



変電所の自動化：新しいデジタル変電所

Version 3.0

Implementation Guide



このドキュメントに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このドキュメントは「現状有姿」として提供されます。

このドキュメントに記載されているすべての表明、情報、および推奨事項は、明示的、黙示的または法定的を問わず、商品性、特定目的への適合性、権利の非侵害、または取引過程、使用、取引慣行から生じる保証を含みますがそれに限定することなく一切の保証をしません。いかなる場合においても、シスコは、このドキュメントに適用できるまたは適用できないことによって、発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、懲罰的、警告的あるいは特殊なあらゆる法律で認められる範囲の損害について、あらゆる可能性がシスコに知らされていても、それらに対する責任を一切負わないものとします。

このドキュメントのすべての印刷版と複製ソフトは管理対象外と見なされます。最新版については、現在のオンラインバージョンを参照してください。

Cisco は世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号は当社の Web サイト

(www.cisco.com/go/offices) をご覧ください。

©2022 CISCO SYSTEMS, INC. ALL RIGHTS RESERVED



目次

はじめに.....	5
ナビゲータ	5
対象読者.....	5
ドキュメントの目的と対象範囲	6
実装ワークフロー	6
変電所の自動化の要件と使用例	6
システムの概要	7
ソリューションの検証トポロジ	7
ハードウェアソフトウェアマトリックス	11
IP アドレッシング	13
ライセンス	14
変電所自動化ソリューションの実装	15
参考資料.....	15
WAN とコアの実装	16
変電所ルータ MPLS バックホール	17
IR8340 : セルラーバックホール.....	26
変電所ルータ マルチリンク バックホール.....	29
LAN の実装.....	41
レガシープロトコルの実装.....	41
RPVST	41
REP	44
ロスレスプロトコルの実装.....	49
PRP	49
HSR	56
タイミングプロトコルの実装.....	61
NTP	61
PTP	64
SCADA の有効化	70
ゾーンベースのファイアウォールの実装	106
QoS の実装.....	118
ネットワーク管理	122
SDWAN を使用した IR8340 管理	122
前提条件	129
DNAC を使用した IR8340 管理	136
ライセンス	137
付録：設定の実行	146



変電所の自動化：新しいデジタル変電所

はじめに

スマートグリッドは、通信および情報技術と統合された配電システムであり、グリッド運用を強化し、顧客サービスを改善し、コストを削減し、新しい環境上の利点を実現します。このドキュメントでは、発電から送配電、スマートビルディング、スマートホーム、およびユーティリティネットワークに接続されたその他のサイトのエンドユーザーに至るまで、電気システムを監視および管理するためのネットワークの全体的な使用法について説明します。OTの世界が従来のITの世界と衝突するにつれて、公益事業の顧客にとってセキュリティはますます重要になっています。今日のニュースには、金銭や情報を盗んだり、サービスを妨害したりするために、重要なネットワークにアクセスしようとするハッカーやテロリストに関する多くの記事があります。

このソリューションは、アクセスを制限し、データを保護し、イベントと変更を記録し、変電所でのアクティビティをモニタリングするための包括的なアプローチを提供することにより、これらの懸念の多くに対処することを意図しています。

ナビゲータ

対象読者

このガイドは、システムアーキテクト、ネットワーク/コンピューティング/システムエンジニア、フィールドコンサルタント、Cisco Customer Experience (CX) スペシャリスト、およびお客様を対象読者としています。読者は、ネットワークングプロトコル、ファイアウォールのセキュリティ概念、暗号化、ディープパケットインスペクション、公開キーインフラストラクチャ、およびシスコの変電所自動化ソリューションアーキテクチャに精通している可能性があります。

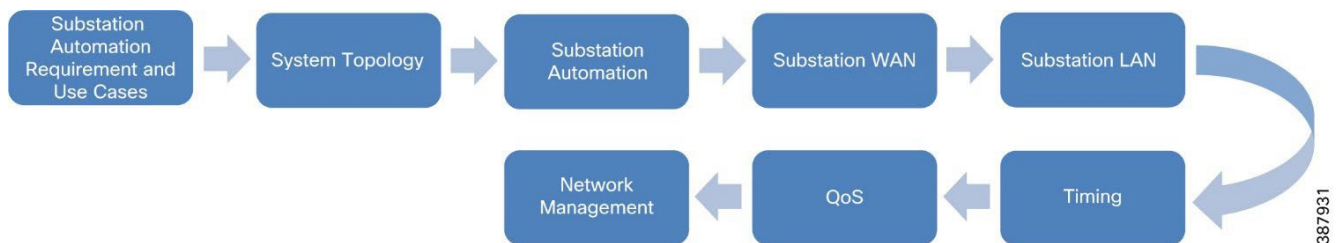
ドキュメントの目的と対象範囲

このガイドは、変電所の自動化、つまり新しいデジタル変電所設計の実装に関する詳細を提供するのに役立ちます。このドキュメントで扱う範囲は、IEC 61850 プロトコル規格に準拠した変電所 LAN 環境のプロセスバスおよびステーションバス向けのシスコソリューションを含む、最新の送電変電所向けのシスコ情報通信技術 (ICT) ソリューションアーキテクチャと実装です。フォールトトレラントなマルチサービスネットワーク設計がどのように実装されるかについて説明します。

実装ワークフロー

本導入ガイドの情報の流れを次の図に示します。このガイドには、読者が全体像を理解するのに役立つように、このドキュメントまたは関連するガイドの他のセクションへの相互参照も含まれている場合があります。

図1 実装ワークフロー



変電所の自動化の要件と使用例

Cisco SA LAN、WAN、およびセキュリティソリューションによって提供される機能は、以前の検証作業以降、進化してきました。変電所の自動化のバージョンである The New Digital Substation は、以下にリストされている最後の検証サイクル以降に行われるさらに重要な開発に焦点を置いています。

- 最近導入された産業用変電所ルータ Cisco IR8340 を変電所自動化ネットワークで使用できることを検証します。
- 最近導入された産業用イーサネットスイッチである Cisco IE 9300 を変電所自動化ネットワークで使用することを検証します。
- PRP、HSR の可用性を備えた新しい変電所ルータ IR8340 でのネットワークレジリエンスプロトコルのサポート。
- ハイアベイラビリティ シームレス冗長性 (HSR) 単一接続ノード (SAN) 。
- Parallel Redundancy Protocol (PRP) RedBox

- 以下の導入による IR8340 でのネットワークベースのタイミングのサポート：
 - 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
 - Precision Time Protocol (PTP) 1588 v2 タイミングプロトコル。
- IE9300 でのネットワークベースのタイミングのサポート：
 - Precision Time Protocol (PTP) 1588 v2 タイミングプロトコル。
 - PRP LAN の両端 (A および B) 上の Precision Time Protocol (PTP) 1588 v2
- Cisco Substation Router IR8340 を管理する SDWAN vManage
- Cisco Substation Router IR8340 および IE9300 を管理する Cisco DNAC。

システムの概要

ソリューションの検証トポロジ

以下は、設計ガイドで説明されているさまざまな設計を検証するために使用されたあらゆるトポロジです。次のトポロジに見られる変電所ルータは、PE ルータとして設定され、MPLS が有効になっています。これらのルータには、設計の推奨事項に従って設定されたさまざまなネットワークレジリエンスプロトコルがあり、さまざまな LAN ネットワークに接続された変電所 LAN デバイスのレイヤ 3 ゲートウェイとして機能し、Operations Control Center に到達します。Operations Control Center および MPLS WAN 接続は、次のトポロジには表示されません。詳細については、以前のバージョンの Grid Security 実装ガイドを参照してください。

図2 変電所ルータの PRP

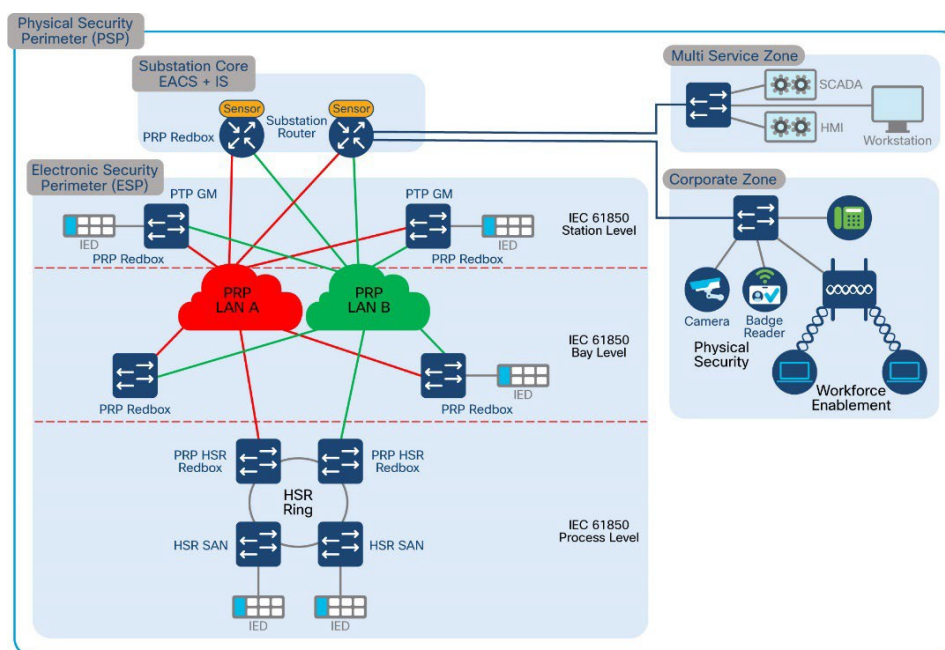


図3 変電所ルータのHSR

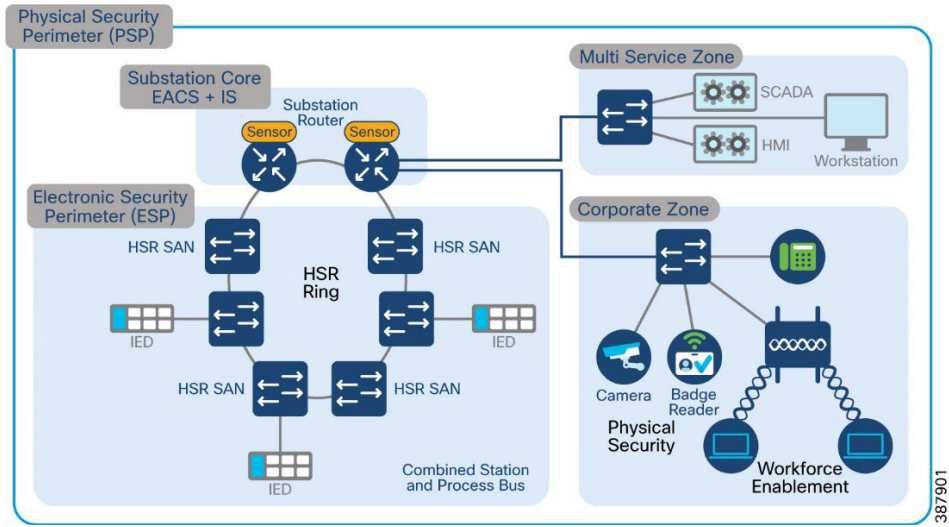
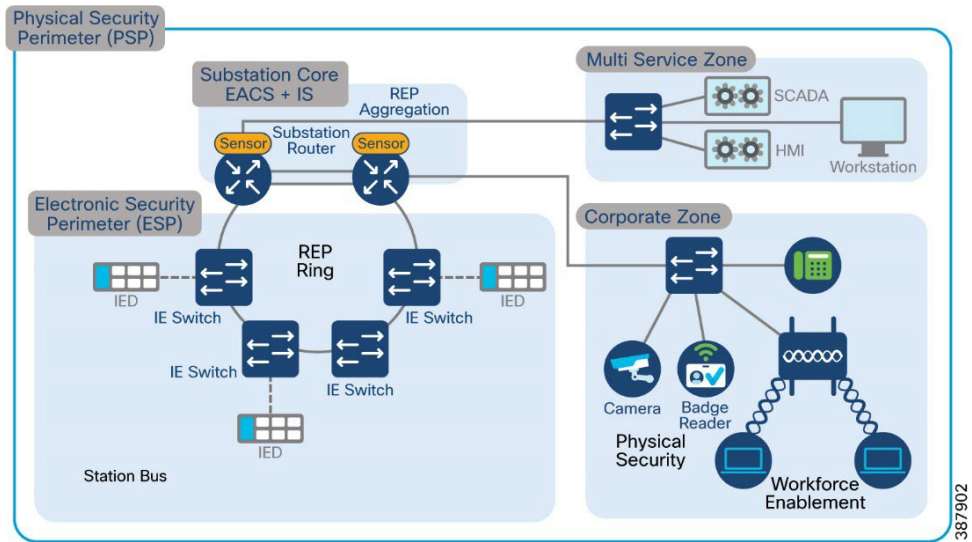


図4 変電所ルータのREP



変電所の設計の主要なコンポーネントは次のとおりです。

ネットワークの復元力

情報通信トポロジ ネットワーク レイヤの高可用性により、ネットワーク障害時にネットワークの回復力とより優れたコンバージェンスが提供されます。さまざまなプロトコルを使用できます。リングトポロジ展開内の一部のレガシーレジリエンス プロトコルは次のとおりです。

■ ラピッド スパニング ツリー (RSTP) は、スパニング ツリー プロトコル (STP) の変形であり、Cisco スイッチを使用した IT プロフェッショナルによって知られ、使用され、信頼されています。

■ Resilient Ethernet Protocol (REP) : 以下で説明するシスコ独自のプロトコル。

ステーションバスおよびプロセスバスの IEC 61850 実装規格、電力事業者変電所の高性能アプリケーションでは、いくつかの重要な要件に対処する必要があります。変電所のアーキテクチャは、両方ともマルチキャストトラフィックタイプである GOOSE とサンプル値の設計要件を満たす必要があります。これには、スケール、セグメンテーション、および通信の要件を満たす高可用性 (HA) とトポロジの選択が含まれます。IEC 61850-5 は、標準のユースケースに基づいた HA および通信要件のガイダンスを提供します。ユースケースによっては、これらのフェールオーバーとリカバリ時間がゼロミリ秒であるため、真に「ヒットレス」なアーキテクチャが必要です。このヒットレス要件を満たすには、2つの選択肢があります。

■ 並列冗長プロトコル (PRP) は、ノード数に制限のないツリートポロジまたはリングトポロジをサポートし、ゼロミリ秒のフェールオーバー/リカバリ要件を提供できます。ただし、PRP には 1 つの欠点があります。PRP では、LAN (LAN-A および LAN-B という名前) を複製し、ネットワーク機器のハードウェアを 2 倍にする必要があります。

■ 高可用性シームレスリング (HSR) もゼロミリ秒のフェールオーバー/回復要件を提供しますが、リングトポロジでのみ利用可能であり、限られた数のデバイスにスケーリングします。HSR では、ESP に重複した LAN (スイッチング インフラストラクチャの 2 倍) は必要ありません。

企業変電所 (CORPSS) ゾーン

企業変電所ゾーンは、社内/企業の「汎用」ネットワークへの自然な拡張です。このゾーンからのトラフィックは、外部ゾーンを通過することによってのみ、他の企業資産に直接アクセスできます。他のゾーン (CIP および ESP) へのアクセスには、追加の資格情報とアクセス制限が必要です。

すべての従業員は、このゾーンを利用して、電子メール、ファイル共有、および外部ゾーンを介したインターネットへの一般的なアクセスなどのビジネスリソースへの基本的な接続を行うことができます。

重要なインフラストラクチャ境界 (CIP) ゾーン

マルチサービスゾーンとも呼ばれる CIP ゾーンは、変電所の「DMZ」です。これは「一部信頼できる」ゾーンであり、企業変電所ゾーンと ESP ゾーン間にファイアウォールセキュリティレベルがあります。そのため、このゾーンは、情報セキュリティ (InfoSec) で強化された Bastion ホストを利用して、企業変電所と ESP ゾーンの間でプロキシされたユーザーレベルのアクセスを許可するように設計されています。このゾーンには、Cisco ISE や ACS などのセキュアポリシーサーバー、ネットワークサービス、およびライトウェイトディレクトリアクセスプロトコル (LDAP) や Active Directory (AD) などのユーザー管理サーバーなど、他のサポートインフラストラクチャが存在する場合があります。

電子的セキュリティ境界 (ESP) ゾーン

ESP ゾーンには、重要インフラストラクチャ/スマートグリッドの適切な機能において積極的な役割を果たすコンポーネントが含まれています。これらのコンポーネントは、変電所ネットワーク上で最も価値があり信頼できるリソースであり、高度に保護されていると見なす必要があります。

ごくわずかな例外を除いて、ネットワークのこの部分からのアウトバウンド通信は大幅に制限する必要があります。このゾーンからセキュリティの低いゾーンへの通信では、ESP ゾーンから接続を開始する「プル」モデルを利用する必要があります。ESP ゾーンへのインバウンド接続は、ビジネスクリティカルなアプリケーションを除き、お勧めできません。

このゾーンは、機械のメンテナンスのためにサブステーションへの直接アクセスを必要とする、適切に精査された従業員に制限されたユーザーレベルのダイレクトアクセスを使用して、IED や保護リレーなどの産業用コンポーネントに限定されたネットワーク接

続を提供することを目的としています。採用するセキュリティモデルに応じて、IED および保護リレーへのアクセスを、十分に吟味され且つ高度にモニタリングされた特定のホストに制限して、個人/企業のラップトップからのアクセスを拒否することもできます。このゾーンからのアウトバウンド接続は厳しく制限されています。

変電所コアゾーン

このゾーンは、インフラストラクチャが電力事業者によって所有されているか、サードパーティのサービスプロバイダーによって提供されているかに関係なく、サブステーショントポロジを残りのインフラストラクチャに接続します。

このゾーンは信頼されていません。この外部ゾーン内の資産のセキュリティ体制は、ほとんどの場合、電力事業者の管理外にあります。

このインターフェイスを通過できるトラフィックは、ファイアウォールの内部ゾーン (ESP、CIP、CORPSS) から暗号化、認証、または最初に開始する必要があります。このゾーンは変電所アーキテクチャの外部と見なされるため、このゾーンの保護はさまざまであり、WAN インフラストラクチャによって提供される保護のみに依存します。

ハードウェア ソフトウェア マトリックス

次の表は、ハードウェア、ソフトウェア、およびソリューションの主要コンポーネントの役割を示しています。これらのソフトウェアバージョンは、シスコソリューション検証ラボで使用されたものであり、このドキュメントが公開された時点ですべて公開されていました。

表1 ハードウェア ソフトウェア マトリックス

デバイス ロール	説明	ハードウェア プラットフォーム	ソフトウェア リリース
変電所ルータ	堅牢なルータ、レイヤ3 ゲートウェイ、レイヤ2 アグリゲータ	IR8340	IOS-XE 17.9.1
変電所ファイアウォール	堅牢なファイアウォール、仮想プライベートネットワーク (VPN) ヘッドエンド (サイト間、RA)、FirePOWER 侵入防御システム (IPS)	ISA3000	FTD : 7.0.1

デバイス ロール	説明	ハードウェア プラットフォーム	ソフトウェア リリース
高耐久性スイッチ	アクセススイッチ : DANH、SANH、RedBox など、スイッチポートのセキュリティ	IE4000	15.2(8)E1
高耐久性スイッチ	アクセススイッチ、スイッチポートセキュリティ	IE5000	15.2(8)E1
高耐久性スイッチ	アクセススイッチ、スイッチポートセキュリティ	IE4010	15.2(8)E1
高耐久性スイッチ	アクセススイッチ、PRP Redbox、スイッチポートのセキュリティ	IE9300	IOS-XE 17.9.1
サイバービジョンセンサーを備えた堅牢なスイッチ	Cisco Cyber Vision Sensor アプリケーション (リリース 4.1.2) をホストし、ネットワークセンサーとして機能するエッジ コンピューティングプラットフォーム	IE3400	IOS-XE 17.9.1S
コントロール/データセンター ファイアウォール	ファイアウォール	FPR4150	FTD : 7.0.1
AAA	ポリシー定義用認証・認可サーバー	Cisco Unified Computing System で仮想マシンとして実行される Identity Services Engine	2.4.0.357 パッチ 10
IPS	FirePOWER IPS デバイスの集中管理および監視サーバー	VMware 用 Firepower Management Center	FMC: 7.0.1
Cisco Cyber Vision Center	IR8340 または IE3400 プラットフォームでホストされている Cisco Cyber Vision センサーアプリケーションを管理するために使用される Cisco Cyber Vision Center。	CVC	4.1.2
SDWAN	WAN 管理	SDWAN	20.8.1
DNAC	LAN 管理	DNAC	2.3.4

IP アドレッシング

この実装は、ラボでの検証作業のための単純なトポロジを想定しています。次の表に、Cisco UCS サーバーにインストールされているトポロジのさまざまなコンポーネントに使用されるあらゆる IP アドレスと VLAN を示します。ASR1K-Virtual は、NTP サーバーと他のコンポーネントへのゲートウェイの両方として機能します。ネットワークは、必要な到達可能性のために、さまざまなコンポーネントの仮想インスタンスに対して定義されます。次のリストには、UCS で定義されているネットワークが含まれています。

- VM_Network : インターネットへのアクセスにラボサブネットの IP アドレスを使用します。トラフィックはタグなしです。
- VM_Internal_Communication : さまざまな VM 間の内部通信にサブネット 192.168.3.x の IP アドレスを使用します。トラフィックはタグなしです。
- ISE_VLAN : 次世代ファイアウォール (NGFW) への通信にサブネット 192.168.2.x の IP アドレスを使用します。トラフィックは VLAN 2 でタグ付けされます。
- Collection_Network : サイバービジョンセンターとサイバービジョンセンサー間の通信にサブネット 192.168.169.x の IP アドレスを使用します。WAN またはインターネット上を流れるとき、トラフィックは IPSec トンネルで暗号化されます。トラフィックは VLAN 169 でタグ付けされます。

表 2 IP アドレス方式

Component	IP Addresses
ジャンプホスト : Windows	192.168.3.106 192.168.2.206 192.168.169.206
Active Directory : Microsoft	192.168.2.204 192.168.3.104
Identity Services Engine	192.168.3.102 192.168.2.202
Cyber Vision Center	192.168.3.113
Firepower Management Console	192.168.3.177
Stealth Watch Management Console	192.168.2.210
Flow Collector	192.168.2.211
ASR 1K - 仮想 - NTP サーバー	192.168.3.108 192.168.2.108 192.168.169.108

Component	IP Addresses
変電所 LAN 管理	192.168.21.0/24 192.168.201.0/24 50.1.0.0/24
変電所 LAN サービス	VRF_SCADA VRF_TSCADA VRF_PLANTLINK VRF_MGMT VRF_GRIDMON VRF_BUSINESS

ライセンス

次の表では、ソリューションに関連する機能を有効にするために必要なハードウェア、ソフトウェア、および対応するライセンスについて説明します。これらのライセンスは、シスコソリューション検証ラボで認定されたものであり、このドキュメントが公開された時点ですべて公開されていました。

表3 ライセンスとコンポーネント

デバイス ロール	ハードウェアプラットフォーム	ライセンス	参照先
変電所ルータ	IR8340	network-advantage IPSEC-HSEC (>250Mbps トラフィック用)	https://www.cisco.com/c/en/us/td/docs/routers/ir8340/software/configuration/b_ir8340_cg_17-8/m_installing_software.html https://www.cisco.com/c/en/us/td/docs/routers/ir8340/software/configuration/b_ir8340_cg_17_7/m-sle-license.html#Cisco_Concept.dita_83d701d7-5072-4685-aadd-4080bb61a1f4
変電所ファイアウォール	ISA3000	Base 以下のライセンスにはサブスクリプションが必要です。 マルウェアの脅威	https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-licenseroadmap.html https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/licensing_the_firepower_system.html
高耐久性スイッチ	IE9300	network-advantage	https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-ie9300-rugged-series/catalyst-ie9300-rugged-series-ds.html#ProductsSpecifications

デバイス ロール	ハードウェア プラットフォーム	ライセンス	参照先
高耐久性スイッチ	IE4000	ipservices	https://www.cisco.com/c/en/us/products/collateral/switches/industrial-ethernet-4000-series-switches/datasheet-c78-733058.html
高耐久性スイッチ	IE5000	ipservices	https://www.cisco.com/c/en/us/products/collateral/switches/industrial-ethernet-5000-series-switches/datasheet-c78-734967.html
高耐久性スイッチ	IE4010	ipservices	https://www.cisco.com/c/en/us/products/collateral/switches/industrial-ethernet-4010-series-switches/datasheet-c78-737279.html?cachemode=refresh
二次変電所ルータ	IR1101	network-advantage	https://www.cisco.com/c/en/us/products/collateral/routers/1101-industrial-integrated-services-router/datasheet-c78-741709.html#Softwarelicensing
高耐久性スイッチ	IE3400	network-advantage	https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-ie3400-rugged-series/datasheet-c78-741760.html
コントロール/ データセンター ファイアウォール	FPR4150	Base 以下のライセンスにはサブスクリプションが必要です。 マルウェアの脅威	https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-licenseroadmap.html https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/licensing_the_firepower_system.html
AAA - ISE	Cisco Unified Computing System で仮想マシンとして実行される Identity Services Engine。	次の機能を備えた従来のライセンス： <ul style="list-style-type: none"> • Base • プラス • Apex • デバイス管理 	https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ise_admin_guide_24/b_ise_admin_guide_24_new_chapter_0110.html

変電所自動化ソリューションの実装

参考資料

Cisco SalesConnect の次のリンクで、SA LAN およびセキュリティソリューション CVD の以前のリリースを参照してください。

- 2.2.1 : Cisco Connected Utilities Substation Security Configuration Guide
<https://www.cisco.com/c/dam/en/us/solutions/collateral/industry-solutions/substation-security.pdf>

- 2.3.2 : Substation Automation Local Area Network and Security Cisco Validated Design
<https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Utilities/SA/2-3-2/CU-2-3-2-DIG/CU-2-3-2-DIG.html>

注記

- この実装ガイドの内容は、主に新しいプラットフォームに適用されます。これは、変電所用のルータとして IR8340 を使用し、産業用イーサネットスイッチとして IE9300 を使用します。
- 変電所ゾーンについて言及されていますが、変電所自動化のリリース、新しいデジタル変電所バージョン 3.0 は、変電所内の 2 つの新製品 IR8340 と IE9300 の導入による ESP ゾーン設計の強化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介して通信するエンドポイント、次のセクションで説明する設計以外のさまざまなフレーバーの HSR および PRP に関連する設計を探している場合は、上記のソリューションドキュメントの古いリリースを参照してください。
- リンクに直接アクセスできない場合は、シスコアカウントチームに資料の提供を依頼してください。貴社は、シスコとの機密保持契約 (NDA) の対象となる必要があります。

WAN とコアの実装

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。次の表は、IR8340 でサポートされているさまざまなモジュールを示しています。これにより、さまざまな接続を使用するオプションが有効になります。

表 4 IR8340 でサポートされるモジュール

製品	説明
IRM-NIM-2T1E1	2 ポート T1/E1 ネットワーク インターフェイス モジュール
IRM-NIM-RS232	RS232 8 ポート シリアル ネットワーク インターフェイス モジュール
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)

製品	説明
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

IR8340 は、送電と配電をサポートする変電所アプリケーションを含む、エネルギー供給インフラストラクチャの通信ニーズをサポートするように設計されています。変電所自動化ネットワーク環境では、IR8340 は ESP ゾーンの端に配置されます。ゾーンベースのファイアウォールや暗号化を含む多くのセキュリティ機能をサポートする IR8340 は、変電所の最も重要な資産を保護するための安全な境界を提供します。IR8340 は、WAN バックホールとして使用できるイーサネット、T1/E1、セルラーインターフェイスをサポートします。このソリューションは、IR8340 をオン ネット変電所ルータまたはオフネット変電所ルータとして位置付けます。

■ オンネット変電所

- ユーティリティ所有の MPLS/IP バックホール
- MPLS PE または CE として機能する変電所ルータ IR8340

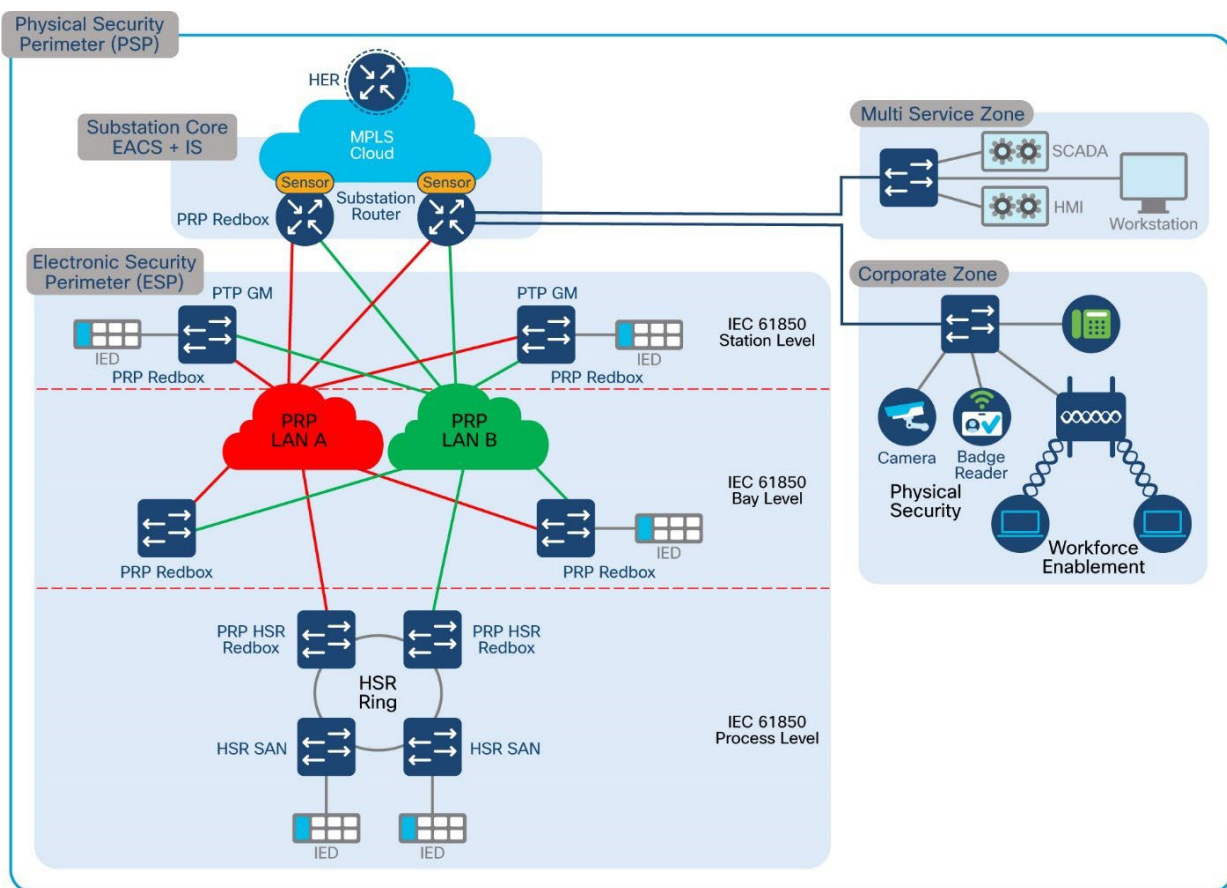
■ オフネット変電所

- 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

変電所ルータ MPLS バックホール

次のトポロジは、このソリューションで変電所ルータとして使用されている Cisco IR8340 を示しています。ルータはプロバイダーエッジとして設定されています。ここでの実装では、MPLS 接続に OSPF と BGP を使用します。SCADA、ネットワーク管理などのさまざまなサービスは、さまざまな SVI でプロビジョニングされます。SVI は、変電所 LAN ネットワークであるレイヤ 2 復元力ネットワークの一部です。要件に従って使用できるさまざまなレジリエンスプロトコルの設定手順については、関連するセクションを参照してください。Cisco IR8340 は、これらのさまざまなサービスへのレイヤ 3 ゲートウェイとして機能します。これらのさまざまなサービスと関連するサブネットは、ノードがプロバイダーエッジルータとして設定されているときに、BGP を使用して MPLS ネットワーク上で交換されます。IR8340 は、カスタマーエッジルータとしても使用でき、OSPF、EIGRP などの関連するルーティングプロトコルを使用してプロバイダーエッジルータに接続して、さまざまなサービスに関連するサブネットを交換できます。

図5 MPLS バックホールを備えた変電所ルータ



コア内のすべてのアグリゲーションデバイスの詳細なエンド ツーエンドの設定は、範囲外であるため、このセクションでは説明しません。このセクションでは、説明した MPLS VPN/L3VPN セットアップを理解するために必要な 2 つの PE デバイスの限定された設定を示します。このセクションでは、MPLS WAN バックホール インターフェイスとして機能するためにイーサネット インターフェイスとシリアル インターフェイスで必要な設定をリストします。

IR8340

WAN インターフェイス イーサネット :

```

!
interface GigabitEthernet0/0/0
description connected to asr903-003
ip flow monitor StealthWatch_Monitor output
ip address 192.168.100.1 255.255.255.0
no ip redirects
ip ospf network point-to-point
load-interval 30
negotiation auto
    
```

```
mpls ip
bfd interval 200 min_rx 200 multiplier 3
lcp max-bundle 2
!
```

変電所ルータ MLPP バックホール :

```
!
controller T1 0/2/0
framing esf
clock source internal
linecode b8zs
cablelength long 0db
channel-group 2 timeslots 1-24
description connected to t1 0/2/2 on asr903
controller T1 0/2/1
framing esf
clock source internal
linecode b8zs
cablelength long 0db
channel-group 1 timeslots 1-24
description connected to T10/2/3 on asr903
!
```

```
!
interface Serial0/2/0:2
no ip address
encapsulation ppp
ppp multilink
ppp multilink group 1
interface Serial0/2/1:1
no ip address
encapsulation ppp
ppp multilink
ppp multilink group 1
!
```

```
!
interface Multilink1
ip address 3.3.3.2 255.255.255.0
zone-member security OUTSIDE
load-interval 30
mpls ip
ppp multilink
ppp multilink group 1
ppp multilink endpoint string mlp1
!
```

OSPF :

```
!  
router ospf 1  
router-id 192.168.199.1  
network 3.3.3.0 0.0.0.255 area 0  
network 192.168.100.0 0.0.0.255 area 0  
network 192.168.199.1 0.0.0.0 area 0  
bfd all-interfaces  
!
```

MPLS グローバル コンフィギュレーション :

```
!  
mpls label protocol ldp  
mpls ldp graceful-restart  
mpls ldp router-id Loopback0  
!
```

BGP の設定 :

```
!  
interface Loopback0  
ip flow monitor StealthWatch_Monitor input  
ip address 192.168.199.1 255.255.255.255  
!  
!  
router bgp 200  
bgp router-id interface Loopback0  
bgp log-neighbor-changes  
neighbor 192.168.201.6 remote-as 200  
neighbor 192.168.201.6 update-source Loopback0  
!  
address-family ipv4  
network 11.9.0.0 mask 255.255.255.0  
network 19.90.0.0 mask 255.255.255.0  
network 20.1.0.0 mask 255.255.255.0  
network 20.2.0.0 mask 255.255.255.0  
network 50.1.0.0 mask 255.255.255.0  
network 177.177.177.0 mask 255.255.255.0  
network 192.168.0.0  
network 192.168.53.0  
network 192.168.54.0  
network 192.168.55.0  
network 192.168.56.0
```

```

network 192.168.57.0
network 192.168.58.0
network 192.168.59.0
network 192.168.60.0
network 192.168.101.0
network 192.168.110.0
network 192.168.155.0
network 192.168.199.2 mask 255.255.255.255
network 192.168.210.0
network 192.168.211.0
neighbor 192.168.201.6 activate
neighbor 192.168.201.6 send-community extended
neighbor 192.168.201.6 next-hop-self
neighbor 192.168.201.6 send-label
exit-address-family
!
address-family vpnv4
neighbor 192.168.201.6 activate
neighbor 192.168.201.6 send-community extended
neighbor 192.168.201.6 next-hop-self
exit-address-family
!
address-family ipv4 vrf VRF_BUSINESS
redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_GRIDMON
redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_MGMT
redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_PLANTLINK
redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_SCADA
redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_TSCADA
redistribute connected
exit-address-family
!

```

HER

WAN インターフェイス イーサネット :

```
!  
interface GigabitEthernet0/0/1  
description connected to asr920-001  
ip address 192.168.69.1 255.255.255.0  
ip ospf network point-to-point  
ip ospf 1 area 0  
load-interval 30  
negotiation auto  
cdp enable  
mpls ip  
bfd interval 200 min_rx 200 multiplier 3  
!
```

OSPF :

```
!  
router ospf 1  
router-id 192.168.201.6  
network 192.168.201.6 0.0.0.0 area 0  
bfd all-interfaces  
mpls ldp sync  
!
```

MPLS グローバル コンフィギュレーション :

```
!  
mpls label protocol ldp  
mpls ldp graceful-restart  
mpls ldp router-id Loopback0  
!
```

BGP の設定 :

```
!  
interface Loopback0  
ip address 192.168.201.6 255.255.255.255  
!  
!  
router bgp 200  
bgp router-id interface Loopback0
```

```
bgp log-neighbor-changes
neighbor 192.168.60.2 remote-as 2001
neighbor 192.168.60.2 shutdown
neighbor 192.168.60.2 ebgp-multihop 255
neighbor 192.168.70.1 remote-as 1001
neighbor 192.168.70.1 ebgp-multihop 255
neighbor 192.168.70.1 update-source Loopback0
neighbor 192.168.111.1 remote-as 200
neighbor 192.168.111.1 ebgp-multihop 255
neighbor 192.168.111.1 update-source Loopback0
neighbor 192.168.113.1 remote-as 200
neighbor 192.168.113.1 ebgp-multihop 255
neighbor 192.168.113.1 update-source Loopback0
neighbor 192.168.198.1 remote-as 200
neighbor 192.168.198.1 update-source Loopback0
neighbor 192.168.198.1 fall-over
neighbor 192.168.198.1 fall-over bfd
neighbor 192.168.199.1 remote-as 200
neighbor 192.168.199.1 update-source Loopback0
neighbor 192.168.199.1 fall-over
neighbor 192.168.199.1 fall-over bfd multi-hop
neighbor 192.168.201.4 remote-as 200
neighbor 192.168.201.4 shutdown
neighbor 192.168.201.4 update-source Loopback0
neighbor 192.168.201.10 remote-as 200
neighbor 192.168.201.10 update-source Loopback0
neighbor 192.168.202.1 remote-as 101
neighbor 192.168.202.1 ebgp-multihop 255
neighbor 192.168.202.1 update-source Loopback0
neighbor 192.168.203.1 remote-as 200
neighbor 192.168.203.1 update-source Loopback0
neighbor 192.168.220.2 remote-as 102
neighbor 192.168.220.2 ebgp-multihop 255
neighbor 192.168.220.2 update-source Loopback0
!
address-family ipv4
bgp additional-paths install
bgp nexthop trigger delay 1
network 30.1.0.0 mask 255.255.255.0
network 30.2.0.0 mask 255.255.255.0
network 140.140.140.0 mask 255.255.255.0
network 141.141.141.0 mask 255.255.255.0
network 192.168.189.0
network 192.168.200.1 mask 255.255.255.255
network 192.168.205.2 mask 255.255.255.255
network 192.168.205.4 mask 255.255.255.255
```



```
network 192.168.220.2 mask 255.255.255.255
network 192.168.223.1 mask 255.255.255.255
redistribute connected
redistribute eigrp 99
neighbor 192.168.60.2 activate
neighbor 192.168.60.2 next-hop-self
neighbor 192.168.60.2 send-label
neighbor 192.168.70.1 activate
neighbor 192.168.70.1 next-hop-self
neighbor 192.168.70.1 send-label
neighbor 192.168.111.1 activate
neighbor 192.168.111.1 send-community extended
neighbor 192.168.111.1 next-hop-self
neighbor 192.168.113.1 activate
neighbor 192.168.113.1 send-community extended
neighbor 192.168.113.1 next-hop-self
neighbor 192.168.198.1 activate
neighbor 192.168.198.1 next-hop-self
neighbor 192.168.198.1 soft-reconfiguration inbound
neighbor 192.168.198.1 send-label
neighbor 192.168.199.1 activate
neighbor 192.168.199.1 weight 40000
neighbor 192.168.199.1 next-hop-self
neighbor 192.168.199.1 soft-reconfiguration inbound
neighbor 192.168.199.1 send-label
neighbor 192.168.201.4 activate
neighbor 192.168.201.4 next-hop-self
neighbor 192.168.201.4 soft-reconfiguration inbound
neighbor 192.168.201.4 send-label
neighbor 192.168.201.10 activate
neighbor 192.168.201.10 next-hop-self
neighbor 192.168.201.10 soft-reconfiguration inbound
neighbor 192.168.201.10 send-label
neighbor 192.168.202.1 activate
neighbor 192.168.202.1 next-hop-self
neighbor 192.168.202.1 soft-reconfiguration inbound
neighbor 192.168.202.1 send-label
neighbor 192.168.203.1 activate
neighbor 192.168.203.1 next-hop-self
neighbor 192.168.203.1 soft-reconfiguration inbound
neighbor 192.168.203.1 send-label
neighbor 192.168.220.2 activate
neighbor 192.168.220.2 next-hop-self
neighbor 192.168.220.2 send-label
exit-address-family
!
```

```
address-family vpnv4
neighbor 192.168.70.1 activate
neighbor 192.168.70.1 send-community extended
neighbor 192.168.70.1 next-hop-self
neighbor 192.168.198.1 activate
neighbor 192.168.198.1 send-community extended
neighbor 192.168.198.1 next-hop-self
neighbor 192.168.199.1 activate
neighbor 192.168.199.1 send-community extended
neighbor 192.168.199.1 next-hop-self
neighbor 192.168.201.4 activate
neighbor 192.168.201.4 send-community extended
neighbor 192.168.201.4 next-hop-self
neighbor 192.168.201.10 activate
neighbor 192.168.201.10 send-community extended
neighbor 192.168.201.10 next-hop-self
exit-address-family
!
address-family ipv4 vrf VRF_BUSINESS
redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_GRIDMON
redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_MGMT
redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_PLANTLINK
redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_SCADA
redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_TSCADA
redistribute connected
exit-address-family
!
```

IR8340 : セルラーバックホール

IR8340 は、統合されたプラグブルモジュールと LTE/5G 機能を備えた外部セルラー ゲートウェイ モジュールの両方をサポートし、これらのユースケースに対応するスループットを向上させます。特定のブランチサイトの有線接続とセルラーエリアのカバー状況に応じて、統合ゲートウェイまたは外部ゲートウェイを選択できます。

ここでは、IR8340 でのセルラー WAN バックホールの実装について説明します。セキュアな FlexVPN トンネルは、緩衝地帯 (DMZ) のヘッドエンドに確立されます。

IR8340 OFF ネット変電所の実装

このセクションでは、Cisco IR8340 変電所ルータでのセルラー バックホール シナリオの実装について説明します。ここで、FlexVPN トンネルは、トンネルインターフェイスを使用してプライマリ セルラー インターフェイス上で確立され、トンネルは HER で設定されたパブリック IP アドレスに接続します。次の設定は、FlexVPN トンネルを確立するために必要です。

IR8340 に適用可能なインターフェイス名を使用する次の設定は、設定が適用されるプラットフォームに適用可能な適切なインターフェイス命名規則を使用して、他のプラットフォームに適用できます。

IR8340 への 4G/5G モジュールの搭載

プラグ可能なモジュールに SIM をインストールし、セルラーインターフェイスを起動する方法の詳細な説明については、次のガイドを参照してください。

<https://www.cisco.com/c/en/us/td/docs/routers/iot-antennas/cellular-pluggable-modules/b-cellular-pluggable-interface-module-configuration-guide.html>

IR8340 SIM のインストール(ゲートウェイにプラグ可能な LTE モジュールがインストールされている必要があります)

IR8340 セルラーインターフェイスの設定例 :

```
!  
!  
interface Cellular0/1/0  
description Cellular Connection to HER Public IP  
mtu 1430  
ip address negotiated
```

```

ip nat outside
ip tcp adjust-mss 1460
dialer in-band
dialer idle-timeout 0
dialer watch-group 1
dialer-group 1
ipv6 enable
pulse-time 1
ip virtual-reassembly
end

!
!
ip route 0.0.0.0 0.0.0.0 Cellular0/4/0
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipv6 permit
!

```

セルラーバックホールを介した Cisco FlexVPN による暗号化トラフィック

IR8340 と HER 間の変電所トラフィックは、FlexVPN トンネルを使用してエンドツーエンドで暗号化できます。トンネルを起動するにはさまざまな方法があり、Flex トンネルの推奨設定は、証明書ベースの認証を設定することです。このソリューションでは、Flex トンネルは PSK (Pre-Share-Key) に基づいて確立されます。

この変電所ソリューションに使用されるサンプル設定を以下に示します。

```

!
!
aaa new-model
aaa authentication login default local
aaa authorization exec default local
aaa authorization network FlexVPN_Author local
aaa session-id common
!
!
crypto ikev2 authorization policy default_no_cert
route set interface
route set access-list FLEX_ACL
crypto ikev2 proposal FlexVPN_IKEv2_Proposal
encryption aes-cbc-256
integrity sha256
group 14
crypto ikev2 policy FLEXVPN_IKEv2_Policy

```

```

proposal FlexVPN_IKEv2_Proposal
crypto ikev2 keyring FLEX_KEYS
peer Substation-HER
address x.x.x.x
pre-shared-key xxxxx
!
crypto ikev2 profile FLEX_CLIENT_PROF
match identity remote address x.x.x.x 255.255.255.255
authentication remote pre-share
authentication local pre-share
keyring local FLEX_KEYS
dpd 30 3 periodic
aaa authorization group psk list FlexVPN_Author default_no_cert
crypto ikev2 fragmentation mtu 1200
crypto ikev2 client flexvpn IKEv2_CLIENT_PROFILE
peer 1 x.x.x.x
client connect Tunnel100
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set esp-aes esp-sha256-
hmac
mode transport
no crypto ipsec profile default
crypto ipsec profile default_No_cert
set transform-set FlexVPN_IPsec_Transform_Set
set pfs group14
set ikev2-profile FLEX_CLIENT_PROF

```

トンネルインターフェイスの設定を以下に示します。

```

interface Tunnel100
ip unnumbered Loopback100
ip mtu 1200
ip nat outside
ip tcp adjust-mss 1160
bfd interval 50 min_rx 50 multiplier 3
tunnel source Cellular 0/4/0
tunnel destination dynamic
tunnel protection ipsec profile default_No_cert
!

