White paper
Cisco public

CISCO
The bridge to possible

Extending your SD-WAN-Managed Enterprise Network to Industrial IoT Routers

How to build an IoT AMI network with an SD-WAN-managed Head-End Router

Contents

Why the extension? IoT device and “things” explosion 3

How would it work? 5

Benefits and Conclusions 8

Software-Defined Wide-Area Networking (SD-WAN) technology is always evolving. The latest shift comes as public enterprises that manage large utility networks tackle new security and scale challenges associated with Internet of Things (IoT) devices—introducing the requirement for a Zero Trust security framework and manageability at scale, at the WAN edge.

Cisco® SD-WAN excels in connecting Enterprise devices (routers and platforms) securely to apply an "application first" paradigm to policy and control plane management. That is, devices can communicate only with destinations consistent with their role and security posture. Using SD-WAN templates and configurations that apply intelligence with role-based policy enables enterprises to dynamically segment and isolate traffic based on context, providing consistent and automated definitions of roles across the WAN.

Looking ahead, Cisco SD-WAN will be tasked with intercepting and securing IoT device and headend traffic at scale to contain emerging threats and prevent lateral movement in the event of a breach. At the same time, Cisco SD-WAN will provide the scalability and high availability that is required of IoT Edge devices.

Let us dive deeper into how this will happen and how it can be achieved with the latest features in Cisco vManage that help bridge the gap between IoT and SD-WAN users.

Why the extension? IoT device and "things" explosion

Enterprise networks were never designed to address the complex mix and scale of users, devices, and locations. They were tied to networks that were nailed to specific devices and/or locations. More specifically, with the advent of IoT came the explosion of ruggedized outdoor routers and gateways that require a new family and class of application(s) custom designed to simplify management the IoT gateways, securely and at scale.

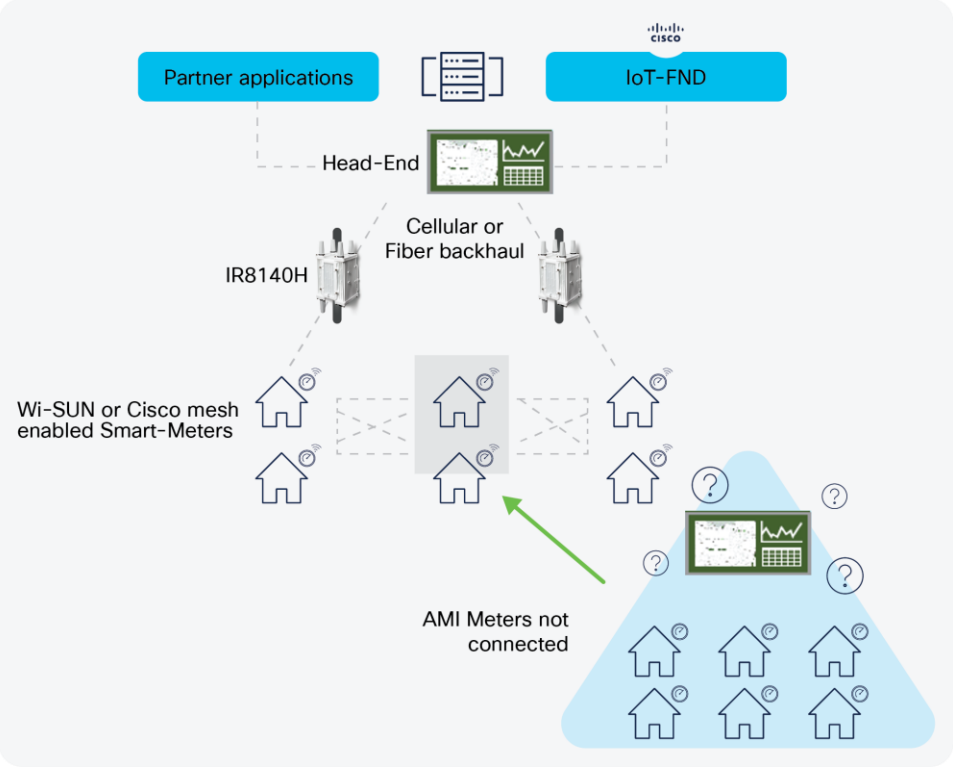

Figure 1.
IoT AMI network use-case

A key use-case for IoT is Advanced Metering Infrastructure, or AMI for short. Using AMI, enormous quantities of electric metering usage data from millions of smart meters are transmitted over WAN backhauls back to the headend or the utility's network operations center. AMI also enables real-time alert reporting, and shutdown of power to a specific location. In addition, other use-cases such as Distribution Automation (DA) and Demand Response provide connectivity to subsets of Distribution Automation devices that need to communicate with each other to manage and control the operation of the electric grid in each area. This functionality requires the use of flexible communication, including IPv6 and peer-to-peer in some cases.

