Important notice

This technical specification is the result of a cooperative effort undertaken at the direction of Cable Europe Labs for the benefit of the cable industry and its customers. This document may contain references to other documents not owned or controlled by Cable Europe Labs. Use and understanding of this document may require access to such other documents.

Designing, manufacturing, distributing, using, selling, or servicing products, or providing services, based on this document may require intellectual property licenses from third parties for technology referenced in this document.

Neither Cable Europe Labs nor any member company is responsible to any party for any liability of any nature whatsoever resulting from or arising out of use or reliance upon this document, or any document referenced herein. This document is furnished on an "AS IS" basis and neither Cable Europe Labs nor its members provides any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement, or fitness for a particular purpose of this document, or any document referenced herein.

Individual copies of the present document can be downloaded from:

http://www.cable-europe.eu/labs

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF) as maintained by the secretariat of Cable Europe Labs.

Users of the present document should be aware that the document may be subject to revision or change of status. If you find errors in the present document, please send your comment to the following services:

labs@cable-europe.eu

Copyright Notification

No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.

© Cable Europe Labs 2012.
All rights reserved.
### Contents

1. Scope ........................................................................................................................................... 6

2. Use Cases ....................................................................................................................................... 7
   2.1 Use case: A Community Wi-Fi Service .................................................................................... 7
      2.1.1 Description ......................................................................................................................... 7
      2.1.2 Service Advertisement ...................................................................................................... 7
      2.1.3 Authentication .................................................................................................................... 7
      2.1.4 Protection of private user ................................................................................................. 7
      2.1.5 Protection of the service .................................................................................................... 7
      2.1.6 Tunnel .............................................................................................................................. 8
   2.1.7 IPv4 Addresses for client Wi-Fi devices .............................................................................. 8
   2.2 Use case: Traffic Isolation ......................................................................................................... 9
      2.2.1 Description ......................................................................................................................... 9
      2.2.2 Private (W)LAN .................................................................................................................. 9
      2.2.3 Public SSIDs ...................................................................................................................... 9
      2.2.4 Broadcast / multicast traffic ............................................................................................. 9
      2.2.4.1 Traffic from client Wi-Fi device ..................................................................................... 9
      2.2.4.2 Traffic to client Wi-Fi device (L2oGRE encapsulated) .................................................... 9
      2.2.4.3 Traffic to client Wi-Fi device (not L2oGRE encapsulated) ............................................. 10
   2.2.5 Multiple services ................................................................................................................. 10
   2.3 Use case: Roaming .................................................................................................................... 10
      2.3.1 Description ......................................................................................................................... 10
      2.3.2 Authentication .................................................................................................................... 10
      2.3.3 IP Provisioning .................................................................................................................. 10
      2.3.4 Other service providers .................................................................................................... 10
      2.3.5 Accounting ....................................................................................................................... 10
      2.3.6 Interfaces between Home and Visited network ............................................................... 11
   2.4 Use case: Mobility ..................................................................................................................... 11
      2.4.1 Description ......................................................................................................................... 11
      2.4.2 IP address .......................................................................................................................... 12
      2.4.3 Traffic routing ..................................................................................................................... 12
      2.4.4 Authentication .................................................................................................................... 12
   2.5 Use case: Multiple simultaneous Wi-Fi based services .......................................................... 12
      2.5.1 Description ......................................................................................................................... 12
      2.5.2 Traffic separation within a tunnel ..................................................................................... 13
      2.5.3 EuroDOCSIS traffic separation ....................................................................................... 13
      2.5.4 Service parameters ............................................................................................................ 13
      2.5.5 QoS..................................................................................................................................... 13
   2.6 Use case: Lawful Intercept and Data Retention ......................................................................... 14
   2.7 Use case: L2 Tunneling ............................................................................................................ 14
      2.7.1 Description ......................................................................................................................... 14
      2.7.2 Wi-Fi Gateway Interfaces ................................................................................................. 15
      2.7.3 Wired LAN ....................................................................................................................... 15
      2.7.4 VPN ................................................................................................................................... 15
      2.7.5 Security/Trust relation ...................................................................................................... 15

3. System Requirements ................................................................................................................... 17
   3.1 Impact on Wi-Fi Gateway ......................................................................................................... 17
   3.2 Impact on CMTS ...................................................................................................................... 17
   3.3 Seamless Authentication ......................................................................................................... 17

4. System Architecture .................................................................................................................... 18
   4.1 High level architecture ........................................................................................................... 18
   4.2 Definition of the components involved ................................................................................. 18
      4.2.1 Wi-Fi Gateway ................................................................................................................... 18
      4.2.2 CMTS ................................................................................................................................ 18
      4.2.3 SoftGRE Tunnel Concentrator / Public Access Gateway ............................................. 18
      4.2.4 AAA Server/Proxy ............................................................................................................ 19
      4.2.5 Captive Portal .................................................................................................................... 19
      4.2.6 DHCP Server ..................................................................................................................... 20
      4.2.7 Application Server/Policy Server ..................................................................................... 20

