

IPv6技術

概要

- IPv6 の概要
- アドレスアーキテクチャ
- パケットフォーマット
- ICMPv6
- NDP
- 自動設定
- セキュリティ
- モビリティ
- API
- IPv6 への移行

IPv6の概要

IPv6とIPv4の違い

- アドレス空間の拡大
 - 32bitから128bitへ
 - 32bit 4,294,967,296 (40億)
 - 128bit 340,282,366,920,938,463,463,374,607,431,768,211,456
- アドレスアーキテクチャ
 - 階層的構造
 - スコープの導入
 - アドレス種別の明確な定義
- マルチキャストの標準化
 - ブロードキャストの廃止

IPv6とIPv4の違い (cont.)

- 高速化への対応
 - ヘッダフォーマットの簡易化
 - 利用されていないフィールドを削除
 - 固定長
 - チェックサムの廃止
 - IP ヘッダオプションの廃止
 - 経路上におけるパケット分割の廃止



情報ネットワーク論1 / 第4回, 第10回資料

5

IPv6とIPv4の違い (cont.)

- リンク層とネットワーク層のアドレス解決
 - ARP → NDP
 - 不到達性の検知
- セキュリティ
 - IPsecを標準とする
- 柔軟性
 - IP 拡張ヘッダ
 - MobileIPv6
 - IPsec
 - Explicit Multicast

情報ネットワーク論1 / 第4回, 第10回資料

6

IPv6 - インターネット本来の姿

- アドレス空間の拡大
 - End-to-End モデルの復活
- 集約可能なアドレス体系
- 新たな要求に対応する機能
 - マルチキャスト
 - MobileIP
 - IPsec
- 自動設定
 - アドレス自動設定機構の標準化
 - ネットワークのリナバリング

情報ネットワーク論1 / 第4回, 第10回資料

7

用語の定義

情報ネットワーク論1 / 第4回, 第10回資料

8

用語の定義

- IPv6 ノード
 - IPv6 を実装したデバイス
- IPv6 ルータ
 - 自分宛以外のパケットを転送する IPv6 ノード
- IPv6 ホスト
 - IPv6 ルータ以外の IPv6 ノード
- リンク
 - ノード間を結ぶメディア

用語の定義 (cont.)

- ネイバ (Neighbor)
 - 同一リンクに接続されているノード
- IPv6 パケット
 - IPv6 ヘッダ + ペイロード
- MTU
 - 最大転送単位
- パス MTU
 - 送信元から送信先までの MTU

用語の定義 (cont.)

- インタフェース
 - ノードからリンクへの接続点
- IPv6 アドレス
 - インタフェースを識別する識別子
- デュアルスタック
 - IPv4 と IPv6 の両方を実装したノード

アドレスアーキテクチャ

IPv6 アドレス表記

- 128bit を 16進数で表す
- 4桁ごとに「:」で区切る
 - 3ffe:501:100c:e320:2e0:18ff:fe98:936d
- 連続する「0」は省略可能
 - 3ffe:0501:100c:e320:0000:0000:0000:0001 → 3ffe:501:100c:e320::0001

IPv6 アドレス構造

- ネットワークプレフィクス とインタフェースID に分かれる
 - ネットワークプレフィクス (上位64bit)
 - ・ 現行では集約可能型アドレス体系に基づいて割り当てられる
 - ホストID (下位64bit)
 - ・ EUI-64
 - ・ Ethernet の場合、MAC アドレスを元に決定

IPv6 アドレス構造 (cont.)

Network Prefix	Interface ID
64bit	64bit

例えば、あるネットワークではこのような割り当てが行われる

IPv6 : 2001:218:1800::/48

IPv4 : 45.0.0.0/8

(subnetでは...)

2001:218:1800:e100::/64

2001:218:1800:e200::/64

45.0.1.0/24

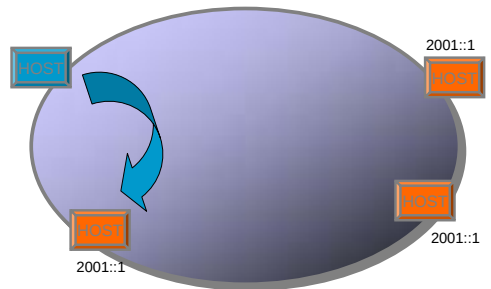
アドレス種別

- Unicast Address
 - 単一のインタフェースに対して割り当てられる
- Anycast Address
 - 複数のインタフェースに対して割り当てられ、そのうちのどれか1つに対して配送される
- Multicast Address
 - 複数のインタフェースに対して割り当てられ、それらすべてに配送される

アドレス種別 (cont.)

- Loopback Address
 - 自分自身を差すアドレス `::1`
- IPv4 互換アドレス
 - `::IPv4 address`
 - `::203.178.142.1`
 - 自動トンネリングのために使われるアドレス
- IPv4 射影アドレス
 - `::ffff:IPv4 address`
 - `::ffff:203.178.142.1`
 - IPv4 しか実装していないノードであることを表すアドレス表記

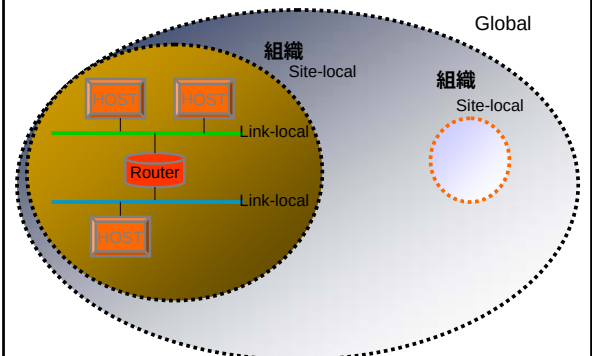
Anycast とは



スコープの概念

- Global address
 - インターネット全体において有効な, 単一なアドレス
- Link-Local address
 - 同一リンク上のみ有効なアドレス
 - `fe80::1`
- Site-Local address
 - サイト内でのみ有効なアドレス
 - `fc00::1000:0:0:0:1`

スコープの概念 (cont.)



集約可能アドレス体系

- 集約可能なアドレス体系(RFC2374)
- ネットワークポロジに沿ったアドレス割り当て

FP	TLA ID	RE	NLA ID	SLA ID	Interface ID
3	13	8	24	16	64

FP Format Prefix
 RE Reserved
 TLA ID Top-Level Aggregation Identifier
 NLA ID Next-Level Aggregation Identifier
 SLA ID Site-Level Aggregation Identifier

Format Prefix

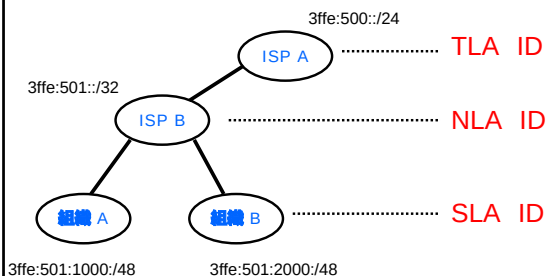
用途	Prefix	占有空間
Reserved	0000 0000	1/256
Unassigned	0000 0001	1/256
Reserved for NSAP Allocation	0000 001	1/128
Reserved for IPX Allocation	0000 010	1/128
Unassigned	0000 011	1/128
Unassigned	0000 1	1/32
Unassigned	0001	1/16
Aggregatable Global Unicast Address	001	1/8
Unassigned	010	1/8
Unassigned	011	1/8
Unassigned	100	1/8
Unassigned	101	1/8

Format Prefix (cont.)

