# Internet Gateways

*Bluetooth*® White Paper

**Date** 2016-Feb-04

**Revision** v01

**Group Prepared By** Smart Environment Study Group

**Feedback Email** smartenv-main@bluetooth.org

**Abstract**:
This white paper describes various options available to create Internet Gateways for Bluetooth Low Energy Devices.

*Revision History*

| Revision Number | Date | Comments |
|---|---|---|
| D05r00 | 2014-May-08 | First draft, based on presentation to April 2014 F2F |
| D05r01 | 2014-May-16 | Proposed responses to SG review (Hansen)<br>New material for sections 4 and 5.<br>Accept some editorial comments. |
| D05r02 | 2014-May-19 | Comments from Charles |
| D05r03 | 2014-Aug-29 | Revise to address NAT and firewalls<br>Revise to incorporate comments from Hansen, Gordon and Blair |
| D05r04 | 2014-Oct-03 | Revise to include references to the whole system, including a cloud component and a supervisor component |
| D05r05 | 2014-10-07 | After review at SE SG CC 6 Oct 2014. Comments solicited! |
| D05r06 | 2014-10-23 | Comments from Charles Gordon. Also added section describing proposal for using a cloud server to get past NAT firewalls. |
| D05r07 | 2014-10-23 | Response to Charles |
| D05r08 | 2014-10-24 | More contributions; added references |
| D05r09 | 2014-10-27 | Discussion at CC; accepted changes |
| D05r10 | 2014-11-10 | Accept changes, send for last SE SG review |
| D05r11 | 2014-11-17 | Consolidate and process comments |
| D05r12 | 2014-11-24 | Today's conference call |
| D05r13 | 2014-12-01 | Today's conference call |
| D05r14 | 2014-12-08 | Today's conference call |
| D05r15 | 2014-12-15 | Today's conference call: accept agreed changes |
| D05r16 | 2015-01-30 | Proposed comment resolutions |
| D05r17 | 2015-02-05 | Discussion from 2/2/15 CC |
| D05r18 | 2015-03-07 | Discussion from 3/2/15 CC: accept changes |
| D05r19 | 2015-03-16 | Today's conference call |
| D05r20 | 2015-03-23 | Today's conference call: scope issues in 6.2 |
| D05r21 | 2015-03-30 | Proposed response to new comments |
| D05r22 | 2015-04-05 | Comment resolution |
| D05r23 | 2015-04-15 | F2F edits |
| D05r24 | 2015-04-15 | F2F edits |
| WPr25 | 2015-04-21 | Respond to TE edits |
| WPr26 | 2015-04-27 | Checked and approved by Study Group |
| WPr27 | 2015-04-29 | Clean after last TE review |
| WPr28 | 2015-05-30 | Partial comment response |
| WPr29 | 2015-06-01 | Consider some comments at 1 Jun CC |
| WPr30 | 2015-06-05 | Merge in comments from all sources |
| WPr31 | 2015-06-06 | Proposed comment resolutions |
| WPr32 | 2015-06-08 | Results after 8 Jun CC, and additional proposed comment resolutions |
| WPr33 | 2013-07-13 | Clean version |
| WPr34 | 2015-08-10 | Revised comment resolution; chat with Nick Hunn |
| WPr35 | 2015-08-10 | Add figure captions – suggested by SIG TE team |
| WPr36 | 2015-08-17 | Ready to return to BARB for 2nd round review: clean and markup versions |
| WPr37 | 2015-09-01 | Proposed responses to BARB |

| Revision Number | Date | Comments |
|---|---|---|
| WPr38 | 2015-09-03 | Proposed responses to Tech Editor: change title, and all instances of Bluetooth Internet Gateways to Internet Gateways, replace BIG by Internet Gateways. |
| WPr39 | 2015-09-21 | Process more BARB comments |
| WPr40 | 2015-09-30 | Clean BARB version |
| WPr41 | 2015-10-12 | Process more BARB comments |
| WPr42 | 2015-10-12 | Clean BARB version |
| WPr43 | 2015-22-12 | Clean up from editor comments |
| WPr43 | 2016-01-20 | Approved by BARB |
| v01 | 2016-02-04 | Approved by the Bluetooth SIG Board of Directors |

*Contributors*

| Name | Company |
|---|---|
| Joe Decuir | CSR |
| Chris Hansen | Intel |
| Charles Gordon | Digi |
| Ian Blair | CSR |
| Cuno Pfister | Oberon Microsystems |
| Kim Schultz | Samsung Denmark |
| Dave Richkas | Microchip |
| Tim Wei | ITV |
| Victor Zhodzishsky | Broadcom |
| Kranti Kambhampati | Vensi |
| Younghwan Kwan | LGE |
| Jacky Tien | BDE |
| Nick Hunn | WiFore |

**DISCLAIMER AND COPYRIGHT NOTICE**

THIS DOCUMENT IS PROVIDED “AS IS” AND BLUETOOTH SIG, ITS MEMBERS AND THEIR AFFILIATES MAKE NO REPRESENTATIONS OR WARRANTIES WHATSOEVER, AND DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OF MERCHANTABILITY, TITLE, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, THAT THE CONTENTS OF THIS DOCUMENT IS FREE FROM ERROR OR ANY WARRANTY OTHERWISE ARISING OUT OF THIS DOCUMENT.

