

6LoWPAN - Adaptação do Protocolo IPv6 para a Internet das Coisas

Hermano Pereira

Universidade Tecnológica Federal do Paraná - UTFPR

Avenida Sete de Setembro, 3165

Curitiba-PR - CEP 80.230-910

E-mail: pereira@hermano.com.br

Resumo—O padrão 6LoWPAN permite que dispositivos com recursos escassos venham a fazer parte da Internet convencional, ou seja, a Internet das Coisas. Neste artigo é feito um levantamento sobre o padrão 6LoWPAN, suas funções, novos protocolos e a adaptação de outros protocolos.

I. INTRODUÇÃO

A Internet das Coisas vem se destacando tanto no mercado como na comunidade científica devido à junção de dois mundos diferentes: a Internet e as pequenas coisas, tais como controles remotos, sensores, alarmes, entre outros. Essas pequenas coisas são os dispositivos que estão fazendo parte do dia-a-dia das pessoas, porém estão no mercado sem terem acesso via Internet, e muitas vezes limitados apenas ao acesso local. A IETF, que é a entidade responsável pelos padrões e protocolos da Internet, observou essa necessidade e está com diversos grupos de trabalho em andamento para atender essa demanda. O principal trabalho da IETF no momento certamente é o padrão 6LoWPAN. O objetivo deste artigo foi fazer um levantamento de como funciona o padrão 6LoWPAN e as mudanças na pilha de protocolos, visto que os dispositivos chamados de coisas, são dispositivos que possuem baixa capacidade computacional, baixa consumo de energia e baixa taxa de dados.

A seção II fala sobre o 6LoWPAN na Internet das Coisas; na seção III é observado o uso do padrão IEEE 802.15.4 como base das redes 6LoWPAN; As topologias são descritas na seção IV e como a camada de adaptação de 6LoWPAN é introduzida na pilha de protocolos está descrita na seção V. As funções da camada de adaptação são o resumo de endereços (seção VI), a fragmentação do datagrama IPv6 (seção VII) e a compressão do datagrama IPv6 (seção VIII). O 6LoWPAN precisou de protocolo próprio para descoberta de vizinhos, o 6LoWPAN-ND na seção IX; também houve a necessidade de um protocolo específico para o roteamento, o RPL na seção X. Além da compressão de cabeçalhos IPv6, também houve especificação para comprimir o cabeçalho UDP, na seção XI; e um protocolo compatível e semelhante ao HTTP, chamado CoAP, na seção XII. Detalhes de segurança e criptografia em redes 6LoWPAN na seção XIII. E por fim, a prospecção (seção XIV) e considerações finais (seção XV).

II. 6LoWPAN E A INTERNET DAS COISAS

Permitir que dispositivos computacionalmente restritos possam ser acessados por protocolos da Internet é o objetivo da Internet das Coisas (*Internet of Things* - IoT) [1]. Esses dispositivos, chamados de coisas (*things*), são dispositivos comuns no dia-a-dia das pessoas, tais como lâmpadas, controles remotos, sensores de presença; mas também são encontrados em ambientes hospitalares, veículos, automação industrial, entre outros ambientes. De acordo com a Cisco, em 2020 haverá mais de 50 bilhões de dispositivos na IoT; e em média haverá 6,5 dispositivos por habitante do planeta, os quais irão interagir com os protocolos da Internet [2]. A IoT consiste em interconectar esses mundos diferentes da tecnologia: a Internet e as redes pessoais sem fio (WPAN - *Wireless Personal Area Network*) e, ainda, as redes de sensores sem fio (WSN - *Wireless Sensors Network*), assim ilustra a figura 1. Suportar comunicação com baixo consumo de energia, altamente confiável e compatível com a Internet, são requisitos para a IoT conforme [3]. Porém, ao adicionar mais dispositivos para à Internet, torna necessário que o endereçamento seja adequado, e isso pode ser suprido pelo padrão de endereçamento do IPv6 (*Internet Protocol version 6*); e, além disso, o protocolo IPv6 precisa ser adaptado para a transmissão de dados entre dispositivos restritos de recursos. Fazer tal adaptação foi o objetivo do padrão 6LoWPAN (IPv6 over Low power WPAN).

