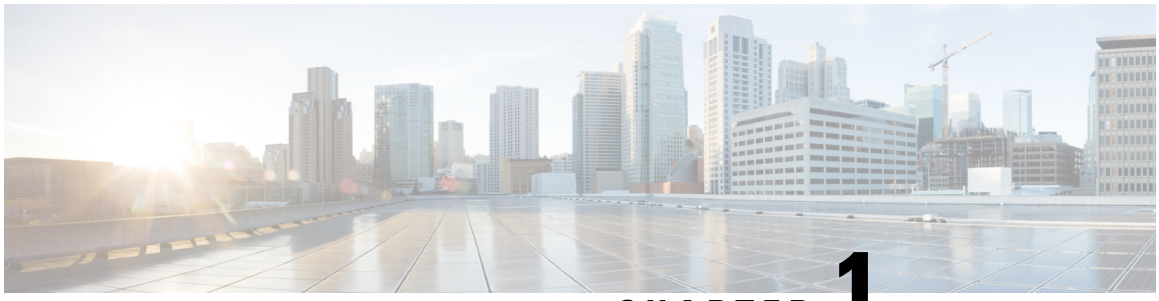
SD-WAN for Utility Distributed Automation

First Published: 2023-05-11

Last Modified: 2023-05-11

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Introduction

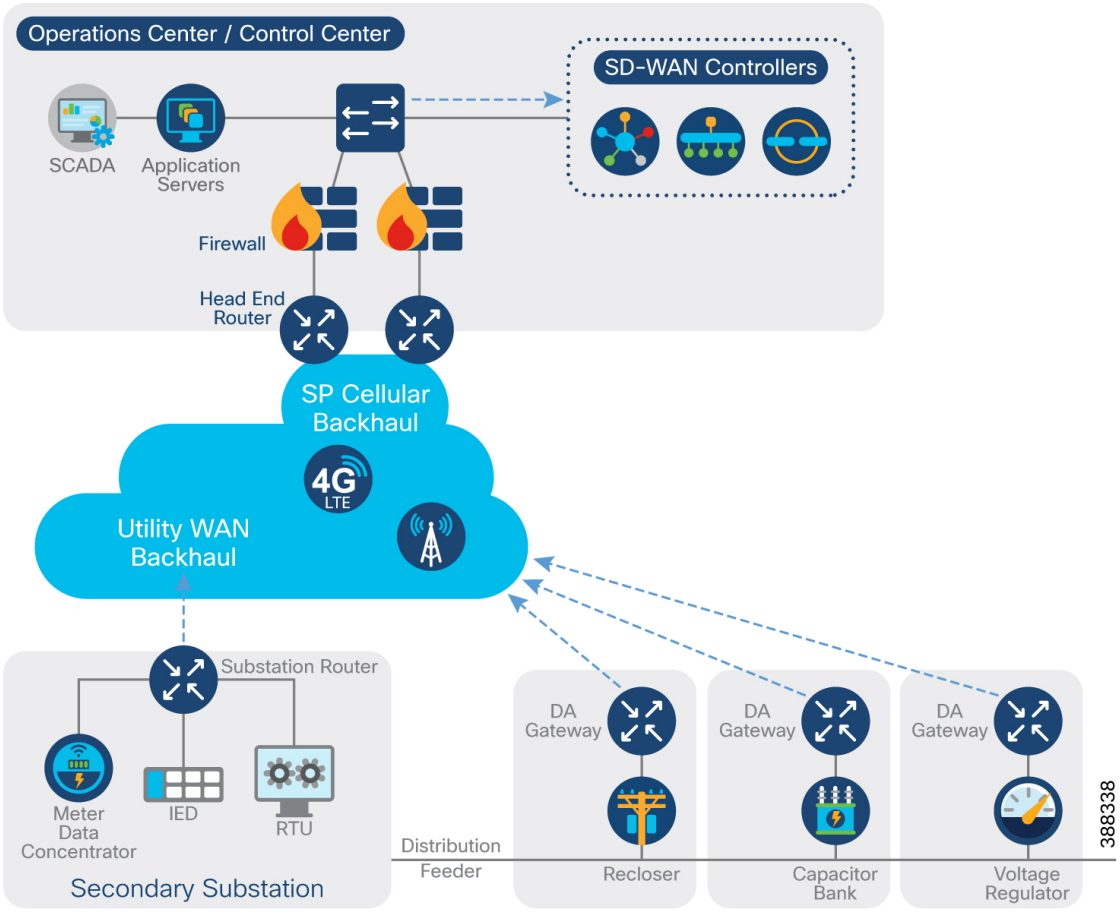
This document describing the Distribution Automation (DA) solution builds on top of the horizontal information captured in the IoT Industrial Router Extension to SD-WAN Small Branch Design Case Study guide. This document is written based on software versions 17.10.1 for IOS-XE, and 20.10 for vManage. For device onboarding, please refer to the SD-WAN Enterprise CVD guide. The purpose of this document is aimed at enabling communication between DA utility controller devices and the Control Center.

The goals of Distribution Automation in the Utility grid is for the control and monitoring of grid assets for tasks such as real-time adjustment to changing load conditions, integration of distributed generation assets, perform fault location identification and service restoration (FLISR), and reacting to failure conditions within the Distribution grid and other use cases, usually without operator intervention.

To enable these goals, multiple controller devices, referred to in this document as field devices, are deployed along the distribution feeder lines as well as at the distribution substations. These controller devices can provide information to the Utility Control Center and are also capable of acting upon control commands received from the Control Center. To enable this bidirectional communication between controller device and the Control Center, a secure communication infrastructure is needed.

Cisco Distribution Automation (DA) gateways can be leveraged to achieve this secure communication path between field controller devices and Control Center. Cisco DA gateways can be used to connect to a local controller device using IP/Ethernet or serial interfaces. Cisco DA gateways help in relaying critical information from field devices to the Utility Control Center. The decision (manual/automatic) made at the Control Center can then be relayed back to the field devices, which can act upon the instruction received from the Utility Control Center. Real-time data acquisition and communication with utility databases and other automated systems is made possible.

Figure 1: SD-WAN Architecture for Distribution Automation solution



The SD-WAN controllers, SCADA and other Application servers are hosted within this Distribution System Operator (DSO) Control Center layer. Example of backhaul types could be public/private LTE or Utility owned WAN backhaul such as MPLS, Metro ethernet, Microwave radio or leased lines.

Within the secondary substation block, the Cisco IR1101 should be positioned as a Secondary Substation router. It is certified for substation use by IEC61850-3 and IEEE1613, has a small compact form factor, and offers multiple backhaul options such as Ethernet, DSL, 4G/5G cellular.

Along the distribution network feeders, the IR1101 should be positioned as a Distribution Automation gateway. It can be easily mounted with a DA device cabinet and be powered by the same DC supply. It also has extended environmental capabilities to cope with the variations in temperature, humidity, and vibration.

This document addresses these communications requirements as an architecture and addresses the key use cases that follow.

Distribution Automation technologies are commercially available for wide-scale utility deployments. The key for the utility is to identify and unlock the value that these solutions provide. Applications that may have the greatest potential are those that directly assist operations and efficiency such as management of peak load via demand response, predictive technologies for advanced maintenance or equipment replacement and secure communications for equipment, and system restoration technologies.

Automated control of devices in distribution systems is the closed-loop control of switchgear, voltage controllers, and capacitors based on recommendations of the distribution system optimization algorithms. These closed loop systems often have rigorous communications systems requirements that vary from manufacturer to manufacturer and by application. The communications system must meet the most rigorous standards and do so at scale. Volt/VAR control is one example of a key application to optimize the distribution grid for the utility.

A utility fault may occur when a short circuit between two phases occurs or for other reasons. The fault in any one of the feeders can affect many customers. Before the fault on the line can be corrected, it must be identified and isolated from the larger utility network. This identification and isolation is done by placing reclosers in the network. The reclosers are, in turn, connected to the recloser controller. The recloser controller is a connected gateway, which establishes a connection to the Control Center.

When a fault is identified, the reclosers perform the trip operation and the fault is isolated from the larger network. This trip operation can be automated or can be sent from the Control Center. Once the fault is corrected, the close operation on the circuit, which is done from the Control Center, can be executed. This is commonly referred to as Fault, Location, Isolation, and Service Restoration (FLISR), and is also one of the key use cases for a utility in a grid resiliency effort.

Distribution Automation Use Cases

Distribution Automation (DA) refers to the monitoring and control of devices located on the distribution feeders, such as line reclosers, load break switches, sectionalizers, capacitor banks and line regulators, and devices located in the distribution substation. DA is an overlay network deployed in parallel to the distribution feeder. It enables two-way communication between controllers used in the distribution feeder and the intelligence application that resides in the Utility Control Center or Secondary Substation for improving grid reliability, availability, and control.

The distribution feeder comes out of the distribution Substation. Various distribution automation controllers for example, Intelligent Electronic Devices in the feeder, such as the recloser controller, voltage regular controller, and capacitor bank controller, are positioned along the distribution feeder. Key functions and operations of Distribution Automation include protecting the distribution system, managing the fault, measuring the energy usage, managing the assets, and controlling and managing system performance.

