変電所の自動化：新しいデジタル変電所設計ガイド

シスコは、拡張性、安全性、復元力に優れたマルチサービス対応型ネットワークを実現する、包括的な変電所自動化ソリューションの提供に取り組んでいます。ソリューションリリースでは、実際のお客様の進化し続ける導入シナリオに継続的に対応します。以前のソリューションリリースで取り上げたユースケースでは、変電所の自動化、管理、報告に加えて、物理的なセキュリティアーキテクチャ、リモートエンジニアリング アクセス、リモートワークフォース管理、および高精度なタイミングの配電について説明しました。Cisco Validated Design (CVD) では、シリアルおよびイーサネットベース環境、電子的セキュリティ境界 (ESP)、マルチサービス、および企業ネットワークゾーンのトポロジの他にも、Quality of Service (QoS)、高可用性などに関する幅広い内容を取り上げています。

変電所自動化 3.0 設計ガイドの CVD は、ソリューションバージョン 1.5、2.2.1、2.3.1 の後続バージョンです。ソリューションバージョン 2.3.2 では、以前のリリースで述べられたトピックが再び取り上げられることは**ありません**。現在も有効で推奨されている過去の設計については、以前のソリューションドキュメントを参照してください (7 ページの「その他の関連ドキュメント」を参照)。

はじめに

変電所の自動化 CVD バージョン 3.0 には、シスコによる検証済みの変電所自動化ソリューション アーキテクチャの開発に関する最新情報が記載されています。このドキュメントに関連するソリューションリリースの目的は、シスコの産業用イーサネット (IE) スイッチ製品ラインに最近追加されたハードウェアとソフトウェアの機能を活用して、電力事業者の変電所自動化の設計と実装を推進すること、および変電所の LAN 向け Cisco DNA-Center とワイドエリアネットワーク向け vManage を使用したソフトウェアデファインド ネットワーク管理機能を紹介することです。

要約

電力事業者はかつてないほど大きな課題に直面しています。グリッド (送電網) には、より持続性が高く分散化された、変動するエネルギー源の供給が求められています。それに加え、電力事業者は火災や異常気象などの環境影響に翻弄されています。電力事業者のビジネスモデルも、顧客の多様化に伴って進化しています。先進国では電力事業者従業員の多くが退職の時期を迎え、スキルとリソースのギャップが生じています。さらに、世界が二酸化炭素排出量の削減に動いているため、電力事業者は供給電力の拡大を求められています。その一方で、この業界は進化を続けるサイバーセキュリティリスクの絶え間ない脅威にもさらされています。

シスコの変電所自動化ソリューションにより、電力事業者は、新しいビジネスモデルのサポート、法的要件への準拠、供給電力の拡大、再生可能エネルギー源の統合、運用コストの削減、グリッド運用リスクの軽減すべてが可能になります。このソリューションは、中核の遠隔監視制御・情報取得 (SCADA) システムをサポートするだけでなく、重要資産の保護と電力管理に関連する主要なユースケースにも対応します。新しくなったテクノロジーとネットワーク管理機能を通じて、ネットワーク設置面積を削減し、主要なタスクを自動化することにより、運用コストを削減します。このソリューションのネットワーク インフラストラクチャは、より多くのデバイスをサポートし、より広い帯域幅を処理することができます。また、高い復元力と、時刻同期やアプリケーション ホスティングなど多くの機能も備えています。この変電所自動化ソリューションの基盤を成

しているのが、シスコのグリッド セキュリティ ソリューションの可視性とセキュリティです。このポートフォリオは、幅広い送配変電所および配電変電所のニーズに対応します。最新のソリューションにより、電力事業者は次の課題を克服できます。

- より広い帯域幅を必要とするプロセスおよびステーションバスデバイスの増加
- 変電所の装置用スペースが限られている
- 変電所のデバイスと通信を可視化およびセグメント化してサイバーセキュリティのリスクを軽減する必要がある
- グリッド運用におけるネットワークスキルが欠如している
- レガシーデバイスを統合して監視する必要がある
- 規制要件 (特に NERC-CIP セキュリティ)
- より多くの変電所をサポートするために拡張する必要がある

ビジネスケース

電力事業者はシスコの変電所自動化ソリューションを導入することで、次の分野でさまざまな経営目標を達成できます。

- 重要なグリッド資産を保護し、グリッドの信頼性と安全性を向上
- 運用コストを節減し、効率性を向上
- セキュリティリスクを軽減し、規制コンプライアンスに準拠
- 持続可能なエネルギー源への移行をサポート

保護、信頼性、安全性

現代社会は信頼性の高い電力に頼らざるを得ません。電力事業者は信頼性の目標と照らし合わせて評価されます。変電所の運用は、信頼性の高い電力サービスを維持する上で非常に重要です。また、電力事業者は、長期間にわたって維持および運用できることを期待して高価な資産を調達します。変電所自動化ソリューションは、重要な資産を監視および保護するための重要なコミュニケーション機能を提供するように設計されています。また、高い復元力を備え、グリッドの信頼性を維持し、リモートアクセスを可能にし、安全性を強化します。

このソリューションは、次の方法で信頼性と安全性を確保します。

- 復元力のあるネットワークトポロジとネットワーク レジリエンス プロトコルにより、迅速なロスレス ネット ワークリカバリと一貫したネットワークサービスを実現し、どのようなシングルポイント障害が発生しても変電所の運用を維持
- 平均故障間隔 (MTBF) が非常に長くなるように設計されており、変電所運用の認定 (IEC 61850 など) を受けた堅牢なネットワーク インフラストラクチャを使用
- 稼働時間を維持し、ダウンタイム発生時の障害を抑える復元力のあるネットワーク インフラストラクチャ
- 変電所ネットワークとインフラストラクチャへの安全なリモートアクセスを実現
- ネットワーク管理ツールは、導入を自動化して問題や機能停止を迅速に特定し、機械学習と人工知能を活用してネットワーク問題に迅速に対応することで、素早く解決

運用コストと効率性

電力事業者は、特に料金設定に関する規制が課されていることが多いため、運用コストと効率性に対して非常に敏感です。コストの削減と効率化は重要な課題です。このソリューションでは、次の方法でこれらの課題を克服します。

- 変電所のデジタル化を推進する際に中核となる、IEC 61850、DNP3、Modbus/TCP といった最新のイーサネットベースの変電所プロトコルをサポート
- 特長と機能を製品ラインに統合することで、ルーティング、スイッチング、サイバーセキュリティ、およびネットワークサービス (時刻同期など) を提供するために必要なデバイスの数を削減
- ネットワーク インフラストラクチャで帯域幅とパフォーマンスを強化して、利用可能なデータ量とデータ品質を向上させ (例: テレメトリとセンサーの追加)、既存資産の予知保全、寿命、および効率の向上を実現
- 長い運用ライフサイクルと支援体制で製品をサポート
- 高価な WAN 接続の効率性を高め、運用コストを削減するソフトウェアデファインド ワイドエリア ネットワークをサポート
- ネットワーク管理ツールを導入し、自動化と AI 主導の問題解決により、導入と管理コストを削減

セキュリティおよび法規制の遵守

電力事業者が直面しているサイバーセキュリティの脅威は、複雑度と頻度が増してきています。ダウンタイムとリカバリにかかるコストは増加し、法的規制はますます厳しくなっています。このソリューションには、電力事業者が法的規制を満たしながら、サイバーセキュリティイベントに関するコストを削減して、変電所運用のセキュリティ対策を向上させるために設計された高度なサイバーセキュリティ機能が備わっています。

以下の表に概説されている NERC CIP の主要なセキュリティ要件に対応しています。

表 1　NERC CIP の主要な要件とシスコのテクノロジーサポート

NERC CIP の要件	領域	適用テクノロジー
CIP-002-5.1a	重要なサイバーアセットの特定	Cisco Cyber Vision、IE3400、IE9300、IR8300
CIP-003-8	セキュリティ管理の制御	IR8300 ゾーンベースのファイアウォール、Cisco ISA 3000、Firepower ファイアウォール Cisco DNA-Center、Identity Services Engine、vManage
CIP-005-5	電子的セキュリティ境界	IR8300 ゾーンベースのファイアウォール、Cisco ISA 3000、Cisco Duo、AnyConnect
CIP-007-6	システムセキュリティ管理	Cisco DNA-Center、Identity Services Engine、vManage FirePower Management Center、ISA 3000、Firepower ファイアウォール、Cisco SecureX セキュリティ オーケストレーション
CIP-008-5	インシデント報告と対応計画	Cyber Vision、DNA-Center、ISE、vManage、Firepower Management Center、SecureX
CIP-010-2	設定変更の管理と脆弱性アセスメント	Cisco Cyber Vision、DNA-Center、ISE、vManage

CIP-011-2	情報の保護	ファイアウォールと TrustSec によるセグメンテーション、暗号化通信 (VPN や MacSec など) を備えたネットワーク インフラストラクチャ、TrustSec ベースのセグメンテーションを備えた AnyConnect、DNA-Center、vManage、および ISE
CIP-013-1	サプライ チェーン管理	ネットワーク インフラストラクチャで TrustAnchor をサポートする IEC62443 製品開発認定 (62443-4-10 および 62443-4-20)

その他のサイバーセキュリティ機能は、次のとおりです。

- NERC CIP のガイドラインで定められている電子的セキュリティ境界を確立し、新しい変電所ルータである Cisco IE8340 で産業用ファイアウォールとゾーンベースのファイアウォール サービスを介して変電所の運用を保護
- ネットワーク インフラストラクチャで Cisco TrustSec テクノロジーを使用してゾーンとコンジットを確立し、Cisco DNA-Center および Identity Services Engine アプリケーションを介して展開および管理するための変電所のマイクロセグメンテーションをサポート
- ネットワーク インフラストラクチャ内で Cisco TrustAnchor を使用して安全なネットワーク インフラストラクチャを運用 (セキュアブート、セキュアストア、偽造防止メカニズムなど)
- 接続状態にあるデバイス (IED、RTU、PLC など) の可視化とセキュリティ分析、および Cisco Cyber Vision を介した通信
- 重要資産の識別など、NERC CIP で定められている主要プロセスをサポート
- 変電所のデジタル化を推進する際に中核となる、IEC 61850、DNP3、Modbus/TCP といった最新のイーサネットベースの変電所プロトコルをサポート
- IEC 62443 (産業用サイバーセキュリティ) 認定製品および製品開発

持続可能性

気候変動に対処して持続可能な社会を実現するための取り組みが世界的に重要視され、推進される中、電力事業者は重要な役割を担っています。風力や太陽光などの持続可能性の高いエネルギー源を取り入れる必要がありますが、より迅速な配電網が必要になります。同時に、現代社会の主要システム (交通など) の電化により燃焼時に二酸化炭素を発生させる化石燃料から脱却しようとする動きは、電力システムへの依存に拍車をかけています。主要なインフラストラクチャの強化と改善には、ほとんどの場合、電力網が関わってきます。

このソリューションは、次の方法で電力事業者の持続可能性への取り組みをサポートします。

- 配電システムのデジタル化を推進し、リアルタイムの制御と管理を高速化して、新しいエネルギー源と電力システムに対する需要の増加に対応
- 信頼性が高く安全なリモートアクセスにより、配電システムの迅速な展開とアップグレードを実現
- エネルギー効率が高く、Power over Ethernet をサポートし、各種デバイス (カメラ、アクセスポイントなど) に効率的に電力を供給する循環経済向けのネットワーク インフラストラクチャ

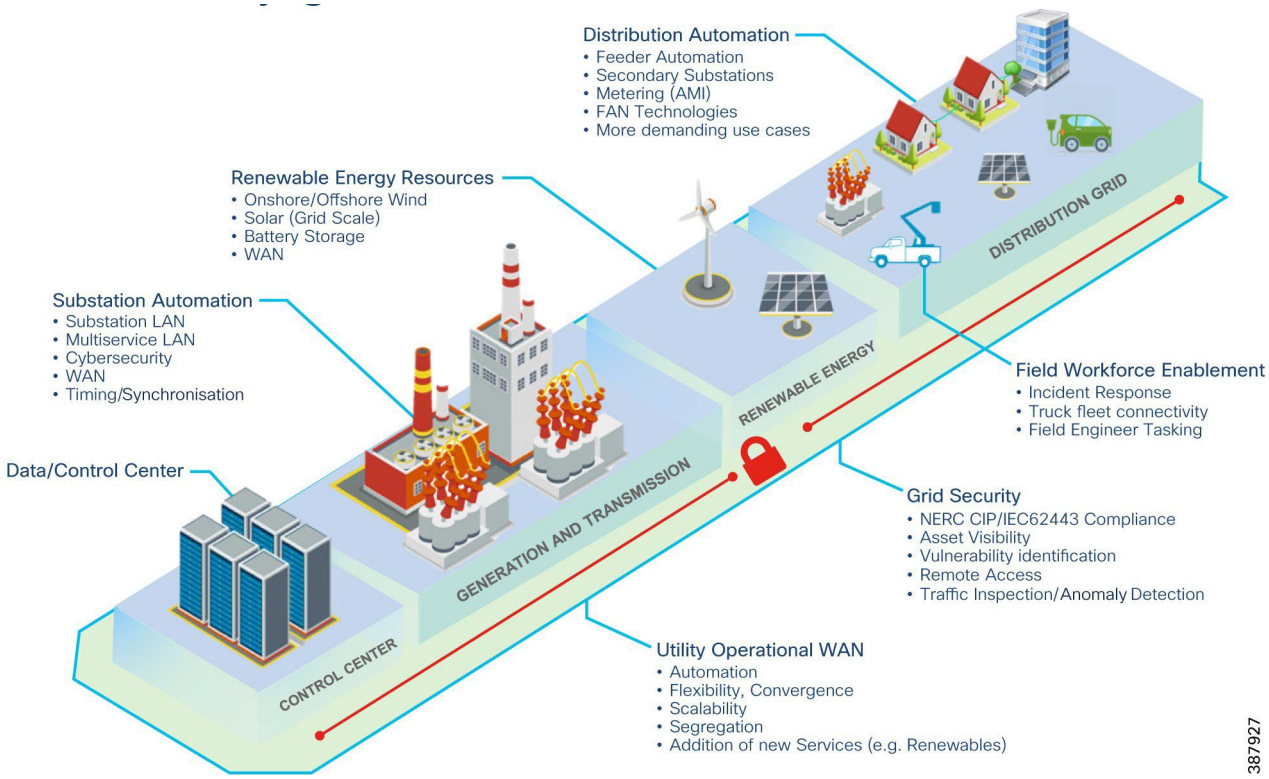
変電所の自動化とは

変電所の自動化は通信および情報技術と統合されたインテリジェントな配電システムであり、グリッド運用の強化、カスタマーサービスの改善、コストの削減を実現し、環境面で新たなメリットをもたらします。シスコの高度な変電所自動化ソリューションでは、送配電システムを監視して管理するためのネットワーク機能とセキュリティ機能を導入および実装する方法につ

いて説明します。このソリューションは、中核の遠隔監視制御・情報取得 (SCADA) システムをサポートするだけでなく、重要資産の保護と電力管理に関連する主要なユースケースや、変電所内に配置または変電所を介して接続されるマルチサービスネットワークにも対応します。

変電所の自動化は、電力グリッドアプリケーションに対するシスコのソリューションサポートにおいて重要な機能です。図 1 は、電力事業の主要機能である発電、配電の自動化、フィールドワークフォースの活用の概要を示しています。

図 1　　電力グリッドと変電所自動化の概要



このソリューションは以前のバージョンに基づいており、次のユースケースをサポートします。

- IEC 61850 GOOSEメッセージングに対応または非対応の変電所自動化
- 位相計測装置 (PMU) を備えた変電所自動化
- 物理的なセキュリティ (監視カメラとアクセス)
- リモートワークフォース管理 (有線のみ)
- 正確なタイミングの配電
- 変電所デバイスへのリモート エンジニアリング アクセス

シスコ変電所自動化ソリューションリリース 2.2.1 では、次のセキュリティトピックについて取り上げています。

- アクセスの制限
- データの保護
- イベントと変更の記録
- 変電所の監視アクティビティ

シスコ変電所自動化ソリューションリリース 2.3.1 では、以下の内容に焦点を当てています。

- PRP および REP を使用した ESP ゾーントポロジの高可用性 (HA)
- GOOSE 検証
- 迅速に停電に対応するネットワーク インフラストラクチャの Dying Gasp
- 2014 IEEE Precision Time Protocol - 電力プロファイルに基づく変電所 LAN の PTP
- ファイアウォールの冗長性

シスコ変電所自動化ソリューションリリース 2.3.2 では、以下の内容に焦点を当てています。

- 以下を利用できるネットワーク レジリエンス プロトコルの進化
  - High-Availability Seamless Redundancy (HSR) シングル通信ノード (SAN)
  - Parallel Redundancy Protocol (PRP) - HSR デュアル RedBox
- 以下の導入によるネットワークベースのタイミングの進化
  - グローバルナビゲーション衛星システム (GNSS) およびグローバル ポジショニング システム (GPS) のサポート
  - PRP LAN の両端 (A および B) 上の Precision Time Protocol (PTP) 1588 v2
- トラフィックフローの異常を監視する Cisco NetFlow および Stealthwatch によるセキュリティの強化
- さまざまなネットワーク アプリケーションおよびトラフィックタイプで一貫性のあるサービスを確保する QoS
- 変電所 LAN 向けに最近導入された産業用イーサネットスイッチ Cisco IE 4010 の検証

変電所自動化の最新情報

このソリューションでは、上記の機能とユースケースの多くがサポートされ、強化されています。このバージョンで取り上げられている新しい重要ポイントは、新製品と機能です。

このソリューションでサポートされる新機能は次のとおりです。

- 変電所 LAN の一元管理と自動化を実現するネットワークの展開と、Cisco DNA-Center による管理
- Cisco ソフトウェア定義型 WAN (SD-WAN) テクノロジー (vManage など) による変電所ワイドエリアネットワーク (WAN) の集中ネットワーク展開と管理

変電所自動化ネットワークおよびセキュリティアーキテクチャに導入された新製品は次のとおりです。

- IEC 61850-3 および IEEE 1613 に準拠し、最大 3 ユニットまでスタック可能な 28 個のギガビット イーサネット ファイバ ポートを搭載し、安全で信頼性が高く低遅延のステーションおよびプロセスバス通信を実現する Cisco Catalyst® IE9300 高耐久シリーズ スイッチ
- 拡張可能な WAN 接続、ファイアウォールセキュリティ、アプリケーション ホスティングを備えた多機能で耐久性に優れたモジュール型の Cisco Catalyst IR8340 ルータ

どちらのプラットフォームも IEC 61850-3 および IEEE 1613 の認定を受けており、以下のプロトコルをサポートしています。

- 信頼性: 多様なレジリエンスプロトコルと同期プロトコル (High-Availability Seamless Redundancy [HSR] やParallel Redundancy Protocol [PRP] など)
- セキュリティの強化: 幅広い機能をサポート。ゾーンベースのファイアウォール (IR8300 のみ)、Cisco TrustSec、IEEE 802.1x ネットワーク アクセス コントロール、Cisco Trust Anchor、Cyber Vision による変電所自動化デバイスと通信の可視化、MACsec
- 精度: 変電所全体の時刻同期をサポート (2017 IEEE Precision Time Protocol - 電力プロファイルなど)
- シンプル: スイッチ向けの Cisco DNA Center、SD-WAN ルーティング機能向けの Cisco vManage を含む幅広い管理オプション

変電所自動化の対象者

このドキュメントは、変電所とワイドエリアネットワークを運用する電気事業者のオペレータ、ならびに配電網を展開、運用、および管理する電気事業者のパートナーおよびベンダーが使用することを目的としています。このドキュメントの情報を完全に理解するには、次のことを行う必要があります。

- 電気事業の運用テクノロジー (OT) の世界についての確固たる基礎力を身に付けている
- IEC 61850 や NERC CIP など、関連する電力業界の標準と規約に精通している
- この CVD の内容は、主にイーサネット接続のインテリジェント エンド デバイス (IED) を採用している電力事業者を対象としています。
- 変電所ゾーンについて言及されていますが、今回リリースされた SA LAN およびセキュリティ CVD バージョン 2.3.2 では、主に ESP ゾーン設計の拡張に焦点を当てています。
- Modbus や DNP3 などのシリアルベースのプロトコルを使用して通信するエンドポイントに関連する設計については、以前にリリースされたソリューションドキュメントを参照してください。
- 関連ドキュメントの Cisco SalesConnect リンクのいずれにもアクセスできない場合は、シスコアカウントチームにドキュメントの提供を依頼してください。ただし、一部のドキュメントについては、シスコとの機密保持契約 (NDA) が必要です。

その他の関連ドキュメント

前述のように、このソリューションは電力事業に焦点を当てた他のシスコソリューションを基盤としており、それらと統合されています。変電所自動化に関連するその他のドキュメントには、次のものがあります。

配電の自動化と二次変電所:

- Secondary Substation Design Guide https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Secondary-Substation/DG/DA-SS-DG.html
- Secondary Substation Implementation Guide https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Secondary-Substation/IG/DA-SS-IG.html

グリッドセキュリティ:

- Grid Security Design Guide https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Grid_Security/DG/DA-GS-DG.html

- Grid Security Implementation Guide https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Grid_Security/IG/DA-GS-IG.html
- Achieving NERC CIP Compliance https://www.cisco.com/c/en/us/solutions/collateral/industries/white-paper-c11-2396807.html

仮想 RTU:

- Virtual RTU Implementation Guide https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Utilities/FAN/Virtual-RTU/IG/CU-VRTU-IG.html

ワイドエリアネットワーク

- Cisco SD-WAN Design Guide https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html

変電所自動化アーキテクチャ

次のセクションでは、変電所自動化のリファレンスアーキテクチャの概要を紹介します。このアーキテクチャは、変電所が重要なコンポーネントである大規模電力システム (BES) のグリッドオペレータ管理に関連する主要機能を表すゾーンに分割されます。ゾーンの分割と定義は、北米電力信頼度協議会 (NERC) が重要インフラ保護 (CIP) について設定した定義と基準に従っています。これは北米のエンティティですが、概念と機能は世界中のグリッド運用に適用できます。

ソリューションの要件

変電所自動化アーキテクチャは、電力網を運用する電力事業者の重要な要件を満たすように設計されています。電力事業者の重要な一連の要件は、北米電力信頼度協議会 (NERC) の重要インフラ保護 (CIP) 基準で定められています。

イーサネットと IP への移行

変電所の保護、制御、測定、および監視アプリケーションを統合するために、新しい通信プロトコルが開発され、国際電気標準会議 (IEC) 61850、変電所の通信ネットワークおよびシステムの傘下で標準化されました。これらのプロトコルには、既存のイーサネット標準が活用されてます。

レガシーのシリアル接続デバイスには、これらの新しいプロトコルを実装するイーサネットポートを備えた最新のインテリジェント電子デバイス (IED) が用意されています。IED には通常、複数の保護、制御、監視、および通信機能が搭載されています。

独自の遅延要件のために特別な考慮が必要な特有の IED の 1 つは、位相計測装置 (PMU) です。PMU は、電圧を測定してデータをレポートできるデバイスです。PMU は、送電網のセグメント間で位相の不均衡が発生しないようにグリッドデバイスを同期するために使用されます。

NERC CIP の概要

北米電力信頼度協議会 (NERC) は、「北米の大規模電力システム (BES) のセキュリティを規制、強化、監視、および管理することを目的とした」重要インフラ保護基準を確立しました。変電所の運用は、BES の重要な機能です。これらの標準規格では、システムのコンポーネント、その重要性、および保護要件が示されており、電力事業者はそれらを満たす必要があります。このソリューションでは、電力事業者とその変電所自動化の運用と関連性が高い用語と概念が繰り返し使用されています。このソリューションは電力事業者の責任の元で実施してください。「NERC CIP 認定」を受けることはできませんが、お客様がその目的を達成するのに役立ちます。

NERC CIP の標準規格は、変電所運用の物理的セキュリティ保護とサイバーセキュリティ保護の両方に焦点を当てています。たとえば、物理的セキュリティ境界 (PSP) と電子的セキュリティ境界 (ESP) があります。NER CIP によると、PSP の定義は「大規模電力システムのサイバーアセット、BES サイバーシステム、または電子的なアクセス制御や監視システムが存在する場所を取り囲み、アクセスが制御される物理的な境界」です。ESP は「BES サイバーシステム周囲の保護ゾーン」と定義されている論理的な境界です。BES サイバーシステムは、BES サイバーアセットで構成されます。

NER CIP によると、PSP の定義は「大規模電力システムのサイバーアセット、BES サイバーシステム、または電子的なアクセス制御や監視システムが存在する場所を取り囲み、アクセスが制御される物理的な境界」です。シスコ変電所アーキテクチャに従って、PSP はさらに次のゾーンに分類されます。

- 変電所コアゾーン
- 電子的セキュリティ境界 (ESP) ゾーン
- マルチサービスゾーン
- 企業変電所ゾーン

変電所の統合と自動化アーキテクチャでは、さまざまなサプライヤのデバイスが業界標準のプロトコルを使用して通信 (相互運用) できるようにする必要があります。電力事業者は、各アプリケーションに最適なデバイスを柔軟に選択できます。ただし、デバイスが業界標準のプロトコルを使用して機能を完全に発揮できるように、サプライヤによって設計されている必要があります。電力事業者で一般的に使用されているプロトコルの一部を以下に示します。

レガシー非同期インターフェイスでサポートされるレガシー SCADA プロトコルは、次のとおりです。

- Modbus
- DNP3
- IEC 60870-5-101

イーサネット インターフェイスを介して転送できる新しい SCADA プロトコルは、次のとおりです。

- IP ベースのプロトコル:
  - Modbus-IP
  - DNP3-IP
  - IEC 60870-5-104
  - IEC 61850 MMS
- レイヤ 2 ベースのプロトコル:
  - IEC 61850 GOOSE
  - IEC 61850 SV

IEC 61850

この国際規格では、変電所の「インテリジェント電子機器」の通信プロトコルが定義されています。世界中の電力事業者が変電所の自動化をデジタル化することに重点を置いているため、このデジタル トランスフォーメーションの重要事項として、この標準規格が採用されています。この標準規格は、以下をはじめとした多くの概念を確立または言及しています。

- 以下を含む、さまざまな用途のデータモデルと通信モデル:
  - イーサネットおよび TCP/IP 経由でリアルタイムプロセスと SCADA データを転送するための Manufacturing Message Specification (MMS)

  - マルチキャスト イーサネット メカニズムを使用して、変電所内の IED 間で厳密な間隔 (4 ミリ秒) でデータ (ステータス、値) を転送するための汎用オブジェクト指向変電イベント (GOOSE)。
  - サンプル値 (SV) は、イーサネット経由で測定デバイスからサンプリングされたアナログ測定値を公開するメカニズムです。
- ネットワーク インフラストラクチャを含む変電所設備の建設、設計、および運用条件。
- 変電所設備の適合性および相互運用性テスト。

このプロトコルのサポートは、このソリューションの重要事項です。61850 通信プロトコルについては、プロトコルについて大きく取り上げる ESP セクションで詳しく説明します。

技術要件の概要

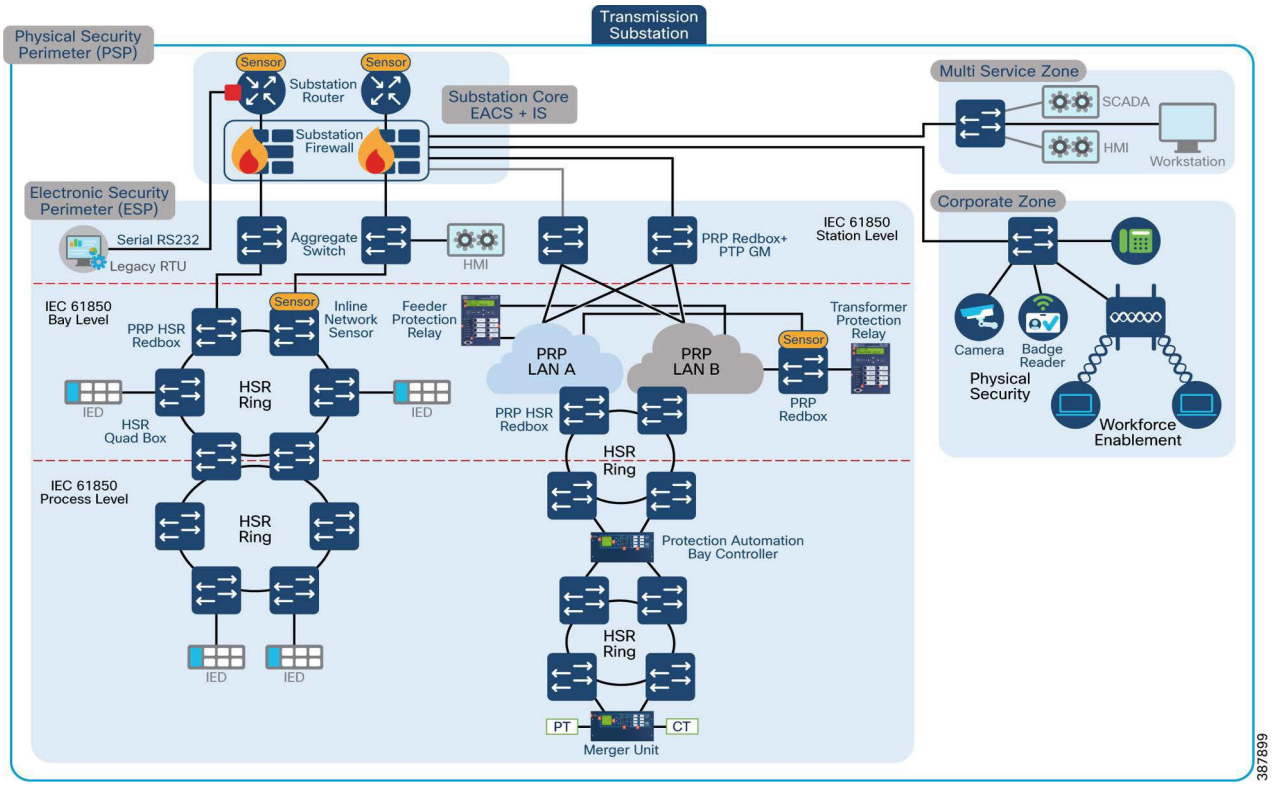
変電所自動化ソリューション設計の主要な技術要件は、以下のとおりです。

- IEC 61850-Goose トラフィックなど、重要な変電所通信のネットワーク遅延とジッターが低く抑えられていること
- ネットワーク障害 (リンク損失、デバイス障害など) の発生時に迅速に回復し、通信損失を削減または排除する復元力を備えたネットワークであること
- スケール
- セキュリティ
- サービスアビリティ
- ユーザビリティ

