

ネットワーク構築 A to Z [II]

～ OSPFを簡単に使う最適WAN設計～

2004年12月3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@ij.ad.jp)



目的

- ダイナミックルーティングが必要な理由
- ダイナミックルーティングの種類と特徴
- 冗長化ネットワークを構築するには
- 広域Ethernetを利用したWANを構築するには
- インターネットVPNを利用したWANを構築するには
- ポリシーごとにWANを使い分けるには
- フローティングスタティックを利用したバックアップを実現するには
- OSPFをエリア分けしなければならないとき



発表内容

- スタティックルーティングとダイナミックルーティングの違い
- 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
- 広域Ethernetを利用したWAN構築
- インターネットVPNを利用したWAN構築
- ポリシーごとのWANの使い分け
- フローティングスタティックを利用したバックアップ
- OSPFエリア構築

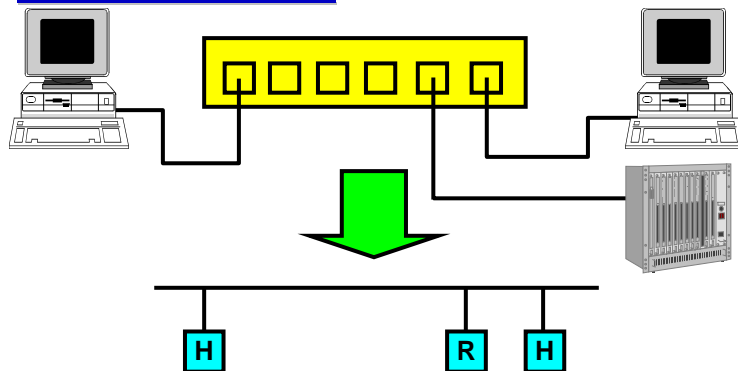


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

3

ネットワーク表記



- ハブ、スイッチなどは1本の線またはSWで表わします。
- ホストはH、A、B、C、D等で、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



2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

4

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
- OSPF解説
- トラブルシューティング

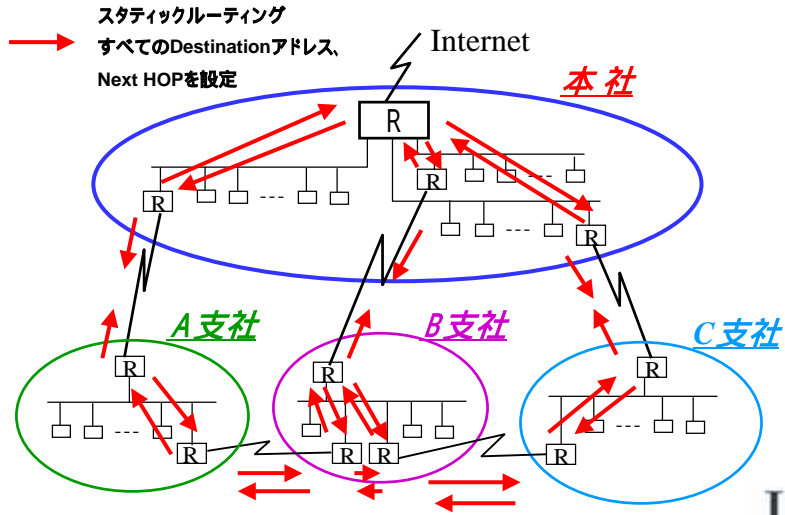


静的な経路制御と動的な経路制御

- 静的(スタティック)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(ダイナミック)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



スタティックルーティングによるネットワーク構築

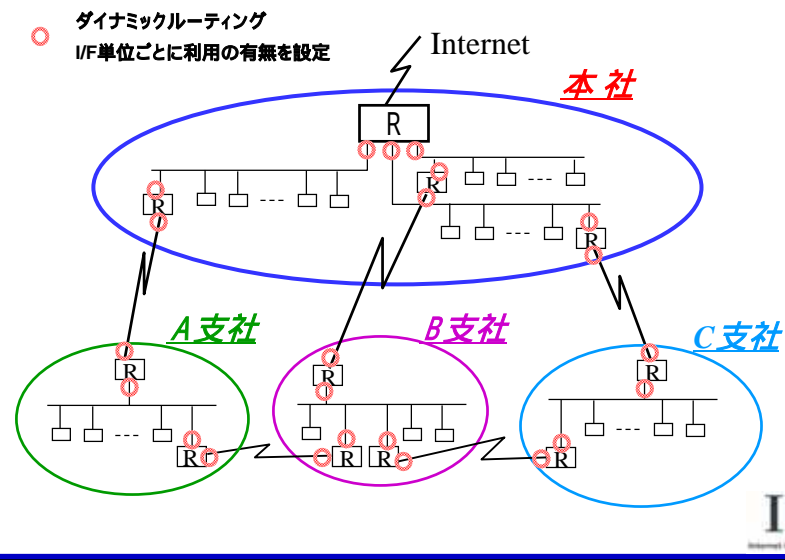


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

7

ダイナミックルーティングによるネットワーク構築

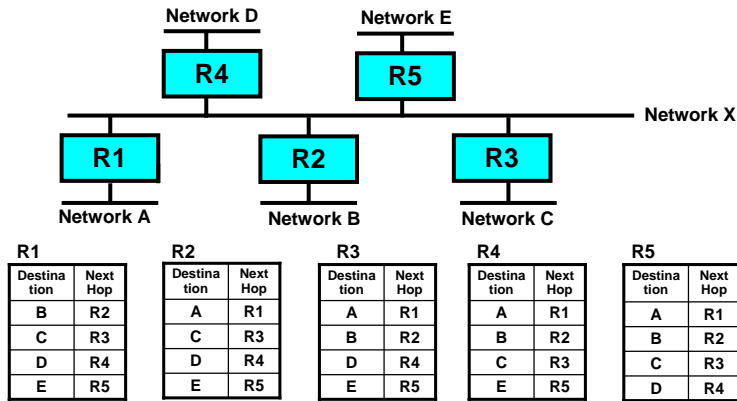


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

8

スタティックルーティングの設定



- スタティックルーティングはそれぞれのルータに設定する

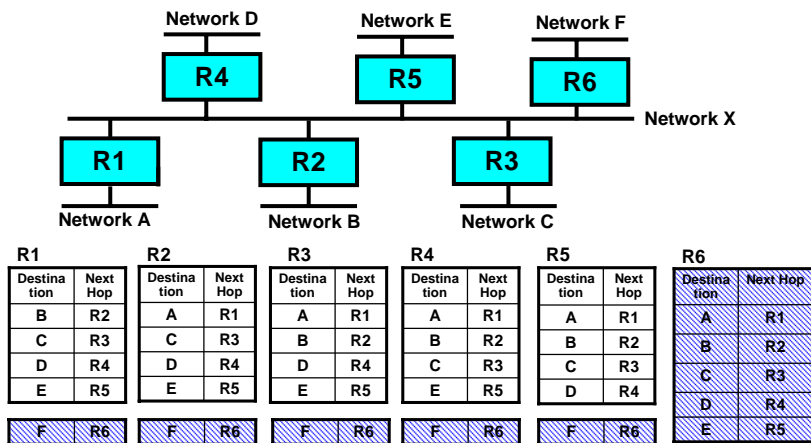


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

9

スタティックルーティングの追加



- ネットワークが追加されると全てのルータに設定を追加する必要がある

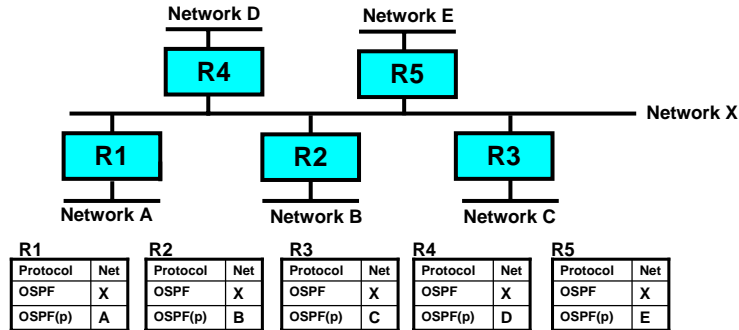


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

10

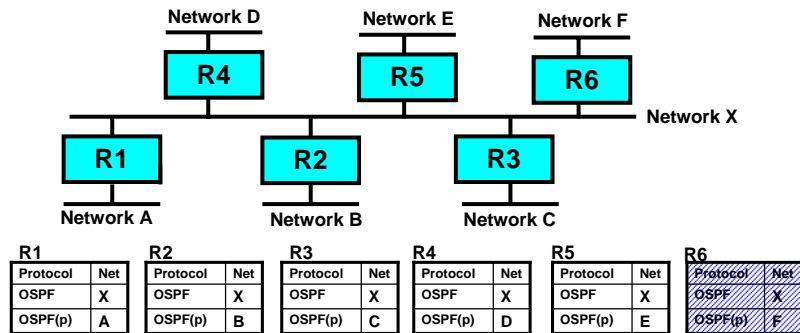
ダイナミックルーティングの設定



- ダイナミックルーティングの設定は使用するプロトコルとネットワークを指定する



ダイナミックルーティングの追加



- ネットワークが追加された場合には追加されたネットワークが接続されているルータのみに設定すればよい

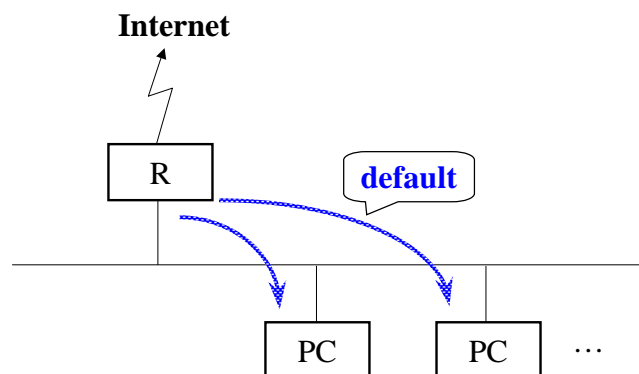


ルーティング設定まとめ

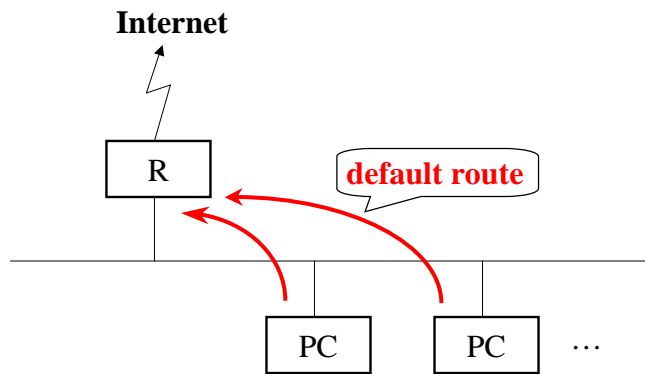
- スタティックルーティングの場合はバックボーンに新しいルータ、ネットワークが接続されると同じバックボーンを利用しているルータ全てに設定を行う必要がある
- ダイナミックルーティングを導入すると新規導入するルータにのみ設定を入れればよい
- ダイナミックルーティングを利用すると自動的にバックアップできる
- 中規模、大規模のネットワークにはダイナミックルーティングを導入したほうが良い



ダイナミックルーティング: 経路情報の伝播



ダイナミックルーティング:伝播後の経路情報



2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

15

ダイナミックルーティングプロトコルの種類

- RIP
 - RFC1058
- RIP 2
 - RFC2453
- OSPF
 - RFC2328
- BGP4
 - RFC1771



2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

16

RIP

- Routing Information Protocol version 1
- RFC1058
- アドレスのみの伝播
 - 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
- netmaskを伝播できる
 - 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を伝播できる
 - 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播する
 - 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
- BGPはここでは扱いません



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解説
 - RIPの知識をベースに解説します



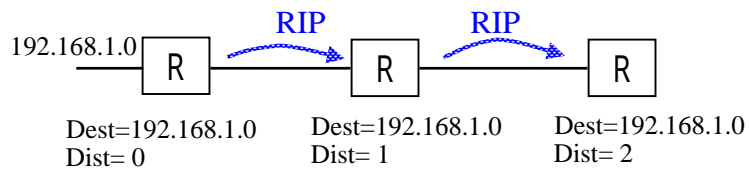
RIPの動作原理 -1

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)



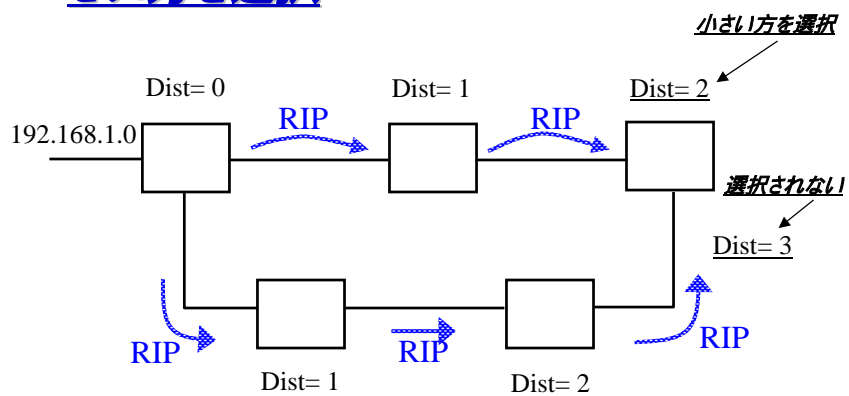
ルータを通る度にdistanceが1追加される



Dest=Destination
Dist= Distance



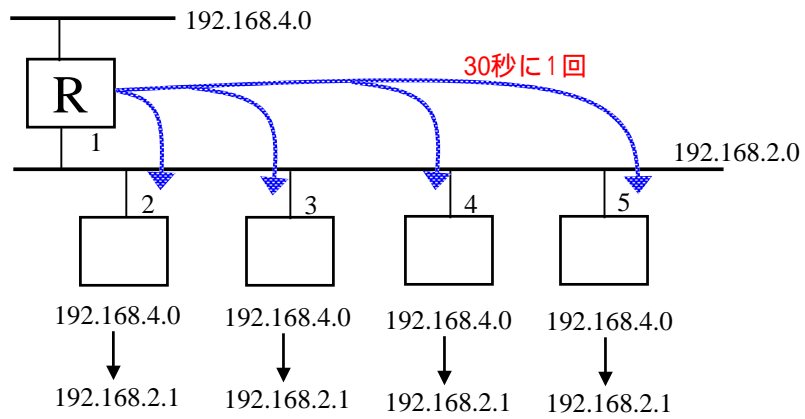
同じdestinationの場合はdistanceが小さい方を選択



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

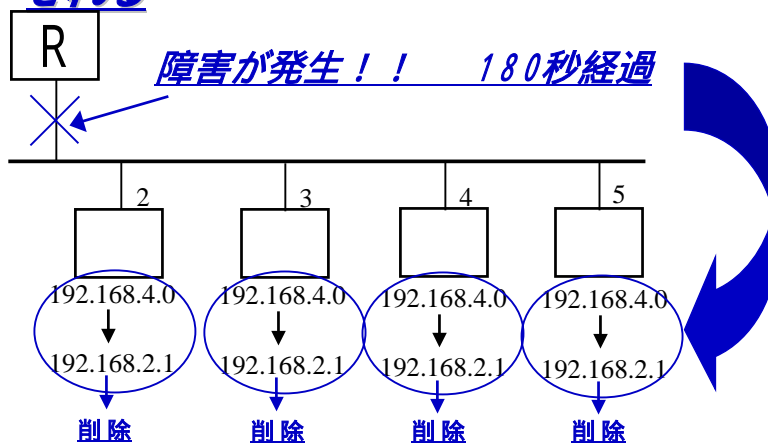


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

27

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



2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

28

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播しない
- 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