Some of the key Distribution Automation use cases are:

- Grid Visibility and Control
  - Distribution Feeder and Secondary Substation Monitoring and Control (DSCADA)
  - Remote Asset Monitoring
- Grid Efficiency
  - Integrated Volt/VAR Control (IVVC)
  - Conservation Voltage reduction (CVC)
- Grid Reliability
  - Fault Location, Isolation, Service Restoration (FLISR)

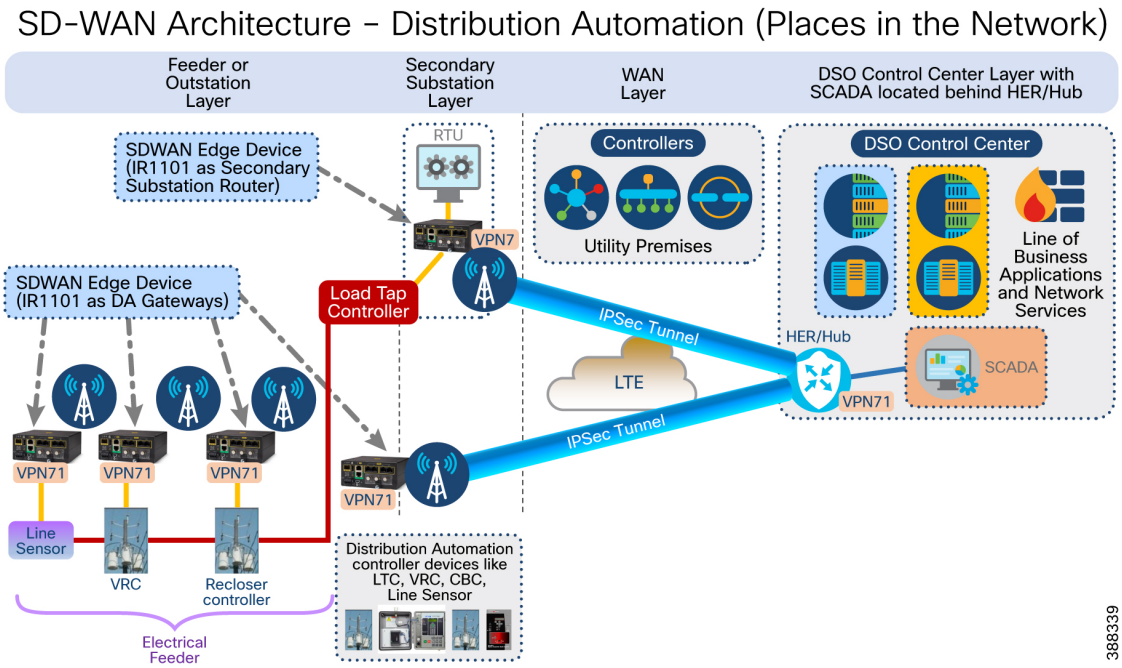
Refer to the Distribution Automation Use Cases section of the Distribution Automation – Secondary Substation Design Guide for more details.

Places In Network

The SD-WAN architecture for the Distribution Automation solution can be divided into multiple layers as shown below:

1. DSO Control Center layer with the distribution management system
2. WAN layer
3. Secondary Substation Layer
4. Feeder or Outstation Layer

Figure 2: SD-WAN Architecture for DA – Places in the Network



Referring to the figure above, notice:

- VPN 71 is representative of SERVICE VPN for SCADA. Customer can select the VPN number of their choice.
- End-to-End VPN segmentation. All SCADA communication contained within VPN 71.
- Other services can be on different VPNs with service isolation
- Hub and Spoke topology is used to minimize the number of connections.
- SCADA communication between Hub and Edge devices happen inside a secure IPSEC Tunnel.

The Cisco SD-WAN Edge devices could be used:

- To enable connectivity for IP-aware outstation devices.
- To enable connectivity for legacy serial outstation devices.

DSO Control Center Layer

The DSO Control Center layer is located behind centralized SD-WAN Edge routers configured to serve the role of the Hub, usually located at the utility Control Center. This specific SD-WAN Edge router is referred to in the rest of the document as HER (Head-End Router). Supervisory Control and Data Acquisition (SCADA) applications are located in this DSO Control Center layer, behind the HER. Various other utility specific applications will also be hosted in this layer.

In this architecture, the SD-WAN controllers are co-located within the DSO Control Center. The SD-WAN controllers should have one leg in the WAN layer as they should be reachable from the other SD-WAN Edge devices like DA gateways and HER for bootstrapping and establishing SD-WAN control connections.

The HER has one leg in the DSO Control Center layer and another leg in the WAN layer. For details about using multiple Hub routers and optimal positioning of SD-WAN controller devices, please refer to the to the Cisco SD-WAN Design Guide and other reference design guides.

WAN Layer

The WAN layer provides the underlying connectivity between DA Gateways and HER. It could be via LTE/5G public internet backhaul, LTE/5G Private backhaul, Ethernet or any other form of WAN technology, which could provide the underlay network. The underlay network provides the basic IP reachability from DA gateway to HER. Then the SD-WAN solution creates secure IPSEC Tunnels over this underlay layer (for example, public/private LTE, 5G) between the DA gateways and the HER. This is called the overlay network.

Secondary Substation Layer

This layer can also be referred to as the distribution substation layer. Industrial Routers positioned within the Secondary Substation premises fall under this layer and are referred to as secondary substation routers, serving as an SD-WAN Edge router in the SD-WAN Architecture. The secondary substation routers connect and aggregate traffic from various IEDs and RTUs present in Secondary Substations to the DSO Control Center.

Feeder or Outstation Layer

Electrical distribution feeder lines originate from the distribution substation and run across the distribution region to serve residential and commercial premises.

Along the Electrical distribution feeder lines, the Cisco DA Gateways are installed with Utility DA Controller devices within a field cabinet, mostly one for one. The Cisco DA Gateways will connect to the DSO Control Center over the IPSEC Tunnel that has been established over the underlying WAN layer.

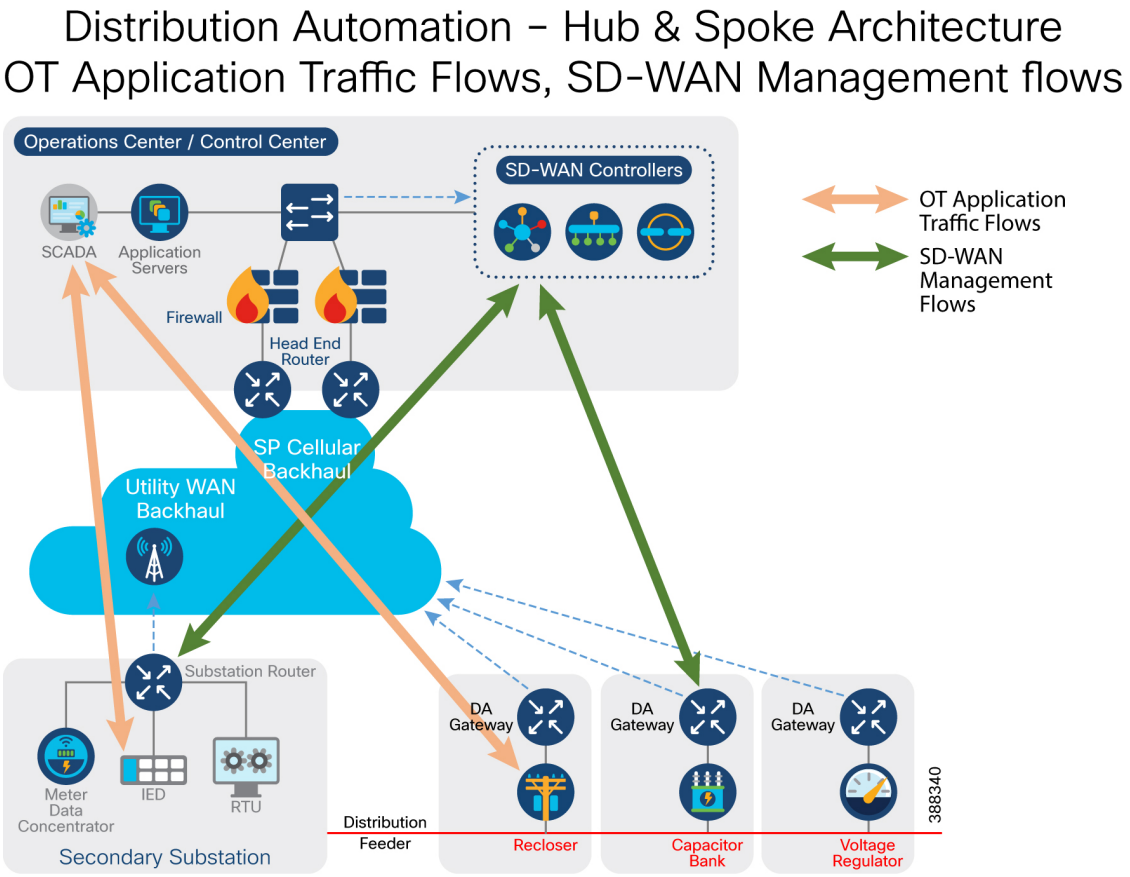
After the DA Gateways successfully establish control connections with SD-WAN controllers, the routers can then be provisioned with validated templates to serve various application traffic or DA use cases. This includes configuring the DA gateways with the last mile connectivity, enabling communications to utility controller devices over Ethernet or Serial interfaces and other configuration required for security or management.

