

コンピュータネットワークの基礎と応用

ルーティングを中心に

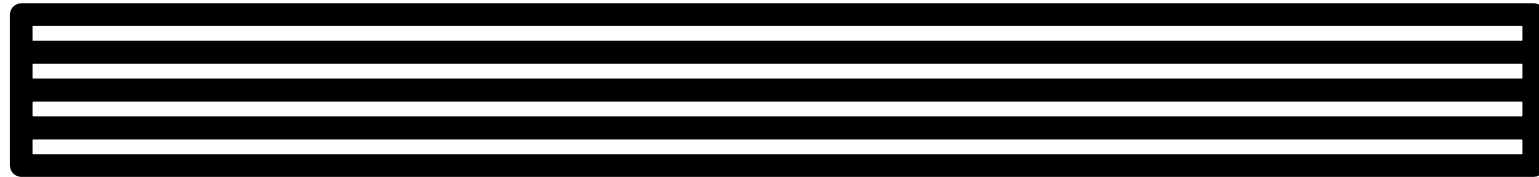
2008/4/5

村上仁一

通信工学

ストリームデータ 昔の主流

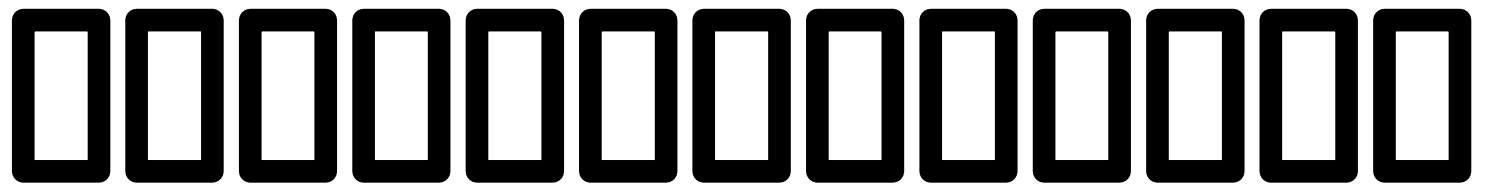
電話、テレビ 「電話交換器（電々公社）」



時間

パケットデータ 今の主流

コンピュータネットワーク, データ通信
携帯電話 「ルータ」



時間

文献

小高知宏, ``TCP/IP で学ぶコンピュータネットワークの基礎'',
森北出版, ISBN4-627-82410-6 (1996)

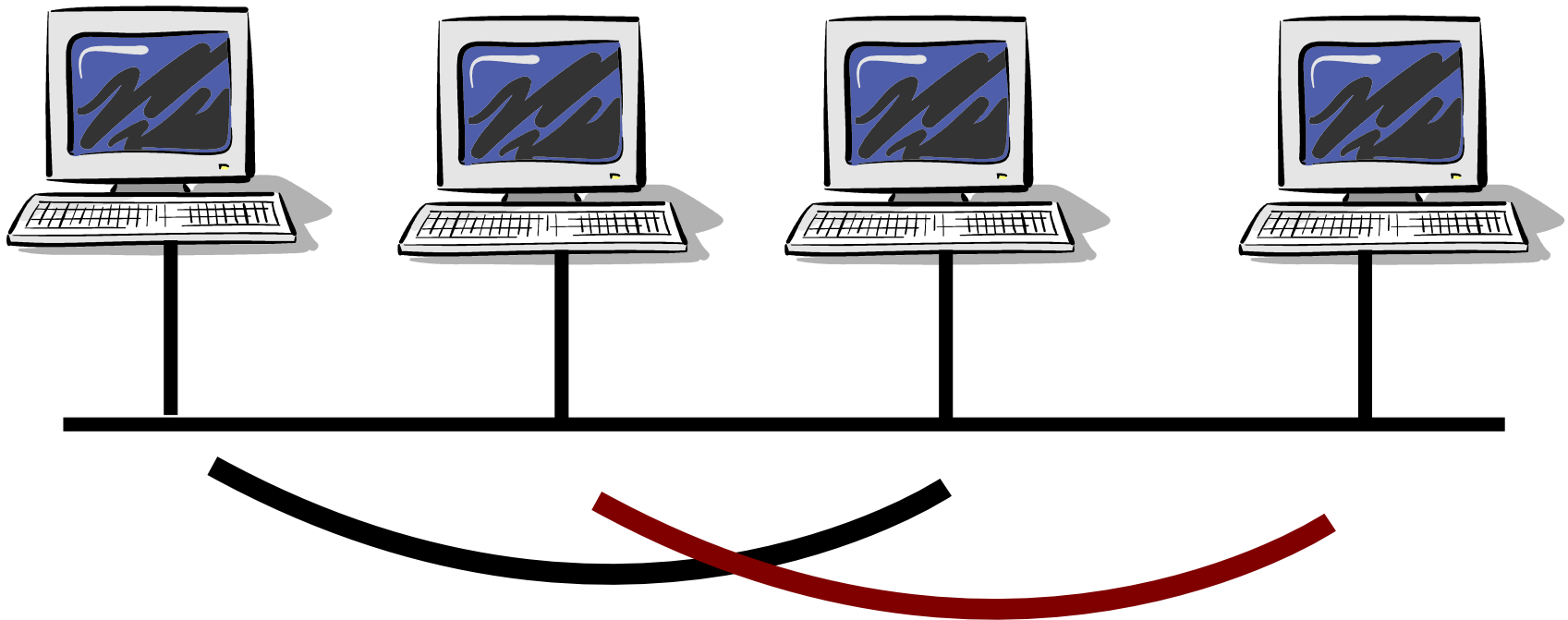
寺田, 菅島, ``TCP/IP セキュリティ実験'',
オーム社, ISBN4-274-06382-8 (2000)

村井 純, ``ネットワークアーキテクチャ'',
<http://www soi.wide.ad.jp/class/20010012>, (2001).

ネットワークの問題

1つのネットワーク（ケーブル）に複数のマシンが接続されたときに、信頼性のあるデータ通信方法の確立

問題点 データの干渉



データ通信の歴史

コンピュータの歴史

- 1) コンピュータ単体で集中処理
バッチ処理
- 2) 集中型データベース (TSS)
データベースは1つのコンピュータに集中
アクセス端末は複数
- 3) 分散型データベース
(リレーショナルデータベース)
データベースが複数のコンピュータに分散

コンピュータの通信

1960年代から

1) 各社、独自のプロトコル

IBM SNA DEC DecNet

XEROX XNS

NEC DINA 電々公社 DCNA

2) 国際標準 OSI ISO

3) 実用研究 TCP / IP

ベンダ独自プロトコルの衰退

標準化による優位性の欠如

DECNET → OSI protocol

Apple talk → TCP/IP 上のアプリケーション

Netware, NetBios → TCP/IP 上のアプリケーション

Xerox XNS → 滅亡

IBM SNA → サバイバル

大型汎用機

業務用

TCP/IP の成功

1990 年代

勝者の決定

OSI の失敗

標準化の遅れ (ISO 標準化プロセスの敗北)

仕様が複雑

TCP/IP の勝利

標準化の速度 (IETF 標準化の勝利)

UNIX との結合

DARPA の支援

仕様が単純、実装重視

OSI 7 階層

階層型プロトコルの概念を明確に定義

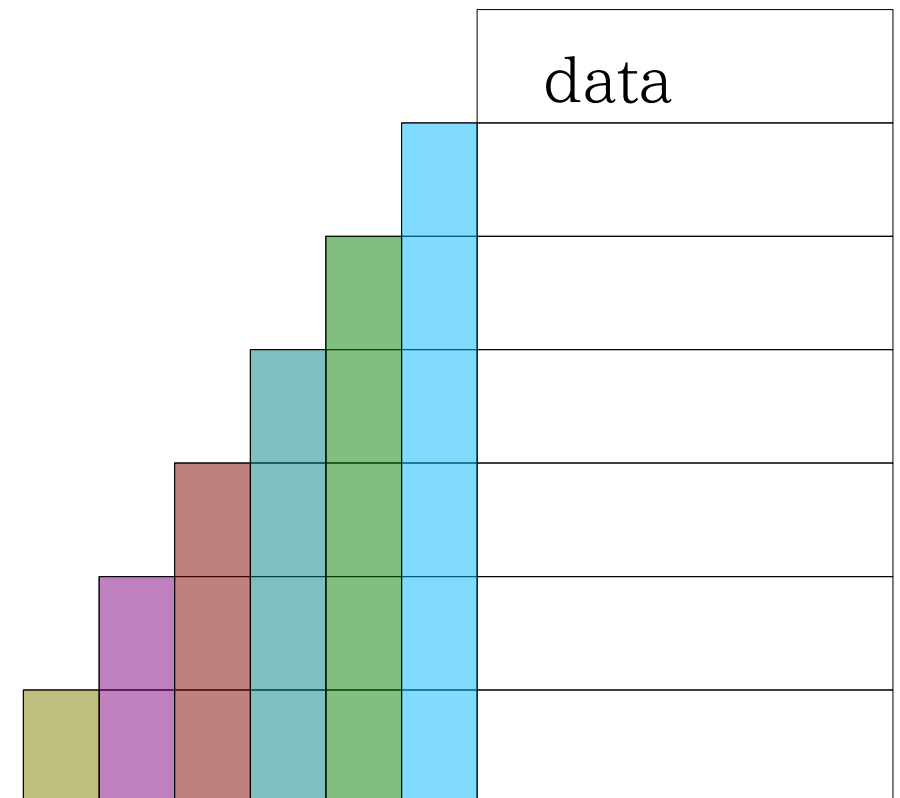
アプリケーション	ユーザが使用するアプリケーション
プレゼンテーション	コンピュータが理解できるバイナリデータ形式に変換
セッション	要求サービスの始まりから終わりまでを管理
トランスポート	信頼性, 順序性, 再送 segment 順序を保証する通信を提供
ネットワーク	複数のネットワークをつなぎ、データを中継
データリンク	ネットワーク上で直結されている機器同士での通信方式を定義
物理	電気信号や光信号を接続

階層化プロトコルの技術的特徴

カプセル化

下位プロトコルは上位プロトコルをカプセル化

アプリケーション
プレゼンテーション
セッション
トランスポート
ネットワーク
データリンク
物理



各階層の header

階層化の特徴

スケーラビリティに貢献
各処理を分散可能

新しい技術への対応が簡単
変化したところだけ交換可能

メリット、デメリット

メリット

単純、明解。 分割開発が可能。
理解しやすい。独立したバージョンアップ
異機種間の相互接続が可能

デメリット

パフォーマンスがでない
カプセル化によるメモリ管理とデータ管理は困難
可変長データの取り扱いは困難

TCP/IP の歴史

1969 年 DARPA 核戦争用の通信プロトコル
ARPANET

IP プロトコル + UNIX + Ethernet (1983)

OSI

アプリケーション
プレゼンテーション
セッション
トランスポート
ネットワーク
データリンク
物理

TCP/IP

アプリケーション
トランスポート
ネットワーク
データリンク / 物理

TCI/IP のアドレス値

TCP/IP

アドレス値

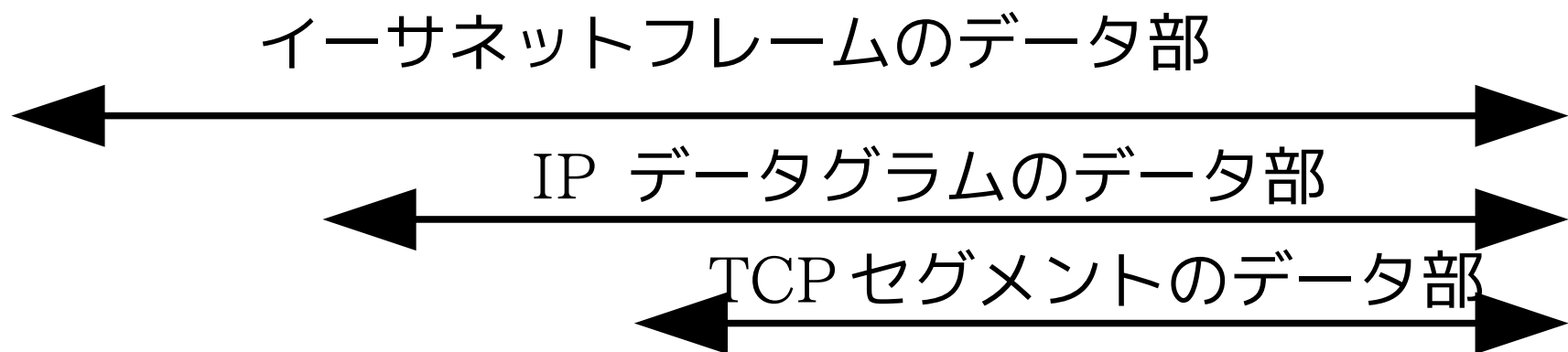
アプリケーション
トランスポート
ネットワーク
データリンク / 物理

アプリケーション telnet ftp Web DNS	
TCP	UD P
IP	
Ethernet frame/ 物理層	

Port 番号

IP アドレス

Mac アドレス



イーサネット フレーム ヘッダ	IP データグラム ヘッダ	TCP セグメント ヘッダ	
-----------------------	------------------	------------------	--

TCP/IP のパッケージ

層		処理単位	アドレス
アプリケーション	Telnet やFTP		
トランスポート	TCP UDP	セグメント	Port
ネットワーク	IP	IP datagram	IP address
データリンク	Ethernet frame	Frame	Mac address
物理	100base-TX,etc		

TCP/IP の階層

インターネットの成功

1990年代

勝者の決定

OSIの失敗

標準化の遅れ (ISO 標準化プロセスの敗北)

仕様が複雑

TCP/IPの勝利

標準化の速度 (IETF 標準化の勝利)

UNIXとの結合

DARPAの支援

仕様が単純、実装重視

ベンダ独自プロトコルの衰退

標準化による優位性の欠如

DECNET → OSI protocol

Apple talk → TCP/IP 上のアプリケーション

Netware, NetBios → TCP/IP 上のアプリケーション

Xerox XNS → 滅亡

IBM SNA → サバイバル

大型汎用機

業務用

物理層

Bit を提供

各伝送媒体に対してビット伝送手順を定義

例：電気信号レベル L:< 0.5 V H:> +3.7V

ビット列伝送手順：同期方法、エラー補正

Ethernet で使用される伝送メディア

有線

同軸ケーブル

UTP(unshilded twist pair) ケーブル

光ファイバー

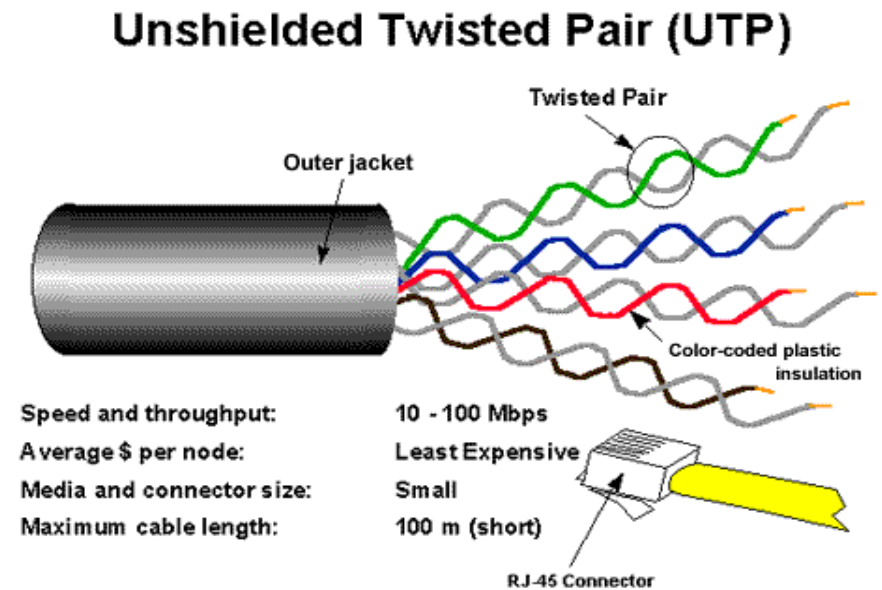
無線

電波

ツイストペアケーブル

対を構成する 2 本の芯線を均等により分け
雑音、漏話を軽減

UTP unshield twist pair
最大伝送距離 100m
STP shield twist pair



Cable の作成方法

ツイストペアケーブルのコネクタ

- 主なもの
 - RJ11 6極 電話用
 - RJ45 8極 LAN/ISDN用
 - RJ48 8極 ISDN新規格用

[RJ48]

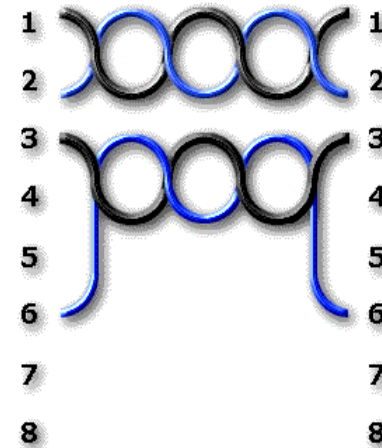


図 10-1-10 ISDN用 RJ48 8極の配線
RJ48は、RJ45のケーブルに追加のピンを付加して使用する。

- ケーブル内の配線
 - ケーブルの色によって決まっている

[T568B]

