CHAPTER 1

Cisco ASR 9000 シリーズ アグリゲーション サービス ルータの概要

この章では、Cisco IOS XR ソフトウェア を実行する Cisco ASR 9000 シリーズ アグリゲーション サービス ルータ について説明します。ルータの概念、機能、およびユーザ インターフェイスについても説明します。

目次

ルータの概要

このルータは、マルチレイヤのイーサネット スイッチングおよび集約プラットフォームです。また、Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）ネットワークの端に配置される Label Edge Router（LER; ラベル エッジ ルータ）でもあります。このルータには、MPLS ネットワークの外部に接続するリンクが含まれています。これにより、企業やサービス プロバイダーのためのアクセスおよび集約サービスが提供されます。

特長および機能

このルータは、サービス プロバイダーが必要とする冗長性、高セキュリティと高可用性、実装、電力、およびその他の要件を満たすために設計されたスケーラブルなキャリアクラス分散フォワーディング ルータです。

このルータにより、ギガビット イーサネット デバイスからのトリプル プレイおよびイーサネット サービス トラフィックが 10 ギガビット イーサネット IP、MPLS 端、またはコアに集約されます。

ここでは、特長および機能について詳しく説明します。

Cisco IOS XR ソフトウェア

このルータで実行される Cisco IOS XR ソフトウェアでは、次の機能が提供されます。

- モジュラ ソフトウェア設計：Cisco IOS XR ソフトウェアは、ネットワークおよびインターネットの能力をお客様に認識していただけるように支援する、シスコの継続的なネットワーキング リーダーシップを代表する製品です。成果重視の次世代ネットワークの要件を満たすため、前例のないルーティング システム スケーラビリティ、高可用性、サービス分離、および管理性を提供します。
- オペレーティング システム インフラストラクチャの保護：Cisco IOS XR ソフトウェアは、メモリ管理やスレッド分散などの最も重要な機能を除くすべての機能を強制的にカーネルの外部で実行するマイクロカーネル アーキテクチャを提供することにより、アプリケーション、ファイル システム、およびデバイス ドライバの障害が広範囲のサービス中断を引き起こすことを防止します。
- プロセスおよびスレッドの保護：各プロセスは（個別のプロセス スレッドであっても）保護された独自のメモリ空間で実行されます。また、プロセス間の通信は、十分に定義され、バージョン管理されたセキュアなアプリケーション プログラミング インターフェイス（API）を介して確立されます。そのため、プロセス障害が他のプロセスに及ぼす影響を最小限に抑えられます。
- Cisco In-Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）：Cisco IOS XR ソフトウェアのモジュール性により、ソフトウェア アップグレードのインストール中にシステムの可用性が維持されます。ISSU または Hitless Software Upgrade（HSU; 中断のないソフトウェア アップグレード）により、シスコ ルータ ソフトウェアのほとんどの機能は、展開済みのサービスに影響を及ぼさずにアップグレードできます。アップグレード対象のシステム コンポーネントは、ソフトウェア パッケージや、選択された機能をまとめたコンポジット ソフトウェアに基づいて決定できます。シスコでは、これらのパッケージおよびコンポジットを事前に設定し、テストすることによってシステムの互換性を確保しています。
- プロセスの再起動：重要なコントロール プレーンのプロセスを手動で再起動したり、プロセス障害に応じてオペレーティング システム全体を自動的に再起動したりできます。この機能は、Cisco IOS XR ソフトウェアの目的である継続的なシステムの可用性をサポートし、顧客やトラフィックに対する中断を最小限に抑えながら、プロセス障害やプロトコル障害からのすばやい回復を可能にします。
- 状態チェックポイント：プロセスを再起動してから次回再起動するまでメモリおよび重要な動作状態を維持することにより、Route-Switch-Processor（RSP; ルート スイッチ プロセッサ）の切り替え時のルーティングの隣接関係およびシグナリング状態を維持できます。