BLUETOOTH SIG, ITS MEMBERS AND THEIR AFFILIATES DISCLAIM ALL LIABILITY, INCLUDING LIABILITY FOR INFRINGEMENT OF ANY PROPRIETARY RIGHTS, RELATING TO USE OF INFORMATION IN THIS DOCUMENT. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL BLUETOOTH SIG, ITS MEMBERS OR THEIR AFFILIATES BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION, LOST REVENUE, PROFITS, DATA OR PROGRAMS, OR BUSINESS INTERRUPTION, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO ANY FURNISHING, PRACTICING, MODIFYING, USE OR THE PERFORMANCE OR IMPLEMENTATION OF THE CONTENTS OF THIS DOCUMENT, EVEN IF BLUETOOTH SIG, ITS MEMBERS OR THEIR AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

v01

If this Document is an intermediate draft, it is for comment only. No products should be designed based on it and it does not represent any commitment to release or implement any portion of the intermediate draft, which may be withdrawn, modified or replaced at any time as a final Document.

No license, express or implied, by estoppel or otherwise, to any intellectual property rights are granted herein.

This document is for comment only and is subject to change without notice.

# Contents

# 1 Overview

Bluetooth Low Energy, branded Bluetooth Smart™, has had a huge market impact since introduction at the end of 2010.

The next chapter begins when Bluetooth Low Energy meets the Cloud.

The purpose of this white paper is to summarize Bluetooth existing technologies, or those in development, to support that next stage in market development.

## 1.1 Statement of Problem or Need

Presently, all major mobile operating systems support Bluetooth Low Energy. This has made Bluetooth Low Energy a de facto cross-platform standard for short-range wireless communication. As a standard, it created new markets for connected accessories.

Apps running on such mobile devices can access Bluetooth Smart sensors and actuators and Web services on the Internet. This means that an app can operate as a Gateway between Bluetooth Smart devices and the Internet. For example, measurements may be uploaded to a health cloud service, or set points and firmware updates may be downloaded to Bluetooth Low Energy devices.

Usually, such Gateway apps are only intermittently connected to the Internet and are highly application specific. Unless a Bluetooth Low Energy device is a Wearable, and therefore stays attached to its user, its connectivity to the mobile device is also sporadic.

For “always on” Internet Gateways, stationary Gateway implementations should be possible as well on dedicated hardware. Standards that enable different applications and different sensors to share the same Gateway are desirable.

This white paper is about how to connect Bluetooth Low Energy devices to Cloud services using Internet Gateways with standard protocols in use between these Gateways and the Internet.

## 1.2 The Networked Environment

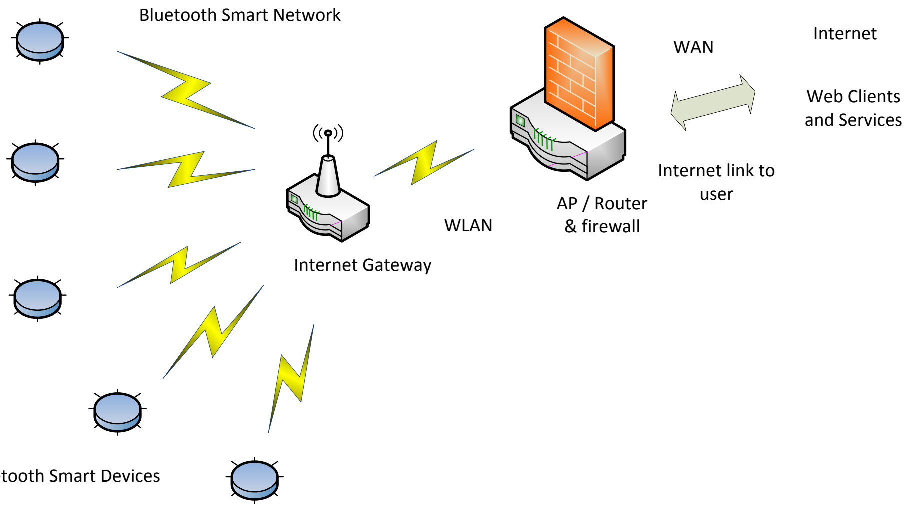
There are five major environments for Bluetooth Low Energy products:

- Personal Area
- Automobile
- Home and Office
- Retail (malls, grocery, etc.)
- Commercial and Industrial

In Personal Area and Automobile, the dominant internet access method is mobile phones with embedded wide area access (e.g., 3G, 4G), embedded Bluetooth Smart Ready™ functionality and the embedded resources to run applications. General Motors began shipping 4G LTE-enabled vehicles in 2015 model cars and trucks. Other manufacturers will follow suit, and we will see the growth of embedded connectivity in this space. This allows an automobile to act as an Internet Gateway for any devices within that automobile.

