Evaluation and recommendations on IPv6 for the Internet of Things

Sébastien Ziegler, Peter Kirstein, Latif Ladid, Antonio Skarmeta

Evaluation and recommendations on IPv6 for the Internet of Things

Sébastien Ziegler, Peter Kirstein, Latif Ladid, Antonio Skarmeta
December 30, 2014

Thanks to the IoT6 European Project (STREP) of the 7th Framework Program (Grant 288445).

Content

IoT6 in a nutshell

IoT6 (www.iot6.eu) was a 3 years FP7 European research project on the Internet of Things supported by the European Commission. It aimed at exploiting the potential of IPv6 [i] and related standards (6LoWPAN [ii], COAP [iii], 6TiSCH [iv], etc.) to overcome current shortcomings and fragmentation of the Internet of Things. Its main challenges and objectives were to research, design and develop a highly scalable, IPv6-based, Service-Oriented Architecture to achieve interoperability, mobility, cloud computing integration and intelligence distribution among heterogeneous smart things components, applications and services. Its potential has been researched by exploring innovative forms of interactions such as:

- Information and intelligence distribution.
- Multi-protocol interoperability with and among heterogeneous devices.
- Use of Identifiers in conjunction with IoT devices and IPv6.
- Device mobility and mobile phone networks integration, to provide ubiquitous access and seamless communication.
- Cloud computing integration with Software as a Service (SaaS).
- IPv6 - Smart Things Information Services (STIS) innovative interactions.

The main outcomes of IoT6 are recommendations on IPv6 features' exploitation for the Internet of Things and an open and well-defined, IPv6-based, Service-Oriented Architecture enabling interoperability, mobility, cloud computing and intelligence distribution among heterogeneous smart things components, applications and services,- including with business process management tools. The project was coordinated by Mandat International from October 2011 until September 2014.

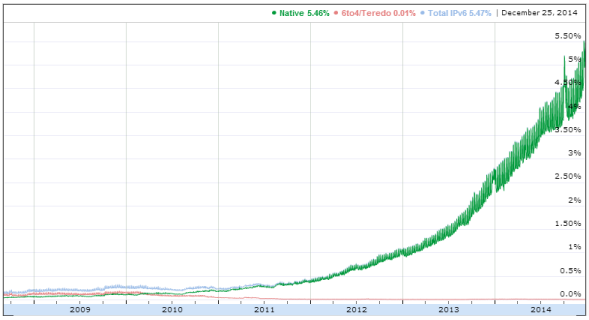
Key IPv6 features

High scalability

IPv6 offers a highly scalable address scheme, with 2^{128} unique public addresses. In practice, IPv6 addresses are subdivided into two segments: 2^{64} bits used for the network routing prefix and subnet ID; and 2^{64} bits reserved for the Host ID.

Growing global adoption and availability

IPv6 has been deployed globally and the move towards its adoption is increasing. By the end of 2014, IPv6 traffic represented over 5% of Google Internet traffic, doubling about every 9 months.



Evolution of IPv6 traffic on Google's servers[v]

Overcoming NAT limitations

Network Address Translation (NAT) [vi] enables several users and devices to associate the same public IP addresses with many more private ones. This solution has been used mainly to cope with the Internet growth. However, it has serious disadvantages for IoT devices by limiting their accessibility: A device can be accessed only if it has first contacted the application and maintained an open channel. Use of NATs is costly and makes it more difficult to share a sensor infrastructure with several different IoT application providers. Moreover, NAT breaks the end-to-end connectivity, adding potential risks in authentication processes. IPv6 enables a highly scalable and NAT-free network deployment.

IP security enablers

IPv6 can provide end-to-end connectivity, with a more distributed routing mechanism. Moreover IPv6 is supported by a large community of users and researchers investigating support and on-going improvement of its security features, including IPSec [vii]. By the additional use of identifiers, and the use of multiple IPv6 addresses for the same end point, it is possible to have different security and access properties for different IoT Applications Providers accessing the same IoT sensor/actuator infrastructure.

Mobility support

IPv6 provides features and solutions to support mobility of end-nodes, as well as mobility of the routing nodes of the network. Some of these work also with IPv4 – but are much more inefficient in the way that they were defined for that protocol.

Stateless Address Auto-configuration (SLAAC)

IoT deployment will be massive. It is particularly important that as many activities can occur in an automated fashion. One aid to this is the *IPv6 stateless address auto-configuration (SLAAC)*, by which a device introduced anew obtains its ipv6 address autonomously.

