

ITプロ/ITエンジニアのための

徹底攻略

試験番号

640-802J*

640-816J

Cisco CCNA

[640-802J][640-816J] 対応

ICND2編

教科書

株式会社ソキウス・ジャパン 編著

*CCNA (640-802J) の出題範囲のうちICND1 (640-822J) に
相当する部分は「徹底攻略 Cisco CCNA/CCENT教科書 ICND1編」
に記載されています。

インプレスジャパン

本書は、CCNA（Cisco Certified Network Associate）およびICND2（Interconnecting Cisco Networking Devices Part 2）の受験用教材です。著者、株式会社インプレスジャパンは、本書の使用による「CCNA」および「INCD2」試験への合格を一切保証しません。

本書の内容については正確な記述に努めましたが、著者、株式会社インプレスジャパンは本書の内容に基づくいかなる試験の結果にも一切責任を負いません。

CCNA、Cisco、Cisco IOS、Catalystは、米国Cisco Systems, Inc.の米国およびその他の国における登録商標です。

その他、本文中の製品名およびサービス名は、一般に各開発メーカーおよびサービス提供元の商標または登録商標です。なお、本文中にはTMおよび®は明記していません。

インプレスジャパンの書籍ホームページ

書籍の新刊や正誤表など最新情報を随時更新しております。

<http://www.impressjapan.jp/>

Web徹底攻略

試験や資格の最新情報、模擬試験などが体験できる資格関連書の専用サイトです。

<http://shikaku.impress.co.jp/>

Copyright © 2009 Socius Japan, Inc. All rights reserved.

本書の内容はすべて、著作権法によって保護されています。著者および発行者の許可を得ず、転載、複写、複製等の利用はできません。

はじめに

Cisco CCNAは、インターネット分野のリーディングカンパニーであるシスコシステムズの認定資格です。

これまでCCNAは、「シスコのルータやスイッチング機器を使用した比較的単純なネットワークの設定やトラブルシューティングが実践できる」ことを認定する、ネットワーク技術者のための登竜門的な資格でした。しかし技術の進展に伴い、アソシエイトレベルであるCCNAに要求される知識範囲は大幅に拡大しています。2007年にはエントリーレベルの資格であるCCENTが登場し、ICND1試験とICND2試験の2つの試験に合格することでCCNAを取得することも可能になりました。

本書はCCNAおよびICND2受験のための学習書です。ネットワークの初心者の方でも無理なく学習を取り組んでいただけるように、ネットワークの基礎知識も丁寧に解説しました。日々シスコ製品に接していても、試験のために機器を自由に操作・検証しながら学習できる方は多くはないでしょう。そこで本書では、ネットワークの構成図や出力を豊富に掲載しました。図を確認し、出力を追っていくことによって、だんだんに実際の設定の感覚が身に付くはずです。また、章末の演習問題では、その章で学習した内容が理解できているか確認していただけると同時に、試験の雰囲気をつかんでいただくためにも有効です。

本書をご活用いただき、より多くの方がシスコのネットワークに親しみ、目指す資格を取得されることを願ってやみません。

2009年2月
著者

シスコ技術者認定の概要

シスコ技術者認定 (Cisco Career Certification) は、インターネットワーキングや同社ルータ製品に関する技術の証明および、エンジニアの育成を目的とした認定資格です。認定基準は米国シスコシステムズにより厳格に定められ、最新のIPネットワークに対応した技術者資格として世界的に認知されています。

シスコ技術者認定資格は、技術分野別に7つのカテゴリに分類されています。それぞれのカテゴリに、エントリー、アソシエイト、プロフェッショナル、エキスパートの4つの認定レベルがあります。

【シスコ技術者認定資格一覧】

認定分野	エントリー	アソシエイト	プロフェッショナル	エキスパート (CCIE)
ルーティング＆スイッチング	CCENT	CCNA	CCNP	CCIE Routing & Switching
デザイン	CCENT	CCNA、CCDA	CCDP	CCDE
ネットワークセキュリティ	CCENT	CCNA Security	CCSP	CCIE Security
サービスプロバイダー	CCENT	CCNA	CCIP	CCIE Service Provider
ストレージネットワーキング	CCENT	CCNA	CCNP	CCIE Storage Networking
ボイス	CCENT	CCNA Voice	CCVP	CCIE Voice
ワイヤレス	CCENT	CCNA Wireless	CCVP	CCIE Wireless

CCENTおよびCCNAの取得方法

CCNAは、次の2つの方法で取得することができます。

- 1科目で取得

- CCNA（試験番号640-802J）

試験時間：90分、出題数：50～60問、受験料：26,775円（税込）

- 以下の2科目に合格することで取得

- ICND1（試験番号640-822J）

試験時間：90分、出題数：40～50問、受験料：13,388円（税込）

- ICND2（試験番号640-816J）

試験時間：75～90分、出題数：40～50問、受験料：13,388円（税込）

※試験時間と問題数は、変更になる可能性があります。

受験申し込み方法

シスコ技術者認定試験を受験するには、ピアソンVUEもしくはピアソンVUEのテストセンターに受験を申し込みます。

● ID番号の取得

ピアソンVUEで初めて受験する場合は、ピアソンVUE IDを取得する必要があります。以下のURLの指示に従って、登録します。

<http://www.vue.com/japan/Registration/index.html>

①ピアソンVUEのWebサイトで申し込み

以下のURLにログイン後、試験名、会場、日時を指定します。

URL : <http://www.vue.com/japan/index.html>

②ピアソンVUEのコールセンターで申し込み

以下の受付番号に電話をし、申し込みます。

Tel : 0120-355-173 または0120-355-583

Fax : 0120-355-163

E-mail : [pjvpreg@pearson.com](mailto:pvjpreg@pearson.com)

営業時間：土日祝日を除く平日、午前9時～午後6時

③テストセンター

以下のサイトで受験を希望するテストセンターを選択し、電話で申し込みます。テストセンターによっては、受験当日の申し込みを受け付けているところもあります。

<http://www.vue.com/japan/TestcentersList/>

試験日程

ピアソンVUEの各試験会場で随時、受験することができます。

CCNAの問い合わせ先

試験の概要、受験後の認定証の取得に関する詳細および問い合わせについては、シスコのWebサイトを参照してください。

- ・シスコシステムズ

URL <http://www.cisco.com/jp/index.shtml>

本書の活用方法

本書は解説ページと演習問題の2部構成になっています。

解説

● 用語

ネットワーク技術の習得に、用語の理解は不可欠です。すぐに参照したい用語には米印（※）を付け、脚注で解説しました。また、アスタリスク（*）を付けた用語は巻末の用語集で説明しています。

● 構文

ルータやスイッチの設定・管理操作に必要な構文を多数掲載しています。構文は次のルールで記述しています。



- ・ **太字** ……表記されたとおり入力する。省略形で入力できるコマンドもある
- ・ **< >** ……引数。該当する文字や値を入力する
例) <username> → ユーザ名を入力する
- ・ **[]** ……オプション。必要に応じて設定する要素
- ・ **{ | }** ……選択。{}で括られたものから、いずれか1つを選択して入力する
例) { a | b } → 「a」か「b」のいずれかを入力する

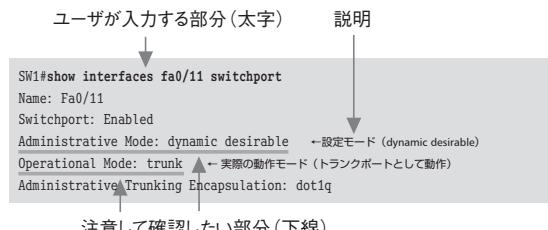
ユーザモード、特権モードのいずれも可能な場合のプロンプトは「#」で示しました。また、モードは以下のとおり省略しています。

- ・ ユーザEXECモード → ユーザモード
- ・ 特権EXECモード → 特権モード
- ・ コンフィギュレーションモード → コンフィグモード

巻末に構文索引を掲載しましたので活用してください。

● 出力

実際の設定作業を理解しやすくするために、本書ではコマンドの出力結果を数多く掲載しています。出力の中、ユーザが入力する部分は太字で示しました。また、必要な事項を的確に参照できるように、重要なポイントには適宜下線や説明を付加しています。



● 本書で使用したマーク

解説の中で重要な事項や補足情報は次のマークで示しています。

 Point	重要な技術情報や試験対策のうえで必ず理解しておかなければならぬ重要事項
 Memo	試験対策としては必須ではないが、解説の内容を理解したり、知識を深めたりするために役立つ情報

演習問題

各章の最後には5問の演習問題が用意されています。演習問題を解くことによって、理解度を確認できるだけでなく、試験の出題傾向を把握することができます。

●【問題】

シスコ技術者認定試験には、さまざまな出題形式があります。出題形式の詳細は付録で説明していますので、参照してください。各章の演習問題には選択形式の問題を、付録ではシミュレーション形式の問題を、それぞれ実際の試験と同じイメージで掲載しました。

多肢選択式

問題文を読んで、選択肢の中から正しいもの、あるいは誤りのあるものを選びます。必要に応じて、ネットワーク図や出力を参照します。

5. 次の図の構成でOSPFをシングルエリア環境で動作させると、R2ルータで実行する必須のあるコマンドを選びなさい。(3つ選択)



- A. (config-router) #network 172.16.0.0 0.0.255.255 area 0
- B. (config) #network 10.1.0.0 0.0.255.255 area 0
- C. (config-router) ospf 123
- D. (config-router) ospf 0
- E. (config-router) #network 10.1.16.0 0.0.0.15.255 area 0
- F. (config-router) #network 10.1.16.0 0.0.0.0 area 0
- G. (config-router) #network 172.16.13.64 0.0.0.63 area 1
- H. (config-router) #network 10.1.16.0 0.0.0.31 area 0

●【解答】

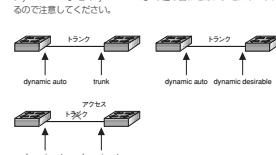
演習問題の解答と解説を読んで、理解できているかどうかを確認します。

解答と解説

解答のポイントを説明しています。必要に応じて、本文の参照箇所を示しています。また、正解の選択肢は太字で表記しています。

4. B, D

2つのスイッチ間を結ぶリンクをトランクにする方法は、互いの設定に影響します。片方のスイッチポートタイプが「dynamic auto」の場合、対向スイッチのスイッチポートタイプが「trunk」(B)または「dynamic desirable」(D)のどちらかにする必要があります。スイッチポートタイプの組み合わせについては、30ページを参照。選択肢は不正なコマンドです。



※ 本書に掲載したURLは2009年2月現在のものです。URLとWebサイトの内容は変更になる可能性があります。

目次

はじめに	3
シスコ技術者認定の概要	4
本書の活用方法	6

第1章 VLANとVTP

1-1 VLANの概要	14
1-2 VLANの動作	18
1-3 アクセスポートとトランクポート	21
1-4 VLANの設定	29
1-5 VLANの検証	36
1-6 VTP	45
1-7 VTPの設定	53
1-8 VTPの検証	56
1-9 音声VLAN	64
1-10 演習問題	67
1-11 解答	69

第2章 VLAN間ルーティング

2-1 VLAN間ルーティングの概要	74
2-2 VLAN間ルーティングの設定	76
2-3 演習問題	83
2-4 解答	86

第3章 スパニングツリープロトコル

3-1 スパニングツリープロトコルの概要	90
3-2 スパニングツリープロトコルの動作	96
3-3 スパニングツリープロトコルのポート状態	103
3-4 スパニングツリートポロジの設計	106
3-5 PVST+	109
3-6 スパニングツリープロトコルの設定	114
3-7 スパニングツリープロトコルの検証	118
3-8 スパニングツリープロトコルのFast機能	123
3-9 高速スパニングツリープロトコル	130
3-10 EtherChannel	141
3-11 演習問題	144
3-12 解答	147

第4章 リンクステートルーティング

4-1	ルーティングの概要	154
4-2	リンクステートルーティング	169
4-3	OSPFの概要	171
4-4	OSPFの階層設計	178
4-5	ルータID	183
4-6	隣接関係とLSDBの管理	185
4-7	OSPFネットワークタイプ	195
4-8	OSPFの基本設定	197
4-9	OSPFの検証	202
4-10	OSPFのオプション設定	221
4-11	OSPFの認証	230
4-12	演習問題	237
4-13	解答	239

第5章 ハイブリッドルーティング

5-1	EIGRPの概要	244
5-2	EIGRPの動作とDUALアルゴリズム	246
5-3	EIGRPのメトリック	257
5-4	EIGRPの基本設定	260
5-5	EIGRPの検証	264
5-6	EIGRPのオプション設定	274
5-7	EIGRPの認証	281
5-8	演習問題	287
5-9	解答	290