- Ethernet Virtual Connection（EVC; イーサネット仮想接続）：イーサネット サービスは、特定のサービス タイプまたはエンド ユーザに所属するトラフィックをネットワーク経由で運ぶ個別の EVC を使用してサポートされています。EVC ベースのサービスは、MPLS ベースの L2VPN およびネイティブ IEEE ブリッジ配置と併用して使用できます。
- 柔軟な VLAN 分類 : VLAN を Ethernet Flow Point（EFP; イーサネット フロー ポイント）で分類すると、シングルタグ VLAN、ダブルタグ VLAN（QinQ および IEEE 802.1ad）、隣接する VLAN 範囲、隣接しない VLAN リストなどに分けられます。
- IEEE ブリッジング：このソフトウェアでは、IEEE 802.1Q、IEEE 802.1ad、および QinQ VLAN カプセル化メカニズムに基づいて、ルータ上のネイティブ ブリッジングがサポートされています。
- IEEE 802.1s Multiple Spanning Tree（MST; マルチプル スパニング ツリー）: MST では IEEE 802.1w Rapid Spanning Tree Protocol（RSTP; ラピッド スパニング ツリー プロトコル）がマルチプル スパニング ツリーに拡張され、収束とロード バランシングが迅速になります。
- MST アクセス ゲートウェイ：この機能により、傷害回復機能を持つファスト コンバージェンスなメカニズムが提供され、イーサネット ベースのアクセス リングに集約および接続できます。
- Virtual Private LAN Service（VPLS）: VPLS は VPN の一種で、管理された IP/MPLS ネットワーク上において、単一のブリッジ ドメインで複数のサイトを接続できます。VPLS により、お客様にはイーサネット インターフェイスが提供されます。また、サービスの帯域幅は物理インターフェイスに縛られないため、サービス プロバイダーとお客様に対して LAN と WAN の境界が単純化され、迅速で柔軟なサービスのプロビジョニングが可能になります。VPLS のすべてのサービスが、実際の場所に関係なく、同一の LAN 上にあるように表示されます。
- Hierarchical VPLS（H-VPLS; 階層型 VPLS）: H-VPLS では、VPLS ネットワークの端で階層が 1 つ、規模を拡大して提供されます。QinQ アクセスおよび H-VPLS 疑似回線アクセス オプションがサポートされています。
- Virtual Private WAN Services/Ethernet over MPLS（VPWS/EoMPLS）: EoMPLS は、疑似回線を使用して、MPLS コア上でイーサネット フレームを転送します。MPLS バックボーン上で疑似回線を使用して、出力インターフェイスまたはサブインターフェイスに EFP を個別にまたはポート全体を転送できます。
- 疑似回線冗長化：疑似回線冗長化により、失敗したプライマリ 疑似回線を保護するバックアップ疑似回線の定義がサポートされています。
- マルチセグメント疑似回線ステッチング：マルチセグメント疑似回線ステッチングは、相互接続関係を形成するために、2 つの疑似回線を 1 つにインターワーキングする方法です。
- IPv4 マルチキャスト：IPv4 マルチキャストでは、インターネット グループ管理プロトコル バージョン 2 および 3（IGMPv2/v3）、Protocol Independent Multicast の Source Specific Multicast（SSM）および Sparse Mode（SM）、Multicast Source Discovery Protocol（MSDP）、Anycast Rendezvous Point（RP）がサポートされています。
- IGMP v2/v3 スヌーピング：このレイヤ 2 メカニズムにより、L2VPN ネットワーク上でマルチキャスト メンバシップが効率的に追跡されます。個別の IGMP Join が、VLAN レベルまたは疑似回線レベルでスヌーピングされます。次に、結果が単一のアップストリーム Join メッセージにまとめられます。住宅用ブロードバンド環境では、この機能により、ネットワークで監視しているチャネルだけをダウンストリームのユーザに送信できるようになります。

柔軟なイーサネット

このルータは転送にイーサネットを使用します。イーサネットでは、次のような機能が提供されます。

- Ethernet Virtual Connection（EVC）：イーサネット サービスは、特定のサービス タイプまたはエンド ユーザに所属するトラフィックをネットワーク経由で運ぶ個別の EVC を使用してサポートされています。EVC ベースのサービスは、MPLS ベースの L2VPN およびネイティブ IEEE ブリッジ配置と併用して使用できます。
- 柔軟な VLAN 分類：VLAN を Ethernet Flow Point（EFP）で分類すると、シングルタグ VLAN、ダブルタグ VLAN（QinQ および IEEE 802.1ad）、隣接する VLAN 範囲、隣接しない VLAN リストなどに分けられます。
- IEEE ブリッジング：このソフトウェアでは、IEEE 802.1Q、IEEE 802.1ad、および QinQ VLAN カプセル化メカニズムに基づいて、ルータ上のネイティブ ブリッジングがサポートされています。
- IEEE 802.1s Multiple Spanning Tree（MST）：MST では IEEE 802.1w Rapid Spanning Tree Protocol（RSTP）がマルチプル スパニング ツリーに拡張され、収束とロード バランシングが迅速になります。
- MST アクセス ゲートウェイ：この機能により、傷害回復機能を持つファスト コンバージェンスなメカニズムが提供され、イーサネット ベースのアクセス リングに集約および接続できます。

