CHAPTER 2

Deployment Models and Information Flows

This chapter discusses common deployment models for an energy management solution using the Cisco Network Building Mediator. Following the deployment models, a detailed discussion is provided of the protocols necessary for the operation of the management interface of the Mediator over the IP network infrastructure.

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. 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. Note that other interactive data flows to entities such as a utility company may be required for automated-demand response (ADR) or dynamic pricing applications. Partner VPN connectivity may be centralized or distributed. Centralizing the partner VPN connectivity to a single entrance point, such as a campus location, provides a more scalable, cost effective, and manageable solution. However, it also requires MSP partner traffic to traverse the enterprise network infrastructure.

Centralized partner VPN connectivity is typically used for medium to large sized energy management solution deployments, where the locations are already connected via an enterprise WAN infrastructure. Distributed partner VPN connectivity is typically used for small energy management solution deployments with only a handful of independent locations, which may or may not be connected by an enterprise network infrastructure. Distributing the partner VPN connectivity typically requires Internet connectivity and VPN hardware at each site in which a Cisco Network Building Mediator is deployed. However, it does not require MSP partner traffic to traverse an enterprise network infrastructure.

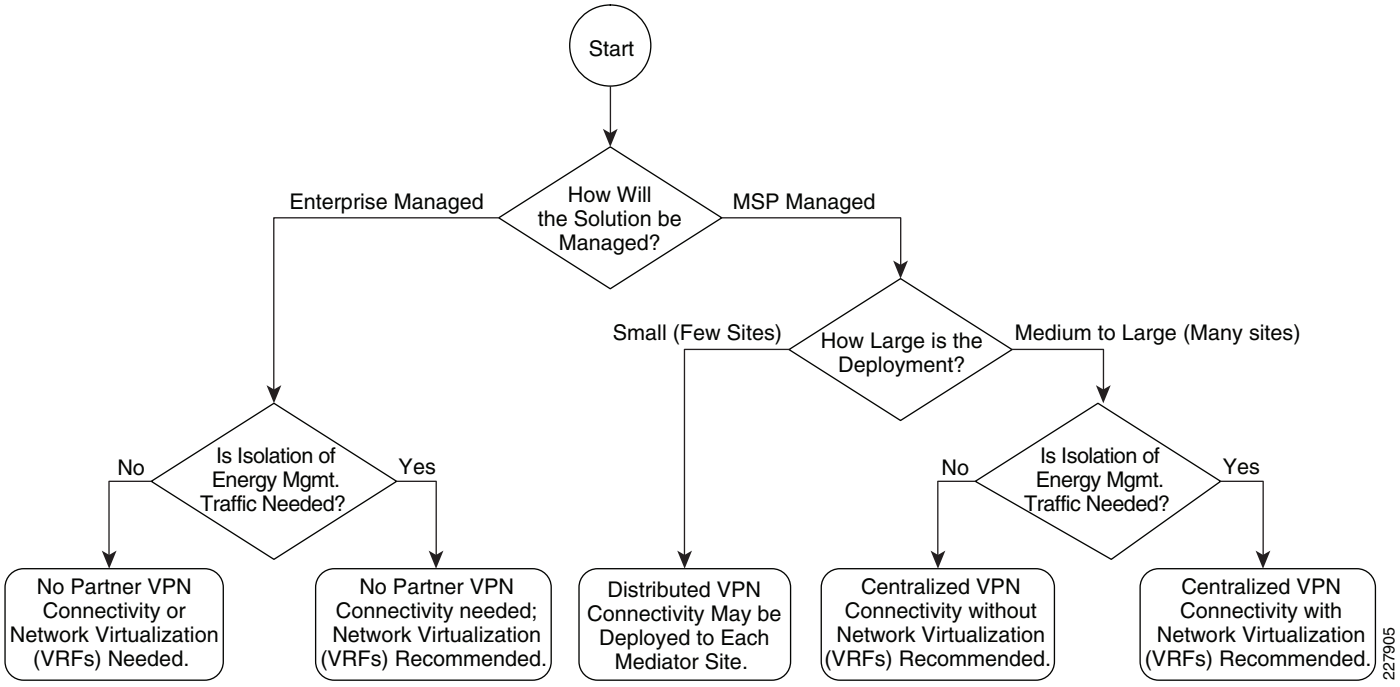
With the second deployment model, the enterprise customer may use a Cisco partner to deploy and then manages the energy management system themselves. This model requires full management and monitoring capabilities to and from the Mediators and management workstations within the enterprise. However, partner VPN connectivity may not be needed. Logging data may still be exported from the Mediators to a MSP via the Internet in order to provide cloud services such as Energy Scoreboards, ADR, AFDD, and dynamic pricing applications. Alternatively, logging data may be collected within an enterprise archiving server and an internal Energy Scorecard deployed using a partner or internally developed.

