

コンピュータネットワーク
第6回 TCP/IP Protocol Suite (2/2)
TCPとUDP

静岡理科大学
情報学部 コンピュータシステム学科
幸谷 智紀

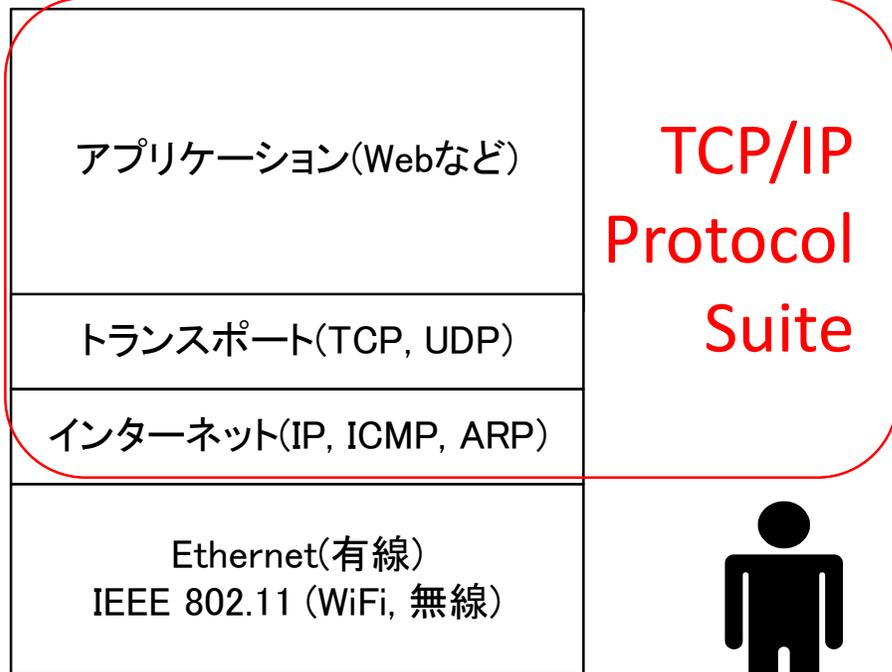
<https://na-inet.jp/compnet/>

本日の内容

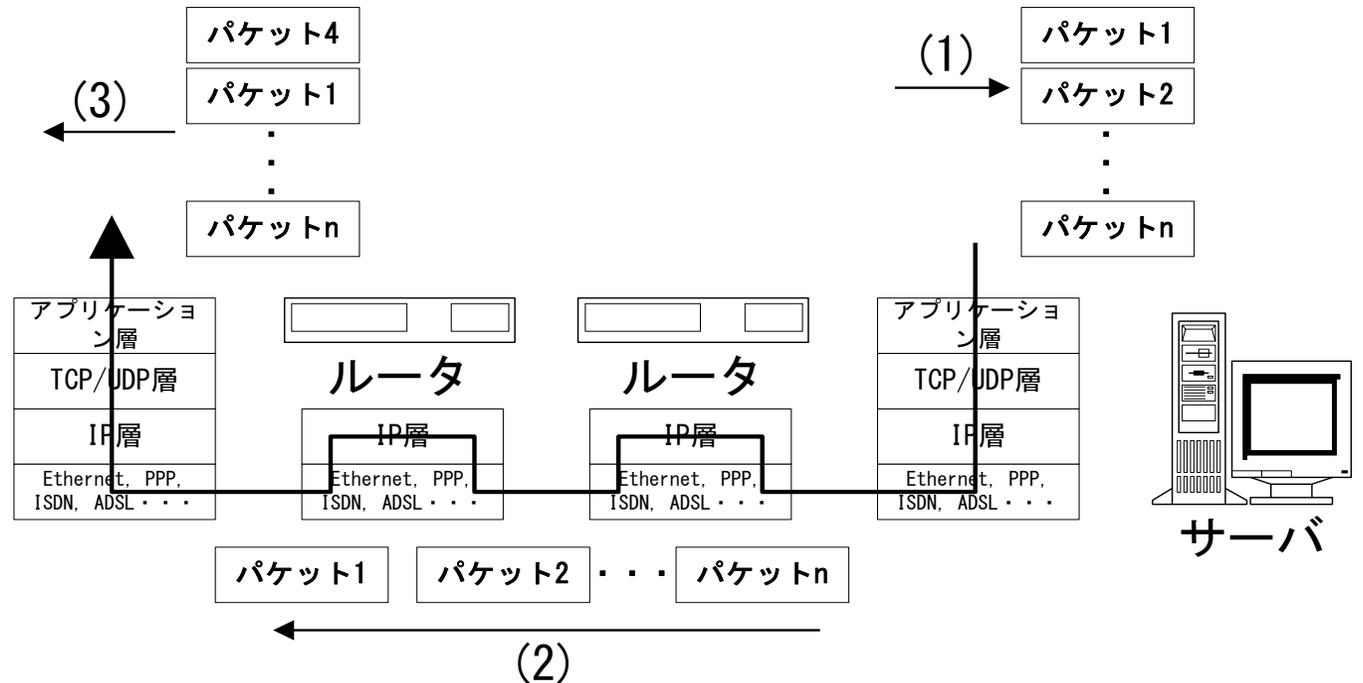
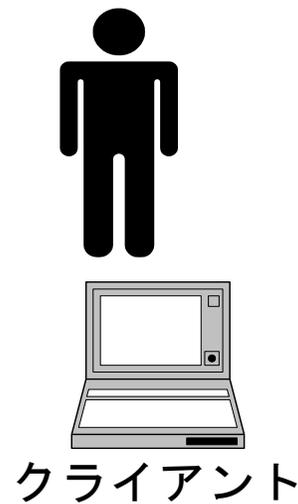
- IPアドレス管理
 - サブネット分割
 - DHCP
- IPヘッダの構造
 - IPv4ヘッダとIPv6ヘッダ
- TCPとUDP
- TCPの機能
 - コネクション維持の仕組み
 - 輻輳制御

(復習) TCP/IP Protocol Suite

TCP/IP + Ethernet, 802.11
(WiFi)



- IP層 . . . IP Addressing, Routing等を担当
- TCP/UDP層 . . . コネクションの維持, 誤り制御, フロー制御(輻輳制御)を行う。
- アプリケーション層 . . . HTTP, HTTPS, FTP, NTP...



