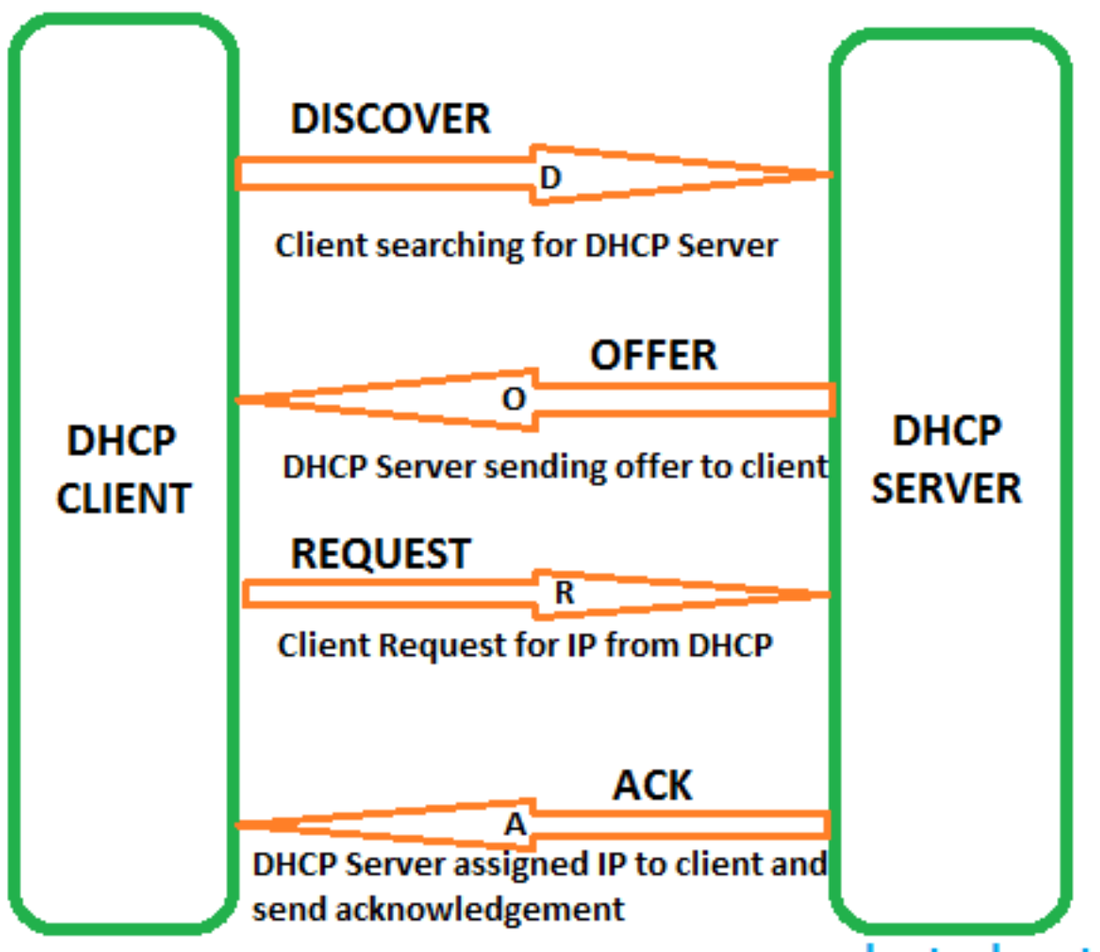
アドレス解決プロトコル (ARP)



フレーム	送信元 IPアドレス	送信元 イーサネット・アドレス	あて先 IPアドレス	あて先 イーサネット・アドレス
ホスト1から2へ，CSネット上で	IP1	E1	IP2	E2
ホスト1から4へ，CSネット上で	IP1	E1	IP4	E3
ホスト1から4へ，EEネット上で	IP1	E4	IP4	E6