In home, office, and retail spaces, the dominant Internet access method is a wired broadband modem, e.g., DSL or cable, with an embedded bridge to Ethernet (802.3) and/or Wi-Fi (802.11) with an embedded network firewall.

The following figure illustrates an example of a Smart Environment:



v01

*Figure 1.1: Example of Smart Environment using Bluetooth Smart devices*

## 1.3 Connecting the Internet to the Gateway

The home network configuration typically does not support HTTP web servers embedded behind the firewall. This means that web crawlers cannot find your devices through the firewall.

## 1.4 Types of Low Energy Devices

This paper describes three types of Bluetooth Low Energy devices that may communicate with an Internet Gateway (IG).

1. Low Energy Servers
2. Low Energy Clients
3. Native IP Devices

### 1.4.1 Low Energy Servers

These devices are Peripherals supporting Generic Access Profile (GAP) and Generic Attribute Profile (GATT) Services [1]. Low Energy Servers use advertising channels to announce their availability. A GAP Central and GATT client device may choose to connect to them.

These devices probably represent the majority of Bluetooth Low Energy devices deployed today.

### 1.4.2 Low Energy Clients

A majority of Low Energy Clients are general purpose Smart Ready clients, which download applications (over the Internet) to control particular servers. These Smart Ready clients could download an Internet Gateway application. This represents a majority of smartphones, and many tablets, and most Bluetooth-enabled PCs.

### 1.4.3 Native IP Devices

These are Bluetooth Low Energy devices that use IPv6 [7] and 6LoBTLE [8].

## 1.5 Use Cases

### 1.5.1 Monitor Home from the Internet

Joe and his wife are returning home from their European vacation. They turned lowered the heat setpoint in their home before they left to save money. Their plane just landed at the airport, and they are about an hour away from home. Joe activates his smartphone and runs an app on it that connects to his Bluetooth-enabled thermostat at home, which enables Joe to increase the heat setpoint so their house will be warm by the time he and his wife arrive. The app finds Joe’s thermostat by accessing the Internet Gateway at Joe’s home. All of this is hidden from Joe who simply runs an app on his smartphone to adjust the thermostat. Access to the thermostat (and other devices in Joe’s home) is protected so that hackers cannot access them.

### 1.5.2 Bluetooth Devices Send Status to Servers on the Internet

There is a Bluetooth-enabled water meter installed at Joe’s house. The water meter wakes up once a week and sends water usage information to the utility’s server. The meter only needs to support Bluetooth Smart, so it can run on batteries or from harvested power from the water meter. The meter connects to the utility’s server through an Internet Gateway, which handles Internet communication for it. Joe can access the meter reading through his utility account and monitor his water usage. The utility saves money by not needing a meter reader to visit each meter.

### 1.5.3 Monitor a Person from the Internet

Joe’s father is 90 and not as resilient as he once was. To ensure his father is cared for in case of a medical emergency, Joe has persuaded his father to allow Joe to install an Internet Gateway application on his smartphone.

Joe has configured it to bond to devices that his father wears, which monitor aspects of his father’s health. He has configured the Gateway to allow two sets of Internet connections:

- To a healthcare provider that his father trusts
- To Joe and his brothers and sisters

# 2 Functional Requirements

Internet Gateways support three types of Low Energy devices:

- Bluetooth Low Energy Servers (2.1)
- Bluetooth Internet-aware Low Energy clients (2.2)
- Bluetooth IP-native 6LoBTLE Nodes (2.3)