用途	Prefix	占有空間
Unassigned	110	1/8
Unassigned	1110	1/16
Unassigned	1111 0	1/32
Unassigned	1111 10	1/64
Unassigned	1111 110	1/128
Unassigned	1111 1110 0	1/512
Link-Local Unicast Address	1111 1110 10	1/1024
Site-Local Unicast Address	1111 1110 11	1/1024
Multicast Address	1111 1111	1/256

Unassigned は 今後 Unicast として扱う

アドレス割り当て



TLA (Top Level Aggregator)

- RIRs (ARIN, RIPE, APNIC) から割り当てられる
- /29 のアドレス空間を持つ
- Default-free の経路交換を行う

FP	TLA ID	RE	NLA ID
3	13	8	24

本来の割り当て

FP	TLA ID	SubTLA ID	NLA ID
3	13	13	19

現状の割り当て

NLA (Next Level Aggregator)

- TLA からアドレスを取得する ISPや組織
- サブネットを設定することが可能
- /30~/48 のアドレス空間を保有

FP	TLA ID	RE	NLA ID
3	13	8	24

本来の割り当て

FP	TLA ID	SubTLA ID	NLA ID
3	13	13	19

現状の割り当て

SLA (Site Level Aggregator)

- NLA からアドレスを取得する組織
- /49~/64 のアドレス空間を保有

FP	TLA ID	SubTLA ID	NLA ID	SLA ID
3	13	13	19	16

TLA 取得の条件

- 3ヶ月以内に native IPv6 サービスを開始する
- Transit サービスを行う (leaf サイトとなてはいけない)
- Registry サービスを行う
- Registry データを定期的に RIR に報告する
- IANA にアドレス登録料を払う

SLA has been gone!

- SLAはもはや概念的に消失
 - NLAがあれば十分だね
 - RFC3513
 - 割り当て方針の変更
 - Global routing prefix + Subnet ID
 - Interface ID (64bit)
 - APNIC assignment
 - Global routing prefix: /32 (= TLA)
 - 32bit assignment for networks (= Subnet ID)

Ethernet と IPv6 アドレス

- インタフェース部はMAC アドレスを利用して自動生成される
- EUI-64
 - 00:e0:18:98:93:6d (MAC address) →
3ffe:501:100c:e320:2e0:18ff:fe98:936d

その他の Unicast Address

- Link Local Address
 - 同一リンク上にて有効なアドレス
fe80::2e0:18ff:fe98:936d

10 bits	56 bits	64 bits
1111111010	00000.....0000	interface Id

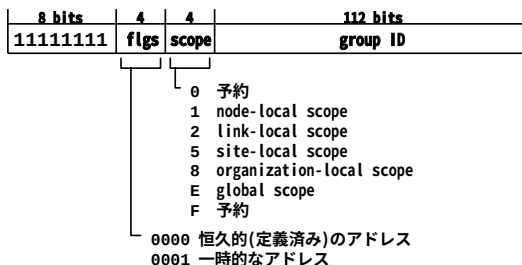
- Site Local Address
 - 同一サイト内にて有効なアドレス
fec0::2e0:18ff:fe98:936d

10 bits	38 bits	16 bits	64 bits
1111111011	00000..0	Subnet ID	interface Id

Anycast Address

- Unicast Address の一部
- 複数のインタフェースが同一アドレスを所有
- パケットはどれか1つのインタフェースに到達

マルチキャストアドレス



定義済みマルチキャストアドレス

FF00:0:0:0:0:0:0:0 予約
 FF01:0:0:0:0:0:0:0 予約
 :
 FF0F:0:0:0:0:0:0:0 予約
 FF01:0:0:0:0:0:0:1 ノード内の全 IPv6 ノード
 FF02:0:0:0:0:0:0:1 リンク内の全 IPv6 ノード
 FF01:0:0:0:0:0:0:2 ノード内の全 IPv6 ルータ
 FF02:0:0:0:0:0:0:2 リンク内の全 IPv6 ルータ
 FF02:0:0:0:0:0:0:C DHCP サーバ/リレーエージェント
 FF02:0:0:0:0:1::x:x 要請ノード アドレス

全 IPv6 ノードに対する通信例

```
% ping6 ff02::1%eth0
PING ff02::1(ff02::1) from fe80::2e0:18ff:fe98:936d eth0: 56 data bytes
64 bytes from ::1: icmp_seq=0 hops=64 time=1.2 ms
64 bytes from fe80::2a0:b7ff:fe9a:6527: icmp_seq=0 hops=64 time=1.3 ms (DUPI)
64 bytes from fe80::2e0:18ff:fe01:81f7: icmp_seq=0 hops=64 time=1.4 ms (DUPI)
64 bytes from fe80::2d0:b7ff:fe9a:6b58: icmp_seq=0 hops=64 time=1.7 ms (DUPI)
64 bytes from fe80::2e0:18ff:feab:c706: icmp_seq=0 hops=64 time=1.8 ms (DUPI)
64 bytes from fe80::240:26ff:fe66:a4: icmp_seq=0 hops=64 time=1.8 ms (DUPI)
64 bytes from fe80::200:86ff:fe42:55ff: icmp_seq=0 hops=64 time=1.9 ms (DUPI)
64 bytes from fe80::2a0:18ff:feab:34c8: icmp_seq=0 hops=64 time=2.2 ms (DUPI)
64 bytes from fe80::210:4bff:fe92:cc93: icmp_seq=0 hops=64 time=2.2 ms (DUPI)
64 bytes from fe80::250:70ff:fe01:d2c8: icmp_seq=0 hops=64 time=2.3 ms (DUPI)
64 bytes from fe80::2a0:ccff:fe73:34f7: icmp_seq=0 hops=64 time=2.4 ms (DUPI)
64 bytes from fe80::2e0:18ff:feab:8460a: icmp_seq=0 hops=64 time=2.6 ms (DUPI)
```

ノードの持つアドレス

- 各インタフェースごとのリンクローカルアドレス
- Global Unicast アドレス
- ループバックアドレス
- 全ノードマルチキャストアドレス
- 要請ノードマルチキャストアドレス
- ノードの属するその他のマルチキャストアドレス

ノードの持つアドレス例 (NetBSD)

```
de0: flags=0863<UP,BROADCAST,NOTRAILERS,RUNNING,SIMPLEX,MULTICAST> mtu 1500
address: 00:00:f8:03:db:34
media: Ethernet autoselect
status: active
inet 203.178.138.146 netmask 0xfffffff8 broadcast 203.178.138.151
inet6 fe80::200:f8ff:fe03:db34de0 prefixlen 64 scopeid 0x2
inet6 2001:200:0:4400:200:f8ff:fe03:db34 prefixlen 64
inet6 2001:200:0:4400::1 prefixlen 64
inet6 fec0::4401:0:1:1 prefixlen 64
lo0: flags=0009<UP,LOOPBACK,MULTICAST> mtu 33228
inet 127.0.0.1 netmask 0xffff0000
inet6 ::1 prefixlen 128
inet6 fe80::1%lo0 prefixlen 64 scopeid 0x4
```

ノードが参加する マルチキャストアドレス例(Linux)