第6章 VLSMと経路集約

6-1	VLSM	294
6-2	経路集約	302
6-3	演習問題	308
6-4	解答	310

第7章 アクセスコントロールリスト

7-1	アクセスコントロールリスト	314
7-2	ワイルドカードマスク	325
7-3	番号付き標準アクセスコントロールリスト	328
7-4	番号付き拡張アクセスコントロールリスト	333
7-5	名前付きIPアクセスコントロールリスト	338
7-6	アクセスコントロールリストの検証	343
7-7	シーケンス番号によるアクセスコントロールリストの編集	346
7-8	VTYアクセスの制御	351
7-9	アクセスコントロールリストのトラブルシューティング	355
7-10	アクセスコントロールリストの応用	361
7-11	演習問題	368
7-12	解答	370

第8章 NATとPAT

8-1	NATおよびPATの概要	374
8-2	NATの設定	384
8-3	PATの設定	388
8-4	NATおよびPATの検証	392
8-5	NATおよびPATのトラブルシューティング	400
8-6	演習問題	406
8-7	解答	408

第9章 IPv6

9-1	IPv6の概要	412
9-2	IPv6アドレスの表記	416
9-3	IPv6アドレスのタイプ	420
9-4	IPv6アドレスの割り当て	428
9-5	IPv6の設定と検証	431
9-6	IPv6ルーティングプロトコル	437
9-7	IPv4からIPv6への移行	445
9-8	演習問題	451
9-9	解答	453

第10章 フレームリレー

10-1	フレームリレーの概要	456
10-2	フレームリレーの基本設定	469
10-3	NBMA問題とフレームリレーサブインターフェイスの設定	473
10-4	フレームリレーの検証	483
10-5	演習問題	489
10-6	解答	491

第11章 VPN

11-1	VPNの概要	494
11-2	IPsecの概要	500
11-3	IPsecのセキュリティサービス	505
11-4	暗号化アルゴリズムと鍵交換	512
11-5	演習問題	515
11-6	解答	517

用語集

用語集	520
-----	-----

付 錄 シミュレーション問題

シミュレーション問題	566
------------	-----

索引	596
Cisco IOSコマンド構文索引	605

第1章

VLANとVTP

1-1 VLANの概要

1-2 VLANの動作

1-3 アクセスポートとトランクポート

1-4 VLANの設定

1-5 VLANの検証

1-6 VTP

1-7 VTPの設定

1-8 VTPの検証

1-9 音声VLAN

1-10 演習問題

1-11 解答

1-1

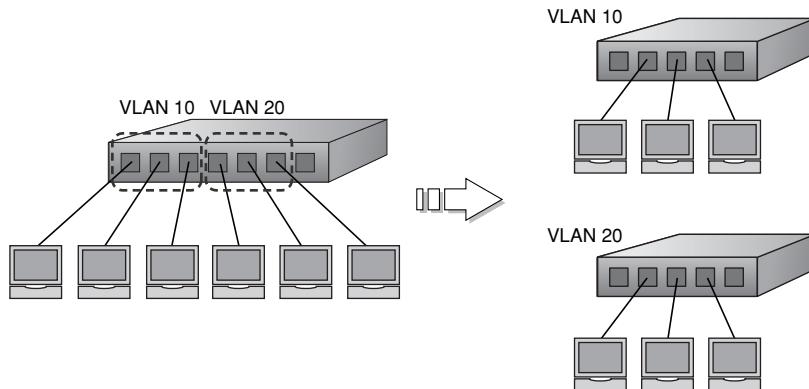
VLANの概要

仮想LAN（VLAN）は、物理的な接続とは関係なくノードをグループ化し、仮想的なLANセグメントを形成する技術です。規模が拡大し、より複雑になる現在のキャンパスネットワークにおいて、欠くことのできない技術です。

■ VLANの概要

VLANはVirtual LAN（仮想LAN）の略であり、ここでいうLANとはブロードキャストドメイン^{*1}を指しています。VLANを使用すると、本来はルータ（L3デバイス）でしかできなかったブロードキャストドメインの分割を、レイヤ2レベルで分割することができ、1台のスイッチを、あたかも複数のスイッチを使ってユーザをグループ分けしているかのように扱うことができます。

【VLANのイメージ】

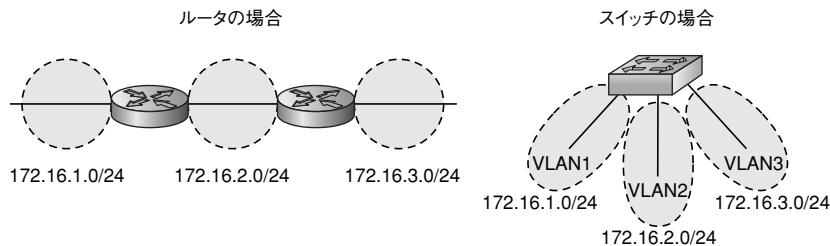


VLANは、ルータによって分割されたネットワークと同様に機能します。したがって、各VLANはそれぞれ1つのサブネットに対応するため、次のように定義されます。

VLAN = ブロードキャストドメイン = サブネット（論理ネットワーク）

*1 【ブロードキャストドメイン】 broadcast domain：宛先がすべてのノードであるブロードキャストトラフィックが流れていく範囲のこと。ルータのインターフェイスで分割されるため、ホストがルータを介さない（ルーティングしない）で直接通信することができるネットワークを指す

【ブロードキャストドメインの分割】



■ VLANのメリット

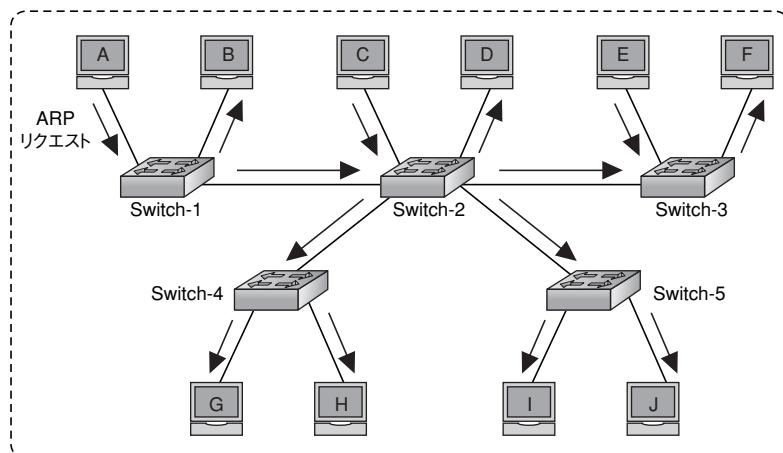
VLANを使用すると、ブロードキャストドメインを論理グループで分割することができます。これによって、物理的な配置を意識せずに、LANをより柔軟に設計できるようになります。

VLANを導入することによって、次のようなメリットがあります。

● ブロードキャストトラフィックの局所化

1つのブロードキャストドメインを複数に分割することでブロードキャストトラフィックの影響を局所化することができます。

【1つのブロードキャストドメインによる影響】



上の図のような、複数のスイッチで構成される1つのブロードキャストドメインがあるとしましょう。ホストAはホストBにデータを送る前に、ARP^{※2}リクエスト

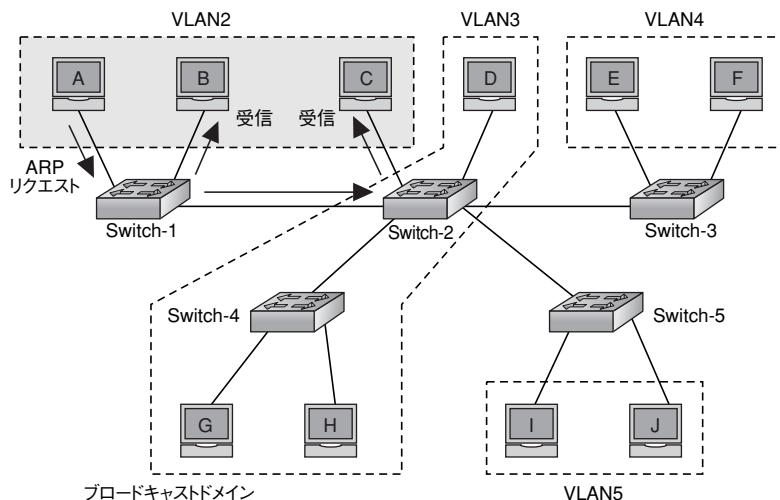
※2 【ARP】(アーフ) Address Resolution Protocol : IPアドレスを基にしてMACアドレスを得るためのTCP/IPのネットワーク層プロトコル

(ブロードキャスト) を送信したとします。このとき各スイッチは、受信したブロードキャストフレームをフラッディング^{※3}します。そのため、ブロードキャストドメインに所属するすべてのコンピュータにARPリクエストが転送されます。

ネットワークの規模が拡大し多くのコンピュータが接続されると、当然のことながらブロードキャストトラフィックが増加します。これでは、ネットワーク全体のパフォーマンスが低下するだけでなく、コンピュータのCPUにも負荷がかかりてしまいます。

VLANを設定すると、次の図のようにVLAN単位でブロードキャストドメインを分割することができます。そのため、ホストAが送信したブロードキャストフレームは、同じVLAN2に所属するホストBとホストCにのみ転送されるため、増加するブロードキャストトラフィックの悪影響を最小限に抑えることができます。

【VLANによるブロードキャストドメイン分割の例】



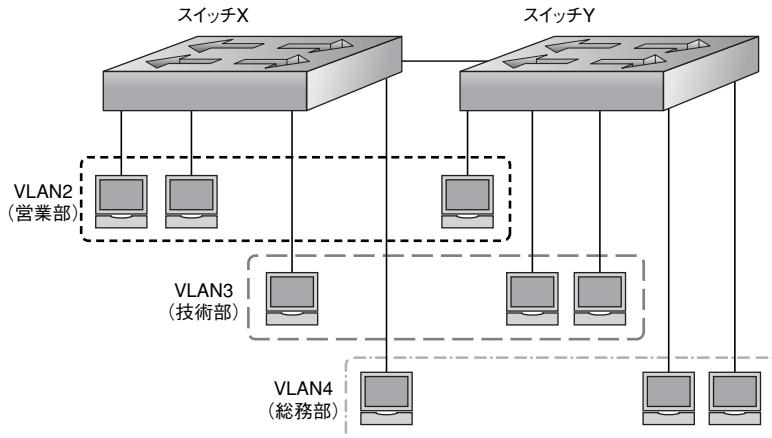
● 柔軟なネットワークのセグメント化

VLANを実装すると、コンピュータが接続されたスイッチポートにVLAN ID (VLANの識別番号) を割り当てるだけでブロードキャストドメインが分割されます。そのため、組織変更や部署の配置変更があった場合でも、ネットワークの物理的な配線はそのまま変更することなく、管理者はスイッチポートに割り当てるVLAN IDを変更するだけで柔軟に論理ネットワークをセグメント化 (グループ化) することができます。

※3 【フラッディング】flooding: 受信したポートを除くすべてのポートにフレームを転送するトラフィックの送出方法のこと。ネットワーク上のすべての端末に対してデータを洪水 (flooding) のように流すことからこう呼ばれている

なお、VLANは1つのスイッチ上に設定することも、複数のスイッチにまたがつて構成することもできます。

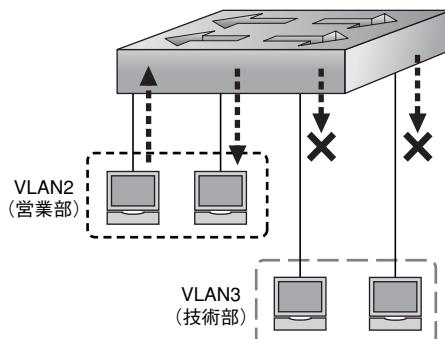
【柔軟なネットワークセグメント化】



● セキュリティの強化

VLANを実装すると、あるVLANに所属するポートは同じVLANのブロードキャストを共有しますが、異なるVLANのブロードキャストは共有されません。その結果、VLAN単位でトラフィックを分離することになり、セキュリティを強化できます。

【VLANによるセキュリティの強化】



1-2 VLANの動作

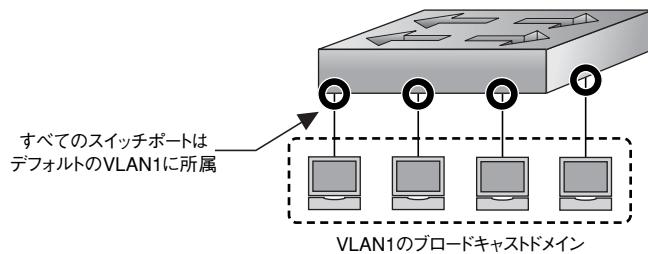
VLANがどのようにしてブロードキャストドメインを分割しているかを知るために、VLANの動作について理解しておく必要があります。本節では、VLANの動作と管理VLANの役割について説明します。

