The TR-069 protocol and its ability to manage QoS policies on the CPE

William Lupton

2Wire, Inc

(representing the DSL Forum)

Outline

- DSLHome initiative
- TR-069 and related standards
  - Role within DSL Forum auto-configuration architecture
  - TR-069 protocol (CWMP)
  - TR-069 data models
- TR-069 and QoS management
  - TR-098 QoS data model
  - TR-069 for configuring QoS policy
  - TR-069 for monitoring QoS performance
- Conclusions

DSLHome Initiative

DSLHome Initiative

- The DSL Forum launched the DSLHome initiative in June 2003
  - To tackle the CPE management problem
  - To enable new services for end users
- Participation by CPE and chipset vendors, operators, service providers, equipment vendors, and application providers
- The DSLHome remote management protocol (TR-069 or CWMP) is **access technology agnostic**

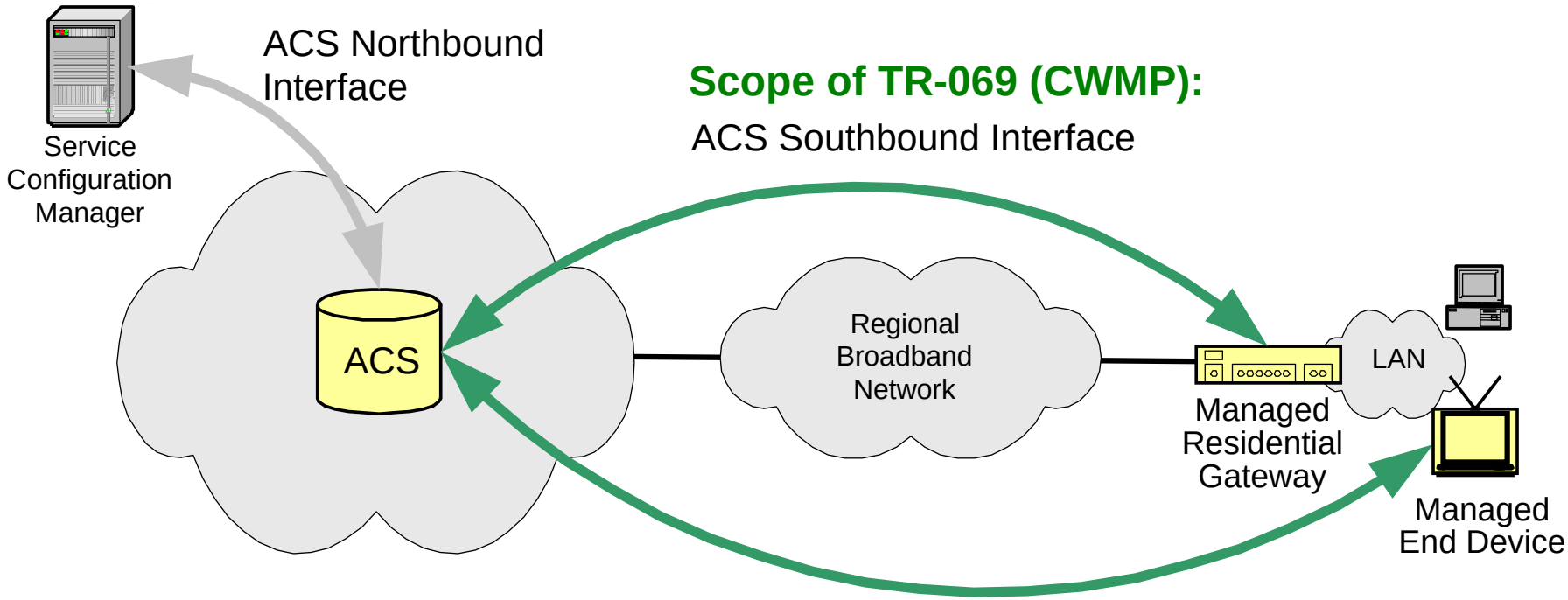
TR-069 and Related Standards

Role Within Auto-Config Architecture

- TR-046 defines a three layer DSL Forum auto-configuration architecture