© Cable Europe Labs
4.2.8 VPN Endpoint ................................................................. 20
4.3 Definition of the interfaces and protocols involved ................................................................. 20
4.3.1 EuroDOCSIS ................................................................. 20
4.3.2 802.11 ................................................................. 20
4.3.3 DHCPv4 ................................................................. 20
4.3.4 RADIUS ................................................................. 21
4.3.5 HTTP(S) ................................................................. 21
4.3.6 SNMP ................................................................. 21
4.3.7 COPS ................................................................. 21
4.4 Wi-Fi Gateway Reference Architecture .................................................................................. 21
4.4.1 Interfaces .................................................................. 21
4.4.2 Multiple SSIDs ........................................................... 22
4.4.3 DHCP intercept parameters .................................................. 22
4.4.4 Traffic classification and encapsulation (upstream) .......................................................... 22
4.4.4.1 NAT / Bridge .................................................. 22
4.4.4.2 Classifiers .......................................................... 22
4.4.4.3 Policies ............................................................... 23
4.4.4.3.1 Tunnel endpoint ...................................... 23
4.4.4.3.2 VLAN .......................................................... 23
4.4.4.3.3 TOS set .......................................................... 23
4.4.4.4 Provisioning ...................................................... 24
4.4.5 Traffic decapsulation and forwarding (downstream) ............................................................ 24
4.4.5.1 Destination MAC address (outer header) equals eRouter tunneling interface MAC address .... 24
4.4.5.2 Destination MAC address equals eRouter primary interface MAC address .................. 25
4.4.5.3 Destination MAC address does not equal eRouter (primary/tunneling interface) MAC address 25
4.4.6 IP fragmentation ...................................................... 25
4.4.7 DHCP client ............................................................. 25
4.4.7.1 NAT/Router Interface ........................................... 25
4.4.7.2 Tunneling Interface ............................................... 25
4.4.8 RADIUS client ........................................................... 26
4.4.9 Wi-Fi bandwidth management ................................................................. 26
4.4.9.1 WMM QoS ...................................................... 26
4.4.9.2 Backwards compatibility ............................................ 27
4.4.10 Wi-Fi Radar compatibility .................................................. 27
4.5 Known constraints ............................................................ 28
5 List of References ...................................................................... 29
6 Appendix A: Impact of IPv6 .......................................................... 31
6.1 IPv6 Addresses for client devices ......................................................................................... 31
6.2 Multicast traffic leakage ......................................................................................... 31
6.3 IPv6 classifiers ......................................................................................... 31
List of figures
Figure 1: Use Case: Community Wi-Fi Service ................................................................. 8
Figure 2: Use Case: Traffic Isolation ................................................................................. 9
Figure 3: Use Case: Roaming ......................................................................................... 11
Figure 4: Use Case: Client Wi-Fi device mobility ......................................................... 12
Figure 5: Use Case: Multiple Wi-Fi based services ...................................................... 14
Figure 6: Use case: L2 Tunneling .................................................................................. 15
Figure 7: Architecture Overview ................................................................................... 19
Figure 8: Traffic Classification and Forwarding .............................................................. 23
Figure 9: Packet Encapsulation (example) ................................................................. 24

List of tables
Table 1: DSCP to WMM Traffic Class Mapping .......................................................... 26
1 Scope

This document describes an end-to-end solution and requirements for the Wi-Fi gateway that supports adding new (wireless) services over a cable operator’s network with Wi-Fi gateways.

Support of a community Wi-Fi service was one of the main drivers for this development, but the architecture and requirements provide support for other Wi-Fi based services as well.

In a community Wi-Fi service, subscribers are granted a best-effort internet connection through the community Wi-Fi SSID, broadcasted by any of the Wi-Fi gateways, deployed by the cable operator. This type of service must at least support roaming among cable operator Wi-Fi networks but should also be applicable to non-cable operator Wi-Fi networks. In case of roaming, the roaming partner’s network is called the visited network, while the cable operator’s network of the subscriber is called the home network.

Although an end-to-end architecture is defined in this document and the required functionality is described for each of the components in this architecture, only the Wi-Fi gateway itself is fully specified. Interoperability between different types of Wi-Fi gateways is the main purpose of this document.

As a secondary objective for this document, the interface between home and visited network is defined in order to allow a standard way of letting users authenticate to these wireless service(s).

Lawful intercept and data retention mechanisms are outside the scope of this document. This means that dedicated components, required for this type of functionality, will not be described in this document; however, requirements will be set for the components in the described architecture to support lawful intercept and data retention where needed.

The document makes a distinction between 2 phases of deployment. The requirements, described for phase 1 are applicable to existing hardware in the field and are applicable within a reasonable time frame. Phase 2 describes the next step and allows us to describe enhancements to the model, making use of technologies that are not yet available at the time of writing (like Hotspot 2.0 capable devices, the evolvement of softGRE and dynamic provisioned services).

The document describes an architecture and requirements that are applicable to IPv4 networks. Requirements for IPv6 network are written in appendix TBC, describing the extra requirements and potential pitfalls when migrating from IPv4 to IPv6.

The Wi-Fi gateway reference architecture, described in this document still supports a private Wi-Fi network on the Wi-Fi gateway also, which will be deployed as a separate (private) SSID that is configurable by the subscriber.

Based on this document, a separate requirements document is written which will describe the requirements for the Wi-Fi gateway component. That document is written as a requirement gap analysis from the WR-SP-WIFI-GW-I02 document from CableLabs.
2 Use Cases

2.1 Use case: A Community Wi-Fi Service

2.1.1 Description

In this use case we build a Wi-Fi community service for the customers of the cable operator. The use case is described in Figure 1: Use Case: Community Wi-Fi Service.

A community Wi-Fi service is built using the customers’ Wi-Fi gateways that provide already a (private) Wi-Fi network for the customers. The idea is to add a new service to these Wi-Fi gateways, allowing customers to have a best-effort internet connection over Wi-Fi through any Wi-Fi gateway of the operator available.

2.1.2 Service Advertisement

Users that would like to connect to the internet through this community service, should be able to easily distinguish a Wi-Fi network providing this service among other Wi-Fi networks available.

2.1.3 Authentication

A user that connects to the service for the first time, should be provided with a clear login screen, asking the user for his credentials and these credentials must be checked against a central database with user credentials, located at the cable operator. Only in the case that this authentication step is successful, the user should get internet connectivity over this Wi-Fi network.

When the user connects for the second time to this service, the user’s client Wi-Fi device, should take care of the authentication and user credentials should not have to be re-entered.

In case an architecture is used with an open SSID coupled to a captive portal, this approach will not be possible and the user will have to re-enter his credentials each time he makes a new connection to the network, unless some kind of intelligent connection manager is available on the user’s client Wi-Fi device that takes care of this authentication through the captive portal.

