ホスティングサービスにおける ARP Spoofing対策

さくらインターネット(株)
技術部　大久保修一
ohkubo@sakura.ad.jp

今日のAgenda

- はじめに
- ARP Spoofingとは？
- ARP Spoofingの発生事例
- ARP Spoofingの検出システム
- ARP Spoofingの防止策
- まとめ

はじめに

- 2008/6/1～6/2にかけて、弊社サービス「専用サーバ10Mスタンダード」の一部においてARP Spoofingによる通信障害が発生しました。
- 大変ご迷惑をおかけいたしました m(__)m

- 障害情報は下記に掲載されています。
  - http://support.sakura.ad.jp/page/news/20080602-001.news

- 雑誌にもARP Spoofingに関する記事が掲載されました。
  - 日経コンピュータ6/15号
  - 日経ネットワーク8月号

- ※障害の詳細は、本セッションの中で解説いたします。

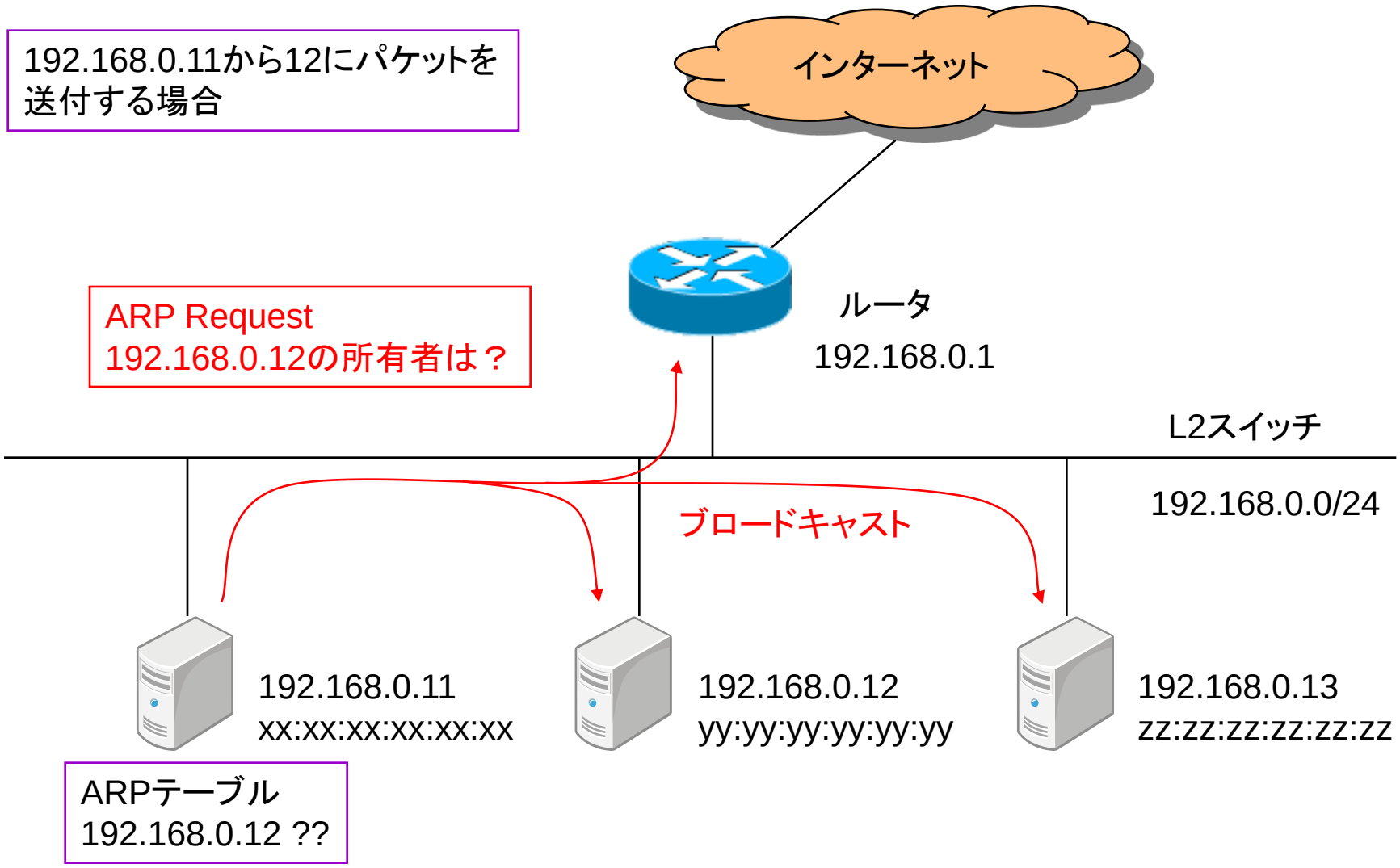
ARP Spoofingとは？

- ARP解決におけるIPアドレスの詐称
- 自分に割り当てられていないIPアドレス宛のARP Requestに応答(ARP Reply)する。
- プロトコル的には、、、

  ARP Request、もしくはARP ReplyのSender IP Addressフィールドに、自分に割り当てられていないIPアドレスをセットしたARPパケットを送信すること。
- 他ホスト宛の通信を乗っ取り、通信の傍受、改ざんがなされる可能性がある。