Multicast and group operations

IPv6 allows devices to join multicast groups, enabling single operations to be performed on the whole group rather than individual devices. Multicast was available for IPv4; however its implementation was such that it endangered Internet operation, and had to be abandoned for IPv4. Another mechanism introduced with IPv6 is *AnyCast*. Here a device provides a special packet on a LAN, and any relevant device will respond; only the first received is considered.

Address scope flexibility

An important feature for IoT is that of *scope*. This allows an operation to be performed on IPv6 addresses and yet limits the extent covered by the scope. This is important for the implementation of several high level protocols, like auto-configuration and multicast.

Availability of a whole set of complementary standards

Many protocols used for IPv6 application deployment over the Internet have been developed over many years. While some could have been developed over IPv4, they were not. It is particularly the case of several IoT-related standards, such as 6LoWPAN (a compressed version of IPv6 for wireless networks), RPL[viii] (an improved routing standard for low-power and lossy networks), or 6TiSCH (enabling time synchronization across constrained networks). Other standards, such as MIP (for mobility support) and CoAP can be deployed in IPv4 networks but are more adequate and efficient in IPv6 ones.

Overcoming stack size limitations

Recent work on the REST suite with optimized Operating Systems like Contiki[ix] have demonstrated that the OS takes only 11.5 Kbytes, and a complete REST IPv6 system, including datagram transport and security, can fit into 70 Kbyte. This is well within the capability of current device controllers.

Multiple IP Addresses per device

IPv4 address limitations make it difficult for a device to have multiple IP addresses; it is foreign to its routing concepts. This is a severe barrier to different applications providers using the same IoT infrastructure. IPv6 eases the potential use of various IP addresses for a single device.

Use of Identifiers in the context of IPv6

The Use of Identifiers for devices as a primary tool rather than just addresses has many advantages even for IPv4. When combined with IPv6, it facilitates the use of different access rights and device descriptions for the same device, by assigning different identities for different roles.

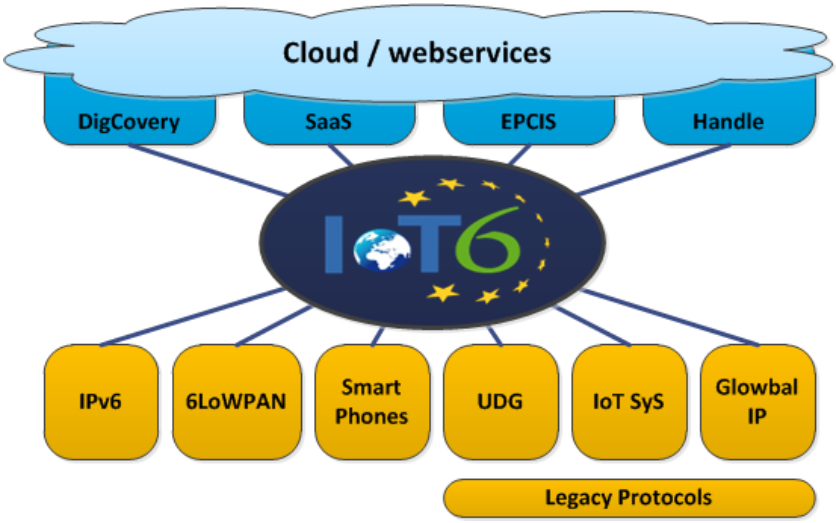
IoT6 Architecture

IoT6 designed and tested an IPv6-based architecture to integrate heterogeneous IoT components. An IoT6 stack has been developed based on IPv6/6LoWPAN at the network layer, combined with CoAP/HTTP, JSON and oBIX. The IoT6 Stack has been deployed in four environments: Contiki-motes, OSGi-Gateway, Digcovery-server and Mobile-phone. These implementations provide the functionalities of IPv6 connectivity and open service layer, enabling IoT6 components interoperability.