ストレートケーブル



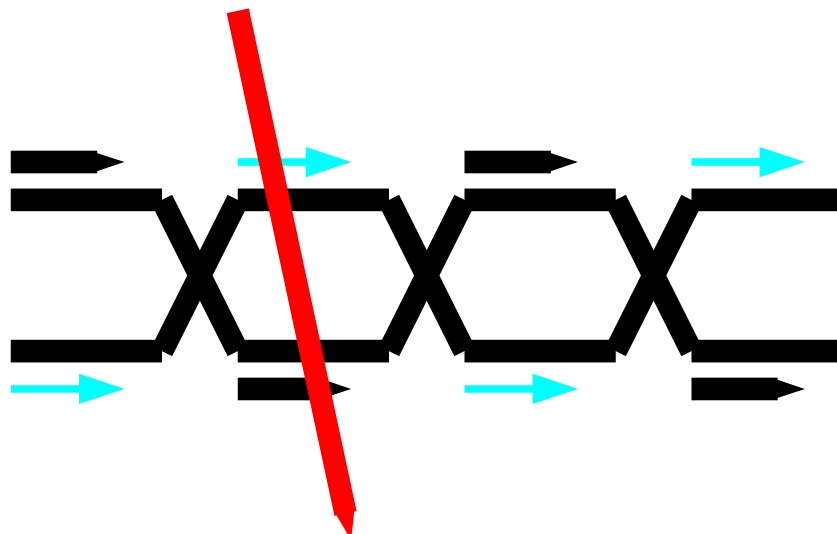
Correct Wiring



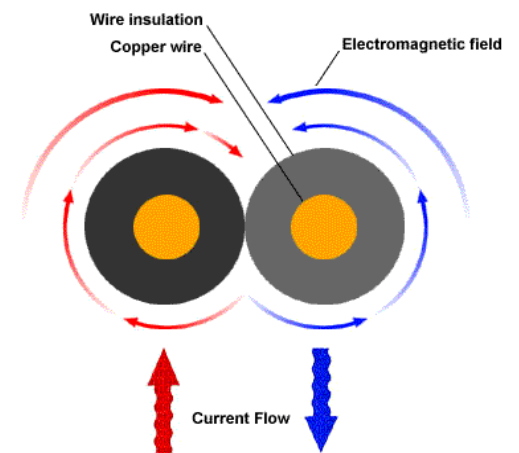
UPS ケーブルのノイズ耐性

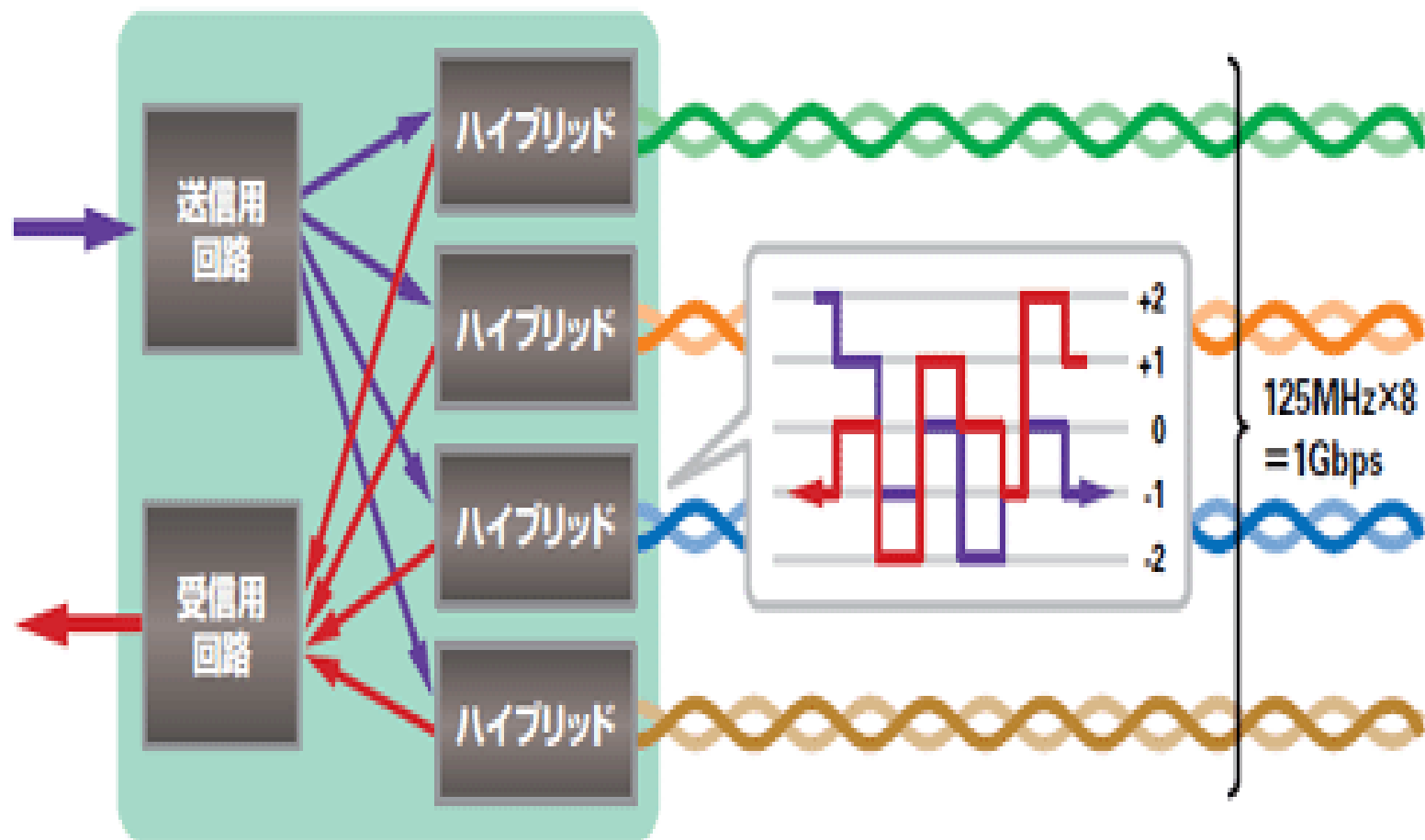
実用的、もっとも平衡度が高いケーブル

撚り線によって高い平衡性
外部からのノイズを打ち消し
ケーブル自体が発生するノイズを打ち消し
他のケーブルにノイズの影響を受けない。



外部からの電磁誘導

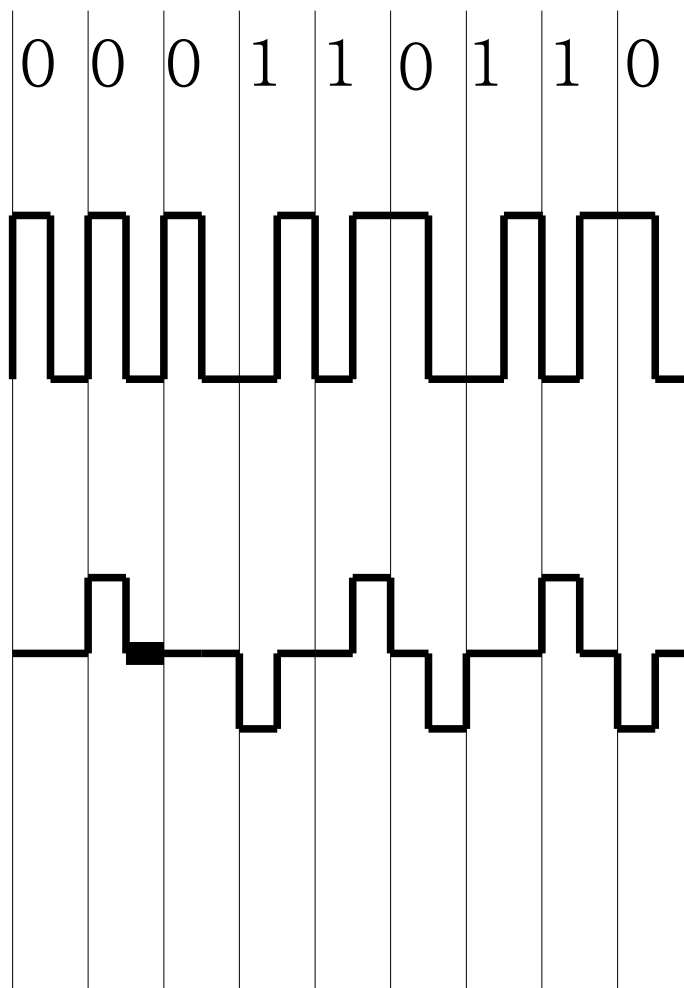




1000base-T

マンチェスタ
(10base-Tで使
用)

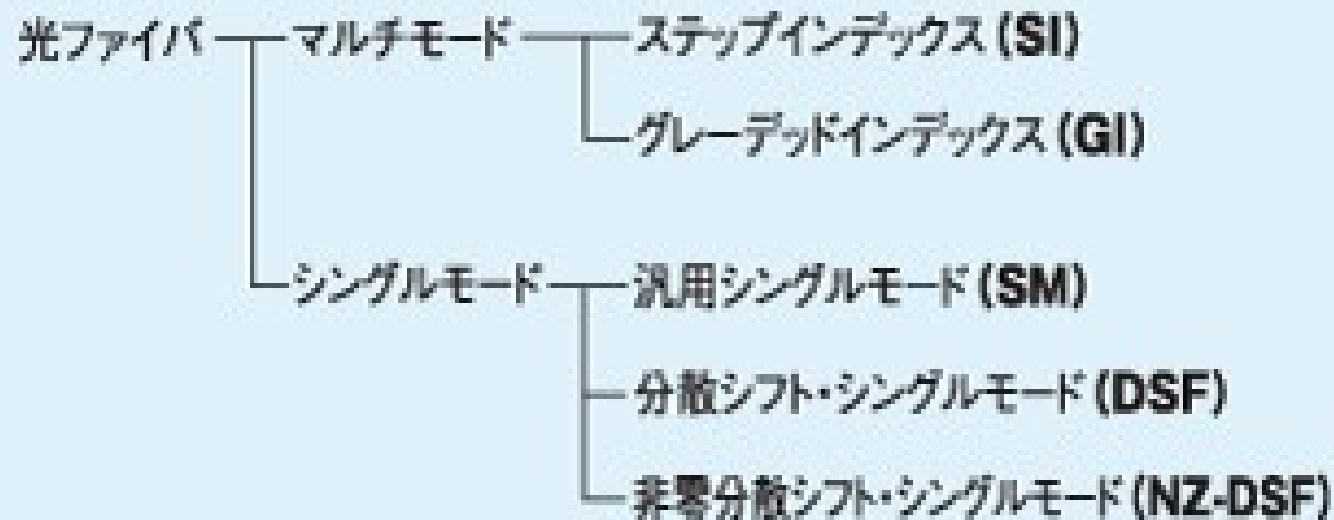
3 値信号
MLT-
3+4B5B
(100base-
TX)



符号の方式

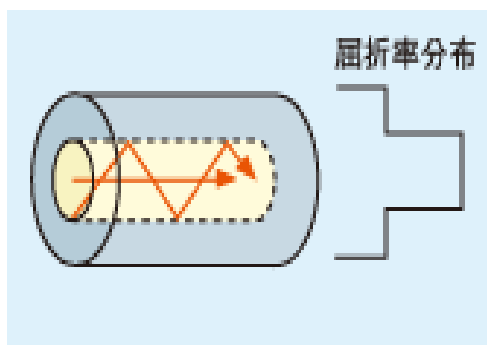
光ファイバーの種類

光ファイバの分類



マルチモード

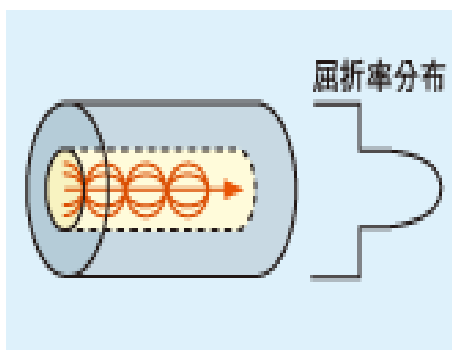
ステップインデックス



短距離

マルチモード

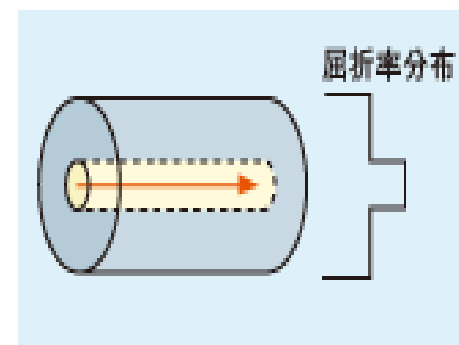
グレーデッドインデックス



LAN

シングルモード

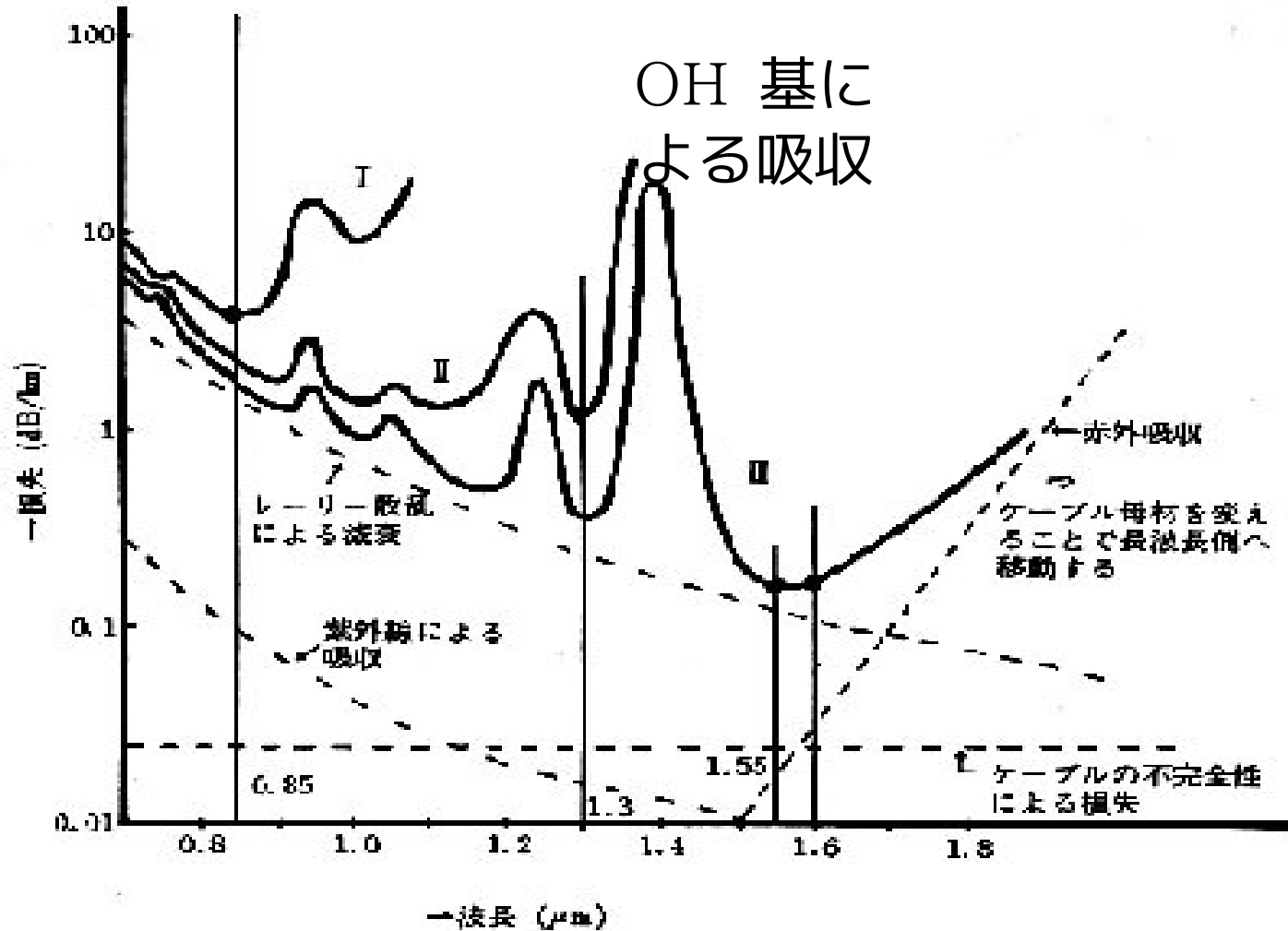
汎用シングルモード



長距離伝送

レーリー散乱

材料の分子振動吸収による損失



1.3um 1.5um

利用される周波数

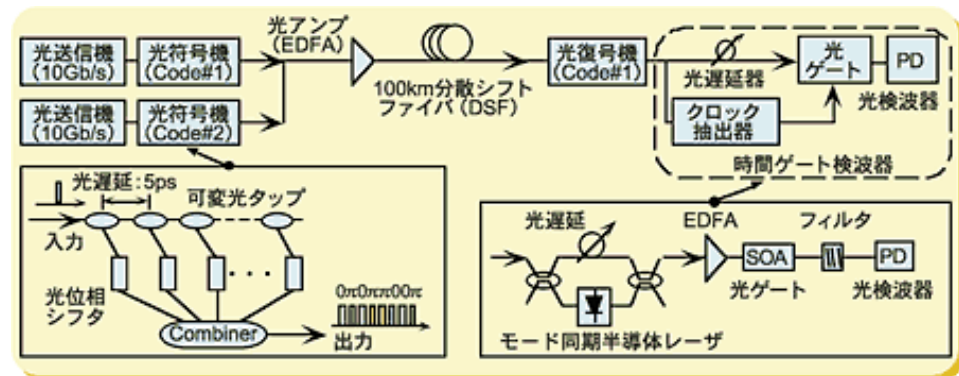
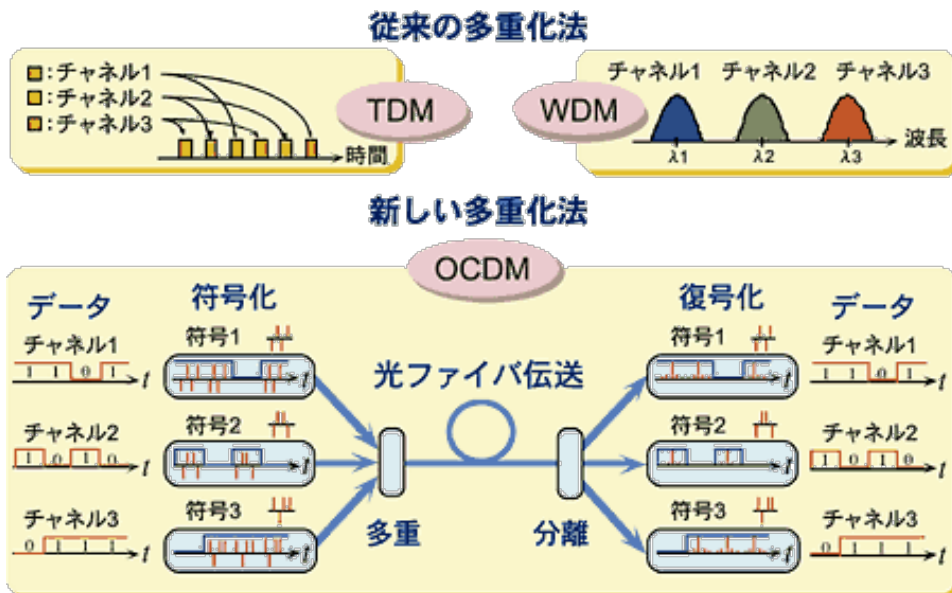
光ファイバーの損失特性

波長分割多重光通信

1990年代 周波数や位相を変調する光波通信の研究が開始

複数の波長に情報をのせて多重化する
波長分割多重光通信システムが開発

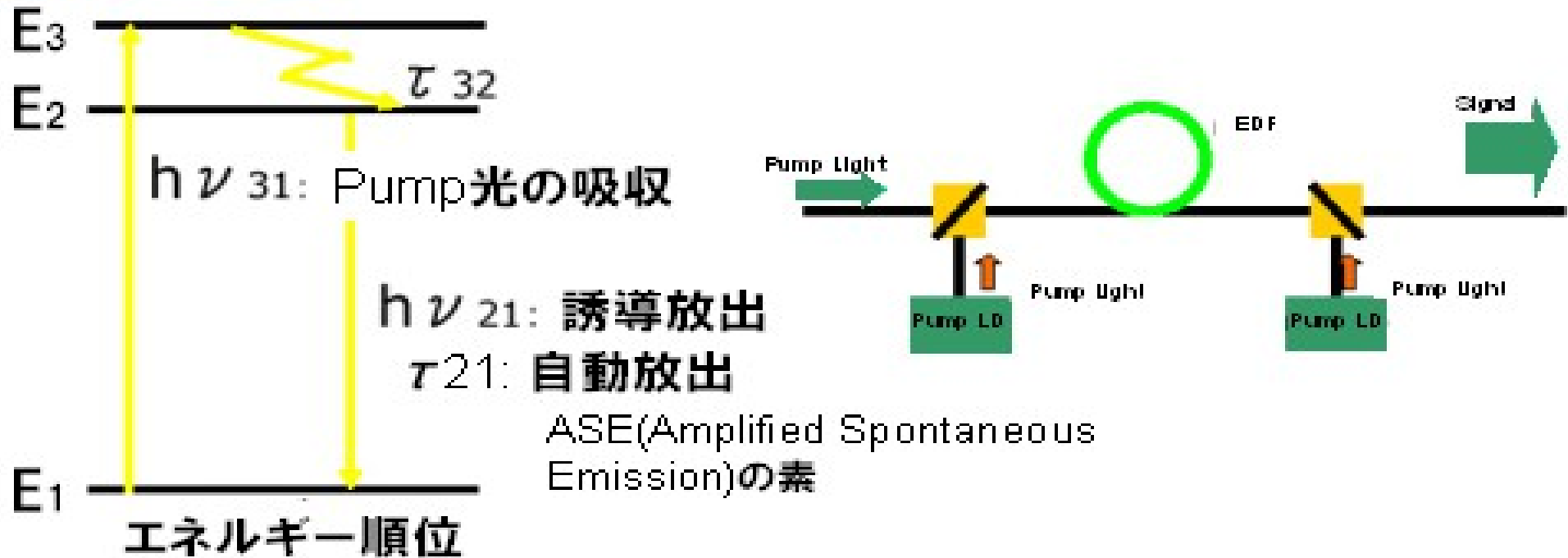
ケーブルあたりの容量が飛躍的に増加



光増幅 (Er 添付ファイバ)



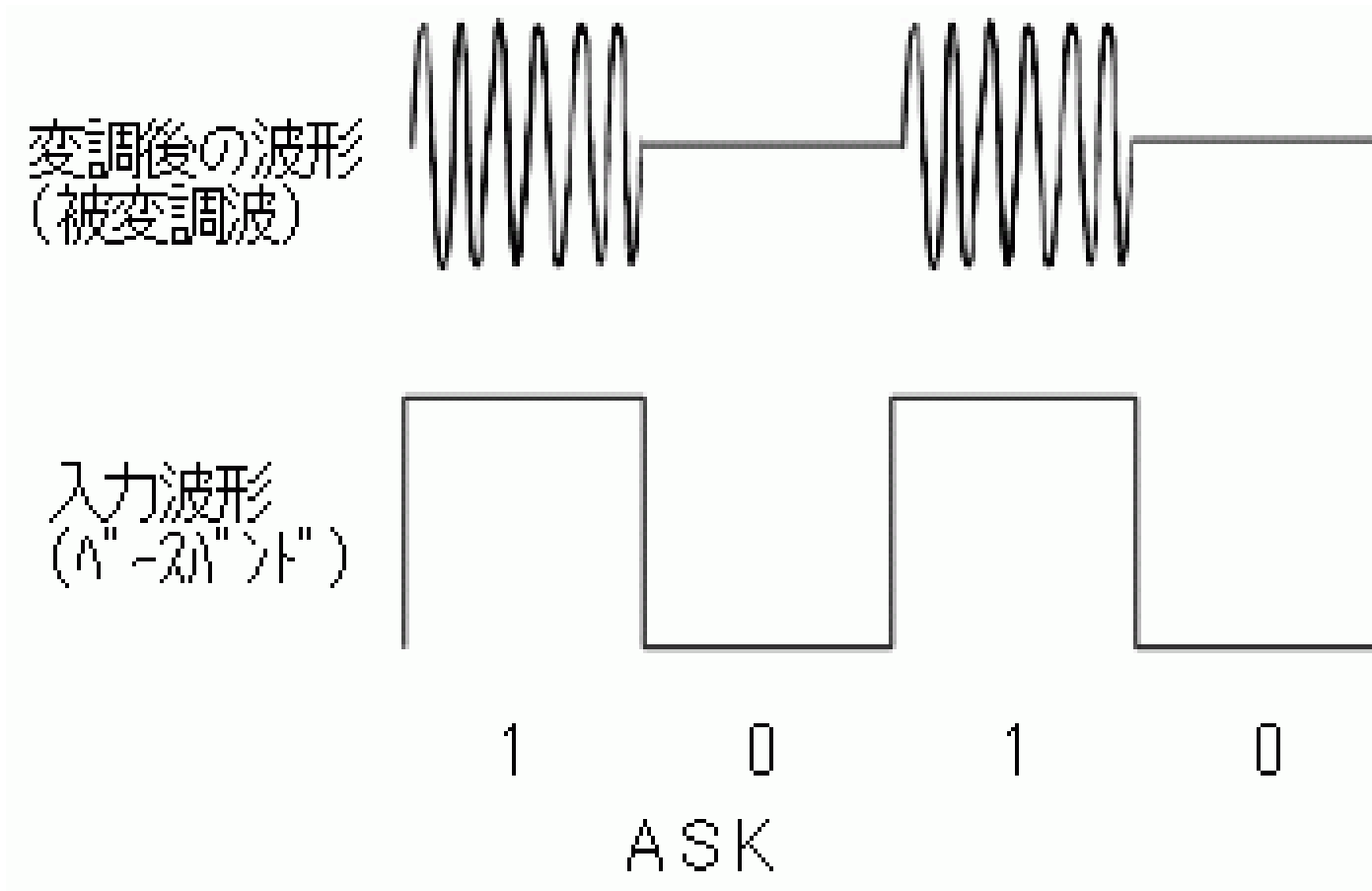
EDFAによる光増幅の原理



無線 変調方式

デジタル変調

振幅変調	(ASK)	
周波数変調	(FSK)	
位相変調	(PSK)	
振幅位相変調	(APSK)	
直交振幅変調	(QAM)	
直交周波数分割多重方式	(OFDM)	



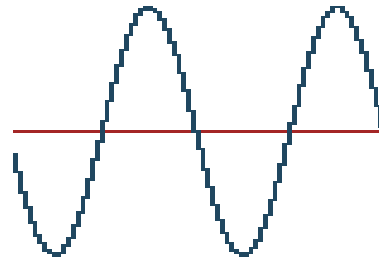
振幅変調方式 (デジタル) 50bit/s

周波数変調方式 (フリス ル) 300bit/s

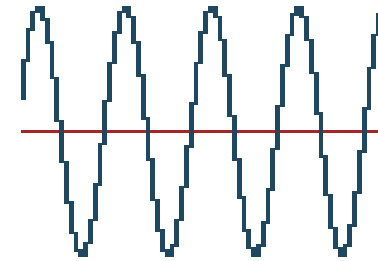
From Computer Desktop Encyclopedia
© 2007 The Computer Language Co., Inc.