サブネット分割

192.168.0.0/16などのIPアドレスグループを，ネットマスク(プレフィックス長)を長くすることによって，複数のIPアドレスグループに分割すること。

- 2分割・・・192.168.0.0/17, 192.168.128.0/17
- 4分割・・・192.168.0.0/18, 192.168.64.0/18, 192.168.128.0/18, 192.168.192.0/18
- 8分割・・・192.168.0.0/19, 192.168.32.0/19, 192.168.64.0/19, 192.168.96.0/19, 192.168.128.0/19, 192.168.160.0/19, 192.168.192.0/19, 192.168.224.0/19
-

→分割したサブネット毎に最低一つ以上のゲートウェイ(デフォルトゲートウェイ)が必要になる。

→LANの単位ごとに何台のマシンが必要になるかを事前に把握しておくこと。
最大接続数+ α を確保できるサブネット分割でなければならない

IPアドレス管理

- 静的→手動で設定
- 動的→DHCP(Dynamic Host Configuration Protocol)で実施
 - 自動的にIPアドレス(+ネットマスク+デフォルトゲートウェイ)の設定を行う
 - MACアドレスのチェックを行うか否か
 - MACアドレスに固定のIPアドレスを割り当て
 - MACアドレスに場所に応じたIPアドレスを割り当て

DHCP

1. EthernetからのブロードキャストによってDHCPサーバを発見する
2. DHCPサーバはクライアントに応答を返す
3. クライアントがDHCPサーバにIPアドレス(+ネットマスク+デフォルトゲートウェイ他)の要求を行う
4. DHCPサーバがクライアントに要求された情報を返す
5. クライアントが必要な設定を行う

Aterm WG1800HP(家庭用Wi-Fiルータ)のDHCP設定例



• ルータの役割

1. DHCPサーバ・・・プライベートIPアドレスで割り振るのが普通
2. NAT・・・グローバルIPアドレス（外側口）とプライベートIPアドレス(LAN側)とのIPアドレスの付け替えをパケット単位で行う

トップページ > 詳細設定 > IPv4LAN側設定

IPv4LAN側設定

ⓘ ご注意ください

本項目の設定値を間違えた場合は、通信ができなくなる可能性があります。通常は、初期値のまま使用してください

設定変更は即時に有効となります。[設定] ボタンをクリックしたあと、本商品にアクセスできなくなる場合があります。ブラウザを一度終了し、接続する端末と本商品の設定をあわせたと、WWWブラウザを開きなおしてください。

また、[保存] ボタンをクリックするまでは設定内容が保存されませんので、[保存] ボタンをクリックして設定内容

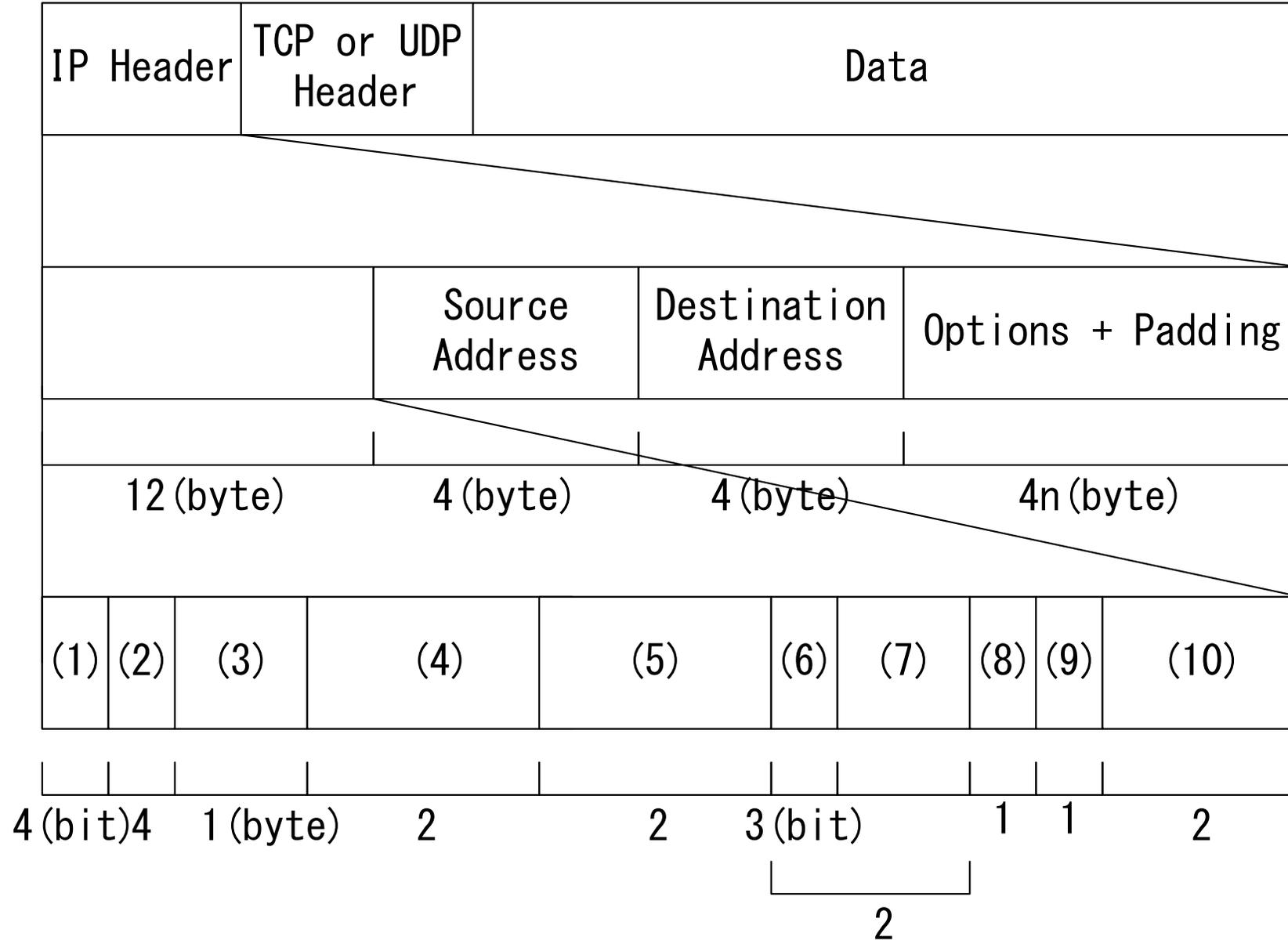
IPアドレス/ネットマスク ?