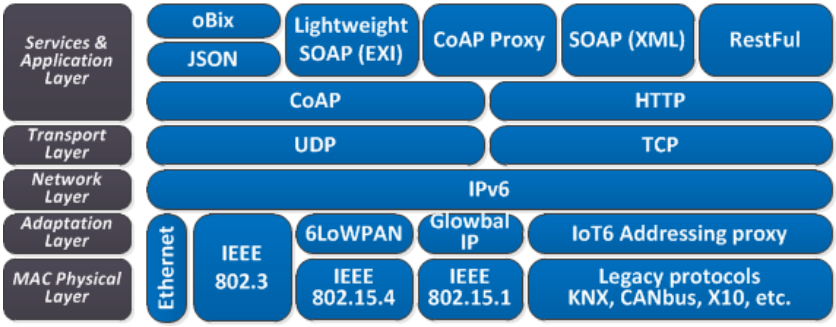
The IoT6 Open Service layer[x] is based on a scalable architecture to support discovering, registering and looking-up services and resources of heterogeneous and ubiquitous IoT devices. IoT6 developed four main elements: global Digcovery, local Digrectory, smart object and mobile Digcovery. Global Digcovery is a centralized platform that enables any IoT client to lookup IoT resources and services through standard interfaces such as HTTP and CoAP. In a local domain, each Digrectory registers fine-grained descriptions of the IoT resources and services following the scalable DNS infrastructure to support distributed local queries. The smart object implementation enables the autonomous registration and M2M access of resources and services available from IoT devices using mDNS and CoAP protocols, respectively.

In addition, we implemented and provided other transversal functionalities such as semantic description, context-aware search and communication interfaces to achieve a unifying architecture. First, we provided a homogeneous semantic description based on CoAP links, oBIX data format and JSON message structure to support interoperability in heterogeneous IoT domains. Second, we integrated the MongoDB search engine in the proposed architecture to support a scalable context-aware look-up based on geo-location, domain and type of resources. Third, we provided the communication interfaces to enable interoperability between the proposed elements with heterogeneous IoT things and clients. The proposed architecture is compatible with existing protocols based on standardized technologies such as IPv6 and DNS. Moreover, the architecture supports the integration of heterogeneous IoT devices including 802.15.4 sensors, RFID tags, building actuators, and mobile phones. The architecture also provides an open service layer to interact with

end-user applications through standardized interfaces such as web services (HTTP), and constrained applications (CoAP).



Heterogeneous integration through IoT6



IoT6 protocol architecture

Demonstrating the potential of IPv6

Legacy protocol integration

IoT6 researched the potential of IPv6 addresses as identifiers for heterogeneous IoT devices. It demonstrated that part of the Address space associated with each routable IPv6 address could be used to address non-IP end devices from legacy deployments, such as KNX and BACNET. This mechanism pioneered by UDG[xi], and further specified and fine-tuning by IoT6, has led to a formal proposal for communication at the IETF. The project also developed a lightweight module named IoTSys[xii] to ease the integration of legacy protocols devices into IPv6 and IoT6.

Identifier integration

In IoT6 we showed how IPv6 can be combined with identification solutions. It can be used, for instance, to assist security, by storing security and authentication tokens in the attribute store of the information system. The potentially complex task of restricting access to end -devices to authorized processes is resolved in a proxy manner – removing the need to put too much complexity in the end-devices. It enables role-based descriptions of a device by providing several application-specific identities (including IPv6 addresses as attributes of the identifier). Because processes and devices have similar identifier characteristics, the attributes can include the identifier prescribing the access process for a device. Some of these advantages were demonstrated in the implementation by using the existing Handle Identifier-resolution system[xiii].

Multiple IPv6-based integrations demonstrated

Globally, IoT6 has demonstrated that IPv6 and the IoT6 architecture could be used to integrate heterogeneous components together, including:

- Devices using legacy protocols, such as KNX, BACnet, X10, ZigBee, etc.
- Cloud-based applications with Software as a Service (SaaS),
- Smart phones;
- Tags and Smart Things Information Systems (STIS) such as EPCIS
- Smart city, by integrating the sensors of the smart city of Santander into its architecture.

Smart board and smart routing

IoT6 has developed a customized smart board to support multi-protocol integration and smart routing experiments. It demonstrated the possibility to use the network layer and IPv6 header to develop simple smart routing, enabling for instance a temperature sensor data to be duplicated and routed to a security server in case of abnormal temperature.

International impact and standardization effort

On the international stage, the IoT6 consortium has initiated and set up the IEEE Subcommittee on IoT as well as the ETSI IP6 SGI. IoT6 has cooperated closely with the IPv6 Forum, the IoT Forum and the International Telecommunication Union. In another domain, IoT6 has paved the way to a new web of cooperation links between European and Korean research communities.