The Primary Management platform for the use-cases mentioned above is the Field Network Director (FND) that enables configuration, device, and fault management at scale and securely. It allows end-to-end lifecycle management of the Cisco Border router—the IR8140H that caters to the use-cases mentioned above, at the same time capable of managing millions of IPv6 Smart meters and DA devices connected via RF-mesh (900MHz) to the Border router.

How do you extend your SD-WAN-managed headend to pull in the devices and use-cases mentioned above?

Using the new Remote Access functionality in Cisco SD-WAN, this is now possible. Existing IoT router will function as a Remote Access client in Flex-VPN mode connected back to the headend. The headend router, in this case the c8000v or Cisco Catalyst® 8500 series Edge platforms will be managed by vManage. This brings multiple benefits of SD-WAN to the IoT world.

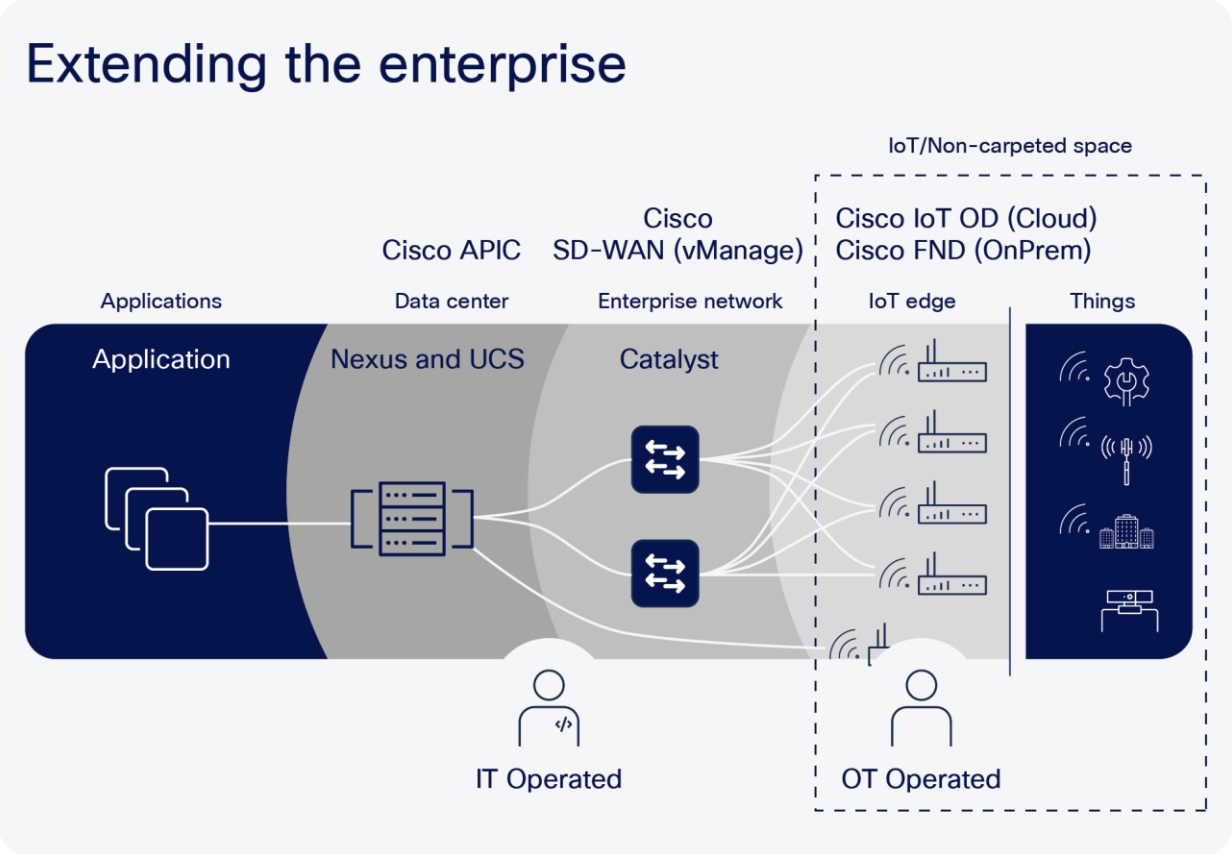

Figure 2.
Extending the Enterprise SD-WAN to IoT

- IoT Edge devices acting as remote access nodes keep the same IOS and management features that would otherwise need to be pulled into SD-WAN controller mode
