不正RAの傾向と対策

アラクサラネットワークス(株) ネットワーク技術部
鈴木伸介 〈suz@alaxala.net〉

AlaxalA
For The Guaranteed Network

0. はじめに

本講演の流れ

IPv6は、一部プロトコルの挙動は若干違うが、基本的にはIPv4と同じ

→ 基本的にはIPv4のセキュリティ対策が適用可能

例. TCPへの攻撃対策, Phishing詐欺対策, …

→「一部のプロトコル挙動の違い」が、既存のIPv4セキュリティ対策にどう影響するかを考える必要あり

本発表では、IPv4/v6で大きく異なる部位であるRA(Router Advertisement)に注目します。

- はじめに
  RAとは? DHCPv6との違いは?
- 不正RAの傾向
  想定されうる脅威, 流れる契機
- 不正RAの対策
  流れても見つけられるようにする、流せなくする
  各案の比較

注意 「万能薬」はありません

（IPv6にかぎったことではありませんが）

セキュリティ対策の効果は

・放置したことによる被害

・対策を講じることによるコスト

のバランスで決まります。両者のバランスは、ケースバイケースで異なるため、「一般的にどこでも通じる万能な答え」はありません。

そのため、各セキュリティ対策の適用に際しては、利害得失を正しく理解した上で適用是非を判断する必要があります。

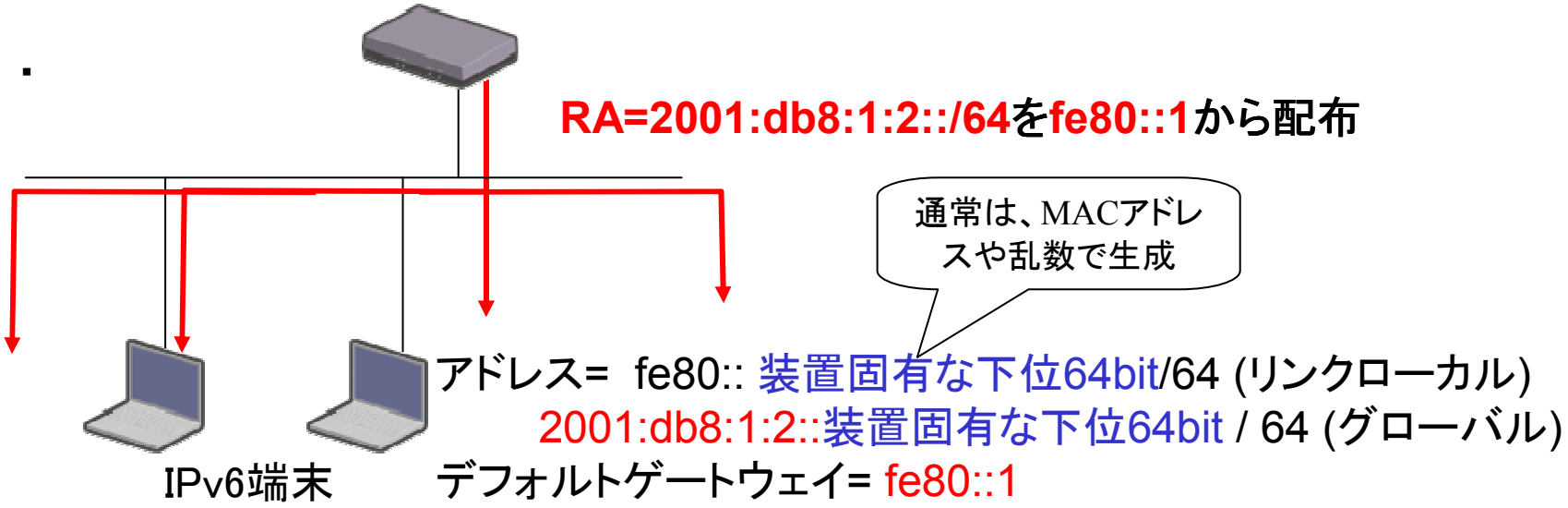
RA (Router Advertisement) とは?

・IPv6グローバルアドレス生成に用いるプロトコル
  - ルータが、RAでPrefix・デフォルトゲートウェイをマルチキャストで広告
  - 端末が、受信したPrefixからグローバルアドレス+デフォルトゲートウェイ設定

・2種類のRA広告
  - 端末からの要求(Router Solicitation=RS)により、送付 (solicited RA)
  - RS受信とは無関係に、ルータが自発的に送付する(unsolicited RA)

・いずれの場合も、端末は、RAパケットを1つ受信するだけで、アドレス+デフォルトゲートウェイを生成

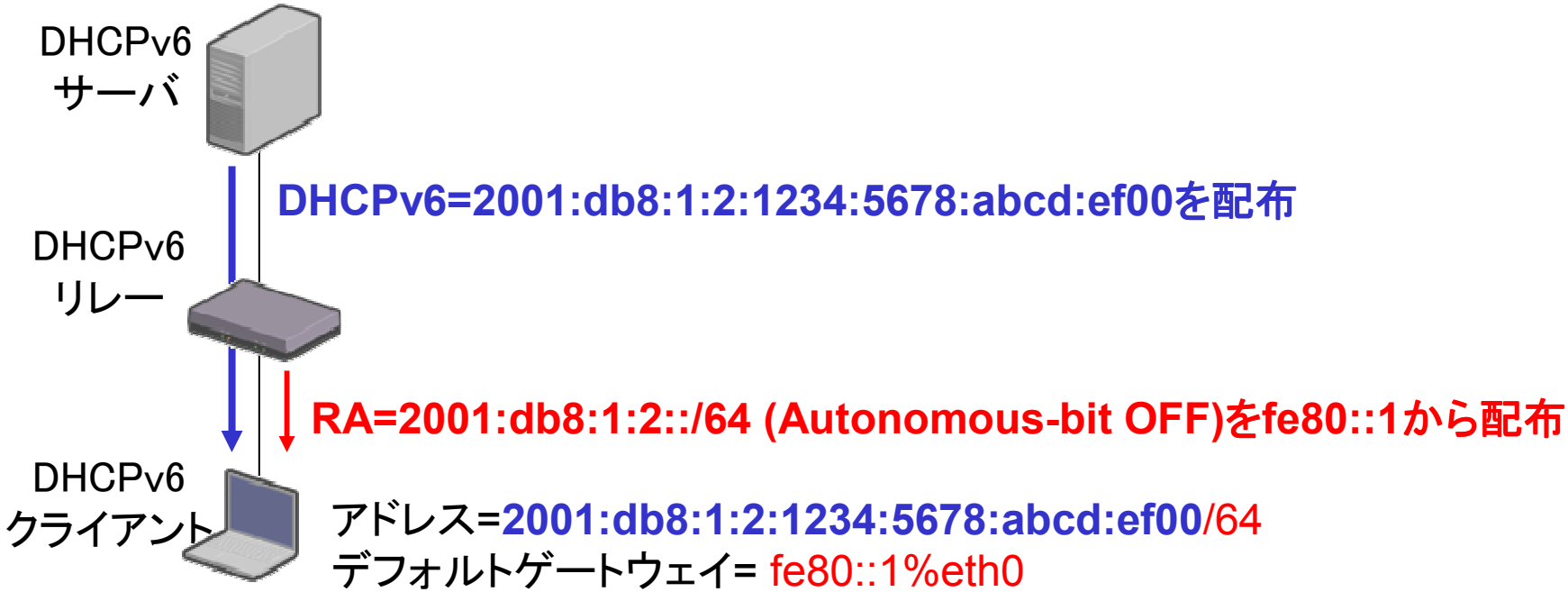
・



DHCPのIPv6版もあるはずだが…

- IPv4 DHCPと同様なプロトコルやり取りを行うが、DHCPv6単体では動作不能
  - DHCPv6では、デフォルトゲートウェイやPrefix長を配布できない
  - 端末でDHCPv6を起動するトリガーはRA (M-flag, O-flag)

=> 実質的にRA必須



参考）DHCPv4/DHCPv6/RAで配布できる情報の比較

現状、DHCPv6で配布できない情報は多数ある

- 黄色= DHCPv4/RAでは配れるが、DHCPv6では配れない情報
- 青色= RAでは配れるが、DHCPv6では配れない情報

		RA	DHCP v6	DHCP v4
アドレス関連	インタフェースのプレフィックス情報 （Prefix , Prefix長）	○	×	○
	インタフェースのプレフィックス情報 （有効期間, Onlink情報）	○	×	×
	インタフェースのアドレス情報(アドレス, 有効期間)	×	○	○
	Prefix DelegationのPrefix情報 (Prefix, Prefix長, 有効期間)	×	○	×
経路関連	デフォルトルータ情報 (IPアドレス, 有効期間)	○	×	○
	デフォルトルータ情報 (MACアドレス,優先度)	○	×	×
	デフォルトルート以外の経路情報	○	×	×
その他	NDP情報 (キャッシュ有効期間, NDP再送時間)	○	×	×
	TTL	○	×	×
	MTU	○	×	×
	DNSサーバ情報	○	○	○
	その他サーバ情報(NTP, SIP, …)	×	○	○

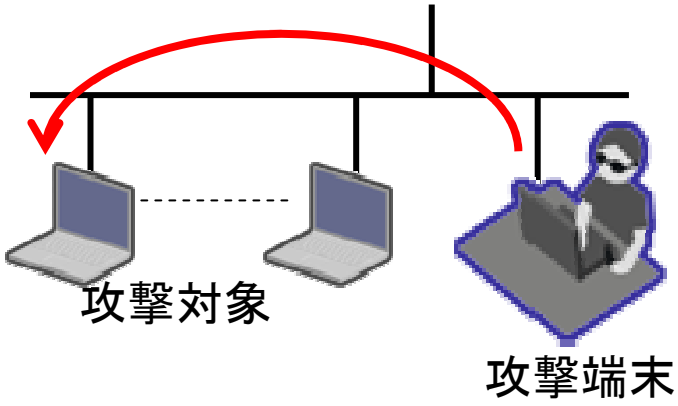
1. 不正RAの脅威

1(1) 不正RAとは?