IoT6 outreach, dissemination and exploitation

IoT6 has dedicated an intensive effort to disseminate its activities and recommendations, including:

- 46 deliverables;
- 19 Scientific peer-reviewed publications;
- 144 dissemination activities, including 75 events attended and 24 organized or co-organized.

The project dedicated a particular focus on industrial exploitation with:

- 4 patents filled;
- SME handbook which is available on IoT6 website;
- Several research projects using IoT6 outcomes, including IoT Lab[xiv];
- 3 IoT testbeds have been designed and/or extended according to IoT6 architecture, including distributed testbeds across Europe and with Asia[xv];
- IoT6 has supported directly the emergence of 4 startups exploiting IPv6 for IoT applications and solutions[xvi] and has received several awards, including from the IPSO Alliance contest.

Key lessons learned and Recommendations

After three years of intensive research on IPv6 and IoT, a certain clear conclusions emerged:

- **IPv6 is a strategic enabler for IoT scalability, manageability and interoperability;**
- **IPv6 is a convenient multi-systems and cross-domain integrator;**
- **There will be a logical and increasing IPv6 – IoT Integration;**
- **IPv6 deployment is an accelerating reality** (as shown in the figure below)**;**
- **For large deployments with multiple applications providers using to the same sensor infrastructure, there is no alternative to IPv6. Moreover, Identifier-based systems will greatly ease operational security;**
- **There is a need for global IoT standards enabling cross-domain interoperability and such standards are likely to be IPv6-based.**

The foregoing leads us to three specific recommendations:

- **The EU is invited to consider IPv6 as a key enabler for the IoT research and market potential and to communicate internally and externally on this matter;**
- **Future EU-funded IoT research projects, testbeds and architectures should be IPv6 compliant by requirement;**
- **The European research community should be encouraged to contribute and play a more active role in IoT standardization and IoT interoperability solution design.**

For any complementary information, do not hesitate to visit the IoT6 website www.iot6.eu and/or to contact us at iot6@mandint.org

End notes and references

[i] "Internet Protocol, Version 6 (IPv6)", RFC 2460, IETF: https://www.ietf.org/rfc/rfc2460.txt
[ii] "IPv6 over Low power WPAN (6LoWPAN)", RFC 6282, IETF https://www.ietf.org/rfc/rfc6282.txt
[iii] "Constrained Application Protocol (CoAP)", RFC 7252, IETF: https://www.ietf.org/rfc/rfc7252.txt
[iv] IPv6 over the TSCH mode of IEEE 802.15.4e (6TiSCH), IETF: http://datatracker.ietf.org/wg/6tisch/charter/
[v] Google IPv6 stats on December 25 2014 at http://www.google.com/intl/en/ipv6/statistics.html
[vi] The IP Network Address Translator (NAT), RFC 1631, IETF: https://www.ietf.org/rfc/rfc1631.txt and IP Network Address Translator (NAT) Terminology and Considerations, RFC 2663, IETF: https://www.ietf.org/rfc/rfc2663.txt
[vii] Security Architecture for the Internet Protocol, RFC 4301, IETF: https://www.ietf.org/rfc/rfc4301.txt, as well as Security Architecture for the Internet Protocol, RFC 2401, IETF: https://www.ietf.org/rfc/rfc2401.txt and IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap, RFC 6071, IETF: https://www.ietf.org/rfc/rfc6071.txt
[viii] IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL), RFC 6550, IETF, https://www.ietf.org/rfc/rfc6550.txt
[ix] Contiki is an open source operating system for the Internet of Things, http://www.contiki-os.org
[x] More details in the IoT6 deliverable D3.3 available at: http://www.iot6.eu/deliverables
[xi] UDG is an IPv6-based multi-protocol control and monitoring system using IPv6 as a common identifier for devices using legacy protocols. It was developed by a Swiss research project and used by IoT6 for research purpose. More information on UDG ongoing developments at: www.devicegateway.com
[xii] More details in the IoT6 deliverables available at: http://www.iot6.eu/deliverables
[xiii] Handle system www.handle.net and "Handle system overview", RFC3650, IETF: https://www.ietf.org/rfc/rfc3650.txt
[xiv] IoT Lab is a FP7 European research project exploring the potential of crowd sourcing and crowd sensing for the IoT. More information at: http://www.iotlab.eu
[xv] Including Smart HEPIA, UMU testbed and MI testbed (including IoT Lab and MI-BUPT pilot testbed).
[xvi] Including Odins, Novaccess, Hops and Vbrain.

The IoT6 project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement n. 288445.