■ VLANの動作

VLANはVLAN IDと呼ばれる番号によって識別されます。Catalystスイッチには、工場出荷時に各種メディアに対してデフォルトVLANと呼ばれるVLANが設定されています。イーサネットのデフォルトVLANは、VLAN1です。すべてのスイッチポートはデフォルトでVLAN1に所属しています。また、CDP^{※4}およびVTPアドバタイズメント^{※5}はVLAN1上に伝送されます。

◎トーカンリングおよびFDDIのデフォルトVLANはCCNAの範囲を超えるため、本書では言及しません。

【イーサネットのデフォルトVLAN】



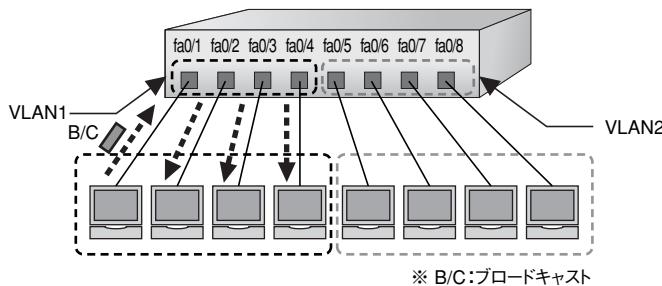
スイッチポートにVLANを割り当てるのをVLANメンバーシップといいます。スイッチはブロードキャストフレームを受信すると、受信ポートと同じVLANがメンバーシップされているポートだけにフラッディングします。

次の図ではスイッチポートfa0/1～fa0/4にはVLAN1、fa0/5～fa0/8にはVLAN2がメンバーシップされています。スイッチは、fa0/1ポートでブロードキャストフレームを受信すると、fa0/1が所属しているVLAN1と同じVLANが割り当てられているfa0/2、fa0/3、fa0/4に転送します。異なるVLANが割り当てられているfa0/5～fa0/8へは転送されません。結果として、ブロードキャストドメインが分割されることになります。

※4 【CDP】(シーディーピー) Cisco Discovery Protocol : 隣接するCiscoデバイスの情報を知ることができます。Cisco独自のレイヤ2プロトコル

※5 【VTPアドバタイズメント】(ブイティーピーアドバタイズメント) VTP advertisement : VTPで通知されるメッセージのこと。VTPアドバタイズメントには、ドメイン名、パスワード、リビジョン番号、VLAN情報などが含まれる

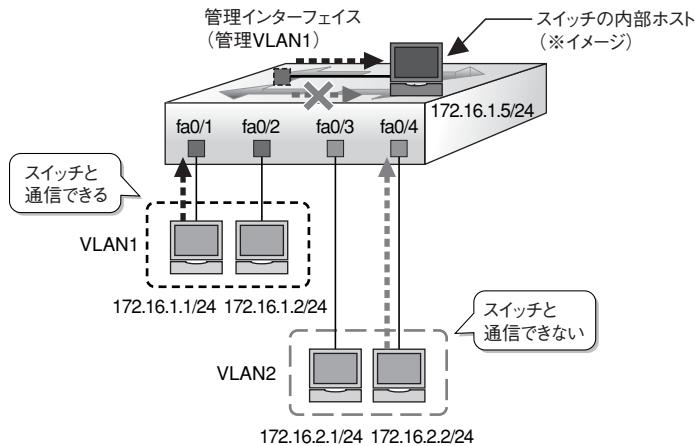
【VLANの動作】



■ 管理VLAN

管理VLANは、スイッチに1つだけ存在する特別なVLANで、デフォルトではVLAN1が管理VLANに設定されています。スイッチには管理VLAN用に用意された管理インターフェイスと呼ばれる仮想のインターフェイスがあります。管理インターフェイスは、レイヤ2スイッチ内部で動作するレイヤ3ホストのように動作します。この管理インターフェイスにIPアドレスを割り当てることで、スイッチ自身がTCP/IP通信を行うことができます。たとえば、管理者がリモートからスイッチへTelnet接続したり、SNMP^{※6}を使用して管理したりすることができます。したがって、スイッチと通信するには、管理VLANへアクセスできなくてはなりません。

【管理VLAN】



※6 【SNMP】(エスエヌエムピー) Simple Network Management Protocol：ネットワーク上のさまざまな機器を監視および制御することができる管理プロトコル

スイッチ（管理インターフェイス）にIPアドレスを割り当てるには、`interface vlan <vlan-id>`コマンドでインターフェイスコンフィギュレーションモードに移ってから、IPアドレスとサブネットマスクを設定します。また、VLAN1の管理インターフェイスはデフォルトでshutdown状態であるため、`no shutdown`コマンドを使って有効にする必要があります。

構文 スイッチに対するIPアドレスの設定（インターフェイスコンフィグモード）

```
(config)#interface vlan <vlan-id>
(config-if)#ip address <ip-address> <subnet-mask>
(config-if)#no shutdown
```

引数	説明
vlan-id	管理VLANのVLAN IDを指定（デフォルトは1）
ip-address	IPアドレスを指定
subnet-mask	サブネットマスクを指定

【Catalystスイッチに対するIPアドレスの設定例】

```
SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#interface vlan 1      ←管理VLANに「1」を指定
SW1(config-if)#ip address 172.16.1.5 255.255.255.0      ←IPアドレスを割り当てる
SW1(config-if)#no shutdown      ←インターフェイスを有効にする
SW1(config-if)#end
SW1#
2d18h: %SYS-5-CONFIG_I: Configured from console by console
SW1#show interface vlan 1      ←管理インターフェイスの状態を確認
Vlan1 is up, line protocol is up      ←有効化されている
Hardware is EtherSVI, address is 0021.1c77.50c0 (bia 0021.1c77.50c0)
Internet address is 172.16.1.5/24      ←IPアドレスが割り当てられている
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA, loopback not set
<以下省略>
```

1-3

アクセスポートとトランクポート

VLANを構成するスイッチポートは、1つのVLANに所属するアクセスポートと複数のVLANに所属するトランクポートに分類されます。それぞれのスイッチポートの特徴とトランкиングプロトコルの役割を理解しましょう。

■ アクセスポート

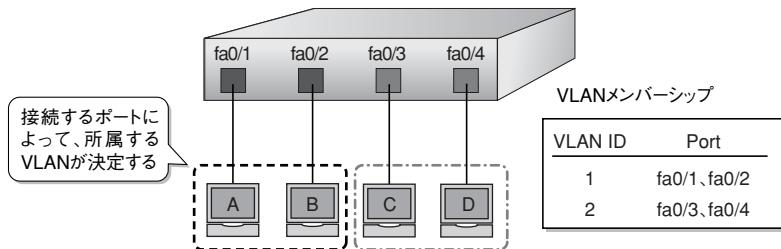
アクセスポートは1つのVLANにのみ所属するポート、つまり、1つのVLANフレームのみを転送するポートです。アクセスポートの設定には、スタティック（静的）とダイナミック（動的）の2つの方法があります。

● スタティックVLAN

スタティックVLANは、管理者がポートに対して手動で割り当てるVLANで、ポートベースVLANとも呼ばれています。

スタティックVLANで割り当てたVLAN IDは固定されるため、管理者はネットワークの構造を把握しやすく、設定も容易になるというメリットがあります。ただし、誤ってケーブルを別のポートと接続すると、ユーザがほかのVLANに属してしまうというリスクもあります。

【スタティックVLANの例】



● ダイナミックVLAN

ダイナミックVLANは、ポートに接続されたノードのMACアドレスに基づいてVLANメンバーシップを動的に決定するVLANです。

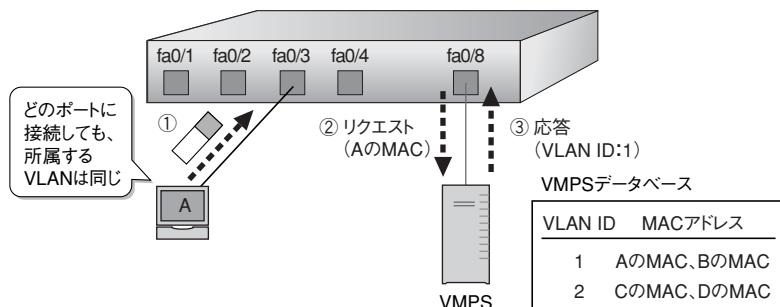
ダイナミックVLANを使用するには、どのMACアドレスを持つノードがどのVLANに所属するかというマッピング情報をあらかじめ準備しておく必要があります。このデータベースを持つサーバをVMPS（VLAN Management Policy Server）と呼びます。ダイナミックVLANが設定されたスイッチポートは、コンピュータを接続して最初のフレームを受信すると、送信元MACアドレスがどのVLANに所属するかをVMPSに問い合わせます。

ダイナミックVLANは、スタティックVLANに比べて管理が複雑になりますが、

接続されるコンピュータが固定で決まっていない会議室や共有スペースといった、不特定多数のユーザが利用するような場所で使用すると効果的です。なお、Catalyst 6500シリーズなど一部のスイッチはVMPS機能を持つため、スイッチ自身がVMPSとして動作することも可能です。

次の図では、fa0/1からfa0/4にダイナミックVLANが設定されています。fa0/3ポートにホストAを接続して最初のフレームを受信すると、フレームヘッダの送信元MACアドレスに基づいてVMPSにVLAN IDをリクエストします。VMPSからの応答によって動的にfa0/3にVLAN1がメンバーシップされます。ダイナミックVLANではこのように、ホストAはどのポートにケーブルを接続しても常にVLAN1に属することができます。

【ダイナミックVLANの例】



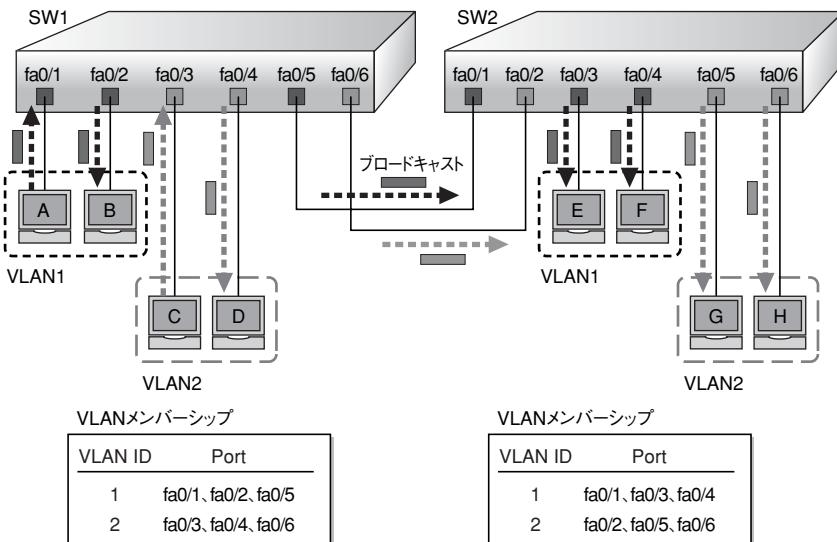
■ トランクポート

トランクポートは複数のVLANに所属するポート、つまり複数のVLANフレームを転送するポートです。トランクポートは、同じVLANが複数のスイッチにまたがって構成される場合に使用されます。

2台のスイッチ間をアクセスポートで接続する場合、VLANの数だけスイッチポートおよびケーブルが必要になります。

次の図では、スイッチ間をアクセスポートで接続しています。SW1はホストAが送信したブロードキャストフレームを受信すると、fa0/1に割り当てられているVLAN1が属するすべてのポート (fa0/2とfa0/5) にフラッディングします。ホストCのブロードキャストも同様に、VLAN2のすべてのポートにフラッディングされます。これによって、複数のスイッチにまたがってVLAN (ブロードキャストドメイン) を構成することができます。しかし、スイッチ間をアクセスポートで接続するため、新しいVLANを追加するたびにスイッチ間を接続する物理ポートとケーブルが必要になってしまいます。

【アクセスポートで接続する場合】



この問題を解決するのがトランクです。トランクは、1本の物理リンク上で複数のVLANトラフィックを伝送する技術です。トランクとして設定されたトランクポートでスイッチ間を接続し、フレームを転送する際にVLAN識別情報を付加します。対向のスイッチではフレームに付加されたVLAN識別情報を基にフレームの転送先を決定します。

