情報ネットワーク論（第５回）
ＩＰプロトコルその２

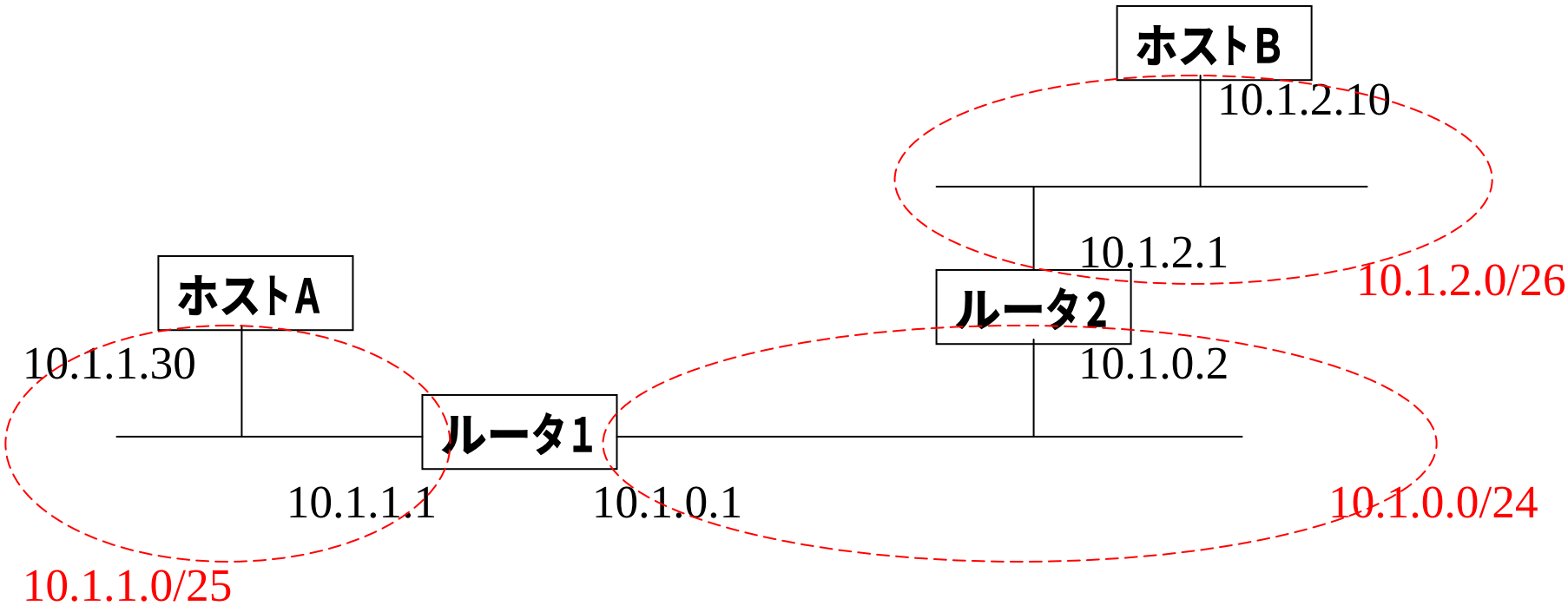
Ｈ１５，５，１４

ファイル保存位置

¥¥ism-srv¥www¥情報ネットワーク論

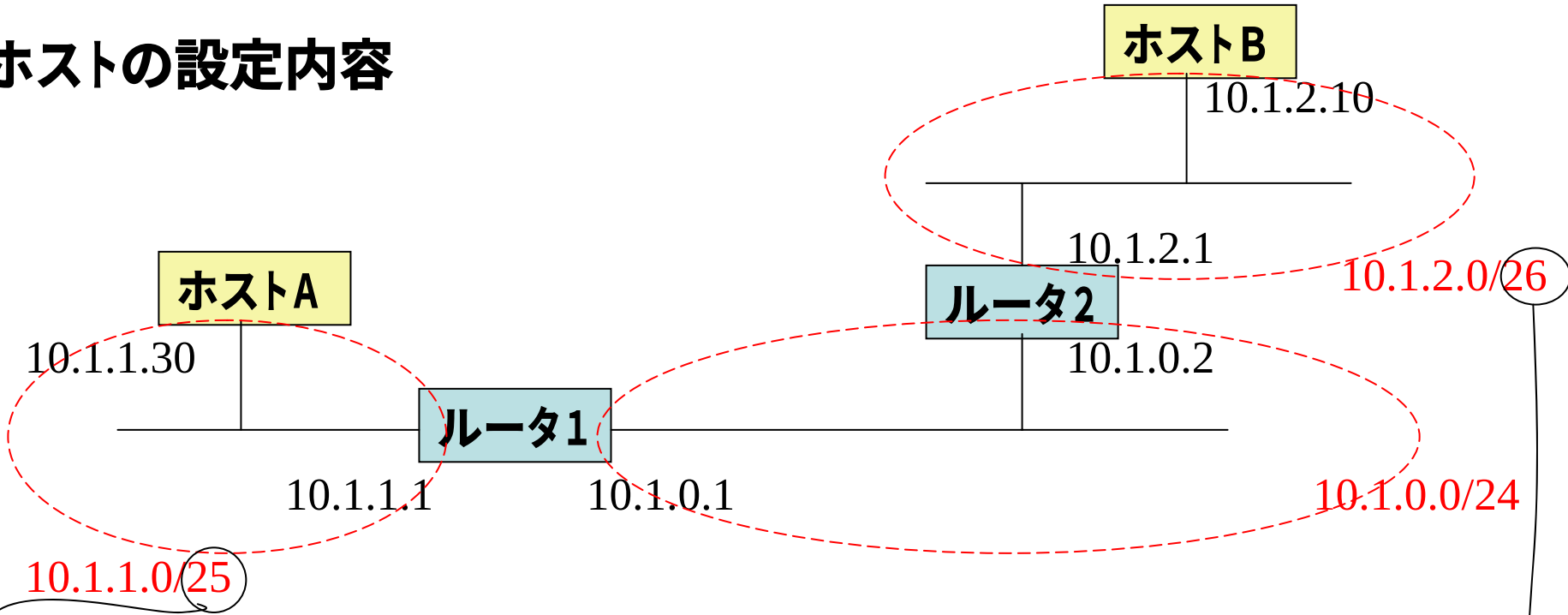
第4回の演習

・ホストA、ホストBに設定すべき、IPアドレス、サブネットマスク、デフォルトゲートウェイを示せ。



・IPアドレスの枯渇に対応するためにとられている短期解を2つあげ、それぞれ説明せよ。

ホストの設定内容



	ホストAの設定内容	ホストBの設定内容
IPアドレス	10. 1. 1. 30	10. 1. 2. 10
サブネットマスク	255.255.255.128	255.255.255.192
デフォルトゲートウェイ	10. 1. 1. 1	10. 1. 2. 1

25ビット

00001010 00000001 00000001 00011110

11111111 11111111 11111111 10000000

26ビット

00001010 00000001 00000010 00001010

11111111 11111111 11111111 11000000

ホストの設定内容と経路制御表の関係

	ホストAの設定内容	ホストBの設定内容
IPアドレス	10. 1. 1. 30	10. 1. 2. 10
サブネットマスク	255.255.255.128	255.255.255.192
デフォルトゲートウェイ	10. 1. 1. 1	10. 1. 2. 1

ホストAの経路制御表

ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ	次のルータ
0.0.0.0/0	10.1.1.1
10.1.1.0/25	10.1.1.30

||

ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ	ｻﾌﾞﾈｯﾄﾏｽｸ	次のルータ
0.0.0.0	0.0.0.0	10.1.1.1
10.1.1.0	255.255.255.128	10.1.1.30

ホストBの経路制御表

ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ	次のルータ
0.0.0.0/0	10.1.2.1
10.1.1.0/26	10.1.2.10

IPアドレスの枯渇に対応するためにとられている短期解決策

1. CIDR （Classless InterDomain Routing）

・クラス分けをなくしたIPアドレスの考え方

・アドレスの取得はクラスCのみ

・従来のクラスA、クラスBは返却

・できるだけアドレスを統合する（連続するアドレス範囲）

2. プライベートアドレス

・私的なネットワーク内でのみ利用できるアドレス

・アドレス取得機関への申請は不要

・外部との通信に使用してはいけない

・外部との通信はNAT(Network Address Translator)を介して実現

データリンクとＭＴＵ (Maximum Transmission Unit)

データリンクによりＭＴＵが異なる

ＭＴＵの違いを抽象化するため、パケットの分割処理を行う
(フラグメント)

