TCP/IP

情報通信ネットワーク特論
TCP/IP (3)

2004/04/21（WED）

渡邊　晃

担当：　鈴木秀和

参考文献

- マスタリングTCP/IP 入門編 [第3版]
  - 竹下隆史・村山公保
    荒井 透・苅田幸雄　共著
  - オーム社（2002）

流れ

- 第6章　TCPとUDP
  - TCPとUDP
  - ポート番号
  - TCPの目的と特徴
    - シーケンス番号と確認応答
    - 再送制御と重複制御
    - ウィンドウ制御
    - フロー制御
    - 輻輳制御
  - IPトンネリング
- 第7章　経路制御プロトコル
  - 静的/動的経路制御
  - 経路制御アルゴリズム
  - RIP（Routing Information Protocol）
  - OSPF（Open Shortest Path First）
- 第8章　アプリケーションプロトコル
  - DNS（Domain Name System）
  - その他のアプリケーションプロトコル

TCP/IP

第６章
TCPとUDP

Transport Layer（L4）

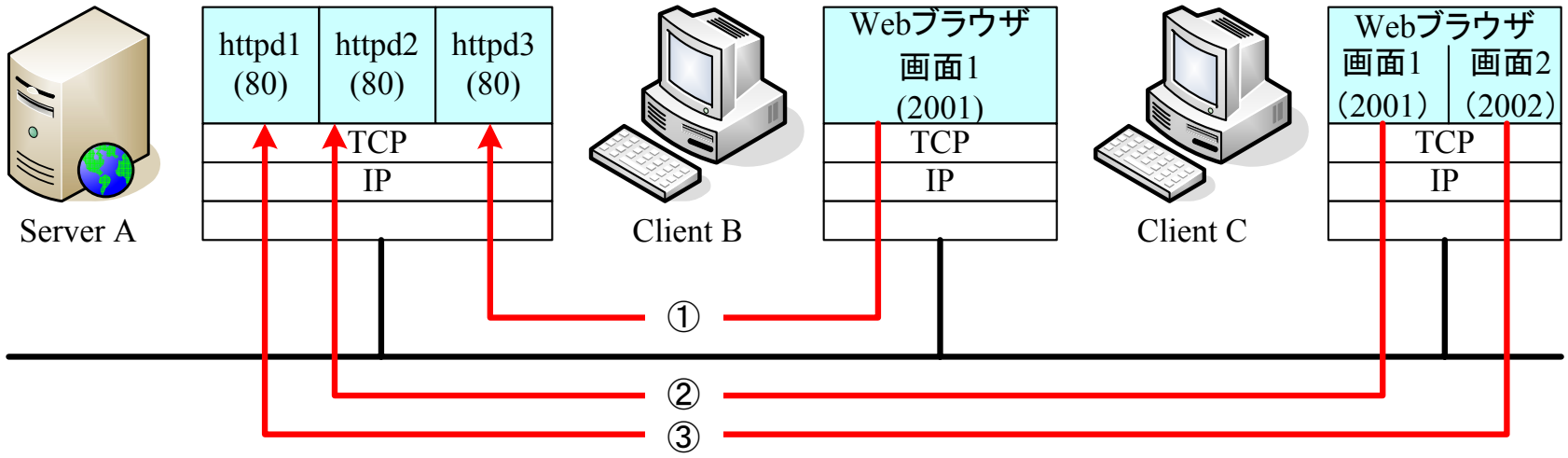
TCPとUDP

- TCP（Transmission Control Protocol）
  - コネクション指向，信頼性のあるストリーム型プロトコル
  - アプリケーションに信頼性を保証
  - ネットワークの利用効率を向上させる仕組み
    - 順序制御，再送制御，フロー制御，輻輳回避制御 etc…

- UDP（User Datagram Protocol）
  - コネクションレス指向，信頼性のないデータグラム型プロトコル
  - アプリケーションが完全に制御しなければならない
  - UDPに適した通信
    - 画像，音声，動画などの高速リアルタイム通信
    - マルチキャスト，ブロードキャスト

ポート番号

- 同一コンピュータ内で通信しているプログラムを識別
- 送信元/宛先IPアドレス，送信元/宛先ポート番号，プロトコル番号の5つで通信を識別



①	Client B	Server A	6	2001	80	Data
②	Client C	Server A	6	2001	80	Data
③	Client C	Server A	6	2002	80	Data

IPヘッダ：送信元IP，宛先IP，プロトコル番号

TCPヘッダ：送信元ポート番号，宛先ポート番号

ポート番号の決め方

- 標準で決められている番号
  - サーバが提供するアプリケーションの番号
    - Well-known Port Number　0～1023
    - 登録されたポート番号　　1024～49151

- ダイナミックな割り当て法
  - クライアントがサーバに要求する際に割り当てられる番号
  - OSがアプリケーションごとにポート番号を制御（重複管理）
    - ダイナミックポート番号　　49152～65535

- 多くのシステムではこれを無視して1024以上の未使用ポートが順番に割り当てられる

代表的なWell-known Port Number

	Port No.	Application
TCP	20	FTP [Default Data]
	21	FTP [Control]
	23	Telnet
	25	SMTP
	80	HTTP
	110	POP3
	443	HTTPS
UDP	53	DNS
	67	DHCP [Server]
	68	DHCP [Client]
	161	SNMP
	520	RIP

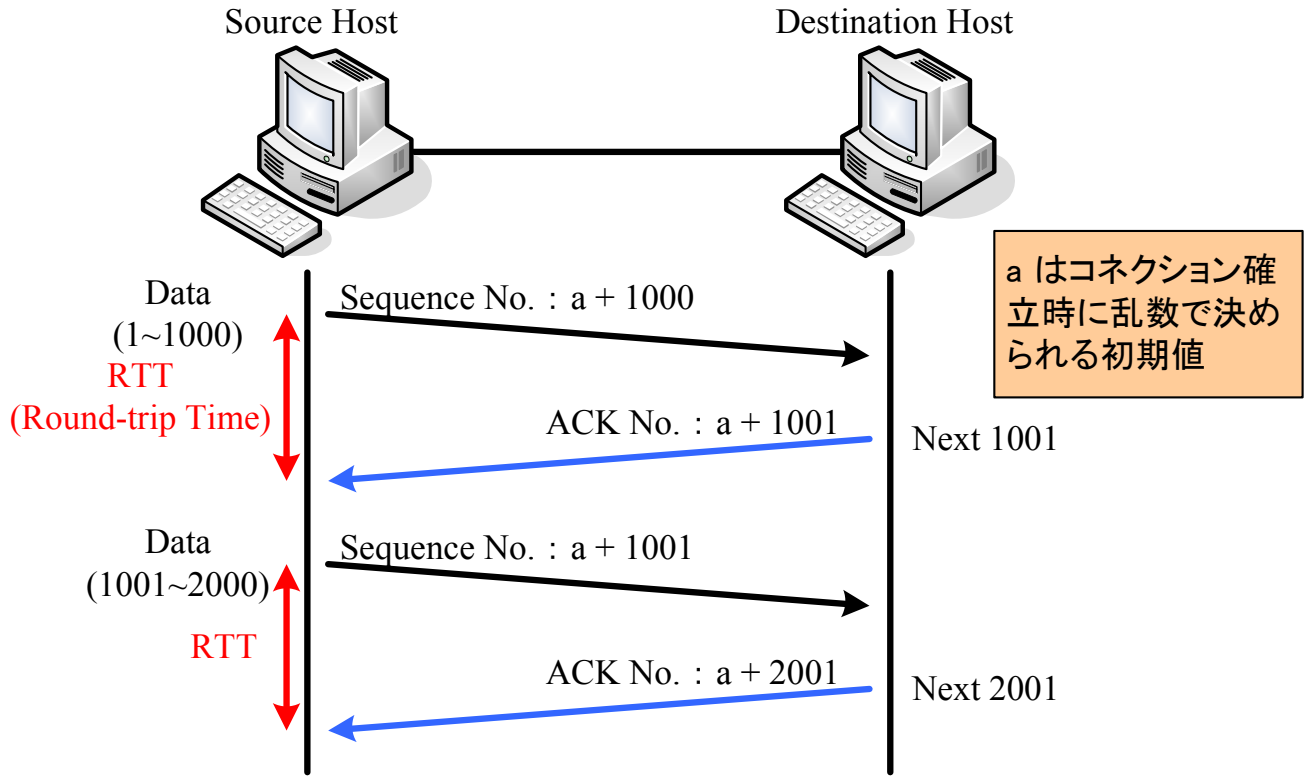
TCPの目的と特徴

- 通信の際に考慮しなければならない問題
  - データの破損やパケットの喪失
  - パケットの重複，順序の入れ替わり

- 信頼性を実現するための機能
  - チェックサム　（TCPヘッダとデータの信頼性を保証）
  - シーケンス番号　（パケットの順序制御）
  - 確認応答　（パケットが宛先に届いたことの確認）
  - 再送制御　（確認応答喪失の場合の制御）
  - コネクション管理　（相手の状態確認と通信準備）
  - ウィンドウ制御　（通信性能を向上させる制御）
  - 遅延確認応答　（応答を故意に遅らせる方法）
  - ピギーバック　（データ送信で確認応答を兼ねる方法）