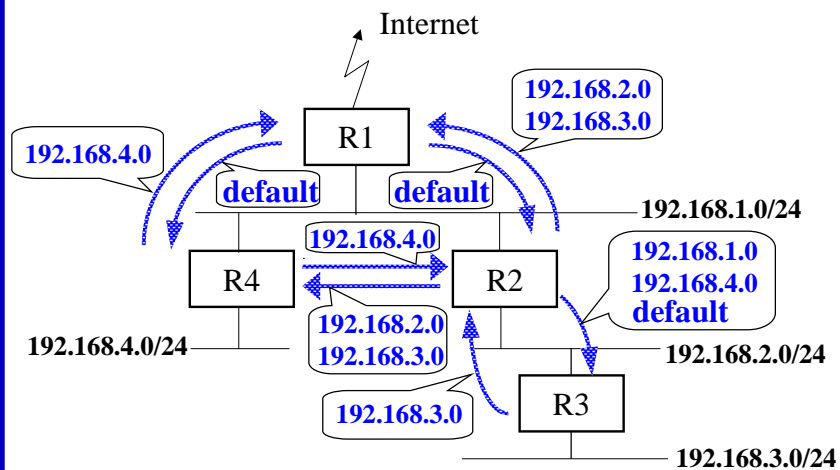


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

29

RIP伝播

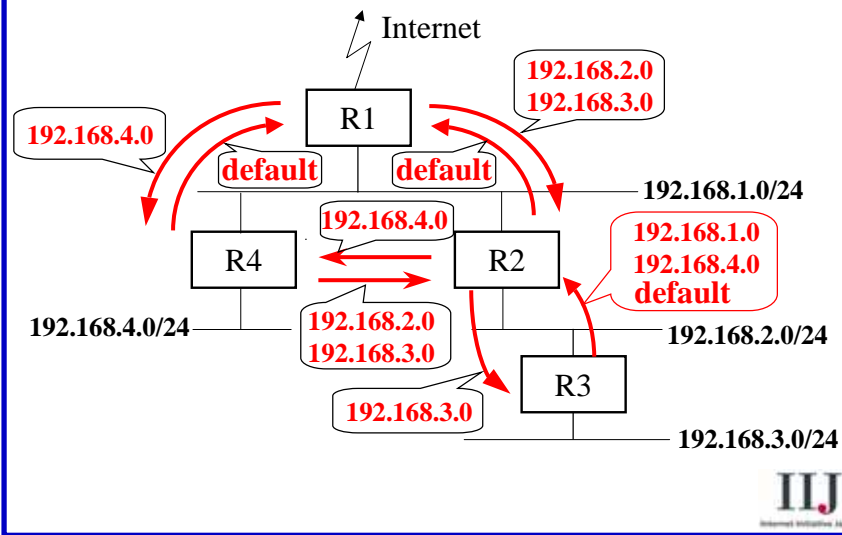


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

30

RIP伝播後の経路情報



2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

31

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

IIJ
Internet Initiative Japan

2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

32

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

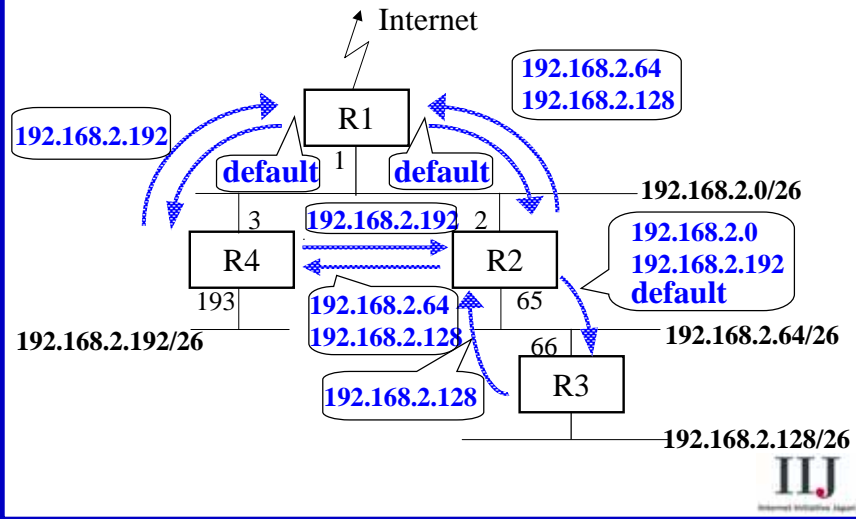


RIPのまとめ-2

- 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



2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

35

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

2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

36

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

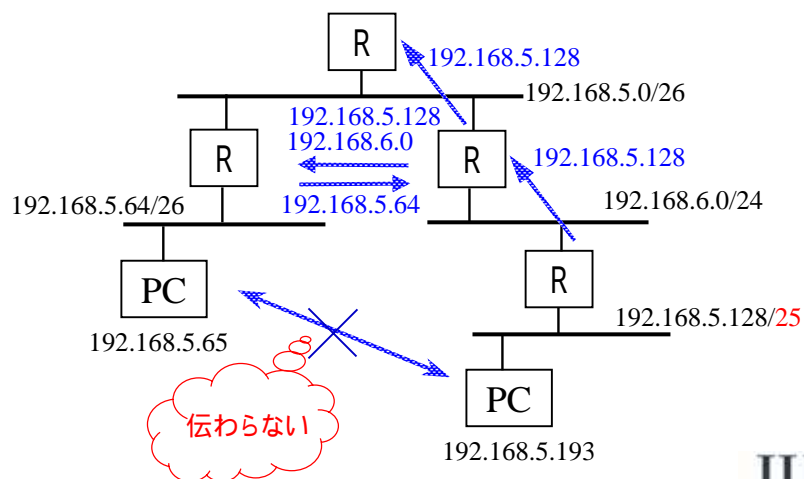


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

37

VLSMありのネットワーク構成



2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

38

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が伝播しない-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

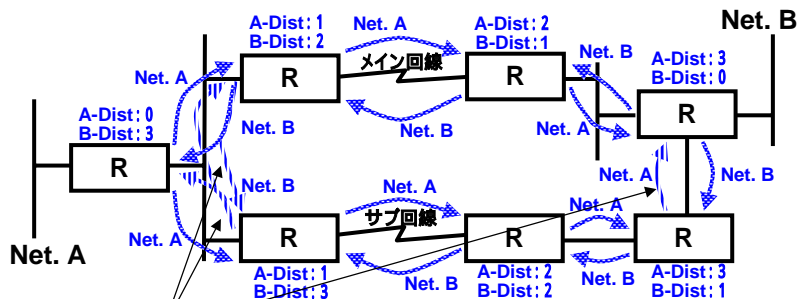


トラブルシューティング- RIPが伝播しない-2

- 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を伝播できない
 - unicastで広告するように設定する
 - unicastで広告して良いのか？



RIPを用いたバックアップ-経路の伝播(定常時)

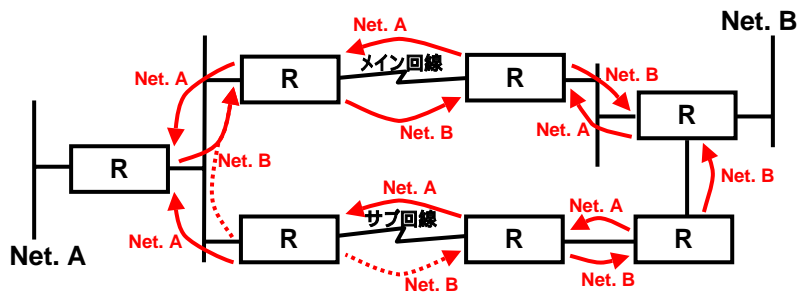


他方よりもDistanceが
大きい
ため
選択
され
ない

- 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



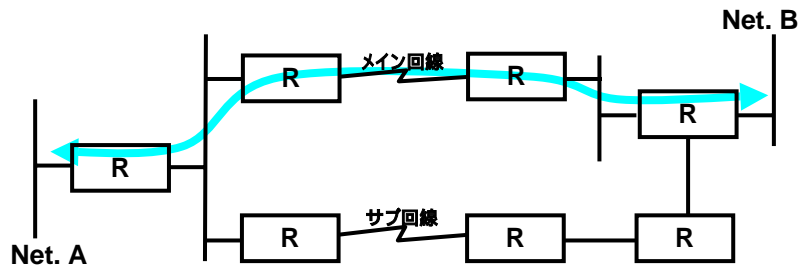
RIPを用いたバックアップ-ルーティングテーブル(定常時)



- RIPの経路情報が伝播することにより、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

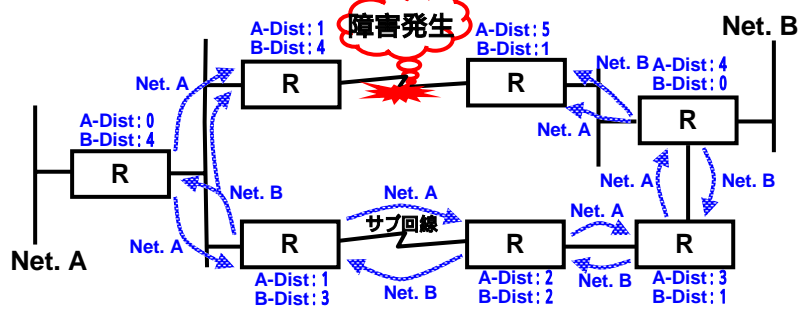


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

45

RIPを用いたバックアップ-経路の伝播(障害時)



- メイン回線に障害が発生したため、経路情報の伝播が変化する

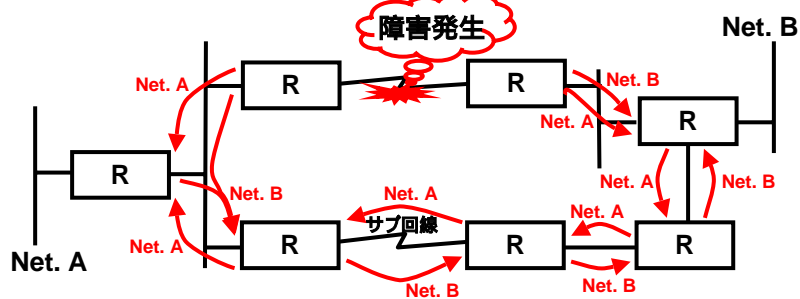


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

46

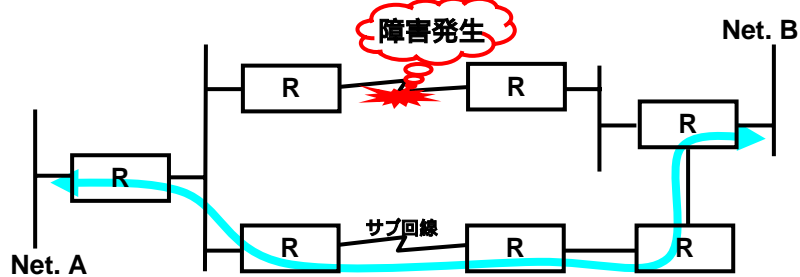
RIPを用いたバックアップ-ルーティングテーブル(障害時)



- 経路情報の伝播が変化するため、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解説 - 1

● 解説方針

- ここではOSPFを知らない方のために一般的な利用法について解説します。
- わかりやすさを重視して説明するため、RFCで定義されている厳密なOSPFの定義とは異なる部分もありますが、ご了承願います。
- 大規模ネットワークではBGPとの連携は欠かせませんが、ここでは説明しません。



OSPF解説 - 2

● Link State型ルーティングプロトコル

- ネットワークトポロジをLSA(Link State Advertisement)と呼ばれる形式でデータベース化し、最適な経路を選択する。
 - RIPやBGPと異なり、単純な経路交換を行なわないため、経路フィルタをかけることは難しい
- トポロジに変更が合った場合にすぐ変更がかかる
- ルータ故障検出も可能
 - HELLOパケットによりルータの故障を検出し、バックアップ経路を選択できる。
 - 切り替え時間がRIPよりずっと早い(数秒~1分程度)

