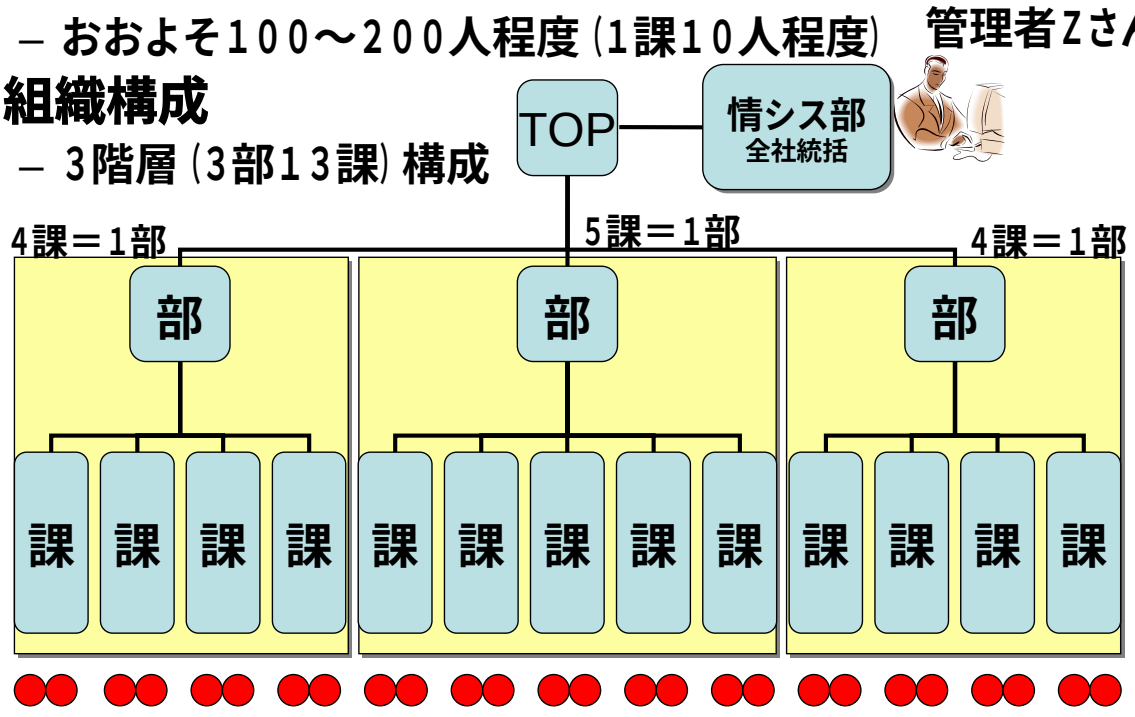
第1部　　ネットワーク構築

担当

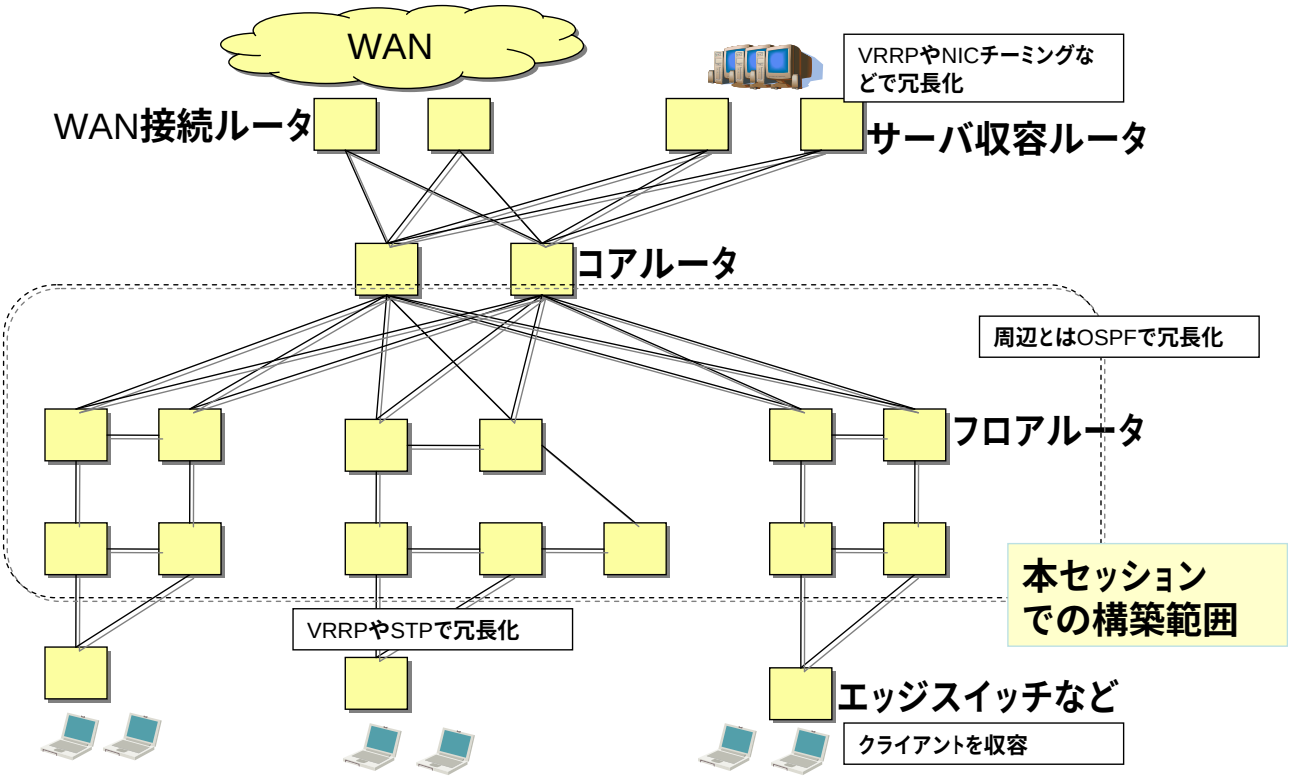
宍倉弘祐／NTTコミュニケーションズ株式会社

架空企業A社について

- **架空企業Aの規模**
  - おおよそ100～200人程度（1課10人程度）
- **組織構成**
  - 3階層（3部13課）構成

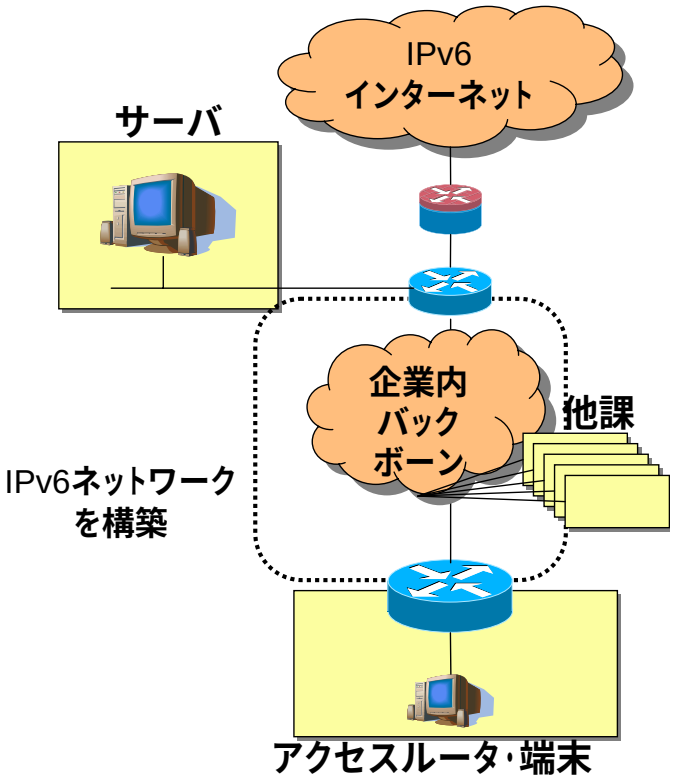


架空企業Aのネットワーク構成



第1部のアウトライン

1. アドレッシング
2. ルーティング
3. フィルタリング



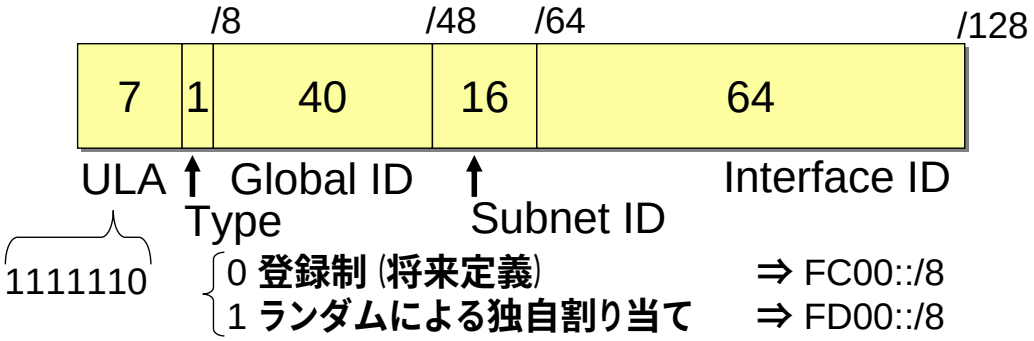
1. アドレッシング

アドレスの種類と選択

- IPv4では
  - インターネットとの接続点はグローバルアドレス
  - 内部はプライベートアドレス
    - 外部とはNAT経由で通信
- IPv6では
  - インターネットとの接続点はグローバルアドレス
  - 内部は
    1. グローバルアドレス
    2. ユニークローカルユニキャストアドレス
       (IPv4でのプライベートアドレス相当)
       - 外部とは NAT相当のもの経由で通信?

ユニークローカルユニキャストアドレス

- Unique Local IPv6 Unicast Address**の構造**



- FD00::/8 **をアドレス空間として使用**
- Global ID**を**ランダム**に生成する**
  - **独自に使用可能 (申請の必要はない)**
  - **サンプルとして時刻を種にする方法が示される。**
    trunc(SHA1(NTP current time + EUI-64), 40bit)

ユニークローカルユニキャストアドレス

- Global ID**の一意性の保証について**
  - RFC4193**では完全な一意性は保証していない**