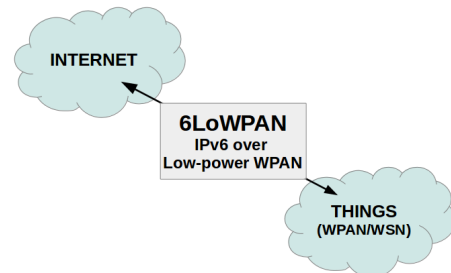


Figura 1. Internet, 6LoWPAN e as coisas.

III. IETF 6LoWPAN E IEEE 802.15.4

O grupo de trabalho 6LoWPAN [4] foi designado pela IETF (*Internet Engineering Task Force*) para fazer com que o

protocolo IPv6 viesse operar sobre o padrão de redes sem fio 802.15.4 do IEEE (*Institute of Electrical and Electronics Engineers*). As seguintes características são definidas pelo padrão IEEE 802.15.4 [5] para a comunicação entre os dispositivos de redes sem fio: baixa complexidade, baixo custo, baixo consumo de energia e baixa transferência de dados. O IEEE 802.15.4 opera nos mesmos canais de Bluetooth e WiFi, são 16 canais de banda não-licenciada na faixa de 2400 a 2483.5 MHz, e as taxas de transmissão podem atingir até 250 Kbps. A preferência pelo IEEE 802.15.4 para a padronização de dispositivos IoT está no seu baixo consumo de energia, conforme o trabalho de [6] o consumo de energia durante o tempo de repouso (*sleep*) nesse padrão é notavelmente mais baixo do que os padrões IEEE 802.11 (WiFi) e IEEE 802.15.1 (Bluetooth). Além disso, outros padrões como ZigBee, WirelessHART e ISA100 operam sobre IEEE 802.15.4; porém, a integração com o protocolo IPv6 é feita com 6LoWPAN.

IV. TOPOLOGIAS

Existem dois tipos de topologia em uma rede IEEE 802.15.4 [5]: estrela (*star*) ou ponto-a-ponto (*peer-to-peer*); e a sua formação é composta por dois tipos de dispositivos: RFDs (*Reduced Function Devices*) e FFDs (*Full Function Devices*). Os RFDs são dispositivos que ficam na ponta da topologia e são reduzidos computacionalmente, e possivelmente são aqueles que implementam o tempo de repouso (*sleep*) para economizar o uso de energia de uma bateria. Já os FFDs são dispositivos que possuem mais recursos e podem assumir mais funções, como a comutação entre outros nós na rede sem fio e, até mesmo, assumir a função de nó raiz (também chamado *sink*) - coordenador PAN da topologia (ilustração na figura 2). Essa configuração é válida para redes tipo *star*, mas também é possível formar topologias *peer-to-peer* onde os nós envolvidos fazem comutação assim como uma rede *mesh*.

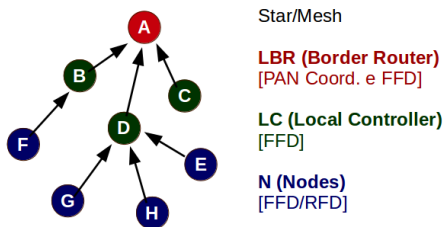


Figura 2. Topologia estrela e dispositivos (IEEE 802.15.4 vs 6LoWPAN)

A topologia formada pelo padrão 6LoWPAN (RFCs 4919 [7] e 6568 [8]) apenas se adapta ao padrão IEEE 802.15.4, e são definidos três tipos de dispositivos: LBR (*LoWPAN Border Router*), LC (*LoWPAN Local Controller*) e N (*LoWPAN Node*). O dispositivo LBR é o mesmo nó raiz FFD, o qual é responsável em fazer a ponte entre uma rede local WPAN e uma rede IPv6. Os dispositivos LC, podendo ser FFDs ou RFDs, são aqueles que fazem a comutação e controle dos dispositivos finais. Por sua vez os dispositivos N, também podem ser FFDs ou RFDs, atuam como dispositivos finais em uma rede 6LoWPAN. Em uma topologia *star*, um nó LBR

é configurado como raiz entre diversos nós LCs e Ns, já a topologia *mesh* é formada por dispositivos LBRs (ilustração na figura 2).