  - TR-062: ATM layer auto-configuration
  - TR-044: IP layer auto-configuration
  - **TR-069**: complex service auto-configuration
- TR-069 is **access technology agnostic**
  - WAN connectivity must already have been established
  - Is defined by the DSL Forum but is not specific to DSL deployments
    - At least one DOCSIS TR-069 deployment is expected in 2006
    - Also note *WT-142: Framework for TR-069 enabled PON devices*

Scope of TR-069 (CWMP)

ITU-T



ACS: Auto-Configuration Server
CPE: Customer Premises Equipment
CWMP: CPE WAN Management Protocol

TR-069 Functional Components

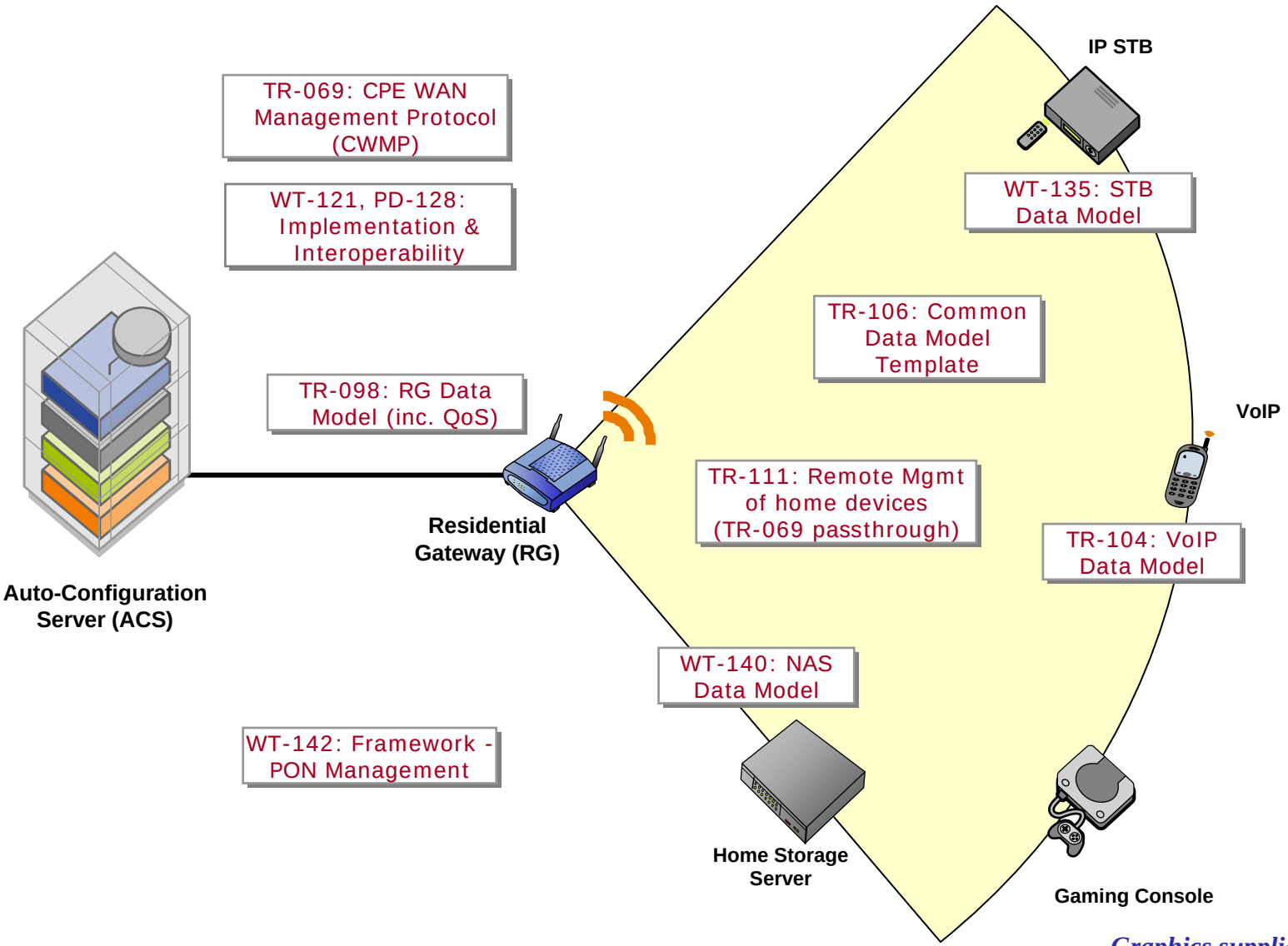
- Auto-configuration and dynamic service provisioning
  - Initial CPE configuration
  - Re-provisioning at any subsequent time
  - Vendor-specific configurations
- Software / firmware management
  - File download initiation
  - Notification of the success or failure of a file download
- Status and performance monitoring
- Dynamic notifications and log files
- Diagnostics

