# Aplicações, benefícios e desafios da utilização de IPv6 no cenário da Internet das Coisas

João Borges

20 de agosto de 2013

## 1 Introdução

Com a miniaturização dos sistemas computacionais (MEMS - *Micro Electromecanical Systems*) surgiram novas possibilidades de aplicações e, principalmente, novas formas de interação entre estes sistemas e seus usuários.

Ainda no início da década de 90, o pesquisador e cientista do Xerox PARC (*Palo Alto Research Center Incorporated*) Mark Weiser visionava o surgimento de novas aplicações e formas de utilização do computador, que seria mais tarde compreendido como o início de um novo paradigma computacional – a Computação Ubíqua [1].

Este novo paradigma pode ser caracterizado pela mudança na forma de interação entre o homem e o computador. Através da total imersão da capacidade computacional em atividades do cotidiano das pessoas, os usuários interagirão agora com os chamados "objetos inteligentes". Por objetos inteligentes pode-se compreender como qualquer dispositivo computacional capaz de realizar processamento, armazenamento e comunicação, e que esteja embarcado em objetos e equipamentos de uso comum, como geladeiras e luminárias. Tais objetos comuns tornam-se "inteligentes" uma vez que há um poder computacional agregado a suas funcionalidades.

Desta forma, o computador convencional é, então, substituído por uma série de computadores embarcados em objetos presentes no ambiente, permitindo a interação do usuário com estes objetos de forma inteligente, sem necessitar da inserção de dados da forma convencional por parte do usuário. Isto é, agora os próprios objetos inteligentes podem detectar a presença de um determinado usuário e agir conforme o contexto que julguem necessário para este usuário. O ambiente dotado de objetos inteligentes é também denominado por ambiente inteligente, como é o clássico exemplo da casa inteli-

gente [2], capaz de auxiliar nas tarefas cotidianas de seus moradores/usuários através da inteligência computacional de seus objetos.

A Internet das Coisas, do inglês *Internet of Things* (IoT), consiste na integração destes objetos inteligentes à Internet, podendo ser acessados como qualquer outro dispositivo de rede [3].

# 2 Fundamentos

Uma vez que os objetos inteligentes constituem-se pela agregação de um sistema computacional embarcado em si, capaz de monitorar e/ou controlar o seu funcionamento, é importante notar que o dispositivo computacional a ser embarcado precisa ser minúsculo, de forma a não interferir no funcionamento normal deste objeto. Sendo assim, o *hardware* que constitui um objeto inteligente é, geralmente, computacionalmente limitado. Estes dispositivos possuem baixo poder de processamento, alguns dotados de microcontroladores de 8 bits com cerca de 8 MHz de frequência, pouco espaço de armazenamento, cerca de 128 Kbytes a 1 Mbyte, e baixa largura de banda para transmissão e recepção, algo em torno de 1 kbps podendo ir até 1 Mbps [4]. Uma outra grande limitação computacional que estes dispositivos podem apresentar é a restrição de energia, alguns sendo alimentados por meio de baterias, o que limitará o seu funcionamento ao tempo de vida de sua bateria.

Uma grande linha de pesquisa, que muitos sugerem como a base para o desenvolvimento dos ambientes inteligentes que hoje é o objeto da IoT, é o estudo das Redes de Sensores Sem Fio (RSSF). Uma RSSF é uma rede composta por estes dispositivos computacionalmente limitados, e que tem como principal objetivo realizar a coleta de dados de um determinado ambiente físico, por meio de sensores dos mais diversos tipos, e enviá-los para um ponto de coleta, estação-base, que irá processá-los e deles extrair as percepções do ambiente [4]. Por sensores, podemos entender como qualquer dispositivo capaz de monitorar um determinado fenômeno ou estado do ambiente. Como exemplos de tipos de dados de sensoriamento temos desde sensores de temperatura e pressão, passando por sensores de movimento e posicionamento, até sensores capazes de detectar movimentos cardíacos e outras funções do corpo humano.

Desta forma, muitos dos avanços alcançados na resolução dos problemas existentes nas RSSFs podem ser adaptados para a realidade da IoT [5]. Alguns dos principais problemas que já possuem soluções no universo das RSSFs são aqueles referentes às restrições computacionais dos dispositivos, principalmente quanto à economia da sua limitada energia. Como exemplo para o problema da comunicação a curtas distâncias, uma vez que a escassa

energia não pode ser utilizada para transmissões com maior potência, há a definição do padrão IEEE 802.15.4 [6] para comunicação em enlace, que suporta desde a possibilidade de períodos de alternância entre os modos de ligado e desligado do transmissor/receptor de rádio para economizar energia, até a criação de uma topologia *ad-hoc* para a descoberta e comunicação entre os dispositivos em seu raio de alcance.