In addition to the choice of whether an MSP will deploy and manage the solution, or whether the solution will be managed by the enterprise customer, the network design engineer must also decide whether traffic isolation is a requirement in order to support the energy management solution. Network virtualization refers to the creation of logically isolated network partitions overlaid on top of a common enterprise physical network infrastructure.

Network virtualization is accomplished through the deployment of Virtual Routing and Forwarding (VRF) technology. VRF technology is a path isolation technique used to restrict the propagation of routing information, so that only subnets belonging to a particular virtual network (VPN) are included in any VPN-specific routing tables. This results in the creation of independent logical traffic paths over a shared physical network infrastructure. VRFs can be used to separate and isolate energy management traffic flows from normal data traffic in order to provide an additional layer of network security for the energy management solution.

Figure 2-1 summarizes the choices for deployment of the energy management solution over an enterprise network infrastructure.

Figure 2-1 Energy Management Solution Deployment Flowchart



Information Flows

This section discusses some of the information flows and network protocols required on the energy management interface or north side of the Cisco Network Building Mediator for operation over the IP network infrastructure. These protocols can be separated into two broad categories---Management Services Protocols and Cloud Services Protocols.

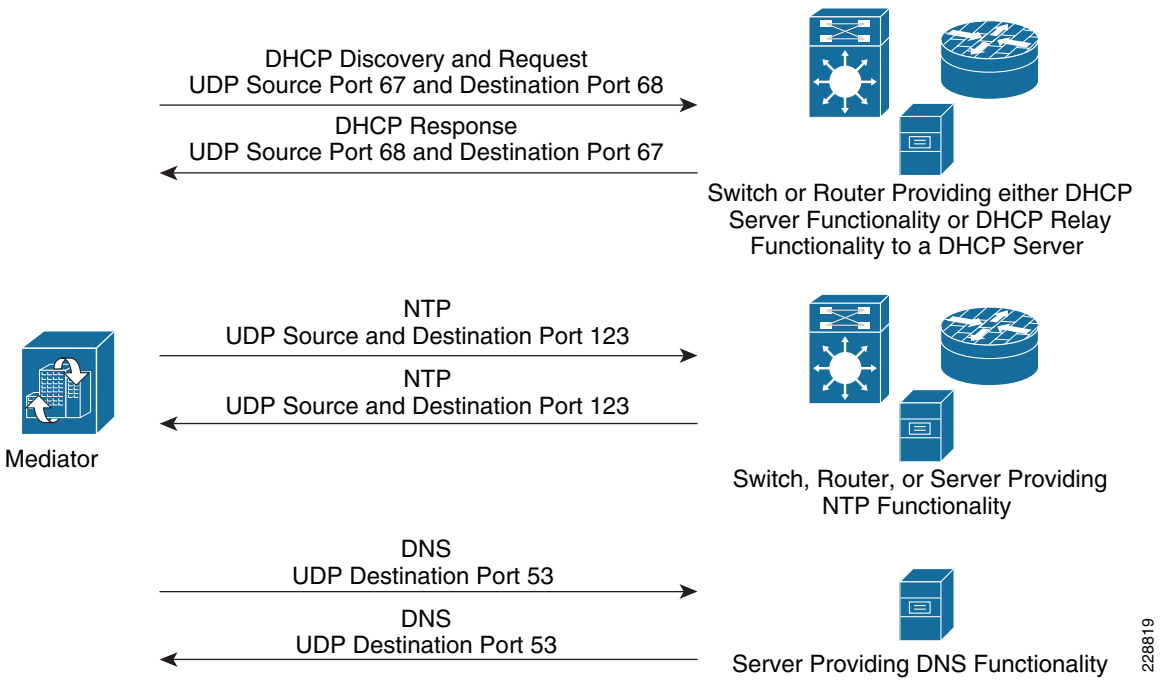
Note The current version of this design guide does not include discussion of the information flows and protocols between the actual building devices (chillers, boilers, HVAC systems, etc) and the building systems interface or south side of the Mediator. Future revisions may include discussions of such flows as well.

