



SMBプロダクトWebセミナー

デザイン・設定ノウハウ
-L3スイッチ編



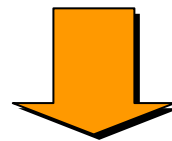
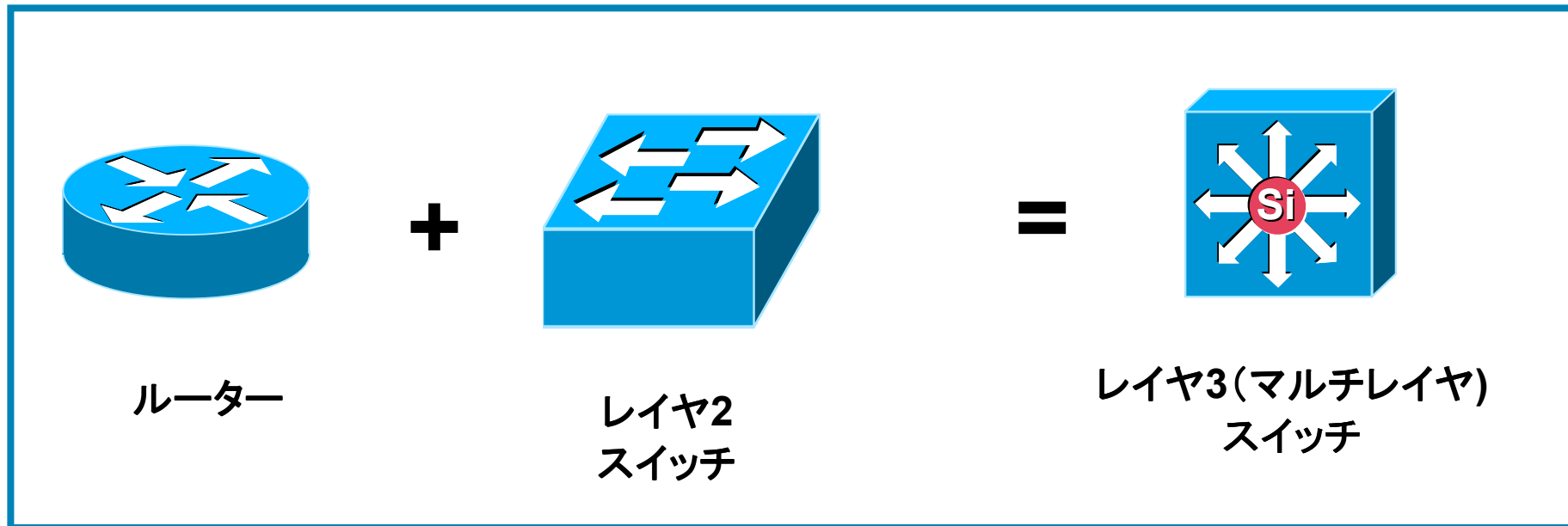
09/03/11

シスコシステムズ合同会社

Agenda

1. レイヤ3スイッチって？
2. レイヤ3スイッチを使ったキャンパスデザインのコツ
3. レイヤ3スイッチの設定
4. まとめ
5. 補足資料（コマンドによる設定）

1.1 レイヤー3スイッチって何？



ルーターしかできなかったレイヤ3（ネットワーク層）以上の機能とスイッチングハブのポート密度を合せ持った装置

1.2 ルーターとレイヤ3スイッチの違いは？

	ルーター	レイヤ2スイッチ	レイヤ3スイッチ
物理ポート数	少ない	多い	多い
VLAN	対応 (サブインターフェース)	対応	対応
ルーティング	可	不可	可
ダイナミックルーティングプロトコル	可	不可	可
パケット転送	CPU 処理	ハードウェア処理 (レイヤ2フレーム)	ハードウェア処理 (IP パケット)

2009年3月現在、シスコの製品では下記のようなレイヤ3スイッチがあります

- Catalyst 6500 シリーズ
- Catalyst 4500 SupervisorEngine 2*・4・5・6E シリーズ
- Catalyst 3750 シリーズ
- Catalyst 3560 シリーズ



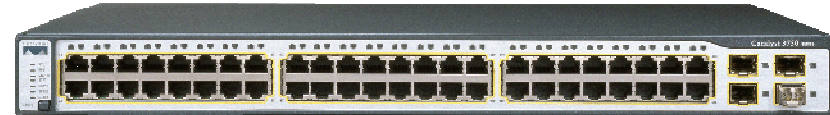
<http://www.cisco.com/web/JP/product/hs/switches/index.html>

* Catalyst4500 SUP2 は限定的なレイヤ3機能となります

1.3 レイヤ3スイッチの機能



Catalyst 3560-24PS

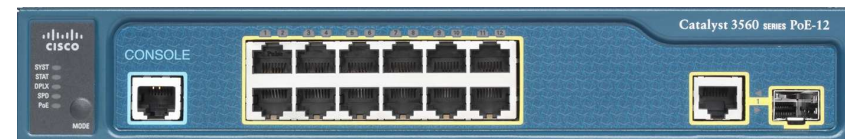


Catalyst 3750-48TS

- ✓ 多数のポートを持ち、ユーザの端末を集約できる
- ✓ VLAN 機能を持ち、論理的なネットワーク分割ができる。ネットワークの物理構成をシンプルにできる
- ✓ セグメント分けによる、安全な LAN を構築できる
- ✓ IP ルーティングができる
- ✓ 転送などの機能をハードウェア (TCAM) で高速処理。ノンブロッキング (ワイヤーレート) 転送が可能に



Catalyst 3560-8PC



Catalyst 3560-12PC



2. レイヤ3スイッチを使った LAN デザイン



2.1 レイヤ3スイッチの機能- VLAN 間ルーティング

VLAN (Virtual LAN) は、ブロードキャストドメインを論理的に分割する技術

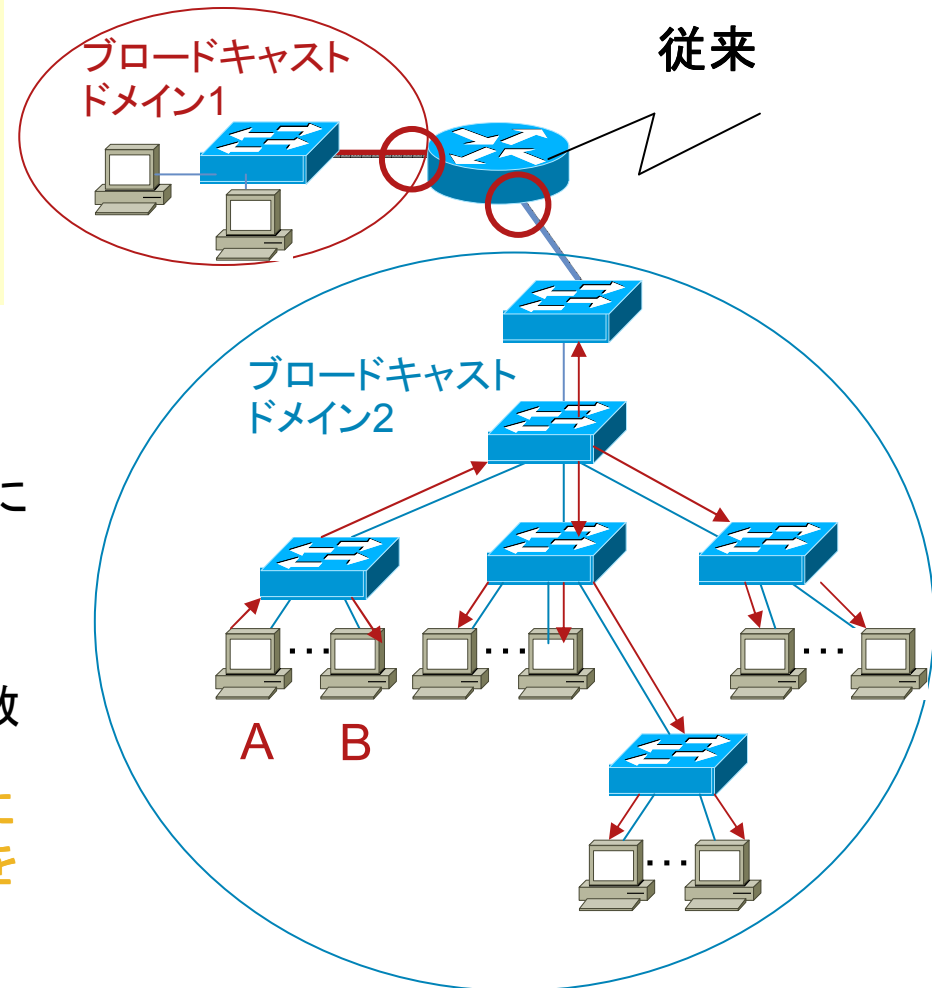
ブロードキャストドメインとは

- ▶ 同一の IP サブネットに所属するドメイン
- ▶ ドメイン内ではマルチキャスト・ブロードキャストパケットが伝播する
= ネットワーク全体のパフォーマンスに影響する