L2VPN

このルータは、次の機能を提供する L2VPN を使用します。

- Virtual Private LAN Service（VPLS）：VPLS は VPN の一種で、管理された IP/MPLS ネットワーク上において、単一のブリッジ ドメインで複数のサイトを接続できます。VPLS により、お客様にはイーサネット インターフェイスが提供されます。また、サービスの帯域幅は物理インターフェイスに縛られないため、サービス プロバイダーとお客様に対して LAN と WAN の境界が単純化され、迅速で柔軟なサービスのプロビジョニングが可能になります。VPLS のすべてのサービスが、実際の場所に関係なく、同一の LAN 上にあるように表示されます。
- Hierarchical VPLS（H-VPLS）：H-VPLS では、VPLS ネットワークの端で階層が 1 つ、規模を拡大して提供されます。QinQ アクセスおよび H-VPLS 疑似回線アクセス オプションがサポートされています。
- Virtual Private WAN Services/Ethernet over MPLS（VPWS/EoMPLS）：EoMPLS は、疑似回線を使用して、MPLS コア上でイーサネット フレームを転送します。MPLS バックボーン上で疑似回線を使用して、出力インターフェイスまたはサブインターフェイスに EFP を個別にまたはポート全体を転送できます。
- 疑似回線冗長化：疑似回線冗長化により、失敗したプライマリ 疑似回線を保護するバックアップ疑似回線の定義がサポートされています。
- マルチセグメント疑似回線ステッチング：マルチセグメント疑似回線ステッチングは、相互接続関係を形成するために、2 つの疑似回線を 1 つにインターワーキングする方法です。

マルチキャスト

このルータは、次の機能を提供するマルチキャストをサポートしています。

- IPv4 マルチキャスト：IPv4 マルチキャストでは、インターネット グループ管理プロトコル バージョン 2 および 3（IGMPv2/v3）、Protocol Independent Multicast の Source Specific Multicast（SSM）および Sparse Mode（SM）、Multicast Source Discovery Protocol（MSDP）、Anycast Rendezvous Point（RP）がサポートされています。
- IGMP v2/v3 スヌーピング：このレイヤ 2 メカニズムにより、L2VPN ネットワーク上でマルチキャスト メンバシップが効率的に追跡されます。個別の IGMP Join が、VLAN レベルまたは疑似回線レベルでスヌーピングされます。次に、結果が単一のアップストリーム Join メッセージにまとめられます。住宅用ブロードバンド環境では、この機能により、ネットワークで監視しているチャネルだけをダウンストリームのユーザに送信できるようになります。

運用管理および保守（OAM）

このルータは、さまざまなタイプの Operation, Administration, and Maintenance（OAM; 運用管理および保守）をサポートしています。これにより、次の機能が提供されます。

- E-OAM（IEEE 802.3ah）：イーサネット リンク レイヤ OAM は、リンクのヘルスを監視し、障害切り離しを支援するための物理リンク OAM を提供する、EOAM の重要なコンポーネントです。イーサネット リンク レイヤ OAM を IEEE 802.1ag と共に使用することにより、リンク障害を高速に検出し、ローカルな障害をリモート側ノードにシグナリングできます。
- E-OAM（IEEE 802.1ag）：イーサネット接続障害管理は、IEEE 802.1 のブリッジおよび LAN によるパスの発見と検証を可能にする、さまざまなメカニズムおよび手順を提供する EOAM のサブセットです。
- MPLS OAM：このプロトコルは、Label Switched Path（LSP; ラベル スイッチド パス）PING、LSP TraceRoute、および Virtual Circuit Connectivity Verification（VCCV; 仮想回線接続性検証）をサポートしています。

レイヤ 3 ルーティング

このルータは、レイヤ 3 ルーティングと、次のような幅広い IPv4 サービスおよびルーティング プロトコルをサポートする Cisco IOS XR ソフトウェアを実行します。

