Grant Agreement No.: 258378

FIGARO

Future Internet Gateway-based Architecture of Residential Networks

Instrument: Collaborative Project

Thematic Priority: THEME [ICT-2009.1.1] The Network of the Future

Requirements for federated network organization and heterogeneous network optimizations

Due date of deliverable: 30.09.2011
Actual submission date: 30.09.2011

Start date of project: October 1st 2010 Duration: 36 months
Project Manager: Henrik Lundgren, Technicolor R&D Paris
Revision: v. 1.0

Abstract

This document identifies and describes the main requirements for FIGARO network organization and optimization. Selected FIGARO networking use cases are described in detail along with their main imposed requirements. This work leverages earlier FIGARO work on requirements and initial architectural considerations. We organize the requirements according to the main FIGARO functional modules and then discuss the implications on these modules' interfaces. This document will be used in subsequent work as input to the development of FIGARO networking solutions as well as to the FIGARO overall architecture.

Project co-funded by the European Commission in the 7th Framework Programme (2007-2013)		
Dissemination Level		
PU	Public	✓
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Document Revision History

Version	Date	Description of change	Editors	Authors
V.1.0	30.09.2011	Final version submitted to the EC	THRDF, TRDP	THRDF, TRDP, POLITO, TID

Table of Contents

1 INTRODUCTION

The Future Internet Gateway-based Architecture of Residential netwOrks (FIGARO) project envisions that residential networks connected at the edge of the Internet are becoming an integral part of the Internet, and that content will be created and delivered to/from hundreds of millions households hosting these residential networks. Towards this vision, FIGARO proposes an evolvable Future Internet architecture based on gateway-based federation of residential networks. In FIGARO, the residential gateways undertake the role of federators. These gateways interconnect the residential network with the Internet, are responsible for aggregating a multitude of devices and services within the residential network, and are control points where many Internet-based services pass through.

Figure 1 shows residential networks connected at the edge of the Internet and illustrates a simplified view including the two types of gateway-centric residential network federations. The upper part illustrates external federation interconnecting multiple gateways to form a cooperative overlay across residential networks. This federation enables to offer added value in terms of e.g., resource sharing and collaborative network optimizations. For example, access network sharing for increased bandwidth and improved service delivery, and wireless neighbourhood optimization in terms of load-balancing, interference management, etc. The right-most residential network illustrates an example of an internal network federation consisting of a mix of regular IP-based network and other sector-specific networks (possibly non-IP) e.g., for home automation and e-health. The internal federation enables features such as communication, resource, and content sharing among the involved networks as well as a common interface to these networks through the gateway.

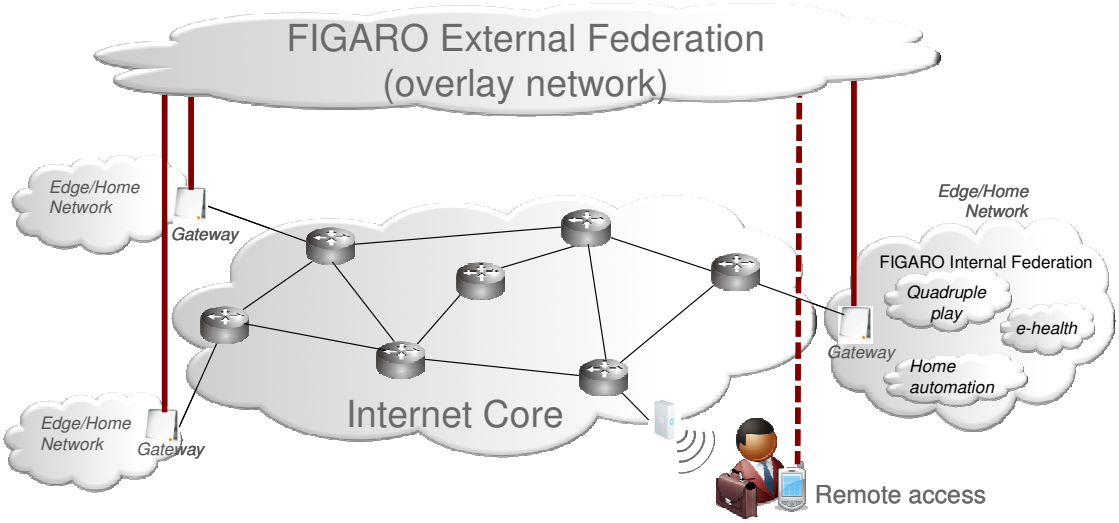

Figure 1 – FIGARO gateway-based external and internal network federations.

The work in WP3 focuses on developing innovative networking solutions that leverage the network federation concept and aims to improve network performance and end-user QoE of digital content and services. In particular, we consider the following main scenarios: (i) neighborhood community networks to share wireless networks and Internet access networks to exploit unused network capacity and overcome bottlenecks; (ii) enhanced remote home network access for improved service; (iii)

network- and content-aware optimizations for improved video service delivery; and (iv) communication across heterogeneous networking technologies[1].

In this deliverable, we identify and describe the main requirements for FIGARO network organization and optimization. We describe selected FIGARO networking use cases in detail and derive their main derived requirements. This work leverages and extends earlier FIGARO work on requirements and initial architectural considerations from WP1. Based on this work and the derived requirements, we introduce a preliminary set of FIGARO functional modules as seen from the networking use cases' perspective. We then organize the requirements according to these modules, and finally briefly discuss the implications on these modules' interfaces. This document will be used in subsequent work as feedback to architectural work in WP1 and as input to the development of FIGARO networking solutions in this WP. We therefore provide a rough outline of the work ahead.

The remainder of this document is organized as follows. Section 2 provides detailed use case scenarios and derives their requirements. We identify FIGARO functional modules based on these requirements in Section 3. The functional modules' interfaces are discussed in Section 4. Section 5 provides a rough roadmap and Section 6 concludes this deliverable.

[1] Note that internal federation and heterogeneous cross-sector networking and service solutions are addressed in WP5, wherefore WP3 focuses more on the external federation scenarios.

2 USE-CASE DESCRIPTION AND REQUIREMENTS

FIGARO will provide innovative networking solutions that improve network performance and end-user QoE of digital content and services. These solutions will leverage the gateway for network federation and content-awareness. This section provides an extension to the networking-related use cases and requirements that were briefly introduced in the FIGARO deliverable D1.1 "Requirements Document". In this section, we provide detailed use case descriptions and derive their corresponding requirements.

For convenience, below we briefly overview the use cases that we later will describe in detail:

- *Federated neighbourhood network optimizations.*
  - ***Backhaul bandwidth aggregation***: client devices connect to neighbouring APs and exploit their (unused) access network bandwidth to increase performance.
  - ***Wireless neighbourhood optimization****:* networks in the neighbourhood collaborate to exchange monitoring data and perform wireless network optimizations.
  - ***Load-balancing****:* the client associations to APs are load-balanced across neighbour APs for improved performance.
  - ***Eco-*management**: the client associations to APs are managed across the neighbourhood such that a maximum number of gateways can be turned off to save power.
- *Remote access.*
  - ***"Foreign" federation gateway access***: remote clients connect to other federated gateways to exploit resources, such as Internet access, storage, or computational power.
  - ***Remote access to home network and its content/services*:** remote clients connect to the home gateway to enjoy content or services.
- *Gateway-assisted video streaming optimizations.*
  - ***Transparent multi-path adaptive video streaming****:* the home gateway transparently provides multi-path transport support to improve video streaming services.
  - ***Video-aware wireless optimizations****:* the gateway exploits information about the video stream characteristics to improve the video streaming quality over a wireless network.
- *Heterogeneous technologies management*.
  - ***Sensor data collection***: the gateway acts as an interconnection hub for wireless sensor and actuators with the aggregation and processing capability of the FIGARO architecture.
  - ***Media independent handover***: the home gateway is integrated within a wider Media independent handover (MIH) capable access network.

We organize the rest of this section according to the use cases listed above. For each use case we provide the following information:

- *Scenario* – the scenario description or story about the use case.
- *Actors* – the devices that are involved in the use case.
- *Pre-conditions* – the necessary conditions that must exist for this use case to be considered.
- *Trigger* – the trigger or action that causes this use case to initiate.
- *Events* – the series of events or steps that this use case involves.
- *Post-conditions* – the operation after the events of the use case has been executed.
- *Variations* – the description of possible and interesting variations of the current use case.
- *Requirements* – the description of the derived requirements.

2.1 Federated neighbourhood network optimizations

2.1.1 Backhaul bandwidth aggregation

This use case is based on client devices that can connect to neighbouring APs and exploit their (unused) access network bandwidth to increase performance.

Scenario

We envision a service that can benefit from the close proximity of Wi-Fi-enabled gateways in range with spare backhaul bandwidth. Users with low quality of DSL line or with congested backhaul link could benefit from extra bandwidth provided by the different neighbor gateways.

This scenario is *Client-initiated*: A client will virtualize its wireless card and cycle over the gateways in a TDMA fashion, effectively aggregating the bandwidth of the multiple gateways backhauls in range both uplink and downlink.