For further information:

IoT6 Research project

c/o Mandat International

iot6@mandint.org

http://www.iot6.eu

Sebastien Ziegler

IoT6 Project Coordinator

Evaluation and recommendations on IPv6 for the Internet of Things

Sébastien Ziegler, Peter Kirstein, Latif Ladid, Antonio Skarmeta
December 30, 2014

Thanks to the IoT6 European Project (STREP) of the 7th Framework Program (Grant 288445).

Content

IoT6 in a nutshell

IoT6 (www.iot6.eu) was a 3 years FP7 European research project on the Internet of Things supported by the European Commission. It aimed at exploiting the potential of IPv6 [i] and related standards (6LoWPAN [ii], COAP [iii], 6TiSCH [iv], etc.) to overcome current shortcomings and fragmentation of the Internet of Things. Its main challenges and objectives were to research, design and develop a highly scalable, IPv6-based, Service-Oriented Architecture to achieve interoperability, mobility, cloud computing integration and intelligence distribution among heterogeneous smart things components, applications and services. Its potential has been researched by exploring innovative forms of interactions such as:

- Information and intelligence distribution.
- Multi-protocol interoperability with and among heterogeneous devices.
- Use of Identifiers in conjunction with IoT devices and IPv6.
- Device mobility and mobile phone networks integration, to provide ubiquitous access and seamless communication.
- Cloud computing integration with Software as a Service (SaaS).
- IPv6 - Smart Things Information Services (STIS) innovative interactions.

The main outcomes of IoT6 are recommendations on IPv6 features' exploitation for the Internet of Things and an open and well-defined, IPv6-based, Service-Oriented Architecture enabling interoperability, mobility, cloud computing and intelligence distribution among heterogeneous smart things components, applications and services,- including with business process management tools. The project was coordinated by Mandat International from October 2011 until September 2014.

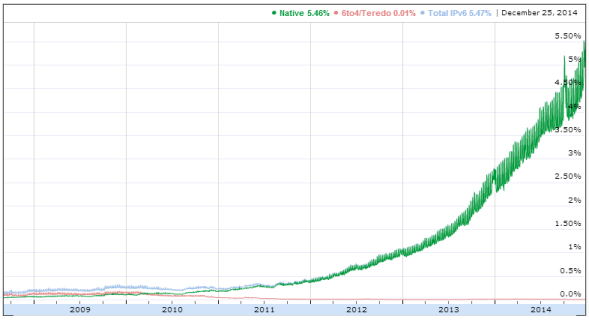
Key IPv6 features

High scalability

IPv6 offers a highly scalable address scheme, with 2^{128} unique public addresses. In practice, IPv6 addresses are subdivided into two segments: 2^{64} bits used for the network routing prefix and subnet ID; and 2^{64} bits reserved for the Host ID.

Growing global adoption and availability

IPv6 has been deployed globally and the move towards its adoption is increasing. By the end of 2014, IPv6 traffic represented over 5% of Google Internet traffic, doubling about every 9 months.



Evolution of IPv6 traffic on Google's servers[v]

Overcoming NAT limitations

Network Address Translation (NAT) [vi] enables several users and devices to associate the same public IP addresses with many more private ones. This solution has been used mainly to cope with the Internet growth. However, it has serious disadvantages for IoT devices by limiting their accessibility: A device can be accessed only if it has first contacted the application and maintained an open channel. Use of NATs is costly and makes it more difficult to share a sensor infrastructure with several different IoT application providers. Moreover, NAT breaks the end-to-end connectivity, adding potential risks in authentication processes. IPv6 enables a highly scalable and NAT-free network deployment.

IP security enablers

IPv6 can provide end-to-end connectivity, with a more distributed routing mechanism. Moreover IPv6 is supported by a large community of users and researchers investigating support and on-going improvement of its security features, including IPSec [vii]. By the additional use of identifiers, and the use of multiple IPv6 addresses for the same end point, it is possible to have different security and access properties for different IoT Applications Providers accessing the same IoT sensor/actuator infrastructure.

Mobility support

IPv6 provides features and solutions to support mobility of end-nodes, as well as mobility of the routing nodes of the network. Some of these work also with IPv4 – but are much more inefficient in the way that they were defined for that protocol.

Stateless Address Auto-configuration (SLAAC)

IoT deployment will be massive. It is particularly important that as many activities can occur in an automated fashion. One aid to this is the *IPv6 stateless address auto-configuration (SLAAC)*, by which a device introduced anew obtains its ipv6 address autonomously.