IPアドレス/ネットマスク(ビット指定) ? /

DHCPサーバ ?

DHCPサーバ機能 ?	<input checked="" type="checkbox"/> 使用する
リースタイム(時間) ?	<input type="text" value="24"/>
アドレス割当パターン ?	手動設定 ▾
割当先頭アドレス ?	<input type="text" value="192.168.1.128"/>
割当数 ?	<input type="text" value="32"/>
WINSサーバアドレス ?	<input type="text"/>

IPv4 Header(1/3)



IPv4 Header(2/3)

(1) Version Number

(IPv4の場合は“4 = 0100”)

(2) Internet Header Length(ヘッダ長)

32bit(4byte)を1単位として表わす(最短で“5”=20byte)

(3) Type of Service(TOS, サービスタイプ)

QoS(Quality Of Service)を定義する。

(4) Total Length(パケット長の長さ)

8bit(1byte)を1単位として表わす。

(5) Identification(ID, 識別子)

パケットが分割された(fragmentation)場合, 再構成する際に使用されるID番号。

IPv4 Header(3/3)

(6) Flag

パケット分割の許可・不許可を表わす。

(7) Fragment Offset(フラグメントオフセット)

分割されたパケットのどの部分であるかを表わす数値。8bit(1byte)を1単位とする。

(8) Time To Alive(TTL, 生存時間)