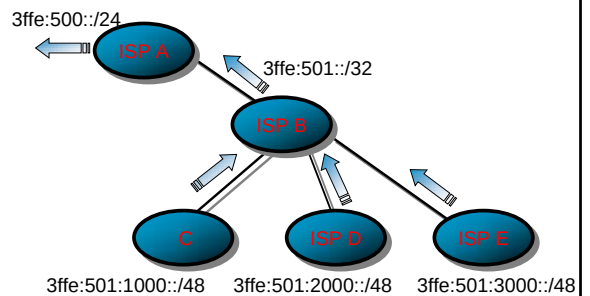
% netstat -g

Interface	RefCnt	Group	
lo	1	ff02::1	
eth0	1	ff02::9	<- RIPvng
eth0	3	ff02::1:ff98:936d	<- Solicited Multicast
eth0	1	ff02::1	<- All node Multicast
eth0	1	ff02::2	<- All router Multicast

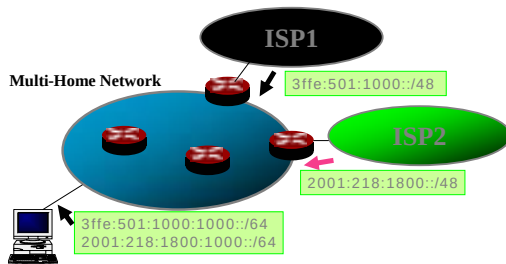
IPv6 の経路制御

2001:200:160::/48	fe80::2eb:18ff:fe98:a28dgvpc0 UG1	0	0	9180	pvc0
2001:200:161::/48	fe80::2eb:18ff:fe98:a28dgvpc0 UG1	0	0	9180	pvc0
2001:200:162::/48	fe80::2eb:18ff:fe98:a28dgvpc0 UG1	0	0	9180	pvc0
2001:200:180::/48	fe80::2eb:18ff:fe98:a28dgvpc0 UG1	0	0	9180	pvc0
2001:200:180:2::/64	fe80::2eb:18ff:fe98:a28dgvpc0 UG1	0	3	9180	pvc0
2001:200:180:3::/64	fe80::2eb:18ff:fe98:a28dgvpc0 UG1	0	0	9180	pvc0
2001:200:180:300::/64	fe80::2eb:18ff:fe98:a28dgvpc0 UG1	0	0	9180	pvc0
2001:200:180:a00::/64	fe80::2eb:18ff:fe98:a28dgvpc0 UG1	0	0	9180	pvc0
2001:200:180:800::/64	fe80::2eb:18ff:fe98:a28dgvpc0 UG1	0	0	9180	pvc0
2001:200:180:8940::/64	fe80::2eb:18ff:fe98:a28dgvpc0 UG1	0	0	9180	pvc0
2001:200:200::/48	fe80::2eb:18ff:fe98:a28dgvpc0 UG1	0	0	9180	pvc0
2001:200:300::/48	fe80::2eb:18ff:fe98:a28dgvpc0 UG1	0	0	9180	pvc0
2001:200:500::/48	fe80::2eb:18ff:fe98:a28dgvpc0 UG1	0	0	9180	pvc0
2001:200:600::/48	fe80::2eb:18ff:fe98:a28dgvpc0 UG1	0	0	9180	pvc0
2001:200:800::/48	fe80::2eb:18ff:fe98:a28dgvpc0 UG1	0	0	9180	pvc0
2001:200:900::/48	fe80::2eb:18ff:fe98:a28dgvpc0 UG1	0	0	9180	pvc0
2001:200::/35	fe80::2eb:18ff:fe98:a28dgvpc0 UG1	0	0	9180	pvc0
2001:228::/35	fe80::2eb:18ff:fe98:a28dgvpc0 UG1	0	10	9180	pvc0

経路の集約



マルチホームへの対応



マルチホームの課題

- NLA -> TLA への経路広告は Aggregation が必須
- 異なる TLA をまたいでマルチホームが困難
- draft-ietf-ipngwg-ipv6-2260-01
 - 組織の Edge router でトンネリング

パケットフォーマット

IPv4 ヘッダ

Ver	HL	TOS	Total Length	
Identification		Flag	Fragment Offset	
TTL	Protocol	Header Checksum		
Source Address				
Destination Address				
Options			Padding	

赤文字は IPv6 にて削除もしくは
名称変更されたフィールド

IPv4

IPv6 ヘッダ

Ver	Traffic Class	Flow Label
Payload Length	Next Header	Hop Limit
Source Address		
Destination Address		

IPv6

- 赤字は IPv4 から名称が変更されたフィールド
- 固定長となった

IPv6 ヘッダのフィールド

- | | |
|-----------------------|----------------------|
| ● Version | 番号6 |
| ● Traffic Class | トラフィッククラス (diffserv) |
| ● Flow Label | フローラベル (real-time) |
| ● Payload Length | ペイロード長 (オクテット単位) |
| ● Next Header | 続くヘッダのタイプ(RFC1700) |
| ● Hop Limit | ルータを通過することに減 |
| ● Source Address | 発信元アドレス |
| ● Destination Address | 宛先アドレス |

拡張ヘッダ

- ホップごとのオプションヘッダ
 - Hop-by-hop option
 - オプションは別定義
- 終点オプションヘッダ
 - オプションは別定義
- ルーティングヘッダ
- フラグメントヘッダ
- 認証ヘッダ
- 暗号化ヘッダ
- 終点オプションヘッダ(最終)
 - オプションは別定義

拡張ヘッダ (2)

IPv6 Header TCP Header

Next Header = TCP	
----------------------	--

IPv6 Header EXT Header TCP Header

Next Header = EXT	Next Header = TCP	
----------------------	-------------------	--

IPv6 Header EXT Header EXT Header TCP Header

Next Header = EXT	Next Header = EXT	Next Header = TCP	
----------------------	----------------------	----------------------	--

拡張ヘッダ (3)

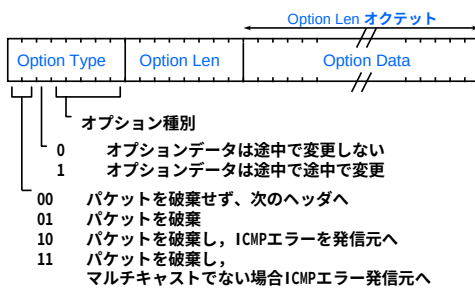
- 順序の推奨
 - 処理の効率化を期待
 - 違う順序でも処理できればいけない
- すべてのノードで処理すべきものと分離
 - ホップ・バイ・ホップ・オプション
 - 終点オプション
- 処理できないヘッダはICMPでエラー返送
もしくは無視
- 拡張ヘッダの長さは8オクテットの整数倍

ホップバイホップオプションヘッダ

- パス上のすべてのノードで処理する拡張ヘッダ
- 一つまたは複数のオプションを含む

8bit	8bit	
Next Header	Hdr Ext Len	Option
Option		Option

オプションの形式



ルーティング・ヘッダ

- 途中経路を発信元が指定
 - 現在 type 0 のみ規定

Next Header	Hdr Ext Len	Routing Type	Segment Left
Reserved			
Address[0]			
Address[1]			
...			
Address[n]			

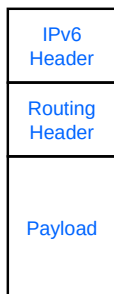
ルーティング・ヘッダ

- Hdr Ext Len
 - ルーティング・ヘッダの長さ
 - 8 オクテット単位で表現
- Routing Type
 - 現在 Type 0 のみ定義
- Segment Left
 - 残りの経路情報の数

ルーティングヘッダの処理手順

- IPv6ヘッダの送り先アドレスに到達したときに処理
 - Segment Left > Hdr Ext Len / 2
 - エラー送信
 - Segment Left = 0
 - 最終到着地
 - Segment Left < Hdr Ext Len / 2
 - IPv6 ヘッダのあて先アドレスを書き換えて転送
- マルチキャストアドレスに対しては適用せず

ルーティングヘッダ処理手順 (cont.)



