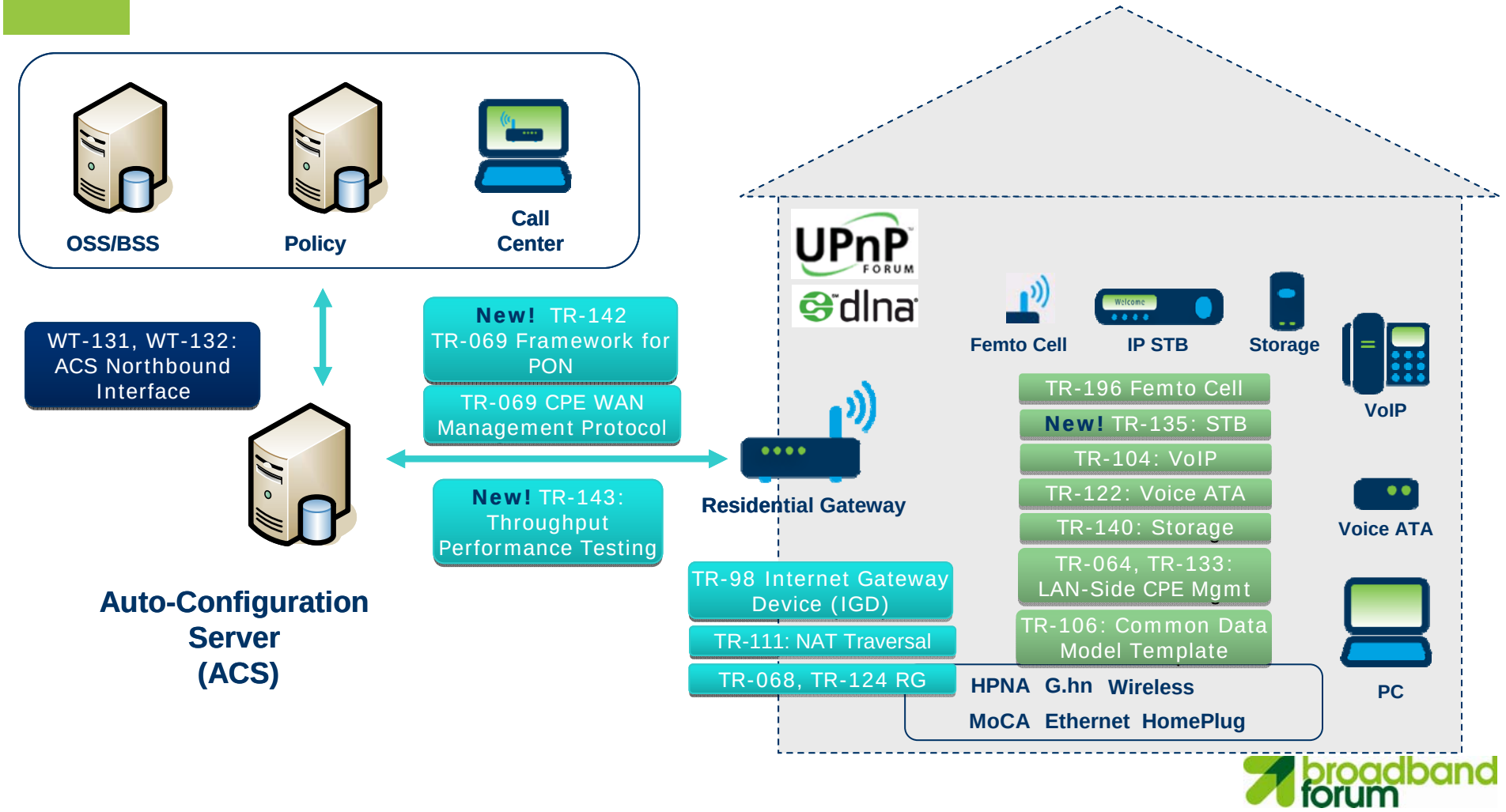
Broadband Forum - Remote Management Work

Why Standardize Management Protocols?

