経路制御入門
～ネットワーク設計の基本～

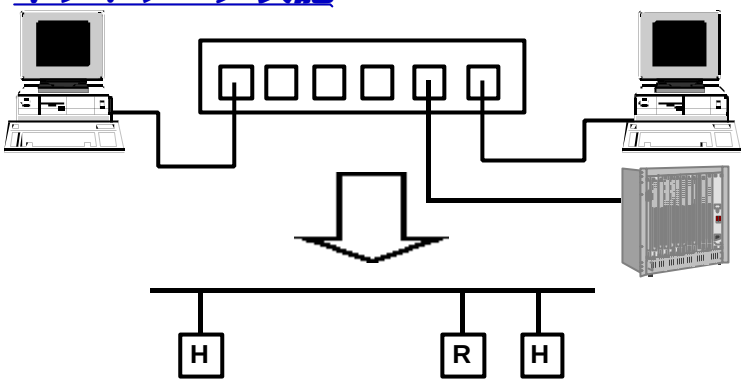
1999年12月15日

株式会社インターネットイニシアティブ
山口 二郎 (jiro-y@iij.ad.jp)

目的

- データリンク層とネットワーク層の役割
- ハブ、スイッチ、ルータの違い
- 静的経路制御と動的経路制御
- ダイナミックルーティングの動作原理
- ダイナミックルーティングを用いたバックアップ、バランシング
- ネットワーク設計
- アドレスの割り当てポリシー

ネットワーク表記

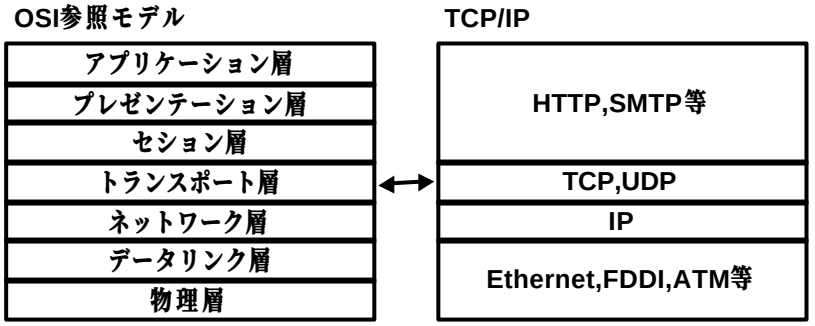


- ハブ、スイッチなどは1本の線で表わします。
- ホストはH、ルータはR等で表記します
- レイヤ３スイッチなどは説明中ではルータと区別していません

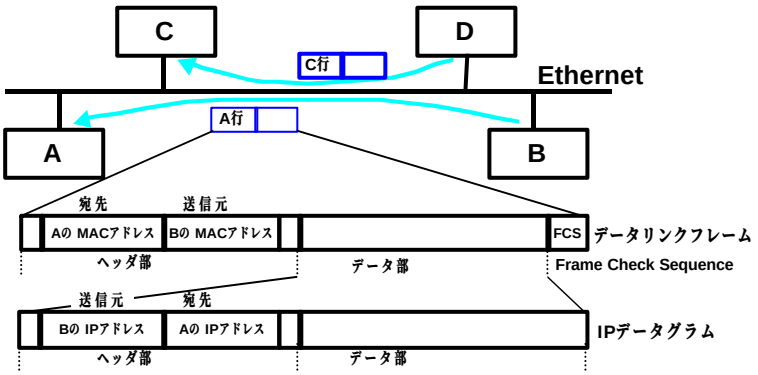
データリンクフレームとルーティング

- ここではデータリンク層とネットワーク層の役割を解説します
- MACアドレス（イーサネットアドレス）とIPアドレスの両方のアドレスが必要な訳
- ルーティングがなぜ必要なのか
- ルーティングがなくても通信できるのはなぜか

OSI参照モデルとTCP/IP



Ethernetを流れるIPデータグラム



Connectedなネットワーク

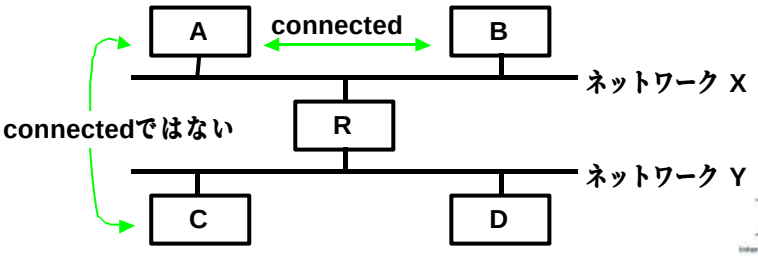
- A、bは直接同じネットワークに接続している
  - MACアドレス、IPアドレスの対応表を ARP(address resolution protocol) などにより持っている

↓

- これを「connected」な状態という

↓

- ルーティング設定が不要で、ハブなどで接続すると通信できる



Connectedではないネットワーク

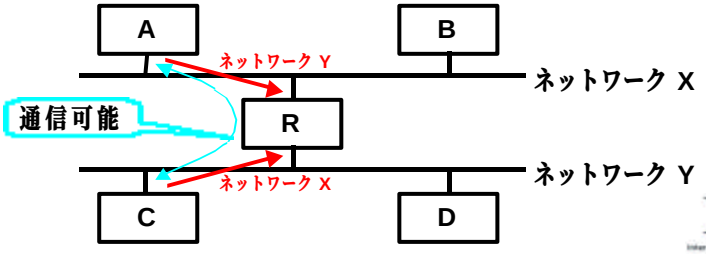
- A、Cはそれぞれ異なるネットワークに接続しているため connectedではない

↓

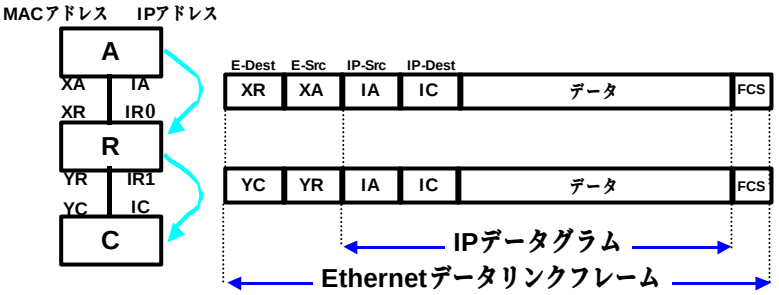
- ルーティング設定が必要
  - A: ネットワークYを Rにルーティング
  - C: ネットワークXを Rにルーティング

↓

- これにより、A⇔C間の相互通信が可能となる
  - Rは A,C共に connectedなため、通信が可能



データリンクフレームの状態



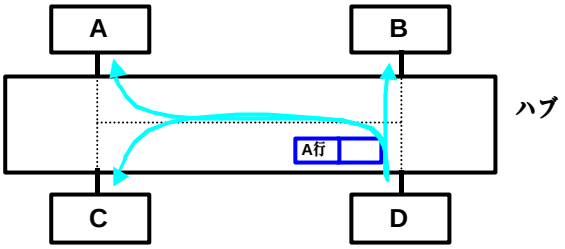
- IPデータグラムの宛先、送信元は途中で変化しない
- データリンクフレームはルータを通過する毎に変化する
- 「データリンクフレームの宛先」＝「IPデータグラムの宛先」とは限らない

スイッチとルータの機能の違い

- ハブとスイッチの機能の違い
- スイッチを有効に使う方法
- ルータを利用するための設定
- ネットワーク設定の自動化
- スイッチとルータの違い
- スイッチの耐障害性
- ルータの耐障害性
- Broadcast flood問題

ハブとスイッチの違い-1

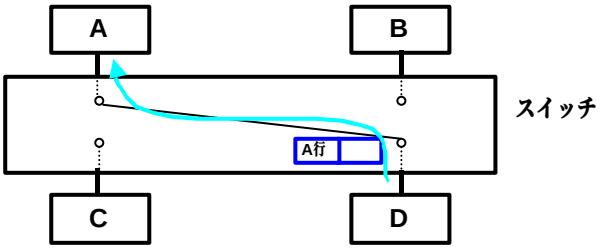
ハブで構成した場合



- ハブは全てのポートが常時接続された状態になっている
- このため異なるポート間の通信を、通信に関係の無い他のポートに伝搬して、他の通信を妨げる

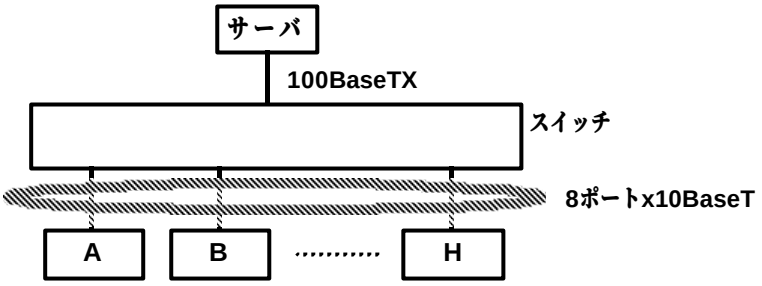
ハブと スイッチの違い-2

スイッチで構成した場合



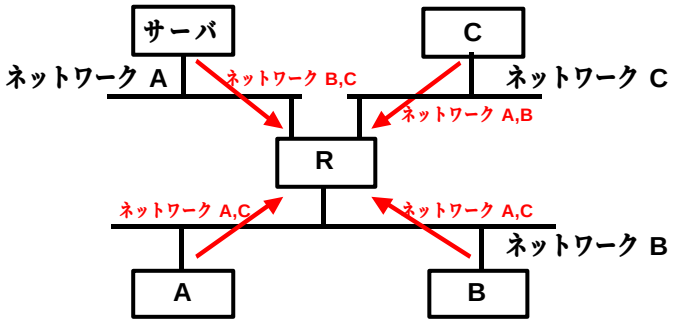
- スイッチは、ポート毎に接続されている機器のMACアドレスを学習し、通信時には必要なポート間のみで通信する

スイッチを有効に使うには



- 主にサーバ、ホスト間のトラフィックの場合に有効
- A ⇔ サーバ
⋮
H ⇔ サーバ } それぞれ10BaseTをフルに利用可能

ルータを利用するための設定

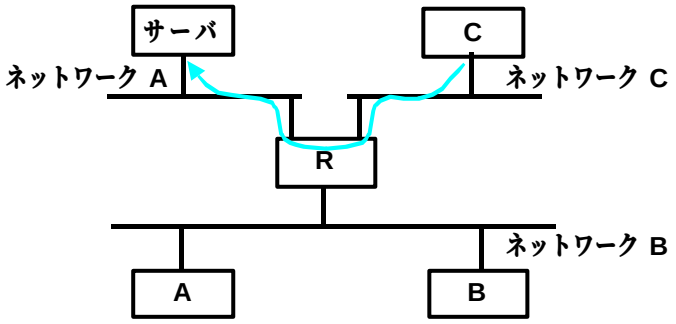


- ネットワークをサブネットに分割する
- 通信相手のネットワークのルーティングを設定する
  - DHCP,ダイナミックルーティングプロトコルなどで自動化することもできる

