



Cisco Catalyst 9000 シリーズ スイッチ 実践ガイド(基本機能編)

シスコシステムズ合同会社

2020年 1月10日



はじめに

『Cisco Catalyst 9000 シリーズ スイッチ実践ガイド
(基本機能編)』を手にとっていただき、ありがとうございます。

Cisco Catalyst 9000 シリーズを安心して導入できるよう
シスコ SE にて検証した結果をベースに本ガイドを作成しました。

今後の SE ライフにご活用いただけましたら幸いです。



本書でお伝え したいこと

- ✓ 初めて Cisco Catalyst 製品を設定する
- ✓ 既存機器からマイグレーションしたい
- ✓ まずはラボで触ってみたい

本書には、デザイン、コンフィギュレーション、Tips を詰め合わせました。

本書をご利用いただくことにより、価値訴求のポイントが 1 つでも増え、また効率的に構築を進めることができるためのツールとなれば幸いです。

注意事項

- 本書は IOS-XE 16.12.1 をベースにした内容に基づいて作成しています。以降のバージョンで仕様変更などにより実装が異なるケースが発生することもありますので、あらかじめご了承ください。また、最新版に関しましては、リリース ノートやコンフィギュレーション ガイド等を参照いただきますようお願いいたします。
- ラボの検証は IOS-XE 16.9.3 で実施しています。実環境へ導入する際には顧客要件に合わせて十分な検証を行った上で進めるようにしてください。
- 本書で利用されている IP アドレス、パスワード、コミュニティ名などは、適宜変更してご利用ください。

目次 1/2

1 シスコが目指す方向性

1.1 Cisco DNA とは？

1.2 Cisco Catalyst 9000 シリーズ

2 デザイン編

2.1 導入

2.2 要件の整理

2.3 アクセスレイヤの構成

2.4 ディストリビューションレイヤの構成

2.5 コアレイヤの構成

2.6 物理的構成

2.7 論理構成

2.8 LAN 外への接続

2.9 無線 LAN の構成

2.10 IP マルチキャスト

目次 2/2



3 機能編

- 3.1 Stack
- 3.2 IOS Management
- 3.3 Basic L2 / L3
- 3.4 QoS
- 3.5 Security
- 3.6 AVC



4 実装編

- 4.1 デザイン例



5 Cisco DNA 連携編

- 5.1 Cisco DNA 連携ソリューション



6 まとめと今後

- 6.1 まとめと今後

1

シスコが目指す 方向性

1.1 Cisco DNA とは？

1.2 Cisco Catalyst 9000 シリーズ

1.1 Cisco DNA とは ?

これからのネットワークのアプローチ

従来のネットワーク

ハードウェア中心

手動でスキルに依存

継ぎ足しのセキュリティ

ログ分析、事後対応

これからのネットワーク

ソフトウェア中心

自動化

組み込みセキュリティ

リアルタイム分析、
予防的対応

目指す方向性

Cisco DNA = Cisco Digital Network Architecture の略称で SDN の先にある新しいネットワークを実現するアーキテクチャ

見える化 (Assurance)



セキュリティ

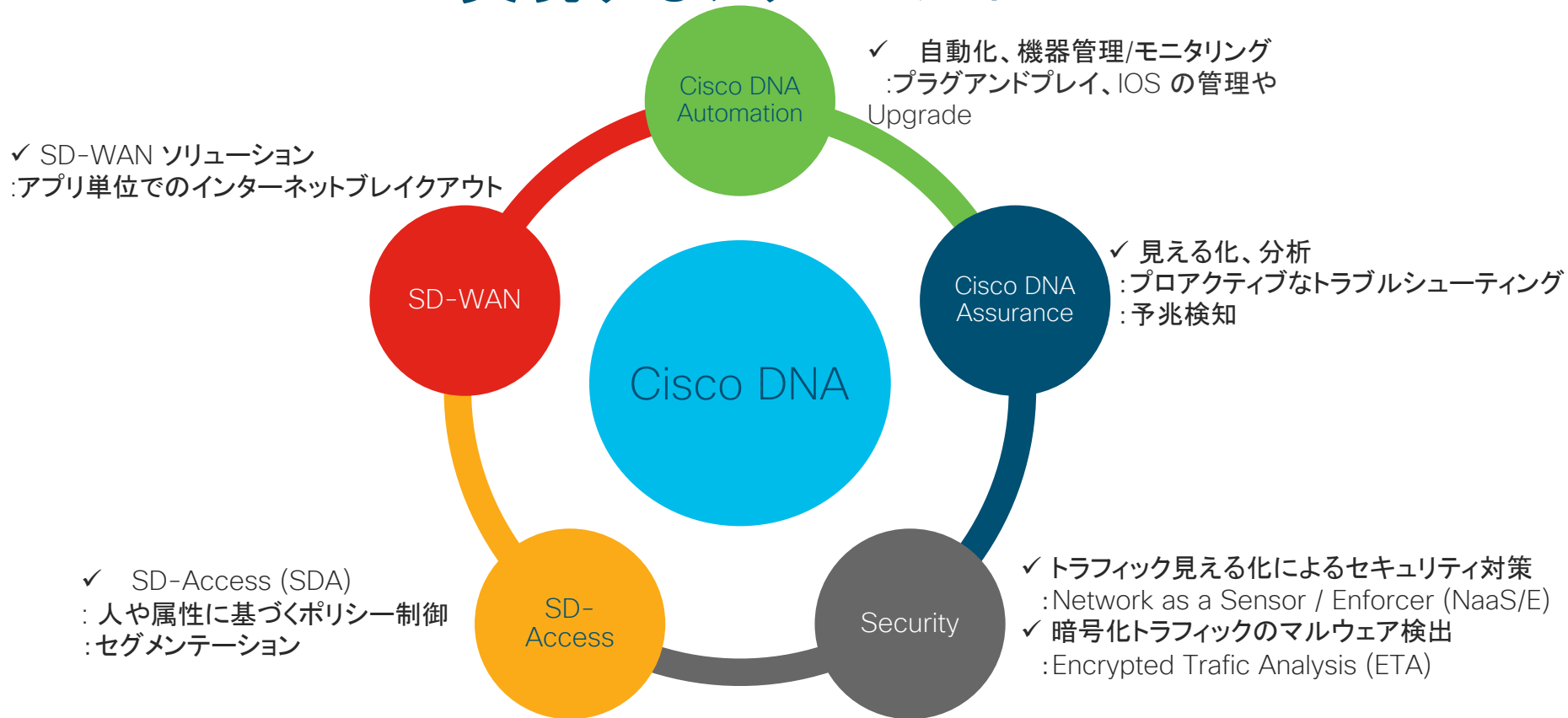


Intent-Based
(意図に応じて操作できる)
Networking

自動化 (Automation)



Cisco DNA で実現するソリューション



1.2 Cisco Catalyst 9000 シリーズ

Cisco Catalyst 9000 プラットフォーム



高い将来適合性



ASIC として業界
最高のプログラム
可能性



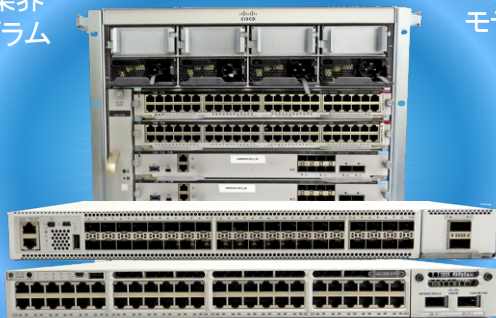
モデル駆動型
API



SNMP に替わる
ストリーミング
テレメトリ



サードパーティの
ツールとも容易に
インテグレーション



クラウド対応



統合されたセキュリティ



Open IOS®XE



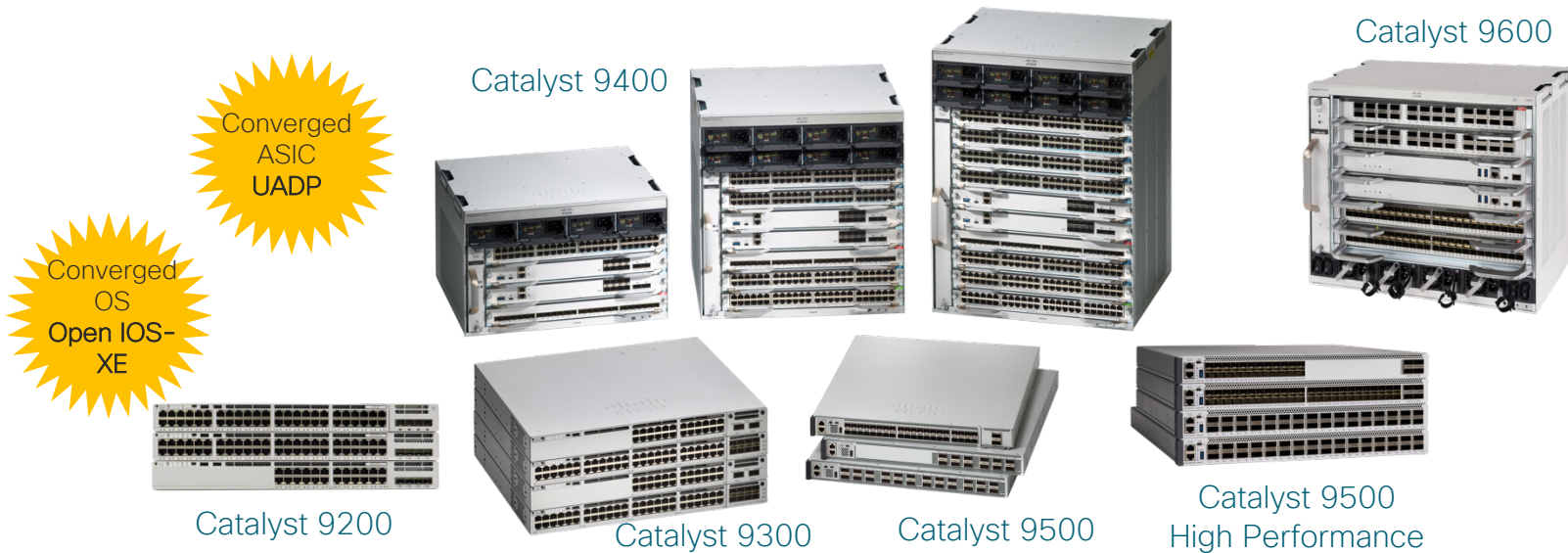
リロードの必要の無
いパッチ対応

Catalyst 9000 プラットフォーム

Intent-based Networks の
基盤

製品ラインナップ

ソフトウェア、ハードウェア アーキテクチャを共通プラットフォーム化



IOS-XE




共通のソフトウェア アーキテクチャ


UADP Family


共通のハードウェア アーキテクチャ


UADP – 革新的な次世代 ASIC




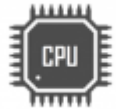
-  Investment Protection
Flexible Pipeline
-  Universal Deployments
Adaptable Tables
-  Enhanced Scale/Buffering
Multicore resource share

 123
384K Flex
Counters

 Shared
Lookup

 Up to 1.6T
Bandwidth

 Up to 2X to 4X
Forwarding + TCAM

 CPU
Embedded
Microprocessors

 Up to 36MB
Packet Buffer

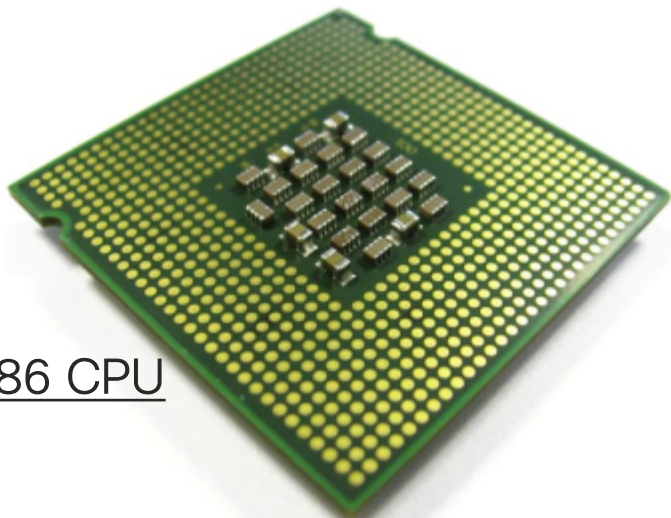
 Up to 64K x2
NetFlow Records

フレキシブル&プログラマブル ASIC – 新しいテクノロジーに適応

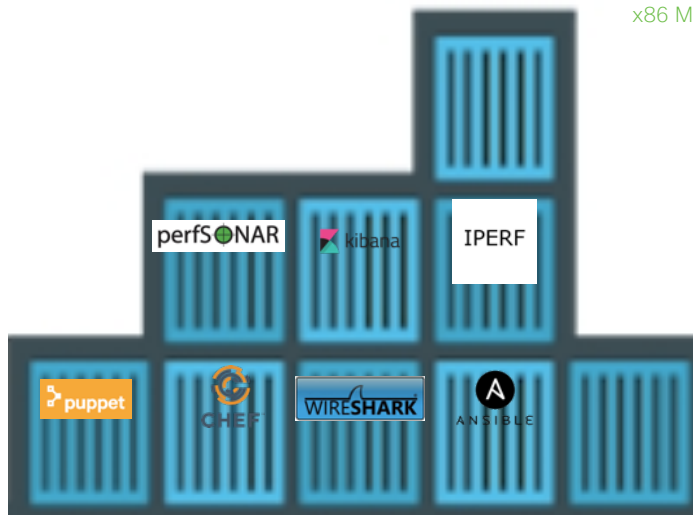
X86 CPU - 3rdパーティ アプリとの親和性



x86 Multi-core CPU



x86 CPU



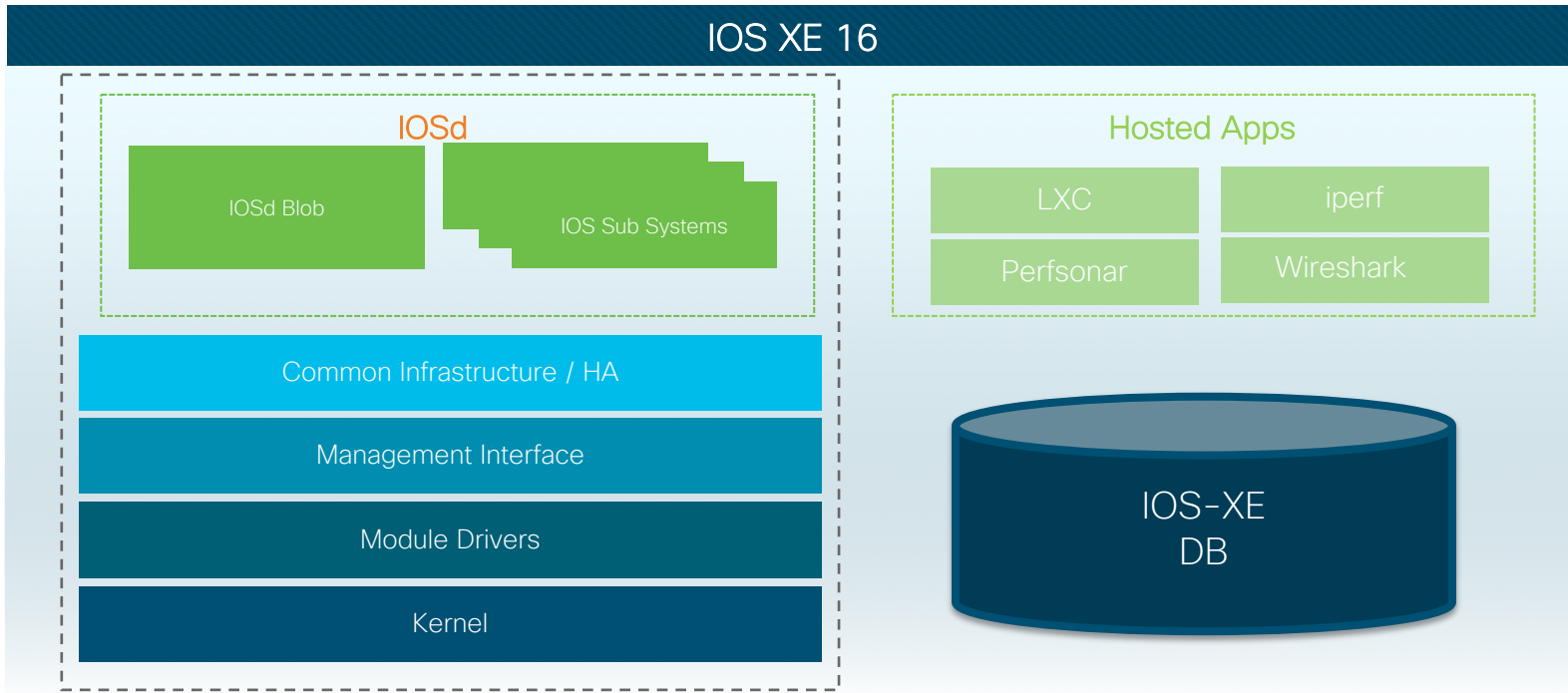
x86 ベースの サードパーティアプリケーション

x86 CPU がホスティング、コンテナ、サードパーティアプリケーションを実現

Open IOS XE - 柔軟なオペレーティング システム



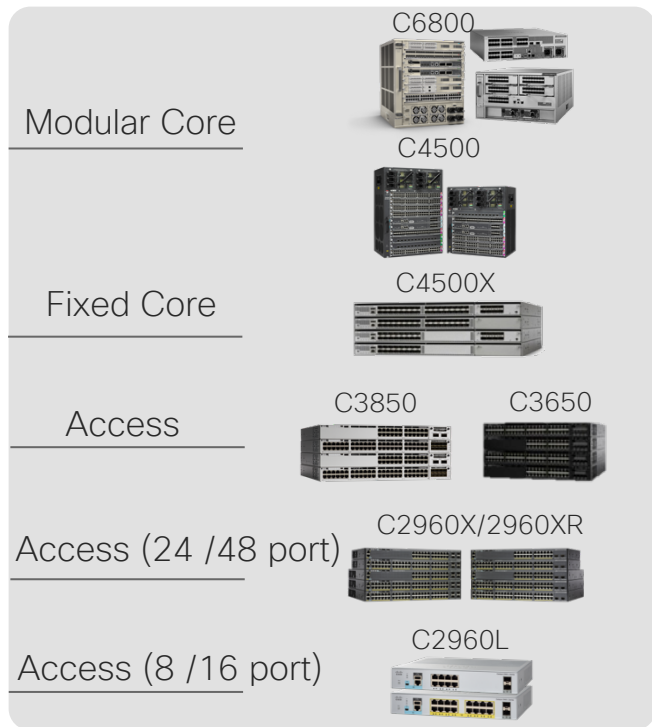
Open and Extensible
IOS-XE



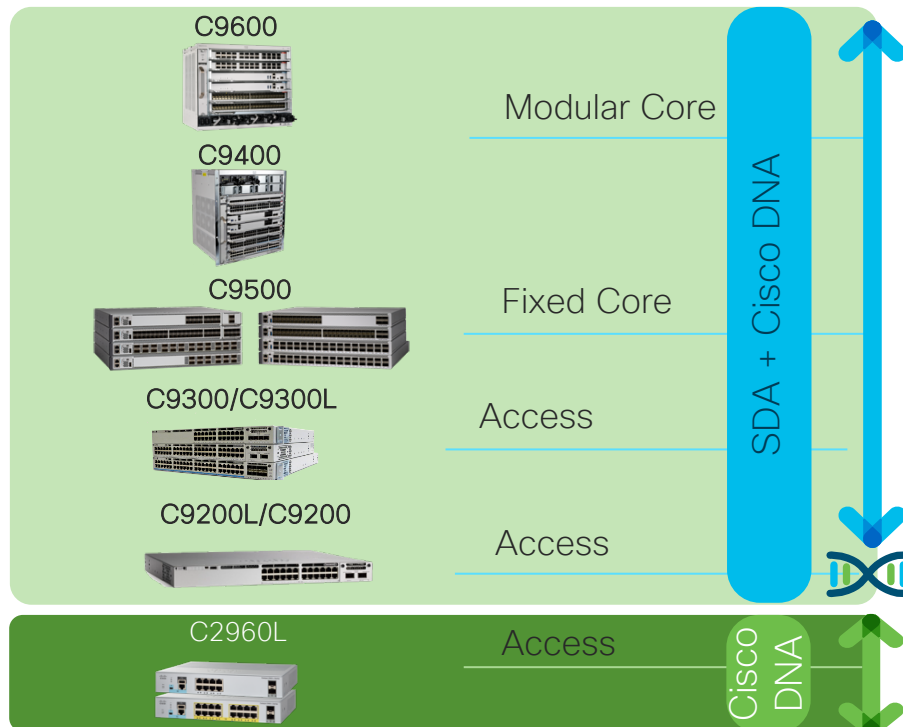
オープン、モデルドリブン、かつセキュア オペレーティング システム

現行機種からのマイグレーションパス

これまで



これから



ライセンス体系

シスコは継続的なビジネスに注力すべく、リカーリング モデルにシフト

従来のライセンス体系

Perpetual (無期限)

IP Services

IP Base

LAN Base



Cisco Catalyst 9000 新しいライセンス体系

Network ライセンス
Perpetual (無期限)

Network
Advantage

Network
Essentials

+

Cisco DNA ライセンス
Subscription (定期契約)

+

Cisco DNA
Advantage

+

Cisco DNA
Essentials

(3 / 5 / 7年間から選択)

2

デザイン編

- 2.1 導入
- 2.2 要件の整理
- 2.3 アクセスレイヤの構成
- 2.4 ディストリビューションレイヤの構成
- 2.5 コアレイアの構成
- 2.6 物理的設定
- 2.7 論理構成

2.1 導入

2.1 導入

LAN デザインのコンセプト

「デザイン」の重要性

Cisco Catalyst 9000 シリーズは、主に企業、組織内の LAN への導入を想定しています。LAN（あるいはキャンパス LAN）は、建物のフロアなど広がりのある空間に分散して配置されたコンピュータなどが接続され、その範囲内や外に対するデータ通信の環境を提供します。企業、組織のネットワークやIT全体の中でも非常に重要な位置づけにあります。

LAN が本来期待される機能、性能と費用対効果を十分に発揮するには、明確な意図と根拠に基づく構成の実施、いわゆるデザインのステップを適切に進める必要があります。ここでいうデザインには、全体的な接続構成、機種選定と台数の確定、接続方式の選択、機能性能を活用するための共通化された設定の確定までを含みます。

これからご紹介するデザインの手法を応用することで、現在と将来の LAN に以下の利点をもたらすことができます。

■ 利点:

- 構築や運用が容易になる
- 将来のネットワーク拡張や更新に対応できる柔軟性があり、重点ポイントを明確化できる(柔軟性)
- 障害発生においても稼働を継続しつつ、高速な回復を行う(高可用性、耐障害性)
- LAN 全体の最大性能と最小コストのバランスを把握(費用対効果の明確化)

本資料では、デザインを行う際に必要となる検討項目の他、Catalyst 9000 シリーズを設定する上で注意すべき点や推奨される設定の内容を、構築の手順に沿ってご紹介します。

2.1 導入

LAN デザインの方針

「デザイン」の手法

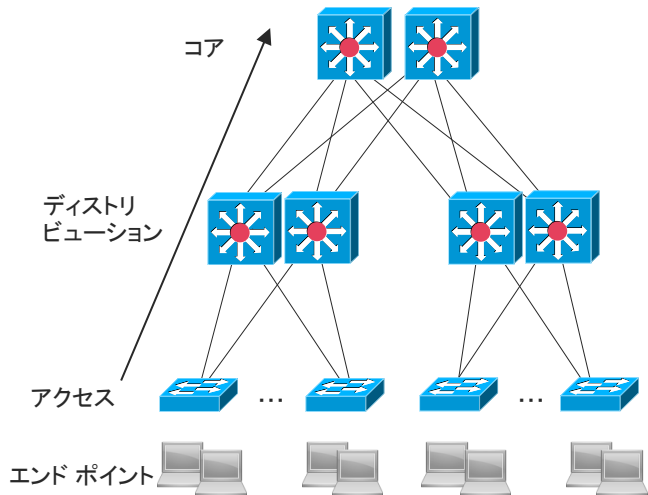
本文書では LAN において必ず基本要件となる「接続される端末(エンドポイント)の種類と数」を起点とし、直接接続されるスイッチの側から構成を順次決定していく、ボトムアップの手順を採用しています。

その理由は、具体的な要件がボトム側、つまり LAN に接続されるエンドポイント側に存在し、エンドポイントに提供するネットワーク サービスという観点から、明確な根拠に基づいたデザインに着手できるためです。また、必然的にスイッチの台数の多くなるボトム側で、必要最低限の機能に絞った機種と台数をいち早く確定できるため、全体コストの抑制のプランが立てやすくなります。

シスコでは、LAN を設計する際に、コア / ディストリビューション / アクセスという 3 つのレイヤを定義し、そのレイヤごとに特定の機能や役割を持たせて、LAN ネットワーク デザインをする「3 階層モデル」を推奨しています。ボトムアップの手順は、まずアクセス レイヤから順にデザインを検討することを意味しています。

次頁で 3 階層モデルのご紹介をします

(注)今回は、エンドポイントは全て有線接続(イーサネット 1000BASE-T)とします。無線 LAN を含むネットワークについては、本文書のデザインを応用しながら無線 LAN デザインの原則に基づいて検討する必要があります。



3 階層モデル

ネットワーク サービスを提供するエンドポイントに近いアクセスレイヤから、要件に基づいて機器やデザインを決定していくボトムアップの手順

2.1 導入

3 階層モデルとは

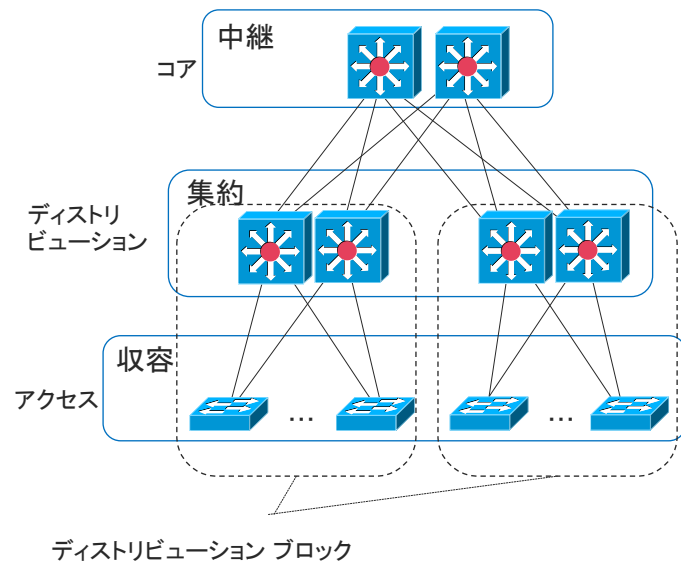
■ LAN を「收容・集約・中継」という役割に従って区分し階層(レイヤ)の概念で整理

- **收容** - **アクセスレイヤ**: 多数のスイッチで構成
エンドポイントが直接接続するインターフェースを提供する。エンドポイント個別の制御等を行う。
このレイヤに属するスイッチを「アクセススイッチ」と呼ぶ。
- **集約** - **ディストリビューションレイヤ**: 冗長化された2台1組で構成、複数を配置
アクセスレイヤからのリンクを集め、まとまった単位(ディストリビューションブロック)を形成する。ブロック内のアクセスレイヤに対しIPルーティングやセキュリティポリシーなどの高度な機能を提供する。
このレイヤに属するスイッチを「ディストリビューションスイッチ」と呼ぶ。
- **中継** - **コアレイヤ**: LAN内に2台
ディストリビューションレイヤを相互接続する。LAN内外へ転送を高速に行う。
このレイヤに属するスイッチを「コアスイッチ」と呼ぶ。

■ 3階層モデルの特徴

- 各階層に特定の機能と役割がある
- 各レイヤごとに設計を行うことで、機能や役割に焦点を当てることができ、設計手順が簡素化される
- 運用、拡張、および管理が容易になる
- 大規模なLAN環境でも、3階層モデルに収束が可能

ただし、小規模なLANや物理的制限がある場合は、単一のディストリビューションブロックのみでコアレイヤがない2階層となることもあります。



3 階層モデル

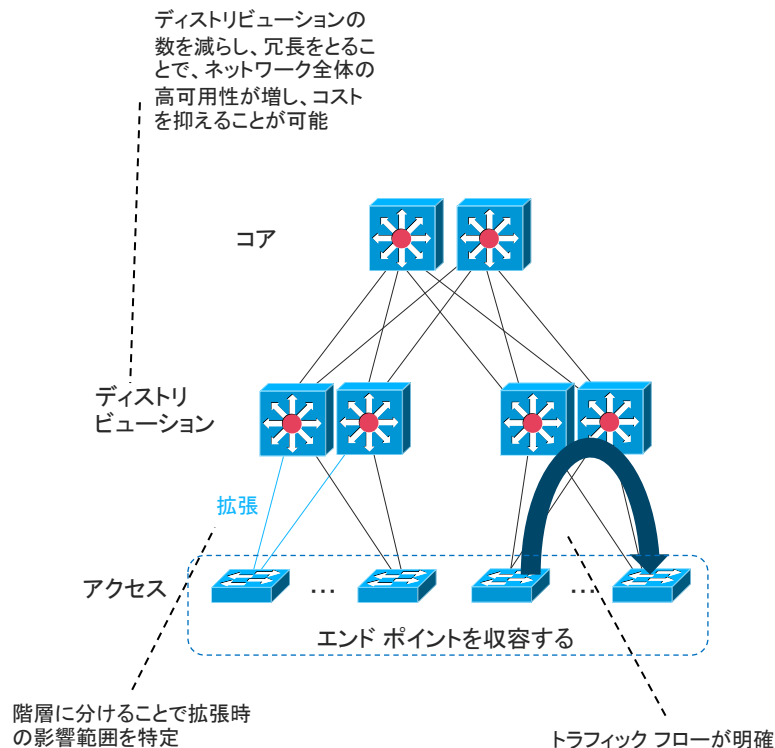
2.1 導入

3 階層モデルの利点

■ 3 階層モデルの採用で得られる利点:

- **コスト削減:**
エンドポイントを安価なアクセススイッチで收容することにより、高度な機能が集中し、高価になりがちなディストリビューションの数を極小化することができ、コスト削減が可能である
- **高可用性:**
ディストリビューション / コアスイッチで冗長を取るなど、集中投資を行うことで、ネットワーク全体の高可用性を実現し、ネットワークに十分な障害対策を盛り込める
- **拡張性/柔軟性:**
拡張の計画を立てやすく、また拡張時の影響範囲の特定が可能である
- **障害の極小化:**
各層で役割を分け、トラフィックフローを明確にすることにより、障害時のネットワーク収束時間を迅速にする

(本文書での Catalyst 9000 シリーズによる LAN 構成は、Cisco DNA のキャンパス ネットワークのソリューションである Cisco SD-Access へ構成を移行する選択肢も取れる構成になっています。その場合、ISE、Cisco DNA Center の各製品と適切なライセンスの追加が必要となります)



2.1 導入

3 階層モデルにおける論理構成の配置

3 階層モデルを最大限に活かす、VLAN と L3 ルーティングの論理構成の配置についてご説明します。

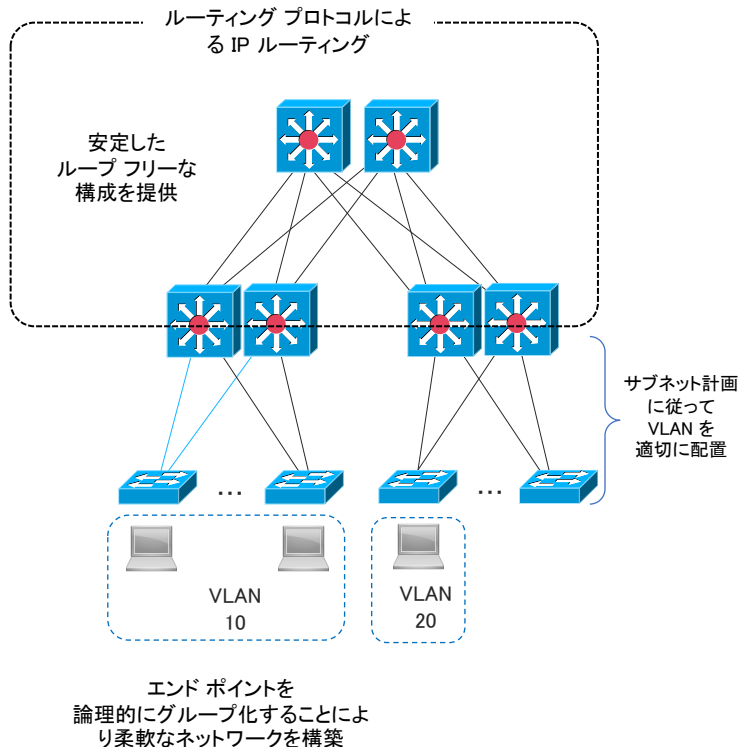
まず、VLAN の柔軟性を活用するため、アクセス-ディストリビューション間で VLAN を適用します。VLAN を利用する理由は、以下の通りです。

- エンド ポイントを論理的にグループ化しネットワークを分割
- ブロードキャストを利用するためルータを配置する必要性なし
- ブロードキャストドメインが限定されトラフィックが削減

次に L3 ルーティングの安定性をディストリビューション-コア間に適用します。

- L3 でネットワーク経路の柔軟で高速な切り替えが可能
- ループフリー構成を確約する L3 ルーティング プロトコル を使用するため、ループ構成について検討する必要なし

3 階層モデルは、デュアル スタック IPv4 IPv6 の環境に対応しています。同じ 3 階層モデルの概念を利用することが可能なため、IPv4 から IPv6 へ移行する場合に構成変更を検討する必要がありません。



2.2 要件の整理

2.2 要件の整理

要件の整理

ネットワークを構成するにあたり、要件を以下の情報を参考にに基づき整理します。
具体的な要件は、ボトムアップでネットワーク構成をデザインするにあたり、LAN ネットワークサービスを提供するエンドポイントから出る、根拠ある大切な情報となります。

まず、ネットワークを提供するネットワーク サービスの要件を確認します。

- 収容するエンドポイントの種類と数（これらの情報よりアクセス スイッチ必要ポート数を算出します）
- セグメンテーション / フィルタリング（同端末でまとめることで、機器に投入する設定の簡素化に繋がります。）
- ユーザと機器に対する認証（認証フローが明確になり、また高額になりがちな必要機能を有するスイッチの減少に繋がります。）
- 機器の配置（物理環境における制約などを考慮します）
- 必要帯域
- コスト計算

次に、ネットワークを提供する場所と対象範囲の確認を行い、構築規模を把握します。距離や広さは機器選定や台数に関わる重要な要件です。

- 拠点の場所と数
- 建屋 / フロア / フロア内エリアの範囲

ご参考: 要件で考慮される設計要素

■ ネットワーク構築の対象となる空間的範囲

- 拠点、建屋、フロア、フロア内エリアなど

■ 提供するネットワーク サービス

- ポートの数
- 通信帯域
- ネットワークのセグメンテーション (分割)
- フィルタリング (どのパケットを通すか)
- 認証の有無、認証方法

■ エンドポイントの種類と台数

- 種類
 - デスクトップ コンピュータ
 - IP 電話
 - ビデオ端末
 - プリンタ
 - カメラなど
- 各々の台数

■ 環境 / 制約条件: スイッチ設置場所を確認

- ワイヤリング クローゼット
- サーバルーム
- ラック構成

■ 環境 / 制約条件: フロア内ケーブリング

- 既設/新設
- スプライス ボックス
- UTP
 - カテゴリ
 - ケーブル長
- パッチパネル

■ 環境 / 制約条件: フロア間ケーブリング

- 既設/新設
- ケーブルの種類 (SMF / MMF / UTP)
 - DSF、NZ-DSF
 - カテゴリ
 - ケーブル長
- スプライス ボックス

2.3 アクセス レイヤ の構成

ケーススタディ（要件定義）

具体的なキャンパス ネットワークの例を 2 つ用いて要件を整理します。

A 構成 小規模構成シナリオ

■ ネットワークを提供するネットワーク サービスの要件

- 収容するエンド ポイントの種類と数(下図参照)
- 必要帯域
 - PC:1G、プリンタ:500K、IP電話:100K

■ 要件 2：ネットワークを提供する場所と対象範囲の確認

- 1ビル 2フロア

2F	250 PC/プリンタ 50 IP電話
1F	250 PC/プリンタ 50 IP電話

B 構成 大規模構成シナリオ

■ ネットワークを提供するネットワーク サービスの要件

- 収容するエンド ポイントの種類と数(下図参照)
- 必要帯域
 - PC:1G、プリンタ:500K、IP電話:100K

■ 要件 2：ネットワークを提供する場所と対象範囲の確認

- ビル1棟 4フロア 1フロアにつき東西エリア

4F	700 PC/プリンタ 80 IP電話
3F	1000 PC/プリンタ 160 IP電話
2F	1000 PC/プリンタ 160 IP電話
1F	400 PC/プリンタ 80 IP電話

2.3 アクセスレイヤの構成

エンドポイントのグループピング

要件より、エンドポイントをグループ分けします。最適なアクセススイッチの機種、台数、收容方法決定のためには、グループ分けをすることが必須です。

グループピングの必要性:

- 最適にエンドポイントをアクセススイッチに配分して收容し、適切な障害範囲の分散を行う
- アクセススイッチに求める機能(例 PoEの有無)の必要台数を明確にでき、スイッチの型番の集約によるコスト削減につながる
- 同じエンドポイントをまとめることにより、スイッチごとの設定パターンの簡素化に繋がり、通信フローが明確になり、障害を起こしにくく、管理しやすいネットワークを実現

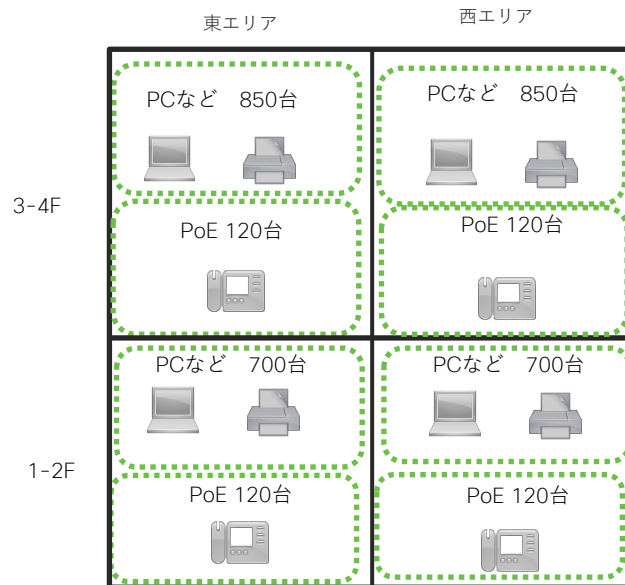
エンドポイントのグループ分け方針は以下の大きく3つに分けて行います。

1. エンドポイントの種類分類
2. 配置する場所
3. 冗長分散

1. エンドポイントの種類分類

設定の簡素化/適切な機能を持つ收容スイッチを選択するため、以下の方針でまとめます。

- 同じエンドポイント種類で統一します。混在させすぎると設定が複雑になるため2種類までが推奨です。
- PoEが必要なエンドポイントはなるべく集約し、PoE型番スイッチの数を極小化しコスト削減します。
- 同じエンドポイント種類は2台以上に分散させます。単一スイッチ障害で同一フロアエリア内のエンドポイントが全断しないようにするためです。



B構成を
エンドポイントの種類(PoEの有無)
配置する場所(1-2F/3-4F)
冗長分散(東・西)
で分配

2.3 アクセスレイヤの構成

グループ化されたエンドポイントを配分

他にもエンドポイントは、様々な分別の要素があります。

- 一般ユーザ / ハイエンドユーザ(広帯域) / 機密情報を扱うユーザ
- IP 電話 (PoE)
- ビデオ会議 (広帯域、QoS を利用)
- プリンタ (バーストラフィックがある)

2. 配置する場所

グループ分けにより、エンドポイントとアクセススイッチの距離を最適化します。

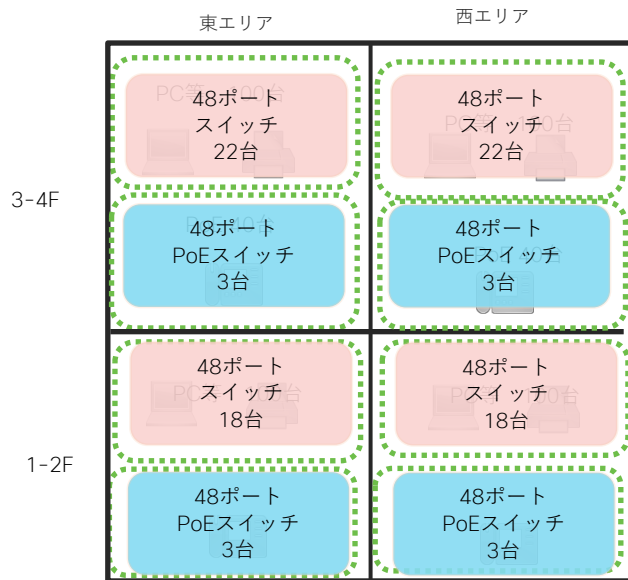
3. 冗長分散

単一スイッチ障害で同一フロア エリア内のエンドポイントが全断を避けるため、グループを分けます。(グループピングの結果例は前頁の図をご参照ください。)

エンドポイントを収容するアクセススイッチのポート数は、以下で想定することを推奨します。

- 24 ポート モデルの場合: 20 ポート収容、4 ポートは予備
- 48 ポート モデルの場合: 40 ポート収容、8 ポートは予備

分別したエンドグループに対し、アクセススイッチを上記の想定収容ポート数で割り当てます。その結果を右図に記載しています。



グループピングをもとにアクセススイッチを選定

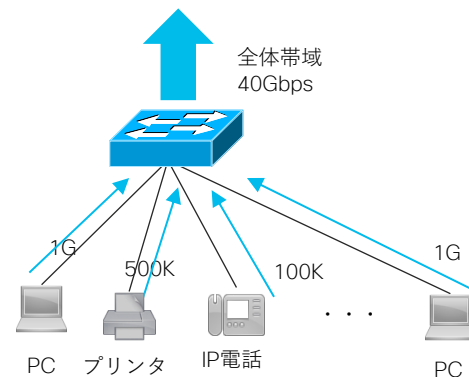
2.3 アクセスレイヤの構成

スイッチごとの全体帯域を算定

エンドポイントグループをアクセススイッチへ配分したことにより、各アクセススイッチのアップリンクで必要な全体帯域量が決定します。

以下のポイントに従い、全体帯域量を決定します。

- エンドポイント毎に必要な帯域量を定める
 - PC :1Gbps
 - IP電話 :100Kbps
 - デスクトップ型ビデオ会議端末 :5Mbps
 - プリンタ :500Kbps
- 時間によるトラフィックの性質の変化を考慮する
 - バースト型：一次的に大量のトラフィックが流れる 例:Webトラフィック
 - リアルタイム型：遅延が許されないトラフィック 例:ビデオ会議
- 将来のネットワーク使い方の変化にも対応できる帯域量を検討する
(QoS を利用しても、ネットワークサービスの品質を保てない状況の想定)
 - ビデオ会議の導入
 - VDI の利用など



2.3 アクセスレイヤの構成

オーバサブスクリプション比からアップリンク帯域を決定

全体帯域を把握できたら、オーバサブスクリプション比の割合を検討し、アップリンクで用意すべき帯域を決定します。

(オーバサブスクリプション比は要件により、エンドポイントグループごとに異なることもあります)。

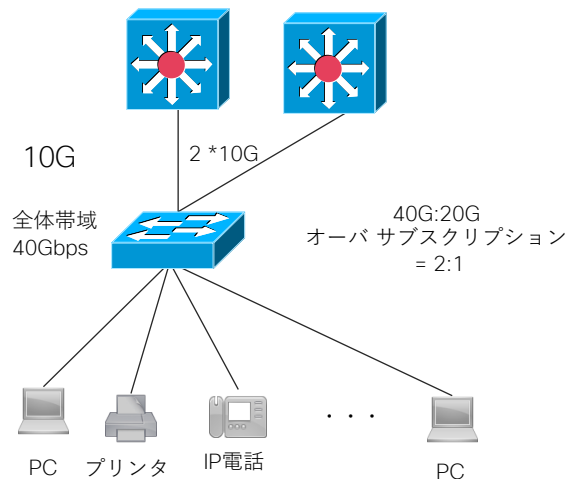
- PCメインの場合は、帯域を重視した1:1のノンブロッキングから、コストを重視した1:20まで要件に合わせて検討可能です。
昔のデザインガイドでは、1:20と記載がありましたが、オーバサブスクリプション比をエンドポイントグループごとに細かく検討し、コスト削減を目指すのは得策ではありません。現在では、帯域当たりのコストは大きく下がってきているためです。(例: 10G)
- 遅延に厳しいIP電話、ビデオ会議端末などはオーバサブスクリプションがない1:1を推奨します。

オーバサブスクリプションが決定したら、アップリンクの帯域を考慮することにより、アップリンクに必要な本数が決定され、具体的なオーバサブスクリプション値も算出できます。

アップリンクの種類別の例は以下の通りです。

- 2/4ポート x 1 / 10G
- (場合によっては2x40Gなど)

以上で、アクセススイッチの必要ポート数やポートの種類、アップリンクに必要な帯域量が決定しました。アクセススイッチの選定において、アップリンクの形状の検討は、ディストリビューションの情報が必要となるため、次の章でご説明します。そのため、本章では、アクセススイッチは仮決定となります。



2.3 アクセスレイヤの構成

ケーススタディ (アクセスレイヤ)

A 構成 小規模構成シナリオ

2F	250 PC/プリンタ 50 IP電話
1F	250 PC/プリンタ 50 IP電話

要件より、エンドポイントのグループ分けを行う。

- ・エンドポイントの種類分類: PoEの有無
- ・配置する場所: 1 / 2F フロア
- ・冗長分散: 有

PoE 無し
500 PC / プリンタ
36 端末 / 1 スイッチ



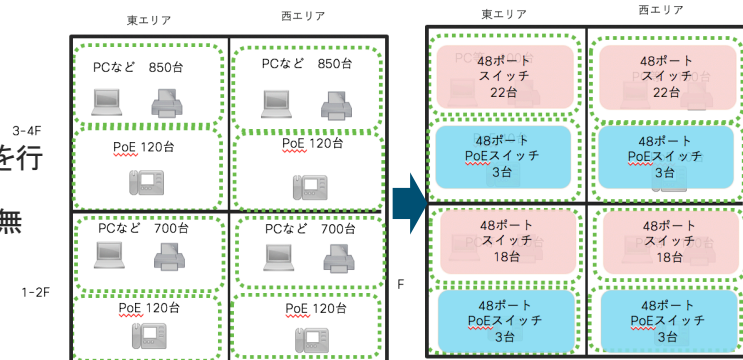
PoE 有り
100 IP電話
25 端末 / 1 スイッチ



B 構成 大規模構成シナリオ

要件より、エンドポイントのグループ分けを行う。

- ・エンドポイントの種類分類: PoEの有無
- ・配置する場所: 1-2F 東/西 フロア
3-4F 東/西 フロア
- ・冗長分散: 有



18 * 48ポートスイッチ

1-2F 東



3 * 48ポートPOEスイッチ

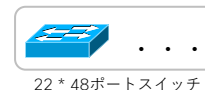


18 * 48ポートスイッチ

1-2F 西

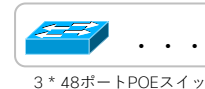


3 * 48ポートPOEスイッチ

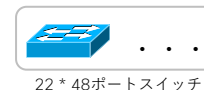


22 * 48ポートスイッチ

3-4F 東



3 * 48ポートPOEスイッチ



22 * 48ポートスイッチ

3-4F 西



3 * 48ポートPOEスイッチ

2.4 ディストリビューションレイヤの構成

アクセスレイヤからのアップリンク総数のまとめと集約単位

ディストリビューションでは、アクセスレイヤからの様々なアップリンク種類を集約し、コアに渡します。既設配線を用いる場合は、ディストリビューションスイッチの設置場所や、その条件を考慮する必要があります。

■ エンドポイントによりオーバーサブスクリプションは異なる

同じ LAN ネットワーク デザインの中でも、エンドポイントのグループごとに求められる帯域条件(オーバーサブスクリプション比)はそれぞれ異なる事があります。一般的なエンドポイントに比べて、広帯域が求められるエンドポイントは、オーバーサブスクリプション比率の低い値(1:1-2:1)が求められます。

■ 将来の拡張について

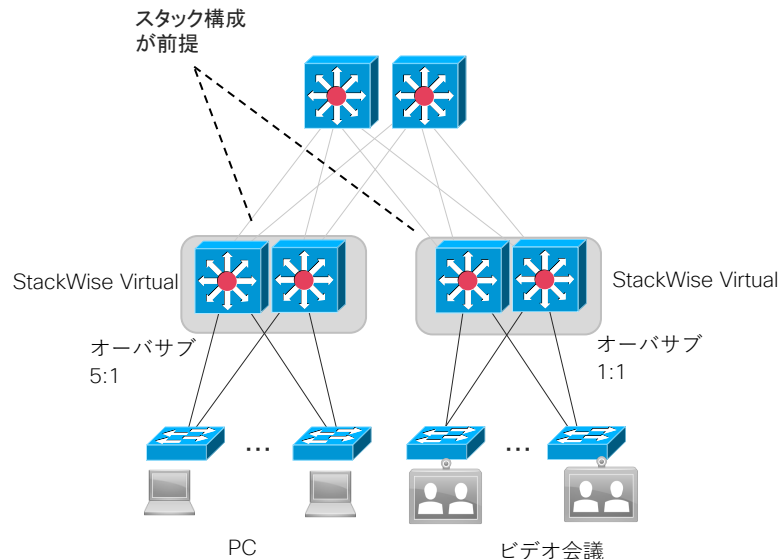
アクセススイッチの拡張や、アクセススイッチのアップリンクの帯域増強を考慮する必要があります。トランシーバを交換することによって、1G から10G、40G へ帯域を増強する方法は、管理や作業が簡単であり推奨です。

■ スタック技術の活用

ディストリビューションスイッチは、StackWise、StackWise Virtual の活用を前提とします。ディストリビューションが1台の論理スイッチとして動作するメリットは、「2.6 物理的設定」章に記載しています。

• StackWise Virtual とは

Stack ケーブルを利用せず、従来のポートを使用して StackWise を実現する機能です。そのため、StackWise Virtual 用のインタフェースを別途確保する必要があります。必要インタフェースや数は「3.1 Stack」章内の「StackWise Virtual」項目に記載しています。



アクセス – ディストリビューション間接続を決定

アクセスからディストリビューション間の接続方式を決めます。これによりアクセスのアップリンク方式が決定し、アクセス スイッチの機種が決定します。

必要な帯域量を確認した後、距離、メディア(ケーブル)、接続方式を決定します。(必要帯域はアクセスの章で決定しています)。

- 距離は、フロア間配線、フロア内配線、室内配線 等、必要な距離により用いるメディアや接続方式が異なります。
- メディア(ケーブル)は、既設配線または新規配線のどちらであるか確認を行います。新規である場合は、以下の中より選択します。
 - マルチ モード ファイバ OM1、OM2、OM3、OM4
 - シングル モード ファイバ G.625
 - UTP カテゴリ 5E、6、6A、7
- 接続方式を選択します。
 - MMF 10GBASE-SR、10GBASE-LRM、1000BASE-SX
 - SMF 10GBASE-LR、1000BASE-LX
 - UTP 1000BASE-T

以上の情報より、アクセス スイッチの機器と、アクセス スイッチのアップリンクで利用するトランシーバを決定します。

ディストリビューションからのアップリンクの検討

ディストリビューションからコア間のアップリンク帯域の検討は、クラウド サービスの利用の帯域量や、QoS の利用により、エンド ポイント側からはオーバ サブスクリプションが無いように見せることができるなど、様々な要因が考慮されます。

■ オーバ サブスクリプション比

1:1 ~ 1:4 の範囲におさめるようにします。広帯域リンクを導入した場合にはアップリンクの方が過大になる場合もありますが、問題ありません。

■ アップリンクの検討

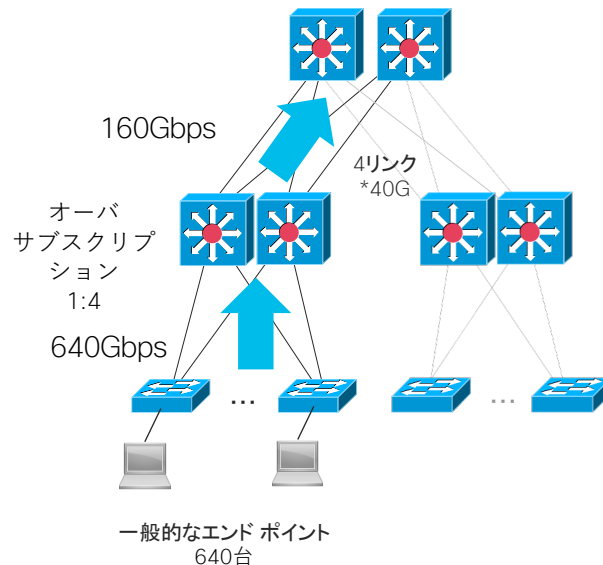
必要帯域量より、オーバ サブスクリプションを決め、アップリンク種類の選択します。

チャンネルを組むか、またはそれ以上の帯域を選択するか、の選択肢があります。

- 10G / 40G / 100G より選択
- チャンネルの使用の有無 (例:40Gの場合 4 *10G または 1 *40G)

■ 既設ケーブルがある場合

オーバ サブスクリプションを十分に考慮し、集約するディストリビューション スイッチを決定する必要があります。



以上を考慮し、ディストリビューション スイッチの機種を最終決定を行います。

ケース スタディ (ディストリビューション レイヤ)

A 構成 小規模構成シナリオ

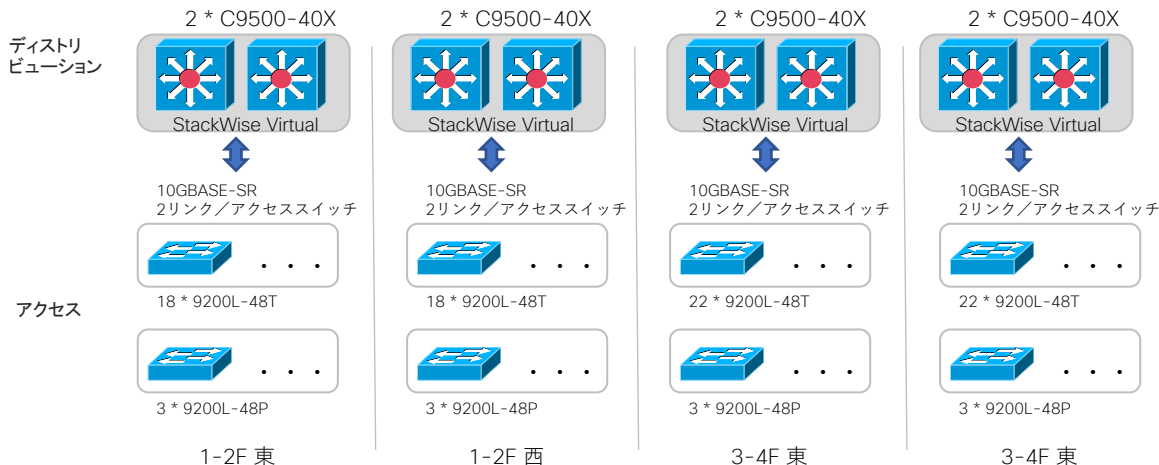
A構成はポート数が少ない構成のため、1台のスイッチにコアとディストリビューションの両方の役割を持たせた、2階層の構成で完成。

ディストリビューション スイッチ 1台あたり、アクセス スイッチからのアップリンク 22本 を収容する。



B 構成 大規模構成シナリオ

アクセス-ディストリ間には、40端末を収容するアクセススイッチ1台につき、アップリンク10G*2を採用すると、オーバサブ 20G : 40G 約 1:2 となる。
ディストリビューション スイッチ 1台あたり、アクセス スイッチからのアップリンク 10G* 21または25本 を収容するため、C9500-40Xを選定。

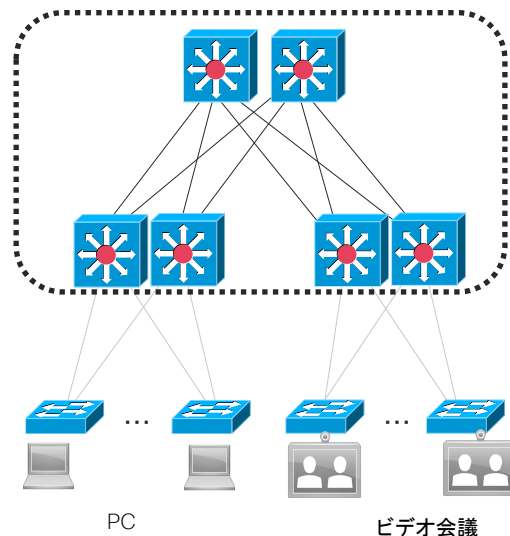


2.5 コアレイヤの構成

2.5 コアレイヤの構成

ディストリビューションレイヤからのアップリンクをまとめる

- コアは LAN ネットワークのバックボーンとして、ディストリビューションレイヤからのアップリンクをまとめ、トラフィックを中継します。コアがダウンするとシステム全体が停止するため機器冗長は必須です。また、電源を二重化し、必要に応じてスーパーバイザの冗長を推奨します。
- コアは 10G、40G、100G のアップリンクを収容します。既設配線を用いる場合は、コアスイッチの設置場所や、その条件を考慮する必要があります。
- 将来的なディストリビューションブロックの増設の可能性を考慮し、必要ポート数、必要トラフィック転送能力を決定します。



2.5 コアレイヤの構成

ディストリビューションーコア間接続を決定 コアスイッチの機種決定

次に、ディストリビューションからコア間の接続方式を決定することでコアの機器が決定します。

- 必要な帯域量を確認後、距離、利用するケーブル、接続方式を決定します。
- 距離は、フロア間配線、フロア内配線、室内配線など、必要な距離により用いるメディアや接続方式が異なります。
- メディア(ケーブル)は、既設配線または新規配線のどちらであるか確認を行います。
新規である場合は、以下の中より選択します。
 - マルチモードファイバ OM1、OM2、OM3、OM4
 - シングルモードファイバ G.625
 - DAC (ダイレクトアタッチケーブル)
- 次に、接続方式を選択します。
 - MMF
 - SMF
 - DAC

以上の情報より、コアの機器を決定します。

※コアスイッチ間相互の物理接続の必要性は後述の StackWise Virtual のコアへの適用の検討次第です。

参考：ケーブルの種類と特徴

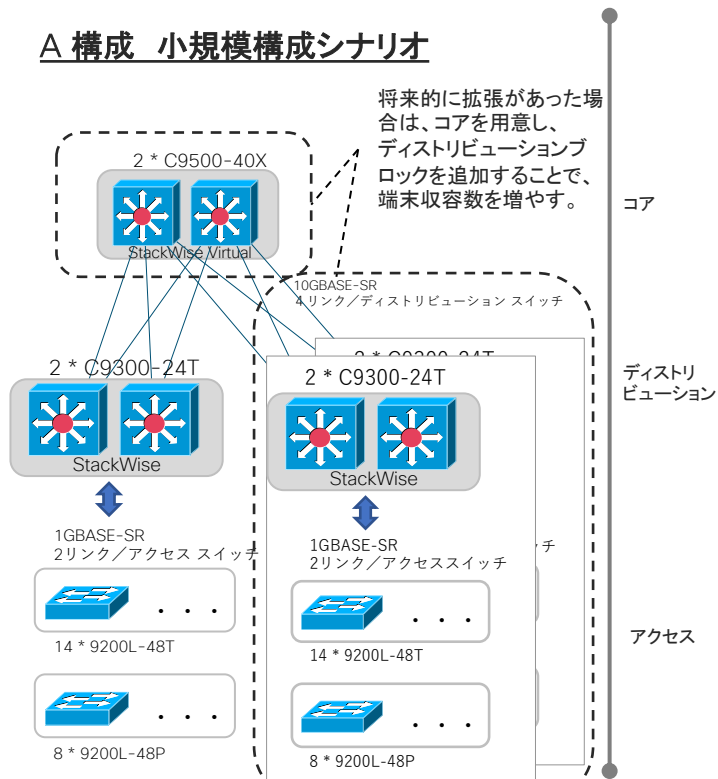
	MMF (マルチモード ファイバ)	SMF (シングルモード ファイバ)	UTP	DAC (ダイレクトアタッチ ケーブル)
特徴	<ul style="list-style-type: none"> 複数のモード(光信号)を使う コア系が太く曲げに強い。伝送損失が大きいため短距離伝送に向く 	<ul style="list-style-type: none"> 1つのモード(光信号)を使う コア系が小さく曲げに弱い。伝送損失が低く長距離伝送に向く 	<ul style="list-style-type: none"> 2本1組の細い銅線を縊り合せ、4組(計8本)を組み合わせた銅線ケーブルを用いて電気信号で伝送する方式を使う ファイバーに比べ安価。コネクタの形状規格は RJ-45 	<ul style="list-style-type: none"> 両端がトランシーバの形状が付いた、ケーブル Twinax ケーブルとも呼ぶ。
メディア (ケーブル)	OM1 :ギガビット イーサ向け、 200m までの伝送 OM2 :ギガビット イーサ向け、 500m までの伝送 OM3 :10 ギガビット イーサネット向け OM4 :長距離10G / 40G / 100G イーサネット向け	G.652(OS1/OS2)	カテゴリ 5E、6、6A、7	
接続方式	10G / 40G / 100G	10G / 40G / 100G	1G	10G / 40G / 100G

2.5 コアレイヤの構成

ケーススタディ (コアレイヤ)

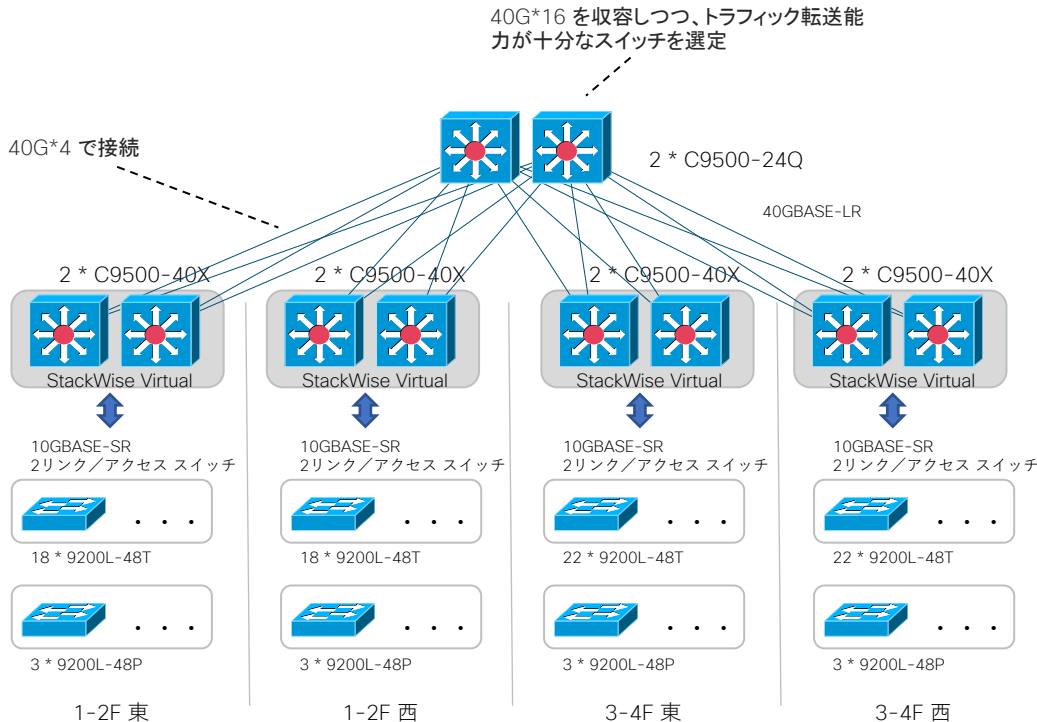
A 構成 小規模構成シナリオ

将来的に拡張があった場合は、コアを用意し、ディストリビューションブロックを追加することで、端末収容数を増やす。



B 構成 大規模構成シナリオ

40G*16 を収容しつつ、トラフィック転送能力が十分なスイッチを選定



2.6 物理的設定

2.6 物理的設定

スタック設定の検討 アクセスレイヤ / ディストリビューションレイヤ

各レイヤにおいて、Cisco Catalyst 9000 シリーズのスタック機能 (StackWise / StackWise Virtual) を採用する際の適否を記載しています。

■ アクセスレイヤ

スタック適用の有効性は限定的です。

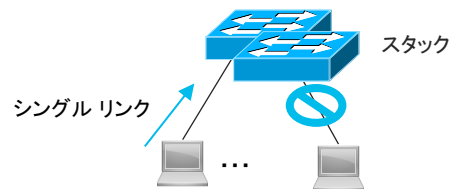
各エンドポイントは原則、単一のリンクでの接続が想定されるため、障害発時スタックによる冗長化が通信回復の手段となりません(右図参照)。

一方で、スイッチの管理単位を統合/削減する、もしくはアップリンクの本数を削減する目的では、スタックの適用は有効となります。スタック適用でアップリンクの本数を削減した場合は、それに応じたオーバサブスクリプション比を考慮した設計であるように注意が必要です。

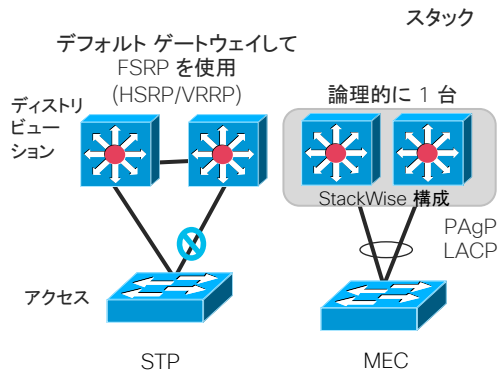
■ ディストリビューションレイヤ

スタック適用により、とくにアクセスレイヤとの接続において以下のような大きなメリットを引き出すことができます。

- MEC (Multi-Chassis EtherChannel) と組み合わせることで冗長化された機器とリンクの論理的な単一化がはかられ、LAN の最も大きな課題である L2 ループフリー構成が担保される
- MEC を利用した冗長リンク上のトラフィック負荷分散が効率的に行え、全体性能の最大化に寄与する
- 冗長化において必要とされてきた FHRP (HSRP/VRRP) の設定や仮想 IP アドレス確保、VLAN のリンク間分散の設計などが不要となる。



機器/リンク/ポート障害が発生した場合、通信不可となり、機器冗長をとっても可用性は高まらない



2.6 物理的設定

スタック設定の検討 コアレイヤ

■ コアレイヤ

コアレイヤは「スタック適用なし」「スタック適用あり」のいずれかを下記の視点で選択します。

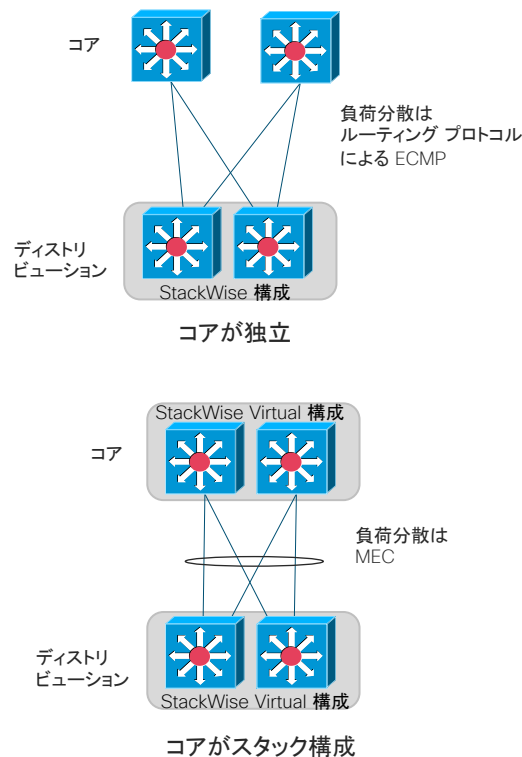
• スタック適用なし

コアレイヤでは、ルーティングプロトコルを前提としたループフリーな IP 経路に収束し、かつ ECMP (等コスト マルチパス) を利用したトラフィックのリンク間負荷分散が利用できます。スタックの最大のメリットであるループフリー / リンク負荷分散に相当する機能はすでに実装されているといえますので、このためにスタックを適用する積極的な理由はありません。また、コアスイッチは LAN 全体で 2 台ともともと少なく、個別に管理運用する利点が勝る場合が多くなります。

