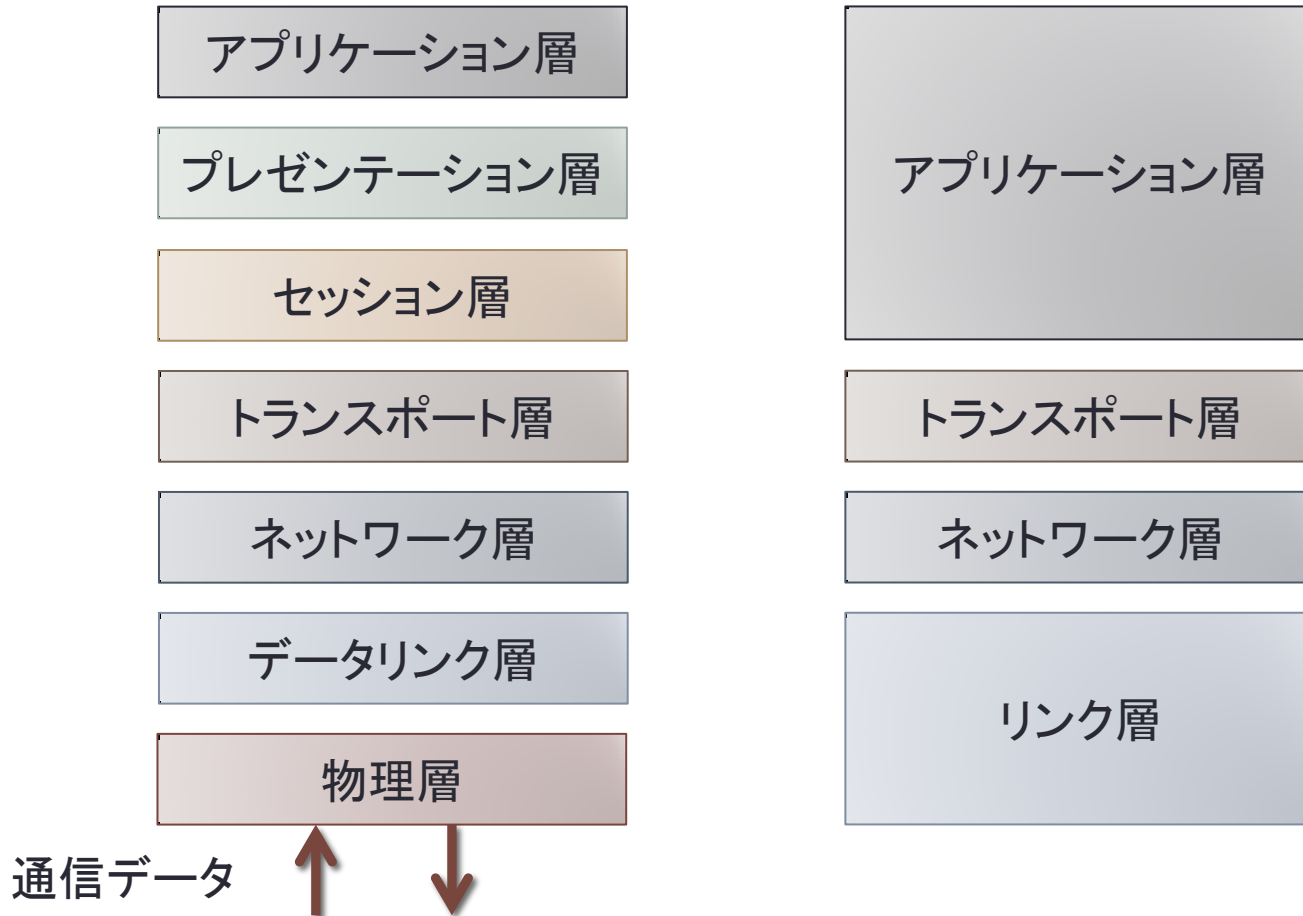


情報通信ネットワーク 第6回

理工学部情報科学科

松澤 智史

本日は……ネットワーク層(続き)



今日のコンテンツ

- ICMP(Internet Control Message Protocol)
 - ネットワーク層のもう1つの主要プロトコル
- IPv6
 - 次世代のIP

ICMP(Internet Control Message Protocol)

- ネットワーク上の到達不能ホストやネットワーク等をみつける
- ホストの生存確認を行う
- 無駄な経路を修復する

などの機能がある

ICMPエコー(要求or応答)

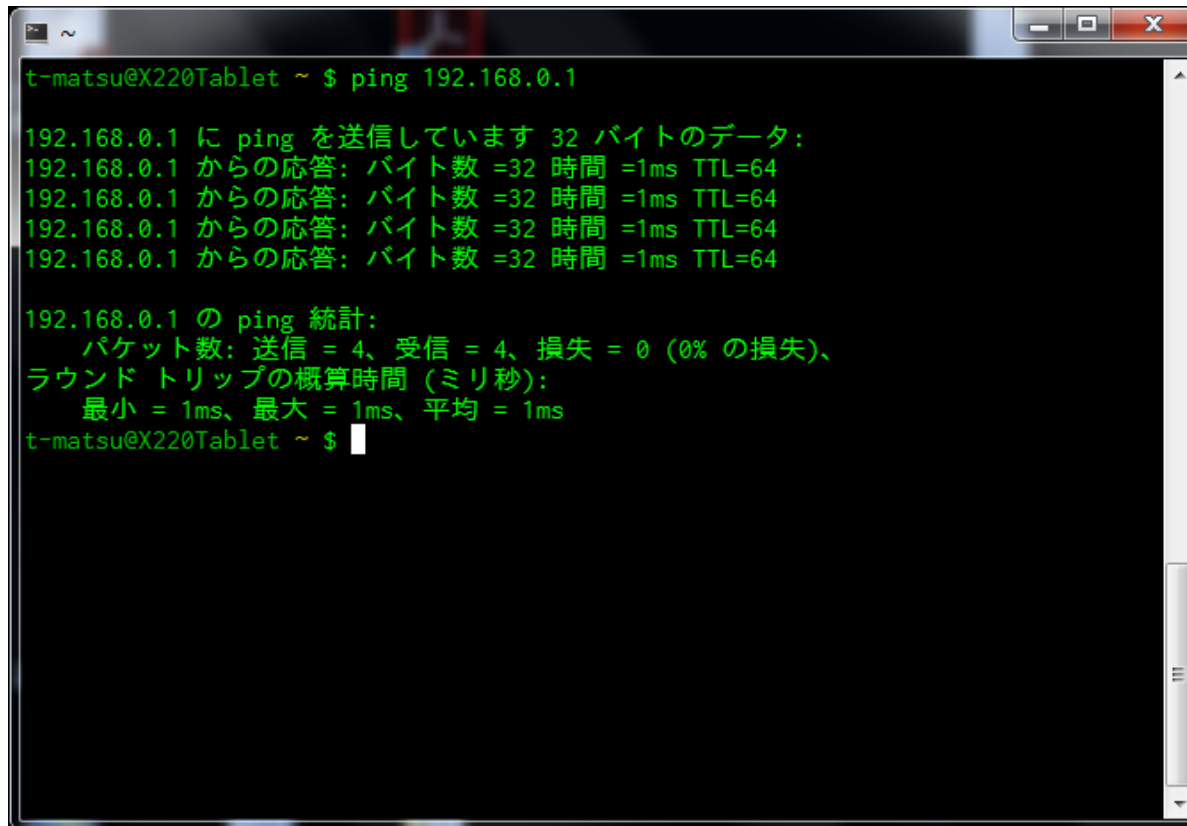
0	8	16	31
タイプ Type icmp_type	コード Code icmp_code	チェックサム Checksum icmp_cksum	
識別子 Identification icmp_id		シーケンス番号 Sequence Number icmp_seq	
データ icmp_data			

- タイプ
 - … エコー要求(8)or エコー応答(0)が入る
- コード
 - … 0が入る
- 識別子
 - … パケットの識別に使われる。(固定値が使われることも多い)
- シーケンス番号
 - … 送信側の送った順番.エコー応答は要求と同じ値を使用.
- データ
 - … バイナリデータ.エコー応答は要求と同じ値を使用.
 - (pingは時刻が入っている)

ICMPエコーを使用したプログラム

ping

- ICMPエコー要求と応答を利用したホストの生存確認



```
t-matsu@X220Tablet ~ $ ping 192.168.0.1

192.168.0.1 に ping を送信しています 32 バイトのデータ:
192.168.0.1 からの応答: バイト数 =32 時間 =1ms TTL=64
192.168.0.1 からの応答: バイト数 =32 時間 =1ms TTL=64
192.168.0.1 からの応答: バイト数 =32 時間 =1ms TTL=64
192.168.0.1 からの応答: バイト数 =32 時間 =1ms TTL=64

192.168.0.1 の ping 統計:
   パケット数: 送信 = 4、受信 = 4、損失 = 0 (0% の損失)、
   ラウンド トリップの概算時間 (ミリ秒):
     最小 = 1ms、最大 = 1ms、平均 = 1ms
t-matsu@X220Tablet ~ $
```

wiresharkで確認

The screenshot shows the Wireshark network protocol analyzer interface. The title bar indicates a local area connection (*ローカル エリア接続). The menu bar includes File (F), Edit (E), View (V), Go (G), Capture (C), Analyze (A), Statistics (S), Telephony (Y), Wireless (W), Tools (I), and Help (H). The toolbar contains various icons for file operations, capture control, and analysis. The packet list pane shows a list of captured packets, with packet 107 selected. The packet details pane shows the selected packet's structure, including the Internet Control Message Protocol (ICMP) header and body. The packet bytes pane shows the raw data of the selected packet in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
87	9.303943	192.168.0.151	192.168.0.1	ICMP	74	Echo (ping) request id=0x00...
89	9.304956	192.168.0.1	192.168.0.151	ICMP	74	Echo (ping) reply id=0x00...
96	10.303950	192.168.0.151	192.168.0.1	ICMP	74	Echo (ping) request id=0x00...
97	10.305083	192.168.0.1	192.168.0.151	ICMP	74	Echo (ping) reply id=0x00...
→ 107	11.304956	192.168.0.151	192.168.0.1	ICMP	74	Echo (ping) request id=0x00...
← 108	11.305871	192.168.0.1	192.168.0.151	ICMP	74	Echo (ping) reply id=0x00...