```

上記の設定により、HER で FlexVPN トンネルを確立できます。付録セクションの HER 設定を参照してください。

FlexVPN トンネルが確立された後、コントロールセンターと変電所ルータ間のルートは、IKEV2 プレフィックス挿入または BGP/OSPF/EIGRP などの動的ルーティングプロトコルのいずれかを使用して交換できます。

以下のアクセスリストを使用して、IKEv2 プレフィックス インジェクションを使用してルートを確立します。安全なトンネル間の共有ルートを許可するには、暗号 IKEv2 承認ポリシーで同じものを設定します。

```
ip access-list standard FLEX_ACL
10 permit x.x.x.x
11 permit x.x.x.x
12 permit x.x.x.x
```

変電所ルータ マルチリンク バックホール

マルチリンク インターフェイスは、マルチリンク PPP (MLP) バンドルを代表する仮想インターフェイスです。マルチリンク インターフェイスはハンドルされたリンクの設定を調整し、集約リンクのための単一のオブジェクトを提示します。ただし、集約される個々の PPP リンクも設定する必要があります。したがって、複数のシリアルインターフェイスでマルチリンク PPP をイネーブルにするには、最初にマルチリンク インターフェイスを設定し、次に各シリアル インターフェイスを設定して同じマルチリンク インターフェイスに追加する必要があります。

IR8340 ルータには、2つのネットワーク インターフェイス モジュール (NIM) スロット、0/2 と 0/3 があります。T1/E1 ネットワーク インターフェイス モジュール IRM-NIM-2T1E1 は、これらの2つのスロットにインストールできます。これは2ポート チャネライズド データ モジュールであり、ポートごとに T1/E1 の 24/31 チャネルグループをサポートします。各 T1/E1 モジュールには、P0 と P1 の2つのポートがあります。各ポートは、次の設定でコントローラにリンクされています。

- モジュールがスロット 0/2 にある場合、2つのコントローラ 0/2/0 と 0/2/1 があります。
- モジュールがスロット 0/3 にある場合、2つのコントローラ 0/3/0 と 0/3/1 があります。

IR8340 設定

このソリューションでは、OSPF/EIGRP を使用して、マルチリンク インターフェイスが設定され、稼働状態になった後、ルータ間でルートを交換します。

1. カード タイプの設定

T1/E1 ネットワーク インターフェイス モジュールは、カードタイプが設定されるまで動作しません。

```
card type t1 0 2 (if E1 is required, use no card type t1 and use E1)
```

2. T1/E1 コントローラの設定

```
controller T1 0/2/0
framing esf
framing clock source internal
framing linecode b8zs
framing cablelength long 0db
framing channel-group 2 timeslots 1-24
```

同様に、コントローラ T1 0/2/1 を設定します。

3. マルチリンク インターフェイスの設定

```
interface multilink1
ip address x.x.x.x y.y.y.y
ppp multilink
ppp multilink group 1
ppp multilink endpoint string < mlp1>
```

4. シリアルインターフェイス 0/2/0 および 0/2/1 を設定し、インターフェイスをマルチリンク インターフェイスにバンドルします。

```
interface Serial 0/2/0:1
no ip address
encapsulation ppp
ppp multilink
ppp multilink group 1
```

同様に、シリアルインターフェイス 0/2/1:1 を設定し、ppp 設定を適用します。

マルチリンク設定の確認

```
Router#sh ppp multilink interface Multilink 1

Multilink1
Bundle name: mlp1
Remote Endpoint Discriminator: [1] mlp1
Local Endpoint Discriminator: [1] Router
Bundle up for 19:10:19, total bandwidth 3072, load 1/255
Receive buffer limit 24000 bytes, frag timeout 1000 ms
Bundle is Distributed
0/0 fragments/bytes in reassembly list
0 lost fragments, 2 reordered
0/0 discarded fragments/bytes, 0 lost received
0x95D3 received sequence, 0x5B8E sent sequence
Platform Specific Multilink PPP info
NOTE: internal keyword not applicable on this platform
Interleaving: Disabled, Fragmentation: Disabled
```

```
Member links: 2 active, 0 inactive (max 16, min not set)
Se0/2/0:2, since 19:10:18
Se0/2/1:1, since 19:10:17
```

ダイナミックルーティングプロトコルを使用してルータ間でルートを交換します。この場合、EIGRP が使用されます。

```
!  
!  
router eigrp 1  
router-id <loopback/Multilink address>  
network <x.x.x.x y.y.y.y>  
!  
!
```

WAN の冗長性

セルラー/イーサネット経由の WAN バックホール冗長性

変電所ルータでは、HER とのセキュアトンネルが確立されます。セルラー/イーサネット インターフェイスを介してトンネルを確立でき、トンネルは HER で終了します。プライマリ トンネルは、セルラーインターフェイスを介して確立されます。セカンダリ（またはバックアップ）トンネルは、イーサネット インターフェイスを介して確立されます。プライマリ/バックアップトンネルはアクティブ/スタンバイモードで動作します。つまり、次のようになります。

- フェールオーバー：プライマリトンネルに障害が発生すると、セカンダリトンネルがアクティブになります。
- 回復：プライマリトンネルが稼働している場合、セカンダリトンネルは非アクティブ化されます
- 自動フェールオーバー/回復は、EEM の助けを借りて処理されます

バックホールの冗長設定

変電所ルータの冗長設定を以下に示します。

- トンネル 0 はプライマリトンネルです。それはセルラーインターフェイスを介して確立されます
- トンネル 1 はセカンダリトンネルです。イーサネット インターフェイスを介して確立されます。

両方のトンネルは、同じ IPSec トンネル保護モードを使用します。両方のトンネルは、HER で設定された同じパブリック IP アドレスに接続します。以下の設定は、FlexVPN トンネル、トンネル設定、およびインターフェイス設定を確立するために必要です。

IR8340 に適用可能なインターフェイス名を使用する次の設定は、設定が適用されるプラットフォームに適用可能な適切なインターフェイス命名規則を使用して、他のプラットフォームに適用できます。

```
!  
interface Tunnel0  
description Primary IPSec tunnel to HER1.ipg.cisco.com  
ip unnumbered Loopback0  
tunnel source Cellular0/4/0  
tunnel destination <HER_Public_IP_address>  
tunnel protection IPSec profile FlexVPN_IPSec_Profile  
!  
interface Tunnel1  
description IPSec tunnel to HER1.ipg.cisco.com  
ip unnumbered Loopback0  
ipv6 unnumbered Loopback0  
tunnel source GigabitEthernet0/0/0  
tunnel destination <HER_Public_IP_address>  
tunnel protection IPSec profile FlexVPN_IPSec_Profile  
!  
interface Cellular0/4/0  
mtu 1430  
ip address negotiated  
dialer in-band  
dialer idle-timeout 0  
dialer-group 1  
ipv6 enable  
pulse-time 1  
!  
interface GigabitEthernet0/0/0  
ip address dhcp  
!
```

EEM スクリプト：自動フェールオーバー/回復

通常の動作モードでは、変電所ルータはセルラーインターフェイス経由でトンネル 0 を介して安全に HER に接続します。トンネル 0 は、変電所ルータと HER 間の主要な通信モードになります。セルラーインターフェイスを介した接続に障害が発生した場合、ルータと HER 間の通信を復元して保護する必要があります。異なるメディア（イーサネット）を介

したルータと HER 間の接続のこの回復は、動作可能である必要があります。このネットワークのフェールオーバー操作により、パケット損失が最小限に抑えられ、トンネル 1 を介した安全な接続が可能になります。トンネル 0 に障害が発生した場合に負荷を処理するためのトンネル 1 のアクティブ化は、フェールオーバーと呼ばれます。

セルラー経由の接続が回復すると、ルータと HER はトンネル 0 を使用して安全に通信できます。トンネル 1 からトンネル 0 へのこの切り替えは、回復と呼ばれます。

スイッチオーバーが自動になるように、EEM スクリプトは変電所ルータで設定されます。EEM スクリプトは、セルラーインターフェイスの回線プロトコルを追跡します。次の設定がルータに適用されます。

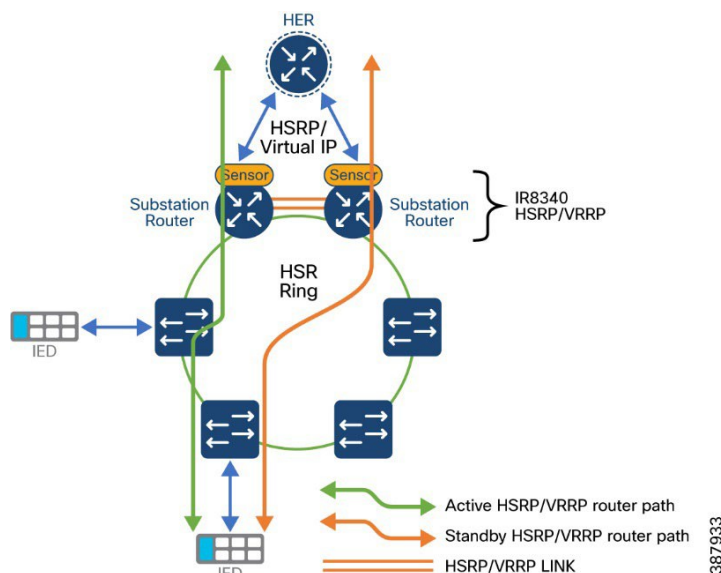
注：リストされている設定は参照のみを目的としています。

```
!  
!  
track 20 interface Cellular0/4/0 line-protocol  
delay down 5  
!  
event manager applet ACTIVATE_SECONDARY  
event track 20 state down  
action 1 cli command "enable"  
action 2 cli command "configure terminal"  
action 3 cli command "ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0/0 200"  
action 4 cli command "interface GigabitEthernet0/0/0 "  
action 5 cli command "no shutdown"  
action 6 cli command "end"  
action 99 syslog msg "NOTE: Cellular down, switching to Ethernet "  
!  
event manager applet DEACTIVATE-SECONDARY  
event track 20 state up  
action 1 cli command "enable"  
action 2 cli command "configure terminal"  
action 3 cli command "interface GigabitEthernet0/0/0 "  
action 4 cli command "shutdown"  
action 5 cli command "end"  
action 99 syslog msg "NOTE: Connectivity Restored on Cellular"  
!  
!
```

注：上記の設定は、他の変電所ルータプラットフォームおよび DA ゲートウェイにも適用できますが、プラットフォーム間のインターフェイス名の変更のみが異なります。

同様に、セルラー/セルラー、セルラー/MLPPP、MLPPP/MPLS の場合、同じ EEM スクリプトを適切に変更して使用できます。

図6 HSRP/VRRP LAN トラフィックフロー



HSRP

HSRP は、デフォルトゲートウェイ IP アドレスが設定された IEEE 802 LAN 上の IP ホストにファーストホップ冗長性を確保することでネットワークの可用性を高めるシスコの標準方式です。HSRP を使用すると、特定のルータの可用性に依存せず IP トラフィックをルーティングできます。また、一連のルータ インターフェイスを組み合わせることで、1 台の仮想ルータ、または LAN 上のホストへのデフォルトゲートウェイのように機能させることができます。ネットワークまたはセグメント上に HSRP を設定すると、仮想 MAC (メディアアクセスコントロール) アドレス、および設定されたルータグループ間で共有される IP アドレスを使用できるようになり HSRP が設定された複数のルータは、仮想ルータの MAC アドレスおよび IP ネットワークアドレスを使用できるようになります。仮想ルータは、実際には存在しません。仮想ルータは、相互にバックアップ機能を提供するように設定されている複数のルータの共通のターゲットを表します。1 台のルータがアクティブなルータとして、もう 1 台のルータがスタンバイルータとして選択されます。スタンバイルータは、指定されたアクティブルータが故障した場合に、グループの MAC アドレスおよび IP アドレスを制御するルータです。

注：HSRPグループ内のルータには、ルーテッドポート、スイッチ仮想インターフェイス(SVI)など、HSRPをサポートする任意のルータインターフェイスを指定できます。

HSRPは、ネットワーク上のホストからのIPトラフィックに冗長性を提供することで、ネットワークの可用性を高めます。アクティブルータは、ルータインターフェイスのグループ内でパケットのルーティングを実行するために選択されたルータです。スタンバイルータは、アクティブルータが故障した場合、または事前に設定した条件が満たされた場合に、ルーティング作業を引き継ぐルータです。

HSRPは、ホストがルータディスカバリプロトコルをサポートしておらず、選択されたルータのリロードや電源故障時に新しいルータに切り替えることができない場合に有効です。HSRPをネットワークセグメントに設定すると、HSRPは仮想MACアドレスとIPアドレスを1つずつ提供します。このアドレスは、HSRPが動作するルータインターフェイスグループ内のルータインターフェイス間で共有できます。プロトコルによってアクティブルータとして選択されたルータは、グループMACアドレス宛てのパケットを受信し、ルーティングします。 n 台のルータでHSRPが稼働している場合、 $n+1$ 個のIPアドレスおよびMACアドレスが割り当てられます。

指定されたアクティブルータの故障をHSRPが検出すると、選択されているスタンバイルータがホットスタンバイグループのMACアドレスおよびIPアドレスの制御を引き継ぎます。この時点で新しいスタンバイルータも選択されます。HSRPが稼働しているデバイスは、マルチキャストUDPベースのhelloパケットを送受信することにより、ルータ障害の検出、アクティブルータおよびスタンバイルータの指定を行います。インターフェイスにHSRPが設定されている場合、そのインターフェイスではインターネット制御メッセージプロトコル(ICMP)のリダイレクトメッセージがデフォルトでディセーブルとなっています。

レイヤ3で動作するスイッチ間で複数のホットスタンバイグループを設定すると、冗長ルータをさらに活用できます。そのためには、インターフェイスに設定するホットスタンバイコマンドグループごとにグループ番号を指定します。たとえば、スイッチ1のインターフェイスをアクティブルータ、スイッチ2のインターフェイスをスタンバイルータとして設定できます。スイッチ2の別のインターフェイスをアクティブルータ、スイッチ1の別のインターフェイスをスタンバイルータとして設定することもできます。

上の図 7 のトポロジは、HSRP 用に設定されたネットワークのセグメントを示しています。各ルータには、仮想ルータの MAC アドレスおよび IP ネットワーク アドレスが設定されています。ルータ A の IP アドレスをネットワーク上のホストに設定する代わりに、デフォルトルータとして仮想ルータの IP アドレスを設定します。IED がパケットをノースバウンドに送信すると、仮想ルータの MAC アドレスに送信されます。何らかの理由により、アクティブルータがパケットの転送を停止すると、スタンバイルータが仮想 IP アドレスおよび仮想 MAC アドレスに回答してアクティブルータとなり、アクティブルータの作業を行います。IED は引き続き仮想ルータの IP アドレスを使用して、ノースバウンド宛てのパケットをアドレス指定します。これにより、ルータはそのパケットを受信してホストに送信します。以前のルータが動作を再開するまで、HSRP により、既存のアクティブなルータは、セグメント上のデータセンターと通信する必要がある IED に中断のないサービスを提供し、ホスト間のパケットを処理する通常の実行し続けることができます。

HSRP の構成

HSRP の詳細な設定については、次のドキュメントを参照してください。

<https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html>

この変電所ソリューションでは、5 つのホットスタンバイ HSRP グループがさまざまな LAN トラフィックの冗長性を確保できるように設定されています。

このソリューションでは、次の VLAN がさまざまな変電所トラフィックに使用されます。

VLAN 751 : IEC61850 GOOSE 用

VLAN 752 : IEC61850 サンプル値用

VLAN 753 : MMS 用

VLAN 754 : SCADA DNP3 トラフィック

VLAN 755 : IPV4 トラフィック用

設定例を以下に示します。

```
!  
interface Vlan751  
ip address x.x.x.1 y.y.y.y
```

```

standby 1 ip x.x.x.100
standby 1 priority 10
standby 1 preempt
standby 1 track 100 decrement 10
!
interface Vlan752
ip address x.x.x.1 y.y.y.y
standby 1 track 100 decrement 10
standby 2 ip x.x.x.100
standby 2 priority 10
standby 2 preempt
!
interface Vlan753
ip address x.x.x.1 y.y.y.y
standby 3 ip x.x.x.10
standby 3 priority 10
standby 3 preempt
standby 3 track 100 decrement 10
standby 4 priority 10
!
interface Vlan754
ip address x.x.x.1 y.y.y.y
standby 4 ip x.x.x.10
standby 4 priority 10
standby 4 preempt
standby 4 track 100 decrement 10
!
interface Vlan755
ip address x.x.x.1 y.y.y.y
standby 5 ip x.x.x.10
standby 5 priority 10
standby 5 preempt
standby 5 track 100 decrement 10

```

ここでは、*track* コマンドを使用してアクティブルータの到達可能性をチェックします。宛先への到達可能性が失敗した場合、プライオリティが減少し、スタンバイがアクティブルータになります。

アクティブルータの WAN インターフェイスから HER への到達可能性の検証が行われます。アクティブルータの WAN インターフェイスから HER への到達可能性が失敗した場合、スタンバイルータはアクティブになり、到達可能性が回復すると、自動フェールオーバーリカバリが実行されます。

WAN インターフェイスの設定

```

interface GigabitEthernet0/0/0
description connected to HER on G0/2/6

```

```
ip address x.x.x.x 255.255.255.0
sbfd interval 150 min_rx 450 multiplier 3
end
```

追跡 CLI 設定は次のとおりです。

```
“track 100 ip route x.x.x.x 255.255.255.255 reachability”
```

他のルータでも同様に、プライオリティが「10」未満の HSRP を有効にして、スタンバイルータにします。

両方の冗長ルータで設定が完了すると、優先順位が最も高いルータがアクティブルータになります。

2つのグループを設定した後に HSRP を確認するには、次を実行します。

```
Router# show standby
VLAN751 - Group 1
Local state is Standby, priority 9, may preempt
Hellotime 3 holdtime 10
Next hello sent in 00:00:02.182
Hot standby IP address is 192.168.x.x configured
Active router is 192.168.x.x expires in 00:00:09
Standby router is local
Standby virtual mac address is 0000.0c07.ac01

VLAN752 - Group 2
Local state is standby, priority 9, may preempt
Hellotime 3 holdtime 10
Next hello sent in 00:00:02.262
Hot standby IP address is 192.168.x.x configured
Active router is 192.168.x.x expires in 00:00:05
Standby router is local
Standby virtual mac address is 0000.0c07.ac64
```

HSRP を設定するためのベストプラクティス

HSRP を調整する際に考慮する必要がある重要な要素の 1 つは、そのプリエンプティブな動作です。プリエンプションにより、プライマリ HSRP ピアは、障害またはメンテナンスイベントの後にオンラインに戻ったときに、プライマリロールを再び引き受けます。

STP/RSTP ルートは特定のサブネットまたは VLAN の HSRP プライマリと同じデバイスである必要があるため、プリエンプションは望ましい動作です。HSRP と STP/RSTP が同期していない場合、ディストリビューション スイッチ間の相互接続はトランジットリンクになり、トラフィックはマルチホップ L2 パスを使用してデフォルトゲートウェイに到達します。

HSRP プリエンプションでは、スイッチの起動時間とネットワークの残りの部分への接続を認識する必要があります。プライマリスイッチがコアへの L3 接続を確立する前に、HSRP ネイバー関係が形成され、プリエンプションが発生する可能性があります。この場合、完全な接続が確立されるまでトラフィックがドロップされる可能性があります。

推奨されるベストプラクティスは、システムブート時間を測定し、HSRP preempt delay ステートメントをこの値より 50% 大きい値に設定することです。これにより、HSRP プリエンプションの発生が許可される前に、HSRP プライマリ ディストリビューション ノードがネットワークのすべての部分への完全な接続を確立することが保証されます。

VRRP

仮想ルータ冗長プロトコル (VRRP) は、LAN 上の VRRP ルータに対し、1 台または複数台の仮想ルータの役割をダイナミックに割り当てる選択プロトコルです。この場合、マルチアクセス リンク上にある何台かのルータが同じ仮想 IP アドレスを使用できるようにします。VRRP ルータは、LAN に接続された 1 つ以上の他のルータと連係して VRRP プロトコルを実行するように設定されます。VRRP 設定では、1 台のルータが仮想マスター ルータとして選定され、他のルータは仮想マスター ルータが機能を停止した場合のバックアップとして動作します。

VRRP の制限事項

- スイッチは HSRP または VRRP のいずれかをサポートしますが、両方をサポートしません。スイッチは HSRP と VRRP の両方が設定されたスタックに参加できません。
- スイッチの VRRP 実装は、テキストベースの認証だけをサポートします。
- IPv4 および IPv6 グループに対する VRRP を同時にイネーブルにはできません。

以下の VRRP の詳細設定とトラブルシューティング手順を参照してください。

https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-0/addr_serv/configuration/guide/ic40_crs1book_chapter10.html#:~:text=VRRP%20is%20an%20IP%20routing,router%20as%20their%20default%20gateway.

設定例を以下に示します。

```
!  
interface Vlan751  
ip address x.x.x.1 255.255.255.0  
vrrp 1 ip x.x.x.x  
vrrp 1 timers advertise msec 150  
vrrp 1 track 1 decrement 20  
end  
  
interface Vlan752  
ip address x.x.x.1 255.255.255.0  
vrrp 1 ip x.x.x.x  
vrrp 1 timers advertise msec 150  
vrrp 1 track 1 decrement 20  
end  
!
```

VRRP を確認するには

```
Router#sh vrrp all  
Vlan751 - Group 1  
State is Master  
Virtual IP address is 192.168.x.100  
Virtual MAC address is 0000.5e00.0101  
Advertisement interval is 0.150 sec  
Preemption enabled  
Priority is 100  
Master Router is 192.168.x.1 (local), priority is 100  
Master Advertisement interval is 0.150 sec  
Master Down interval is 1.059 sec  
FLAGS: 1/1  
  
Vlan752 - Group 2  
State is Master  
Virtual IP address is 192.168.x.100  
Virtual MAC address is 0000.5e00.0102  
Advertisement interval is 0.150 sec  
Preemption enabled  
Priority is 100
```

Master Router is 192.168.x.1 (local), priority is 100
Master Advertisement interval is 0.150 sec
Master Down interval is 1.059 sec
FLAGS: 1/1

ベストプラクティスと制限事項

- VRRP は、マルチアクセス、マルチキャスト、またはブロードキャスト対応イーサネット LAN で使用するために設計されています。VRRP は既存のダイナミック プロトコルの代替にはなりません。
- VRRP は、イーサネット、ファストイーサネット、ブリッジグループ仮想インターフェイス (BVI) 、およびギガビットイーサネットインターフェイス、マルチプロトコルラベルスイッチング (MPLS) バーチャルプライベートネットワーク (VPN) 、VRF を認識する MPLS VPN、および VLAN 上でサポートされます。
- BVI インターフェイスの初期化に関連して転送遅延が発生するため、VRRP アドバタイズタイマーの時間は BVI インターフェイスでの転送遅延時間と同じにするか、または長く設定する必要があります。このように設定することで、最近初期化された BVI インターフェイス上にある VRRP ルータが無条件にマスターロールを引き継ぐことがなくなります。BVI インターフェイスでの転送遅延を設定するには、bridge forward-time コマンドを使用します。vrrp timers advertise コマンドを使用して、VRRP アドバタイズ時間を設定します

LAN の実装

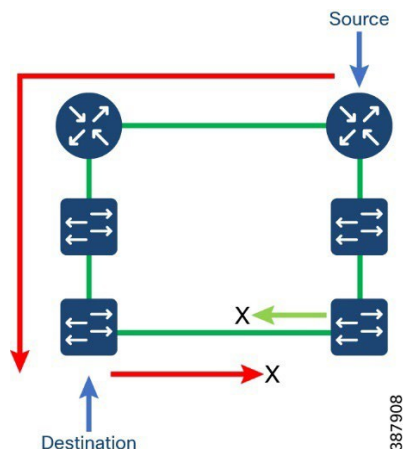
レガシープロトコルの実装

RPVST

Rapid PVST+ は、VLAN ごとに実装されている IEEE 802.1w (RSTP) 規格です。(手作業で STP をディセーブルにしていない場合、) STP の 1 つのインスタンスは、設定されている各 VLAN で実行されます。VLAN 上の各 Rapid PVST+ インスタンスには、1 つのルートスイッチがあります。Rapid PVST+ の実行中には、VLAN ベースで STP をイネーブルまたはディセーブルにできます。Rapid PVST+ は、デフォルト VLAN (VLAN1) と、

ソフトウェアで新たに作成された新しい VLAN でデフォルトでイネーブルになります。
Rapid PVST+ はレガシー IEEE 802.1D STP が稼働するデバイスと相互運用されます。

図 7 Rapid Per VLAN Spanning Tree



VLAN ごとに Rapid PVST+ を有効にするには、以下の手順を実行します。

設定手順

注 必要な VLAN を識別し、RPVST リングに参加しているすべてのスイッチでそれらを設定します。

```
!  
vlan 1,201,501,1501  
no shut  
end  
!
```

注 RPVST リングのインターフェイスを識別し、識別された VLAN を許可するトランクポートを設定します。

```
!  
interface gigabitEthernet 0/1/5  
switchport mode trunk  
switchport trunk allowed vlan 1,201,501,1501  
end  
!
```

注 対象のデバイスで RPVST を有効にするには、以下を設定します。

```
!  
spanning-tree mode rapid-pvst  
spanning-tree vlan-range  
!
```

スパニングツリートポロジに参加しているすべての関連デバイスで、上記の手順を繰り返します。

Rapid PVST+ の設定情報を表示するには、次のいずれかの処理を実行します。

確認

```
!  
spanning-tree mode rapid-pvst  
spanning-tree extend system-id  
spanning-tree portfast trunk  
spanning-tree portfast trunk  
!
```

```
switch# show spanning-tree [options]
```

次の例では、VLAN 1 のスパニングツリーの詳細を表示します。

```
Router#show spanning-tree vlan 1
```

```
G0:VLAN0001  
Spanning tree enabled protocol rstp  
Root ID Priority 32769  
Address 0029.c23c.5bc0  
Cost 4  
Port 14 (GigabitEthernet0/1/4)  
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  
  
Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)  
Address 14a2.a093.fa71  
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  
Aging Time 300 sec
```

```
Interface Role Sts Cost Prio.Nbr Type  
-----  
Gi0/1/2 Desg FWD 4 128.12 P2p  
Gi0/1/4 Root FWD 4 128.14 P2p
```

<i>Gi0/1/8</i>	<i>Desg FWD 4</i>	<i>128.18 P2p Edge</i>
<i>Ap0/1/1</i>	<i>Desg FWD 2</i>	<i>128.22 P2p</i>

ベスト プラクティス

- コアスイッチをルートブリッジにすることを推奨します。バックアップルートブリッジを選択することもお勧めします。デュアル冗長コアスイッチがある場合、1つはルートブリッジで、もう1つはバックアップになります。プライマリルートブリッジのブリッジプライオリティを最適な値 (4096) に設定し、バックアップルートブリッジを次に最適な値 (8192) に設定します。
- エンドデバイスに接続するすべてのポートでコマンド「spanning-tree portfast」を設定することをお勧めします。

REP

Resilient Ethernet Protocol (REP) はシスコ独自のプロトコルで、スパニングツリー プロトコル (STP) に代わるプロトコルとして、ネットワークループの制御、リンク障害の処理、コンバージェンス時間の改善を実現します。REP は、セグメントに接続されているポートのグループを制御することで、セグメントがブリッジングループを作成するのを防ぎ、セグメント内のリンク障害に応答します。

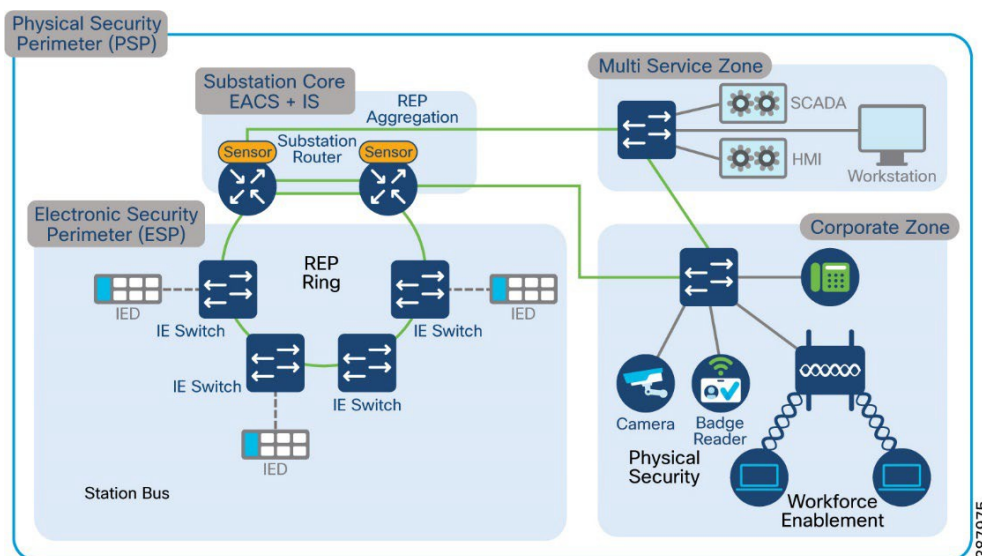
次のトポロジは、ステーションバスがレジリエンスプロトコルとして REP を使用して接続され、CORP とマルチサービスゾーンの両方も REP を使用して接続されているシナリオを示しています。IR8340 Cisco 変電所ルータは、REP リングの両方を集約し、レイヤ3 ゲートウェイとして機能します。NTP は、REP リング上のタイミグプロトコルとして使用されます。このトポロジでは、トランクポートを使用して複数の VLAN を作成できるため、さまざまなサービスを作成したり、さまざまなデバイスを接続したり、VLAN への関連トラフィックを制限したりするオプションが提供されます。HSRP や VRRP などのレイヤ3 ゲートウェイ冗長プロトコルは、IR8340 で有効にできます。HSRP または VRRP の設定手順については、この実装ガイドの各セクションを参照してください。

次の REP 機能は IR8340 ではサポートされていません。

- REP Fast
- REP デイゼロ
- REP セグメント ID 自動検出
- REP がネゴシエートされました

注: PTP over REP は、このソリューションでテストされた IOS-XE バージョンの IR8340 および IE9300 ではサポートされていません。

図8 異なるゾーンに複数の REP リングを備えた変電所ルータ



設定手順

REP インターフェイスを設定する手順は次のとおりです。

1. 必要な VLAN を識別し、REP リングに参加しているすべてのスイッチでそれらを設定します。

!

```
vlan 1,201,501,1501
no shut
end
!
```

2. REP リングのインターフェイスを識別し、識別された VLAN を許可するトランクポートを設定します。

```
!
interface gigabitEthernet 0/1/5
switchport mode trunk
switchport trunk allowed vlan 1,201,501,1501
!
```

3. REP リングを形成するために、参加しているすべてのスイッチの識別されたインターフェイスで REP を有効にします。

```
!  
inte gigabitEthernet 0/1/5  
rep seg 1 <edge> <preferred> rep seg 1  
end  
!
```

注：各セグメントに1つのプライマリエッジポートを含めて、2つのエッジポートを設定する必要があります。

- (オプション) **edge**：エッジポートとしてポートを設定します。**primary** キーワードなしで **edge** を入力すると、ポートがセカンダリエッジポートとして設定されます。各セグメントにあるエッジポートは2つだけです。
- (オプション) **primary**：プライマリエッジポート (VLAN ロードバランシングを設定できるポート) としてポートを設定します。
- (オプション) **no-neighbor**：エッジポートとして外部 REP ネイバーを使用せずにポートを設定します。そのポートはエッジポートのすべての特性を継承するため、他のエッジポートと同じように設定できます。

注：各セグメントにあるプライマリエッジポートは1つだけですが、2つの異なるスイッチにエッジポートを設定して **primary** キーワードを両方のスイッチに入力しても、その設定は許容されます。ただし、REP ではセグメント プライマリエッジポートとして1つのポートだけが選択されます。**show rep topology** 特権 EXEC コマンドを入力すると、セグメントのプライマリエッジポートを特定することができます。

- (オプション) **preferred**：ポートが優先代替ポートであるか、VLAN ロードバランシングの優先ポートであるかを示します。

注：ポートを優先に設定しても、代替ポートになるとは限りません。同等に可能性のあるポートよりやや可能性が高くなるだけです。通常、前に障害が発生したポートが、代替ポートとなります。

確認

リングに参加しているすべてのスイッチとスイッチのそれぞれのインターフェイスで REP を設定した後、次のコマンドを使用して確認できます。

```
show rep topology segment <segment id>
```

```

Router#show rep to seg 1
REP Segment 1
BridgeName          PortName  Edge Role
-----
Router              Gi0/1/6  Pri  Alt
RIO-SA              Gi1/1    Open
RIO-SA              Gi1/2    Open
IE2KU-REP001        Gi0/1    Open
IE2KU-REP001        Gi0/2    Open
IE2KU-REP002        Gi0/2    Open
IE2KU-REP002        Gi0/1    Open
clarke-003-REP      Gi1/0/25 Open
clarke-003-REP      Gi1/0/26 Open
sumatra-PP-1        Gi0/1/5  Open
sumatra-PP-1        Gi0/1/7  Open
Router              Gi0/1/5  Sec  Open

```

Router#

REP を監視するために使用できる他の同様のコマンドは「**show interface <interface> rep detail**」です。

特定のインターフェイスまたはすべてのインターフェイスの REP の設定とステータスを表示します。

- (オプション) detail : インターフェイス固有の REP 情報を表示します。

```

Router#show inte gigabitEthernet 0/1/5 rep detail
GigabitEthernet0/1/5  REP enabled
Segment-id: 1 (Edge)
PortID: 000F14A2A093F9F0
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 001014A2A093F9F0E856
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
REP-ZTP Status: Not supported
REP Segment Id Auto Discovery Status: Not supported
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
LSL Ageout Retries: 5
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 837, tx: 771
HFL PDU rx: 1, tx: 1
BPA TLV rx: 558, tx: 161

```


BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 6, tx: 6
EPA-COMMAND TLV rx: 1, tx: 1
EPA-INFO TLV rx: 99, tx: 137

“show rep topology detail”

セグメント内のプライマリおよびセカンダリ エッジ ポートを含む、1 セグメントまたは全セグメントの REP トポロジ情報を表示します。

- (オプション) archive : 最後の安定したトポロジを表示します。

注 : アーカイブのトポロジは、スイッチをリロードすると保持されません。

- (任意) detail : 詳細なアーカイブ情報を表示します。

ベスト プラクティス

ロード バランシング時のリンク障害や VLAN ブロッキングの通知のメッセージをソフトウェアでリレーすることによって発生する遅延を回避するために、REP は HFL で通常のマルチキャスト アドレスにパケットをフラッディングします。これらのメッセージは REP セグメントだけではなくネットワーク全体にフラッディングされます。ドメイン全体の管理 VLAN を設定することで、これらのメッセージのフラッディングを制御することができます。

REP 管理 VLAN を設定する場合、次の注意事項に従ってください。

- 管理 VLAN を設定しない場合、デフォルトは VLAN 1 です。
- スイッチとセグメントで 1 つの管理 VLAN だけが可能です。ただし、これはソフトウェアによって強制的に設定されません。
- 管理 VLAN は RSPAN VLAN になりません。

REP 管理 VLAN を設定するには、次の手順に従います。

```
Switch# configure terminal  
Switch (config)# rep admin vlan <vlan id>  
Switch (config-if)# end
```

ロスレスプロトコルの実装

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。

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。

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した場合、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。

PRP チャンネルまたはチャンネルグループは、2つのギガビット イーサネット インターフェイス (アクセス、トランクまたはルーテッド) を単一のリンクに集約する論理インターフェイスです。チャンネルグループでは、番号の小さいギガビット イーサネット メンバーポートがプライマリポートであり、LAN_A に接続します。番号の大きい方のポートがセカンダリポートで、LAN_B に接続します。これらのメンバーポートの少なくとも1つが稼働し続け、トラフィックを送信する場合、PRP チャンネルは稼働したままになります。両方のメンバーポートがダウンした場合、チャンネルもダウンします。

次の表に、さまざまな PRP モードとプラットフォームサポートを示します。

表5 PRP モードとサポートされるプラットフォーム

PRP モード	プラットフォーム
PRP Redbox	IR8340、IE9300、IE5000、IE4000、IE4010、IE3400
PRP HSR Redbox	IE4000

PRP を介した PTP	IE5000、IE3400、IE4010
--------------	----------------------

次のセクションでは、IR8340 の PRP に関する詳細のみをリストします。他の PRP モードの詳細については、前のリファレンスセクションにリストされている変電所自動化ソリューションガイドの以前のバージョンを参照してください。

Cisco IR8340 でサポートされる PRP チャネルグループの合計数は、ルータごとに 2 であり、各グループで利用できるインターフェイスは固定されています。

- PRP チャネルグループ 1 は常に LAN_A には Gi0/1/4 を使用し、LAN_B には Gi0/1/5 を使用します。
- PRP チャネルグループ 2 は、常に LAN_A に Gi0/1/6 を使用し、LAN_B に Gi0/1/7 を使用します。

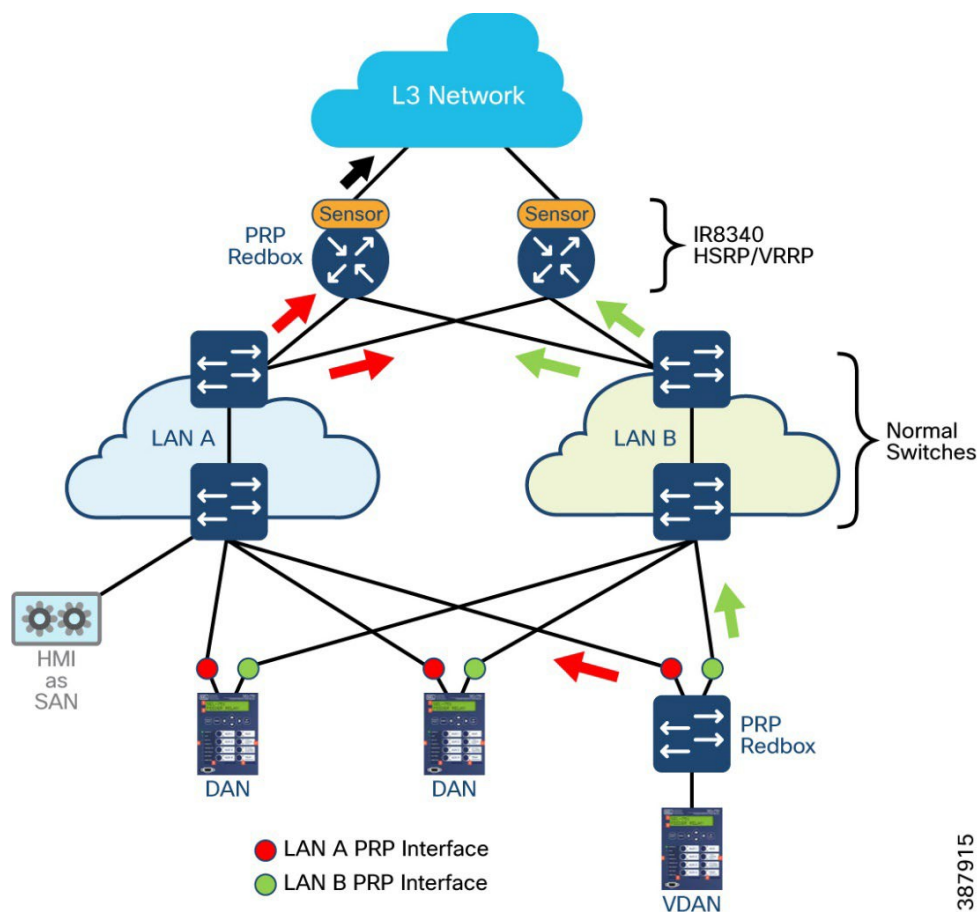
Cisco IE9300 でサポートされる PRP チャネルグループの総数、つまり IE-9320-26S2C-A と IE-9320-26S2C-E は、スイッチごとに 2 つであり、各グループで使用できるインターフェイスは固定されています。

- PRP チャネルグループ 1 は、常に LAN_A に Gi1/0/21 を使用し、LAN_B に Gi1/0/22 を使用します
- PRP チャネルグループ 2 は、常に LAN_A に Gi1/0/23 を使用し、LAN_B に Gi1/0/24 を使用します。

次のトポロジは、PRP Redbox として設定された 2 つの IR8340 ルータを示しています。IR8340 ルータは、PRP、LAN A、および LAN B の LAN セグメントに接続されているデバイスの L3 ゲートウェイとしても機能します。PRP の LAN A および LAN B は RSTP が有効になっています。また、REP、STP などの他のレジリエンスプロトコルを使用して設定することもできます。レジリエンスプロトコルの設定については、このガイドのそれぞれのセクションを参照してください。この実装ガイドの検証に使用された IOS-XE バージョンでは、IR8340 が PRP 上の PTP をサポートしていないため、NTP は PRP LAN リンク上のタイミングプロトコルとして使用されます。このトポロジでは、トランクポートを使用して複数の VLAN を作成できるため、さまざまなサービスを作成したり、さまざまなデバイスを接続したり、VLAN への関連トラフィックを制限したりするオプションが提供されます。HSRP や VRRP などのレイヤ 3 ゲートウェイ冗長プロトコルは、IR8340 で有効にできます。HSRP または VRRP の設定手順については、この実装ガイドの各セクションを参照してください。

次のセクションでは、PRP Redbox として設定された Cisco IR8340 で PRP チャンネルを有効にする手順を示します。同じ手順に従って、Cisco IE9300 スイッチで PRP チャンネルを有効にすることができます。

図9 L3 ゲートウェイの冗長性を備えた PRP Redbox



設定手順

1. 必要な VLAN を特定し、PRP トポロジに参加しているすべてのスイッチでそれらを設定し、設定された VLAN のシャットダウンを解除します。

vlan 1-2507,2509-4094

2. PRP チャンネルのインターフェイスを識別し、識別された VLAN を許可するトランクポートを設定します。インターフェイス GigabitEthernet 0/1/4 および 0/1/5 は、このサンプルトポロジで使用され、設定を保存します。

```
interface gigabitEthernet 0/1/5
switchport mode trunk
switchport trunk allowed vlan 1-2507,2509-4094
end
```

3. PRP チャンネルとそれぞれの VLAN を設定します。

```
interface prp-channel 1
switchport
switchport trunk allowed vlan 1-2507,2509-4094
switchport mode trunk
end
```

4. PRP チャンネルを PRP メンバーインターフェイスに接続します。両方のメンバーインターフェイスが設定されていることを確認し、設定を保存します。

```
interface GigabitEthernet0/1/4
prp-channel-group 1
end
```

確認

参加しているルータまたはスイッチで PRP を設定した後、確認のために次のコマンドを使用します。

```
Router#show prp channel summary
Flags: D - down      P - bundled in prp-channel
       R - Layer3    S - Layer2
       U - in use
```

```
Number of channel-groups in use: 1
Group PRP-channel Ports
-----+-----+-----
1   PR1(SU)   Gi0/1/4(P), Gi0/1/5(P)
```

```
Router#show prp channel 1 detail
PRP-channel: PR1
-----
Layer type = L2
Ports: 2   Maxports = 2
Port state = prp-channel is Inuse
Protocol = Enabled
Ports in the group:
1) Port: Gi0/1/4
   Logical slot/port = 0/4   Port state = Inuse
```

```
Protocol = Enabled
2) Port: Gi0/1/5
Logical slot/port = 0/5 Port state = Inuse
Protocol = Enabled
```

```
Router#
Router#show prp channel 1 status
PRP-channel: PR1
-----
Port state = prp-channel is Inuse
Protocol = Enabled
sumatra-pp-2#
```

次のコマンドを使用して、PRP に関連するさまざまな統計を確認します。

```
Router#show prp statistics ?
egressPacketStatistics Egress packet statistics
ingressPacketStatistics Ingress packet statistics
nodeTableStatistics Node table statistics
pauseFrameStatistics Pause frame statistics
ptpPacketStatistics PTP packet statistics

Router#show prp statistics ingressPacketStatistics
PRP channel-group 1 INGRESS STATS:
ingress pkt lan a: 113060
ingress pkt lan b: 145488
ingress crc lan a: 0
ingress crc lan b: 0
ingress danp pkt acpt: 13168
ingress danp pkt dscrd: 11625
ingress supfrm rcv a: 78692
ingress supfrm rcv b: 86607
ingress over pkt a: 0
ingress over pkt b: 0
ingress pri over pkt a: 0
ingress pri over pkt b: 0
ingress oversize pkt a: 0
ingress oversize pkt b: 0
ingress byte lan a: 9408873
ingress byte lan b: 11577700
ingress wrong lan id a: 0
ingress wrong lan id b: 88005
ingress warning lan a: 0
ingress warning lan b: 0
ingress warning count lan a: 0
ingress warning count lan b: 2
```

ingress unique count a: 1456
ingress unique count b: 0
ingress duplicate count a: 7682
ingress duplicate count b: 3943
ingress multiple count a: 7682
ingress multiple count b: 3943

PRP channel-group 2 INGRESS STATS:

ingress pkt lan a: 0
ingress pkt lan b: 0
ingress crc lan a: 0
ingress crc lan b: 0
ingress danp pkt acpt: 0
ingress danp pkt dscrd: 0
ingress supfrm rcv a: 0
ingress supfrm rcv b: 0
ingress over pkt a: 0
ingress over pkt b: 0
ingress pri over pkt a: 0
ingress pri over pkt b: 0
ingress oversize pkt a: 0
ingress oversize pkt b: 0
ingress byte lan a: 0
ingress byte lan b: 0
ingress wrong lan id a: 0
ingress wrong lan id b: 0
ingress warning lan a: 0
ingress warning lan b: 0
ingress warning count lan a: 0
ingress warning count lan b: 0
ingress unique count a: 0
ingress unique count b: 0
ingress duplicate count a: 0
ingress duplicate count b: 0
ingress multiple count a: 0
ingress multiple count b: 0

Router#

Router#show prp statistics egressPacketStatistics

PRP channel-group 1 EGRESS STATS:

duplicate packet: 87990
supervision frame sent: 13411
packet sent on lan a: 111248
packet sent on lan b: 111270
byte sent on lan a: 7975915
byte sent on lan b: 7977924
egress packet receive from switch: 97949

```
overrun pkt: 0
overrun pkt drop: 0
PRP channel-group 2 EGRESS STATS:
duplicate packet: 0
supervision frame sent: 0
packet sent on lan a: 0
packet sent on lan b: 0
byte sent on lan a: 0
byte sent on lan b: 0
egress packet receive from switch: 0
overrun pkt: 0
overrun pkt drop: 0
```

Router#

次のコマンドを使用して、PRP 制御情報と監視フレーム情報を表示します。

```
Router#show prp control ?
VdanTableInfo          VDAN table information
ptpLanOption           PTP LAN option
ptpProfile             PTP profile
supervisionFrameLifeCheckInterval Supervision frame life check interval
supervisionFrameOption Supervision frame option
supervisionFrameRedboxMacaddress Supervision Redbox MacAddress
supervisionFrameTime   Supervision frame time
```

Router#

ベスト プラクティス

- prp-channel インターフェイスで bpdudfilter を設定します。スパニングツリー BPDU フィルタは、すべての入力および出力 BPDU トラフィックをドロップします。このコマンドは、ネットワーク内に独立したスパニングツリードメイン (ゾーン) を作成するために必要です。

spanning-tree bpdudfilter enable

- LAN-A/B ポートを設定して、FORWARD モードにすばやく移行します。この項はオプションですが、強く推奨されます。これにより、PRP RedBox と LAN-A および LAN-B スイッチエッジポートでのスパニング ツリー コンバージェンス時間が改善されます。また、RedBox PRP インターフェイスに直接接続されている LAN_A/LAN_B ポートでこのコマンドを設定することを強くお勧めします。

spanning-tree portfast edge trunk

```
!
interface prp-channel 1
spanning-tree bpdupfilter enable
spanning-tree portfast trunk
!
```