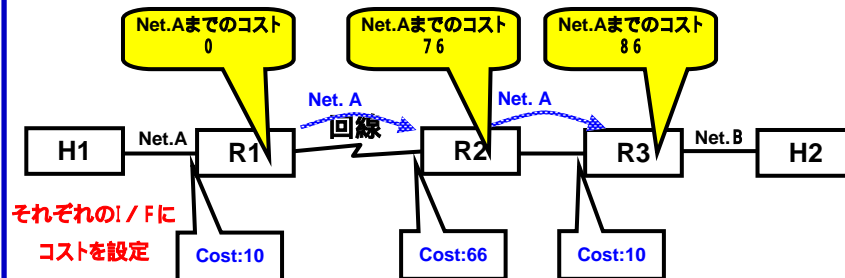


OSPFコストとは

- OSPFではRIPでいうDistanceの代わりにコストを利用する
 - OSPFコストは0 ~ 65535の値を取る
 - インターフェース毎に自由にコストを設定することができる
 - コストは小さければ小さいほどネットワーク的に近距離に見せられる
 - ルータによっては回線速度に応じて自動的にコストを付与するものもあるが、ネットワークの高速化などに対応できなくなるだけでなく、運用が困難になるため、明示的に設定したほうが良い



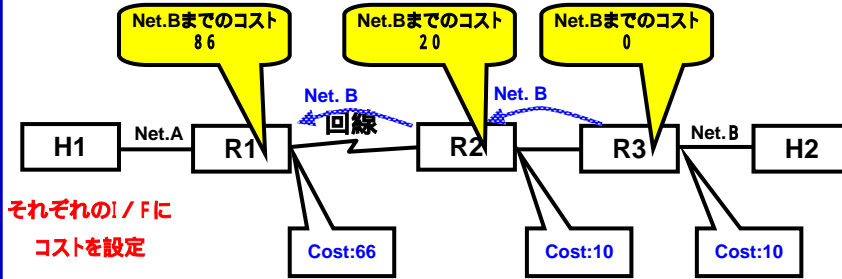
簡単なOSPFコストの計算法 - 1



- R1から見たH1への経路
 - R1は直接Net.Aに接続されているため、同じNet.Aに接続されているH1はコスト0として見える
- R2から見たH1への経路
 - R2からは(R1のI/Fに設定されたNet.Aのコスト+R1と接続するI/Fに設定されたコスト)となる
- R3から見たH1への経路
 - R3からは(R2から見たNet.Aのコスト+R2と接続するI/Fに設定されたコスト)となる



簡単なOSPFコストの計算法 - 2

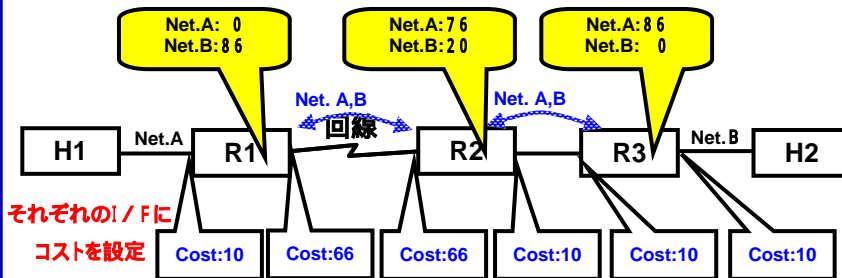


それぞれのI/Fに
コストを設定

- R3から見たH2への経路
 - R3は直接Net.Bに接続されているため、同じNet.Bに接続されているH2はコスト0として見える
- R2から見たH2への経路
 - R2からは(R3のI/Fに設定されたNet.Bのコスト+R3と接続するI/Fに設定されたコスト)となる
- R1から見たH2への経路
 - R1からは(R2から見たNet.Bのコスト+R2と接続するI/Fに設定されたコスト)となる



簡単なOSPFコストの計算法 - 3



それぞれのI/Fに
コストを設定

- 同じI/Fに同じコストを付けることにより、行きと帰りのコストを一致させることができる
- 行きと帰りで異なるコストを付与することもできるが、管理が煩雑になるため、理由なく行なうべきではない
- ここで示した図は経路を交換しているように書かれているが、実際はトポロジデータベースの交換により経路を確定している

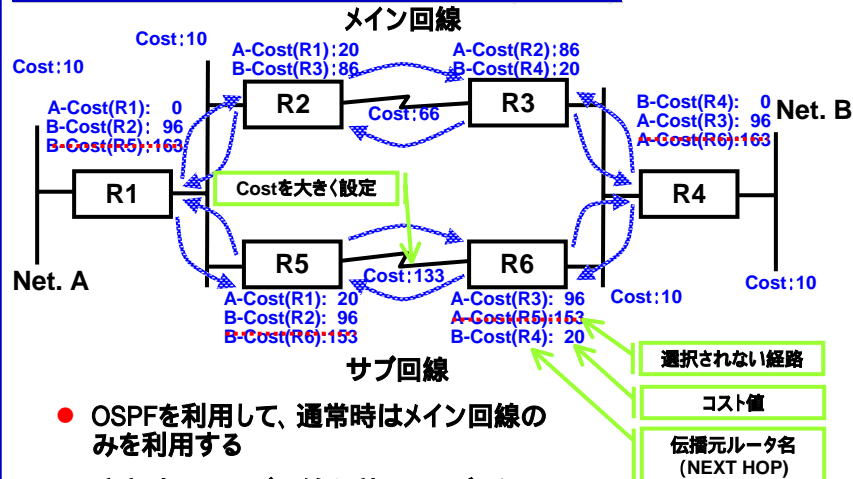


バックアップ、バランシングを行なうには

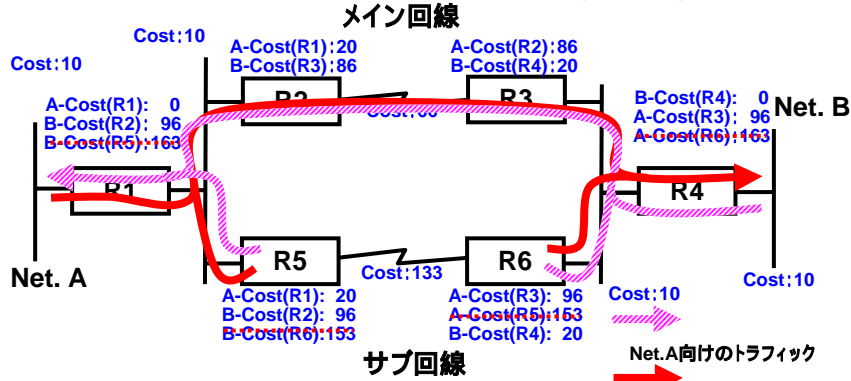
- OSPFでは複数の経路を持った場合にバックアップやバランシングを行なうことができる
- 異なるコストの経路がある場合
 - コストが小さい経路をメインとして利用しコストが大きい経路をバックアップとして利用できる
- 同じコストの経路がある場合
 - バランシングを行ない、トラフィック分散することが可能
 - バランシングを行なっている経路の1つが切断されても残った経路でバックアップすることも可能



OSPFを用いたバックアップ-経路の伝播(通常時)



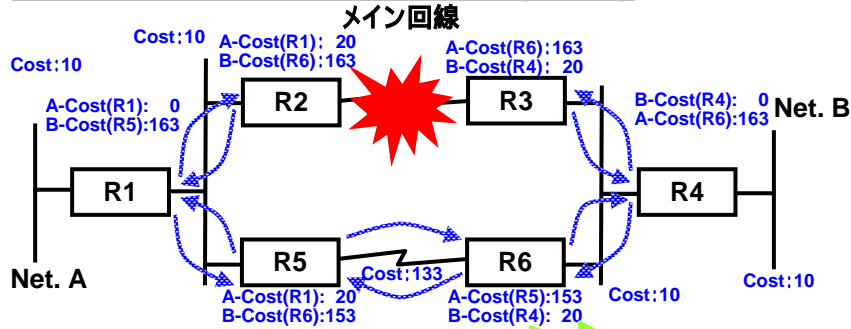
OSPFを用いたバックアップ-トラフィックの流れ(通常時)



- サブ回線にもOSPF HELLOパケットが流れるため、トラフィックをゼロにはできない



OSPFを用いたバックアップ-経路の伝播(障害時)

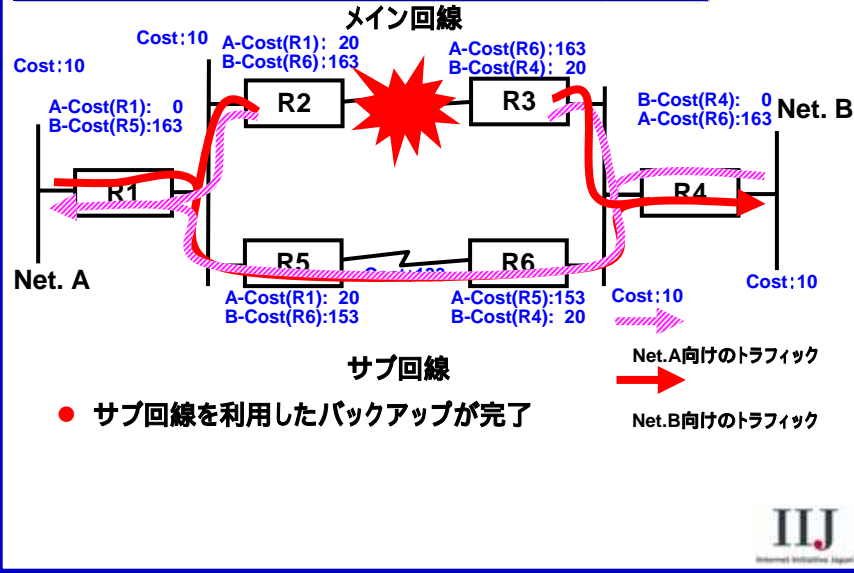


- 回線の切断によりR2-R3間のネットワークが削除される

コスト値
伝播元ルータ名 (NEXT HOP)



OSPFを用いたバックアップトラフィックの流れ(障害時)



2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

59

OSPFバックアップルーティングの特徴

- RIPとは異なり、すばやいバックアップが可能
- バックアップ用の回線上もOSPF HELLOが流れるため、サブ回線を切断することはできない
 - ISDNなどでバックアップさせるにはOSPFだけのチューニングでは難しい
- 2本の回線を別々の用途に利用して障害時にそれぞれバックアップとして利用することが可能

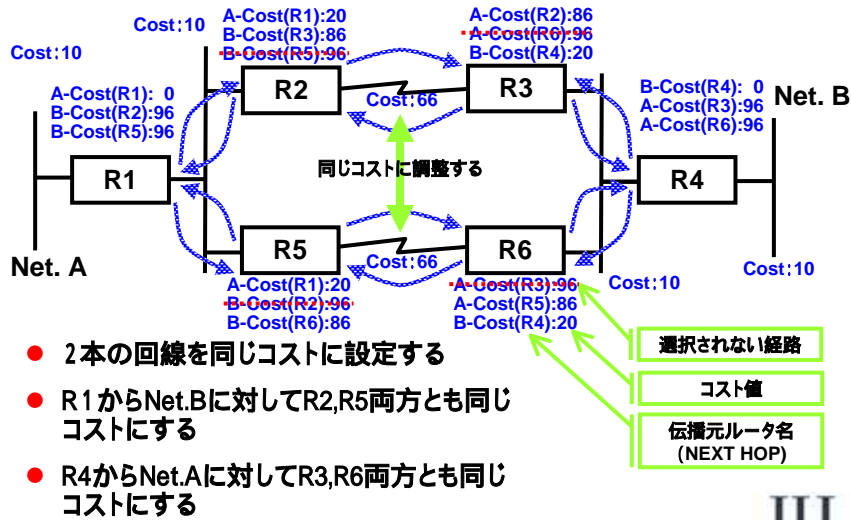
IIJ
Internet Initiative Japan

2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

60

OSPFを用いたバックアップ、バランシング-経路の伝播(通常時)



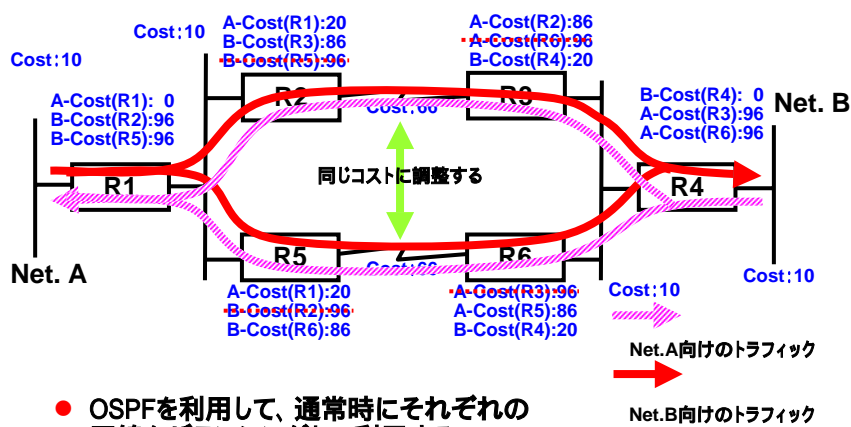
- 2本の回線を同じコストに設定する
- R1からNet.Bに対してR2,R5両方とも同じコストにする
- R4からNet.Aに対してR3,R6両方とも同じコストにする

2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

61

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)



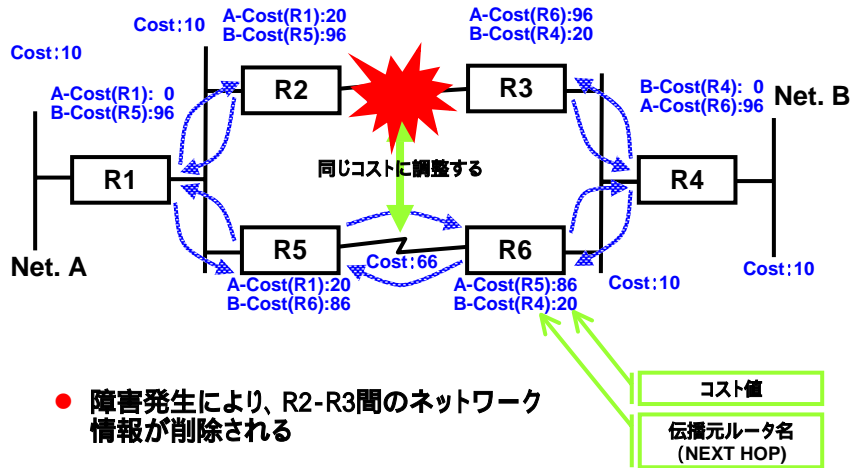
- OSPFを利用して、通常時にそれぞれの回線をバランシングして利用する

2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

62

OSPFを用いたバックアップ、バランシング-経路の伝播(障害時)

