Lecture 7

Smart home:

Home Gateway middleware initiative

The context

- The SOHO (small office, home office) network: it has a single Internet connection, transfers files, there is a printer/scanner, and has a wireless router to allow wireless devices (laptop, phone, tablet) connectivity within appropriate range.

- High-speed connections prompted a strong desire among consumers to do much more with their home networks:
  - include store and stream media;
  - integrate TVs as the 'hub' from which to access data and entertainment, use mobile phones to access or transport media and many more;
  - BUT, the reality for most consumers is that they don't have the skills to install and manage a network of this complexity.

The Home Gateway Initiative

- December 2004: 9 telecom operators founded HGI to work together for a common home gateway specification.

- HGI is a non-profit organisation created to define guidelines and specifications for broadband home gateways.

- Requirements for the home gateway:
  - the need to manage the home gateway and network(s);
  - *allowing the right device or application to connect to the right service platform with the right QoS;*
  - achieve a better home integrated environment.

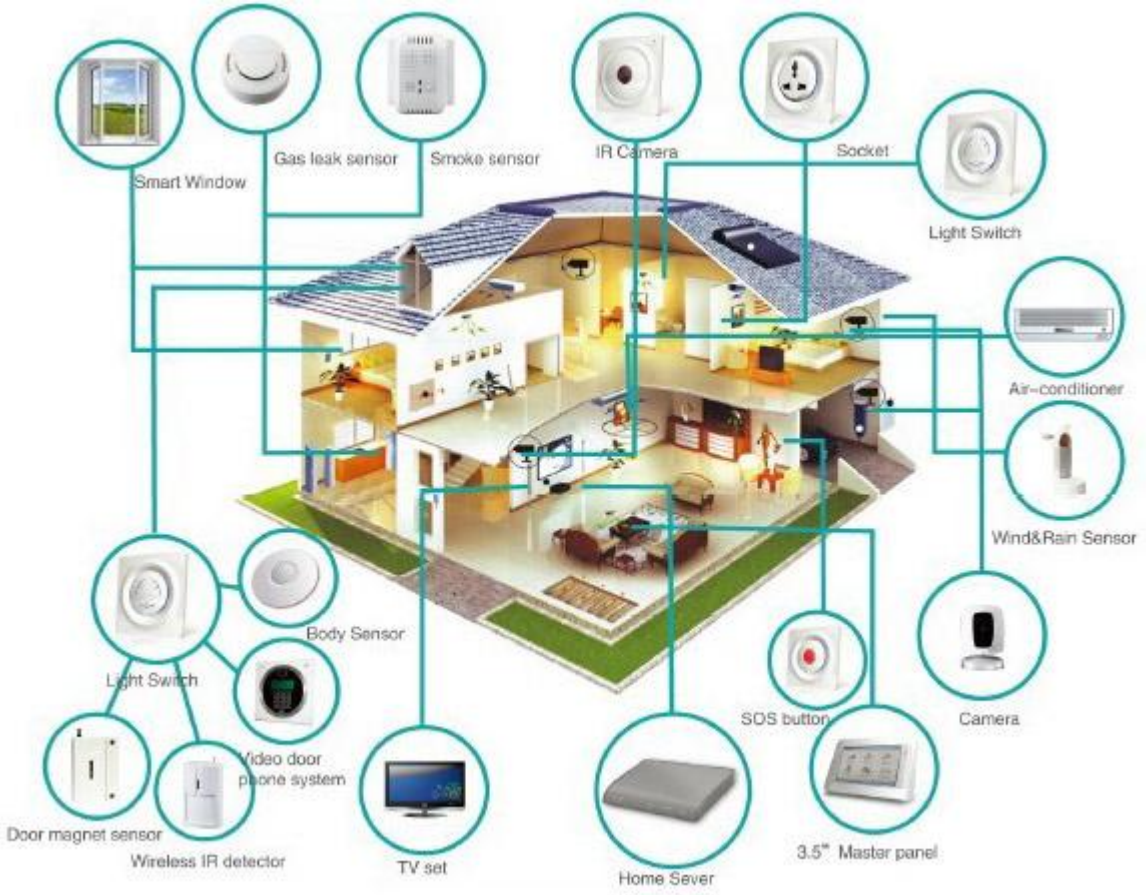
Aims

- Premium QoS. Customers expect premium services to be offered, such as IPTV and IP-telephony. New services are similar to premium gaming with guaranteed QoS.

