TR-069: A Brief Overview

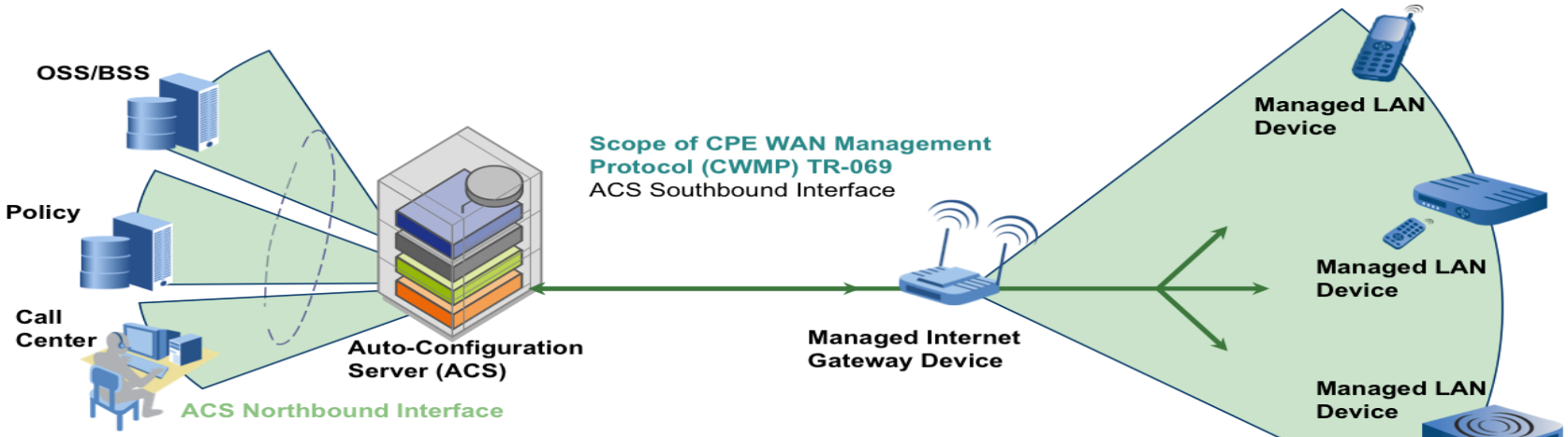
Jason Walls, QA Cafe
BroadbandHome WG Co-Chair
June 26 2014

CPE WAN Management Protocol (CWMP)

TR-069 Defines CWMP

- CWMP is the CPE WAN Management Protocol
- Provides secure auto-configuration, troubleshooting, and maintenance and monitoring of CPE
- Industry leading solution for remote device management
- Managing a projected 250 million devices worldwide
- De-facto standard, referenced and/or endorsed by 3GPP, ISO, ATIS, ETSI, ITU-T, UPnP, HGI, etc.

TR-069 Architectural Components



Management Functions

- Bootstrap
- Service Provisioning
- Firmware and Software Module Management
- Diagnostics
- Fault and Performance Monitoring
- Large and growing set of defined object models