TR-069 and End Devices

- TR-069 can be used for managing
  - Residential Gateways (RG)
  - End Devices (ED)
- Two approaches
  - RG acts as proxy for the ED
  - ED is managed directly
- TR-111 defines extra rules that allow
  - RG to discover TR-069 EDs within the LAN
  - ACS to contact TR-069 EDs even for non-TR-069 RGs (uses STUN; RFC 3489)

TR-069 Family

ITU-T



Graphics supplied by Motive

CWMP Protocol Stack

ITU-T

Layer (top down)	Description
CWMP Application	CWMP client (CPE) or server (ACS). Sessions are always initiated by the CPE (although the ACS can request that a session be created).
RPC Methods	CWMP defines standard Remote Procedure Call (RPC) methods. The first method of a session is always a CPE → ACS "Inform" method. Other methods manage objects within the hierarchical data model.
SOAP	SOAP 1.1 (Simple Object Access Protocol). Describes how to use XML to invoke RPC Methods.
HTTP	HTTP 1.1 (Hypertext Transfer Protocol).
SSL/TLS	SSL 3.0 (Secure Socket Layer) or TLS 1.0 (Transport Layer Security).
TCP/IP	TCP over IPv4.

CWMP Data Model

- CPE configuration, status, statistics and diagnostics are described using hierarchical data models
  - TR-106: common data model template
  - TR-098: RG data model (including QoS)
  - TR-104: VoIP data model
  - WT-135, WT-140, *etc.* (work in progress, new work)
- For example
  - **Device.ManagementServer.URL** is the URL on which a CPE should contact the ACS
- RPC methods use these hierarchical names