Multicast and group operations

IPv6 allows devices to join multicast groups, enabling single operations to be performed on the whole group rather than individual devices. Multicast was available for IPv4; however its implementation was such that it endangered Internet operation, and had to be abandoned for IPv4. Another mechanism introduced with IPv6 is *AnyCast*. Here a device provides a special packet on a LAN, and any relevant device will respond; only the first received is considered.

Address scope flexibility

An important feature for IoT is that of *scope*. This allows an operation to be performed on IPv6 addresses and yet limits the extent covered by the scope. This is important for the implementation of several high level protocols, like auto-configuration and multicast.

Availability of a whole set of complementary standards

Many protocols used for IPv6 application deployment over the Internet have been developed over many years. While some could have been developed over IPv4, they were not. It is particularly the case of several IoT-related standards, such as 6LoWPAN (a compressed version of IPv6 for wireless networks), RPL[viii] (an improved routing standard for low-power and lossy networks), or 6TiSCH (enabling time synchronization across constrained networks). Other standards, such as MIP (for mobility support) and CoAP can be deployed in IPv4 networks but are more adequate and efficient in IPv6 ones.

Overcoming stack size limitations

Recent work on the REST suite with optimized Operating Systems like Contiki[ix] have demonstrated that the OS takes only 11.5 Kbytes, and a complete REST IPv6 system, including datagram transport and security, can fit into 70 Kbyte. This is well within the capability of current device controllers.

Multiple IP Addresses per device

IPv4 address limitations make it difficult for a device to have multiple IP addresses; it is foreign to its routing concepts. This is a severe barrier to different applications providers using the same IoT infrastructure. IPv6 eases the potential use of various IP addresses for a single device.

Use of Identifiers in the context of IPv6

The Use of Identifiers for devices as a primary tool rather than just addresses has many advantages even for IPv4. When combined with IPv6, it facilitates the use of different access rights and device descriptions for the same device, by assigning different identities for different roles.

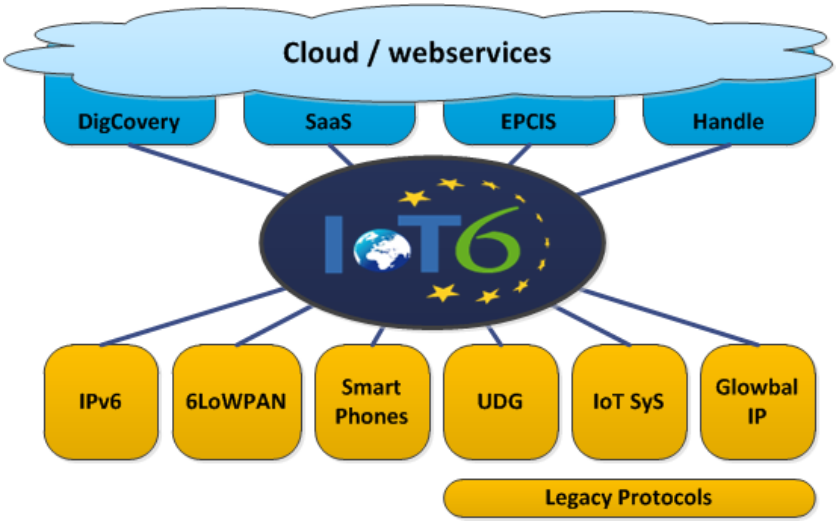
IoT6 Architecture

IoT6 designed and tested an IPv6-based architecture to integrate heterogeneous IoT components. An IoT6 stack has been developed based on IPv6/6LoWPAN at the network layer, combined with CoAP/HTTP, JSON and oBIX. The IoT6 Stack has been deployed in four environments: Contiki-motes, OSGi-Gateway, Digcovery-server and Mobile-phone. These implementations provide the functionalities of IPv6 connectivity and open service layer, enabling IoT6 components interoperability.