変電所自動化リファレンスアーキテクチャ

現代の電力事業ネットワーク全体は分散環境下にあり、グリッドオペレータとコントローラは変電所内に物理的に配置されていません。実際、電力事業者のオペレータは、ワイドエリアネットワーク (WAN) インフラストラクチャを介して接続されたリモート運用・制御センターから作業することが一般的です。オペレータは、遠隔地にある変電所を管理するために遠隔監視制御･情報取得 (SCADA) アプリケーションを使用します。図 2 は、シスコの新たなデジタル変電所自動化のリファレンスアーキテクチャを示しています。

図 2　　変電所自動化リファレンスアーキテクチャ



シスコの新しいデジタル変電所アーキテクチャは、運用・制御センター (緩衝地帯 Z)、WAN 層、送電変電所の物理的セキュリティ境界 (PSP)、および他の二次変電所、ローカルマルチサービス、企業ネットワークの WAN 接続で構成されます。さらに、PSP は、変電所コア、電子的セキュリティ境界 (ESP)、マルチサービス、および企業 (CORP) ゾーンに分割されます。IEC 61850 標準に基づいて、ESP はさらにステーション、ベイ、およびプロセスレベルに細分化されます。

変電所コアと WAN ネットワーク

変電所コアゾーンは、NERC CIP の電子的アクセスポイント (EAP) と中継システム (IS) に従って、2 つの異なるインターフェイスを提供します。EAP は、電子的セキュリティ境界上のサイバー アセット インターフェイスであり、電子的セキュリティ境界外のサイバーアセットと電子的セキュリティ境界内のサイバーアセット間でルータブルな通信を可能にします。中継システムは、許可されたユーザーのみにインタラクティブ リモート アクセスを制限するためにアクセス制御を実行する 1 つまたは一連のサイバーアセットです。中継システムは、電子的セキュリティ境界内に配置してはなりません。

変電所ルータとファイアウォールは変電所コアゾーンに配置され、EAP および IS 機能を提供します。変電所ルータは、変電所のローカルエリアネットワークと電力制御またはエンタープライズ WAN 間のインターフェイスとして機能します。WAN は長距離データ通信を介してアクセスされる遠隔地のセグメントで構成されているため、電力事業者が所有する WAN またはコモンキャリアを使用できます。変電所ルータが電力事業者所有のバックホール/MPLS ネットワークの一部として接続されている場合、オンネット変電所ルータで変電所ルータを定義します。変電所ルータがパブリック/セルラーネットワークに接続されている場合、変電所ルータはオフネット変電所ルータと呼ばれます。

シスコ変電所ルータは、インラインファイアウォール (ゾーンベースのファイアウォール) 機能を提供できます。または、変電所ルータ以外に専用のファイアウォールを配置して、ESP、マルチサービス、および企業ゾーンを保護することもできます。これにより、変電所の端に Demilitarized Zone (DMZ; 緩衝地帯) が必要な独自の設計になります。変電所ネットワークに出入りするすべての通信は、DMZ ファイアウォールを通過する必要があります。変電所のエッジから出るゾーントラフィックは、

IPSec を使用して暗号化し、レイヤ 3 バーチャル プライベート ネットワーク (L3VPN) テクノロジーを使用して個別の論理ネットワークに分離する必要があります。

シスコによる変電所自動化ネットワーク設計のベストプラクティスでは、WAN を通過するゾーントラフィックについては、L3VPN を分離することが推奨されています。これにより、共有インフラストラクチャは、物理的には共通しているが論理的に分離されたネットワークを介してゾーントラフィックを伝送できます。電力事業者所有のプライベート WAN のマルチプロトコル ラベル スイッチング (MPLS) またはサービスプロバイダーの専用線サービスは、このモデルの実現に役立ちます。これは、セグメンテーションに関するシスコのセキュリティ推奨事項と一致しています。

変電所のエッジにある DMZ ファイアウォールは、変電所への制御されたアクセスを提供するのに役立ちます。また、変電所ゾーン間のセグメンテーションと分離を実現します。変電所の LAN 環境は、IEC 61850 規格で指定されているように、次の 3 つの機能コンポーネントブロックまたはゾーンで構成されます。

- マルチサービス
- 企業変電所
- 電子的セキュリティ境界

変電所ルータには、変電所の ESP 内でレガシー RS232 RTU を接続する際に、直接接続するオプションがあります。レガシー SCADA トラフィックをコントロールセンターに転送するための設計オプションは複数あります。これらのオプションについては、「レガシーデバイス接続」のセクションで詳しく説明します。

外部 PTP グランドマスターを変電所ルータに接続して、PTP サービスを ESP ゾーンに提供できます。

電力事業者 WAN

電力事業者 WAN は、多くの場合、送電サービスオペレータ (TSO) のコントロールセンターをさまざまな変電所や他のフィールドネットワークおよびアセットに接続する専用の WAN インフラストラクチャです。電力事業者 WAN 接続には、パブリックバックホール用のセルラー LTE/5G オプション、電力事業者所有のプライベートネットワークに接続するファイバポート、専用回線、MPLS PE 接続オプションに加えて、複数の T1/E1 回線を集約するレガシーマルチリンク PPP バックホールなどの一連のテクノロジーを組み込むことができます。

WAN 回線とバックホール障害オプションは、Cisco SDWAN ソリューションを使用して効率的に設計、プロビジョニング、および管理されます。詳細については、次の URL を参照してください。

https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html

電子的セキュリティ境界 (ESP)

電子的セキュリティ境界は、NERC CIP の CIP-005-5「Cyber Security - Electronic Security Perimeter」で定められているように、「大規模電力システム (BES) のサイバーシステムへの電子的アクセスを管理する目的で」使用される論理的なセグメント化です。ESP ゾーンには、変電所のすべてのグリッド運用インフラストラクチャが含まれます。ESP は変電所で最も重要なゾーンであり、最高水準のセキュリティと可用性が求められます。ESP への電子的アクセスは、電子的アクセス制御システム (EACS) の役割です (NERC CIP の定義を参照)。シスコのアーキテクチャでは、EACS は変電所コアおよび WAN ネットワークの重要な機能です。ESP ネットワークは、変電所インフラストラクチャに重要な通信サービスとサイバー セキュリティ サービスを提供します。オペレーション コントロール センターの SCADA アプリケーションは、変電所インフラストラクチャからデータを収集して変電所の運用を管理するために、ESP へのネットワークアクセスを必要とします。

マルチサービスゾーン

マルチサービスの重要インフラ保護 (CIP) ゾーンには、イーサネット接続のバッジリーダー、ビデオ監視カメラ、ローカル認証、許可、およびアカウンティング (AAA)、ロギングアプリケーションなどの物理的なセキュリティコンポーネントが実装されています。コントロールセンターから変電所の ESP ゾーンへのリモートアクセスが必要な場合は、ジャンプサーバー、または別のセキュリティゾーンでデバイスを管理するために使用するコンピュータをマルチサービスゾーンに設置することを推奨します。マルチサービスゾーンは、Cisco Identity Services Engine (ISE)、Splunk、およびアプリケーションゲートウェイやブローカ機能などのサービスを必要とするダウンストリーム ユーティリティ アプリケーションといったセキュリティアプリケーションの場所に適しています。これらのアプリケーションとサービスのセグメント化は、このゾーン内でも強く推奨されており、仮想 LAN (VLAN) を使用して実現できます。このゾーンは、NERC CIP の電子的アクセス制御システム (EACS) および電子的アクセス監視システム (EAMS) にマッピングされています。

ローカル企業ネットワークゾーン

企業変電所 (CorpSS) ゾーンは、変電所内に企業ネットワークが延長されたものです。ここでは、従業員が電子メール、Web、またはインターネットにアクセス (中央サイトを経由) するためのワイヤレスイーサネット接続 (Wi-Fi)、音声サービス、および一般的なイーサネット接続が提供されます。これは、変電所内にあるリモートロケーションの拡張エンタープライズです。このゾーンは最も安全性の低いゾーンであり、IP 電話、ビデオエンドポイント、企業アプリケーション用の Wi-Fi 接続や有線 PC などのデバイスとサービスが含まれます。このゾーンは、NERC CIP の物理的アクセス制御システム (PACS) および物理的アクセス監視システム (PAMS) にマッピングされます。

オペレーション・コントロールセンター

オペレーション・コントロールセンターは、次のような多くの一元化されたアプリケーションとインフラストラクチャをホストします。

- エネルギー管理システム (EMS) と停電管理システム (OMS)
- 電力事業者 WAN 経由で複数の変電所から送られてきたトラフィックを集約するヘッドエンドルータ (HER)
- さまざまな OT アプリケーションを保護するファイアウォールベースの DMZ
- Cisco の Digital Network Architecture Center、ISE、ワイヤレス LAN コントローラ (WLC)、SDWAN vManage、Firepower Management Center (FMC) などの変電所ネットワークを監視および管理するためのネットワークおよびポリシー管理ツール
- Cyber Vision Center などの産業用サイバーセキュリティツール。

電子的セキュリティ境界ゾーン – 設計上の考慮事項

ESP は重要な変電所の運用をサポートするネットワークです。ネットワークアーキテクチャは、HSR や PRP などのロスレスレジリエンス プロトコルの使用を含め、高可用性の重要性を考慮して設計されています。以下はネットワークアーキテクチャの簡略図です。

電子的セキュリティ境界 (ESP) ゾーンには、すべてのグリッド運用インフラストラクチャが含まれており、最高水準のセキュリティを備えます。このセキュリティゾーンは、SCADA、保護サービス、変圧器の運用などのアプリケーションによってさらに細分化することを強く推奨します。ESP は変電所で最も重要なゾーンであり、最高水準のセキュリティと可用性が求められます。イーサネットネットワークのセグメント化を実現する 1 つの方法は、変電所のエッジファイアウォールで VLAN を終端することです。リモート端末ユニット (RTU)、インテリジェントな電子機器 (IED)、プログラマブル ロジック コントロー

ラ (PLC)、リレー、変圧器、電力モニターなどのデバイスが ESP ゾーン内にあります。ESP ゾーンには、IEC 61850 規格で定められているステーションバスとプロセスバスが含まれています。Cisco ESP ゾーンのリファレンスアーキテクチャ図については、図 4 を参照してください。

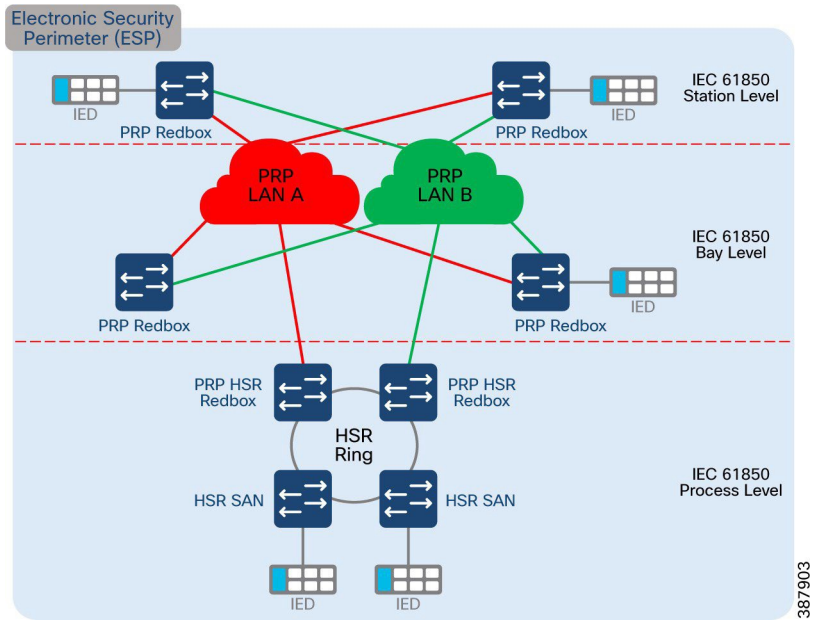
展開モデルは通常、変電所の ESP ゾーンのサイズに基づきます。変電所の IED は、ハブアンドスポーク、リング、ツリーなど、さまざまなトポロジオプションのいずれかに組み込まれた Cisco IE スイッチに接続できます。シスコは、Resilient Ethernet Protocol (REP)、Parallel Redundancy Protocol (PRP)、Highly Available Seamless Ring (HSR) などの可用性の高い冗長化メカニズムを提供しています。トポロジスタイルと冗長化プロトコルの選択肢は、アプリケーションの要件によって異なります。冗長性と復元力については、このセクションの CVD で後から詳しく説明します。

ESP アーキテクチャ

ESP は重要な変電所の運用をサポートするネットワークです。ネットワークアーキテクチャは、HSR や PRP などのロスレス レジリエンス プロトコルの使用を含め、高可用性の重要性を考慮して設計されています。以下はネットワークアーキテクチャの簡略図です。電子的セキュリティ境界は、NERC CIP の CIP-005-5 「Cyber Security - Electronic Security Perimeter」で定められているように、「大規模電力システム (BES) のサイバーシステムへの電子的アクセスを管理する目的で」使用される論理的なセグメント化です。ESP ゾーンには、変電所のすべてのグリッド運用インフラストラクチャが含まれます。ESP は変電所で最も重要なゾーンであり、最高水準のセキュリティと可用性が求められます。ESP ネットワークは、変電所インフラストラクチャに重要な通信サービスとサイバー セキュリティ サービスを提供します。オペレーション コントロール センターの SCADA アプリケーションは、変電所インフラストラクチャからデータを収集して変電所の運用を管理するために、ESP へのネットワークアクセスを必要とします。

次のサンプルトポロジは、さまざまなレベルの ESP ゾーンを示しています。

図 3　　Cisco ESP ゾーンのリファレンスアーキテクチャ



ステーションバス

ステーションバスは変電所全体を接続し、中央管理ベイと個別ベイの間の接続を提供します。ステーションバスは、ベイ内の IED、分散コントローラ、およびヒューマン マシン インターフェイス (HMI) を接続します。また、ベイを相互に接続したり、

ゲートウェイ/ゲートウェイルータにベイを接続したりします。多くの場合、接続される数百の IED は、通信パラメータやアプリケーション/目的に基づいて、物理的または論理的にセグメント化されています。

プロセスバス

プロセスバスは、主要な測定および制御機器を IED に接続します。プロセスバスは、変流器 (CT)、計器用変圧器 (PT)、データ収集ユニット (DAU)、統合ユニット (MU) などの開閉所の送信元デバイスからデータを処理して測定、制御および保護についての決定を行う IED とリレーに未処理の電源システム情報 (電圧と電流のサンプル値、装置のステータス) を送ります。

通常、プロセスバスはベイに限定されますが、バスバー保護および差分保護トラフィックは複数のベイにまたがる場合があります。

ステーションバスとプロセスバスの組み合わせ

ネットワークの観点からステーションバスとプロセスバスを 1 つのネットワーク構造に収めることは可能ですが (1 Gbit/s 以上など、十分な帯域幅がある場合)、さまざまな理由からそれらを分離することが賢明です。たとえば、プロセスバスでのアプリケーション トラフィック量が多い場合には、バスを分離してステーションバスの負荷を減らすことを検討してください。これらのバスを組み合わせる必要がある場合は、プロセスバスとステーションバスを結合するときにシングルポイント障害を回避することを検討してください。

多くの可能なトポロジ設計オプションの詳細については、IEC 61850-90-4 を参照してください。

アプリケーションとプロトコル

IEC 61850

以下は、IEC-61850 から引用したトラフィッククラスの定義です。

IEC 61850-8-1 で定義されている MMS (Manufacturing Message Specification) トラフィックにより、SCADA、OPC サーバー、ゲートウェイなどの MMS クライアントがすべての IED オブジェクトに「垂直に」アクセスできます。一部のプロセスバスの IED は MMS をサポートしていませんが、このトラフィックはステーションバスとプロセスバスの両方を流れます。MMS プロトコルは、ネットワーク層 (レイヤ 3) で動作するクライアント/サーバー (ユニキャスト) プロトコルです。したがって、IP アドレスで動作し、ルータを越えることができます。1 つの動作モードでは、MMS クライアント (一般に SCADA またはゲートウェイ) は、特定のデータ項目の要求を、その IP アドレスで識別される IED の MMS サーバーに送信します。サーバーは、要求されたデータを応答メッセージでクライアントの IP アドレスに返します。別のモードでは、クライアントは、イベントの発生時に自発的に通知を送信するようにサーバーに指示できます。

GOOSE (Generic Object-Oriented Substation Events) は、IED がベイ内またはベイ間で「水平に」データを交換することを可能にします。これが、回路ブレーカーのインターロック、測定、トリップなどの作業に使用されます。通常、GOOSE はレイヤ 2 マルチキャストトラフィックに基づいて、ステーションバス上を流れますが、それをプロセスバスや WAN にまで拡張できます。GOOSE では短い情報メッセージが使用されます。GOOSE の要件では、損失が発生する可能性が低いこと、またバジェット遅延はわずか数ミリ秒であることが定められています。

サンプル値 (SV) プロトコル (IEC 61850-9-2 で定義) は主に、センサーから IED にアナログ値 (電流と電圧) を送信するために使用されます。このトラフィックは、通常はプロセスバスを流れますが、バスバー保護や位相測定などのために、ステーションバスを流れることもあります。

ESP トラフィック要件

IEC 61850-8-1 規格に従って、GOOSE では、時間的制約のある重要なコミュニケーションについては、パブリッシャ/サブスクライバ通信を使用します。GOOSE は、任意の形式のデータ (ステータス、値) がデータセットにグループ化された後に送

信される制御モデルです。GOOSE データはイーサネットデータフレームに直接埋め込まれており、伝送速度と信頼性を確保するためのメカニズムが搭載されています。

GOOSE は、IED がベイ内またはベイ間で「水平に」データを交換することを可能にします。これが、回路ブレーカーのインターロック、測定、トリップなどの作業に使用されます。通常、GOOSE はレイヤ 2 マルチキャストトラフィックに基づいて、ステーションバス上を流れますが、それをプロセスバスや WAN にまで拡張できます。GOOSE では短い情報メッセージが使用されます。GOOSE の要件では、損失が発生する可能性が低いこと、またバジェット遅延はわずか数ミリ秒であることが定められています。

GOOSE は変電所内の IEC 61850 トラフィックタイプの 1 つです。タイムセンシティブな性質があり、低遅延の転送を必要とします。レイヤ 2 ドメイン内での識別と分類を容易にするために、一般的な 0x88b8 の EtherType が使用されます。一方、SV パケットでは、一般的な 0x88bA の EtherType が使用されます。

GOOSE トラフィックは、多少の到着間隔のジッターや遅延に対処できます。GOOSE では、SV トラフィック (およびレイヤ 2 マルチキャスト) と比較すると、優先処理がわずかに劣ることがあります。

IEC 61850 では、ネットワークでの PCP を使用した分類と優先処理のために、IED によってマークが付けられた VLAN ID 0 を使用して、GOOSE およびサンプル値 (SV) フレームに優先順位のタグが付けるように規定されています。IEEE C37.238-2011 では、VLAN タグの使用が義務付けられています。今後のリビジョンでは、VLAN がオプションになる可能性があります。GOOSE、SV、および C37.238-2011 のデフォルトでは、優先順位コードポイント (PCP) 値を 4 にして、優先順位がタグ付けされます。

IED QoS の優先順位付けは、電力システムのエンジニアリング段階で割り当てられ、変電所構成記述 (SCD) ファイルに記録されます。ネットワークが QoS 値を再度マーク付けすることを決定した場合、エンジニアリング設計への影響を考慮してください。

遅延要件が 3 ミリ秒から 100 ミリ秒の GOOSE トラフィックには、複数のタイプとクラスがあります。IEC 61850-90-4 の QoS 分類では、トリップおよびインタートリップの GOOSE フレームは有線優先順位を高くする必要があると述べられています。

インターロック用の GOOSE フレームの優先順位は中程度にする必要があります。最後に、ハートビートやアナログ値などの他の GOOSE フレームには、中程度の優先順位を割り当てる必要があります。

さまざまな GOOSE、SV、MMS、および時刻同期メッセージと、それらのアプリケーションや通信要件を区別するのに役立つ詳細情報を表 2 に記載しています。

表 2　　IEC 61850 プロトコルと要件

通信バス	w機能タイプ/メッセージ		プロトコル	最長遅延	帯域幅	優先順位	アプリケーション
プロセス	1A、トリップ	GOOSE	レイヤ 2 マルチキャスト	3 ミリ秒未満	低	高	保護
プロセス	1B. その他	GOOSE	レイヤ 2 マルチキャスト	200 ミリ秒未満	低	高	保護
プロセスとステーション	2. 中速	MMS	IP/TCP	100 ミリ秒未満	低	低 ~ 中	制御
プロセスとステーション	3. 低速	MMS	IP/TCP	500 ミリ秒未満	低	低 ~ 中	制御
プロセス	4. raw データ	SV	レイヤ 2 マルチキャスト	208.3 ミリ秒未満	大きい	大きい	プロセスバス
プロセスとステーション	5. ファイル転送	MMS	IP/TCP/FTP	1000 ミリ秒未満	中	低い	管理

プロセスと ステーション	6. 時刻の同期	時刻の 同期	PTP (レイヤ 2)		低	中 ~ 高	一般的な位相、SV
ステーションバス	7. コマンド	MMS	IP		Low	低 ~ 中	制御

ステーションバスとプロセスバスのプロトコルの場所

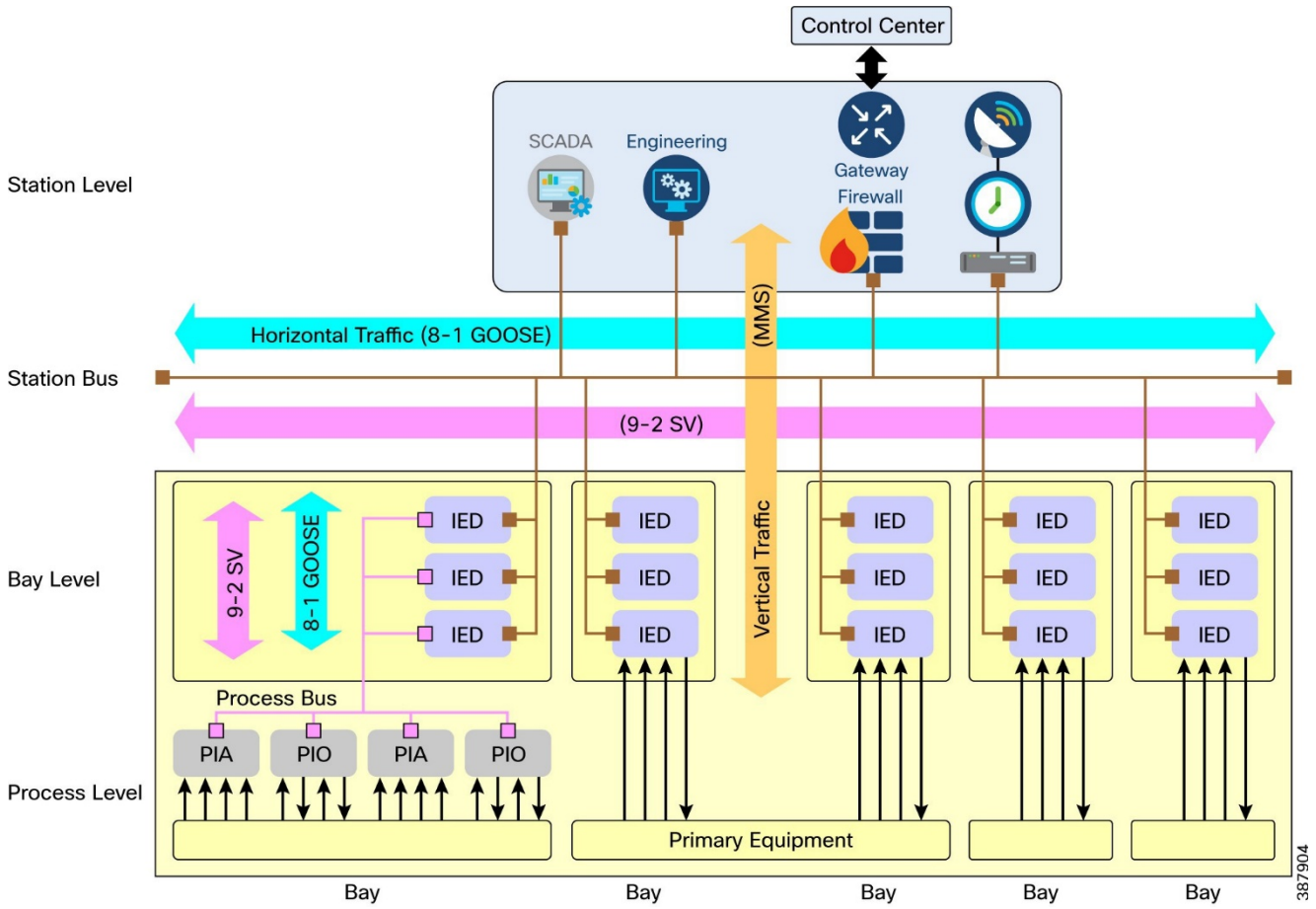
ステーションバスで一般的に見られるプロトコルには、GOOSE (レイヤ 2 マルチキャスト)、MMS、SNTP、SNMP、FTP など (他には伝送制御プロトコル (TCP)/IP やユーザー データグラム プロトコル (UDP)/IP レイヤ 3 ユニキャスト) があります。

プロセスバスで見られるプロトコルは、SV (レイヤ 2 マルチキャスト) です。GOOSE (レイヤ 2 マルチキャスト) トラフィックや、MMS (レイヤ 3 ユニキャスト) トラフィックの場合もあります。プロセスバスデバイスを接続するインフラストラクチャは、重要なトラフィックにリアルタイムのサービス品質を提供することが期待されています。

ステーションバスから SV トラフィックを強制的に排除するという厳しい要件はありません。実際、バスバーの保護では、ステーションバスの SV トラフィックが必要になる場合があります。この場合、ステーションバスでこうした SV トラフィックのジッターとレイテンシの許容度を低く保つために、QoS を設定する必要があります。

図 4 は IEC 61850 規格から直接引用したものです。ステーションバスとプロセスバスで MMS、GOOSE、および SV トラフィックが通常確認される場所を示しています。

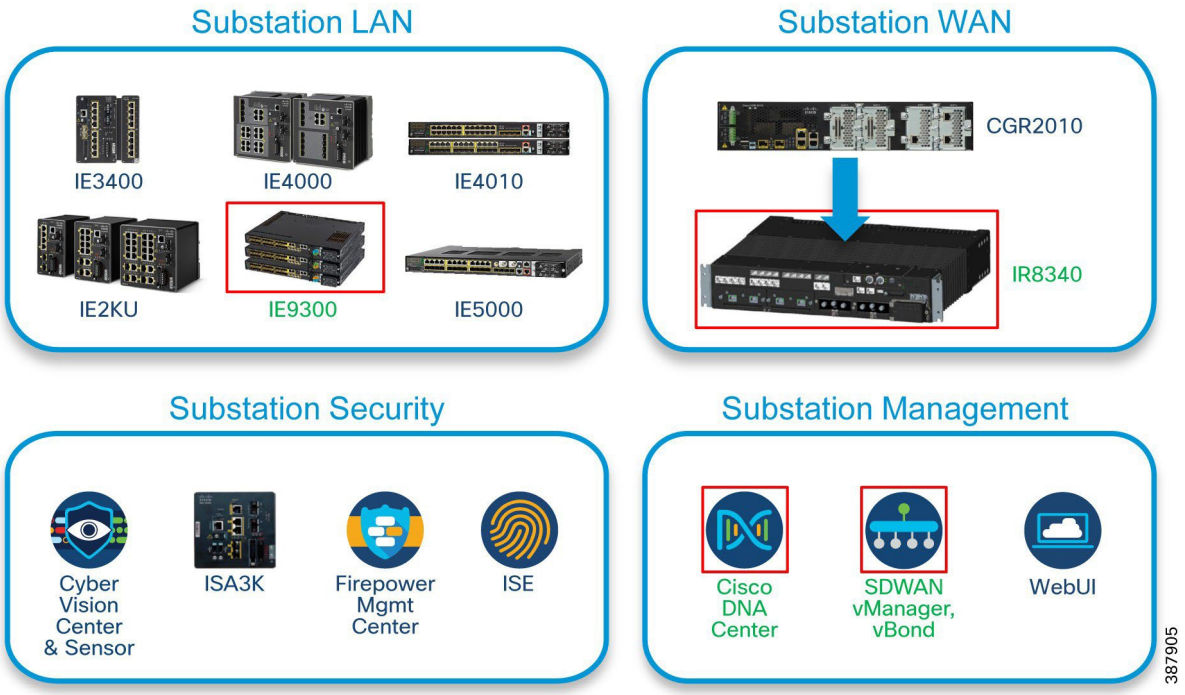
図 4　　ステーションプロセスとプロセスバスで MMS、GOOSE、SV が確認される場所