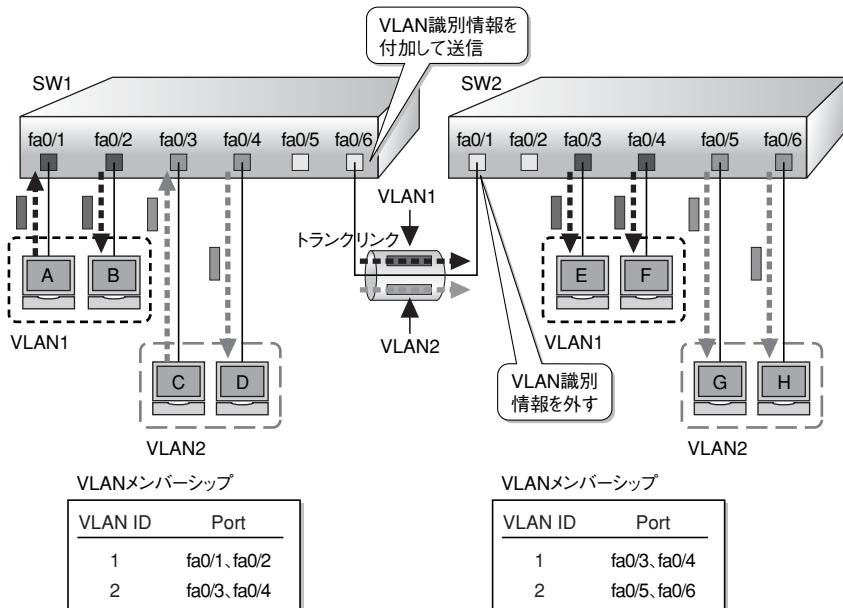
なお、トランクリンクでは、イーサネットフレームの最大サイズ（1,518バイト）よりも大きく、1,600バイト以下のフレームをベビージャイアントフレーム^{※7}として処理することができます。

次ページの図では、スイッチ間をトランクポートで接続しています。トランクポートで接続されたリンクをトランクリンクと呼びます。トランクリンク上では複数のVLANトラフィックを伝送することができます。

たとえば、SW1はホストAからのプロードキャストフレームを受信すると、VLAN1が属するfa0/2とトランクポート（fa0/6）にフラッディングします。このとき、トランクポートから送信されるフレームにはVLAN識別情報が付加されて伝送されます。対向のSW2では、トランクポート（fa0/1）でフレームを受信すると、VLAN識別情報を読み取って該当するVLAN1が属するfa0/3とfa0/4にフラッディングします。ホストCからのプロードキャストを受信した場合も、SW1は同様にフラッディングします。

※7 【ベビージャイアントフレーム】baby giant frame：最大1,600バイトまでのイーサネットフレームのこと。パケットサイズ（MTUサイズ）は1,552バイト（ヘッダー／トレーラを含まず）。通常、スイッチの非トランクポートでは1,500バイトを超えるフレームをサポートしていないが、トランクポートとして設定することで大きなサイズのフレームをサポートすることができる。

【トランクポートで接続する場合】



同一のリンク上で伝送される異なるVLANのトラフィックは、VLAN識別情報によって区別されます。VLAN識別情報は、トランクポートからフレームを転送する際に付加されます。対向スイッチがフレームを受信し、フレームを該当するポートから転送する際にはVLAN識別情報は取り除かれます。

■ トランкиングプロトコル

2台のスイッチ間をトランクリンクとして動作させるには、それぞれをポイントツー・ポイントで接続し、両端で同じ種類のトランкиングプロトコル^{※8}を使用する必要があります。

トランкиングプロトコルには、IEEE 802.1QとISLの2つがあります。

● IEEE 802.1Q

IEEE 802.1QはIEEE^{※9}により標準化されているプロトコルで、「dot1q（ドットイ

※8 【トランкиングプロトコル】Trunking Protocol：トランクリンク上でVLAN識別情報を付加するプロトコル。最も一般的なものにIEEE 802.1Qがある

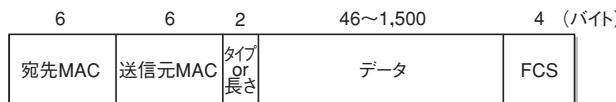
※9 【IEEE】(アイソリブルイ) Institute of Electrical and Electronics Engineers：米国電気電子学会。1963年に米国電気学会と無線学会が合併して発足し、世界約150カ国に会員が在籍している。IT分野では主にデータ伝送技術やネットワーク技術の標準を定めている

チキー)」と略して呼ばれています。

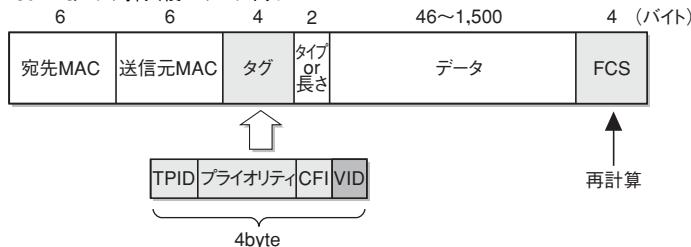
IEEE 802.1Qでは、トランクリンク上でイーサネットフレームの送信元MACアドレスフィールドとタイプ（または長さ）フィールドの間に「タグ」と呼ばれる4バイトのフィールドを挿入します。このとき、元のフレームが変更されるためFCS^{※10}を再計算します。

【802.1Qタギング】

標準のイーサネットフレーム



802.1Qのタグ挿入後のイーサネットフレーム



【802.1Qタグに含まれる情報】

フィールド	サイズ(ビット)	説明
TPID	16	Tag Protocol Identifier。タグが付加されたフレームであることを受信側に通知。イーサネットの場合「0x8100」が入る
プライオリティ	3	フレームの優先度を定義することができるQoS ^{※11} の機能
CFI	1	Canonical Format Indicator。アドレス形式を示す値。トーカンリング ^{※12} で使用するため、イーサネットでは「0」が入る
VID	12	VLAN Identifier。0~4095の範囲のVLAN ID

※10 【FCS】(エフシーエス) Frame Check Sequence：データリンク層でカプセル化する際に、データの後ろに付加するエラー検出のための制御情報。FCS内にはCRCと呼ばれる整合性を確認するための値が入る

※11 【QoS】(キューオーエス) Quality of Service：パケットの優先度に応じて扱いを区別し、重要なアプリケーションの通信を輻輳や遅延から守るための仕組み。特に音声や動画などのリアルタイム性が要求される通信で必要となる技術

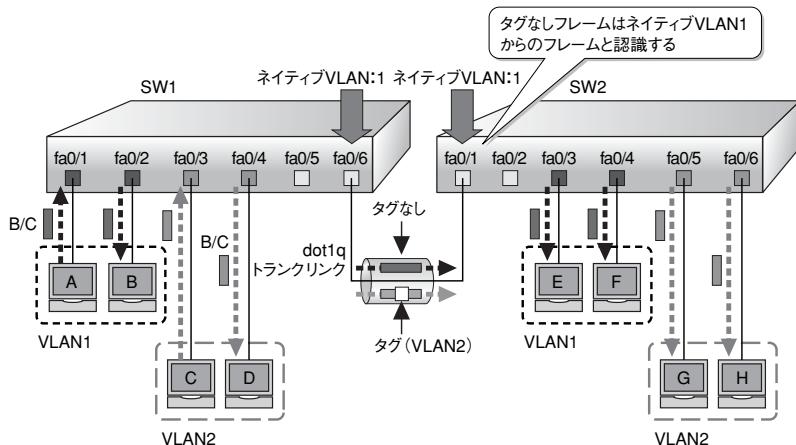
※12 【トーカンリング】Token Ring：IBMが提唱し、IEEE 802.5で標準化されたリング型トポロジのLAN。トーカンといわれる送信権を巡回させて送信する順番を決める。通信速度は4Mbpsまたは16Mbps

IEEE 802.1Q トランクではネイティブVLANがサポートされています。ネイティブVLANとは、トランクリンク上でタグを付加しないで転送されるVLANです。

タグなしのフレームを受信した対向側では、それがネイティブVLANからのトラフィックであると認識します。そのため、トランクリンクの両端でネイティブVLANのIDを一致させておく必要があります。IDが異なると、構成によってはループが発生する場合があります。

ネイティブVLANとして指定するVLAN IDは、トランクリンクごとに設定することができます。デフォルトではVLAN1に設定されています。

【ネイティブVLAN】



● ISL

ISL (Inter-Switch Link) はシスコが独自で開発したトランкиングプロトコルです。ISLでは、トランクリンク上でイーサネットフレームの前にISLヘッダ (26バイト) を付加し、さらに後ろに新しいFCS (4バイト) を付加してカプセル化します。

【ISLカプセル化】



【ISLヘッダに含まれる情報】

フィールド	サイズ(ビット)	説明
DA	40	Destination Address。宛先アドレス。ISLカプセル化フレームであることを示すマルチキャストアドレス (0x01-00-0C-00-00) が入る
Type	4	送信元フレームタイプを示す。イーサネットの場合は「0000」が入る
User	4	プライオリティの定義などで使用する。通常は「0」が入る
SA	48	Source Address。送信側CatalystスイッチのトランクポートのMACアドレスが入る
LEN	16	DA、Type、User、SA、LEN、FCSを除いたフレーム長を示す
AAA03	24	標準SNA 802.2LLCヘッダ。固定値「0xAA-AA-03」が入る
HSA	24	SAの先頭3バイトのコピー
VLAN	15	VLAN Identifier。ただし、VLAN IDを示すのは下位10ビットであるため、0~1023の範囲となる
BPDU	1	フレームがBPDU ^{※13} かCDP ^{※14} であるかを示す
INDEX	16	フレームがどのポートから転送されたかを示す
RES	16	トーカンリングとFDDI ^{※14} で特別に意味を持たせるために予約している

※13 【BPDU】(ビーピーディーユー) Bridge Protocol Data Unit : STPで制御情報を交換するためのメッセージのこと。ブリッジID、パスコスト、タイマー情報などが含まれている。BPDUによってルートブリッジを選出し、STPツリーが作成および維持される

※14 【FDDI】(エフディーディーアイ) Fiber Distributed Data Interface : ANSI (米国規格協会) が標準化したリング型LANの規格。伝送速度は100Mbpsで光ファイバケーブルを使用する

トランクリンク上で30バイトもフレームサイズが増加するISLは、現在ではほとんど使用されず、IEEE 802.1Qが一般的に使用されています。Catalyst 2950やCatalyst 2960など一部のCatalystスイッチでは、IEEE 802.1Qのみをサポートしています。

Point トランкиングプロトコルの比較

IEEE 802.1QとISLの特徴をまとめると、次のようにになります。

【IEEE 802.1QとISLの比較】

トランкиングプロトコル	802.1Q	ISL
規格	IEEEによって標準化	シスコ独自
方式	タギング方式	カプセル化方式
ネイティブVLAN	サポート	サポートなし
フレームの増加サイズ	4バイト	30バイト (ヘッダ: 26、FCS: 4)
ペーパージャイアントフレーム	1,522バイト	1,548バイト
FCSの処理	再計算	追加
VLAN ID	12ビット	10ビット
サポートするVLAN数	$2^{12} = 4,096$	$2^{10} = 1,024$

1-4

VLANの設定

VLANを構成するには、VLANを作成し、スイッチポート（アクセスまたはトランク）の設定を行います。本節では、Catalystスイッチを使用してVLANを構成するために必要なコマンドについて説明します。

■ VLANの作成

VLANを作成するには、グローバルコンフィギュレーションモードから`vlan <vlan-id>`コマンドを使用し、VLANコンフィギュレーションモードに移行します。オプションでVLANに識別しやすい名前を設定することができます。名前を指定しない場合は、VLANの後ろにVLAN IDが追加された名前がデフォルトで設定されます。

構文 VLANの作成（グローバルコンフィギュレーションモード）

```
(config)#vlan <vlan-id>
(config-vlan)#name <vlan-name> (オプション)
(config-vlan)#exit
```

引数	説明
vlan-id	VLAN IDを1～4094の範囲で指定。カンマ (,) やハイフン (-) を使い、同時に複数のVLANを作成することも可能 例) VLAN2を作成する場合 : (config)#vlan 2 VLAN10と20を作成する場合 : (config)#vlan 10,20 VLAN2～10を作成する場合 : (config)#vlan 2-10
vlan-name	VLAN名を指定（オプション）。nameコマンド自体を省略した場合、VLAN IDを付加した名前が設定される 例) VLAN2の場合 : VLAN0002

作成したVLANを削除するには、グローバルコンフィギュレーションモードから`no vlan <vlan-id>`コマンドを使用します。なお、自動的に生成されるデフォルトのVLAN（VLAN1および1002～1005）を削除することはできません。

