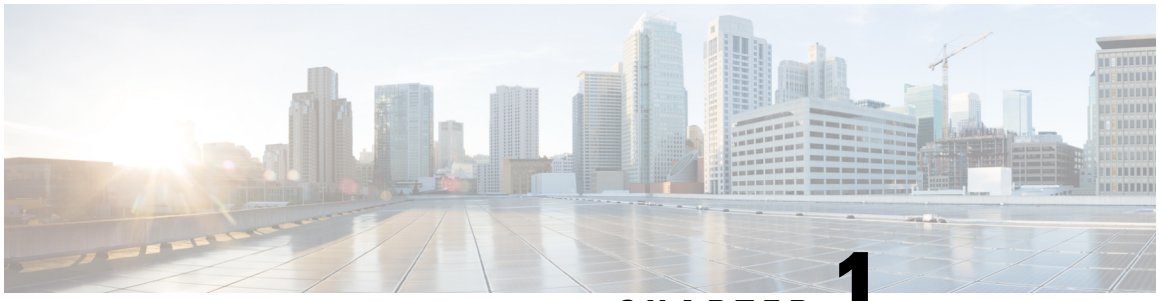
SD-WAN for Remote Condition Monitoring and Control Design Guide

First Published: 2023-04-24

Last Modified: 2023-04-24

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



CHAPTER 1

SD-WAN for Remote Condition Monitoring and Control

Introduction

Many industries rely on equipment and other assets deployed at geographically remote locations for their line of business to function properly. Having visibility into the current condition of these devices is critical in ensuring that the day-to-day operations work smoothly, and when something does go wrong, it can be responded to quickly for resolution. The Cisco SD-WAN solution based on vManage can work with industrial Internet of Things (IOT) routers to provide reliable, secure connectivity for the end devices themselves, as well as other sensors, cameras, and other equipment that supports the operation of the end devices.

Some examples of use cases for remote condition monitoring and control are shown in the table below.

Use Case	Related Monitoring and/or Control Activity
Food Industry (incl. food storage and transportation)	Monitoring freezer and cold room temperature and humidity
Remote Environmental Controls	Monitoring temperature, humidity brightness
Water Management	Monitoring water tank levels, lakes/reservoir levels, water flow through distribution pipelines
Video Surveillance	Monitoring CCTV cameras with video analytics to detect over/underfill conditions and physical security breaches
Distribution Pipelines (water, gas)	Monitoring for leaks and water/gas flow through pipelines
Waste Management	Monitoring wastewater levels and starting/stopping pumping stations
Flood Management	Detecting road conditions and control of closure gates for known low lying flood areas
Industrial Process control	Remote emergency power shut off and restoration
HVAC Systems	Monitoring of rooftop AC units for temperature, and vibration for preventative maintenance

Use Case	Related Monitoring and/or Control Activity
General Equipment Monitoring	Monitoring of equipment temperature, vibration, tank levels

This document builds on other existing documents that describe the Cisco SD-WAN solution and IOT hardware offerings in detail and helps show how they can be combined to provide a scalable, secure network. Readers should already have some familiarity with Cisco SD-WAN and IOT. Prior to reading this document, it is recommended to be familiar with the following resources:

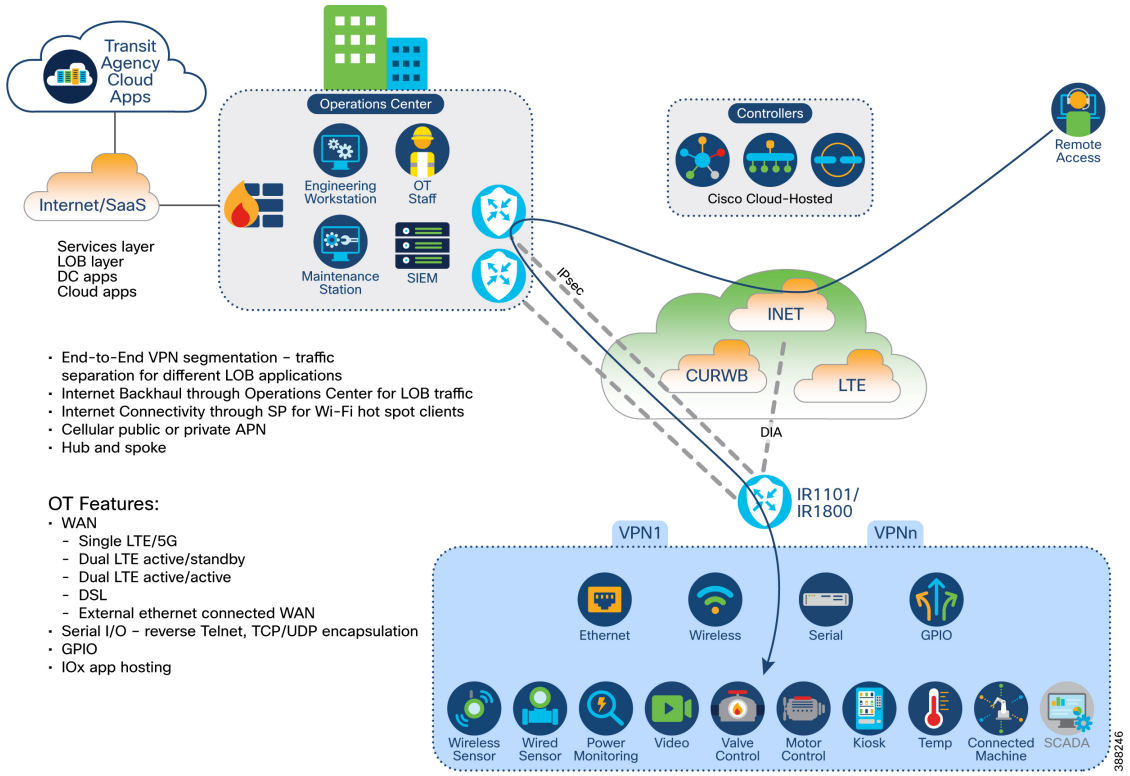
Cisco SD-WAN Small Branch Design Case Study – This document provides a great overview of general SD-WAN concepts in the context of a "small branch" which has many commonalities with a typical IOT deployment used in a mass transit or fleet scenario.

Cisco IoT Industrial Router Extension to the SD-WAN Small Branch Design Case Study– This document builds on the previous one, with a focus on areas that are unique or at least emphasized by IOT use cases in general. This document also has detailed configuration examples for many of the IOT features.

Architecture

A conceptual diagram is shown below depicting industrial routers in cabinets supporting monitoring of a distribution pipeline sensor and sharing readings to provide visibility to warnings and imminent dangerous conditions.

Figure 1: SD-WAN Architecture for Remote Condition Monitoring and Control



Requirements

WAN Connectivity

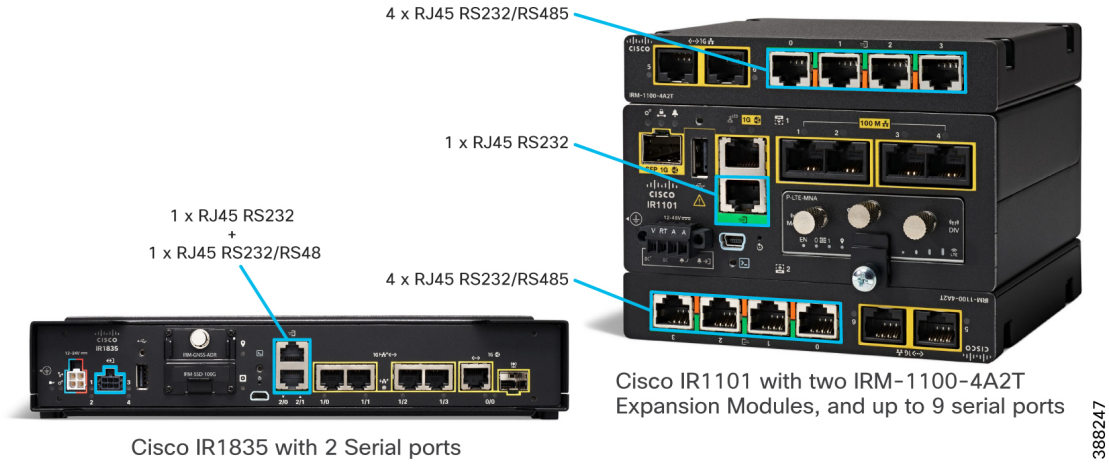
Remote condition monitoring deployments are by nature very spread out geographically, and thus very dependent on different WAN technologies. From the operations center with redundant highspeed fiber backhaul, to very remote assets in the field with potentially a slow or lossy cellular or even satellite connection, the requirements of each type of site needs to be analyzed carefully.