Carrier

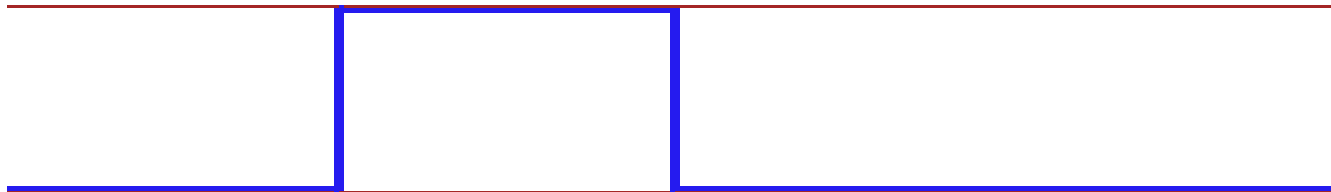
0



1



Modulating Wave (digital)



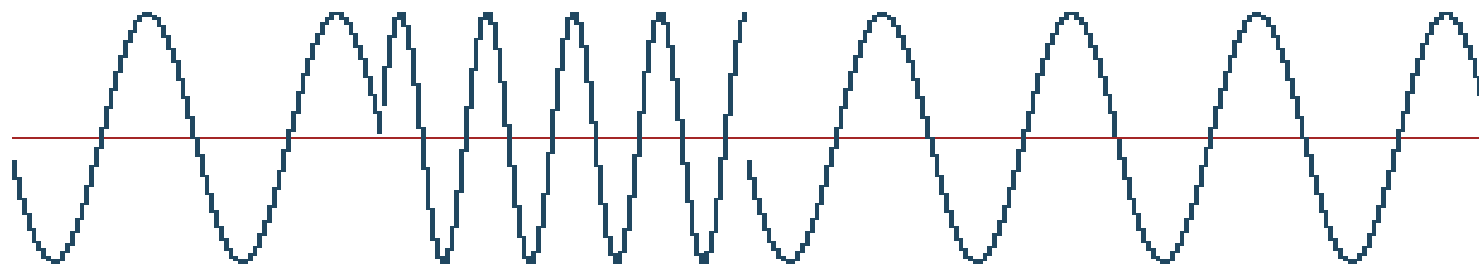
0

1

0

0

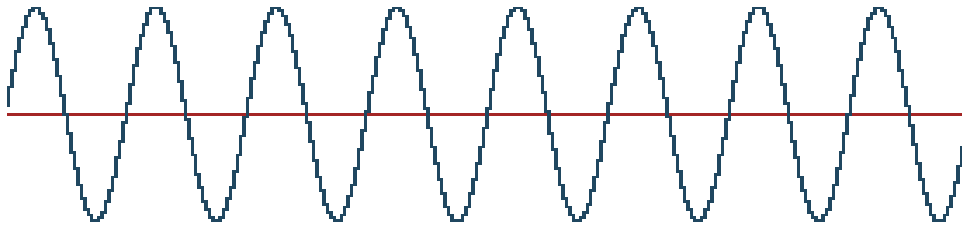
Modulated Result



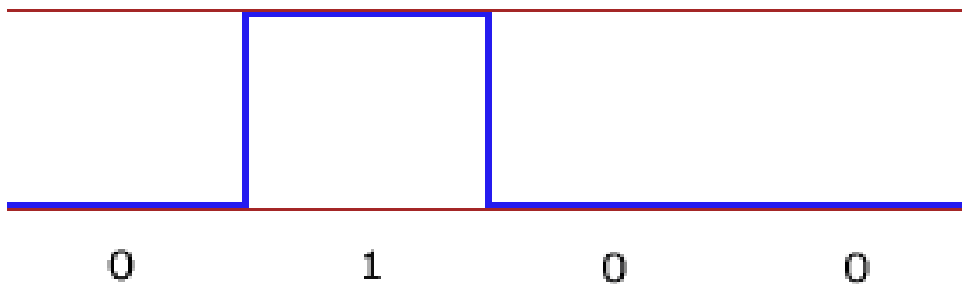
位相変調方式 (デジタル) 9600bps/s

From Computer Desktop Encyclopedia
© 2007 The Computer Language Co. Inc.

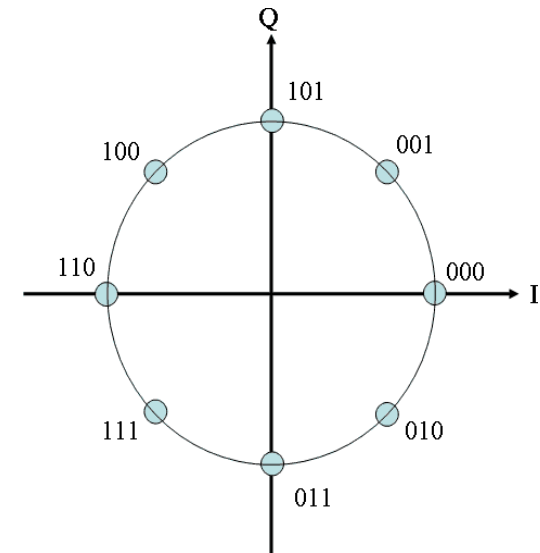
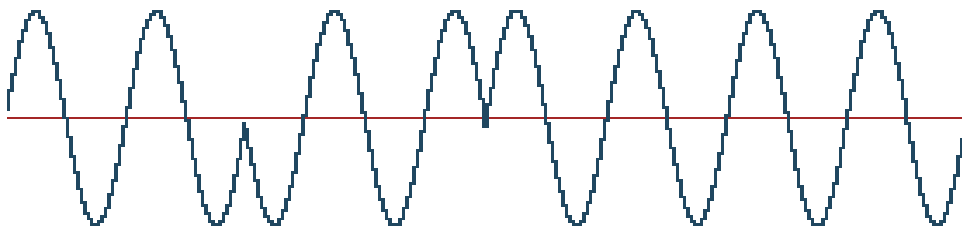
Carrier



Modulating Wave (digital)



Modulated Result

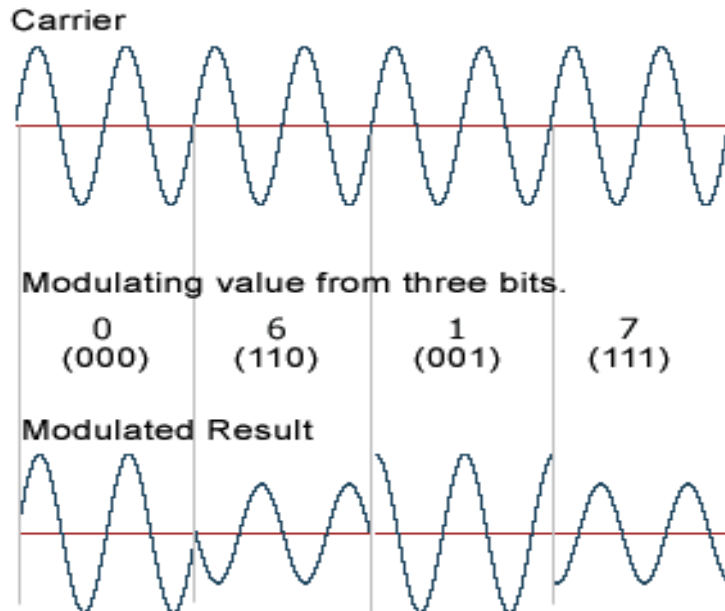


直交振幅変調 (QAM)

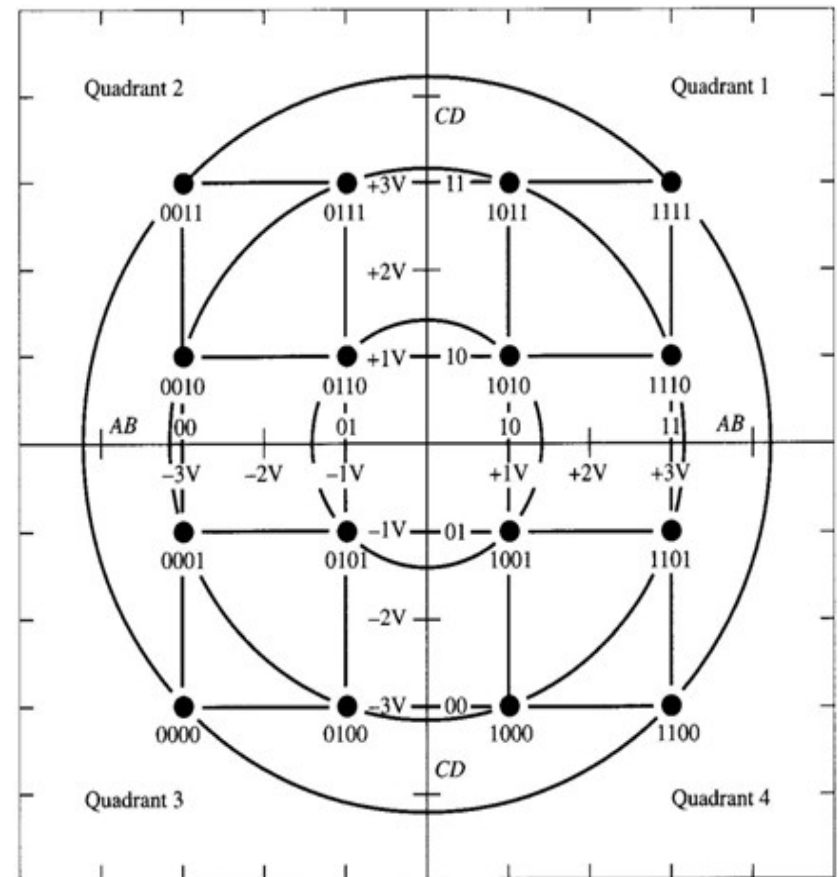
互いに独立な2つの搬送波の振幅と位相を変調

From Computer Desktop Encyclopedia
© 2007 The Computer Language Co. Inc.

DIGITAL QAM (8QAM)



Note: Only four (0, 6, 1 and 7) out of the eight possible modulation states (0-7) are shown in this illustration.



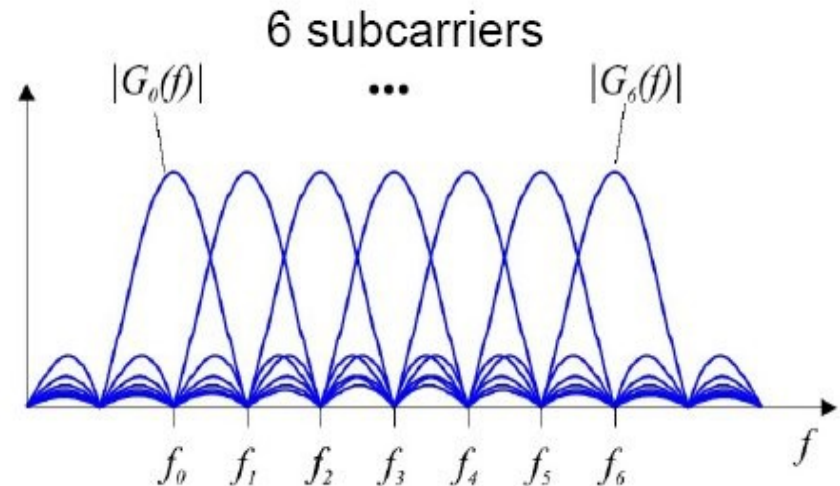
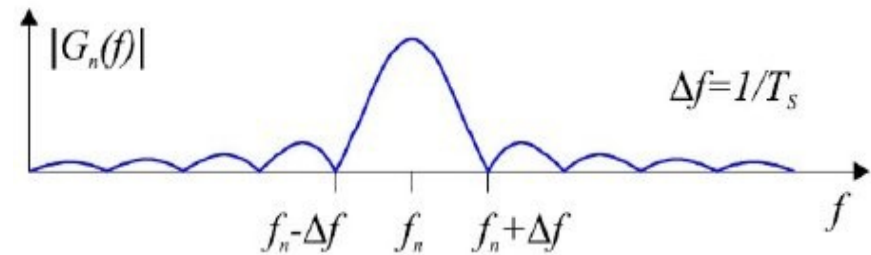
直交周波数分割多重方式 OFDM

マルチキャリア方式
お互いのサブキャリアが直交
サブキャリアは QAM 変調

サブチャネル同士の混信なし
高いスペクトル効率を得られ、理論上の限界
1 subcarrier

使用例：

ADSL
無線 LAN (IEEE 802.11a
以降)
地上波デジタル



データリンク層

隣接する装置 (ホスト) 間における通信手順

同一の伝送メディア

異なる伝送メディアとの通信にはゲートウェイが必要

送受信されるデータの format

データグラム型 ベストエフォート

データリンクフレーム

装置間におけるデータの誤り検出、訂正

物理層の特性を考慮して安定したデータ転送

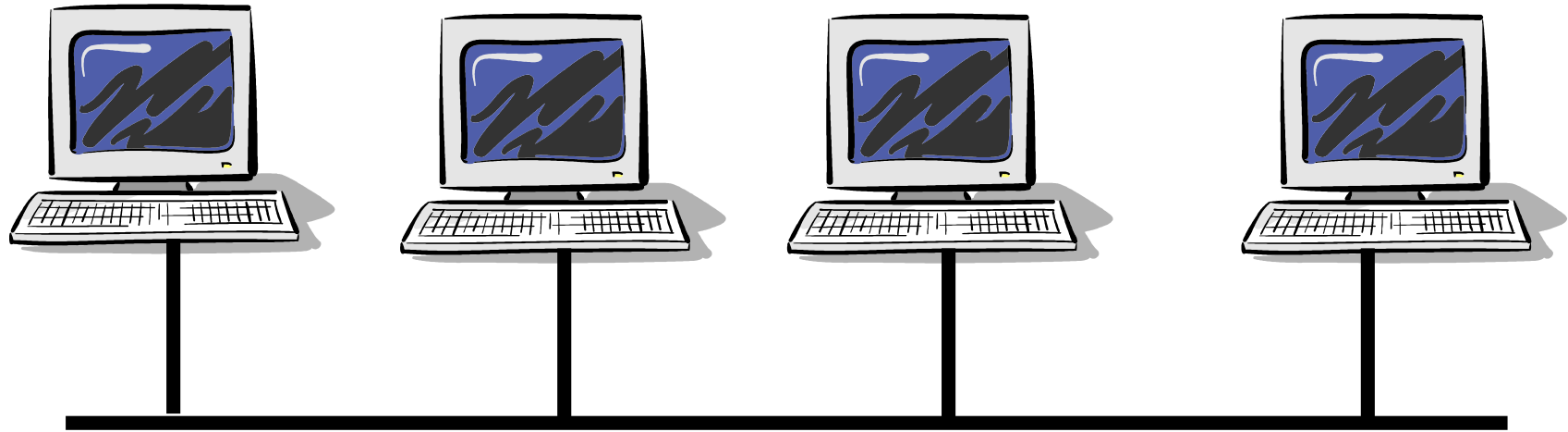
ネットワーク層に対するインターフェース

物理層のビットレベルの伝送機能を使用して、

フレーム単位の交換機能を実現

データリンク層 (1つのネットワークを構成)

隣接する装置(ホスト)間における通信手順



ネットワーク

ハブ

Ethernet

Xerox PARC (Palo Alto Research Center) によって発明
Xerox, intel, Dec によって Ethernet 2.0 を設定
IEEE 802.3

フレーム交換による通信
Ethernet フレームによる通信

伝送帯域
10Mbps ~ 100Mbps

データリンク層

LAN を中心とする IEEE802.x

Ethernet 802.3

Token Ring 802.5

IEEE802 データリンク層を 2 つのサブレイヤに分離

MAC (Medium access control)

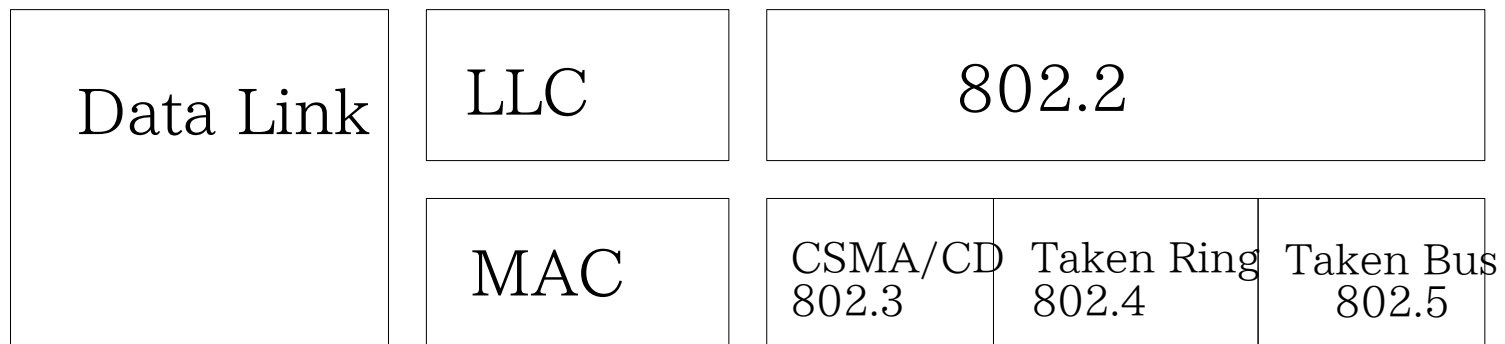
各 LAN に特有な問題

データが、どのように送れるか定義

LLC (Logical link protocol)

複数の上位層プロトコルがデータリンクを共用するためのフィールドを定義

論理アドレスを決定 (MAC)



Half-duplex/Full-duplex

Half-duplex (半2重通信)

送信中は受信不可能

CSMA/CD

Full-Duplex (全2重通信)