HSR

国際規格 IEC 62439-3-2016 の第 5 節では、HSR、高可用性シームレス冗長性について説明しています。HSR は PRP と同じ結果を達成しますが、リングトポロジで動作するように設計されています。任意のトポロジの並列独立ネットワーク 2 つ (LAN-A と LAN-B) の代わりに、HSR は反対方向のトラフィックを持つリングを定義します。ポート A はリング A でトラフィックを反時計回りに送信し、ポート B はリング B でトラフィックを時計回りに送信します。パケット形式は PRP とは異なり、RCT の代わりに HSR は、L2 MacSa アドレスまたは VLAN タグフィールドの後に HSR Ethertype を持つ HSR ヘッダーを導入します。

HSR リングに接続するノードは DANH と呼ばれます。PRP と同様に、SAN は RedBox のサービスを介して HSR リングに接続されます。

HSR リング内の各ノードは、一方のポートから受信したフレームを HSR ペアの他方のポートに転送します。ノードが一方のポートで受信したフレームを他方のポートに転送しない条件が 3 つあります。

- 受信したフレームは、元のノードにリングを回って戻ってきました。
- 宛先 MAC アドレスが受信ノードの上流に属するユニキャストフレーム。
- ノードはすでに同じフレームを同じ方向に送信していました。このルールは、無限ループでフレームがリング内でスピンするのを防ぐためのものです。

HSR のプラットフォームと機能のサポートを次の表に示します。詳細な設定については、「Substation Automation Local Area Network and Security Cisco Validated Design」を参照してください：

<https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Utilities/SA/2-3-2/CU-2-3-2-DIG/CU-2-3-2-DIG.html>

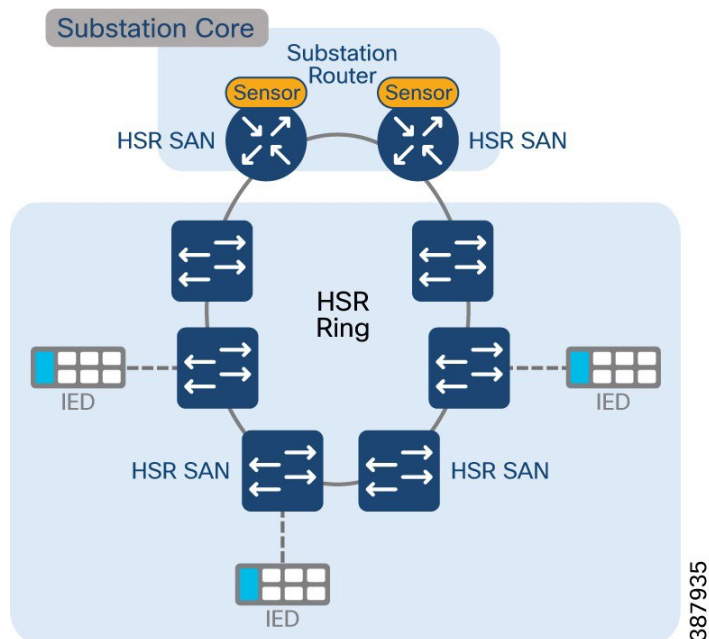
表6 HSR モードとサポートされるプラットフォーム

機能	プラットフォーム	Cisco IOS ソフトウェア
HSR-SAN (単一接続ノード)	IE4000/IE5000/IE4010 IR8340	15.2(8)E1 17.9.1
HSR-PRP Redbox	IE4000	15.2(8)E1
HSR-Quadbox	IE4000	15.2(8)E1

IR8340 でサポートされる HSR リングの総数は、ルータごとに 1 リングであり、各グループに使用できるインターフェイスは次のとおりです。

- HSR リンググループ 1 は、LAN_A には Gi0/1/4 または Gi0/1/6 を使用し、LAN_B には Gi0/1/5 または Gi0/1/7 を使用します。

図10 HSR トポロジ



設定手順

1. 必要な VLAN を特定し、HSR トポロジに参加しているすべてのスイッチでそれらを構成し、グローバル コンフィギュレーション モードですべての VLAN のシャットダウンを解除します。

```
vlan 1-2507,2509-4094
```

2. HSR リングのインターフェイスを識別し、識別された VLAN を許可するトランクポートを設定します。インターフェイス GigabitEthernet 0/1/6 および 0/1/7 は、このサンプルトポロジで使用され、設定を保存します

```
interface gigabitEthernet 0/1/6
switchport mode trunk
switchport trunk allowed vlan 1-2507,2509-4094
end
```

3. HSR リングとそれぞれの VLAN を設定し、インターフェイス hsr-ring を解除します

```
interface hsr-ring 1
switchport
switchport trunk allowed vlan 1-2507,2509-4094
switchport mode trunk
```

4. HSR リングを HSR メンバーインターフェイスに接続します。両方のメンバーインターフェイスが設定されていることを確認し、設定を保存します

```
interface GigabitEthernet0/1/6
hsr-ring 1
```

確認

参加しているルータまたはスイッチで HSR を設定した後、次のコマンドを検証に使用できます。

```
Router#sh hsr ring 1 detail
HSR-ring: HS1
-----
Layer type = L2
Operation Mode = mode-H
Ports: 2 Maxports = 2
Port state = hsr-ring is In use
Protocol = Enabled Redbox Mode = hsr-san
```

Ports in the ring:

- 1) Port: Gi0/1/6
Logical slot/port = 0/6 Port state = In use
Protocol = Enabled
- 2) Port: Gi0/1/7
Logical slot/port = 0/7 Port state = In use
Protocol = Enabled

Ring Parameters:

Redbox MacAddr: 38fd.f85b.c54e
Node Forget Time: 60000 ms
Node Reboot Interval: 500 ms
Entry Forget Time: 400 ms
Proxy Node Forget Time: 60000 ms
Supervision Frame COS option: 0
Supervision Frame CFI option: 0
Supervision Frame VLAN Tag option: Disabled
Supervision Frame MacDa: 0x00
Supervision Frame VLAN id: 0
Supervision Frame Time: 3 ms
Life Check Interval: 1600 ms
Pause Time: 25 ms
fpgamode-DualUplinkEnhancement: Enabled

Router# **sh hsr ring status**

HSR-ring: HSI

Port state = hsr-ring is In use
Protocol = Enabled Redbox Mode = hsr-san

Router# **sh hsr ring 1 summary**

Flags: D - down H - bundled in HSR-ring
R - Layer3 S - Layer2
U - in use s - suspended

Number of hsr-rings in use: 1

Group HSR-ring Ports

-----+-----+-----
1 HSI(SU) Gi0/1/6(H), Gi0/1/7(H)

次のコマンドを使用して、HSR リングに関連するさまざまな統計を確認します。

Router#**sh hsr statistics egressPacketStatistics**

duplicate packets: 7477
supervision frames: 1140

```
packets sent on port A: 1239544
packets sent on port B: 1152183
byte sent on port a: 160600821
byte sent on port b: 149151641
```

```
Router#sh hsr statistics ingressPacketStatistics
HSR ring 1 INGRESS STATS:
  ingress pkt port A: 1193537
  ingress pkt port B: 1281119
  ingress crc port A: 0
  ingress crc port B: 0
  ingress danh pkt portAcpt: 1269191
  ingress danh pkt dscrd: 1181133
  ingress supfrm rcv port A: 4032
  ingress supfrm rcv port B: 4628
  ingress overrun pkt port A: 0
  ingress overrun pkt port B: 0
  ingress byte port a: 154514635
  ingress byte port b: 165959497
```

次のコマンドを使用して、他の HSR 関連情報を確認できます。

```
Router#sh hsr ?
node-table HSR Node Table
ring      Ring information
statistics HSR Statistics information
vdan-table HSR VDAN Table
```

制限事項

- 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-SAN モードのみがサポートされています
- HSR アラームのサポートは提供されていません
- リング内のノードの最大数は 50 に制限されています
- HSR-PTP は、このリリースではサポートされていません

タイミングプロトコルの実装

NTP

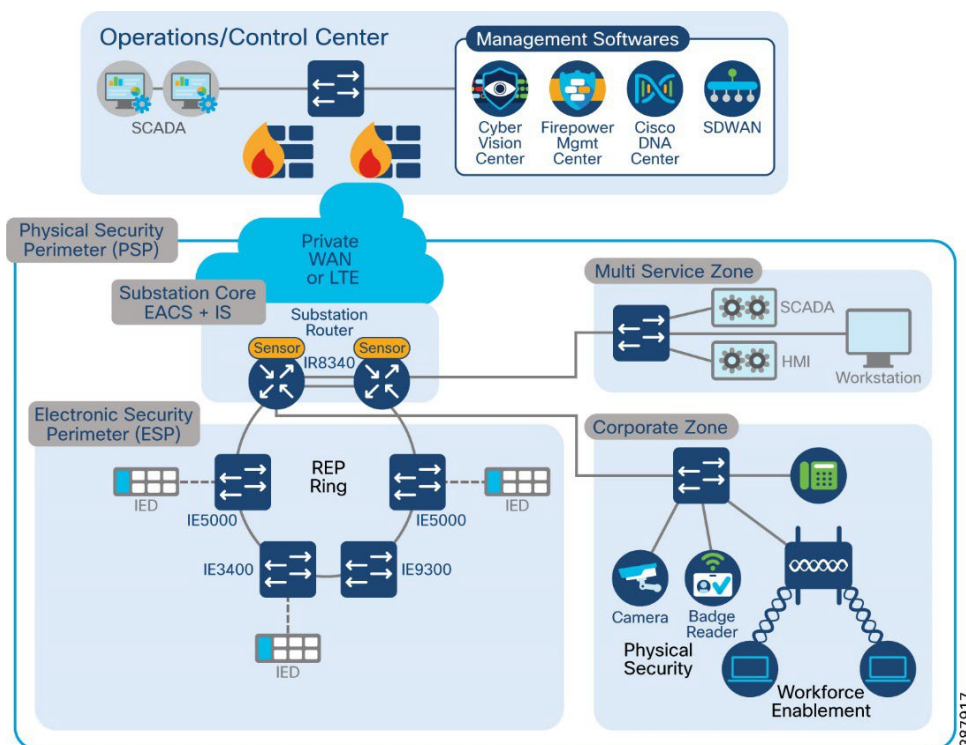
ネットワーク タイム プロトコルは、TCP/IP ネットワーク間でクロックを同期するためのネットワークプロトコルです。NTP は、クロックの階層型システムを使用して、ネットワーク上の異なるホスト間で時刻を同期します。

このソリューションガイドでは、REP リング上のタイミングプロトコルとして NTP の使用を推奨しています。Cisco IR8340 および IE9300 デバイスを使用した PTP over REP リングは、このソリューションガイドで検証された IOS-XE バージョンではサポートされていないことに注意してください。

次のトポロジは、REP リングが Cisco IR8340 ルータに集約されていることを示しています。IR8340 ルータは NTP の親として機能し、REP リング内のスイッチと REP リングに接続されているデバイスは IR8340 NTP 親からクロッキングを取得します。IR8340 は、次のような複数のソースからクロックを取得するように設定できます。

- NTP の基準クロックとしての PTP。
- より良いクロック品質を持つ別の NTP 親。

図 11 変電所の NTP



次のセクションでは、NTP の設定に関連するさまざまな手順を示します。

設定手順

1. NTP 親として機能するデバイスで次のコマンドを使用します。この例では、NTP 親として機能するデバイスで NTP の参照クロックとして PTP を使用します。PTP が設定され、同期されていることを確認します。PTP の設定手順については、このガイドの関連セクションを参照してください。

```
!  
ptp clock boundary domain 0 profile power  
clock-port dynamic1  
  transport ethernet multicast interface Gi0/1/4  
clock-port dynamic2  
  transport ethernet multicast interface Gi0/1/2  
  vlan 4001  
clock-port dynamic3  
  transport ethernet multicast interface Gi0/1/5  
clock-port dynamic4  
  transport ethernet multicast interface Gi0/1/6  
clock-port dynamic5  
  transport ethernet multicast interface Gi0/1/8  
!
```

```
Router#config t  
Enter configuration commands, one per line. End with CNTL/Z.  
ntp master  
ntp refclock ptp  
end  
Router#write
```

2. 次のコマンドを使用して、NTP 親からクロックを取得するデバイスで設定します。たとえば、クロッキングを必要とするスイッチやその他のシスコのネットワークデバイスなどです。回復力を確保するために、複数の NTP サーバーを使用することもできます。

```
Router#config t  
Enter configuration commands, one per line. End with CNTL/Z.  
ntp server 50.1.0.1  
ntp source Vlan 501  
end  
Router#write
```

確認

次のコマンドを使用して、NTP を確認します。

NTP 親として機能するデバイスで

```
Router#show ntp status
Clock is synchronized, stratum 1, reference is .PTP.
nominal freq is 250.0000 Hz, actual freq is 249.0581 Hz, precision is 2**10
ntp uptime is 910000 (1/100 of seconds), resolution is 4016
reference time is E6A8847B.FFBE7988 (14:57:23.999 IST Thu Aug 18 2022)
clock offset is 0.9998 msec, root delay is 0.00 msec
root dispersion is 463.52 msec, peer dispersion is 450.92 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000116 s/s
system poll interval is 1024, last update was 709 sec ago.
Router#
Router#show ntp associations

address      ref clock    st when poll reach delay offset disp
*~127.127.6.1 .PTP.        0 713 1024 37 0.000 0.999 450.92
~127.127.1.1 .LOCL.       7 9 16 377 0.000 0.000 1.204
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
Router#
```

NTP 親からクロックを取得するデバイスで

```
Switch#show ntp status
Clock is synchronized, stratum 2, reference is 50.1.0.1
nominal freq is 250.0000 Hz, actual freq is 250.0020 Hz, precision is 2**10
ntp uptime is 8252800 (1/100 of seconds), resolution is 4000
reference time is E6A886ED.91A9FD78 (09:37:49.569 UTC Thu Aug 18 2022)
clock offset is -0.5000 msec, root delay is 1.00 msec
root dispersion is 470.58 msec, peer dispersion is 3.71 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000008011 s/s
system poll interval is 128, last update was 262 sec ago.
Switch#
Switch#show ntp associations

address      ref clock    st when poll reach delay offset disp
*~50.1.0.1   .PTP.        1 132 128 377 1.000 -0.500 3.719
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
Switch#
Switch#show clock detail
09:42:19.650 UTC Thu Aug 18 2022
```

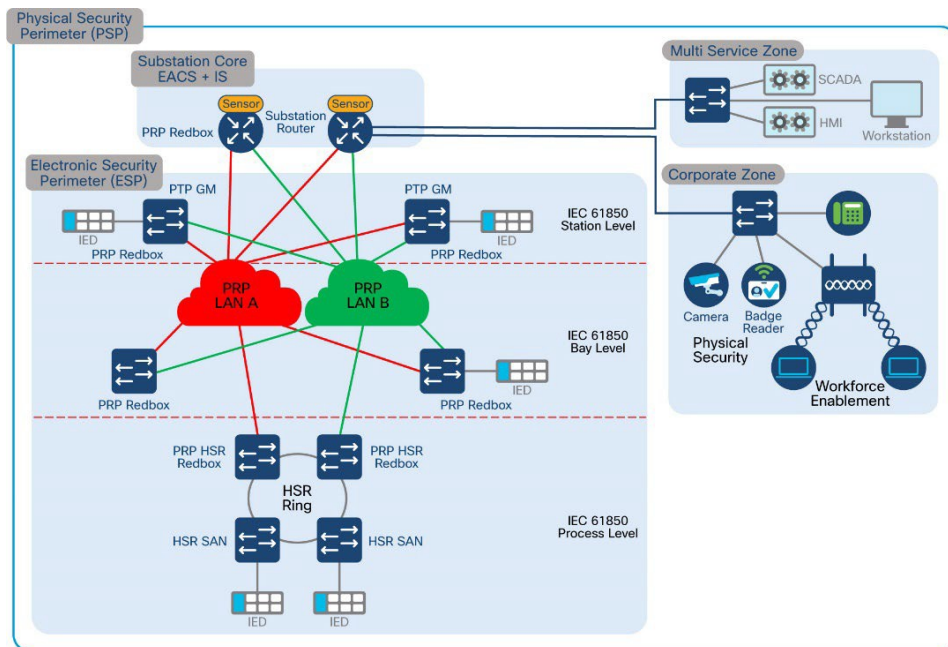

Time source is NTP Switch#

PTP

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。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。このドキュメントでは、この IEEE 1588 プロファイルとそれに関連する設定値を参照するときに、電力プロファイルモードという用語を使用します。

次のトポロジは、IE5000 を PTP グランドマスターとして示し、Cisco IE9300 を PTP を備えた PRP Redbox として示しています。IE5000 は GNSS 接続をサポートしているため、PTP グランドマスターとして設定されます。必要に応じて、他の PTP グランドマスターをトポロジに接続できます。

図12 変電所 LAN の PTP



以下は、GNSS、PTP グランドマスター、PTP 境界クロック、および PTP 透過クロックを設定するために必要な手順です。

設定手順

- GNSS アンテナを IE5000 の GNSS 入力ポートに接続します。GNSS 機能は、バージョン ID (VID) v05 以降および GNSS 受信機ファームウェアバージョン 1.04 を持つ IE 5000 SKU のみサポートされます。これらの詳細を確認するには、show version コマンドを使用します。
- GNSS が GPS 衛星と同期するまで待ちます。確認するには、show gnss status コマンドを使用します。
- スイッチをグランドマスター境界クロックモードに設定します。PTP は、スイッチのインターフェイスで明示的に無効になっていません。必要に応じて、インターフェイスで PTP を有効にして、PTP パケットを送信します。

```
!  
ptp profile power  
ptp mode gmc-bc pdelay-req  
ptp domain 3  
ptp priority <priority1> <priority2>  
!
```

- Cisco IE9300 は、PRP Redbox および PTP 境界クロックとして設定されています。Cisco IE9300 は PTP over PRP をサポートしています。PTP over PRP 用に Cisco IE9300 で次を設定します。インターフェイス GigabitEthernet1/0/21 および GigabitEthernet1/0/22 は、PRP チャネルメンバーインターフェイスです。同様に、PTP パケットを送信する必要がある他のインターフェイスを設定できます。デフォルトでは、スイッチはタグなしで PTP パケットを送信します。PTP パケットを特定の VLAN でタグ付けする必要がある場合は、その VLAN がスイッチの関連するすべてのインターフェイスで許可され、特定のインターフェイスで有効になっていることを確認してください。

```
!  
ptp clock boundary domain 3 profile power  
clock-port dynamic2  
transport ethernet multicast interface Gi1/0/21  
clock-port dynamic3  
vlan 1  
transport ethernet multicast interface Gi1/0/22  
!
```

- その他の Cisco Industrial Ethernet スイッチは、PTP トランスペアレントクロックとして設定されています。前述のとおり、PTP パケットの送信に参与するスイッチでは、それぞれの VLAN を有効にしてアクティブにする必要があります。
- 次のコマンドを使用して、PTP トランスペアレントクロックを有効にします。一部の Cisco Industrial Ethernet スイッチは、異なるバージョンの PTP Power プロファイル viz (IEEE C37.238-2011 および 2017) をサポートしています。それらは下位互換性があります。参加デバイスで適切なバージョンが有効になっていることを確認します。

```

!
ptp profile <profile version>
ptp mode p2ptransparent
ptp domain 3
!

```

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6 PTP の役割、プラットフォーム、およびサポートされるプロファイル

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
グラントマスター	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	PTP 電力プロファイル 2011 P.TP 電力プロファイル 2017
PTP 境界クロック	IE9300、IE4000、IE4010、IE3400	PTP 電力プロファイル 2011
PTP Over PRP Redbox	IE5000、IE4000、IE4010、IE3400	
PTP over HSR	IE5000、IE4000、IE4010、IE3400	

確認

次のコマンドを使用して、PTP に関連するさまざまな機能を確認します。

注：次のコマンドは、IOS イメージを実行する Cisco IE 5000、IE4010、IE3400、および IE4000 でサポートされています。

```
IE5000-GM#show gnss status
```

```
GNSS status: Enable  
Constellation: GPS  
Receiver Status: OD  
Survey progress: 100  
Satellite count: 8  
PDOP: 1.00 TDOP: 1.00  
HDOP: 0.00 VDOP: 0.00  
Alarm: None
```

```
IE5000-GM#show clock detail
```

```
13:25:39.215 IST Tue Aug 23 2022  
Time source is GNSS  
IE5000-GM#
```

```
IE5000-GM#show ptp clock
```

```
PTP CLOCK INFO  
PTP Device Type: Grand Master clock - Boundary clock  
PTP Device Profile: Power Profile IEEE-C37.238-2011  
Clock Identity: 0x0:BF:77:FF:FE:2C:36:80  
Clock Domain: 3  
Number of PTP ports: 28  
PTP Packet priority: 4  
Time Transfer: Linear Filter  
Priority1: 128  
Priority2: 128  
Clock Quality:  
Class: 6  
Accuracy: Within 250ns  
Offset (log variance): N/A  
Offset From Master(ns): 0  
Mean Path Delay(ns): 0  
Steps Removed: 0  
Local clock time: 13:26:42 IST Aug 23 2022
```

```
IE5000-GM#
```

```
IE5000-GM#show ptp parent
```

```
PTP PARENT PROPERTIES  
Local Clock:  
Clock Identity: 0x0:BF:77:FF:FE:2C:36:80
```

Local Port Number: 0

Parent Clock:

Parent Clock Identity: 0x0:BF:77:FF:FE:2C:36:80

Parent Port Number: 0

Observed Parent Offset (log variance): N/A

Observed Parent Clock Phase Change Rate: N/A

Grandmaster Clock:

Grandmaster Clock Identity: 0x0:BF:77:FF:FE:2C:36:80

Grandmaster Clock Quality:

Class: 6

Accuracy: Within 250ns

Offset (log variance): N/A

Priority1: 128

Priority2: 128

IE5000-GM#

注：次のコマンドは、IOS-XE Polaris イメージを実行している Cisco IE9300 でサポートされています。

clarke-002-PRP#show clock detail

**12:59:42.464 IST Tue Aug 23 2022*

Time source is PTP

clarke-002-PRP#

clarke-002-PRP#show ptp clock dataset time-properties

CLOCK [Boundary Clock, domain 3]

Current UTC Offset Valid: FALSE

Current UTC Offset: 37

Leap 59: FALSE

Leap 61: FALSE

Time Traceable: TRUE

Frequency Traceable: TRUE

PTP Timescale: TRUE

Time Source: GPS

clarke-002-PRP#

clarke-002-PRP#show prp control ptpProfile

PRP channel-group 1 PTP PROFILE value is 0x0 (l2-power)

PRP channel-group 2 PTP PROFILE value is 0x0 (l2-power)

clarke-002-PRP#show prp control ptpLanOption

PRP channel-group 1 PTP LAN OPT value is 0x3

PRP channel-group 2 PTP LAN OPT value is 0x0

clarke-002-PRP#

注：次のコマンドは、IOS イメージを実行する Cisco IE 5000、IE4010、IE3400、および IE4000 でサポートされています。

```
IE4010-005#show ptp clock  
PTP CLOCK INFO  
PTP Device Type: Peer to Peer transparent clock  
PTP Device Profile: Power Profile IEEE-C37.238-2017  
Clock Identity: 0x0:BF:77:FF:FE:27:DB:80  
Clock Domain: 3  
Number of PTP ports: 28  
PTP Packet priority: 4  
Delay Mechanism: Peer to Peer  
Local clock time: 11:17:04 IST Aug 23 2022
```

```
IE4010-005#show clock detail  
11:17:08.545 IST Tue Aug 23 2022  
Time source is PTP  
IE4010-005#
```

ベスト プラクティス

- PTP over PRP 機能を利用する場合は、PTP グランドマスター (GM) を両方の PRP LAN に接続することをお勧めします。そうしないと、PTP GM が接続されている単一の LAN 内のデバイスのみを同期できます。
- PTP が不要なインターフェイスで PTP を無効にします。
- PTP トランスペアレントクロックのピアツーピア トランスペアレント モードを設定して、ジッターを減らし、PTP パケットの蓄積を遅らせます。

```
Switch(config)# ptp mode p2pttransparent
```

- 次のコマンドを使用して、Organization_extension および Alternate_timescale TLV を使用せずに、非標準の PTP グランドマスター アナウンス メッセージを処理するようにスイッチを設定します。

```
Switch(config)# ptp allow-without-tlv
```

- 相互運用性のシナリオでは、C37.238:2011 標準に従って 0 (ゼロ) である既定の PTP ドメイン値を使用するのが最適です。IE スイッチのデフォルトの PTP ドメイン値は 0 (ゼロ) に設定されています。これは、次のコマンドを使用して設定することもできます。

Switch(config)# ptp domain

SCADA の有効化

変電所および関連機器の適切な機能を確保するために、ほとんどのユーティリティは SCADA システムを使用してモニタリングと制御を自動化しています。新しいサイトは通常、変電所と関連機器をモニタリングおよび制御するために SCADA システムを実装します。ただし、古い施設でも、SCADA システムを追加したり、既存の SCADA システムをアップグレードして新しいテクノロジーを利用したりすることでメリットを得ることができます。

SCADA の実装は、大きく 2 つの方法に分類できます。

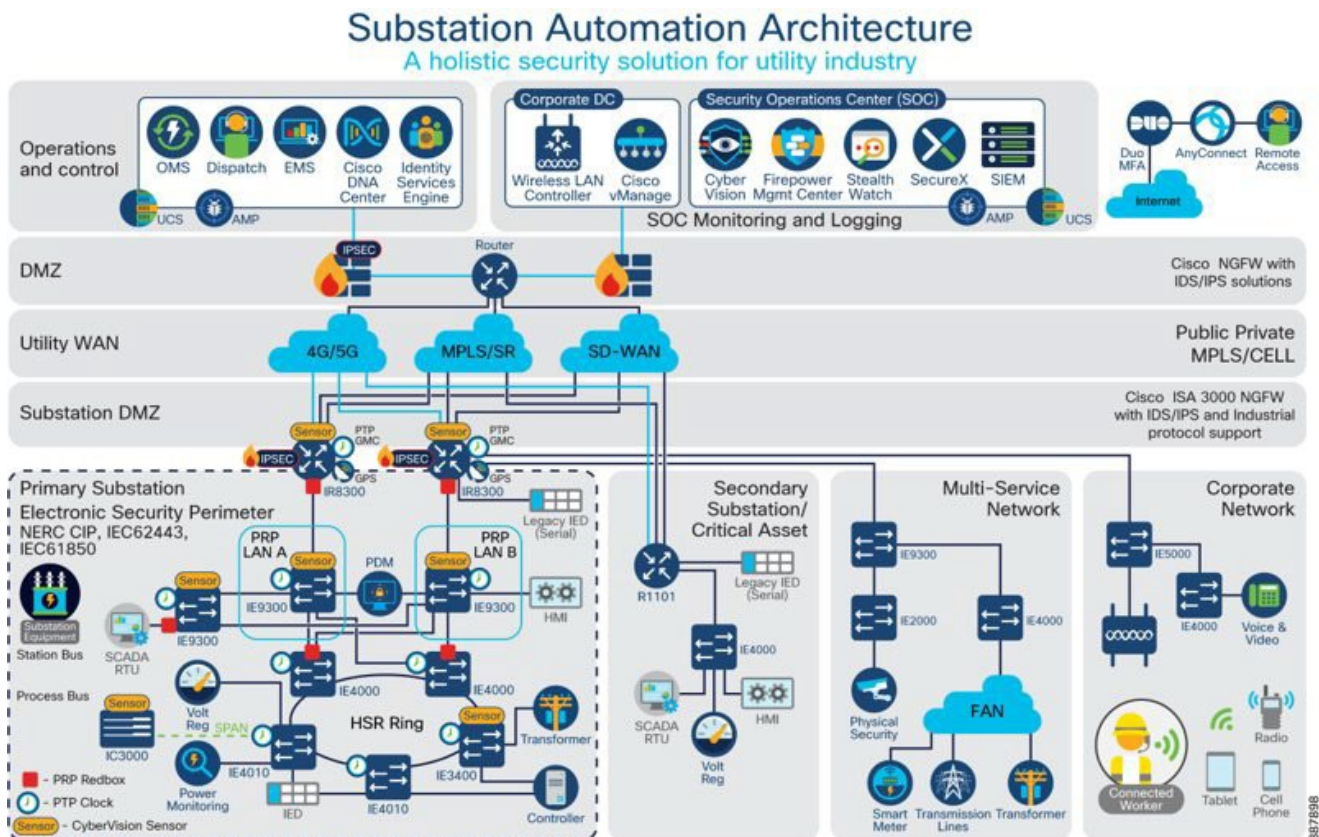
- Modbus IP、DNP3/IP、T104、および MMS プロトコルに基づくイーサネット/IP SCADA の実装
- Modbus シリアル、DNP3 シリアル、T101 プロトコルに基づくレガシー SCADA の実装。

レガシー SCADA は、Raw ソケットを使用するか、プロトコル変換を使用する 2 つの方法で実装されます。

- Raw ソケットを使用したシリアルベースの SCADA
- SCADA プロトコル変換

SCADA 検証トポロジ

図13 SCADA を使用した変電所自動化の検証トポロジ



Raw ソケットを使用したシリアルベースの SCADA との SCADA 通信

Modbus

電力事業者の SCADA アプリケーションで使用するために特別に開発された Modbus は、現在、これらのシステムで主要なプロトコルになっています。また、石油とガス、水、廃水など、他の産業でも人気が高まっています。Modbus 仕様では、複数のデータ型が定義されています。各タイプ内で、バリエーションがサポートされる場合があります。これらのバリエーションは、データが 16 ビットまたは 32 ビットの整数値、32 ビットまたは 64 ビットの浮動小数点値として送信されるかどうかを示す場合があります。

データの読み取り（入力）

Modbus 仕様は、入力を個別に、またはグループとして読み取る複数の方法をサポートしています。レポートにはデータタイプとポイント番号、値、および（オプションで）タイムスタンプが含まれているため、FEP ステーションはポーリングされた変更イベントデータを簡単に処理できます。

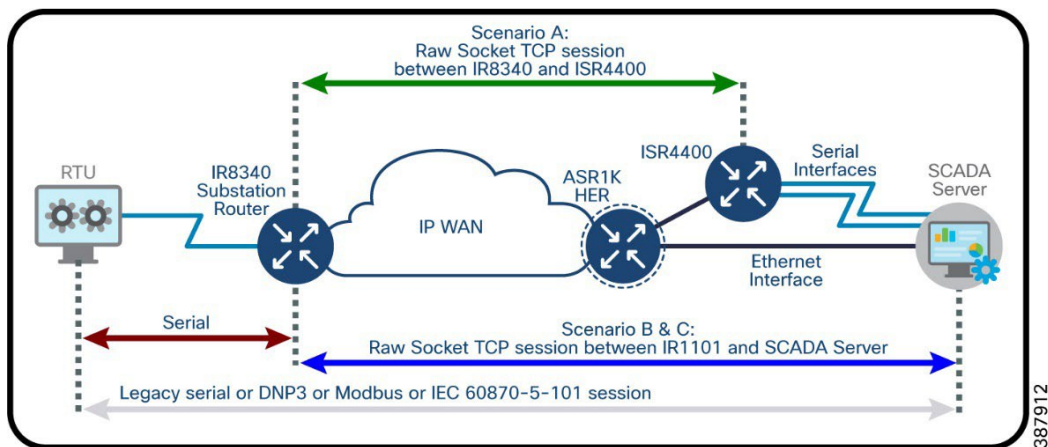
制御動作（出力）

Modbus は、書き込み操作による制御操作をサポートします。Modbus 出力オブジェクトも読み取り/書き込みです。出力オブジェクトを読み取ると、出力統計（つまり、最後に書き込まれたコマンド）が返されます。制御点の実際の値は、バイナリまたはアナログ入力を介してモニタリングできます。

実装の詳細

Cisco IR8340 は、シリアル経由でサウスバウンドのアクチュエータまたはセンサーに接続され、Modbus を SCADA 通信プロトコルとして使用します。Northbound FEP および Southbound Modbus アクチュエータは、TMW Distributed Test Manager (DTM) アプリケーションを使用してシミュレートされます。

図 14 SCADA Raw ソケットの実装図



IR8340 シリアルポートと SCADA Raw ソケットの有効化

IR8340 でプロトコル変換を有効にして設定するには、その前に IR8340 のシリアルポートを有効にし、そのポートで SCADA カプセル化を有効にする必要があります。

SCADA システム内のコントロールセンターと RTU 間のエンドツーエンド通信を可能にする Modbus シリアルプロトコルスタックを設定できます。

```
SUMATRA-CELLULAR#sh running-config interface s 0/3/0
Building configuration...
```

```
Current configuration: 89 bytes
!
interface Serial0/3/0
  physical-layer async
  no ip address
  encapsulation raw-tcp
end
```

```
SUMATRA-CELLULAR#
```

次の例は、シリアルポート 0/3/0 を有効にし、そのインターフェイスでカプセル化を有効にして SCADA プロトコルをサポートする方法を示しています。

raw ソケット TCP の設定

この例は、raw ソケットのパラメータを設定する方法を示しています。

```
SUMATRA-CELLULAR#sh running-config | sec line 0/3/0
line 0/3/0
  raw-socket tcp keepalive 10
  raw-socket tcp server 5012 99.99.99.2
  raw-socket special-char 7
  raw-socket packet-timer 1000
  raw-socket packet-length 1400
  stopbits 1
SUMATRA-CELLULAR#
```

設定の確認

```
SUMATRA-CELLULAR#sh raw-socket tcp sessions
----- TCP Sessions -----
-----
Interface tty          vrf_name          socket  mode  local_ip_addr  local_port  dest_ip_addr
dest_port  up_time          idle_time/timeout
-----
0/3/0  50
-----
0/3/0  50
51815  00:01:04  00:01:04/300sec
-----
SUMATRA-CELLULAR#

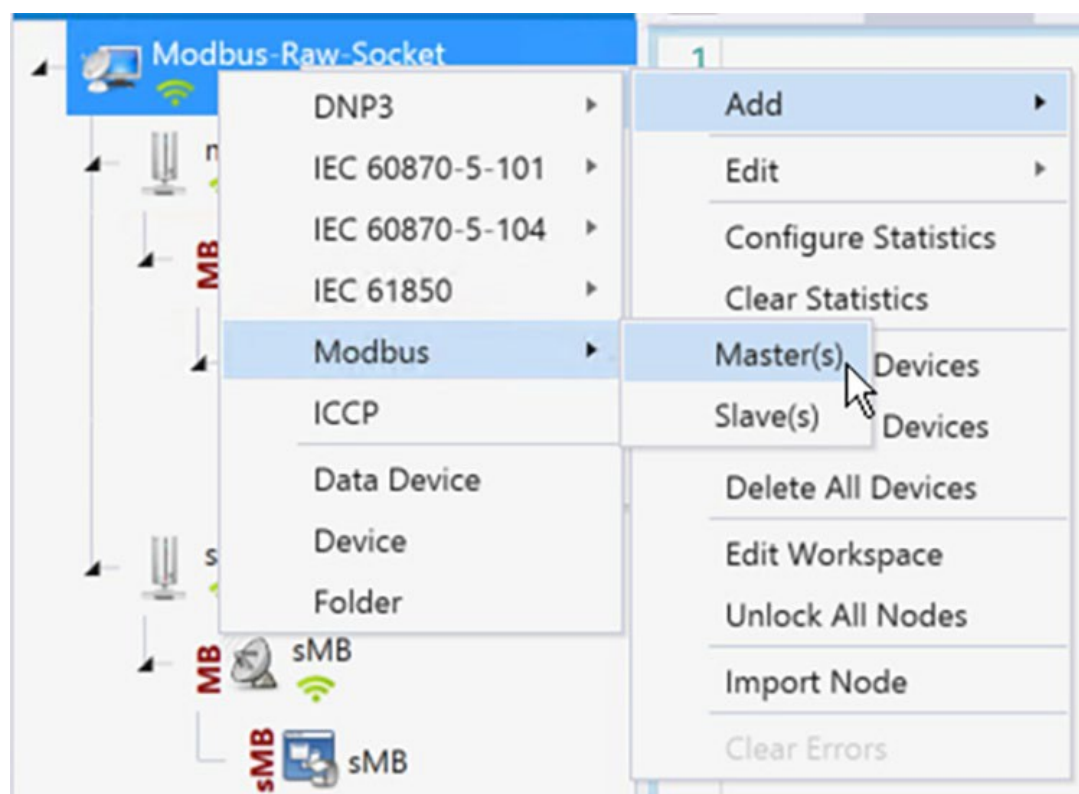
SUMATRA-CELLULAR#sh raw-socket tcp statistic
----- TCP-Serial Statistics -----
-
Interface  tty          vrf_name          sessions  tcp_in_bytes  tcp_out_bytes
tcp_to_tty_frames  tty_to_tcp_frames
-----
0/3/0  50
858    857
-----
SUMATRA-CELLULAR#
```

SCADA FEP 設定

トポロジに従って、SCADA FEP はコントロールセンターに存在します。SCADA FEP が SCADA Outstation/IED と通信するには、次の設定が必要です。この実装では、Modbus は Modbus Raw ソケットサーバーの代わりに SCADA FEP として機能しました。以下に示す設定は、Modbus に固有のものであります。

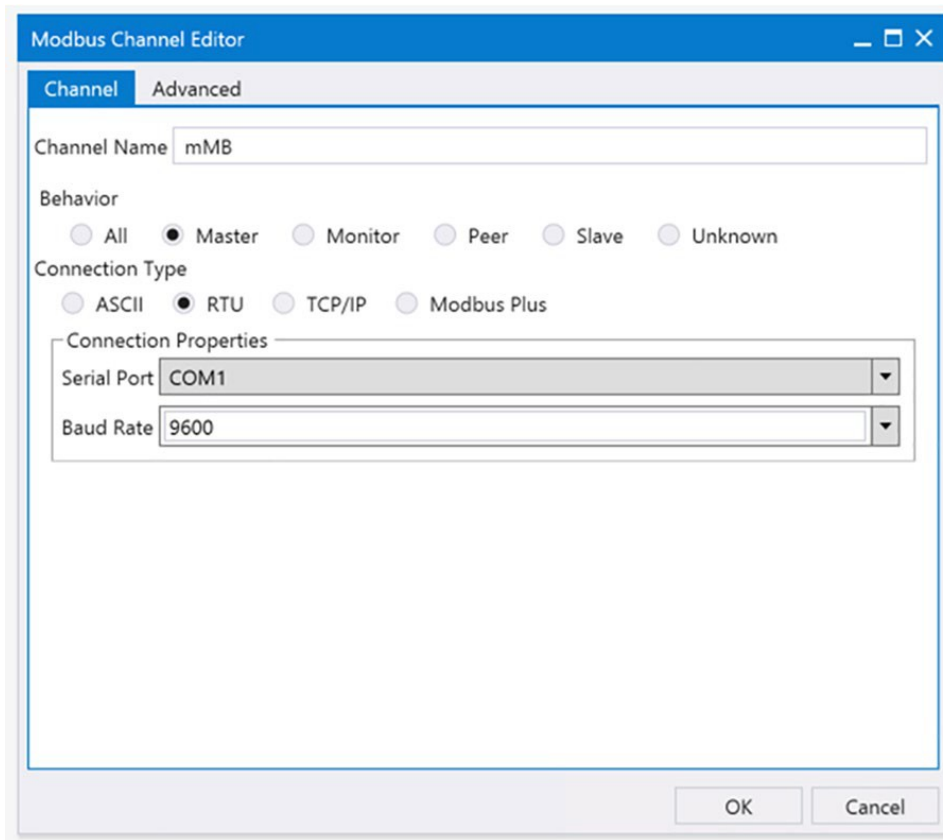
1. SCADA FEP アプリケーションを開き、[Add a new Modbus Master(s)] をクリックします。

図15 Modbus FEP の作成



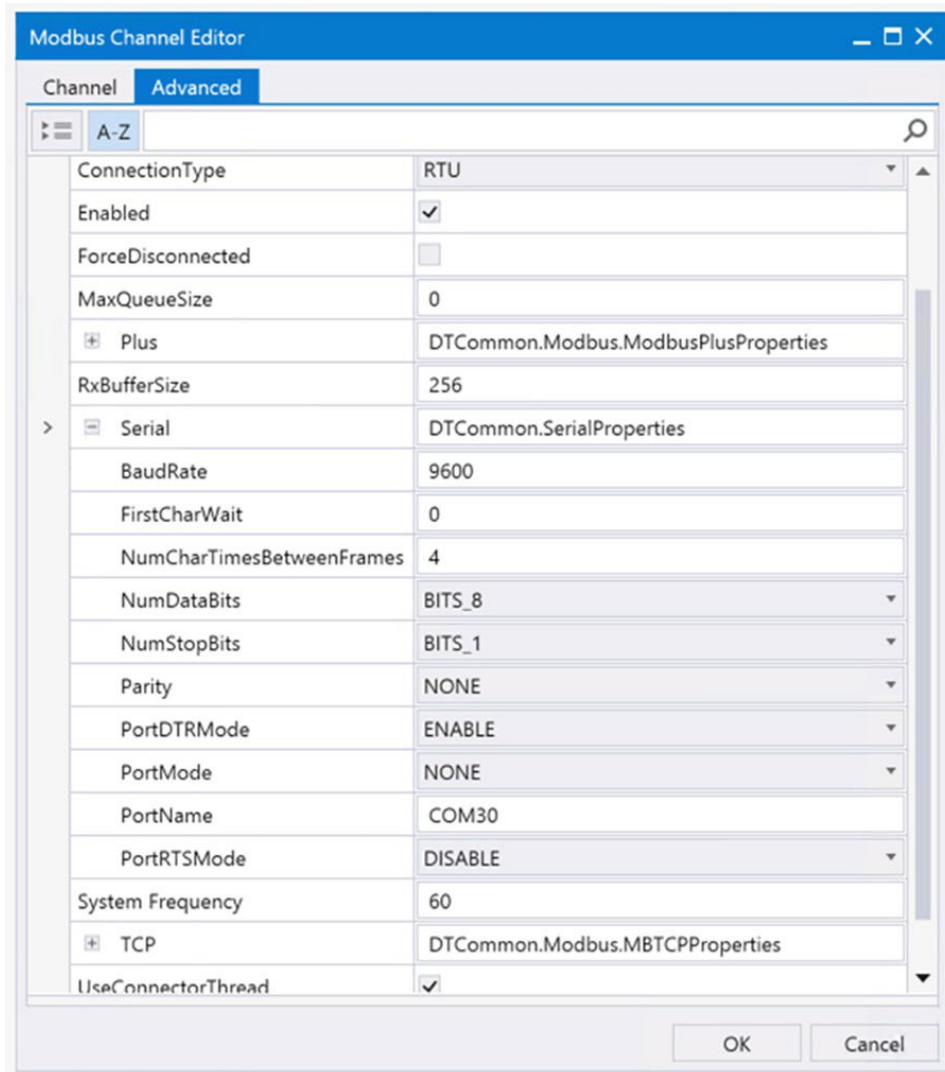
2. 図 16 のように SCADA FEP Modbus チャンネルを設定します。

図 16 Modbus FEP チャンネルの設定



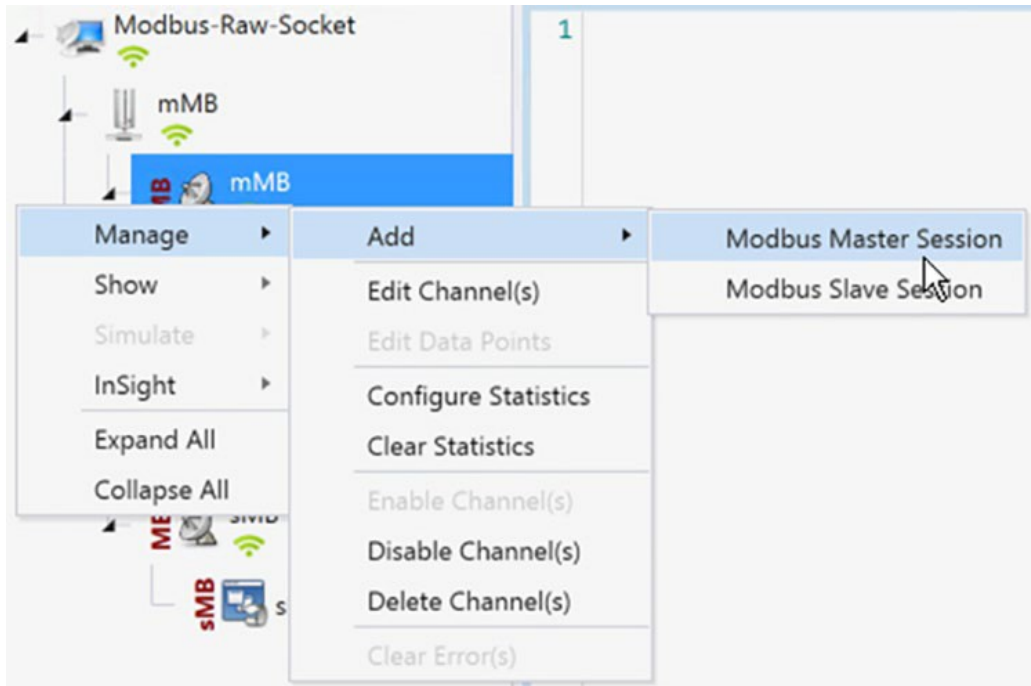
3. 図 17 のように、高度 FEP Modbus チャンネルを設定します。

図 17 Modbus FEP 高度チャンネルの設定



4. 図 18 に示すように、メニュー項目から Modbus FEP セッションを作成します。

図 18 Modbus FEP セッションの作成



5. デフォルトで作成されるサンプル Modbus データポイントテーブル。

図 19 Modbus FEP データポイントの表

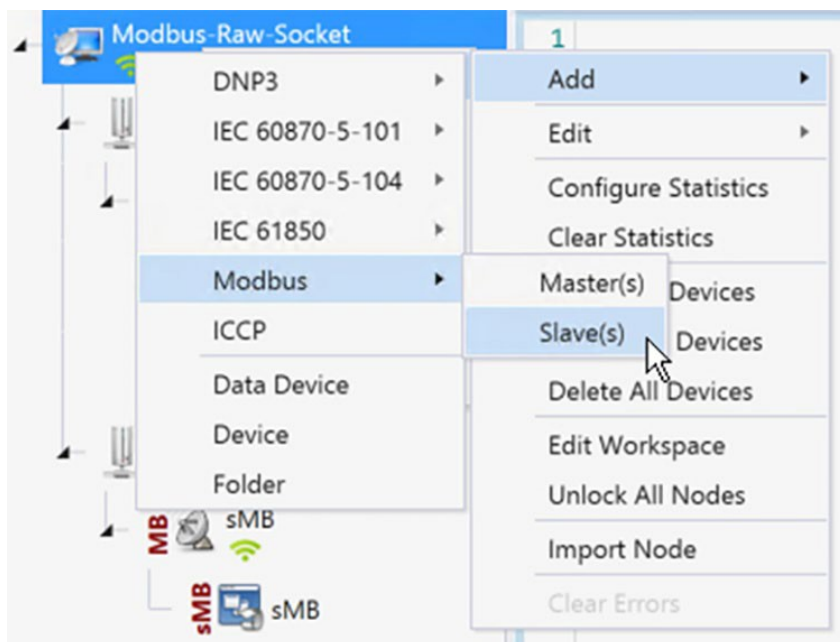
Name	Point Type	#	Value	Quality	Timestamp	Host
COIL #0	[0] Coils	0	Off	N/A	9/15/2022 3:03:51 PM	DTHost2
COIL #1	[0] Coils	1	Off	N/A	9/15/2022 3:03:51 PM	DTHost2
COIL #2	[0] Coils	2	Off	N/A	9/15/2022 3:03:51 PM	DTHost2
DREG #0	[1] Discrete Input Registers	0	Off	N/A	9/15/2022 3:03:51 PM	DTHost2
DREG #1	[1] Discrete Input Registers	1	Off	N/A	9/15/2022 3:03:51 PM	DTHost2
DREG #2	[1] Discrete Input Registers	2	Off	N/A	9/15/2022 3:03:51 PM	DTHost2
HREG #0	[4] Holding Registers	0	0	N/A	9/15/2022 3:03:51 PM	DTHost2
HREG #1	[4] Holding Registers	1	0	N/A	9/15/2022 3:03:51 PM	DTHost2
HREG #2	[4] Holding Registers	2	0	N/A	9/15/2022 3:03:51 PM	DTHost2
IREG #0	[3] Input Registers	0	0	N/A	9/15/2022 3:03:51 PM	DTHost2
IREG #1	[3] Input Registers	1	0	N/A	9/15/2022 3:03:51 PM	DTHost2
IREG #2	[3] Input Registers	2	0	N/A	9/15/2022 3:03:51 PM	DTHost2