2 台のコアスイッチ間は、直接の相互物理接続を行わず、ディストリビューションレイヤと各々ルーティングを行います。

• スタック適用あり

スタック構成をコアで行う場合は、さらにディストリビューションレイヤのスタックそれぞれと完全な MEC を構成することで、機器の管理点数の削減とトラフィックのリンク間負荷分散を同時に行えます。



リンク アグリゲーション (EtherChannel)

■ レイヤ間リンクへの EtherChannel の適用

Cisco Catalyst 9000 シリーズで StackWise や StackWise Virtual で冗長した機器の筐体間で分散させた物理リンク間で EtherChannel を組むことを MEC (Multi-Chassis EtherChannel) と呼びます。

ディストリビューション レイヤでのスタック適用と併せて、アクセス-ディストリビューション間の複数リンクを EtherChannel として論理的に束ねる設定をします。ディストリビューション側は MEC となります。MEC の利用により、冗長化、トラフィックのリンク間負荷分散が自動的に行われます。また、障害時の通信復旧までの時間は50 ミリ秒から 600 ミリ秒と高速に収束します。

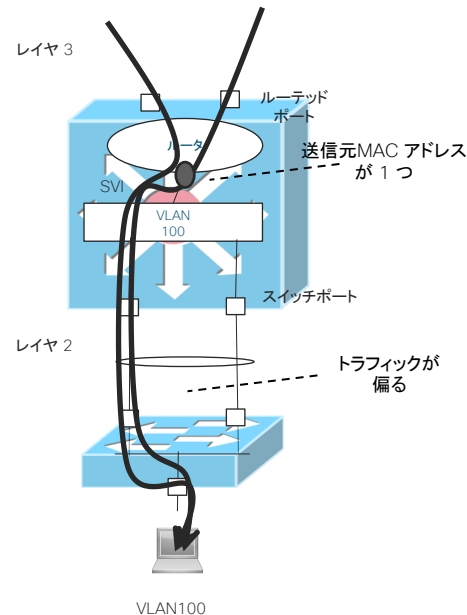
コアにスタックを適用した場合は、ディストリビューション、コアの双方が MEC となるように EtherChannel を構成します。

■ リンク間のロードバランス アルゴリズムの考慮

Cisco Catalyst 9200 シリーズのそれぞれの初期設定は、送信元 MAC アドレス (src-mac) の値のハッシュ値に基づいてリンク間でトラフィックを分散します。(Catalyst9600の初期設定は、送信元、送信先のIPアドレスのハッシュ値に基づいて分散)

適切な IP ルーティング構成ではトラフィックの送信元 MAC アドレスが SVI やルーテッド インターフェースの MAC アドレスに収束するため、初期設定のままではひとつのリンクにトラフィックが偏ります。ロード バランシングの設定を送信元と送信先 IP アドレス (src-dst-ip) に変更が必須となります。

- 必要に応じてトラフィックの偏りを考慮し、送信元と送信先 IP アドレス (src-dst-ip) 以外の選択で調整、変更を行うことでリンク アグリゲーションの効果を高めることができます。



ロード バランス を初期設定 (送信元 MAC アドレス) のままにした場合

2.6 物理的設定

UDLD

UDLD (Uni-Directional Link Detection)は、レイヤ 2 フレームを用いて、リンクの状態を監視し単一方向リンク障害を検出する、Cisco Catalyst シリーズに組み込まれているプロトコルです。

単一方向リンク障害は、正常に送受信している状態から、何らかの理由で送信もしくは受信ができなくなった状態を指します(右図)。とくに送信と受信の芯とコネクタが明確に分かれている光ファイバケーブルで発生しやすいです。単一方向リンク障害時には、正しく障害検知ができず、STP の BPDU が正しく送受信されず動作に悪影響を与える、EtherChannel で障害が起こったリンクにもトラフィックが流れ続ける、といった事象の発生の可能性があります。

UDLD は単一方向リンク障害の状態を検知し、そのリンクを正しく停止させる方法として有効です。

UDLD の推奨設定は、以下の通りです。

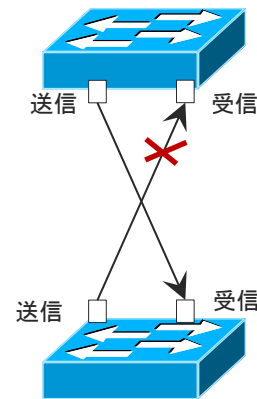
- **アグレッシブ モードを使用**

UDLD 対向のポートが UDLD パケットを受信しなくなったとき、UDLD はネイバーと接続を再確立しようと、8 度失敗するとポートをディセーブルにします。初期設定ではディセーブルになっています。

- **メッセージ タイムはデフォルト設定を使用**

UDLD は、片方向リンク時の重大障害を回避するセーフティ ネットとして利用するため、メッセージタイムの設定変更により迅速さを求めなくても、十分効果が見込まれます。

UDLD のメッセージ タイムをミリ秒まで早めた、“Fast UDLD” は、Cisco Catalyst 9500 シリーズ以上の製品のみをサポートとなります。リンクの対向で “Fast UDLD” をサポートしている必要があるため、現在のところはCisco Catalyst 9000 シリーズでは UDLD を利用することが一般的です。



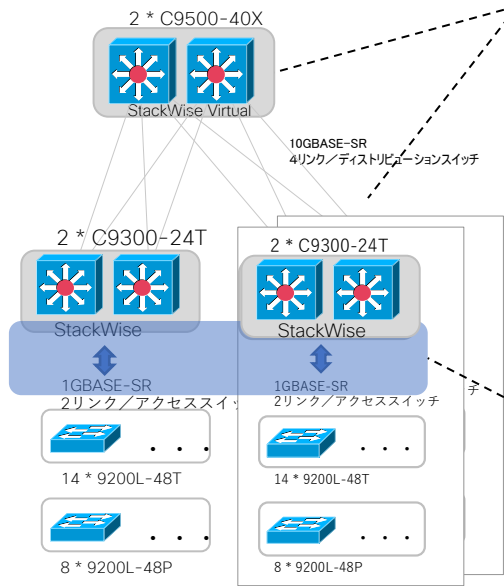
単一方向リンク障害

ケーススタディ (物理的設定)

A 構成 小規模構成シナリオ

コアで StackWise Virtual を行い機器の管理数を削減する構成

コアレイヤ
StackWise Virtual
ディストリビューションレイヤ
StackWise 480

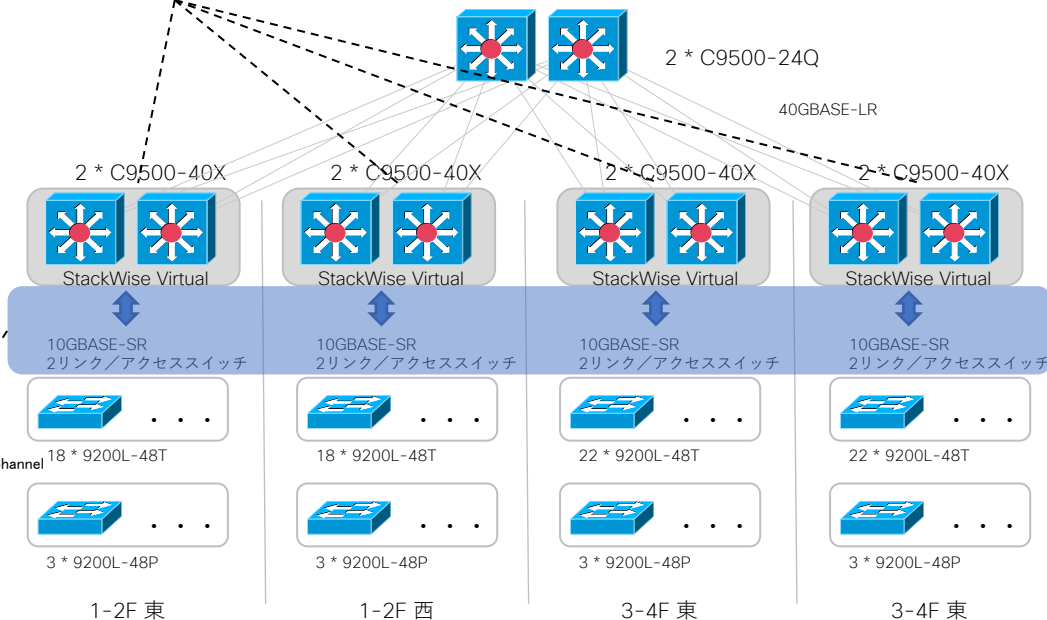


B 構成 大規模構成シナリオ

コアは個別で管理を行い、負荷分散は ECMP を利用する StackWise Virtual を使用しない構成

ディストリビューションレイヤ
StackWise Virtual

MEC: Multi-Chassis EtherChannel
(PAgPによる設定)



2.7 論理構成

レイヤ 2 とレイヤ 3 の配置

LAN において柔軟性と堅牢性を両立させるために、レイヤ 2 機能 (VLAN をベースとしたブリッジング) とレイヤ 3 機能 (IP ルーティング) の適切な配置は根幹を成す検討項目です。

■ アクセス - ディストリビューション間

VLAN を配置しレイヤ 2 機能を活用します。1 サブネット/ 1 VLAN を原則とし、かつ各 VLAN はディストリビューション ブロック内で完結させます。VLAN 配置の以下の利点を活かすよう配慮します。

- 複数のアクセス スイッチ間にまたがる VLAN によりエンドポイント側サブネットが柔軟に配置できる。
- 機器/リンクの物理的な変更なしにサブネット配置を容易に変更できる。
- エンドポイントが異なるアクセス スイッチへ移動しても IP アドレスの変更なく通信可能となる。ディストリビューションスイッチはエンドポイントの VLAN (サブネット) に対するデフォルト

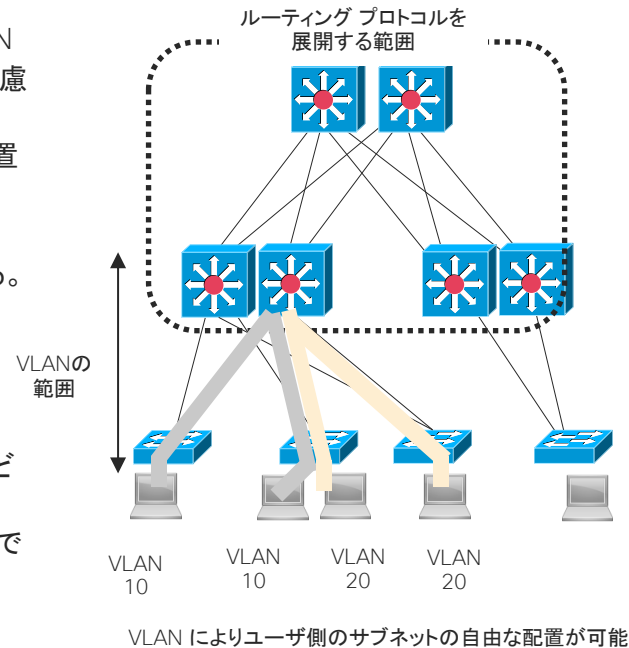
ゲートウェイ
機能を提供します。

■ ディストリビューション - コア間

ルーティング プロトコルを用いた IP ルーティングのレイヤ 3 機能を動作させます。OSPF などのルーティ

ング プロトコルは明示的にループ フリーとなる経路制御を行うため、LAN の根幹となる部分での適切

な稼働により LAN 全体を安定化させ、かつ障害時の影響範囲を極小化できます。



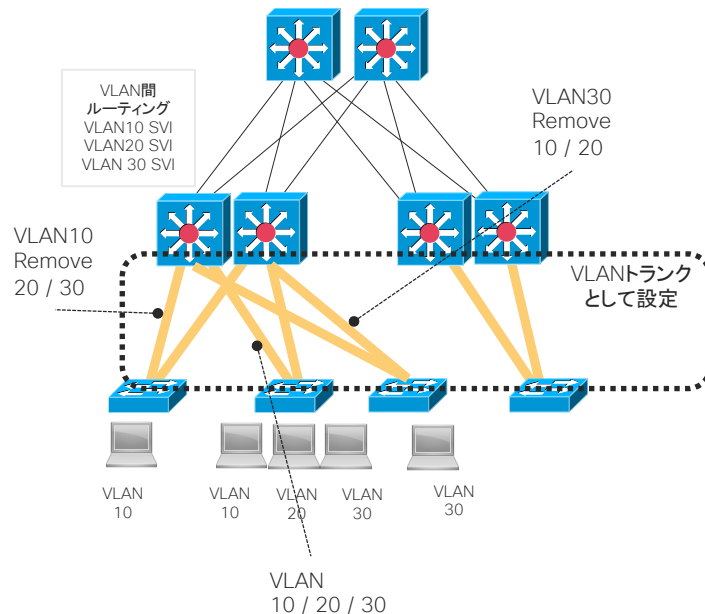
レイヤ 2 設定 - VLAN 設定

アクセス - ディストリビューション間は、VLAN トランク設定にすることを原則とします。VLAN トランク ポートで VLAN の追加/変更は、switchport trunk allowed vlan add / remove のコマンドで行います。

このような方針により、管理や設定において、以下の利点を享受することができます。

- 個別の VLAN 番号に依存しないインターフェース設定の簡素化/統一化
 - VLAN 追加・変更時の作業簡素化
 - VLAN 追加・変更時の他の VLAN の通信断などの影響の防止
 - IEEE 802.1Q 内の 3 ビットの優先度情報 (CoS) を利用した QoS 設定の適用
- ディストリビューション スイッチではディストリビューション ブロック内の VLAN に応じて SVI を作成し、レイヤ 3 ルーティングに組み入れます。

コア - ディストリビューション間では、原則としてルーテッド インターフェース設定とし、VLAN 設定、VLAN トランク ポート設定を行いません。詳細は「レイヤ 3 設定」で述べられています。



レイヤ 2 設定 - STP 設定

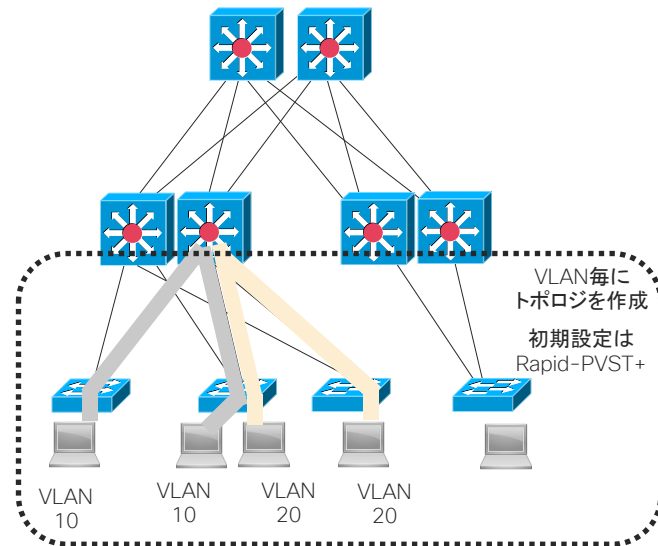
STP (Spanning Tree Protocol) は、LAN の安定性の最大の課題であるレイヤ 2 ループ発生の抑制のための重要な機能です。

Cisco Catalyst 9000 シリーズの初期設定の STP モードは Rapid-PVST+ です。Rapid-PVST+ では VLAN ごとに STP トポロジーが構成されるため、VLAN の追加削除や有効範囲の変更を行っても他の VLAN に影響を与えません。また、アクセス スイッチ上で利用されない VLAN はこまめに VLAN トランク ポートから取り除くことで、STP 計算による負荷が軽減されます。

- 想定外の VLAN 範囲の拡大/経路生成を防止するため、VLAN 1 は全ての VLAN トランク ポートとアクセス ポートから取り除くことを推奨します。管理用通信に用いる VLAN は、別途新たな VLAN ID で用意します。

スタックと MEC の採用によりアクセス - ディストリビューション間のレイヤ 2 構成においてループ フリー構成が担保されていますが、セーフティネットとして必ず STP を稼働させてください。Rapid-PVST+ の初期設定のままで想定外のループ形成の防止として十分機能します。

※Cisco Catalyst シリーズの初期設定の STP モードは 2015 年の IOS バージョン 15.2(4)E から Rapid-PVST+ に変更されています。



レイヤ 3 設定

レイヤ 3 (IP ルーティング)の設定はディストリビューションおよびコアにおいて行います。

■ ルーティング対象となる IP インターフェースの設定

エンドポイントが配置された IP サブネットのルーティングのため、ディストリビューションスイッチの SVI (VLAN インターフェース) に IP アドレス設定を行い、ルーティング対象とします。

ディストリビューション - コアのリンクについてはルーテッド インターフェース設定、具体的には "no switchport" を適用した物理インターフェース(または MEC ポートチャネル インターフェース)に対し IP アドレスの設定を行い、ルーティング プロトコルを動作させます。このリンクには、OSPF Prefix Suppression のように経路対象から除外できる機能があれば適用を積極的に検討します。ルーテッド インターフェイスでなく SVI を設定しルーティングを行うと以下の欠点があり、推奨されません。

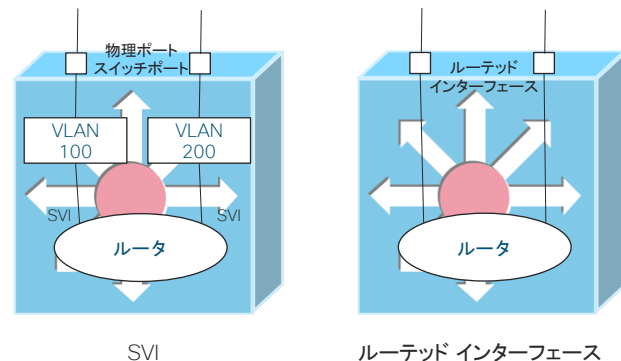
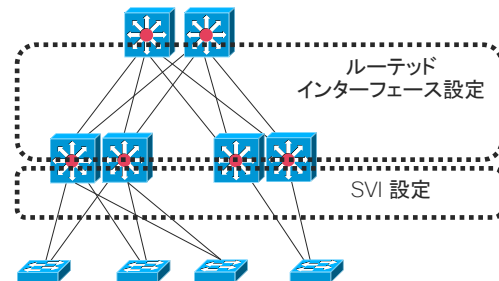
- インターフェースダウン動作に物理インターフェースと SVI の 2 段階を経るため、リンク障害検知に遅延が加わる余地ができる。
- 管理する VLAN が増加し不必要な STP トポロジも生成され、想定外に通信可能なバックドアの発生や設計と異なるトラフィックパスが生成されるリスクが生じる。

■ ルーティング プロトコルの選択

各ルーティング プロトコルのもつ適性を考慮し、選択します。

例えば IPv4 / IPv6 デュアル スタックでは、設定/トポロジ設計が簡素化される「OSPFv3 Address Families (シングルトポロジ OSPFv3)」の採用を積極的に検討します。

また、不等コスト負荷分散や ハブ スポーク型 WAN と一体化したルーティングを行う場合は、EIGRP が適しています。



2.7 論理構成

IP アドレス配置

LAN 上の IP アドレス配置は既存のポリシーがあればそれに従います。以下は、一般的な設定および 3 階層構成を前提としたアドレス配置方針の例です。

■ アクセス - ディストリビューション間 VLAN 上のサブネット

エンドポイントが参加するサブネットとなり、ディストリビューション スイッチの SVI をデフォルトゲートウェイとします。IPv4 では 16~24 ビット長ネットマスク、IPv6 では 64 ビット長プリフィクスで設定されることが多くあります。IPv4 においては細かすぎる分割 (ネットマスク 25 ビット長以上) は配置の柔軟性を損なうことがあります。

■ ディストリビューション - コア間リンクの上のサブネット

ルーテッドインターフェースで IP アドレスは対向 2 ノード分のみ用いられます。アドレススペースの節約のためには最長のネットマスク長/プリフィクス長を設定します。(IPv4 : 30 ビット長、IPv6 : 127 ビット長)。

■ ディストリビューション スイッチおよびコア スイッチ上のループバック インターフェース

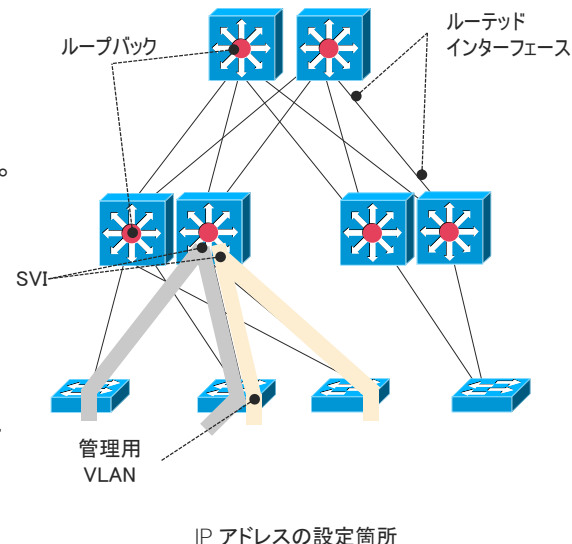
レイヤ 3 機能を有するこれらのスイッチでは、必ずループバック インターフェースを設定し IP アドレスを最大長のネットマスク長/プリフィクス長(IPv4 : 32 ビット長、IPv6 : 128 ビット長)で付与します。

■ 管理用 IP アドレス

アクセス スイッチでは、エンドポイントの VLAN と異なる管理用の VLAN に IP アドレスを付与します。ディストリビューション/コア スイッチでは、ループバック インターフェースのひとつを管理用に使用します。※Catalyst 9000 シリーズは管理専用の物理インターフェースを有し、アウトオブバンド管理に利用することができます。ただし、NetFlow Data Export ができないなどの制限があり、注意が必要です。

■ 経路集約を考慮した計画

実際の経路集約の実施の有無にかかわらず、可能な限り LAN 全体、およびディストリビューション ブロックの単位で IPv4 のネットマスク、IPv6 のプリフィクスで整然と集約できるように全体の IP アドレス配置計画を行います。セキュリティや QoS のための ACL 定義など、管理運用性が向上します。



OSPF による IPv4 ルーティングのベスト プラクティス設定

ここでは「IPv4 ルーティングのために OSPFv2 を用いる」と想定した場合の設定ベスト プラクティスのひとつを提示します。対象は、レイヤ 3 機能を配置するディストリビューション レイヤおよびコア レイヤの Cisco Catalyst 9000 シリーズです。

■ OSPF のベスト プラクティス設定

ディストリビューション レイヤおよびコア レイヤの Cisco Catalyst 9000 への OSPF 設定の例は右および次頁以降のようになります。障害時の収束時間の短縮と CPU 負荷の削減、経路数の抑制、その他設定の簡素化を考慮したベスト プラクティス設定です。

■ OSPF エリア設計

すでにネットワークで用いられている OSPF エリア設計方針があれば、それに従います。コア レイヤを中心とする LAN 全体で 1 つの一般エリアを構成する場合、コア レイヤの Cisco Catalyst 9000 を ABR としたスタブ エリアもしくは Totally - Stubby の設定を検討します。また、エリア外に向けた適切なルート集約を行います。

■ Catalyst9000 シリーズにおけるルーティングの考慮点

IPv4 での OSPF に限りませんが、Catalyst 9000 シリーズでは以下の点を考慮します。

- TCAM プログラミング/ TCAM 容量に由来するハードウェア (ASIC) 転送時の経路数上限を越えないように設計する (経路数上限についてはデータシート等を参照)。

例 : Catalyst 9300 : 約 7,000 (IOS-XE 16.9.x 時点)

- デフォルトで経路負荷分散での偏り (Polarization) の対策がなされている。

CEF ロード バランシングの “Universal” モード(機器単体毎に生成した個別の数字を加味した、冗長経路間のトラフィック分散のランダム化)が設定されており、基本的には Polarization が発生せず帯域の最大化が図られる。

共通設定

```
router ospf <プロセスID>
router-id <IPv4アドレス>
ispf
log-adjacency-changes
auto-cost reference-bandwidth 100000
timers throttle spf 10 100 5000
timers throttle lsa all 10 100 5000
timers lsa arrival 80
passive-interface Loopback<番号>
passive-interface Loopback<番号>
. . .
! ABRで必要に応じて設定
area <OSPFエリア番号> stub no-summary
area <OSPFエリア番号> range <集約対象IPv4ネットワーク>
<IPv4サブネットマスク> cost 10
```

OSPF による IPv4 ルーティングのベスト プラクティス設定

適用コマンドの解説

コマンド	設定モード	説明
router-id <IPv4アドレス>	router	OSPF Router ID の明示的設定
ispf	router	Incremental SPF : SPF 再計算範囲を最適化
auto-cost reference-bandwidth 100000	router	100Gbps のリンクまで考慮したコスト計算の基準帯域
timers throttle spf 10 100 5000 timers throttle lsa all 10 100 5000 timers lsa arrival 80	router	SPF 再計算と LSA 生成の抑制タイマーを調整
dampening	interface	IP Event Dampening : フラッピングの影響を緩和
ip ospf <プロセスID> area <OSPF エリア番号>	interface	OSPF をインターフェイス レベルで有効化
ip ospf network point-to-point	interface	オーバーヘッドの少ないネットワーク タイプへ変更
ip ospf prefix-suppression	interface	ルーティング対象から除外 (中継リンクのみ)
carrier-delay msec 0	interface	リンク ダウン検知時の遅延を最小化 (1Gbps 以上のリンクでは有効な設定とならない場合あり)

ディストリビューションレイヤ / VLAN インターフェイス設定

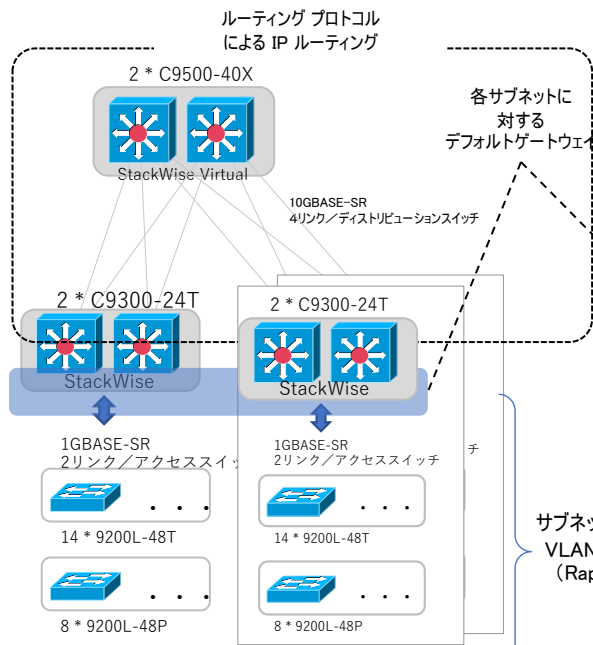
```
interface vlan <番号>
dampening
ip address <IPv4ネットワーク> <IPv4サブネットマスク>
ip ospf <プロセスID> area <OSPFエリア番号>
logging event link-status
load-interval 30
carrier-delay msec 0
```

ディストリビューションレイヤ / コアレイヤ間ルーテッドインターフェイス設定

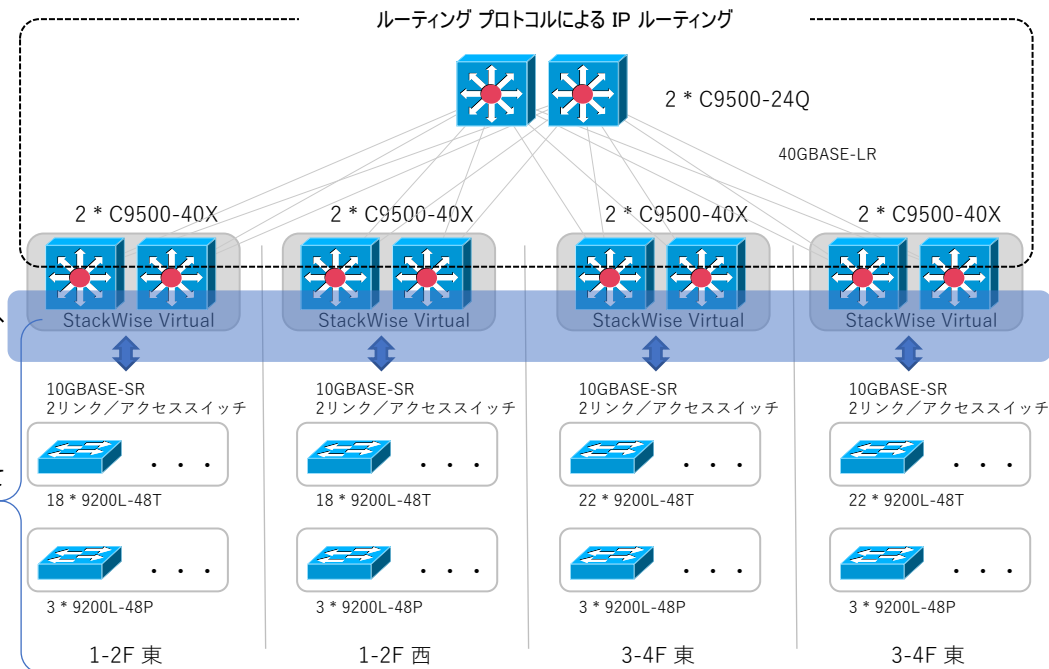
```
interface <インターフェイス名・番号>
dampening
ip address <IPv4ネットワーク> <IPv4サブネットマスク>
ip ospf <プロセスID> area <OSPFエリア番号>
ip ospf network point-to-point
ip ospf prefix-suppression
logging event link-status
load-interval 30
carrier-delay msec 0
```

ケーススタディ (論理的設定)

A構成 小規模構成シナリオ



B構成 大規模構成シナリオ



2.8 LAN 外への接 続

2.8 LAN外への接続

WANへの接続

他のサイトとの通信のための WAN の接続において、高度な QoS の適用や IPsec VPN による通信暗号化の実施を念頭にルータ機器を想定します。以下の点を原則とし構成します。

1. WAN 接続に必要な機能、設定を集約した独立した機能ブロックとして位置づける
2. コアレイヤに直結し、他のディストリビューション ブロックから物理的または論理的に独立させる

コアがスタック構成でなく相互に独立している場合には、個別の物理インターフェースをルーテッド ポート設定とし、ECMPを用いた構成とします。

コアがスタック構成の場合には MEC 設定とし、ポートチャネル論理インターフェースをルーテッドポート設定とします。ルータ側でもリンク アグリゲーション(機能名 Link Bundling、Port Channel など)を用います。

コア スイッチと WAN ルータには以下のようなギャップが生じることが多く、対応する必要があります。

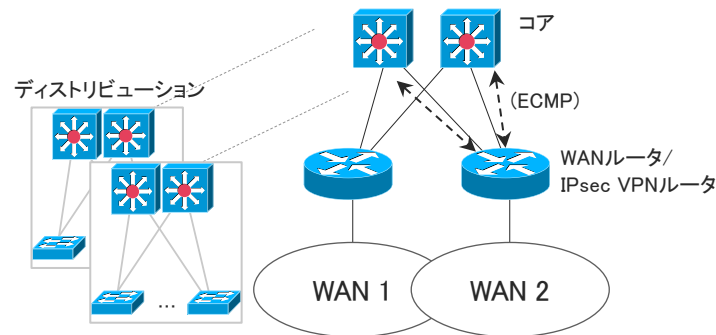
- インターフェース速度のギャップ (コア 40G に対するルータ 10G、1G など)

コア スイッチ側にて QSA、ブレイクアウトケーブルなどで対応

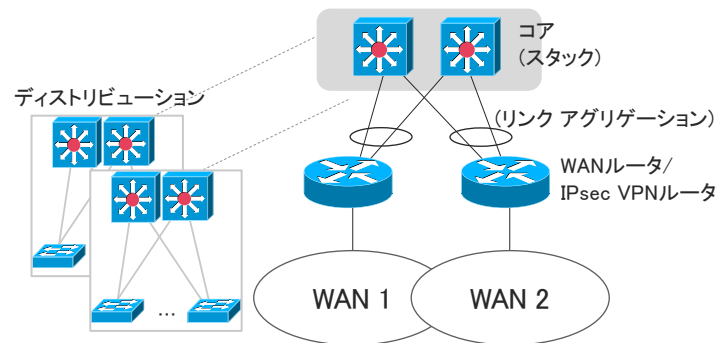
※ シスコ製 QSA、および Catalyst9000 シリーズの 10GBASE-X ポートは 1G SFP に対応しています。

- 転送性能のギャップ (ルータの全体転送性能が最大 2Gbps である、など)

ルータにて Ingress / Egress Shaping や IEEE802.3x Flow Control ポーズ送信機能で対応



コアが独立している場合の接続例



コアがスタック構成の場合の接続例

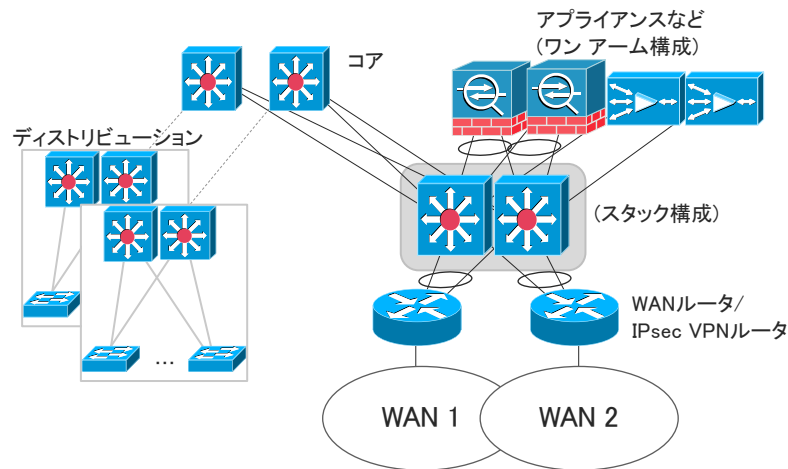
2.8 LAN外への接続

WANへの接続

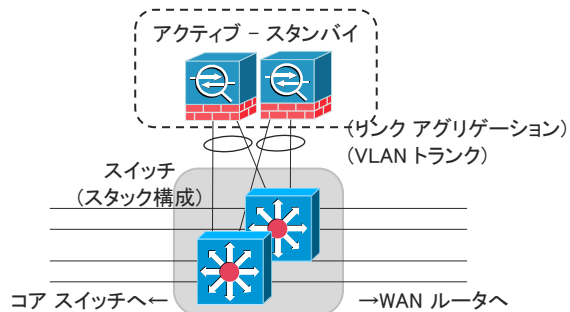
WAN接続に対する付加機能として、ファイアウォール、IPS、WAN高速化装置などのアプライアンスを配置する場合には、スタック構成のスイッチを配置した上で、各アプライアンスをスイッチに接続します。

各アプライアンスのリンクはすべてスイッチに対する直結、いわゆる「ワンアーム構成」とします。ワンアーム構成の利点として、アプライアンス側の様々な機能構成への柔軟な対応、使用する物理インターフェース数の最適化、不具合時のアプライアンスのネットワークからの切り離しが容易、などがあります。

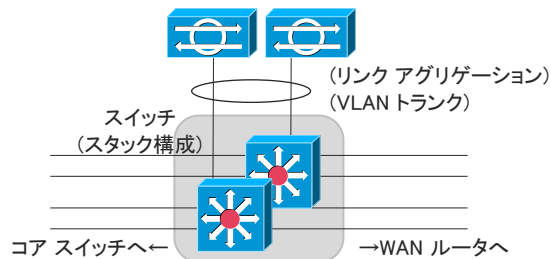
アプライアンスが冗長化されている場合、通信フロー毎に一意に同一のアプライアンスに転送されるよう、スイッチ側でアプライアンス転送時のリンクアグリゲーションや WCCP の負荷分散を適切に設定する必要があります。



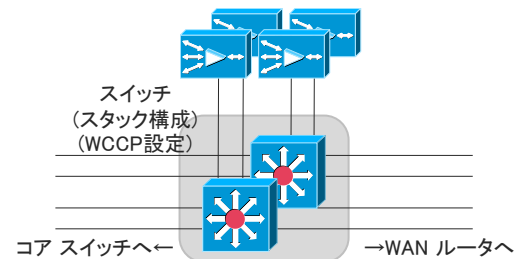
WAN 接続への各種アプライアンスの追加



ファイアウォール等



プロミスクラス型機器



プロキシ型機器

2.8 LAN外への接続

WANへの接続

アプライアンスのワン アーム構成の例

アプライアンスの例	スイッチのインターフェース設定	アプライアンスの インターフェース構成、設定	アプライアンスの 転送方式	考慮事項
レイヤ 3 ファイアウォール (アクティブ-スタンバイ冗長)	<ul style="list-style-type: none"> 対向アプライアンス毎の単一の物理リンク VLAN トランク 	<ul style="list-style-type: none"> 単一の物理リンク VLAN トランク 	IP ルーティング (VLAN 間ルーティング)	<ul style="list-style-type: none"> 単一リンク障害時の帯域縮退に留意する。帯域縮退を避ける場合にはスイッチ側でリンク アグリゲーション最小リンク数の設定を行う。 (config-if)# port-channel min-links <最小リンク数>
レイヤ 2 ファイアウォール インライン型 IPS (アクティブ-スタンバイ冗長)	<ul style="list-style-type: none"> 対向アプライアンス毎に複数物理リンクのリンク アグリゲーション VLAN トランク 	<ul style="list-style-type: none"> 複数物理リンクのリンク アグリゲーション VLAN トランク 	VLAN 間ブリッジング	
インライン型 IPS (複数のスタンドアロン機器の 並行設置)	<ul style="list-style-type: none"> 対向アプライアンス複数をもたがるリンク アグリゲーション VLAN トランク 	<ul style="list-style-type: none"> 単一の物理リンク、または複数物理リンクのリンク アグリゲーション VLAN トランク 		<ul style="list-style-type: none"> スイッチ側リンク アグリゲーションの負荷分散を送信元 IP アドレスと送信先 IP アドレスに基づくハッシュにする(負荷分散先アプライアンスの一意性確保) (config)# port-channel load-balance src-dst-ip など
プロミスキュス型 IPS NetFlow 生成装置	<ul style="list-style-type: none"> 複数の対向アプライアンスにまたがるリンク アグリゲーション ポートミラーリング 	<ul style="list-style-type: none"> 単一の物理リンク 	転送なし	
WAN 高速化装置 アプリケーション プロキシ	<ul style="list-style-type: none"> 対向アプライアンス毎の単一の物理リンク アクセス VLAN ポート WCCP または PBR (ブラウザ上の明示的プロキシ設定を用いる場合は必要なし) 	<ul style="list-style-type: none"> 単一の物理リンク 	IP ルーティング	<ul style="list-style-type: none"> アプライアンス間の負荷分散は WCCP に基づく決定、またはアプライアンス側でのクラスターリング機能などで行う。(負荷分散先アプライアンスの一意性確保) ※Catalyst 9000 シリーズは IPv6 での WCCP をサポートしていません (IOS-XE 16.12 時点)

2.9 無線 LAN の 構成

無線 LAN アクセスポイントの接続

※ここでは無線 LAN アクセスポイントのスイッチへの接続に際しての考慮点について述べます。
サイトサーベイを伴う無線 LAN のセル設計や無線 LAN アクセスポイントの配置計画は対象外とします。

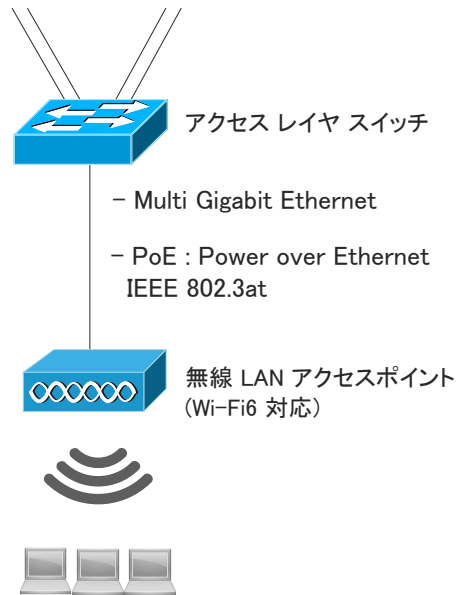
■ PoE+ による給電

無線 LAN の展開においては、個々の無線 LAN アクセスポイントへの合理的な給電方法として PoE : Power over Ethernet が用いられます。Wi-Fi6 に至る高速化の性能を最大限引き出すために、PoE での給電機器側で IEEE 802.3at PoE+ (最大 30W) への対応が必要とされます。

■ mGig での広帯域化

また、Wi-Fi6 は実効速度が 1Gbps を大きく上回るとされ、1000BASE-T (1Gbps) のリンクではボトルネックとなり高速化の利点を活かせなくなります。従来からの銅線イーサネットのケーブルである UTP を用いて 2.5Gbps / 5Gbps の速度を実現する mGig : Multi-Gigabit Ethernet への対応が Wi-Fi6 無線 LAN アクセスポイントで行われています。2.5Gbps (2.5GBASE-T) においてはカテゴリ 5e 以上、5GBASE-Tにおいてはカテゴリ 6 以上の UTP での接続となります。

これら無線 LAN アクセスポイントへ有線接続を提供するアクセスレイヤのスイッチでは、収容する無線 LAN アクセスポイントの台数に応じた PoE+ および mGig に対応したポートを必要数搭載した機種を選択します。とくに、使用する PoE+ ポートの合計に応じた十分な給電能力の余力 (給電バジェット)、mGig ポート含むダウンリンク総帯域に応じたアップリンク総帯域を確保できるような機種、台数を考慮する必要があります。



無線 LAN アクセスポイントの接続

無線 LAN のクライアントの接続する VLAN として、以下の 2 つのパターンを無線 LAN の用途やトラフィックパターン、ネットワーク構成に応じて選択します。

- 無線 LAN コントローラ上に定義された VLAN (Central Switching)
- 無線 LAN アクセスポイントが接続するスイッチ上に定義された VLAN (Local Switching)

Central Switching と Local Switching、および接続先 VLAN は、「WLAN」(SSID と無線 LAN 認証方式の定義のセット) 毎に設定することができます。ただし、Local Switching は「Flexconnect モード」で起動したアクセスポイントでのみ可能です。

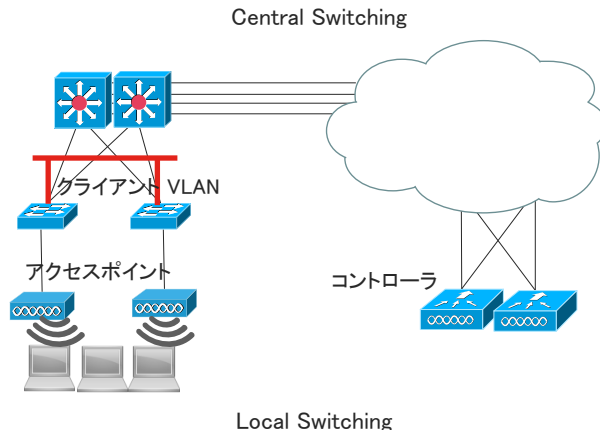
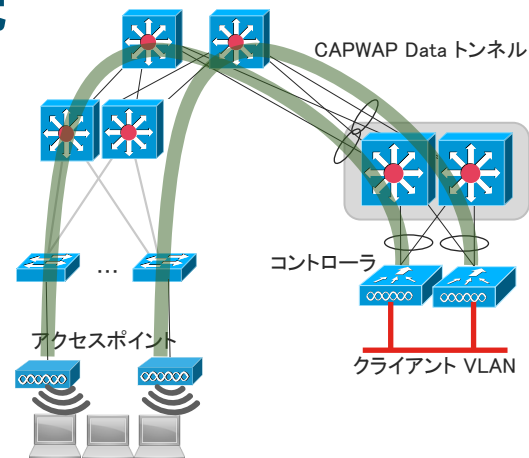
■ Central Switching

Central Switching の利点として、各ディストリビューション スイッチおよびアクセス スイッチに VLAN を個別に設定することなく、一括してコントローラ上に無線 LAN 用の VLAN を配置でき、柔軟で迅速な無線 LAN の展開、中央集中のトラフィック制御が可能です。無線 LAN トラフィックはアクセスポイントとコントローラ間で「CAPWAP Data」でカプセル化されトンネリングされます。

Central Switching においても、ACL で指定した特定のトラフィックのみ選択的に Local Switching 相当の転送を行う「Split Tunneling」機能が利用可能です。Split Tunneling の利用は、アクセスポイントが Flexconnect モードである必要があります。

■ Local Switching

Local Switching は、直近のスイッチ上からトラフィックが転送され、Central Switching のような無線 LAN トラフィックのコントローラへのトンネリングで生じるトラフィックの迂回がありません。また、コントローラの転送能力や物理リンク帯域によるボトルネックによる影響の懸念はなくなります。



2.10 IP マルチキャスト

マルチキャストのためのネットワーク

■ ループフリーなユニキャスト経路形成の重要性

IPv4、IPv6 のマルチキャストは PIMv2 を用いたオンデマンドで動的な経路形成です。PIMv2 による受信側から送信側へのシグナリング (PIM Join) をユニキャストの経路に従って行うことでつくられたパスを、逆方向に向かう形で実際のマルチキャスト パケットが転送されます (RPF : Reverse Path Forwarding)。そのため、ネットワーク全体でループのない安定した IPv4、IPv6 のユニキャストのルーティングがなされていることが前提条件となります。

■ ECMP (Equal Cost Multi-Path) におけるマルチキャストトラフィック分散

IPv4 では初期状態で、マルチキャスト機器は PIM Join を経路上の対向 IP アドレスが最大の PIM ネイバーにのみ送られ、ECMP においても結果として単一の経路に偏った転送となります。IP Multicast Load Splitting 機能を有効にすると、PIM Join の送信を ECMP 上に分散させ、結果としてマルチキャストトラフィックのトラフィックが ECMP で分散されます。全ての L3 スイッチ、およびルータにて「(config)# ip multicast multipath」コマンドで同機能を有効化します。IPv6 では同機能は初期状態で有効です。

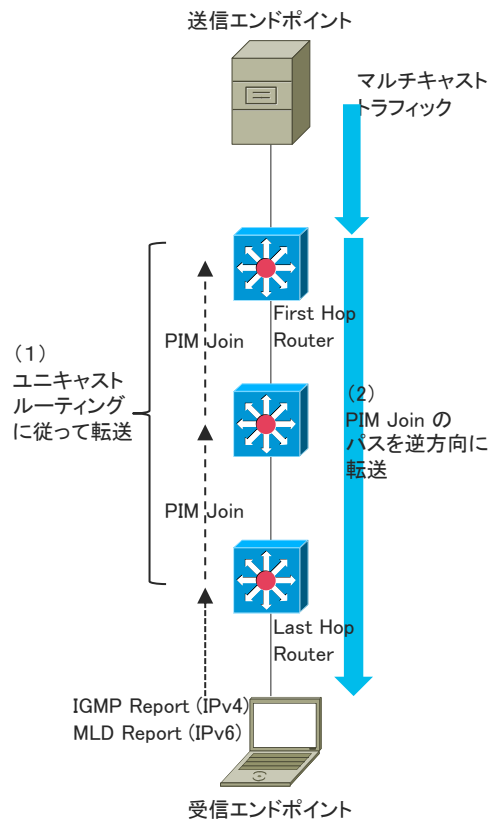
■ リンクアグリゲーション上のマルチキャストトラフィック分散

マルチキャスト パケットの転送において、リンク アグリゲーションにおける物理リンク間の負荷分散はユニキャストパケットと同様の負荷分散方式に従います。

グループアドレスの割り当てを送信エンドポイントの IP アドレスに基づき行った下記のような例では、送信元、送信先アドレスの XOR が一致するため、ハッシュを基にした負荷分散アルゴリズムの結果、特定の物理リンクへのトラフィック集中が発生します。

(Source, Group) : (10.10.10.1, 239.10.10.1), (10.10.10.2, 239.10.10.2), ... (10.x.y.z, 239.x.y.z)

この場合には、負荷分散の要素に UDP ポート番号を加える、などの設定変更により、偏りが解消されます。



RPF に基づくマルチキャスト転送

PIM 動作モードにおける SSM の選択

■ PIM 動作モード : SSM の積極的な検討

マルチキャスト ルーティングにおける PIM の動作モードは主に以下があります。

- Source-Specific Multicast : SSM / PIM-SSM - RFC4607
- PIM Sparse Mode : PIM-SM (Any Source Multicast : ASM) - RFC7761 旧RFC4601

※ Bidirectional PIM はごく特殊なアプリケーションでのみ適用されるため、ここでは検討範囲外とします。PIM Dense Mode は一般的な用途では事実上使われることはありません。

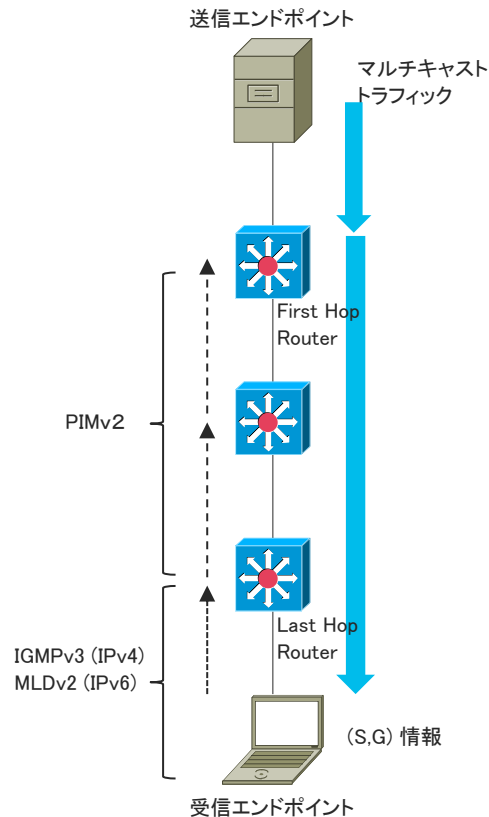
SSM では、PIM-SMで必須の Rendezvous Point : RP の設置が不要です。RP の設置とその情報の安全で確実なネットワーク内への伝播には多岐にわたる項目の検討と煩雑な設計を要しますが、それらが不要で設計が格段に簡素化される SSM の採用をまず第一に検討します。また既に PIM-SM が動作している場合にも、互換性を利用しながら SSM への移行をはかるようにします。

■ SSM 導入における考慮点

SSM ではマルチキャスト受信エンドポイントが IGMPv3 (IPv4) 、MLDv2 (IPv6) をサポートしていること、および受信するマルチキャストのグループアドレスに加え送信元 IP アドレスの情報を有していることが前提となります。

また、IGMP Snooping および MLD Snooping が、ディストリビューションおよびアクセス スイッチのマルチキャスト受信エンドポイントの存在しうる VLAN で有効になっていることを確認します。

Catalyst 9000 シリーズでは、IGMPv3 および MLDv2 においては、Basic Snooping のみのサポートです。これは、同一のグループアドレスのマルチキャストトラフィックは、送信元が異なっても区別されることなく受信エンドポイントのポートヘレイヤ2転送されることを意味します。このため、SSM を採用する場合でも同じグループ アドレスを複数のマルチキャストに使い回すことは得策ではありません。



3

機能編

3.1 Stack

StackWise Virtual, StackWise,
StackPower

3.2 IOS Management

Upgrade, ISSU, GOLD, PoE, WireShark,
Energywise, Blue Beacon, TDR

3.3 Basic L2/L3

EtherChannel, VTP, STP, MST, REP,
FHRP, VRF, IGMP

3.4 QoS

QoS, Policing, DTS, WRED, H-QoS,
Auto-QoS

3.5 Security

DAI, IP Source Guard, First Hop Security,
SISF, Trustworthy, Cisco Secure Boot,
MACsec, ネットワーク認証

3.6 AVC

AVC

3.1 Stack

StackWise Virtual
StackWise

<電力の共有>

StackPower

Stack 機能のサポートについて

目的	機能名	C9600	C9500	C9400	C9300/ C9300L	C9200/ C9200L	備考
データの共有 (機器冗長)	StackWise Virtual	○	○	○			UTP / STP ケーブルによる構成 構成台数は 2 台
	StackWise				○	○	専用ケーブルによる構成 最大構成台数は 8 台
電力の共有 (電源冗長)	StackPower				○		専用ケーブルによる構成 最大構成台数は 4 台

StackWise Virtual

機能説明①

StackWise Virtual 機能では、2 台のスイッチ機器を 1 つの論理スイッチとして動作することができ、拡張性や耐障害性に対応します。

■ 特徴

1つの論理スイッチ内の2台のスイッチ機器では、設定やその他の情報を共有します。

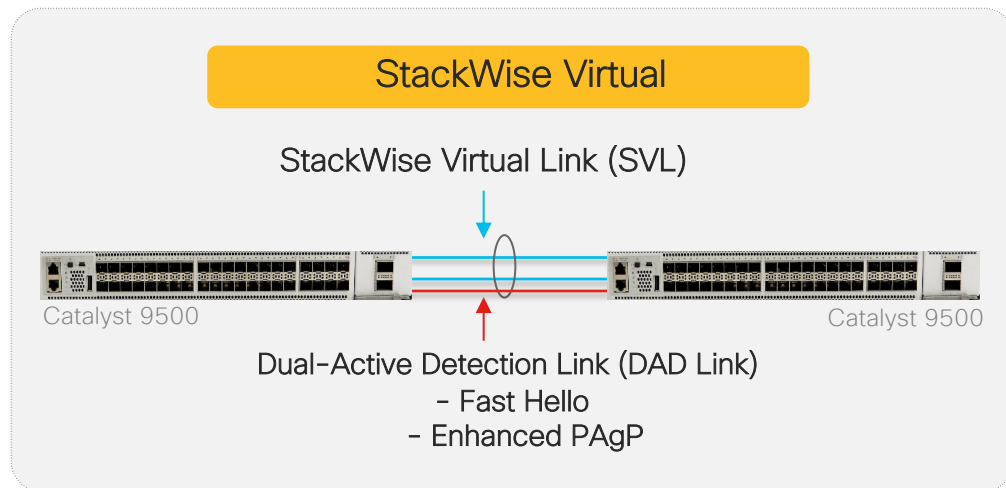
■ 既存機器との比較

類似テクノロジーである VSS 機能と比較し考え方は同じになります。

コマンドに関しては改善され両機器で同じ設定を入れます。

■ 注意点

同じ StackWise Virtual のスイッチは互換性のある IOS-XE の Version、同じライセンスのみにて サポートしていません。



StackWise Virtual

機能説明②

■ 手順

- ① stackwise-virtual
- ② domain <1-255>
- ③ interface range TenG x/y/z
- ④ stackwise-virtual link <1-255>
- ⑥ interface range TenG x/y/z
- ⑦ stackwise-virtual dual-active-detection
- ⑨ copy run start
- ⑩ reload

■ 注意事項

- ・SWV(StackWise Virtual)を構成する 2 台のスイッチは、OS バージョン、ライセンス、機器モデルを揃える必要があります。
- ・機器のモデルおよび OS バージョンにより、SVL リンク、DAD リンクの指定ポート、および最大数が異なります。

StackWise Virtual

SWV 設定①

■ 1 台目のスイッチへ設定

```
Switch(config)#stackwise-virtual
Please reload the switch for Stackwise Virtual configuration to take effect
Upon reboot, the config will be part of running config but not part of start up config.
Switch(config-stackwise-virtual)#domain 1
Switch(config)#interface range tenGigabitEthernet 1/0/39-40
Switch(config-if-range)#
Switch(config-if-range)#stackwise-virtual link 1
WARNING: All the extraneous configurations will be removed for TenGigabitEthernet1/0/39 on reboot
INFO: Upon reboot, the config will be part of running config but not part of start up config.
WARNING: All the extraneous configurations will be removed for TenGigabitEthernet1/0/40 on reboot
INFO: Upon reboot, the config will be part of running config but not part of start up config.
Switch(config-if-range)#exit
Switch(config)#
Switch(config)#interface range tenGigabitEthernet 1/0/37-38
Switch(config-if-range)#stackwise-virtual dual-active-detection
WARNING: All the extraneous configurations will be removed for TenGigabitEthernet1/0/37 on reboot.
INFO: Upon reboot, the config will be part of running config but not part of start up config.
WARNING: All the extraneous configurations will be removed for TenGigabitEthernet1/0/38 on reboot.
INFO: Upon reboot, the config will be part of running config but not part of start up config.
Switch(config-if-range)#exit
Switch(config)#stack-mac persistent timer 0
WARNING: Stack MAC persistency timer value of 0 means that, after a
WARNING: master switchover, the current stack-mac will continue
WARNING: to be used indefinitely.
WARNING: The Network Administrators must make sure that the old
WARNING: stack-mac does not appear elsewhere in this network
WARNING: domain. If it does, user traffic may be blackholed.
Switch(config)#exit
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#save
Switch#reload
```

reload 実施後 2 台目の設定に移る

StackWise Virtual

SWV 設定②

■ SWV 設定後の確認

```
Switch#show switch
Switch/Stack Mac Address : 0027.90bf.0c00 - Local Mac Address
Mac persistency wait time: Indefinite
```

```
      H/W  Current
Switch#  Role  Mac Address  Priority Version  State
-----
*1      Active  0027.90bf.0c00  15   V01   Ready
2      Standby  0027.90bf.0c80  14   V01   Ready
```

```
Switch#show stackwise-virtual
Stackwise Virtual Configuration:
```

```
Stackwise Virtual : Enabled
Domain Number : 1
```

Enabled になっていること

```
Switch  Stackwise Virtual Link  Ports
-----
1      1                          TenGigabitEthernet1/0/39
                          TenGigabitEthernet1/0/40
2      1                          TenGigabitEthernet2/0/39
                          TenGigabitEthernet2/0/40
```

```
Switch# show stackwise-virtual link
Stackwise Virtual Link(SVL) Information:
```

```
Flags:
```

```
Link Status
```

```
U-Up D-Down
Protocol Status
```

```
S-Suspended P-Pending E-Error T-Timeout R-Ready
```

```
Switch  SVL  Ports  Link-Status  Protocol-Status
-----
1      1      TenGigabitEthernet1/0/39  U  R
          TenGigabitEthernet1/0/40  U  R
2      1      TenGigabitEthernet2/0/39  U  R
          TenGigabitEthernet2/0/40  U  R
```

SVL が指定したポートであり、Up になっていること

StackWise Virtual

障害時の動作確認

#	大項目	#	小項目	詳細
1	DAD Link 障害	1	All DAD Link down	StackWise Virtual の状態および、通信への影響なし
		2	Single DAD Link down	StackWise Virtual の状態および、通信への影響なし
2	機器障害	1	Active 電源断	期待通りの動作、Standby が Active に切り替わり、Active が Standby で立ち上がる
		2	Standby 電源断	期待通りの動作、Active が Active を保持し、Standby が Standby で立ち上がる
3	SVL Link 障害	1	All SVL Link down	期待通りの動作、Active がリカバリーへ移行
		2	Single SVL Link down	期待通りの動作、StackWise Virtual の状態への影響なし

3.1 Stack

StackWise Virtual

障害時の動作確認 1 - 1 All DAD Link down

■ 抜線時に DAD Link の Status が Down に変化

```
JU08-C9500#show stackwise-virtual dual-active-detection  
Dual-Active-Detection Configuration:
```

Switch	Dad port	Status
1	TenGigabitEthernet1/0/1	up
	TenGigabitEthernet1/0/2	up
2	TenGigabitEthernet2/0/1	up
	TenGigabitEthernet2/0/2	up



```
JU08-C9500#show stackwise-virtual dual-active-detection  
Dual-Active-Detection Configuration:
```

Switch	Dad port	Status
1	TenGigabitEthernet1/0/1	down
	TenGigabitEthernet1/0/2	down
2	TenGigabitEthernet2/0/1	down
	TenGigabitEthernet2/0/2	down

■ SVL の状態には変化なし

```
JU08-C9500#show stackwise-virtual neighbors  
Stackwise Virtual Link(SVL) Neighbors Information:
```

Switch	SVL	Local Port	Remote Port
1	1	TenGigabitEthernet1/0/39	TenGigabitEthernet2/0/39
		TenGigabitEthernet1/0/40	TenGigabitEthernet2/0/40
2	1	TenGigabitEthernet2/0/39	TenGigabitEthernet1/0/39
		TenGigabitEthernet2/0/40	TenGigabitEthernet1/0/40



```
JU08-C9500#show stackwise-virtual neighbors  
Stackwise Virtual Link(SVL) Neighbors Information:
```

Switch	SVL	Local Port	Remote Port
1	1	TenGigabitEthernet1/0/39	TenGigabitEthernet2/0/39
		TenGigabitEthernet1/0/40	TenGigabitEthernet2/0/40
2	1	TenGigabitEthernet2/0/39	TenGigabitEthernet1/0/39
		TenGigabitEthernet2/0/40	TenGigabitEthernet1/0/40

StackWise Virtual

障害時の動作確認 1 - 1 All DAD Link down

■ DAD Link を Down させたときのログ

```
*Dec 19 07:16:47.632: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/0/1, changed state to down
*Dec 19 07:16:47.713: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet2/0/1, changed state to down
*Dec 19 07:16:48.513: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet2/0/2, changed state to down
*Dec 19 07:16:48.546: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/0/2, changed state to down
*Dec 19 07:16:48.633: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/1, changed state to down
*Dec 19 07:16:48.713: %LINK-3-UPDOWN: Interface TenGigabitEthernet2/0/1, changed state to down
*Dec 19 07:16:49.514: %LINK-3-UPDOWN: Interface TenGigabitEthernet2/0/2, changed state to down
*Dec 19 07:16:49.548: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/2, changed state to down
*Dec 19 07:16:49.512: %STACKMGR-1-DUAL_ACTIVE_CFG_MSG: Switch 2 R0/0: stack_mgr: Dual Active Detection links are not available anymore
*Dec 19 07:16:49.547: %STACKMGR-1-DUAL_ACTIVE_CFG_MSG: Switch 1 R0/0: stack_mgr: Dual Active Detection links are not available anymore
```

■ DAD Link を Up させたときのログ

```
*Dec 19 07:19:13.244: %LINK-3-UPDOWN: Interface TenGigabitEthernet2/0/1, changed state to up
*Dec 19 07:19:13.267: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/1, changed state to up
*Dec 19 07:19:13.244: %STACKMGR-1-DUAL_ACTIVE_CFG_MSG: Switch 2 R0/0: stack_mgr: Dual Active Detection link is available now
*Dec 19 07:19:13.267: %STACKMGR-1-DUAL_ACTIVE_CFG_MSG: Switch 1 R0/0: stack_mgr: Dual Active Detection link is available now
*Dec 19 07:19:14.245: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet2/0/1, changed state to up
*Dec 19 07:19:14.268: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/0/1, changed state to up
*Dec 19 07:19:14.398: %LINK-3-UPDOWN: Interface TenGigabitEthernet2/0/2, changed state to up
*Dec 19 07:19:14.420: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/2, changed state to up
*Dec 19 07:19:15.399: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet2/0/2, changed state to up
*Dec 19 07:19:15.421: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/0/2, changed state to up
```

3.1 Stack

StackWise Virtual

障害時の動作確認 1 - 2 Single DAD Link down

■ 抜線時に DAD Link の Status が Down に変化

```
JU08-C9500#show stackwise-virtual dual-active-detection  
Dual-Active-Detection Configuration:
```

Switch	Dad port	Status
1	TenGigabitEthernet1/0/1	up
	TenGigabitEthernet1/0/2	up
2	TenGigabitEthernet2/0/1	up
	TenGigabitEthernet2/0/2	up



```
JU08-C9500#show stackwise-virtual dual-active-detection  
Dual-Active-Detection Configuration:
```

Switch	Dad port	Status
1	TenGigabitEthernet1/0/1	down
	TenGigabitEthernet1/0/2	up
2	TenGigabitEthernet2/0/1	down
	TenGigabitEthernet2/0/2	up

■ SVL の状態には変化なし

```
JU08-C9500#show stackwise-virtual neighbors  
Stackwise Virtual Link(SVL) Neighbors Information:
```

Switch	SVL	Local Port	Remote Port
1	1	TenGigabitEthernet1/0/39	TenGigabitEthernet2/0/39
		TenGigabitEthernet1/0/40	TenGigabitEthernet2/0/40
2	1	TenGigabitEthernet2/0/39	TenGigabitEthernet1/0/39
		TenGigabitEthernet2/0/40	TenGigabitEthernet1/0/40



```
JU08-C9500#show stackwise-virtual dual-active-detection neighbors  
Stackwise Virtual Link(SVL) Neighbors Information:
```

Switch	SVL	Local Port	Remote Port
1	1	TenGigabitEthernet1/0/39	TenGigabitEthernet2/0/39
		TenGigabitEthernet1/0/40	TenGigabitEthernet2/0/40
2	1	TenGigabitEthernet2/0/39	TenGigabitEthernet1/0/39
		TenGigabitEthernet2/0/40	TenGigabitEthernet1/0/40

StackWise Virtual

障害時の動作確認 1 - 2 Single DAD Link down

■ DAD Link を Down させたときのログ

```
*Dec 19 07:25:46.747: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet2/0/1, changed state to down
*Dec 19 07:25:46.774: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/0/1, changed state to down
*Dec 19 07:25:47.748: %LINK-3-UPDOWN: Interface TenGigabitEthernet2/0/1, changed state to down
*Dec 19 07:25:47.775: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/1, changed state to down
```

■ DAD Link を Up させたときのログ

```
*Dec 19 07:27:25.157: %LINK-3-UPDOWN: Interface TenGigabitEthernet2/0/1, changed state to up
*Dec 19 07:27:25.184: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/1, changed state to up
*Dec 19 07:27:26.157: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet2/0/1, changed state to up
*Dec 19 07:27:26.184: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/0/1, changed state to up
```

3.1 Stack

StackWise Virtual

障害時の動作確認 2 - 1 Active 電源断

■ 電源断後に Active が Member に、Standby が Active に変化

```
JU08-C9500#sh switch
Switch/Stack Mac Address : 0027.90be.fa80 - Local Mac Address
Mac persistency wait time: Indefinite
```

			H/W	Current		
Switch#	Role	Mac Address	Priority	Version	State	
*1	Active	0027.90be.fa80	1	V01	Ready	
2	Standby	00a3.d15b.0980	1	V01	Ready	



```
JU08-C9500#sh switch
Switch/Stack Mac Address : 0027.90be.fa80 * Foreign Mac Address
Mac persistency wait time: Indefinite
```

			H/W	Current		
Switch#	Role	Mac Address	Priority	Version	State	
1	Member	0000.0000.0000	0	V01	Removed	
*2	Active	00a3.d15b.0980	1	V01	Ready	

■ 電源投入後に元 Active が Standby として立ち上がる

```
JU08-C9500#sh switch
Switch/Stack Mac Address : 0027.90be.fa80 - Local Mac Address
Mac persistency wait time: Indefinite
```

			H/W	Current		
Switch#	Role	Mac Address	Priority	Version	State	
1	Standby	0027.90be.fa80	1	V01	Ready	
*2	Active	00a3.d15b.0980	1	V01	Ready	