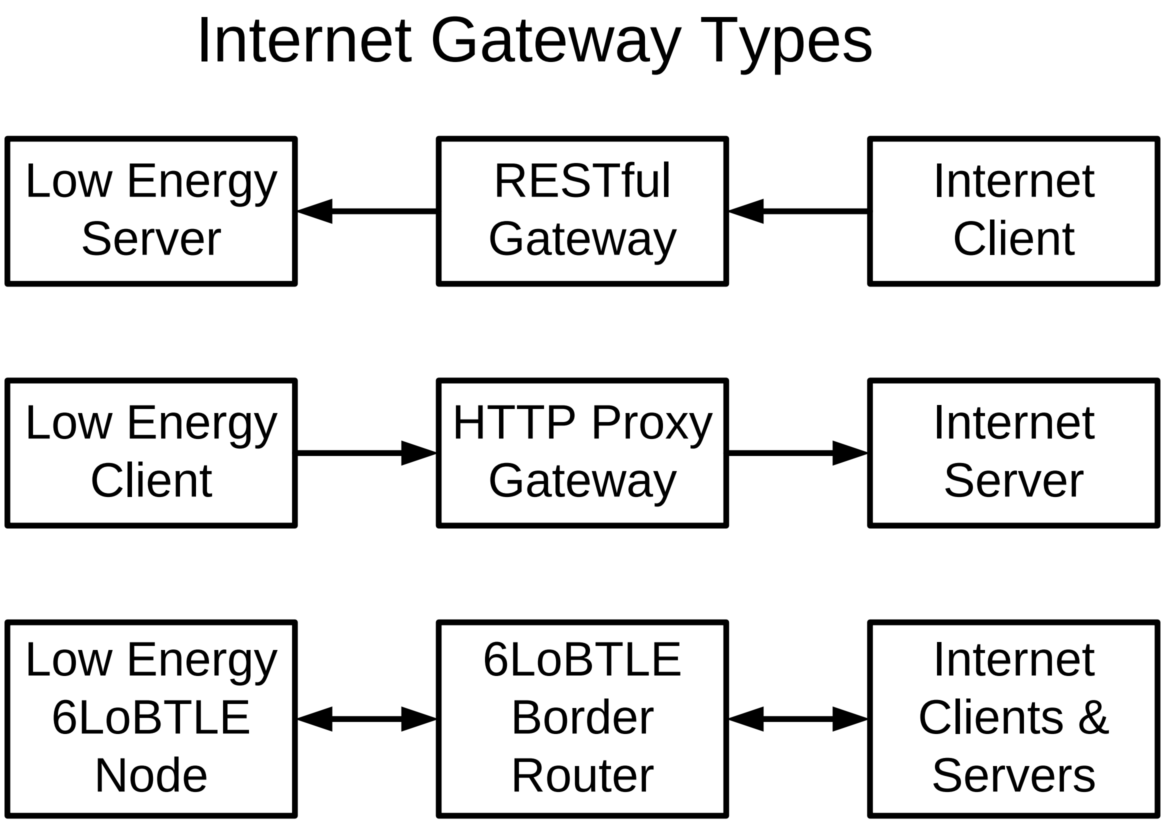


***Figure 2.1:*** *Internet Gateway types*

## 2.1 Internet Gateway Support for Bluetooth Smart Servers

The Bluetooth Special Interest Group (SIG) has defined a model for an Internet Gateway to support Low Energy Servers. These techniques are most applicable today as it supports existing GATT servers. A remote web client, working with a Gateway, impersonates a local GATT client.

This kind of Internet Gateway needs five components:

1. An Internet connection.
2. An HTTP server: to expose itself and securely connect to local Smart Server devices.

3. A GAP RESTful API [4] to allow remote Internet access to the Generic Access Profile (GAP) through a Gateway (GAP Central role) to find and connect to attached Low Energy Server devices (GAP Peripheral role).
4. A GATT RESTful API [5], to allow remote Internet access to the Generic Attribute Profile (GATT) through a Gateway (GATT Client role) to access and control connected Low Energy Server devices (GATT Server role).
5. A security engine to bridge Bluetooth Security Manager Protocol (key generation and encryption) [3] with Internet Protocol Transport Layer Security [11], and to authenticate Low Energy Server devices.

The Bluetooth SIG has published specifications for the RESTful APIs: [4][5].

## 2.2 Internet Gateway Support for Bluetooth Internet-Aware Low Energy Clients

This will allow Internet-aware clients to reach through an HTTP Proxy Service (HPS) on an Internet Gateway to access HTTP web services.

This type of Internet Gateway requires 3 components:

1. An Internet connection.
2. An HTTP Proxy Service (HPS) [6].
3. A security engine, to bridge Bluetooth Security Manager Protocol (key generation and encryption) with Internet Protocol Transport Layer Security [11], and to authenticate Internet-aware Smart Clients.

## 2.3 Internet Gateway Support for Bluetooth IP-Native Low Energy Nodes

The Bluetooth SIG Adopted a Bluetooth specification to support 6LN 6LoBTLE Low Energy Nodes (GAP Peripheral Role). This will let 6LN Low Energy Node devices to connect through a 6LBR 6LoBTLE Border Router in an Internet Gateway (GAP Central Role) from IPv6 web clients and to IPv6 web servers and services [7].

This type of Internet Gateway requires 5 components:

1. An Internet connection
2. An IPv6 Internet Border Router
3. Internet Profile Support Profile (IPSP) [7]
4. Bluetooth Core with Connection oriented Channel feature [2]
5. 6LoBTLE-6LoWPAN functionality over Bluetooth Low Energy [8]

# 3 Internet Gateway Platforms

A Bluetooth Smart Ready system which implements one or several functions required by the Internet Gateway has the following elements:

1. An embedded operating system that can run GATT client applications
2. An Internet connection
3. A Bluetooth stack which exposes an API for Bluetooth Low Energy functionality
4. Optional: User interface – from the application, for use monitoring and control
5. Power: Mains power, replaceable battery or rechargeable battery

Typical implementations:

1. Most smartphones and tablets sold today, including Android, iOS and Windows Phone
2. Bluetooth-equipped PCs; the Bluetooth connection might be a simple USB add-on
3. Stand-alone dedicated Bluetooth Internet Gateway
4. Home Access Point, broadband modem, set-top box, etc.

Internet access to the Internet Gateway can be provided through a 3G/4G modem, Wi-Fi, Ethernet, Power Line Communications (IEEE 1901), etc.