送信中に受信可能

伝送メディアを専有

例 switching HUB など

CSMA/CD 方式

Ethernet で採用

Carrier Sense

通信を行いたいステーションは聴取を行う。
他のステーションが通信中の場合は待機

Multiple Access

複数のステーションが同じメディアを共有

Collision Detection

通信中をメディアを監視

衝突を検出

衝突が検出されたら random に待って再送

CSMA / CD

A がデータ送信



衝突 ← B がデータ送信



B が衝突を検知

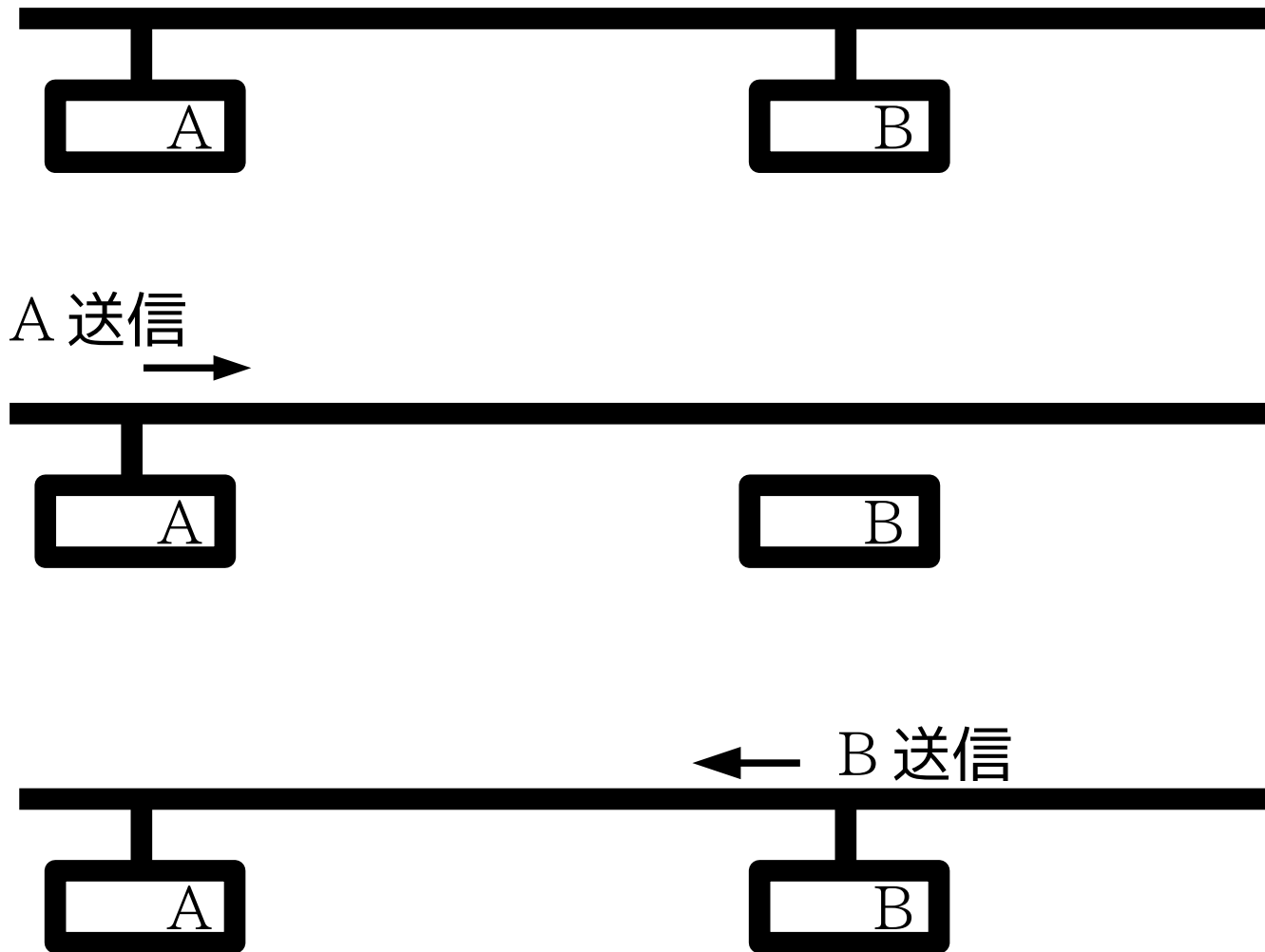


A が衝突を検知

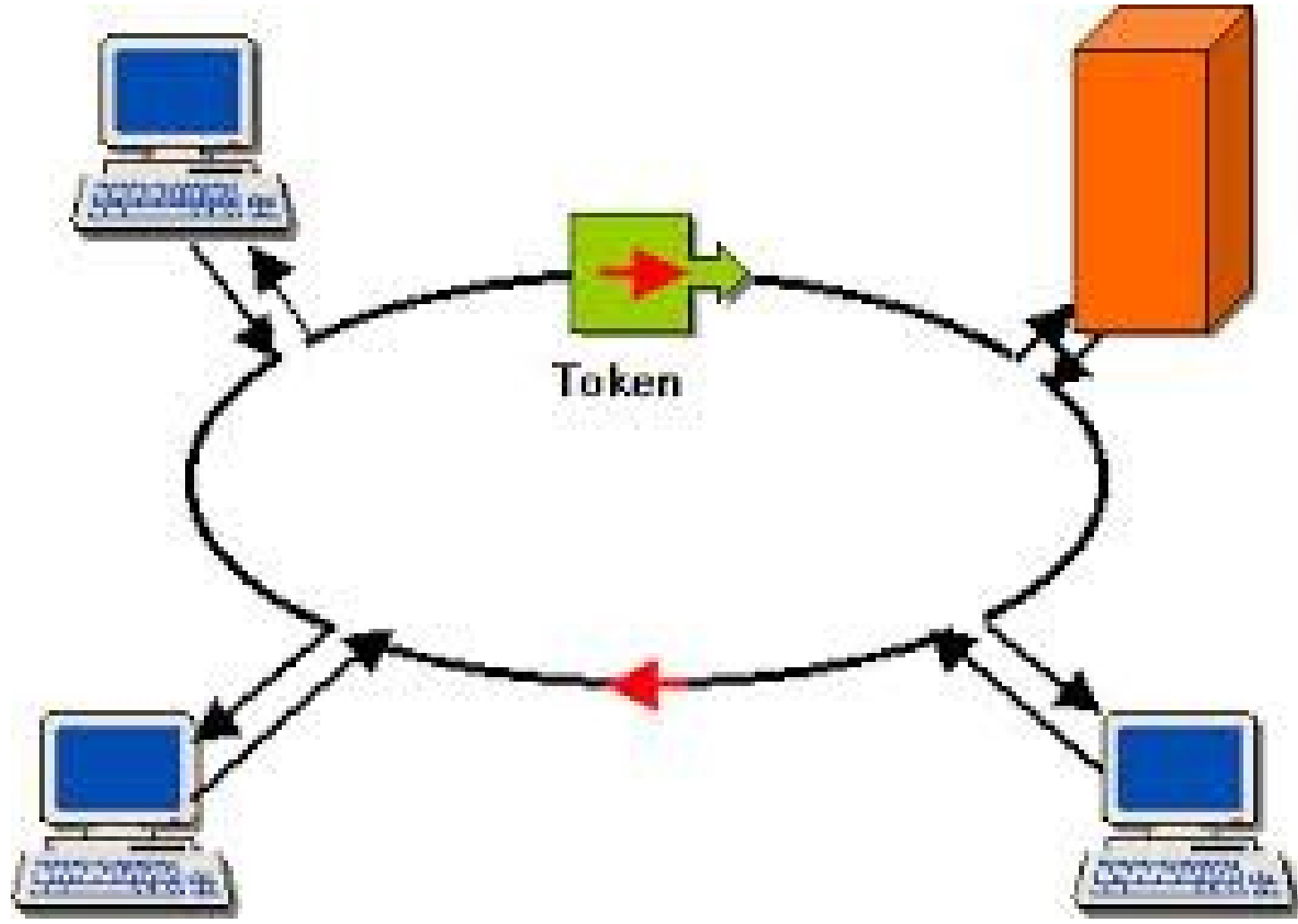


Aはランダム時間(1)
停止

Bはランダム時間(2)
停止



トークンリング



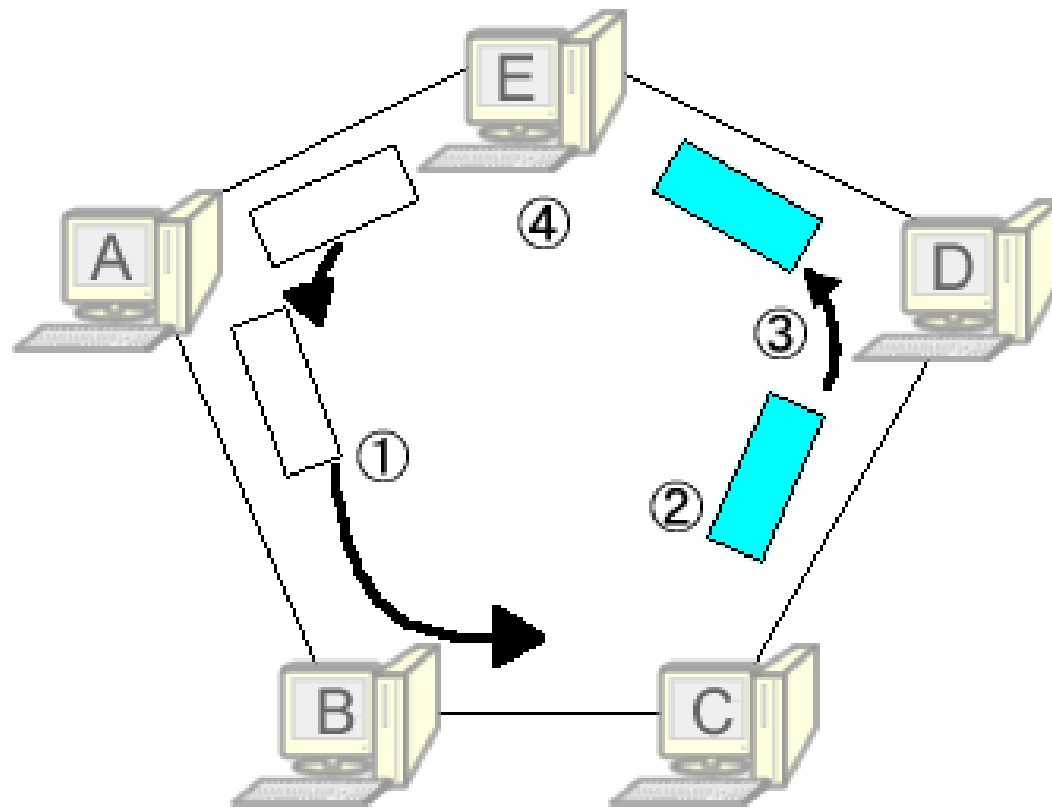
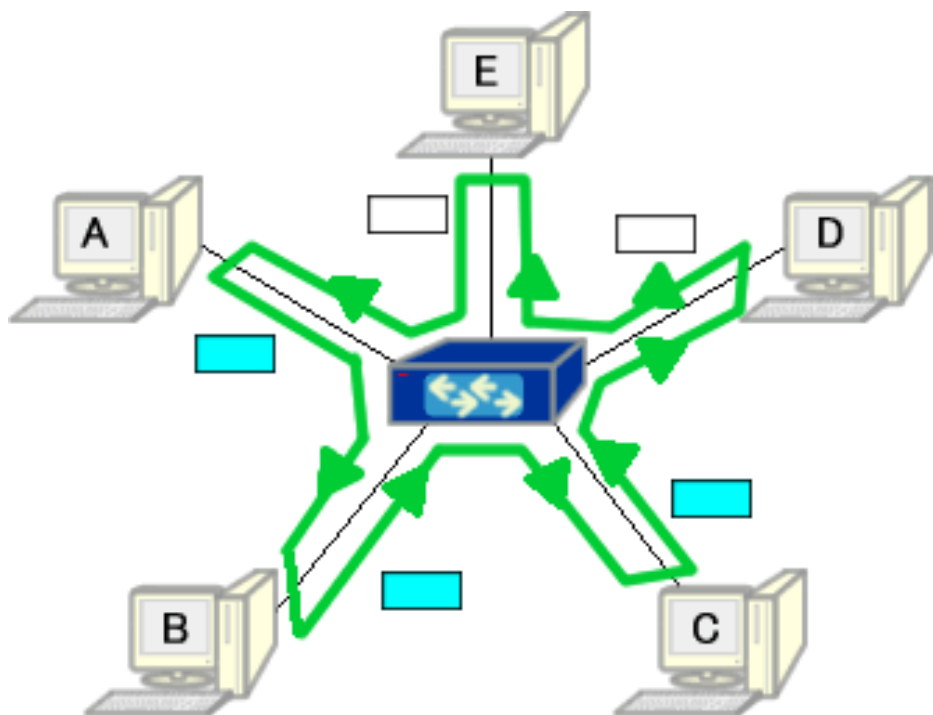


図 6.2.2 トークンパッシング方式



改良型トークンパッシング方式

● トークン

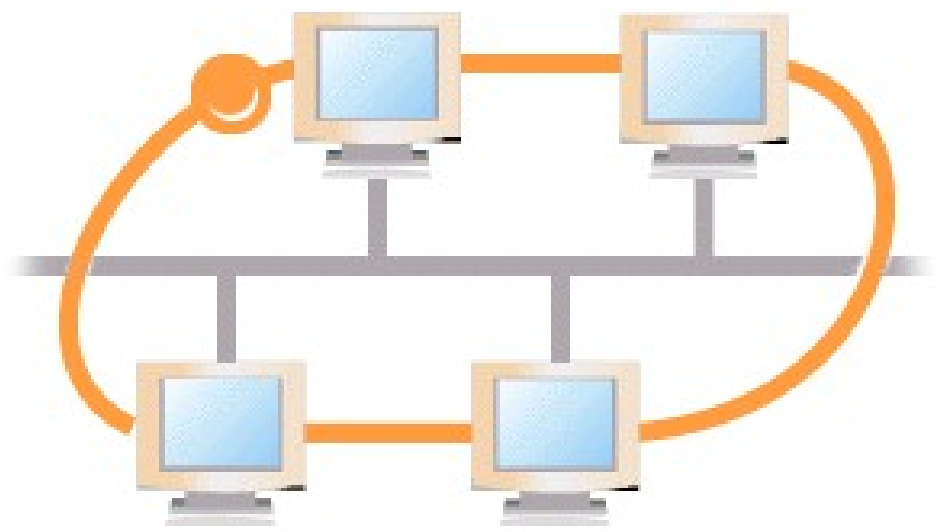


図 6.2.4 トークンパッシング・リング型
(トークン バス)

無線 LAN

規格	策定期期	変調方式	周波数帯	チャンネル幅	公称速度
IEEE 802.11	1997年6月	DSSS	2.4 - 2.5GHz		2Mbps
IEEE 802.11b	1999年10月	DSSS/CCK	2.4 - 2.5GHz	20M	11Mbps / 22Mbps
IEEE 802.11a	1999年10月	OFDM	5.15 - 5.35GHz 5.47 - 5.725GHz	20M	54Mbps
IEEE 802.11g	2003年6月	OFDM	2.4 - 2.5GHz	20M	54Mbps
IEEE 802.11j	2004年12月	OFDM	4.9 - 5.0GHz 5.03 - 5.091GHz	Japanese Only	54Mbps

規格	策定期期	変調方式	周波数帯	チャンネル幅	公称速度
IEEE 802.11n	2009年9月	OFDM	2.4 - 2.5GHz 5.15 - 5.35GHz 5.47 - 5.725GHz	20/40MHz MIMO (複数アンテナ) 64QAM	65Mbps - 600Mbps
IEEE 802.11ac	2014年1月	OFDM	5.15 - 5.35GHz 5.47 - 5.725GHz	80/160MHz 256QAM MIMO	290Mbps - 6.9Gbps
IEEE 802.11ad	2013年1月	シングルキャリア/OFDM	57 - 66GHz		4.6Gbps - 6.8Gbps

無線 LAN のセキュリティ

IEEE 802.11i

WEP → WPA

暗号化方式

1) WEP (Wired Equivalent Privacy)

鍵 40bit (128bit) 152 or 256 bit

2) WPA(Wi-Fi Protected Access)

TKIP (Temporal Key Integrity Protocol)

鍵 128bit

3) WPA2

AES (Advanced Encryption Standard)

((CCMP(Counter mode with CBC-MAC Protocol)))

暗号化方式	暗号化アルゴリズム	完全性の検証	WEP	WPA	WPA2
WEP	RC4	CRC32	必須	-	-
TKIP	RC4	Michael	-	必須	任意
CCMP	AES	CCM	-	任意	必須

ユーザー認証

認証方式 802.1x

方式	双方向認証	クライアント証明書	サーバ証明書
<u>EAP</u>	△	なし	なし
LEAP	○	なし	なし
FAST	○	なし	なし
PEAP	○	オプション	あり
TTLS	○	オプション	あり
TLS	○	あり	あり

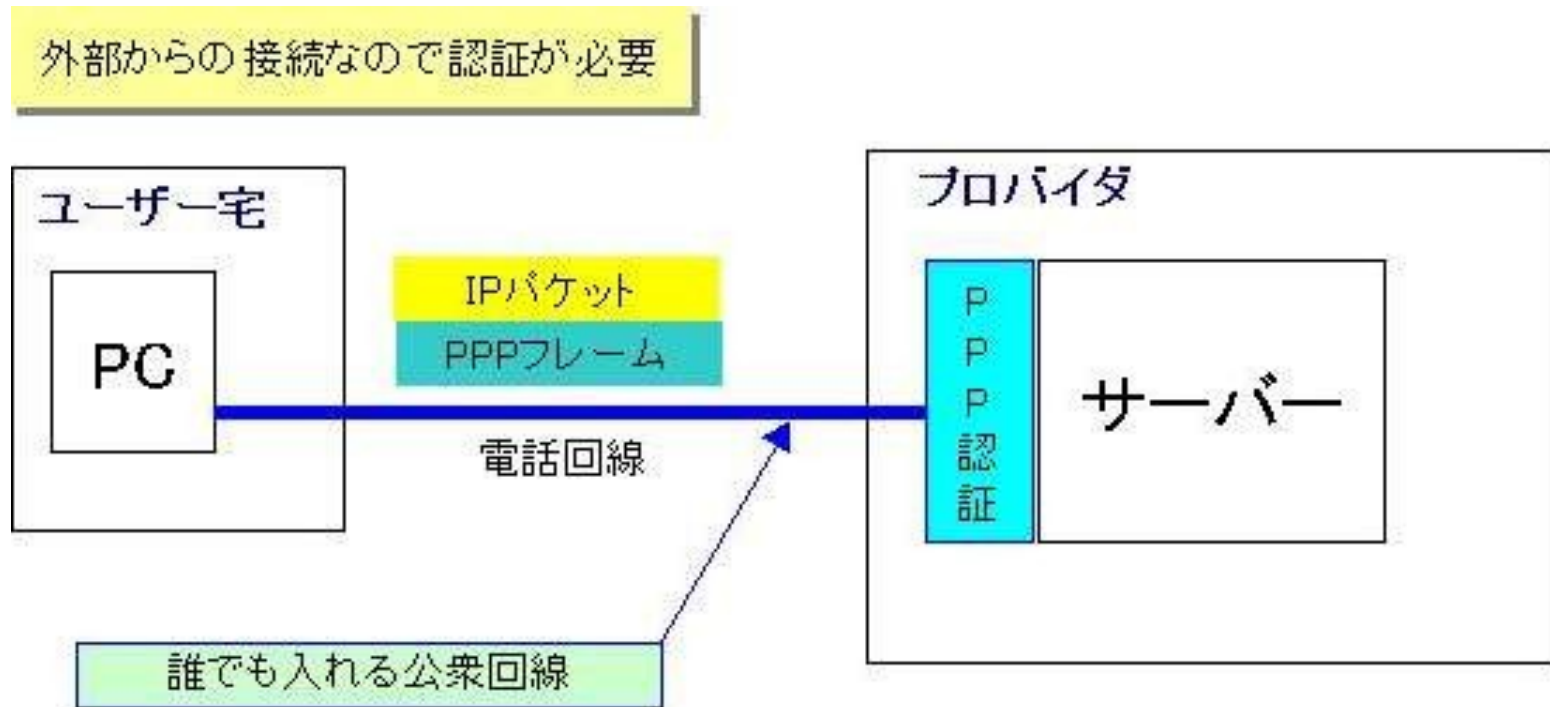
PPP
(Point of Point Protocol)

前身 SLIP

二台の機器の間で仮想的な専用の伝送路を確立し、相互に安定的にデータの送受信

PPPoE
(PPP over Ether)
Ethernet フレームに PPP フレームを追加

PPP (Point to Point Protocol)