シーケンス番号と確認応答

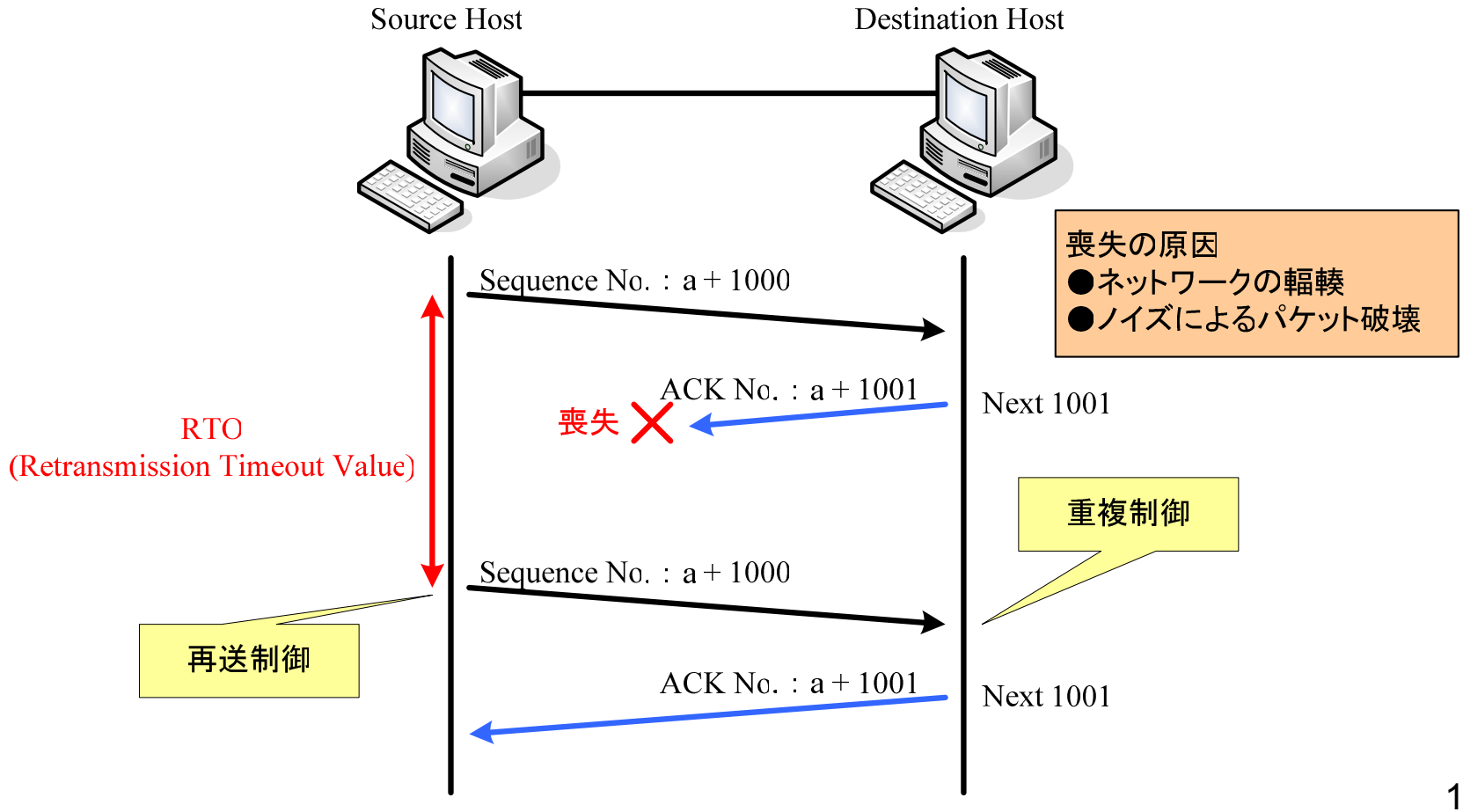
- 送信データが受信ホストに到達後
  - ACK（Positive Acknowledgement）：正しく受信した際の応答
  - NACK（Negative Acknowledgement）：ACKの逆



RTTが大きい＝スループットが悪い

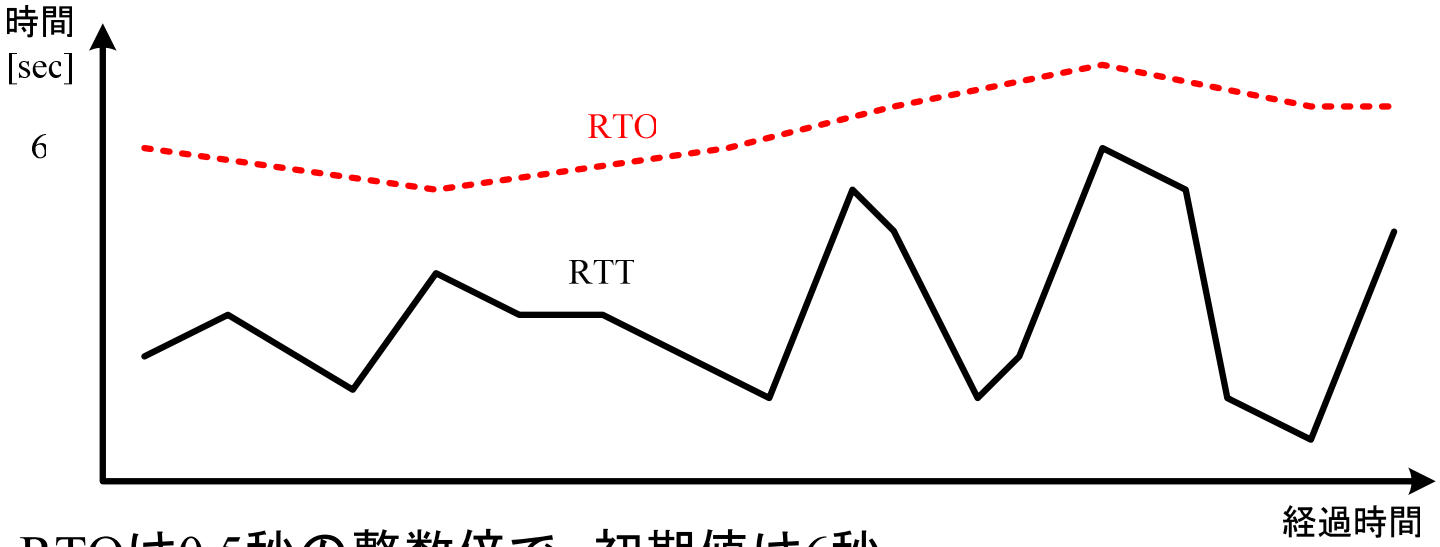
再送制御と重複制御

- 再送タイムアウト時間（RTO）
  - 再送せずに確認応答の到着を待つ時間
- 重複制御
  - 重複して受信したパケットの破棄



RTOの決定

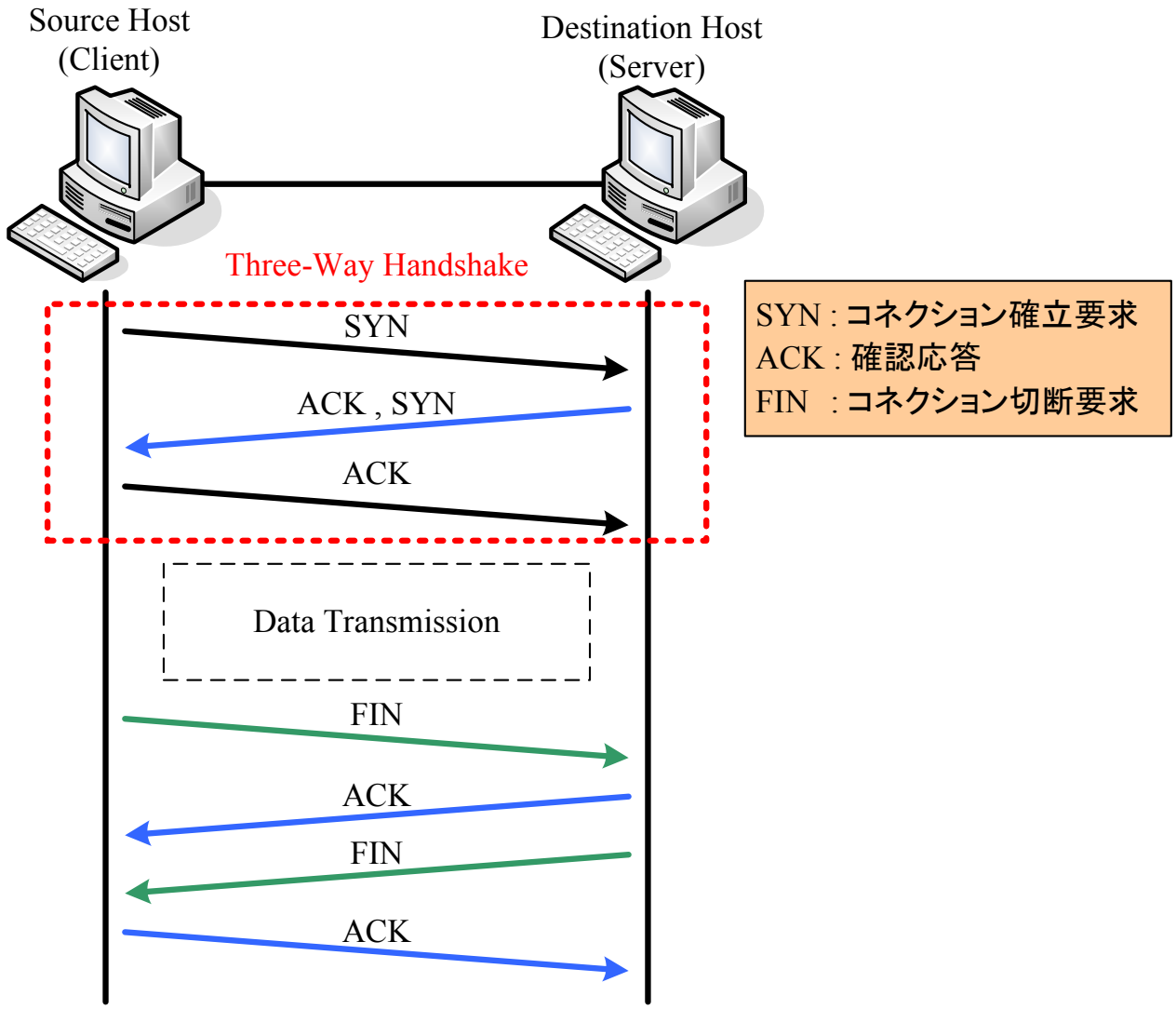
- 理想は「この時間を経過したらACKが帰ってくることはない」という確率が最も高くなる時間
  - ネットワークの距離や混雑度により適正値は変化
- パケット送信するたびにRTTとその揺らぎを計測
  - 揺らぎ（ジッタ；Jitter）：RTTの分散
  - RTO＝（RTTの平均）＋（Jitter×k）