SCADA Outstation/IED 設定

トポロジによると、SCADA Outstation/IED はフィールドエリアにあります。SCADA Outstation/IED が SCADA FEP と通信するには、次の設定が必要です。この実装では、実際の SCADA デバイスの代わりに SCADA DTMW シミュレータを使用しました。

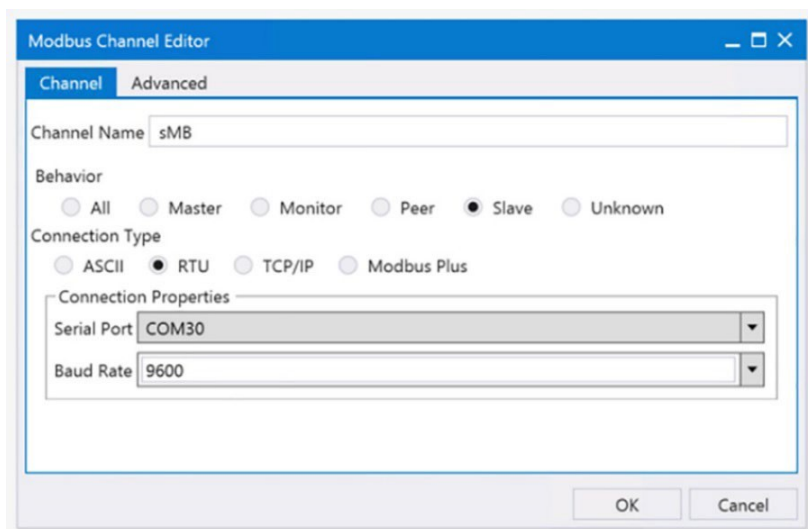
1. SCADA Outstation/IED アプリケーションを開き、[Add a new DNP3 Outstation/IED] をクリックします。
2. [Channel] タブから、図 20 のように SCADA FEP を設定します。

図 20 Modbus IED の作成



3. 図 21 のように SCADA Outstation Modbus チャンネルを設定します。

図 21 Modbus IED チャンネルの設定



4. 図 22 のように Advanced Outstation/IED Modbus チャンネルを設定します。

図 22 Modbus IED 高度チャンネルの設定

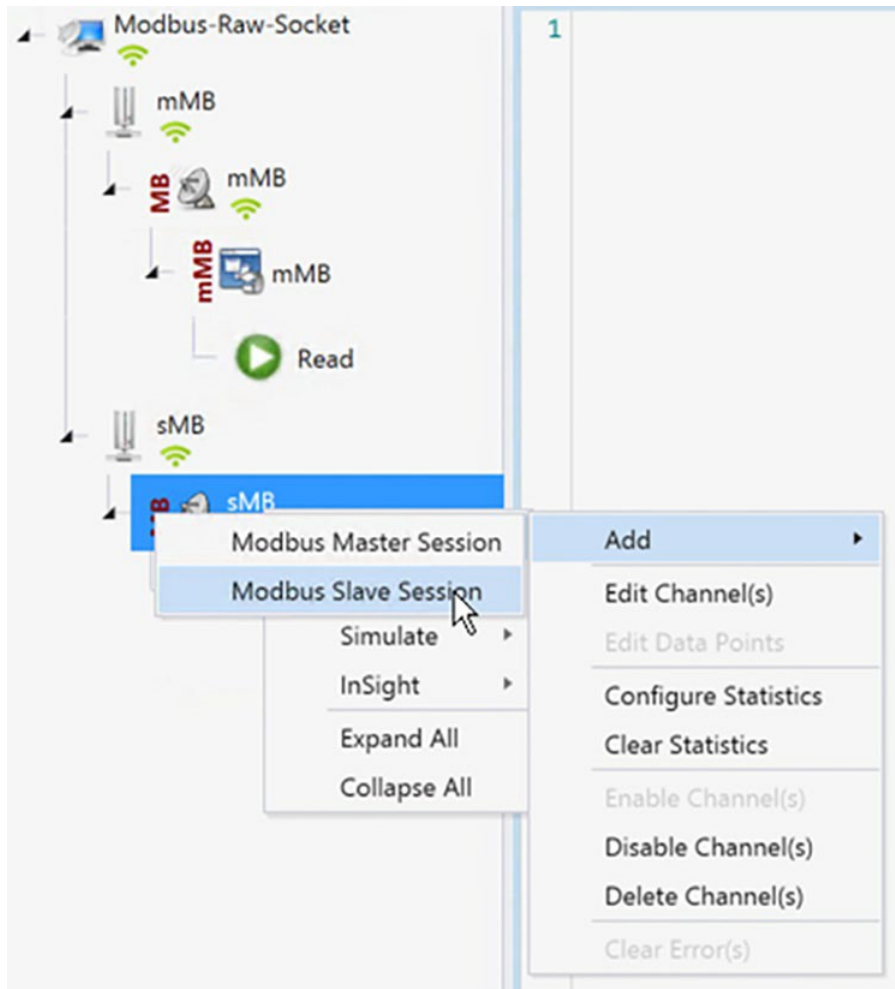
The screenshot shows the 'Modbus Channel Editor' dialog box with the 'Advanced' tab selected. The dialog is titled 'Modbus Channel Editor' and has a search bar at the top right. The 'Channel' tab is active, and the channel name is 'sMB'. The configuration is as follows:

Property	Value
ChannelName	sMB
ChannelResponseTimeout	10000
ConnectDelay	0
ConnectionType	RTU
Enabled	<input checked="" type="checkbox"/>
ForceDisconnected	<input type="checkbox"/>
MaxQueueSize	0
Plus	DTCCommon.Modbus.ModbusPlusProperties
RxBufferSize	256
Serial	DTCCommon.SerialProperties
BaudRate	9600
FirstCharWait	0
NumCharTimesBetweenFrames	4
NumDataBits	BITS_8
NumStopBits	BITS_1
Parity	NONE
PortDTRMode	ENABLE
PortMode	NONE
PortName	COM30
PortRTSMODE	DISABLE
System Frequency	60

At the bottom of the dialog, there are 'OK' and 'Cancel' buttons.

5. 図 23 に示すように、メニュー項目から Modbus Outstation/IED セッションを作成します。

図 23 Modbus IED セッションの作成



SCADA の操作

FEP と Outstation/IED はネットワーク経由で通信できます。ポーリング操作と制御操作は、FEP から開始されます。非送信要求レポートは、Outstation/IED から FEP に送信されます。図 25 と図 26 は、SCADA FEP からのポーリング操作を示しています。制御および非送信要求レポートも FEP アナライザのログに表示されます。

Modbus ポーリング

ポーリング操作は FEP によって実行されます。FEP はすべてのレジスタ値が読み取られて FEP に送信される一般的なポーリングを実行できます。図 27 では、FEP 側で実行された一般的なポーリングが表示されます。

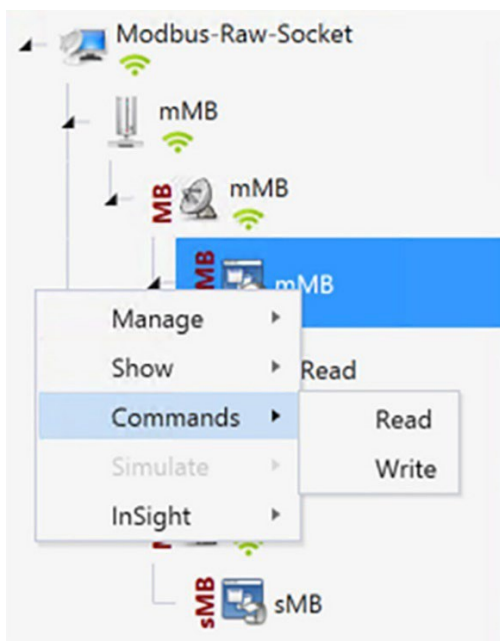
1. 以下の表は、SCADA Outstation/IED アプリケーションの初期データポイントを示しています。

図24 Modbus IED データポイントの表

Name	Point Type	#	Value	Quality	Timestamp	Host
COIL #0	[0] Coils	0	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
COIL #1	[0] Coils	1	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
COIL #2	[0] Coils	2	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
DREG #0	[1] Discrete Input Registers	0	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
DREG #1	[1] Discrete Input Registers	1	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
DREG #2	[1] Discrete Input Registers	2	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
HREG #0	[4] Holding Registers	0	0	N/A	9/15/2022 2:24:25 PM	DTHost3
HREG #1	[4] Holding Registers	1	0	N/A	9/15/2022 2:24:25 PM	DTHost3
HREG #2	[4] Holding Registers	2	0	N/A	9/15/2022 2:24:25 PM	DTHost3
IREG #0	[3] Input Registers	0	0	N/A	9/15/2022 2:24:25 PM	DTHost3
IREG #1	[3] Input Registers	1	0	N/A	9/15/2022 2:24:25 PM	DTHost3
IREG #2	[3] Input Registers	2	0	N/A	9/15/2022 2:24:25 PM	DTHost3

2. [FEP] を右クリックして [Commands] を選択し、[Read] メニュー項目を選択します。

図25 Modbus 読み取りコマンド



- 読み取りウィンドウを使用して、レジスタ値 0 から始まる COILS を読み取ります。

図26 Modbus Read コマンド設定ウィンドウ

The screenshot shows a 'Read' configuration window with the following details:

- Name:** Read
- Description:** Read Coils, Discrete Inputs, Holding Registers, or Input Registers
- Command Options:**
 - Type: Coils
 - Start: 0
 - Quantity: 10
- Scheduler:**
 - On Connect
 - Periodically
 - 00:00:09.000
- Buttons:** Execute, Apply, OK, Close

- FEP データテーブルで、特定のレジスタの COILS 値が IED/Outstation レジスタ値の値に従って更新されていることを確認します。

図27 更新された Modbus FEP データポイントの表

Name	Point Type	#	Value	Quality	Timestamp	Host
COIL #0	[0] Coils	0	Off	N/A	9/15/2022 3:03:51 PM	DTHost2
COIL #1	[0] Coils	1	Off	N/A	9/15/2022 3:03:51 PM	DTHost2
COIL #2	[0] Coils	2	Off	N/A	9/15/2022 3:03:51 PM	DTHost2
DREG #0	[1] Discrete Input Registers	0	Off	N/A	9/15/2022 3:03:51 PM	DTHost2
DREG #1	[1] Discrete Input Registers	1	Off	N/A	9/15/2022 3:03:51 PM	DTHost2
DREG #2	[1] Discrete Input Registers	2	Off	N/A	9/15/2022 3:03:51 PM	DTHost2
HREG #0	[4] Holding Registers	0	0	N/A	9/15/2022 3:03:51 PM	DTHost2
HREG #1	[4] Holding Registers	1	0	N/A	9/15/2022 3:03:51 PM	DTHost2
HREG #2	[4] Holding Registers	2	0	N/A	9/15/2022 3:03:51 PM	DTHost2
IREG #0	[3] Input Registers	0	0	N/A	9/15/2022 3:03:51 PM	DTHost2
IREG #1	[3] Input Registers	1	0	N/A	9/15/2022 3:03:51 PM	DTHost2
IREG #2	[3] Input Registers	2	0	N/A	9/15/2022 3:03:51 PM	DTHost2

Modbus 制御

制御操作は、エンドデバイスの操作を制御する目的で、SCADA FEP から SCADA Outstation/IED に制御コマンドを送信します。制御コマンドを実行し、その結果をアナライザ

に表示することができます。制御リレー出力の値が変更され、その値が FEP に通知されます。SCADA 制御操作は、次の一連のステップで検証されています。

1. 初期保有レジスタのステータスは、SCADA Outstation/IED に記録されます。図 28 は、制御コマンドを Outstation/IED に送信する前の保持レジスタの状態を示しています。次に、Northbound シミュレータからコマンドを発行して、レジスタの状態を ON に変更します。

図 28 Modbus IED の初期データポイントの表

Name	Point Type	#	Value	Quality	Timestamp	Host
COIL #0	[0] Coils	0	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
COIL #1	[0] Coils	1	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
COIL #2	[0] Coils	2	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
DREG #0	[1] Discrete Input Registers	0	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
DREG #1	[1] Discrete Input Registers	1	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
DREG #2	[1] Discrete Input Registers	2	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
HREG #0	[4] Holding Registers	0	0	N/A	9/15/2022 2:46:50 PM	DTHost3
HREG #1	[4] Holding Registers	1	0	N/A	9/15/2022 2:24:25 PM	DTHost3
HREG #2	[4] Holding Registers	2	0	N/A	9/15/2022 2:24:25 PM	DTHost3
IREG #0	[3] Input Registers	0	0	N/A	9/15/2022 2:24:25 PM	DTHost3
IREG #1	[3] Input Registers	1	0	N/A	9/15/2022 2:24:25 PM	DTHost3
IREG #2	[3] Input Registers	2	0	N/A	9/15/2022 2:24:25 PM	DTHost3

2. 以下の書き込みウィンドウを使用して、FEP から Outstation/IED に書き込みまたは制御コマンドを送信します。このウィンドウでは、コマンドは開始値 0 で保持レジスタに書き込まれ、値は 1 です。

図 29 Modbus 制御コマンド設定ウィンドウ

Write

Name: Write Select Device(s)

Description
Write Coils or Holding Registers

Command Options

Type: HoldingRegisters

Start: 0

Quantity: 1

Value: 1

Scheduler

On Connect Periodically 00:00:01.000

Execute Apply OK Close

- IED データテーブルで、保持レジスタが前の手順の書き込みまたは制御コマンドの値で更新されていることを確認します。

図 30 制御コマンドで更新された Modbus IED

Name	Point Type	#	Value	Quality	Timestamp	Host
COIL #0	[0] Coils	0	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
COIL #1	[0] Coils	1	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
COIL #2	[0] Coils	2	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
DREG #0	[1] Discrete Input Registers	0	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
DREG #1	[1] Discrete Input Registers	1	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
DREG #2	[1] Discrete Input Registers	2	Off	N/A	9/15/2022 2:24:25 PM	DTHost3
HREG #0	[4] Holding Registers	0	1	N/A	9/15/2022 2:47:52 PM	DTHost3
HREG #1	[4] Holding Registers	1	0	N/A	9/15/2022 2:24:25 PM	DTHost3
HREG #2	[4] Holding Registers	2	0	N/A	9/15/2022 2:24:25 PM	DTHost3
IREG #0	[3] Input Registers	0	0	N/A	9/15/2022 2:24:25 PM	DTHost3
IREG #1	[3] Input Registers	1	0	N/A	9/15/2022 2:24:25 PM	DTHost3
IREG #2	[3] Input Registers	2	0	N/A	9/15/2022 2:24:25 PM	DTHost3

SCADA プロトコル変換の使用例

IR8340 は、次のプロトコルに対してプロトコル変換を実行します。

- IEC 60870 T101 と IEC 60870 T104 の送受信。
- DNP3 シリアルから DNP3 IP へ

SCADA の詳細については、次の URL にある『Cisco IR8340 SCADA Configuration Guide』を参照してください。

https://www.cisco.com/c/en/us/td/docs/routers/ir8340/software/configuration/b_ir8340_cg_17_7/m_scada.html

このセクションでは、次の SCADA プロトコル変換シナリオの実装に関する詳細について説明します。

DNP3 シリアル (サウスバウンド) から DNP3 IP (ノースバウンド) への変換の使用例

DNP3

電力事業者の SCADA アプリケーションで使用するために特別に開発された DNP は、現在、これらのシステムで主要なプロトコルになっています。また、石油とガス、水、廃水など、他の産業でも人気が高まっています。DNP 仕様では、かなりの数のデータ型が定義されています。各タイプ内で、複数のバリエーションがサポートされる場合があります。これらのバ

リエーションは、データが 16 ビットまたは 32 ビットの整数値、32 ビットまたは 64 ビットの浮動小数点値として送信されるかどうか、タイムスタンプの有無、および品質インジケータ（フラグ）の有無を表す場合があります。

データの読み取り（入力）

DNP3 仕様は、入力を個別に、またはグループとして読み取る複数の方法をサポートしています。たとえば、複数のタイプのデータを 1 つのメッセージにカプセル化して、効率を向上させることができます。タイムスタンプとデータ品質情報も含めることができます。

DNP3 は変更イベントもサポートしています。変更イベントをポーリングすることにより、変更された値のみが報告されるため、FEP ステーションは回線上の全体的なトラフィックを削減できます。これは一般に、例外によるレポート（RBE）と呼ばれます。効率をさらに向上させるために、DNP3 は非送信要求レポートもサポートしています。非送信要求レポートを使用すると、Outstation/IED デバイスは、FEP からのポーリングを待つことなく、値の変更に応じて更新を送信できます。

FEP ステーションは、変更イベントデータ（ポーリングまたは非送信請求）を簡単に処理できます。これは、レポートにデータタイプとバリエーション、ポイント番号、値、および（オプションで）タイムスタンプと品質インジケータが含まれているためです。

制御動作（出力）

DNP3 は、出力オブジェクトグループ（制御リレー出力ブロックまたは CROB およびアナログ出力ブロック）を介した制御操作をサポートします。DNP3 出力オブジェクトも読み取り/書き込みです。出力オブジェクトを読み取ると、出力統計（つまり、最後に書き込まれたコマンド）が返されます。制御点の実際の値は、バイナリまたはアナログ入力を介してモニタリングできます。

DNP3 は、パルス出力やペア出力など、制御アプリケーションで一般的に使用されるさまざまな機能もサポートしています。

実装の詳細

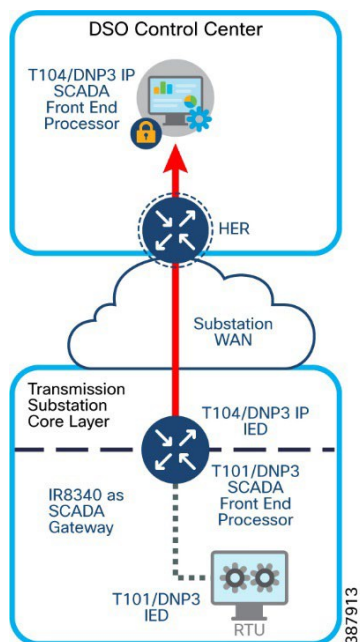
Cisco IR8340 はシリアル経由でサウスバウンドのアクチュエータまたはセンサーに接続され、SCADA 通信プロトコルとして DNP3 を使用します。Southbound DNP3 アクチュエータは、TMW DTM アプリケーションを使用してシミュレートされます。Northbound DNP3 IP SCADA ソフトウェアは、TMW Distributed Test Manager (DTM) アプリケーションを使用してシミュレートされます。

ネットワークでは、コントロールセンターは常に、IR8340 との通信時にネットワーク内の FEP として機能します。IR8340 は、RTU と通信するときにコントロールセンターのプロキシ FEP ステーションとして機能します。

IR8340 は、次を実行するために SCADA ゲートウェイとして機能するプロトコル変換を提供します。

1. RTU からデータを受信し、コントロールセンターから RTU データに設定コマンドを中継する。
2. 設定コマンドをコントロールセンターから受信し、RTU データをコントロールセンターに中継します。

図 31 プロトコル変換の実装図



IR8340 シリアルポートと SCADA カプセル化の有効化

IR8340 でプロトコル変換を有効にして設定するには、その前に IR8340 のシリアルポートを有効にし、そのポートで SCADA カプセル化を有効にする必要があります。

SCADA システム内のコントロールセンターと RTU 間のエンドツーエンド通信を可能にする DNP3 シリアルおよび DNP3 IP プロトコルスタックを設定できます。

```
SUMATRA-CELLULAR#sh run interface Serial0/3/0
interface Serial0/3/0
physical-layer async
no ip address
encapsulation scada
end
SUMATRA-CELLULAR#
```

上記の例は、シリアルポート 0/3/0 を有効にし、そのインターフェイスでカプセル化を有効にして SCADA プロトコルをサポートする方法を示しています。

DPN3-serial

次の例は、DPN3 シリアルプロトコルスタックのパラメータを設定する方法を示しています。

```
SUMATRA-CELLULAR#sh run | sec dnp3-serial
scada-gw protocol dnp3-serial
channel serial
    unsolicited-response enable
    bind-to-interface Serial0/3/0
session serial1
    attach-to-channel serial
SUMATRA-CELLULAR#
```

DNP3 IP

次の例は、DNP3 IP パラメータの設定例を示しています。

```
SUMATRA-CELLULAR#sh run | sec dnp3-ip
scada-gw protocol dnp3-ip
channel ip
    link-addr dest 4
    tcp-connection local-port default remote-ip 192.168.4.171/0
session ip1
    attach-to-channel ip
    link-addr source 3
```

```
map-to-session serial1
SUMATRA-CELLULAR#
```

プロトコル変換の開始または停止

ルータでプロトコル変換エンジンを起動するには、次のコマンドを入力します。

```
SUMATRA-CELLULAR# configure terminal
SUMATRA-CELLULAR(config)#scada-gw enable
```

ルータのプロトコル変換エンジンを停止するには、次のコマンドを入力します。

```
SUMATRA-CELLULAR# configure terminal
SUMATRA-CELLULAR(config)# no scada-gw enable
```

設定の確認

```
SUMATRA-CELLULAR#sh scada tcp
DNP3 network channel [ip]: 4 max simultaneous connections

conn: local-ip: 99.99.99.2 local-port 20000    remote-ip 192.168.4.171    data-socket 1
```

```
Total:
  1 current client connections
  0 total closed connections
```

```
SUMATRA-CELLULAR#
```

```
SUMATRA-CELLULAR#sh scada statistics
DNP3 network Channel [ip]:
  210 messages sent, 7 messages received
  0 timeouts, 0 aborts, 0 rejections
  202 protocol errors, 202 link errors, 0 address errors
```

```
DNP3 serial Channel [serial]:
  520 messages sent, 108 messages received
  2 timeouts, 0 aborts, 0 rejections
  0 protocol errors, 8 link errors, 0 address errors
```

```
SUMATRA-CELLULAR#
```

```
SUMATRA-CELLULAR#
```

```
SUMATRA-CELLULAR#sh line 0/3/0
```

Tty	Line	Typ	Tx/Rx	A	Modem	Roty	AccO	AccI	Uses	Noise	Overruns	Int
0/3/0	50	TTY	9600/9600	-	-	-	-	-	0	0	0/0	Se0/3/0

```
Line 0/3/0, Location: "", Type: ""
```

```
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 9600/9600, no parity, 1 stopbits, 8 databits
Status: Ready
Capabilities: none
Modem state: Ready
Modem hardware state: noCTS noDSR DTR noRTS
```

```
SUMATRA-CELLULAR#sh run int serial0/3/0
Building configuration...
```

```
Current configuration : 87 bytes
!
interface Serial0/3/0
physical-layer async
no ip address
encapsulation scada
end
```

```
SUMATRA-CELLULAR#
```

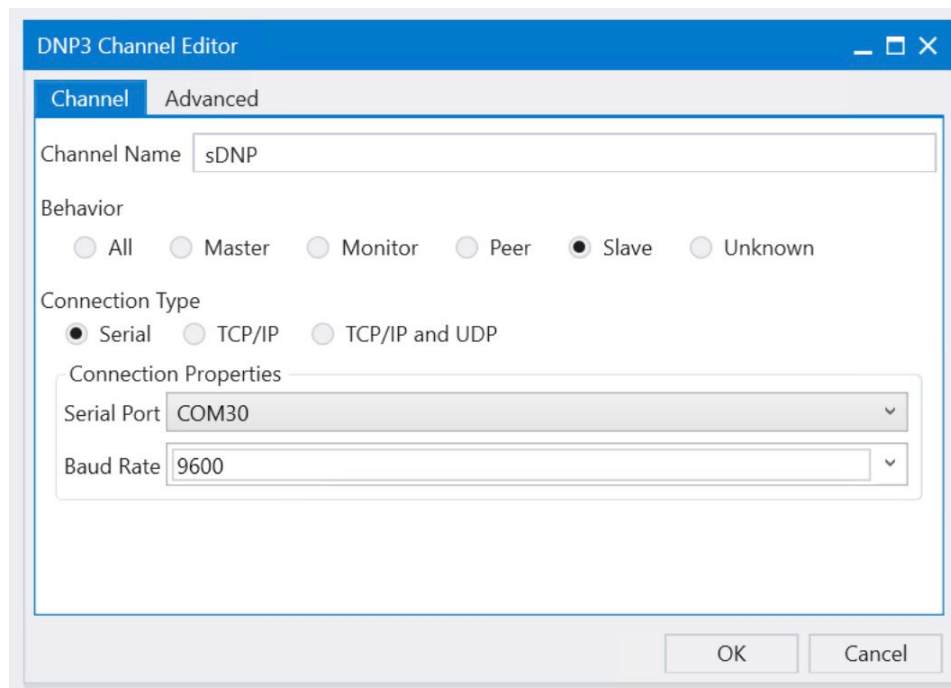
サウスバウンド DNP3 TMW 設定

チャンネル設定

Southbound シリアル IED は、TMW ソフトウェアを使用してシミュレートされます。この例では、図 27 に示すように、ボーレート 9600 のシリアルポート COM30 が Cisco IR8340 の Async0 に接続されています。

1. DNP3 IED チャンネルの作成

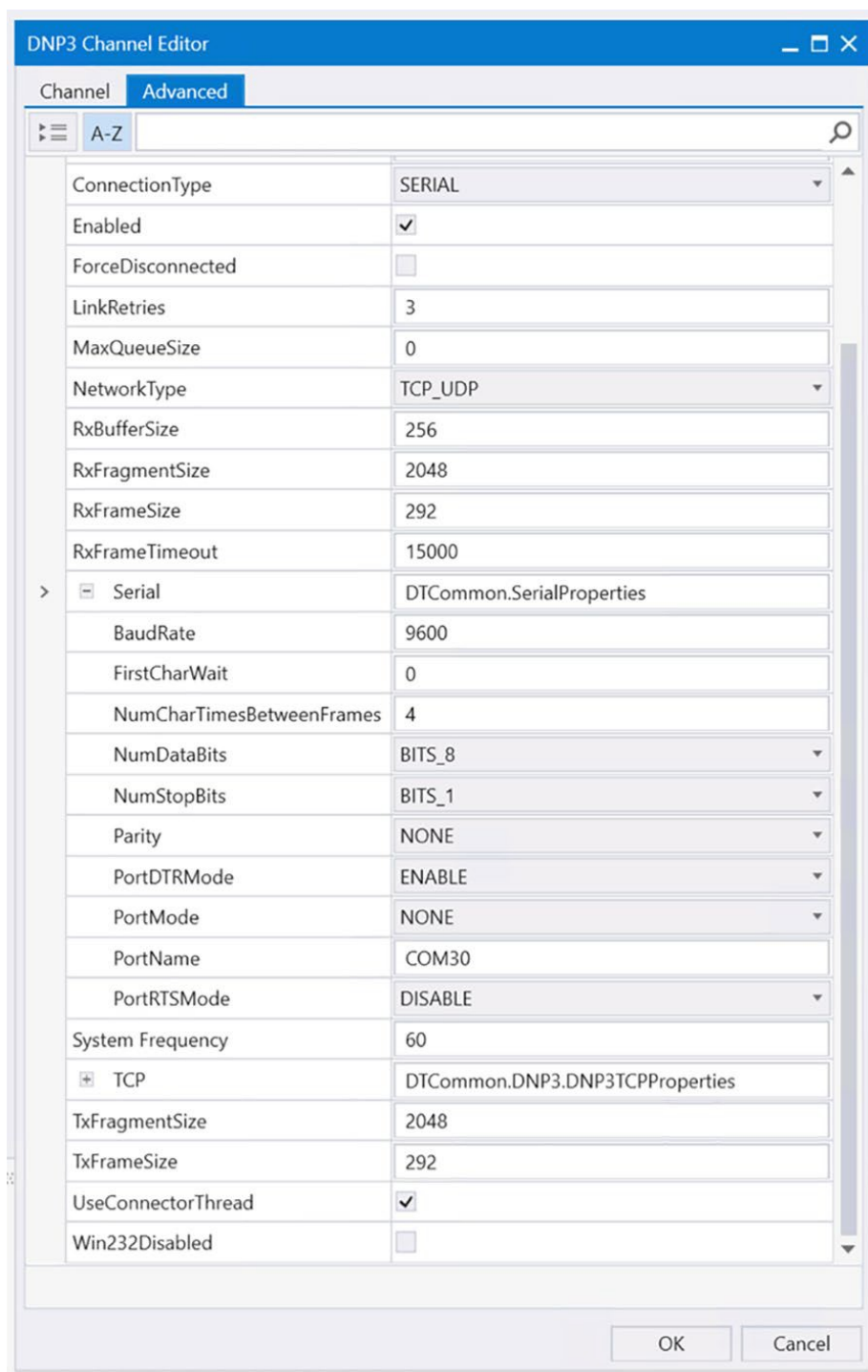
図32 DNP3 IED チャンネルの設定



2. DNP3 IED 高度チャネル設定の作成

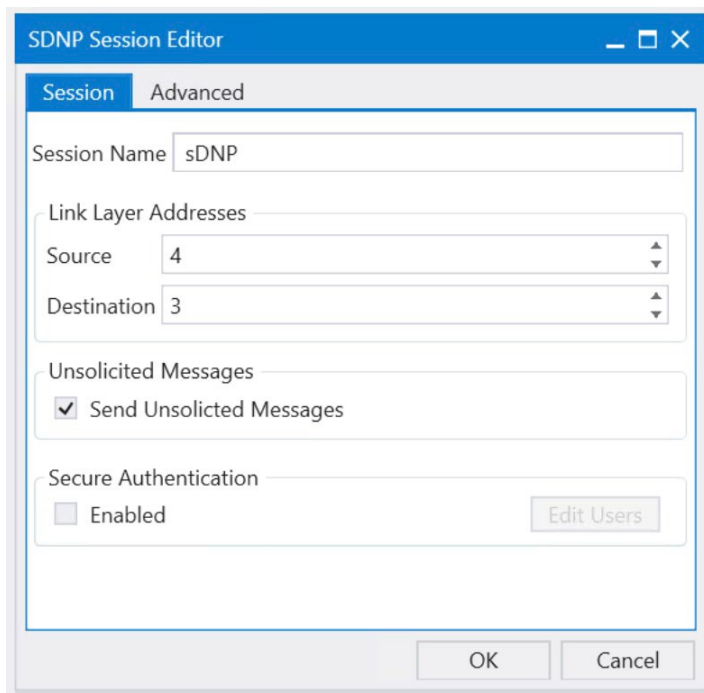
図33 DNP3 IED 高度チャネルの設定

Parity が None に設定されていること、ポートが DTR モードで設定されていること、StopBits が 1 であること、DataBits が 8 であることを確認します。



3. DNP3 IED セッションを作成します。DNP3 サウスバウンドシリアル RTU シミュレータは Outstation/IED として設定され、ソース層と宛先層はそれぞれ 4 と 3 として設定されます。図 34 を参照してください。

図 34 DNP3 IED セッションの作成



ノースバウンド DNP3 IP TMW 設定

DNP3 IP チャネル設定

TMW DTM ソフトウェアは、DNP3 IP で設定されます。FEP モードは、Control Center SCADA ソフトウェアをシミュレートするために使用されます。図 30 を参照してください。

図 35 DNP3 FEP チャネルの設定

The screenshot shows the 'DNP3 Channel Editor' dialog box with the 'Advanced' tab selected. The configuration is as follows:

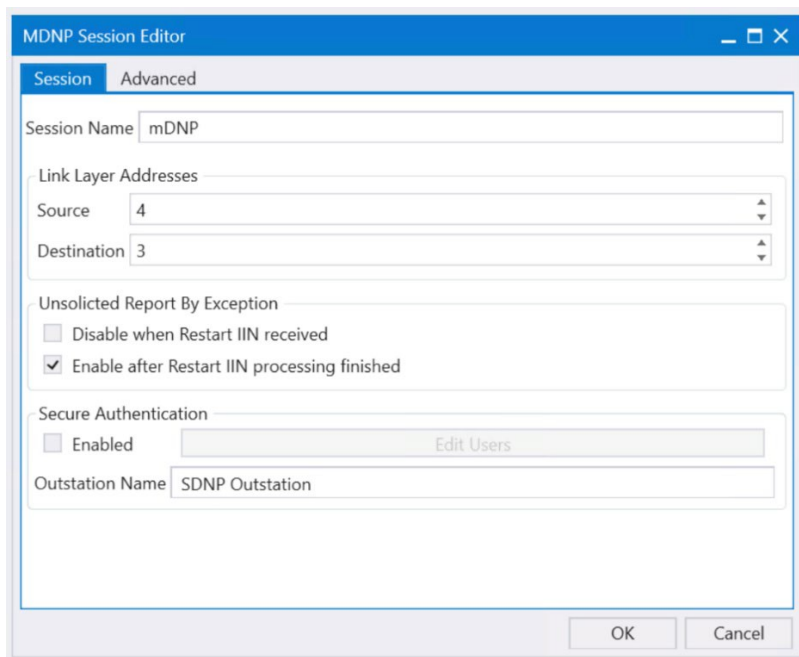
- Channel Name:** mDNP
- Behavior:** Master (selected), All, Monitor, Peer, Slave, Unknown
- Connection Type:** TCP/IP (selected), Serial, TCP/IP and UDP
- Connection Properties:**
 - Mode:** Client (selected), Server
 - Local Address:** 192.168.4.171 - ASIX AX88179 USB 3.0 to Gigabit Ethernet Adapter #3
 - Remote Address:** 99.99.99.2
 - Port:** 20,000

Buttons for 'OK' and 'Cancel' are visible at the bottom right.

DNP3 IP セッション関連の設定

DNP3 IP リンク層アドレス 4 および 3 を設定します。図 36 を参照してください。

図 36 DNP3 FEP セッションの設定



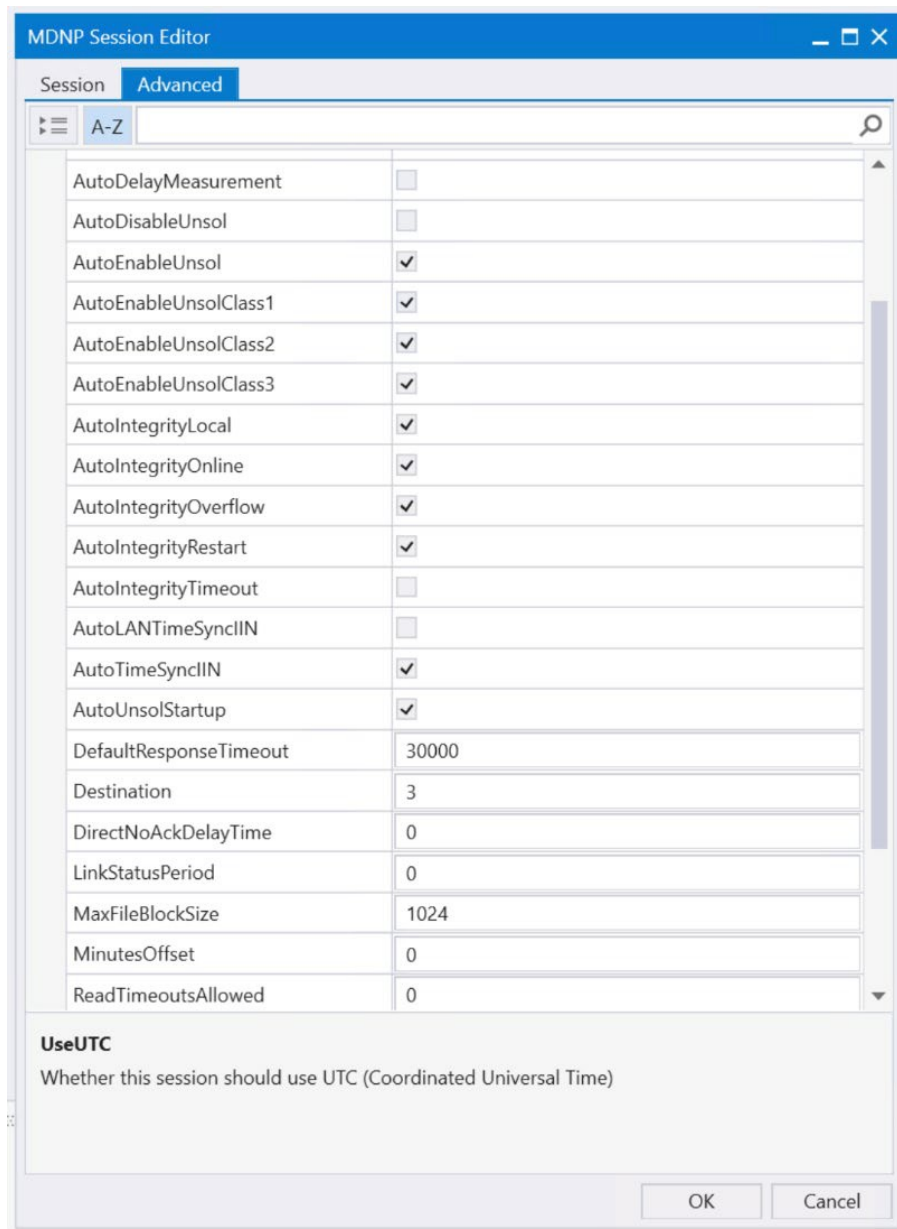
The screenshot shows the 'MDNP Session Editor' dialog box with the 'Advanced' tab selected. The 'Session Name' is set to 'mDNP'. Under 'Link Layer Addresses', 'Source' is set to 4 and 'Destination' is set to 3. In the 'Unsolicited Report By Exception' section, the checkbox 'Enable after Restart IIN processing finished' is checked. The 'Secure Authentication' section has the 'Enabled' checkbox unchecked. The 'Outstation Name' is set to 'SDNP Outstation'. 'OK' and 'Cancel' buttons are at the bottom right.

Field	Value
Session Name	mDNP
Link Layer Addresses - Source	4
Link Layer Addresses - Destination	3
Unsolicited Report By Exception - Enable after Restart IIN processing finished	Checked
Secure Authentication - Enabled	Unchecked
Outstation Name	SDNP Outstation

DNP3 IP 詳細設定

AutoTimeSyncIIN、AutoEnabledUnsol、AutoIntegrityOnline、および AutoIntegrityRestart は、有効にする必要がある高度な DNP3 IP 設定です。詳細については、図 37 を参照してください。

図 37 DNP3 FEP 高度セッションの設定



The screenshot shows the 'MDPN Session Editor' dialog box with the 'Advanced' tab selected. The dialog contains a list of configuration options, each with a checkbox or a text input field. The 'UseUTC' section at the bottom has a descriptive text and is currently unchecked.