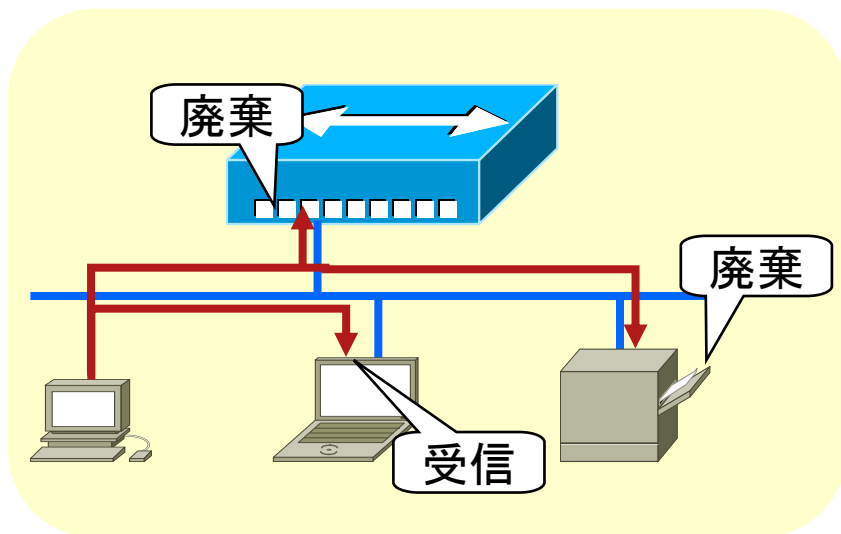


LAN 内では、ブロードキャストドメインを適切に分割しなければならない

ルータでは・・・分割できるブロードキャストドメインの数がルータの物理ポートの数に依存してしまう
一方スイッチは **VLAN** と物理ポート数により、より多くのブロードキャストドメインを自由に作ることができる

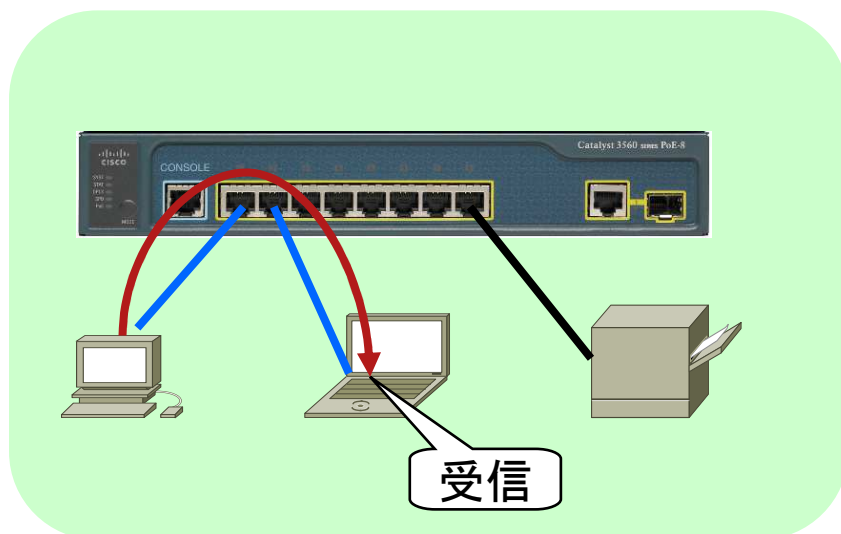


2.2 ハブとスイッチの違い



スイッチングハブの場合

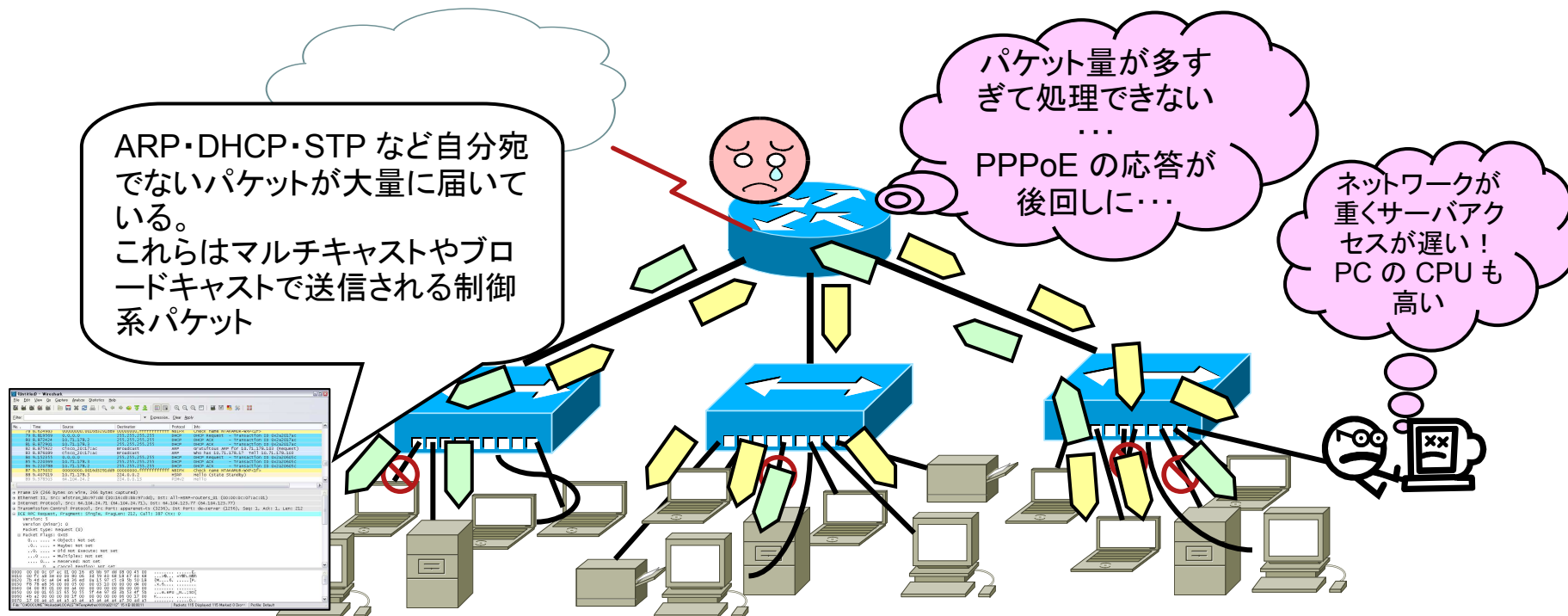
- ブロードキャストドメインの分割ができない
→ 不要なフレームが全てのノードに届き、端末側で処理/廃棄されている
- すべてのポートが同一の銅線上に接続されている状態と同じ
→ 帯域幅も共有
- アクセス制限不可
→ 盗聴される可能性も



L2/3 スwitchの場合

- レイヤ2レベルで、必要なポートにだけ転送
→ 帯域の有効利用
- VLAN 機能でブロードキャストドメインを分割
→ 同ドメイン内のみでフラッド(ブロードキャストパケット・マルチキャストパケット)
- アクセスリストによる制限可能
→ 不正な通信をさせない・盗聴させない

2.3 ルータ+ハブのネットワークのデメリット



ハブを使った LAN では、理論上 255 台までの端末を接続することができますが、ルータでの処理負荷やネットワーク上の帯域の有効化の観点から、多くの端末を接続することは望ましくありません