ネットワーク設定の自動化

- DHCP (Dynamic Host Configuration Protocol)
  - アドレスの自動割り当てを行う
  - RFC2131
  - 主にクライアントで用いられる
  - Renumberを自動的に行うため、ポータビリティがある
- ダイナミックルーティングプロトコル
  - 自動的にルーティングが設定される
  - 主にルータ間で用いられる
  - RIP,RIP2,OSPFなどがある
  - 障害時に迂回路などを自動的に選択する

スイッチとルータの違い



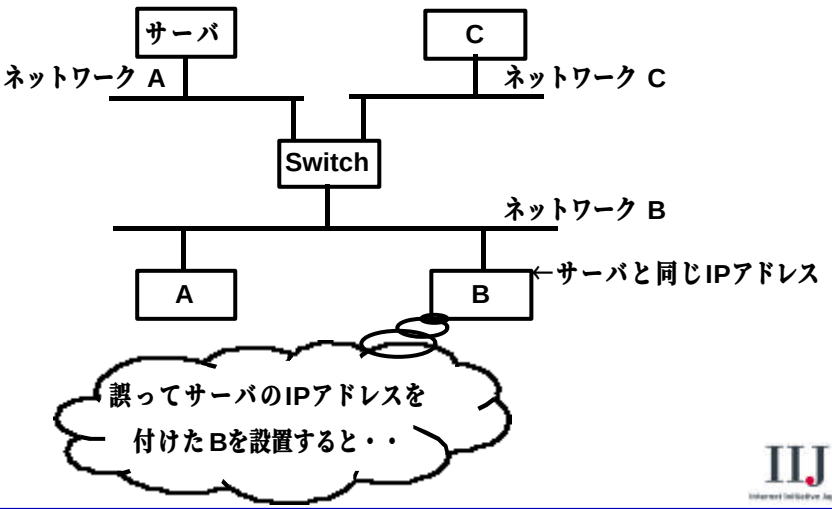
- ルータは、あるネットワーク間の通信を他の関係の無いネットワークに伝搬しない

スイッチとルータの機能の違い

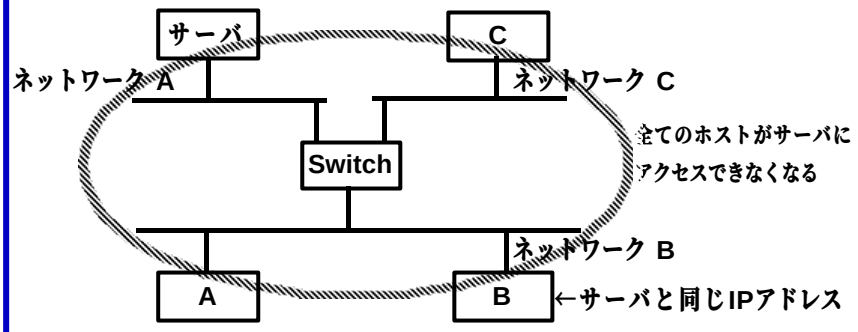
- ハブとスイッチの機能の違い
  - スイッチは異なるポートの通信を他のポートに伝搬しない
- スイッチとルータの違い
  - ルータは異なるネットワークの通信を他のネットワークに伝搬しない
  - スイッチとは異なり、ルーティングの設定が必要
  - サブネット分割が必要
- スイッチを有効に使うには
  - トラフィックが集中するようなポートにはスイッチを導入する

次に問題点について検討する

スイッチの耐障害性-1

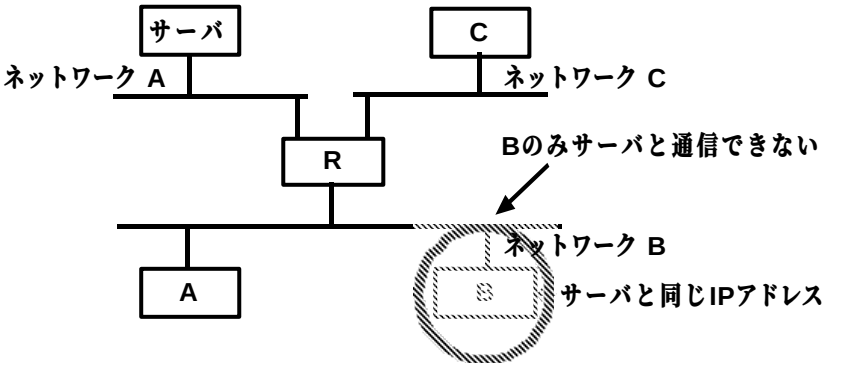


スイッチの耐障害性-2



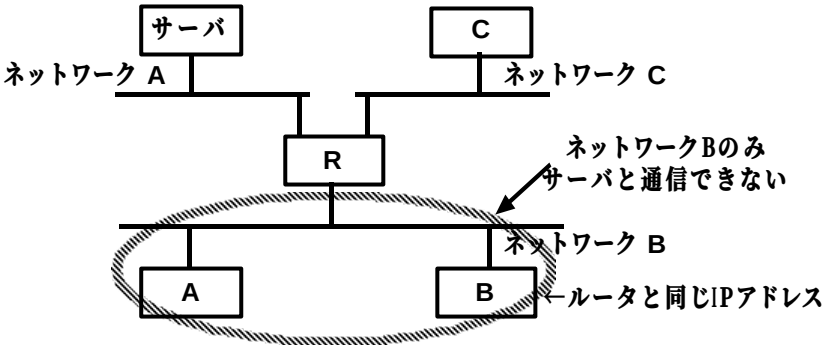
- スイッチでは、1クライアントの間違った設定の影響がネットワーク全体に及ぶ

ルータの耐障害性-1



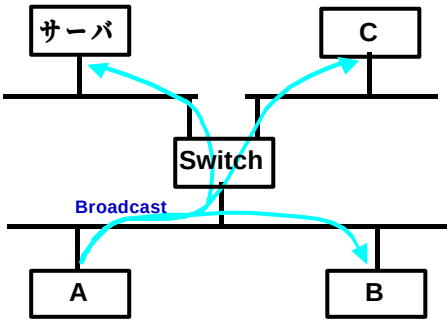
- ルータでは、1クライアントの間違った設定があったとしても、ネットワーク全体に影響を与えることはない

ルータの耐障害性-2



- 最悪の場合でも、ルータでは1クライアントの間違った設定の影響は同一セグメント内にとどまる

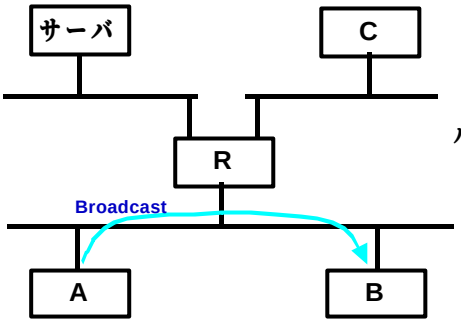
Broadcast Flood-1



Broadcastパケットはスイッチの全てのポートに影響を与える

- ホスト数が増えると、broadcastパケットも無視できないトラフィックとなる
- Windows系の OSはこのようなbroadcastパケットを大量に発生させる傾向がある

Broadcast Flood-2



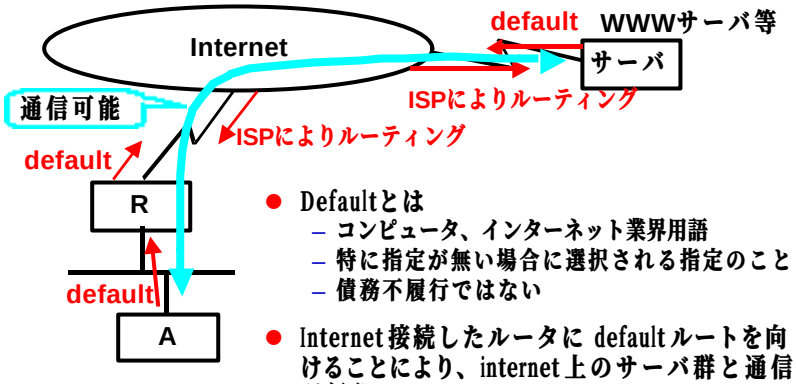
ルータは Broadcastパケットを
他のネットワークに通さない

- Broadcast floodは発生しない
- 大規模ネットワークにも対応

スイッチ VS ルータ

- スイッチの利点
  - ルーティングを考慮しなくて良い
  - ハブに比べて効率的なネットワークを構築することができる
- ルータの利点
  - ダイナミックルーティングプロトコルでバックアップ構成が可能
  - Broadcast floodが発生しない
  - 規模が大きくなってもスケールする
  - 障害時に被害を最小限に抑えることができる
  - 障害時の切り分け作業が比較的行いやすい
- 結論
  - ルータでサブネット化を行い、トラフィックが集中するようなポートにはスイッチを導入する

インターネットへの接続形態



- Defaultとは
  - コンピュータ、インターネット業界用語
  - 特に指定が無い場合に選択される指定のこと
  - 債務不履行ではない
- Internet接続したルータに defaultルートを向けることにより、internet上のサーバ群と通信が行える
- Internet接続にはルーティングは必須

経路制御解説

- ここではダイナミックルーティングの原理について解説します
- 静的経路制御（スタティック）、動的経路制御（ダイナミック）の特徴
- ダイナミックルーティングの動作原理
- ダイナミックルーティングの種類、特徴
- RIP解説
- VLSM
- トラブルシューティング

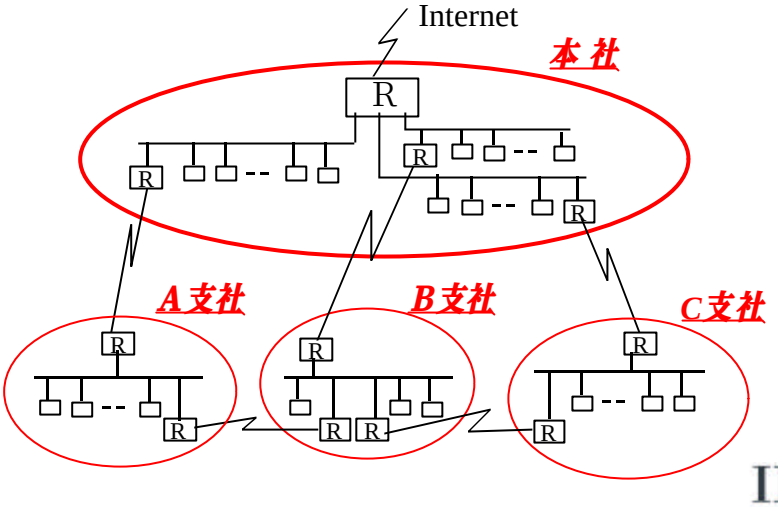
静的な経路制御と動的な経路制御

- 静的な経路制御の特徴
  - 手作業により固定的に経路を設定する
  - 安定している
  - トラフィックや伝送障害の影響を受けない
  - ルーティングプロトコルのためのトラフィックが発生しない
- 動的な経路制御の特徴
  - 自動的に経路を設定する
  - ネットワークの変化に対応できる
  - 自動的に最適経路を選択できる
  - 自動的にバックアップ経路を選択できる