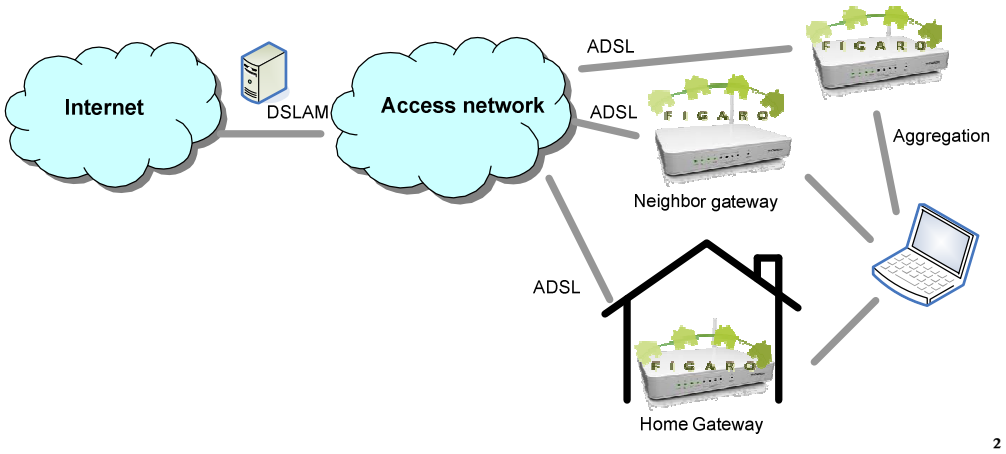

Figure 2 : Backhaul bandwidth aggregation

Actors

Federated gateways and their wireless clients.

Pre-conditions

High density of multiple overlapping WLANs connected to broadband backhauls (such as a city neighbourhood).
Federation members are willing to share their spare broadband bandwidths in exchange of being able to use the spare bandwidth of others as well.
Wireless clients should have high SNR/high wireless data rate conditions toward nearby wireless gateways.
Clients must be aware of the backhaul traffic load of gateways within their wireless range as well as local wireless traffic load by out-of-band channel or by estimation.

Trigger

A monitoring service (on the client or on the gateway) detects that local traffic load is higher than the local backhaul bandwidth.

Events

The monitoring service detect that local traffic load is higher than the local backhaul bandwidth and trigger the backhaul aggregation to be initiated..
The client detects surrounding federated gateways by exploiting information gathered through the radio interface.
Clients activates virtualization of its wireless interface and connects to neighbouring gateways (APs).
Client monitors bandwidth availability.

Post-conditions

When the backhaul aggregation service is active, traffic generated at each client is flowing through the available bandwidth of the neighbor gateways.

Variations

*S*ome backhaul links can be used as backup or support for differentiated traffic can be introduced in order to accelerate certain applications instead of plain aggregation. Contextual information, such as link quality, number of stations sharing the links, and general AP utilization (broadband link occupancy, CPU usage etc.), will be used to take decisions.

Requirements

We have identified the following main requirements:
- *QoS mechanisms* should be present in the gateway to enable backhaul aggregation in a fair way
- *Traffic monitoring* is needed to insure to react to traffic condition change
- *Incentive mechanism* is necessary to reward users that contributes to the system, including the case were the contribution is more important than the benefit.
- *Contract information* about the bandwidth subscribed should be taken in account to avoid the tragedy of commons, were users paying for small backhaul end up using the spare bandwidth of users paying expensive contracts.
- *an AAA service* is required for secure and accountable operation of gateway federations

2.1.2 Wireless neighbourhood optimization

The federated neighbourhood network collaborates in exchanging monitoring data and performing wireless network optimizations (e.g., interference mitigation) to improve performance.

Scenario

A set of gateways that are members of a neighbourhood federation collaborate to optimize their wireless network operation by exchanging wireless network configurations and/or performance information, and coordinate to optimize their wireless networks. The gateways collaborate using dedicated protocols in terms of exchanging selected monitoring data, as well as in terms of executing optimization procedures and implementing the computed wireless configurations (this may be e.g., channel assignment, power control, directional communication, etc).

This scenario is *gateway-initiated*.

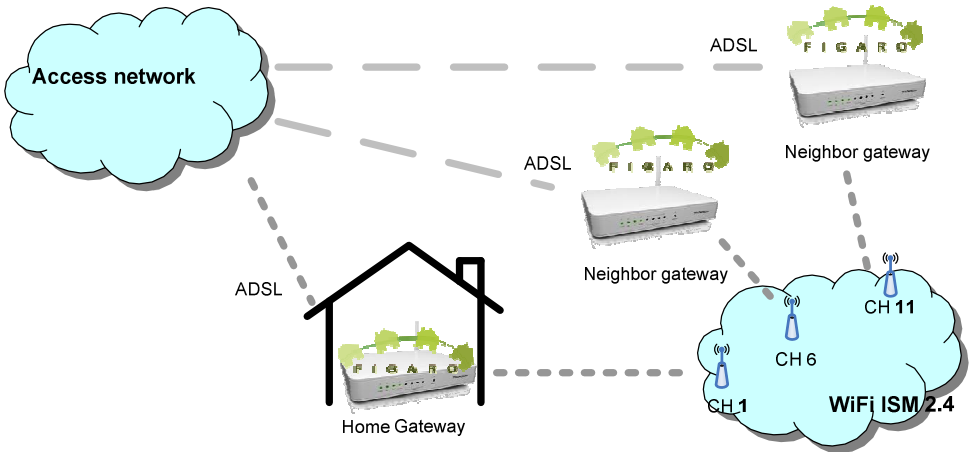

Figure 3 : Wireless neighbourhood optimization

Actors

Gateways in the neighbourhood federation.

Pre-conditions

A set of federated gateways with knowledge of their own environment through monitoring.
Each Gateway hosts a management service that provides wireless network reconfiguration capabilities.

Trigger

Each gateway periodically runs an optimization check routine. Alternatively, the process can be also triggered by poor (network/service) performance detected by a monitoring service, or the process can be also user-triggered at the gateway user interface level.

Events

Neighbourhood optimization is triggered by periodicity, monitoring service, or by the user.
Gateways in the neighbourhood federation exchange information about their wireless network configurations, and potentially about their current performance, and about any specific requirements that must be met by their individual services or applications.
Gateways coordinate to perform network optimization.
One gateway (possibly the initiator) is elected to centralize the computation of the optimization and to deliver the optimization outcome to neighbouring participating gateways.

Post-conditions

Each gateway has applied the proposed optimized wireless settings and their performance has measurable improvement.

Variations

An alternative operation is that gateways do not explicitly exchange monitoring data, but deduce information through simple overhearing. For example, a gateway monitors the presence of beacons of nearby wireless devices, gathers their configurations (e.g., their channel number) and identifies those issued by other Figaro gateways. In order to minimize the radio channel overlap, the gateway (initiator) contacts the neighbouring Figaro gateways through an out-of-band (backhaul) link and coordinates with them the choice of channels. An automated reconfiguration of each gateway follows.

Requirements

We have identified the following main requirements:
- *an identification service* that use the beacon system that broadcast SSID information in wireless networks will be used to identify FIGARO gateways;
- *an AAA service* is required for secure and accountable operation of gateway federations
- *Traffic monitoring* of the home network is continuously performed;
- *Data collection and aggregation service* is used to expose data to all involved federation members;
- *A communication channel* (inband or out of band) is used to enabling sharing of the selected information;
- *An optimization engine* will process the local and foreign wireless network information

2.1.3 Load-balancing

The client associations to APs are load-balanced across neighbour APs for improved performance in high-traffic scenarios.

Scenario

A gateway serving client devices through an 802.11 interface detects that the clients, though active, are saturating the channel capacity. It therefore contacts neighbouring gateways within radio range and sharing a radio coverage of some of its clients to perform a selected handover, after which saturation is relieved (*gateway-initiated balancing)*. Likewise, a client that detects overload conditions with the gateway currently serving it, may switch to a different gateway chosen among the ones it overhears (*client-initiated balancing).*

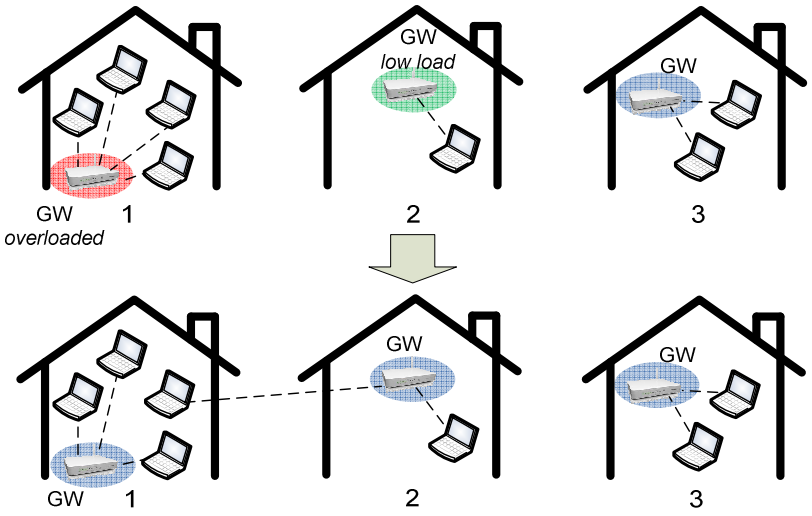

Figure 4 : Load-balancing scenario

Example of congestion relief through load balancing.
At the beginning, GW 1 finds itself in congested status following the activation of a streaming video and a data backup to a cloud service on 2 out of 4 of its WSs. GW 2 is in light status (shaded in green) and GW 3 is in regular status (shaded in blue). In order to decrease its load, GW 1 initiates an offload request toward its neighbours. GW 3 rejects it, because accepting it would have pushed it into congested status. GW 2 accepts the request and one wireless station from GW 1 associates to GW 2, and the equilibrium depicted in the last row of the figure (i.e., all Gateways in regular status) is reached.