一つのサブネットに收容される端末数は、50台以内が理想的。
それを越える場合は、L3 スイッチを適切にご提案ください

2.4 レイヤ3スイッチを使った LAN デザイン

シスコでは継続的なネットワークへの要求に応えるため、**モジュラーデザイン**を推奨しています

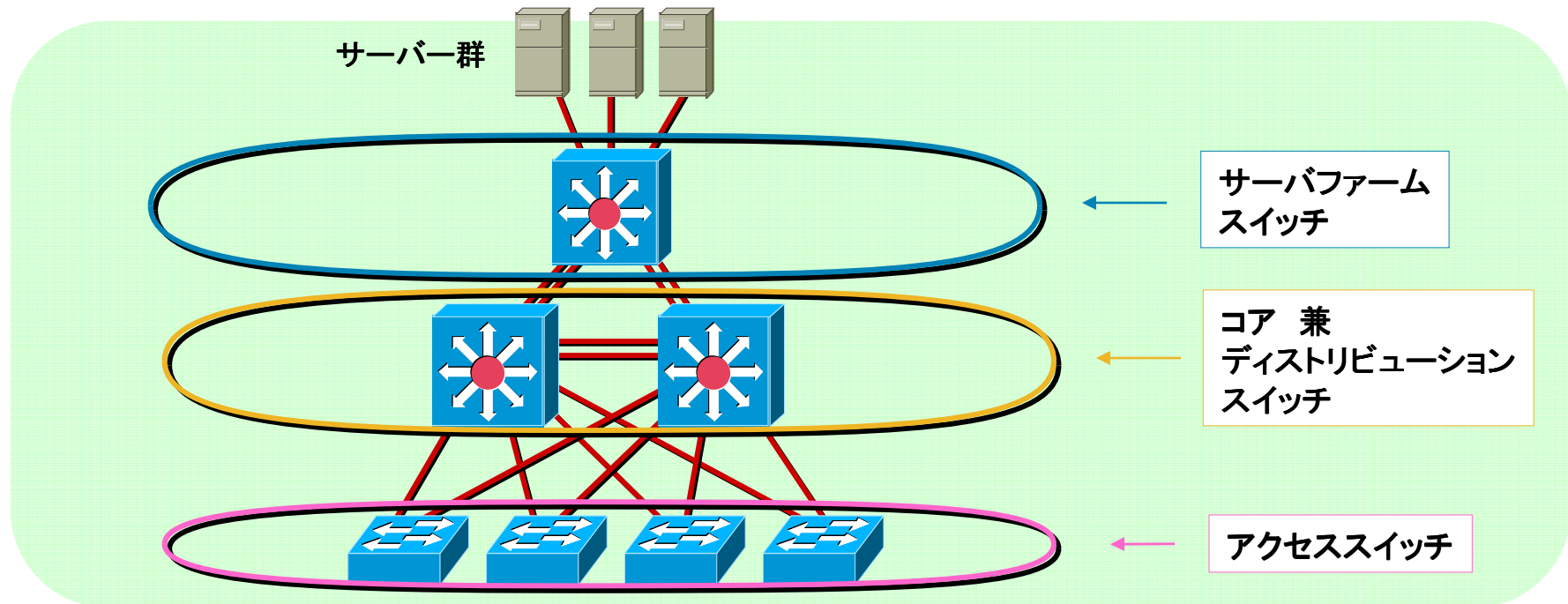
モジュラーデザインとは…

ネットワーク全体を3つのレイヤに分け、各レイヤごとに機能を分離させる階層化型ネットワークデザイン手法

モジュラーデザインのメリット

- ✓ 拡張性があり、将来のネットワーク拡張が容易
- ✓ 故障発生時に、故障個所の特定が容易
- ✓ トラブルをモジュール内に限定することができる
- ✓ ネットワーク上のトラフィックを分散しやすい(負荷分散)

2.5 可用性の高いネットワークデザイン例



3つのレイヤ区分と役割

コアレイヤ(バックボーン)

