LAN/WAN基礎研修の振り返り
(Cisco機器の基本操作)

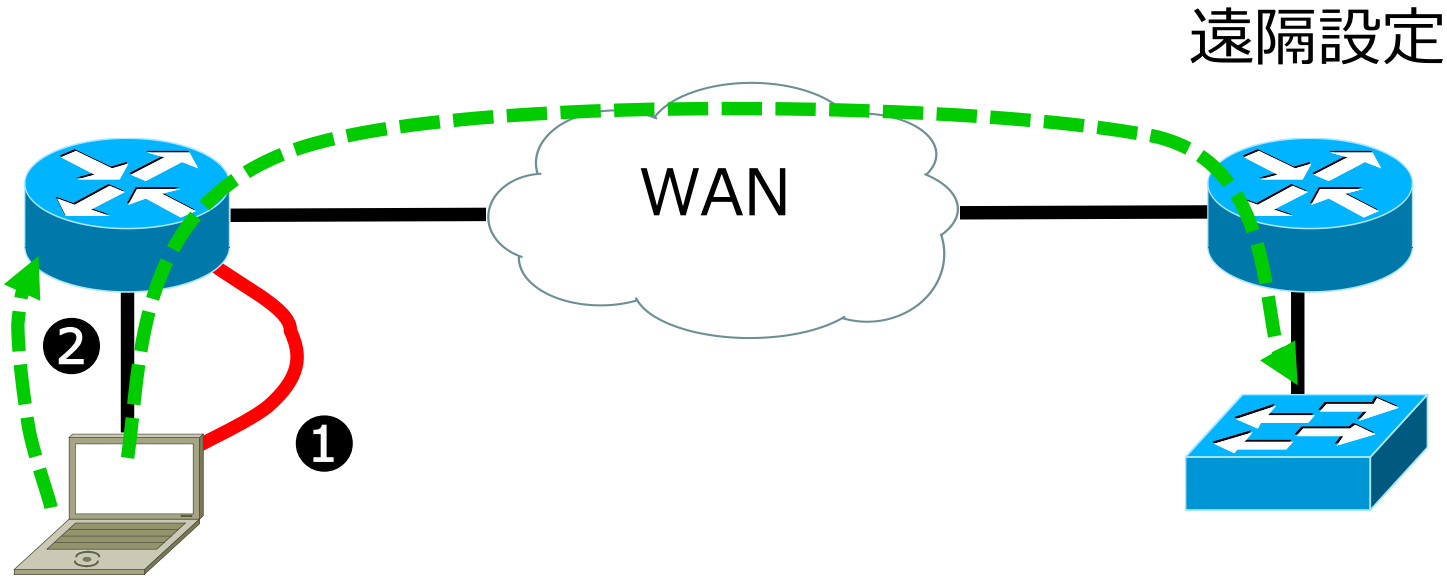
●ルータ（Cisco891F）

①ルーテッドポート
　インターネット接続、VPN接続など

②コンソールポート
　Config設定のためにConsoleケーブルでPCと接続するポート

③スイッチングハブポート
　クライアントPCの接続など

●Cisco機器の設定方法



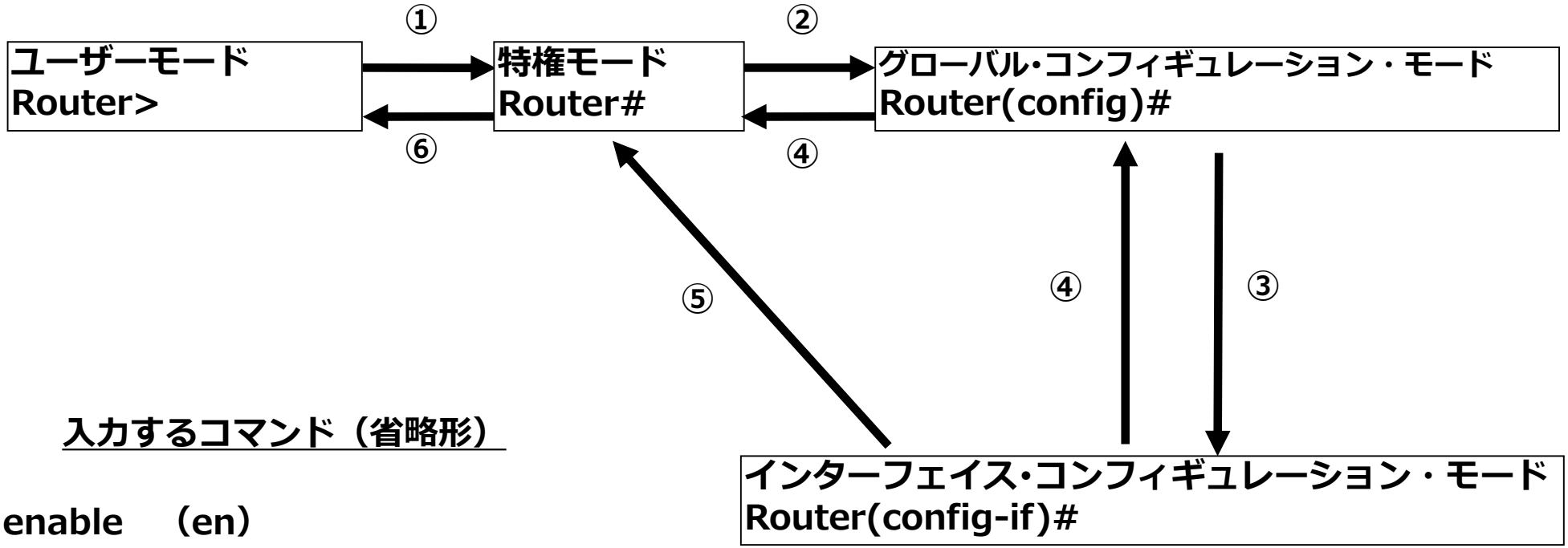
❶コンソール接続

コンソールケーブルを使用しConfig設定する

❷Telnet接続

ネットワーク経由でリモートアクセス（Telnet）を行い設定変更する

●主な設定モード



入力するコマンド（省略形）

① enable　（en）
② configure terminal（conf t）
③ interface xx　(int fa 8)　　xxはfastethernet 8など
④ exit （exi）
⑤ end
⑥ disable（disa）

●確認コマンド(show running-config)

```
Router#sh run
Building configuration...

Current configuration : 1556 bytes
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ip source-route
!
 --More--
```

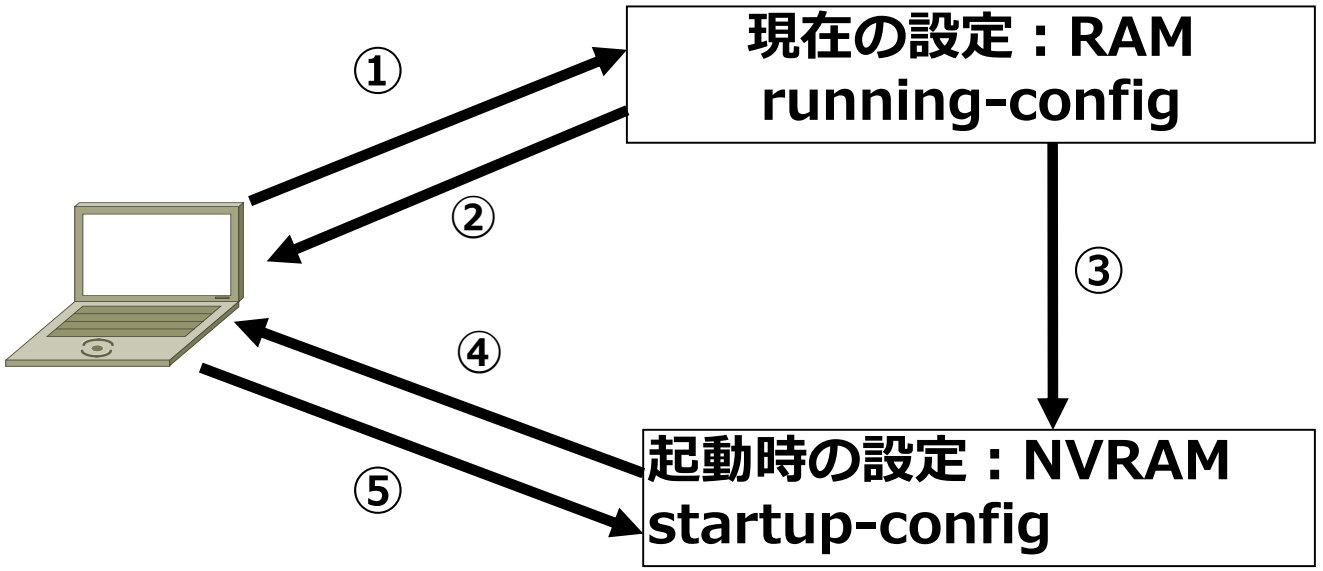
●確認コマンド(show ip interface brief)

```
Router#sh ip int brie
Interface              IP-Address      OK? Method  Status                Protocol
Async3                 unassigned      YES unset   down                  down
BRI0                   unassigned      YES unset   administratively down down
BRI0:1                 unassigned      YES unset   administratively down down
BRI0:2                 unassigned      YES unset   administratively down down
FastEthernet0          unassigned      YES unset   administratively down down
GigabitEthernet0       unassigned      YES unset   down                  down
GigabitEthernet1       unassigned      YES unset   down                  down
GigabitEthernet2       unassigned      YES unset   down                  down
GigabitEthernet3       unassigned      YES unset   down                  down
GigabitEthernet4       unassigned      YES unset   down                  down
GigabitEthernet5       unassigned      YES unset   down                  down
GigabitEthernet6       unassigned      YES unset   down                  down
GigabitEthernet7       unassigned      YES unset   down                  down
GigabitEthernet8       unassigned      YES unset   administratively down down
Vlan1                  unassigned      YES unset   down                  down
```

●確認コマンド(show ip route)

```
Router#sh ip ro
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C          10.10.100.0/24      is directly connected, GigabitEthernet0
L          10.10.100.1/32      is directly connected, GigabitEthernet0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C          172.16.0.0/16       is directly connected, Vlan1
L          172.16.100.1/32     is directly connected, Vlan1
     192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
C          192.168.100.0/24  is directly connected, FastEthernet8
L          192.168.100.1/32  is directly connected, FastEthernet8
S     192.168.200.0/24   [1/0]   via   192.168.100.254
```

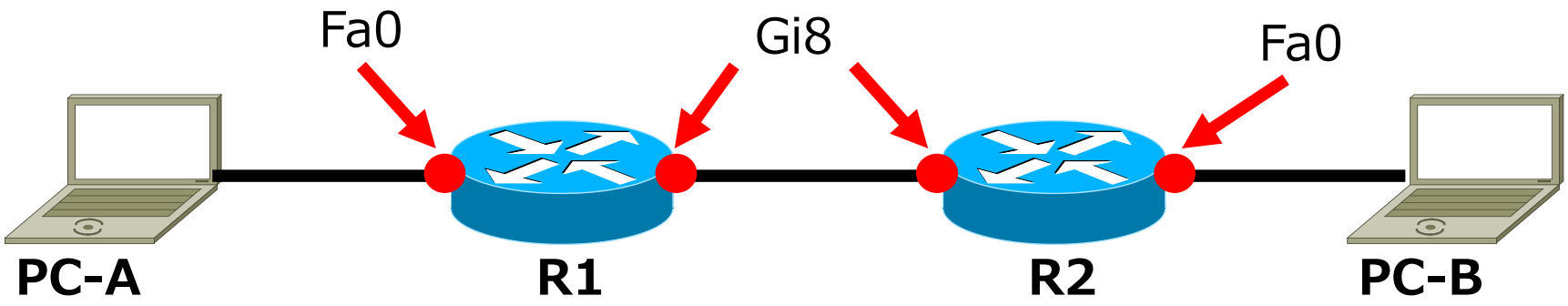
●保存と初期化



入力するコマンド（省略形）

① configure terminal　（conf t）
② show running-config（sh run）
③ copy running-config startup-config（copy run star）
④ show startup-config（sh star）
⑤ erase startup-config（era star）

●スタティックルーティング演習



R1
Gi8 : 10.1.100.9 /30
Fa0 : 192.168.1.46 /28

R2
Gi8 : 10.1.100.10 /30
Fa0 : 192.168.1.62 /28

●演習のルータ設定

```
>en
#conf t
(config)# int fa 0
(config-if)# ip address IPアドレス サブネットマスク
(config-if)# no shutdown
(config-if)# exit
(config)# int gi 8
(config-if)# ip address IPアドレス サブネットマスク
(config-if)# no shutdown
(config-if)# exit
(config)# ip route ネットワークアドレス サブネットマスク ネクストホップアドレス
(config)# end
```

1章
L2SW/L3SW

●L2スイッチ(Catalyst2960X)

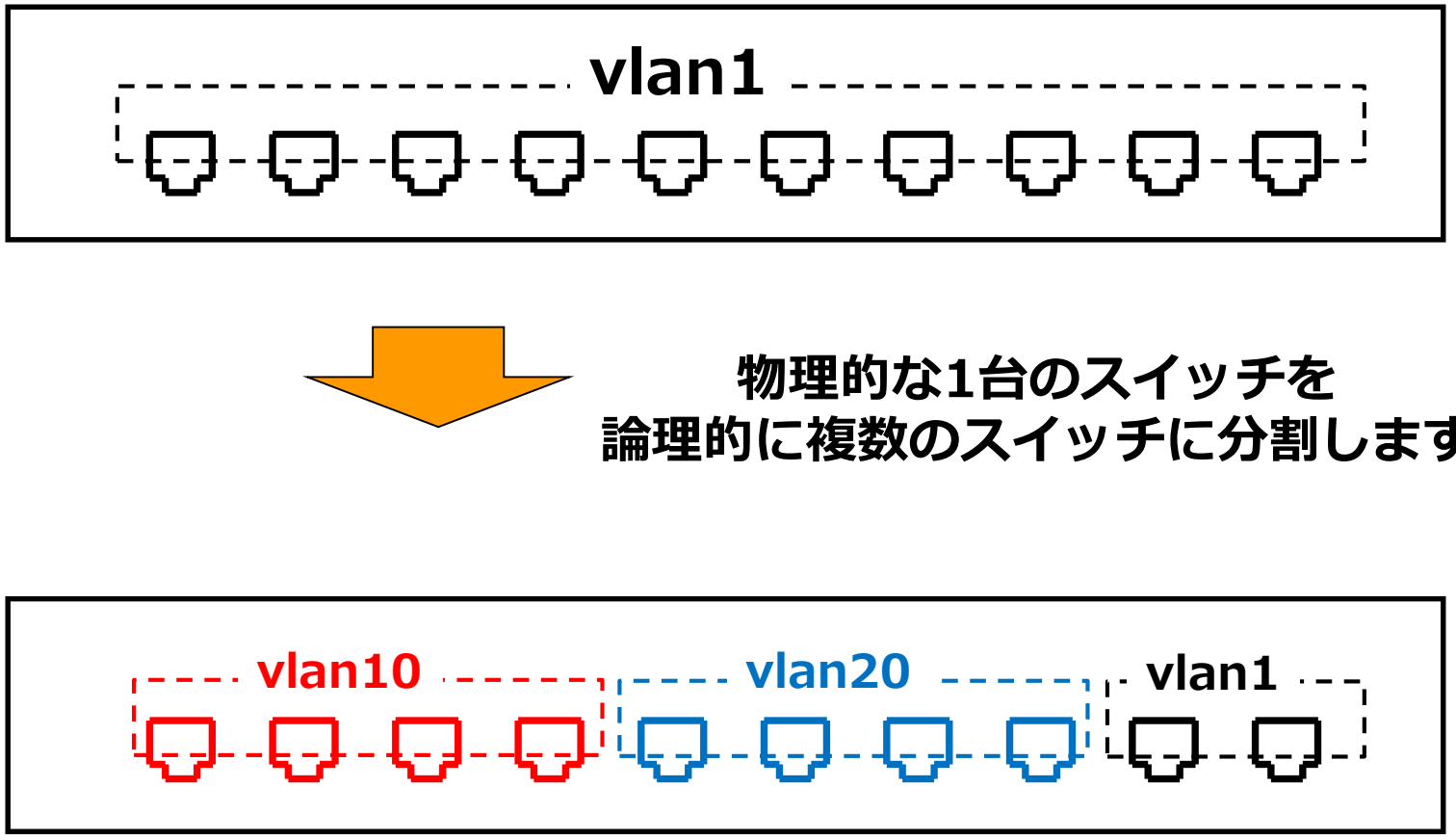
①インターフェース
GigabitEthernet　1/0/1

ポート番号

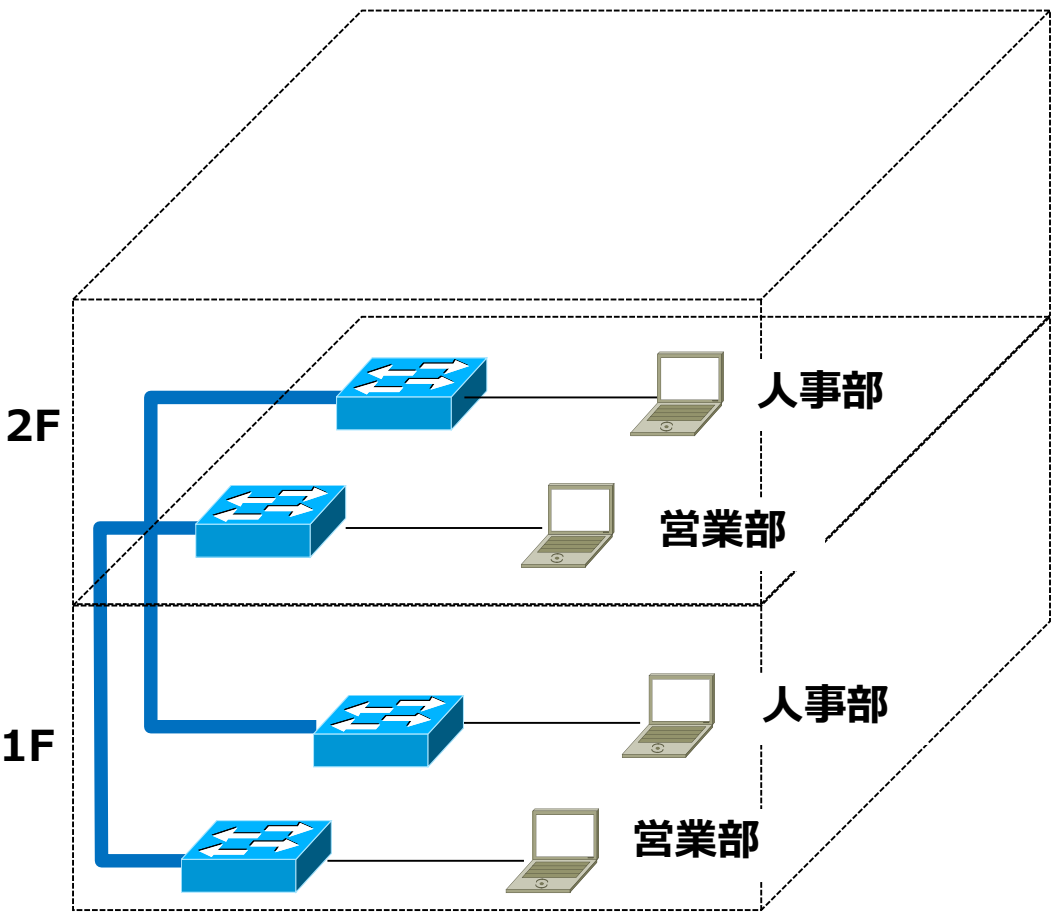
インターフェイスタイプ　スタック番号　スロット番号

②Consoleポート
Config設定のためにConsoleケーブルでPCと接続するポート

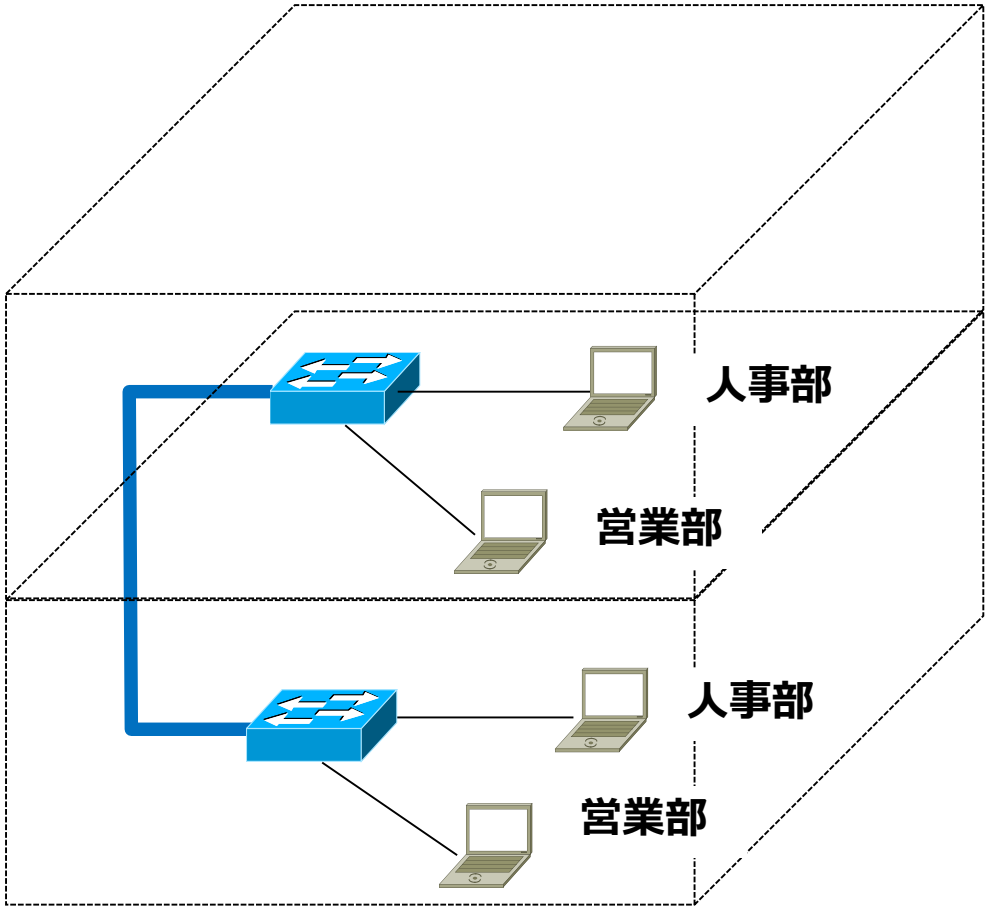
●vlan（Virtual Local Area Network）



●vlanの用途



部署ごとにスイッチを配置



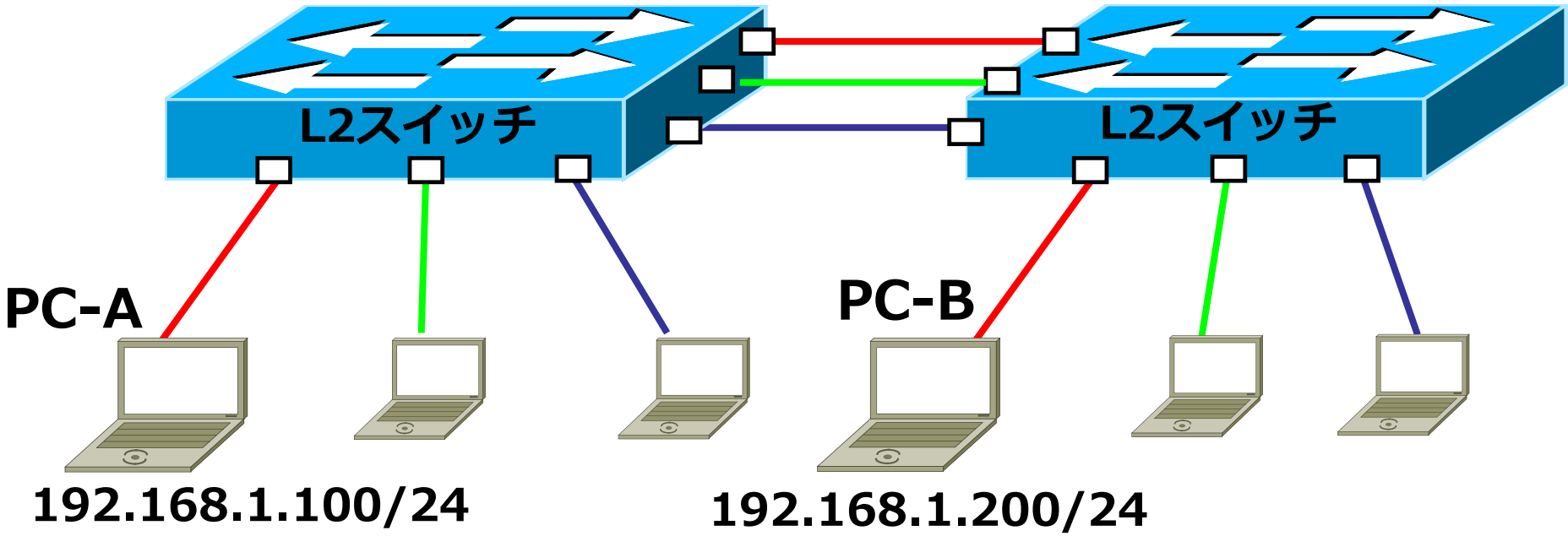
vlanを使用して柔軟な配置

●L2スイッチの基本設定（演習）

PC：192.168.1.100/24

設定項目	設定値
ホスト名	SW
特権パスワード	ntt
VTYパスワード（Telnet）	nttntt
vlan1	
IPアドレス サブネットマスク	192.168.1.1 255.255.255.0

●vlan作成と適用（演習）



vlan10
vlan20
vlan30

vlan－ID	Port－No
10	1～5
20	6～10
30	11～15

●複数のインターフェースを設定

(config)#interface **range** gigabitEthernet ***portnumber - portnumber***
(config-if-range)#

例：Gi 1/0/1～1/0/12を一括設定

(config)#interface **range** gigabitEthernet 1/0/1 – 12

(config-if-range)#

●確認コマンド(show vlan)