Property	Value
AutoDelayMeasurement	<input type="checkbox"/>
AutoDisableUnsol	<input type="checkbox"/>
AutoEnableUnsol	<input checked="" type="checkbox"/>
AutoEnableUnsolClass1	<input checked="" type="checkbox"/>
AutoEnableUnsolClass2	<input checked="" type="checkbox"/>
AutoEnableUnsolClass3	<input checked="" type="checkbox"/>
AutoIntegrityLocal	<input checked="" type="checkbox"/>
AutoIntegrityOnline	<input checked="" type="checkbox"/>
AutoIntegrityOverflow	<input checked="" type="checkbox"/>
AutoIntegrityRestart	<input checked="" type="checkbox"/>
AutoIntegrityTimeout	<input type="checkbox"/>
AutoLANTimeSyncIIN	<input type="checkbox"/>
AutoTimeSyncIIN	<input checked="" type="checkbox"/>
AutoUnsolStartup	<input checked="" type="checkbox"/>
DefaultResponseTimeout	30000
Destination	3
DirectNoAckDelayTime	0
LinkStatusPeriod	0
MaxFileBlockSize	1024
MinutesOffset	0
ReadTimeoutsAllowed	0

UseUTC
Whether this session should use UTC (Coordinated Universal Time)

OK Cancel

整合性調査の使用例

DNP3 仕様は、入力を個別に、またはグループとして読み取る複数の方法をサポートしています。整合性ポーリングは、クラス 0 からのデータ（静的データと呼ばれる）と、クラス 1、2、および 3 からのデータ（イベントデータ）を返します。Outstation/IED の設定方法によっては、これがすべてではない場合もあります。

整合性ポーリングは、デバイスからすべてのイベント（クラス 1、2、および 3）および静的（クラス 0）データを取得します。通常、デバイスの再起動後、通信が失われた後、またはすべてのデータが正確であることを確認するために定期的送信されます。この整合性ポーリングは、図 38 と図 39 に示すノースバウンド DTM アプリケーションから実行されます。

図 38 DNP3 整合性データポーリング

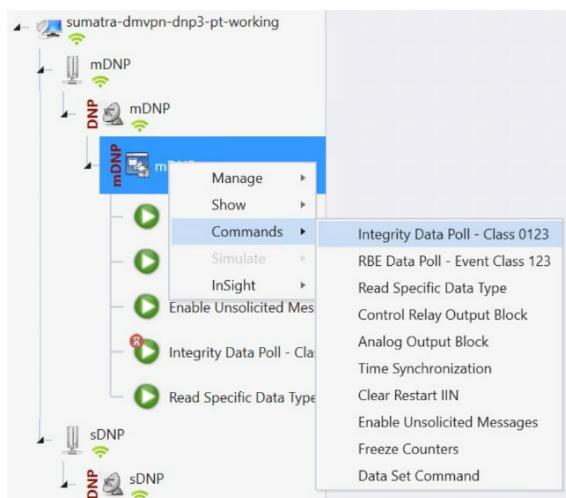
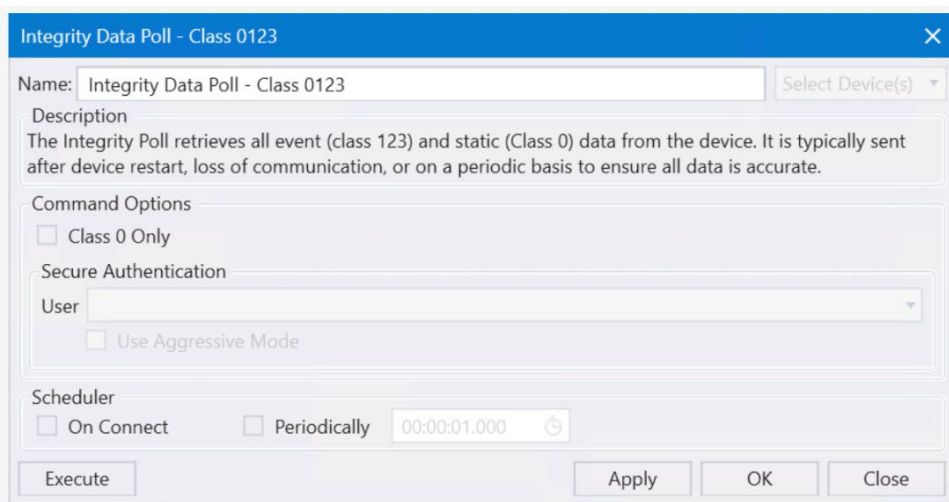


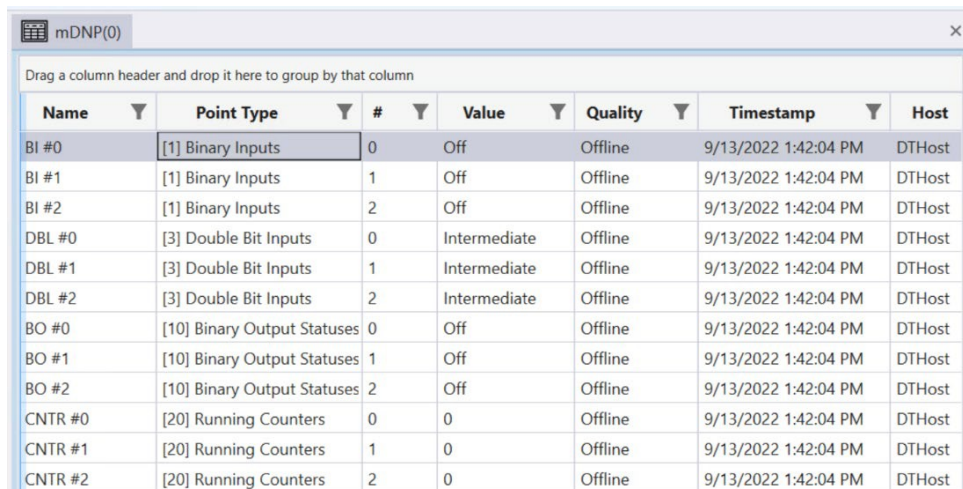
図 39 整合性データポーリング実行ウィンドウ



[Apply] をクリックし、[Execute] をクリックしてポーリングを開始します。

Northbound DTM アプリケーションのポーリング結果を図 40 に示します。
DNP3 IP セッションの下にある [Show Point List] オプションをクリックします。

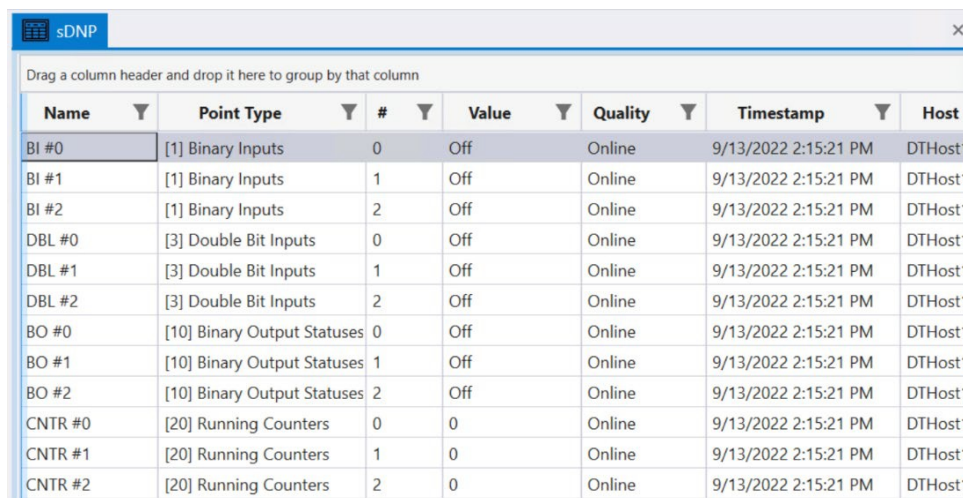
図 40 整合性ポーリング後に更新された DNP3 FEP データポイントのリスト



Name	Point Type	#	Value	Quality	Timestamp	Host
BI #0	[1] Binary Inputs	0	Off	Offline	9/13/2022 1:42:04 PM	DTHost
BI #1	[1] Binary Inputs	1	Off	Offline	9/13/2022 1:42:04 PM	DTHost
BI #2	[1] Binary Inputs	2	Off	Offline	9/13/2022 1:42:04 PM	DTHost
DBL #0	[3] Double Bit Inputs	0	Intermediate	Offline	9/13/2022 1:42:04 PM	DTHost
DBL #1	[3] Double Bit Inputs	1	Intermediate	Offline	9/13/2022 1:42:04 PM	DTHost
DBL #2	[3] Double Bit Inputs	2	Intermediate	Offline	9/13/2022 1:42:04 PM	DTHost
BO #0	[10] Binary Output Statuses	0	Off	Offline	9/13/2022 1:42:04 PM	DTHost
BO #1	[10] Binary Output Statuses	1	Off	Offline	9/13/2022 1:42:04 PM	DTHost
BO #2	[10] Binary Output Statuses	2	Off	Offline	9/13/2022 1:42:04 PM	DTHost
CNTR #0	[20] Running Counters	0	0	Offline	9/13/2022 1:42:04 PM	DTHost
CNTR #1	[20] Running Counters	1	0	Offline	9/13/2022 1:42:04 PM	DTHost
CNTR #2	[20] Running Counters	2	0	Offline	9/13/2022 1:42:04 PM	DTHost

上記の Northbound シミュレータでのポーリング結果。バイナリ入力の4つのレジスタ値 (0、1、2) が受信されました。Southbound IED シミュレータでは、これらはバイナリ入力レジスタ値 (0、1、および 2) にマップされます。

図 41 DNP3 IED データポイントの表



Name	Point Type	#	Value	Quality	Timestamp	Host
BI #0	[1] Binary Inputs	0	Off	Online	9/13/2022 2:15:21 PM	DTHost
BI #1	[1] Binary Inputs	1	Off	Online	9/13/2022 2:15:21 PM	DTHost
BI #2	[1] Binary Inputs	2	Off	Online	9/13/2022 2:15:21 PM	DTHost
DBL #0	[3] Double Bit Inputs	0	Off	Online	9/13/2022 2:15:21 PM	DTHost
DBL #1	[3] Double Bit Inputs	1	Off	Online	9/13/2022 2:15:21 PM	DTHost
DBL #2	[3] Double Bit Inputs	2	Off	Online	9/13/2022 2:15:21 PM	DTHost
BO #0	[10] Binary Output Statuses	0	Off	Online	9/13/2022 2:15:21 PM	DTHost
BO #1	[10] Binary Output Statuses	1	Off	Online	9/13/2022 2:15:21 PM	DTHost
BO #2	[10] Binary Output Statuses	2	Off	Online	9/13/2022 2:15:21 PM	DTHost
CNTR #0	[20] Running Counters	0	0	Online	9/13/2022 2:15:21 PM	DTHost
CNTR #1	[20] Running Counters	1	0	Online	9/13/2022 2:15:21 PM	DTHost
CNTR #2	[20] Running Counters	2	0	Online	9/13/2022 2:15:21 PM	DTHost

このドキュメントの目的のために、完全性ポーリングのバイナリ入力レジスタ値について説明しました。

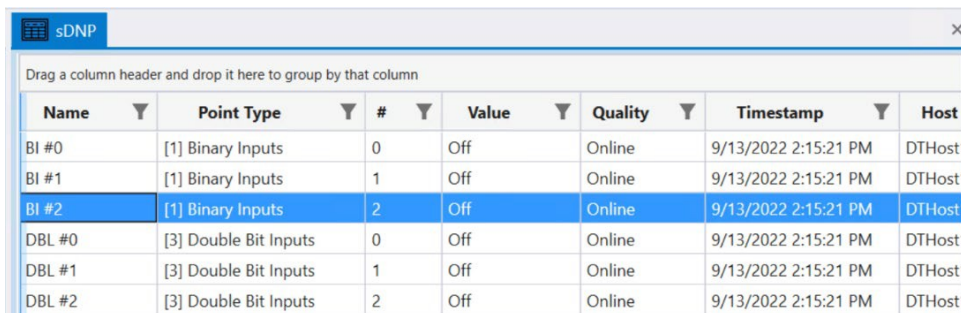
非送信要求レポート

DNP3 は非送信要求レポートをサポートしています。つまり、Outstation/IED デバイスは、FEP からのポーリングを待つことなく、値の変更に応じて更新を送信できます。

以前の整合性ポーリングの場合、サウスバウンド入力レジスタ #2 がオフになっていることがわかりました。サウスバウンドレジスタ #2 は、ノースバウンドのレジスタ #2 としてマップされます。サウスバウンドレジスタの状態を変更すると、ノースバウンドレジスタの状態が自動的に変更されます。

ノースバウンド DTM アプリケーションの入力レジスタ #2 値の状態チェックを確認します。この場合は OFF です。図 42 を参照してください。

図 42 BI レジスタ 2 を含む DNP3 IED データポイントの表

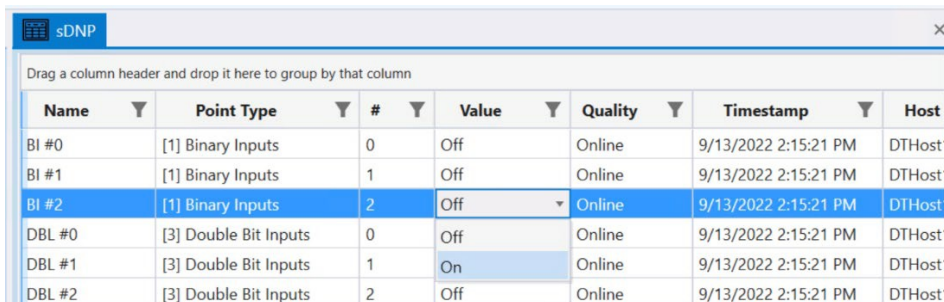


Name	Point Type	#	Value	Quality	Timestamp	Host
BI #0	[1] Binary Inputs	0	Off	Online	9/13/2022 2:15:21 PM	DTHost
BI #1	[1] Binary Inputs	1	Off	Online	9/13/2022 2:15:21 PM	DTHost
BI #2	[1] Binary Inputs	2	Off	Online	9/13/2022 2:15:21 PM	DTHost
DBL #0	[3] Double Bit Inputs	0	Off	Online	9/13/2022 2:15:21 PM	DTHost
DBL #1	[3] Double Bit Inputs	1	Off	Online	9/13/2022 2:15:21 PM	DTHost
DBL #2	[3] Double Bit Inputs	2	Off	Online	9/13/2022 2:15:21 PM	DTHost

Southbound アプリケーションで、レジスタ #2 の値を [ON] (右クリックして切り替え) に変更します。

ノースバウンド アプリケーションで、バイナリ入力レジスタ値 #2 の非送信要求レポートが観察されます。

図 43 DNP3 IED バイナリ入力レジスタの切り替え



Name	Point Type	#	Value	Quality	Timestamp	Host
BI #0	[1] Binary Inputs	0	Off	Online	9/13/2022 2:15:21 PM	DTHost
BI #1	[1] Binary Inputs	1	Off	Online	9/13/2022 2:15:21 PM	DTHost
BI #2	[1] Binary Inputs	2	On	Online	9/13/2022 2:15:21 PM	DTHost
DBL #0	[3] Double Bit Inputs	0	Off	Online	9/13/2022 2:15:21 PM	DTHost
DBL #1	[3] Double Bit Inputs	1	On	Online	9/13/2022 2:15:21 PM	DTHost
DBL #2	[3] Double Bit Inputs	2	Off	Online	9/13/2022 2:15:21 PM	DTHost

バイナリ入力レジスタ # 2 の値をオフからオンに切り替えます。

図 44 非送信請求メッセージによって更新された DNP3 FEP データポイントの表

Name	Point Type	#	Value	Quality	Timestamp	Host
BI #0	[1] Binary Inputs	0	Off	Offline	9/13/2022 1:42:04 PM	DTHost
BI #1	[1] Binary Inputs	1	Off	Offline	9/13/2022 1:42:04 PM	DTHost
BI #2	[1] Binary Inputs	2	On	Online	9/13/2022 2:23:24 PM	DTHost
DBL #0	[3] Double Bit Inputs	0	Intermediate	Offline	9/13/2022 1:42:04 PM	DTHost
DBL #1	[3] Double Bit Inputs	1	Intermediate	Offline	9/13/2022 1:42:04 PM	DTHost
DBL #2	[3] Double Bit Inputs	2	Intermediate	Offline	9/13/2022 1:42:04 PM	DTHost

図 44 に示すように、更新された値は ON です。

Control コマンド

DNP3 では、バイナリ出力ステータスレジスタは、制御コマンドまたは書き込み操作に使用されます。ノースバウンド DTM アプリケーションからレジスタ値 #1 に CROB コマンドを発行してみます。この場合、レジスタ値 #1 に書き込みます。ノースバウンドアプリケーションのレジスタ値 #1 は、サウスバウンドアプリケーションのレジスタ値 #1 にマップされます。ノースバウンドから制御コマンドを発行する前のサウスバウンド TMW アプリケーションバイナリ出力ステータスレジスタ #1 のステータスチェック。図 45 で、バイナリ出力レジスタ #1 のステータスが OFF であることがわかります。

図 45 DNP3 IED バイナリ出力レジスタ 1

Name	Point Type	#	Value	Quality	Timestamp	Host
BI #0	[1] Binary Inputs	0	Off	Online	9/13/2022 2:15:21 PM	DTHost
BI #1	[1] Binary Inputs	1	Off	Online	9/13/2022 2:15:21 PM	DTHost
BI #2	[1] Binary Inputs	2	On	Online	9/13/2022 2:23:24 PM	DTHost
DBL #0	[3] Double Bit Inputs	0	Off	Online	9/13/2022 2:15:21 PM	DTHost
DBL #1	[3] Double Bit Inputs	1	Off	Online	9/13/2022 2:15:21 PM	DTHost
DBL #2	[3] Double Bit Inputs	2	Off	Online	9/13/2022 2:15:21 PM	DTHost
BO #0	[10] Binary Output Statuses	0	Off	Online	9/13/2022 2:37:21 PM	DTHost
BO #1	[10] Binary Output Statuses	1	Off	Online	9/13/2022 2:38:50 PM	DTHost
BO #2	[10] Binary Output Statuses	2	Off	Online	9/13/2022 2:15:21 PM	DTHost

次に、Northbound シミュレータからコマンドを発行して、レジスタの状態を ON に変更します。図 46 を参照してください。

図 46 DNP3 CROB 制御コマンド

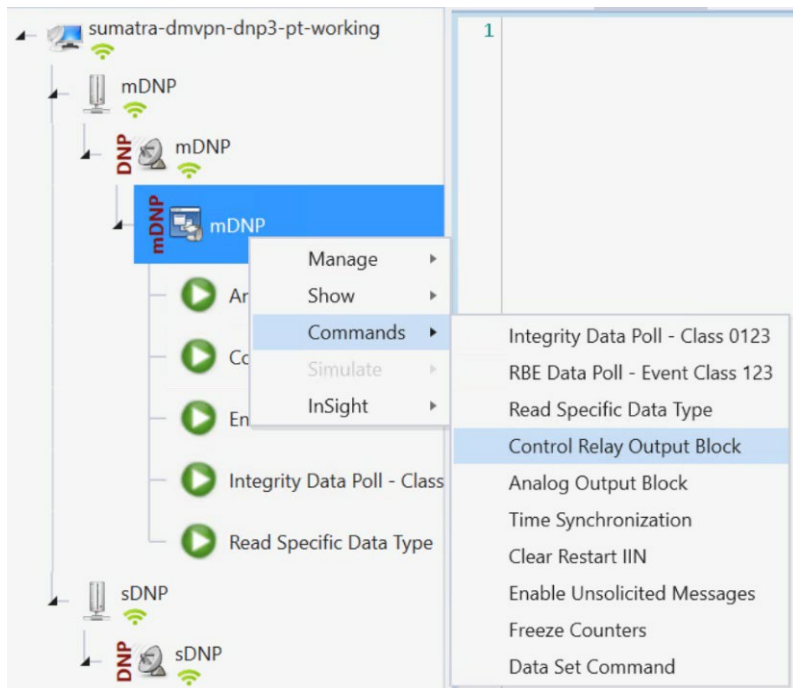
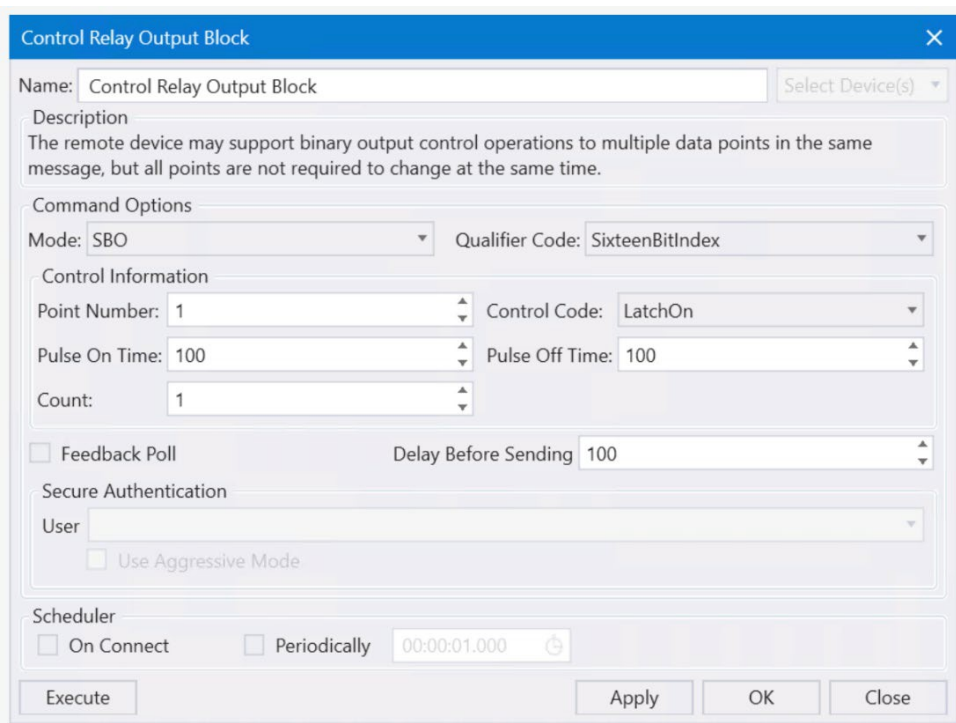


図 47 DNP3 CROB 設定ウィンドウ

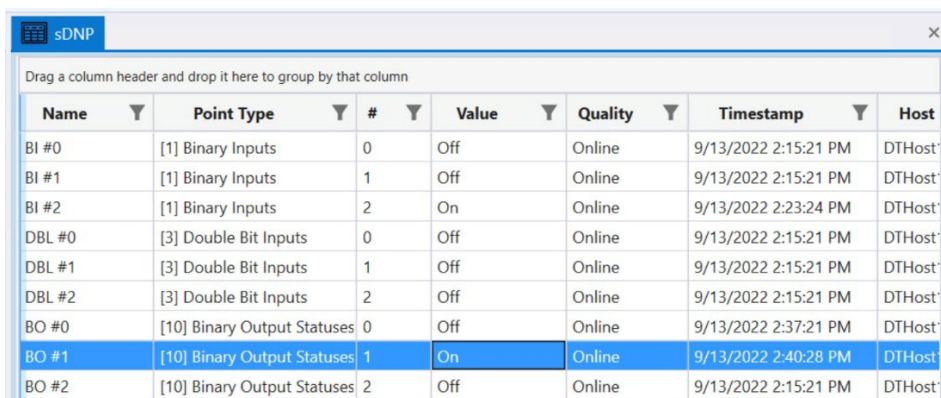


コマンド LatchOn は、上の図 47 のポイント番号 1 で実行されます。モードは SBO です。制御コードは LatchOn です。

[Apply] をクリックし、[Execute] をクリックして、Northbound DTM アプリケーションからコマンドを実行します。

図 48 に示すように、サウスバウンド TMW アプリケーションのバイナリ出力ステータスレジスタ #1 の値が OFF から ON に変更されます。

図 48 CROB コマンドで更新された DNP3 IED データポイント



Name	Point Type	#	Value	Quality	Timestamp	Host
BI #0	[1] Binary Inputs	0	Off	Online	9/13/2022 2:15:21 PM	DTHost
BI #1	[1] Binary Inputs	1	Off	Online	9/13/2022 2:15:21 PM	DTHost
BI #2	[1] Binary Inputs	2	On	Online	9/13/2022 2:23:24 PM	DTHost
DBL #0	[3] Double Bit Inputs	0	Off	Online	9/13/2022 2:15:21 PM	DTHost
DBL #1	[3] Double Bit Inputs	1	Off	Online	9/13/2022 2:15:21 PM	DTHost
DBL #2	[3] Double Bit Inputs	2	Off	Online	9/13/2022 2:15:21 PM	DTHost
BO #0	[10] Binary Output Statuses	0	Off	Online	9/13/2022 2:37:21 PM	DTHost
BO #1	[10] Binary Output Statuses	1	On	Online	9/13/2022 2:40:28 PM	DTHost
BO #2	[10] Binary Output Statuses	2	Off	Online	9/13/2022 2:15:21 PM	DTHost

SCADA イーサネット/IP の使用例

IR8340 は、次のプロトコルをサポートしています。

- IEC 60870 T104 と IEC 60870 T104 間の送受信
- DNP3 IP から DNP3 IP へ

SCADA の詳細については、次の URL にある『Cisco IR8340 SCADA Configuration Guide』を参照してください。

https://www.cisco.com/c/en/us/td/docs/routers/ir8340/software/configuration/b_ir8340_cg_17_7/m_scada.html

このセクションでは、次の SCADA DNP3 IP シナリオの実装の詳細について説明します。

サウスバウンド DNP3 TMW 設定

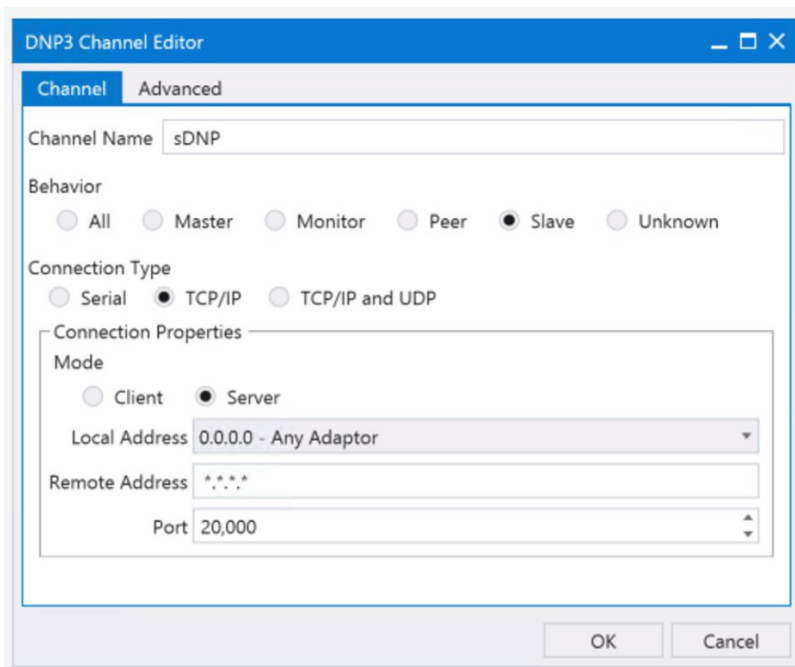
チャンネル設定

サウスバウンドイーサネット IED は、TMW ソフトウェアを使用してシミュレートされます。この例では、図 49 に示すように、ボーレート 9600 のシリアルポート COM30 が Cisco IR8340 の Async0 に接続されています。

次の手順を実行します。

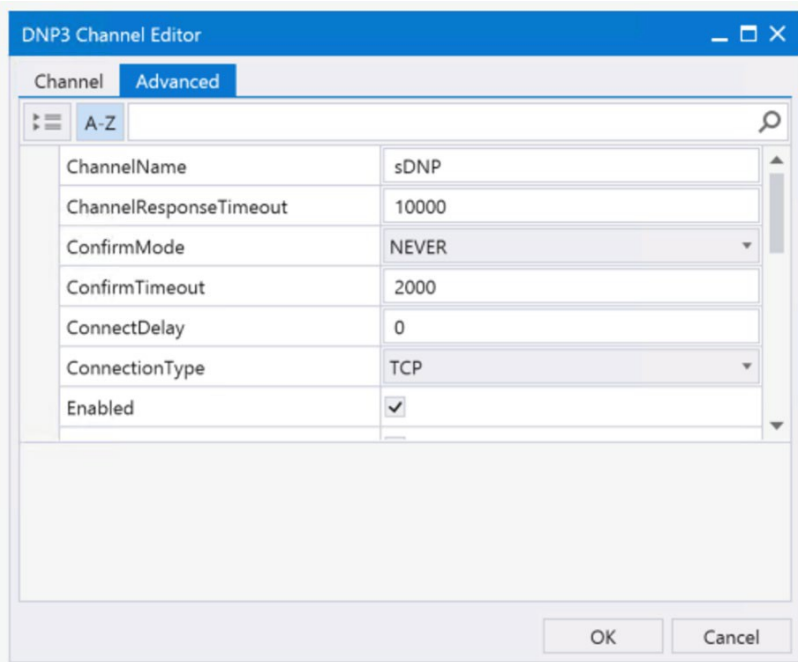
1. DNP3 IP IED チャンネルを作成します。

図 49 DNP3 IP IED チャンネルの設定



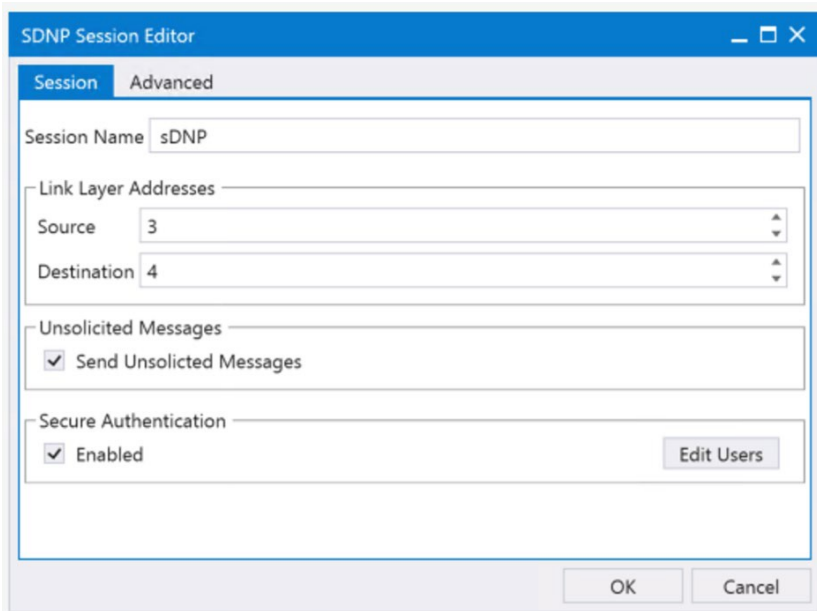
2. DNP3 IED 高度チャネルの設定を作成します。

図 50 DNP3 IP IED 高度チャネルの設定



4. DNP3 FEP セッションを作成します。DNP3 サウスバウンドシリアル RTU シミュレータは Outstation/IED として設定され、ソース層と宛先層はそれぞれ 4 と 3 として設定されます。図 51 を参照してください。

図 51 DNP3 IP IED セッションの作成



IED および DNP3 IP FEP のその他の設定は、プロトコル変換セクションで説明されているものとすべて同じです。このドキュメントのプロトコル変換セクションで説明されているように、unsolicit メッセージ、ポーリングおよび制御コマンドなどの SCADA 操作に従ってください。

追加 Scada-gw 機能

グローバル コンフィギュレーションでは、プロトコル変換の機能に使用できるさまざまな CLI があります。cli 設定については、以下を参照してください。

「scada-gw protocol force reset-link」。

RTU では、シリアル正しい初期化を確実にするために、Reset-Link メッセージを Link-status メッセージとともに送信する必要があります。この新しい設定 CLI を使用して、この機能を選択的にオンにすることができます。

新しい CLI を config に追加すると、新しい初期化シーケンスは次のようになります。

1. リンクのリセット
2. リンクステータス
3. 書き込み時間
4. 未承諾を有効にする
5. クラス 1/2/3/0

「Scada-gw protocol clock passthru」

クロックパススルーが有効になっていて、ルータが DNP3-IP マスターからタイムスタンプを受け取っていない場合は、ルータのハードウェアの時刻がダウンストリームの RTU に送信されます。DNP3-IP マスターから新しいタイムスタンプを受信すると、ルータは DNP3-IP マスターから送信された新しいタイムスタンプを RTU に送信し始めます。

「scada-gw protocol interlock」

このコマンドは、両方のプロトコルでサポートされます。DNP3-IP マスターがダウンしているか到達不能な場合、ルータはシリアルリンクを切断します。同様に、RTU へのシリアルリンクがダウンすると、DNP3-IP マスターへの TCP 接続が解除されます。

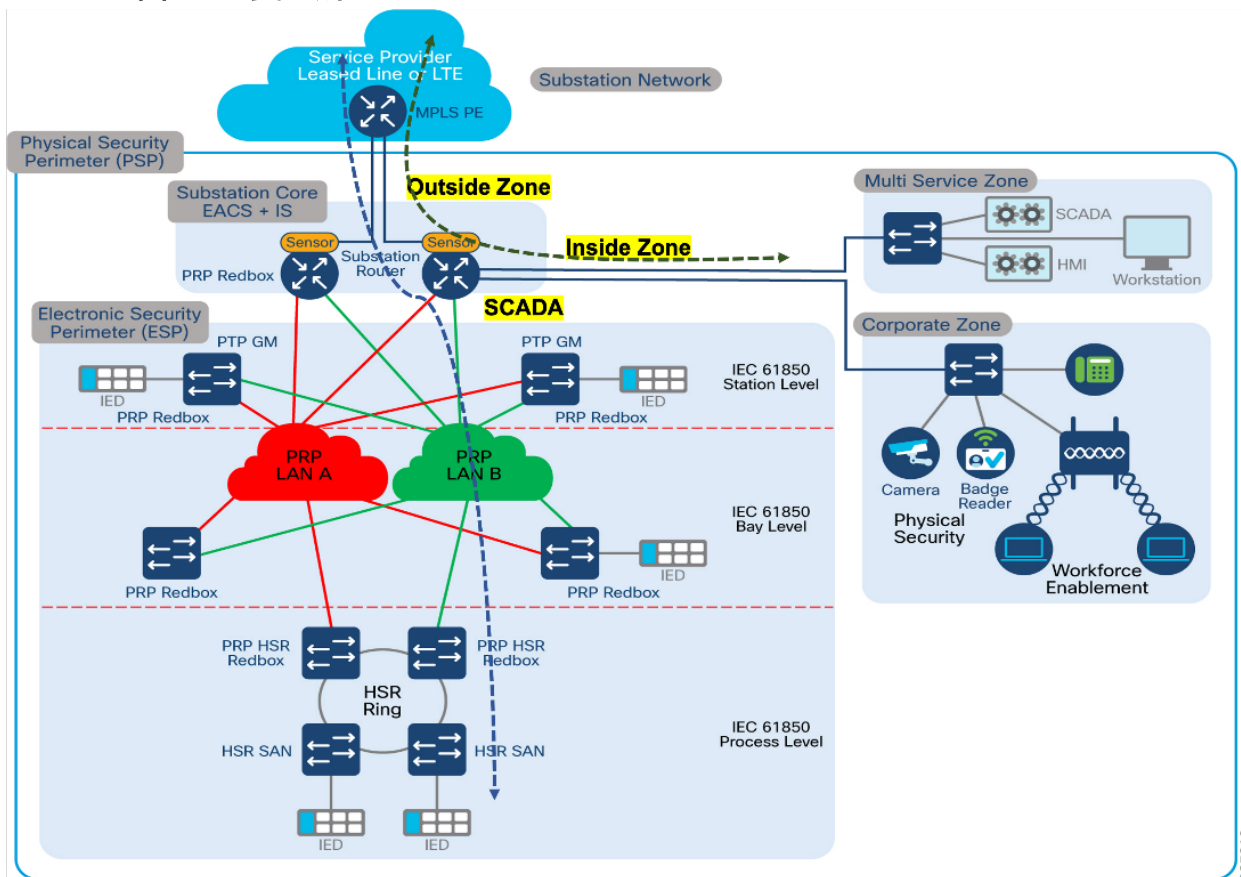
「Scada-gw protocol ignore direction」

以前は古い RTU がピアツーピアモードで使用されていた場合もあります。これらの RTU は、メッセージヘッダーのビット DIR=1 を設定することで、DNP3 シリアル下位およびプライマリのロールを動的にスワップしました。Cisco ルータで使用される ASE の SCADA スタックは、常に DNP3 シリアルプライマリとして設定されています。この場合、DIR=1 の DNP3 シリアルから受信したすべてのパケットが無視され、RTU からの多くのメッセージが廃棄されました。これらのシナリオを処理するために、新しい SCADA 設定 CLI が追加されました。この CLI を有効にすると、ルータは、DIR=1 の場合でも RTU からの着信パケットを受け入れることができます。

ゾーンベースのファイアウォールの実装

サブステーションルータから発信または通過するすべてのトラフィックは、IOS ゾーンベースのファイアウォールを有効にすることで保護できます。ゾーンベースのファイアウォール (ZBFW) IOS 機能を有効にして、不要なフローを検出およびブロックできます。ZBFW は主にセキュリティゾーンを処理します。ここでは、ルータインターフェイスをさまざまなセキュリティゾーンに割り当て、ゾーン間のトラフィックを制御できます。また、トラフィックはゾーンを通過するときに動的に検査されます。ゾーンベースのファイアウォールは、HTTP、POP3、Sun RPC、IM アプリケーション、および P2P ファイル共有のアプリケーション検査と制御をサポートします。セルラー、イーサネット、または FlexVPN トンネルなどの WAN に面するインターフェイスは外部ゾーンに配置され、IED などの LAN ネットワークデバイスおよび他の同様のエンドポイントとエッジコンピューティング アプリケーション (内部論理インターフェイス) に接続されるインターフェイスは内部ゾーンに配置されます。ゾーン間通信は拒否され、必要に応じてそのようなトラフィックを許可するファイアウォールポリシーを指定しない限り、異なるゾーンにあるインターフェイス間でトラフィックが拒否されます。

図 52 変電所のゾーンベースのファイアウォール



387910

次のファイアウォールポリシーは、外部ゾーンと内部ゾーンの間で定義されています。

- SCADA トラフィックポートを許可する必要があります。次に例を示します。
 - Modbus ポート 502
 - DNP3 ポート 20000
 - IEC 60870-5-104 ポート 2404
 - IEC 61850 MMS ポート 102。
- 変電所ルータが SCADA トラフィックの暗号化を使用する場合、トラフィックは IPSEC FlexVPN によって暗号化されます。したがって、SCADA プロトコルポートを開く必要はありません。次の IPSEC FlexVPN ポートを許可します。
 - ISAKMP : UDP 500
 - ESP : プロトコル 50
 - ISAKMP NAT トラバーサル : UDP 4500 (NAT-T)

- FND、Cyber Vision Center、その他の同様のアプリケーションなどの管理アプリケーションに必要なポートを開きます。
- ゾーン内通信が許可され、同じゾーンにあるインターフェイス間でトラフィックが暗黙的に流れます。

セカンダリ変電所ルータでゾーンベースのファイアウォールを設定するには、次の手順が必要です。

1. ゾーンを作成する前に、セキュリティの観点から見ると同様のインターフェイスをグループ化する必要があります。デフォルトでは、同じゾーン内のインターフェイス間のトラフィックはポリシーの制約を受けず、自由にゾーンを通過できます。ファイアウォールゾーンはセキュリティ機能に使用されます。
2. レイヤ3 およびレイヤ4 ファイアウォールポリシーの設定

```
!
ip access-list extended MISSION-CRITICAL-DATA-IN
  9 permit tcp host 192.168.101.2 eq 20000 host 192.168.4.171
  10 permit tcp host 192.168.101.2 eq 20001 host 192.168.4.171
  11 permit tcp host 192.168.101.2 eq 20002 host 192.168.4.171
  12 permit tcp host 192.168.101.2 eq 20003 host 192.168.4.171
  13 permit tcp host 192.168.101.2 eq 20004 host 192.168.4.171
  14 permit tcp host 192.168.101.2 eq 20005 host 192.168.4.171
  19 permit tcp host 192.168.101.2 eq 20100 host 192.168.4.171
  29 permit tcp host 192.168.101.2 eq 20200 host 192.168.4.171
  39 permit tcp host 192.168.101.2 eq 20300 host 192.168.4.171
  41 permit tcp host 192.168.211.2 host 192.168.2.206 eq 502
  50 permit udp any any
  70 permit icmp 192.168.101.0 0.0.0.255 host 192.168.4.171
```

```
!
ip access-list extended MISSION-CRITICAL-DATA-OUT
  9 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20000
  10 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20001
  11 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20002
  12 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20003
  13 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20004
  14 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20005
  19 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20100
  29 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20200
  39 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20300
  41 permit tcp host 192.168.2.206 host 192.168.211.2 eq 502
```

```

50 permit udp any any
70 permit icmp 192.168.101.0 0.0.0.255 host 192.168.4.171
!

!
ip access-list extended FTP_IN_OUT
1 permit tcp 192.168.110.0 0.0.0.255 host 192.168.2.176 eq ftp log
2 permit tcp host 192.168.199.2 host 192.168.2.176 eq ftp log
3 permit tcp host 192.168.199.2 host 192.168.2.206 eq ftp
13 permit tcp 50.1.0.0 0.0.0.255 host 192.168.2.176 eq ftp log
!

!
ip access-list extended FTP_OUT_IN
1 permit tcp host 192.168.2.176 192.168.110.0 0.0.0.255 eq ftp
2 permit tcp host 192.168.2.176 host 192.168.199.2 eq ftp
3 permit tcp host 192.168.2.206 host 192.168.199.2 eq ftp
!

!
class-map type inspect match-any IN-IN
    match protocol ssh
    match protocol tcp
    match protocol udp
    match protocol icmp
    match protocol https
    match protocol http
    match protocol login
class-map type inspect match-any OUT-SCADA
    match protocol ntp
    match protocol ssh
    match protocol syslog
    match protocol icmp
    match access-group name MISSION-CRITICAL-DATA-OUT
    match protocol snmp
class-map type inspect match-any SCADA-OUT
    match protocol ntp
    match protocol ssh
    match protocol syslog
    match protocol icmp
    match access-group name MISSION-CRITICAL-DATA-IN
class-map type inspect match-any IN-OUT
    match protocol icmp
    match protocol telnet
    match protocol http

```

```

match protocol https
match protocol ssh
match protocol syslog
match protocol udp
match access-group name FTP_IN_OUT
match protocol tcp
match access-group 102
match protocol login
class-map type inspect match-any OUT-IN
match protocol icmp
match protocol telnet
match protocol http
match protocol https
match protocol ssh
match protocol syslog
match access-group name FTP_OUT_IN
match protocol tcp
match access-group 102
match protocol udp
match protocol snmp
!

```

3. セキュリティゾーンとゾーンペアを作成します。

```

!
zone security INSIDE
zone security OUTSIDE
zone security SCADA
zone-pair security IN-IN-PAIR source INSIDE destination INSIDE
service-policy type inspect IN-IN
zone-pair security IN-OUT-PAIR source INSIDE destination OUTSIDE
service-policy type inspect IN-OUT
zone-pair security OUT-IN-PAIR source OUTSIDE destination INSIDE
service-policy type inspect OUT-IN
zone-pair security OUT-SCADA-PAIR source OUTSIDE destination SCADA
service-policy type inspect OUT-SCADA
zone-pair security SCADA-OUT-PAIR source SCADA destination OUTSIDE
service-policy type inspect SCADA-OUT
!

```

4. インターフェイスをそれぞれのゾーンに割り当てます。この例では、GigabitEthernet0/0/0 が OUTSIDE インターフェイスです。VLAN 101、VLAN 501、VLAN 110、VLAN201 は INSIDE インターフェイスです。

```

!
interface GigabitEthernet0/0/0
description connected to asr903-003
ip flow monitor StealthWatch_Monitor input
ip address 192.168.100.1 255.255.255.0
zone-member security OUTSIDE
ip ospf network point-to-point
load-interval 30
negotiation auto
bfd interval 50 min_rx 50 multiplier 3
end
!
!
interface Vlan101
ip address 192.168.101.1 255.255.255.0
zone-member security SCADA
load-interval 30
service-policy input HOST-INPUT-MARKING
end
!
interface Vlan201
ip address 192.168.211.1 255.255.255.0
zone-member security SCADA
load-interval 30
vrrp 1 name MODBUS-IED-1
vrrp 1 ip 192.168.211.100
vrrp 1 timers learn
vrrp 1 priority 200
service-policy input HOST-INPUT-MARKING
end
!
interface Vlan501
description REP-Mgmt
ip address 50.1.0.1 255.255.255.0
zone-member security INSIDE
standby 0 ip 50.1.0.100
standby 0 timers msec 30 msec 120
standby 0 priority 200
standby 0 preempt
load-interval 30
service-policy input TEST_MGMT_TRAFFIC
end
!
interface Vlan1051
description HSRP-GRP-1

```



```
ip address 192.168.110.2 255.255.255.0
zone-member security INSIDE
standby 1 ip 192.168.110.1
standby 1 priority 10
standby 1 preempt
standby 1 track 100 decrement 10
bfd interval 999 min_rx 999 multiplier 3
```

!

5. この機能の機能は、次のコマンドを使用して確認できます。

```
Router#show policy-map type inspect zone-pair sessions
Zone-pair: IN-IN-PAIR
Service-policy inspect : IN-IN
```

```
Class-map: IN-IN (match-any)
Match: protocol ssh
Match: protocol tcp
Match: protocol udp
Match: protocol icmp
Match: protocol https
Match: protocol http
Match: protocol login
Inspect
```

```
Class-map: class-default (match-any)
Match: any
Drop (default action)
0 packets, 0 bytes
Zone-pair: IN-OUT-PAIR
Service-policy inspect : IN-OUT
```

```
Class-map: IN-OUT (match-any)
Match: protocol icmp
Match: protocol telnet
Match: protocol http
Match: protocol https
Match: protocol ssh
Match: protocol syslog
Match: protocol udp
Match: access-group name FTP_IN_OUT
Match: protocol tcp
Match: access-group 102
Match: protocol login
```

Inspect

Established Sessions

Session ID 0x00009B76 (192.168.110.7:8)=>(192.168.2.108:42999)
icmp SIS_OPEN
Created 00:00:07, Last heard 00:00:07
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B79 (192.168.110.6:8)=>(192.168.2.176:39395)
icmp SIS_OPEN
Created 00:00:03, Last heard 00:00:03
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B7C (192.168.110.5:8)=>(192.168.2.108:39409)
icmp SIS_OPEN
Created 00:00:02, Last heard 00:00:02
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B70 (192.168.110.8:8)=>(192.168.2.176:48757)
icmp SIS_OPEN
Created 00:00:28, Last heard 00:00:28
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B5E (50.1.0.2:8)=>(192.168.2.176:45393)
icmp/icmp SIS_OPEN
Created 00:01:01, Last heard 00:01:01
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B71 (192.168.110.8:8)=>(192.168.2.108:48758)
icmp SIS_OPEN
Created 00:00:28, Last heard 00:00:28
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B63 (192.168.110.51:8)=>(192.168.2.176:39731)
icmp SIS_OPEN
Created 00:00:53, Last heard 00:00:53
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B56 (192.168.110.6:8)=>(192.168.2.108:39392)
icmp SIS_OPEN
Created 00:01:02, Last heard 00:01:02
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B66 (50.1.0.3:8)=>(192.168.2.176:46126)
icmp/icmp SIS_OPEN
Created 00:00:38, Last heard 00:00:38
Bytes sent (initiator:responder) [36:36]
Session ID 0x00000000 (192.168.110.5:54555)=>(192.168.2.206:514)
syslog SIS_OPEN
Created 21:33:57, Last heard 00:00:01
Bytes sent (initiator:responder) [427019:0]
Session ID 0x00009B67 (192.168.110.7:8)=>(192.168.2.176:42996)
icmp SIS_OPEN
Created 00:00:37, Last heard 00:00:37

Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B60 (192.168.110.8:8)=>(192.168.2.108:48756)
icmp SIS_OPEN
Created 00:00:58, Last heard 00:00:57
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B75 (192.168.110.7:8)=>(192.168.2.176:42998)
icmp SIS_OPEN
Created 00:00:07, Last heard 00:00:07
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B7B (192.168.110.5:8)=>(192.168.2.176:39408)
icmp SIS_OPEN
Created 00:00:02, Last heard 00:00:02
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B6C (192.168.110.6:8)=>(192.168.2.108:39394)
icmp SIS_OPEN
Created 00:00:33, Last heard 00:00:33
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B6B (192.168.110.6:8)=>(192.168.2.176:39393)
icmp SIS_OPEN
Created 00:00:33, Last heard 00:00:33
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B68 (192.168.110.7:8)=>(192.168.2.108:42997)
icmp SIS_OPEN
Created 00:00:37, Last heard 00:00:37
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B74 (50.1.0.3:8)=>(192.168.2.176:46127)
icmp/icmp SIS_OPEN
Created 00:00:09, Last heard 00:00:09
Bytes sent (initiator:responder) [36:36]
Session ID 0x00000024 (50.1.0.7:53458)=>(192.168.2.211:2055) udp
SIS_OPEN
Created 21:32:44, Last heard 00:00:02
Bytes sent (initiator:responder) [260604:0]
Session ID 0x00009B7D (50.1.0.2:8)=>(192.168.2.176:45395)
icmp/icmp SIS_OPEN
Created 00:00:01, Last heard 00:00:01
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B6D (192.168.110.5:8)=>(192.168.2.176:39406)
icmp SIS_OPEN
Created 00:00:32, Last heard 00:00:32
Bytes sent (initiator:responder) [36:36]
Session ID 0x00009B7A (192.168.110.6:8)=>(192.168.2.108:39396)
icmp SIS_OPEN
Created 00:00:03, Last heard 00:00:03
Bytes sent (initiator:responder) [36:36]

Session ID 0x00009B64 (192.168.110.51:8)=>(192.168.2.108:39732)
 icmp SIS_OPEN
 Created 00:00:53, Last heard 00:00:53
 Bytes sent (initiator:responder) [36:36]
 Session ID 0x00009B5C (192.168.110.5:8)=>(192.168.2.108:39405)
 icmp SIS_OPEN
 Created 00:01:02, Last heard 00:01:02
 Bytes sent (initiator:responder) [36:36]
 Session ID 0x00000001 (192.168.110.5:50579)=>(192.168.5.11:514)
 syslog SIS_OPEN
 Created 21:33:57, Last heard 00:00:01
 Bytes sent (initiator:responder) [427019:0]
 Session ID 0x00009B6E (192.168.110.5:8)=>(192.168.2.108:39407)
 icmp SIS_OPEN
 Created 00:00:32, Last heard 00:00:32
 Bytes sent (initiator:responder) [36:36]
 Session ID 0x00009B73 (192.168.110.51:8)=>(192.168.2.108:39734)
 icmp SIS_OPEN
 Created 00:00:24, Last heard 00:00:24
 Bytes sent (initiator:responder) [36:36]
 Session ID 0x00009B5F (192.168.110.8:8)=>(192.168.2.176:48755)
 icmp SIS_OPEN
 Created 00:00:58, Last heard 00:00:58
 Bytes sent (initiator:responder) [36:36]
 Session ID 0x00009B6F (50.1.0.2:8)=>(192.168.2.176:45394)
 icmp/icmp SIS_OPEN
 Created 00:00:31, Last heard 00:00:31
 Bytes sent (initiator:responder) [36:36]
 Session ID 0x00009B72 (192.168.110.51:8)=>(192.168.2.176:39733)
 icmp SIS_OPEN
 Created 00:00:24, Last heard 00:00:24
 Bytes sent (initiator:responder) [36:36]
 Session ID 0x00009B5B (192.168.110.5:8)=>(192.168.2.176:39404)
 icmp SIS_OPEN
 Created 00:01:02, Last heard 00:01:02
 Bytes sent (initiator:responder) [36:36]

Class-map: class-default (match-any)

Match: any

Drop (default action)

0 packets, 0 bytes

Zone-pair: OUT-IN-PAIR

Service-policy inspect : OUT-IN

```

Class-map: OUT-IN (match-any)
  Match: protocol icmp
  Match: protocol telnet
  Match: protocol http
  Match: protocol https
  Match: protocol ssh
  Match: protocol syslog
  Match: access-group name FTP_OUT_IN
  Match: protocol tcp
  Match: access-group 102
  Match: protocol udp
  Match: protocol snmp
Inspect
  Established Sessions
    Session ID 0x00009B77 (192.168.2.108:8)=>(50.1.0.2:24433) icmp
SIS_OPEN
  Created 00:00:35, Last heard 00:00:35
  Bytes sent (initiator:responder) [36:36]
    Session ID 0x00009B69 (192.168.2.108:8)=>(50.1.0.3:24429) icmp
SIS_OPEN
  Created 00:01:05, Last heard 00:01:05
  Bytes sent (initiator:responder) [36:36]
    Session ID 0x0000000D (192.168.2.108:2530)=>(50.1.0.7:2530) udp
SIS_OPEN
  Created 21:33:55, Last heard 00:00:05
  Bytes sent (initiator:responder) [41856:41856]
    Session ID 0x00009B78 (192.168.2.108:8)=>(50.1.0.3:24434) icmp
SIS_OPEN
  Created 00:00:35, Last heard 00:00:35
  Bytes sent (initiator:responder) [36:36]
    Session ID 0x00009B87 (192.168.2.108:8)=>(50.1.0.2:24436) icmp
SIS_OPEN
  Created 00:00:05, Last heard 00:00:05
  Bytes sent (initiator:responder) [36:36]
    Session ID 0x00009B86 (192.168.2.108:8)=>(50.1.0.3:24435) icmp
SIS_OPEN
  Created 00:00:05, Last heard 00:00:05
  Bytes sent (initiator:responder) [36:36]
    Session ID 0x0000000B (192.168.2.108:2530)=>(50.1.0.7:1967) udp
SIS_OPEN
  Created 21:33:55, Last heard 00:00:05
  Bytes sent (initiator:responder) [136292:62784]
    Session ID 0x00009B6A (192.168.2.108:8)=>(50.1.0.2:24430) icmp
SIS_OPEN
  Created 00:01:05, Last heard 00:01:05

```

Bytes sent (initiator:responder) [36:36]

Class-map: class-default (match-any)

Match: any

Drop (default action)

0 packets, 0 bytes

Zone-pair: OUT-SCADA-PAIR

Service-policy inspect : OUT-SCADA

Class-map: OUT-SCADA (match-any)

Match: protocol ntp

Match: protocol ssh

Match: protocol syslog

Match: protocol icmp

Match: access-group name MISSION-CRITICAL-DATA-OUT

Match: protocol snmp

Inspect

Established Sessions

Session	ID	0x00009B5A
(192.168.4.171:49366)=>(192.168.101.2:20100) tcp SIS_OPEN		
Created 00:01:32, Last heard 00:00:29		
Bytes sent (initiator:responder) [139:1739]		
Session	ID	0x00009B42
(192.168.4.171:49349)=>(192.168.101.2:20002) tcp SIS_OPEN		
Created 00:01:46, Last heard 00:00:41		
Bytes sent (initiator:responder) [139:1739]		
Session	ID	0x00009B57
(192.168.4.171:49363)=>(192.168.101.2:20005) tcp SIS_OPEN		
Created 00:01:32, Last heard 00:00:29		
Bytes sent (initiator:responder) [139:1739]		
Session	ID	0x00009B4A
(192.168.4.171:49357)=>(192.168.101.2:20003) tcp SIS_OPEN		
Created 00:01:40, Last heard 00:00:37		
Bytes sent (initiator:responder) [139:1739]		
Session	ID	0x00009B44
(192.168.4.171:49351)=>(192.168.101.2:20001) tcp SIS_OPEN		
Created 00:01:46, Last heard 00:00:41		
Bytes sent (initiator:responder) [139:1739]		
Session	ID	0x00009B41
(192.168.4.171:49348)=>(192.168.101.2:20000) tcp SIS_OPEN		
Created 00:01:47, Last heard 00:00:41		
Bytes sent (initiator:responder) [139:1739]		
Session	ID	0x00009B58
(192.168.4.171:49364)=>(192.168.101.2:20004) tcp SIS_OPEN		

```
Created 00:01:32, Last heard 00:00:29
Bytes sent (initiator:responder) [139:1739]
Session ID 0x00009B65
(192.168.4.171:49375)=>(192.168.101.2:20300) tcp SIS_OPEN
Created 00:01:19, Last heard 00:00:17
Bytes sent (initiator:responder) [139:1739]
Session ID 0x00009B61
(192.168.4.171:49368)=>(192.168.101.2:20200) tcp SIS_OPEN
Created 00:01:26, Last heard 00:00:22
Bytes sent (initiator:responder) [166:2566]
```

```
Class-map: class-default (match-any)
Match: any
Drop (default action)
0 packets, 0 bytes
Zone-pair: SCADA-OUT-PAIR
Service-policy inspect : SCADA-OUT
```

```
Class-map: SCADA-OUT (match-any)
Match: protocol ntp
Match: protocol ssh
Match: protocol syslog
Match: protocol icmp
Match: access-group name MISSION-CRITICAL-DATA-IN
Inspect
```

```
Class-map: class-default (match-any)
Match: any
Drop (default action)
0 packets, 0 bytes
Router#
```

QoS の実装

Quality of Service (QoS) とは、選択したネットワークトラフィックに優先サービスを提供するネットワークの機能を指します。以下により、さらに改善され、予測可能なネットワークサービスを提供することができます。

- 専用帯域幅のサポート：セルラーリンクのアップロード/ダウンロード帯域幅/スループットは異なります

- 損失特性の削減：変電所のリアルタイムトラフィックの優先順位付け
- ネットワークの輻輳の回避と管理：マルチサービストラフィック
- ネットワーク全体でのトラフィックの優先順位の設定：マルチサービス機能

IED、リモートワークフォース、およびネットワーク管理の使用例からのトラフィックを区別して優先順位を付ける必要があるため、マルチサービス変電所自動化ソリューションを設計する場合、QoS は重要な機能です。機密データを転送する場合、特に WAN バックホールリンクが提供する帯域幅が限定されている場合は、ネットワークデバイスによって生じる推定伝送損失、遅延、ジッターを理解しておく必要があります。

異なる帯域幅機能（セルラー）を持つデュアル WAN インターフェイスの場合、QoS ポリシーを適用して、これらの制限された帯域幅リンクを通過できるトラフィックに優先順位を付けたり、ドロップできるトラフィックを決定したりする必要があります。

マルチサービス変電所ソリューションでは、QoS DiffServ および CoS (IEEE 802.1p) を次のように分類されるトラフィックに適用できます。

- IPv4 トラフィック：変電所トラフィック、プロトコル変換 (RTU モニタリング)、およびネットワーク管理
- レイヤ 2 トラフィック：イーサネット インターフェイス間の IEC 61850 GOOSE/SV トラフィックスイッチや、変電所間の WAN リンクを介してブリッジされる IEC 61850 トラフィックなどの変電所自動化。

Substation Lan QoS については、次の「Substation LAN Cisco Validated Design」を参照してください。<https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Utilities/SA/2-3-2/CU-2-3-2-DIG/CU-2-3-2-DIG.html#pgfId-234948>

レイヤ 3（セルラー、イーサネット）インターフェイスでの変電所ルータ QoS アクション。出力トラフィックに対する QoS アクションのシーケンスは次のようになります。

1. 分類
2. マーキング
3. キューイング

以下は、変電所ソリューションでの QOS 実装に必要な構成です。DSCP マーキングとアクセスリストは、優先順位付けのためにトラフィックを照合するために使用されます。

Class-map Configurations,

```
!  
class-map match-any MISSION-CRITICAL  
  match ip dscp af31 af32 af33 af43  
class-map match-all CALL-SIGNALING  
  match ip dscp cs3  
class-map match-any TRANSACTIONAL  
  match ip dscp cs2 af21 af22 af23 cs4 af41 af42  
class-map match-all VOICE  
  match ip dscp ef  
class-map match-any MISSION-CRITICAL-DATA  
  match access-group name MISSION-CRITICAL-DATA
```

!