Internet Control Message Protocol

- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0x4d50 [correct]
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence number (BE): 11 (0x000b)
- Sequence number (LE): 2816 (0x0b00)

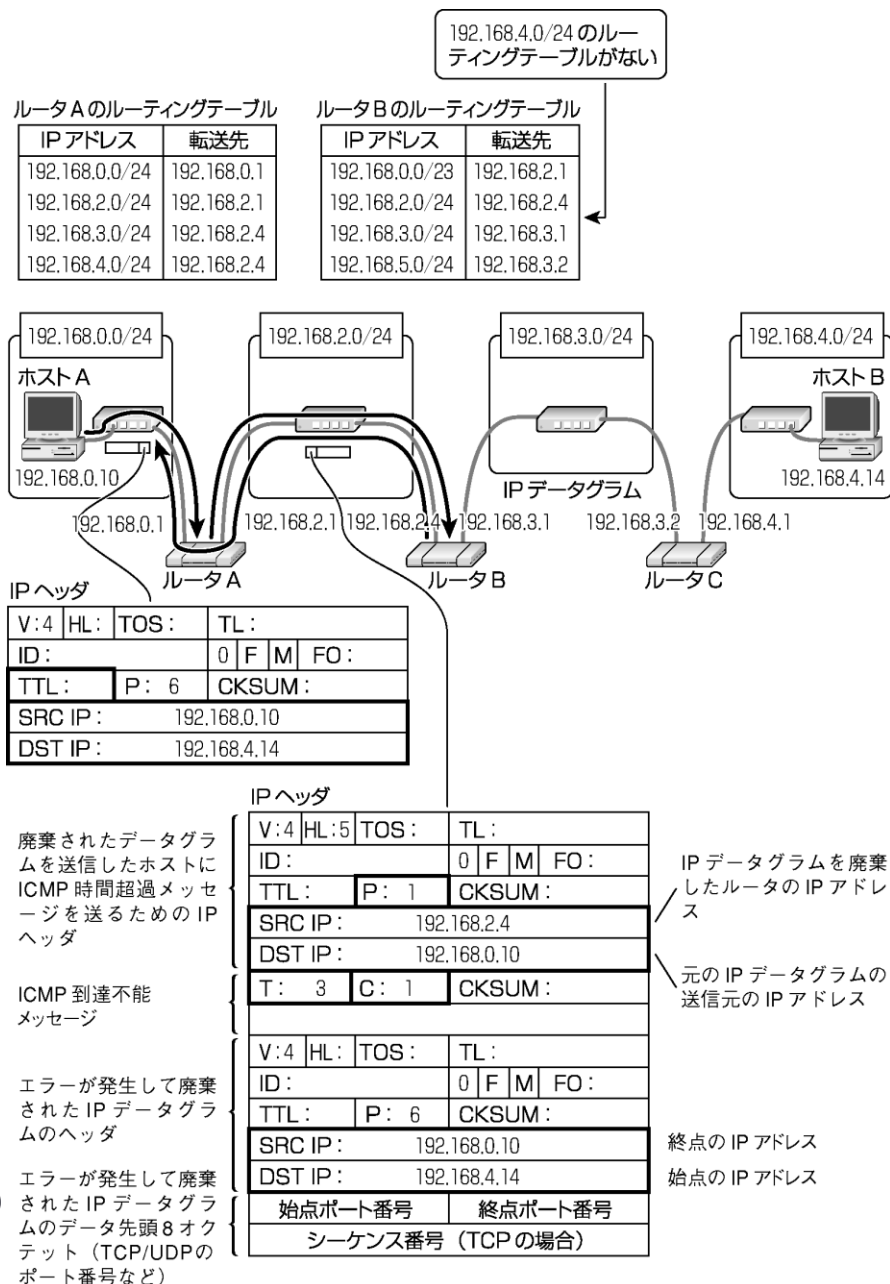
0000 00 80 6d 7a 0b 49 f0 de f1 c2 36 e1 08 00 45 00 ..mz.I.. ..6...E.
0010 00 3c 07 2a 00 00 80 01 b1 ae c0 a8 00 97 c0 a8 .<.*.... ..
0020 00 01 08 00 4d 50 00 01 00 0b 61 62 63 64 65 66MP.. ..abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

wireshark_pcapng_1BBFF53B-B1EB-4163-92E4-9DDE632394B2_20160525220827_a0114d | パケット数: 129 · 表示: 10 (7.8%) | プロファイル: Default

ICMP到達不能

0	8	16	31
タイプ Type icmp_type	コード Code icmp_code	チェックサム Checksum icmp_cksum	
未使用 icmp_pmvoid		次の MTU Next MTU icmp_nextmtu	
データ (IP ヘッダとそれに続く 64 ビット) icmp_data			

- タイプコード
- ICMP到達不能(3)が入る
0. ネットワーク到達不能
 1. ホスト到達不能
 2. プロトコル到達不能
 3. ポート到達不能
 4. フラグメントが必要だがDFフラグがたっている
 5. ソースルーティングが失敗した
- 次のMTU
- 経路MTU探索で使用する
次データリンクのMTUが入る
- データ
- エラーを発生させたIPデータグラムの
IPヘッダなどが入る



ICMPリダイレクト

0	8	16	31
タイプ Type icmp_type	コード Code icmp_code	チェックサム Checksum icmp_cksum	
ルータの IP アドレス Gateway Internet Address icmp_gwaddr			
データ (IP ヘッダとそれに続く 64 ビット) icmp_data			

- タイプ ICMPリダイレクト(5)が入る
- コード
- 0.ネットワークアドレスリダイレクト
 - 1.ホストアドレスリダイレクト
 - 2.そのネットワークに対するリダイレクト
 - 3.ホストアドレスに対するリダイレクト

ルータのIPアドレス

ルーティングテーブルの転送先に
記述するIPアドレス

次データリンクのMTUが入る

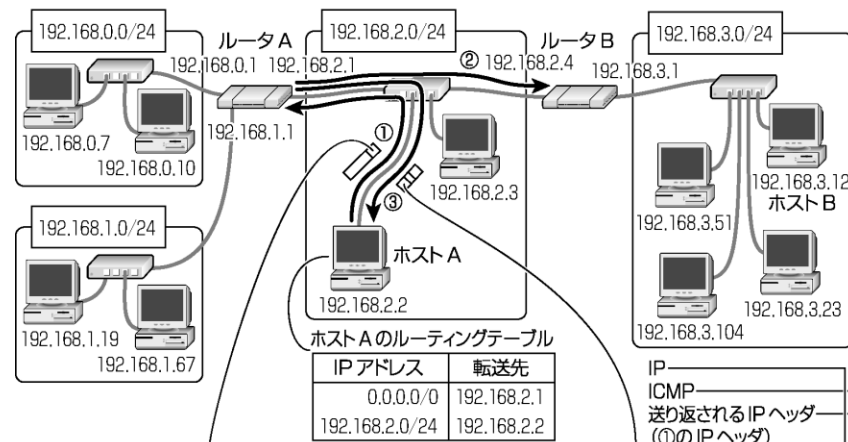
データ リダイレクトが必要と考えられる
IPデータグラムのIPヘッダなどが入る

ルータ A のルーティングテーブル

IP アドレス	転送先
192.168.0.0/24	192.168.0.1
192.168.1.0/24	192.168.1.1
192.168.2.0/24	192.168.2.1
192.168.3.0/24	192.168.2.4

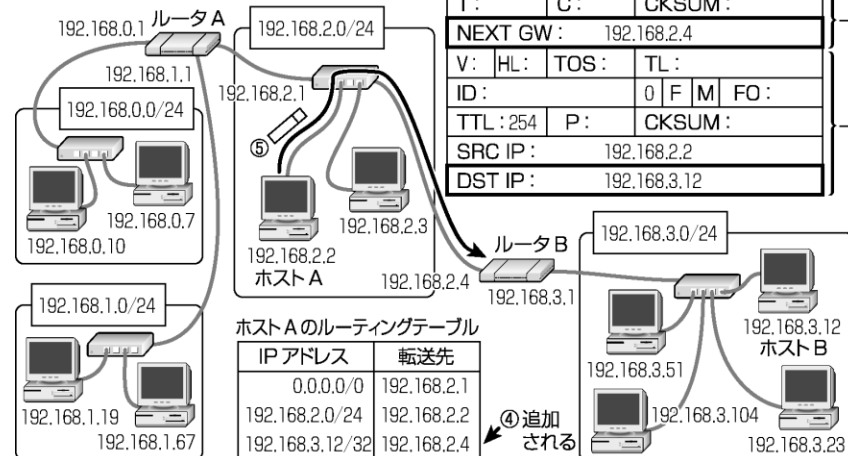
ルータ B のルーティングテーブル

IP アドレス	転送先
192.168.0.0/23	192.168.2.1
192.168.2.0/24	192.168.2.4
192.168.3.0/24	192.168.3.1



V:	HL:	TOS:	TL:			
ID:			0	F	M	FO:
TTL: 254	P:		CKSUM:			
SRC IP:			192.168.2.2			
DST IP:			192.168.3.12			

V: 4	HL: 5	TOS:	TL:
ID:		0	F M FO:
TTL: 254	P: 1	CKSUM:	
SRC IP:		192.168.2.1	
DST IP:		192.168.2.2	
T:	C:	CKSUM:	
NEXT GW:		192.168.2.4	
V:	HL:	TOS:	TL:
ID:		0	F M FO:
TTL: 254	P:	CKSUM:	
SRC IP:		192.168.2.2	
DST IP:		192.168.3.12	



ICMP時間超過メッセージ

0	8	16	31
タイプ Type icmp_type	コード Code icmp_code	チェックサム Checksum icmp_cksum	
未使用 icmp_void			
データ (IP ヘッダとそれに続く 64 ビット) icmp_data			