Routing Header 中にある
宛先 IPv6 address を順に
IPv6 Header の中につめこむ

中継点パケット分割の廃止

- 中間のルータにおけるパケット分割を廃止
- 始点のみでパケット分割
- パケット転送の高速化
- 拡張ヘッダを利用してパケット分割
- Path MTU Discovery によるパケットサイズ調整

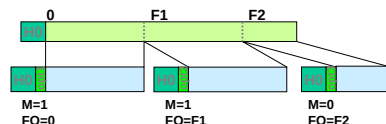
フラグメント・ヘッダ

- パスMTUを越えたとき発信元は細分化
- 8オクテットの倍数で (最後を除く)

Next Header	Reserved	Fragment Offset	Re M
Identification			

- Fragment Offset - 元データの始点からのオフセット(8オクテット単位)
- M - More bit
 - ・ 1:フラグメントが続く, 0:最後のフラグメント
- Identification - 発信元が生成する識別子

フラグメントの構成



Next Header	Reserved	Fragment Offset	Re M
Identification			

終点オプション・ヘッダ

- 終点に通知するオプション情報を指定

8bit	8bit	
Next Header	Hdr Ext Len	Option
Option		Option

No Next Header

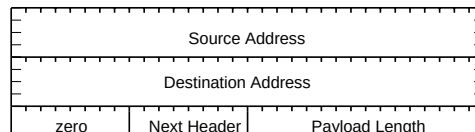
- つぎに拡張ヘッダが続かないときのヘッダタイプ
- ペイロードがないときのヘッダの終端

フローラベル

- 発信元が乱数を用いて設定
 - 20ビット
 - フローを識別
- 途中経路のルータが利用
 - フローごとの特別なQoS
 - 実時間通信
 - パケット処理の高速化

仮想ヘッダ

- TCP, UDPのIPv6上の仮想ヘッダ
- チェックサムの計算に用いる

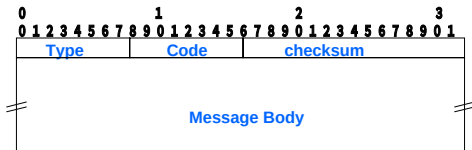


ICMPv6

ICMPv6

- Internet Control Message Protocol for IPv6
- IP における通信の制御
 - エラー通知
 - 通信状況の通知
- ICMP を使ったアプリケーション
 - ping, traceroute
- IPv4 ICMP の考え方を基本的に継承

ICMPv6 パケットフォーマット



Type Value

Type	Semantics
1	Destination unreachable
2	Packet is too big
3	Time exceeded
4	Parameter problem
128	Echo request
129	Echo reply

Path MTU発見プロトコル

- 動的にPath MTUを発見
 - 最初のリンクのMTUを初期値
 - ICMPの Too Big Message を受けると小さく
 - 適当な周期 (たとえば10分) で再調査



NDP (Neighbor Discovery Protocol)

NDP の機能

- ARP(Address Resolution Protocol) から NDP(Neighbor Discovery Protocol)へ
- ICMPとして実装
- IP 層とリンク層の対応付けを解決
 - 近隣ノードの発見
 - 近隣ノード到達性の検知
 - 重複アドレスの検知
 - Multicast を利用

NDP の機能 (cont.)

- 自動設定
 - ルータ発見
 - ルータ種別の検知
 - 自動アドレス設定
- 到達性
 - 到達性の検知
 - 不到達性の検知
- リダイレクト

NDP メッセージタイプ

- Router Solicitation
 - ノードがルータに問い合わせ
 - Solicited Address に対して行う
- Router Advertisement
 - プリフィックス, アドレス設定情報, ホップリミット推奨値
- Neighbor Solicitation
 - リンク層アドレス問い合わせ, 確認
- Neighbor Advertisement
 - 問い合わせへの応答
- Redirect
 - よりよい経路への変更指示

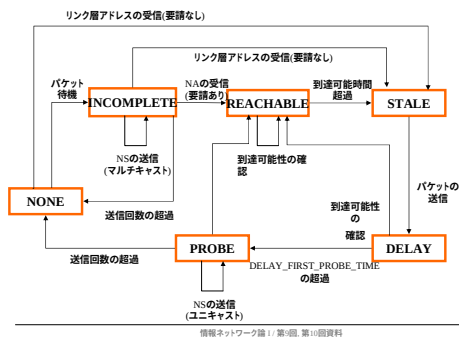
Solicited Multicast Address

```
eth0   リンク方法イーサネット ハードウェアアドレス 00:EO:18:98:93:6D
inetアドレス:203.178.143.49 ブロードキャスト203.178.143.255 マスク255.255.255.0
inet6アドレス: fe80::2e0:18ff:fe98:936d/10 範囲:リンク
inet6アドレス: 3ffe:505:d::1/64 範囲:グローバル
inet6アドレス: 3ffe:505:d:1000:2e0:18ff:fe98:936d/64 範囲:グローバル
inet6アドレス: 3ffe:501:100c:d210:2e0:18ff:fe98:936d/64 範囲:グローバル
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RXパケット:11876764 エラー:0 損失:0 オーバラン:4 フレーム:0
TXパケット:9069672 エラー:0 損失:0 オーバラン:0 キャリア:0
衝突(Collisions):0 TXキュー長:100
割り込み:11
```

NDP の動作例

```
tcpdump: listening on fxp0
09:52:22.010935 2001::218:1800:c050:210:f3ff:fe03:5445 >
ff02::1:ff00:567: icmp6: neighbor sol: who has
2001::218:1800:c050::567
09:52:23.010935 2001::218:1800:c050:210:f3ff:fe03:5445 >
ff02::1:ff00:567: icmp6: neighbor sol: who has
2001::218:1800:c050::567
09:52:24.010937 2001::218:1800:c050:210:f3ff:fe03:5445 >
ff02::1:ff00:567: icmp6: neighbor sol: who has
2001::218:1800:c050::567
09:52:24.010399 fe80::200:87ff:fe28:e090 >
2001::218:1800:c050:210:f3ff:fe03:5445 : icmp6: neighbor adv: tgt is
fe80::200:87ff:fe28:e090
```

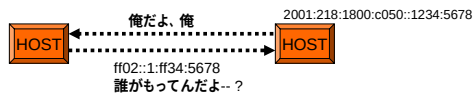
NDPの状態遷移



73

Solicited Address

- リンク層アドレス解決のための IP アドレス
- 2001:218:1800:c050::1234:5678
 - ff02::1:ff34:5678 に対してリンク層アドレスを問い合わせる
 - 2001:218:1800:c050::1234:5678 のアドレスを持つホストは、ff02::1:ff34:5678 への問い合わせに応える