!

Policy-map Configurations,

!

```
policy-map HOST-INPUT-MARKING  
  class VOICE  
    set dscp ef  
  class CALL-SIGNALING  
    set dscp cs3  
  class MISSION-CRITICAL-DATA  
    set dscp af31  
  class TRANSACTIONAL  
    set dscp af21  
  class class-default
```

```
policy-map HOST-QUEUE-PACKETS  
  class VOICE  
    bandwidth remaining percent 30  
    queue-limit 96 packets  
  class TRANSACTIONAL  
    bandwidth remaining percent 20  
    queue-limit 96 packets  
  class MISSION-CRITICAL  
    priority  
  class class-default  
    bandwidth remaining percent 25  
    queue-limit 272 packets
```

上記のポリシーマップは、出力トラフィック（プライオリティキューイング、分類）の WAN（セルラー/イーサネット）インターフェイスに適用できます。

```
interface Cellular 0/4/0
service-policy output HOST-QUEUE-PACKETS
```

次のコマンドを使用して、WAN インターフェイスに適用されている QOS ポリシーを確認できます。これにより、クラス/ポリシーマップの設定に基づいて分類されたトラフィックの packets 数が表示されます。

```
Router#sh policy-map interface g 0/0/0 output
GigabitEthernet0/0/0
```

```
Service-policy output: HOST-QUEUE-PACKETS
queue stats for all priority classes:
```

```
Queueing
queue limit 512 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
```

```
Class-map: VOICE (match-all)
```

```
634 packets
30 second offered rate 0000 bps, drop rate 0000 bps
Match: ip dscp ef (46)
Queueing
queue limit 96 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
bandwidth remaining 30%
```

```
Class-map: TRANSACTIONAL (match-any)
```

```
125 packets
30 second offered rate 0000 bps, drop rate 0000 bps
Match: ip dscp cs2 (16) af21 (18) af22 (20) af23 (22) cs4 (32) af41 (34)
af42 (36)
Queueing
queue limit 96 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
bandwidth remaining 20%
```

```
Class-map: MISSION-CRITICAL (match-any)
```

```
1534 packets
30 second offered rate 0000 bps, drop rate 0000 bps
Match: ip dscp af31 (26) af32 (28) af33 (30) af43 (38)
Priority: Strict, b/w exceed drops: 0
```

```
Class-map: class-default (match-any)
  24560 packets, 450 bytes
  30 second offered rate 0000 bps, drop rate 0000 bps
  Match: any
  Queueing
    queue limit 272 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
    bandwidth remaining 25%
```

ネットワーク管理

SDWAN を使用した IR8340 管理

Substation Automation LAN 展開用の Cisco SD-WAN は、Cisco SD-WAN End-to-End Deployment Guide に基づいており、SD-WAN エッジルータとして Cisco IR8340 を使用するようにその範囲を拡大しています。この実装は、Cisco クラウド管理サービスで実行されるコントローラをサポートします。

前提条件

- このガイドは、ユーザーが Cisco SD-WAN コントローラをすでにインストールしていることを前提としています。インストールの詳細については、次のリソースを参照してください：
 - オンプレミス展開：
<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/cisco-sd-wan-overlay-network-bringup.html>
 - クラウド展開：
<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/knowledge-base/cloudops.html>
- データセンターおよびエンタープライズ ブランチ サイトは、Cisco SD-WAN エンドツーエンド導入ガイドに従ってすでに設定されています。
- Cisco WAN エッジルータが設置され、設定の準備が整いました。IOS XE SD-WAN ルータがすでに IOS XE から SD-WAN コードに変換されていること。
- Cisco WAN エッジルータに隣接するデバイスが設定されていること。
- vBond IP アドレスまたはホスト名は、vManage 管理設定で設定する必要があります。

- vSmart はテンプレートに添付されています。
- SDWAN イメージは、最初からすべてのモジュールをサポートしていない可能性があります。サポートされているモジュールについては、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。

IR8340 のオンボーディング

SD-WAN ネットワークに接続するルータを起動するには、次の 3 つの方法があります。

- ゼロタッチ展開のための PnP。
- 静的 IP 設定またはデフォルト以外のセルラープロファイルでトランスポートに接続されているデバイスなど、追加の設定なしではインターネット接続を取得できないデバイス用のブートストラップ。
- CLI、コンソール経由での手動設定の追加

これらの方法について、以下で説明します。

オンボーディング前

WAN エッジデバイスがオーバーレイに参加してアクティブになるには、有効で承認されたシリアル番号ファイルを vManage にアップロードする必要があります。この認定シリアル番号ファイルには、ネットワークで許可されているすべての WAN エッジルータのシリアル番号とシャーシ番号が示されます。vManage はこのファイルをコントローラに送信します。また、このリストのシリアル番号に一致するデバイスのみがコントローラによって検証され、正常に認証されます。

IOS XE SD-WAN ルータの認証済みシリアル番号は、プラグアンドプレイ (PnP) 接続ポータルから取得します。PnP Connect ポータルは、ネットワークデバイスのオンボーディングを自動化し、手動の介入なしで構成設定を適用するためにも使用されます。

このガイドでは、スマートアカウントを使用して PnP Connect にデバイスを追加し、vBond プロファイルに関連付けるために必要な手順を説明します。PnP 接続の理解を深めるには、次のリンクを参照してください。

<https://www.cisco.com/c/en/us/products/collateral/software/smart-accounts/guide-c07-744931.html#4Deploymentoptions>

PnP Connect でのデバイスの追加

スマートアカウントとバーチャルアカウントが Cisco Commerce Workspace の注文に追加されている場合、デバイスを PnP Connect に自動的に追加できます。調達プロセスでデバイスが追加されていない場合は、次の手順に従います。

1. `show crypto pki certificates CISCO_IDEVID_SUDI` コマンドを使用して、デバイスからシリアル番号と証明書のシリアル番号を取得します。

```
Router# show crypto pki certificates CISCO_IDEVID_SUDI
Certificate
  Status: Available
  Certificate Serial Number (hex): XXXXXXXXXX
  Certificate Usage: General Purpose
  Issuer:
    o=Cisco
    cn=High Assurance SUDI CA
  Subject:
    Name: IR8340-K9
    Serial Number: PID:IR8340-K9 SN:XXXXXXXXXX
    cn=IR8340-K9
    ou=ACT-2 Lite SUDI
    o=Cisco
    serialNumber=PID:IR8340-K9 SN:XXXXXXXXXX
  Validity Date:
    start date: 10:11:36 UTC Feb 8 2021
    end date: 20:58:26 UTC Aug 9 2099
  Associated Trustpoints: CISCO_IDEVID_SUDI
```

2. <https://software.cisco.com> に移動します。
3. [Network Plug and Play] セクションで、[Plug and Play Connect] リンクをクリックします。
4. 右上隅で正しいバーチャルアカウントが選択されていることを確認します。
5. [Add Device] ボタンをクリックします。

6. [Enter Device Info Manually] ラジオボタンを選択します。または、コンマ区切り値 (CSV) ファイルをアップロードすることもできます。
7. [Next] をクリックします。
8. [Identify Device] ボタンをクリックします。
9. 手順 1 で取得したシリアル番号、ベース PID (IR8340-K9) 、および選択した vBond コントローラプロファイルを入力します。
10. [Save] をクリックします。ウィザード画面を開くには、[Next] をクリックします。
11. [Review & Submit] で、[Submit] をクリックします。
12. [Done] をクリックします。
13. ルータが追加されると、デバイスのリストが表示されます。最近追加されたデバイスを選択し、[Edit Selected] をクリックします。
14. デバイスの [Certificate Serial Number] 列の下のスペースをクリックし、ステップ 1 の情報を入力します。
15. [Submit] をクリックします。
16. デバイスは、保留中(リダイレクト)を示す黄色のステータスで表示されます。デバイスが PnP 自動オンボーディングプロセスを使用してオンボーディングされている場合、この状態は [Redirect Successful] に変わります。それ以外の場合は、現在の状態のままになります。

承認された WAN エッジシリアル番号を vManage にロードする

承認されたデバイスを vManage にアップロードするには、2 つの方法があります。

方法 1：スマートアカウントとの同期

1. vManage GUI で、[**Configuration > Devices**] に移動します。
2. [WANエッジリスト (WAN Edge List)] タブが選択されていることを確認します。
3. [Sync Smart Account] をクリックします。ユーザー名とパスワードの入力を求めるウィンドウが開きます。
4. シスコ Web サイトのユーザー名およびパスワードを入力します。アップロードされたリストを検証するチェックボックスは、デフォルトでオンになっています。

5. [同期 (Sync)] をクリックします。ステータスが成功と表示されるまで待機します。

注：PNP ポータルに追加された新しいデバイスについては、vManage をスマートアカウント/仮想アカウントと再同期する必要があります。

方法 2：ファイルを手動でアップロードする

1. <https://software.cisco.com> に移動します。
2. [Network Plug and Play] セクションで、[Plug and Play Connect] リンクをクリックします。
3. 右上隅で正しいバーチャルアカウントが選択されていることを確認します。
4. [Controller Profiles] テキストをクリックします。
5. 正しいコントローラプロファイルの横にある [Provisioning File text] をクリックします。
6. ポップアップウィンドウで、ドロップダウンリストからコントローラのバージョンを選択します。[18.3 and newer] を選択します。[Download] ボタンをクリックしてファイルをコンピュータに保存します。
7. vManage GUI で、左側のパネルの [Configuration > Devices] に移動します。
8. [WAN エッジリスト (WAN Edge List)] タブが選択されていることを確認します。
9. [Upload WAN Edge List] ボタンをクリックします。ポップアップウィンドウが表示されます。ファイルを選択します。
10. リストを検証してコントローラに送信するには、チェックボックスをオンにします。[Upload] をクリックします。[Validate] を選択しないと、すべてのデバイスが無効として表示され、ネットワーク上で起動してオーバーレイに参加する場合は、個別に有効に変更する必要があります。
11. 表示される確認ボックスで [OK] を選択します。
12. リストが正常にアップロードされ、正常にアップロードされたルータの数を通知するポップアップウィンドウが開きます。[OK] を選択します。

リストが vBond および vSmart コントローラに正常にプッシュされたことを示すページが表示されます。

デバイスをテンプレートに関連付ける

デバイスをデバイステンプレートに関連付けると、構成がデバイスに関連付けられます。

このプロセス中に、テンプレートのすべての変数に値を割り当てる必要があります。

1. [Configuration > Templates] に移動します。
2. [Device] タブで、使用するテンプレートを特定します。
3. 行の右側にあるその他のアクション (...) アイコンをクリックし、[Attach Devices] をクリックします。[Attach Devices] ダイアログボックスが開きます。
4. 左側の [Available Devices] 列で、グループを選択して 1 つ以上のデバイスを検索するか、リストからデバイスを選択するか、[Select All] をクリックします。
5. 右向きの矢印をクリックして、デバイスを右側の [Selected Devices] 列に移動します。
6. [Attach] をクリックします。
7. 完全な設定を作成およびプッシュするには、最初にデバイステンプレートに関連付けられたフィーチャーテンプレートに関連付けるすべての変数を定義する必要があります。これを行うには、GUI 内で変数の値を手動で入力するか、変数とその値のリストを含む CSV ファイルをアップロードする方法の 2 つがあります。各オプションの詳細な手順は、このセクションの最後に記載されています。
8. [Next] ボタンをクリックします。次の画面では、設定アクションがテンプレートに接続されたデバイスに適用されることが示されます。
9. (オプション) 左側のデバイスを選択して、[Config Preview] タブの IOS XE SD-WAN ルータにプッシュされる設定を表示します。
10. (オプション) 画面の上部にある [Config Diff] タブを選択して、現在のローカル設定と、プッシュしようとしている新しい設定の違いを確認します。

11. (オプション) ロールバックタイマーを表示または変更するには、左下隅にある [Configure Device Rollback Timer] テキストを選択できます。ロールバックタイマーは保護メカニズムです。設定の変更後にルータに到達できない場合は、以前の設定にロールバックします。タイマーは 6 ~ 15 分の任意の値に設定できます。それを無効にすることを推奨します。[Save] または [Cancel] をクリックして、メインウィンドウに戻ります。
12. [Configure Devices] を選択します。複数のデバイスを設定する場合、ポップアップウィンドウは、複数のデバイスへの変更をコミットすることを警告します。デバイスの設定の変更を確認するチェックボックスをオンにします。[OK] を選択します。次に、設定がデバイスにプッシュされます。完了すると、vManage は Done-Scheduled ステータスを表示し、デバイスはオフラインですが、接続が確立されたときにテンプレートがプッシュされるようにスケジュールされていることを示します。
13. (オプション) デバイステンプレートに関連付けられたデバイスを表示するには、[Configuration > Template] の順に移動します。[Device] タブでテンプレートを特定し、接続されているデバイスの数を示す [Device Attached] 列をクリックします。ポップアップウィンドウに、接続されているデバイスが表示されます。

ブートストラップ設定ファイルの生成

この手順は、次のセクションで説明するブートストラップ方法を使用してデバイスをオンボーディングする場合にのみ必要です。

1. vManage で、[Configuration > Devices] の順に移動します。
2. 該当するデバイスの行の右側にある [その他のアクション] アイコン (...) をクリックし、[Generate Bootstrap Configuration] を選択します。
3. 開いたダイアログボックスで、[Cloud-init] ラジオボタンが選択されていることを確認し、[OK] をクリックします。
4. ファイルが生成され、その内容がポップアップウィンドウに表示されます。
5. [Download] をクリックします。

6. ファイルの名前を `ciscosdwan.cfg` に変更します（大文字と小文字が区別されます）。
7. `ciscosdwan.cfg` ファイルをブート可能な USB ドライブまたはデバイスのブートフラッシュにコピーします。ファイルには、表示されているとおり名前を付ける必要があります。そうしないと、デバイスがファイルを読み取れません。

方法：プラグアンドプレイ

デバイスが以下の要件を満たしている場合、デバイスは起動し、PNP Connect ポータルにアクセスして vBond IP アドレスを取得します。ルータは vBond への安全なトンネルを確立し、認証後、vBond は vManage IP アドレスを Cisco IOS XE ルータに送信します。ルータはセキュアトンネルを介して vManage に接続し、vManage は完全な設定を Cisco IOS XE ルータに送信します。最後に、ルータは安全なトンネルを介して vSmart に接続します。認証後、SD-WAN ファブリックに参加します。このプロセスでは、手動による介入や設定は必要ありません。

前提条件

- デバイスはネットワークに接続されています。
- デバイスは DHCP IP アドレスを取得し、PnP ポータルと vBond に到達できます。
- デバイスに設定がありません。
- デバイスは、有効またはステージングとして vManage にインポートされます。
- デバイスはデバイステンプレートに割り当てられています。

方法：ブートストラップ

デバイスが以下の前提条件を満たしている場合、デバイスの起動時に、USB ドライブまたはブートフラッシュから設定ファイルを読み取り、設定情報を使用してネットワークに参加します。この設定により、ネットワーク接続が有効になり、システムパ

ラメータと vBond アドレスが提供されます。デバイスが vBond によって認証されると、vManage 情報を取得します。ルータは vManage との通信を確立し、オーバーレイネットワークに参加します。IOS XE SD-WAN のインストールを実行する前に、ブートフラッシュにコンフィギュレーション ファイルをコピーすることをお勧めします。IOS XE SD-WAN のインストールが完了すると、デフォルトのワンタイムユーザー admin は削除され、デフォルトのパスワードは 1 回使用でき、その後は変更する必要があります。

前提条件

- デバイスはネットワークに接続されています。
- SD-WAN コントローラはネットワーク上で到達可能である必要があります。
- ブートストラップ設定は、デバイスのブートフラッシュまたはデバイスに接続された起動可能な USB ドライブにロードされます。
- デバイスは、有効またはステージングとして vManage にインポートされます。
- デバイスはデバイステンプレートに割り当てられています。

方法：手動設定

ルータを SD-WAN ネットワークに手動でオンボーディングするには、次の手順を実行します。

1. 入力されたログイン情報を使用して vManage GUI にログインします。
2. コンソールを使用して IR8340 ルータにログオンします。
3. IR8340 Cisco Edge ルータがクラウドインフラに到達可能であることを確認するために必要な接続を行います。
4. ルータで実行されている ROM バージョンと IOS-XE バージョンを確認します。SDWAN をサポートする最新の推奨バージョンであることを確認してください。必要に応じて、rommon と IOS-XE をアップグレードしてください。IOS-XE の以降のリリースでは、別の SDWAN イメージをルータにロードする必要はありません。

5. SDWAN クラウド インフラストラクチャに到達するために Cisco Edge デバイスが接続されているルータが、起動時に Cisco Edge ルータに IP アドレス、デフォルトゲートウェイ、および DNS サーバーアドレスを提供するように設定されていることを確認します。このシナリオでは、SA-HER は dhcp サーバーであり、パラメータを IR8340 Cisco Edge ルータに割り当てます。
6. asr1002-HX に最新の IOS-XE イメージがある場合、次を実行します。
 - 実行コンフィギュレーションのバックアップを取ります。
 - 「controller-mode enable」を発行します
 - ルータは、「No day 0 Bootstrap configuration available」という警告メッセージとともにリロードされます。リロードを続行します。
 - ルータがリロードされると、インターフェイスは dhcp に割り当てられた IP アドレス、デフォルトルート、および DNS サーバーを取得します。
 - dhcp の代わりに、静的 IP アドレスとデフォルトルートをプロビジョニングすることもできます。
 - ルータは PNP プロセスを開始します。PNP 登録プロセスを停止するには、「pnpa service Discovery stop」コマンドを使用します。
 - ping を使用して、Cisco Edge ルータからクラウドインフラへの到達可能性を確認します。
 - 「show sdwan certificate serial」コマンドの出力を収集します。
シャーシ番号:IR8340-K9-FDO2506J99H、ボードID シリアル番号:XXXXXXXX、
件名 S/N : XXXXXXXX
 - これらの詳細を CSV 形式のファイルに入力します。
フォーマット : シャーシ番号、製品 ID、証明書のシリアル番号、sudi シリアル
 - 証明書のシリアル番号は、ボードのシリアル番号と同じです
 - Sudi のシリアル番号は Subject S/N と同じです。

- vManage ページから、[Devices] メニューに移動します。左上隅 → [Configuration] → [Devices] をクリックします。
 - WAN Edge リストオプションを選択し、適切な詳細を含む CSV ファイルをアップロードします。
 - メインメニューから、[Administration > Settings] の順に移動します。
- 組織名と vBOND の詳細を書き留めます。
- ルータで次の設定を作成して適用します。system-ip、domain-id、site-id は重要な属性です。

```

Router#config-transcation
!
system
system-ip 192.168.60.100
domain-id 1
site-id 2001
admin-tech-on-failure
sp-organization-name "IOT-BU - 238964"
organization-name "IOT-BU - 238964"
vbond vbondviptela.net port 12346          <<<<<<< VBOND Detail
!
interface Tunnell
no shutdown
ip unnumbered GigabitEthernet0/0/0  <<<<<<< Interface through which internet is reachable for the
topology.
tunnel source GigabitEthernet0/0/0
tunnel mode sdwan
exit
sdwan
interface GigabitEthernet0/0/0
tunnel-interface
encapsulation ipsec
exit
hostname IR8340-vEDGE-001
commit
exit
!

```

Device Management

ソフトウェア アップグレード

vManage を使用してアップグレードする場合は、vManage またはリモート vManage に直接ロードされたコードイメージを使用してアップグレードできます。また、リモートファイルサーバ上にあるコードイメージを使用してアップグレードすることもできます。この手順では、任意のデバイスのソフトウェアが vManage ソフトウェアリポジトリにアップロードされます。

vManage での画像のアップロード

1. [Maintenance] > [Software Repository] の順に移動します。リポジトリは、イメージを vManage、リモートファイルサーバー、またはリモート vManage にローカルに保存します。
2. [Add New Software] をクリックし、ドロップダウンリストから [vManage] を選択します。
3. イメージファイルをドロップするか、ローカルコンピュータ上のイメージを参照するように求めるダイアログボックスが表示されます。
4. 必要な画像を読み込み、[Upload] ボタンをクリックします。ウィンドウに、イメージが vManage にロードされていることが示されます。完了すると、イメージが正常にアップロードされたことを示すメッセージが表示され、バージョン、ソフトウェアの場所 (vManage) 、および使用可能なファイルがリポジトリに追加されます。

デバイスのアップグレード

1. dir bootflash: コマンドを使用して、イメージをダウンロードするための十分なスペースがデバイスにあることを確認します。下部に空き容量が表示されます。必要に応じてファイルを削除します。
2. [Maintenance] > [Software Upgrade] の順に移動し、[Current Version] 列でコードバージョンを確認します。
3. アップグレードが必要な場合は、アップグレードするルータの横にあるチェックボックスをオンにして、[Upgrade] ボタンをクリックします。新しいダイアログボックスが表示されます。

4. vManage が選択されていることを確認します。ドロップダウンリストから新しいコードバージョンを選択します。
5. [Activate and Reboot] チェックボックスをオンにして、[Upgrade] をクリックします。デバイスはソフトウェアを取得してインストールし、アクティブ化するために再起動します。必要に応じて、ボックスをオフのままにして、後でイメージをアクティブにすることができます。

イメージのアクティブ化

すでにインストールされているがアクティブ化されていないイメージの場合は、次の手順に従います。

1. [Maintenance] > [Software Upgrade] の順に移動し、[Current Version] 列でコードバージョンを確認します。
2. アクティブ化するルータの横にあるチェックボックスをオンにして、[Activate] をクリックします。新しいダイアログボックスが表示されます。
3. アクティブ化する準備が整ったイメージがインストールされている場合は、[Version] ドロップダウンメニューに表示されます。バージョンを選択し、[Active] をクリックします。ルータは新しいバージョンで再起動します。

ベスト プラクティス

- ルータをさまざまなアップグレードグループに分割します。システムテンプレートの [device groups] フィールドでタグを使用してグループを識別できます。1 つまたは複数のテストサイトをターゲットにし、それらのルータを最初のアップグレードグループに含めます。
- デュアルルータサイトでは、各ルータを異なるアップグレードグループに配置し、同時にいずれかをアップグレードしないでください。
- アップグレードグループ内のすべてのルータは並行してアップグレードできます（最大 32 台の WAN エッジルータ）が、vManage またはリモートファイルサーバーがルータへの同時ファイル転送を処理できる機能を考慮してください。
- 最初のアップグレードグループをアップグレードし、コードを事前に指定した時間安定した状態で実行させてから、追加のアップグレードグループのアップグレードに進みます。

- ディスクがいっぱいにならないようにするには、vManage を使用して古いバージョンをクリーンアップします。古いバージョンを削除するには、[Maintenance > Software Upgrade] に移動し、クリアするデバイスを選択して [Delete Available Software] を選択します。ダイアログボックスで、削除する画像を選択し、[Delete] をクリックします。

デバイスの再起動

[Maintenance > Device Reboot] に移動して、ルータを再起動します。[WAN Edge] タブが表示されていることを確認してください。再起動するデバイスを選択し、[Reboot] をクリックします。ポップアップウィンドウでアクションを確認します。

デバイスターミナルに接続する

[Tools > SSH terminal] に移動します。左側のパネルで接続するデバイスを選択します。デバイスへのターミナルウィンドウが表示されます。デバイスログイン情報を入力してください。

ソリューションの一部として検証された他のシナリオについては、次の表のドキュメントのリストを参照してください。

表9 SDWAN テンプレートと設定

テンプレート (Template)	参照先
Device Template	https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/system-interface/vedge-20-x/systems-interfaces-book/configure-devices.html
SVI を使用した VPN インターフェイス	https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/system-interface/ios-xe-17/systems-interfaces-book-xe-sdwan/configure-interfaces.html#c-VPN_Interface_SVI-12319

VPN の設定	https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/segmentation/vEdge-20-x/segmentation-book/segmentation.html#d221e494a1635
ハブアンドスポークの一元化されたポリシー	https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge-20-x/policies-book/centralized-policy.html
ゾーンベースのファイアウォール	https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge-20-x/security-book/m-fwirewall-17.html#c_Zone_Based_Firewall_Configuration_Examples_12252.xml

DNAC を使用した IR8340 管理

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。

管理機能

インストール

Cisco DNA Center アプライアンスのインストールについては、

<https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-installation-guides-list.html> を参照してください。

ライセンス

この実装では、Cisco Smart Software Manager On-Prem (Cisco SSM On-Prem) ツールを Cisco DNA Center ライセンスに使用しました。Cisco SSM On-Prem のインストールについては、https://www.cisco.com/web/software/286285517/152313/Smart_Software_Manager_On-Prem_8-202006_Installation_Guide.pdf を参照してください。

アップグレード

Cisco DNA Center のアップグレードに関する情報は、https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/upgrade/b_cisco_dna_center_upgrade_guide.html にあります。

変電所ルータの検出

Cisco DNA Center はネットワークデバイスを検出し、それらを管理対象のインベントリに追加できます。これにより、管理者は中央の視点から環境を維持およびモニタリングできます。デバイス制御機能をディスカバリプロセスに追加して、その後のプロビジョニング設定またはインベントリの変更が行われたときに、Cisco DNA Center を介した管理のためにデバイスを準備することができます。デバイスを検出するには、次の手順を実行します。

DNA で検出する前の前提条件

ネットワークデバイスが Cisco DNA Center によって検出されるようにするには、前のセクションで Cisco DNA Center で設定したように、CLI および SNMP ログイン情報をデバイスに設定する必要があります。この実装で使用されるネットワークデバイスの設定例は次のとおりです。

1. ネットワークデバイスで CLI SSH ユーザーログイン情報を設定します。Cisco Catalyst 9300 スイッチスタックの設定例：

```
username <username> privilege 15 password 7 <password> enable secret  
<password>
```

2. ネットワークデバイスで SNNMPv3 ログイン情報を設定します。Cisco Catalyst 9300 スイッチスタックの設定例：

```
snmp-server group default v3 priv  
snmp-server group ciscogrp v3 priv read SNMPv3All write SNMPv3None  
snmp-server view SNMPv3All iso included  
snmp-server view SNMPv3None iso excluded
```

```
snmp-server community <CommunityString> RWsnmp-server user <username>  
default v3 auth md5 <password> priv aes 128 <password>
```

3. ネットワークデバイスで SSH バージョン 2 アクセスを有効にします。Cisco Catalyst 9300 スイッチスタックの設定例：

```
ip ssh source-interface Loopback0  
crypto key generate rsa modulus 2048  
ip ssh version 2  
!  
line vty 0 4  
login local  
transport preferred ssh  
transport input all  
line vty 5 15  
login local  
transport preferred ssh  
transport input all  
!
```

1. Cisco DNA Center Web インターフェイスから、[Tools > Discovery] に移動します。
2. [Add Discovery] ボタンをクリックします。

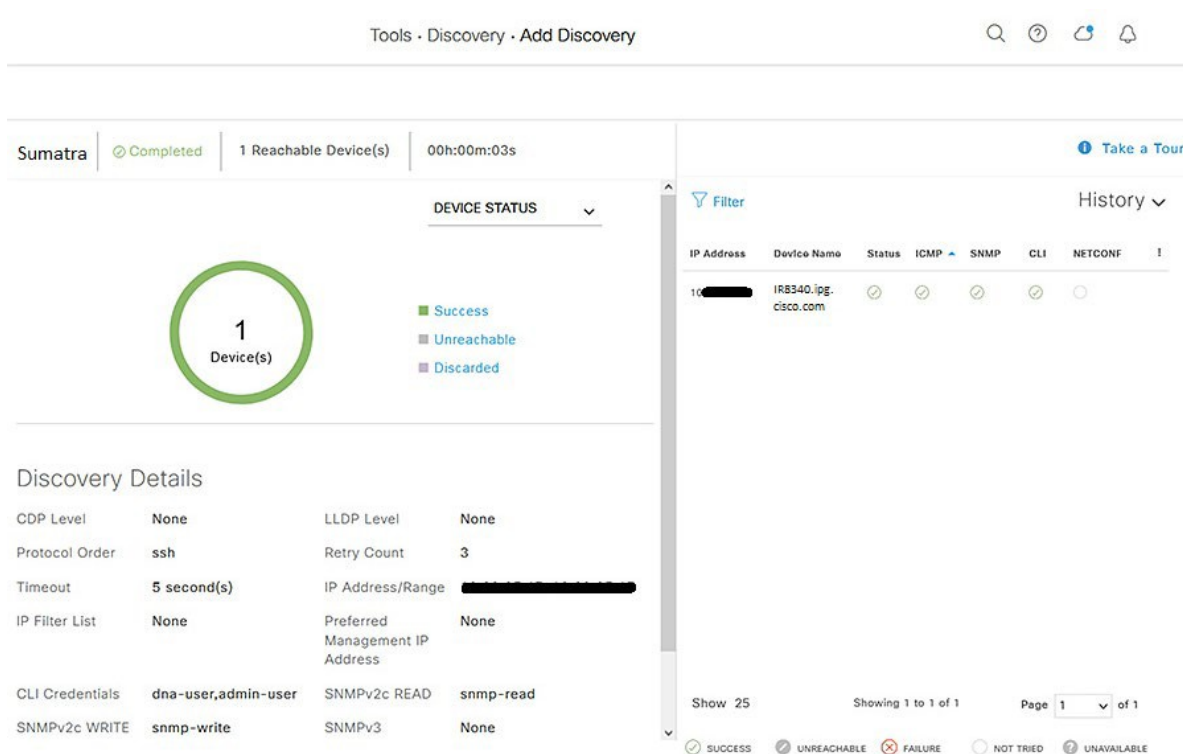
- 下部にあるデバイスの制御可能性が有効になっている場合に注意してください(デフォルトで有効になっています)。有効にすると、Cisco DNA Center は検出中にデバイスに SNMP または NETCONF ログイン情報を設定します(既存の SNMP または NETCONF 設定を上書きしません)。Cisco DNA Center モニタリング機能を利用するには、デバイス制御機能を使用することをお勧めします。

注：現在、Cisco IE スイッチは NETCONF 経由で検出できますが、現在のリリースには追加機能はありません。デバイスに構成変更を加えたくない場合は、[Disable] リンクをクリックします。

- [Discovery Name] フィールドに、検出される関連デバイスの名前を入力します。
- [IP Address/Range] で、適切な [Discovery Type] を選択します。
 - [CDP] には、検出するデバイスの [IP Address] を入力します。[CDP レベル] をデフォルト以外に変更して、元のデバイスに対してより多くのまたはより少ない隣接デバイスを検出することができます。

- [IP Address/Range] で、[From] フィールドに、スキャンする最小の IP アドレスを入力します。[To] フィールドに、スキャンする最大の IP アドレスを入力します。1 つのデバイスのみが検出されている場合は、両方のフィールドに同じ IP アドレスを入力します。デバイスの検出には、IP アドレスによる方法をお勧めします。
 - [LLDP] の場合、検出するデバイスの [IP Address] を入力します。[LLDP Level] をデフォルト以外に変更して、元のデバイスに対してより多くのまたはより少ない隣接デバイスを検出することができます。
3. [Credentials] で、[CLI, SNMPv2c Read, SNMPv2c Write] などが必要なエンティティのトグルボタンをクリックします。検出されるデバイスは、検出を成功させるためにこれらのログイン情報の少なくとも 1 つの形式を受け入れる必要があり、CLI ログイン情報は必須です。
 4. [Discover] ボタンをクリックします。検出プロセスが開始され、[Discovery] ページに進行状況が表示され、現在のステータスが自動更新されて表示されます。プロセスが完了すると、成功または失敗の結果が表示され、検出されたデバイスがインベントリに追加されます。

図 53 変電所ルータのDNAC 検出



検出後、デバイスをサイトとプロビジョニングに割り当てます。これは、個別に、または同じ手順で実行できます。

サイトのみに割り当て：

1. [Provision] > [Network Devices] > [Inventory] に移動します。
2. 左側の階層から、[Global] > [Unassigned Devices] を選択します。
3. リストで新しく検出されたデバイスを見つけ、チェックボックスをオンにします。[Actions] ドロップダウンリストから、[Provision] > [Assign Device to Site] の順に選択します。
 - a. [Assign Device to Site] スライドインペインで、[Choose a Site] リンクをクリックします。階層から目的のサイトをクリックし、[Save] ボタンをクリックします。[Next] ボタンをクリックします。
 - b. デプロイされる設定を確認し、[Next] ボタンをクリックします。
 - c. すぐに変更するには、[Now] ラジオボタンをクリックします（将来の日時に割り当てをスケジュールする場合は、[Later] ラジオボタンをクリックして日付と時刻を指定します）。
 - d. [Assign] ボタンをクリックします。

デバイスが割り当てられると、指定したサイトのデバイスリストに追加されます。デバイスの制御可能性が有効になっている場合、デバイスをサイトに割り当てると、次の設定がトリガーされることに注意してください（該当する場合）。

- コントローラ証明書
- SNMPトラップサーバ定義
- Syslog サーバ定義
- NetFlow サーバ定義
- IPDT の有効化

サイトへの割り当てとプロビジョニング：

1. [Provision] > [Network Devices] > [Inventory] に移動します。
2. 左側の階層から、[Global] > [Unassigned Devices] を選択します。
3. リストで新しく検出されたデバイスを見つけ、チェックボックスをオンにします。[Actions] ドロップダウンリストから、[Provision] > [Provision device] の順に選択します。
 - a. [Assign Site] ステップで、[Choose a site link] をクリックし、目的のサイトを選択します。[Save] ボタンをクリックし、[Next] ボタンをクリックします。（サイトの割り当てが以前に行われている場合は、ここでの操作は必要ありません）。
 - b. 設定するテンプレート設定がある場合は、[Advanced Configuration] ステップで、[Device] リストからデバイスを選択します。完了したら、またはテンプレートが適用されていない場合は、[Next] ボタンをクリックします。
 - c. [Overview] ステップで、デバイスに追加する設定を確認します。[Deploy] ボタンをクリックします。デバイスがプロビジョニングされると、指定したサイトのデバイスリストに表示されます。

注：Cisco DNA Center リリース 2.2.3.3：

- 検出される前に AAA ですでに設定されているデバイスのプロビジョニングは失敗します。Cisco DNA Center を使用して AAA をプッシュする前に、AAA 設定を削除します。

インベントリ

Cisco DNA Center Inventory には、デバイスを管理するためのさまざまな機能があります。PnP を介してデバイスが検出されるか、インベントリに追加されると、そのデバイスをプロビジョニングして、指定されたネットワーク設定をデバイスに追加することができます。さらに、デバイスが完全に管理された後、Inventory はコンプライアンスとソフトウェアの検証に加えて、デバイス設定を変更したり、

デバイスの交換を開始したりするオプションを提供できます。次のセクションでは、Inventory の監視および管理機能の一部について詳しく説明します。

イメージリポジトリ

Cisco DNA Center は Cisco.com と通信して、サポートされているデバイススイートの利用可能なソフトウェアイメージを、直接またはプロキシ経由で取得します。ネットワーク設定と同様に、ソフトウェアバージョンをサイトごとに指定して、デバイス間で一貫した動作を保証できます。デバイスが検出され、サイトに追加されたら、次の手順を実行して、デバイスタイプごとにイメージリポジトリ内のゴールデンイメージを変更できます。

1. Cisco DNA Center Web インターフェイスから、[Design > Image Repository] に移動します。
2. 左の階層から目的のサイトを選択します。
3. [Devices] リストから、各デバイスを展開して、使用可能なすべてのソフトウェアイメージを表示します。[Golden Image] 列の矢印ボタンをクリックして関連するイメージをダウンロードし、続いて表示される [Download Image] ダイアログボックスで、[Mark the image as golden after download] チェックボックスをオンにして、そのイメージをその特定のデバイスタイプのゴールデンイメージとして設定します。
4. 必要に応じて、他のデバイスとサイトについて繰り返します。

ソフトウェア イメージの管理

デバイスは、Cisco.com からイメージをダウンロードし、そのイメージをデバイスにプッシュして、アップグレードを実行する Cisco DNA Center を介して自動的にアップグレードできます。さらに、必要なイメージを Cisco DNA Center にアップロードするオプションがあり、アップグレードを事前にスケジュールできます。イメージがゴールデンとして設定されていることを確認したら（「[イメージリポジトリ](#)」セクションを参照）、次の手順を実行してデバイスのソフトウェアイメージを更新します。

1. Cisco DNA Center Web インターフェイスから、[Provision > Network Devices > Inventory] に移動します。
2. 左の階層から、アップグレードするデバイスがあるサイトを選択します。
3. アップグレードするデバイスの横にあるチェックボックスをオンにし、[Actions] ドロップダウンリストから [Software Image > Update Image] を選択します。

4. [Image Upgrade] スライドインペインで、アップグレードするデバイスのチェックボックスをオンにして、[Next] ボタンをクリックします。
5. [Software Distribution] の下で、[Now] オプションボタンをクリックします (将来の日付と時刻にアップグレードをスケジュールする場合は、[Later] オプションボタンをクリックして日付と時刻を指定します)。[Next] ボタンをクリックします。
6. [Software Activation] で、[Initiate Image Activation after Image Distribution] チェックボックスをオンにします。イメージをデバイスにプッシュするだけで、アップグレードを開始しない場合は、ボックスをオフのままにして、開始日時を指定するか、下部にある [Skip Activation] リンクをクリックします。[Initiate Flash Cleanup after Activation] チェックボックスをオンにすることもできます。これにより、アップグレード後に未使用のソフトウェアイメージのファイルがデバイスから自動的に削除されます。[Next] ボタンをクリックします。
7. [Summary] ステップで、アップグレードの詳細を確認し、[Submit] ボタンをクリックします。

ソフトウェアイメージの管理に関する注記：

- Cisco DNA Center は、存在する場合、sdfash でのイメージのインストールと実行を優先します。ソフトウェアが sdfash が存在するフラッシュからインストールモードで実行されている場合、アップグレードは失敗します。
- イメージが sdfash で実行されていて、vfat としてフォーマットされている場合、アップグレードは成功します。ext4 のみでフォーマットされている場合 (Cisco Cyber Vision の場合)、アップグレードは失敗します。sdfash のパーティション分割の詳細については、[IOS XE Devices with Cisco Cyber Vision](#) を参照してください。これにより、ソフトウェア イメージと iox アプリケーションを sdfash から同時に実行できます。
- 更新プロセスにより、デバイスのリロードがトリガーされ、デバイスと接続されているエンドポイントのネットワーク接続に影響します。

[Inventory] ページで、[Actions] ドロップダウンリストから [Software Image > Image Update Status] を選択して、更新のステータスを確認できます。さらに、インベントリから、指定されたゴールデンイメージを実行していないデバイスを [Compliance status] 列で確認するか、[Focus] ドロップダウンリストから [Software Images] を選択することができます。

テンプレート

Cisco DNA Center テンプレートを使用すると、新しい設定であるか、既存の設定であるかにかかわらず、検出されたデバイスまたは管理対象デバイスの設定を自動化できます。テンプレートの使用例とヒントについては、[付録](#)を参照してください。テンプレートを作成するには、次の手順を実行します。

1. Cisco DNA Center Web インターフェイスから、[Tools > Template Editor] に移動します。
2. [Plus] ボタンをクリックし、[Create Template] を選択します。
 - a. [Template Type] で、[Regular Template] オプションボタンをクリックします。
 - b. [Template Language] で、[Velocity] オプションボタンをクリックします。Jinja オプションも使用できます。詳細については、Cisco DNA Center のドキュメント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/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3.html.
 - c. [Name] に、テンプレートの名前を入力します。
 - d. [Project Name] ドロップダウンリストから関連するプロジェクトを選択します。たとえば、プラグアンドプレイ中に新しいデバイスの初期構成に使用するテンプレートを作成するには、**オンボーディング設定**を選択します。
 - [Device Type] の下の [Edit] リンクをクリックします。
 - 展開可能なリストをナビゲートして、関連するすべてのデバイスのチェックボックスをオンにします。
 - e. 上部にある [Add New Template] リンクに [Back] をクリックします。
 - f. [Software Type] ドロップダウンリストから、シスコのソフトウェアのタイプを選択します。
 - g. [Add] ボタンをクリックします。
 - h. Template Editor ペインが表示され、設定用の CLI コマンドを入力できます。変数は、引数でドル記号を示すことによって使用できることに注意してください。たとえば、以下です：

```
ip address $address 255.255.255.0
```

- i. 必要な構成をすべて追加したら、[Actions] ドロップダウンリストから [Save] を選択し、[Commit] を選択します。

注: 既存のテンプレートを変更しても、それらが再度プロビジョニングされるまで、関連付けられたデバイスの設定変更はトリガーされません。

ネットワーク プロファイル

Cisco DNA Center ネットワークプロファイルを使用すると、サイトにテンプレートを添付できるため、デバイスがサイトに追加されると、Cisco DNA Center はテンプレートで指定された設定を自動的に適用します。ネットワークプロファイルを作成するには、次の手順を実行します。