タイプ ICMP 時間超過(11)が入る

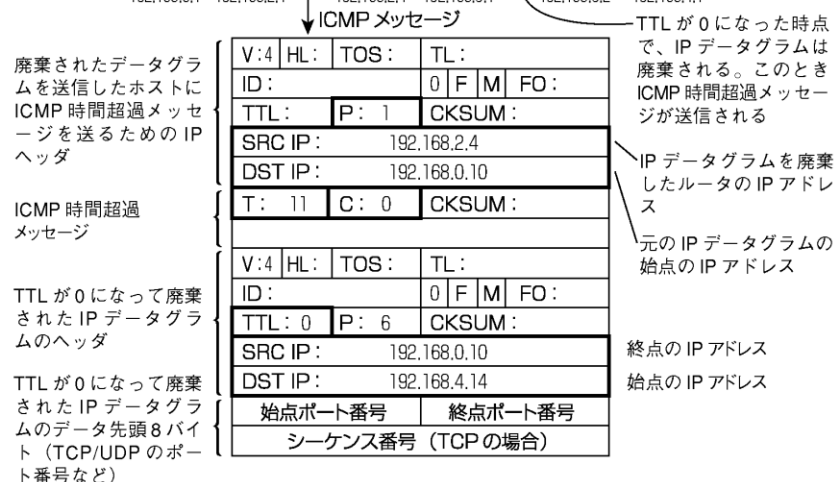
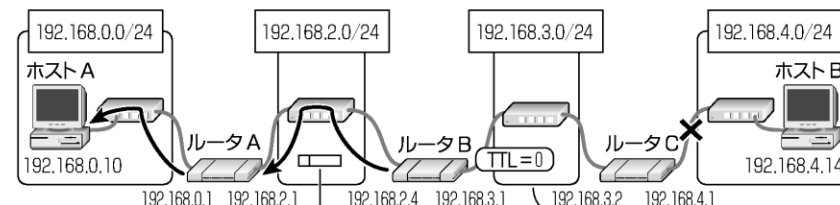
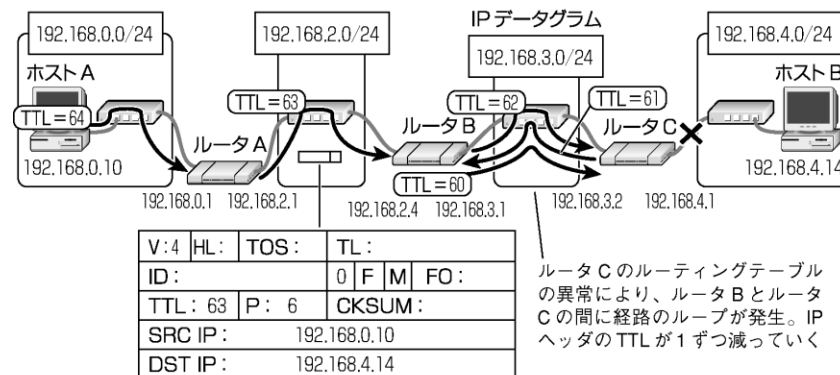
コード 0.時間超過(TTLが0になった)

データ 1.フラグメントのリアセンブルが失敗してタイムアウト
リダイレクトが必要と考えられる
IPデータグラムのIPヘッダなどが入る。

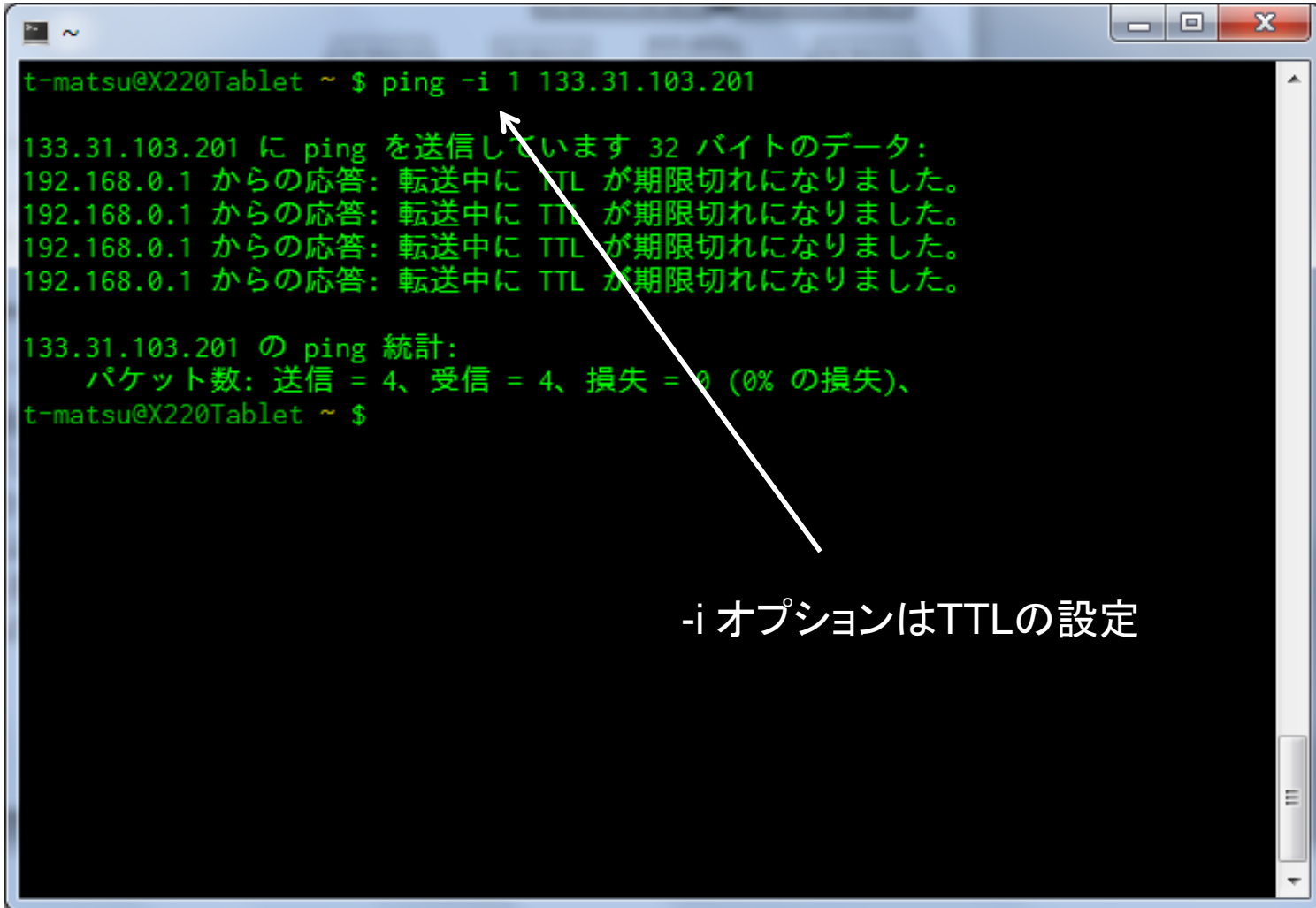
IP アドレス	転送先
192.168.0.0/23	192.168.2.1
192.168.2.0/24	192.168.2.4
192.168.3.0/24	192.168.3.1
192.168.4.0/24	192.168.3.2

矛盾

IP アドレス	転送先
192.168.0.0/23	192.168.3.1
192.168.2.0/24	192.168.3.1
192.168.3.0/24	192.168.3.1
192.168.4.0/24	192.168.3.1



ICMP時間超過メッセージ



```
t-matsu@X220Tablet ~ $ ping -i 1 133.31.103.201

133.31.103.201 に ping を送信しています 32 バイトのデータ:
192.168.0.1 からの応答: 転送中に TTL が期限切れになりました。
192.168.0.1 からの応答: 転送中に TTL が期限切れになりました。
192.168.0.1 からの応答: 転送中に TTL が期限切れになりました。
192.168.0.1 からの応答: 転送中に TTL が期限切れになりました。

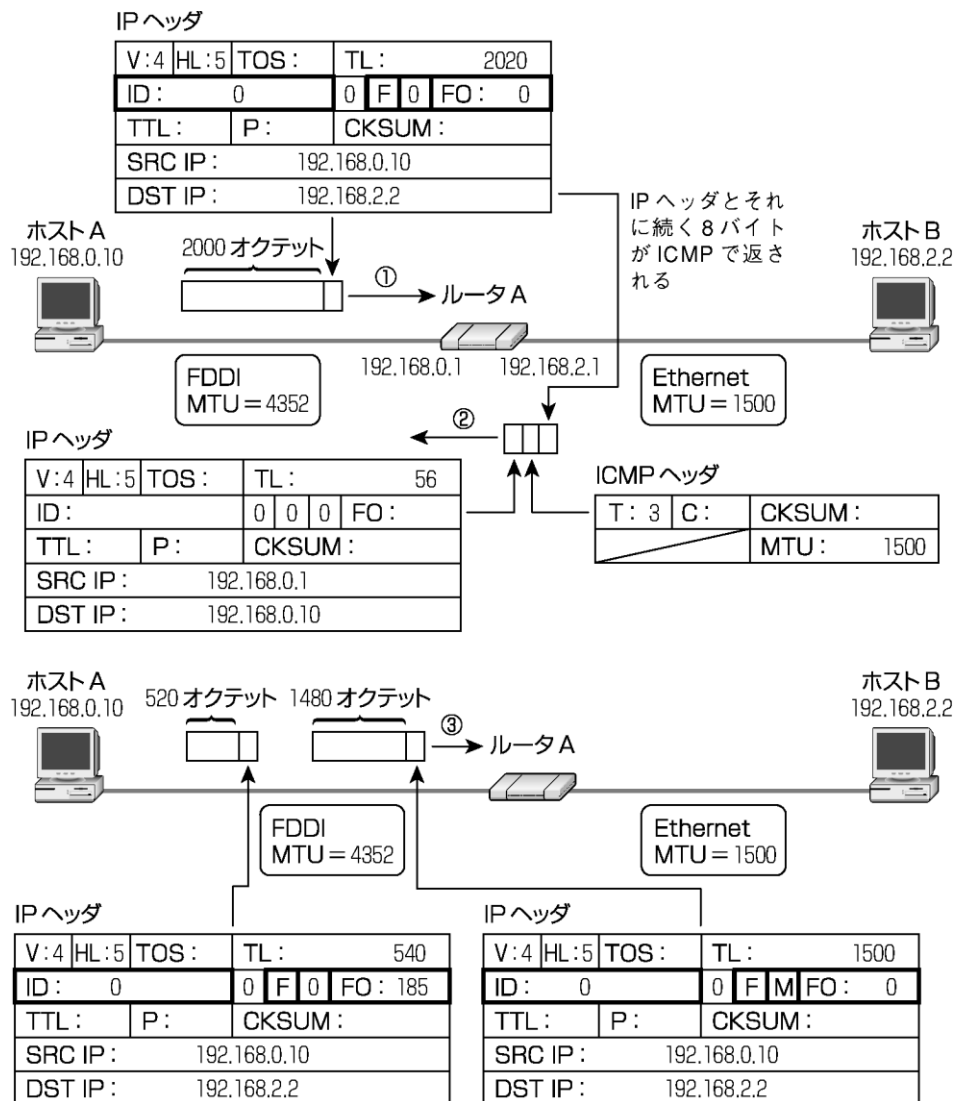
133.31.103.201 の ping 統計:
   パケット数: 送信 = 4、受信 = 4、損失 = 0 (0% の損失)、
t-matsu@X220Tablet ~ $
```