## 3.1 Smart Ready System with RESTful API Internet Gateway Application

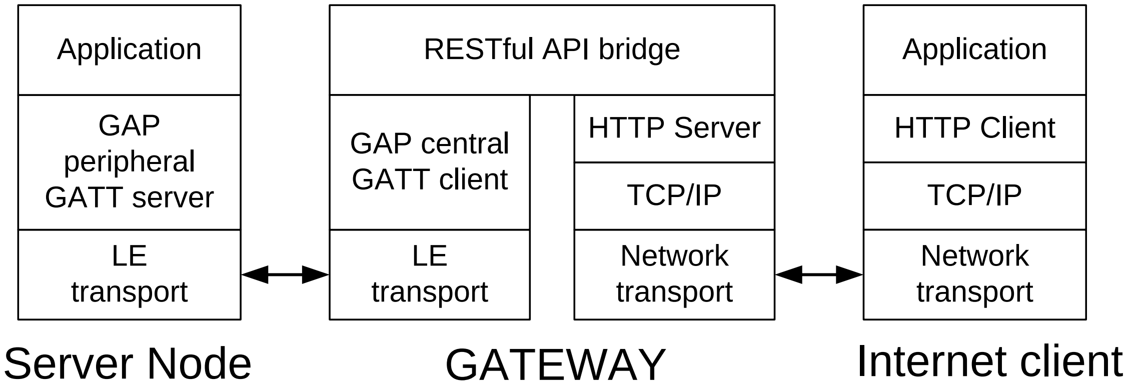


***Figure 3.1:*** *Internet Gateway using RESTful APIs*

As referenced in Section 2.1 there are five elements needed to support Bluetooth Smart Servers.

The first requirement is to support a web server. Adding an HTTP web server, with an HTTP RESTful API Bridge, is implementation specific.

An Internet Gateway application for a Smart Ready GATT client should find and expose local devices subject to interactive user control.

The RESTful API Bridge implements the GAP and GATT RESTful APIs, and in turn drive GAP and GATT client applications.

The GAP API allows a remote device to attempt HTTP/HTTPS access to any connected Node (aka Low Energy Server) or included GATT Service. If the remote client requests HTTPS access, the security engine shall initiate and establish the best Bluetooth Low Energy security available; LE Security Mode 1 Level 3 or 4 is preferred.

The security engine is something that needs to be protected. A hostile application, downloaded into a Smart Ready device, may attempt to interfere with the security engine in several ways, such as intercepting communications, intercepting security keys, and/or establishing alternate access to attached Low Energy servers. The Internet Gateway must resist being provoked to download unsolicited applications from attackers.

The Internet Gateway itself may have one or more management interfaces:

- A secure one, accessible to an authenticated local user
- A public one, exposed to visiting web clients

## 3.2 Smart Ready System with HTTP Proxy Internet Gateway Application

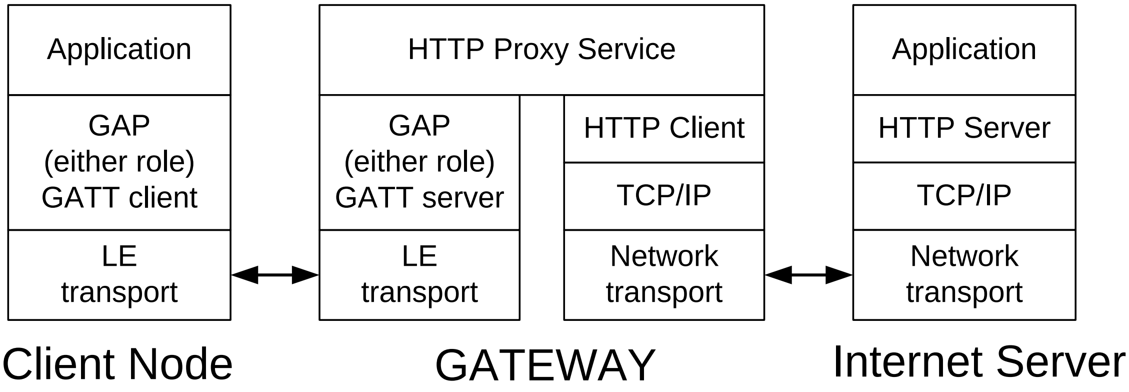


***Figure 3.2:*** *Internet Gateway using HTTP Proxy Service*

As referenced in Section 2.2, there are three essential elements in an HTTP Proxy Internet Gateway.

The HTTP Proxy Server application running on the Gateway is a GATT server with respect to attached Bluetooth Smart clients. It must be discoverable and connectable. The HPS client may act as a GAP Central or Peripheral.

It does need an HTTP/HTTPS proxy engine pointed to the Internet.

The HPS application will look like a Bluetooth GATT Server to attached Bluetooth Smart Client devices. The HPS provides a number of Characteristics that the HTTP Proxy will use to compose and send HTTP messages and receive, interpret and report HTTP responses.

Any attached Bluetooth client device can initiate Bluetooth security protocols. Security Mode 1 Levels 3 or 4 is preferred. In these cases the client profile must use the HPS Security Characteristic. The HTTP Proxy shall use these controls to request and set up Transport Layer Security with the remote Internet web server.

