Gateway Agent - First Amendment to the High Level Design Document

Scope

The Gateway Agent HLD through update 1 assumes that only the Control App, while connected to the proximal network, can initiate new cloud services. Typically a Control App is installed in an AllJoyn device, such as a Smart Phone. Once installed the Control App arranges for installation of the appropriate Connector App in the gateway node for its cloud service. It also enables the user to create a remote profile for which of their AllJoyn devices will connect to the cloud service. This approach is well matched for consumer/retail products where the cloud services are initiated with the installation of a Control App (a mobile app from a typically downloaded from a mobile app store).

However, this services model is not well matched for managed Services Providers who offer home automation, security, entertainment and similar services that must be remotely and securely provisioned. Additionally, today's connected products often come with a bundled cloud service, placing the product's provider in the role of a Services Provider. For Services Providers, it is critical that everything work automatically when the new product is plugged in for the first time. It is also important to most Services Providers to be able to limit what changes their customer can make to their their services gateway or hub, that will run the Gateway Agent.

The Services Provider also needs access and full control of the gateway or hub after installation, both to provide updates and to provide customer support. To handle this, both new services and the remote profile need to be fully manageable by the Services Provider. The Connector App must also be able to be initially installed, updated and deactivated/removed by the Services Provider. This First Amendment to the Gateway Agent HLD defines a new remote management mode called "Service Provider Mode." The features, requirements and high level architecture are included in this Amendment. The non-Service Provider Mode is now called "Consumer Mode" and remains as defined in the HLD.

Service Provider Mode - Remote Provisioning for Services Providers

The Service Provider Mode implements remote provisioning for cloud services for AllJoyn devices via the Gateway Agent management application. The Service Provider Mode provides the features required for directly provisioning the device running the Gateway Agent remotely and securely, and acts much like a machine driven Control App to provision the cloud services. The Service Provider Mode is implemented using secure and proven remote management based on the TR-069 family of standards from Broadband Forum.

Service Provider Mode Remote Management Requirements

1. Automatically register a new Gateway Agent device and the subscriber (user) for the cloud services when it is installed
2. At the time of new services activation enable installation of a new Connector App remotely (from outside of the proximal network) if it is required for the new cloud services.
3. Multiple Connector Apps are supported in Service Provider Mode. Each can be remotely managed, even if originally installed by the subscriber from a Control App.
4. Add the capability to for the Services Provider to block the customer from installing or modifying Connector Apps using the Control App of the non-Enterprise Consumer Mode.
5. The Service Provider Mode utilizes the same Connector App requirements as the Consumer mode.
   - This is key to enabling either type of services deployment to be available without requiring modification of the Connector App.
   - Affinegy is contributing a Connector App that supports the Gateway Agent HLD in either Consumer Mode or Service Provider Mode. This is based on XMPP and will be separately documented as a reference sample Connector App. This XMPP connector provides its own remote access and NAT traversal, which is separate from the Service Provider Mode management.
6. A Connector App that is installed through the Service Provider Mode will normally be locked from modification by a Control App in Consumer Mode.
7. Profiles for Service Provider Mode may optionally be synchronized with the remote management server.
8. NAT traversal to enable remote management shall be supported when the gateway device that is running the Gateway Agent is connected behind a NAT firewall. This will be performed using either the TR–069 UDP based STUN method, or the XMPP method of TR–069a5. Both methods will be available however the first release contribution will be based on the STUN method that is mature and proven.
9. Service Provider Mode provides additional optional remote management features for the Services Provider. These relate primarily to the management of the hardware device that is running the Gateway Agent application.
   - Ability to update/replace the firmware image of the gateway device
   - Ability to transfer remote management control to a new service provider domain
   - Ability to diagnose and manage various settings of the gateway device that is running the Gateway Agent

Note - this first release for Service Provider Mode does not include direct TR–069 based proxy management of the AllJoyn LAN devices. This would overlap with the features of the Connector App (for example the XMPP Connector) that is the basis for remote messaging and management of the AllJoyn devices. However the foundation is provided to add TR-069 proxy management when desired for provisioning of services to AllJoyn LAN devices (such as configuring individual IP cameras for their video server entries, etc).

Service Provider Mode Implementation Architecture

A very high level of security is critical for the Service Provider Mode. Services that are delivered in this fashion usually are part of a paid service subscription that includes contractual service quality agreements. The remote management technology for Service Provider Mode is based on the Broadband Forum TR–069 family of standards. In particular TR–069 amendment 5 (the core remote management protocol and NAT traversal), and TR–157 which covers software module installation and management. The details of these standards are included here only by reference.

Security implications - in this services provider model, the operator has total control of the gateway hardware device, including the ability to totally replace all firmware in the device consistent with their own agreement with their subscribers. The roles of the Connector App and the Control App are the same as in the HLD with the same security restrictions when used by the subscriber (user). With the Service Provider Mode, however the TR–069 management can override any other setting in the Gateway, including those made the their subcriber. The Services Provider acts as a super administrator for the device running the Gateway Agent in the Service Provider Mode.