Some CWMP RPC Methods

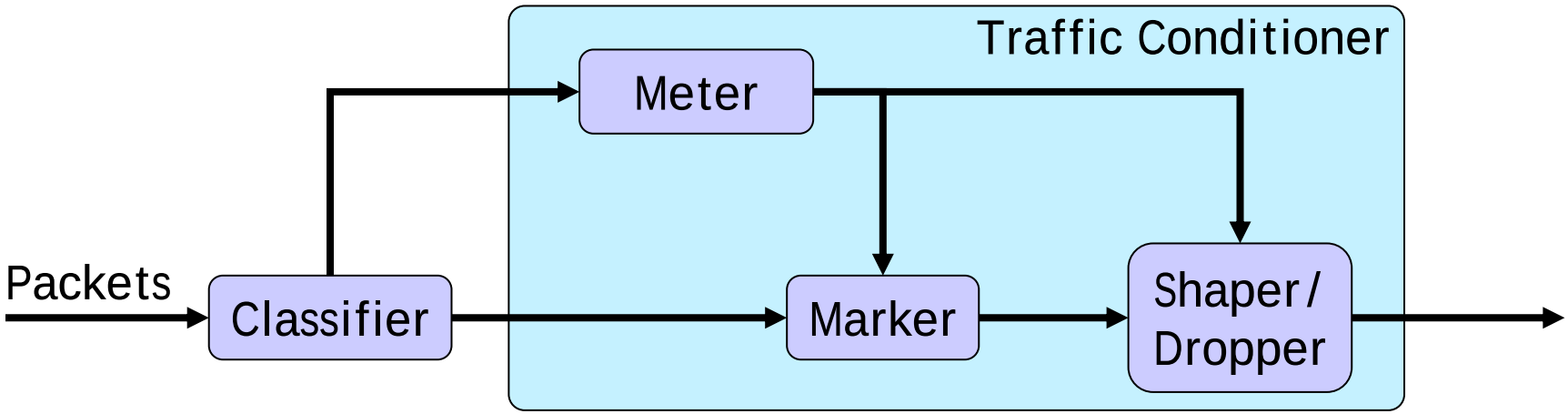
ITU-T

Method	Direction	Description
Inform	CPE→ACS	Initiates a CWMP session.
GetRPC Methods	CPE→ACS ACS→CPE	Returns a list of supported RPC Methods (**which may include vendor-specific ones**).
Get Parameter Names	ACS→CPE	Returns a list of supported objects and parameters (**which may include vendor-specific ones**).
Set/Get Parameter Values	ACS→CPE	Sets or gets parameter values (can get sub-hierarchies in a single call).
Set/Get Parameter Attributes	ACS→CPE	Sets or gets parameter attributes, e.g. enabling or disabling notifications, or managing access lists.
Add/Delete Object	ACS→CPE	Adds or deletes an object within the data model, e.g. creates a QoS classification rule.
Download	ACS→CPE	Initiates download of a file, e.g. new firmware.

TR-069 and QoS Management

RFC 2475 (Diffserv) QoS Model

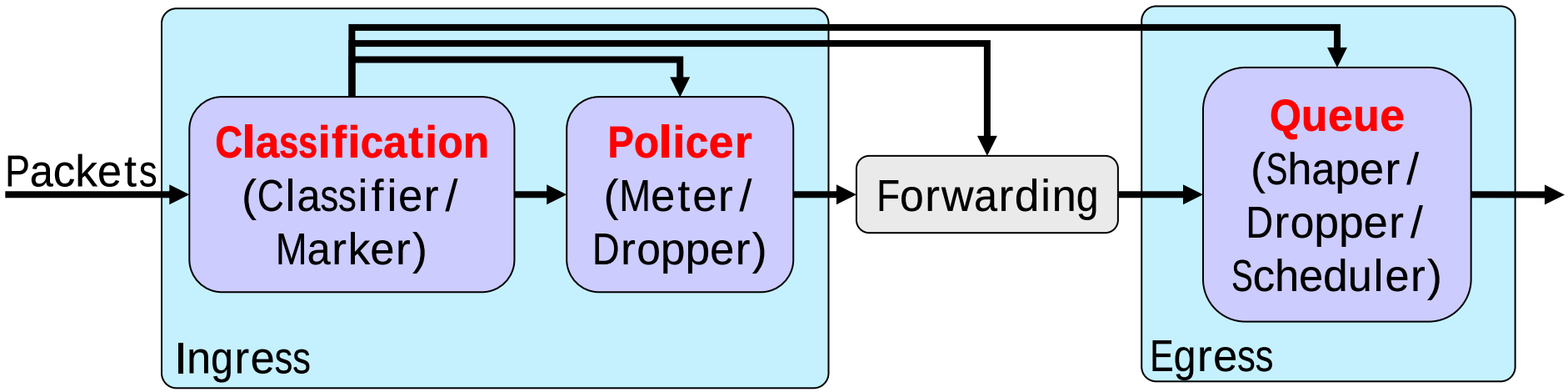
- TR-098 QoS data model is based on the RFC 2475 packet classification and traffic conditioning model