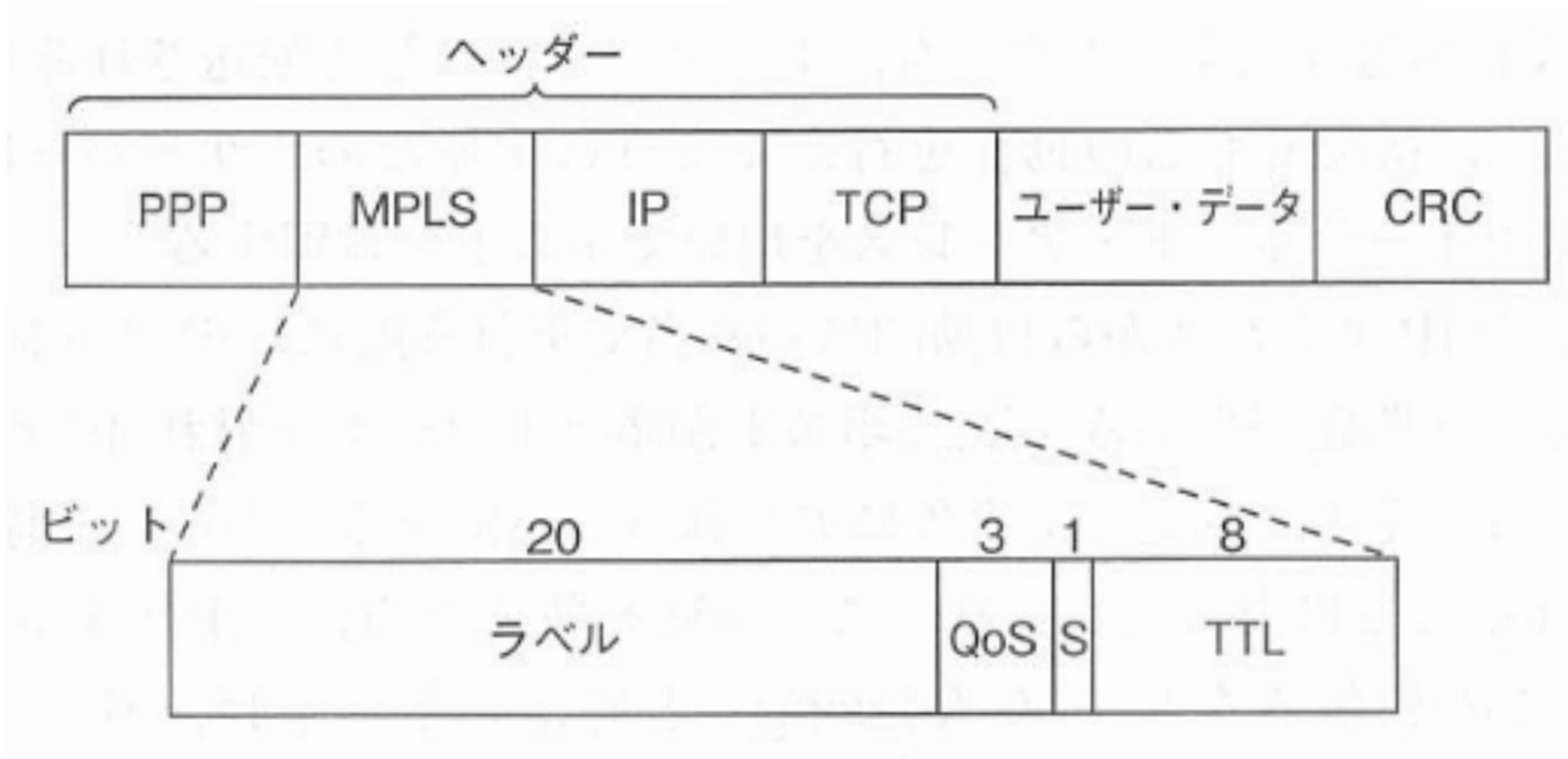
DHCP—The Dynamic Host Configuration Protocol