  - **適切な乱数を使えば衝突の可能性は限りなく低い**
  - **ランダム割り当ての運用状況を見て、一意割り当て (**centrally assign**) の検討を行うという議論もあった**
    - **この場合、**FC00::/8 (type = 0) **空間を使用予定**

- ULA**の運用上の注意点**
  - **グローバル空間へのリーク**
    - **ルーティング**, DNS**クエリ**
  - **そもそも、**IPv6**でも**NAT**？**

(参考)文書作成用アドレス空間 (2001:db8::/32)

- APNICが文書作成用にアドレス空間を予約
- マニュアルや設定サンプルへの利用を想定
- ローカルアドレスではないので通信のために利用してはならない = ルーティングしない

- 参考ドキュメント
  - APINIC “IPv6 Documentation Prefix”
    http://www.apnic.net/info/faq/ipv6-documentation-prefix-faq.html
  - “IPv6 Address Prefix Reserved for Documentation”, RFC3849

グローバルアドレスの選択

1. 上位ISPから取得
   - ISPが顧客に/48～/64を割り当てるのが一般的
     - (例)NTT Comのスーパー OCNデュアルでは 2001:380:xxxx::/48を割り当て

2. JPNICから取得
   - トランジットISPを冗長化出来る
     1. プロバイダ非依存アドレス(PI)を取得する
     2. ISPとして、大きなブロック(/32)を取得する

3. 6to4等自動トンネル技術のアドレスを利用

JPNICから取得

- プロバイダ非依存アドレス(PI)を取得する
  - 今後3ヶ月以内にマルチホーム接続をする
  - エンドサイトである(割り当てられたアドレスは自組織のみで使用し、再割り当てを行わない)