情報ネットワーク論 I / 第4回 第10回資料

74

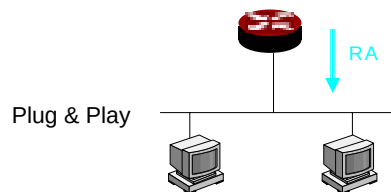
自動設定機能

情報ネットワーク論 I / 第4回 第10回資料

75

ホスト自動設定

- Stateless Address Auto Configuration
- アドレスと経路を自動設定
- NDP として実装
- EUI-64 を用いたアドレス



情報ネットワーク論 I / 第4回 第10回資料

76

ルータリナンバリング

- ネットワークのアドレスリナンバリング
- draft-ietf-ipngwg-router-renum-10 にて制定中
- 組織内のネットワークアドレスを自動で動的に変更可能

セキュリティ機能

IPsec の目標

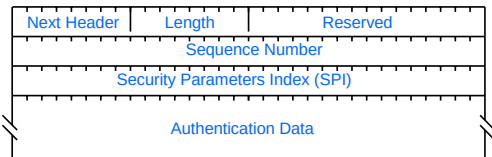
- 機構はアルゴリズムに独立であり, 取り替え可能であること
- デフォルトアルゴリズムを指定
 - keyed MD5, DES CBC, ...
- 3つの要求を充足
 - 認証
 - 改ざん防止
 - 機密保護

2つのセキュリティ メカニズム

- AH — Authentication Header
 - 認証と完全性を保証
- ESP — Encapsulating Security Payload
 - 機密性を保証

認証ヘッダ(AH)

- AH — Authentication Header
- IPv6パケットの認証と完全性を確保



認証ヘッダ (cont.)

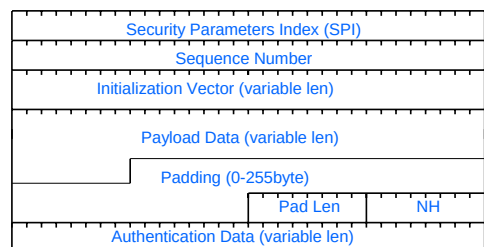
- Length: Payload長
- SPI: セキュリティアソシエーション識別子
- Sequence Number: 通し番号
- Authentication Data: 認証のためのデータ

Security Parameters Index

- 送信者と受信者の間で事前に合意のもと、セSecurity Association(SA)を確立し、受信者が乱数をもとに、SPIの値を割り当て
- SAとSPIから以下の情報が一意に決定
 - 暗号アルゴリズム
 - モード
 - 鍵
 - 鍵長

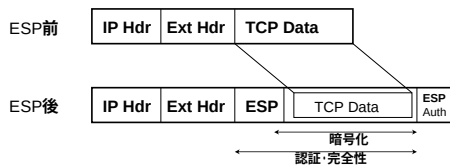
暗号化ヘッダ(ESP)

- ESP — Encapsulating Security Payload
- IPv6パケットの機密性を確保

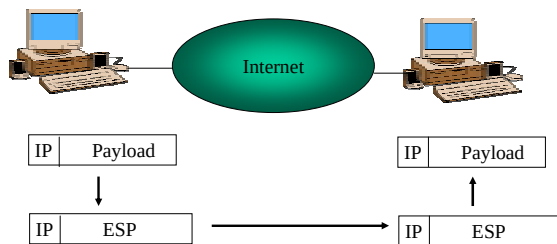


ESP - トランスポートモード

- ペイロードを暗号化して、ESPに入れる

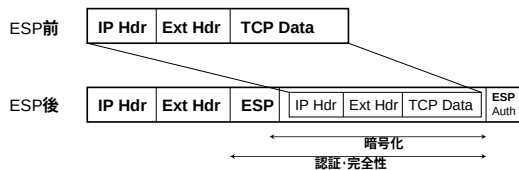


トランスポートモード

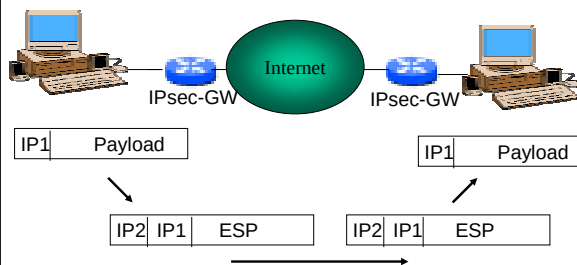


ESP - トンネルモード

- IPデータグラム全体を暗号化して



トンネルモード



鍵管理

- IPv6コアの範囲外
 - 上位プロトコルまたは人手で配布
 - 新しい方式の可能性
- 要求
 - 人手による設定
 - 同一ノード間で複数のアソシエーションの設定が可能
 - ユーザオリエンテッド, ホストオリエンテッドな設定が可能なこと

モビリティ機能

Mobile IPv6 の概要

- draft-ietf-mobileip-ipv6-13
- 移動しても IPv6 address が変わらず通信できる技術
 - 携帯電話
 - 移動中に通信が切断されない

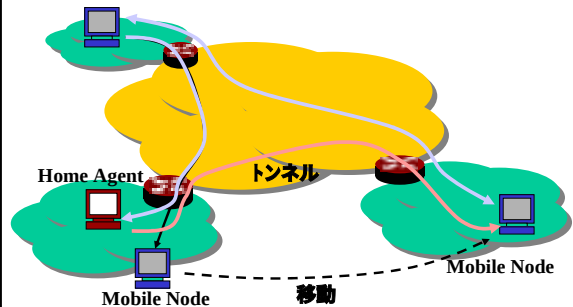
Mobile IPv6 用語

- Mobile Node (MN)
 - 移動するノード
- Home Link
 - Mobile Node の基本となる場所
- Home Address
 - Home Link でもらった IP address
- Care of Address
 - 移動先でもらったIP address

Mobile IPv6 用語 (cont.)

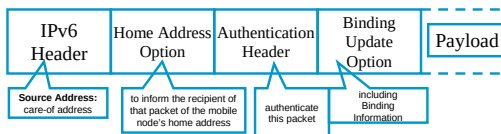
- Home Agent (HA)
 - Home Link にいるルータ
- Correspondent Node (CN)
 - Mobile Node の通信相手
- binding
 - Home Address と Care of Address を対応付ける動作

Mobile IP: 端末+サーバによるローミングサービス

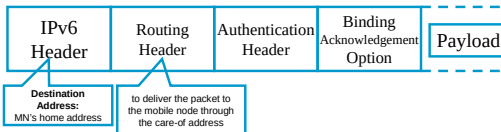


Binding の仕組み

Binding Update



Binding Acknowledgement

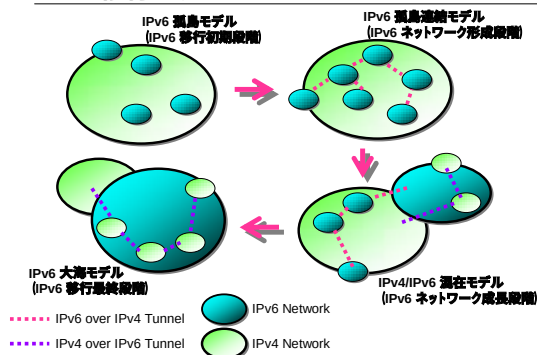


IPv6への移行

IPv4 から IPv6 へ

- IPv4 と IPv6 は直接通信不可能
- IPv6 ネットワークは IPv4 ネットワークと独立して存在
- 混在した環境
- 新たなネットワークに IPv6 が採用