: 社内全体を束ねるネットワーク

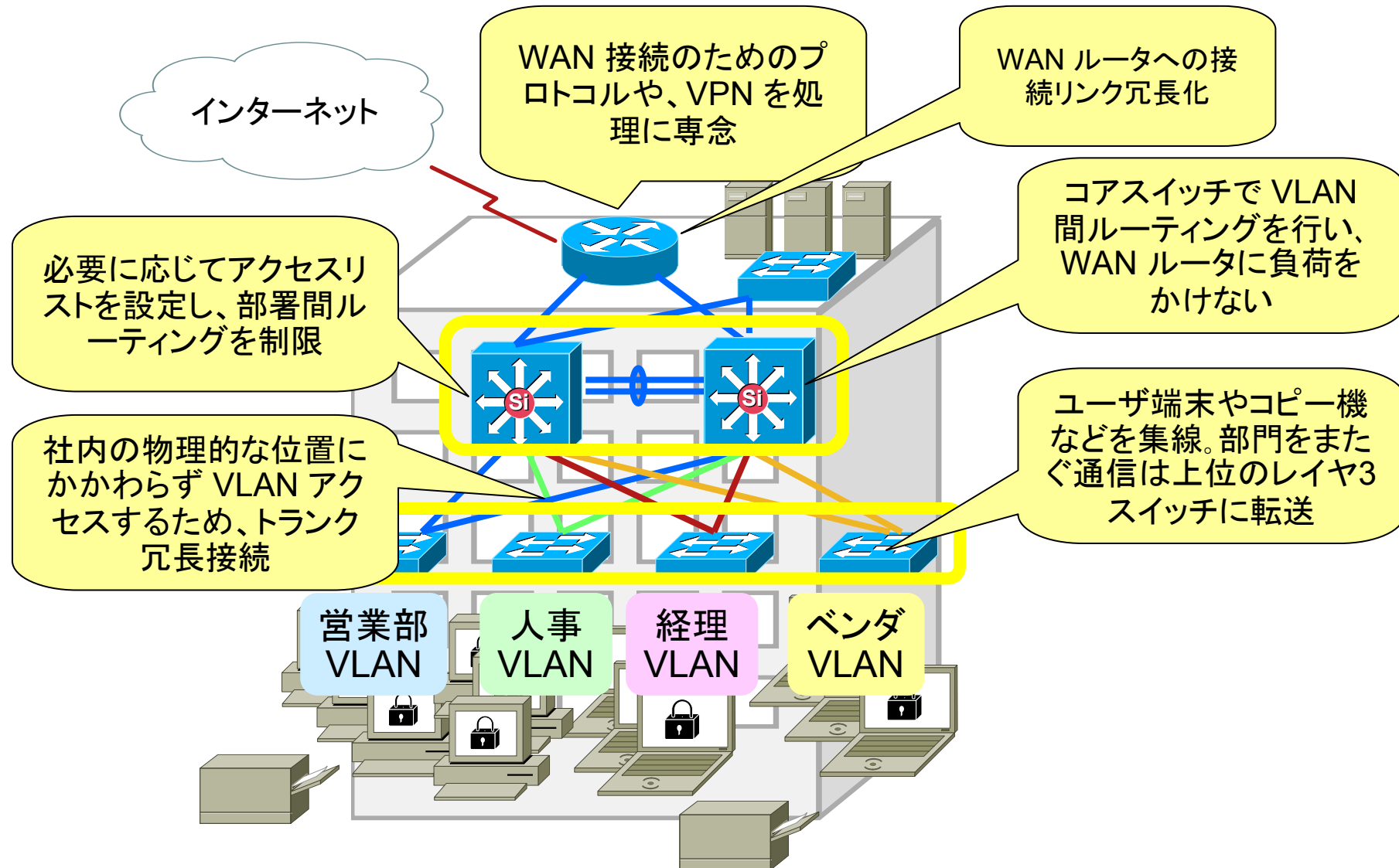
ディストリビューションレイヤ

: ブロック(建物など)内を束ねるネットワーク

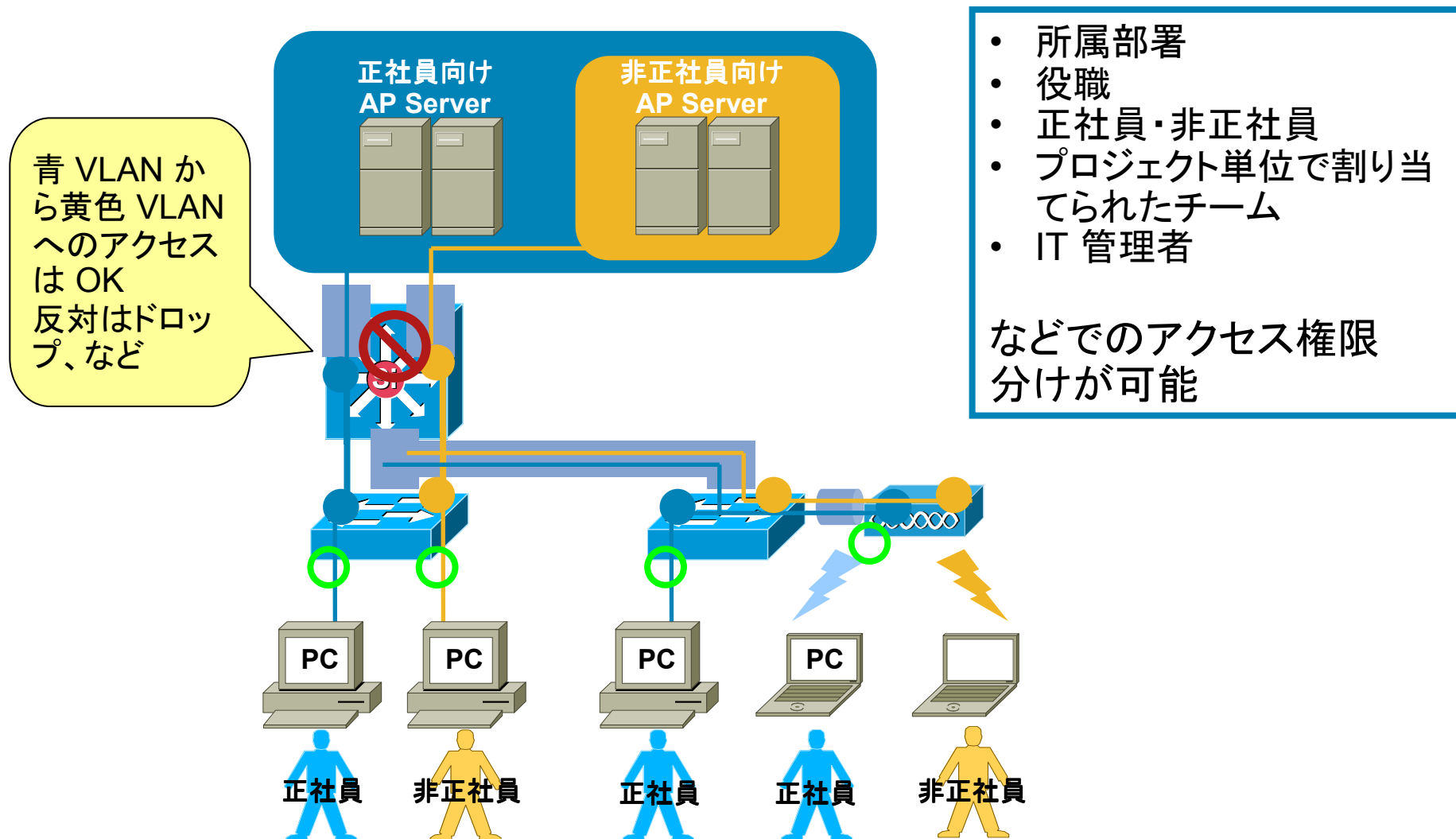
アクセスレイヤ

: 実際のユーザ PC を束ねるネットワーク

2.6 レイヤ3スイッチを使ったデザインのポイント



2.7 VLAN を使ったアクセスイメージ



2.8 簡単ソリューションパック

基本的な構成のネットワークをスピーディに導入するため、“簡単ソリューションパック”としてご用意しております



基本インフラ ソリューション
各種拡張ソリューション導入時の基本となるネットワークをご提供します。

対象企業規模：100人以下
対象製品：シスコルータ 800 シリーズ/ 1812J
シスコカタリスト LAN スイッチ 2960 シリーズ/ 3560 シリーズ

問題点

- ・ 事務所を移転するけれど、新しいネットワーク インフラはどうしたらいいだろう…
- ・ ユーザが勝手にハブをつないでトラブルが多発している…
- ・ 家庭用のネットワーク機器ではなく、ビジネスで使えるインフラが欲しい…
- ・ 現状のインフラ、セキュリティは万全？
- ・ 将来必要な拡張可能な構成のインフラが欲しい…

既存のルータ・スイッチをアップグレードしたり、新規にネットワークを設置する場合の基本ソリューション



ソリューション

- ・ オフィスの規模別を選ぶ標準構成
- ・ 世界で鍛えられた運用性
- ・ 充実したセキュリティ機能
- ・ 将来のセキュリティ強化やIP電話導入にも対応
- ・ 実環境で高速、安全
- ・ 移行や追加に柔軟に対応でき、投資を無駄にしない

シスコルータ

ルータで回線と接続。ルータ・スイッチはVPNでリモートメンテナンス。

インターネット

シスコカタリスト LAN スイッチ

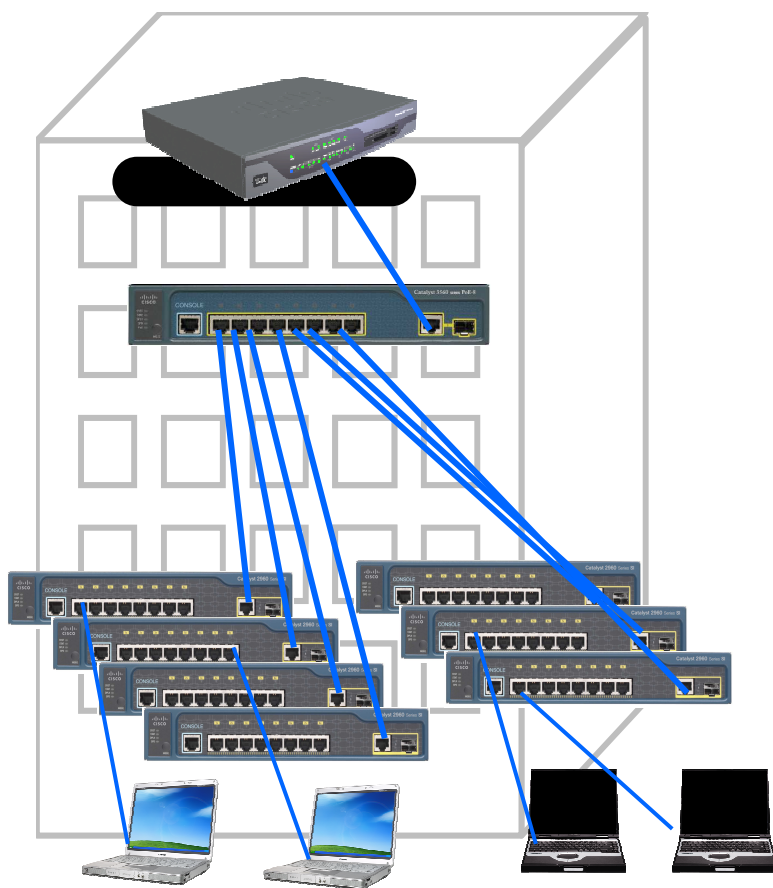
シスコカタリスト LAN スイッチ

LAN スイッチでPCを接続するのに必要なポート数を確保。さらにスイッチのセキュリティ機能で、接続できる端末を制限。トラブルを未然に防ぐための各種機能を利用。

他の事務所とVPNにて接続。

2.8 簡単ソリューションパック (cont.)

例えば、ユーザ数50名規模のオフィスの場合・・・



20～50人のオフィス

		製品型番	製品説明	単価	個数	DIS標準価格	備考
ルータ	本体	CISCO 881-K9		¥78,840	1	¥78,840	*1
	ライセンス	SL-880-AIS		¥18,240	1	¥18,240	
	保守	CON-SNT-C881	スマートネット 8x5x 翌営業日配送※	¥5,760	1	¥5,760	
	合計					¥102,840	
コア スイッチ	本体	WS-C3560-8PC-S	レイヤー3 コンパクトスイッチ	¥169,440	1	¥169,440	
	保守	CON-SNT-WSC3568	スマートネット 8x5x 翌営業日配送※	¥10,680	1	¥10,680	
	合計					¥180,120	
エッジ スイッチ	本体	WS-C2960-8TC-S	レイヤー2 コンパクトスイッチ	¥96,600	7	¥676,200	
	保守	CON-SNT-2968TCS	スマートネット 8x5x 翌営業日配送※	¥6,120	7	¥42,840	
	合計					¥719,040	
総合計						¥1,002,000	