# 3 Diferenças entre RSSF e IoT

Embora os estudos e pesquisas relacionados aos problemas e especificadades das RSSFs já estejam em um ponto onde alguns possam considerar maduro, em sua grande maioria eles resolvem problemas confinados à sua topologia interna. A Figura 1 ilustra a topologia convencional de uma RSSF, que constitui-se por uma rede composta por sensores que comunicam-de entre si através de uma tecnologia de acesso ao meio sem fio específica, geralmente IEEE 802.15.4 ou outra mais simples, e um destes nós está conectado diretamente a uma máquina externa.

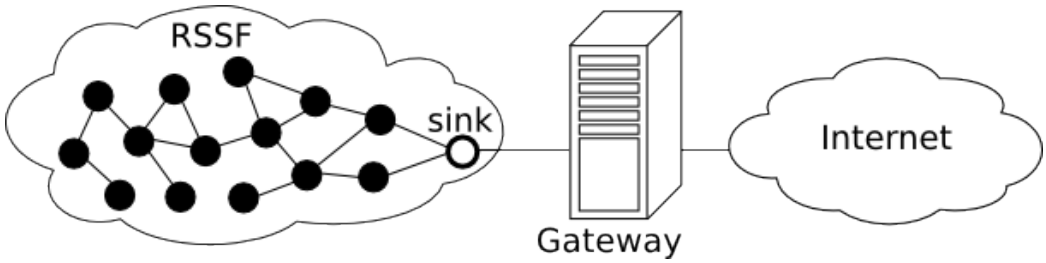


Figura 1: Topologia e acesso aos dados de uma RSSF

Na maioria de suas aplicações, os nós que constituem uma RSSF são responsáveis por coletar/sensoriar dados do ambiente e enviá-los para o nó conectado à máquina externa à rede. Este nó onde é concentrado o envio de todos os dados coletados é denominado sorvedouro, ou *sink* em inglês. Para que os dados de uma RSSF possam ser acessados por uma entidade externa à rede e, consequentemente, possam ser disponibilizados na Internet, é necessário a inserção de um outro elemento neste cenário, que realizará o papel de um *gateway*. Neste cenário a RSSF nada mais é para as entidades externas do que uma espécie de banco de dados distribuído, capaz de retornar dados conforme suas coletas e, em alguns casos, suportando inclusive consultas aos seus nós por meio de linguagens de consulta padrão SQL (*Structured Query Language*) [7].

Contudo, é importante que se destaque que este *gateway* é o que pode-se chamar de "*gateway* de aplicação", responsável por realizar traduções para as solicitações e respostas entre as duas redes distintas. Embora esta característica seja possível e desejada por algumas aplicações de RSSF, esta não é, de forma alguma, um ponto positivo quando trata-se do cenário da computação ubíqua e ambientes inteligentes da IoT. Em outras palavras, para se ter acesso de uma máquina externa a um determinado objeto inteligente, seria necessário que uma consulta fosse enviada para um terceiro componente que realizaria a tradução desta consulta e a enviaria para o objeto desejado, realizando o processo inverso durante a resposta desta consulta.

A utilização de um *gateway* para este tipo de caso traz algumas desvantagens. Vasseur e Dunkels [3] destacam como principais problemas desta utilização a complexidade inerente à tradução realizada pelo *gateway*, bem como a falta de flexibilidade e escalabilidade nesta abordagem. Sobre o primeiro problema, o processo de tradução entre protocolos não é uma tarefa simples, podendo prejudicar o desempenho na realização das tarefas do *gateway*, impactando em maiores atrasos na comunicação.

Do ponto de vista da flexibilidade e escalabilidade destas redes, pode-se destacar que a inserção deste *gateway* pode ser encarado como um gargalo na rede, que poderá inviabilizar que novas entidades possam comunicar-se através dele com um desempenho satisfatório bem como inserir um único ponto de falha na comunicação. Além disso, também irá afetar o princípio da comunicação fim-a-fim entre as aplicações, o que poderá prejudicar o surgimento de novas aplicações, que ainda não são suportadas pelos algoritmos de tradução do *gateway*.

Quanto a estes problemas, facilmente pode-se realizar um paralelo com um problema bem comum existente nas redes IP (*Internet Protocol*) [8]. Este é o problema do isolamento das redes privadas por meio de técnicas de NAT (*Network Address Translation*) [9]. O NAT, que foi uma solução temporária para o esgotamento dos endereços IP, em sua versão 4, trouxe problemas similares à inserção de um *gateway* de aplicação no processo de comunicação fim-a-fim.