JPNICから取得

- ISPとして、大きなブロック(/32)を取得する
  - IPアドレス管理指定事業者としてIPv4アドレスの割り振りを受けている場合
    - 他組織へIPv6アドレスを割り当てを行う
    - 2年以内に割り振りを受けたIPv6アドレスの経路をグローバルインターネットへ広告する
  - その他の場合
    - 200以上のネットワークに対して、2年以内にIPv6アドレスの割り当てを行う計画がある
    - IPv6アドレスを割り当てた組織に対し、IPv6の接続性を提供する計画がある

アドレス空間の大きさの検討

- アドレス空間は
  「セグメント数 × ネットワークの大きさ」

- IPv4ではセグメント毎にnetmask長を変更
  - ルータ間などP2Pリンクでは/30
  - 収容NWでは端末台数に応じて/26〜/28など

- IPv6ではセグメントは一般的に/64で統一
  - IPv6を有効にするセグメント数 × /64
  - 一般的な割り当ての/48は 約6万5千個×/64

アドレッシングポリシーの考慮ポイント

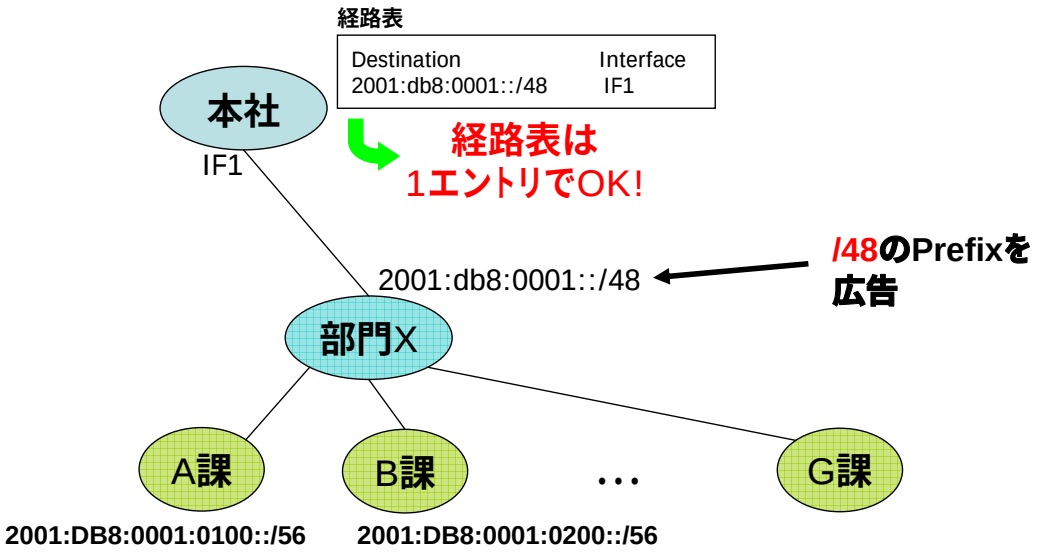
- 基本的にはIPv4と同様
  - 経路集約可能であること
    - HWリソース(ルーティングテーブルを保持するメモリ、検索にかかるCPU処理)を最小限に
  - 体系化されていること
    - 設備/端末用、ルータ間/拠点間用、組織毎等の種類により分別することで、アドレス表やACLコンフィグの管理負荷の軽減
  - 拡張性があること
    - スペースに余裕を持たせ、将来の拡張に備える

アドレッシングポリシーの考慮ポイント

- IPv6ではこんなことも
  - アプリやサービス毎に複数のアドレスを付与
    - IPv6では、端末に複数のアドレスが付与可能
    - アプリケーション単位でのアクセス制御、QoS制御も
      - IP電話はこのブロック、など
  - 視覚判別しやすく
    - 既存の情報(部署コードや、v4アドレス等)と視覚的に近づける方法も