Device Management

ACS

ACS sends requests to CPE via established CWMP Session

RPC

RPC Response

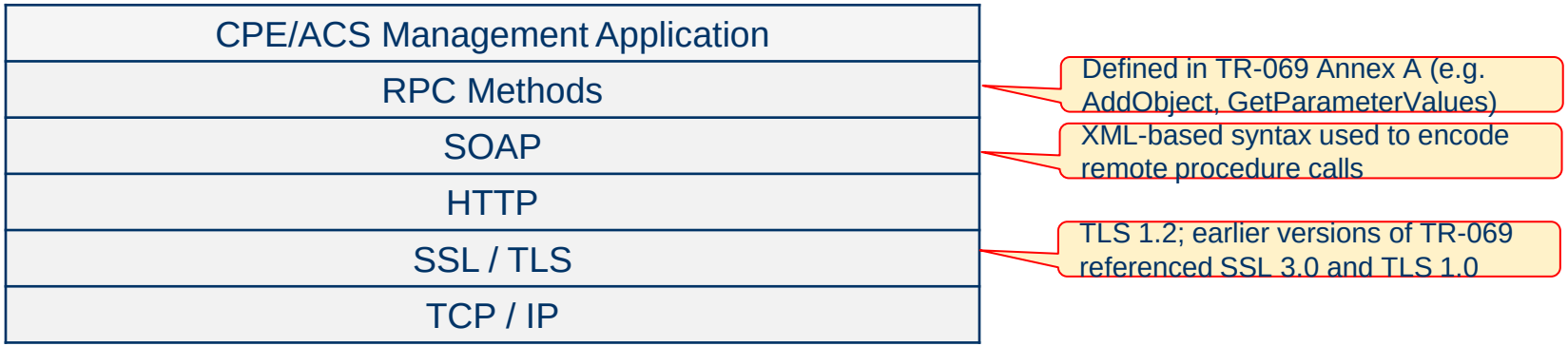
Managed Device

Generic Operation / Scenario	RPC Method (CWMP)
Get (“Device.DeviceInfo.”)	GetParameterValues
Create (“Device.NAT.PortMapping.”)	AddObject
Set (“Device.NAT.PortMapping.2.LeaseDuration”, 3600)	SetParameterValues
Delete (“Device.NAT.PortMapping.2.”)	DeleteObject
EnableNotification (“Device.Hosts.HostNumberOfEntries”)	SetParameterAttributes
Upgrade Firmware, Backup Configuration	Download, Upload
Manage Software Modules	ChangeDUState
Capability Discovery	GetRPCMethods, GetParameterNames
Reboot, Reset	Reboot, FactoryReset

Hierarchical object names

Note: CPE requests (ACS RPCs) not shown

Protocol Stack



- Management applications are an area of innovation
  - The application uses CWMP on the CPE/ACS; it is not part of the protocol
- Built on web protocols
  - Standards-based (e.g. TCP/IP, TLS 1.2, HTTP 1.1, SOAP 1.1)
  - Built-in security (e.g. TLS – transport layer security, HTTP shared secrets)
- Unconventional SOAP/HTTP binding
  - HTTP connections are initiated by the CPE but most SOAP requests are initiated by the ACS. This means a SOAP request from an ACS to a CPE is sent over an HTTP response.

Events and Notifications

BOOTSTRAP

BOOT

SCHEDULED

PERIODIC

CONNECTION REQUEST

VALUE CHANGE (Active or Passive)

TRANSFER COMPLETE

DIAGNOSTICS COMPLETE

More…

CWMP Protocol

- Current version is TR-069 Amendment 5 (CWMP version 1.4)
- Since inception, have added software module management and proxy support, expanding devices and objects that can be managed

Data Modelling

Information/Data Models

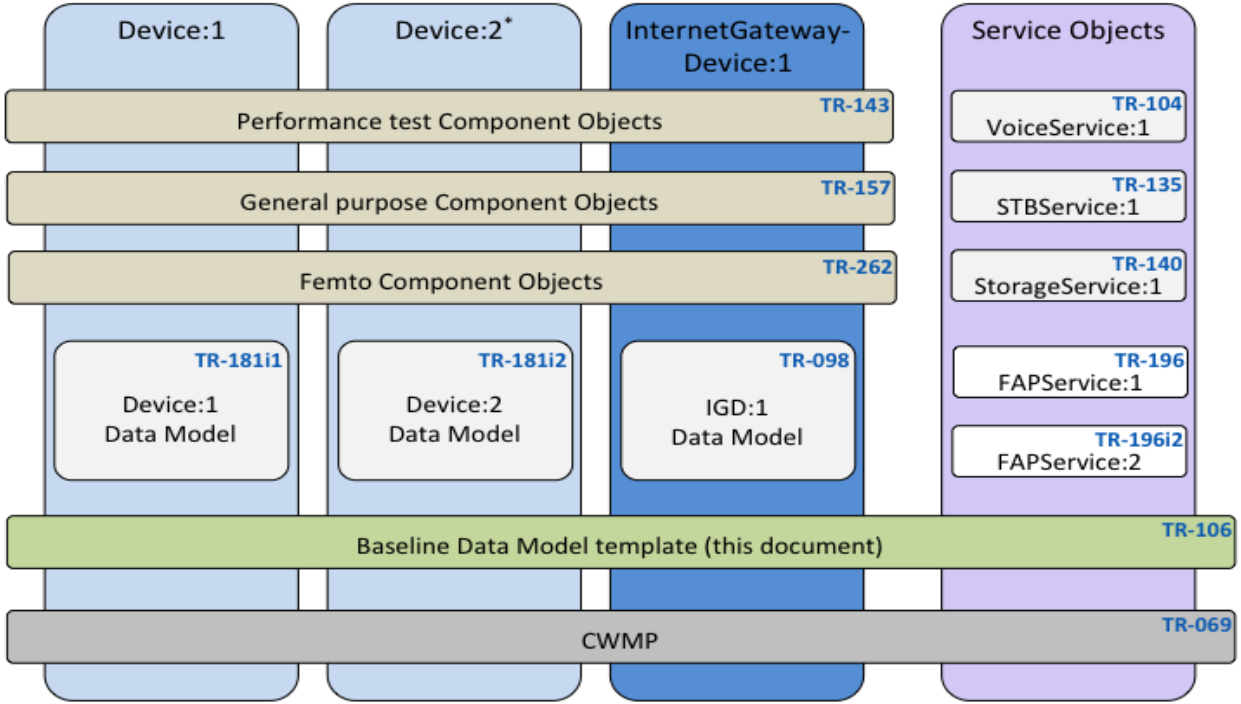
- Documents other than TR-069 specify the managed objects (data models) for specific types of devices and services
- These include *Root Data Models* and *Service Data Models*
- A CPE must support <u>one</u> Root Data Model:

  InternetGatewayDevice:1 (TR-098) – for RGs/NIDs
  Device:1 (TR-181 Issue 1) – for End Devices within LAN
  Device:2 (TR-181 Issue 2) – for either (next-gen data model)

- A CPE may also support some Service Data Models:

  VoiceService:1 (TR-104) – for VoIP
  STBService:1 (TR-135) – for Set-top box
  StorageService:1 (TR-140) – for NAS
  FAPService:1,2 (TR-196 Issue 1 & 2) – for Femto Cell

- Service Data Models define added functionality related to the delivery of specific services



* The Device:2 Data Model applies to all types of device, including Internet Gateway Devices (it includes everything that is in the IGD:1 data model)

Discovery/Device Definition

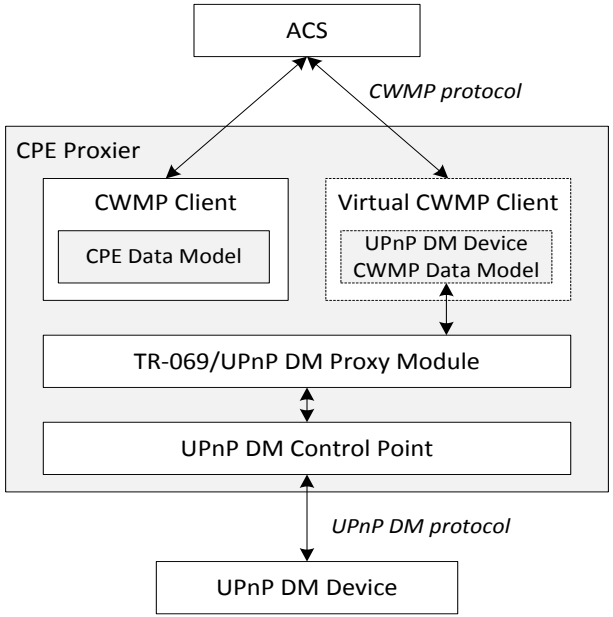
Device Type Definition

- ACS can learn device capabilities and state in several ways
- SupportedDataModel gives list of URLs to Device Type Definitions
- DT documents are xml documents that reference standard or vendor specific data models and describe what a device supports

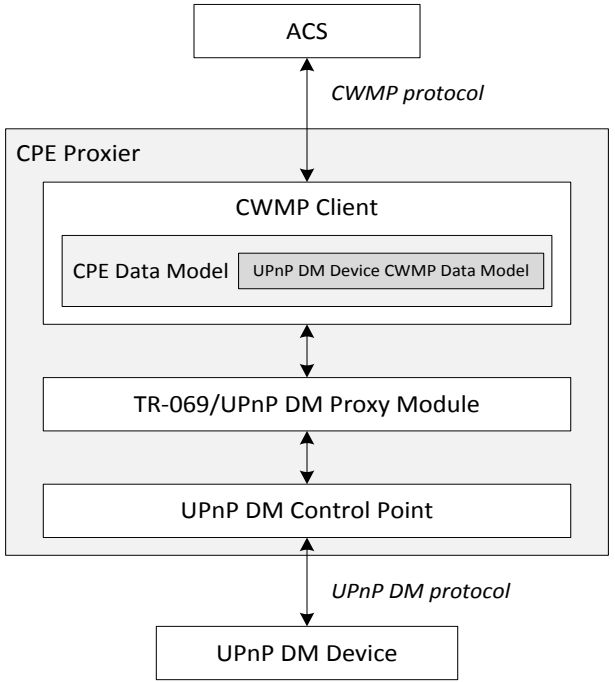
Proxy for non-CMWP devices

CWMP Proxy

- TR-069 and CWMP data models provide the ability to manage devices that do not support CWMP natively.
- Proxy support can be in the form of virtual devices (that have their own CWMP endpoint) or embedded devices (devices that add functions to the proxier’s data model.