Manufacturers would be quite happy not to standardise	• Can define and use proprietary protocols • Ties customer into manufacturer's management systems AND managed devices, i.e. both ends of the protocol
Service Providers want choice	• Competition keeps the price down • So service providers push for standards: standards organizations define them • Manufacturers add vendor extensions to try to persuade the service providers to buy their products anyway
Standards support end-to-end management	• e.g. configure QoS settings on all devices involved in delivering a service

BroadbandHome™

Remote Management Framework

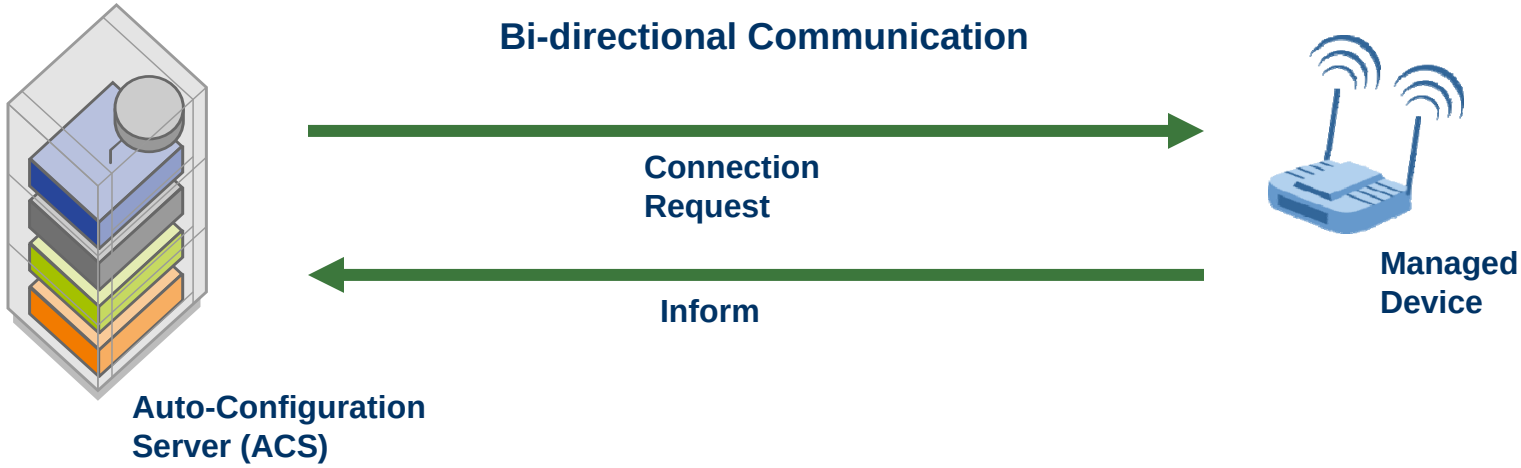


Summary of TR-069 (CWMP) Benefits

- Profitable and seamless service deployment
  - Reduce costs
  - Enable services
  - Improve customer experience
- Higher layer protocol – network (and device) agnostic
- Robust functionality
  - Granular device and service control
  - Flexible, policy-based management
- Well-defined extensibility mechanisms
  - New devices and services
  - Vendor differentiation
- Standard web technologies
  - Scalable
  - Secure
  - Widespread
- Applicable to full range of devices on home network
  - Annexes F (device/gateway association) and G (NAT traversal)

broadband forum

TR-069: CWMP Protocol



ACS Discovery

CWMP Connection Initiation

- Bootstrap – first connect to network
- Requested by ACS – Scheduled or immediately
- Asynchronous Notifications
  - Active – as soon as value changes
  - Passive – report value next inform