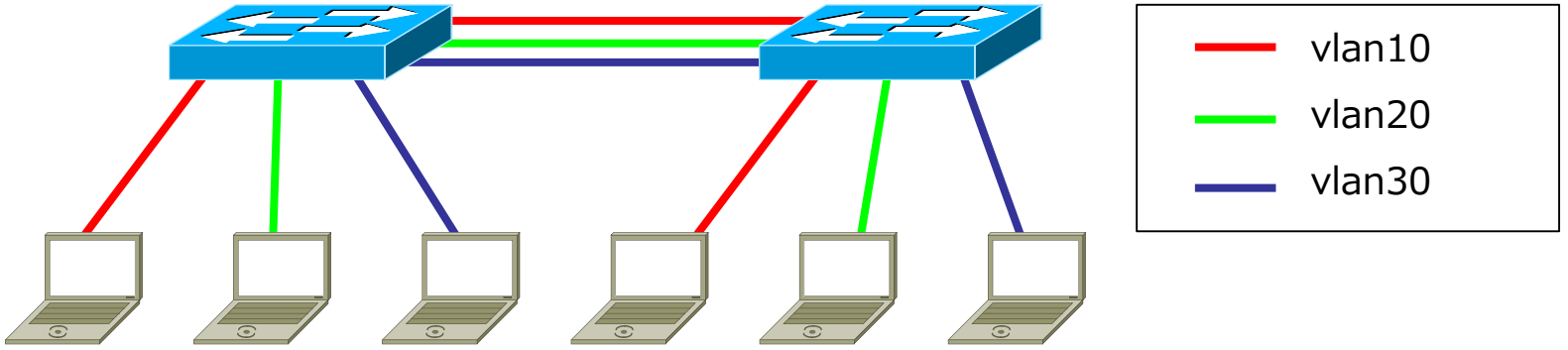
```
Switch#sh vl

vlan Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gi1/0/23, Gi1/0/24,  Gi1/0/25
                                                 Gi1/0/26, Gi1/0/27,   Gi1/0/28

10   vlan10                            active    Gi1/0/1, Gi1/0/2, Gi1/0/3
       ❶                                        Gi1/0/4, Gi1/0/5, Gi1/0/6
                                                Gi1/0/7, Gi1/0/8, Gi1/0/9
                                                Gi1/0/10, Gi1/0/11

20   vlan20                            active    Gi1/0/12, Gi1/0/13, Gi1/0/14
                                                Gi1/0/15, Gi1/0/16, Gi1/0/17
                                                Gi1/0/18, Gi1/0/19, Gi1/0/20
                                                Gi1/0/21, Gi1/0/22
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

❷

●タグvlan （トランク）

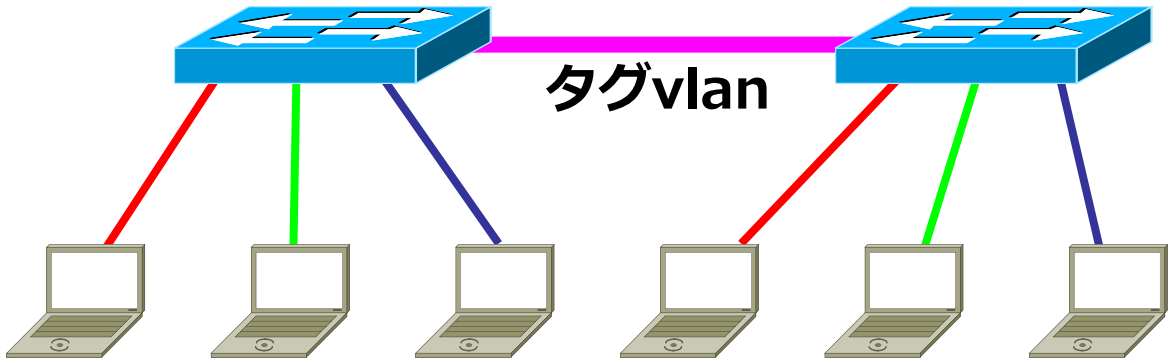
■タグvlan未使用（アクセスポート）

「1つのvlanに所属し、そのvlanのフレームを送受信することができるポート」



■タグvlan使用（トランクポート）

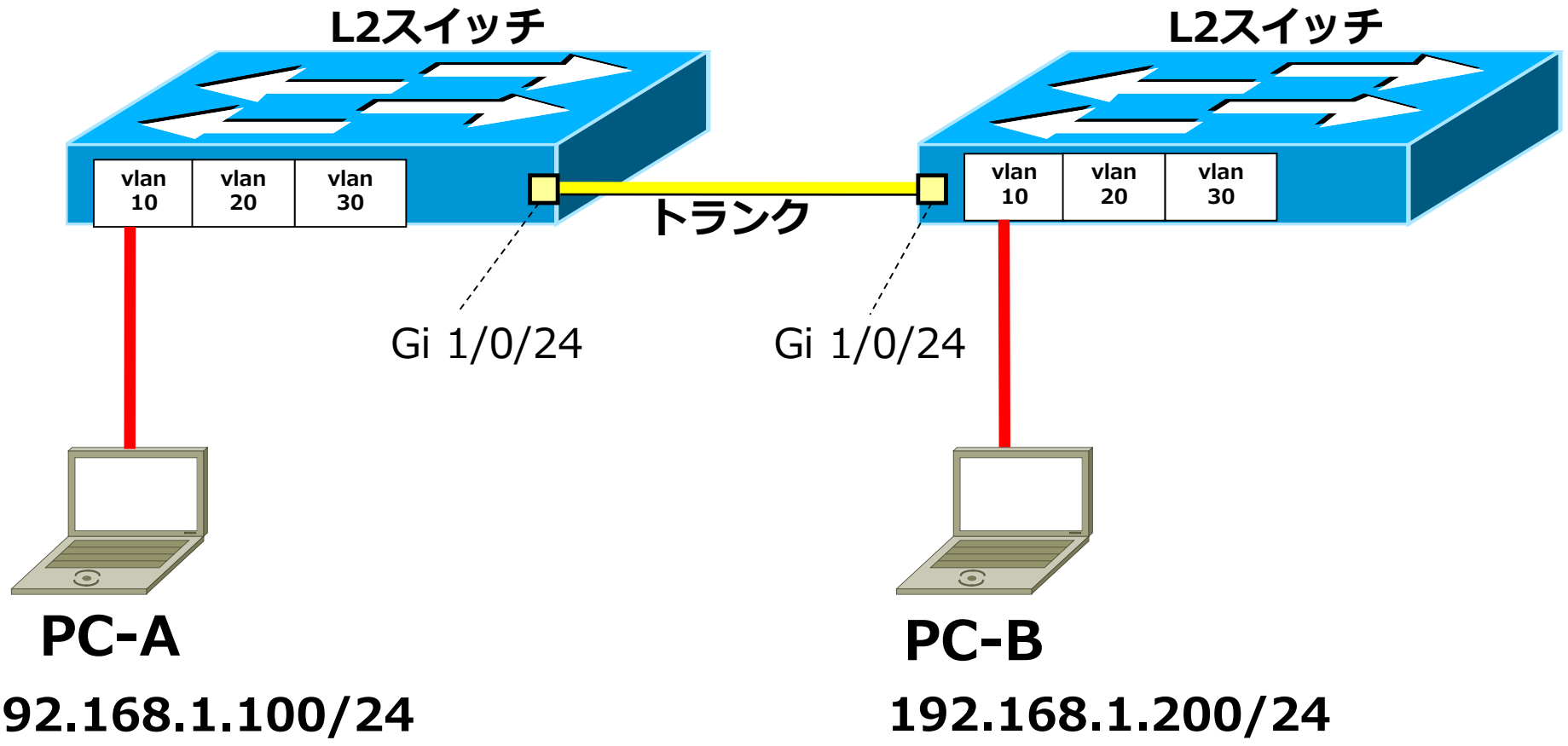
「複数のvlanに所属し、複数のvlanのフレームを送受信することができるポート」



●確認コマンド(show interfaces trunk)

```
SW#sh int tru

Port          Mode         Encapsulation  Status        Native vlan
Gi 1/0/24     on           802.1q         trunking      1

 ❶                          ❷                           ❸
Port          Vlans allowed on trunk
Gi 1/0/24     1-4094

              ❹
Port          Vlans allowed and active in management domain
Gi 1/0/24     1,10,20,30

Port          Vlans in spanning tree forwarding state and not pruned
Gi 1/0/24     1,10,20,30
```

●トランク接続（演習）


L2スイッチ
L2スイッチ
vlan 10
vlan 20
vlan 30
vlan 10
vlan 20
vlan 30
トランク
Gi 1/0/24
Gi 1/0/24
PC-A
192.168.1.100/24
PC-B
192.168.1.200/24

●Catalystスイッチの初期化

1. vlanデータベース削除

作成したvlan情報はデータベースとして別ファイル(vlan.dat)に保存されるため、別途削除が必要です。

2. NVRAMの設定削除

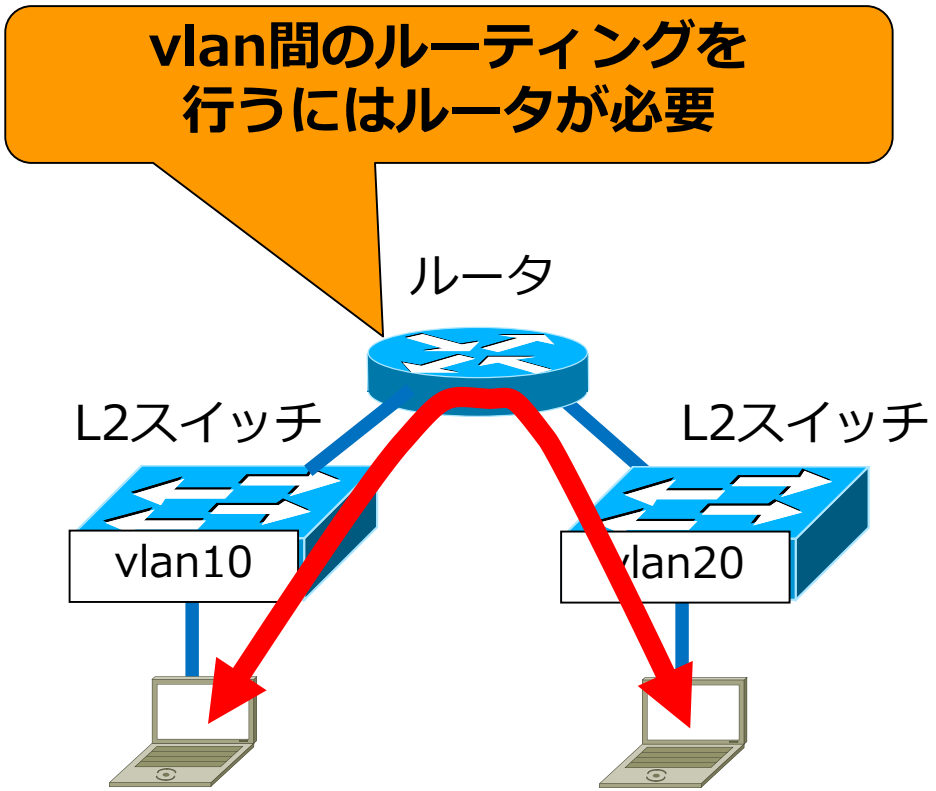
startup-configを削除します。

3. 再起動

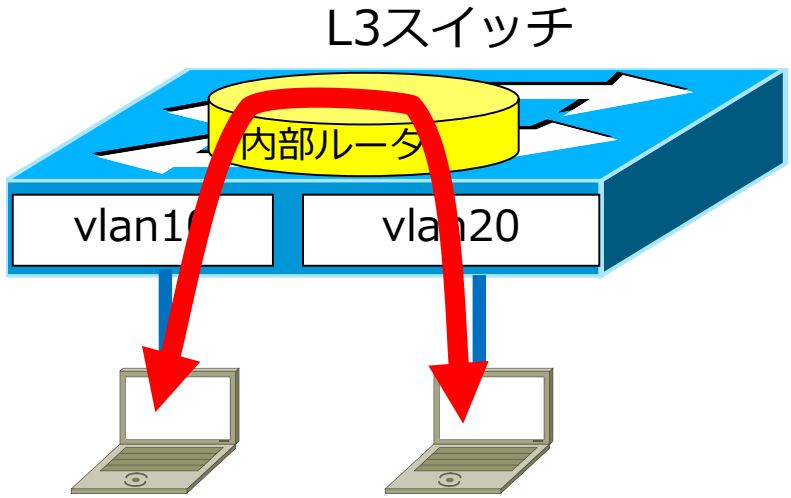
startup-configが削除された状態で起動することで初期化が完了します。

●vlan間ルーティングの構成例

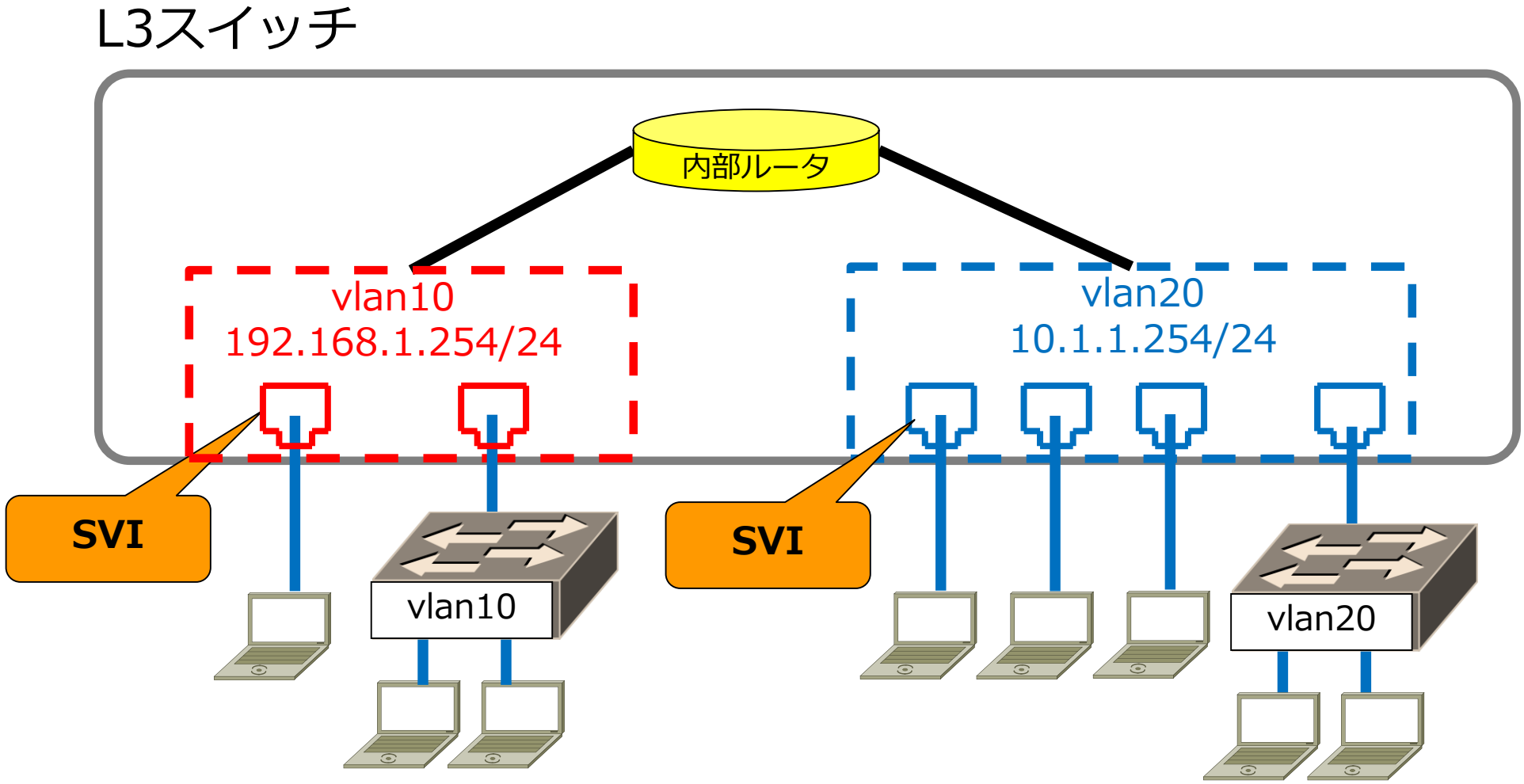
L2スイッチの場合



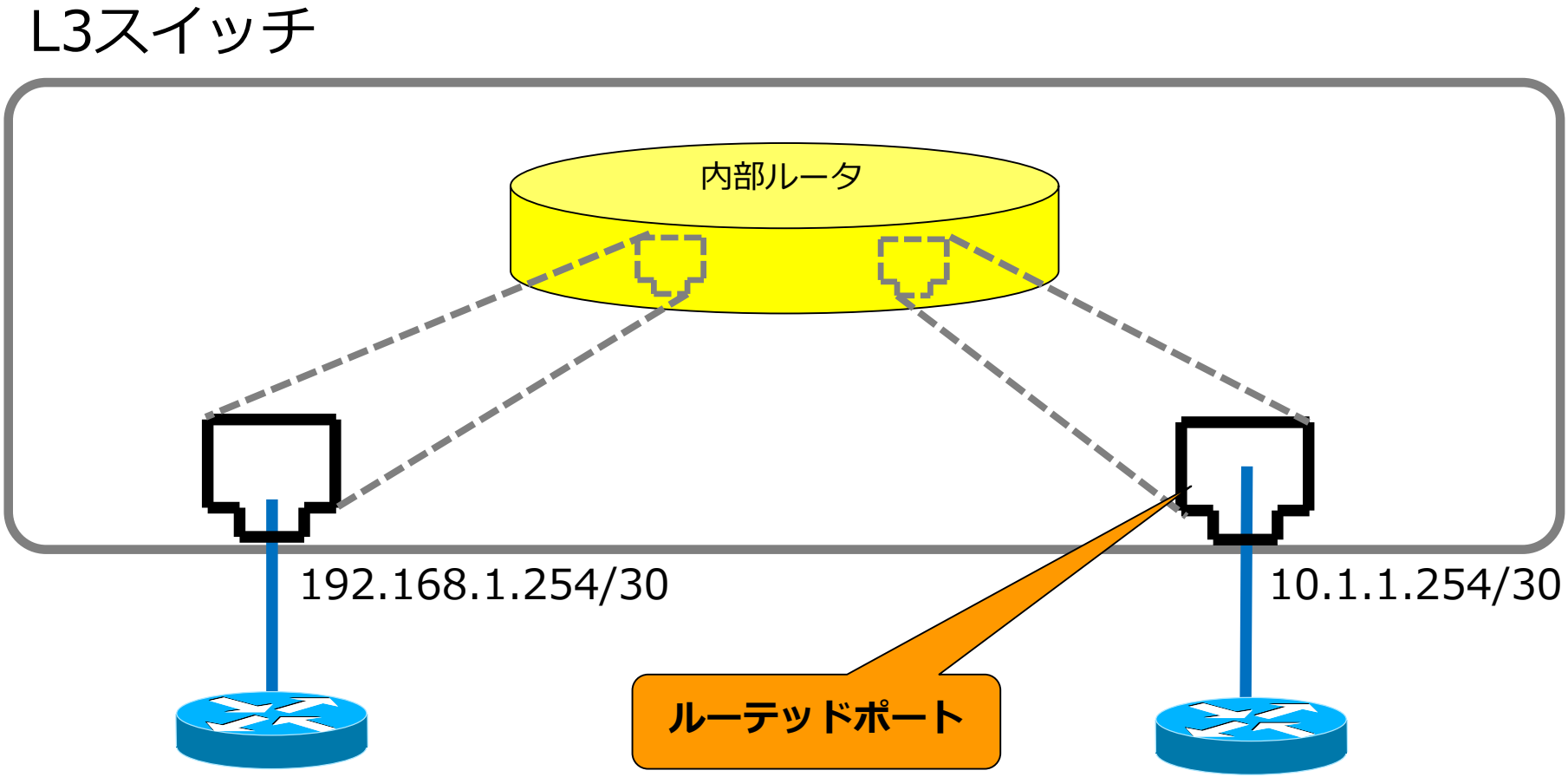
L３スイッチの場合



●SVI（Switched Virtual Interface）



●ルーテッドポート



●L3スイッチの基本設定

- **内部ルータ機能の有効化（デフォルトは無効）**

  Switch(config)# **ip routing**

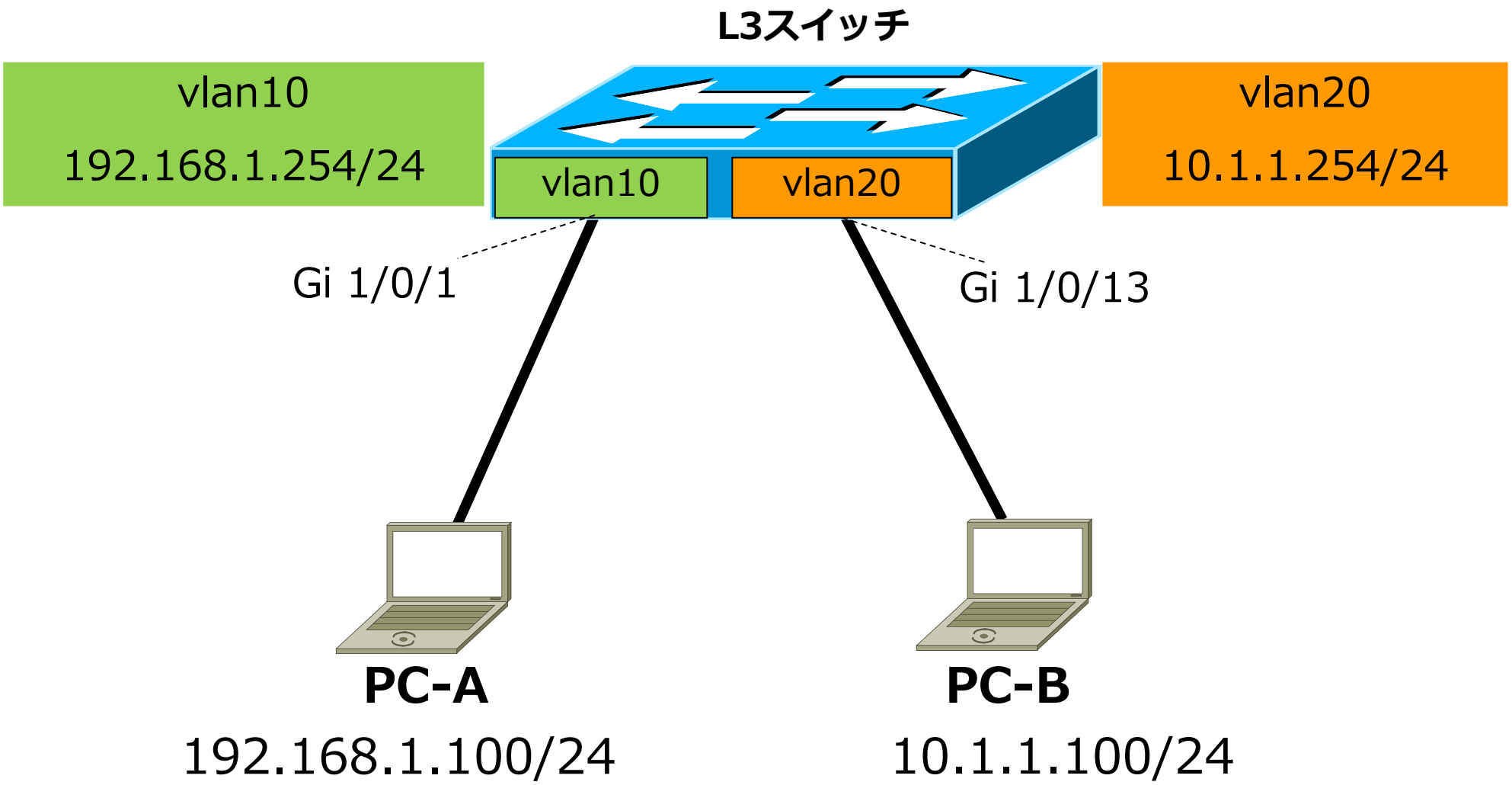
- **SVI　(Switch Virtual Interface)**

  Switch(config)# **vlan xx**
  Switch(config-vlan)# **exit**
  Switch(config)# **int gi 1/0/xx**
  Switch(config-if)# **switchport access vlan xx**
  Switch(config-if)# **switchport mode access**
  Switch(config)# **int vlan xx**
  Switch(config-if)# **ip address [address] [subnetmask]**

- **ルーテッドポート**

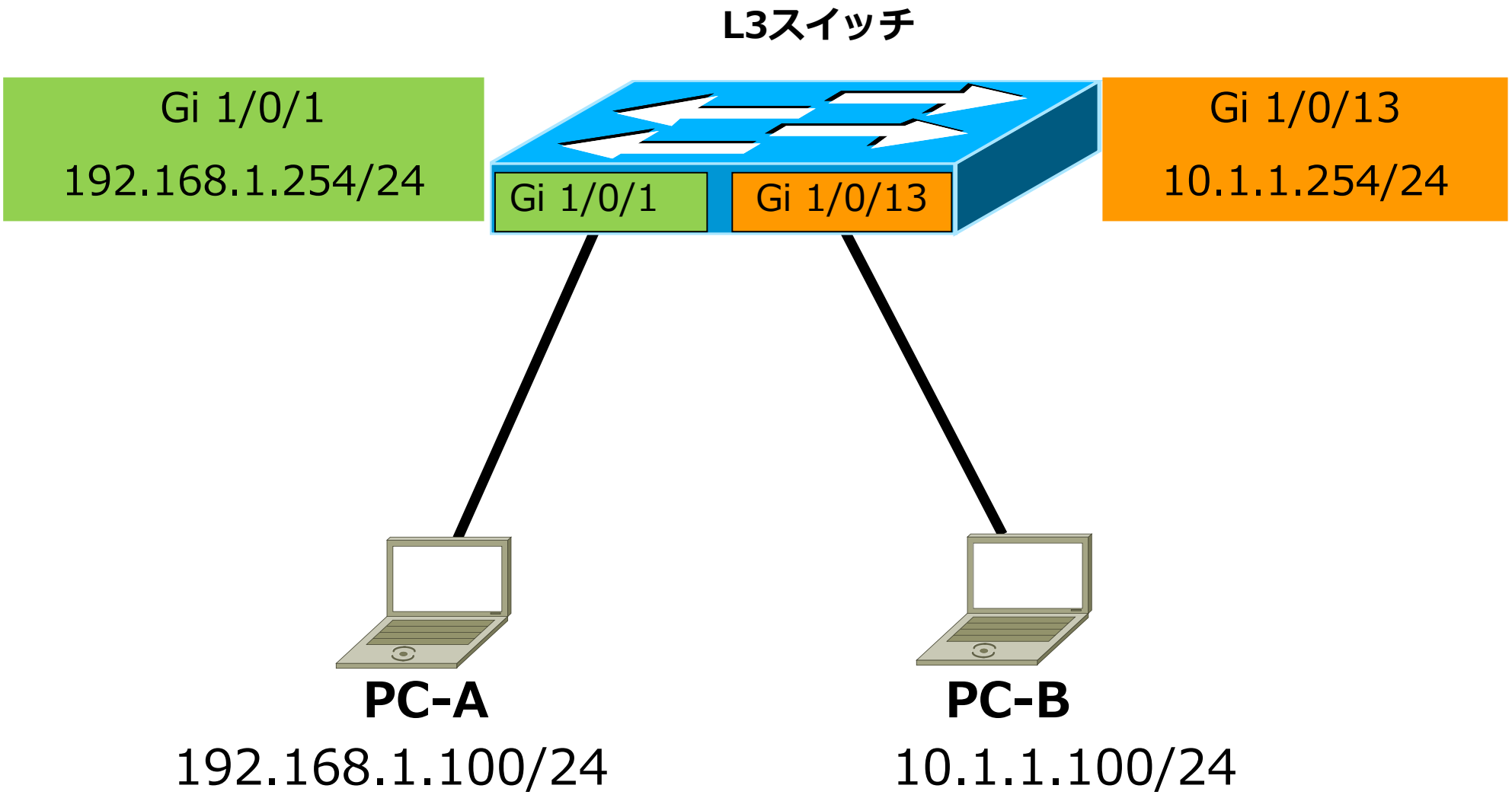
  Switch(config)# **int gi 1/0/xx**
  Switch(config-if)# **no switchport**
  Switch(config-if)# **ip address [address] [subnetmask]**

●SVI（演習）


L3スイッチ
vlan10
192.168.1.254/24
vlan20
10.1.1.254/24
vlan10
vlan20
Gi 1/0/1
Gi 1/0/13
PC-A
192.168.1.100/24
PC-B
10.1.1.100/24

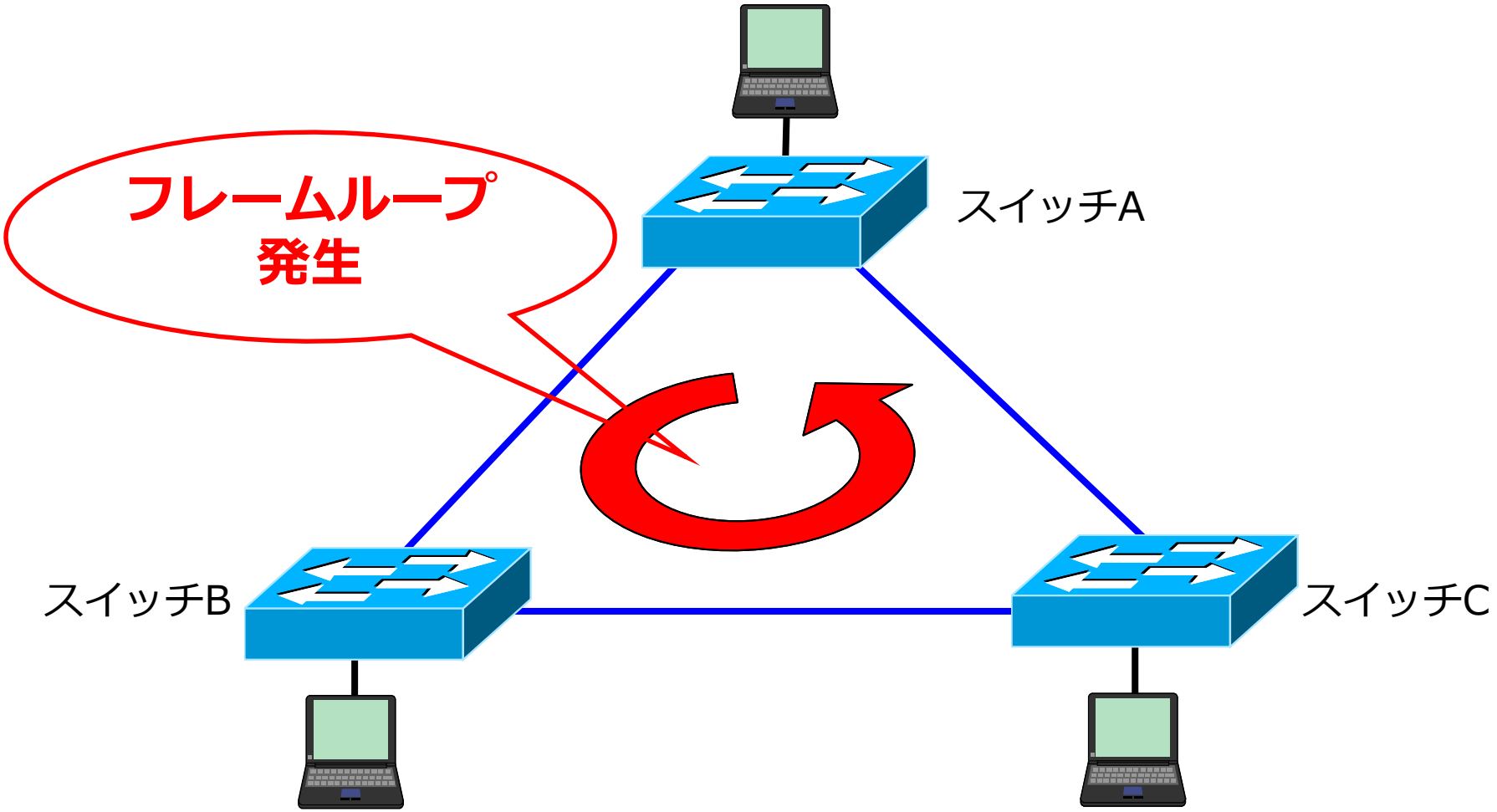
●ルーテッドポート（参考演習）

演習前に必ずL3スイッチを初期化してから実施して下さい



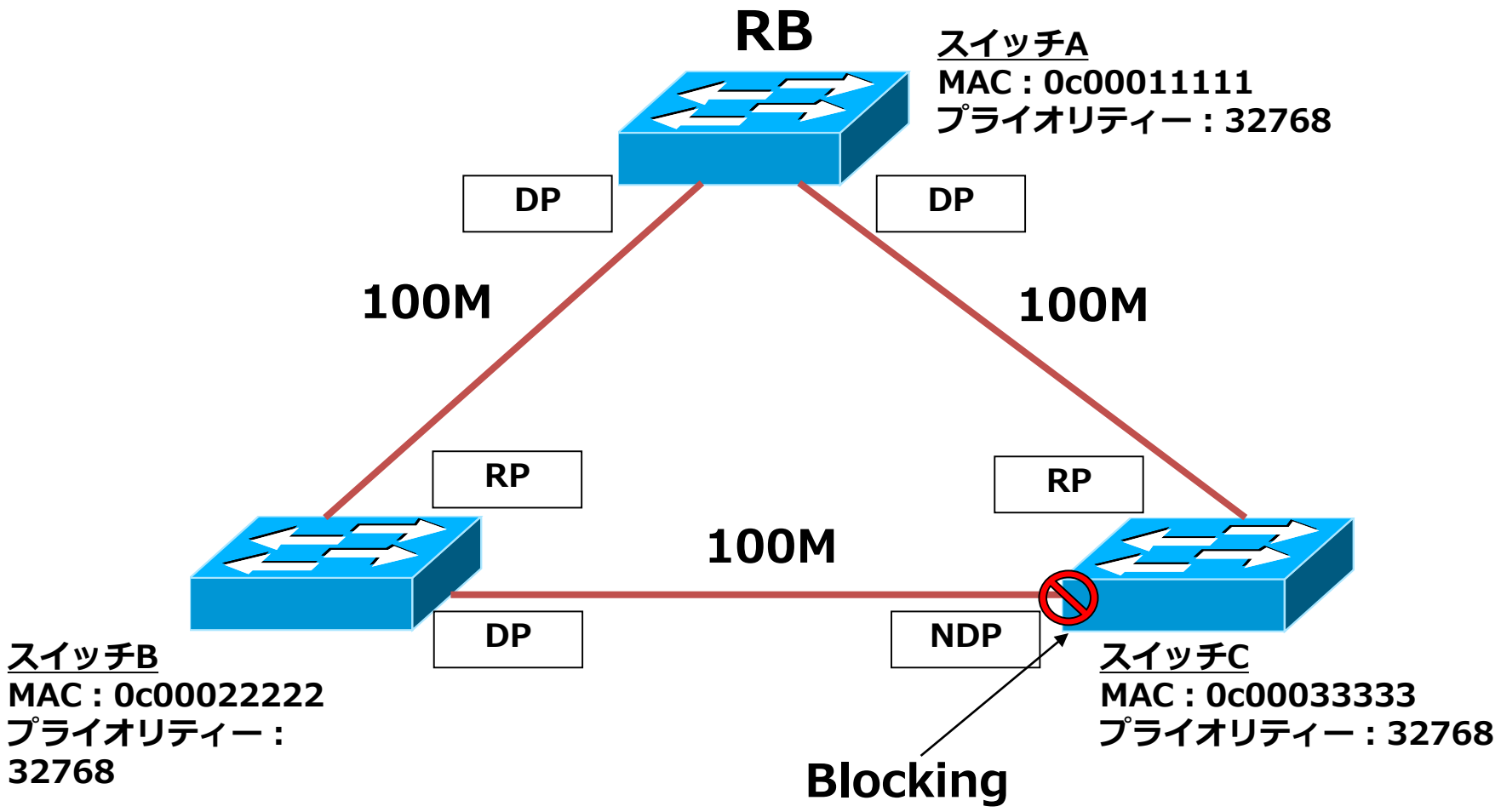
第2章
STP
(スパニングツリープロトコル)

●ループ回避



ネットワークに冗長構性を持たせる為に複数経路を用意したところループが発生

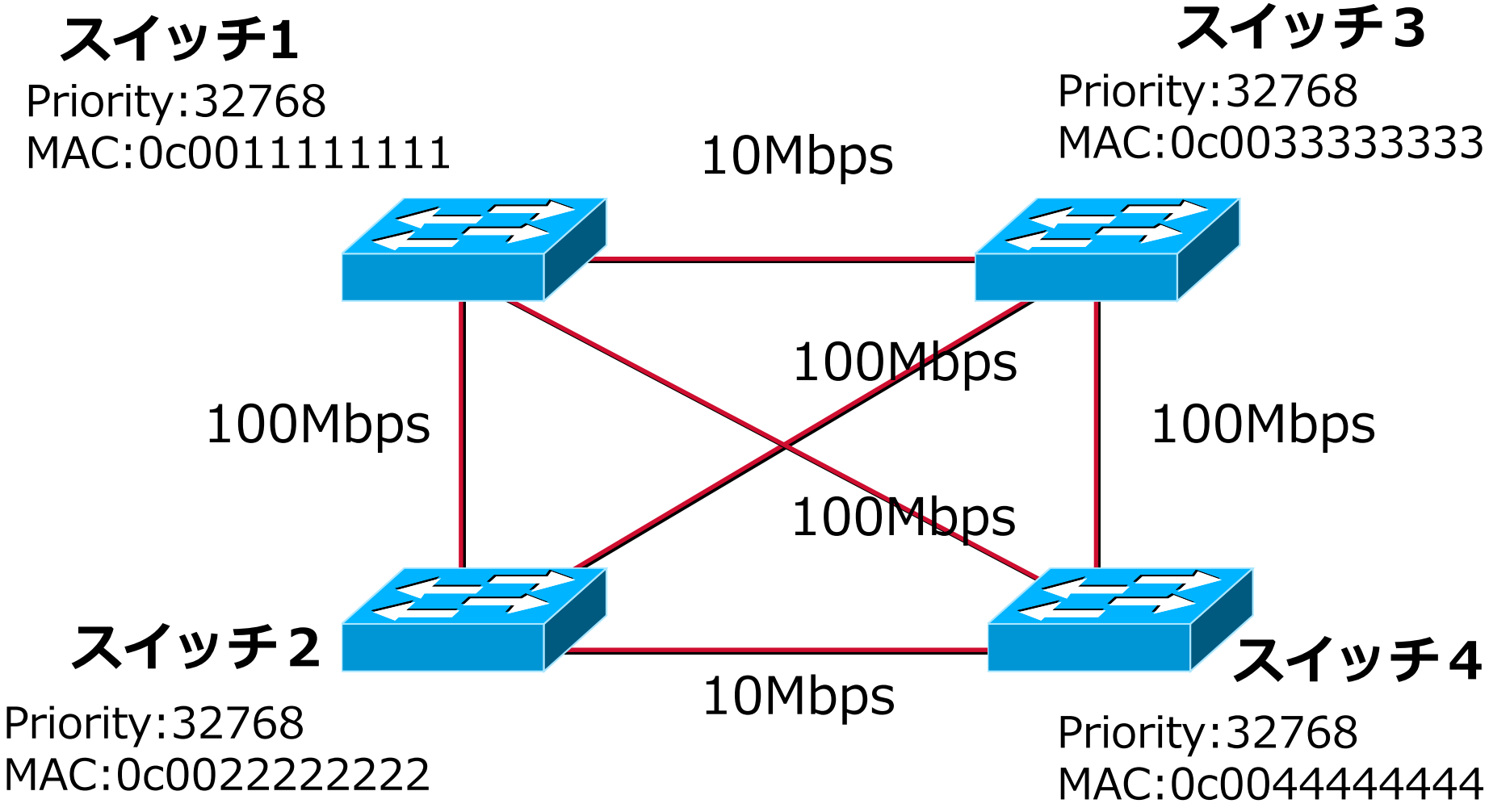
●STPの動作



※BPDUとは…

スイッチのループ構成を検出して、冗長リンクをブロックするためのスパニングツリープロトコル(IEEE802.1d)で利用される制御フレーム。ブリッジID、ルートブリッジのIDおよびルートブリッジへのパスコスト等を含み、データリンクの選択が可能である。デフォルトでは2秒に1度送信される。

●演習問題


スイッチ1
Priority:32768
MAC:0c0011111111
スイッチ３
Priority:32768
MAC:0c0033333333
10Mbps
100Mbps
100Mbps
100Mbps
100Mbps
スイッチ２
Priority:32768
MAC:0c0022222222
10Mbps
スイッチ４
Priority:32768
MAC:0c0044444444

●ポート状態

ポートの状態	ﾌﾚｰﾑ転送	MAC学習	BPDU送受信	備考
ブロッキング	×	×	△	NDP, ※△:受信のみ
リスニング	×	×	○	
ラーニング	×	○	○	
フォワーディング	○	○	○	RP, DP

20秒

15秒

15秒

●STPの設定コマンド

①スパニングツリーの有効化　※cisco社はデフォルトで有効（ベンダによって異なります）

Switch(config)# spanning-tree mode pvst　　※Per-VLAN Spanning Tree

②スパニングツリーをVlanごとに設定（PVST）

Switch(config)#spanning-tree vlan *vlan-id*
※デフォルトは、vlan1

③上記スパニングツリーの無効化

Switch(config)# no spanning-tree mode pvst
Switch(config)#no spanning-tree vlan *vlan-id*

④スパニングツリーのルートブリッジの設定（プライオリティを静的に設定）

Switch(config)#spanning-tree vlan *vlan-id* priority *priority*

※priority値は、4096単位ですが、IOSにより任意の値が設定可能

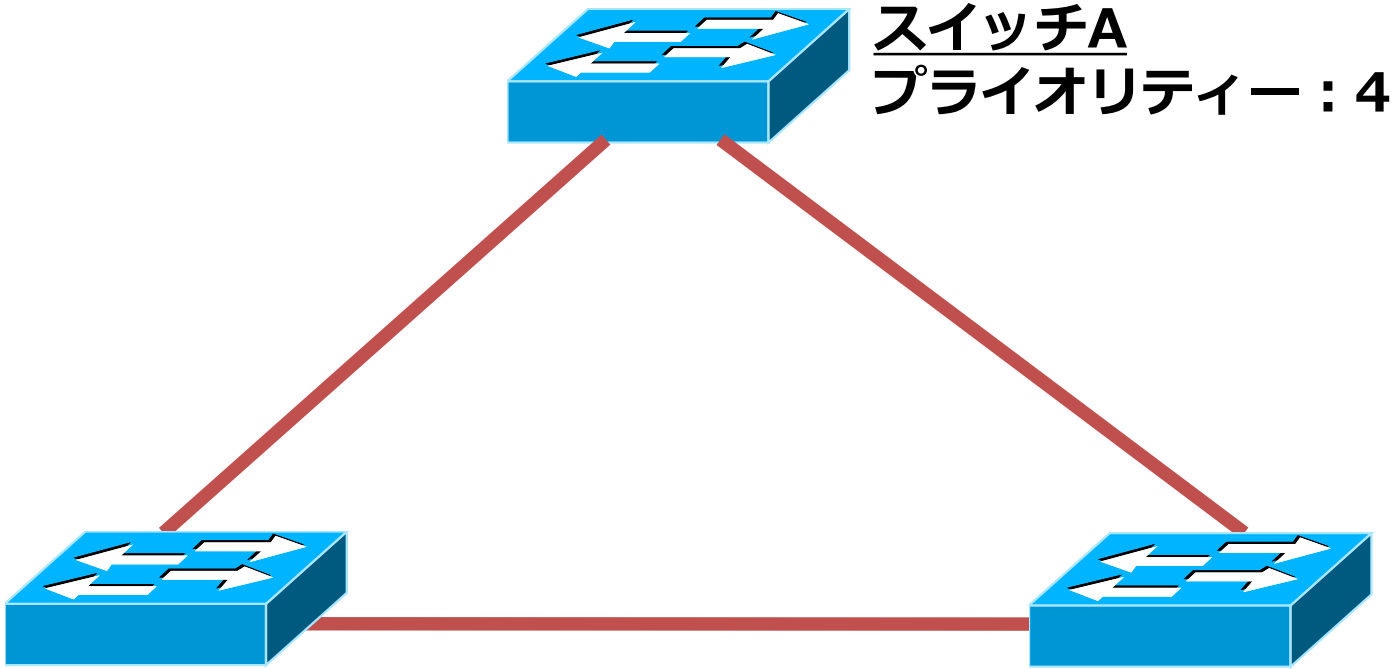
●確認コマンド(show spanning-tree)

<確認コマンド>

Switch#sh span

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0015.63d8.8c80
              Cost        19
              Port        23 (FastEthernet1/0/23)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0015.63d8.9200
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface          Role      Sts    Cost       Prio.Nbr     Type
------------------ ---- --- -------- -------- ------------------------------------
Fa1/0/1          Desg    FWD    19         128.3        P2p Edge
Fa1/0/23         Root    FWD    19         128.25       P2p
Fa1/0/24         Altn    BLK    19         128.26       P2p
```