-i オプションはTTLの設定

ICMPの注意点

- 概念的にはネットワーク層プロトコルであるが、実装ではIPの上位層に位置する
 - 下位に必ずIPを用いる
- 便利であるが、大量の応答パケットを生成させることもできるためICMPを通さない設定のルータも多い

経路MTU探索



フラグメントの問題点

1. ルータの負荷の上昇
2. フラグメント化データ喪失時の転送効率低下

途中のルータでは出来るだけフラグメント処理を発生させない方が良い。

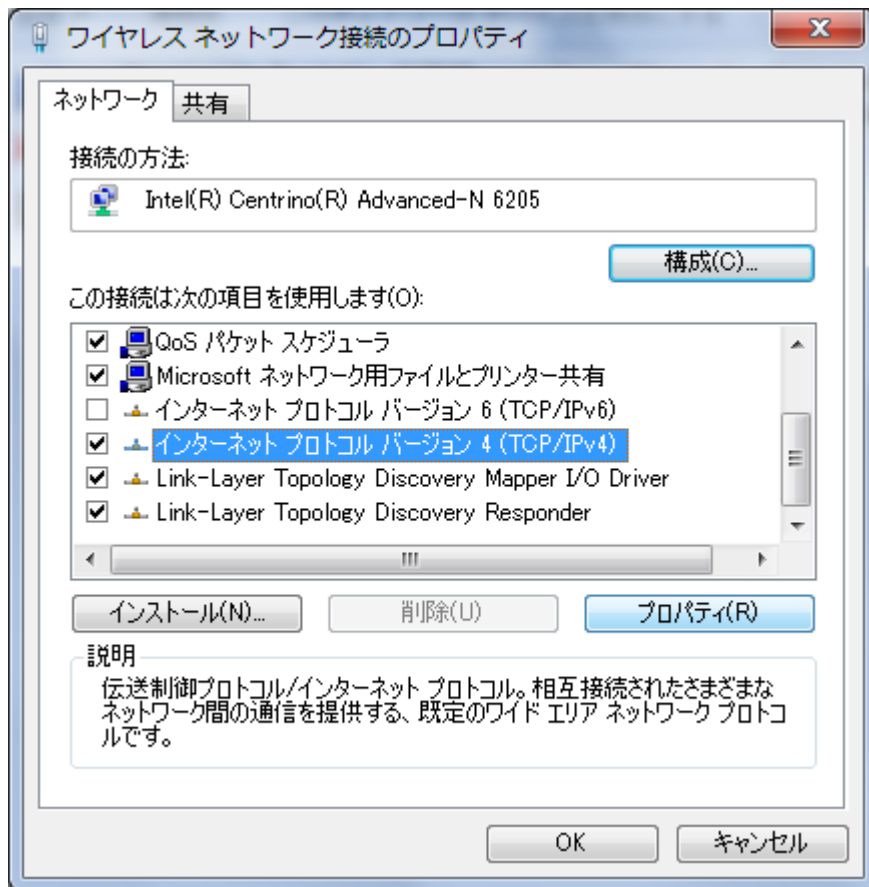
が

IPパケットのサイズを小さくすると転送効率が悪くなる。

この解決法が経路MTU探索である。

これでIP,ICMPの話はおしまい

実践してみよう まずはIP自力設定



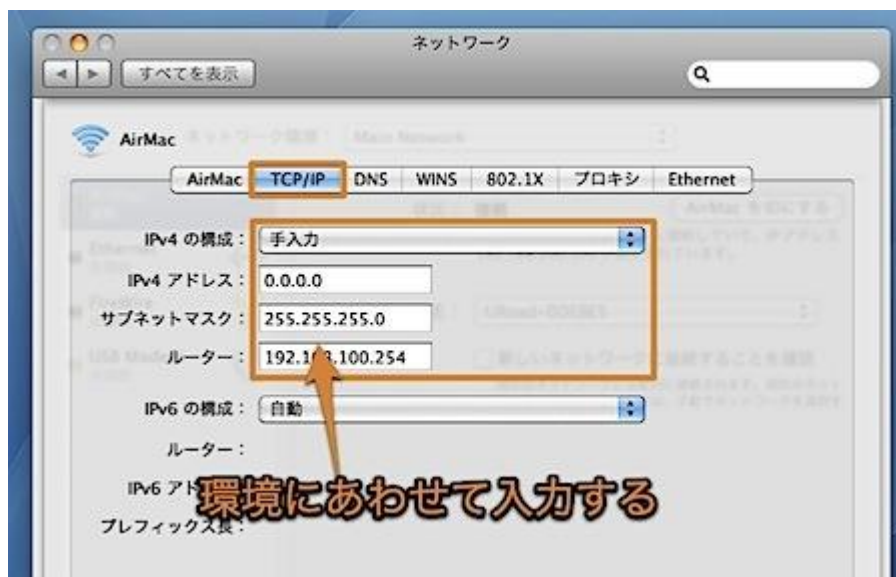
Windows

1. (マイ)ネットワーク右クリック
2. プロパティ
3. アダプタの設定
4. 対象を右クリック
5. プロパティ

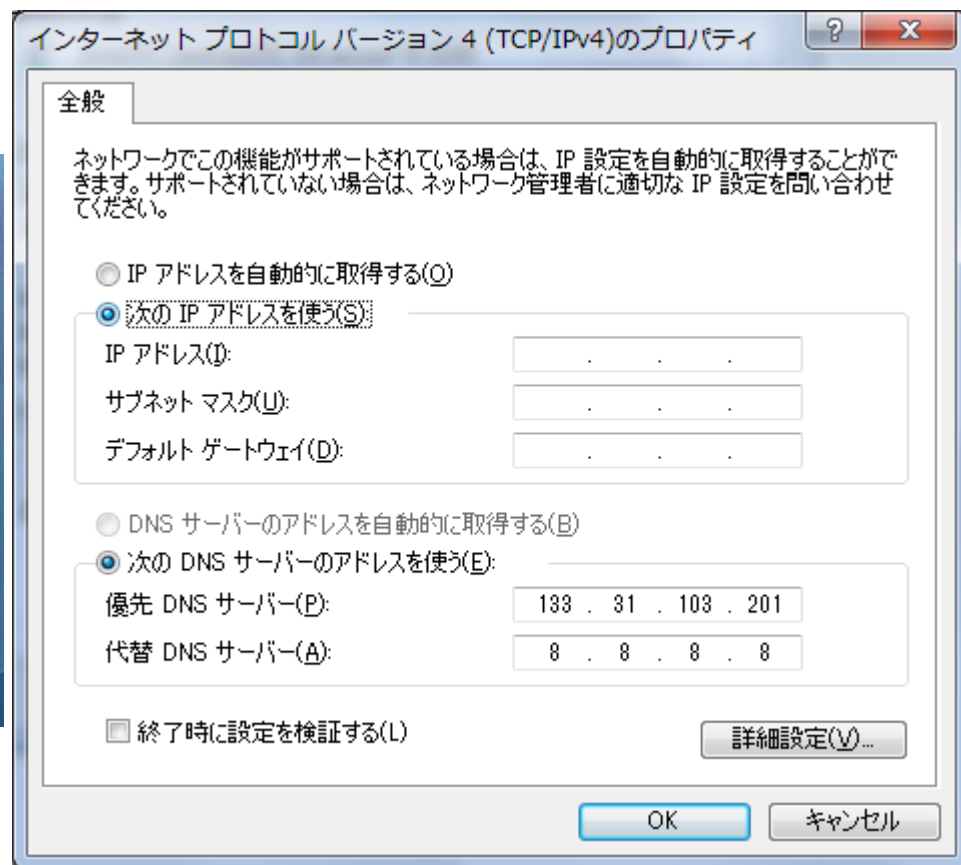
Mac

1. システム環境設定
2. ネットワーク
3. TCP/IPタブ
4. IPv4の構成

IP設定画面



MAC



Windows

手動設定するIPアドレスは **192.168.11.学籍番号** を名乗ること

実験

- サブネットマスクを0.0.0.0にするとどうなる？
- 他の人にpingを飛ばしてみよう
 - arpのパケットも確認できる
- ブロードキャストアドレスにpingを飛ばすとどうなる？
- それぞれの様子をwiresharkで観察してみよう