V. PILHA DE PROTOCOLOS

Seguindo o modelo de camadas de redes de computadores, as subcamadas PHY (*Physical Layer*) e MAC (*Media Access Control*) fazem parte da camada física que competem ao padrão IEEE 802.15.4. Para que as camadas superiores pudessem ter acesso ao meio físico, isso ficou a cargo do padrão 6LoWPAN [7], o qual define uma camada de adaptação (*LoWPAN Adaptation Layer*). O 6LoWPAN tem a função de comprimir cabeçalhos IPv6, fragmentar datagramas e resumir endereços IPv6 (mais detalhes nas seções VI, VII e VIII). Nas camadas superiores também são necessárias adaptações para que se reduza a sobrecarga de informações em uma rede IoT. Na camada de rede (*Network Layer*) estão os protocolos: IPv6 (roteável), ICMPv6 (mensagens de controle), 6LoWPAN-ND (descoberta de vizinhos) e RPL (roteamento), tais protocolos estão detalhados nas seções IX e X. Para o transporte também foi necessário reduzir a quantidade de informações, assim na camada de transporte (*Transport Layer*) encontra-se o protocolo UDP e o seu cabeçalho reduzido está detalhado na seção XI. Para a comunicação fim-a-fim entre as aplicações, um protocolo da camada de aplicação (*Application Layer*) baseado no HTTP foi especificado: o CoAP, detalhado na seção XII. As camadas e os respectivos protocolos estão ilustrados na figura 3.

Aplicação	CoAP
Transporte	UDP
Rede	IPv6 (ICMPv6 / 6Lo-DP / RPL)
Adaptação	6LoWPAN
Enlace	IEEE 802.15.4 MAC
Física	IEEE 802.15.4 PHY

Figura 3. Pilha de protocolos e a camada de adaptação 6LoWPAN

VI. RESUMO DE ENDEREÇOS

Devido ao tamanho máximo de um quadro IEEE 802.15.4 estar limitado à 127 bytes, isso fez com que esses padrões viessem a encontrar formas de resumir o endereço MAC e o endereço IPv6. Na subcamada MAC, o endereço pode ter 64 bits (8 bytes) no formato *macExtendedAddress* ou pode ser reduzido a 16 bits (2 bytes) no formato *macShortAddress*, economizando assim 48 bits (6 bytes) [5]. O endereço estendido é único e definido pelo fabricante da placa de rede, já o endereço reduzido é configurável.

Já o endereço IPv6 contém 128 bits (16 bytes), e conforme especificado na RFC 6282 [9] na camada de adaptação é possível resumir os endereços de acordo com uma identificação de contexto (CID - *Context Identifier*). Pode-se assumir os seguintes formatos de endereçamento: i)

Normal, 128 bits; ii) 64 bits, suprimindo os primeiros 64 bits (neste caso pode utilizar o EUI-64 - *Extended Unique Identifier*); iii) 16 bits, suprimindo os primeiros 112 bits (neste caso é utilizado um endereçamento específico e local); iv) 0, suprimindo inteiramente os 128 bits, mas se torna necessária a comutação com base no endereço MAC.

Se considerar os endereços de origem e destino, o uso de endereços completos pode levar à 384 bits (48 bytes): 128 bits para o MAC (64+64 bits de origem e destino) e 256 bits para o IPv6 (128+128 bits de origem e destino). Mas se os endereços forem resumidos, pode-se economizar até 352 bits (44 bytes) ao se utilizar apenas 32 bits no MAC (16+16 bits de origem e destino). Porém o resumo máximo suprime as informações necessárias para roteamento na camada de adaptação, então o mínimo para um datagrama roteável seriam os 16 bits adicionais para identificar o destino do datagrama, mesmo assim a economia pode chegar até 336 bits (42 bytes): 32 bits no MAC (16+16 de origem e destino) e 16 bits no IPv6 (apenas destino).