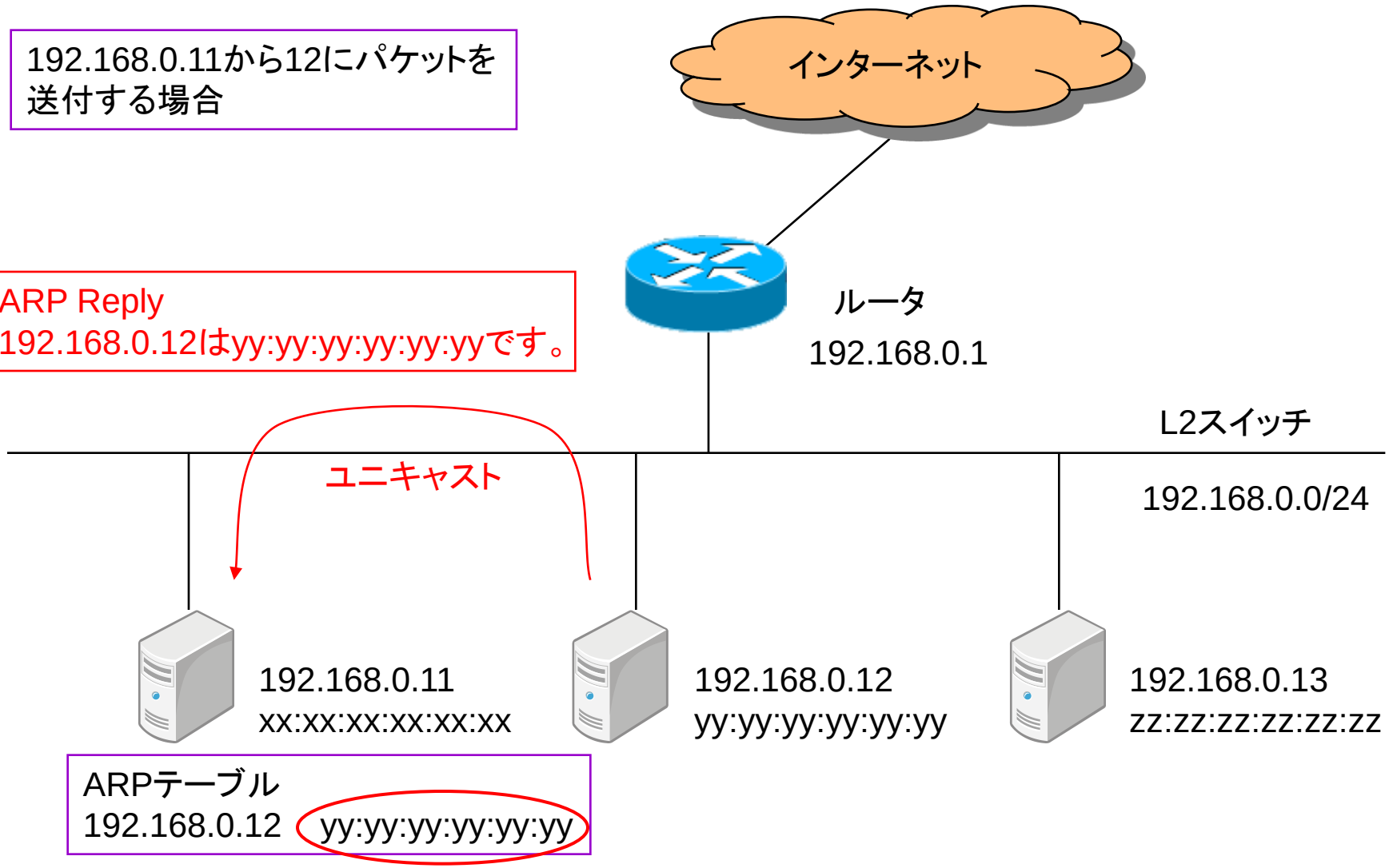
ARPの動作について

192.168.0.11から12にパケットを送付する場合



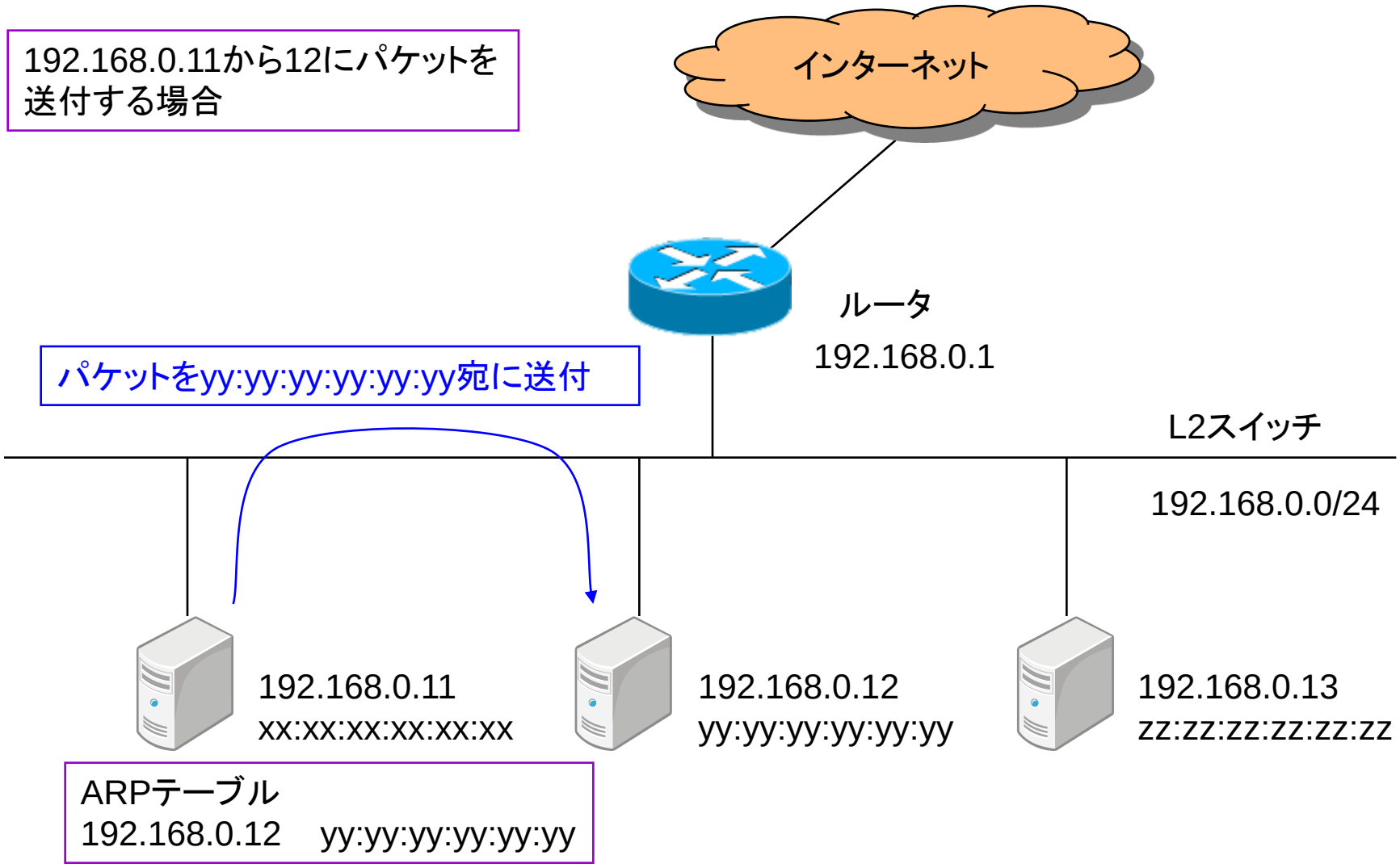
ARPの動作について

192.168.0.11から12にパケットを送付する場合



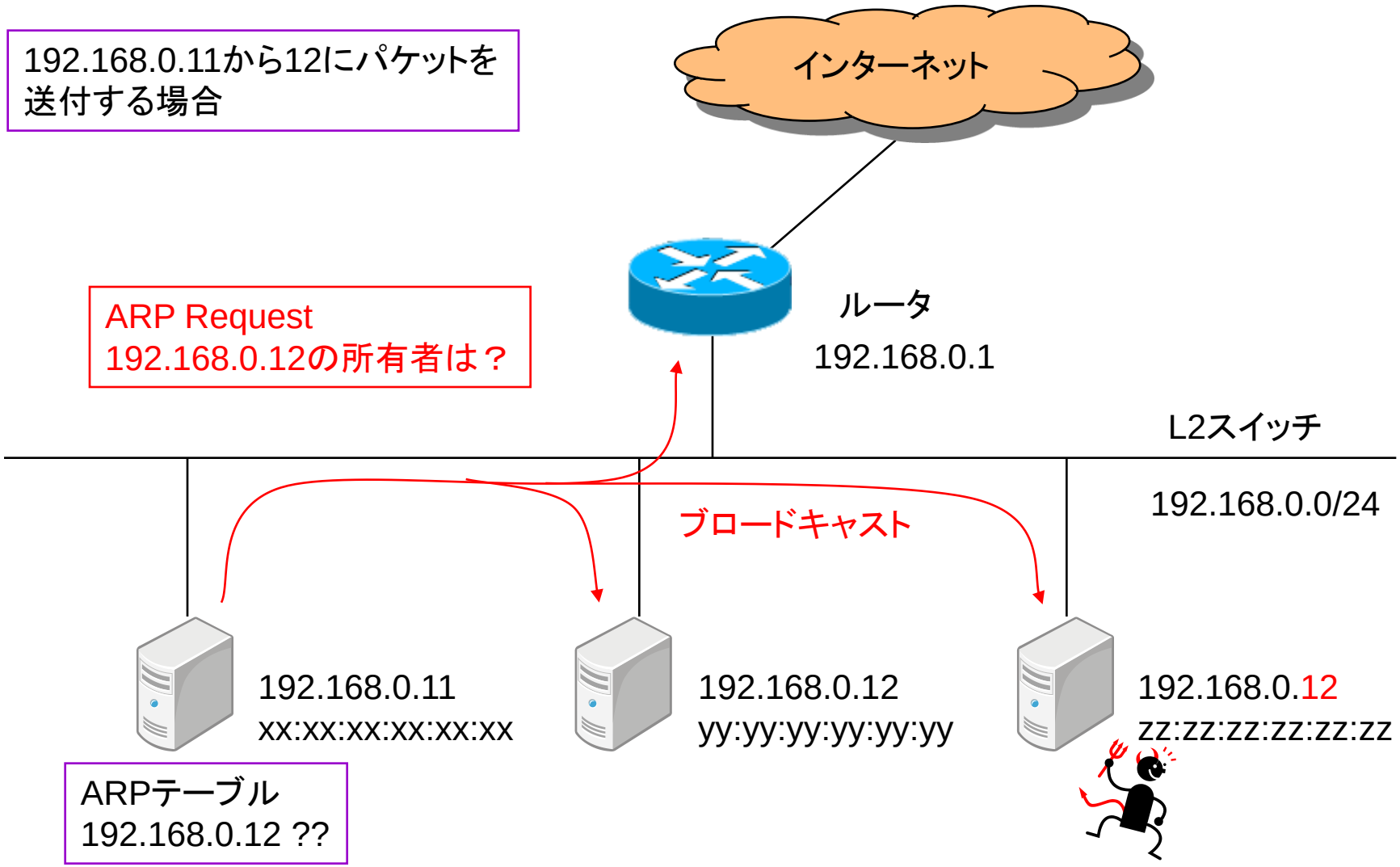
ARPの動作について

192.168.0.11から12にパケットを送付する場合



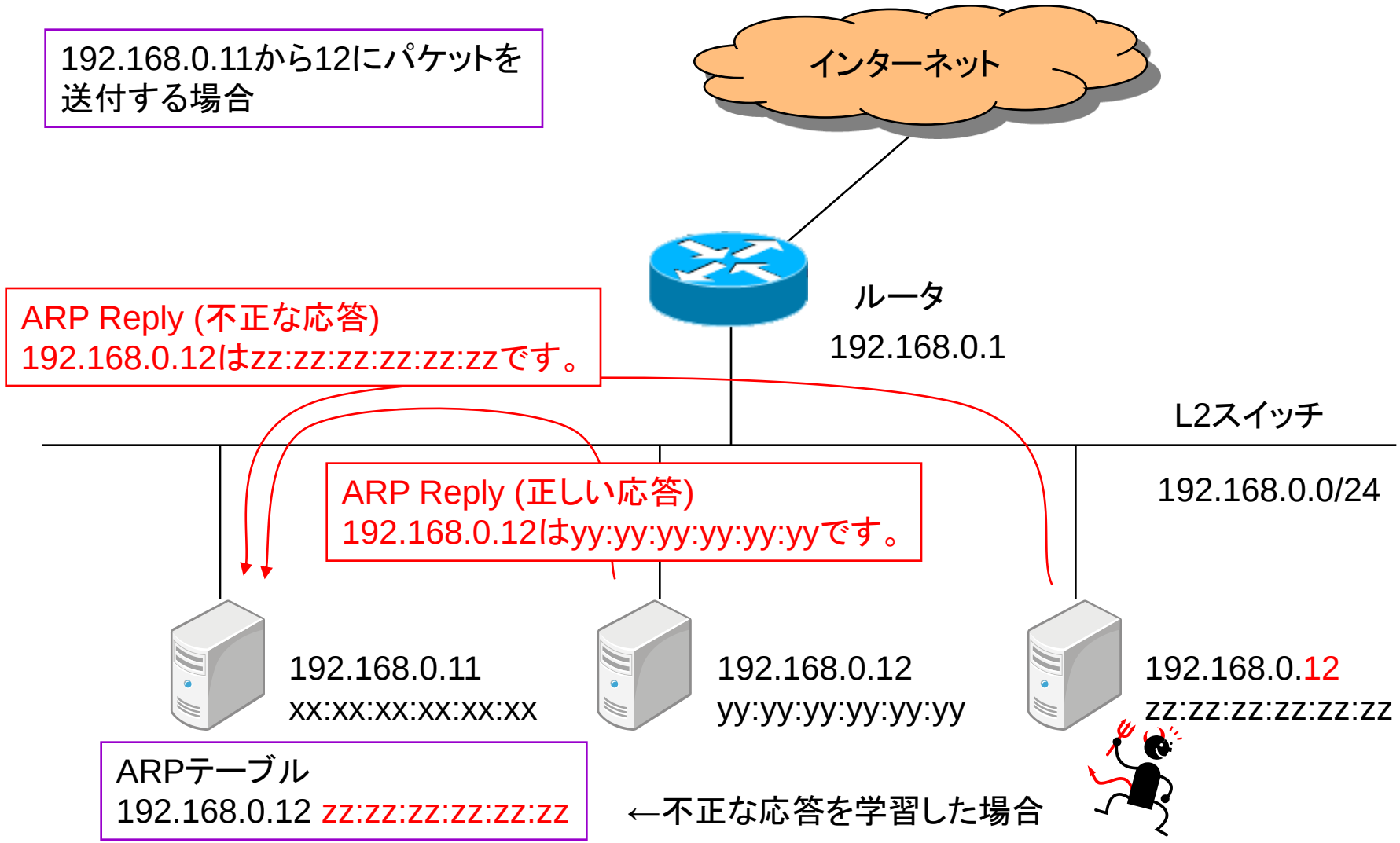
ARP Spoofing発生時

192.168.0.11から12にパケットを送付する場合



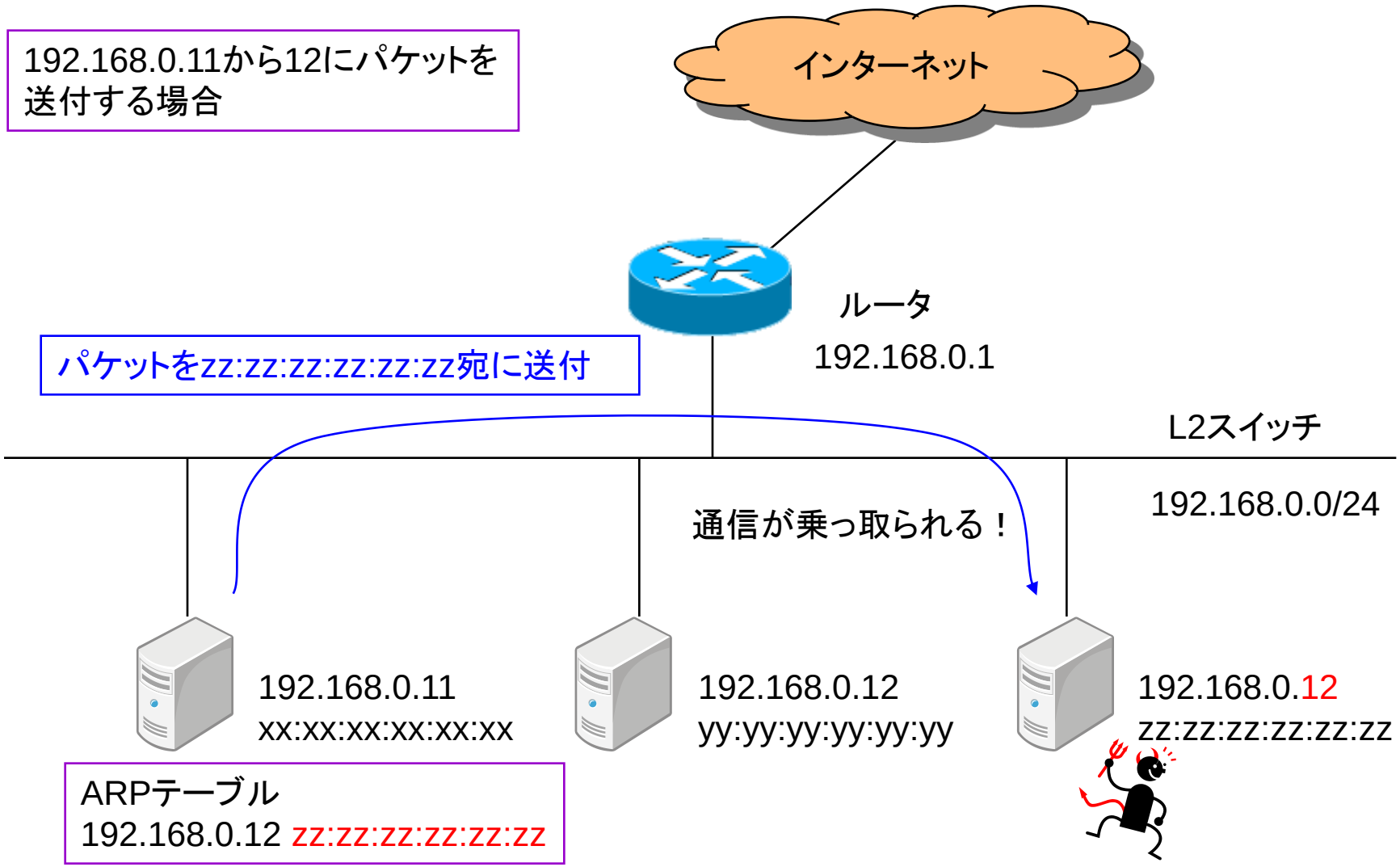
ARP Spoofing発生時

192.168.0.11から12にパケットを送付する場合



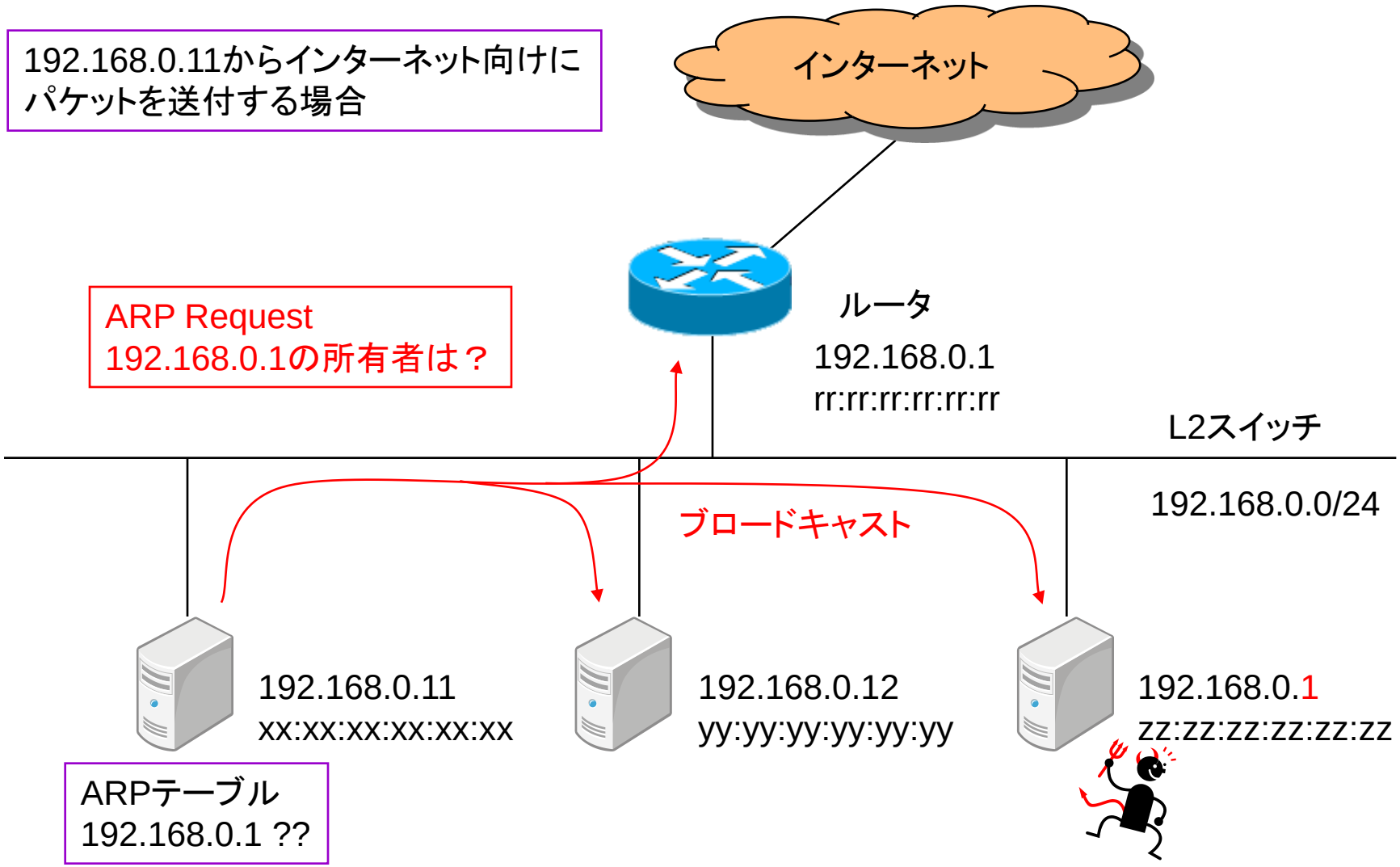
ARP Spoofing発生時

192.168.0.11から12にパケットを送付する場合



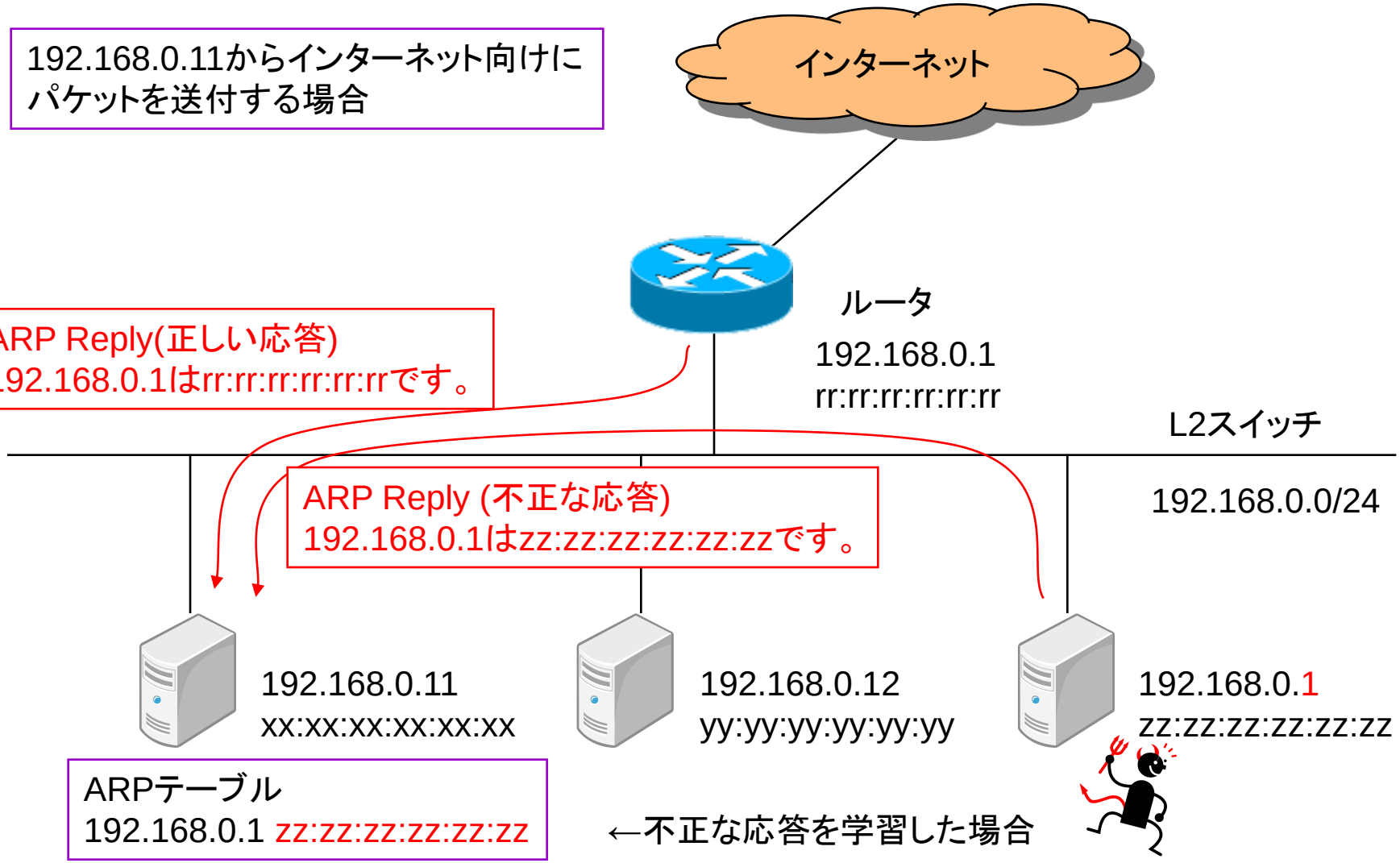
インターネット向け通信の場合