- Intermediate System to Intermediate System（IS-IS）
- Open Shortest Path First（OSPF）
- スタティック ルーティング
- IPv4 マルチキャスト
- Routing Policy Language（RPL; ルート ポリシー言語）
- Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）
- Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）

MPLS VPN

このルータは、次の機能を提供する MPLS VPN をサポートしています。

- MPLS L3VPN : MPLS の IP VPN 機能により、Cisco IOS ソフトウェアまたは Cisco IOS XR ソフトウェア ネットワークで、スケーラブルな IPv4 レイヤ 3 VPN バックボーン サービスを展開できるようになります。IP VPN は、付加価値サービスを展開または管理するために企業が使用する基盤です。付加価値サービスには、ビジネス顧客に対するネットワーク取引およびテレフォニー サービスをホスティングするアプリケーションやデータが含まれます。
- Carrier Supporting Carrier（CSC）: CSC により、MPLS VPN サービス プロバイダーは、別のバックボーン サービス プロバイダーを使用して地理的に離れたサイトに接続しながら、顧客の VPN のプライベート アドレス空間を維持できます。これは、IETF RFC 4364 の定義に従って実装されます。

QoS

このルータは、さまざまなタイプの Quality Of Service（QOS）をサポートしています。これにより、次の機能が提供されます。

- QoS : 最大で 3,000,000 キューを使用できる総合的な QoS サポート、3 つのパラメータによるスケジューラに基づいた Class-Based Weighted Fair Queuing（CBWFQ; クラスベース重み付け均等化キューイング）、Weighted Random Early Detection（WRED; 重み付けランダム早期検出）、優先度の伝達をサポートした厳密な 2 レベル プライオリティ スケジューリング、および 2 レート 3 カラー（2R3C）ポリシングがすべてサポートされます。
- Cisco IOS XR ソフトウェア : このソフトウェアは、ポリシング、マーキング、キューイング、廃棄、シェーピングなど、豊富な QoS 機能をサポートしています。また、オペレーティング システムにより、Modular QoS CLI（MQC; モジュラ QoS CLI）がサポートされています。モジュラ CLI は、さまざまなシスコ プラットフォームでさまざまな QoS 機能を設定するために使用します。
- H-QoS : EVC には、4 つの階層レベル（ポート、EFP グループ、EFP、およびサービス クラス）を持つ H-QoS サポートが提供されます。レベルのサポートにより、サービスごと、エンド ユーザごとの QoS 精度を使用できます。

MPLS TE

このルータは、次の機能を提供する MPLE TE をサポートしています。

- MPLS TE : Cisco IOS XR ソフトウェアは、Traffic Engineering/Fast Reroute（TE-FRR; トラフィック エンジニアリング /Fast Reroute）、Resource Reservation Protocol（RSVP; リソース予約プロトコル）、Label Distribution Protocol（LDP; ラベル配布プロトコル）、Targeted Label Distribution Protocol（T-LDP; ターゲット ラベル配布プロトコル）などの MPLS プロトコルをサポートしています。
- MPLS TE Preferred Path : 優先トンネル パス機能により、特定の TE トンネルに疑似回線をマッピングできます。アタッチメント回線は、リモート プロバイダー側のルータ IP アドレスではなく、特定の MPLS TE トンネル インターフェイスに相互接続されています（Interior Gateway Protocol（IGP）または Label Distribution Protocol（LDP）を使用して到達できます）。

高可用性

このルータは、高可用性を必要とする企業ネットワークでの使用を目的としています。高い Mean Time Between Failures（MTBF; 平均故障間隔）レートと低い Mean Time To Resolve（MTTR; 平均修復時間）レートを提供する設計になっています。これにより、停止が最小限に抑えられ、最大限の可用性が達成されます。これは、次の機能によって実現されます。

- コンポーネントの冗長性
  - 二重電源
  - 冷却システム
- 障害検出
- 管理機能
- 高可用性機能
  - Non-Stop Forwarding（NSF）: Cisco IOS XR ソフトウェアは、短時間のコントロール プレーンの停止中にトラフィック損失のない転送をサポートしています。これは、IETF によって標準化されたグレースフル リスタート拡張のためのシグナリングおよびルーティング プロトコル実装を通じて行われます。NSF では、隣接するノードが NSF を認識する必要があります。
  - プロセスの再起動性（中断を最小限に抑えた再起動）
  - Stateful Switchover（SSO ; ステートフル スイッチオーバー）
  - In-Service Software Upgrade（ISSU）
  - MPLS TE Fast Reroute（FRR）
  - Bidirectional Forwarding Detection（BFD; 双方向フォワーディング検出）
  - 標準の IEEE 802.3ad リンク集約バンドル