フラグメントは８バイト単位

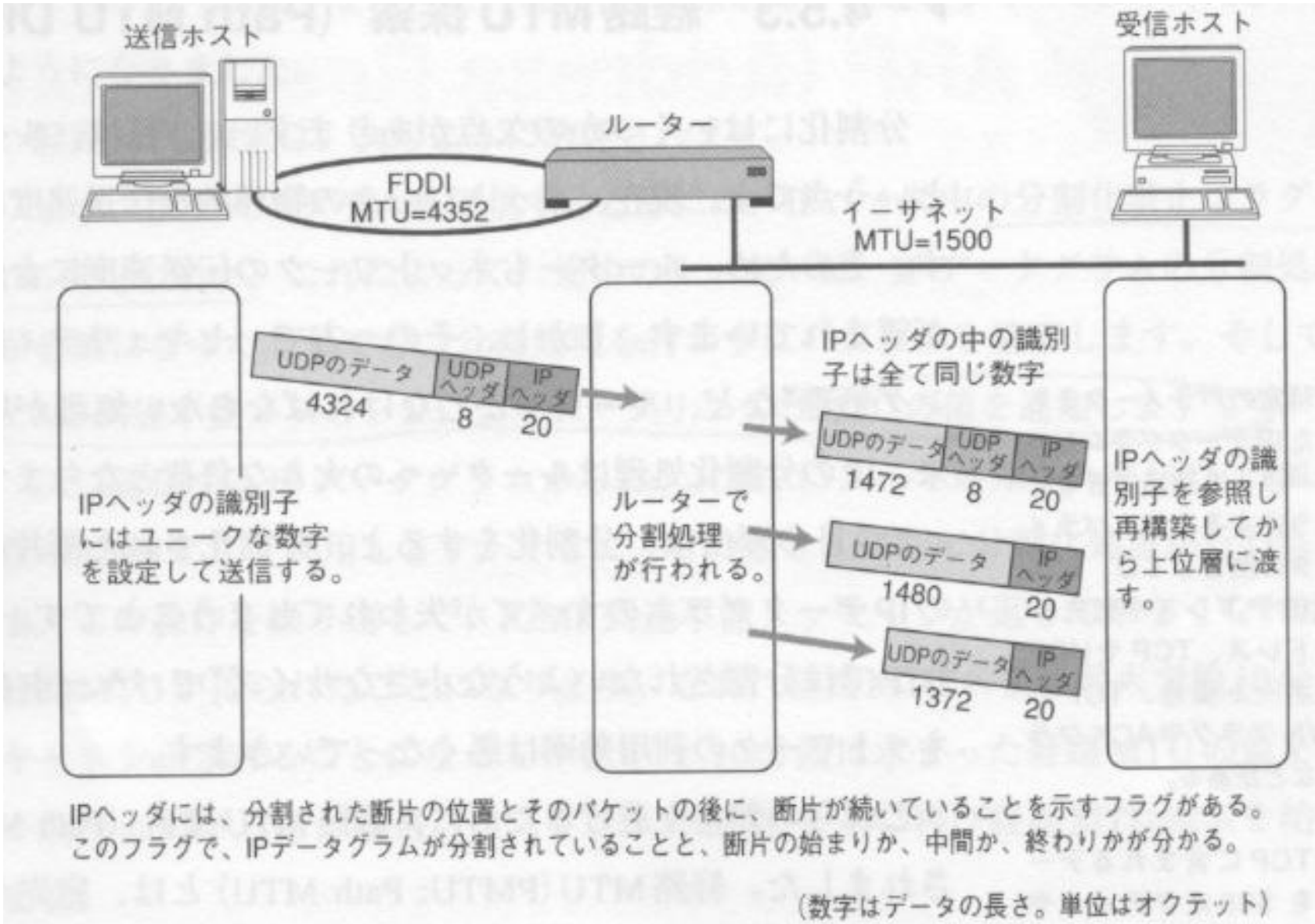
再構築処理は終点ホストでのみ行う

理由：パケットの経路が固定ではない

ルータに負担をかけない

データリンク	MTU(ﾊﾞｲﾄ)
FDDI	4352
イーサネット	1500
PPP	1500
IP over ATM	9180

IPデータグラムの分割と再構築（P133）



で行う

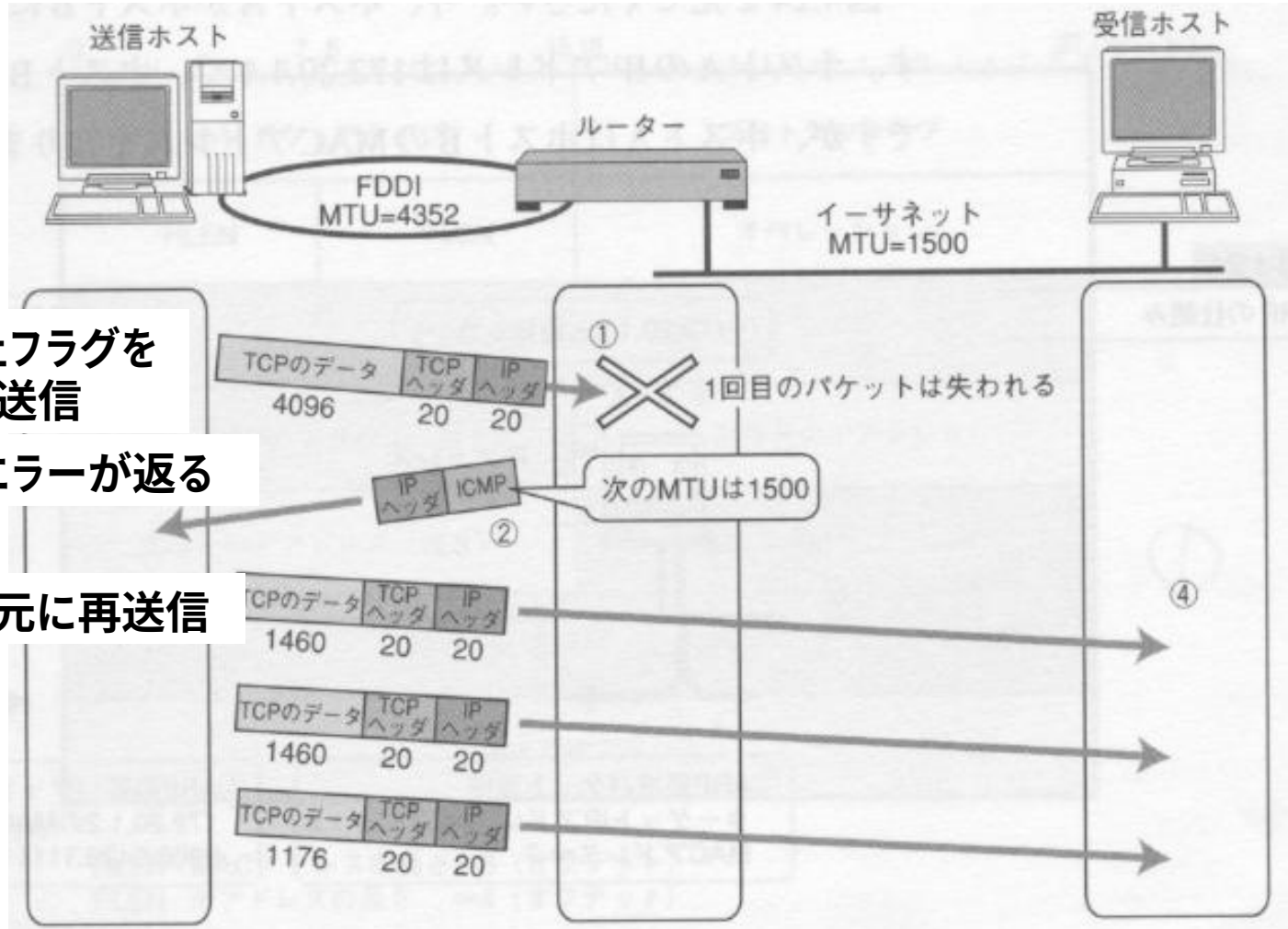
上位ソフトはフラグメントが発生していることを意識しない･･･MTUの違いを抽象化している

経路MTU探索（P135）

分割禁止フラグを
設定して送信

エラーが返る

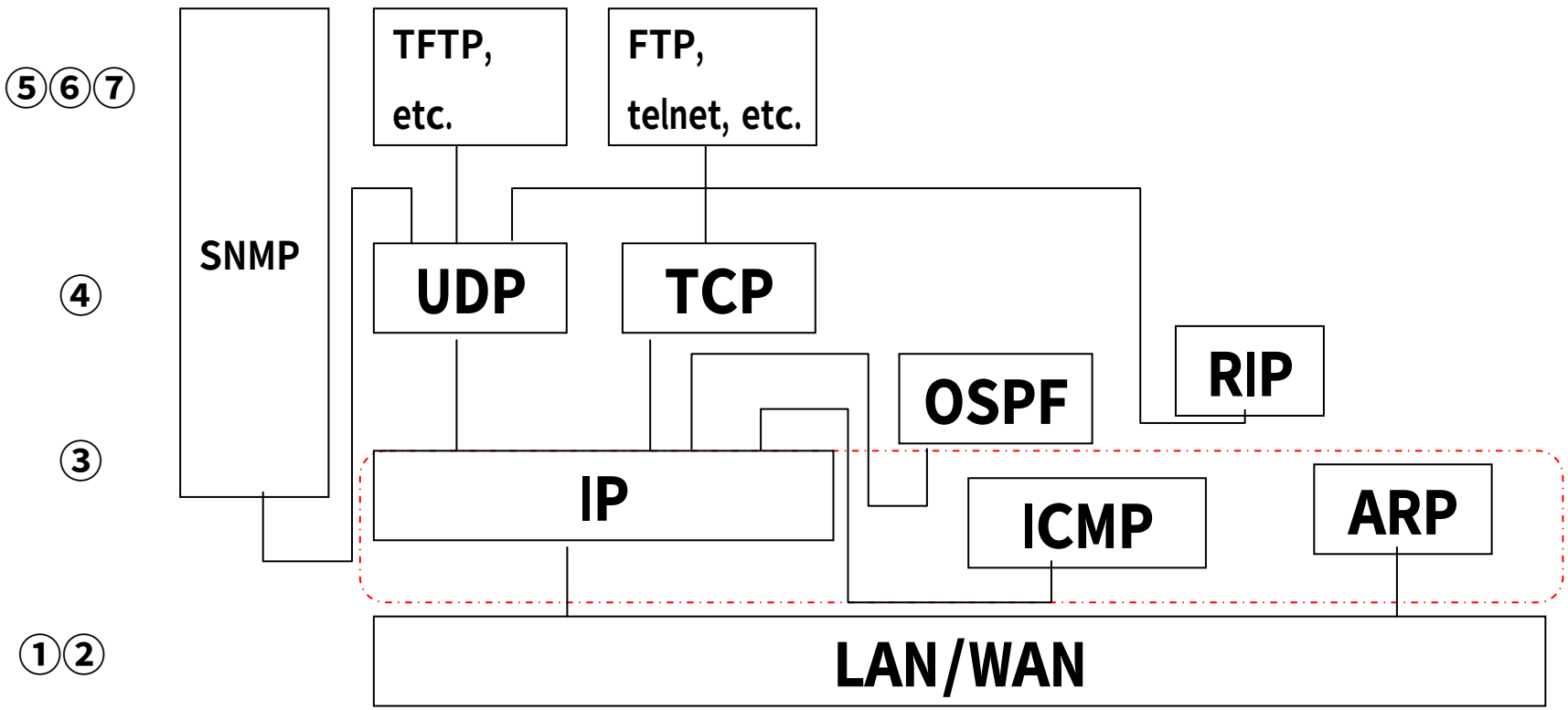
エラー情報を元に再送信



① IPヘッダの分割禁止フラグを設定して送信する。ルーターでパケットは失われる。
② ICMPにより次のMTUの大きさを知る。
③ TCPの再送処理によってデータが再送される。このとき、TCPがIPで分割されない大きさに区切ってからIP層に渡す。IPでは分割処理は行われない。
④ 再構築は不要。データはそのままTCP層へ渡される。