ESP ポートフォリオ

このセクションでは、変電所自動化ソリューションで ESP 向けの主要な製品を紹介します。ESP ネットワークとセキュリティインフラストラクチャの構成、監視、管理に使用されるネットワークおよびセキュリティ製品について説明します。サイバーセキュリティとネットワーク管理ツールの設計ガイダンスは、他のセクションまたはドキュメントに記載されています。以下は、変電所 ESP インフラストラクチャの主要部分を示しています。

図 5　　変電所自動化 LAN ポートフォリオ



ネットワークおよびサイバーセキュリティ ポートフォリオは、さまざまな面で数多くの重要な役割を果たしています。以下の表は、それらの役割と関連する製品を示しています。

表 3　　役割と製品

役割	製品
変電所ルータ、ゾーンベースのファイアウォール電子的アクセス制御システムと中継システム、レガシーデバイス接続	IR8300
ステーションバススイッチ	IR8300、IE9300、IE5000、IE3400、IE4000、IE4010
電力プロファイルをサポートするプロセスバススイッチ	IE9300、IE3400、IE4010、IE4000
変電所ファイアウォール	ISA3000
企業ゾーンおよび CIP ゾーンスイッチ	IE5000、IE4000、IE2000
企業ゾーン内の Wi-Fi アクセスポイント	IW6300
中央ヘッドエンドルータ	ASR1K
中央ヘッドエンド ファイアウォール	FPR4150
OT 可視化マネージャ	Cyber Vision Center

表 3　　役割と製品

役割	製品
OTインラインセンサー	IE3400、IE9300、IR8300 で動作するサイバービジョンセンサー
PRP RedBox	IE5000、IE4000、IE4010、IE9300、IR8340
PRP HSR RedBox および HSR QuadBox	IE4000
PRP インフラストラクチャ スイッチ	IE4000、IIE2000u、E4010、IE3400、IE9300
HSR SAN	IE4000、IE4010、IE3400、IE5000
PTP グランドマスター	IE5000、IR8340
PTP トランスペアレントクロック	IE5000、IE4000、IE4010、IE9300、IR8340
PTP 境界クロック	IE5000、IE4000、IE4010、IE9300、IR8340
PRP を介した PTP	IE5000、IE9300、IE4000、IE4010
変電所 LAN ネットワーク管理	DN2-HW-APL (L と XL を含む)
変電所 WAN 管理	vManage

注: IE2000 SKU は PTP 電源プロファイルをサポートしていません。

一般的な変電所設備の要件

一般的な変電所設備の要件の一部を以下に示します。各設備の正確な情報については、それぞれのプラットフォームガイドを参照してください。

- IEEE 1613 および IEC 61850-3 への準拠 - すべての製品が KEMA サードパーティの検証に合格
- 稼働寿命を延ばすため、可動部品のないネットワーク インフラストラクチャ
- 電力事業に固有の機能が追加された高度な IOS ソフトウェア機能
- すべてのスイッチシリーズの特定のモデルでの PoE/PoE+ サポートによる電力と接続の組み合わせ
- レイヤ 2 LanBase またはフルレイヤ 3 の IP サービスイメージが利用可能
- 交換在庫を減らして導入を簡素化するため、製品ライン全体で共通電源を使用
- 復元力のある運用のための冗長電源入力または電源
- 広い電源範囲をサポート (低および高電圧 AC/DC をサポート)
- IEEE 1588 v2 PTP が C37.238 (電力プロファイル) をサポートし、エンドデバイスクロックを同期化
- Modbus メモリマップをサポート (統計の表示のみ)
- 広い範囲の動作温度をサポート -40 C ~ +75 C
- アラームコンタクト - 入力および出力
- すべてのコンポーネント (電源を含む) に適用される 5 年間の期限付きハードウェア保証
- 現場での交換が容易なスワップドライブ

- Dying Gasp
- デバイスの交換を簡素化する SD-Flash

Cisco IR 8300

Cisco Catalyst IR8300 高耐久性シリーズ ルータは、シスコ初の産業グレードの完全統合型ルーティングおよびスイッチング プラットフォームです。IR8300 は、業界をリードする Cisco Catalyst 製品を強化する Cisco Unified Access Data Plane (UADP) Application-Specific Integrated Circuit (ASIC) および Quantum Flow Processor (QFP) 上に構築されており、ネットワーク進化の最新のニーズに対応する優れた柔軟性と適応性を提供するように設計されています。IR8300 は、米国の公共安全 FirstNet サービスと新しい 5G サービスをサポートし、高速化されたサービス、多層セキュリティ、エッジ インテリジェンス向けに構築されています。エネルギー、運輸、石油天然ガス産業に見られる過酷で厳しい環境に配備できます。詳細については、https://www.cisco.com/c/en/us/products/collateral/routers/catalyst-ir8300-rugged-series-router/nb-06-cat-ir8340-rugged-ser-rout-ds-cte-en.html [英語] を参照してください。

IR8300 は変電所アーキテクチャにおいて多くの役割を果たします。電力事業者 WAN、EACS、LEAP、復元力のあるステーションバススイッチ、ゾーンベースのファイアウォールに復元力のある送電や配電を行う変電所のヘッドエンドルータとしての役割などが含まれます、Cyber Vision Sensor、PTP グランドマスタークロックをホストし、レガシーデバイスにシリアルベースの接続を提供します。この製品は、Cisco の DNA-Center または vManage のいずれかによって管理されます。

図 6　　Cisco IR 8340

Cisco Catalyst IR8340 は、変電所コアゾーンに送電変電所ルータとして導入できます。さらに、IR8340 は OT フローとアセットの可視性をキャプチャするためのネットワークセンサーの Cyber Vision として機能できるだけでなく、インラインファイアウォールや VPN 終端として機能することもできます。

IR8340 の詳細については、「変電所コアおよび電力事業者 WAN」のセクションを参照してください。

Cisco IE 9300

Cisco Catalyst IE9300 高耐久性シリーズ スイッチは、高密度な光ファイバポートスイッチです。特に設置面積が小さく、堅牢なフォームファクタを備えた変電所 LAN アーキテクチャのパフォーマンスの課題に対応するように設計されています。Catalyst IE9300 は変電所の自動化と管理にアプローチする新しい方法の一部です。最近リリースされた Catalyst IR8300 高耐久性シリーズ ルータとともに、変電所の LAN と WAN を統合する検証済みのアーキテクチャを提供し、グリッドの近代化に必要なパフォーマンス、セキュリティ、スケール、および管理を強化します。

Cisco IE9300 は、ステーションバスおよびプロセスバスの PRP LAN インフラストラクチャ スイッチ、PRP RedBox として導入できます。IE9300 の詳細については、以下を参照してください。

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-ie9300-rugged-series/catalyst-ie9300-rugged-series-ds.html

図 7　　Cisco IE9300

シスコ機器と参考資料を次の表に示します。

表 4　　製品と参考資料

Cisco 識別子	参照URL
IE3300	http://www.cisco.com/go/ie3300
IE3400	http://www.cisco.com/go/ie3400
IE4000	http://www.cisco.com/go/ie4000
IE4010	http://www.cisco.com/go/ie4010
IE5000	http://www.cisco.com/go/ie5000
Cyber Vision	https://www.cisco.com/c/en/us/support/security/cyber-vision/series.html
ASR1000	http://www.cisco.com/go/asr1k

復元力とトポロジ

復元力は、ネットワーク障害が発生した場合でもサービスを提供する通信ネットワークの能力と、障害発生時に復元にかかる時間で定義できます。スイッチやリンクなどの追加のネットワーク要素を導入することで、信頼性が向上し、リンクの損失やスイッチの動作障害が発生した場合でも通信が維持されます。冗長トポロジは、通信を中断させ、ネットワークの非冗長部分にも影響を与える可能性のあるシングルポイント障害を回避します。電力事業者の変革で、さまざまなネットワーク接続にイーサネットを採用する場合、レジリエンスプロトコルの選択肢がいくつかありますレジリエンスプロトコルを選択する前に考慮すべき重要事項のいくつかを以下に示します。

- 変電所のアプリケーション、特に運用を維持するための通信の重要性
- ネットワークトポロジ。一部のレジリエンスプロトコルは、特定のトポロジを念頭に置いて設計されています。
- 通信許容レベル。一部のアプリケーションは、通信でさまざまなレベルの伝送損失が発生しても動作するように設計されています。
- 重要なフローとそれらが通過するネットワーク インフラストラクチャを把握する論理データフローとトラフィックパターン
- さまざまなタイプのトラフィックの遅延要件
- レジリエンスプロトコルを使用したネットワークの管理、導入、および監視は、多くのネットワーク管理アプリケーションでサポートされていない可能性があるため、手動での設定と監視が必要になる場合があります
- 時刻同期と精度
- リモート接続では、ネットワークの復元力の重要性が高まります。
- 拡張性。一部のレジリエンスプロトコルにはサイズに制限があります (リングサイズなど)。
- アップグレード能力。レジリエンスプロトコルが呼び出される可能性があり、ネットワーク インフラストラクチャをアップグレードする場合に考慮が必要です。
- 相互運用性。さまざまなネットワークベンダーが多様なレジリエンスプロトコルをサポートしているため、ベンダーが混在すると、選択したレジリエンスプロトコルの相互運用性を考慮する必要が生じます。
- コスト。復元力を導入すると、インフラストラクチャの追加やトラフィックの増加により、一般的に追加コストがかかります。

シスコは、Resilient Ethernet Protocol (REP)、Parallel Redundancy Protocol (PRP)、Highly Available Seamless Ring (HSR) などの可用性の高い冗長化メカニズムを提供しています。次のセクションでは、さまざまなレジリエンスプロトコルについて説明します。プロトコルは次のとおりです。

- スパニングツリープロトコル (STP): STP は、最も一般的なレイヤ 2 レジリエンスプロトコルであり、相互運用が可能です。他のプロトコルに比べて回復に時間がかかり、効果が小さいため、変電所 LAN ネットワークでは推奨されません。
- Resilient Ethernet Protocol (REP): REP は、リングおよび同心リングトポロジに使用されるシスコ独自のプロトコルです。30 ~ 50 ミリ秒で回復するため、変電所アプリケーションに適している場合があります。
- Parallel Redundancy Protocol (PRP): Parallel Redundancy Protocol (PRP) は、国際規格 IEC 62439-3 で定義されています。PRP は、イーサネット ネットワークでヒットレス冗長性（障害後の回復時間ゼロ）を提供するように設計されています。
- High-availability Seamless Recovery (HSR): HSR は国際規格 IEC 62439-3-2016 第 5 条で定義されています。HSR は PRP のようなロスレスプロトコルですが、HSR はリングトポロジで動作するように設計されています。

PRP や HSR などのロスレス レジリエンス プロトコルを使用すると、ネットワーク障害が発生した場合でも、変電所の ESP ゾーンの重要なリアルタイムトラフィックを時間通りに配信できます。イーサネットリンクやスイッチ全体でダウンタイムが発生しても、重要なアプリケーション トラフィック全体が失われることはありません。したがって、遅延要件は守られます。

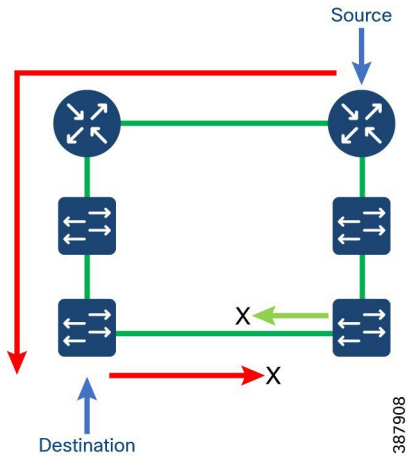
スパニングツリープロトコル

スパニングツリープロトコルは、ネットワーク内のループを回避しながらパスを冗長化するためのレイヤ 2 リンク管理プロトコルです。レイヤ 2 イーサネット ネットワークの正常な動作を実現するには、どの 2 つのステーション間でもアクティブ パスを 1 つにする必要があります。エンド ステーション間に複数のアクティブ パスがあると、ネットワークにループが生じます。このループがネットワークに発生すると、エンド ステーションにメッセージが重複して到着する可能性があります。また、スイッチも複数のレイヤ 2 インターフェイスのエンド ステーション MAC アドレスを学習する可能性が出てきます。このような状況によって、ネットワークが不安定になります。スパニングツリーの動作は透過的であり、エンド ステーション側で、単一 LAN セグメントに接続されているのか、複数セグメントからなるスイッチド LAN に接続されているのかを検出することはできません。

STP は、スパニングツリー アルゴリズムを使用し、スパニングツリーのルートとして冗長接続ネットワーク内のスイッチを 1 つ選択します。スパニングツリー アルゴリズムは、アクティブトポロジでのポートの役割に基づいて各ポートに役割を割り当てることにより、スイッチドレイヤ 2 ネットワーク上で最良のループフリーパスを算出します。

シスコの産業用イーサネットルータおよびスイッチでは、3 つのモードのスパニングツリーがサポートされています。Per VLAN Spanning Tree (PVST+)、Rapid Per VLAN Spanning Tree (RPVST+)、および Multiple Spanning Tree Protocol (MSTP) です。

図 8　　スパニングツリープロトコル



PVST+ : このスパニングツリー モードは、IEEE 802.1D 標準およびシスコ独自の拡張機能に準拠します。すべてのイーサネット ポートベースの VLAN で使用されるスパニングツリーのデフォルト モードです。PVST+ はスイッチ上の各 VLAN でサポートされる最大数まで動作し、各 VLAN にネットワーク上でのループフリー パスを提供します。

Rapid PVST+ : このスパニングツリー モードは、IEEE 802.1w 標準に準拠した高速コンバージェンスを使用する以外は PVST+ と同じです。高速コンバージェンスを行うため、Rapid PVST+ はトポロジ変更を受信すると、ポート単位でダイナミックに学習した MAC アドレス エントリをただちに削除します。このような場合、PVST+ では、ダイナミックに学習した MAC アドレス エントリには短いエージング タイムが使用されます。

MSTP : このスパニングツリー モードは IEEE 802.1s 標準に準拠しています。複数の VLAN を同一のスパニングツリー インスタンスにマッピングし、多数の VLAN をサポートする場合に必要となるスパニングツリー インスタンスの数を減らすことができます。MSTP は、（IEEE802.1 W に基づいて）RSTP の上で稼働します。これは、転送遅延をなくし、ルート ポートと指定ポートを迅速にフォワーディング ステートに移行することで、スパニングツリーの高速コンバージェンスに対応します。MSTP を稼働する場合、RSTP は必須です。

このソリューションでは、相互運用性を考慮して、Rapid Per VLAN Spanning Tree プロトコルと MSTP の使用を推奨します。通常、スパニングツリーは、IEC61850 などの多くの変電所アプリケーションに対して十分な速さで回復しません。スパニングツリーに基づく迅速な可用性とループ保護を実現するため、スイッチのアクセスポートで PortFast を有効にすることを推奨します。

設計上の考慮事項

- RSTP は、自動 LAN 構成とループ防止を主な目的としています。新しいシスコプラットフォームの多くでは、高速スパニングツリープロトコルがデフォルトで有効になっているため、物理リンクの接続時にループが自動的に回避されます。
- リンクやブリッジの障害に対する冗長性を備えていますが、
- エンドデバイスへのリンク障害に対する復元力を備えていません。通常、ブリッジが失われると、接続されているすべてのデバイスが失われます。
- RSTP は、トランクリンクまたはブリッジに障害が発生した場合にシームレスな回復を提供しません。ステーションバスを使用するほとんどのアプリケーションについては、十分な速さで回復します。
- IEC 62439-1-2012 を参照することを推奨しています。ネットワークの実際のトポロジとトポロジ内のネットワークデバイスの数を認識して、一般的なメッシュトポロジやツリートポロジで最悪の場合に RSTP の回復にかかる時間を計算する方法が示されています 。
- ネットワーク上のすべてのスイッチがデフォルトのスパニングツリー設定で有効になっている場合、最小の MAC アドレスを持つスイッチがルートになります。ルートになるように、最適なスイッチの優先順位を引き上げる (数値を引き下げる) と、スパニングツリーの再計算が強制的に行われ、最適なスイッチをルートとした新しいトポロジが形成されます。ゲートウェイルータ IR8340 をルートにすることを推奨しています。
- スパニングツリー トポロジがデフォルトのパラメータに基づいて算出された場合、スイッチド ネットワークの送信元エンド ステーションから宛先エンド ステーションまでのパスが最適にならない場合があります。たとえば、ルート ポートよりプライオリティの高いインターフェイスに高速リンクを接続すると、ルート ポートが変更される可能性があります。最高速のリンクをルートポートにすることが重要です。ギガビット イーサネット ポートのスパニングツリー ポート プライオリティをルート ポートより高くする（数値を小さくする）と、ギガビット イーサネット ポートが新しいルート ポートになります。

Resilient Ethernet Protocol

Resilient Ethernet Protocol (REP) は、大規模なレイヤ 2 ネットワーク、特にリングトポロジの高速コンバージェンス要件を満たすように設計されたシスコ独自のプロトコルです。REP は、単純なリングベースのトポロジでスパニングツリーの必要

性をなくし、標準のイーサネットハードウェアで動作するように設計されています。REP は、シスコの産業用ルータ (IR8300)、産業用イーサネット (IE)、およびキャリアイーサネット (CE) プラットフォームに実装されています。

REP のメリットは次のとおりです。

- リングトポロジで高速かつ予測可能なコンバージェンスを提供します。通常のコンバージェンス時間は 50 ~ 250 ミリ秒の範囲です。
- 確定的でスケーラブルです。
- スパニングツリーと共存します。業界標準プロトコルである G.8032 は、後に REP から派生したものです。
- 設定が簡単でわかりやすいです。
- 一般的にリングトポロジで展開されます。
- リングとセグメントの階層を使用して、リング、セグメント、および任意のトポロジをサポートします。
- プライマリエッジおよび代替ポートで VLAN を選択してブロックすることで、負荷を分散します。

設計上の考慮事項

- REP トポロジで最適なコンバージェンスを実現するには、1 Gbps の光ファイバスイッチ間リンクが推奨されます。
- REP Fast は、サポート対象のプラットフォームとリンクで有効にできます。

  REP Fast は、ギガビットイーサネットの回復遅延を解決します。リンク障害を検出するキープアライブとして機能するビーコンに依存しています。REP リングインターフェイスが REP Fast で設定されている場合、直接接続されているリングネイバーに特別なビーコンフレームが 3 ミリ秒ごとに送信されます。また、同じネイバーから 3 ミリ秒ごとに特別なビーコンフレームを受信することを想定しています。3 つのビーコンフレームを連続して受信できないと、REP のリンク障害イベントに変換されます。このようにして、REP Fast は 10 ミリ秒以内にダウンしているリンクを検出できます。これは、リンク速度やメディアタイプに関係ありません。REP Fast は、銅線および光ファイバリンクで機能します。銅線ギガビットイーサネットによるリンク障害の検出が遅い問題を解決します。リンク障害が検出されると、通常の REP プロトコルが障害から回復し、代替パスを介してイーサネット転送を再開します。
- REP 管理 VLAN の設定。
- REP セグメントに接続されているデバイスやスイッチの数、REP セグメント内に構成された VLAN の数、および REP セグメントで使用される MAC アドレスの数を考慮する必要があります。この要素の組み合わせが、フェールオーバー時の REP セグメントの回復時間に影響します。
- 電力事業者の変電所自動化ネットワークで推奨されるプラットフォームは、スタックを介して変電所に必要なすべての関連機能を有効にできるスタッキングをサポートしていません。したがって、この設計ガイドでは、単一の配電スイッチを使用することを推奨します。
- Precision Timing Protocol: REP を介した電力プロファイル (c38.238 2011 または 2017) は、一部のプラットフォームではサポートされていません。それぞれのプラットフォームガイドで PTP over REP のサポートを確認することを推奨します。そのため、NTP がアプリケーションに適している場合は、タイミングプロトコルとして使用することを推奨します。たとえば、SCADA や妨害レコーダなどの変電所アプリケーションでは、ミリ秒単位のタイミング精度が必要であり、既存のイーサネット通信ネットワーク上で動作する Network Time Protocol (NTP) システムを使用できます。ステーションバスの展開では通常、ミリ秒の範囲のタイミングを必要とし、より高い精度を必要とするプロセスバスの展開とは異なり、NTP の使用が適しているため、GOOSE および SV メッセージに PTP 電力プロファイルを使用できます。

Parallel Redundancy Protocols (PRP)

Parallel Redundancy Protocol（PRP）は、国際規格 IEC 62439-3 で定義されています。PRP は、イーサネット ネットワークでヒットレス冗長性（障害後の回復時間ゼロ）を提供するように設計されています。PRP は異なる方式を使用します。こ

の方式では、2 つのネットワーク インターフェイスを 2 つの独立した分離されたパラレルネットワーク (LAN-A と LAN-B) に接続することで、(ネットワーク要素ではなく) エンドノードが冗長性を実装します。これらのデュアル通信ノード (DAN) のそれぞれには、ネットワーク内の他のすべての DAN への冗長パスがあります。ネットワーク障害から回復するために、RSTP や REP などのプロトコルを使用してメッシュトポロジまたはリングトポロジで接続されたネットワーク要素によって冗長性を提供できます。この場合、ネットワーク障害が発生するとネットワーク内の一部が再構成され、トラフィックが再び流れるようになります (通常、ブロックされたポートを開くことによって)。これらの冗長性スキームでは、ネットワークが回復し、トラフィックが再び流れるまでに数ミリ秒から数秒かかることがあります。

Cisco IE 4000、Cisco IE 4010、Cisco IE 5000 スイッチ、Cisco IE9300 スイッチ、および Cisco IR8340 変電所自動化ルータが、PRP の復元力を備えています。

設計上の考慮事項

- PRP LAN_A および LAN_B ネットワークは、次の基準を満たす必要があります。
  - 非接続性: LAN A および LAN B ネットワークは、ループを回避するためにレイヤ 2 接続を使用して相互に接続できません。
  - 分離性: LAN A および LAN B ネットワークは、独自の独立したネットワークデバイスと物理接続を備えた別個のネットワークです。
  - 独立性: LAN A のシングル通信ノードは、LAN B の別のシングル通信ノードと通信できませんが、コントロールセンターの SCADA などのアプリケーションとは独立して通信できます。LAN A で障害が発生した場合、PRP LAN A のトラフィックにのみ影響し、PRP LAN B のトラフィックは損失なく流れ続けます。
  - 並列: PRP LAN A と LAN B の両方が同様の LAN トポロジで展開され、これらの LAN に接続された PRP RedBox によって生成された重複パケットを転送するため、いずれかの PRP LAN でネットワーク障害が発生した場合にもロスレスの復元力を提供します。各 LAN で遅延とホップを同じように設定することを推奨します。たとえば、LAN ごとに異なる接続オプションを使用することが考えられます。
- 産業用イーサネットスイッチ (RedBox 以外) を LAN A と LAN B の両方に接続しないでください。LAN A と LAN B の産業用イーサネットスイッチ間の直接リンクは許可されていません。レイヤ 2 パスを使用して直接接続すると、ループが発生します。
- PRP DAN および RedBox が 6 バイトの PRP トレーラをパケットに追加するため、システム MTU 1506 およびシステムジャンボ MTU 1506 をスイッチで有効にする必要があります。
- PRP 監視フレームは個別の VLAN (オプション) で送信でき、QOS 処理のために PRP 監視フレームにマーク付けできます。
- LAN A と LAN B は、RSTP、REP などのレジリエンスプロトコルを実行して、SAN デバイスの各 LAN の復元力を強化できます。LAN は、リングトポロジまたはスタートポロジのいずれかにすることができます。遅延が大きくならないようにするため、両方の PRP LAN に同様のトポロジと接続を使用することを推奨します。
- PRP チャネルは、対象の 1 つの VLAN のみを許可するアクセスポートとして、または対象の複数の VLAN を許可するトランクポートとして設定できます。複数のエンドデバイスが PRP RedBox に接続されており、VLAN を介してピアと通信する必要がある場合に、PRP チャネルをトランクポートとして使用できます。また、PRP RedBox が PRP ネットワークに接続された複数のデバイスを集約するレイヤ 3 ゲートウェイとして配置されている場合にも使用できます。

PRP ネットワークには、さまざまなトポロジを含めることができます。変電所自動化 LAN ネットワークに展開できる PRP トポロジのいくつかの例を以下に示します。

トポロジ例

冗長 LAN ネットワークを備えた基本的な PRP

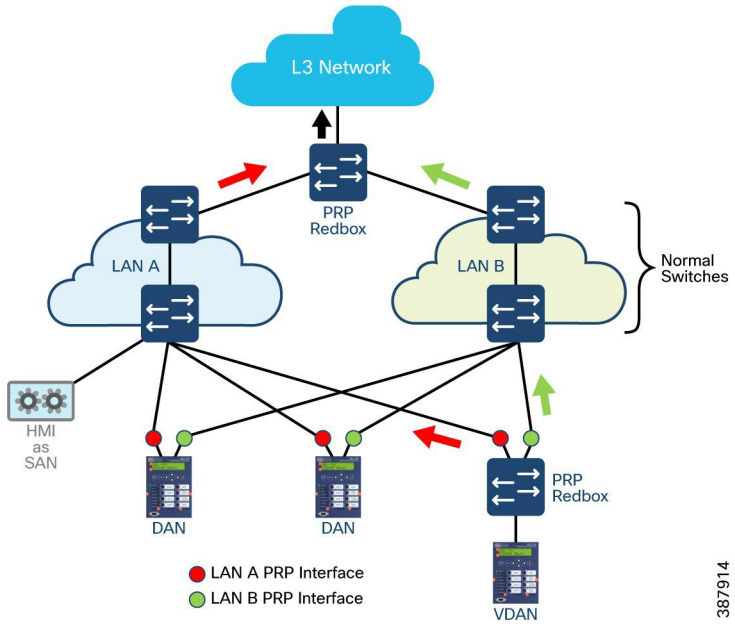
次の図は 2 つの LAN がある PRP トポロジを示しています。各 LAN は多数のスイッチで構成されています。各 LAN のスイッチは、リング内のループを回避するようにスパニングツリーまたは REP を設定して、リングトポロジの形式にすることもできます。各 LAN のスイッチは、シングル通信ノードへの接続を提供できます。このトポロジは、デュアル通信ノード、PRP 対応 IED、またはネットワークデバイスを 2 つのリンクに接続する機能も提供します。1 つは各 LAN に接続されるため、障害が発生した場合に冗長性と復元力が実現します。

DAN は、2 つのネットワーク インターフェイスを介して 2 つのパケットを宛先ノードに同時に送信します。宛先ノードが重複パケットを容易に区別できるように、シーケンス番号を含む冗長制御トレーラ（RCT）が各フレームに追加されます。宛先 DAN は最初のパケットを正常に受信すると RCT を削除してパケットを消費します。2 番目のパケットが正常に到着すると、そのパケットは破棄されます。パスの 1 つで障害が発生した場合、トラフィックは中断されることなくもう一方のパスに流れ続け、回復時間ゼロを実現します。

LAN-A または LAN-B のいずれかにのみ接続するネットワーク内の非冗長エンドポイントは、シングル通信ノード（SAN）と呼ばれます。次の図は、LAN-A のいずれかのスイッチに SAN として接続された HMI を示しています。

冗長ボックス (RedBox) は、2 つのネットワークポートがなく、PRP を実装していないエンドノードが冗長性を実装する必要がある場合に使用されます。このようなエンドノードは、デバイスに代わって 2 つの異なるネットワークへの接続を提供する RedBox に接続できます。RedBox の背後にあるノードは、DAN などの他のノードに表示されるため、「仮想 DAN (VDAN)」と呼ばれます。RedBox 自体は DAN であり、VDAN に代わってプロキシとして機能します。次の図は、PRP をサポートしていないが冗長性が必要な IED を PRP RedBox 機能をサポートするシスコの産業用イーサネットスイッチに接続すると、IED に冗長性と復元力が提供されることを示しています。

図 9　　冗長 LAN ネットワークを備えた基本的な PRP



このトポロジの主な特徴は次のとおりです。

- 2 つのパラレルネットワークによるロスレス冗長性。
- LAN A および LAN B のスイッチは、PRP プロトコルを認識する必要はなく、LAN 間にリンクや共有スイッチがない限り、スターやリングなどのトポロジをサポートできます。