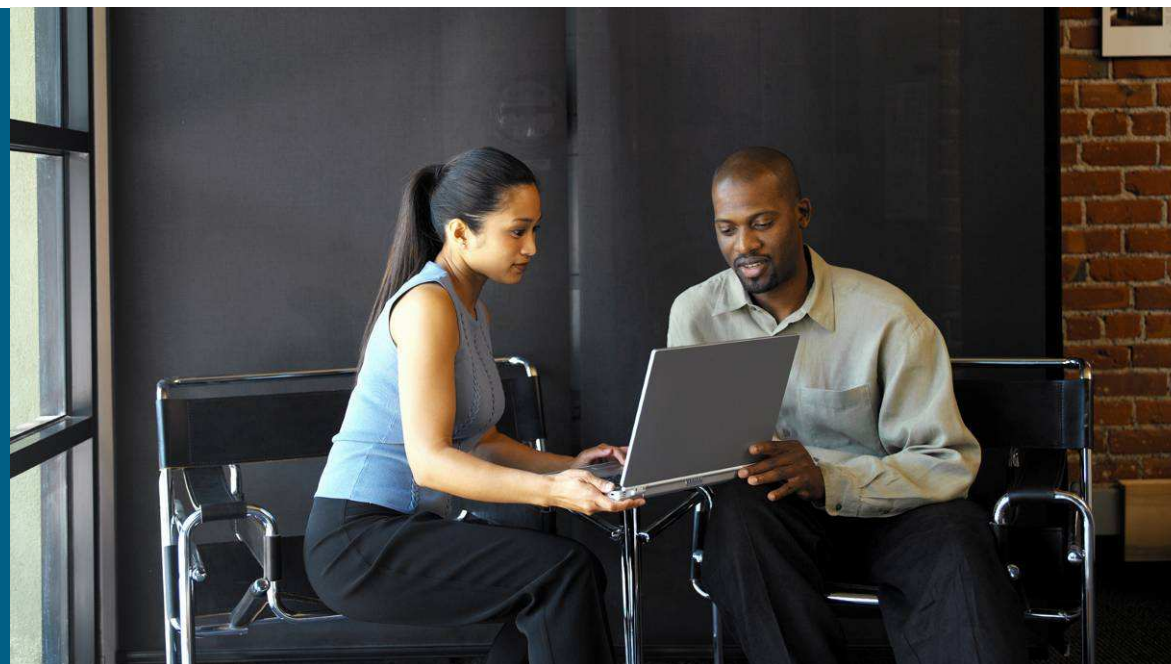
シスコキャピタル クイックリースをご利用いただいた場合、3年の残価設定型で、月々27,800円（リース総額 1,000,800円）

シスコなら！💡

最小 8ポートモデルからの充実のレイヤ3スイッチラインナップ（8・12・24・48ポート）

中小規模のコア兼ディストリビューションスイッチに最適！

3. レイヤ3スイッチ の設定



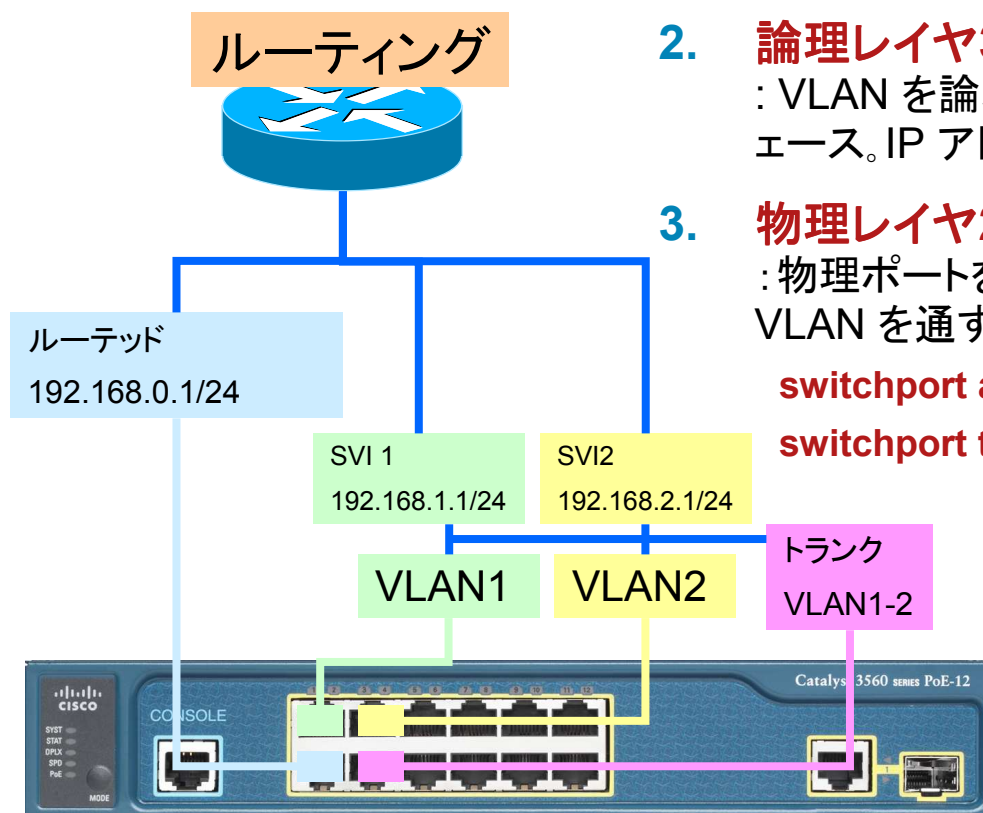
3.1 レイヤ3スイッチの構造

レイヤ3スイッチでは、VLAN を利用したサブネット間通信をサポートするため、下記の3つのインターフェースモードを使い分けます

1. **物理レイヤ3インターフェース (ルーテッドモード)**
: ルーターと同じく、1ポート=1サブネットとし IP アドレスを持つ
2. **論理レイヤ3インターフェース (SVI モード)**
: VLAN を論理セグメントとするために作成する論理インターフェース。IP アドレスを持つ
3. **物理レイヤ2インターフェース (Switchport モード)**
: 物理ポートを VLAN に割り当てるアクセスポートと、複数の VLAN を通す Trunk モードがある。