IPv6

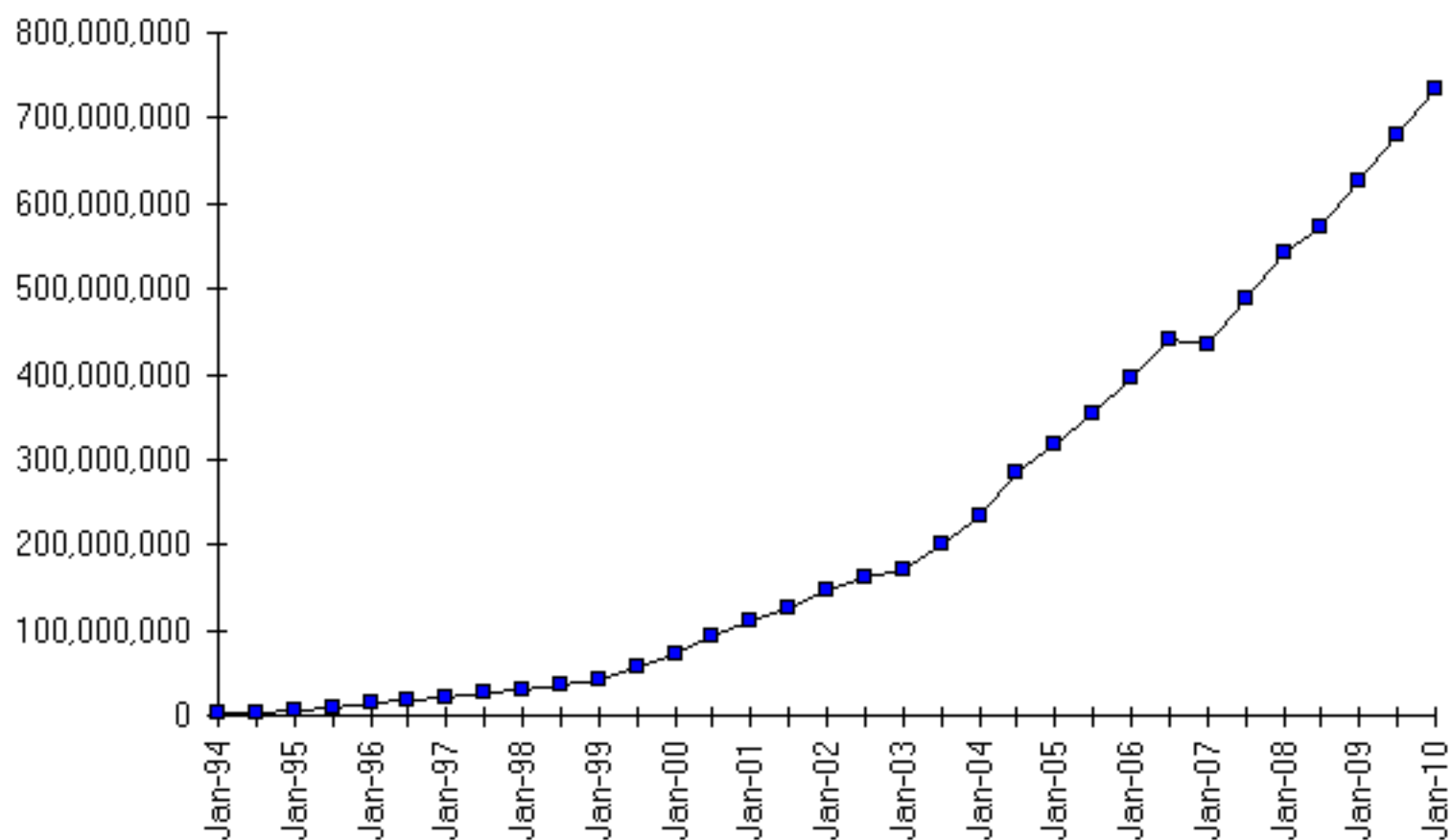
- 次世代のInternet Protocol
- 前回までの講義で扱ったIPはv4
- 転送効率, 機能ともにIPv4を上回る……………が,
そこまで普及していない**悲しいプロトコル**

誕生の背景

IPv4アドレスの枯渇

- おさらい: IPv4は32bit \Rightarrow 43億個のアドレス
- インターネットのユーザは約33億
(<http://www.internetworldstats.com/stats.htm> 2016 5/25確認時点)
- 一人当たり1～2個のグローバルアドレスを使用できる計算になる

Internet Domain Survey Host Count



Source: Internet Systems Consortium (www.isc.org)

実はこのIPアドレス枯渇の話・・

- 90年代後半からあと数年でIPアドレスは足りなくなると言われてきた
- 月日は流れ、もうあれから15年近い歳月が流れた・・・・・
- その間、何度もあと数年でIPアドレスは足りなくなると言われてきた

足りない詐欺

にもかかわらず、
近年またIPアドレスの枯渇問題が再燃



IPアドレス枯渇問題の理由を知ろう

IPアドレス割り当ての仕組み

IPアドレスの割り当ては、IANA(Internet Assigned Numbers Authority)が調整し、アドレスブロックを地域IPレジストリ(北米はARIN、ヨーロッパはRIPE、アジア太平洋はAPNIC)に割り当てることによって実行されている。これを受けて次に、大規模ISP(インターネットサービスプロバイダー)が地域IPレジストリに対して IPアドレスブロックの割り当てを申請する。アドレスブロックを割り当てられた大規模ISP は、その中から、小規模ISP に対してアドレスを割り当てることになる。さらにそれはエンドユーザーへの割り当てへとつながる。

(JPNIC から抜粋)

つまりIPアドレス使用の権利を大元から一部委譲される形を取っている

割り当て方

アドレスブロック(連続した固まり)をまとめて譲り受ける

悪名高きクラスフル割り当て

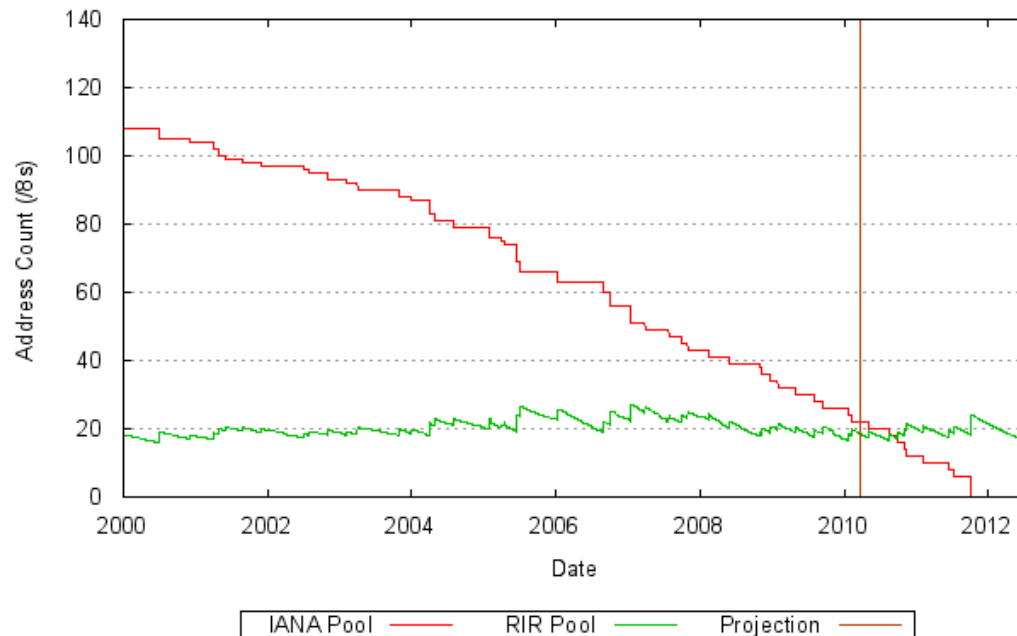
- クラスA ネットワーク部8bit ホスト部24bit 256の組織に16,777,216個ずつ
- クラスB ネットワーク部16bit ホスト部16bit 65535の組織に65535個ずつ
- クラスC ネットワーク部24bit ホスト部8bit 16777216の組織に256個ずつ

IPアドレス枯渇問題の理由を知ろう

CIDR (Classless Inter-domain Routing) 採用で多少緩やかになったが、使用しているアドレス/確保しているアドレスはどこも1-3割程度が現状

- 2009年8月の段階で未割り当てIPアドレスは約5億個ある
- 年間2億のペースで割り当てられている

演繹法での予測



IPアドレス枯渇問題の理由を知ろう

なぜ2011年までもったか？

- CIDR採用による割り当ての工夫 (クラスBの分割など)
- DHCPによるIPアドレスの動的使用による共有利用
- NAT等による有効利用

IPアドレス枯渇問題の解決法？

アドレスの有効利用しよう的な方法（延命措置）

- 既割り当て未使用IPを減らす
 - IPアドレスの回収・分割割り当て
- アドレス1つあたりの利用ホストを増やす
 - プライベートアドレス割り当て
 - ラージスケールNAT(キャリアグレードNAT)

アドレス空間を広げちゃおう的な方法

- IPv6

2008年あたりから色々な団体で枯渇の対処やIPv6の導入の必要性を公的に発表

米国防総省 <http://www.internetnews.com/bus-news/article.php/3286831>

IPv4アドレス枯渇対応タスクフォース <http://kokatsu.jp/blog/ipv4/>

NIC <http://www.nic.ad.jp/ja/ip/ipv4pool/ipv4exh-report-071207.pdf>

総務省 http://www.soumu.go.jp/menu_news/s-news/2008/pdf/080617_2_bt1.pdf

IPv6これまでの歴史

- 1992年 INET92にて技術標準化の話が検討される
- 1993年 IETFにIPng(Internet Protocol Next Generation)が設けられる
- 1994年 IETFでSIPPのアドレス長を128bitに拡張したSIPP16をIPngの基本仕様検討のベースとして採用しIPv6と命名される
- 1998年 WIDEプロジェクトのメンバー達が中心となったKAME/TAHI/USAGIプロジェクトによるソフトウェアの開発研究開始
 - KAME BSD系OSでのIPv6実装プロジェクト (刈込から命名)
 - TAHI IPv6プロトコル検証技術開発プロジェクト
 - USAGI LinuxのIPv6プロジェクト
- 2006年 プロトコルスタックが統合され, KAMEプロジェクト終了