動的な経路制御を選択しなければならない理由-1

- ネットワークの変化に対応しなければならない
- 勝手にネットワークが延びる
- あまりに多くて設定がめんどう

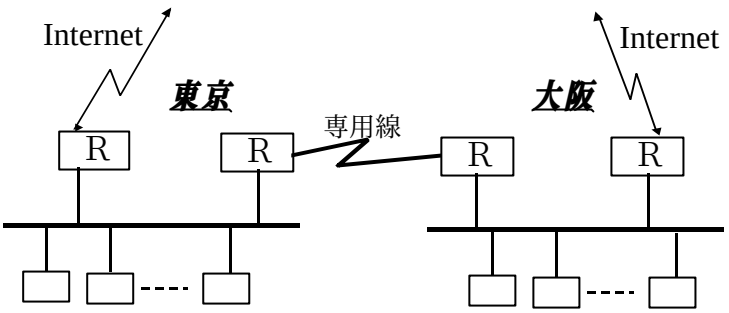
複雑に延びるネットワーク



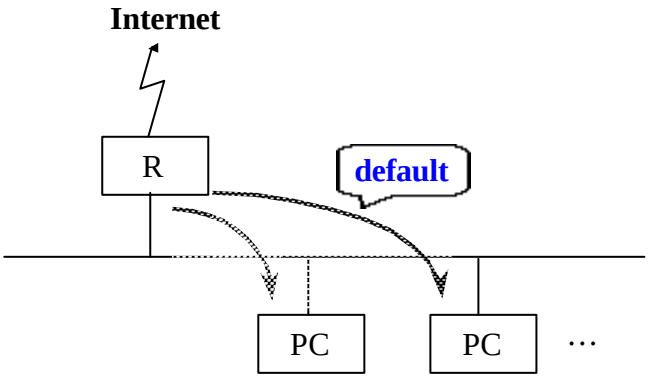
動的な経路制御を選択しなければならない理由-2

- 自動的に最適経路を選択できる
  - 管理できないほど複雑なネットワークトポロジー
- 自動的にバックアップ経路を選択できる
  - 死守するネットワークが存在する
  - 障害時に強い構成を考える

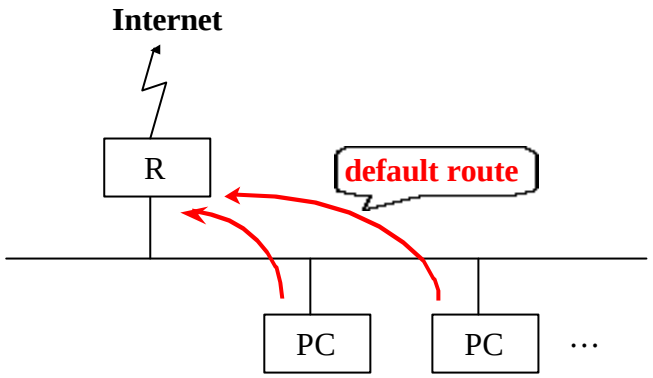
東京、大阪バックアップ



ダイナミックルーティング：経路情報の伝搬



ダイナミックルーティング：伝搬後の経路情報



ダイナミックルーティングプロトコルの種類

- RIP
  - RFC1058
- RIP2
  - RFC2453
- OSPF
  - RFC2328
- BGP4
  - RFC1771

RIP

- Routing Information Protocol version 1
- RFC1058
- アドレスのみの伝搬
  - VLSM使用不可
- ベクトル距離経路制御
- Broadcastのみ
- UNIXに標準添付されている（routed）

RIP2

- Routing Information Protocol version 2
- RFC2453
- Subnet Maskを伝搬できる
  - VLSM使用可能
- ベクトル距離経路制御
- RIPと互換性があり、併用も可能
- Multicastを利用可能
  - ホストの軽減を図る
- 最近では対応したroutedがある

OSPF - 1

- Open shortest path first
- RFC2328
- Protocol 89
  - TCP (protocol 6)でもUDP(protocol 17)でもない
- netmaskを伝搬できる
  - VLSM利用可能

OSPF - 2

- Multicast(224.0.0.5/224.0.0.6)を利用する
- Load-balancingを行う
- UNIX標準で添付されていない
  - gated等をインストールする必要がある

BGP4 - 1

- Border Gateway Protocol version 4
- RFC1771
- TCP 179
- EGPとしてのEBGPとIGPとしてのIBGPがある
- AS pathの長さにより経路を選択する

BGP4 - 2

- 複数の経路が存在する場合は最適経路のみ伝搬する
- Load-balancingは行わない
- Updateプロトコルである
- Aggregateできる。Classless Inter-Domain Routing(CIDR)対応

ダイナミックルーティングの解説

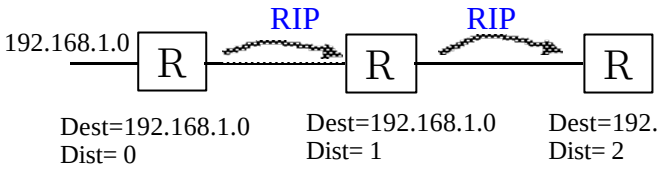
- RIPを理解する
  - RIPを理解すれば、OSPF、BGP4を概念的に理解することは容易
- 現場ではいまだにRIPが使用される場合がある
  - OSPFを利用できないルータが存在するため
  - Defaultだけを流すのでRIPで十分
- OSPF事例も取り上げる

RIPの動作原理 -1

ベクトル距離経路制御
(vector-distance/Bellman-Ford)

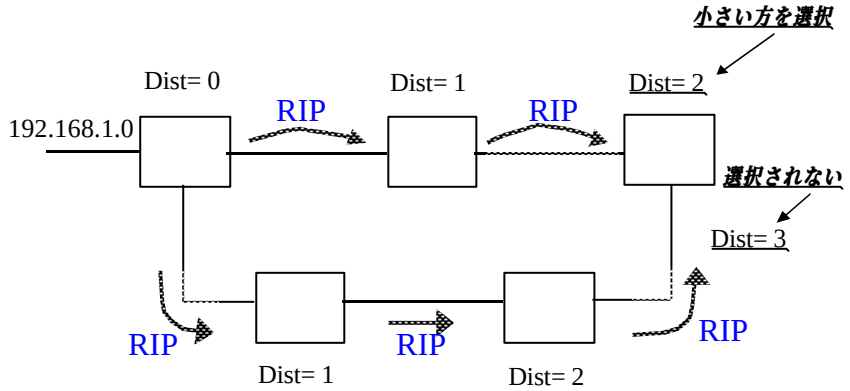
vector=destination(ネットワーク)
distance=HOP count(通過したルータの数)

