

ネットワーク設計構築 A to Z [I]

～基礎から始める最適ネットワーク設計～

2006年12月5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

- データリンク層とネットワーク層の役割は
- 障害が起りにくいネットワークを設計するには
- ネットワークの冗長化を行うには
- L2ループ対策をするには
- 適切な機器選定をするには
- ルーティングとは



発表内容

- データリンク層とネットワーク層の役割
- ハブ、ルータの違い
- ネットワーク設計
- アドレスの割り当てポリシー
- ネットワークの冗長化
- L2ループ対策
- ルータとレイヤ3スイッチの違い
- ネットワーク構築
- ネットワークトラブルシューティング

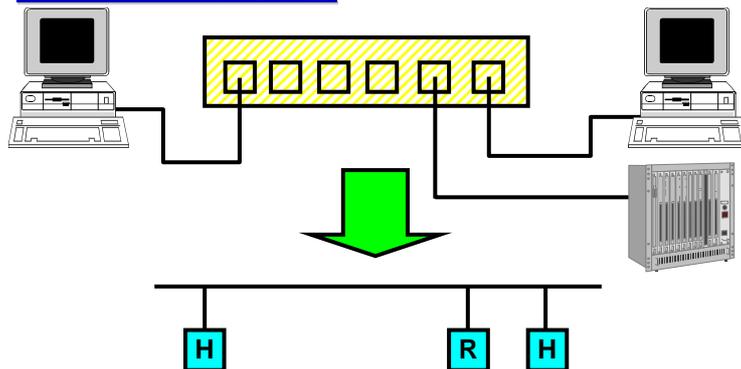


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

3

ネットワーク表記



- ハブなどは1本の線またはHUB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が、区別が必要な場合は都度記述します



2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

4

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
- データリンク層の種類
- 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



2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

5

OSI参照モデルとTCP/IP

OSI参照モデル

7	アプリケーション層
6	プレゼンテーション層
5	セッション層
4	トランスポート層
3	ネットワーク層
2	データリンク層
1	物理層

TCP/IP

HTTP,SMTP等
TCP,UDP
IP
Ethernet,ADSL,専用線等



OSIレイヤ

レイヤ2:データリンク層

レイヤ3:ネットワーク層



2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

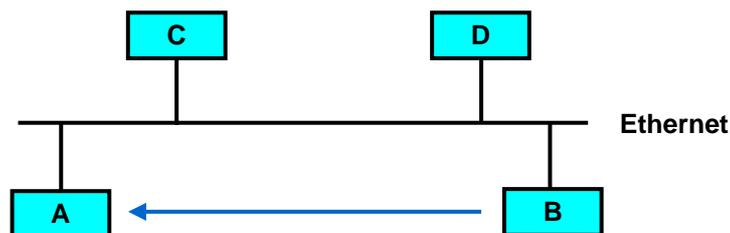
6

データリンク層の種類

- Multi Access Media (ARP)
 - MAC(Media Access Control)アドレスを用いて通信を行う
 - MACアドレスとIPアドレスとの対応はARP(Address Resolution Protocol)を用いる
 - Ethernet等
- Multi Access Media (固定)
 - 特定の識別子とIPアドレスに結び付け、固定的に設定を行う
 - フレームリレー、ATM等のMulti Access Mode
 - EthernetでIPアドレスとMACアドレスを固定的に設定
- Point to Point Media
 - 通信相手が物理もしくは仮想I/Fで特定されるもの
 - 64k,128k,1.5M,6M,45M,150M,600M,2.4G,10Gなどの専用線
 - フレームリレー、ATM等のPoint to Point Mode
 - PPPoEを利用したEthernet



ARPの動作-1



Host	IPアドレス	MACアドレス
A	192.168.0.1	00-00-f8-05-22-c9
B	192.168.0.2	不明
C	192.168.0.3	不明
D	192.168.0.4	不明

Host AのIP/MACアドレス対応表

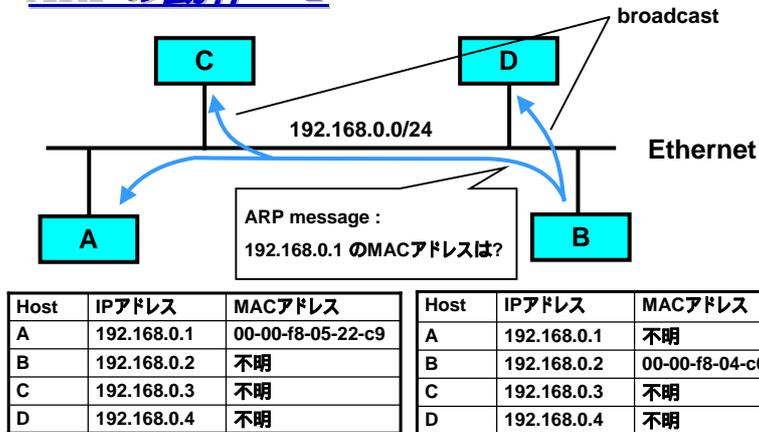
Host	IPアドレス	MACアドレス
A	192.168.0.1	不明
B	192.168.0.2	00-00-f8-04-c0-11
C	192.168.0.3	不明
D	192.168.0.4	不明

Host BのIP/MACアドレス対応表

- BはAに通信したいが、BはAのMACアドレスがわからない



ARPの動作-2



Host AのIP/MACアドレス対応表

Host BのIP/MACアドレス対応表

- BはAのMACアドレスを尋ねるメッセージをbroadcastする

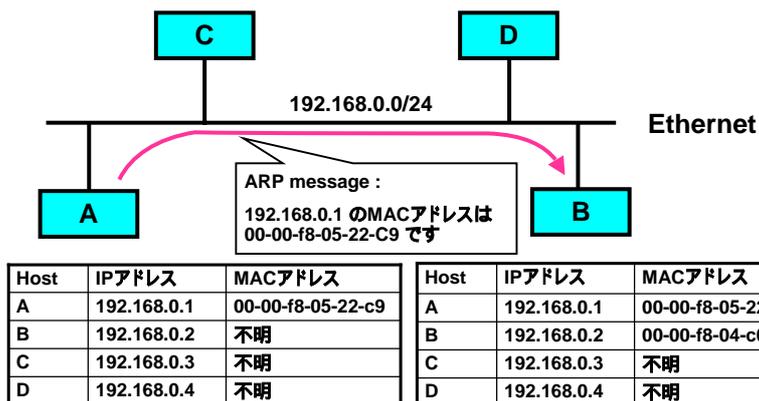


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

9

ARPの動作-3



Host AのIP/MACアドレス対応表

Host BのIP/MACアドレス対応表

- Aは自分のMACアドレスをBに返答する

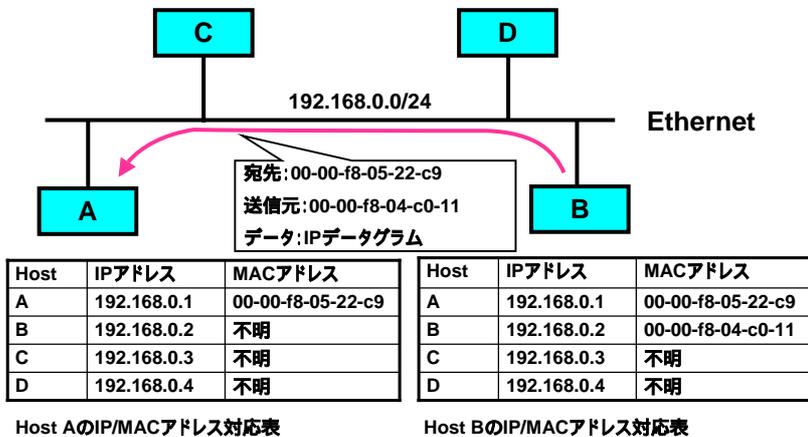


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

10

ARPの動作-4



- BはAに対してデータを送ることができるようになる



Multi Access Media(ARP) - 1

- ARP (Address Resolution Protocol)
 - ARPとはIPアドレスとMACアドレスを対応させるためのプロトコル(IP以外のプロトコルでも利用されますが、IPに限って説明します)
- IP/MACアドレス表
 - IP/MACアドレス対応表のことを「ARPテーブル」「ARPキャッシュテーブル」「ARPキャッシュ」などと呼ばれている
- ARPキャッシュ
 - ARPテーブルに登録されたIP/MACアドレスは一定時間保持(キャッシュ)される
 - ARPテーブルにIP/MACアドレスが存在するときはARPによるbroadcastは行われず、ARPテーブルにしたがって通信が行われる。
 - 一定時間後、IP/MACアドレスはARPテーブルから削除され、その後通信が行われた場合には再びARPを実施する
 - キャッシュすることで、ARPによるデータリンク層のbroadcastを抑制している



Multi Access Media(ARP) - 2

- ARPキャッシュのクリア
 - 機器の交換などでIP/MACアドレス対応に変化がある場合はARPキャッシュをクリアを行う必要がある場合がある
 - arp -d (ホストなど)
 - clear arp (ルータなど)
 - 最近のネットワーク機器やOSは機器交換後に明示的にARPキャッシュをクリアしなくても高速にARPキャッシュ反映されるような実装が増えている

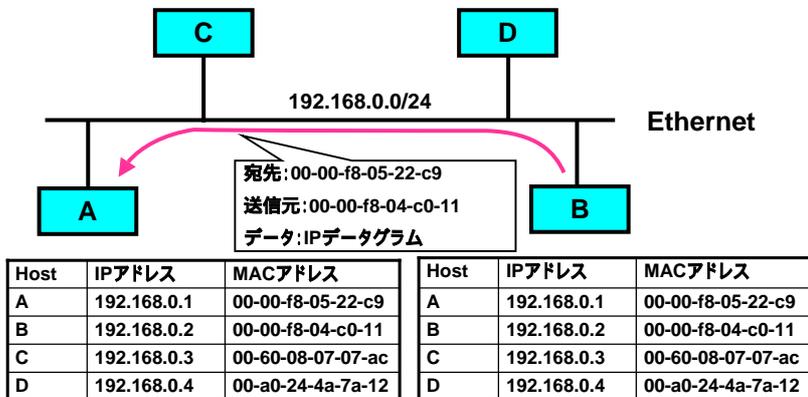


Multi Access Media(ARP) - 3

- ARPのメリット
 - 他の機器のIP/MACアドレス対応表を設定する必要が無い
 - 機器交換を行ってもARPキャッシュがクリアされれば自動的に反映される
- ARPの運用上の注意点
 - 機器交換の際にARPキャッシュをクリアしないとすぐに通信できないことがある
 - broadcastが利用されるため大規模なレイヤ2ネットワークでは帯域を圧迫する
 - Globalセグメントで多くの利用されていないアドレスが存在すると、インターネットから未使用アドレスに対するアクセスによりLANが輻輳することがある
 - インターネット上のウイルスに感染したホストなどからのポートスキャンにより発生する(NIMDAなど)
 - 未使用アドレスの個数×リトライ回数のbroadcastが発生する
詳しくは後述



固定IP/MACアドレス対応表の動作



Host AのIP/MACアドレス対応表(固定)

Host BのIP/MACアドレス対応表(固定)

- IP/MACアドレス対応表は事前に固定的に設定されるため、BはAに対してデータを送ることができる



Multi Access Media(固定)

- ARPを用いず固定的に物理アドレスとIPアドレスを結びつける
- ARPを用いないためbroadcastが発生しない
- broadcastが利用できないため、ARPが利用できない場合に利用
- 機器交換などでIP/MACアドレス対応が変化する場合にはすべての機器の設定を変更する必要がある
- ATMではVPI/VCIを固定的に設定する



Point to Point Mediaの動作



Host	IPアドレス
A	192.168.0.1
B	192.168.0.1以外の 192.168.0.0/24

Host	IPアドレス
A	192.168.0.2以外の 192.168.0.0/24
B	192.168.0.2

Host Aの通信先

- Point to Point Mediaに属しているすべてのネットワークは相手側に送り出す (ARPや固定アドレス表は不要)
- Point to Point Mediaから来たフレームはすべて受け取る
- IP層によってはA、B間をループしてしまうこともある

Host Bの通信先



Point to Point Media-1

- 自分以外の属しているネットワークに対するすべての通信をPoint to Point Mediaに送り出す
- Point to Point Mediaから来たフレームはすべて受け取る
- 受け取ったフレームはIP層で評価される
- IP層の評価によってはPoint to Point Mediaでループすることもある
- すべてのフレームを選択せずに送り出し、受け取るためMACアドレス、broadcastは不要

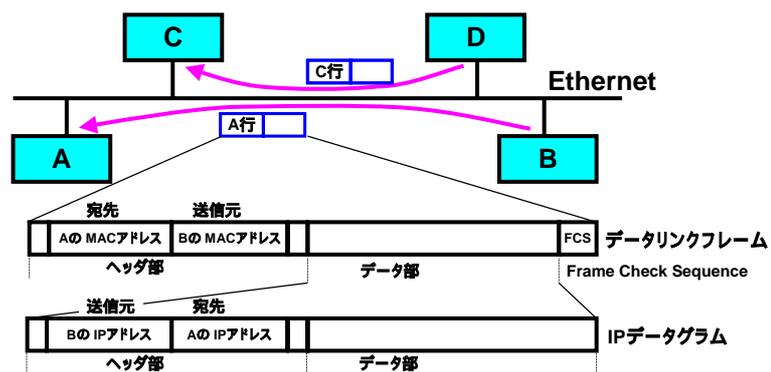


Point to Point Media-2

- ATM専用線も設定によりPoint to Point Mediaとして利用することが可能
- ネットワークは一般的に/30もしくはunnumberedが利用される
 - 192.168.0.0/30 (ネットワーク例)
 - 192.168.0.1 (Router 1)
 - 192.168.0.2 (Router 2)
 - unnumberedインターフェースへのルーティングはインターフェース名などが利用される
 - ip route 172.16.0.0 255.255.0.0 Serial0/0