Some remote fixed assets can leverage existing wired infrastructure such as ethernet or DSL, or they can rely on wireless technologies including cellular (LTE and 5G). These sites typically use relatively low bandwidth.

The WAN technology chosen must be a balance of price and performance characteristics that meet the needs of the device or application being monitored. In some cases, like a remote weather station that is reporting atmospheric conditions, it may be acceptable to have a high latency and low bandwidth because the amount of data, and the criticality of that data is low. In this case a single external satellite modem may be acceptable. In other scenarios where the router is connected to industrial equipment that could have safety implications if there is a problem, resilient WAN connectivity with low latency is worth the added cost and complexity.

Serially Connected Devices

Devices that use a RS232 or RS485 serial connection can rely on the Cisco Industrial IOT router like the IR1101, IR1800 series, or IR8340 to provide connectivity across the WAN to centralized controls and monitoring devices. The Cisco IOT routers each have a variety of serial ports that can be connected directly to these devices. The routers will usually use TCP or UDP to encapsulate the serial data in a “raw-socket” that then traverses the WAN as IP packets inside a Service VPN. Elsewhere in the network, like in the Operations Center, the raw-socket connection will terminate on another Cisco router where the serial data is decapsulated and finally connected to the end device via serial. This encapsulation is transparent to the connected devices who see the connectivity as just being a point-to-point serial connection.



Ethernet and IP Connected Sensors

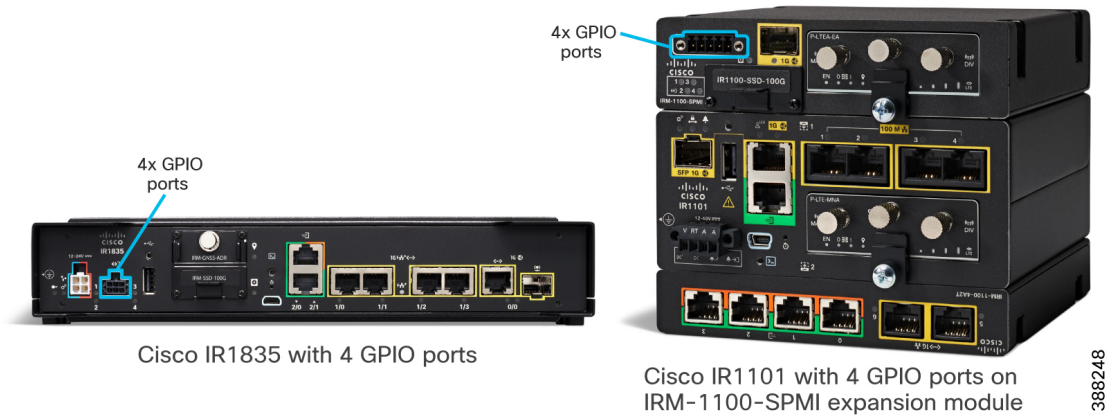
Sensors and other devices that support Ethernet and IP connectivity can leverage the robust feature set of Cisco IOS-XE and vManage SD-WAN. For remote sites with only a few ethernet connected devices, the IOT router itself can provide the necessary switchports. For sites with more devices, connectivity can be expanded by adding one or more subtended Cisco industrial ethernet (IE) switches behind the IOT router. Power over Ethernet (PoE) from the router or switch can be used to provide both power and connectivity over a single cable to the sensor or device.