- Any service - Any device. Customers want to access broadband services from any appropriate appliance in the home, which means that devices must be integrated with the home environment and services need to be adapted to the capabilities of the home network. *New services can be created by combining the different capabilities of devices in the home*, e.g. using the different displays and speakers to enable video rich communication. The customer also wants the capability to exchange multimedia content simply and easily between devices.

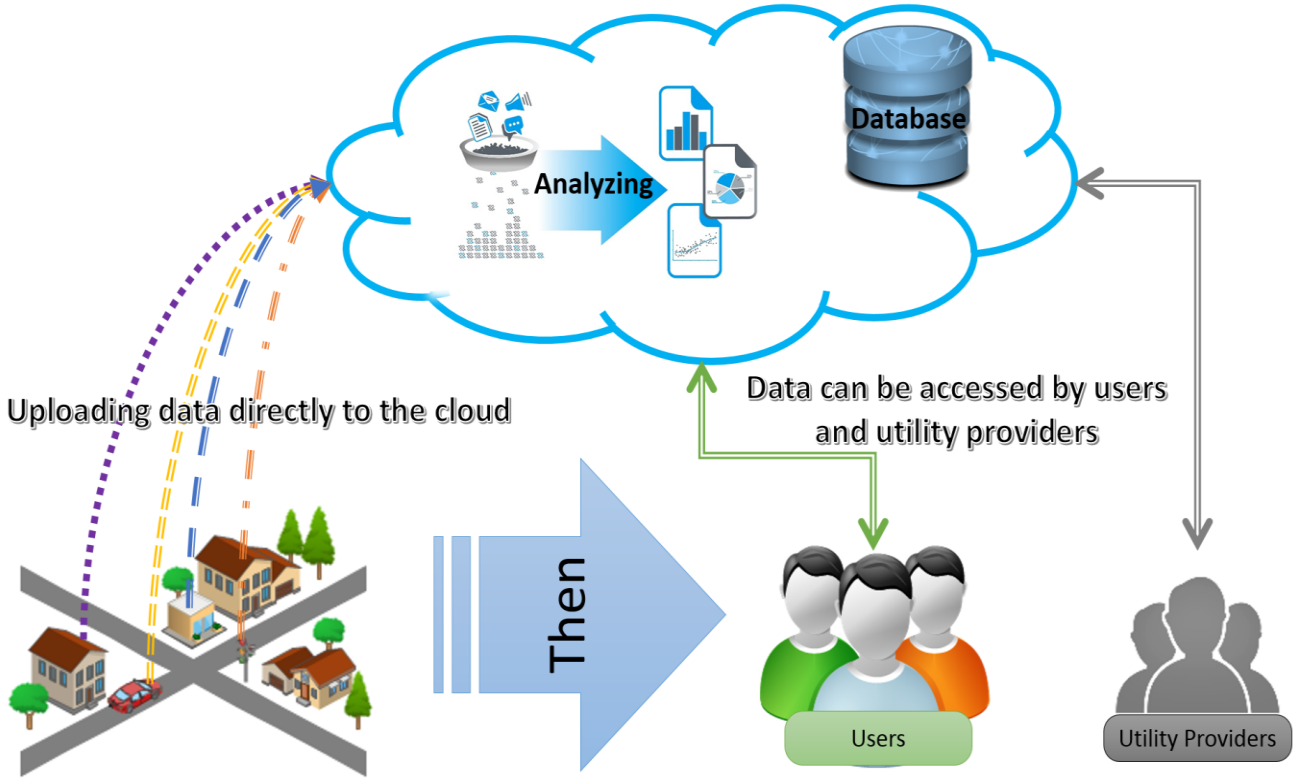
- Any service - Any place. It is also expected that customers will increasingly demand the same services from wherever they are – beyond the home environment. For example - from a Wi-Fi hotspot, from hotels, or even other consumers' homes. To enable this, users must be able to access their home environment in a secure way. Capabilities that are network independent must be introduced (for example directory, authentication, etc.) and these must be independent of the device used (any screen can be used to access a customer service set).