192.168.0.11からインターネット向けにパケットを送付する場合



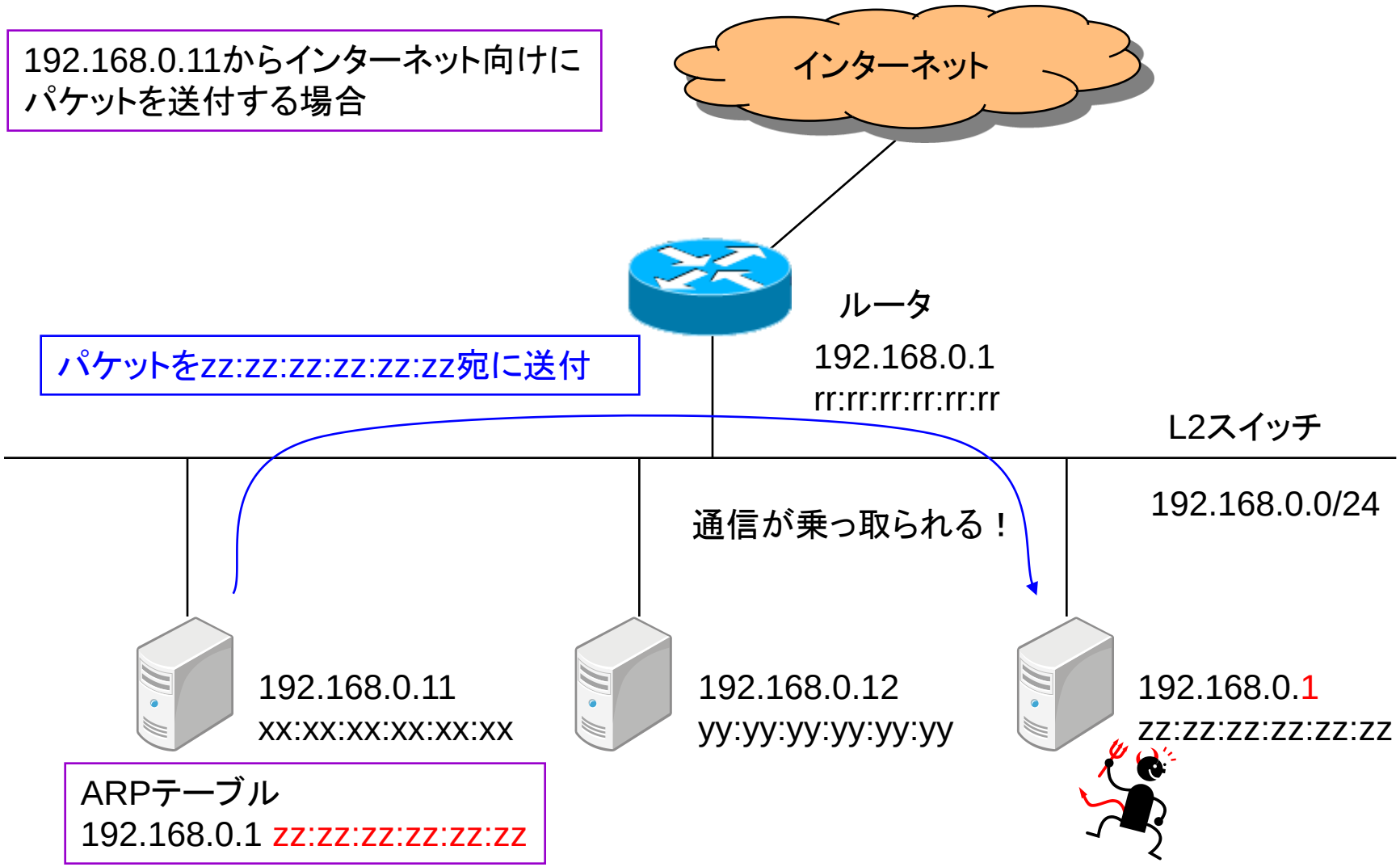
インターネット向け通信の場合

192.168.0.11からインターネット向けにパケットを送付する場合



インターネット向け通信の場合

192.168.0.11からインターネット向けに
パケットを送付する場合



弊社サービス別のARPスプーフィング影響度合

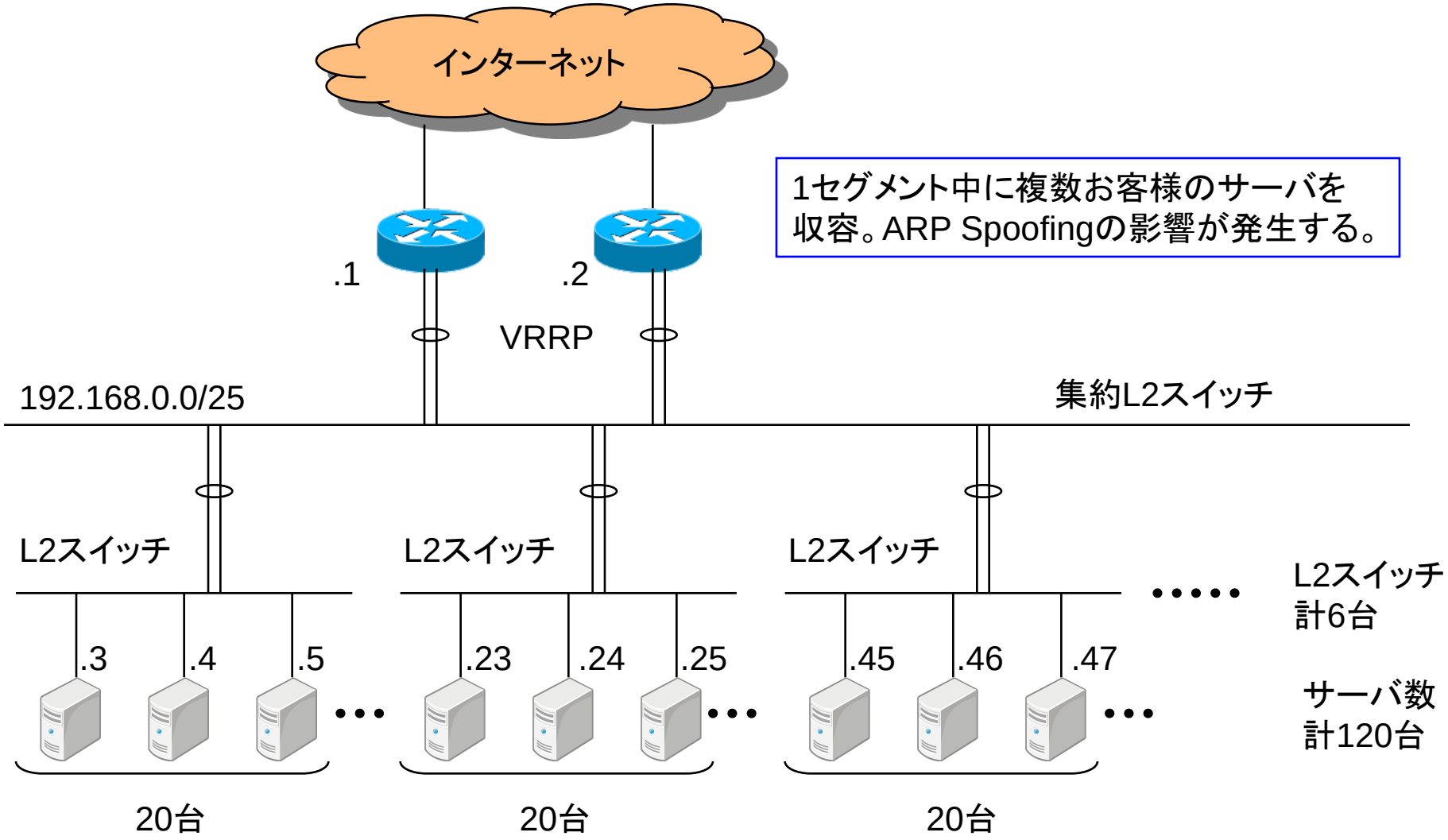
- 専用サーバ
  - お客様にサーバのroot権限を渡すため、設定ミスなどによるARP Spoofing発生の可能性がありえる。
  - サーバがクラックされてARP Spoofingが発生するケースもある。

ARP Spoofing発生時の他社お客様への影響

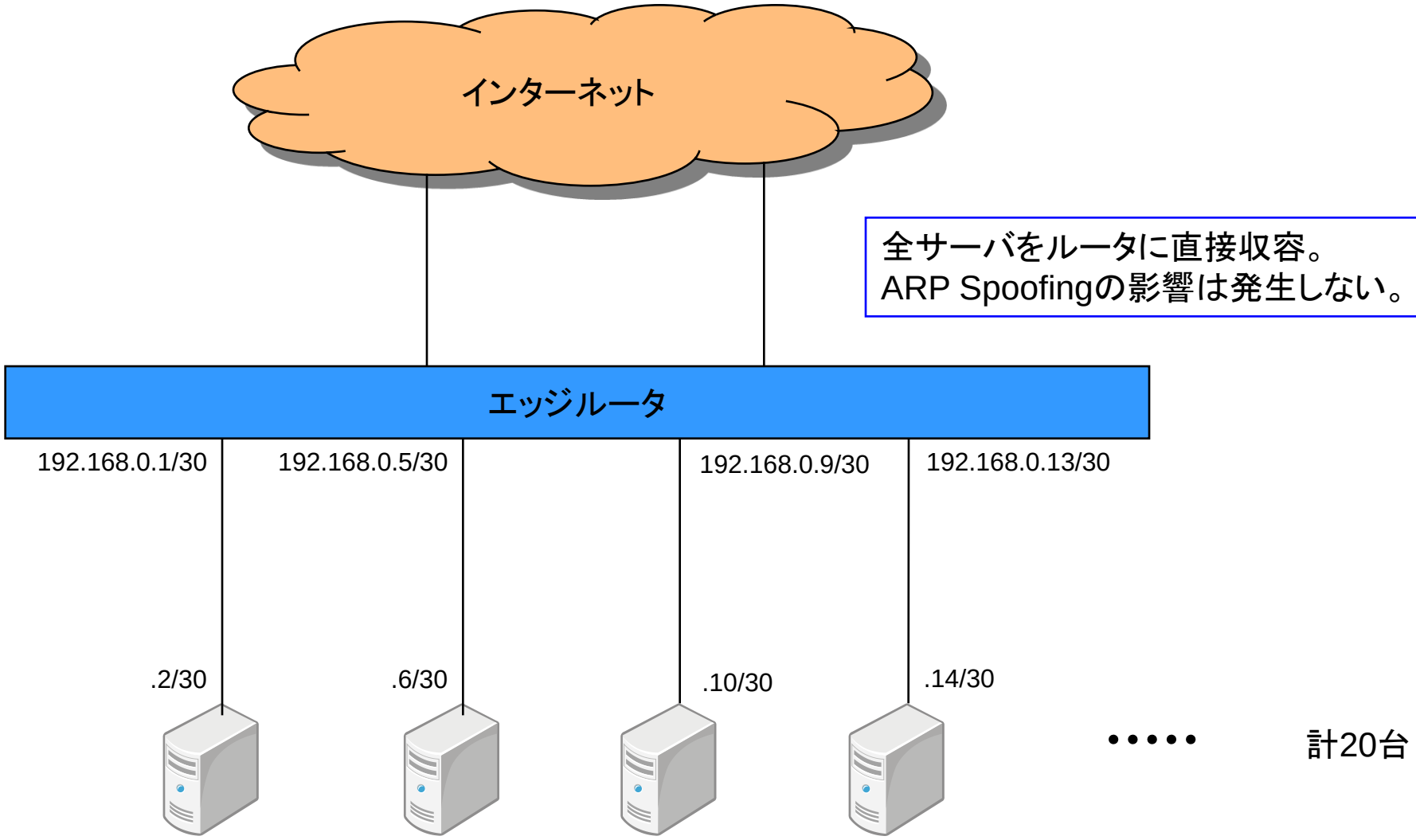
回線帯域	帯域共有	帯域保証
10M	影響あり	影響あり
100M	影響あり	影響なし
1000M	影響なし	N/A

※サービスのご提供時期によりサーバの収容構成が異なる場合がありますので、構成の詳細は弊社カスタマーセンターにお問い合わせください。

専用サーバサービス(10M帯域共有の例)



専用サーバサービス(100M帯域保証の例)