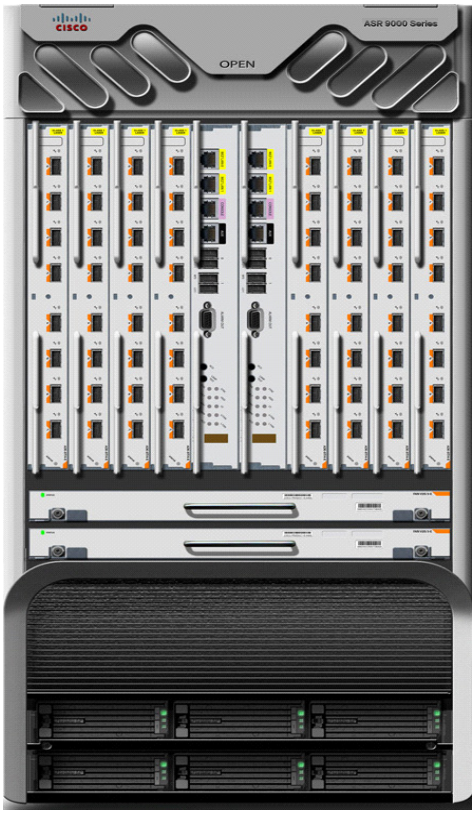
システム構成

このルータは、次のような独立型シャーシ上で Cisco IOS XR ソフトウェア を実行します。AC バージョンと DC バージョンがあります。

- 6 スロットのシャーシ
- 10 スロットのシャーシ

図 1-1　　6 スロットのシャーシ

図 1-2　　10 スロットのシャーシ



各タイプのシャーシは、スロットあたり 40G をサポートし、入れ替え可能なルートスイッチプロセッサ（RSP）とラインカード（LC）を共有できます。各シャーシでは、2 つのスロットが RSP 用に指定されており、残りのスロットはトラフィックを伝送するラインカードを格納します。RSP はラインカードに相互接続され、シャーシの管理および制御を提供します。すべてのラインカードは、ネットワーク側トランク カードまたは加入者側カードとして使用できるだけでなく、任意の接続形態で使用できます。

このルータには、次のラインカードを使用します。

- 40x1GE イーサネット ラインカード
- 4x10GE イーサネット ラインカード
- 8x10GE イーサネット ラインカード

管理およびセキュリティ

このルータには、次に示す管理機能とセキュリティ機能に加え、タスク ID の割り当てなど、ルータ タスクを実行できるユーザを制御する管理オプションがあります。

管理性

- Command-Line Interface（CLI; コマンドライン インターフェイス）: CLI は、ルータの管理およびメンテナンスを行い、基本的なルータ機能を設定するためのユーザ インターフェイスです。
- Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）: SNMP は、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション レイヤ プロトコルです。
- Management Information Base（MIB; 管理情報ベース）: MIB は、デバイス上で管理できるオブジェクトのデータベースです。MIB の例としては、IP-MIB（RFC4293）、CISCO-BULK-FILE-MIB、CISCO-CONFIG-COPY-MIB、CISCO-CONFIG-MAN-MIB、CISCO-ENHANCED-IMAGE-MIB、CISCO-ENHANCED-MEMORY-POOL-MIB、CISCO-ENTITY-FRU-CONTROL-MIB、CISCO-ENTITY-SENSOR-MIB、ENTITY-MIB、CISCO-ENTITY-ASSET-MIB、ENTITY-STATE-MIB、ENTITY-SENSOR-MIB、CISCO-ENTITY-ALARM-MIB、CISCO-FLASH-MIB、CISCO-IF-EXTENSION-MIB、CISCO-MEMORY-POOL-MIB、CISCO-RF-MIB（1:1 RP Card）、CISCO-SYSLOG-MIB、EVENT-MIB、IF-MIB および RFC1213-MIB、SNMP-COMMUNITY-MIB、SNMP-FRAMEWORK-MIB、SNMP-NOTIFICATION-MIB、SNMP-TARGET-MIB、IPv6-MIB、BRIDGE-MIB、DOT3-OAM-MIB、CISCO-IETF-PW-MIB、CISCO-CLASS-BASED-QOS-MIB、ETHERLIKE-MIB、BGP4-MIB（シスコ拡張を含む）、MPLS TE STD MIB、TE-FRR-MIB、および CISCO-IETF-IPMROUTE-MIB、IEEE-8021-CFM-MIB、DOT3-OAM-MIB などがあります。
- TFTP：ネットワークを介して、あるコンピュータから別のコンピュータへファイルを転送できるようにします。通常は、クライアント認証（たとえば、ユーザ名およびパスワード）を使用しません。
- Network Time Protocol（NTP; ネットワーク タイム プロトコル）: 分散された一連のタイム サーバ間でタイムキーピングを同期します。
- Cisco IOS XR ソフトウェアの管理性：この機能は、モジュラ CLI、SNMP、およびネイティブ XML インターフェイスを含む業界標準の管理インターフェイスを提供します。
- Cisco Active Network Abstraction（ANA）: Cisco ANA は、マルチテクノロジー、マルチサービス ネットワーク環境のための、柔軟な、ベンダー中立のネットワーク リソース管理ソリューションです。Cisco ANA はネットワークと Operations Support System（OSS; オペレーション サポー