本来は秒単位だが、中継ホスト(ルータ)を通過するごとに必ず1減らす。0になったらパケットは転送されず、その場で廃棄される。

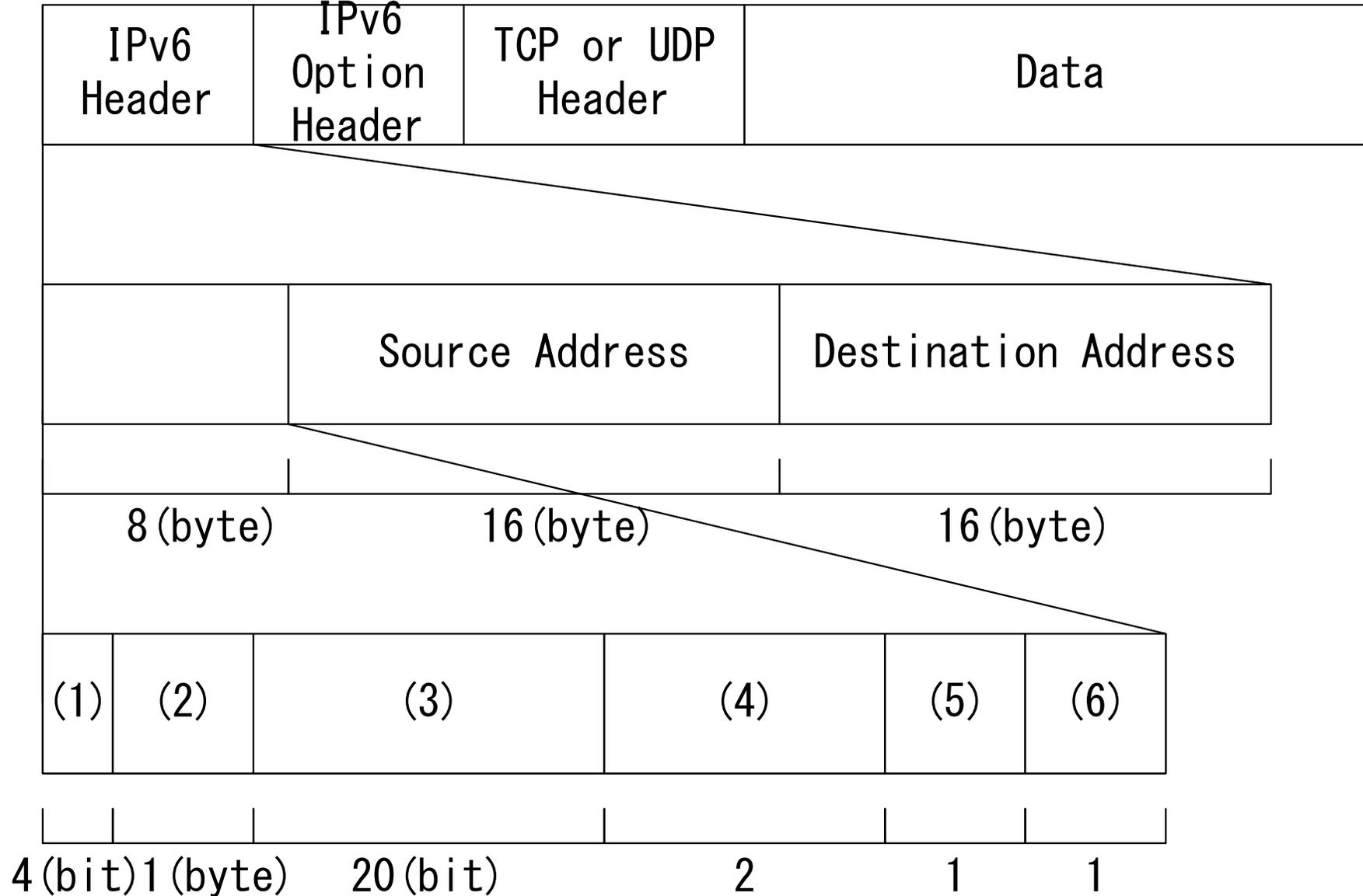
(9) Protocol

上位層のプロトコルを表わす。ICMP="1", TCP="6", UDP="17"

(10) Header Checksum

ヘッダ部分のチェックサムを格納する。

IPv6 Header(1/2)



IPv6 Header(2/2)

(1)Version

IPv6の場合は“6”=0110

(2)Traffic Class

QoSのために使用される。

(3)Flow Label

一連のIPパケットが通常とは異なる取り扱いをする場合に使用される。

(4)Payload Length

パケット長が、8bit(1byte)を1単位として表わされる。

(5)Next Header

IPv6 Headerに続く Option Headerの形式を表わす。

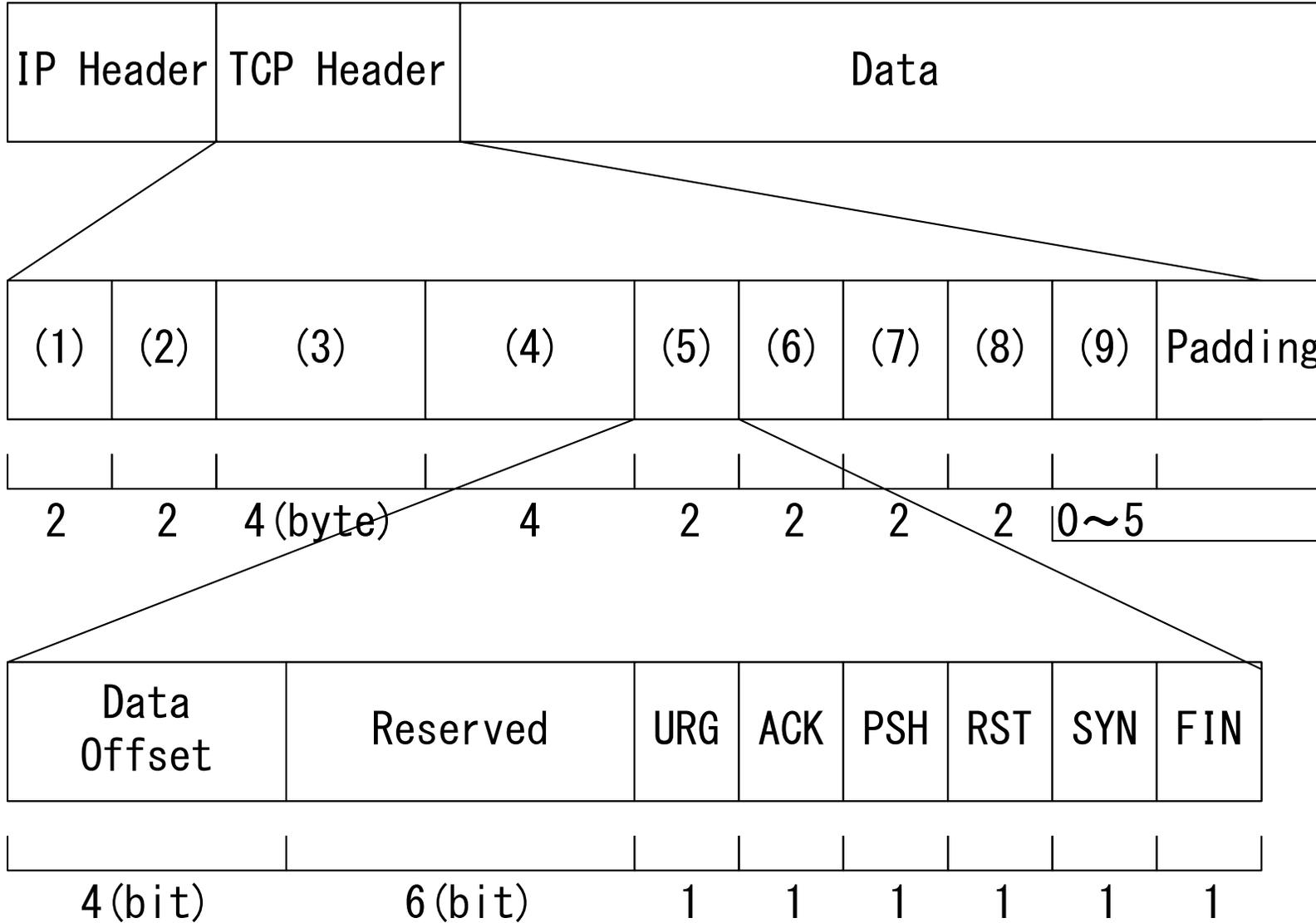
(6)Hop Limit

中継限界数。TTLと同様、各ホストを通るたびに1減らされ、0になるとその場で廃棄される。

TCP

- コネクション指向のプロトコル
- 「接続開始」「接続中（この間にデータの送受信を行う）」
「接続終了」の状態間を行き来する。
- TCP用のポート番号でプロトコル種別をする。
- ○電話, ×電報