VII. FRAGMENTAÇÃO DO DATAGRAMA IPv6

Outra função importante da camada de adaptação 6LoWPAN é a fragmentação de datagramas, pois a MTU (*Maximum Transmission Unit*) de 127 bytes para quadros IEEE 802.15.4, é incompatível com a definição mínima de 1280 bytes de MTU do datagrama IPv6 (ilustração na figura 4). Para isso, os documentos RFCs (*Requests For Comments*) 4919 [7] e 4944 [10] especificam como os datagramas IPv6 poderão ser fragmentados na camada de adaptação. Nesse processo, cada datagrama IPv6 é fragmentado em partes menores para serem encapsulados em quadros IEEE 802.15.4, que podem ter a carga útil variável até 102 bytes, e assim são adicionados três campos de informação para cada fragmento: tamanho do datagrama, *tag* do datagrama e *offset* do datagrama. Essas informações também estão relacionadas com a compressão de cabeçalhos que é o assunto da próxima seção. Em especial, um pequeno resumo adicionado durante a fragmentação está no primeiro datagrama que não precisa carregar o campo de *offset*, pois subentende-se que o campo *offset* é zero. O uso de fragmentação é um recurso que deve ser evitado por sensores que possui baixa capacidade, pois isso pode fazer com que seja necessário memória (*buffer*) suficiente para reordenar e remontar os fragmentos recebidos, causando uma maior sobrecarga em dispositivos que possuem restrição de recursos.

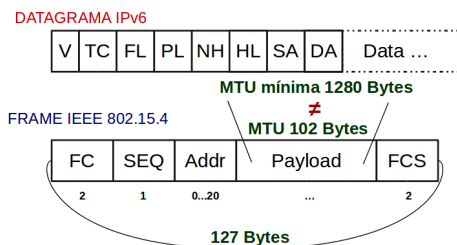


Figura 4. Fragmentação de datagramas vs MTUs

VIII. COMPRESSÃO DE CABEÇALHOS IPv6

Se considerar a MTU de 127 bytes de um quadro IEEE 802.15.4, e se forem adicionadas as informações básicas de cabeçalho da subcamada MAC (23 bytes) e adição da verificação de erros (2 bytes) - FCS - *Frame Check Sequence* - restam apenas 102 bytes de carga útil (*payload*) para a camada de adaptação. E, se considerar o nível de segurança mais alto do IEEE 802.15.4, serão necessários mais 21 bytes de cabeçalho MAC, reduzindo ainda mais a carga útil para 81 bytes. Ao se considerar o cabeçalho IPv6 de 40 bytes (RFC 2460 [11]) e, ainda, o cabeçalho UDP de 8 bytes (RFC 768 [12]), restariam apenas 33 bytes de carga útil para a camada de aplicação. Portanto, faz-se necessário a compressão dos cabeçalhos IPv6 na camada de adaptação 6LoWPAN visando aumentar a carga útil para as camadas superiores.

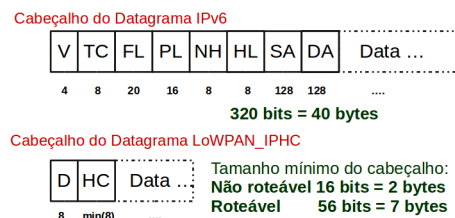


Figura 5. Compressão de cabeçalhos IPv6

O documento RFC 4944 [10] define 8 tipos de cabeçalhos, esses cabeçalhos são identificados com um código de envio (*dispatch*). Cada código identifica se os quadros são LoWPAN ou IPv6; se o cabeçalho está ou não comprimido; se o datagrama está fragmentado ou não; informações de *broadcasting* ou de roteamento *mesh*, com códigos reservados para o uso futuro. A técnica definida como LoWPAN_HC1 (*Header Compression 1*) pode fazer a compressão de um cabeçalho IPv6 de 40 bytes para até 2 bytes sem contabilizar o código de envio, ou seja, 3 bytes contando com o código de envio; uma economia de 37 bytes. Porém, o LoWPAN_HC1 não leva em conta a compressão do campo de limite de saltos (*hop limit*) do protocolo IPv6, que são 8 bits adicionais; para tanto, o documento RFC 6282 [9] veio a propor uma melhoria, comprimindo também este campo do cabeçalho. Sendo assim um novo código de envio foi adicionado através da técnica chamada LoWPAN_IPHC (*IPv6 Header Compression*). Uma melhoria foi na utilização dos bits restantes do próprio código de envio para carregar informações do cabeçalho e, além disso, uma mudança no contexto de endereçamento para identificar se há ou não endereços de origem e destino. Sendo assim o cabeçalho do protocolo IPv6 pode ser reduzido de 40 bytes para 2 bytes (incluindo o código de envio), e no caso de um datagrama ser roteável, um mínimo de 7 bytes (incluindo o código de envio) - ilustração na figura 5. Em suma, um cabeçalho IPv6, de um datagrama roteável, ao ser comprimido pode representar uma economia de 33 bytes.