Hub and Spoke Architecture

The architecture follows a centralized Hub and Spoke design.

- Head-End Routers (HER) located in DSO Control Center performs the role of the Hub router.
- Secondary substation routers/DA gateways perform the role of the Spoke routers.

Figure 3: Distribution Automation – Hub and Spoke Architecture – Application Traffic Flows



Application traffic flow follows North South type of communication between the DSO Control Center and the IEDs and DA controller devices.

Example of North South OT/Application Traffic communication as follows:

- Communication between SCADA located in DSO Control Center and Recloser controller located behind DA Gateway.
- Communication between SCADA located in DSO Control Center and IED/RTU located behind Secondary Substation Router

Similarly, the SD-WAN management flows occur between the SD-WAN controllers and the DA Gateways (Cisco SD-WAN Edge devices).

East-West communication (field device to field device) between the DA gateways is not covered in this version of the design.

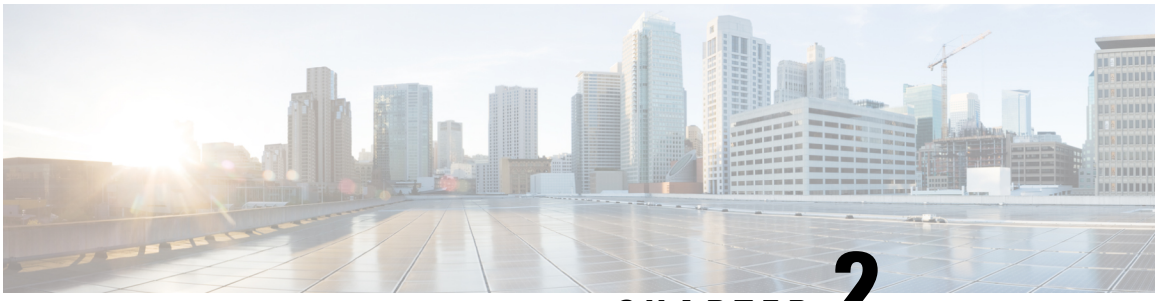
Traffic Isolation with Service VPNs

Service VPNs are a fundamental part of an SD-WAN overlay network. They are defined to isolate and securely transport the North South critical OT/Application Traffic communication from the rest of the non-critical communication. Different traffic types can and should be segregated by separate Service VPNs.

As each service VPN is segregated, each VPN maintains its own routing table allowing the Utility to use its own addressing and subnet plans per VPN.

Within a service VPN, any connected and static routes can be advertised under the Advertise OMP sub section.

The NAT section under the Service VPN template can be used to enable connectivity to IP-aware SCADA outstations. These outstations are located behind either the secondary substation router or the DA gateway router along the feeder.



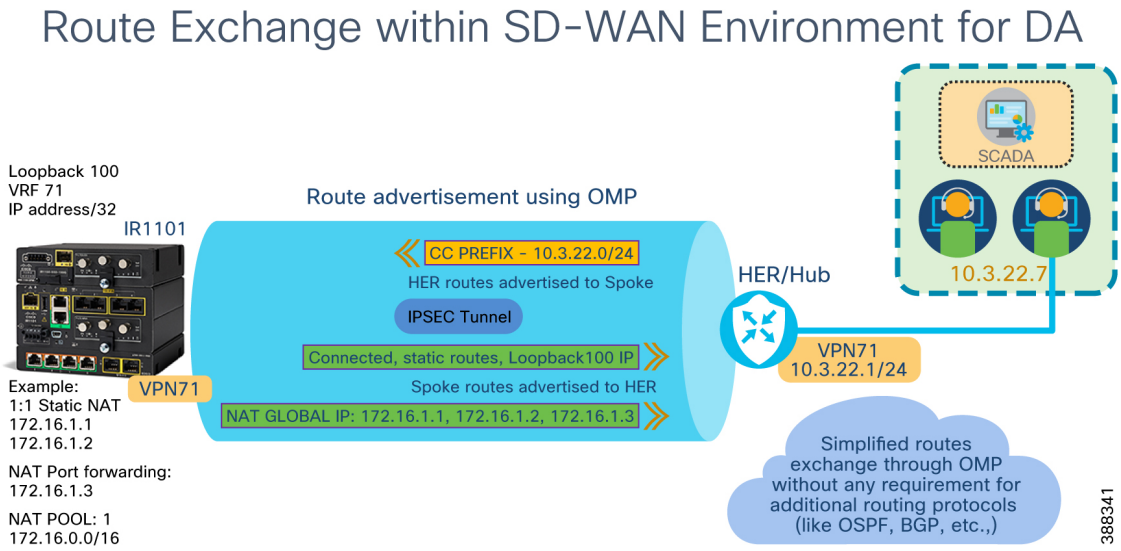
CHAPTER 2

Connecting SCADA Outstations Using Cisco SD-WAN Edge Gateway

Route Exchange within SD-WAN environment for DA

This section shows how the routes are exchanged between the Cisco SD-WAN Edge gateway (IR1101) and the Hub routers.

Figure 4: Route Exchange within SD-WAN Environment for DA



The above figure shows how the routes are exchanged between the Hub and Spokes.

Routes advertised by Hub to Spoke:

- The Control Center prefix (CC PREFIX) – 10.3.22.0/24

Routes advertised by Spoke to Hub, showing NAT also used in this scenario for end devices:

- The Static NAT Translated Source IP addresses 172.16.1.1, 172.16.1.2
- The PORT FORWARD NAT Translated Source IP addresses 172.16.1.3
- Loopback IP, connected subnets (such as local switchport VLANs) and static routes on the IR1101.

Enabling connectivity to IP-aware outstations

Connectivity to IP outstations is enabled using Feature templates in vManage.

Commonly used templates are:

- The Cisco VPN template to isolate the communication inside a Service VPN and to use NAT functionality
- The SVI Template is used to create a switched virtual interface like for example, interface vlan123, and to add switched Layer2 interfaces under it. If IP-aware outstations are connected to layer2 interfaces of the Cisco SD-WAN Edge gateway, this template should be used.

Refer to the *Static 1:1 NAT, Static N:1 Port Forwarding, and Hybrid NAT/PAT*section of the IoT Industrial Router Extension to SD-WAN Small Branch Design Case Study guide for general understanding of NAT usage.

The outstation can be presented by the DA Gateway to the Control Center using a translated source IP address (dedicated or shared). If a dedicated address is used, it is referred as 1:1 Static NAT scenario. If a shared IP is used in combination with dedicated ports, it referred as NAT Port Forwarding.Cisco SD-WAN Gateways enable last mile connectivity to the customer field devices such as controller devices, IEDs, other IP aware devices. These last mile customer owned field devices are referred to as **outstations** in this section.

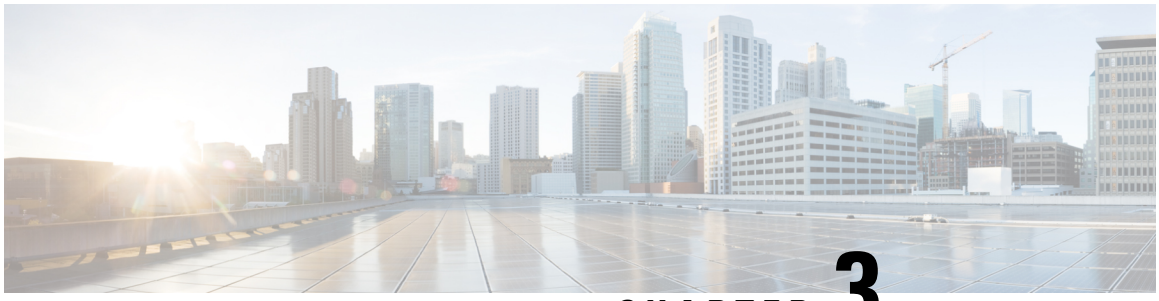
Note The Translated source IP address is often referred to as Global IP in this document. Control Center uses this IP (and port) to reach the appropriate outstation behind Cisco SD-WAN Edge gateway (DA Gateway).

For deployments involving tens of thousands of these last mile outstations, having the field technician configure each outstation with a unique IP address is more prone to human error. This assignment of unique IP address (Intra service-VPN translated source IP address) should be within the control of the vManage user – who can remotely configure and (if needed) reconfigure, from the comfort of the Control Center.

There are four approaches to connect the outstation to the Hub Router and Control Center:

- **Dedicated routable IP address** - A dedicated routable IP subnet used for each DA gateway VLAN. The utility must maintain a record of each site subnet used and not duplicate the subnets across any sites.
- **Static NAT (1:1)** - The DA Gateway requires one unique global IP address to represent each outstation. DA Gateway serving 2 outstations would require 2 NAT global IP. For example, NAT global IP1 is required to represent outstation 1. NAT global IP2 is required to represent outstation 2, and so on.
- **Port Forwarding (N:1)** – 1 global IP for all outstations behind DA Gateway. DA Gateway requires one common global IP address to represent multiple outstations. Unique Port numbers are then used to forward traffic to the desired outstation. DA gateway serving 4 outstations would require 1 NAT global IP. Combination of one common NAT global IP + unique port is used to represent unique **resources** on each outstation device or separate devices. For example:
  - NAT global IP3 + port 20000 could represent a DNP3 outstation located behind the DA gateway.
  - NAT global IP3 + port 20001 could represent a second DNP3 outstation located behind the DA gateway.
  - NAT global IP3 + port 2222 could represent SSH access to DNP3 outstation located behind the DA gateway.
  - NAT global IP3 + port 502 could represent MODBUS outstation located behind the DA gateway.