弊社サービス別のARPスプーフィング影響度合

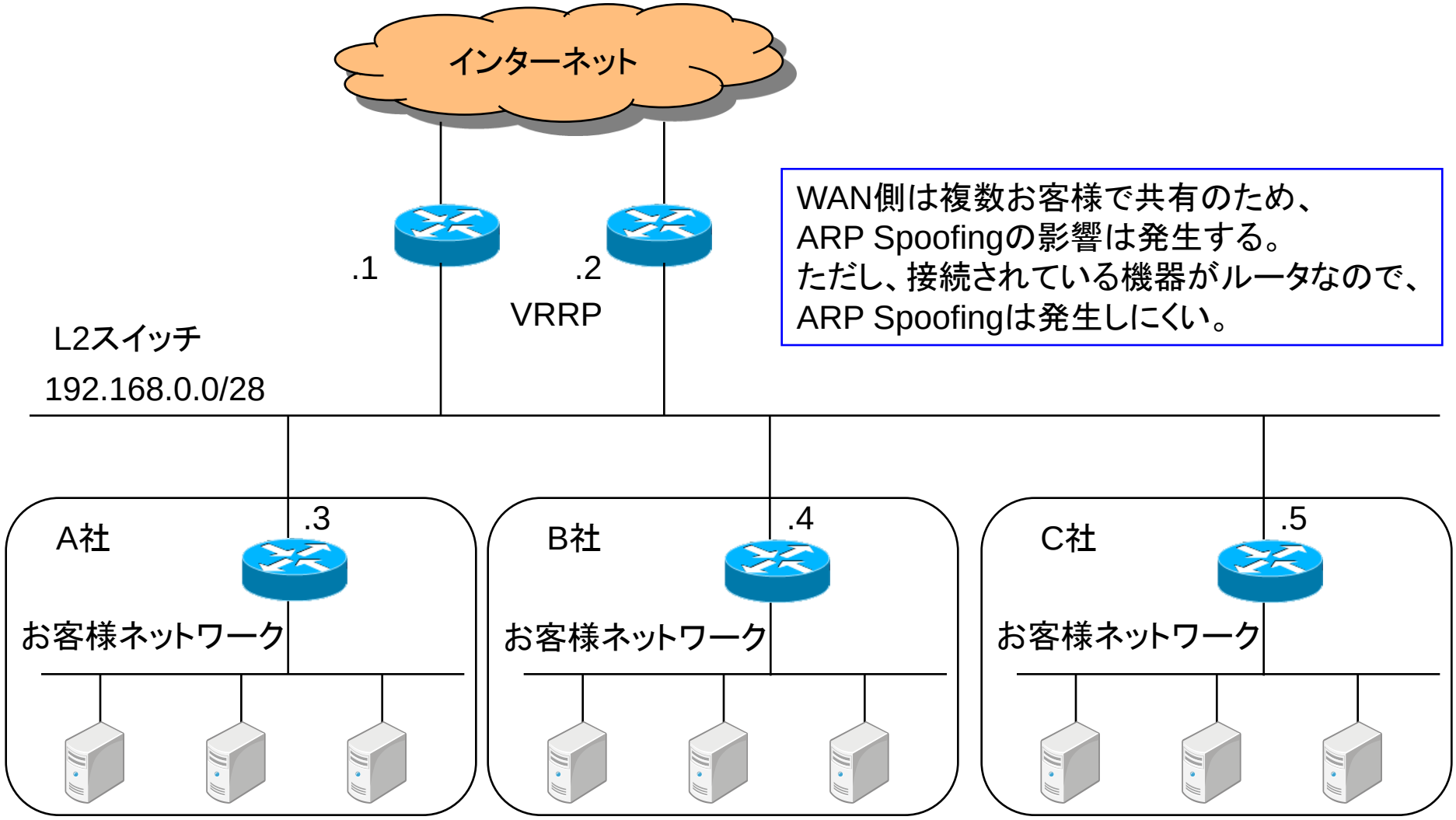
- ハウジング
  - WAN側セグメントをお客様ごとに分離するメニューでは、影響なし。
  - WAN側セグメントを複数のお客様で共有するメニューでは、影響あり。
  - 共有セグメントでもルータ接続を前提としているため、クラッキングによるARP Spoofing発生度合いも低い。

ARP Spoofing発生時の他社お客様への影響

回線帯域	帯域共有	帯域保証
10M	影響あり	影響なし
100M	影響あり	影響なし
1000M	影響なし	影響なし

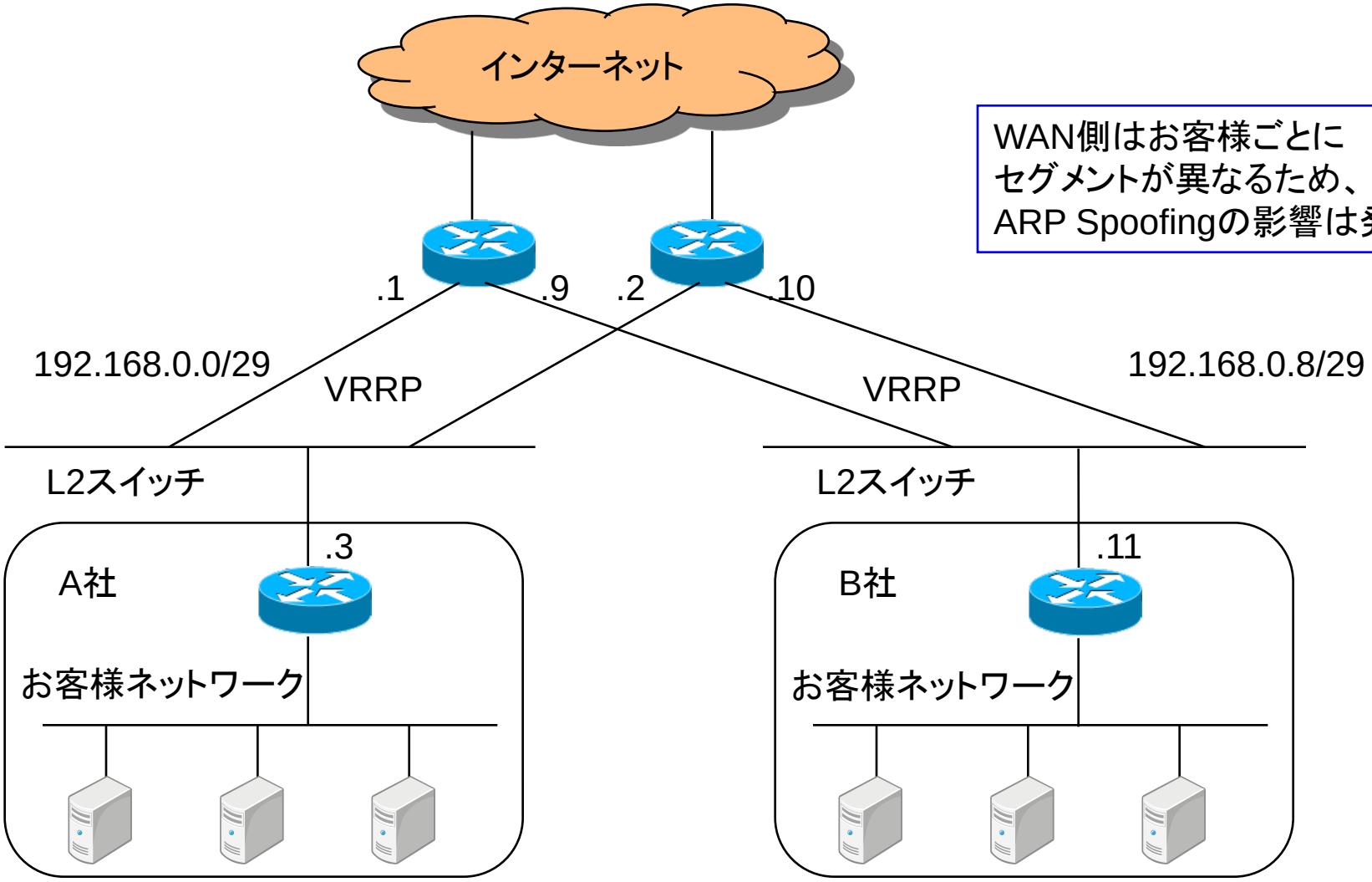
※サービスのご提供時期によりサーバの収容構成が異なる場合がありますので、構成の詳細は弊社カスタマーセンターにお問い合わせください。

ハウジング(10M/100M帯域共有型の例)



WAN側は複数お客様で共有のため、
ARP Spoofingの影響は発生する。
ただし、接続されている機器がルータなので、
ARP Spoofingは発生しにくい。

ハウジング(10M/100M帯域保証型の例)



WAN側はお客様ごとに
セグメントが異なるため、
ARP Spoofingの影響は発生しない

ARP Spoofing発生事例

- ケース1
  - 専用サーバにて、セグメント内の未使用IPアドレスを無断で利用。
  - 予備で確保しているIPアドレスや、解約サーバのIPアドレスを網羅的に使用。
  - 実害が無いので、気づきにくい。
  - お客様が意図的にやっているケースがあり、連絡して元に戻していただく。
- ケース2
  - 専用サーバにて、他の特定お客様のIPアドレスを乗っ取る。
  - 被害者から通信ができないと申告あり。
  - 加害者のサーバがクラックされていた。
  - OSの再インストールを実施。
- ケース3
  - 専用サーバにて、セグメント内の全IPアドレスを乗っ取る。
  - 影響範囲はセグメント全体に波及する。

ARP Spoofing発生事例

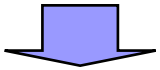
ケース3：セグメント内の全IPアドレスを乗っ取られた場合の
ルータのARPテーブル

```
#sho arp mac-a [redacted] a3ef
      IP Address              MAC Address          Type        Age       Port
1     [redacted] 3            [redacted] a3ef      Dynamic     7         5-6
2     [redacted] 4            [redacted] a3ef      Dynamic     5         5-6
3     [redacted] 5            [redacted] a3ef      Dynamic     2         5-6
4     [redacted] 10           [redacted] a3ef      Dynamic     2         5-6
5     [redacted] 13           [redacted] a3ef      Dynamic     2         5-6
6     [redacted] 15           [redacted] a3ef      Dynamic     2         5-6
7     [redacted] 16           [redacted] a3ef      Dynamic     2         5-6
8     [redacted] 17           [redacted] a3ef      Dynamic     2         5-6
9     [redacted] 19           [redacted] a3ef      Dynamic     2         5-6
10    [redacted] 21           [redacted] a3ef      Dynamic     6         5-6
11    [redacted] 23           [redacted] a3ef      Dynamic     2         5-6
12    [redacted] 24           [redacted] a3ef      Dynamic     3         5-6
```

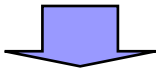
1台のサーバが大量のIPアドレスを利用

ARP Spoofing検出と対処方法

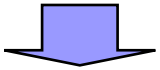
- 全エッジルータのARPテーブルを監視



- 下記の場合を不正とみなす。
  - 1つのMACアドレスで複数のIPアドレスが見えている場合。(専用サーバの場合)
  - 複数のIPアドレスのMACアドレスが一度に変化した場合 。(全サービス共通)



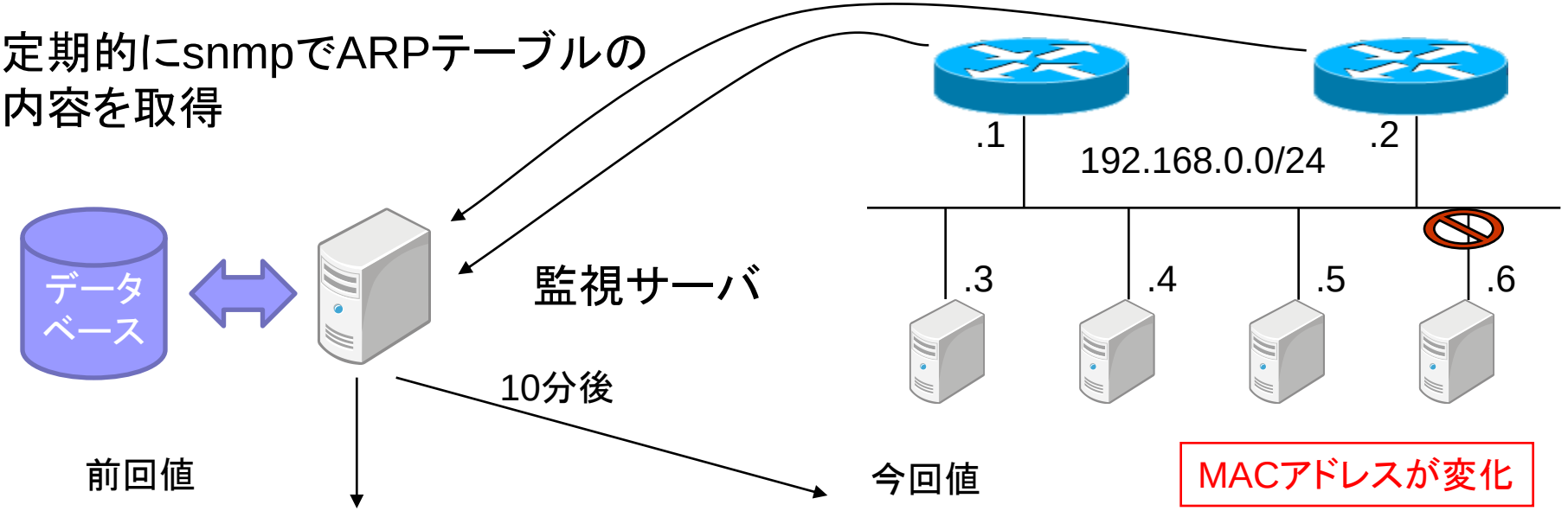
- データベースにて加害者の元IPアドレスを検索し、接続スイッチとポート番号を割り出す。



- 回線の抜去、もしくはポートのシャットダウンにてサーバの切り離しを行う。

ARP Spoofing検出システム

定期的にsnmpでARPテーブルの
内容を取得



前回値

IPアドレス	MACアドレス
192.168.0.3	aa:aa:aa:aa:aa:aa
192.168.0.4	bb:bb:bb:bb:bb:
192.168.0.5	cc:cc:cc:cc:cc:
192.168.0.6	dd:dd:dd:dd:dd:dd