- RTOは0.5秒の整数倍で，初期値は6秒
- リトライアウトすると，ネットワークや相手ホストに異常が発生していると見なして，強制的にコネクションを切断

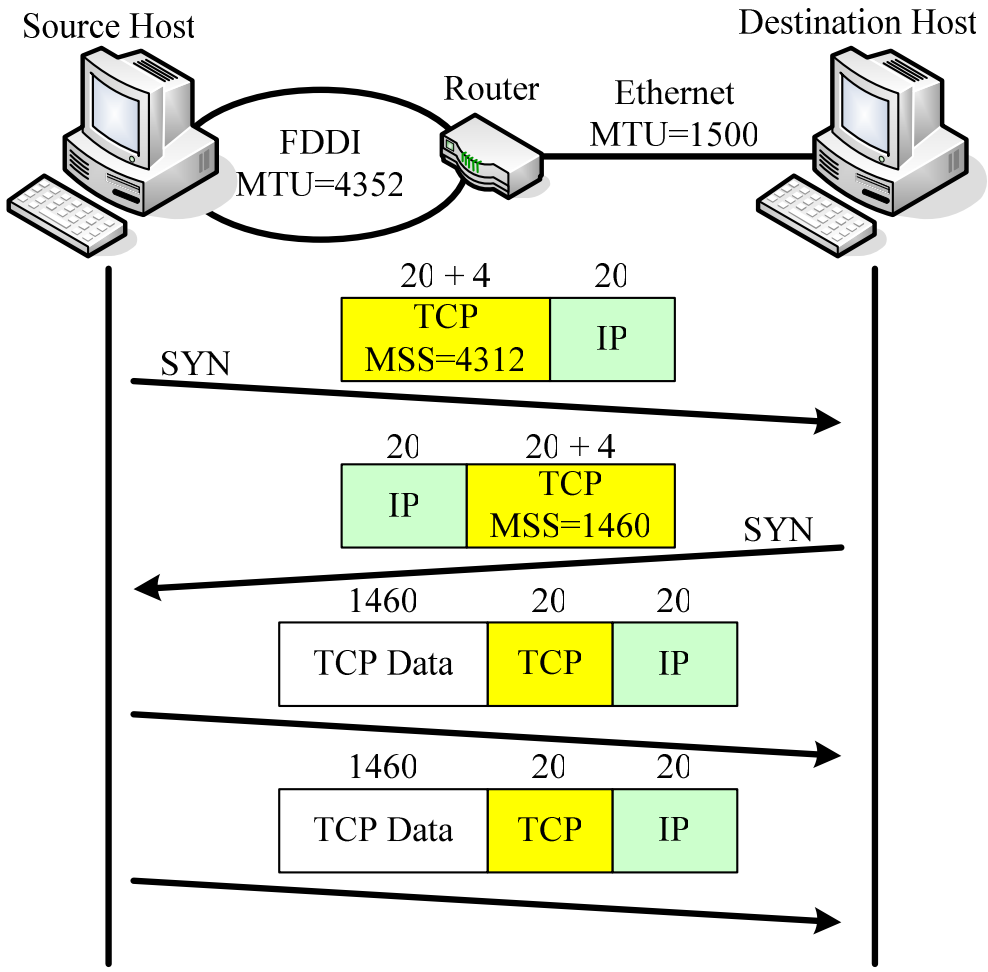
コネクション管理

- TCPは通信に先立ちコネクションを確立
  - 無駄な転送を行わない
  - シーケンス番号の初期値の決定



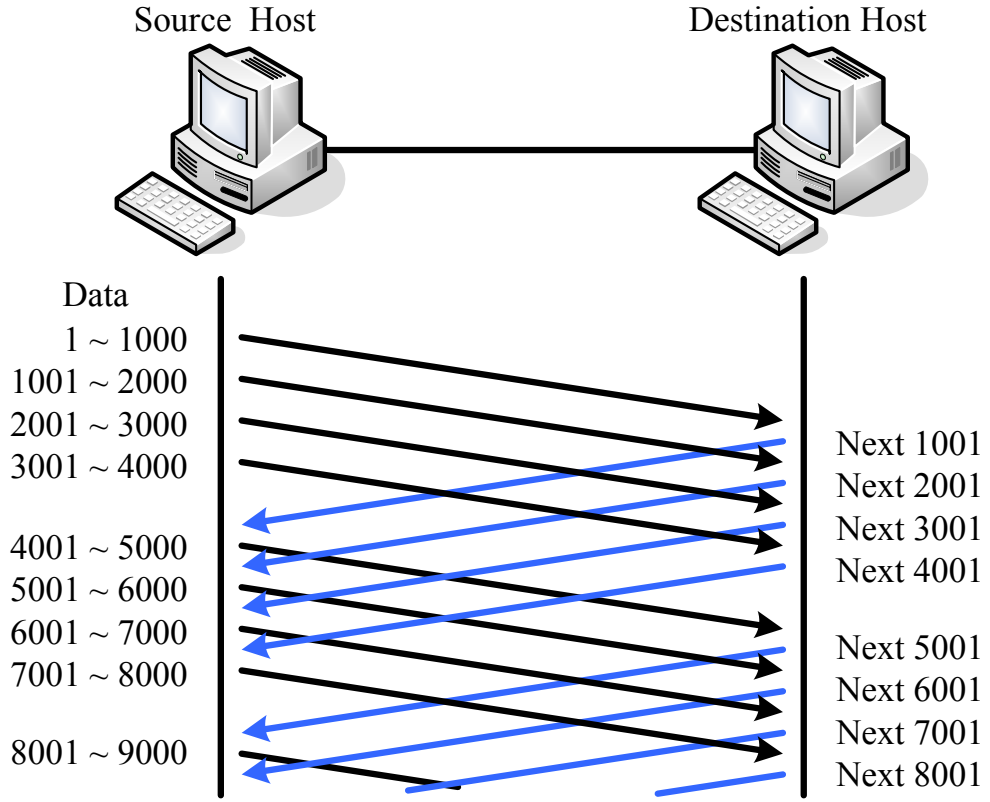
セグメント単位でデータ送信

- 最大セグメント長（MSS；Maximum Segment Size）
  - 通信を行うデータ単位
  - 理想はIPで分割処理されない最大の大きさ

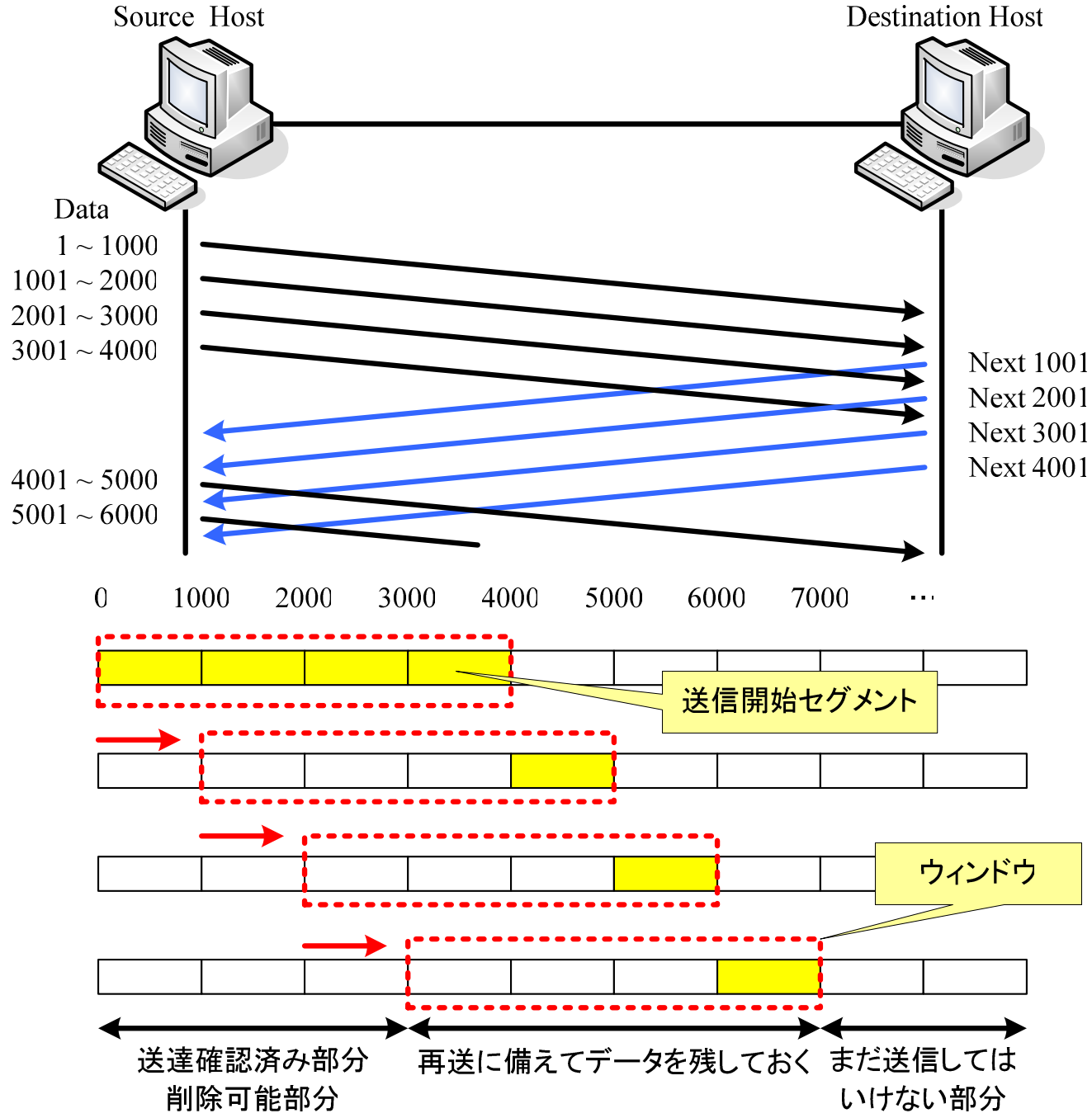


ウィンドウ制御による速度向上

- 1セグメント単位で送信するとRTTが長くなる
- ウィンドウ制御
  - RTTが長くなっても性能が低下しないように制御
  - ウィンドウサイズを設定
    - 確認応答を待たずに送信できるデータの大きさ
  - 大きな受信バッファにより複数セグメントを並列的に処理