ト システム）間で動作し、実際のネットワーク要素が実際のネットワークを作成するように、Virtual Network Element（VNE; 仮想ネットワーク要素）をソフトウェアベースの仮想ネットワークに集約します。Cisco ANA は、ネットワーク コンポーネントをダイナミックに検出し、ネットワーク要素のステータスをほぼリアルタイムで追跡します。Cisco ANA は、次のものをサービス プロバイダーに提供します。

  - OSS アプリケーションとネットワーク情報の統合の簡素化
  - ネットワーク リソースを管理するための柔軟な共通インフラストラクチャ
  - すべてのネットワーク要素のための一貫性のある手順およびインターフェイス

セキュリティ

- Cisco IOS XR ソフトウェア：このソフトウェアは、ACL、コントロール プレーンの保護、ルーティング認証、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）、TACACS+、Remote Authentication Dial In User Service（RADIUS; リモート認証ダイヤルイン ユーザ サービス）、IP セキュリティ（IPSec）、Secure Shell（SSH; セキュア シェル）プロトコル、SNMPv3、および主要な Routing Policy Language（RPL）のサポートを含む総合的なネットワーク セキュリティ機能を提供します。
- レイヤ 2 ACL：このセキュリティ機能を使用すると、EVC のパケットを MAC アドレスに基づいてフィルタリングできます。
- レイヤ 3 ACL：この機能は、IPv4 プロトコルのパケット属性によって ACL を照合します。
- セキュリティ：多数の重要なセキュリティ機能がサポートされています。
  - 標準の IEEE 802.1ad L2CP（レイヤ 2 コントロール プロトコル）および BPDU（ブリッジ プロトコル データ ユニット）フィルタリング
  - EFP またはブリッジ ドメインごとの MAC 制限
  - 任意のインターフェイスまたはポート上でのユニキャスト、マルチキャスト、およびブロードキャスト ストーム制御ブロッキング
  - Unknown Unicast Flood Blocking（UUFB; 不明なユニキャスト フラッディングの防止）
  - Dynamic Host Configuration Protocol（DHCP）スヌーピング
  - Unicast Reverse Path Forwarding（URPF; ユニキャスト リバース パス転送）
  - コントロール プレーン セキュリティ
- Secure Shell（SSH）
- Control Plane Policing（CoPP; コントロール プレーン ポリシング）

ルータの初期設定

Cisco ASR 9000 シリーズ アグリゲーション サービス ルータの初期設定は、ルータの起動時にソフトウェアによって自動的に決定されます。したがって、全般的な設定情報を設定する必要はありません。また、特定の RSP をアクティブにするために、明示的な設定を行う必要もありません。起動時にソフトウェアによって自動的に選択された RSP がアクティブになります。

このルータには複数の RSP ペアが存在しないため、RSP の選択肢は RSP0、RSP1 のいずれかだけです。通常は、スロット番号が小さい RSP が選択されます。この RSP を使用できない場合は、他のスロットの RSP がルート プロセス コントローラとして選択され、プライマリ RSP になります。フェールオーバーやスイッチオーバー時には、アクティブ ロールがスタンバイ RSP に移行されます。