（数字はデータの長さ。単位はオクテット）

ARPとICMPの位置づけ

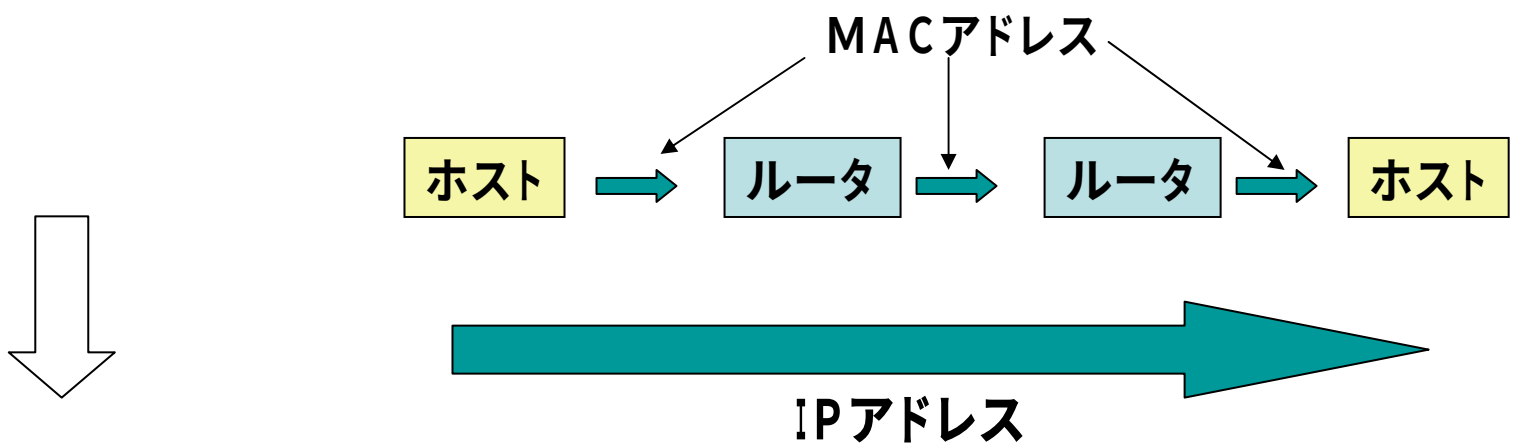


ＡＲＰ（Address Resolution Protocol）

エンドエンドの指定はＩＰアドレス

実際の通信はＭＡＣアドレスでバケツリレー

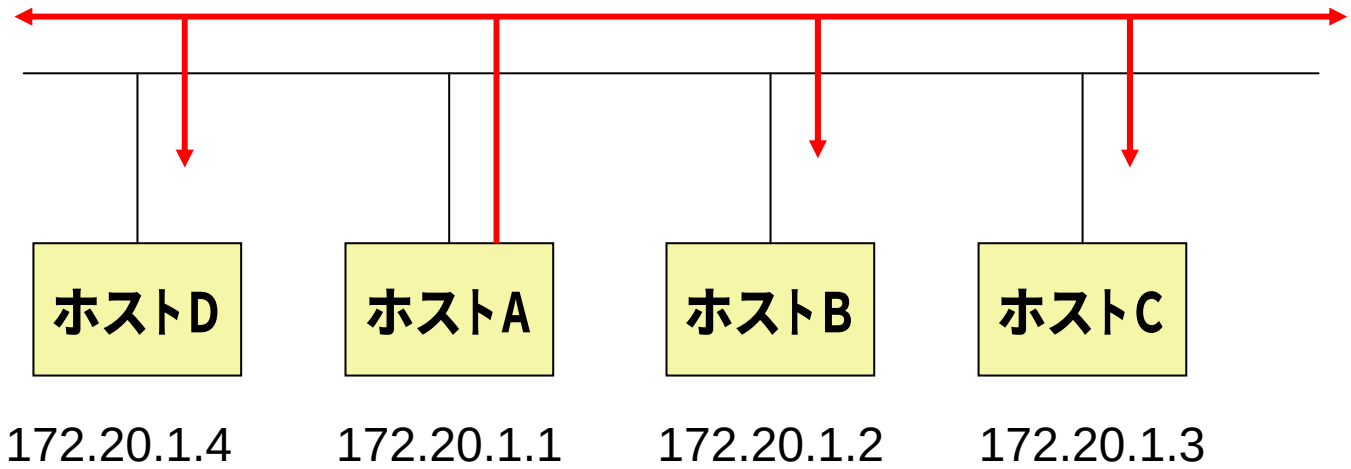
ＩＰアドレスとＭＡＣアドレスのマッピングが必要



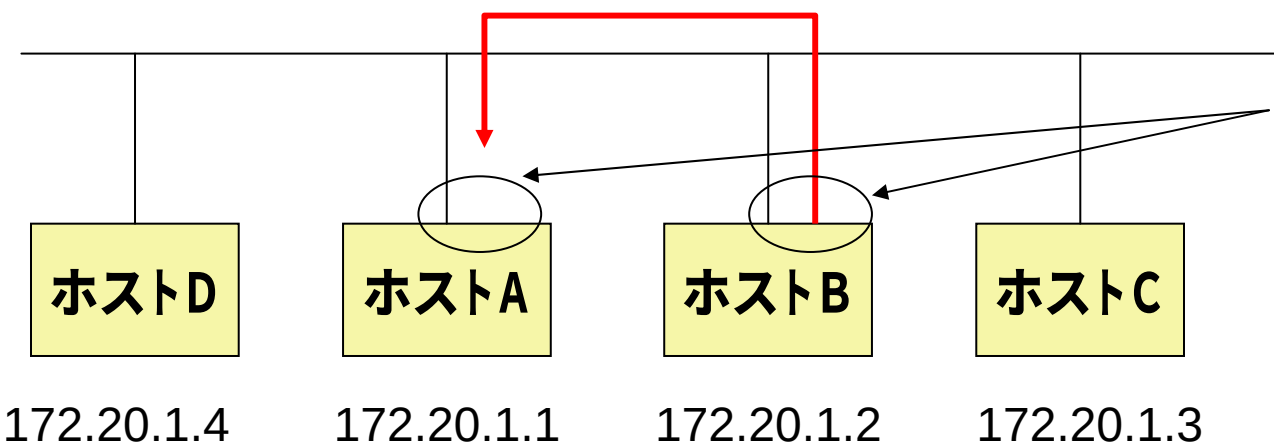
ＡＲＰ（Address Resolution Protocol）

ＡＲＰの動作

ＡＲＰ要求パケット（ブロードキャスト）　172.20.1.2と通信したい



ＡＲＰ応答パケット（ユニキャスト）　172.20.1.2が自ＭＡＣアドレスを報告



ホストAとホストBに相手のIPアドレスとＭＡＣアドレスの対応テーブルが一時的に作成される

（キャッシュ）

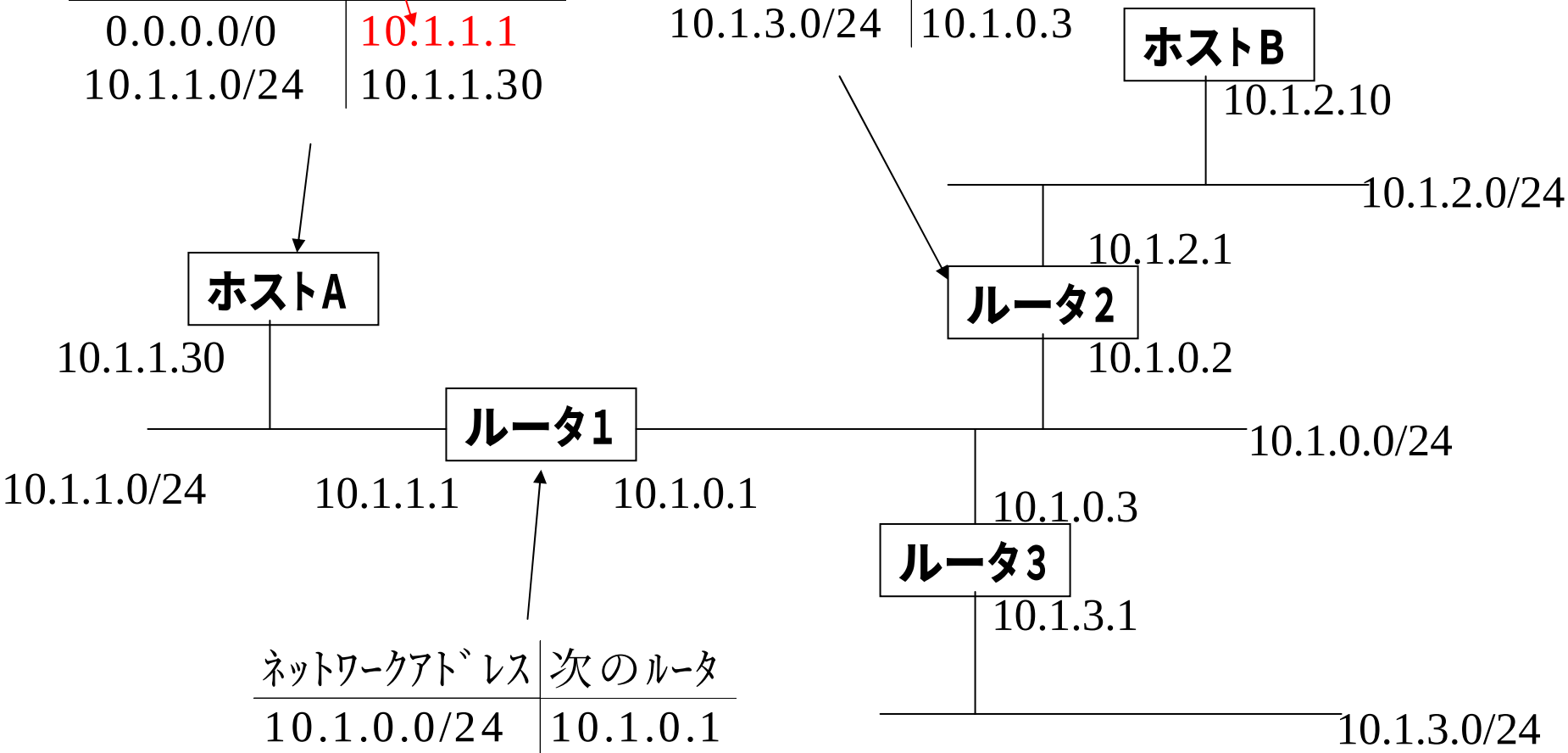
ＡＲＰのパケットフォーマット（Ｐ１３７）

ホストAからホストBまでの通信例

宛先10.1.2.10の次のルータは
10.1.1.1 (デフォルトゲートウェイ)

ネットワークアドレス	次のルータ
0.0.0.0/0	10.1.1.1
10.1.1.0/24	10.1.1.30

ネットワークアドレス	次のルータ
10.1.0.0/24	10.1.0.2
10.1.1.0/24	10.1.0.1
10.1.2.0/24	10.1.2.1
10.1.3.0/24	10.1.0.3



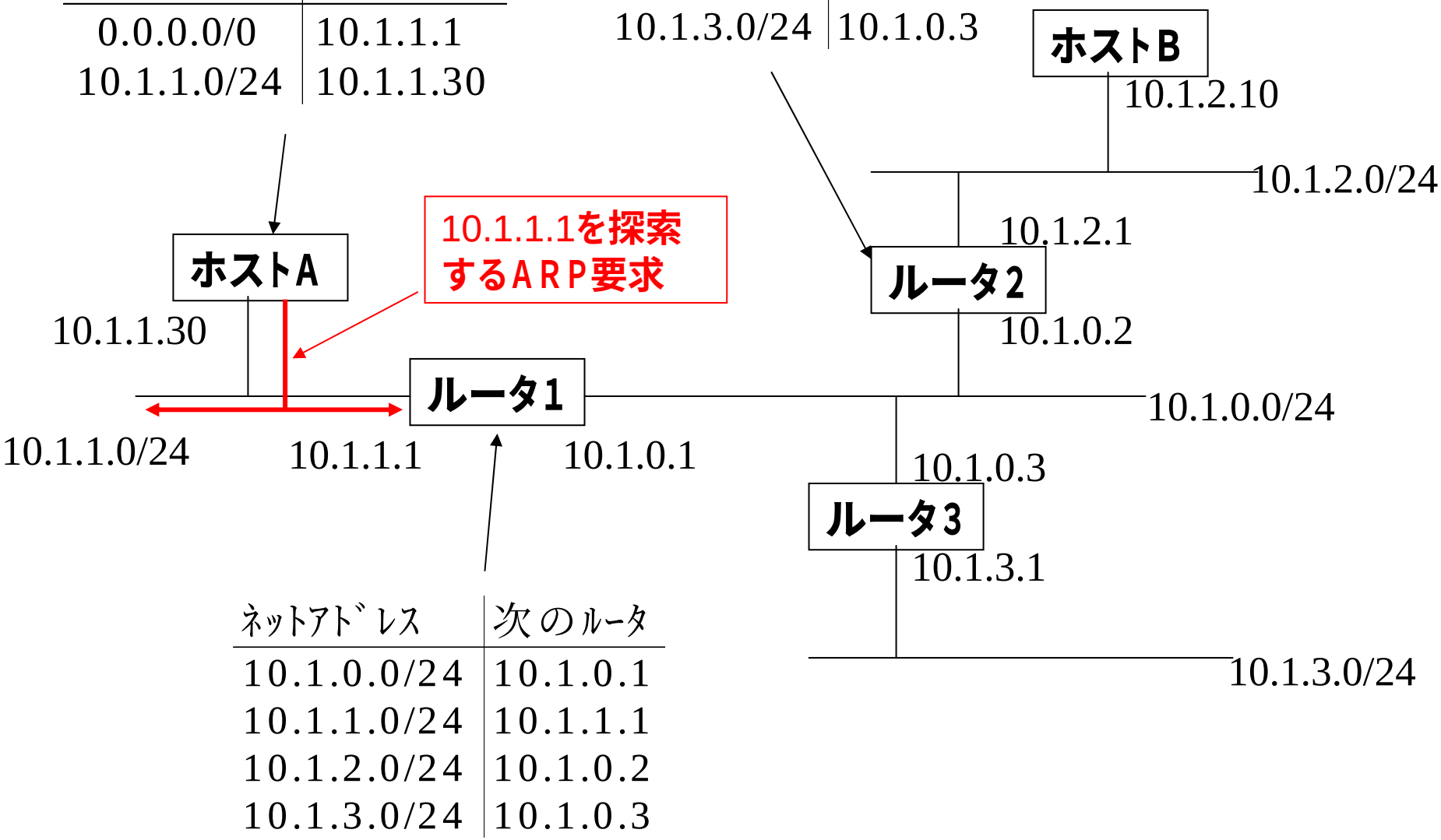
ネットワークアドレス	次のルータ
10.1.0.0/24	10.1.0.1
10.1.1.0/24	10.1.1.1
10.1.2.0/24	10.1.0.2
10.1.3.0/24	10.1.0.3