Device Control

- Get, Set Parameter Values and Attributes
- Add, Delete Objects
- Reboot, Reset to Factory Defaults
- Initiate Firmware Download
- Initiate diagnostic tests

broadband forum

Applying CWMP (TR-069) to Residential Gateway

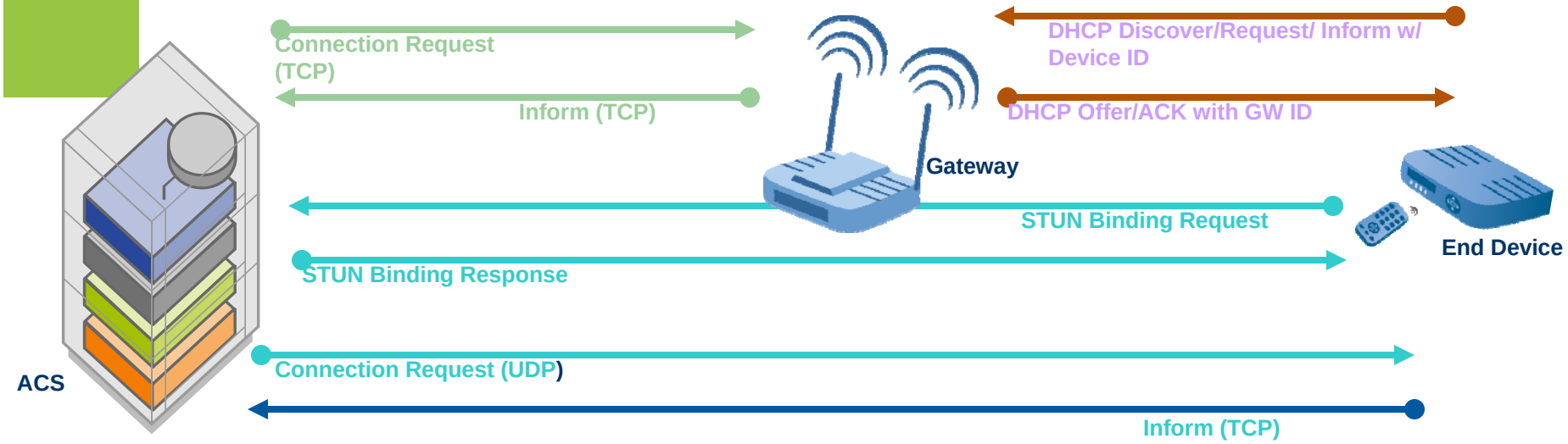
- Management Functions
  - Auto Configuration
  - Service Provisioning
  - Firmware Management
  - Diagnostics
  - Fault and Performance Monitoring
- Interdependent TRs
  - TR-098: Internet Gateway Device (IGD) Data Model
  - TR-106: Data model - defines general template for data model definition
  - TR-122: Base Requirements for Consumer-Oriented Analog Terminal Adapter Functionality
  - TR-124: Functional Requirements for Broadband Residential Gateway Devices
  - TR-142: Framework for TR-069 enabled PON devices
  - TR-143: Enabling Network Throughput Performance Tests and Statistical Monitoring

Applying CWMP (TR-069) to Home Network End Device

- Management Functions
  - Auto Configuration
  - Service Provisioning
  - Firmware Management
  - Diagnostics
  - Fault and Performance Monitoring
- Interdependent TRs
  - TR-064: LAN-Side DSL CPE Configuration
  - TR-068: Base Requirements for an ADSL Modem with Routing
  - TR-104: VoIP Provisioning data model
  - TR-111: Applying TR-069 to Remote Management of Home Networking Devices
  - TR-135: STB Data Model supporting IPTV
  - TR-140: Storage Data Model
  - TR-143: Enabling Network Throughput Performance Tests and Statistical Monitoring

broadband forum

Applying CWMP to Home Network End Device



Annex F – Device/Gateway Association

- End Device and Gateway exchange DeviceID via DHCP
  - Independent of device address assignment
- Populate relevant objects in data model
  - ManagedDevices table in GW
  - GatewayInfo object in end device
  - ACS can perform optional cross-check

STUN – Simple Traversal of UDP through NATs (RFC 3489)

Annex G – NAT traversal for ConnectionRequest

- ACS enables STUN client on device
- Device creates STUN binding with STUN server
  - CPE uses STUN protocol to determine NAT type and public address and communicates to STUN server
  - Uses STUN to maintain UDP binding through NAT gateway
- ACS sends UDP ConnectionRequest to address communicated to STUN server
- CPE responds w/ TCP Inform