※ "stack-mac persistent timer 0" の設定により、
MAC アドレスが引き継がれている

3.1 Stack

StackWise Virtual

障害時の動作確認 2-1 Active 電源断

■ 電源断後に表示されるログ

```
%IOSXE_INFRA-6-CONSOLE_ACTIVE: R0/0 console active. Press RETURN to get started!  
*Dec 21 04:27:19.221: %HMANRP-6-HMAN_IOS_CHANNEL_INFO: HMAN-IOS channel event for switch 2: EMP_RELAY: Channel UP!  
*Dec 21 04:27:19.221: %PLATFORM-6-HASTATUS: RP switchover, received chassis event to become active  
*Dec 21 04:27:19.229: %HMANRP-6-EMP_NO_ELECTION_INFO: Could not elect active EMP switch, setting emp active switch to 0: EMP_RELAY: Could not elect switch with mgmt port UP  
*Dec 21 04:27:19.300: %REDUNDANCY-3-SWITCHOVER: RP switchover (PEER_NOT_PRESENT)  
*Dec 21 04:27:19.300: %REDUNDANCY-3-SWITCHOVER: RP switchover (PEER_DOWN)  
*Dec 21 04:27:19.300: %REDUNDANCY-3-SWITCHOVER: RP switchover (PEER_REDUNDANCY_STATE_CHANGE)  
*Dec 21 04:27:19.288: %STACKMGR-1-DUAL_ACTIVE_CFG_MSG: Switch 2 R0/0: stack_mgr: Dual Active Detection link is available now  
*Dec 21 04:27:19.869: %LINK-3-UPDOWN: Interface Lsmpl19/3, changed state to up  
*Dec 21 04:27:19.870: %LINK-3-UPDOWN: Interface EOBC19/1, changed state to up  
*Dec 21 04:27:19.870: %LINK-3-UPDOWN: Interface LIIN19/2, changed state to up  
*Dec 21 04:27:20.870: %LINEPROTO-5-UPDOWN: Line protocol on Interface Lsmpl19/3, changed state to up  
*Dec 21 04:27:20.870: %LINEPROTO-5-UPDOWN: Line protocol on Interface EOBC19/1, changed state to up  
*Dec 21 04:27:20.870: %LINEPROTO-5-UPDOWN: Line protocol on Interface LIIN19/2, changed state to up  
*Dec 21 04:27:20.882: %CALL_HOME-6-CALL_HOME_ENABLED: Call-home is enabled by Smart Agent for Licensing.  
*Dec 21 04:27:20.882: %SMART_LIC-5-COMM_RESTORED: Communications with the Cisco Smart Software Manager or satellite restored  
*Dec 21 04:27:21.838: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/1, changed state to down  
*Dec 21 04:27:21.838: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/2, changed state to down  
*Dec 21 04:27:21.838: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/3, changed state to down  
*Dec 21 04:27:21.840: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/4, changed state to down  
*Dec 21 04:27:21.845: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/39, changed state to down  
*Dec 21 04:27:21.845: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/40, changed state to down  
*Dec 21 04:27:21.897: %LINK-3-UPDOWN: Interface Null0, changed state to up  
*Dec 21 04:27:21.897: %LINK-3-UPDOWN: Interface Vlan30, changed state to up  
*Dec 21 04:27:21.902: %LINK-3-UPDOWN: Interface TenGigabitEthernet2/0/3, changed state to up  
*Dec 21 04:27:21.902: %LINK-3-UPDOWN: Interface TenGigabitEthernet2/0/4, changed state to up  
*Dec 21 04:27:21.905: %LINK-3-UPDOWN: Interface Port-channel2, changed state to up  
*Dec 21 04:27:21.905: %LINK-3-UPDOWN: Interface Port-channel3, changed state to up  
*Dec 21 04:27:21.905: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up  
*Dec 21 04:27:21.905: %LINK-3-UPDOWN: Interface Loopback0, changed state to up  
*Dec 21 04:27:21.915: %LINK-5-CHANGED: Interface Vlan1, changed state to administratively down  
*Dec 21 04:27:21.968: %STACKMGR-1-DUAL_ACTIVE_CFG_MSG: Switch 2 R0/0: stack_mgr: Dual Active Detection links are not available anymore  
*Dec 21 04:27:22.898: %LINEPROTO-5-UPDOWN: Line protocol on Interface Null0, changed state to up  
*Dec 21 04:27:22.901: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet2/0/3, changed state to up  
*Dec 21 04:27:22.903: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet2/0/4, changed state to up  
*Dec 21 04:27:22.905: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel2, changed state to up  
*Dec 21 04:27:22.905: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel3, changed state to up  
*Dec 21 04:27:29.814: %HMANRP-6-EMP_NO_ELECTION_INFO: Could not elect active EMP switch, setting emp active switch to 0: EMP_RELAY: Could not elect switch with mgmt port UP
```

3.1 Stack

StackWise Virtual

障害時の動作確認 2 - 2 Standby 電源断

■ 電源断後に Active に変化は見られず、Standby が Member に変化

```
JU08-C9500#sh switch
Switch/Stack Mac Address : 0027.90be.fa80 - Local Mac Address
Mac persistency wait time: Indefinite
```

Switch#	Role	Mac Address	H/W	Current	Priority	Version	State
1	Standby	0027.90be.fa80	1	V01	1	V01	Ready
*2	Active	00a3.d15b.0980	1	V01	1	V01	Ready



```
JU08-C9500#sh switch
Switch/Stack Mac Address : 0027.90be.fa80 - Foreign Mac Address
Mac persistency wait time: Indefinite
```

Switch#	Role	Mac Address	H/W	Current	Priority	Version	State
1	Member	0000.0000.0000	0	V01	0	V01	Removed
*2	Active	00a3.d15b.0980	1	V01	1	V01	Ready

■ 電源投入後に元 Active が Standby として立ち上がる

```
JU08-C9500#sh switch
Switch/Stack Mac Address : 0027.90be.fa80 - Local Mac Address
Mac persistency wait time: Indefinite
```

Switch#	Role	Mac Address	H/W	Current	Priority	Version	State
1	Standby	0027.90be.fa80	1	V01	1	V01	Ready
*2	Active	00a3.d15b.0980	1	V01	1	V01	Ready

3.1 Stack

StackWise Virtual

障害時の動作確認 2-2 Standby 電源断

■ 電源復旧後に表示されるログ

```
*Dec 21 04:54:22.953: %LINK-3-UPDOWN: Interface TenGigabitEthernet2/0/1, changed state to up
*Dec 21 04:54:22.965: %LINK-3-UPDOWN: Interface TenGigabitEthernet2/0/2, changed state to up
*Dec 21 04:54:22.974: %LINK-3-UPDOWN: Interface TenGigabitEthernet2/0/39, changed state to up
*Dec 21 04:54:22.983: %LINK-3-UPDOWN: Interface TenGigabitEthernet2/0/40, changed state to up
*Dec 21 04:54:22.954: %STACKMGR-1-DUAL_ACTIVE_CFG_MSG: Switch 2 R0/0: stack_mgr: Dual Active Detection link is available now
*Dec 21 04:54:22.974: %NIF_MGR-6-PORT_LINK_UP: Switch 2 R0/0: nif_mgr: Port 39 on front side stack link 0 is UP.
*Dec 21 04:54:22.974: %NIF_MGR-6-PORT_CONN_PENDING: Switch 2 R0/0: nif_mgr: Port 39 on front side stack link 0 connection is PENDING.
*Dec 21 04:54:23.954: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet2/0/1, changed state to up
*Dec 21 04:54:23.965: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet2/0/2, changed state to up
*Dec 21 04:54:23.974: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet2/0/39, changed state to up
*Dec 21 04:54:23.983: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet2/0/40, changed state to up
*Dec 21 04:54:30.629: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet2/0/1, changed state to down
*Dec 21 04:54:32.629: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet2/0/1, changed state to up
*Dec 21 04:54:33.532: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet2/0/2, changed state to down
*Dec 21 04:54:35.532: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet2/0/2, changed state to up
*Dec 21 04:54:35.550: %NIF_MGR-6-PORT_LINK_DOWN: Switch 2 R0/0: nif_mgr: Port 39 on front side stack link 0 is DOWN.
*Dec 21 04:54:35.550: %NIF_MGR-6-PORT_CONN_DISCONNECTED: Switch 2 R0/0: nif_mgr: Port 39 on front side stack link 0 connection has DISCONNECTED: CONN_ERR_PORT_LINK_DOWN_EVENT
*Dec 21 04:54:36.552: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet2/0/39, changed state to down
*Dec 21 04:54:38.551: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet2/0/39, changed state to up
*Dec 21 04:54:38.445: %NIF_MGR-6-PORT_LINK_DOWN: Switch 2 R0/0: nif_mgr: Port 40 on front side stack link 0 is DOWN.
*Dec 21 04:54:38.445: %NIF_MGR-6-PORT_CONN_DISCONNECTED: Switch 2 R0/0: nif_mgr: Port 40 on front side stack link 0 connection has DISCONNECTED: CONN_ERR_PORT_LINK_DOWN_EVENT
*Dec 21 04:54:38.829: %NIF_MGR-6-PORT_LINK_UP: Switch 2 R0/0: nif_mgr: Port 39 on front side stack link 0 is UP.
*Dec 21 04:54:38.829: %NIF_MGR-6-PORT_CONN_PENDING: Switch 2 R0/0: nif_mgr: Port 39 on front side stack link 0 connection is PENDING.
*Dec 21 04:54:39.445: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet2/0/40, changed state to down
*Dec 21 04:54:41.447: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet2/0/40, changed state to up
*Dec 21 04:54:41.846: %NIF_MGR-6-PORT_LINK_UP: Switch 2 R0/0: nif_mgr: Port 40 on front side stack link 0 is UP.
*Dec 21 04:54:41.846: %NIF_MGR-6-PORT_CONN_PENDING: Switch 2 R0/0: nif_mgr: Port 40 on front side stack link 0 connection is PENDING.
*Dec 21 04:54:48.342: %NIF_MGR-6-PORT_CONNECTION_STATUS_CHANGE: Switch 2 R0/0: nif_mgr: PORT lpn:39 changed state from Pending to Ready.
*Dec 21 04:54:48.342: %NIF_MGR-6-PORT_CONN_READY: Switch 2 R0/0: nif_mgr: Port 39 on front side stack link 0 connection is READY.
*Dec 21 04:54:48.344: %NIF_MGR-6-STACK_LINK_UP: Switch 2 R0/0: nif_mgr: Front side stack link 0 is UP.
*Dec 21 04:54:48.344: %STACKMGR-6-STACK_LINK_CHANGE: Switch 2 R0/0: stack_mgr: Stack port 1 on Switch 2 is up
*Dec 21 04:54:52.761: %STACKMGR-6-SWITCH_ADDED: Switch 2 R0/0: stack_mgr: Switch 1 has been added to the stack.
*Dec 21 04:54:53.970: %STACKMGR-6-SWITCH_ADDED: Switch 2 R0/0: stack_mgr: Switch 1 has been added to the stack.
*Dec 21 04:54:56.610: %IOSD_INFRA-6-IFS_DEVICE_OIR: Device usbflash0-1 added
*Dec 21 04:54:56.635: %SMART_LIC-5-EVAL_START: Entering evaluation period
*Dec 21 04:54:56.636: %SMART_LIC-5-EVAL_START: Entering evaluation period
*Dec 21 04:54:56.665: %IOSD_INFRA-6-IFS_DEVICE_OIR: Device usbflash0-1 added
*Dec 21 04:52:35.144: %IOSXE-3-PLATFORM: Switch 1 R0/0: kernel: igb 0000:0c:00:0: The NVM Checksum Is Not Valid
```


3.1 Stack

StackWise Virtual

障害時の動作確認 2 - 2 Standby 電源断

■ 電源復旧後に表示されるログ(続き)

```
*Dec 21 04:53:26.938: %PMAN-5-EXITACTION: Switch 1 R0/0: pyp: Process manager is exiting:
*Dec 21 04:54:56.985: %FED_PM-3-FRU_SWITCH_TIMEOUT: Switch 1 R0/0: fed: Transceiver update timed out. Remove and re-insert all FRUs in this switch to recover.
*Dec 21 04:54:57.309: %NIF_MGR-6-PORT_LINK_UP: Switch 1 R0/0: nif_mgr: Port 39 on front side stack link 0 is UP.
*Dec 21 04:54:57.309: %STACKMGR-6-STACK_LINK_CHANGE: Switch 1 R0/0: stack_mgr: Stack port 2 on Switch 1 is nocable
*Dec 21 04:54:57.309: %NIF_MGR-6-PORT_CONN_PENDING: Switch 1 R0/0: nif_mgr: Port 39 on front side stack link 0 connection is PENDING.
*Dec 21 04:54:57.309: %NIF_MGR-6-PORT_CONNECTION_STATUS_CHANGE: Switch 1 R0/0: nif_mgr: PORT lpn:39 changed state from Pending to Ready.
*Dec 21 04:54:57.309: %STACKMGR-6-STACK_LINK_CHANGE: Switch 1 R0/0: stack_mgr: Stack port 1 on Switch 1 is down
*Dec 21 04:54:57.309: %NIF_MGR-6-PORT_CONN_READY: Switch 1 R0/0: nif_mgr: Port 39 on front side stack link 0 connection is READY.
*Dec 21 04:54:57.309: %STACKMGR-1-DUAL_ACTIVE_CFG_MSG: Switch 1 R0/0: stack_mgr: Dual Active Detection link is available now
*Dec 21 04:54:57.309: %NIF_MGR-6-STACK_LINK_UP: Switch 1 R0/0: nif_mgr: Front side stack link 0 is UP.
*Dec 21 04:54:57.309: %STACKMGR-6-STACK_LINK_CHANGE: Switch 1 R0/0: stack_mgr: Stack port 1 on Switch 1 is up
*Dec 21 04:54:57.309: %STACKMGR-6-SWITCH_ADDED: Switch 1 R0/0: stack_mgr: Switch 1 has been added to the stack.
*Dec 21 04:54:57.309: %STACKMGR-6-SWITCH_ADDED: Switch 1 R0/0: stack_mgr: Switch 1 has been added to the stack.
*Dec 21 04:54:58.108: %STACKMGR-1-DUAL_ACTIVE_CFG_MSG: Switch 1 R0/0: stack_mgr: Dual Active Detection link is available now
*Dec 21 04:54:58.654: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/1/1, changed state to down
*Dec 21 04:54:58.655: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/1/2, changed state to down
*Dec 21 04:54:58.656: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/1/3, changed state to down
*Dec 21 04:54:58.656: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/1/4, changed state to down
*Dec 21 04:54:58.656: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/1/5, changed state to down
*Dec 21 04:54:58.656: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/1/6, changed state to down
*Dec 21 04:54:58.656: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/1/7, changed state to down
*Dec 21 04:54:58.656: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/1/8, changed state to down
*Dec 21 04:54:58.656: %LINK-3-UPDOWN: Interface FortyGigabitEthernet1/1/1, changed state to down
*Dec 21 04:54:58.656: %LINK-3-UPDOWN: Interface FortyGigabitEthernet1/1/2, changed state to down
*Dec 21 04:54:58.973: %IOSD_INFRA-6-IFS_DEVICE_OIR: Device usbflash0-1 added
*Dec 21 04:54:59.344: %HMANRP-6-HMAN_IOS_CHANNEL_INFO: HMAN-IOS channel event for switch 1: EMP_RELAY: Channel UP!
*Dec 21 04:54:59.345: %HMANRP-6-EMP_NO_ELECTION_INFO: Could not elect active EMP switch, setting emp active switch to 0: EMP_RELAY: Could not elect switch with mgmt port UP
*Dec 21 04:55:02.528: %PLATFORM_PM-6-MODULE_INSERTED: SFP module inserted with interface name Te1/0/3
*Dec 21 04:55:05.476: %PLATFORM_PM-6-MODULE_INSERTED: SFP module inserted with interface name Te1/0/4
*Dec 21 04:55:25.973: %PLATFORM_PM-6-FRULINK_INSERTED: 2x40G uplink module inserted in the switch 1 slot 1
*Dec 21 04:55:26.170: %PLATFORM_PM-6-MODULE_INSERTED: SFP module inserted with interface name Te1/0/1
*Dec 21 04:55:26.171: %PLATFORM_PM-6-MODULE_INSERTED: SFP module inserted with interface name Te1/0/2
*Dec 21 04:55:27.343: %PLATFORM_PM-6-MODULE_INSERTED: SFP module inserted with interface name Te1/0/39
*Dec 21 04:55:27.374: %PLATFORM_PM-6-MODULE_INSERTED: SFP module inserted with interface name Te1/0/40
*Dec 21 04:55:28.171: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/1, changed state to up
*Dec 21 04:55:28.172: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/2, changed state to up
*Dec 21 04:55:29.171: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/0/1, changed state to up
*Dec 21 04:55:29.171: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/0/2, changed state to up
*Dec 21 04:55:29.373: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/39, changed state to up
*Dec 21 04:55:29.375: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/40, changed state to up
*Dec 21 04:55:30.373: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/0/39, changed state to up
*Dec 21 04:55:30.374: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/0/40, changed state to up
*Dec 21 04:56:56.353: %IOSXE_REDUNDANCY-6-PEER: Active detected switch 1 as standby.
*Dec 21 04:56:56.352: %STACKMGR-6-STANDBY_ELECTED: Switch 2 R0/0: stack_mgr: Switch 1 has been elected STANDBY.
*Dec 21 04:57:01.422: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion (raw-event=PEER_FOUND(4))
*Dec 21 04:57:01.422: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion (raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))
*Dec 21 04:57:42.440: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEEDED: Bulk Sync succeeded
*Dec 21 04:57:43.441: %RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
*Dec 21 04:57:45.887: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/3, changed state to up
*Dec 21 04:57:45.893: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/4, changed state to up
*Dec 21 04:57:46.887: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/0/3, changed state to up
*Dec 21 04:57:46.893: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/0/4, changed state to up
```

3.1 Stack

StackWise Virtual

障害時の動作確認 3 - 1 All SVL Link down

■ SVL 全断後に Active が Recovery-mode に、Standby が Active に変化 (両Act)

SBY側

```
JU08-C9500#show switch
Switch/Stack Mac Address : 0027.90be.fa80 - Local Mac Address
Mac persistency wait time: Indefinite
```

			H/W	Current		
Switch#	Role	Mac Address	Priority	Version	State	

*1	Active	0027.90be.fa80	1	V01	Ready	
2	Member	0000.0000.0000	0	V01	Removed	

Act側

```
JU08-C9500(recovery-mode)#show switch
Switch/Stack Mac Address : 0027.90be.fa80 - Foreign Mac Address
Mac persistency wait time: Indefinite
```

			H/W	Current		
Switch#	Role	Mac Address	Priority	Version	State	

1	Member	0000.0000.0000	0	V01	Removed	
*2	Active	00a3.d15b.0980	1	V01	Ready	

■ SVL 復旧後に元 Active で Reload を実施、その後 Standby として立ち上がる

```
*Dec 21 07:07:46.408: %NIF_MGR-6-DAD_RECOVERY_RELOAD_ALERT: Switch 2 R0/0: nif_mgr: Switch is in recovery mode, needs Reload now. one or more SVL is up
```

```
JU08-C9500#show switch
Switch/Stack Mac Address : 0027.90be.fa80 - Local Mac Address
Mac persistency wait time: Indefinite
```

			H/W	Current		
Switch#	Role	Mac Address	Priority	Version	State	

*1	Active	0027.90be.fa80	1	V01	Ready	
2	Standby	00a3.d15b.0980	1	V01	Ready	

上記のように、
元 Active 側に reload を促すメッセージが表示される。

3.1 Stack

StackWise Virtual

障害時の動作確認 3 - 1 All SVL Link down

■ SVL 抜線後に表示されるログ(1 / 2)

```
*Dec 21 07:05:41.507: %NIF_MGR-6-PORT_LINK_DOWN: Switch 2 R0/0: nif_mgr: Port 39 on front side stack link 0 is DOWN.
*Dec 21 07:05:41.507: %NIF_MGR-6-PORT_CONN_DISCONNECTED: Switch 2 R0/0: nif_mgr: Port 39 on front side stack link 0 connection has DISCONNECTED: CONN_ERR_PORT_LINK_DOWN_EVENT
*Dec 21 07:05:41.610: %NIF_MGR-6-PORT_LINK_DOWN: Switch 1
%IOSXE_INFRA-6-CONSOLE_ACTIVE: R0/0 console active. Press RETURN to get started!
Configuration succeed, but fail to parse the address. Perhaps DNS configuration is not done yet or you configure an invalid address.
*Dec 21 07:05:42.998: %PLATFORM-6-HASTATUS: RP switchover, received chassis event to become active
*Dec 21 07:05:43.003: %HMANRP-6-HMAN_IOS_CHANNEL_INFO: HMAN-IOS channel event for switch 1: EMP_RELAY: Channel UP!
*Dec 21 07:05:43.015: %HMANRP-6-EMP_NO_ELECTION_INFO: Could not elect active EMP switch, setting emp active switch to 0: EMP_RELAY: Could not elect switch with mgmt port UP
*Dec 21 07:05:43.026: %REDUNDANCY-3-SWITCHOVER: RP switchover (PEER_NOT_PRESENT)
*Dec 21 07:05:43.027: %REDUNDANCY-3-SWITCHOVER: RP switchover (PEER_DOWN)
*Dec 21 07:05:43.027: %REDUNDANCY-3-SWITCHOVER: RP switchover (PEER_REDUNDANCY_STATE_CHANGE)
*Dec 21 07:05:43.033: %PLATFORM-6-HASTATUS: RP switchover, sent message became active. IOS is ready to switch to primary after chassis confirmation
*Dec 21 07:05:43.035: %PLATFORM-6-HASTATUS: RP switchover, received chassis event became active
*Dec 21 07:05:43.136: %IOSD_INFRA-6-IFS_DEVICE_OIR: Device usbflash0-2 removed
*Dec 21 07:05:42.989: %NIF_MGR-6-PORT_LINK_DOWN: Switch 1 R0/0: nif_mgr: Port 40 on front side stack link 0 is DOWN.
*Dec 21 07:05:42.989: %NIF_MGR-6-PORT_CONN_DISCONNECTED: Switch 1 R0/0: nif_mgr: Port 40 on front side stack link 0 connection has DISCONNECTED: CONN_ERR_PORT_LINK_DOWN_EVENT
*Dec 21 07:05:42.989: %NIF_MGR-6-STACK_LINK_DOWN: Switch 1 R0/0: nif_mgr: Front side stack link 0 is DOWN.
*Dec 21 07:05:42.989: %STACKMGR-6-STACK_LINK_CHANGE: Switch 1 R0/0: stack_mgr: Stack port 1 on Switch 1 is down
*Dec 21 07:05:43.075: %STACKMGR-1-DUAL_ACTIVE_CFG_MSG: Switch 1 R0/0: stack_mgr: Dual Active Detection link is available now
*Dec 21 07:05:43.282: %PLATFORM-6-HASTATUS_DETAIL: RP switchover, received chassis event became active. Switch to primary (count 1)
*Dec 21 07:05:43.371: %LINK-3-UPDOWN: Interface Lsmpi18/3, changed state to up
*Dec 21 07:05:43.372: %LINK-3-UPDOWN: Interface EOBC18/1, changed state to up
*Dec 21 07:05:43.372: %LINK-3-UPDOWN: Interface LIIN18/2, changed state to up
*Dec 21 07:05:44.371: %LINEPROTO-5-UPDOWN: Line protocol on Interface Lsmpi18/3, changed state to up
*Dec 21 07:05:44.371: %LINEPROTO-5-UPDOWN: Line protocol on Interface EOBC18/1, changed state to up
*Dec 21 07:05:44.372: %LINEPROTO-5-UPDOWN: Line protocol on Interface LIIN18/2, changed state to up
```

3.1 Stack

StackWise Virtual

障害時の動作確認 3 - 1 All SVL Link down

■ SVL 抜線後に表示されるログ(2 / 2)

```
*Dec 21 07:05:44.570: %CALL_HOME-6-CALL_HOME_ENABLED: Call-home is enabled by Smart Agent for Licensing.
*Dec 21 07:05:44.571: %SMART_LIC-5-COMM_RESTORED: Communications with the Cisco Smart Software Manager or satellite restored
*Dec 21 07:05:45.081: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/40, changed state to up
*Dec 21 07:05:45.345: %LINK-3-UPDOWN: Interface TenGigabitEthernet2/0/1, changed state to down
*Dec 21 07:05:45.345: %LINK-3-UPDOWN: Interface TenGigabitEthernet2/0/2, changed state to down
*Dec 21 07:05:45.345: %LINK-3-UPDOWN: Interface TenGigabitEthernet2/0/3, changed state to down
*Dec 21 07:05:45.347: %LINK-3-UPDOWN: Interface TenGigabitEthernet2/0/4, changed state to down
*Dec 21 07:05:45.351: %LINK-3-UPDOWN: Interface TenGigabitEthernet2/0/40, changed state to down
*Dec 21 07:05:45.587: %LINK-3-UPDOWN: Interface Null0, changed state to up
*Dec 21 07:05:45.588: %LINK-3-UPDOWN: Interface Vlan30, changed state to up
*Dec 21 07:05:45.588: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/1, changed state to up
*Dec 21 07:05:45.589: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/2, changed state to up
*Dec 21 07:05:45.589: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/3, changed state to up
*Dec 21 07:05:45.590: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/4, changed state to up
*Dec 21 07:05:45.594: %LINK-3-UPDOWN: Interface Port-channel2, changed state to up
*Dec 21 07:05:45.595: %LINK-3-UPDOWN: Interface Port-channel3, changed state to up
*Dec 21 07:05:45.607: %LINK-5-CHANGED: Interface Vlan1, changed state to administratively down
*Dec 21 07:05:46.587: %LINEPROTO-5-UPDOWN: Line protocol on Interface Null0, changed state to up
*Dec 21 07:05:46.587: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up
*Dec 21 07:05:46.588: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/0/1, changed state to up
*Dec 21 07:05:46.590: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/0/2, changed state to up
*Dec 21 07:05:46.590: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/0/3, changed state to up
*Dec 21 07:05:46.591: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/0/4, changed state to up
*Dec 21 07:05:46.597: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel2, changed state to up
*Dec 21 07:05:46.597: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel3, changed state to up
*Dec 21 07:05:53.575: %HMANRP-6-EMP_NO_ELECTION_INFO: Could not elect active EMP switch, setting emp active switch to 0: EMP_RELAY: Could not elect switch with mgmt port UP
```

3.1 Stack

StackWise Virtual

障害時の動作確認 3 - 1 All SVL Link down

■ SVL 復旧後に表示されるログ

```
*Dec 21 07:07:37.636: %NIF_MGR-6-PORT_LINK_UP: Switch 1 R0/0: nif_mgr: Port 40 on front side stack link 0 is UP.  
*Dec 21 07:07:37.636: %NIF_MGR-6-PORT_CONN_PENDING: Switch 1 R0/0: nif_mgr: Port 40 on front side stack link 0 connection is PENDING.  
*Dec 21 07:07:38.636: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/0/40, changed state to up  
*Dec 21 07:07:41.872: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/39, changed state to up  
*Dec 21 07:07:41.872: %NIF_MGR-6-PORT_LINK_UP: Switch 1 R0/0: nif_mgr: Port 39 on front side stack link 0 is UP.  
*Dec 21 07:07:41.872: %NIF_MGR-6-PORT_CONN_PENDING: Switch 1 R0/0: nif_mgr: Port 39 on front side stack link 0 connection is PENDING.  
*Dec 21 07:07:42.872: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/0/39, changed state to up  
*Dec 21 07:07:42.937: %NIF_MGR-6-PORT_CONNECTION_STATUS_CHANGE: Switch 1 R0/0: nif_mgr: PORT lpn:40 changed state from Pending to Ready.  
*Dec 21 07:07:42.937: %NIF_MGR-6-PORT_CONN_READY: Switch 1 R0/0: nif_mgr: Port 40 on front side stack link 0 connection is READY.  
*Dec 21 07:07:42.937: %NIF_MGR-6-STACK_LINK_UP: Switch 1 R0/0: nif_mgr: Front side stack link 0 is UP.  
*Dec 21 07:07:42.937: %STACKMGR-6-STACK_LINK_CHANGE: Switch 1 R0/0: stack_mgr: Stack port 1 on Switch 1 is up  
*Dec 21 07:07:45.938: %NIF_MGR-6-PORT_CONNECTION_STATUS_CHANGE: Switch 1 R0/0: nif_mgr: PORT lpn:39 changed state from Pending to Ready.  
*Dec 21 07:07:45.938: %NIF_MGR-6-PORT_CONN_READY: Switch 1 R0/0: nif_mgr: Port 39 on front side stack link 0 connection is READY.
```

3.1 Stack

StackWise Virtual

障害時の動作確認 3 - 2 Single SVL Link down

- スタックの状態に変化はなし、抜線した SVL ステータスが Up から Down へ、Protocol ステータスが Ready から Suspended へ変化

```
JU08-C9500#show stackwise-virtual link
Stackwise Virtual Link(SVL) Information:
```

```
-----
Flags:
```

```
-----
Link Status
```

```
-----
U-Up D-Down
```

```
Protocol Status
```

```
-----
S-Suspended P-Pending E-Error T-Timeout R-Ready
```

Switch	SVL	Ports	Link-Status	Protocol-Status
1	1	TenGigabitEthernet1/0/39	D	S
		TenGigabitEthernet1/0/40	U	R
2	1	TenGigabitEthernet2/0/39	D	S
		TenGigabitEthernet2/0/40	U	R

StackWise

StackWise 機能は、複数のスイッチ機器を1つの論理スイッチとして動作することができ、拡張性や耐障害性に対応します。

■ 特徴

1つの論理スイッチ内では共有した設定やその他の情報を共有しスタックの機器内にて共有されます。

運用を中断することなく、動作中のスタックに対して機器を追加したり削除することができます。

■ 既存機器との比較

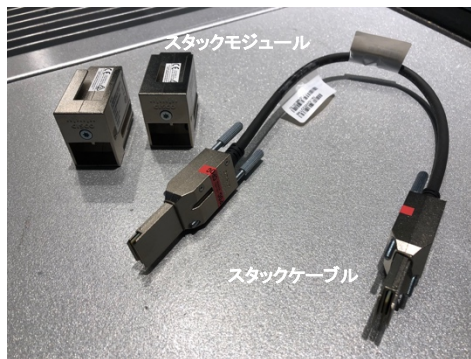
StackWise の動作や、コマンドに関しては同じになります。

物理的な Stack モジュールやケーブルは専用品となりますので異なる機種との互換性や相互接続はありません。

■ 注意点

同じ IOS-XE の Version、同じライセンスのみにて StackWise 機能をサポートしています。

一部の製品にてスタック モジュールやスタックケーブルが同様の形状をしていますが、接続サポートしていません。



<C9200L-STACK-KIT>

- ・C9200L SKU専用スタックモジュール X 2個
- ・データスタック 50cm ケーブル X 1本 (STACK-KITの標準選択ケーブル)
- ・50cm ケーブル長の他に1m、3mを選択可能

< STACK-T1-xxCM >

- ・C9300で使用できる。スタックケーブル
- ・ケーブル長は50cm、1m、3m

StackWise

Cisco Catalyst 9200 シリーズの場合、StackWise を構成するには機器に対応した STACK-KIT が別途必要となり、オプション購入になります。

■ スタックモジュールの取り付け

機器購入時と同時に STACK-KIT を購入している場合、取り付けられた状態で出荷されます。

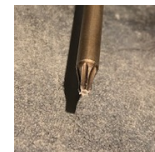
本体購入後に STACK-KIT を購入した場合や、障害などでスタックモジュールを交換することになった場合は取り付け作業が必要になります。StackWise テクノロジーはリング構成になるため、1 台の機器について 2 つのスタック モジュールを取り付けます。

スタック モジュールの取り付け、取り外しには、トルクス(T15) ドライバーが必要になります。トルクスを回さないで取り付けることはできません。

■ スタック モジュールの取り外し

トルクス(T15)ドライバーを使用し取り外しを行います。

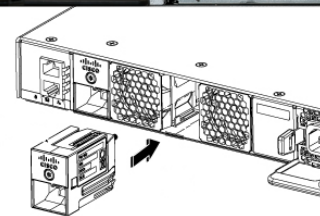
スタック モジュール自体には取っ手が無いため、スタック ケーブルを取り付けた状態でケーブルを持って引き出します。



トルクスT15の形状



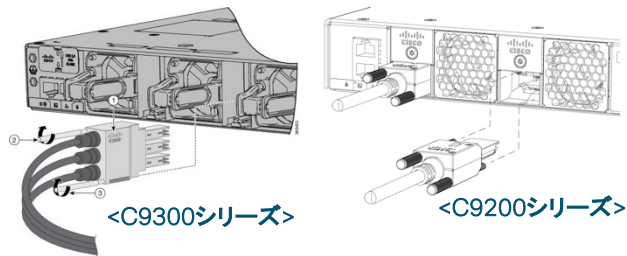
スタック ケーブルを取り付けた状態



※ STACK-KIT を別途購入した場合はレンチ型のトルクスT15が付属されています。

～StackWise～ 続き

StackWise テクノロジーでは最大 8 台の機器を構成に組むことができます。



■ スタック ケーブルの取り付け

StackWise のコネクタ部にスタック ケーブルを取り付け、2 本のネジを時計回りに締めます。

※必要以上に取り付け取り外しを行わないでください。

— StackWiseケーブル

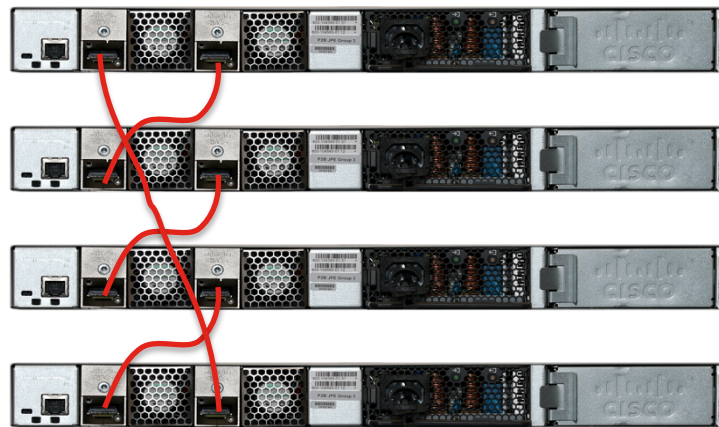
■ StackWise の 2 台の接続構成イメージ

スタック ケーブルはクロスになるように取り付けを行ってください。



Cisco Catalyst 9300
例

■ StackWise の 4 台の接続構成イメージ



Cisco Catalyst 9200 例

StackWise

■ StackWise の接続について

電源が ON の状態からスタック ケーブルを接続すると、スタック機器内で優先順位を決定しアクティブ(マスター)スイッチの決定、マスター スイッチ以外の機器に関しては一度再起動を行ってスタック グループ内に参加します。

アクティブ機器になる条件は以下の通りになります。

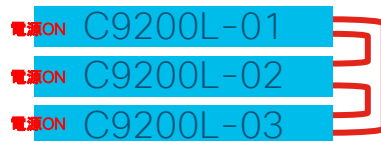
1. プライオリティを設定しておくことにより優先してアクティブになります。プライオリティが同じの場合は MAC アドレス値がもっとも小さいスイッチがアクティブなる。
2. 設定に関係なくアクティブ スイッチを決めたい場合は、アクティブ スイッチにしたい電源を最初に入れ、1 分以降に他のスイッチの電源を入れる。

一度、スタック グループ構成になった機器は、スタック構成から離れた場合でも設定を引き続き使用することは可能になりますが、再度スタック グループ構成に戻した場合は、一度再起動を行ってからスタック グループ内に参加します。

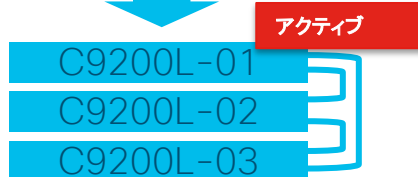
■ 注意

StackWise 構成になると、両機器とも同じコンソール表示になります。

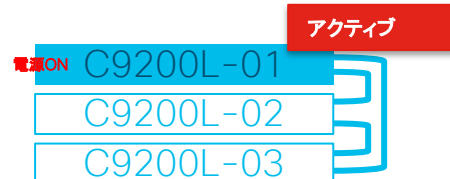
ほぼ同時に機器の電源を ON した場合、または電源 ON からスタックケーブルを接続した場合



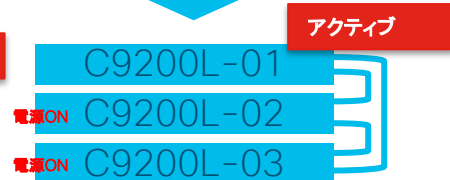
マスターの選出。高いプライオリティ値、同じ値の場合は MAC アドレスが若い機器
マスター機器以外は再起動



設定に関係なくアクティブを選択したい場合



1分以降に他機器の電源 ON



StackWise

■ プライオリティ値の設定

アクティブ(マスター)スイッチを決めるための値を設定します。
(デフォルトで 1、最優先値で 15 になります。)

```
C9200#switch 1 priority 10  
WARNING: Changing the switch priority may result in a configuration change for that switch. New Switch Priority  
will be effective after next reboot. Do you want to continue?[y/n]? [yes]: yes  
C9200#
```

デフォルトで 1、最高値で 15 になります。

スタック構成が変更されるため、再起動などの通信の影響があることを警告しています。問題なければ“yes”と入力してください。

■ スイッチ番号を変更する設定

```
C9200#switch 2 renumber 3  
WARNING: Changing the switch number may result in a configuration change for that switch. The interface  
configuration associated with the old switch number will remain as a provisioned configuration. New Switch  
Number will be effective after next reboot. Do you want to continue?[y/n]? [yes]: yes  
C9200#
```

スイッチ 2 の番号を 3 に変更します。

スタック構成が変更されるため、通信の影響があることを警告しています。問題なければ“yes”と入力してください。

<注意>

再起動後に有効になります。

3.1 Stack

StackWise

■ StackWise 構成の確認

```
C9200#show switch
Switch/Stack Mac Address : 70b3.17e3.f600 - Local Mac Address
Mac persistency wait time: Indefinite
                          H/W  Current
```

```
Switch#  Role  Mac Address  Priority Version  State
```

```
-----
--
*1  Active  70b3.17e3.f600  10  V01  Ready
 2  Standby 70b3.17e9.cf00   1  V01  Ready
```

```
C9200#
```

■ StackWise 接続構成の確認

```
C9200#show switch stack-port summary
Sw#/Port#  Port Status  Neighbor  Cable Length  Link OK  Link Active  Sync OK  #Changes to
LinkOK  In Loopback
```

```
-----
1/1  OK      2      50cm      Yes  Yes  Yes  3  No
1/2  OK      2      50cm      Yes  Yes  Yes  4  No
2/1  OK      1      50cm      Yes  Yes  Yes  1  No
2/2  OK      1      50cm      Yes  Yes  Yes  1  No
```

```
C9200#
```

<注意>

StackWise 構成になると、両機器とも同じコンソール表示になります。実機器の確認には Blue Beacon が便利です。

MAC アドレス : 70b3.17e3.f600 側がアクティブであることを確認。

スタック ポートの状態、接続ケーブル長などが表示されます。

3.1 Stack

StackWise

■ 特定の機器を再起動する場合

```
C9200#reload slot 2
Proceed with reload?[confirm]
```

```
reboot: Restarting system
Initializing Hardware...
```

スイッチ 2 をリブートします。

再起動の確認を求められます。

```
C9200#reload slot 1
System configuration has been modified. Save? [yes/no]: yes
Building configuration...
[OK]
Proceed with reload?[confirm]
```

```
reboot: Restarting system
Initializing Hardware...
```

スイッチ 1 をリブートします。

設定が保存されていない場合は設定を保存するかどうかの確認を求められます。”yes“か“no”をタイプしてください。

再起動の確認を求められます。

■ スタック機器全体を再起動する場合

```
C9200#reload
Proceed with reload? [confirm]
```

```
reboot: Restarting system
Initializing Hardware...
```

スタック構成全体を再起動します。

再起動の確認を求められます。

```
C9200#reload
System configuration has been modified. Save? [yes/no]: yes
Building configuration...
[OK]Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm]
```

```
reboot: Restarting system
Initializing Hardware...
```

スタック構成全体を再起動します。

設定が保存されていない場合は設定を保存するかどうかの確認を求められます。”yes“か“no”をタイプしてください。

再起動の確認を求められます。

3.1 Stack

StackWise

■ 機器の設定リフレッシュについて

スタック構成から外したスイッチを単体で設定する場合、設定を削除および、スイッチのスタック番号も変更する必要があります。

```
C9200#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
C9200#
C9200#reload
System configuration has been modified. Save? [yes/no]: no
Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm]
~再起動後~
Switch#show running-config
:
interface GigabitEthernet3/0/1
:
Switch#switch 3 renumber 1
WARNING: Changing the switch number may result in a configuration change for that switch. The
interface configuration associated with the old switch number will remain as a provisioned
configuration. New Switch Number will be effective after next reboot. Do you want to continue?[y/n]?
[yes]: yes
Switch#
Switch#reload
System configuration has been modified. Save? [yes/no]: no
Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm]
~再起動後~
Switch#show running-config
:
interface GigabitEthernet3/0/1
```

<注意>

スイッチのスタック番号の変更後、再起動が必要になります。

設定の削除を行います。

機器の再起動をおこないます。

設定の保存は行わないため“no”を入力してください。

再起動の確認を求められます。

設定を削除してもスタック構成時の設定が残っています。
Interface が “3” から始まっている。

スタック構成時の初期値の“1”に変更する。

スタック構成が変更されるため、通信の影響があることを警告
しています。問題なければ“yes”と入力してください。

再起動を行い、設定を確定させます。

設定の保存を確認されます。設定が無い場合は“no”を選択し
てください。

←再起動の確認を求められます。

スタック構成時の設定が初期値になっていることを確認します。

3.1 Stack

StackPower

StackPower 機能では、スイッチ機器の電源供給を異なるスイッチ機器にも供給し動作することができ、拡張性や耐障害性に対応します。

■ 特徴

スイッチの電源供給を他のスイッチ間と共有することが可能となり、スイッチに電源を1台追加して、StackPower メンバー間の電源の冗長を可能にします。

本機能は Cisco Catalyst 9300 シリーズのみサポートしています。

■ 既存機器との比較

Cisco Catalyst 3850 と StackPower の動作に関しては同じになりますが、show コマンドに関しては表示が異なります。

■ 注意

StackPower 機能の構成は最大 4 台までになります。

■ 参考

StackPower 内のスイッチ機器間で「StackWiseを組む」/「StackWise を組まずに独立して動作させる」のいずれも可能です。ただし、StackPower 内で StackWise を組む場合には全てのスイッチ機器を同一の StackWise グループにする必要があります。また、StackWise は最大 8 台で構成できますが、StackPower 内で構成する場合には最大 4 台までとなります。



<StackPowerケーブルの種類>

CAB-SPWR-30CM : 30cmのStackPowerケーブル

CAB-SPWR-150CM : 150cmのStackPowerケーブル

StackPower

StackPower を構成するには機器に対応した StackPower ケーブルが別途必要となります。

■ StackPower ケーブルの取り付け

StackPower コネクタ部に StackPower ケーブルを差し込み 1 本のネジを時計回りに締めます。

※必要以上に取り付け取り外しを行わないでください。

■ StackPower ケーブルの取り外し

StackPower ケーブルのネジ(1 本)を半時計回りに緩めます。

StackPower ケーブルを引き抜いてください。

■ 注意

StackPower ケーブルは、標準構成で1機器につき 1 本の Stack Power ケーブル(30cm 長)が付属されています。

30cm 長以外の StackPower ケーブルはイコール型番にて追加発注する必要があります。

ケーブルの両端に緑色と黄色の印がありますが、スイッチ間接続の場合に方向の制限はありません。

(電源供給専用の機器 XPS と接続する場合に必要となります。)

■ 推奨

電源分散させた 2 系統以上の電源入力を推奨します。



StackPower ケーブルを 1 本取り付けした状態

3.1 Stack

StackPower

StackPower テクノロジーでは最大 4 台の機器を構成に組み込むことができます。

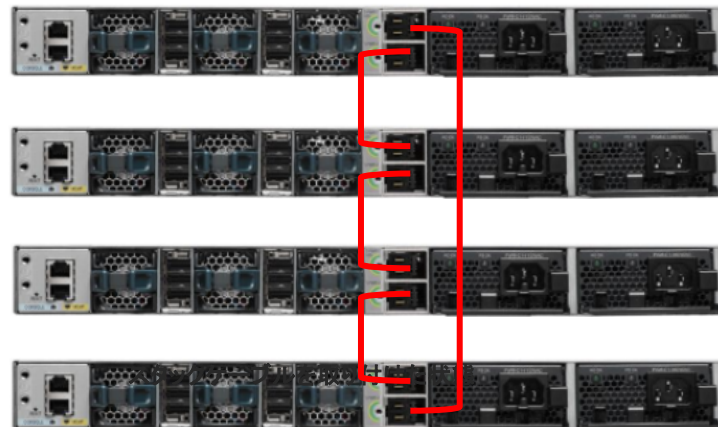


StackPower 動作時の LED 表示

<StackPower 2 台の接続構成イメージ>



<StackPower 4 台の接続構成イメージ>



— StackPower ケーブル

3.1 Stack

StackPower

■ StackPower の状態確認コマンド

```
C9300#show stack-power budgeting
```

Power Stack Name	Stack Mode	Stack Topolgy	Total Pwr(W)	Rsvd Pwr(W)	Alloc Pwr(W)	Sw_Avail Pwr(W)	Num SW	Num PS
------------------	------------	---------------	--------------	-------------	--------------	-----------------	--------	--------

Powerstack-1	SP-PS	Ring	1100	0	575	0	1	1
--------------	-------	------	------	---	-----	---	---	---

Power Stack SW Name	PS-A (W)	PS-B (W)	Power Budgt(W)	Alloc Power(W)	Poe_Avail Pwr(W)	Consumd Pwr Sys/PoE(W)
---------------------	----------	----------	----------------	----------------	------------------	------------------------

1 Powerstack-1	1100	0	1145	575	570	182 /0
----------------	------	---	------	-----	-----	--------

Totals:			575	570	182 /0	
---------	--	--	-----	-----	--------	--

```
C9300#
```

Stack Mode :電源供給のモード
Stack Topolgy :StackPowerの構成
Standaln(単体)|Ring(StackPower構成)
Total Pwr(W) :電源モジュールの合計電源量
Alloc Pwr(W) :他スイッチへの電源供給可能量

Poe Avail Pwr(W) :PoWの電源供給可能量
Consumd Pwr Sys/PoE(W):実電源消費量

■ StackPower の接続状態確認コマンド

```
C9300#show stack-power neighbors
```

Power Stack Name	Stack Mode	Stack Topolgy	Total Pwr(W)	Rsvd Pwr(W)	Alloc Pwr(W)	Sw_Avail Pwr(W)	Num SW	Num PS
------------------	------------	---------------	--------------	-------------	--------------	-----------------	--------	--------

Powerstack-1	SP-PS	Ring	1100	0	575	0	1	1
--------------	-------	------	------	---	-----	---	---	---

Power Stack SW Name	Port 1 Status	Port 1 Neighbor SW:MAC	Port 2 Status	Port 2 Neighbor SW:MAC
---------------------	---------------	------------------------	---------------	------------------------

1 Powerstack-1	Conn	-:501c.b079.eb80	Conn	-:700b.4ff4.fd80
----------------	------	------------------	------	------------------

```
C9300#
```

Port 1 Status :StackPowerコネクタ1の接続有 (Conn|NoConn)
Port 1 Neighbor SW:MAC :StackPowerコネクタ1の接続先機器のMAC アドレス
Port 2 Status :StackPowerコネクタ2の接続有無
Port 2 Neighbor SW:MAC :StackPowerコネクタ2の接続先機器のMAC アドレス

3.1 Stack

StackPower

■ 電源を落とした際のログ

```
C9300#  
*Apr 1 12:12:17.939: %PLATFORM_FEP-1-FRU_PS_SIGNAL_FAULTY: Switch 1: signal on power supply A is faulty  
C9300#
```

電源供給の停止により電源モジュール A が止まってしまったログ

■ 電源を落としている状態での StackPower の状態確認コマンド

```
C9300#show stack-power budgeting  
Power Stack      Stack Stack  Total  Rsvd  Alloc  Sw_Avail  Num Num  
Name            Mode  Topolgy Pwr(W) Pwr(W) Pwr(W)  Pwr(W)  SW  PS  
-----  
Powerstack-1    SP-PS Ring    0     0    575     0    1  0  
  
Power Stack      PS-A PS-B Power  Alloc  Poe_Avail  Consumd Pwr  
SW Name          (W)  (W)  Budget(W) Power(W)  Pwr(W)  Sys/PoE(W)  
-----  
1 Powerstack-1    0    0    785    575    210    183 /0  
-----  
Totals:          575    210    183 /0  
  
C9300#
```

Total Pwr(W)が 0 になりスイッチ内で電源供給が 0 である表示

PS-A(W)、PS-B(W)の表示も同様

3.1 Stack

StackPower

StackPower の設定では、デフォルトで有効になっています。必要に応じて無効にすることも可能です。

■ StackPower の無効化

```
C9300#
C9300#conf t
C9300(config)#stack-power switch 1
C9300(config-switch-stackpower)#
C9300(config-switch-stackpower)#standalone
*Apr 1 12:29:44.438: %PLATFORM_STACKPOWER-6-CABLE_EVENT: Switch 1 stack power cable 2 removed
C9300(config-switch-stackpower)#end
C9300#
```

StackWise 時の Switch 番号を入力。単体の場合は 1

無効化の設定。元に戻す場合は、“no standalone” を入力

■ StackPower 無効化の確認

```
C9300#show stack-power
Power Stack      Stack Stack Total Rsvd Alloc Sw_Avail Num Num
Name            Mode Topolgy Pwr(W) Pwr(W) Pwr(W) Pwr(W) SW PS
-----
Powerstack-11   SP-PS Stndaln 1100  0   575  525   1  1
C9300#
```

Stack のステータスが Stndaln(standalone) であることを確認

StackPower

StackPower では、2 種類のモードで実行するよう、StackPower を設定できます。

■ 電源共有モード (power-shared) :

すべての入力電力を電源負荷に使用できます。電源スタックのすべてのスイッチ(最大 4 台)の総使用可能電力が、単一の大きな電源モジュールとして扱われ、電力は、すべてのスイッチおよび PoE ポートに接続されているすべての受電デバイスで使用できます。(デフォルトのモードであり、Cisco Catalyst 9300 シリーズでは電力共有モードを推奨しています。)

■ 冗長モード(redundant) :

システムで最大の電源モジュールが電源バジェットから減算され、総使用可能電力が減りますが、これによって、電源モジュールに障害が発生した場合のバックアップ電源を提供します。スイッチおよび受電デバイスのプールで使用できる電力は減りますが、電源障害または極端な電力負荷が発生した場合でも、スイッチまたは受電デバイスのシャットダウンが必要になる可能性が減ります。

また、上記の 2 つのモードとは別に、電力障害発生時の電力供給量を厳密に管理するか、少しの電源余力がある場合そのまま動作させるかのモードがあります。どちらのモードにおいても、電力供給の使用可能な電力がなくなると、電源供給が拒否されます。

■ 厳密モード(strict) :

電源モジュールに障害が発生し、使用可能電力が電源供給の電力よりも下がった場合、実際に消費される電力が使用可能電力よりも低くても、システムは受電デバイスの負荷制限によって電源供給を分散させます。

■ 非厳密モード(no strict) :

実際の電力が使用可能電力を超えない限り、電源スタックが割り当て超過状態で稼働でき、安定した状態のままです。このモードでは、受電デバイスが通常の電力を超えて電力を引き出すと、電源スタックが負荷制限を開始することがあります。デバイスは最大電力では稼働せず、スタックの複数の受電デバイスが同時に最大電力を必要とすることはほぼないため、通常は問題になりません。(デフォルトのモードになります。)

3.1 Stack

StackPower

■ power-shared & strict の設定の場合

```
C9300#conf t
C9300(config)#stack-power stack Powerstack-1
C9300(config-stackpower)#mode power-shared strict
C9300(config-stackpower)#end
C9300#
```

■ power-shared & no strict の設定の場合: (デフォルト値)

```
C9300#conf t
C9300(config)#stack-power stack Powerstack-1
C9300(config-stackpower)#mode power-shared
C9300(config-stackpower)#end
C9300#
```

■ redundant & strict の設定の場合

```
C9300#conf t
C9300(config)#stack-power stack Powerstack-1
C9300(config-stackpower)#mode redundant strict
C9300(config-stackpower)#end
C9300#
```

■ redundant & no strict の設定の場合

```
C9300#conf t
C9300(config)#stack-power stack Powerstack-1
C9300(config-stackpower)#mode redundant
C9300(config-stackpower)#end
C9300#
```

<参考>

設定を変更する場合は、
C9300(config-stackpower)#no mode
を入力してから設定してください。

<注意>

StackPower メンバ機器は全て同じモード設定に
してください。

StackPower

電源供給の優先順位について、StackPower の電源供給を行うにあたり電源が失われ、負荷制限が必要になった場合に、スイッチとポートがシャットダウンされる順序を設定することができます。

■ Low port priority 値:

低優先順位ポートとして設定されたスイッチの PoE ポートの電源プライオリティを設定します。

範囲は 1 ~ 27 となり、1 が優先度が高くなります。High port priority 値 に設定する値、および Switch priority 値 に設定する値よりも大きな数字にする必要があります。(デフォルト値は22)

■ High port priority 値:

高優先順位ポートとして設定されたスイッチの PoE ポートの電源プライオリティを設定します。

値は 1 ~ 27 となり、1 が優先度が高くなります。High port priority 値 は、Low port priority 値 に設定する値よりも小さく、Switch priority 値 に設定する値よりも大きな数字にする必要があります。(デフォルト値は 13)

■ Switch priority 値:

スイッチの電源プライオリティを設定します。

範囲は 1 ~ 27 となり、1 が優先度が高くなります。この値は、Low port priority 値 および High port priority 値 に設定する値よりも小さな数字にする必要があります。(デフォルト値は 4)

<参考>

CLI による設定がされていない機器では、MAC アドレスの大小に従い Priority が付与されます。StackPower を 4 台で構成している場合は、MAC アドレスが一番小さい機器が最大 -3 された値となり、一番大きな機器がデフォルト値になります。(StackPower を 2 台で構成している場合は、MAC アドレスの小さい機器が -1 された値になります。)

3.1 Stack

StackPower

電源供給の優先順位を明示的に設定する場合は、以下のコマンドにより設定を行います。

■ Low port priority 値の設定例

```
C9300#conf t
C9300(config)#stack-power stack Powerstack-1
C9300(config-stackpower)#power-priority low 24
C9300(config-stackpower)#end
C9300#
```

■ High port priority 値の設定例

```
C9300#conf t
C9300(config)#stack-power stack Powerstack-1
C9300(config-stackpower)# power-priority high 14
C9300(config-stackpower)#end
C9300#
```

■ Switch priority 値の設定例

```
C9300#conf t
C9300(config)#stack-power stack Powerstack-1
C9300(config-stackpower)# power-priority switch 5
C9300(config-stackpower)#end
C9300#
```

<注意>

StackPower メンバ内では必ず全て異なる数値にしてください。

3.1 Stack

StackPower

■ 電源供給の優先順位設定の確認

```
C9300# Switch#show stack-power detail
```

Power Stack Name	Stack Mode	Stack Topology	Total Pwr(W)	Rsvd Pwr(W)	Alloc Pwr(W)	Sw_Avail Pwr(W)	Num SW	Num PS
Powerstack-1	SP-PS	Ring	1100	0	575	0	1	1

```
Power stack name: Powerstack-1
```

```
Stack mode: Power sharing
```

```
Stack topology: Ring
```

```
Switch 1:
```

```
Power budget: 1145
```

```
Power allocated: 575
```

```
Low port priority value: 22
```

```
High port priority value: 13
```

```
Switch priority value: 4
```

```
Port 1 status: Connected
```

```
Port 2 status: Connected
```

```
Neighbor on port 1: 501c.b079.eb80
```

```
Neighbor on port 2: 700b.4ff4.fd80
```

```
Switch#
```

現在の優先順位設定の確認

StackPower

■ StackPower 5 台構成をした場合

```
C9300#  
*Apr 1 08:33:43.307: %PLATFORM_STACKPOWER-3-INVALID_TOPOLOGY: Invalid  
power stack topology observed by switch 1. More than four switches are connected in  
ring topology
```

```
*Apr 1 08:36:47.593: %PLATFORM_STACKPOWER-4-PRIO_CONFLICT: Switch 1's  
power stack has conflicting power priorities  
C9300#
```

StackPower 構成が 4 台を超える構成となっており警告のメッセージを表示

3.2 IOS Management

Upgrade

ISSU

GOLD

PoE

WireShark

Energywise

Blue Beacon

TDR

Upgrade

機能説明

Upgrade の機能では、本機器のソフトウェアのバージョン アップ、またはバージョン ダウンを実施します。

■ 手順

- ① install remove inactive
- ② copy usbflash0:*.bin flash:
- ③ boot system flash:*.conf
- ④ install add file *.bin activate commit

■ 注意事項

- WebUI 上での実施はできません。
- “request platform software” コマンドは、IOS XE Gibraltar 16.10.1 以降では非推奨となっています。
代わりに “install” コマンドをご使用ください。

3.2 IOS Management

Upgrade

Upgrade 設定①

■ フラッシュの中の古いファイルを整理する設定

```
Switch#install remove inactive
install_remove: START Wed Mar 6 07:16:24 UTC 2019
Cleaning up unnecessary package files
No path specified, will use booted path flash:packages.conf
Cleaning flash:
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
cat9k-cc_srdriver.16.09.01.SPA.pkg
File is in use, will not delete.
cat9k-espbase.16.09.01.SPA.pkg
File is in use, will not delete.
cat9k-guestshell.16.09.01.SPA.pkg
File is in use, will not delete.
cat9k-rpbase.16.09.01.SPA.pkg
File is in use, will not delete.
cat9k-rpboot.16.09.01.SPA.pkg
File is in use, will not delete.
cat9k-sipbase.16.09.01.SPA.pkg
File is in use, will not delete.
cat9k-sipspace.16.09.01.SPA.pkg
File is in use, will not delete.
cat9k-srdriver.16.09.01.SPA.pkg
File is in use, will not delete.
cat9k-webui.16.09.01.SPA.pkg
File is in use, will not delete.
cat9k-wlc.16.09.01.SPA.pkg
File is in use, will not delete.
```

```
packages.conf
File is in use, will not delete.
done.
```

The following files will be deleted:

```
[switch 1]:
/flash/cat9k-cc_srdriver.16.09.02.SPA.pkg
/flash/cat9k-espbase.16.09.02.SPA.pkg
/flash/cat9k-guestshell.16.09.02.SPA.pkg
/flash/cat9k-rpbase.16.09.02.SPA.pkg
/flash/cat9k-rpboot.16.09.02.SPA.pkg
/flash/cat9k-sipbase.16.09.02.SPA.pkg
/flash/cat9k-sipspace.16.09.02.SPA.pkg
/flash/cat9k-srdriver.16.09.02.SPA.pkg
/flash/cat9k-webui.16.09.02.SPA.pkg
/flash/cat9k-wlc.16.09.02.SPA.pkg
/flash/cat9k_iosxe.16.09.01.SPA.bin
/flash/cat9k_iosxe.16.09.01.SPA.conf
```

Do you want to remove the above files? [y/n]

```
[switch 1]:
Deleting file flash:cat9k-cc_srdriver.16.09.02.SPA.pkg ...
done.
Deleting file flash:cat9k-espbase.16.09.02.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.09.02.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.09.02.SPA.pkg ... done.
```

```
Deleting file flash:cat9k-rpboot.16.09.02.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.09.02.SPA.pkg ... done.
Deleting file flash:cat9k-sipspace.16.09.02.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.09.02.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.09.02.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.16.09.02.SPA.pkg ... done.
Deleting file flash:cat9k_iosxe.16.09.01.SPA.bin ... done.
Deleting file flash:cat9k_iosxe.16.09.01.SPA.conf ... done.
SUCCESS: Files deleted.
--- Starting Post_Remove_Cleanup ---
Performing Post_Remove_Cleanup on all members
[1] Post_Remove_Cleanup package(s) on switch 1
[1] Finished Post_Remove_Cleanup on switch 1
Checking status of Post_Remove_Cleanup on [1]
Post_Remove_Cleanup: Passed on [1]
Finished Post_Remove_Cleanup
```

SUCCESS: install_remove Wed Mar 6 07:18:59 UTC 2019
Switch#

Upgrade

Upgrade 設定②

■ フラッシュに新しいイメージファイルをコピーする設定

```
Switch#copy usbflash0:cat9k_iosxe.16.09.02.SPA.bin flash:
Destination filename [cat9k_iosxe.16.09.02.SPA.bin]? cat9k_iosxe.16.09.02.SPA.bin
Copy in
progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCC...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
```

700524979 bytes copied in 131.313 secs (5334772 bytes/sec)

Switch#

ここでは USB からコピーしているが TFTP サーバからコピーすることも可能 (tftp:)

■ コピー後のファイルを確認

```
Switch#dir flash:*.bin
Directory of flash:/*.bin

Directory of flash:/

647178 -rw- 700524979 Mar 6 2019 07:22:13 +00:00
cat9k_iosxe.16.09.02.SPA.bin
11353194496 bytes total (7475007488 bytes free)
Switch#
```

ファイル名を確認

Upgrade

Upgrade 設定③

■ ブート変数を設定

```
Switch(config)#boot system flash:packages.conf
Switch(config)#
Switch(config)#exit
Switch#write
Switch#write
*Mar  6 07:23:17.316: %SYS-5-CONFIG_I: Configured from console by consolememo
Switch#write memory
Building configuration...
[OK]
```

グローバル コンフィギュレーション モードで実施

設定の保存

■ 次回起動時に変更が反映されているか確認

```
Switch#show boot system
-----
Switch 1
-----
Current Boot Variables:
BOOT variable = flash:packages.conf;

Boot Variables on next reload:
BOOT variable = flash:packages.conf;
Manual Boot = no
Enable Break = no
Boot Mode = DEVICE
iPXE Timeout = 0
Switch#
```

ファイル名を確認

3.2 IOS Management

Upgrade

Upgrade 設定④

■ ソフトウェアのインストール

```
Switch#install add file flash:cat9k_iosxe.16.09.02.SPA.bin activate /flash/cat9k-cc_srdriver.16.09.02.SPA.pkg
commit
install_add_activate_commit: START Wed Mar 6 07:25:05 UTC 2019 This operation requires a reload of the system. Do you want to
*Mar 6 07:25:06.621: %INSTALL-5-INSTALL_START_INFO: Switch proceed? [y/n]
1 R0/0: install_engine: Started install one-shot --- Starting Activate ---
flash:cat9k_iosxe.16.09.02.SPA.bininstall_add_activate_commit: Performing Activate on all members
Adding PACKAGE [1] Activate package(s) on switch 1
--- Starting initial file syncing --- --- Starting list of software package changes ---
Info: Finished copying flash:cat9k_iosxe.16.09.02.SPA.bin to the Old files list:
Selected switch(es) Removed cat9k-cc_srdriver.16.09.01.SPA.pkg
Finished initial file syncing Removed cat9k-espbase.16.09.01.SPA.pkg
Removed cat9k-guestshell.16.09.01.SPA.pkg
Removed cat9k-rpbase.16.09.01.SPA.pkg
Removed cat9k-rpboot.16.09.01.SPA.pkg
Removed cat9k-sipbase.16.09.01.SPA.pkg
Removed cat9k-sipspa.16.09.01.SPA.pkg
Removed cat9k-srdriver.16.09.01.SPA.pkg
Removed cat9k-webui.16.09.01.SPA.pkg
Removed cat9k-wlc.16.09.01.SPA.pkg
--- Starting Add --- New files list:
Performing Add on all members Added cat9k-cc_srdriver.16.09.02.SPA.pkg
[1] Add package(s) on switch 1 Added cat9k-espbase.16.09.02.SPA.pkg
[1] Finished Add on switch 1 Added cat9k-guestshell.16.09.02.SPA.pkg
Checking status of Add on [1] Added cat9k-rpbase.16.09.02.SPA.pkg
Add: Passed on [1] Added cat9k-rpboot.16.09.02.SPA.pkg
Finished Add Added cat9k-sipbase.16.09.02.SPA.pkg
Added cat9k-sipspa.16.09.02.SPA.pkg
Added cat9k-srdriver.16.09.02.SPA.pkg
Added cat9k-webui.16.09.02.SPA.pkg
Added cat9k-wlc.16.09.02.SPA.pkg
install_add_activate_commit: Activating PACKAGE Finished list of software package changes
Following packages shall be activated: [1] Finished Activate on switch 1
/flash/cat9k-wlc.16.09.02.SPA.pkg
/flash/cat9k-webui.16.09.02.SPA.pkg
/flash/cat9k-srdriver.16.09.02.SPA.pkg
/flash/cat9k-sipspa.16.09.02.SPA.pkg
/flash/cat9k-sipbase.16.09.02.SPA.pkg
/flash/cat9k-rpboot.16.09.02.SPA.pkg
/flash/cat9k-rpbase.16.09.02.SPA.pkg
/flash/cat9k-guestshell.16.09.02.SPA.pkg
/flash/cat9k-espbase.16.09.02.SPA.pkg
Checking status of Activate on [1]
Activate: Passed on [1]
Finished Activate
--- Starting Commit ---
Performing Commit on all members
*Mar 6 07:41:20.525: %INSTALL-5-
INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 1 R0/0:
rollback_timer: Install auto abort timer will expire in 7200 seconds [1]
Commit package(s) on switch 1
[1] Finished Commit on switch 1
Checking status of Commit on [1]
Commit: Passed on [1]
Finished Commit
[1]: Performing Upgrade_Service
%IOSXEBOOT-4-BOOTLOADER_UPGRADE: (local/local): Starting
boot preupgrade300+0 records in
300+0 records out
307200 bytes (307 kB, 300 KiB) copied, 0.309814 s, 992 kB/s
SUCCESS: Upgrade_Service finished
Install will reload the system now!
SUCCESS: install_add_activate_commit Wed Mar 6 07:41:33 UTC
2019
Switch#
Chassis 1 reloading, reason - Reload command
```

“y” を選択

Upgrade

Upgrade 設定⑤

スイッチのバージョンの確認

■バージョンアップ前

```
Switch#show ver
Cisco IOS XE Software, Version 16.09.01
Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.9.1,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Tue 17-Jul-18 17:00 by mcpre
...
```

■バージョンアップ後

```
Switch#show ver
Cisco IOS XE Software, Version 16.09.02
Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.9.2,
RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Mon 05-Nov-18 19:32 by mcpre
...
```

ISSU

機能説明

ISSU(In-Service Software Upgrade) 機能では、サービスを停止させることなく本機器のソフトウェアのバージョンアップを実施します。冗長構成を組まれた機器を 1 台ずつバージョン アップすることで、バージョン アップ中においても通信を継続させます。

■ 手順

- ① `show ver | in INSTALL` **ブートモードがInstallになっているかを確認**
- ② `show boot system` **自動ブートになっているかを確認**
- ③ `install add file flash:cat9k_iosxe.XX.XX.XX.SPA.bin activate issu commit` **アップグレードを実施(ロールバック不可)**

	9400	9500	9600
ISSU	16.9.1以降	16.9.2以降	16.11.1以降
ISSU on StackWise Virtual	16.9.2以降*	16.12.1以降 (9500-Hのみ)	未対応

■ 注意事項

- 異なるトレイン間での ISSU は非対応。
- *StackWise Virtualモード時、同一筐体内のスーパーバイザーの冗長化は未対応。

ISSU

機能説明

ISSU(In-Service Software Upgrade) 機能では、サービスを停止させることなく本機器のソフトウェアのバージョンアップを実施します。冗長構成を組まれた機器を 1 台ずつバージョン アップすることで、バージョン アップ中においても通信を継続させます。

- 手順
 - ① `show ver | in INSTALL` ブートモードがInstallになっているかを確認
 - ② `show boot system` 自動ブートになっているかを確認
 - ③ `install add file flash:cat9k_iosxe.XX.XX.XX.SPA.bin activate issu commit` アップグレードを実施(ロールバック不可)

■ 注意事項

- ISSUを実行するには、バージョンサポートバージョン差異あり(後述p.X「ISSU バージョン互換性」)
- 両機器でブート モードがインストール モードである必要があります。(インストール モードは xxx.pkg で、バンドルモードは xxx.bin でブートを行う)
- Manual-boot が無効である必要があります。
- StackWise VirtualによるISSU、Dual SupervisorによるISSUがあります。(対応機種後述p.X「Cisco Catalyst 9000 シリーズの ISSU」)

3.2 IOS Management

ISSU

ISSU の設定①

■ ブート モードの確認

```
C9500#show ver | in INSTALL
  1 50 C9500-40X 16.9.3 CAT9K_IOSXE INSTALL
*  2 50 C9500-40X 16.9.3 CAT9K_IOSXE INSTALL
C9500#
```

BUNDLE であった場合は INSTALL へ変更すること

■ ブート設定の確認

```
C9500#show boot system
-----
Switch 1
-----
Current Boot Variables:
BOOT variable = flash:packages.conf;

Boot Variables on next reload:
BOOT variable = flash:packages.conf;
Manual Boot = no
Enable Break = no
Boot Mode = DEVICE
iPXE Timeout = 0
-----

Switch 2
-----
Current Boot Variables:
BOOT variable = flash:packages.conf;

Boot Variables on next reload:
BOOT variable = flash:packages.conf;
Manual Boot = no
Enable Break = no
Boot Mode = DEVICE
iPXE Timeout = 0
```

手動ブートになっていないことを確認

3.2 IOS Management

ISSU

ISSU の設定②

■ ISSU の実施

```
C9500#add file flash:cat9k_iosxe.16.09.03.SPA.bin activate issu commit
install_add_activate_commit: START Tue Mar 26 15:20:03 JST 2019
*Mar 26 06:20:04.536: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine: Started
install one-shot ISSU flash:cat9k_iosxe.16.09.03.SPA.bininstall_add_activate_commit: Adding ISSU
```

```
--- Starting initial file syncing ---
[1]: Copying flash:cat9k_iosxe.16.09.03.SPA.bin from switch 1 to switch 2
[2]: Finished copying to switch 2
Info: Finished copying flash:cat9k_iosxe.16.09.03.SPA.bin to the selected switch(es)
Finished initial file syncing
```

```
--- Starting Add ---
Performing Add on all members
[1] Add package(s) on switch 1
[1] Finished Add on switch 1
[2] Add package(s) on switch 2
[2] Finished Add on switch 2
Checking status of Add on [1 2]
Add: Passed on [1 2]
Finished Add
```

```
install_add_activate_commit: Activating ISSU
```

```
NOTE: Going to start Oneshot ISSU install process
```

```
STAGE 0: Initial System Level Sanity Check before starting ISSU
```

```
-----
--- Verifying install_issu supported ---
--- Verifying standby is in Standby Hot state ---
--- Verifying booted from the valid media ---
--- Verifying AutoBoot mode is enabled ---
Finished Initial System Level Sanity Check
```

Image ファイルは装置間でコピーされる

最初にスタンバイからインストールが開始

```
STAGE 1: Installing software on Standby
```

```
-----
--- Starting install_remote ---
Performing install_remote on Chassis remote
[2] install_remote package(s) on switch 2
[2] Finished install_remote on switch 2
install_remote: Passed on [2]
Finished install_remote
```

ISSU 開始前の事前確認

3.2 IOS Management

ISSU

ISSU の設定③

■ ISSU の実施

STAGE 2: Restarting Standby

```
-----  
--- Starting standby reload ---  
Finished standby reload
```

```
--- Starting wait for Standby to reach terminal redundancy state ---
```

```
*Mar 26 06:22:53.908: %SMART_LIC-5-EVAL_START: Entering evaluation period  
*Mar 26 06:22:53.909: %SMART_LIC-5-EVAL_START: Entering evaluation period  
*Mar 26 06:22:53.934: %HMANRP-5-CHASSIS_DOWN_EVENT: Chassis 2 gone DOWN!
```

```
...  
*Mar 26 06:22:55.912: %LINK-3-UPDOWN: Interface TenGigabitEthernet2/0/3, changed state to down  
*Mar 26 06:22:55.914: %LINK-3-UPDOWN: Interface TenGigabitEthernet2/0/4, changed state to down  
*Mar 26 06:22:55.914: %LINK-3-UPDOWN: Interface TenGigabitEthernet2/0/5, changed state to down  
*Mar 26 06:22:56.929: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet2/0/40,  
changed state to down  
*Mar 26 06:28:23.015: %STACKMGR-6-STANDBY_ELECTED: Switch 1 R0/0: stack_mgr: Switch 2 has  
been elected STANDBY.
```

```
*Mar 26 06:28:28.044: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion  
(raw-event=PEER_FOUND(4))
```

```
*Mar 26 06:28:28.044: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion  
(raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))
```

```
*Mar 26 06:28:28.861: %REDUNDANCY-3-IPC: IOS versions do not match.
```

```
*Mar 26 06:29:10.383: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEEDED: Bulk Sync succeeded  
*Mar 26 06:29:11.384: %RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)Finished wait for  
Standby to reach terminal redundancy state
```

スタンバイで再起動が開始

アクティブでインストールが開始

STAGE 3: Installing software on Active

```
-----  
--- Starting install_active ---  
Performing install_active on Chassis 1
```

```
*Mar 26 06:29:13.591: %LINK-3-UPDOWN: Interface TenGigabitEthernet2/0/3, changed state to up  
*Mar 26 06:29:13.595: %LINK-3-UPDOWN: Interface TenGigabitEthernet2/0/4, changed state to up  
*Mar 26 06:29:13.741: %LINK-3-UPDOWN: Interface TenGigabitEthernet2/0/10, changed state to up  
*Mar 26 06:29:14.591: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet2/0/3,  
changed state to up  
*Mar 26 06:29:14.595: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet2/0/4,  
changed state to up  
*Mar 26 06:29:16.208: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet2/0/10,  
changed state to up  
usr/binos/conf/pglobals-pd.sh: line 16:  
/tmp/chassis/local//chasfs/midplane/chassis_type: No such file or directory  
[1] install_active package(s) on switch 1  
[1] Finished install_active on switch 1  
install_active: Passed on [1]  
Finished install_active
```

3.2 IOS Management

ISSU

ISSU の設定④

■ ISSU の実施

アクティブで再起動が開始

STAGE 4: Restarting Active (switchover to standby)

--- Starting active reload ---

New software will load after reboot process is completed
SUCCESS: install_add_activate_commit Tue Mar 26 15:30:26 JST 2019
Chassis 1 reloading, reason - Non participant detected
C9500#Mar 26 15:30:28.577: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload fp
action requested
Mar 26 15:30:29.805: %PMAN

Initializing Hardware...