ホストAからホストBまでの通信例

②

ネットアドレス	次のルータ
0.0.0.0/0	10.1.1.1
10.1.1.0/24	10.1.1.30

ネットアドレス	次のルータ
10.1.0.0/24	10.1.0.2
10.1.1.0/24	10.1.0.1
10.1.2.0/24	10.1.2.1
10.1.3.0/24	10.1.0.3



ネットアドレス	次のルータ
10.1.0.0/24	10.1.0.1
10.1.1.0/24	10.1.1.1
10.1.2.0/24	10.1.0.2
10.1.3.0/24	10.1.0.3

ホストAからホストBまでの通信例

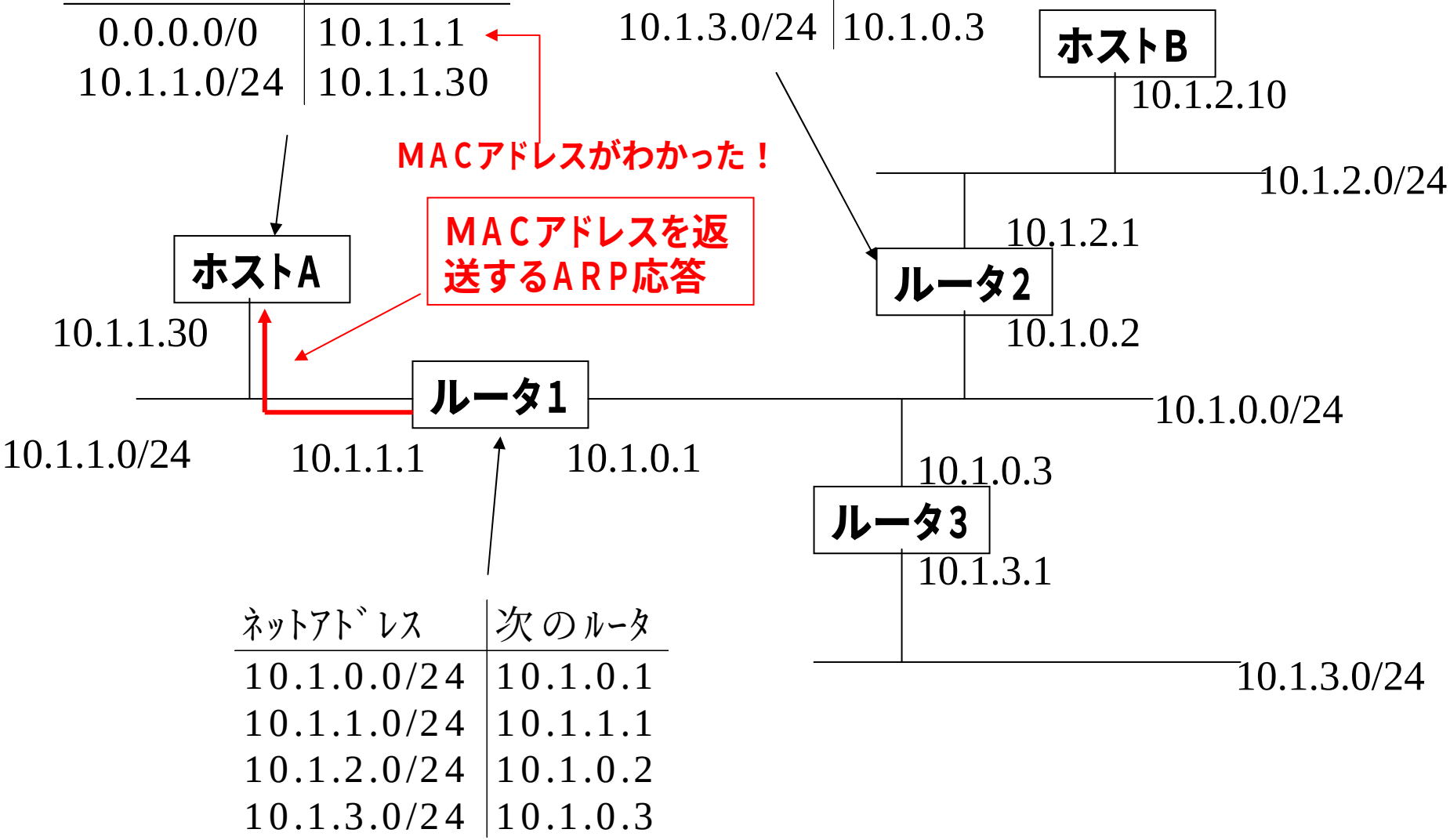
③

ネットアドレス	次のルータ
10.1.0.0/24	10.1.0.2
10.1.1.0/24	10.1.0.1
10.1.2.0/24	10.1.2.1
10.1.3.0/24	10.1.0.3

ネットアドレス	次のルータ
0.0.0.0/0	10.1.1.1
10.1.1.0/24	10.1.1.30

MACアドレスがわかった！

MACアドレスを返送するARP応答



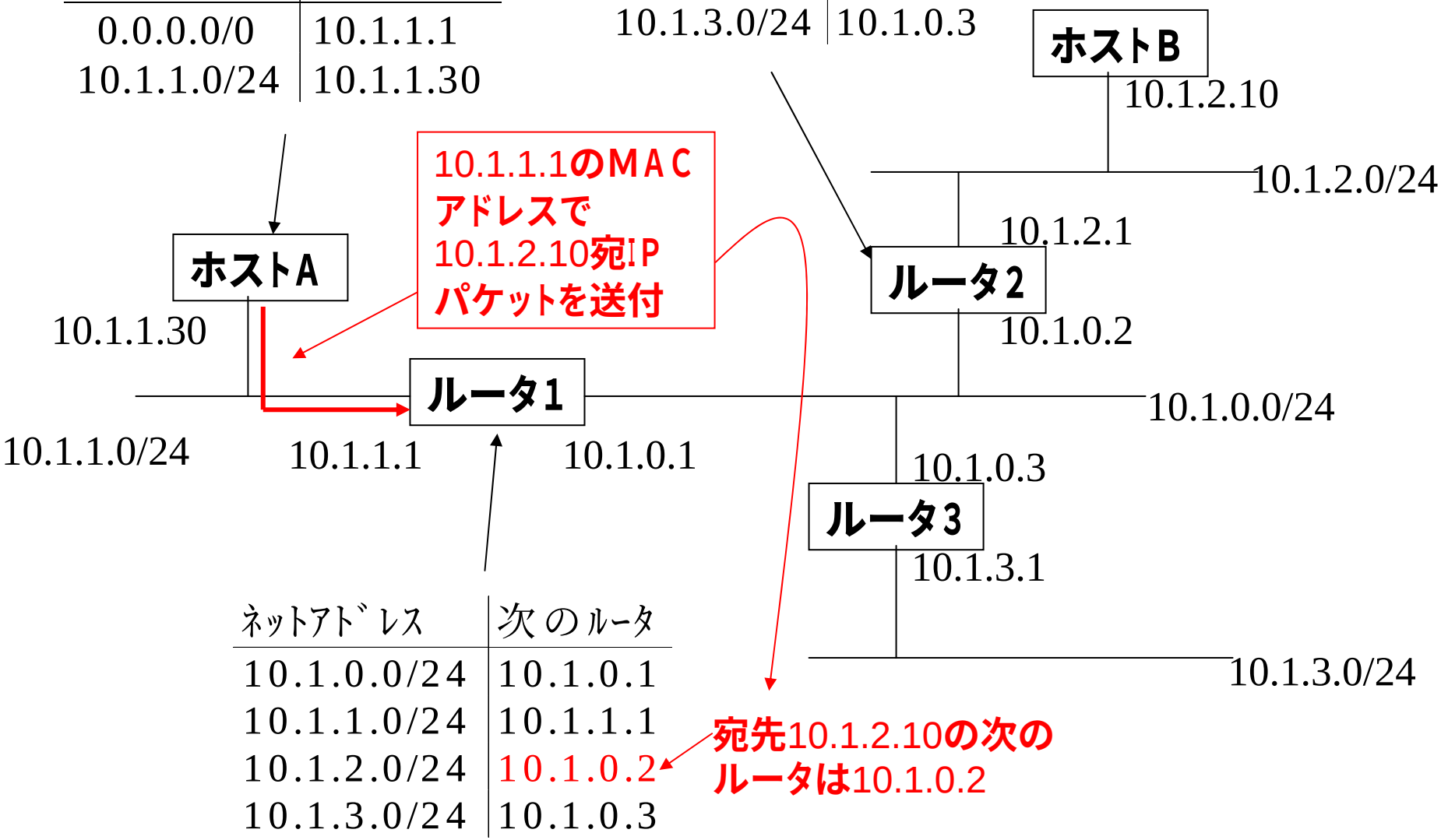
ネットアドレス	次のルータ
10.1.0.0/24	10.1.0.1
10.1.1.0/24	10.1.1.1
10.1.2.0/24	10.1.0.2
10.1.3.0/24	10.1.0.3

ホストAからホストBまでの通信例

④

ネットアドレス	次のルータ
0.0.0.0/0	10.1.1.1
10.1.1.0/24	10.1.1.30

ネットアドレス	次のルータ
10.1.0.0/24	10.1.0.2
10.1.1.0/24	10.1.0.1
10.1.2.0/24	10.1.2.1
10.1.3.0/24	10.1.0.3