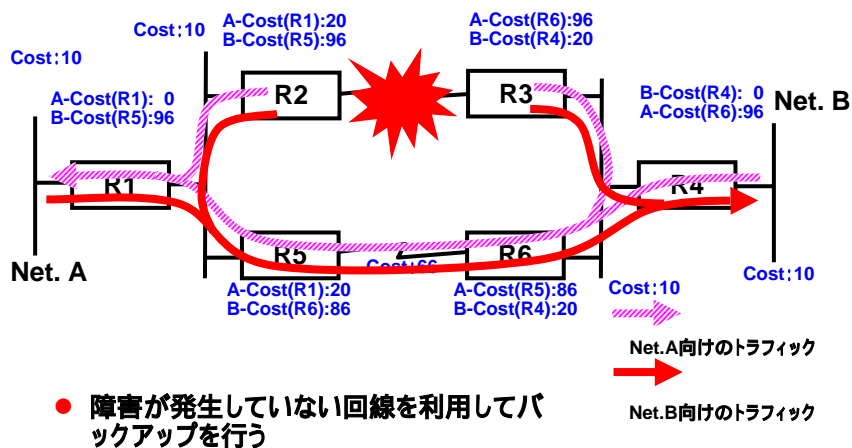


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

63

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)



2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

64

バックアップ、バランシングの特徴

- 障害発生時には50%の帯域でバックアップ
- バランシングは基本的に1:1でバランスするため、速度の異なる回線をバランスさせることは難しい
- 2本の回線を有効に利用し、回線コストを抑えることができる
- LAN等に利用すると100Mbpsメディアを200Mbpsメディアとして利用することもできる



初心者のためのOSPF設定 - 1

- エリア
 - 必ず0を設定する
 - OSPFでは経路の集約のためにエリアという概念があるが、小規模なネットワークではバックボーンエリア=エリア0だけで構築すればよく、エリアを分けて構築する必要はない
 - エリア0以外のエリアは必ずエリア0と接している必要があるため、むやみにエリア分けをするとバックボーンの拡張が難しくなる
 - ISPなど大規模ネットワークとなるとBGP+OSPFが主流であり、経路の集約という観点ではBGPのほうが優れているため、バックボーン以外のエリアを積極的に使っていくことはあまりない
 - 使用機器などの制限によりBGPが利用できず、OSPFで多くの経路を扱う場合にはエリアを利用して経路集約を図る必要がある
- デフォルトルート
 - 必ずstaticなどでデフォルトルートを確認してからOSPFでデフォルトルートを流す
 - 余力があればExternal Type 1で流す



初心者のためのOSPF設定 - 2

● Staticからの経路注入

– デフォルトルートなどと同じくExternal Type 1で流す

- OSPFではOSPF以外のstaticやRIPなどから経路を注入するときExternal Type 1とExternal Type 2が選べるようになっている

■ External Type 1とは

- 注入時に付与したコストに、注入された場所から実際にOSPFの経路を受け取るルータまでのOSPFコストを加えて評価する。同じ経路が複数注入されたときに最も近い出口から出るように制御するために使われる。Staticは注入された箇所が最も近いと判断できるため、Type 1が向いている。

■ External Type 2とは

- 注入時に付与したコストをそのまま維持する。同じ経路が複数注入されたときに注入の際に付けられた優先順位に基づいて評価される。これはBGPなど他のプロトコルの情報をOSPFで実現するために有効な手法だが、現状BGPをそのままOSPFには流せないため、あまり意味がない

- Ciscoのルータはデフォルト設定がExternal Type 2であるため、注意が必要

■ External Type 1とExternal Type 2を混ぜない

- OSPFコストとは別にExternal Type 1 > External Type 2という優先順位があるため、障害の切り分けが難しくなる



初心者のためのOSPF設定 - 3

● ルータID

– 小規模では特に気にしなくても良いが、loopbackインターフェースを設定したほうが良い。

- OSPFではルーター間通信にルータID(ルータについてのIPアドレス)を用いる。
- 通常はloopbackインターフェースを設定するとそのアドレスが使われる
- 同じアドレスを複数のルータのloopbackインターフェースに付けると誤動作するため、注意が必要

● ルータを立ち上げる順番

– 能力が高く、負荷が低いルータを先に立ち上げたほうがよい。

- OSPFではDR(Designated Router)「指定ルータ」、BDR(Backup DR)、DROTHERが立ち上がった順に決まり、Ethernetなどマルチアクセスメディアの通信はDRが情報を管理するため、処理能力の余裕があるルータに行なわせたほうが良い。
- 小規模では意識しなくても問題が発生しないことがほとんど。



トラブルシューティング-RIPv2とOSPFが伝播しない

- 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を利用すべき
- 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
- バランシングなどを行なう場合はOSPFを用いる



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

- 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

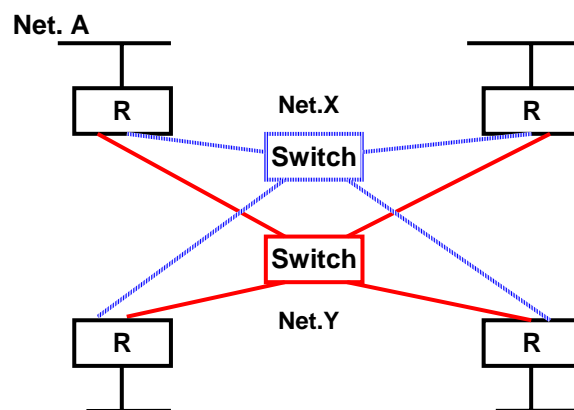


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

71

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

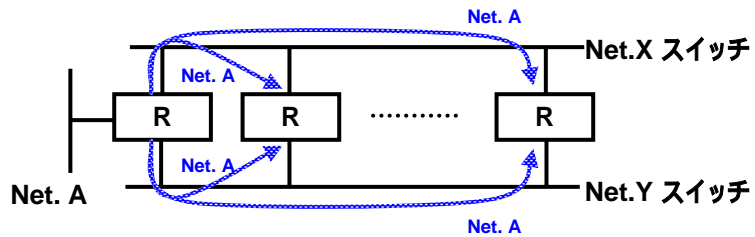


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

72

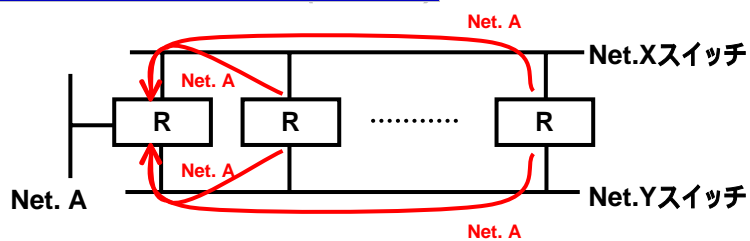
デュアル構成 + OSPFを用いたバックアップ、バランシング 経路の伝播(通常時)



- OSPFで Net.Aの経路情報を広告する
- 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播する



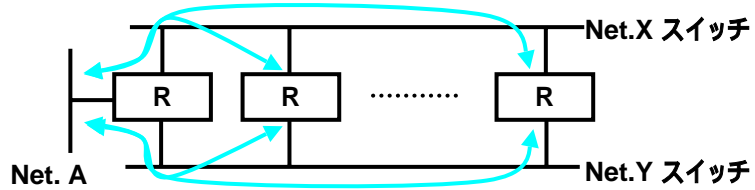
デュアル構成 + OSPFを用いたバックアップ、バランシング ルーティングテーブル(通常時)



- 伝播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播してきたため、2つの経路情報が設定される



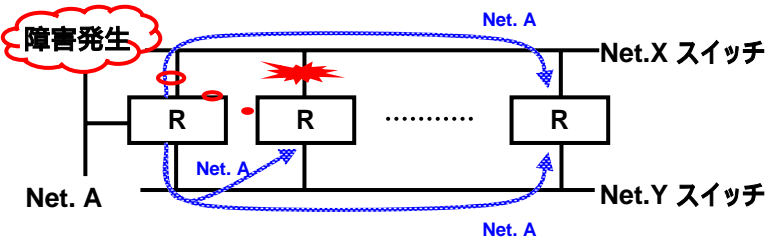
デュアル構成 + OSPFを用いたバックアップ、バランシング
-トラフィックの流れ(通常時)



- 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



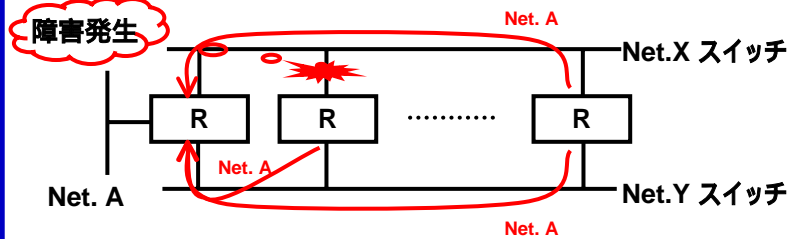
デュアル構成 + OSPFを用いたバックアップ、バランシング
-経路の伝播(障害時)



- 障害発生により、経路情報の伝播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)



- 伝播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

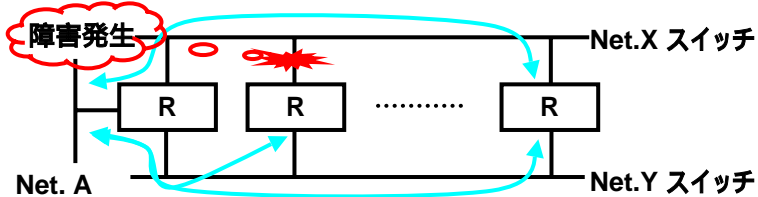


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

77

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

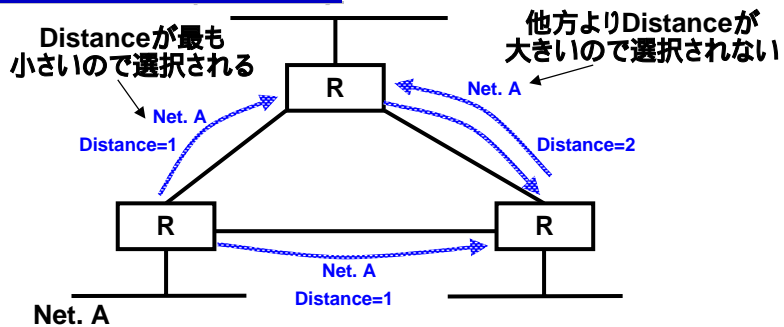


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

78

リングトポロジによるバックアップ -経路の伝播(通常時)



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

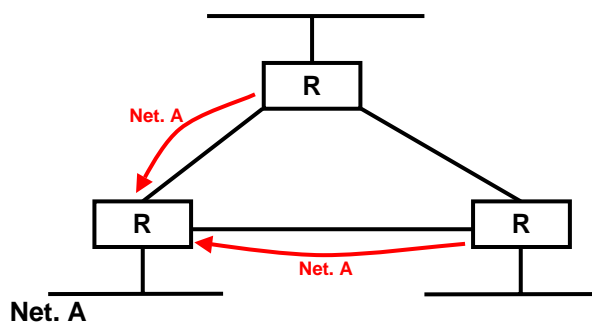


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

79

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)



- 伝播した経路情報から、各ルータに経路情報が設定される

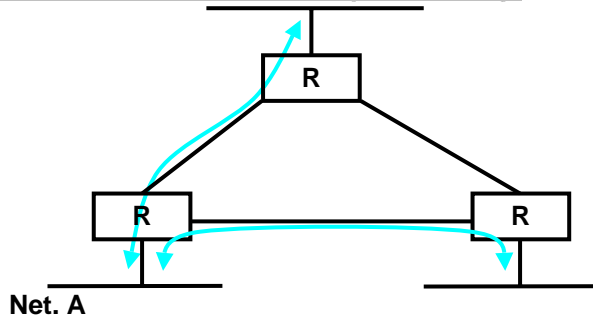


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

80

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

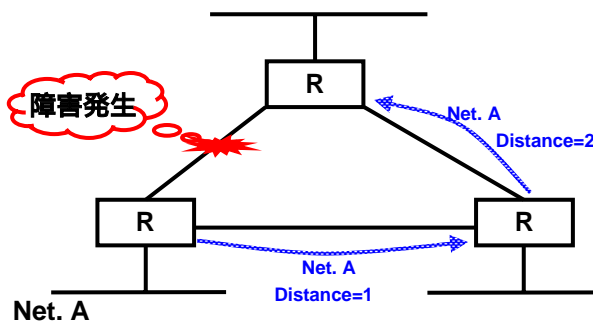


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

81

リングトポロジによるバックアップ - 経路の伝播(障害時)



- 障害により、経路情報の伝播に変化が生じる

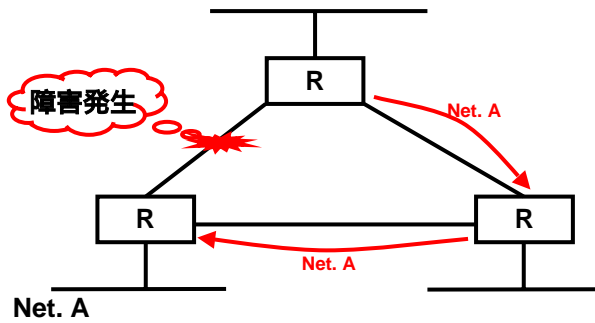


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

82

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)