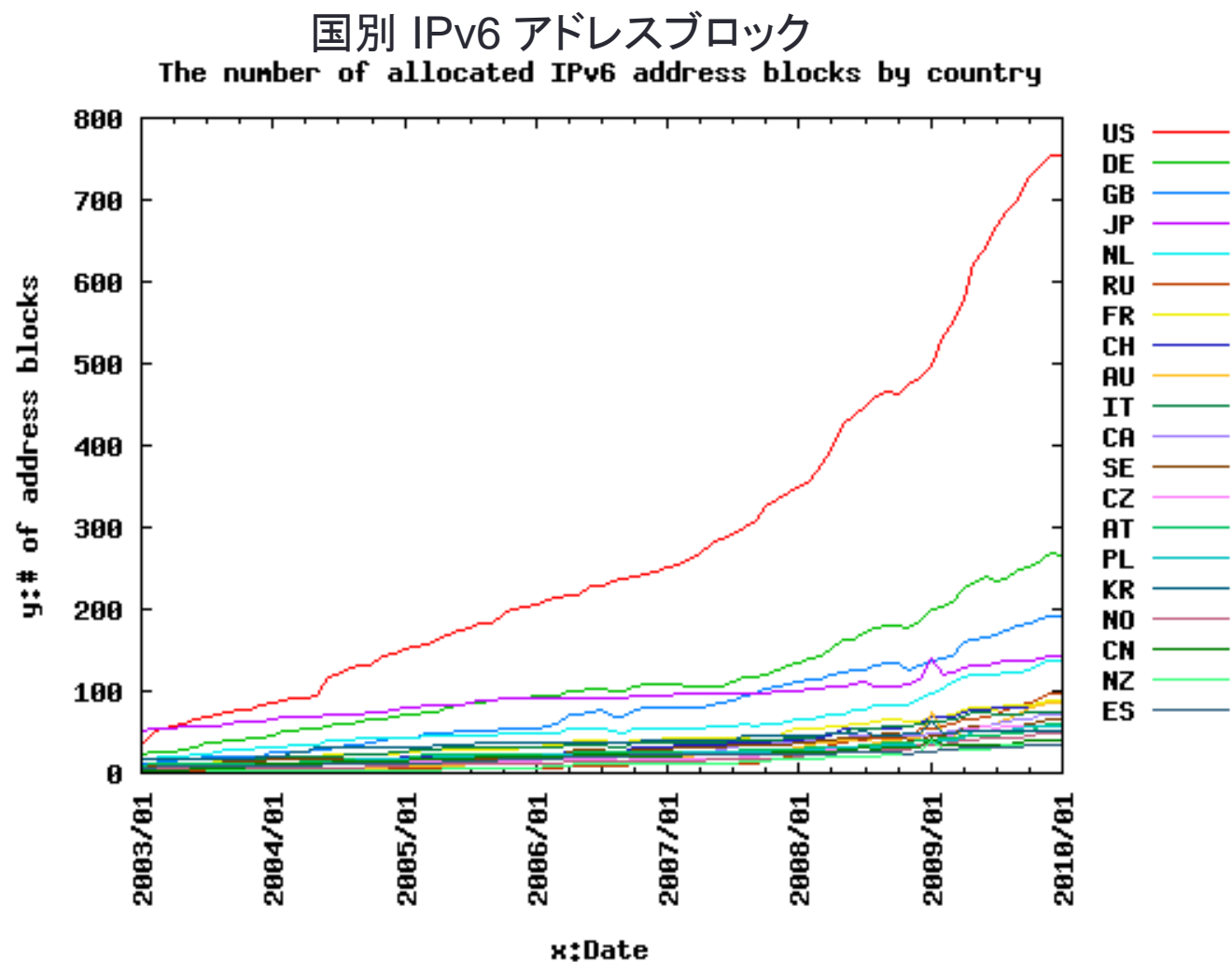
IPngの候補とその選定

- IPngの候補はよく似たものを含め多くの提案があったが、最終的に以下の3つに絞られた
 - CATNIP(Common Architecture for Next Generation Internet Protocol)
 - IP CLNP IPXの統合を目指したプロトコル
 - SIPP(Simple Internet Protocol Plus)
 - IPv4からの発展型としての提案で、IPv4でうまく機能していたものは残し、機能していないものは削除したプロトコル
 - TUBA(TCP and UDP with Bigger Addresses)
 - CLNPでIPv4を置き換え、アドレス空間の拡張を行ったプロトコル NSAP(Network Service Access Point)と呼ばれる可変長アドレス空間が特徴
- 選定基準の19項目によりCATNIPはまだ検討不十分で未完成すぎたため、最終的にはSIPPとTUBAの2つに絞られた
- アドレス空間が固定長、可変長であることが議論になり、プログラマの敷居をあげてインターネット発展を削ぐことがないよう、固定長のSIPPが採用され、以後の拡張をIPv6と名付けられた

IPv6の特徴

- アドレス空間
 - IPv4 32bit $2^{32} = 4.29 \times 10^9$
 - IPv6 128bit $2^{128} = 3.40 \times 10^{38}$
 - 世界人口60億, 人間の細胞を60兆個とすると, 細胞1つに約940兆個のアドレスをつけてもまだ余る
- 新たな機構
 - シンプルな構造・高い拡張性
 - アドレスの階層化
 - セキュリティ
 - プラグアンドプレイ
 - QoS通信サポート
 - マルチキャスト通信サポート
 - モビリティサポート
- 新規構築の効果
 - IPv4でオプション実装されていたものが基本実装になっていることにより, 様々なサービスや規格の策定が容易になる

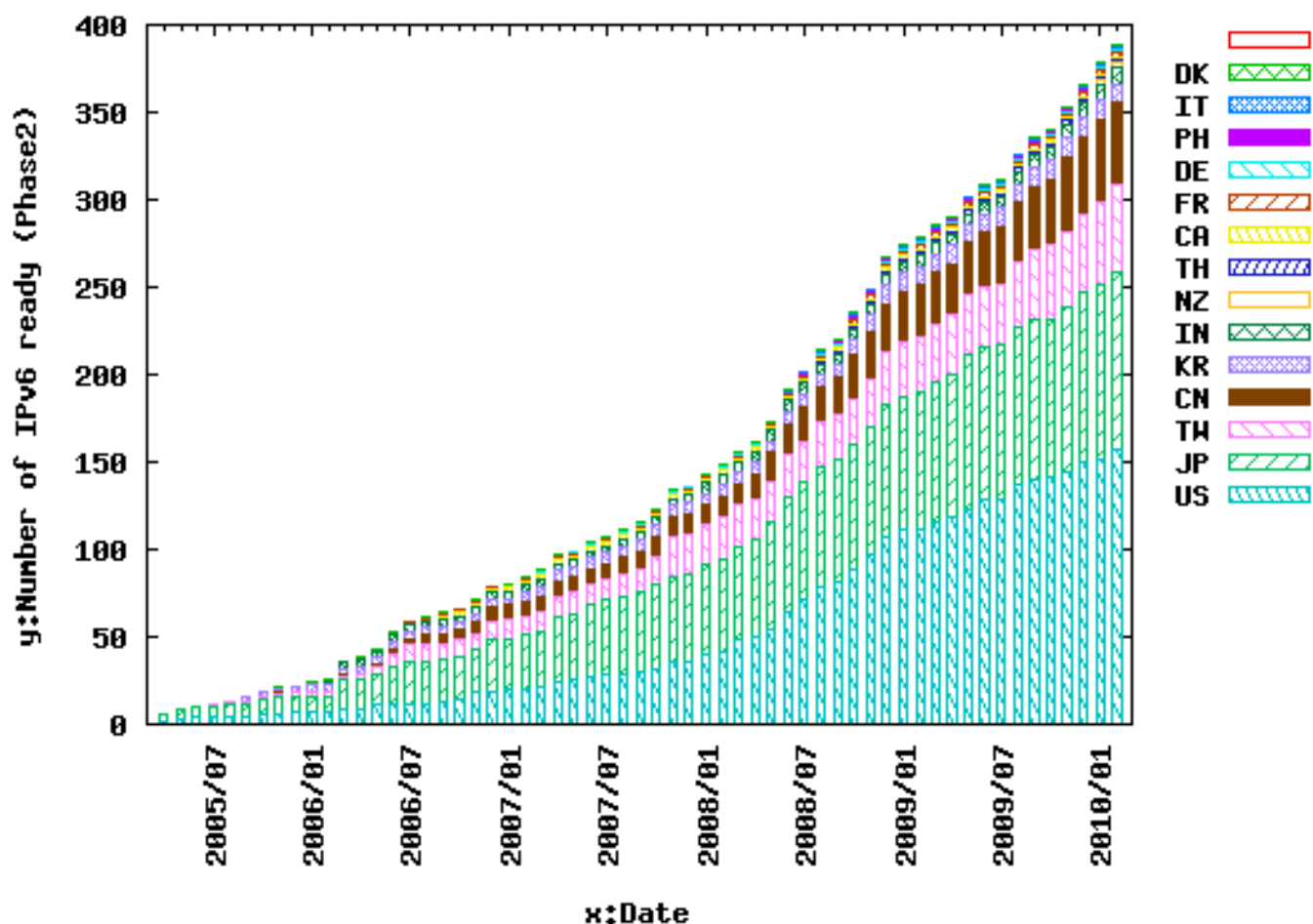
IPv6普及状況



IPv6普及状況

国別 Phase2 の登録機器数

The number of IPv6 ready (Phase2) by country



IPV6 アドレッシング

IPv6のアドレッシングアーキテクチャ

□ アドレスタイプ

- ユニキャストアドレス
- エニーキャストアドレス
- マルチキャストアドレス

□ アドレッシングモデル

- ノード単位ではなくインタフェース単位に割り当てられる
- すべてのインタフェースは最低1つのリンクローカルアドレスを持ち、リンク外との通信時には、さらにグローバルアドレスorサイトローカルアドレスを割り当てる

□ アドレスの表記方法

- 128bitのアドレスを16bitごとに”.”で区切って16進数表記する
 - 3ffe:0500:1010:0200:0000:0000:0000:0009 連続する0は省略可能
 - 3ffe:500:1010:200:0:0:0:9 連続する複数のフィールドで0が続く場合は1か所のみ”.”で省略可能
 - 3ffe:500:1010:200::9
- IPv4アドレス表記との併用も可能
 - 0:0:0:0:FFFF:192.168.1.1 → ::FFFF:192.168.1.1
- プレフィックス表記はIPv4と同様に使用できる
 - 3ffe:500:1010:200:0:0:0:0/64

IPv6のアドレッシングアーキテクチャ

- アドレスブロックの割り当て

プレフィックス	割り当て	プレフィックス	割り当て	プレフィックス	割り当て
0000 0000	予約済	001	集約可能グローバルアドレス	1111 0	未割当
0000 0001	未割当	010	未割当	1111 10	未割当
0000 001	NSAPアドレス マッピング用予約済	011	未割当	1111 110	ユニークローカル ユニキャストアドレス
0000 010	IPXアドレス マッピング用予約済	100	未割当	1111 1110 0	未割当
0000 011	未割当	101	未割当	1111 1110 10	リンクローカル アドレス
0000 1	未割当	110	未割当	1111 1110 11	サイトローカル アドレス
0001	未割当	1110	未割当	1111 1111	マルチキャスト アドレス