Actors

Federated gateways and their wireless clients.

Pre-conditions

For the gateway-initiated balancing:
The gateways monitor the same load metric ("MAC-layer Achieved Throughput") on the Monitoring module. A preloaded electromagnetic map of the building or indoor location techniques can help predicting the achievable bit rates at clients.

For the client-initiated balancing:
Clients maintain a local list of available gateways and their RSSI; clients can monitor the available bandwidth on neighbouring gateways (or receive direct information through signalling); client and gateways share a common signalling channel

Trigger

Gateway-initiated balancing: The Monitoring module detects a high traffic condition because the "MAC-layer Achieved Throughput" exceeds the threshold (set by the user)
Client-initiated balancing: The client locally detects a high traffic condition, i.e., the loss rate it experiences is suddenly increased, or the latency has surged.

Events

For the gateway-initiated balancing:
The gateway contacts neighbouring gateways to establish who is/are willing to serve its clients.
Neighbouring gateways predict their load increase if accepting the offered clients, then return positive/negative reply.
The gateway evaluates all replies received within a time interval.
If possible, the gateway performs a selected handover to reduce its load, thus removing the saturation condition.

For the client-initiated balancing:
The client constantly monitors the state of other gateways by querying their Monitoring modules
The client sends a new association request to a gateway of its choice and the chosen gateway returns a positive/negative answer within a time limit and based on its current load.

Post-conditions

After a handover, the monitored metric drops below the trigger-threshold. If after a handover the saturation condition persists, the procedure is repeated.

Variations

For Client-initiated: poor coverage (low bit rate) at one or more of gateway clients due to obstacles (walls, cupboards, metal frames) could trigger a search for a better gateway connection among federated neighbouring gateways.
If no neighbouring gateway is found for any successful handover and the high-traffic condition persists, the procedure is repeated after some time.

Requirements

We have identified the following main requirements:
- *an inter-gateway signalling protocol* will be used to exchange traffic load levels and to request offloading and wake-up procedures;
- *an AAA service* is required for secure and accountable operation of gateway federations;
- *wake-on-lan reliable* procedures should be available to perform efficient management.

2.1.4 Eco-management

Manage federated gateways with overlapping coverage in low-traffic scenarios.

Scenario

We envision a service that can migrate some light user's connections to a neighbour's AP in range (as long as it has enough free capacity to route it). This way, users with light traffic that usually prevents their APs to enter into sleep mode can be migrated. Gateways can be turned off to cut down on wasted energy due to high baseline consumption.

Gateway initiated: A gateway serving client devices through an 802.11 interface detects that the clients, though active, are sending/receiving small amounts of traffic ("whispering"). It therefore contacts neighbouring gateways (within radio range and sharing a radio coverage of its clients) to hand them over and, possibly, to go to sleep for some time.

Client initiated (Broadband Hitch-Hiking): Clients that are sending/receiving small amounts of traffic decide to disconnect from their AP and connect to another federated AP with spare bandwidth within radio range.

The APs without traffic can go to sleep for some time, thus saving power and reducing electromagnetic pollution. Optionally, other ISP-side network equipment such as DSLAMS (ports or even entire line cards) can be also put to sleep, dramatically reducing power consumption.

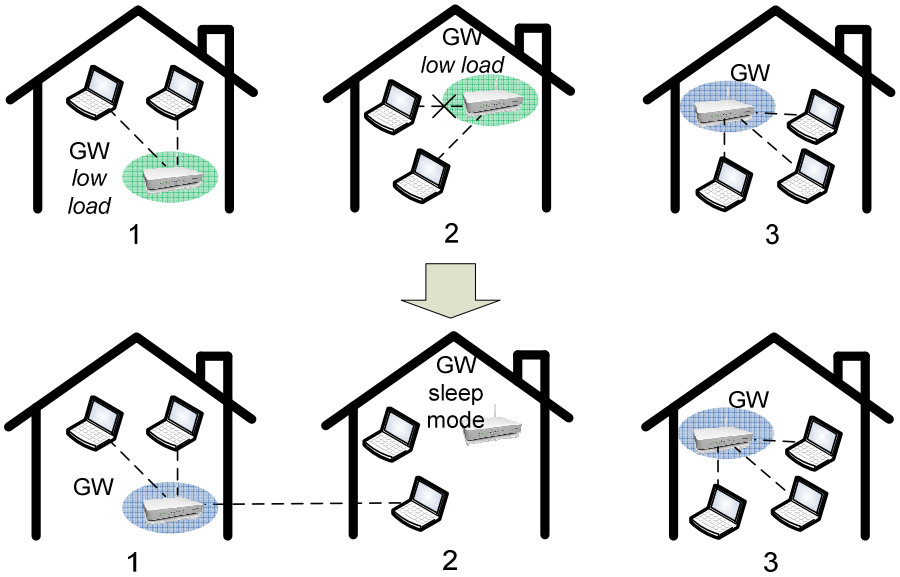

Figure 5 : Eco-management

Example of energy management.
The example shows a case of energy saving through the switching off of some Gateways.

With reference to the upper row of the figure, in household 1, we assume that one wireless station is ``whispering", i.e., occasionally sending low background traffic (mainly, status update for some applications and other signalling). The other wireless station completes the download of a software update and starts whispering as well. As a result, the Gateway in household 1 (GW 1, for short) goes in underloaded status (shaded in light green). Next door, one of the WSs in household 2 is engaged in peer-to-peer downloading, while the other wireless station is browsing Wikipedia.
The wireless station running the peer-to-peer application shuts down, hence also the status of GW 2 shifts to underloaded. Finally, in household 3, we assume one wireless station listening to music streamed over the Internet, while the other two are browsing. Their Gateway is in Regular status (shaded in blue).
Upon switching to underloaded status, GW 1 and GW 2 will start vying for the chance to offload their WSs and turn themselves off to save energy. Through a protocol exchange over the backhaul, we assume that GW 3 rejects the help request by either neighbours since it establishes that accepting any of their WSs would force it into overloaded status. GW 2, instead, ``wins" the competition thanks to its lower traffic load compared to GW 1: thus it hands its only active wireless station to GW 1 and goes ``off". Upon accepting the next-door WS, GW 1 switches to Regular status and the equilibrium shown in the second row of the figure is reached.

Actors

Gateways in federated homes, wireless clients

Pre-conditions

High density of multiple overlapping WLANs connected to broadband backhauls (such as a city neighbourhood).
Federation members are willing to share their spare broadband bandwidths in exchange of being able to use it when needed.
Preferably users typically see multiple 802.11 gateways in range with high quality.
Traffic of the clients in the home network is light (during periods of time)
Some federation access/security mechanisms are in place to prevent unauthorized access.

Gateway initiated:
The gateways monitor the same load metric (“MAC-layer Achieved Throughput”) on the Monitoring module.
A preloaded electromagnetic map of the building or indoor location techniques can help predicting the achievable bit rates at clients.

Client initiated:
Clients can know the traffic load of the gateways through a out-of-band channel or by estimating it

Trigger

Gateway-initiated balancing: The Monitoring module detects a low traffic condition because the “MAC-layer Achieved Throughput” is lower than a threshold (set by the user).
Client-initiated balancing: The client locally detects a low traffic condition, i.e., “MAC-layer Achieved Throughput” is lower than a threshold (set by the user).

Events

Gateway initiated:
The gateway contacts neighbouring gateways to establish who is/are willing to serve its clients
Neighbouring gateways predict their load increase if accepting the offered clients, then return positive/negative reply
The gateway evaluates all replies received within a time interval
If the gateway finds a possible allocation for all of its clients and succeeds in handing them over, it can turn itself off. Sleeping Gateways can be awoken by nearby Gateways through wake-on WLAN procedures on an accessory wireless interface (see Requirements).

Client initiated:
A wireless client locally checks if its demand is less than a threshold value and in the case that it is, it moves its traffic to a random neighbour gateway that fulfils certain constraints (e.g. spare bandwidth but still is not overloaded with traffic). It then lets the local gateway switch off. If the gateway had assigned to it some neighbours and thus increases its traffic over a threshold, the wireless clients return to their local gateways and search for other opportunities to migrate. The threshold controls the aggressiveness of energy saving. Its value selected such that heavy users do not migrate their traffic unnecessarily as migration has associated QoS costs.