Smart home



https://www.linkedin.com/pulse/20140922120509-194646369-m2m-utilities-an-energy-efficient-smart-home-ecosystem

Smart meter – cloud app



Requirements

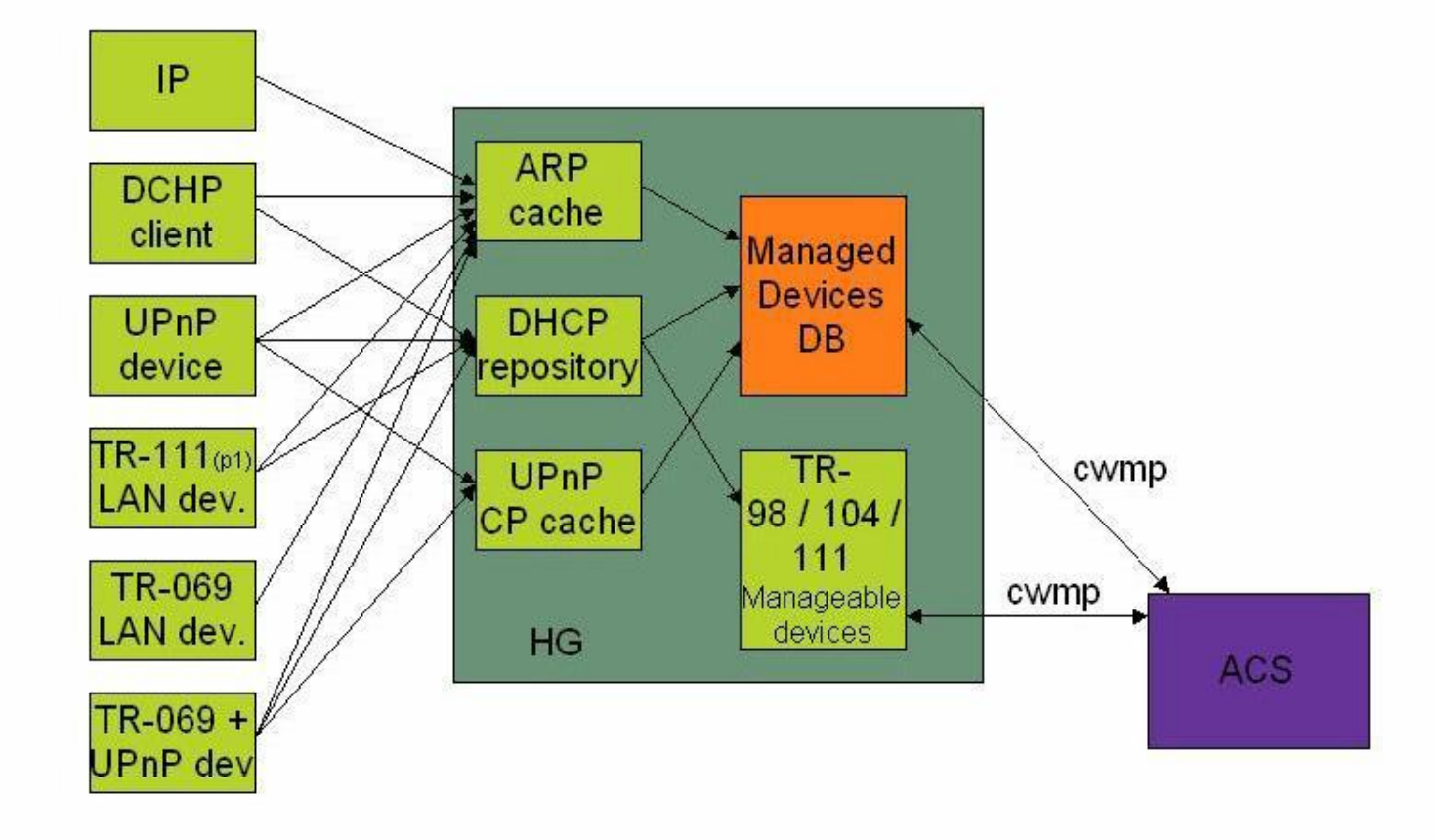
- The Home Gateway must be *technology agnostic and be managed by a single entity;*
- The Home Gateway (including broadband connection provisioning and management, software maintenance, etc.) and associated devices and services must be *easy to install and configure.* They must also be manageable by the BSP – RMS (Broadband Service Provider – Remote Management Service);
- Home-office support functions, e.g. Home Gateway must support appropriate *connections to corporate resources;*
- Acting as a proxy for those devices in the home that are not capable to communicate over the broadband network and thus hiding the complexities of the home network from the broadband network and visa versa. This class of devices includes legacy telephones and consumer electronics.
- *QoS*
- Home gateway router and/or bridge.