- 伝播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

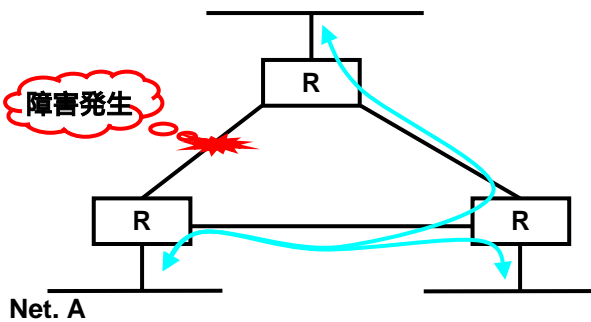


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

83

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



2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

84

WAN構築

ここでは利用回線別のWAN構築の方法について解説します

- 広域Ethernetを利用したWAN
- インターネットVPNを利用したWAN

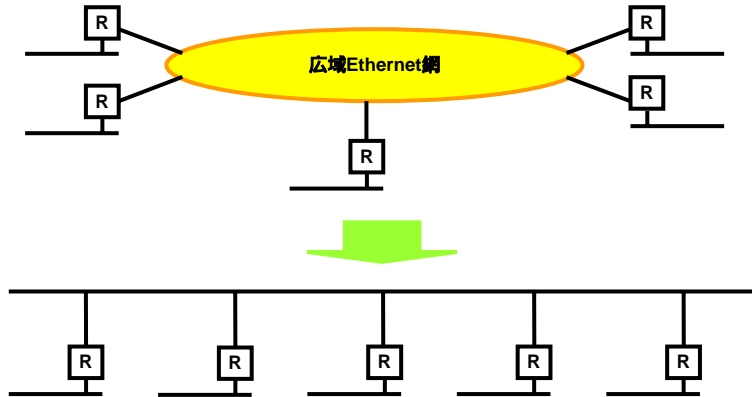


広域Ethernetを利用したWAN

- 広域Ethernetを利用する理由
 - 安価
 - IP以外のパケットが通る(SNAなど)
 - ATMやPOSなどの高価なWAN I/Fが不要
 - ルータを利用せずにHUBだけでネットワークが構築できる
 - Tag VLANを利用して複数のVLANを複数拠点に容易に持っていくことができる
- 今回とりあげるポイント
 - IPのみを利用、ルータを利用、ダイナミックルーティング



ネットワーク構成



- 広域Ethernet網はLANのEthernetと同様に見える
- 基本的にはLANと同じ設計手法が使える

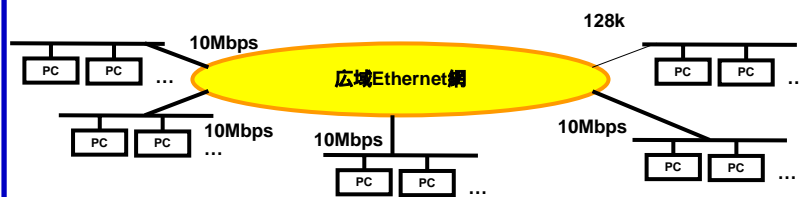


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

87

HUBのみで構成した場合



- 広域EthernetはLANと同様にHUBのみでもネットワークを構成することができる。

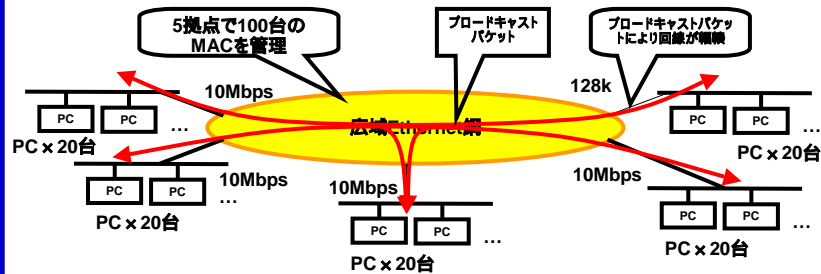


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

88

HUBのみで構成した場合の問題点



- HUBのみで構築し、PC端末を直接広域Ethernetに接続すると広域Ethernet内で管理すべきMACが増加する。
- これによりARPやWindows系のブロードキャストが増加し、回線の細い拠点で輻輳する。

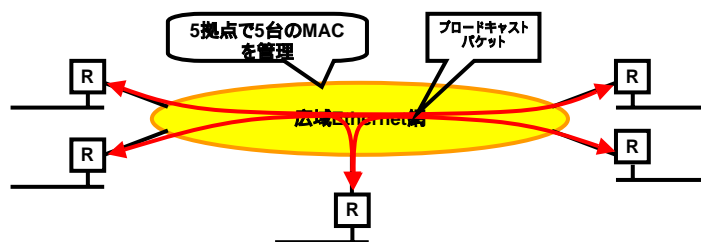


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

89

ルータを設置した場合



- ルータを設置した場合には広域Ethernet内のMACはルータの台数に限られるため、ブロードキャストの増加を防ぐことができる。



2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

90

ルータを設置すべきか

- ルータを設置すべきか、HUBのみで構築すべきか
 - 広域EthernetはHUBだけで容易にネットワークを構築できるが、スケールするネットワークとするためにはルータを設置すべきである。
 - 小規模拠点などHUBのみで構築が必要な場合にはルータ接続拠点とは異なるVLANで構築することが望ましい。

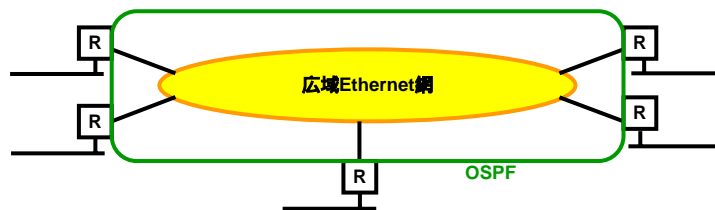


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

91

広域EthernetでのOSPFの利用



- 広域Ethernet網でのOSPFの利用
 - 広域EthernetではLANと同様にダイナミックルーティングが利用できるが、一般的にはOSPFを用いられることが多い。
 - 広域Ethernet網でのOSPF利用のポイントについて解説する

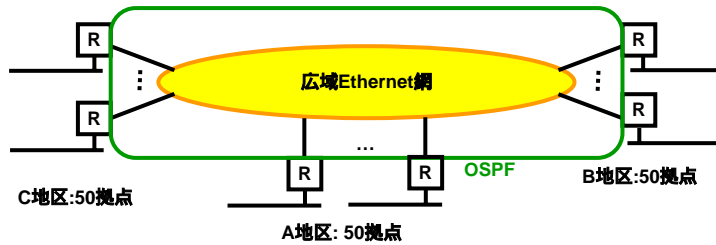


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

92

多拠点でのOSPFの利用



- 多くの拠点を1つの広域Ethernet網で結び、OSPFを動かす。
- 図ではA,B,C地区それぞれに50拠点接続しており、合計150台のルータが同一の広域Ethernet網を利用している。

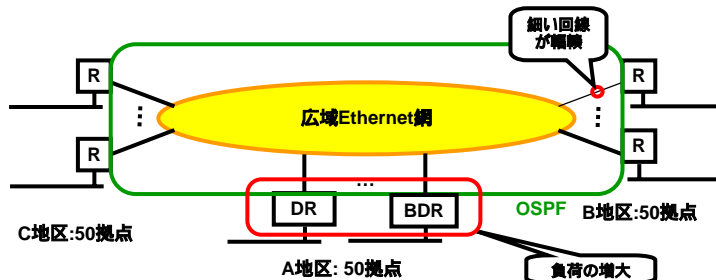


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

93

OSPF 利用時のトラブルシューティング



- 細い回線の輻輳
 - OSPFのHelloパケットにより細い回線が輻輳してしまう
- DR/BDRの負荷増大
 - DRおよびBDRに負荷が集中し、不安定となる
 - DR,BDRに高いスペックのルータが必要となる

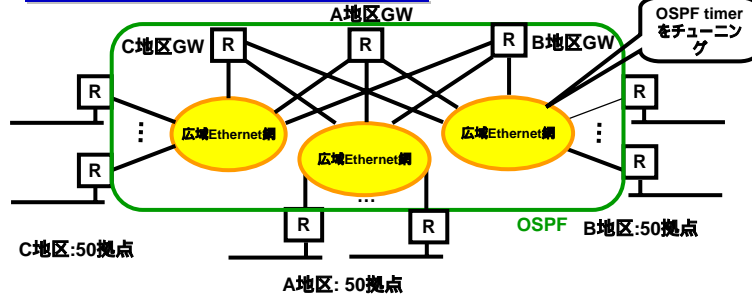


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

94

OSPFトラブル解決法



- 広域Ethernet網の分割及び中継ルータの設置
 - 巨大すぎる広域Ethernet網を1セグメント50台程度として分割
 - それぞれの広域Ethernet網を中継するルータを設置
 - 広域Ethernetを分割することで、OSPFマルチキャストを減らすことができる
 - セグメントの分割により、DR、BDRを分散配置でき、負荷を下げることもできる
- OSPF timerのチューニング
 - 細い回線を収容している広域Ethernet網のOSPFのHello間隔を伸ばし、輻輳を回避する



広域Ethernetを利用したWAN:まとめ

- HUBのみで構築すべきか、ルータを設置すべきか
 - ルータを設置したほうがスケールする
 - HUBのみの構成とルータ設置の構成が混在する場合にはTag VLANなどを利用して異なるネットワークに収容する
- ルータの設置台数が50台を超えるようであれば広域Ethernetを分割して、それぞれのネットワークを接続する中継ルータを用意する
- 細い回線を利用する場合にはOSPF timerをチューニングして輻輳しないようにする

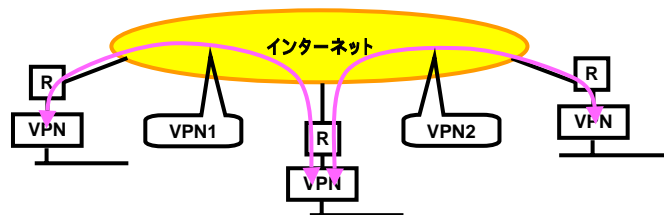


インターネットVPNを利用したネットワーク

- インターネットのプロードバンド化と低価格化、VPN装置の低価格化と高性能化により、急激にインターネットVPNが普及してきました。
- ここではネットワークという切り口からWANとしてインターネットVPNを利用していきます
- VPNにはさまざまなプロトコル、暗号化技術、認証システムなどの要素がありますが、プライベートネットワーク間で影響を受ける部分にのみ着目して解説します。暗号化されたパケットの状態など、プライベートネットワーク間では隠される要素につきましてはここではブラックボックスとして扱います。



一般的なインターネットVPN構成



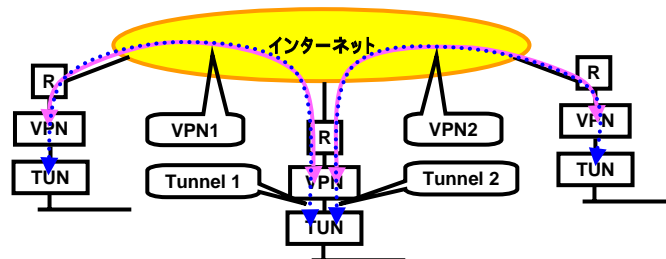
- 一般的なインターネットVPNの構成
 - インターネット接続ルータの下にVPN装置を設置し、VPN装置間でVPNを張る
 - VPNに流せるパケットはVPN依存
 - 暗号化パケットのスループットの低いVPN装置ではVPN間でOSPFなどのダイナミックルーティングが利用できないことが多い



スループットとダイナミックルーティングなどを両立するためには



ネットワーク化されたインターネットVPN構成



- ネットワーク化されたインターネットVPN構成
 - インターネット接続ルータの下にVPN装置を設置し、VPN装置間でVPNを張る(IPsecなど)
 - VPN装置の内側にtunnelルータを設置し、VPN上にtunnelを張る(GRE、ipipなど)
 - Tunnelは暗号化する必要はない
 - Tunnelは専用線と同等に見えるため、ダイナミックルーティングが利用できる
 - VPN装置はダイナミックルーティングを利用できなくてよい



2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

99

VPNで利用されるプロトコル

- IPsec
 - IP Security Protocol
 - 認証、暗号化を行う
 - RFC2401 ~ 2412, 2451, 2857, 3526, 3554, 3566, 3602
 - Protocol 50(ESP:encapsulating security payload)
 - Protocol 51(AH:authentication header)
- GRE
 - Generic Routing Encapsulation
 - レイヤ3 tunnelを行う
 - RFC1701, 1702
 - Protocol 47(GRE)
- IPIP
 - IP Encapsulation within IP
 - レイヤ3 tunnelを行う
 - RFC2003
 - Protocol 4(IP-ENCAP:IP encapsulated in IP)
- GIF
 - Generic Tunnel Interface
 - IPIPをUNIXなどで扱うときに利用される
 - IPIP tunnelのことをGIF tunnelと呼ぶこともある

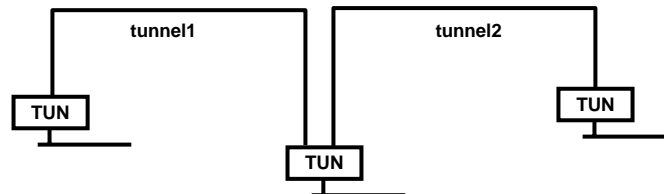


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

100

ネットワーク化されたインターネットVPN構成



- プライベート側からみたネットワーク構成
 - Tunnelルータ間はtunnel1およびtunnel2の2つの専用線で接続されていることと同様に扱える
 - OSPFなどのダイナミックルーティングを容易に扱うことができる