●STPによるループ回避（演習）

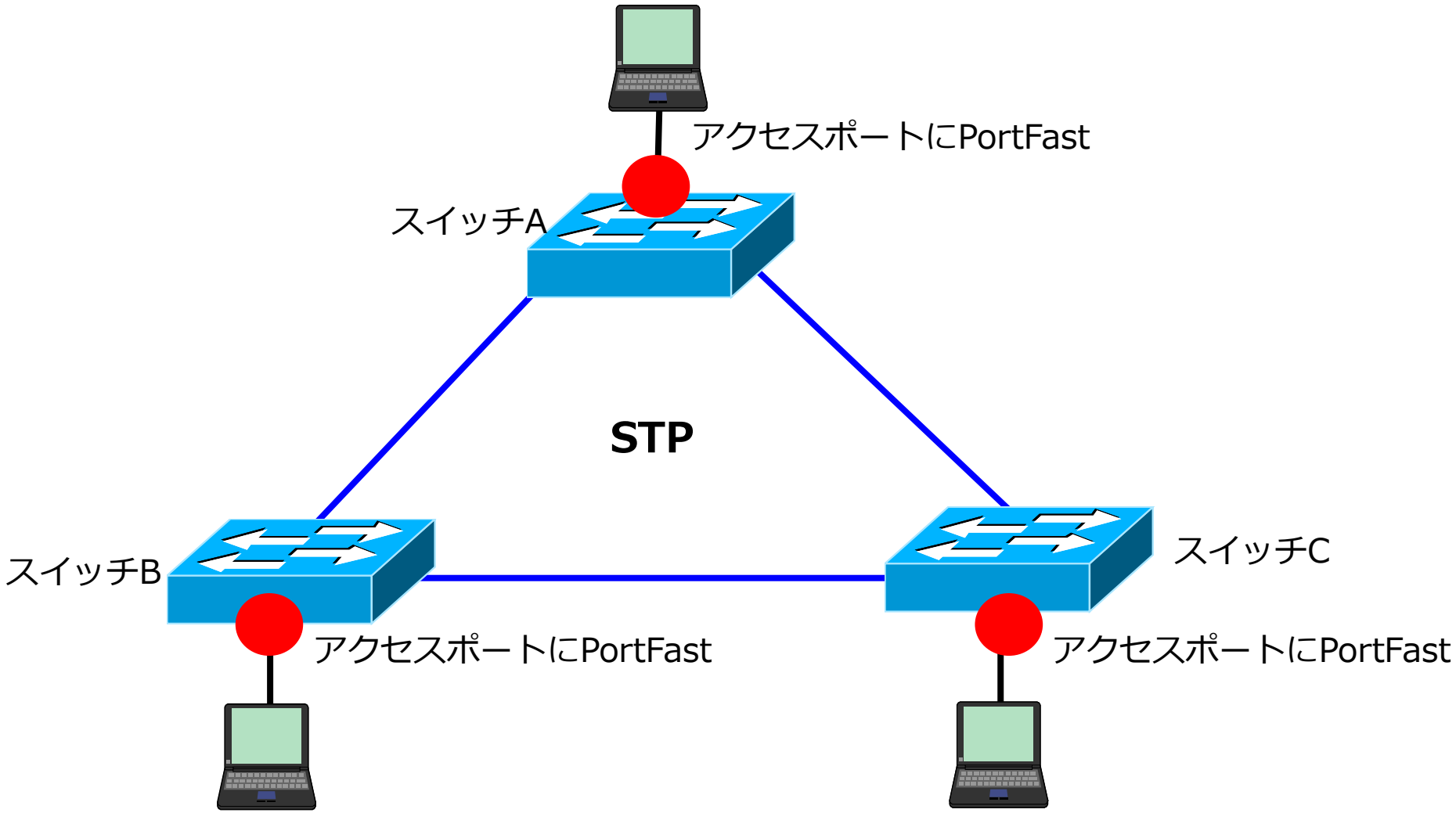


スイッチA
プライオリティー：4096

スイッチB
プライオリティー：8192

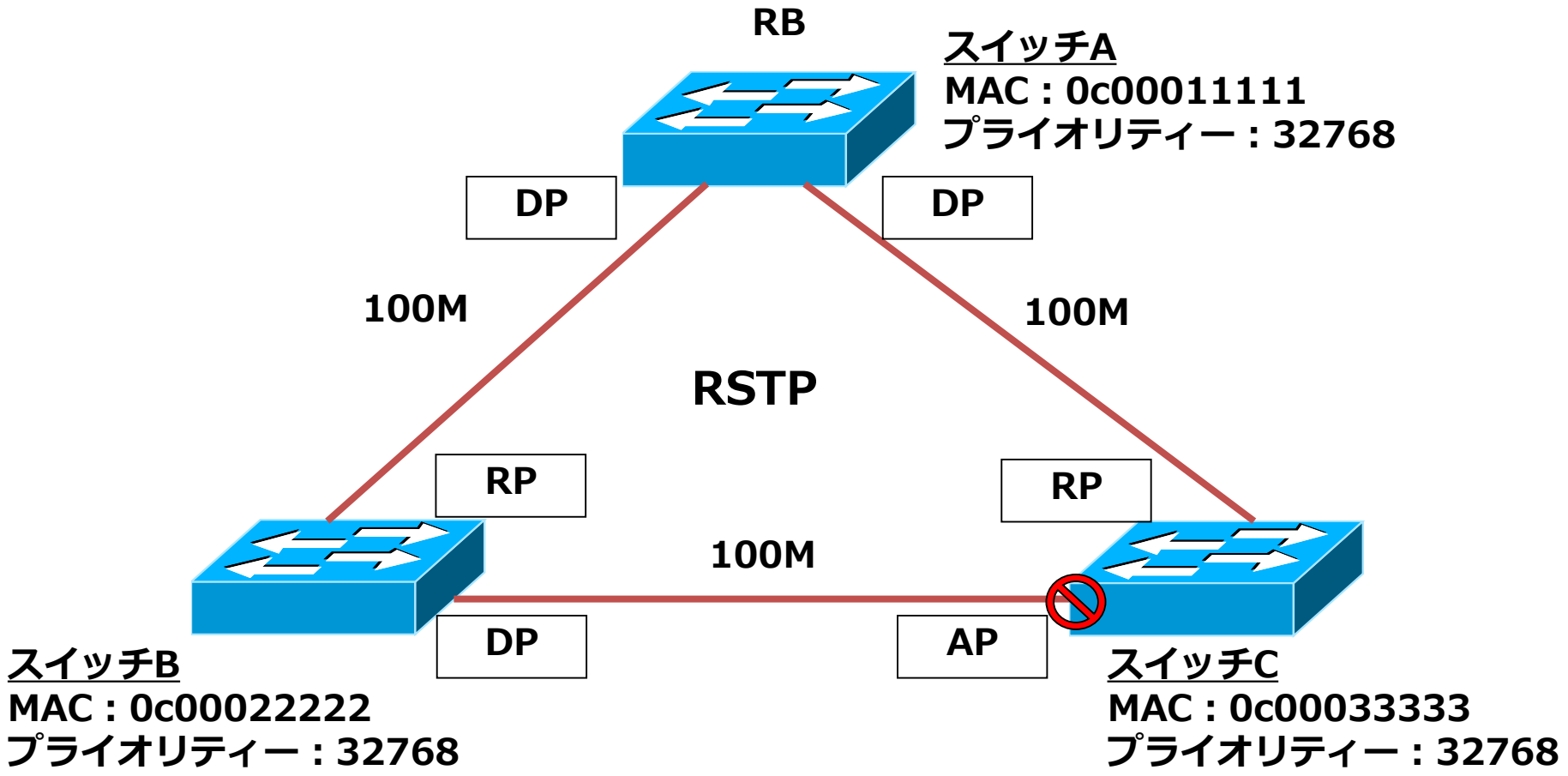
スイッチC
プライオリティー：デフォルト

●PortFast



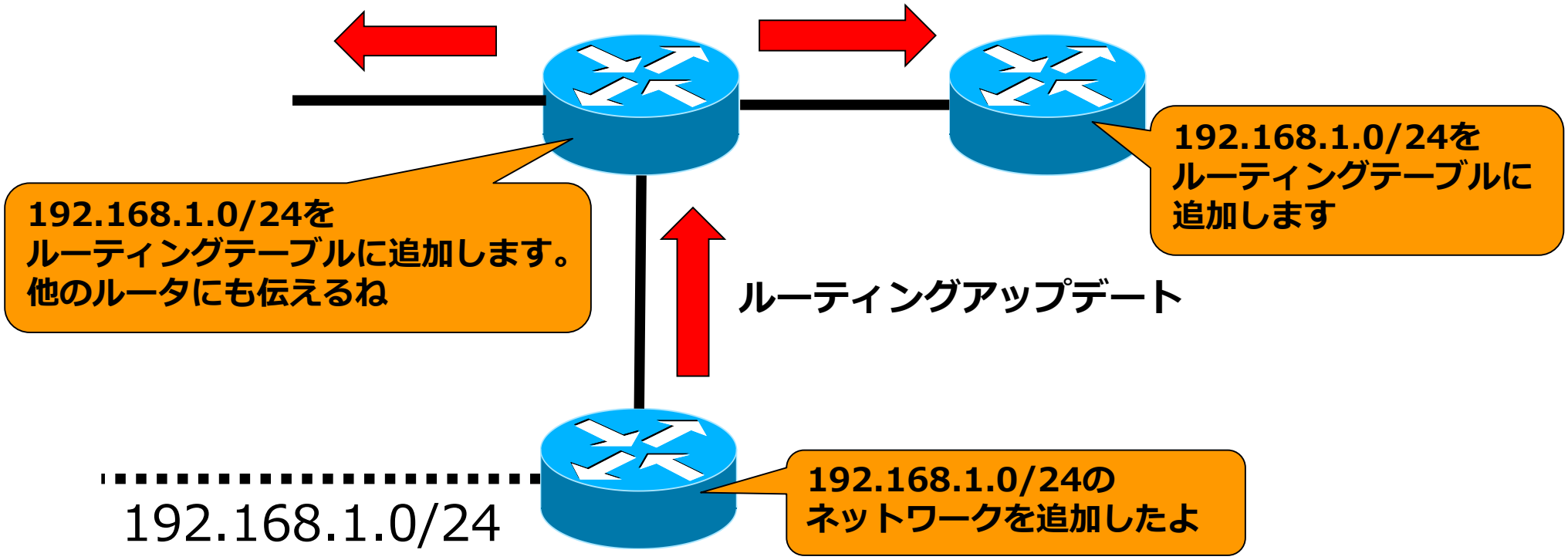
※PortFastが設定できるのは、アクセスポートだけです。
トランクポートでは、設定できません。

●RSTPによるループ回避



第3章
OSPF
(ダイナミックルーティングプロトコル)

●ダイナミックルーティング

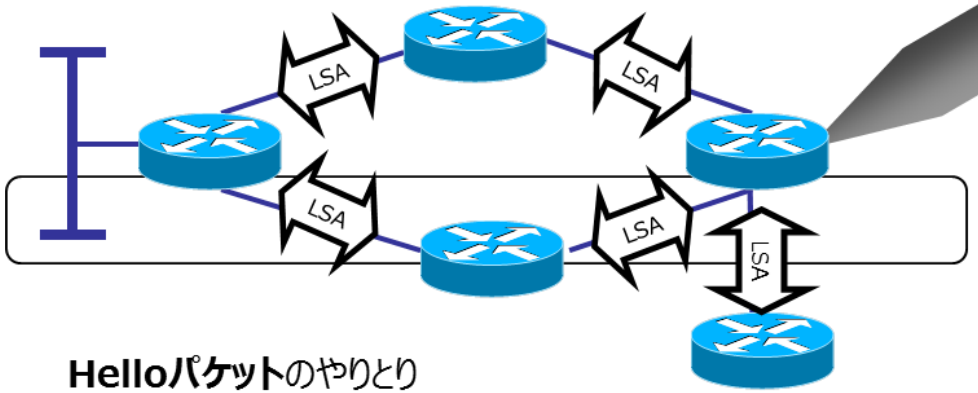


●OSPF概要

- SPFアルゴリズムを採用し、高速な収束を実現
- メトリックとしてパスコストを採用
- イコールコストマルチパスのサポート
- ルーティング情報の交換にマルチキャスト、ユニキャストを使用
- VLSM(可変長サブネットマスク)をサポート