RFC 2475: Logical View of a Packet Classifier and Traffic Conditioner

TR-098 QoS Data Model

- Top-level **Classification**, **Policer** and **Queue** tables define the functionality shown below
- Additional **Flow** and **App** tables (not shown) allow application-aware classification



How RFC 2475 components are modelled in TR-098

Configuring QoS Policy

- So the RG's QoS policy can be configured
- But what about managed EDs?
  - The ED data model, e.g. TR-104 for a VoIP phone or WT-135 for an STB, may allow egress priority markings to be configured
- And what about unmanaged EDs?
  - Egress priority markings can be determined based on service class, e.g. "Upstream Voice", "Upstream Video" (but there are no standard mappings)
- And what about unmanaged LAN devices in general?
  - Can rely on "good citizenship", i.e. on honoring layer 2 / 3 priority markings
- In the longer term, the RG, and both managed and unmanaged LAN devices, may support a LAN QoS signalling protocol such as UPnP QoS

Monitoring QoS Performance

ITU-T

- Currently, not many status / statistics / diagnostics parameters are available, e.g.
  - **Policer**: packet and byte counts
  - **Queue**: current buffer length
- Likely to see DSL Forum contributions in this area
  - Will become available in new versions of the data model
  - In the meantime, vendors and organisations (e.g. HGI) can define extensions
  - Such extensions need not be brought to the DSL Forum for standardisation…
  - …but standardisation should be encouraged, since it promotes interoperability

Conclusions

Conclusions

ITU-T

- TR-069 (CWMP)
  - Extensible and flexible management protocol
  - Access technology agnostic
  - Active promotion of TR-069 for access technologies other than DSL, e.g. cable/DOCSIS, fibre/PON (WT-142)
  - Many companies (CPE, ACS, middleware, chipset vendors) and operators have adopted TR-069
  - Other bodies are adopting TR-069: ITU-T SG16 Q21, HGI, …
- TR-098 (RG data model)
  - Rich modelling of RG QoS policy
  - Adopted for HGI QoS
    - No extensions needed in order to meet HGI requirements