Management Services Protocols

Management services include the protocols and information flows required for provisioning the Mediator onto the network infrastructure. They also include the protocols and information flows required for configuring the Mediators, creating control logic which is then deployed onto the Mediator, and for monitoring and managing the Mediators.

Device provisioning protocols can include Dynamic Host Configuration Protocol (DHCP), Domain Name Services (DNS), and Network Time Protocol (NTP). Figure 2-2 shows an example of these flows.

Figure 2-2 Management Flows—Device Provisioning



DHCP support is needed if the Mediator uses dynamic IP addressing. In such cases, either the local Catalyst switch or Cisco router connected to the Mediator Ethernet interface can be configured with DHCP server functionality to hand out IP addresses. Alternatively, the switch or router can be configured with DHCP relay functionality to relay the request to a DHCP server centrally located within a data center or campus service module. DHCP uses UDP ports 67 and 68.

Note From a security perspective, configuring access control down to specific IP addresses and protocols is discussed throughout this document. The use of DHCP to provide IP addressing to the Mediator may complicate the configuration of access control lists on firewalls, Layer 3 switches, and routers. In such

situations, the network administrator may need to either ensure the Mediator always receives the same IP address from the DHCP server, or the access control lists may need to be expanded to include the range of addresses which the Mediator may receive. Note that the second alternative presents a somewhat larger security concern since access control to the energy management solution is less specific.

DNS is required if the hostnames are configured within the Mediator. If hostnames are used, the Mediator must query a DNS server in order to translate the names to IP addresses in order to reach the destinations. For campus locations, DNS servers may be centrally located within a data center or campus service module. Additional DNS servers may be deployed within branch locations. DNS uses UDP destination port 53 for queries to the server and responses from the server.

NTP is recommended for time synchronization of devices across the network infrastructure. This is particularly important if schedules are implemented within the Mediator. Also, the periodic exporting of log data requires accurate time synchronization of Mediators in order to make sense of the logged data. Network administrators typically synchronize the clocks of network infrastructure devices, so the local Catalyst switch or Cisco router connected to the Mediator Ethernet interface can be configured with NTP functionality to synchronize the clock of the Mediator. Alternatively, a server centrally located within the data center service module or campus service module can serve as the NTP server to synchronize all Mediators. NTP uses UDP source and destination port 123.

Note that when deploying a separate VRF for the energy management solution (also referred to as the Building Infrastructure Network or BIN VRF within this document), the network administrator must carefully consider how DHCP, DNS, and NTP services are provided for the energy management solution. In deployments where centralized servers provide these functions, a separate set of servers dedicated to the energy management VRF may need to be deployed. Alternatively, connectivity between the energy management VRF and the another VRF (either the global VRF or a VRF dedicated to provide such services) may need to be provisioned. Chapter 5, “Data Center/Campus Service Module Design Considerations” discusses some design options around connectivity between the energy management VRF and other VRFs.

As mentioned above, management services also include protocols required for configuring the Mediators, creating control logic deployed onto the Mediator, and for monitoring and managing the Mediators. These services are provided through the management applications listed in Table 2-1.

Table 2-1 Mediator Configuration and Management Applications

Application Name	Description
configTOOL	ConfigTOOL is a software application that runs on an enterprise energy management workstation or managed service provider (MSP) partner workstation, which is used to configure the system settings, protocols, and services on the Mediator. The XML file created by configTOOL, which holds the Mediator configuration, is named broadway.xml.
perfectHOST	PerfectHOST is an application that runs on an enterprise energy management workstation or MSP partner workstation, which provides an intuitive graphical programming tool for creating control logic that resides on the Mediator. Logic is built by adding functional building blocks called templates to the canvas and connecting them together to create drawings. PerfectHOST comes with a pre-built library of 1,000 + templates such as I/O, logic, and protocol.
OMEGA	OMEGA is a software suite used to program and configure the Mediator. The OMEGA software tools are served to the browser of the enterprise energy management workstation or MSP partner workstation by the Mediator's internal Web server.