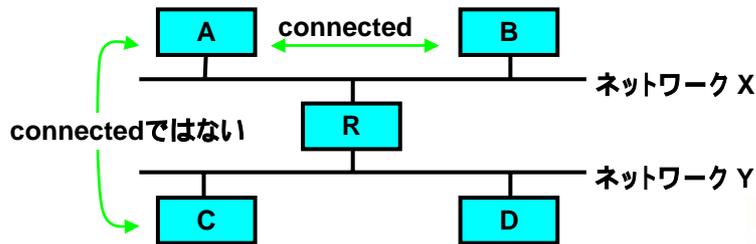


Ethernetを流れるIPデータグラム



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



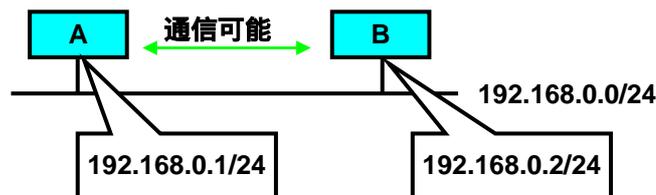
2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

21

ネットワーク層から見たConnectedなネットワーク - 1

- Aのアドレス
 - 192.168.0.1/24
- Aから見たConnectedなアドレス空間
 - 192.168.0.0 ~ 192.168.0.255
- Bに192.168.0.2 ~ 192.168.0.254のアドレスを付ける
 - Bに192.168.0.2を付ける
 - A-B間の通信が可能



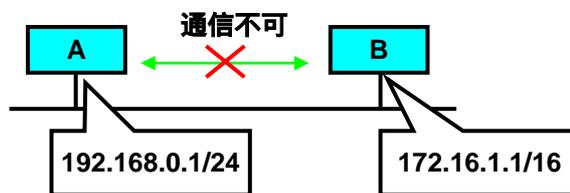
2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

22

ネットワーク層から見たConnectedなネットワーク - 2

- Aのアドレス
 - 192.168.0.1/24
- Aから見たConnectedなアドレス空間
 - 192.168.0.0 ~ 192.168.0.255
- Bに192.168.0.2 ~ 192.168.0.254以外のアドレスを付ける
 - A-B間の通信ができない



2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

23

Connectedではないネットワーク - 1

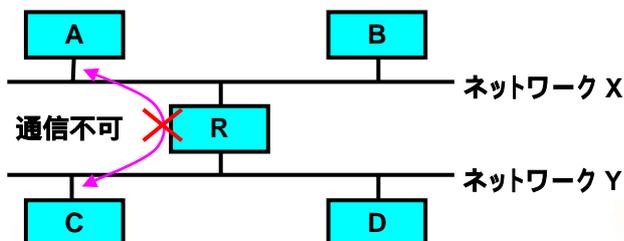
- A, Cはそれぞれ異なるネットワークに接続しているため connectedではない
- ルーティング設定なしではA, C間の通信はできない

Aのルーティングテーブル

destination	Next Hop	到達性
X	Connected	到達可
Y	なし	到達不可

Cのルーティングテーブル

destination	Next Hop	到達性
X	なし	到達不可
Y	Connected	到達可



2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

24

Connectedではないネットワーク - 2

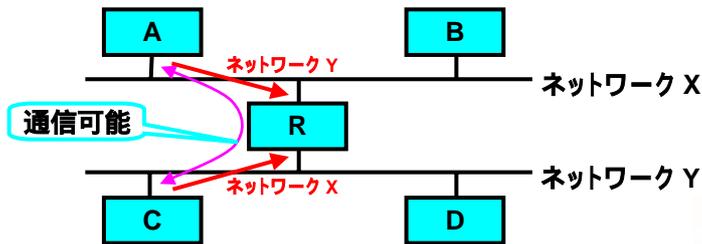
- ルーティング設定を行なう
 - A: ネットワークYを Rにルーティング
 - C: ネットワークXを Rにルーティング
- これにより、A C間の相互通信が可能となる
 - Rは A,C共に connectedなため、アドレスを設定するだけで通信が可能

Aのルーティングテーブル

destination	Next Hop	到達性
X	Connected	到達可
Y	R	到達可

Cのルーティングテーブル

destination	Next Hop	到達性
X	R	到達可
Y	Connected	到達可



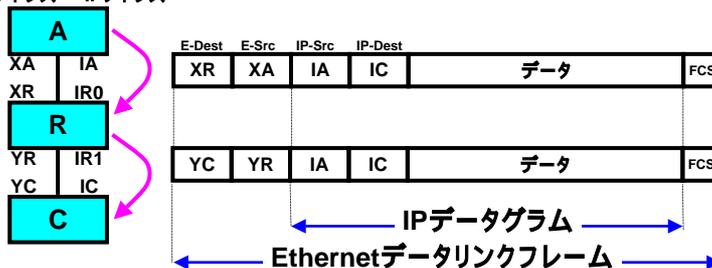
2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

25

データリンクフレームの状態

MACアドレス IPアドレス



- 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

2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

26

ネットワーク用語のまとめ

- Destination, Destination Address
 - 目的地という意味。ネットワークでは文字どおり目的地アドレス、宛先アドレスとして扱われる。Destination (デスティネーション) とそのまま使われることが多い。経路制御ではアドレスだけでなく、マスク情報を含んだネットワーク情報もDestinationとして扱われる。
- NEXT HOP, NEXT HOP Address
 - 次に配送すべきアドレス。ルータやホストはDestinationがConnectedでない場合に次に配送すべきアドレス (NEXT HOP) を参照してIPパケットを送信する。IPパケットを受け取ったルータやホストはその次に配送すべきアドレス (NEXT HOP) に送信し、これらを繰り返してDestinationに到達する。
- ルーティング、ルーティング情報
 - 経路。DestinationとNEXT HOPをペアとしたもの。
- ルーティングテーブル
 - ルータやホストが持っているルーティングの一覧
- ルーティングする
 - ルータが正常にルーティングテーブルに基づいてIPパケットを送り出している状態「このルータはきちんとルーティングしている」



データリンクフレームとルーティングのまとめ

- データリンク層、ネットワーク層共にConnectedな状態であればルーティング設定をせずに通信が可能
- Connectedでないネットワーク、ホストとの通信には必ずルータの設置、ルーティング設定が必要
- 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



ハブとルータの機能の違い

- リピータハブとスイッチングハブの機能の違い
- スwitchングハブを有効に使う方法
- 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witchングハブとルータの違い
- スwitchングハブの耐障害性
- ルータの耐障害性
- Broadcast flood問題
- スwitchングハブの耐ウイルス障害性
- ルータの耐ウイルス障害性



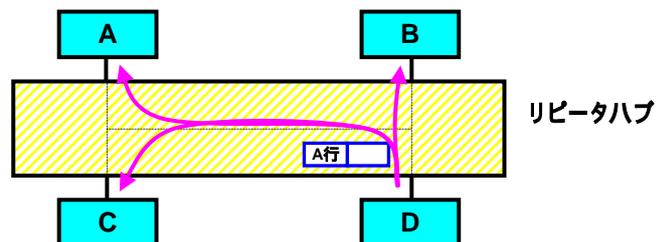
2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

29

リピータハブとスイッチングハブの違い-1

リピータ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播して、他の通信を妨げる



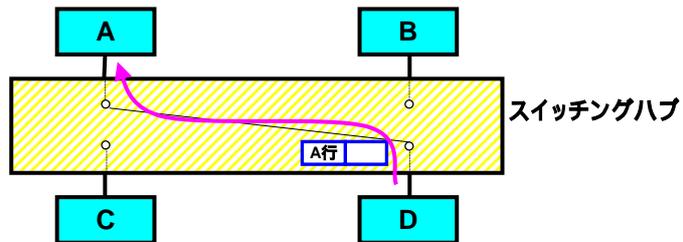
2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

30

リピータハブとスイッチングハブの違い-2

スイッチングハブで構成した場合



- スイッチングハブは、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

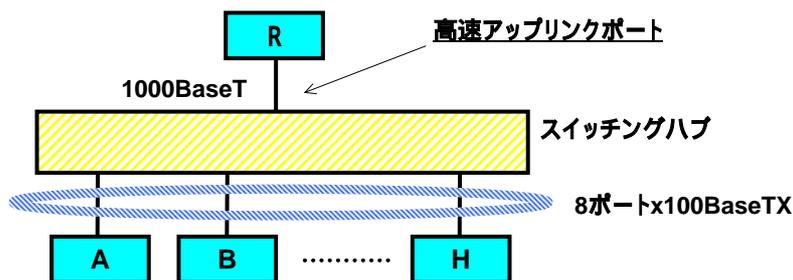


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

31

スイッチングハブを有効に使うには



- 主にルータ、ホスト間のトラフィックの場合に有効
- A ルータ } それぞれ100BaseTXをフルに利用可能
 ⋮ }
 H ルータ }

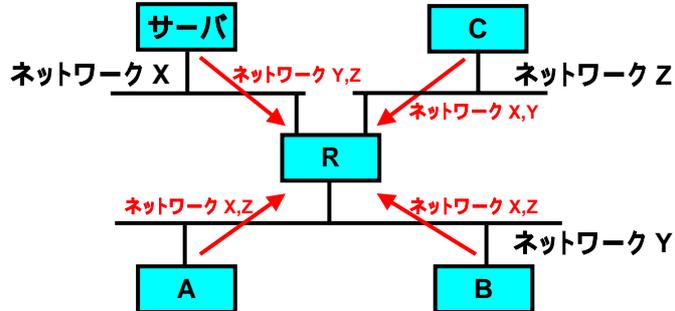


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

32

ルータを利用するための設定 - 1



- 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

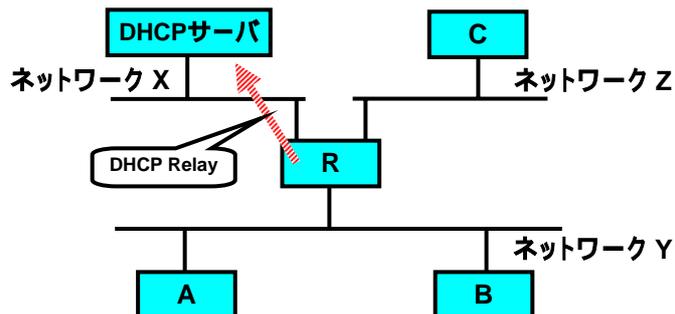


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

33

ルータを利用するための設定 - 2



- DHCPサーバ設定
 - DHCPサーバは同一ネットワークに存在する必要がある
 - ルータのDHCP Relay設定により異なるネットワークでもDHCPを利用できる



2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

34

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

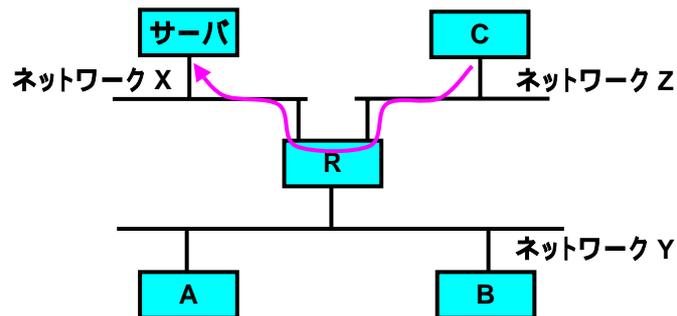


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

35

スイッチングハブとルータの違い



- 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播しない



2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

36

スイッチングハブとルータの機能の違い

- リピータハブとスイッチングハブの機能の違い
 - スwitchングハブは異なるポートの通信を他のポートに伝播しない
- スwitchングハブとルータの違い
 - 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播しない
 - スwitchングハブとは異なり、ルーティングの設定が必要
 - サブネット分割が必要
- スwitchングハブを有効に使うには
 - トラフィックが集中するようなポートにはスswitchングハブの高速アップリンクポートを利用する

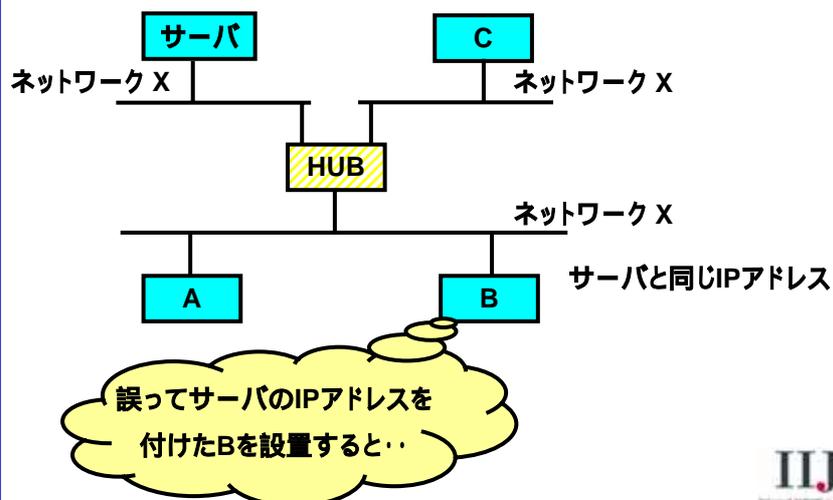


次に問題点について検討する

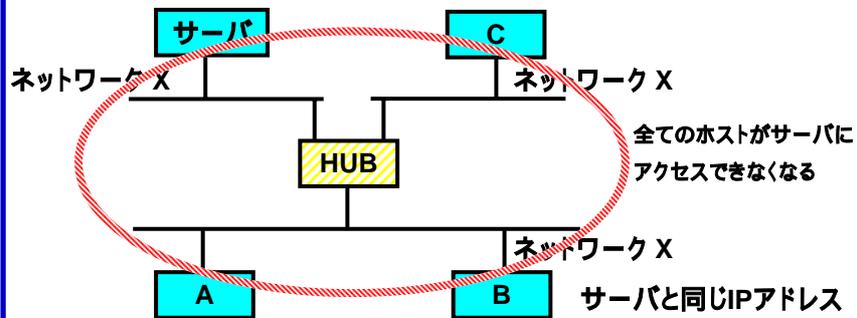
以後、特に指定が無い場合にはスswitchングハブをHUBもしくはレイヤ2スswitch(L2SW)と記述します