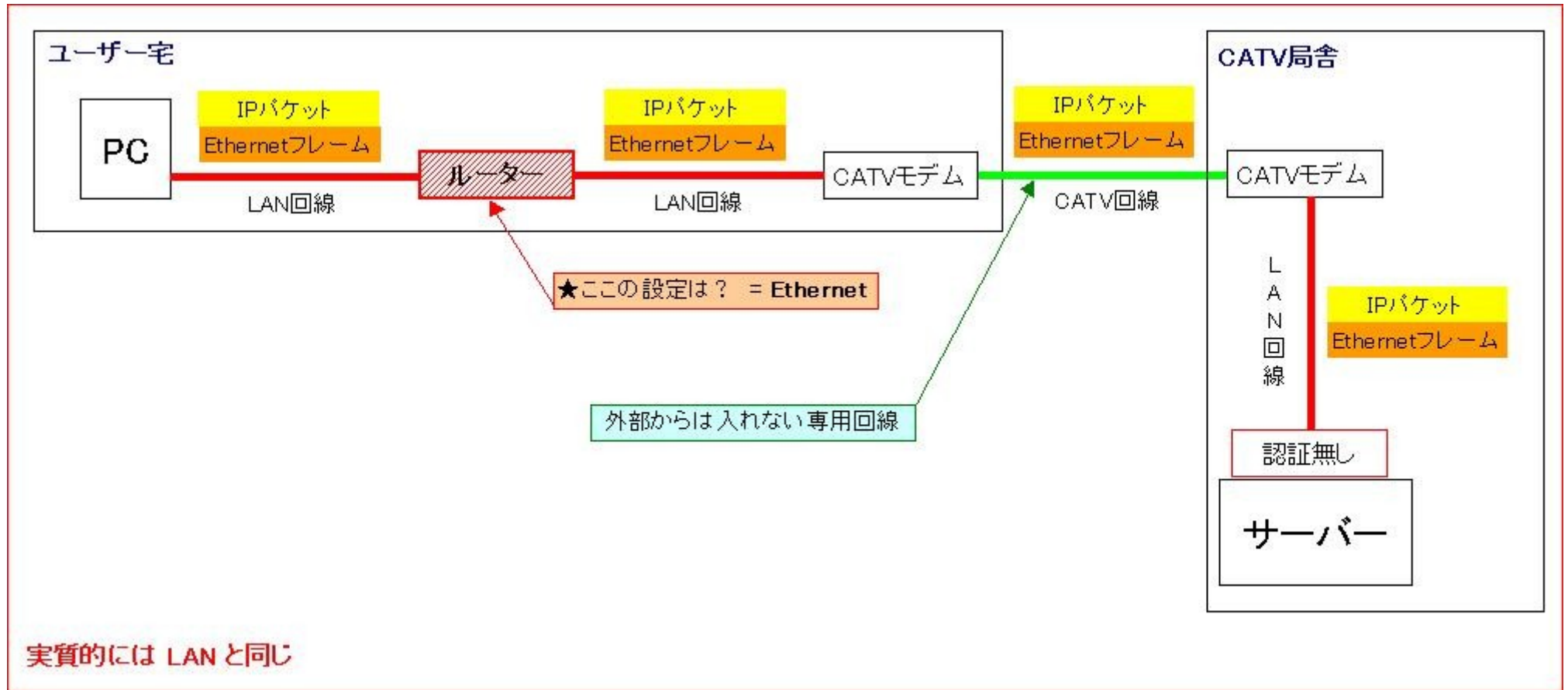
■ Ethernet

内部からの接続なので認証の必要無し



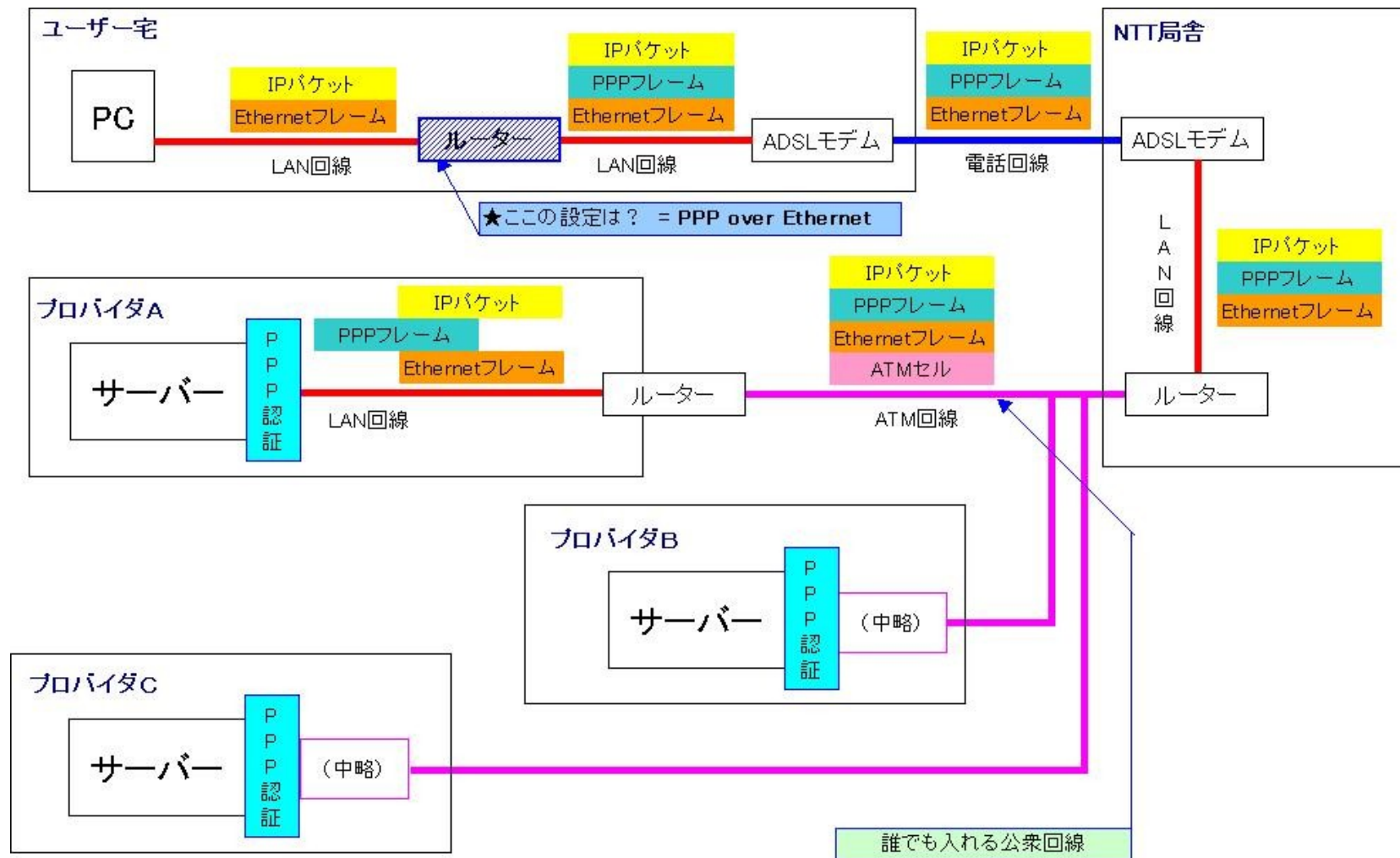
★ ルーター (CATV回線)

使用プロトコル: Ethernet

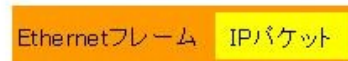


★ ルーター (フレッツ ADSL)

使用プロトコル：PPPoE (PPP over Ethernet)

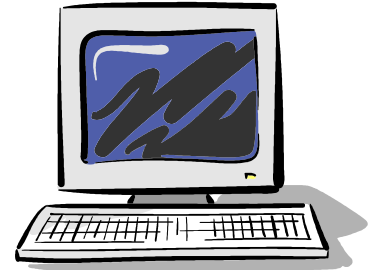


これが PPPoE だ！
正確には右図のように
カプセル化する。



データリンク層のアドレス

MAC アドレス



宛先の指定、発信元の指定に用いる Mac address: 00:D0:B7:60:A5:5

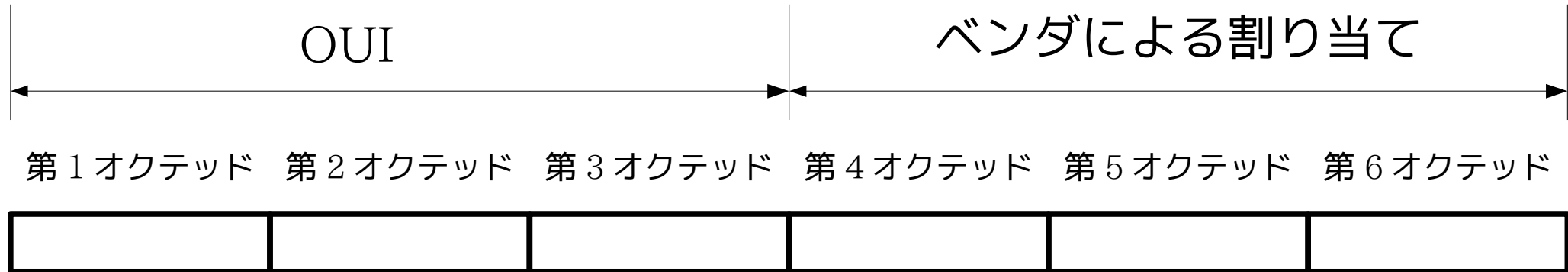
ノードを識別

通信機器毎にユニークなアドレス (48 bits)

固定で割り当て

NIC (Network Interface Card) が管理

MAC アドレス



OUI (organization unique identification) ベンダーコード
ベンダに割り当てられる固定値
1つのベンダは複数の OUI を取得可能

G/I グループアドレス ブロードキャストアドレス

G/L 0:IEEE によって割り当てられたアドレス
1:自由に使用できるアドレス

Ethernet Frame

データリンク層では Frame の単位でデータの通信

宛先、発信元の指定

誤りの検出

Frame Format

Ethernet format

プリアンブル 8(byte)	宛先 アドレス 6	送信元 アドレス 6	Type 2	データ 46~1500	FCS 4
-------------------	-----------------	------------------	-----------	----------------	----------

IEEE 802.3 format

プリアンブル 7(byte)	S F P	宛先 アドレス 6	送信元 アドレス 6	長さ	SDC SST AAL PP	データ 43~1497	FCS 4
-------------------	-------------	-----------------	------------------	----	-------------------------	----------------	----------

プリアンブル

受信柄がビット同期をとるためのフィールド

101010101010101.....01011(64bit)

フレームデータの先頭を識別

ネットワーク層 (TCP/IP)

パケットを提供

ネットワーク内のノード間でのデータ交換機能

End System 間の通信の定義

ノードに対するアドレスの付与

パケットの定義

ES,IS のアドレスの構造

パケットの形式

パケットの経路制御

同報通信

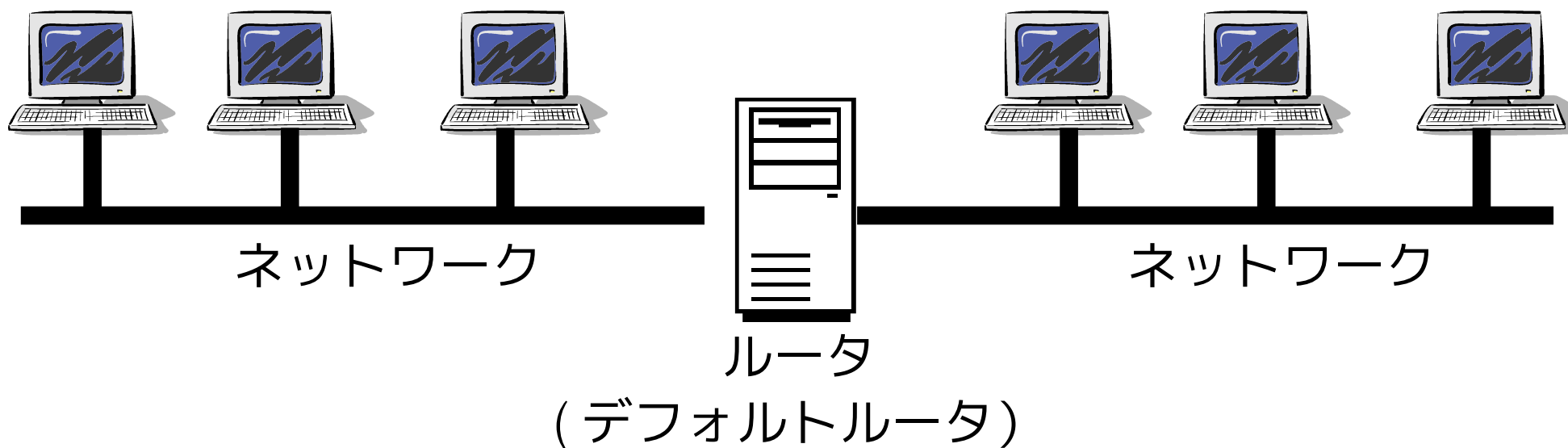
ネットワーク層

ネットワークの接続

IP の基本

パケットリレー方式

中継ノードは自分宛の packets でなければ次へ
判断は、ネットワーク層
転送はリンク層



IP の基本

パケットリレー方式

中継ノードは自分宛の packets でなければ次へ

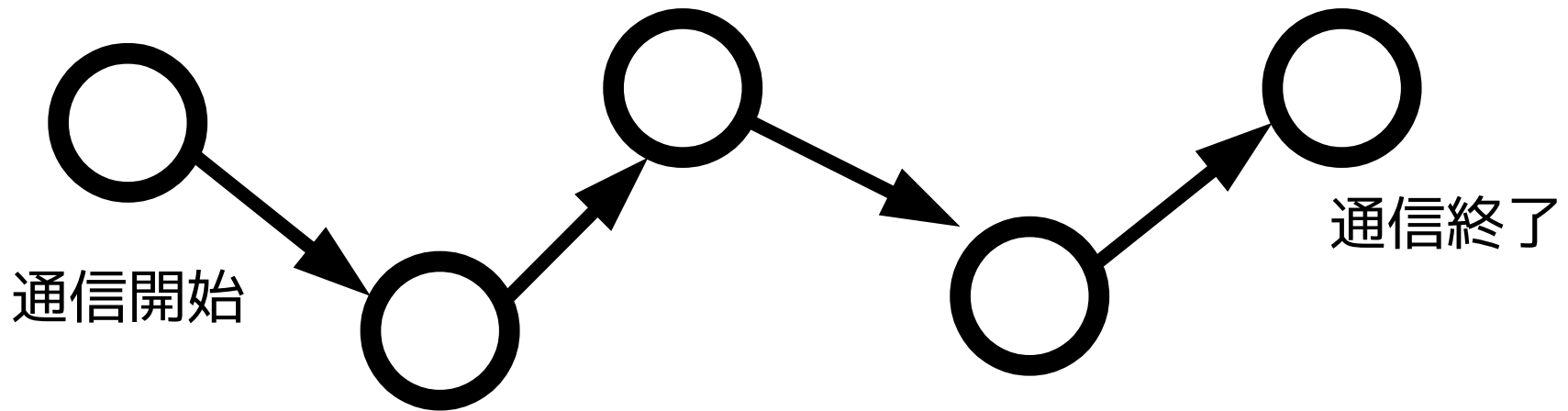
判断は、ネットワーク層

転送はリンク層

ベストエフォート方式

中継ノードは、パケットを捨てたら報告

ICMP echo message



IP アドレス

インターネットプロトコルの識別子

V4 32 bits 192.168.0.1

相手と自分を認識

表記方法 通常、10進

IP アドレスの構造

アドレス構造

ネットワーク部とホスト部から構成

ネットマスクによる柔軟な構造

階層的にネットワークを管理

複数のネットワークを 1つのアドレスで管理

Ver	IHL	TOS	Total Length
Identification	Flag	Fragment offset	
TTL	Protocol	Header CheckSum	
Source IP Address			
Destination IP Address			
Destination IP Address			



4 octets

IP ヘッダ

Ver version 現在は 4

IHL ヘッダの長さ 4octet を 1 としてカウント

TOS Type of Service 配送のタイプ

Total Length Ip データグラム全体の大きさ

TTL time to live

データグラムの寿命

1つのホストを経由すると 1つ減る

初期値は 64

Protocol 上位層は何か？

Header CheckSun

Header 部分の検証 (データが壊れていないか？)

IP アドレス (ネットワークの接続)

グローバルアドレス

(世界で1つだけのアドレス 日本 JPNIC が管理)

プライベートアドレス

(自由に使用しても良いアドレス 世界中に複数あり。
グローバルアドレスとのルーティングは不可)

プライベートアドレス

Class A	1個	10.0.0.0 ~ 10.255.255.255.
Class B	16個	172.16.0.0 ~ 172.31.255.255
Class C	256個	192.168.0.0 ~ 192.168.255.255

ネットワーク層のアドレス

IP アドレス

Class A	0XXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX
Class B	10XX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX
Class C	110X	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX
Class D	1110	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX
Class E	1111	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX

IP V4 32 bits

IP アドレスのクラス

- Class A 1つのネットワークに最大 1677261 台接続可能
- Class B 1つのネットワークに最大 65536 台接続可能
- Class C 1つのネットワークに最大 256 台接続可能

IP アドレスと物理アドレスの対応

IP アドレスはネットワーク層での識別

実際にデータを送るときは、リンク層のアドレスが必要

ARP による解決

データグラムの転送前に行われるアドレス解決方法

ARP

Address Resolution
Protocol

IP アドレスと MAC アドレスの対応

IP アドレス : ルーティングに必要な ネットワーク層での識別
MAC アドレス : 実際の機械の固有アドレス

< 実際にデータを送るときは、MAC アドレスが必要 >

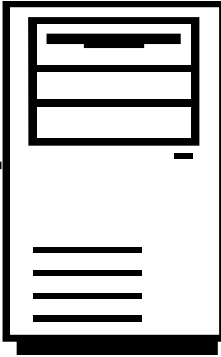
ARP: 機械を立ち上げたときや、一定時間ごとに行われる
IP アドレスと MAC アドレスの対応表

IP address :192.162.0.11
Mac address: 00:01:80:0E:CD:5B

IP address :192.162.0.13
Mac address: 00:90:45:FE:D0:53



ルータ



ネットワーク 192.162.0.0

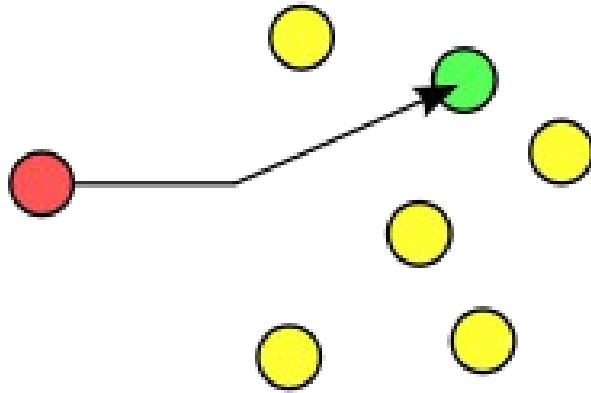
IP address :192.162.53.34
Mac address: 00:D0:B7:60:A5:5M

IP address :192.162.53.13
Mac address: 00:0D:61:31:1B:1B

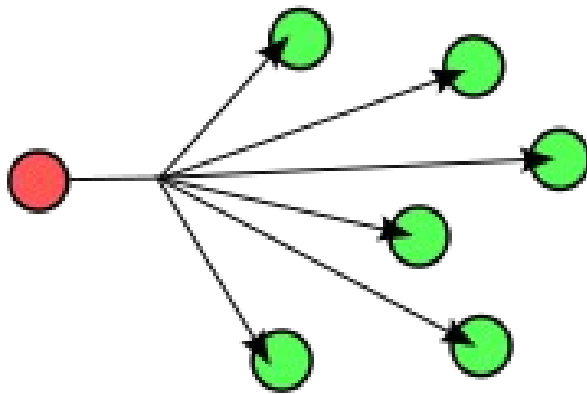


ネットワーク 192.162.53.0

ルーティングトポロジー

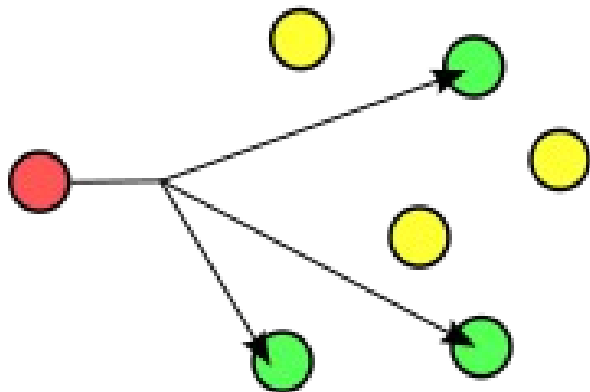


ユニキャスト
(default)



ブロードキャスト
(ARP)

チェルノブイリパケット



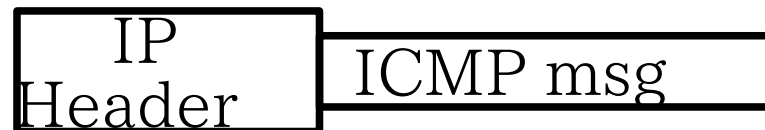
マルチキャスト
(放送)

IP-V4 では脆弱

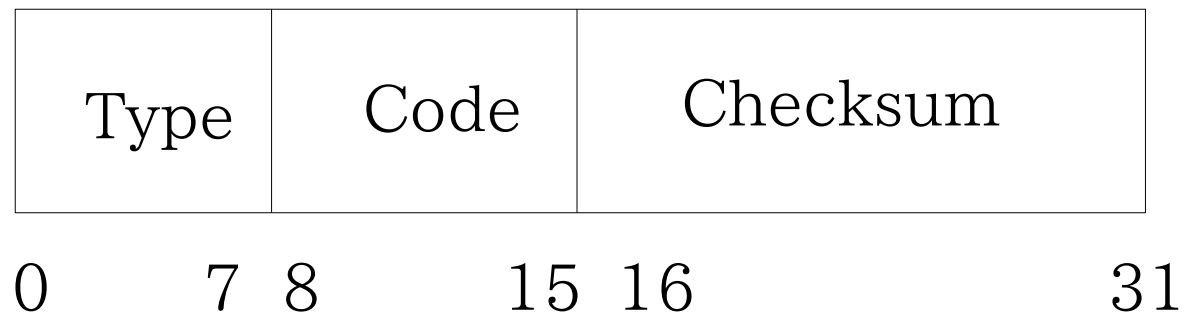
ICMP

Internet control message protocol
(RFC792)

address-mask request
ICMP time-stamp request
ICMP information request
ICMP echo request



ICMP msg の形式



タイプ フィールドには 15 種類

コード フィールドには特定の状態を示す値

チェックサム フィールドには ICMP msg 全体をカバー

Ping ICMP

IP ルーティング (TCP/IP の骨格)