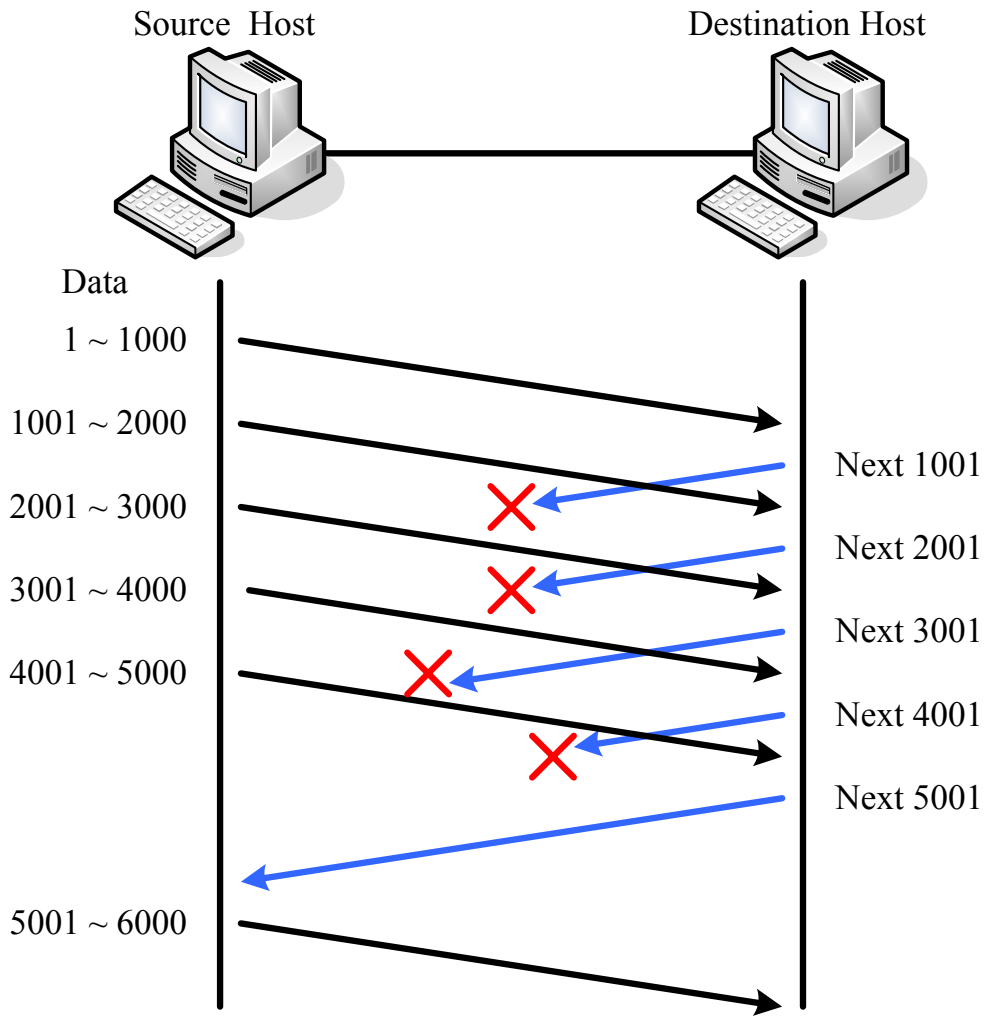


スライディングウィンドウ方式



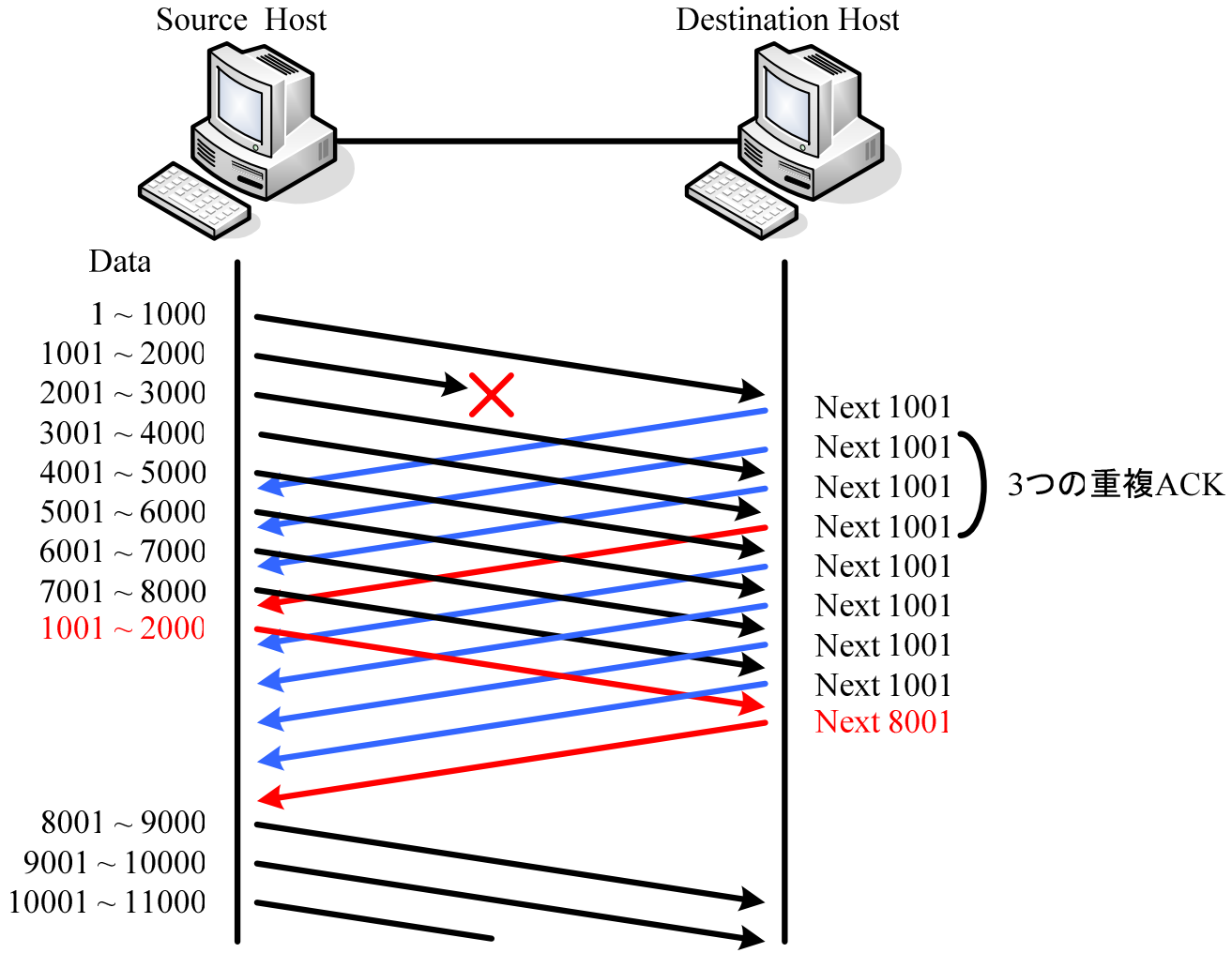
ウィンドウ制御による通信障害対策

- ACKが不着の場合
  - 最後のACKが返ってきたらウィンドウをスライド



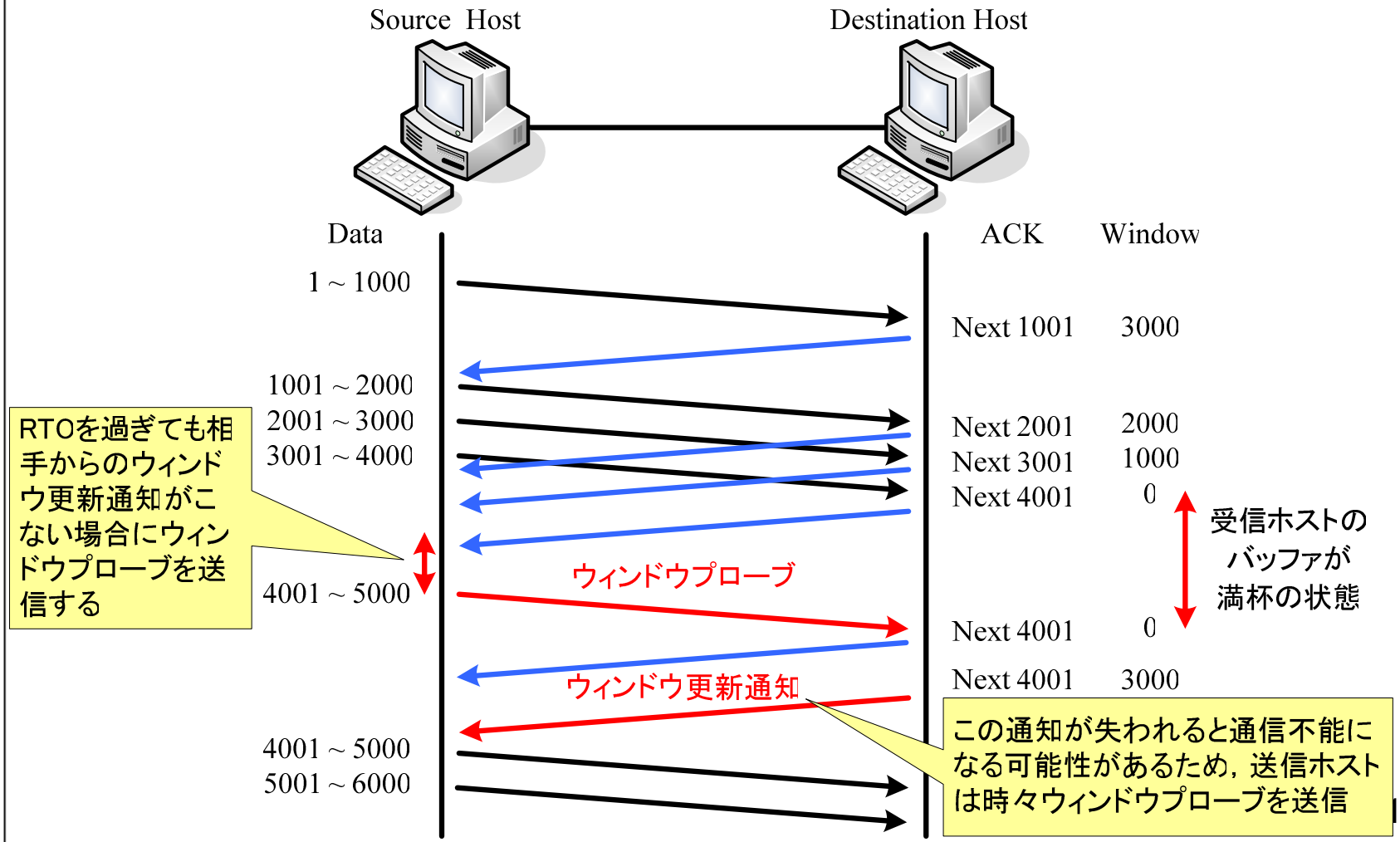
ウィンドウ制御による通信障害対策

- 送信元からのデータが不着の場合
  - 高速再送制御（Fast Retrans-mission）
    - 一度受信したACKと同じACKをさらに3回受信したら再送