ルータを通る度にdistanceが１追加される



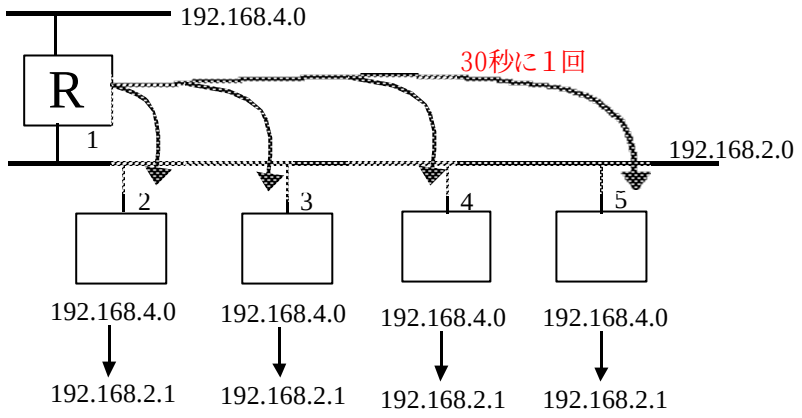
Dest=Destination
Dist= Distance

同じdestinationの場合はdistanceが小さい方を選択

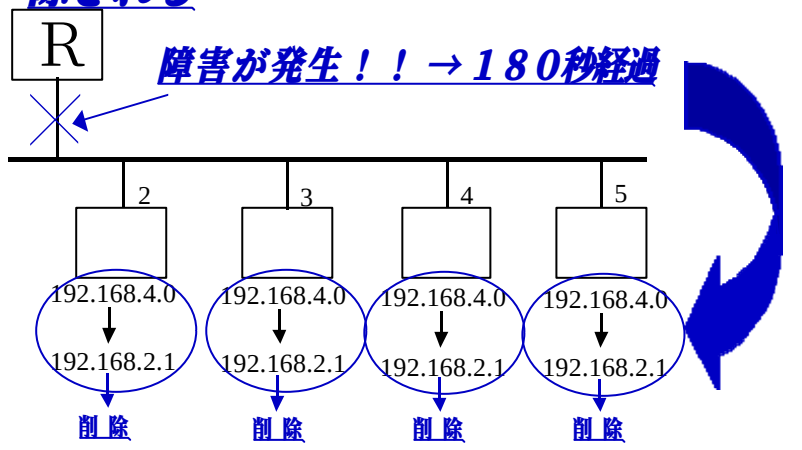


同じDestination同じDistanceの場合は
最初に到着した経路を選択

３０秒ごとにbroadcastされる



3分間経路が到着しないと経路は削除される

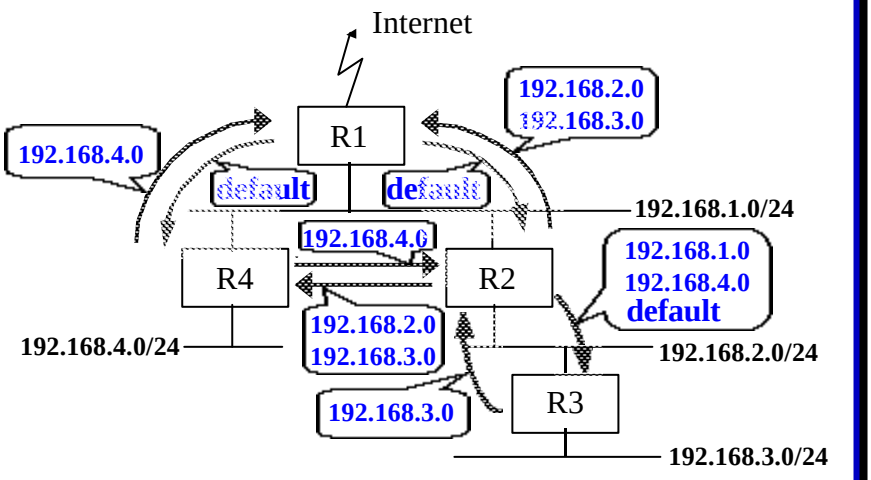


RIPで得られた経路情報は１８０秒

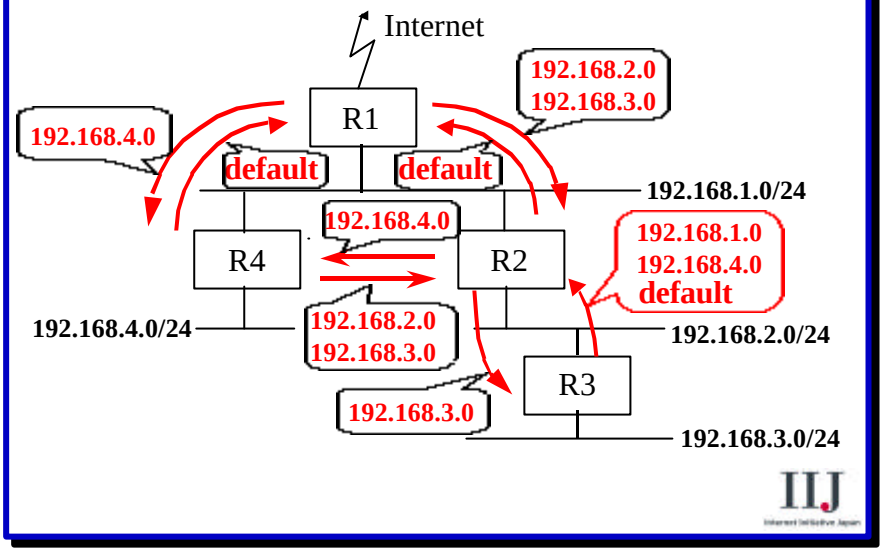
RIPの動作原理-2

- ネットワーク障害時には3分間で経路が切り替わる。 複数ルータがある場合には3分×ルータ数
- RIPはネットマスクを伝搬しない
- クラスフルなマスクと見なされる
  - 利用可能な例
    - 192.168.1.0/24
    - 172.16.0.0/16
    - 10.0.0.0/8

RIP伝搬



RIP伝搬後の経路情報



RIPの動作原理-3

- 利用不可能な例
  - 192.168.1.0/26
  - 172.16.0.0/24
- 0.0.0.0というアドレスはdefaultとして機能する

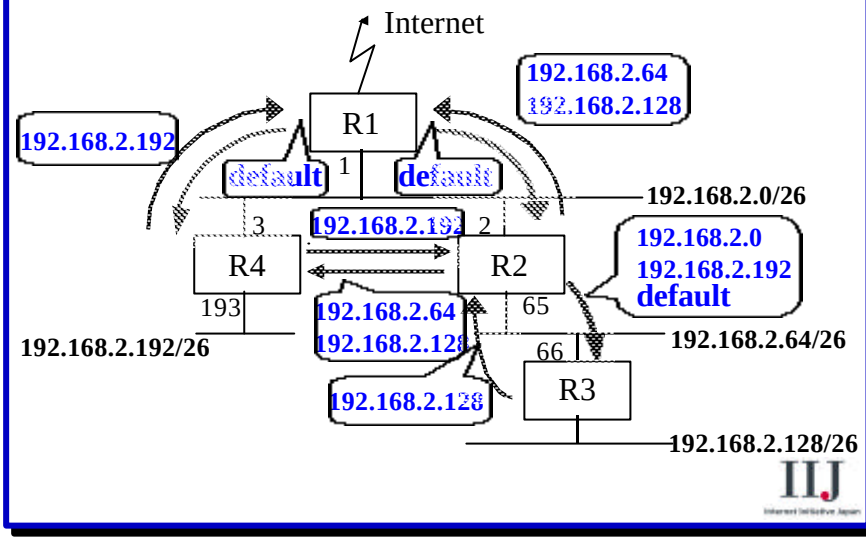
RIPのまとめ-1

- ベクトル距離経路制御(vector-distance/bellman-ford)
  - Vector=destination(ネットワーク)
  - Distance=hop count(通過したルータの数)
- ルータを通る度にdistanceが1追加される
- 同じdestinationの場合はdistanceが小さい方を選択
- 同じdestination同じdistanceの場合は最初に到着した経路を選択

RIPのまとめ-2

- 30秒ごとにbroadcastする
- 3分間経路が到着しないと経路は削除される
- ネットワーク障害時には3分間で経路が切り替わる。
  - 複数ルータがある場合には3分×ルータ数

Subnetmaskありのネットワーク構成



RIPでSubnetmaskを利用する場合-1

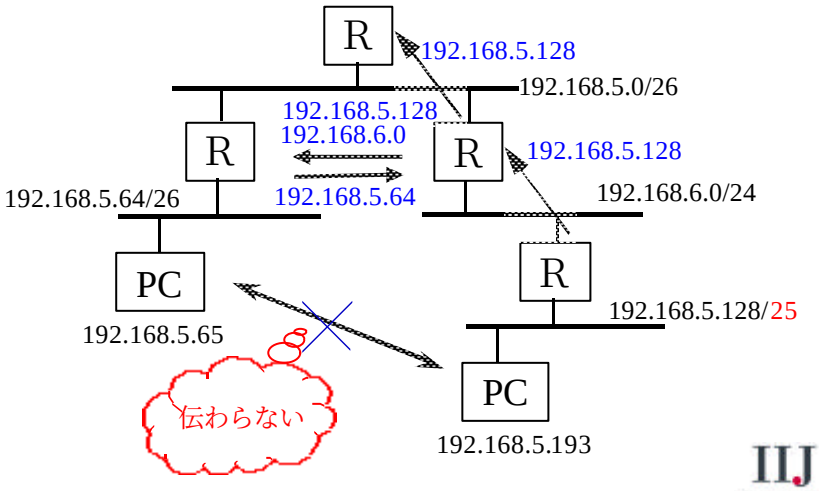
- インターフェースに設定されているnetmaskを適用
- 192.168.2.1/26 ルータのアドレス、マスクの場合

RIPで得られたdestination	ルーティングテーブル
192.168.2.64	192.168.2.64/26
192.168.2.65	192.168.2.65/32
192.168.2.128	192.168.2.128/26
192.168.2.192	192.168.2.192/26
192.168.3.0	192.168.3.0/24
192.168.3.64	192.168.3.64/32

RIPでSubnetmaskを利用する場合-2

- インターフェースに設定されているnetmaskが適用できない場合、RIPでは経路制御できない

VLSMありのネットワーク構成



VLSM(Variable Length Subnet Mask)

- ネットワーク例
  - 192.168.5.0/26
  - 192.168.5.64/26
  - 192.168.5.128/25
- 192.168.5.1が192.168.5.128を受け取った場合
  - 192.168.5.128/26と誤認する
  - 192.168.5.192～192.168.5.255がルーティングされない
- RIPだけではVLSMに対応できない
  - VLSM対応には RIP2、OSPFを利用

ルータでのRIP制御

聞く	広告	
○	○	RIPのみで運用可能
×	○	defaultのみ広告を行うなどで利用
○	×	defaultを告知しない場合に利用

トラブルシューティング- RIPが伝搬しない-1

- 同じbroadcastアドレスを利用していない
  - Broadcastアドレスが異なっている場合
  - 192.168.1.0/24を利用の場合
    - 192.168.1.255　network+all-1
    - 192.168.1.0　network+all-0
    - 255.255.255.255　all-1
    - 0.0.0.0　all-0
- 古いルータやワークステーション等はall-0,all-1固定の場合がある

トラブルシューティング- RIPが伝搬しない-2

- Broadcastアドレスがfilterされている
  - 255.255.255.255,0.0.0.0などがインターフェースのoutputでfilterされていないか？
- プロトコル、ポートがfilterされている
  - UDP 520がfilterされていないか？
- Unnumberedのi/fでbroadcastを伝搬できない
  - unicastで広告するように設定する
  - unicastで広告して良いのか？

トラブルシューティング-RIPv2とOSPFが伝搬しない

- ルータのfilter等でmulticastアドレスや、protocol、portなどが制限されていないか注意する
  - RIP2
    - 224.0.0.9
    - UDP 520
  - OSPF
    - 224.0.0.5/224.0.0.6
    - Protocol 89
- Multicastをサポートしない場合
  - OSによってはmulticastを受けられない場合がある
    このときはbroadcastにて代用する

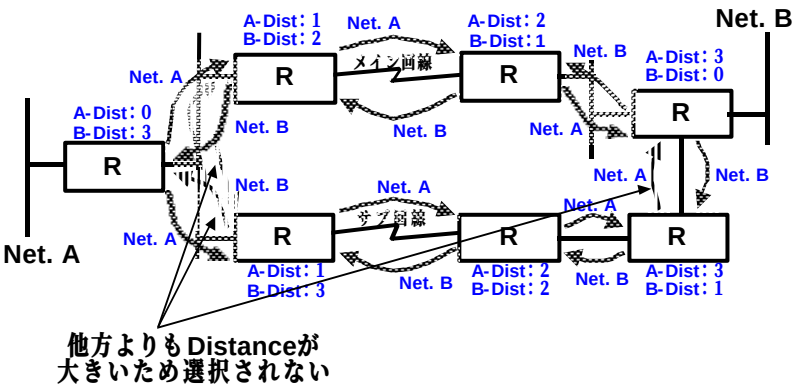
ダイナミックルーティングのまとめ

- VLSMを考慮するとRIP2,OSPFへの移行が望まれる
- 単純なネットワーク構成はstaticを選択
- Defaultのみを利用する場合はRIPでも十分

ダイナミックルーティングプロトコルを用いた障害に強いネットワーク構成

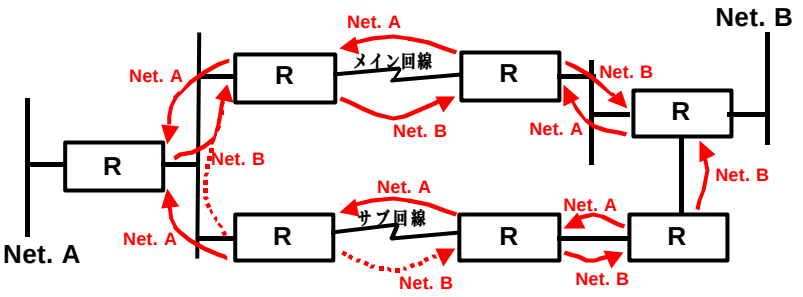
- RIPを用いたバックアップ
- OSPFを用いたバックアップ、バランシング
- デュアル構成＋OSPFによるバックアップ、バランシング
- リングトポロジによるバックアップ
- ATM障害検出