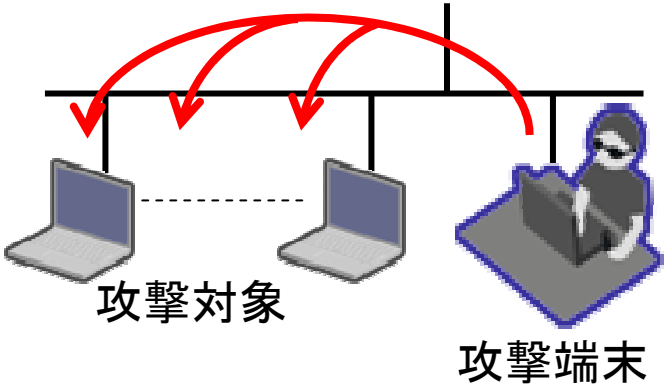
・不正RA＝ネットワーク管理者が元々流すつもりのないRA
・本質的には、DHCPv4サーバの偽装と一緒

・RAはパケット1つ流すだけでLANセグメント内全体に波及
→不正RAによる攻撃は、通常の攻撃よりもインパクト大
(※DHCPでは(事実上)unicastで端末−サーバ間のやりとりをするため、そこまで大きく波及させることが出来ない)

通常の攻撃:
1パケットで1端末しか攻撃できない



RA:
1パケットでLANセグメント全体を攻撃可能



1(2) 不正RAが端末にもたらす脅威

端末の立場では、RAが不正かどうかは判断できない

→RAを受信した端末は、プロトコルの規定通りにアドレスやデフォルトゲートウェイを生成

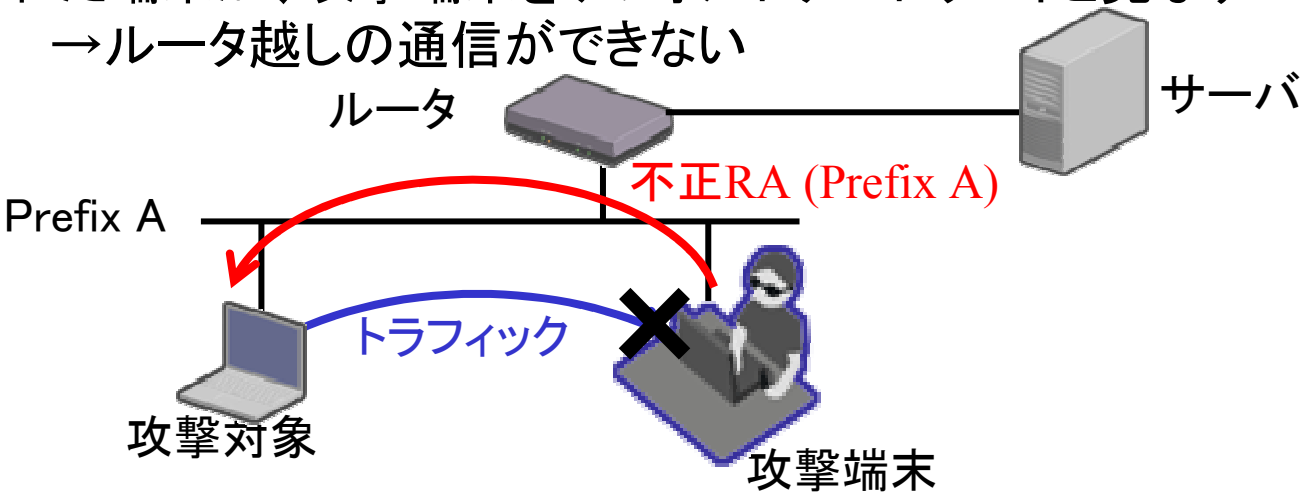
→下記のような脅威が発生

不正な生成物 / 脅威	アドレス	デフォルトゲートウェイ
①通信断	○	○
②盗聴	×	○
③詐称	○	○
④DoS	○	×

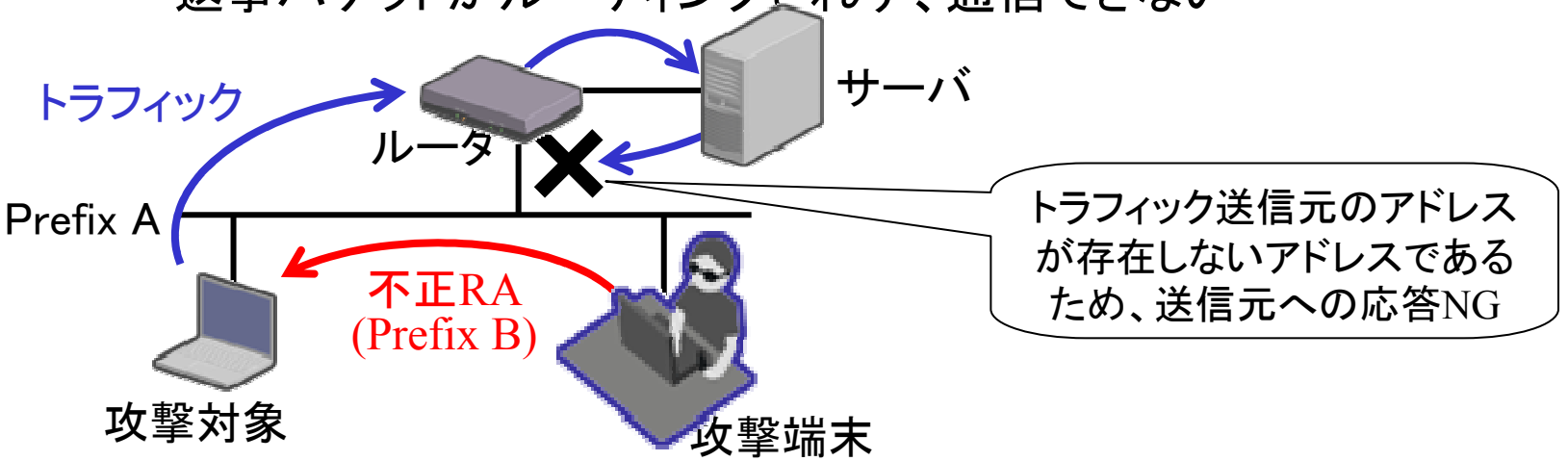
特に最近は「デフォルトでIPv6 on」な端末も多いため、「何も対策を講じないこと」の潜在リスクが高まっている。

1(3) 不正RAによる通信断の例

攻撃された端末が、攻撃端末をデフォルトゲートウェイと見なす
→ルータ越しの通信ができない

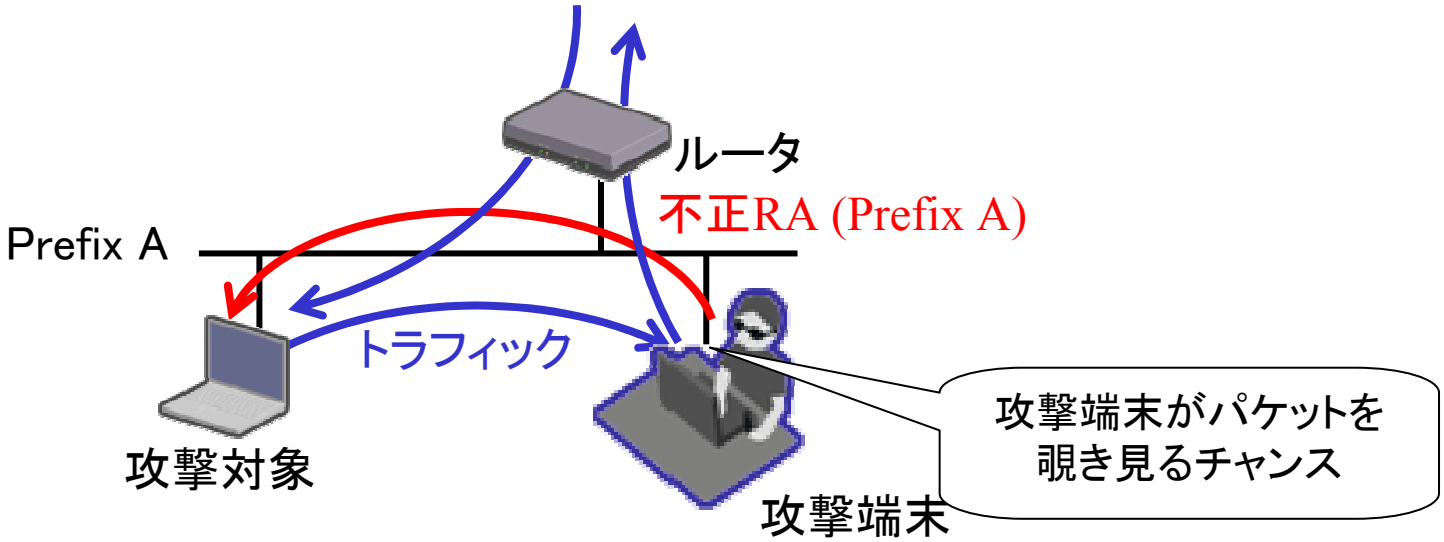


攻撃された端末が、網上に存在しないソースアドレスを使用
→返事パケットがルーティングされず、通信できない



1(4) 不正RAによる盗聴の例

攻撃された端末が、攻撃端末をデフォルトゲートウェイと見なす＆
攻撃端末が正しくL3ルーティングをする
　→　攻撃端末は、攻撃された端末が知らない間に、
　　トラフィックを覗き見可能