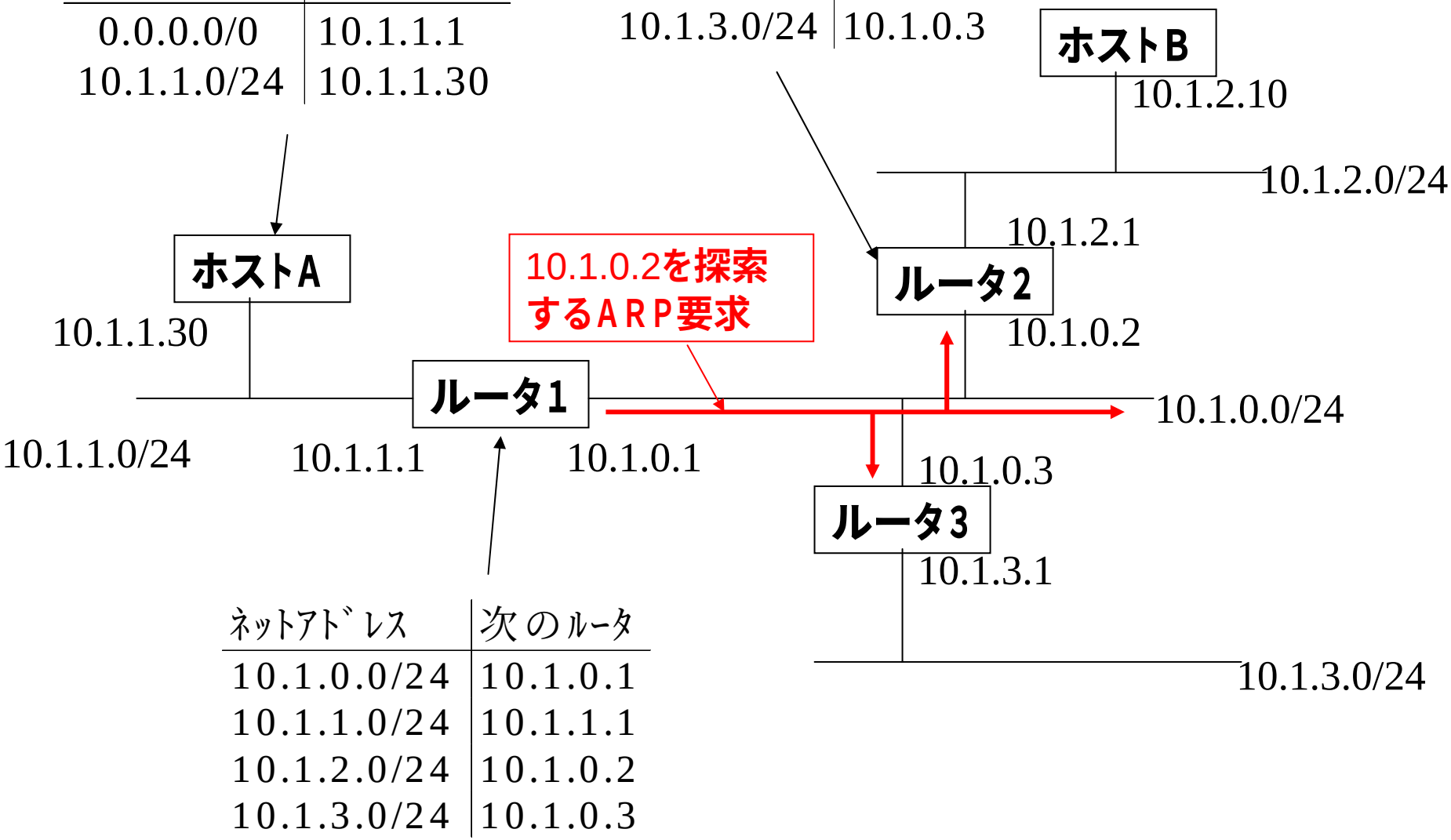
ネットアドレス	次のルータ
10.1.0.0/24	10.1.0.1
10.1.1.0/24	10.1.1.1
10.1.2.0/24	10.1.0.2
10.1.3.0/24	10.1.0.3

宛先10.1.2.10の次のルータは10.1.0.2

ホストAからホストBまでの通信例

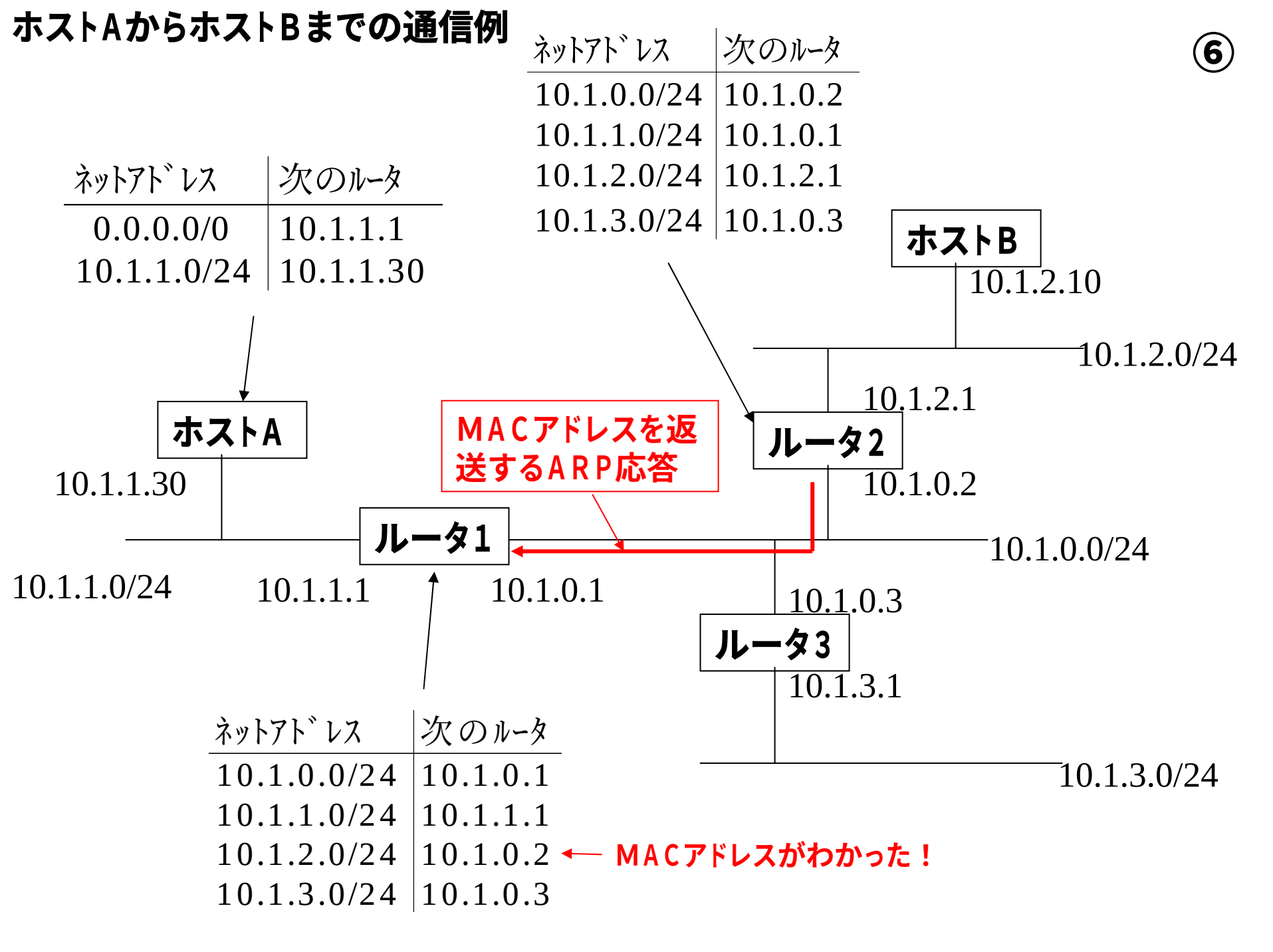
ネットアドレス	次のルータ
0.0.0.0/0	10.1.1.1
10.1.1.0/24	10.1.1.30

ネットアドレス	次のルータ
10.1.0.0/24	10.1.0.2
10.1.1.0/24	10.1.0.1
10.1.2.0/24	10.1.2.1
10.1.3.0/24	10.1.0.3



ネットアドレス	次のルータ
10.1.0.0/24	10.1.0.1
10.1.1.0/24	10.1.1.1
10.1.2.0/24	10.1.0.2
10.1.3.0/24	10.1.0.3

ホストAからホストBまでの通信例



ホストAからホストBまでの通信例

⑦

ネットアドレス	次のルータ
10.1.0.0/24	10.1.0.2
10.1.1.0/24	10.1.0.1
10.1.2.0/24	10.1.2.1
10.1.3.0/24	10.1.0.3

宛先10.1.2.10の次のルータは10.1.2.1（自分自身）＝ホストBは直結

ネットアドレス	次のルータ
0.0.0.0/0	10.1.1.1
10.1.1.0/24	10.1.1.30

ホストB

10.1.2.10

10.1.2.0/24

10.1.2.1

ホストA

10.1.1.30

10.1.0.2のMACアドレスで10.1.2.10宛IPパケットを送付

ルータ2

ルータ1

10.1.0.0/24

10.1.1.0/24

10.1.1.1

10.1.0.1

10.1.0.3

ルータ3

10.1.3.1

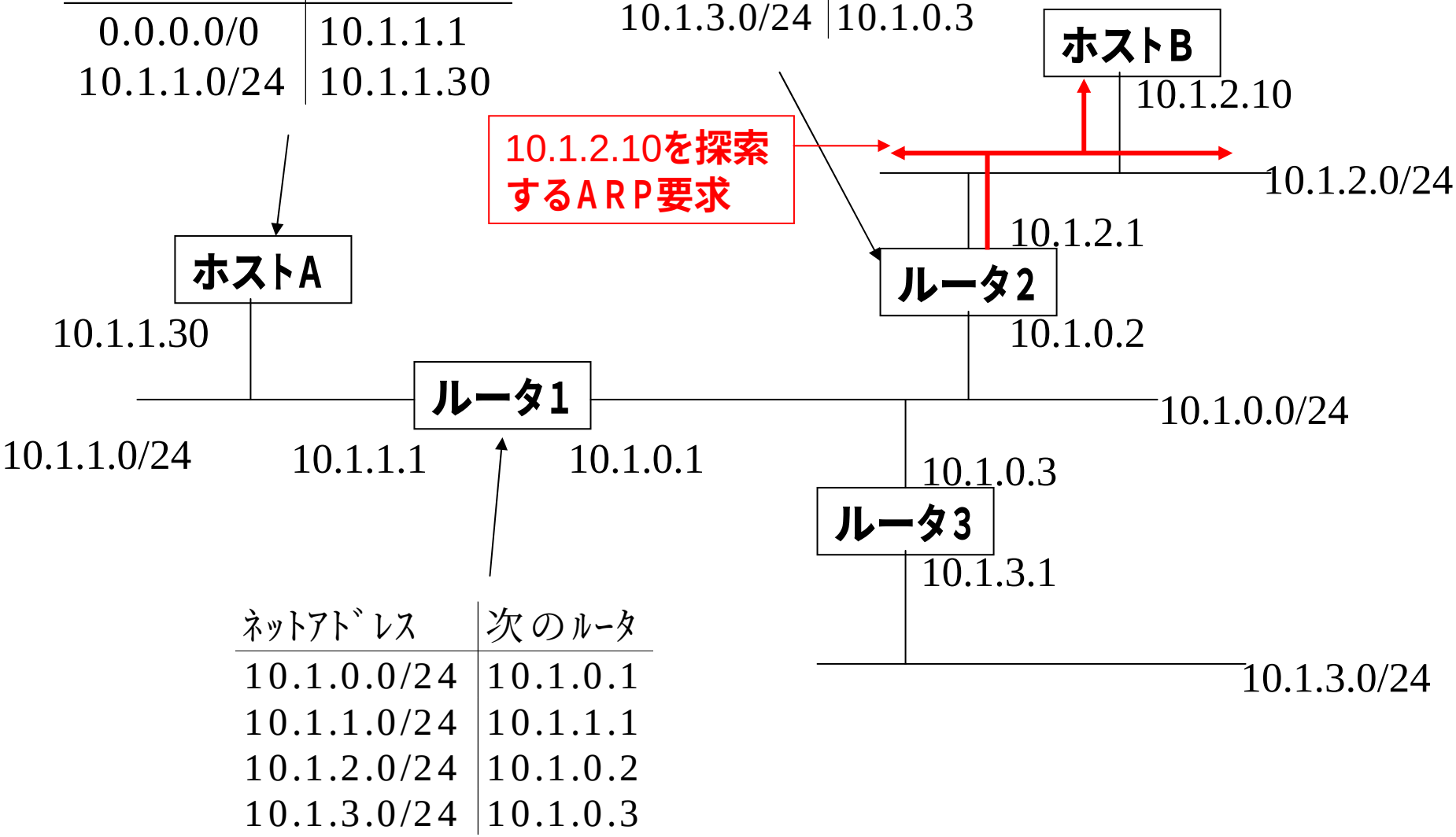
10.1.3.0/24

ネットアドレス	次のルータ
10.1.0.0/24	10.1.0.1
10.1.1.0/24	10.1.1.1
10.1.2.0/24	10.1.0.2
10.1.3.0/24	10.1.0.3