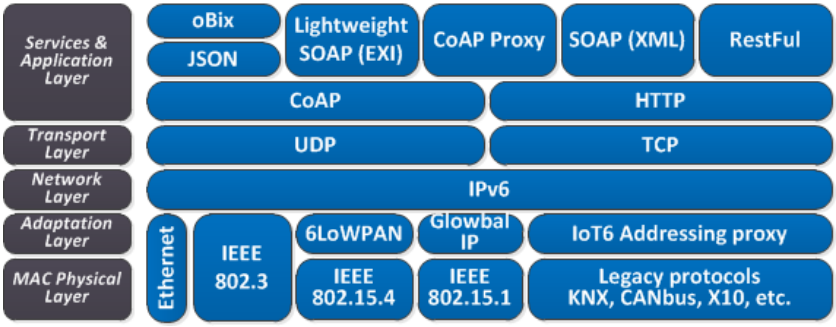
The IoT6 Open Service layer[x] is based on a scalable architecture to support discovering, registering and looking-up services and resources of heterogeneous and ubiquitous IoT devices. IoT6 developed four main elements: global Digcovery, local Digrectory, smart object and mobile Digcovery. Global Digcovery is a centralized platform that enables any IoT client to lookup IoT resources and services through standard interfaces such as HTTP and CoAP. In a local domain, each Digrectory registers fine-grained descriptions of the IoT resources and services following the scalable DNS infrastructure to support distributed local queries. The smart object implementation enables the autonomous registration and M2M access of resources and services available from IoT devices using mDNS and CoAP protocols, respectively.

In addition, we implemented and provided other transversal functionalities such as semantic description, context-aware search and communication interfaces to achieve a unifying architecture. First, we provided a homogeneous semantic description based on CoAP links, oBIX data format and JSON message structure to support interoperability in heterogeneous IoT domains. Second, we integrated the MongoDB search engine in the proposed architecture to support a scalable context-aware look-up based on geo-location, domain and type of resources. Third, we provided the communication interfaces to enable interoperability between the proposed elements with heterogeneous IoT things and clients. The proposed architecture is compatible with existing protocols based on standardized technologies such as IPv6 and DNS. Moreover, the architecture supports the integration of heterogeneous IoT devices including 802.15.4 sensors, RFID tags, building actuators, and mobile phones. The architecture also provides an open service layer to interact with

end-user applications through standardized interfaces such as web services (HTTP), and constrained applications (CoAP).



Heterogeneous integration through IoT6



IoT6 protocol architecture

Demonstrating the potential of IPv6

Legacy protocol integration

IoT6 researched the potential of IPv6 addresses as identifiers for heterogeneous IoT devices. It demonstrated that part of the Address space associated with each routable IPv6 address could be used to address non-IP end devices from legacy deployments, such as KNX and BACNET. This mechanism pioneered by UDG[xi], and further specified and fine-tuning by IoT6, has led to a formal proposal for communication at the IETF. The project also developed a lightweight module named IoTSys[xii] to ease the integration of legacy protocols devices into IPv6 and IoT6.

Identifier integration

In IoT6 we showed how IPv6 can be combined with identification solutions. It can be used, for instance, to assist security, by storing security and authentication tokens in the attribute store of the information system. The potentially complex task of restricting access to end -devices to authorized processes is resolved in a proxy manner – removing the need to put too much complexity in the end-devices. It enables role-based descriptions of a device by providing several application-specific identities (including IPv6 addresses as attributes of the identifier). Because processes and devices have similar identifier characteristics, the attributes can include the identifier prescribing the access process for a device. Some of these advantages were demonstrated in the implementation by using the existing Handle Identifier-resolution system[xiii].

Multiple IPv6-based integrations demonstrated

Globally, IoT6 has demonstrated that IPv6 and the IoT6 architecture could be used to integrate heterogeneous components together, including:

- Devices using legacy protocols, such as KNX, BACnet, X10, ZigBee, etc.
- Cloud-based applications with Software as a Service (SaaS),
- Smart phones;
- Tags and Smart Things Information Systems (STIS) such as EPCIS
- Smart city, by integrating the sensors of the smart city of Santander into its architecture.

Smart board and smart routing

IoT6 has developed a customized smart board to support multi-protocol integration and smart routing experiments. It demonstrated the possibility to use the network layer and IPv6 header to develop simple smart routing, enabling for instance a temperature sensor data to be duplicated and routed to a security server in case of abnormal temperature.

International impact and standardization effort

On the international stage, the IoT6 consortium has initiated and set up the IEEE Subcommittee on IoT as well as the ETSI IP6 SGI. IoT6 has cooperated closely with the IPv6 Forum, the IoT Forum and the International Telecommunication Union. In another domain, IoT6 has paved the way to a new web of cooperation links between European and Korean research communities.