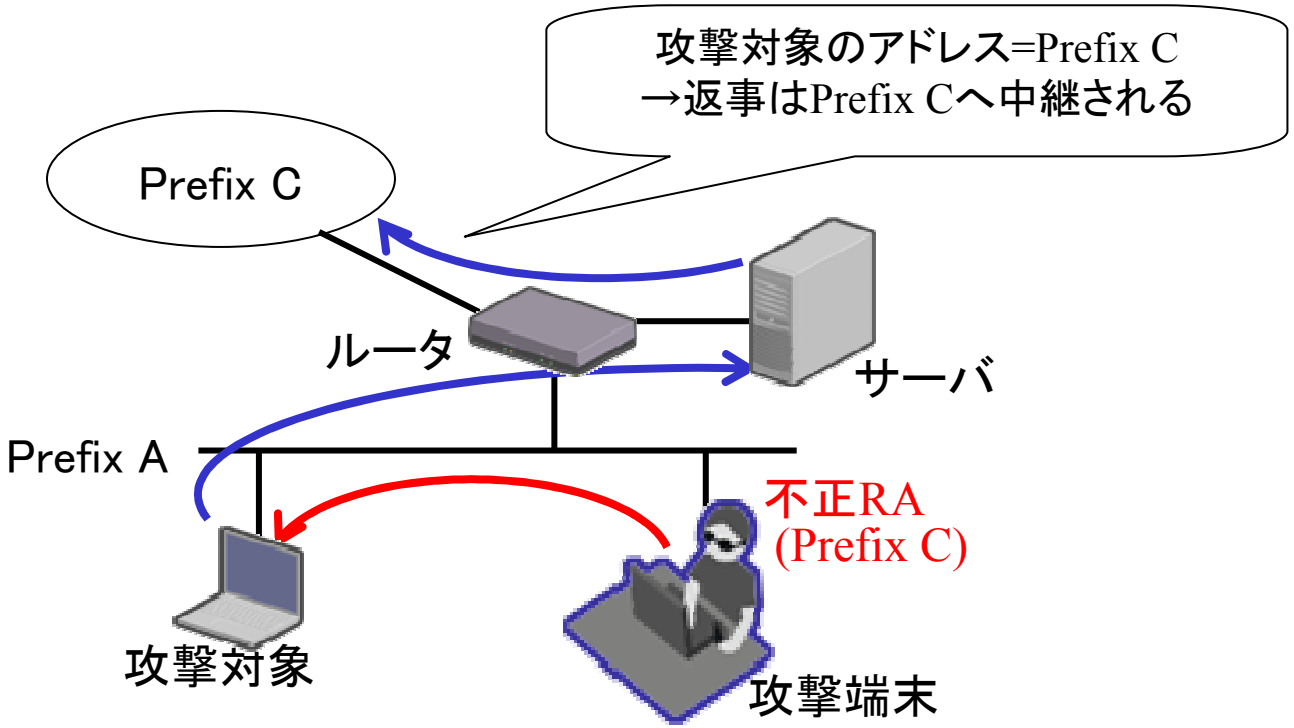


1(6) 不正RAによる詐称の例

攻撃された端末が、全くよそにあるソースアドレスを使用

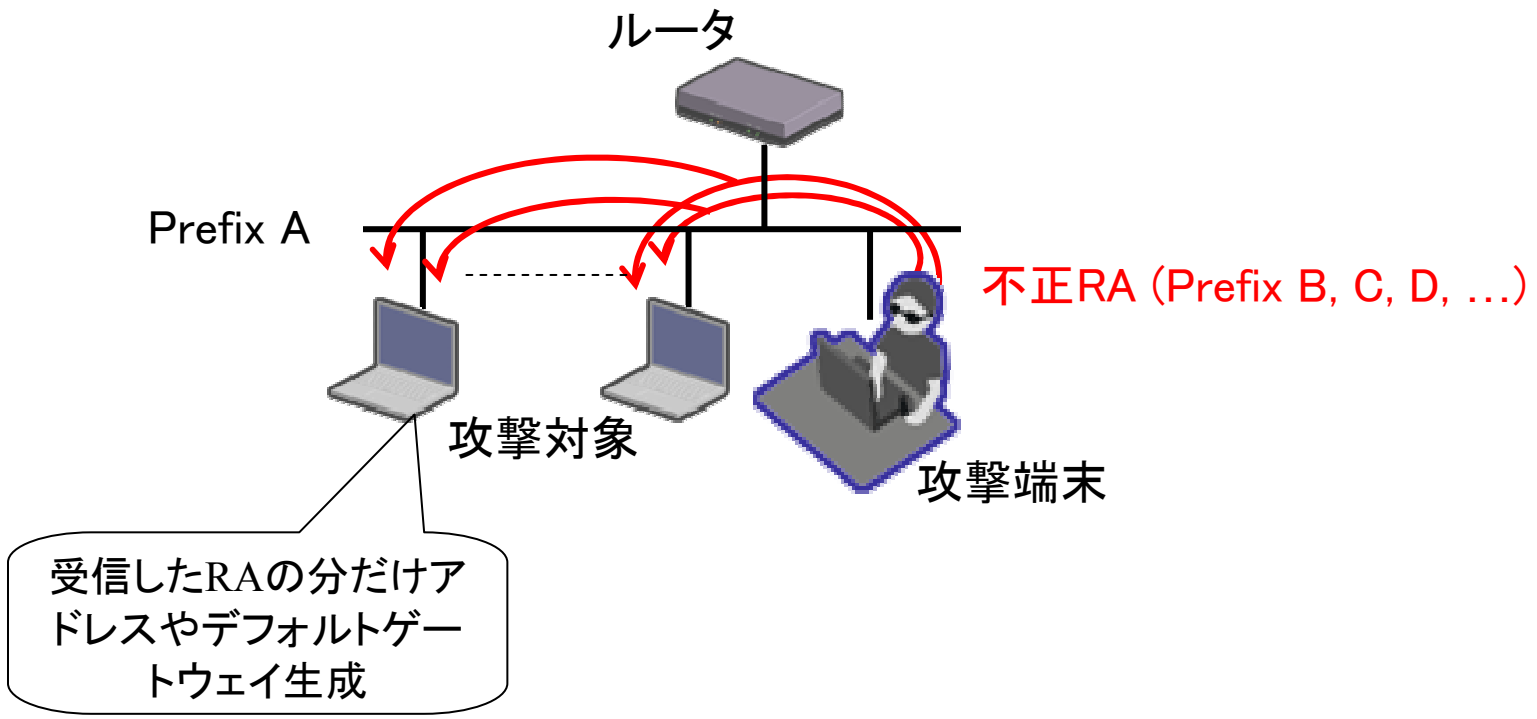
①サーバは、よそからのアクセスだと思い込む（アクセス解析の妨害）

②サーバからの返事は、そのソースアドレスへ向かう（遠隔攻撃）



1(5) 不正RAによるDoSの例

攻撃された端末は、何も考えず、受信したRAでアドレスやデフォルトゲートウェイを生成
→攻撃端末が多種多様なRAを流すと、端末は、その個数に比例した量のアドレスやデフォルトゲートウェイを生成　→　メモリ不足に陥る



2. 不正RAはそんなに流れるものなのか?

2(1) 不正RAが流れる原因

・原因別に考えると、下記3種類に大別される

①網攻撃のために、意図的に流されたRA

②オペレーションミスで、誤って流れたRA

③網設計ミスで、誤って流れたRA

・意外と流れることが多いのが実情。

②は「おかしなことが起こって、初めて気づく」ことが多い

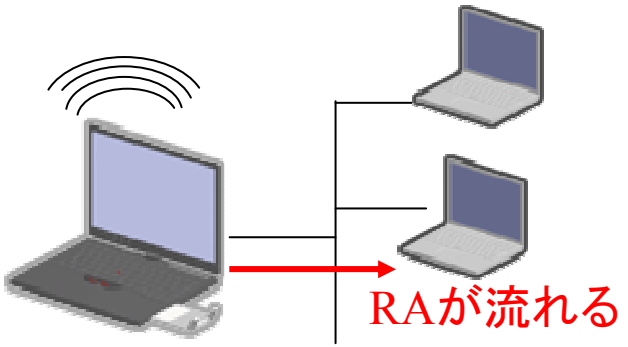
③は「IPv6をONにしてみて、初めて気づく」ことが多い

2(1) オペレーションミスで、誤って流れるRA

例) WindowsでICS (Internet Connection Sharing)がONだと、外部接続を共有する側のリンクにRAが自動的に流れる

・無線LANを複数端末で共有

・6to4などでIPv6コネクティビティ確保



http://technet.microsoft.com/ja-jp/library/cc779985(WS.10).aspx

※Windows は米国 Microsoft Corporation の米国およびその他の国における登録商標です

例) コンフィグ作業中に一度誤ったアドレスを設定してしまった

(config-if)# ipv6 nd prefix *Prefix-A* ...<ret>

*Prefix-B*の打ち間違いだったので、再入力

(config-if)# no ipv6 nd prefix *Prefix-A* ... <ret>

規格上は、ここでPrefix-Aをリセットする RAが数個流れるが...

(config-if)# ipv6 nd prefix *Prefix-B* ... <ret>

=> たまたま上記のリセット用RAを受信し損ねた端末(e.g. サスペンド中)は *Prefix-A, Prefix-B*の両方を学習したまま

2(2) 網設計ミスで、誤って流れるRA

・世の中には「マルチキャストと相性の悪いL2技術」が意外に多い

例) IPv4サブネットVLAN

IEEE802.1x認証VLAN

…

・IPv4は偶々「ユニキャストさえ正しく動けば何とかなった」が、

IPv6は「マルチキャストも正しく動かないとダメ」(RAはマルチキャストで流れるため)

→マルチキャストと相性の悪いVLANでIPv6を動かすと、

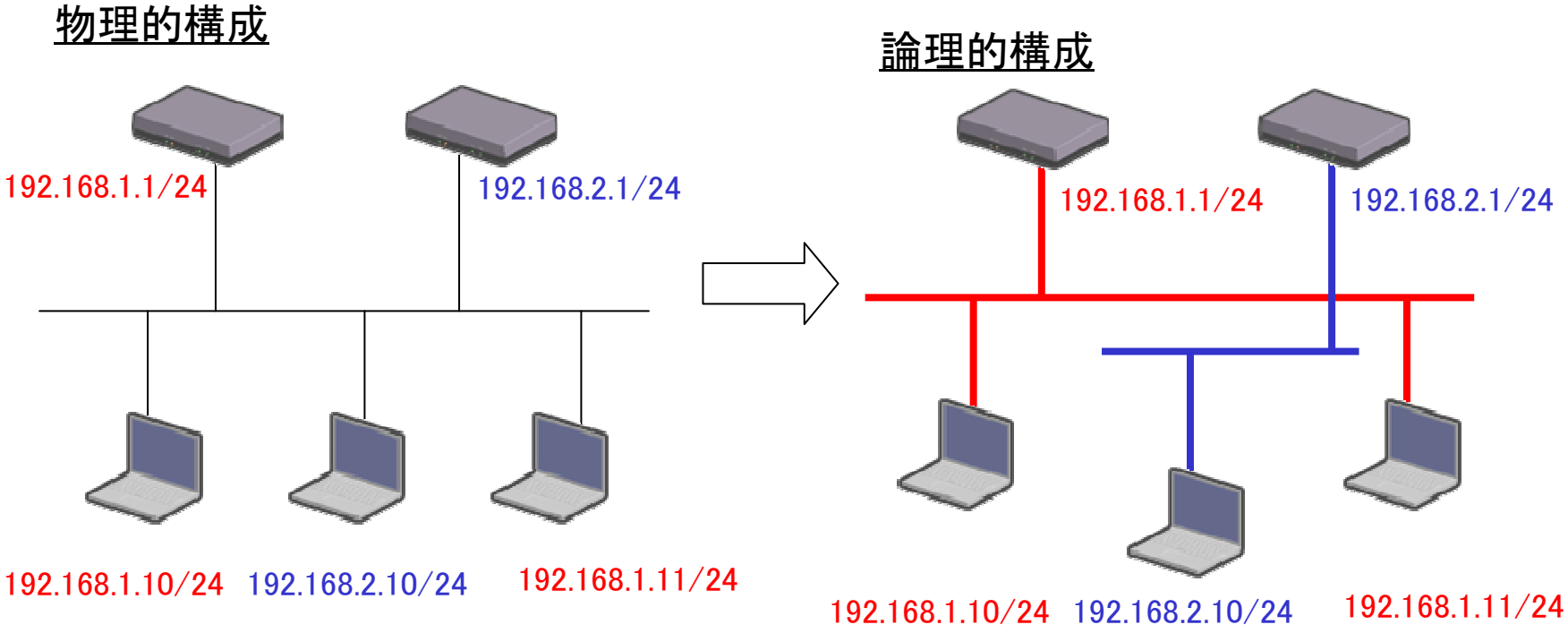
「異なるIPサブネットにRAが漏れる」ように見える

2(2) 網設計ミスで、誤って流れるRA

例) IPv4サブネットVLAN

同じVLAN上に、複数のIPv4サブネットを共存させる

IPアドレスにより、ブロードキャストドメインを分割する。

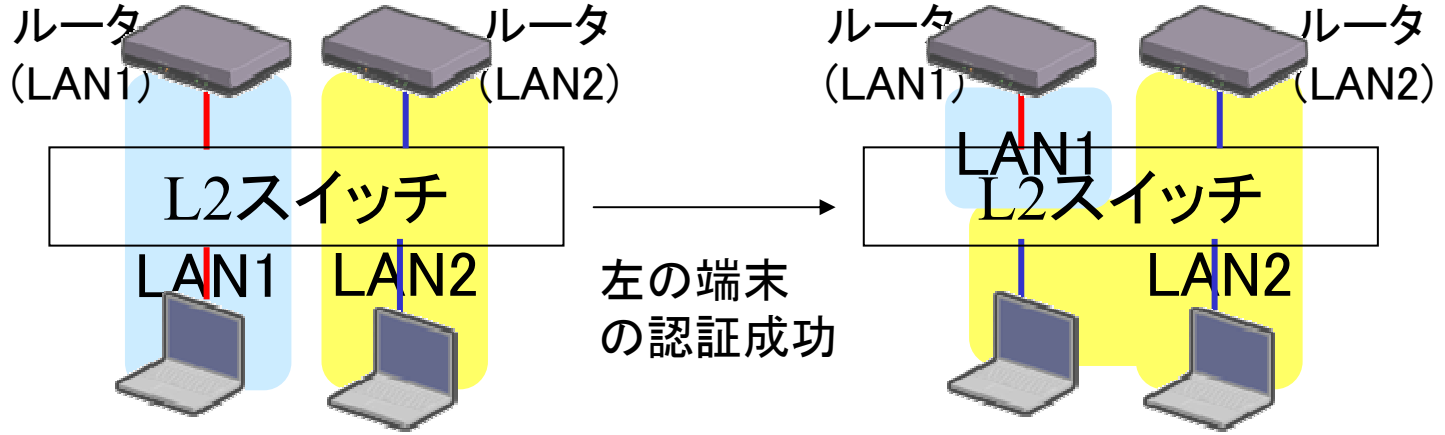


論理的構成に合わせてルータから赤青2種類のRAを流すと、全ての端末に2種類のRAが届く (論理的に別ネットワークだが、物理的には同一ネットワークなので)