HUBの耐障害性-1



HUB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

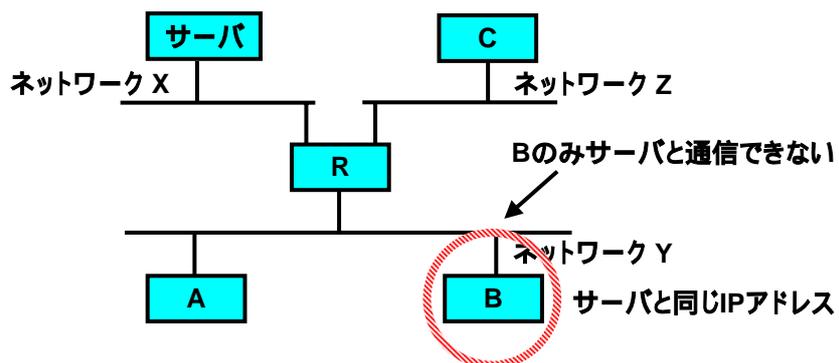


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

39

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

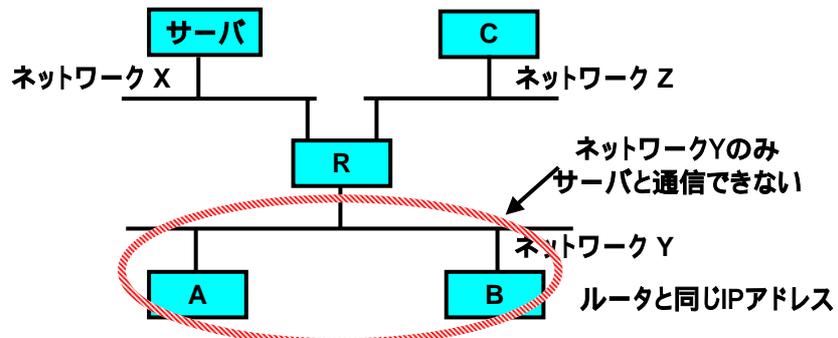


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

40

ルータの耐障害性-2



- 最悪の場合でも、ルータでは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

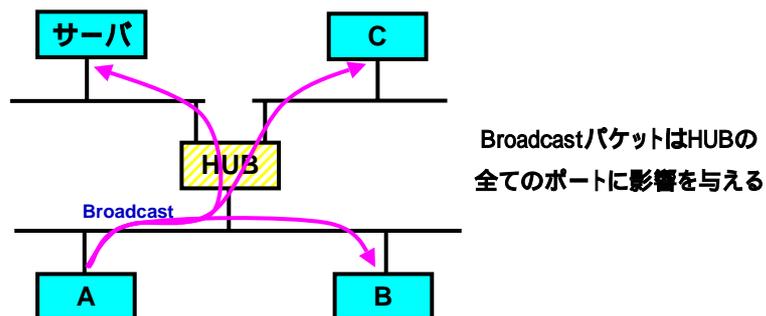


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

41

Broadcast Flood-1



- 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

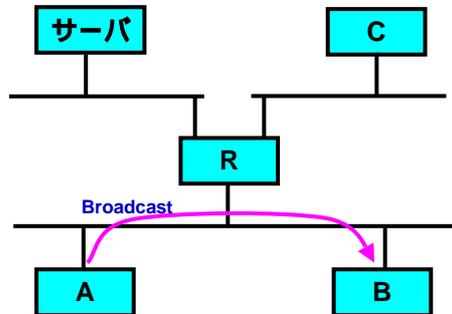


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

42

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

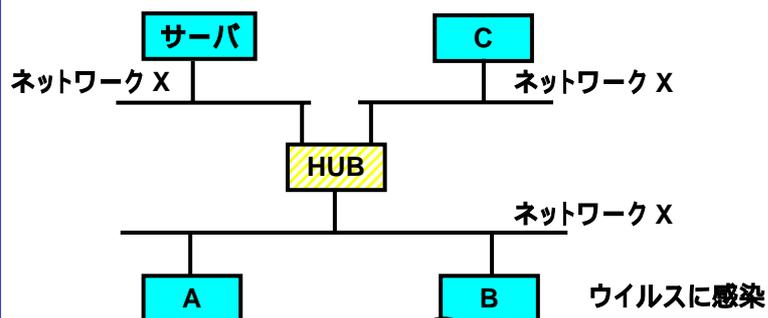


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

43

HUBの耐ウイルス障害性-1

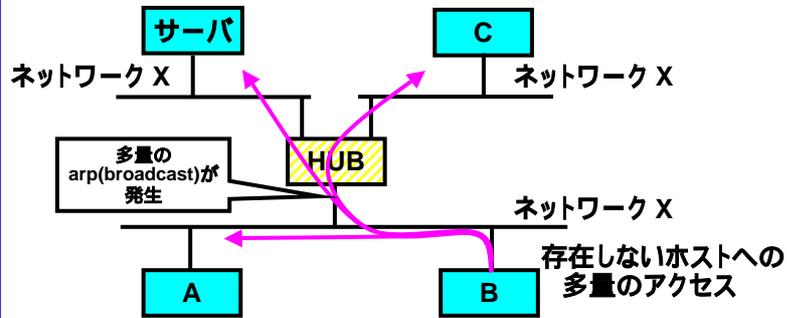


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

44

HUBの耐ウイルス障害性 2



- ウイルスの感染によって存在しないホストへの多量のアクセスが発生する
- 存在しないホストへのアクセスは多量のarp(broadcast)を発生させる
- arp(broadcast)はHUBのすべてのポートを占有する

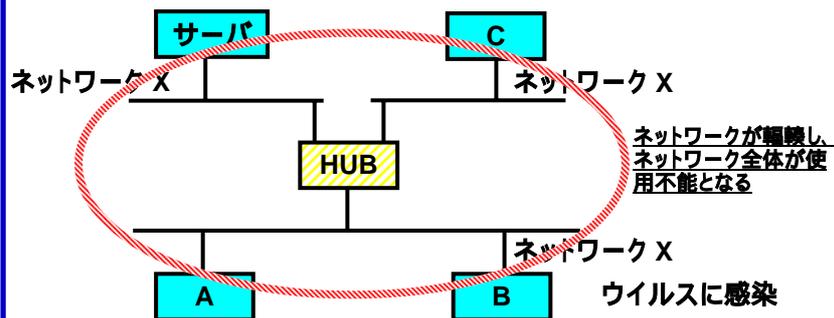


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

45

HUBの耐ウイルス障害性-3



- スイッチのみの構成では、1台のウイルス感染がネットワーク全体を使用不能にする

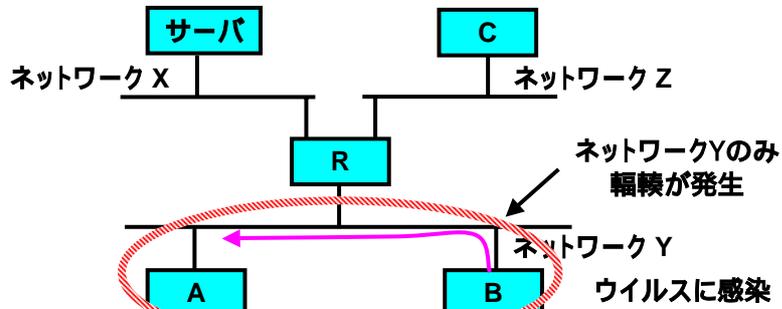


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

46

ルータの耐ウイルス障害性-1



- ルータでは、ウイルス感染ホストによる多量のarp(broadcast)の影響は接続ネットワークに限られる

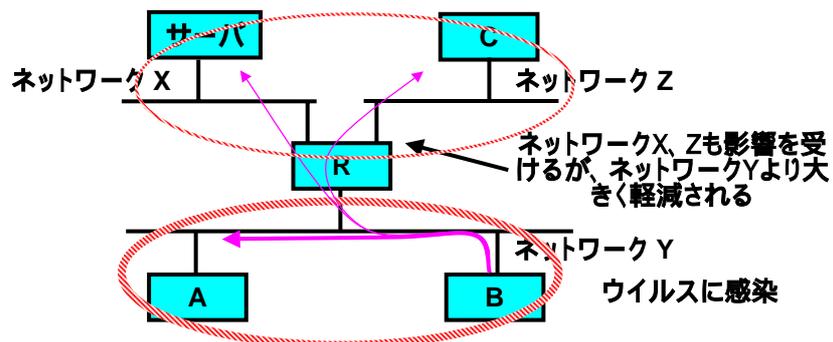


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

47

ルータの耐ウイルス障害性-2



- ルータを越えるパケットも存在するが、ネットワークYに比べるとネットワークX、Zへの影響は小さくなる

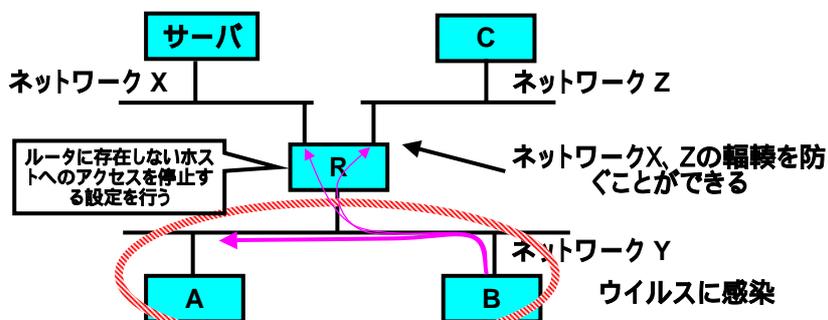


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

48

ルータの耐ウイルス障害性-3



- 存在しないホストに対するフィルタをルータに行うことでネットワークX、Zに対する輻輳を防ぐことができる
- ネットマスクをできる限り小さくすることでフィルタと同様の効果を得ることができる



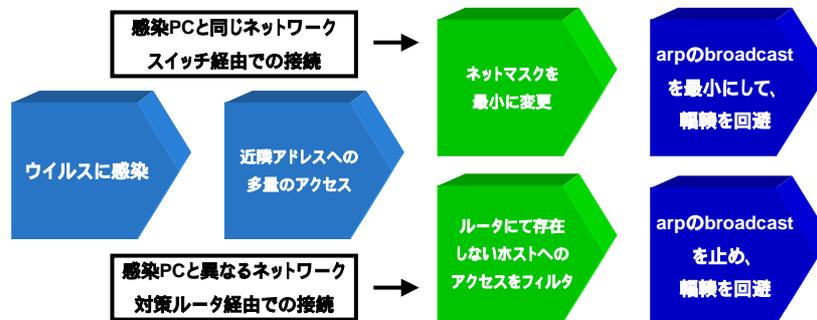
ウイルス感染によるネットワーク輻輳の仕組み



- ウイルスに感染
 - メール、Web、持ち込みPCなどでLAN内にウイルス感染PCが接続される
- 近隣アドレスへの多量のアクセス
 - ウイルス感染PCよりLANに割り当てられている近隣のアドレスに対して多量のアクセスを試みる
- 多量のarpが発生
 - ネットワークに存在しているホストに対してはarpは1度だけ実行される
 - 接続可能な状態にもかかわらずネットワークに存在していないホストに対しては毎回arpが実行される
- arpのbroadcastによりネットワークが輻輳
 - 未使用アドレスの個数×リトライ回数(通常8回程度)のbroadcastが発生する
 - 50台ほどのホストが接続されている状態でのbroadcastの状況は
 - ネットマスク/24利用で(255-50) × 8=1,640回のbroadcast
 - ネットマスク/16利用で(65535-50) × 8=523,988回のbroadcast
 - さらに複数感染した場合には感染PC数を乗じたアクセスとなる



ウイルス感染によるネットワーク輻輳の対策



- ルータにて存在しないホストへのアクセスをフィルタ
 - ルータにて存在しないホストへのアクセスをフィルタすることでarpの発生を止め、輻輳を回避することができる
- ネットマスクを最小に変更
 - ネットマスクを最小にすることで、arpの発生を最小限にし、輻輳を回避することができる



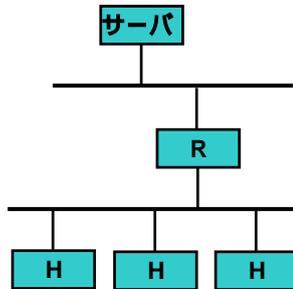
スイッチングハブ VS ルータ

- スイッチングハブの利点
 - ルーティングを考慮しなくて良い
 - リピータ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
 - 高速アップリンクポートを有効に利用できる
- 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
 - ウイルス感染によるネットワーク輻輳を回避できる
 - 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きやすい
- 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ングハブの高速アップリンクポートを利用する



ネットワーク設計-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
- クライアントはDHCPによりアドレスの割り当てとdefault経路を得る
- Broadcast floodのサーバへの影響を防ぐ



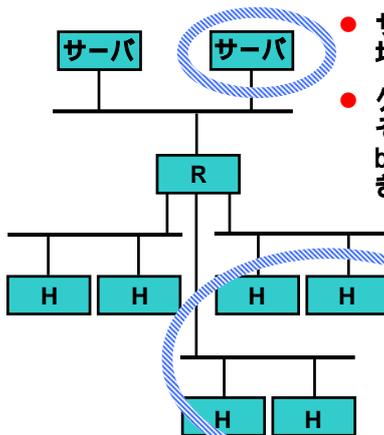
2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

53

ネットワーク設計-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

ネットワークの追加

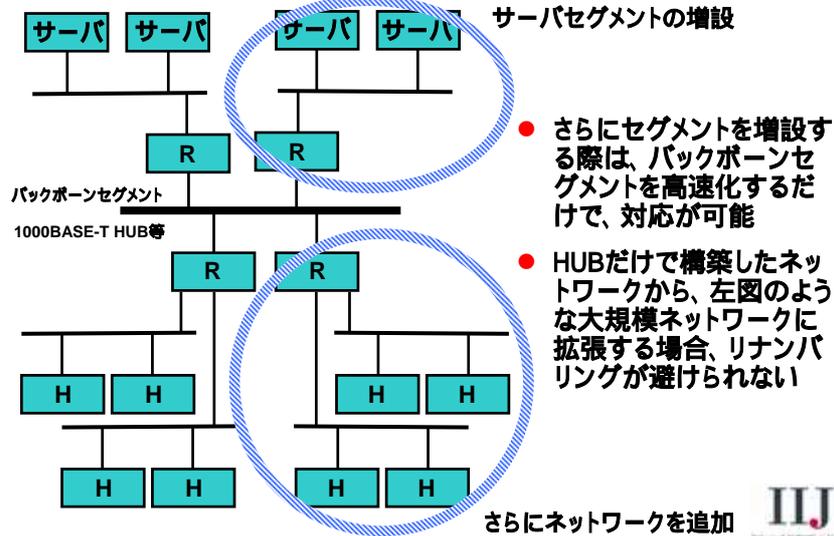


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

54

ネットワーク設計-3



2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

55

ネットワーク設計のまとめ

- 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HUBの高速アップリンクポートを利用する
- 規模の拡大を見越したネットワークポロジの設計