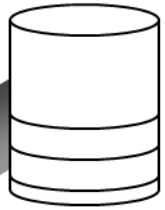
●ルーティングテーブルの作成方法

①LSA



Helloパケットのやりとり
→隣接関係を作る
→LSA交換

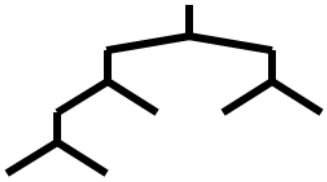
②



LSDB
→受信したLSAをLSDBに保存し、
LSDBにあるLSAを基にネットワーク
構成図を作成（トポロジマップ）

③ SPFアルゴリズム
→ LSDBを基に自分を基点とした最適経路を判断

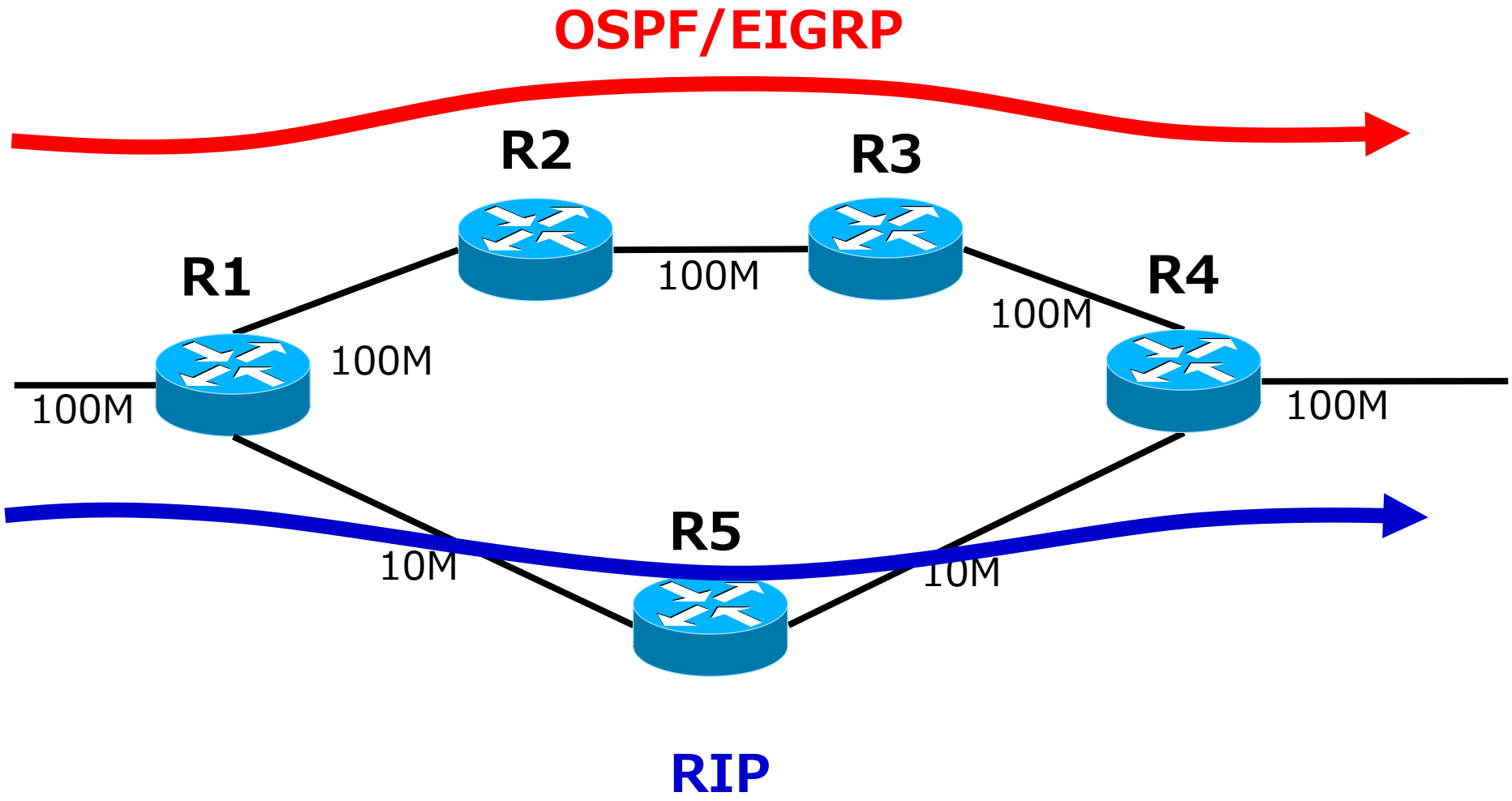
④ SPFツリー



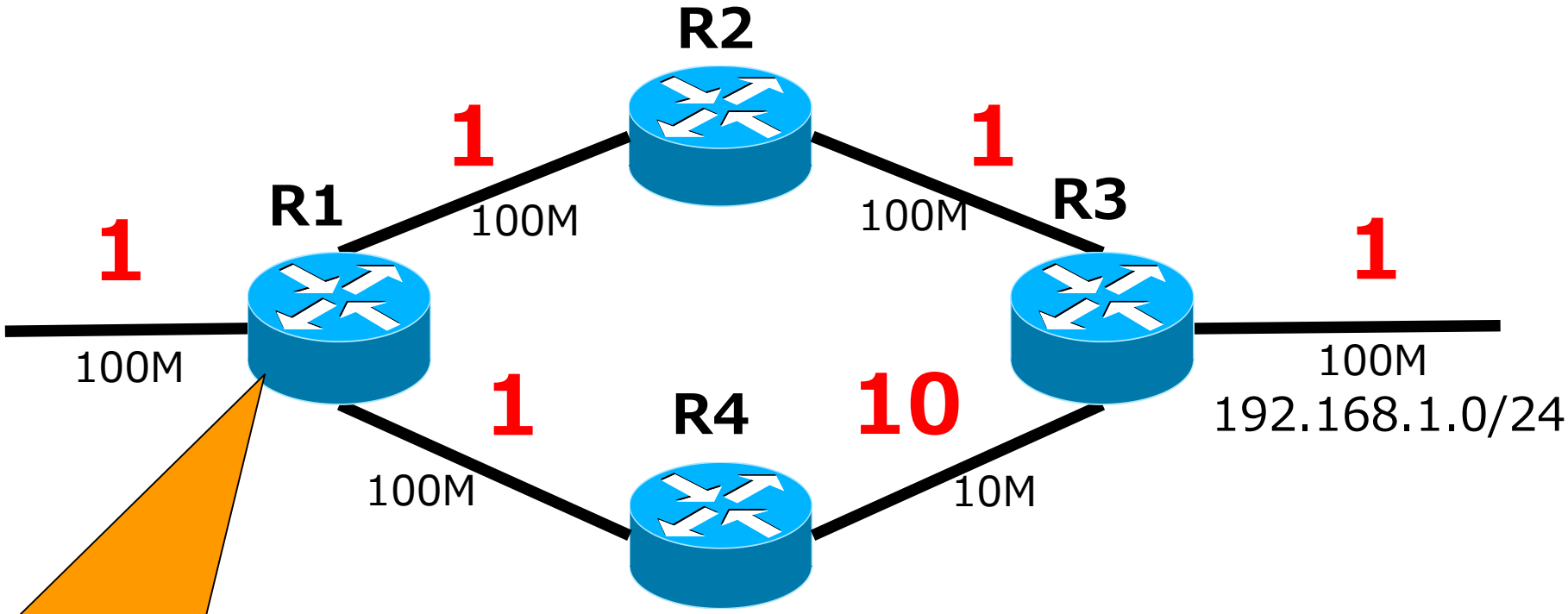
⑤ OSPFルート

⑥ルーティングテーブル		
宛先ネットワーク	ネクストホップ	メトリック

●ルーティングメトリック



●パスコスト



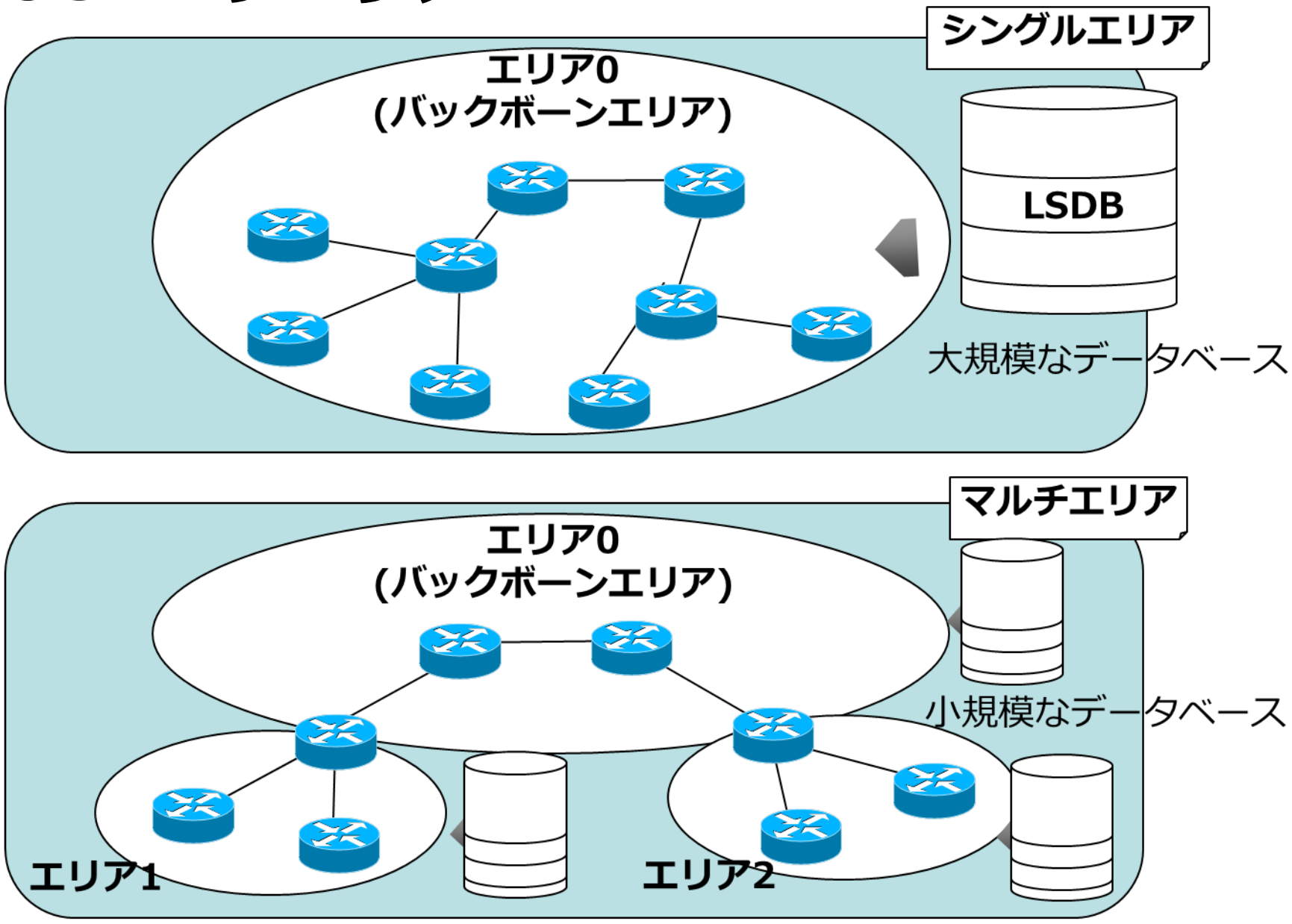
インターフェースのパスコストを算出

コスト＝100÷帯域幅

R1から192.168.1.0 /24 への
パスコストを累計

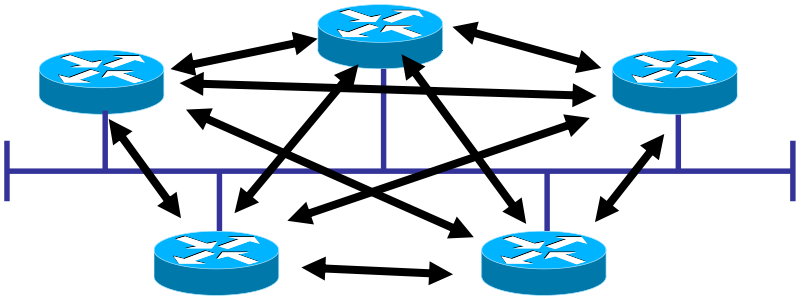
	パスコスト累計
R2経由	**3**
R4経由	**12**

●OSPFのエリア


シングルエリア
エリア0
(バックボーンエリア)
LSDB
大規模なデータベース
マルチエリア
エリア0
(バックボーンエリア)
小規模なデータベース
エリア1
エリア2

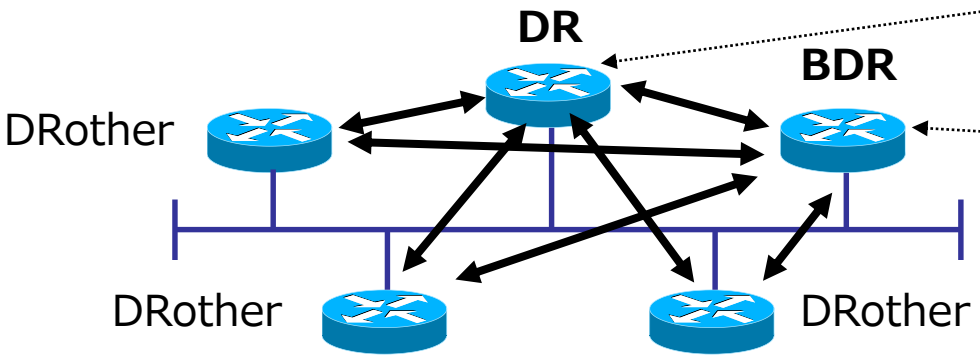
●マルチアクセスネットワークにおける代表ルータの概念

DR選定がない場合



ルータの数が増えるほど、やりとりするリンクステート情報の数が膨大になる。

DR選定がある場合



マルチアクセスネットワーク上で代表して他のルータとの隣接関係を確立。

DRをバックアップ。

●OSPFの基本設定

Router(config)# router ospf [プロセスID]　※OSPF設定モードに入るコマンド

・[プロセスID]・・・OSPFプロセスの識別番号。1～65,535の任意の値

(config-router)# network [ネットワークアドレス] [ワイルドカードマスク] area [エリアID]

・[ネットワークアドレス]・・・有効にするネットワークのネットワークアドレス
・[ワイルドカードマスク] ・・・アドレスのワイルドカードマスク
・[エリアID] ・・・そのネットワークが所属するエリアのID。基本値は0である

【設定例】

```
router ospf 1
network 192.168.1.0 0.0.0.255 area 0
network 192.168.2.252 0.0.0.3 area 0
network 172.16.0.0 0.0.255.255 area 0
```

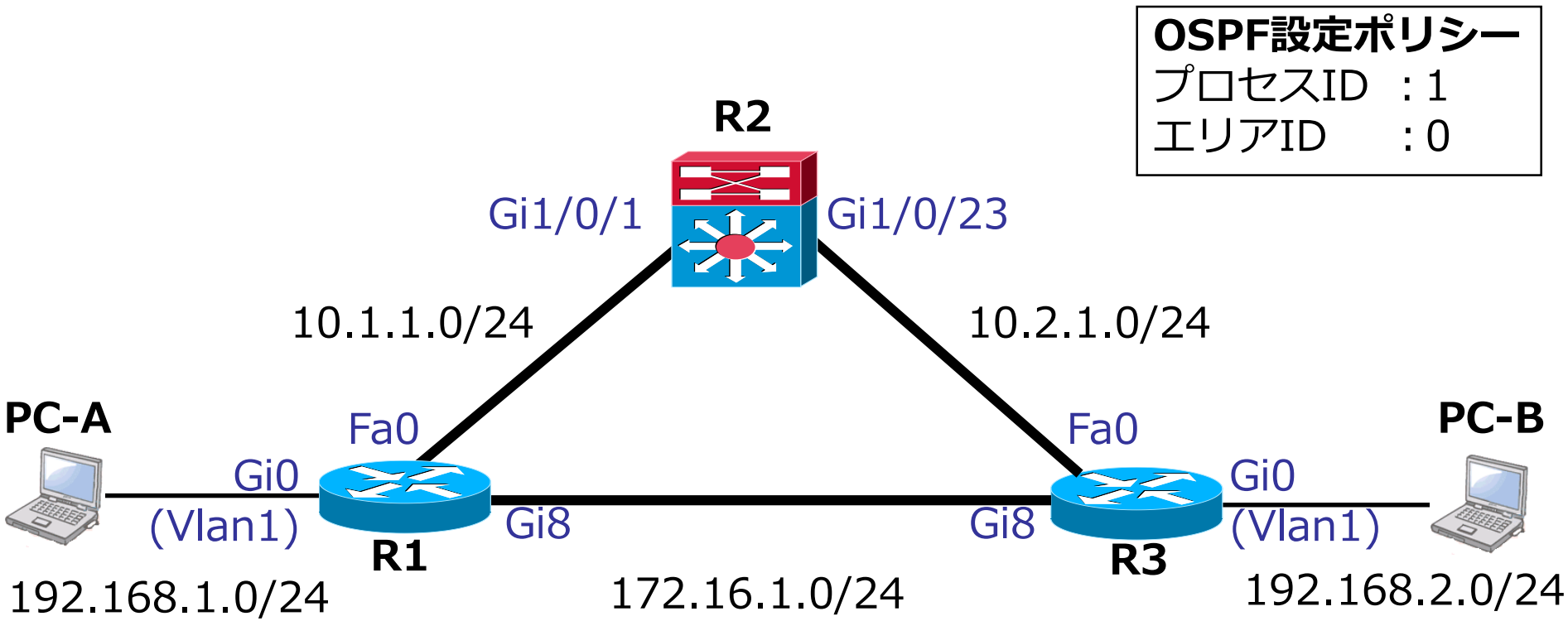
●確認コマンド(show ip route)

```
Router#sh ip ro

     172.16.0.0/24 is subnetted, 3 subnets
O       172.16.1.0 [110/65] via 172.16.101.1, 00:10:18, FastEthernet0
     10.0.0.0/24 is subnetted, 2 subnets
O       10.0.10.0  [110/11] via 172.16.11.1, 00:10:18, GigabitEthernet0
O       10.0.1.0   [110/2] via 172.16.101.1, 00:10:18, FastEthernet8
❶                   ❷      ❸
```

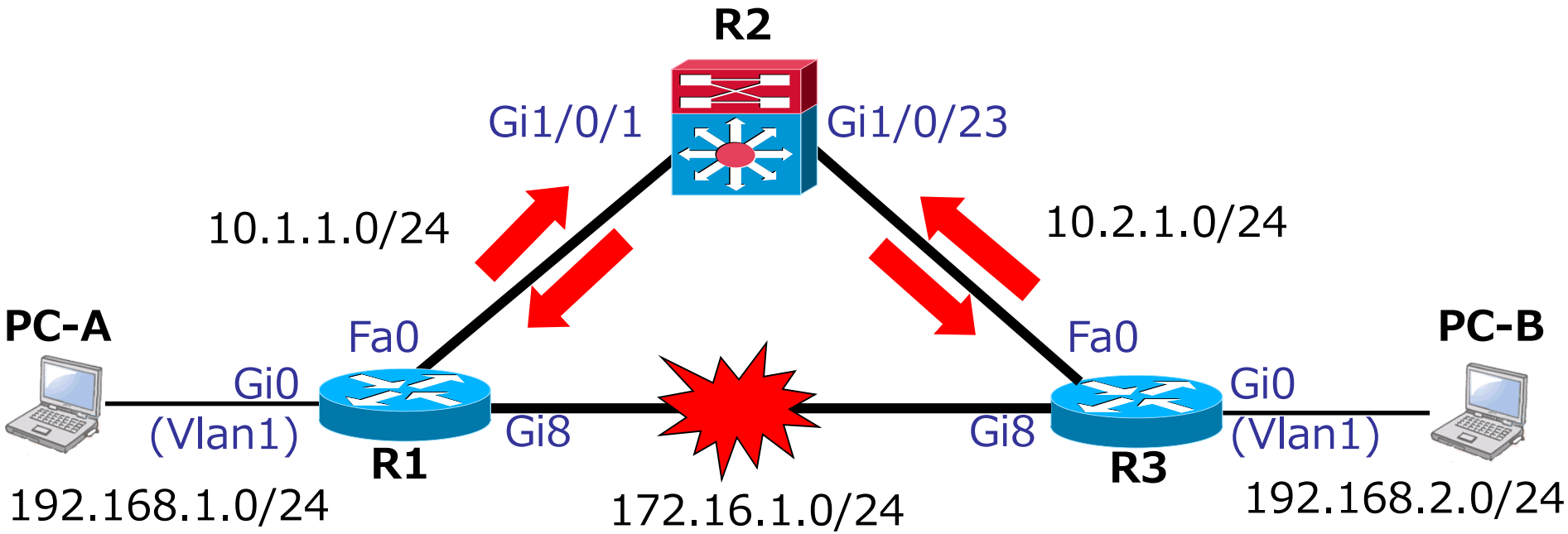
●確認コマンド(show ip ospf　neighbor)

```
Router#sh ip o ne

                                  ❶
Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.101.1      1   INIT/ -         00:00:30      10.0.1.1      FastEthernet 8
172.16.102.1      1   FULL/DR         00:00:30      10.0.2.1    GigabitEthernet 0
```

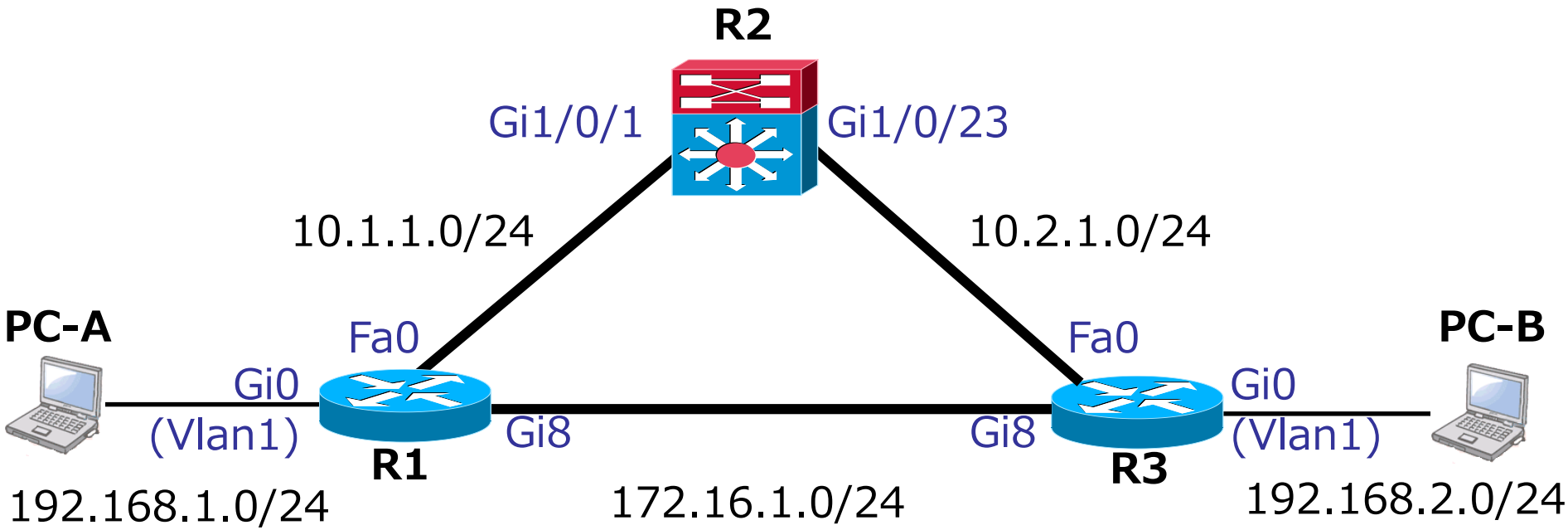
●OSPFネットワーク構築(演習)



●障害時の経路確認(演習)

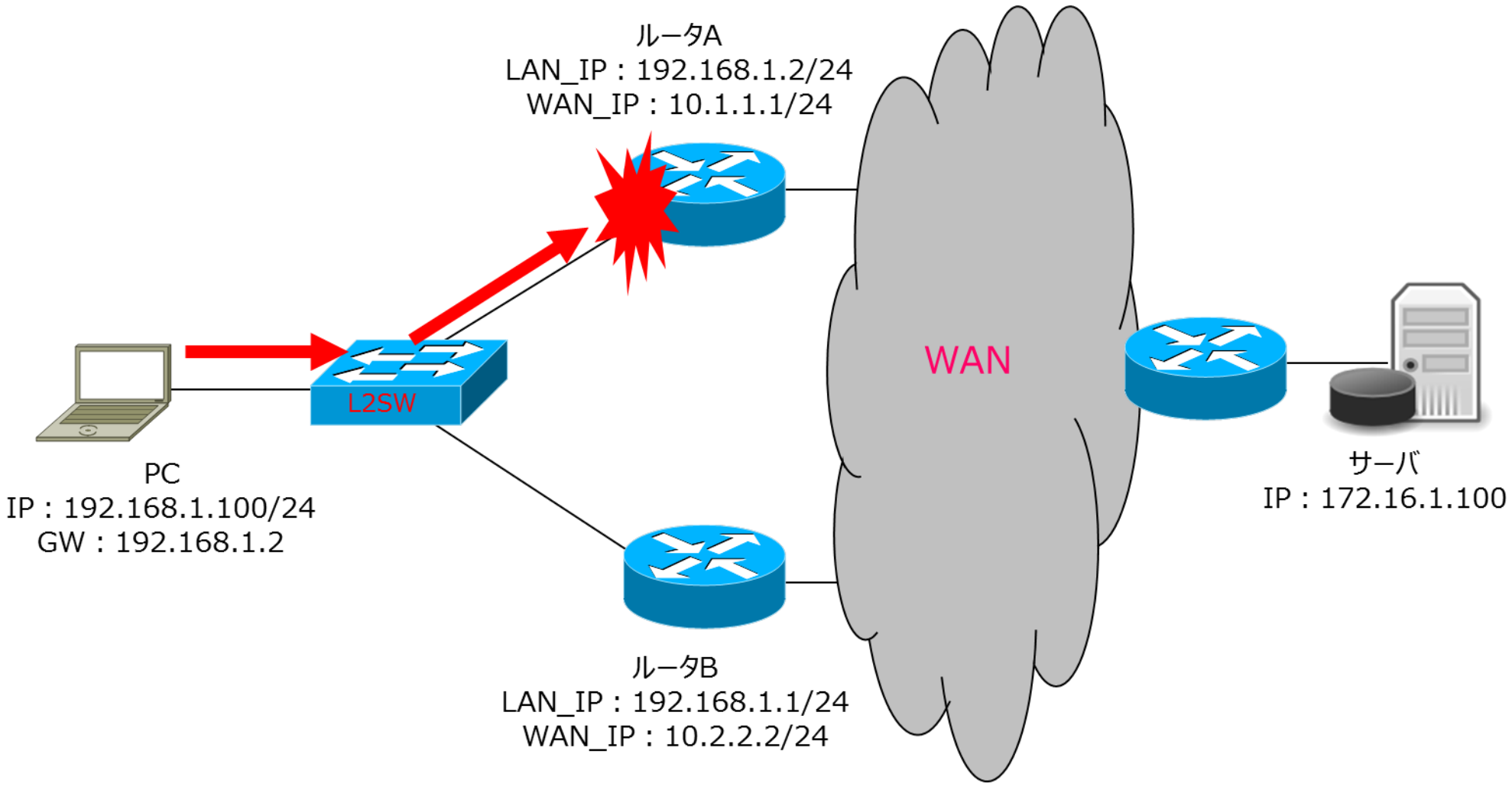

R2
Gi1/0/1
Gi1/0/23
10.1.1.0/24
10.2.1.0/24
PC-A
Fa0
Fa0
PC-B
Gi0
(Vlan1)
Gi8
Gi8
Gi0
(Vlan1)
R1
R3
192.168.1.0/24
172.16.1.0/24
192.168.2.0/24