Virtual Device



Embedded Device

broadband forum

A Look Down the Road

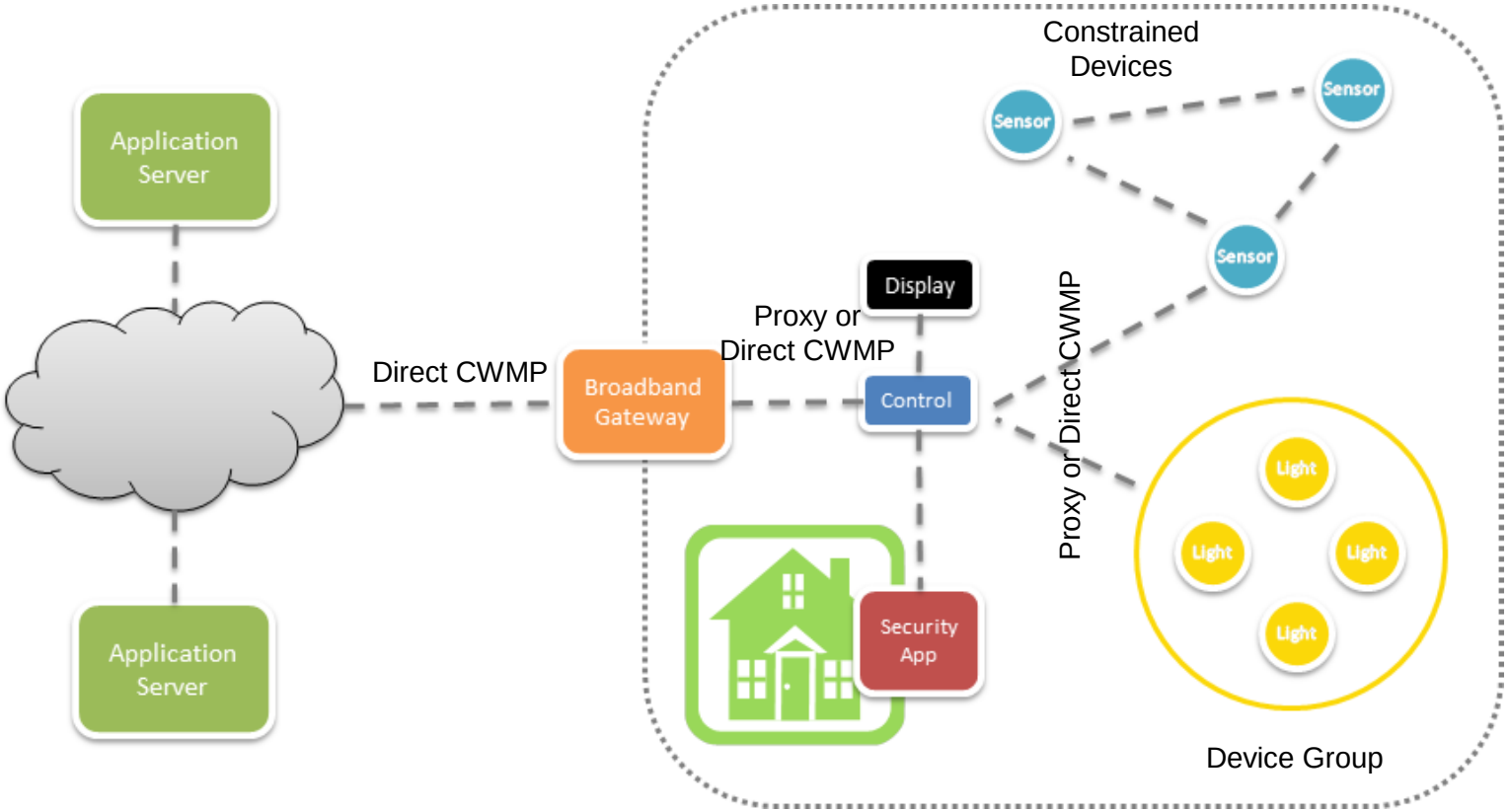
Future Work for Current Uses

- Separating protocol from transport: allowing use of TR-069 over protocols/channels other than HTTP
- Leveraging data model work in more areas
- Planning future versions of CMWP to apply to more types of devices with different constraints.

NFV (There, I said it)

Future Work for New Uses

- Addressing constrained devices – building a modular protocol so that implementers use what they need and not what they don’t
- Ability for multiple managers to address their own pieces of device/application functionality
- Addressing both management and control situations – endpoints can assume roles that are management-like to perform smart home functions



Using CWMP at a variety of interfaces