CVP5: IR1101 for Roadways: Wired SD-WAN with LTE as Last Resort in Routed Mode with ISE Integration

Overview

This single-router SD-WAN configuration is for the Cisco Industrial Router IR1101. It is designed specifically for this platform with all its unique interface names and modules to aid in the rapid deployments at small to medium sized locations where flexibility, simplicity and standardization are key. This catalog represents a Cisco Validated Profile (CVP) suited for deployments at roadways and intersections. This network configuration is wired transport with single LTE connectivity as last resort. This configuration offers network segmentation via 4 secure VPN (VPN 10,20,30,40) with 1 VLAN per VPN (10,20,30,40) respectively. It also provides for connected client 802.1X and MAC authentication via integration with Cisco Identity Services Engine (ISE). Integration with ISE can be as a Radius server for port authentication or also with TrustSec segmentation.

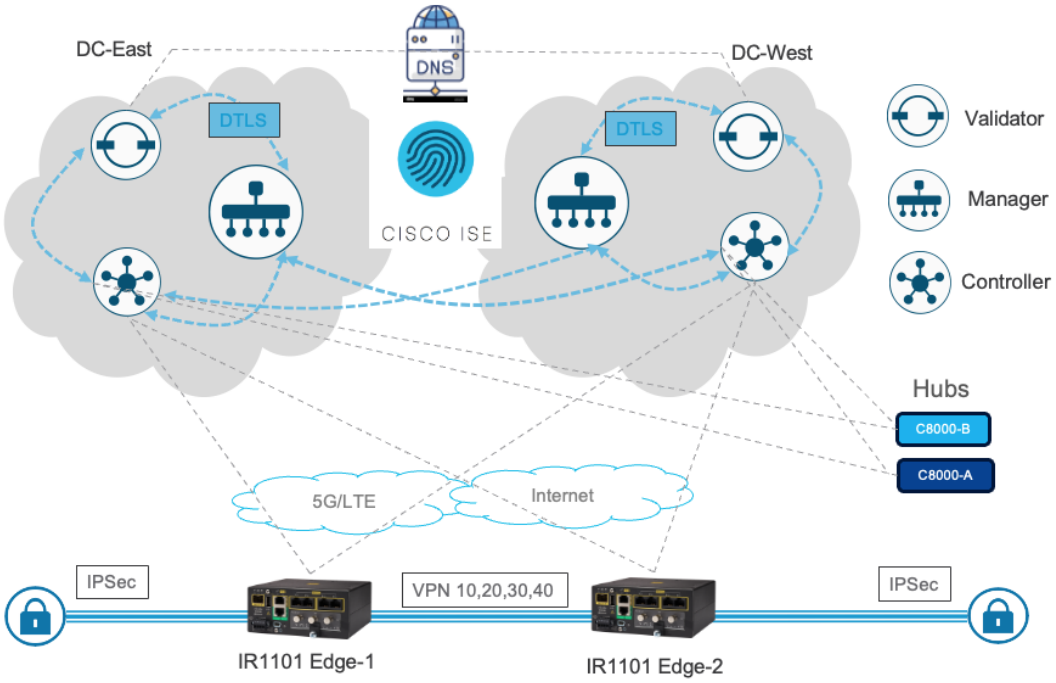


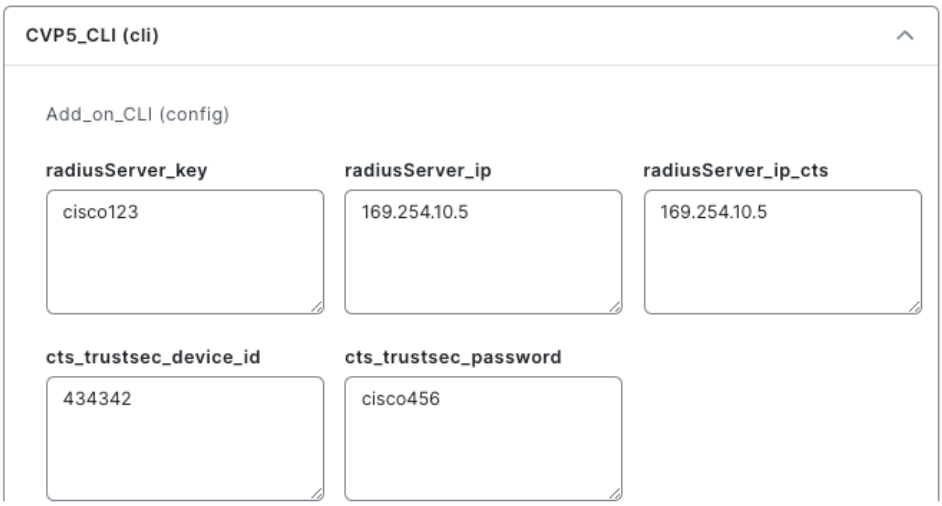
Fig 1: Configuration Catalog Design

Configuration Catalog Details

Ethernet LAN connectivity is mapped into 4 VPN for security and granular control, but user can assign multiple ports to same VLAN at catalog install time:

- Fa0/0/1 – Access Port - VPN 10 - VLAN 10 with SVI and DHCP pool
- Fa0/0/2 – Access Port - VPN 20 - VLAN 20 with SVI and DHCP pool
- Fa0/0/3 – Access Port - VPN 30 - VLAN 30 with SVI and DHCP pool
- Fa0/0/4 – Trunk - VPN 40 – Allowed VLANS 10,20,30,40 - with SVI and DHCP pool
- User will need to provide IP address and key to their ISE server at config deploy time as “radiusServer_key” and “radiusServer_ip” (see image) to allow connected clients

to perform MAC followed by 802.1x authentication, in that order. If user also wishes to configure TrustSec, the “radiusServer_ip_cts” should also be set to same IP as previous radius server IP and remaining TrustSec parameters provided as needed. If user wishes to only have radius port authentication without TrustSec, then all parameters with cts in name are still required, but dummy values are recommended (specially for “radiusServer_ip_cts”) to avoid unneeded interaction with ISE server for TrustSec.



- Default catalog behavior is to reach ISE server from VPN4 using a predefined Loopback40 interface. The ISE server also needs to be added in WAN Manager UI Administration-> Integration Management.

Further details on functionality provided by this catalog entry which can be changed for the device at deployment time:

- One or more Hubs are required to be deployed as shown. Hubs need to be deployed using a configuration group not provided here as part of this catalog entry. The hubs will facilitate communication between connected devices behind edge routers and the enterprise network by advertising to edge devices a default route or a list of subnets the edge devices need to reach in the enterprise. It will be up to the Hub to allow also for edge traffic to reach the internet or block it if not needed at the edge. It is also necessary to assign each edge device a unique Service VPN subnet and IP address to allow for return traffic.
- The Service VPN (LAN) side is configured to advertise static and connected routes for all 4 VPNs or flexible integrations at sites with routed LAN access layer. User will need to enter unique subnet for each edge device at deployment time to route back from a Hub router to each edge. By default, the catalog provides default values for all SVI in each VPN as well as DHCP pool parameters which user can change at deploy time one device at a time or using a CSV file to deploy many devices at once. User will also need to advertise all subnets from the hub router to edge devices, including a default route as needed. If user does not want to have a DHCP server in the service VPN, the “VPNx SVI1

DHCP Server Network", Mask and Default gateway can be set to dummy values to prevent any connected device from having DHCP service or access through DHCP.

- Default DNS servers (Cisco DNS) are provided in VPN0, which user can change at catalog install time.
- A DHCP Server is configured for each VPN allowing connected clients to receive IP addresses from service VPN, as well as default gateway and DNS servers. These values should be added as needed at deploy time (no defaults provided).
- Multiple timers for BFD and OMP have been tuned to reduce LTE bandwidth usage while maintaining SD-WAN functionality.
- A primary and secondary NTP servers with corresponding VPN for access can be configured with primary as preferred source. Also, NTP on wired can be disabled if needed.
- User can set the router console rate (default provided).
- Point router logs to a server of their choice and provide the IP address at catalog install time (default set to 169.254.1.1). Default catalog behavior is to reach Logging server from VPN 4 using a predefined Loopback40 interface. If logging server is not present or needed, catalog defaults can be left as is.
- Assign a loopback IP address to the field "VPN4 Loopback IP" under the service section. This can be assigned same IP address as "System IP" address and serves as a troubleshooting IP as it is advertised and reachable from the Hub. This loopback IP is also It is also used as the source interface to communicate with ISE and Logging servers.
- Enter either a static GPS coordinates for the device to display in UI/MAP or if the device has LTE modem with GPS, then it can be enabled. Both GPS and NMEA must be enabled and the mode set to "standalone" to acquire GPS signal. Modem GPS coordinates will override static coordinates in UI/MAP. If NMEA data streaming is also required, source/destination IP and port should be provided to forward the GPS stream.

NOTES:

1. "device tracking" using dhcp4 instead of ARP is applied in CLI template and usage of dhcp snooping are currently needed on IOS-XE 17.16 or lower to support ISE integration on IR1101.
2. "line vty" config in CLI template is needed to allow ISE users to ssh and enable to router using local user.