TCPヘッダ(1/4)



TCPヘッダ(2/4)

(1)Source Port(始点ポート)

パケットの送信元のポート番号を表わす。

(2)Destination Port(終点ポート)

パケットの受信先のポート番号を表わす。

(3)Sequence Number

送信したデータのbyte数を表わす。

(4)Acknowledge Number

確認応答番号(次に受信すべきデータのSequence Number)を表わす。

TCPヘッダ(3/4)

(5)

- Reserved (予約領域)
TCPでは使用しないので、0としておく。
- Data Offset
TCPが運んでいるデータがヘッダ先頭部からどこにあるのかを、32bit(4byte)を1単位として表わす。オプションがない場合は(1)~(8)までの“5”=20byte目からとなる。
- Control bit . . . パケットの意味を表わすbit
 - URG(Urgent Flag) . . . 緊急用のパケット
 - ACK(Acknowledgement Flag) . . . 肯定確認応答
 - PSH(Push Flag) . . . 速やかに上位層へ渡すパケット
 - RST(Reset Flag) . . . コネクションの強制初期化
 - SYN(Synchronize Flag) . . . シーケンス番号の同期
 - FIN(Fin Flag) . . . 以後送信するデータなし

TCPヘッダ(4/4)

(6)Window Size

フロー制御の際に使われるWindow Sizeを格納する。

(7)Checksum

(8)Urgent Pointer

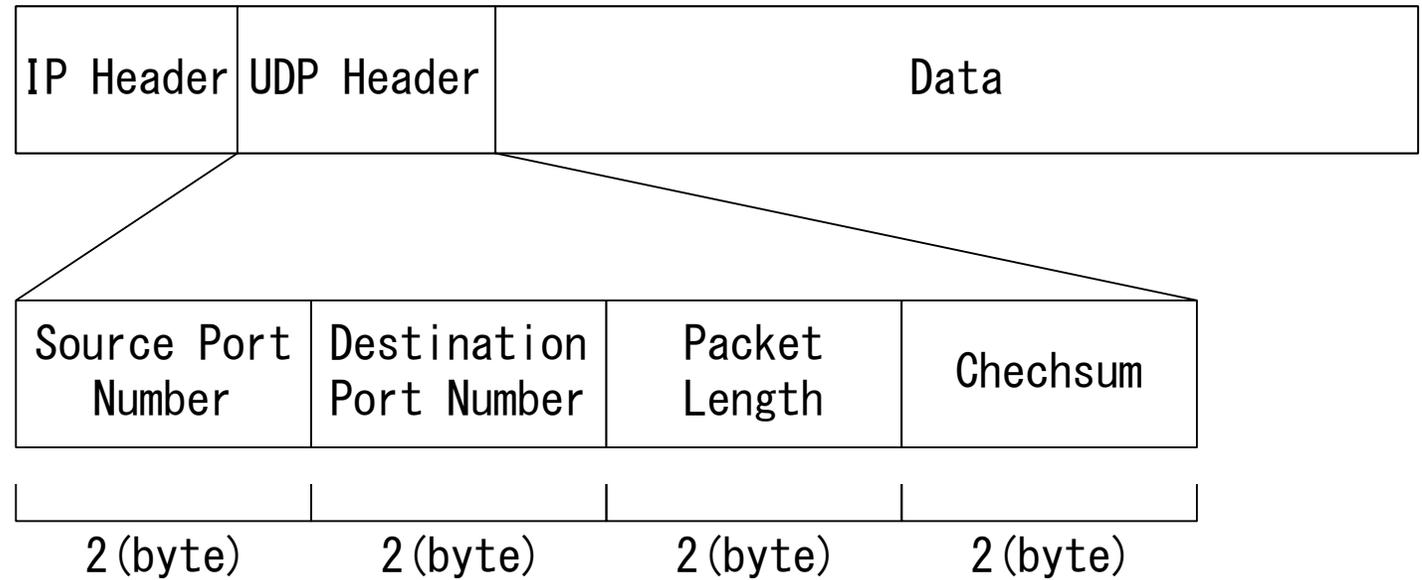
URG bitが“1”の時，受信バッファの順を飛び越える必要のある緊急のパケット内のデータ数を8bit(1byte)単位で格納する。

(9)Option

MSS(Maximum Segment Size)の交換, SACK(選択確認応答)の使用, などに使用される。

UDP

- コネクション指向でないデータの送受信を行うためのプロトコル。パケットの送受信はそれぞれ一方通行。
- 映像・音声のリアルタイム処理にも利用される。
- UDP用のポート番号でプロトコル種別をする。
- ×電話, ○電報
- IP + データ



主要なアプリケーション

アプリケーション	Port Number	ICMP	UDP	TCP
Ping		○		
Traceroute(Tracert)		○		
DHCP			○	
NTP	123		○	
TFTP	69		○	
SNMP	161,162		○	
SMTP	25			○
SSH, Telnet	22, 23			○
FTP	20,21			○
HTTP,HTTPS	80, 443			○
DNS	53		○	○
NETBIOS	137, 138, 139		○	○