System Bootstrap, Version 16.9.1r [FC2], RELEASE SOFTWARE (P)
Compiled Tue 05/29/2018 14:59:59.99 by rel

Current ROMMON image : Primary
Last reset cause : PowerOn
C9500-40X platform with 16777216 Kbytes of main memory

boot: attempting to boot from [flash:packages.conf]

boot: reading file packages.conf

```
#  
#####  
#####  
#####  
#####  
#####  
#####
```

Mar 26 06:32:21.693: %PMAN-5-EXITACTION: C0/0: pvp: Process manager is exiting:

Waiting for 120 seconds for other switches to boot

#####

Switch number is 1

All switches in the stack have been discovered. Accelerating discovery

ISSU バージョン互換性

- ISSUはサポートバージョンが異なるため、リファレンス「Catalyst 3850、9400、および 9500 シリーズ スイッチのインサービス ソフトウェア アップグレード (ISSU)」を確認する必要があります。

https://www.cisco.com/c/ja_jp/support/docs/switches/catalyst-9500-series-switches/214406-in-service-software-upgrade-issu-on-ca.html



サポートされる アップグレード/ダウングレードパス

- 16.9.x <-> 16.9.x
(同一EMリリース間)
- 16.9.x <-> 16.12.x
(EMリリース間)

サポートされない アップグレード/ダウングレードパス

- 16.9.x <-> 16.10.x, 16.11.x
(SM-EMリリース間)
- 16.10.1 <-> 16.10.2
(同一SMリリース間)
- 16.x.x <-> 17.x.x
(メジャーリリース間)

- SM= 標準メンテナンスリリース
- EM= 拡張メンテナンスリリース

Cisco Catalyst 9000 シリーズの ISSU

	9200 9200L	9300 9300L	9400	9500	9500-H	9600
StackWise Virtual ISSU	—	—	16.9.2～※ ₁ Network Advantage	16.9.2～※ ₁ Network Advantage	16.12.1～ Network Advantage	16.12.1～ Network Advantage
筐体内冗 長 ISSU	—	—	16.9.1～※ _{1,2} Network Advantage	—	—	16.11.1～ Network Advantage

※1. 16.9.x -> 16.10.x/16.11.x のアップグレードパスはサポートされない

※2. 16.9.1 -> 16.9.2 のアップグレードパスはサポートされない

GOLD

機能説明①

GOLD(Generic Online Diagnostics)は、ハードウェア コンポーネントの健全性をチェックし、システムに潜在的な障害などがなく正常に動作していることを確認します。

■ 特徴

GOLD の実装では、ハードウェア コンポーネントの健全性をチェックし、システムに潜在的な障害などがなく正常に動作していることを確認します。

テストのなかには、システム起動時(ブートアップ診断)に実施されるものもあれば、システム稼働中(ランタイム診断)に実施されるものもあります。

■ 変更点

起動時の診断では、これまでの Cisco Catalyst 2000 シリーズなどでは起動時に POST のログ結果が表示されていましたが、本製品では正常起動時のログは表示されなくなりました。CLI により確認することは可能です。

■ 注意

Cisco Catalyst 9000 シリーズの機種によってテスト項目が異なります。

■ ブート アップ診断結果

```
C9200-01#show diagnostic post
Stored system POST messages:
```

```
Switch 1
-----
```

```
POST: CRYPTO Tests : Begin
POST: CRYPTO Tests : End, Status Passed
```

```
POST: PORT Loopback: loopback Test : Begin
POST: PORT Loopback: loopback Test : End, Status Passed
```

```
POST: SIF Tests : Begin
POST: SIF Tests : End, Status Passed
```

```
POST: Thermal, Temperature Tests : Begin
POST: Thermal, Temperature Tests End, Status Passed
```

```
C9200-01#
```

POST テスト時にエラーがある場合は、“Status Failed”と表示されます。

GOLD

機能説明②

■ ランタイム診断の種類

```

C9200-01#show diagnostic content switch 1
switch 1:
Diagnostics test suite attributes:
M/C/* - Minimal bootup level test / Complete bootup level test / NA
B/* - Basic ondemand test / NA
P/V/* - Per port test / Per device test / NA
D/N/* - Disruptive test / Non-disruptive test / NA
S/* - Only applicable to standby unit / NA
X/* - Not a health monitoring test / NA
F/* - Fixed monitoring interval test / NA
E/* - Always enabled monitoring test / NA
A/I - Monitoring is active / Monitoring is inactive
      Test Interval  Thre-
ID  Test Name          Attributes  day hh:mm:ss.ms shold
-----
1) DiagGoldPktTest -----> *BPN*X**I  not configured n/a
2) DiagThermalTest -----> *B*N****A  000 00:01:30.00 5
3) DiagPhyLoopbackTest -----> *BPD*X**I  not configured n/a
4) DiagScratchRegisterTest -----> *B*N****A  000 00:01:30.00 5
5) TestUnusedPortLoopback -----> *BPN****I  not configured n/a
6) DiagStackCableTest -----> ***D*X**I  not configured n/a
7) DiagMemoryTest -----> *B*D*X**I  not configured n/a

```

■ デフォルト値

ID 2) DiagThermalTest

ID 4) DiagScratchRegisterTest

あらかじめ決められたインターバルで自動的に実行されます他の項目に関してはマニュアル実行させるか、スケジュール実行させる必要があります。

■ 機種別診断対応表

	C9200	C9300	C9500
DiagGoldPktTest (MAC レベル)	○	○	○
DiagThermalTest (温度センサ)	○	○	○
DiagFanTest (ファン)	—	○	○
DiagPhyLoopbackTest (PHY チップ)	○	○	○
DiagScratchRegisterTest (ASIC チップ)	○	○	○
TestUnusedPortLoopback (ポートおよび ASIC のデータパス)	○	○	○
TestPortTxMonitoring (ポートの動作)	—	○	○
DiagStackCableTest (スタック ケーブル)	○	○	—
DiagMemoryTest (メモリ)	○	○	○



各項目の詳細に関しては次ページで説明しています。

GOLD

機能説明③

■ ランタイム診断の詳細説明

1) DiagGoldPktTest :

各ポートの MAC レベルでのループバック テストです。ASIC が発する GOLD パケットをループ バックさせ、返ってきたパケットを元のパケットと照合する検査を行います。このテストはスイッチの転送機能の中断を伴いません (Non-disruptive test)。ヘルス モニタリング テストとして実行できません。

2) DiagThermalTest :

システムの温度および温度センサーのテストです。センサーが読み取った温度が、警告レベルにあたる温度しきい値を下回っていることを確認します。このテストはスイッチの転送機能の中断を伴いません (Non-disruptive test)。ヘルス モニタリング テストとして実行できます。

3) DiagFanTest :

冷却ファン モジュールのテストです。すべての冷却ファン モジュールが挿入され、正しく動作していることを検証します。このテストはスイッチの転送機能の中断を伴いません (Non-disruptive test)。ヘルス モニタリング テストとして実行できます。

4) DiagPhyLoopbackTest :

各ポートの PHY レベルのループバック テストです。PHY レベルでパケットをループバックさせ、返ってきたパケットを元のパケットと照合する検査を行います。このテストの実行中はスイッチの転送機能の中断が発生します (Disruptive test)。ヘルスモニタリングテストとして実行できません。

5) DiagScratchRegisterTest :

ASIC の状態をテストします。ASIC 上のレジスタに値を書き込み、その値をあらためて読み取り正しくレジスタ値が保持されることを検査します。このテストはスイッチの転送機能の中断を伴いません (Non-disruptive test)。ヘルス モニタリング テストとして実行できます。

6) TestUnusedPortLoopback :

ポート、および ASIC へのデータバスのループバック テストをします。シャットダウンされている未使用ポートに対して VLAN 内フラッディングされるパケットを CPU から送信し、返ってきたパケットを元のパケットと照合する検査を行います。このテストはスイッチの転送機能の中断を伴いません (Non-disruptive test)。ヘルス モニタリング テストとして実行できます。

7) TestPortTxMonitoring :

各ポートが正しい動作状態にあることをテストします。定期的に各ポートの送信カウンタをポーリングし、正しく転送パケットが送信され、スタックが発生していないことを検査します。このテストはスイッチの転送機能の中断を伴いません (Non-disruptive test)。ヘルス モニタリング テストとして実行できます。

8) DiagStackCableTest :

StackWise のパスのループバック機能をテストします。このテストの実行中はスイッチの転送機能の中断が発生します (Disruptive test)。ヘルス モニタリング テストとして実行できません。

9) DiagMemoryTest :

ASIC 上のメモリのテストを行います。MBIST 標準に基づく網羅的テストパターンを利用してメモリを検査します。このテストの実行中はスイッチの転送機能の中断が発生します (Disruptive test)。ヘルス モニタリング テストとして実行できません。テスト完了後はスイッチの再起動が必要となります。

<補足>

ヘルス モニタリングとは、バックグラウンドでユーザが指定した間隔で実行されます。デフォルトでは、30 秒ごとにヘルス モニタリング テストが実行されます。

GOLD

ランタイム診断設定①

■ ランタイム診断のマニュアル実行

```
C9200-01#diagnostic start switch 1 test 1
C9200-01#
*Feb 20 02:59:02.020: %DIAG-6-TEST_RUNNING: switch 1: Running DiagGoldPktTest{ID=1} ...
*Feb 20 02:59:02.067: %DIAG-6-TEST_OK: switch 1: DiagGoldPktTest{ID=1} has completed
successfully
C9200-01#
```

■ ランタイム診断のスケジューリング実行

```
C9200-01#
C9200-01#configure terminal
C9200-01(config)# diagnostic schedule switch 1 test 1 daily 11:50
C9200-01(config)#
C9200-01(config)# diagnostic schedule switch 1 test 3 week sun 21:00
C9200-01(config)#
C9200-01(config)# diagnostic schedule switch 1 test 3 on February 20 2019 12:53
Diagnostic[switch 1]: Scheduling test(s) 3 may disrupt normal system operation and requires reload
C9200-01(config)#
```

1) DiagGoldPktTest のマニュアル実行例

<注意>

実行には<ランタイム診断の種類>に記載されている項目 (ID 1~7) を実行できますが、
ID 3) DiagPhyLoopbackTest
の実行には Interface が Down/Up します。
ID 6) DiagScratchRegisterTest
の実行にはパケット ロスが発生します。
ID 7) DiagMemoryTest
の実行には再起動が発生します。

毎日の時間を設定しての実行例

毎週の曜日と時間を設定しての実行例

一回限りの日時を設定しての実行例

<注意>

ID 3), 6), 7) に関しては、データ通信の影響の確認メッセージが表示されます。

GOLD

ランタイム診断設定②

■ ランタイム診断のログ メッセージ結果

```
C9200-01#  
*Feb 20 03:52:59.235: %DIAG-6-SCHED_RUNNING: switch 1: Performing Scheduled Online Diagnostic...  
*Feb 20 03:52:59.235: %DIAG-6-TEST_RUNNING: switch 1: Running DiagGoldPktTest{ID=1} ...  
*Feb 20 03:52:59.276: %DIAG-6-TEST_OK: switch 1: DiagGoldPktTest{ID=1} has completed successfully  
*Feb 20 03:52:59.276: %DIAG-6-SCHED_COMPLETE: switch 1: Scheduled Online Diagnostic is completed
```

■ ランタイム診断の結果

```
c9200-01#show diagnostic events  
Diagnostic events (storage for 500 events, 51 events recorded)  
Number of events matching above criteria = 51  
Event Type (ET): I - Info, W - Warning, E - Error
```

Time Stamp	ET [Card]	Event Message
02/19 21:39:46.745	E [TBD]	Message Out of Order
02/19 21:39:46.745	E [TBD]	Message Out of Order
02/19 21:39:46.745	E [TBD]	Message Out of Order
:		
:		
02/20 12:21:43.754	I [1]	DiagGoldPktTest Passed
02/20 12:21:50.232	I [1]	DiagPhyLoopbackTest Passed
02/20 12:21:50.232	I [1]	TestUnusedPortLoopback Passed

<注意>

再起動すると、イベント結果はクリアされます。

3.2 IOS Management

GOLD

ランタイム診断設定③

■ ランタイム診断のポートごとの診断結果

```
C9200-01#sh diagnostic switch 1
```

```
Current bootup diagnostic level: minimal
```

```
switch 1: SerialNo : JAE22490RSA
```

```
Overall Diagnostic Result for switch 1 : PASS
```

```
Diagnostic level at card bootup: minimal
```

```
Test results: (. = Pass, F = Fail, U = Untested)
```

```
1) DiagGoldPktTest:
```

```
Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
```

```
-----
```

```
. . . . .
```

```
Port 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
```

```
-----
```

```
. . . . .
```

```
Port 49 50 51 52
```

```
-----
```

```
. . . . .
```

PoE

機能説明

PoE (Power over Ethernet) 機能では、ツイスト ペア ケーブル (UTP/STP ケーブル) を利用して、PoE 対応機器 (無線 AP、IP-Phone など) に電力を供給できる機能です。PoE がサポートされた本製品では全ポート^{*1}を PoE+ (Power over Ethernet Plus) 性能でサポートします。

■ 特徴

従来機種の一部にあった「115 ~ 240V AC」の電圧の仕様はなく、すべての機種が「100 ~ 240 V AC」に対応しています。

また、機器のリブートにおいても PoE の電源供給は切れることなく供給が可能です。スイッチ再起動中の中断がないため、無線 LAN アクセスポイントなどの PoE 受電機器の再起動の発生を抑制し、さらに医療機器や照明などの IoT 機器といった稼働の中断が許されない機器への給電の用途にも対応可能となります。

■ 変更点

大きな変更点として、機器の電源が通電されると、オペレーティング システムが完全にロードされるのを待つことなく、PoE 電力供給を開始します。

クラス	最大供給量	ケーブル	規格	別名
3	15.4W	Cat5e	IEEE802.3af	PoE
4	30W	Cat5e	IEEE802.3at	PoE+
5, 6	60W	Cat5e	IEEE802.3bt type3	UPoE ^{*2}

^{*1}: アップリンクを省きます。

^{*2}: 2011年に独自規格として弊社からリリースされていたが、2018年9月にIEEE802.3btとして承認されました。また、IEEE802.3btにはtype3とtype4があり、それぞれの最大供給量は、type3は60W、type4は90Wとなっております。

PoE

Cisco Catalyst 9200 と Cisco Catalyst 9300 の違い

Cisco Catalyst 9200 L シリーズは、各 PID 専用の電源モジュールです。

- PoE 機能無し機器用(C9200-24T,-48T): [PWR-C5-125WAC](#)
- PoE 対応 24 ポート機器用(C9200-24P): [PWR-C5-600WAC](#)
- PoE 対応 48 ポート機器用(C9200-48P): [WR-C5-1KWAC](#)

Cisco Catalyst 9200 シリーズでは UPOE (Universal Power Over Ethernet、最大 60W) は未サポートになります。



Cisco Catalyst 9300 シリーズは、異なる電源モジュールを下記表の組み合わせで利用する事が可能です。

Cisco Catalyst 9300 シリーズでは UPoE (Universal Power Over Ethernet、最大60W)をサポートしております。

PoE のオプション	24 ポート スイッチ	48 ポート スイッチ
PoE (1 ポートあたり 最大 15.4 W)	(1) 715 W	次は電源の組み合わせです。 (1) 1100 W (1) 715 W + (1) 715 W
PoE+ (1 ポートあたり 最大 30 W)	次は電源の組み合わせです。 (1) 1100 W (1) 715 W + (1) 715 W	次は電源の組み合わせです。 (1) 1100 W + (1) 715 W (2) 1100 W
Cisco UPOE (1 ポートあたり 最大 60 W)	(2) 1100 W	次は電源の組み合わせです。 (1) 1100 W + (1) 715 W (2) 1100 W ※最大 30 個の PoE ポートがフル Cisco UPOE を受信できます。

3.2 IOS Management

PoE

Cisco Catalyst 9200/9200L シリーズでサポートされる電源モジュール、供給量、最大接続台数の目安

本体 PID	サポートされる電源モジュールと構成	最大 PoE 電源供給量	PoE 対応機器の接続台数の目安
C9200-24T, -48T C9200L-24T-4G/4X C9200L-48T-4G/4X	PWR-C5-125WAC* 1 台 (プライマリ電源のみ)	0 W	PoE 未対応
	PWR-C5-125WAC* 2 台 (セカンダリ電源追加)	0 W	PoE 未対応
C9200-24P C9200L-24P-4G/4X	PWR-C5-600WAC* 1 台 (プライマリ電源のみ)	370 W	IEEE802.3at (PoE+) 最大 30W なら*最大 12 ポート IEEE802.3af (PoE) 最大 15.4W なら*最大 24 ポート
	PWR-C5-600WAC* 2 台 (セカンダリ電源追加)	740 W	IEEE802.3at (PoE+) 最大 30W なら*最大 24 ポート IEEE802.3af (PoE) 最大 15.4W なら*最大 48 ポート
C9200-48P C9200L-48P-4G/4X	WR-C5-1KWAC* 1 台 (プライマリ電源のみ)	740 W	IEEE802.3at (PoE+) 最大 30W なら*最大 24 ポート IEEE802.3af (PoE) 最大 15.4W なら*最大 48 ポート
	WR-C5-1KWAC* 2 台 (セカンダリ電源追加)	1440W	IEEE802.3at (PoE+) 最大 30W なら*最大 48 ポート IEEE802.3af (PoE) 最大 15.4W なら*最大 48 ポート

PoE

Cisco Catalyst 9300 シリーズでサポートされる電源モジュールの組み合わせ、供給量

本体 PID	デフォルト電源モジュール	デフォルト最大 PoE 電源供給量	セカンダリ電源 350W	セカンダリ電源 715W	セカンダリ電源 1100W	セカンダリ電源 715W DC
C9300-24T, -48T	PWR-C1-350WAC*1 台 *2 台	0 W	0 W	0 W	0 W	0 W
C9300-24P	PWR-C1-715WAC	445 W	720 W*	720 W*	720 W*	720 W*
C9300-48P	PWR-C1-715WAC	437 W	787 W	1152 W	1440 W*	1152 W
C9300-24U	PWR-C1-1100WAC	830 W	1180 W	1440 W*	1440 W*	1440 W*
C9300-48U	PWR-C1-1100WAC	822 W	1172 W	1537 W	1800 W**	1537 W
C9300-24UX	PWR-C1-1100WAC-P	560 W	910 W	1275 W	1440 W*	1275 W
C9300-48UXM	PWR-C1-1100WAC-P	490 W	840 W	1205 W	1590 W	1205 W
C9300-48UN	PWR-C1-1100WAC-P	645 W	995 W	1360 W	1745 W	1360 W

* ハードウェアのポート数と PoE の規格に基づく制限 (例: PoE+ 30W * 24ports = 720W)

** デザインに基づく制限 (UPoE 60W * 30 = 1800W)

■ 注意点

Cisco Catalyst 9300 シリーズの 1100 WAC 電源モジュールは 125V 以上の電圧をサポートしています。
日本国内における 100V 電圧では、この要件を満たすことができず、実質 200V の電圧で使用いただくこととなります。

3.2 IOS Management

PoE

PoE コマンド ライン操作①

■ 機器への電源供給後に IOS-XE の起動を待たずに PoE 給電する設定: (初期値:無効)

```
C9200-01#configure terminal
C9200-01(config)#interface gigabitEthernet 1/0/1
C9200-01(config-if)#power inline port poe-ha
```

<注意>

機器への電源投入後、PoE への給電は約 60~50 秒で供給されます。

■ 機器のリブートを行っても継続して PoE 給電する設定: (初期値:無効)

```
C9200-01#configure terminal
C9200-01(config)#interface gigabitEthernet 1/0/1
C9200-01(config-if)#power inline port perpetual-poe-ha
```

■ ポートごとの電源供給量の制限、無効化、初期値化: (初期値:自動 30W)

```
C9200-01#configure terminal
C9200-01(config)#interface gigabitEthernet 1/0/1
C9200-01(config-if)#power inline auto max 15400
C9200-01(config-if)#
C9200-01(config)#interface gigabitEthernet 1/0/2
C9200-01(config-if)#power inline never
C9200-01(config-if)#
C9200-01(config)#interface gigabitEthernet 1/0/3
C9200-01(config-if)#power inline auto
```

最大 PoE 供給量を 15.4W に制限

PoE 供給を無効化

初期値の最大30Wに設定

<注意>

最大の供給量の単位は mW となり、最大の供給量が 15.4W の場合は 15400 を入力します。

全ポートで最大 15.4W の電力供給の確保に対し、最大供給値を 15000 と設定した場合電源不足になります。

3.2 IOS Management

PoE

PoE コマンドライン操作②

■ 供給電源量の監視設定：(初期値:無効)

```
C9200-01#configure terminal
C9200-01(config)#interface gigabitEthernet 1/0/1
C9200-01(config-if)#power inline police
C9200-01(config-if)#
C9200-01(config)#interface gigabitEthernet 1/0/2
C9200-01(config-if)# power inline police action log
C9200-01(config-if)#
C9200-01(config)#interface gigabitEthernet 1/0/3
C9200-01(config-if)# power inline police action errdisable
C9200-01(config-if)#
```

給電の監視を有効化
(ポートブロック)

給電の監視を有効化
(エラーログの表示)

給電の監視を有効化
(ポートブロック)

■ PoE の給電を受電機器に強制的に給電する設定：(初期値:自動30W)

```
C9200-01#configure terminal
C9200-01(config)#interface gigabitEthernet 1/0/1
C9200-01(config-if)#power inline static max 30000
C9200-01(config-if)#
```

30W 給電に固定設定

■ PoE の優先電源供給の設定：(初期値:Low)

```
C9200-01#configure terminal
C9200-01(config)#interface gigabitEthernet 1/0/1
C9200-01(config-if)#power inline port priority high
C9200-01(config-if)#
```

電源供給の優先化

<機能>

受電機器の障害や粗悪な PoE 受電機器により多くの電源を消費しようとした場合にエラー ログの表示やポートをブロックするアクションをとります。
(しきい値の 5% 多い消費電力を1秒以上続いた場合に発動します)

<注意>

この供給電力は事前に割り当てられ、電力供給が確保されます。
このワット数は、IEEE クラスまたは受電装置の CDP メッセージでは調整されなくなります。(固定給電)

<注意>

電源モジュールの障害により供給電力が低下した場合、低優先ポートに接続された PoE デバイスがシャットダウンされます。

3.2 IOS Management

PoE

PoE コマンド ライン操作③

■ PoE 給電状況の確認

```
C9200-01#show power inline
Module Available Used Remaining
(Watts) (Watts) (Watts)
-----
1      1480.0  26.0  1454.0
Interface Admin Oper Power Device Class Max
(Watts)
-----
Gi1/0/1 auto on 26.0 AIR-AP2802I-Q-K9 4 30.0
Gi1/0/2 auto off 0.0 n/a n/a 30.0
Gi1/0/3 auto off 0.0 n/a n/a 30.0
:
Gi1/0/24 auto off 0.0 n/a n/a 30.0
```

PoE 供給可能電力量、現在の使用電力量の表示、現在の使用可能電力量

Gi1/0/1 のポートにおいて、AP が接続され、15.4W が供給されていることを確認

■ 供給電源量の監視状況設定後の確認

```
C9200-01#show power inline police
Module Available Used Remaining
(Watts) (Watts) (Watts)
-----
1      1480.0  26.0  1454.0
Interface Admin Oper Admin Oper Cutoff Oper
State State Police Police Power Power
-----
Gi1/0/1 auto on errdisable ok 26.0 9.8
:
Gi1/0/24 auto off none n/a n/a n/a
```

Gi1/0/1 のポートにおいて、供給電力が 15.4W、実電源消費量が 7.2W。
発動した場合のアクションは errdisable に移行される設定であることを確認

Wireshark

機能説明

Cisco Catalyst Wireshark (Packet Capture)の機能では、スイッチ上で転送パケットをキャプチャし libpcap 形式 (.pcap)で保存することができます。また、CLI 上で簡易的なパケットデコード表示も可能です。

■ 特徴

パケットのキャプチャを行う際、従来はスイッチの設定変更や PC の準備など時間を要していた機能をスイッチの機能として盛り込んでいます。これにより作業開始までの時間を削減することができ運用負荷や問題切り分けの時間を短縮します。

■ 注意事項

バーストなどのパケット キャプチャが発生した場合は CPU 稼働率が高くなる可能性があります。本機能の利用には Cisco DNA Advantage ライセンスが必要になります。(サブスクリプション ライセンス) Cisco Catalyst 9200 シリーズはキャプチャを行い、pcapとして保存が可能です。

■ 補足

Wireshark (ワイヤシャーク)は、ネットワーク アナライザのソフトウェアです。
<https://www.wireshark.org/>

Wireshark

Wireshark コマンド ライン操作①

■ キャプチャ設定コマンド例(最低限): (インターフェイス、対象パケット、保存先)

```
C9300#monitor capture mycap interface GigabitEthernet1/0/1 both
C9300#monitor capture mycap match any
C9300#monitor capture mycap file location flash:mycap.pcap
C9300#
```

■ キャプチャ設定コマンド例

```
C9300#monitor capture mycap interface GigabitEthernet1/0/1 in
C9300#monitor capture mycap match ipv4 10.0.0.0/24 any
C9300#monitor capture mycap file location flash:mycap.pcap
C9300#monitor capture mycap limit duration 60 packets 50
C9300#monitor capture mycap buffer size 100
C9300#
```

```
C9300#monitor capture mycap match ipv4 protocol tcp 10.0.0.0/24 any eq 80
```

```
C9300# monitor capture mycap vlan 10 both
```

<注意>

- 設定や条件はキャプチャを停止するときに変更可能です。
- キャプチャ取得方向にて BOTH を設定してから IN を設定しても有効になりませんでした。一度 no コマンドにて削除してから再度設定をしてください。
- インターフェイス、IP アドレス、ポート番号などは 1 つのキャプチャ設定に各 1 種類しか設定ができません。
必要に応じて、マスクの変更や、レンジ、別キャプチャ名での設定により対応をお願いします。
- バッファ サイズの設定を上書きすると、保存先が消えてしまいます。

<注意>

特権 EXEC モードからの実行になります。

キャプチャ インターフェイスを vlan10 にした場合の設定例

3.2 IOS Management

Wireshark

Wireshark コマンド ライン操作②

■ キャプチャの実行コマンド

```
C9300#monitor capt mycap start
Started capture point : mycap
C9300#
Mar 26 10:48:29.072: %BUFCAP-6-ENABLE: Capture Point mycap enabled.
```

```
C9300#monitor capt mycap start
Capture mycap is already active
Unable to activate Capture.
C9300#
```

<注意>

同じキャプチャ名で再度キャプチャを実行した場合、ファイルは上書きされます。

すでに実行しているにも関わらず再度実行した場合の表示例

■ 最低限の設定が抜けていて、キャプチャが実行できない場合の表示例

```
C9300#monitor capture mycap3 start
A file by the same capture file name already exists, overwrite?[confirm]
Filter not attached to capture
Capture statistics collected at software:
  Capture duration - 0 seconds
  Packets received - 0
  Packets dropped - 0
  Packets oversized - 0
  Packets dropped in asic - 0
Unable to activate Capture.
C9300#
```

フィルタが設定されていない旨の表示

結果、キャプチャが実行されないメッセージ

Wireshark

Wireshark コマンド ライン操作③

■ キャプチャの停止コマンド

```
C9300#monitor capt mycap stop
Capture statistics collected at software:
  Capture duration - 31 seconds
  Packets received - 10
  Packets dropped - 0
  Packets oversized - 0
  Packets dropped in asic - 0
Capture buffer will exists till exported or cleared
Stopped capture point : mycap
Mar 26 10:52:14.598: %BUFCAP-6-DISABLE: Capture Point mycap disabled.
C9300#
```

キャプチャを停止した時点のキャプチャ情報

■ キャプチャの停止条件に該当して停止した場合の表示例

```
C9300#
Capture mycap stopped - Capture duration limit reached
Capture statistics collected at software:
  Capture duration - 60 seconds
  Packets received - 20
  Packets dropped - 0
  Packets oversized - 0
  Packets dropped in asic - 0
Capture buffer will exists till exported or cleared
Mar 26 10:55:20.764: %BUFCAP-6-DISABLE: Capture Point mycap disabled.
C9300#
```

60 秒経過したために停止した例

<参考>

事前の設定にて、キャプチャの終了条件を設定している場合は停止のコマンドは必要ありません。
(任意でキャプチャを終了させたい場合)

Wireshark

Wireshark コマンド ライン操作④

■ Wireshark のキャプチャ設定の確認コマンド例

```
C9300#show monitor capture mycap  
Status Information for Capture mycap
```

Target Type:

Interface: GigabitEthernet1/0/1, Direction: IN

Status : Inactive

Filter Details:

IPv4

Source IP: 10.0.0.0/24

Destination IP: any

Protocol: tcp

Destination port(s) : = 80

Buffer Details:

Buffer Type: LINEAR (default)

File Details:

Associated file name: flash:mycap032602.pcap

Limit Details:

Number of Packets to capture: 100

Packet Capture duration: 360

Packet Size to capture: 0 (no limit)

Maximum number of packets to capture per second: 1000

Packet sampling rate: 0 (no sampling)

Target Type:

Interface: Vlan,

Ingress: 10

Egress: 10

Status : Active

キャプチャの条件

キャプチャのインターフェイス及び、キャプチャの取得方向 (IN、OUT、BOTH: 両方向)

キャプチャの動作有無 (Inactive: 停止、Active: 実行中)

キャプチャのフィルタ

ポート番号 top 80 を指定してパケットの送信元 10.0.0.0/24 から送信先はすべて対象の表示例

キャプチャ結果の保存先

保存先のディレクトリとファイル名

キャプチャを停止する条件

キャプチャ実行後の停止条件。表示例では 60 秒間、50 パケットまたは、100MB (いずれかの早い値)

キャプチャ対象を VLAN10 を設定した場合の表示例

キャプチャの動作有無 (Inactive: 停止、Active: 実行中)

3.2 IOS Management

Wireshark

Wireshark コマンド ライン操作⑤

■ ファイルに保存されたキャプチャ データの表示例

```
C9300#show monitor capture file flash:mycap.pcap
Starting the packet display ..... Press Ctrl + Shift + 6 to exit

 1  0.000000 b8:38:61:83:18:1d -> b8:38:61:83:18:1d LOOP 60 Reply
 2  3.907931 b8:38:61:83:18:1d -> 01:00:0c:cc:cc:cc CDP 431 Device ID: AP2602l Port ID: GigabitEthernet0
 3  9.995596 b8:38:61:83:18:1d -> b8:38:61:83:18:1d LOOP 60 Reply
 4  19.793680 cc:70:ed:f6:81:01 -> 01:00:0c:cc:cc:cc DTP 60 Dynamic Trunk Protocol
 5  19.793719 cc:70:ed:f6:81:01 -> 01:00:0c:cc:cc:cc DTP 90 Dynamic Trunk Protocol
C9300#
```

■ ファイルに保存されたキャプチャ データの表示例

```
C9300#show monitor capture file flash:mycap.pcap display-filter "ip.src == 10.0.0.2" brief
Starting the packet display ..... Press Ctrl + Shift + 6 to exit

 1  0.000000000 10.0.0.2 -> 10.0.0.1 ICMP 114 Echo (ping) request id=0x002e, seq=0/0, ttl=254
 3  0.000908000 10.0.0.2 -> 10.0.0.1 ICMP 114 Echo (ping) request id=0x002e, seq=1/256, ttl=254
 5  0.002961000 10.0.0.2 -> 10.0.0.1 ICMP 114 Echo (ping) request id=0x002e, seq=2/512, ttl=254
 7  0.004835000 10.0.0.2 -> 10.0.0.1 ICMP 114 Echo (ping) request id=0x002e, seq=3/768, ttl=254
 9  0.006850000 10.0.0.2 -> 10.0.0.1 ICMP 114 Echo (ping) request id=0x002e, seq=4/1024, ttl=254
11  0.008768000 10.0.0.2 -> 10.0.0.1 ICMP 114 Echo (ping) request id=0x002e, seq=5/1280, ttl=254
13  0.010695000 10.0.0.2 -> 10.0.0.1 ICMP 114 Echo (ping) request id=0x002e, seq=6/1536, ttl=254
15  0.012728000 10.0.0.2 -> 10.0.0.1 ICMP 114 Echo (ping) request id=0x002e, seq=7/1792, ttl=254
17  0.014652000 10.0.0.2 -> 10.0.0.1 ICMP 114 Echo (ping) request id=0x002e, seq=8/2048, ttl=254
19  0.016682000 10.0.0.2 -> 10.0.0.1 ICMP 114 Echo (ping) request id=0x002e, seq=9/2304, ttl=254
21  0.018655000 10.0.0.2 -> 10.0.0.1 ICMP 114 Echo (ping) request id=0x002e, seq=10/2560, ttl=254
23  0.020575000 10.0.0.2 -> 10.0.0.1 ICMP 114 Echo (ping) request id=0x002e, seq=11/2816, ttl=254
```

<参考>

フィルタ条件は以下の表示などがあります。

ip.src	:送信元の IP アドレスの値
ip.dst	:宛先の IP アドレスの値
ip.addr	:送信元または、宛先のIPアドレスの値
eth.src	:送信元の MAC アドレスの値
eth.dst	:宛先の MAC アドレスの値
eth.addr	:送信元または、宛先の MAC アドレスの値
ip	:IPv4 のみ
tcp	:tcp のみ
udp	:udp のみ

3.2 IOS Management

Wireshark

Wireshark コマンド ライン操作⑥

■ ファイルに保存されたキャプチャ データを USB メモリへ保存

キャプチャ データを PC などで確認する際にはキャプチャ データを USB などにコピーすることにより PC での確認が可能になります。PC での確認の際には、libpcap 形式(.pcap) が表示できるアナライザ ソフトを準備していただく必要があります。

```
C9300-24#show flash:
-#- --length-- -----date/time----- path
 2  2097152 May 09 2019 08:50:26.0000000000 +00:00 nvram_config
 3  2097152 May 09 2019 08:50:26.0000000000 +00:00 nvram_config_bkup
 4  700524979 Mar 26 2019 12:36:55.0000000000 +00:00 cat9k_iosxe.16.09.02.SPA.bin

344  4096 Mar 12 2019 08:42:29.0000000000 +00:00 tracelogs/modules
345  13900 Mar 12 2019 06:08:29.0000000000 +00:00 webuiTmp.pcap
346  9208 Mar 26 2019 12:05:36.0000000000 +00:00 cat9k-wlc.16.09.03.SPA.pkg
347 15836096 Mar 26 2019 12:39:18.0000000000 +00:00 cat9k-webui.16.09.02.SPA.pkg
348  133 Mar 26 2019 12:19:53.0000000000 +00:00 .fpga_upg_run.log
349  9152 Mar 26 2019 12:39:18.0000000000 +00:00 cat9k-wlc.16.09.02.SPA.pkg
350  7554 Mar 26 2019 12:39:38.0000000000 +00:00 cat9k_iosxe.16.09.02.SPA.conf
7592071168 bytes available (3184406528 bytes used)
```

```
C9300-24#
*May 10 08:49:05.306: %IOSD_INFRA-6-IFS_DEVICE_OIR: Device usbflash0 added
C9300-24#
C9300-24#copy flash: usbflash0:
Source filename []? webuiTmp.pcap
Destination filename [webuiTmp.pcap]?
Copy in progress...C
13900 bytes copied in 0.052 secs (267308 bytes/sec)
C9300-24#
```

3.2 IOS Management

Wireshark

キャプチャファイルの PC 表示

The screenshot shows the Wireshark interface with a network capture file named 'webuiTmp.pcap' open. The main pane displays a list of captured packets. The selected packet is a DHCP Discover packet (No. 7) with the following details:

No.	Time	Source	Destination	Protocol	Length	Info
7	0.000021	0.0.0.0	255.255.255.255	DHCP	346	DHCP Discover - Transaction ID 0xe2cc81b3

The packet details pane shows the following structure:

- Frame 1: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface 0
- Ethernet II, Src: Cisco_60:e0:6e (58:ac:78:60:e0:6e), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
- 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 951
- Internet Protocol Version 4, Src: 172.16.0.254, Dst: 224.0.0.5
- Open Shortest Path First

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 01 00 5e 00 00 05 58 ac 78 60 e0 6e 81 00 03 b7 ..^...X. x`n...
0010 08 00 45 c0 00 68 05 7e 00 00 01 59 25 ec ac 10 ..E..h~...Y%...
0020 00 fe e0 00 00 05 02 01 00 34 c0 a8 01 02 00 00 .....4.....
0030 00 00 45 7b 00 00 00 00 00 00 00 00 00 00 ff ff ..E{.....
0040 ff 00 00 0a 12 01 00 00 00 28 ac 10 00 fe ac 10 .....(.....
0050 00 04 c0 a8 04 fe c0 a8 05 fe 7f 48 00 08 00 01 .....H...
0060 00 04 00 00 00 01 00 12 00 04 00 00 00 41 80 00 .....A...
0070 00 08 00 00 00 09 00 00 00 41
```

EnergyWise

機能説明

EnergyWise 機能では、電力配分の最適化や、電源供給の供給や停止をコントロールし電力量の削減を行うことが可能になります。

■ 特徴

従来の Cisco Catalyst 2000 シリーズから基本機能は変更されていません。

曜日や時間によって、Interface の Up/Down をコントロールすることが可能となり、Interface の Up に伴う電力消費や、PoE などの電力供給の削減を行い、コストの削減や CO2 の削減に貢献します。

■ 注意事項

EnergyWise の設定は、各物理 Interface ごとに設定を行いますが、最初にグローバル コンフィギュレーション モードからドメインの設定を行う必要があります。

3.2 IOS Management

EnergyWise

EnergyWise コマンドライン操作①

■ EnergyWise の基本設定

```
C9200-01#configure terminal
C9200-01(config)#energywise domain cisco security shared-secret 0 cisco
C9200-01(config)#
C9200-01(config)#time-range onlabfloor02
C9200-01(config-time-range)#absolute start 00:00 01 January 2019
C9200-01(config-time-range)#periodic weekdays 7:00 to 19:00
C9200-01(config-time-range)#periodic weekend 17:10 to 17:15
C9200-01(config-time-range)#
C9200-01(config-time-range)#time-range offlabfloor02
C9200-01(config-time-range)#absolute start 00:00 01 January 2019
C9200-01(config-time-range)#periodic weekdays 00:00 to 07:00
C9200-01(config-time-range)#periodic weekdays 19:00 to 23:59
C9200-01(config-time-range)#periodic weekend 00:00 to 17:09
C9200-01(config-time-range)#periodic weekend 17:16 to 23:59
C9200-01(config-time-range)#
C9200-01(config-time-range)#interface giga 1/0/1
C9200-01(config-if)#energywise level 10 recurrence importance 80 time-range onlabfloor02
C9200-01(config-if)#energywise level 0 recurrence importance 80 time-range offlabfloor02
C9200-01(config-if)#energywise name AP
C9200-01(config-if)#energywise role manager
C9200-01(config-if)#
```

<機能1>

Periodic の設定に関しては、平日 (weekdays) や、週末 (weekend) の他に、毎日 (daily) や、曜日指定 (sunday, monday など) を行うことも可能

←最初にドメインの設定(必須)

←InterfaceのUpの時間設定

開始日時

平日の Up の時間

週末の Up の時間

Interface の Down の時間設定

開始日時

平日の Down の時間

週末の Down の時間

G1/0/1 に定義

Level10(電力On)の定義

Level0(電力Off)の定義

<機能2>

Level 10 は電力供給

Level 0 は電力休止になります。

EnergyWise では電力レベルを一元管理することにより一連の電力レベルを定義しています。単独で動作させる場合は他の Level を使用することはありません。

3.2 IOS Management

EnergyWise

EnergyWise コマンドライン操作②

■ EnergyWise の動作確認

```
C9200-01#sh energywise recurrences
System level recurrence
Level Time-range
-----
```

Id	Interface	Class	Action	Lvl	Cron/Time-range
1	Gi1/0/1	QUERY SET	10	onlabfloor02	
2	Gi1/0/1	QUERY SET	0	offlabfloor02	

```
Alarms
Endpoint   Id   Interface  Lvl Status
-----
```

■ 時間設定の確認

```
C9200-01#show time-range
time-range entry: offlabfloor02 (active)
  absolute start 00:00 01 January 2019
  periodic weekdays 0:00 to 7:00
  periodic weekdays 19:00 to 23:59
  periodic weekend 0:00 to 17:09
  periodic weekend 17:16 to 23:59
  used in: EnergyWise
time-range entry: onlabfloor02 (inactive)
  absolute start 00:00 01 January 2019
  periodic weekdays 7:00 to 19:00
  periodic weekend 17:10 to 17:15
  used in: EnergyWise
```

Interface G1/0/1 に 2 つの時間設定がされていることを確認

<機能>

Periodic の設定に関しては、平日 (weekdays) や、週末 (weekend) の他に、毎日 (daily) や、曜日指定 (Sunday、Monday など) を行うことも可能

2 つの時間設定がされており、有効な状態であることを確認

<注意>

時間の連携に関しては、機器内の時間を参照して動作しています。事前にタイムゾーンの設定や、NTP の設定を行うことを推奨しています。

3.2 IOS Management

EnergyWise

EnergyWise コマンドライン操作③

- EnergyWise 動作の確認: Interface G1/0/1 が Down 状態から時間 (週末の17:10) になると Up 状態に移行されることを確認

```
C9200-01#show time-range
time-range entry: offlabfloor02 (active)
  absolute start 00:00 01 January 2019
```

時間の設定が Down 側が有効になっていることを確認

```
periodic weekend 0:00 to 17:09
```

17:09 まで有効(厳密には 17:09:59 まで有効)

```
periodic weekend 17:16 to 23:59
used in: EnergyWise
```

```
time-range entry: onlabfloor02 (inactive)
  absolute start 00:00 01 January 2019
```

```
periodic weekdays 7:00 to 19:00
```

```
periodic weekend 17:10 to 17:15
```

Up 側は 17:10 から有効

```
used in: EnergyWise
```

```
C9200-01#
```

```
Feb 24 17:10:03.304: %ILPOWER-7-DETECT: Interface Gi1/0/1: Power Device detected: IEEE PD
```

```
Feb 24 17:10:04.304: %ILPOWER-5-POWER_GRANTED: Interface Gi1/0/1: Power granted
```

←17:10 になると、interface に電源が供給され G1/0/1 が UP することを確認

```
Feb 24 17:10:08.289: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to up
```

```
Feb 24 17:10:09.289: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up
```

```
C9200-01#sh clock
```

```
17:10:29.910 JST Sun Feb 24 2019
```

現時刻の確認

```
C9200-01#sh time-range
```

```
time-range entry: offlabfloor02 (inactive)
  absolute start 00:00 01 January 2019
```

```
used in: EnergyWise
```

```
time-range entry: onlabfloor02 (active)
```

時間の設定が Up 側が有効になっていることを確認

```
  absolute start 00:00 01 January 2019
```

```
periodic weekdays 7:00 to 19:00
```

```
periodic weekend 17:10 to 17:15
```

```
used in: EnergyWise
```

Blue Beacon

機能説明①

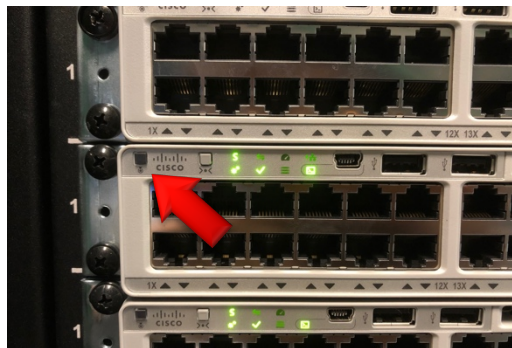
Blue Beacon の機能では本機器の全面と背面に連動する LED を搭載しており、アクセスしている機器を簡単に識別できます。

■ 特徴

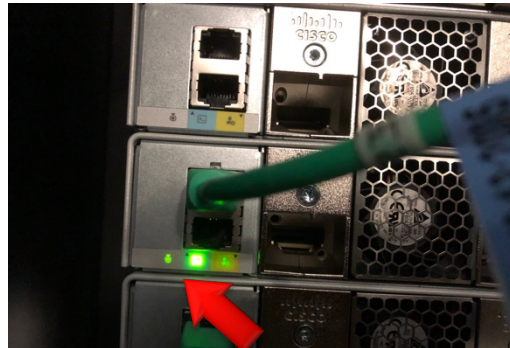
前面にある Blue Beacon のボタンを押すか、CLI により設定を有効にすると、ボタン自体が青く点灯し、同時に背面の Blue Beacon のLEDが点灯します。これにより、機器の識別が容易となり、運用管理の負荷が軽減されます。

Cisco Catalyst 9000 シリーズからの新機能になります。

<前面の Blue Beacon 通常状態>



<背面の Blue Beacon 通常状態>



<注意>

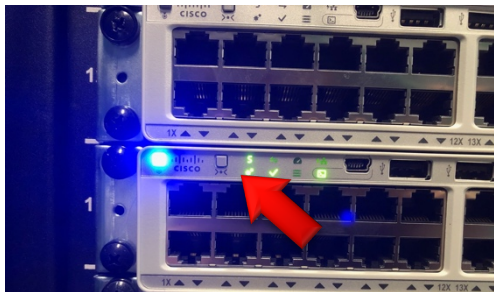
背面の LED 部分に関して
右隣の LED の影響によって少し光っているように見えます。

Cisco Catalyst 9200では、他の Cisco Catalyst 9000 シリーズでは設定方法が異なります。

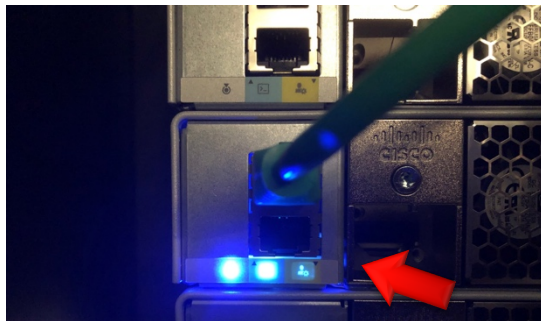
Blue Beacon

機能説明 ②

<前面の Blue Beacon が点灯の状態>



<背面の Blue Beacon が点灯の状態>



<注意>

Blue Beacon をボタンで有効にする場合は前面のボタンでしか有効になりません。
(背面は LED は表示のみになります。)

背面の Blue Beacon の光が強いため、右隣の LED が青色に光っているように見えます。

<Cisco Catalyst 9300
前面の Blue Beacon が点灯の状態>



<Cisco Catalyst 9500
前面の Blue Beacon が点灯の状態>



3.2 IOS Management

Blue Beacon

Cisco Catalyst 9200 シリーズにおける Blue Beacon の設定

■ CLI による Blue Beacon を有効にする設定

```
C9200-01#configure terminal
C9200-01(config)#hw-module beacon on switch 1
C9200-01(config)#
C9200-01(config)#exit
C9200-01#
C9200-01#
```

■ CLI による Blue Beacon を無効にする設定

```
C9200-01#configure terminal
C9200-01(config)#hw-module beacon off switch 1
C9200-01(config)#
C9200-01(config)#exit
C9200-01#
C9200-01#
```

または、

```
C9200-01#configure terminal
C9200-01(config)#no hw-module beacon on switch 1
C9200-01(config)#
C9200-01(config)#exit
C9200-01#
C9200-01#
```

Blue Beacon

Cisco Catalyst 9300 シリーズおよび Cisco Catalyst 9500 シリーズにおける Blue Beacon の設定

■ CLI による Blue Beacon を有効にする設定

```
C9300#hw-module beacon slot 1 on
C9300#
*Apr  5 09:03:26.709: %PLATFORM_LED-6-BEACON_LED_TURNED: Switch 1 Beacon LED turned ON
C9300#
```

Blue Beacon の LED 表示を有効にする設定

ログ表示

■ CLI による Blue Beacon を無効にする設定

```
C9300#hw-module beacon slot 1 off
C9300#
*Apr  5 09:18:25.784: %PLATFORM_LED-6-BEACON_LED_TURNED: Switch 1 Beacon LED turned OFF
C9300#
```

Blue Beacon の LED 表示を無効にする設定

ログ表示

3.2 IOS Management

Blue Beacon

Blue Beacon のログメッセージ

■ Blue Beacon のログメッセージ結果

C9200-01#

Feb 24 12:25:54.128: %PLATFORM_LED-6-BEACON_LED_TURNED: Switch 1 Beacon LED turned ON

Blue Beaconが有効 (ONの点灯状態)

Feb 24 12:38:08.010: %PLATFORM_LED-6-BEACON_LED_TURNED: Switch 1 Beacon LED turned OFF

Blue Beaconが無効 (OFFの消灯状態)

C9200-01#

■ CLI による Blue Beacon の結果

C9200-01#show beacon
Switch# Beacon Status

*1 ON

Blue Beaconが有効 (ONの点灯状態)

C9200-01#
C9200-01#show beacon
Switch# Beacon Status

*1 OFF

Blue Beaconが無効 (OFFの消灯状態)

C9200-01#

TDR

TDR(Time Domain Reflector)機能では、UTP/STP ケーブル自体の問題の診断および解決を行うことができます。

■ 特徴

UTP/STP 銅線ツイストペアケーブルの断線やショート(短絡)の有無や、断線箇所までのおおよその距離の把握が可能です。

TDR を実行すると、ローカル デバイスがケーブル経由で信号を送信して、反射信号を最初の信号と比較します。

■ 他機器との比較

コマンドや動作に関しては他機器と同じになります。

Cisco Catalyst 9300 シリーズは16.9.2 より、
Cisco Catalyst 9200 シリーズは 16.12.1よりサポートします。

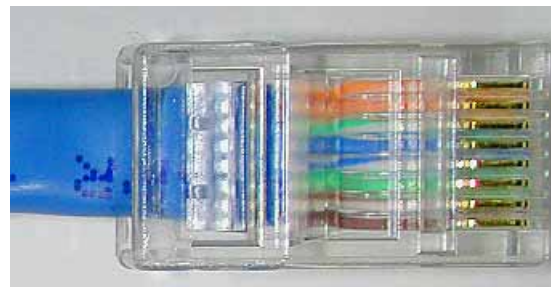
■ 注意事項

TDR のサポートは銅線 イーサネット(ツイストペアケーブル)のみサポートしており、SFPやSFP+ ポートなどではサポートされません。

対向に機器を接続した状態(IEEE 802.3 に準拠)を前提に実施してください。

■ 結線

- 1.PairA (橙白)
- 2.PairA (橙)
- 3.PairB (緑白)
- 4.PairC (青)
- 5.PairC (青白)
- 6.PairB (緑)
- 7.PairD (茶白)
- 8.PairD (茶)



3.2 IOS Management

TDR

TDR では、実行コマンドで測定を行い、確認コマンドで実行結果を確認します。

■ TDR テストの実行コマンド

```
C9300#test cable-diagnostics tdr interface gigabitEthernet 2/0/10
TDR test started on interface Gi2/0/10
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
C9300#
```

TDR テストの実行コマンド

<注意>

TDR のテストを実行時、該当 Interface の Down / Up が発生します。
テストは約 10 秒の時間を要します。

■ TDR テストの実行結果の確認コマンド

```
C9300#show cable-diagnostics tdr interface gigabitEthernet 2/0/10
TDR test last run on: March 05 05:20:19
```

Interface	Speed	Local pair	Pair length	Remote pair	Pair status
-----------	-------	------------	-------------	-------------	-------------

Gi2/0/10	1000M	Pair A	4 +/- 10 meters	Pair B	Normal
		Pair B	9 +/- 10 meters	Pair A	Normal
		Pair C	4 +/- 10 meters	Pair D	Normal
		Pair D	2 +/- 10 meters	Pair C	Normal

C9300#

TDR の実行結果

ツイスト ペア ケーブルが正しく結線されている場合の表示

```
C9300#show cable-diagnostics tdr interface gigabitEthernet 2/0/10
TDR test last run on: March 05 05:19:43
```

Interface	Speed	Local pair	Pair length	Remote pair	Pair status
-----------	-------	------------	-------------	-------------	-------------

Gi2/0/10	1000M	Pair A	N/A	N/A	Not Completed
		Pair B	N/A	N/A	Not Completed
		Pair C	N/A	N/A	Not Completed
		Pair D	N/A	N/A	Not Completed

C9300#

TDR テスト実行コマンドの入力後、10 秒を待たずに結果を表示しようとした場合の結果

TDR

■ 接続対向機器が 1G インターフェースの場合

```
C9300#show cable-diagnostics tdr interface gigabitEthernet 2/0/10  
TDR test last run on: March 07 03:25:11
```

```
Interface  Speed Local pair Pair length      Remote pair Pair status  
-----  
Gi2/0/10  1000M Pair A   4  +/- 10 meters Pair B   Normal  
          Pair B   0  +/- 10 meters Pair A   Normal  
          Pair C   4  +/- 10 meters Pair D   Normal  
          Pair D   2  +/- 10 meters Pair C   Normal
```

```
C9300#
```

■ 接続対向機器が 100M インターフェースの場合

```
C9300#show cable-diagnostics tdr interface gigabitEthernet 2/0/12  
TDR test last run on: March 07 03:25:13
```

```
Interface  Speed Local pair Pair length      Remote pair Pair status  
-----  
Gi2/0/12  100M  Pair A   9  +/- 10 meters N/A   Normal  
          Pair B  10  +/- 10 meters N/A   Normal  
          Pair C   1  +/- 5 meters N/A   Short  
          Pair D   1  +/- 5 meters N/A   Short
```

```
C9300#
```

100M サポート インターフェースの場合 Pair C、Pair D は無視してください。

TDR

■ 接続対向機器が不明の場合

```
C9300#show cable-diagnostics tdr interface gigabitEthernet 2/0/14
TDR test last run on: March 07 03:31:51
```

Interface	Speed	Local pair	Pair length	Remote pair	Pair status
-----------	-------	------------	-------------	-------------	-------------

Gi2/0/14	auto	Pair A	1 +/- 5 meters	N/A	Open
		Pair B	1 +/- 5 meters	N/A	Open
		Pair C	1 +/- 5 meters	N/A	Open
		Pair D	1 +/- 5 meters	N/A	Open

```
C9300#
```

<注意>

接続対向機器が接続されていない場合、接続対向機器の電源が落ちている場合は TDR の計測ができません。

TDR

■ 擬似障害ケーブルを作成

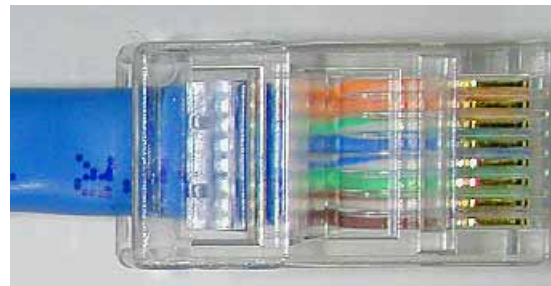
1. Pair A 断線(橙X)
2. Pair C 断線(青X)
3. Pair A ショート(橙 & 橙白)
4. Pair AC 間一部ショート(橙 & 青)
5. Pair C 内逆接続(青 <----> 青白)
6. Pair C と Pair D 間で一部逆接続(青白 <----> 茶白)
7. Pair C と Pair D 間を逆接続(青&青白 <----> 茶&茶白)

■ 検証構成

- a. Catalyst9300 (G2/0/10) ----- 1G接続 ----- (G1/0/1) Catalyst9200

■ 結線

- 1.PairA (橙白)
- 2.PairA (橙)
- 3.PairB (緑白)
- 4.PairC (青)
- 5.PairC (青白)
- 6.PairB (緑)
- 7.PairD (茶白)
- 8.PairD (茶)



ストレートケーブルを使用(※両端同じ結線)

3.2 IOS Management

TDR

■ 擬似障害ケーブルの診断結果 1. Pair A 断線(橙 X)

```
C9300#show cable-diagnostics tdr interface gigabitEthernet 2/0/10
TDR test last run on: March 11 13:25:27
```

Interface	Speed	Local pair	Pair length	Remote pair	Pair status
-----------	-------	------------	-------------	-------------	-------------

```
-----
Gi2/0/10 1000M Pair A 3 +/- 5 meters Pair B Open
Pair B 9 +/- 10 meters Pair A Normal
Pair C 7 +/- 10 meters Pair D Normal
Pair D 7 +/- 10 meters Pair C Normal
```

```
C9300#
```

■ 擬似障害ケーブルの診断結果 2. Pair C 断線(青 X)

```
C9300#show cable-diagnostics tdr interface gigabitEthernet 2/0/10
TDR test last run on: March 11 13:29:51
```

Interface	Speed	Local pair	Pair length	Remote pair	Pair status
-----------	-------	------------	-------------	-------------	-------------

```
-----
Gi2/0/10 1000M Pair A 7 +/- 10 meters Pair B Normal
Pair B 10 +/- 10 meters Pair A Normal
Pair C 0 +/- 5 meters Pair D Open
Pair D 5 +/- 10 meters Pair C Normal
```

```
C9300#
```

■ 擬似障害ケーブルの診断結果 3. Pair A ショート(橙 & 橙白)

```
C9300#show cable-diagnostics tdr interface gigabitEthernet 2/0/10
TDR test last run on: March 11 13:31:52
```

Interface	Speed	Local pair	Pair length	Remote pair	Pair status
-----------	-------	------------	-------------	-------------	-------------

```
-----
Gi2/0/10 auto Pair A 0 +/- 5 meters N/A Short
Pair B 0 +/- 10 meters N/A Normal
Pair C 0 +/- 10 meters N/A Normal
Pair D 0 +/- 10 meters N/A Normal
```

```
C9300#
```

■ 擬似障害ケーブルの診断結果 4. Pair AC間一部ショート(橙&青)

```
C9300#show cable-diagnostics tdr interface gigabitEthernet 2/0/10
TDR test last run on: March 11 13:33:06
```

Interface	Speed	Local pair	Pair length	Remote pair	Pair status
-----------	-------	------------	-------------	-------------	-------------

```
-----
Gi2/0/10 100M Pair A 0 +/- 5 meters N/A Short/Crosstalk
Pair B 0 +/- 10 meters N/A Normal
Pair C 0 +/- 5 meters N/A Short/Crosstalk
Pair D 0 +/- 10 meters N/A Normal
```

```
C9300#
```

3.2 IOS Management

TDR

■ 擬似障害ケーブルの診断結果 5. Pair C 内逆接続(青 <--> 青白)

```
C9300#show cable-diagnostics tdr interface gigabitEthernet 2/0/10
TDR test last run on: March 11 13:35:43
```

Interface	Speed	Local pair	Pair length	Remote pair	Pair status

Gi2/0/10	1000M	Pair A	9 +/- 10 meters	Pair A	Normal
		Pair B	7 +/- 10 meters	Pair B	Normal
		Pair C	9 +/- 10 meters	Pair C	Normal
		Pair D	7 +/- 10 meters	Pair D	Normal

```
C9300#
```

■ 擬似障害ケーブルの診断結果

6. Pair C と Pair D 間で一部逆接続(青白 <--> 茶白)

```
C9300#show cable-diagnostics tdr interface gigabitEthernet 2/0/10
TDR test last run on: March 11 13:38:02
```

Interface	Speed	Local pair	Pair length	Remote pair	Pair status

Gi2/0/10	100M	Pair A	10 +/- 10 meters	N/A	Normal
		Pair B	7 +/- 10 meters	N/A	Normal
		Pair C	3 +/- 5 meters	N/A	Short/Crosstalk
		Pair D	3 +/- 5 meters	N/A	Short/Crosstalk

```
C9300#
```

■ 擬似障害ケーブルの診断結果 7. Pair C と Pair D 間を逆接続(青&青白 <--> 茶&茶白)

```
C9300#show cable-diagnostics tdr interface gigabitEthernet 2/0/10
TDR test last run on: March 11 13:39:26
```

Interface	Speed	Local pair	Pair length	Remote pair	Pair status

Gi2/0/10	1000M	Pair A	5 +/- 10 meters	Pair A	Normal
		Pair B	9 +/- 10 meters	Pair B	Normal
		Pair C	9 +/- 10 meters	Pair D	Normal
		Pair D	9 +/- 10 meters	Pair C	Normal