IPv6のアドレッシングアーキテクチャ

□ユニキャストアドレス

アドレスを2部位にわけ、上位をサブネットプレフィックス、下位をインタフェースIDと呼ぶ

□集約可能グローバルユニキャストアドレス

□IPv4アドレス埋め込み型IPv6アドレス

□IPv4互換IPv6アドレス

□IPv4マップド(射影)IPv6アドレス

□ローカル利用IPv6ユニキャストアドレス

□リンクローカルユニキャストアドレス

□サイトローカルユニキャストアドレス

□特別なアドレス

□未定義アドレス

□ループバックアドレス

□エニーキャストアドレス

複数のインタフェースに割り当てられたアドレスでエニーキャストアドレス宛に送出されたパケットは「最も近い1つの」インタフェースに届けられる

□マルチキャストアドレス

インタフェースのグループに割り当てられたアドレスで、そのアドレス宛に送出されたパケットは、「そのグループに所属するすべての」インタフェースに届けられる

集約可能グローバルユニキャストアドレス

- RFC 2374『IPv6 の集約可能グローバルユニキャストアドレス形式』

3bit	13bit	8bit	24bit	16bit	64bit
001	TLA ID	Res	NLA ID	SLA ID	Interface ID

- TLA(Top Level Aggregation)
- Res(Reserve)
 - 使用されない
- NLA(Next Level Aggregation)
 - NLAは更に分割可能 その場合は(NLA1,NLA2,...)となる
- SLA(Site Level Aggregation)

IPv4アドレス組み込み型IPv6アドレス

- IPv4互換IPv6アドレス

- IPv6を利用してIPv4インフラストラクチャ上でデータを交換するデュアルスタックノードにより使用されるアドレス
- 0:0:0:0:0:0:133.31.103.10 または ::133.31.103.10 などと表記される

80bit	16bit	32bit
0000.....000	0000	IPv4 アドレス

- IPv4マッピング(射影)IPv6アドレス

0:0:0:0:0:FFFF:133.31.103.10 または ::FFFF:133.31.103.10 などと表記される

- IPv4専用ノードをIPv6ノードとして表現するために使われる
- 内部表現のためにのみ使用でき, IPv6パケットの送信元アドレスや宛先アドレスとして使用されることはない

80bit	16bit	32bit
0000.....000	FFFF	IPv4 アドレス

ローカル利用IPv6ユニキャストアドレス

□ リンクローカルユニキャストアドレス

- 特定のリンク内だけで利用するアドレス (FE80::/10)
- プラグアンドプレイ機能を実現するために必要な初期の通信などに使用される

10bit	54bit	64bit
1111111010	0	Interface ID

□ サイトローカルユニキャストアドレス

- 特定のサイト内で利用するアドレス (FEC0::/10)
- IPv4で利用されているプライベートアドレスをより明確に定義したもの

10bit	54bit	64bit
1111111011	Subnet ID	Interface ID

- 2004年9月 RFC3879にて廃止 でも継続使用は許可
- 2008年4月 RFC5156 代替としてユニークローカルユニキャストアドレス (FC00::/7)

特別なユニキャストアドレス

- 未定義名アドレス
 - いかなるノード、インタフェースにも割り当ててはならないアドレスとして0:0:0:0:0:0:0:0がある
- ループバックアドレス
 - ループバックアドレスとしては0:0:0:0:0:0:0:1 (::1)が用意されている

```
[t-matsu@mail]/home/t-matsu >ifconfig
eth0      Link encap:Ethernet  HWaddr 00:11:11:7A:CF:FD
          inet addr:192.168.0.10  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::211:11ff:fe7a:cffd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:29631236 errors:0 dropped:0 overruns:0 frame:0
          TX packets:38505309 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:904050245 (862.1 MiB)  TX bytes:2207240920 (2.0 GiB)
          Interrupt:169

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:19509 errors:0 dropped:0 overruns:0 frame:0
          TX packets:19509 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:20987013 (20.0 MiB)  TX bytes:20987013 (20.0 MiB)

[t-matsu@mail]/home/t-matsu >
```

エニーキャストアドレス

- 複数のインタフェースに割り当てられる
- エニーキャストアドレス宛に送出されたパケットは、ネットワーク上最も近い1つのインタフェースに届けられる
- エニーキャスト用のアドレスブロックは用意されていない
(通常のグローバルユニキャストアドレスを用いる)
- 始点アドレスとして用いることができない
- 一種の機能アドレスとして用いる(GW, FW, ディレクトリサーバ)

マルチキャストアドレス

- マルチキャストアドレス宛に送出されたパケットは、そのグループに属するすべてのインタフェースに届けられる

8bit	4bit	4bit	112bit
11111111	Flag	Scope	Group ID

□ Flag

4bit用意されているが現在使われてるのは
最下位bitのみ
0は恒久割り当て、1は一時的割り当て

□ Scope

到達範囲を示す 右表参照

Ex FF02::101

あるリンク内のNTPサーバ

FF0E::101

インターネット上のNTPサーバ

値	定義	値	定義
0	Reserve	8	Organization
1	IF Local	9	未定義
2	Link Local	A	未定義
3	未定義	B	未定義
4	未定義	C	未定義
5	Site Local	D	未定義
6	未定義	E	Global Scope
7	未定義	F	Reserve

DNSの対応

- AAAAレコード

- 名前からIPv4アドレスへのマッピングにAレコードを使うように、名前からIPv6アドレスへのマッピングのための資源レコードにAAAAが追加された

- IP6.INT

- IPv4アドレスから名前へマッピングするための特別なドメインin-addr.arpa.と同等にIPv6アドレスからのマッピング用にIP6.INT.が追加された

```
[t-matsu@mail]/home/t-matsu >dig www.kame.net

<<>> DiG 9.3.1 <<>> www.kame.net
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30540
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; QUESTION SECTION:
;www.kame.net.                IN      A

;; ANSWER SECTION:
www.kame.net.                21319   IN      A      203.178.141.194

;; AUTHORITY SECTION:
kame.net.                    18930   IN      NS      mango.itojun.org.
kame.net.                    18930   IN      NS      orange.kame.net.

;; ADDITIONAL SECTION:
orange.kame.net.            18930   IN      A      203.178.141.194
orange.kame.net.            18930   IN      AAAA    2001:200:0:8000::42
orange.kame.net.            18930   IN      AAAA    2001:200:0:8002:203:47ff:fea5:3085

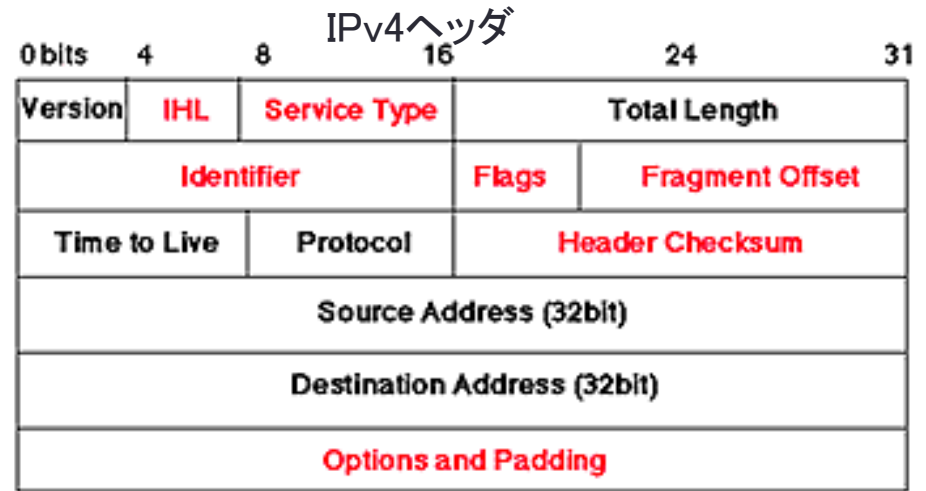
;; Query time: 0 msec
;; SERVER: 192.168.0.7#53(192.168.0.7)
;; WHEN: Sun Mar 28 10:29:06 2010
;; MSG SIZE  rcvd: 169

[t-matsu@mail]/home/t-matsu >
```



IPv6技術仕様

IPv6基本ヘッダ



□ Class

IPv6パケットのクラスや優先度

□ Flow Label

IPv6ルータに特別扱いさせるためにつけるラベル

□ Payload Length

IPv6基本ヘッダの後に続く部分の長さ (単位: オクテット)

□ Next Header

IPv6基本ヘッダに続くヘッダのヘッダタイプまたはプロトコル番号

□ Hop Limit

パケットがフォワードされるたびに1つ減る IPv4のTTL

IPv6拡張ヘッダ

- ホップバイホップオプションヘッダ
配送経路上の各ノードで調べられるオプションを付与
- 経路制御ヘッダ
配送経路上の任意のノードを指定
- 断片ヘッダ
終点までのパスMTUより大きなパケット送信時に使用
- 終点オプションヘッダ
終点ノードのみに運ぶオプションを付与
- 認証・暗号ペイロードヘッダ
通信相手の認証・偽造改竄検出等

主なヘッダタイプとプロトコル番号

番号	ヘッダタイプ・プロトコル番号
0	ホップバイホップオプション
4	IPv4 (カプセル化)
6	TCP
17	UDP
41	IPv6 (カプセル化)
43	経路制御
44	断片
50	暗号ペイロード
51	認証
58	ICMPv6
59	次ヘッダなし
60	終点オプション

IPv6基本ヘッダ Next=TCP	TCPヘッダ	データ
-----------------------	--------	-----

IPv6基本ヘッダ Next=経路制御	経路制御ヘッダ Next=TCP	TCPヘッダ	データ
------------------------	---------------------	--------	-----

拡張ヘッダを含んだIPv6パケットの例

File Edit View Go Capture Analyze Statistics Telephony Tools Help



Filter: Expression... Clear Apply

No. .	Time	Source	Destination	Protocol	Info
7	4.874490	203.178.8.1	192.168.0.3	UDP	Source port: 58584 Destination port: 58584
8	5.295823	fe80::25b1:c494:5c6f:5825	ff02::c	SSDP	M-SEARCH * HTTP/1.1
9	5.862636	192.168.0.3	203.178.8.1	UDP	Source port: 63277 Destination port: 63277
10	5.876326	203.178.8.1	192.168.0.3	UDP	Source port: 58584 Destination port: 58584
11	6.864819	192.168.0.3	203.178.8.1	UDP	Source port: 63277 Destination port: 63277
12	6.882470	203.178.8.1	192.168.0.3	UDP	Source port: 58584 Destination port: 58584
13	8.295694	fe80::25b1:c494:5c6f:5825	ff02::c	SSDP	M-SEARCH * HTTP/1.1
14	8.750800	2001:0:cf2e:3096:3038:8d2:2cfd:c8d1	2001:200:0:8002:203:47ff:fea5:3085	ICMPv6	Echo request