Next to the model with the login screen to provide user credentials, the architecture must support the model where the user authenticates using other means also (user certificate, SIM card credentials).

The service must be supported on a Wi-Fi network with no security and a captive portal. The service must also be supported on a Wi-Fi network with WPA/WPA2 and 802.1X as authentication mechanism.

Security measurements must be in place to prevent the theft of user credentials by a man-in-the-middle attack.

2.1.4 Protection of private user

As the Wi-Fi gateway’s radio is a shared resource between multiple SSIDs, there is a need for requirements that make sure that the bandwidth, used by this community Wi-Fi service, does not limit the bandwidth that is reserved for the private traffic of the customer behind the Wi-Fi gateway. These requirements should apply to both the EuroDOCSIS and Wi-Fi connection.

2.1.5 Protection of the service

To prevent a user from inadvertently turning off the community service provided by the Wi-Fi gateway, fail-safe features are required for the configuration process.
The Wi-Fi gateway must support prohibiting the subscriber from disabling the access point radio as this would turn off all SSIDs. However, the Wi-Fi gateway must support disabling this feature, which implies allowing the subscriber to shut down the Wi-Fi radio. In the latter case, it is the responsibility of the operator to implement a polling mechanism to check the status of the Wi-Fi radio interface, in case this information is needed by the operator. The Wi-Fi gateway must provide a method for the subscriber to disable the wireless interface impacting only the subscriber’s SSID.

The Wi-Fi gateway must not impact or provide any information regarding the operator configured SSIDs when the subscriber configures the subscriber designated SSID. (references WR-SP-WIFI-GW-I02-120216)

2.1.6 Tunnel

All traffic from and to this community Wi-Fi SSID must be encapsulated in a layer2 GRE tunnel.

The provisioning of the layer2 tunnel endpoint is done through MIB-objects; these can be provided in the CM config-file or through SNMP. Optionally, the provisioning should also be possible via RADIUS attributes, which would allow a more dynamic behaviour of configured/used tunnel endpoints for a Wi-Fi gateway.

The AAA traffic (RADIUS) is routed outside of the tunnel. In case the tunnel concentrator needs information that resides in these RADIUS messages, the AAA server should have an interface to the tunnel concentrator. This interface, however, is not further described in this document.

2.1.7 IPv4 Addresses for client Wi-Fi devices

This service must support both private and public IPv4 ranges for client Wi-Fi devices that connect to the Wi-Fi network; however, the translation between private and public IP address (NAT) must not be performed by the Wi-Fi gateway as this would compromise any lawful intercept functionality.

Figure 1: Use Case: Community Wi-Fi Service
2.2 Use case: Traffic Isolation

2.2.1 Description

This use case describes the traffic isolation requirements that must apply on the multiple services/SSIDs that are deployed via the Wi-Fi gateway. Traffic isolation applies both between different users, using the same service as between a user, making use of a public service and the customer on the private (W)LAN network of the Wi-Fi gateway.

![Diagram of traffic isolation](image)

**Figure 2: Use Case: Traffic Isolation**

2.2.2 Private (W)LAN

There must be a clear separation of traffic between the private traffic (wireless and wired) and the traffic from the other services that are deployed via the Wi-Fi network on the Wi-Fi gateway.

2.2.3 Public SSIDs

There must not be any leakage of traffic between different SSIDs on the same Wi-Fi gateway.

2.2.4 Broadcast / multicast traffic

Broadcast/multicast block behaviours (upstream/downstream) must be configurable per SSID.

2.2.4.1 Traffic from client Wi-Fi device

Broadcast/multicast traffic from client Wi-Fi device to Wi-Fi gateway must only be forwarded in the upstream (HFC).

2.2.4.2 Traffic to client Wi-Fi device (L2oGRE encapsulated)

Broadcast/multicast traffic to client Wi-Fi devices must be blocked at the Wi-Fi gateway.

There is one exception from this rule and that is for DHCP Offer/Ack messages as these can be broadcast on the MAC layer and are needed for a successful DHCP sequence. In this case the
Wi-Fi gateway must convert the DHCP Offer/Ack broadcast messages to unicast messages and can use the Client MAC address field which is present in these messages.

2.2.4.3 Traffic to client Wi-Fi device (not L2oGRE encapsulated)

Traffic from and to the private SSID will not be L2oGRE encapsulated. If needed, other Wi-Fi based services could also be configured to not encapsulate the packets in a L2oGRE tunnel.

Broadcast/multicast traffic to client Wi-Fi devices must not be blocked at the Wi-Fi gateway as ARP-requests can come from the CMTS.

In this case it is not possible to establish complete traffic separation between different client Wi-Fi devices on the same SSID.

2.2.5 Multiple services

It must be possible to have the same level of separation of traffic between different Wi-Fi based services on the same SSID as between different SSIDs on a Wi-Fi gateway.

2.3 Use case: Roaming

2.3.1 Description

The use case, described here, depicts the model where multiple service providers agree to let customers roam between their networks.

As a definition, we name the network of the roaming partner that is used to get a connection the visited network and the network of the customer is called the home network.

2.3.2 Authentication

The home network must provide an RADIUS interface to allow the visited network to authenticate the user. Routing of authentication traffic from the visited network to the home network is done based on the realm name that needs to be present as part of the user credentials.

The user will have to re-enter his credentials the first time it connects to the service through a visited network. After this first time however, subsequent connections via the same visited network must not require re-entering user credentials, unless an architecture with a captive portal is used.

2.3.3 IP Provisioning

The roaming partner network provides IP address management and traffic routing for roaming subscribers.

2.3.4 Other service providers

The model should support other service providers (e.g. hotspot providers), next to cable operators.

2.3.5 Accounting

It must be possible to do accounting for the connections, made by a user, on visited networks, based on session time and session traffic volume.