```
C9300#
```

<注意>

- 5. Pair C 内逆転の結果にもある通り、Pair 中での極性は判定できません。(以前と同様)
- スイッチ と AP 間にパワー インジェクタがある場合では、インジェクタ前後の検証では同様の結果の表示となります。TDR 使用時には配線を分割して TDR を使用する必要があります。
- ケーブル長に関しては目安程度になります。(以前と同様)

3.3 Basic L2/L3

EtherChannel

VTP

STP

MST

REP

FHRP

VRF

IGMP

EtherChannel

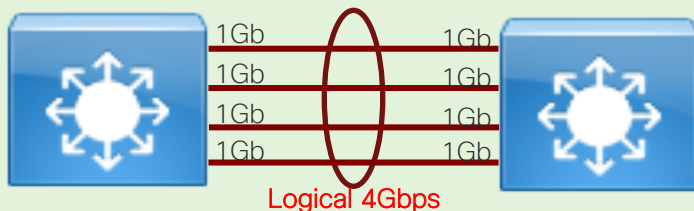
■ EtherChannel

- 複数の物理リンクを 1 つの論理リンクにバンドルし、帯域幅を確保する技術です。
- バンドルしている物理リンクの 1 つに障害が発生したとしても、残りのリンクを用いて通信が可能なので回線冗長も可能になります。

■ Multi-chassis EtherChannel (MEC)

- EtherChannel の 1 つ、複数筐体に対して別々のリンクを使用します。

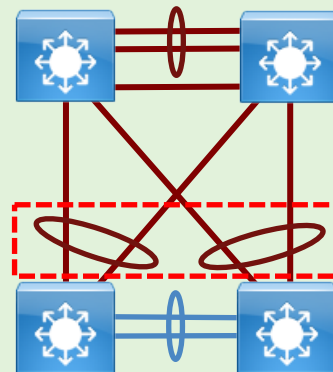
<対応プロトコル>
PAgP、LACP、Static



Layer2/Layer3 リンク双方に対応

<対応プロトコル>
PAgP、LACP、Static

StackWise や StackWise Virtual を構成する複数の筐体にまたがって EtherChannel を構成する方法です。筐体の単一障害時にも EtherChannel リンクの可用性を確保します。



EtherChannel の設定例

■ EtherChannel の作成: LACP Active モード

```
C9300-1#conf t
C9300-1(config)#interface range gi1/0/4-5
C9300-1(config-if-range)#channel group 1 mode active
Creating a port-channel interface Port-channel 1
```

■ EtherChannel の負荷分散方式の設定

```
C9300-1(config)#port-channel load-balance ?
dst-ip          Dst IP Addr
dst-mac         Dst Mac Addr
dst-mixed-ip-port Dst IP Addr and TCP/UDP Port
dst-port       Dst TCP/UDP Port
extended       Extended Load Balance Methods
src-dst-ip     Src XOR Dst IP Addr
src-dst-mac    Src XOR Dst Mac Addr
src-dst-mixed-ip-port Src XOR Dst IP Addr and TCP/UDP Port
src-dst-port   Src XOR Dst TCP/UDP Port
src-ip        Src IP Addr
src-mac       Src Mac Addr
src-mixed-ip-port Src IP Addr and TCP/UDP Port
src-port      Src TCP/UDP Port
```

<注意>

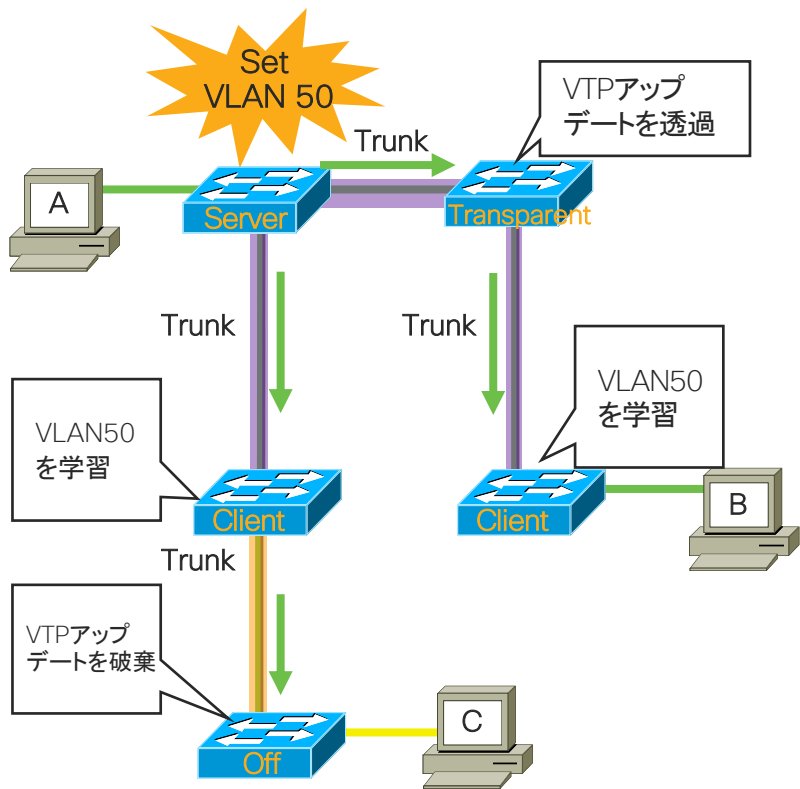
Catalyst 上では設定に応じて PortChannel XX (XX は設定時のグループ番号)という論理インターフェイスが自動生成されます。

- デフォルトは送信元 MAC (src-mac) に従いロード バランスされます。
- Extended オプションを使うことで、送信元および宛先的方式を組み合わせた、拡張ロード バランスを指定することができます。

Cisco Catalyst 9000 の EtherChannel

	9200 9200L	9300 9300L	9400	9500 9500-H	9600
サポート	○	○	○	○	○
ライセンス	Network Essentials	Network Essentials	Network Essentials	Network Essentials	Network Essentials
最大チャネル数	48	128	128	128	128
最大メンバ数	PAgP: 8 LACP: 16	PAgP: 8 LACP: 16	PAgP: 8 LACP: 16	PAgP: 8 LACP: 16	PAgP: 8 LACP: 16

VTP (VLAN Trunking Protocol)



- ネットワークを構成する複数のスイッチにわたり、VLAN の追加、削除、名前の変更を集中管理することで、VLAN 設定の整合性を維持するためのプロトコルです。
- Trunk リンクでのみ動作します。
- VTP Version 3 から認証、拡張 VLAN (VLAN ID が 4094 まで) をサポートします。
- 4 つのモード:
 - Server: VLAN 情報を集中管理し、変更があれば Client スイッチにアップデートを送信
 - Client: VTP アップデートを受信し、更新する
 - Transparent: VTP アップデートをパス スルーする
 - Off: VTP アップデートを破棄する

VTP の設定とログ

C9300-1 VTP Server 設定・ログ:

```
C9300-1#conf t
C9300-1(config)#vtp version 3
C9300-1(config)#vtp domain catalyst
Changing VTP domain name from manufacturing to catalyst
C9300-1(config)#
*Jan 23 04:05:49.017: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to catalyst.
C9300-1(config)#vtp mode server
Setting device to VTP Server mode for VLANs.
C9300-1(config)#end
```

VTP ドメインを設定する必要があります。

C9300-2 VTP Client 設定・ログ:

```
C9300-2#conf t
C9300-2(config)#vtp version 3
C9300-2(config)#vtp domain catalyst
Changing VTP domain name from manufacturing to catalyst
C9300-2(config)#
*Jan 23 04:04:55.014: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to catalyst.
C9300-2(config)#vtp mode client
Setting device to VTP Client mode for VLANs.
C9300-2(config)#end
```

1 台の VTP サーバが VTP クライアントに対して VLAN の設定変更を通知します。

VTP の設定確認

C9300-1 VTP 設定確認:

C9300-1#show vtp status

VTP Version capable : 1 to 3

VTP version running : 3

VTP Domain Name : catalyst

VTP Pruning Mode : Disabled

VTP Traps Generation : Disabled

Device ID : 70b3.17fa.f100

Configuration last modified by 172.16.1.2 at 1-23-19 04:56:46

Local updater ID is 172.16.1.2 on interface V110 (lowest numbered VLAN interface found)

Feature VLAN:

VTP Operating Mode : Server

Maximum VLANs supported locally : 1005

Number of existing VLANs : 13

Configuration Revision : 1

MD5 digest : 0x81 0x17 0xD5 0xBF 0xC7 0x87 0x9E 0x3D
0xE6 0x33 0x0D 0x52 0xEF 0x21 0x2D 0x10

VTP バージョンが確認できます。

VTP のモードが確認できます。
2号機ではこれが Client になっています。

Cisco Catalyst 9000 の VTP

	9200 9200L	9300 9300L	9400	9500 9500-H	9600
サポート	○	○	○	○	○
ライセンス	Network Essentials	Network Essentials	Network Essentials	Network Essentials	Network Essentials

STP (Spanning Tree Protocol)

機種ごとのスケーラビリティ

インスタンス数などの変更と設定時のログについて編集必要

	C9600	C9500-H	C9500	C9400	C9300 C9300L	C9200	C9200L
使用可能なVLAN ID 数 ^{*1}	4K	4K	4K	4K	4K	4K	1024
Active VLAN 数(SVI) ^{*2}	1000	1000	1000	1000	1000	1000	512
インスタンス数	1000	1000	256	256	256	128	128

PVST+/Rapid PVST+ で構成したときのインスタンスが上記を超過してしまう場合、MST で構成いただくことを推奨しています。

インスタンス数＝トポロジー数となりインスタンスはトポロジーを形成する単位となります。
C9200 を例に次ページにて表記します。

■ 注意事項

本情報は 2019 年 10 月時点での情報となり、今後変更される可能性があります。

最新版に関しましては、該当機器のリリース ノートやコンフィギュレーション ガイド等を参照いただきますようお願いいたします。

<https://www.cisco.com/c/en/us/support/switches/index.html>

*1: システム予約による VLAN ID を含みます。

*2: IOS-XE16.12.1 時点における推奨 Active VLAN 数になります。

STP (Spanning Tree Protocol)

VLAN とインスタンス数 (Cisco Catalyst 9200L の場合)

・VLAN ID として使用可能な数字: 1~4094

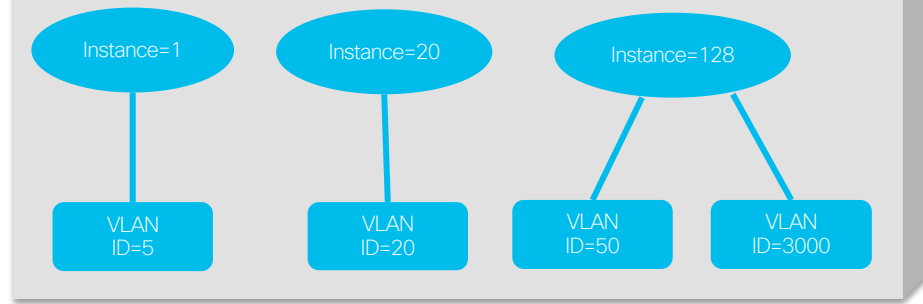


・機器上 (DB) に設定可能な VLAN 最大数:
1024 個



Cisco Catalyst 9200L 機器

・機器上での STP インスタンス数:
128 個



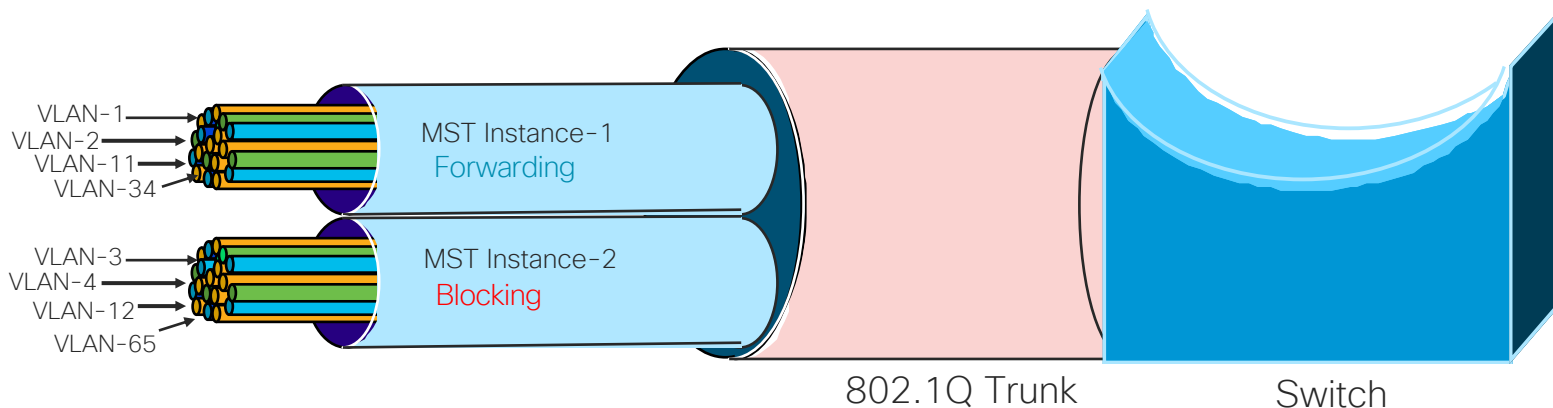
・機器上で同時 Active な VLAN 最大数:
512 個

VLAN Configuration Guide, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9200 Switches)
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9200/software/release/16-12/configuration_guide/vlan/b_1612_vlan_9200_cg.html

※ ここでは、設計に必要なとなるVLANやSpanning Tree等のスケーラビリティ情報について、Catalyst 9200を例に示しました。設計の際は、実際に利用する製品・バージョンにて同様な情報を確認するようお願いいたします。

MST (Multiple Spanning-Tree)

- 多数の VLAN が存在する環境で簡素な設定と VLAN 運用が可能な STP の方式です。
- 単一のインスタンスに複数の VLAN 情報を格納した STP の共通トポロジーをスイッチ間で構成します。
- Cisco Catalyst 9000 シリーズでは 1 インスタンスに所属できる VLAN 数に制限がありません。
- スイッチ間で、リージョン名、リビジョン番号、MST インスタンス ID と VLAN の対応を同じにする必要があります。
- 従来の PVST / Rapid PVST+ と互換性があるため、既存の環境から柔軟に展開することができます。



MST の基本設定と確認

C9300-1 MST設定:

```
C9300-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
C9300-1(config)#spanning-tree mst configuration
C9300-1(config-mst)#instance 1 vlan 10-20
C9300-1(config-mst)#name RegionTEST
C9300-1(config-mst)#revision 1
```

C9300-1 MST設定確認:

```
C9300-1(config-mst)#show pending
Pending MST configuration
Name [RegionTEST]
Revision 1 Instances configured 2
```

Instance Vlans mapped

```
-----
0      1-9,21-4094
1      10-20
-----
```

```
C9300-1(config-mst)#
C9300-1(config-mst)#end
C9300-1#
```

VLAN と MST インスタンスのマッピング

リージョン名の設定

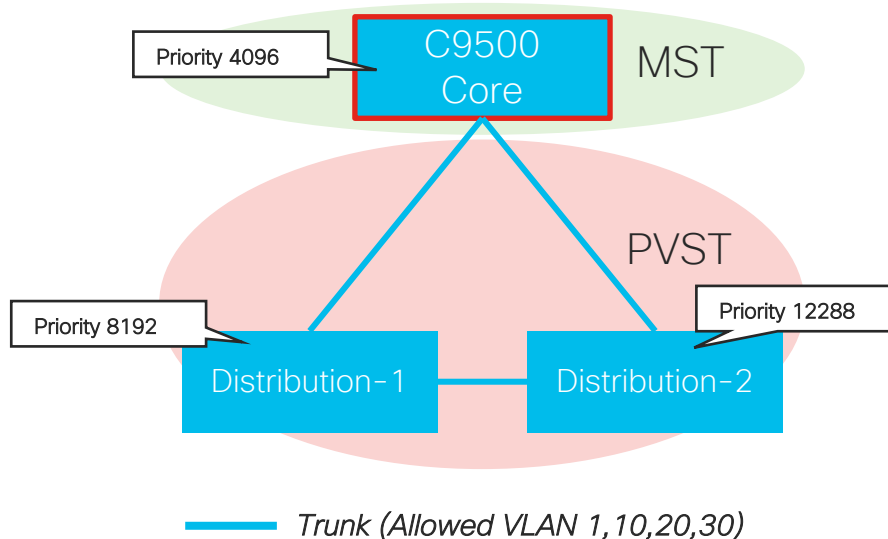
リビジョン番号の設定 (0-65536)

MST コンフィギュレーションモードで show pending をすることで設定情報を確認できる

MST と PVST の相互運用

設定の基本指針

- ① コアを MST モードへ変更し、全体のルートブリッジ (CIST Root) にします。
- ② 整合性を取るため、MST0 の優先度を PVST 領域で定義された全ての VLAN よりも上位 (低 Priority 値) で設定します。



■ C9500

```
spanning-tree mode mst
spanning-tree mst configuration
name cisco
revision 1
instance 1 vlan 10, 20, 30
spanning-tree mst 0 priority 4096
```

■ Distribution-1

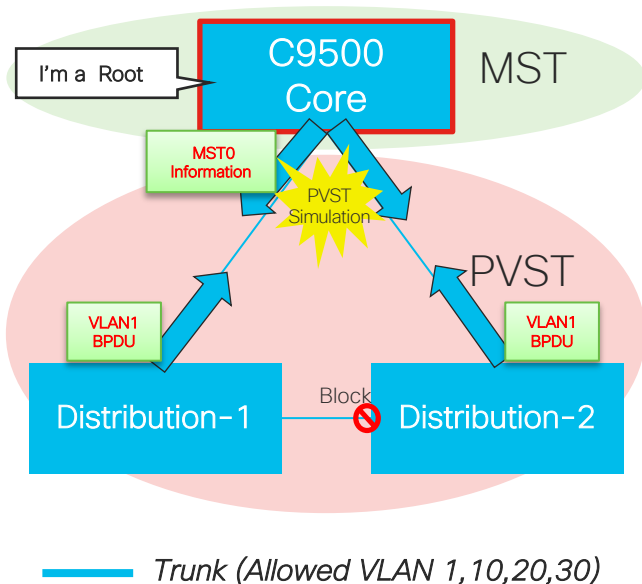
```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1,10,20,30 priority 8192
```

■ Distribution-2

```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1,10,20,30 priority 12288
```

MST と PVST の相互運用

”MST 0” と ”VLAN 1” のブリッジ情報が比較され、C9500 が全体の Root に選定されます。



```
C9500#show spanning-tree mst 0
```

```
##### MST0   vlans mapped: 1-9,11-19,21-29,31-4094
Bridge      address 08ec.f5f7.3380 priority 4096 (0 sysid 0)
Root        this switch for the CIST
Operational hello time 2 , forward delay 15, max age 20, txholdcount 6
Configured  hello time 2 , forward delay 15, max age 20, max hops 20
```

Interface	Role	Sts Cost	Prio.Nbr	Type
Gi1/0/1	Desg FWD	20000	128.1	P2p Bound(PVST)
Gi1/0/2	Desg FWD	20000	128.2	P2p Bound(PVST)

```
Distribution-2#show spanning-tree vlan 10
```

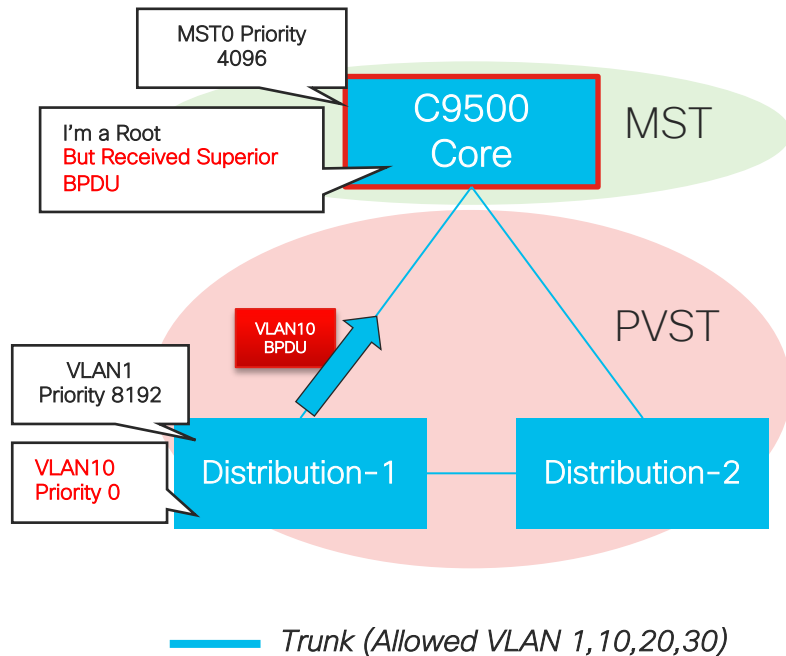
```
VLAN0010
Spanning tree enabled protocol rstp
Root ID Priority 4096
Address 08ec.f5f7.3380
Cost 4
Port 1 (GigabitEthernet1/0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 12298 (priority 12288 sys-id-ext 10)
Address 7488.bb41.f200
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec
```

Interface	Role	Sts Cost	Prio.Nbr	Type
Gi1/0/1	Root FWD	4	128.1	P2p Peer(STP)
Gi1/0/2	Altn BLK	4	128.2	P2p

MST と PVST の相互運用

整合性チェックに失敗する例



- Distribution-1 の VLAN10 Priority を 0 にして動作確認

```
Distribution-1(config)#spanning-tree vlan 10 priority 0
```

- "MST0" と "VLAN1" のブリッジ情報が比較され、C9500 が全体のルートブリッジに選定されます
- しかし、Distribution-1から VLAN10 の上位 BPDU を受信し、整合性チェックに失敗します(ルート ガードに類似)

```
C9500#show spanning-tree mst 0
```

```
##### MST0   vlans mapped: 1-9,11-19,21-29,31-4094
Bridge   address 08ec.f5f7.3380 priority 4096 (4096 sysid 0)
Root     this switch for the CIST
Operational hello time 2 , forward delay 15, max age 20, txholdcount 6
Configured hello time 2 , forward delay 15, max age 20, max hops 20
```

Interface	Role	Sts	Cost	Prio.	Nbr	Type
Gi1/0/1	Desg	BKN*20000	128.1	128.1		P2p Bound(PVST) *PVST_Inc
Gi1/0/2	Desg	BKN*20000	128.2	128.2		P2p Bound(PVST) *PVST_Inc

MST と PVST の相互運用

補足

- PVST 領域内に CIST ルートブリッジを配置することも可能ですが、シスコとしては非推奨
- 詳しくは以下のリンクをご参照ください

Understanding Multiple Spanning Tree Protocol (802.1s)

https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24248-147.html?referring_site=bodynav

REP (Resilient Ethernet Protocol)

■ REP の概要

- 複数のスイッチ間で一貫した REP の設定を行う「セグメント」を定義し、その中での保護対象リンクやブロックポート（転送停止ポート）が任意に指定可能です。

■ 高速切り替え

- 最短 50ミリ秒 の高速切り替えが可能です。(50ミリ秒～200ミリ秒程度)

■ リングの独立冗長

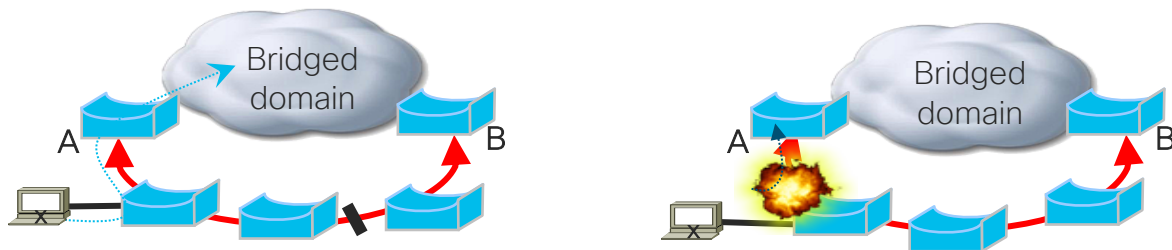
- パス プロテクトを管理、複数のリングを接続する複雑な構成に対応します。
- リング単位の障害検知により障害の局所化、分散が可能です。
- 他の Ring 障害の影響を受けません。

■ 最適経路設計

- リング ネットワークの経路指定、冗長経路設計が可能です。
- EtherChannel による柔軟な帯域増設ができます。

REP の構成

■ Segment



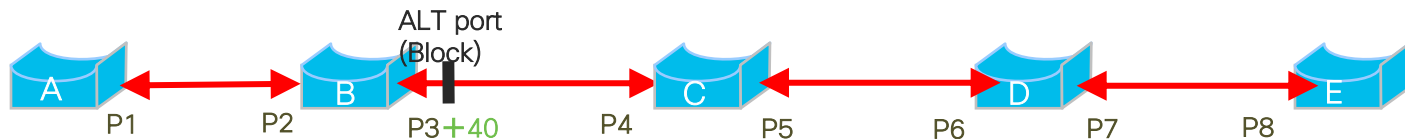
REP セグメントは他の L2 ネットワークに対し A または B のように冗長経路を提供します。障害時ブロック状態を解き冗長経路を提供します。

■ REP Ring



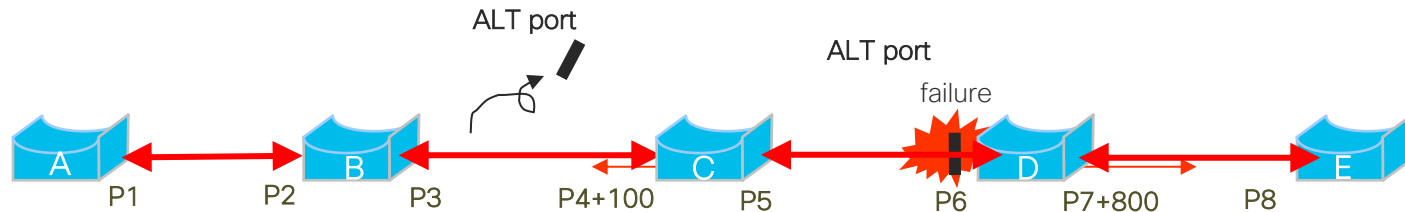
リング状に構成されるときに、REP のセグメントは、2 つのスイッチの間に冗長の接続性を提供します。リングとセグメントの組み合わせにより多種のネットワークを構成できます。

REP セグメント プロトコル 概要



各ポートは 1 つのセグメント ID 上の一部として構成されます。

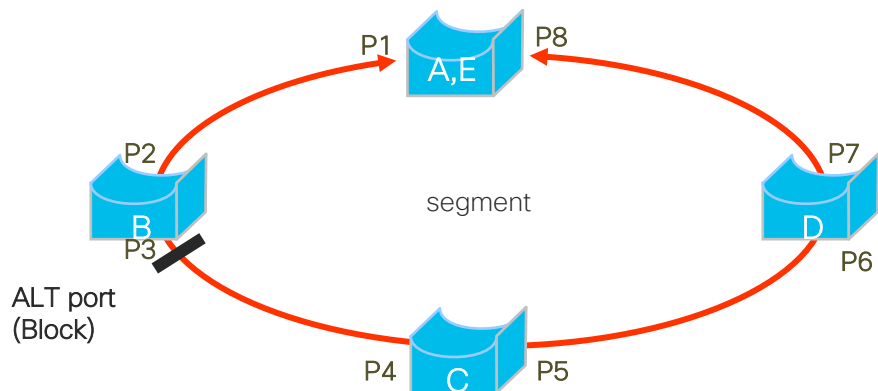
Segment のすべてのリンクで REP が Enable のときに、セグメントを通じ REP Edge “A”と “E”の間(任意の部分)に ALT Port (Block)を決めます。



もし障害が REP セグメント中に起これば、ブロック ポートはデータ フォワードを開始します。

REP セグメント プロトコル 概要

REP セグメント プロトコルを使った Ring Topology

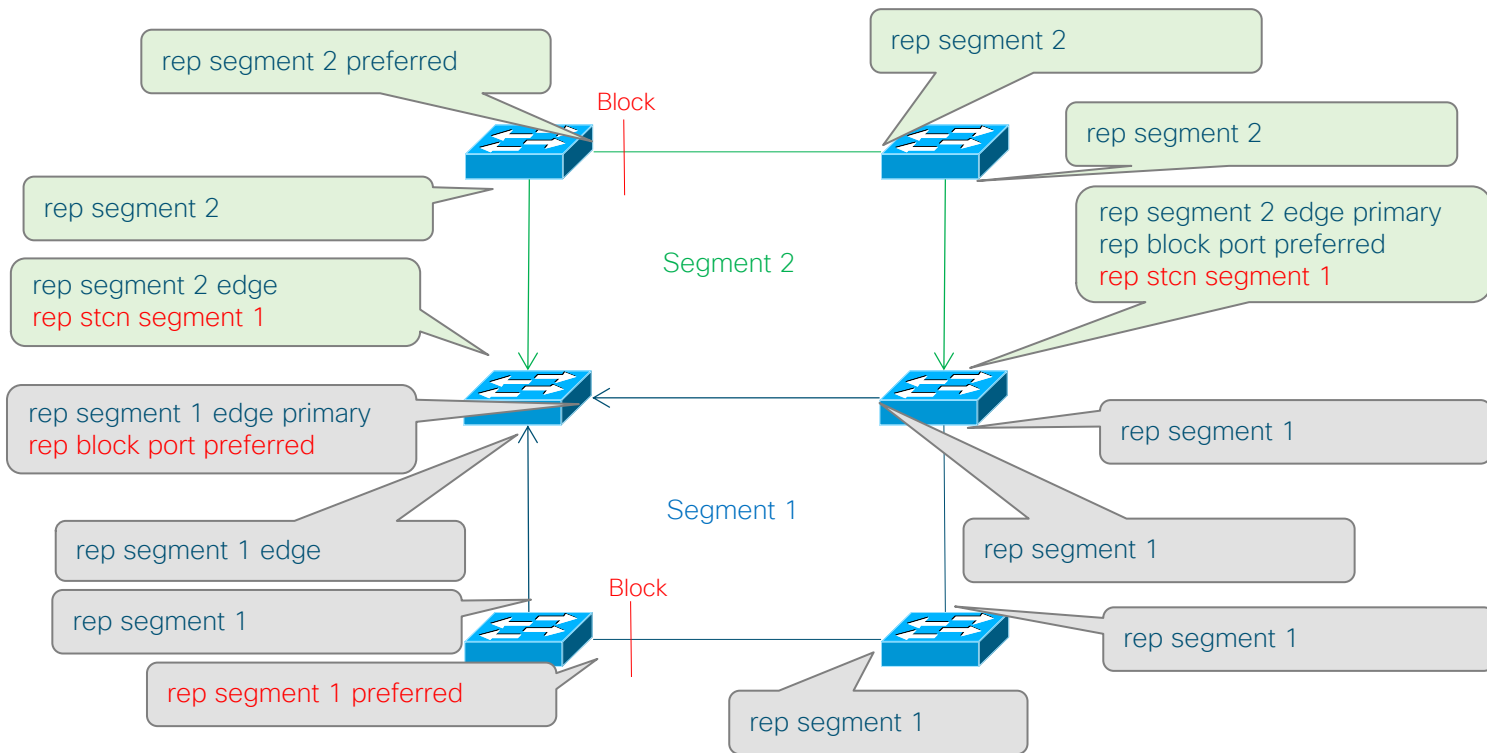


A、E の様に REP Edge Port は 1つの Node に収用することが可能です。

REP 設定例

※ブロックポート (Alt、Failed) はセグメントに 1 つ

- rep stcn segment 1: セグメント 2 の障害をセグメント 1 に通達
- rep block port preferred: ブロックポートを Static に指定するための設定 (プライマリ エッジで設定)
- rep segment 1 preferred: セグメント 1 のブロックポートに指定



3.3 Basic L2/L3

REP の設定確認

C9300-1#[show rep topology](#)

REP Segment 1

BridgeName	PortName	Edge Role
------------	----------	-----------

C9300-1	Gi1/0/3	Pri* Open
C9300-1	Gi1/0/2	Open
C9300-1	Gi1/0/2	Sec Alt

C9300-1#[show rep topology detail](#)

REP Segment 1

C9300-1, Gi1/0/3 (Primary Edge No-Neighbor)

Open Port, all vlans forwarding

Bridge MAC: 701f.5301.2c80

Port Number: 003

Port Priority: 000

Neighbor Number: 1 / [-3]

C9300-1, Gi1/0/2 (Intermediate)

Open Port, all vlans forwarding

Bridge MAC: 701f.5301.2c80

Port Number: 002

Port Priority: 000

Neighbor Number: 2 / [-2]

C9300-1, Gi1/0/2 (Secondary Edge)

Alternate Port, some vlans blocked

Bridge MAC: 70b3.17fa.f100

Port Number: 002

Port Priority: 000

Neighbor Number: 3 / [-1]

REP セグメント 1 に所属しているポート一覧が表示されます。

より詳しい内容が確認できます。

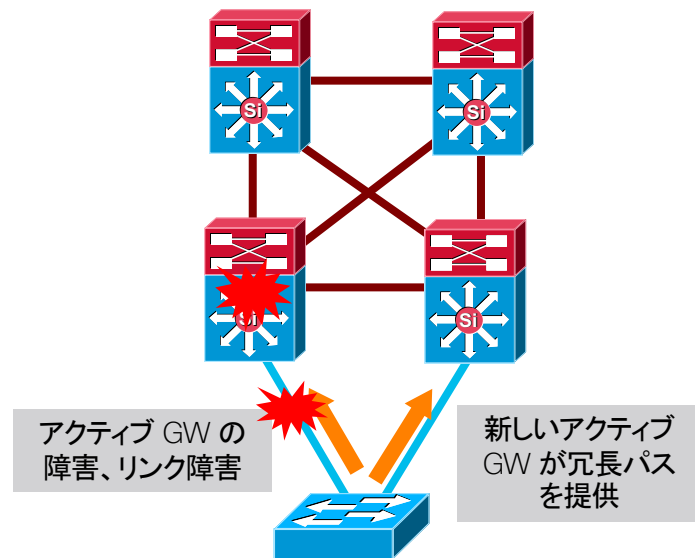
Cisco Catalyst 9000 シリーズの REP

	9200 9200L	9300 9300L	9400	9500
サポート	○	○	○	○
ライセンス	Network Essentials	Network Essentials	Network Essentials	Network Essentials

First Hop Redundancy (FHRP)

IP のネクスト ホップやデフォルト ゲートウェイとなる IP アドレスを複数のルータ / L3 の間で共有し、冗長化 / 高可用化を行う「ゲートウェイ冗長化」機能の総称です。

HSRP	VRRP	GLBP ※Catalyst 9000 未サポート
<ul style="list-style-type: none"> ・シスコ独自プロトコル ・冗長構成を組む機器の中で1台の「Active」と1台の「Standby」のロールが自動決定され、Active は仮想 IP アドレスをもちトラフィックを受信、転送します。 ・Active だった機器の障害発生時は Standby の機器が自動的に Active に切り替わります。また、残りの機器からあらたに Standby が選出されます。 	<ul style="list-style-type: none"> ・標準化プロトコル ・冗長構成を組む機器の中で 1 台の「Master」と1 台以上「Backup」のロールが自動決定され、Master は仮想 IP アドレスをもちトラフィックを受信、転送します。 ・Master だった機器の障害発生時は Backup の機器の中から Active が自動的に再選出されます。 	<ul style="list-style-type: none"> ・シスコ独自プロトコル ・HSRP や VRRP と違い、冗長構成を組んでいるすべての機器が分散処理を行います。 ・AVG (Active Virtual Gateway) と AVF (Active Virtual Forwarder) という役割が各ルータにアサインされ、AVG に障害が起きた場合、他の AVF が AVG に昇格します。



HSRP の設定とログ

C9300-1 設定:

```
C9300-1#conf t
C9300-1(config)#interface vlan 10
C9300-1(config-if)#ip address 172.16.1.2 255.255.255.0
C9300-1(config-if)#standby 1 ip 172.16.1.1
C9300-1(config-if)#end
```

C9300-2 設定:

```
C9300-2#conf t
C9300-2(config)#interface vlan 10
C9300-2(config-if)#ip address 172.16.1.3 255.255.255.0
C9300-2(config-if)#standby 1 ip 172.16.1.1
C9300-2(config-if)#end
```

C9300-1 HSRPログ:

```
*Jan 21 06:09:02.309: %HSRP-5-STATECHANGE: Vlan10 Grp 1 state Standby -> Active
```

C9300-2 HSRPログ:

```
*Jan 21 06:08:00.344: %HSRP-5-STATECHANGE: Vlan10 Grp 1 state Speak -> Standby
```

1号機が、2号機ともに用いる HSRP の仮想 IP アドレスを指定します

設定入力後、このようなログが表示され、それぞれが Active、Standby 状態へ移行したことが確認できます

HSRP の設定確認

C9300-1 HSRP 設定確認:

```
C9300-1#show standby brief
```

```
    P indicates configured to preempt.
```

Interface	Grp	Pri	P	State	Active	Standby	Virtual IP
Vl10	1	100	Active	local	172.16.1.3	172.16.1.1	

C9300-2 HSRP 設定確認:

```
C9300-2#show standby brief
```

```
    P indicates configured to preempt.
```

Interface	Grp	Pri	P	State	Active	Standby	Virtual IP
Vl10	1	100	Standby	172.16.1.2	local	172.16.1.1	

1号機が Active、2号機が Standby であることを確認します

C9300-1 Show Arp:

```
C9300-1#show arp
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	172.16.1.1	103	0000.0c07.ac01	ARPA	Vlan10
Internet	172.16.1.2	0	70b3.17fa.f146	ARPA	Vlan10
Internet	172.16.1.3	0	70b3.17e9.cec6	ARPA	Vlan10
Internet	172.16.1.4	-	701f.5301.2cc6	ARPA	Vlan10
Internet	172.16.1.5	0	701f.53b8.49c6	ARPA	Vlan10

仮想 MAC アドレスが割り当てられていることが確認できます

VRRP の設定とログ

C9300-1 設定:

```
C9300-1#conf t
C9300-1(config)#fhrp version vrrp v3
C9300-1(config)#interface vlan 10
C9300-1(config-if)#vrrp 1 address-family ipv4
C9300-1(config-if-vrrp)#address 172.16.1.1
C9300-1(config-if-vrrp)#end
```

C9300-2 設定:

```
C9300-2#conf t
C9300-2(config)#fhrp version vrrp v3
C9300-2(config)#interface vlan 10
C9300-2(config-if)#vrrp 1 address-family ipv4
C9300-2(config-if-vrrp)#address 172.16.1.1
C9300-2(config-if-vrrp)#end
```

C9300-1 VRRPログ:

```
*Jan 22 02:48:52.425: %VRRP-6-STATE: Vlan10 IPv4 group 1 state INIT -> BACKUP
*Jan 22 02:48:56.037: %VRRP-6-STATE: Vlan10 IPv4 group 1 state BACKUP -> MASTER
```

C9300-2 VRRPログ:

```
*Jan 22 02:48:43.487: %VRRP-6-STATE: Vlan10 IPv4 group 1 state INIT -> BACKUP
```

VRRP v3 を有効にします

1号機が、2号機ともに用いる VRRP の仮想 IP アドレスを指定します

設定入力後、このようなログが表示され、それぞれが Master、Backup 状態へ移行したことが確認できます

VRRP の設定確認

C9300-1 VRRP 設定確認:

```
C9300-1#show vrrp detail
```

```
Vlan10 - Group 1 - Address-Family IPv4
```

```
Description is "ipv4test"
```

State is MASTER

```
State duration 15 mins 39.644 secs
```

Virtual IP address is 172.16.1.1

Virtual MAC address is 0000.5E00.0101

```
Advertisement interval is 1000 msec
```

```
Preemption enabled
```

```
Priority is 100
```

Master Router is 172.16.1.2 (local), priority is 100

```
Master Advertisement interval is 1000 msec (expires in 898 msec)
```

```
Master Down interval is unknown
```

```
FLAGS: 1/1
```

```
VRRPv3 Advertisements: sent 1042 (errors 0) - rcvd 0
```

```
VRRPv2 Advertisements: sent 0 (errors 0) - rcvd 0
```

(以下略)

1号機が Master (2号機が Backup) という状態を確認します

割り当てた仮想 IP アドレスと与えられた仮想 MAC アドレスを確認できます

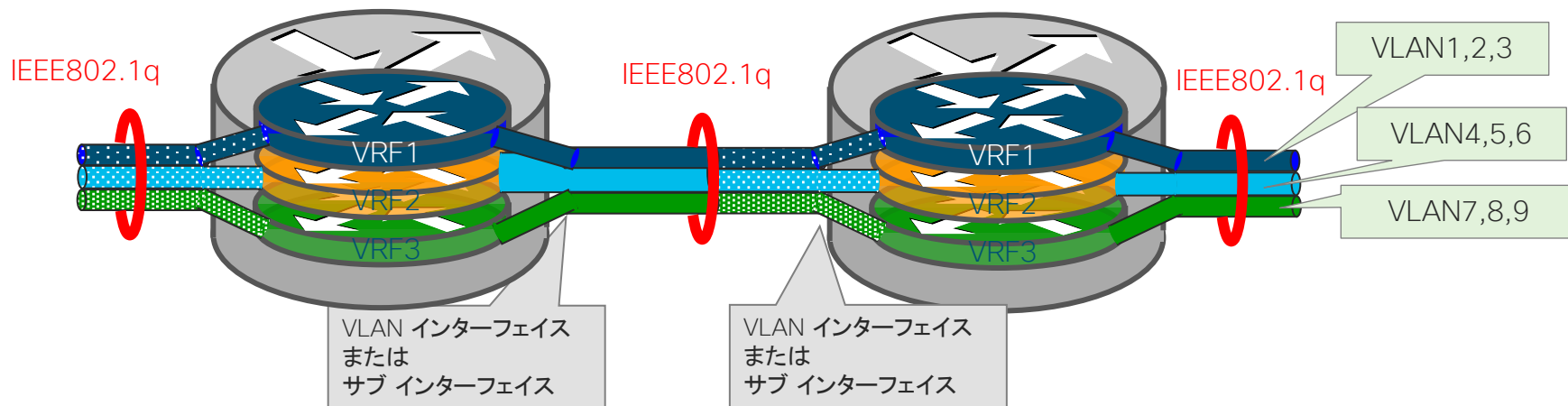
現在の Master の確認と priority 値を確認できます

Cisco Catalyst 9000 シリーズの FHRP

	9200 9200L	9300 9300L	9400	9500 9500-H	9600
HSRP サポート	○ Network Advantage	○ Network Advantage	○ Network Advantage	○ Network Advantage	○ Network Advantage
VRRP サポート	○ Network Essentials	○ Network Essentials	○ Network Essentials	○ Network Essentials	○ Network Essentials
GLBP サポート	×	×	×	×	×

VRF (Virtual Routing and Forwarding)

- ルーティング テーブルの仮想化技術です。
- 1 つの機器上に複数のルーティング テーブルを保持し、それぞれ別のルーティング プロトコルを動作させることも可能です
- 物理 / 論理インターフェイスそれぞれをいずれかのルーティング テーブルにひもづけ、ルーティング テーブルごとに独立した転送処理を同時に行います。



※VRFは通信キャリアが複数顧客に同時にサービスする MPLS-VPN で開発されました。MPLS-VPN から切り離された単独の機能名は「VRF-Lite」の呼称が与えられてきましたが、ここでは一貫して「VRF」とします。

VRF の設定

C9500 VRF の設定:

```
C9500-1#conf t
C9500-1(config)#ip vrf RED
C9500-1(config-vrf)#rd 1:100
C9500-1(config-vrf)#exit
C9500-1(config)#ip vrf BLUE
C9500-1(config-vrf)#rd 2:200
C9500-1(config-vrf)#interface port-channel 2
C9500-1(config-if)#no switchport
C9500-1(config-if)#ip vrf forwarding RED
C9500-1(config-if)#ip address 192.168.1.2 255.255.255.0
C9500-1(config-if)#no shut
C9500-1(config-if)#interface port-channel 3
C9500-1(config-if)#no switchport
C9500-1(config-if)#ip vrf forwarding BLUE
C9500-1(config-if)#ip address 192.168.2.2 255.255.255.0
C9500-1(config-if)#no shut
C9500-1(config-if)#end
```

2つの VRF を作成しています

VRF の設定をインターフェイスに適用します
(※ IP アドレスがインターフェイスにもともと登録されている場合、VRF のコマンドにより初期化されるため再入力が必要です)

VRF の設定確認

C9500 VRF の設定確認:

C9500-1# show ip route vrf RED

Routing Table: RED

(中略)

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.1.0/24 is directly connected, Port-channel2

L 192.168.1.2/32 is directly connected, Port-channel2

C9500-1# show ip route vrf BLUE

Routing Table: BLUE

(中略)

Gateway of last resort is not set

192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.2.0/24 is directly connected, Port-channel3

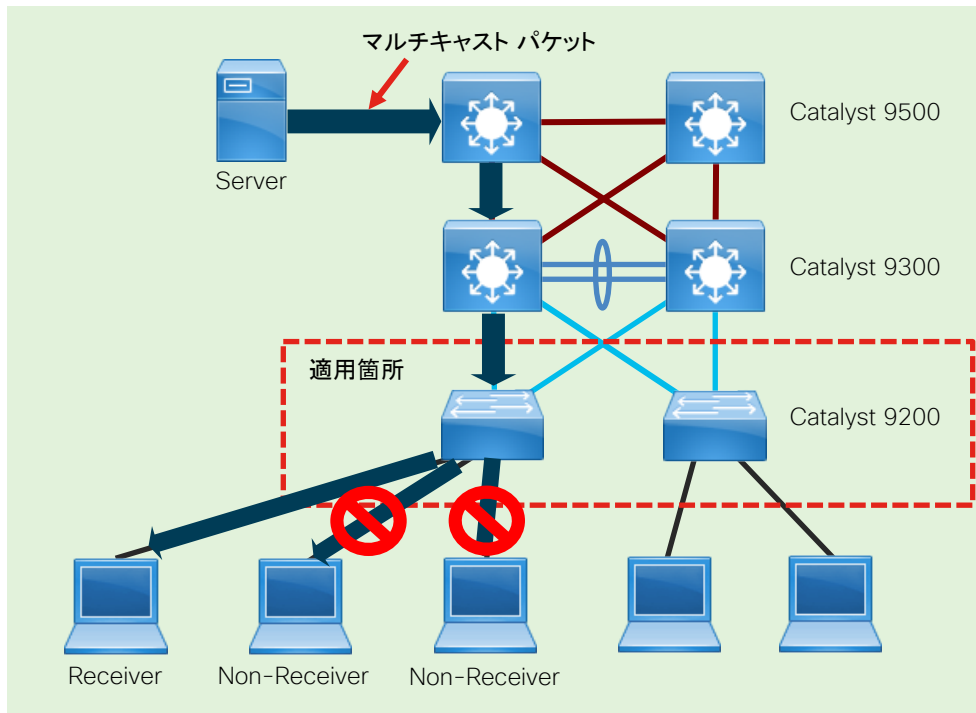
L 192.168.2.2/32 is directly connected, Port-channel3

Cisco Catalyst 9500 の中に別々のルーティング
テーブルを保持している状態が確認できます

Cisco Catalyst 9000 シリーズの VRF

	9200L	9200	9300 9300L	9400	9500 9500-H	9600
サポート	○	○	○	○	○	○
ライセンス	Network Advantage					
最大VRF数	1	4	256	256	256	1024

IGMP Snooping / MLD Snooping



■ IGMP Snooping

- VLAN 環境で IPv4 マルチキャスト パケットを余分に転送させないように制御することで帯域幅の消費を抑える技術です。
- Catalyst スイッチでは基本的に**有効化**されています。
- 同一 VLAN 内にいるマルチキャスト パケットの Receiver をスイッチが認識することでフラディングを行わないように動作します

■ MLD Snooping

- VLAN 環境で IPv6 マルチキャスト パケットを余分に転送させないように制御することで帯域幅の消費を抑える技術です。
- Catalyst スイッチでは基本的に**無効化**されています。
- 同一 VLAN 内にいるマルチキャストパケットの Receiver をスイッチが認識することでフラディングを行わないように動作します

IGMP Snooping と MLD Snooping の設定と確認

IGMP Snooping の設定確認:

```
C9300-1#show ip igmp snooping
Global IGMP Snooping configuration:
```

```
-----
IGMP snooping           : Enabled
Global PIM Snooping     : Disabled
IGMPv3 snooping         : Enabled
Report suppression      : Enabled
TCN solicit query       : Disabled
TCN flood query count   : 2
Robustness variable     : 2
Last member query count : 2
Last member query interval : 1000
(以下略)
```

MLD Snooping の設定:

```
C9300-1#conf t
C9300-1(config)#ipv6 mld snooping
(C9300-1(config)#ipv6 mld snooping vlan [vlan-id])
C9300-1(config)#end
```

MLD Snooping の設定確認:

```
C9300-1#show ipv6 mld snooping
Global MLD Snooping configuration:
```

```
-----
MLD snooping           : Enabled
Global PIM Snooping     : Disabled
MLDv2 snooping         : Disabled
Listener message suppression : Disabled
TCN solicit query       : Disabled
TCN flood query count   : 2
Robustness variable     : 2
Last listener query count : 2
Last listener query interval : 1000
(以下略)
```

Cisco Catalyst 9000 シリーズの Multicast Capability

	9200 9200L	9300 9300L	9400	9500 9500-H	9600
IGMP (v1, v2, v3)	○	○	○	○	○
IGMP snooping (v1, v2, v3)	○	○	○	○	○
MLD (v1, v2)	○	○	○	○	○
MLD snooping (v1, v2)	○	○	○	○	○
PIM-SM	○	○	○	○	○
PIM SSM	○	○	○	○	○
PIM Bi-Dir	×	○*	○*	○*	○*

* 16.12.1以降でサポート

3.4 QoS

QoS

Policing

DTS

WRED

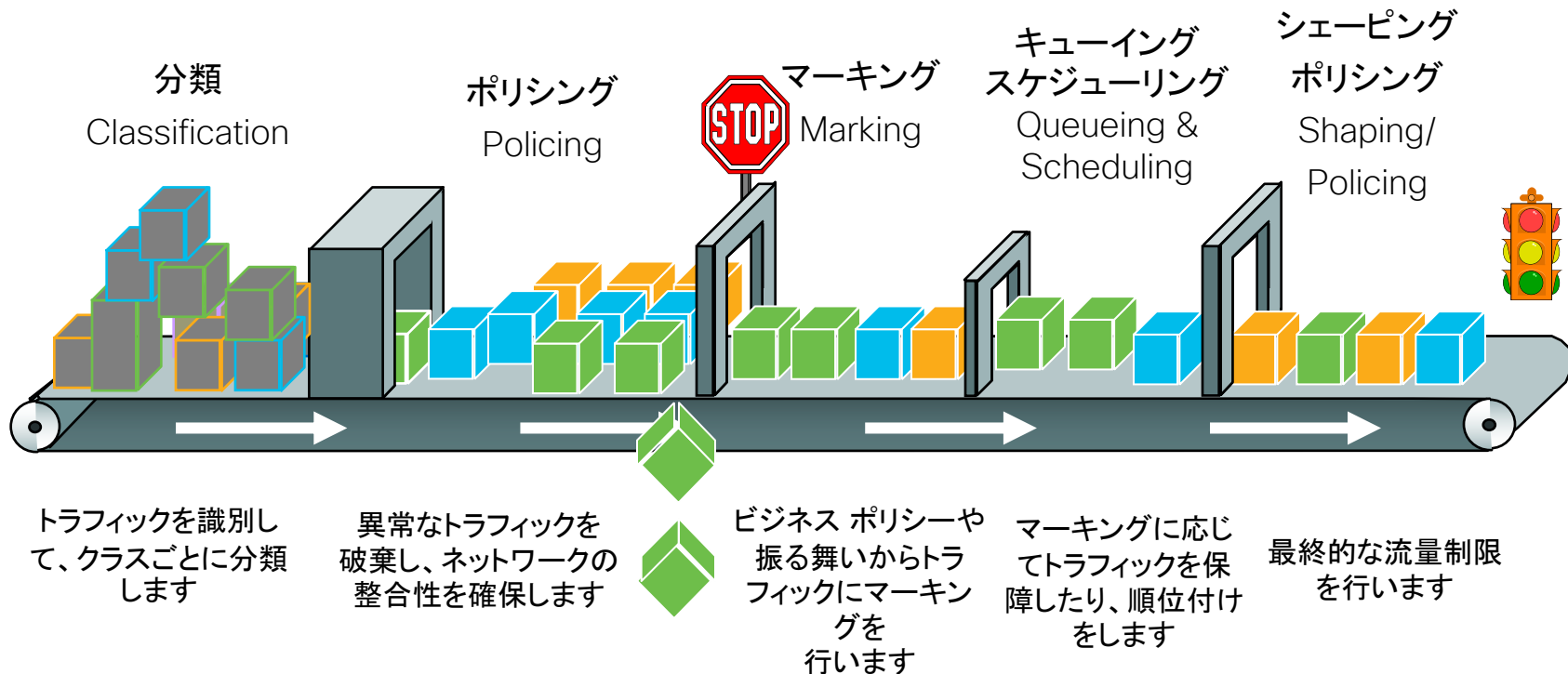
H-QoS

Auto-QoS

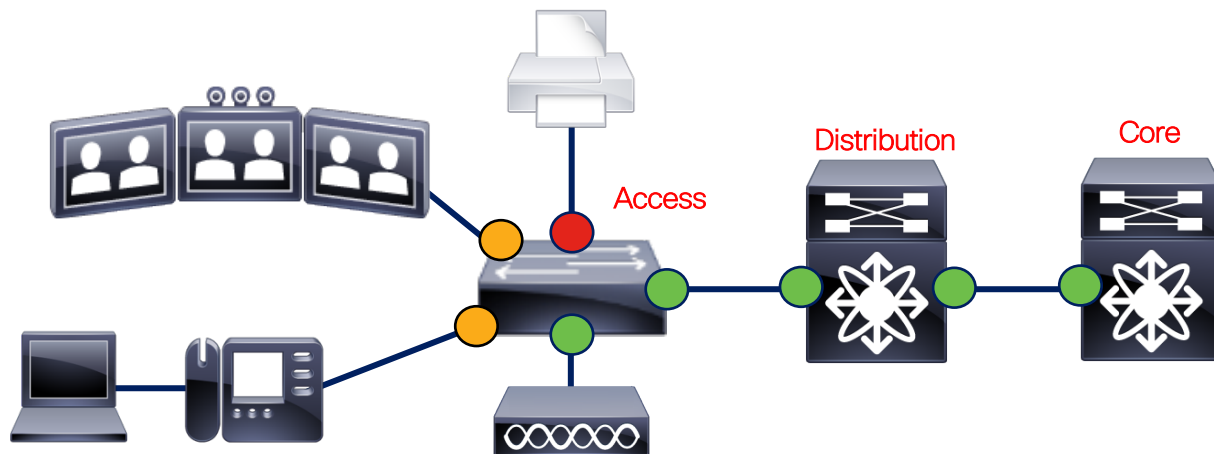
QoS はなぜ必要か

- バーストから重要なトラフィックを守りたい
時々ビデオ会議の画像がブレる / WAN 越しの業務通信で再送が発生している
- 遅延に敏感なアプリケーションを優先させたい
Voice / Video / Collaboration App etc...
- 新しいアプリケーション、業務システムにすぐ対応したい
Campus LAN / DC LAN で柔軟にマーキングで対応。WAN Edge で柔軟に帯域を調整
- とにかく重要なトラフィックの packets を落とさない
(TCP/IP はベスト エフォートを前提と作られた)

QoS の基本シーケンス



各階層における QoS の設定例



信頼されるポート

- パケットのマーキングを信頼する
(Cisco Catalyst 9000 シリーズはデフォルトで)
- キューイング



条件付きで信頼される端末

- Trust-CoS / DSCP コマンドにより、条件付きでマーキングを信頼する
- (オプション) マーキング and / or ポリシング
- キューイング



信頼されない端末:

- ポートは明示的に Untrust に設定する
- (オプション) マーキング and / or ポリシング
- キューイング

Cisco Catalyst 9000 シリーズ QoS 設定イメージ

Modular QoS Command Line Interface (MQC)

Cisco Catalyst 9000 シリーズおよびその他の IOS-XE デバイスでは、共通のスタイルでコンフィグが可能です。

MQC は、以下のコンポーネントから構成されます。

`class-map` — マッチ基準に基づいてフローをクラスとして特定

`policy-map` — クラスごとに実施されるポリシー アクションを特定

`service-policy` — あるインターフェイスのある方向に適用される特定の `policy-map`

■ 特徴

- ASIC が新しくなったため(UADP 2.0, 3.0 etc)、バッファ容量も含めスケールが向上している。
- Cisco Catalyst 2960 との比較すると、QoS のベースが MQC ベースに変更されており、従来の IOS ルータのような操作感で設定が可能

MQC コンポーネント

1. トラフィックの分類

“class-map”

トラフィックを分類し、クラスに適用

```
class-map match-all VOIP
match ip dscp 40
class-map match-all BUS
match ip dscp 32
```

2. QoS ポリシーの定義

“policy-map”

各クラスにポリシーを適用

各クラスごとにトラフィックの処理を定義

```
!
policy-map QoS-POLICY
class VOIP
priority percent 25
class BUS
bandwidth remaining percent 90
```

3. QoS ポリシーを論理および物理インターフェイスに適用

“service-policy”

QoS ポリシー適用先

```
interface g1/0/1
service-policy output DIFFSERV_POLICY
```

マーキング 設定例

条件付き信頼ポート

- Trust Device コマンドを使うことで、特定のデバイスがつけるマーキングだけを信頼可能です。
- ※ 同時に複数のデバイスを信頼できません

```
interface GigabitEthernet 1/0/1
  trust device cisco-phone [or]
  trust device cts         [or]
  trust device ip-camera  [or]
  trust device media-player
```

```
interface GigabitEthernet 1/0/1
  trust device cisco-phone
  service-policy input CISCO-IPPHONE
```

Conditional Trust
(CDPネゴシエーション)

- デバイスが検出されない場合 Untrust モードに移行します。
- アップリンクはデフォルトの Trust 状態で問題ありません。

3.4 QoS

マーキング 設定例

クラスベース Static マーキング

```
(config)#policy-map QoS
(config-pmap)#class Important
(config-pmap-c)#set ?
  cos      Set IEEE 802.1Q/ISL class of service/user priority
  dscp     Set DSCP in IP(v4) and IPv6 packets
  ip       Set IP specific values
  mpls     Set MPLS specific values
  precedence Set precedence in IP(v4) and IPv6 packets
  qos-group Set QoS Group
```

```
policy-map MARKING-POLICY
class VOIP
  set dscp ef
class MULTIMEDIA-CONFERENCING
  set dscp af41
class SIGNALING
  set dscp cs3
class TRANSACTIONAL-DATA
  set dscp af21
class BULK-DATA
  set dscp af11
class SCAVENGER
  set dscp cs1
class default
  set dscp default
```

■ Packet ヘッダのマーキング

- CoS – L2 header
- DSCP – L3 header
- IP Precedence – L3 header
- MPLS – MPLS Label

■ その他のマーキング情報

- QoS-group (Ingress only)

※筐体内でのみ有効

3.4 QoS

マーキング 設定例

Table Map を利用した条件付きマーキング

■ Table Map マーキング (DSCP>COS)

Table Map mapx
from 5 to 0
default copy

!

Policy Map flow
Class flow

set dscp cos table mapx

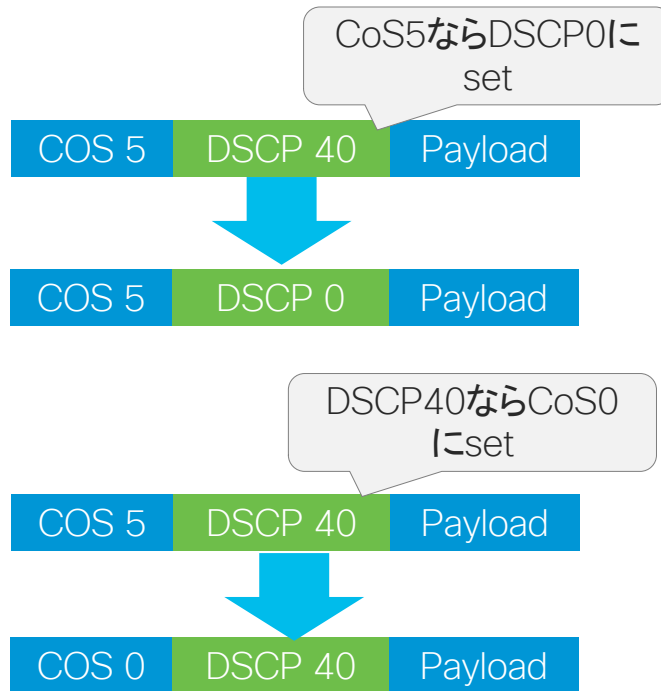
■ Table Map マーキング (COS>DSCP)

Table Map mapx
from 40 to 0
default copy

!

Policy Map flow
Class flow

set cos dscp table mapx



※CoS to CoS や DSCP to DSCP も可能です

パケットの分類 (Classification)

■ 以下のマーキングをもとにパケットを分類

DSCP

CoS - Layer 2

IP Precedence

VLAN

MPLS

QoS-group(内部ラベル)

Class-mapdir flash:

ACL

IPV4 ACL

IPV6 ACL

MAC ACL

```
C9200-2(config-cmap)#match ?
access-group  Access group
cos           IEEE 802.1Q/ISL class of service/user priority values
dscp         Match DSCP in IPv4 and IPv6 packets
group-object  Match object-group
ip           IP specific values
mpls         Multi Protocol Label Switching specific values
precedence   Match Precedence in IPv4 and IPv6 packets
protocol      Protocol
qos-group    Qos-group
vlan         VLANs to match
```

分類 (Classification) 設定例 1

■ ACL ベースの Classification

```
access-list 101 permit ip host 12.4.1.1 host 15.2.1.1
class-map acl-101
description match on access-list 101
match access-group 101
```

■ Layer 2 CoS ベースの Classification

```
class-map cos
match cos 3 4 5
```

■ Layer 3 DSCP ベースの Classification

```
class-map dscp
match dscp af21 af22 af23
```

分類 (Classification) 設定例 2

■ VLAN ID ベースの Classification

```
class-map VWLAN  
  match vlan 110  
class-map DVLAN  
  match vlan 10
```

■ DSCP/Precedence ベースの Classification

```
class-map prec2  
  match ip precedence 2  
class-map ef  
  match ip dscp ef
```

■ 階層型 Classification

```
class-map child  
  match ip precedence 2  
class-map parent  
  match class child
```

分類 (Classification) 設定例 3

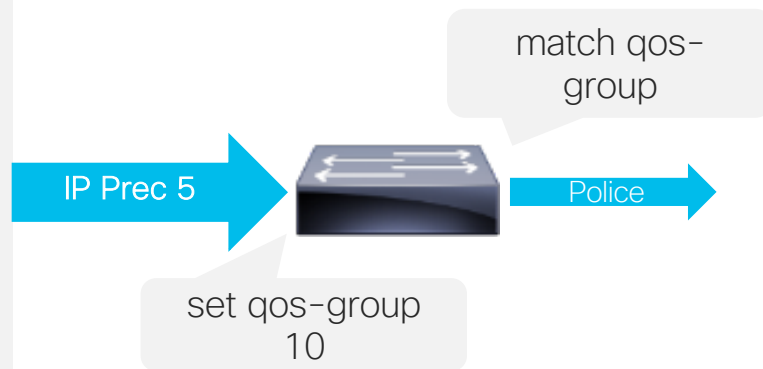
■ QoS Group ベースの Classification

```
class-map voice-interface-1  
match ip precedence 5
```

```
policy-map input-interface-1  
class voice-interface-1  
set qos-group 10
```

```
class-map voice  
match qos-group 10
```

```
policy-map output-interface  
class voice  
police 256000
```

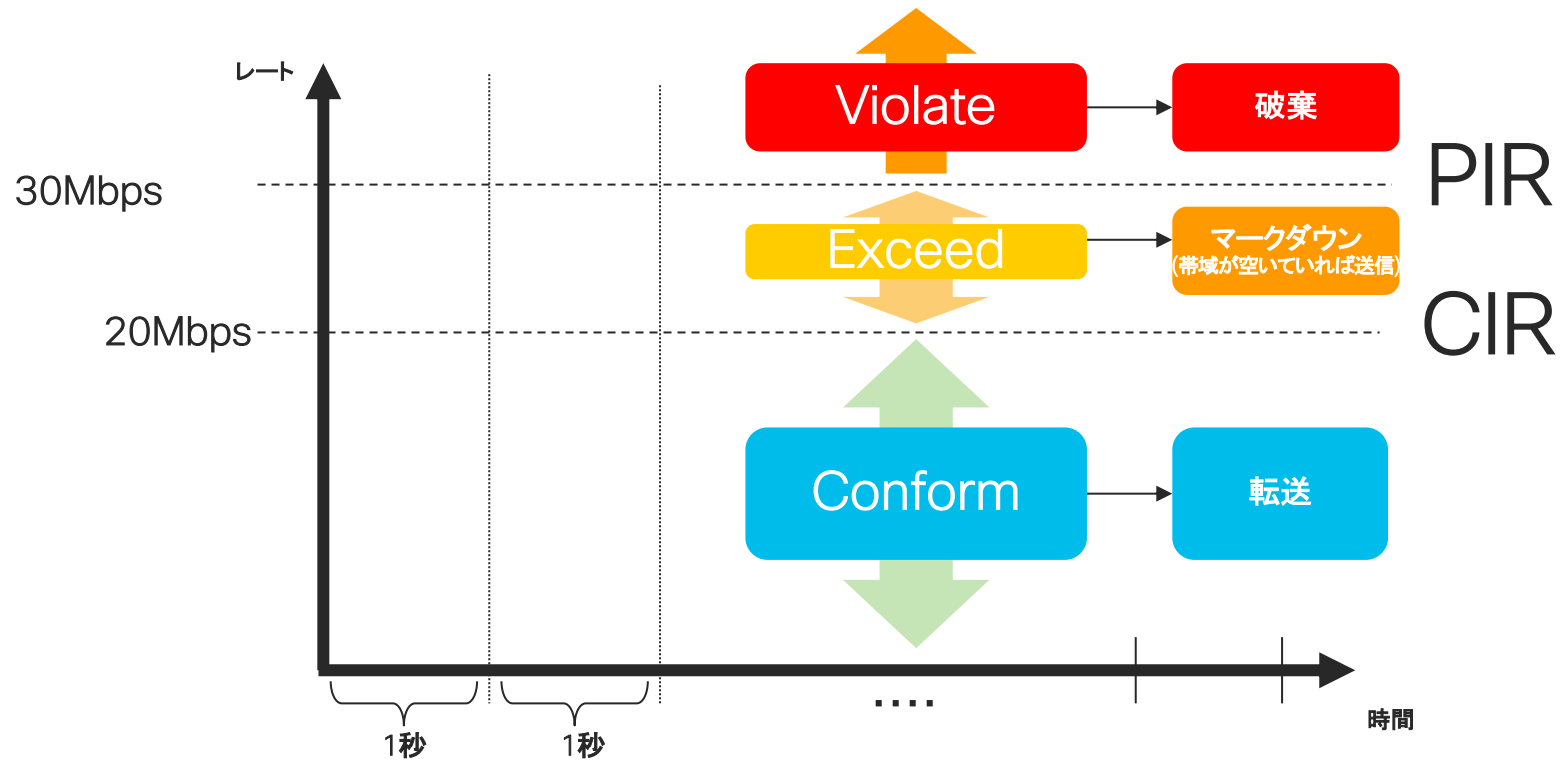


※ QoS グループはデバイス内のみで有効なマーキングです

Cisco Catalyst 9000 シリーズ ポリシングの実装

- ポートや VLAN 上で指定したトラフィックに対して帯域制御、流量確認を行う機能です。
 - 指定した流量を超えた場合は優先度を変更したり、破棄することができます。
- ※ マークダウンは cos2cos、prec2prec、dscp2dscp のみ可能です。
- シングル レートとデュアル レートに対応しています。
- 有線ポートでは、ポリシーごとに最大 63 のポリサーに対応しています。
- Ingress と Egress で利用可能です。

2Rate 3Color ポリシングの概要



3.4 QoS

ポリシング設定例

```
policy-map MARKING&POLICING
class VVLAN-VOIP
set dscp ef
police 128k
  conform-action transmit
  exceed-action drop
class VVLAN-SIGNALING
set dscp cs3
police 32k
  conform-action transmit
  exceed-action drop
class MULTIMEDIA-CONFERENCING
set dscp af41
police 5m
  conform-action transmit
  exceed-action drop
class SIGNALING
set dscp cs3
police 32k
  conform-action transmit
  exceed-action drop
```

...