Affinegy is contributing its TR–069 embedded client for Linux and integrated into OpenWRT for this project which implements these functions. Affinegy is further providing developer access to its hosted TR–069 ACS remote management server, to enable easy product and services implementation using these libraries. Since this implementation for Service Provider Mode fully complies with the Broadband Forum standards - products that adopt these libraries will support any TR–069 ACS server that supports the required standards.

Architecture Diagram

The diagram shows the new software components for Service Provider Mode that are added to enable the TR–069 remote management of connector apps and the related cloud profiles. This diagram includes the same components as in the Non-Enterprise / Consumer mode of the HLD - with the new components and new remote server added.

Service Provider Mode Architecture
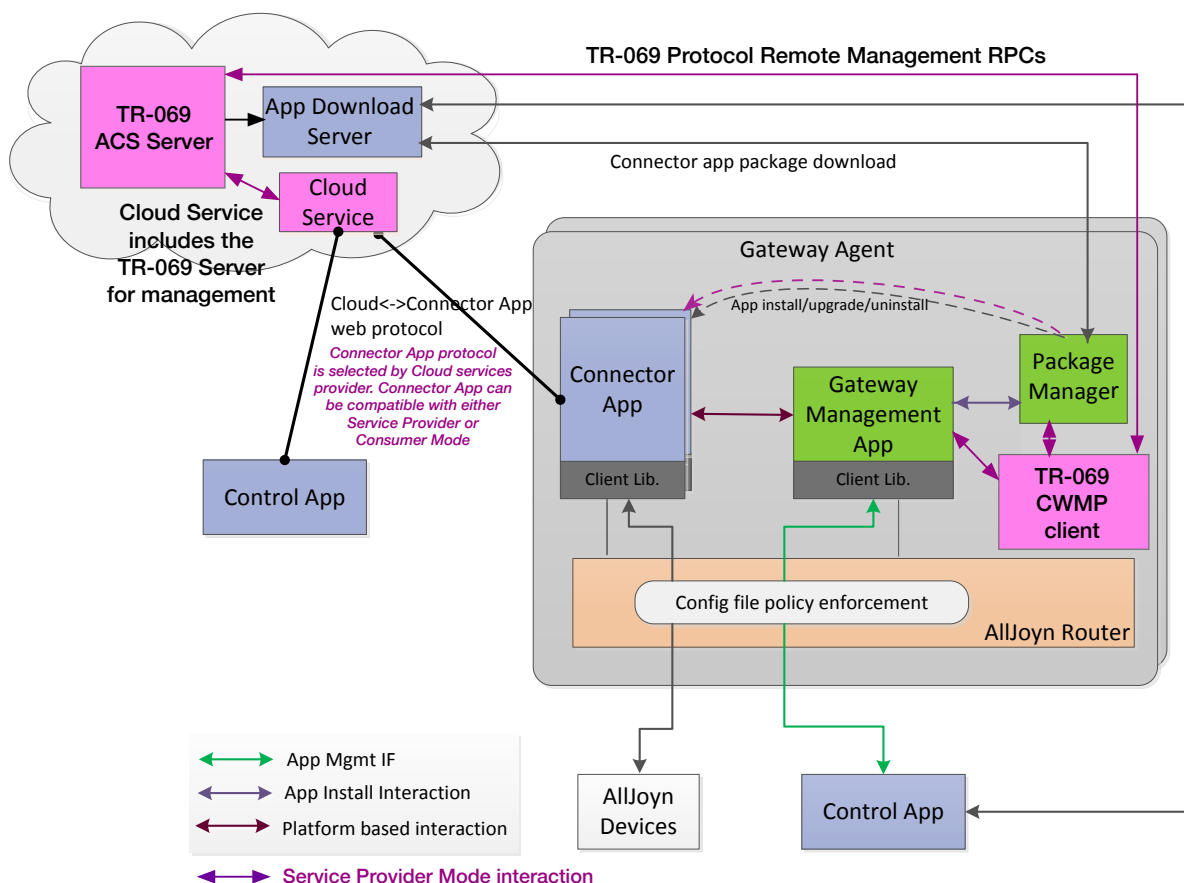
API and Specification Impacts for the Gateway Agent HLD

The Service Provider Mode is implemented using standard specified requirements of the TR-069 and TR-157 standards as implemented and documented in Affinegy's client code contributions. The detailed principals of operation are specified there. Links to these standards are provided below. In principal, the APIs and requirements of the Gateway Agent for Consumer Mode are not changed. However, there are specific interface API needs between the TR-069 embedded CWMP client to integrate the mode switch to in the Gateway Agent application to support the new Service Provider Mode. These have no external access except via the TR-069 remote commands to the embedded TR-069 client. Essentially only a mode switch parameter is needed, however this may touch several places in the current code which is left for detailed review and discussion for implementation within the project team.

Broadband Forum Standards References

The main protocol standard for TR-069

>   http://www.broadband-forum.org/technical/download/TR-069_Amendment-5.pdf

The standard for software module management:

>   http://www.broadband-forum.org/technical/download/TR-157_Amendment-5.pdf