- 独立した LAN A および LAN B ネットワーク インフラストラクチャとリンクの必要性による高コスト
- IEC 62439-3 標準規格第 4 条 (PRP と HSR の両方の標準規格)
- PRP RedBox は、IE-4000、IE-4010、IE-5000、IE-9300、IR8340 および一部の IE-2000u SKU (8、16 ポート) でサポートされています。
- Cyber Vision Sensor、Stealthwatch、Digital Network Architecture Center などのアプリケーションはシームレスに動作します。これらのアプリケーションは、ステートフルなレイヤ 3 接続を使用します。たとえば、Cyber Vision セッションタイムアウトのキープアライブが秒単位で長いため、PRP を介した Cyber Vision Center と Sensor 間の到達可能性やステートフルセッションは影響を受けません。Stealthwatch と Digital Network Architecture Center でも同様の事実が確認されました。詳細については、グリッドセキュリティガイドおよびこのガイドの関連セクションを参照することを推奨します。

冗長レイヤ 3 接続を備えた PRP

次の図は 2 つの LAN がある PRP トポロジを示しています。各 LAN は多数のスイッチで構成されています。各 LAN のスイッチは、リング内のループを回避するようにスパニングツリーまたは REP を設定して、リングトポロジの形式にすることもできます。各 LAN のスイッチは、シングル通信ノードへの接続を提供できます。このトポロジは、デュアル通信ノード (DAN)、PRP 対応 IED、またはネットワークデバイスを 2 つのリンクに接続する機能も提供します。1 つは各 LAN に接続されるため、障害が発生した場合に冗長性と復元力が実現します。DAN は、2 つのネットワーク インターフェイスを介して 2 つのパケットを宛先ノードに同時に送信します。宛先ノードが重複パケットを容易に区別できるように、シーケンス番号を含む冗長制御トレーラ（RCT）が各フレームに追加されます。宛先 DAN は最初のパケットを正常に受信すると RCT を削除してパケットを消費します。2 番目のパケットが正常に到着すると、そのパケットは破棄されます。パスの 1 つで障害が発生した場合、トラフィックは中断されることなくもう一方のパスに流れ続け、回復時間ゼロを実現します。

LAN-A または LAN-B のいずれかにのみ接続するネットワーク内の非冗長エンドポイントは、シングル通信ノード（SAN）と呼ばれます。次の図は、LAN-A のいずれかのスイッチに SAN として接続された HMI を示しています。

冗長ボックス (RedBox) は、2 つのネットワークポートがなく、PRP を実装していないエンドノードが冗長性を実装する必要がある場合に使用されます。このようなエンドノードは、デバイスに代わって 2 つの異なるネットワークへの接続を提供する RedBox に接続できます。RedBox の背後にあるノードは、DAN などの他のノードに表示されるため、「仮想 DAN (VDAN)」と呼ばれます。RedBox 自体は DAN であり、VDAN に代わってプロキシとして機能します。次の図は、PRP をサポートしていないが冗長性が必要な IED を PRP RedBox 機能をサポートするシスコの産業用イーサネットスイッチに接続すると、IED に冗長性と復元力が提供されることを示しています。

次の図は、各 IR8340 変電所ルータが PRP RedBox として機能し、それぞれの LAN に接続することを示しています。IR8340 はレイヤ 3 ゲートウェイとして機能し、HSRP または VRRP がゲートウェイの冗長プロトコルとして使用されます。コントロールセンターや WAN ネットワークと PRP LAN ネットワークに接続されたデバイスの間を流れる L3 トラフィックに冗長性と復元力を提供します。たとえば、MODBUS や DNP3 などの TCP トラフィックは、コントロールセンターの SCADA から PRP LAN ネットワークに接続された 1 つまたは多数の IED に流れるトラフィックである可能性があります。

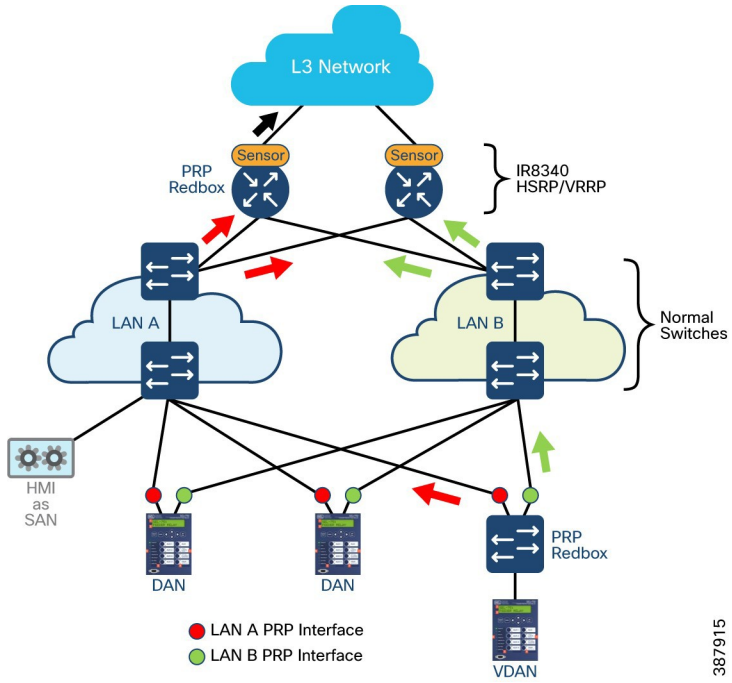
ネットワークの冗長性を最適化するには、Cisco レイヤ 3 HSRP とレイヤ 2 冗長サービスの両方を相互に調整するネットワークを設計する必要があります。HSRP は優先順位に基づいてアクティブルータとスタンバイルータを割り当てます。HSRP グループの中でアクティブ HSRP ルータが最も優先順位が高くなります。優先順位が同じ場合、最も大きい IP アドレスがタイブレーカになります。HSRP の優先順位を設定して、アクティブルータを手動で識別することを推奨します。インターフェイスに対してルーティングを最初にイネーブルにした時点で、完全なルーティング テーブルは存在しません。

このインターフェイスがプリエンプトに設定されている場合はアクティブ ルータになりますが、十分なルーティング処理はできません。この問題を解決するには、ルータがルーティング テーブルを更新できるように遅延時間を設定します。ローカル ルータのプライオリティがアクティブ ルータよりも高い場合、アクティブ ルータとして制御を行います。オプションで遅延値を設定できます。これにより、ローカルルータは、アクティブルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。HSRP は、次の 2 つのタイマーを使用します：hello interval と hold time。hello interval は、hello パケットが他方のピアに送信される頻度を定義します。hold time は、ピアをダウンとしてマーキングするまでの待機時間を示します。hold time は、hello interval の 3 倍以上である必要があります。

デバイスがオブジェクト トラッキング対応として設定されていて、なおかつトラッキング対象のオブジェクトがダウンした場合、デバイスのプライオリティはダイナミックに変更されます。トラッキング プロセスは定期的に、トラッキング対象オブジェクトをポーリングし、値の変更を確認します。トラッキング対象のオブジェクトの変化は、すぐに HSRP に伝えられるか、指定した遅延時間が経過してから HSRP に伝えられます。オブジェクトの値は、アップまたはダウンとして報告されます。トラッキング可能なオブジェクトには、インターフェイスのライン プロトコル ステートや IP ルートの到達可能性などがあります。指定したオブジェクトがダウンすると、HSRP プライオリティが引き下げられます。より優先順位の高い HSRP デバイスは、standby preempt コマンドが設定されている場合にはアクティブなデバイスになることができます。

REP リングの場合、両方のエッジポートをプライマリ HSRP ノードに配置する必要があります。STP の場合、ルートはプライマリ HSRP ノードに配置する必要があります。PRP の場合、優先順位、遅延、プリエンプションなどの前述した HSRP オプションを使用して、プライマリ HSRP ノードを手動で設定することを推奨します。また、高速ピア障害検出のために BFD を使用することも推奨します。

図 10　　Parallel Redundancy Protocol - L3 ゲートウェイの冗長性



変電所自動化の LAN ネットワークに適したその他の PRP トポロジ設計の詳細については、変電所自動化のローカルエリアネットワークとセキュリティについてのシスコ検証済みデザインガイドを参照してください。

このトポロジの主な特徴は次のとおりです。

- 2 つのパラレルネットワークによるロスレス冗長性。
- LAN A および LAN B のスイッチは、PRP プロトコルを認識する必要はなく、LAN 間にリンクや共有スイッチがない限り、スターやリングなどのトポロジをサポートできます。
- 独立した LAN A および LAN B ネットワーク インフラストラクチャとリンクの必要性による高コスト
- 標準規格 IEC 62439-3 Clause 4
- IE-4000、IE-4010、IE-5000、IE-9300、IR8340 および一部の IE-2000u SKU (8、16 ポート) でサポート
- 冗長ルータを介した WAN およびレイヤ 3 ネットワークへの復元力はあるがロスレスではない接続

- Cyber Vision Sensor、Stealthwatch、Digital Network Architecture Center などのアプリケーションはシームレスに動作します。これらのアプリケーションは、ステートフルなレイヤ 3 接続を使用します。たとえば、Cyber Vision セッションタイムアウトのキープアライブが秒単位で長いため、PRP を介した Cyber Vision Center と Sensor 間の到達可能性やステートフルセッションは影響を受けません。Stealthwatch と Digital Network Architecture Center でも同様の事実が確認されました。詳細については、グリッドセキュリティガイドおよびこのガイドの関連セクションを参照することを推奨します。

設計上の考慮事項

- 銅線リンクより高速なコンバージェンスを提供する光ファイバリンクを使用することをお勧めします。
- リンクの帯域幅は、遅延と、HSR および PRP ネットワークに含めることができるノードの数に影響を与えます。
- GOOSE とサンプル値は、出力インターフェイスのプライオリティ キューに分類されて送信されていました。
- マルチキャスト フラッディングを回避するために、各 IED に固有の VLAN を設定してください。
- アクセス/IED 側のインターフェイスでストーム制御を有効にしてください。

High-availability Seamless Redundancy (HSR)

HSR は、国際標準規格 IEC 62439-3-2016 第 5 条で定義されています。HSR は PRP のようなロスレスプロトコルですが、HSR はリングトポロジで動作するように設計されています。HSR は反対方向のトラフィックのあるリングを定義します。第 1 の HSR 対応ポートは、このリングでトラフィックを反時計回りに送信し、第 2 の HSR 対応ポートはトラフィックを時計回りに送信します。HSR のフレーム複製メカニズムは、リング内で 1 つの障害が発生した場合にロスレス冗長性を提供するのに役立ちます。HSR の概要を次の図に示します。

HSR フレーム形式では、送信される追加のプロトコル固有の情報がフレームヘッダー内に含まれます。ヘッダーには、受信したデータがフレームが初めて到着したものか重複して到着したものかを判断するために使用されるシーケンス番号が含まれています。

HSR リングに接続されて、HSR プロトコルをサポートする 2 つのインターフェイスを持つ IED は、「HSR 実装ダブル通信ノード (DANH)」と呼ばれます。SAN は、RedBox を介して HSR リングに接続する必要があります。単一接続の IED は、RedBox に接続されると、仮想デュアル通信ノード (VDAN) と呼ばれるものになります。

HSR RedBox は、RedBox が送信元または接続先となるすべてのトラフィックに対して DANH として機能します。Cisco IE スイッチは HSR RedBox の機能を搭載し、ギガビット イーサネット ポートを使用して HSR リングに接続します。

Cisco IE 4000、Cisco IE 4010、Cisco IE 5000 スイッチ、Cisco IE9300 スイッチ、および Cisco IR8340 変電所自動化ルータが、HSR の復元力を備えています。

設計上の考慮事項

HSR の設計上の考慮事項は、HSR リングとデバイスを他の変電所ネットワークや WAN に相互接続する 3 つのトポロジに分けられます。HSR リングを相互接続する 3 つの方法は次のとおりです。

- 有効な IP トラフィックをルーティングするデュアルレイヤ 3 スイッチ/ルータを介して相互接続
- HSR QuadBox を形成するデュアルスイッチを介して 2 つの HSR リングを相互接続
- HSR リングを 2 つの PRP 冗長 LAN に相互接続

レイヤ 3 ゲートウェイの冗長性を備えた HSR

HSR は HSR-SAN モードで使用され、IED が接続されているアクセスレイヤで冗長性を提供します。HSR リングは、本質的に HSR をサポートする IED で構成することもできます。このようなノードは、デュアル通信ノードと呼ばれます。アクセス

レイヤは Cisco IR8340 Substation ルータによって集約され、レイヤ 2/レイヤ 3 境界とレイヤ 2 ドメインのデフォルトゲートウェイも提供します。ディストリビューション レイヤでは、Hot Standby Router Protocol (HSRP) または Virtual Router Redundancy Protocol を使用して、IP ルーティングにステートレスな冗長性を提供します。次の図は、HSR リングのトポロジを示しています。2 つの IR8340 ルータの一部であり、レイヤ 2/レイヤ 3 の復元力と冗長性を提供します。

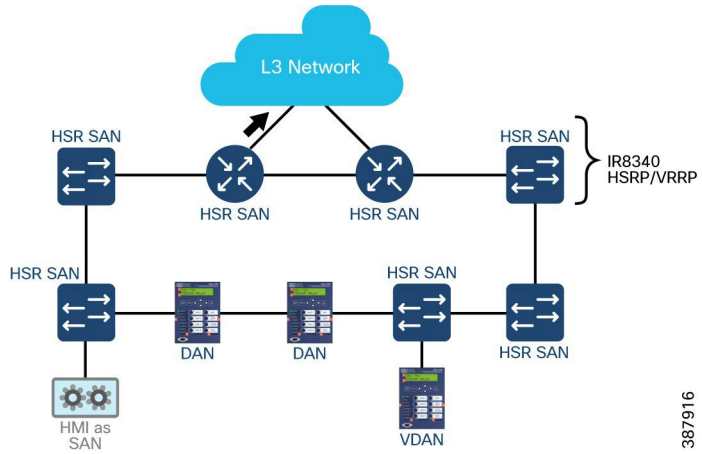
ネットワークの冗長性を最適化するには、Cisco レイヤ 3 HSRP とレイヤ 2 冗長サービスの両方を相互に調整するネットワークを設計する必要があります。HSRP は優先順位に基づいてアクティブルータとスタンバイルータを割り当てます。HSRP グループの中でアクティブ HSRP ルータが最も優先順位が高くなります。優先順位が同じ場合、最も大きい IP アドレスがタイブレーカになります。HSRP の優先順位を設定して、アクティブルータを手動で識別することを推奨します。インターフェイスに対してルーティングを最初にイネーブルにした時点で、完全なルーティング テーブルは存在しません。このインターフェイスがプリエンプトに設定されている場合はアクティブ ルータになりますが、十分なルーティング処理はできません。この問題を解決するには、ルータがルーティング テーブルを更新できるように遅延時間を設定します。ローカル ルータのプライオリティがアクティブ ルータよりも高い場合、アクティブ ルータとして制御を行います。オプションで遅延値を設定できます。これにより、ローカルルータは、アクティブルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。

HSRP は、次の 2 つのタイマーを使用します：hello interval と hold time。hello interval は、hello パケットが他方のピアに送信される頻度を定義します。hold time は、ピアをダウンとしてマーキングするまでの待機時間を示します。hold time は、hello interval の 3 倍以上である必要があります。

デバイスがオブジェクト トラッキング対応として設定されていて、なおかつトラッキング対象のオブジェクトがダウンした場合、デバイスのプライオリティはダイナミックに変更されます。トラッキング プロセスは定期的に、トラッキング対象オブジェクトをポーリングし、値の変更を確認します。トラッキング対象のオブジェクトの変化は、すぐに HSRP に伝えられるか、指定した遅延時間が経過してから HSRP に伝えられます。オブジェクトの値は、アップまたはダウンとして報告されます。トラッキング可能なオブジェクトには、インターフェイスのライン プロトコル ステートや IP ルートの到達可能性などがあります。指定したオブジェクトがダウンすると、HSRP プライオリティが引き下げられます。より優先順位の高い HSRP デバイスは、standby preempt コマンドが設定されている場合にはアクティブなデバイスになることができます。

REP リングの場合、両方のエッジポートをプライマリ HSRP ノードに配置する必要があります。STP の場合、ルートはプライマリ HSRP ノードに配置する必要があります。PRP の場合、優先順位、遅延、プリエンプションなどの前述した HSRP オプションを使用して、プライマリ HSRP ノードを手動で設定することを推奨します。また、高速ピア障害検出のために BFD を使用することも推奨します。

図 11　　High-Availability Seamless Redundancy Protocol - L3 ゲートウェイの冗長性



次に、Cisco IR8340 の HSR の特徴を紹介します。その他のプラットフォームの詳細については、それぞれのプラットフォームガイドを参照してください。変電所自動化の LAN ネットワークに適したその他の HSR トポロジ設計の詳細については、変電所自動化のローカルエリアネットワークとセキュリティについてのシスコ検証済みデザインガイドを参照してください。

このトポロジの主な特徴は次のとおりです。

- Cisco IE 4000、Cisco IE 4010、Cisco IE 5000、および Cisco IR8340 変電所ルータで HSR がサポートされています。
- HSR リングポートは、レイヤ 2 モードでのみ設定できます。
- サポートされる MTU サイズは、最大 1998 バイトです。
- ノードテーブル内のノードの最大数は 512 です。ノードは、同時にリングに接続できるすべての DANH および VDAN デバイスに他なりません。
- リング内のノードの最大数は 50 に制限されています。
- ボックスごとに最大 1 つのリングがサポートされます。HSR と PRP を同じ IR8340 ルータで同時に有効にすることはできません。
- 次のプロトコルと機能は、同じポート上の HSR と相互に排他的です。
  - PRP
  - EtherChannel
  - リンク集約制御プロトコル（LACP）
  - ポート集約プロトコル（PAgP）
  - Resilient Ethernet Protocol（REP）
  - スパニングツリープロトコル
  - PTP
- ポートがリングの一部になると、ポートのメディアタイプ、速度、およびデュプレックス設定を変更することはできません。リングのメンバーシップを構成する前に、これらの設定を適用することを推奨します。
- ポートがリングの一部になると、そのポートをシャットダウンすることはできません。代わりに、必要に応じて HSR リングインターフェイスをシャットダウンできます。ただし、この操作により両方のメンバーポートがシャットダウンされます。
- トランクモードやアクセスモードなどの VLAN 設定は、リングに参加している両方のポートで同じである必要があります。
- インターフェイスが HSR リングに追加されると、プライマリ インターフェイス カウンタのみが更新されます。個々の物理インターフェイスが HSR リングに追加された後、ステータスをチェックしないでください。
- すべてのスイッチでリングを設定する前にポートをシャットダウンしてから、MAC フラップを回避するためにポートを 1 つずつ再度有効にすることを推奨します。
- 物理インターフェイスは、HSR-SAN および HSR-PRP モードのリングとポートに事前定義されており、変更できません。Cisco IR8340 HSR-SAN モードのポート割り当てを次の表に示します。その他のデバイスやモードについては、該当する製品マニュアルを参照してください。

表 5　IR8340 および HSR-SAN ポート

SKU	HSR モード	ポート タイプ	インターフェイス番号
Cisco IR8340	HSR-SAN	リング 1、ポート 1	GE 0/1/4
		リング 1、ポート 2	GE 0/1/5
		リング 2、ポート A	GE 0/1/6
		リング 2、ポート B	GE 0/1/7

HSR-HSR

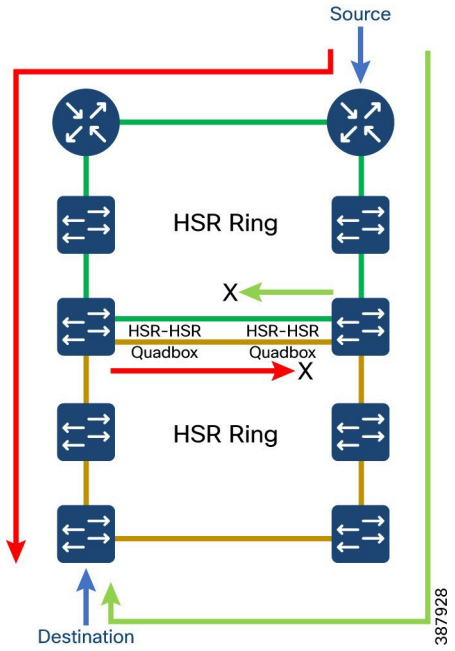
HSR リングも、キースイッチが 2 つの HSR リングに参加しているのと同様の方法で実装できます。これには、HSR-HSR または Quadbox と呼ばれるそれぞれのリングを接続するための 4 つのインターフェイスを使用します。HSR-HSR モードがライセンスされ、有効になっている場合、スイッチはトラフィックの干渉を回避するために、すべての非 HSR ポートを閉鎖します。HSR-HSR スイッチへの接続は、HSR-HSR ポートまたはアウトオブバンド コンソール インターフェイスを介して行うことができます。

HSR-HSR QuadBox 機能は IE4000 でのみサポートされています。各 QuadBox は重複フレームを作成します。トポロジ内に複数の QuadBox があると、同じフレームの複数コピーが生成される可能性があります。ただし、リングの各側には 1 つのコピーだけが送信されるため、最終的には各リングにフレームの 2 つのコピーだけが送信されます。受信した後続のすべての重複フレームは、QuadBox によって破棄されます。

2 つのリング間のトラフィックを分離するには、VLAN およびマルチキャストフィルタを使用して QuadBox を構成できます。これにより、特定の VLAN およびマルチキャストグループがリングを越えないように制限できます。VLAN フィルタリングでは、VLAN 許可リストを使用して VLAN を制限します。マルチキャストフィルタリングでは、フィルタで設定した MAC 宛先アドレス (MACDA) およびオプションのマスクフィルタがパケットと照合されます。一致する場合、そのパケットは破棄されます。IEC 61850 変電所ネットワークでは、HSR は通常、小規模な変電所またはプロセスバス通信に使用されます。

HSR-HSR QuadBox のシナリオ例は、HSR を備えたステーションバスリングとサブリングです。以下は、HSR-HSR QuadBox を使用した単純なトポロジです。

図 12　　HSR - HSR リング



注: HSR QuadBox を介した PTP はサポートされていません。

HSR-PRP Redbox

HSR-PRP（「デュアル RedBox」とも呼ばれる）は、PRP ネットワークと HSR ネットワークを一緒に接続するために使用されます。これは一般に変電所に導入されます。そのため、テスト結果には GOOSE と サンプル値が示されていますが、他の IP プロトコルにも適用できます。次のトポロジは、2 つの RedBox（各 LAN に 1 つずつ）を介して PRP ネットワークに接続される HSR リングを示しています。この例では、IP フレームは PRP ネットワークで発生し、GOOSE フレームとサンプ

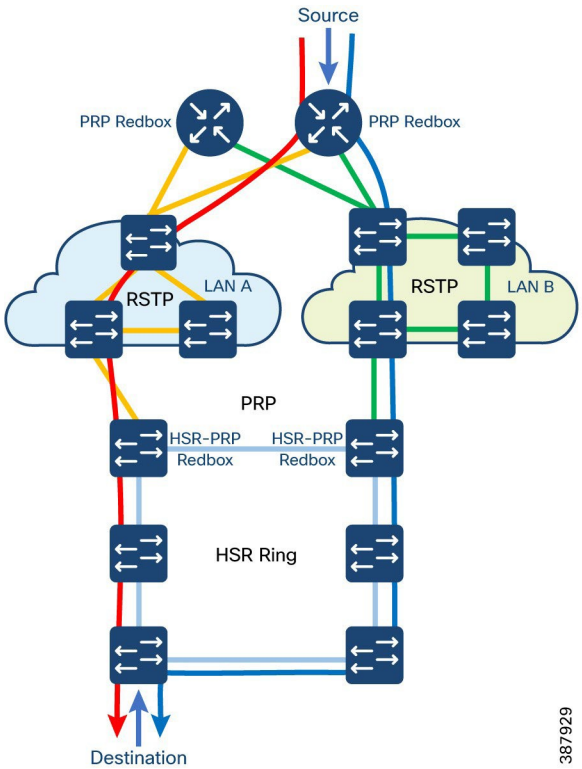
ル値フレームは HSR リングで発生して終了します。このトポロジでの中断は、対応するトラフィックでダウンタイムを発生させず、異なるトラフィックストリームの遅延は期待される要件を確実に満たします。

HSR-PRP RedBox のシナリオ例は、ステーションバスが PRP で、プロセスバスが HSR の場合です。以下は、HSR-PRP QuadBox を使用した単純なトポロジです。

設計上の考慮事項

- HSR-PRP デュアル RedBox モード (IE 4000 のみ) では、デバイスは基本的に 3 ポートデバイスとして機能します。これら 3 つのインターフェイスを除く他のすべてのインターフェイスは、ソフトウェアによってシャットダウンされます。これらの 3 つのインターフェイスは事前定義されています。
  - RedBox A の Gi1/1、Gi1/3、Gi1/4
  - RedBox B の Gi1/2、Gi1/3、Gi1/4
- PathId で識別される最大 6 つの PRP ネットワークを同じ HSR リングに接続できます。
- PRP ネットワークは任意の数の HSR リングに接続できますが、ループが発生するため、これらのリングを相互に接続することはできません。
- HSR-PRP デュアル RedBox モードでは、トラフィックが進行中の HSR-PRP スイッチのリロード中に、リロードされたスイッチとトラフィックを送信している PRP デバイスの送信元 MAC アドレスごとに 1 回、MAC フラップが発生します。したがって、512 個の異なる送信元 MAC アドレスがある場合、MAC フラップは 512 回 (送信元 MAC アドレスごとに 1 回) 観察されます。また、このイベントの後、いくつかの重複パケットが見られます。

図 13　　HSR - ステーションバスおよびプロセスバス用の PRP RedBox



復元力の概要

「最良の」ネットワークトポロジや「最良の」冗長プロトコルはありません。それらすべてに長所と短所があり、特定のアプリケーションでの正しい選択は、多くの要因によって異なります。IEC61850 ベースの変電所自動化ネットワーク用に設計できるネットワークトポロジは数多くあります。次の表は、このガイドで説明されているさまざまなプロトコルの比較を示しています。

表 6　　レジリエンスプロトコルとプロパティ

プロトコル	トポロジ	ノード数	一般的なコンバージェンス
RSTP/MSTP	いずれか	最大ホップ 255	50 ミリ秒 ~ 6 秒
HSR	リング	50	0 ミリ秒
PRP	デュアル独立ネットワーク	無制限	0 ミリ秒
REP (Cisco Proprietary)	リング	24	50 ~ 250 ミリ秒

次の表は、さまざまなトラフィックフローとその復元力の要件、および使用できる適切なレジリエンスプロトコルの一覧です。

表 7　　変電所自動化 LAN トラフィックと復元力の要件

通信形態	サービス	アプリケーション回復の遅延時間	通信回復の遅延時間	注記
SCADA から IED クライアントサーバ	IEC 61850-8-1	800 ミリ秒	400 ミリ秒	REP で対応可能
IED から IED 連携	IEC 61850-8-1	12 ミリ秒	4 ミリ秒	PRP および/または HSR が必要
IED から IED、リバースブロッキング	IEC 61850-8-1	12 ミリ秒	4 ミリ秒	PRP および/または HSR が必要
バスバー保護を除く保護トリップ	IEC 61850-8-1	8 ミリ秒	4 ミリ秒	PRP および/または HSR が必要
バスバー保護	ステーションバスの IEC 61850-9-2	1 ミリ秒未満	バンプレス - 0 ミリ秒	PRP および/または HSR が必要
サンプル値	プロセスバスの IEC 61850-9-2	4 ミリ秒未満	バンプレス - 0 ミリ秒	PRP および/または HSR が必要

各種プラットフォームと復元力の機能

次の表では、シスコの産業用イーサネットスイッチおよび産業用ルータでサポートされているロスレス レジリエンス プロトコルの一部と、それらのさまざまな役割を示します。

表 8　　レジリエンスプロトコル - HSR と役割

HSR の役割	IR と ER
HSR SAN + PTP GM	IE5000
HSR SAN+ トランスペアレントクロックを使用したステー	IE3400 、IE4000、IE5000

ションバスリング	
HSR SAN+ 境界クロックを使用したステーションバスリング	IE4010、IE3400、IE4000
HSR PRP RedBox	IE4000
HSR QuadBox	IE4000
HSR SAN	IE5000、IE4000、IE4010、IE3400、IR8340

表 9　レジリエンスプロトコル - PRP と役割

PRP の役割	IR と IE
PRP RedBox + PTP GM	IE5000
ステーションバス LAN スイッチ非 PRP + トランスペアレントクロック	IE9300、IE3400、IE4000、IE4010、IE2000U
プロセス LAN スイッチ非 PRP + トランスペアレントクロック	IE9300、IE3400、IE4000、IE4010、IE5000
PRP RedBox + HSRP/VRRP	IR8340
PRP HSR RedBox	IE4000

タイミングおよび同期

変電所の自動化はミッションクリティカルなタスクであり、電力事業者は変電所内の大規模な分散型電力グリッドスイッチ間で同期を図ってスムーズな電力伝送を可能にし、電源の完全性を維持する必要があります。

時刻同期は、IED、統合ユニット (MU)、保護ユニット、制御ユニット、イーサネットスイッチなど、変電所の自動化でプロセスを同期する必要がある場所で、内部クロックを正確に同期するために使用されます。これは、ネットワーク応答の正確な制御とグローバル分析、および障害が発生した時間、場所、理由の特定に役立ちます。