ネットワーク規模拡大を考慮したアドレス割り当て

2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

56

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
- 最適なネットマスクでの利用
- 最適なIPアドレスの割り当て方法
 - ネットマスク変更法
 - サブネット追加法



最適なネットマスクでの利用

- ホスト数 50台を想定したネットワーク
 - 172.16.0.0/16 利用の場合
 - 未使用IPアドレス 65484
 - ウイルス感染などによるarp broadcast floodの発生状況
 - $65484 \times 8 = 52万回$ 程度のbroadcastが発生
 - 192.168.0.0/24 利用の場合
 - 未使用IPアドレス 234
 - ウイルス感染などによるarp broadcast floodの発生状況
 - $204 \times 8 = 1632回$ 程度のbroadcastが発生
 - 192.168.0.0/26 利用の場合
 - 未使用IPアドレス 12
 - ウイルス感染などによるarp broadcast floodの発生状況
 - $12 \times 8 = 96回$ 程度のbroadcastが発生
- 最適なマスク設定の必要性
 - 拡張性のために大きめのネットワークである/16や/24を設定するとウイルス感染時に脆弱なネットワークになってしまう
 - broadcastはスイッチングハブであってもすべてのポートを占有するため、少量のパケットでも輻輳が発生しやすい。



最適なネットマスクでの利用

- 拡張性を持たせつつ、マスクを最長(最少ネットワーク)にするにはどうすれば良いか
 - 拡張性を持たせるには未使用IPアドレス空間を持たせる必要がある
 - 未使用アドレス空間を大きくしすぎるとウイルス感染時に脆弱なネットワークになってしまう



最適なIPアドレス割り当てをどうすべきか？

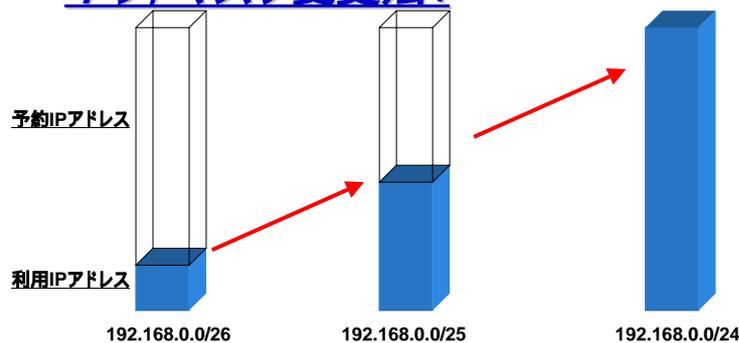


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

59

ネットマスク変更法1



- ネットマスク変更法によるネットワーク拡張
 - 最初から/24程度まで拡張することを前提にIPアドレスを予約する
 - 実際に利用するIPアドレスは/26空間のみとし、/26で不足する場合には/25、/24とマスクを拡張していく
 - /24以上の大きさに対してはサブネット追加を行う

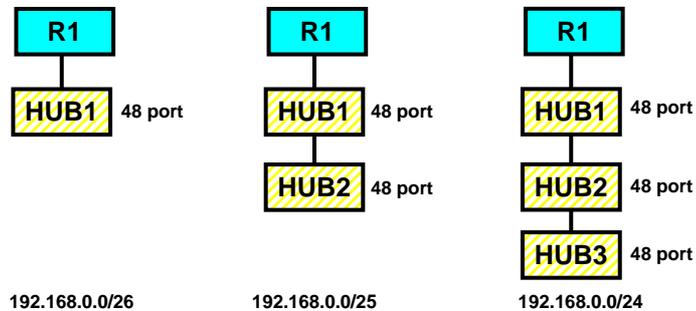


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

60

ネットマスク変更法2



- ネットマスク変更法によるネットワーク拡張
 - マスク変更を前提とした割り当てはL2ネットワークを拡張していく必要があるため、カスケードされたL2ネットワークとなる場合が多い
 - カスケードされたL2ネットワークは障害箇所の特定などが困難となるだけでなく、broadcastドメインを大きくし、パフォーマンスを低下させる

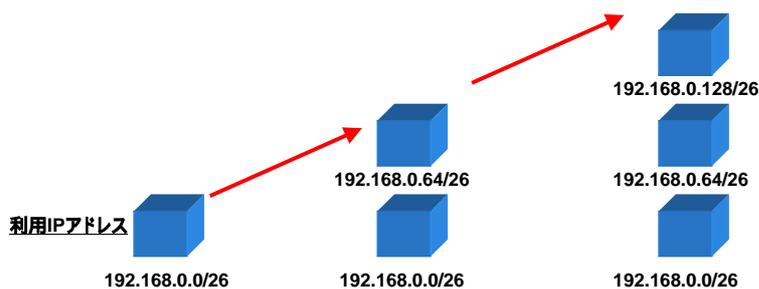


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

61

サブネット追加法1



- サブネット追加法によるネットワーク拡張
 - 実際に利用するIPアドレスは/26空間のみとし、/26が不足した場合には/26サブネットを別に構築する
 - 追加されたネットワークはルータなどを経由してトラフィック交換されるため、L2接続に依存したアプリケーションは利用できない

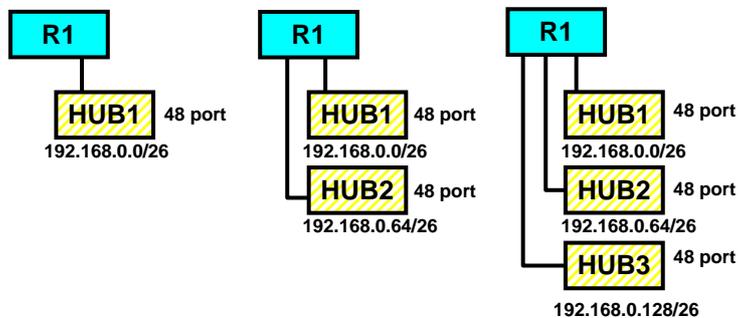


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

62

サブネット追加法2



- サブネット追加法によるネットワーク拡張
 - サブネット追加による拡張では、HUBの物理ポートとサブネットが対応し、HUBの増設に合わせてサブネットも追加される
 - broadcastドメインの広さ(L2ネットワークの大きさ)を一定の大きさに保つことができるため、安定した拡張を行うことができる
 - 管理しやすくするために/24を予約して、/26だけ使っても良い
 - スペース重視: 192.168.0.0/26, 192.168.0.64/26, 192.168.0.128/26
 - 管理重視: 192.168.0.0/26, 192.168.1.0/26, 192.168.2.0/26

2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

63

IPアドレスの割り当てポリシー

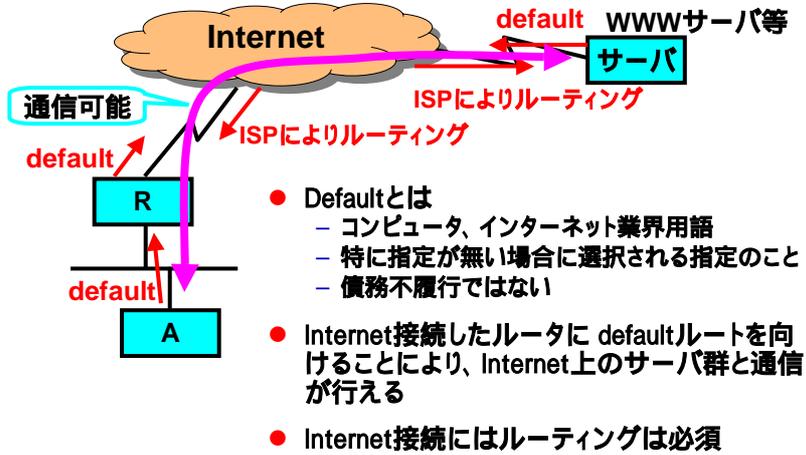
- ネットマスク変更法によるネットワーク拡張
 - 最初から/24程度まで拡張することを前提にIPアドレスを予約する
 - 実際に利用するIPアドレスは/26空間のみとし、/26で不足する場合には/25、/24とマスクを拡張していく
 - L2ネットワークをそのまま拡張できるため、L2接続に依存したアプリケーションも対応可能
 - マスク変更時には同一サブネットの既存ホストの変更が必要となるため、拡張時に負担がかかる
- サブネット追加法によるネットワーク拡張
 - 実際に利用するIPアドレスは/26空間のみとし、/26が不足した場合には/26サブネットを別に構築する
 - 追加されたネットワークはルータなどL3レベルでトラフィック交換されるため、L2接続に依存したアプリケーションは利用できない
 - L2接続に依存したアプリケーションとは、IPアドレスを付与せずプリンタ出力できたり、ファイル交換するアプリケーションがあげられる。
 - このようなアプリケーションはネットワーク拡張に支障をきたすことが多い
 - ネットワークを設計するうえで、あらかじめ24portや48port HUBごとにサブネット化する仕様としておけば容易に拡張することができる
 - L3レベルでのトラフィック交換を前提としたアプリケーション利用とする必要がある
 - 管理しやすくするために/24を予約して、/26だけ使っても良い

2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

64

インターネットへの接続形態

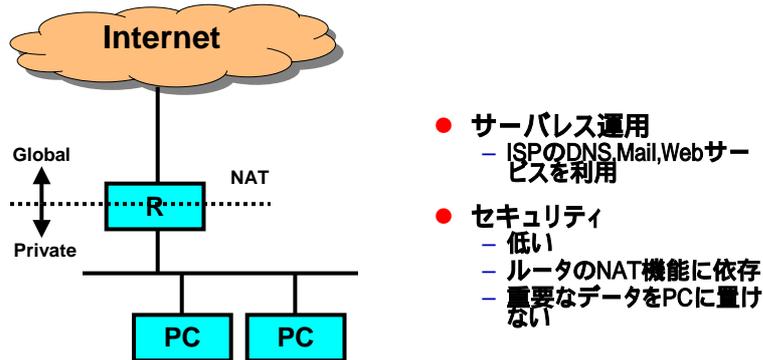


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

65

インターネット接続事例-A



NAT: Network Address Translation

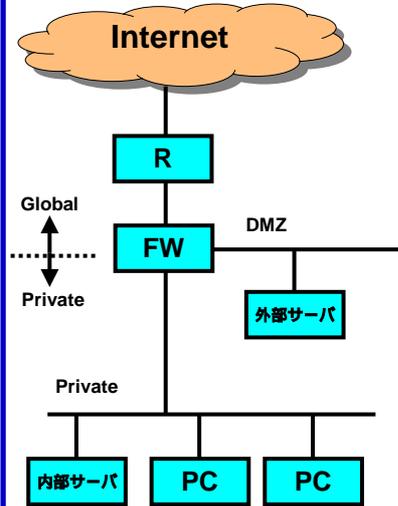


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

66

インターネット接続事例-B



- 自社サーバ運用
- 外部サーバ
 - DMZ (Demilitarized Zone) に設置
 - 公開Web
 - 外部DNS
- 内部サーバ
 - Mail
 - 内部DNS
- セキュリティ
 - 標準的

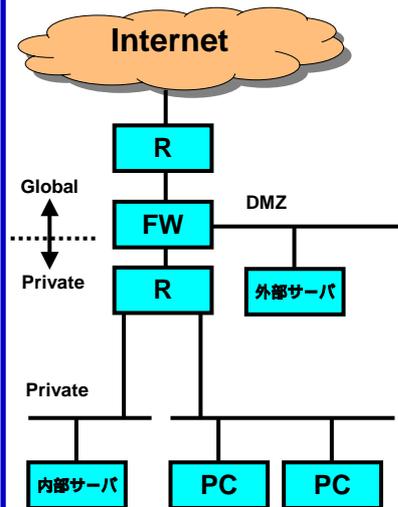


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

67

インターネット接続事例-C



- 自社サーバ運用
- 外部サーバ
 - DMZ (Demilitarized Zone) に設置
 - 公開Web
 - 外部DNS
- 内部サーバ
 - Mail
 - 内部DNS
- セキュリティ
 - 標準的
- 内部サーバの保護

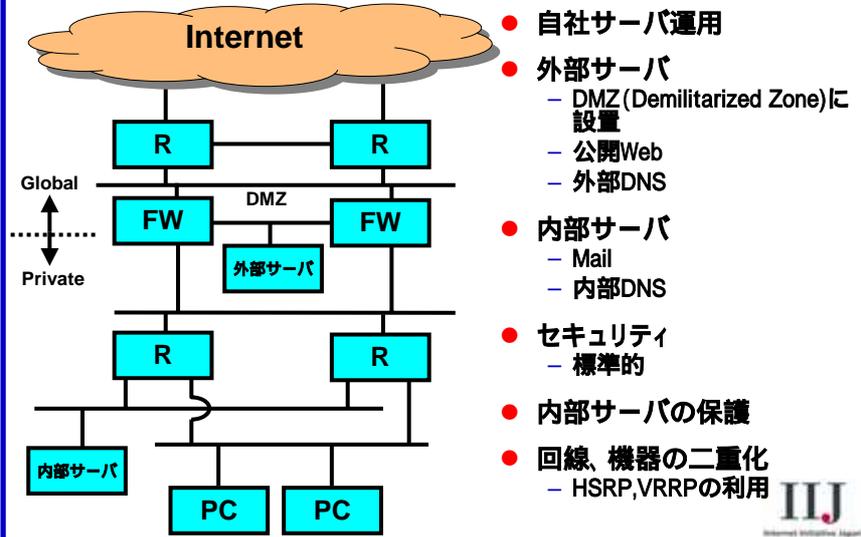


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

68

インターネット接続事例-D



- 自社サーバ運用
- 外部サーバ
 - DMZ (Demilitarized Zone)に設置
 - 公開Web
 - 外部DNS
- 内部サーバ
 - Mail
 - 内部DNS
- セキュリティ
 - 標準的
- 内部サーバの保護
- 回線、機器の二重化
 - HSRP, VRRPの利用