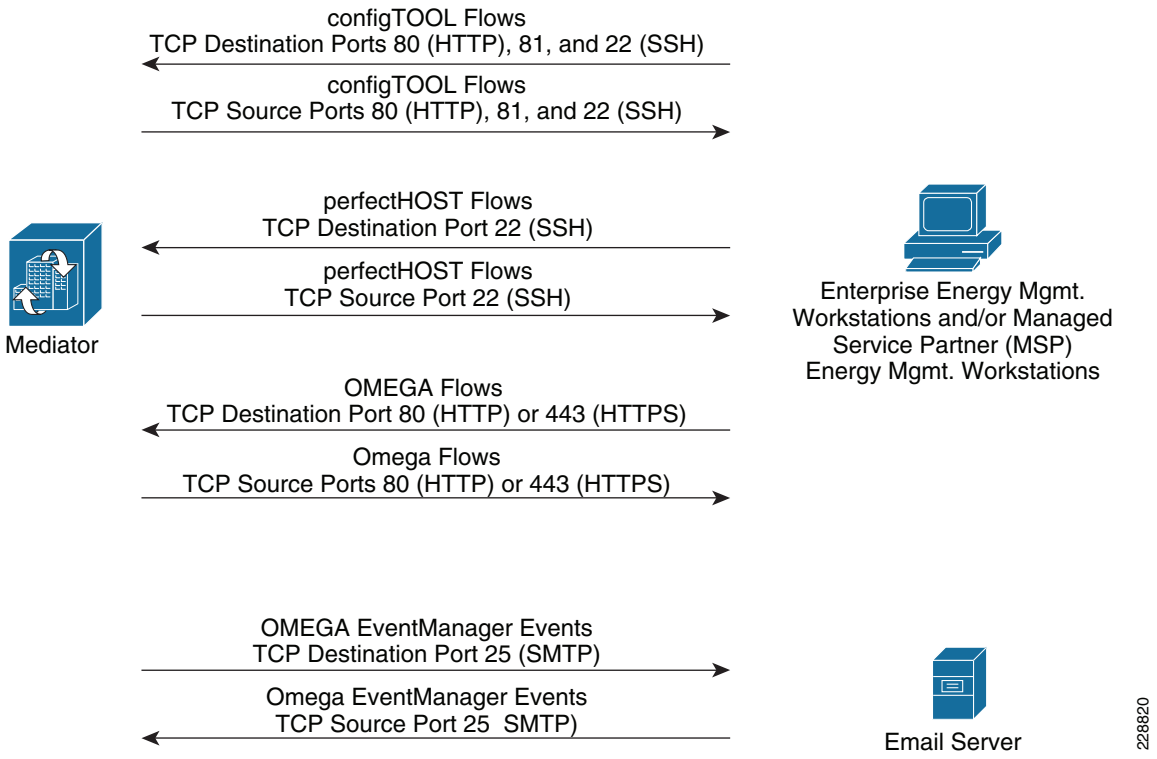
Specific tools within the OMEGA software suite are listed in Table 2-2.