変電所ネットワークのイーサネットネットワークを介した時刻同期に関連する標準プロトコルは 、Network Time Protocol (NTP) と Precise Time Protocol (PTP) の 2 つです。NTP は、一般的な TCP/IP ネットワークのクロックを同期するプロトコルです。サーバー、ワークステーション、スマートフォン、およびネットワーク インフラストラクチャは、通常、NTP をサポートしています。ただし、NTP は秒単位の同期しかサポートできません。PTP は、デバイス間のタイムドリフトがナノ秒単位で測定され、クロックのネットワーク間で非常に高い精度を提供するように設計されたプロトコルです。変電所デバイスがシステム制御やデータ収集などのために高精度クロックを備えるためには、正確な時刻同期が必要です。時刻同期は、電流のサンプル値 (IEC61850-9-2) のタイムスタンプにとって特に重要であり、電圧値には統合ユニット内部の正確なクロックが必要です。

ローカルエリアネットワークを介した時刻同期によりデバイスが同期され、1 つのイーサネットネットワークを介して駆動するデバイスの数を増やすことができます。同じイーサネット通信媒体を介してデータ通信を行うとともに、すべての時刻同期情報を転送することで、ケーブル配線インフラストラクチャとコストが削減されます。

NTP などの標準プロトコルは、ステーションバスに接続された IED と、プロセスバス環境における IEC 61850 GOOSE および SV アプリケーションの IEEE 1588 C37.238 PTP 電力プロファイルの同期に使用できます。シスコの産業用プラットフォームは、NTP と C37.238 PTP 電力プロファイルの両方を同時にサポートします。使用されているレジリエンスプロトコルやアプリケーション要件に応じて、適切なタイミングプロトコルを選択する必要があります。また、複数の場所や地域間で時刻を比較する必要があるため、世界時計である協定世界時 (UTC) に時刻の同期を合わせられることが重要です。

ネットワーク タイム プロトコル

ネットワーク タイム プロトコルは、TCP/IP ネットワーク間でクロックを同期するためのネットワークプロトコルです。NTP は、クロックの階層型システムを使用して、ネットワーク上の異なるホスト間で時刻を同期します。NTP アーキテクチャのクロックには次の 3 つの役割があります。

- サーバー: NTP サーバーは、1 つ以上の NTP クライアントの時刻源として機能します。
- クライアント: NTP クライアントは、クロックを 1 つまたは複数のサーバーと同期させます。
- ピア: NTP ピアにより、2 つのクロックを相互に同期させることができます。本質的に、ピアは相互にクライアントとサーバーになります。

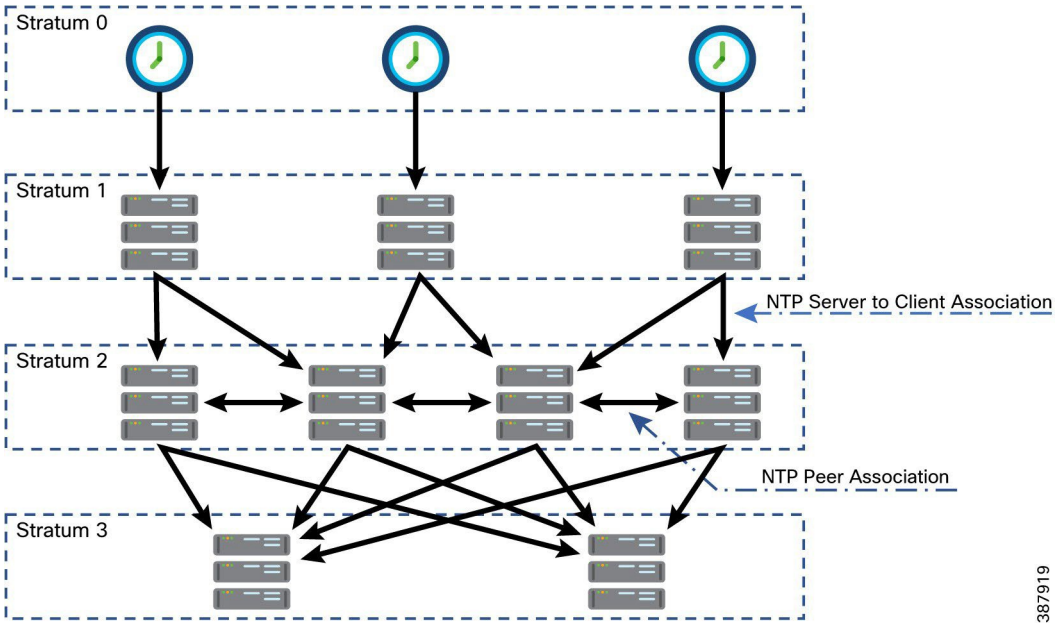
これらの役割は排他的ではなく、変電所自動化アーキテクチャのデバイスはこれらの役割の 1 つ以上を果たします。たとえば、NTP サーバーは通常、NTP 階層の上位のサーバーに対するクライアントです。多くの場合、ネットワーク インフラストラクチャは、アップリンクのクライアントであり、ダウンリンクのサーバーです。

NTP には、タイムサーバーを認証するための限定的な規定があります。ほとんどの導入では、対称キーを使用して認証を行うことができます。また、最近では、Autokey セキュリティプロトコルを使用した導入も一部でサポートされています。NTP 認証については、このガイドの範囲外です。

次の図に示すように、クロック階層は、下位のストラタム番号が基準クロックに近い「ストラタム」に分割されます。基準クロックは、ストラタム 0 クロックとして識別されます。GPS などの GNSS の受信機である場合が多いですが、無線受信機、原子時計、または別の高精度時刻源の場合もあります。

ストラタム 0 クロックは、ストラタム 1 サーバーに直接接続されており、ネットワーク経由で直接アクセスすることはできません。ストラタム 2 サーバーは、NTP プロトコルを使用してネットワーク全体で最初に同期します。ストラタム 2 サーバーは、いくつかのストラタム 1 サーバーのクライアントであり、他のストラタム 2 サーバーのピアであることがよくあります。ストラタム 3 サーバーは、ストラタム 2 サーバーのクライアントであり、他のストラタム 3 サーバーなどのピアである場合があります。

図 14　　NTP クロック階層



クライアント (IED デバイスなど) がクロックを基準クロックと同期させる機能は、そのストラタムレベルに依存します。ストラタム番号が小さいほど、基準クロックとより密接に同期されます。NTP クロックは、UTC と比較して精度が制限されます。これらは一般に、数百ミリ秒または数秒の UTC へのオフセットを許容できる変電所アプリケーションに適しています。

ただし、クライアントが基準クロックと同期する際の精度に影響を与える要因がいくつかあります。

- ネットワークの遅延とジッター
- 非対称ネットワーク
- クロック間のホップ数
- 内部発振器の品質
- オペレーティングシステムの機能

NTP クロックアルゴリズムは、複数のサーバーとの関連付けをサポートしています。複数の入力値を使用して、ローカルクロックの時刻同期の精度を上げます。クロックアルゴリズムは、関連するサーバーの健全性もチェックします。プールと矛盾するサーバーからのクロック更新は無効化され、破棄されます。健全性チェックにより、NTP クライアントで不正なクロックソースでスキューイングが生じるリスクが軽減されます。

電力会社のオペレーションセンターに 2 ~ 4 台の NTP サーバーを展開して、エンタープライズ アプリケーションの中央クロックとして機能させます。アプリケーションの要件に応じて、これらの NTP サーバーは、基準クロックに直接接続するか、インターネット上のパブリックサーバーと同期させることができます。パブリックソースと同期させることを決定した場合、これらの各サーバーは 2 ~ 4 つのパブリックソースと同期させる必要があります。不正なクロックを特定してクロックプールから削除できるように、パブリックソースにはある程度の多様性が必要です。さらに、エンタープライズ ゾーン サーバーは相互にピアである必要があります。大規模な組織では、NTP クライアントに時刻をカスケードするために、組織内に NTP サーバーの追加のストラタムがある可能性があります。ESP ゾーンで高精度の NTP 時間が必要な場合は、変電所自動化 LAN ESP ゾーン内にストラタム 1 サーバーを展開することを検討してください。

パブリック NTP サーバーへのアクセスは、エンタープライズ エッジ ファイアウォールで制御する必要があります。組織内のすべての NTP クライアントを内部 NTP サーバーに同期させることが目的です。したがって、パブリックサーバーへのアクセスは、内部の最上位の NTP サーバーに制限する必要があります。さらに、アクセスは、組織によって信頼されている特定のパブリックサーバーに制限する必要があります。理想的には、外部 NTP サーバーによる認証を使用して、時刻同期が侵害されるリスクを軽減します。

NTP を使用して、DMZ および変電所自動化 LAN ゾーンに展開されたスイッチ、ルータ、ファイアウォール、およびその他のネットワーク インフラストラクチャのクロックを同期します。これらのネットワークデバイスの時刻を同期することは重要です。これにより、複数のネットワークデバイスの syslog を一緒に分析して、システムレベルの障害のトラブルシューティングに役立てることができます。

詳細については、https://www.cisco.com/c/en/us/support/docs/availability/high-availability/19643-ntpm.html [英語] を参照してください。

Precision Time Protocol と電力プロファイル

Precision Time Protocol（PTP）は、IEEE 1588 で、ネットワーク化された測定および制御システムの高精度クロック同期として定義されており、さまざまな精度と安定性の分散デバイスクロックを含むパケットベース ネットワークでクロックを同期させるために開発されました。PTPは、産業用のネットワーク化された測定および制御システム向けに特別に設計されており、最小限の帯域幅とわずかな処理オーバーヘッドしか必要としないため、分散システムでの使用に最適です。

ピーク時課金、仮想発電機、停電の監視/管理などのスマート グリッド電力自動化アプリケーションは、非常に正確な時刻精度と安定性を必要とします。タイミングの精度は、ネットワーク監視の精度とトラブルシューティング能力を向上させます。

時刻精度および同期の提供に加えて、PTP メッセージベース プロトコルは、イーサネット ネットワークなどのパケットベース ネットワークに実装することもできます。イーサネット ネットワークで PTP を使用する利点は次のとおりです。

- 高価な独自のタイミングネットワーク (IRIG など) の代わりに既存のイーサネットネットワークを使用することで、コストを抑えて簡単にセットアップできます。
- PTP データパケットは限られた帯域幅しか必要としない

シスコの産業用イーサネットスイッチおよびルータでは、さまざまな PTP プロファイルがサポートされます。サポートされるプロファイルは次のとおりです。

- デフォルト プロファイル
- 電力プロファイル（C37.238-2011/IEC 61850-9-3 サポート）
- 802.1AS プロファイル
- 拡張電力プロファイル（IEEE C37.238-2017 のサポート：透過クロックモードのみ）

一部のプロファイルは、一部のプラットフォームでサポートされていない場合があります。それぞれのプラットフォームガイドでサポート内容を確認することを推奨します。

電力プロファイルは C37.238-2011 : 電力システムアプリケーションでの IEEE 1588 Precision Time Protocol の使用に関する IEEE ドラフト標準規格プロファイルで定義されています。このマニュアルでは、この IEEE 1588 プロファイルおよび関連設定値を参照する際に、電力プロファイルモードとデフォルト プロファイル モードという用語を使用します。

IEEE 電力プロファイルは、変電所で使用される PTP ネットワークの特定の値または許容値を定義します。定義される値には、最適な物理層、PTP メッセージ用のより高位のプロトコル、および優先されるベスト マスター クロック アルゴリズムが含まれます。電力プロファイルの値は、変電所内、変電所間、および広い地理的領域にわたる一貫した信頼性のあるネットワーク時刻配信を保証します。

拡張電力プロファイルは、透過クロックモードで C37.238-2017 をサポートしています。

拡張電力プロファイルには、電力プロファイル（C37.238-2011）と比較して次の特徴があります。

- このプロファイルは、デフォルトでドメイン番号 254 を使用します。
- 透過クロックモード動作では、「TotalTimeInAccuracy」が各ノードで約 50ns ずつ増加します。

ロール

PTP 同期動作は、デバイスで設定する PTP クロックモードによって異なります。シスコの産業用イーサネットルータおよびスイッチは、次のいずれかのグローバルモードに設定できます。それぞれのプラットフォームガイドでサポート内容を確認することを推奨します。

対象となる主な役割は次のとおりです。

- グランドマスター: 主要な時刻源
- 境界クロック: 時刻を配信するための中継マスタークロック
- トランスペアレントクロック: PTP トラフィックで中継機の遅延を補正した時刻を配信するための中継クロック

グランドマスター

グランドマスタークロックは、PTP ドメイン内の時刻のプライマリソースです。グランドマスタークロックは高品質の発振器を備え、UTC と同期している必要があります。PTP ドメインのグランドマスターは、Best-Master Clock Algorithm (BCMA)

と呼ばれるプロトコルを使用して選択されます。グランドマスターが選択されると、時刻の中心的なプロバイダとなり、スレーブクロックのさまざまな要求に応答します。

境界クロック

境界クロックは、1 つのポートでスレーブになるマルチポートデバイスの産業用イーサネットスイッチです。境界クロックはスレーブクロックとして、内部クロックをマスターに同期します。その後、境界クロックは、産業用イーサネットスイッチの他のポートに接続されている IED デバイスのマスターになります。これらのポートに接続されている他のクロックは、境界クロックに対するスレーブになり、境界クロックの内部クロックと同期します。

産業用イーサネットスイッチの境界クロックモードには 3 つの異なる転送機能があり、次の表に示すように、パケット遅延変動 (PDV) に対して境界クロックが調整される方法を変更します。PDV は、ネットワークフロー内のパケットの一方向エンドツーエンド遅延の差を測定したものであり、一般的にネットワーク「ジッター」と呼ばれているものをより正確に説明します。

表10　PTP 境界クロックと転送機能

転送機能	PDV フィルタリング	コンバージェンス時間
デフォルト（線形）	低い	平均
フィードフォワード	なし	速い
適応型	高	低速

フィードフォワード転送機能は、非常に正確な時刻同期を必要とするアプリケーションで使用できます。フィードフォワード転送では、PDV がフィルタ処理されないため、IES がハードウェアで PTP をサポートしているネットワークでのみ実装する必要があります。

適応型フィルタは、802.11 ワイヤレス LAN などの高い PDV のアプリケーションで使用できます。また、ネットワークが非 PTP 認識スイッチと高い PDV で構成されているアプリケーションでも使用できます。

大規模な PTP ネットワークでは、境界クロックを検討する価値があります。境界クロックがグランドマスターの中継装置として機能する場合に、グランドマスターが多数のデバイスに直接応答する必要性が減ります。

トランスペアレント クロック

トランスペアレントクロックは、遅延補正を PTP パケットに挿入することによって、ネットワーク全体の遅延を補正します。IEEE 1588 仕様では、次の 2 種類のトランスペアレントクロックが定義されています。

エンドツーエンド (E2E) のトランスペアレントクロックは、ネットワーク内の IED とネットワークデバイスが PTP パケットを処理して転送するまでの時間を測定することによって、ネットワーク全体の遅延を補正します。これらの測定値は、PTP パケットの修正フィールドに追加されます。

ピアツーピア (P2P) のトランスペアレントクロックは、ネットワーク内のすべてのデバイスが PTP に対応していることを前提としているため、ピアへの遅延のみを測定します。ピアツーピアメカニズムは、エンドツーエンドのトランスペアレントクロックと互換性がありません

トランスペアレントクロック (ピアツーピアかエンドツーエンドかに関係なく) は、PTP 階層内のノードにはなりません。したがって、マスタークロックもスレーブクロックにもなりません。トランスペアレントクロックは、マスタークロックとスレーブクロックの間でインラインに配置され、これらのデバイス間で時刻を補正します。

トランスペアレントクロックと境界クロックは、ネットワークトポロジ内で共存できます。トランスペアレントクロックは、リングトポロジなど、ノード/スイッチがマスタークロック (GM または BC) からメッセージを受信する方向をトポロジが変更する可能性があるネットワークで役立ちます。トランスペアレントクロックには、エンドデバイスからの要求を処理するアップストリーム マスター クロックを解放してもメリットはありません。**注:** 電力プロファイル 2017 の時点で、ピアツーピアのトランスペアレントクロックが必須です。

次の表では、さまざまなシスコの産業用イーサネットプラットフォームと、それぞれのプラットフォームでサポートされるロールとプロファイルを示します。最新のプラットフォームガイドもあわせて確認することを推奨します。

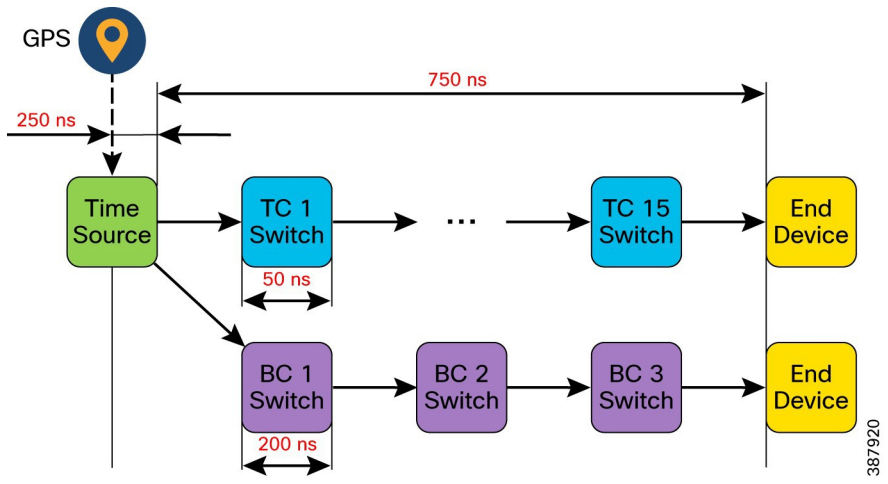
表 11　シスコの産業用イーサネット製品における PTP ロールとプロファイル

PTP ロール	プラットフォーム	サポートされるプロファイル
グランドマスター	IE5000	PTP 電力プロファイル 2011
E2E と P2P の両方の PTP トランスペアレントクロック	IE9300、IE4000、IE4010、IE3400、IE5000、IE2000U	PTP 電力プロファイル 2011 PTP 電力プロファイル 2017
PTP 境界クロック	IE9300、IE4000、IE4010、IE3400、IE5000、IE2000U	PTP 電力プロファイル 2011
PTP Over PRP RedBox	IE5000、IE4000、IE4010、IE3400	
HSR を介した PTP	IE5000、IE4000、IE4010、IE3400	

設計上の考慮事項

ネットワークを構築する際の最初のステップは、基準クロックを見つけて、クロックの不正確さを最小限に抑えることです。トランスペアレントクロックはそれぞれ、時刻の不正確さをもたらします。グランドマスターから IED へのパスでは、同期メッセージが送信される際に通過するさまざまなトランスペアレントクロックの時刻の不正確さが、各トランスペアレントクロックの値によって増加します。シスコの産業用イーサネットデバイスで有効になっている各トランスペアレントクロックは、最大 50 ナノ秒の滞留時間遅延をもたらします。変電所自動化 LAN アプリケーションでは、PTP グランドマスターから IED まで、エンドツーエンドで 1000 ナノ秒の遅延時間が必要です。シスコの産業用デバイスで有効になっている境界クロックは、250 ナノ秒の滞留時間遅延を引き起こし、GPS に接続されたグランドマスターは最大 250 ナノ秒の滞留時間遅延を引き起こします。同じことが次の図で示されています。電力プロファイルモードが有効になっている場合、シスコの産業用イーサーネットスイッチやルータは、Organization_extension と Alternate_timescale の 2 つのタイプ、長さ、値 (TLV) メッセージ拡張子を含まない PTP アナウンスメッセージをドロップします。グランドマスタークロックが PTP に準拠しておらず、これらの TLV なしでアナウンスメッセージを送信する場合は、「ptpallow-without-tlv」コマンドを入力して、アナウンスメッセージを処理するようにデバイスを設定します。

図 15　PTP クロックとエンドツーエンドの遅延



プロセスバスにはより厳しいタイミング要件が適用されるため、PTP グランドマスターや NTP マスターなどの基準クロックをステーションバスに配置し、プロセスバスデバイスをそれと同期させる必要があります。ステーションバスとプロセスバス

を接続するデバイス (イーサネットスイッチまたはブリッジ機能を備えた IED) は、プロセスバスデバイスを同期する PTP トランスペアレントクロックとして機能します。ただし、ステーションバスの基準クロックが使用できなくなった場合、プロセスバス上のデバイス、できればステーションバスとプロセスバスを接続するデバイスが、ステーションバス (まだ動作している場合) とプロセスバスの両方に対して、グランドマスターの役割を引き継ぐ必要があります。ステーションバスが動作を再開すると、接続デバイスはそのマスターの役割を基準クロックに譲ります。可能であれば、障害モード全般が回避されるように冗長クロックを配置し、最悪の場合にオーディナリクロックへのパス内のトランスペアレントクロック数が、オーディナリ グランドマスター クロック数以下になるようにすることを推奨します。

プロセスレベルでのクロック同期は、考慮するアプリケーションやネットワーク アーキテクチャ、およびトポロジによって異なります。過電流などのローカル保護機能の場合、関連するデータは通常、同じ統合ユニットによって収集されるため、外部同期は必要ありません。データが複数の統合ユニットから送られている場合 (差動保護機能など)、統合ユニットを同期する必要があります。特定の機能を実行するために必要な統合ユニットの数は、損失が発生した場合に求められる可用性だけでなく、変電所の地理的な距離やレイアウトによっても異なります。同期する統合ユニットの数は、ベイを使用するなどして最小限に抑える必要があります。ベイは、複数のポイントツーポイントリンクだけでなく、複数のリングまたは複数のスターを基盤としている場合もあります。

時刻源

GMC-BC モードでは、産業用イーサネットスイッチ (IE5000 など) や産業用ルータ (IR8340 など) が変電所のグランドマスターとして機能できます。GMC-BC モードでは、グランドマスターを UTC と同期する 2 つのオプションがあります。NTP から PTP への変換と GNSS レシーバです。Cisco IR8340 および Cisco IE5000 産業用イーサネットスイッチは、NTP から PTP への変換機能をサポートしています。Cisco ルータ IR8340 および Cisco IE 5000 産業用イーサネットスイッチも GNSS レシーバをサポートしています。

IR8340 タイミングモジュールは、IRIG-B (入力/出力)、GNSS、TOD/1PPS、IEEE 1588 v2 (PTP)、SyncE をサポートしています。GNSS は Stratum 3 NTP 再配信をサポートしています。Cisco IE5000 は IRIG-B 入出力インターフェイス (B002、B003、B006、B007、B122、B123、B126、B127 タイムコード)、GNSS/GPS をサポートしています。

GNSS レシーバにより、デバイスはいくつかの異なる衛星コンステレーションの 1 つと同期できます。

- GPS/NAVSTAR: グローバル ポジショニング システム
- GLONASS: Global'naya Navigatsionnaya Sputnikovaya Sistema
- BeiDou: BeiDou Navigation Satellite System

NTP から PTP への変換機能により、産業用イーサネットデバイスは NTP サーバーを PTP ドメインの基準クロックとして使用できます。このモードでは、産業用イーサネットスイッチはクロックを 1 つ以上の NTP サーバーと同期します。スイッチが UTC とどの程度の間隔で同期するかは、NTP 実装の品質によって決まります。

GMの冗長性

グランドマスタークロックは、PTP ドメイン内の時刻のプライマリソースです。このソリューションガイドでは、少なくとも 2 つの PTP グランドマスタークロックを変電所自動化 LAN ネットワークで使用することを推奨しています。ベスト マスター クロック アルゴリズム（BMCA）は PTP 機能の基盤です。BMCA は、ネットワーク上の各クロックが、そのサブドメイン内で認識できるすべてのクロック（そのクロック自体を含む）のうちのベスト マスター クロックを決定する方法を指定します。BMCA は、アナウンス間隔ごとにネットワーク内の各ポート上でローカルかつ継続的に動作し、ネットワーク構成における変更を迅速に調整します。IEEE 1588-2008 に基づく BMCA は、クロックプロパティのアドバタイジングに対するアナウンスメッセージを使用します。

BMCA は、次の基準を使用して、サブドメイン内のベスト マスター クロックを決定します。

- クロック品質（たとえば、GPS は最高品質とみなされます）
- クロックの時刻基準のクロック精度

- 局部発振器の安定性
- グランドマスターに最も近いクロック

IEEE 1588-2008 に基づく BMCA は、受信したデータセットとともに独自のデータセットを使用し、次のプロパティを持つ属性に基づいて、指定された順序で最適なクロックを決定します。

- 優先順位 1: 各クロックにユーザーが割り当てた優先順位。有効な範囲は 0 ~ 255 です。デフォルト値は 128 です。
- クラス: クロックが属するクラス。各クラスには独自の優先順位があります。
- 精度: クロックと UTC 間の精度 (ナノ秒)
- バリアンス: クロックの変動
- 優先順位 2: 最終的な優先順位。有効な範囲は 0 ~ 255 です。デフォルト値は 128 です。
- 固有識別子: 64 ビット拡張固有識別子 (EUI)

BMCA は、ベスト マスター クロックを特定するだけでなく、次のことを保証して、PTP ネットワーク上でのクロック競合の発生を確実に防止します。

- クロックが相互にネゴシエートする必要がない。
- マスタークロック特定プロセスの結果として、マスタークロックが 2 つ存在する、またはマスタークロックが存在しないといった不適切な設定になっていない。

BMCA は常に、ネットワーク上で利用可能な「最良の」グランドマスターを選択します。ほとんどの場合、優先順位 1 と優先順位 2 の値を使用して選択に重みを付け、特定のデバイスを強制的にグランドマスターにすることが有益です。

シスコ産業用イーサネットスイッチ IE5000 と産業用ルータ、または変電所ルータ IR8340 は、GNSS にラッチでき、電力プロファイルモードで PTP グランドマスターとして機能できます。このソリューションガイドで検証された Cisco IOS-XE バージョンによると、IR8340 は PTP Over PRP RedBox、REP、および HSR レジリエンスプロトコルをサポートしていません。IE5000 は、PTP Over PRP および HSR レジリエンスプロトコルをサポートしています。

設計上の考慮事項

- PTP ドメインのプライマリグランドマスターには、信頼できるデバイスを選択することを推奨します。このデバイスには正確で信頼性の高いクロックが必要であり、基準クロックを使用して UTC に同期することが理想的です。
- プライマリグランドマスターは、PTP ドメインの安定性を向上させるため、電源障害などの障害から保護する必要があります。
- セカンダリグランドマスターがグランドマスターになったときのアプリケーションへの影響を最小限に抑えるため、同じ PTP のタイムスケールと UTC オフセットを使用するセカンダリグランドマスターを指定することも推奨されます。
- VLAN 間で時刻を伝搬するには、産業用イーサネットスイッチを境界クロックモードで使用することを推奨します。
- time properties persist コマンドを使用すると、グランドマスターの損失を防ぐことができます。
- 冗長スタートポロジを使用すると、変電所自動化アプリケーションでの時間誤差が減ります。

PRP を介した PTP

Precision Time Protocol (PTP) は Parallel Redundancy Protocol (PRP) を介して動作できます。PTP が PRP ノードの冗長接続を利用できるようにして、その復元力と信頼性を高めます。シスコ産業用イーサネットデバイスは、IEC 62439-3:2016 標準の Annex A に準拠しており、PRP を介して動作する PTP の課題を克服するためのアプローチを図っています。レベルの高い 2 つの変更により、これを実現します。

- PTP パケットに PRP RCT (冗長制御トレーラ) が付加されない
- PTP パケットが PRP の複製ロジックと破棄ロジックをバイパスする (つまり、PTP メッセージは複製されない)にもかかわらず、PTP はスレーブポートとパッシブスレーブポートを介して LAN_A と LAN_B に挿入される (以下を参照)

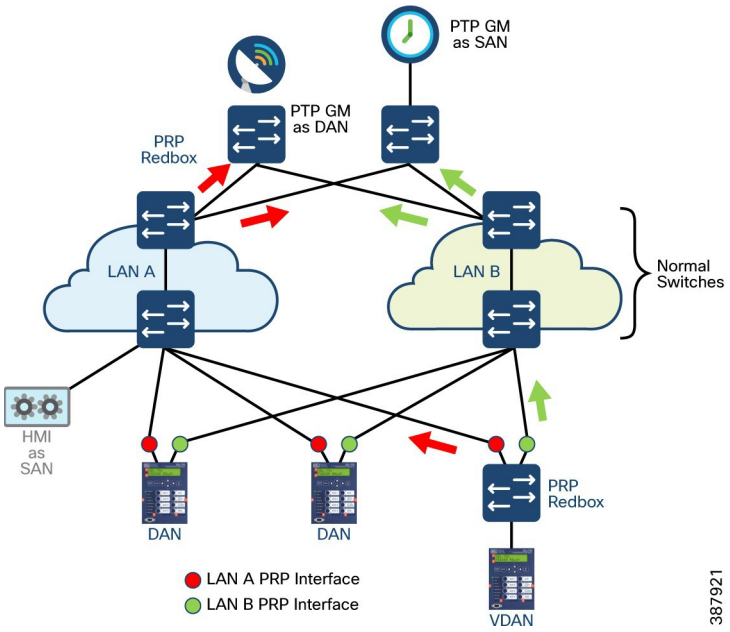
PTP GM を PRP トポロジ内に配置できる方法は次のとおりです。

- 単一の PTP GM は、両方の PRP LAN (LAN-A と LAN-B) に接続する RedBox にすることができます。
- 単一の PTP GM は、PRP RedBox に接続する VDAN にすることができます。
- デュアルスタートポロジ: 2 つの PTP GM を RedBox にすることができ、各 PTP GM は両方の PRP LAN (LAN-A および LAN-B) に接続します。シスコでは、この方法を推奨しています。