超過トラフィックは Drop もしくはリマークも可能です

```
...[continued]
class TRANSACTIONAL-DATA
set dscp af21
police 10m
  conform-action transmit
  exceed-action set-dscp-transmit dscp table TABLE-MAP
class BULK-DATA
set dscp af11
police 10m
  conform-action transmit
  exceed-action set-dscp-transmit dscp table TABLE-MAP
class SCAVENGER
set dscp cs1
police 10m
  conform-action transmit
  exceed-action drop
class class-default
set dscp default
police 10m
  conform-action transmit
  exceed-action set-dscp-transmit dscp table TABLE-MAP
```

ポリサー ベースのマークダウン はテーブルマップを使用する場合のみサポートします
※exceed-action set-dscp-transmit af21 など、設定は入るが動作しないので注意が必要です。Table-Mapをご利用ください

table-map TABLE-MAP
map from 0 to 8
map from 10 to 8
map from 18 to 8

Table-map は複数のクラスで利用可能です

ポリシーの詳細情報

```
Switch#sh policy-map interface tenGigabitEthernet1/0/3  
TenGigabitEthernet1/0/3
```

```
Service-policy input: dscp
```

```
Class-map: dscp46 (match-all)
```

```
61531 packets
```

```
Match: dscp ef (46)
```

```
police:
```

```
rate 10 %
```

```
rate 100000000 bps, burst 3125000 bytes
```

```
conformed 61538000 bytes; actions:
```

```
transmit
```

```
exceeded 0 bytes; actions:
```

```
drop
```

```
conformed 1242000 bps, exceeded 0000 bps
```

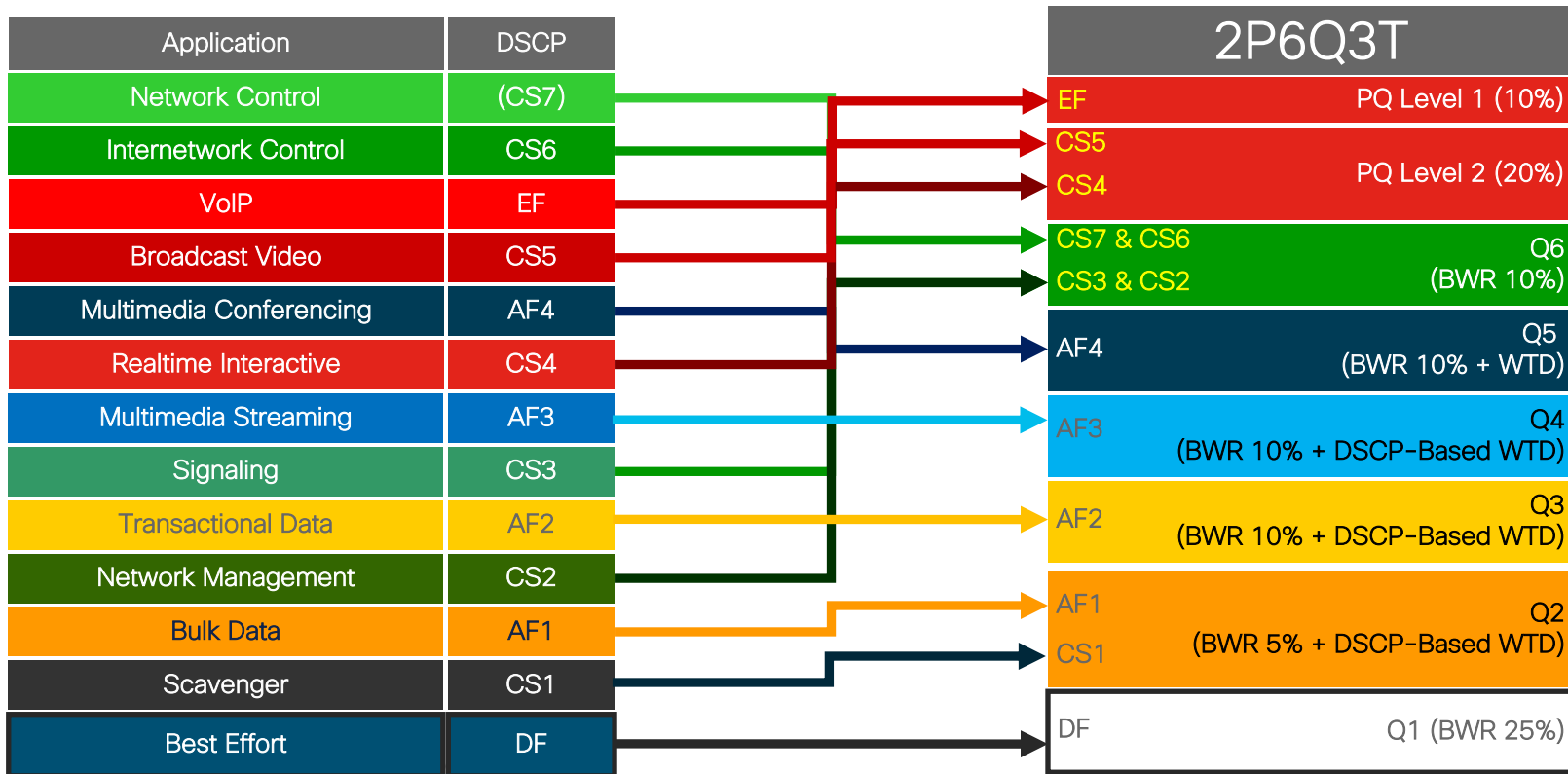
```
Class-map: class-default (match-any)
```

```
5 packets
```

- ポート単位で QoS ポリシーの詳細情報を確認できます。
- Class-map にヒットしたパケットのカウンタや、Conform / Exceed / Violate したパケットのカウンタ確認できます。
- 設定したポリシング レートとバースト レートになっているか、チェックしてください。

Cisco Catalyst 9000 シリーズ 2P6Q3T キューイング モデル

※ Cisco Catalyst 3650/3850 シリーズも同様のモデルを持ちます

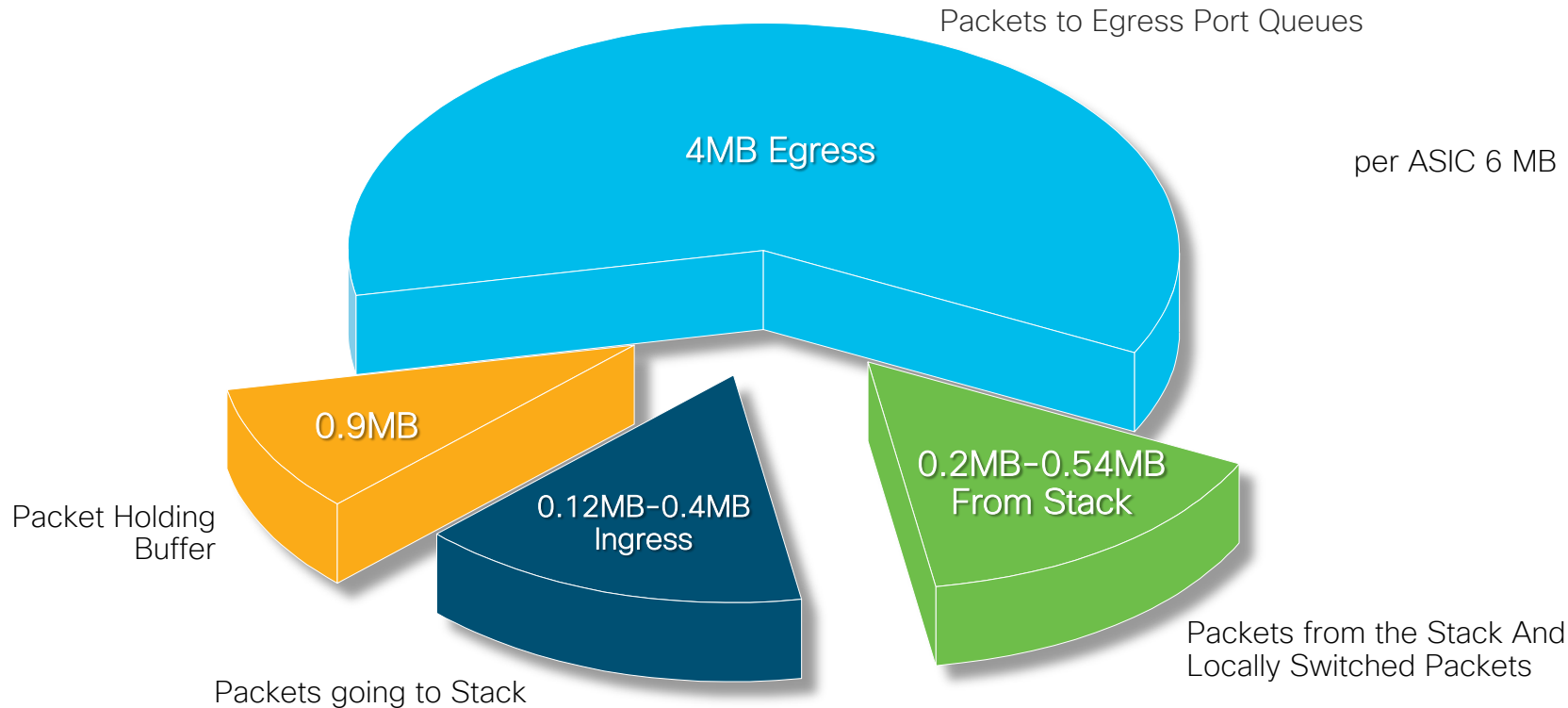


BWR =
Bandwidth
Remaining

WTD =
Weighted
Tail
Drop

Cisco Catalyst 9200 シリーズ

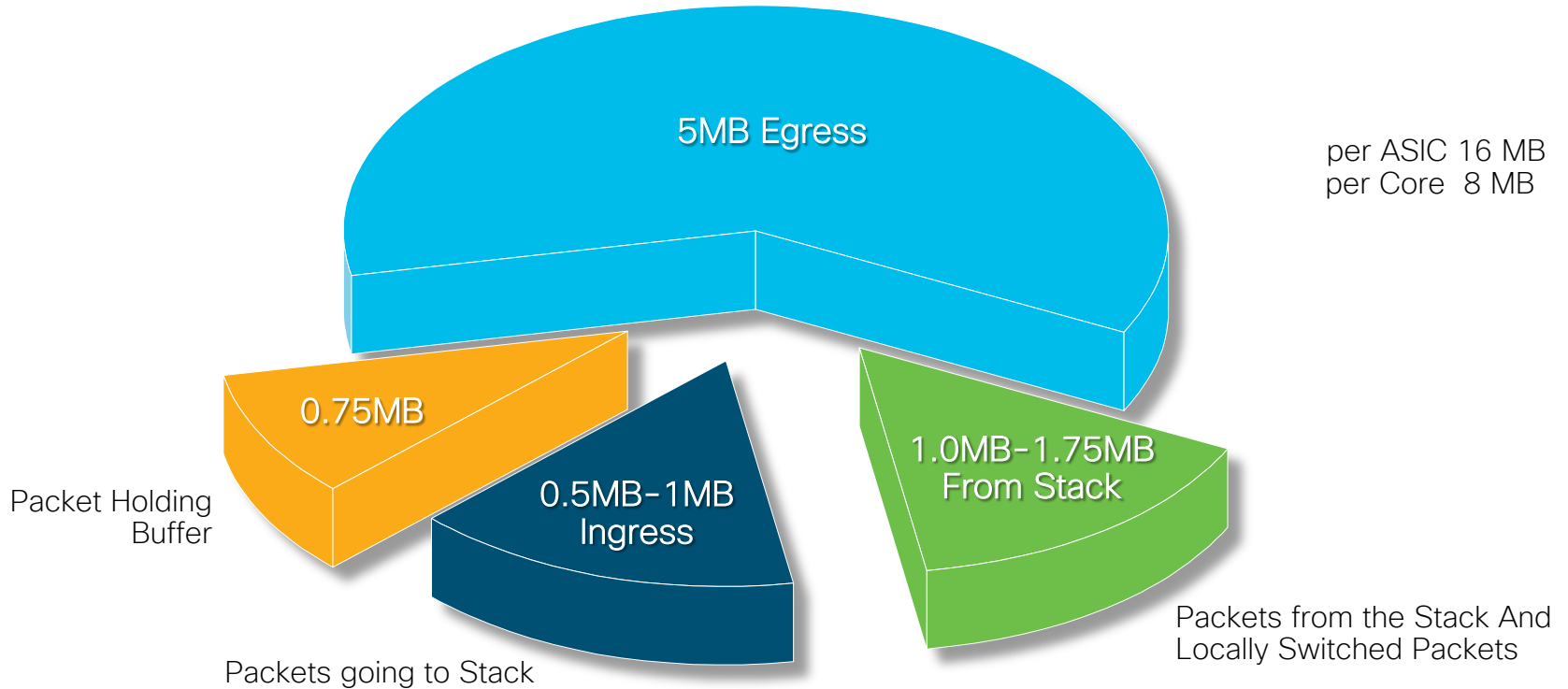
UADP 2.0 Mini バッファ サイズ



Cisco Catalyst 9300 シリーズ

UADP 2.0バッファ サイズ

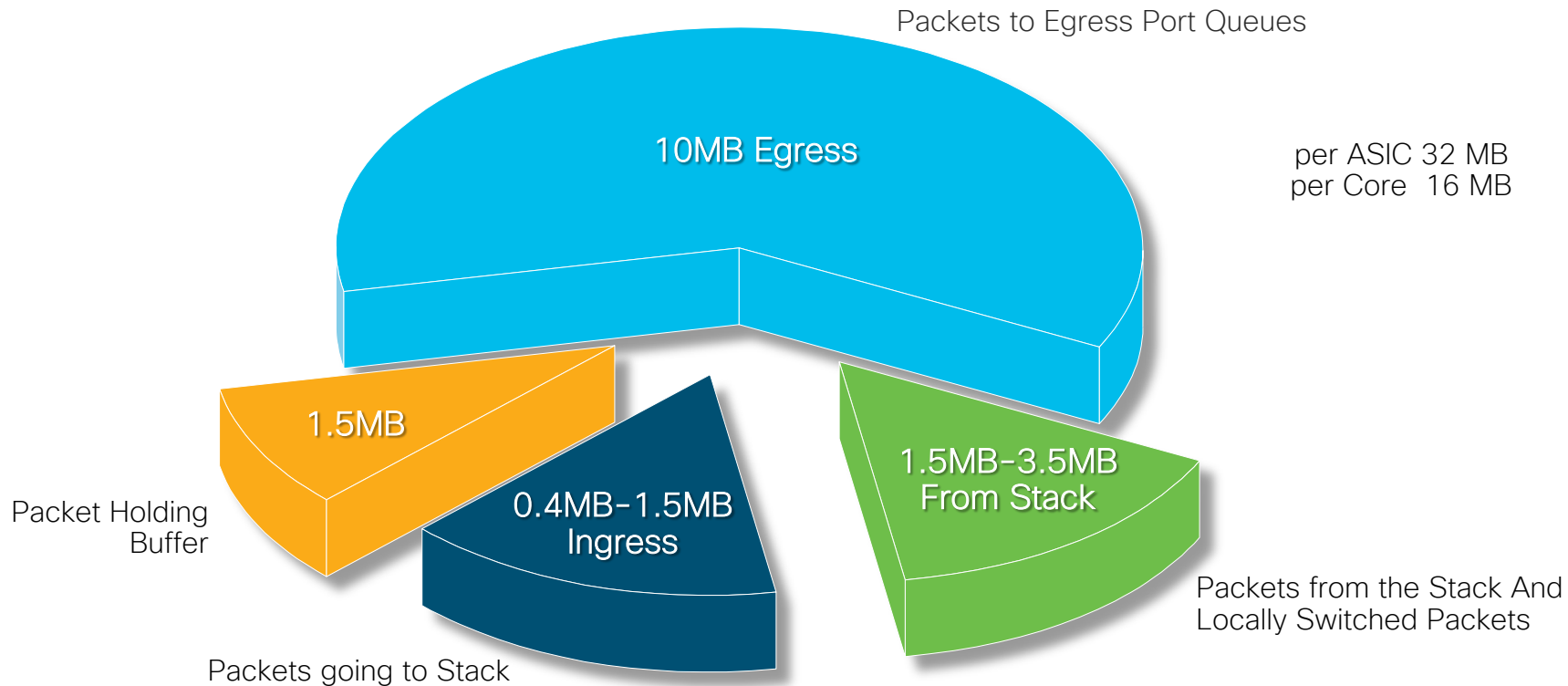
Packets to Egress Port Queues



Cisco Catalyst 9400 / 9500 シリーズ

UADP 2.0 XL バッファ サイズ

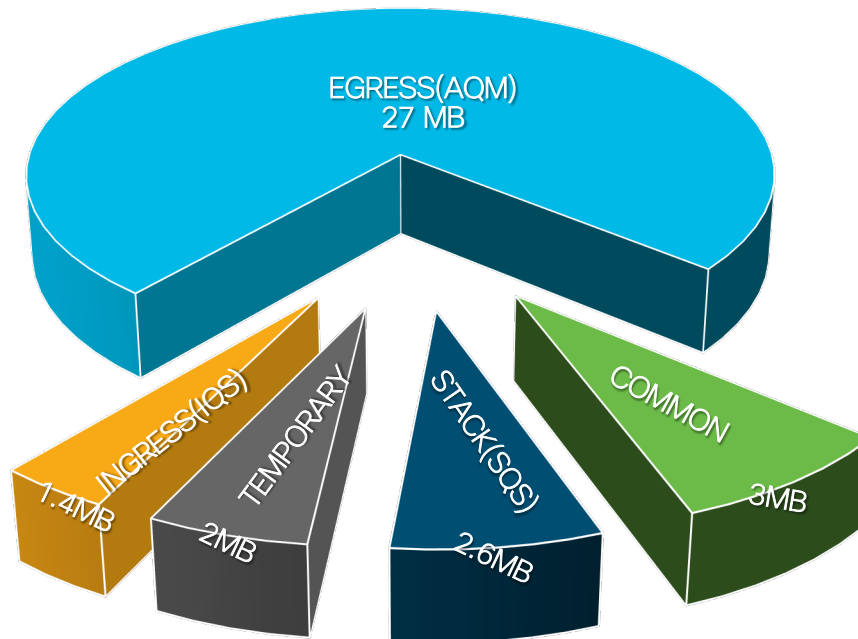
Packets to Egress Port Queues



Cisco Catalyst 9500-H

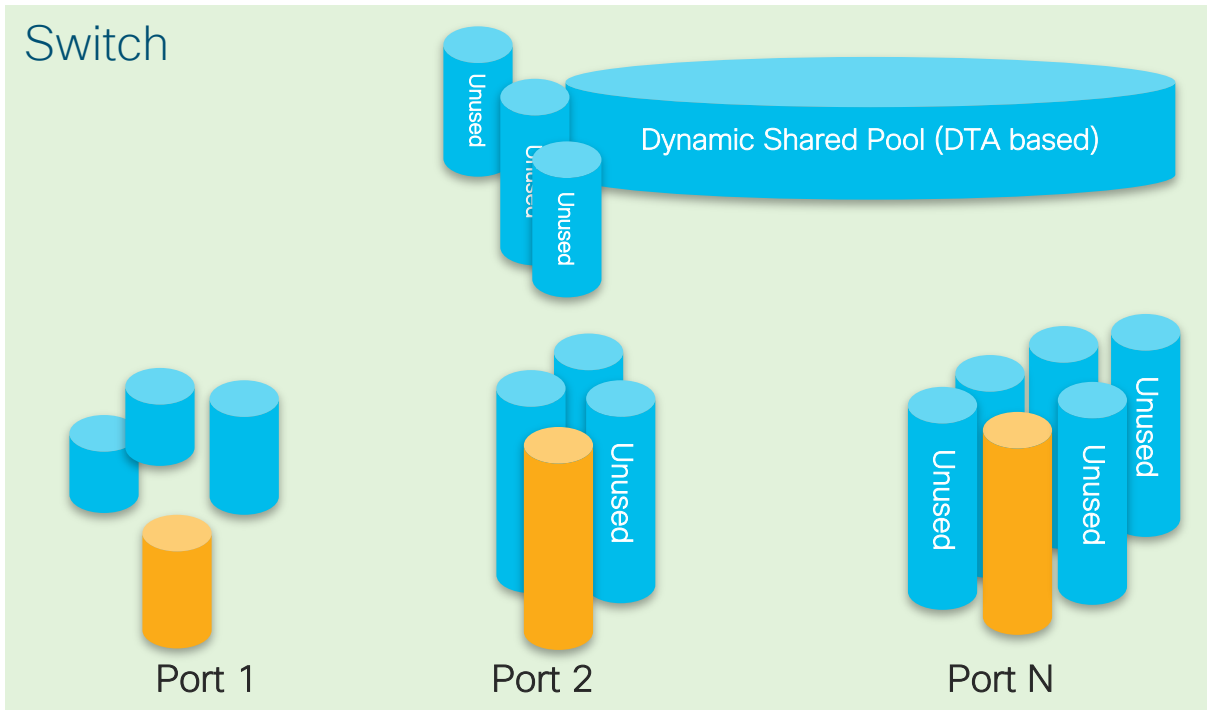
UADP 3.0 バッファ サイズ

- 計36MBの単一バッファを入出力データで共有



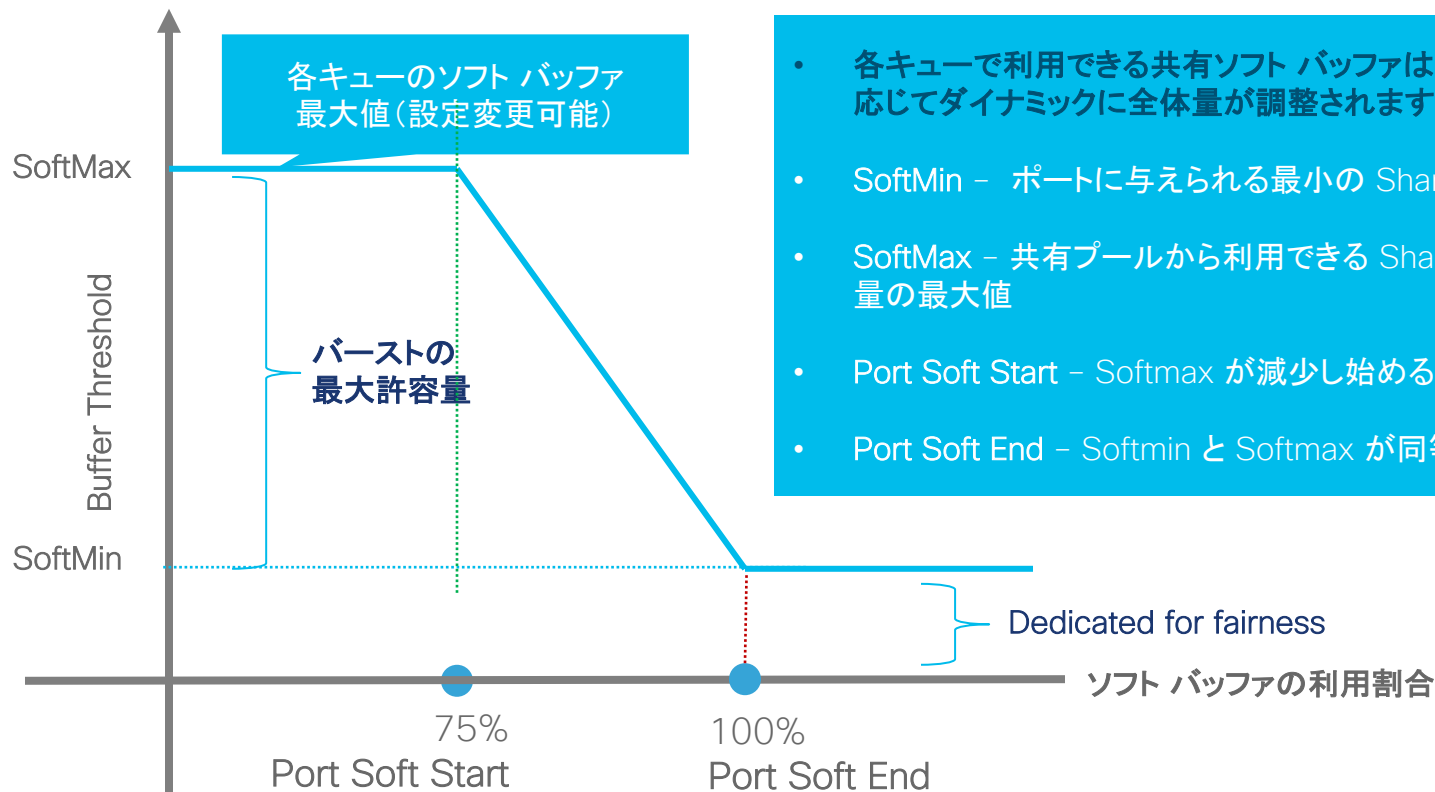
バッファ割り当ての自動調整

Dynamic Threshold and Scaling(DTS)



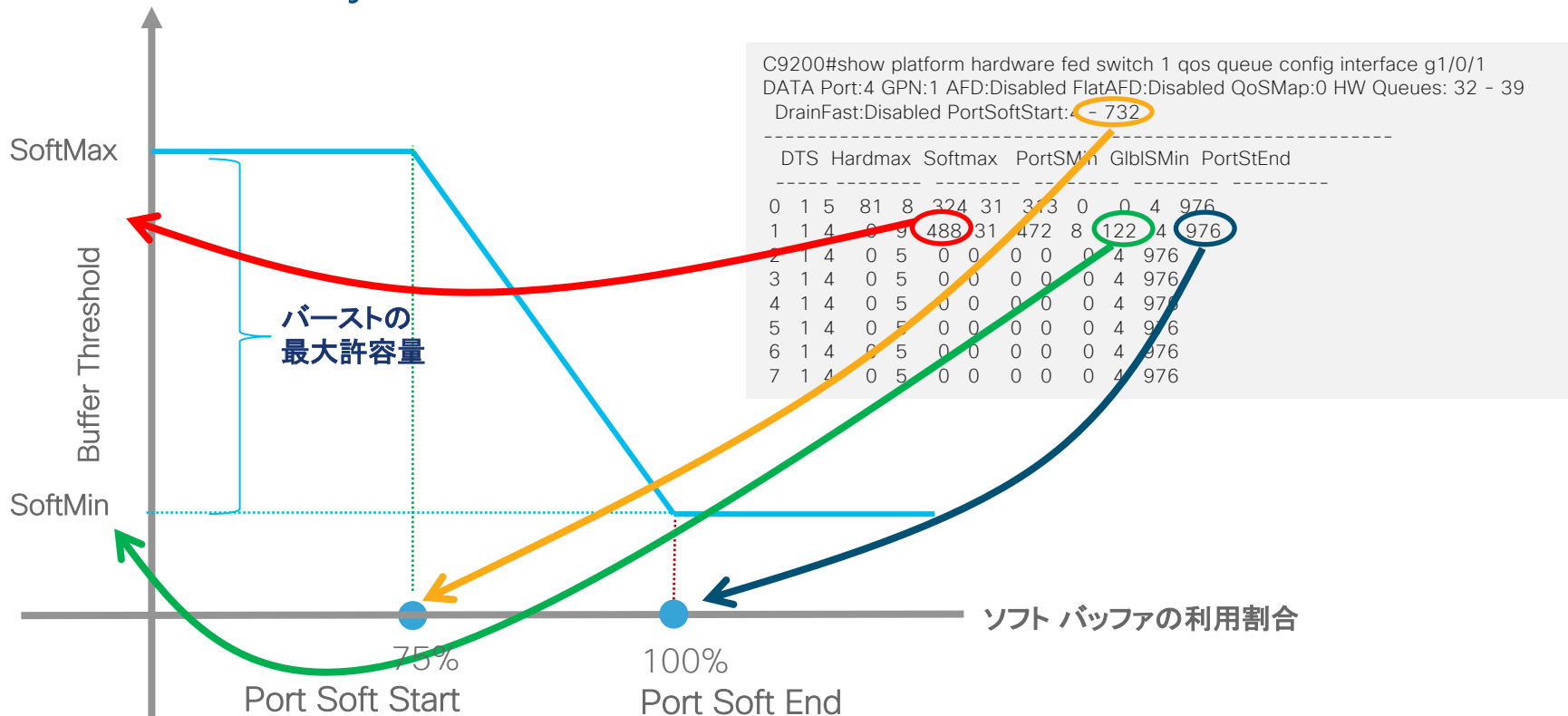
- バッファ リソースを公平かつ効率的に割り当てる機能として、DTS というアルゴリズムが自動で適用されます。
- 輻輳が発生すると、グローバル / ポート リソースの占有に基づいて、着信データに共有バッファ (ソフトバッファ) が柔軟に割り当てられます。
- 共有バッファの最大値はグローバル設定変更で拡張可能です。(後述)

DTS の用語と仕組み



- 各キューで利用できる共有ソフト バッファはその利用量に応じてダイナミックに全体量が調整されます
- SoftMin - ポートに与えられる最小の Shared バッファ
- SoftMax - 共有プールから利用できる Shared バッファ容量の最大値
- Port Soft Start - Softmax が減少し始める瞬間
- Port Soft End - Softmin と Softmax が同等になる瞬間

Cisco Catalyst 9200 シリーズ デフォルト状態での DTS



Queueing 設定イメージ

■ WTD Thresholds

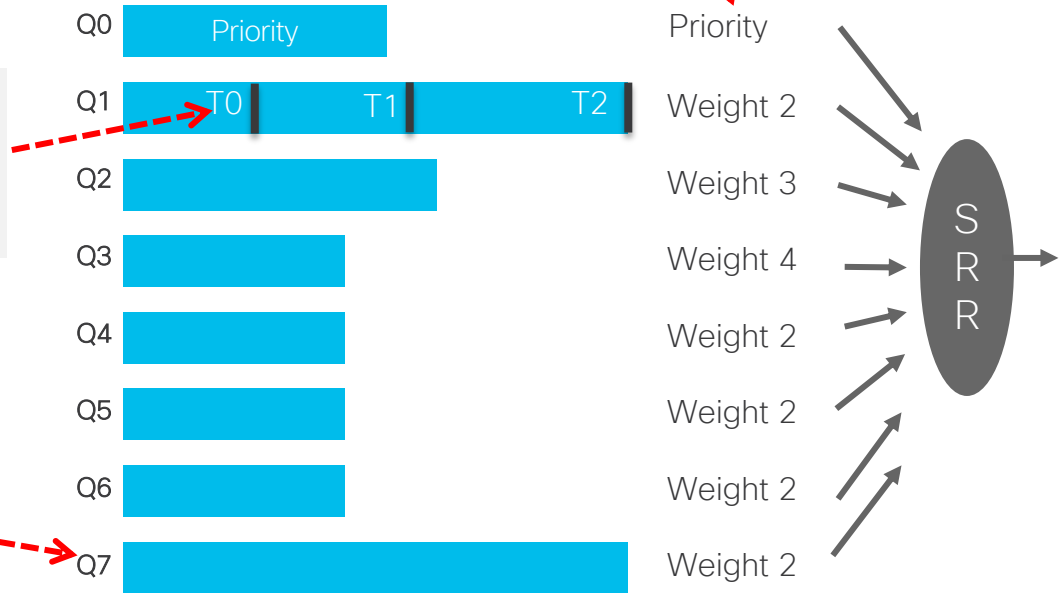
```
(config)#policy-map QoS
(config-pmap)#class Important
(config-pmap-c)#?
queue-limit cos/dscp <value> percent
```

■ Queue size

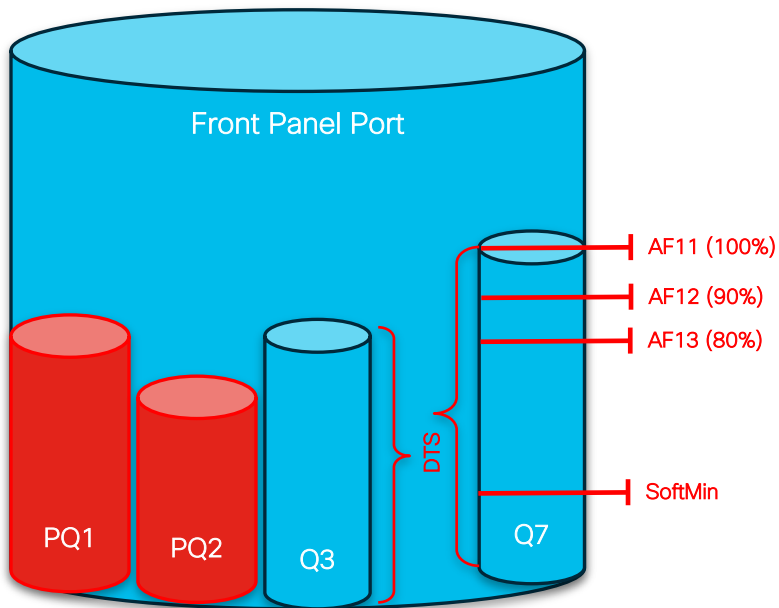
```
(config)#policy-map QoS
(config-pmap)#class Important
(config-pmap-c)#?
queue-buffers ratio XXX
```

■ Weight

```
(config)#policy-map QoS
(config-pmap)#class Important
(config-pmap-c)#?
priority XXX
bandwidth XXX
shape XXX
```



Queueing 設定例



```

policy-map 2P6Q3T
  class PRIORITY-QUEUE
    priority level 1
    police rate percent 10
  class VIDEO-PRIORITY-QUEUE
    priority level 2
    police rate percent 20
  class DATA-QUEUE
    bandwidth remaining percent <number>
    queue-buffers ratio <number>
    queue-limit dscp values af13 cs1 percent 80
    queue-limit dscp values af12 percent 90
    queue-limit dscp values af11 percent 100
  class class-default

interface <type> <index>
  service-policy output 2P6Q3T
  
```

PQ1 を定義

PQ2 を定義

Buffer Size を調整

WTD の閾値を指定

Queue - Buffers Ratio

キュー サイズの指定

- 各キューに割り当てるバッファ量を設定できます。
- ポリシー内で `queue-buffer ratio <=100%` に設定する必要があります。
- 100% 未満で設定した場合、残りのバッファは各キューに均等に割り当てられます。
- Non-PQ で 100% 全て占有すると重要なトラフィックをドロップする可能性があるため注意が必要です。
- 有線ポート / 無線ポート共にサポートしています。
- クラス内部に "bandwidth", "Shape", "priority" の設定が必須です。

■ Queue size

```
policy-map 2P6Q3T
class PRIORITY-QUEUE
  queue-buffers ratio 5
class VIDEO-PRIORITY-QUEUE
  queue-buffers ratio 10
class DATA-QUEUE
  queue-buffers ratio 35
class class-default
  queue-buffers ratio 45
->Total is 5 + 10 + 35 + 45 = 100 %
```

3.4 QoS

Queue - Limit

Weighted Tail Drop (WTD)

WTD はフレーム内の QoS ラベルを使用してそれぞれ異なる閾値を適用できます。

各キューで DSCP、COS に応じて 3 つまで閾値を指定できます。*閾値が1~2個の場合後述

ソフトバッファを考慮し、割り当てられたバッファサイズの 4 倍に閾値が設定されます。

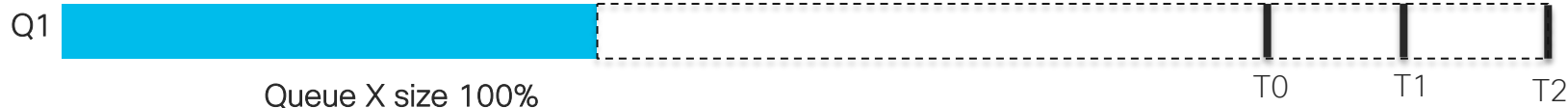
■ WTD Thresholds

```
Policy-map port_queue_threshold
Class dscp-1-2-3-4 (20,90,100)
Bandwidth percent 20
Queue-limit dscp 1 percent 80
Queue-limit dscp 2 percent 80
Queue-limit dscp 3 percent 90
Queue-limit dscp 4 percent 100
```

T_2 (400% of 100% X queue size)

T_1 (90% of T_2)

T_0 (80% of T_2)



Queue - Limit

Weighted Tail Drop (WTD)

Cisco Catalyst 9000 シリーズは WTD Threshold の数が 1 つ、または 2 つの時に以下のように動作します。

■ 2つの閾値を設定した例

```
Policy-map port_queue_threshold
Class dscp-1-2-3
  Bandwidth percent 20
  Queue-limit dscp 1 percent X
  Queue-limit dscp 2 percent X
  Queue-limit dscp 3 percent Y
```

$T2$ (400% of 100% queue size)

$T1$ (Y% of $T2$)

$T0$ (X% of $T2$)

■ 単一の閾値を設定した例

```
Policy-map port_queue_threshold
Class dscp-1-2
  Bandwidth percent 20
  Queue-limit dscp 1 percent Z
  Queue-limit dscp 2 percent Z
```

- $Z \geq 90\%$

$T2$ (400%)

$T1$ (Z% of $T2$)

$T0$ (80% of $T2$)

- $Z < 90\%$

$T2$ (400%)

$T1$ (90% of $T2$)

$T0$ (Z% of $T2$)

初期状態のキュー

- デフォルトは Q0 と Q1 の 2 つのキューが動作します。
 - Q0: コントロールパケットを処理
 - Q1: データパケットを処理

Q0 は 81 のハードバッファを占有し
ソフトバッファが最大 $81 \times 4 = 324$ 割り当てられます

Q1 はハードバッファを持たず
ソフトバッファが 122 割り当てられます
最大ソフトバッファは $122 \times 4 = 488$

Q0T2: $81 + 324 = 405$
(Hardmax + Softmax)

Q1T2: 488(Softmax)

```
C9200#show platform hardware fed switch 1 qos queue config interface g1/0/1
DATA Port:4 GPN:1 AFD:Disabled FlatAFD:Disabled QoSMap:0 HW Queues: 32 - 39
DrainFast:Disabled PortSoftStart:4 - 732
```

	DTS	Hardmax	Softmax	PortSMin	GlblSMin	PortStEnd	-----				
0	1	5	81	8	324	31	313	0	0	4	976
1	1	4	0	9	488	31	472	8	122	4	976
2	1	4	0	5	0	0	0	0	0	4	976
3	1	4	0	5	0	0	0	0	0	4	976
4	1	4	0	5	0	0	0	0	0	4	976
5	1	4	0	5	0	0	0	0	0	4	976
6	1	4	0	5	0	0	0	0	0	4	976
7	1	4	0	5	0	0	0	0	0	4	976

Priority	Shaped/shared	weight	shaping_step	sharpedWeight							

0	0	Shared	50	0	0						
1	0	Shared	75	0	0						
2	0	Shared	10000	0	0						
3	0	Shared	10000	0	0						
4	0	Shared	10000	0	0						
5	0	Shared	10000	0	0						
6	0	Shared	10000	0	0						
7	0	Shared	10000	0	0						

	Weight0	Max_Th0	Min_Th0	Weight1	Max_Th1	Min_Th1	Weight2	Max_Th2	Min_Th2		

0	0	322	0	0	360	0	0	405	0		
1	0	388	0	0	434	0	0	488	0		
2	0	0	0	0	0	0	0	0	0		
3	0	0	0	0	0	0	0	0	0		
4	0	0	0	0	0	0	0	0	0		
5	0	0	0	0	0	0	0	0	0		
6	0	0	0	0	0	0	0	0	0		
7	0	0	0	0	0	0	0	0	0		

Softmax Buffer の拡張

qos queue-softmax-multiplier <100 - 1200>

PQ1 以外のキューが利用できるソフト バッファの最大値を拡張できます(デフォルト値は100%)

■ Default

```
C9200#show platform hardware fed switch 1 qos queue config interface g1/0/1
DATA Port:4 GPN:1 AFD:Disabled FlatAFD:Disabled QoSMap:0 HW Queues: 32 - 39
DrainFast:Disabled PortSoftStart:3 - 732
```

```
-----
DTS Hardmax Softmax PortSMin GblSMin PortStEnd
-----
```

```
0 1 5 81 7 324 31 313 0 0 3 976
1 1 4 0 8 488 31 472 8 122 3 976
2 1 4 0 5 0 0 0 0 0 3 976
3 1 4 0 5 0 0 0 0 0 3 976
4 1 4 0 5 0 0 0 0 0 3 976
5 1 4 0 5 0 0 0 0 0 3 976
6 1 4 0 5 0 0 0 0 0 3 976
7 1 4 0 5 0 0 0 0 0 3 976
```

```
-----
Weight0 Max_Th0 Min_Th0 Weigh1 Max_Th1 Min_Th1 Weight2 Max_Th2 Min_Th2
-----
```

```
0 0 322 0 0 360 0 0 405 0
1 0 388 0 0 434 0 0 488 0
2 0 0 0 0 0 0 0 0 0
3 0 0 0 0 0 0 0 0 0
4 0 0 0 0 0 0 0 0 0
5 0 0 0 0 0 0 0 0 0
6 0 0 0 0 0 0 0 0 0
7 0 0 0 0 0 0 0 0 0
```

■ 1000%

```
C9200#show platform hardware fed switch 1 qos queue config interface g1/0/1
DATA Port:4 GPN:1 AFD:Disabled FlatAFD:Disabled QoSMap:0 HW Queues: 32 - 39
DrainFast:Disabled PortSoftStart:2 - 7320
```

```
-----
DTS Hardmax Softmax PortSMin GblSMin PortStEnd
-----
```

```
0 1 5 81 6 3240 3 303 0 0 5 9760
1 1 4 0 11 4880 3 457 1 152 5 9760
2 1 4 0 5 0 0 0 0 0 5 9760
3 1 4 0 5 0 0 0 0 0 5 9760
4 1 4 0 5 0 0 0 0 0 5 9760
5 1 4 0 5 0 0 0 0 0 5 9760
6 1 4 0 5 0 0 0 0 0 5 9760
7 1 4 0 5 0 0 0 0 0 5 9760
```

```
-----
Weight0 Max_Th0 Min_Th0 Weigh1 Max_Th1 Min_Th1 Weight2 Max_Th2 Min_Th2
-----
```

```
0 0 2646 0 0 2957 0 0 3321 0
1 0 3888 0 0 4346 0 0 4880 0
2 0 0 0 0 0 0 0 0 0
3 0 0 0 0 0 0 0 0 0
4 0 0 0 0 0 0 0 0 0
5 0 0 0 0 0 0 0 0 0
6 0 0 0 0 0 0 0 0 0
7 0 0 0 0 0 0 0 0 0
```

3.4 QoS

サンプルポリシー設定後のキュー

```

policy-map p1
class AutoQos-4.0-Output-Priority-Queue
priority level 1 percent 30
class AutoQos-4.0-Output-Control-Mgmt-Queue
bandwidth percent 10
queue-buffers ratio 10
queue-limit dscp cs2 percent 80
queue-limit dscp cs3 percent 90
queue-limit dscp cs6 percent 90
queue-limit dscp cs7 percent 100
class AutoQos-4.0-Output-Trans-Data-Queue
bandwidth percent 25
queue-buffers ratio 40
class AutoQos-4.0-Output-Multimedia-Strm-Queue
bandwidth percent 10
queue-buffers ratio 10
class class-default
bandwidth percent 25
queue-buffers ratio 25
!
class-Map match-any AutoQos-4.0-Output-Priority-Queue
Match dscp cs4 cs5 ef
Match cos 5
class-Map match-any AutoQos-4.0-Output-Control-Mgmt-Queue
Match dscp cs2 cs3 cs6 cs7
Match cos 3
class-Map match-any AutoQos-4.0-Output-Trans-Data-Queue
Match dscp af21 af22 af23
Match cos 2
class-Map match-any AutoQos-4.0-Output-Multimedia-Strm-Queue
Match dscp af31 af32 af33
    
```

```

C9200#sh platform hardware fed switch 1 qos queue config interface g1/0/1
DATA Port:4 GPN:1 AFD:Disabled FlatAFD:Disabled QoSMap:0 HW
DrainFast:Disabled PortSoftStart:3 - 486
    
```

DTS Hardmax Softmax PortSMIn GblsMin PortStEnd

0	1	7	30	7	30	0	0	0	0	3	648
1	1	4	0	11	78	32	78	8	19	3	648
2	1	4	0	8	324	31	313	8	81	3	648
3	1	4	0	12	80	31	77	8	20	3	648
4	1	4	0	13	204	31	197	8	51	3	648
5	1	4	0	5	0	0	0	0	0	3	648
6	1	4	0	5	0	0	0	0	0	3	648
7	1	4	0	5	0	0	0	0	0	3	648

Priority Shaped/shared weight shaping_step sharpedWeight

0	1	Shaped	850	255	0
1	7	Shared	125	0	0
2	7	Shared	50	0	0
3	7	Shared	125	0	0
4	7	Shared	50	0	0
5	0	Shared	10000	0	0
6	0	Shared	10000	0	0
7	0	Shared	10000	0	0

Weight0 Max_Th0 Min_Th0 Weigh1 Max_Th1 Min_Th1 Weight2 Max_Th2 Min_Th2

0	0	47	0	0	53	0	0	60	0
1	0	62	0	0	69	0	0	78	0
2	0	258	0	0	288	0	0	324	0
3	0	63	0	0	71	0	0	80	0
4	0	162	0	0	181	0	0	204	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0

SoftMax = GblsMin*4

GblsMin=SoftMin

Buffer Ratio 10

Buffer Ratio 40

Buffer Ratio 25

Q0T2 = 30+30

Q1T2 = 78(Softmax)
 Q1T1 = 78*90%
 Q1T0 = 78*80%

3.4 QoS

キューイングトラブルシュート

Label を下の表からマーキングやヘッダ情報に変換し、Queue と Threshold のマッピングを確認できます。

```
show platform hardware fed switch active qos queue label2qmap qmap-egress-data interface <port>
```

Egress DATA Queue Mapping - Asic/Core/Port: 0/0/5

Label	Q	Threshold	VQ	Label	Q	Threshold	VQ	Label	Q	Threshold	VQ
0	1	2	0	1	1	2	0	2	1	2	0
3	1	2	0	4	1	2	0	5	1	2	0
6	1	2	0	7	1	2	0	8	1	2	0
9	1	2	0	10	1	2	0	11	1	2	0
12	1	2	0	13	1	2	0	14	1	2	0

Label Range	Packet Value Reading	Calculate
1 - 64	DSCP	Label - 1 = DSCP
65 - 72	CoS	Label - 65 = CoS
73 - 80	UP Wireless	Label - 73 = UP W
81 - 88	IP Precedence	Label - 81 = IP Prec
89 - 96	MPLS EXP	Label - 89 = EXP
97 - 127	QoS Group	Label - 97 = QoS Grp
128-129	Control	Internal
130 - 133	CPP	Control Policing
0, 134 and above	Not Used	Internal

輻輳回避アルゴリズム

■ Tail Drop (TD)

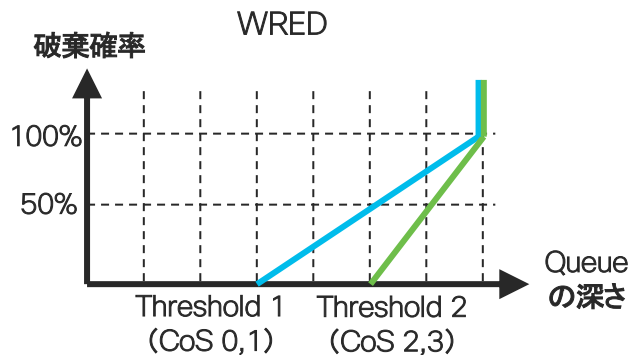
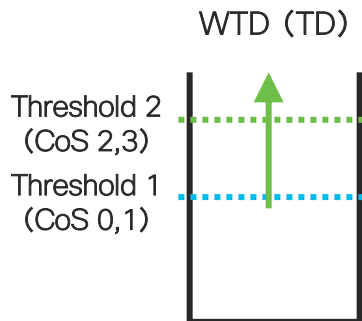
Queue を溢れたものから破棄します。

■ Weighted Tail Drop (WTD)

1 つの Queue の中で優先度ごとに複数の Threshold (しきい値) を決め、それぞれの Threshold を超えたものから破棄します。

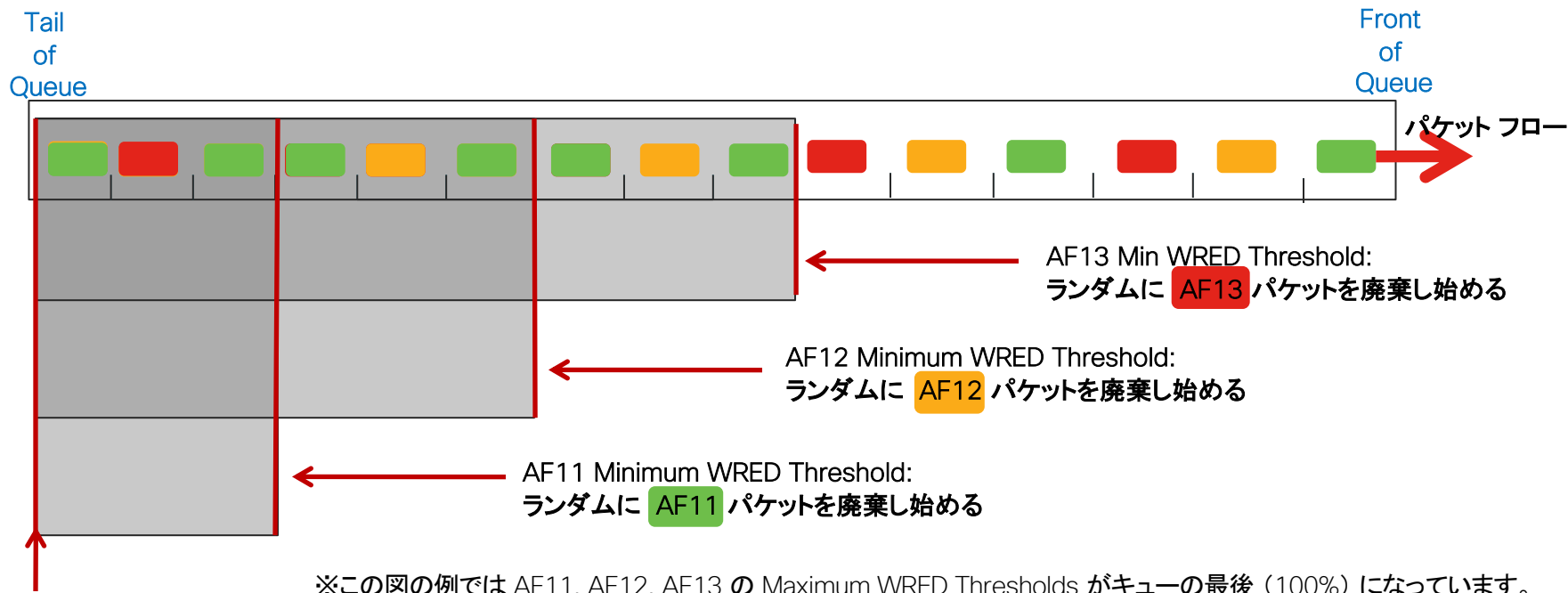
■ Weighted Random Early Detection (WRED)

1 つの Queue の中で優先度ごとに複数の Threshold (しきい値) を決め、それぞれの Threshold によりランダムにパケットを破棄します。

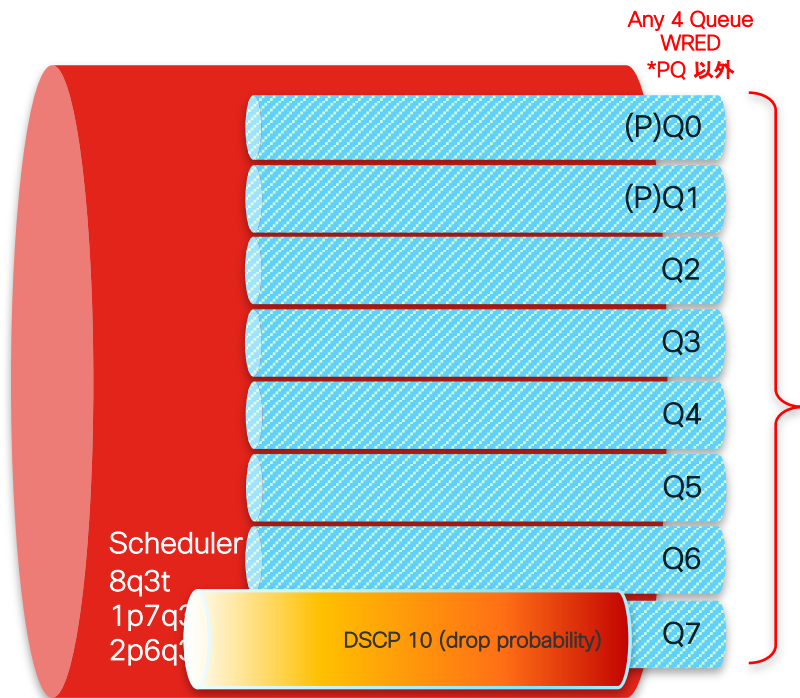


WRED の動作

優先度ベースでパケットをランダムにドロップすることで、TCP アプリを実行するホストに対して再送を促し、輻輳回避を実現する機能です。



Cisco Catalyst 9200 シリーズ WRED 設定例



```

policy-map 2P6Q3T
  class PRIORITY-QUEUE
    priority level 1
  class VIDEO-PRIORITY-QUEUE
    priority level 2
  class DATA-QUEUE
    bandwidth remaining percent <number>
    queue-buffers ratio <number>
    random-detect dscp-based
    random-detect dscp af21 percent 60 80
  
```

PQ は WRED 設定不可

DSCP ベースの WRED 有効化

DSCP AF21 の WRED Threshold を Min60%、Max80に設定

階層型 QoS (H-QoS)

複数のポリシー レベルで QoS 動作を指定して、より細かい粒度でのトラフィック管理を可能にします。

2 レベル入れ子構造のトラフィックポリシーを作成しインターフェイスに適用します。

Classification/Marking

Policing

Shaping

親クラスでポリシングを指定した場合、子クラスでキューイング (priority/BW/Shaping) はできません。

親クラスでのポリシング時は子クラスでマーキング アクションのみサポート。

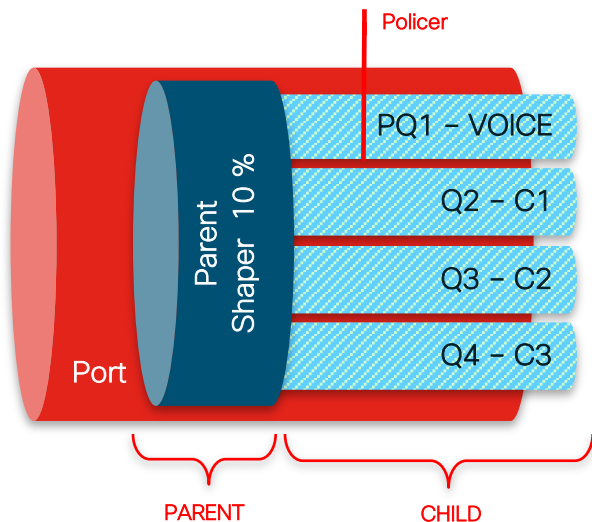
同じ QoS アクションは親クラスと子クラスで指定できません(ただし Shaping を除く)

2 クラスシェーピングをする場合、親クラスではその他のアクションは指定できない。

WRED は子ポリシーで指定可能 (親ポリシーでは指定不可)

H-QoS ユースケース

2 レベル帯域制限 (ポートシェーパ)



```
policy-map PARENT
  class class-default
    shape average percent 10
    service-policy CHILD
```

```
policy-map CHILD
  class VOICE
    priority level 1
    police rate percent 20

  class C1
    bandwidth remaining percent 10

  class C2
    bandwidth remaining percent 20

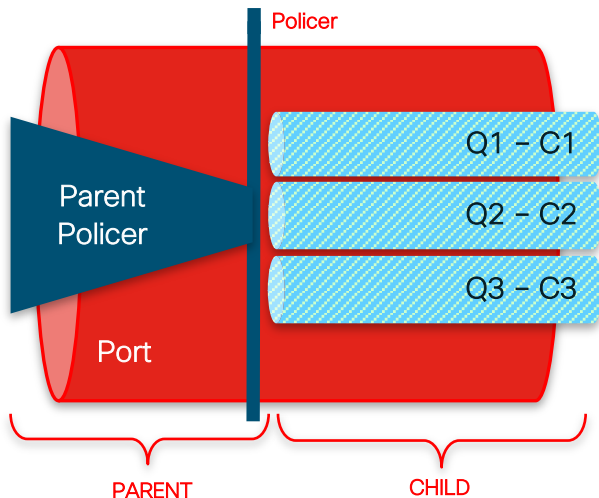
  class C3
    bandwidth remaining percent 70
```

子クラスで Voice クラス
を PQ1 に

- 親クラスで 10% に絞り、子クラスにて Rate 20% で PQ をポリシングします。
- 子クラスでは 1 または 2 の Priority Queue を指定可能。
- 親クラスでのシェーピングは Class-Default のみが実施します。

H-QoS ユースケース

集約ポリシング



```
policy-map PARENT
  class class-default
    police cir percent 30
    service-policy CHILD
```

親ポリサー

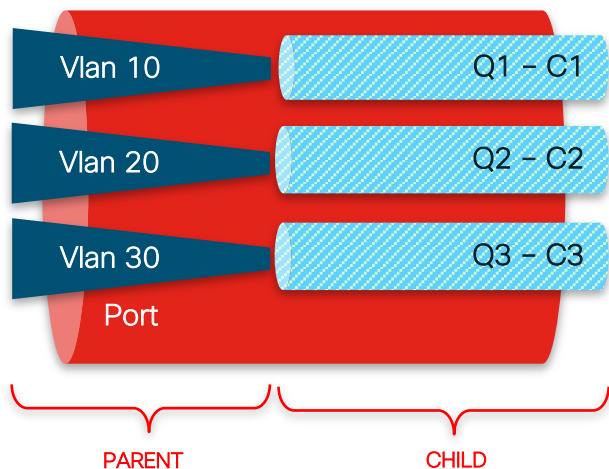
```
policy-map CHILD
  class C1
    set dscp 10
  class C2
    set dscp 20
  class C3
    set dscp 30
```

親ポリシーがポリシングの場合 set のみサポート
されます。子ポリシーでの 2 レベル ポリシングは不可

※ Table-Map を使った条件付きマーキングも可能です

H-QoS ユースケース

Per VLAN ポリシング&マーキング



```
policy-map PARENT
  class vlan10
    police rate percent 10
    service-policy CHILD
  class vlan20
    police rate percent 20
    service-policy CHILD
  class vlan30
    police rate percent 30
    service-policy CHILD

policy-map CHILD
  class C1
    set dscp 10
```

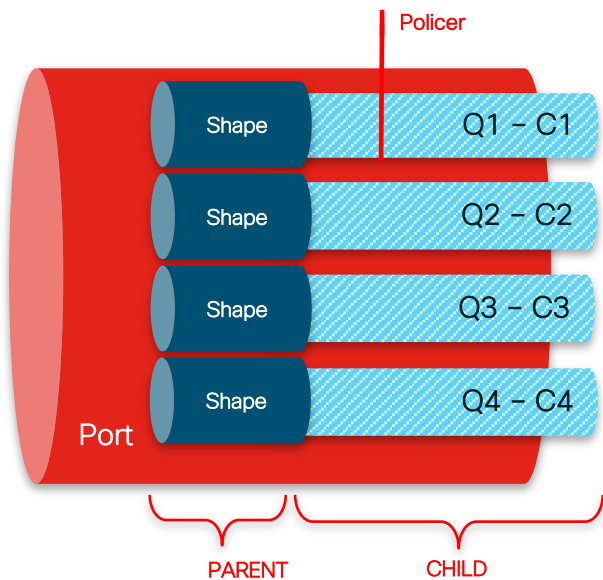
親ポリサー

親ポリシーがポリシングの場合 set のみサポート
されます。子ポリシーでの 2 レベル ポリシングは不可

※ Table-Map を使った条件付きマーキングも可能です

H-QoS ユースケース

親シェーピングおよび子マーキング / ポリシング



```
policy-map PARENT
```

```
class C1
```

```
shape average percent 10
service-policy CHILD
```

```
class C3
```

```
shape average percent 20
service-policy CHILD
```

```
class class-default
```

```
shape average percent 30
service-policy CHILD
```

```
policy-map CHILD
```

```
class C1
```

```
police rate percent 10
set dscp 10
```

親ポリサー

※ Table-Map を使った条件付きマーキングも可能です

Auto QoS

Auto QoS を使うことで、ネットワークに参加する端末タイプごとにクラス マップとポリシーのベスト プラクティスが自動的に反映されます

バージョンによってテンプレートが異なります（現在のバージョンは5.0）

```
auto qos voip {cisco-phone | cisco-softphone | trust}  
auto qos video {cts | ip-camera | media-player}  
auto qos classify [police]  
auto qos trust {cos | dscp}
```

■ Reference (英語)

www.cisco.com/en/US/docs/solutions/Enterprise/Video/autogosmediacampus.pdf

Catalyst 9000 シリーズ Auto QoS v5 テンプレート

```
class-map match-all AUTOQOS-VOICE-DSCP-PQ1
 match dscp ef
class-map match-all AUTOQOS-VIDEO-DSCP-PQ2
 match dscp cs4
 match dscp af41
 match dscp af42
 match dscp af43
 match dscp cs5
class-map match-all AUTOQOS-CONTROL_PLANE-DSCP
 match dscp cs2
 match dscp cs3
 match dscp cs6
 match dscp cs7
class-map match-all AUTOQOS-MULTIMEDIA_STREAMING-DSCP
 match dscp af31
 match dscp af32
 match dscp af33
class-map match-all AUTOQOS-TRANSACTIONAL_DATA-DSCP
 match dscp af21
 match dscp af22
 match dscp af23
class-map match-all AUTOQOS-BULK_DATA-DSCP
 match dscp af11
 match dscp af12
 match dscp af13
class-map match-all AUTOQOS-SCAVENGER-DSCP
 match dscp cs1
```

```
policy-map AUTOQOS-Queueing-OUT
class AUTOQOS-VOICE-DSCP-PQ1
 priority level 1 percent 10
 queue-buffers ratio 5
class AUTOQOS-VIDEO-DSCP-PQ2
 priority level 2 percent 33
 queue-buffers ratio 5
class AUTOQOS-CONTROL_PLANE-DSCP
 bandwidth remaining percent 12
 queue-buffers ratio 5
class AUTOQOS-MULTIMEDIA_STREAMING-DSCP
 bandwidth remaining percent 18
 queue-buffers ratio 10
 queue-limit dscp af31 percent 100
 queue-limit dscp af32 percent 90
 queue-limit dscp af33 percent 80
class AUTOQOS-TRANSACTIONAL_DATA-DSCP
 bandwidth remaining percent 18
 queue-buffers ratio 10
 queue-limit dscp af21 percent 100
 queue-limit dscp af22 percent 90
 queue-limit dscp af23 percent 80
class AUTOQOS-BULK_DATA-DSCP
 bandwidth remaining percent 7
 queue-buffers ratio 20
 queue-limit dscp af11 percent 100
 queue-limit dscp af12 percent 90
 queue-limit dscp af13 percent 80
class AUTOQOS-SCAVENGER-DSCP
 bandwidth remaining percent 1
 queue-buffers ratio 5
class class-default
 bandwidth remaining percent 44
 queue-buffers ratio 40
```

DSCP ベースの Egress キューイングを実行

3.5 Security

DAI

IP Source Guard

First Hop Security

SISF

Trustworthy

Cisco Secure Boot

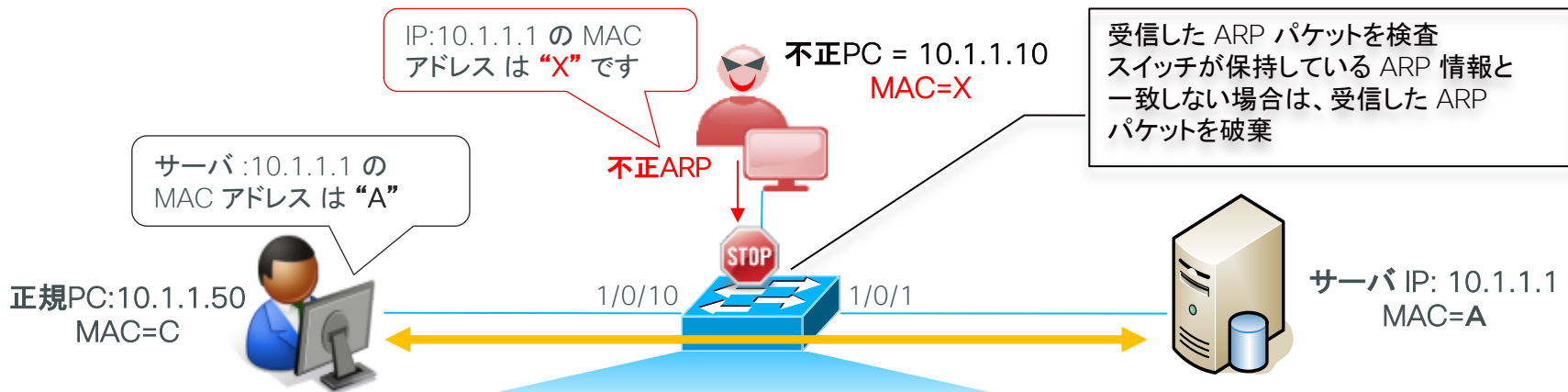
MACsec

ネットワーク認証

Dynamic ARP Inspection (DAI)

Dynamic ARP Inspection は、MAC アドレスと IP アドレスのマッピングをスイッチで管理し、不正な ARP パケットを利用した攻撃からネットワークを守る機能です。この機能により、攻撃者により送信された不正 ARP パケットを検出 / ドロップ を実行しネットワークを守ります。この機能は、DHCP Snooping 機能と併用することで、DHCP により IP アドレスを割り振る場合にも利用可能です。

DAI 機能適用時



MAC アドレス	IP アドレス	VLAN	Interface
A	10.1.1.1	10	GigabitEthernet1/0/1
C	10.1.1.50	10	GigabitEthernet1/0/10

Dynamic ARP inspection 設定例

■ DHCP Snooping と DAI の有効化

```
ip dhcp snooping vlan 211
ip dhcp snooping
```

※snooping設定により、自動的に
device-tracking設定が入ります。

```
ip arp inspection vlan 211
```

show device-tracking policy DT-PROGRAMMATICの出力

Policy DT-PROGRAMMATIC configuration:

```
security-level glean
device-role node
gleaning from Neighbor Discovery
gleaning from DHCP
gleaning from ARP
gleaning from DHCP4
NOT gleaning from protocol unkn
limit address-count for IPv4 per mac 1
tracking enable
```

Policy DT-PROGRAMMATIC is applied on the following targets:

Target	Type	Policy	Feature	Target range
vlan 211	VLAN	DT-PROGRAMMATIC		Device-tracking vlan all

■ Interface でデバイストラッキングを有効化

```
interface GigabitEthernet1/0/1
switchport access vlan 211
switchport mode access
device-tracking
```

※C9kでは、ip device-trackingから、
device-trackingに変更します

show device-tracking policy defaultの出力

Policy default configuration:

```
security-level guard
device-role node
gleaning from Neighbor Discovery
gleaning from DHCP
gleaning from ARP
gleaning from DHCP4
NOT gleaning from protocol unkn
```

Policy default is applied on the following targets:

Target	Type	Policy	Feature	Target range
Gi1/0/17	PORT	default		Device-tracking vlan all