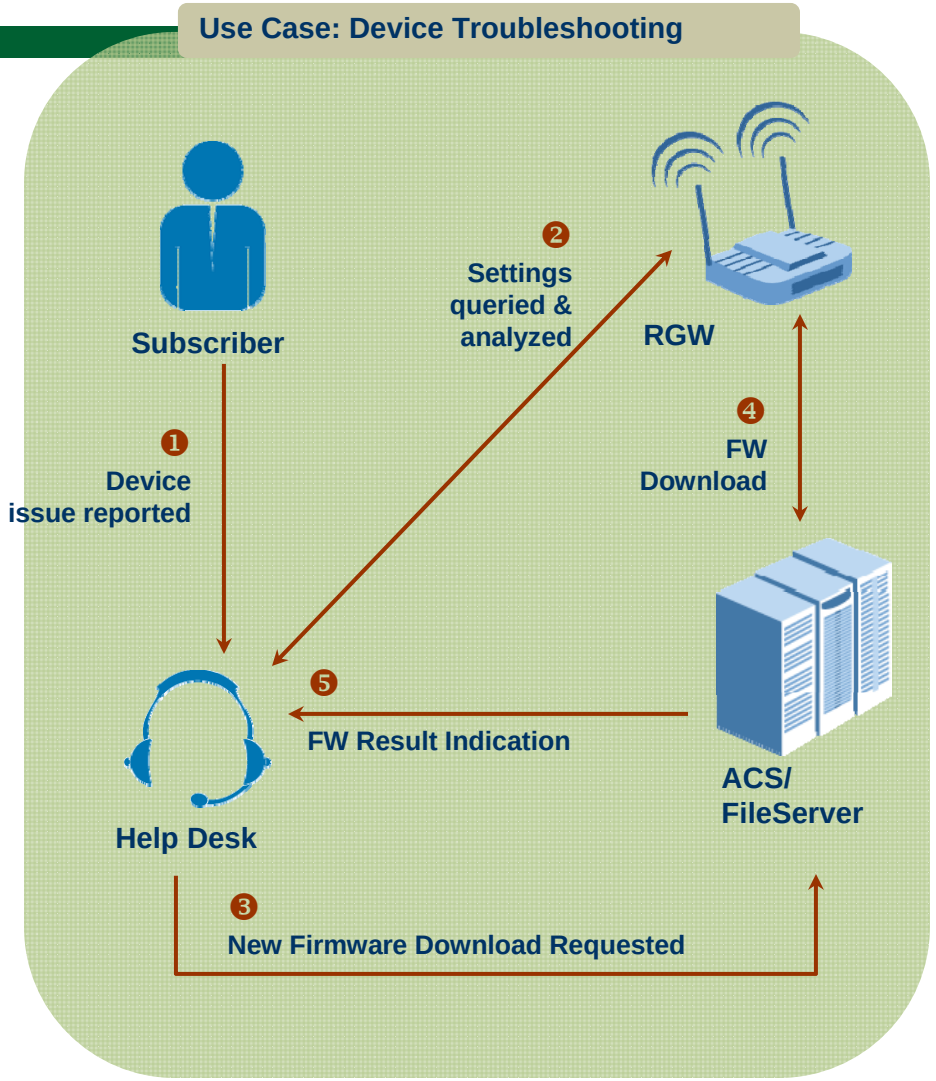
Supporting and/or Building on CWMP

- WT-123: TR-069 Conformance and Interoperability Test Plans
- WT-131: ACS Northbound Interface Requirements
- WT-148: CWMP Scalability Extensions
- WT-157: Component objects for CWMP
- WT-196: Femto Access Point Service Data Model
- PD-174: Management of Non TR-069 Devices
- PD-193: IPv6 Updates to TR-069 Related TRs
- PD-194: Software Module Management using TR-069
- PD-199: TR-069 Bulk Management