Questions

ITU-T

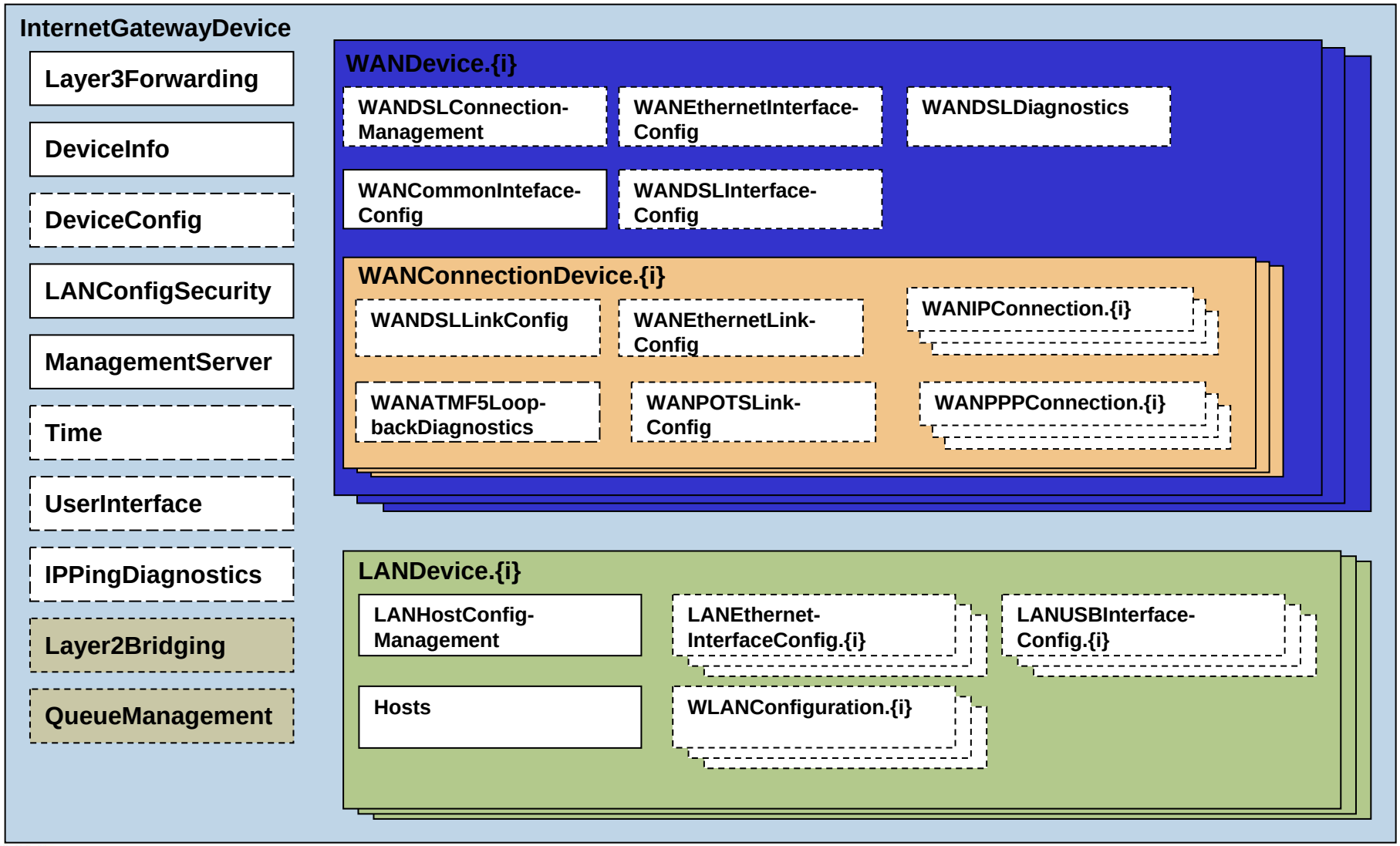
Thank you

Questions?