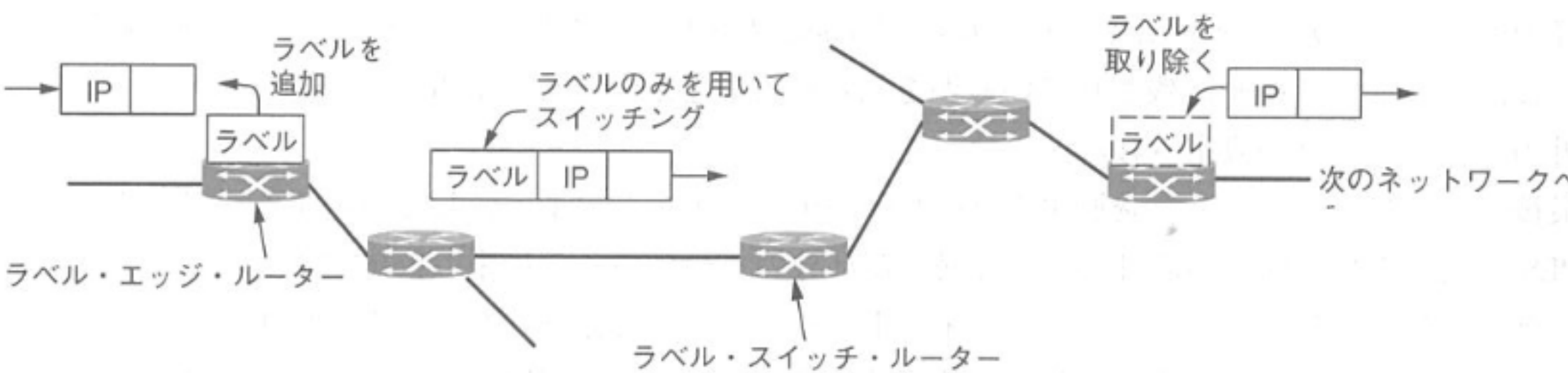




ラベル・スイッチとMPLS

パケットの前にラベルを追加し、宛先アドレスの代わりに
このラベルをもとにパケットの転送を行う

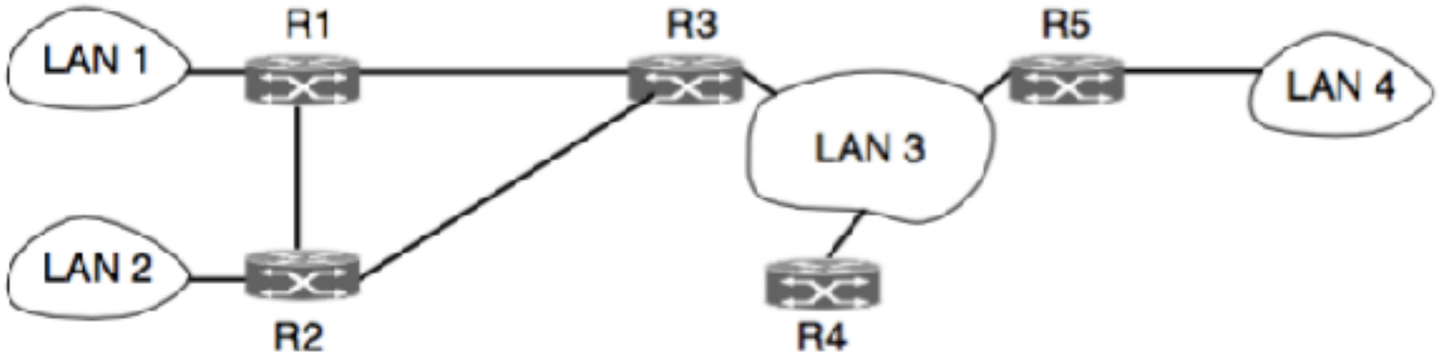




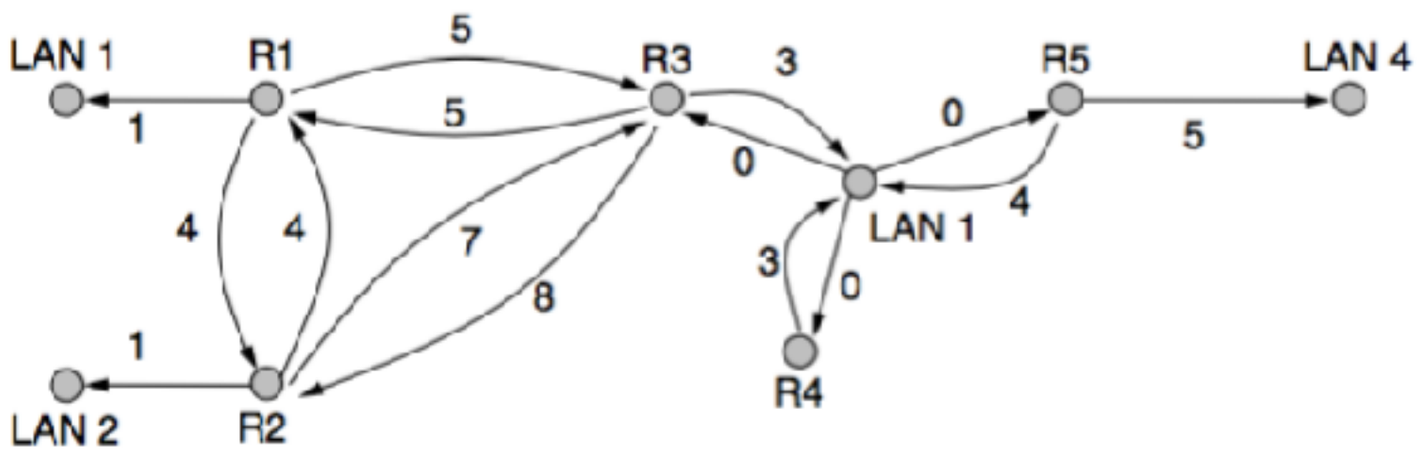
ゲートウェイ内ルーティング・プロトコル
Open Shortest Path First (OSFP)

<u>OSPFの要求</u>

1. アルゴリズムは広く文献で公表されているもの
2. 様々な距離の基準をサポート
3. 動的なアルゴリズムであること
4. サービスの種類に基づいたルーティング
5. 負荷分散
6. 階層的なシステムのサポート
7. セキュリティ