broadband forum

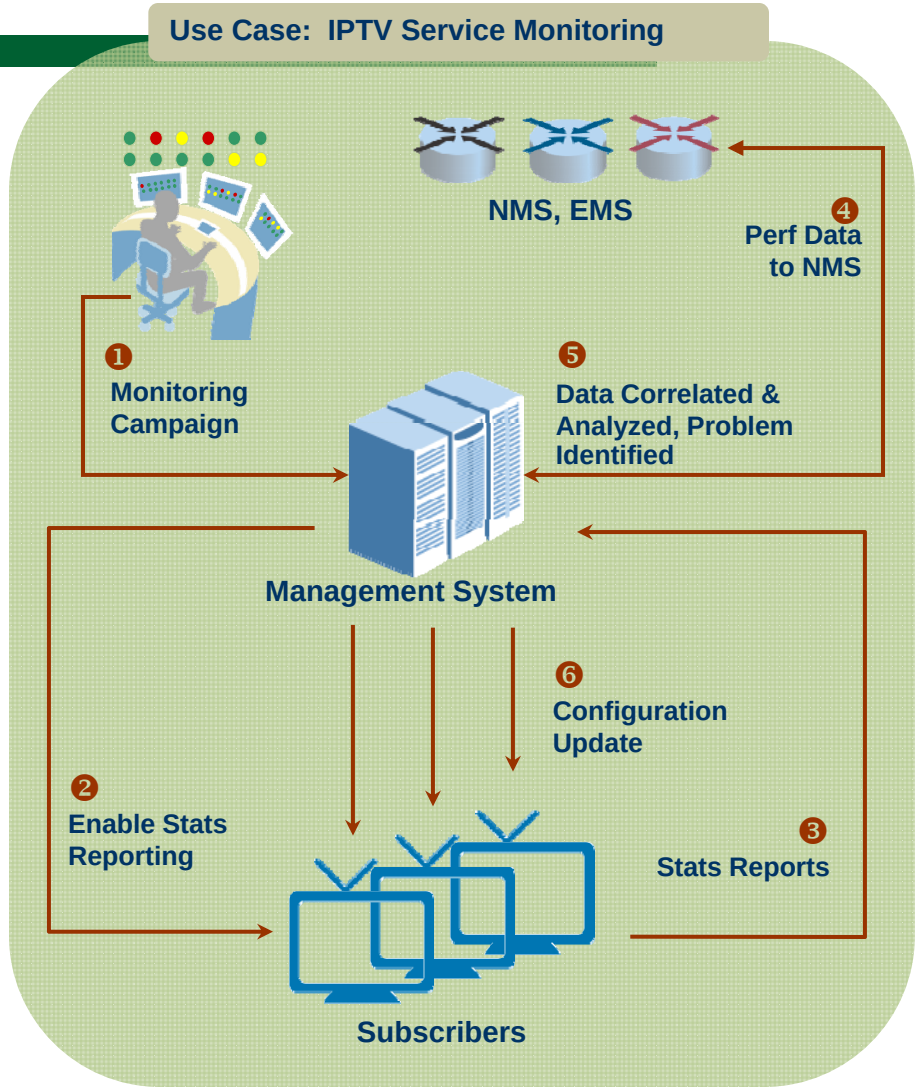
Service Support

- Features
  - Subscriber calls Service Provider call center to report device problem
  - Through the ACS, CSR can query device settings
    - CSR notes that firmware out of date, contains known bug
    - Requests ACS to initiate file download/upgrade
  - RGW reports to ACS when download complete; ACS indicates results to Help Desk
    - ACS could also change configuration settings as appropriate
    - Firmware upgrades could also be managed proactively
- Benefits
  - Reduces call center escalation costs
  - Reduces AHT, increases FCR
  - Streamlines CSR processes
  - Reduces RMA, equipment upgrade costs
  - Enables new device capabilities