Post-conditions

The traffic of the networks is coursed through a minimum number of APs that can support the demand while maintaining the QoS.
The operation is transparent to the users. Wake-up conditions at gateways should take into account abrupt traffic surges and sharing of sleep schedule with other gateways

Variations

For Client-initiated: Poor coverage (low bit rate) at one or more of gateway clients due to obstacles (walls, cupboards, metal frames) could trigger search for a better gateway connection among federated neighbouring gateways.
If no neighbouring gateway set is found for successful handover of all stations, no handover are performed. If the low-traffic condition persists the procedure is repeated after some time.

Requirements

We have identified the following main requirements:
- *an inter-gateway signalling protocol* will be used to exchange traffic load levels and to request offloading and wake-up procedures;
- *an AAA service* is required for secure and accountable operation of gateway federations;
- *wake-on-lan reliable* procedures should be available to perform efficient management.
- *a detection of inactivity at low layers* should be available
- *a modular sleep mode* for the different component is necessary to benefit from the optimization.
- *a minimal density of gateways* is required to implement this scheme, in order to distribute the control among the participant

2.2 Remote access

2.2.1 "Foreign" federation gateway access

This use case leverages the federation to connect to other federated gateway to exploit resources. This can be to gain access to the Internet, but, also to exploit other resources such as computation and storage

Scenario

This use case addresses the support for mobility of end users and remote access to home networks. This includes end users connecting to federation gateways (a foreign gateway implementing federation functions) while being out of home. Once connected to a federation gateway, different services can be offered to the end user. Such services include (but are not limited to) direct Internet access, remote access to the end user's home network, as well as access to various federation resources such bandwidth (already required for Internet and remote home access), computational power, storage, as well as the content shared in the federation.

This is a joined *client and gateway initiated* scheme.

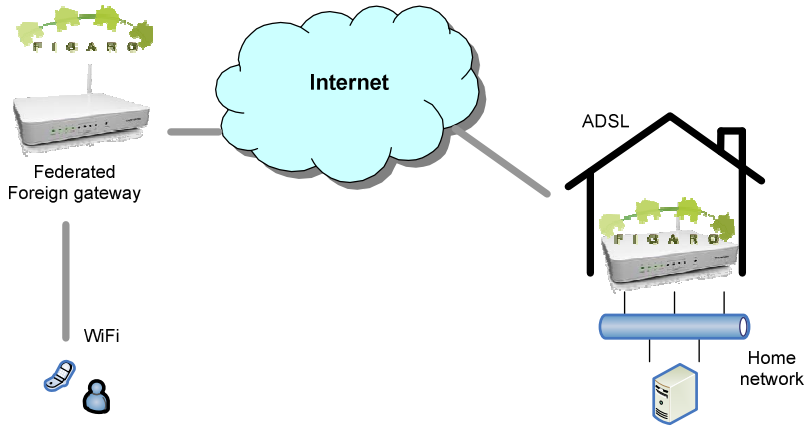

Figure 6 : Foreign federated home access

Actors

End users out of home but still in a federated network.
Gateways implementing external federation functionality and access for remote end users.

Pre-conditions

An end user being out of home who wants to access, through a federation gateway, the Internet, an external federation, and/or her home network.

Client-initiated: the end user carries a device that can connect to a gateway device (in most cases over wireless) and support the necessary security procedures but does not require special dedicated software to supported federated access.

Gateways are assumed to implement external federation functionality and to allow remote end users to connect to the gateway (e.g., through WiFi).

Trigger

Client-initiated: An end user connects to a federation gateway and explicitly signals to that gateway that it wants to access foreign federation services.

Gateway-initiated: a device part of a federated gateway requests association, the gateway detects its origin (e.g.: through authentication credentials provided to the AAA module)..

Events

Client-initiated: the end user selects one or more services to access through the federated gateway, selecting from a list of advertised services received by the federated gateway.

Gateway-initiated: an overlay network is configured following the end user preferences.

Post-conditions

Client-initiated: End-user device connected to a federation gateway. The end user may enjoy one or more offered federation services (connectivity, storage, content access, etc).

Gateway-initiated: Home gateway is providing access to the home network. Foreign federated gateway is providing access to the home gateway.

Variations

3G offloading case:
We consider the case of mobile data offloading: a mobile device with multiple radio technologies, at least one broadband (3G, 4G) and one local supported by FIGARO gateways (e.g. WiFi). The device belongs to a FIGARO federated network and hence has access to the gateway services. In particular it can route part of its traffic through the backhaul connection of the gateway (offloading) to reduce

cost/energy of transmitting through the mobile broadband links. Note that the gateway that the device is connecting to can be its own home gateway (offloading when at home, this would be the most common case), and it can also offload part of the traffic when in range of a "foreign" gateway, i.e., "roaming". The pre-conditions for this case are similar as above; the foreign gateway has to belong to the federation so that the device has permission to roam the gateway. Several technical issues need to be considered: what type of traffic can be offloaded; how much traffic can be offloaded; if there are multiple gateways in range; which ones to use for the offload; how to provide load balancing between the potential gateways, quality of service issues: offloading to reduce cost, increase throughput or increase reliability? An important aspect to consider is how to handle the priorities between the foreign traffic and the home traffic in the gateway. Even if the home user has priority it is possible to relax some of the conditions in case of light delay intolerant traffic (e.g. VoIP).

Another offloading case similar in nature but with further technical implications is a mobile data offloading when the gateways support a standard mobile broadband radio interface (e.g. UMTS in a femtocell). In this case the offloading policies are different since there are no changes required in the devices: i.e., the device will switch to the gateway following the standard algorithms for the technology (SNR, channel occupancy, etc.).

Requirements

We have identified the following main requirements:
- *an inter-gateway signalling protocol* will be used to allow the setup of network connections from federation gateway to the home gateway;
- *an extended inter-gateway protocol* will be used to perform setup between gateways from different federations;
- *an AAA service* is required for secure and accountable operation of gateway federations;
- *Overlay setup and management* is necessary to perform network abstraction.

2.2.2 Remote access to home network and its content/services

This use case demonstrates seamless secure access to resources of the home network.

Scenario

A user is within radio range of an alien WiFi access. By accessing the nearest gateway identified using the Figaro lookup service, the user can access a random gateway providing agnostic VPN services and access through the federated network to the home network.

This use case is both *client* and *gateway initiated*.

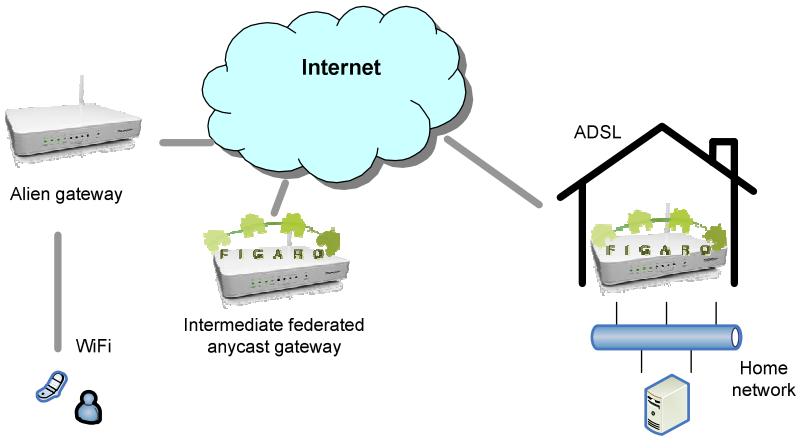

Figure 7 : Remote access to home network and its content

Actors

Federated gateways and their mobile wireless clients.
"Alien" gateways.

Pre-conditions

An end user being out of home who wants to access, through a alien gateway, the Internet, an external federation of gateway, and/or her home network.

Client-initiated: a device that can connect to a gateway device (in most cases over wireless) and support the necessary security procedures and requires special dedicated software to support remote federated access (similar to VPN client).

Gateway-initiated: Alien gateway is a standard Internet router device. Federated gateway is a FIGARO-capable gateway, with support of VPN server functionality.

Trigger

Client-initiated: An end user connecting to a federated gateway through VPN access, or disconnecting.

Events

Client-initiated: An end user device connects to a federation gateway (assuming authentication, etc) through VPN access. The end user selects to use one or more services offered by the federation gateway by selecting the desired network.

Gateway-initiated: the gateway sets up the network overlay accordingly through the VPN interface.

Post-conditions

Client-initiated: An end user connected to an alien gateway with a standard VPN client. The end user may enjoy one or more offered federation services (connectivity, storage, content access, etc) through the secure VPN access.

Gateway-initiated: Closest federated gateway providing access to the federation network and to the home network.

Requirements

We have identified the following main requirements:
- *an inter-gateway signalling protocol* will be used to allow the setup of network connections from federation gateway to the home gateway;
- *a multi-protocol VPN service* will be running on the external gateway at intermediate proximity of the client;
- *The Figaro lookup service* will be used to reach the intermediate gateway.

2.3 Gateway-assisted video streaming optimizations

2.3.1 Transparent multi-path adaptive video streaming

This use case leverages the home gateway to improve video streaming services by, transparently for the end-user, implementing multi-path transport support between the service provider and the home gateway. This provides improved robustness and performance.