GPIO to Control Valves, Power, etc. Remotely

Various digital sensors, alarms, and similar systems with a digital output can be connected to the GPIO interface in Cisco industrial routers. Upon being triggered, the digital input can be used to generate an alert

to be sent upstream to the security operations center. The GPIO ports can also be configured as outputs and used to control external devices like a valve or relay.

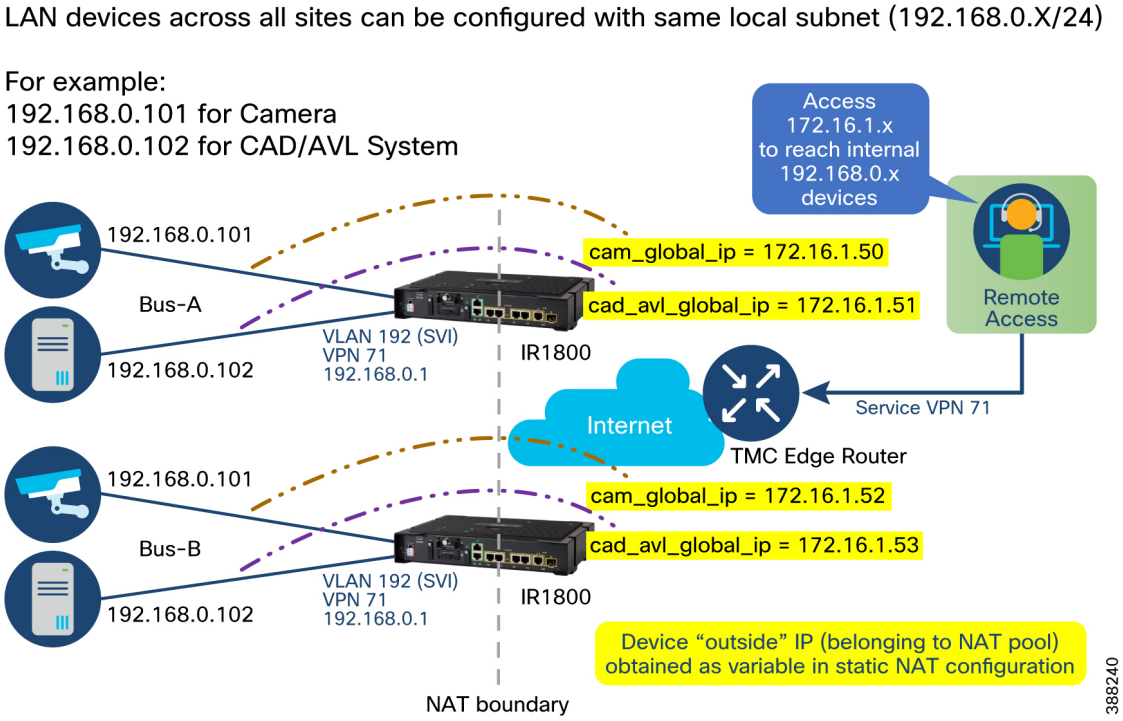
Figure 2:



Direct Internet Access (DIA) for Cloud Servers

In cases where there are sensors, applications, or other devices in the remote site that need to access cloud services, it may be desirable to route traffic directly to the internet. Direct Internet Access (DIA) traffic from subtended devices will be NATed and sent directly out the WAN interface to the internet destination, without traversing the overlay VPN network that connects to other SD-WAN edge routers and the networks beyond them. This direct path can help reduce load on the overlay network and potentially help reduce latency to cloud applications. For example, if a sensor will be reporting metrics to an Amazon Web Services application, it can bypass the SD-WAN overlay network, thus simplifying connectivity. Using this method will limit the security and other SD-WAN features that can be applied to the traffic at a central site.

Figure 3:



Operations Center (Headend) Access for Customer Hosted Servers

Other devices at the remote site will need connectivity to the operations center. These devices can be segmented into a different service VPN than the cloud/internet connected devices. The service VPN is extended across the overlay network to the edge "hub" router at the operations center, thus providing secure resilient connectivity.