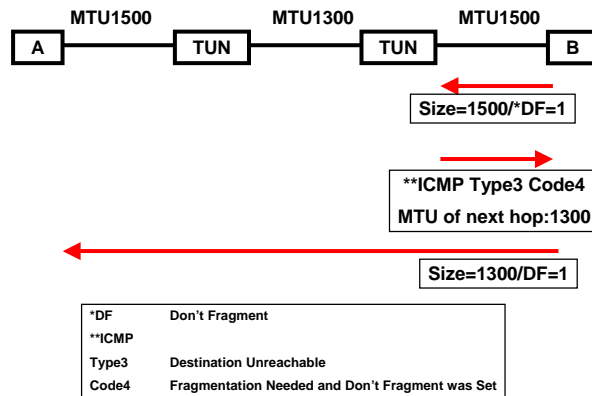


インターネットVPNの解決すべき問題点

- MTUが1500より小さくなることによる問題点
 - インターネットVPNなど既存のネットワークの上にtunnelを張って利用する場合にはMTU(Maximum Transmission Unit)が1500より小さくなることによる問題が発生する
 - Path MTU Discovery Blackhole問題
 - RFC1191 Path MTU Discovery
 - RFC2923 TCP Problems with Path MTU Discovery
 - 詳しくは後述
 - Path MTU Discovery Blackhole以外のMTU1500を必要とするアプリケーションの問題
 - DF=1で送信を行うLANアプリケーション
 - フラグメントによるパフォーマンスの低下
 - 小さいMTU個所を通過する際にフラグメントが許可されていれば、フラグメントすることによりすべてのサイズのIPパケットを通過させることができる
 - ただし、フラグメントによりスループットが低下する恐れがある



Path MTU Discovery の動作原理



● Path MTU Discoveryの原理

- DF=1としたIPパケットを送出し、Destination Unreachableが戻ってきたときに適切なIPパケットサイズに調整して送信することで、エンド-エンド間の最大で最適なMTUを利用する仕組み

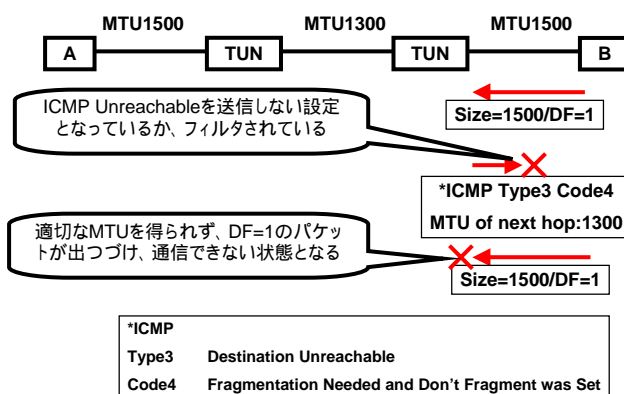


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

103

Path MTU Discovery Black hole 問題



● Path MTU Discovery Black holeとは

- Path MTU Discoveryの原理で重要な役割を持つICMP Unreachableがフィルタされることで、適切なIPパケットの送信が行えず、通信できなくなる状態のこと

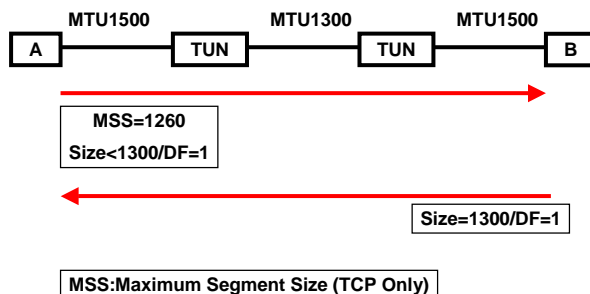


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

104

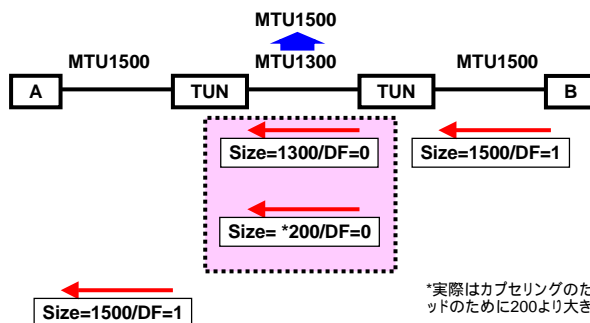
Path MTU Discovery Black hole問題の解決法1



- TCPのMSSを利用する
 - TCPでは一度に送出する最大のセグメントサイズMSSを指定することができる。このパラメータをMTUが小さくなるポイントで書き換えることで、TCPに限りPath MTU Discovery Black holeを解決することができる



Path MTU Discovery Black hole問題の解決法2



- TunnelのMTUを1500に拡張する
 - TunnelのMTUを1500に拡張することで、tunnel区間をパケットを分割して通過させることができる
 - TCP(Protocol:6)以外のUDP(Protocol:17)やESP(Protocol:50)などの1500バイトパケットを通すことができる
 - Path MTU Discovery以外の要因によるDF=1のIPにも対応が可能

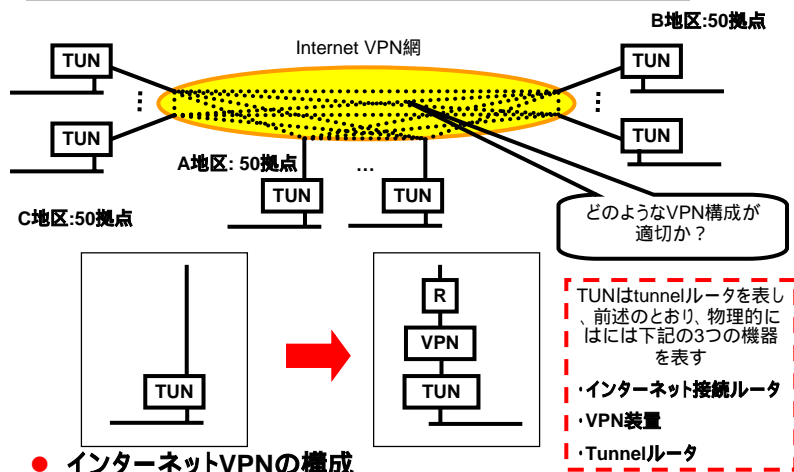


インターネットVPNの問題点の解決

- MTUが1500より小さくなることによる問題点の解決
 - TCPについてはMSS調整により解決を行う
 - Path MTU Discovery Black holeの解決とスルーブット低下の防止が同時に行われる
 - 多くのアプリケーションがTCPを利用しているため、MSS調整により問題が解消することが多い
 - TCP以外のプロトコルはMTU拡張により解決を行う
 - 暗号化パケットのESPやUDPなどTCPでないプロトコルの解決にはMTU拡張を行い、パケットを分割して通すようにする。
 - パケットを分割することでパフォーマンスは低下するが、すべてのIPパケットを通すことができる
 - 2つの手法の併用
 - 'MSS調整'と'MTU拡張'を同時に設定することですべてのIPパケットが通るだけでなく、TCPは効率よく通すことができる。
 - MTUを設定すると自動的にMSS値が決定するようなVPN機器、tunnelルータは2つの手法の併用はできない。
 - Tunnel MTU=1500、MSS=1460ではMTU1300の物理I/Fに対しMSS調整されたパケットがフラグメントしてしまい効率よく転送することができない
 - Tunnel MTU=1300、MSS=1260ではTCP以外のDF=1のIPパケットが通らない、1300バイトより大きいDF=1のUDP、ESPが通らない



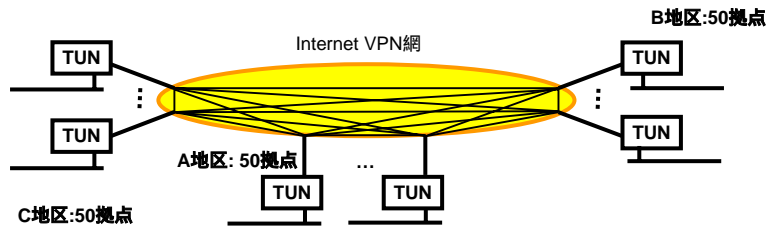
多拠点でのインターネットVPN接続



- インターネットVPNの構成
 - インターネットVPNは各拠点間を自由に結ぶことができる
 - どのような接続法が望ましいのか検討する



VPNフルメッシュ構成



- フルメッシュ構成

- すべての拠点間をVPNで結ぶ
- 拠点の数:mとしたときのVPNの数

$$\text{VPNの数} = \frac{m(m-1)}{2} = \frac{m^2 - m}{2}$$

- VPNの数が拠点数の二乗に比例するため多拠点の管理が煩雑
- 1拠点追加ですべての拠点のVPN機器の変更が必要
- 拠点数が増えたとすべての拠点のVPN機器の性能を上げる必要がある

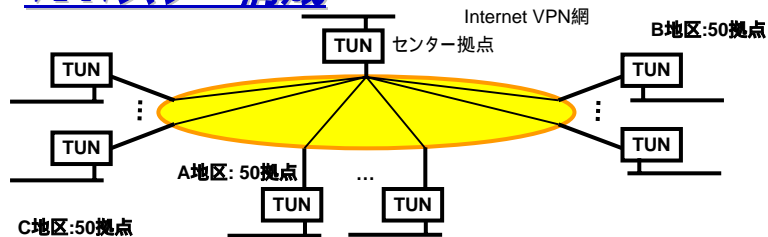


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

109

VPNスター構成



- スター構成

- 各拠点とセンター拠点との間をVPNで結ぶ
- 拠点の数:mとしたときのVPNの数は

$$\text{VPNの数} = m - 1$$

- VPNの数は拠点数に比例するため多拠点の管理が容易
- 1拠点追加でセンター拠点のVPN機器の変更だけで済む
- スターの中心となるセンター拠点のtunnelルータの障害ですべての拠点の通信ができなくなる
- 拠点数が増えたとセンター拠点に多数のVPNを収容する必要があり、高性能なVPN機器が必要となる

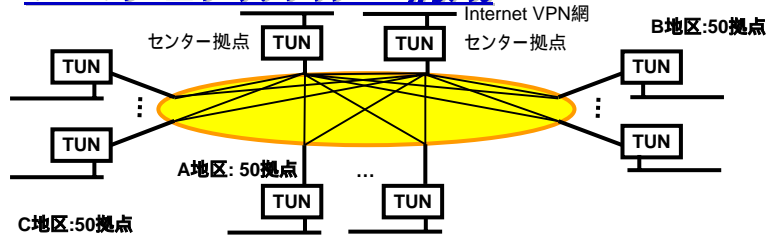


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

110

VPNデュアルスター構成



● デュアルスター構成

- 各拠点から2箇所のセンター拠点にVPNで結ぶ
- 拠点の数:mとしたときのVPNの数は

$$\text{VPNの数} = 2(m-1)$$

- VPNの数は拠点数に比例するため多拠点の管理が容易
- 1拠点追加でセンター拠点のVPN機器の変更だけで済む
- スターの中心となるセンター拠点のtunnelルータに障害が発生してもバックアップされる
- 拠点数が増えるとセンター拠点に多数のVPNを収容する必要があり、高性能なVPN機器が必要となる
- 地区ごとにデュアルスター構成を行い、さらにセンター拠点ともデュアル構成とすることでVPN機器の負荷の集中を防ぐことができる

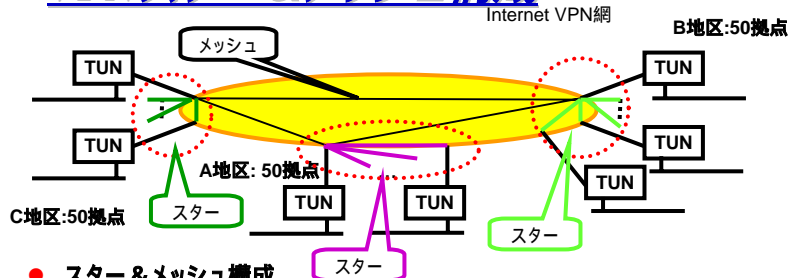


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

111

VPNスター&メッシュ構成



● スター&メッシュ構成

- 地区ごとにスター型にVPNを構成、スター型の頂点の拠点間をメッシュ状にVPNで結ぶ
- 拠点の数:m、スターの頂点をnとしたときのVPNの数は

$$\text{VPNの数} = m - n + \frac{(n^2 - n)}{2} = \frac{n^2 - 3n + 2m}{2}$$

- VPNの数は拠点数に比例するため多拠点の管理が容易
- 頂点の数はVPNの数の二乗に比例するが、多く設置する必要はないためVPNの数への影響は少ない
- 1拠点追加でセンター拠点のVPN機器の変更だけで済む
- スターの頂点のtunnelルータの障害が発生しても全体ではなく局所化した障害となる
- スター構成をデュアルスター構成に変更すればバックアップも可能



2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

112

ポリシーごとのWANの使い分け

VoIPや基幹系データなど高信頼性を要求される通信とインターネットアクセスなど信頼性よりも広帯域を要求される通信を複数のWANを使って使い分ける方法を2つ紹介します

- PBRを利用したWANの使い分け
- ネットワークポロジによりWANの使い分け

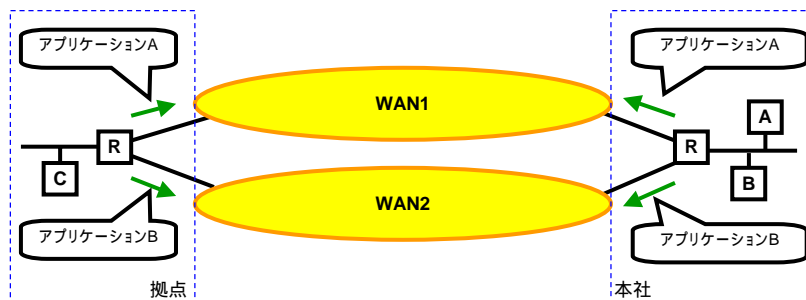


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

113

PBRを利用したWANの使い分け設定



- 本社側のアプリケーションサーバAはWAN1を利用し、アプリケーションサーバBはWAN2を利用するようにルータにてPBR(Policy-Based Routing)を設定する
- PBRはIPアドレスごと、利用アプリケーション(利用ポート)などによりNext Hopを指定することができる
- 通常のルーティングではdestination(宛先アドレス)ごとに経路を設定することしかできないが、PBRによりsource(送信元アドレス)や利用ポートなどにより経路を設定することができる