Scenario

An end-user selects a streaming video service that will be received via the gateway. The Streaming server, outside the home network, supports streaming over concurrent multiple paths, e.g., through appropriate transport-layer protocols such as SCTP, although the end-user device does not. The Gateway intercepts the multi-path signalling and acts as an end-point for the multi-path transport protocol, while aggregating the video stream over a standard single-path transport protocol, for the benefit of the end user device. The targeted video quality is HD, 3D or multi-view content that is difficult to deliver when using a single network path. The service achieves improved robustness and aggregate throughput, resulting in a better user experience.

This is a *gateway-initiated* use case.

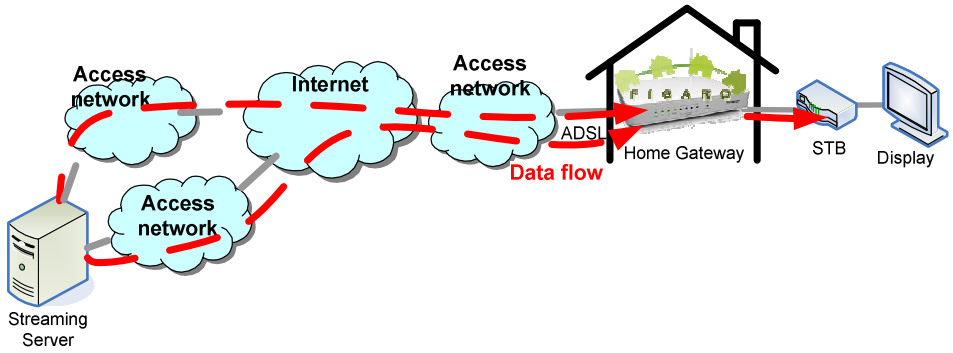

Figure 8 - Multipath video streaming

Actors

Federated gateway, and a content/streaming server

Pre-conditions

The server is multi-homed (has multiple IP addresses) and supports a multi-path capable transport protocol such SCTP.

The gateway supports the same multi-path capable protocol. The multi-path streaming enhancement service is installed and running on the gateway. Gateway should be able to intercept video service request from client and the reply from the video server.

Trigger

The end-user requests content from a multi-path capable server, which offers a concurrent multi-path connection in the connection-opening signalling. The gateway intercepts the multi-path signalling and acts as multi-path connection end point.

Events

The end-user initiates the connection request with a remote video server.
The gateway transparently intercepts the request and forwards it to the multi-path video server, acting as request originator.
The video server accepts the request and opens a multi-path connection with the gateway, streaming the requested content.
The gateway, receives the stream from the server, aggregates it on a single connection and forwards it to the requesting end-user.

Post-conditions

The end user device plays back an aggregated video flow delivered by the Gateway.

The gateway aggregates a multi-path connection to create a single connection for the client.

Variations

Multi-homed gateway: the gateway may activate an additional communication path (e.g. 802.11a connection to a neighbouring federation gateway having sufficient unused bandwidth) to demonstrate the benefits of multi-path without a multi-homed server.

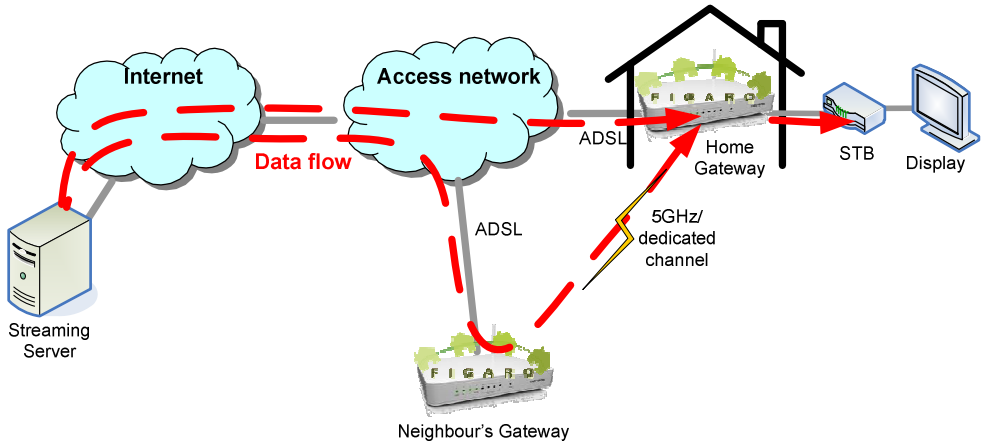

Figure 9 - Multipath video streaming leveraging multihomed gateway

Multi-homed gateway and server: combination of both the nominal case and the first variation.

Requirements

We have identified the following main requirements:
- *An inter-gateway signalling protocol* will be used to allow the setup of network connections from federation gateway to the home gateway;
- *A multi-path transport protocol* must be supported (CMT SCTP or MPTCP) on the gateway
- *A HTTP streaming application* needs to be deployed on the client
- *A HTTP proxy analyser* should be running on the gateway to intercept streaming request and perform multi-path switch
- *A monitoring service on the link quality* of the selected neighbouring gateways should be performed

2.3.2 Video-aware wireless optimizations

This use case leverages the gateway to exploit information about the video stream characteristics and optimize the wireless network for improved end-user quality of experience.

Scenario

The end-user selects a piece of content (e.g., a video) that is stored locally on a server in the home. The content is distributed wirelessly to the rendering device. The wireless network is auto-configuring to optimize its setting based on the video streaming requirements (e.g., the video streaming rate). This will result in a more robust transmission of the video content and thus a better user experience.

This is mainly a *gateway-initiated* use case.

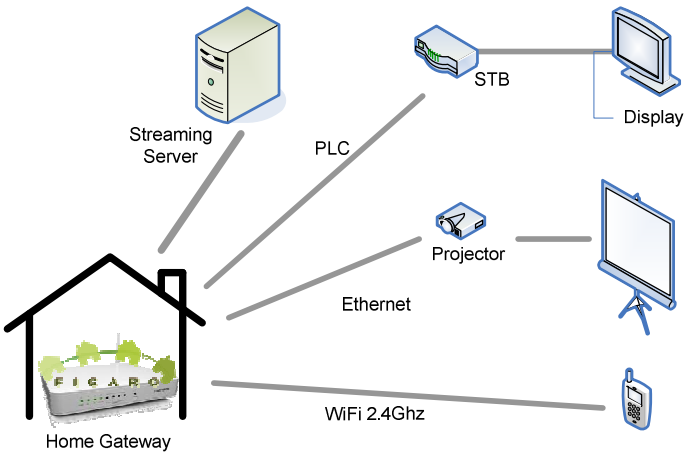

Figure 10 : Video-aware wireless optimizations

Actors

A server providing content.
A client or rendering device requesting content.
A wireless interface on the gateway that adapts its settings based on content requirements.

Pre-conditions

A server in the home network hosts content.
The gateway comprises a wireless AP.
The gateway must be able to obtain video streaming information (e.g., video streaming rate).
The gateway must able to continuously adapt the wireless configuration.

Trigger

The start of the video stream over a wireless home network is detected.

Events

End user selects a video from the content server and selects the rendering device.
The video stream is being wirelessly transmitted from a wireless AP (the gateway) to a rendering device.

The gateway detects the transmission of the video stream and obtains the additional video streaming information.
The gateway starts optimizing wireless configuration for this video flow over the specific wireless link based on the requirements deduced from the video streaming information.

Post-conditions

The wireless network operates in an adaptive manner to optimize its configuration to best support the transported content.

Variations

Multiple videos: In the case of multiple videos being transmitted simultaneously over the same wireless link, the videos are multiplexed in an optimal fashion.
Competing best-effort traffic: In the case of competing best-effort traffic in the home network, optimization mechanisms will give priority to the video streams.

Requirements

We have identified the following main requirements:
- A *monitoring service* that can detect the start of a video stream.
- A *monitoring service* that can provide video streaming information. This may be real time monitoring or it can be simply accessing pre-recorded information.
- A *monitoring service* that provide network performance statistics, such as frame error rate, available bandwidth, and MAC layer achievable goodput.
- A *network management service* that can continuously modify its wireless network configuration.
- A *network management service* that allows to prioritize between different types of data traffic.

2.4 Heterogeneous technologies management

2.4.1 Sensor data collection

This use case introduces the gateway as a seamless interconnection hub for wireless sensor and actuators with the aggregation and processing capability of the FIGARO architecture.

Scenario

This use case is designed to address the special case of the wireless sensors networks, which are developing rapidly in the home through the use of sensors (temperature, fire…) and actuators (switches…). In order to have a long battery life these devices are relying on low power radio technology build around the IEEE802.15.4 standard with a set of protocol and applications features already specified in the ZigBee standard. Due to low power constraints, these devices do not exhibit lot of capacity or processing power, and therefore rely on "sink" devices to collect and process the data they generate. The Figaro gateway should exhibit such a capability in order to collect transparently data and make it available to other devices based on heterogeneous connectivity. As well, the Figaro gateway should present API to access and pass data, as well as an API to perform actions on the wireless sensors networks for devices that does not have a IEEE802.15.4 compatible radio.

This is a *gateway and client initiated* use case.