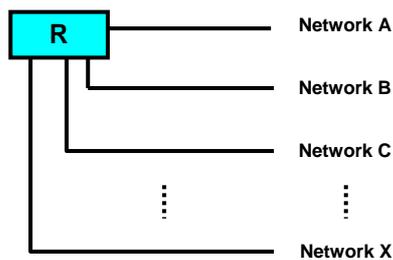


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

69

ネットワーク拡張(スター型)



- スター型拡張
 - スター型のネットワーク拡張はルーティングを単純化できるだけでなくポリシー制御も容易なため、小規模から大規模まで幅広く利用されている
- 特徴
 - ルーティングが容易
 - ポリシー制御が容易
 - 大規模となると集約されるルータを高性能化する必要がある
 - 多くのネットワークを収容できるルータが必要となるが、VLANなどの利用で安価に構成できるようになった



ネットワーク拡張の基本であり、特別な事情がない限り、まずこの形式を検討すべきである

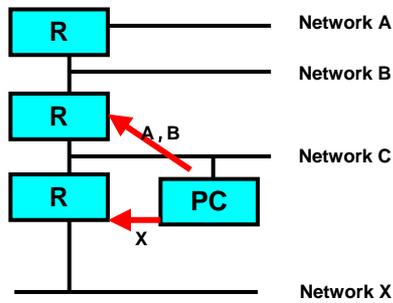


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

70

ネットワーク拡張(数珠型)



物理的にこの形式しか組めない場合
を避けて避けるべき構成である

● 数珠型拡張

- フロアやビル間などを1つのネットワークで構成し、かつ、そのネットワーク上にクライアントが繋がるモデル

● 特徴

- 大規模になるにつれてルーティングが複雑になる
- 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が混在し、誤動作する恐れがある

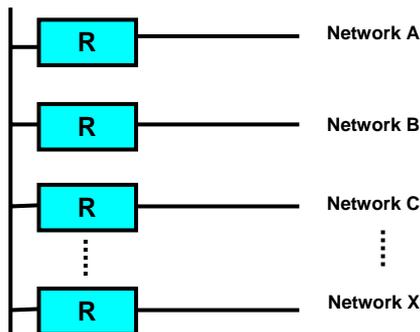


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

71

ネットワーク拡張(L2バックボーン型)



ルータのみに接続するバックボーンネットワーク



同一構内などのLAN接続などに有効に利用できる

● L2バックボーン型拡張

- 1つのL2をルータが共有し、PCやサーバとルータを混在させないようにする。

● 特徴

- ルーティングはルータのみで行えるため、スタティックからダイナミックまで拡張が可能
- 1つのL2を共有するため、長距離の伝送が難しい
- 1つのL2が大きくなりすぎる前にバックボーンの階層化を検討する必要がある

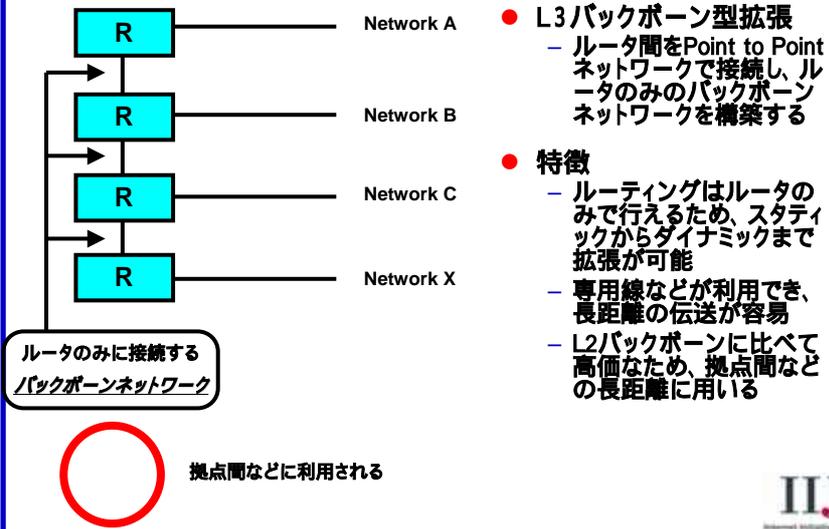


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

72

ネットワーク拡張(L3バックボーン型)

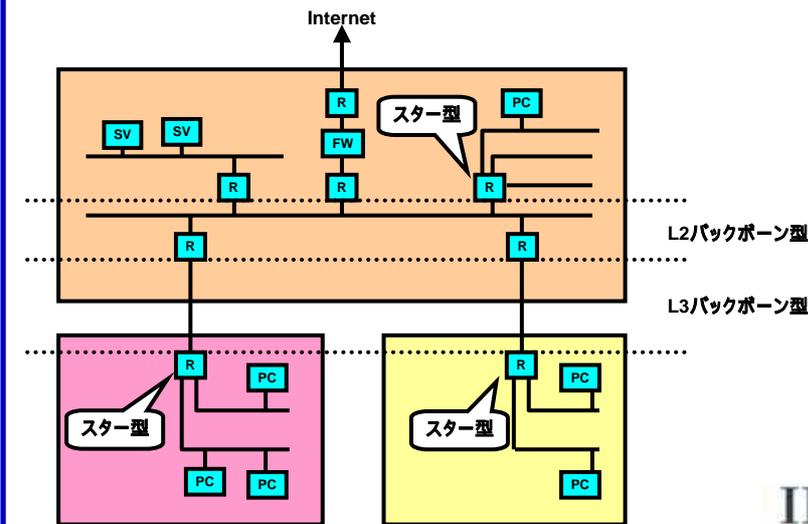


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

73

ネットワーク拡張事例



2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

74

ネットワーク拡張のまとめ

- 小規模な同一構内のネットワークにはスター型を用いる
- 中規模の同一構内のネットワークにはL2バックボーン型を用いる
- 拠点間を結ぶネットワークにはL3バックボーン型を用いる
- 数珠型接続はできる限り避けるようにする

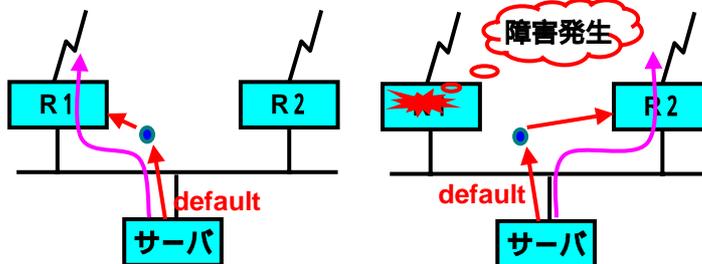


ネットワーク構築に利用される冗長化の仕組み

- 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~60秒程度必要
- 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
 - Ethernet専用線等のdownしないI/Fでは利用できない。
- HSRP/VRRP
 - 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/VRRP-1



- 障害時には仮想MACアドレスがR1からR2に切り替わる
 - 利用しているHUBによっては、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ります

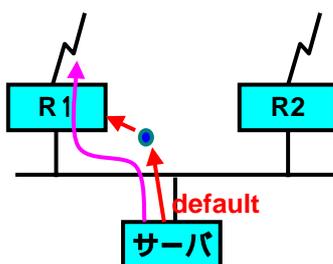


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

77

HSRP/VRRP-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

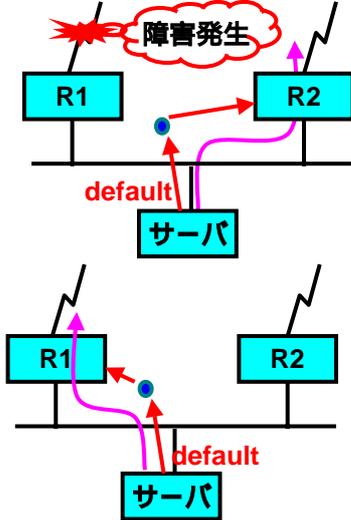


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

78

HSRP/VRRP-3



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

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



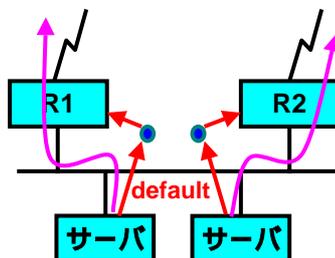
2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

79

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

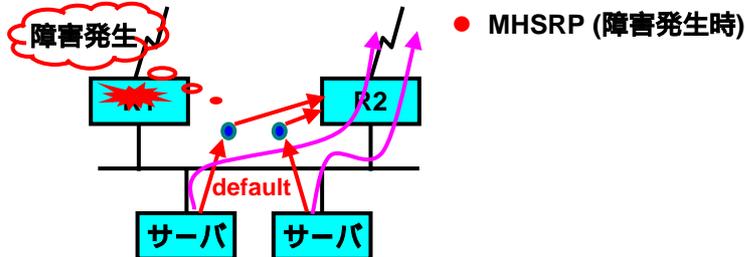


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

80

MHSRP-2



- 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

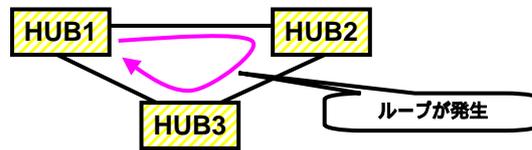


HSRP/VRRPまとめ

- 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
 - Hot Standby Router Protocol
 - RFC2281 (Informational)
 - Cisco社のパテント
- VRRP
 - Virtual Router Redundancy Protocol
 - RFC2338 (Proposed Standard)
 - ルータやファイアウォールなどに実装されている
- MHSRP
 - 1つのネットワークに複数のHSRPを同時利用し、負荷分散することが可能



STPの動作-1



- STPを利用しない場合
 - STPを利用せずにHUBの冗長化するとループが発生する
- ループの発生により様々な問題が発生
 - 各HUBのアドレステーブルに混乱が生じる
 - 同じフレームが二重に届き、上位層の異常な動作につながる
 - Broadcast floodが発生する



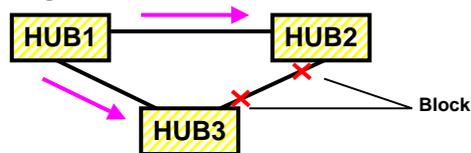
2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

83

STPの動作-2

Root Bridge



- STPを利用する
 - STPの利用によりRoot Bridgeからツリーが構成され、冗長経路はブロッキングされる
 - ブロッキングによりループを防ぐ
- ブロッキングとは
 - 通信が止められている状態
 - ただし、STPのHelloは通信されている



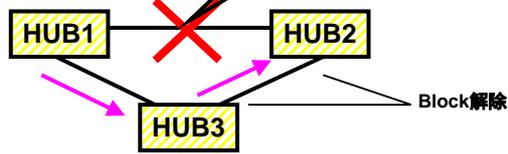
2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

84

STPの動作-3

Root Bridge



- 障害発生が発生した場合
 - 障害発生によりブロッキングが解除され、バックアップされる



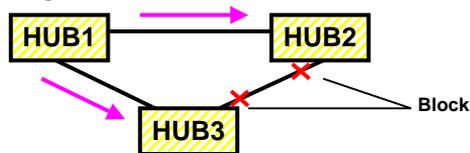
2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

85

STPの動作-4

Root Bridge



- 障害が復旧すると
 - 再びSTPによりRoot Bridgeからツリーが構成され、冗長経路はブロッキングされる

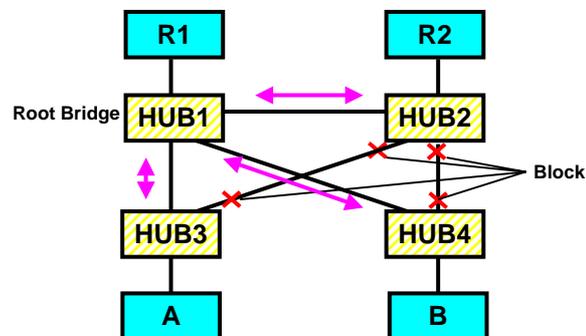


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

86

STP事例-1



- 全てのHUBをRoot Bridgeに最短となるように設計
- STPにより冗長化経路をブロッキングする

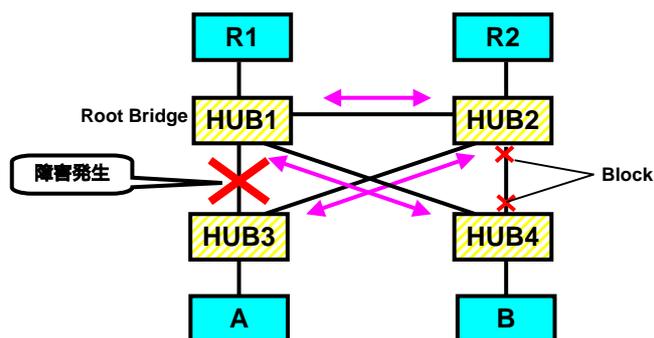


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

87

STP事例-2



- 障害が発生するとSTPによりバックアップ経路に切り替わる

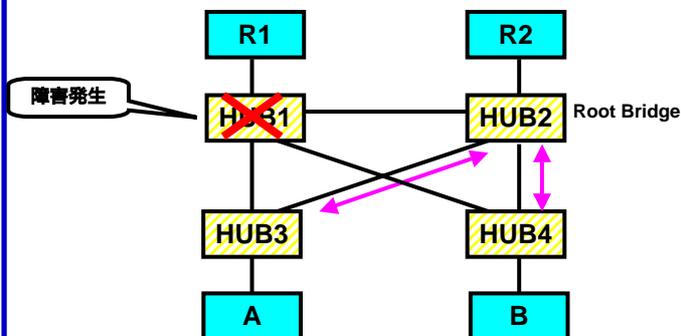


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

88

STP事例-2



- HUBに障害が発生した時もSTPによりバックアップされる
- Root Bridgeに障害が発生した場合には切り替えに時間がかかる



2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

89

STPまとめ

- STP (Spanning Tree Protocol)
- IEEE 802.1Dの中で定義されている
- データリンク層(L2)プロトコル
- Root Bridgeからツリーを構成する
- ブロッキングによりループを防止する
- 遠隔地への伝送時などに有効に利用される
- Root BridgeはMACなどにより決定されるが、設定することも可能