RIPを用いたバックアップ-経路の伝搬（定常時）



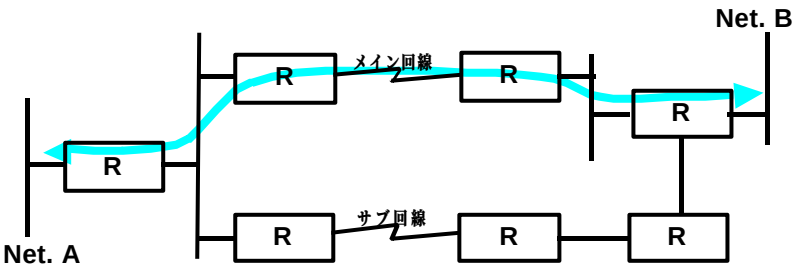
- RIPを利用し、主にバックアップを目的とした構成
- 通常時はメイン回線のみを利用する

RIPを用いたバックアップ -ルーティングテーブル（定常時）



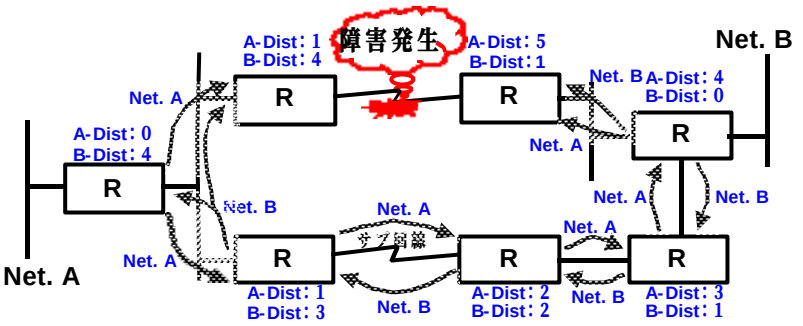
- RIPの経路情報が伝搬することにより、各ルータに経路情報が設定される
- Distanceの違いから、メイン回線側の経路が選択される

RIPを用いたバックアップ-トラフィックの流れ（定常時）



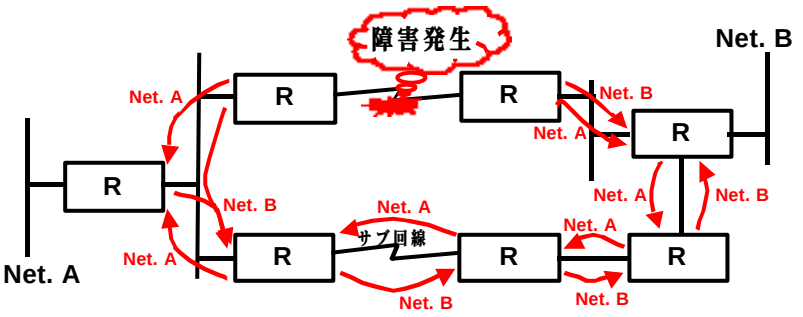
- 通常時はメイン回線のみが利用される

RIPを用いたバックアップ-経路の伝搬（障害時）



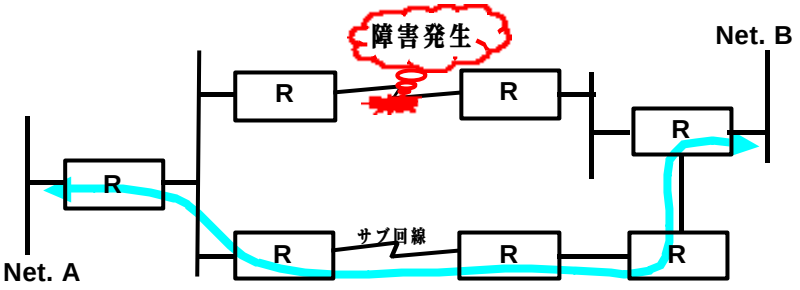
- メイン回線に障害が発生したため、経路情報の伝搬が変化する

RIPを用いたバックアップ-ルーティングテーブル（障害時）



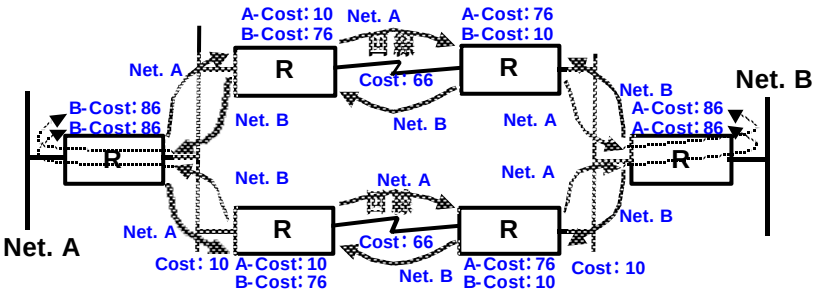
- 経路情報の伝搬が変化するため、各ルータに設定されている経路情報が変更される

RIPを用いたバックアップ-トラフィックの流れ（障害時）



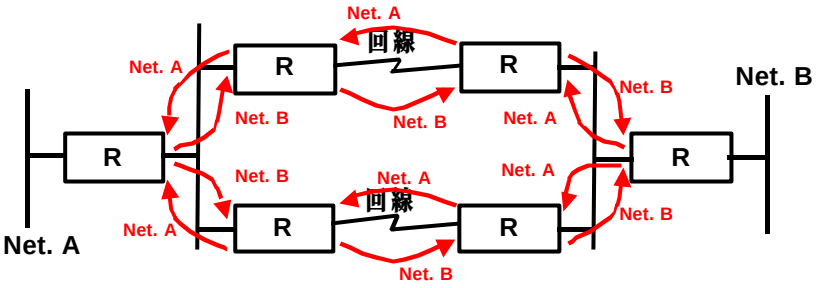
- メイン回線に障害が発生しているため、トラフィックの流れも変化する
- サブ回線を利用して、通信のバックアップを行う

OSPFを用いたバックアップ、バランシング-経路の伝搬（通常時）



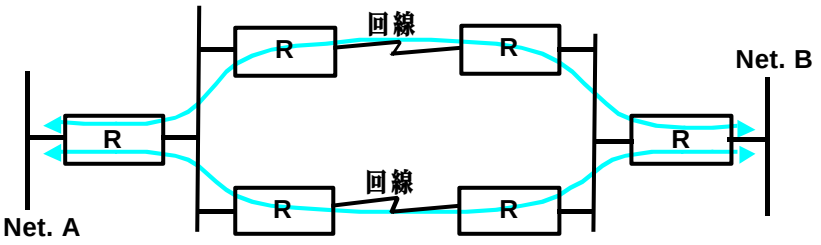
- OSPFを利用して、通常時もそれぞれの回線をバランシングして利用する
- 障害時にはどちらか一方の回線を利用してバックアップを行う

OSPFを用いたバックアップ、バランシング-ルーティングテーブル（通常時）



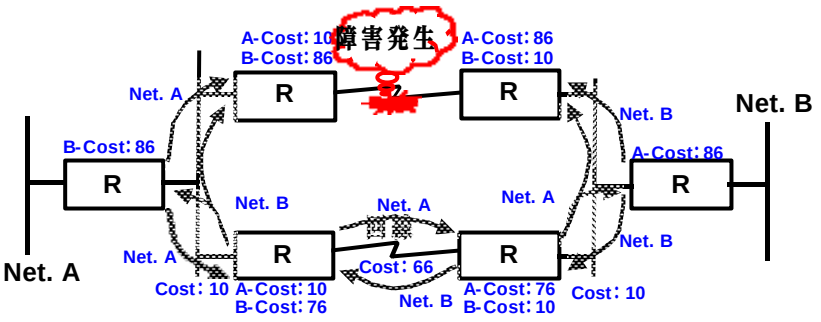
- 広報されてきた経路情報のcos tが同じであれば、OSPFの機能で両方の経路が有効になる