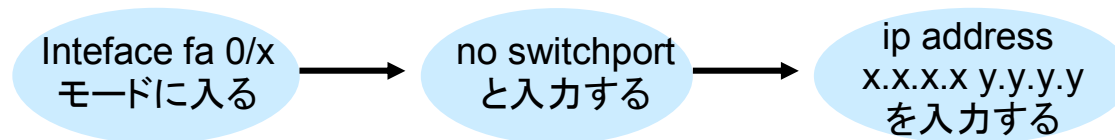
switchport access モード: 単一の VLAN に所属させる

switchport trunk モード: 複数の VLAN トラフィックを通す



3.2 CLI による設定手順

1. ルーテッドインターフェースの設定手順

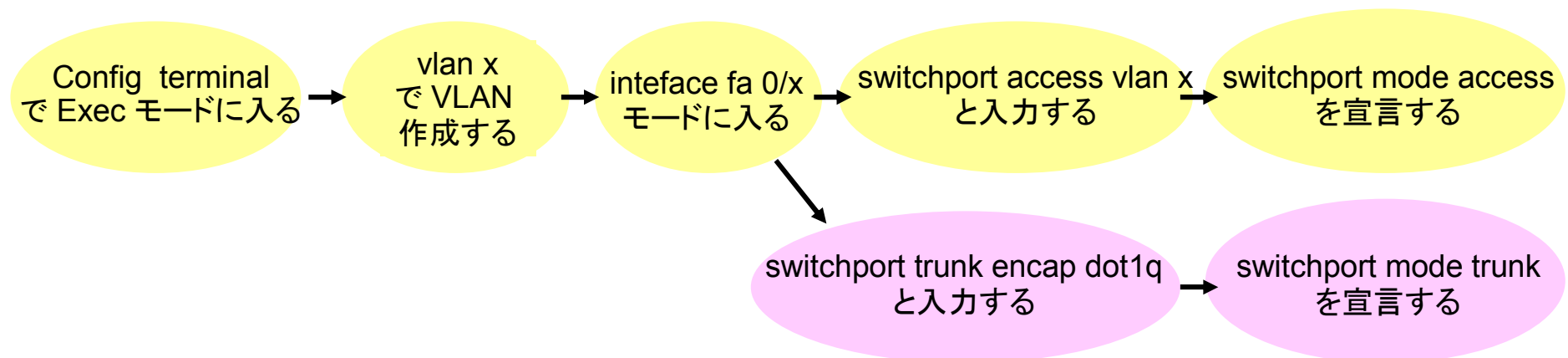


詳細は補足資料のコマンド
解説をご覧ください

2. SVI (Switch Virtual Interface) の設定手順



3. Switchport の設定手順

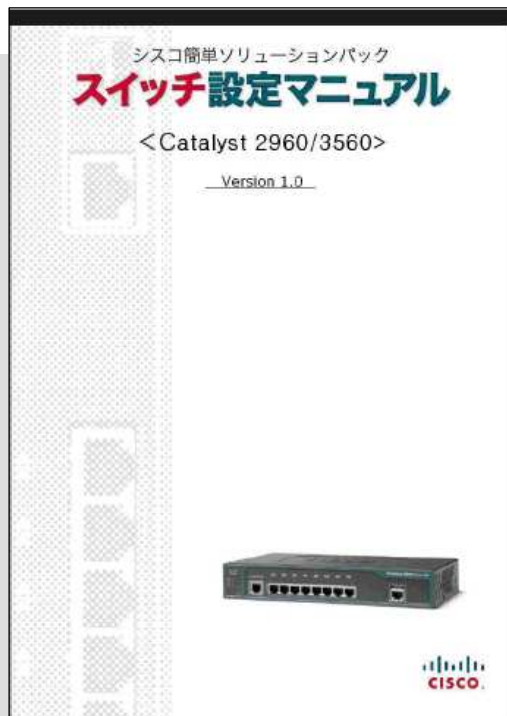


3.3 GUI による設定

- GUI ツールでの設定方法

→ 簡単ソリューションパッケージガイドをご覧ください

http://www.cisco.com/web/JP/partners/pec/smbp/kantan_manual_switch.pdf



第 4 章 レイヤ3 スイッチの設定 (Catalyst 3560 シリーズ)
4.1 VLAN の概要
4.2 VLAN 作成およびポートへの割り当て
4.3 VLAN インターフェイスへの IP アドレス設定
4.4 ルーティング設定

4. まとめ

- レイヤ3スイッチとは、ルーターの機能を持ち、かつポート密度の高いスイッチ
- VLAN 機能を使って、ネットワークのセグメント化ができる。かつ、レイヤ3スイッチで VLAN 間のルーティングおよびアクセス制御ができる
- 目安として、50台以上の端末を接続するような LAN 環境では、レイヤ3スイッチでの階層化が非常に有効になる
- WAN (インターネット) 接続ルータには、出来るだけ余計な負荷をかけず、WAN 接続に専念させることが望ましい
- すべての端末がスイッチングハブに接続されているようなネットワークは、不要なパケットが常に全体に流れ、トラフィックが溢れやすい環境

レイヤ3スイッチの導入により、安全で拡張性のある
堅牢なネットワークを構築することができます

リファレンス

- 簡単ソリューションパック・ウェブセミナー (要 Cisco.com ログイン)

http://www.cisco.com/web/JP/event/tra_ccc/ccc/pec/smbp.html



2008年11月26日	シスコ簡単ソリューションパック - セキュリティ設定マニュアル紹介	技術向け	WebEX記録(28:56) PDF 設定マニュアル
2008年11月19日	Aironet 簡単設定マニュアル	技術向け	WebEX記録(23:52) PDF
2008年11月12日	シスコ簡単ソリューションパック - スイッチ設定マニュアル紹介	技術向け	WebEX記録(30:28) PDF 設定マニュアル
2008年11月5日	シスコ簡単ソリューションパック - ルータ設定マニュアル紹介	技術向け	WebEX記録(26:37) PDF 設定マニュアル
2008年10月29日	シスコ簡単ソリューションパック - 営業向けセミナー	営業・技術向け	WebEX記録(35:14) PDF

- シスコ技術者認定トレーニング(集合型・有料)

ICND v2

http://www.cisco.com/web/JP/event/tra_ccc/ccc/certprog/testing/current_exams/640-816.html

補足資料

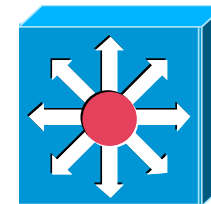


□ レイヤ3スイッチ設定コマンド集

物理ポート設定

基本設定 3 項目

- Speed (10/100/1000)
- Duplex (half, full, auto)
- Status (shutdown, no shutdown)



```
Switch(config-if)#speed
```

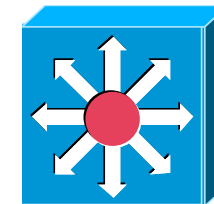
```
Switch(config-if)#duplex
```

```
Switch(config-if)#no shutdown
```

- * ポートの設定パラメータ(speed, duplex)はスイッチの機種で異なります。
- * デフォルトのポート設定も機種によって異なります。

物理ポート設定

Supervisor IOS は
L2 + L3 の機能を統合したOSです。
そのため、物理インターフェースに
直接IPアドレスの指定が可能です。



L2設定を行う場合には
switchport
と設定しなければVLANの割り当て、Trunk設定は受け付けません。

ポートを **Layer 2** として設定

```
Switch(config-if)# switchport
```

ポートを **Layer 3** として設定

```
Switch(config-if)# no switchport
```

- * 機種によってデフォルトのポート設定が異なります。
- * L3機能を含んでいないSwitch でこのコマンドはサポートされていません。

設定確認

- 設定確認 -

```
Switch#show interfaces <interface-number>
```

```
Switch#show interfaces status
```

Switch#show interfaces status

Port	Name	Status	Vlan	Duplex	Speed	Type
Gi1/1		disabled	routed	full	1000	1000BaseSX
Gi1/2		disabled	routed	full	1000	No GBIC
Gi3/1	To-2960A_G0/3	connected	130	full	1000	1000BaseT
Gi3/2	To-2960A_G0/4	connected	130	full	1000	1000BaseT
Gi3/3	To-3750B_G0/3	connected	trunk	full	1000	1000BaseT
Gi3/4	To-3750B_G0/4	connected	trunk	full	1000	1000BaseT
Gi3/5		notconnect	routed	full	1000	1000BaseT
Gi3/6		notconnect	routed	full	1000	1000BaseT

ポートの名前

shut or
no shut?

L2port or
L3 port??

* Cat6500 での表示画面です

VLAN の作成

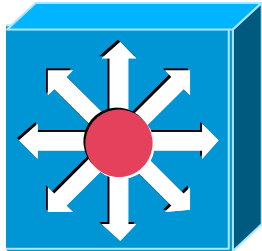
- グローバルコンフィグレーションモードから作成(Sup IOS)

```
Switch(config)#vlan <vlan-id>
```

VLANを作成、または追加する

```
Switch(config-vlan)#name <name>
```

VLANの名前を設定(オプション)



VLAN ID のサポートについて

Normal VLAN ... 1 – 1005 まで(VTP 利用可)

Extended VLAN ... 1006 – 4096 まで(VTP 利用不可)