■ スイッチポートのネゴシエーション

DTP（Dynamic Trunking Protocol）は、スイッチポートをアクセスポート、またはトランクポートのどちらにするかを動的に決定するためにシスコが独自で開発したネゴシエーションプロトコルです。DTPを利用すると、対向のスイッチポートの設定に合わせてアクセスポートまたはトランクポートのいずれかで動作します。

スイッチポートを動的にネゴシエーション^{※15}させるには、インターフェイスコンフィ

※15 【ネゴシエーション】negotiation : 2台の機器同士が相互に情報を交換しながら設定を決定すること

ギュレーションモードからswitchport modeコマンドを使用し、引数にdynamic desirableまたはdynamic autoキーワードを指定します。両者の違いは次の構文の表を参照してください。

構文 スイッチポートの設定（インターフェイスコンフィグモード）

```
(config-if)#switchport mode { access | trunk | dynamic desirable | dynamic auto }
```

引数	説明
access	ネゴシエーションに関係なくアクセスポートに設定する。自らDTPの送信をしない
trunk	ネゴシエーションに関係なくトランクポートに設定する。DTPを送信して対向にトランクポートになるようネゴシエートする
dynamic desirable	ネゴシエートして対向がtrunk、dynamic desirable、dynamic autoのいずれかの場合、トランクポートとして動作する。DTPを送信してネゴシエートする（積極的）
dynamic auto	ネゴシエートして対向がtrunk、dynamic desirableのいずれかの場合、トランクポートとして動作する。対向からDTPを受信しない場合、アクセスポートとして動作する。自らDTPを送信せず、応答のみ行う（消極的）

※ デフォルトの動作モードは、Catalyst 2950ではdynamic desirable、Catalyst 2960ではdynamic autoのように製品によって異なる

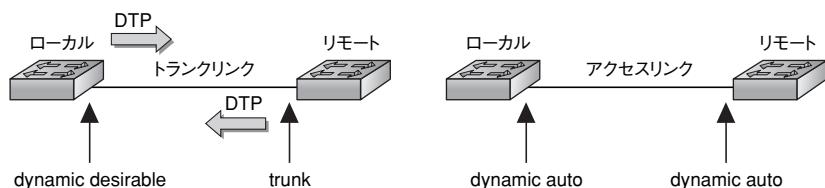
2台のスイッチ間を結ぶリンクがトランクになるかアクセスになるかは、互いの設定に影響します。次の表に、スイッチポートタイプの組み合わせを示します。

【スイッチポートタイプの組み合わせ】

リモート	access	trunk	dynamic desirable	dynamic auto
access	アクセス	推奨しない	アクセス	アクセス
trunk	推奨しない	トランク	トランク	トランク
dynamic desirable	アクセス	トランク	トランク	トランク
dynamic auto	アクセス	トランク	トランク	アクセス

※ トランクが802.1Qの場合は、access指定側のVLANとtrunk指定側のNative VLANが一致すると、そのVLANのみ通信が可能だが、互いの認識が異なる設定なので推奨されない

【組み合わせの例】



● DTPネゴシエーションの停止

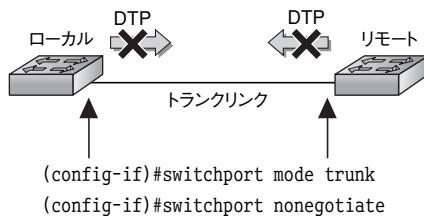
DTPのネゴシエーションを停止するには、`switchport nonegotiate`コマンドを使用します。

構文 DTP送信の停止（インターフェイスコンフィグモード）

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

たとえば、2台のスイッチのポートを固定でトランクポートまたはアクセスポートに設定しネゴシエートさせる必要がない場合には、switchport nonegotiateコマンドを設定しておくとDTPを送信しなくなるため、不要なトラフィックを削減することができます。

【DTPネゴシエーションを停止してトランクリンクを設定する】



Point VLAN ID

CatalystスイッチでサポートされるVLAN ID（VLAN番号）の範囲は0～4095ですが、実際に使用できる範囲は、インストールされているiOSソフトウェアの種類とVTP^{※16}の動作モードによって異なります。VLAN IDの範囲まとめると、次のようになります。

【VLAN IDの範囲】

VLAN ID	説明
0、4095	システムでのみ使用するVLAN
1	シスコのイーサネットのデフォルトVLAN
2~1001	イーサネットの標準VLAN
1002~1005	シスコのトーカンリングとFDDIのデフォルトVLAN
1006~4094	イーサネットの拡張VLAN

※ イーサネットの拡張VLAN範囲を使用することができる原因是、Enhanced Software Image (ESI: 拡張ソフトウェアイメージ) がインストールされており、VTPの動作モードがトランスペアレントの場合のみ

※16 【VTP】(ヴィティーピー) VLAN Trunking Protocol：Cisco独自のVLAN管理プロトコル。複数のスイッチでVLAN情報の整合性を保つことができる

■ アクセスポートの設定 (VLANメンバーシップ)

VLANを作成しても、そのVLANをポートにメンバーシップするまでブロードキャストドメインは分割されません。アクセスポートでは、ポートが所属するVLANを1つだけ割り当てます。すべてのアクセスポートはデフォルトでVLAN1に所属しています。

スイッチポートに特定のVLANを割り当てる場合、VLAN1からは自動的に外されます。

スイッチポートを固定でアクセスポートに指定し、VLANメンバーシップを設定するには、次のコマンドを使用します。

構文 アクセスポートの設定 (インターフェイスコンフィギュレーションモード)

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

構文 VLANメンバーシップの設定 (インターフェイスコンフィギュレーションモード)

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

引数	説明
vlan-id	特定のVLAN IDを1～4094の範囲で指定

スイッチポートをデフォルトのVLAN1に戻すには、インターフェイスコンフィギュレーションモードからno switchport access vlan (または、switchport access vlan 1) コマンドを使用します。

なお、switchport access vlanコマンドによるVLANメンバーシップは、スタティックVLANになります。ダイナミックVLANを設定する場合は、switchport access vlan dynamicコマンドを使用します。

■ トランクポートの設定

スイッチポートを固定でトランクポートにする場合、先のswitchport mode trunkコマンドの設定のほかに、トランкиングプロトコルを指定する必要があります。ただし、Catalyst 2950/2960のようにIEEE 802.1Qしかサポートしていないスイッチでは、プロトコルを指定する必要はありません (プロトコルを選択するコマンド自体存在しません)。

なお、DTPネゴシエーションによって動的にトランクポートになる場合は、トランкиングプロトコルも動的に決定されます。

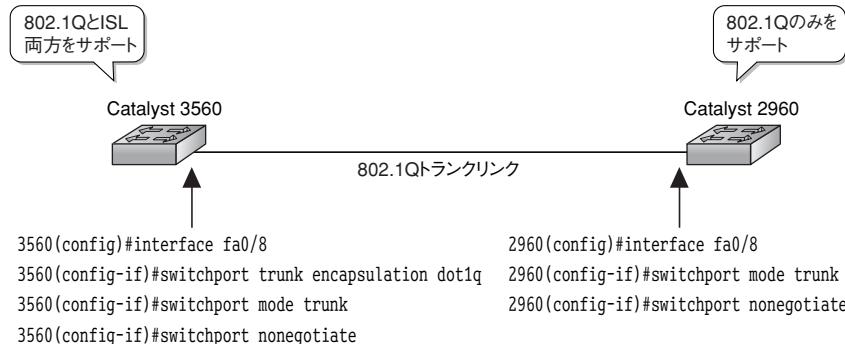
構文 トランкиングプロトコルの指定 (インターフェイスコンフィギュレーションモード)

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

引数	説明
dot1q	IEEE 802.1Qを指定
isl	ISLを指定

IEEE 802.1QとISLの両方のプロトコルをサポートしているスイッチは、先に「トランкиングプロトコルを指定するコマンド」、次に「固定でトランクポートにするコマンド」の順番で実行します。

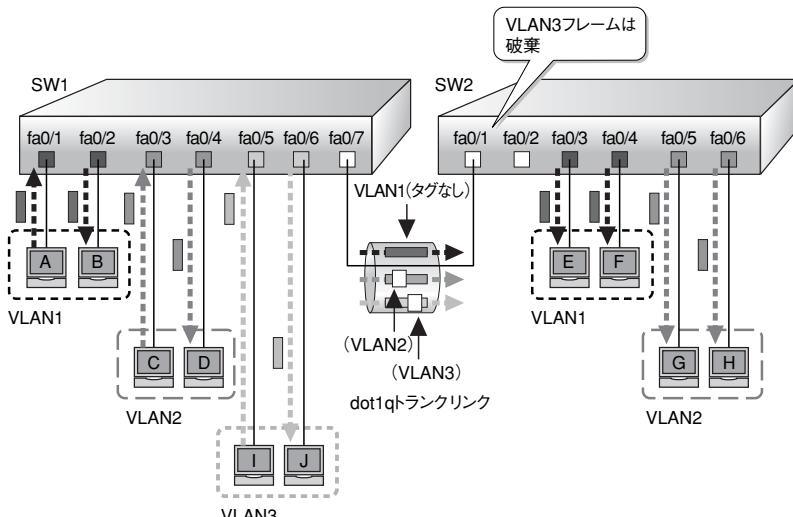
【固定で802.1Qのトランクポートに設定する例】



● allowed VLAN

トランクポートは複数のVLANフレームを転送するポートです。デフォルトでは、トランクが有効になるとスイッチに存在するすべてのVLANが許可されます。したがって、構成によっては不要なフレームもトランク上で転送されてしまいます。

【すべてのVLANに所属するトランクポートの例】



たとえば、前ページの図において2台のスイッチにVLAN1、2、3が存在しているとします。VLAN3に属するホストはSW1にのみ接続されています。トランクポートですべてのVLANが許可されている場合、ホストIが送信したブロードキャストフレームは、VLAN3が属するSW1のfa0/6とfa0/7にフラッディングされます。しかし、SW2ではVLAN3フレームを受信してもVLAN3が属するポートがないため、フレームを破棄するだけです。

トランクポートに不要なVLANフレームを転送させずに、必要なVLANだけを許可する機能を**allowed VLAN**といいます。allowed VLANを設定するには、次のコマンドを使用します。

構文 allowed VLANの設定（インターフェイスコンフィグモード）

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

引数	説明
vlan-id	トランクポートで許可するVLAN IDを指定。「,」(カンマ) や「-」(ハイフン) を使用して複数のVLANを指定可能 例) VLAN1と10と20を指定する場合 : 1,10,20 VLAN1から3を指定する場合 : 1-3

先述のとおり、802.1QトランクポートのネイティブVLANはデフォルトでVLAN1になっています。ネイティブVLANの番号を変更するには、トランクポートのインターフェイスコンフィギュレーションモードから次のコマンドを使用します。

構文 ネイティブVLANの設定（インターフェイスコンフィグモード）

```
(config-if)#switchport trunk native vlan <vlan-id>
```

引数	説明
vlan-id	ネイティブVLANのVLAN IDを指定

Memo allowed VLANの変更

スイッチポートで許可するVLANをあとから追加したり、あるいは削除、変更したりするには、switchport trunk allowed vlanコマンドの後ろに次のオプションを使用します。

引数	説明
add	現在許可されているVLANはそのままで、さらに指定したVLANを追加する
remove	現在許可されているVLANから、指定したVLANを取り除く。ただし、デフォルトVLAN（1、1002～1005）は削除不可
except	指定したVLANを除く、すべてのVLANを許可する（VLANを反転指定する）
all	すべてのVLANを許可する（デフォルト）

たとえば、最初にswitchport trunk allowed vlan 1-3,10を実行し、あとでVLAN20を追加したい場合は、次のようにコマンドを入力します。

```
(config-if)#switchport trunk allowed vlan add 20
```

Memo interface rangeコマンド

複数のスイッチポートに同じパラメータを設定する場合、interface rangeコマンドで専用のモード「(config-if-range)#」に移り、まとめてコマンドを設定することができます。この機能を利用すると、1回のコマンド入力で複数個のスイッチポートに対して同じ設定ができるのでとても便利です。

複数のスイッチポートのモードに移るには、グローバルコンフィギュレーションモードからinterface rangeコマンドを入力し、通常のポート指定のあとに「-」（ハイフン）または「,」（カンマ）を入力してポート番号を指定します。