Table 2-2 OMEGA Tools

OMEGA Tool	Description
System	OMEGA system allows the network administrator to view and modify Mediator network settings, backup and restore the Mediator, upload Mediator keys, reset OMEGA, and troubleshoot the Mediator through the Mediator message log.
EventManager	EventManager is an OMEGA tool for creating and viewing events on Mediators. It is typically used to define alarm conditions that, when met, display alarm events in EventManager and deliver e-mails. EventManager can view and acknowledge the events in multiple Mediators defined within a “cloud”.
SecurityManager	SecurityManager service allows the network administrator to define and manage access to resources on the Mediator, including authorization and restriction of the ability of users to view information, to modify settings, to add, modify, or delete files, etc.
TrendManager	TrendManager is a service that allows the network administrator to configure and manage trends. Trends are log nodes that record changes in the values of specified nodes over time. Trends can be viewed as graphs directly from the Mediator.
WebScheduler	WebScheduler allows network administrators to make customized project and system schedules with an Internet browser.
WebExpress	WebExpress is a Web page authoring tool within the Mediator which allows network administrators to create Web monitor drawings using customizable widgets, graphics, and live datapoints from the Mediator.
Web SiteBuilder	Web SiteBuilder allows network administrators to quickly create and customize the look and feel of the “Home Page” of the Mediator or default Web page.

Figure 2-3 shows the protocols required to enable the flows needed by the Mediator configuration and management applications.

Figure 2-3 Management Flows—Device Configuration, Logic Configuration, and Monitoring



ConfigTOOL uses TCP ports 80 (HTTP), 81, and 22 (SSH) to establish connectivity to the Mediator and download the broadway XML file to configure it. PerfectHOST uses TCP port 22 (SSH) in order to establish connectivity and download the control logic it creates into the Mediators. The various applications which make up the OMEGA software suite use TCP ports 80 (HTTP) or 443 (HTTPS). Figure 2 shows that for each of these applications, the flow is initiated from the enterprise energy management or MSP partner workstation to the Mediators. However, the reverse traffic must be allowed through the network infrastructure for the session to be established as well. Note, however, that OMEGA EventManager can initiate events outbound from the Mediator to e-mail servers via TCP port 25 (SMTP).

One additional protocol that may be used by the Mediators is the Remote Node Abstraction (RNA) protocol. RNA is the protocol used to share node values (such as data points) between Mediators. RNA allows two or more Mediators on the same network to share points in a peer-to-peer manner or hierarchical manner. RNA uses TCP port 5150 as shown in Figure 2-4.

Figure 2-4 Management Flows—Remote Node Abstraction (RNA)

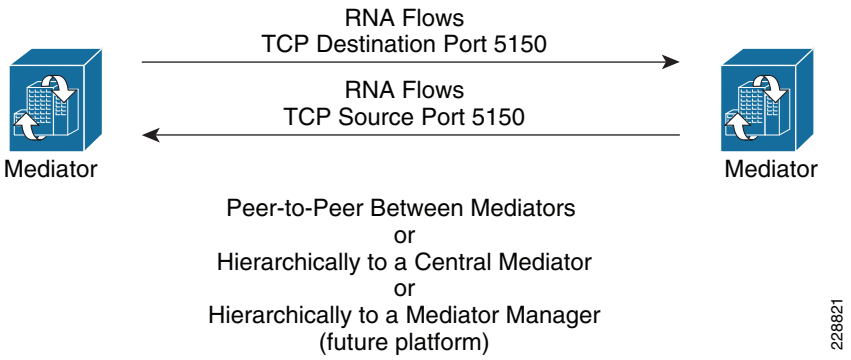


Figure 2-4 shows a scenario where the Mediator on the left has aliased a node on the Mediator on the right. Therefore the RNA flow is initiated by the Mediator on the left, with a destination TCP port of 5150. The response (return traffic) has a source TCP port of 5150. Chapter 5, "Data Center/Campus Service Module Design Considerations" discusses the hierarchical portal model further.

Cloud Services Protocols

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 to cloud services servers located on the Internet. Datapoints can be periodically logged in intervals from 15 seconds to 1,800 seconds (30 minutes) and stored on the Mediator until they are ready to be exported. The Mediator is capable of exporting periodic logged data via File Transfer Protocol (FTP), Secure File Transfer Protocol (SFTP), Hypertext Transfer Protocol (HTTP) POST, Secure Hypertext Transfer Protocol (HTTPS) POST, and Simple Mail Transfer Protocol (SMTP). Periodic logged data can be exported in intervals from every minute to once every week (providing sufficient buffering capacity exists to hold the periodic logged data between exports). The Mediator is capable of sending the logged data in various formats, although the XML data format is most commonly used. Example 2-1 shows an example of an FSG XML format showing multiple data points.