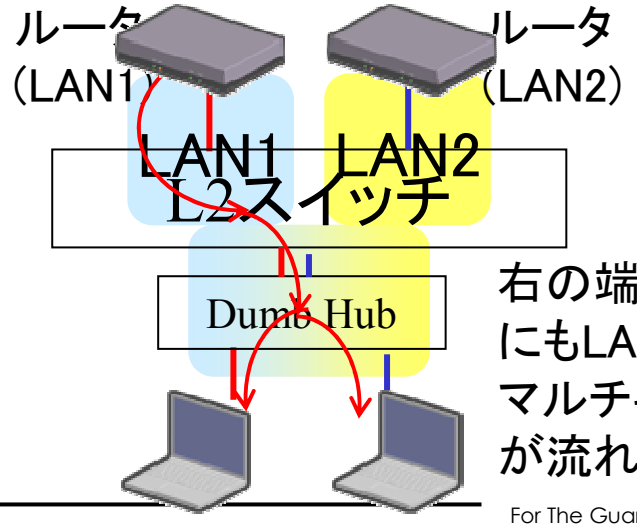
2(2) 網設計ミスで、誤って流れるRA

例) IEEE802.1x

①IEEE802.1xでは、端末の認証結果によって、端末収容VLAN
を変えることが出来る (e.g. 検疫ネットワーク)



②IEEE802.1xを用いたシステムでは、1つのポートに複数の端末が
ぶら下がることもある (ポート単位ではなく、MAC単位で、アクセス制御)
(esp. 無線LAN)
→上流から流れたマルチキャスト
パケットは複数VLANに漏れる



3. 不正RAの対策

4. 不正RAの防止策の概要

・不正RAの本質は「不正なパケットがマルチキャストで拡散されること」

・下記3種類に大別される

1) 混信しても困らないように、同じ値でRA広告
※正当なRAがサブネット間で漏れるケース限定

2) 流れたら、検知する
※マルチキャストで拡散される分、逆に見つけやすいことに着目

3) そもそも流れない/使われないようにする
※「不正RA対策」というより、「マルチキャスト対策」に近いものが多い

どれがよいかは、コストと効果のトレードオフ次第

4(1) 混信しても困らないよう、同じ値でRA広告

・混信するRAのパラメータが同じ値ならば、端末の立場では何も困らない → 意図せず混信した場合でも端末への影響0

・実際にアドレスを生成するプロトコルにより、RAのパラメータの合わせ方が2種類ある

i) RAでアドレス生成

ii) DHCPv6でアドレス生成

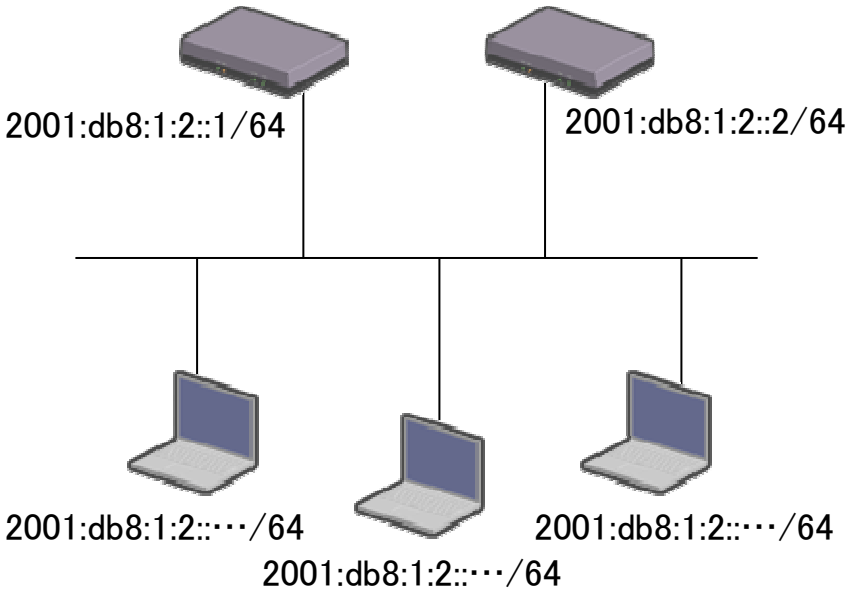
・オペレーションミスで流れたRAに対しては無効だが、網設計ミスで流れたRAに対しては有効

4(1) 例1. RAでアドレス生成する場合

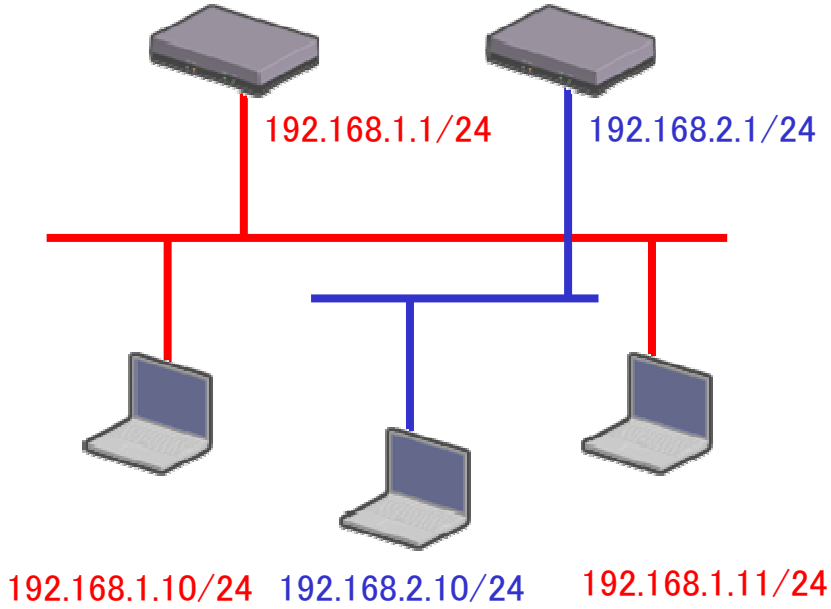
「IPv4では別サブネット」でも、「IPv6では同じサブネット」とする
　元々単なるアドレス不足でIPv4サブネットを分けた場合には、これで十分

※ネットワーク運用ポリシーの都合上、サブネット分割する場合には対応不能。。。

IPv6網構成



IPv4網構成



4(1) 例2. DHCPv6でアドレス生成

DHCPv6でアドレス生成 + DHCPv6で配布できない情報のパラメータ合致

[デフォルトゲートウェイの混信防止]
①ルータのリンクローカルアドレスを全て同じにする
②RAのMACアドレス通知オプションをOFFにする
[Prefixの混信防止]
③RAで広告するPrefixは、自動設定の対象外とする
[端末間通信の保証]
④RAで広告するPrefixは、Onlinkではないことにする
⑤ICMPv6 RedirectをOFFにする

※DHCPv6によるアドレス配布が大前提。。。

```
interface vlan 10
   ipv6 address 2001:db8:abcd:10::1/64
 ①ipv6 address fe80::1 link-local
   ipv6 nd management-config-flag
 ②ipv6 nd no-advertise-link-address        ④          ③
   ipv6 nd prefix 2001:db8:abcd:10::/64 off-link no-autoconfig
 ⑤no ipv6 redirects

interface vlan 11
   ipv6 address 2001:db8:abcd:11::1/64
 ①ipv6 address fe80::1 link-local
   ipv6 nd management-config-flag
   ipv6 nd no-advertise-link-address
   ipv6 nd prefix 2001:db8:abcd:11::/64 off-link no-autoconfig
   no ipv6 redirects
```

4(1) 例2. DHCPv6でアドレス生成 (cont.)

DHCPv6だけでアドレス生成できるようにする

IPv4同様、DHCPv6でデフォルトゲートウェイやプレフィック長を流せるようにする = RAなしで、DHCPv6だけでアドレス生成 (現在、IETFにて議論中)

長所)

DHCPv4と同様な運用が可能

短所)

DHCPv6のプロトコル仕様の改変が必要

→現状、対応した実装はなし

RAによるアドレス生成が無効になるわけではない

→端末側でRAを無効にすることが大前提

4(2) 不正RAが流れたら検知する

・「不正RAはほとんど流れない」「流れるとしたらオペレーションミス」と仮定し、「不正RAが流れたら検知する」ことだけに注力するのも一案。

→できることは限られる代わり、安価なことがメリット

・実現方法はいくつかある

例1. ルータのリンクローカルアドレスを、手動設定

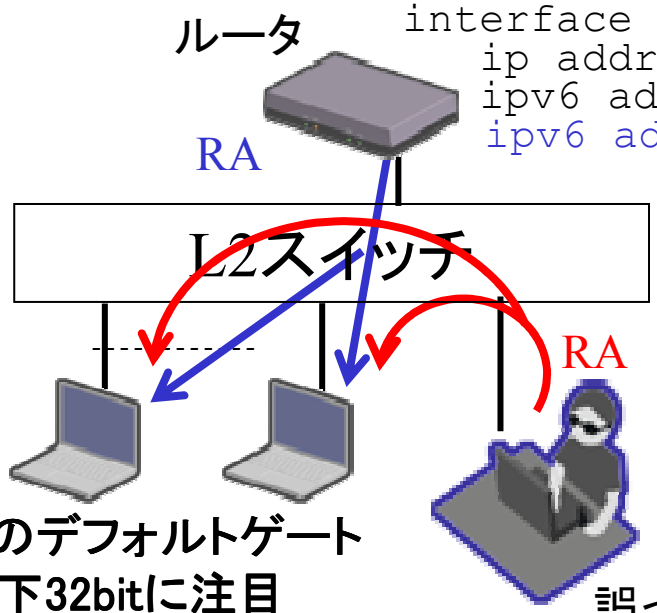
例2.　RA監視サーバを設置

例3. SAVI (Source Address Verification Improvements (*))

*) 標準化作業中

4(2) 例1. ルータアドレス手動設定による不正RA検知

ルータのリンクローカルアドレスを、自動設定値ではなく、わかりやすい値に手動設定
→ デフォルトゲートウェイのアドレスから、不正RAを容易に発見可能




```
interface vlan 10
   ip address 192.168.2.1 255.255.255.0
   ipv6 address 2001:db8:abcd:10::1/64
   ipv6 address fe80::192:168:2:1 link-local
```