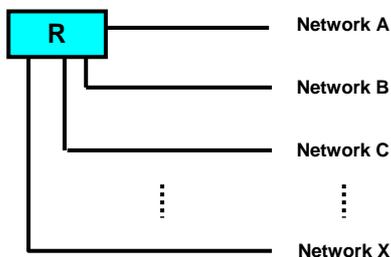


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

90

VLAN Trunk-1



- VLAN Trunkしない場合
 - 多くのネットワークを接続する場合、VLAN Trunkを利用しないとルータに多くのインターフェースを用意する必要があり、コストがかかる

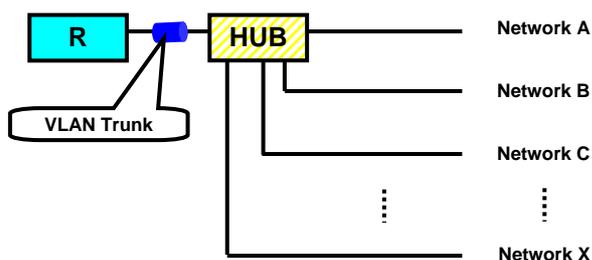


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

91

VLAN Trunk-2



- VLAN Trunkを利用する
- VLAN Trunkによりルータのインターフェースが1つであっても仮想的に複数のインターフェースがあるように見せることができる
- ルータと比較して安価なHUBのポートをルータのインターフェースとして見せることができる



2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

92

VLAN Trunkまとめ

- VLAN
 - Virtual LAN
 - 1つのHUB内の異なるLANの扱いをVLANと呼ぶ
 - VLAN Trunk、タグVLANのことを略してVLANと呼ぶこともある
- VLAN Trunk
 - 複数のVLANを1つのデータリンク層でまとめて通信する
 - 「タグ付VLAN」、「タグVLAN」とも呼ばれる
 - IEEE 802.1Qで定義されている
 - メーカー独自のものも存在する
- VLAN Trunkによりルータのインターフェースが1つであっても仮想的に複数のインターフェースがあるように見せることができる
- ルータに比較して安価なHUBのポートをルータのインターフェースとして見せることができる
- HUBをカスケードして利用する場合にはHUBのダウンを検知できなくなるため注意が必要

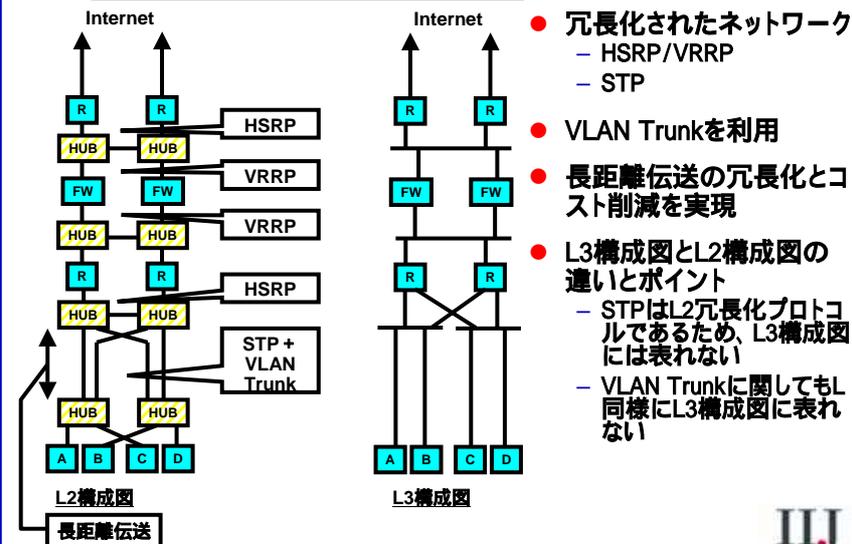


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

93

STP+VLAN Trunk事例



2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

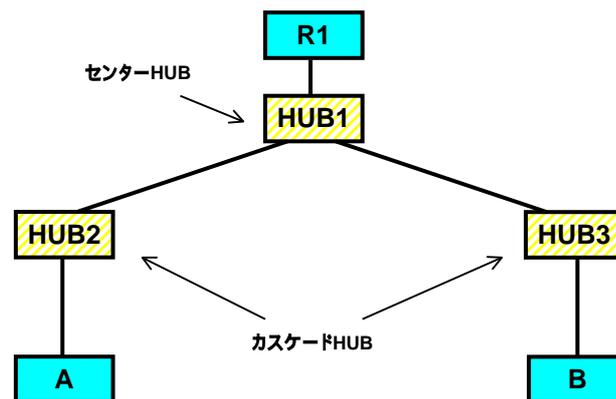
94

L2ループ対策

- ネットワーク構築に必要なL2ループ対策法について解説します
- L2ループを発生させないための設定に関して解説します
 - L2ループの発生パターン
 - Scheduler設定による障害の軽減
 - STPによる対策
 - Storm controlによる対策



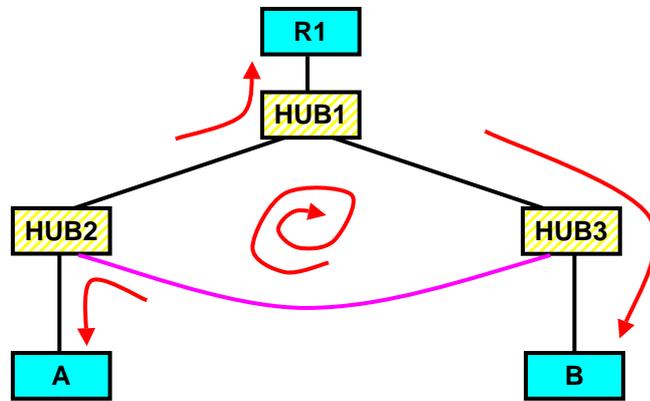
カスケード接続-1



- センターHUBに2台のカスケードHUBを構成した場合
- カスケードHUBはオフィスの机上などに設置



L2ループタイプ1:カスケードHUB間ループ接続



- ユーザが誤って隣同士のHUBを接続してしまう
- センターHUBを巻き込んだL2ループが発生

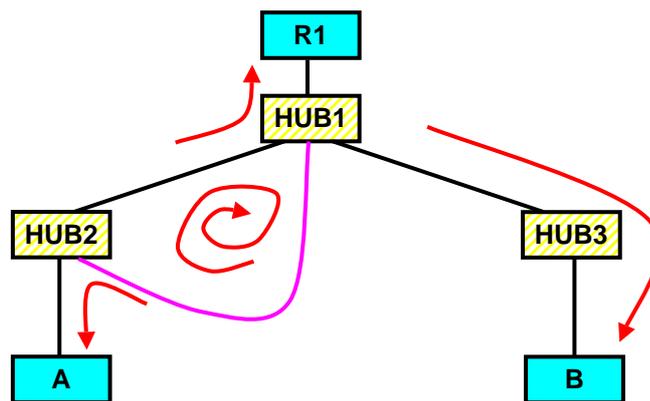


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

97

L2ループタイプ2:センターHUB二重接続



- ユーザが誤って上位HUBと2本接続してしまう
- センターHUBを巻き込んだL2ループが発生
- 情報コンセントが近くに2つあった場合に発生しやすい

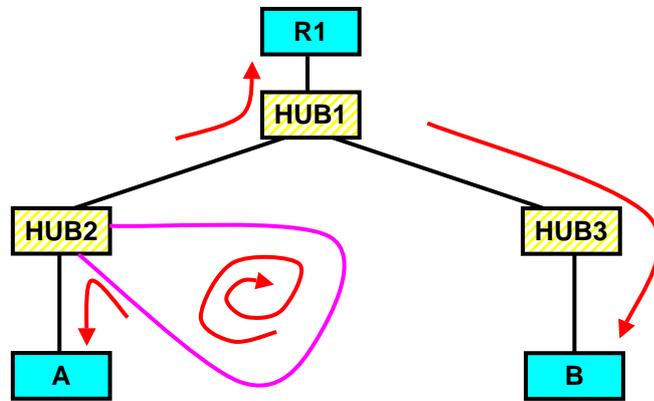


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

98

L2ループタイプ3:カスケードHUB内ループ接続



- ユーザが誤ってカスケードHUBでループ配線をしてしまう
- カスケードHUB内でL2ループが発生
- 他のHUBにもアップリンクを通して影響を及ぼす

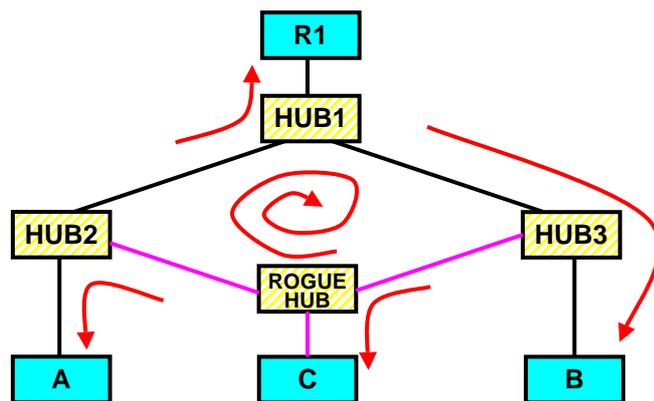


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

99

L2ループタイプ4: ROGUE HUBによるカスケードHUB間ループ接続



- ユーザが不正なHUBを他の2つのHUBに誤った構成で接続してしまう
- センターHUBを巻き込んだL2ループが発生

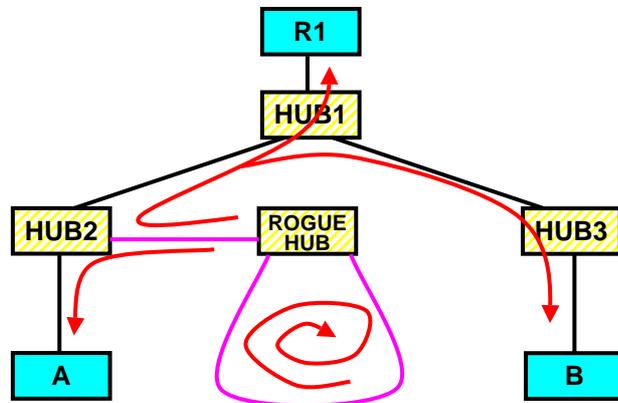


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

100

L2ループタイプ5:ループ状態のROGUE HUBの接続



- ユーザが不正なHUBを接続した上で誤ってループ配線をしてしまう
- 不正HUB内でL2ループが発生
- 他のHUBにもアクセスポートを通じて影響を及ぼす

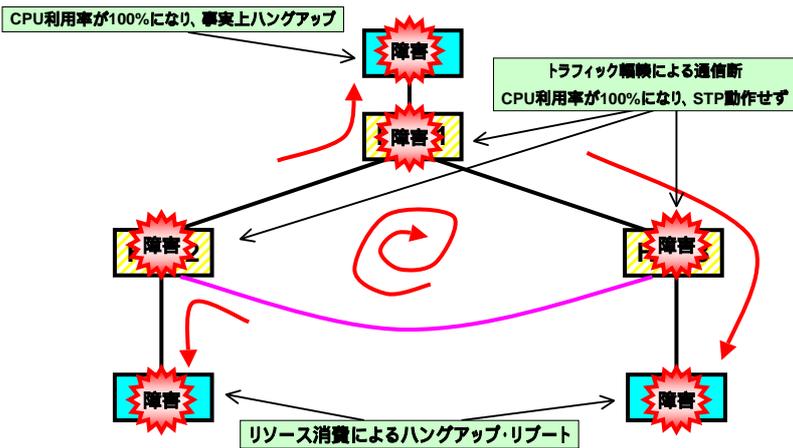


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

101

L2ループ発生時の障害



- L2ループ発生時に様々な問題が発生

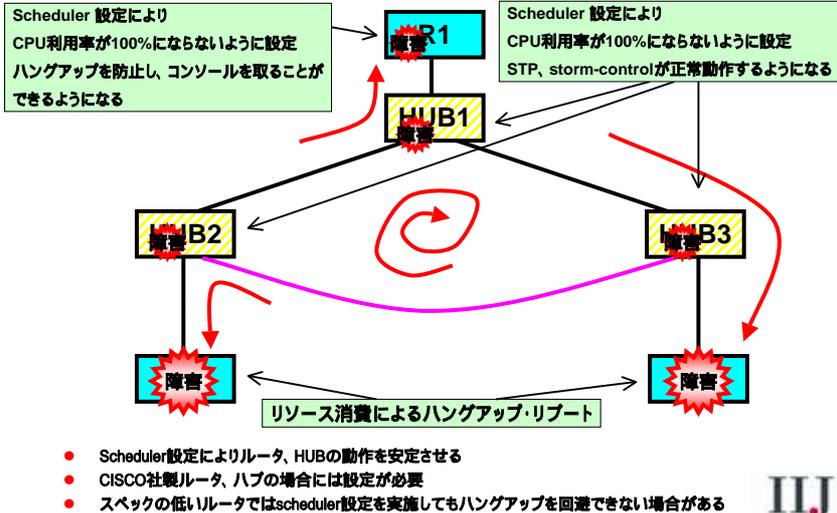


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

102

L2ループ発生時の障害の軽減



2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

103

L2ループ発生時の障害の軽減

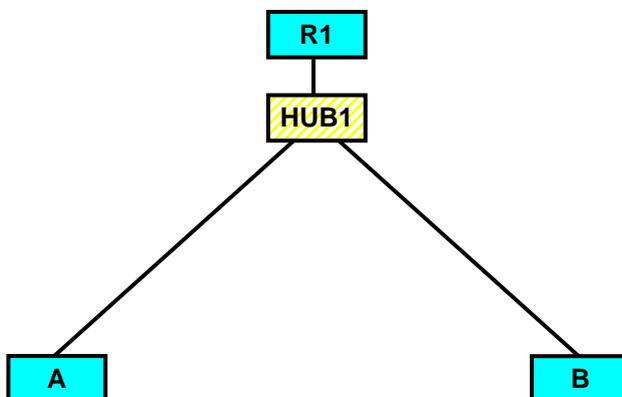
- Scheduler設定
 - CISCO社製ルータ、ハブに設定
 - ブロードキャスト、マルチキャストの受信量が一定量を越えるとCPU利用率が100%となり、ルータやHUBが事实上ハングアップし、コンソールを取ることができなくなる現象が発生する。このコマンド設定によりハングアップを回避することができる
 - L2ループが発生すると多量のブロードキャスト、マルチキャストが発生するため、L2ループ対策を行うには必ず設定する必要がある
 - このコマンドを利用しないと、ループを回避するためのSTPやstorm-controlが正常に動作しないことがある
 - スペックの低いルータではscheduler設定を実施してもハングアップを回避できない場合がある
- 設定パラメータ(CISCO社推奨値)
 - 新機種設定
 - scheduler allocate 3000 1000
 - 従来機種設定
 - scheduler interval 500