シンプルな構造

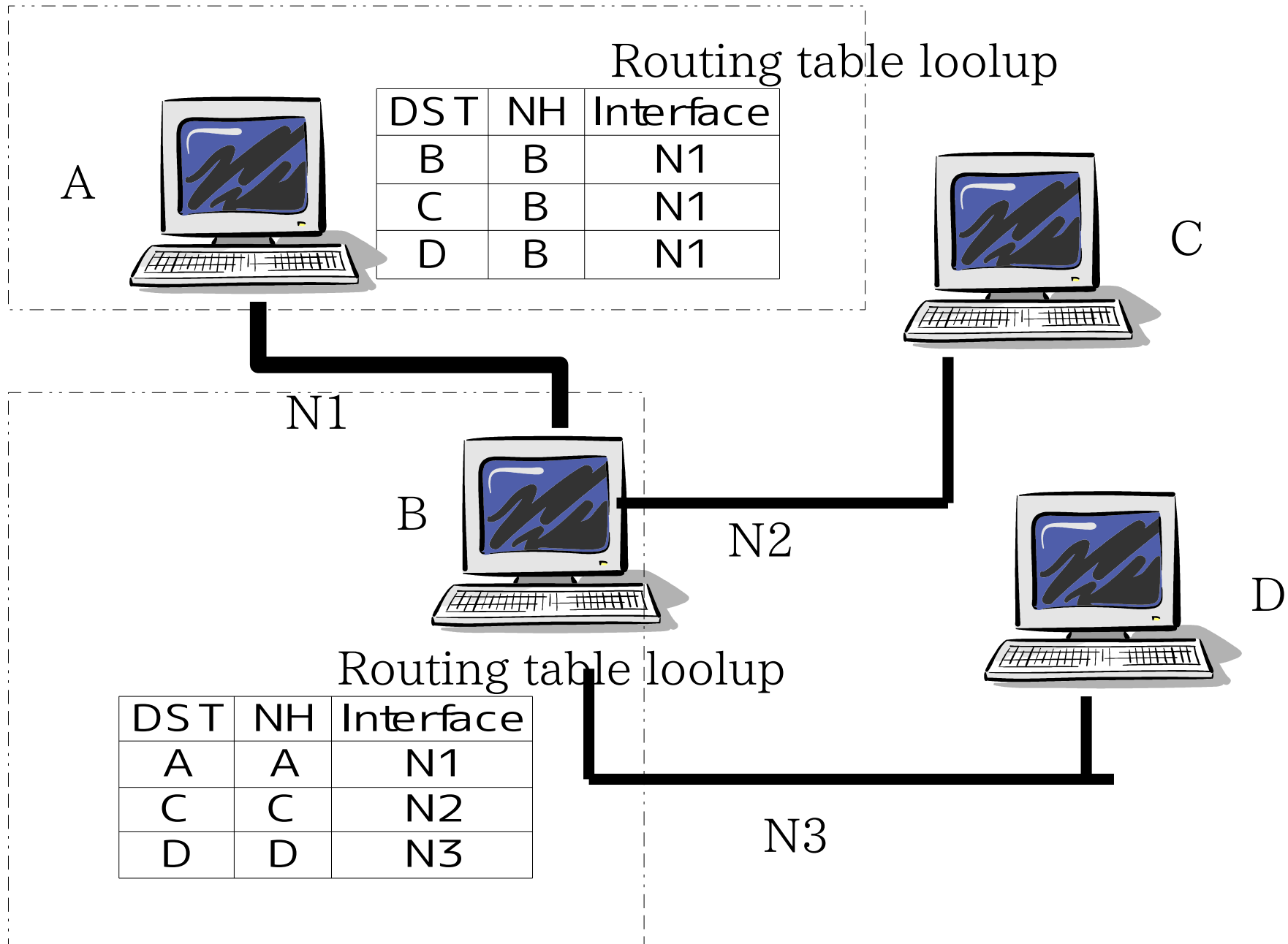
宛先が共有 (同一) ネットワーク → 直接転送

宛先が別のネットワーク → デフォルトルータへ転送

ルーティングテーブル

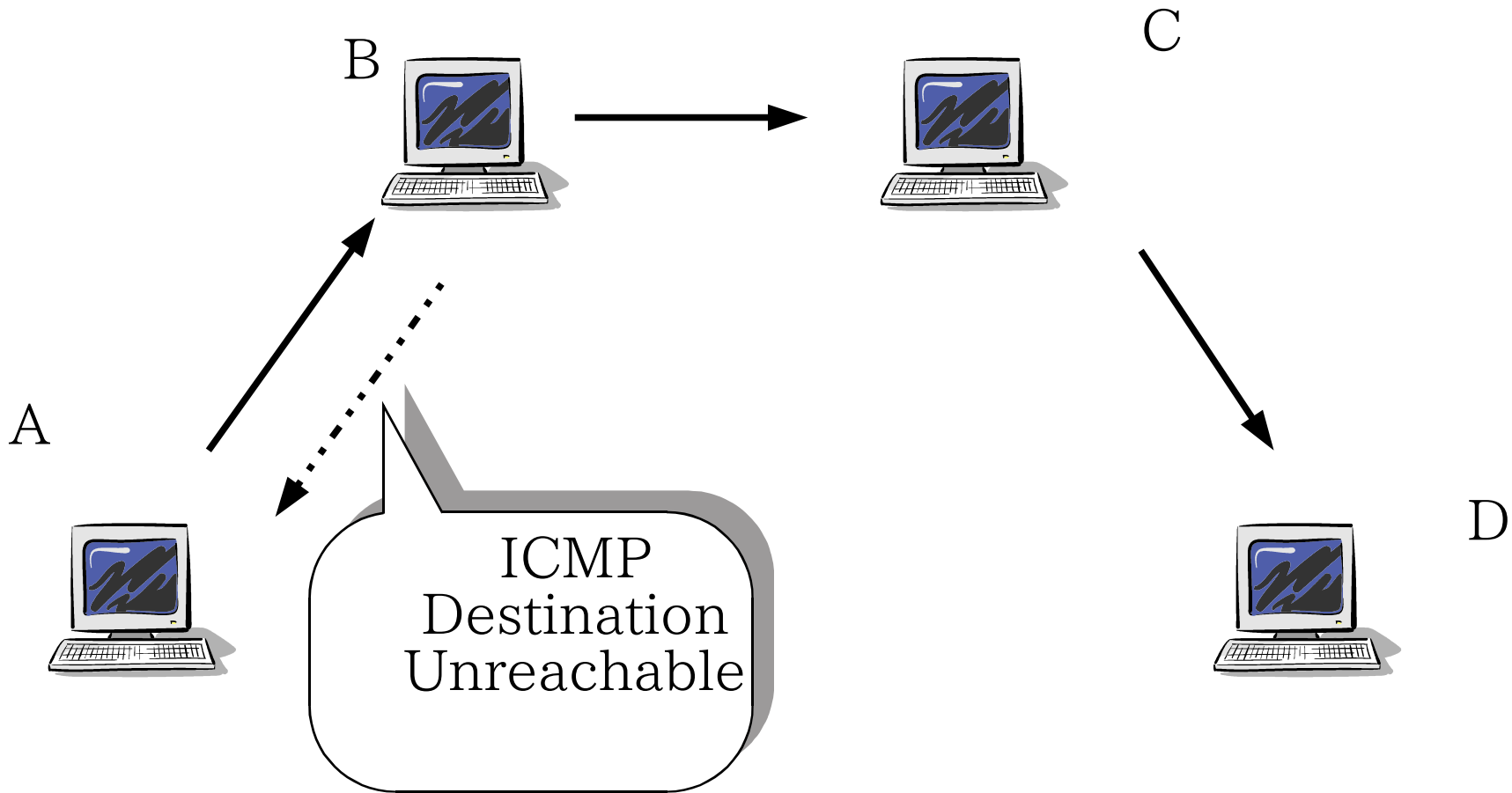
終点	次のホイップ	方向(interface)
終点	次のホイップ	方向(interface)
終点	次のホイップ	方向(interface)
終点	次のホイップ	方向(interface)

IP forwarding



No Route to Host

BがDへの経路をもたない。



経路制御

静的経路制御 (static routing)

人間が手で経路を設定 route

コンピュータが複雑になると、大量の設定が必要

動的経路制御 (Dynamic routing)

RIP, IGRP,.....,

コンピュータが時動的に経路を計算

迂回回路があれば、自動的に経路を交換

A



宛先	ルータ	インターフェース
Default(0.0.0.0)	192.168.0.254	Eth0
192.168.0.0	Default(0.0.0.0)	Eth0

C



eth0
192.168.0.1

eth0
192.168.0.254

eth0
192.168.0.2

B



宛先	ルータ	インターフェース
192.168.0.0	Default(0.0.0.0)	Eth0
192.168.1.0	Default(0.0.0.0)	Eth1

eth0
192.168.1.1

Eth1
192.168.1.254

eth0
192.168.1.2



宛先	ルータ	インターフェース
Default(0.0.0.0)	192.168.1.254	Eth0
192.168.1.0	Default(0.0.0.0)	Eth0

D

Static routing

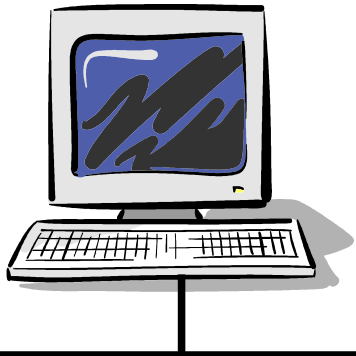
Default gateway を利用した

例



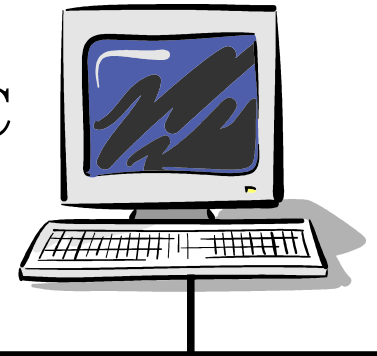
E

A



宛先	ルータ	インターフェース
192.168.0.0	192.168.0.1	Eth0
192.168.1.0	192.168.1.254	Eth0

C

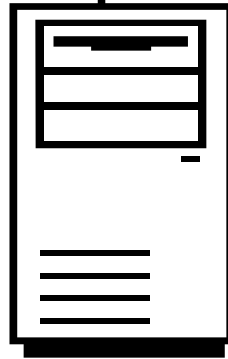


eth0
192.168.0.1

eth0
192.168.0.254

eth0
192.168.0.2

B



宛先	ルータ	インターフェース
192.168.0.0	192.168.0.254	Eth0
192.168.1.0	192.168.1.254	Eth1

eth0
192.168.1.1

Eth1
192.168.1.254

eth0
192.168.1.2

D



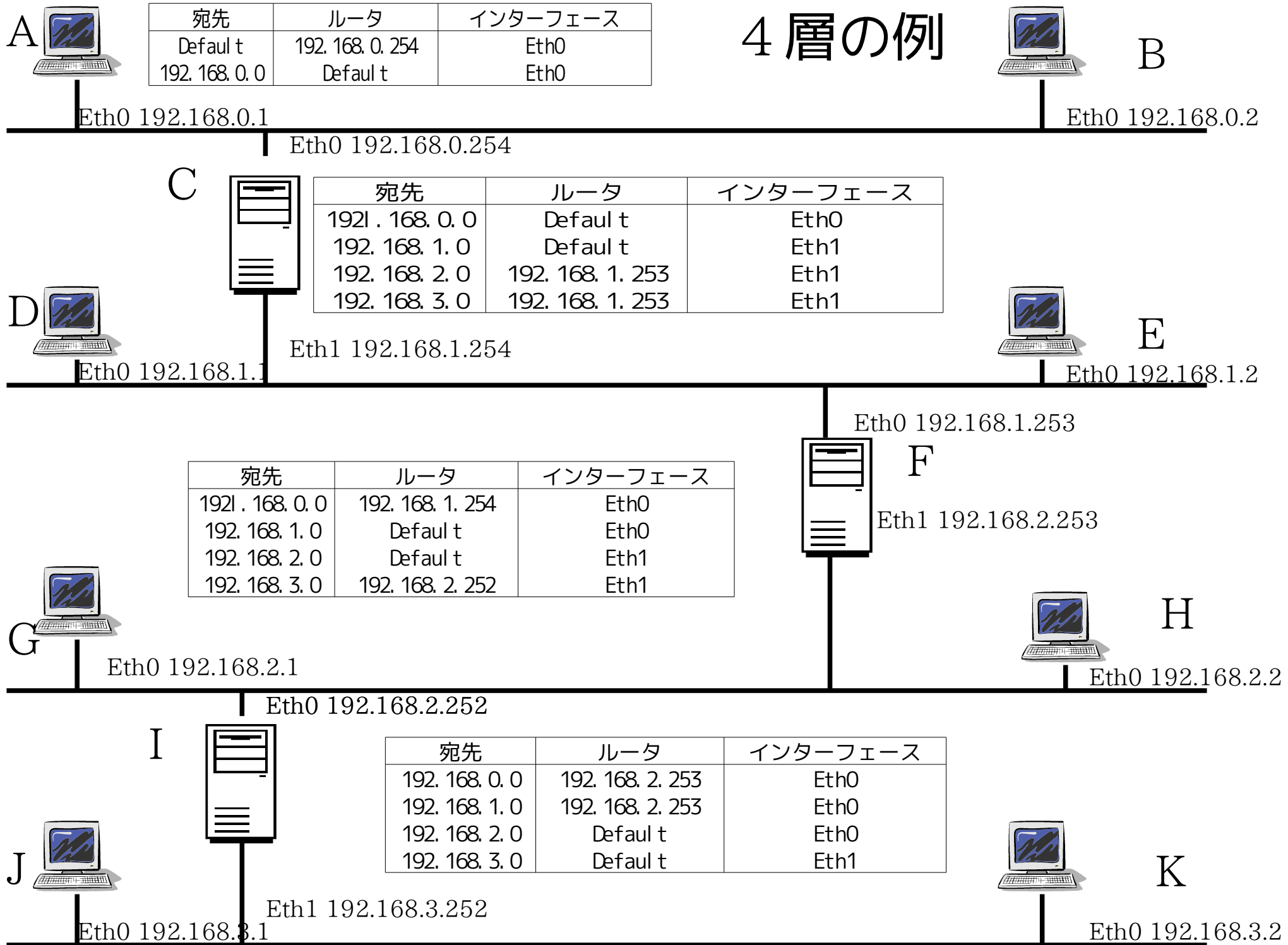
宛先	ルータ	インターフェース
192.168.1.0	192.168.1.1	Eth0
192.168.0.0	192.168.1.254	Eth0

Static routing

E



4層の例



ルーティングアルゴリズム RIP

隣接ルータと経路表を交換
経路表をブロードキャスト

コストはホップ数
distance vector 型アルゴリズム
通知されたコスト +1
16 ホップを無限に接続

経路表の更新

必要に応じて経路表を更新

経路表にない経路が通知された場合

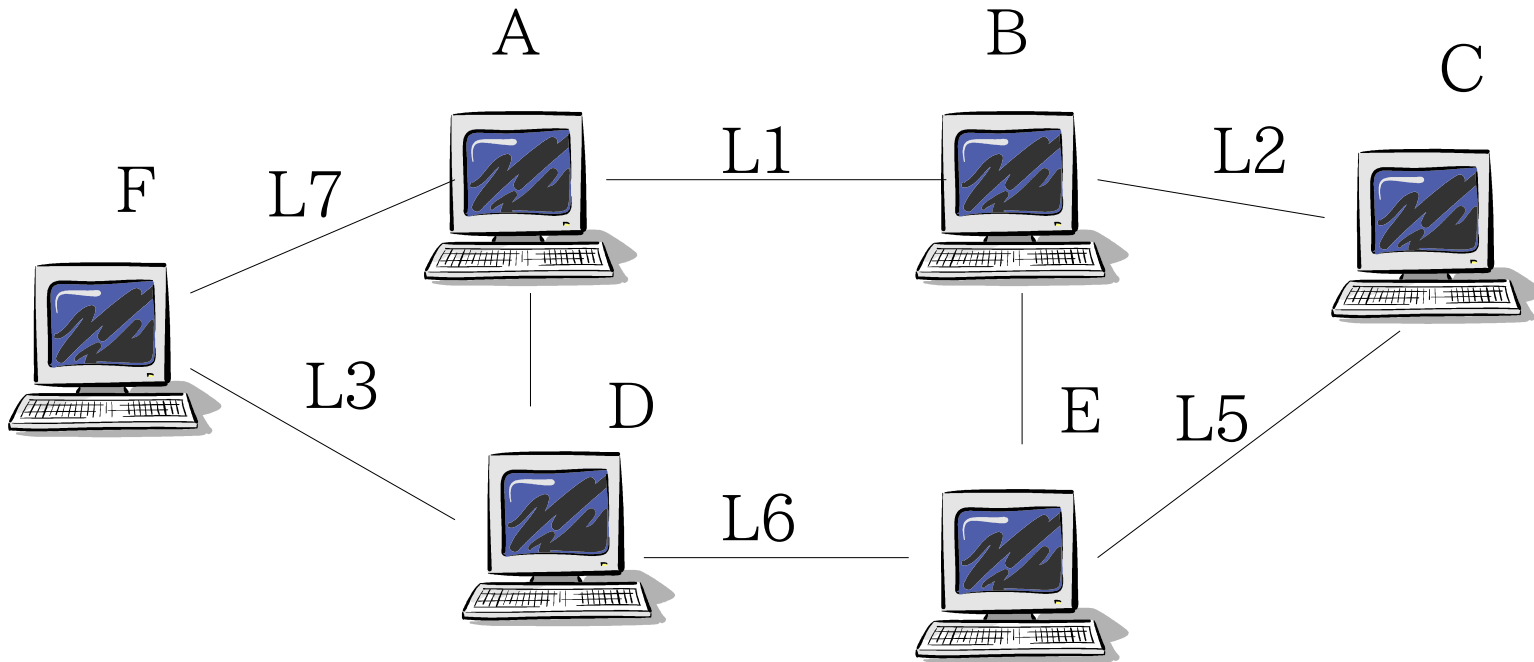
終点までコストが低い経路が通知された場合

経路表のネクストホップから通知された場合

各ルータは 30 秒毎に経路表を通知

トポロジの変化への対応

180 秒通知がない場合、経路は切断とする。



From E to	Link	Cost
E	Local	0
B	L4	1
C	L5	1
D	L6	1
A	L6	3

OSPF

Open Shortest Path First

リンクステート型アルゴリズム

Loop Free

計算量 多い

信頼性あり

IP に最適化

IAB が推奨

Hello Sub-protocol

リンク、ネットワークの接

続監視

LSA Flooding

ルータの接続情報

経路制御情報の伝搬

SPF 計算

トポロジの計算

Area functionality

経路制御ドメインの分割

他のルーティングプロトコル

IS-IS (Intermediate System-intermediate System)

IGRP (Interior gateway Routing Protocol)

EIGRP (Enhanced IGRP)

IP V 4 の問題点

アドレス空間の枯渇

IP アドレス 32 bit 43 億

経路制御情報の氾濫

現在 41000 経路

ユーザ環境の変化

通信の継続性

モバイルコンピュータ

通信の実時間性

画像、音声通信

セキュリティ

IP V6

広がるインターネットへの対応

利用者数 ホスト数の増加

経路制御情報の増加

環境の変化への追従

小型化、高性能化、廉価

移動ホスト

実時間通信

セキュリティとプライバシー

トランスポート層 (TCP/IP)

データ転送の信頼性を確保するための方式を定めたもの。

TCP

高い信頼性を実現するためのプロトコル
信頼性の保証メッセージの順番の保証,
受信確認, 誤り時の再送を提供

UDP

信頼性の保証なし
データグラムの到達保証, 順番保証の機能なし
アプリケーション依存

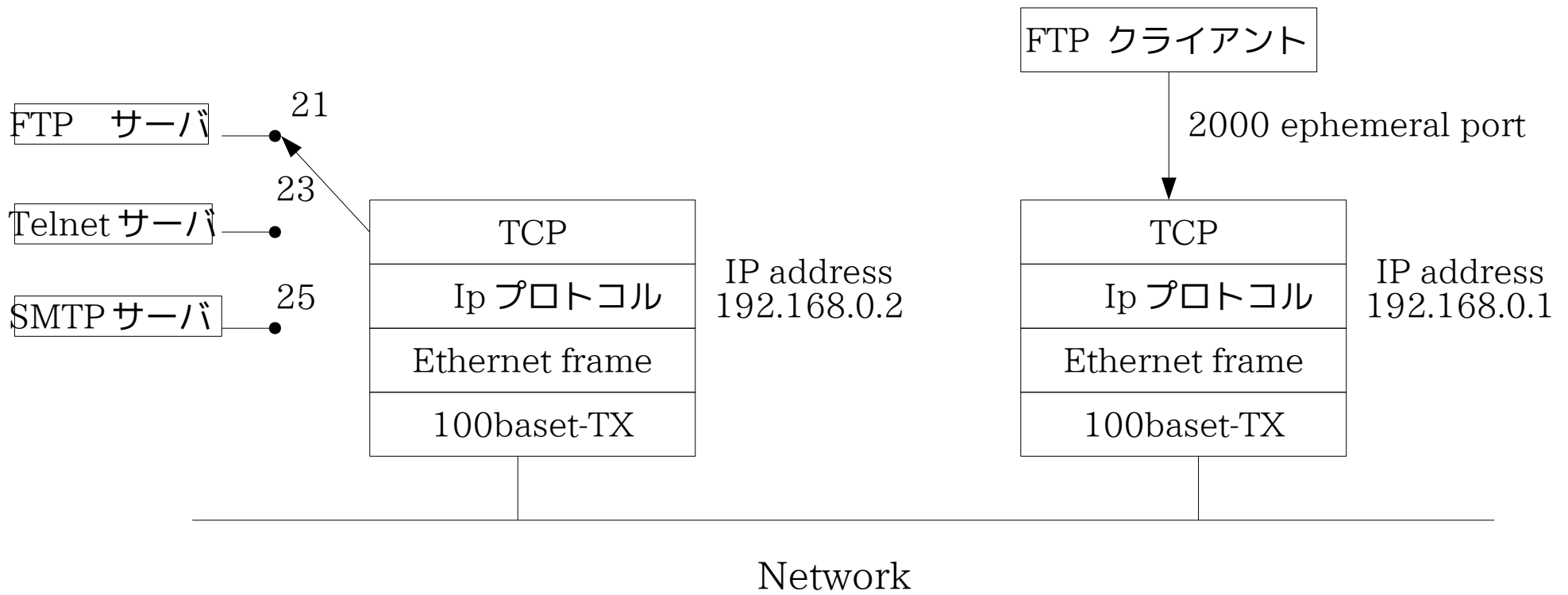
最大メッセージ長が規定

IP プロトコルをそのままアプリケーションに提供

トランスポート層の port

アプリケーション	ポート番号	種類
Ftp	21	TCP/UDP
Telnet	23	TCP/UDP
Smtp	25	TCP/UDP
Domwin	53	TCP/UDP