ホストAからホストBまでの通信例

ネットアドレス	次のルータ
0.0.0.0/0	10.1.1.1
10.1.1.0/24	10.1.1.30

ネットアドレス	次のルータ
10.1.0.0/24	10.1.0.2
10.1.1.0/24	10.1.0.1
10.1.2.0/24	10.1.2.1
10.1.3.0/24	10.1.0.3



ネットアドレス	次のルータ
10.1.0.0/24	10.1.0.1
10.1.1.0/24	10.1.1.1
10.1.2.0/24	10.1.0.2
10.1.3.0/24	10.1.0.3

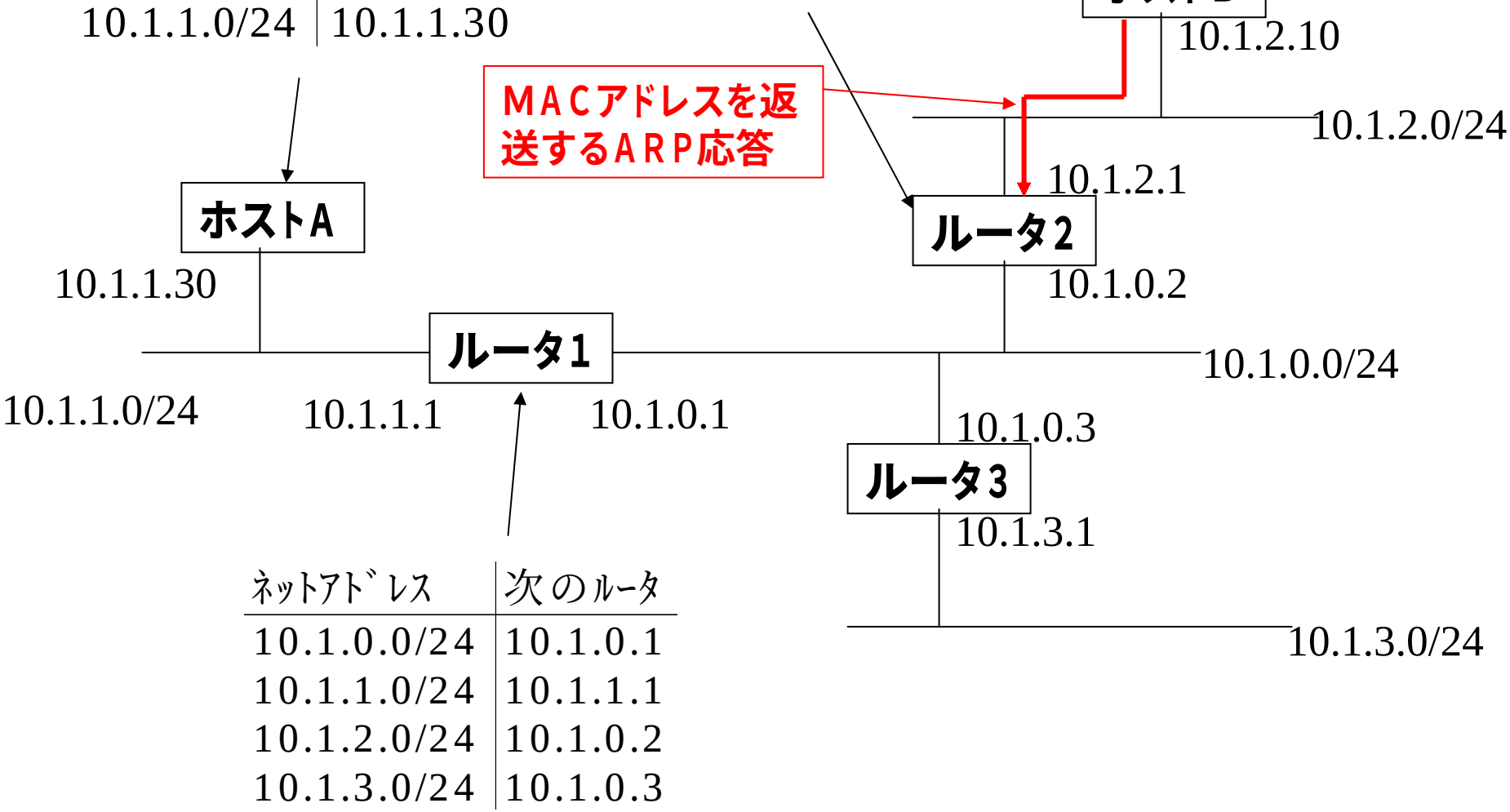
ホストAからホストBまでの通信例

ネットアドレス	次のルータ
0.0.0.0/0	10.1.1.1
10.1.1.0/24	10.1.1.30

ネットアドレス	次のルータ
10.1.0.0/24	10.1.0.2
10.1.1.0/24	10.1.0.1
10.1.2.0/24	10.1.2.1
10.1.3.0/24	10.1.0.3

ホストBのMACアドレスがわかった！

MACアドレスを返送するARP応答

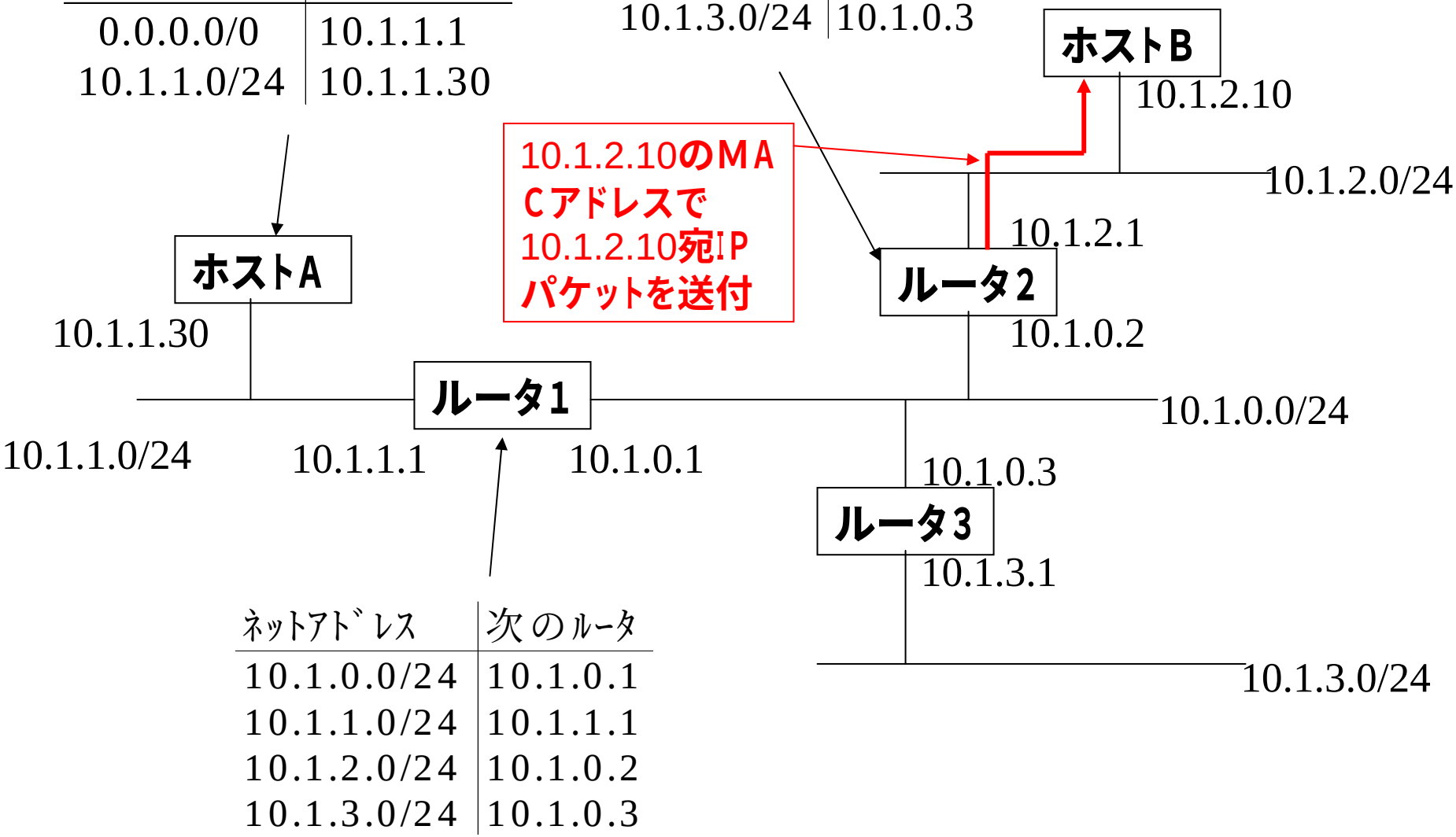


ネットアドレス	次のルータ
10.1.0.0/24	10.1.0.1
10.1.1.0/24	10.1.1.1
10.1.2.0/24	10.1.0.2
10.1.3.0/24	10.1.0.3

ホストAからホストBまでの通信例

ネットアドレス	次のルータ
0.0.0.0/0	10.1.1.1
10.1.1.0/24	10.1.1.30

ネットアドレス	次のルータ
10.1.0.0/24	10.1.0.2
10.1.1.0/24	10.1.0.1
10.1.2.0/24	10.1.2.1
10.1.3.0/24	10.1.0.3



ネットアドレス	次のルータ
10.1.0.0/24	10.1.0.1
10.1.1.0/24	10.1.1.1
10.1.2.0/24	10.1.0.2
10.1.3.0/24	10.1.0.3

ＡＲＰの動作（補足）

・ＡＲＰで得た情報はキャッシュされる

・２回目以降の通信ではＡＲＰは不要　①→④→⑦→⑩

・逆方向の通信ではＡＲＰは不要（すでにキャッシュされた情報を使えるため）

・一定時間無通信状態が続くとキャッシュの情報は消える

・サーバ、クライアントのＭＡＣアドレスが変わっても大丈夫

（カードの不良交換など）

・クライアントのＩＰアドレスが変わっても大丈夫

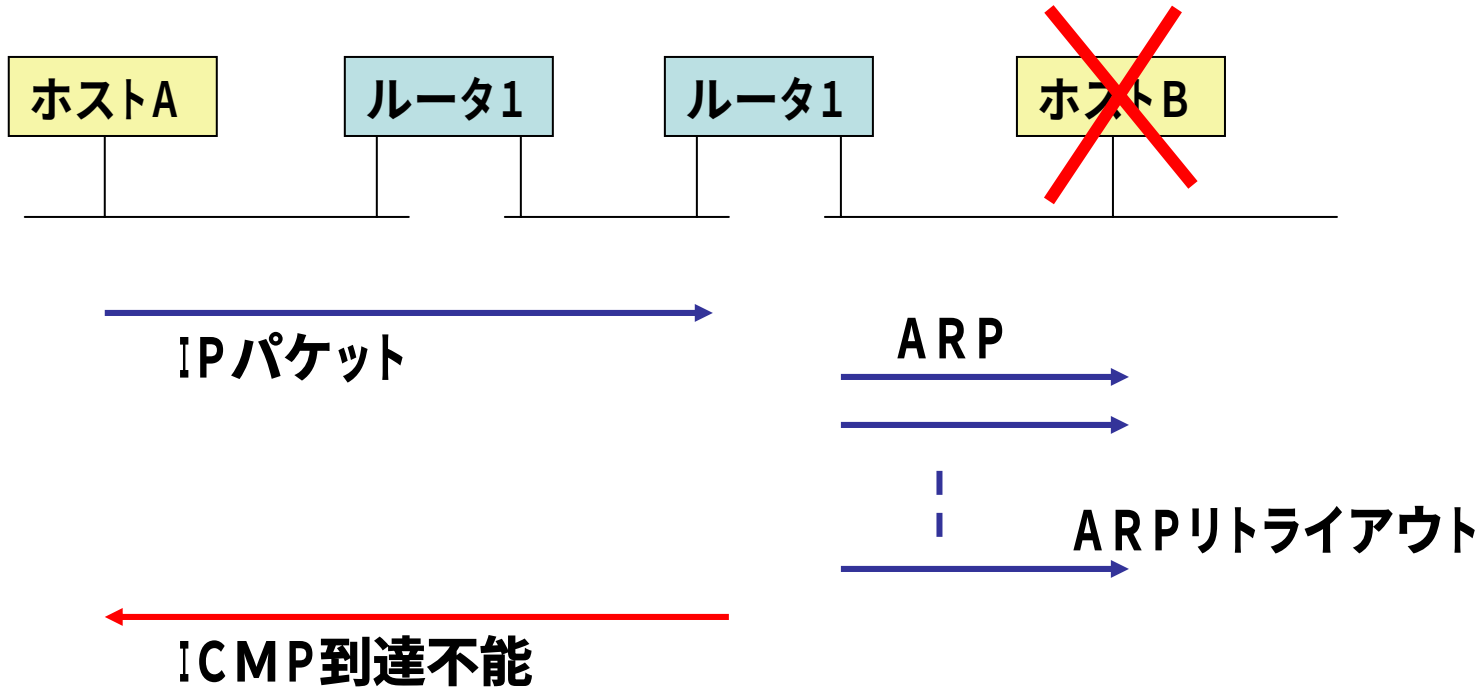
（ＤＨＣＰの適用時など）

ＩＣＭＰ(Internet Control Message Protocol)