For accounting purposes, the architecture must be able to detect ended sessions (due to a client disconnecting or idle time outs). This must be the responsibility of the visited network (Wi-Fi gateway).
2.3.6 Interfaces between Home and Visited network

It should be possible to forward both the authentication traffic and data traffic from the visited network to the home network. The interface to forward data traffic, however, is outside the scope of this document.

In case carrier-grade NAT is used in the visited network, there could be a potential issue with forwarding the data traffic to the home network. How this issue is solved is outside the scope of this document.

The home and visited network must provide an interface (RADIUS) to communicate accounting details. The architecture must also support an implementation with a central AAA Radius broker where the AAA proxy inside the visited network can send all RADIUS traffic to, coming from roaming subscribers.

![Figure 3: Use Case: Roaming](image)

2.4 Use case: Mobility

2.4.1 Description

This use case describes what is required when there are multiple overlapping Wi-Fi networks, deployed by the cable operator, and the user is capable of roaming from one Wi-Fi gateway to another within the same network of the cable operator.
2.4.2 IP address

When the client Wi-Fi device roams from one Wi-Fi gateway to another, without losing connection (which is only possible when SSID stays the same), it must be possible to keep the same IP address for the client Wi-Fi device.

An additional requirement here could be that all Wi-Fi gateways that broadcast a specific public SSID, should support all Wi-Fi based services that are possible on this SSID. If not, the client Wi-Fi device could decide to roam to another Wi-Fi gateway that broadcasts the same SSID and could get stuck because the service that it was using on the first Wi-Fi gateway is not available on the second one.

2.4.3 Traffic routing

The cable operator’s network must be capable of detecting this change and must be able to re-route the traffic, intended for the client Wi-Fi device, to the correct Wi-Fi gateway.

2.4.4 Authentication

The user should not have to re-enter his credentials when arriving on the new Wi-Fi gateway.

---

2.5 Use case: Multiple simultaneous Wi-Fi based services

2.5.1 Description

The use case, described in this section, deals with the possibility of deploying multiple Wi-Fi based services on a Wi-Fi gateway.

It must be possible to identify the service at the AAA server by including extra information in the RADIUS messages, destined for the AAA server. Identification may be useful to identify authentication mechanisms, QoS parameters, forwarding parameters, ...

There are 3 possible ways of identifying a service at the AAA server:
- The service is deployed on a separate SSID (SSID is included in RADIUS messages)
- The service requires separate user credentials (with another realm)
- The service can be chosen via a captive portal which is shared among different services. In this case the captive portal is responsible for adding extra options to the RADIUS messages to the AAA server to identify the service.

The identification of the service at the AAA server can be a single one from the list above or a combination of them.

The services itself are outside the scope of this document; however a general architecture is described in this document.

The figure describes a general model with 2 services deployed: the community Wi-Fi service, described in one of the previous use cases and another, general, Wi-Fi based service that supports dynamic QoS, depicted by the application/policy server and the second client Wi-Fi device.

2.5.2 Traffic separation within a tunnel

It should be possible to identify multiple services within a single tunnel. The Wi-Fi gateway must at least support VLAN tagging the traffic before it is tunneled.

2.5.3 EuroDOCSIS traffic separation

It should be possible to define a separate service flow to run a specific Wi-Fi based service over, even if multiple of these services run over the same tunnel. In that case we will use the TOS bits from the outer IP header to identify the service and classify it to a specific service flow.

2.5.4 Service parameters

It must be possible to define, for each Wi-Fi based service separately, the SSID, the tunnel endpoint, a TOS-bits definition (for the outer IP header if tunnelling is used) and a VLAN id (for the inner 802.3 packet if tunnelling is used).

The selection of a SSID to run the Wi-Fi based service over, implies Wi-Fi security mode and defines if the traffic for this service is bridged/NAT, as these parameters can only be defined per SSID.

Each Wi-Fi based service can have its own service flow parameters and service flow classifiers.

2.5.5 QoS

It should be possible to define different QoS-parameters for each different service; however, it depends on the specific nature of the Wi-Fi based service that is being deployed, if QoS is needed or not.

For the first phase, described by this document, only static configuration of QoS must be supported, For QoS on the (Euro-)DOCSIS network, this means that the configuration is done through the CM config file.

In the second phase also dynamic QoS should also be possible and set up only when users make use of a particular service. On EuroDOCSIS, a policy server can be used for this purpose, making use of the COPS protocol to dynamically add/change/delete service flows/classifiers.

In order to realize QoS on the Wi-Fi part of the network, for traffic from the Wi-Fi gateway to the client Wi-Fi devices, the Wi-Fi gateway must support WMM which allows prioritization of traffic.
QoS on the wireless traffic from client Wi-Fi devices to the Wi-Fi gateway is outside the scope of this document.

![Diagram of Wi-Fi network](image)

**Figure 5: Use Case: Multiple Wi-Fi based services**

### 2.6 Use case: Lawful Intercept and Data Retention

This use case is out of scope for this document.

### 2.7 Use case: L2 Tunneling

#### 2.7.1 Description

The use case, described in this section, deals with the possibility of tunneling L2 traffic from client devices, connected to the Wi-Fi gateway, to a remote network.

It must be possible to configure the Wi-Fi gateway to forward all L2 traffic from the client devices (including client devices, connected through a wired interface), connected to the Wi-Fi gateway, through a tunnel, to a remote network.

In case the Wi-Fi gateway behaves in bridged mode (no NAT/router functionality enabled), this includes all DHCP traffic from/to the client devices. As such, the DHCP server for these client devices needs to be located in the remote network.

In case the NAT/router functionality is enabled on the Wi-Fi gateway, the NAT/router interface of the Wi-Fi gateway behaves as a single client device for the Wi-Fi gateway and, as such, it must be possible to tunnel all traffic from this client device.

In this case, the Wi-Fi gateway, or more precise the router inside the Wi-Fi gateway, will act as the local DHCP server and hands out (private) IP addresses to client devices, connected to it.
2.7.2 Wi-Fi Gateway Interfaces

As the Wi-Fi gateway bridges the gap between the core network and the remote network, some of its parts must be accessible (for configuration/monitoring purposes) from the core network, others from the remote network.