    - タイムアウトによる再送よりも高速



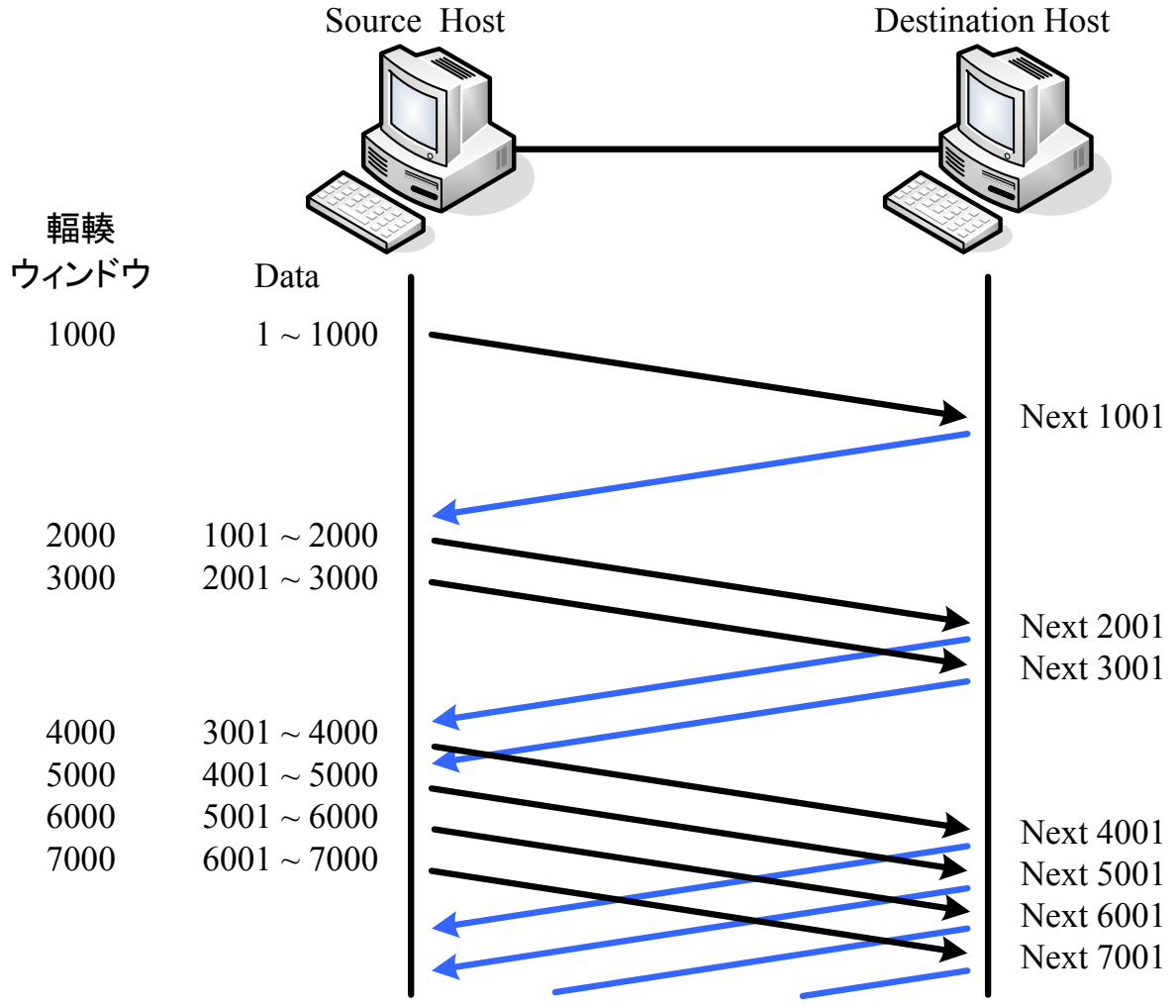
フロー制御（流量制御）

- フロー制御（流量制御）
  - 受信側バッファがあふれそうになると，ウィンドウサイズを小さくして送信側の送信量を抑制
  - ウィンドウサイズの大きさは受信ホストが決定する

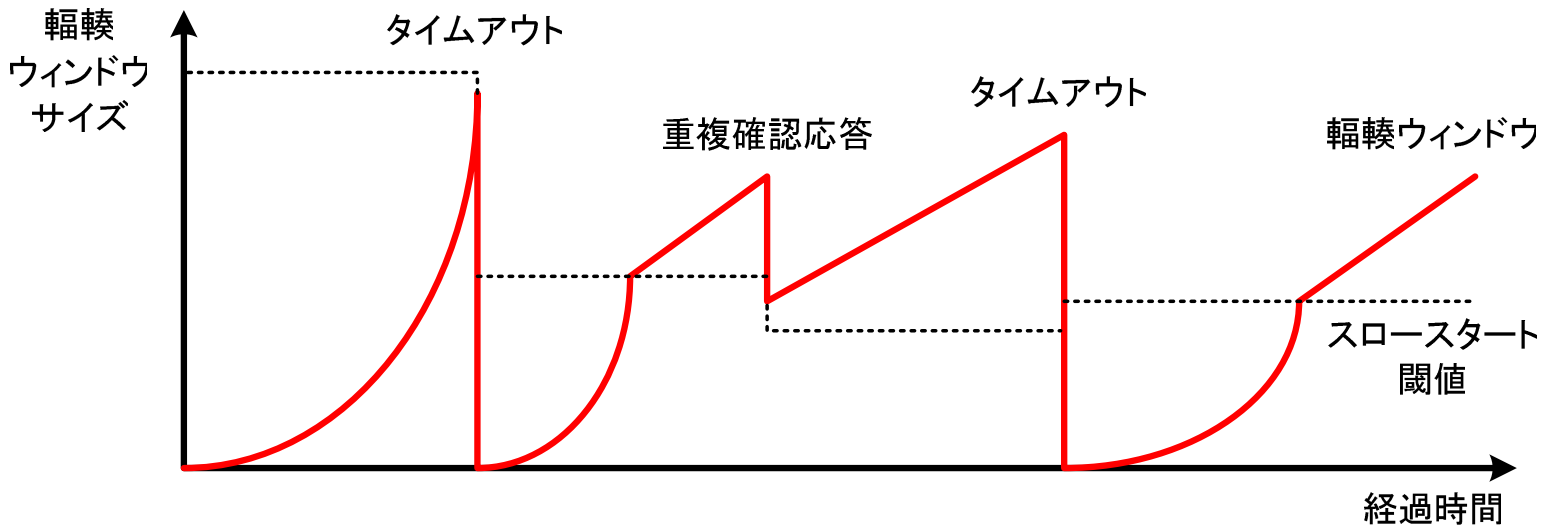


輻輳制御

- スロースタートによりデータの送信量を制御
  - ACKを受信するたびに1MSSずつ輻輳ウィンドウを拡大
  - 輻輳ウィンドウと通知されたウィンドウを比較して小さい方の値だけパケットを送信



