



Problems of Traditional Building Systems

Traditional building systems consist of siloed networks built and maintained as individual systems such as lighting; Heating, Ventilating, and Air Conditioning (HVAC); metering; fire; Uninterruptible Power Supplies (UPS); video surveillance; physical access; and others. The duplication of networks for each of these systems results in higher installation, commissioning, and maintenance costs. Many of the systems that consume energy within buildings implement communication protocols and formats, limiting access to important information and building functionality. Proprietary building-automation systems and black boxes provide access to only a subset of the energy consuming systems within a facility. The lack of unification amongst all these disparate building systems and lack of centralized monitoring and control across global operations leads to inefficiencies and increased energy consumption.

New Open Energy Management Systems

Cisco's Network Building Mediator is an open, any-to-any networked energy, facility, and sustainability platform developed specifically to connect to the wide range of existing building systems and normalize building system informational data. Using cloud services such as Automated Demand Response (ADR), this data can be correlated across each system at a site, multiple systems at a site, and multiple sites over time. Underperforming sites can be identified and adjusted, resulting in significant energy savings and cost reductions. Through the use of controlled energy systems, it is also possible to participate in an ADR and dynamic-pricing programs from utility companies, potentially gaining additional cost savings. The Network Building Mediator will also provide critical energy usage and forecast information to Smart Grid programs as they become available.

Cisco Network Building Mediator

The Cisco Network Building Mediator is the centerpiece of the open sustainability and energy management solution. It is a hardened network appliance connecting disparate building systems of various communication protocols onto the IP network. Cisco routing platforms have connected multiprotocol networks for years; now this functionality is extended to include building systems with the Mediator. The Mediator aggregates

and normalizes building systems data, making it available through an open XML interface. The Mediator comes in the following two models:

- The Cisco Network Building Mediator 4800, targeted for campus deployments.
- The Cisco Network Building Mediator 2400, targeted for branch deployments.

Network Design Implications

When designing a converged IP network infrastructure to support both traditional IT services (for example, voice, video, and data applications) and energy management systems, the design engineer should be particularly aware of the security implications involved. These security requirements must be balanced against the business requirements of the energy management system itself, including its evolution over time.

The Cisco Network Building Mediator contains two Ethernet ports, one of which can be used for the management network segment, while the other can be used for the segment which houses IP-based building system devices. These interfaces are typically referred to as *north side* for the management interface and *south side* for the building systems interface.

When the Mediator is integrated with critical energy and facility management systems, it is recommended to improve security by isolating the network segments connected to the Mediator from the rest of the IP network infrastructure and tightly controlling access to these network segments. The management network segment (for example, a *north side* segment) should be separated wherever possible from the network segment that the building devices are connected to (for example, a *south side* segment), especially when using IP-based energy management systems protocols such as BACnet/IP, Modbus/TCP, etc. Although many of the open standards for IP-based energy management systems protocols have security features such as encryption and authentication, actual implementations by vendors may not offer these security features. Many offerings of IP-based energy management systems protocols often use broadcast technologies, requiring the need for flat networks and/or specialized broadcast servers. Therefore, isolating these network segments is prudent.

Network isolation within the LAN infrastructure can be accomplished through several methods, including separate physical switches dedicated to energy management systems. The preferred method is to use separate logical VLAN segments

provisioned off of a converged switch infrastructure. Using a converged switch infrastructure design has the advantage of lower overall hardware and reoccurring maintenance costs.

Access control to the energy management systems segments can be accomplished through the following methods:

- Dedicated firewall appliances, such as the Cisco ASA 5500 Series.
- Firewall services integrated within a router or switch platform, such as the IOS Firewall feature set of Cisco ISR router platforms, or the Firewall Services Module (FWSM) of the Cisco Catalyst 6500 Series switch platforms.
- Access-control lists (ACLs) within a Layer-3 switch or a router platform.
- Site-to-site or client-based IPsec VPN connectivity.

The use of secure management protocols (for example, encrypted and authenticated) is highly recommended. Specific protocols required for management and cloud services should be identified and tied to unique source and destination IP addresses for firewall, ACL, or IPsec VPN connectivity.

Management services include protocols required for provisioning the Mediator onto the network infrastructure. These can include DHCP, DNS, NTP, HTTP/S, and FTP/S. Management services include protocols required for creating applications deployed on the Mediator through perfectHOST as well as HTTP/S for monitoring such applications. Additional protocols can include Remote Node Abstraction (RNA), SSH/SCP for secure file transfers, and SMTP used for alarm notification and/or exporting of data logs.

Note Protocols required for management services are often bidirectional and may need to be established both inbound to the Mediator and outbound from the Mediator.

Cloud services include protocols necessary for services such as Energy Scoreboards, Enterprise Energy Management (EEM), event reporting, ADR, dynamic pricing, and Automated Fault Detection and Diagnostics (AFDD). Data is typically logged and exported uni-directionally from the Mediator through SFTP/FTP or through HTTP/S POST to support such services.