Uma solução óbvia para ambos os casos é a remoção deste componente intermediador da comunicação, permitindo que o acesso entre máquinas e objetos inteligentes se dê de forma direta, sem necessitar a tradução das solicitações/respostas. Ou, ainda quando houver a necessidade um elemento de ligação entre as duas redes, devido às diferentes tecnologias de acesso ao meio, por exemplo IEEE 802.15.4 e IEEE 802.11 [10], que este não realize mais traduções, mas sim um processo de encaminhamento/roteamento entre os nós das duas diferentes redes.

# 4 A importância do IPv6 para IoT

Tendo-se destacado as principais diferenças entre as RSSF e a IoT, do ponto de vista do isolamento tolerável entre uma RSSF e o mundo externo a ela, e da constante necessidade que um elemento externo tem em acessar diretamente um objeto inteligente da IoT, como uma geladeira ou televisor, é necessário que estas diferenças sejam consideradas na escolha de uma solução viável para cada um destes cenários.

Quanto ao cenário da IoT, é importante notar que em suas aplicações destaca-se a necessidade de acesso direto aos objetos inteligentes. Por acesso direto, entende-se a abstração entre a comunicação de uma aplicação do lado do usuário e uma outra aplicação do lado do objeto inteligente, que permitirá o acesso e controle às suas funcionalidades. Portanto, uma primeira característica desejada para este caso é a interoperabilidade na comunicação entre os dispositivos. E, um dos maiores exemplos de interoperabilidade entre distintas redes de computadores é a Internet. De forma mais direta, na utilização do protocolo IP para a comunicação entre os dispositivos de rede.

A utilização de IP para esta comunicação agrega, diretamente, a necessidade da estruturação das premissas de comunicação em forma de camadas, seguindo a arquitetura TCP/IP [11]. A diferença entre as tecnologias de acesso serão resolvidos por meio das camadas 1 (física) e 2 (enlace) desta arquitetura, e a integração que permitirá a comunicação entre um usuário e um objeto inteligente dar-se-á, agora, através da unicidade de apenas um protocolo de rede, o IP (camada 3 da arquitetura). Esta abordagem permitirá a interoperabilidade entre as redes, uma vez que ambas seguirão um mesmo protocolo de rede.

Sobre o ponto de vista da flexibilidade, seguindo este novo modelo de organização, uma vez que o acesso direto, via rede, é permitido entre os usuários e os objetos inteligentes, a criação de novas aplicações segue a mesma filosofia da Internet. Isto é, para a comunicação entre duas aplicações em máquinas distintas, necessita-se apenas que ambas implementem o mesmo protocolo de aplicação, deixando a rede e seus componentes intermediários isentos desta responsabilidade. Assim, o surgimento de novas aplicações não está mais limitado às funcionalidades de um *gateway*.

Além disso, o fato da não existência de um *gateway*, mas sim um roteador entre as diferentes redes, acrescentará a vantagem da inexistência de um gargalo na comunicação, permitindo uma maior escalabilidade da rede, por meio da redução da complexidade de tradução, passando agora a ter-se apenas o roteamento entre as duas redes, um processo bem mais simples.

Contudo, tudo isto que foi discutido como vantagens da utilização do IP como protocolo de rede para a interoperabilidade na IoT somente será

possível se for garantida a comunicação fim-a-fim entre os usuários de um ambiente inteligente e seus objetos inteligentes. E, assim como já foi aqui citado, um problema similar à inserção de um *gateway* para a comunicação entre diferentes redes é a utilização da estratégia de NAT para as redes IPv4. Portanto, para este novo cenário da IoT, onde milhares de novos dispositivos necessitarão de acesso fim-a-fim entre seus usuários e eles, e que não poderão sofrer com as soluções temporárias à escassez de endereços IPv4, é visível que a melhor solução para este contexto é a utilização da evolução deste protocolo de rede, o IPv6 [12].

Uma das principais motivações para a utilização do protocolo IPv6 para a IoT reside na quantidade de endereços IP disponíveis. Enquanto que no IPv4 a quantidade de IP's é da ordem de $2^{32}$ endereços, considerando endereços privados e demais reservados, para o IPv6 este número equivale a $2^{128}$, onde 128 é o tamanho em bits de um endereço IPv6. Contudo, além disto, esta nova definição do protocolo IP em sua versão 6 pode ser caracterizada pelo retorno aos princípios fundamentais da arquitetura IP, que foram as ideias base para a criação da Internet [3].