- ＩＰを補助するプロトコル
- フォーマットはＩＰパケットを使う
- エラー通知、診断などの問い合わせ

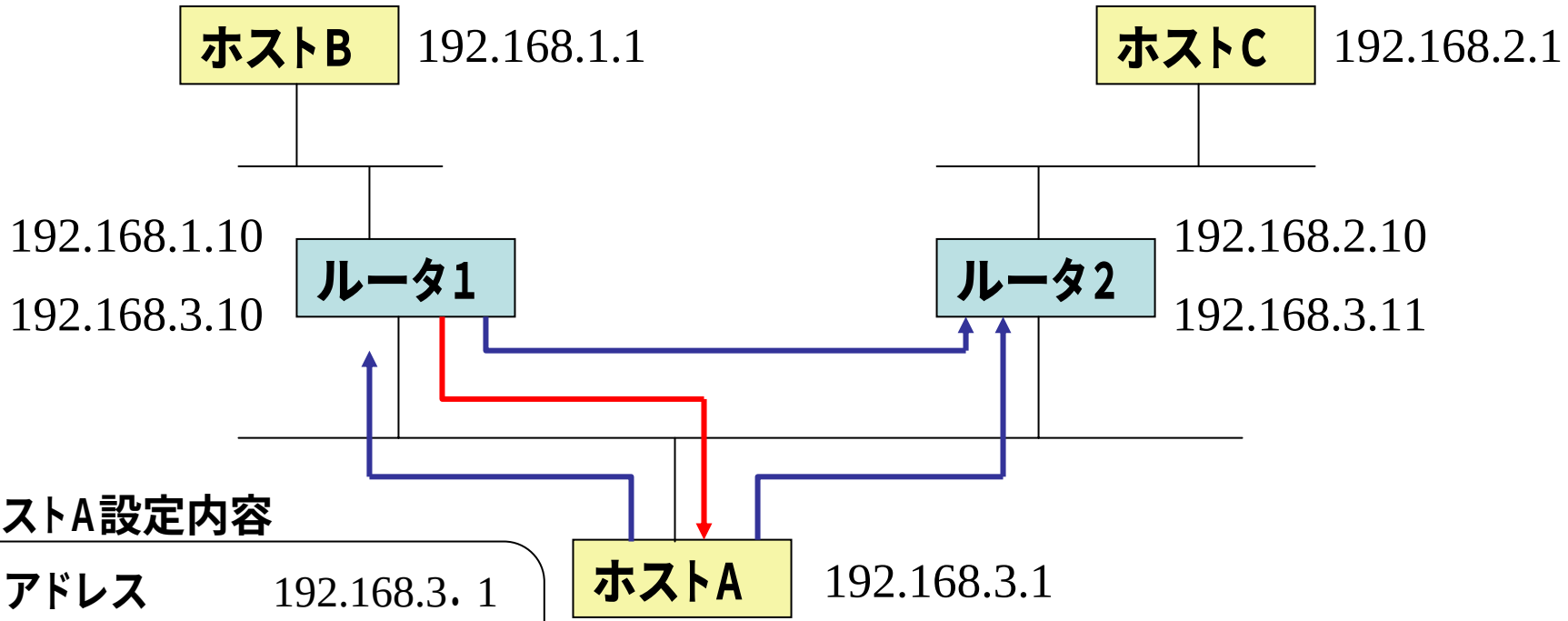
タイプ(10進)	内容
０	エコー応答(Echo Reply)
３	到達不能(Destination Unreachable)
５	リダイレクト(Redirect)
８	エコー要求(Echo Request)
１１	時間超過(Time Exceeded)

ICMP到達不能



ｺｰﾄﾞ番号	ＩＣＭＰ到達不能メッセージ
0	Network Unreachable
1	Host Unreachable
4	Fragment Needed and Don't Fragment was Set

ICMPリダイレクト



ホストA設定内容

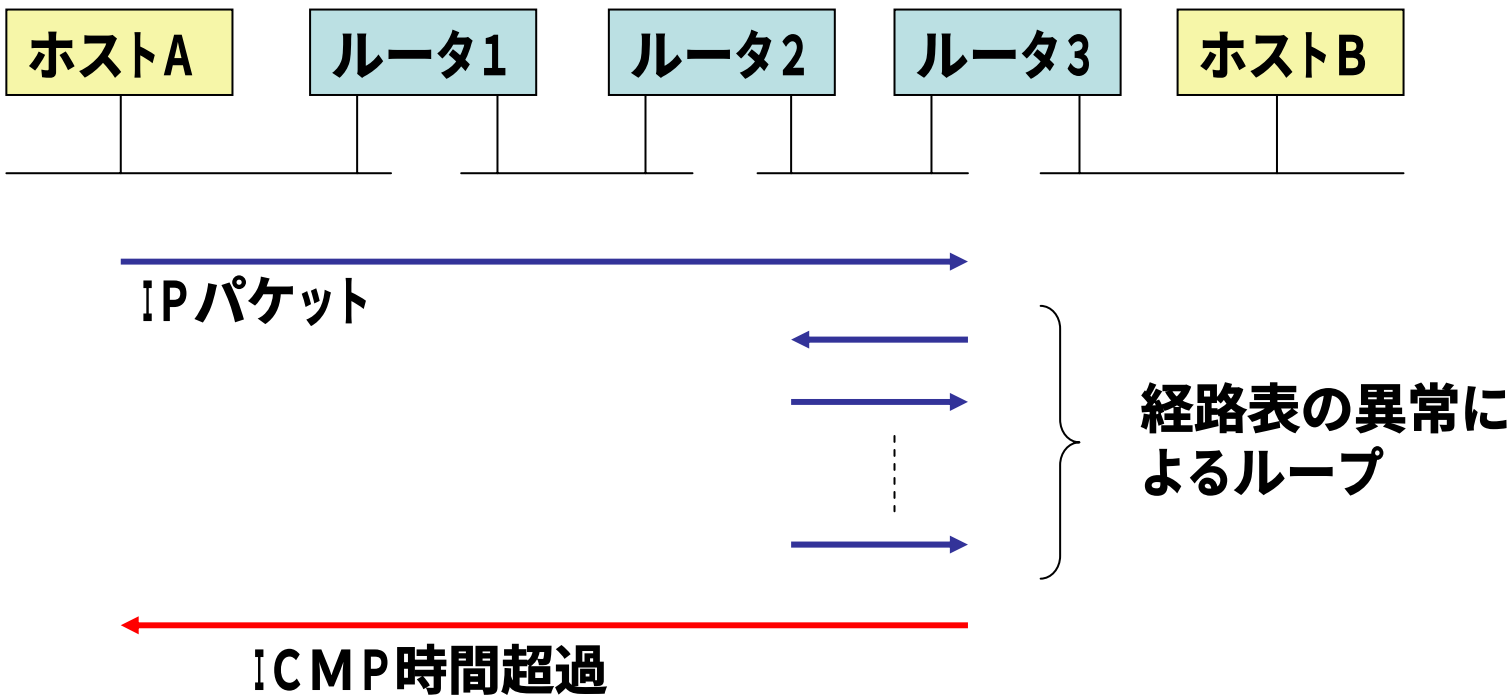
IPアドレス	192.168.3．1
ｻﾌﾞﾈｯﾄﾏｽｸ	255.255.255.0
ﾃﾞﾌｫﾙﾄｹﾞｰﾄｳｪｲ	192.168.3.10

ホストA 経路制御表

ネットアドレス	次のルータ
0.0.0.0/0	192.168.3.10
192.168.3.0/24	192.168.3.1
192.168.2.0/24	192.168.3.11

リダイレクトを受けて一部経路を変更

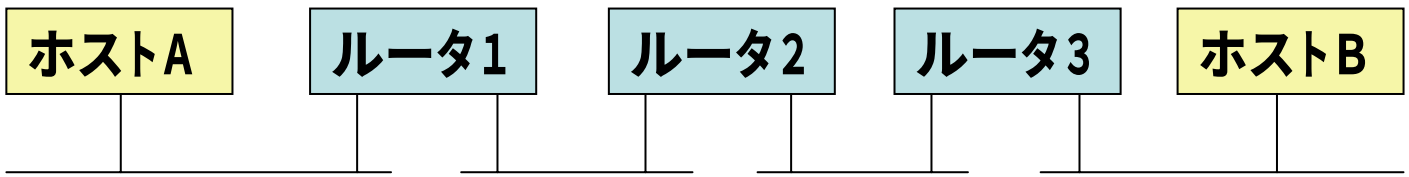
ＩＣＭＰ時間超過



ルータはIPパケットを中継するとき、ＴＴＬフィールドの値を１つ減算する。

－－－＞ＴＴＬ＝０になるとＩＣＭＰ時間超過メッセージを送信元IPアドレス宛に送信する。

ICMPエコー



ICMPエコー要求 (ホストB宛)

ICMPエコー応答

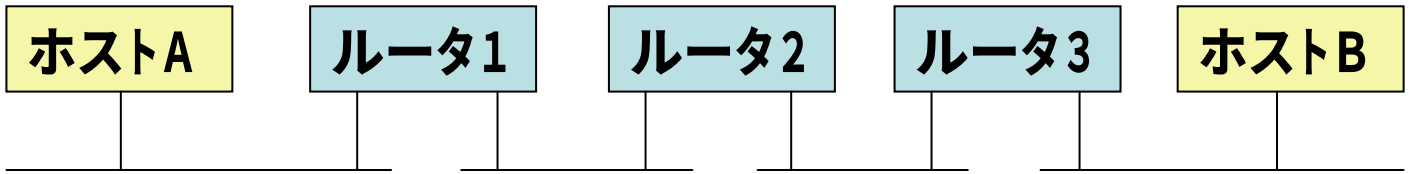
ICMPエコー要求 (ルータ2宛)

ICMPエコー応答

ICMPエコーを受信したノードは、同一の情報を送信元に返送しなければならない。

PING (Packet InterNetwork Groper)

tracert (Windows), traceroute (UNIX)