OSPFを用いたバックアップ、バランシング-トラフィックの流れ（通常時）



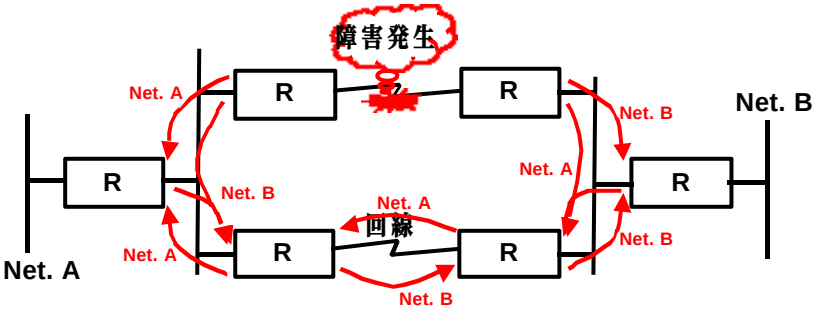
- 複数の経路が設定されているため、それぞれの回線をバランシングして利用する

OSPFを用いたバックアップ、バランシング-経路の伝搬（障害時）



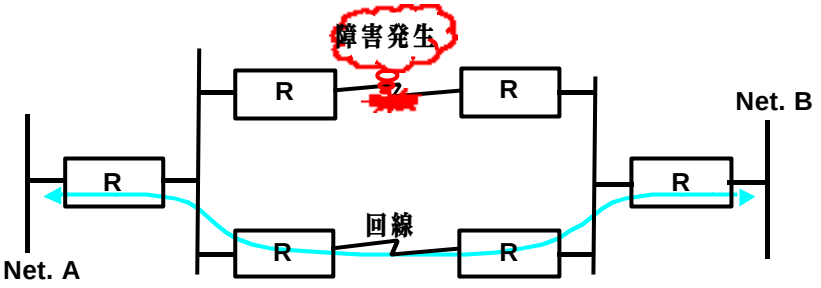
- 一方の回線に障害が発生し、広報される経路に変化が生じる

OSPFを用いたバックアップ、バランシング-ルーティングテーブル（障害時）



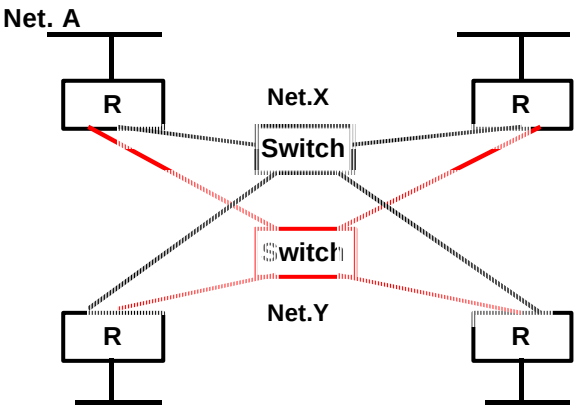
- 広報される経路情報が変化するため、各ルータの経路情報も変化する

OSPFを用いたバックアップ、バランシング-トラフィックの流れ（障害時）

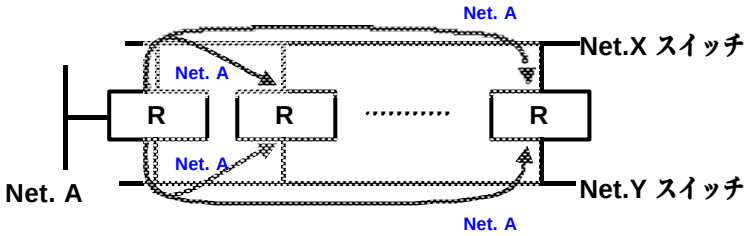


- 一方の回線に障害が発生した場合には、全てのトラフィックをもう一方の回線を利用してバックアップする

デュアル構成＋OSPFを用いたバックアップ、バランシング接続図

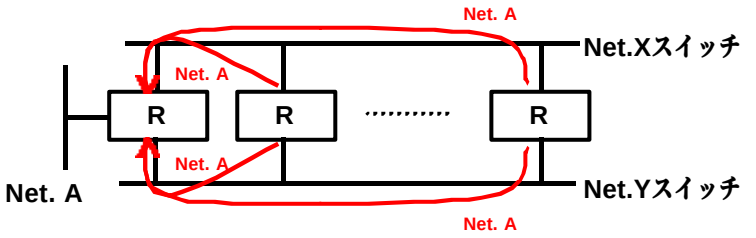


デュアル構成＋OSPFを用いたバックアップ、バランシング - 経路の伝搬（通常時）



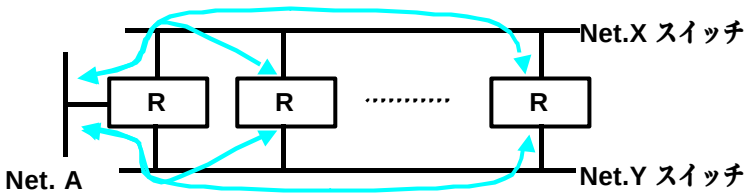
- OSPFで Net.Aの経路情報を広報する
- 経路情報は各ルータに対して、2つのスイッチから等価に伝搬する

デュアル構成＋OSPFを用いたバックアップ、バランシング - ルーティングテーブル（通常時）



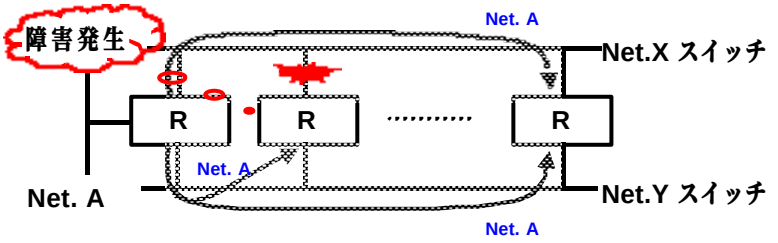
- 伝搬した経路情報により、各ルータに経路情報が設定される。
- ２つのスイッチから等価な経路情報が伝搬してきたため、２つの経路情報が設定される

デュアル構成＋OSPFを用いたバックアップ、バランシング -トラフィックの流れ（通常時）



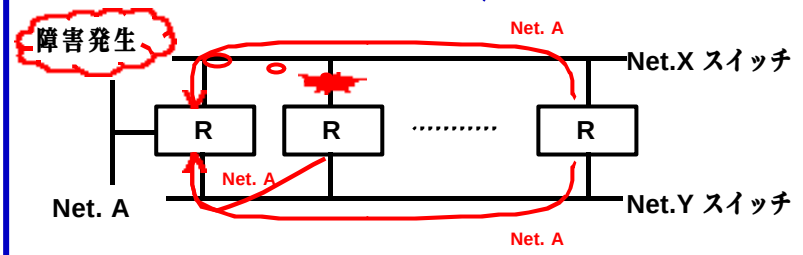
- 通常時には、2つのスイッチを経由するトラフィックがバランスする

デュアル構成＋OSPFを用いたバックアップ、バランシング -経路の伝搬（障害時）



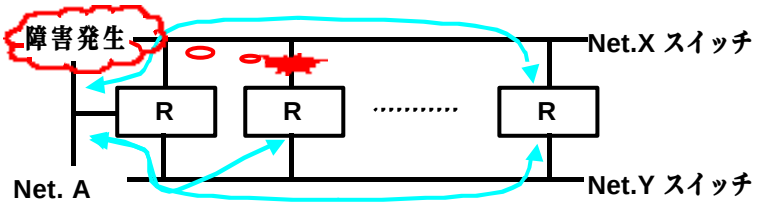
- 障害発生により、経路情報の伝搬に一部に変化が生じる

デュアル構成＋OSPFを用いたバックアップ、バランシング -ルーティングテーブル（障害時）



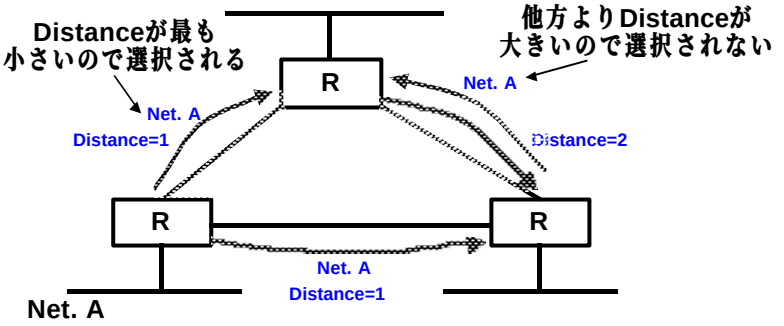
- 伝搬する経路情報が変化するため、各ルータに設定されている経路情報も変化する
- 一方のスイッチからの経路が消えても、もう一方のスイッチからの経路でバックアップを行う

デュアル構成＋OSPFを用いたバックアップ、バランシング -トラフィックの流れ（障害時）



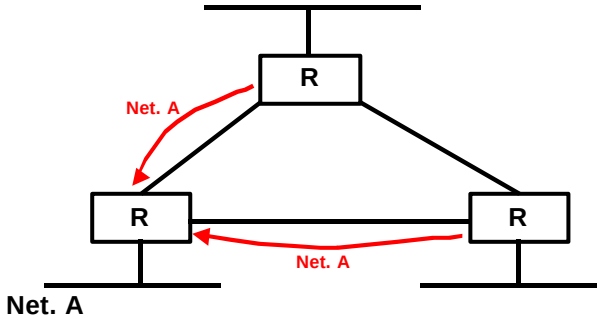
- 障害時には、2つのスイッチどちらかを利用して障害を迂回することができる

リングトポロジによるバックアップ -経路の伝搬（通常時）



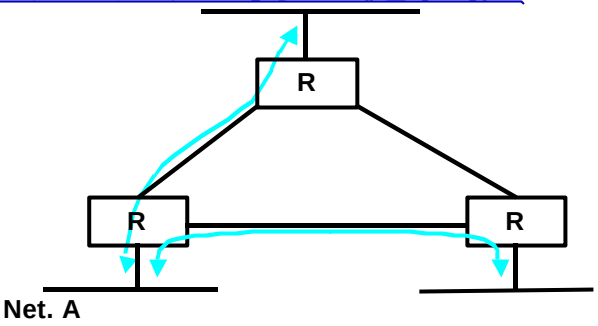
- RIPで Net.Aの経路情報を広報する
- 通常時は最短な経路が優先される

リングトポロジによるバックアップ -ルーティングテーブル（通常時）



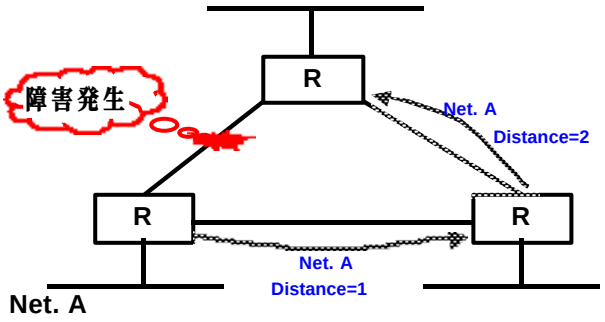
- 伝搬した経路情報から、各ルータに経路情報が設定される

リングトポロジによるバックアップ - トラフィックの流れ（通常時）



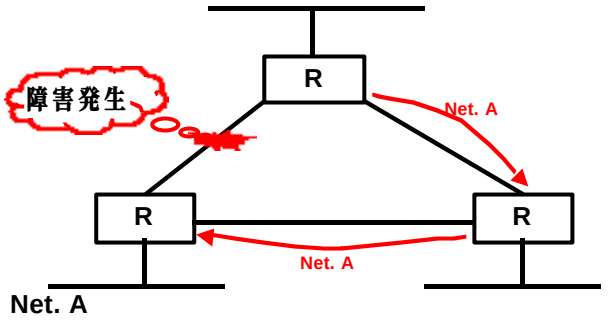
- 通常時は最短な経路が優先されて、通信が行われる

リングトポロジによるバックアップ -経路の伝搬（障害時）



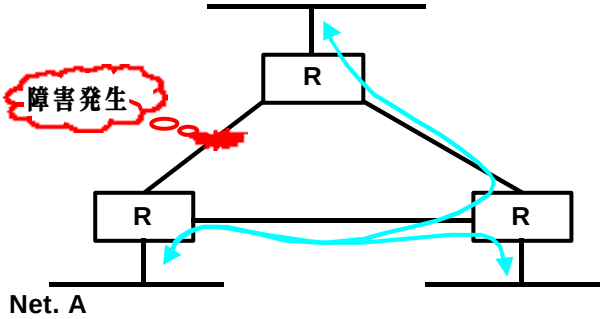
- 障害により、経路情報の伝搬に変化が生じる

リングトポロジによるバックアップ -ルーティングテーブル（障害時）



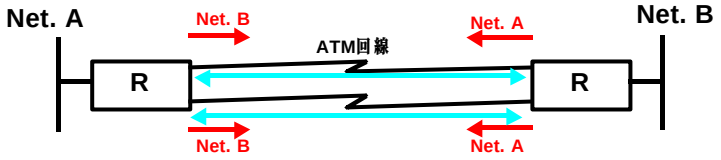
- 伝搬する経路情報の変化により、ルータに設定されている経路情報も変化する

リングトポロジによるバックアップ -トラフィックの流れ（障害時）

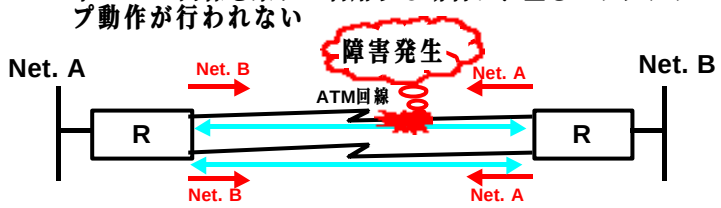


- 障害時には、遠回りな経路を利用して通信をバックアップする

ATM障害検出-1



- VPの downを検出して自動的にインターフェースを shutdownすることができない(cisco IOS11.X)
- このため、上記のように staticにルーティングを設定し、2本のATM回線を束ねて利用する場合に、望むバックアップ動作が行われない