Alguns destes princípios são: (i) a autoconfiguração dos nós em um enlace, que é uma característica fundamental para a operação prolongada dos objetos inteligentes, bem como na impossibilidade de manter um elemento encarregado de configurar os objetos em um ambiente inteligente, que poderão constituir-se de muitos componentes, até milhares, tornando esta tarefa muito complexa de ser alcançada; (ii) a otimização dos cabeçalhos do IPv6, com a retirada de campos desnecessários, a remoção de alguns campos mais específicos para cabeçalhos de extensão e ainda a fixação do tamanho do cabeçalho base são modificações que permitirão um melhor desempenho durante o tratamento dos pacotes IPv6, tarefa esta essencial para qualquer dispositivo de rede, principalmente aqueles com baixo poder computacional; e (iii) uma maior preocupação com a segurança e autenticação durante a comunicação, preocupações estas ainda mais justificadas quando os dados trafegados pelos objetos da IoT estão diretamente relacionados com a privacidade de seus usuários, como suas preferências e características pessoais, bem como suas atividades cotidianas e íntimas.

# 5 Desafios da utilização de IPv6 para IoT

Conforme previamente dito, uma das principais motivações na utilização do IPv6 para a IoT é a sua vasta quantidade de endereços disponíveis, que permitirá a atribuição de um, ou mais, endereços IPv6 a cada objeto inteligente, possibilitando que o seu acesso seja realizado de maneira a não ferir o

princípio de comunicação fim-a-fim. Contudo, esta vantagem também acrescenta uma nova preocupação para os desenvolvedores que implementarão esta nova versão do protocolo para os sistemas embarcados da IoT, que diz respeito às limitações do *hardware* e das camadas subjacentes ao IP nestes dispositivos.

Com relação ao tamanho do novo cabeçalho IPv6, era de se esperar que, enquanto no IPv4, que um endereço de rede tinha o tamanho de 32 bits e o tamanho mínimo de um cabeçalho IP é de 20 bytes, o tamanho de um cabeçalho IPv6 que possui endereços com tamanho de 128 bits fosse bem superior a estes 20 bytes. O cabeçalho IPv6 possui um tamanho de 40 bytes, exatamente o dobro do tamanho de sua versão 4 [13].

Embora este tamanho seja fixo, o que auxilia na otimização de seu processamento, ainda é suficientemente grande quando o dispositivo que armazenará tais pacotes possui pouca memória disponível para isto. Além disso, enquanto a especificação do IPv6 requer um valor mínimo de MTU (*Maximum Transmission Unit*) de 1280 bytes para as suas camadas superiores, para aqueles dispositivos que operarão IPv6 acima do protocolo IEEE 802.15.4 como camada de enlace, terá de operar com apenas 127 bytes, que é o valor do MTU deste protocolo de enlace. E, em alguns casos, alguns destes 127 bytes ainda serão utilizados por campos do IEEE 802.15.4. No pior caso, restarão apenas 81 bytes para o IPv6. Destes 81 bytes, após remover os 40 bytes do cabeçalho IPv6, restarão apenas 41 bytes e, em caso da utilização do TCP como protocolo de transporte, outros 20 byte serão utilizados para este protocolo [3]. Neste pior cenário, para a aplicação restarão apenas 21 bytes, que nos casos de aplicações baseadas em campos textuais, somente poderão ser utilizados 21 caracteres por pacote.

Para estes casos mais críticos de limitações no tamanho dos pacotes pelas camadas inferiores à de rede, foi idealizada uma camada de adaptação do protocolo IPv6 denominada 6LoWPAN (*Low-power Wireless Personal Area Network*) [14]. Esta adaptação baseia-se nas características do protocolo de enlace IEEE 802.15.4 que incluem, além das aqui já discutidas, suporte tanto a endereços físicos de 64 bits (endereços MAC – *Media Access Control*) quanto a endereços curtos de 16 bits, baixas taxas de transmissão de 20 Kbps a 250 Kbps, suporte ao estabelecimento de topologia em nívell de enlace, suporte a uma grande quantidade de dispositivos, que podem altenar entre períodos de inatividade, quando desligam seu rádio ou quando movem-se para fora do alcance de seus vizinhos entre outros [6].

Dentre os serviços providos pelo 6LoWPAN, dois que se destacam são: (i) a fragmentação de pacotes e a sua posterior remontagem, (ii) a compressão do cabeçalho IPv6. Estes dois serviços têm como principal objetivo otimizar a utilização dos poucos bits disponíveis para a camada de rede, seu cabeçalho

e *payload*. A fragmentação ocorre quando a quantidade de dados que o pacote IPv6 precisa enviar é maior do que o tamanho permitido em um simples quadro IEEE 802.15.4. A compressão do cabeçalho IPv6 consiste, basicamente, na ideia de evitar a inserção no pacote de informações desnecessárias e redundantes, e na supressão de cabeçalhos e campos que possuem valores comuns, tipicamente campos com valores 0).