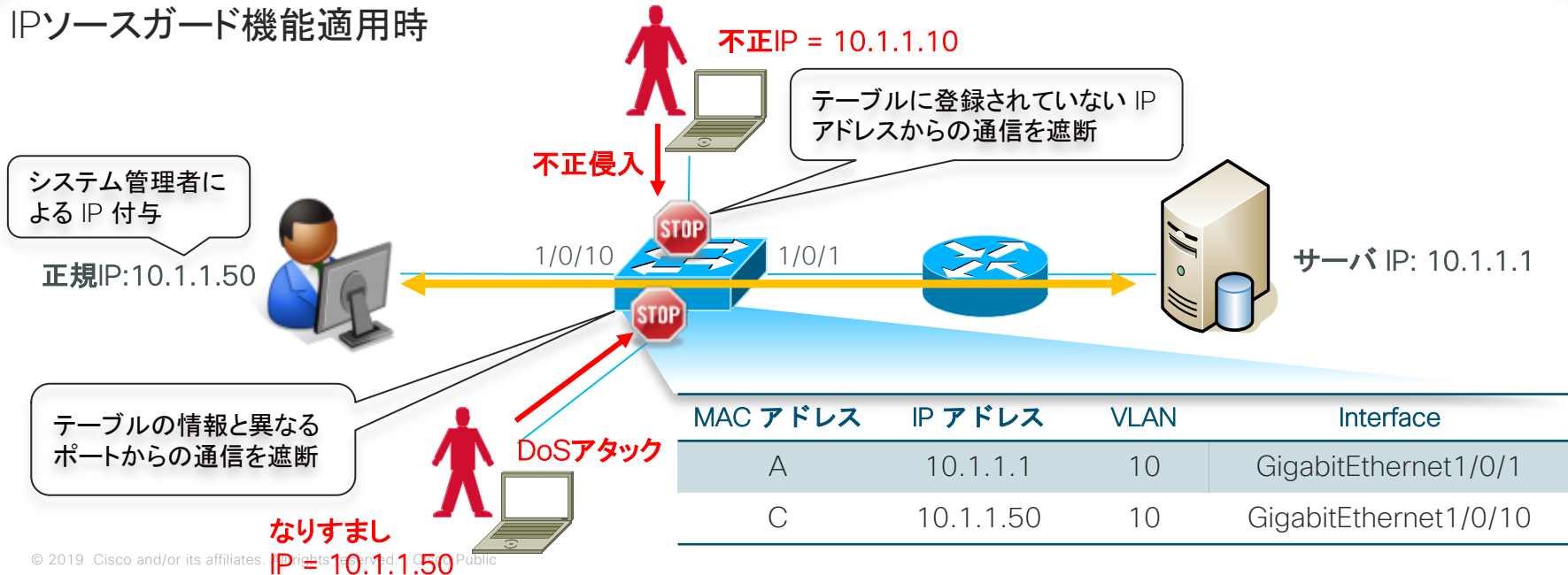
※DT-PROGRAMMATIC よりも、物理インターフェイスに適用するポリシーが優先されます

IP Source Guard

IP ソースガード機能は、IP アドレス とポートのマッピング テーブルを保持しこのテーブルにマッチしない IP トラフィックを遮断することにより、不正な IP アドレスからの通信を制限するセキュリティ機能です。この機能を利用して、攻撃者のネットワーク侵入を未然に防止できます。

この機能は、DHCP Snooping 機能と併用することで、DHCP により IP アドレスを割り振る場合にも利用可能です。

IPソースガード機能適用時



IP Source Guard 設定例

■ DHCP Snooping の有効化

```
ip dhcp snooping vlan 211
ip dhcp snooping
```

■ Device Tracking のポリシーを作成

```
device-tracking policy TEST01
limit address-count 100
no protocol arp
tracking enable
```

no protocol arp

- ARP をスヌーピングしないように設定します
- IP Source Guard 動作には設定必須です

■ Interface で IP source guard を有効化

```
interface GigabitEthernet1/0/1
switchport access vlan 211
switchport mode access
device-tracking attach-policy TEST01
ip verify source tracking
```

※物理インターフェイスに
ポリシー適用

show device-tracking policy TEST01の出力

```
Policy TEST01 configuration:
security-level guard
device-role node
gleaning from Neighbor Discovery
gleaning from DHCP
NOT gleaning from ARP
gleaning from DHCP4
NOT gleaning from protocol unkn
limit address-count 100
tracking enable
```

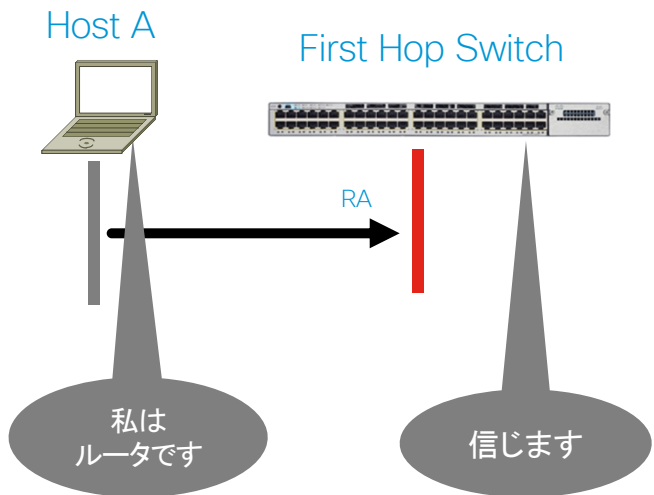
Policy TEST01 is applied on the following targets:

Target	Type	Policy	Feature	Target range
Gi1/0/17	PORT	TEST01		Device-tracking vlan all

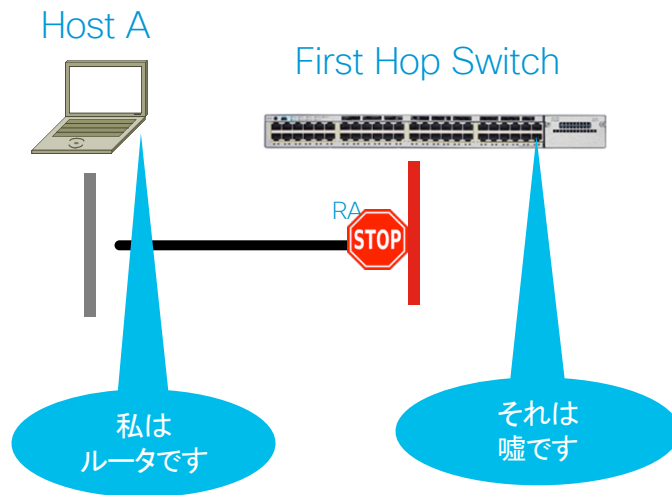
IPv6 First Hop Security - RA Guard

不正 Router Advertisements を阻止

<RA Guard なし>

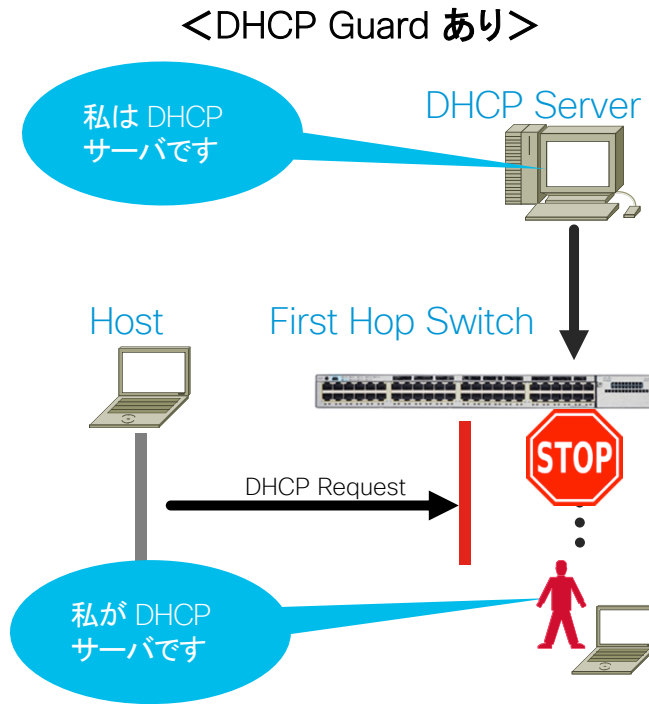
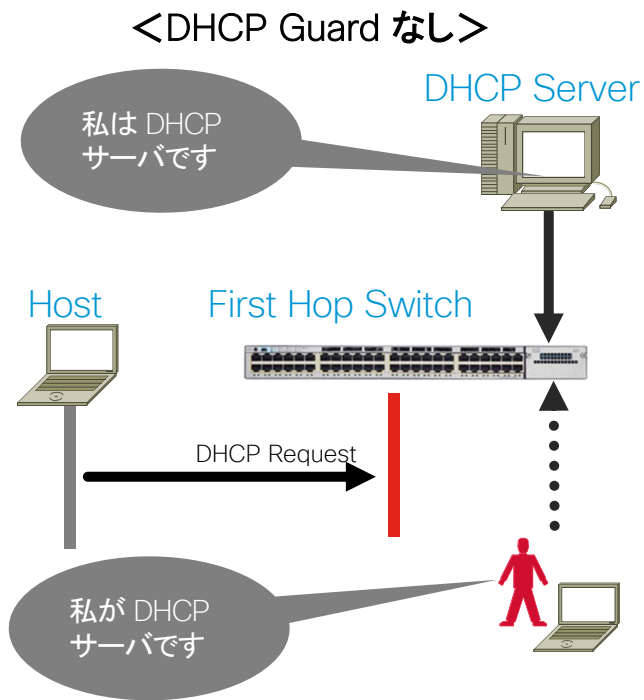


<RA Guard あり>



IPv6 First Hop Security - DHCP Guard

不正 DHCP レスポンスを阻止



RA Guard / DHCP Guard 設定例

<RA Guard>

■ RA ガード ポリシーを作成

```
ipv6 nd rguard policy TEST01  
device-role host
```

※手動でRA guardのポリシーを設定します

■ Interface に RA ガード ポリシーをアタッチ

```
interface GigabitEthernet1/0/1  
switchport access vlan 211  
switchport mode access  
device-tracking  
ipv6 nd rguard attach-policy TEST01
```

※Device-Tracking 有効化します

<DHCP Guard>

■ DHCP ガード ポリシーを作成

```
ipv6 dhcp guard policy TEST01  
device-role client
```

※手動でDHCP guardのポリシーを設定します

■ Interface に DHCP ガード ポリシーをアタッチ

```
interface GigabitEthernet1/0/1  
switchport access vlan 211  
switchport mode access  
device-tracking  
ipv6 dhcp guard attach-policy TEST01
```

※Device-Tracking 有効化します

SISF-based Device-Tracking

- Switch Integrated Security Feature based(SISF ベース)の Device Tracking 機能は、従来の IP Device-Tracking と IPv6 Snooping に代わる新しいデバイス情報を補足する機能 (IOS-XE 16.3.x以降)です。
- SISF は、スイッチが受信したトラフィックをスヌープし、デバイス ID(MAC および IP アドレス)を抽出して、それらをバインディング テーブルに保存します
- IEEE 802.1X、Web 認証、Cisco TrustSec、LISP などの多くの機能が本機能を使用します
- SISF ベースのデバイス トラッキングは、IPv4とIPv6の両方をサポートします
- Cisco Catalyst 9000 シリーズでは SISF-based Device-Tracking を IP Device-Tracking の代替として使う必要があります

show device-tracking database 一部抜粋

Network Layer Address	Link Layer Address	Interface	vlan	prIvl	age	state	Time left
L 192.168.202.254	0000.0c9f.f460	Vl1025	1025	0100	1684mn	DOWN	
L 192.168.201.254	0000.0c9f.f461	Vl1026	1026	0100	1683mn	REACHABLE	
ARP 192.168.201.51	50f7.22ae.25c1	Gi1/0/2	1026	0005	4mn	REACHABLE	39 s try 0
ARP 192.168.201.14	000c.29ec.d0b4	Gi1/0/1	1026	0005	91s	REACHABLE	210 s try 0
DH4 192.168.201.13	000c.29bd.d112	Gi1/0/1	1026	0025	3mn	REACHABLE	86 s try 0(590324 s)
ARP 192.168.201.12	000c.29dc.e708	Gi1/0/1	1026	0005	29s	REACHABLE	286 s try 0
DH4 192.168.201.11	000c.298f.15e1	Gi1/0/1	1026	0025	65s	REACHABLE	247 s try 0(590330 s)

SISF-based Device-Tracking の作成

■ 手動作成

自分で Profile 作成可能です。

自動生成よりも優先度は高いです

device-tracking policyでプロファイルを作成して、VLAN Configurationまたは物理インターフェイスに適用可能です

VLAN より物理インターフェイスの方が優先されます

■ 自動生成

下記のそれぞれの場合に自動的に作成されます

IEEE 802.1X, web authentication, Cisco TrustSec, and IPSG features: enter the `ip dhcp snooping vlan` vlan command.

Cisco Locator/ID Separation Protocol.

EVPN on VLAN

ip dhcp snooping 設定時の自動生成ポリシー サンプル

```
C9200-1#show device-tracking policy DT-PROGRAMMATIC
Policy DT-PROGRAMMATIC configuration:
```

```
security-level glean
device-role node
```

```
gleaning from Neighbor Discovery ←ipv6 ND情報収集有効
gleaning from DHCP ←ipv6 DHCP情報収集有効
gleaning from ARP ←ipv4 ARP情報収集有効
gleaning from DHCP4 ←ipv4 DHCP情報収集有効
```

```
NOT glean from protocol unkn
limit address-count for IPv4 per mac 1
tracking enable
```

Policy DT-PROGRAMMATIC is applied on the following targets:

Target	Type	Policy	Feature	Target range
vlan 211	VLAN	DT-PROGRAMMATIC		Device-tracking vlan all
vlan 212	VLAN	DT-PROGRAMMATIC		Device-tracking vlan all
vlan 213	VLAN	DT-PROGRAMMATIC		Device-tracking vlan all
vlan 214	VLAN	DT-PROGRAMMATIC		Device-tracking vlan all
vlan 215	VLAN	DT-PROGRAMMATIC		Device-tracking vlan all

IP Device Tracking との違い

IP Device Tracking (IPDT) のコンフィグ

SISF-Based のコンフィグ (Cisco IOS XE Denali 16.3.7以降)

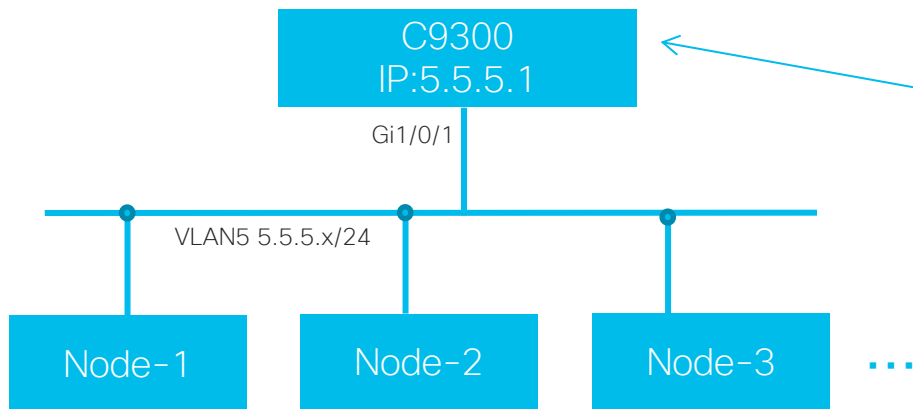
ip device tracking probe count	デフォルト値（3回）に設定され、変更できません
ip device tracking probe delay	デフォルト値（10秒）に設定され、変更できません
ip device tracking probe interval	device-tracking binding reachable-lifetime
ip device tracking probe use-svi	デフォルトの動作として設定され、変更できません
ip device tracking probe auto-source [fallback host-ip-address subnet-mask] [override]	device-tracking tracking auto-source [fallback host-ip-address subnet-mask] [override]
ip device tracking trace-buffer	サポートされていません
ip device tracking maximum n	device-tracking policy <Policy name> limit address-count <n>
ip device tracking maximum 0	サポートされていません
clear ip device tracking all	サポートされていません

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/16-9/configuration_guide/sec/b_169_sec_3850_cg/configuring_sisf_based_device_tracking.html

SISF-Device Tracking 動作確認

SISF-DT を有効にしたときの Device Tracking データベースの状態と Limit Address Count を超えた際の動作を確認します

トポロジー



```
ip dhcp snooping vlan 1-4094  
ip dhcp snooping
```

```
device-tracking policy TEST  
limit address-count 2  
no protocol udp  
tracking enable
```

```
interface GigabitEthernet1/0/1  
switchport access vlan 5  
switchport mode access  
device-tracking attach-policy TEST
```

※ C9300 の DT の最大値は 32,000 まで設定可能です

Device Tracking データベースの確認

Limit address - count 2

```
C9300-1#show device-tracking database
Binding Table has 3 entries, 2 dynamic (limit 100000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol, DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT -
Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match    0002:Orig trunk          0004:Orig access
0008:Orig trusted trunk  0010:Orig trusted access 0020:DHCP assigned
0040:Cga authenticated   0080:Cert authenticated  0100:Statically assigned

   Network Layer Address      Link Layer Address Interface    vlan prlvl age state    Time left
ARP 5.5.5.11                 502f.a8b0.f701 Gi1/0/1      5 0005 150s REACHABLE 155 s try 0
ARP 5.5.5.7                  580a.2013.ebc1 Gi1/0/1      5 0005  3mn REACHABLE 126 s try 0
L 5.5.5.1                    701f.5301.2cc7 V15          5 0100  58mn REACHABL
```

Local の SVI を除いて 3 台目以降のデバイス IP はデータベースに保存されません

Limit address count 2 の状態で通信状況確認

■ 各デバイスからゲートウェイへの通信状況を確認

```
Node-1#ping 5.5.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
Node-2#ping 5.5.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

```
Node-3#ping 5.5.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Device Tracking Table Limit を超えても、C9300 の SVI(5.5.5.1) へは通信は可能です。

3.5 Security

IP Source Guard を設定し通信状況を確認

```
Node-1#ping 5.5.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
Node-2#ping 5.5.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

```
Node-3#ping 5.5.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

■ C9300 に IP Source Guard を追記

```
interface GigabitEthernet1/0/1
switchport access vlan 5
switchport mode access
device-tracking attach-policy TEST
ip verify source tracking
```

デバイストラッキング データ ベースに載ってない IP は
通信不可になります

3.5 Security

Device Tracking データベースの確認

Limit address - count 3

```
C9300-1#show device-tracking database
Binding Table has 4 entries, 3 dynamic (limit 100000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol, DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other
Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match    0002:Orig trunk        0004:Orig access
0008:Orig trusted trunk  0010:Orig trusted access  0020:DHCP assigned
0040:Cga authenticated   0080:Cert authenticated  0100:Statically assigned
```

Network Layer Address	Link Layer Address	Interface	vlan	prlvl	age	state	Time left
ARP 5.5.5.11	502f.a8b0.f701	Gi1/0/1	5	0005	3mn	REACHABLE	128 s try 0
ARP 5.5.5.8	b08b.cf48.a901	Gi1/0/1	5	0005	2s	REACHABLE	307 s
ARP 5.5.5.7	580a.2013.ebc1	Gi1/0/1	5	0005	3mn	REACHABLE	98 s try 0
L 5.5.5.1	701f.5301.2cc7	Vl5	5	0100	68mn	REACHABLE	

Local の SVI を除いて 3 台分のアドレスはテーブル上に載ります

Limit address count 3 の状態で通信状況確認

■ 各デバイスからゲートウェイへの通信状況を確認

```
Node-1#ping 5.5.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
Node-2#ping 5.5.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

```
Node-3#ping 5.5.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

当然、どの端末もゲートウェイへは通信可能です

Trustworthy システム

機器の製造プロセスや、機器の起動 / 稼働中において
ハードウェアおよびソフトウェアの完全性 (Integrity) を担保するための、仕組みの総称のことです。

完全性の担保とは：

ハードウェアは、メーカーが提供する正規品であるか、
ソフトウェアは、改ざんされていないか、

機器の”起動”と”稼働中”に検証 (check / validation) をします。



リスク低減



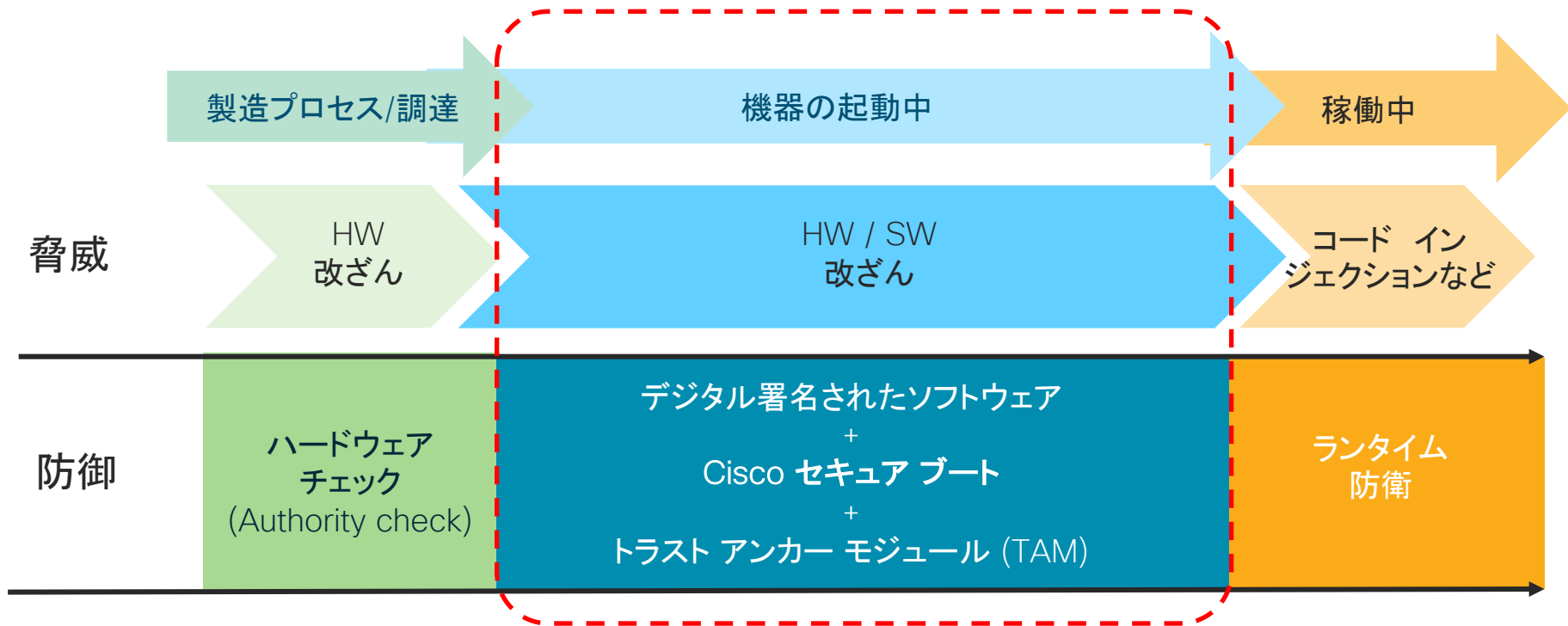
機器の完全性の可視化



脅威の早期検知

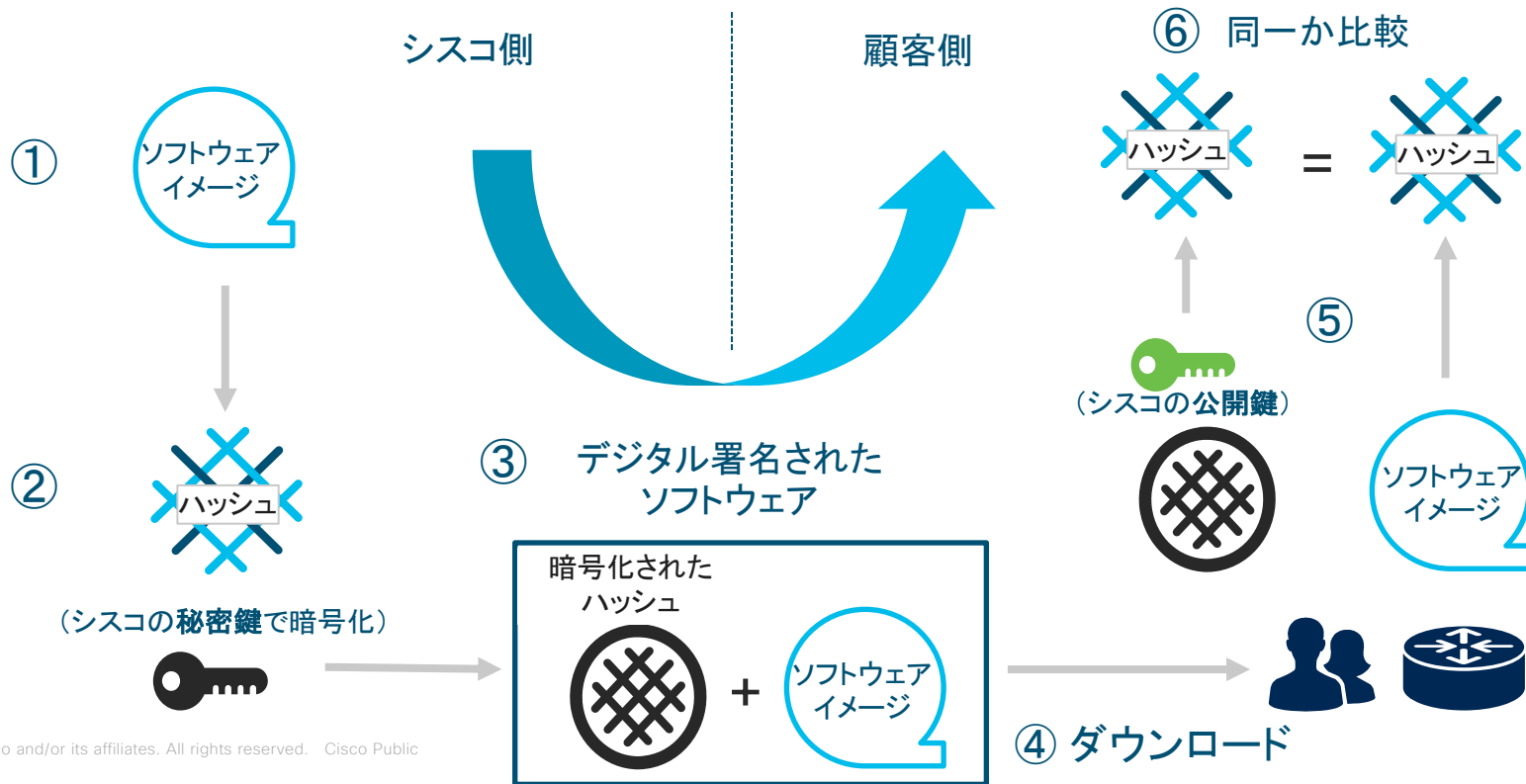
Trustworthy システムの概要

Trustworthy システム =
機器の調達、起動と稼働中において
HW/SWの完全性を担保するための仕組み



デジタル署名されたソフトウェア

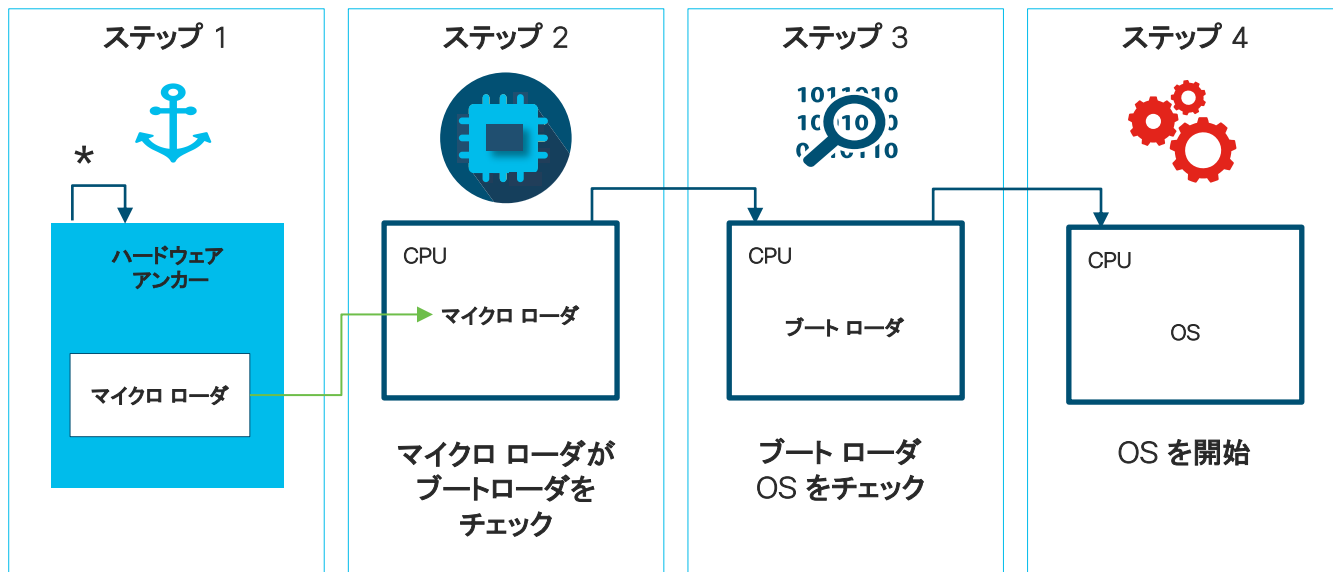
ソフトウェアの完全性



Cisco セキュア ブート

Microloader : 起動プロセス (Bootloader / BIOS) のチェック機能をハードウェア レベルに組み込むことによって、ソフトウェアの整合性、完全性を担保します。

Cisco Secure Boot



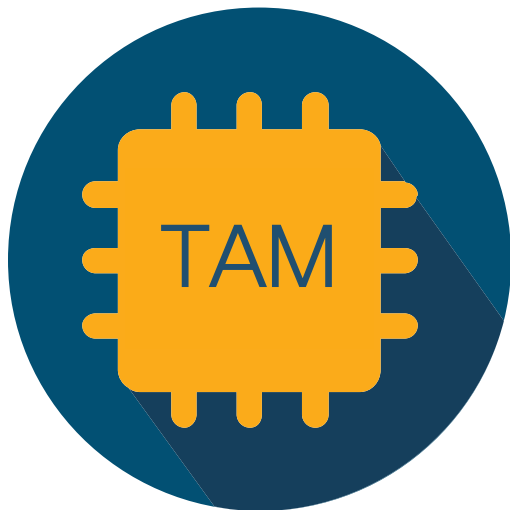
※最初の命令は CPU 上で実行され、ハードウェアに保存される
→改ざん不可

UEFI



トラスト アンカー モジュール (TAM)

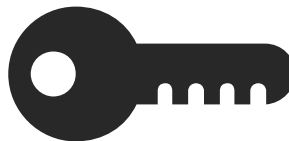
ハードウェアの完全性



マイクロ ローダ
製造元でインストールされるソフトウェア
ソフトウェアのブート ローダ



X.509 Secure Unique Device ID (SUDI)
製造元でインストールされる証明書
ハードウェアのシリアル番号
デバイス固有の公開鍵



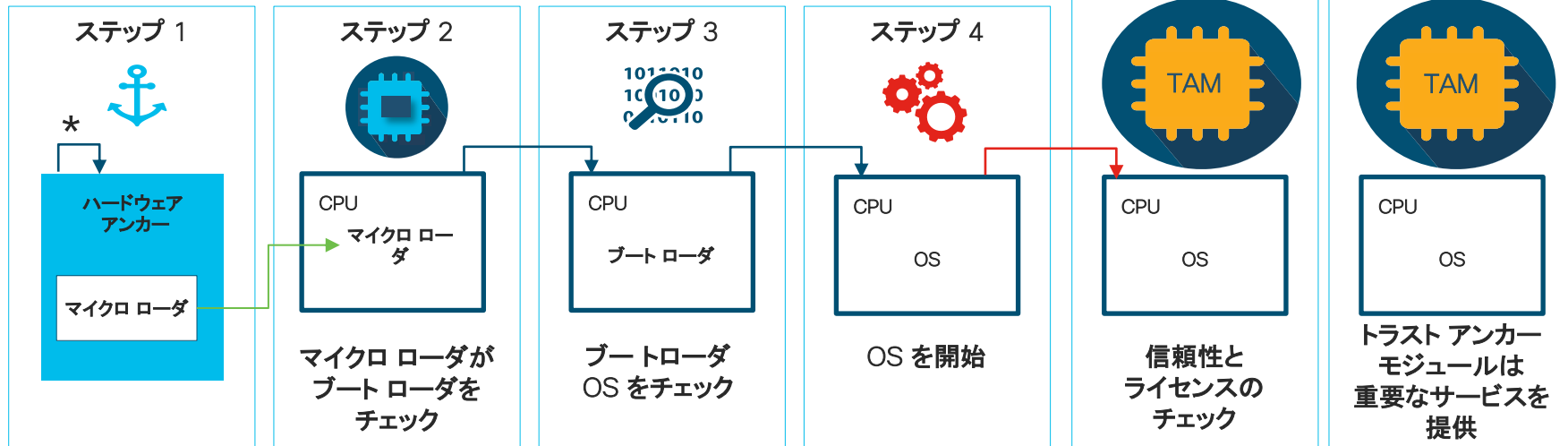
秘密鍵
製造元でインストールされるキー
デバイス固有の秘密鍵

Cisco セキュアブート & トラスト アンカー モジュール

ソフトウェアがハードウェアの完全性をチェック

Trust Anchor Module : 正規のハードウェア情報が刻印されたチップを搭載。OS が確認し、正規のハードウェアであることを担保(正規のものでない場合にはコンソール画面にアラート表示)します。

Cisco Secure Boot



* 最初の命令は CPU 上で実行され、ハードウェアに保存される → 改ざん不可

↓ ソフトウェア信頼性チェック
↓ ハードウェア信頼性チェック

3.5 Security

ブートアップ時のソフトウェア検証

※マイクロ ロードの検証は表示されないが、もし検証に失敗するとブートが失敗します

■ ROMMON Secure Boot Verification

```
Initializing Hardware ...
```

```
System integrity status: 00000610  
Rom image verified correctly
```

```
System Bootstrap, Version 15.4(3r)S, RELEASE SOFTWARE (fc1)  
Copyright (c) 1994-2014 by cisco Systems, Inc.  
<snip>
```

■ IOS Secure Boot Verification

```
<snip>  
#####  
Boot image size = 425853700 (0x19620304) bytes
```

```
Package header rev 1 structure detected  
Calculating SHA-1 hash...done  
validate_package: SHA-1 hash:  
    calculated 334207fa:464503d3:2e7abd5f:160919d0:b425523b  
    expected  334207fa:464503d3:2e7abd5f:160919d0:b425523b
```

```
RSA Signed RELEASE Image Signature Verification Successful.  
Package Load Test Latency : 6511 msec  
Image validated  
<snip>
```

MACsec (MAC security)

イーサネット通信を暗号化する技術により
通信を傍受されても内容を盗み見されることがありません

Cisco Catalyst 9200 / 9200L は、
L2 アクセス スイッチとして **MACsec に初めて対応しました**

MACsec の暗号化チップ搭載
ラインレート性能のハードウェア
処理です

適用箇所	MACsec	Cat 9200		Cat9200L	
		IOS-XE	License	IOS-XE	License
スイッチ間	128 Bits SAP	16.10.1	Network Essentials	16.9.1	Network Essentials
	128 Bits MKA	16.10.1	Network Essentials	16.9.1	Network Essentials
端末からスイッチ	128 Bits MKA	対応予定		対応予定	

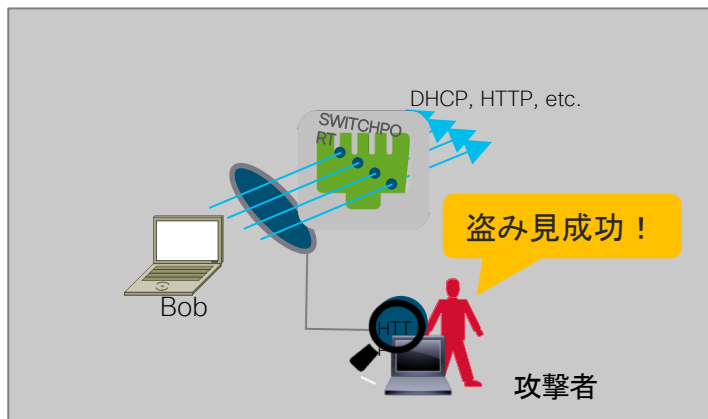
■ 注意点

- ・MACsec 設定が相互でミスマッチする場合は Link Down になるのでご注意ください。
- ・HA 構成、端末からスイッチでのMACsecは 16.12.1から対応しております。

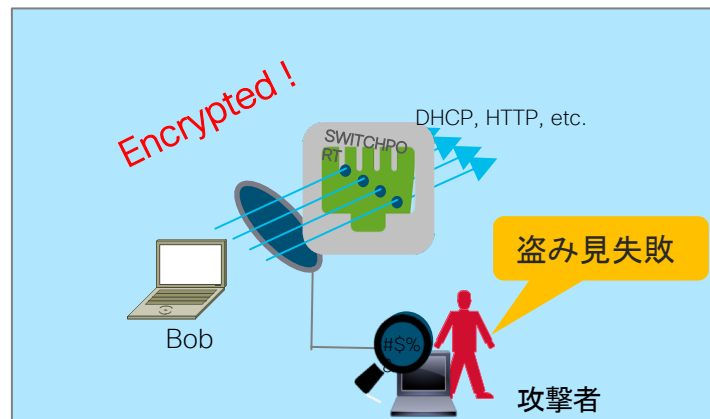
端末 - スイッチ間における MACsec 暗号化

端末 - スイッチ間の暗号化(IEEE 802.1X を利用)

MACsec が無いとき



MACsec があるとき



Step1

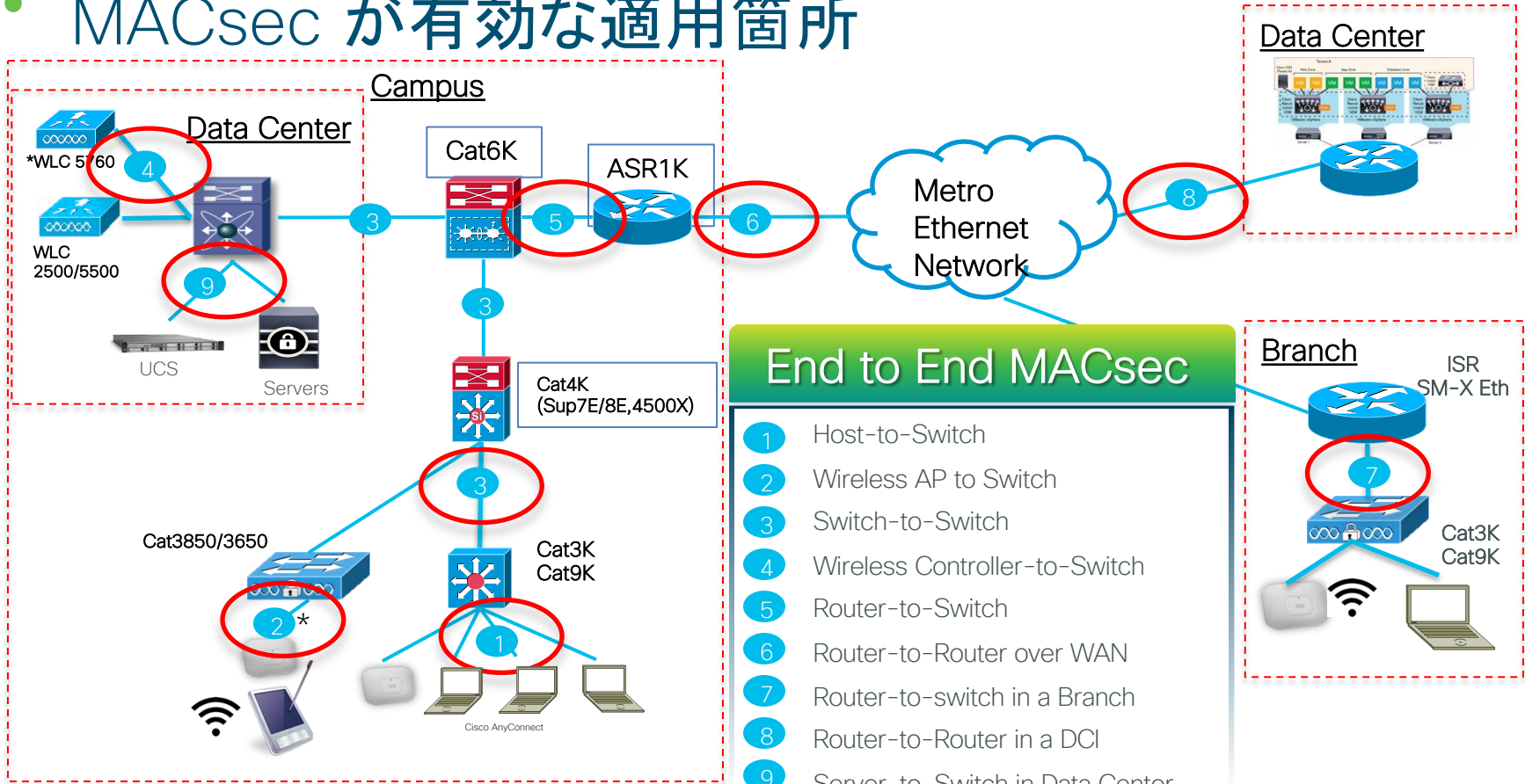
IEEE 802.1X は、エンドポイントを認証し、必要な暗号化キー情報を両側に転送します

Step2

認証から派生したマスターキーを使用して、MACsec は通信を暗号化します

※ サプリカントとして AnyConnect を利用 (IOS-XE 16.10.1以降)

MACsec が有効な適用箇所



MACsec のキー導出スキーム

MACsec はキー導出スキームには大きく 2 つの仕組みがあります。

	SAP (Security Association Protocol)	MKA (MACsec Key Agreement)
概要	シスコ独自のキー ネゴシエーション プロトコル	IEEE802.1X-2010 で定義
適用箇所	スイッチ間の暗号化にのみ利用	スイッチ間、端末とスイッチ間およびルータで利用
利用モード	マニュアル モード IEEE802.1x モード	マニュアル モード IEEE802.1x モード

3.5 Security

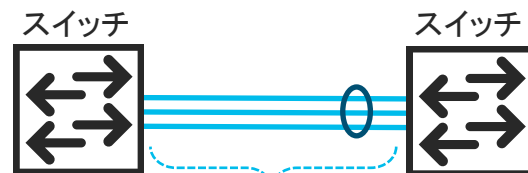
MACsec の設定方法

スイッチ間の暗号化 (1/2)

```
key chain macsectest macsec
key 1111111
  cryptographic-algorithm aes-128-cmac
  key-string 0123456789abcdef0123456789abcdef
  lifetime local 12:12:12 Jan 1 2019 infinite
```

```
mka policy macsectest
key-server priority 200
macsec-cipher-suite gcm-aes-128      #default
```

```
Interface gi1/0/10
switchport mode trunk
macsec network-link
mka policy macsectest
mka pre-shared-key key-chain macsectest
macsec replay-protection window-size 10
```



暗号化され
たデータ
スイッチ間ネゴシエーション: EAPoL

スイッチ間の設定なので、“network-link”を選択します

3.5 Security

MACsec の設定方法

スイッチ間の暗号化 (2/2)

```
C9200L#show macsec interface gi1/0/10
```

MACsec is enabled

Replay protect : enabled

Replay window : 0

Include SCI : yes

Use ES Enable : no

Use SCB Enable : no

Admin Pt2Pt MAC : forceTrue(1)

Pt2Pt MAC Operational : no

Cipher : GCM-AES-128

Confidentiality Offset : 0

MACsec 有効化しま
す

Capabilities

ICV length : 16

Data length change supported: yes

Max. Rx SA : 16

Max. Tx SA : 16

Max. Rx SC : 8

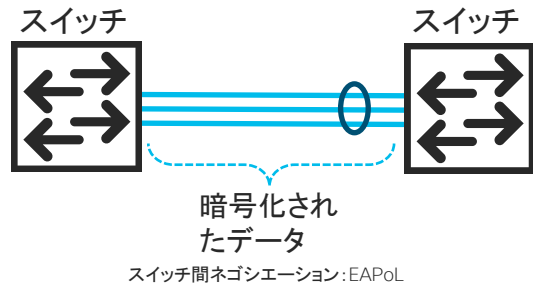
Max. Tx SC : 8

Validate Frames : strict

PN threshold notification support : No

Ciphers supported : GCM-AES-128

AES128 bit で暗号化します

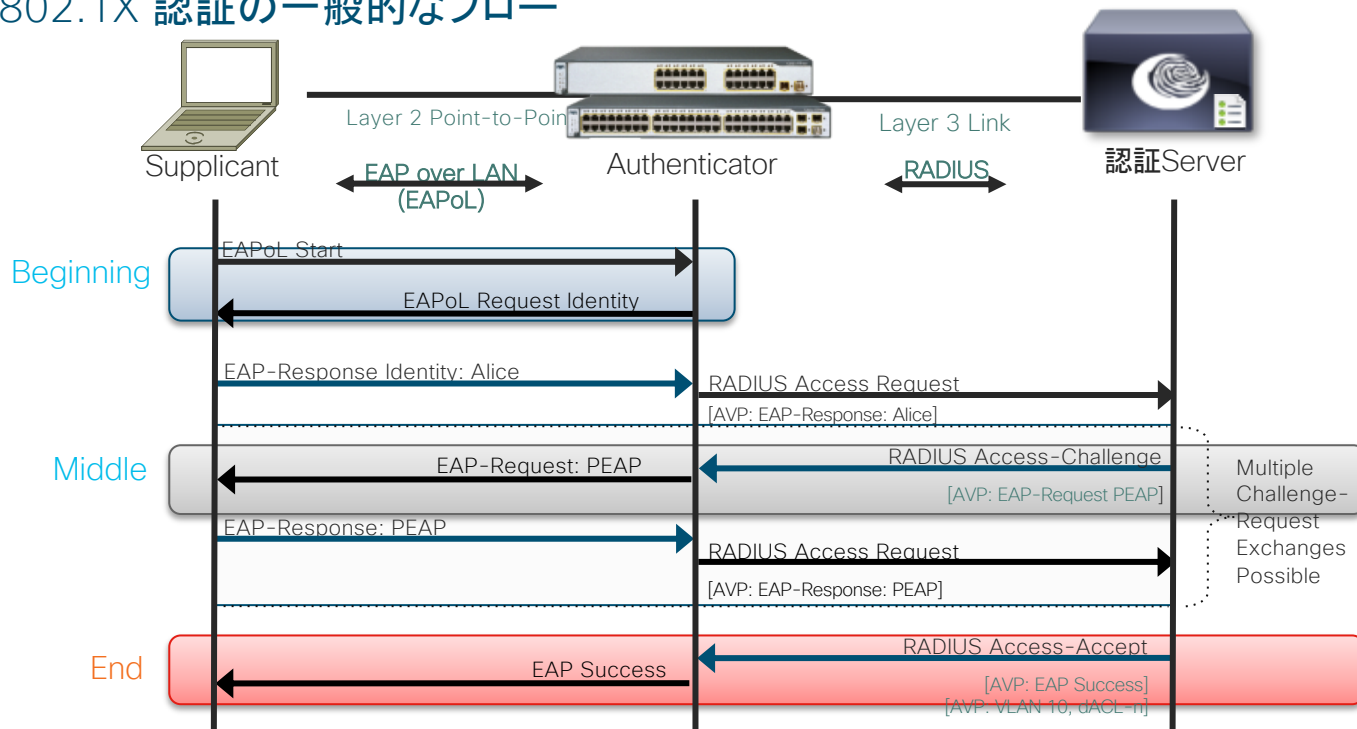


9200 シリーズだとサポートされている暗号化スイートは
GCM-AES-128 のみです

※ 注意: マルチ シャーシ イーサ チャンネルにて MACsec 利用時、マスターの切り替わりが発生した際は、MKA が保持されず、セッションの再確立に数十秒要し、その間当該リンクは通信不可となります。

ネットワーク認証

IEEE 802.1X 認証の一般的なフロー



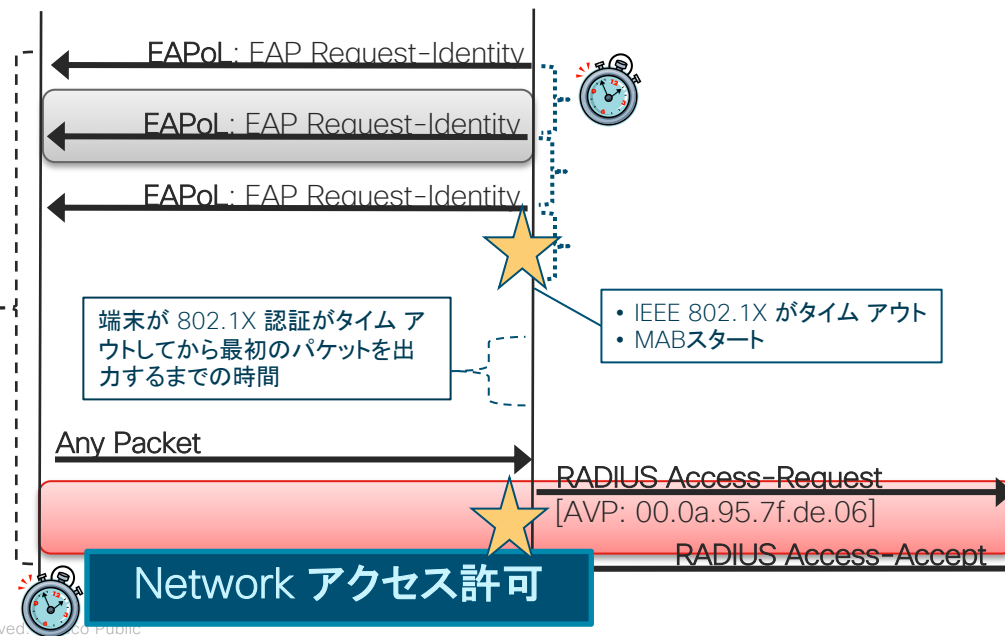
- EAPoL は転送メカニズムを指しており、認証に関する仕組みは提供しません
- 802.1X 認証を利用する場合、端末サブリカント側で EAP タイプを選択する必要があります
- EAP-TLS (クライアント証明書)、PEAP (ユーザ名 / パスワード) など

ネットワーク認証

MAC Authentication Bypass (MAB) のフロー

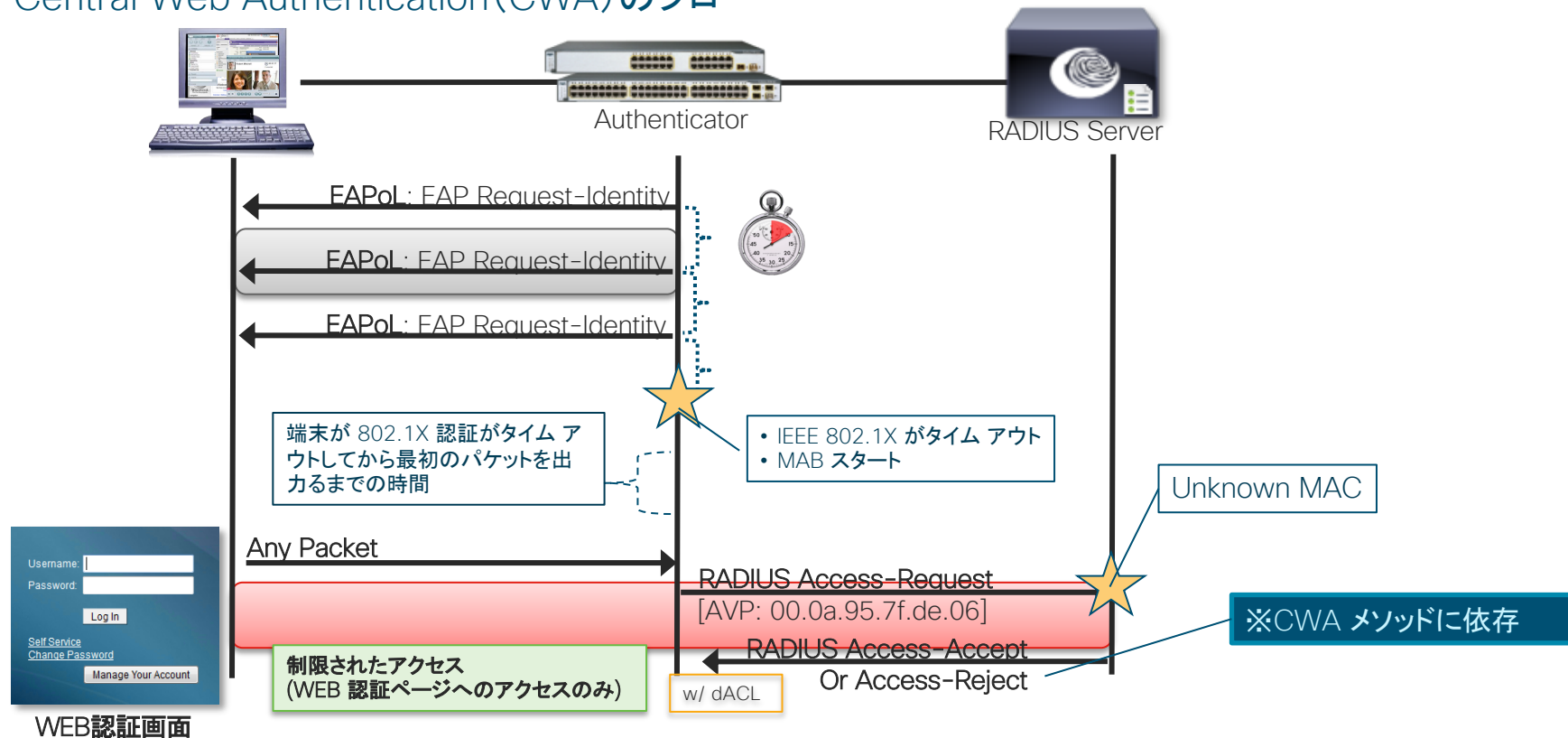


リンクアップ後、ネットワークアクセスが許可されるまでの時間



ネットワーク認証

Central Web Authentication(CWA)のフロー



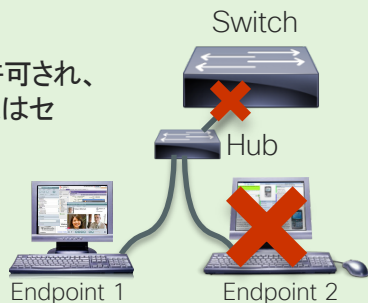
ネットワーク認証のホストモード

ネットワーク認証には主に下記の4つのモードが存在します

Single Host

単一 MAC アドレスのみが許可され、
2 台目以降の MAC アドレスはセ
キュリティ違反となります

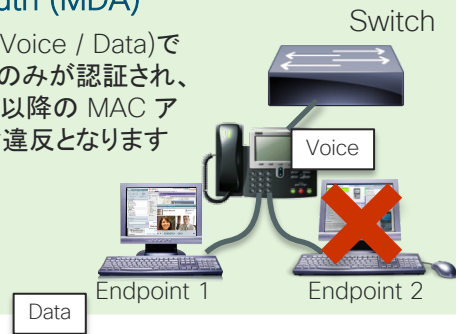
VLAN dACL



Multi-Domain Auth (MDA)

それぞれのドメイン(Voice / Data)で
単一 MAC アドレスのみが認証され、
各ドメインの 2 台目以降の MAC ア
ドレスはセキュリティ違反となります

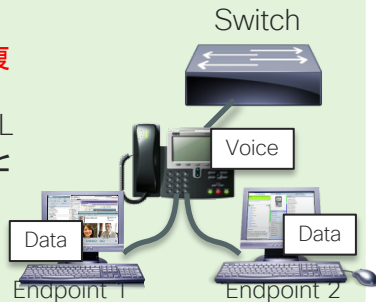
VLAN dACL



Multi-Authentication

音声端末は 1 台、Data 端末は**複
数台同時に認証可能**で、それぞ
れのホストに対して、異なるdACL
/ dVLAN ポリシーを適用するこ
とができます

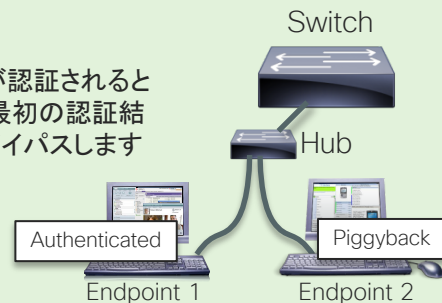
VLAN* dACL



Multi-Host

最初の MAC アドレスが認証されると
2 台目以降のホストは最初の認証結
果に相乗りし、認証をバイパスします

VLAN*



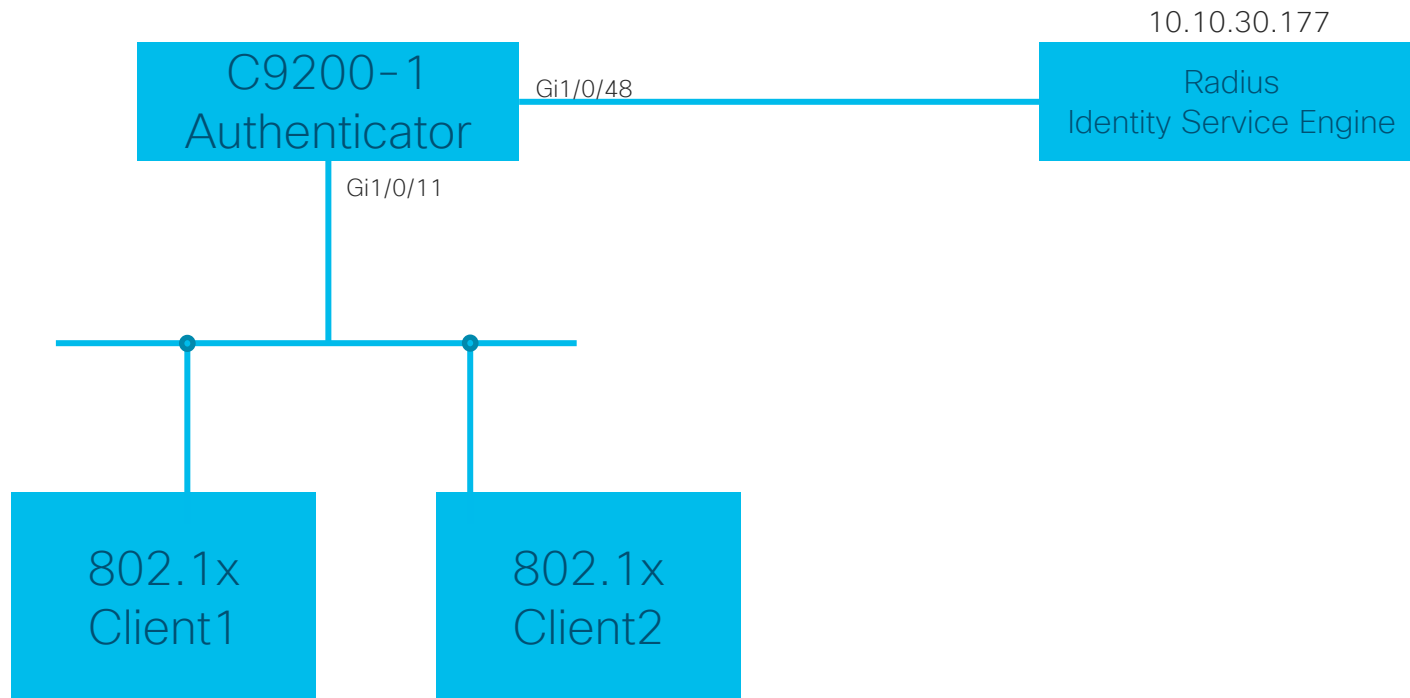
Cisco Catalyst 9200L シリーズ 認証 検証結果サマリ

島 Hub 配下の有線端末を想定した Multi-auth 設定でも、dot1x、MAB、CWA は正常に動作します

ホスト モード	VLAN 割当	dot1x	MAB	CWA
Single Host	無し	○	○	○
	Dynamic vlan	○	○	○
Multi-Authentication	無し	○	○	○
	Dynamic vlan	○	○	○

設定例① 802.1X Multi認証 + Dynamic VLAN

Cisco Catalyst 9200 L で 802.1X Multi 認証→ユーザごとに Dynamic VLAN を動作させる設定



ISE 設定サンプル

■ User 情報の追加

Username	Identity Group
user1	vlan211
user2	vlan212

■ 認可 Profile の設定

AuthZ Profiles	Vlan
vlan211_permit	211
vlan212_permit	212

■ 認可ルールの設定

Identity Group	Results
vlan211	vlan211_permit
vlan212	vlan212_permit

Network Access Users

Status	Name	User Identity Groups	Admin
<input type="checkbox"/> Enabled	ad01	staff-group	
<input type="checkbox"/> Enabled	caadmin	ALL_ACCOUNTS (default)	
<input type="checkbox"/> Enabled	sponsor	ALL_ACCOUNTS (default)	
<input type="checkbox"/> Enabled	user1	vlan211	
<input type="checkbox"/> Enabled	user2	vlan212	
<input type="checkbox"/> Enabled	user3	ALL_ACCOUNTS (default)	
<input type="checkbox"/> Enabled	user4	ALL_ACCOUNTS (default)	

Access Type = ACCESS_ACCEPT
 Tunnel-Private-Group-ID = 1:211
 Tunnel-Type = 1:13
 Tunnel-Medium-Type = 1:6

Access Type = ACCESS_ACCEPT
 Tunnel-Private-Group-ID = 1:212
 Tunnel-Type = 1:13
 Tunnel-Medium-Type = 1:6

▼ Authorization Policy

► Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	vlan211	if vlan211	then vlan211_permit
<input checked="" type="checkbox"/>	vlan212	if vlan212	then vlan212_permit
<input checked="" type="checkbox"/>	Permit_all	if Any	then PermitAccess
<input checked="" type="checkbox"/>	Default	if no matches, then DenyAccess	

802.1X マルチ認証設定例

```
aaa new-model
```

AAA の有効化

```
aaa authentication dot1x default group radius  
aaa authorization network default group radius  
aaa accounting dot1x default start-stop group radius
```

認証、認可、アカウントングで利用する、サーバグループを指定

```
aaa server radius dynamic-author  
client 10.10.30.177 server-key cisco  
auth-type all
```

Radius サーバの情報と共有鍵の情報を指定

```
dot1x system-auth-control
```

```
radius server ISE  
address ipv4 10.10.30.177 auth-port 1812 acct-port 1813  
key cisco
```

サーバグループを定義

```
interface GigabitEthernet1/0/11  
switchport mode access  
device-tracking  
authentication host-mode multi-auth  
authentication order dot1x mab  
authentication port-control auto  
authentication periodic  
mab  
dot1x pae authenticator  
spanning-tree portfast
```

Interface 上で認証を有効化しマルチ認証モードに指定

<注意点>

- C9200L の認証ポートは mode access で設定します
- C9200L 上で Dynamic vlan でアサインする VLAN の作成が必要です

Cisco Catalyst 9200 L show command 1

Cisco Catalyst 9200 L でマルチ認証が成功し 2 つのデバイスを確認できます

```
Switch#show authentication sessions int gi1/0/11
```

Interface	MAC Address	Method	Domain	Status	Fg	Session ID
Gi1/0/11	2852.6168.d101	dot1x	DATA	Auth		A51E0A0A0000004D35EC5E80
Gi1/0/11	2c0b.e9ad.ad81	dot1x	DATA	Auth		A51E0A0A0000004C35EC5378

Key to Session Events Blocked Status Flags:

- A - Applying Policy (multi-line status for details)
- D - Awaiting Deletion
- F - Final Removal in progress
- I - Awaiting IIF ID allocation
- P - Pushed Session
- R - Removing User Profile (multi-line status for details)
- U - Applying User Profile (multi-line status for details)
- X - Unknown Blocker

3.5 Security

Cisco Catalyst 9200 L show command 2

```
Switch#show authentication sessions int gi1/0/11 details
```

```
Interface: GigabitEthernet1/0/11
```

```
IIF-ID: 0x1AA0AC98
```

```
MAC Address: 2c0b.e9ad.ad81
```

```
IPv6 Address: Unknown
```

```
IPv4 Address: Unknown
```

```
User-Name: user1
```

```
Status: Authorized
```

```
Domain: DATA
```

```
Oper host mode: multi-auth
```

```
Oper control dir: both
```

```
Session timeout: 3600s (local), Remaining: 2972s
```

```
Timeout action: Reauthenticate
```

```
Common Session ID: A51E0A0A0000004C35EC5378
```

```
Acct Session ID: 0x00000009
```

```
Handle: 0x1a00000c
```

```
Current Policy: POLICY_Gi1/0/11
```

MAC アドレス 2c0b.e9ad.ad81
を持つ端末のユーザ ID

```
Local Policies:
```

```
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
```

```
Security Policy: Should Secure
```

```
Server Policies:
```

```
Vlan Group: Vlan: 211
```

User1 にアサインされる VLAN
211

```
Method status list:
```

Method	State
dot1x	Authc Success

```
Interface: GigabitEthernet1/0/11
```

```
IIF-ID: 0x1D17F138
```

```
MAC Address: 2852.6168.d101
```

```
IPv6 Address: Unknown
```

```
IPv4 Address: Unknown
```

```
User-Name: user2
```

```
Status: Authorized
```

```
Domain: DATA
```

```
Oper host mode: multi-auth
```

```
Oper control dir: both
```

```
Session timeout: 3600s (local), Remaining: 2975s
```

```
Timeout action: Reauthenticate
```

```
Common Session ID: A51E0A0A0000004D35EC5E80
```

```
Acct Session ID: 0x0000000a
```

```
Handle: 0xc000000d
```

```
Current Policy: POLICY_Gi1/0/11
```

MAC アドレス
2852.6168.d101を持つ端末の
ユーザ ID

```
Local Policies:
```

```
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
```

```
Security Policy: Should Secure
```

```
Server Policies:
```

```
Vlan Group: Vlan: 212
```

User2 にアサインされる VLAN
212

```
Method status list:
```

Method	State
dot1x	Authc Success

認証ログの確認 1

Identity Services Engine

Home Operations Policy Guest Access Administration Work Centers

RADIUS Livelog TACACS Livelog Reports Troubleshoot Adaptive Network Control

Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 8 Client Stopped 0

Show Live Sessions Add or Remove Columns Refresh Reset Repeat Counts

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
2019-01-10 05:47:56.460			5	08:CC:A7:5F:06:08	08:CC:A7:5F:06:08	Unknown	Wired_C9200L >> Wired_MAB >> Default	Wired_C9200L >> Permit_all	PermitAccess
2019-01-10 05:46:59.912			6	user2	28:52:61:68:D1:01	Unknown	Wired_C9200L >> Wired_dot1x >> Default	Wired_C9200L >> vlan212	vlan212_permit
2019-01-10 05:46:57.288			4	user1	2C:08:E9:AD:AD:81	Unknown	Wired_C9200L >> Wired_dot1x >> Default	Wired_C9200L >> vlan211	vlan211_permit
2019-01-10 05:44:36.602			0	28:52:61:68:D1:41	28:52:61:68:D1:41	Unknown	Wired_C9200L >> Wired_MAB >> Default	Wired_C9200L >> Permit_all	PermitAccess

認証ログの確認 2

Overview

Event	5200 Authentication succeeded
Username	user2
Endpoint Id	28:52:61:68:D1:01
Endpoint Profile	Unknown
Authentication Policy	Wired_C9200L >> Wired_dot1x >> Default
Authorization Policy	Wired_C9200L >> vlan212
Authorization Result	vlan212_permit

Result

State	ReauthSession:A51E0A0A0000004735E2C9F0
Class	CACS:A51E0A0A0000004735E2C9F0:ise20a/336458508/30
Tunnel-Type	(tag=1) VLAN
Tunnel-Medium-Type	(tag=1) 802
Tunnel-Private-Group-ID	(tag=1) 212
cisco-av-pair	profile-name=Unknown
License Types	1