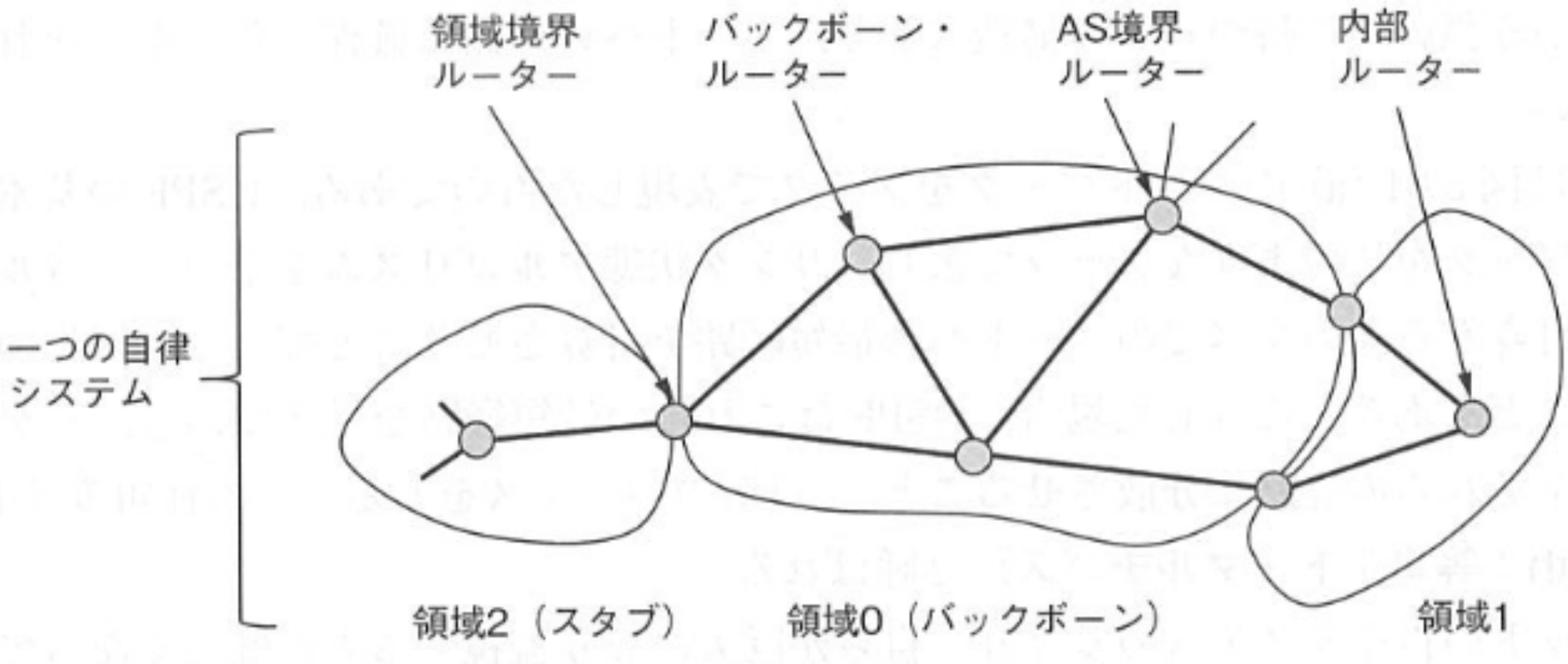


(a)



(b)

ゲートウェイ内ルーティング・プロトコル



OSPF メッセージ

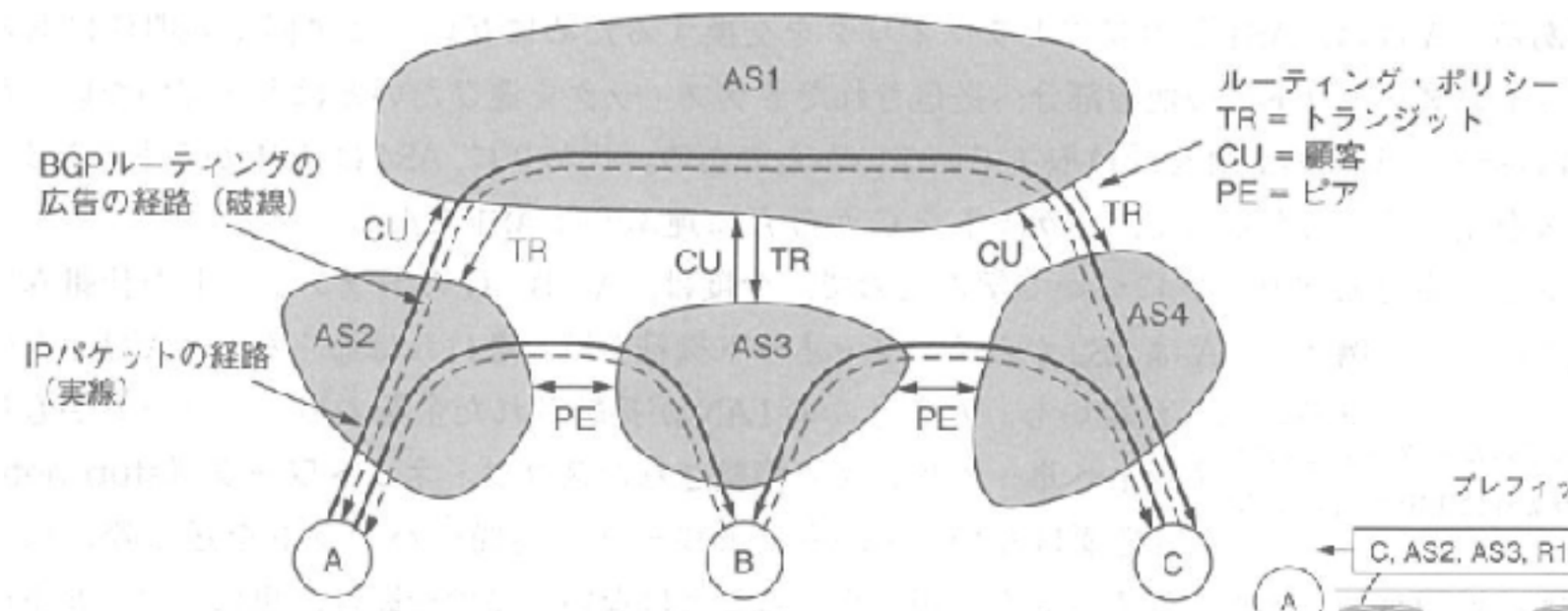
メッセージの種類	記述
ハロー	隣接ルーターを知るために用いる
リンク状態更新	送信元のコストを隣接ルーターに伝える
リンク状態確認	リンク状態更新メッセージの確認
データベース記述	送信元が保持している更新情報の告知
リンク状態要求	パートナーへ情報提供を求める