- Hybrid Approach: Using combination of both the approaches described in the second and third point.
  - Both the approaches can co-exist, but for different outstations. For example:
    - Outstation1 can be represented with NAT global IP 1 (1:1 Static NAT)
    - Outstation2 can be represented with NAT global IP 2 (1:1 Static NAT)
    - Outstations 3 and 4 are represented with NAT global IP 3 + port combinations (Port Forwarding)



CHAPTER 3

Configuration Guideline for Private/Local IP Outstations

Adopting the “Keep it Simple” approach for field technician, the configuration of outstation by the field technician could stay the same, whether it is the Static NAT or the Port Forwarding approach.

This section gives a templated guideline for the field technicians to configure the private local IP address on the outstations connected behind the Cisco SD-WAN Edge gateway. In the table below is a list of a simple allocation of Local IP address ranges for distinct types of outstations. Choose a preferred Local IP range for different types of the outstation.

Table 1: Field Technicans Reference Table Sample

Type of Outstation	NAT Local IP Range
DNP3 Outstation	192.168.0.121- 192.168.0.150
MODBUS Outstation	192.168.0.151- 192.168.0.200
T104 Outstation	192.168.0.41- 192.168.0.80

The technicians configure the IP devices connected behind the DA gateway with an IP address selected from the relevant local IP pool.

Keeping it simple is very important. Adapting this approach would mean the field technician would just require the table in his hand, and can set the same configuration at location1, location 2, location 10, location 1000, location 10k, and so on.

Example1: Field technician to deploy multiple DNP3 outstations behind the Cisco DA Gateway.

The DNP3 Outstation range is used because they are all DNP3 outstations.

- NAT Local IP range for DNP3 outstation is 192.168.0.121-192.168.0.150
- Configure the first DNP3 outstation with first IP of the range (say 192.168.0.121)
- Configure the second DNP3 outstation with second IP of the range (say 192.168.0.122)

- Additional DNP3 outstations can be configured with successive IPs like 192.168.0.123, 192.168.0.124 and so on.

Example2: Field technician to deploy 2 DNP3 outstations and 1 MODBUS Outstation.

- NAT Local IP range for DNP3 outstation is 192.168.0.121-192.168.0.150
- NAT Local IP range for MODBUS outstation is 192.168.0.151-192.168.0.200
- Configure the first DNP3 outstation with 192.168.0.121
- Configure the second DNP3 outstation with 192.168.0.122
- Configure the first MODBUS Outstation with 192.168.0.151

Example3: Field technician to deploy 3 T104 outstations and 1 MODBUS Outstation.

- NAT Local IP range for T104 outstation is 192.168.0.41-192.168.0.80
- NAT Local IP range for MODBUS outstation is 192.168.0.151-192.168.0.200
- Configure the first T104 outstation with 192.168.0.41
- Configure the second T104 outstation with 192.168.0.42
- Configure the third T104 outstation with 192.168.0.43
- Configure the first MODBUS Outstation with 192.168.0.151

Mapping between private IP subnet and NAT global IP address

Refer to the *Mapping between private IP subnet and NAT global IP address* section of the "IoT Industrial Routers Extension to SD-WAN Small Branch Design Case Study" guide.

NAT - 1:1 STATIC scenario

This section corresponds to "Static 1:1 NAT" section of "IoT Industrial Routers Extension to SD-WAN Small Branch Design Case Study" guide. The focus is on on a scenario where each outstation, controller device, or IED is represented to the Operations Center with a unique single NAT Global IP address.

Example scenario: Field technician to deploy 3 DNP3 outstations and 1 MODBUS Outstation.

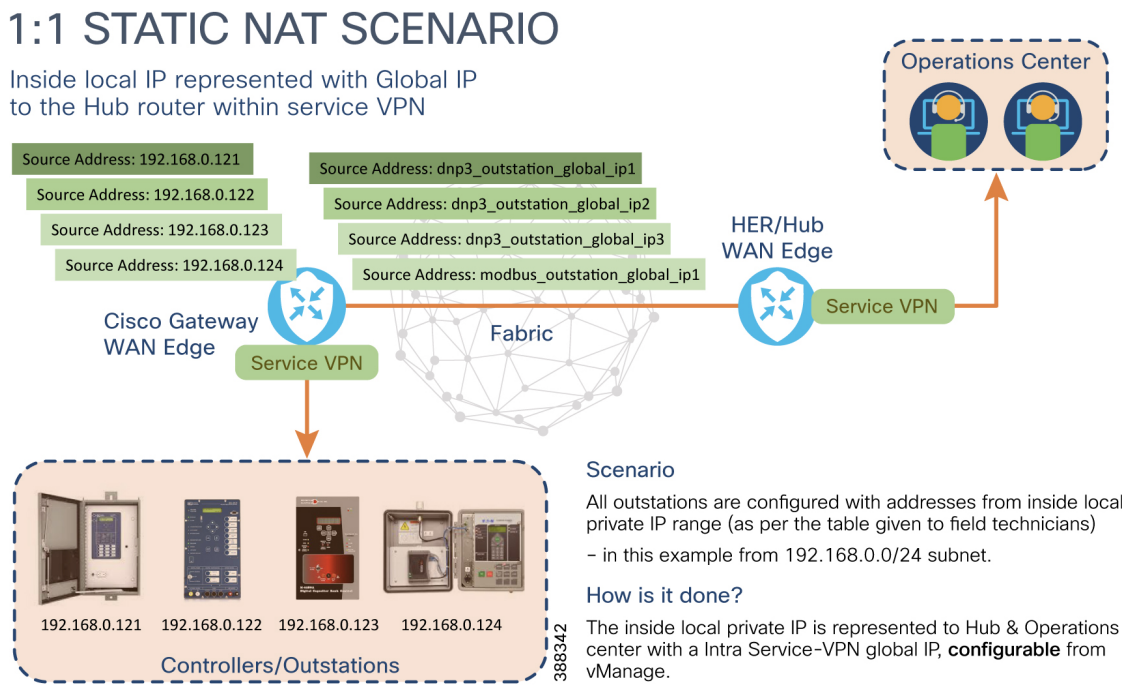
- NAT Local IP range for DNP3 outstation is 192.168.0.121-192.168.0.150
- NAT Local IP range for MODBUS outstation is 192.168.0.151-192.168.0.200
- Configure the first DNP3 outstation with 192.168.0.121
- Configure the second DNP3 outstation with 192.168.0.122
- Configure the third DNP3 outstation with 192.168.0.123
- Configure the first MODBUS Outstation with 192.168.0.151

This 192.168.0.0/24 subnet is Private local IP subnet of the outstation. As per NAT pool1 definition, the 172.16.0.0/16 subnet is used as Global IP subnet.

The vManage user selects and configures three unique global IPs from the NAT pool 1 to represent DNP3 outstation1, DNP3 outstation2 and DNP3 outstation3. The fourth unique global IP is used to represent the MODBUS outstation1.

To enable scaling the same template across thousands of DA gateways, the NAT Global IP address is assigned as a device value to the variable (also referred as device specific key) defined under **Feature Template > Cisco VPN > NAT > Static NAT** section. This NAT global IP needs to be selected out of the NAT Pool number (referred to in the centralized control policy). Values for such variables can be populated under device values of a router by a vManage user. Device values are accessible under the **Configuration > Templates > Device** templates page. Using this technique, the vManage user can remotely assign and re-assign the desired NAT Global IP address for each router.

Figure 5: 1:1 Static NAT Scenario



In the figure above, the field technician configures outstations with fixed IP addresses across hundreds of thousands of different locations.

In the topology above, focusing around the **Cisco Gateway WAN Edge**:

- On the left side, source address represents private local IP address – 192.168.0.X
- On the right side, the same source address is now represented by NAT global IP address.

This NAT global IP address is configurable by a vManage user and is reachable within service VPN. For example,

- The inside IP address of 192.168.0.121 is represented to Hub & Control Center with IP address represented by dnp3_outstation_global_ip1
- The inside IP address of 192.168.0.122 is represented to Hub & Control Center with IP address represented by dnp3_outstation_global_ip2
- The inside IP address of 192.168.0.123 is represented to Hub & Control Center with IP address represented by dnp3_outstation_global_ip3
- The inside IP address of 192.168.0.151 is represented to Hub & Control Center with IP address represented by modbus_outstation_global_ip1

- The Control Center or any application behind the Hub can use the NAT global IP address to uniquely identify the outstation and to monitor/control/manage them.

Note In the above example, four OMP routes would be visible on Hub Router (per DA gateway)

first OMP route for dnp3_outstation_global_ip1,

second OMP route for dnp3_outstation_global_ip2,

third OMP route for dnp3_outstation_global_ip3,

fourth OMP route for modbus_outstation_global_ip1

Across several locations, the outstations would all have the IP address from the private subnet (192.168.0.0/24), but it would be represented to the Control Center with unique NAT global IP address, configurable from vManage. This allows tremendous flexibility in remotely mapping the NAT global IP address to the customer owned Outstations, while at the same time, the field technician's job is kept simple -- to configure the IP address from the 192.168.0.0/24 subnet.