Service Monitoring

- Performance Monitoring
  - Service Provider enables monitoring for subset of STBs
  - Determines which statistics to collect and report interval
  - Adjust device configuration as appropriate
    - IGMP
    - QoS
    - May also require adjustment to other network/IPTV delivery systems
- Benefits
  - Service provider control over statistics collected
    - Focus on key metrics, amount of data, reporting traffic
  - Proactive discovery of service issues
  - More intelligent network planning and ongoing adjustment



SDOs Using/referencing TR-069 CWMP for Service Provider Management

- 3GPP
- ATIS IIF
- DVB (Digital Video Broadcast) IPI
- ETSI TS 183065
- Femto Forum
- FSAN
- Home Gateway Initiative (HGI)
- ITU-T SG HN / IPTV
- Open IPTV Forum
- Universal Plug and Play (UPnP)
- WiMax Forum

broadband forum

Relationship of TR-069 to Other Home Network Management Protocols

WAN Versus LAN Protocols

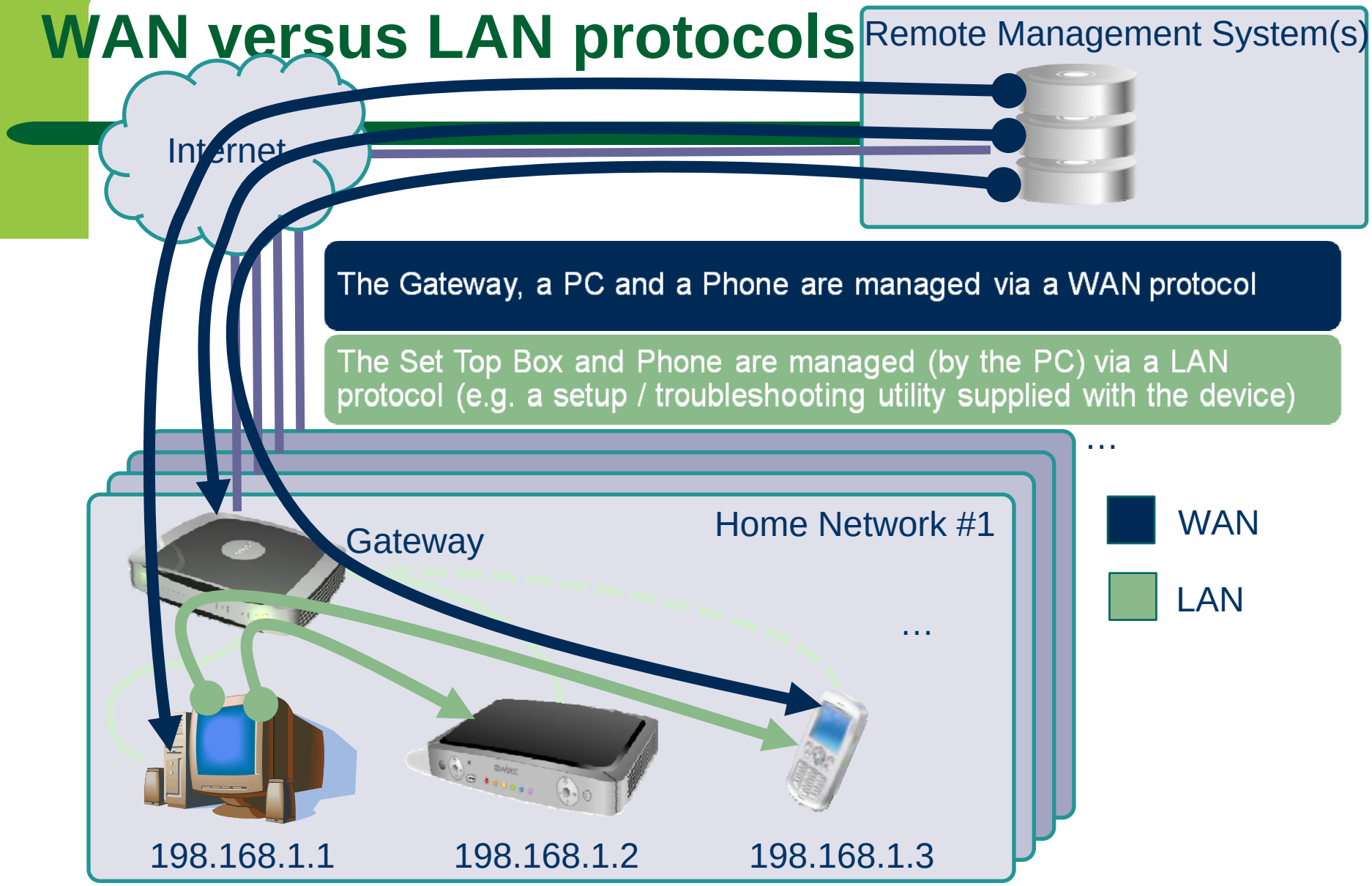
The protocols mentioned so far are WAN management protocols