2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

104

カスケードHUB接続の禁止-1



- カスケードHUB接続を禁止する
- 禁止しても不正 HUB接続を防止することは難しい



2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

105

カスケードHUB接続の禁止 - 2

- カスケードHUB接続の禁止
 - カスケードHUBを禁止し、センターHUBから直接端末を接続するように構成を変更する
 - カスケードHUBの接続に関するL2ループを回避することができる
- カスケードHUB接続の禁止の限界
 - センターHUBコスト、配線コストがかかるため、現実的に実施が難しい
 - 不正HUBが接続されてしまうと、カスケードHUBを禁止しても意味がなくなってしまう

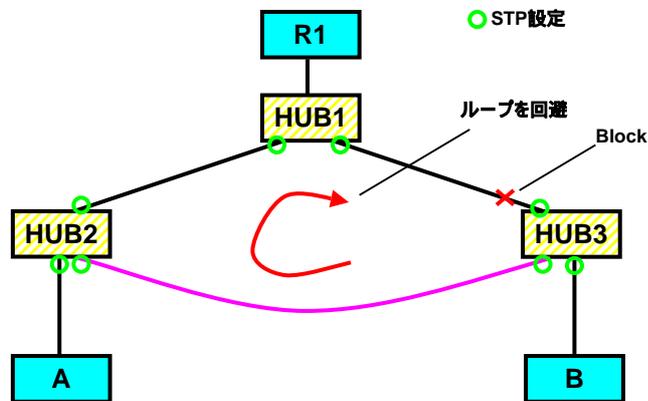


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

106

L2ループの回避 STP設定 - 1



- STPを設定することで内部ループを回避することができる
- 副作用で不要なSTPパケットが端末側に流れてしまう
- カスケードHUBがSTPに対応している必要がある



2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

107

L2ループの回避 STP設定 - 2

- STP設定
 - ループが発生する可能性があるポートにSTPを設定することで、方がループが発生した場合に、これを回避することができる
 - カスケードHUBがSTPに対応してなければならない
 - 安価なHUBは対応していない場合が多い
 - STPに対応していない場合にはループ回避できない
- STP設定に伴う副作用
 - HSRP/VRRPなどとの同時利用時に誤動作を起こす
 - STP設定を行うと、STPネゴシエーション時間のためにリンクアップするものの通信ができない状態が発生する。この状態時にHSRP/VRRPが障害と誤検知し、Standby側がActive状態となり、すべてのHSRP/VRRPルータがActiveとなってしまう。
 - HSRP/VRRPのtimerをチューニングすることで回避することができるが、切り替え時間を長く設定する必要がある
 - STPパケットが端末まで流れてしまう
 - 正常に利用している端末にまでSTPパケットが流れてしまい、利用帯域を圧迫してしまう。
 - 高負荷時にはSTPパケットを優先するため、若干のパケットロスが生じる

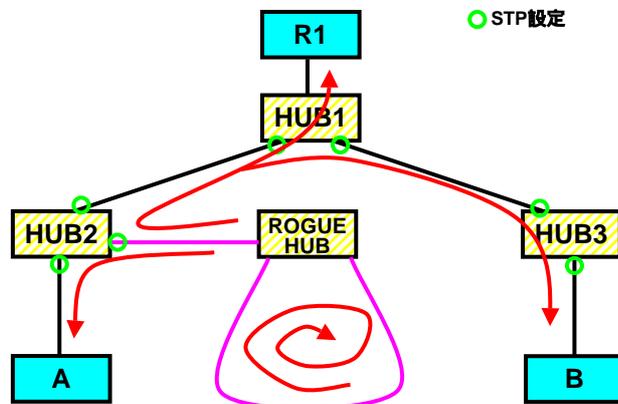


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

108

L2ループの回避 外部ループとSTP設定 - 1



- STPを設定しても不正HUBなどによる外部ループを回避できない



2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

109

L2ループの回避 外部ループとSTP設定 - 2

- STP設定によるL2ループ回避の範囲
 - STP設定によるL2ループ回避はSTP対応HUBにてループを検知できるトポロジのみに対応
 - STPを設定することで様々な副作用が生じるため、設定するリスクに対して効果が薄い
- 外部ループとSTP設定
 - STPを設定しても不正HUBなどによる外部ループによるトラフィック流入を回避できない



STPを利用せず、外部ループに対応した対策とは？

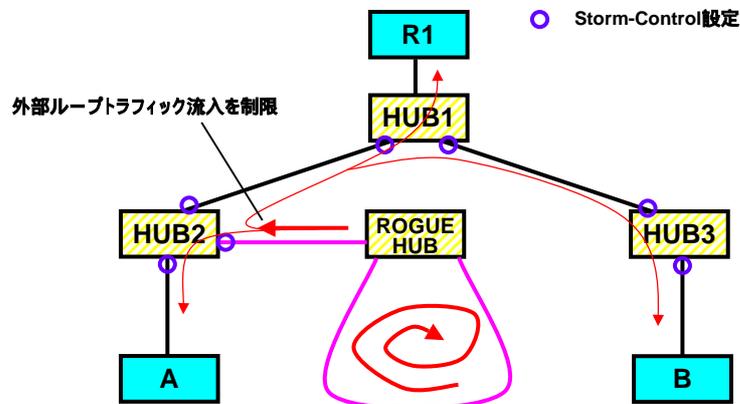


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

110

L2ループの回避 Storm-Control設定 - 1



- Storm-Controlにて外部ループからのトラフィック流入を抑制
- ネットワークを守ることはできるが、根本的な原因となっているループを止めることはできない



2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

111

L2ループの回避 Storm-Control設定 - 2

- Storm-Control設定
 - 特定の packet タイプ (unicast, broadcast, multicast) のトラフィックが一定トラフィック量を超えた時に、パケットを破棄する設定
 - 指定のトラフィック量を下回った場合には再びパケットの受信を開始する
 - トラフィックはIPアドレスやMACアドレスで特定のトラフィックを指定することができない
 - broadcast, multicastはL2ループが発生した場合にL3機器に大きな影響を与えるため、storm-control設定をした方がよい
- Storm-Control設定例
 - インターフェースの10.00%(10Mbps)を越えるbroadcastもしくはmulticastパケットを受信した場合にはパケットを破棄する。
 - トリガーとなったパケットがインターフェースの1.00%(1Mbps)を下回った場合にはパケットの受信を再開する

```
interface FastEthernet0/1
storm-control broadcast level 10.00 1.00
storm-control multicast level 10.00 1.00
```

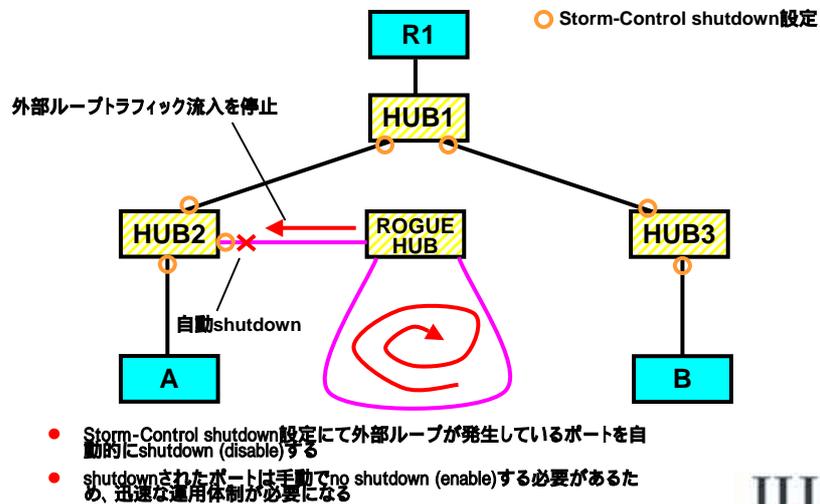


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

112

L2ループの回避 Storm-Control shutdown設定-1



2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

113

L2ループの回避 Storm-Control shutdown設定-2

- Storm-Control shutdown設定
 - 特定のパケットタイプ(unicast, broadcast, multicast)のトラフィックが一定トラフィック量を超えた時に、インターフェースをshutdownする設定
 - トラフィックはIPアドレスやMACアドレスで特定のトラフィックを指定することができない
 - ループの原因となるトラフィックを完全に止めることができる
 - 手動でno shutdownしないかぎり復旧しない
 - 迅速で適切な運用体制を維持する必要があり、放置すると一部の端末が長時間通信できない状態となる
- Storm-Control shutdown設定例
 - インターフェースの10.00%(10Mbps)を超えるbroadcastもしくはmulticastパケットを受信した場合には該当のポートをshutdownする。

```
interface FastEthernet0/1
storm-control broadcast level 10.00
storm-control multicast level 10.00
storm-control action shutdown
```

2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

114

ルータとレイヤ3スイッチ

● ルータとレイヤ3スイッチの違いについて解説します

- 今までルータとレイヤ3スイッチは区別してきませんでした。
- 機器選定などで必要となる違いについて解説します

- ルータとレイヤ3スイッチの比較表
- ルータを選択する構成
- レイヤ3スイッチを選択する構成
- レイヤ2スイッチ付きルータとは
- ルータとレイヤ3スイッチの最適配置



ルータとレイヤ3スイッチの比較表

	ルータ	L2SW付ルータ	L3SW-L	L3SW-M	L3SW-H
コスト	低～高	低～高	低	中	高
L3性能	中	中	高	高	高
ポート数	1～	4～	12～	24～	24～
ポート単価	高	中	低	低	中
L3ルーティング					
スタティックルーティング					
ダイナミックルーティング					
Ethernet					
ISDN			×	×	
Ethernet以外の専用線			×	×	
PPPoE			×	×	
VPN			×	×	
NAT			×	×	
L2スイッチング	×				
STP	×				
SPANポート	×				
Storm-Control	×				

ルータ: L2SWを搭載していないルータ
 L2SW付ルータ: L2SWを搭載しているルータ
 L3SW-L: 固定構成ローエンドレイヤ3スイッチ
 L3SW-M: 固定構成ミドルレンジレイヤ3スイッチ
 L3SW-H: モジュール構成ハイエンドレイヤ3スイッチ

製品によっては機能が追加もしくは削除されているものがあります。



ルータを選択する構成

- ルータを選択する構成
 - Ethernet以外の専用線を利用
 - ISDNを利用
 - VPNを利用
 - PPPoEを利用
 - NATを利用
 - 利用ポート数が少ない
 - 高いスループットは必要としない
 - 100Mbps以下
 - ハイエンドルータは高スループットだが、ポート単価は高い
 - ダイナミックルーティングの対応が豊富
 - 柔軟にWANに対応

ISDN: Integrated Services Digital Network (NTT INS64, INS1500など)

VPN: Virtual Private Network

PPPoE: PPP over Ethernet (NTT FLET'S網などで利用)



2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

117

レイヤ3スイッチを選択する構成

- レイヤ3スイッチを選択する構成
 - LAN、WANともにEthernetのみ利用
 - 利用ポート数が多い
 - レイヤ2スイッチとしても利用
 - サーバやPCを直接接続
 - 高いスループット
 - 100Mbps ~
 - STP、Storm-Controlなどの機能を利用
 - SPANポートを利用したパケットモニターが必要
 - ハイエンド機器では拡張モジュールなどでルータと同機能を持つことが可能

SPAN: Switched Port Analyzer (ミラーポートとも呼ばれる)



2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

118

レイヤ2スイッチ付きルータとは

- レイヤ2スイッチ付きルータとは
 - ルータにレイヤ2スイッチが搭載された機器
 - レイヤ3性能はルータと同じで、レイヤ3スイッチに劣る
 - STP、Storm-Control、SPANポートなどレイヤ2スイッチの機能を利用することができる
 - VPN、NAT、PPPoEなどルータの持つ機能をそのまま利用できる
 - 設定はレイヤ3スイッチのように扱うことが可能
 - 利用できるポート数はルータより多く、レイヤ3スイッチより少ない
 - ポート単価はルータより安く、レイヤ3スイッチより高い
 - 小規模拠点のゲートウェルルータ兼センタースイッチとして利用
 - レイヤ2スイッチ機能はレイヤ3スイッチに搭載されている同機能に劣る場合がある(VLAN数の制限など)



ルータとレイヤ3スイッチの最適配置

- ルータとレイヤ3スイッチの最適配置
 - ルータは豊富なWANインターフェースやNATなどのアプリケーション機能を持つため、WAN接続部分に配置する
 - レイヤ3スイッチは高いスループットを活かすためにLAN間接続のコアスイッチとして配置する
 - 小規模拠点などはレイヤ2スイッチ付きルータ1台でWAN、LAN両方のルーティング機能を持たせる



ネットワーク構築

- ネットワーク構築に必要なL2ネットワークの構成法について解説します
- 配線に必要な部材について紹介します

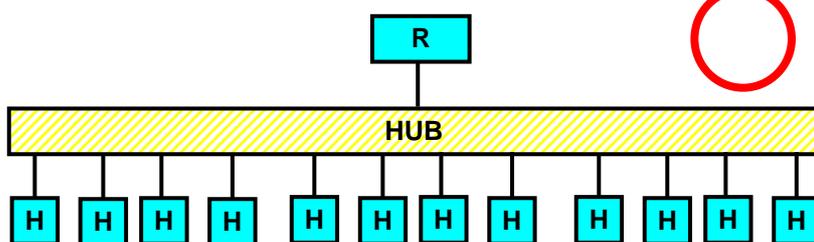


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

121

L2ネットワーク構成 カスケードなし



- 標準的なカスケードの無いL2ネットワーク
- ホストの数だけ多ポートのHUBを用意する必要がある
- 遅延は少なく、L2障害発生の可能性も低く安定している
- HUBのカスケード接続は許可しないことで、L2ループなどの障害発生を防止できる