Note If the topology used is Hub and Spoke, then this NAT global IP address is reachable within the relevant service VPN, only from the Hub router and the network behind it.

Definition under Service VPN – Static NAT

- The static 1:1 NAT definition would contain the rules for mapping the local IP to NAT global IP address variable. The NAT global IP address variable (for example, dnp3_outstation_global_ip1) is configured as a variable to obtain user input. This input variable is populated by the vManage user.
- The local IP address is referred to as **Source IP Address** in vManage.
- The NAT global IP address is referred to as the **Translated Source IP Address** in vManage.
- Static NAT Direction is **inside**.

An example of the static 1:1 NAT definition with mapping between local address and NAT global address is given below.

Also recommending the address range associated in **Table 1: Field technicians reference table sample**, and the three configuration examples discussed at the first of this section.

The outstation global addresses (172.16.0.X) that the Control Center communicates with are assigned as device values to the variables configured called dnp3_outstation_global_ip1, dnp3_outstation_global_ip2, dnp3_outstation_global_ip3 and modbus_outstation_global_ip1.

Configuration to be done under the **Feature Template > Cisco VPN > NAT sub section > Static NAT** section.

For example, if three DNP3 outstations and one MODBUS outstation would be used behind a Cisco SD-WAN gateway, the **Cisco VPN > Static NAT** sub section can be configured with 4 Static NAT entries shown below:

Table 2:

Source IP Address	Translated Source IP Address Variable
192.168.0.121	dnp3_outstation_global_ip1
192.168.0.122	dnp3_outstation_global_ip2
192.168.0.123	dnp3_outstation_global_ip3
192.168.0.151	modbus_outstation_global_ip1

After the centralized policy is activated and the configurations are pushed to the Cisco SD-WAN Edge gateway, the IP address value configured on vManage for the "dnp3_outstation_global_ip1" variable could then be used to reach the DNP3 outstation 1 located behind the Cisco SD-WAN Edge gateway.

Points to Note

- All Outstations are configured with the same private IP 192.168.0.X across thousands of locations.
- 172.16.0.0/16 NAT pool 1 is defined to represent the outstations (global IP) to the Operation/Control Center.
- Each outstation is identified with unique global IP from the defined NAT pool 1. The actual IP address is entered as a variable in the vManage device values.
- At the Operation/Control Center, this global IP is used to uniquely identify the outstation across locations.

Impact of routes on Head-End Router

Taking an example of four outstations behind a Cisco SD-WAN gateway (assigned with 1:1 Static NAT - service VPN reachable IP address) would mean 4 route information on the head end router for every Cisco SD-WAN gateway deployed. Each spoke router would advertise each static NAT entry as host route individually to the Head End Router. This would mean 40k OMP routes on head end router for a deployment of 10k Cisco SD-WAN gateways.

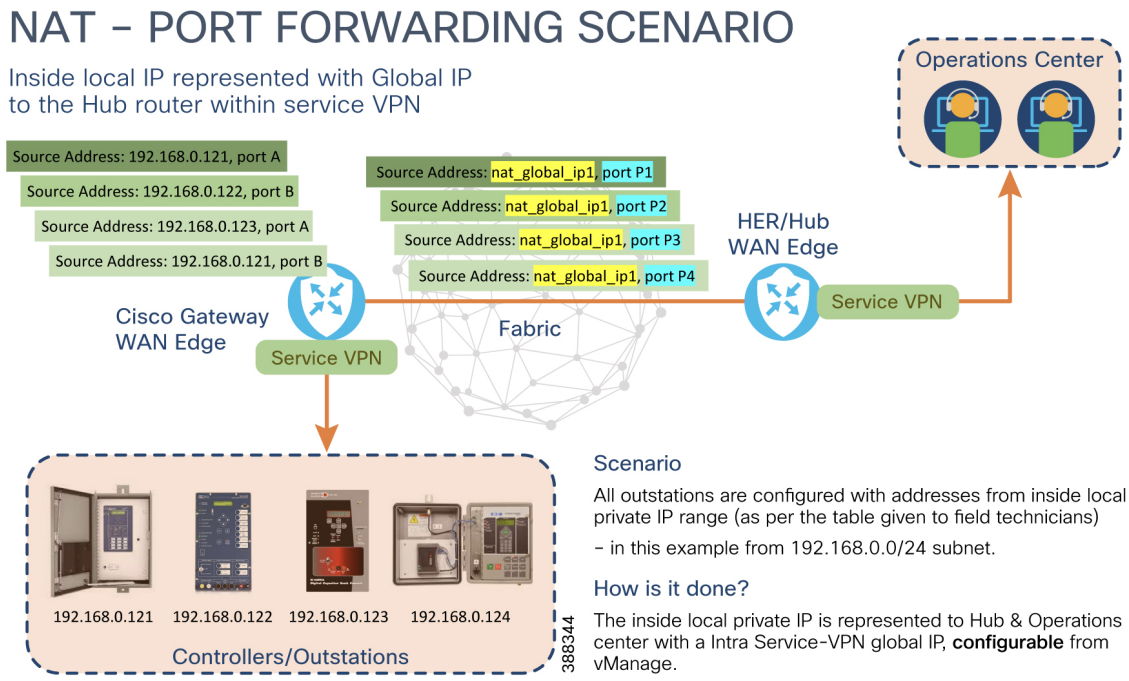
This scaling should be considered when selecting the appropriate Headend routers for the control center.

NAT – Port Forwarding scenario

This section covers the scenario where all the outstations (behind the Cisco DA Gateway) can be represented to the Control Center with one shared NAT Global IP address (also referred as Translated source IP address).

User input to such (device specific key) variables can be populated under the device values of each router by the vManage user. This way, a vManage user can remotely assign and re-assign the desired NAT Global IP address for each router.

Figure 6: N:1 NAT - Port Forwarding Scenario – configurable under Service VPN template



In the above figure, field technician configures outstations with fixed IP addresses for outstations, across hundreds of thousands of different locations.

Note The port number of the outstation must be recorded. It could be either the default port number or a custom port number as configured by the field technician.

In the topology above, focusing around the “Cisco Gateway WAN Edge”:

- On the left side, source address represents not just private local IP address – 192.168.0.X. Instead, a combination of private local IP address and its port number.
- On the right side, the same (source address, source port) is now represented by (NAT global IP address, NAT translated port).

This NAT global IP address and NAT translated port are configurable by vManage user and is reachable within service VPN. For example,

- The inside IP address of **192.168.0.121 (and service port A**) is represented to Hub & Operations center with IP address represented by nat_global_ip1 and port P1.
- The inside IP address of 192.168.0.122 (and service port B) is represented to Hub & Operations center with IP address represented by nat_global_ip1 and port P2.
- The inside IP address of **192.168.0.123 (and service port A)** is represented to Hub & Operations center with IP address represented by nat_global_ip1 and port P3.

Note In the above example, only one NAT Global IP is used, which is nat_global_ip1.

Therefore, only one OMP route would be visible on the Hub Router.

- The Operations center or any application behind the Hub can use this same NAT global IP address, **but the unique port number** to uniquely identify the service on the outstation and to monitor/control/manage the outstation.Paying close attention to first and fourth point above, the same outstation 192.168.0.121 is serving two different service ports (A & B).

Note Global IP1, port P1 represents service port A on Outstation 192.168.0.121

Global IP1, port P4 represents service port B on Outstation 192.168.0.121

Across number of locations, the outstations would all have the IP address from the private subnet (192.168.0.0/24), but it would be represented to the Operations center with one NAT global IP address per Cisco DA gateway, configurable from vManage. This allows tremendous flexibility in remotely mapping the NAT global IP address + port combinations to represent the service ports on the customer owned outstations. Example of service ports would be DNP3, MODBUS, HTTP, SSH, FTP, and so on.

Whether it is Static 1:1 NAT (or) N:1 port forwarding, the field technician's job is kept simple (to configure the IP address from the 192.168.0.0/24 subnet).

Note If the topology used is Hub & Spoke, then this NAT global IP address is reachable within a service VPN, only from the Hub router and the network behind it.

Definition under Service VPN – PORT FORWARD:

- The "PORT FORWARD" definition would contain the rules for mapping the (Local IP, local port) to (NAT Global IP, NAT translated port). Also, please refer to figure titled *N:1 Port Forwarding Scenario – configurable under Service VPN template.*
-
  - The local IP is also referred as private IP, inside IP, "Source IP Address." For example, it corresponds to 192.168.0.X configured on outstation.
  - The local port is also referred as Inside port, "Source Port" and so on. For example, these are port A, Port B associated with 192.168.0.X outstations.
  - The Global IP can also be referred as "Translated Source IP address," NAT Global IP address. For example, it corresponds to "nat_global_ip1"
  - The NAT translated port can also be referred as "Translate Port," and this corresponds to ports "P1, P2, P3 and P4".
- These values can either be hard coded or configured as user defined key/variables
- The NAT global IP address variable (for example, nat_global_ip1) is configured as a variable. This input variable is populated by the vManage user.