IPv4/v6のデフォルトゲートウェイの下32bitに注目
⇒表示が違っていたら、意図せぬRAが流れている

誤ってRAを流してしまった端末

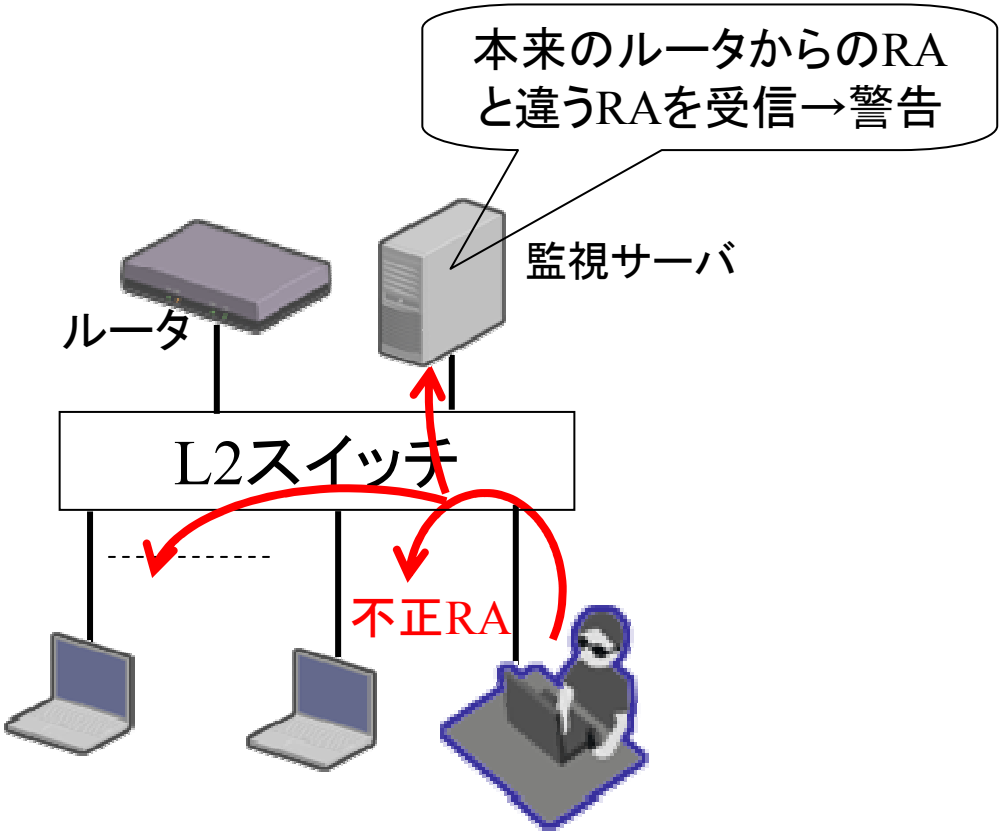
※デフォルトゲートウェイのMACアドレスだけ詐称する攻撃は見破りにくい。。。
(source link-layer address option)

4(2) 例2. RA監視サーバによる不正RA検知

RA監視サーバをLAN上に設置

例. NDP Mon (http://ndpmon.sourceforge.net/)

RAmond (http://ramond.sourceforge.net/)



※Unicastで流れる不正RAは検出困難。。。

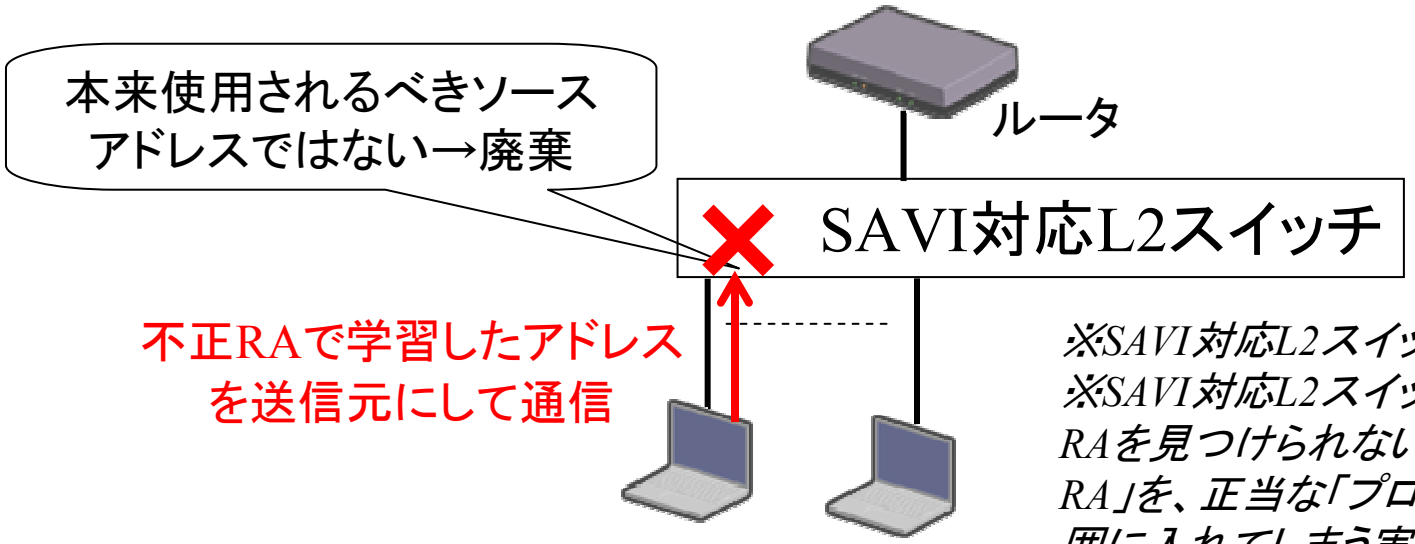
4(2) 例3. SAVIによる不正RA検知

SAVI (Source Address Verification Improvements)

- Dynamic ARP InspectionやDHCP-snoopingの親戚

  L2スイッチでDHCPv6やNDPのプロトコルの内容を覗き見し、「プロトコルのやりとり上、ありえないソースアドレス」ならば廃棄

- IETFにて標準化中



※SAVI対応L2スイッチの導入が必須。。。
※SAVI対応L2スイッチを導入しても、不正RAを見つけられない場合もある。(「不正なRA」を、正当な「プロトコルのやりとり」の範囲に入れてしまう実装ではNG)
※L2スイッチのSAVI機能自体に対するDoSも可能。。。

4(2) 不正RAを検知した後は?

・不正RAを検知した後の対処策もいくつかあります

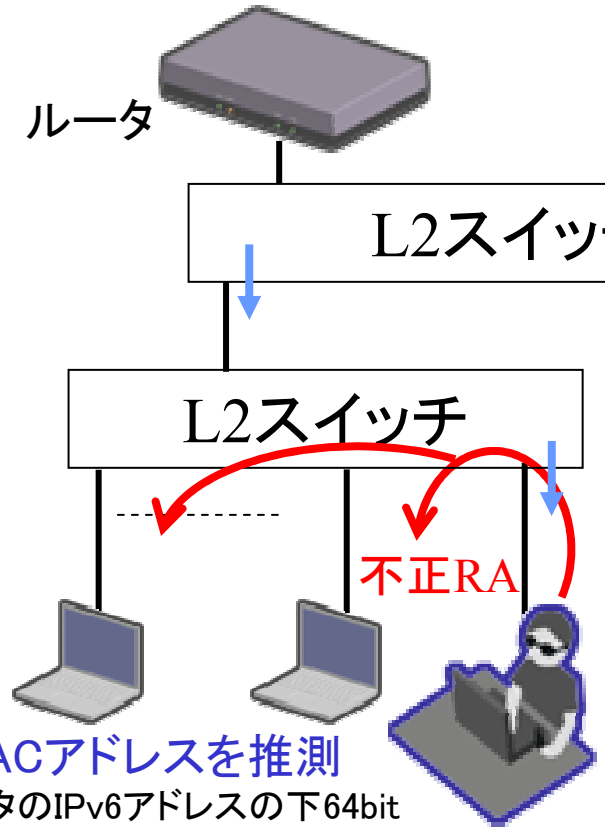
例1. 端末のありかを特定

例2. 不正RAを打ち消すRAを流す（毒消し）

4(2) 不正RAを検知した後の対策例

（例1）

不正RAの送信元MACアドレスに注目して、RA発信元を追跡
→該当端末を網から外す



②該当MACのありかを調べる
（スイッチのFDB, ARPテーブル,
DHCPv4サーバの履歴, …）

FDBから判断される「不正RA送信元MAC」のありか

①不正RAのMACアドレスを推測
e.g. デフォルトルータのIPv6アドレスの下64bit
デフォルトルータのIPv6アドレスのMACアドレス
（source-link-layer address option）

※「FDBを見ても存在しないMAC」を不正RAで広告されると対応不能。。。
(source-link-layer address optionのみ詐称)

4(2) 不正RAを検知した後の対策例

（例2）

「意図せぬRAをリセットするRA」を出すサーバを設置

※オープンソースで色々開発されています

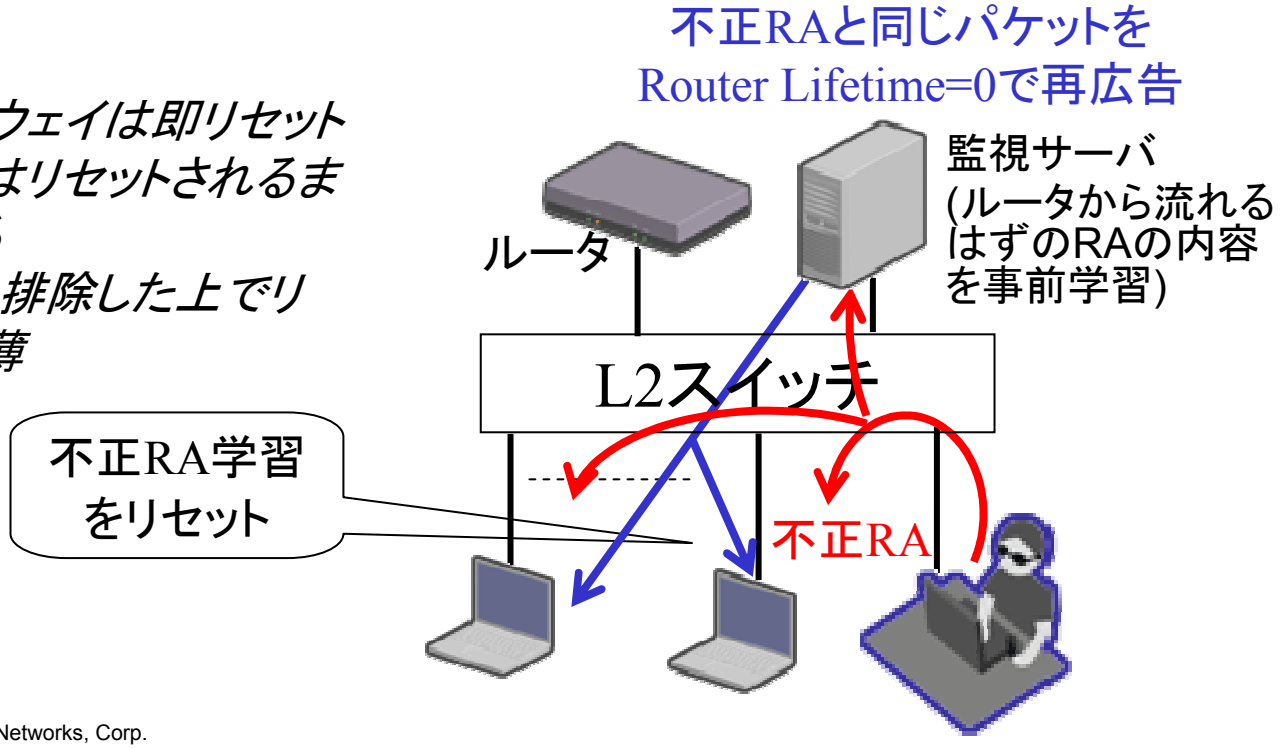
KAME rafixd (http://www.kame.net/)