- この例では概ね５０%のパケットをこぼしてしまう。

ATM障害検出-2

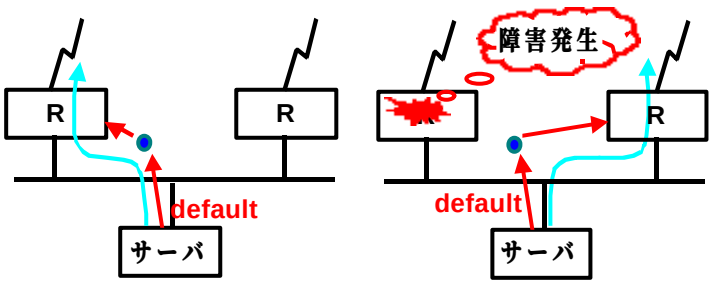
- OSPFを用いて動的に経路制御してバランシングを行えば、ATM回線でも障害検出が可能とる

- OSPFが障害を検出し、回線を利用しなくなるのでパケットをこぼさない

ダイナミックルーティング以外のバックアップ、バランシング技術

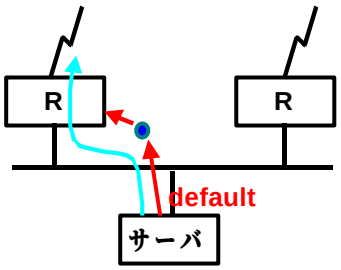
- STP(spanning tree protocol)
  - レイヤ２での冗長構成
  - 障害の発生から spanning tree変更までには10秒程度必要
- FDDI DAS(dual attachment station)
  - レイヤ２での冗長構成
  - ほぼ瞬時に切り換わる
- I/F downと static
  - I/Fの downを検出するとその i/fに向いているroutingが消えることを利用したbackup
  - ATM専用線等では回線断が I/F downとならないため、利用できない
    - OAMセルを keepalive代わりに利用することで、回線断を検出可能にしようとしている (IOS12.x)
- HSRP
  - 一つの仮想的な MACアドレスを複数のルータで共有することで、サーバ等でダイナミックルーティングを利用せずに障害時の切り換えを行う

HSRP-1



- 障害時には MACアドレスとルータの対応を変更するため
  - デフォルト設定では以下の停止が伴う
    - 切り換えに 10秒
    - 切り戻しに 30秒
  - スイッチ等にルータを接続している場合には、ポート、MACアドレスの対応に食い違いが生じるため、さらに切り換えに時間を要する場合がある

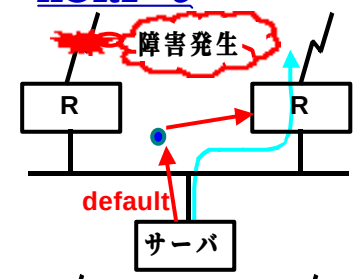
HSRP-2



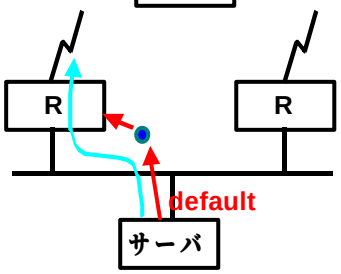
- HSRP+Interface Tracking（通常運用時）

- Interfaceの downを検出して、Trackingすることで回線障害時にactiveルータの切り換えを行う

HSRP-3

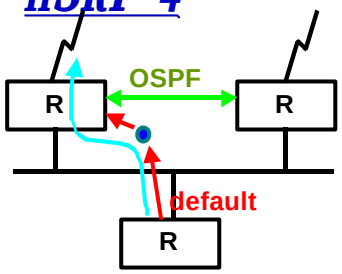


- HSRP+InterfaceTracking（障害発生時）
  - Interface Trackingにより切り替え
  - 10秒間停止

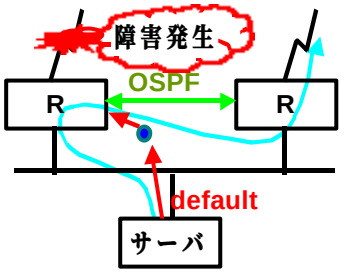


- HSRP+Interface Tracking（障害復旧時）
  - 復旧により切り戻しが発生
  - 30秒間停止

HSRP-4

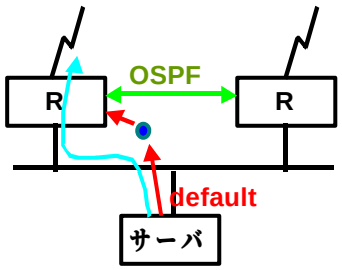


- HSRP+OSPF(通常運用時)
  - ルータ障害時のみHSRPを利用して、回線障害時にはOSPFを利用してバックアップを行う



- HSRP+OSPF(障害発生時)
  - 回線断により、OSPFにて切り換え
  - 1～3秒間停止

HSRP-5

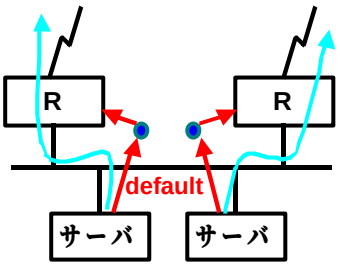


- HSRP+OSPF(障害復旧時)
  - 復旧したために切り戻し発生
  - 経路の切り換えのみなので停止なし

- ダイナミックルーティングは切り戻しに停止を伴わないため、ルータ間はOSPF等のダイナミックルーティングを利用したほうが良い

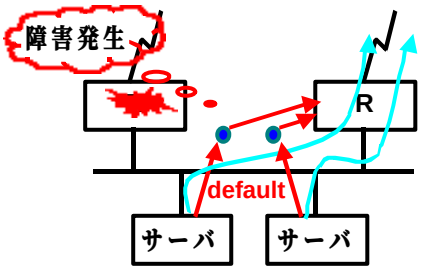
MHSRP-1

- マルチグループを用いて MHSRPを利用すれば、サーバ毎にトラフィックを分ける事ができる



- MHSRP (通常運用時)
  - それぞれのサーバは対応する HSRPの仮想アドレスに defaultを向ける

MHSRP-2

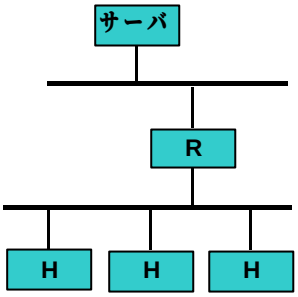


- MHSRP (障害発生時)

- なお、MHSRPにはグループID衝突問題があるため、オープンなネットワークでの利用には注意が必要

ネットワークの拡張を考慮した設計-1

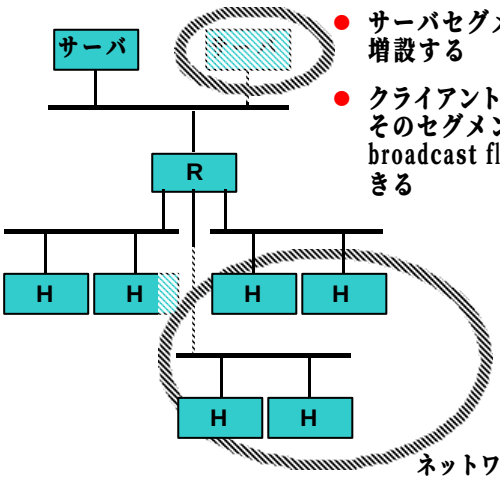
左図ネットワーク構成の特徴



- 小規模であってもサーバのセグメントを分離する
  →サーバの安全性を確保する
- クライアントはDHCPによりアドレスの割り当てとデフォルト経路を得る
- Broadcast floodのサーバへの影響を防ぐ

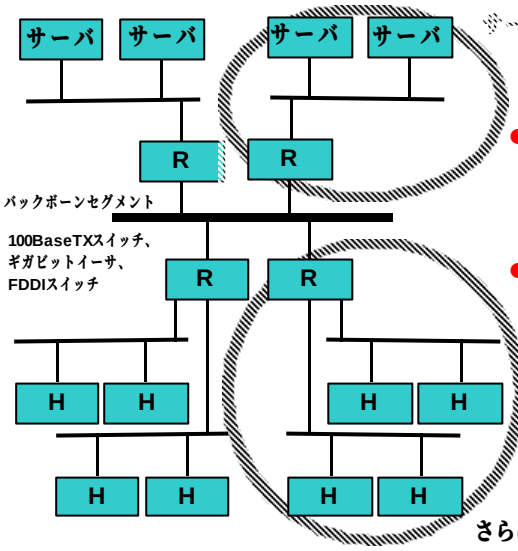
ネットワークの拡張を考慮した設計-2

サーバの増設



- サーバセグメントの安全性を保ちつつ増設する
- クライアントセグメントのbroadcast をそのセグメント内に留められるため broadcast flood現象の発生を抑制できる

ネットワークの拡張を考慮した設計-3



サーバセグメントの増設

- さらにセグメントを増設する際は、バックボーンセグメントを高速化するだけで、対応が可能
- スイッチングベースのネットワークから、左図のような大規模ネットワークに拡張する場合、リナンバリングが避けられない

さらにネットワークを追加

ネットワーク設計

- スケーラビリティを考慮するとサブネット化は不可欠
- 安全性を考慮してサーバは別のセグメントに
- トラフィックの集中するサーバ、ルータなどにはスイッチを導入する
- 規模の拡大を見越したネットワークトポロジの設計

⇩

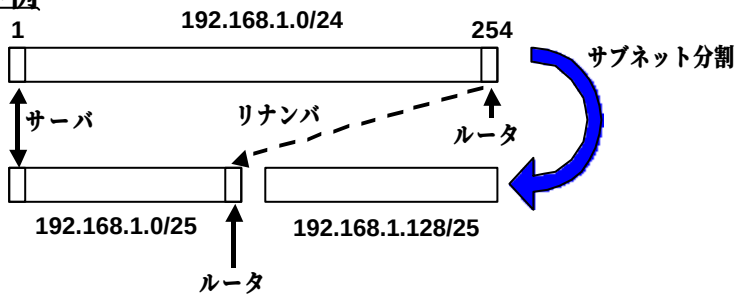
ネットワーク規模拡大を考慮したアドレス割り当て

アドレスの割り当てポリシーとは

- 規模の拡大を想定しネットワークアドレスの組織内割り当てを考える
- アドレスを先頭から詰めて使用するべきか、それとも先頭と後ろから使用していくべきか
- 各部署に割り当てる時は、どのように割り当てていけばいいのか
- 各部署内で各ホストに割り当てる場合にどのように割り当てていけば良いのか