●Cost値の設定・確認(参考演習)

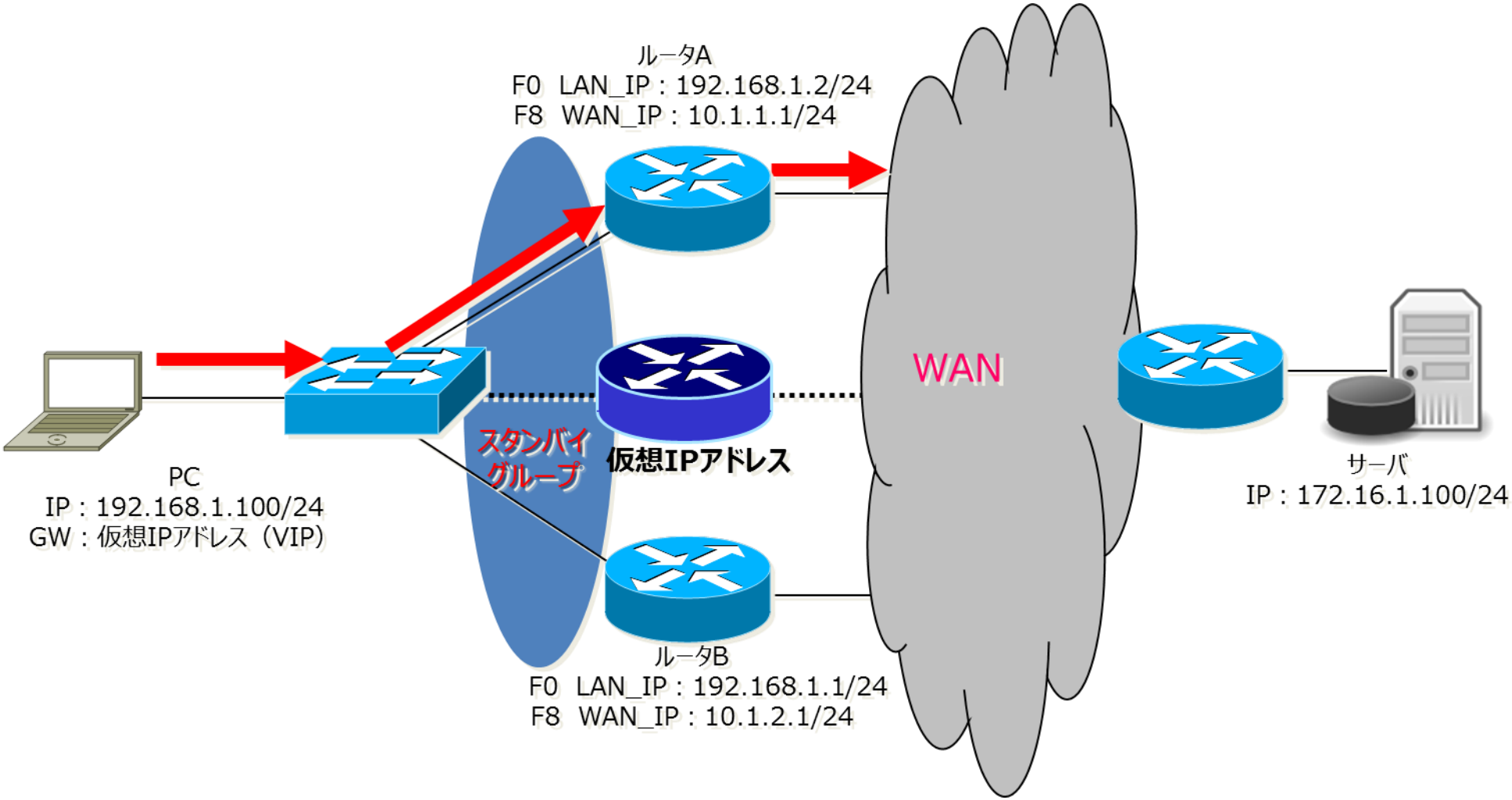


第4章
HSRP・VRRP
(冗長化プロトコル)

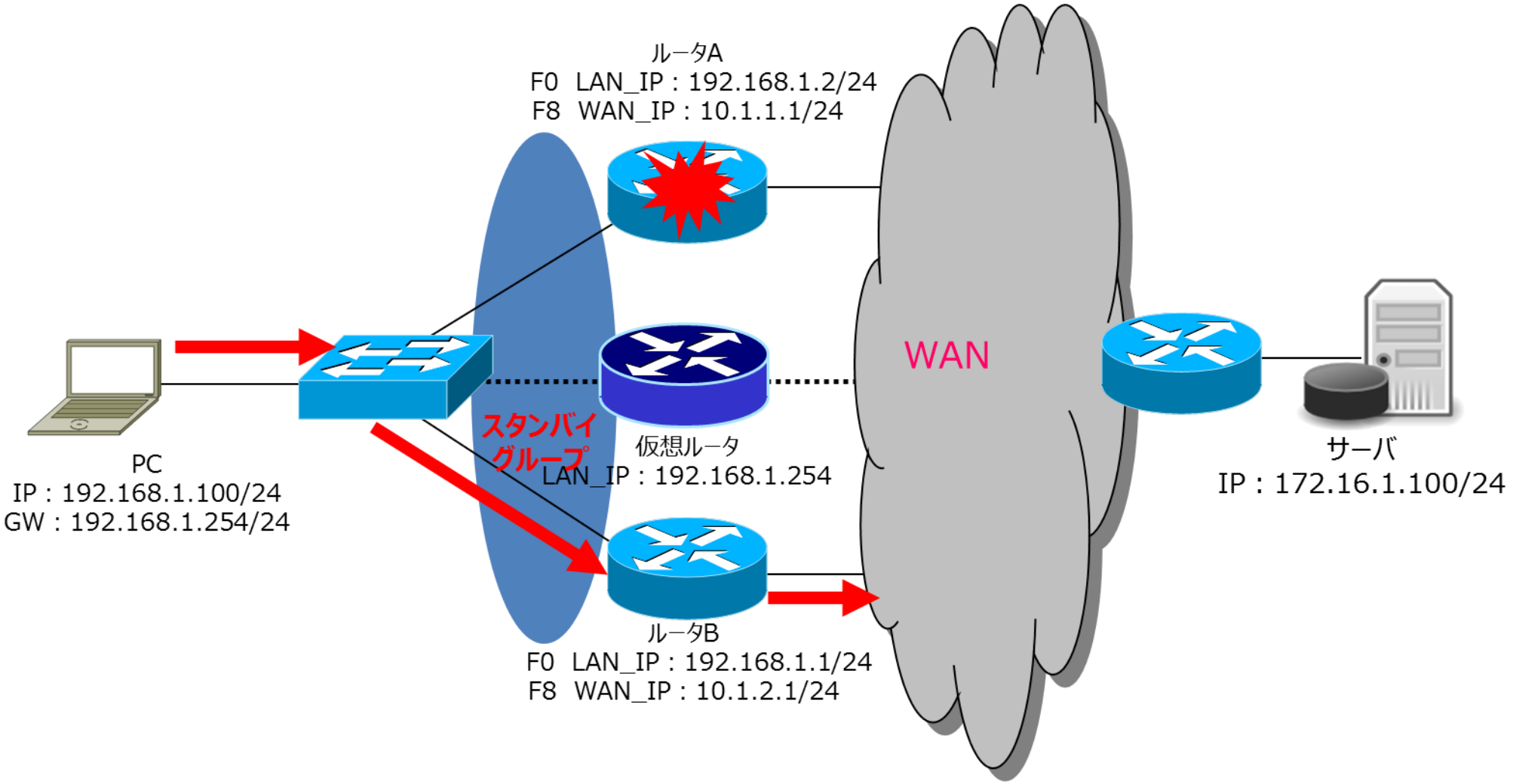
●デフォルトゲートウェイを使用した設定



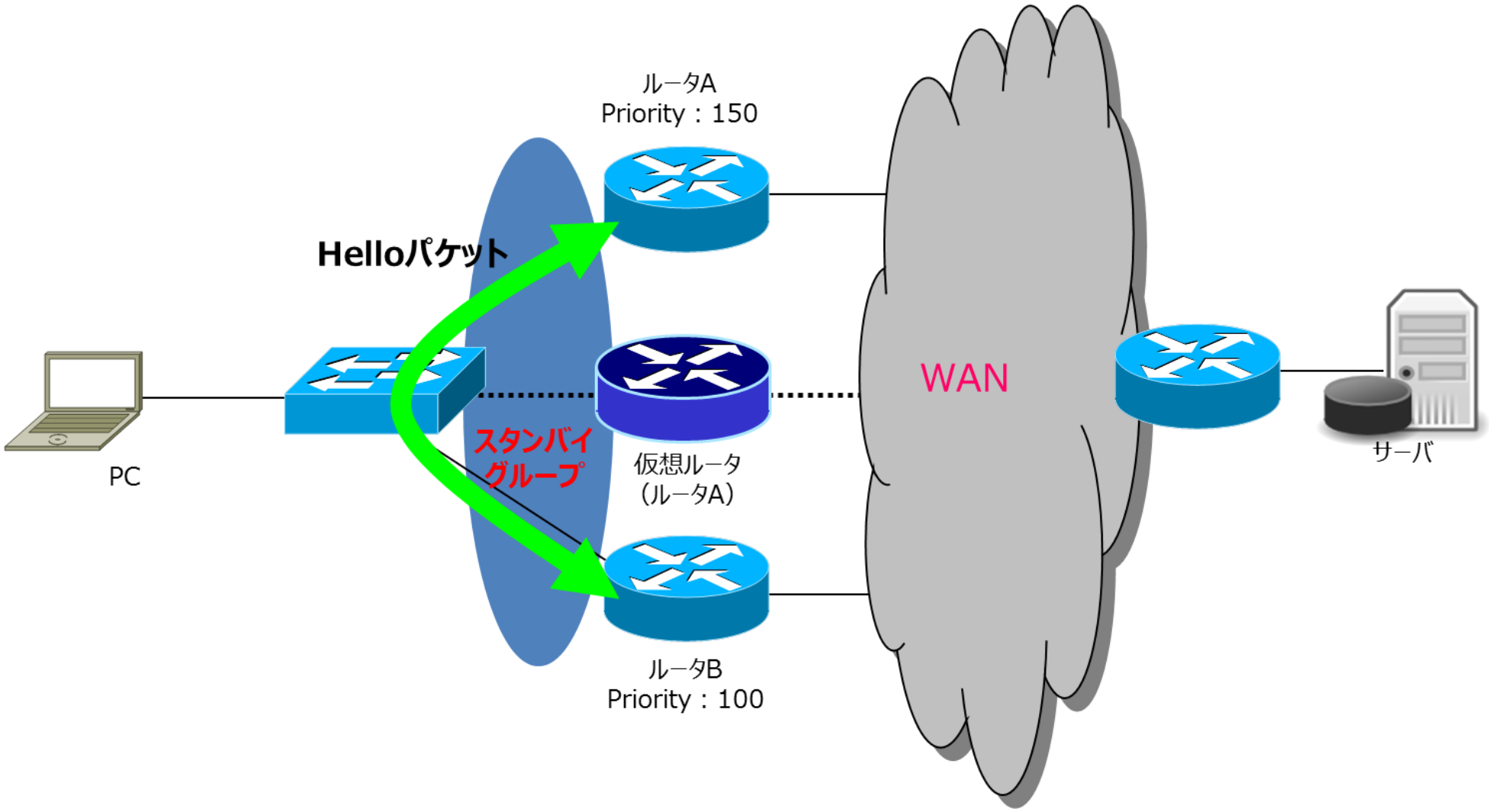
●HSRPの通信イメージ



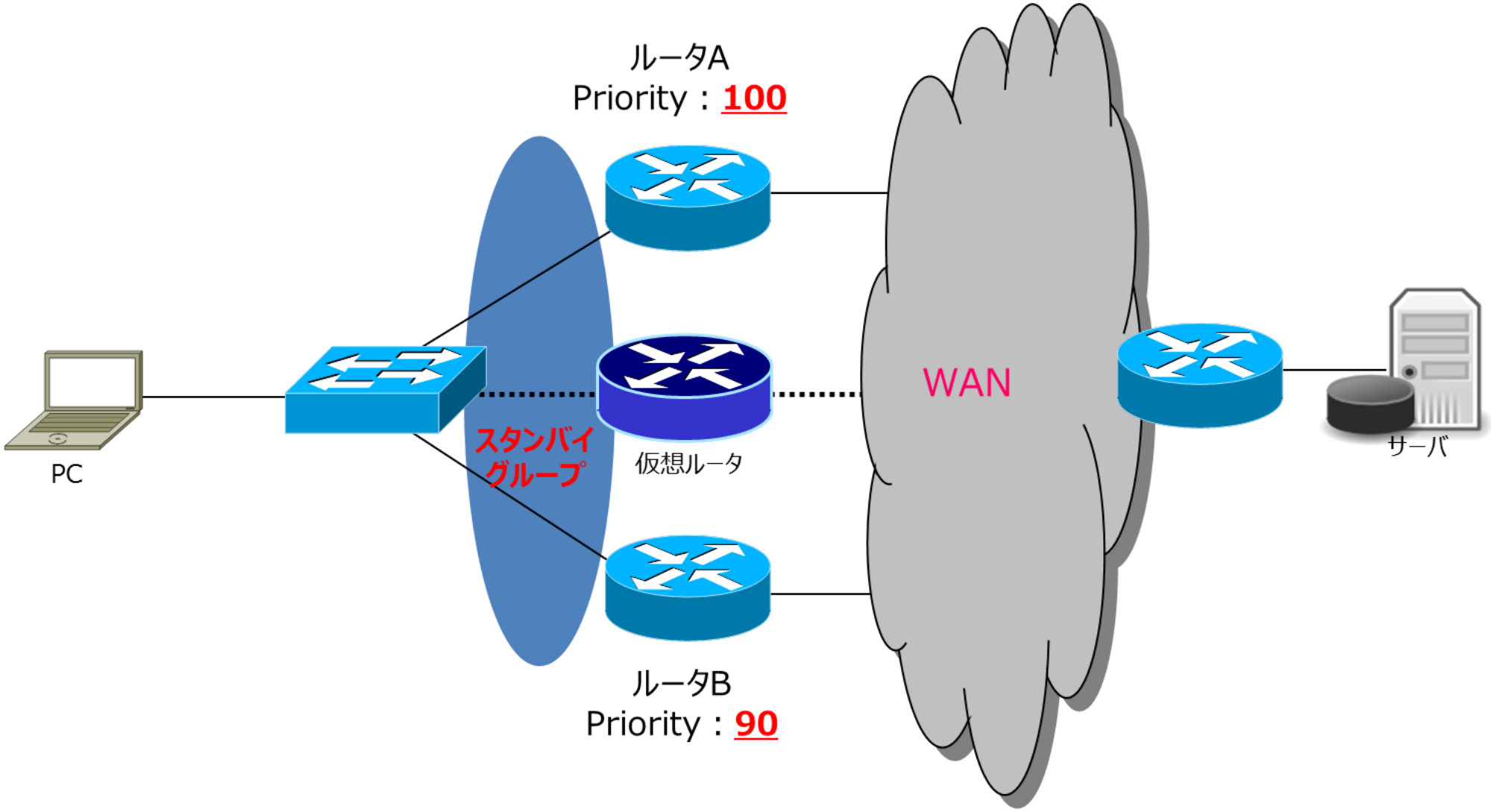
●HSRPの通信イメージ（続き）



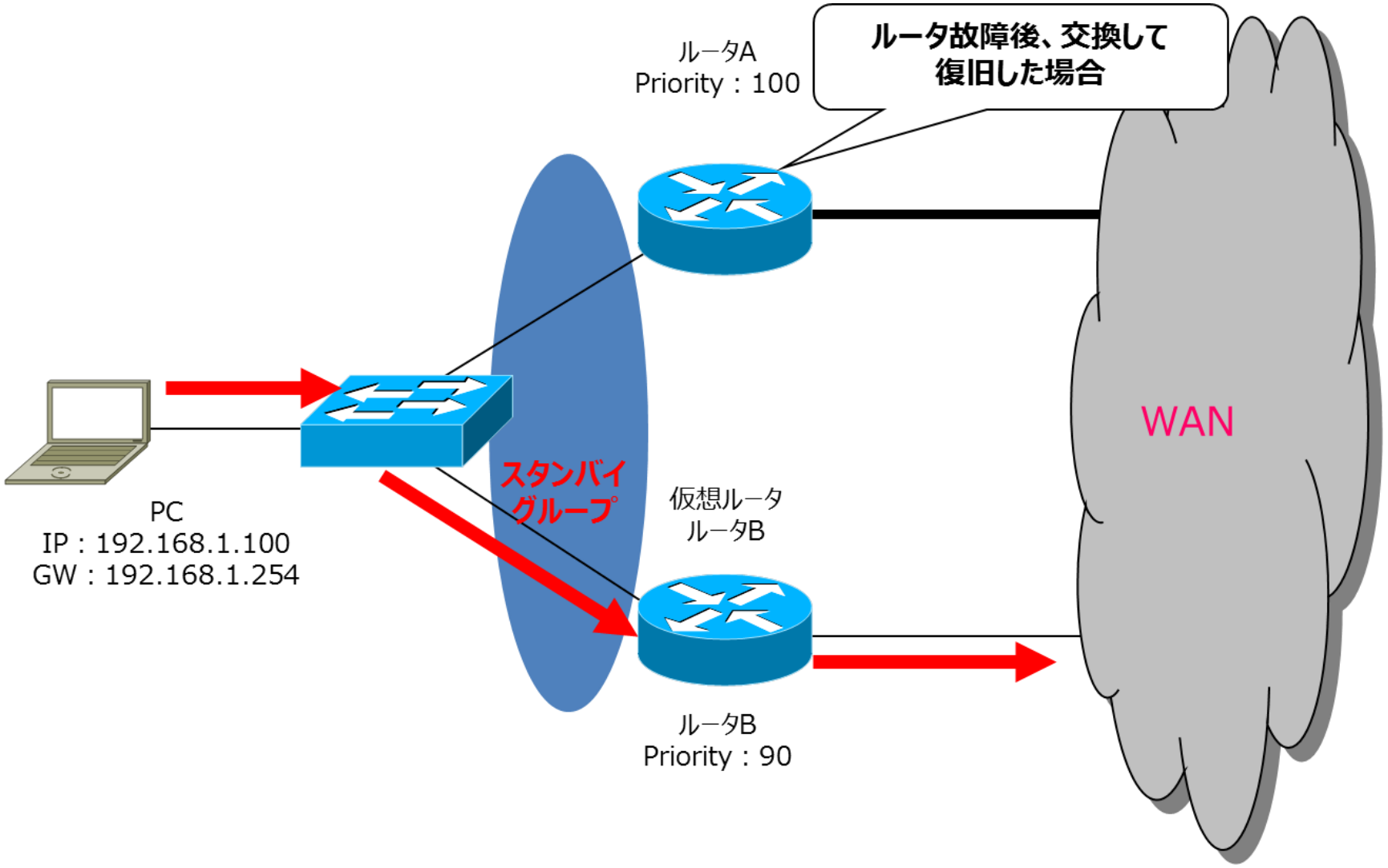
●Helloメッセージ


ルータA
Priority：150
Helloパケット
PC
スタンバイ
グループ
仮想ルータ
（ルータA）
ルータB
Priority：100
WAN
サーバ

●HSRPのプライオリティ



●HSRPスタンバイプリエンプト



※上記経路は、プリエンプトを設定していない場合

●HSRPの設定コマンド

■HSRPの設定コマンド

（config-if)#standby　[*group-number]*　ip　*ip-address*

■検証コマンド

#show　standby　brief

■設定例

interface　vlan 1
ip　address　1 0 .0.0.1　255.255.255.0
standby　10　ip　10.0.0.254

●HSRPの設定コマンド

■HSRPスタンバイプライオリティの設定コマンド

（config-if)#standby　[*group-number]*　priority　*priority-value*

■HSRPスタンバイプリエンプトの設定コマンド

（config-if)#standby　[*group-number]*　preempt

■設定例

interface　vlan 1
ip　address　10.0.0.1　255.255.255.0
standby　10　ip　10.0.0.254
standby　10　priority　90
standby　10　preempt

●HSRP確認コマンド

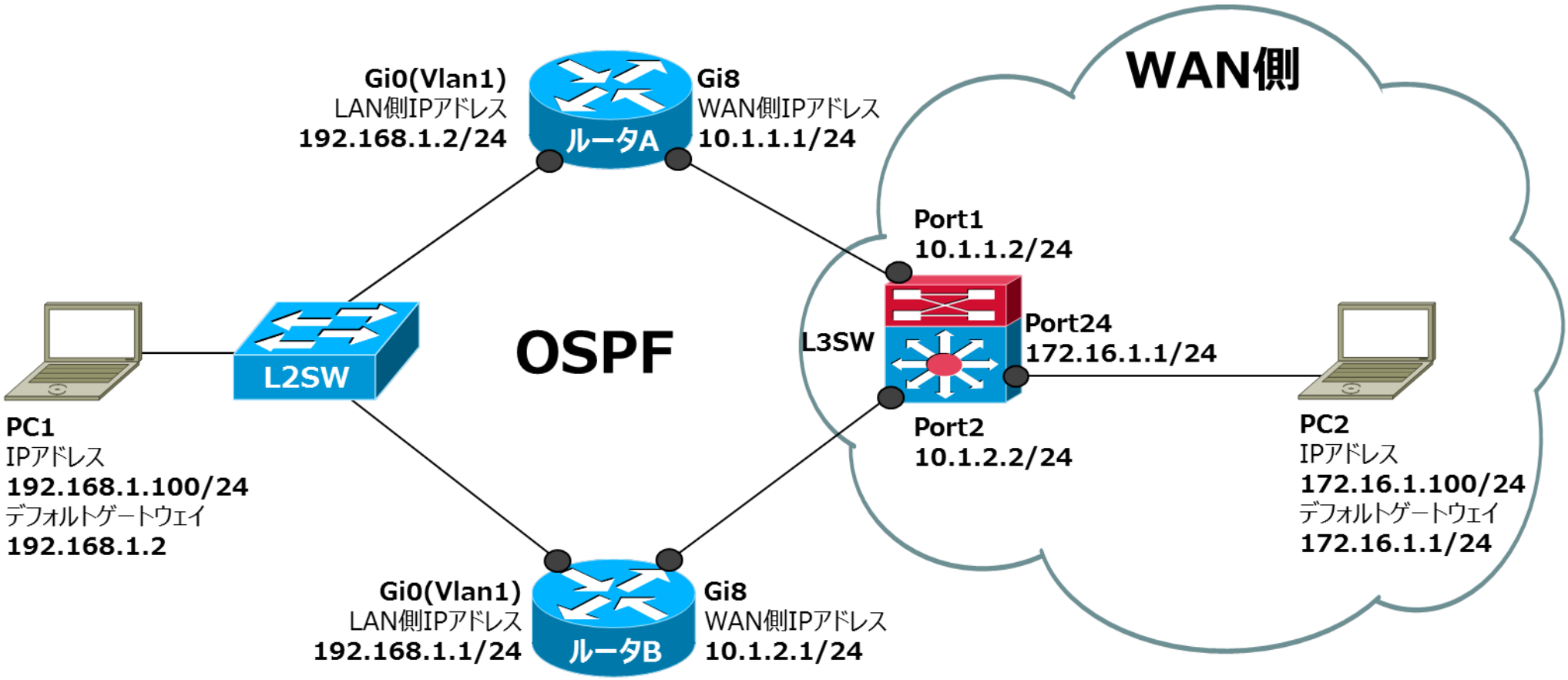
R1#show standby

```
Vlan 1 - Group 10
  State is Standby
    4 state changes, last state change 00:10:56
  Virtual IP address is 192.168.1.254
  Active virtual MAC address is 0000.0c07.ac0a
    Local virtual MAC address is 0000.0c07.ac0a (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.832 secs
  Preemption enabled
  Active router is 192.168.1.1, priority 100 (expires in 9.836 sec)
  Standby router is local
  Priority 95 (configured 105)
  IP redundancy name is "hsrp-Fa0-10" (default)
```

R1#show standby brief

```
                     P indicates configured to preempt.
Interface   Grp Prio P State         Active          Standby         Virtual IP
vlan1        10   95   P Standby  192.168.1.1   local       192.168.1.254
```

●事前設定_HSRP使用前（演習）



●事前設定_ルータAの設定(Config)

```
> en
# conf t
(config)# hostname RouterA
(config)# int vlan 1
(config-if)# ip address 192.168.1.2 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
(config)# int gi 8
(config-if)# ip address 10.1.1.1 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
(config)# router ospf 1
(config-router)# network 192.168.1.0 0.0.0.255 area 0
(config-router)# network 10.1.1.0 0.0.0.255 area 0
(config-router)# end
# copy run start
```