Deployment Models

The deployment of energy management systems often follows two models. In the first model, a managed service provider (MSP) deploys or uses a Cisco partner to deploy the system for the enterprise customer. In this model, the customer or the MSP manages the system on a day-to-day basis. This deployment model implies full management and monitoring capabilities to and from the Mediators for both the MSP and the enterprise customer concurrently. The most common method for the MSP to provide this service is connectivity via IPsec VPNs. Other interactive data flows to entities such as a utility company may be required for automated-demand response or dynamic pricing applications.

For the second model, the enterprise customer may use a Cisco partner to deploy, and then manages the energy management system themselves. This deployment model requires full management and monitoring capabilities to and from the Mediators and management workstations within the enterprise. Logging data may still be exported from the Mediators to an MSP in order to provide cloud services such as an Energy Scoreboards, ADR, AFDD, and dynamic pricing applications.

Specific considerations for the branch and campus *Places-in-the-Network (PINs)* designs are discussed in the following subsections.

Branch PIN Design Considerations

When designing the network to support one or more Mediators within a branch location, the design engineer must first determine the deployment model. As mentioned above, installations involving a deployment partner often require VPN access to and from the Mediators within the branch back to the MSP network.

VPN access can take the form of a dedicated VPN router and/or switch separated from the existing branch IT network through a Cisco ASA 5500 firewall appliance. Although this type of implementation provides a high degree of isolation and access control, the duplication of the switch infrastructure, dedicated VPN router, and firewall appliance results in higher hardware and ongoing maintenance costs.

The preferred approach is to provision separate VLAN segments on the existing branch Catalyst switch platform for energy management. A single Cisco ISR branch router can provide both the WAN access to the branch from the enterprise campus network, as well as the VPN access from the MSP network (with appropriate software image and licensing). In cases where an IPsec VPN provides the enterprise WAN connectivity, an additional VPN tunnel can be provisioned to the MSP network. In the case where private enterprise WAN connectivity is provisioned, a separate Internet connection could be provisioned on the Cisco ISR branch router. The Cisco IOS Firewall feature set would be used to provide access control between the energy management systems VLANs and the rest of the enterprise network, including the MSP network. If a higher level of isolation is desired, IPsec VPN tunnels can be provisioned internally within the enterprise network (for example, between the Network Operations Center (NOC) and the branch ISR router). Comparatively, this design option results in lower hardware and ongoing maintenance costs, but the management and reoccurring costs of an additional VPN connection for each branch location may prohibit the scaling of this implementation.

For large implementations, centralizing the MSP VPN connectivity to a campus or data center location provides a much more scalable and manageable deployment. The deployment shown in below uses a separate VPN router deployed within the Internet edge of a campus to terminate the IPsec VPN connection from the MSP. Access control configured on the Internet edge firewall allows the MSP to access only the energy management systems subnets (i.e., subnets with Mediators deployed) throughout the enterprise network. Additionally, a combination of ACLs and firewalls on Layer-3 branch switches and ISR routers limits access to only the energy management systems within the individual branches.

Alternatively, complete segregation of all communication could be achieved using VRFs. The centralized VPN connectivity from the MSP to all of the enterprise energy management systems using a segmented VRF would provide complete path-isolation of the energy management systems traffic and require only a centralized security policy.

Enterprise customers typically handle the day-to-day operations and management of building system networks. [Figure 1](#) shows how the NOC segments may be provisioned within a location to

centrally manage the building system deployment. Access control to and from the enterprise NOC segments can be achieved through a FWSM deployed in Cisco Catalyst 6500 service switches within the data center.

Campus PIN Design Considerations

As with the branch network, the design engineer must first determine the deployment model when designing the campus network to support an energy management solution. When MSP access is required, separate VPN connectivity from each campus building is again possible but not scalable. Where possible, it is recommended to centralize the VPN access from the MSP network, providing a more maintainable and cost effective solution.

With the deployment of Layer-3 switches in the access layer as well as the Cisco Catalyst 6500 switches within the distribution layer of campus buildings, a wider range of access control exists within the campus compared to the branch. If Layer-2 access switches are deployed within campus buildings, either ACLs or a FWSM can be deployed within the Cisco Catalyst 6500 distribution switches.

Finally, the deployment of a separate VRF for energy management systems can provide the additional advantage of complete path-isolation of the energy management systems traffic across the campus network infrastructure.

Summary

The Cisco Network Building Mediator is the centerpiece of the open sustainability and energy management solution, aggregating and normalizing energy management systems, and making them available through an open XML interface over an IP network infrastructure. As the Mediator interfaces with critical energy management systems, the design engineer must be cognizant of the requirements for tight access controls. Access control can be accomplished through multiple mechanisms, including IPsec VPN connectivity, firewall appliances, VRF segmentation, integrated firewall services, and ACLs within router and switch platforms.

For more information, visit the following URL:

<http://www.cisco.com/go/designzone>

Figure 1 Example Branch and Campus Mediator Design with Centralized VPN Connectivity