HG network architecture

- Bridged model: in this model the HG would be a pure L2 device, and run MAC address learning between all its WAN and LAN interfaces. Packet forwarding through the HG would happen at the L2, Ethernet level on the basis of this learnt MAC address to port mapping. All devices on the home network would need to belong to the same subnet. LAN side traffic would be sent to the WAN interface when the destination MAC address was not recognized as being on the LAN. Broadcast traffic on the LAN would also be sent to the WAN.

- Routed model: a model in which private IP-addresses would be assigned by a DHCP server running on the HG, service (Internet, voice, video, etc.) connectivity being realized through NAT running on the HG. All devices in the HN would need to belong to the same subnet to ensure connectivity on the HN itself. Some applications (e.g. VPNs) would need NAT pass-through in the HG in order to work properly across the NAT. The HG could either run a routing protocol or be configured with (a set of) simple static routes.

Device discovery and management



The discovered ID information is used by the HG to fill a Managed Devices Data Base that can be read by the remote management server.

Device management

- End-device management mechanisms can be divided into two main categories:
  - Device Discovery. This task is performed by the HG; it will discover and manage end devices (ED) in the home network through DHCP, UPnP and TR-069. This data will be accessible to the RMS.
  - Device configuration. The supported mode of operation is the direct configuration of the ED by the RMS.

Adding IoT to the smart home

- New specifications ratified by UPnP Forum provide a base for IoT by integrating with non-IP connected devices while adding enhanced security, richer audio/video features, and the UPnP®+ Cloud Architecture for virtualizing and enabling secure sharing of devices and content over the Internet.

- UPnP Forum has already produced control protocols for lights, thermostats, automatic blinds, and security cameras. In addition, support for any device with a combination of sensors and/or actuators can be added easily thanks to the use of extensible data models.

UPnP+ cloud architecture

- UPnP technologies allow someone to find and display content from a media server in the home, present an overview or background information about it, and play back a selected video on a TV, tablet, or phone.
- New scenario: a user now has the ability to securely invite one or more users in different locations to a “virtual room” and play that same video back for friends and family on their devices, over the Internet. The owner has complete control to configure each participant using role-based access rights including read, write, or full control levels.
- This level of group interaction is possible using the UPnP+ Cloud Architecture, which incorporates the industry standard Extensible Messaging and Presence Protocol (XMPP), a communications protocol for message-oriented middleware based on Extensible Markup Language (XML).

Discovery service conclusions

- Two discovery services were presented, Jini and UPnP. These two services can be part of a more complex middleware system that supports distributed applications.
- They involve device/service description (e.g., in XML) and remote execution.
- Optionally, events can be notified to interested parties.
- Architecturally, Jini and UPnP are different.

Links

- http://www.homegatewayinitiative.org