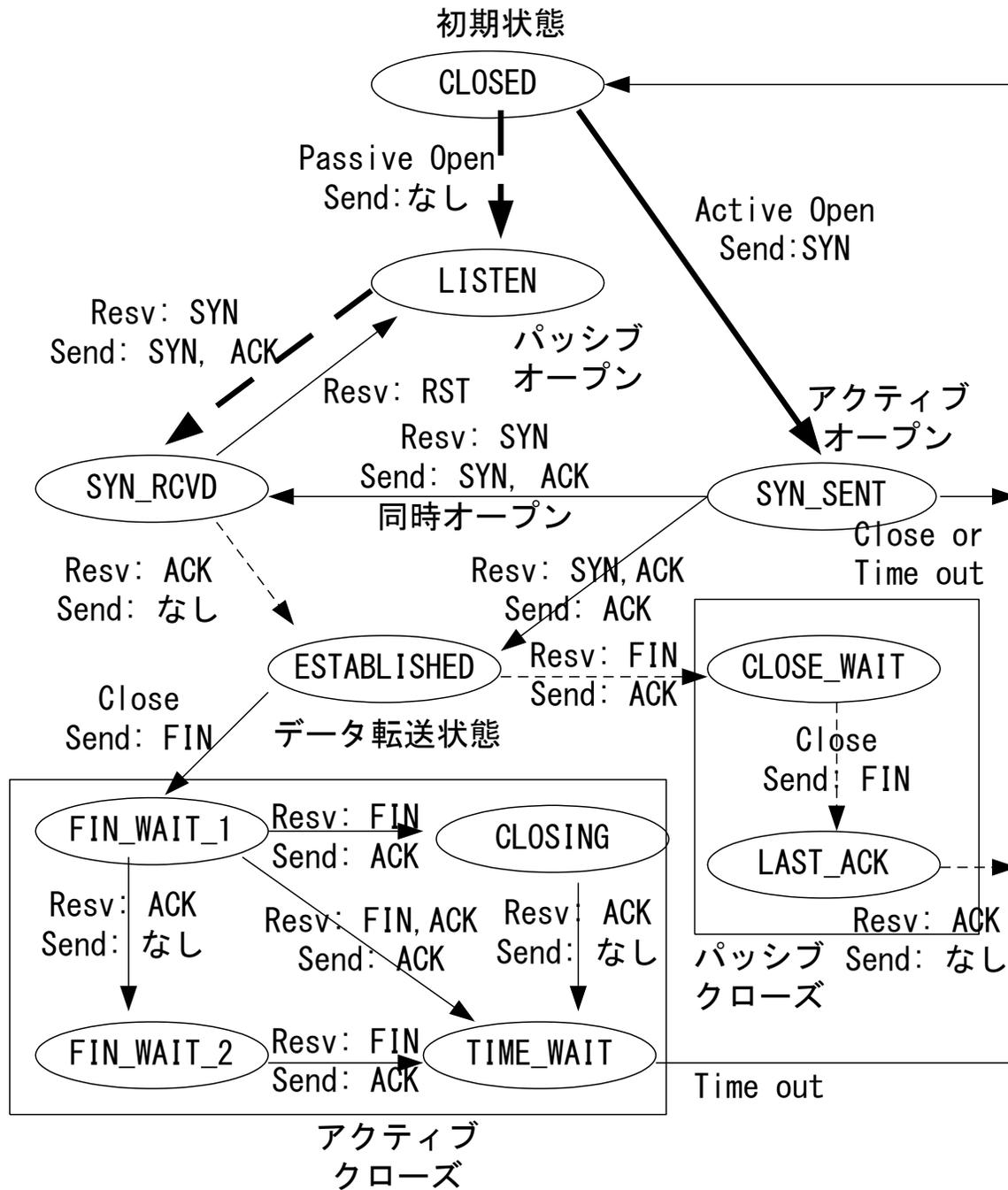
- 主要なアプリケーションはTCPベースが多い

→○TCP/IP, ×UDP/IP

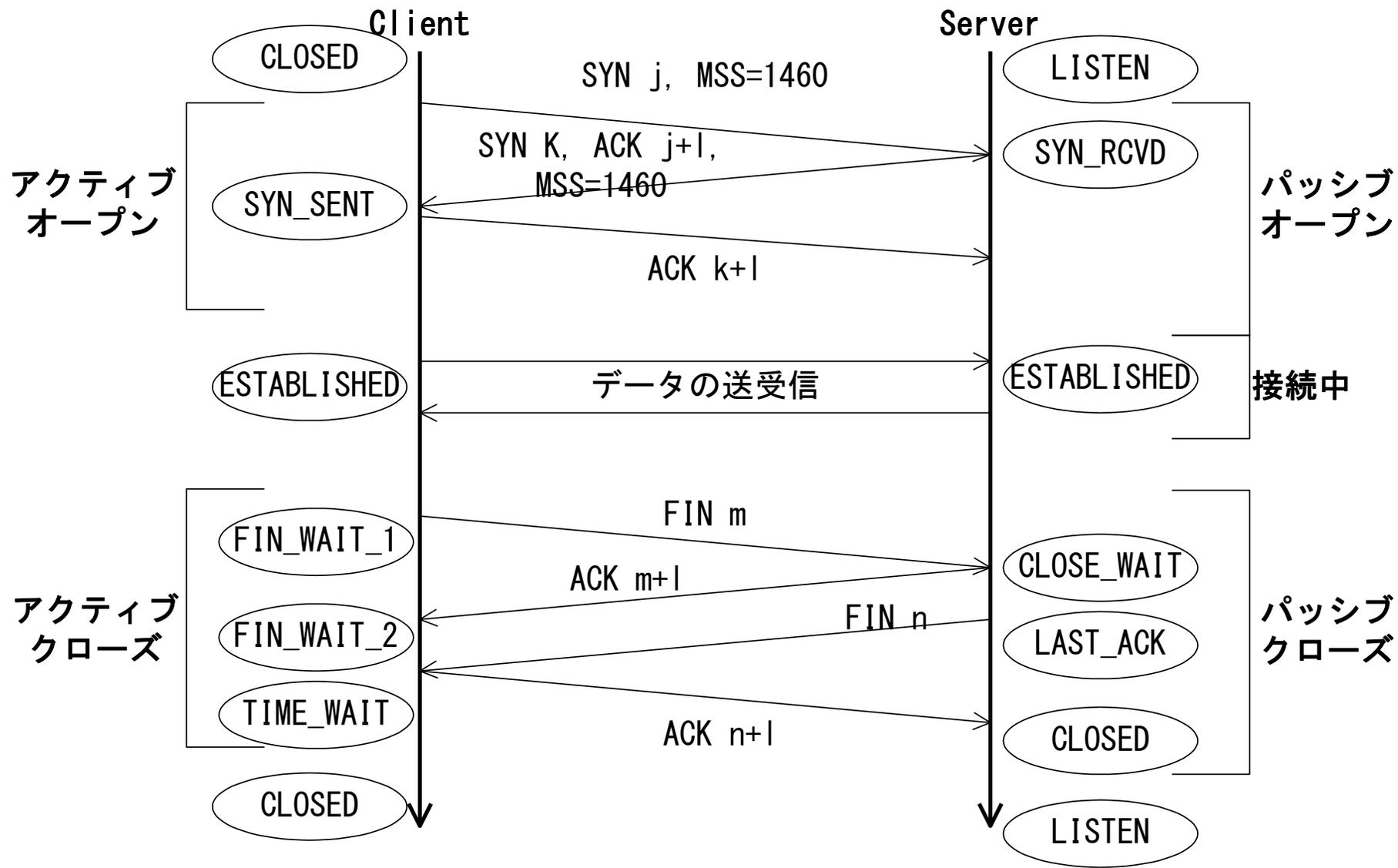
ICMP . . . Internet Control Message Protocol