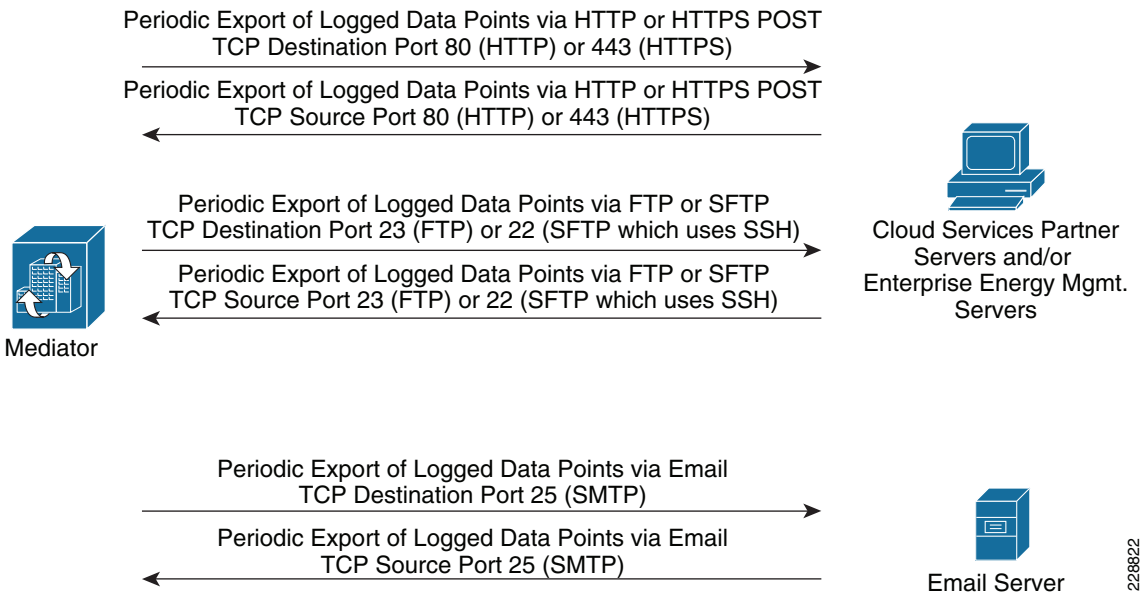
Example 2-1 Example Mediator Data Export in FSG XML Format

```
<data info="RTP_Cisco_Systems" key="RTP000000001">
 <device info="ESE_Lab_Meter_A" key="rtp001">
  <channel name="Volts_B2C" Totalized="N" uom="Voltage" key="5" Delta="N"
meastype="Volts">
   <value timestamp="2009-09-24T13:15:00">280
   </value>
  </channel>
  <channel name="Amps_Phase_B" Totalized="N" uom="Current" key="2" Delta="N"
meastype="Amps">
   <value timestamp="2009-09-24T13:15:00">531
   </value>
  </channel>
  <channel name="Amps_Phase_C" Totalized="N" uom="Current" key="3" Delta="N"
meastype="Amps">
   <value timestamp="2009-09-24T13:15:00">516
   </value>
  </channel>
```

```
  <channel name="Amps_Phase_A" Totalized="N" uom="Current" key="1" Delta="N"
meastype="Amps">
   <value timestamp="2009-09-24T13:15:00">505
   </value>
  </channel>
  <channel name="KVA" Totalized="N" uom="Power" key="8" Delta="N" meastype="KVA">
   <value timestamp="2009-09-24T13:15:00">1261.41912
   </value>
  </channel>
  <channel name="Power_Factor" Totalized="N" uom="Ratio" key="9" Delta="N"
meastype="Ratio">
   <value timestamp="2009-09-24T13:15:00">0.95
   </value>
  </channel>
  <channel name="Volts_A2B" Totalized="N" uom="Voltage" key="4" Delta="N"
meastype="Volts">
   <value timestamp="2009-09-24T13:15:00">273
   </value>
  </channel>
  <channel name="Volts_A2C" Totalized="N" uom="Voltage" key="6" Delta="N"
meastype="Volts">
   <value timestamp="2009-09-24T13:15:00">273
   </value>
  </channel>
  <channel name="Volts_3_Phase" Totalized="N" uom="Voltage" key="7" Delta="N"
meastype="Volts">
   <value timestamp="2009-09-24T13:15:00">478
   </value>
  </channel>
 </device>
</data>
```

Figure 2-5 shows the protocols required to enable the data flows associated with the periodic export of logged data from the Mediators.