2.7.3 Wired LAN

As it must be possible to tunnel all L2 traffic to the remote network, the Wi-Fi gateway must support tunneling traffic from/to its ethernet interfaces also (next to the traffic from/to its wireless interface(s)).

2.7.4 VPN

To tunnel the L2 traffic, received on the tunnel concentrator from the client devices behind the Wi-Fi gateway, to the remote network, a VPN solution should be used.

The technical requirements for this VPN solution are outside scope for this document.

2.7.5 Security/Trust relation

In this use case, there is no pre-authentication in the form of 802.1x (EAP/RADIUS) as used in the Community WiFi use case for instance. Because the tunnel (GRE) is stateless and does not include any means of signaling, an alternative method is required to build a trust relation between the Wi-Fi gateway and the core network (tunnel concentrator/AAA server).
The proposed scenario is that the MSO (core network) provisions a security key in the cable modem config file. This key, together with the CM_MAC must then be inserted in option 82 of the client DHCP discover, which is tunneled to the tunnel concentrator.

This option 82 in the DHCP discover will trigger the tunnel concentrator to send a Access-Request message to the AAA server and as such, the AAA server can check if the request is coming from a ‘trusted’ HGW before the request is relayed to the remote network. If the check fails, the AAA server will send a Access-Reject and the tunnel concentrator will drop the DHCP packets causing the DHCP transaction to fail.

REMARK: As the security key is sent via the CM config file, it is recommended to use EAE (early authentication and encryption) to protect theft of this security key.
3 System Requirements

3.1 Impact on Wi-Fi Gateway

Extra functionality (especially the classification/forwarding/encapsulation mechanisms and possible fragmentation/reassembly), needed on the Wi-Fi gateway to support the described use cases, must not have any impact on the performance of the Wi-Fi gateway.

The maximum achievable throughput in case any kind of tunneling (GRE/VLAN), NAT or fragmentation/reassembly is enabled, must equal the maximum speeds offered by operators today and in the near future in their premium subscriptions.

3.2 Impact on CMTS

The CMTS must be agnostic to these new services, at least for the first phase, described by this document.

3.3 Seamless Authentication

A user that connects to the service for the first time should be provided with a clear login screen, asking the user for his credentials and these credentials must be checked against a central database with user credentials, located at the cable operator.

Next to the model with the login screen to provide user credentials, the architecture must support the model where the user authenticates using other means also (certificate, SIM card credentials).

When the user connects for the second time to this service, the user’s client Wi-Fi device, should take care of the authentication and user credentials should not have to be re-entered, unless an architecture is deployed with an open SSID coupled to a captive portal. In the case of an architecture with a captive portal, this kind of behaviour is only possible when using some kind of intelligent connection manager, installed on the client Wi-Fi device that takes care of this authentication through the captive portal.

The user should not have to re-enter his credentials when directly roaming between different Wi-Fi gateways on cable operator’s network. Again, this requirement can only be fulfilled in case an architecture is used with an secured SSID (WPA/WPA2-Enterprise)

The user will have to re-enter his credentials the first time it connects to the service through a visited network. After this first time however, subsequent connections via the same visited network must not require re-entering user credentials.

Routing of authentication traffic from the visited network to the home network is done based on the realm name that needs to be present as part of the user credentials.
4 System Architecture

4.1 High level architecture

The architecture describes the different components that are needed to provide the services described in the paragraph 2. Some of the components described may be optional, depending on the services that are provided. The function of each component in the architecture is further described in paragraph 4.2.

4.2 Definition of the components involved

4.2.1 Wi-Fi Gateway

The Wi-Fi Gateway (GW) provides the 802.11 air interface. The GW integrates an 802.11 Access Point (AP) with a EuroDOCSIS cable modem. Open and secured SSIDs are provided.

The Wi-Fi GW must also provide a RADIUS signalling client in support of AAA functions.

The Wi-Fi GW blocks unauthorized traffic.

The Wi-Fi GW must be capable of detecting new/ended sessions with client Wi-Fi devices.

The Wi-Fi GW must implement router functionality (NAT, firewall, ...)

The Wi-Fi GW must be capable of classifying traffic and, if configured, encapsulate the traffic to send it over one or more SoftGRE tunnels. This classification and forwarding functionality must not have any impact on the performance of the Wi-Fi GW.

The Wi-Fi GW must support 802.1Q, again, without any performance impact.

The Wi-Fi GW must be capable of DHCP snooping to add/override extra DHCP options for the DHCP server.

The Wi-Fi GW must support WMM to prioritize Wi-Fi traffic to client Wi-Fi devices.

4.2.2 CMTS

The CMTS controls access and use of the EuroDOCSIS access network.

4.2.3 SoftGRE Tunnel Concentrator / Public Access Gateway

The Public Access Gateway provides an interface to the internet for roamed in subscriber traffic.

A SoftGRE Tunnel Concentrator serves as an endpoint for a SoftGRE tunnel between the endpoint and the Wi-Fi GWs.

When the tunnel concentrator is linked to a service (SSID) that requires authentication (secure SSID or open SSID with a captive portal), it should have an interface to an AAA server/proxy.

The tunnel concentrator must also implement the inter-AP mobility, i.e. when a subscriber roams between Wi-Fi GWs within the same network.
4.2.4 AAA Server/Proxy

The AAA server contains the subscriber profile of Wi-Fi subscribers or has an interface to a database that contains this information.

It receives AAA signalling from the Wi-Fi GWs and authenticates the subscriber.

It can also receive AAA signalling from the visited AAA proxy and authenticates the subscriber.

It also receives usages reports from the visited network AAA proxy to perform accounting.

The AAA server needs to establish a security association with the visited network AAA proxy.