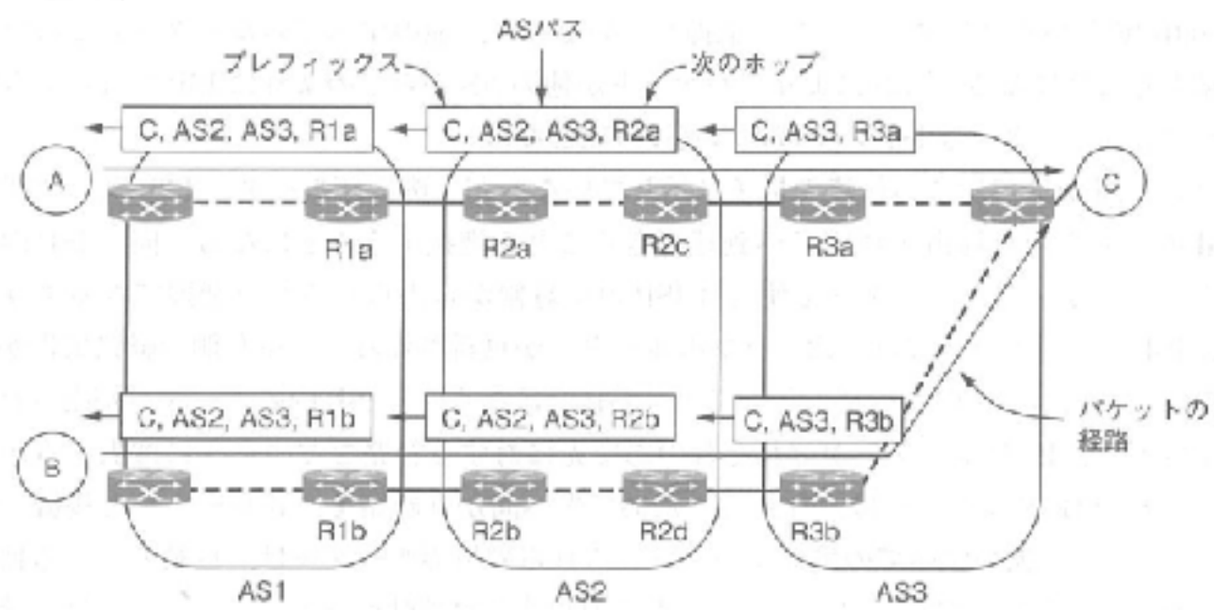
ゲートウェイ外ルーティング・プロトコル

Boarder Gateway Protocol(BGP)

BGPのルールの一例

1. 教育ネットワーク上で商用トラフィックを運んではならない
2. ペンタゴンからのトラフィックはイラクを通さない
3. Verizon社ではなく、料金の安いTeliaSonera社を利用する
4. 性能が悪いためオーストラリアではAT&Tを利用しない
5. Apple社のトラフィックはGoogle社を通さない