例) FastEthernet0/1～8の8個のポートを設定する場合

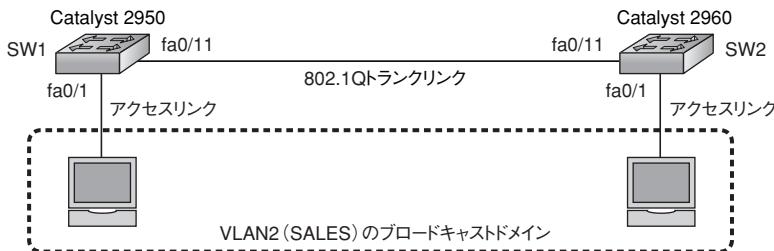
```
(config)#interface range fa0/1-8
(config-if-range) #
```

例) FastEthernet0/1、3、7の3個のポートを設定する場合

```
(config)#interface range fa0/1, fa0/3, fa0/7
(config-if-range) #
```

1-5 VLANの検証

VLANを作成したら、そのVLANが適切に追加されているか確認する必要があります。また、設定を変更した場合も、変更が反映されているか確認しなければなりません。VLANは確認コマンドによって、さまざまな要素を表示することができます。本節では、次の構成を例に、VLANの検証方法を説明します。



■ VLANの確認

スイッチに存在しているすべてのVLANに関する情報を確認するには、`show vlan`コマンドを使用します。

出力の前半には左からVLAN ID、VLAN名、ステータス、およびそのVLANが所属しているアクセスポートが表示されます。後半には、VLANタイプ、FDDIで使用するSAID（セキュリティアソシエーションID）、MTU^{※17}、使用中のSTP^{※18}、およびFDDI*またはトークンリングで使用するパラメータなどが表示されます。なお、`show vlan brief`コマンドを使用すると、前半部分のみを表示することができます。

構文 すべてのVLANの表示（ユーザモード、特権モード）

```
#show vlan [ brief ]
```

※17 【MTU】(エムティーユー) Maximum Transmission Unit：最大伝送ユニット。一度に転送することができるデータの最大値を示す値。単位はバイトで、イーサネットでは1,500バイトが一般的である

※18 【STP】(エスティーピー) Spanning Tree Protocol：スパニングツリープロトコル。フレームのループを回避して冗長ネットワークを維持するレイヤ2プロトコル

【show vlanの出力例】

SW1#show vlan ←すべてのVLAN情報を表示								
VLAN	Name			Status	Ports			
1	default			active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Gi0/1, Gi0/2			
1002	fdci-default			act/unsup	③			
1003	token-ring-default			act/unsup				
1004	fdinnet-default			act/unsup				
1005	trnet-default			act/unsup				
① ②		VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo
						Stp	BrdgMode	Trans1
								Trans2
1	enet	100001	1500	-	-	-	-	0 0
1002	fdci	101002	1500	-	-	-	-	0 0
1003	tr	101003	1500	-	-	-	-	0 0
1004	fdnet	101004	1500	-	-	-	ieee	0 0
1005	trnet	101005	1500	-	-	-	ibm	0 0
④								
Remote SPAN VLANs								
Primary Secondary Type			Ports					

SW1#show vlan brief ←briefキーワードを付加			
VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Gi0/1, Gi0/2
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdinnet-default	act/unsup	
1005	trnet-default	act/unsup	
SW1#			

- ① スイッチに存在しているVLAN ID
- ② VLANの名前
- ③ VLANが所属するアクセスポート（トランクポートは非表示）
- ④ MTUサイズ

VLANを新規作成したら、そのVLANが追加されたことを確認する必要があります。show vlanコマンドの後ろにidまたはnameキーワードを付加することで、特定のVLANに関する情報のみを表示することができます。

構文 特定のVLANの表示（ユーザモード、特権モード）

```
#show vlan [ id <vlan-id> | name <vlan-name> ]
```

引数	説明
vlan-id	VLAN ID（番号）を指定
vlan-name	VLAN名を指定。英字は大文字と小文字が区別される

【VLANの作成】

```
SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#vlan 2      ←VLAN2を新規作成
SW1(config-vlan)#end
SW1#
3d15h: %SYS-5-CONFIG_I: Configured from console by console
SW1#show vlan ?
  brief      VTP all VLAN status in brief
  id         VTP VLAN status by VLAN id
  ifindex    SNMP ifIndex
  internal   VLAN internal usage
  mtu        VLAN MTU information
  name       VTP VLAN status by VLAN name
  private-vlan Private VLAN information
  remote-span Remote SPAN VLANs
  summary    VLAN summary information
  |
  Output modifiers
<cr>
SW1#
```

【作成したVLANの確認（要約表示）】

SW1#show vlan brief

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Gi0/1, Gi0/2
2	VLAN0002	active	
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdдинet-default	act/unsup	
1005	trnet-default	act/unsup	
	Primary Secondary Type		Ports

【作成したVLANの確認（特定のVLANのみ）】

SW1#show vlan id 2 ←VLAN2の情報のみ表示（IDで指定）

VLAN	Name	Status	Ports							
2	VLAN0002	active								
VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
2	enet	100002	1500	-	-	-	-	-	0	0

Remote SPAN VLAN

DisabledSW1#show vlan name VLAN0002 ←VLAN2の情報のみ表示（名前で指定）

VLAN	Name	Status	Ports
2	VLAN0002	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
2	enet	100002	1500	-	-	-	-	-	0	0

Remote SPAN VLAN

Disabled

Primary	Secondary	Type	Ports
---------	-----------	------	-------

SW1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SW1(config)#vlan 2

SW1(config-vlan)#name SALES ←VLANの名前を変更

SW1(config-vlan)#end

SW1#

3d15h: %SYS-5-CONFIG_I: Configured from console by console

SW1#

SW1#show vlan name SALES ←VLAN2の情報のみ表示（名前で指定）

VLAN	Name	Status	Ports
------	------	--------	-------

2	SALES	active	
---	-------	--------	--

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
------	------	------	-----	--------	--------	----------	-----	----------	--------	--------

2	enet	100002	1500	-	-	-	-	-	0	0
---	------	--------	------	---	---	---	---	---	---	---

Remote SPAN VLAN

Disabled

Primary	Secondary	Type	Ports
---------	-----------	------	-------

SW1#

■ VLANメンバーシップの確認

すべてのスイッチポートのVLANメンバーシップを確認するには、先述のshow vlanコマンドを使用します。デフォルトでは、すべてのポートはVLAN1に所属しています。また、show vlanコマンドの「ports」の出力にはアクセスポートだけが表示されます。ただし、show vlan id <vlan-id> およびshow vlan name <vlan-name>コマンドの出力ではアクセスポートとトランクポートの両方が表示されます。

【show vlan briefコマンドの出力例】

```
SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#interfaces fa0/1
SW1(config-if)#switchport access vlan 2 ← VLAN2をメンバーシップする
SW1(config-if)#end
SW1#
3d15h: %SYS-5-CONFIG_I: Configured from console by console
SW1#show vlan brief

VLAN Name                      Status    Ports
-----  -----
1    default                     active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                         Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                         Fa0/10, Gi0/1, Gi0/2
2    SALES                       active    Fa0/1
                                         ↑ VLAN2にメンバーシップされたアクセスポート
1002 fddi-default               act/unsup
1003 token-ring-default         act/unsup
1004 fddinet-default            act/unsup
1005 trnet-default              act/unsup
SW1#
```

■スイッチポートの確認

スイッチポートの設定や動作状況を表示するには、`show interfaces <interface> switchport`コマンドを使用します。このコマンドではアクセスポートとトランクポートの両方の情報が表示されます。また、使用中のトランкиングプロトコルやDTPが有効になっているかなどを確認することもできます。

構文 特定ポートのVLAN情報の表示（ユーザモード、特権モード）

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

【`show interfaces fa0/1 switchport`コマンドの出力例（アクセスポートの場合）】

```
SW1#show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic desirable ← 設定モード (dynamic desirable)
Operational Mode: static access ← 実際の動作モード (アクセスポートとして動作)
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 2 (SALES) ← このポートが所属しているVLANおよびVLAN名
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false

Appliance trust: none
SW1#
```

【show interfaces fa0/11 switchportコマンドの出力例（トランクポートの場合）】

```
SW1#show interfaces fa0/11 switchport
Name: Fa0/11
Switchport: Enabled
Administrative Mode: dynamic desirable ←設定モード (dynamic desirable)
Operational Mode: trunk ← 実際の動作モード (トランクポートとして動作)
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q ←トランкиングプロトコルはIEEE 802.1Q
Negotiation of Trunking: On ←DTPネゴシエーションが有効
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default) ←ネイティブVLANは1
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false

Appliance trust: none
SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#interfaces fa0/11
SW1(config-if)#switchport mode trunk ←モードを固定でトランクに設定
SW1(config-if)#switchport nonegotiate ←DTPを停止
SW1(config-if)#end
SW1#
SW1#show interfaces fa0/11 switchport
Name: Fa0/11
Switchport: Enabled
Administrative Mode: trunk ←設定モード (トランクに固定)
Operational Mode: trunk ← 実際の動作モード (トランクポートとして動作)
Administrative Trunking Encapsulation: dot1q
```

```

Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off ←DTPネゴシエーションが無効
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
<以下省略>

```

■ トランクポートの要約情報の確認

show interfaces <interface> trunkコマンドは、トランクポートに関する要約情報を表示します。この出力では、トランクリンク上で実際に転送可能なVLANフレームを確認することができます。

【show interfaces fa0/11 trunkコマンドの出力例】

```

SW1#show interfaces fa0/11 trunk

  Port        Mode         Encapsulation  Status        Native vlan
Fa0/11      on          802.1q          trunking      1
             ↑           ↑             ↑           ↑
             ①          ②            ③          ④

  Port        Vlans allowed on trunk
Fa0/11      1-4094      ← ⑤

  Port        Vlans allowed and active in management domain
Fa0/11      1-2          ← ⑥

  Port        Vlans in spanning tree forwarding state and not pruned
Fa0/11      1-2          ← ⑦
SW1#

```

- ① ポート番号を表示
- ② 設定されているモードを表示（固定のtrunkの場合「on」、accessの場合「off」）
- ③ トランкиングプロトコルを表示（DTPによってダイナミックに設定された場合「n-802.1q」と表示）
- ④ トランク状況を表示（非トランクの場合は「not-trunking」と表示）
- ⑤ トランクリンク上で許可されたVLAN（デフォルトではすべてのVLANを許可）
- ⑥ トランクリンク上で現在アクティブなVLAN
- ⑦ トランクリンク上で実際に転送可能なVLAN

1-6 VTP

VTPは、VLANのメンテナンスを容易にするシスコ独自のVLAN管理プロトコルです。VTPではVLAN情報を管理ドメインに属する複数のCatalystスイッチで同期させることでVLANの整合性を維持します。

■ VTPの概要

VTP (VLAN Trunking Protocol) は、トランクリンクで接続された複数のスイッチとVLAN情報を同期するシスコ独自のプロトコルです。VLANが複数のスイッチにまたがって構成される場合、各スイッチで同じVLAN情報を管理する必要があります。大規模なスイッチドネットワークにおいて一貫したVLAN情報を維持することは、ネットワーク管理者にとって容易な作業ではありません。

VTPを使用すると、管理者はVLAN設定を1台のスイッチ上だけで実行すれば済むため、作業を簡略化することができ、VLANの追加・削除・名前変更などを繰り返してもVTP管理ドメインのすべてのスイッチでVLAN設定の整合性を維持することができます。

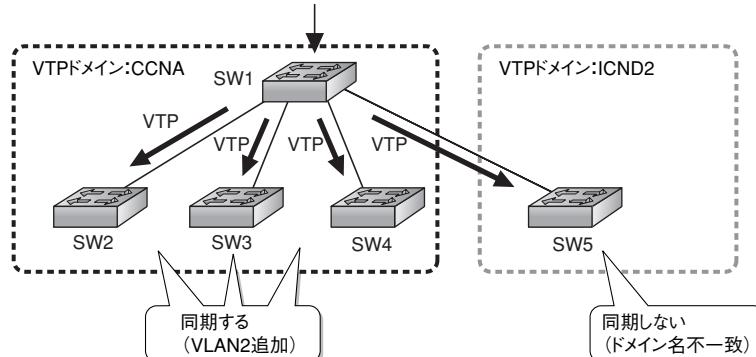
VTPでは、VTPアドバタイズメントがトランクポートにのみ伝搬されるため、管理ドメイン内のスイッチはトランクリンクで接続されている必要があります。トランクングプロトコルは、IEEE 802.1QとISLの両方をサポートしています。

■ VTPドメイン

同じVTP環境を共有している複数のスイッチをVTPドメインといいます。Catalystスイッチは1つのVTPドメインにのみ所属することができ、受信したVTPアドバタイズメントに含まれるドメイン名が自身と異なる場合は同期しません。