As a security attack surface, this is more obscure. An attacker could monitor Internet traffic if it were delivered over wireless means (e.g. Wi-Fi). An attacker might then follow this to the Gateway itself, and perhaps to the Bluetooth LE signals and attached devices. In this case, the Gateway itself should be resistant to downloading unsolicited applications, and the Bluetooth clients have Security Mode 1 Levels 3 or 4 in use.

## 3.3 Smart Ready System with IPSP Border Router Application

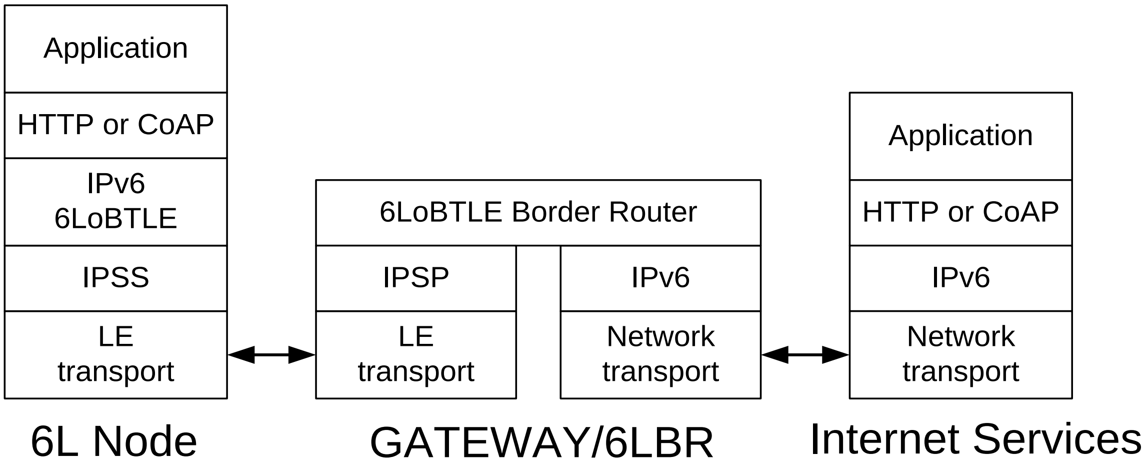


***Figure 3.3:*** *Internet Gateway using Internet Protocol Support Service and Profile*

As referenced in Section 2.3, there are five essential elements.

The Border Router application is a client with respect to attached Bluetooth server Nodes. It implements IPSP, which hears advertisements and connects to IPSS Nodes. IPSP uses GAP and GATT for device and service discovery. The Smart Ready system, and the attached devices, must support Bluetooth Core v4.1 with the L2CAP Connection Oriented Channel feature [2]. A fixed PSM is chosen through L2CAP on both sides, and it carries IPv6/6LoWPAN traffic directly.

The Border Router [8] directs IP traffic between the Internet and each connected Node.

Security is simple in the Border Router itself. Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS) should be negotiated end-to-end between each Node and the respective far end application. The Node itself may be able to negotiate and terminate TLS [9].

# 4 General Requirements

## 4.1 Backwards Compatibility

An Internet Gateway based on the RESTful APIs has no backwards compatibility issues. A web client working through this type of Gateway should be indistinguishable from a local Smart Client system from the point of view of a Bluetooth GATT Server and GAP Peripheral.

An Internet Gateway based on the HTTP Proxy Service (HPS) will require Internet awareness from new Bluetooth Smart Clients.

An Internet Gateway based on Internet Protocol Support Server (IPSS) and Profile (IPSP) as a Border Router will support new Smart Nodes which have native IPv6 support.

## 4.2 Impact on the Existing Bluetooth Core Features

An Internet Gateway based on the RESTful Server APIs will not impact the existing Bluetooth Core Features.

An Internet Gateway based on HPS will provide service to a Bluetooth Core Specification v4.0 compliant device.

An Internet Gateway based on IPSP will require Bluetooth Core Specification v4.1 compliant connection oriented channels [2].

## 4.3 Impact on Bluetooth Security

Internet Gateways of all types should require the best available Security from the SIG Core Specifications and from the IETF community.

Internet Gateways shall support LE Security Mode 1 Level 3 [1]. They should all be upgradable to support LE Security Mode 1 Level 4, i.e., LE Secure Connections, included in the Bluetooth Core Specification v4.2 [3], as soon as practicable.

In addition to link-level security, implementers may also use higher level standards which specify end-to-end application level security.

## 4.4 Impact on Bluetooth Privacy

The Bluetooth SIG is engaged in ongoing development of Privacy features.

Implementations of Internet Gateways of any kind should allow deployment of the latest version of privacy. These have been upgraded in the Bluetooth Core Specification v4.2.

## 4.5 Interoperability

An Internet Gateway that supports the RESTful APIs driven by an Internet HTTP client should be able to interoperate with any defined Bluetooth Smart Server as a compliant client.

An Internet Gateway that supports HPS will be subject to Bluetooth Qualification testing to assure interoperability.