LAN-A または LAN-B 内のデバイスだけが GM と同期されるため、GM は LAN-A または LAN-B に接続した SAN になることはできません。

次の図は、2 つの PTP グランドマスタークロックが両方の LAN に接続されているサンプルトポロジを示しています。PTP グランドマスタークロックの 1 つは、PRP RedBox として機能できるシスコ産業用イーサネットスイッチの 1 つに接続されるシングル通信ノードであり、もう 1 つのクロックは、GNSS に接続して PTP 電力プロファイルのグランドマスターとして機能できるシスコ産業用イーサネットデバイスの 1 つで有効になっています。

図 16　　PRP を介した PTP クロック



デュアル通信ノード (DAN) および PRP-RedBox スイッチは、両方の PRP ポートを介して PTP 同期情報を受信します。LAN-A ポートと LAN-B ポートは、PTP グランドマスターと同期された異なる仮想クロックを使用します。ただし、ローカルクロック (図では VDAN) を同期するために使用されるポート (図では SLAVE) は 1 つだけです。LAN-A ポートが SLAVE の場合、LAN-A ポートの仮想クロックが VDAN の同期に使用されます。もう一方の PRP ポートである LAN-B は、PASSIVE_SLAVE と呼ばれます。LAN-B ポートの仮想クロックは、引き続き同じ PTP グランドマスターに同期されますが、LAN-A がダウンしない限り、VDAN の同期には使用されません。次に、LAN-B ポートがスレーブの役割を引き継ぎ、ローカルクロックの同期を継続するために使用されます。

VDAN の場合、PRP RedBox は 2 つの PRP ネットワークを介して PTP を処理します。同様に、図に示されているすべての DAN、VDAN、および RedBox は引き続き同期されます。SAN については、冗長性を備えていないことに注意してください。この例では、LAN-A がダウンすると、SAN として接続された HMI は同期を失います。

この変更により、VDAN は、LAN-A ポートの仮想クロックと LAN-B ポートの仮想クロックの間のオフセットが原因で、そのクロックに瞬間的な同期のずれが発生する場合があります。両方のクロックが同じ GM に同期されているため、同期のずれはせいぜい数マイクロ秒です。このずれは、LAN-A ポートが SLAVE に戻り、LAN-B ポートが PASSIVE_SLAVE になるときにも発生します。

次の表に、PRP を介した PTP 電力プロファイルをサポートするシスコ産業用イーサネットプラットフォームを示します。最新の正確な情報については、プラットフォームガイドを参照してください。

表 12　シスコ産業用イーサネットプラットフォームおよび PRP を介した PTP

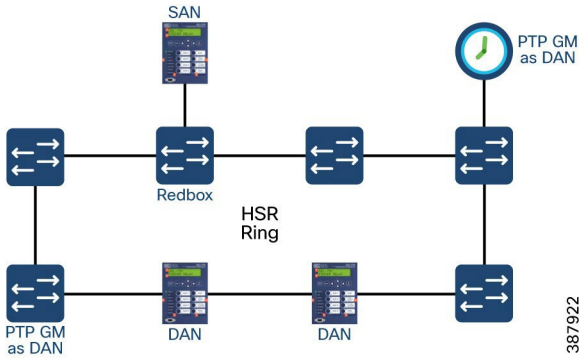
プラットフォーム	IE4000	IE5000	IE3400	IE9300
PRP を介した PTP 電力プロファイル	対応	対応	対応	対応

HSR を介した PTP

HSR の複製/破棄ロジックを PTP パケットに使用し、冗長性を通して PTP に高可用性を提供することはできません。

次の図は、HSR ネットワークで PTP クロック同期がどのように機能するかを示しています。この例では、VDAN/SAN が PTP グランドマスタークロックです。デュアル通信デバイスは、HSR ポートを介して PTP 同期情報を受信します。ただし、ローカルクロックを同期するために使用されるポート (図では SLAVE) は 1 つだけです。もう一方の HSR ポート (図では PASSIVE) は、引き続き同期情報を受信しますが、ローカルクロックの同期には使用されません。RedBox のポート A が SLAVE で、ポート B が PASSIVE であるとします。ポート A がダウンすると、ポート B がスレーブの役割を引き継ぎ、RedBox のローカルクロック同期を継続するために使用されます。

図 17　HSR を介した PTP クロック



HSR ネットワークの PTP グランドマスターは、RedBox、VDAN/SAN、または DANH です。

次の表に、PRP を介した PTP 電力プロファイルをサポートするシスコ産業用イーサネットプラットフォームを示します。最新の正確な情報については、プラットフォームガイドを参照してください。

表 13　シスコ産業用イーサネットプラットフォームおよび HSR を介した PTP

プラットフォーム	IE4000	IE5000	IE3400
PRP を介した PTP 電力プロファイル	対応	対応	対応

VLAN およびトランキング

産業用セキュリティのベストプラクティスとして、IEC62443 ゾーンおよびコンジットに準拠したアーキテクチャにネットワークを移行することを推奨します。攻撃が産業用ネットワークやインフラストラクチャ全体に広がるのを防ぐために、互いに通信する必要のないアセットを個別のネットワークセグメントまたはゾーンに配置することを推奨します。NERC CIP コンプライアンスでは、変電所内および変電所間のアセットの重要度に基づいて、複数の「ゾーン」に分割するよう制定されています。L2 VLAN、L3 VRF、ファイアウォール、セキュリティグループタグ (VLAN または IP アドレスの割り当てに関係なくセグメント化が可能) など、ネットワークにセグメンテーションを導入するメカニズムは多数あります。VLAN により、ネットワークを論理的に分割できます。さまざまなレイヤで行うことができますが、レイヤ 2 を使用するのが最も一般的です。ファイアウォールにより、さまざまなゾーンに出入りするインバウンドおよびアウトバウンドトラフィックを制御します。このセクションでは、VLAN について説明します。

VLAN は、メディアを共有するトラフィックのタイプを分割する方法です。たとえば、次のようになります。

- ESP ゾーン: VLAN を使用した OT トラフィック セグメンテーション
  - MMS SCADA VLAN
  - DNP3 SCADA VLAN
  - GOOSE VLAN (プロセスおよびステーションバス)
  - SV VLAN (プロセスバス)
  - エンジニアリング部門の VLAN
  - PTP VLAN
- 企業ゾーン
  - 監視カメラ VLAN
  - VOIP VLAN
  - WLAN 用のリモートワークフォースのユースケース VLAN
- CIP ゾーン
  - VLAN/IP サブネット
  - HMI
  - SCADA MMS

VLAN はトラフィックを分離するだけで、トランクトラフィックを減らすことを目的としていません。通常、トランクリンクはエッジリンクよりも帯域幅が大きいため、セグメント化する必要はありません。原則として、VLAN 1 のデバイスは、VLAN 2 のデバイスが存在することさえ認識できません。異なる VLAN 上のデバイスは、同じ物理メディアを共有しているにもかかわらず、消費する帯域幅によってのみ相互に影響します。必要に応じて、VLAN 間の通信はレイヤ 3 ルータを介して行われます。VLAN は、レイヤ 2 ブロードキャストドメイン (ブロードキャスト、マルチキャスト、およびユニキャストトラフィックが移動する距離を定義します) を分割し、最初のセキュリティバリアとして機能します。これは、VLAN へのアクセスがネットワークデバイスによって完全に管理されるためです。誤って間違ったポートに接続されたデバイスは通信できません。ただし、VLAN のデータセキュリティは脆弱です。ネットワークの設定不備は潜在的な抜け穴になり、設定が監視されないためです。エッジポートに接続されたエンドデバイスは、通常、VLAN に対応していません。

IEC 61850 は、802.1Q 優先順位のタグ付けを使用して、優先順位の低い MMS や管理トラフィックよりも重要なアプリケーションを保護するために、タイムクリティカルなバストラフィックに特権を与えます。GOOSE と SV トラフィックはレイヤ 2 マルチキャストを使用します。このトラフィックはネットワーク全体に伝播し、すべてのブリッジとすべての IED に到達し

ます。これは、ネットワーク内にあるすべてのリンクの帯域幅に影響を与え、すべてのブリッジとすべての IED で処理時間の遅延が大きくなります。したがって、ステーションバスが多数のデバイスに接続されている場合は、マルチキャストトラフィックを除外できるブリッジで区切られたセグメントに分割することを推奨します。次の図に示すように、さまざまな電圧レベルに応じてステーションバスを分割するのが自然な方法です。

VLAN トランクとは、複数の VLAN が単一のイーサネットリンクを通過できるようにする一方で、それぞれの VLAN でそのトラフィックを分離したままにするネットワーク構成を指します。

サービス品質と重要なトラフィックの保護

Cisco CVD ソリューションでのエンドツーエンドの Quality of Service (QoS) を展開する目的は、さまざまなネットワークアプリケーションやトラフィックタイプを制御し、想定どおりにサービスを提供することです。QoS を実装すると、リソース (帯域幅、機器など) の完全な制御と、いくつかのトラフィックタイプ (ネットワーク管理、物理セキュリティ管理など) とミッションクリティカルなトラフィック (SCADA、PMU、GOOSE) の共存が保証されます。ソリューションの設計と QoS の検証を慎重に行うことで、ミッションクリティカルなトラフィックの損失を軽減し、さまざまなアプリケーションでリソースを効率的に活用できます。

- 専用帯域幅のサポート
- 損失特性の減少
- ネットワークの輻輳の回避と管理
- ネットワーク トラフィックのシェーピング
- ネットワーク全体でのトラフィックの優先順位の設定

QoS は損失、遅延、およびジッターの影響を受けやすいデータを転送を必要がある変電所の自動化をサポートするネットワークにとって重要です。帯域幅が制限されている場合は特に重要です。遅延の影響を受けやすい変電所のアプリケーションには、リアルタイム制御および保護メッセージング (C37.118 同期フェーザデータ、61850 GOOSE、同期フェーザメッセージングなど) が含まれます。

QoS ポリシーを定義して、EtherType やサービスクラス (CoS) に基づいて入力パケットを分類し、適切な QoS グループ値を設定し、QoS グループを使用して出力をさらに処理できます。シスコでは、EtherType に基づいて GOOSE/SV 入力パケットを分類し、出力のプライオリティキューに GOOSE/SV パケットを挿入することを推奨しています。残りのトラフィックは、保証帯域幅が設定されたクラスに入れることができます。

次の表は、変電所自動化 LAN で見られるいくつかの異なるトラフィックタイプ、対応する遅延要件、パケットが流れるバス、対応する推奨の入力・出力分類と QoS 処理を示しています。各展開には、推奨される優先順位のバリエーションが組み込まれている場合があります。そのために、推奨事項にはテンプレートモデルが組み込まれており、必要に応じて追加の粒度を挿入できるようになっています。

表 14　変電所自動化 LAN トラフィックと QoS の要件

トラフィックタイプ	分類基準	出力			注記
メカニズム	入力 QoS グループマーキング	シェーピング	帯域幅保証	輻輳回避	
GOOSE/GSSE/SV	1	プライオリティキューイング (ポリシーオプションあり)	プライオリティキューイング (ポリシングオプションあり)	非対応	ステーションバスとプロセスバスに適用

トラフィックタイプ	分類基準	出力			注記
ネットワーク管理	2	非対応	対応	任意	ステーションバスとプロセスバスに適用
物理的なセキュリティ	3	非対応	対応	任意	ステーションバスとプロセスバスに適用
[ネットワークサービス（Network Service）]	2	非対応	対応	任意	ステーションバスとプロセスバスに適用
リモートコマンドセンター	2	非対応	対応	任意	ステーションバスとプロセスバスに適用
モバイル リモートエンジニアリング	2	非対応	対応	任意	ステーションバスとプロセスバスに適用
リモートワークフォース	4	非対応	対応	任意	ステーションバスとプロセスバスに適用
PTP	4	いいえ	プライオリティキューイング (ポリシングオプションあり)	非対応	ステーションバスとプロセスバスに適用

シスコ産業用イーサネットスイッチは、モジュール型 QoS コマンド ライン インターフェイスをサポートしています。モジュール型アプローチは、次の手順を使用して実装できます。

1. トラフィックの識別と分類: アクセス制御リスト (ACL)、IP アドレス、CoS、IP Differentiated Services Code Point (DSCP; DiffServ コードポイント) などのさまざまな分類ツールを使用できます。ツールの選択肢は、トラフィックタイプによって異なります。
2. 識別されたトラフィックで QoS 機能を実行します。使用可能な QoS 機能には、キューイング、ポリシング、マーキング、およびシェーピングがあります。選択可能な機能は、入力または出力アプリケーションのトラフィックフロー要件によって異なります。
3. 該当するインターフェイスに適したポリシーマップを適用します。

ストーム制御

ストーム制御は、LAN インターフェイスがブロードキャスト ストームによって混乱しないようにします。ブロードキャスト ストームは、ブロードキャスト パケットがサブネットにフラッディングすると発生し、過剰なトラフィックが生み出され、ネットワーク パフォーマンスを低下させます。プロトコルスタック実装またはネットワーク設定のエラーが、ブロードキャスト ストームの原因になります。

変電所コアおよび電力事業者 WAN - 設計上の考慮事項

変電所コアは、さまざまな変電所ゾーンを電力事業者 WAN と相互接続する機能です。NERC CIP 標準で指定されているように、ESP を相互接続するには、電子的アクセス制御システム (EACS) が必要であり、変電所コアの一部と見なされます。さらに、多くの場合、レガシーシリアルデバイスを接続し、電力事業者の WAN を介してオペレーションおよびコマンドセンター内の SCADA アプリケーションに接続を提供するのは、変電所ルータの役割です。

ここでは、次の内容について説明します。

- 変電所コアと電力事業者 WAN、技術プロトコルとアプリケーションプロトコルの要件
- 機器ポートフォリオ
- ESP を接続して保護するための EACS 設計オプション
- レガシープロトコルの設計オプション
- WAN の設計オプション

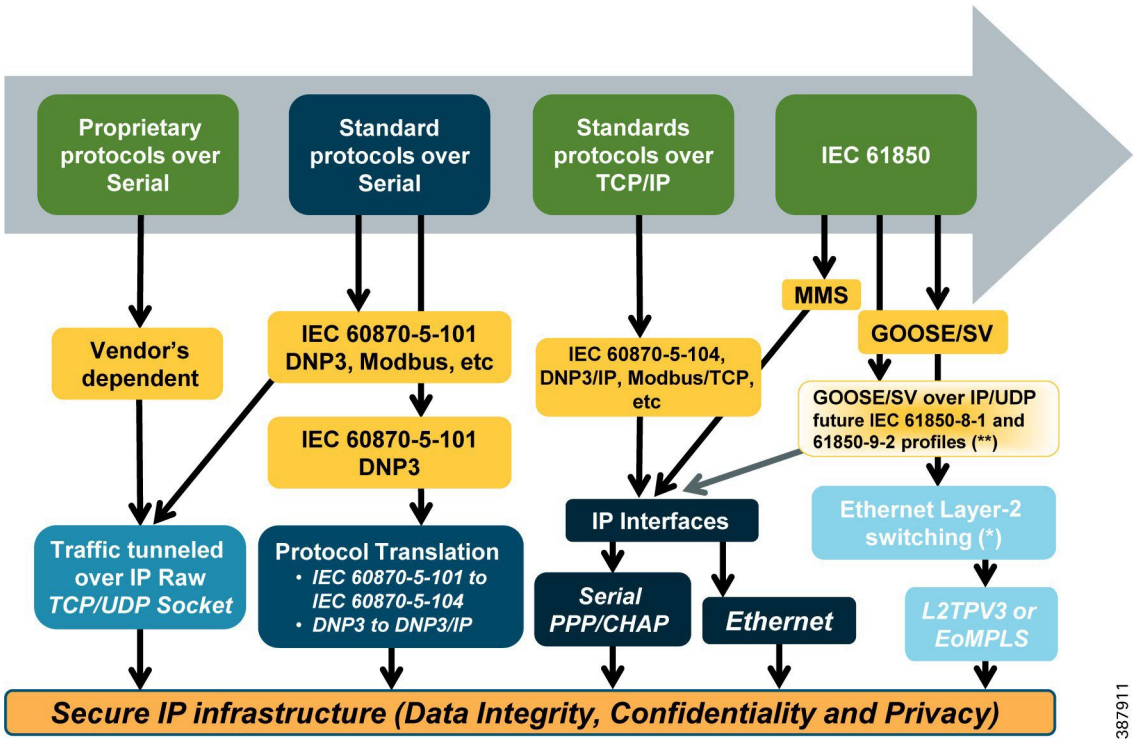
変電所のコアおよび変電所 WAN ネットワーク - 要件

アプリケーションとプロトコル

過去 10 年以上にわたり、変電所のオペレータは変電所の運用を、IEC 61850、DNP3 TCP、Modbus-TCP、IEC 60870-5-104 などの標準ネットワーク (イーサネット、TCP/IP) ベースの通信プロトコルに着実に移行してきました。これらはすべて、ESP ゾーンの一部としてカバーされています。それにもかかわらず、さまざまな理由で標準的なネットワーク接続に移行するのが容易ではない、あるいはコストがかかるデバイスが変電所に存在することが多くあります。そのようなデバイスでは、DNP、Modbus、IEC 60870-5-101 など、さまざまなシリアルベースのレガシー SCADA プロトコルが使用されることがよくあります。

これらのデバイスは変電所の運用に不可欠なことが多いため、変電所オペレータの集中型 SCADA アプリケーションに相互接続する必要があります。変電所コアは、これらのデバイスへの主要な接続を提供し、電力事業者の WAN を介してオペレーションセンターにプロトコルで通信します。このセクションでは、これらのプロトコルによる接続とバックホールに関する設計ガイダンスを提供しました。

図 18　　SCADA プロトコル



技術情報

変電所コア - ポートフォリオ

IR8300 プラットフォームには、2 つの NIM スロットと 2 つの PIM スロット、およびタイミングモジュールがあります。IR8300 には 12 個の LAN インターフェイスがあります。POE を備えた 4 つの銅線、4 つのコンボ SFP/銅線、4 つの SFP ポート、および 2 つの WAN 接続用のコンボ SFP/銅線ポート。すべての LAN と WAN は 1 GE です。IRM-NIM-2T1E1 2 ポート ネットワーク インターフェイス T1/E1 モジュールは、マルチリンク PPP WAN バックホール用にバンドルできます。

WAN 接続では、次の LTE 取り外し可能インターフェイスモジュールがサポートされています。

表 15　IR8340 LTE 取り外し可能インターフェイスモジュール

LTE 取り外し可能インターフェイスモジュール	WAN 接続
P-LTEAP18-GL	4G/CAT18 LTE Advanced Pro Pluggable：グローバル
P-LTE-MNA	4G/CAT6 LTE Advanced Pluggable（北米およびヨーロッパ向け）
P-LTE-EA	ヨーロッパおよび北米向け CAT6 Advanced Pluggable
P-LTE-LA	APAC、LATAM、ANZ 向け CAT6 Advanced Pluggable

WAN モジュールの詳細については、次を参照してください。

https://www.cisco.com/c/en/us/products/collateral/routers/catalyst-ir8300-rugged-series-router/nb-06-cat-ir8340-rugged-ser-rout-ds-cte-en.html

Cisco IR8340 変電所ルータは、電力事業者 WAN、VPN、およびファイアウォール機能について、次の機能をサポートしています。

- 変電所から 1 つまたは複数のコントロールセンターにトラフィックをルーティングするための静的および動的ルーティングオプション
- 他の変電所、マルチサービスとの相互接続
- 下のネット展開の図に示すように、TSO 所有の MPLS バックホールネットワークに接続するための MPLS PE および CE 機能を実行する能力
- LAN 上のアドレスを WAN またはインターネット上の別のアドレスに変換して、適切なルーティングを行い、NAT 機能を使用して LAN デバイスのサイバーセキュリティを保護する機能。
- 変電所の LAN トラフィックとデバイスを不正アクセスから保護するゾーンベースのファイアウォール。
- いくつかの標準プロトコルのいずれかを使用する仮想プライベートネットワーク (VPN) - セキュリティ保護されていないパブリック通信ネットワークを介して安全なリモートの電力事業者サーバーへの隔離された通信トンネルを確立し、メッセージフローの中断または監視から保護するメッセージの強力な暗号化を行います。
- 変電所に出入りする重要なトラフィックに優先順位を付けるために、Diffserv の形式で QoS 機能を実行する能力
- 変電所のユースケース要件に基づいてマルチキャストルーティングを実行する能力
- 外部パス障害の認識と代替パス経由のトラフィックの再ルーティング - BGP、OSFP、EIGRP
- 最初の希望の冗長プロトコル - VRRP および HSRP
- トラフィックの動作と診断の監視、警告、およびロギング

- ルータおよびネットワーク構成管理のためのネットワーク管理プロトコル (SNMP) 通信。
- リモート管理コンピュータ/サーバーとのセキュアシェル (SSH) ネットワーク Web サーバー通信 - ルータの設定と構成をリモートで管理する別の方法。
- LAN Network Time Protocol、NTP、および Simple NTP (SNTP) との日付/時刻情報の交換。
- PTP 電力プロファイルのグランドマスタークロックまたはトランスペアレントクロックとして機能する能力
- 分散型コンピューティング向けのアプリケーションをホストする機能
- インラインネットワークセンサーとして機能し、OT フローおよびアセットの可視性のために Cisco Cyber Vision Sensor ソフトウェアをホストする機能
- POE テクノロジーを使用してエンドポイントを強化する機能
- GNSS 入力

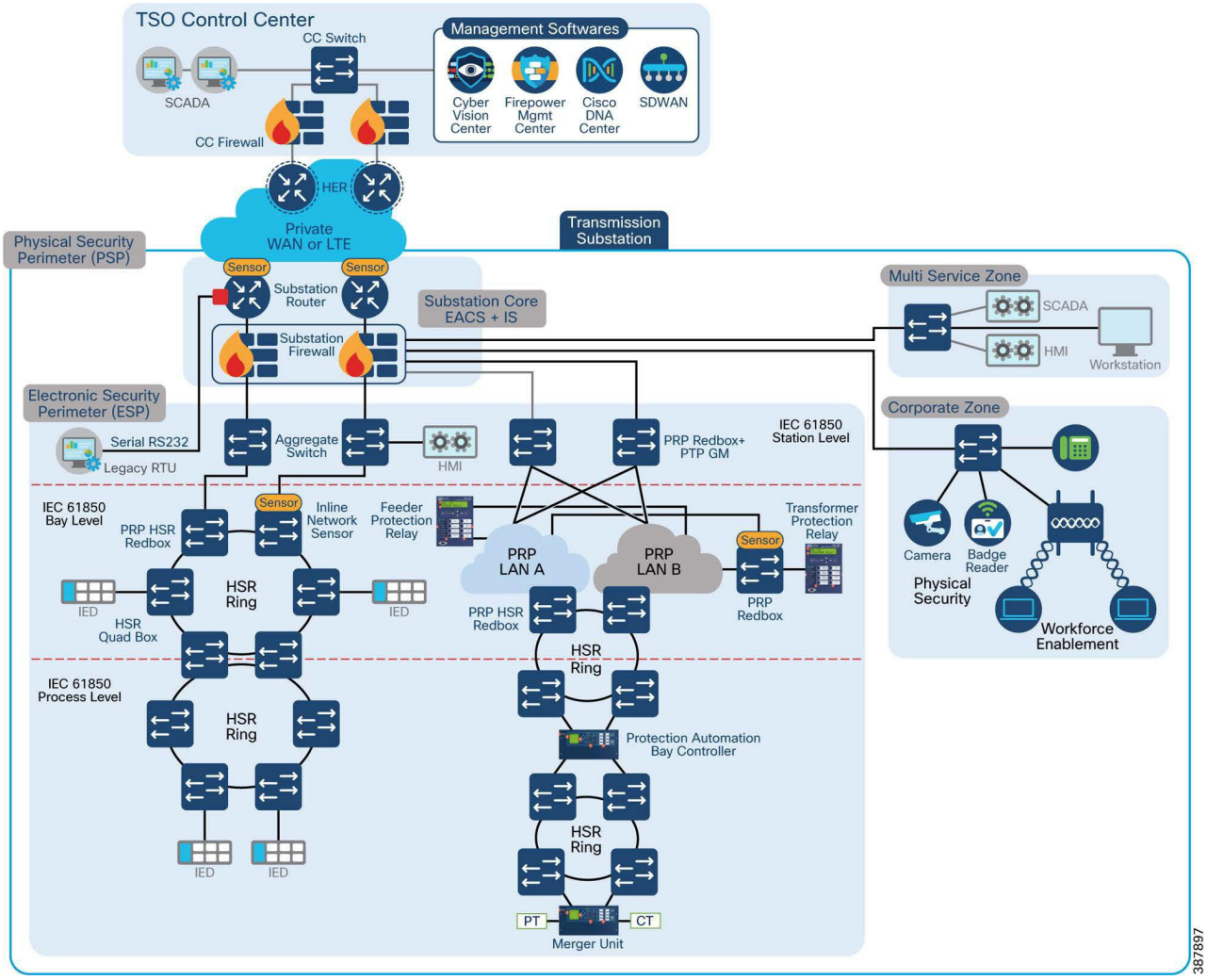
EACS の設計上の考慮事項

設計オプション 1

EACS とルータの組み合わせ

ESP ゾーンと変電所コアゾーン間の L3 ルーティング。次の図に示すように、変電所コアとマルチサービス/企業ゾーン (L2) の間の L2。

図 19　　ESP ゾーンと変電所コアゾーン間の L3 ルーティング



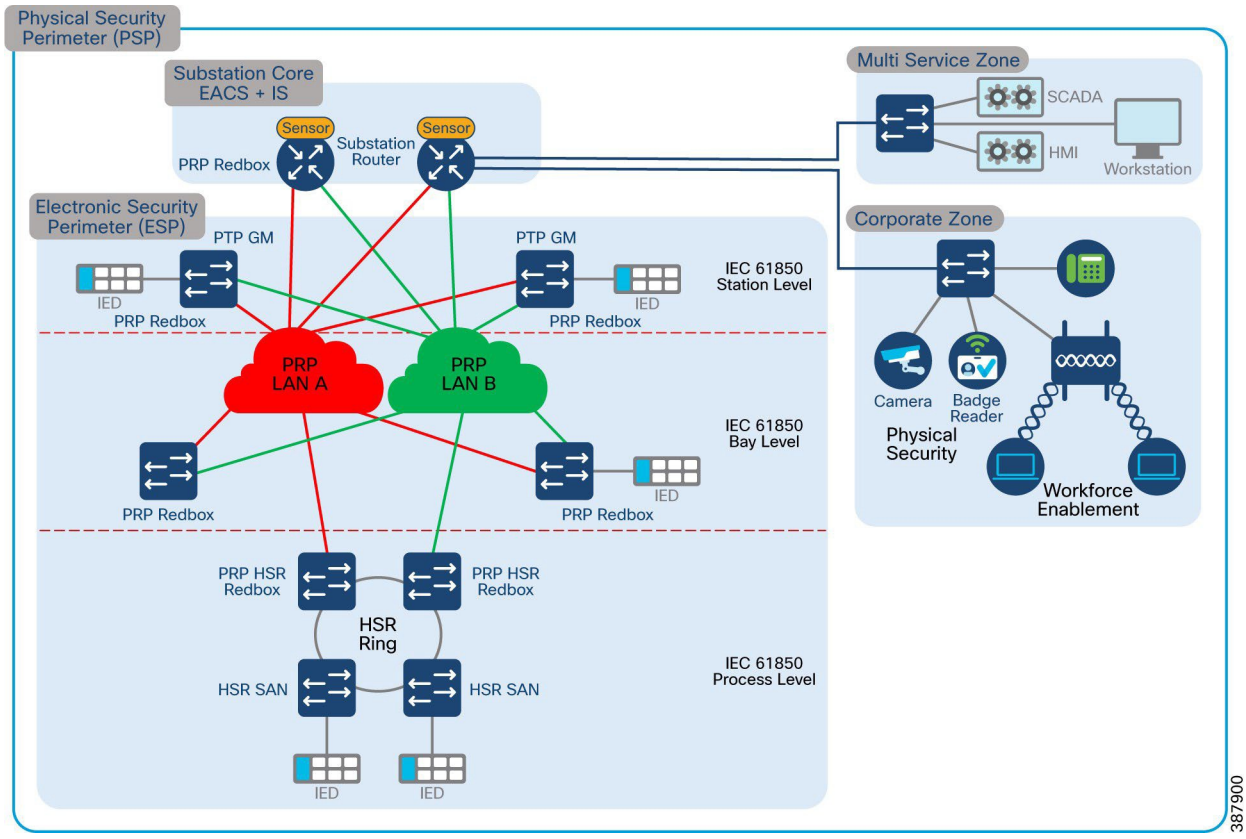
設計オプション 2

ESP ステーションバス (L2) とマルチサービス/企業ゾーン (L2) を直接集約するコアゾーンの変電所ルータ

変電所ルータの ESP ゾーンからの集約 L2 トラフィックには、複数のサブ設計オプションがあります。

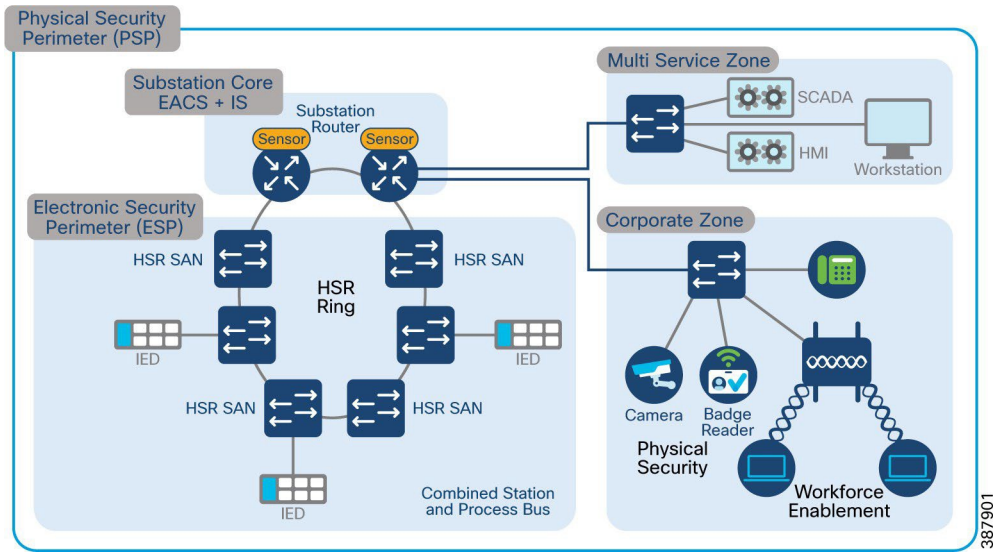
- オプション A - 下の図に示すように、IEC 61850 ステーションバスの一部となり、PRP RedBox として使用される変電所ルータ。マルチサービスおよび企業ゾーンは、変電所ルータにスター型に接続するか、アプリケーション要件に基づいて REP または RSTP のような L2 リングプロトコルを実行できます。