IPv6移行モデル



移行のための技術

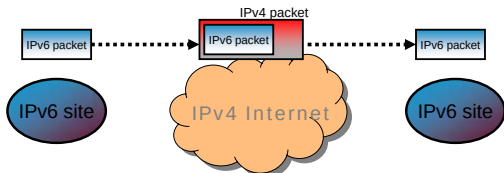
- 緩やかな移行
- デュアルスタック
 - IPv4/IPv6 プロトコルスタック両方を実装
- IPv6 in IPv4 トンネリング
 - 既存の IPv4 ネットワーク上に IPv6 ネットワークを構築する手法
 - カプセル化とも呼ばれる
- トランスレータ
 - IPv4 ホストと IPv6 ホストの相互通信を実現する技術
 - パケットの変換を行う

デュアルスタック

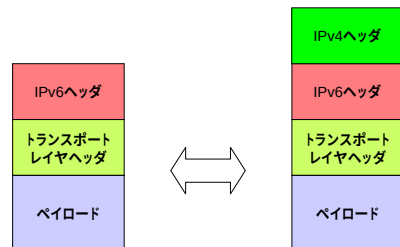
- IPv6/IPv4 両方のプロトコルスタックを実装
 - 現在の IPv6 対応プラットフォームでは全てデュアルスタックモデルを採用して接続性を確保
 - NetBSD/FreeBSD/BSD/Linux/Win2k/Macintosh
 - どちらのスタックを使って通信をするかを決める手順がポイント
- 通信相手に応じてプロトコルを切り替えて通信
 - 通信相手が IPv4 ホスト
 - IPv4 で通信
 - 通信相手が IPv6 もしくは IPv4/IPv6 ホスト
 - IPv6 で通信

IPv6 in IPv4 トンネリング

- IPv6 サイト同士を、仮想的なリンクによって接続
 - IP Tunneling (IP in IP) 技術を利用
 - Mbone でのIP multicast トンネリングと同じコンセプト
 - IP カプセル化によって、IPv6 パケットを IPv4 パケットとして配送



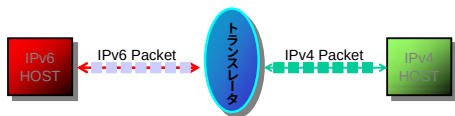
Packet Format



IPv6パケットのトンネリング(IPv6 in IPv4)

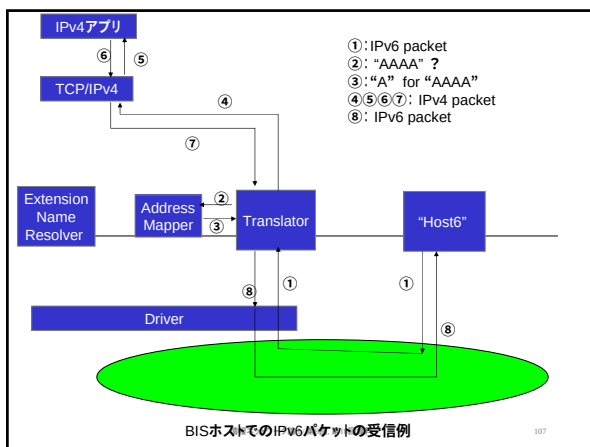
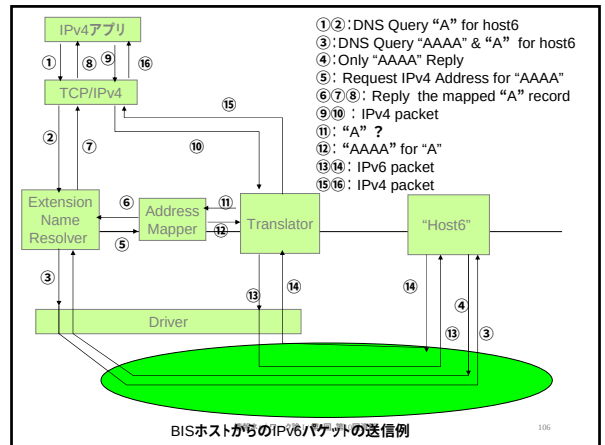
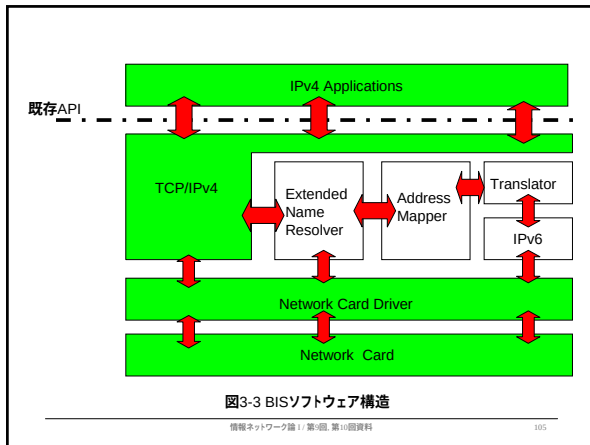
トランスレータ

- IPv4 パケットと IPv6 パケットを相互に変換する機構
 - IP 層で変換 (NAT-PT)
 - トランスポート層で変換 (FAITH)
 - アプリケーション層で変換 (SOCKS64)



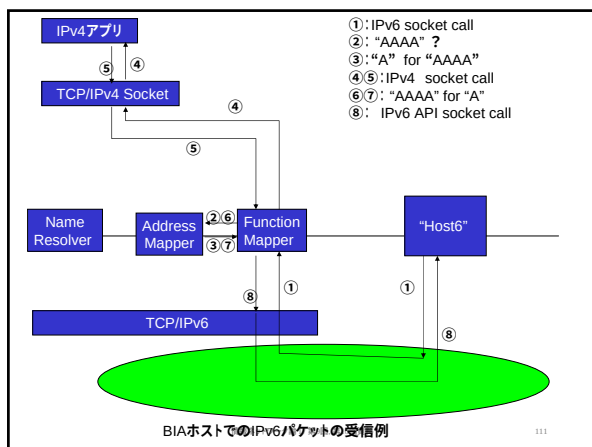
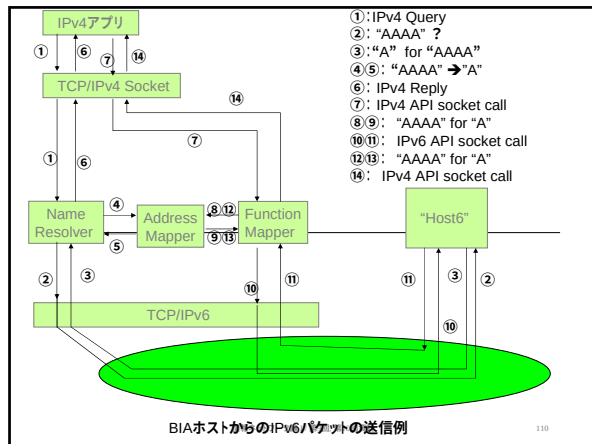
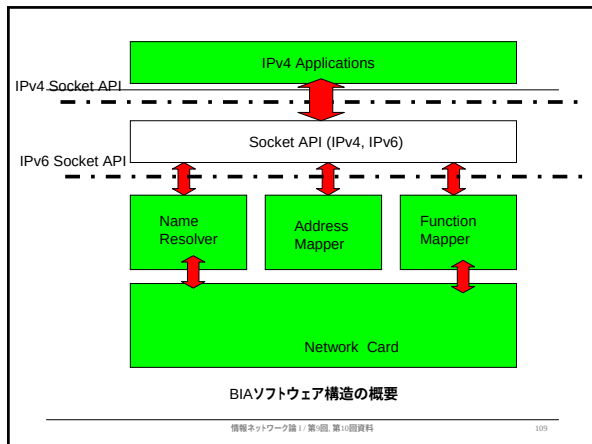
IPv4-IPv6 相互接続