NDP Mon (http://ndpmon.sourceforge.net/)

RAmond (http://ramond.sourceforge.net/)

Scapy Script (http://ipv6hawaii.org/?p=143)

※デフォルトゲートウェイは即リセットされるが、アドレスはリセットされるまでに2時間程かかる
→不正RA送信元を排除した上でリセットしないと効果薄



4(3) 不正RAが流れない/使われないようにする

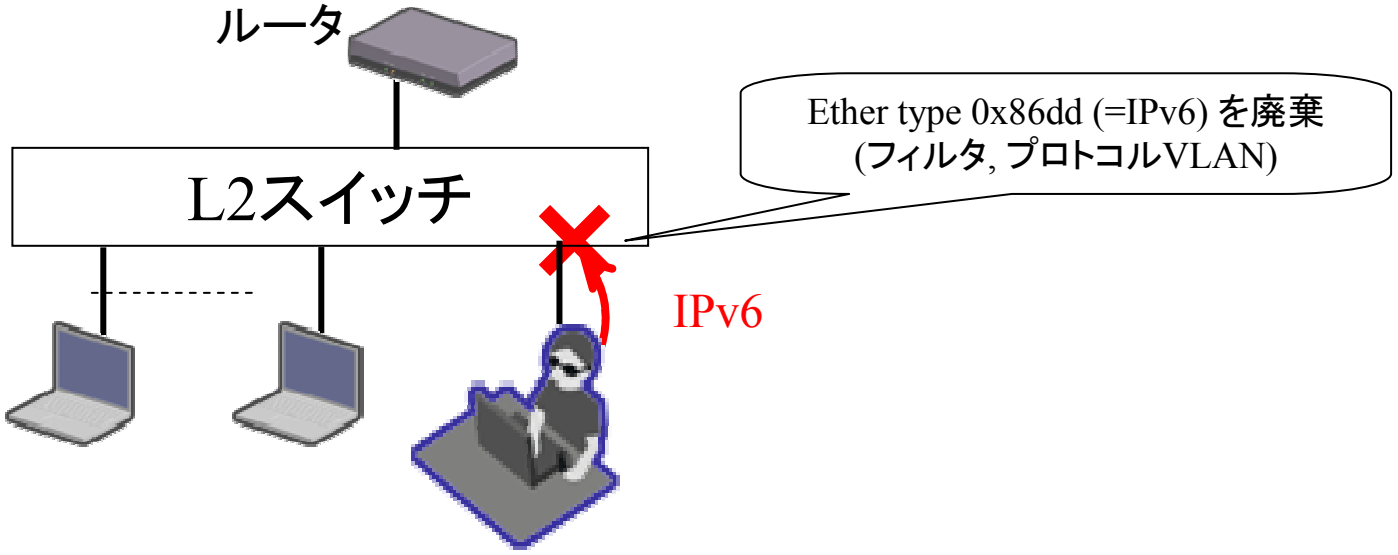
対策を講じる場所により、下記のように大別されます

対策箇所	手法
網側	①網側で不正RAを排除 i) IPv6パケットを廃棄 ii) 端末収容ポートでRAをフィルタ廃棄 iii) 端末間のL2直接通信を許容しない iv) 端末-ルータ間をPoint-to-Pointで接続 v) IPv6パケットを廃棄+ IPv6 over IPv4トンネル
端末側	②端末側で不正RAを使わないようにする i) Router Preferenceにより、本物RAを優先使用 ii) SeNDによるRA認証 iii) パーソナルファイアウォールでRAを廃棄

※細字:標準化作業中 or 実装なし

4(3) ①網側で不正RAを排除

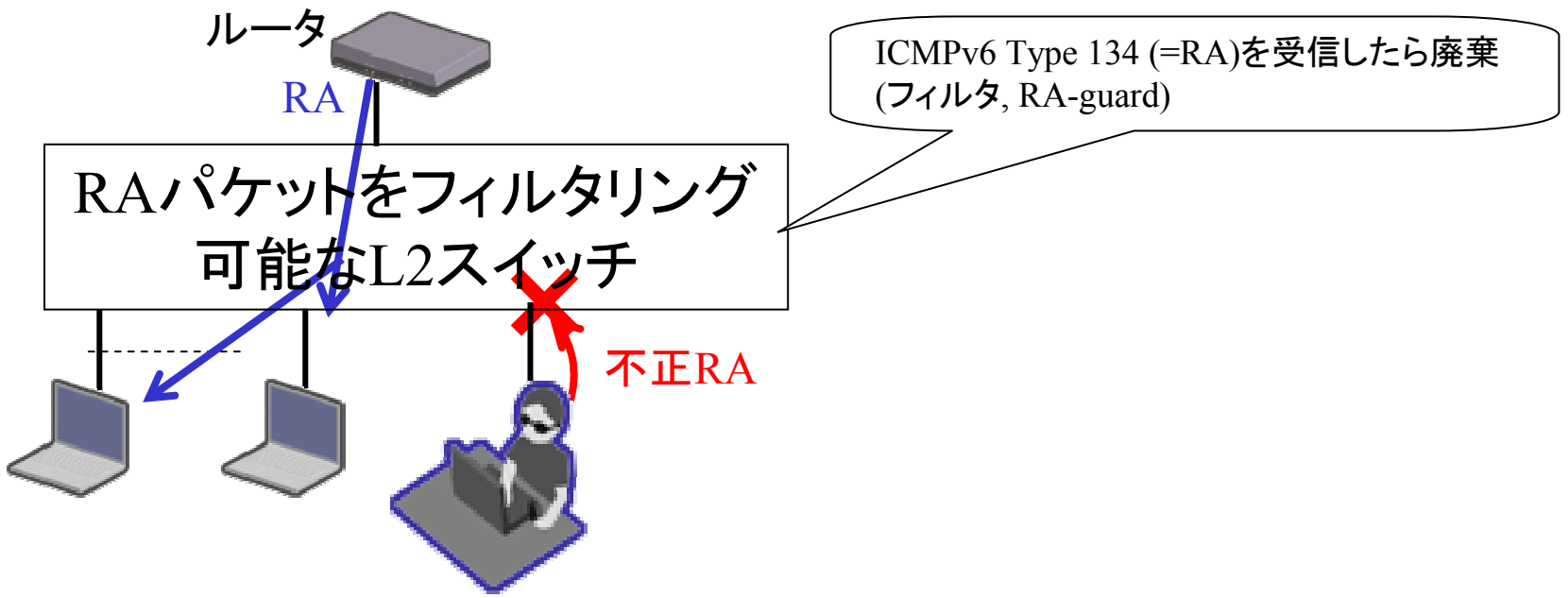
i) L2スイッチにて、IPv6パケットを全て廃棄



※IPv6は未来永劫動かない。。。

4(3) ①網側で不正RAを排除

ii) 端末収容ポートでRAをフィルタ廃棄



※RAフィルタ機能を有するL2スイッチ導入が必須。。。

4(3) ①網側で不正RAを排除

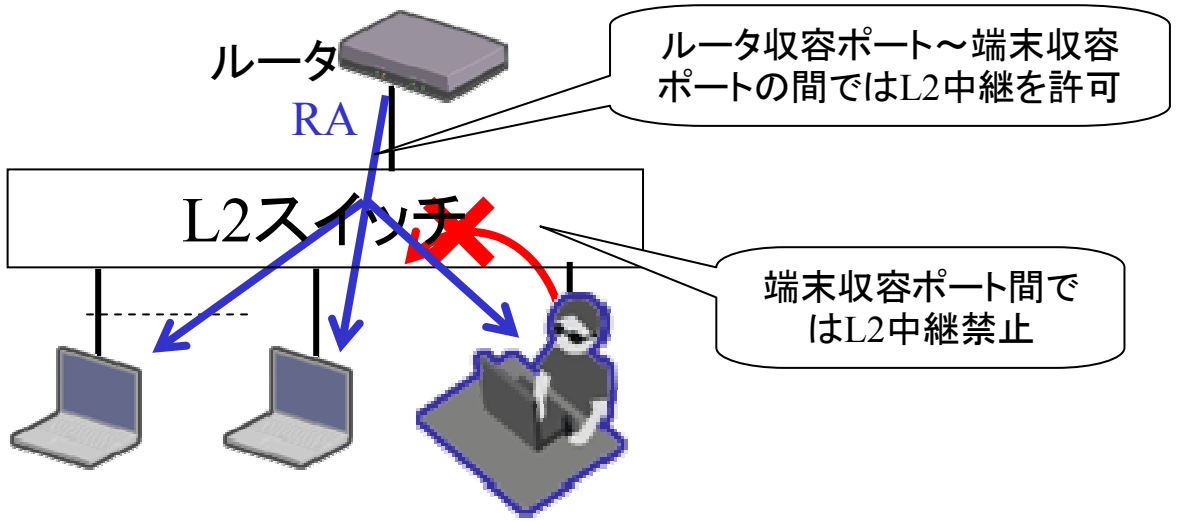
iii) 端末間のL2直接通信を許容しない

※色々な名称で提供されています

- 有線LAN業界)

プライベートVLAN(RFC5517), アップリンクVLAN, ポート間中継遮断機能, VLAN Aggregation (RFC3069), …

- 無線LAN業界) プライバシーセパレーション, ワイヤレスパーティション機能, …

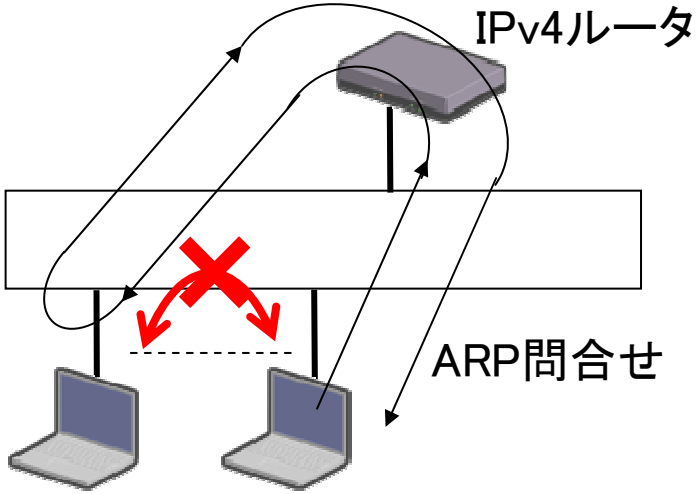


4(3) ①網側で不正RAを排除

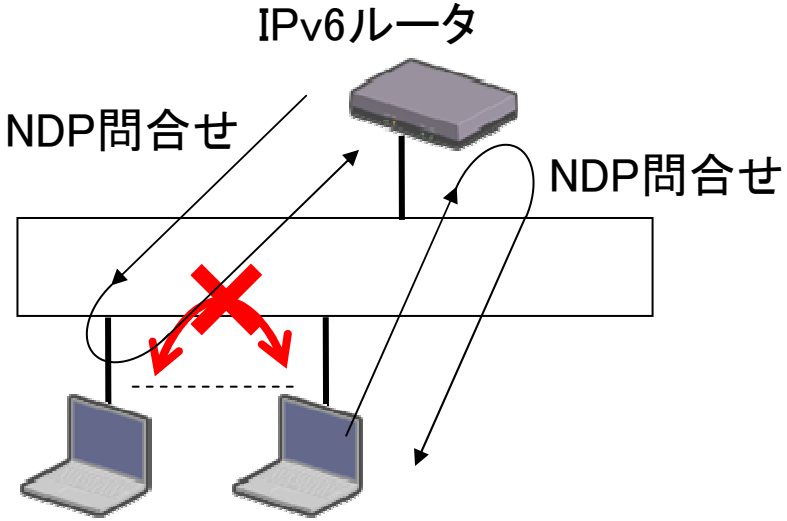
iii) 端末間のL2直接通信を許容しない (cont.)