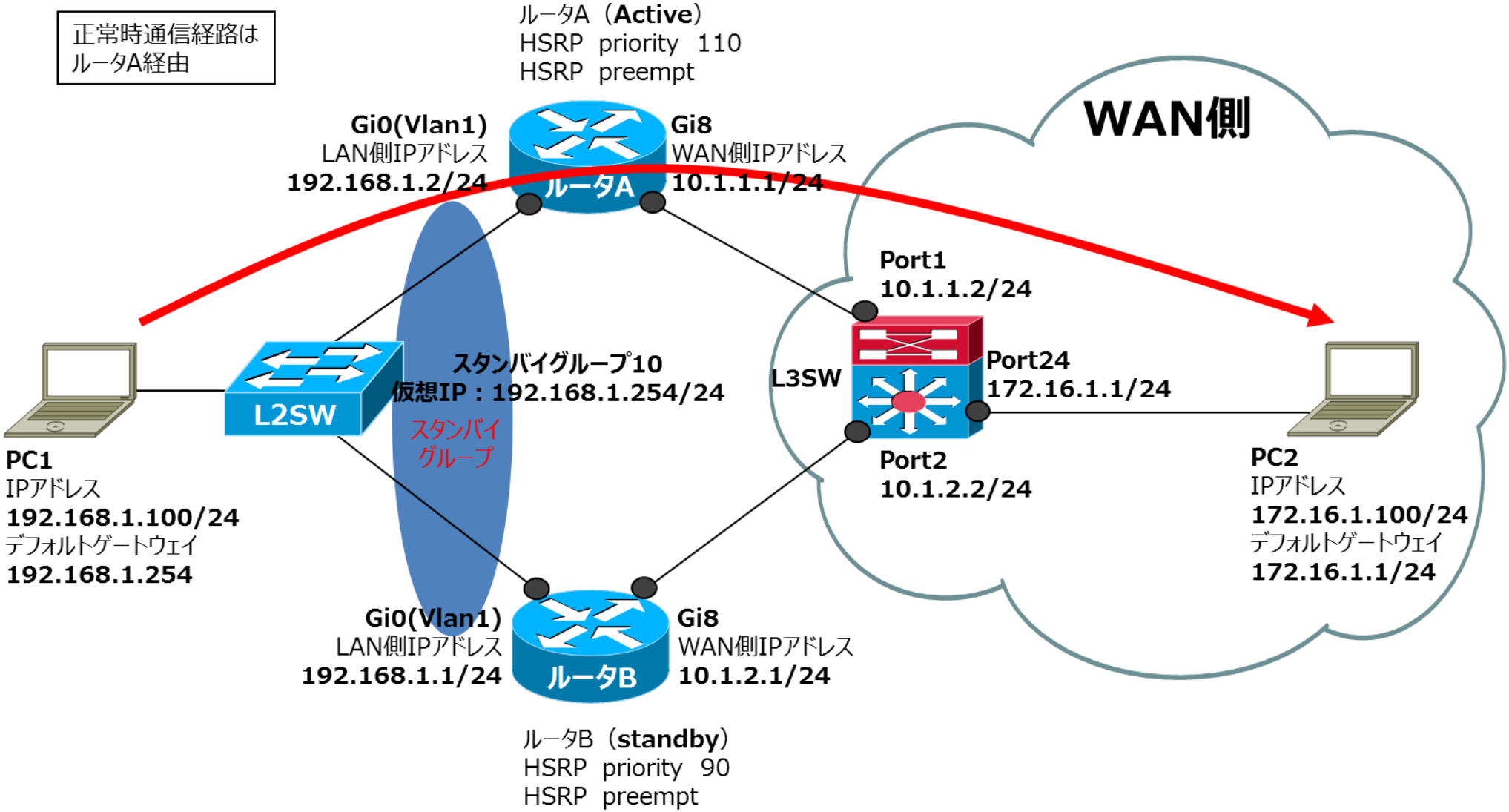
●事前設定_ルータBの設定(Config)

```
> en
# conf t
(config)# hostname RouterB
(config)# int vlan 1
(config-if)# ip address 192.168.1.1 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
(config)# int gi 8
(config-if)# ip address 10.1.2.1 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
(config)# router ospf 1
(config-router)# network 192.168.1.0 0.0.0.255 area 0
(config-router)# network 10.1.2.0 0.0.0.255 area 0
(config-router)# end
# copy run start
```

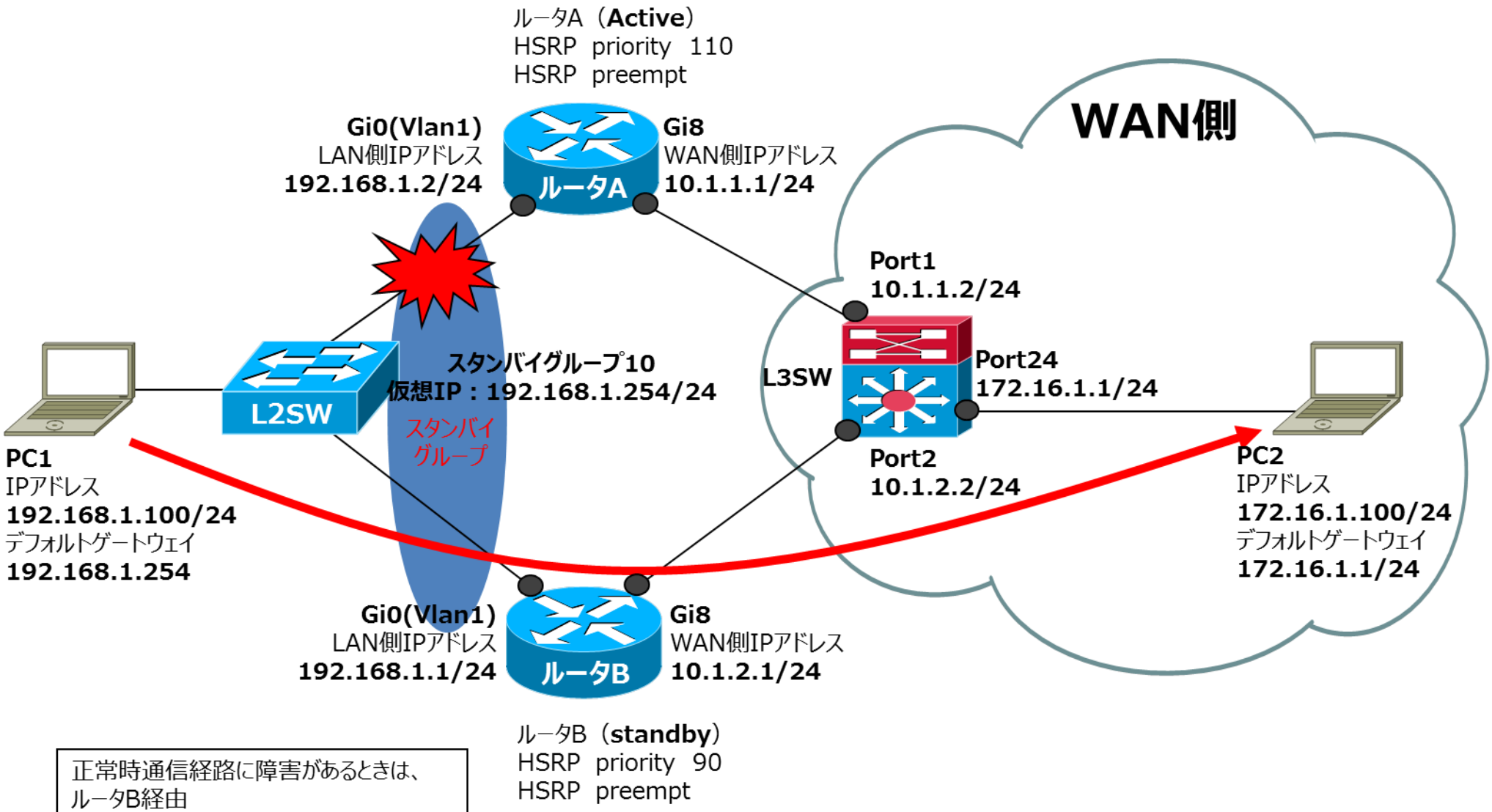
●事前設定_Cat3850の設定(Config)

```
> en
# conf t
(config)# ip routing
(config)# int gi 1/0/1
(config-if)# no switchport
(config-if)# ip address 10.1.1.2 255.255.255.0
(config-if)# exit
(config)# int gi 1/0/2
(config-if)# no switchport
(config-if)# ip address 10.1.2.2 255.255.255.0
(config-if)# exit
(config)# int gi 1/0/24
(config-if)# no switchport
(config-if)# ip address 172.16.1.1 255.255.255.0
(config-if)# exit
(config)# router ospf 1
(config-router)# network 10.1.1.0 0.0.0.255 area 0
(config-router)# network 10.1.2.0 0.0.0.255 area 0
(config-router)# network 172.16.1.0 0.0.0.255 area 0
(config-router)# end
# copy run start
```

●HSRPの最適化オプション(演習)

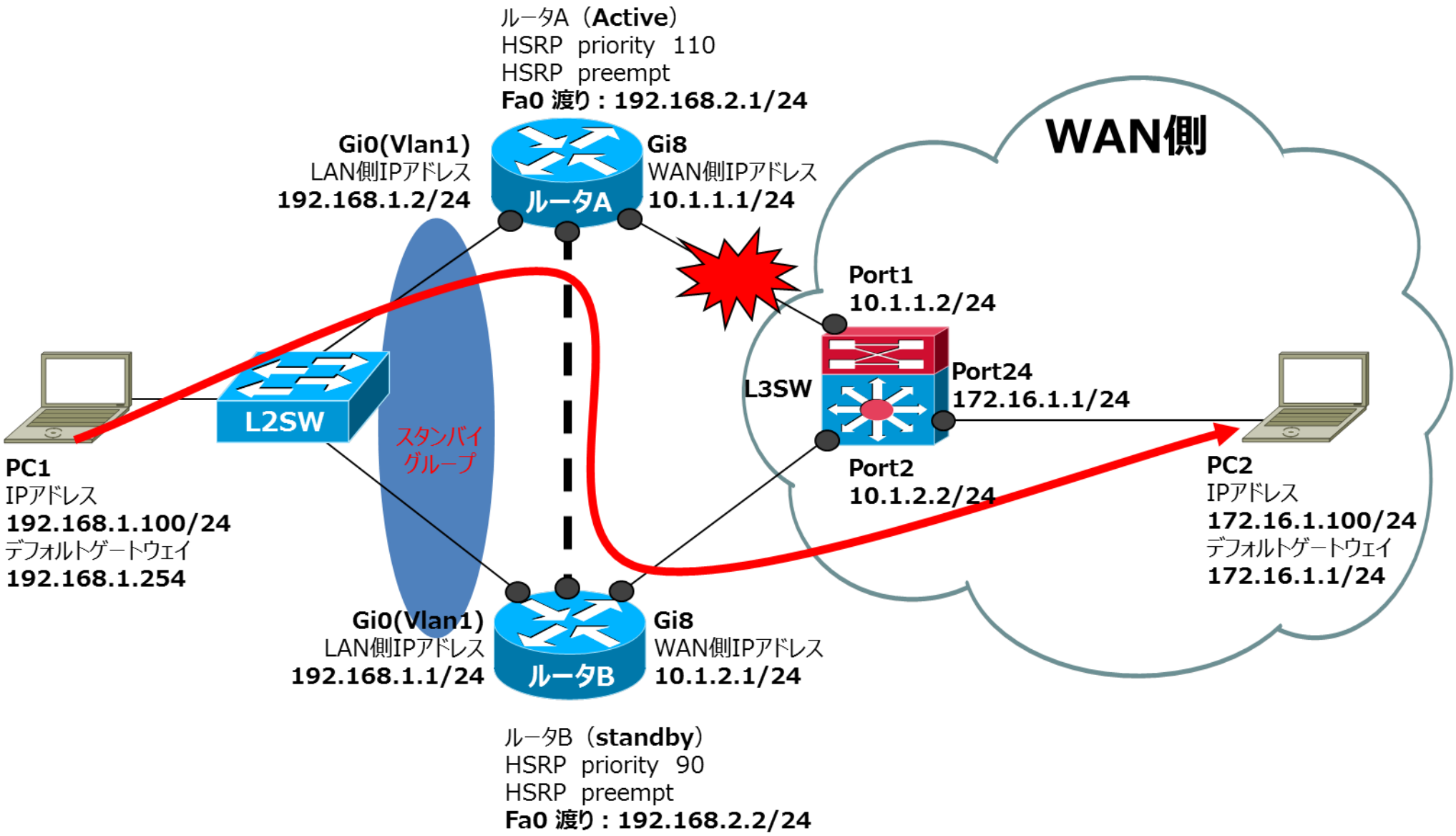


●障害発生・疎通確認（演習）

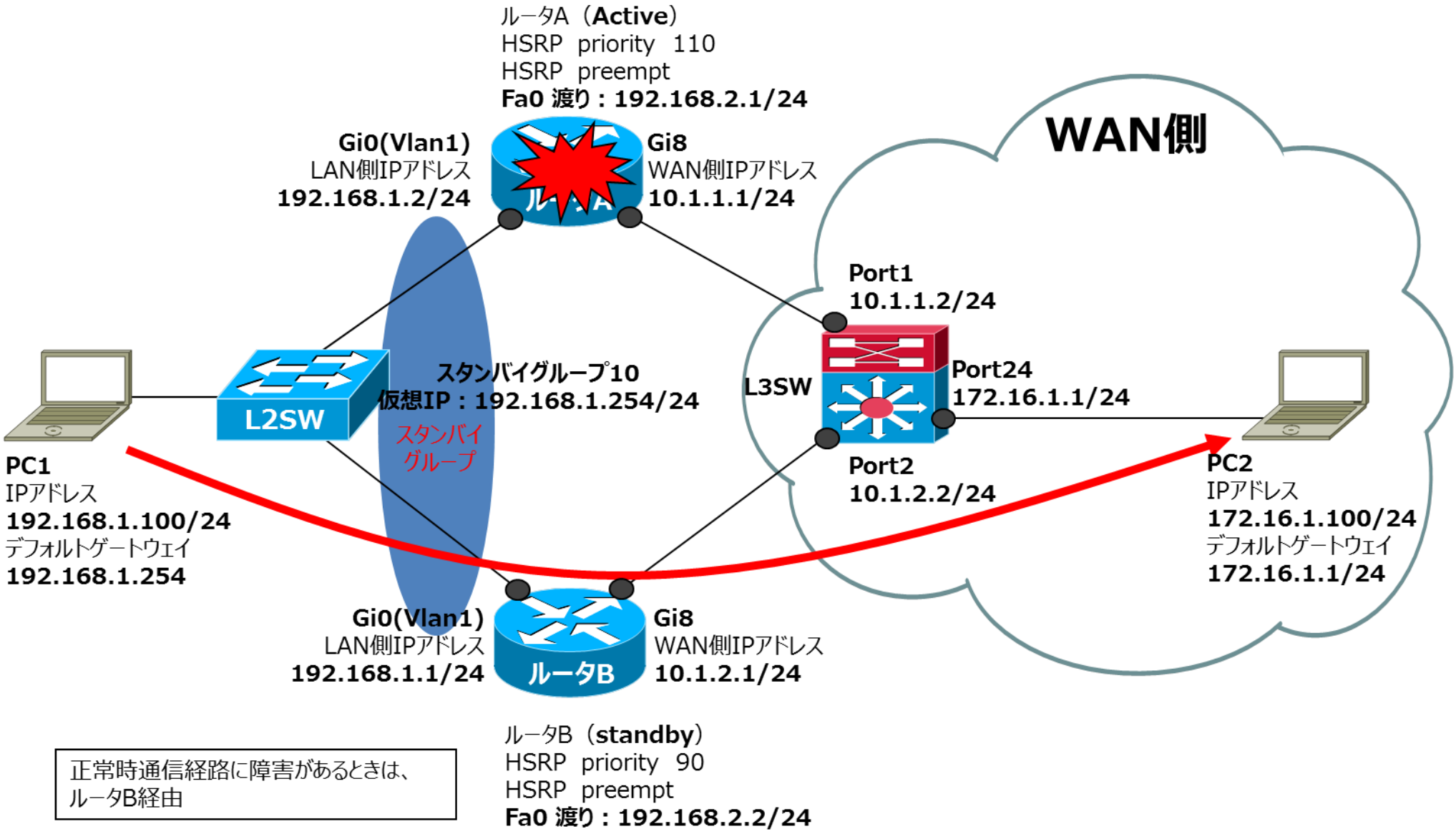


正常時通信経路に障害があるときは、
ルータB経由

●障害発生・疎通確認（演習）

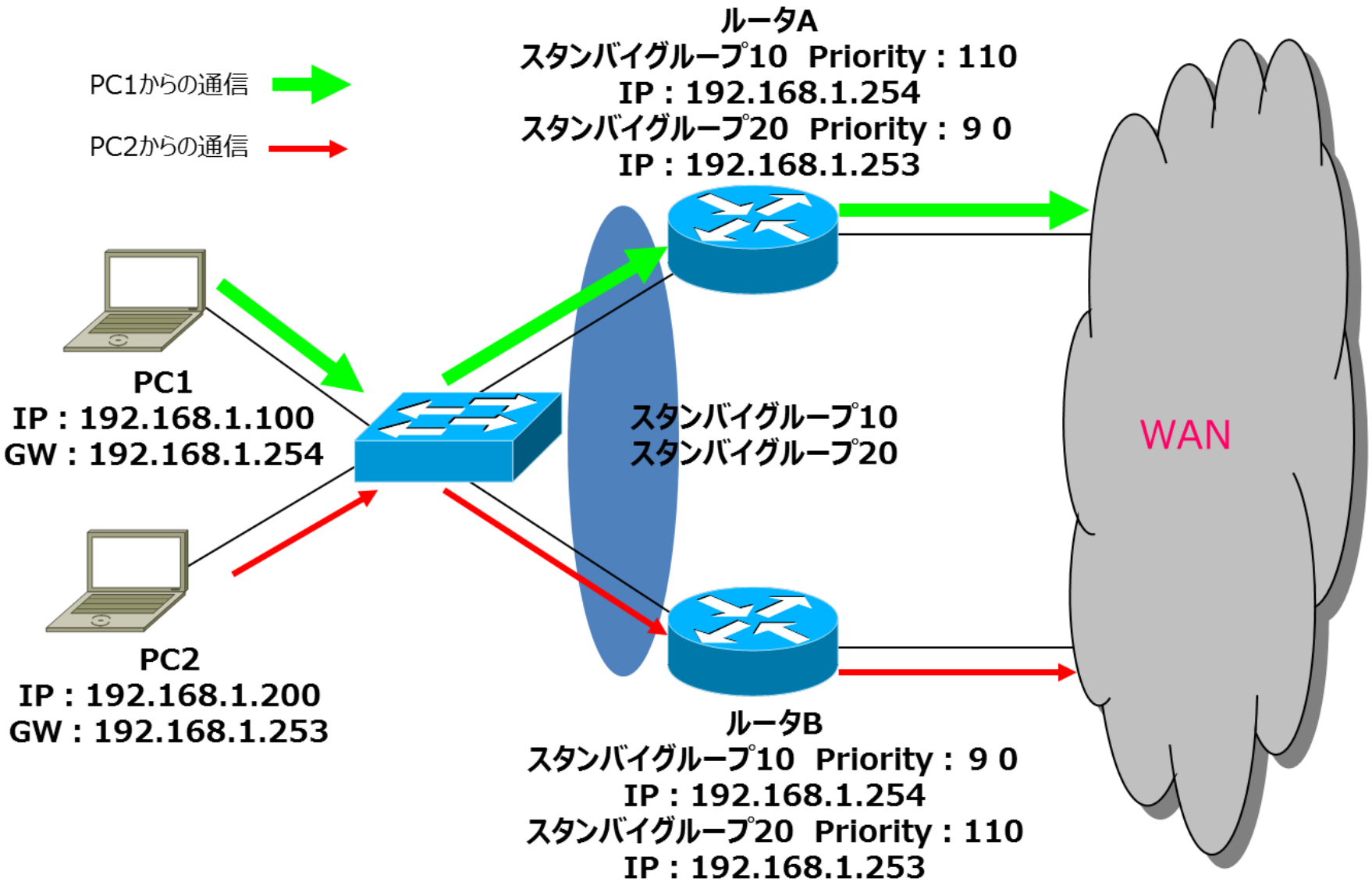

ルータA（Active）
HSRP priority 110
HSRP preempt
Fa0 渡り：192.168.2.1/24
Gi0(Vlan1)
LAN側IPアドレス
192.168.1.2/24
Gi8
WAN側IPアドレス
10.1.1.1/24
ルータA
WAN側
Port1
10.1.1.2/24
L3SW
Port24
172.16.1.1/24
Port2
10.1.2.2/24
L2SW
スタンバイ
グループ
PC1
IPアドレス
192.168.1.100/24
デフォルトゲートウェイ
192.168.1.254
PC2
IPアドレス
172.16.1.100/24
デフォルトゲートウェイ
172.16.1.1/24
Gi0(Vlan1)
LAN側IPアドレス
192.168.1.1/24
Gi8
WAN側IPアドレス
10.1.2.1/24
ルータB
ルータB（standby）
HSRP priority 90
HSRP preempt
Fa0 渡り：192.168.2.2/24

●障害発生・疎通確認（演習）



正常時通信経路に障害があるときは、
ルータB経由

●HSRPを使用したロードシェアリング



●HSRPの設定と検証に使用するコマンド

設定例

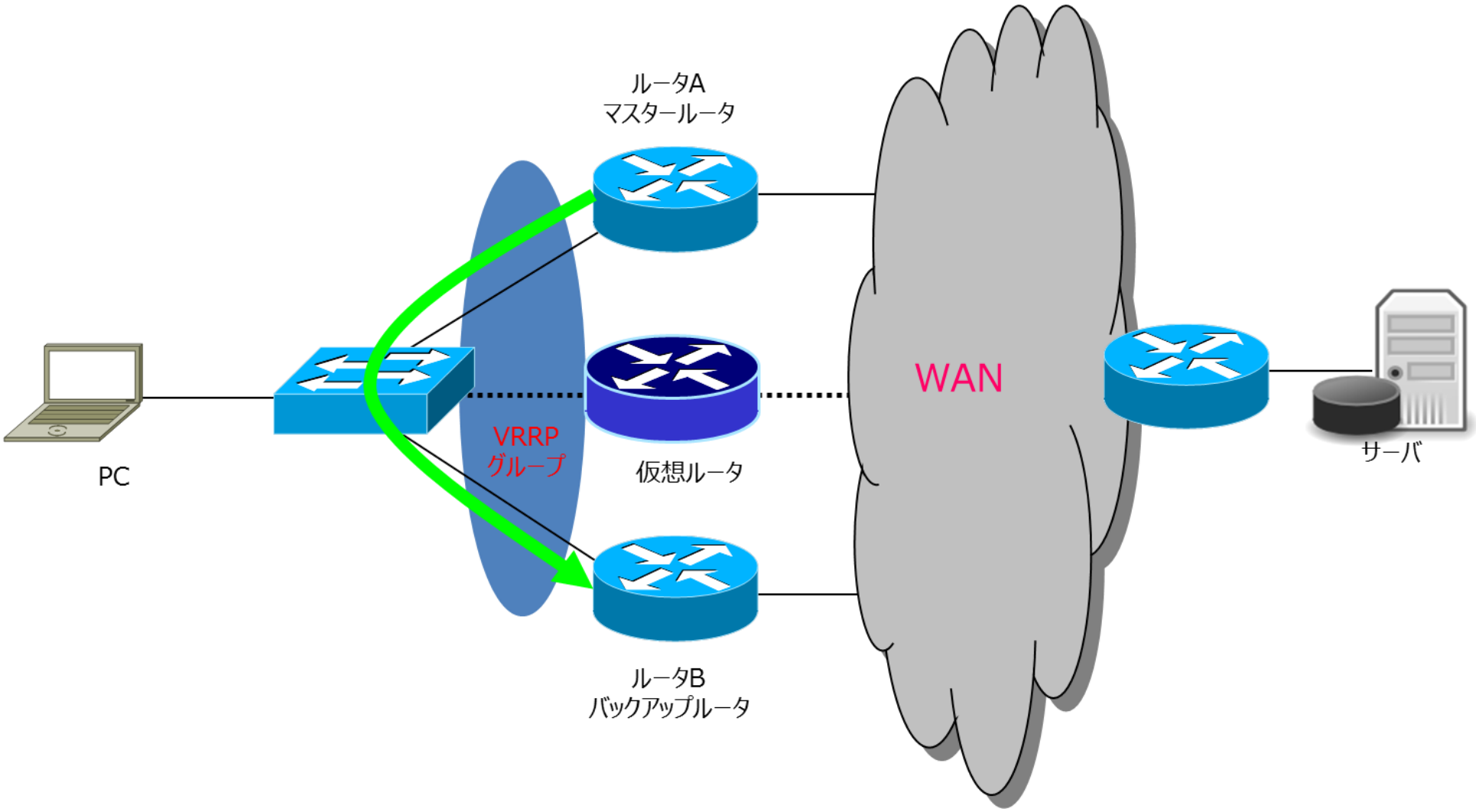
RouterA

```
interface　fa0
ip　address　192.168.1.2　255.255.255.0
standby　10　ip　192.168.1.254
standby　10　priority　110
standby　20　ip　192.168.1.253
standby　20　priority　90
```

RouterB

```
interface　fa0
ip　address　192.168.1.1　255.255.255.0
standby　10　ip　192.168.1.254
standby　10　priority　90
standby　20　ip　192.168.1.253
standby　20　priority　110
```

●VRRPとHSRPの相違点



●VRRPの設定と検証に使用するコマンド

■VRRPの設定コマンド
(config-if)#vrrp　[*group-number*]　ip　[*virtual-gateway-address*]

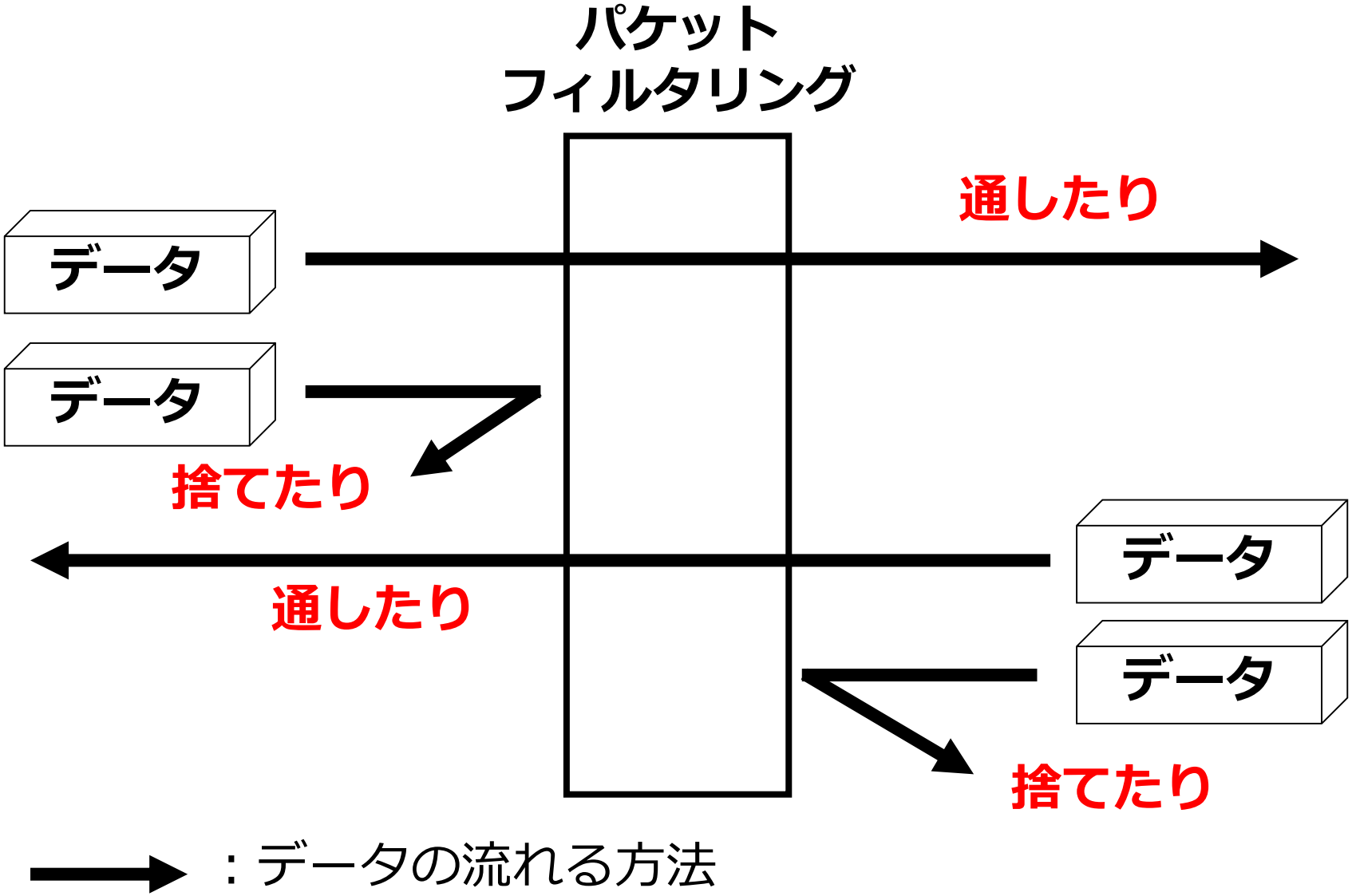
■VRRPのプライオリティの設定
(config-if)#vrrp　[*group-number*]　priority　*[priority-value*]