管理インターフェイス

全般的なルータ設定情報を設定する必要はありませんが、管理インターフェイスを手動で設定する必要があります。RSP0 または RSP1 のいずれか、または同時に両方の管理ポートを設定します。

- Telnet
- Secure Shell（SSH）
- コンソール サーバ

このルータには、次のセクションで説明するさまざまなルータ管理インターフェイスが用意されています。

- 「コマンドライン インターフェイス」（P.1-11）
- 「拡張可能言語 API」（P.1-12）
- 「簡易ネットワーク管理プロトコル」（P.1-12）

コマンドライン インターフェイス

CLI は、ルータの管理およびメンテナンスを行い、基本的なルータ機能を設定するためのユーザ インターフェイスです。ユーザは、CLI を通じて Cisco IOS XR コマンドを実行します。

CLI は、このマニュアルのすべての手順で使用されます。他のルータ管理インターフェイスを使用する前に、まず CLI を使用してそれらのインターフェイスのインストールおよび設定を行う必要があります。ルータを設定するための CLI の使用に関するガイドラインについては、次の章で説明します。

- 第 3 章「一般的なルータ機能の設定」
- 第 4 章「その他のルータ機能の設定」
- 第 5 章「コマンドライン インターフェイス（CLI）のヒント、手法、およびショートカット」

ハードウェア インターフェイスやソフトウェア プロトコルの管理タスクなど、CLI のその他の手順については、「表記法」（P.xii）に示すCisco IOS XR ソフトウェアのドキュメントを参照してください。

拡張可能言語 API

Extensible Markup Language（XML; 拡張可能言語）アプリケーション プログラミング インターフェイス（API）は、ルータを管理し、監視するためのクライアント アプリケーションおよび PERL スクリプトをすばやく開発するために使用する XML インターフェイスです。クライアント アプリケーションでは、XML API タグ内の要求を符号化してルータに送信することにより、ルータを設定したり、ルータからステータス情報を要求したりできます。ルータは、要求を処理し、符号化された XML API タグの形式で応答をクライアントに送信します。XML API は、Telnet、SSH、Secure Socket Layer（SSL; セキュア ソケット レイヤ）トランスポートなど、すぐに使用できるトランスポート レイヤをサポートしています。

詳細については、Cisco IOS XR ソフトウェアドキュメント（「表記法」（P.xii）に記載）を参照してください。

簡易ネットワーク管理プロトコル

簡易ネットワーク管理プロトコル（SNMP）は、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション レイヤ プロトコルです。ネットワーク管理者は、SNMP で転送されたデータ（1 秒あたりのパケット数、ネットワーク エラー レートなど）を使用することにより、ネットワークのパフォーマンスを監視し、ネットワークの問題を見つけて解決し、ネットワークの成長を計画できます。

Cisco IOS XR ソフトウェアは、SNMP v1、v2c、および v3 をサポートしています。SNMP は、RFC と呼ばれるインターネット ドキュメントで定義されたインターネット Network Management Framework（NMF; ネットワーク管理フレームワーク）と呼ばれる大規模なアーキテクチャの一部です。SNMPv1 NMF は RFC 1155、1157、および 1212 で定義され、SNMPv2 NMF は RFC 1441 ～ 1452 で定義されています。SNMP v3 の詳細については、RFC 2272 および 2273 を参照してください。

SNMP は、さまざまな商用インターネットワークや、大学および研究組織で使用されるインターネットワークを管理するための人気のあるプロトコルです。SNMP に関する標準化活動は、最新技術を使用した SNMP ベース管理アプリケーションがベンダーによって開発され、リリースされても続けられます。SNMP は比較的単純なプロトコルですが、そのフィーチャ セットは、今日の異種ネットワークを管理する際に発生するさまざまな問題を処理するための十分な能力を提供します。

詳細については、Cisco IOS XR ソフトウェアドキュメント（「表記法」（P.xii）に記載）を参照してください。

コンソール ポート経由でのルータの接続

Cisco IOS XR ソフトウェアを実行する新しいルータに初めて接続する場合は、コンソール ポート経由で接続します。標準的なルータ設定および管理はイーサネット ポートを使用して行いますが、このポートを使用する前に、使用している LAN 用にコンソール ポートを設定しておく必要があります。