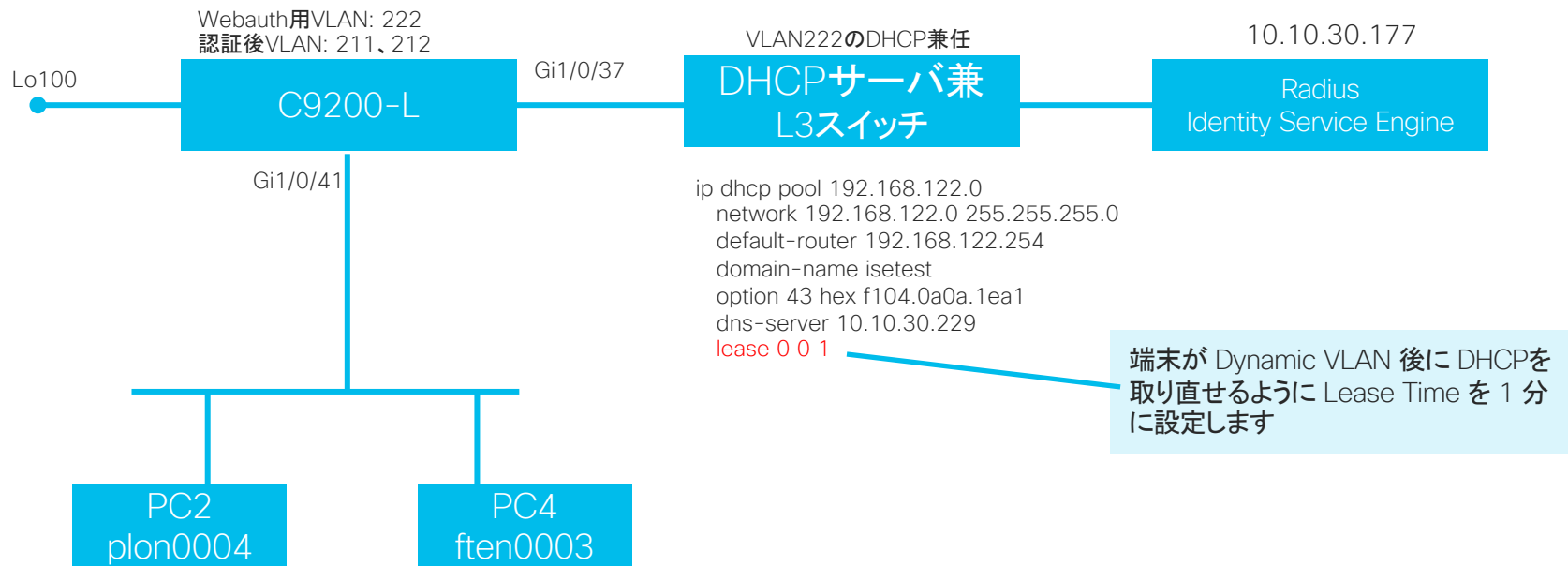
Authentication Details

Source Timestamp	2019-01-10 04:01:41.787
Received Timestamp	2019-01-10 04:01:41.788
Policy Server	ise20a
Event	5200 Authentication succeeded
Username	user2
User Type	User
Endpoint Id	28:52:61:68:D1:01
Calling Station Id	28-52-61-68-D1-01
Endpoint Profile	Unknown
Authentication Identity Store	Internal Users
Identity Group	User Identity Groups:vlan212,Unknown

Authentication Method	dot1x
Authentication Protocol	EAP-MD5
Service Type	Framed
Network Device	C9200L
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	10.10.30.165
NAS Port Id	GigabitEthernet1/0/11
NAS Port Type	Ethernet
Authorization Profile	vlan212_permit
Response Time	7

設定例② CWA Multi 認証 + Dynamic VLAN

Cisco Catalyst 9200 L で CWA Multi 認証 → ユーザごとに Dynamic VLAN を動作させる設定例



3.5 Security

CWA Multi 認証 設定例

```
aaa new-model
aaa group server radius ISE
 server name radius
aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa server radius dynamic-author
 client 10.10.30.177 server-key cisco
!
dot1x system-auth-control
!
!
interface GigabitEthernet1/0/37
 switchport access vlan 222
 switchport mode access
!
interface GigabitEthernet1/0/41
 switchport access vlan 222
 switchport mode access
 device-tracking
 authentication host-mode multi-auth
 authentication order mab
 authentication port-control auto
 mab
 spanning-tree portfast
```

CoA 設定

Device-Tracking 有効が必須です

```
interface Vlan222
 ip address 192.168.122.155 255.255.255.0
!
ip http server
ip http secure-server
!
ip access-list extended redirect
 deny icmp any any
 deny udp any any eq domain
 deny udp any any eq bootps
 deny ip any host 10.10.30.177
 permit tcp any any eq www
 permit tcp any any eq 443
!
ip radius source-interface Vlan222
!
snmp-server community public RO
!
!
radius server radius
 address ipv4 10.10.30.177 auth-port 1812 acct-port 1813
 key cisco
```

ISE で設定する redirect と同じ
名前で ACL 作成が必要です

ISE 設定サンプル

Download ACL の定義

CWA 用にアクセス許可する ACL を DACL として登録

Downloadable ACL List > Temp_Cat2kx

Downloadable ACL

* Name

Description

* DACL Content

1234567	permit icmp any any
8910111	permit udp any any eq domain
2131411	permit ip any host 10.10.30.177
1617181	
9202122	
2324252	
6272829	
3031323	
3343536	
3738394	

▶ Check DACL Syntax

ISE の IP アドレス

3.5 Security

ISE 設定サンプル

WEB 認証の認可プロファイルの設定

Authorization Profiles > CWA_Test

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Common Tasks

DACL Name

CWA 用の Authorization Profile を作成

下記を選択

Web Redirecton: CWA

ACL: redirect

Value: Self-registration Guest Portal

Common Tasks

Web Redirection (CWA, MDM, NSP, CPP)

Centralized Web Auth

ACL

Value

Display Certificates Renewal Message

Static IP/Host name/FQDN

先ほど作成した DACL を選択します

Attributes Details

Access Type = ACCESS_ACCEPT

DACL = Temp_Cat2kX

cisco-av-pair = url-redirect-acl=redirect

cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=0ce17ad0-6d90-11e5-978e-005056bf2f0a&action=cwa

完成した Attribute を確認します

ISE 設定サンプル

WEB 認証後の認可プロファイルの設定

Dynamic VLAN 用の Authorization Profile を作成

Authorization Profiles > **vlan211_permit**

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

▼ **Common Tasks**

DACL Name

ACL (Filter-ID)

VLAN

▼ **Attributes Details**

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:211
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6

完成した Attribute を確認します

VLAN211 に移動させる設定

ISE 設定サンプル

WEB 認証後の認可プロファイルの設定

Dynamic VLAN 用の Authorization Profile を作成

Authorization Profiles > **vlan212_permit**

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

▼ **Common Tasks**

DAACL Name

ACL (Filter-ID)

VLAN Tag ID ID/Name

▼ **Attributes Details**

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:212
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6

完成した Attribute を確認します

VLAN212 に移動させる設定

ISE 設定サンプル

Policy Sets の設定

▼ Authentication Policy

Identity Source Details

Name Internal Endpoints

Options

If authentication failed REJECT

If user not found CONTINUE

If process failed DROP

Wired_MAB で、If user not found 時に、CONTINUE を選択します

▼ Authorization Policy

▶ Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Guest2	GuestType_Guest1 AND Network Access:UseCase EQUALS Guest Flow	then vlan212_permit
✓	Guest1	Network Access:UseCase EQUALS Guest Flow	then vlan211_permit
✓	CWA	Session:PostureStatus EQUALS Unknown	then CWA_Test

Condition:
Identity Group: GuestType_Guest1 AND
Network Access: UseCase EQUALS Guest Flow
Permission:
Vlan212_permit(先ほど作成したAuthZ Profile)

Condition:
Network Access: UseCase EQUALS Guest Flow
Permission:
vlan211_permit(先ほど作成したAuthZ Profile)

Condition:
Session: PostureStatus EQUALS Unknown
Permission:
CWA_Test(先ほど作成したAuthZ Profile)

認証ログの確認

Plon0004 には、vlan211_permit がアサイン

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device
2019-02-26 00:40:59.713			0	plon0004	00:0C:29:DC:E7:08	Windows10-Works...	Wired_C9200L >> Wir...	Wired_C9200L >> Gu...	vlan211_permit	
2019-02-26 00:40:59.713				plon0004	00:0C:29:DC:E7:08	Windows10-Works...	Wired_C9200L >> Wir...	Wired_C9200L >> Gu...	vlan211_permit	C9200L
2019-02-26 00:40:59.707					00:0C:29:DC:E7:08					C9200L
2019-02-26 00:40:58.103				plon0004	00:0C:29:DC:E7:08					
2019-02-26 00:37:56.703			0	ften0003	00:0C:29:EC:D0:B4	Windows10-Works...	Wired_C9200L >> Wir...	Wired_C9200L >> Gu...	vlan212_permit	
2019-02-26 00:37:56.703				ften0003	00:0C:29:EC:D0:B4	Unknown	Wired_C9200L >> Wir...	Wired_C9200L >> Gu...	vlan212_permit	C9200L
2019-02-26 00:37:56.695					00:0C:29:EC:D0:B4					C9200L
2019-02-26 00:37:54.060				ften0003	00:0C:29:EC:D0:B4					
2019-02-26 00:37:52.397			0	00:50:56:57:CA:1	00:50:56:57:CA:BA	VMWare-Device	Wired_C9200L >> Wir...	Wired_C9200L >> CWA	CWA_Test	
2019-02-26 00:37:52.397				00:50:56:57:CA:1	00:50:56:57:CA:BA	VMWare-Device	Wired_C9200L >> Wir...	Wired_C9200L >> CWA	CWA_Test	C9200L
2019-02-26 00:37:52.396			0	00:50:56:5A:40:1	00:50:56:5A:40:2C	VMWare-Device	Wired_C9200L >> Wir...	Wired_C9200L >> CWA	CWA_Test	
2019-02-26 00:37:52.396				00:50:56:5A:40:1	00:50:56:5A:40:2C	VMWare-Device	Wired_C9200L >> Wir...	Wired_C9200L >> CWA	CWA_Test	C9200L
2019-02-26 00:37:11.416			1	00:0C:29:BD:D1:1	00:0C:29:BD:D1:12	VMWare-Device	Wired_C9200L >> Wir...	Wired_C9200L >> CWA	CWA_Test	
2019-02-26 00:37:11.209			1	00:0C:29:8F:15:E	00:0C:29:8F:15:E1	VMWare-Device	Wired_C9200L >> Wir...	Wired_C9200L >> CWA	CWA_Test	

Ften0003 には、vlan212_permit がアサイン

3.5 Security

CWA 後の Device Tracking DB

```
C9200-1#show device-tracking database
```

```
Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
```

```
No time source, *04:08:20.008 UTC Tue Feb 26 2019
```

```
Binding Table has 12 entries, 10 dynamic (limit 100000)
```

```
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol, DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
```

```
Preflevel flags (prlvl):
```

```
0001:MAC and LLA match    0002:Orig trunk        0004:Orig access
```

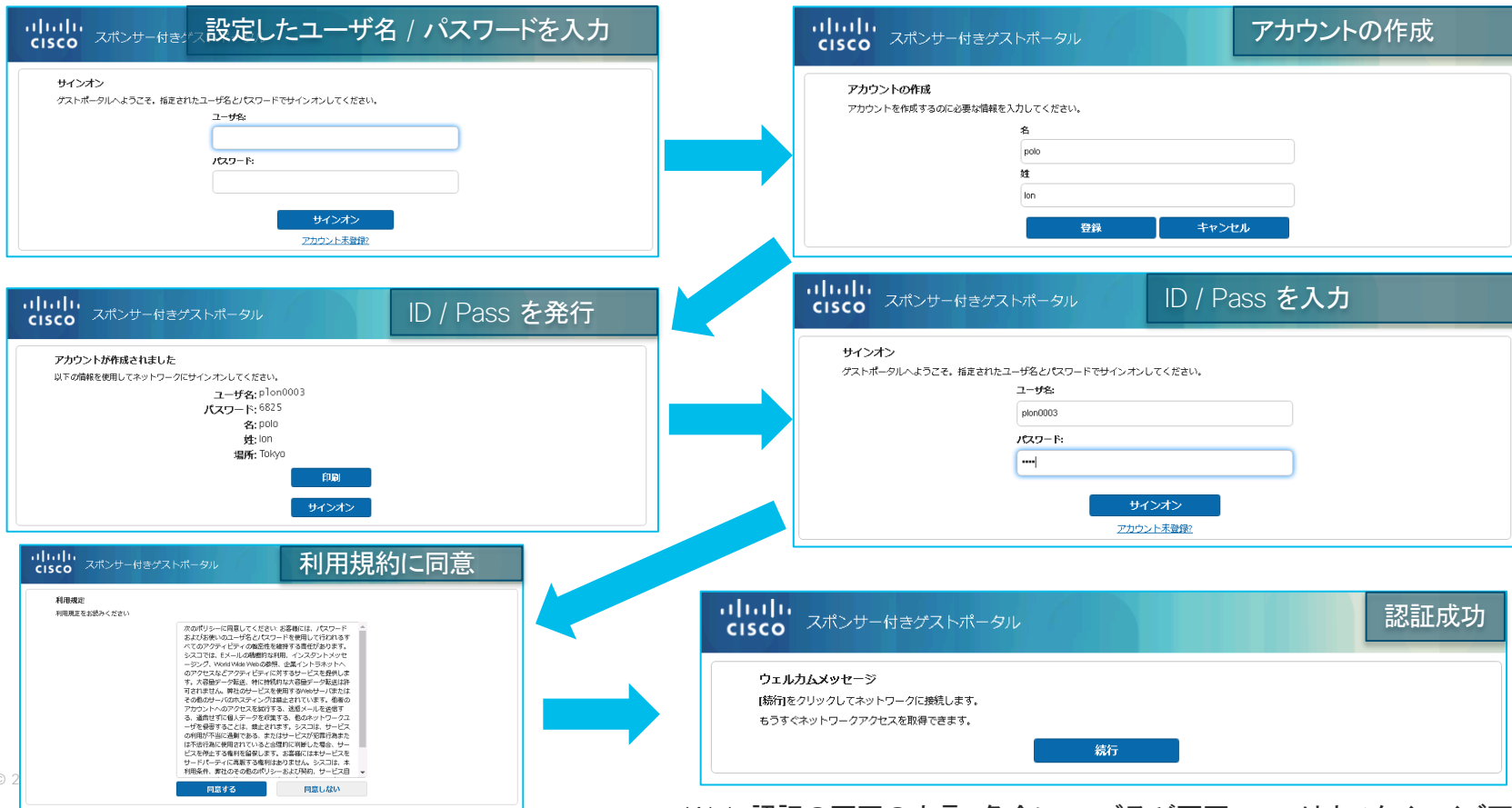
```
0008:Orig trusted trunk  0010:Orig trusted access  0020:DHCP assigned
```

```
0040:Cga authenticated   0080:Cert authenticated  0100:Statically assigned
```

DTDB には両方の端末情報が保存されます

Network Layer Address	Link Layer Address	Interface	vlan	prlvl	age	state	Time left
L 212.212.212.254	70b3.17fa.f15a	VI212	212	0100	157mn	REACHABLE	
DH4 212.212.212.1	000c.29ec.d0b4	Gi1/0/41	212	0025	36s	REACHABLE	268 s(84669 s)
L 211.211.211.254	70b3.17fa.f141	VI211	211	0100	6976mn	REACHABLE	
DH4 211.211.211.87	000c.29dc.e708	Gi1/0/41	211	0025	66s	REACHABLE	236 s(84859 s)
ARP 211.211.211.85	2c86.d25f.e9c1	Gi1/0/48	211	0005	1s	REACHABLE	307 s(49090 s)
DH4 211.211.211.82	5897.bd31.bf52	Gi1/0/48	211	0025	35s	REACHABLE	275 s try 0(48861 s)
ARP 192.168.202.13	000c.29bd.d112	Gi1/0/41	222	0005	28s	REACHABLE	280 s
ARP 192.168.201.12	000c.29dc.e708	Gi1/0/41	211	0005	26mn	STALE	84486 s
ARP 192.168.201.11	000c.298f.15e1	Gi1/0/41	222	0005	30s	REACHABLE	281 s
ARP 192.168.122.110	000c.29dc.e708	Gi1/0/41	211	0005	25mn	STALE	85358 s
ARP 192.168.122.108	000c.29dc.e708	Gi1/0/41	211	0005	26mn	STALE	83302 s
ARP 169.254.234.131	000c.29dc.e708	Gi1/0/41	211	0005	25mn	STALE	85840 s

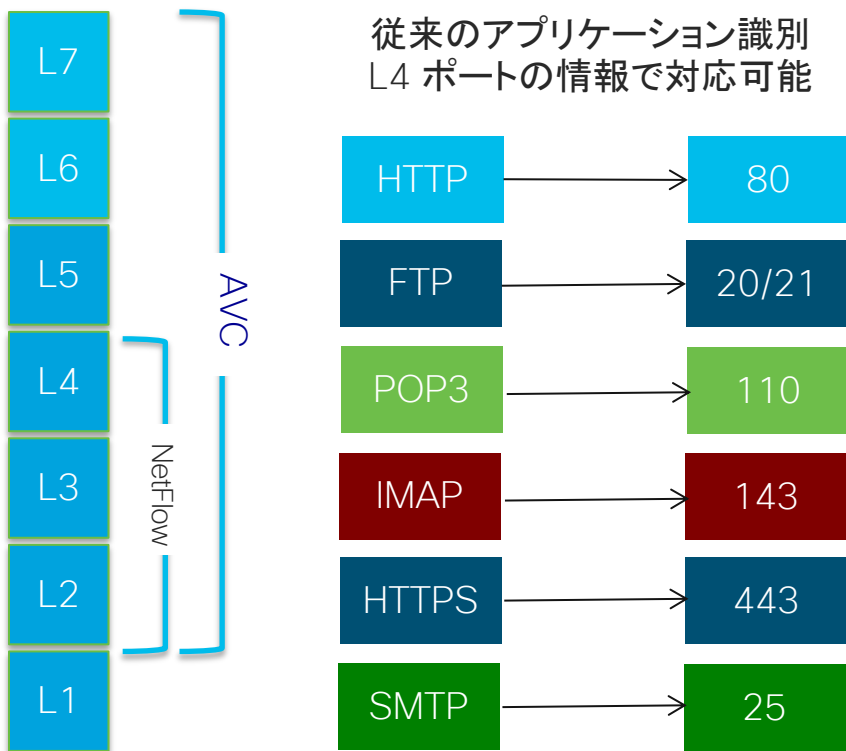
ISE での WEB 認証フロー サンプル



3.6 AVC

AVC

ネットワーク可視化の課題



昨今のアプリケーション

GMail	Exchange
BitTorrent	SAP
skype	iTunes
CiTRiX	Rhapsody
SharePoint	Webex
You Tube	talk

同一の L4 ポート(例:TCP:80)を利用するさまざまなアプリケーションを識別する必要があるため、上位レイヤの情報の収集が必要です

AVC 機能

A Application Recognition (アプリケーション認識)

- 次世代ディープ パケット インスペクション技術
NBAR2: Network Based Application Recognition 2
- ダイナミック / プロトコル パックアップ グレード
- カスタム アプリケーション

V Visibility (可視化)

- プロトコル ディスカバリ - インターフェイス単位、方向単位 (in,out)
- Flexible NetFlow を利用したアプリケーション情報の収集

C Control (制御)

- アプリケーション ベース QOS

AVC 機能とライセンス

	Cisco Catalyst 9500H 9600	Cisco Catalyst 9500/9400 9300/9300L	Cisco Catalyst 9200/9200L	備考
Flexible NetFlow	○	○	○	Cisco DNA Essentials ライセンスが必要です。
NBAR2	×	○*	×	C95/93 以上で、かつ Cisco DNA Advantage ライセンスが必要です。
Application Base QoS	×	○*	×	C95/93 以上で、かつ Cisco DNA Advantage ライセンスが必要です。

Flexible NetFlow 設定

Cisco DNA Essentials 以上で利用可能な汎用的な設定例

```
flow record IPv4_INGRESS
match ipv4 version
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match interface input
match ipv4 tos
collect interface output
collect counter bytes long
collect counter packets long
```

適用インターフェイス方向は **input** を想定しています。Output の場合は **match interface out** に変更必要。
方向ごとの適用可能な **match** 情報の詳細はコンフィグガイドをご確認ください。

```
flow exporter NETFLOW_TO_STEALTHWATCH
description Export Netflow to Stealthwatch
destination 10.10.31.100
transport udp 2055
```

VRF を利用した **destination** 指定も可能だが管理ポート (Gi0/0)からは **Export** はサポートされません。設定できても正しく情報が転送されません。

```
flow monitor IPv4_NETFLOW_IN
record IPv4_INGRESS
exporter NETFLOW_TO_STEALTHWATCH
cache timeout active 60
```

フローコレクターとして **Stealthwatch** を想定しています。PI の場合はポート番号 **9991** です。ご利用予定のフローコレクタに合わせて変更してください。

Flexible NetFlow 設定

Cisco DNA Essentials 以上で利用可能な汎用的な設定例

■ 事前に定義した monitor 情報を物理インターフェイスか、もしくは VLAN に設定

*SVIインターフェイスに適用できません

1. 物理インターフェイスで情報を収集する場合の設定

*必要なインターフェイスに全て投入する必要があります

```
interface GigabitEthernet1/0/1
switchport access vlan 10
switchport mode access
ip flow monitor IPv4_NETFLOW_IN input
```

2. VLAN 上で適用する場合

*VLAN 内を通過する全ての通信を収集可能で、VLAN ごとに適用可否を設定できます

```
vlan configuration 10
ip flow monitor IPv4_NETFLOW_IN input
```

Flexible NetFlow 設定

Cisco DNA Essentials 以上で利用可能な汎用的な設定例

■ 動作確認 : Gi1/0/1 配下の端末からの TELNET 通信を監視

```
C9200-2#show flow monitor IPv4_NETFLOW_IN cache
```

```
Cache type:           Normal (Platform cache)
```

```
Cache size:           10000
```

```
Current entries:      0
```

```
Flows added:          6
```

```
Flows aged:           6
```

```
- Inactive timeout   ( 15 secs)   6
```

```
IPV4 SOURCE ADDRESS: 172.16.1.200
```

```
IPV4 DESTINATION ADDRESS: 172.16.1.2
```

```
TRNS SOURCE PORT:    32865
```

```
TRNS DESTINATION PORT: 23
```

```
INTERFACE INPUT:     Gi1/0/1
```

```
IP VERSION:          4
```

```
IP TOS:               0xC0
```

```
IP PROTOCOL:         6
```

```
interface output:    Null
```

```
counter bytes long:  515
```

```
counter packets long: 11
```

C9200L は output interface が Nullとなります
C9300/C9500は output interface も収集可能です

3.6 AVC

Flexible NetFlow 設定

Cisco DNA Advantage でアプリケーション情報を取得する場合の設定例

```
flow record LANCOPE1_IN
match ipv4 version
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match interface input
match application name
collect interface output
collect counter bytes long
collect counter packets long
collect timestamp absolute first
collect timestamp absolute last
```

```
flow exporter NETFLOW_TO_STEALTHWATCH
description Export Netflow to Stealthwatch
destination 10.10.31.100
transport udp 2055
```

```
flow monitor IPv4_NETFLOW
exporter NETFLOW_TO_STEALTHWATCH
cache timeout active 60
record LANCOPE1_IN
```

match application name でアプリケーション情報を収集します
match ipv4 tos は利用できないため削除してください
アプリケーション情報を収集する場合はこの条件以上の条件は投入できません

Flexible NetFlow 設定

Cisco DNA Advantage でアプリケーション情報を取得する場合の設定例

■ 事前に定義した monitor 情報を物理インターフェイスに設定

*アプリケーション情報を収集する場合は物理インターフェイスに適用する必要があります

*VLAN でも設定はできるが情報が収集されません

```
interface GigabitEthernet1/0/3
switchport access vlan 10
switchport mode trunk
ip flow monitor IPv4_NETFLOW input
```

Flexible NetFlow 設定

Cisco DNA Advantage でアプリケーション情報を取得する場合の設定例

■ 動作確認 : Gi1/0/3 配下の端末からの TELNET 通信を監視

```
C9300-2#show flow monitor IPv4_NETFLOW cache
Cache type:          Normal (Platform cache)
Cache size:          10000
Current entries:     1
```

```
Flows added:         22
Flows aged:          21
- Inactive timeout ( 15 secs)  21
```

```
IPV4 SOURCE ADDRESS: 172.16.1.200
IPV4 DESTINATION ADDRESS: 172.16.1.2
TRNS SOURCE PORT:    13913
TRNS DESTINATION PORT: 23
INTERFACE INPUT:     Gi1/0/3
IP VERSION:          4
IP PROTOCOL:          6
APPLICATION NAME:     port telnet
interface output:    Gi1/0/2
counter bytes long:   757
counter packets long: 11
timestamp abs first: 19:18:11.801
timestamp abs last:  19:18:11.801
```

C9300 で APPLICATION NAMEが収集できていることを確認

C9300 では output interface も収集できている

NBAR2 単体設定

Cisco DNA Advantage でアプリケーション情報を NBAR2 のみで取得する場合の設定例

■ 設定方法

```
interface GigabitEthernet1/0/3
switchport access vlan 10
switchport mode trunk
ip nbar protocol-discovery
```

■ 動作確認

```
C9300-2#show ip nbar protocol-discovery top-n
```

```
GigabitEthernet1/0/3
```

Protocol	Input	Output
	Packet Count	Packet Count
	Byte Count	Byte Count
	5min Bit Rate (bps)	5min Bit Rate (bps)
	5min Max Bit Rate (bps)	5min Max Bit Rate (bps)
telnet	315	256
	21591	18621
	0	0
	1000	1000
Total	315	256
	21591	18621
	0	0
	1000	1000

NetFlow でアプリケーション情報を取得する場合は、nbar設定と FNF 設定を同じインターフェース上に適用可能ですが、アプリケーション情報を取得しない FNF 設定は投入できないため、NBAR2 をインターフェースに設定した場合、FNF は VLAN に設定する必要があります

設定したインターフェースでどのプロトコルがどの程度利用されているか確認が可能です。NetFlow と異なり送信元/宛先の IP などは分かりません

3.6 AVC

NBAR2 単体設定

Cisco DNA Advantage でアプリケーション情報を NBAR2 のみで取得する場合の設定例

NBAR2 情報は WEB 管理画面での設定 / 表示も可能です

アプリケーションの可視性

Enable AVC

ポリシーの定義

1

インターフェイスを追加/削除するには、ドラッグアンドドロップまたはダブルクリックするか、(選択済みインターフェイス)に対応するボタンをクリックします。

使用可能(39)

有効(1)

すべてを有効化

表示画面は、全体かインターフェイスごとに表示可能です

アプリケーションの可視性

送信元のタイプ: インターフェイス

方向: 両方

使用状況

1.20pps

756.40pps

393.20pps

0pps

17.45 18.00 18.15 18.30 18.45 19.00 19.15 19.30

100.0%

ビジネス関連 スキャンング デフォルト

アプリケーション	使用率(%)	使用状況	受信	送信
Teinnet	100.00	39.3KB	21.1KB	18.2KB

設定画面は監視したいインターフェイスをクリックするだけで設定できます

プロトコルパック

Cisco DNA Advantage での設定例

NBAR2 においてアプリケーション識別を行うシグニチャは、プロトコル パックとして数か月ごとに提供され、無停止でアップデートが可能です。

- プロトコル パックのアップデート コマンド、適用後即時反映され、通信に影響はありません

```
C9300-2(config)#ip nbar protocol-pack flash:pp-adv-cat9k-169.1-34-42.0.0.pack
```

```
C9300-2#show ip nbar version
```

```
NBAR software version: 34
NBAR minimum backward compatible version: 34
```

```
Loaded Protocol Pack(s):
```

```
Name:          Advanced Protocol Pack
Version:       38.0
Publisher:     Cisco Systems Inc.
NBAR Engine Version: 34
State:        Active
```

プロトコル パック
アップデート前と後のバージョンを確認できます

```
C9300-2#show ip nbar version
```

```
NBAR software version: 34
NBAR minimum backward compatible version: 34
```

```
Loaded Protocol Pack(s):
```

```
Name:          Advanced Protocol Pack
Version:       42.0
Publisher:     Cisco Systems Inc.
NBAR Engine Version: 34
Creation time: Thu Mar 28 10:40:34 UTC 2019
File:         flash:pp-adv-cat9k-169.1-34-42.0.0.pack
State:        Active
```

4

実装編

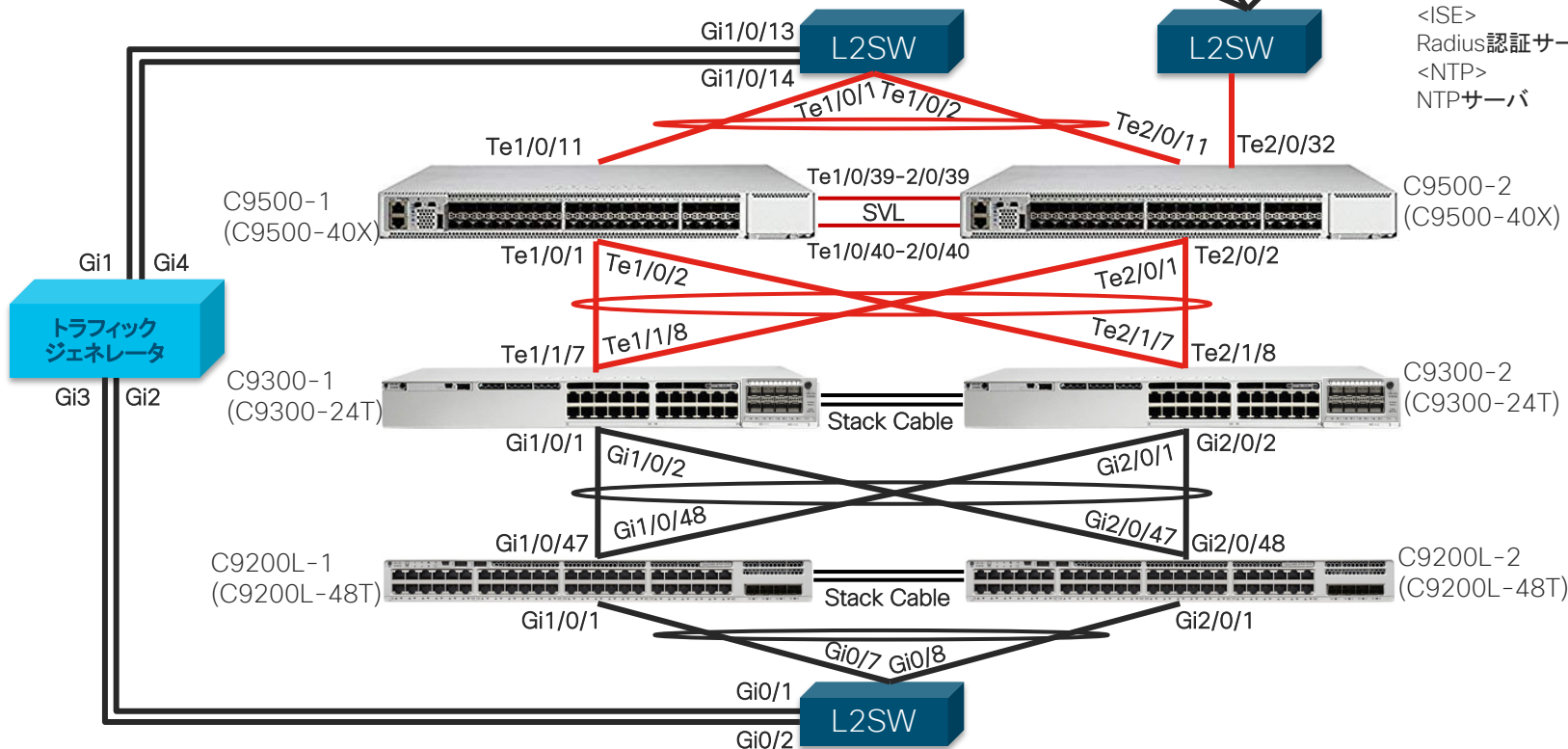
- 4.1 ネットワーク構成例
- 4.2 構成のポイント
- 4.3 コンフィギュレーション

4.1 ネットワーク 構成例

4.1 ネットワーク構成例

物理構成図

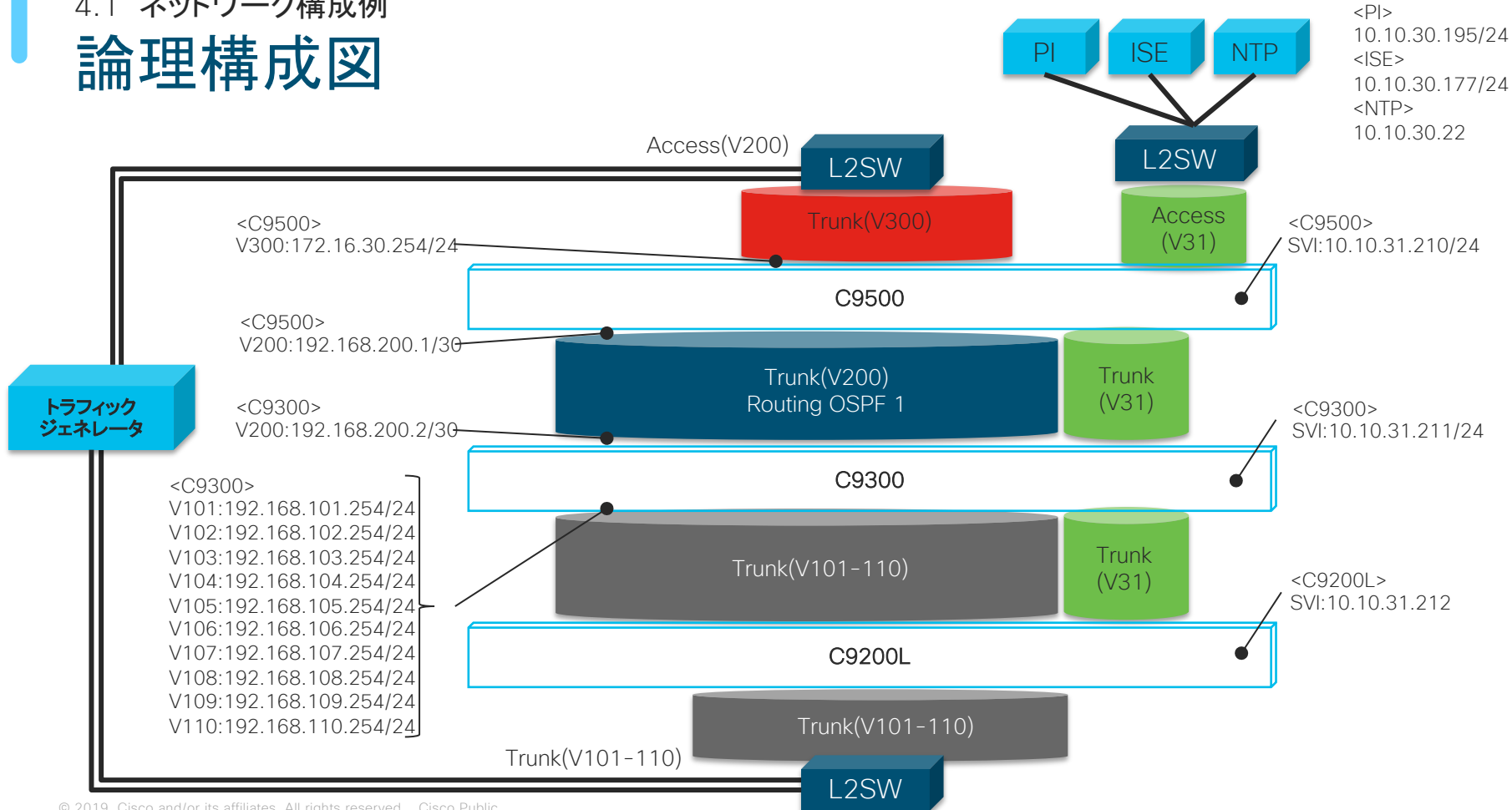
※ IOS-XE 16.9.3 で検証



— 10Giga(光)
— 1Giga(UTP)



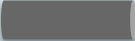

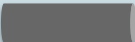



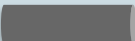




<PI>
SNMP, Syslog, NetFlow
<ISE>
Radius認証サーバ
<NTP>
NTPサーバ

4.1 ネットワーク構成例 論理構成図



4.1 ネットワーク構成例

セグメント体系

VLAN 番号	アドレス体系	使用用途	使用色	備考
31	10.10.31.0/24	管理セグメント		ユーザセグメントとは分離
101	192.168.101.0/24	ユーザ利用セグメント 1		D/G は C9300
102	192.168.102.0/24	ユーザ利用セグメント 2		〃
103	192.168.103.0/24	ユーザ利用セグメント 3		〃
104	192.168.104.0/24	ユーザ利用セグメント 4		〃
105	192.168.105.0/24	ユーザ利用セグメント 5		〃
106	192.168.106.0/24	ユーザ利用セグメント 6		〃
107	192.168.107.0/24	ユーザ利用セグメント 7		〃
108	192.168.108.0/24	ユーザ利用セグメント 8		〃
109	192.168.109.0/24	ユーザ利用セグメント 9		〃
110	192.168.110.0/24	ユーザ利用セグメント 10		〃
200	192.168.200./30	コア - ディストスイッチ間セグメント		OSPF によるルーティング
300	172.16.30.0/24	サーバセグメント		D/G は C9500

構成機器

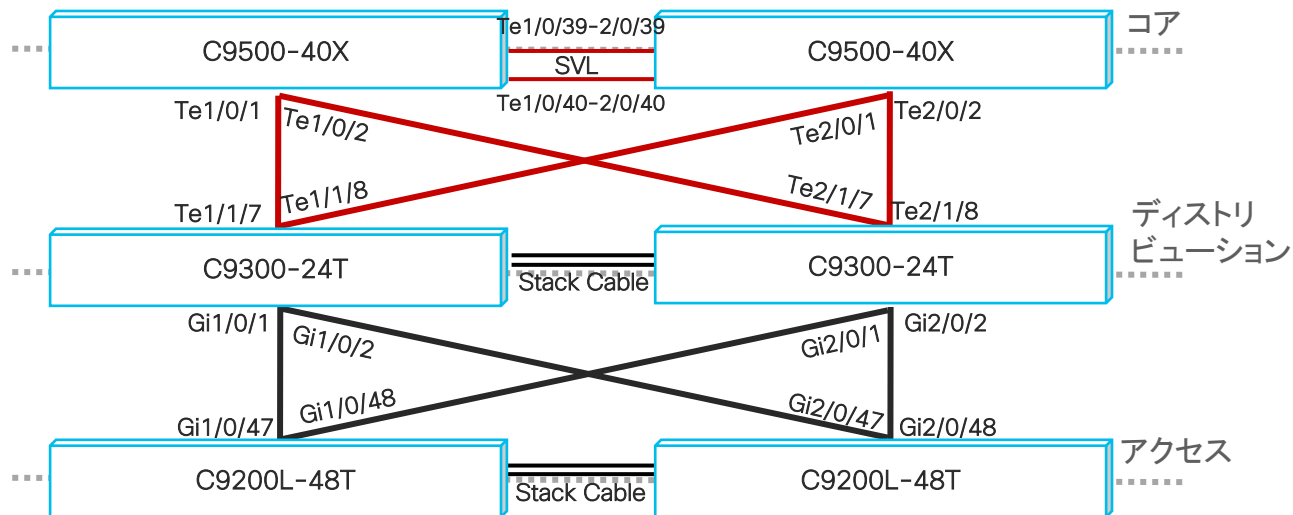
役割	名称	機種	OS version	ライセンス
コア	C9500-1	C9500-40X	16.9.3	Network Advantage Cisco DNA Advantage
	C9500-2	C9500-40X	16.9.3	Network Advantage Cisco DNA Advantage
ディストリビューション	C9300-1	C9300-24T	16.9.3	Network Advantage Cisco DNA Advantage
	C9300-2	C9300-24T	16.9.3	Network Advantage Cisco DNA Advantage
アクセス	C9200L-1	C9200L-48P	16.9.3	Network Essentials Cisco DNA Essentials
	C9200L-2	C9200L-48P	16.9.3	Network Essentials Cisco DNA Essentials

4.2 構成のポイント

4.2 構成のポイント

物理構成

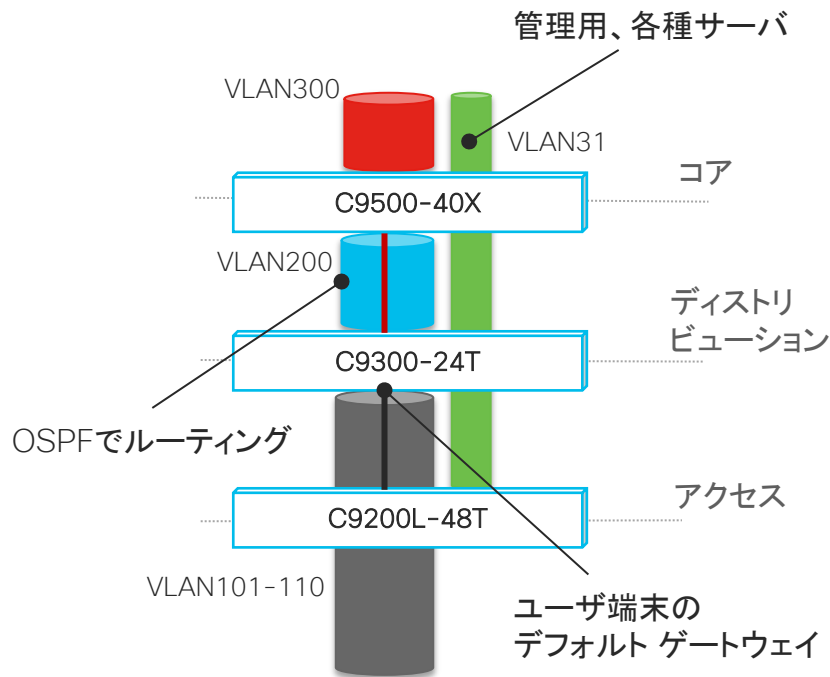
- コア - ディストリビューション間は 10G イーサネット(光ファイバ)
- ディストリビューション - アクセス間は 1G イーサネット(UTP)



論理構成

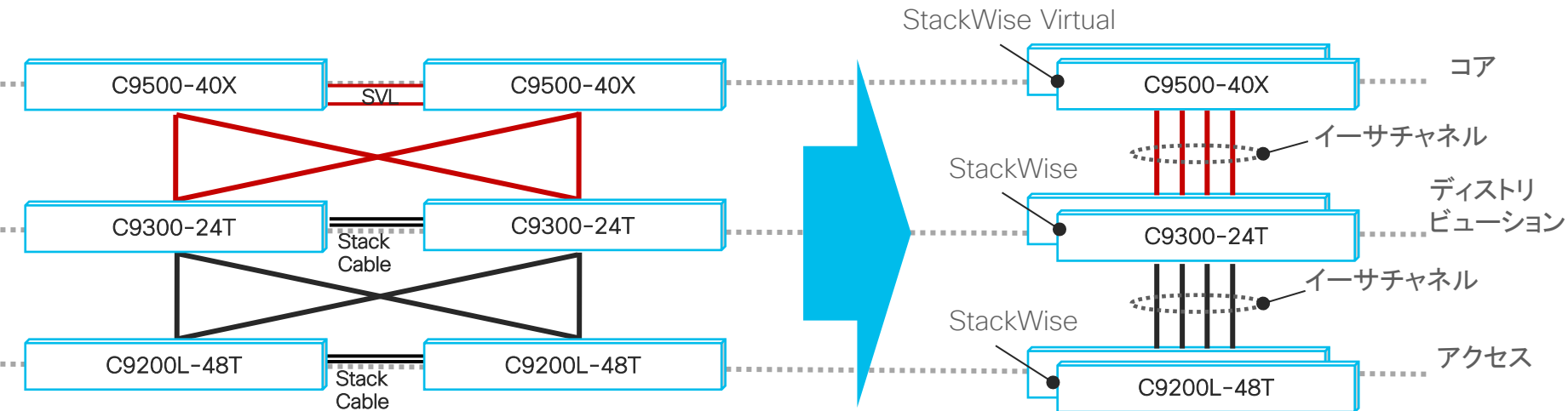
■ 論理構成

- コア、ディストリビューション スイッチは L3
 - アクセス スイッチは L2
 - VLAN ベースで構成し、L3 については SVI を利用
 - ユーザ端末のデフォルト ゲートウェイはディストリビューション スイッチ
 - コア - ディストリビューション間には OSPF でルーティング
 - 管理用、各種サーバ セグメントは VRF にて論理分割
- ※但し、アクセス スイッチは VRF 未対応



冗長構成

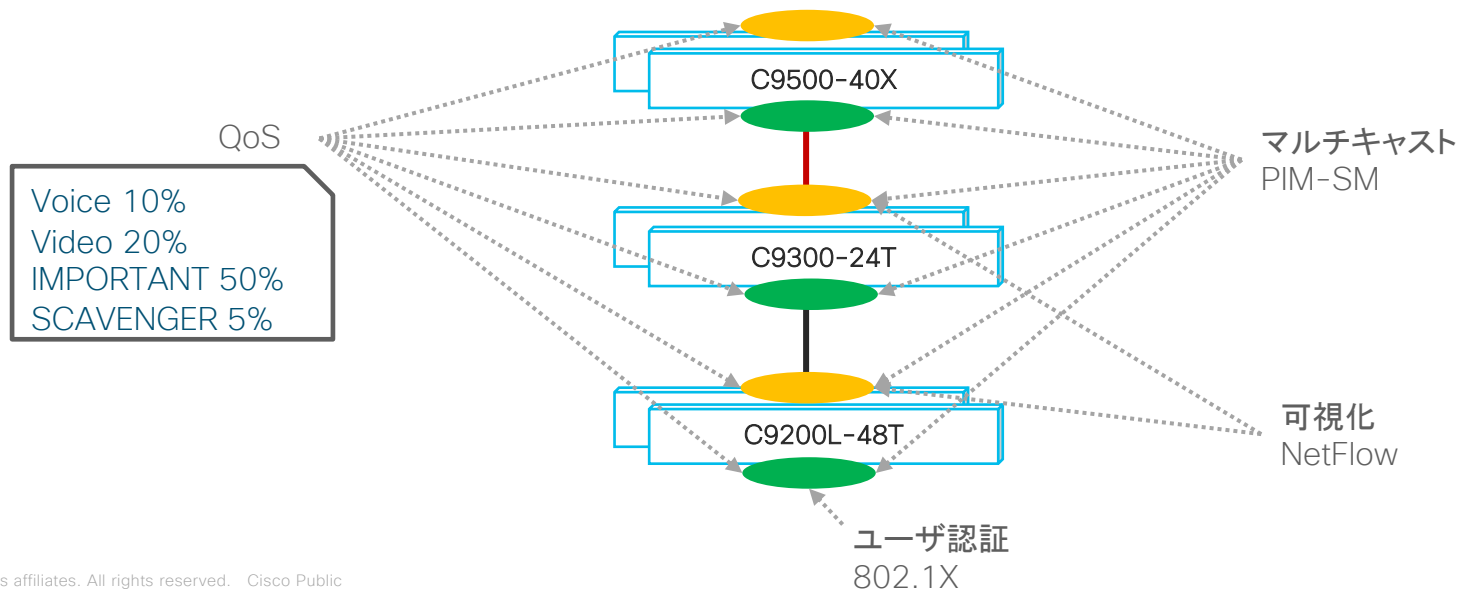
コア、ディストリビューション、アクセススイッチは全て筐体冗長とし、イーサ チャンネルによる経路冗長構成とする



4.2 構成のポイント

主要な機能

- QoS : 電話、ビデオ、重要トラフィック、その他トラフィックの帯域を制御
- マルチキャスト : ビデオ配信に対応するため、マルチキャスト PIM-SM を設定
- 認証 : ユーザを 802.1X で認証
- 可視化 : フロー情報を可視化するため、NetFlow を設定



4.2 構成のポイント

関連コンフィギュレーション

■ QoS

```
!  
policy-map Queueing  
  class VoIP  
    priority level 1 percent 10  
  class VIDEO  
    priority level 2 percent 20  
  class IMPORTANT  
    bandwidth remaining percent 50  
  class SCAVENGER  
    bandwidth remaining percent 5  
policy-map system-cpp-policy  
!  
.....  
!  
interface GigabitEthernet1/0/1  
  switchport trunk allowed vlan 31,101-110  
  switchport mode trunk  
  load-interval 30  
  channel-group 2 mode active  
  service-policy output Queueing  
!
```

■ マルチキャスト(PIM-SM)

```
!  
ip multicast-routing  
ip domain name cisco.com  
!  
.....  
!  
interface Vlan200  
  ip address 192.168.200.1 255.255.255.252  
  ip pim sparse-mode  
  ip ospf network point-to-point  
  ip ospf 1 area 0  
!  
.....  
!  
ip forward-protocol nd  
ip pim bsr-candidate Vlan200 0  
ip pim rp-candidate Vlan200  
!
```

4.2 構成のポイント

関連コンフィギュレーション

■ 認証 (802.1X)

```
aaa new-model
!
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
!
aaa server radius dynamic-author
  client 10.10.30.177 server-key cisco
  auth-type all
!
radius server ISE
  address ipv4 10.10.30.177 auth-port 1812 acct-port 1813
  key cisco
!
interface GigabitEthernet1/0/1
  switchport mode access
  device-tracking
  authentication host-mode multi-auth
  authentication order dot1x mab
  authentication port-control auto
  authentication periodic
  mab
  dot1x pae authenticator
  spanning-tree portfast
```

■ 可視化 (NetFlow)

```
!
flow record FLOW_RECORD
  match ipv4 version
  match ipv4 protocol
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  collect counter bytes long
  collect counter packets long
  collect timestamp absolute first
  collect timestamp absolute last
!
!
flow exporter NETFLOW_TO_PI
  description Export Netflow to PI
  destination 10.10.30.195
  source Loopback0
  transport udp 9991
!
!
flow monitor IPv4_NETFLOW
  exporter NETFLOW_TO_PI
  cache timeout active 60
  record FLOW_RECORD
!
!
interface GigabitEthernet2/0/47
  switchport trunk allowed vlan 31,101-110
  switchport mode trunk
  ip flow monitor IPv4_NETFLOW input
  ip flow monitor IPv4_NETFLOW output
  load-interval 30
  macsec network-link
  mka policy macsectest
  mka pre-shared-key key-chain macsectest
  channel-group 1 mode active
  service-policy output Queueing
!
```

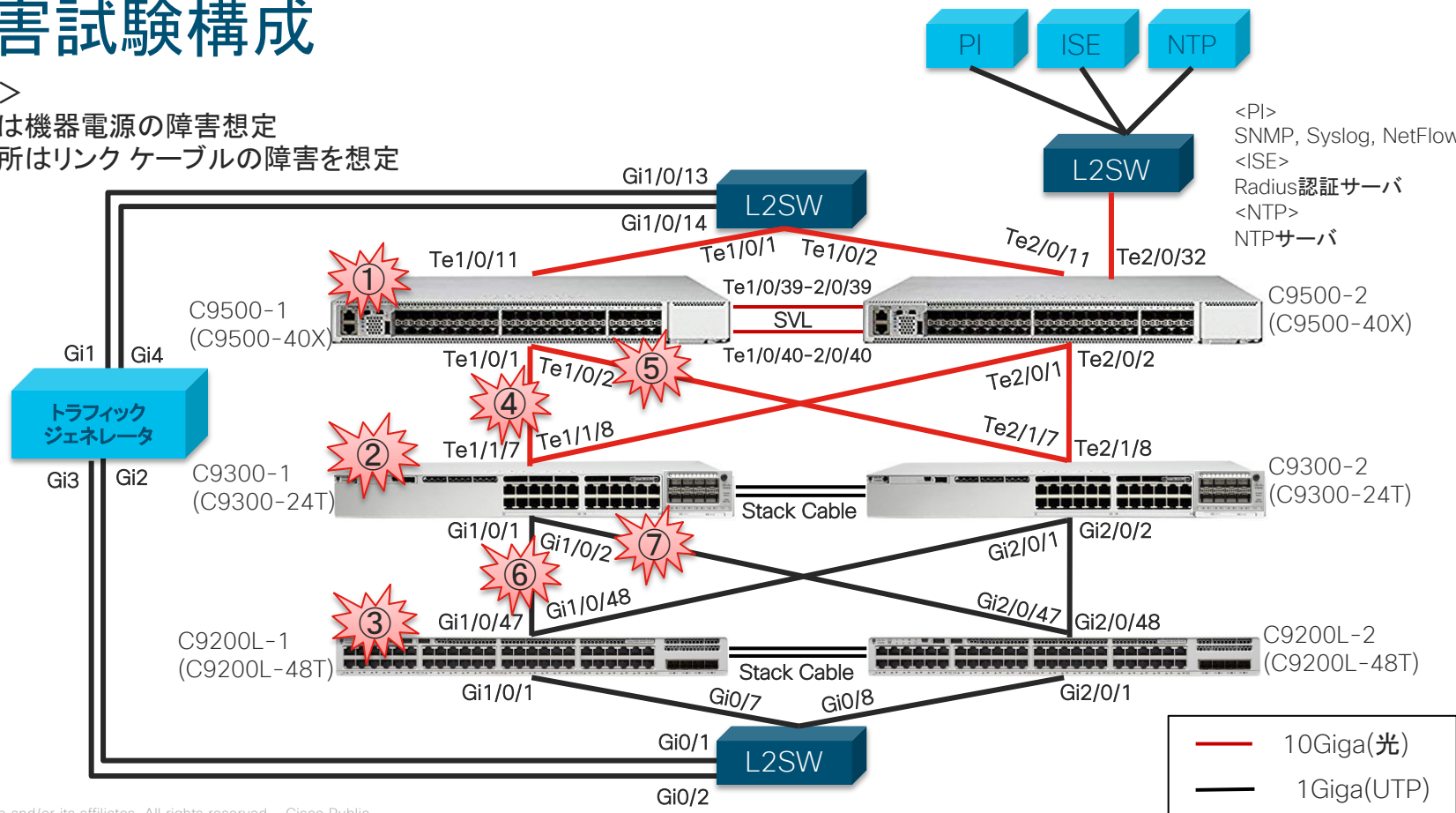
4.2 構成のポイント

障害試験構成

<検証箇所>

①②③箇所は機器電源の障害想定

④⑤⑥⑦箇所はリンク ケーブルの障害を想定



4.2 構成のポイント



障害試験結果

障害パターン	ダウン リンク		アップ リンク		備考
	切断 (ミリ秒)	切り戻し (ミリ秒)	切断 (ミリ秒)	切り戻し (ミリ秒)	
① C9500-1 電源障害	26	9	29	7	
② C9300-1 電源障害	67	18	69	20	
③ C9200-1 電源障害	1680	20	1557	9	
④ C9500-1 リンク障害 Te1/0/1	4	4	93	4	
⑤ C9500-1 リンク障害 Te1/0/2	4	3	127	20	
⑥ C9300-1 リンク障害 Gi1/0/1	0	3	76	24	
⑦ C9300-1 リンク障害 Gi1/0/2	0	1	44	26	

4.3 コンフィグ レーション

設定

検証で使用した各機器の設定内容となります。
アイコンをクリックしていただくことにより設定内容が表示されます。

機種	サンプル設定ファイル
Catalyst 9500 サンプル設定	 C9500_Sample_cfg
Catalyst 9300 サンプル設定	 C9300_Sample_cfg
Catalyst 9200 サンプル設定	 C9200_Sample_cfg

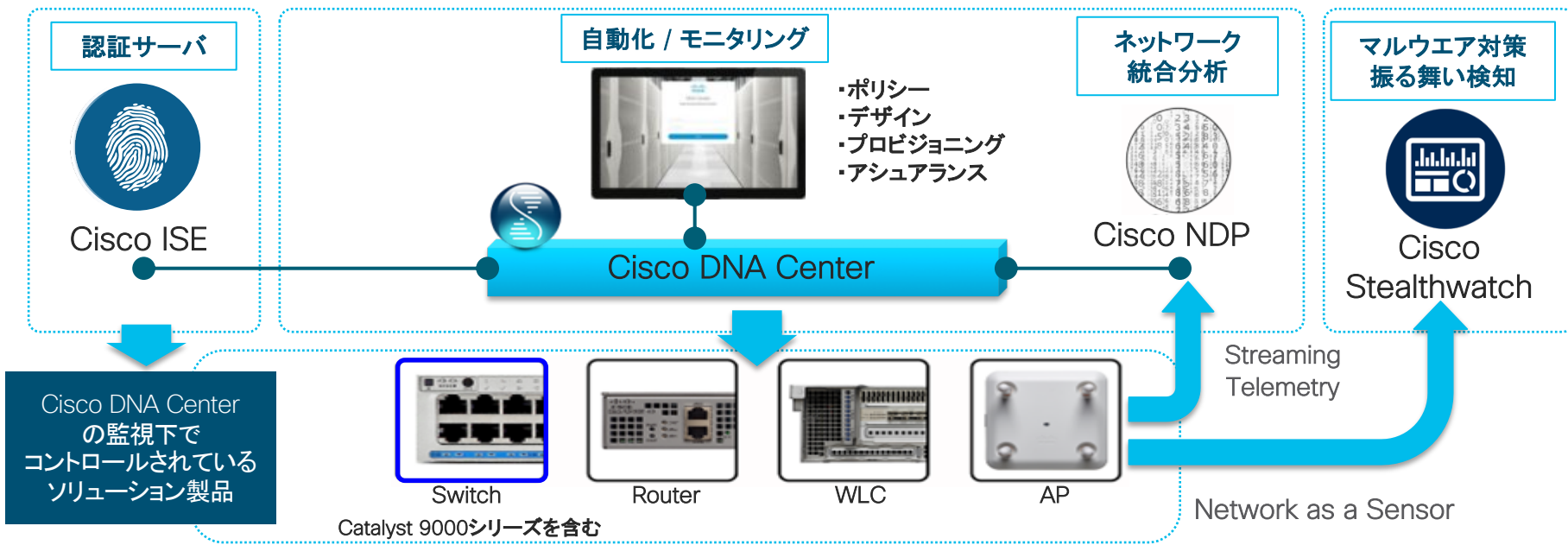
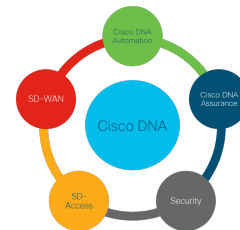
5

Cisco DNA 連携編

5.1 Cisco DNA 連携ソリューション

Cisco DNA を実現するにあたり

Cisco Catalyst 9000 シリーズでは、Cisco DNA Center を中心に必要なに応じてさまざまなプロダクトと連携することにより、Cisco DNA ソリューションを実現し運用管理をサポートします。



自動化、モニタリング

Cisco DNA Center の導入により



Cisco DNA Center ではネットワークプラグアンドプレイにより機器の導入 / 運用を容易にします。また、Cisco DNA Center ではネットワークの一元管理を可能にするダッシュボードがあり、簡単に機器の設定、プロビジョニング(導入設計)、ポリシーの適用などの一元管理を可能とします。

PnP サーバ

Cisco DNA Center 上で動作

サイト管理、コンフィグ、デバイスイメージ (IOS など)、ワークフロー

上位 API が提供されるため、コンフィグ生成アプリやオーダーツールと組み合わせた利用が可能

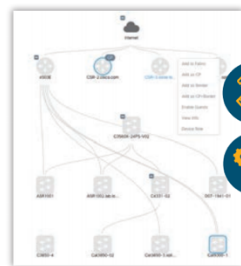
プラグアンドプレイ

PnP エージェント

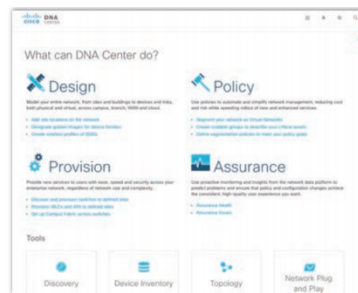
ルータ、スイッチ、ワイヤレス AP で動作する共通エージェント機能

展開プロセスを自動化

従来の CNS を刷新



デザイン / プロビジョニング



Cisco DNA Center
ダッシュボード



ポリシー設計と運用



アシュアランス

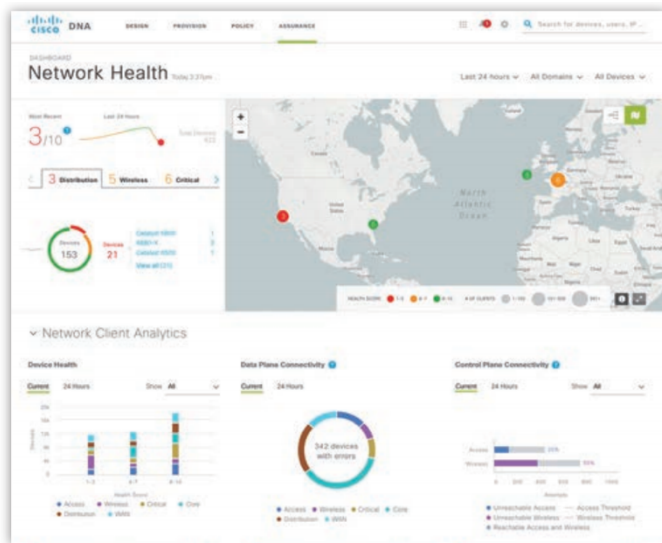
ネットワーク統合分析

Cisco DNA Center の導入により

Cisco DNA
AutomationCisco DNA
Assurance

利用者、利用端末、アプリケーションなどのトラフィック情報を収集し、可視化します。
また、その情報をもとに相関分析や機械学習アルゴリズム(AI)を活用してネットワークの利用傾向やトラブルの予兆把握などに役立ちます。

ダッシュボードによる可視化の例



パフォーマンス問題を予知として検出

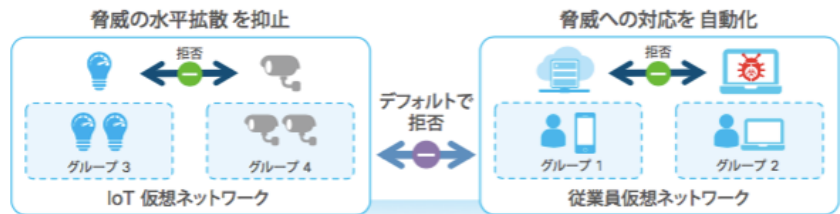


認証サーバ

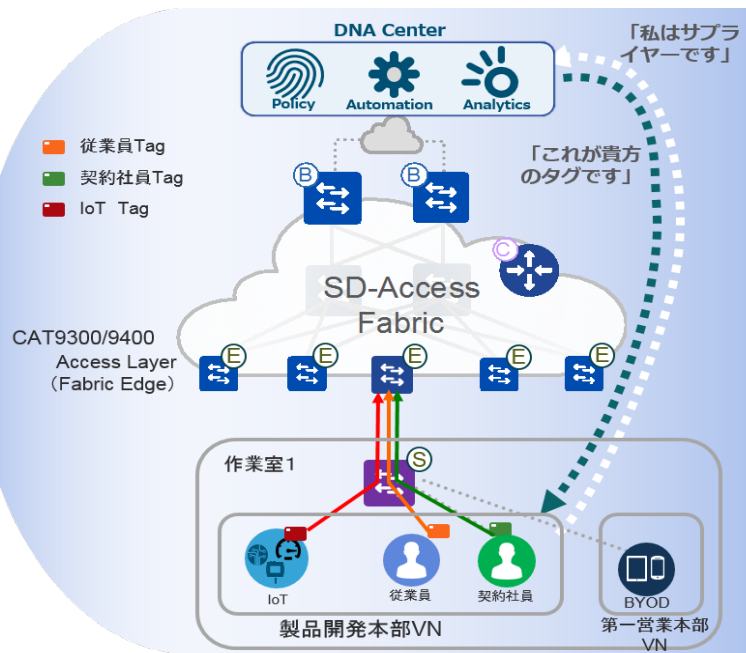
Cisco ISE と連携することにより

従来の VLAN、IP アドレスの管理を取り払い、認証に基づきセグメンテーションとアクセス コントロールを自動化することでネットワーク 設定変更の迅速化を可能にします。

<事前に設定したルール>



- ・事前に認証ユーザーごとにタグ情報を割り当てグループ単位での認証を行います。
- ・タグ間でのアクセスコントロールや、機器の設定情報を Cisco DNA Center で集中管理します。



5.1 Cisco DNA 連携ソリューション

マルウェア対策 振る舞い検知

Cisco Stealthwatch を導入することにより

ネットワーク全体をセキュリティ センサー化して全体を常に監視し、マルウェアなどの脅威の活動状況を可視化することが可能になります。

- NetFlow 情報を元にトラフィックの振舞い異常を検出することで、マルウェアが亜種、新種問わず、感染の可能性がある端末の特定が可能となります。
- 攻撃だけでなく、情報漏えいを目的とした大量のファイル ダウンロードも検出可能です。

ネットワーク スキャン

複数のホストに対する TCP、UDP、ポート スキャン

ワームの伝播

ワームに感染したホストが複数のサブネットの同じポートの スキャンと接続を行い、その他のホストが同じ動作を模倣

Denial of Service(サービス拒否)

SYN Half Open、ICMP/UDP/Port Flood

ボットネットの検出

内部ホストと外部の C&C サーバと通信

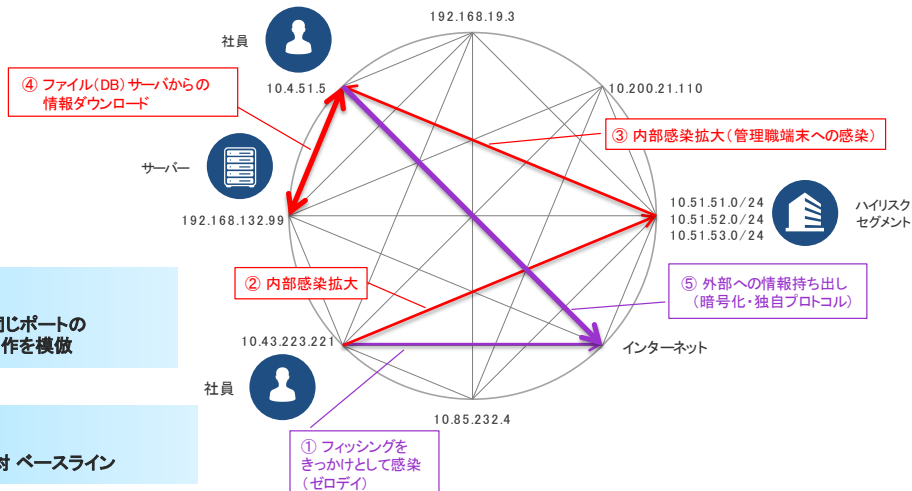


データの漏えい

大規模なアウトバウンド ファイル転送対 ベースライン

ポリシー違反

ベースラインが設定されたホストで事前に設定されたしきい値を越える



※ Cisco ISE と連携することにより、アラートだけでなくデバイスの隔離も可能となります。

6

まとめと今後

6.1 まとめと今後

最後に

本書の内容はいかがでしたでしょうか？

- ✓ ネットワークデザインの考え方
- ✓ 基本機能の動作
- ✓ 具体的な実装例と構成のポイント
- ✓ Cisco DNA から見たシスコが進む方向性



Cisco Catalyst 9000 シリーズを身近に感じていただけたのではないのでしょうか。

なお、本資料はシスコの SE が実際に実機を触ったことがベースとなり作成をさせていただきました。今後もシスコ SE は検証した内容をベースにアップデートを続けていきたいと考えています。

本書にお付き合いいただき、ありがとうございました。

©2019 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(1502R)

この資料の記載内容は2020年1月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

2068-1906-000-X