図 20　　ESP ゾーンとマルチサービスゾーンを集約する変電所ルータ



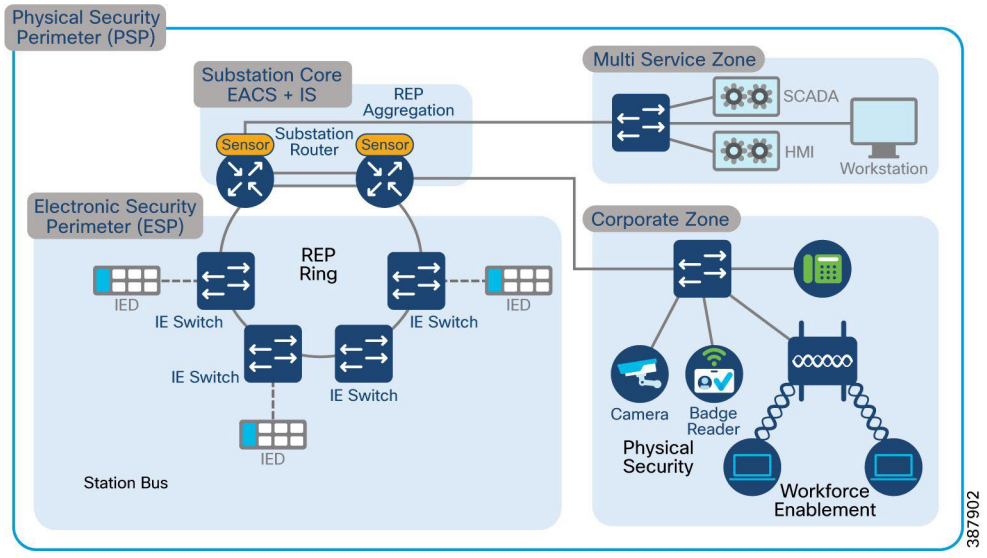
- オプション B - 下の図に示すように、IEC 61850 ステーションバスの一部となり、HSR SAN として使用される変電所ルータ、および上記のオプションのような他のゾーン設計。

図 21　　HSR SAN としての変電所ルータ



- オプション C - ESP、マルチサービス、および企業ゾーンからの複数の REP リングを終端する変電所ルータ。

図 22　　さまざまなゾーンに複数の REP リングを持つ変電所ルータ



さまざまな ESP 設計オプションの長所と短所については、この CVD の後半にあるセクションで説明します。オプションについては、「アーキテクチャ」セクションを参照してください。

レガシー SCADA プロトコルの設計上の考慮事項

raw ソケット

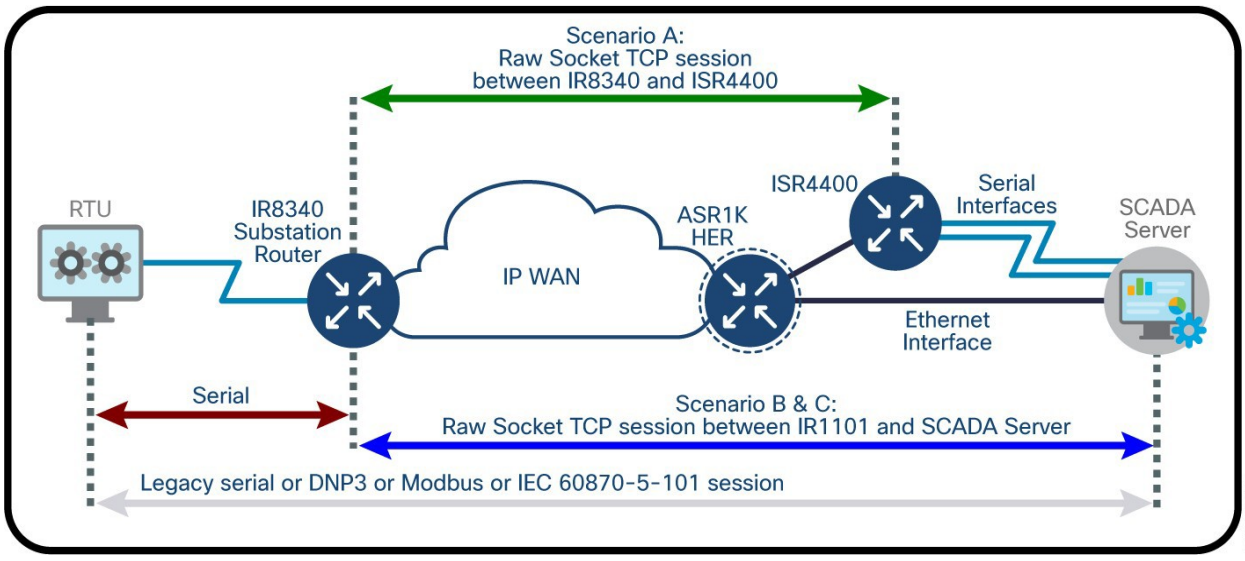
raw ソケットにより、電力事業者アプリケーションの IP ネットワークを介して、1 つのシリアルインターフェイスから別のシリアルインターフェイスに文字ストリームを転送できます。RS232 および RS485 を物理層として使用するシリアル通信は、10 年以上にわたり電力事業者の主力の通信方式でした。現在、業界内でイーサネットへの移行が進んでいます。ただし、イーサネットや新しい IED を既存の通信システムに組み込むには、イーサネットとシリアルデバイスの両方のハイブリッドネットワークをサポートする必要があります。raw ソケットは、リモート端末ユニット (RTU) から遠隔監視制御・情報取得 (SCADA) データを転送します。raw ソケットは、非同期シリアル回線を介したポイントツーポイントおよびポイントツーマルチポイント接続をサポートし、組み込み自動 TCP 接続再試行メカニズムを備えています。特定のパケット長、特定の文字、またはタイムアウト時のデータのパケット化と送信は、raw ソケット内でサポートされているサブ機能です。監視制御 (SCADA) データは、変電所からコントロールセンターに転送されます。SCADA 通信の遅延は、500 ミリ秒から 5 秒の範囲です。

raw ソケットの TCP トランスポート

TCP raw ソケット トランスポートは、クライアント/サーバモデルを使用します。1 つの非同期シリアル回線で、最大 1 つのサーバと複数のクライアントを設定できます。raw ソケット クライアントは RTU からシリアル データのストリームを受信し、そのバッファにこのデータを蓄積してから、ユーザ指定のパケット化基準に基づいてデータをパケットに格納します。raw ソケットクライアントは、raw ソケットサーバーとの TCP 接続を開始し、パケット化したデータを IP ネットワークを介して raw ソケットサーバーに送信します。これにより、パケットからシリアルデータが取得され、それがシリアルインターフェイスに送信され、電力事業者の管理システムに送信されます。

次の図は、ポイントツーポイントの raw ソケットサービスの 3 つの異なる展開シナリオを示しています。

図 23　　raw ソケットの TCP トランスポート



シナリオ A: ヘッドエンドの IR8340 と SCADA ルータ間の raw ソケット - SCADA サーバー上の変更なし - COM ポートを介した通信。

シナリオ B: IR8340 と SCADA サーバー間の raw ソケット - サーバー上の SCADA アプリケーションの変更はありませんが、IP/シリアル リダイレクタ ソフトウェアが COM ポートを IPv4 アドレス + アドレス + TCP ポートにマッピングし、イーサネット インターフェイスを介して通信を実行します。

シナリオ C: IR8340 と SCADA サーバー間の raw ソケット - SCADA アプリケーションは、raw ソケット (IPv4 アドレス + TCP ポート) およびイーサネット インターフェイスを介して直接通信する方法を認識しています。

注: シナリオ A は拡張性がありません。raw ソケットが展開されているシナリオ B またはシナリオ C が推奨されます。

raw ソケットの UDP トランスポート

UDP トランスポートは、ピアツーピア モデルを使用しています。非同期シリアル回線には複数の UDP 接続を設定できます。raw ソケット UDP 対向は RTU からシリアルデータのストリームを受信し、そのバッファにこのデータを蓄積してから、ユーザー指定のパケット化基準に基づいてデータをパケットに格納します。raw ソケット UDP 対向は、IP ネットワークを介してパケット化データをもう一方の終端の raw ソケットピアに送信します。これにより、パケットからシリアルデータが取得され、それがシリアルインターフェイスに送信され、電力事業者の管理システムに送信されます。

プロトコル変換

電力業界において、レガシーベースの SCADA プロトコルから IP ベースのプロトコルへの移行が開始されることに伴い、レガシーベースのプロトコルと新しい IP ベースのプロトコルの両方を相互運用できるようにする移行戦略が必要になります。IR8340 の SCADA ゲートウェイ機能とも呼ばれるプロトコル変換が、これを実現します。

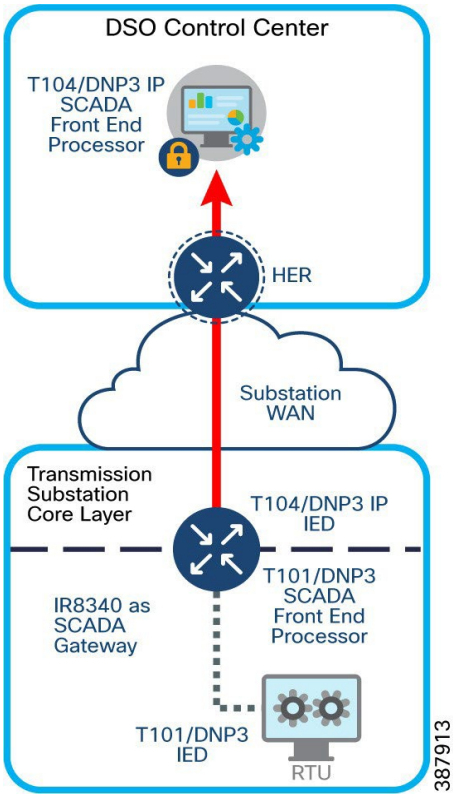
SCADA ゲートウェイ機能により、以下の間で次の変換が可能になります。

- IEC-60870-5-101 および IEC-60870-5-104
- DNP3 シリアルおよび DNP3 IP

次のソフトウェアスタックは、シスコ変電所ルータ IR8340 に実装されています。

- IEC-101 および DNP3 シリアルプロトコルスタック
- IEC-104 および DNP3 IP プロトコルスタック
- 以下の間の変換モジュール
  - IEC-101 および IEC-104
  - DNP3 シリアルおよび DNP3 IP

図 24　　SCADA プロトコル変換



上の図では、IR8340 は SCADA ゲートウェイとして機能し、T101 マスターおよび T104 スレーブ機能を実装します。シリアルインターフェイスごとに 1 つの RTU が接続されます。DA ゲートウェイ/セカンダリ自動化ルータは、T101 スレーブ RTU の T101 マスターとして機能します。次に、DA ゲートウェイ/セカンダリ変電所ルータは、コントロールセンターに存在する SCADA T104 マスターに対する T104 スレーブとして機能します。このシナリオは、ポイントツーポイントのプロトコル変換シナリオを示しています。

T101/T104 プロトコル変換機能

- T101/T104 は、それぞれ IEC 60870-5-101 および IEC 60870-5-104 標準を指します。
- T101 は、シリアル通信を介したポイントツーポイントリンクとマルチドロップリンクをサポートします。
- T104 は、TCP/IP トランスポートおよびネットワークプロトコルを利用して、T101 で指定されているアプリケーションデータ (ASDU) を伝送します。
- 「平衡型」および「不平衡型」の通信タイプを許可します。
- 平衡モードは、いずれかのステーションがトランザクションを開始できるポイントツーポイントリンクに限定されます (dnp3 未承認応答と同様)。不平衡モードは、マスターステーションだけがプライマリフレームを送信できるマルチドロップリンクに適しています。

DNP3/DNP3 IP プロトコル変換機能

シリアルスタック

- 90 秒ごとに RTU からのすべてのデータをポーリングします。
- 90 秒ごとに RTU にローカル時刻を提供します。

- RTU との間のファイル転送をサポートします。
- RTU で未承認応答を有効化/無効化します

IP スタック

- ローカルデータでコントロールセンターの要求に応答します。
- コントロールセンターからそのような要求を受信すると、RTU へのカウンタ問い合わせをトリガーします。
- コントロールセンターからそのような要求を受信すると、RTU への制御トランザクションをトリガーします。
- コントロールセンターとのファイル転送をサポートします。
- コントロールセンターへの未承認応答の送信を有効化/無効化します。

電力事業者 WAN 設計上の考慮事項

アーキテクチャのセクションで説明されているように、WAN 層は送電サービスオペレータ (TSO) のコントロールセンターと送電変電所を集約します。変電所ルータとして導入された Cisco IR8340 は、変電所のローカルエリアネットワークと電力制御またはエンタープライズ WAN 間のインターフェイスとして機能します。

- オンネット変電所
  - 電力事業者所有の MPLS/IP バックホール
  - MPLS CE として機能する変電所ルータ IR8340
- オフネット変電所
  - パブリックバックホール (専用回線/セルラーバックホール)
  - IPSEC (FlexVPN/DMVPN) スポークとして機能する変電所ルータ IR8340

図 25　　オンネット変電所

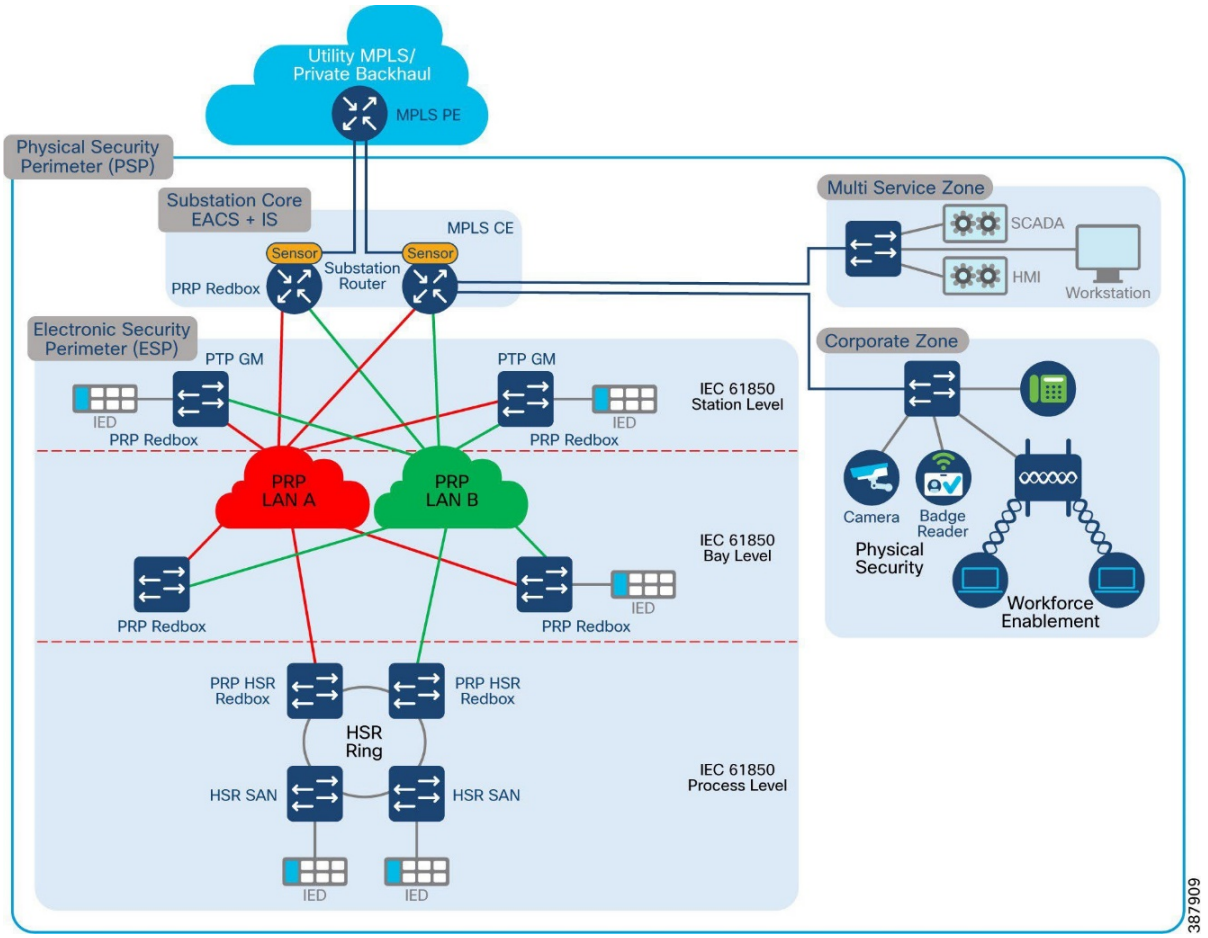
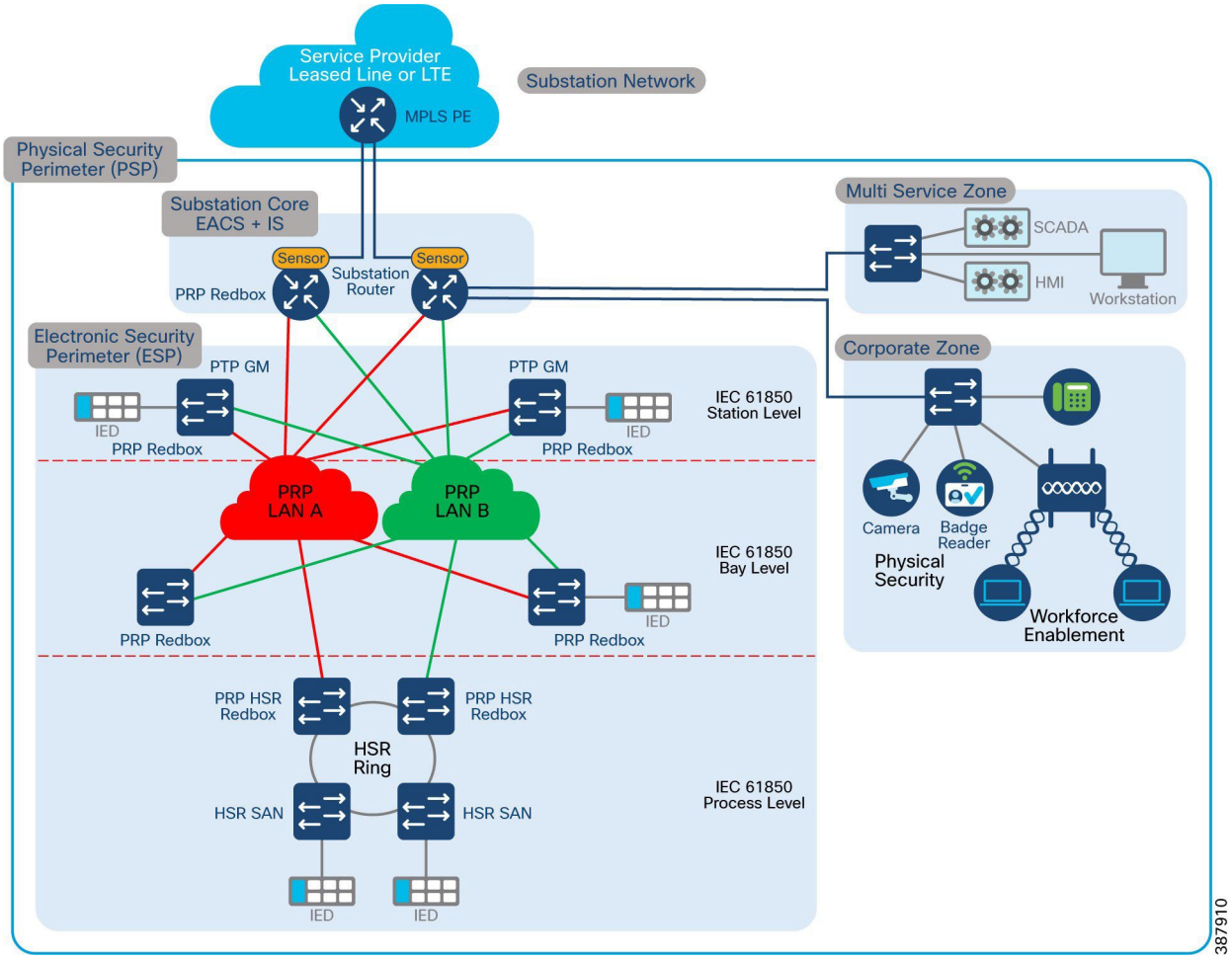


図 26　　オフネット変電所



WAN バックホールの冗長性

このシナリオでは、WAN バックホールパスの潜在的な障害に対処します。

- SA ルータ IR8340 は、さまざまな集約ルータを接続するさまざまなバックホールインターフェイスで展開できます。
- バックホール インターフェイスには、Cisco IOS がサポートするインターフェイスのタイプ (セルラーまたはイーサネット) の組み合わせにすることができます。
- WAN バックホールの冗長性は、複数のオプションを使用して設計できます。
  - オプション 1 : 単一トンネル FlexVPN トンネルピボットのデュアル バックホール インターフェイス (デュアル ISP)
  - オプション 2: デュアルトンネル (アクティブ/アクティブ) とデュアル ISP

変電所自動化ルータの WAN バックホールの冗長性は、配電の自動化/二次変電所ゲートウェイ設計に似ています。WAN バックホールの冗長性設計の詳細については、次の DA CVD を参照してください。

https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Secondary-Substation/DG/DA-SS-DG/DA-SS-DG-doc.html

ネットワーク管理

変電所 LAN と Cisco DNA-Center

Cisco Digital Network Architecture Center では直感的に一元管理できるため、ご使用のネットワーク環境全体でポリシーを素早く簡単に設計、プロビジョニングして適用できます。Cisco DNA Center の GUI は、ネットワークの可視性を提供し、ネットワークの情報を使用してネットワークのパフォーマンスを最適化し、ユーザーおよびアプリケーション エクスペリエンスの向上を実現します。このガイドでは、非 SDA (非ファブリック) 設計に焦点を当てています。ネットワークの正常性がネットワーク管理者に可視化されていないことや、ソフトウェアのアップグレードや設定変更などの手動による保守作業は、変電所自動化 LAN ネットワークにおける一般的な課題の一部です。

Cisco DNA Center を TSO コントロールセンターのアプリケーションとして配置することを推奨しますが、場所に関する最終的な決定は、特定のお客様の要件を考慮して行う必要があります。次のような利点があります。

- DNA Center は、実稼働環境の運用状態を維持するための重要な機能を実行します。重要な機能には、実稼働ネットワークのアシュアランスとモニタリング、特定された問題の手順ガイド付きの修復、デバイスの交換などがあります。
- 実稼働環境用の個別のインスタンスは、運用要件を確実に維持するのに役立ちます。実稼働環境の運用要件は、エンタープライズシステムに比べて非常に厳しく、内容も多岐にわたります。エンタープライズネットワークと実稼働ネットワークの両方をサポートする DNA Center インスタンスでは、不注意な変更や更新が実稼働システムに影響を及ぼし、ダウンタイムにつながる可能性があります。

Cisco DNA Center を追加する際の重要な考慮事項の一部を以下に示します。

- Cisco DNA Center では、管理するすべてのネットワークデバイスへの接続が必要です。つまり、検出およびモニターする必要があるすべてのデバイスに、ルーティング可能で Cisco DNA Center に到達可能な IP アドレスを割り当てる必要があります。
- Cisco DNA Center では、ライセンス情報と更新のためにインターネット接続が必要です。スマート ライセンス プロキシの使用を推奨します。また、プロキシサービスを介したセキュアアクセスを、Cisco DNA Center で必要な URL および完全修飾ドメイン名にのみ許可することを推奨します。詳細については、以下を参照してください。

  https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/hardening_guide/b_dnac_security_best_practices_guide.html

- Cisco DNA Center と管理対象デバイスの間に産業用ファイアウォールがある場合は、ファイアウォールで必要なポートが許可されていることを確認してください。
- Cisco DNA Center が提供するすべてのソリューションで最適なパフォーマンスを実現するには、遅延を 100 ミリ秒以下にする必要があります。最大遅延は 200 ミリ秒 RTT です。100 ミリ秒から 200 ミリ秒の遅延に対応していますが、インベントリ収集や管理対象デバイスとの連携を伴うその他のプロセスなど、特定の機能では実行時間が長くなる可能性があります。
- Cisco ISE は、Cisco DNA Center と互換性のあるバージョンで展開する必要があります。互換性情報については、次のリンクを参照してください。

  https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-device-support-tables-list.html

Cisco DNA Center の確認されている制限事項の一部を以下に示します。

- Cisco DNA Center では、ネットワークアドレス変換 (NAT) 境界の背後にある管理 IP アドレスを持つネットワークデバイスを管理できません。

- Firepower Threat Defense (FTD) ソフトウェアを実行するファイアウォールは Cisco DNA Center ではサポートされていませんが、産業用ファイアウォールの背後に接続されたデバイスは Cisco DNA Center でプロビジョニングおよび管理できます。
- Cisco DNA Center は、PRP、HSR、REP、DLR などのレジリエンスプロトコルの自動ワークフローやアシュアランスをサポートしていません。スイッチは引き続き Cisco DNA Center で検出でき、ソフトウェアアップグレード、コンプライアンス、デバイスアシュアランスなどの機能を利用できます。
- Cisco DNA Center では、サードパーティベンダーの製品を管理できません。

Cisco DNA Center の主要機能の一部を以下に示します。

- 既存スイッチの検出
- 新しいスイッチのオンボーディング
- デバイスの交換
- ネットワーク インフラストラクチャのソフトウェアアップグレード
- ネットワーク インフラストラクチャのソフトウェア、構成、およびセキュリティコンプライアンス
- Cisco DNA Center を介したスイッチ設定
- ネットワークデバイスとエンドポイント ネットワーク ステータスの監視 (IACS デバイスを含む)
- Cisco DNA Center が提供するトラブルシューティングおよび修復ツール
- ネットワークインサイト
- セキュリティ分析

ここでは、デバイスを検出してプロビジョニングする前、またはアシュアランスを使用する前に、Cisco DNA Center で必要な準備作業について説明します。

このセクションは、DNA Center アプライアンスが設置され、ソフトウェアがインストールされていることを前提としています。これらのトピックについては、産業オートメーション向け Cisco DNA Center 導入ガイドで詳しく説明します。ここでは、次の設計作業について取り上げます。

- Cisco DNA Center でのロールベースのアクセス制御を確立します。このガイドで紹介されている Cisco DNA Center のタスクを実行するための適切な権限を持つユーザを作成するために必要です。
- Cisco DNA Center ではユーザーがロールに割り当てられます。このロールにより、ユーザーがシステムで実行できる操作のタイプが決まります。次の定義済みロールは、Cisco DNA Center でサポートされているロールの一部です。
  - ネットワーク管理者ロール
  - オブザーバ ロール
  - Super-Admin ロール

推奨される事前定義ロールは、以下のとおりです。

- ネットワークをプロビジョニングする必要があるユーザーは、Network-Admin-Role を使用する必要があります。
- アシュアランスとインベントリの可視性を必要とするユーザーは、Observer-Role を使用する必要があります。
- Super-Admin-Role を使用できるのは、Cisco DNA Center のシステム管理者に限られます。