新しいルータには名前、IP アドレス、またはその他の資格情報が設定されていないため、端末を使用して、コンソール ポート経由でルータに接続し、速度を 115200 に設定します。リモート ターミナルの設定値は、115200 に合わせる必要があります。

コンソール ポート経由でルータに接続したら、IP アドレスを使用して管理ポートを設定します。これにより、SSH または Telnet を使用してルータに接続できるようになります。

（注）　confreg 0x0 を実行すると、デフォルトの速度設定が復元されます。デフォルトの 115200 から設定を変更した場合は、後でリセットする必要があります。

コンソール ポート経由でルータに接続するには、次の手順に従います。

手順概要

1. ルータの電源を投入します。
2. **コンソール ポートに端末を接続します。**
3. ターミナル エミュレーション プログラムを起動します。
4. **Enter** キーを押します。
5. ルータにログインします。
6. **admin**
7. **show dsc**

詳細手順

	コマンドまたはアクション	目的
ステップ 1	ルータの電源を投入します。	ルータを起動します。 • このステップが必要なのは、電源がオンになっていない場合だけです。 • 電源の取り付けおよび制御については、「表記法」（P.xii）に記載されているハードウェアの文書を参照してください。
ステップ 2	コンソール ポートに端末を接続します。	ルータへの通信パスを確立します。 • 初期設定時、ルータと通信できるのはコンソール ポート経由だけです。 • ルータのコンソール ポートは、ターミナル エミュレーション プログラムを実行している端末またはコンピュータへのシリアル ケーブル接続用に設計されています。 • 端末の設定は次のとおりです。 – ビット/秒：115200 – データ ビット：8 – パリティ：なし – ストップ ビット：2 – フロー制御：なし • コンソール ポートで使用するケーブルの要件の詳細については、「表記法」（P.xii）に記載されているハードウェアの文書を参照してください。

	コマンドまたはアクション	目的
ステップ 3	ターミナル エミュレーション プログラムを起動します。	（省略可能）ルータ通信用にコンピュータを準備します。 • 端末経由で接続している場合、この手順は不要です。 • 端末は、別のデバイスにキーストロークを送信し、そのデバイスから文字を受信します。コンピュータをコンソール ポートに接続する場合は、ターミナル エミュレーション プログラムを使用してルータと通信する必要があります。ターミナル エミュレーション プログラムの使用については、そのプログラムのマニュアルを参照してください。
ステップ 4	**Enter** キーを押します。	ルータとの通信を開始します。 • コンソール ポートに接続したときにテキストまたはルータ プロンプトが表示されない場合は、**Enter** キーを押して通信を開始します。 • **Enter** キーを押してもテキストが表示されない場合は、初回の起動手順が完了するのを待ってから **Enter** キーを押します。 • 表示メッセージのためにプロンプトを見失った場合は、**Enter** キーをもう一度押します。 • ルータに `Username:` というプロンプトが表示されます。
ステップ 5	ルータにログインします。	ルータ管理セッションのアクセス権を確立します。 • ルート システムのユーザ名およびパスワード、またはシステム管理者によって提供されたユーザ名およびパスワードを入力します。 • ログイン後、ルータに CLI プロンプトが表示されます。詳細については、「CLI プロンプト」（P.3-6）を参照してください。
ステップ 6	**admin** **例：** `RP/0/RSP0/CPU0:router# admin`	ルータを管理 EXEC モードにします。

ステップ 7	**show dsc**
	
	例：
	`RP/0/RSP0/CPU0:router(admin)#sh dsc`
	`NODE ROLE`
	`========================`
	`0/RSP0/CPU0 DSC`
	`0/RSP1/CPU0 Backup DSC`
	`RP/0/RSP0/CPU0:RO-A(admin)#`
		コンソール ポートに正常に接続されたことを確認できるように、ルータの RSP 情報を表示します。

ギガビット イーサネットおよび 10 ギガビット イーサネット インターフェイスの設定

ルータに接続したら、ギガビット イーサネットおよび 10 ギガビット イーサネット インターフェイスを手動で設定する必要があります。これらのインターフェイスはデータ トラフィック専用で、管理トラフィック用ではないため、SSH または Telnet を使用して、ギガビット イーサネットおよび 10 ギガビット イーサネット インターフェイスの一部である IP アドレスには接続できません。

関連情報

ルータにログインしたら、「CLI プロンプト」（P.3-6）の説明に従って全般的なルータ設定を行うことができます。