1. Cisco DNA Center Web インターフェイスから、[Design > Network Profiles] に移動します。
2. [Add Profile] ドロップダウンリストから、適切なデバイスタイプを選択します。
 - a. [Profile Name] フィールドに名前を入力します。
 - b. [OnBoarding Template(s)] タブを選択して、未設定のデバイスのプラグアンドプレイ中に使用するテンプレートに関連付けるか、[Day-N Template(s)] タブを選択して、プロビジョニング中にプッシュされる追加設定のテンプレートに関連付けます。
 - c. [Add Template] ボタンをクリックします。
 - [Add Template] スライドインペインで、[Add Template] リストから関連するテンプレートを選択します。
 - [Add] ボタンをクリックします。
 - d. [保存 (Save)] ボタンをクリックします。

注：テンプレートをネットワークプロファイルに追加しても、それらが再度プロビジョニングされるまで、該当する既存のデバイスの構成変更はトリガーされません。

アシュアランス、デバイスヘルス、および DNA セキュリティについては、詳細について次の Cisco Validated Document 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_IG.html

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。

リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。

あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

付録：設定の実行

HER

```
Substation-HER#show running-config
```

```
Building configuration...
```

```
Current configuration : 33102 bytes
```

```
!
```

```
! Last configuration change at 10:41:10 IST Thu Sep 15 2022 by admin
```

```
! NVRAM config last updated at 10:41:10 IST Thu Sep 15 2022 by admin
```

```
!
```

```
version 17.3
```

```
service timestamps debug uptime
```

```
service timestamps log uptime
```

```
service call-home
```

```
platform qfp utilization monitor load 80
```

```
no platform punt-keepalive disable-kernel-core
```

```
platform hardware crypto-throughput level 8-25g
```

```
!
```

```
hostname Substation-HER
```

```
!
```

```
boot-start-marker
```

```
boot system bootflash:asr1000-universalk9.17.03.04a.SPA.bin
```

```
boot-end-marker
```

```
!
```

```
!
```

```
vrf definition Mgmt-intf
```

```
!
```

```
address-family ipv4
```

```
exit-address-family
```

```
!
```

```
address-family ipv6
```

```
exit-address-family
```

```
!
```

```
vrf definition VRF_BUSINESS
```

```
rd 199:104
```

```
route-target export 199:104
```

```
route-target import 199:104
```

```
!
```

```
address-family ipv4
```

```
exit-address-family
```

```
!
```

```
vrf definition VRF_GRIDMON
```

```
rd 199:102
```

```
route-target export 199:102
```

```
route-target import 199:102
```

```
!
```

```
address-family ipv4
```

```
exit-address-family
!
vrf definition VRF_MGMT
rd 199:101
route-target export 199:101
route-target import 199:101
!
address-family ipv4
exit-address-family
!
vrf definition VRF_PLANTLINK
rd 199:105
route-target export 199:105
route-target import 199:105
!
address-family ipv4
exit-address-family
!
vrf definition VRF_SCADA
rd 199:111
route-target export 199:111
route-target import 199:111
route-target import 101:111
!
address-family ipv4
  route-target export 199:111
  route-target import 199:111
  route-target import 101:111
exit-address-family
!
vrf definition VRF_TSCADA
rd 199:103
route-target export 199:103
route-target import 199:103
!
address-family ipv4
exit-address-family
!
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization exec default local
aaa authorization network FlexVPN_Author local
!
!
!
```

```
!  
!  
aaa session-id common  
clock timezone IST 5 30  
clock calendar-valid  
!  
!  
!  
!  
!  
!  
!  
ip name-server xx.xx.xx.xx  
ip domain name isg.cisco.com  
!  
ip dhcp pool ASR1002-HX-DHCP  
network 192.168.60.0 255.255.255.0  
default-router 192.168.60.1  
dns-server xx.xx.xx.xx  
!  
ip dhcp pool SUMATRA-vEDGE-001  
network 192.168.66.0 255.255.255.0  
default-router 192.168.66.1  
dns-server xx.xx.xx.xx  
!  
ip dhcp pool ASR1002-HX-MPLS-POOL  
network 192.168.6.0 255.255.255.0  
dns-server xx.xx.xx.xx  
!  
ip dhcp pool SUMATRA-vEDGE-001-MPLS  
network 192.168.7.0 255.255.255.0  
default-router 192.168.7.1  
dns-server xx.xx.xx.xx  
!  
ip dhcp pool CSR1000vEdge-001  
network 192.168.85.0 255.255.255.0  
dns-server xx.xx.xx.xx  
default-router 192.168.85.1  
!  
ip dhcp pool IR1101-cEDGE  
network 192.168.8.0 255.255.255.0  
dns-server xx.xx.xx.xx  
default-router 192.168.8.1  
!  
!  
!  
login on-success log  
ipv6 unicast-routing  
l2tp-class L2TP_TUNNEL_TEST
```

```
hidden
authentication
digest secret 0 xxxxxxxx hash SHA1
hello 100
hostname Substation-HER
password xxxxxxxx
receive-window 50
retransmit retries 10
timeout setup 400
!
!
!
!
!
!
!
!
subscriber templating
!
!
!
!
!
mpls label protocol ldp
mpls ldp igp sync holddown 1
mpls traffic-eng tunnels
multilink bundle-name authenticated
!
!
!
key chain DMVPN
key 1
  key-string dmvpn
!
!
!
!
!
!
!
!
!
!
license udi pid ASR1002-HX sn XXXXXXXX
license accept end user agreement
license boot suite FoundationSuiteK9
license boot suite AdvUCSuiteK9
```

```

license boot level adventerprise
license solution level appxk9
license solution level securityk9
memory free low-watermark processor 991004
!
!
spanning-tree extend system-id
diagnostic bootup level minimal
!
username cisco privilege 15 password 0 xxxxxxxx
username admin privilege 15 password 0 xxxxxxxx
!
redundancy
mode none
!
bridge-domain 1
member vni 6001
member GigabitEthernet0/2/15 service-instance 1
!
bridge-domain 601
no mac learning
!
bridge-domain 1000
crypto ikev2 authorization policy default_No_cert
route set interface
route set access-list FLEX_ACL
!
no crypto ikev2 authorization policy default
!
crypto ikev2 redirect gateway init
! (IKEv2 Cluster load-balancer is not enabled)
crypto ikev2 proposal FlexVPN_IKEv2_Proposal_No_cert
encryption aes-cbc-256
integrity sha256
group 14
!
crypto ikev2 policy FlexVPN_IKEv2_Policy_No_cert
proposal FlexVPN_IKEv2_Proposal_No_cert
!
crypto ikev2 keyring ANY
peer ANY
  address 0.0.0.0 0.0.0.0
  pre-shared-key sentryo
!
!
!
crypto ikev2 profile FLEX_SERVER_PROF_No_cert_1
match identity remote address 0.0.0.0
match identity remote fqdn domain isg.cisco.com

```

```

identity local address 89.89.89.1
authentication remote pre-share
authentication local pre-share
keyring local ANY
aaa authorization group psk list FlexVPN_Author default_No_cert
virtual-template 4
!
crypto ikev2 fragmentation
!
!
cdp run
!
lldp run
pseudowire-class L2TP_PW_TEST
encapsulation l2tpv3
sequencing both
protocol l2tpv3 L2TP_TUNNEL_TEST
ip local interface Loopback1
ip pmtu
ip dfbit set
ip tos reflect
ip ttl 100
!
!
class-map match-any TRANSACTIONAL
match ip dscp cs2 af21 af22 af23 cs4 af41 af42
class-map match-all VOICE
match ip dscp ef
class-map match-any MISSION-CRITICAL-DATA
match access-group name MISSION-CRITICAL-DATA
class-map match-any MISSION-CRITICAL
match ip dscp cs3 af31 af32 af33 cs6
class-map match-all CALL-SIGNALING
match ip dscp cs3
!
policy-map HOST-INPUT-MARKING
class VOICE
  set dscp ef
class CALL-SIGNALING
  set dscp cs3
class MISSION-CRITICAL-DATA
  set dscp af31
class class-default
policy-map HOST-QUEUE-PACKETS
class VOICE
  priority
class MISSION-CRITICAL
  bandwidth remaining percent 30
  queue-limit 96 packets

```



```
class TRANSACTIONAL
  bandwidth remaining percent 20
  queue-limit 96 packets
class class-default
  bandwidth remaining percent 25
  queue-limit 272 packets
policy-map UPLINK-QUEUE-PACKETS
class VOICE
  priority
class MISSION-CRITICAL
  bandwidth remaining percent 30
  queue-limit 96 packets
class TRANSACTIONAL
  bandwidth remaining percent 20
  queue-limit 96 packets
class class-default
  bandwidth remaining percent 25
  queue-limit 272 packets
!
!
!
!
!
!
!
crypto isakmp invalid-spi-recovery
!
crypto ipsec security-association replay disable
crypto ipsec security-association replay window-size 512
!
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set_No_cert esp-aes esp-sha256-hmac
mode transport
crypto ipsec fragmentation after-encryption
crypto ipsec df-bit clear
!
!
crypto ipsec profile default_No_cert_1
set transform-set FlexVPN_IPsec_Transform_Set_No_cert
set pfs group14
set ikev2-profile FLEX_SERVER_PROF_No_cert_1
!
!
!
!
!
!
!
!
```

```
interface Loopback0
ip address 192.168.201.6 255.255.255.255
!
interface Loopback1
ip address 192.168.200.1 255.255.255.255
!
interface Loopback12
ip address 12.12.12.1 255.255.255.255
ip ospf network point-to-point
ip ospf 12 area 0
!
interface Loopback99
ip address 192.168.13.1 255.255.255.255
!
interface Loopback100
ip address 10.60.60.1 255.255.255.255
bfd interval 50 min_rx 50 multiplier 3
!
interface Loopback101
ip address 10.70.70.1 255.255.255.255
!
interface Loopback111
ip address 192.168.220.4 255.255.255.255
!
interface Loopback200
ip address 192.168.117.1 255.255.255.255
!
interface Tunnel100
no ip address
!
interface GigabitEthernet0/0/0
description connected to DMZ switch
ip address xx.xx.xx.xx xx.xx.xx.xx
ip nat outside
negotiation auto
!
interface GigabitEthernet0/0/1
description connected to asr920-001
ip dhcp relay information trusted
ip dhcp relay information option-insert
ip dhcp relay information check-reply
ip address 192.168.69.1 255.255.255.0
ip nat inside
ip ospf network point-to-point
ip ospf 1 area 0
load-interval 30
negotiation auto
cdp enable
mpls ip
```

```
mpls ldp discovery transport-address 192.168.201.6
mpls traffic-eng tunnels
bfd interval 200 min_rx 200 multiplier 3
service-policy output UPLINK-QUEUE-PACKETS
!
interface GigabitEthernet0/0/2
description connected to ixia card 2 por 1
mtu 9216
no ip address
load-interval 30
negotiation auto
!
interface GigabitEthernet0/0/2.1201
encapsulation dot1Q 1201
vrf forwarding VRF_SCADA
ip address 12.0.1.1 255.255.255.0
!
interface GigabitEthernet0/0/2.1202
encapsulation dot1Q 1202
vrf forwarding VRF_TSCADA
ip address 12.0.2.1 255.255.255.0
!
interface GigabitEthernet0/0/2.1203
encapsulation dot1Q 1203
vrf forwarding VRF_PLANTLINK
ip address 12.0.3.1 255.255.255.0
!
interface GigabitEthernet0/0/2.1204
encapsulation dot1Q 1204
vrf forwarding VRF_MGMT
ip address 12.0.4.1 255.255.255.0
!
interface GigabitEthernet0/0/2.1205
encapsulation dot1Q 1205
vrf forwarding VRF_GRIDMON
ip address 12.0.5.1 255.255.255.0
!
interface GigabitEthernet0/0/2.1206
encapsulation dot1Q 1206
vrf forwarding VRF_BUSINESS
ip address 12.0.6.1 255.255.255.0
!
interface GigabitEthernet0/0/2.3001
encapsulation dot1Q 3001
ip address 30.1.0.1 255.255.255.0
!
interface GigabitEthernet0/0/2.3002
encapsulation dot1Q 3002
ip address 30.2.0.1 255.255.255.0
```

```

!
interface GigabitEthernet0/0/3
description connected to ixia card 2 port 2
mtu 9216
no ip address
load-interval 30
negotiation auto
service instance 990 ethernet
  encapsulation dot1q 990
  rewrite ingress tag pop 1 symmetric
  bridge-domain 601
!
service instance 997 ethernet
  encapsulation dot1q 997
  rewrite ingress tag pop 1 symmetric
  bridge-domain 1000
!
!
interface GigabitEthernet0/0/3.140
encapsulation dot1Q 140
ip address 140.140.140.1 255.255.255.0
!
interface GigabitEthernet0/0/3.799
encapsulation dot1Q 799
xconnect 192.168.199.1 799 encapsulation mpls
!
interface GigabitEthernet0/0/4
ip address 99.99.99.100 255.255.255.0
negotiation auto
bfd interval 50 min_rx 50 multiplier 3
!
interface GigabitEthernet0/0/5
description connected to xx.xx.xx.xx PC ethernet - asr G5
ip address 192.168.228.1 255.255.255.252
negotiation auto
!
interface GigabitEthernet0/0/6
description Phy_Loop
no ip address
negotiation auto
service instance 990 ethernet
  encapsulation dot1q 990
  rewrite ingress tag pop 1 symmetric
  l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptpdp R4 R5 R6 R8 R9 RA RB RC RD
RF
  bridge-domain 601 split-horizon group 0
!
service instance 997 ethernet
  encapsulation dot1q 997

```

```

rewrite ingress tag pop 1 symmetric
l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptpdp R4 R5 R6 R8 R9 RA RB RC RD
RF
bridge-domain 1000
!
service instance 998 ethernet
encapsulation dot1q 998
rewrite ingress tag pop 1 symmetric
l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptpdp R4 R5 R6 R8 R9 RA RB RC RD
RF
bridge-domain 1000
!
service instance 1001 ethernet
encapsulation dot1q 1001
rewrite ingress tag pop 1 symmetric
l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptpdp R4 R5 R6 R8 R9 RA RB RC RD
RF
bridge-domain 1000
!
service instance 1002 ethernet
encapsulation dot1q 1002
rewrite ingress tag pop 1 symmetric
l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptpdp R4 R5 R6 R8 R9 RA RB RC RD
RF
bridge-domain 1000
!
service instance 1052 ethernet
encapsulation dot1q 1052
rewrite ingress tag pop 1 symmetric
l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptpdp R4 R5 R6 R8 R9 RA RB RC RD
RF
bridge-domain 1000
!
service instance 1053 ethernet
encapsulation dot1q 1053
rewrite ingress tag pop 1 symmetric
l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptpdp R4 R5 R6 R8 R9 RA RB RC RD
RF
bridge-domain 1000
!
service instance 1054 ethernet
encapsulation dot1q 1054
rewrite ingress tag pop 1 symmetric
l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptpdp R4 R5 R6 R8 R9 RA RB RC RD
RF
bridge-domain 1000
!
service instance 1055 ethernet
encapsulation dot1q 1055

```

```

rewrite ingress tag pop 1 symmetric
l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptpdp R4 R5 R6 R8 R9 RA RB RC RD
RF
bridge-domain 1000
!
service instance 1056 ethernet
encapsulation dot1q 1056
rewrite ingress tag pop 1 symmetric
l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptpdp R4 R5 R6 R8 R9 RA RB RC RD
RF
bridge-domain 1056
!
service instance 1057 ethernet
encapsulation dot1q 1057
rewrite ingress tag pop 1 symmetric
l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptpdp R4 R5 R6 R8 R9 RA RB RC RD
RF
bridge-domain 1000
!
service instance 1058 ethernet
encapsulation dot1q 1058
rewrite ingress tag pop 1 symmetric
l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptpdp R4 R5 R6 R8 R9 RA RB RC RD
RF
bridge-domain 1000
!
service instance 2502 ethernet
encapsulation dot1q 2502
rewrite ingress tag pop 1 symmetric
l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptpdp R4 R5 R6 R8 R9 RA RB RC RD
RF
bridge-domain 601 split-horizon group 1
!
!
interface GigabitEthernet0/0/7
description Phy_Loop
no ip address
load-interval 30
negotiation auto
!
interface GigabitEthernet0/0/7.989
encapsulation dot1Q 989
xconnect 192.168.205.2 989 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.990
encapsulation dot1Q 990
xconnect 192.168.220.3 990 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.991

```

```
encapsulation dot1Q 991
xconnect 192.168.205.2 991 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.992
encapsulation dot1Q 992
xconnect 192.168.205.2 992 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.993
encapsulation dot1Q 993
xconnect 192.168.223.1 993 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.994
encapsulation dot1Q 994
xconnect 192.168.223.1 994 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.995
encapsulation dot1Q 995
xconnect 192.168.223.1 995 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.996
encapsulation dot1Q 996
xconnect 192.168.223.1 996 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.997
encapsulation dot1Q 997
xconnect 192.168.223.1 997 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.998
encapsulation dot1Q 998
xconnect 192.168.202.2 998 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.1001
encapsulation dot1Q 1001
xconnect 192.168.199.2 1001 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2502
encapsulation dot1Q 2502
xconnect 192.168.199.2 2502 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2503
encapsulation dot1Q 2503
xconnect 192.168.199.2 2503 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2504
encapsulation dot1Q 2504
xconnect 192.168.199.2 2504 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2505
encapsulation dot1Q 2505
```

```

xconnect 192.168.199.2 2505 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2506
encapsulation dot1Q 2506
xconnect 192.168.199.2 2506 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2507
encapsulation dot1Q 2507
xconnect 192.168.199.2 2507 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2508
encapsulation dot1Q 2508
xconnect 192.168.199.2 2508 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2509
encapsulation dot1Q 2509
xconnect 192.168.199.2 2509 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2560
encapsulation dot1Q 2560
xconnect 192.168.199.2 2560 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface TenGigabitEthernet0/1/0
description connected to FPR4010 port 8
ip address 192.168.70.2 255.255.255.0
service-policy input HOST-INPUT-MARKING
!
interface TenGigabitEthernet0/1/1
no ip address
!
interface TenGigabitEthernet0/1/2
no ip address
!
interface TenGigabitEthernet0/1/3
no ip address
shutdown
!
interface TenGigabitEthernet0/1/4
no ip address
!
interface TenGigabitEthernet0/1/5
no ip address
!
interface TenGigabitEthernet0/1/6
no ip address
!
interface TenGigabitEthernet0/1/7
no ip address
!

```



```

interface GigabitEthernet0/2/0
description connected to ixia 10.64.66.36 card 1 port 14
no ip address
negotiation auto
!
interface GigabitEthernet0/2/0.143
encapsulation dot1Q 143
ip address 143.143.143.1 255.255.255.0
!
interface GigabitEthernet0/2/1
description connected to Laptop SCADA FEP
ip address 192.168.189.1 255.255.255.0
negotiation auto
!
interface GigabitEthernet0/2/2
description connected to ixia card 1 port 10
ip address 171.171.171.1 255.255.255.0
negotiation auto
!
interface GigabitEthernet0/2/3
description connected to gig0/0/0 SUMATRA-P3-01
ip address 192.168.66.1 255.255.255.0
ip nat inside
negotiation auto
cdp enable
!
interface GigabitEthernet0/2/4
ip address 90.90.90.1 255.255.255.0
ip nat outside
negotiation auto
!
interface GigabitEthernet0/2/5
no ip address
shutdown
negotiation auto
!
interface GigabitEthernet0/2/6
description connected to sumatra-pp-2 on G0/0/0
ip address 89.89.89.1 255.255.255.0
negotiation auto
bfd interval 50 min_rx 50 multiplier 3
!
interface GigabitEthernet0/2/7
no ip address
speed 1000
no negotiation auto
!
interface GigabitEthernet0/2/7.152
encapsulation dot1Q 152

```

```
ip address 152.152.152.1 255.255.255.0
!  
interface GigabitEthernet0/2/8  
no ip address  
negotiation auto  
!  
interface GigabitEthernet0/2/9  
description connected to SA-1002HX-002 gi0/0/0  
ip address 192.168.60.1 255.255.255.0  
ip nat inside  
negotiation auto  
mpls ip  
mpls label protocol ldp  
!  
interface GigabitEthernet0/2/10  
description connected to UCS xx.xx.xx.xx on VMNIC 8  
ip address 192.168.85.1 255.255.255.0  
ip nat inside  
negotiation auto  
cdp enable  
!  
interface GigabitEthernet0/2/11  
description connected to SA-1002HX-002 gi0/0/1  
ip address 192.168.6.1 255.255.255.0  
ip nat inside  
ip ospf network point-to-point  
ip ospf 1 area 0  
negotiation auto  
cdp enable  
mpls ip  
mpls label protocol ldp  
!  
interface GigabitEthernet0/2/12  
no ip address  
shutdown  
negotiation auto  
!  
interface GigabitEthernet0/2/13  
no ip address  
negotiation auto  
!  
interface GigabitEthernet0/2/14  
no ip address  
shutdown  
negotiation auto  
!  
interface GigabitEthernet0/2/15  
description connected to IXIA card 2 port 13  
no ip address
```

```

negotiation auto
service instance 1 ethernet
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
!
!
interface GigabitEthernet0/2/16
description connected to IR1101
ip address 69.69.69.1 255.255.255.0
ip ospf network point-to-point
ip ospf 12 area 0
negotiation auto
!
interface GigabitEthernet0/2/17
description connected to IR1101-cEDGE-002
ip address 192.168.8.1 255.255.255.0
ip nat inside
negotiation auto
cdp enable
!
interface GigabitEthernet0
vrf forwarding Mgmt-intf no
ip address
shutdown
negotiation auto
!
interface Virtual-Template4 type tunnel
bandwidth 1000000
ip unnumbered Loopback100
tunnel source GigabitEthernet0/2/6
tunnel bandwidth transmit 1000000
tunnel bandwidth receive 1000000
tunnel protection ipsec profile default _No_cert_1
!
interface nve1
no ip address
source-interface Loopback12
member vni 6001
  ingress-replication 12.12.12.2
!
!
!
router eigrp 99
bfd interface GigabitEthernet0/0/4
bfd interface GigabitEthernet0/2/6
network 10.0.0.0
network 89.89.89.0 0.0.0.255
network 99.99.99.0 0.0.0.255
network 140.140.140.0 0.0.0.255

```

```
network 143.143.143.0 0.0.0.255
network 152.152.0.0
network 192.168.2.0
network 192.168.4.0
network 192.168.13.0
network 192.168.89.0
network 192.168.200.0
network 192.168.201.0
network 192.168.228.0
redistribute bgp 200 metric 100 1 255 1 1500
eigrp router-id 10.60.60.1
!
router ospf 1
router-id 192.168.201.6
network 192.168.201.6 0.0.0.0 area 0
bfd all-interfaces
mpls ldp sync
!
router ospf 12
router-id 12.12.12.1
network 12.12.12.1 0.0.0.0 area 0
bfd all-interfaces
!
router bgp 200
bgp router-id interface Loopback0
bgp log-neighbor-changes
neighbor 192.168.60.2 remote-as 2001
neighbor 192.168.60.2 shutdown
neighbor 192.168.60.2 ebgp-multihop 255
neighbor 192.168.70.1 remote-as 1001
neighbor 192.168.70.1 ebgp-multihop 255
neighbor 192.168.70.1 update-source Loopback0
neighbor 192.168.111.1 remote-as 200
neighbor 192.168.111.1 ebgp-multihop 255
neighbor 192.168.111.1 update-source Loopback0
neighbor 192.168.113.1 remote-as 200
neighbor 192.168.113.1 ebgp-multihop 255
neighbor 192.168.113.1 update-source Loopback0
neighbor 192.168.198.1 remote-as 200
neighbor 192.168.198.1 update-source Loopback0
neighbor 192.168.198.1 fall-over
neighbor 192.168.198.1 fall-over bfd
neighbor 192.168.199.1 remote-as 200
neighbor 192.168.199.1 update-source Loopback0
neighbor 192.168.199.1 fall-over
neighbor 192.168.199.1 fall-over bfd multi-hop
neighbor 192.168.201.4 remote-as 200
neighbor 192.168.201.4 shutdown
neighbor 192.168.201.4 update-source Loopback0
```

```

neighbor 192.168.201.10 remote-as 200
neighbor 192.168.201.10 update-source Loopback0
neighbor 192.168.202.1 remote-as 101
neighbor 192.168.202.1 ebgp-multihop 255
neighbor 192.168.202.1 update-source Loopback0
neighbor 192.168.203.1 remote-as 200
neighbor 192.168.203.1 update-source Loopback0
neighbor 192.168.220.2 remote-as 102
neighbor 192.168.220.2 ebgp-multihop 255
neighbor 192.168.220.2 update-source Loopback0
!
address-family ipv4
  bgp additional-paths install
  bgp nexthop trigger delay 1
  network 30.1.0.0 mask 255.255.255.0
  network 30.2.0.0 mask 255.255.255.0
  network 140.140.140.0 mask 255.255.255.0
  network 141.141.141.0 mask 255.255.255.0
  network 192.168.189.0
  network 192.168.200.1 mask 255.255.255.255
  network 192.168.205.2 mask 255.255.255.255
  network 192.168.205.4 mask 255.255.255.255
  network 192.168.220.2 mask 255.255.255.255
  network 192.168.223.1 mask 255.255.255.255
  redistribute connected
  redistribute eigrp 99
  neighbor 192.168.60.2 activate
  neighbor 192.168.60.2 next-hop-self
  neighbor 192.168.60.2 send-label
  neighbor 192.168.70.1 activate
  neighbor 192.168.70.1 next-hop-self
  neighbor 192.168.70.1 send-label
  neighbor 192.168.111.1 activate
  neighbor 192.168.111.1 send-community extended
  neighbor 192.168.111.1 next-hop-self
  neighbor 192.168.113.1 activate
  neighbor 192.168.113.1 send-community extended
  neighbor 192.168.113.1 next-hop-self
  neighbor 192.168.198.1 activate
  neighbor 192.168.198.1 next-hop-self
  neighbor 192.168.198.1 soft-reconfiguration inbound
  neighbor 192.168.198.1 send-label
  neighbor 192.168.199.1 activate
  neighbor 192.168.199.1 weight 40000
  neighbor 192.168.199.1 next-hop-self
  neighbor 192.168.199.1 soft-reconfiguration inbound
  neighbor 192.168.199.1 send-label
  neighbor 192.168.201.4 activate
  neighbor 192.168.201.4 next-hop-self

```

```

neighbor 192.168.201.4 soft-reconfiguration inbound
neighbor 192.168.201.4 send-label
neighbor 192.168.201.10 activate
neighbor 192.168.201.10 next-hop-self
neighbor 192.168.201.10 soft-reconfiguration inbound
neighbor 192.168.201.10 send-label
neighbor 192.168.202.1 activate
neighbor 192.168.202.1 next-hop-self
neighbor 192.168.202.1 soft-reconfiguration inbound
neighbor 192.168.202.1 send-label
neighbor 192.168.203.1 activate
neighbor 192.168.203.1 next-hop-self
neighbor 192.168.203.1 soft-reconfiguration inbound
neighbor 192.168.203.1 send-label
neighbor 192.168.220.2 activate
neighbor 192.168.220.2 next-hop-self
neighbor 192.168.220.2 send-label
exit-address-family
!
address-family vpnv4
neighbor 192.168.70.1 activate
neighbor 192.168.70.1 send-community extended
neighbor 192.168.70.1 next-hop-self
neighbor 192.168.198.1 activate
neighbor 192.168.198.1 send-community extended
neighbor 192.168.198.1 next-hop-self
neighbor 192.168.199.1 activate
neighbor 192.168.199.1 send-community extended
neighbor 192.168.199.1 next-hop-self
neighbor 192.168.201.4 activate
neighbor 192.168.201.4 send-community extended
neighbor 192.168.201.4 next-hop-self
neighbor 192.168.201.10 activate
neighbor 192.168.201.10 send-community extended
neighbor 192.168.201.10 next-hop-self
exit-address-family
!
address-family ipv4 vrf VRF_BUSINESS
redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_GRIDMON
redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_MGMT
redistribute connected
exit-address-family
!

```

```

address-family ipv4 vrf VRF_PLANTLINK
  redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_SCADA
  redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_TSCADA
  redistribute connected
exit-address-family
!
ip tcp path-mtu-discovery
ip telnet source-interface GigabitEthernet0/0/0
ip http server
ip http authentication local
ip http secure-server
ip forward-protocol nd
!
ip ftp source-interface Loopback1
ip ftp username xxxxxxxx
ip ftp password xxxxxxxxxxxx
ip tftp source-interface GigabitEthernet0/2/9
ip dns server
ip pim rp-address 12.12.12.1
ip nat inside source static tcp 192.168.205.2 22 interface GigabitEthernet0/2/4 43
ip nat inside source list NAT_INSIDE_POOL interface GigabitEthernet0/0/0 overload
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0/0
ip route 192.168.21.0 255.255.255.0 192.168.70.1
ip route 192.168.220.2 255.255.255.255 99.99.99.2 255
ip ssh source-interface GigabitEthernet0/0/0
ip ssh version 2
!
ip access-list standard FLEX_ACL
13 permit 89.89.89.0
14 permit 99.99.99.0
15 permit 192.168.169.1
10 permit 10.60.60.0 0.0.0.255
11 permit 192.168.220.0 0.0.0.255
16 permit 140.140.140.0 0.0.0.255
20 permit 192.168.2.0 0.0.0.255
30 permit 192.168.4.0 0.0.0.255
40 permit 192.168.5.0 0.0.0.255
50 permit 192.168.199.0 0.0.0.255
60 permit 192.168.200.0 0.0.0.255
80 permit 192.168.202.0 0.0.0.255
90 permit 192.168.203.0 0.0.0.255
100 permit 192.168.204.0 0.0.0.255
110 permit 192.168.210.0 0.0.0.255

```

```
!  
ip access-list extended MISSION-CRITICAL-DATA  
10 permit tcp any eq 20000 any  
20 permit tcp any eq 20100 any  
30 permit tcp any eq 20101 any  
40 permit tcp any eq 20102 any  
50 permit udp any eq 1234 any  
60 permit udp any eq 1235 any  
ip access-list extended NAT_INSIDE_POOL  
10 permit ip 192.168.60.0 0.0.0.255 any  
11 permit ip 192.168.85.0 0.0.0.255 any  
12 permit tcp 192.168.85.0 0.0.0.255 any  
13 permit udp 192.168.85.0 0.0.0.255 any  
14 permit icmp 192.168.85.0 0.0.0.255 any  
15 permit esp 192.168.85.0 0.0.0.255 any  
16 permit ahp 192.168.85.0 0.0.0.255 any  
20 permit tcp 192.168.60.0 0.0.0.255 any  
30 permit udp 192.168.60.0 0.0.0.255 any  
40 permit icmp 192.168.60.0 0.0.0.255 any  
50 permit esp 192.168.60.0 0.0.0.255 any  
60 permit ahp 192.168.60.0 0.0.0.255 any  
71 permit ip 192.168.66.0 0.0.0.255 any  
72 permit tcp 192.168.66.0 0.0.0.255 any  
73 permit udp 192.168.66.0 0.0.0.255 any  
74 permit icmp 192.168.66.0 0.0.0.255 any  
75 permit esp 192.168.66.0 0.0.0.255 any  
76 permit ahp 192.168.66.0 0.0.0.255 any  
77 permit ip any any  
78 permit gre any any  
81 permit ip 192.168.6.0 0.0.0.255 any  
82 permit tcp 192.168.6.0 0.0.0.255 any  
83 permit udp 192.168.6.0 0.0.0.255 any  
84 permit icmp 192.168.6.0 0.0.0.255 any  
85 permit esp 192.168.6.0 0.0.0.255 any  
86 permit ahp 192.168.6.0 0.0.0.255 any  
91 permit ip 192.168.7.0 0.0.0.255 any  
92 permit tcp 192.168.7.0 0.0.0.255 any  
93 permit udp 192.168.7.0 0.0.0.255 any  
94 permit icmp 192.168.7.0 0.0.0.255 any  
95 permit esp 192.168.7.0 0.0.0.255 any  
96 permit ahp 192.168.7.0 0.0.0.255 any  
101 permit ip 192.168.8.0 0.0.0.255 any  
102 permit tcp 192.168.8.0 0.0.0.255 any  
103 permit udp 192.168.8.0 0.0.0.255 any  
104 permit icmp 192.168.8.0 0.0.0.255 any  
105 permit esp 192.168.8.0 0.0.0.255 any  
106 permit ahp 192.168.8.0 0.0.0.255 any  
!  
!
```



```

!
snmp-server community public RO
snmp-server trap link ietf
snmp-server trap link switchover
snmp-server location SA-HER
snmp-server contact SCADA
snmp-server host 192.168.5.11 version 2c public
snmp ifmib ifindex persist
!
tftp-server bootflash:ASR1002-HX-JAE225206QL.cfg
tftp-server bootflash:ciscosdwan.cfg
!
!
!
!
control-plane
!
!
!
!
!
!
line con 0
exec-timeout 0 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
transport input all
transport output all
!
call-home
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be used as contact email address to send SCH
notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
    active
    destination transport-method http
ntp master
ntp server xx.xx.xx.xx
ntp server xx.xx.xx.xx
!
!
!
!
!
end

```

IE9300-PRP :

clarke-002-PRP#show running-config

Building configuration...

Current configuration : 21708 bytes

```
!  
! Last configuration change at 17:34:23 IST Wed Sep 21 2022 by admin  
!  
version 17.10  
service timestamps debug datetime msec  
service timestamps log datetime msec  
service internal  
service call-home  
platform punt-keepalive disable-kernel-core  
!  
hostname clarke-002-PRP  
!  
!  
vrf definition Mgmt-vrf  
!  
address-family ipv4  
exit-address-family  
!  
address-family ipv6  
exit-address-family  
!  
logging userinfo  
no logging console  
aaa new-model  
!  
!  
aaa group server radius AAASERVER  
  server name CISCOISE  
!  
aaa authentication login default local  
aaa authentication dot1x default group AAASERVER  
aaa authorization exec default local  
aaa authorization network default group radius  
aaa authorization network SGLIST group AAASERVER  
aaa authorization auth-proxy default group AAASERVER  
aaa authorization configuration default group AAASERVER  
aaa accounting auth-proxy default start-stop group AAASERVER  
aaa accounting dot1x default start-stop group AAASERVER  
aaa accounting exec default start-stop group AAASERVER  
aaa accounting network default start-stop group AAASERVER  
!  
!
```

```
aaa server radius policy-device
  key xxxxxxxx
!
aaa server radius dynamic-author
  client 192.168.2.202 server-key xxxxxx
  server-key xxxxxx
!
aaa session-id common
!
!
!
clock timezone IST 5 30
boot system switch all
sdflash:ie9k_iosxe.BLD_V1710_THROTTLE_LATEST_20220913_143247_V17_10_0_41.SSA.bin
switch 1 provision ie-9320-26s2c
!
!
!
!
ip routing
!
!
!
!
login on-success log
!
!
!
!
!
!
flow record StealthWatch_Record
  description NetFlow record format to send to StealthWatch
  match datalink mac source address input
  match datalink mac destination address input
  match ipv4 tos
  match ipv4 protocol
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  collect transport tcp flags
  collect counter bytes long
  collect counter packets long
!
!
flow exporter StealthWatch_Exporter
  description StealthWatch Flow Exporter
  destination 192.168.2.211
```

```

source Vlan11
transport udp 2055
option application-table
!
!
flow monitor StealthWatch_Monitor
description StealthWatch Flow Monitor
exporter StealthWatch_Exporter
cache timeout active 60
cache timeout update 5
record StealthWatch_Record
!
!
table-map policed-dscp
map from 0 to 8
map from 10 to 8
map from 18 to 8
map from 24 to 8
map from 46 to 8
default copy
table-map AutoQos-4.0-Trust-Cos-Table
default copy
!
!
dot1x system-auth-control
memory free low-watermark processor 84281
!
!
mac access-list extended TEST_MAC_ACL
permit any any 0x88B8 0x0
mac access-list extended TEST_MAC_SV
permit any any 0x88BA 0x0
mac access-list extended TEST_PTP_POWER
permit any any 0x88F7 0x0
diagnostic bootup level minimal
dying-gasp primary syslog secondary snmp-trap
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
!
!
alarm-profile defaultPort
alarm not-operating
syslog not-operating
notifies not-operating
!
alarm facility sd-card enable
alarm facility sd-card syslog

```

```

alarm facility sd-card notifies
alarm facility power-supply relay major
alarm facility power-supply notifies
alarm facility power-supply disable
!
enable password xxxxxx
!
username admin privilege 15 password 0 xxxxxx
!
redundancy
 mode sso
crypto engine compliance shield disable
!
!
!
!
!
vlan 2508,4040
!
lldp run
!
class-map match-any system-cpp-police-ewlc-control
  description EWLC Control
class-map match-any AutoQos-4.0-Output-Multimedia-Conf-Queue
  match dscp af41 af42 af43
  match cos 4
class-map match-any system-cpp-police-topology-control
  description Topology control
class-map match-any system-cpp-police-sw-forward
  description Sw forwarding, L2 LVX data packets, LOGGING, Transit Traffic
class-map match-any AutoQos-4.0-Bulk-Data-Class
  match access-group name AutoQos-4.0-Acl-Bulk-Data
class-map match-any AutoQos-4.0-Output-Bulk-Data-Queue
  match dscp af11 af12 af13
  match cos 1
class-map match-any system-cpp-default
  description EWLC data, Inter FED Traffic
class-map match-any AutoQos-4.0-Multimedia-Conf-Class
  match access-group name AutoQos-4.0-Acl-MultiEnhanced-Conf
class-map match-all TEST_COS_52_ADV_UI_CLASS
  description TEST_COS_52_ADV_UI_CLASS UI_policy_DO_NOT_CHANGE
  match cos 5
class-map match-all NETWORK_MGMT
  match access-group name NETWORK_MGMT
class-map match-all TEST_DSCP_33
  match dscp 33
class-map match-any system-cpp-police-sys-data
  description Openflow, Exception, EGR Exception, NFL Sampled Data, RPF Failed
class-map match-all TEST_COS_51_ADV_UI_CLASS

```

```

description TEST_COS_51_ADV_UI_CLASS UI_policy_DO_NOT_CHANGE
match cos 4
class-map match-all TEST_DSCP_23
match dscp 23
class-map match-any AutoQos-4.0-Output-Priority-Queue
match dscp cs4 cs5 ef
match cos 5
class-map match-any system-cpp-police-punt-webauth
description Punt Webauth
class-map match-any AutoQos-4.0-Output-Multimedia-Strm-Queue
match dscp af31 af32 af33
class-map match-any system-cpp-police-l2lvs-control
description L2 LVX control packets
class-map match-any system-cpp-police-forus
description Forus Address resolution and Forus traffic
class-map match-any system-cpp-police-multicast-end-station
description MCAST END STATION
class-map match-any AutoQos-4.0-Voip-Data-CiscoPhone-Class
match cos 5
class-map match-all COS_6
match cos 6
class-map match-any system-cpp-police-high-rate-app
description High Rate Applications
class-map match-any system-cpp-police-multicast
description MCAST Data
class-map match-any AutoQos-4.0-Voip-Signal-CiscoPhone-Class
match cos 3
class-map match-all QOS_GRP_4
match qos-group 4
class-map match-any system-cpp-police-l2-control
description L2 control
class-map match-any system-cpp-police-dot1x-auth
description DOT1X Auth
class-map match-any system-cpp-police-data
description ICMP redirect, ICMP_GEN and BROADCAST
class-map match-any system-cpp-police-stackwise-virt-control
description Stackwise Virtual OOB
class-map match-any non-client-nrt-class
class-map match-any AutoQos-4.0-Default-Class
match access-group name AutoQos-4.0-Acl-Default
class-map match-any system-cpp-police-routing-control
description Routing control and Low Latency
class-map match-any system-cpp-police-protocol-snooping
description Protocol snooping
class-map match-any AutoQos-4.0-Output-Trans-Data-Queue
match dscp af21 af22 af23
match cos 2
class-map match-any system-cpp-police-dhcp-snooping
description DHCP snooping

```

```

class-map match-any AutoQos-4.0-Transaction-Class
  match access-group name AutoQos-4.0-Acl-Transactional-Data
class-map match-any system-cpp-police-ios-routing
  description L2 control, Topology control, Routing control, Low Latency
class-map match-all class_test_CRITICAL
  match ip precedence 5
class-map match-any AutoQos-4.0-Scavenger-Class
  match access-group name AutoQos-4.0-Acl-Scavenger
class-map match-any system-cpp-police-system-critical
  description System Critical and Gold Pkt
class-map match-all TEST_GOOSE2_ADV_UI_CLASS
  description TEST_GOOSE2_ADV_UI_CLASS UI_policy_DO_NOT_CHANGE
  match access-group name TEST_MAC_SV
class-map match-all TEST_GOOSE3_ADV_UI_CLASS
  description TEST_GOOSE3_ADV_UI_CLASS UI_policy_DO_NOT_CHANGE
  match access-group name TEST_PTP_POWER
class-map match-any AutoQos-4.0-Signaling-Class
  match access-group name AutoQos-4.0-Acl-Signaling
class-map match-all TEST_GOOSE1_ADV_UI_CLASS
  description TEST_GOOSE1_ADV_UI_CLASS UI_policy_DO_NOT_CHANGE
  match access-group name TEST_MAC_ACL
class-map match-any AutoQos-4.0-Output-Scavenger-Queue
  match dscp cs1
class-map match-all TEST_COS_3
  match cos 3
class-map match-any system-cpp-police-ios-feature
  description
  ICMPGEN,BROADCAST,ICMP,L2LVXCntrl,ProtoSnoop,PuntWebauth,MCASTData,Transit,DOT1XAuth,S
  wfwfwd,LOGGING,L2LVXData,ForusTraffic,ForusARP,McastEndStn,Openflow,Exception,EGRExcption,NflSa
  mpled,RpfFailed
class-map match-all TEST_COS_5
  match cos 5
class-map match-any AutoQos-4.0-Output-Control-Mgmt-Queue
  match dscp cs2 cs3 cs6 cs7
  match cos 3
!
policy-map AutoQos-4.0-Output-Policy
  class AutoQos-4.0-Output-Priority-Queue
    priority level 1 percent 30
  class AutoQos-4.0-Output-Control-Mgmt-Queue
    bandwidth remaining percent 10
    queue-limit dscp cs2 percent 80
    queue-limit dscp cs3 percent 90
    queue-limit dscp cs6 percent 100
    queue-limit dscp cs7 percent 100
    queue-buffers ratio 10
  class AutoQos-4.0-Output-Multimedia-Conf-Queue
    bandwidth remaining percent 10
    queue-buffers ratio 10

```

```

class AutoQos-4.0-Output-Trans-Data-Queue
bandwidth remaining percent 10
queue-buffers ratio 10
class AutoQos-4.0-Output-Bulk-Data-Queue
bandwidth remaining percent 4
queue-buffers ratio 10
class AutoQos-4.0-Output-Scavenger-Queue
bandwidth remaining percent 1
queue-buffers ratio 10
class AutoQos-4.0-Output-Multimedia-Strm-Queue
bandwidth remaining percent 10
queue-buffers ratio 10
class class-default
bandwidth remaining percent 25
queue-buffers ratio 25
policy-map TEST_COS_5
class TEST_COS_51_ADV_UI_CLASS
class TEST_COS_52_ADV_UI_CLASS
policy-map pp2
class NETWORK_MGMT
policy-map AutoQos-4.0-Trust-Cos-Input-Policy
class class-default
set cos cos table AutoQos-4.0-Trust-Cos-Table
policy-map system-cpp-policy
policy-map TEST_RADIUS_DSCP
class TEST_DSCP_23
set ip precedence 2
class TEST_DSCP_33
set ip precedence 2
class QOS_GRP_4
police cir 8000
exceed-action drop
policy-map TEST_OUTSTATION_MARKING
class class_test_CRITICAL
set cos 5
policy-map TEST_GOOSE
class TEST_GOOSE1_ADV_UI_CLASS
set cos 4
police cir 10000000
exceed-action drop
class TEST_GOOSE2_ADV_UI_CLASS
set cos 4
police cir 10000000
exceed-action drop
class TEST_GOOSE3_ADV_UI_CLASS
set qos-group 4
policy-map TEST_DSCP_MARKING
class TEST_COS_5
set dscp ef

```



```

class TEST_COS_3
  set dscp af43
policy-map AutoQos-4.0-Classify-Input-Policy
class AutoQos-4.0-Multimedia-Conf-Class
  set dscp af41
class AutoQos-4.0-Bulk-Data-Class
  set dscp af11
class AutoQos-4.0-Transaction-Class
  set dscp af21
class AutoQos-4.0-Scavenger-Class
  set dscp cs1
class AutoQos-4.0-Signaling-Class
  set dscp cs3
class AutoQos-4.0-Default-Class
  set dscp default
policy-map AutoQos-4.0-CiscoPhone-Input-Policy
class AutoQos-4.0-Voip-Data-CiscoPhone-Class
  set dscp ef
  police cir 128000 bc 8000
  conform-action transmit
  exceed-action set-dscp-transmit dscp table policed-dscp
class AutoQos-4.0-Voip-Signal-CiscoPhone-Class
  set dscp cs3
  police cir 32000 bc 8000
  conform-action transmit
  exceed-action set-dscp-transmit dscp table policed-dscp
class AutoQos-4.0-Default-Class
  set dscp default
!
!
!
!
!
!
!
!
!
!
!
interface PRP-channel1
  switchport trunk allowed vlan 1-2507,2509-4094
  switchport mode trunk
  spanning-tree portfast trunk
  spanning-tree bpdupfilter enable
!
interface GigabitEthernet1/0/1
!
interface GigabitEthernet1/0/2
  description connected to clarke001 gi1/0/2

```

```

switchport trunk allowed vlan 1-2507,2509-4094
switchport mode trunk
ip flow monitor StealthWatch_Monitor input
load-interval 30
service-policy output TEST_RADIUS_DSCP
!
interface GigabitEthernet1/0/3
switchport trunk allowed vlan 1-2507,2509-4094
switchport mode trunk
!
interface GigabitEthernet1/0/4
switchport trunk allowed vlan 1-2507,2509-4094
switchport mode trunk
!
interface GigabitEthernet1/0/5
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
description connected Ixia 1/11
switchport trunk allowed vlan 1,111
switchport mode trunk
load-interval 30
authentication event fail action next-method
authentication host-mode multi-host
authentication order mab
authentication priority mab
authentication port-control auto
authentication violation restrict
mab
dot1x pae authenticator
dot1x timeout tx-period 3
spanning-tree portfast trunk
!
interface GigabitEthernet1/0/12
description Test_MAB
switchport access vlan 111
switchport mode access
switchport voice vlan dot1p
ip flow monitor StealthWatch_Monitor input
authentication event fail action next-method

```

```

authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication violation restrict
mab
dot1x pae authenticator
dot1x timeout tx-period 3
service-policy output pp2
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
switchport trunk allowed vlan 1-2507,2509-4094
switchport mode trunk
ip flow monitor StealthWatch_Monitor input
load-interval 30
prp-channel-group 1
service-policy input TEST_GOOSE
!
interface GigabitEthernet1/0/22
switchport trunk allowed vlan 1-2507,2509-4094
switchport mode trunk
ip flow monitor StealthWatch_Monitor input
load-interval 30
prp-channel-group 1
service-policy input TEST_GOOSE
!
interface GigabitEthernet1/0/23
shutdown
!
interface GigabitEthernet1/0/24
shutdown
!
interface GigabitEthernet1/0/25
!