【VTPドメイン】

```
SW1(config)#vlan 2
SW1(config-vlan)#name SALES
```



※スイッチ間はすべてトランクリンク

■ VTPモード

VTPには、サーバ、クライアント、トランスペアレント（透過）の3種類の動作モードがあり、Catalystスイッチはいずれか1つのモードで動作します。各モードの特徴は、次のとおりです。

● サーバモード（デフォルト）

サーバモードは、VLANの作成、変更、削除ができるデフォルトのモードです。

設定したVLAN情報は、VTPアドバタイズメントによって通知します。また、同じVTPドメイン内のスイッチが生成したVTPアドバタイズメントを受信した場合は自身でも同期し、さらにはほかのスイッチに転送します。

● クライアントモード

クライアントモードでは、自身ではVLANの作成、変更、削除はできませんが、VLANデータベースにある任意のVLANをアドバタイズすることは可能です。

受信したVTPアドバタイズメントによって同期し、さらにはほかのスイッチに転送します。

● トランスペアレント（透過）モード

トランスペアレントモードでは、VLANの作成、変更、削除ができますが、それをほかのスイッチに通知しません。VTPアドバタイズメントを受信すると、同期せずにほかのスイッチに転送します。

トランスペアレントモードのスイッチは、ほかのスイッチとVLAN情報を共有せず、ローカルで使用するVLANを作成することも、ほかのスイッチと同じVLANを作成することも可能です。VTPを使用せずに、各スイッチでVLANを設定する場合は、トランスペアレントモードに設定します。

Point VTPモード

VTPモードの特徴をまとめると、次のようにになります。

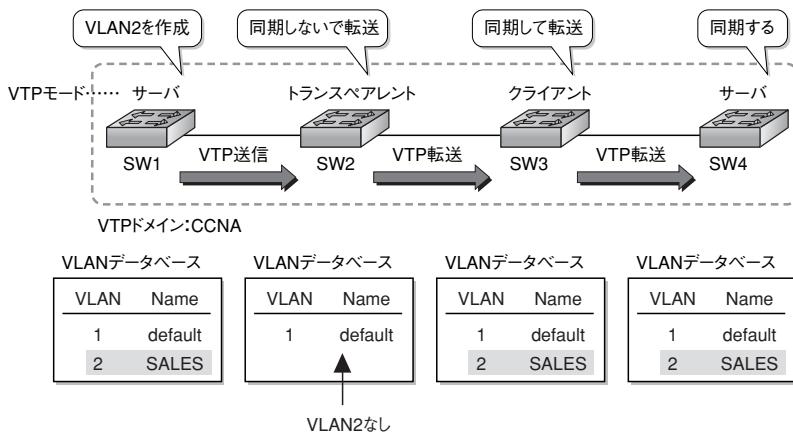
【VTPモードの特徴】

VTPモード	サーバ	クライアント	トランスペアレント
VLAN作成・変更・削除	○	×	○
VTPアドバタイズの転送	○	○	○
同期	○	○	×

※デフォルトはサーバモード

次の図の例では、トランスペアレントモードのSW2では、VLAN情報を作成する機能がないためVLAN2が追加されません。SW1とSW3（またはSW4）でVLAN2に所属するノードが存在する場合、SW2でもVLAN2を作成する必要があります。

【VTPモードの動作】



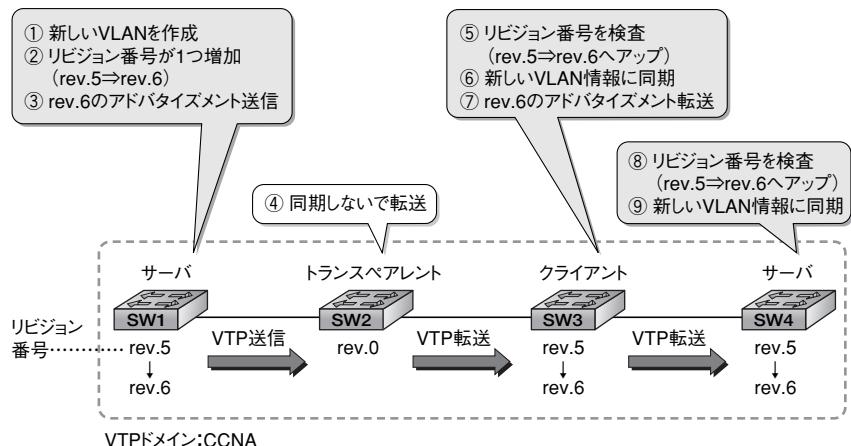
■ VTPのコンフィギュレーションリビジョン番号

VTPアドバタイズメントは、定期的（デフォルトは5分間隔）、あるいはVLAN設定が変更されたタイミングで管理ドメイン内にフラッディングされます。VTPアドバタイズメントは、レイヤ2マルチキャストフレームを使用してトランクリング上にVLAN1で送信されます。

VTPで最も重要な要素にコンフィギュレーションリビジョン番号があります。このリビジョン番号は、VTPアドバタイズメントによって通知されたVLAN情報が最新であるかを識別するためのものです。初期設定は「0」で、サーバモードのスイッチがVLAN情報を変更するたびに1つ増加し、VTPアドバタイズメントで通知されます。ほかのスイッチは自身が保存しているリビジョン番号より数値が大きい場合、最新の情報だと判断してVLAN設定を新しい情報に書き換えます。

なお、トранスペアレントモードのスイッチはVLAN情報を同期しないため、受信したVTPアドバタイズメントのVLAN情報が最新かどうか判断する必要がありません。そのため、トランスペアレントモードで動作するスイッチのコンフィギュレーションリビジョン番号は常に「0」に設定されます。

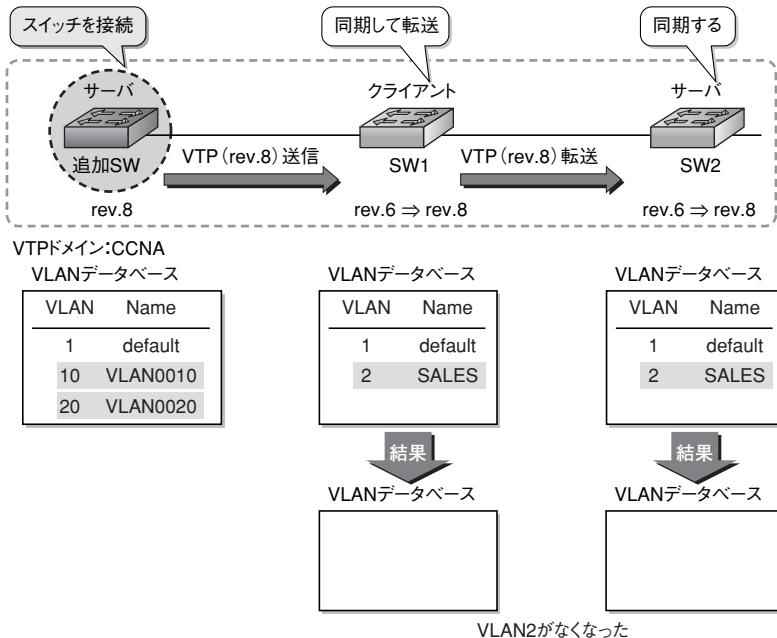
【VTPのコンフィギュレーションリビジョン番号】



Memo コンフィギュレーションリビジョン番号の注意

既存のVTPドメイン環境にスイッチを新しく接続する場合、追加スイッチがサーバモードでリビジョン番号が既存VTPドメインの番号よりも大きいと、追加スイッチが持つVLAN情報に同期し、デフォルトVLANを除くすべてのVLAN情報を失う危険性があります。

【追加スイッチがサーバモードでリビジョン番号が大きい場合】



追加スイッチがクライアントモードでも、保存しているリビジョン番号が大きい場合は、追加スイッチのVLAN情報をアドバタイズするため、誤ってVLANが消去されることがあります。

以上のような問題を回避するには、既存VTPドメインにスイッチを接続する場合、追加スイッチのVTPモードをいったんトランスペアレントモードにしてリビジョン番号を「0」にし、その後、サーバまたはクライアントモードに設定してリビジョン番号をリセットします。また、VTP管理ドメインにはオプションでパスワードを設定することができます。パスワードを設定した場合、受信したVTPアドバタイズメントに含まれるVTPドメイン名とパスワードの両方が自身の保持する設定と一致しない限り、VLAN情報を同期しません。パスワードを利用して同期するための条件を厳しくすることで、新しく追加したスイッチによってVLAN情報を失う危険性を減少させることができます。

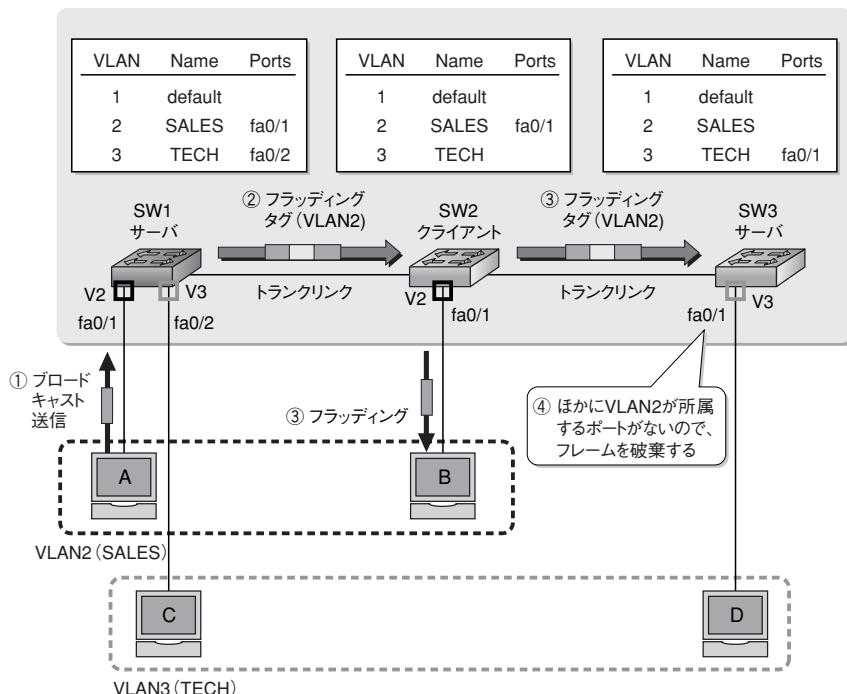
■ VTPプルーニング

VTPプルーニングは、必要なVLANからのトラフィックだけをトランクリンク上にフラッディングさせる機能です。VTPプルーニングを使用すると、動的にallowed VLAN設定と同等の機能を提供し、管理者に負担をかけずにトランクリンク上の利用可能な帯域幅を増加します。ただし、デフォルトVLAN（VLAN1およびVLAN1002～1005）はプルーニングの対象外です。

次の図では、VTP プルーニングが無効になっているため、トランクポートはすべての VLAN トランクの転送が許可されています。

【VTPプルーニング無効の場合】

VTPドメイン:CCNA



- ① ホストAがブロードキャストフレームを送信したとします。
 - ② SW1はfa0/1（アクセスポート：VLAN2）でブロードキャストフレームを受信し、トランクリング上にフラッディングします。
 - ③ このブロードキャストフレームを受信したSW2は、fa0/1（アクセスポート：VLAN2）とトランクポート上にフラッディングします。

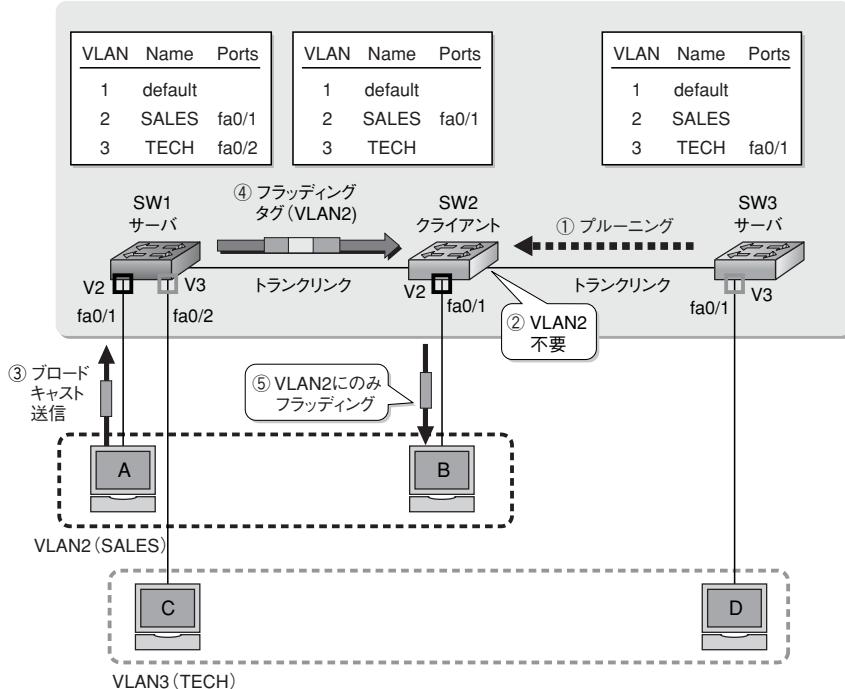
- ④ さらにブロードキャストフレームを受信したSW3は、受信したポート以外にVLAN2が所属するアクセスポートやトランクポートが存在しないため、ブロードキャストフレームを破棄します。