Frame 14 (94 bytes on wire, 94 bytes captured)

Ethernet II, Src: HonHaiPr_47:f6:6c (c4:17:fe:47:f6:6c), Dst: I-0DataD_69:0e:ac (00:a0:b0:69:0e:ac)

Internet Protocol, Src: 192.168.0.3 (192.168.0.3), Dst: 207.46.48.150 (207.46.48.150)

User Datagram Protocol, Src Port: 63277 (63277), Dst Port: teredo (3544)

Teredo IPv6 over UDP tunneling

Internet Protocol Version 6

0110 = Version: 6

[0110 = This field makes the filter "ip.version == 6" possible: 6]

.... 0000 0000 = Traffic class: 0x00000000

.... 0000 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000

Payload length: 12

Next header: ICMPv6 (0x3a)

Hop limit: 21

Source: 2001:0:cf2e:3096:3038:8d2:2cfd:c8d1 (2001:0:cf2e:3096:3038:8d2:2cfd:c8d1)

Destination: 2001:200:0:8002:203:47ff:fea5:3085 (2001:200:0:8002:203:47ff:fea5:3085)

Internet Control Message Protocol v6

```

0000  00 a0 b0 69 0e ac c4 17 fe 47 f6 6c 08 00 45 00  ...1.... .G.I..E.
0010  00 50 37 21 00 00 80 11 43 0c c0 a8 00 03 cf 2e  .P7!.... C.....
0020  30 96 f7 2d 0d d8 00 3c a0 24 60 00 00 00 00 0c  0..-...< .$. ....
0030  3a 15 20 01 00 00 cf 2e 30 96 30 38 08 d2 2c fd  :. .... 0.08...
0040  c8 d1 20 01 02 00 00 00 80 02 02 03 47 ff fe a5  .. .... .G...
0050  30 85 80 00 57 ad b9 e0 30 a7 cb b2 08 01  0...W... 0.....

```

プラグアンドプレイ機能

- IPv4では
 - 基本的に手動設定で行う
 - 自動で行うにはDHCPサーバを設置してDHCPを利用する
- IPv6では
 - アドレス設定・次ホップルータの情報取得などの機能を標準で備えている
 - ARP等のリンク層解決プロトコルはICMPv6で定義され、汎用的になった
- アドレス自動設定
 - ステートレス
 - ホスト自身が持つ情報と同一リンクのルータから得られる情報(ICMPv6で得る)を使用
 - 次スライド以降のアドレス生成の説明は基本的にステートレス設定の話
 - ステートフル
 - DHCPv6を使用



プラグアンドプレイ機能

- リンクローカルアドレスの生成
 - Fe80::/64にインターフェース識別子を付加して生成する
 - インタフェース識別子はリンクの種類によって異なる
 - Ethernetの場合, MACアドレスをEUI-64フォーマットに変換したものが使われる
- 重複アドレス検出
 - ICMPv6のネイバー要請メッセージ, ネイバー広告メッセージで検出する
- グローバルアドレス, サイトローカルアドレスの生成
 - ICMPv6のルータ広告メッセージによってプレフィックスを得る
 - その後インタフェース識別子を付加して生成する
- アドレス有効期間切れ
 - ルータ広告メッセージには有効期間(推奨有効期間, 最終有効期間)が設定されている
- 次ホップの決定
 - ICMPv6のルータ広告メッセージによって得たプレフィックスを使用する
 - デフォルトルータは広告メッセージを送信したルータになる

プラグアンドプレイ機能

- リンク層アドレス解決
 - 次ホップIPアドレスに対するネイバーキャッシュが存在すればそれを使用する
 - ない場合は, 次ホップIPアドレスをターゲットとしたネイバー要請メッセージ(ICMPv6)をマルチキャストする
 - ネイバー要請メッセージを受信したノードは, ターゲットが自分であればネイバー広告メッセージ(ICMPv6)を返す
- リダイレクト
 - ルータはより良い次ホップノードの情報をホストに通達する
 - ICMPv6のリダイレクトメッセージで実現する
- 到達不能の検出
 - ネイバー要請メッセージとネイバー広告メッセージで検出できる

セキュリティ機能(IPSec)

- IPv6ではセキュリティ機能(IPSec)が必須となっている
- AHとESPと呼ばれる2つのプロトコルで構成されている
- 機能
 1. 通信内容の秘匿
 2. 通信相手の認証
 3. 通信内容の偽造検出
 4. 再生攻撃の検出
- AH(Authentication Header)
 - 2.3.4の機能を提供
 - MD5 SHA-1 といったハッシュアルゴリズム使用
- ESP(Encapsulating Security Payload)
 - 1.3の機能を提供
 - DES のような共通鍵暗号アルゴリズムを使用
- AHとESPは組み合わせて使用することができる



セキュリティ機能(IPSec)

- モード

- トランスポートモード

- IP層より上位のプロトコルを保護する際に用いる
 - TCPやUDP ICMPなどを保護



- トンネルモード

- IPパケット全体を保護する際に用いる
 - VPNなどに使用



セキュリティ機能(IPSec)

- SA(Security Association)

IPSecを利用する2つのノード間におけるセキュリティパラメータ
パラメータは主に,

- 利用する機能(AH / ESP)
- 利用するアルゴリズム (DES, 3DES, MD5, SHA-1,...)
- 利用する鍵
- 利用するモード(トランスポート/トンネル)

がある

IPSecでは SPI(Security Parameter Index)フィールドの32bitで
表記される

- IKE(The Internet Key Exchange)

- 秘密鍵情報の交換を安全に行う
- IPSecに必要な機能だが, 定義上はIPSecに含まれる場合や, 別の独立プロトコルとして扱われる場合がある

セキュリティ機能(IPSec)

- AH(Authentication Header)

AH Format

Next Header	Payload Length	Reserved
Security Parameters Index (SPI)		
Sequence Number		
Authentication Data (variable)		

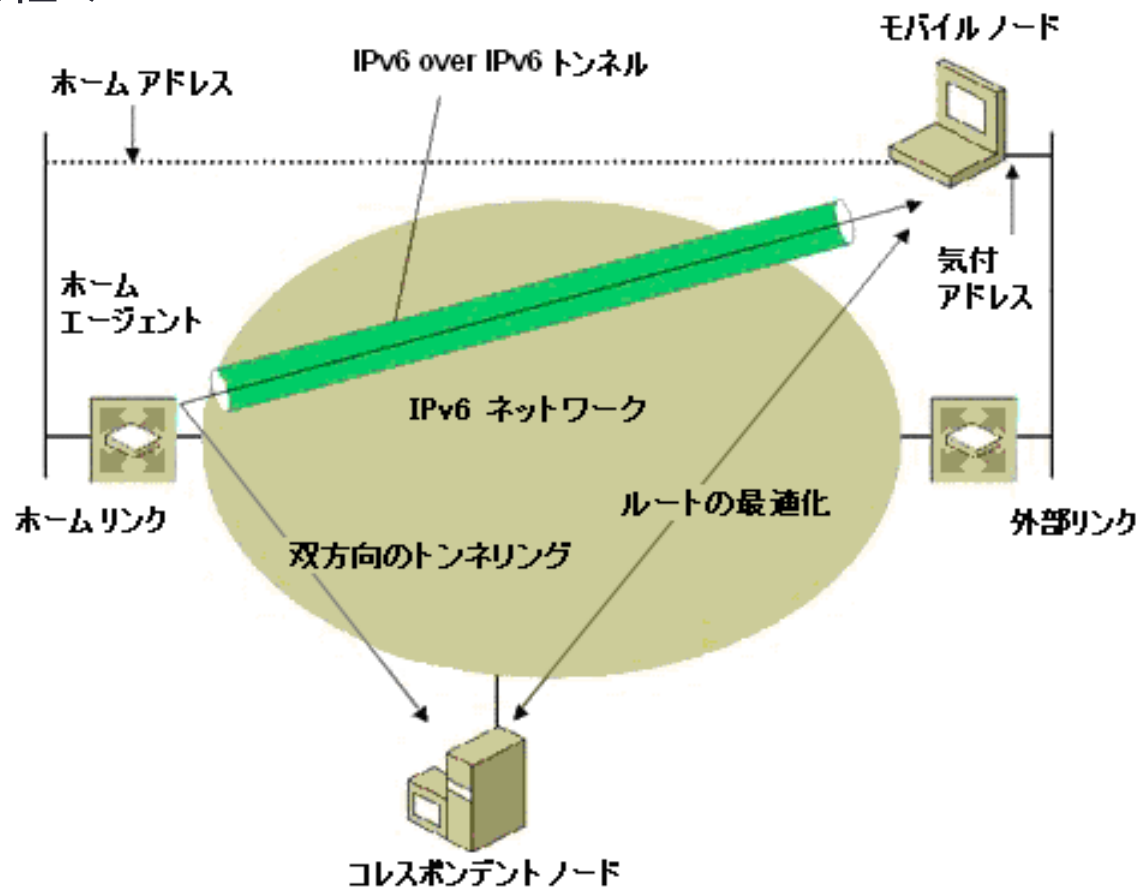
- ESP(Encapsulating Security Payload)

ESP Format

Security Parameters Index (SPI)		
Sequence Number		
Payload Data (variable)		
Padding (0 ~ 255 byte)		
	Pad Length	Next Header
Authentication Data (variable)		

モビリティ機能(Mobile IPv6)

移動通信中でも同じIPアドレスを使って途切れることなく通信を継続するための仕組み



IPv6への移行に関する技術

- デュアルスタック
 - 1つの通信装置にIPv4とIPv6両方の通信機能を実装する
- トンネリング
 - IPv6パケットをIPv4パケットでカプセル化し, IPv6ネットワークの島同士を繋ぐ
- トランスレータ
 - パケットおよびプロトコルを通信途上で動的に変換しIPv4ノードとIPv6ノードの異種プロトコル間の相互接続通信を実現する

今回のまとめ

- ICMP

- 到達不能を検知したり、ホストの生存確認を行うことができる
ネットワーク層のプロトコル
- 実装ではIPの上位層に位置する

- IPv6

- 次世代のIP
- 128ビットの広大なアドレス空間を持つ
- プラグアンドプレイ機能, セキュリティ機能, エニーキャストなどが追加
- 拡張性にすぐれる
- IPv4と互換性がない

質問あればどうぞ

次回はトランスポート層！