Well known Port Number



FTP のポート制御

FTP のアソシエーション

プロトコル	FTP
送信元IP address	192.168.0.1
送信元ポート番号	2000
受信元IP address	192.168.0.2
受信元ポート番号	21

1

16

32

Bits

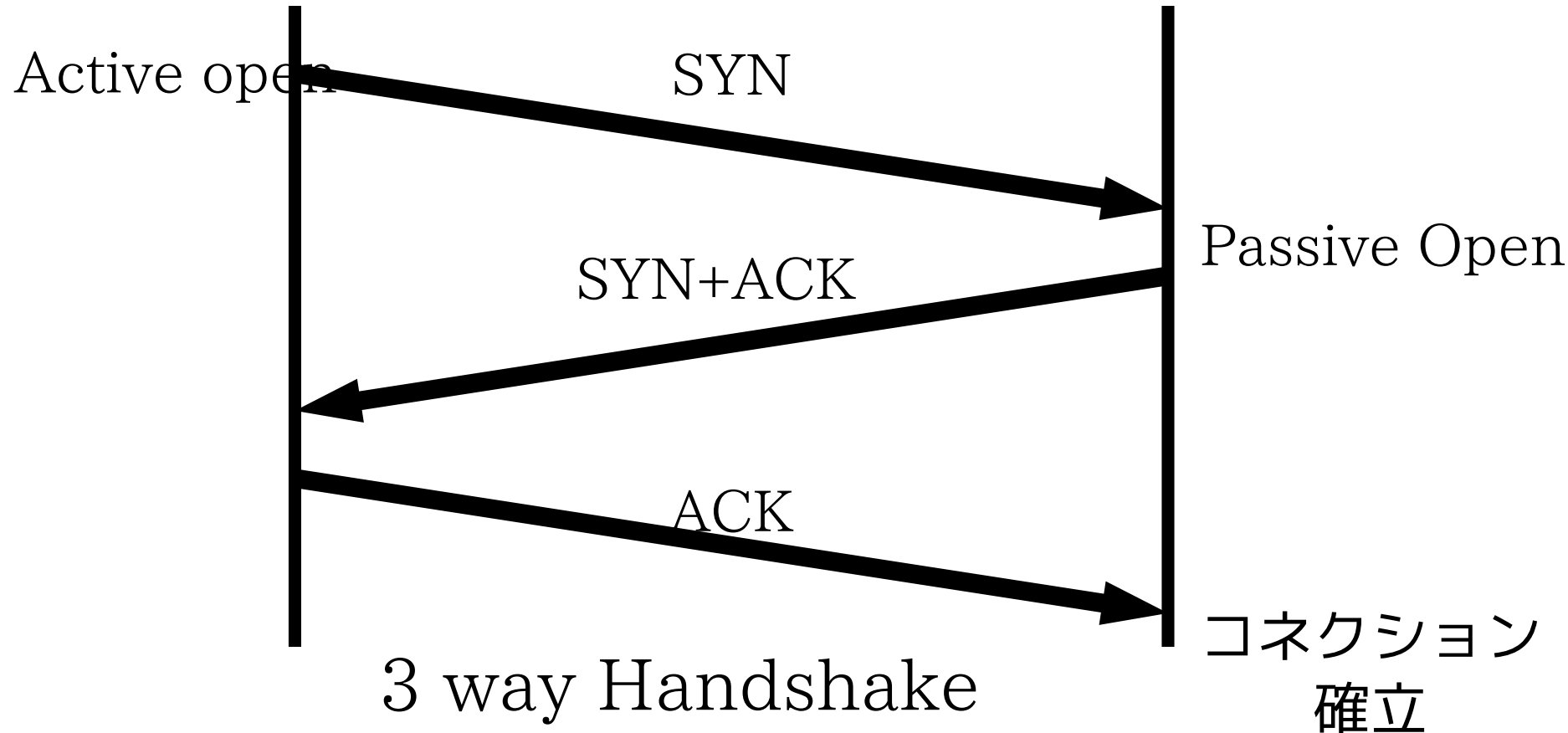
SRC PORT: 送信元ポート番号			DEST PORT: 宛先ポート番号		
SEQ: 送信用順序番号			ACK: 応答確認番号		
OFF	RES	Code Bit	Window		
Checksum			Uegent Pointer: 緊急ポインタ		
Option: オプション					
データ					

TCP セグメント

URG	Urgent Flag
	緊急に処理すべきデータ
ACK	Acknowledgement Flag
	確認応答番号フィールドが有効
PSH	Push Flag
	できるだけ早くデータをアプリケーションに渡す
SYN	Synchronize Flag
	コネクションの確立要求
FIN	Fin Flag
	通信の終了

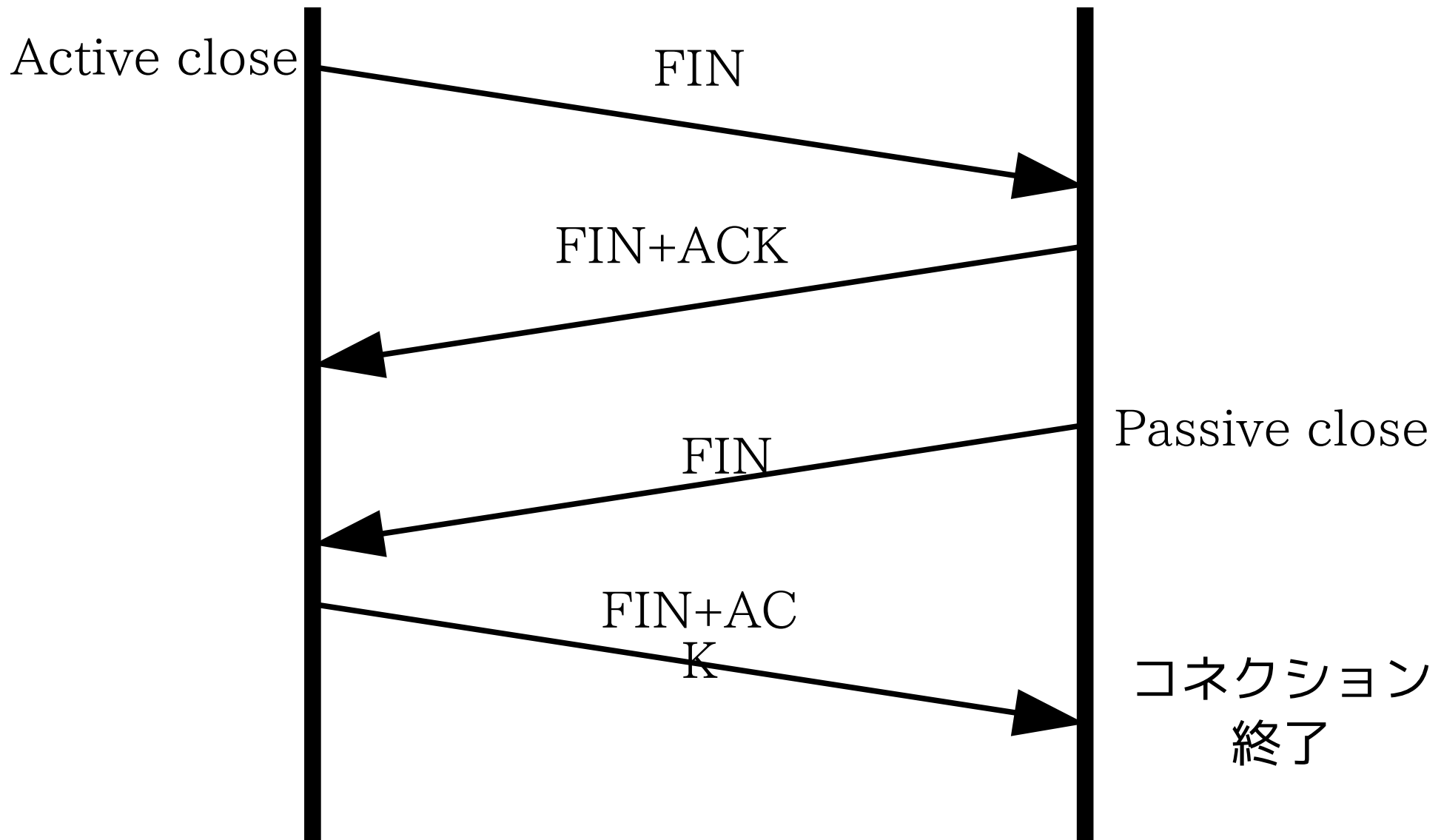
TCP FLAG

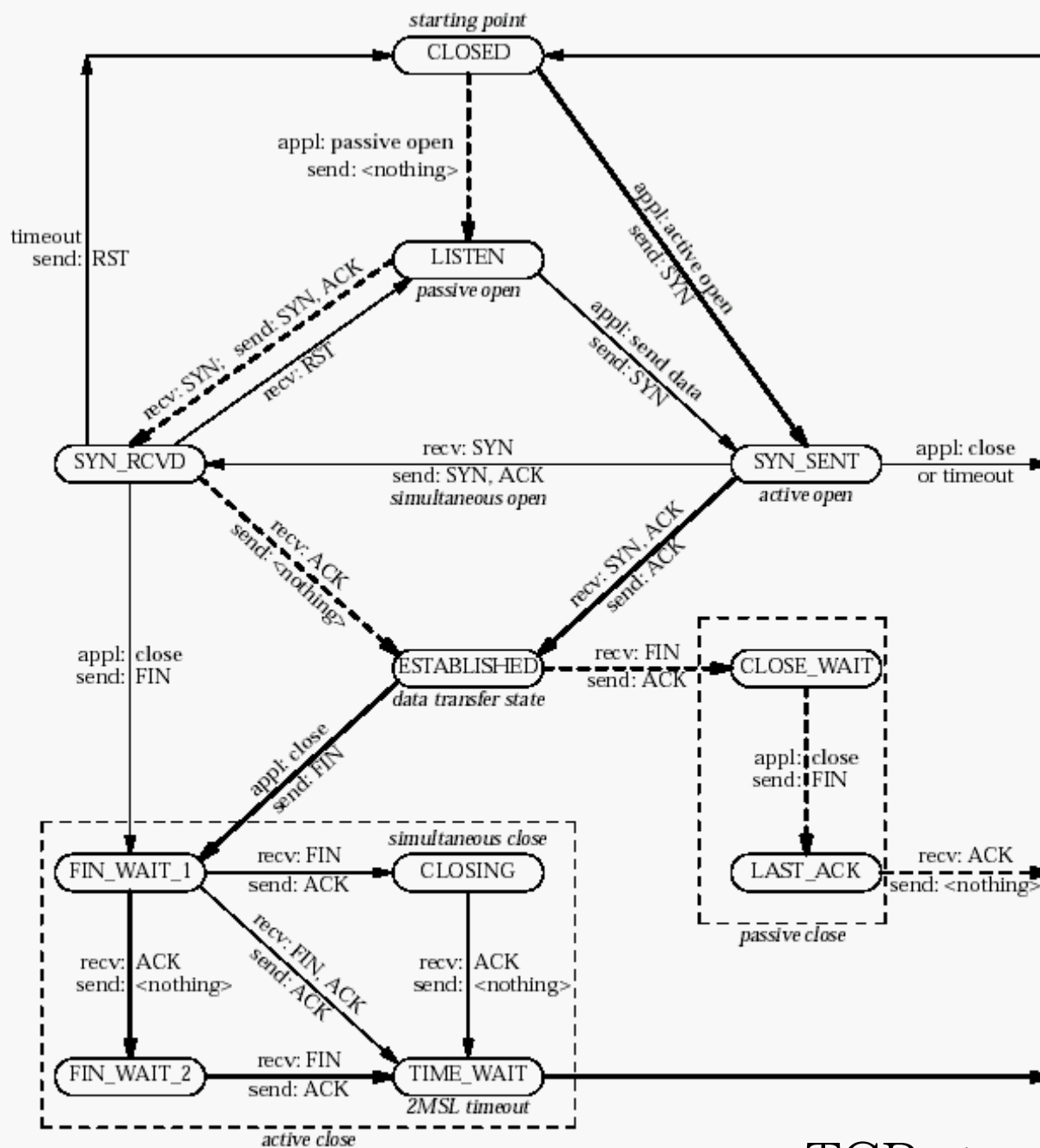
TCP におけるコネクションの確立



セッションコントロール
(内部から接続可能. 外部から接続不可能)

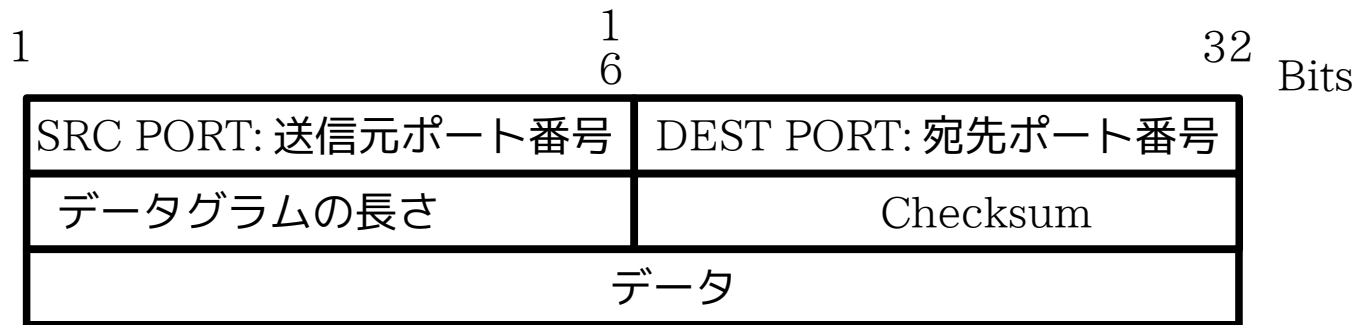
TCPにおけるコネクションの終了





—→ normal transitions for client
 - - - → normal transitions for server
 appl: state transitions taken when application issues operation
 recy: state transitions taken when segment received
 send: what is sent for this transition

TCP stage diagram



UDP セグメント

パケットフィルタ (firewall)

送信元 Mac address

データ転送量

宛先 Mac address

1日あたりのトラフィック量

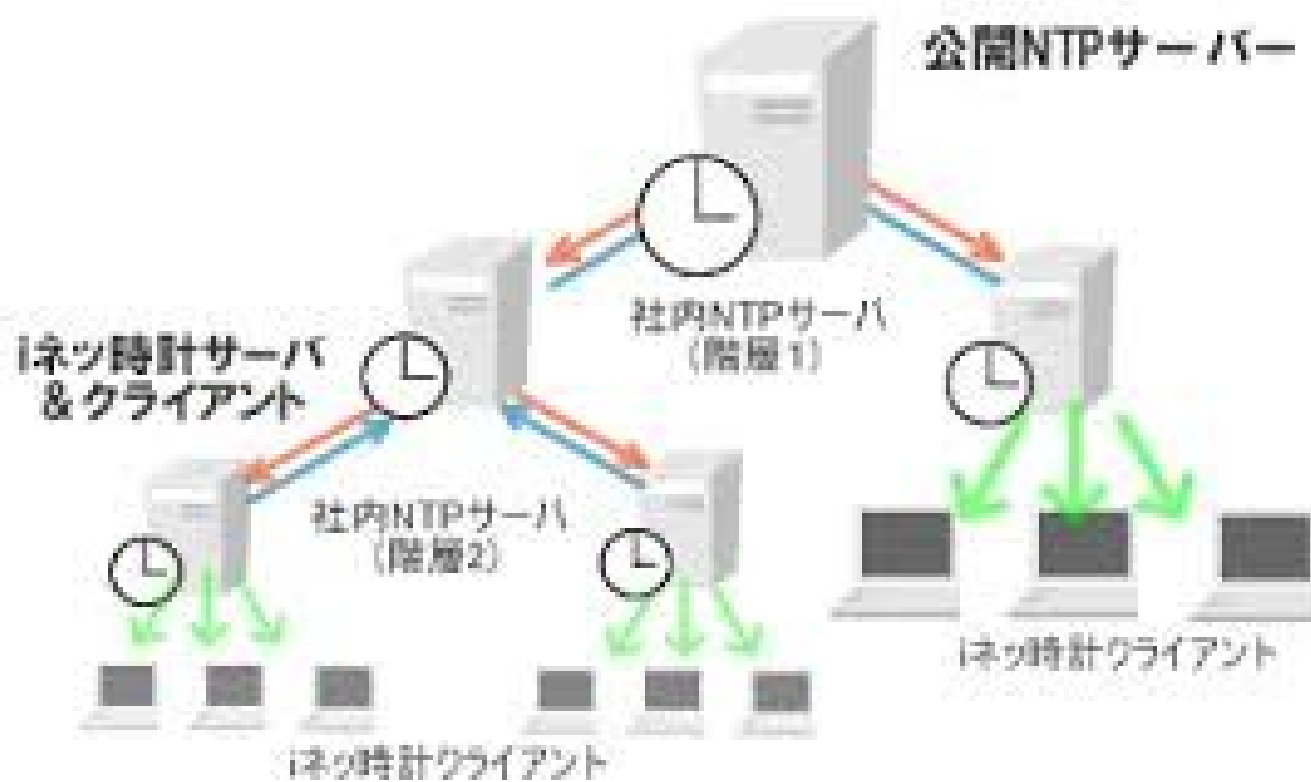
送信元 IP address

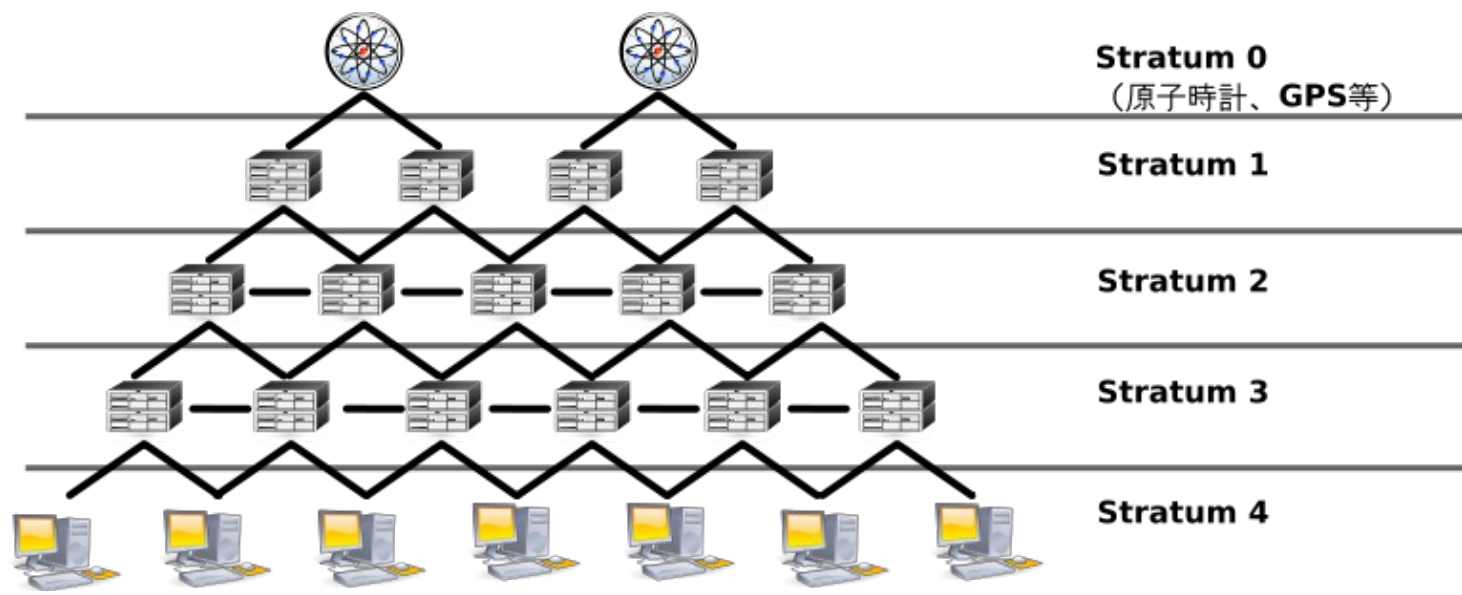
宛先 IP address

送信元 port number

宛先 port number

セッションコントロール
(ACKの制御)