Routing between visited network AAA proxy and home network AAA server is done based on the realm name that needs to be part of the username, provided by the subscribers during the authentication process on the visited network.

The AAA server is also used to establish a trust relation between the Wi-Fi GW and the Tunnel Concentrator.

4.2.5 Captive Portal

The captive portal provides a sign in web page for subscribers on a clear SSID. The captive portal sends user credentials to a network component that provides the AAA RADIUS client or use the RADIUS protocol itself to contact the AAA server/proxy.

Content displayed to the user during sign in may be provided or hosted by the visited network, or a combination of visited and home networks.
The organization of content displayed to the user is beyond the scope of this specification.

The selection of the Wi-Fi based service through the captive portal is outside the scope of this document.

4.2.6 DHCP Server

The DHCP server controls the IP addresses that are provided to the client devices that make use of these new services over Wi-Fi.

Both private and public IPv4 ranges are supported.

The DHCP Server should be able to distinguish DHCP Discover/Request messages from devices, using these services and should be able to distribute the configured IP ranges accordingly.

In case L2 tunneling is used, the DHCP server in the remote network is responsible for the distribution of IP addresses to client devices behind the Wi-Fi gateway (bridged mode) or to the primary eRouter interface of the Wi-Fi gateway (NAT/router mode).

4.2.7 Application Server/Policy Server

A Policy Server will be needed only when dynamic QoS needs to be setup when new services are deployed that require this functionality. The policy server uses the COPS protocol to communicate with the CMTS and initiate a DSx sequence between CMTS and Wi-Fi GW to setup/breakdown a dynamic service flow and classifiers.

4.2.8 VPN Endpoint

A VPN Endpoint is necessary when L2 traffic, arriving at the tunnel concentrator, needs to be forwarded to a remote network. A VPN is setup between the tunnel concentrator in the core network and a VPN Endpoint in the remote network.

The kind of VPN technology is used for this purpose is outside the scope of this document.

4.3 Definition of the interfaces and protocols involved

4.3.1 EuroDOCSIS

Data between eCM and CMTS is transported using the EuroDOCSIS protocol.

4.3.2 802.11

802.11 is the protocol used on the wireless layer between client Wi-Fi device and Wi-Fi gateway

4.3.3 DHCPv4

The DHCP protocol is used by the client devices to get an IP address.

In the case NAT is used on the Wi-Fi gateway (for the private SSID), the Wi-Fi gateway will need to act as an DHCP server to distribute the private IPv4 addresses to the client devices. In this case the Wi-Fi gateway will also act as a DHCP client to acquire a (public) ip address on its WAN interface.

In the case the traffic is bridged on the Wi-Fi gateway (for the public SSIDs), the DHCP messages from/to client devices are intercepted by the Wi-Fi gateway (which can add extra options) and forwarded.
4.3.4 RADIUS

The RADIUS protocol used in 3 situations:

- When the security mode of a public SSID is set to WPA/WPA2 Enterprise, EAP authentication messages are encapsulated in RADIUS messages in the path between Wi-Fi gateway and AAA server.
- When the security mode of a public SSID is set to open, RADIUS messages will be used between the captive portal and the AAA server to authenticate a user.
- The RADIUS protocol will also be used for accounting purposes, where the Wi-Fi gateway signals the start and end of a client session to the AAA server.

4.3.5 HTTP(S)

HTTP is the protocol used to transfer webpages to the browser on a client Wi-Fi device.

In case of an architecture with a captive portal, the secure version of HTTP, HTTPS, will be used to transfer the login page to the client Wi-Fi device and the credentials in the opposite direction.

HTTP can also be used to access the configuration-webpage of the eRouter in case it supports this.

4.3.6 SNMP

The SNMP protocol is used to make configuration adjustments to the eRouter or retrieve monitoring info from the eRouter.

4.3.7 COPS

COPS is the protocol used by the policy server to signal to CMTS that dynamic QoS (service flows/classifiers) are needed by a specific CM.

4.4 Wi-Fi Gateway Reference Architecture

4.4.1 Interfaces

In order to realize the requirement that some parts of the Wi-Fi Gateway must be accessible by the core network and others by the remote network (cfr. section 2.7), the Wi-Fi Gateway must provide following interfaces, with each interface having its own MAC address and IP stack (cfr. Figure 8):

- CM (RF) interface: MAC/IP address for the cable modem, used on the EuroDOCSIS layer. This is the main interface that must be used for configuration/monitoring/provisioning purposes of both the CM and eRouter interfaces. Configuration/provisioning must be available through SNMP or the CM config file. Monitoring must be available through SNMP.
- eRouter primary interface: MAC/IP address for the eRouter, used as WAN-interface in case NAT/router mode is enabled. This interface may also provide a basic configuration/monitoring interface for the eRouter part.
- eRouter tunneling interface: MAC/IP address for the eRouter, used as source/destination address for respectively upstream/downstream tunneled traffic, in case tunneling is enabled.

REMARK: The first (CM) and last (eRouter tunneling) interface are provisioned/accessible by the core network, the middle one (eRouter primary) can be provisioned/accessible through the tunnel by the remote network in the L2 tunneling use case.

For traffic separation and traffic forwarding configuration purposes, each SSID must be a separate identifiable interface, all ethernet ports together must be a separate identifiable interface and the eRouter primary interface must also be a separate identifiable interface.
Optionally, each ethernet port should be a separate identifiable interface.

4.4.2 Multiple SSIDs

In order to provide the client Wi-Fi devices the impression of multiple physical Access Points in the same area, multiple SSIDs on the same Wi-Fi gateway are used. All the SSIDs configured in a single Wi-Fi gateway share the same radio and the physical channel.

The Wi-Fi gateway must support at least four SSIDs using the multiple BSSID model (single SSID per beacon, multiple beacons, multiple BSSIDs).

The Wi-Fi gateway must support a residential subscriber or enterprise controlled SSID, managed by the subscriber via a local web page.