# 6 Conclusões

A integração entre as estratégias e avanços da Internet com os conceitos e pesquisas direcionadas à criação dos ambientes inteligentes tem se destacado como uma promissora linha de estudo e desenvolvimento, capaz de revolucionar a forma como os usuários utilizam os sistemas computacionais, auxiliando-os ainda mais na resolução dos desafios de suas tarefas cotidianas. A Internet das Coisas tem despertado o interesse não somente nos entusiastas deste novo paradigma, mas também dos investidores, que estimam lucros da ordem de bilhões de dólares já para os próximos anos.

No entanto, para que este cenário de ambientes inteligentes, computação ubíqua e conectividade total entre objetos inteligentes por meio da Internet torne-se uma realidade, ainda faz-se necessário que muitos esforços sejam empreendidos, tanto por pesquisadores quanto empresas, com o intuito de encontrar soluções eficientes e otimizadas para as necessidades deste novo cenário.

Contudo, é fácil notar que um dos principais desafios cuja solução servirá de base para todas as posteriores reside na necessidade de garantir-se que todos estes objetos inteligentes possuam conectividade, isto é, que possam acessar e ser acessados por meio de uma rede de comunicação. Nesta direção, muita coisa já foi conduzida para uma solução aceita por todos os seus pesquisadores e desenvolvidores, que é a adoção do IPv6 como o protocolo de rede que permitirá tal conectividade.

Neste documento foi discutida a importância do IPv6 para a criação de um ambiente inteligente da IoT, sendo capaz de suportar uma grande quantidade de objetos inteligentes, uma característica inerente a este novo cenário, e que permite garantir a comunicação fim-a-fim entre estes dispositivos. Além disso, também foram apresentadas otimizações e adaptações do IPv6 que serão de grande valia para a utilização eficiente dos limitados recursos computacionais dos dispositivos embarcados, principais componentes da IoT.

# Referências


[1] Mark Weiser. The Computer for the 21ST Century. *Scientific American*, 265(3):94–104, 1991.

[2] S.S. Intille. Designing a home of the future. *IEEE Pervasive Computing*, 1(2):76–82, April 2002.

[3] Jean-Philippe Vasseur and Adam Dunkels. *Interconnecting Smart Objects with IP: The Next Internet*. Morgan Kaufmann Publishers Inc., 2010.

[4] Antonio A F Loureiro, José Marcos S Nogueira, Linnyer B Ruiz, Raquel A Mini, Eduardo F Nakamura, and Carlos M S Figueiredo. Wireless Sensor Networks (in Portuguese). In *Proceedings of the 21st Brazilian Symposium on Computer Networks (SBRC'03)*, pages 179–226, Natal, RN, Brazil, May 2003.

[5] Joao B. Borges Neto, Rossana M. C. Andrade, and Pedro F. Ribeiro Neto. Wireless Sensor Networks Advances for Ubiquitous Computing. In *Designing Solutions-Based Ubiquitous and Pervasive Computing: New Issues and Trends*, chapter 9, pages 175–189. IGI Global, 2010.

[6] IEEE Computer Society. *IEEE Standard for Local and metropolitan area networks — Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)*. Number June. IEEE, 2011.

[7] P F Ribeiro Neto, Angelo Perkusich, Maria Ligia Barbosa Perkusich, and H O Almeida. A Formal Verification and Validation Approach for Real-Time Database. In Aristides Dasso and Ana Funes, editors, *Verification, Validation and Testing in Software Engineering*. Idea Group Inc., Hershey, PA, 2005.

[8] J. Postel. Internet protocol, 1981.

[9] P. Srisuresh and K. Egevang. Traditional ip network address translator (traditional nat), 2001.

[10] IEEE Computer Society. *IEEE Standard for Information technology — Telecommunications and information Local and metropolitan area networks — Part 11 : Wireless LAN Medium Access Control (MAC)*. IEEE Computer Society, 2007.

[11] J. Postel. Transmission control protocol, 1981.

[12] S. Deering and R. Hinden. Internet protocol, version 6 (ipv6) specification, 1998.

[13] James F. Kurose and Keith W. Ross. *Redes de Computadores e a Internet - Uma Abordagem Top-down.* Pearson, 5a ed edition, 2010.

[14] N. Kushalnagar, G. Montenegro, and C. Schumacher. Ipv6 over low-power wireless personal area networks (6lowpans): Overview, assumptions, problem statement, and goals, 2007.