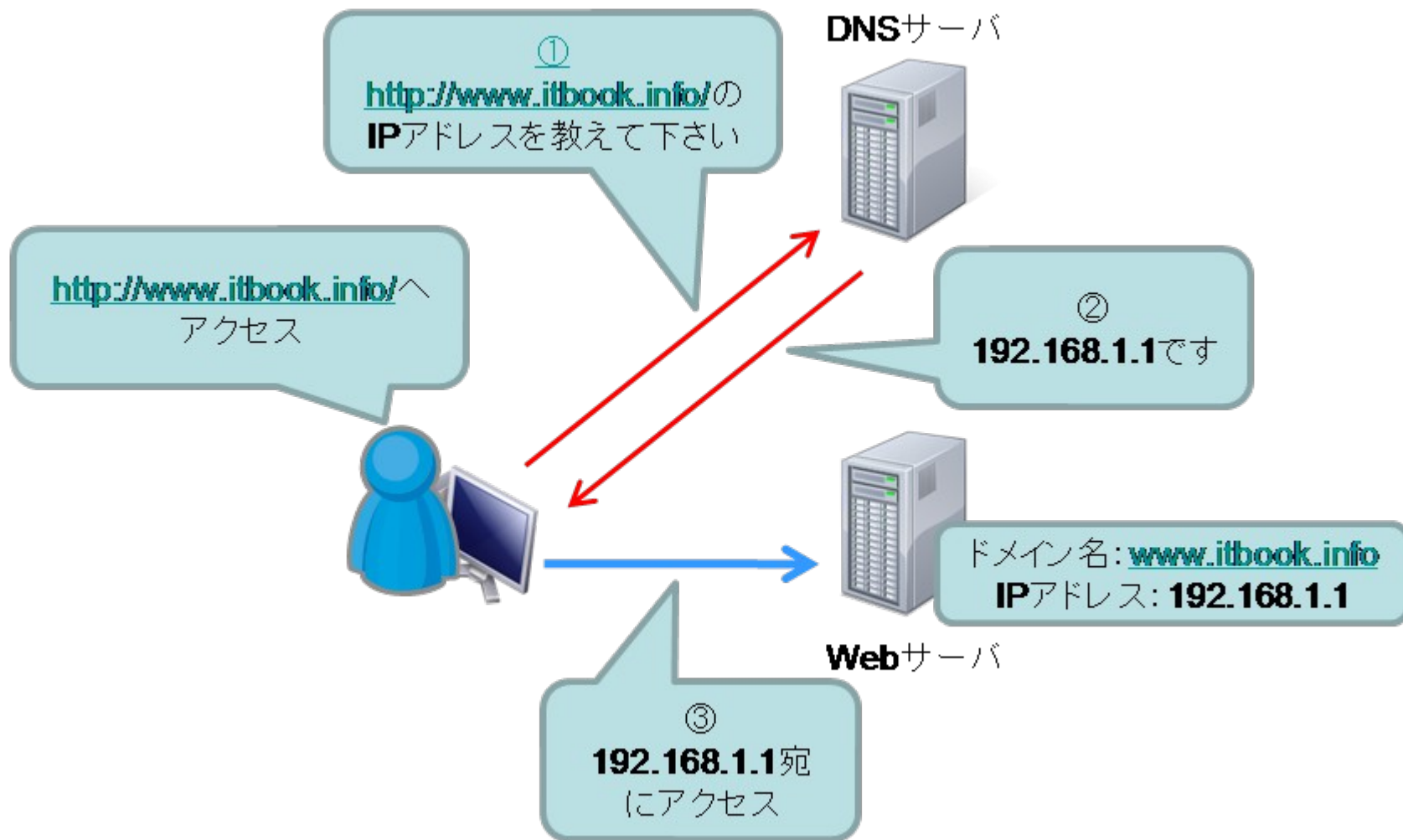
Stratum 0
(原子時計、GPS等)

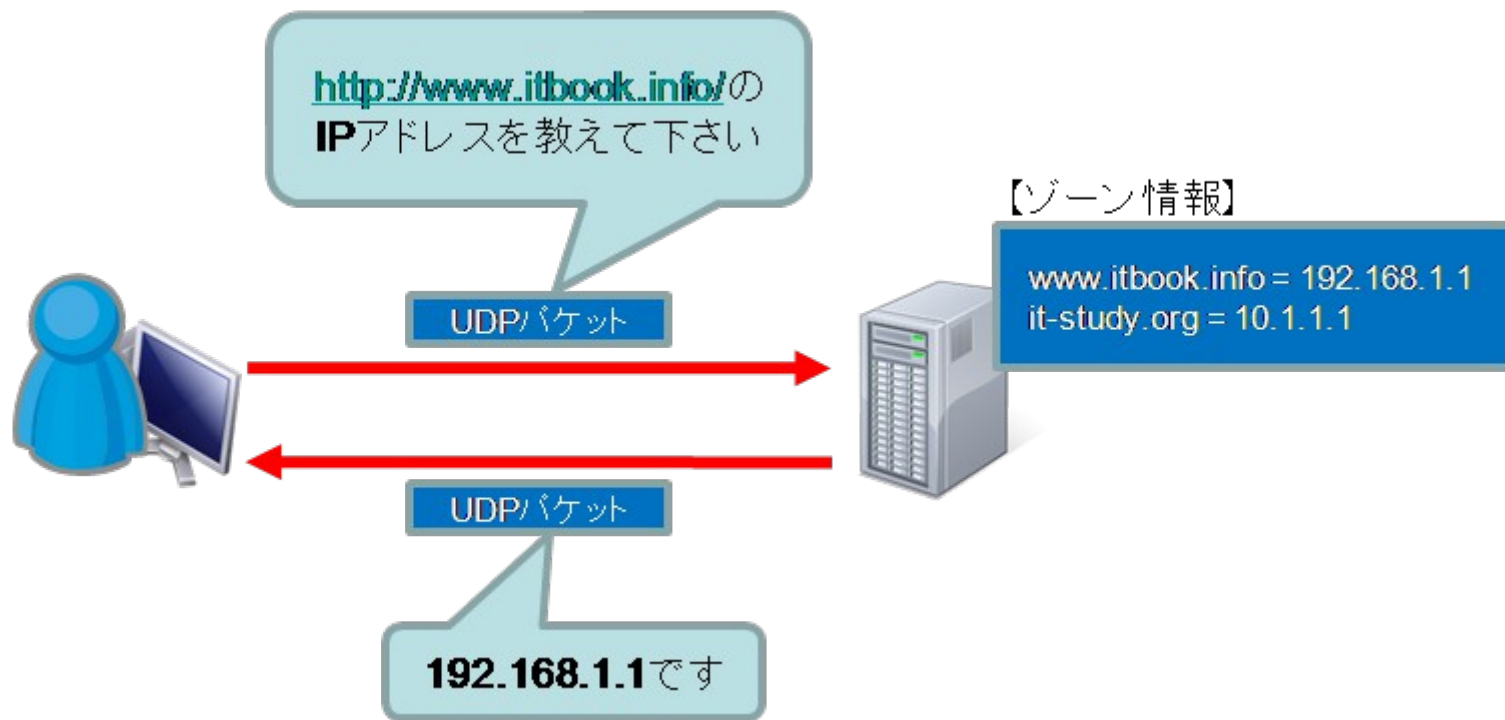
Stratum 1

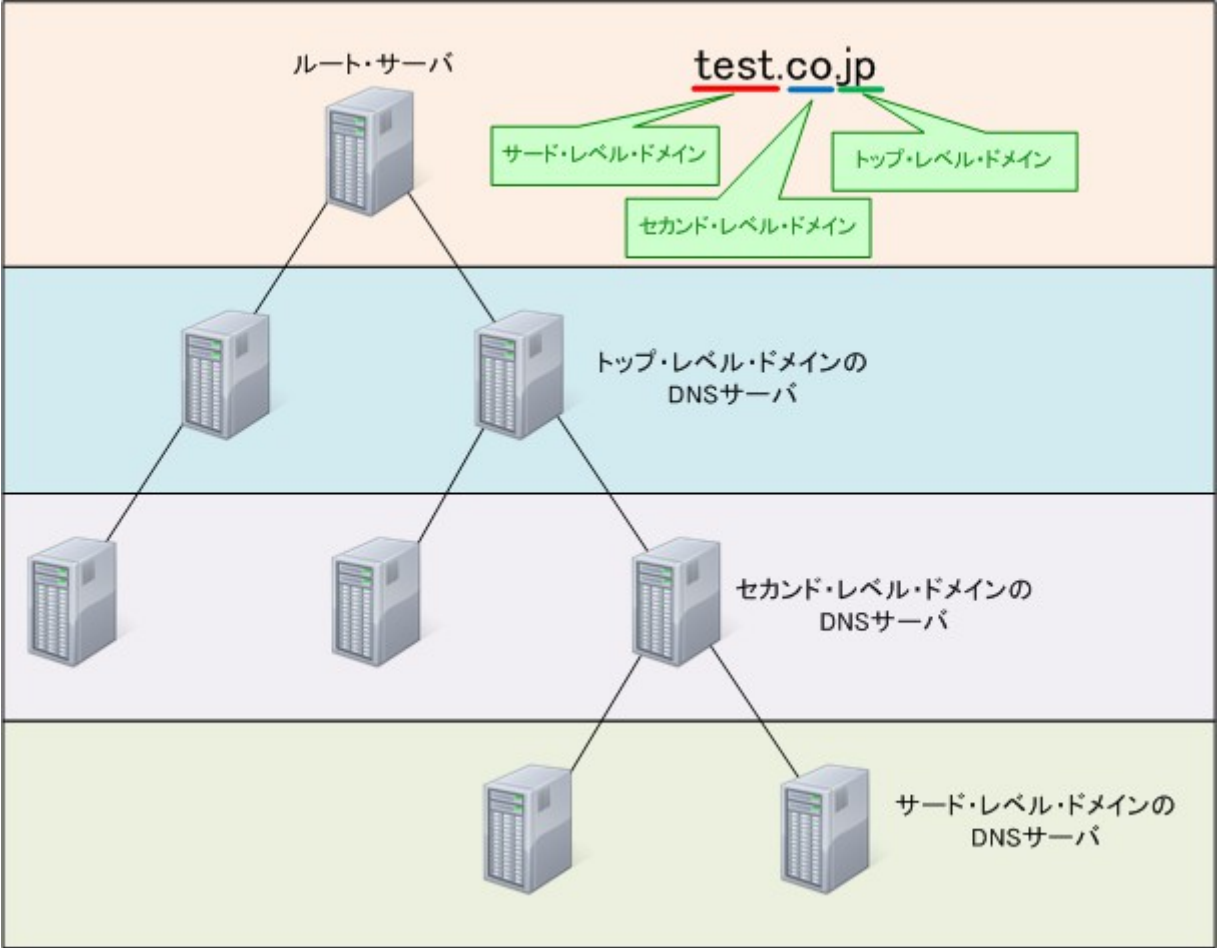
Stratum 2

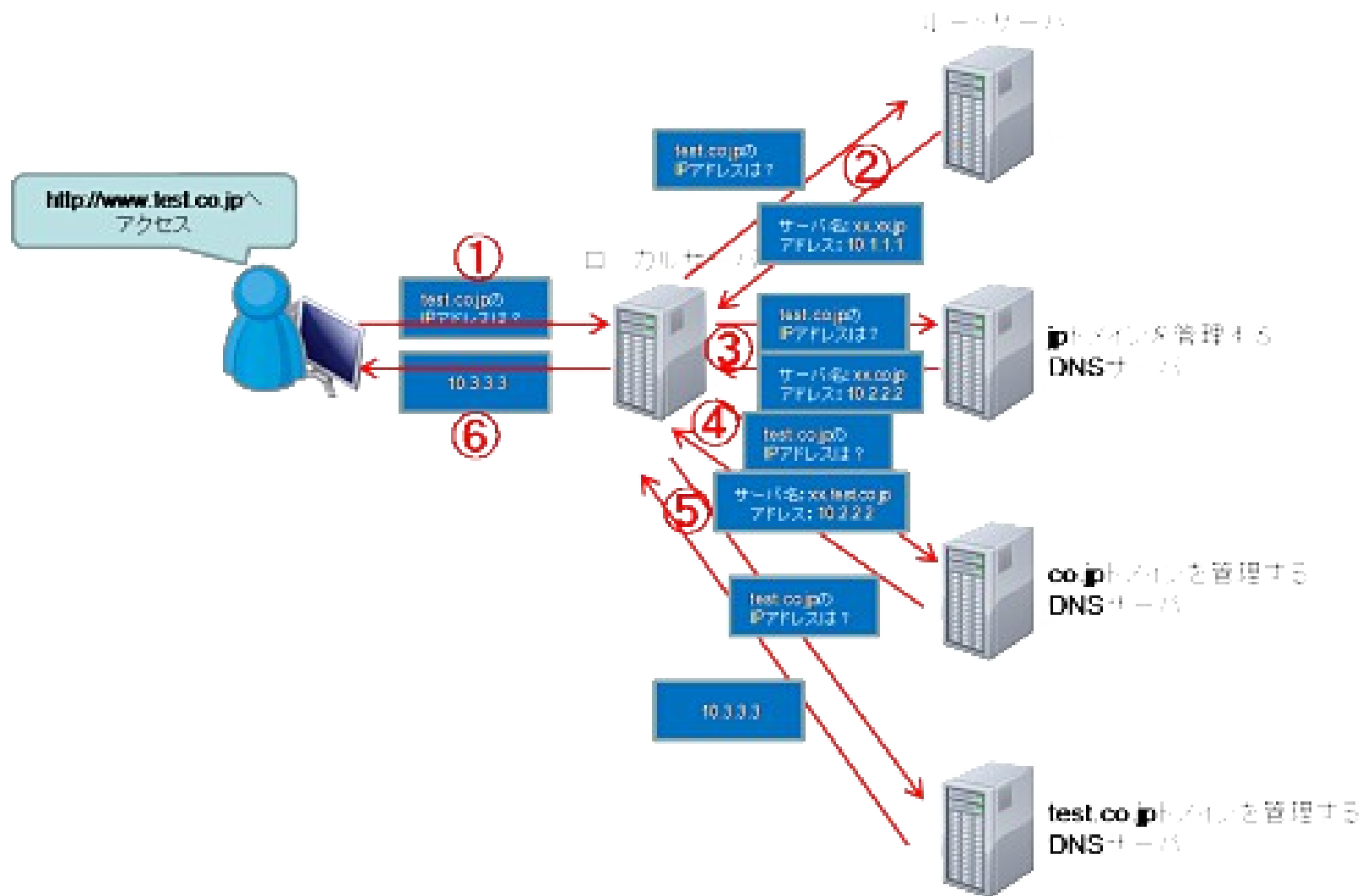
Stratum 3

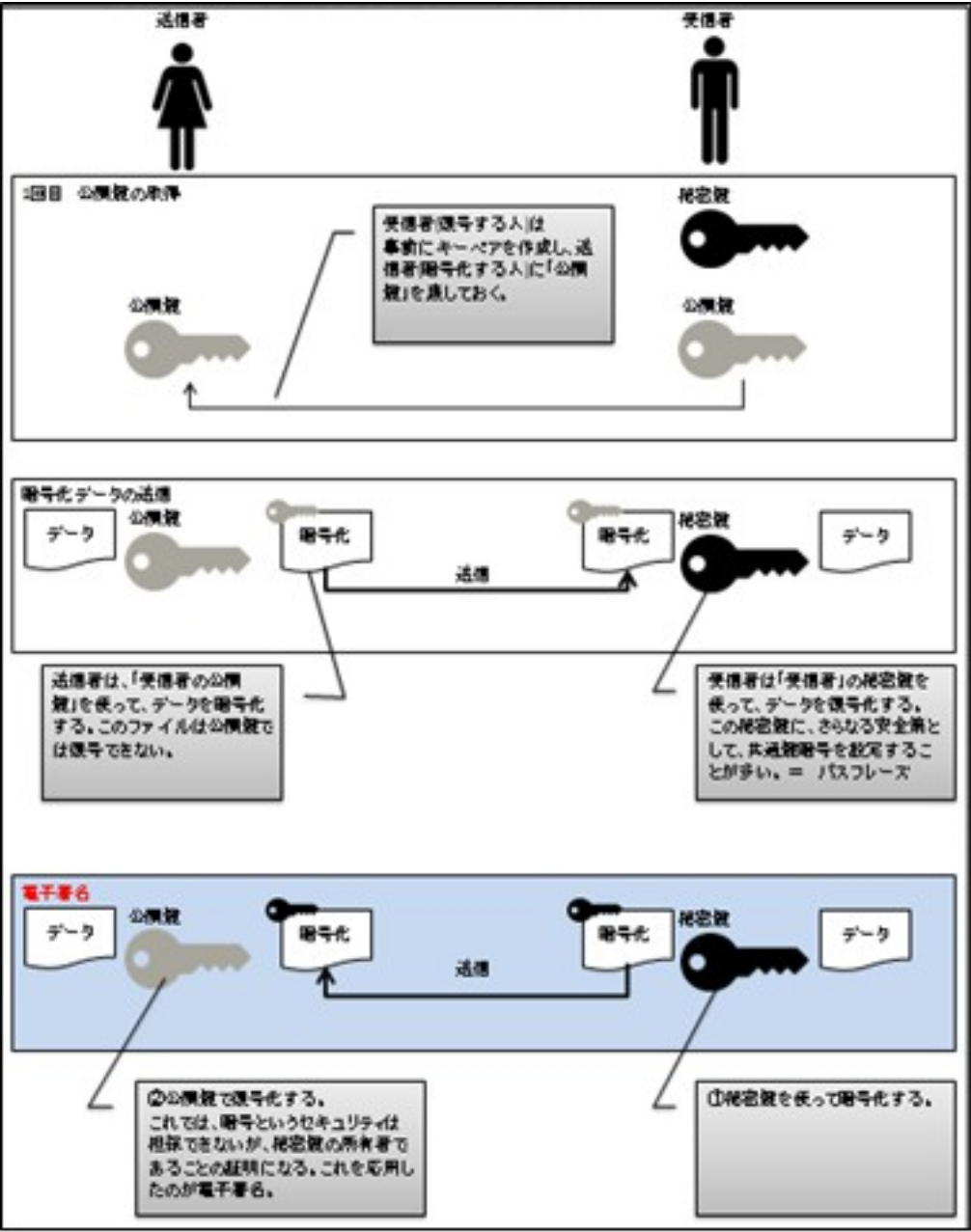
Stratum 4





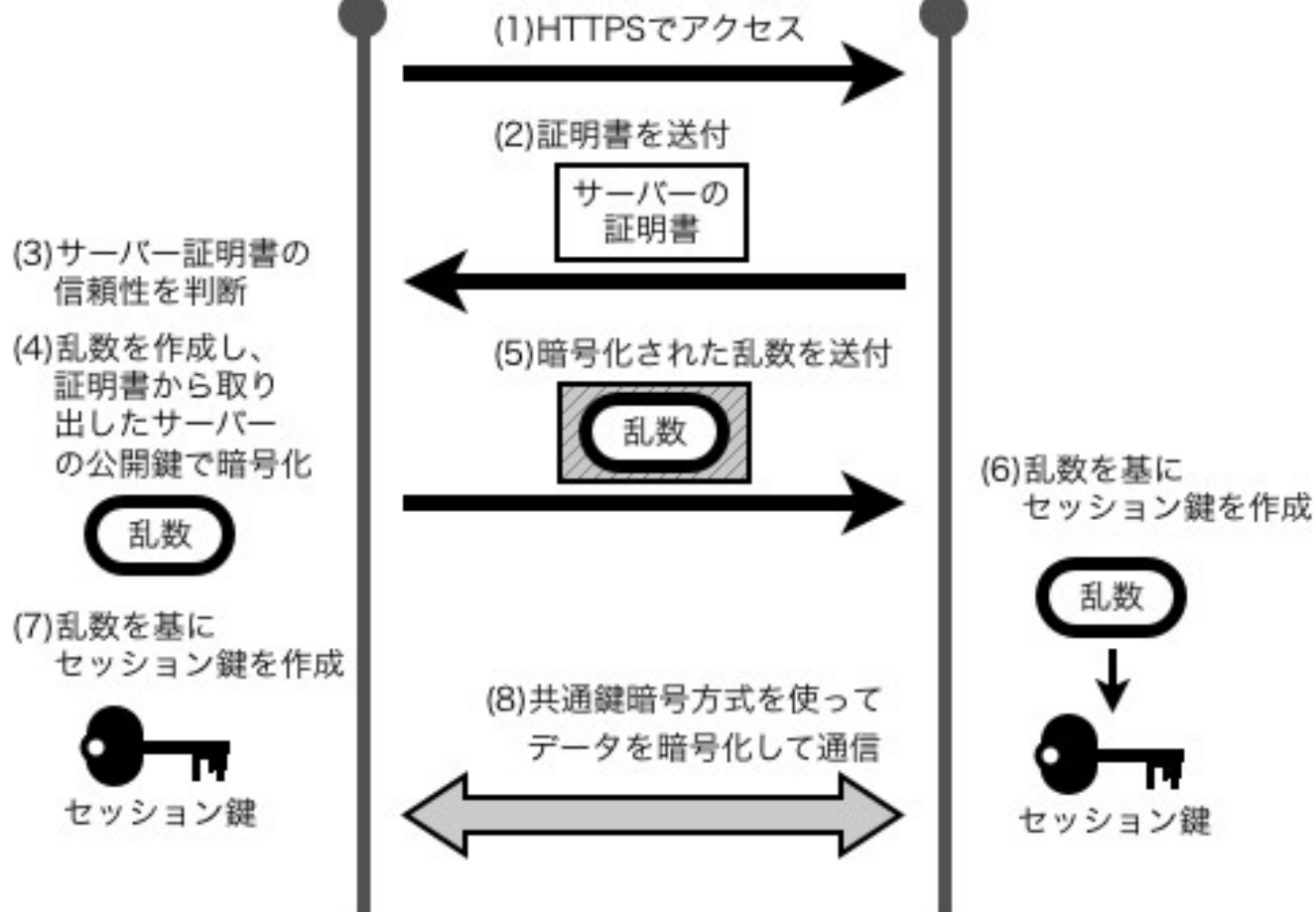






Webブラウザ

サーバー



参考文献

小高知宏, ``TCP/IP で学ぶコンピュータネットワークの基礎'',
森北出版, ISBN4-627-82410-6 (1996)

寺田, 菅島, ``TCP/IP セキュリティ実験'',
オーム社, ISBN4-274-06382-8 (2000)

村井 純, ``ネットワークアーキテクチャ'',
<http://www.soi.wide.ad.jp/class/20010012>, (2001).