- ルータ・ホスト間のエラー・制御情報を交換するためのプロトコル。
 - ICMPv4 . . . IPv4用のICMP
 - ICMPv6 . . . IPv6用のICMP
- TCP/UDP層が制御のために使用することが多い。
- Ping, Tracerouteで使用されている。

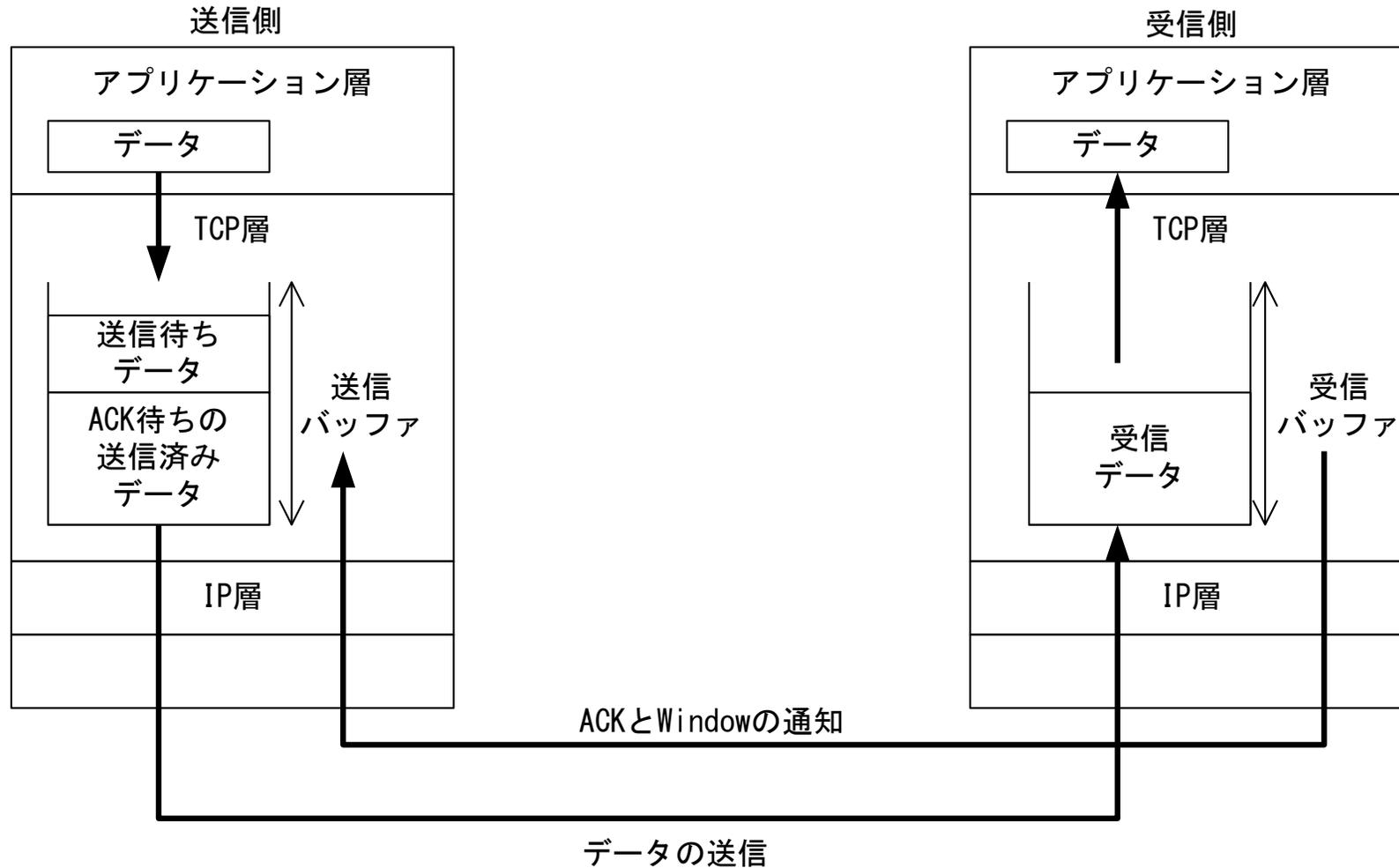
TCP状態遷移図



TCP接続例



Established時のTCPのパケットの流れ



①輻輳(Congestion)制御
・・・ネットワーク混雑に応じた送受信するデータの量の制御

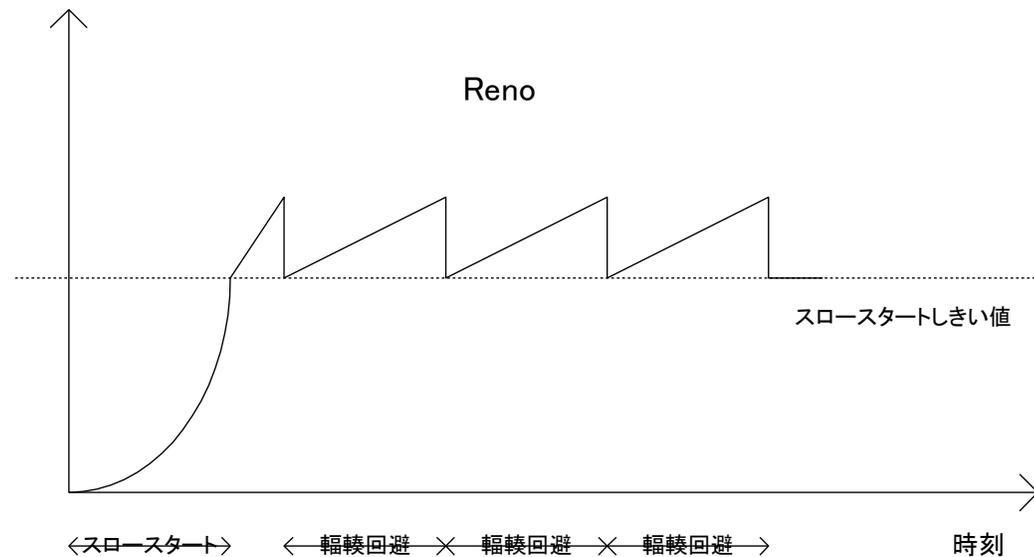
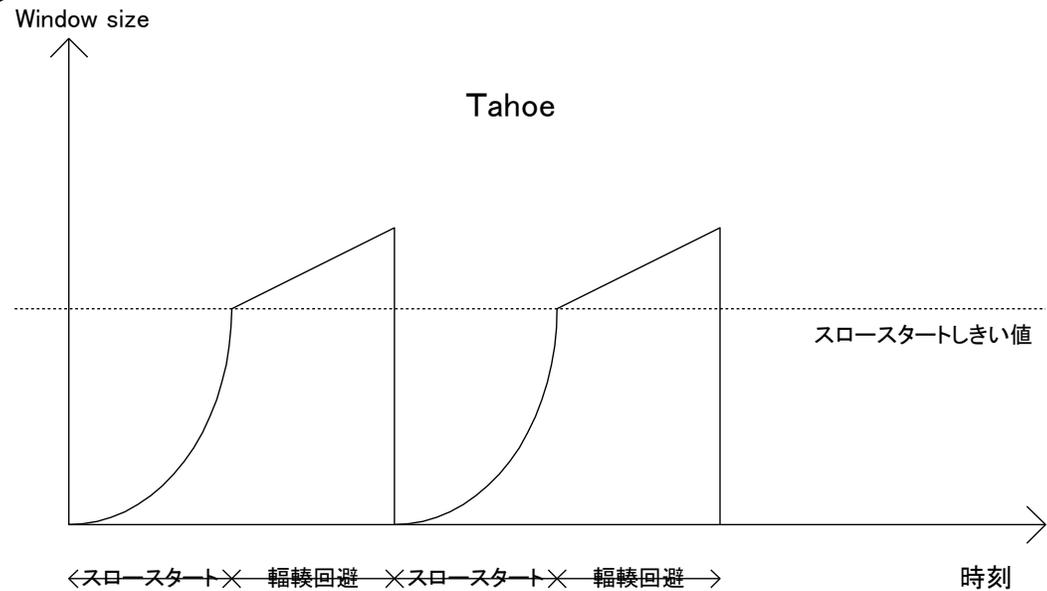
②誤り制御
・・・データの正常性の確認。CRCチェックし、誤りがあれば再送要求をして再送。

TCPの改良

- Tahoe(1980年代後半から)
 - 初めて輻輳制御アルゴリズムが取り入れられる (輻輳Windowの導入)
- Reno(1990年代初期から/RFC2581)
 - Tahoeの輻輳制御アルゴリズムの改良
- New Reno(Experimental/RFC2582)
- Vegas(Experimental)

輻輳回避のアルゴリズム

- スロースタート
- 輻輳回避



[復習] 本日の内容

- IPアドレス管理
 - サブネット分割
 - DHCP
- IPヘッダの構造
 - IPv4ヘッダとIPv6ヘッダ
- TCPとUDP
- TCPの機能
 - コネクション維持の仕組み
 - 輻輳制御

本日の課題 <https://forms.office.com/r/A8SYZzQH4H>

1. 133.88.0.0/16を4等分したときのそれぞれのサブネットを「ネットワークアドレス/プレフィックス長」で書け。
2. IP層の上で動作するTCPの特徴を述べよ。
3. IP層の上で動作するUDPの特徴を述べよ。
4. TCPの制御のうち重要なものを2つ挙げよ。

コンピュータネットワーク 第6回 本日の課題