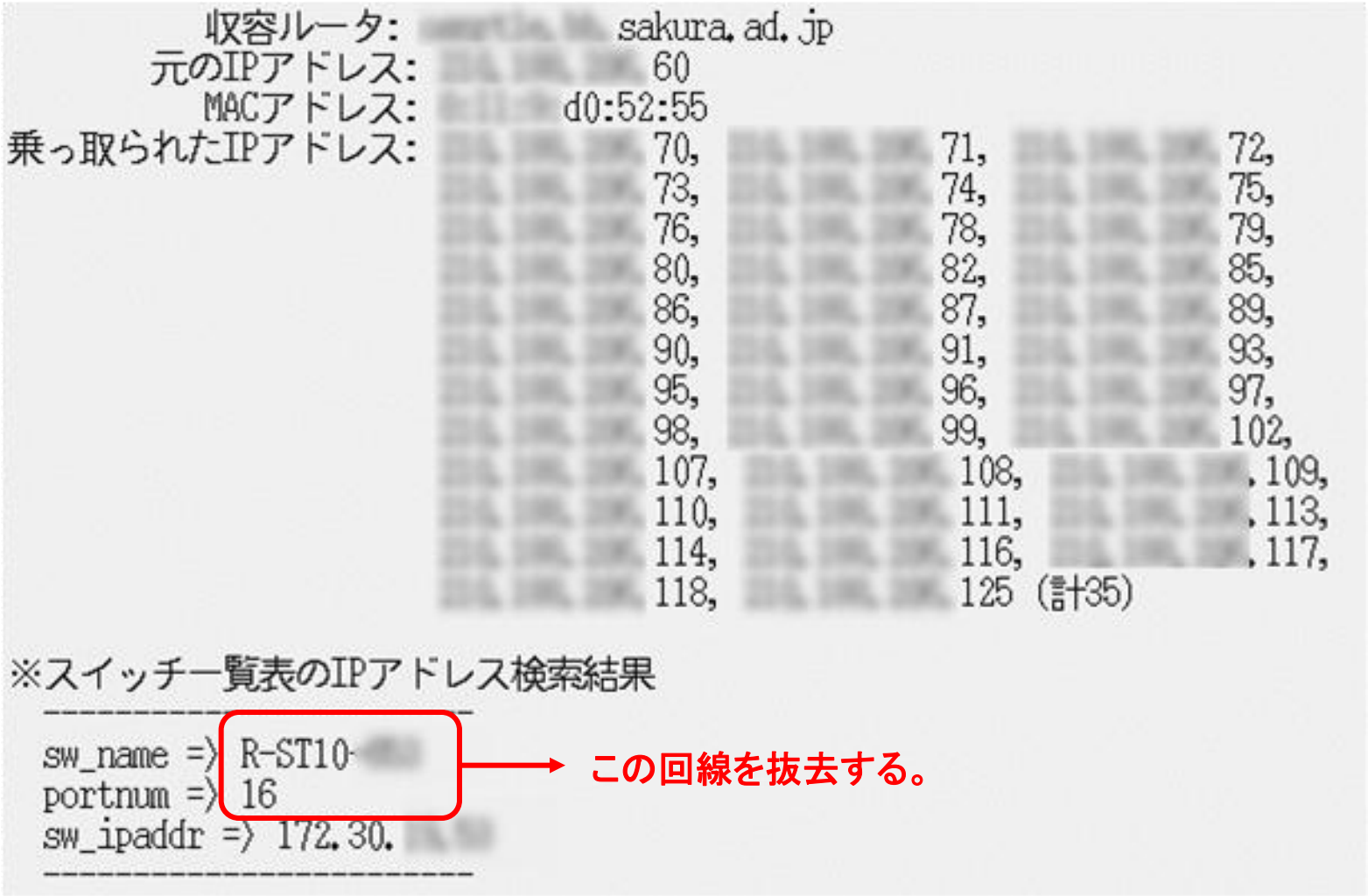
今回値

MACアドレスが変化

IPアドレス	MACアドレス
192.168.0.3	dd:dd:dd:dd:dd:dd
2.168.0.4	dd:dd:dd:dd:dd:dd
2.168.0.5	dd:dd:dd:dd:dd:dd
192.168.0.6	dd:dd:dd:dd:dd:dd

前回値より元の
IPアドレスを検索

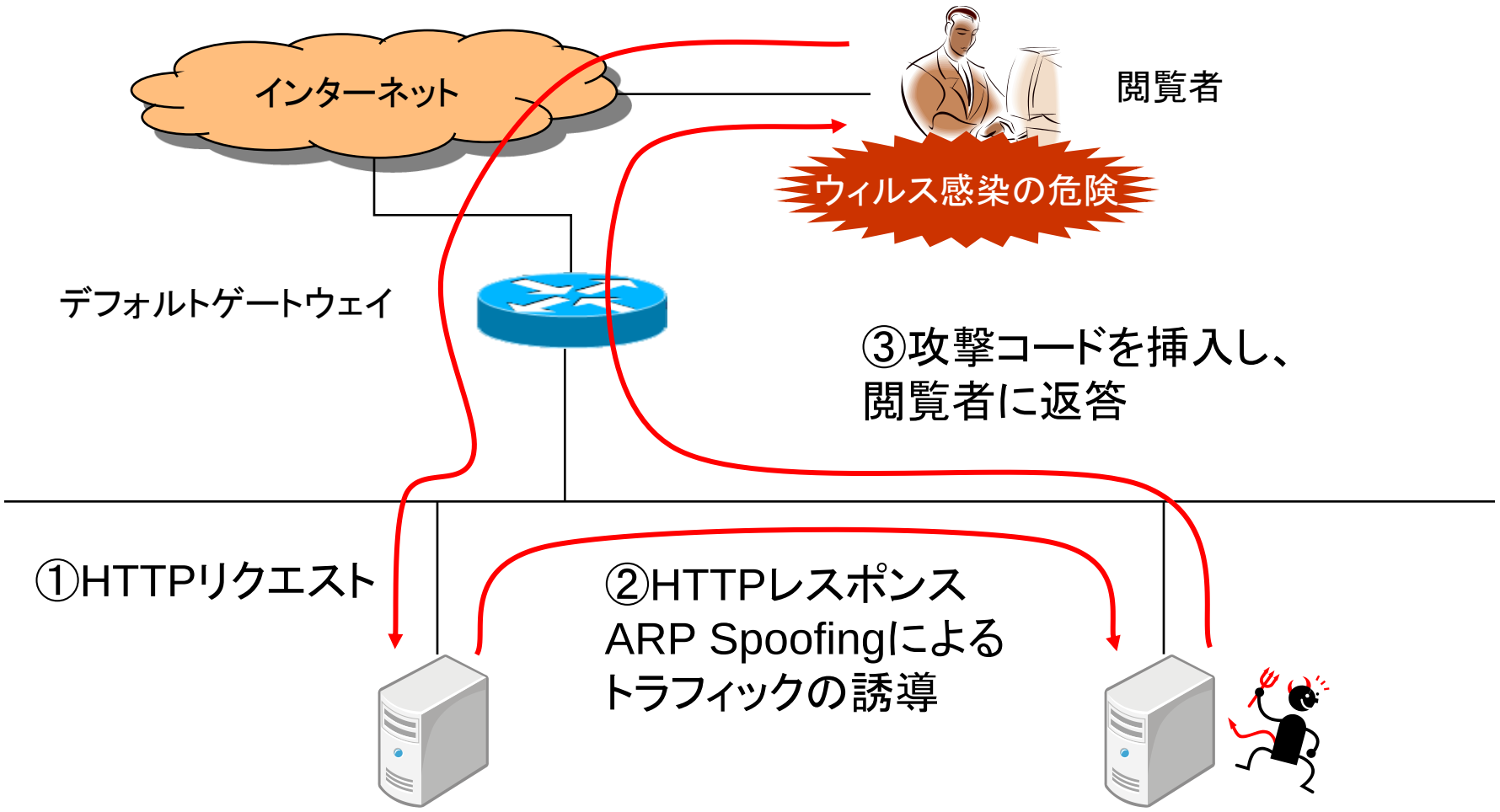
ARP Spoofing検出例



ARP Spoofing発生事例(ケース4)

- ケース4(2008/6/1～6/2に発生した事例)
  - デフォルトゲートウェイのIPアドレスを乗っ取る。
    - 同セグメント内のサーバからインターネット向け通信を横取り。
  - さらにHTTPトラフィックを改竄して、Webの閲覧者に返答。
    - <iframe>タグを使った攻撃コードを挿入。
    - 閲覧者にてウイルス対策がなされていない場合、ウイルス感染など被害を受けた可能性があった。

ARP Spoofing発生事例(ケース4)



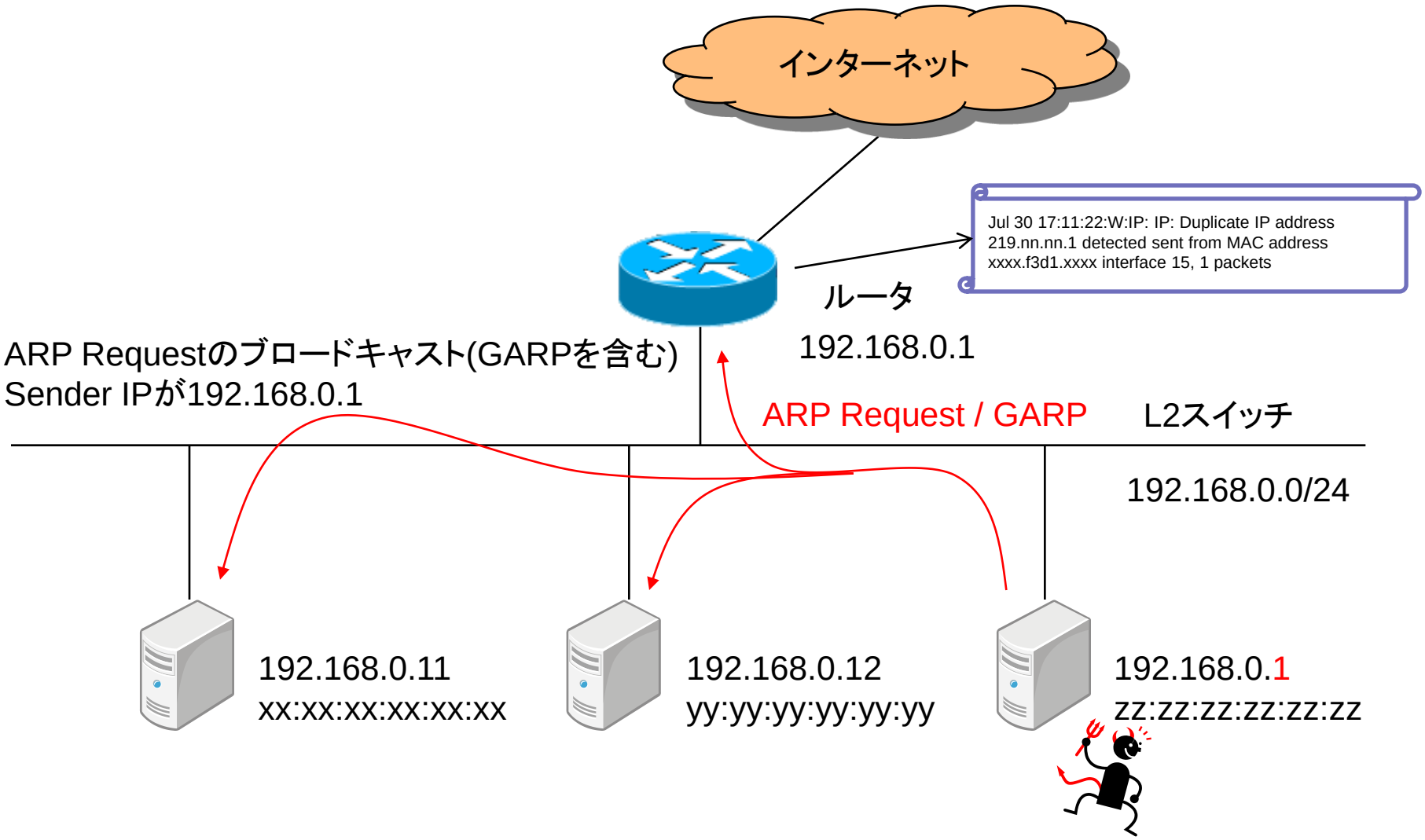
検出方法

- ルータのログを監視

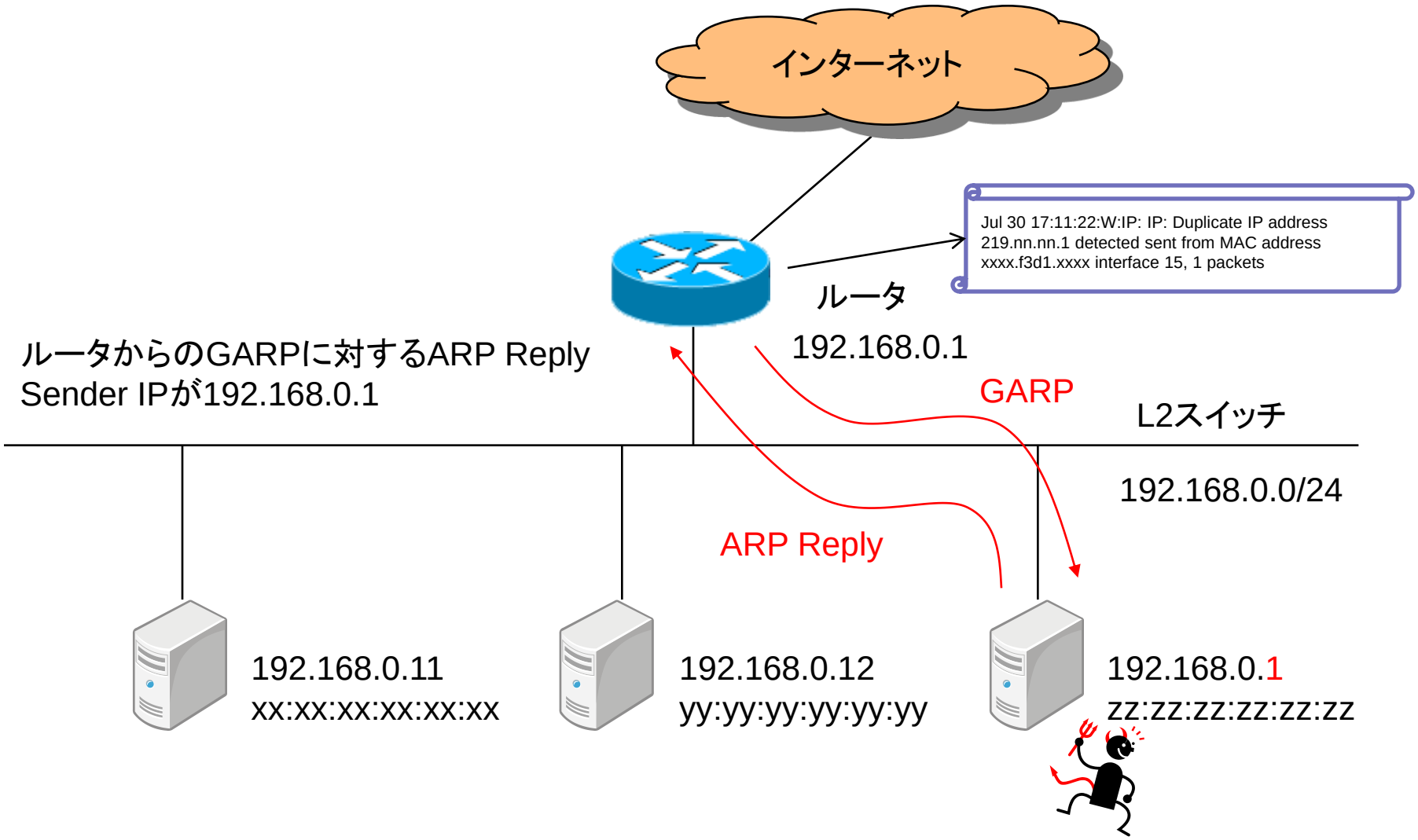
> Jul 30 17:11:22:W:IP: IP: Duplicate IP address 219.nn.nn.1 detected sent from MAC address xxxx.f3d1.xxxx interface 15, 1 packets