- BIS (Bump-in-the-Stack)
- BIA (Bump-in-the-Application)
- 6-to-4
- SIIT
- NAT-PT/NAPT-PT
- SOCKS
- トンネル ブローカ
- ISATAP
- DSTM (Dual Stack Transition Mechanism)



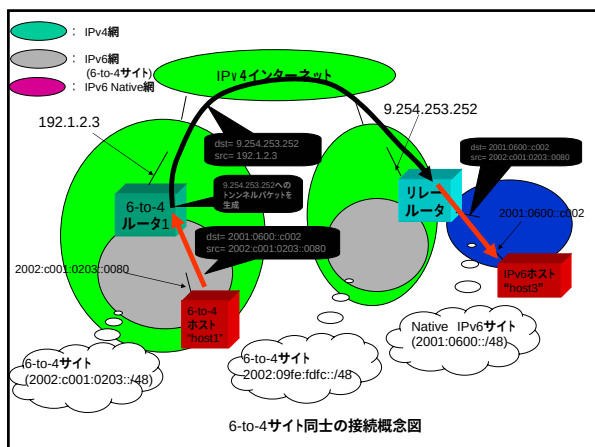
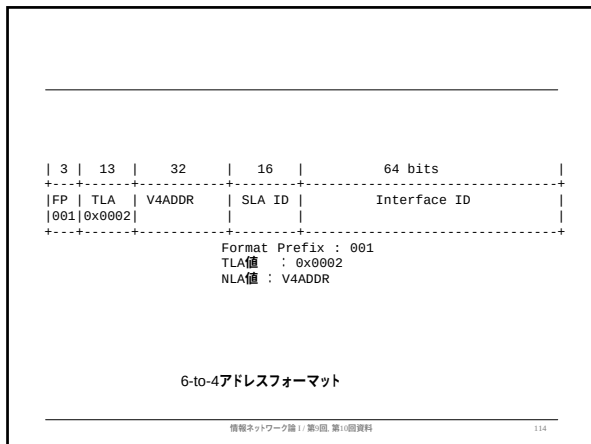
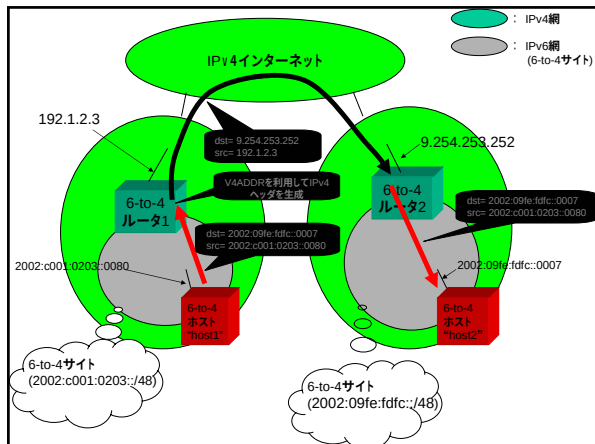
IPv4-IPv6 相互接続

- BIS (Bump-in-the-Stack)
- BIA (Bump-in-the-Application)
- 6-to-4
- SIIT
- NAT-PT/NAPT-PT
- SOCKS
- トンネル プロローカ
- ISATAP
- DSTM (Dual Stack Transition Mechanism)



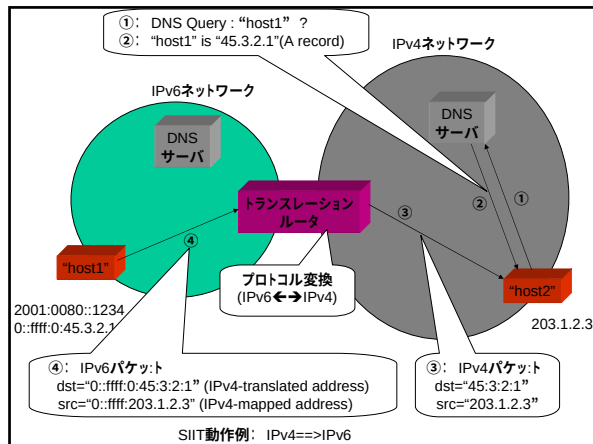
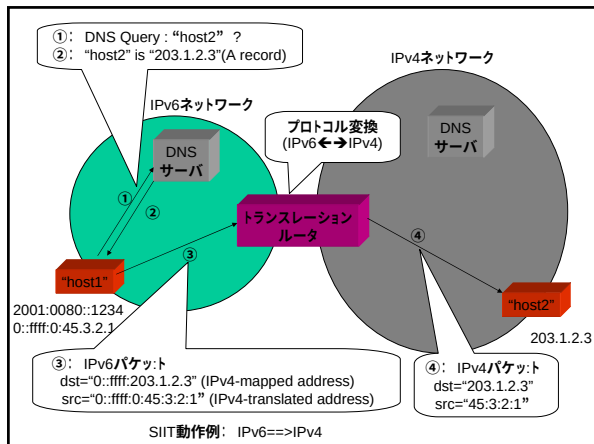
IPv4-IPv6 相互接続

- BIS (Bump-in-the-Stack)
- BIA (Bump-in-the-Application)
- 6-to-4
 - IPv4ネットワークの上にp2pのIPv6-in-IPv4トンネルを自動生成
 - IPv6サイトは、IPv4アドレス(V4ADDR)と、IPv6 Prefix(2002::/16)を持つ
 - ・ V4ADDRはIPv4ドメインでのルーティングに使用する。
 - IPv6ノードは 6-to-4仮想インターフェースを持つ
 - IPv6ノードは、2002::V4ADDR::/48 のIPv6アドレスを持つ
 - Protocol ID(IPv4のヘッダ部) は、"41"にセット
- SIIT
- NAT-PT/NAPT-PT
- SOCKS
- トンネル ブローカ
- ISATAP
- DSTM (Dual Stack Transition Mechanism)