輻輳ウィンドウの変化

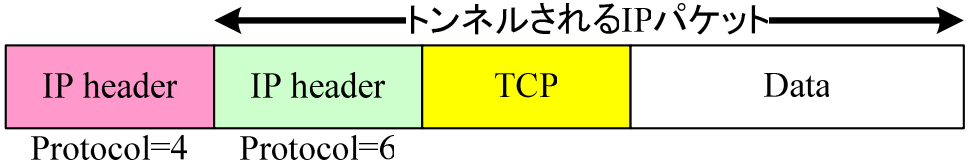


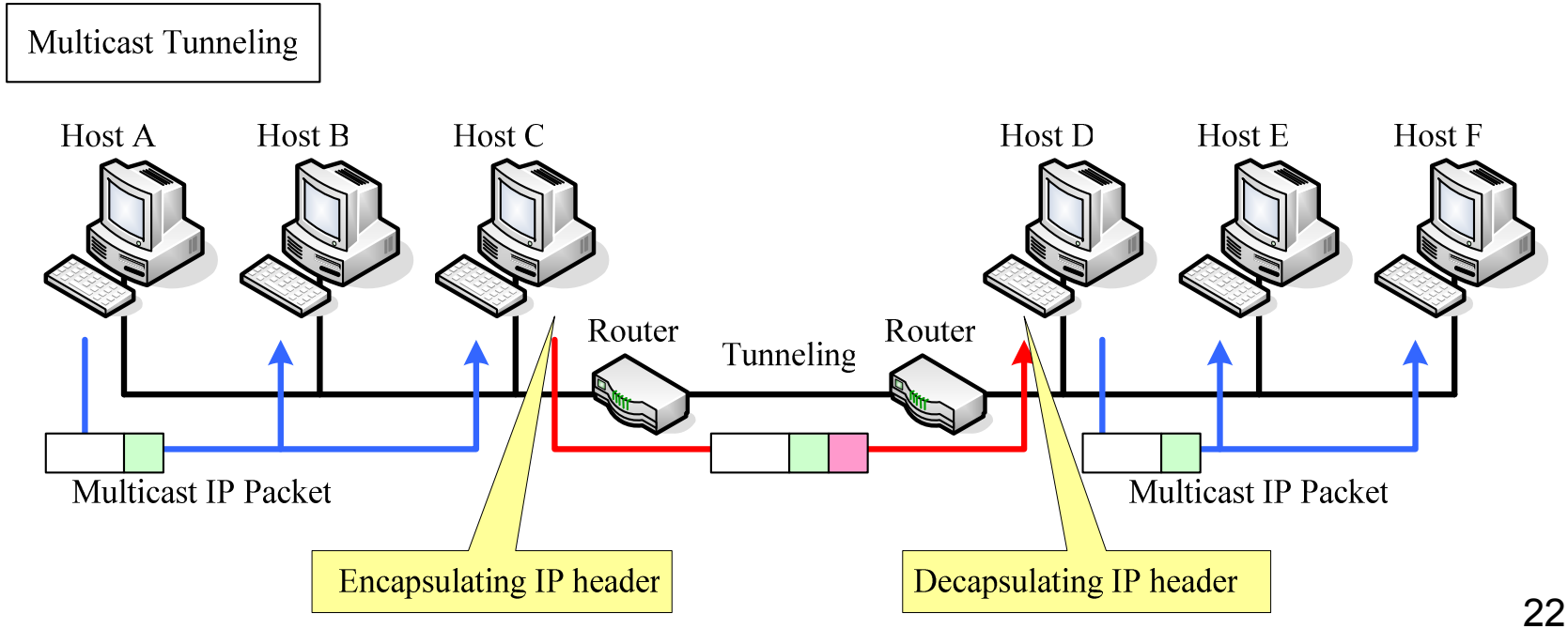
- 最初およびタイムアウト時はスロースタート
  - タイムアウトになるまでは指数関数的に増加
  - スロースタート閾値を超えると直線的に増加
- タイムアウトによる再送制御
  →スロースタート＝輻輳ウィンドウ/2
- 重複確認応答（高速再送制御）
  →スロースタート＝輻輳ウィンドウ/2
  →ウィンドウサイズ＝スロースタート+3セグメント

IPトンネリング

- IPパケットをIPヘッダでカプセル化した通信
  - 同一データリンク内でのみ可能だった通信が，ルータを越えて行える
  - 通常の経路制御を無視したパケット通信が可能

（例）IPv6 over IPv4, L2TP, IPsec, Mobile IP, etc





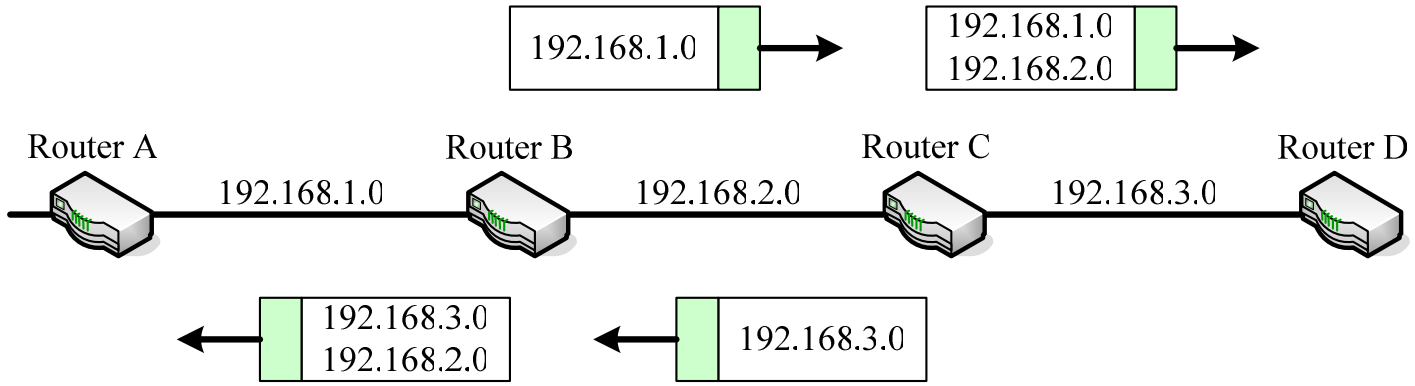
TCP/IP

第7章
経路制御プロトコル

Routing Protocol

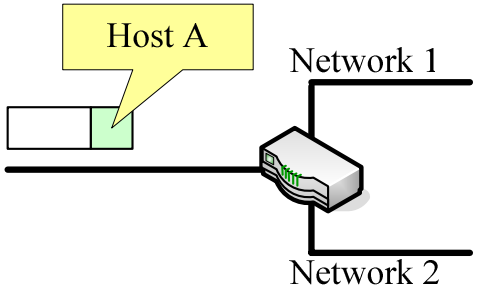
静的と動的な経路制御

- 静的経路制御（Static Routing）
  - ルータ，ホストに固定的に経路情報を設定
  - 管理者の負担増
    - ネットワーク上全てのルータを設定
    - 新しいネットワーク追加時は全てのルータを再設定
    - ネットワーク障害時も手動で再設定
- 動的経路制御（Dynamic Routing）
  - ルーティングプロトコルにより自動的に経路制御を設定
  - プロトコルの種類によっては初期設定が複雑
    - 新しいネットワーク追加時は該当ルータのみを再設定
    - ネットワーク障害時も自動で再設定



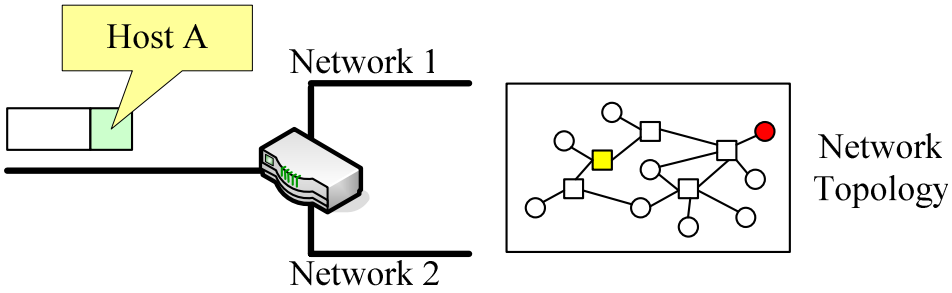
経路制御アルゴリズム

- 距離ベクトル型（Distance-Vector）
  - ネットワークの方向と距離から経路制御表を作成
  - ネットワーク構造が複雑
    →経路の収束が遅い，経路にループが生じやすい



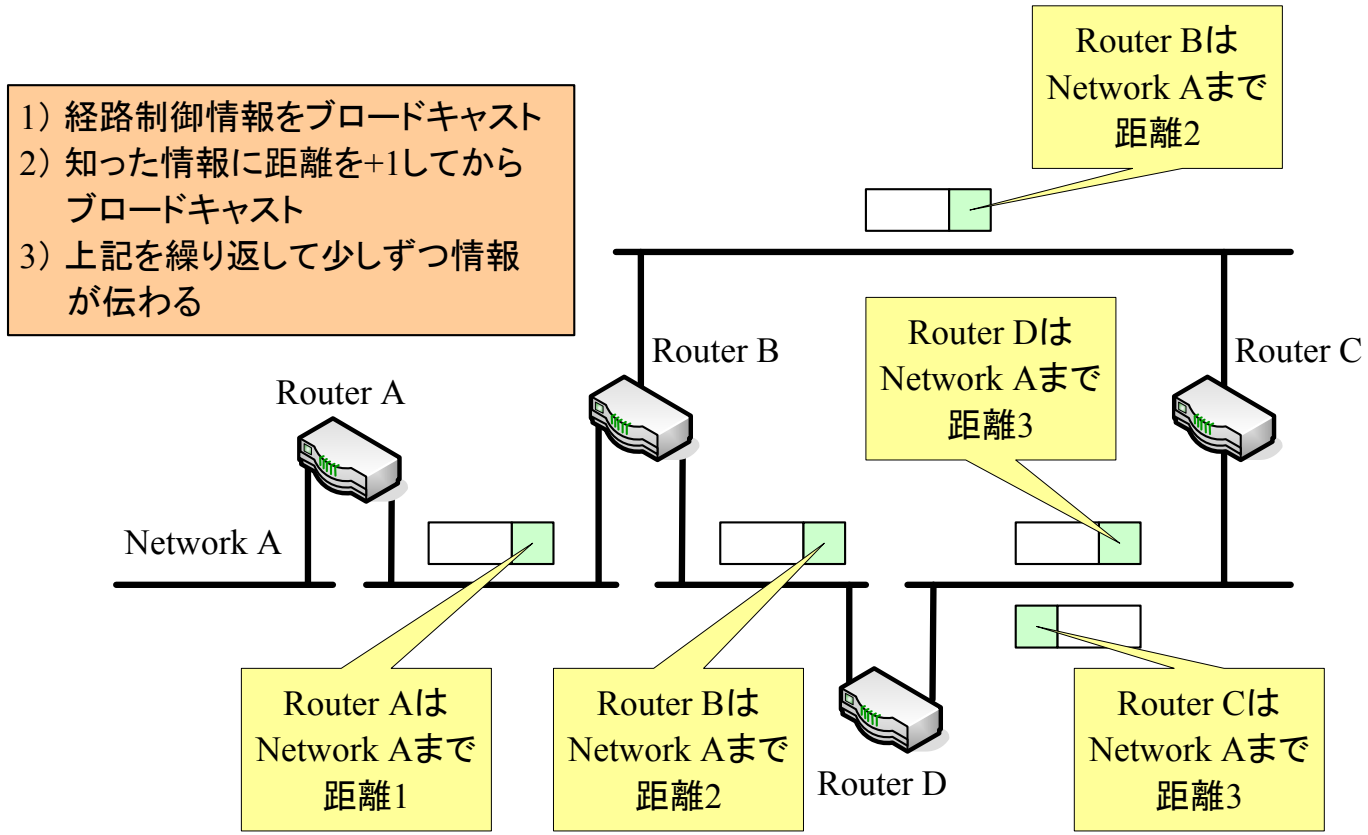
端末	方向	距離
Host A	Network 1	3
Host A	Network 2	8