IX. DESCOBERTA DE VIZINHOS COM 6LoWPAN-ND

Um recurso importante em redes IPv6 é o mapeamento de endereços de rede para endereços MAC, e isso é feito pelo protocolo NDP (*Network Discovery Protocol*), documentado nas RFCs 4861 [13] e 4862 [14]. Um problema na implementação desse protocolo em redes 6LoWPAN está na grande quantidade de mensagens de *multicast* que podem inundar e onerar dispositivos que operam em tempo de espera (*sleep*). Além disso, a compressão de cabeçalhos também afeta o uso deste protocolo. Como solução o documento RFC 6775 [15] especifica um protocolo específico de descoberta para esse tipo de rede, o protocolo 6LoWPAN-ND (*Network Discovery*).

Diversas modificações foram feitas no protocolo 6LoWPAN-ND em relação ao NDP: 1) mensagens de RA (*Router Advertisement*) são enviadas apenas quando são solicitadas, ao contrário das mensagens enviadas periodicamente no protocolo NDP; 2) resolução de endereços com uso de *multicast* desabilitada; 3) mensagens *unicast* com informações específicas para os nós que saem do tempo de repouso para identificar seu roteador padrão; 4) modificações específicas para a divulgação de prefixos de endereçamento em redes 6LoWPAN; 5) novo mecanismo para detectar endereços duplicados. Além disso, foram necessários novos campos no protocolo ICMPv6 (*Internet Control Message Protocol*) para atender as funcionalidades do protocolo 6LoWPAN-ND.

X. ROTEAMENTO

Conforme o documento RFC 6606 [16] é possível fazer dois tipos de roteamento em redes 6LoWPAN: *mesh-under* para roteamento na camada de adaptação e *route-over* na camada de rede. Para o roteamento *mesh-under* os dispositivos FFDs em uma topologia IEEE 802.15.4 podem fazer comutação de quadros e, portanto, o cabeçalho LoWPAN_HC1 pode ser configurado para carregar informações de roteamento *mesh*. Porém o documento RFC 4944 [10] não especifica como as tabelas de roteamento serão construídas.

Já, para *route-over* o grupo de trabalho ROLL (*Routing over Low power and Lossy Networks*) [17] foi designado para trabalhar com padrões de roteamento para esse tipo de rede. Como resultado o protocolo RPL (*IPv6 Routing Protocol for Low power and Lossy Networks*) foi especificado na RFC 6550 [18]. O objetivo do protocolo RPL é formar uma árvore de escoamento entre os nós que seja livre de *loopings*, formando assim um grafo da topologia conhecido como DAG (*Directed Acyclic Graph*). Pequenas topologias são formadas por DODAGs (*Destination Oriented DAG*) onde um nó principal, conhecido como *sink* ou apenas LBR em redes 6LoWPAN, que é o nó responsável por interconectar os nós adjacentes com os outros nós LBRs.

Cada nó que ingressa em uma topologia RPL DODAG, primeiro envia mensagens DIS (*DODAG Information Solicitation*) com o intuito de avisar aos nós vizinhos que há um novo nó RPL. Os nós vizinhos, então, enviam suas informações de roteamento através de mensagens DIO (*DODAG Information Object*), o qual contém um valor de classificação (*rank*) para

auxiliar os outros nós na decisão de roteamento. Por sua vez, o novo nó também faz o cálculo do seu próprio valor de *rank* e envia aos nós vizinhos. Além disso, o novo nó faz sua confirmação de escolha do nó pai através de mensagens DAO (*Destination Advertisement Object*) que chegarão até o nó raiz. O protocolo RPL, apesar de conter uma variedade de opções para tratar de métricas de roteamento, na prática contém poucas mensagens de roteamento e um algoritmo de pingo (*trickle*). Esse algoritmo faz com que o tempo de mensagens trocadas entre os nós seja incrementado na medida em que a topologia fica estável, sendo assim atrativo para dispositivos que dispõem de pouca energia e necessitam enviar poucas mensagens de configuração.