アドレッシングによる経路集約

- 階層的なアドレッシングと、経路集約

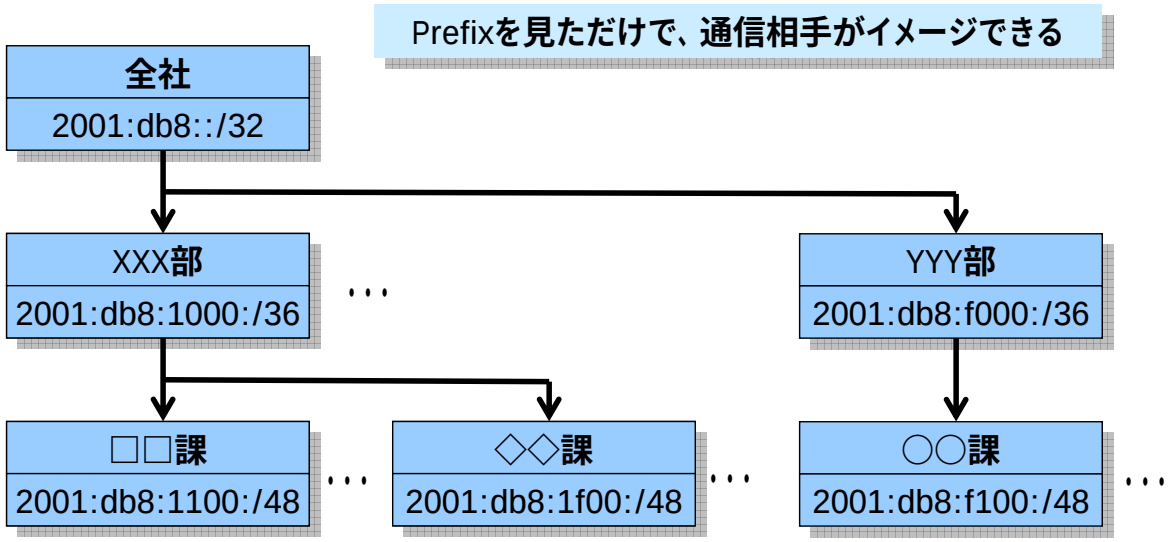


複数アドレスの付与

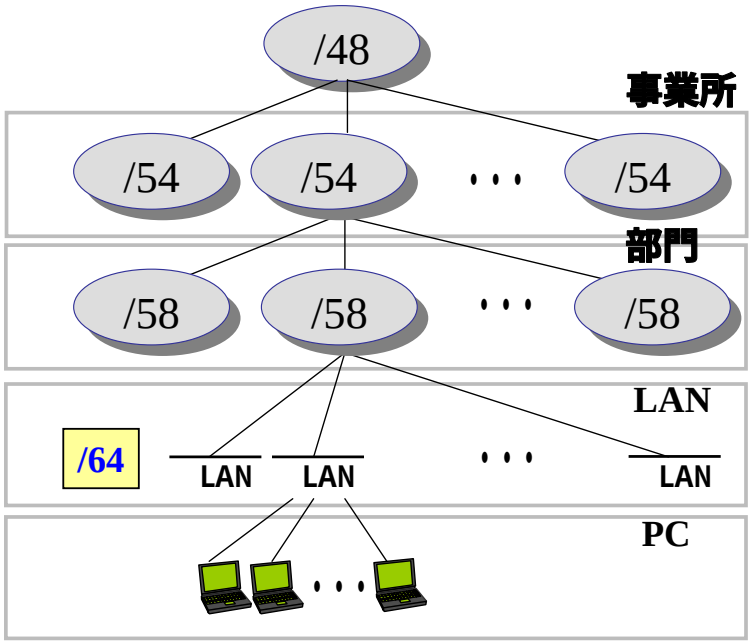
- IPv6では、端末のIFに複数のアドレスを付与できるため、複数のサービスを提供する機器には複数のアドレスをつけることも可能
  - 異なるFQDNで同じIPアドレスを参照したり、エイリアスを利用したりするのと結果は同等

```
% ifconfig -a
fxp0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1280
        inet6 fe80::206:5bff:fe3b:XXXX%fxp0 prefixlen 64 scopeid 0x1
        inet6 2001:db8:4fd::25 prefixlen 64
        inet6 2001:db8:4fd::110 prefixlen 64
        ether 00:06:5b:3b:XX:XX
        media: Ethernet autoselect (100baseTX <full-duplex>)
        status: active
```

アドレスの視覚判別



/48の割り当て例その1



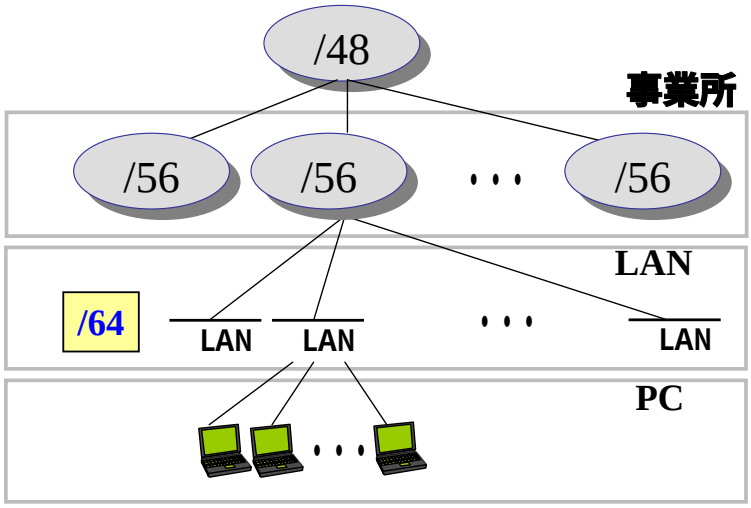
各事業所に/54（最大64事業所）

各部門に/58（最大16部門）

各LANには/64（最大64個）

各LANに64bit分のPCが接続可能

/48の割り当て例その2



各事業所に/56（最大256事業所）

各LANには/64（最大256個）

各LANに64bit分のPCが接続可能

各リンクへのアドレス割り当て

- /64　(RFC3177で推奨)
  - RA(後述)による自動設定のためには/64必須
  - 通常、配下のNWに64bit分以上の端末は接続しないと想定
- /65〜/127など
  - アドレス節約のために使うこともできる
    - P2Pリンクに/126など
  - 特別なアドレスと衝突しないように注意が必要
    - Router Anycast (RFC3513)
    - ルータ間リンクに/127は避けるべき(RFC3627)

各機器へのアドレス付与

- クライアント端末
  - RA(Router Advertisement)で動的設定が可能
  - 企業NWではDHCPv6も(詳細は端末編にて)
- ルータ機器やサーバ機器
  - RAから自動生成してしまうと管理しづらい
    - 長く複雑
    - NICや装置を交換するとアドレスが変わる
  - わかりやすいアドレスを静的に設定