- ただし、ルータにARP Request(GARP)、もしくはARP Replyが届いた場合のみ。
- ルータにARPパケットが届かないと、ログが記録されない。

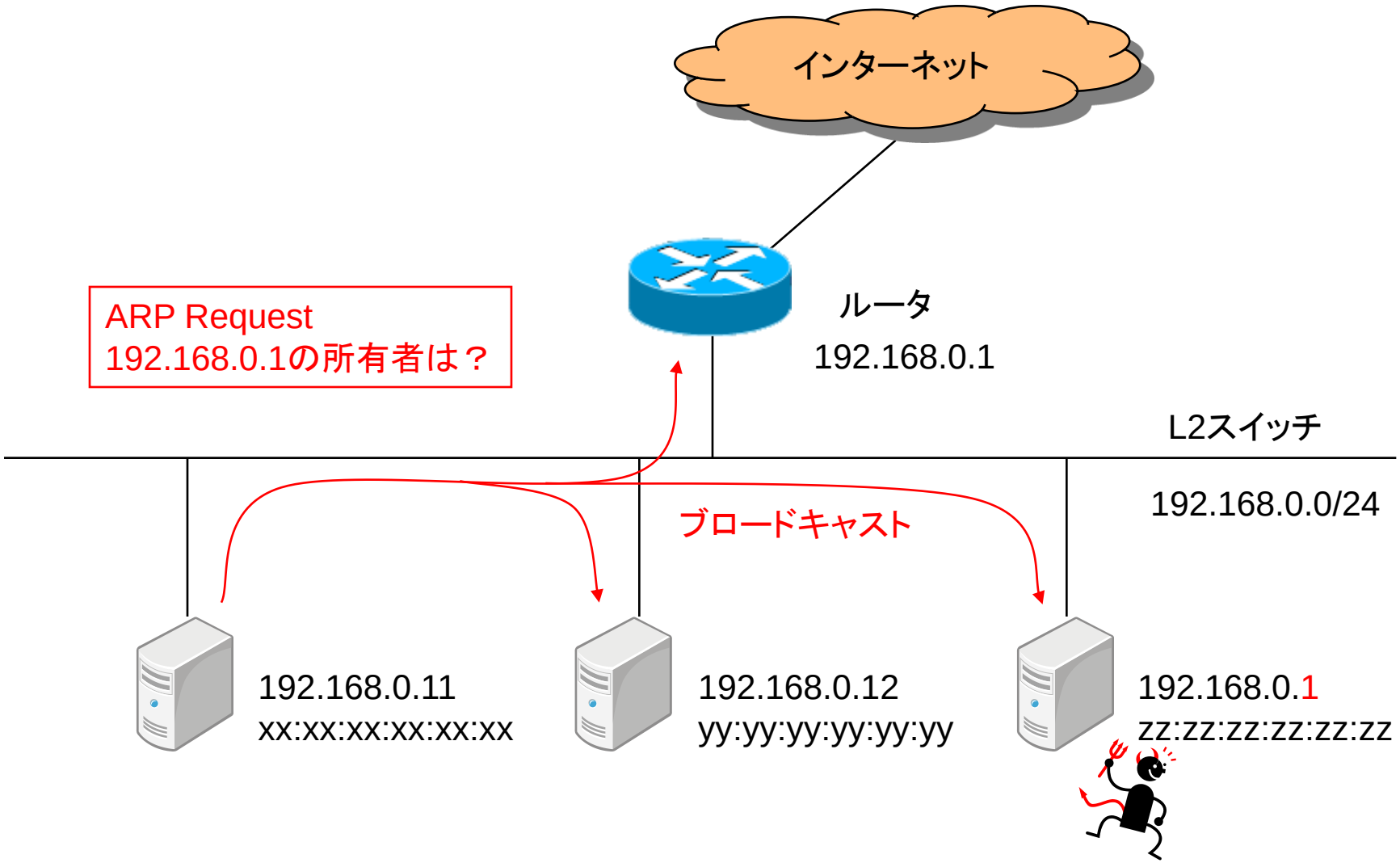
IPアドレス重複のログが出力されるケース



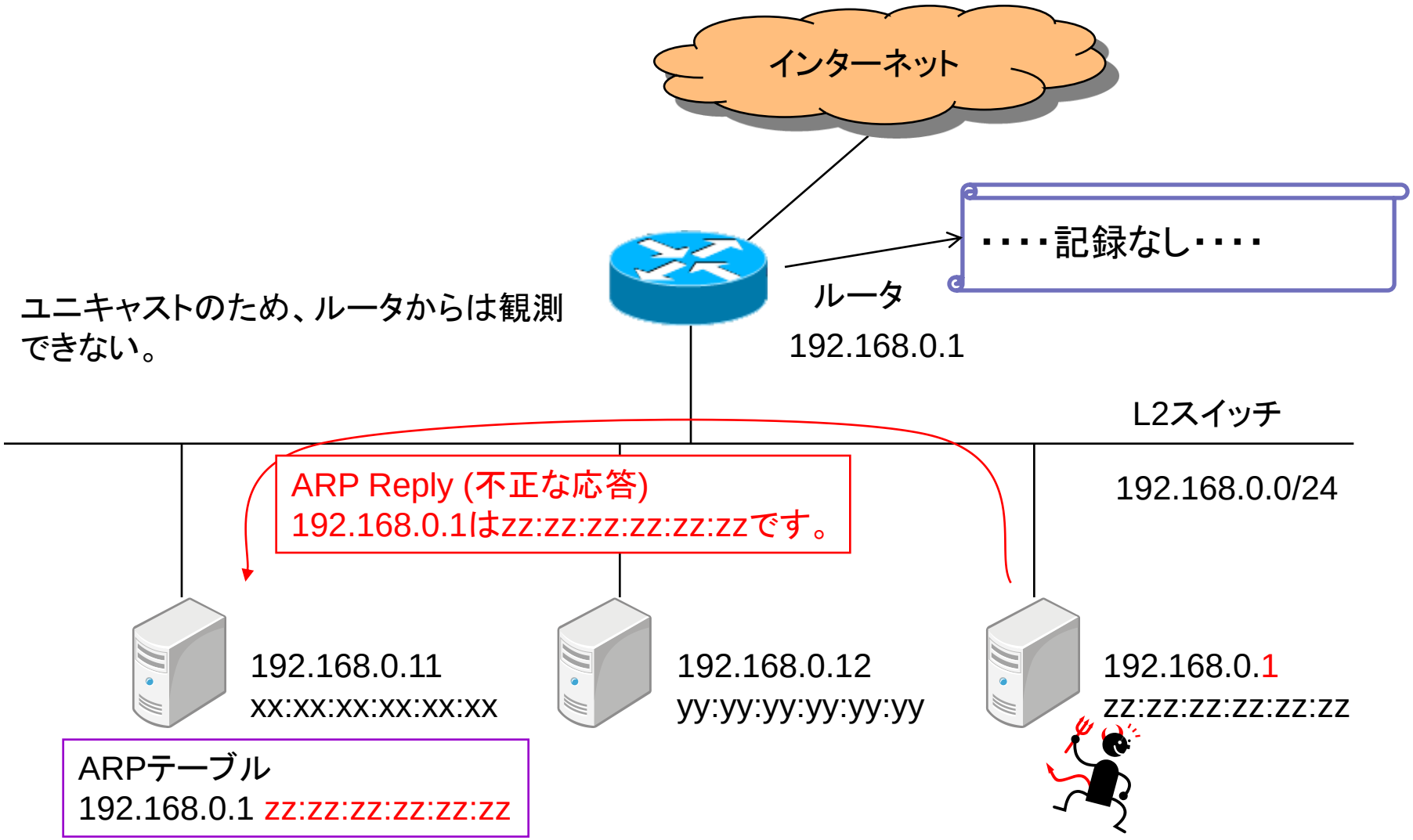
IPアドレス重複のログが出力されるケース



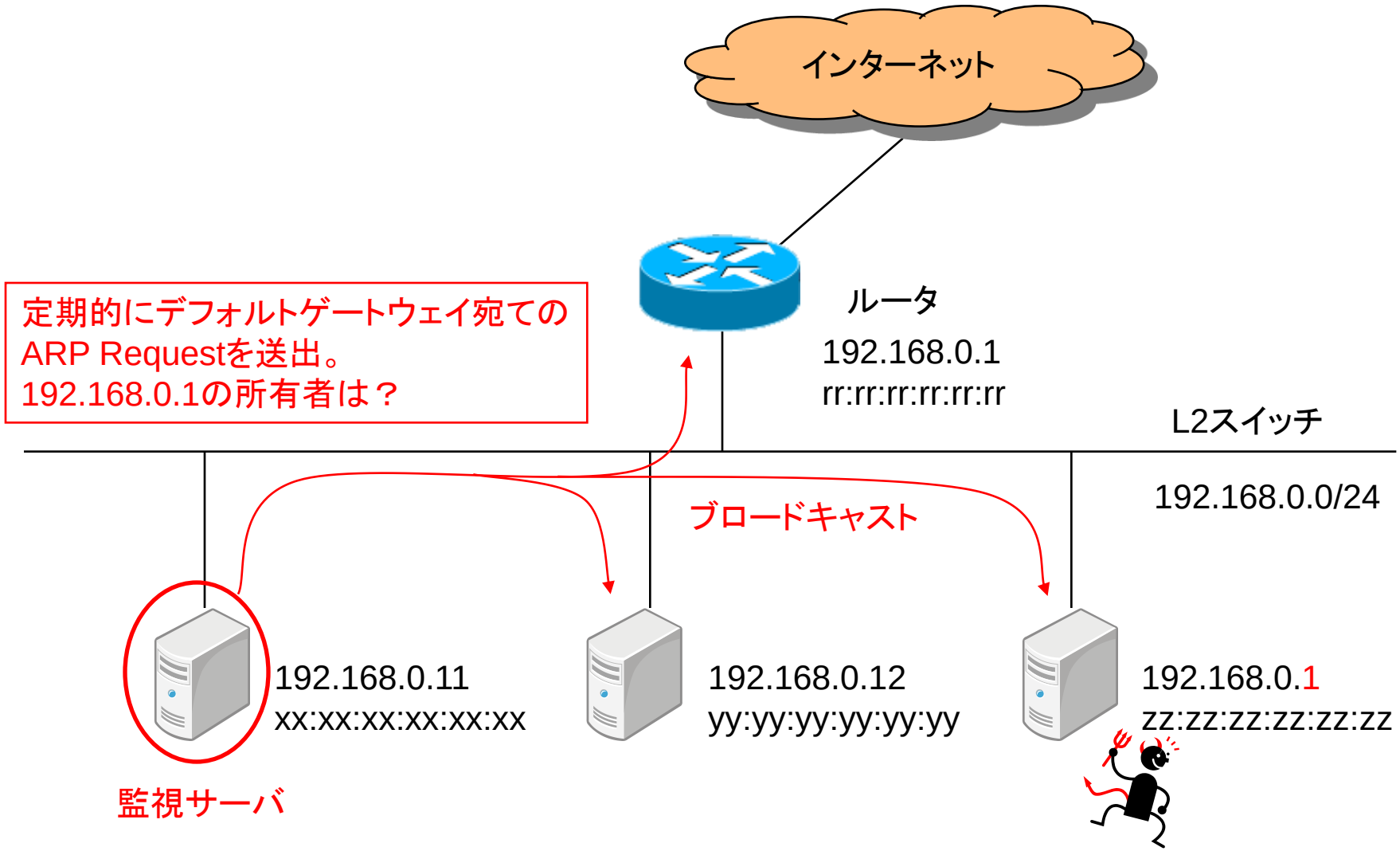
IPアドレス重複のログが出力されないケース



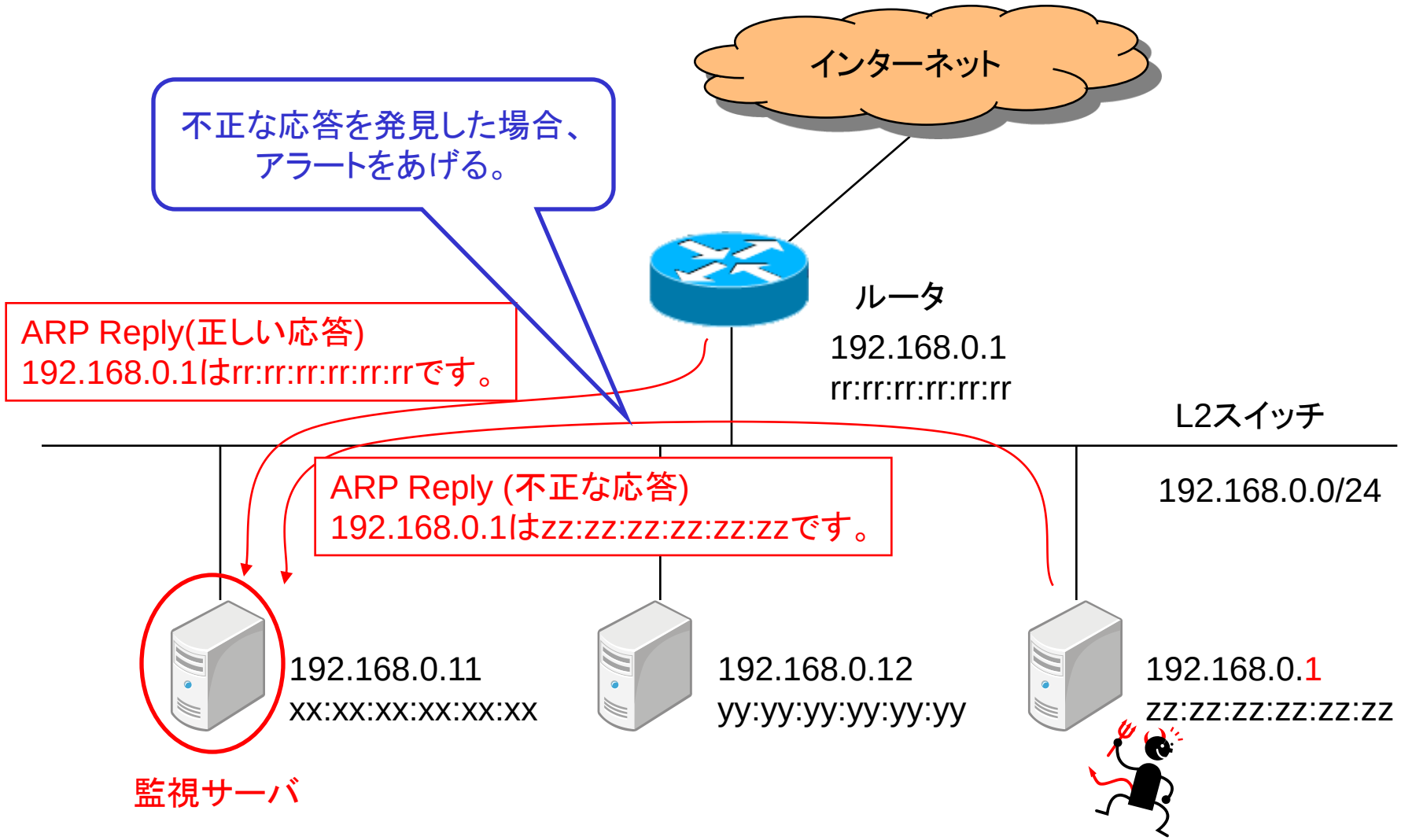
IPアドレス重複のログが出力されないケース



ARP監視サーバ設置


インターネット
ルータ
192.168.0.1
rr:rr:rr:rr:rr:rr
定期的にデフォルトゲートウェイ宛てのARP Requestを送出。
192.168.0.1の所有者は？
L2スイッチ
192.168.0.0/24
ブロードキャスト
192.168.0.11
xx:xx:xx:xx:xx:xx
監視サーバ
192.168.0.12
yy:yy:yy:yy:yy:yy
192.168.0.1
zz:zz:zz:zz:zz:zz