XI. COMPRESSÃO DE CABEÇALHOS UDP

Na camada de transporte, o protocolo UDP (*User Datagram Protocol*) é utilizado para transportar mensagens em redes 6LoWPAN, e no documento RFC 4944 [10] é especificada uma compressão do cabeçalho UDP de 8 bytes para 4 bytes. Neste caso a técnica HC_UDP permite comprimir os campos de porto de origem e de destino e, também, comprimir o campo tamanho. Uma melhoria para a compressão neste cabeçalho está no documento RFC 6282 [9], onde o cabeçalho LoWPAN_NHC permite que o protocolo UDP suprima a informação de verificação de erros (*checksum*); permitindo, assim, comprimir o cabeçalho UDP de 8 bytes para apenas 2 bytes.

XII. PROTOCOLO DE APLICAÇÃO COAP

Como na *Internet* os aplicativos estão convergindo para o ambiente *web*, a IETF designou um grupo para trabalhar com padrões de aplicações *web* para redes do tipo 6LoWPAN, grupo este chamado de CoRE (*Constrained RESTful Environments*) [19]. Para isso, este grupo trabalhou com especificações de *web services* RESTful (*Representation State Transfer*) e permitir a compatibilidade com o protocolo HTTP (*Hypertext Transfer Protocol*). Este trabalho resultou no protocolo CoAP (*Constrained Application Protocol*) conforme o documento RFC 7252 [20]. Por operar de maneira semelhante ao protocolo HTTP, o CoAP possui os mesmos métodos como GET e POST, tipo de conteúdo (*content-type*) e até mesmo identificador para acesso remoto URI (*Uniform Resource Identifier*). Além de parecer uma versão binária do HTTP, o protocolo CoAP, este também pode fazer com que as mensagens sejam confirmáveis ou não, visto que esta confiabilidade não foi implementada nas camadas inferiores. Por fim, não há uma comparação de tamanho entre CoAP e HTTP, até porque o CoAP possui poucos recursos, mas o simples fato de codificar em binário (por exemplo o método POST) ao invés de bytes no caso do HTTP, irá permitir aos nós que possam carregar mais informações de carga útil com relação às informações de controle e configuração.

XIII. SEGURANÇA E CRIPTOGRAFIA

De acordo com o padrão IEEE 802.15.4 [5] é possível implementar um forte mecanismo de proteção na subcamada

MAC. A transmissão de quadros entre os nós pode ser configurada com ou sem autenticação e com ou sem confidencialidade. Sendo assim, é possível ter 8 níveis de segurança: nível 0 sem segurança; no níveis 1 ao 3 os quadros são autenticados com MIC (*Message Integrity Code*) de 32, 64 e 128 bits; no nível 4 os quadros são apenas criptografados com AES (*Advanced Encryption Standard*); nos níveis 5 ao 7 os quadros são criptografados e autenticados com 32, 64 e 128 bits com algoritmo AES-CCM (*Counter with Cipher Block Chaining-Message*). Este último acaba adicionando 21 bits no cabeçalho da subcamada MAC.

Nas demais camadas não há especificação de autenticação e confidencialidade, porém o protocolo DTLS (Datagram Transport Layer Security) é o que melhor se adequa para fazer a proteção das mensagens CoAP da camada de aplicação. Este protocolo opera sobre UDP e está documentado na RFC 6347 [21]. Este protocolo adiciona uma sobrecarga na comunicação em redes com recursos escassos, porém atribui uma certa proteção na pilha de protocolos 6LoWPAN.