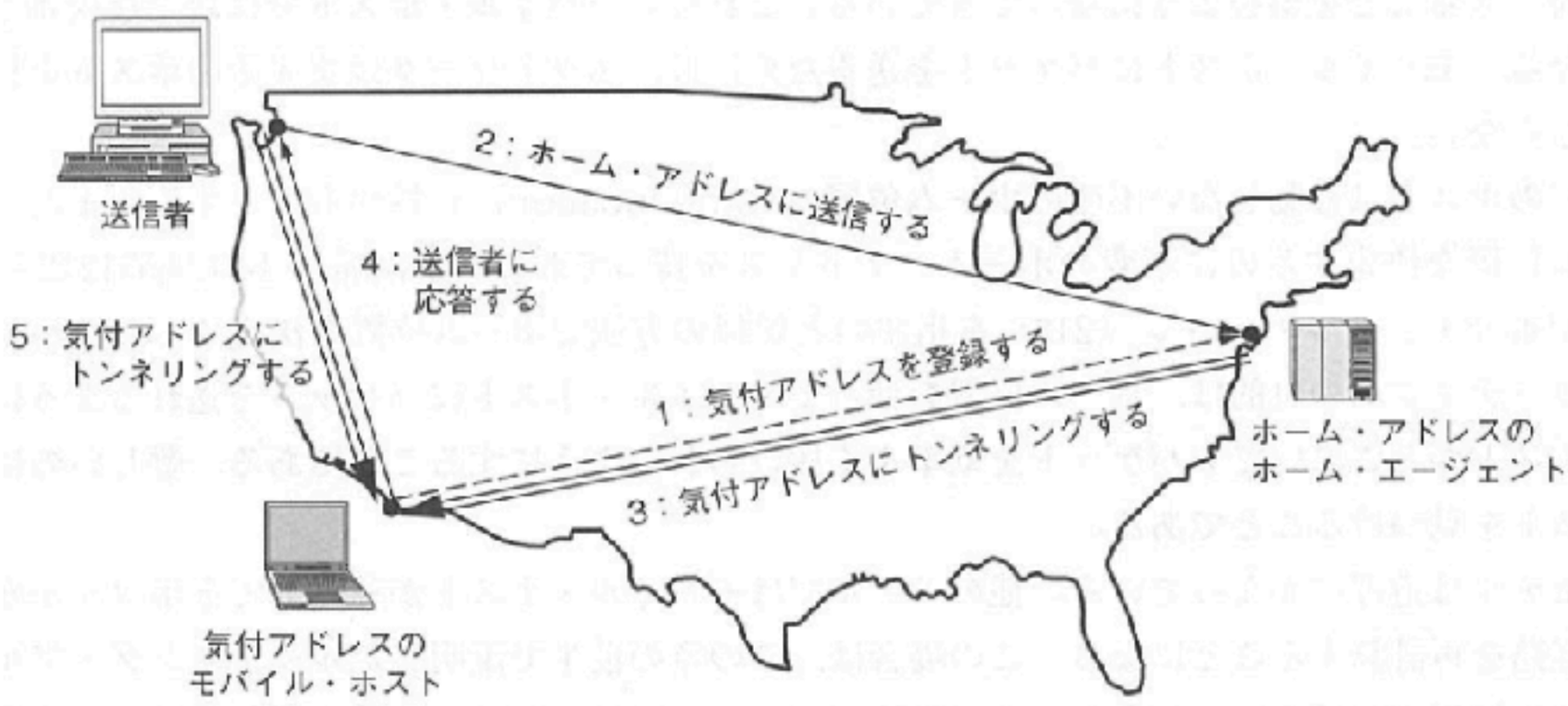


インターネットのマルチキャスト

クラスDのIPアドレス
224.0.0.0/24はマルチキャスト用に予約されている
224.0.0.1　：LAN上の全てのシステム
224.0.0.2　：LAN上の全てのルータ
224.0.0.5　：LAN上の全てのOSFPルータ
224.0.0.251：LAN上の全てのDNSサーバ

モバイル IP

1. 各モバイル・ホストはどこでもそのホームIPアドレスを使えなかればならない
2. 固定ホストに対するソフトウェアの変更は許されない
3. ルータ・ソフトウェアとテーブルに対する変更は許されない
4. モバイル・ホストに対する大部分のパケットは遠回りさせない
5. ホストがホームにあった場合、オーバーヘッドは発生させない



講義日程

		授業計画		課題
05/11	第９回	ネットワーク層１ ルーティング・輻輳制御	５章	ルーティングの種類を理解し 輻輳制御手法を説明できる
05/15	第１０回	ネットワーク層２ インターネットとサービス品質	５章	インターネットの制御プロトコルを理解し ネットワーク間の接続について説明できる
05/18	第１１回	トランスポート層１ トランスポート・プロトコルの要素	６章	誤り制御とフロー制御を理解し 輻輳制御について説明できる
05/22	第１２回	トランスポート層２ UDP と TCP	６章	TCP の信頼性を理解し TCP のコネクション管理を説明できる
05/25	第１３回	アプリケーション層 DNS, 電子メール, www	７章	DNS, 電子メール, www のしくみを理解し ストリーミング，P2P について説明できる
05/29	第１４回	ネットワークセキュリティ１ 対称鍵暗号，公開鍵暗号	８章	暗号アルゴリズムを理解し SHA-1,2 と RSA について説明できる
06/01	第１５回	ネットワークセキュリティ２ デジタル署名，認証プロトコル	８章	電子メール,Web のセキュリティ の脅威について把握できる

↑

期末試験