* VLANの中でも 1002-1005 は特定用途に予約されているため、一般的な VLAN に指定できません

Catalyst 6000/6500シリーズ ... 4000 VLAN ID

Catalyst 4500 シリーズ ... 4000 VLAN ID

Catalyst 3750 シリーズ ... 4000 VLAN ID

Catalyst 2960 シリーズ ... 4000 VLAN ID

* 同時に Active にできる VLAN 数については機種ごとに異なります。詳細は各機種のコンフィギュレーションガイド、リリースノート等を参照してください。

VLAN の設定確認

- 設定確認 -

```
Switch#show vlan (brief)
```

現在設定されているVLANが表示されます。

```
Switch#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	
129 NW-6506S-6509C	active	Gi1/1, Gi3/5, Gi4/16, Po1
130 NW-6506S-3750A	active	Po2
132 NW-6506S-3750B	active	Po3
134 NW-6506S-6506A	active	Gi4/6, Po4
138 NW-6506S-4006B	active	Gi4/9
1002 fddi-default	active	
1003 token-ring-default	active	

* 表示画面はCat6500のもので

VLAN Trunk (VLANタギング・タグVLAN) の設定

VLANの多重化

● カプセル化タイプ

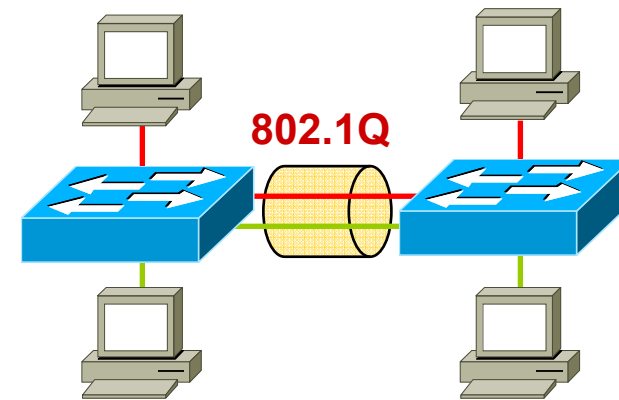
IEEE 802.1Q

* 一部の機種では、シスコ独自のプロトコル ISL にも対応

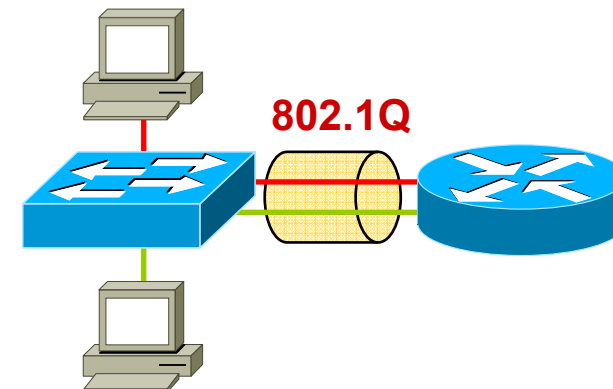
● Point-to-Point

Switch to Switch
Router to Switch

● Switch to Switch



● Router to Switch



Trunk ポートの設定方法

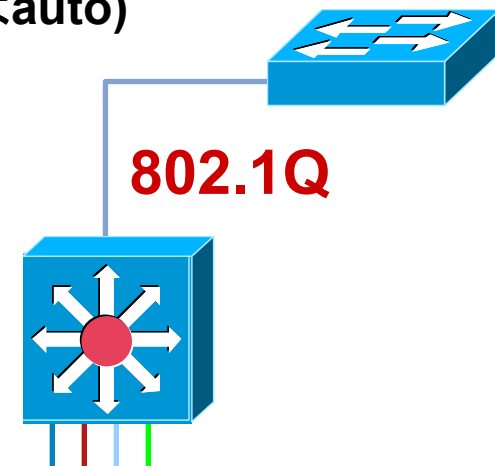
1. カプセル化タイプを指定します。

```
Switch(config-if)# switchport trunk encapsulation < dot1q / isl >
```

2. ポートのモードを静的にトランクに設定します。(デフォルトはauto)

```
Switch(config-if)# switchport mode trunk
```

- * 1、2 の順番に入れてください
- * ただし、2960では 2 のみ (802.1Q のみサポートのため)
- * DTP を完全に OFF にしたい場合は
mode trunk と併せて、**switchport nonegotiate** を入力してください。



Trunk allowed VLAN の設定

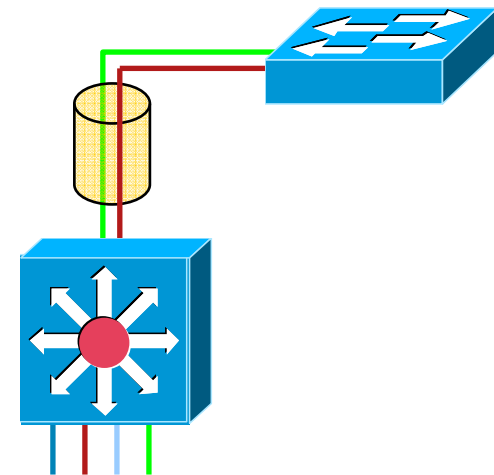
- Trunk の中を通すVLANを設定します。

```
Switch(config-if)#switchport trunk allowed vlan <vlan-number>
```

例: Switch(config-if)# switchport trunk allowed vlan 50-100, 200-250

- * allowed vlan を設定しなければデフォルトでは全部の VLAN がTrunk されます
- * この他にも add, remove 等のオプションを使用することが可能です。
- * 機種によってはトランクからVLAN 1(共通VLAN)を省略することができません。

→ この設定により、ブロードキャストドメインを小さくし余計なトラフィックを抑制することが可能



Trunk設定確認(1)

- 設定確認 -

```
Switch#show interfaces <interface> switchport
```

```
3750A#sh int gi 0/1 switchport
```

```
Name: Gi0/1
```

```
Switchport: Enabled
```

```
Administrative Mode: trunk
```

```
Operational Mode: trunk (member of bundle Po1)
```

```
Administrative Trunking Encapsulation: dot1q
```

```
Operational Trunking Encapsulation: dot1q
```

```
Negotiation of Trunking: Off
```

```
Access Mode VLAN: 1 (default)
```

```
Trunking Native Mode VLAN: 1 (default)
```

```
Trunking VLANs Enabled: 1,192-223,1002-1005
```

```
Pruning VLANs Enabled: 2-1001
```

* 表示画面はCat3750のものです

Trunk設定確認(2)

- 設定確認 -

```
Switch#show interfaces trunk
```

```
3750B#sh int trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Gi0/7	on	802.1q	trunking	1
Gi0/8	on	802.1q	trunking	1
Po1	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Gi0/7	1,192-223,1002-1005
Gi0/8	1,192-223,1002-1005
Po1	1,192-223,1002-1005

Port	Vlans allowed and active in management domain
Gi0/7	1,192-193,196,198,223
Gi0/8	1,192-193,196,198,223
Po1	1,192-193,196,198,223

Port	Vlans in spanning tree forwarding state and not pruned
Gi0/7	1,192-193,196,198,223
Gi0/8	1,192-193,196,198,223
Po1	1,192-193,196,198,223

* 表示画面はCat3750のものです

アクセスポートへの VLAN のマッピング

- ポートを1つの VLAN のみに設定するためには、下記の設定を行いアクセスポートに設定します

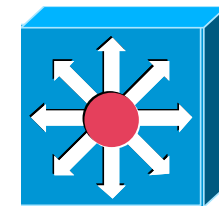
1. ポートに VLAN を割り当てます。

```
Switch(config-if)#switchport access vlan <vlan-ID>
```

2. ポートのモードを静的にアクセスモードにします。(DTP をOFF)

```
Switch(config-if)#switchport mode access
```