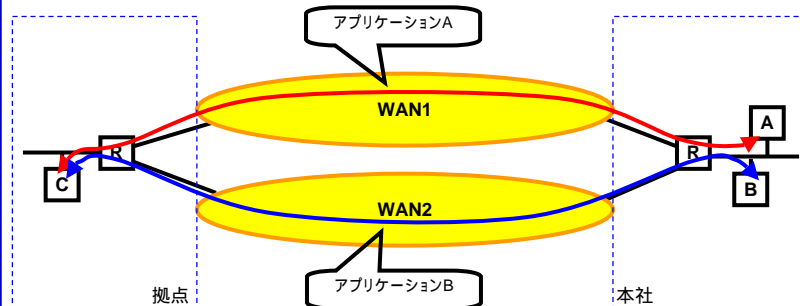


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

114

PBRを利用したWANの使い分け



- 拠点側クライアントCよりアプリケーションサーバAおよびBにアクセスする回線を使い分けすることができる
- PBRはIPアドレスごと、利用アプリケーション(利用ポート)などによりNext Hopを指定することができる



2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

115

PBRを利用したWANの使い分けのまとめ

- PBR(Policy-Based Routing)はIPアドレスごと、利用アプリケーション(利用ポート)などによりNext Hopを指定することができる
- Next Hopを異なったWANに設定することでアプリケーションごとに利用回線を使い分けすることができる
- 通常のルーティングではdestination(宛先アドレス)ごとに経路を設定することしかできないが、PBRによりsource(送信元アドレス)や利用ポートなどにより経路を設定することができる
- PBRはstaticと同様に固定的に経路を設定するため、2つのWANの相互の冗長化は難しい

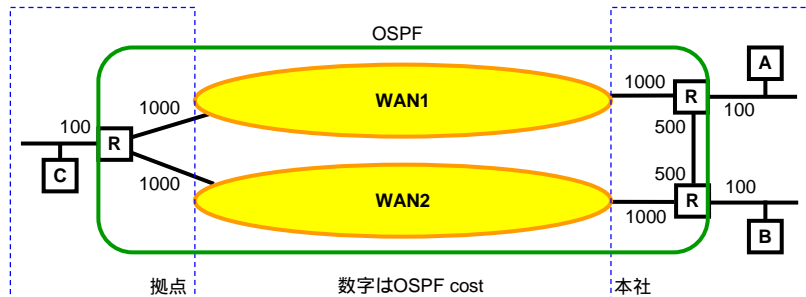


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

116

ネットワークポロジによるWANの使い分け設定



- 本社側のアプリケーションサーバAはWAN1を収容しているルータに接続し、アプリケーションサーバBはWAN2を収容しているルータに収容する。
- 本社ルータ間が高めのOSPF cost(500)を設定する
- WANにはLANより高いOSPF cost(1000)を設定する
- 拠点側ルータのWAN側は本社側と同じOSPF cost(1000)を設定する

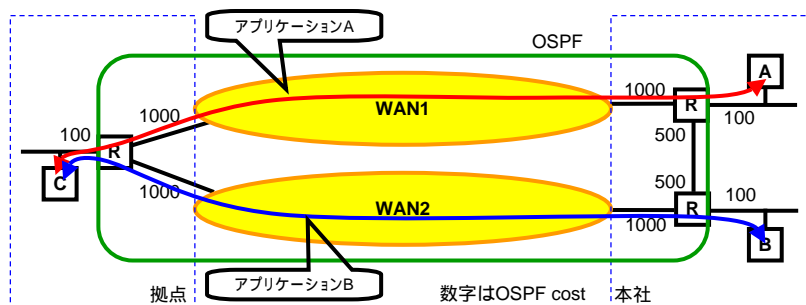


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

117

ネットワークポロジによるWANの使い分け



- 拠点側ルータから見るとAに対してはWAN1を経由しBに対してはWAN2を経由するように経路制御される
- 本社側WAN1収容ルータはCに対してWAN1を経由し、WAN2収容ルータはCに対してWAN2を経由するように経路制御される
- 実質的にアプリケーションごとにWANを使い分けができる

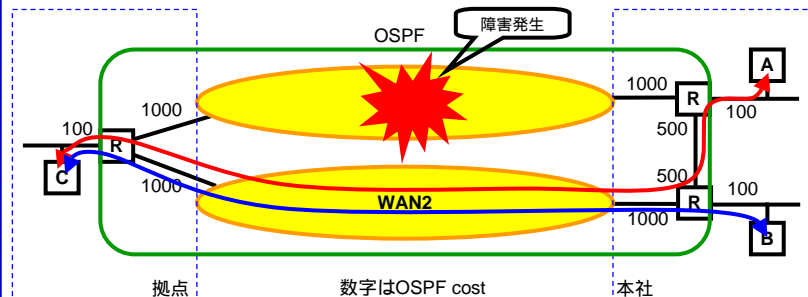


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

118

ネットワークポロジによるWANの使い分け 障害時



- WAN1に障害が発生した場合にはWAN2を利用してバックアップすることができる
- 障害復旧時は自動的に復旧する
- WAN2障害時にも同様にバックアップを行うことが可能



2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

119

ネットワークポロジによるWANの使い分けのまとめ

- 本社側のアプリケーションサーバAはWAN1を収容しているルータに接続し、アプリケーションサーバBはWAN2を収容しているルータに収容する。
- WAN収容ルータ間が高めのOSPF costを設定し、WANにはLANより高いOSPF costを設定する
- OSPF cost調整により、実質的にアプリケーションごとにWANを使い分けることができる
- OSPFなどのダイナミックルーティングを利用できるため、冗長化が可能
- RIPなどのOSPF以外のダイナミックルーティングでも実現可能
- 既存ネットワークによってはIPアドレスのリナンバなどの構成変更が必要になる



2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

120

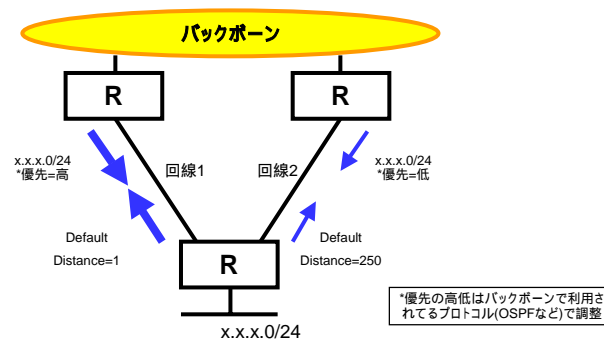
フローティングスタティックを利用したバックアップ

フローティングスタティックを利用したバックアップ手法を2つ紹介します

- **スタティック・スタティック バックアップ**
 - スタティックルーティングだけでバックアップを実現します
- **ダイナミック・スタティック バックアップ**
 - ダイナミックルーティングとスタティックルーティングを併用してバックアップを実現します



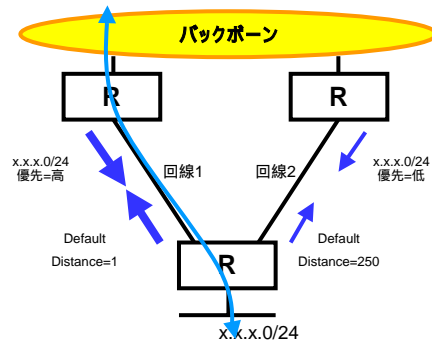
スタティック・スタティックバックアップ 設定



- **拠点側ルータ**
 - 優先度の高いdefault(distance=1)を回線1に設定し、優先度の低いdefault(distance=250)を回線2に設定する。
- **センター側ルータ**
 - 優先度の高くない拠点向け経路(x.x.x.0/24)を回線1に設定し、優先度を低くない拠点向け経路を回線2に設定する
 - バックボーン側の優先度はOSPF costなどで調整



スタティック・スタティックバックアップ 通常時



- 通常時の動作
 - 回線1に設定された優先度の高い経路が有効となる
- 通常時のトラフィック
 - 回線1のみ利用される

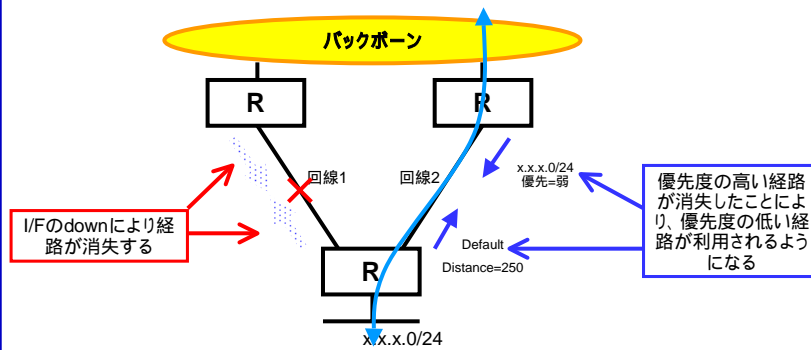


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

123

スタティック・スタティックバックアップ 障害時



- 障害時の動作
 - 回線障害などの要因によりI/Fがdownし、優先度の高い経路が消失する
 - 優先度の高い経路が消失することにより優先度の低かった経路が選択され、利用されるようになる
- トラフィック
 - 回線2によりバックアップされる

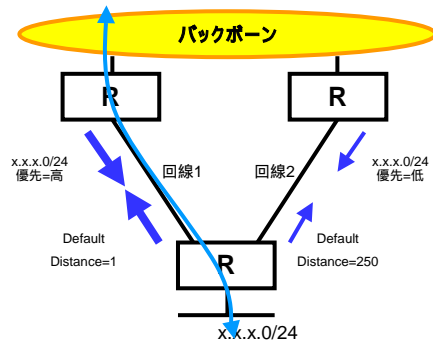


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

124

スタティック・スタティックバックアップ 復旧時



- 復旧時の動作
 - 回線が復旧し、I/Fがupすることで回線1に設定された優先度の高い経路が有効となる
- 通常時のトラフィック
 - ふたたび回線1のみ利用されるようになる



2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

125

スタティック・スタティックバックアップ 特徴

- スタティック・スタティックバックアップ
 - フローティングスタティックを利用したスタティック・スタティックバックアップはI/F downにより回線障害を検知し、優先度の低いスタティックを有効にすることでバックアップを実現する
 - ダイナミックルーティングを利用せずに容易にバックアップが実現できる
 - 回線障害時にI/Fがdownしない回線は利用できない
 - Ethernet専用線
 - PPPoEなどを利用した回線
 - VPN/tunnel
 - HUBを経由したLAN

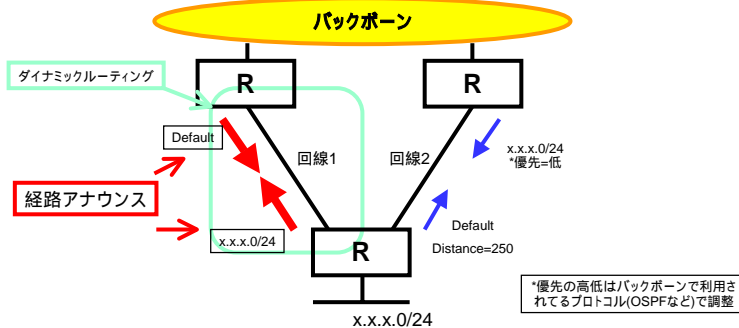


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

126

ダイナミック・スタティックバックアップ 設定



- 拠点側ルータ
 - ダイナミックルーティングを利用して回線1に拠点側経路(x.x.x.0/24)をアナウンスする。優先度の低いdefault(distance=250)を回線2に設定する。
- センター側ルータ
 - ダイナミックルーティングを利用してdefaultを回線1にアナウンスする。優先度を低くした拠点向け経路を回線2に設定する
 - バックボーン側の優先度はOSPF costなどで調整

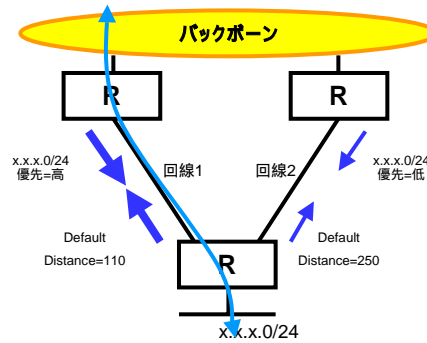


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

127

ダイナミック・スタティックバックアップ 通常時



- 通常時の動作
 - 回線1を利用したダイナミックルーティングにより優先度の高い経路が設定される。
- 通常時のトラフィック
 - 回線1のみ利用される

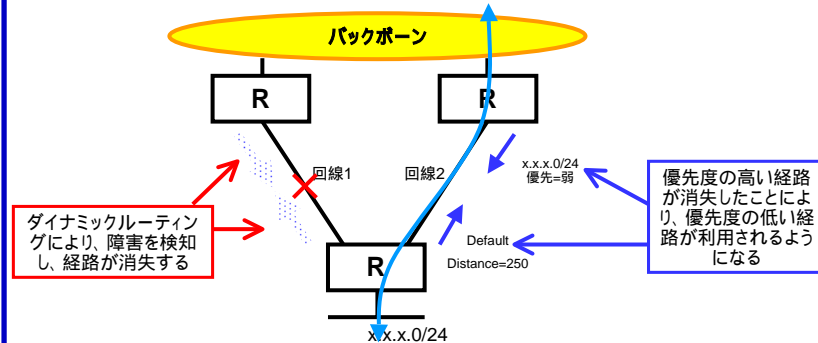


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

128

ダイナミック・スタティックバックアップ 障害時



- 障害時の動作
 - 回線障害などの要因をダイナミックルーティングが検知し、優先度の高い経路が消失する
 - 優先度の高い経路が消失することにより優先度の低かった経路が選択され、利用されるようになる
- トラフィック
 - 回線2によりバックアップされる

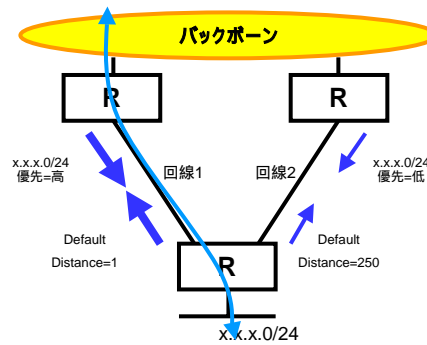


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

129

ダイナミック・スタティックバックアップ 復旧時



- 復旧時の動作
 - 回線が復旧し、ダイナミックルーティングが再び有効となり、回線1に優先度の高い経路が設定される
- 通常時のトラフィック
 - ふたたび回線1のみ利用されるようになる