An Internet Gateway that supports IPSP will be subject to Bluetooth Qualification testing to assure interoperability.

# 5 Industry Trends

## 5.1 Home and Mobile Connectivity

Bluetooth Low Energy has a crucial role to play in the Internet of Things, particularly in competition with other low-power radios: low data rate and low duty cycle, where the ability to run on coin cells or harvested power is essential.

Other standard radio technologies, like the IEEE 802.11/Wi-Fi Alliance and the IEEE 802.15.4/ZigBee Alliance, already have some presence in this market. Devices using proprietary radios, like Z-Wave, ANT, and RF4CE are also present.

There are other wireless methods being deployed, including the IEEE 1901/HomePlug Alliance which uses house AC wiring.

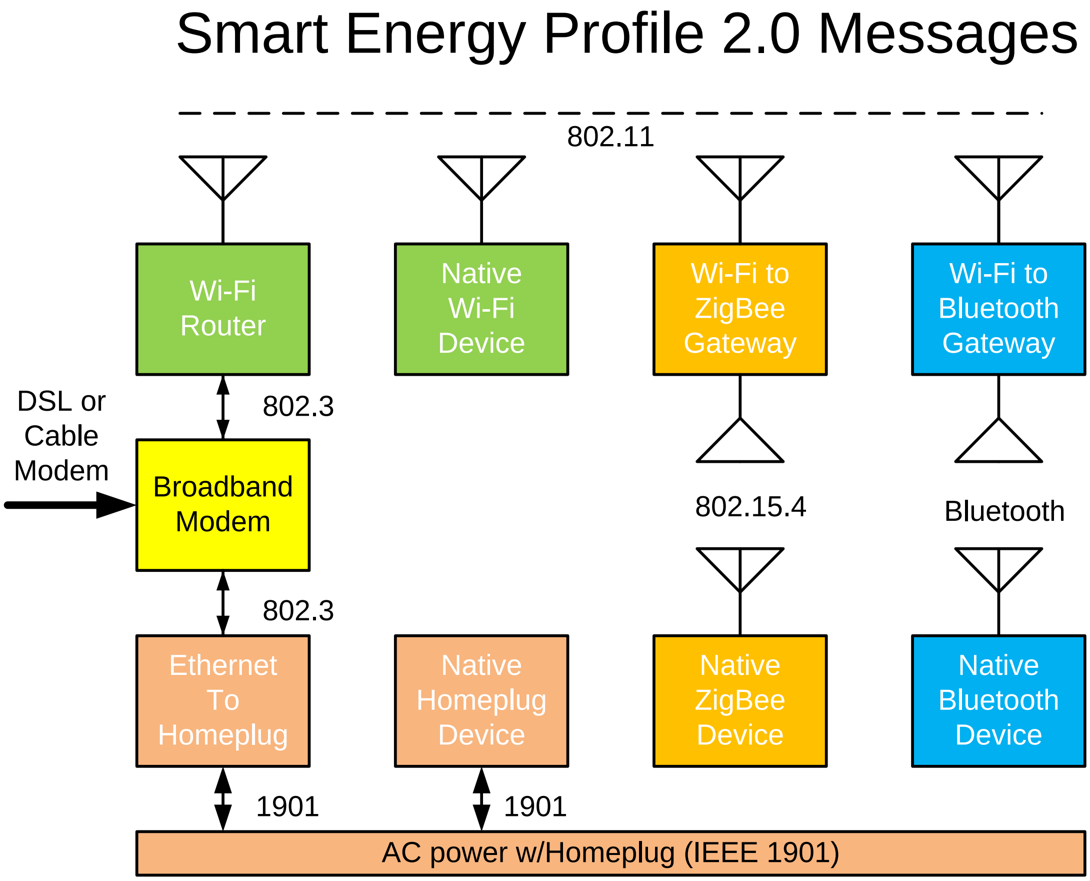


***Figure 5.1:** Provision a home for Smart Energy Profile 2.0 (IEEE 2030.5) communications*

## 5.2 Market Timing

Today, the market is large and fertile with ideas, but there is very little interoperability. This will persist for some time. Note the abundance of Standards Defining Organizations (SDOs) and companies promoting competing visions.

## 5.3 Bluetooth Device Shipments

Existing Bluetooth markets have total run rates which are in the mid-seven figures units per year, but they are climbing quickly.

Recent projections for Total Available Markets [10]:

| Application | Total Available Market, exceeding |
|---|---|
| Phone accessories (Internet / apps devices) | 10 billion |
| Smart Energy (meters and displays) | 1 billion |
| Home Automation (major appliances and HVAC) | 5 billion |
| Health, Wellness, Sports and Fitness | 10 billion |
| Assisted Living | 5 billion |
| Animal Tagging | 3 billion |
| Intelligent Transport systems | 1 billion |
| M2M (Internet-connected devices) | 10 billion |
| Toys | 10 billion |

***Figure 4.2:*** *Expected Total Available Markets*

## 5.4 Effect on Existing Scenarios

The Bluetooth Internet Gateways using RESTful APIs make existing Low Energy Servers more useful. However, they also expose new Security attack surfaces. The industry making these Gateways (applications and devices) must be proactive in deploying and enabling the best security available and protecting users from attacks.