IPパケット（ホストB宛、TTL＝1）

ICMP時間超過

IPパケット（ホストB宛、TTL＝2）

ICMP時間超過

IPパケット（ホストB宛、TTL＝3）

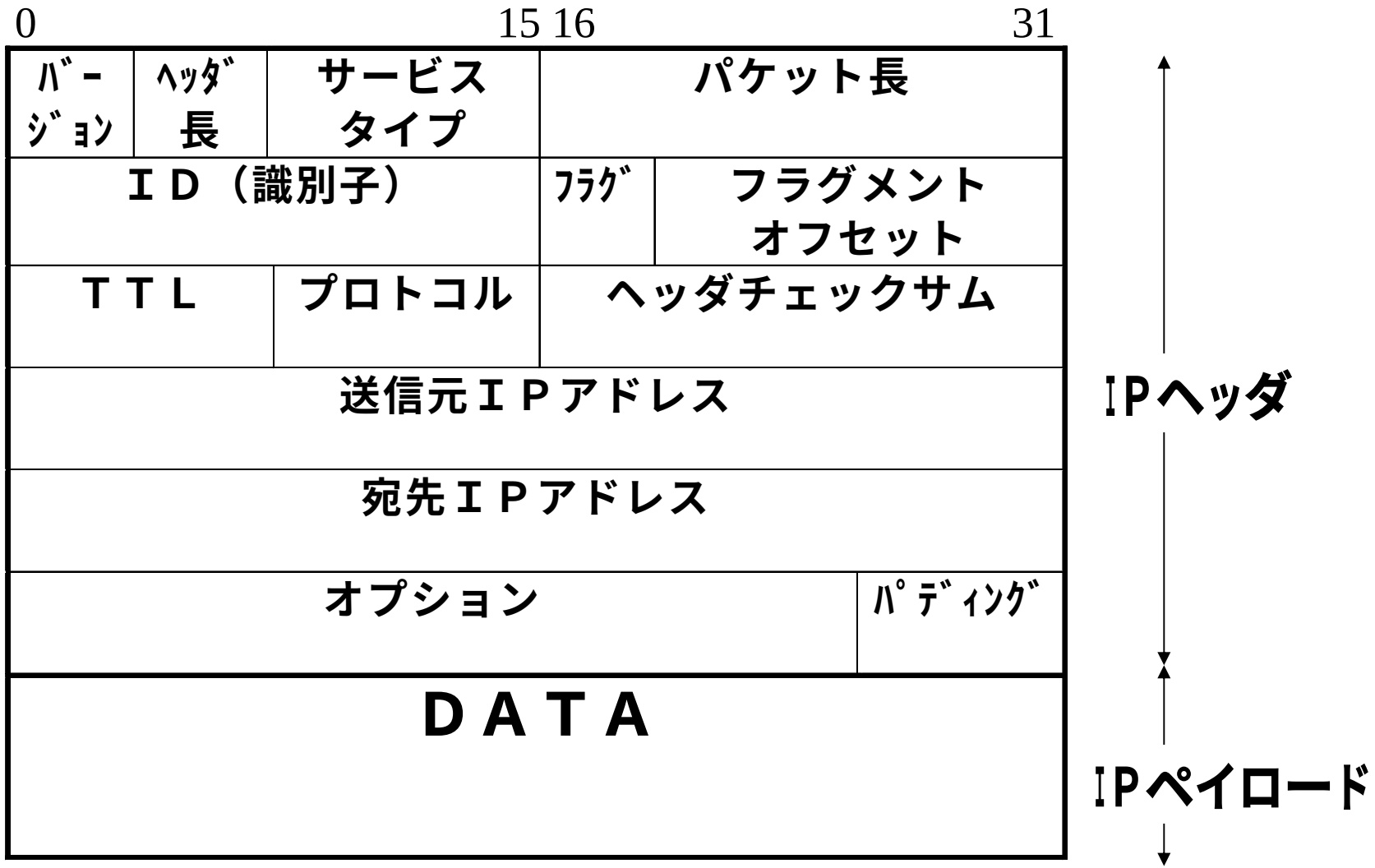
ICMP時間超過

IPパケット（ホストB宛、TTL＝4）

ICMP時間超過

宛先ホストまでの中継装置をすべて知ることができる

IPヘッダ(150)


0
15 16
31
ﾊﾞｰｼﾞｮﾝ
ﾍｯﾀﾞ長
サービスタイプ
パケット長
ＩＤ（識別子）
ﾌﾗｸﾞ
フラグメントオフセット
ＴＴＬ
プロトコル
ヘッダチェックサム
送信元ＩＰアドレス
宛先ＩＰアドレス
オプション
ﾊﾟﾃﾞｨﾝｸﾞ
ＤＡＴＡ
IPヘッダ
IPペイロード

バージョン；4または6。

ヘッダ長；ヘッダの大きさを表す。4バイト単位。オプションのない場合は5。

サービスタイプ；パケットの優先度を示す。現在ほとんど使われていない。

パケット長；IPヘッダを含めたパケット全体の長さを示す。バイト単位。
最大65535バイト（16ビット）。

ID（識別子）；IPパケットを送信するたびに1つ増加する。フラグメントを復元する歳の識別子に用いる。

フラグ；フラグメントの制御を行う。

ビット0；未使用。0でなければならない。

ビット1；分割（フラグメント）してよいかどうかを指示する。

0－分割可能

1－分割不可能

ビット2；分割されたパケットの場合、最後のパケットか否かを示す。

0－最後のフラグメントパケット

1－途中のフラグメントパケット

フラグメントオフセット；分割されたフラグメントがオリジナルデータのどこに位置していたかを示す。単位は8バイト。

TTL (Time To Live)；もともとはパケットがネットワークに存在してよい時間（生存時間）を秒単位で示したもの。実際はルータを通過するたびに1つずつ減算される。0になったらパケットは破棄される。

プロトコル；上位層のプロトコルを示す。

1； ICMP

6； TCP

17；UDP

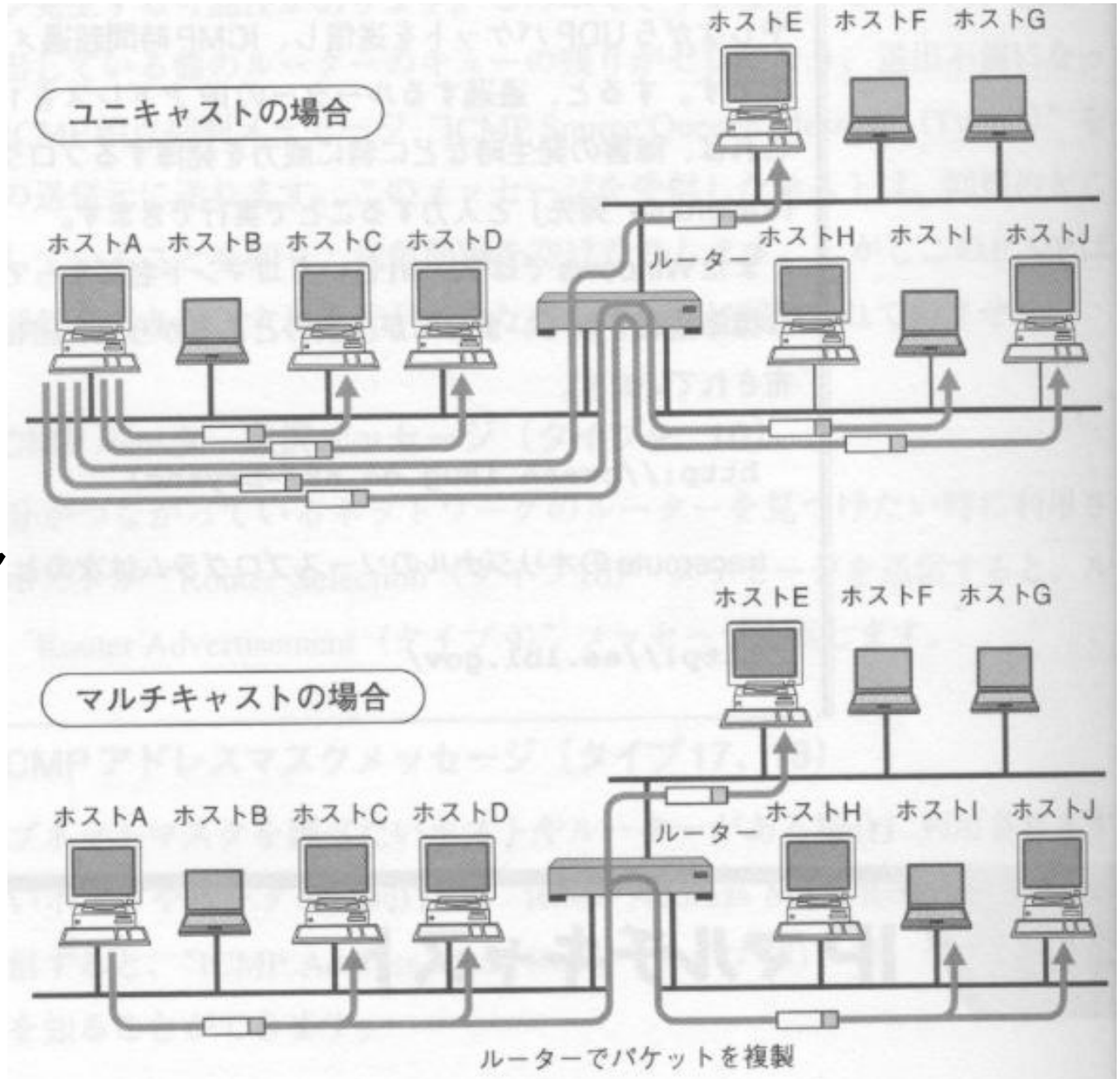
ヘッダチェックサム；IPヘッダのエラーチェック用。

送信元IPアドレス，宛先IPアドレス；エンドエンドのIPアドレスを示す。

オプション；テストやデバッグ時に使用する。通常は使わない。

パディング；ヘッダ長を32ビットの整数倍にするためのダミーデータ。

マルチキャスト



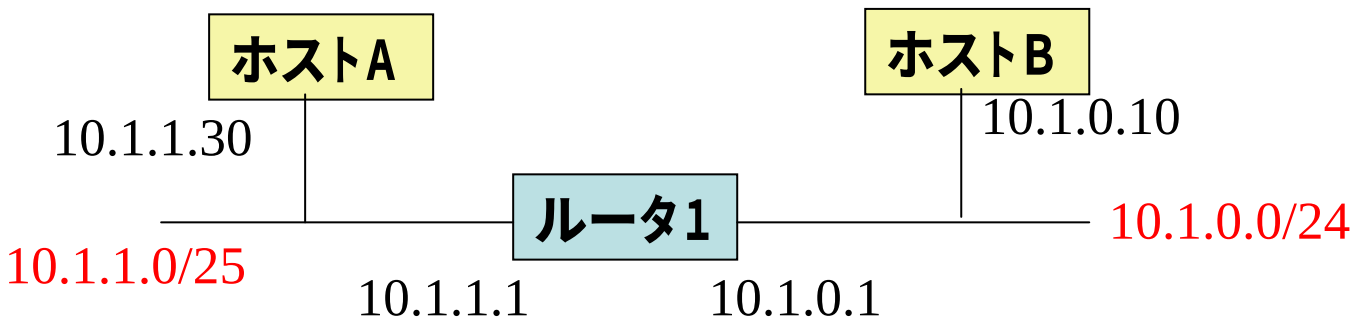
・マルチキャストアドレスを使う

・ルータでパケットを複製する

演習

①下図のネットワークにおいて、ホストA、ホストB、ルータ1が保持する経路制御表を示せ。

②ホストA→ホストBの転送を行うためにホストA、ルータ1、ホストBはどのような動作をするか。ＡＲＰの動作を含めて、経路制御表を用いて説明せよ。



ホストAの経路制御表

ネットワークアドレス	次のルータ
0.0.0.0/0	
	10.1.1.30

ルータ1の経路制御表

ネットワークアドレス	次のルータ
10.1.1.0/25	
10.1.0.0/24	