各機器へのアドレス付与

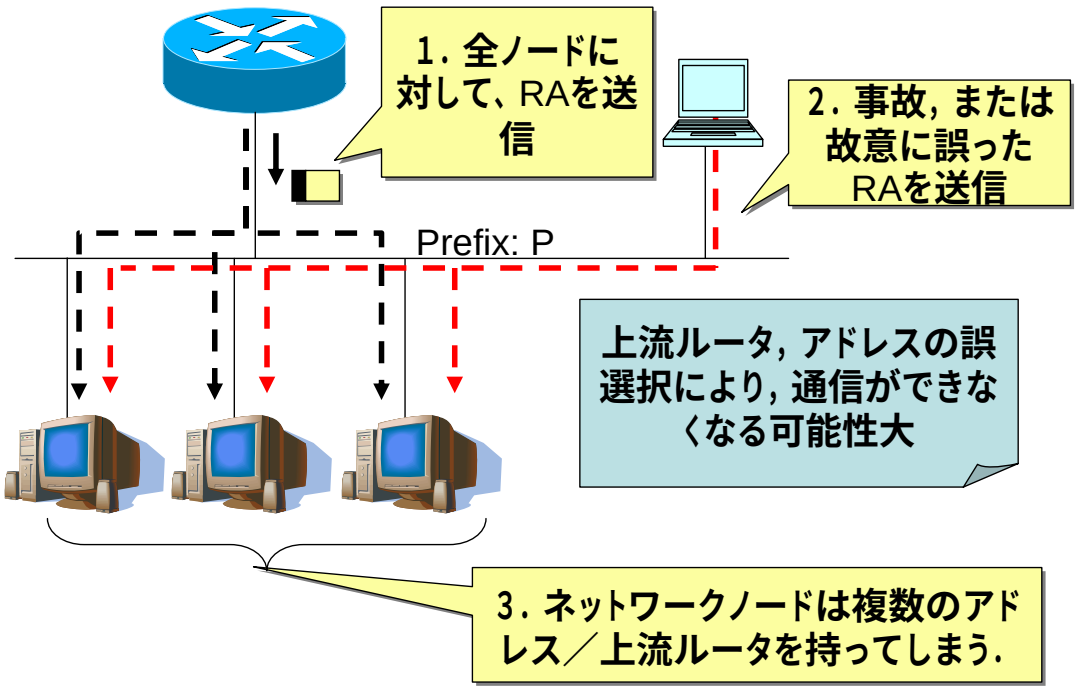
- ルータ機器やサーバ機器
  - わかりやすいアドレスを静的に設定
  - サーバのアドレス設定例
    - <prefix>::<サービスのポート番号>
    - 2001:db8::53　(DNSサーバ)
    - 2001:db8::25　(SMTPサーバ)
    - 2001:db8::80　(WWWサーバ)
  - ルータのアドレス設定例
    - <prefix>::<上流に近い順番>
    - 2001:db8::1　　(上位ルータのIF)
    - 2001:db8::5　　(そのセグメントの5番目のルータのIF)

RAに関する注意

- RA設定
  - /64のprefixが必須(RFC4861)
  - 必要箇所のみ有効化し、意図しない動作を予防
    - ルータ機器の実装によっては、IFのIPv6設定でRAが自動で有効になることがあるので、明示的に抑止設定
- 誤ったRAへの対応
  - 設定ミスなどにより、誤ったRAが広告されることがある

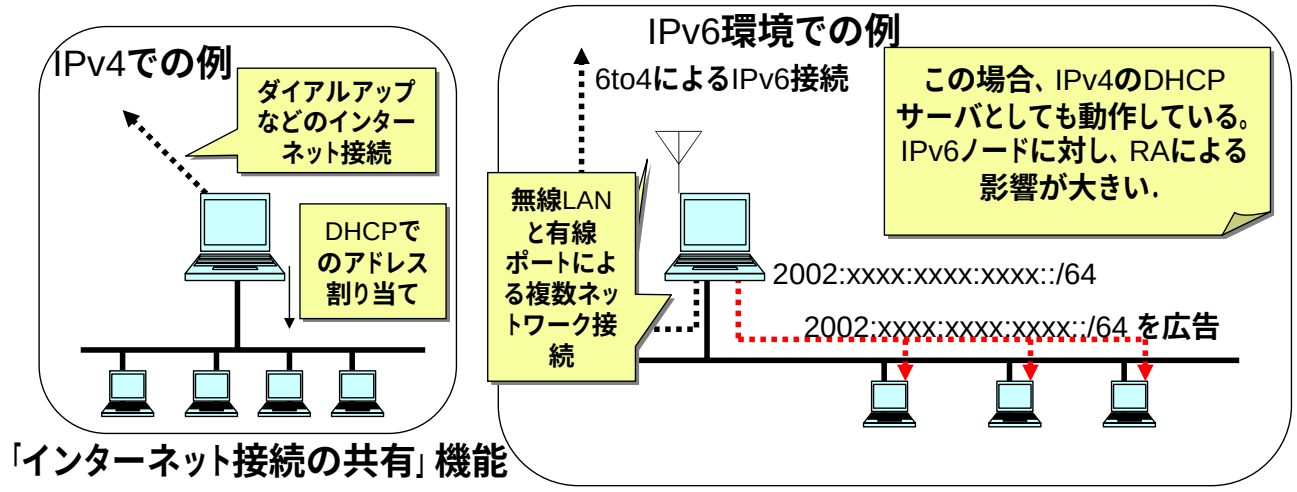
誤ったRA

- 誤ったRA



誤ったRA

- 誤ったRAの実例
  - Windows XP
    - 複数のネットワークインタフェースを持ち、「インターネット接続の共有」が on になっていると、RAを始めることがある。

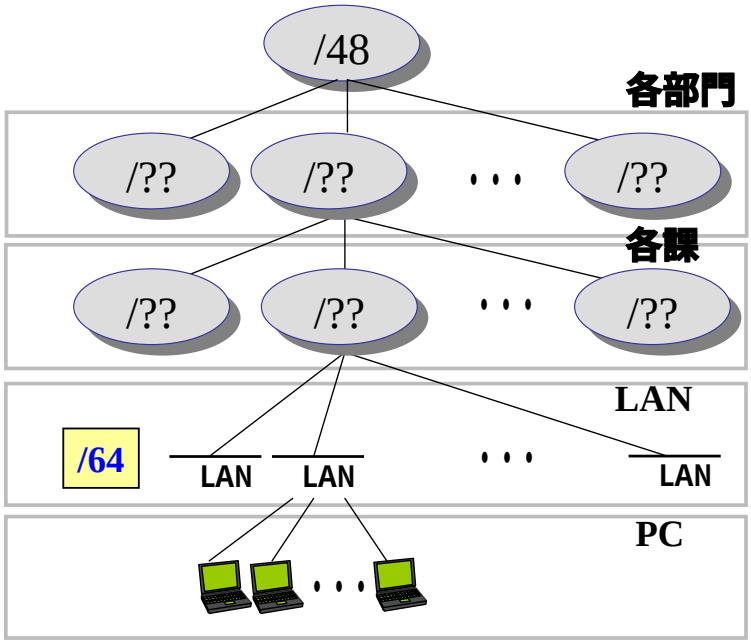


誤ったRA

- 誤ったRAが送信されてしまったら
  - RAの取り消し
    - RAパケットには、ルータの“ライフタイム”フィールドがある．これを‘0’にして，再度広告することにより、無効化できることがある
  - 端末のリセット
    - 該当する全端末をリセットして、回復を試みる