※RAに限らず、全ての端末間L2直接通信がNG
→下記のような機能に支障あり
アドレス重複検出
リンク内ブロードキャストで動くプロトコル (簡易メッセンジャー, Zeroconf系)

※ルータ越しの端末間通信を実施されるためには、IPv4ルータにIPv4 Local-proxy-ARP機能が必要 (IPv6では相当機能が標準で備わっている (RA でonlink-flag=OFF で prefix広告)



端末間の直接通信NG→ルータがARP解決の仲介を行う必要あり(=Local proxy-ARP)

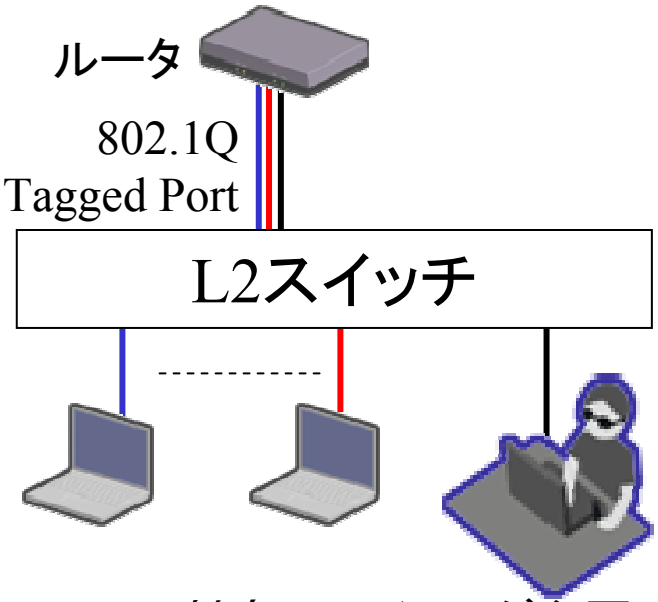


IPv6端末には標準で「connected経路でも、自分以外の宛先は全てルータに投げる」モードあり (Onlink-flag OFF)

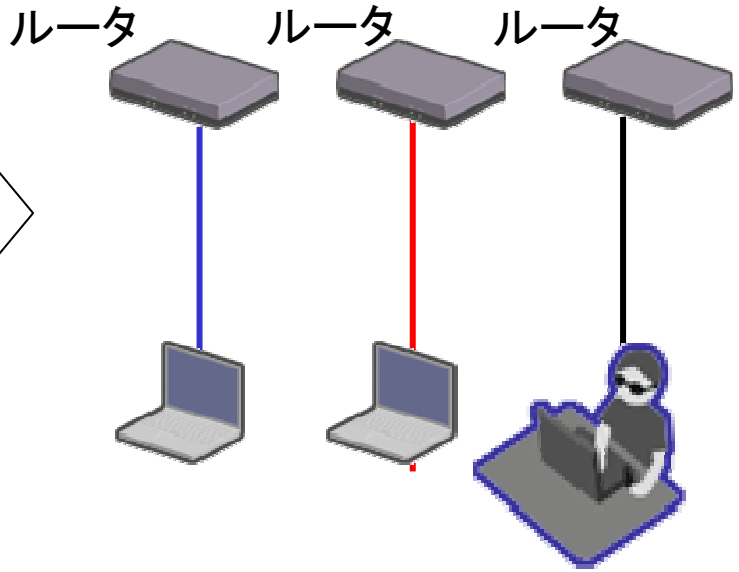
4(3) ①網側で不正RAを排除

iv) 端末-ルータ間をPoint-to-Pointで接続

物理的構成



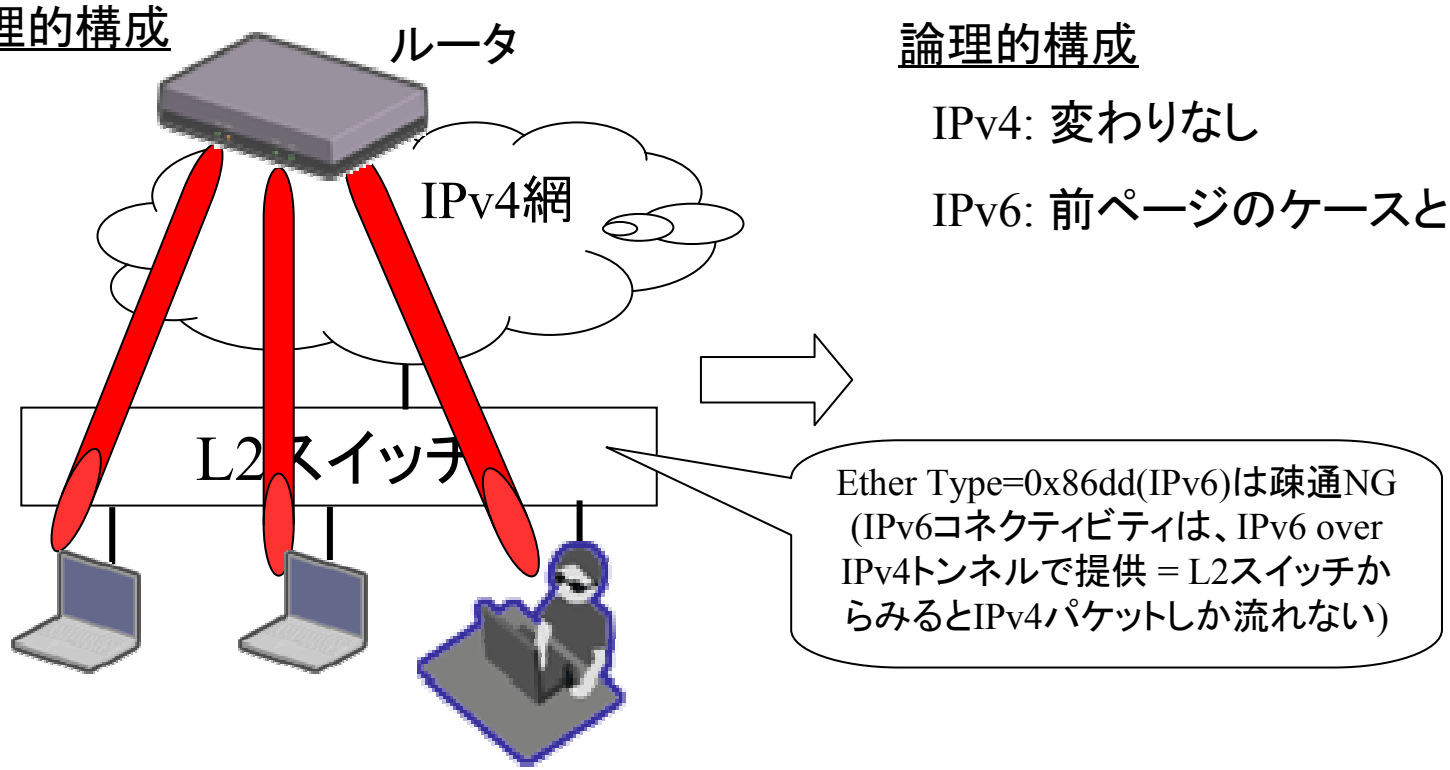
論理的構成



※Tag VLAN対応L2スイッチが必要。。。
※IPv4アドレスのリナンバリング要。。。
※前ページ同様、「リンク内ブロードキャストで動くプロトコル」に影響あり
※IPv4アドレスの使用効率が悪化。。。
例) 元々192.168.0.0/24で済んでいた = 253端末収容可能
各Point-to-Pointリンクに同じ空間で/30を割当 = 64端末収容可能

4(3) ①網側で不正RAを排除

v) i)の策を取った上で、IPv6コネクティビティは、自動IPv6 over IPv4トンネルで提供



※自動トンネル自体がセキュリティホールになりうる

・トンネル終端ルータの詐称リスク

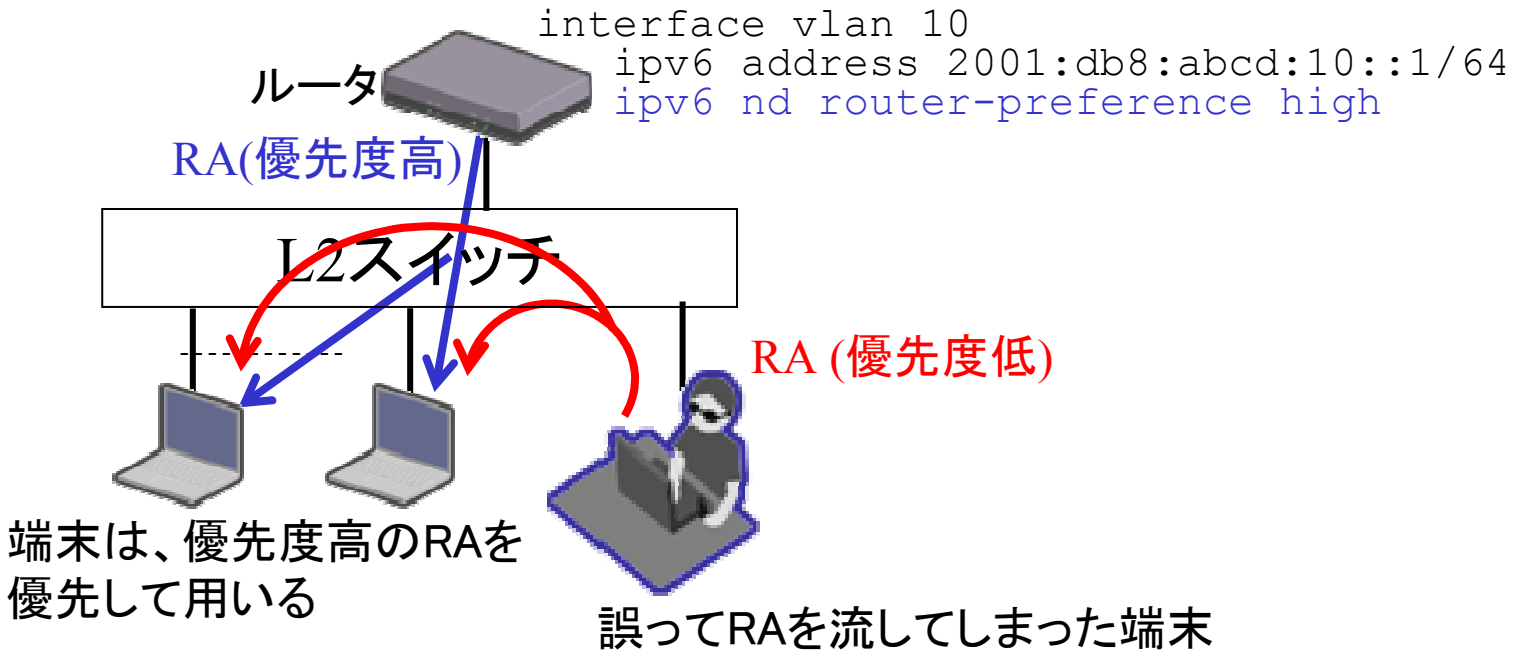
・ファイアウォールやパケットフィルタとの相性悪

→少なくとも「ある程度動作範囲を絞って動くトンネリングプロトコル」が必須

(ISATAP, 6rdなど)