サイトを作成してネットワーク階層を定義します。サイトは、ネットワーク内の物理的な場所や機能によってデバイスをグループ化します。

- ネットワーク階層は、ネットワークの場所を表します。これにより、エリア、建物、フロアを含むサイトの階層が可能になります。エリア、建物、フロアは、サイト情報と呼ばれます。サイト情報を作成すると、設計の設定や構成を適用する場所を簡単に特定できます。Cisco DNA Center のサイトは、デバイスに適用するネットワーク設定、ソフトウェアイメージ、およびカスタマイズされたテンプレートを決定します。
- デバイスクレデンシャル、DHCP、NTP サーバーなど、これらのサイトに適用するネットワーク設定を指定します。これらの設定は、自動ワークフローの一環としてサイトに属するデバイスに適用される場合があります。
- ネットワークプロファイルを作成します。スイッチの場合、ネットワークプロファイルは構成テンプレートをサイトに関連付けます。
- ネットワークプロファイルは、1 つまたは複数のサイトのルータ、スイッチ、および WLC の設定を標準化するための Cisco DNA Center の重要な概念です。スイッチの場合、サイト情報、デバイス製品ファミリ、および関連タグに基づいて、構成テンプレートをデバイスに割り当てるためにプロファイルが使用されます。同様の構成を必要とするデバイスの場合、テンプレートは、変数とロジックステートメントを固有の設定のプレースホルダーとして使用することにより、構成時間を短縮するのに役立ちます。
- ネットワーク インフラストラクチャ アップグレードのソフトウェア イメージ リポジトリを管理します。
- Cisco DNA Center はイメージ タイプとバージョンに従い、固有のソフトウェアイメージをすべて保存します。ソフトウェアイメージは、表示、インポート、および削除できます。
- Cisco IR8340 変電所ルータは非ファブリックデバイスであることに注意してください。Cisco IR8340 は、テンプレートポストを使用して、シスコ産業用イーサネットスイッチ IE9300 を搭載する必要がある Digital Network Architecture Center に最初にオンボードする必要があります。

詳細については、次のガイドを参照してください。

https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/IA_Networking/DNA_Center_IA/DNA_Center_IA.html

WAN と vManage

Cisco SD-WAN ソリューションは、企業でのデジタルおよびクラウド変革を実現する、エンタープライズ向けのオーバーレイ方式 WAN アーキテクチャです。ルーティング、セキュリティ、集中型ポリシー、およびオーケストレーションを大規模なネットワークに統合します。このソリューションは、マルチテナント、クラウド経由のオペレーションを提供し、高度に自動化された、セキュア、スケーラブル、アプリケーション認識型で、優れた分析機能を備えています。Cisco SD-WAN テクノロジーは、一般的な WAN 導入の問題と課題に対応します。次のような利点があります。

- 集中型ネットワークおよびポリシー管理、および運用の簡素化。変更管理と導入の時間を短縮します。
- MPLS と低コストブロードバンドの組み合わせ、またはアクティブ/アクティブ方式のトランスポートの組み合わせ。キャパシティを最適化し、帯域幅コストを削減します。
- データセンター、ブランチ、クラウドに拡張するトランスポートに依存しないオーバーレイ。
- 導入の柔軟性。コントロールプレーンとデータプレーンが分離されているため、コントローラをオンプレミスまたはクラウドに導入できます。Cisco WAN エッジルータの導入は、物理的または仮想的に行うことができ、ネットワーク内の任意の場所に導入できます。
- 堅牢で包括的なセキュリティ。データの強力な暗号化、エンドツーエンドのネットワーク セグメンテーション、ゼロトラスト セキュリティ モデルによるルータおよびコントローラの証明書 ID、コントロールプレーンの保護、アプリケーション ファイアウォール、Cisco Umbrella™ の挿入、ファイアウォール、他のネットワークサービスを含みます。

- パブリッククラウドへのシームレスな接続と、ブランチへの WAN エッジの移動。
- リアルタイムのサービスレベル契約（SLA）を適用するアプリケーション認識型ポリシーに加えて、アプリケーションの可視性と認識。
- SaaS アプリケーションの動的な最適化。ユーザのアプリケーション パフォーマンスが向上します。
- アプリケーションとインフラストラクチャを可視化する豊富な分析。迅速なトラブルシューティングを可能にし、効果的なリソース計画のための予測と分析を支援します。

ここでは、Cisco SD-WAN ソリューションの概要について説明します。コントロールプレーン、データプレーン、ルーティング、認証、SD-WAN デバイスのオンボーディングなど、ソリューションのアーキテクチャとコンポーネントについて説明します。このセクションは、vManage バージョン 20.8.1 に基づいています。

- Cisco SD-WAN ソリューションは、個別のオーケストレーション、管理、コントロール、およびデータの各プレーンで構成されています。
- オーケストレーション プレーンは、SD-WAN オーバーレイへの SD-WAN ルータの自動オンボーディングを支援します。
- 管理プレーンは、中央構成とモニタリングの役割を担います。
- コントロールプレーンは、ネットワークトポロジを構築して維持し、トラフィックが流れる場所を決定します。
- データプレーンは、コントロールプレーンからの決定に基づいてパケットを転送する役割を担います。

Cisco SD-WAN ソリューションの主要なコンポーネントは、vManage ネットワーク管理システム（管理プレーン）、vSmart コントローラ（コントロールプレーン）、vBond オーケストレータ（オーケストレーション プレーン）、および WAN エッジルータ（データプレーン）で構成されます。

- vManage：この集中型ネットワーク管理システムは、ソフトウェアベースで、アンダーレイおよびオーバーレイネットワーク内のすべての Cisco SD-WAN デバイスと接続されたリンクを容易にモニタ、設定、および維持するための GUI インターフェイスを提供します。Day0、Day1、Day2 運用の一元管理を提供します。
- vSmart コントローラ：このソフトウェアベースのコンポーネントは、SD-WAN ネットワークの集中型コントロールプレーンの役割を担います。このコンポーネントは、各 WAN エッジルータへのセキュアな接続を維持し、Overlay Management Protocol（OMP）を介してルートおよびポリシー情報を配布し、ルートリフレクタとして動作します。また、WAN エッジルータから発信される暗号キー情報を反映することで、WAN エッジルータ間のセキュアなデータプレーン接続を調整し、非常にスケーラブルな IKE レスアーキテクチャを実現します。
- vBond オーケストレータ：このソフトウェアベースのコンポーネントは、WAN エッジデバイスの初期認証を実行し、vSmart、vManage、および WAN エッジ接続を調整します。また、ネットワークアドレス変換（NAT）の背後にあるデバイス間の通信を可能にするための重要な役割も担います。
- WAN エッジルータ：このデバイスは、ハードウェアアプライアンスまたはソフトウェアベースのルータとして使用でき、物理サイトまたはクラウドに配置され、1 つ以上の WAN トランスポートを介してサイト間でセキュアなデータプレーン接続を提供します。トラフィック転送、セキュリティ、暗号化、Quality of Service（QoS）、Border Gateway Protocol（BGP）や Open Shortest Path First（OSPF）などのルーティングプロトコルを担当します。

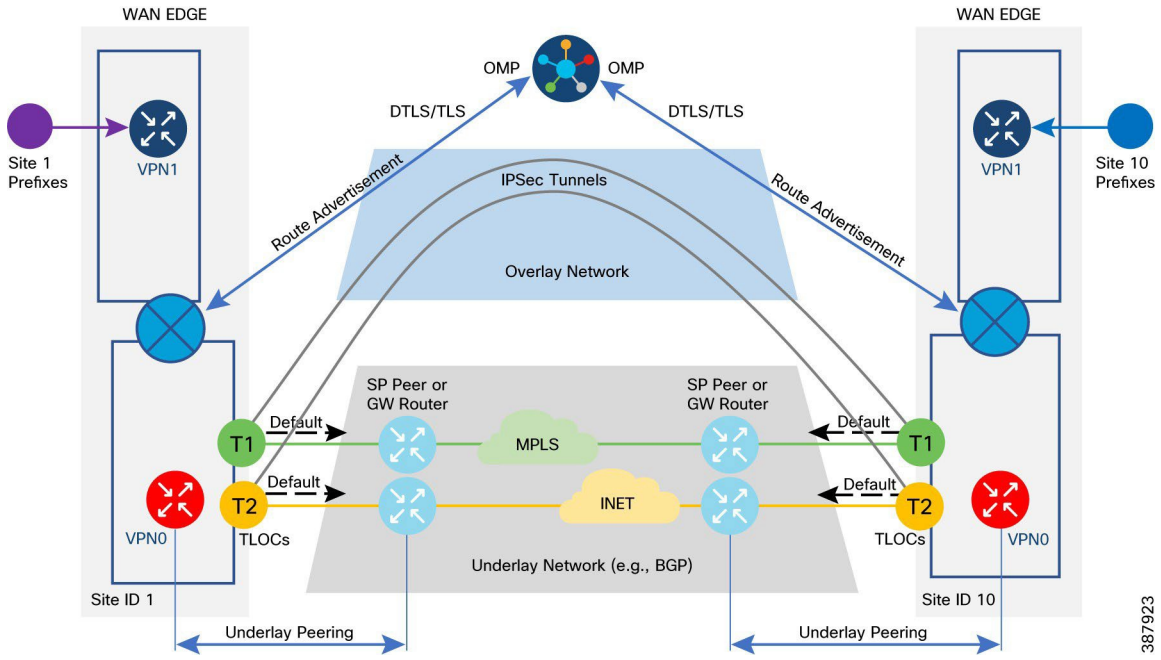
Cisco SD-WAN ネットワークは、アンダーレイネットワークとオーバーレイネットワークの 2 つの部分に分かれています。アンダーレイネットワークは、ルータやスイッチなどのネットワークデバイスを接続し、従来のルーティングメカニズムを使用してデバイス間でトラフィックをルーティングする物理ネットワーク インフラストラクチャです。SD-WAN ネットワークでは、通常、これは WAN エッジルータからトランスポートネットワークへの接続、およびトランスポートネットワーク自体で構成されます。アンダーレイネットワークに接続するネットワークポートは、VPN 0（トランスポート VPN）の一部です。

トランスポートネットワークのサービス プロバイダー ゲートウェイへの接続を取得するには、通常、静的デフォルトゲートウェイを設定する (最も一般的) か、BGP や OSPF などのダイナミック ルーティング プロトコルを設定します。アンダーレ

イネットワークのルーティングプロセスは VPN 0 に限定され、その主な目的は、IPsec トンネルを構築してオーバーレイネットワークを形成できるように、他の WAN エッジルータ上の TLOC への到達可能性を確保することです。

アンダーレイネットワークを使用してサイト間を通過する IPsec トンネルは、SD-WAN オーバーレイネットワークの形成に役立ちます。オーバーレイ管理プロトコル (OMP) は、BGP に似た TCP ベースのプロトコルで、オーバーレイネットワークのルーティングを提供します。このプロトコルは、セキュアな DTLS または TLS 接続を介してコントロールプレーン情報が交換される vSmart コントローラと WAN エッジルータ間で実行されます。vSmart コントローラは、ルートリフレクタのように機能します。WAN エッジルータからルートを受信し、それらにポリシーを適用して処理し、オーバーレイネットワーク内の他の WAN エッジルータにルートをアドバタイズします。

図 27　　SDWAN 論理ネットワーク



お客様は、複数の柔軟なコントローラ導入オプションを利用できます。コントローラは次のように導入できます。

- シスコがホストするクラウドでは、コントローラを AWS または Azure に展開できます。単一または複数のゾーンを導入に使用できます。ほとんどのお客様は、導入が容易で拡張性に優れているため、シスコのクラウドホスト型コントローラを選択します。シスコは、証明書を使用してコントローラをプロビジョニングし、規模と冗長性の要件を満たします。シスコは、バックアップ/スナップショットとディザスタリカバリを担当します。お客様には、vManage へのアクセス権が付与され、デバイスの設定テンプレートと制御およびデータポリシーが作成されます。
- マネージド サービス プロバイダー（MSP）またはパートナーがホストするクラウド内。これはプライベートクラウドでホストされるか、パブリッククラウドでホストされ、AWS または Azure に導入されます。通常、MSP またはパートナーは、コントローラのプロビジョニングと、バックアップおよびディザスタリカバリを担当します。
- 組織が所有するプライベートクラウドまたはデータセンターでのオンプレミス。通常、お客様は、コントローラのプロビジョニングと、バックアップおよびディザスタリカバリを担当します。金融機関や政府機関などの一部のお客様は、主にセキュリティおよびコンプライアンスの理由により、オンプレミス導入を選択する場合があります。

オンプレミスコントローラの導入

オンプレミスコントローラの導入は、セキュリティとコンプライアンス上の理由から、電力事業者のお客様に推奨される導入オプションです。このタイプのコントローラの導入では、コントローラはデータセンターまたはプライベートクラウドにオン

プレミスで導入されます。通常、企業の IT 組織はコントローラのプロビジョニングとバックアップとディザスタリカバリを担当します。金融機関や政府機関などの一部のお客様は、主にセキュリティ コンプライアンスの理由により、オンプレミス導入を選択する場合があります。

オンプレミスの導入では、NAT、パブリック IP、および/またはプライベート IP を使用してコントローラを配置する方法が複数あります。オンプレミスの導入の一般的なオプションは次のとおりです。

制御接続は、パブリックにルーティング可能な IP アドレスを使用して、インターネット トランスポートと MPLS トランスポートの両方を介して確立されます。パブリックにルーティング可能な IP アドレスは、コントローラに直接割り当てることも、1 対 1 の NAT を使用して割り当てることもできます。

制御接続は、プライベート（RFC 1918）IP アドレスを使用して MPLS トランスポートを介して確立され、パブリックにルーティング可能な IP アドレスを使用してインターネットを介して確立されます。vBond は、いずれかのトランスポートからアクセス可能な、パブリックにルーティング可能な IP アドレスを使用できます。または、MPLS トランスポートを介して、プライベート RFC 1918 IP アドレス経由でアクセスできます。

WAN エッジ導入

WAN エッジルータは、リモートサイト、キャンパス、およびデータセンターに導入され、SD-WAN オーバーレイネットワークを介してサイトとの間でデータトラフィックをルーティングします。

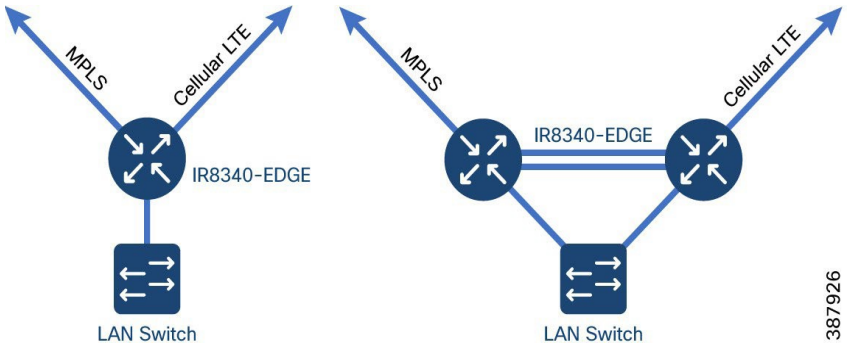
サイトに WAN エッジルータを導入する場合は、トラフィックスループットとサポートされるトンネル数などに応じてプラットフォームを選択し、適切なサイズにする必要があります。冗長性を確保するために、2 番目の WAN エッジルータを追加することをお勧めします。導入時には、適切な冗長性を確保するために、WAN エッジルータは通常、すべてのトランスポートに接続されます。IPsec カプセル化トンネルは、他の WAN エッジルータのロケーションへのデータトラフィックを暗号化し、BFD セッションもこれらのトンネル上で形成されます。サービス VPN から発信されるユーザトラフィックは、トンネルに転送されます。トランスポートまたはトランスポートへのリンクがダウンし、WAN エッジルータがその状態を検出すると、BFD がタイムアウトし、両側のトンネルがダウンします。残りのトランスポートまたはトランスポートリンクは、トラフィックに使用できます。

使用できるトランスポートには、さまざまな選択肢と組み合わせがあります。トランスポートはアクティブ/アクティブ状態で導入され、その使用方法は非常に柔軟です。非常に一般的なトランスポートの組み合わせは、MPLS とインターネットです。MPLS はビジネスクリティカルなトラフィックに使用でき、インターネットはバルクトラフィックやその他のデータに使用できます。一方のトランスポートがダウンすると、もう一方のトランスポートを使用して、サイトとの間でトラフィックをルーティングできます。インターネットはほとんどの場所で信頼性が高く、ほとんどのアプリケーションの SLA を満たすことができるため、多くの場合、サイトは代わりに 2 つのインターネット トランスポートを導入します。

LTE はトランスポートの選択肢として頻繁に使用され、アクティブモードで導入できます。または、他のすべてのトランスポートが使用できなくなるまでアクティブにならない、ラストリゾート回線として導入できます。

以下は、一般的な WAN エッジ環境の一部です。これは詳細なリストではありません。

図 28　　SDWAN WAN エッジ環境



Cisco IR8340 変電所ルータは、電力事業者の変電所自動化ネットワークで SDWAN エッジルータとして使用できます。Cisco IR8340 変電所ルータのオンボーディングにはさまざまな方法があります。

- プラグ アンド プレイ
  - Cisco IR8340 変電所ルータは、devicehelper.cisco.com 経由で PnP 接続して、SD-WAN 関連情報を取得します。
  - Cisco IR8340 変電所ルータは、セキュアトンネルを介して vBond に接続します。
  - 認証が完了すると、vBond は vManage IP および vSmart IP アドレスを Cisco IR8340 変電所ルータに送信します。
  - vManage は、完全な設定を Cisco IR8340 変電所ルータに送信します。
  - Cisco IR8340 変電所ルータは、セキュアトンネルを介して vSmart に接続します。認証が完了すると SD-WAN ファブリックに加わります。

    それぞれの変電所ルータ IR8340 で作成され、関連するすべての設定で構成されるテンプレートがルータに適用され、同じものが展開されます。
- オンサイト ブートストラップ プロセス
  - SD-WAN Cisco IOS XE のみでサポートされます。IR8340 は IOS-XE イメージを実行します。このデバイスは、オンサイト ブートストラップ プロセスを使用してオンボーディングすることもできます。
  - Cisco vManage を使用して構成ファイルを生成します。
  - 構成ファイルをブート可能な USB ドライブにコピーしてドライブをデバイスに接続するか、構成をデバイスのブートフラッシュにコピーします。
  - デバイスを起動します。
  - ブートアップ時に、SD-WAN Cisco IOS XE ルータはファイル名 ciscosdwan.cfg で bootflash: または usbflash: を検索します。
  - それぞれの変電所ルータ IR8340 で作成され、関連するすべての設定で構成されるテンプレートがルータに適用され、同じものが展開されます。

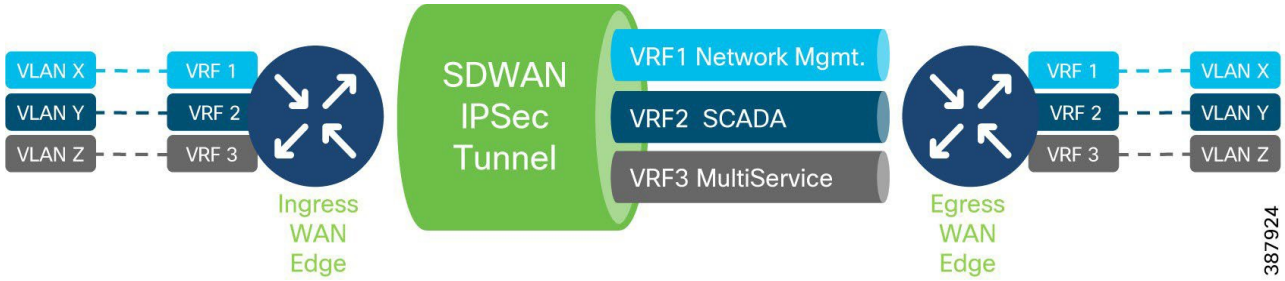
詳細については、導入ガイドを参照してください。

その他の一般的な設計上の考慮事項

- 電力事業者の変電所自動化ネットワークでは、IR8340 は SDWAN 変電所エッジルータとして機能し、ASR1000 シリーズはヘッドエンド WAN エッジルータとして機能します。
- ハブアンドスポーク設計では、変電所とヘッドエンド間でトラフィックを流す必要があります。場合によっては、その後にスポークツースポーク設計で変電所間でトラフィックを流す必要があります。
- トラフィックの分離は、セキュリティ戦略の鍵となります。ルータに入るトラフィックは、ユーザトラフィックを分離するだけでなく、ルーティングテーブルを分離する VPN に割り当てられます。これにより、ある VPN のユーザは、明示的に設定しない限り、別の VPN にデータを送信できなくなります。
  - VPN 0 はトランスポート VPN です。これには、WAN トランスポートに接続するインターフェイスが含まれています。イーサネット、LTE などのさまざまなバックホールを WAN トランスポートとして使用するように構成できます。
  - VPN 512 は管理 VPN です。Cisco SD-WAN デバイスとの間でアウトオブバンド管理トラフィックを伝送します。
- 電力事業者の変電所自動化環境では、IR8340 が入力 WAN エッジになります。変電所 LAN からのトラフィックを集約し、変電所のコントロールセンターでさらに分析するため、同じものを IPSec トンネル経由で転送します。SA LAN か

らのトラフィックは、SCADA、ネットワーク管理、VOIP、ビデオなどのさまざまなサービスのデータであり、処理のためにコントロールセンターに転送されます。これらの各トラフィックストリームには、異なる優先順位を付けることができます。WAN では、このような多種多様なデータストリームに対して、ソリューションに従って必要な優先順位を付ける必要があります。

図 29　　SDWAN WAN エッジ VRF 環境



- WAN バックホールの 1 つが失敗した場合、WAN エッジルータは復元力を示す必要があります。たとえば、入力 WAN エッジルータで、イーサネット WAN バックホールに障害が発生した場合、セルラーをバックアップ WAN バックホールとして使用できます。
- vManage を使用した WAN エッジルータでの Day 0、Day 1、および Day 2 運用の一括管理により、障害、構成、アカウンティング、パフォーマンス、およびセキュリティを集中管理します。
- 豊富なポリシーとテンプレートを使用して、運用を簡素化し、導入を合理化します。その結果、IR8340 WAN エッジルータでサポートされるように、ゾーンベースのファイアウォール、該当する QoS ポリシー、アクセス/トランクポート、NTP、PRP など、さまざまなサービスの変更管理や導入の時間が短縮されます。

ネットワーク管理の概要

Cisco SD-WAN テクノロジーは、一般的な WAN 導入の問題と課題に対応します。次のような利点があります。

- 集中型ネットワークおよびポリシー管理、および運用の簡素化。変更管理と導入の時間を短縮します。
- MPLS と低コストブロードバンドの組み合わせ、またはアクティブ/アクティブ方式のトランスポートの組み合わせ。キャパシティを最適化し、帯域幅コストを削減します。
- データセンター、ブランチ、クラウドに拡張するトランスポートに依存しないオーバーレイ。
- 導入の柔軟性。コントロールプレーンとデータプレーンが分離されているため、コントローラをオンプレミスまたはクラウドに導入できます。Cisco WAN エッジルータの導入は、物理的または仮想的に行うことができ、ネットワーク内の任意の場所に導入できます。
- データの強力な暗号化、エンドツーエンドのネットワーク セグメンテーション、ルータとコントローラーの証明書 ID を含む堅牢で包括的なセキュリティ。
- パブリッククラウドへのシームレスな接続と、ブランチへの WAN エッジの移動。
- アプリケーションとインフラストラクチャを可視化する豊富な分析。迅速なトラブルシューティングを可能にし、効果的なリソース計画のための予測と分析を支援します。

次に、電力事業者の環境におけるいくつかの課題に対処する Cisco DNA Center の機能について説明します。

- プロアクティブな修復のためのネットワークのモニタリングと分析: Cisco DNA Assurance を使用すると、ネットワーク上のすべてのポイントをセンサーに変え、アプリケーション パフォーマンスやユーザー接続に関する継続的なテレメトリをリアルタイムで送信できます。これにより、自動的なパストレースの可視性とガイド付きの修復が連動し、ネットワークの問題が表面化する前に数分で解決されます。

- ネットワークメンテナンスおよび設定タスクの導入と自動化の簡素化: Cisco DNA Automation は、ゼロタッチ デバイス プロビジョニング、ソフトウェアイメージ管理、デバイス交換フロー、およびネットワーク プロビジョニング タスクを提供し、大規模なデバイスの導入、設定、およびメンテナンスを容易にします。さらに、ネットワークがビジネスの目的に合っていることを保証するコンプライアンスチェックが提供されます。
- ネットワークに接続するエンドポイントの一貫したセキュリティポリシー: このソリューションは、Cisco DNA Center、Cisco Identity Services Engine (ISE)、および Cisco Cyber Vision を使用して、アセットと相互連携の可視性を強化し、ネットワークをセグメント化するためのセキュリティポリシーを作成します。

結論

この『変電所の自動化 - 新たなデジタル変電所』の CVD バージョンでは、以下の内容を取り上げました。

- 電子的セキュリティ境界 (ESP) ゾーンのイーサネット
- 新しい Cisco IE 9300 および IR8340。
- Cisco IR8340 における High-Availability Seamless Redundancy (HSR) シングル通信ノード (SAN) プロトコルと Parallel Redundancy Protocol のサポート。
- Cisco IR8340 での HSR および Parallel Redundancy Protocol (PRP) ロスレスプロトコルの実装オプション。
- Precision Time Protocol (PTP) 1588 をサポートする Cisco IE9300。
- 2 つの PRP LAN 上の PTP 1588 v2 展開をサポートする Cisco IE9300 スイッチ。
- Cisco IR8340 変電所ルータの Cisco Cyber Vision Sensor 機能のサポート。
- サイバーセキュリティの課題解決に向けて進化するシスコのソリューション、および Cisco IE スイッチでトラフィックの可視性、セグメンテーション、および異常検出を向上させるために Cisco NetFlow と Stealthwatch を活用する価値。
- 上記すべてのアーキテクチャと検証済みの実装例を紹介し、何を実現できるかを示します。

このドキュメントは、変電所におけるイーサネットの普及を目的としています。イーサネットは、有線によるシリアルベースの変電所環境の代わりとなる、インテリジェントで管理性と柔軟性に優れ、費用対効果の高い環境の構築に役立ちます。シスコの検証済みアーキテクチャを使用することで、変電所自動化の計画と実装に向けた課題を克服できます。

用語一覧

この SA CVD バージョン 3.0 で使用されている略語を表 16 に記載します。

表 16　略語

略語	定義
AAA	認証、許可、アカウンティング
ACL	アクセス制御リスト
AP	Access Point（アクセス ポイント）
CBWFQ	Class-Based Weighted Fair Queuing（クラスベースの重み付け均等化キューイング）
CE	キャリア イーサネット

表 16　略語 (続き)

略語	定義
CG	コネクテッドグリッド
CIP	重要インフラ保護
CLI	コマンドライン インターフェイス
CoS	Class of Service
CorpSS	企業変電所
CT	変流器
CVD	Cisco Validated Design
DANH	HSR 実装ダブル通信ノード
DAU	データ収集装置
DMZ	Demilitarized Zone（緩衝地帯）
DSC	DiffServ コード ポイント
ESP	電子的セキュリティ境界
GM	グランドマスター
GNSS	グローバルナビゲーション衛星システム
GOOSE	Generic Object-Oriented Substation Events
GPS	グローバル ポジショニング システム
HA	High Availability（高可用性）
HMI	ヒューマン マシン インターフェイス
HQoS	階層型サービス品質
HSR	High-Availability Seamless Redundancy
IA	産業用オートメーション
IE	(シスコの) 産業用イーサネット
IEC	国際電気標準会議
IED	インテリジェント エンド デバイス
IND	Cisco Industrial Network Director
IP	インターネット プロトコル
IRIG	射程間計装グループ
ISE	Identity Services Engine
IT	情報技術
L3VPN	レイヤ 3 バーチャル プライベート ネットワーク
LAN	ローカル エリア ネットワーク
MAC	Media Access Control; メディア アクセス コントロール
MQC	モジュラ QoS コマンドライン インターフェイス
MMS	Manufacturing Message Specification
MPLS	マルチプロトコル ラベル スイッチング
MU	統合ユニット

用語一覧

表 16　　略語 (続き)

略語	定義
NDA	機密保持契約
NERC	北米電力信頼度協議会
NIST	国立標準技術研究所
NMS	ネットワーク管理システム
OAM	運用およびメンテナンス
OT	運用テクノロジー
PCP	優先順位コードポイント
PI	(Cisco) Prime Infrastructure
PLC	プログラマブル ロジック コントローラ
PMU	位相計測装置
PoE	Power Over Ethernet
PRP	Parallel Redundancy Protocol
PT	計器用変圧器
PTP	Precision Time Protocol
QoS	Quality of Service
RedBox	冗長ボックス
REP	Resilient Ethernet Protocol
RCT	冗長制御トレーラ
RSTP	高速スパニングツリープロトコル
RTU	リモート端末ユニット
SA	変電所の自動化
SAN	シングル通信ノード
SCADA	遠隔監視制御・情報取得
SCD	変電所構成記述
STP	スパニングツリープロトコル
SV	サンプル値
TCP	伝送制御プロトコル
TLV	型、長さ、値
TR	技術レポート
UCA IuG	電力事業者の通信アーキテクチャ国際ユーザーグループ
UDP	ユーザー データグラム プロトコル
VDAN	仮想デュアル通信ノード
VID	Version Identifier
VLAN	仮想ローカル エリア ネットワーク
WAN	Wide Area Network：ワイドエリア ネットワーク
Wi-Fi	IEEE 802.11x ワイヤレスイーサネット接続