- Existing customers keep using the same headend
- You can leverage benefits of Flex-VPN to add to the scale of existing SD-WAN deployment without the added overhead of managing IoT endpoints—in this case smart meters or distribution automation nodes (sometimes in the **millions!**)
- Use management tools custom designed for AMI/DA/DR: IoT-FND

How would it work?

The topology below illustrates how this will work. The Flex-VPN tunnel that carries all the IPv6 AMI and DA data is provisioned and managed by vManage. The IoT devices are managed by the IoT Field Network Director. The ZTP (Zero Touch Provisioning) process shows how this is accomplished.

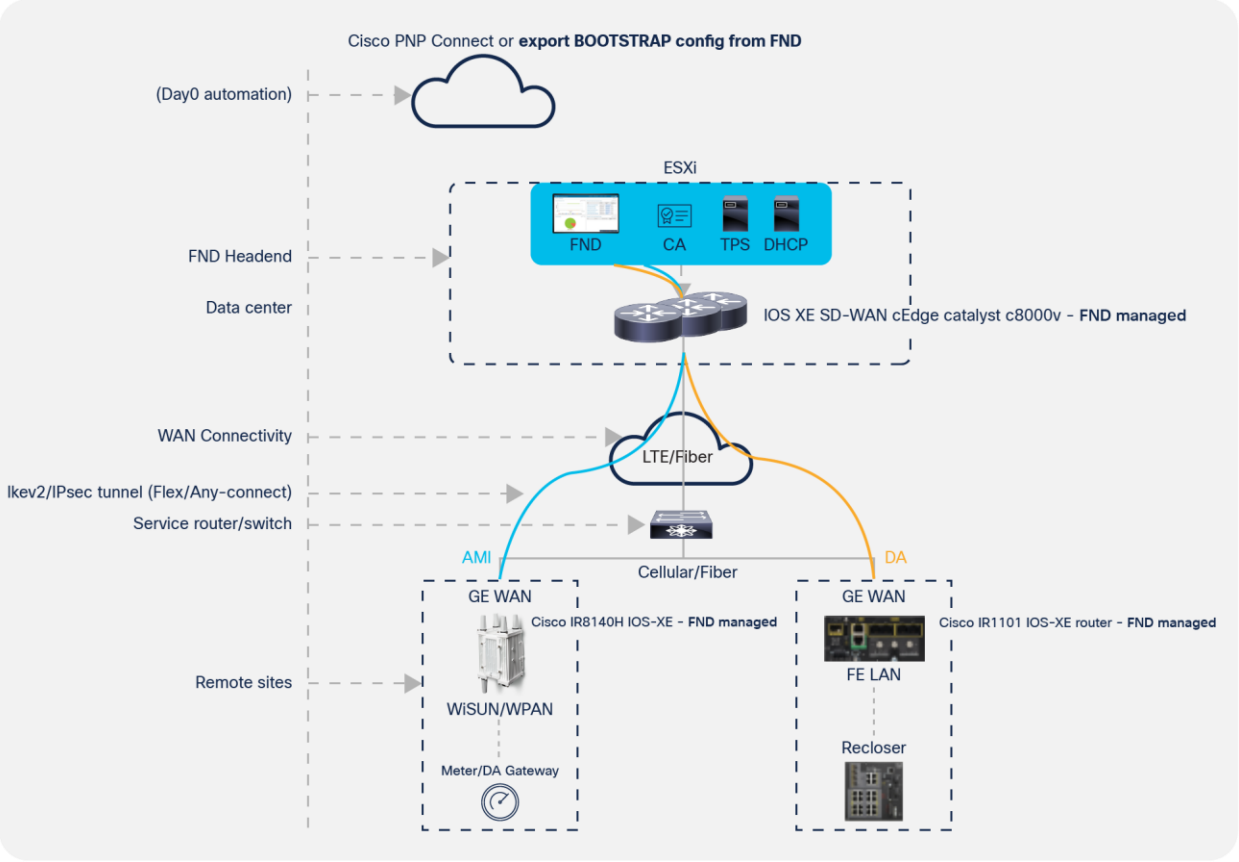

Figure 3.
SDWAN + IOT architecture

The figure above shows the current way that the AMI architecture and solution works with only the Field Network Director (FND) managing the entire network including the headend. Customers migrating to SD-WAN-based solutions will integrate the existing AMI headend infrastructure as shown below.