4(3) ②端末側で不正RAを使用しないようにする

i) 本当のルータからのRAを優先して使用（Router Preference; RFC4191）

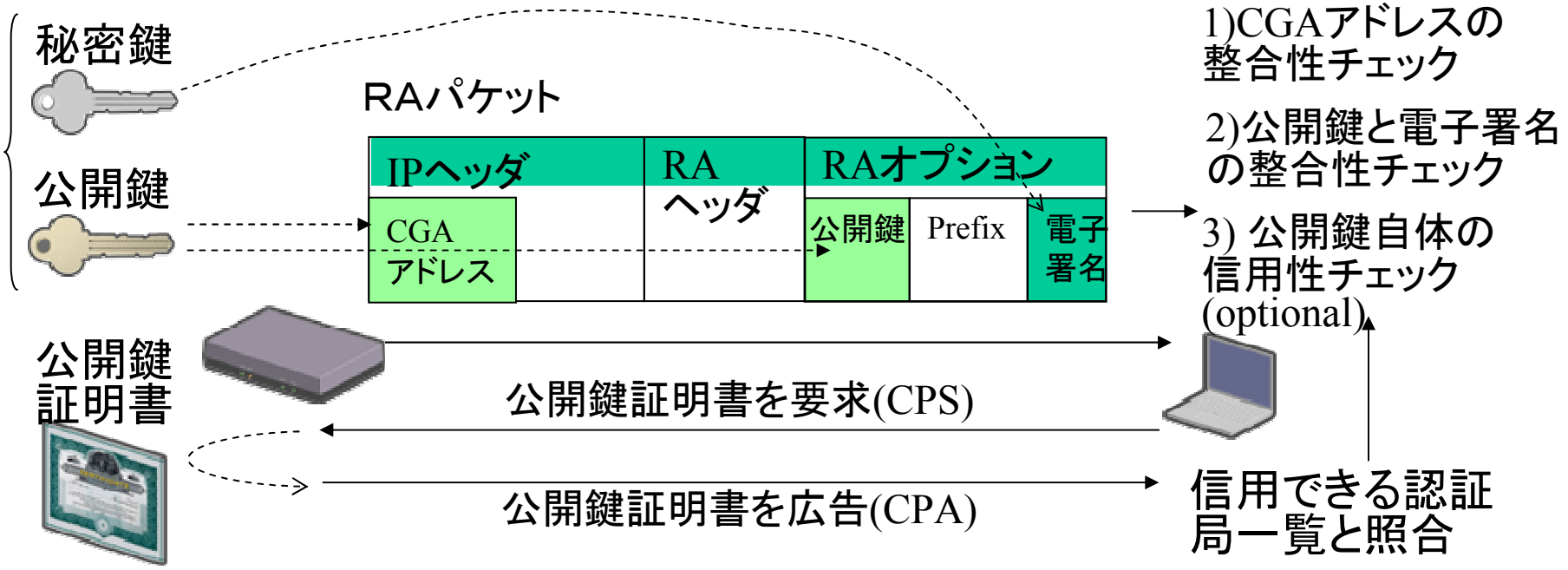


※優先度高のRAで不正RAを流された場合には効果なし（RAの誤送信に対して有効）
※デフォルトゲートウェイの選択ミスは解決できるものの、
ソースアドレスの選択ミスまでは解決できない可能性あり
（「特定ルータからのRAを優先」することで、何を優先できるかは実装依存）

4(3) ②端末側で不正RAを使用しないようにする

ii) SeND(Secure Neighbor Discovery)

・ルータが、RAパケットに認証情報を付加
　　公開鍵 (CGA option)
　　秘密鍵で計算した電子署名 (RSA signature option)
　　ソースアドレスを公開鍵のhashで生成 (CGAアドレス)
・端末が上記を元に、「不整合なRA」を廃棄
・自己署名証明書対策のため、公開鍵証明書を別途取得することも可能
　(SSL同様、端末が「信用できる認証局一覧」事前に持っている前提)



CGA=Cryptographically Generated Address, CPS= Certificate Path Solicitation, CPA= Certificate Path Advertisement

4(3) ②端末側で不正RAを使用しないようにする

ii) SeND (Secure Neighbor Discovery) (cont.)

※SeNDの課題

・まだあまり普及していない

→結局SeND未サポートなルータ・端末を信用せざるを得ない

・全端末・ルータに公開鍵/秘密鍵(+公開鍵証明書)を持たせる必要あり

→普及が困難

・結局「証明書を有すること」しか確認できない

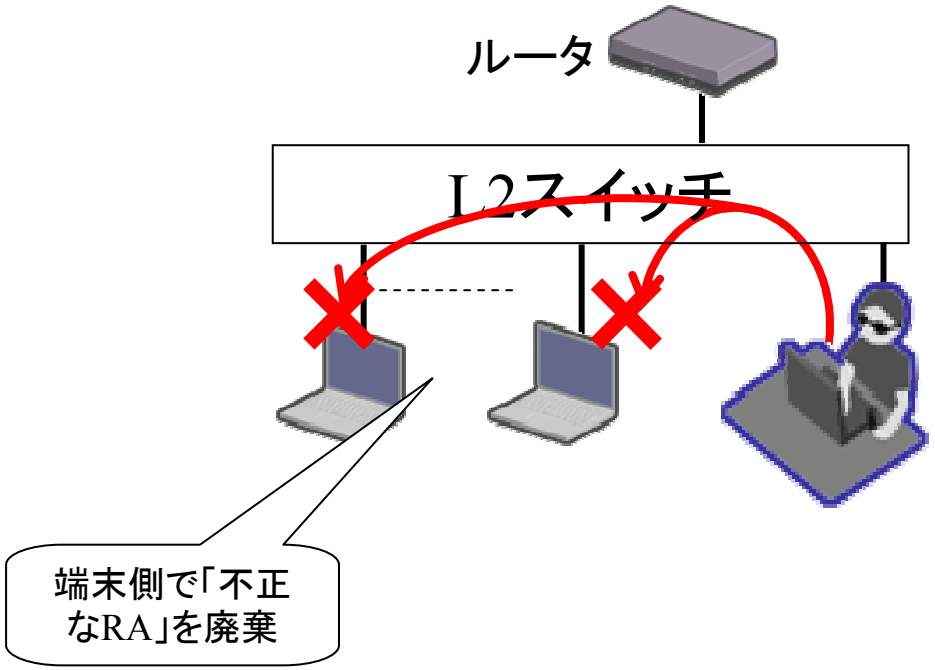
→証明書取得済の端末から異常なRAが流れてきた場合は、防ぎようがない
(送信元を特定する助けにはなるのは、認証局署名の公開鍵証明書がある場合のみだが、公開鍵証明書確認はSeNDではoption)

・仮に普及しても、IPv4の同様な攻撃に対する答えにはならない

・SeND自体に対するDoS攻撃は可能

4(3) ②端末側で不正RAを使用しないようにする

iii) パーソナルファイアウォールでRA廃棄



※端末側で「不正なRA」をどうやって設定すればよいか?
※仮に設定できたとしても、端末起動時にはうまく働かない場合あり
(RS/RAのやりとりが終わった後で、パーソナルファイアウォールが立ち上がる実装もある)

4(4) 各手法の費用対効果の比較（今出来ること）

		ルータアドレス手動設定	RA監視サーバ	①i) IPv6全廃棄	①ii) RA廃棄	①iii) 端末間L2通信廃棄	①iv) 端末をPtoP収容	①v) 端末をトンネル収容	②i) RA優先度設定
費用（装置更新・増設）	端末	なし	なし	なし	なし	なし	なし	ほぼなし	ほぼなし
	網側機器	なし	あり	ほぼなし	あり	あり	ほぼなし	ほぼなし	ほぼなし
効果（IPv4への影響）	既存運用維持	OK	OK	OK	OK	一部NG（いい意味でも悪い意味でも）		OK	OK
	アドレス枯渇対策	変化 なし	変化なし	IPv6導入不可	変化なし	変化なし	IPv4アドレス消費増	変化なし	変化なし
効果（攻撃耐性）	悪意あるユーザのRA	OK	OK	OK	OK	OK	OK	OK	NG
	Unicast RA	NG	NG	OK	OK	OK	OK	OK	NG
	RA以外のNDP詐称	NG	NG	OK	NG	OK	OK	OK	NG
	セキュリティ対策自体	OK	OK	OK	OK	OK	OK	トンネル依存	OK

条件付きで有効な技術

不正RA対策とは独立に、講じておいてよい技術

4(4) 各手法の費用対効果の比較(将来技術)

それなりの効果はあるものの、まだ技術課題も多い (そのため、標準化未完了/普及がまだ不十分)

		DHCPv6のみでアドレス生成	SAVI	②ii) SeND	②iii)パーソナルファイアウォール
費用(装置更新・増設)	端末	かなりあり(DHCPv6対応, RA無効化)	なし	かなりあり(SeND対応)	かなりあり(RAフィルタ対応パーソナルファイアウォール)
	網側機器	あり(DHCPv6サーバ)	かなりあり(SAVI対応スイッチ)	あり(SeND対応ルータ)	あり(ポリシー配布サーバ)
効果(IPv4への影響)	既存運用維持	OK	OK	OK	OK
	セキュリティ改善	特になし	あり	特になし	あり
	アドレス枯渇対策	変化なし	変化なし	変化なし	変化なし
技術課題	「不正」の定義が変わる	不正DHCPv6対策	「不正なRA」の定義	SeND対応端末からの不正RA対策が必要	「不正なRA」の定義 「不正なポリシー配布」の対策
	運用手順	端末でのDHCPv6起動契機	–	全端末・ルータへの公開鍵/秘密鍵インストール	信頼できるポリシー配布方式(鶏卵問題)
	DoS	–	考慮要	考慮要	–

4(5) まとめ

・不正RA対策とは独立に、下記のルータ設定はお勧め（費用低＆効果あり＆副作用なし）
- Routerのリンクローカルアドレスをわかりやすい値に手動設定
- Router優先度の設定

・お勧めの不正RA対策は、「どこを割り切れるか」次第で決まってくる
- 不正RAを検出できれば十分、と割り切れる
  →RA監視サーバ導入
- IPv6の出番は今後一切ない、と割り切れる
  →IPv6全廃棄
- IPv6はトンネル経由で導入できれば十分、と割り切れる
  →IPv6全廃棄+IPv6トンネル収容
- IPv6導入を機に端末収容スイッチを更新する、と割り切れる
  →RA廃棄 or 端末間L2通信廃棄
- IPv6導入を機にIPv4端末収容方式を見直す、と割り切れる
  →端末をPoint-to-Point収容