ARP監視サーバ設置

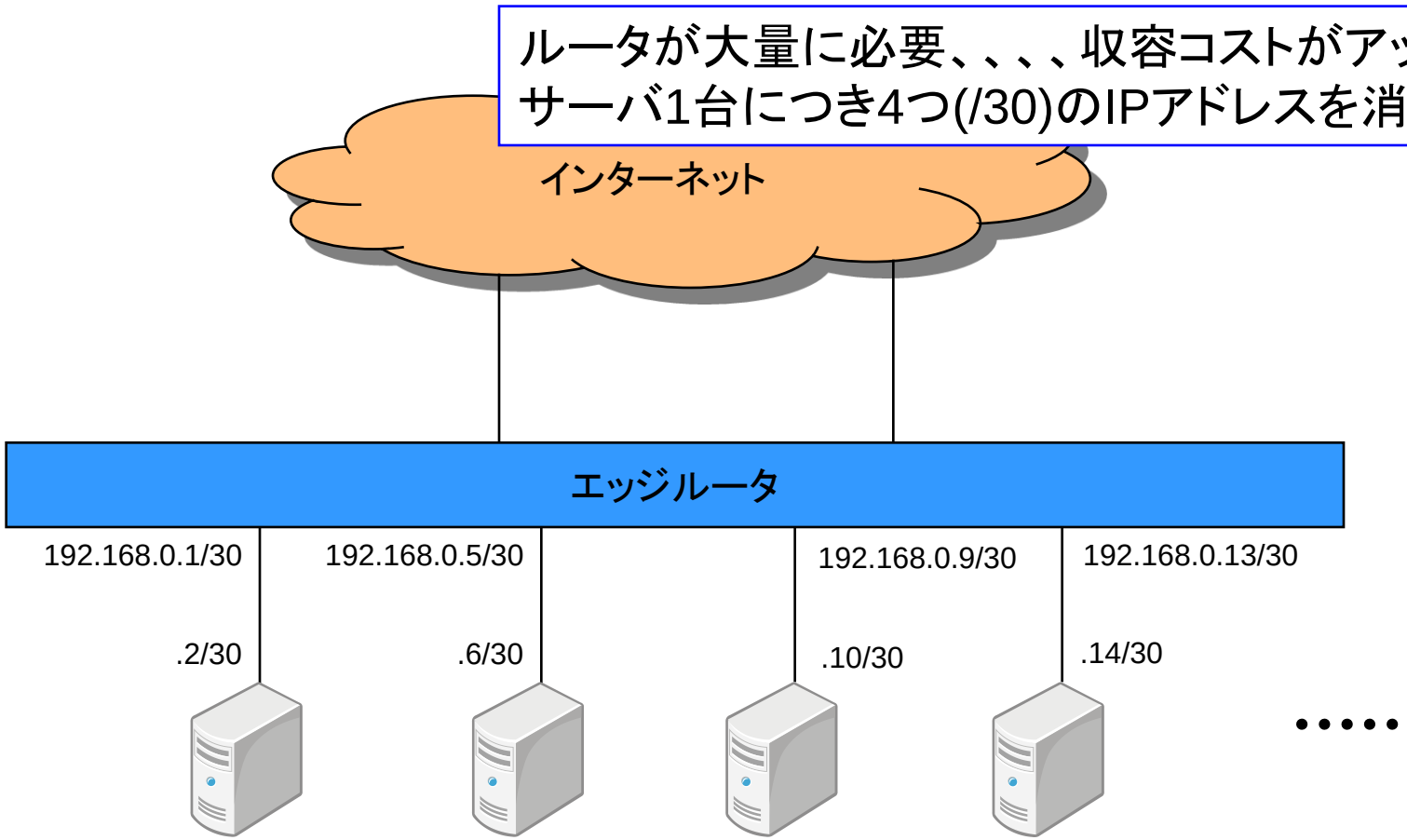

インターネット
不正な応答を発見した場合、
アラートをあげる。
ルータ
192.168.0.1
rr:rr:rr:rr:rr:rr
ARP Reply(正しい応答)
192.168.0.1はrr:rr:rr:rr:rr:rrです。
L2スイッチ
192.168.0.0/24
ARP Reply (不正な応答)
192.168.0.1はzz:zz:zz:zz:zz:zzです。
192.168.0.11
xx:xx:xx:xx:xx:xx
監視サーバ
192.168.0.12
yy:yy:yy:yy:yy:yy
192.168.0.1
zz:zz:zz:zz:zz:zz

ARP Spoofing防止策

- 検出はある程度できるが、そもそも防止する方法は無いのか？
- いくつか案があるが、それぞれ一長一短がある。
  - その１：全サーバをルータ直収にする。
  - その２：L2スイッチでARPフィルタを書く。
  - その３：同一スイッチのサーバ間の通信を禁止する。
  - その４：サーバにてデフォルトゲートウェイ宛のStatic ARPを書く。

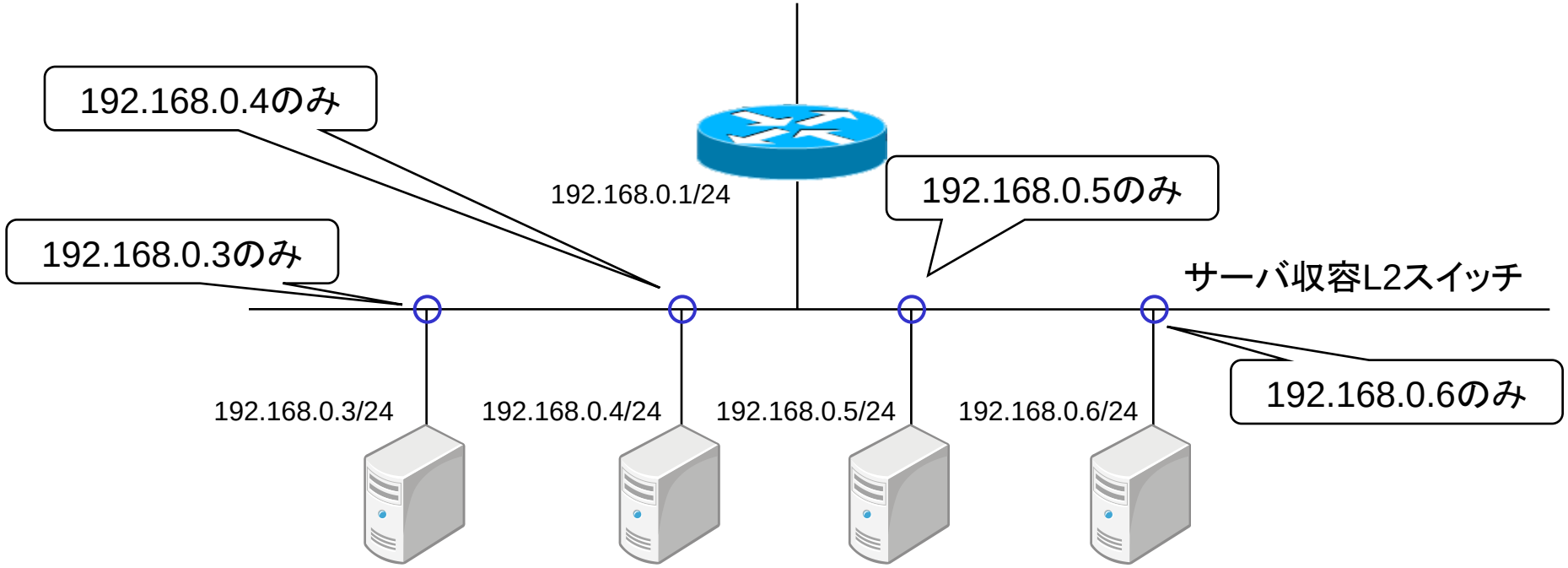
ARP Spoofing防止策（その1）

- 全サーバをルータ直収にする。



ARP Spoofing防止策（その2）

- L2スイッチでARPフィルタを書く。



ARPパケットのフォーマット

ARP Request

```
⊟ Ethernet II, Src: 00:90:27:57:86:49 (00:90:27:57:86:49), Dst
  ⊞ Destination: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
  ⊞ Source: 00:90:27:57:86:49 (00:90:27:57:86:49)
    Type: ARP (0x0806)
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: 00:90:27:57:86:49 (00:90:27:57:86:49)
    Sender IP address: 61.211.224.205 (61.211.224.205)
    Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
    Target IP address: 61.211.224.221 (61.211.224.221)
```

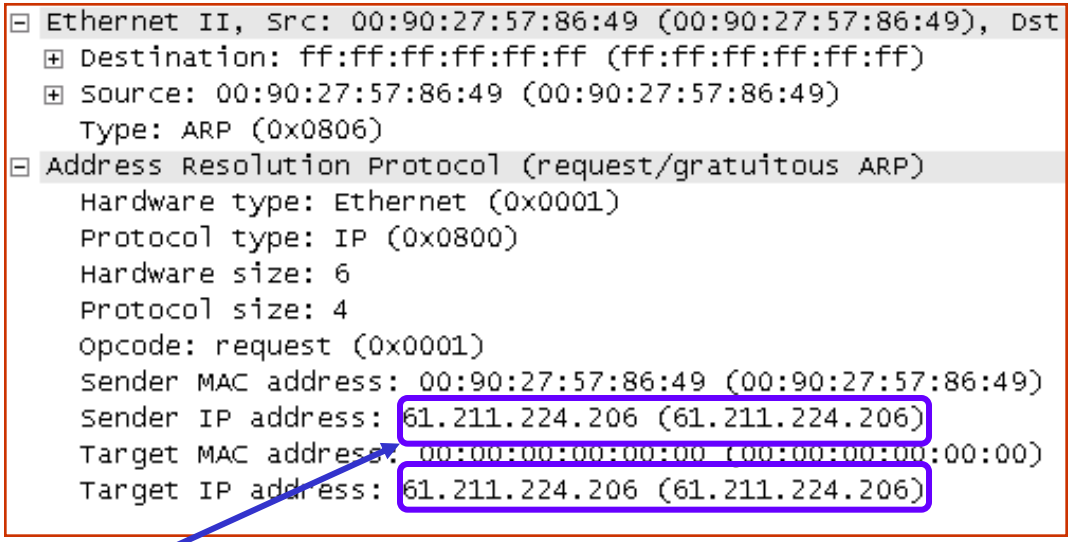
ここのSender IP addressを制限する

ARP Reply

```
⊟ Ethernet II, Src: 00:11:09:65:84:7c (00:11:09:65:84:7c), Dst
    n: 00:90:27:57:86:49 (00:90:27:57:86:49)
    :11:09:65:84:7c (00:11:09:65:84:7c)
    Type: ARP (0x0806)
    Trailer: 00000000000000000000000000000000
⊟ Address Resolution Protocol (reply)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (0x0002)
    Sender MAC address: 00:11:09:65:84:7c (00:11:09:65:84:7c)
    Sender IP address: 61.211.224.221 (61.211.224.221)
    Target MAC address: 00:90:27:57:86:49 (00:90:27:57:86:49)
    Target IP address: 61.211.224.205 (61.211.224.205)
```

ARPパケットのフォーマット

Gratuitous ARP
(ARP Requestの一種)



ここのSender IP addressを制限する

※ARP Requestと同じだが、Sender IP addressとTarget IP addressが同じ。

IPアドレスの重複確認や、自身のMACが変化した際に他のホストのARPテーブルの書き換えを促すために利用される。

ARPパケットフィルタ設定例

1番ポートから受信するARPパケットのSender IP addressを192.168.0.3に限定する場合の設定

```
packet-filter rule1 add condition ingress-port 1
packet-filter rule1 add condition arp operation 1
packet-filter rule1 add action discard
packet-filter rule2 add condition ingress-port 1
packet-filter rule2 add condition arp operation 1
packet-filter rule2 add condition arp sender-ip 192.168.0.3/32
packet-filter rule2 add action not-discard
```

ARP operation=1
ARP Request

```
packet-filter rule3 add condition ingress-port 1
packet-filter rule3 add condition arp operation 2
packet-filter rule3 add action discard
packet-filter rule4 add condition ingress-port 1
packet-filter rule4 add condition arp operation 2
packet-filter rule4 add condition arp sender-ip 192.168.0.3/32
packet-filter rule4 add action not-discard
```