- リンク状態型（Link-State）
  - ネットワーク全体の接続状態を理解して経路制御表を生成
  - 各ルータが保持する情報が同じ
    →情報が正しいものか確認するのが困難



RIP（Routing Information Protocol）

- 距離ベクトル型ルーティングプロトコル
  - 経路制御情報を定期的にブロードキャスト
    - 送信間隔：30秒
    - 6回（180秒）待っても来ない場合は接続が切れたと判断



経路制御表の作成方法(RIP)

- ルータ間の情報交換により距離ベクトルDB作成
- 距離(ホップ数)が小さい経路から経路制御表を作成

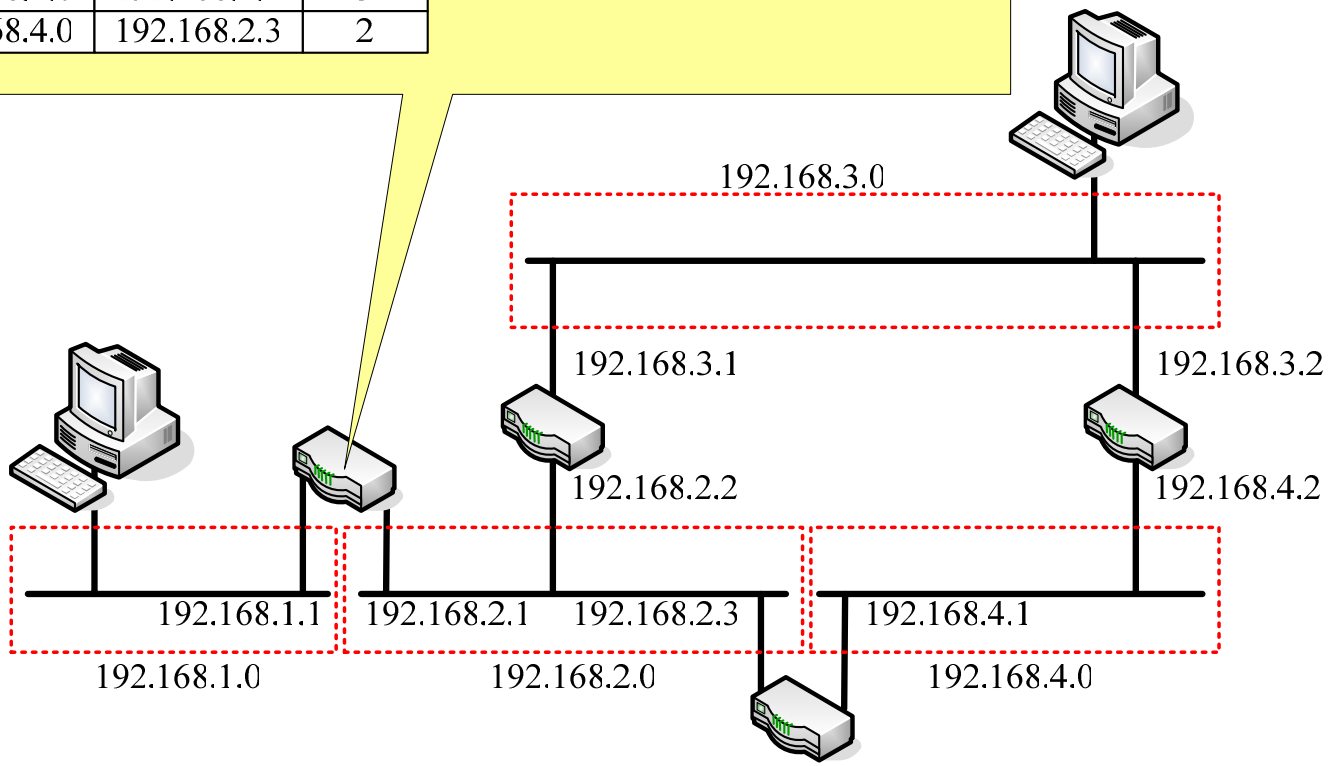
距離ベクトルデータベース

IPアドレス	方向	距離
192.168.1.0	192.168.1.1	1
192.168.2.0	192.168.2.1	1
192.168.3.0	192.168.2.2	2
192.168.3.0	192.168.2.3	3
192.168.4.0	192.168.2.2	3
192.168.4.0	192.168.2.3	2

→

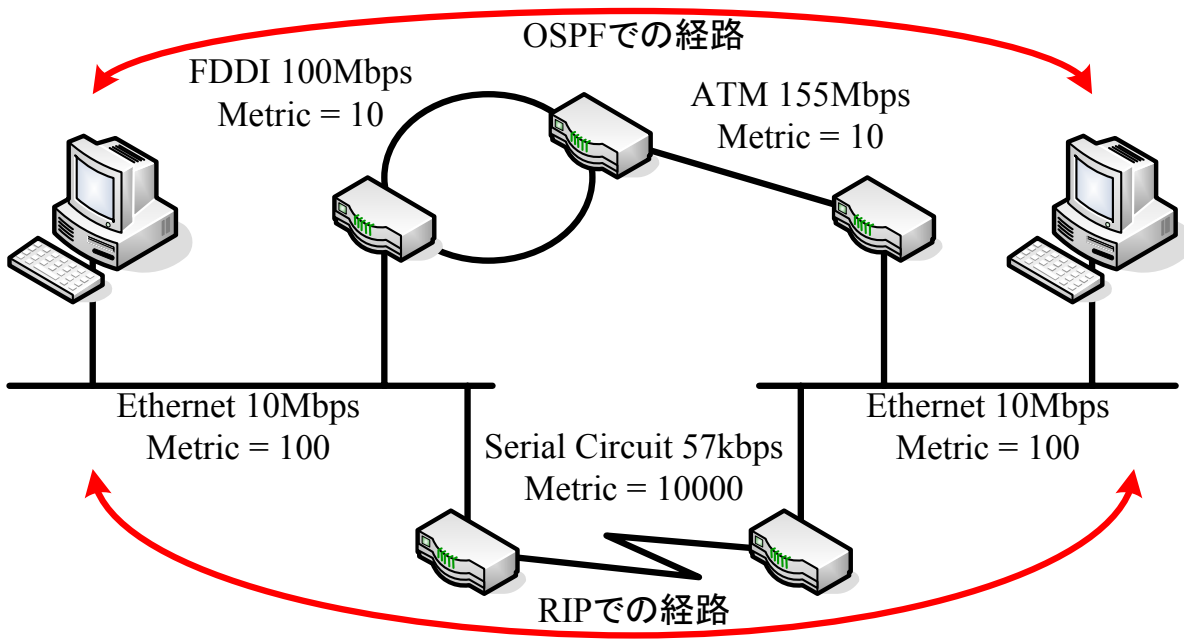
ルーティングテーブル

IPアドレス	次のルータ
192.168.1.0	192.168.1.1
192.168.2.0	192.168.2.1
192.168.3.0	192.168.2.2
192.168.4.0	192.168.2.3



OSPF（Open Shortest Path First）

- リンク状態型ルーティングプロトコル
  - 5つの制御パケットにより経路の確認・更新など行う
    - Hello Packet, Database Description Packet, Link State Request Packet, Link State Update Packet, Link State ACK Packet
  - Helloパケットで接続確認
    - 送信間隔：10秒
    - 4回（40秒）待っても来ない場合は接続が切れたと判断
- 各リンクのメトリックが小さくなるように経路制御



経路制御表の作成方法(OSPF)

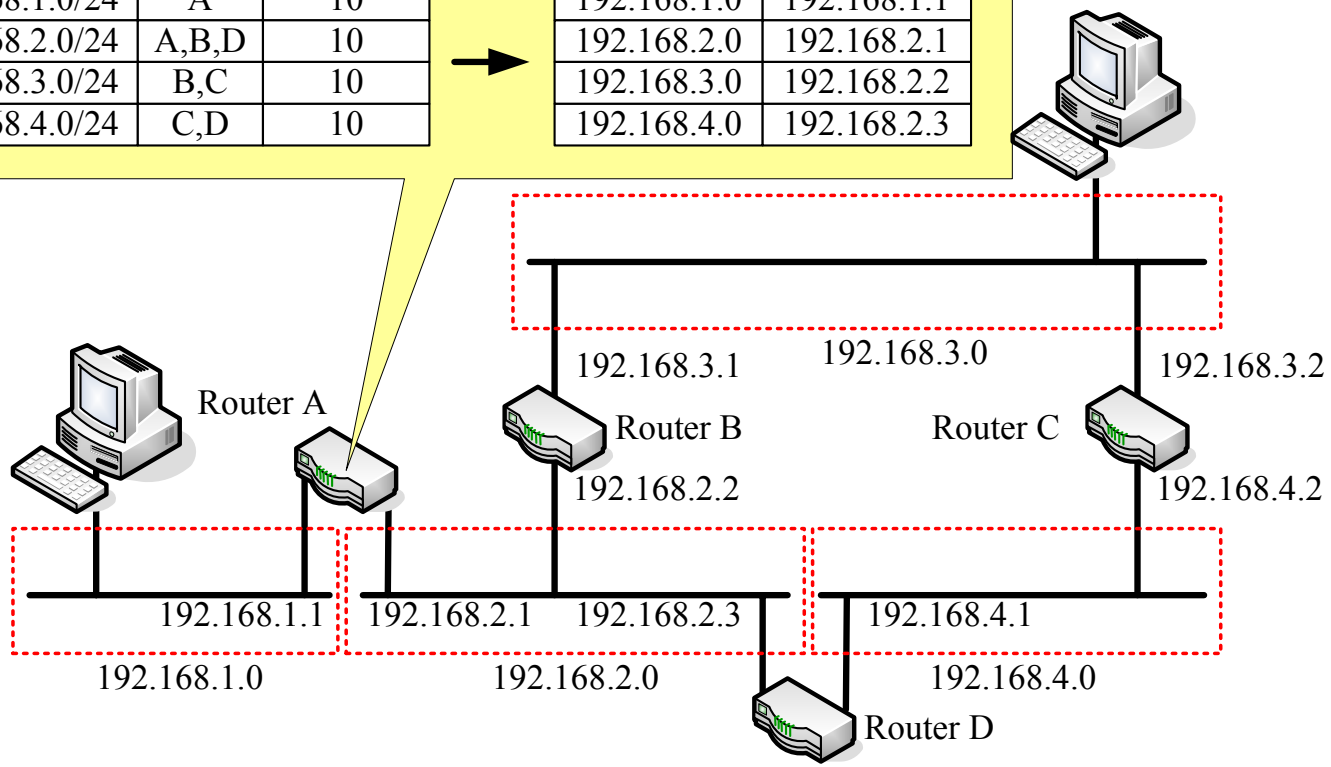
- 各ルータはOSPFによりリンク状態DBを作成
- DBを元にダイクストラ法により経路制御表を作成
- ネットワーク規模が大きいと最短経路の算出時間大
  - エリアを定義して細かく管理することで負担を軽減