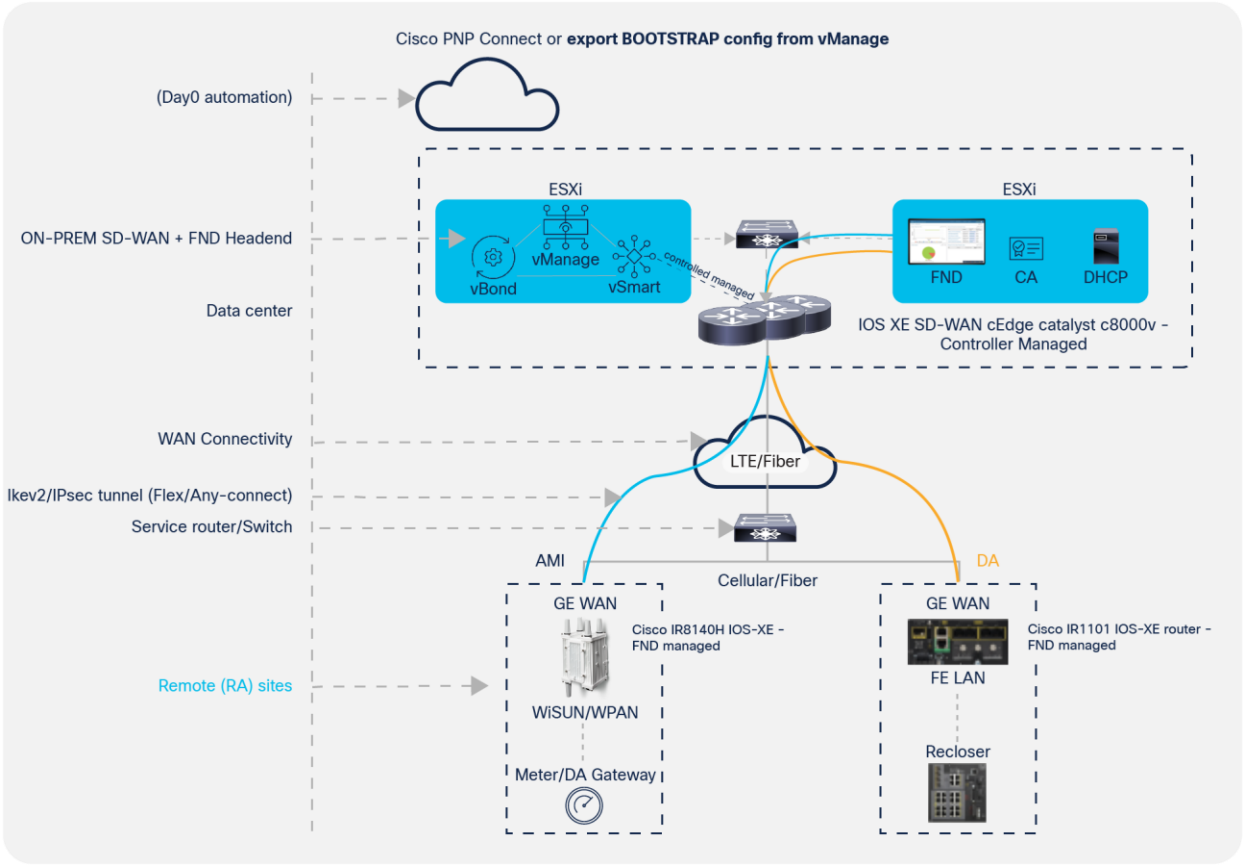

Figure 4.
Topology overview

The ZTP process is shown below. The first step is to provision the c8000v or Catalyst 8500 in vManage, and then provision the IoT routers and devices.