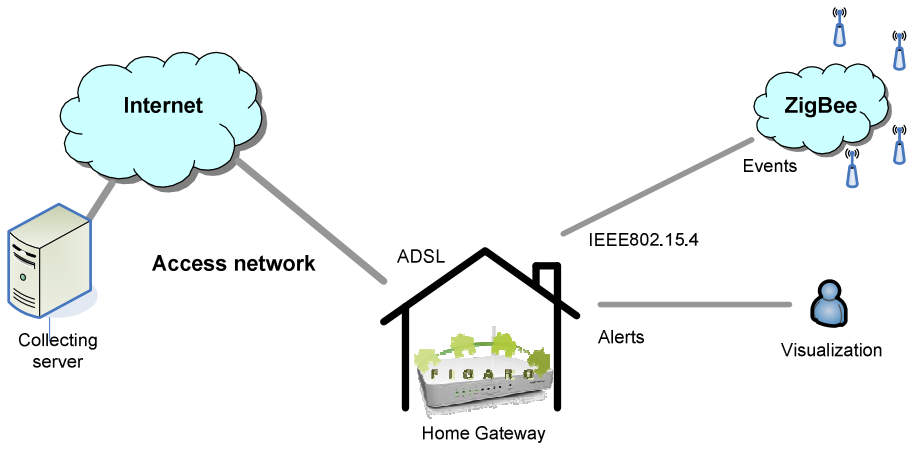

Figure 11 : Wireless Sensor Network scenario

Actors

End-user wireless sensor modules, gateway

Pre-conditions

Client-initiated: Sensor platform build on IEEE802.15.4 radio standard (Temperature, contact sensor…) with a well-defined communication protocol (ZigBee).
Gateway-initiated: For some type of data, some statistics analysis and logic engine is implemented in the gateway to present a high-level end user vision (last max value, last fastest rise etc…) and event generation (alarm, alert…).

Trigger

Client-initiated: The sensor module, while powered and during its duty cycle transmits periodically or on demand a value obtained from its on-board digital or analogic sensors.

Events

The wireless sensor module transmits some values from the sensors.

The wireless packet is received and decoded by the gateway which will translate it in a comprehensive value (analogic sensors is typically a voltage that need a conversion due to the ADC used). The value is stored and eventually processed by internal logic depending of the sensors used. Finally the data can be later requested by other devices.

Post-conditions

The end user should enjoy transparent access to the settings of the wireless sensors networks (periodicity of measurements, battery life, and status of the wireless sensor modules) as well as the past data collected.

Variations

This use case is adapted to a scenario where the wireless sensor protocol is known (in this case the value carried by the sensor can be interpreted by the gateway and transformed as a service). Also, the gateway could be used as a simple router in case of wireless sensors networks based on technology similar to 6lowpan.

Requirements

We have identified the following main requirements:
- *A event-loop manager* is needed to receive and perform processing, storage and adaptation of the data received on the IEEE802.15.4 radio according to Zigbee protocol;
- A basic protocol to request/publish data collection info should be available on the gateway;
- *A ZigBee hardware radio interface* should be present in the gateway to insure hardware radio and protocol compatibility.

2.4.2 Media independent handover

This use case describes the integration of the FIGARO gateway within a wider Media independent handover (MIH) capable access network, in order to facilitate seamless handover between heterogeneous access networks and interact with the gateway mobility management mechanisms.

Scenario

This use case addresses the situations where a user is in the process of viewing/reading some content as he walks in/walks out of the home environment. The goal of media independent handover is to let the user seamlessly continue enjoying the content when the layer-2 access network changes (e.g., between 802.11 and 4G). An IEEE standard (IEEE 802.21) already handles these situations and the Figaro gateway should be designed so as to assist it. Beside acting as a point of access for the WiFi network, the FIGARO gateway should act as MIH point of service (MIH PoS), i.e., a network entity that exchanges MIH messages with the mobile node during the handover procedure from/to the outside 4G to/from the inside WiFi.

This is a *mixed gateway and client initiated* use case.

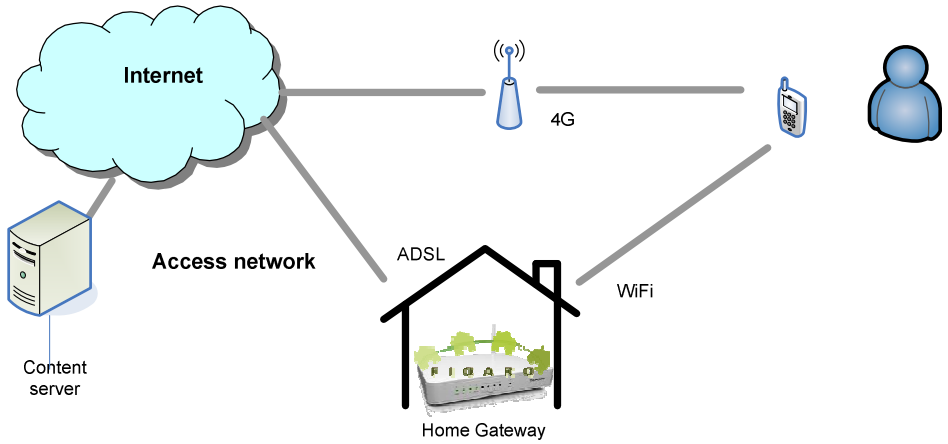

Figure 12 : Media Independent Handover

Actors

Gateway and mobile/wireless devices.

Pre-conditions

An end user carries a portable device on which a file is being downloaded (or a multimedia show is being watched). The user is about to leave home (resp. enter his home) and wants the file to continue downloading (or the show to continue streaming, or to resume after being paused) over the 4G network (resp., over the home WiFi).

Client-initiated: File downloaded from the client though the home gateway connection or through external 4G access.
Gateway-initiated: Capable of accessing the file and detecting the client device.

Trigger

Client-initiated: The portable device tracks its position through either GPS coordinates, cell information or physical layer notifications (e.g., weakening of WiFi signal could mean that the user is leaving home and MIH functions must be triggered).
Position information is returned to the MIIS (see "Requirements" below) on the Gateway who informs the portable device if MIH must be initiated.

Events

Client-initiated: After the MIH function is initiated, the link layer is activated in search of the desired link (e.g., when leaving home, the 4G interface can be switched on). When the target network has been acquired and a connection is established, a "Link Detected" indication event is pushed to the MIH layer. The device starts a network layer handover procedure, e.g. using Mobile IP.

Gateway-initiated: When the handover has occurred, the target network (4G when leaving home, the home network and the gateway when entering home) must inform the former serving network that any resource associate to the client must be released.

Post-conditions

The end user continues to enjoy uninterrupted connectivity and does not need to restart downloading/streaming.

Variations

This use case can also be applied to WiFi clients being handed over to different Figaro gateways (see "Load Balancing" e "Eco-management" scenarios). The WiFi client can query an information server (a neighbourhood broker, for example) to obtain the Wi-Fi network information of the nearby gateway without directly scanning through the Wi-Fi interface. Using the information provided by the information server, the mobile node can switch its WiFi interface to associate to the new Gateway.

Requirements

We have identified the following main requirements:
- *A Media-independent information service (MIIS*) is needed to provide a framework through which a user terminal can acquire network information within a geographical area to facilitate handovers;
- *Support for IEEE 802.21* and *a mobility management protocol* at the network layer (typically, Mobile IP) for the gateway and the client.

If the handover involves the 3G/4G network, the latter **must** support IEEE 802.21.

3 REQUIREMENTS CATEGORIZATION

In this section we consolidate and categorize the requirements derived from the use cases in the previous section. We use this consolidation to identify a set of core functionality of the Figaro architecture from the networking (WP3) perspective.

We identify the following categories by analyzing the use case requirements and group them as follows:

- *Federation operational requirements*
  - **Lookup services** keep track of gateway's services and location.
  - **AAA** provides authentication, authorization and accounting.
  - **Gateway management** is responsible for fault/configuration/performance management, service deployment and resource allocation.
- *Local gateway requirements*
  - **Network management** controls network adapters, enforces QoS, fairness and prioritization. Manages multi-path communication, bandwidth aggregation, load-balancing and eco-friendliness.
  - **Monitoring** allows aggregation and processing of data gathered by active or passive means.
  - **Control Network Proxy** acts as a bridge between the sensors and the IP world.
  - **Federation Control Box** manages access control to devices and sensor data.
- *Services/Applications*
  - **Services/applications** that are networking related and needed by certain use cases.
- *Platform requirements*
  - **Hardware** is related to gateway and device hardware.
  - **Resource virtualization** refers to the concept of virtualizing networking hardware

Figure 13 illustrates this module organization. It should be noted that this is a draft organization from the viewpoint of the WP3[2]. For additional clarity and for future use, we divide the organization in two vertical domains, namely the *platform (or owner) domain* and the *service domain*. Similarly, we make a horizontal division to indicate the scope of the modules; *Gateway* means local to the gateway device; *Per domain* refer to a broader domain outside the single home, e.g., a neighbourhood federation; *Global* relates to modules that are global or universal to the FIGARO system.

In the following sub-sections we discuss the requirements for these functional modules.

[2] This will be input to the overall architecture in WP1. However, viewpoints from other WPs may impact this organization, so future refinements are expected.