組織全体でのアドレスの割り当て-1

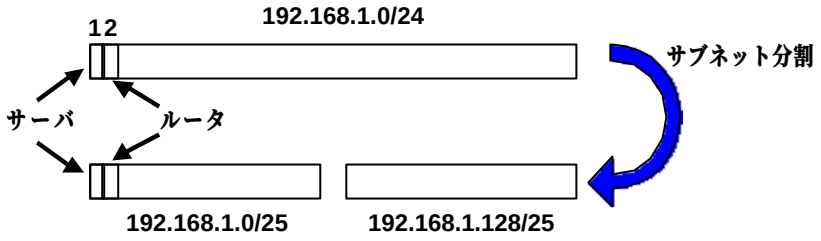
悪い例



- アドレスを先頭と後ろから使用した場合、サブネット分割を行う必要が生じた場合に、リナンバー作業を行う必要が出てしまう。

組織全体でのアドレスの割り当て-2

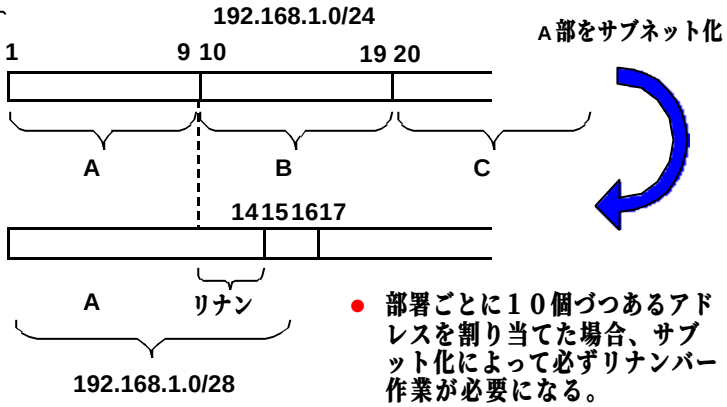
良い例



- アドレスを前詰めで使用した場合、サブネット分割を行っても、リナンバー等の無駄な作業を行う必要がない。

部署ごとのアドレスの割り当て-1

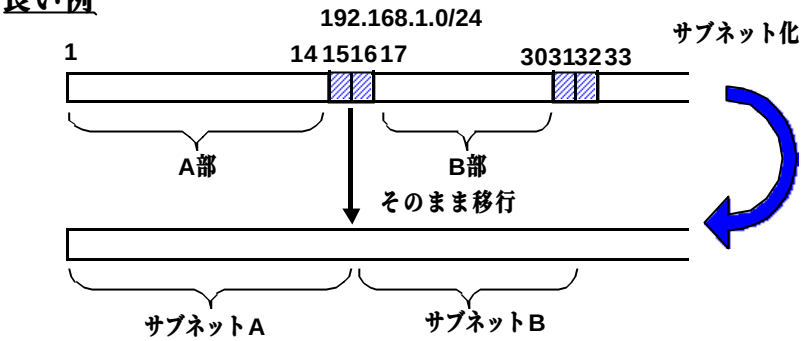
悪い



- 部署ごとに１０個づつあるアドレスを割り当てた場合、サブネット化によって必ずリナンバー作業が必要になる。

部署ごとのアドレスの割り当て-2

良い例

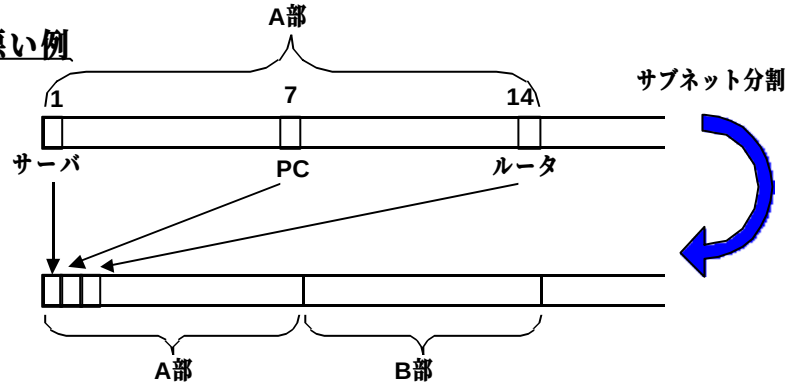


192.168.1.0/28

- 予めサブネットを意識して部署毎にアドレスを割り当てることにより、リナンバー作業を防ぐことができる

部署内でのアドレスの割り当て-1

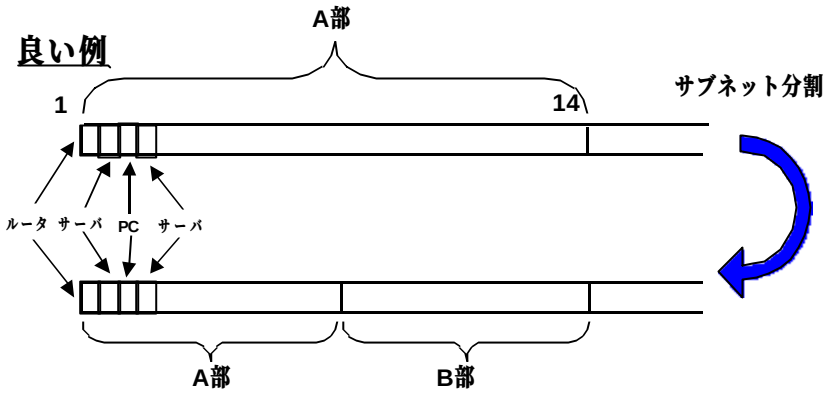
悪い例



- 部署内でルータやサーバ等利用目的別に割り当てるアドレス空間を決めてしまうと、さらなるサブネット化に対応できず、リナンバー作業が発生してしまう。

部署内でのアドレスの割り当て-2

良い例

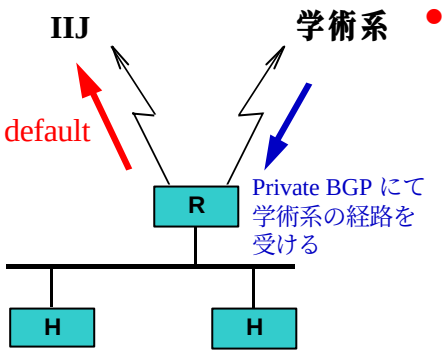


- アドレスを前詰めで使用すればさらなるサブネット化にもスムーズに対応できる

アドレスの割り当てポリシーとは

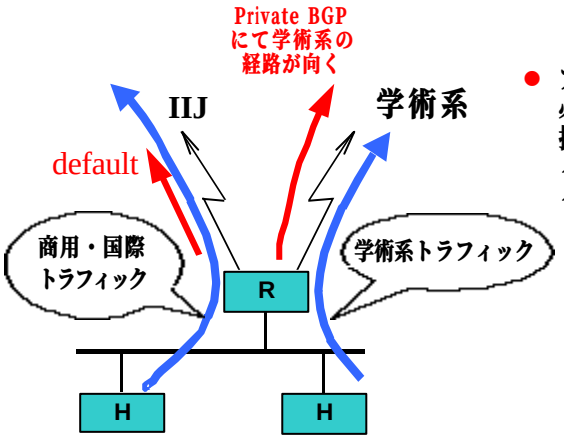
- アドレスを先頭から詰めて使用するべきか、それとも先頭と後ろから使用していくべきか
  - 先頭から詰めて使用する
- 各部署に割り当てる時は、どのように割り当てていけばいいのか
  - サブネット化を考慮して、例えばA部に1～14、B部に17～30のように割り当てる
- 各部署内で各ホストに割り当てる場合にどのように割り当てていけば良いのか
  - 先頭から前詰めで使用する

プライベートBGPによるマルチホーム接続



- プライベートAS番号を用いたBGPにより、必要に応じた経路を選択し、他の経路については左図の様にデフォルト経路を向ける

プライベートBGPによるマルチホーム接続



- プライベートBGPにより必要に応じた経路を選択することで学術トラフィックと商用・国際トラフィックの分散を行う

マルチホーム接続形態-1

- 東阪IP型(IPルーティング)
  - 東京は東京からインターネットへ接続し、大阪は大阪から接続するが、万一どちらかの回線に障害が生じた場合に、自営線を通じて互いにバックアップとして機能する接続形態。全てのアプリケーションにおいてバックアップを行うことができる。
- 東阪FW型(firewall)
  - 東阪IP型と同様の形態を取るが、ファイアウォールの内側の自営線を用いたバックアップを行う。ただしバックアップできるアプリケーションはファイアウォールの機能により限定される。
- 束ね型(cisco balance)
  - 異なるキャリア回線を束ねて使用することにより回線障害時のバックアップを実現する。ただしルータ障害には対応できない。全てのアプリケーションにおいてバックアップを行うことができる。
- アプリケーション型
  - Squidやsendmailを利用して、バックアップを実現するアプリケーション毎にバックアップの設計を行う必要があるが、ダイナミックルーティングプロトコルを用いずにバックアップが実現できる。

マルチホーム接続形態-2

- 銀行型
  - 外部からのwebに対するバックアップを実現する型。東阪FW型、アプリ型、理系総合大学型との併用が可能。
- 老舗大学型(PI、プライベートBGP)
  - プライベートBGPにより非商用の経路を選択的に受けることにより、商用・非商用トラフィックの分散を実現できる。優先度の異なるデフォルト経路によりバックアップを実現することもできる。全てのアプリケーションにおいて使用可能。
- 文系大学型(NAT、PA、プライベートBGP)
  - 商用・非商用トラフィックの分散を行うことができるが、使用できるアプリケーションはNATの機能に依存する。ただし、メールやweb配信等外部から直接コネクションがあるアプリケーションのバックアップが行えない。
- 理系大学型(NAT、PA、プライベートBGP)
  - 文系大学型の拡張型で、アプリケーション型や銀行型を併用することでアプリケーションレベルでのバックアップを実現できる。
- 総合大学型(PA、proxy、プライベートBGP)
  - Proxyサーバがプライベート BGPによって経路を選択することにより、商用・非商用トラフィック分散を行うことができる。優先度の異なるデフォルト経路によりバックアップを実現することもできる。使用できるアプリケーションはproxyサーバが中継できるものに限られる。

まとめ－1

- データリンク層とネットワーク層の違い
  - データリンクフレームは中継が起こる毎に変化する
  - IPデータグラムは変化しない
  - データリンクフレームの宛先＝IPデータグラムの宛先とは限らない
- ハブとスイッチ、スイッチとルータの違い
  - それぞれを有効に配置する
- インターネット接続にはルーティングは必須
- ダイナミックルーティングは基本を理解すれば応用できる

まとめ－2

- VLSM導入にはRIP2、OSPFを利用
- ダイナミックルーティングを利用すれば障害に強いネットワークを構築できる
- サーバなどの安全性を要求されるものは別のセグメントに配置する
- ネットワークの拡張を考慮したアドレス割り当てポリシーで運用する
- マルチホームの検討は慎重に行う