* ポートに対しては1つの VLAN のみマッピング可能です



VLANのマッピング確認

- 設定確認 -

```
Switch#show vlan
```

```
Switch#show interfaces status
```

```
Switch#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	
129 NW-6506S-6509C	active	Gi1/1, Gi3/5, Gi4/16
130 NW-6506S-3750A	active	Po2
132 NW-6506S-3750B	active	Po3
134 NW-6506S-6506A	active	Gi4/6, Po4
138 NW-6506S-4006B	active	Gi4/9

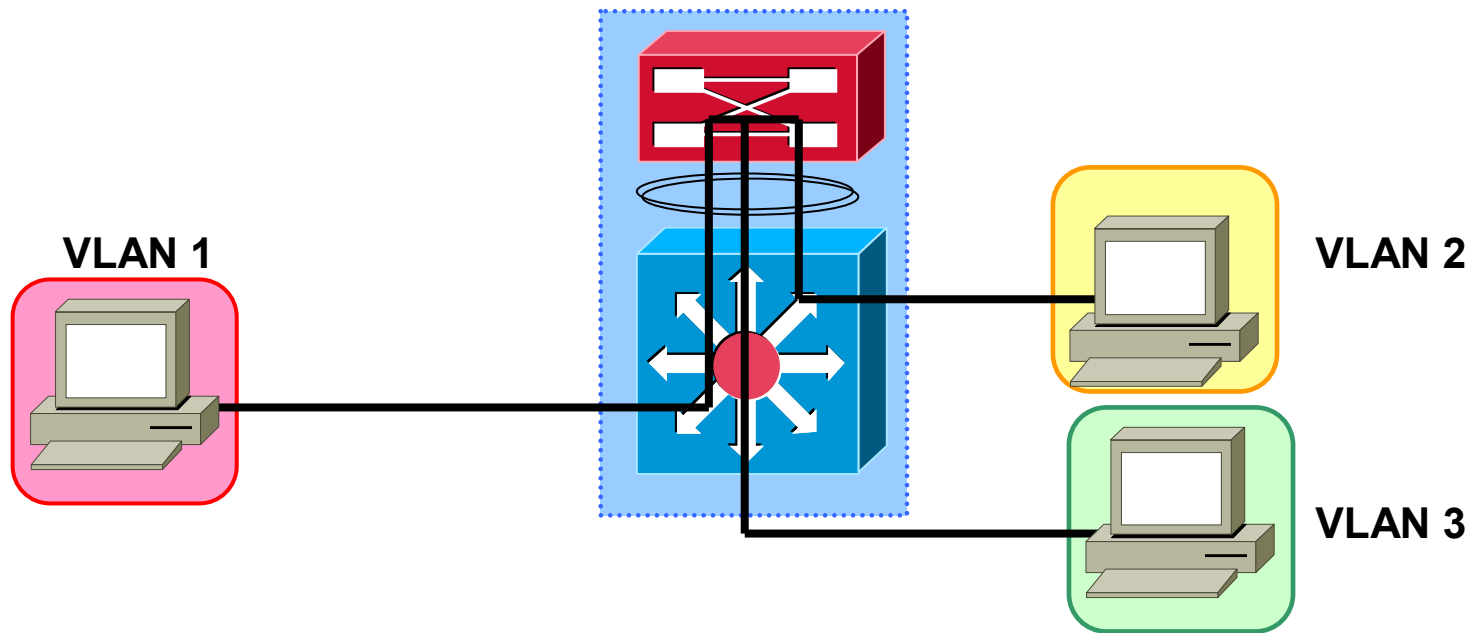
* 表示画面はCat6500のものです

Routing の設定手順

L3スイッチでルーティングを行うためには以下のような設定をする必要があります。

- Routing機能の有効化(enable)
- SVIの作成
- SVI, Routed Port各インターフェースのIPアドレス の設定
- Routing Protocol の設定 (オプション)
- スタティックルート、デフォルトルート設定(オプション)

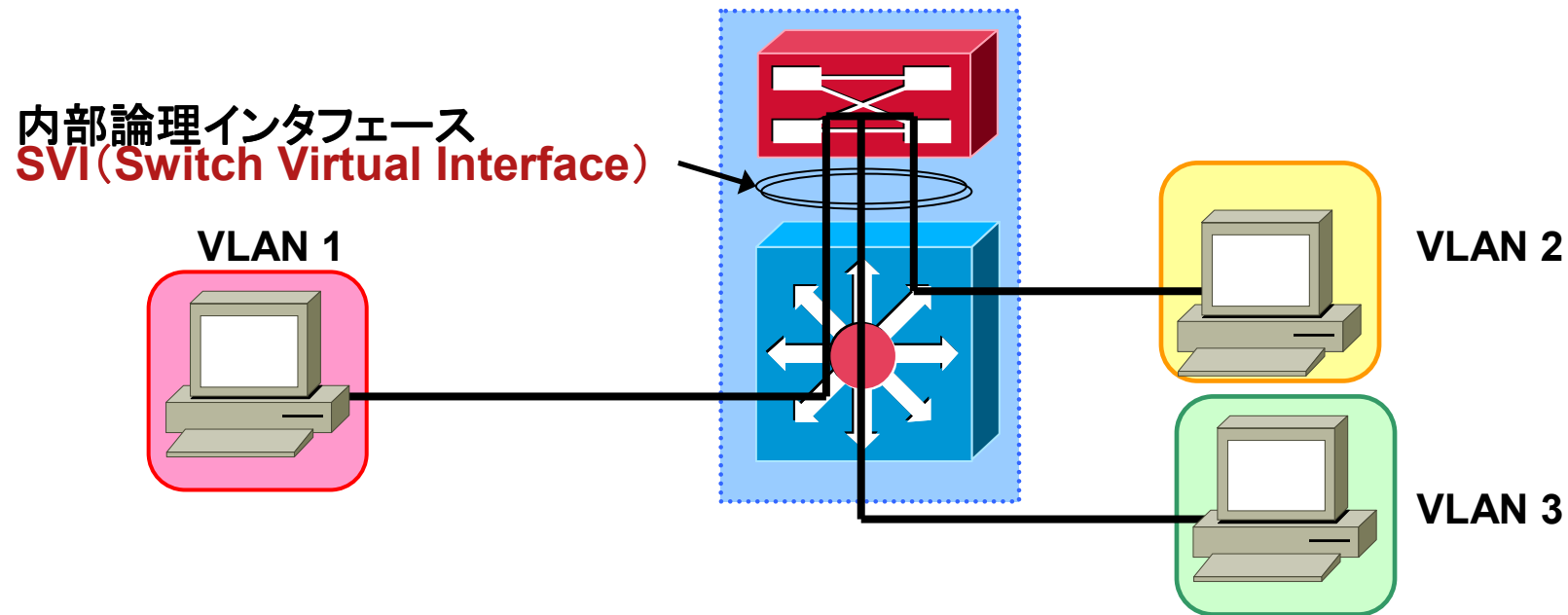
Routing の有効化



```
Switch(config)# ip routing
```

機種によりこのコマンドはデフォルトで有効になっている場合もあります。

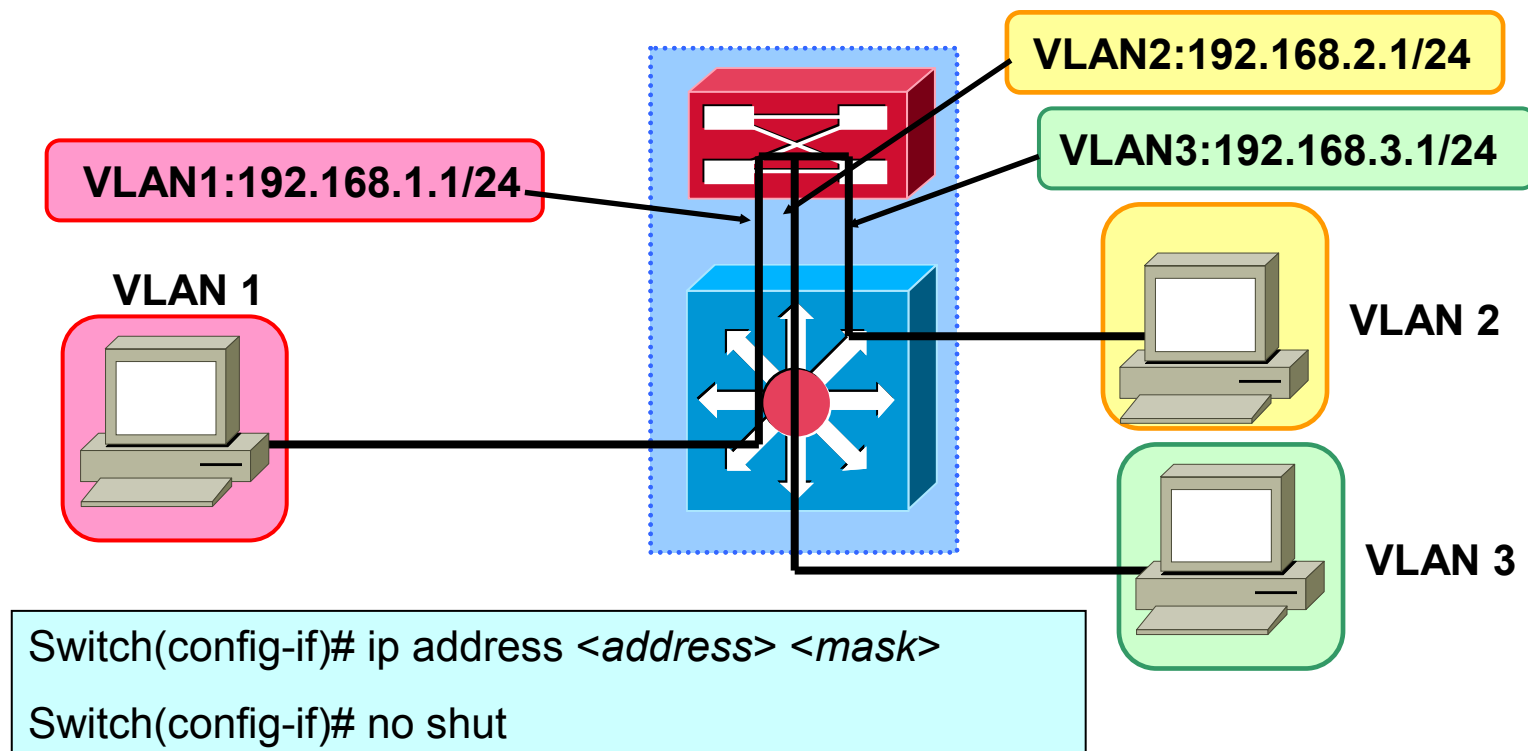
SVI の作成



```
Switch(config)#interface vlan <vlan-id>
```

例: Switch(config)# interface vlan 3
Switch(config-if)#

SVI, 物理インタフェース(Routed Port) への IP address 設定



例: **Switch(config)# int vlan 3**
Switch(config-if)# ip address 192.168.3.1 255.255.255.0

例: **Switch(config)# int gi 0/3**
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.1.3.1 255.255.255.0