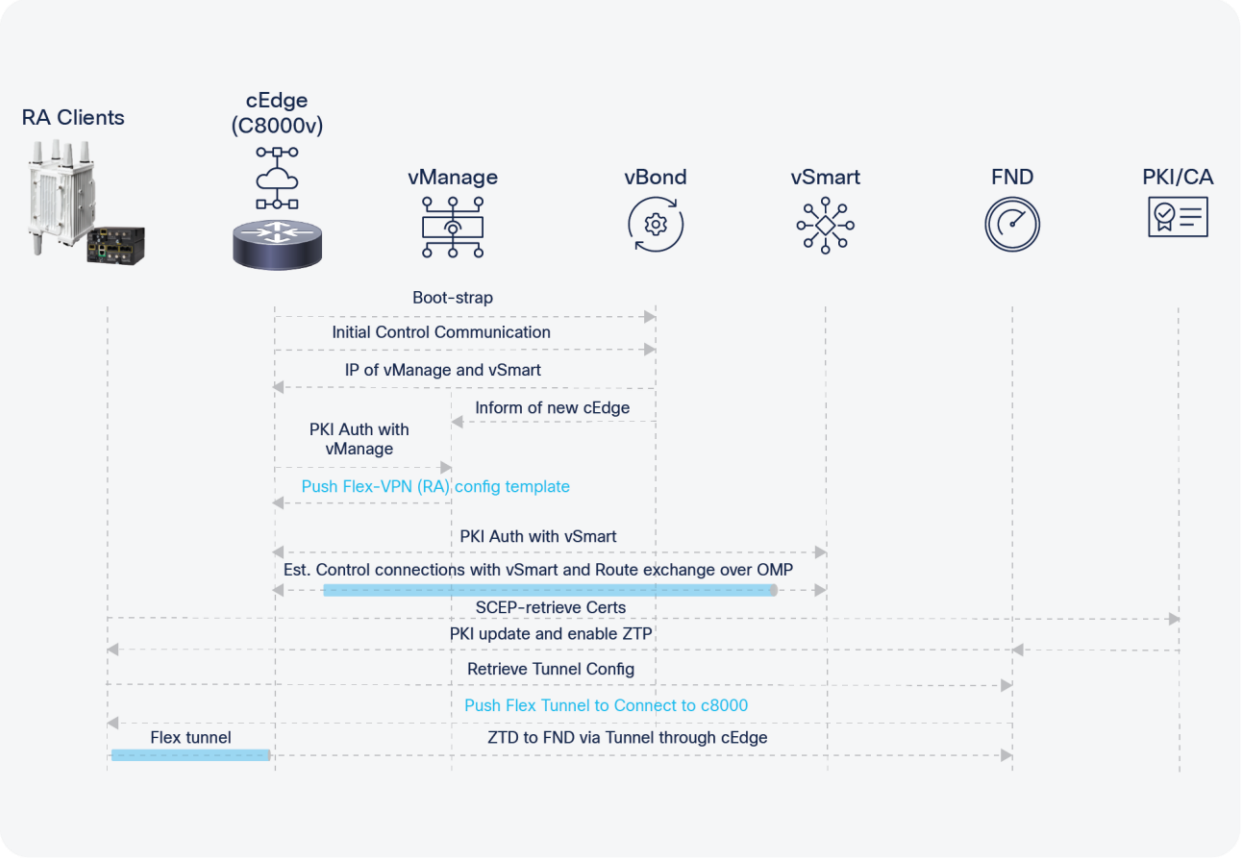

Figure 5.
ZTP process

The router now has a path back to the headend via the c8000v and the IoT-FND Management platforms—with the AMI endpoints behind the IR8100 ready to be managed by the Field Network Director.

Benefits and Conclusions

There are numerous benefits **to extending your SD-WAN-managed enterprise network with industrial IoT routers:**

- This approach is highly beneficial to existing Cisco SD-WAN, AMI/DA customers looking to extend the network outdoors and to eliminate the need for separate OT/IT deployments
- You get to keep the original Remote Access IoT router mode (autonomous) and deployment configurations for RA (remote) clients
- You can use the benefits of Flex-VPN to add to scale of existing SD-WAN deployment without the added overhead of managing the Remote Access clients via vSmart
- RA clients function as branch LAN users, and SD-WAN benefits are extended through to them via the RA headend:
  - Application visibility, application-aware routing policies transferred via the RA headend to RA clients
  - App-QoE, Quality of Service (QoS)
  - Rate limiting and traffic shaping via the RA headend and policies applied by vManage to the Flex-VPN Tunnel
- Scaling to millions of RA clients has no impact on Cisco SD-WAN scale limitations

Learn more, visit: cisco.com/go/ir8100

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C11-3134262-00 08/22