The Wi-Fi gateway must support independently configurable parameters on a per SSID basis that includes but is not limited to: the SSID name, security type, bridge mode/NAT and broadcast/multicast behaviour (section 2.2.4).

4.4.3 DHCP intercept parameters

The HGW must support adding/overriding options in the DHCP Discover/Request messages from client devices if configured to do so.

Independent configuration of these parameters must be possible per interface.

4.4.4 This information must at least include eCM MAC address (option 82.2) and SSID (option 60). The HGW must also support adding a security key to option 82 if such a key was provided via the CM configfile.

Traffic classification and encapsulation (upstream)

Figure 7 shows the reference architecture for the Wi-Fi gateway with respect to the traffic classification and encapsulation. The general idea is that traffic (NATted or bridged) will be classified and that the matched classifier will link to a policy, which defines the way the data packets are encapsulated before they are send upstream by the eCM.

4.4.4.1 NAT / Bridge

The Wi-Fi gateway must support NAT/bridge behavior configuration for each interface independently.

In case NAT is enabled for an interface, the NATted packets must have following source addresses:
- Source MAC address = eRouter (primary interface) MAC address
- Source IP address = eRouter (primary interface) IP address

4.4.4.2 Classifiers

Classification can be performed, based on the following parameters of the data traffic:
- Interface
  - SSID
  - Ethernet (port)
  - eRouter primary interface (NATted traffic)
- Source and/or destination MAC address
- Source and/or destination IP address (optional mask)
- IP protocol
- Source and/or destination UDP/TCP port number
4.4.4.3 Policies

A policy will define how packets are encapsulated/altered before forwarding them to the eCM. The items that define a policy are described in the sections below.

There are 2 policies with a special purpose:
- The default policy, which is the policy that is applied for packets that don’t match any classifier
- The drop policy, which drops the packets that match a classifier, attached to it.

Figure 8 shows the result of how a packet could look like after the policy is applied.

4.4.4.3.1 Tunnel endpoint

In case no tunnel endpoint is defined, no tunnelling is performed. Otherwise L2oGRE encapsulation of the packets is performed.

The protocol type in the GRE header must be set to “Transparent Ethernet Bridging” (0x6558).

The source IP address of the outer IP header must be the eRouter (tunneling interface) IP address.

REMARK: if the eRouter primary interface is choosen as classifier that links to a policy that defines a tunnel endpoint, all NATted/routed traffic from the eRouter will be tunneled through the same GRE tunnel. However, further classification for other forwarding policy items (like VLAN tagging) should be possible on these GRE-tunneled NATted/routed packets.

4.4.4.3.2 VLAN

In case a VLAN ID is defined, the VLAN header is attached to the packet before (optional) tunnel encapsulation is performed.

4.4.4.3.3 TOS set

The policy will define the value of the TOS bits in the IP header. In case the policy also defines a tunnel endpoint, this value will define the TOS bits in the outer IP header.

Figure 8: Traffic Classification and Forwarding
Figure 9: Packet Encapsulation (example)

4.4.4.4 Provisioning

The primary method to provision the classifiers and policies will be through MIBs which can be set via SNMP or via the CM config file.

A more dynamic method is to dynamically add/change/remove classifiers and link them to specific policies, based on VSA attributes in the RADIUS responses from the AAA server. This method is not required for the first phase, described by this document.

In the latter case, it’s the responsibility of the Wi-Fi gateway to notify the AAA server when a client Wi-Fi device disconnects (RADIUS accounting) and it’s the responsibility of the AAA server to remove the classifier on the Wi-Fi gateway that was specifically (dynamically) added for that client Wi-Fi device.

4.4.5 Traffic decapsulation and forwarding (downstream)

4.4.5.1 Destination MAC address (outer header) equals eRouter tunneling interface MAC address

In this situation, the packet is L2oGRE.

In this case, the protocol type in the outer IP header equals 47 (GRE), the Wi-Fi gateway must first decapsulate the packet before further processing it.

In case the inner packet is VLAN tagged, the Wi-Fi gateway must strip off the VLAN tag.

In case the inner packet is NATted, the Wi-Fi gateway must forward the inner packet, based on the information (TCP/UDP port numbers) in the header and its NAT mapping table.
The inner packet is forwarded on the Wi-Fi with the correct SSID, based on the client-MAC-address-to-SSID mapping that is maintained by the Wi-Fi gateway.

4.4.5.2 Destination MAC address equals eRouter primary interface MAC address

The Wi-Fi gateway must forward the packet, based on the information (TCP/UDP port numbers) in the header of the packet and its NAT mapping table or forward it to its local IP stack in case it is not a NATted packet, but instead, a packet directly addressed to the eRouter (HTTP/SNMP)

4.4.5.3 Destination MAC address does not equal eRouter (primary/tunneling interface) MAC address

In this situation, the packet is bridged and not L2oGRE encapsulated.

In case the packet is VLAN tagged, the Wi-Fi gateway must strip off the VLAN tag.

The packet is forwarded on the Wi-Fi with the correct SSID, based on the client-MAC-address-to-SSID mapping that is maintained by the Wi-Fi gateway.

4.4.6 IP fragmentation

Because GRE encapsulation and 802.1Q VLAN tagging could lead to IP fragmentation on the EuroDOCSIS interface (MTU limitation), the Wi-Fi gateway must support IP fragmentation.

If fragmentation is needed in the upstream direction, it must be performed after GRE encapsulation in order to not drop packets with the DF bit set.

In the downstream direction reassembly of fragmented GRE-encapsulated packets must be supported up to 2 fragments per configured GRE tunnel endpoint.

In the upstream direction, if the Wi-Fi gateway receives fragmented packets, it must not drop/reassemble them before GRE encapsulation is performed.

In the downstream direction, the Wi-Fi gateway must not drop/reassemble inner fragmented packets.