The translate source IP address (for example, 172.16.0.X) that the operation center communicates with, are assigned as device values to the variables defined, such as nat_global_ip1.

An example of the port forwarding NAT definition with mapping between (source IP address, source port) and (translate source IP address, translate port) is given below.

Also recommending recollecting the address range associated in **Table 1: Field technicians reference sample table**, as well as the three examples mentioned under "Guideline for Private/Local IP configuration on Customer outstations".

Subset of below definition can be chosen according to the deployment needs and configured under the **Feature Template > Cisco VPN > NAT sub section > PORT FORWARD** section.

Table 3:

Outstation Description	Source IP Address	Source Port	Translated Source IP Address	Translate Port (Must be unique)
DNP3 device 1	192.168.0.121	20000	nat_global_ip1	20001
DNP3 device 2	192.168.0.122	20000		20002
DNP3 device 3	192.168.0.123	20000		20003
MODBUS device 1	192.168.0.151	502		25001
MODBUS device 2	192.168.0.152	502		25002
T104 device 1	192.168.0.41	2404		30001
T104 device 2	192.168.0.42	2404		30002

Ports listed in the "Translate Port" column are only a guideline. Any preferred range of port numbers can be used.

For example, if three DNP3 outstations and one MODBUS outstation are to be used behind a Cisco SD-WAN gateway, the **Cisco VPN > Static NAT** sub section can be configured with values shown in the table below.

Table 4:

Outstation Description	Source IP Address	Source Port	Translated Source IP Address	Translate Port (must be unique)
DNP3 device 1	192.168.0.121	20000	nat_global_ip1	20001
DNP3 device 2	192.168.0.122	20000		20002
DNPe device 3	192.168.0.123	20000		20003
MODBUS device 1	192.168.0.151	502		502

In another example, if three T104 outstations and three MODBUS devices are connected behind a Cisco gateway, then the **Cisco VPN > Static NAT** sub section can be configured with values shown in the table below.

Table 5:

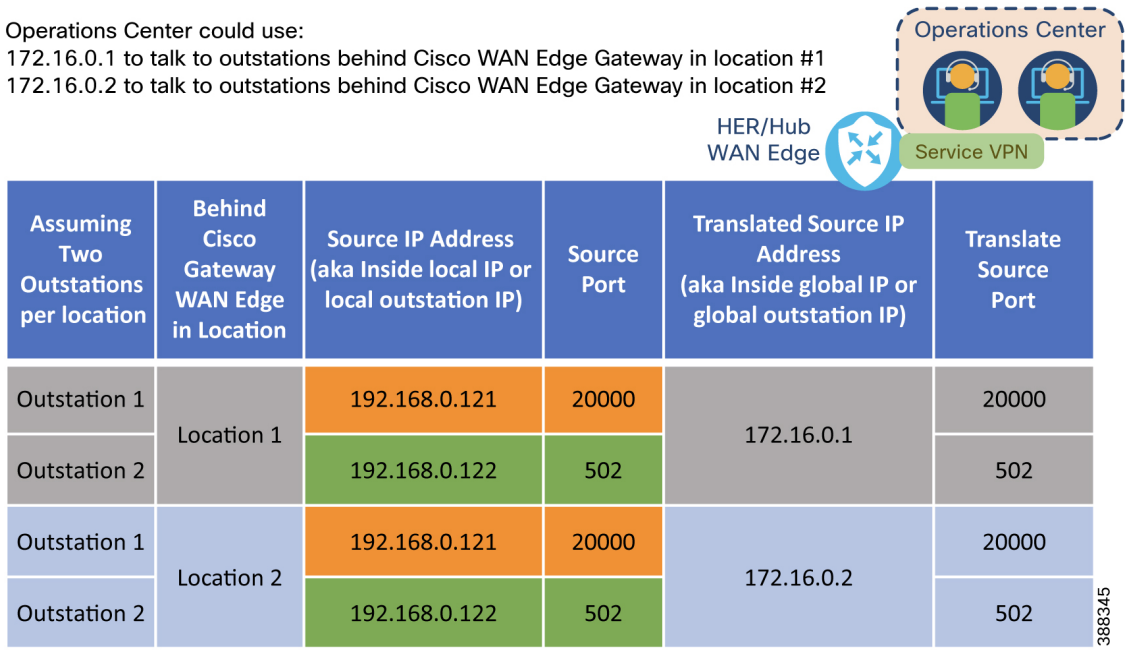
Outstation Description	Source IP Address	Source Port	Translated Source IP Address	Translate Port (must be unique)
T104 device 1	192.168.0.41	2404	nat_global_ip1	2404
T104 device 2	192.168.0.42	2404		24002
T104 device 3	192.168.0.43	2404		24002
MODBUS device 1	192.168.0.151	502		502
MODBUS device 2	192.168.0.152	502		25002
MODBUS device 3	192.168.0.153	502		25003

After the centralized policy is activated and the configurations are pushed to Cisco SD-WAN Edge gateway, the combination of "Translated source IP address" and "Translate Port" (for example, user value for "nat_global_ip1" could then be used to reach the corresponding outstation).

For example,

- (nat_global_ip1 + port 2404) can be used to access T104 device 1.
- (nat_global_ip1 + port 24002) can be used to access T104 device 2.
- (nat_global_ip1 + port 502) can be used to access MODBUS device 1.
- (nat_global_ip1 + port 25003) can be used to access MODBUS device 3.

Figure 7: N:1 NAT – PORT FORWARD scenario – Accessing outstation across locations with NAT global IP address.



In the figure above, the Operations center is located behind the Hub router and is part of service VPN. In this example, two outstations are located behind each Cisco SD-WAN Edge Gateway.

- Outstation1 in location1 and location2 (and across all the locations) are configured with same local outstation IP of 192.168.0.121
- Outstation2 in location1 and location2 (and across all the locations) are configured with same local outstation IP of 192.168.0.122

In summary:

To access Outstation 1 in location1, Control center needs to talk to 172.16.0.1 on port 20000.

To access Outstation 2 in location1, Control center needs to talk to 172.16.0.1 on port 502.

To access Outstation 1 in location2, Control center needs to talk to 172.16.0.2 on port 20000.

To access Outstation 2 in location2, Control center needs to talk to 172.16.0.2 on port 502.

Points to Note

- All Outstations are configured with the same private IP 192.168.0.X across thousands of locations.
- 172.16.0.0/16 NAT pool 1 is defined to represent the outstations (global IP) to Operation/Control Centre.
- Each Cisco SD-WAN Edge gateway is identified with unique global IP (out of defined Nat pool 1). The IP address is defined as a variable in vManage device values. The Global IP is the "Translated Source IP Address."
- At the Operation/Control Centre, this "global IP + Translated source Port" combination is used to communicate with the corresponding outstation.

Impact of routes on Head End Router

Irrespective of number of outstations connected behind the Cisco SD-WAN gateway, every spoke router would advertise only one host route (single NAT Global IP aka Translated Source Address) to the Hub router. This would mean 10k OMP routes on the hub router for 10k Cisco SD-WAN Edge gateway deployments.

Advantages of Port Forwarding

Can represent multiple outstations behind Cisco SD-WAN Edge gateway with single NAT global IP address, by doing port forwarding.

Because only one NAT global IP address is used per Cisco SD-WAN Edge gateway, it conserves the route resources on the Hub router, as it needs to store only one IP route information per Cisco SD-WAN Edge gateway.

Can co-exist along with 1:1 static NAT if required.

Disadvantages of Port Forwarding with Mitigation Approach

This section would be applicable only if the Applications residing in the Control Center cannot communicate on custom port numbers. Even if the application can communicate only on fixed port number, if outstations behind the WAN Edge gateway are listening on different ports, then also it is not a disadvantage.

The disadvantage is applicable only if:

- The Application in Control Center can communicate on fixed ports only.
- If there are more than one outstation behind the same Cisco SD-WAN Edge gateway, which are talking the same protocol. For example, in case of 3 DNP3 outstations listening on default port of 20000, the

applications in the control/Operations center should be capable of talking to the single NAT global IP address on 3 different port numbers, say 20000, 20001, and 20002. One port for each outstation belonging to same family. If not, it can still be mitigated with the help of Hybrid approach mentioned in the next section.

This would not be a disadvantage if the control center application can communicate on custom port numbers.

For example, assuming the DNP3 headend Application in control center has a limitation that it can communicate only on default port 20000, port forwarding can be used to communicate with (first) DNP3 outstation1 using "Translated Source IP Address" of 172.16.0.1 + port 20000.

With reference to the figure *Service VPN: NAT – Hybrid Approach,* the section below describes the mitigation solutions to enable connectivity to second DNP3 outstation4.