(実習) IPv6アドレス設計

- 下記の条件で、アドレス設計を考えます



・将来は、部が200ぐらい増えるとして

・将来は、各課にルータ間リンクや、端末収容セグメント(LAN)が最大10個程度として

・各LANには/64を割り当てる

・各LANに64bit分のPCが接続可能

(実習) IPv6アドレスの設定

- 図を元に、VLANインターフェースにアドレスを設定します
- 設定すべきVLANインターフェースが複数ありますので、うまく分担してください
- ルータ向けにはRAを抑制
  PC向けにはRAを送出してください

(実習) IPv6アドレスの設定

- すでにIPv4設定されているVLANインタフェースにIPv6アドレスを設定します
  - 全部で3個 or 4個

VLAN100インターフェースへ移行

```
(config)# interface vlan 100
```

IPv6を利用可能にする

```
(config-if)# ipv6 enable
```

IPv6アドレスの設定

```
(config-if)# ipv6 address 2001:db8:X:Y::Z/64
```

2. ルーティング

IPv6ルーティング

- IPv4と基本は同じ
- 経路情報は「宛先prefixとnext-hopアドレス」
  - next-hopアドレスはリンクローカルアドレス
- prefix長が長い方を優先で選択
  - /48より、/64経路を優先

ルーティングポリシーの考慮ポイント

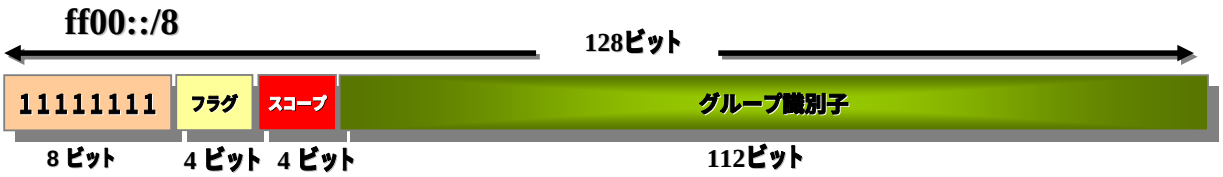
- IPv4とIPv6のルーティングは別で考える
  - IPv4, IPv6どちらか片方の障害に依存させない
  - ルーティングプロセスのCPU/Memory負荷は、IPv4, IPv6で別々に管理する
- ルーティングプロトコルの選択
  - v6化するNWの範囲・規模
  - 求められる信頼性
  - 管理の容易性

ルーティングプロトコル

- IPv6ルーティングプロトコルは、通信にリンクローカルマルチキャストを用いることが多い
  - 既存のL2機器でマルチキャストに対しておかしな動作をしないかどうか
- トラブル切り分け
  - 該当するリンクローカルマルチキャストパケットの疎通を確認(IPv6 ping)

リンクローカルマルチキャスト

- IPv6はマルチキャスト通信を多用



値	スコープ
0	予約
1	インタフェースローカルスコープ
2	リンクローカルスコープ
3	予約
4	管理ローカルスコープ
5	サイトローカルスコープ
6 - 7	未割り当て
8	組織ローカルスコープ
9 - D	未割り当て
E	グローバルスコープ
F	予約

すべてのノード
ff01::1
ff02::1
すべてのルータ
ff01::2
ff02::2
ff05::2

リンクローカルマルチキャスト

- “ff02::1” **への** ICMP echo
  - リンクローカルスコープの「すべてのノード」宛てアドレス
  - ルータも、ノードの一部
  - 自分からも返答があることに注意
- **ルーティングプロトコルのマルチキャストアドレス宛への**ICMP echo
  - ff02::9 (RIPngルータ)
  - ff02::5 (OSPFv3ルータ)
- リンクローカルアドレスは自動付与なので、対向機器のアドレスがわからなくても可能

ルーティングプロトコルの種類

- static routing
  - v4同様、これで十分なことも多い
- RIPng
  - ほとんどのIPv6対応ルータで実装されている
- OSPFv3
  - 対応ルータが多い
- BGP4+
  - ISP間の接続で使われている
- その他
  - マルチキャストが必要な場合はPIM-SM等

static routing

- IPv4 static routingとの主な違い
  - Next-hopアドレスをリンクローカルアドレス、グローバルアドレスのどちらでも記述できる場合がある
- 注意点
  - Next-hopアドレスをリンクローカルにする場合
    - IF指定が必要
    - “link-local”という別オプションが用意されている場合も

RIPng

- RIPv2 との主な違い
  - UDPポート521を使用
  - FF02::9宛てのリンクローカルマルチキャストを使用
  - Next-hopアドレスはリンクローカルアドレスを使用

OSPFv3

- OSPFv2との主な違い
  - LSA の追加･変更
  - LSA-IDの付与規則の変更
  - 認証機能の削除(代わりにIPv6のAH, ESP利用)
  - 使用アドレス (グローバルアドレスがなくても動く)
    - ユニキャスト fe80::/64
    - 全てのOSPFルータ宛 ff02::5
    - DR/BDR宛 ff02::6
- 注意点
  - Router-idは32bitのものが必要

BGP4+(MP-BGP)