IoT6 outreach, dissemination and exploitation

IoT6 has dedicated an intensive effort to disseminate its activities and recommendations, including:

- 46 deliverables;
- 19 Scientific peer-reviewed publications;
- 144 dissemination activities, including 75 events attended and 24 organized or co-organized.

The project dedicated a particular focus on industrial exploitation with:

- 4 patents filled;
- SME handbook which is available on IoT6 website;
- Several research projects using IoT6 outcomes, including IoT Lab[xiv];
- 3 IoT testbeds have been designed and/or extended according to IoT6 architecture, including distributed testbeds across Europe and with Asia[xv];
- IoT6 has supported directly the emergence of 4 startups exploiting IPv6 for IoT applications and solutions[xvi] and has received several awards, including from the IPSO Alliance contest.

Key lessons learned and Recommendations

After three years of intensive research on IPv6 and IoT, a certain clear conclusions emerged:

- **IPv6 is a strategic enabler for IoT scalability, manageability and interoperability;**
- **IPv6 is a convenient multi-systems and cross-domain integrator;**
- **There will be a logical and increasing IPv6 – IoT Integration;**
- **IPv6 deployment is an accelerating reality** (as shown in the figure below)**;**
- **For large deployments with multiple applications providers using to the same sensor infrastructure, there is no alternative to IPv6. Moreover, Identifier-based systems will greatly ease operational security;**
- **There is a need for global IoT standards enabling cross-domain interoperability and such standards are likely to be IPv6-based.**

The foregoing leads us to three specific recommendations:

- **The EU is invited to consider IPv6 as a key enabler for the IoT research and market potential and to communicate internally and externally on this matter;**
- **Future EU-funded IoT research projects, testbeds and architectures should be IPv6 compliant by requirement;**
- **The European research community should be encouraged to contribute and play a more active role in IoT standardization and IoT interoperability solution design.**

For any complementary information, do not hesitate to visit the IoT6 website www.iot6.eu and/or to contact us at iot6@mandint.org

End notes and references

[i] "Internet Protocol, Version 6 (IPv6)", RFC 2460, IETF: https://www.ietf.org/rfc/rfc2460.txt
[ii] "IPv6 over Low power WPAN (6LoWPAN)", RFC 6282, IETF https://www.ietf.org/rfc/rfc6282.txt
[iii] "Constrained Application Protocol (CoAP)", RFC 7252, IETF: https://www.ietf.org/rfc/rfc7252.txt
[iv] IPv6 over the TSCH mode of IEEE 802.15.4e (6TiSCH), IETF: http://datatracker.ietf.org/wg/6tisch/charter/
[v] Google IPv6 stats on December 25 2014 at http://www.google.com/intl/en/ipv6/statistics.html
[vi] The IP Network Address Translator (NAT), RFC 1631, IETF: https://www.ietf.org/rfc/rfc1631.txt and IP Network Address Translator (NAT) Terminology and Considerations, RFC 2663, IETF: https://www.ietf.org/rfc/rfc2663.txt
[vii] Security Architecture for the Internet Protocol, RFC 4301, IETF: https://www.ietf.org/rfc/rfc4301.txt, as well as Security Architecture for the Internet Protocol, RFC 2401, IETF: https://www.ietf.org/rfc/rfc2401.txt and IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap, RFC 6071, IETF: https://www.ietf.org/rfc/rfc6071.txt
[viii] IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL), RFC 6550, IETF, https://www.ietf.org/rfc/rfc6550.txt
[ix] Contiki is an open source operating system for the Internet of Things, http://www.contiki-os.org
[x] More details in the IoT6 deliverable D3.3 available at: http://www.iot6.eu/deliverables
[xi] UDG is an IPv6-based multi-protocol control and monitoring system using IPv6 as a common identifier for devices using legacy protocols. It was developed by a Swiss research project and used by IoT6 for research purpose. More information on UDG ongoing developments at: www.devicegateway.com
[xii] More details in the IoT6 deliverables available at: http://www.iot6.eu/deliverables
[xiii] Handle system www.handle.net and "Handle system overview", RFC3650, IETF: https://www.ietf.org/rfc/rfc3650.txt
[xiv] IoT Lab is a FP7 European research project exploring the potential of crowd sourcing and crowd sensing for the IoT. More information at: http://www.iotlab.eu
[xv] Including Smart HEPIA, UMU testbed and MI testbed (including IoT Lab and MI-BUPT pilot testbed).
[xvi] Including Odins, Novaccess, Hops and Vbrain.