参考コンフィグ

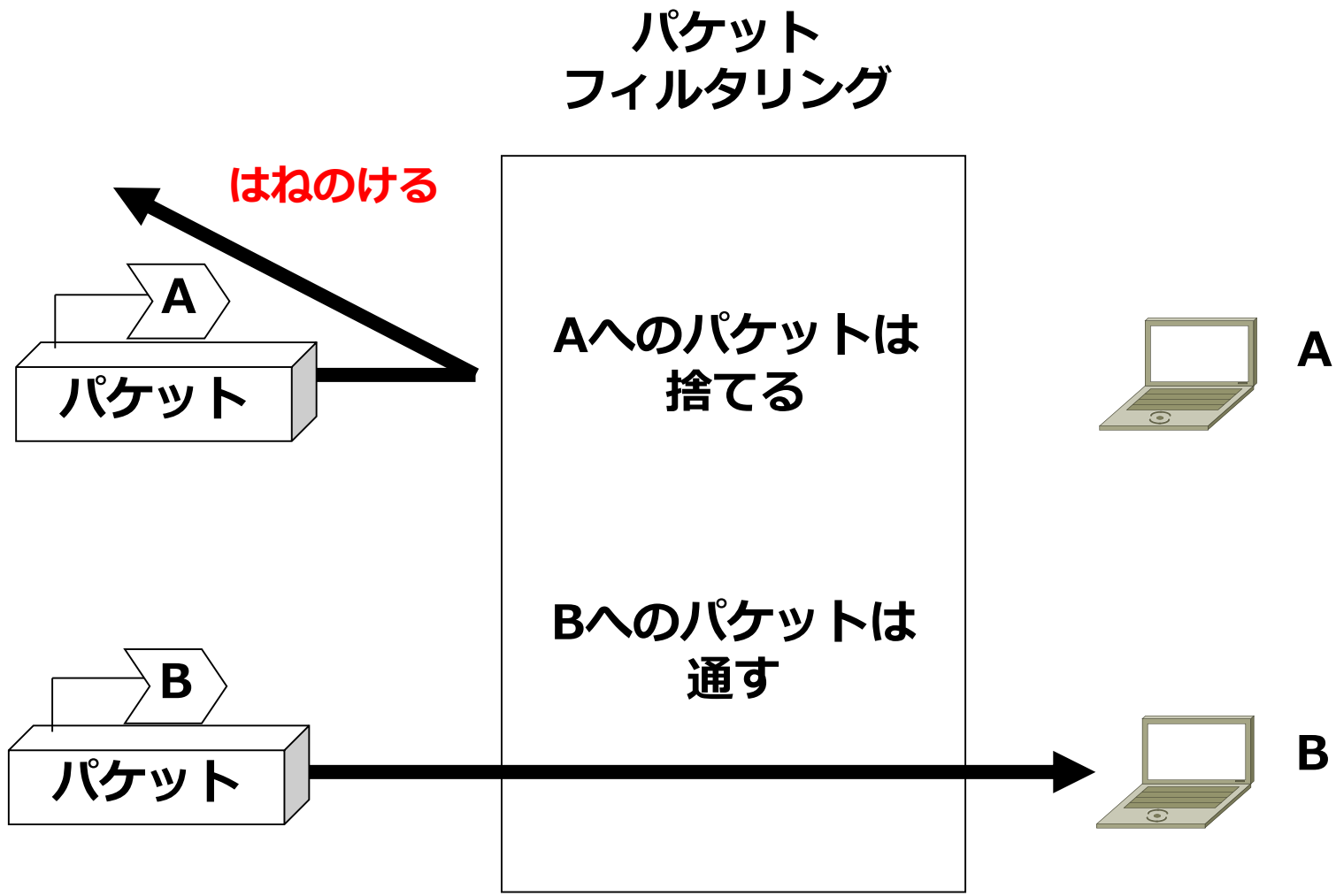
Router
interface　fa0
ip　address　192.168.1.2　255.255.255.0
vrrp　10　ip　192.168.1.254
vrrp　10　priority　110

第5章
ACL
(アクセスコントロールリスト)

●パケットフィルタリングの動作



●パケットとヘッダ情報



※パケットとは、TCP/IPネットワークにおけるデータの最小単位を指す

●パケットを分別するための指標

1．IPアドレス

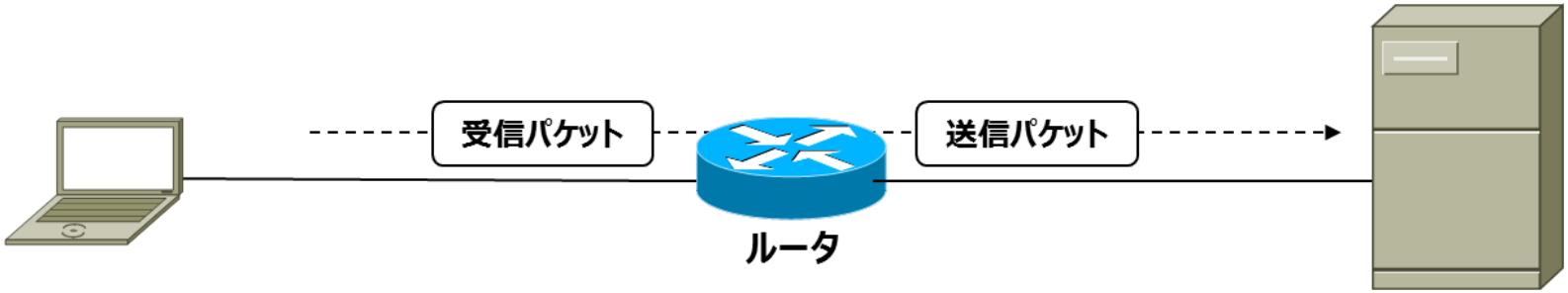
2．ポート番号

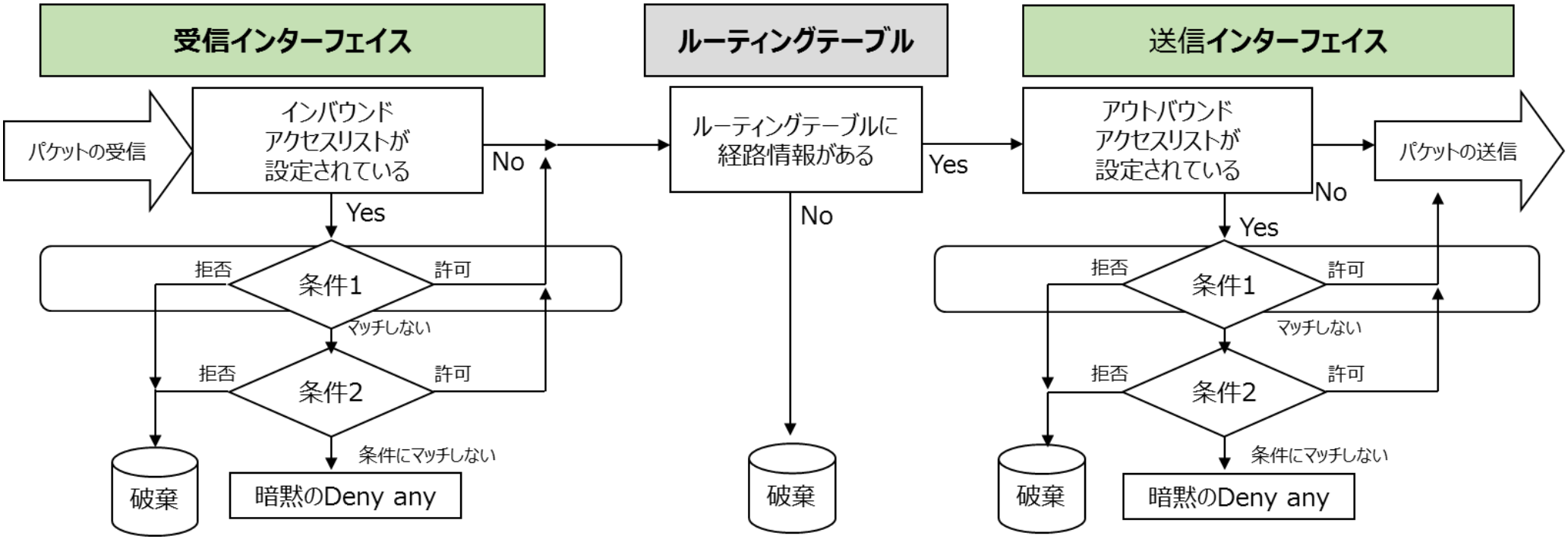
3．プロトコル

4．フラグ

5．データの方向

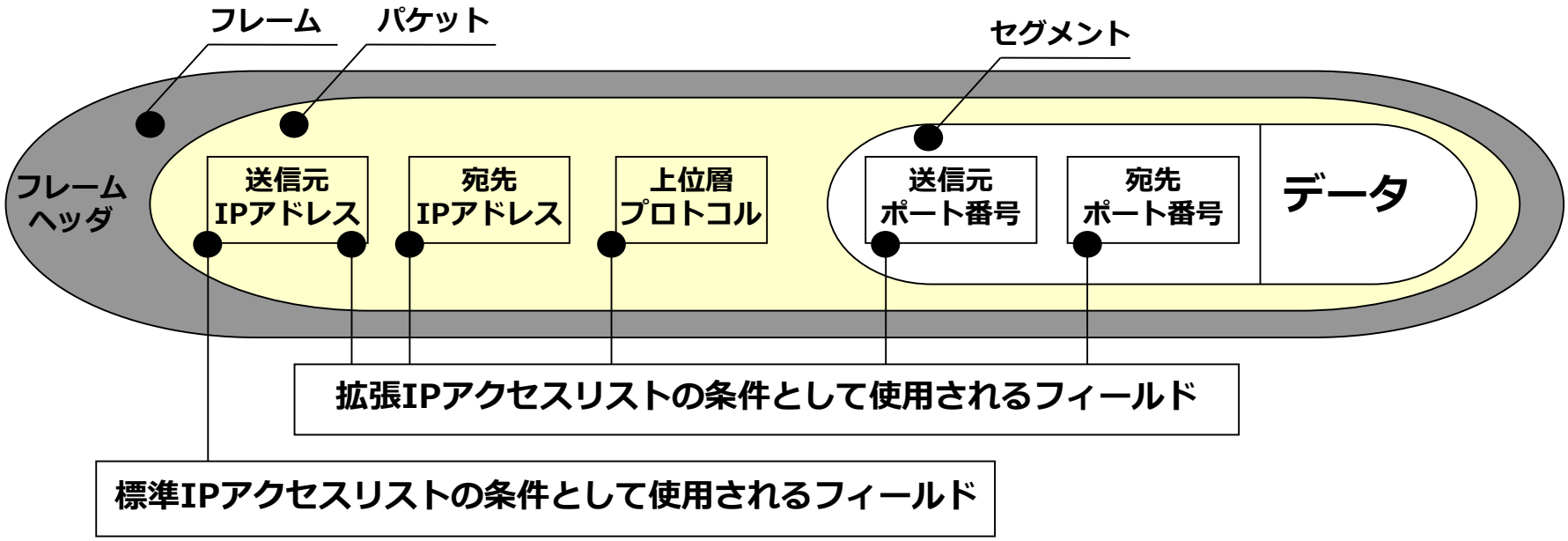
●アクセスリストの概要（Cisco）





●IPアクセスリストの特徴

アクセスリストには、**標準IPアクセスリスト**と**拡張IPアクセスリスト**があります



アクセスリストの識別方法

アクセスリストのタイプ	番号の範囲
標準IPアクセスリスト	1～99，1300~1999（IOS12.0以降で使用可能）
拡張IPアクセスリスト	100～199，2000~2699 （IOS12.0以降で使用可能）

●ワイルドカードマスクの特徴

●ネットワークマスクやサブネットマスクは「IPアドレスのネットワーク部の範囲」を表す

１０進表記のIPアドレス	１９２	１６８	5	2
２進数表記の IPアドレス	11000000	10101000	00000101	00000010
２進数表記の ネットワークマスク	11111111	11111111	11111111	00000000
１０進数表記の ネットワークマスク	２５５	２５５	２５５	0

●ワイルドカードマスクは「アクセスリストでチェックする範囲」を表す

１０進数表記の IPアドレス	１９２	１６８	5	2
２進数表記の IPアドレス	11000000	10101000	00000101	00000010
２進数表記の ワイルドカードマスク	00000000	00000000	00000000	11111111
１０進数表記の ワイルドカードマスク	0	0	0	２５５

●標準IPアクセスリストの設定

１．access-listコマンドで標準IPアクセスリストを作成します。

●**Router(Config)#　access-list　アクセスリスト番号　アクション　送信元アドレス**

①　②　③

① 標準ＩＰアクセスリストでは，1～99,1300～1999を指定可能
② permit（許可）もしくはdeny（拒否）を指定
③ IPアドレスとワイルドカード・マスクで指定

２．作成した標準IPアクセスリストを適切なインターフェイスに適用します。

●**Router(Config-if)#　ip　access-group　作成したアクセスリスト番号　適用処理方法**

④　⑤

④ ①で作成したアクセスリスト番号と同じ番号を指定
⑤ in（インバウンド）もしくはout（アウトバウンド）を指定
※指定しない場合、デフォルト値で「out」が適用

●標準IPアクセスリスト設定例

グローバルコンフィグレーションモードに変更する

①**(config)#access-list　?**

<1-99>・・・一覧から標準IPアクセスリストのうち適当なアクセスリスト番号を選択する

② **(config)#access-list　1 0　?**

permit・・・許可する

deny・・・・拒否する

③**(config)#access-list　1 0　deny　?**

any・・・すべてのホスト

host・・ホストを1台のみ指定する場合

④ **(config)#access-list　1 0　deny　host 192.168.11.1**

192.168.11.1は、許可しない(ホストの場合は、1台のみの設定で使用)

最後にアクセスリストをポートに設定する

⑤ (config)#**interface　fa xx**・・・アクセスリストをポートに設定する

⑥ (config-if)#**ip access-group 10 out**・・・IPは忘れずに

●拡張IPアクセスリストの設定

1．access-listコマンドで拡張IPアクセスリストを作成します。

●**Router(Config)#　access-list　アクセスリスト番号　アクション　プロトコルタイプ**
①　②　③

送信元IPアドレス　送信元ポート番号　宛先アドレス　オプション　宛先ポート番号
④　⑤　⑥　⑦　⑧

① 拡張IPアクセスリストでは，100～199，2000～2699を指定可能
② permit（許可）もしくはdeny（拒否）を指定
③ ip,icmp,ospf,tcp,udpなど該当するプロトコルを指定
④ IPアドレスとワイルドカード・マスクで指定
⑤ 指定しなくても良い。指定しない場合は全ポート番号が対象となる
⑥ IPアドレスとワイルドカード・マスクで指定
⑦ eq（～と等しい）などプロトコルに指定するものに応じて指定
⑧ 指定しなくても良い。指定しない場合は全ポート番号が対象となる

2．作成した拡張IPアクセスリストを適切なインターフェイスに適用します。

●Router(Config-if)#　**ip　access-group　作成したアクセスリスト番号　適用処理方法**
⑨　⑩

⑨ ①で作成したアクセスリスト番号と同じ番号を指定
⑩ in（インバウンド）もしくはout（アウトバウンド）を指定
※指定しない場合、デフォルト値で「out」が適用

●拡張IPアクセスリストの設定例

①(config)#**access-list　?**
<100-199>・・・一覧から拡張IPアクセスリストのうち適当なアクセスリスト番号を選択する
② (config)#**access-list　110　?**
permit・・・許可する
deny・・・・拒否する
③(config)#**access-list　110　deny　?**
プロトコル一覧が表示される(telnetをフィルタする)
④ (config)#**access-list　110　deny　tcp　?**
条件に指定する送信元アドレス
⑤(config)#**access-list　110　deny　tcp　any　?**
条件に指定する宛先アドレス
⑥ (config)#**access-list　110　deny　tcp　any　host　172.16.19.1　?**
tcpの何に対してかの設定の一覧が表示される
⑦(config)#**access-list　110　deny　tcp　any　host　172.16.19.1　eq　telnet**
⑧(config)#**access-list　110　permit　ip　any　any**(0.0.0.0 255.255.255.255)
暗黙のDenyがあるため，最終行にAll Permitの設定

最後にアクセスリストをポートに設定する
⑨ (config)#**interface　fa xx**・・・アクセスリストをポートに設定する
⑩ (config-if)#**ip access-group 110 in**・・・拡張は送信元に近い方に設定する

●ポート番号表

主なウェルノンポート一覧表

ポート番号	TCP/UDP	サービス名	説明
20	TCP	ftp-data	File Transfer [Default Data]
21	TCP	ftp	File Transfer [Control]
23	TCP	telnet	Telnet
25	TCP	smtp	Simple Mail Transfer
53	TCP/UDP	domain	Domain Name Server
69	UDP	tftp	Trivial File Transfer
80	TCP	http	HTTP
110	TCP	pop3	Post Office Protocol - Version 3
143	TCP	Imap	Internet Message Access Protocol
161	UDP	Snmp	SNMP
443	TCP	https	HTTPS（SSL）

●アクセスリストの設定確認

■Router#**sh ip interface**

//

FastEthernet0 is up, line protocol is up
Internet address is 172.16.1.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is 100

■Router#**sh access-lists**

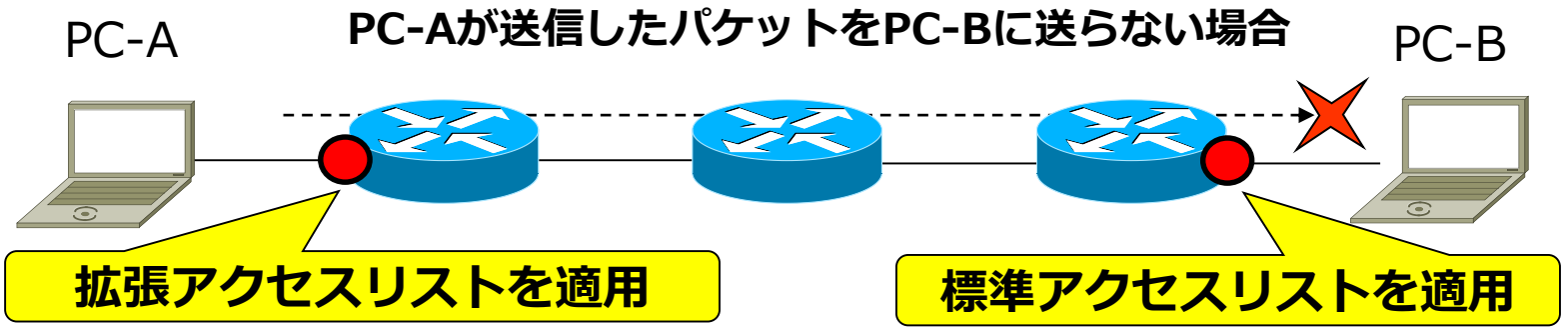
Extended IP access list 100
10 deny tcp host 172.16.1.1 host 192.168.1.1 eq www (9 matches)
20 permit ip any any (16 matches)

●アクセスリスト作成時の注意点

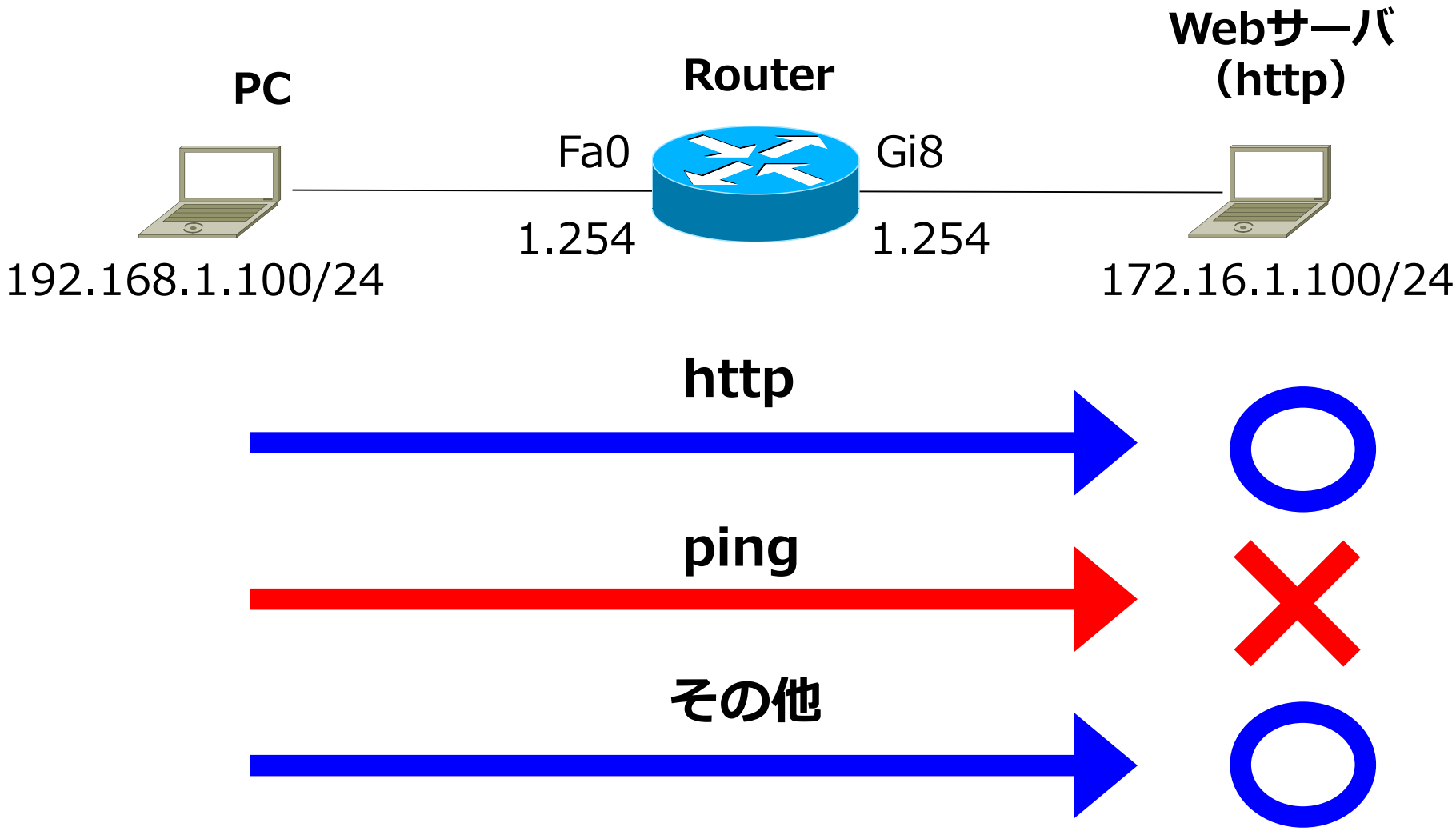
①作成するアクセスリストの「順番」
※特に、最終行の「**暗黙の deny any**」に注意

②作成するアクセスリストで使用する「番号」
※「標準」か「拡張」のどちらか

③作成したアクセスリストの適用場所
※要件によりますが、**標準＝宛先近く**、**拡張＝送信元近く**、で適用

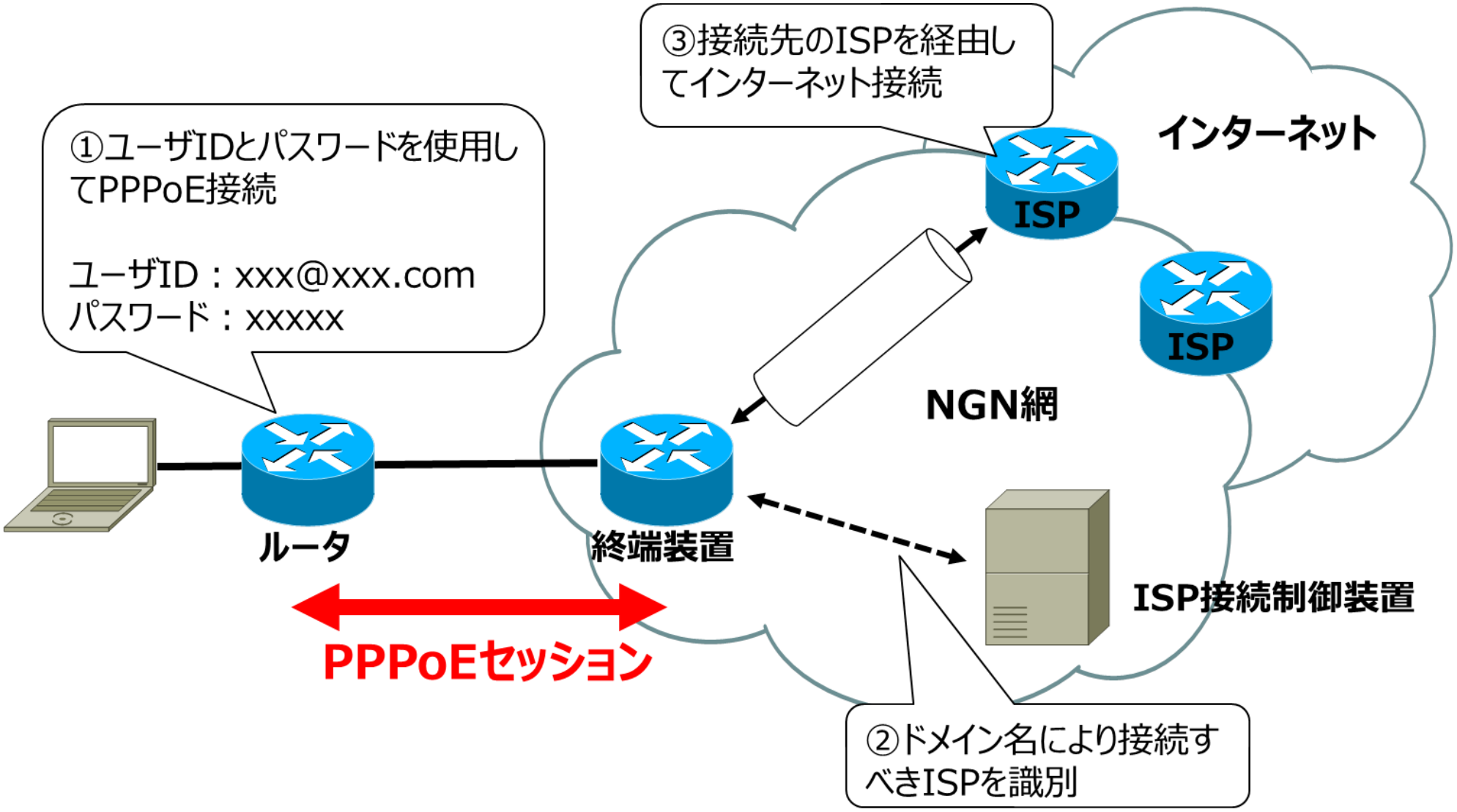


●ACL（演習）


PC
Router
Webサーバ
（http）
Fa0
Gi8
1.254
1.254
192.168.1.100/24
172.16.1.100/24
http
ping
その他