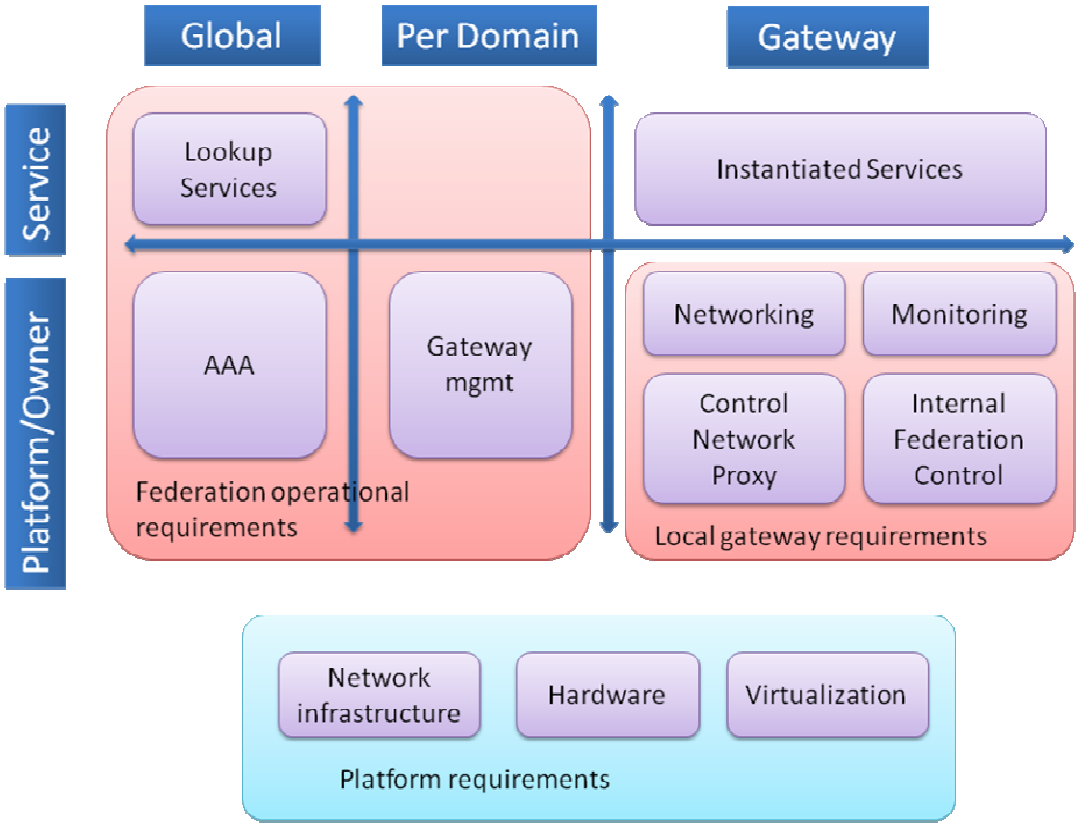

Figure 13 – Organization of functional modules derived from the requirements

3.1 Federation operational requirements

3.1.1 Lookup services

A federation gateway look-up/tracker service must be available that allows a gateway to register and discover their neighbours. Such as service should record, among other things:

- gateway reachability information (public IP address if available, ports on which services are mapped, rendezvous server if behind a NAT etc.);
- physical location (to exploit services requiring radio reachability);
- gateway capabilities (available services, available storage space, available bandwidth, users information etc.);
- broadcast beacon-based identification for FIGARO gateways in the wireless neighbourhood.

3.1.2 AAA

An Authentication, Authorization, and Accounting (AAA) service is required for secure and accountable operation of the gateway federation, in most use cases. Federation-specific authentication mechanisms (such as Federated Group Keys) should be deployed on the AAA module.

3.1.3 Gateway management

An external federation module must be present on each gateway that supports well-defined signalling and communication protocols to exchange configuration and performance information. The gateway

must build and maintain a distributed state machine coherent among all gateways in the same federation. The gateway must rely on an optimized protocol to reduce overhead when exchanging information between gateways.

In particular, we have identified the following requirements:

- *An inter-gateway signalling protocol* that:
  - exchange traffic load levels
  - request offloading and wake-up procedures;
  - allow the setup of network connections from federation gateway to the home gateway;
  - perform setup between gateways from different federations;
- *A communication channel* (in-band or out-of-band) that enables sharing of the selected information;
- *Overlay setup and management* that enables to perform network abstraction.

3.2 Local gateway requirements

3.2.1 Networking

3.2.1.1 Management

A set of network "management" functions are needed for network operation of some use cases. More specifically:

- A *network management service* that
  - allows to prioritize between different types of data traffic.
  - *includes a network optimization engine* that processes the local and foreign wireless network and monitoring information.
  - can continuously modify its wireless network configuration (e.g., based on the optimization engine output).
- *A event-loop manager* is needed to receive and perform processing, storage and adaptation of the data received on the IEEE802.15.4 radio according to Zigbee protocol;
- *A HTTP proxy analyser* should be running on the gateway to intercept streaming request and perform multi-path switching.

3.2.1.2 Policies

There is a need to enforce fairness among users and gateways:

- Backhaul aggregation should not maximize the individual station throughput without taking fairness into account (this can lead to grossly unfair throughput distributions, which can discourage user participation).
- Fairness mechanisms need to provide QoS to AP owners, since they always have priority over the neighbours' traffic. This applies to most neighbourhood federation scenarios.
- Fairness mechanisms must also request input from monitoring services to adapt fast to sudden changes in traffic without losing its QoS/fairness properties.
- Ideally, there should be some prioritization scheme that rewards users that contribute more of their bandwidth to the system by providing them more benefit. Alternatively a credit scheme could give strong incentives to the users to participate (maybe beyond energy savings).

3.2.1.3 Networking Protocol Support

Naturally, we assume that the FIGARO gateways support a rich set of networking technologies and protocols. A few specific requirements were identified through the use cases, namely:

- multi-path transport protocols, such as CMT-SCTP or MPTCP, for multi-path adaptive video streaming.
- VPN protocols and architectures to allow remote access to the federation.
- *a Media-independent information service (MIIS*) to provide a framework through which a user terminal can acquire network information within a geographical area to facilitate handovers;
- *IEEE 802.21* and *a mobility management protocol* at the network layer (e.g., Mobile IP or similar) to enable heterogeneous handover.
- *ZigBee hardware radio interface* should be present in the gateway to insure hardware radio and protocol compatibility.

3.2.1.4 Lower layer control

The gateway lower layers should be capable of detecting inactivity and switch-off unused resources, including whole modules as low as the Physical Layer. In particular:

- *a detection of inactivity at low layers* should be available, and
- *a modular sleep mode* for the different component is necessary to benefit from eco-management.
- *wake-on-lan reliable* procedures are needed to perform efficient load-balancing and eco-management.
- *ZigBee hardware radio interface* should be present in the gateway to insure hardware radio and protocol compatibility.

3.2.2 Monitoring

Network modules must be able to access accurate and detailed network monitoring data for the home network and the access network. In addition, the quality of the inter-gateway communication link with neighbouring gateways is monitored or computed from neighbourhood gateway locations. An external federation module must be able to access and share certain monitoring data with other federation gateways.

More specifically, the following requirements were identified:

- *Traffic monitoring* is needed to be able to react to traffic condition change.
- *Certain traffic monitoring* of the home network should be continuously performed;
- *A data collection and aggregation service* should expose data to selected federation members involved in a certain operation;
- A protocol to request/publish data collection info should be available on the gateway;
- *A monitoring services should be able to*
    - *monitor the link quality* of the selected neighbouring gateways.
    - accept requests from applications to monitor or intercept a particular type of traffic.
    - notify an application/service about the presence of a given type of traffic.
    - detect the start of a video stream.
    - provide information about a certain video streaming, either in real time monitoring or simply by accessing pre-recorded information in a data base.
    - provide network performance statistics, such as frame error rate, available bandwidth, and MAC layer achievable goodput, etc.

- Optionally, for load-balancing and eco-management to be most efficient it would be advisable to maintain or acquire an electromagnetic map of the building and have indoor localization capabilities on the terminals.

Please note that a discussion about monitoring and a specification of monitoring metrics and data formats are available in FIGARO Deliverable D2.1 "Report on the specification of metrics and data formats". We refer the reader to that document for additional details.

3.2.3 Control Network Proxy

The home gateway must have a IEEE 802.15.4 interface and be able to act as a ZigBee bridge. This is a requirement for most current energy/home automation/e-health services. Although such services may over time migrate to IP, we keep ZigBee as a requirement at this phase of the project. Please note that FIGARO WP5 addresses aspects related to cross-sector services and internal federation, wherefore we do not elaborate further on this topic in this document.

3.2.4 Internal Federation Control

The sensor data collection use-case presented in this document relies on the capability to access the sensor data from IP connected devices. Further use-cases originating from FIGARO WP5 through the course of the project might input additional requirements to manage access control to devices and sensor data.