- A WAN management server manages a LAN device
- Some protocols are point-to-point (1-1), e.g. TR-069
- LAN devices do not use the protocol to communicate with each other (it's not designed for that)
- Some protocols are associated (in the public mind) with a particular access technology, e.g. TR-069 was defined by the DSL (now Broadband) Forum to be independent of access technology

Contrast with LAN management protocols

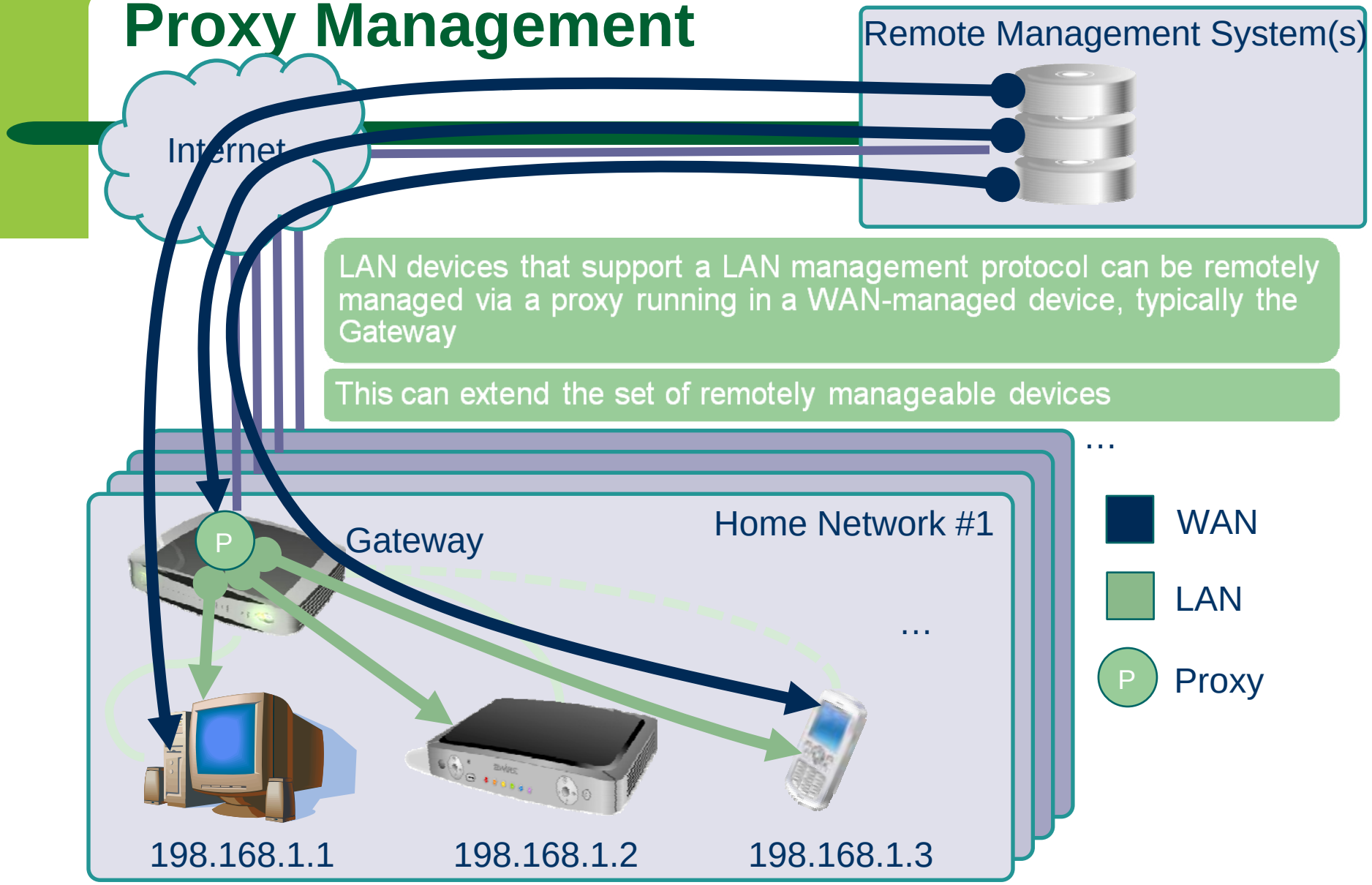
- A LAN device manages another LAN device
- Protocols are typically many-to-one (N-1), e.g. UPnP
- Such protocols are guaranteed neutral to the access technology