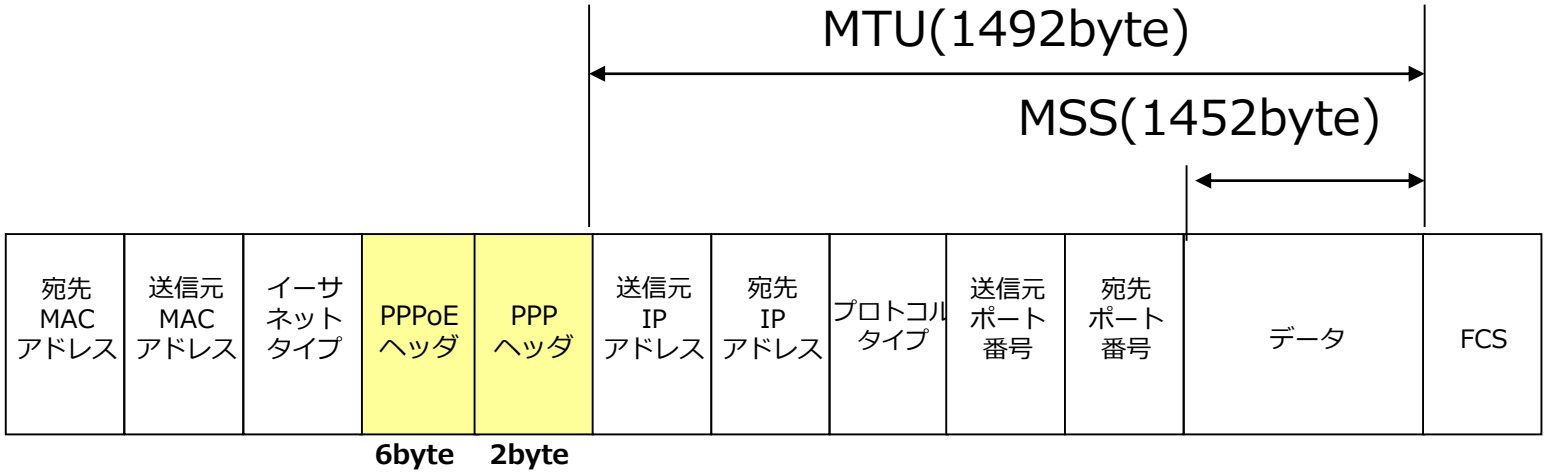
第6章
インターネット接続技術

●PPP/PPPoE

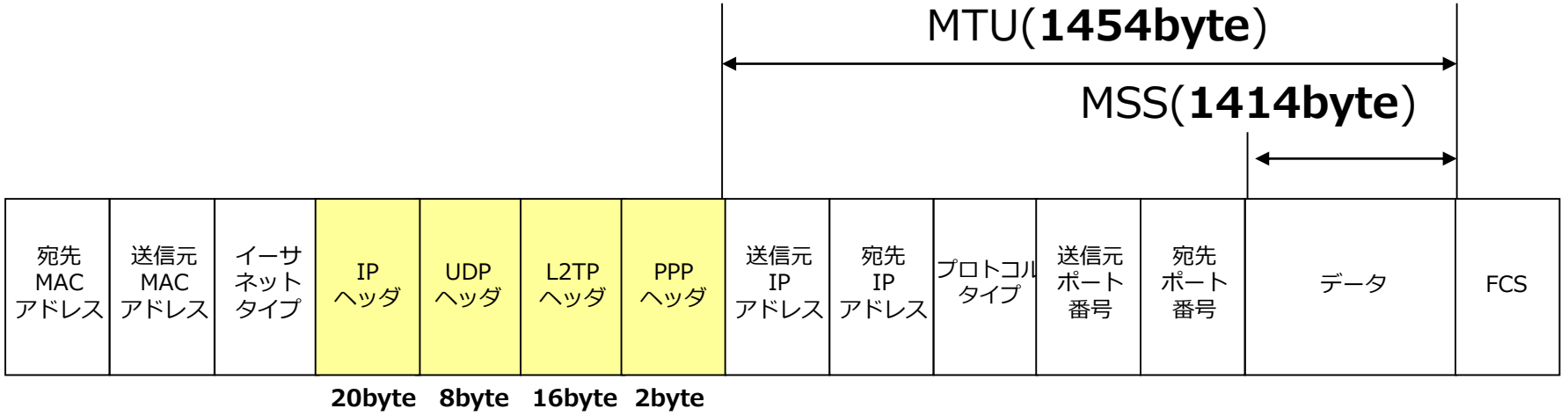

③接続先のISPを経由してインターネット接続
インターネット
①ユーザIDとパスワードを使用してPPPoE接続
ユーザID：xxx@xxx.com
パスワード：xxxxx
ISP
ISP
NGN網
ルータ
終端装置
ISP接続制御装置
PPPoEセッション
②ドメイン名により接続すべきISPを識別

●PPPoE/L2TP(NGN網内）フレーム

◆PPPoEフレーム

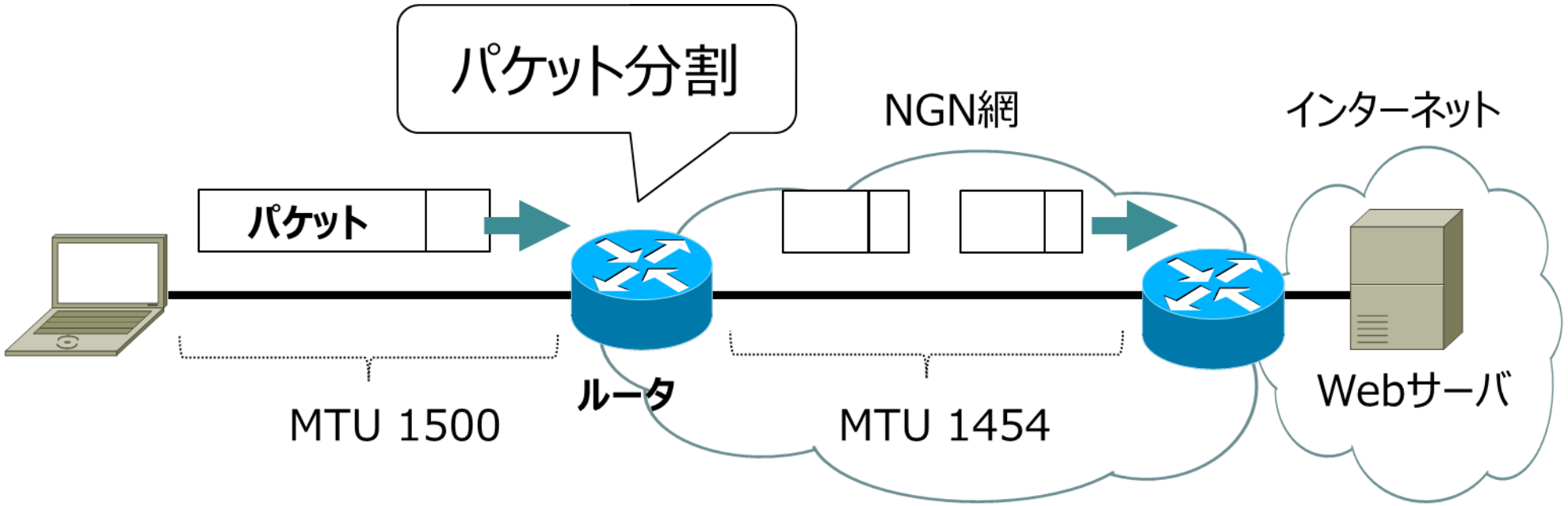


◆L2TPフレーム（NGN網内）



●フラグメント

パケットがルータを通過する際、送信先の伝送路のMTUサイズより
パケットのMTUサイズが大きい場合、**フラグメント（パケット分割）**
が発生する場合があります。



●Path MTU Discovery

■ Path MTU Discoveryの動作例

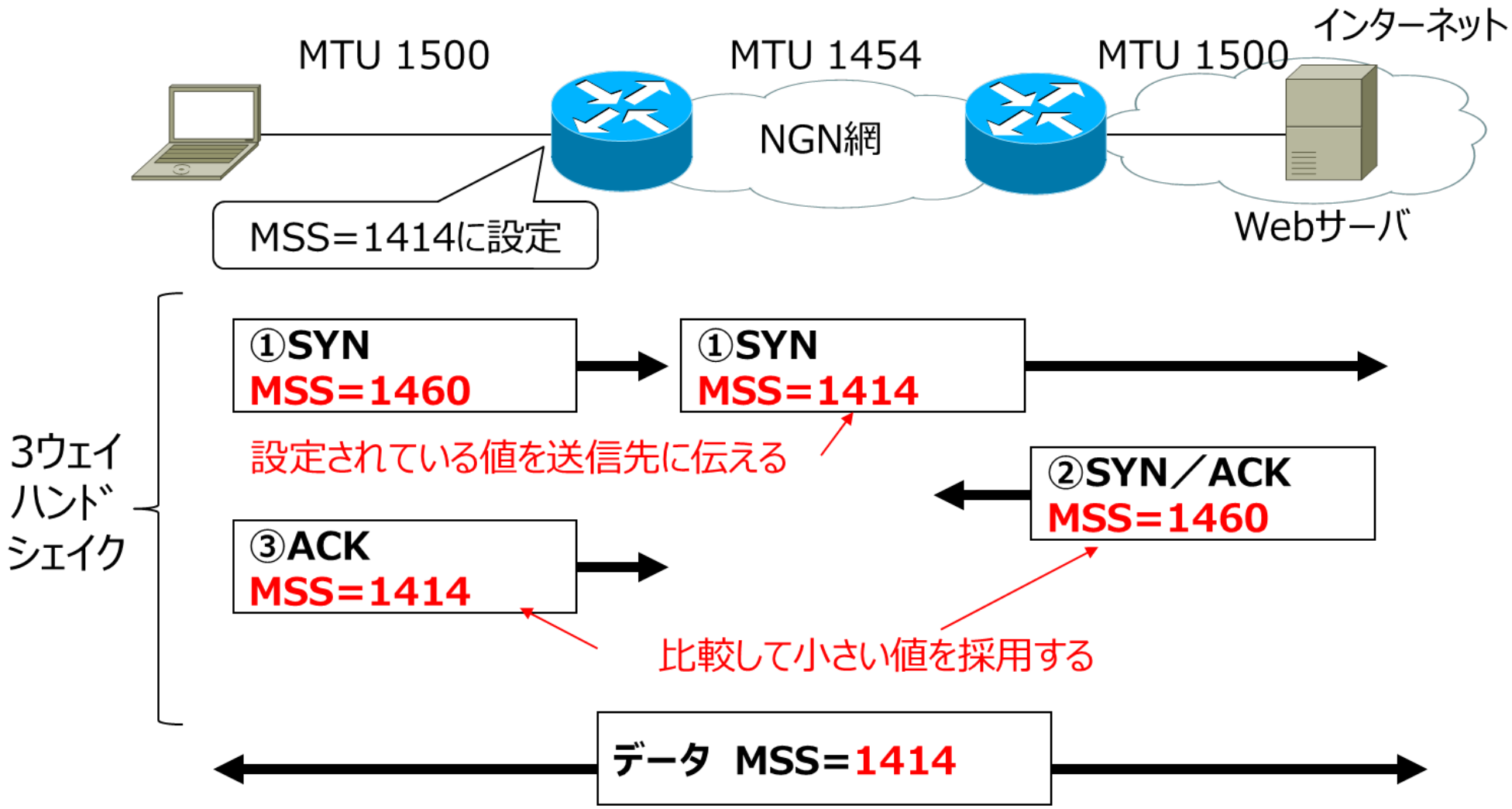
①ルータへ転送
DF=1　MTU=1500

②パケット破棄
DF=1のため分割できない

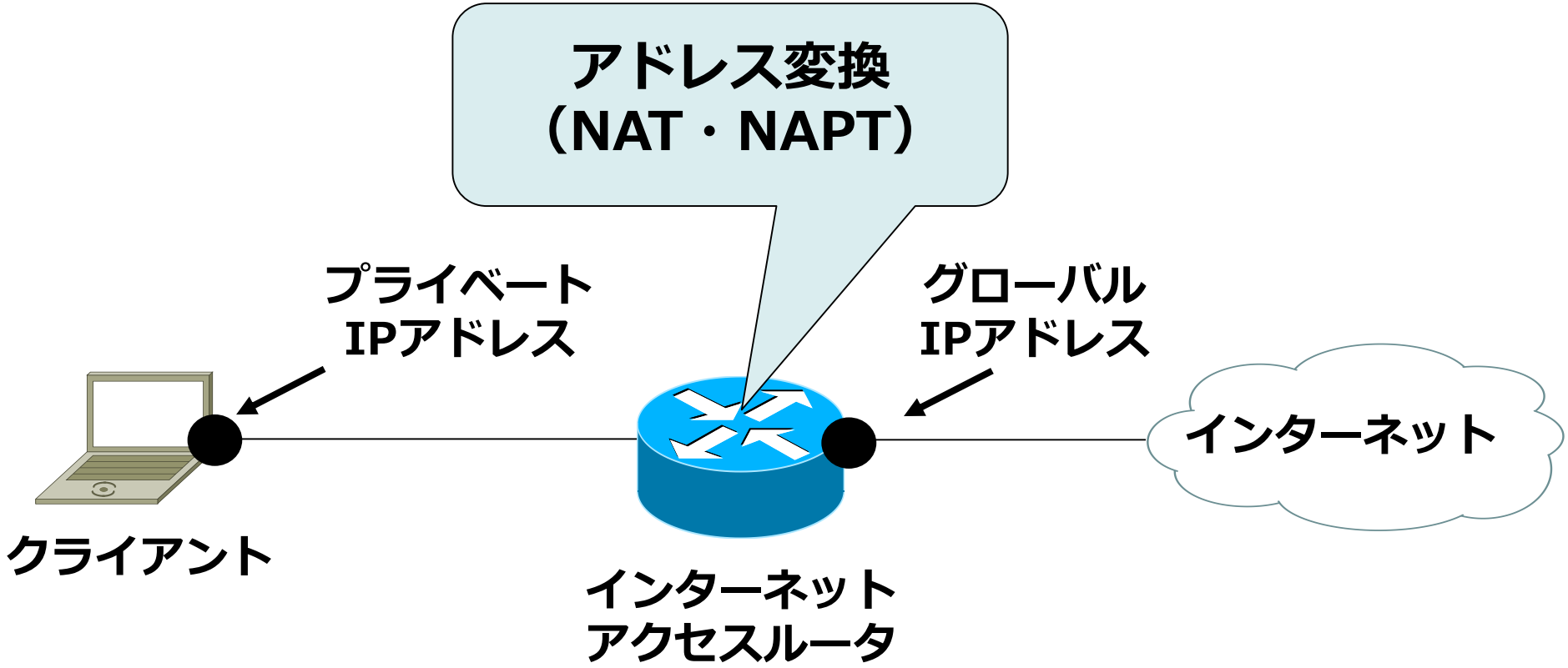
③ICMPによるエラー報告
Type=3　Code=4

④MTU変更・再送
DF=1　MTU=1454

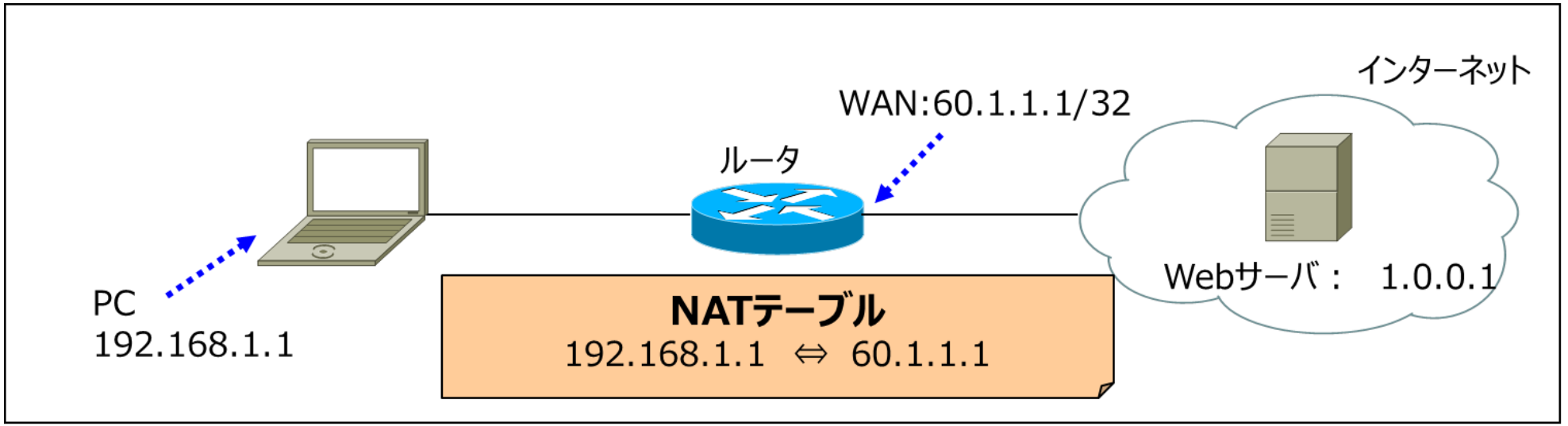
●3ウェイハンドシェイクによるMSS値の決定



●アドレス変換（NAT・NAPT）



●NAT（Network Address Translation）



【PC → サーバ】送るIPヘッダの中身

宛先IP	送信元IP
1.0.0.1	192.168.1.1

⇒

宛先IP	送信元IP
1.0.0.1	60.1.1.1

【サーバ → PC】送られてきたIPヘッダの中身

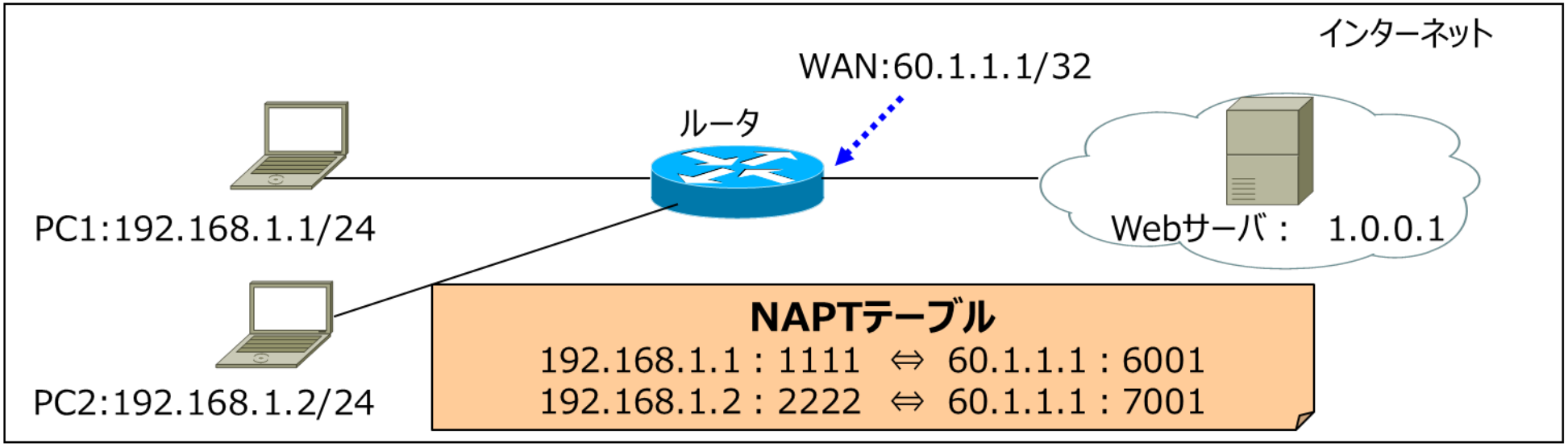
宛先IP	送信元IP
192.168.1.1	1.0.0.1

⇐

宛先IP	送信元IP
60.1.1.1	1.0.0.1

⇒ ルータを通過する際に、1対1のNATテーブルを作成します。
⇐ NATテーブルを参照し、IPヘッダを変換します。

●NAPT（Network Address Port Translation）



【PC1 → サーバ】送るIPヘッダの中身

宛先IP	宛先Port	送信元IP	送信元Port
1.0.0.1	80	192.168.1.1	1111

⇒

宛先ＩＰ	宛先Port	送信元IP	送信元Port
1.0.0.1	80	60.1.1.1	6001

【サーバ → PC1】送られてきたIPヘッダの中身

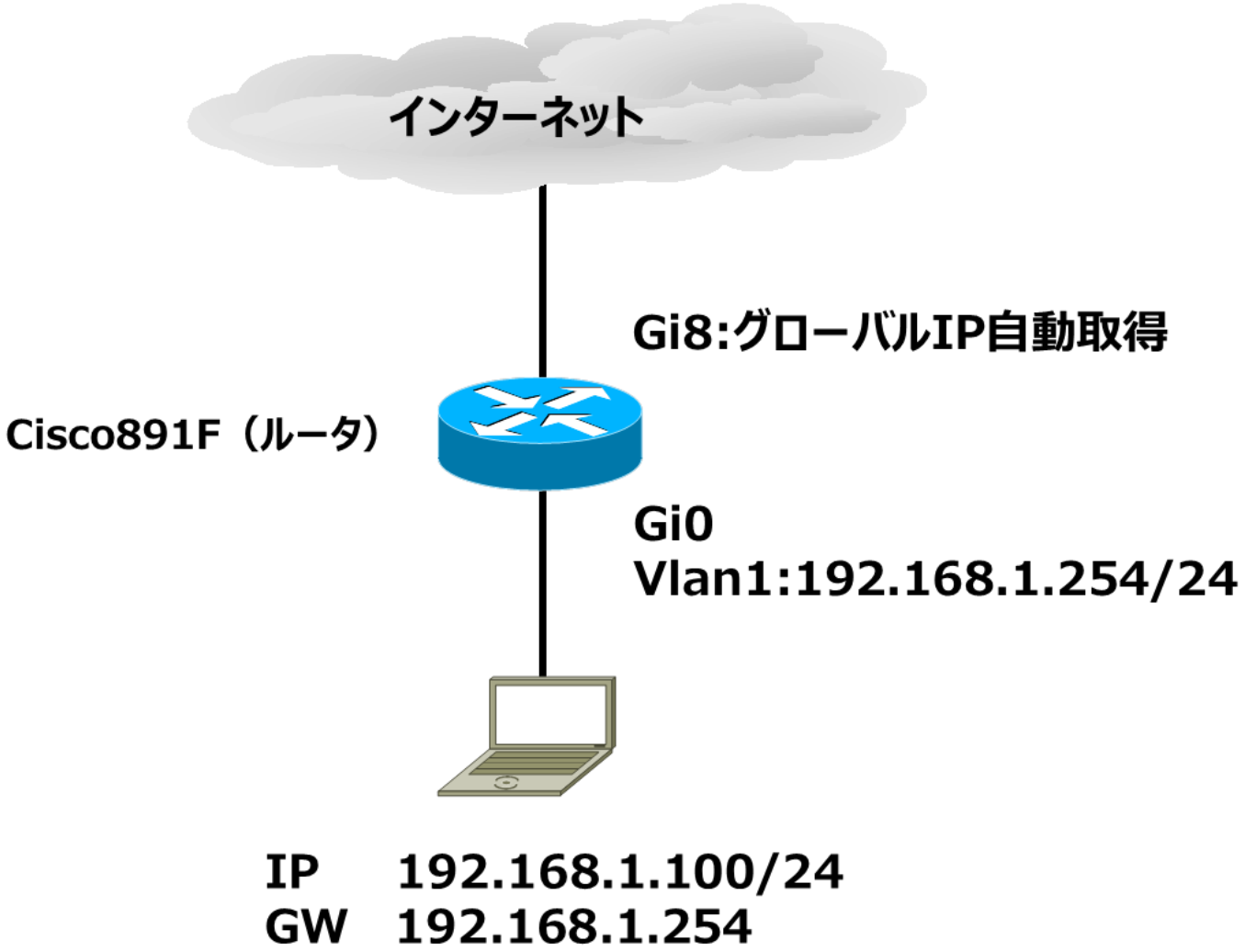
宛先IP	宛先Port	送信元IP	送信元Port
192.168.1.1	1111	1.0.0.1	80

⇐

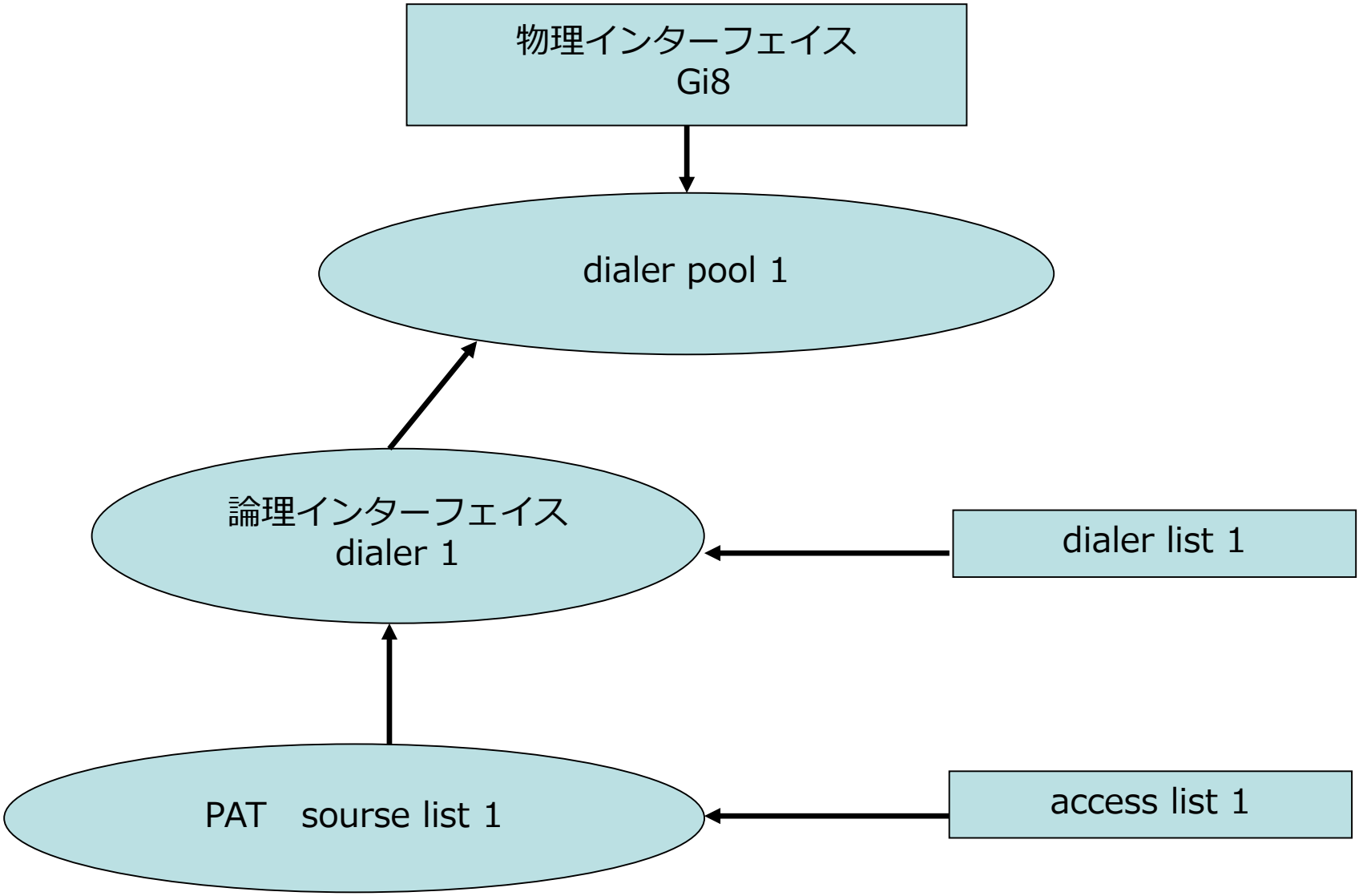
宛先IP	宛先Port	送信元IP	送信元Port
60.1.1.1	6001	1.0.0.1	80

IPアドレス変換にポート番号も含めて変換することで、
複数の端末を同時接続させることができる

●PPPoE接続(演習)


インターネット
Gi8:グローバルIP自動取得
Cisco891F（ルータ）
Gi0
Vlan1:192.168.1.254/24
IP　192.168.1.100/24
GW　192.168.1.254

●dialerインタフェースのコンポーネント



Cisco891F　マスカレードNAT　設定コマンド解説

※テキスト参照

Cisco891F　マスカレードNAT　設定コマンド解説

※テキスト参照