2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

130

ダイナミック・スタティックバックアップ 特徴

- **ダイナミック・スタティックバックアップ**
 - フローティングスタティックを利用したダイナミック・スタティックバックアップはダイナミックルーティングにより回線障害を検知し、優先度の低いスタティックを有効にすることでバックアップを実現する
 - 回線障害時にI/Fがdownしない回線であっても利用が可能
 - Ethernet専用線
 - PPPoEなどを利用した回線
 - VPN/tunnel
 - HUBを経由したLAN
 - バックアップ側回線のトラフィックを通常時ゼロにすることができるため、ISDNなどの回線をバックアップに利用することが可能

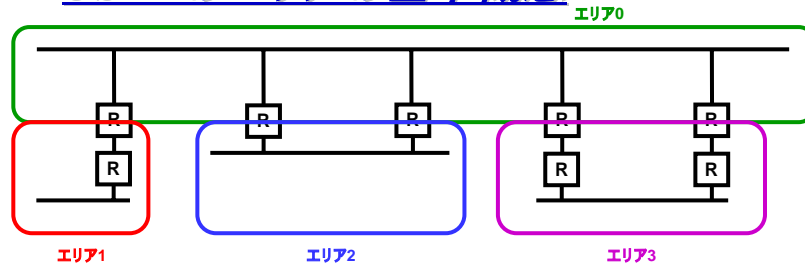


OSPFのエリアを利用した構築

- **OSPFのエリア**
 - OSPFは経路集約のためにネットワークをいくつかのエリアに分けることができる。
 - 先の説明にあったように小規模から中規模のネットワークではエリアを分ける必要はほとんどない
 - 利用機器の制約からBGPを利用することができず、OSPFのみで大規模なネットワークを設計する場合にはエリア分けを検討する価値はある
- **間違いやすいOSPFのエリア**
 - 間違いやすいOSPFのエリアの概念を具体例を示して解説する



OSPFのエリアの基本概念



- バックボーンエリア
 - バックボーンエリアと呼ばれるエリア0は必ず存在しなければならない
- バックボーン以外のエリアはバックボーンエリアに接していなければならない
 - エリア1、エリア2、エリア3は必ずエリア0に接している
- エリア境界はルータになる
 - ネットワークがエリア境界となることはない
 - 同じネットワークは同じエリアになる
- 同じI/Fに複数のエリアを設定することはできない
 - 1つのルータのI/Fには1つのエリアにだけ属することができる
 - Passive interface設定であっても1つのエリアにだけ属する

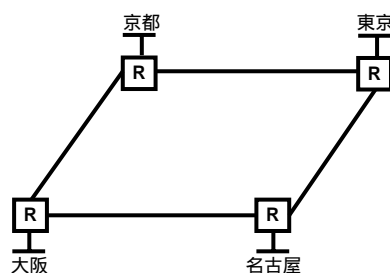


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

133

OSPFエリア構築事例



- 4拠点を結ぶバックボーンを適切にエリア分けする
- 各拠点には実際には多くのネットワークがあることを想定
- イメージとしては各拠点到にエリアを分ければよいように見える

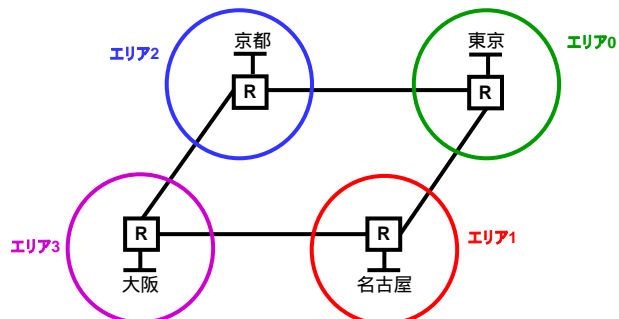


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

134

OSPFエリア構築事例 回答例



- 拠点ごとにそれぞれをエリアとした場合
- 一見よさそうに見えますが？

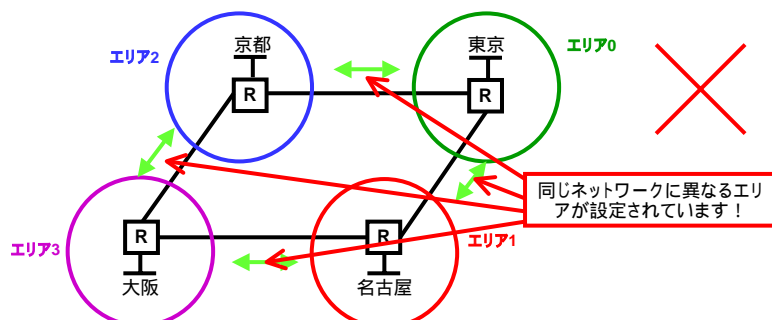


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

135

OSPFエリア構築事例 回答例



- 同じネットワークに異なるエリアが設定されているため動作しません！

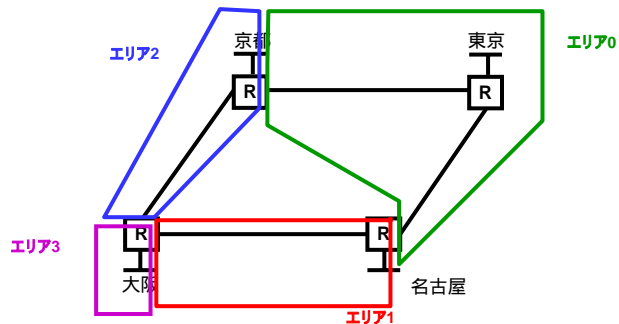


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

136

OSPF エリア構築事例1 回答例2



- 東京側から大阪側にかけて同じインターフェースを同じエリアにするように設定
- 一見よさそうに見えますが？

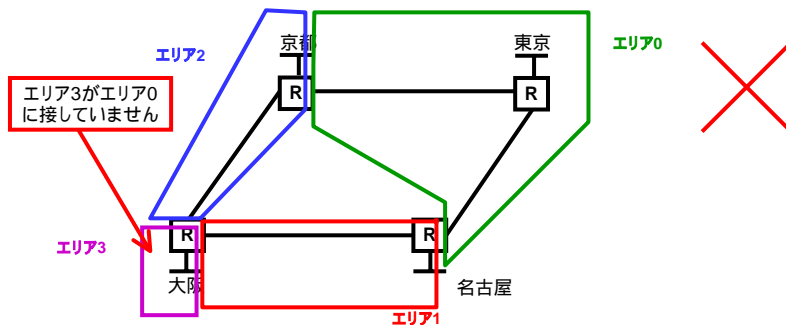


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

137

OSPF エリア構築事例1 回答例2



- エリア3がエリア0に接していないため、動作しません
- VL(Virtual Link)という技術により仮想的にエリア0に接するよう見せ、動作させることもできますが、適切なエリア分けをした場合に比べて煩雑でバックアップに問題があります。東京に障害が発生すると正常にバックアップされません

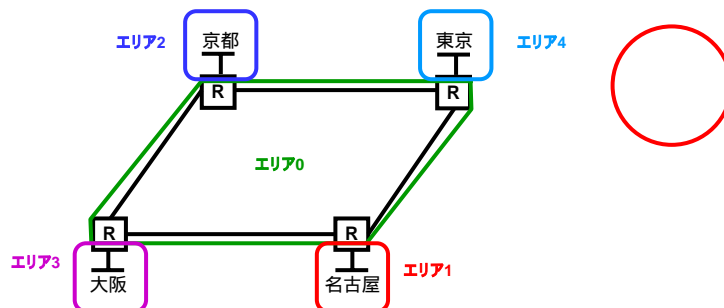


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

138

OSPF エリア構築事例1 正解



- 各拠点を結ぶネットワークにはエリア0を設定する
 - すべての拠点到にエリア0が存在するため、各拠点到に自由にエリアを追加することができる
 - 東京が障害となってもバックアップが可能
- 各拠点到には各拠点到に閉じるエリアを設定する
 - 各拠点到に閉じる経路を集約することができる

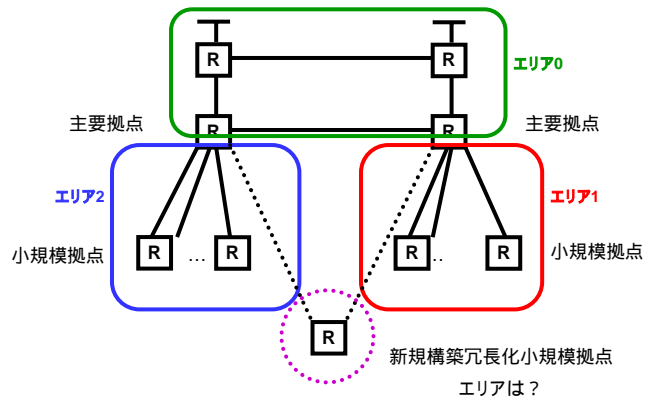


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

139

OSPF エリア構築事例2



- 事例1に従い、バックボーンエリアと各拠点到ごとに適切にエリアを分け、小規模拠点到を主要拠点到にまとめて収容している
- 冗長化のために複数の主要拠点到から小規模拠点到を接続する場合に、どのようにエリアを分ければよいか？

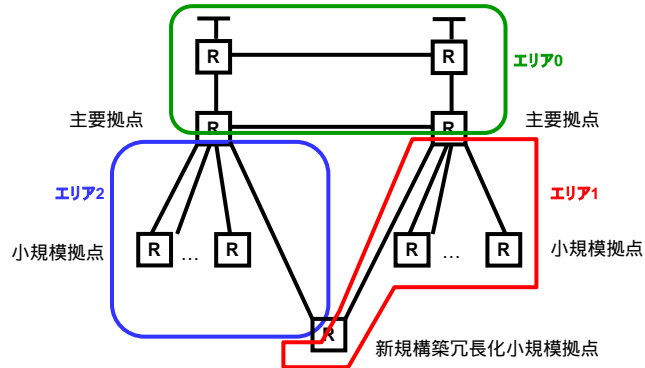


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

140

OSPF エリア構築事例2 回答例1



- 冗長化拠点をエリア1に属するように設定。
- エリア2からも1本冗長化拠点到伸ばす
- すべてのエリアがエリア0に接していて、一見よさそうに見えますが？

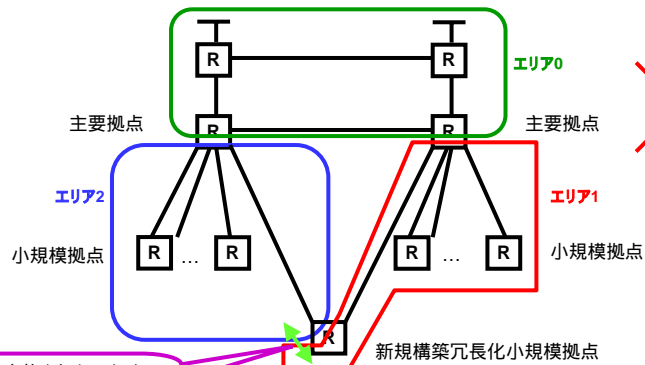


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

141

OSPF エリア構築事例2 回答例1



経路交換されないため、
バックアップされない

- エリア1の経路はエリア0を経由して交換されるため、バックアップされません

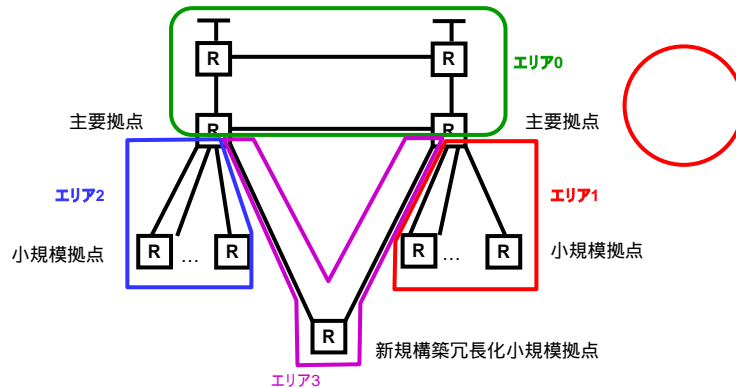


2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

142

OSPF エリア構築事例2 正解



- 冗長化拠点用に新たなエリア3を設定
- エリア3は2箇所エリア0に接し、それぞれ異なる回線を通るようにする
- 同様の構成の冗長化小規模拠点は同じエリア3に設定が可能



2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

143

OSPF のエリアを利用した構築:まとめ

- OSPFエリア分けの方法
 - 主用拠点間など迂回経路となりうるすべてのルータにエリア0を設定する必要がある
 - 特定の拠点にのみ接続する小規模拠点などはエリアを分けることで経路集約が可能
- OSPFエリア分けの必要性
 - OSPFエリア分けの方法のひとつとして「すべてエリア0で構成する」という選択肢を忘れてはいけない
 - 大規模なネットワークはBGPなどOSPF以外のプロトコルを利用して多くの経路を交換することも検討すべき



2004/12/3

Copyright © 2004 Internet Initiative Japan Inc.

144

まとめ-1

- 一定の規模を超えるとスタティックルーティングよりダイナミックルーティングの方が容易に管理することができるようになる
- ダイナミックルーティングは「経路の流れる方法と、経路が向く方向が逆になる」という基本法則を理解すればどのようなIGPを利用してネットワーク設計をすることができる
- 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
- OSPFを利用すればバランシングとバックアップを同時に実現可能



まとめ-2

- 広域Ethernetを利用した大規模なWANでは適切な規模ごとにネットワークを分離して細い回線の輻輳を防止する必要がある
- インターネットVPNではVPN装置だけでなくtunnelルータを設置することで専用線と同様にダイナミックルーティングを利用したネットワークを構築することができる
- インターネットVPNではPath MTU Discovery Block holeの解決をはかる必要がある
- PBRやネットワークポロジにより複数のWAN回線をアプリケーションごとに使い分けることができる
- フローティングスタティックとダイナミックルーティングを併用してISDNなどを利用したバックアップを実現できる
- OSPFのエリアは通常はエリア0だけを利用して構築すればよいが、OSPFのみで大規模なネットワークを構築する際は適切なエリア分けを行わなければならない