Mitigation solution1: To enable communication with another DNP3 outstation 4 located behind the same gateway, static NAT can be leveraged. Hence, the DNP3 headend Application can communicate with DNP3 outstation4 using another "Translated Source IP Address" of 172.16.0.2 + default DNP3 port of 20000

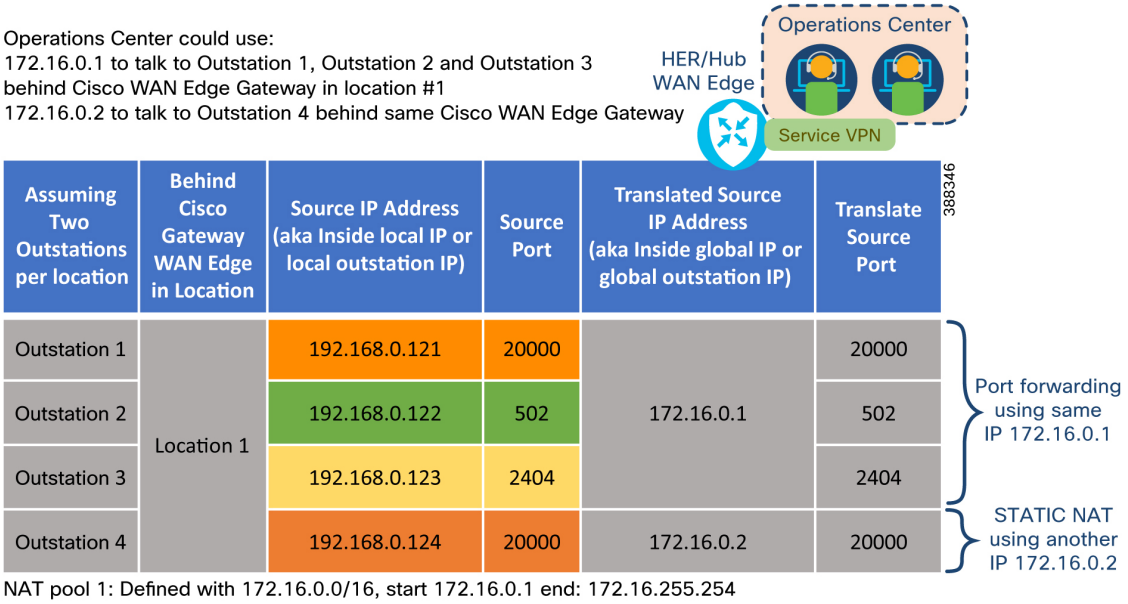
Mitigation solution2: Alternatively, port forwarding also can be leveraged but with another "Translated Source IP Address" like 172.16.0.2 instead of the first "Translated Source IP Address" (which is 172.16.0.1) used for outstation1.

NAT Hybrid Approach Using Static NAT + Port Forwarding

Consider a scenario, where there are 4 outstations connected behind a Cisco WAN Edge Gateway. Available options are:

- Use static NAT and represent each outstation with unique NAT global IP (Translated source IP address). This uses **4 translated source IP address** from NAT pool.
- Use Port forward and represent all the outstations with one common NAT global IP and using port numbers to differentiate between. This uses **1 translated source IP address** from NAT pool.
- Hybrid Approach, which combines the best of the two worlds, where we represent majority of outstations with one common NAT global IP and use static NAT where exclusive access to outstation is needed on multiple port numbers.

Figure 8: Service VPN: NAT – Hybrid Approach



In the figure above, four outstations are enabled for connectivity with the help of Cisco SD-WAN Edge gateway. First 3 outstations are enabled for connectivity with the help of port forwarding. The last outstation4 is enabled for connectivity with the help of Static NAT using another NAT global IP (172.16.0.2)

The Operations center can communicate with:

- Outstation1 using “Translated source IP Address” of 172.16.0.1 and destination port 20000.
- Outstation2 using “Translated source IP Address” of 172.16.0.1 and destination port 502.
- Outstation3 using “Translated source IP Address” of 172.16.0.1 and destination port 2404.
- Outstation 4 using “Translated source IP Address of 172.16.0.2

This way, the DA Gateway advertises only two routes (172.16.0.1/32 and 172.16.0.2/32) to the Hub router.

If the Headend applications that can communicate only on fixed ports, this hybrid approach can be used as mitigation step.

Static NAT vs Port Forwarding considerations

Configuration Simplicity vs Memory Conservation on Hub Router

In scenarios where a single connected outstation needs to be reached on many port numbers (for example, SSH, FTP, DNP3, HTTP, and so on), use of STATIC (1:1) NAT can be considered. Port forwarding can also serve the same purpose, but every port needs to be individually configured – this provides a slight configuration overhead to the vManage user.

On the other hand, usage of port forwarding option advertises only one IP per SD-WAN gateway, thereby consuming less routing table resource on the Hub router. Even if there are ten outstations connected behind the SD-WAN gateway, only one route resource would be considered in the “port forwarding” approach.

Though this involves a bit of one-time configuration overhead, it saves on the ongoing memory utilization at the Hub/Head-end Router forever.

Unrestricted Access to Resource vs Selective Access to Resource

With STATIC (1:1) NAT, all the ports of the outstations are available to use from the Operations center simultaneously. There is unrestricted access to all the resources on the outstation.

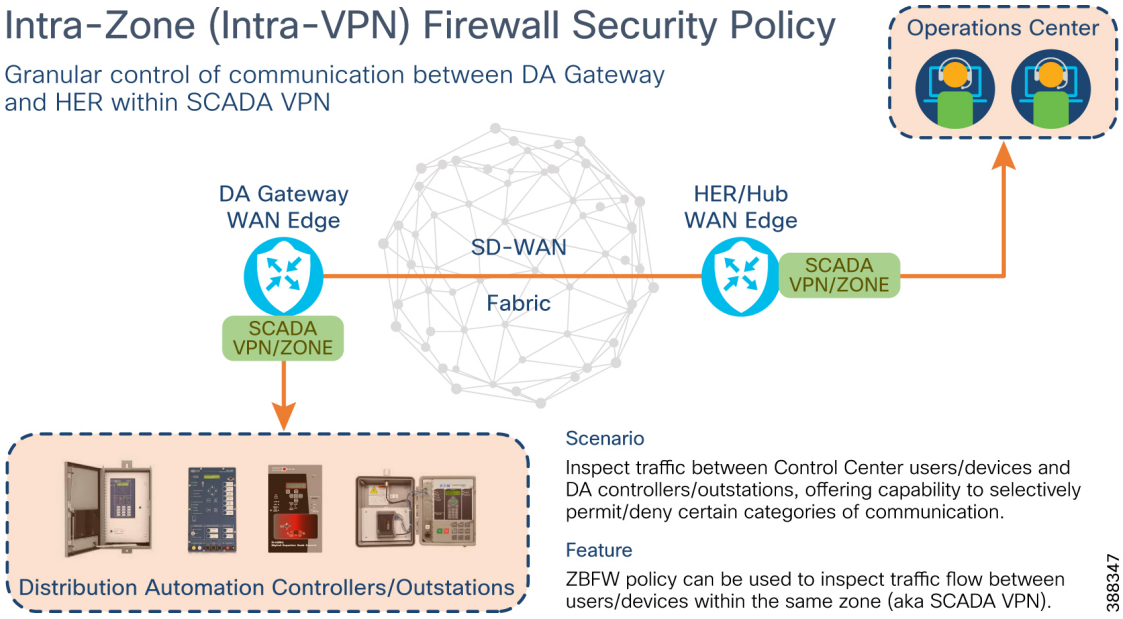
With port forwarding, only selective ports of the outstations are made available for access from the operations centre, thus offering a layer of security by restricting the access only to ports that are port forwarded and blocking access to rest of the ports. Thus, access is granted only for port forwarded ports and unnecessary access to other resources on the outstation.

Based on number of outstations connected

Cisco SD-WAN Edge Gateway could be used to connect multiple outstations, or it could be used to connect only one outstation per gateway in some use cases. In cases where multiple outstations are connected, usage of port forwarding is recommended. In cases where only one outstation is connected per gateway, either port forwarding or static (1:1) NAT can be used.

Intra-VPN Zone based firewall

Figure 9: Intra-VPN Firewall Security Policy



The communication between Operations/Control Center and End devices is isolated inside dedicated service VPN/Zone. In the above figure, VPN-N is used to contain the application traffic communication between Operations Center & end devices.

Within the same VPN, communication between Control Center and End devices can be selectively permitted or denied, with the help of Firewall security configuration options.

Zone Based Firewall (aka Security Policy) could be used to selectively permit/deny flows between Control Center and IP-aware end devices.

Available granular controls are:

- Source IP/List, Source Port(s)

- Destination IP/List, Destination Port(s)
- Protocols
- Application list

Inspect option should be chosen to allow return communication for permitted traffic.

Listed below are just a few examples, but not limited to it are:

- Permitting access for end devices to reach selective IPs in control centre.
- Denying the end devices from accessing SSH or HTTP in control centre.
- Permitting control Center to access the outstation via SSH, monitor/control via HTTP(S).
- Selectively permitting the above operations from specific hosts of control center and so on.

Note Traffic within the LAN segment of a particular service VPN is not inspected (that is, Traffic that is locally switched on the IR1101 switchports.