## 5.5 New Scenarios Created

Bluetooth Internet Gateways create new scenarios. The three most crucial of these are

- Monitoring devices around a person
- Monitoring devices around a home
- Monitoring devices around other buildings

## 5.6 Effect on Bluetooth Brand

The Bluetooth brand is already well known.

Opportunity: Big jump in end user utility.

# 6 Technical Requirements

## 6.1 Effective Throughput

The effective throughput of the connection between the Internet client and the Bluetooth device will be the lesser of the throughput of the Bluetooth connection between the Internet Gateway and the Bluetooth device and the throughput between the Internet Gateway and the Internet client (which will normally be determined by the level of service the end user purchases from his ISP).

## 6.2 Internet Access

Most networks are protected by Network Address Translation (NAT) firewalls. These firewalls serve two purposes. They make it possible for many devices behind the firewall to share a single public IP address, and they protect devices behind the firewall from unauthorized access. This creates problems when clients on the Internet need to initiate a connection to a device behind the firewall.

- Since all of the devices behind the firewall share the same public IP address, there is no way for the Internet client to identify the server by IP address or to connect to it directly.
- Most firewalls also block all traffic except to or from specific IP port numbers. Typically IP port numbers that can be reliably used are the ones reserved for HTTP and HTTPS traffic (ports 80 and 443, respectively).

The first problem to solve is to provide a way for Bluetooth devices to advertise themselves on the Internet and for Internet clients to find them. The standard way to solve this problem is by using a cloud server. The Internet Gateway will have to connect to a well-known server on the Internet using the HTTP or HTTPS port. It can then register itself and the authorized local Bluetooth devices in range. The cloud server maintains a database of Internet Gateways and their associated devices. When an Internet client wants to access a Bluetooth device, it connects to the cloud server and searches the server’s database for the device it wants to connect to.

Once the Internet client finds the device it wants to connect to, the next problem to solve is to find some way for the two devices to actually talk to each other. The Internet Gateway and Internet client are both behind firewalls, so neither can make a direct connection to the other. The cloud server is used as an intermediary. After the Internet Gateway registers itself with the cloud server, it keeps the connection open. When the client wants to send a message to the Internet Gateway, it sends a message to the cloud server, which forwards it onto the Internet Gateway. The Internet Gateway sends the reply to the cloud server, which forwards it to the client. The Internet Gateway and the Internet client encapsulate the messages in an extra protocol layer that has the extra information the cloud server needs to route the messages to the correct party.

# 7 Applications of Internet Gateways

There are many applications that Internet Gateways enable.

- Build Bluetooth Low Energy networks around people
- Build Bluetooth Low Energy networks around homes and buildings

## 7.1 Bluetooth Low Energy Networks around People

Smart Ready devices, like smartphones and tablets, follow people. These are the obvious places to deploy Internet Gateway applications around people.

They usually have wide area network connection, 3G or 4G.

They frequently have rechargeable batteries.

The Bluetooth SIG has already defined an extensive set of standard GATT applications. Internet Gateways extends them to the web.

## 7.2 Bluetooth Low Energy Networks around Homes and Buildings

Internet Gateways to service homes and larger buildings have different needs.

- They need constant Internet access
- They need constant power
- They don't need to be portable

**Examples of this type of Internet Gateway deployment:**

### 7.2.1 Smart Ready Tablet

Start with an existing tablet: Android, iOS, Windows.

Download Internet Gateway applications that support one or more of the Internet Gateway models.

The tablet may also be able to download software that can translate aspiring standard Internet of Things APIs into common Bluetooth GATT profiles and services. Examples include Automation IO, HVAC control, and lighting control.

### 7.2.2 Stand-Alone Internet Gateway

Start with a home or building with deployed Wi-Fi AP service.

Deploy one or more Internet Gateways (RESTful, HPS, IPSP).

The user or installer needs to access the Gateway UI, perhaps via the simple embedded UI. Configure connections to local Bluetooth Smart devices of any type (Servers, clients, 6LoBTLE).

There may be intermediate devices that map IoT standards to native Bluetooth GATT protocols.

# 8 References

[1] Bluetooth Core Specification, v4.0 or later

[2] Bluetooth Core Specification, v4.1 or later

[3] Bluetooth Core Specification, v4.2 or later

[4] Bluetooth GAP REST API

[5] Bluetooth GATT REST API

[6] Bluetooth HTTP Proxy Service

[7] Bluetooth Internet Protocol Support Profile

[8] IETF RFC , Transmission of IPv6 packets over Bluetooth Low Energy (informative) https://datatracker.ietf.org/doc/draft-ietf-6lo-btle/

[9] IETF RFC 2818, HTTP Over TLS

[10] Bluetooth Smart Market Projections, Bluetooth Europe HIS 2014

[11] IETF RFC 2246, Transport Layer Security