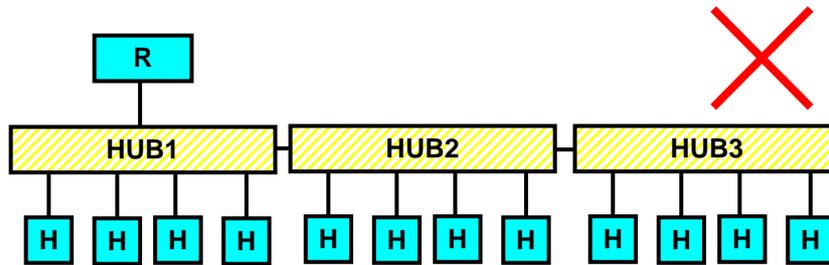


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

122

L2ネットワーク構成 横繋ぎカスケード



- 横繋ぎカスケードによるL2ネットワーク
- 安価なHUBをカスケード接続利用できる
- 障害発生時に障害箇所の特定が困難
- カスケードポイントに障害が発生するとL2ネットワークが分断し、正常に冗長化できない
- 誤ったカスケード構成によりループが発生する可能性がある

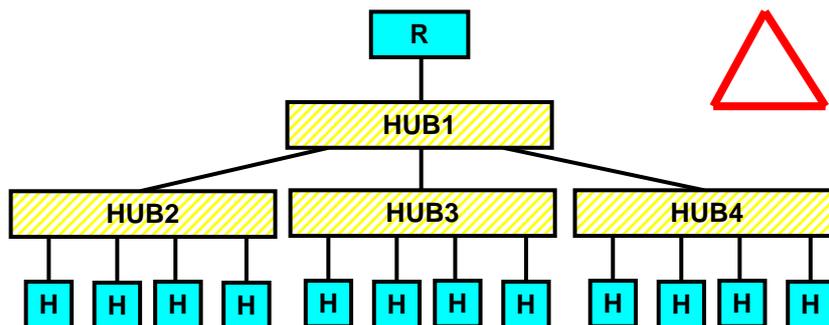


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

123

L2ネットワーク構成 ツリー型カスケード



- ツリー型カスケードによるL2ネットワーク
- 安価なHUBをカスケード接続利用できる
- 障害箇所をある程度局所化できる
- カスケードポイントに障害が発生するとL2ネットワークが分断し、正常に冗長化できない
- 誤ったカスケード構成によりループが発生する可能性がある

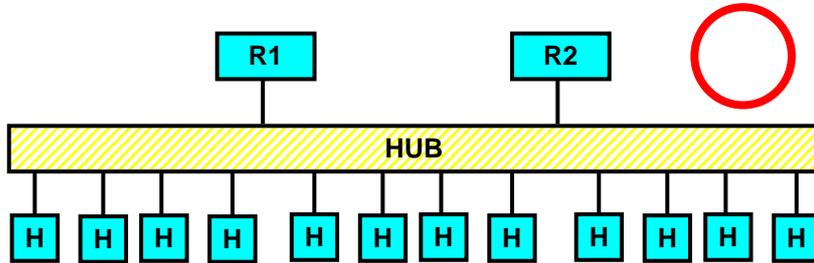


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

124

冗長化L2ネットワーク構成 カスケードなし



- 標準的なカスケードの無いL2ネットワーク
- ホストの数だけ多ポートのHUBを用意する必要がある
- 遅延は少なく、L2障害発生の可能性も低く安定している
- HUBのカスケード接続は許可しないため、L2ループなどの障害発生を防止できる
- 1台のHUBの障害で1つのL2ネットワークが全滅してしまうため、完全な冗長化とはならない

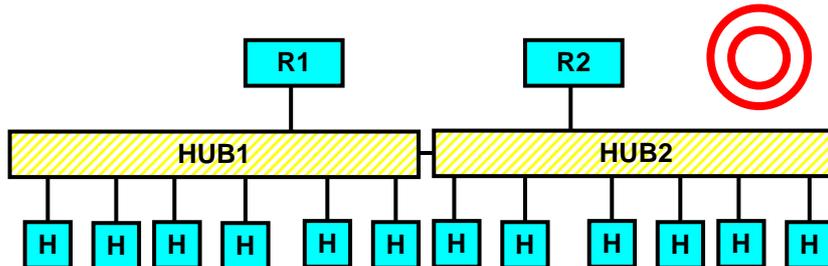


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

125

冗長化L2ネットワーク構成 2台カスケード



- 2台カスケードによるL2ネットワーク
- カスケードポイントに障害が発生するとL2ネットワークが分断し、正常に冗長化できない
 - この区間のみSTPやチャネル接続などにより冗長化をはかる方法もある
 - STPを利用することで、STP要因による障害も発生する可能性があるため、カスケードケーブルが短い場合には冗長化せずに接続する方がよい
- 1台のHUBが故障してももう1台のHUBによりL2ネットワークの一部が動作し続ける
- ホストも冗長化し、2台のHUBに接続すれば完全な冗長化を図ることが可能

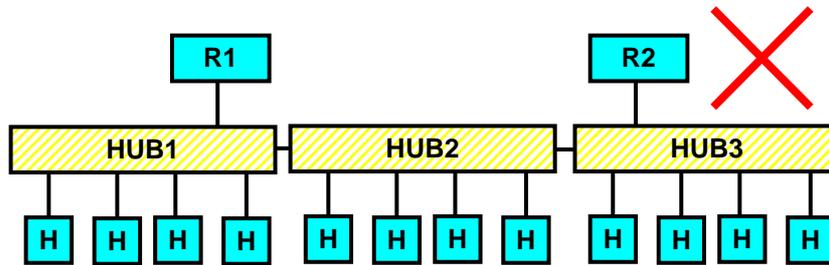


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

126

冗長化L2ネットワーク構成 3台以上カスケード



- 3台以上カスケードによるL2ネットワーク
- 安価なHUBをカスケード接続利用できる
- 障害発生時に障害箇所の特定が困難
- HUB2に障害が発生するとL2ネットワークが分断し、正常に冗長化できない
- 3台以上をカスケードし、冗長化を図るにはSTPが必要になる

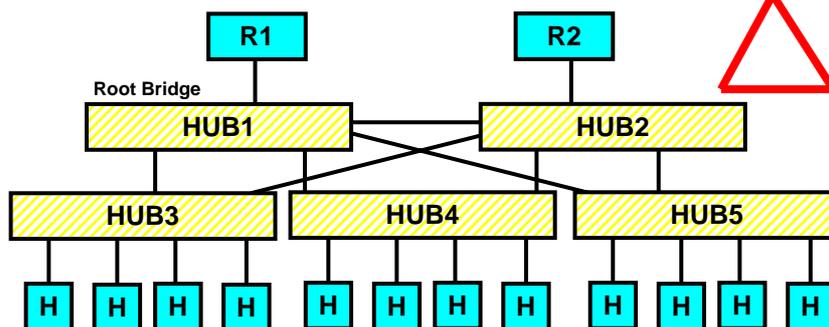


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

127

冗長化L2ネットワーク構成 STP利用



- STPを利用したカスケードによるL2ネットワーク
- 安価なHUBをカスケード接続利用できる
- 障害発生時にはSTPの状態を確認するスキルが必要
- カスケードポイントに障害が発生してもSTPにより冗長化される
- STPの特性により、障害時の切り替え時間、切り戻り時の通信不通時間が長くなる



2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

128

L2ネットワーク構成のまとめ

- L2ネットワークは極力カスケードしないほうがよい
- 多くのホストを収容する場合には多ポートのHUBを利用する
- 多ポートのHUBでも収容できない場合にはサブネットを分割し、異なるL2/L3ネットワークに収容する
- やむを得ずカスケードする場合にはツリー型カスケードとする
- L2ループを防止するため、カスケードするHUBを管理する
- 冗長化ネットワーク構成を組む場合にはカスケードは2台までとする
- 3台以上のカスケードを行う必要がある場合にはSTPを利用する必要がある



配線部材 (メタル)

Ethernet規格と対応ケーブル

	カテゴリ3	カテゴリ5	カテゴリ5e	カテゴリ6
10BASE-T				
100BASE-TX				
1000BASE-T				
1000BASE-TX				

カテゴリ5e:エンハンスド・カテゴリ5

- HUB-端末間
 - カテゴリ5eを推奨
 - カテゴリ6であればすべての規格に対応するが、コスト高となる
- ルータ-HUB間
 - カテゴリ6を推奨
 - 1000BASE-TXを利用しない場合でも今後のLANの高速化への対応と下位規格での安定した品質を提供できる



配線部材 (光ファイバ)

Ethernet規格と対応光ファイバ

	MMF	SMF	DSF	最大延長
100BASE-FX				2km
100BASE-BX10-D/U				10km
1000BASE-SX				220m ~ 550m
1000BASE-LX				550m/10km
1000BASE-ZX				70km
1000BASE-BX10-D/U				10km
10GBASE-SR				26m ~ 82m
10GBASE-LR				10km
10GBASE-ER				40km

MMF: Multi-mode Fiber
SMF: Single-mode Fiber
DSF: Dispersion Sifted Single-mode Fiber

- 同一ラック内、同一フロア内
 - MMFを推奨
 - SMFでも支障はないが、安価な1000BASE-SX対応HUBを利用できなくなるため、コスト高となる
 - MMF新規格であれば50/125 μm GI(Graded Index)ファイバを選択
 - 異なるフロア間
 - SMFを推奨
 - MMFでは長距離を引き伸ばすことができない
 - SMFはWAN同様の延長や事前敷設、10GbEにも利用可能
 - SMFは多くのメディアコンバータにも対応しており、100BASE-TXや1000BASE-Tを安価に延長できる
 - 異なるビル間
 - SMFを推奨
 - 長距離となる場合にはDSFを検討しても良いが、通常利用することは無い
- 最大延長は光ファイバの品質などにより変動します

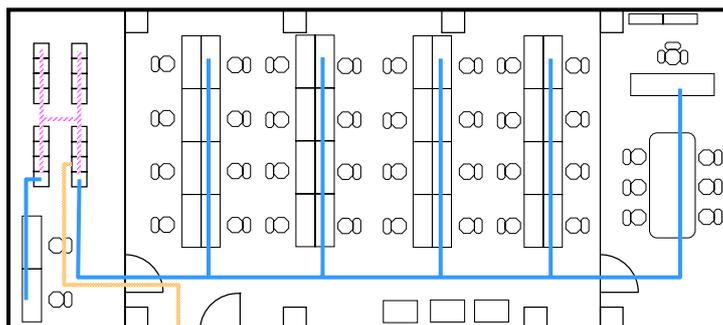


2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

131

配線例



他のフロアへ

— Cat5e (100BASE-TX端末接続用)
- - - Cat6 (1000BASE-Tサーバ接続用)
- - - SMF (1000BASE-LXフロア間用)

- 適切なケーブル敷設により低コストと高い拡張性を実現する
 - 端末接続用にはCat5eで100BASE-TXを利用 (1000BASE-Tまで対応可能)
 - サーバ接続用にはCat6で1000BASE-Tを利用
 - フロア間接続にはSMF(光ファイバ)で1000BASE-LXを利用



2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

132

ネットワークトラブルシューティング

- Ethernetを利用したLANや回線で遅かったり、エラーが出る
 - Duplexミスマッチ
 - 対向となる通信機器のDuplexが異なることによる通信エラー
 - Late collisionなどが検出される
 - Full Duplex-Full Duplex(全二重同士)/Half Duplex-Half Duplex(半二重同士)など、おなじDuplexに設定することで問題は解消する
 - Autoに設定するとHalf Duplexとなる機器
 - Autoに設定しないとFull Duplex動作しない機器
 - Full Duplexに設定するとエラーが出る機器
 - ケーブル不良
 - ケーブル自体、コネクタ、継ぎ手、パッチパネルなどの不良による品質劣化による通信エラー
 - CRCエラーなどが検出される
 - ケーブルの交換、継ぎ手やパッチパネル区間を無くすか品質の高いものに交換することで問題は解消する
 - 継ぎ手やパッチパネルなどは極力なくして配線したほうがよい
 - 市販ケーブルであってもクロストークなどが測定できるケーブルテスターでテストを行う



2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

133

ネットワークトラブルシューティング

- Ethernetを利用したLANや回線で遅かったり、エラーが出る(続き)
 - STPに起因する問題
 - 利用していないSTPによる通信エラー
 - ネットワーク高負荷時にCRCエラーが0.01%程度観測される
 - STPをoffにすることで問題は解消する
- HSRP/VRRPが一時的に両方がアクティブなり、誤動作する
 - STPに起因する問題
 - STPネゴシエーション時にリンクはあがっている状態にも関わらず通信できない状態が発生し、このとき、HSRP/VRRPが誤動作する
 - STPをoffもしくはportfastに設定する
 - VLAN trunkに起因する問題
 - VLAN trunkのネゴシエーション時に、リンクはあがっている状態にも関わらず通信できない状態が発生し、このとき、HSRP/VRRPが誤動作する
 - VLAN trunk上でHSRP/VRRPを利用しないようにネットワークを変更する
 - HSRP/VRRP timerを調整し、hold timeをネゴシエーション時間より長くする



2006/12/5

Copyright © 2006 Internet Initiative Japan Inc.

134

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
- リピータハブとスイッチングハブ、スイッチングハブとルータの違い
 - スwitchingハブはリピータハブに比べLANを有効に利用できる
 - スwitchingハブのみのネットワークはbroadcastに脆弱で、ウイルスを原因としたLAN輻輳を起こしてしまう
 - ルータを利用することでbroadcast floodを回避し、ウイルスを原因としたLAN輻輳を回避でき、障害に強ネットワークを構築することができる
- インターネット接続にはルーティングは必須
- 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



まとめ - 2

- 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
- 冗長化のためにSTP、HSRP/VRRPなどを利用する
- VLAN Trunkによりポート単価を下げる事が可能
- L2ループが発生に備え、Storm-Controlなどの対策を実施する
- L2ネットワーク構築では極力カスケード接続を避ける
- ルータとレイヤ3スイッチを最適配置する
- 配線はできるがきりパッチパネルを利用せず、I/Fのエラーの状況からトラブルを解決する