Backup Material

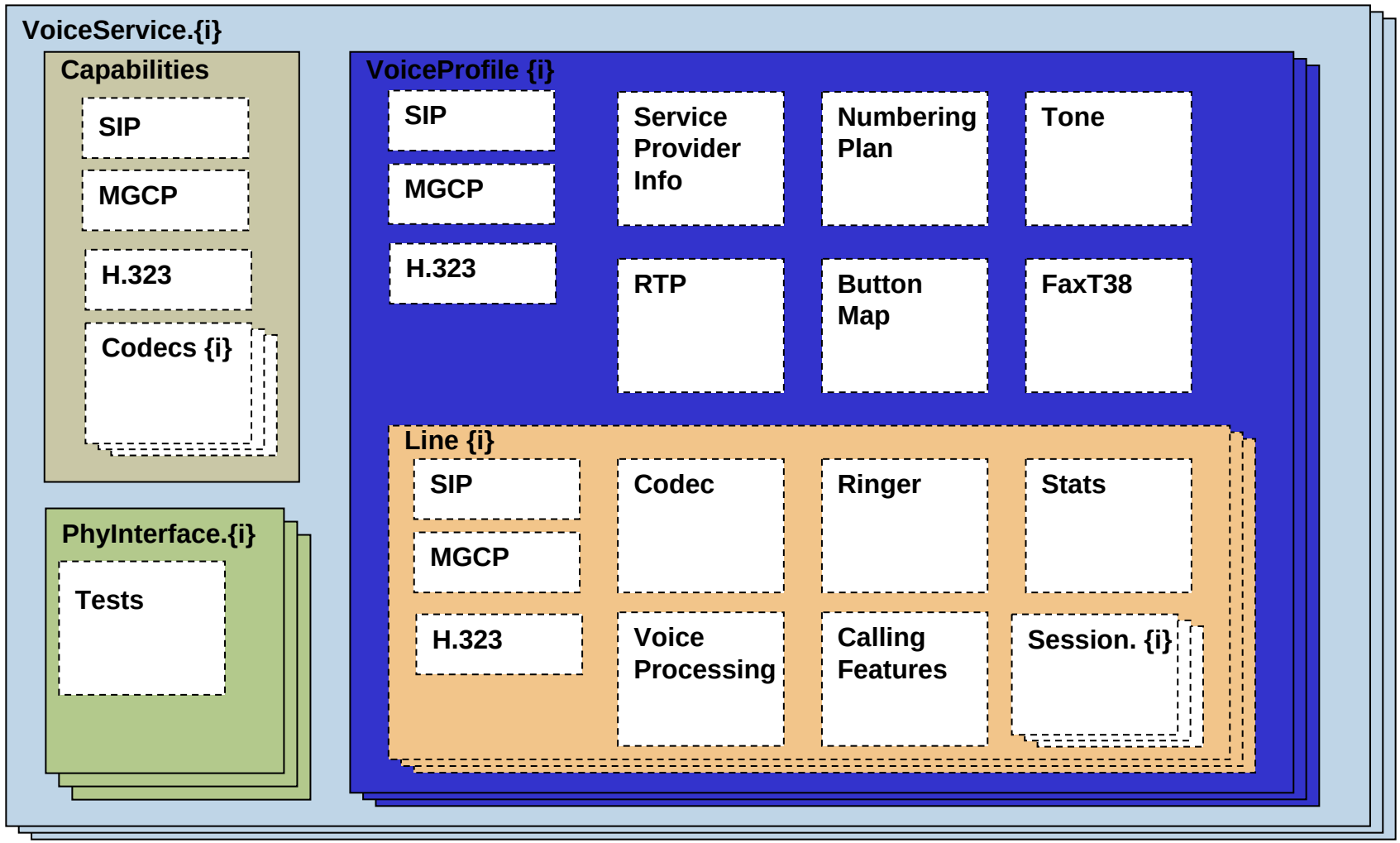
RG Data Model

ITU-T



VoIP Data Model

ITU-T



Graphics supplied by Motive

QoS Data Model: Classification

- All packets are (conceptually) classified immediately after ingress
  - Classification rules are ordered, and are applied in order until a match is found
  - Each rule is the logical AND of one or more criteria
  - Criteria can be at layer 1 (e.g. physical port), layer 2 (e.g. VLAN ID, VPI/VCI, MAC address, priority), layer 3 (e.g. IP address, packet length, DSCP value), layer 4 (e.g. port), or higher layers (which require application-specific logic)
  - There are also some special criteria, e.g. the value of the DHCP vendor class (option 60)
  - Some criteria, e.g. MAC and IP addresses, can be masked
  - All criteria can be negated
- Classification results are layer 2 /3 priority markings, **Policer** instance, forwarding policy, and **Queue** instance

QoS Data Model: Policer

- All packets are (conceptually) policed after being classified
  - The Policer instance number is one of the classification results
- Each Policer instance specifies Meter and Dropper functionality
  - Includes rate requirements and behaviour when these requirements are exceeded

QoS Data Model: Queue

- All packets are queued after the forwarding decision has been made (i.e. once the egress interface is known)
  - The Queue instance number is one of the classification results
  - Queues are assumed to be instantiated on all the egress interfaces for which they are needed
- Each Queue instance specifies Shaper, Dropper and Scheduler functionality