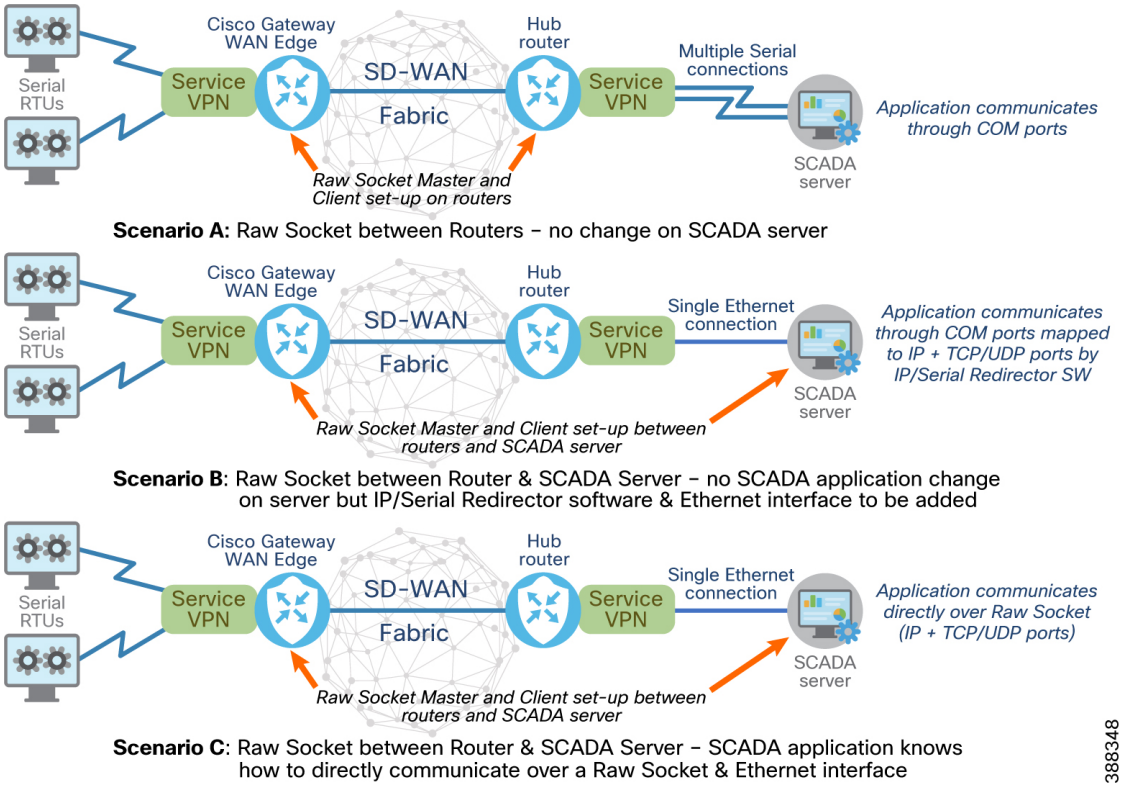
Enabling Connectivity to Serial Outstations

Connectivity to serial outstations is enabled using of CLI Add on templates.

Connectivity between serial outstations and the control center are provided by the raw socket (TCP or UDP) feature.

Three deployment scenarios for point-to-point raw socket

Figure 10: Three deployment scenarios for point-to-point raw socket service



Scenario A - Raw socket between Cisco SD-WAN Edge gateway and SCADA Router in headend; no change on SCADA server; SCADA server communicates through physical serial COM ports. The Hub router can also act as SCADA router if it is capable of terminating the raw socket and providing multiple physical serial ports, one per raw socket connection. If not, separate SCADA router may be needed between the Hub router and SCADA server.

Scenario B - Raw socket between Cisco SD-WAN Edge gateway and SCADA Server; no SCADA application change on server but IP/Serial Redirector software maps COM port to IPv4 address + TCP/UDP port. Hub router & SCADA server connected via Ethernet.

Scenario C - Raw socket between Cisco SD-WAN Edge gateway and SCADA Server; SCADA application knows how to directly communicate over a raw socket (IPv4 address + TCP/UDP port). Hub router & SCADA server connected via Ethernet.

Scenario A is not scalable. Scenario B or Scenario C are highly recommended for raw socket deployments. In scenario A, multiple physical serial connections are needed, whereas in Scenarios B & C, single ethernet connection alone is sufficient and it removes the requirement to have multiple physical serial connections.

Raw Socket TCP Transport

Refer refer to IoT Industrial Routers Extension to SD-WAN Small Branch Design Case Study" for more on raw socket TCP and UDP operation.

TCP raw socket transport uses a client-server model. At most, one server and multiple clients can be configured on a single asynchronous serial line. A raw socket client receives streams of serial data from the RTUs and accumulates this data in its buffer, then places the data into packets, based on user-specified packetization criteria. The raw socket client initiates a TCP connection with the raw socket server and sends the packetized

data across the IP network to the raw socket server, which retrieves the serial data from the packets and sends it to the serial interface, and onto the utility management.

In case of raw socket TCP, the following are sub options:

- Cisco DA gateway could be used as TCP server, listening for connections from Control center (or)
- Cisco DA gateway could be used as TCP client to initiate the connections to Control Center.

Raw Socket UDP Transport

User Datagram Protocol (UDP) transport uses a peer-to-peer model. Multiple UDP connections can be configured on an asynchronous serial line. The raw socket UDP peer receives streams of serial data from the RTUs and accumulates this data in its buffer, and then places the data into packets based on user-specified packetization criteria. Raw socket UDP peer sends the packetized data across the IP network to the raw socket peer at the other end, which retrieves the serial data from the packets and sends it to the serial interface, and on to the utility management system.

Configurations

Enabling Connectivity to IP-aware Outstations

Configuration for below section corresponds to “Static 1:1 NAT, Static N:1 Port Forwarding” section – hyperlink to be added.

Centralized control policy definition

The definition below of Centralized policy configuration can be configured under the “Traffic Data” definition of “Traffic Rules” section.

Figure 11:

Match criteria

- DATA_PREFIX matches on “192.168.0.0/24” subnet.
- Match condition:
  - Match on Source IP
  - Match on Source Data prefix list: DATA_PREFIX
- Action: Accept
  - With NAT pool 1

NAT pool definition

“NAT sub section” configuration is available under Feature Template of service VPN configuration.

Figure 12:

Figure 13:

For NAT pool definition, refer to Example of NAT pool1 definition.

NAT – 1:1 STATIC scenario – Configuration

This configuration corresponds to “Static NAT” section under NAT.

This example assumes a scenario, where two DNP3 outstations and one camera were enabled for connectivity with the Cisco SD-WAN Edge Gateway.

Table 6:

Source IP Address	Translated Source IP Address
192.168.0.121	dnp3_outstation_global_ip1
192.168.0.122	dnp3_outstation_global_ip2
192.168.0.201	camera_global_ip1

Click on **New Static NAT** to create new entry.

Here is an example definition for representing “192.168.0.121” end device with “Translated Source IP Address” represented by “dnp3_outstation_global_ip1” variable.

Figure 14:

Similarly, entries can be created for below two end devices as well. After you have entered the information, click **Save** to save the configuration.

- 192.168.0.122 - dnp3_outstation_global_ip2
- 192.168.0.201 - camera_global_ip1

Figure 15:

NAT – Port Forwarding scenario – Configuration

This configuration corresponds to “PORT FORWARD” section under NAT.

To facilitate one to one comparison in config between “Static NAT” and “PORT FORWARD,” the same example scenario has been chosen, where two DNP3 outstations and one camera were enabled for connectivity with Cisco SD-WAN Edge Gateway. This time, it is with port a forwarding example.

Table 7:

End Device Description	Source IP Address	Source Port	Translated Source IP Address	Traslate Port (must be unique)
DNP3 device 1	192.168.0.121	20000	nat_global_ip1	20001
DNP3 device 2	192.168.0.122	20000		20002
Camera 1	192.168.0.201	80		40001

Under “PORT FORWARD,” click on “New Port Forwarding Rule” to create new entry.

Here is an example definition for representing “192.168.0.121” end device listening on port 20000 with “Translated Source IP Address” represented by “nat_global_ip1” variable on port 20001.

For the Operations center to communicate with DNP3 device 1 on port 20000, it needs to talk to IP “nat_global_ip1” and port 20001, which in turn gets translated and forwarded to 192.168.0.121 end device on port 20000.

Figure 16:

In a similar way, entries can also be created for the two end devices below. When done, click **Save** to save the configuration.

Table 8:

End Device Description	Source IP Address	Source Port	Translated Source IP Address	Translate Port (Must be unique)
DNP3 device 2	192.168.0.122	20000	nat_global_ip1	20002
Camera 1	192.168.0.201	80		40001

Figure 17:

Enabling Connectivity to Serial Outstations

Raw Socket TCP Transport - IR1101 as TCP Client - configuration

```
interface Async0/3/2

vrf forwarding 71 (VRF defines the service VPN that Raw Socket connections will use)

no ip address

encapsulation raw-tcp

media-type rs232


line 0/3/2

speed 9600

databits 8

stopbits 1

parity none

raw-socket tcp client <scada_ip>  <src port> <listening port> <loopback_ip_variable>
```

Raw Socket TCP Transport – IR1101 as TCP Server/Listener - configuration

```
interface Async0/3/0

vrf forwarding 71

no ip address

encapsulation raw-tcp

media-type rs232


line 0/3/0

speed 9600
```

```
databits 8

stopbits 1

parity none

raw-socket tcp server <raw_socket_listening_port>
```

Raw Socket UDP Transport - configuration

Refer to the *Serial I/O* section of the guide IoT Industrial Router Extension to SD-WAN Small Branch Design Case Study for information about existing caveats on serial usage.