```

```

interface GigabitEthernet1/0/26
!
interface GigabitEthernet1/0/27
!
interface GigabitEthernet1/0/28
!
interface AppGigabitEthernet1/0/1
  switchport voice vlan dot1p
!
interface Vlan1
  no ip address
!
interface Vlan111
  ip address 192.168.21.52 255.255.255.0
!
interface Vlan177
  ip address 177.177.177.3 255.255.255.0
!
interface Vlan751
  ip address 192.168.177.5 255.255.255.0
!
ip tcp selective-ack
ip tcp mss 1460
ip tcp window-size 131072
ip http server
ip http authentication local
ip http secure-server
ip forward-protocol nd
ip ftp source-interface Vlan111
ip ftp username xxxxxxxx
ip ftp password xxxxxxxx
ip route 192.168.2.0 255.255.255.0 192.168.21.99
ip ssh bulk-mode 131072
!
ip access-list extended AutoQos-4.0-Acl-Bulk-Data
  10 permit tcp any any eq 22
  20 permit tcp any any eq 465
  30 permit tcp any any eq 143
  40 permit tcp any any eq 993
  50 permit tcp any any eq 995
  60 permit tcp any any eq 1914
  70 permit tcp any any eq ftp
  80 permit tcp any any eq ftp-data
  90 permit tcp any any eq smtp
  100 permit tcp any any eq pop3
ip access-list extended AutoQos-4.0-Acl-Default
  10 permit ip any any
ip access-list extended AutoQos-4.0-Acl-MultiEnhanced-Conf
  10 permit udp any any range 16384 32767

```

```

20 permit tcp any any range 50000 59999
ip access-list extended AutoQos-4.0-Acl-Scavanger
 10 permit tcp any any range 2300 2400
 20 permit udp any any range 2300 2400
 30 permit tcp any any range 6881 6999
 40 permit tcp any any range 28800 29100
 50 permit tcp any any eq 1214
 60 permit udp any any eq 1214
 70 permit tcp any any eq 3689
 80 permit udp any any eq 3689
 90 permit tcp any any eq 11999
ip access-list extended AutoQos-4.0-Acl-Signaling
 10 permit tcp any any range 2000 2002
 20 permit tcp any any range 5060 5061
 30 permit udp any any range 5060 5061
ip access-list extended AutoQos-4.0-Acl-Transactional-Data
 10 permit tcp any any eq 443
 20 permit tcp any any eq 1521
 30 permit udp any any eq 1521
 40 permit tcp any any eq 1526
 50 permit udp any any eq 1526
 60 permit tcp any any eq 1575
 70 permit udp any any eq 1575
 80 permit tcp any any eq 1630
 90 permit udp any any eq 1630
100 permit tcp any any eq 1527
110 permit tcp any any eq 6200
120 permit tcp any any eq 3389
130 permit tcp any any eq 5985
140 permit tcp any any eq 8080
ip access-list extended NETWORK_MGMT
 10 permit ip any host 192.168.2.176
 20 permit tcp any host 192.168.2.176
 30 permit udp any host 192.168.2.108
 40 permit 22 any any
 50 permit 21 any any
!
ip radius source-interface Vlan111
ip sla responder
ip sla responder udp-echo ipaddress 192.168.2.108 port 2526
logging alarm informational
logging origin-id
ip logging host 192.168.5.11
logging host 192.168.2.206
!
snmp-server community public RO
snmp-server trap link ietf
snmp-server trap link switchover
snmp-server location CLARKE-002

```

```

snmp-server contact SCADA
snmp-server host 192.168.5.11 version 2c public
snmp-server manager
snmp ifmib ifindex persist
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute nas-port-id include circuit-id
radius-server dscp auth 33 acct 23
!
radius server CISCOISE
address ipv4 192.168.2.202 auth-port 1812 acct-port 1813
pac key xxxxxx
!
!
!
control-plane
service-policy input system-cpp-policy
!
!
line con 0
exec-timeout 0 0
stopbits 1
line aux 0
line vty 0 4
length 0
transport input all
line vty 5 15
transport input ssh
!
call-home
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be used as contact email address to send SCH
notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
active
destination transport-method http
!
ptp clock boundary domain 3 profile power
clock-port dynamic1
transport ethernet multicast interface Gi1/0/2
clock-port dynamic2
transport ethernet multicast interface Gi1/0/21
clock-port dynamic3
transport ethernet multicast interface Gi1/0/22
clock-port dynamic4
transport ethernet multicast interface Gi1/0/12
clock-port dynamic5

```

```
transport ethernet multicast interface Gi1/0/11
!  
!  
!  
!  
!  
!  
!  
end
```

IR8340

```
Sumatra-001#show running-config  
Building configuration...
```

Current configuration : 43642 bytes

```
!  
! Last configuration change at 14:52:59 IST Wed Sep 21 2022 by admin  
!
```

version 17.11

service timestamps debug datetime msec localtime show-timezone year

service timestamps log datetime msec localtime show-timezone year

service internal

service call-home

platform qfp utilization monitor load 80

platform punt-keepalive disable-kernel-core

platform hardware throughput crypto T0

!

hostname Sumatra-001

!

boot-start-marker

boot system flash:ir8340-universalk9.SSA.bin

boot-end-marker

!

!

vrf definition VRF_BUSINESS

rd 199:104

route-target export 199:104

route-target import 199:104

!

address-family ipv4

exit-address-family

!

vrf definition VRF_GRIDMON

rd 199:102

route-target export 199:102

route-target import 199:102

!

```
address-family ipv4
exit-address-family
!
vrf definition VRF_MGMT
rd 199:101
route-target export 199:101
route-target import 199:101
!
address-family ipv4
exit-address-family
!
vrf definition VRF_PLANTLINK
rd 199:105
route-target export 199:105
route-target import 199:105
!
address-family ipv4
exit-address-family
!
vrf definition VRF_SCADA
rd 199:111
route-target export 199:111
route-target import 199:111
route-target import 101:111
!
address-family ipv4
route-target export 199:111
route-target import 199:111
route-target import 101:111
exit-address-family
!
vrf definition VRF_TSCADA
rd 199:103
route-target export 199:103
route-target import 199:103
!
address-family ipv4
exit-address-family
!
card type t1 0 2
logging userinfo
no logging console
aaa new-model
!
!
aaa group server radius AAASERVER
server name CISCOISE
!
aaa authentication login default local
```



```
aaa authentication dot1x default group AAASERVER
aaa authorization exec default local
aaa authorization network default group AAASERVER group radius
aaa authorization network SGLIST group AAASERVER
aaa authorization auth-proxy default group AAASERVER
aaa authorization configuration default group AAASERVER
aaa accounting dot1x default start-stop group AAASERVER
!
!
aaa server radius policy-device
  key xxxxx
!
aaa server radius dynamic-author
  client 192.168.2.202 server-key xxxxxx
  server-key xxxxxx
!
aaa session-id common
ethernet cfm ieee
ethernet cfm global
clock timezone IST 5 30
rep admin vlan 1991 segment 2
rep multicast-fast-convergence
!
!
!
!
!
no ip nbar classification dns learning cache-ttl-zero
!
!
!
!
no ip domain lookup
ip domain name sumatra-001.cisco.com
!
ip dhcp pool TEST_POOL
  network 192.168.0.0 255.255.255.0
  default-router 192.168.0.1
!
!
!
login on-success log
l2tp-class L2TP_TUNNEL_TEST
  hidden
  authentication
  digest secret 0 xxxxxx hash SHA1
  hello 100
hostname Sumatra-001
password xxxxxx
```

```
receive-window 50
retransmit retries 10
timeout setup 400
!
!
!
!
!
!
!
!
subscriber templating
!
!
!
!
!
vtp mode off
!
mpls ldp igp sync holddown 1
multilink bundle-name authenticated
!
flow record StealthWatch_Record
description NetFlow record format to send to StealthWatch
match datalink mac source address input
match datalink mac destination address input
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect transport tcp flags
collect interface input
collect interface output
collect counter bytes long
collect counter packets long
collect timestamp sys-uptime first
collect timestamp sys-uptime last
!
!
flow exporter StealthWatch_Exporter
description StealthWatch Flow Exporter
destination 192.168.2.211
source Loopback1
transport udp 2055
option application-table
!
!
```

```
flow monitor StealthWatch_Monitor
description StealthWatch Flow Monitor
exporter StealthWatch_Exporter
cache timeout active 60
cache timeout update 5
record StealthWatch_Record
!
ptp clock forward-mode
!
!
!
!
!
cts sxp enable
no license feature hseck9
license udi pid IR8340-K9 sn FDO2551J707
license boot level network-advantage
license smart url https://smartreceiver-stage.cisco.com/licservice/license
license smart url smart https://smartreceiver-stage.cisco.com/licservice/license
license smart transport smart
archive
log config
logging enable
logging size 500
path ftp://192.168.2.176/sumatra-001
write-memory
memory free low-watermark processor 67541
!
diagnostic bootup level minimal
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1,201,501,1501 priority 4096
!
mac access-list extended GOOSE
permit any any 0x88B8 0x0
mac access-list extended PTP
permit any any 0x88F7 0x0
mac access-list extended SV
permit any any 0x88BA 0x0
dot1x system-auth-control
geo database
no power main redundant
!
!
enable password xxxxxxxx
!
username admin privilege 15 password 0 xxxxxxxx
!
```

```

redundancy
 mode none
bfd fast-timers-on-slow-interface
!
!
!
!
controller T1 0/2/0
 framing esf
 clock source internal
 linecode b8zs
 cablelength long 0db
 channel-group 2 timeslots 1-24
 description connected to t1 0/2/2 on asr903
!
controller T1 0/2/1
 framing esf
 clock source internal
 linecode b8zs
 cablelength long 0db
 channel-group 1 timeslots 1-24
 description connected to T10/2/3 on asr903
!
!
vlan internal allocation policy ascending
!
vlan 55,101,119,177,201,210,500-501,997-998,1001
!
vlan 1051
 name HSRP-GRP-1
!
vlan 1052-1060
!
vlan 1501
 remote-span
!
vlan 1990-1991,2340,4001
!
track 1 ip sla 1 reachability
 delay down 5 up 5
!
track 100 ip route 192.168.201.4 255.255.255.255 reachability
!
track 200 ip route 192.168.201.6 255.255.255.255 reachability
!
lldp run
!
class-map match-any MGMT_TRAFFIC
 match protocol ftp

```

```

match protocol ssh
match protocol ntp
match protocol http
match protocol https
class-map match-any PREC_ROUTINE
  match precedence 0
class-map match-any DSCP_af21_af22
  match ip dscp af21
  match ip dscp af22
  match dscp af21
  match dscp af22
  match dscp af23
  match dscp af12
  match dscp af11
class-map type ngs-w-qos match-any SCADA_PTP_NGSW
  match access-group name GOOSE
  match access-group name SV
  match access-group name PTP
class-map match-any SCADA_SV
  match access-group name SV
class-map match-all TEST_DSCP_af11
  match dscp af11
class-map match-all TEST_DSCP_af22
  match dscp af22
class-map match-all TEST_DSCP_af12
  match dscp af12
class-map match-all TEST_DSCP_af21
  match dscp af21
class-map match-any EXP_2
  match mpls experimental topmost 2
class-map match-any EXP_3
  match mpls experimental topmost 3
class-map match-any EXP_0
  match mpls experimental topmost 0
class-map match-any EXP_1
  match mpls experimental topmost 1
class-map match-any EXP_4
  match mpls experimental topmost 4
class-map match-any EXP_5
  match mpls experimental topmost 5
class-map type ngs-w-qos match-any TEST_COS_3_NGSW
  match cos 3
class-map type ngs-w-qos match-any TEST_COS_2_NGSW
  match cos 2
class-map type ngs-w-qos match-any TEST_COS_1_NGSW
  match cos 1
class-map type inspect match-any IN-IN
  match protocol ssh
  match protocol tcp

```

```

match protocol udp
match protocol icmp
match protocol https
match protocol http
match protocol login
class-map match-all COPP-MONITORING
  match access-group name coppacl-monitor
class-map type ngs-w-qos match-any TEST_COS_5_NGSW
  match cos 5
class-map type ngs-w-qos match-any TEST_COS_4_NGSW
  match cos 4
class-map match-all COPP-MANAGEMENT
  match access-group name coppacl-mgmt
class-map type inspect match-any OUT-SCADA
  match protocol ntp
  match protocol ssh
  match protocol syslog
  match protocol icmp
  match access-group name MISSION-CRITICAL-DATA-OUT
  match protocol snmp
class-map type inspect match-any SCADA-OUT
  match protocol ntp
  match protocol ssh
  match protocol syslog
  match protocol icmp
  match access-group name MISSION-CRITICAL-DATA-IN
class-map match-any QOS_GRP_6
  match qos-group 6
class-map match-any QOS_GRP_7
  match qos-group 7
class-map match-all COPP-CRITICAL-APP
  match access-group name coppacl-critical-app
class-map match-any TRANSACTIONAL
  match ip dscp cs2 af21 af22 af23 cs4 af41 af42
class-map match-all COPP-REMAINING-IP
  match access-group name coppacl-classification
class-map match-all VOICE
  match ip dscp ef
class-map match-any MISSION-CRITICAL-DATA
  match access-group name MISSION-CRITICAL-DATA-IN
class-map match-any SCADA_GOOSE
  match access-group name GOOSE
class-map match-any PREC_CRITIC
  match precedence 5
class-map match-any SCADA_PTP
  match access-group name PTP
class-map match-all COPP-ARP
  match protocol arp
class-map type inspect match-any IN-OUT

```

```

match protocol icmp
match protocol telnet
match protocol http
match protocol https
match protocol ssh
match protocol syslog
match protocol udp
match access-group name FTP_IN_OUT
match protocol tcp
match access-group 102
match protocol login
class-map type inspect match-any OUT-IN
match protocol icmp
match protocol telnet
match protocol http
match protocol https
match protocol ssh
match protocol syslog
match access-group name FTP_OUT_IN
match protocol tcp
match access-group 102
match protocol udp
match protocol snmp
class-map match-any PREC_3
match ip precedence 3
class-map match-any PREC_2
match ip precedence 2
class-map match-any MISSION-CRITICAL
match ip dscp cs3 af31 af32 af33 cs6
class-map match-any PREC_1
match ip precedence 1
class-map match-any PREC_0
match ip precedence 0
class-map type ngs-w-qos match-any NGSW_QOS_GRP_7
match qos-group 7
class-map match-any PREC_5
match ip precedence 5
class-map match-any PREC_4
match ip precedence 4
class-map match-all CALL-SIGNALING
match ip dscp cs3
class-map match-all COPP-FRAGMENTS
match access-group name coppacl-frag
class-map match-all COPP-BGP
match access-group name coppacl-bgp
class-map match-all COPP-UNDESIRABLE
match access-group name coppacl-drop
class-map match-all COPP-IGP
match access-group name coppacl-igp

```

```

!
policy-map TEST_EXP_CLASS
class EXP_0
  shape average 10000000
class EXP_1
  shape average 10000000
class EXP_2
  shape average 10000000
class EXP_3
  shape average 10000000
class EXP_4
  shape average 10000000
class EXP_5
  shape average 10000000
policy-map TEST_MGMT_TRAFFIC
class MGMT_TRAFFIC
  police cir 100000000
  conform-action transmit
  exceed-action transmit
policy-map type inspect SCADA-OUT
class type inspect SCADA-OUT
  inspect
class class-default
policy-map HOST-INPUT-MARKING
class VOICE
  set dscp ef
class CALL-SIGNALING
  set dscp cs3
class MISSION-CRITICAL-DATA
  set dscp af31
class class-default
policy-map HOST-QUEUE-PACKETS
class VOICE
  priority
class MISSION-CRITICAL
  bandwidth remaining percent 30
  queue-limit 96 packets
class TRANSACTIONAL
  bandwidth remaining percent 20
  queue-limit 96 packets
class class-default
  bandwidth remaining percent 25
  queue-limit 272 packets
policy-map TEST_INPUT
class PREC_CRITIC
  set precedence 5
class PREC_ROUTINE
  set precedence 0
policy-map PARENT

```



```

class class-default
  shape average 1000000000
  service-policy TEST_INPUT
policy-map type inspect IN-IN
class type inspect IN-IN
  inspect
class class-default
policy-map TEST_QOS_OUT
class QOS_GRP_7
  priority 1
class QOS_GRP_6
  priority 2
policy-map TEST_OUT_DSCP
class DSCP_af21_af22
policy-map type inspect OUT-IN
class type inspect OUT-IN
  inspect
class class-default
policy-map UPLINK-QUEUE-PACKETS
class VOICE
  priority level 1
class MISSION-CRITICAL
  priority level 2
class TRANSACTIONAL
  bandwidth remaining percent 20
  queue-limit 96 packets
class class-default
  bandwidth remaining percent 25
  queue-limit 272 packets
policy-map TEST_RADIUS_DSCP
class TEST_DSCP_af11
  set dscp af11
class TEST_DSCP_af12
  set dscp af12
class TEST_DSCP_af21
  set dscp af21
class TEST_DSCP_af22
  set dscp af22
policy-map type ngsw-qos TEST_COS_CLASS_NGSW
class TEST_COS_1_NGSW
  set mpls experimental imposition 1
class TEST_COS_2_NGSW
  set mpls experimental imposition 2
class TEST_COS_3_NGSW
  set mpls experimental imposition 3
class TEST_COS_4_NGSW
  set mpls experimental imposition 4
class TEST_COS_5_NGSW
  set mpls experimental imposition 5

```

```

class SCADA_PTP_NGSW
  set qos-group 7
policy-map type ngsw-qos TEST_COS_PRIORITY
class TEST_COS_1_NGSW
  set qos-group 7
policy-map type ngsw-qos TEST_OUTPUT
class NGSW_QOS_GRP_7
  priority level 1
  set cos 7
  police cir 100000000
  conform-action transmit
  exceed-action drop
policy-map COPP
class COPP-FRAGMENTS
  police 32000 1500 1500 conform-action transmit exceed-action transmit
class COPP-UNDESIRABLE
  police 8000 1500 1500 conform-action drop exceed-action drop
class COPP-BGP
  police 125000 1500 1500 conform-action transmit exceed-action transmit
class COPP-IGP
  police 125000 1500 1500 conform-action transmit exceed-action transmit
class COPP-MANAGEMENT
  police 192000 1500 1500 conform-action transmit exceed-action transmit
class COPP-MONITORING
  police 64000 1500 1500 conform-action transmit exceed-action transmit
class COPP-CRITICAL-APP
  police 50000 1500 1500 conform-action transmit exceed-action transmit
class COPP-ARP
  police 32000 1500 1500 conform-action transmit exceed-action transmit
class COPP-REMAINING-IP
  police 8000 1500 1500 conform-action transmit exceed-action transmit
class class-default
  police 8000 1500 1500 conform-action transmit exceed-action transmit
policy-map type inspect IN-OUT
class type inspect IN-OUT
  inspect
class class-default
policy-map type inspect OUT-SCADA
class type inspect OUT-SCADA
  inspect
class class-default
policy-map type ngsw-qos SCADA_IN
class SCADA_PTP_NGSW
  priority level 1
!
pseudowire-class L2TP_PW_TEST
  encapsulation l2tpv3
  sequencing both
  protocol l2tpv3 L2TP_TUNNEL_TEST

```



```

ip flow monitor StealthWatch_Monitor output
ip address 192.168.100.1 255.255.255.0
no ip redirects
zone-member security OUTSIDE
ip ospf network point-to-point
load-interval 30
negotiation auto
mpls ip
bfd interval 200 min_rx 200 multiplier 3
lacp max-bundle 2
!
interface Multilink1
ip address 3.3.3.2 255.255.255.0
zone-member security OUTSIDE
load-interval 30
mpls ip
ppp multilink
ppp multilink group 1
ppp multilink endpoint string mlp1
service-policy output UPLINK-QUEUE-PACKETS
!
interface Multilink2
ip address 5.5.5.2 255.255.255.0
shutdown
mpls ip
ppp multilink
ppp multilink group 2
ppp multilink endpoint string mlp2
!
interface Multilink100
no ip address
ppp multilink
ppp multilink group 100
!
interface VirtualPortGroup0
description Routing Port pkt capture
ip address 136.1.2.1 255.255.255.0
no mop enabled
no mop sysid
!
interface VirtualPortGroup1
ip address 137.1.2.1 255.255.255.0
ip mtu 1200
zone-member security INSIDE
ip tcp adjust-mss 1160
no mop enabled
no mop sysid
!
interface GigabitEthernet0/0/0

```

```

description connected to asr903-003
ip flow monitor StealthWatch_Monitor input
no ip address
zone-member security OUTSIDE
ip ospf network point-to-point
load-interval 30
negotiation auto
bfd interval 50 min_rx 50 multiplier 3
channel-group 1 mode active
!
interface GigabitEthernet0/0/1
description connected to asr903-003
ip flow monitor StealthWatch_Monitor input
no ip address
load-interval 30
shutdown
negotiation auto
service-policy output UPLINK-QUEUE-PACKETS
!
interface GigabitEthernet0/0/1.1101
encapsulation dot1Q 1101
vrf forwarding VRF_SCADA
ip address 15.1.0.2 255.255.255.0
ip ospf network point-to-point
ip ospf 101 area 0
bfd interval 50 min_rx 50 multiplier 3
!
interface GigabitEthernet0/0/1.1102
encapsulation dot1Q 1102
vrf forwarding VRF_TSCADA
ip address 16.1.0.2 255.255.255.0
ip ospf network point-to-point
bfd interval 50 min_rx 50 multiplier 3
!
interface GigabitEthernet0/0/1.1103
encapsulation dot1Q 1103
vrf forwarding VRF_PLANTLINK
ip address 17.1.0.2 255.255.255.0
ip ospf network point-to-point
bfd interval 50 min_rx 50 multiplier 3
!
interface GigabitEthernet0/0/1.1104
encapsulation dot1Q 1104
vrf forwarding VRF_MGMT
ip address 18.1.0.2 255.255.255.0
ip ospf network point-to-point
bfd interval 50 min_rx 50 multiplier 3
!
interface GigabitEthernet0/0/1.1105

```

```

encapsulation dot1Q 1105
vrf forwarding VRF_GRIDMON
ip address 19.1.0.2 255.255.255.0
ip ospf network point-to-point
bfd interval 50 min_rx 50 multiplier 3
!
interface GigabitEthernet0/0/1.1106
encapsulation dot1Q 1106
vrf forwarding VRF_BUSINESS
ip address 20.1.0.2 255.255.255.0
ip ospf network point-to-point
bfd interval 50 min_rx 50 multiplier 3
!
interface GigabitEthernet0/1/0
switchport access vlan 500
switchport mode access
!
interface GigabitEthernet0/1/1
description connected to TGN card 2 port 4
switchport access vlan 2502
switchport trunk allowed vlan 1-500,502-4094
switchport mode access
mtu 9216
load-interval 30
!
interface GigabitEthernet0/1/2
description connected to IE3400-SA02-01
switchport trunk allowed vlan 1,201,204,210,4001
switchport mode trunk
ip flow monitor StealthWatch_Monitor input
spanning-tree portfast trunk
!
interface GigabitEthernet0/1/3
description connected to PD6500-Camera
switchport access vlan 500
switchport mode access
ip flow monitor StealthWatch_Monitor input
authentication event fail action next-method
authentication host-mode multi-host
authentication order mab
authentication priority mab
authentication port-control auto
authentication violation restrict
mab
dot1x pae authenticator
dot1x timeout tx-period 3
!
interface GigabitEthernet0/1/4
description connected to IE3400-SA02-005

```

```

switchport trunk allowed vlan 1,1001,1051-1062,3001-3006
switchport mode trunk
ip flow monitor StealthWatch_Monitor input
carrier-delay msec 1
media-type rj45
!
interface GigabitEthernet0/1/5
description connected gi0/1/7 sumatra-pp-1
switchport trunk allowed vlan 1,201,501,1501
switchport mode trunk
ip flow monitor StealthWatch_Monitor input
load-interval 30
rep segment 1 edge
rep lsl-retries 3
rep lsl-age-timer 3000
service-policy input TEST_COS_CLASS_NGSW
!
interface GigabitEthernet0/1/6
description REP-Ring connected to IE2KU-REP001
switchport trunk allowed vlan 1,201,501,1501
switchport mode trunk
ip flow monitor StealthWatch_Monitor input
load-interval 30
rep segment 1 edge primary
rep preempt delay 15
rep lsl-retries 3
rep lsl-age-timer 3000
service-policy input TEST_COS_CLASS_NGSW
!
interface GigabitEthernet0/1/7
description connected to .148 PC
switchport access vlan 101
switchport mode access
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky xxxx.xxxx.xxxx
switchport port-security
!
interface GigabitEthernet0/1/8
description connected Ixia
switchport trunk allowed vlan 1,501
switchport mode trunk
spanning-tree portfast trunk
service-policy input TEST_COS_CLASS_NGSW
!
interface GigabitEthernet0/1/9
switchport trunk allowed vlan 1990,1991
switchport mode trunk
shutdown

```

```
rep segment 2 edge primary
!  
interface GigabitEthernet0/1/10  
switchport trunk allowed vlan 1990,1991  
switchport mode trunk  
shutdown  
rep segment 2 edge  
!  
interface GigabitEthernet0/1/11  
switchport mode trunk  
!  
interface AppGigabitEthernet0/1/1  
switchport trunk allowed vlan 2340  
switchport mode trunk  
!  
interface Serial0/2/0:2  
no ip address  
encapsulation ppp  
ppp multilink  
ppp multilink group 1  
!  
interface Serial0/2/1:1  
no ip address  
encapsulation ppp  
ppp multilink  
ppp multilink group 1  
!  
interface Serial0/3/1  
no ip address  
shutdown  
!  
interface Serial0/3/2  
no ip address  
shutdown  
!  
interface Serial0/3/3  
no ip address  
shutdown  
!  
interface Serial0/3/4  
no ip address  
shutdown  
!  
interface Serial0/3/5  
no ip address  
shutdown  
!  
interface Serial0/3/6  
no ip address
```



```

shutdown
!
interface Serial0/3/7
no ip address
shutdown
!
interface Serial0/3/0
physical-layer async
no ip address
encapsulation scada
!
interface Vlan1
no ip address
!
interface Vlan55
description Jumbo-Fragmentation
mtu 9216
ip address 192.168.155.1 255.255.255.0
zone-member security INSIDE
!
interface Vlan101
ip address 192.168.101.1 255.255.255.0
zone-member security SCADA
load-interval 30
service-policy input HOST-INPUT-MARKING
!
interface Vlan119
ip address 11.9.0.1 255.255.255.0
!
interface Vlan177
ip address 177.177.177.1 255.255.255.0
zone-member security INSIDE
!
interface Vlan201
ip address 192.168.211.1 255.255.255.0
zone-member security SCADA
load-interval 30
vrrp 1 name MODBUS-IED-1
vrrp 1 ip 192.168.211.100
vrrp 1 timers learn
vrrp 1 priority 200
service-policy input HOST-INPUT-MARKING
!
interface Vlan210
ip address 192.168.210.1 255.255.255.0
ip nat outside
zone-member security INSIDE
!
interface Vlan500

```

```

description Cisco IP Camera
ip address 192.168.0.1 255.255.255.0
zone-member security INSIDE
load-interval 30
!
interface Vlan501
description REP-Mgmt
ip address 50.1.0.1 255.255.255.0
zone-member security INSIDE
standby 0 ip 50.1.0.100
standby 0 timers msec 30 msec 120
standby 0 priority 200
standby 0 preempt
load-interval 30
service-policy input TEST_MGMT_TRAFFIC
!
interface Vlan1001
no ip address
xconnect 192.168.200.1 1001 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface Vlan1051
description HSRP-GRP-1
ip address 192.168.110.2 255.255.255.0
zone-member security INSIDE
standby 1 ip 192.168.110.1
standby 1 priority 10
standby 1 preempt
standby 1 track 100 decrement 10
bfd interval 999 min_rx 999 multiplier 3
!
interface Vlan1052
ip address 192.168.111.2 255.255.255.0
zone-member security INSIDE
standby 1 track 100 decrement 10
standby 2 ip 192.168.111.1
standby 2 priority 10
standby 2 preempt
bfd interval 999 min_rx 999 multiplier 3
!
interface Vlan1053
ip address 192.168.53.2 255.255.255.0
zone-member security INSIDE
standby 3 ip 192.168.53.1
standby 3 priority 10
standby 3 preempt
standby 3 track 100 decrement 10
standby 4 priority 10
bfd interval 999 min_rx 999 multiplier 3
service-policy input HOST-INPUT-MARKING

```

```

!
interface Vlan1054
 ip address 192.168.54.2 255.255.255.0
 zone-member security INSIDE
 standby 4 ip 192.168.54.1
 standby 4 priority 10
 standby 4 preempt
 standby 4 track 100 decrement 10
 bfd interval 999 min_rx 999 multiplier 3
 service-policy input HOST-INPUT-MARKING
!
interface Vlan1055
 ip address 192.168.55.2 255.255.255.0
 zone-member security INSIDE
 standby 5 ip 192.168.55.1
 standby 5 priority 10
 standby 5 preempt
 standby 5 track 100 decrement 10
 bfd interval 999 min_rx 999 multiplier 3
 service-policy input HOST-INPUT-MARKING
!
interface Vlan1056
 ip address 192.168.56.2 255.255.255.0
 zone-member security INSIDE
 standby 6 ip 192.168.56.1
 standby 6 priority 10
 standby 6 preempt
 standby 6 track 100 decrement 10
 bfd interval 999 min_rx 999 multiplier 3
 service-policy input HOST-INPUT-MARKING
!
interface Vlan1057
 ip address 192.168.57.2 255.255.255.0
 zone-member security INSIDE
 standby 7 ip 192.168.57.1
 standby 7 priority 10
 standby 7 preempt
 standby 7 track 100 decrement 10
 bfd interval 999 min_rx 999 multiplier 3
 service-policy input HOST-INPUT-MARKING
!
interface Vlan1058
 ip address 192.168.58.2 255.255.255.0
 zone-member security INSIDE
 standby 8 ip 192.168.58.1
 standby 8 priority 10
 standby 8 preempt
 standby 8 track 100 decrement 10
 bfd interval 999 min_rx 999 multiplier 3

```

```

service-policy input HOST-INPUT-MARKING
!
interface Vlan1059
ip address 192.168.59.2 255.255.255.0
zone-member security INSIDE
standby 9 ip 192.168.59.1
standby 9 priority 10
standby 9 preempt
standby 9 track 100 decrement 10
bfd interval 999 min_rx 999 multiplier 3
service-policy input HOST-INPUT-MARKING
!
interface Vlan1060
ip address 192.168.60.2 255.255.255.0
zone-member security INSIDE
standby 10 ip 192.168.60.1
standby 10 priority 10
standby 10 preempt
standby 10 track 100 decrement 10
bfd interval 999 min_rx 999 multiplier 3
service-policy input HOST-INPUT-MARKING
!
interface Vlan1061
ip address 192.168.61.2 255.255.255.0
!
interface Vlan1062
ip address 192.168.62.2 255.255.255.0
!
interface Vlan1101
no ip address
!
interface Vlan1990
ip address 19.90.0.1 255.255.255.0
zone-member security INSIDE
vrrp 11 ip 19.90.0.100
vrrp 11 timers learn
vrrp 11 priority 50
!
interface Vlan2002
ip address 20.2.0.1 255.255.255.0
!
interface Vlan2340
description LAN port pkt capture
ip address 136.1.1.1 255.255.255.0
!
interface Vlan2501
no ip address
xconnect 192.168.223.1 2501 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!

```

```

interface Vlan2502
  no ip address
  zone-member security INSIDE
  load-interval 30
  xconnect 192.168.200.1 2502 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface Vlan2503
  no ip address
  xconnect 192.168.200.1 2503 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface Vlan2504
  no ip address
  xconnect 192.168.200.1 2504 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface Vlan2505
  no ip address
  xconnect 192.168.200.1 2505 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface Vlan2506
  no ip address
  xconnect 192.168.200.1 2506 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface Vlan2507
  no ip address
  xconnect 192.168.200.1 2507 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface Vlan2508
  no ip address
  xconnect 192.168.200.1 2508 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface Vlan2509
  no ip address
  xconnect 192.168.200.1 2509 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface Vlan2560
  no ip address
  xconnect 192.168.200.1 2560 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface Vlan3001
  vrf forwarding VRF_SCADA
  ip address 30.0.1.1 255.255.255.0
  ip access-group VRF_SCADA out
  load-interval 30
  service-policy input HOST-INPUT-MARKING
!
interface Vlan3002
  vrf forwarding VRF_TSCADA
  ip address 30.0.2.1 255.255.255.0
  load-interval 30

```

```

service-policy input HOST-INPUT-MARKING
!
interface Vlan3003
vrf forwarding VRF_PLANTLINK
ip address 30.0.3.1 255.255.255.0
load-interval 30
service-policy input HOST-INPUT-MARKING
!
interface Vlan3004
vrf forwarding VRF_MGMT
ip address 30.0.4.1 255.255.255.0
load-interval 30
service-policy input HOST-INPUT-MARKING
!
interface Vlan3005
vrf forwarding VRF_GRIDMON
ip address 30.0.5.1 255.255.255.0
load-interval 30
service-policy input HOST-INPUT-MARKING
!
interface Vlan3006
vrf forwarding VRF_BUSINESS
ip address 30.0.6.1 255.255.255.0
load-interval 30
service-policy input HOST-INPUT-MARKING
!
!
router eigrp 1
bfd interface GigabitEthernet0/0/0
bfd interface GigabitEthernet0/0/1
bfd interface Port-channel1
bfd interface Multilink1
bfd interface Multilink2
network 3.3.3.0 0.0.0.255
network 5.5.5.0 0.0.0.255
network 192.168.0.0
network 192.168.75.0
network 192.168.76.0
network 192.168.100.0
network 192.168.199.1 0.0.0.0
shutdown
!
router ospf 101 vrf VRF_SCADA
shutdown
network 15.1.0.0 0.0.0.255 area 0
network 30.0.1.0 0.0.0.255 area 0
bfd all-interfaces
!
router ospf 102 vrf VRF_TSCADA

```

```

shutdown
network 16.1.0.0 0.0.0.255 area 0
network 30.0.2.0 0.0.0.255 area 0
bfd all-interfaces
!
router ospf 103 vrf VRF_PLANTLINK
shutdown
network 17.1.0.0 0.0.0.255 area 0
network 30.0.3.0 0.0.0.255 area 0
bfd all-interfaces
!
router ospf 104 vrf VRF_MGMT
shutdown
network 18.1.0.0 0.0.0.255 area 0
network 30.0.4.0 0.0.0.255 area 0
bfd all-interfaces
!
router ospf 105 vrf VRF_GRIDMON
shutdown
network 19.1.0.0 0.0.0.255 area 0
network 30.0.5.0 0.0.0.255 area 0
bfd all-interfaces
!
router ospf 106 vrf VRF_BUSINESS
shutdown
network 20.1.0.0 0.0.0.255 area 0
network 30.0.6.0 0.0.0.255 area 0
bfd all-interfaces
!
router ospf 1
router-id 192.168.199.1
network 3.3.3.0 0.0.0.255 area 0
network 192.168.100.0 0.0.0.255 area 0
network 192.168.199.1 0.0.0.0 area 0
bfd all-interfaces
!
router bgp 200
bgp router-id interface Loopback0
bgp log-neighbor-changes
neighbor 192.168.201.6 remote-as 200
neighbor 192.168.201.6 update-source Loopback0
neighbor 192.168.201.6 fall-over bfd multi-hop
!
address-family ipv4
network 11.9.0.0 mask 255.255.255.0
network 19.90.0.0 mask 255.255.255.0
network 20.1.0.0 mask 255.255.255.0
network 20.2.0.0 mask 255.255.255.0
network 50.1.0.0 mask 255.255.255.0

```

```
network 137.1.2.0 mask 255.255.255.0
network 177.177.177.0 mask 255.255.255.0
network 192.168.0.0
network 192.168.53.0
network 192.168.54.0
network 192.168.55.0
network 192.168.56.0
network 192.168.57.0
network 192.168.58.0
network 192.168.59.0
network 192.168.60.0
network 192.168.101.0
network 192.168.110.0
network 192.168.155.0
network 192.168.199.2 mask 255.255.255.255
network 192.168.210.0
network 192.168.211.0
neighbor 192.168.201.6 activate
neighbor 192.168.201.6 send-community extended
neighbor 192.168.201.6 next-hop-self
neighbor 192.168.201.6 send-label
exit-address-family
!
address-family vpnv4
neighbor 192.168.201.6 activate
neighbor 192.168.201.6 send-community extended
neighbor 192.168.201.6 next-hop-self
exit-address-family
!
address-family ipv4 vrf VRF_BUSINESS
redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_GRIDMON
redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_MGMT
redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_PLANTLINK
redistribute connected
exit-address-family
!
address-family ipv4 vrf VRF_SCADA
redistribute connected
exit-address-family
!
```



```

address-family ipv4 vrf VRF_TSCADA
  redistribute connected
exit-address-family
!
!
virtual-service
  signing level unsigned
!
!
!
iox
ip tcp selective-ack
ip tcp mss 1460
ip tcp window-size 131072
ip http server
ip http authentication local
ip http secure-server
ip forward-protocol nd
ip ftp source-interface Loopback1
ip ftp username xxxxxxxx
ip ftp password xxxxxxxx
ip tftp source-interface Loopback1
ip nat inside source list NAT_ACL interface Port-channel1 overload
ip route 192.168.221.1 255.255.255.255 Port-channel1
ip route 192.168.222.1 255.255.255.255 Port-channel1
ip route vrf VRF_BUSINESS 0.0.0.0 0.0.0.0 20.1.0.1
ip route vrf VRF_GRIDMON 0.0.0.0 0.0.0.0 19.1.0.1
ip route vrf VRF_MGMT 0.0.0.0 0.0.0.0 18.1.0.1
ip route vrf VRF_PLANTLINK 0.0.0.0 0.0.0.0 17.1.0.1
ip route vrf VRF_SCADA 0.0.0.0 0.0.0.0 15.1.0.1
ip route vrf VRF_TSCADA 0.0.0.0 0.0.0.0 16.1.0.1
ip ssh bulk-mode 131072
ip ssh source-interface Loopback1
!
!
ip access-list standard CVPOOL
  10 permit 169.254.0.0 0.0.0.255
ip access-list standard NAT_ACL
  10 permit 169.254.0.0 0.0.0.3
  20 permit 50.1.0.0 0.0.0.255
!
ip access-list extended FTP_IN_OUT
  1 permit tcp 192.168.110.0 0.0.0.255 host 192.168.2.176 eq ftp log
  2 permit tcp host 192.168.199.2 host 192.168.2.176 eq ftp log
  3 permit tcp host 192.168.199.2 host 192.168.2.206 eq ftp
  13 permit tcp 50.1.0.0 0.0.0.255 host 192.168.2.176 eq ftp log
ip access-list extended FTP_OUT_IN
  1 permit tcp host 192.168.2.176 192.168.110.0 0.0.0.255 eq ftp
  2 permit tcp host 192.168.2.176 host 192.168.199.2 eq ftp

```

3 permit tcp host 192.168.2.206 host 192.168.199.2 eq ftp
ip access-list extended MISSION-CRITICAL-DATA

10 permit tcp any eq 20000 any
11 permit tcp any eq 20001 any
12 permit tcp any eq 20002 any
13 permit tcp any eq 20003 any
14 permit tcp any eq 20004 any
15 permit tcp any eq 20005 any
20 permit tcp any eq 20100 any
30 permit tcp any eq 20101 any
40 permit tcp any eq 20102 any
50 permit udp any eq 1234 any
60 permit udp any eq 1235 any
70 permit icmp 192.168.101.0 0.0.0.255 host 192.168.4.171

ip access-list extended MISSION-CRITICAL-DATA-IN

9 permit tcp host 192.168.101.2 eq 20000 host 192.168.4.171
10 permit tcp host 192.168.101.2 eq 20001 host 192.168.4.171
11 permit tcp host 192.168.101.2 eq 20002 host 192.168.4.171
12 permit tcp host 192.168.101.2 eq 20003 host 192.168.4.171
13 permit tcp host 192.168.101.2 eq 20004 host 192.168.4.171
14 permit tcp host 192.168.101.2 eq 20005 host 192.168.4.171
19 permit tcp host 192.168.101.2 eq 20100 host 192.168.4.171
29 permit tcp host 192.168.101.2 eq 20200 host 192.168.4.171
39 permit tcp host 192.168.101.2 eq 20300 host 192.168.4.171
41 permit tcp host 192.168.211.2 host 192.168.2.206 eq 502
50 permit udp any any
70 permit icmp 192.168.101.0 0.0.0.255 host 192.168.4.171

ip access-list extended MISSION-CRITICAL-DATA-OUT

9 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20000
10 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20001
11 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20002
12 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20003
13 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20004
14 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20005
19 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20100
29 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20200
39 permit tcp host 192.168.4.171 host 192.168.101.2 eq 20300
41 permit tcp host 192.168.2.206 host 192.168.211.2 eq 502
50 permit udp any any
70 permit icmp 192.168.101.0 0.0.0.255 host 192.168.4.171

ip access-list extended VRF_SCADA

1 deny ip 3.0.1.0 0.0.0.255 any log
2 deny ip 4.0.1.0 0.0.0.255 any log
3 deny ip 5.0.1.0 0.0.0.255 any log
4 deny ip 6.0.1.0 0.0.0.255 any log
5 deny ip 7.0.1.0 0.0.0.255 any log
6 deny ip 8.0.1.0 0.0.0.255 any log
7 deny ip 9.0.1.0 0.0.0.255 any log
8 deny ip 10.0.1.0 0.0.0.255 any log

```

9 deny ip 11.0.1.0 0.0.0.255 any log
10 permit ip 12.0.1.0 0.0.0.255 host 30.0.1.2 log
ip access-list extended coppacl-bgp
10 permit tcp any any eq bgp
20 permit tcp any eq bgp any
ip access-list extended coppacl-classification
10 permit tcp any any eq www
20 permit tcp any any lt 1024
30 permit tcp any any gt 1024
40 permit udp any any lt isakmp
50 permit udp any any gt 1000
60 permit ip any any
ip access-list extended coppacl-critical-app
10 permit ip any host 224.0.0.2
20 permit ip any host 224.0.0.102
30 permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
40 permit udp any eq bootps any eq bootps
ip access-list extended coppacl-drop
10 permit udp any any eq 1434
20 permit udp any any eq 1975
ip access-list extended coppacl-frag
10 permit tcp any any fragments
20 permit udp any any fragments
30 permit icmp any any fragments
40 permit ip any any fragments
ip access-list extended coppacl-igp
10 permit ospf any host 224.0.0.5
20 permit ospf any host 224.0.0.6
30 permit ospf any any
40 permit eigrp any any
50 permit pim any any
ip access-list extended coppacl-mgmt
10 permit tcp any any established
20 permit tcp any any eq telnet
30 permit tcp any any eq 22
40 permit udp any any eq snmp
50 permit udp any any eq ntp
60 permit tcp any any eq tacacs
70 permit udp any any eq syslog
ip access-list extended coppacl-monitor
10 permit icmp any any ttl-exceeded
20 permit icmp any any port-unreachable
30 permit icmp any any echo-reply
40 permit icmp any any echo
50 permit icmp any any packet-too-big
!
ip radius source-interface Loopback1
ip sla 1
icmp-echo 192.168.2.108 source-interface Loopback1

```

```

ip sla schedule 1 life forever start-time now
ip sla 2
  icmp-echo 192.168.2.176 source-interface Loopback1
  frequency 5
ip sla schedule 2 life forever start-time now
ip sla 2006
  udp-echo 177.177.177.2 2525 source-ip 177.177.177.1 source-port 2525
  frequency 5
ip sla schedule 2006 life forever start-time now
ip sla 2007
  udp-echo 177.177.177.3 2526 source-ip 177.177.177.1 source-port 2526
  frequency 5
ip sla schedule 2007 life forever start-time now
logging origin-id hostname
logging source-interface Loopback1
logging host 192.168.5.11
logging host 192.168.2.206
ip access-list extended 101
  1 deny udp any eq syslog host 192.168.2.206
log ip access-list extended 102
  10 permit ip any any
arp 169.254.2.2 5254.dd42.d460 ARPA
arp 136.1.1.3 5254.dd05.96c9 ARPA
!
mpls ldp router-id Loopback0
snmp-server community public RO
snmp-server trap link ietf
snmp-server trap link switchover
snmp-server location SUMATRA_001
snmp-server contact SCADA
snmp-server host 192.168.5.11 version 2c public
snmp ifmib ifindex persist
!
tftp-server bootflash:xxxxxxxxx_20210614221401703.lic
!
!
!
radius server CISCOISE
  address ipv4 192.168.2.202 auth-port 1812 acct-port 1813
  pac key xxxxxx
!
!
control-plane
  service-policy input COPP
!
scada-gw protocol dnp3-serial
  channel serial
  unsolicited-response enable
  session serial

```

```

attach-to-channel serial
scada-gw protocol dnp3-ip
channel ip
tcp-connection local-port 23000 remote-ip 192.168.4.171/0
session ip
attach-to-channel ip
map-to-session serial
!
!
!
!
!
line con 0
exec-timeout 0 0
stopbits 1
line aux 0
line 0/3/0
line vty 0 4
logging synchronous
login authentication local
history size 50
transport input all
line vty 5 15
logging synchronous
login authentication local
history size 50
transport input all
!
!
monitor session 1 type erspan-source
source interface Gi0/1/0 - 11
destination
erspan-id 1
mtu 1464
ip address 136.1.1.3
origin ip address 136.1.1.1
!
!
monitor session 5 type erspan-source
source interface Po1
source interface V1101
destination
erspan-id 5
mtu 1464
ip address 136.1.2.3
origin ip address 136.1.2.1
!
!
monitor session 20 source vlan 1

```

```

monitor session 20 destination remote vlan 1501
network-clock synchronization automatic
call-home
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be used as contact email address to send SCH
notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
  active
  destination transport-method http
ntp master
ntp refclock ptp
!
ptp clock boundary domain 0 profile power
clock-port dynamic1
  transport ethernet multicast interface Gi0/1/4
clock-port dynamic2
  transport ethernet multicast interface Gi0/1/2
  vlan 4001
clock-port dynamic3
  transport ethernet multicast interface Gi0/1/5
clock-port dynamic4
  transport ethernet multicast interface Gi0/1/6
clock-port dynamic5
  transport ethernet multicast interface Gi0/1/8
!
!
!
!
!
!
app-hosting appid sensor3
app-vnic AppGigabitEthernet trunk
  vlan 2340 guest-interface 3
  guest-ipaddress 136.1.1.3 netmask 255.255.255.0
app-vnic gateway0 virtualportgroup 1 guest-interface 0
  guest-ipaddress 137.1.2.3 netmask 255.255.255.0
app-vnic gateway1 virtualportgroup 0 guest-interface 1
  guest-ipaddress 136.1.2.3 netmask 255.255.255.0
app-default-gateway 137.1.2.1 guest-interface 0
app-resource docker
  run-opts 1 --rm
app-resource profile custom
  cpu 1155
  memory 2048
  persist-disk 8192
  vcpu 2
end

```