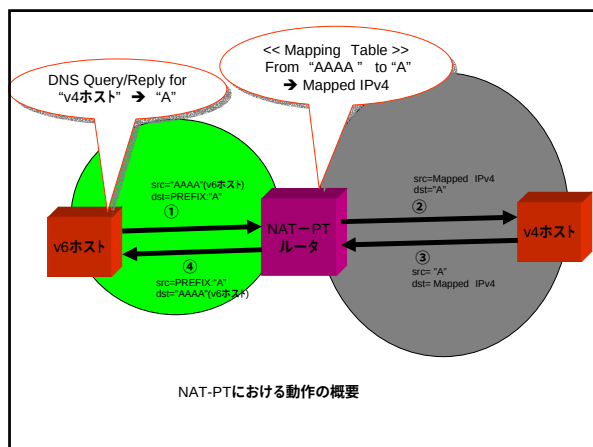
IPv4-IPv6 相互接続

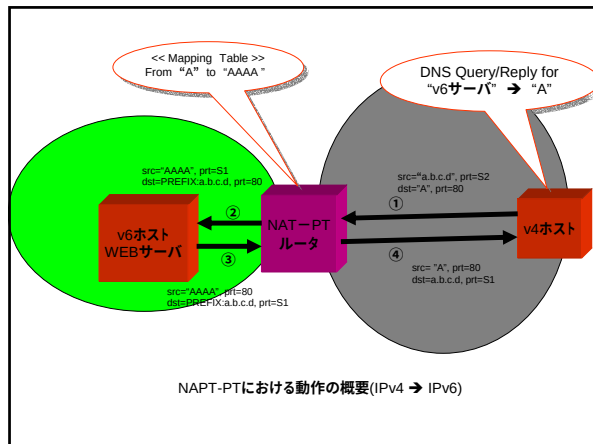
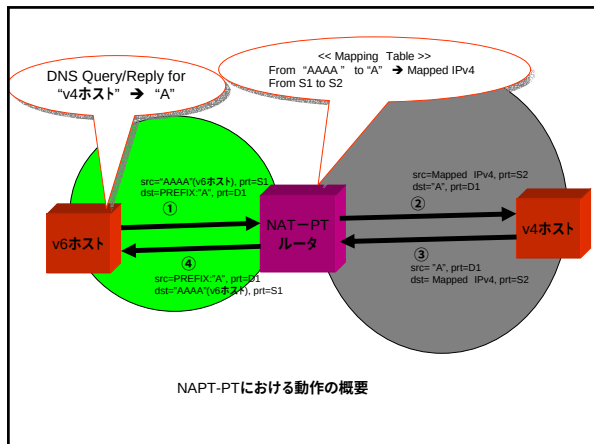
- BIS (Bump-in-the-Stack)
- BIA (Bump-in-the-Application)
- 6-to-4
- SIIT (Stateless IP/ICMP Translation)
- NAT-PT/NAPT-PT
- SOCKS
- トンネル ブローカ
- ISATAP
- DSTM (Dual Stack Transition Mechanism)



IPv4-IPv6 相互接続

- BIS (Bump-in-the-Stack)
- BIA (Bump-in-the-Application)
- 6-to-4
- SIIT
- **NAT-PT/NAPT-PT**
- SOCKS
- トンネル ブローカ
- ISATAP
- DSTM (Dual Stack Transition Mechanism)

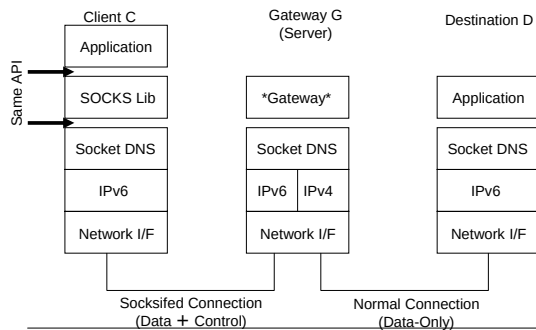




IPv4-IPv6 相互接続

- BIS (Bump-in-the-Stack)
- BIA (Bump-in-the-Application)
- 6-to-4
- SIIT
- NAT-PT/NAPT-PT
- **SOCKS**
- トンネル ブローカ
- ISATAP
- DSTM (Dual Stack Transition Mechanism)

SOCKSを用いたネットワークの相互接続



0	1	3	4	6
0	5	12	7	3

```

+-----+-----+-----+-----+
|ccccccugcccccccc|cccccccccccccccccccc|cccccccccccccccccccc|cccccccccccccccccccc|
+-----+-----+-----+-----+

```

c : company-id ビット (22ビット)
u : universal/local ビット (1ビット),
"u=1"はグローバルスコープ, "u=0"はローカスコープ
g : individual/group ビット(1ビット)
"u=1"はグループアドレス, "g=0"は個別(individual)アドレス
m: 拡張識別子ビット (40ビット)

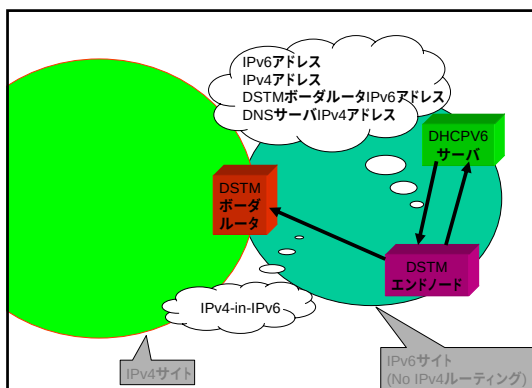
EUI-64フォーマット

3	13	8	24	16	8	8	8	8	32 bits
FP	TLA	RES	NLA	SLA	0x	0x	0x	0x	IPv4 Address
ID	ID	ID	ID	ID	00	00	5E	FE	of Endpoint

ISATAPアドレスフォーマット

IPv4-IPv6 相互接続

- BIS (Bump-in-the-Stack)
- BIA (Bump-in-the-Application)
- 6-to-4
- SIIT
- NAT-PT/NAPT-PT
- SOCKS
- トンネル プロローカ
- ISATAP
- **DSTM (Dual Stack Transition Mechanism)**



DSTMシステム

IPv6 経路制御

- RIP ⇒ RIPng
- BGP4 ⇒ BGP4+
- OSPFv2 ⇒ OSPFv3
- IS-IS ⇒ IS-IS for IPv6

DNS for IPv6

- RFC1886, RFC2874
- IPv6 アドレスのための新しい RR
 - AAAA
 - A6
 - DNAME
- Inverse zone
 - ip6.int. (nibble boundary)
 - ip6.arpa. (bitlabel boundary)

DNS zone file 例(1)

```
$ORIGIN .
$TTL 3600      ; 1 hour
linux-ip6.org  IN SOA  linux6.nezu.wide.ad.jp. sekiya.linux-ip6.org. (
    43          ; serial
    1800        ; refresh (30 minutes)
    900         ; retry (15 minutes)
    172800      ; expire (2 days)
    10800       ; minimum (3 hours)
)
NS      shaku.sfc.wide.ad.jp.
NS      linux6.nezu.wide.ad.jp.
A       203.178.142.218
MX      5 linux6.nezu.wide.ad.jp.
AAAA    2001:200:0:1c01:2b0:d0ff:fe23:d5e5
A6      0 2001:200:0:1c01:2b0:d0ff:fe23:d5e5
```

DNS zone file 例(2)

```
$TTL 3600      ; 1 hour
d.0.0.0.5.0.5.0.e.f.f.3.IP6.INT IN SOA  chiharu.netvillage.ne.jp. sekiya.v6.linux.or.jp. (
    100091601   ; serial
    3600        ; refresh (1 hour)
    900         ; retry (15 minutes)
    3600000     ; expire (5 weeks 6 days 16 hours)
    3600        ; minimum (1 hour)
)
NS      chiharu.netvillage.ne.jp.
NS      shaku.sfc.wide.ad.jp.
$ORIGIN d.0.0.0.5.0.5.0.e.f.f.3.IP6.INT.
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 PTR shaku.v6.linux.or.jp.
d.6.3.9.8.9.e.f.f.f.1.8.0.e.2.0.0.0.1 PTR shaku.v6.linux.or.jp.
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 PTR chiharu.v6.linux.or.jp.
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 PTR ipsmg.v6.linux.or.jp.
```