3.3 Services/applications

There are a few requirements related to networking-related services and applications:

- For the multi-path streaming use-case, an HTTP Streaming application must be deployed and traversing the federated gateway infrastructure. The gateway must run a multi-path streaming service composed of an HTTP proxy capable of triggering the multi-path communication and an interception mechanism registered with the network module capable of selectively intercepting the desired (video streaming) request.
- For the video streaming optimization use-case, a video streaming application must be deployed over the gateway and the terminal.
- A "neighbourhood federation optimization" module must be running on all gateways involved in this neighbourhood optimization.

3.4 Platform requirements

Generally speaking, it is preferable to favour gateway-only modifications to support legacy devices. Since all use-cases will need to scale to a potentially huge number of overlapping gateways, their control should be distributed among their participants. Also, they should be realizable with a minimal intervention on the existing architecture of broadband access networks.
Although the hardware requirements for FIGARO testbed equipments are handled by FIGARO WP1, we highlight a few requirements, from the viewpoint of WP3, related to hardware and resource virtualization

3.4.1 Hardware

For the eco management and multi-path streaming use-cases a *secondary wireless communication interface* is needed. Similarly, in the MIH use-case, the mobile node needs a dual interface (3G and Wi-Fi). For the sensor data collection, a *ZigBee hardware radio interface* should be present in the gateway to insure hardware radio and protocol compatibility. Furthermore, we assume that our FIGARO gateway is equipped with most standard networking technologies.

3.4.2 Resource virtualization

The gateways need to support some form of network virtualization for the LAN interface to provide isolation, allocation, and control. In the case of WiFi this translates into multiple virtual ESSIDs. This is needed to separate traffic from the different classes of users and services.

4 FUNCTIONAL MODULES AND INTERFACES

In the previous sections we have detailed the requirements put by our use-cases on the architecture modules. The purpose of this section is to define the high-level interfaces of the modules taking into account the aforementioned requirements. Figure 14 below summarizes the interactions between the different modules, which we will discuss in the following sub-sections.

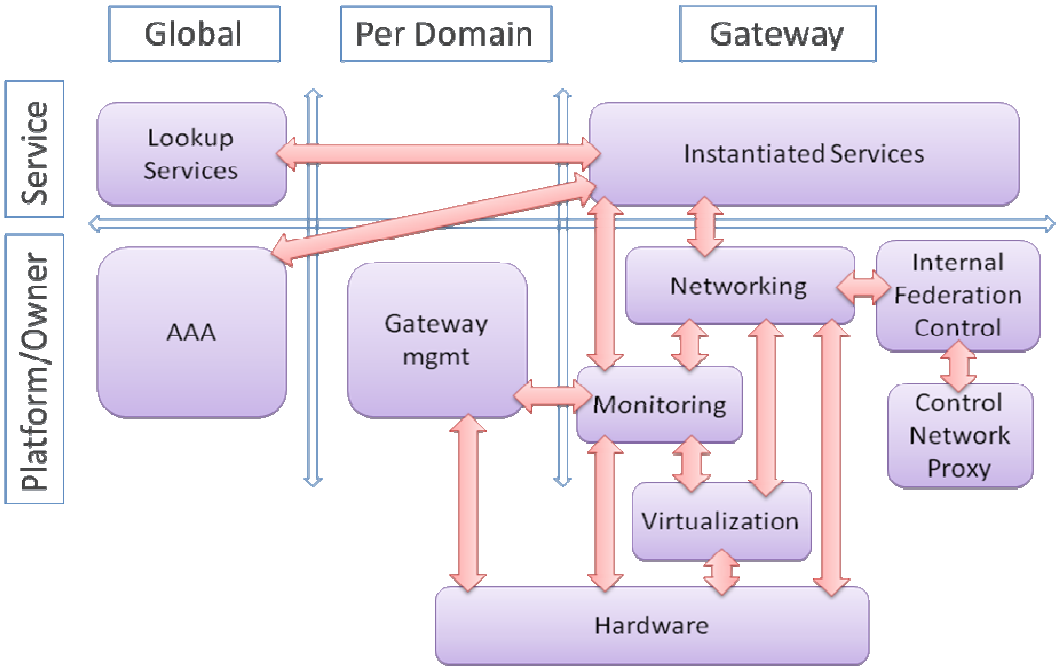

Figure 14 - Functional modules interactions

4.1 Lookup services

The Lookup services interface can be remotely accessed from the gateway services. The functions that need to be exposed by the Lookup Services are essentially registration and lookup of neighbour gateways, summarized in the following high-level interface:

- Gateway registration: allows a gateway to register itself with its location so as to be reachable from other gateways
- Gateway lookup: allows to search gateways with specified characteristics e.g. proximity of a given location

4.2 AAA (authentication, authorization and accounting)

Typical Authentication, Authorization, and Accounting (AAA) functionality is expected for secure and accountable operation of the gateway federation. FIGARO do not impose any specific requirements on standard AAA services.

4.3 Gateway management

The gateway management module needs to support the external federation communication protocols to exchange configuration and performance information with the rest of the federation. It should implement a subscription-based mechanism to collect critical monitoring information from the Monitoring module.
Furthermore, the gateway management performs hardware resource management, by managing power state mode of any component (wireless and wired interface), radio activation and deactivation, as well as main CPU throttling. It should implement advanced energy-management features that allow the gateway to switch itself off and come back online through a cheap Wake-on WLAN module.
The service deployment aspect of the gateway management module is not specifically impacted by our networking use-cases.

4.4 Instantiated services

Instantiated services may need to receive notifications from underlying modules (Monitoring, Networking or Network infrastructure). To do so they implement a subscription-based mechanism to get notified about a selected set of events.

4.5 Network management

The network module allows controlling of network adapters with actions such as:

- Switching on/off a given interface
- Setting and reading physical layer communication parameters
- Creating/destroying a virtual interface bound to a given physical interface

Network infrastructure can be discovered and specific information can be queried by the services.
Network events are exposed by a subscription-based mechanism allowing subscribers to filter out undesired events.
Hooks for selected types of traffic can be requested such that Instantiated services can receive and inspect the traffic.

4.6 Monitoring

This module is responsible for aggregation and processing of monitoring data. As such it allows querying of information using operations like

- Read selected or summary data relative to local/remote gateway.
- Collect a specific metric for a given set of gateways known to be close by.

Thresholds can be set by other modules on selected metrics to receive notifications using a subscription-based mechanism. We refer the reader to FIGARO deliverable D2.1 1 “Report on the specification of metrics and data formats” for a detailed discussion about the monitoring module.

4.7 Control Network Proxy

This module acts as a bridge between the sensors and the IP world. It allows controlling filtering and aggregation settings for messages in the sensor world. The sensor data is made available through a subscription-based mechanism.

4.8 Internal Federation Control

This module interfaces the control network to the Monitoring module. As such it exposes event-based data through a subscription-based mechanism allowing control data to be selectively received.

5 ROADMAP

As presented in the previous sections the complexity and the inter-dependencies of the modules vary greatly. Due to the nature of WP3 and the central position of the Networking module, we will start by developing this module. In a second step we will develop the Network Infrastructure and Gateway Management modules to favour early experimentation with an embryonic federation platform. The remaining modules will be built roughly in parallel in a subsequent step (to be refined during Task 3.2) and initial prototypes of all modules will be available at milestone M3.2. Finally all modules should be finalized and integrated during Task 3.3 towards the final federated network demonstrator ending with milestone M3.3.

The corresponding Gantt chart is represented on Figure 15

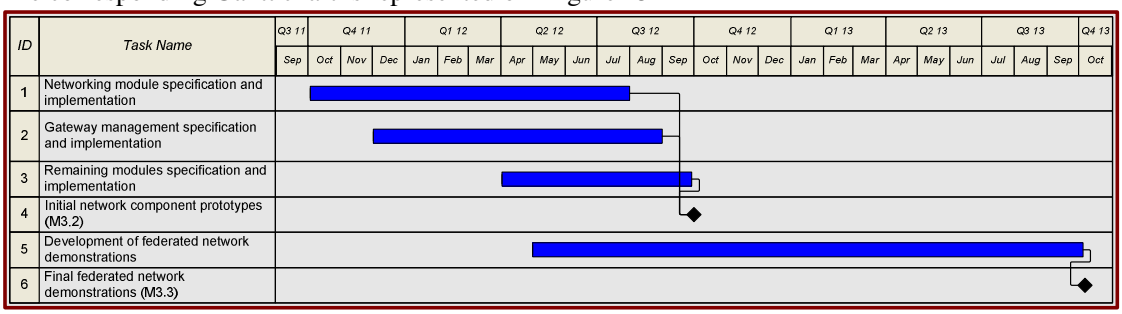

Figure 15- Networking modules and architecture development

6 SUMMARY

In this deliverable we have detailed the rich set of networking use cases considered within the FIGARO project. These use-cases have been used to derive important requirements that impact the FIGARO networking frame in particular, and the FIGARO architecture in general. We analyzed the requirements and categorized them into groups of functional modules. We organized these functional building blocks into a draft architecture as seen by this WP3. Furthermore, we provide a first discussion on the interactions and interfaces between the modules. Further details and development of these modules, their organization, and their interfaces are expected through the course of the project. Finally, we presented a high-level roadmap including a development plan towards completion of the federated networking demonstrations.