リンク状態データベース

ネットワーク	ルータ	メトリック
192.168.1.0/24	A	10
192.168.2.0/24	A,B,D	10
192.168.3.0/24	B,C	10
192.168.4.0/24	C,D	10

ルーティングテーブル

IPアドレス	次のルータ
192.168.1.0	192.168.1.1
192.168.2.0	192.168.2.1
192.168.3.0	192.168.2.2
192.168.4.0	192.168.2.3



TCP/IP

第８章
アプリケーションプロトコル

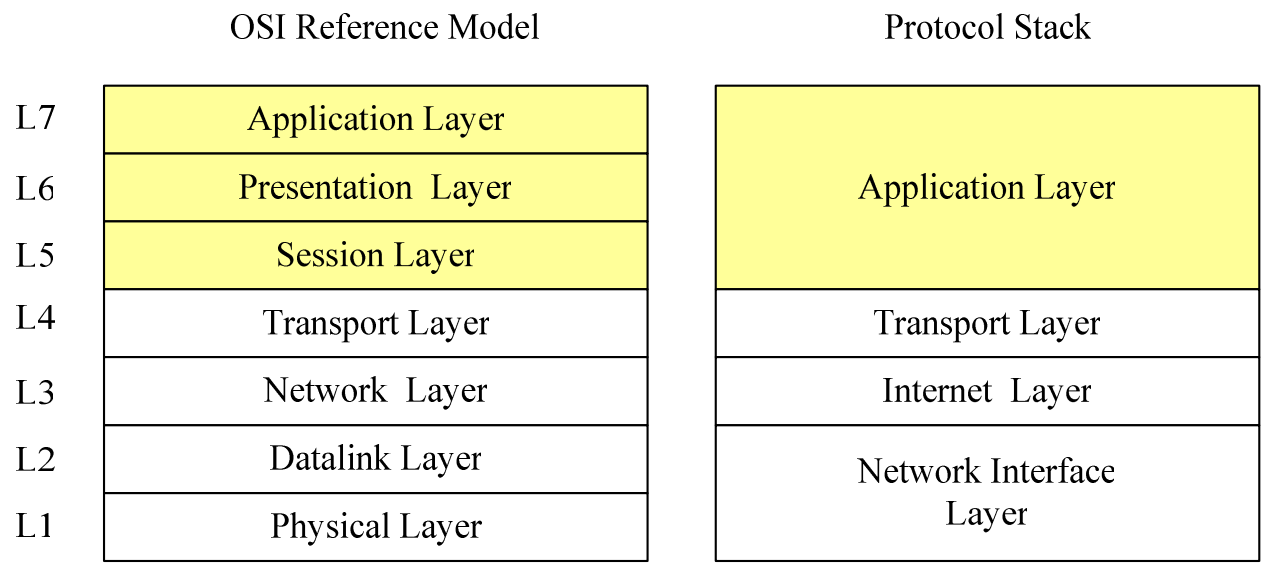
Application Layer（L7）

Presentation Layer（L6）

Session Layer（L5）

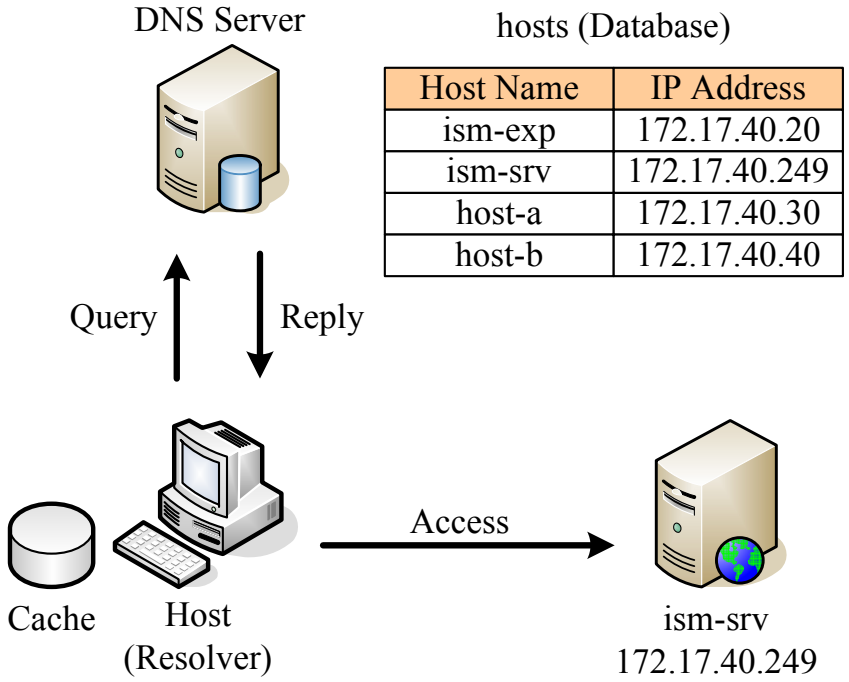
アプリケーションプロトコル概要

- アプリケーションプロトコル
  - 実用的なアプリケーションを実現するために作成
  - 下位層を使ってどのような通信を行うかを決めた仕様
- ネットワークプロトコルの階層化
  - アプリケーション開発者はアプリケーションプロトコルの決定とプログラムの開発だけに専念
  - 相手コンピュータまでのパケット送信などは考えなくてよい



DNS（Domain Name System）

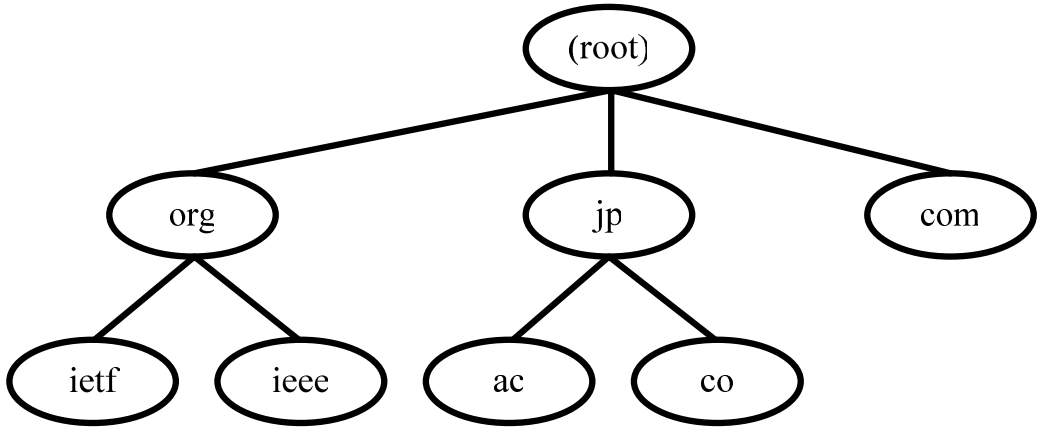
- DNS
  - ネットワーク上のホスト名とIPアドレスを対応させるシステム
    - 正引き（Aレコード）：　　ホスト名→IPアドレス
    - 逆引き（PTRレコード）：　IPアドレス→ホスト名
  - インターネットに広がる分散データベース



覚えにくいIPアドレスではなく簡単なホスト名を利用

ドメイン名の構造

- ドメイン名
  - ホスト名や組織名を識別するための階層構造を持つ名前
  - 複数の英字が「.」で繋がれた構造



meijo-u.ac.jp

名城大学
固有のドメイン名

大学　日本

- FQDN（Fully Qualified Domain Name）
  - ホスト名に続けてドメイン名を記述した形式
    - www.meijo-u.ac.jp
    - www-is.meijo-u.ac.jp
    - taro.joho.meijo-u.ac.jp
  - 各組織単位で自由にホスト名を付けることが可能

その他のアプリケーションプロトコル

- WWW（World Wide Web）
  - HTTP（HyperText Transfer Protocol）
    - WWWの情報の転送等の操作の定義
    - 要求コマンド“GET”によりHTMLデータを取得
- 電子メール
  - SMTP（Simple Mail Transfer Protocol）
    - メールの配送
  - POP（Post Office Protocol）
  - IMAP（Internet Message Access Protocol）
    - メールの受信
- 遠隔ログイン（リモートログイン）
  - TELNET
- ファイル転送
  - FTP（File Transfer Protocol）

TCP/IP

情報通信ネットワーク特論

TCP/IP 基礎　終了

次はMobile IPの基礎編