以上のように、VTPを利用してVLAN情報を同期しても、スイッチにすべてのVLANが所属するアクセスポートが存在するとは限らないため、トランクリンク上に不要なフレームがフラッディングされてしまいます。

サーバモードで動作する1台のスイッチ（SW1またはSW3）でVTPプルーニングを有効にし、管理ドメイン内に伝搬された場合は、次のようにになります。

【VTPプルーニング有効の場合】

VTPドメイン:CCNA



- ① SW3はVLAN2のフレームが不要であることをVTPプルーニングメッセージでSW2へ通知します。
- ② プルーニングメッセージを受信したSW2は、受信したトランクポートの先ではVLAN2のフレームが不要だと認識します。
- ③ ホストAがブロードキャストフレームを送信したとします。
- ④ SW1はfa0/1（アクセスポート：VLAN2）でブロードキャストフレームを受信し、ト

トランクリンク上にフラッディングします。

- ⑤ このブロードキャストフレームを受信したSW2は、fa0/1（アクセスポート：VLAN2）にフラッディングしますが、SW3の方向へフラッディングしません。その結果、不要なVLANからのフラッディングがなくなるため、トランクリンク上の帯域幅を有効利用することができます。

なお、SW3にVLAN2のアクセスポートが追加された場合、SW3はVLAN2のVTPプルーニングを解除するためのメッセージを通知します。

VTPプルーニングを利用すると、スイッチのアクセスポートの状況に応じて動的にトランクリンク上の不要なフラッディングを防ぐことができます。

Point VTPアドバタイズメントに含まれる情報

VTPアドバタイズメントには次の情報が含まれています。

- ・ VTPドメイン名
- ・ VTPパスワード
- ・ コンフィギュレーションリビジョン番号
- ・ VLAN情報

VTPアドバタイズメントには、VTPモードとVLANメンバーシップに関する情報は含まれないことに注意してください。

Memo VTPバージョン

VTPには1～3の3つのバージョンがあり、デフォルトではバージョン1に設定されています。バージョン2ではトーカンリングのサポート機能が追加されていますが、それ以外に大きな違いはありません。トーカンリング環境でVTPを使用する場合はバージョン2に変更する必要があります。

現在主流のVTPバージョンは1および2です。バージョン1および2でサポートするVLAN番号は1～1005の範囲です。1006～4094の拡張範囲のVLANを使用する場合には、トランスペアレントモードに設定する必要があります。

VTPバージョン3では、1006～4094の拡張VLANをサポートしています。ただし、VTPバージョン3は、現時点ではCatalyst OS（非IOS）を実行するCatalystスイッチでのみ使用可能です。

1-7 VTPの設定

VTPでは、ドメイン名やVTPモード、パスワードなど多くの設定事項があります。本節では、「1-6 VTP」で解説したVTPのさまざまな機能の設定コマンドについて説明します。

■ VTPドメイン名の設定

VTPドメイン名は大文字と小文字を区別します。いったんドメイン名を設定すると、削除することはできません。ドメイン名の変更のみ可能です。

VTPドメイン名を設定するには、**vtp domain**コマンドを使用します。

構文 VTPドメイン名の設定（グローバルコンフィグモード）

(config)#**vtp domain <domain-name>**

引数	説明
domain-name	VTPドメイン名を32文字以内で指定

※デフォルトは設定されていない

■ VTPモードの設定

すべてのCatalystスイッチのデフォルトのVTPモードはサーバモードになっています。VTPモードを設定するには、以下のコマンドを使用します。

構文 VTPモードの設定（グローバルコンフィグモード）

(config)#**vtp mode { server | client | transparent }**

■ VTP/パスワードの設定

VTPパスワードも大文字と小文字を区別します。パスワードはオプション機能であるため、設定をしない場合でもVTPの動作に問題はありません。VTPパスワードの設定は**vtp password <password>**コマンドを使用します。パスワードを消去する場合は、**no vtp password**を使用します。

構文 VTP/パスワードの設定（グローバルコンフィグモード）

(config)#**vtp password <password>**

引数	説明
password	VTP/パスワードを32文字以内で指定（オプション）

■ VTPプルーニングの設定

VTPプルーニングの設定は、VTP管理ドメイン内のサーバモードで動作する1台のスイッチで設定します。クライアントモードのスイッチでプルーニングを設定することはできません。

サーバモードのスイッチ上でVTPプルーニングを有効または無効にすると、管理ドメイン全体に伝搬され、ほかのスイッチ（サーバまたはクライアント）上でも同じ設定になります。デフォルトの設定は、Catalyst製品によって異なります。VTPプルーニングの設定をするには、以下のコマンドを使用します。

構文 VTPプルーニングの有効化（グローバルコンフィグモード）

```
(config)#vtp pruning
```

構文 VTPプルーニングの無効化（グローバルコンフィグモード）

```
(config)#no vtp pruning
```

■ VTPバージョンの設定

IOSソフトウェアを実行するCatalystスイッチがサポートしているVTPバージョンは1と2です。デフォルトではバージョン1に設定されています。トータルリンク環境でVTPを使用する場合には、VTPバージョンを2に変更する必要があります。VTPバージョンは、1台のサーバモードのスイッチで設定し、管理ドメイン全体に通知します。

VTPバージョンを設定するには、以下のコマンドを使用します。

構文 VTPバージョンの設定（グローバルコンフィグモード）

```
(config)#vtp version <1 | 2>
```

Memo vlan.dat

VLANおよびVTPの設定は、フラッシュメモリ内にvlan.datというファイル名で格納されます。したがって、Catalystスイッチをファクトリーデフォルト（工場出荷時）の状態に戻すには、次の2つの作業が必要です。

構文 NVRAMのstartup-configの消去（特権モード）

```
#erase startup-config
```

構文 フラッシュメモリのvlan.datの消去（特権モード）

```
#delete flash:vlan.dat
```

【Catalystスイッチの初期化】

```
SW1#erase startup-config      ← startup-configを消去
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]      ← [Enter]キー
[OK]
Erase of nvram: complete
SW1#show startup-config      ← startup-configが消去されたことを確認
startup-config is not present
SW1#delete flash:vlan.dat    ← vlan.datを消去
Delete filename [vlan.dat]?  ← [Enter]キー
Delete flash:vlan.dat? [confirm]  ← [Enter]キー
SW1#show flash:      ← vlan.datが消去されたことを確認

Directory of flash:/
2 drwx      512  Mar 1 1993 00:10:32 +00:00  c2960-lanbase-mz.122-35.SE5

27998208 bytes total (19301888 bytes free)
SW1#
```

VLAN設定を完全に消去するには、上記作業後にスイッチの電源を切るかスイッチを再起動する必要があります。

1-8 VTPの検証

VTPの設定をしたら、設定が適切に行われているか確認する必要があります。確認コマンドの説明をしながら、VTPモードによる出力結果の違いも見ていきましょう。

■ VTPの確認

VTP設定の状態を確認するには、`show vtp status`コマンドを使用します。この出力では、VTPドメイン名、動作モード、リビジョン番号、プルーニングの状態のほかに、VLANデータベースを最後にアップデートしたスイッチのIPアドレスを確認することもできます。

構文 VTPの確認（ユーザモード、特権モード）

```
#show vtp status
```

以下に、工場出荷時のVTPの状態を示します。

【`show vtp status`コマンドの出力例】

```
SW1#show vtp status
VTP Version : 2 ←VTPバージョン
Configuration Revision : 0 ←リビジョン番号
Maximum VLANs supported locally : 255 ←VTPでサポートしているVLAN数
Number of existing VLANs : 5 ←既存のVLAN数
VTP Operating Mode : Server ←VTPモード（サーバモード）
VTP Domain Name :  ←VTPドメイン名（設定なし）
VTP Pruning Mode : Disabled ←プルーニングは無効
VTP V2 Mode : Disabled ←VTPv2は無効（現在v1を使用）
VTP Traps Generation : Disabled ←トラップ通知は無効
MD5 digest : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47
0xBD
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
                                ↑最後にアップデートしたスイッチ
SW1#
```

※VTPでサポートするVLAN数はスイッチ製品によって異なる

■ VTP/パスワードの確認

オプションでVTPパスワードを設定することができます。スイッチに設定したVTPパスワードを確認するには、次のコマンドを使用します。

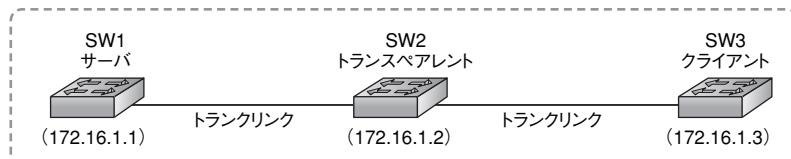
構文 VTP/パスワードの確認（特権モード）

#show vtp password

【show vtp passwordコマンドの出力例】

```
SW1#show vtp password
The VTP password is not configured.      ←VTP/パスワードが設定されていない
SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#vtp password ccna123      ←パスワードを「ccna123」に設定
Setting device VLAN database password to ccna123
SW1(config)#end
SW1#
01:40:49: %SYS-5-CONFIG_I: Configured from console by console
SW1#show vtp password
VTP Password: ccna123      ←VTP/パスワードが「ccna123」に設定された
```

次に、以下の構成で、VTP ドメイン名をCCNAに、VTP パスワードをccna123に設定した場合の出力サンプルを示します。



VTPドメイン名:CCNA、VTPパスワード:ccna123

【SW1のVTP設定：サーバモード、ドメイン名：CCNA、パスワード：ccna123】

```

SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#vtp domain CCNA
Changing VTP domain name from NULL to CCNA
SW1(config)#vtp password ccna123
SW1(config)#end
01:14:13: %SYS-5-CONFIG_I: Configured from console by console
SW1#show vtp status
VTP Version : 2
Configuration Revision : 0      ←初期のリビジョン番号
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode : Server   ←デフォルトの動作モード
VTP Domain Name : CCNA      ←VTPドメイン名
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled      ←バージョン1で動作
VTP Traps Generation : Disabled
MD5 digest : 0x51 0x47 0xB3 0x3F 0x53 0x47 0x00 0xE9
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 172.16.1.2 on interface Vl1 (lowest numbered VLAN interface found)
SW1#show vtp password
VTP Password: ccna123      ←VTPパスワード
SW1#

```

【SW2のVTP設定：トランスペアレントモード、ドメイン名：CCNA、パスワード：ccna123】

```
SW2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW2(config)#vtp domain CCNA
Changing VTP domain name from NULL to CCNA
SW2(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
SW2(config)#vtp password ccna123
SW2(config)#end
01:14:13: %SYS-5-CONFIG_I: Configured from console by console
SW2#show vtp status
VTP Version : 2
Configuration Revision : 0 ←リビジョン番号は常に「0」
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode : Transparent ←トランスペアレントモード
VTP Domain Name : CCNA ←VTPドメイン名
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x51 0x47 0xB3 0x3F 0x53 0x47 0x00 0xE9
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
SW2#show vtp password
VTP Password: ccna123 ←VTP/パスワード
SW2#
```

【SW3のVTP設定：クライアントモード、ドメイン名：CCNA、パスワード：ccna123】

```
SW3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW3(config)#vtp domain CCNA
Changing VTP domain name from NULL to CCNA
SW3(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW3(config)#vtp password ccna123
SW3(config)#end
SW3#
00:57:33: %SYS-5-CONFIG_I: Configured from console by console
SW3#show vtp status
VTP Version : 2
Configuration Revision : 0 ←現在のリビジョン番号（SW1と同期）
Maximum VLANs supported locally : 250
Number of existing VLANs : 5
VTP Operating Mode : Client ←クライアントモード
VTP Domain Name : CCNA ←VTPドメイン名
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x51 0x47 0xB3 0x3F 0x53 0x47 0x00 0xE9
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
SW3#show vtp password
VTP Password: ccna123 ←VTPパスワード
SW3#
```