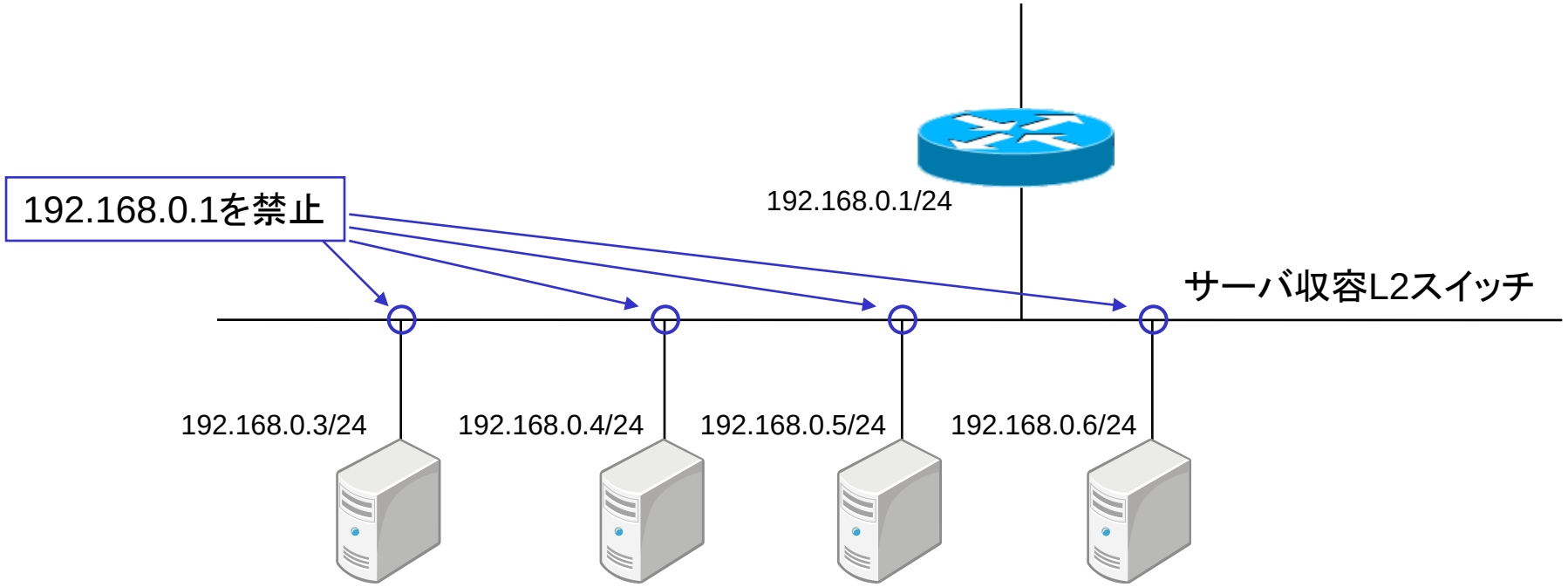
ARP operation=2
ARP Reply

サーバ1台につき、上記14行の設定が必要。。。20台だと、280行の設定。。。
サーバを別のポートに収容変更する際に、設定変更が必要。。。運用が大変！

※国産の水色のスイッチの設定例

ARPパケットフィルタ設定例

- デフォルトゲートウェイのIPアドレスをSender IPとしたARPパケットを、サーバから受信しないようにフィルタする。
  - 運用は楽になる。
  - ルータのIPアドレス詐称には有効だが、他のホストのIPアドレス詐称には効果なし。



ARPパケットフィルタ設定例

2～24番ポートからデフォルトゲートウェイのIPアドレス192.168.0.1をSender IPとした
ARPパケット受信しないような設定

```
packet-filter rule1 block 2-24
packet-filter rule1 add condition arp operation 1
packet-filter rule1 add condition arp sender-ip 192.168.0.1/32
packet-filter rule1 add action discard
```

ARP operation=1
ARP Request

```
packet-filter rule2 block 2-24
packet-filter rule2 add condition arp operation 2
packet-filter rule2 add condition arp sender-ip 192.168.0.1/32
packet-filter rule2 add action discard
```

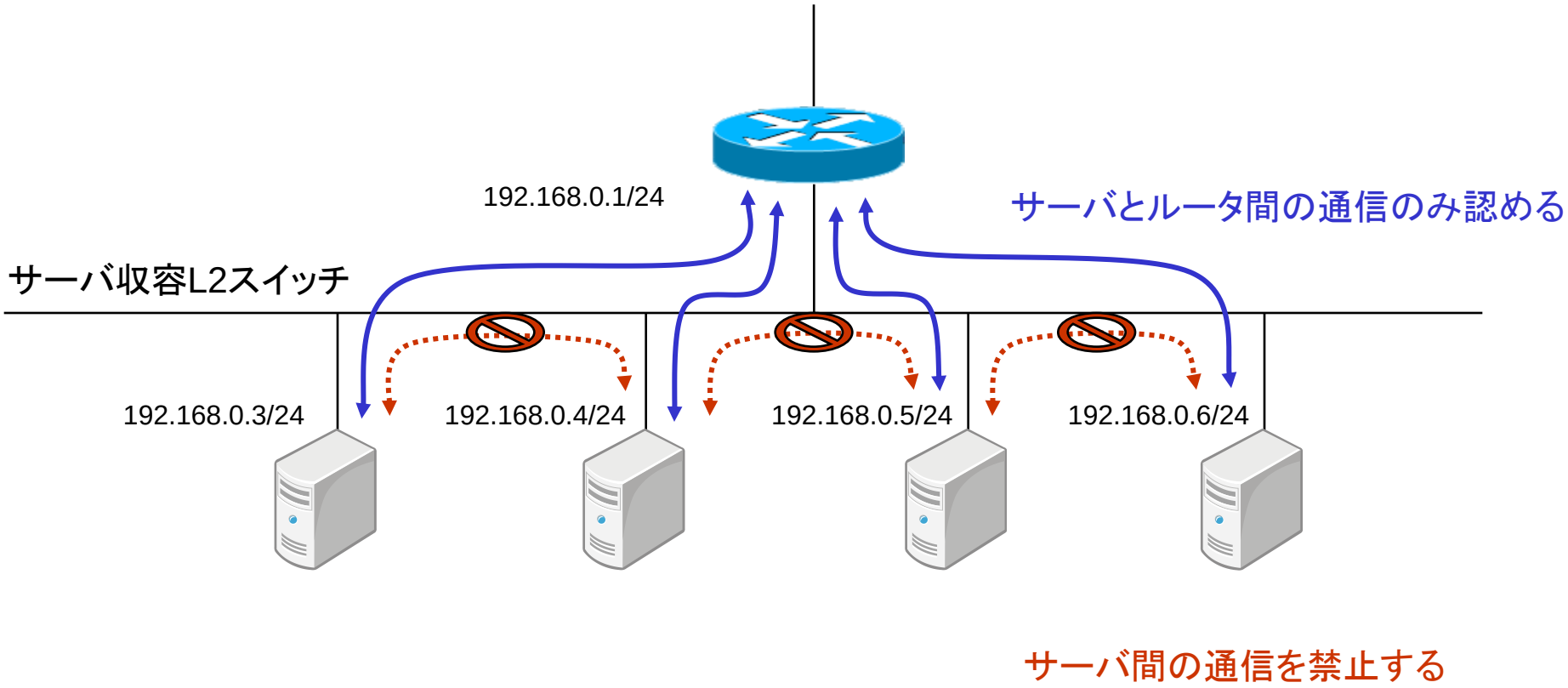
ARP operation=2
ARP Reply

※国産の水色のスイッチの設定例

スイッチ1台につき、上記8行の設定でOK！
ただし、機種によってはblockがポート毎に分かれていないため、configが増える可能性がある。

ARP Spoofing防止策（その3）

- 同一スイッチのサーバ間の通信を禁止する。
- L2スイッチのPort Isolate機能を利用。



ARP Spoofing防止策（その3）

- Port Isolate機能の設定例
- 25番ポートがアップリンクで、1～24番ポートがサーバ向けの場合。

```
forwarding enable
forwarding 1 25
forwarding 2 25
forwarding 3 25
forwarding 4 1-24
```

※国産の水色のスイッチの設定例
「中継パス制限機能」と呼ばれています ☺

Port Isolateの是非

- そもそも、サーバ間の通信を禁止しても良いのか？
- 各サーバにて、同セグメント内の他サーバ宛の通信をルータに向けるようにStatic routeを書く方法もあり。
- 下記の設定を投入して、サーバを出荷する。
- 192.168.0.0/24セグメントでデフォルトゲートウェイが192.168.0.1の場合

Linuxの場合

```
route add -net 192.168.0.0/24 gw 192.168.0.1 eth0
```

/24の経路を1つ書けばOK！

FreeBSDの場合

```
route add -host 192.168.0.3 192.162.0.1
route add -host 192.168.0.4 192.162.0.1
・・・
route add -host 192.168.0.254 192.162.0.1
```

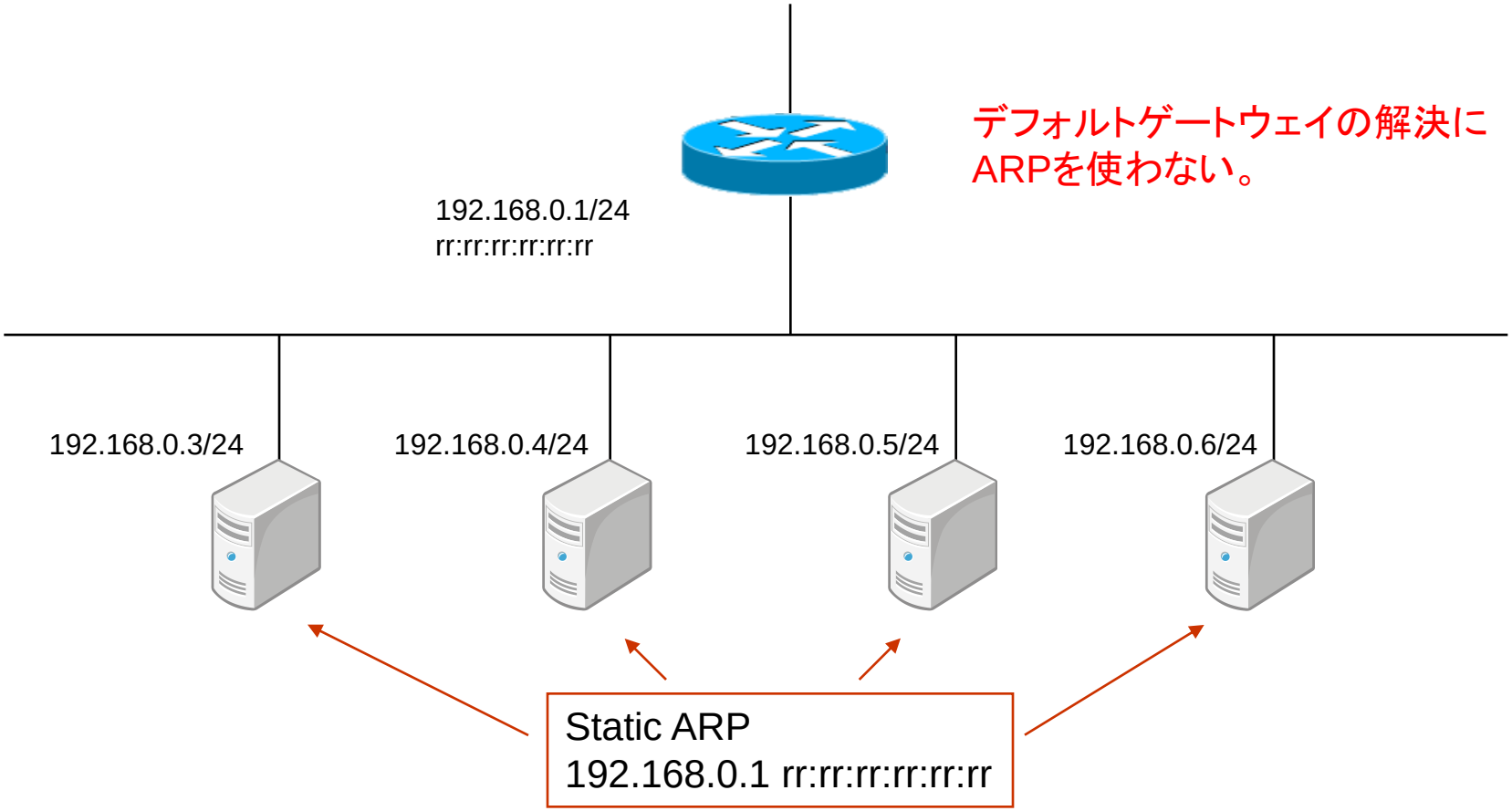
/32単位で全ホスト宛を書く必要がある・・・
約250エントリ・・・

Windowsの場合

省略・・・

ARP Spoofing防止策（その４）

- サーバにてデフォルトゲートウェイ宛のStatic ARPを書く。



Static ARPの懸念点

- VRRPを使っているため、デフォルトゲートウェイのMACアドレスは固定されている。→比較的実装しやすいかも？

  VRRPの仮想MACアドレスフォーマット

  00:00:5e:00:01:<VRID>

  例：VRIDが99の場合 → 00:00:5e:00:01:63
- デフォルトゲートウェイのMACアドレスが変化しないように運用する必要がある。
  - VRIDの変更ができない。
    - VRIDはルータ内でユニークである必要
    - 収容ルータを変更するときに、収容変更先ルータに同一VRIDが存在する場合、VRIDを変更せざるを得ない。
  - 将来VRRP以外の冗長化プロトコルに変更することができない。
- ルータのIPアドレス詐称には有効だが、他のホストのIPアドレス詐称には効果なし。

対策別の有効度合

対策	ゲートウェイの ARP Spoofing	他ホストの ARP Spoofing	現実的？
ルータ直収	有効	有効	×
各ホストARPフィルタ	有効	有効	×
ゲートウェイのみ ARPフィルタ	有効	無効	○
Port Isolate	有効	無効	△
Static ARP	有効	無効	△

○：いけそう
×：たぶん無理
△：できなくなさそうだけど、やりたくない

→ このあたりが対策としては妥当なライン？

次善策(その1)

- ほぼ同時に2つのARP Replyを受け取った場合はどうなる？
  - 正しいARP Replyと詐称されたARP Replyを同時に受信。
  - 受信側は、後に受信したReplyの内容でARPテーブルを書き換える。
  - 後にARP Replyを送信した方が勝ってしまう！
- ルータにてARP Replyの送信を、意図的に遅延させる設定ができるといいかもしれない。
- こんな設定できるルータありますか！？

次善策(その2)

- ルータからGARPを頻繁に送信
  - 配下ホストのARPテーブルをなるべく正しい状態に維持する。
  - ARP Spoofingが発生しても、影響をなるべく最小限にとどめる。

まとめ

- 複数のお客様を同一セグメントに収容する構成
  → ARP Spoofing対策は一筋縄にはいかない。
- 検出と防止策を効果的に組み合わせる必要がある。
- ネットワーク構成によって、対策は変わってくる。
- オペレーションの中で、問題を検出してから早期に問題サーバを切り離す体制作りも重要となってくる。
- 似たような別の問題もあります。
  - MACアドレス詐称(イーサフレームの送信元MACアドレス)
  - IPアドレス詐称(IPヘッダの送信元IPアドレス)
  - 別途対策が必要です。

議論

- ARP Spoofingの発生した事例はありますか？
- ホスティングサービスなどで、ARP Spoofing対策はどのようにされてますか？
  - Static ARPを設定されてる方は？
  - Port Isolate機能を使われている方は？
  - ARPのフィルタを設定されている方は？
- IX事業者さんでARP Spoofing対策はどのようにされてますか？
- ホスティングサーバで同一セグメントのサーバ間の通信を禁止してもよいでしょうか？
  - たまたま、オープンソースの公開サイトが同じセグメントにあって、ソースコードをgetしようとしたら、できないとか。
  - インターネットサーバだと、厳しいかも。
- ARP Spoofingの防止を、もっと簡単にできる仕組みはありますか？
- もっと良いARP Spoofingの検出方法はありますか？