- BGP4 **との主な違い**
  - **パス属性**
    - MP_REACH_NLRI**が追加** (IPv4**以外の経路に対して到達可能であることを示す**)
  - **ピアアドレス**
    - **グローバルアドレス、リンクローカルアドレスどちらも可**

- **注意点**
  - Router-id**は**32bit**のものが必要**
  - **自**AS**番号を、**v4/v6**で別に定義できる機器も**

(**実習**) OSPFv3**の設定**

- **各**VLAN**インタフェースに対して、**OSPFv3**の設定をします**

OSPFv3**の設定** (“10”**はドメイン番号**)

```
(config)# ipv6 router ospf 10
```

ルータID**の設定 (必須・**IPv4**で設定されていれば共通の**32bit**の数字**

```
(config-rtr)# router-id x.x.x.x
```

パッシブインターフェースの設定

```
(config-rtr)# passive-interface vlan 10
```

vlan 10**へ移行**

```
(config)# interface vlan 10
```

OSPFv3**を動作させる。ドメイン**”10”, area”0”**を設定**

```
(config-if)# ipv6 ospf 10 area 0
```

- **終わったら状態確認のコマンドを打ってみましょう**

(実習) OSPFv3の設定

迂回経路の確認

- ルーティングプロトコルが正常に動作しているか、トポロジ図を見て切れても問題ない(はずの)線を抜いてみましょう

3. フィルタリング

基本的な考え方

- フィルタリングの目的
  - ネットワークの外から、そのネットワークへ不正なパケットが流入するのを防ぐ
  - パケットを通すか廃棄するかを、何らかの基準で判断する
- 実装方法
  - FW装置
  - ルータ機器でのパケットフィルタリング
  - 端末機器でのパーソナルファイヤーウォール

IPv6と、NAT

- IPv6ネットワークにおいてNATは避ける
  - アドレスは足りているので、節約の必要はない
  - NAT利用により、NW構成、管理が複雑化
  - IPv6はEnd-to-End通信が前提のため、アプリに制限が出る可能性
  - NATによる安全性？はSPIで対応可能
  - Local Network Protection for IPv6 (RFC 4864)
    - NATと同等のセキュリティの確保方法

NATは安全？

IPv4はプライベートアドレスとNATで安全？
IPv6はグローバルアドレスだから危険？

- NAPTの動き
  - 通信開始時に動的にアドレスとポート変換規則が生成
  - 到着したパケットは、変換規則にマッチすれば内部に転送される
  - 通信終了時に動的に変換規則が消滅

- Stateful Packet Inspection (SPI) の動き
  - 通信開始時に動的に通過ルールが生成
  - 到着したパケットは、通過ルールにマッチすれば内部に転送される
  - 通信終了時に動的に通過ルールが消滅

- IPv6でもSPIで同等の安全性が担保可能

フィルタリングポリシーの考慮ポイント

- **内部→外部**
  - 端末から外部へ向けた通信は許可
- **外部→内部**
  - 確立済みTCPコネクションは通過
  - DNS, NTPは通過
  - ICMPv6 type 1,2,3を通過

    Type 1: Destination Unreachable
    Type 2: Packet Too Big
    Type 3: Time Exceeded
- **(参考)同一リンク**
  - すべての通信を許可(NDPや、ルータ間通信等)

匿名アドレス (RFC4941)

- インターフェイスIDをランダムに生成したIPv6アドレス
  - MACアドレスからEUI-64で生成したインターフェイス識別子では、ホストが容易に特定されてしまうことを回避
- 特徴
  - 現在のアドレスから次に生成されるアドレスの予想が難しい
  - 現在のアドレスから過去に使われたアドレスが推測が難しい
  - 単純なランダム生成ではない
- アクセス制御、アクセスログの管理をふまえて、禁止するというポリシーもありえる
- Windows等の端末で無効化設定可能

Windows XPでの匿名アドレスの無効化設定

- アドレスの表示

```
C:¥> netsh interface ipv6 show address interface="ローカル エリア接続" mode=normal
Interface 6: ローカル エリア接続

Addr Type  DAD State  Valid Life   Pref. Life   Address
---------  ---------- ------------ ------------ --------------------------
Temporary  Preferred   6d22h54m54s     22h52m7s 2001:db8:155b:3837:d902:a54
```

- 匿名アドレスの状態確認

```
C:¥> netsh interface ipv6 show privacy
一時アドレス パラメータ
----------------------------------------------
一時アドレスの使用                    : enabled
有効な生存期間の最大値                : 7d
優先する生存期間の最大値              : 1d
  …
```

- 匿名アドレスの無効化

```
C:¥> netsh interface ipv6 set privacy state=disable mode=persistent
```

ICMPv6

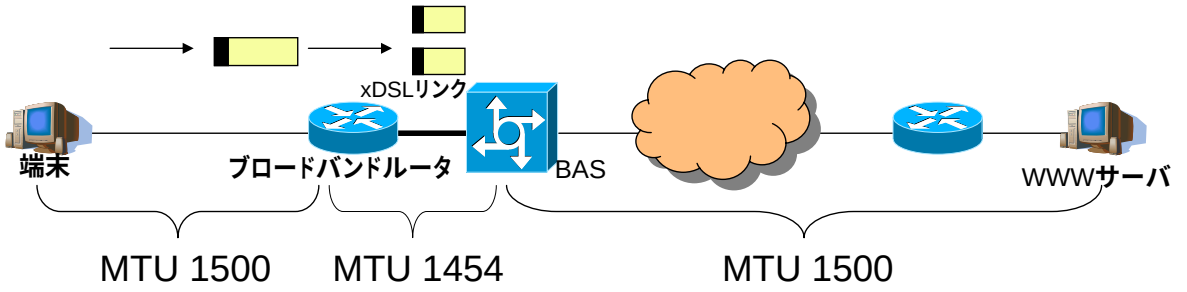
- IPv4では
  - セキュリティ上の理由からICMPを通らないようにしている場合もある
- IPv6では
  - ICMPv6が通信上、重要な役割を果たすため、特定のICMPv6パケットを通過させることが重要
    - 終点到達不能（Destination Unreachable）（Type = 1）
    - パケット過大（Packet Too Big）（Type = 2）
    - 有効期間超過（Time Exceeded）（Type = 3）
  - Recommendations for Filtering ICMPv6 Messages in Firewalls (RFC4890)