Figure 2-5 Cloud Services Flows—Periodic Export of Logged Datapoints



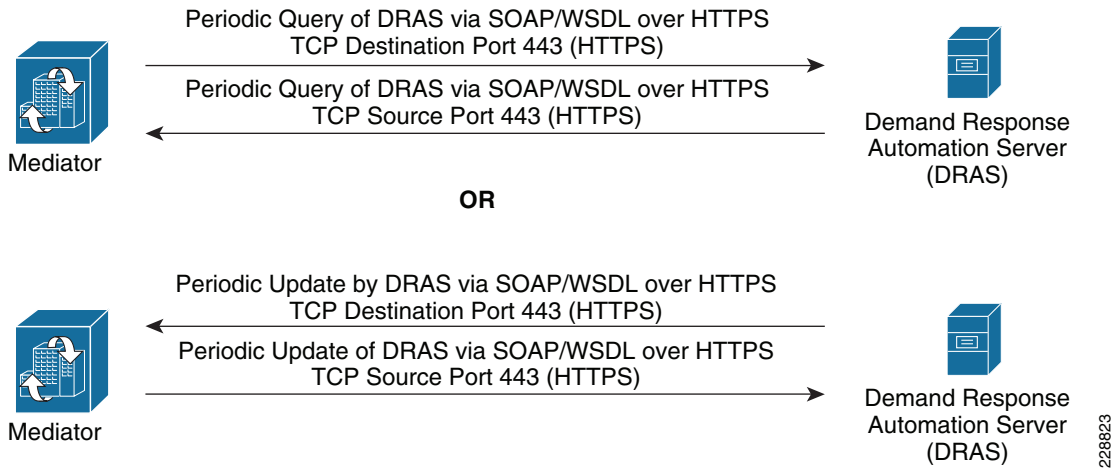
The data flows associated with the periodic export of logged data points are typically initiated from the Mediator outbound to a cloud services partner server and/or an enterprise archiving server. However, the reverse traffic must be allowed back through the network in order for the session to be established. 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. The use of secure protocols (for example, encrypted and authenticated) is highly recommended.

Note The FTP protocol dynamically opens a data channel separate from the control channel, which uses TCP port 23. Stateful firewalls with application-layer inspection open and close the data channel automatically, based upon inspection of the FTP control channel. However, when using ACLs, the network administrator may have to statically open the port range needed for the FTP control channel. Note that SFTP, which uses the SSH protocol (TCP port 22), does not use a separate dynamic data channel.

Automated Demand Response (ADR) systems often use standards-based protocols such as SOAP/WSDL over HTTP/HTTPS in order to exchange event state information between the Mediator and the energy service provider (utility companies, etc.). Figure 2-6 shows an example of some of the flows which may be involved.

Note ADR functionality has not been tested or validated with the Mediator for the current version of this design guide. The example below serves as possible example only. Future revisions may include ADR testing.

Figure 2-6 Cloud Services Flows—Example Automated Demand Response Flows



In the example shown in Figure 2-6, a server (sometimes referred to as an Demand Response Automation Server or (DRAS)) is deployed at the energy service provider location. The Mediator may function as a DRAS client, periodically polling the DRAS for event state information. Alternatively, the DRAS may periodically update the Mediator, although this requires the network administrator to allow connections initiated from the energy service provider into the enterprise network, which may be less desirable. Transport Layer Security (TLS) as well as userid and password are commonly used with ADR systems in order to ensure confidentiality and authenticate the sessions. The Mediator mat then use the event state information from the DRAS to implement pre-programmed logic, such as resetting the setpoints of thermostats, in order shed load and reduce energy consumption.

Specific design considerations for support of the energy management solution within campus and branch locations are discussed in detail in Chapter 3, "Campus Design Considerations" and Chapter 6, "Branch Design Considerations."