WAN versus LAN protocols



broadband forum

Proxy Management



Home Network Management Protocols Summary

LAN management protocols are independent of access technology and are more likely than WAN management protocols to be supported by retail devices

Remotely managed devices can, via management proxies, take advantage of such LAN management protocols, thereby increasing the information about the home network that can be made available to an RMS

UPnP Device Management is one such LAN management protocol that is being standardized

Do I hear privacy concerns? This is a double-edged sword. Do I want to hide the fact that there's a media stream from device A to device B? If I hide this fact, how can it be fixed when it's not working? But by all means hide the details of what is being streamed

UPnP As A LAN Management Protocol – Basis for TR-064

UPnP is both an architecture (UDA) and a set of device-specific APIs (DCPs)

- UDA = UPnP Device Architecture
- DCP = Device Control Protocol

Most existing DCPs are (as the name "DCP" suggests) aimed at device control, e.g.

- UPnP AV: MediaServer and MediaRenderer
- UPnP QoS: Quality of Service

But nothing in the UDA prevents its use for management, e.g.

- UPnP DM: Device Management

There is a better chance that retail devices will support UPnP DM than (say) TR-069

- UPnP is an essential part of the DLNA (Digital Living Network Alliance) guidelines
- UPnP is seen as "neutral"… it's completely independent of the access technology

Other Relevant Home Network Protocols Utilized in TRs or WTs

DHCP	the DHCP server knows a lot about the home network so, if it's remotely managed, it can make that information available to the RMS
Layer 2 media-specific	Layer 2 interfaces embedded into remotely managed devices, e.g. WiFi access points, are typically aware of associated devices, and may also be able to provide statistics or even perform diagnostic tests
LLTD	Link Layer Topology Discovery; part of Windows Rally, it allows discovery of home network topology and related device-specific information; could be useful if a remotely managed device includes an LLTD mapper
LLDP	Link Layer Discovery Protocol; standardized as IEEE 802.1AB so potentially attractive, but currently seems more aimed at the access network and the enterprise
Multicast discovery	mDNS/DNS-SD and SSDP both provide Multicast announcement of services offered by home network devices; broadly speaking, mDNS/DNS-SD is the Apple approach, whereas SSDP is the UPnP discovery protocol
Proprietary	There are many proprietary protocols; if a remotely managed device supports such a protocol it can use it to discover and pass information to the RMS

Summary

- BroadbandHome™ specifications establishes a framework for
  - Auto Configuration
  - Service Provisioning
  - Firmware Management
  - Diagnostics
  - Fault and Performance Monitoring
- BroadbandSuite™ provides WAN management and LAN management of
  - Gateways
  - Home networked end devices
- Leverages existing standards
- Focused on improving customer experience across all managed services

broadband forum

Questions?

Working Together

www.broadband-forum.org