ICMPv6

- フィルタによる影響
  - 終点到達不能
    - TCP等がタイムアウトするまで通信できないことがわからなくなる
    - IPv4へのフォールバックが遅くなる
  - 有効期間超過
    - TCP等がタイムアウトするまで通信できないことがわからなくなる
    - Traceroute6の結果がわからなくなる
  - パケット過大
    - IPv6では経路途中でパケットの断片化（後述）を行なわないため、通信が不安定になる

ICMPv6

- ICMP **パケット過大メッセージ**
  - IPv4**では，経路途中でパケットが分割される**



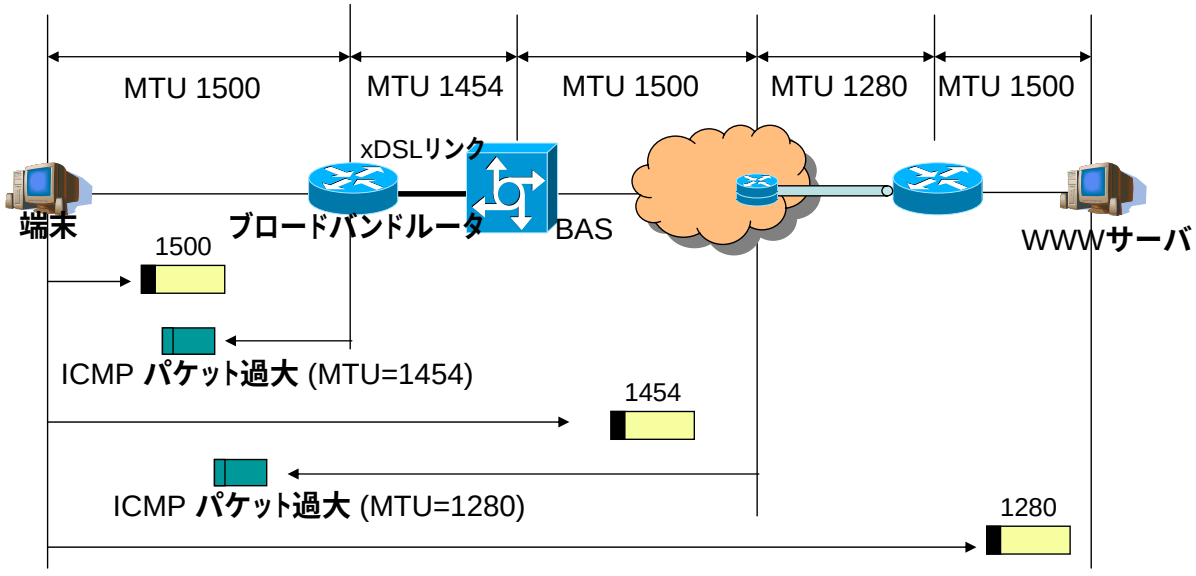
MTU（Maximum Transmission Unit）

  - IPv6**では，経路途中での分割をしない**
    - **途中経路の最大の**MTU**で転送する**

「パスMTU**探索」が重要！**

ICMPv6

- IPv6**でのパス**MTU**探索**（RFC1981）



IPv4 **の パス**MTU**探索**（RFC1191）**と基本的に同等**（**戻ってくる**ICMP**のタイプは違う**）

パケット過大メッセージのフィルタの問題

- IPv4では
  - パスMTUブラックホール問題として知られている
  - 'DF (断片化禁止) ビット'を使用した場合

- IPv6でも(v4同様)
  - 通信ができなかったり、できたり
  - ping応答はあるが，届かないメールがあったり
  - サーバにtelnetやsshではログインできる
  - ファイルがたくさんあるフォルダだと、lsで固まったり

特殊用途のprefix

- 特殊用途のprefixをソースとしたパケットは、基本的にフィルタ出来る
  - Special-Use IPv6 Addresses (RFC5156)
    - 予約済み(元サイトローカル) fec0::/10
    - ULA fc00::/7
    - マルチキャストアドレス ff00::/8
    - ドキュメントアドレス 2001:db8::/32 など
  - IPv4互換アドレス (::a.b.c.d/96)
  - IPv4射影アドレス (::ffff:a.b.c.d/96)
    - IPv4アドレスがa.b.c.dの時

拡張ヘッダについて

- 拡張ヘッダについて
  - IPv6では拡張ヘッダが連続して数珠つなぎ
    - フラグメントヘッダや、hop-by-hopヘッダなど
    - いくつでも続く
    - いくつ先がTCPヘッダなのかわからない
  - 拡張ヘッダ付きパケットについて、フィルタに制限がある実装もあるので注意

その他の注意

- SPI関連
  - ステートフルファイヤーウォールが可能な機器でも、アプリケーションによるので確認が必要
- 機器の管理・運用面の機能に注意
  - IPv6アドレスが表示できなかったり
  - Logに出力できなかったり
- IPv6環境ならではの通信は、要個別検討
  - IPv6環境での、End-to-EndのIPsec
  - P2Pアプリ
  - トンネリング

(実習) フィルタ設定

- フィルタの設定をします

フィルタ名「xxx」を作ります

```
(config)# ipv6 access-list xxx
```

送信元2001:db8::/32からのパケットを許可します

```
(config-ipv6-acl)# 100 permit ipv6 2001:db8::/32
any
```

interfaceへ移行

```
(config)# interface gigabitethernet XXX
```

フィルタをin方向で適用

```
(config-if)# ipv6 traffic-filter xxx in
```