The Wi-Fi gateway must support disabling IP fragmentation. In case IP fragmentation is disabled, upstream packets that exceed the MTU of the EuroDOCSIS interface of the Wi-Fi gateway, will be dropped by the Wi-Fi gateway.

4.4.7 DHCP client

4.4.7.1 NAT/Router Interface

For NAT/router purposes, the Wi-Fi gateway must be capable of performing DHCP on its eRouter primary interface.

The Wi-Fi gateway must support adding extra options to the DHCP messages sent from this eRouter primary interface.

These options must at least include, for the L2 tunnel use case, a security key (option 82) if such a key was provided via the CM configfile.

4.4.7.2 Tunneling Interface

For tunneling purposes, the Wi-Fi gateway must be capable of performing DHCP on its eRouter tunneling interface.

The Wi-Fi gateway must support adding extra options to the DHCP messages sent from this eRouter tunneling interface.
These options must at least include a value (option ?) indicating that this is DHCP for an eRouter tunneling interface.

4.4.8 RADIUS client

The Wi-Fi GW must implement a RADIUS client to the following purposes:

- When the security mode of a public SSID is set to WPA/WPA2 Enterprise, EAP authentication messages are encapsulated in RADIUS messages in the path between Wi-Fi GW and AAA server
- For accounting purposes, where the Wi-Fi GW signals the start and end of a client session to the AAA server

RADIUS messages must be sent with source IP address, the IP address of the eROUTER primary interface.

REMARK: a classifier can be defined (based on eRouter primary interface and/or UDP port numbers) that links to a policy, which is configured for GRE tunneling, in order to also tunnel RADIUS traffic (for the L2 tunneling use case).

The Wi-Fi GW must include following information in each RADIUS message to the AAA server:

- SSID
- Calling-Station-Id: Client Wi-Fi device MAC address
- Called-Station-Id: eROUTER MAC address (WAN interface)

The Wi-Fi GW must support configuring a second AAA server for redundancy purposes.

4.4.9 Wi-Fi bandwidth management

4.4.9.1 WMM QoS

The Wi-Fi gateway must support WMM in order to define QoS on the Wi-Fi interface.

The Wi-Fi gateway must support DSCP to 802.11e TC mapping, described in the WMM specification and shown in Table 1.

<table>
<thead>
<tr>
<th>DSCP Traffic Type</th>
<th>DSCP Value</th>
<th>WMM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control</td>
<td>56 (0x38)</td>
<td>VO (Voice priority)</td>
</tr>
<tr>
<td>Audio</td>
<td>56 (0x38)</td>
<td>VO (Voice priority)</td>
</tr>
<tr>
<td>Video</td>
<td>40 (0x28)</td>
<td>VI (Video priority)</td>
</tr>
<tr>
<td>Best Effort</td>
<td>0 (0x00)</td>
<td>BE (Bulk effort priority)</td>
</tr>
<tr>
<td>Excellent Effort</td>
<td>24 (0x18)</td>
<td>BE (Bulk effort priority)</td>
</tr>
<tr>
<td>Background</td>
<td>8 (0x08)</td>
<td>BK (Bulk priority)</td>
</tr>
</tbody>
</table>
4.4.9.2 Backwards compatibility

In order to protect wireless bandwidth (air-time) for the customer, connected via the private SSID on the Wi-Fi gateway, it must be possible to deny client Wi-Fi devices with very low connection speeds (either because of old hardware or bad SNR).

There are possible 3 methods to accomplish this requirement:

- At the Wi-Fi gateway: only allow association from client Wi-Fi devices with good connection speeds/new hardware. In this case, the Wi-Fi GW must support tri-mode (802.11b/g/n), dual-mode (e.g. 802.11g/n) and single mode (e.g. 802.11n only).
- At the Wi-Fi gateway: disassociate client Wi-Fi devices as soon as their connection speed drops below a predefined threshold.
- Insert the connection speed as a VSA in the RADIUS authentication messages for client Wi-Fi devices and let the AAA server make the decision to allow/deny the connection.

At least one of the above methods must be implemented by the Wi-Fi gateway.

4.4.10 Wi-Fi Radar

The Wi-Fi gateway should support a mechanism to trigger a site survey. When the site survey is triggered, either by a timing constraint or by a manual trigger, the Wi-Fi gateway should perform a site survey and list the SSIDs, BSSIDs (MAC address), SNRs in a MIB table.
4.5 Known constraints

Number of SSIDs per Access Point
Number of SoftGRE Tunnel endpoints supported by Access Point
Number of SSIDs that can be configured in bridged mode per Access Point
Number of simultaneous connected client Wi-Fi devices per Access Point
Number of classifiers
Number of policies
Number of VLAN Ids
MTU constraints for L2oGRE encapsulated/VLAN tagged packets on (Euro)DOCSIS
5 List of References


[802.11g] IEEE 802.11g: Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band, 2003.


[802.1Q] IEEE 802.1Q: Virtual Bridged Local Area Networks, 2011.

[802.1X] IEEE 802.1X: Port-Based Network Access Control, 2011.


[WMM] Wi-Fi Alliance: Wi-Fi Multi-Media QoS based on 802.11e, Version 1.2.0.


[WR-SP-WiFi-GW] Cable Television Laboratories Inc.: Wi-Fi Requirements for Cable Modem Gateways

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For a specific reference, subsequent revisions do not apply. For a non-specific reference, the latest version applies.
6 Appendix A: Impact of IPv6

6.1 IPv6 Addresses for client devices

Both DHCPv6 and stateless autoconfiguration should be allowed by client devices to obtain an IPv6 address.

6.2 Multicast traffic leakage

In order to establish complete traffic separation between client Wi-Fi devices on the same SSID, the Wi-Fi gateway must block all multicast (=destination MAC address equals a multicast MAC address) traffic intended for client Wi-Fi devices.

This requirement implies that only solicited router advertisements are supported.

6.3 IPv6 classifiers

The classifiers, described in section 4.4.4.2 should also support IPv6 addresses as source or destination IP address.