XIV. PROSPECÇÃO

No momento o grupo de trabalho 6LoWPAN da IETF foi concluído [4], mas o resultado de seu trabalho é hoje o padrão de base para outro grupo que prossegue neste segmento, o grupo 6lo (*IPv6 over Network of Resource-constrained Nodes*) [22]. Este grupo está trabalhando com padrões que venham a atender outros meios de acesso além do IEEE 802.15.4, como por exemplo o BT-LE (*Bluetooth Low Energy*). Além disso os outros grupos já citados anteriormente continuam ativos: ROLL [17], CoRE [19] e 6TiSCH. Este último um grupo designado especificamente para atuar na adaptação do 6LoWPAN ao padrão IEEE 802.15.4e [5], conhecido como TSCH (*Timeslotted Channel Hopping*), por isso 6TiSCH (IPv6 over the TSCH mode IEEE 802.15.4e) [23].

XV. CONSIDERAÇÕES FINAIS

O padrão 6LoWPAN permite que o protocolo IPv6 seja utilizado em redes com recursos reduzidos, fazendo resumos de endereços, compressão de cabeçalhos e fragmentação de datagramas. Além disso, outros protocolos precisaram ser especificados para atender esse tipo de rede: 6LoWPAN-ND, RPL e CoAP. O protocolo IPv6, ICMPv6 e UDP precisaram ser adaptados. Esse trabalho do IETF está tornando realidade a conexão de dispositivos limitados de recursos com a Internet mundial, isso está sendo referenciado como a Internet das Coisas (IoT).

REFERÊNCIAS

- [1] J. Tan and S. Koo, "A Survey of Technologies in Internet of Things," in *Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on*, May 2014, pp. 269–274.
- [2] D. Evans, "The Internet of Things - How the Next Evolution of the Internet Is Changing Everything," in *Cisco White Paper*, Apr 2011.
- [3] M. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, and M. Dohler, "Standardized Protocol Stack for the Internet of (Important) Things," *Communications Surveys Tutorials, IEEE*, vol. 15, no. 3, pp. 1389–1406, Third 2013.
- [4] "IETF Working Group - IPv6 over Low power WPAN (6lowpan)." [Online]. Available: <http://datatracker.ietf.org/wg/6lowpan/charter/>
- [5] "P802.15.4 - IEEE Approved Draft Standard for Local and metropolitan area networks - Part 15.4: Low-Rate Wireless Personal Area Networks (WPANs)," 2011. [Online]. Available: <http://standards.ieee.org/getieee802/download/802.15.4-2011.pdf>
- [6] K. Gravogl, J. Haase, and C. Grimm, "Choosing the Best Wireless Protocol for Typical Applications," in *ARCS Workshops*, W. Karl and D. Soudris, Eds. VDE-Verlag, 2011.
- [7] N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals," RFC 4919 (Informational), Internet Engineering Task Force, Aug. 2007. [Online]. Available: <http://www.ietf.org/rfc/rfc4919.txt>
- [8] E. Kim, D. Kaspar, and J. Vasseur, "Design and Application Spaces for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)," RFC 6568 (Informational), Internet Engineering Task Force, Apr. 2012. [Online]. Available: <http://www.ietf.org/rfc/rfc6568.txt>
- [9] J. Hui and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks," RFC 6282 (Proposed Standard), Internet Engineering Task Force, Sep. 2011. [Online]. Available: <http://www.ietf.org/rfc/rfc6282.txt>
- [10] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks," RFC 4944 (Proposed Standard), Internet Engineering Task Force, Sep. 2007, updated by RFCs 6282, 6775. [Online]. Available: <http://www.ietf.org/rfc/rfc4944.txt>
- [11] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC 2460 (Draft Standard), Internet Engineering Task Force, Dec. 1998, updated by RFCs 5095, 5722, 5871, 6437, 6564, 6935, 6946, 7045, 7112. [Online]. Available: <http://www.ietf.org/rfc/rfc2460.txt>
- [12] J. Postel, "User Datagram Protocol," RFC 768 (INTERNET STANDARD), Internet Engineering Task Force, Aug. 1980. [Online]. Available: <http://www.ietf.org/rfc/rfc768.txt>
- [13] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)," RFC 4861 (Draft Standard), Internet Engineering Task Force, Sep. 2007, updated by RFCs 5942, 6980, 7048. [Online]. Available: <http://www.ietf.org/rfc/rfc4861.txt>
- [14] S. Thomson, T. Narten, and T. Jinmei, "IPv6 Stateless Address Autoconfiguration," RFC 4862 (Draft Standard), Internet Engineering Task Force, Sep. 2007. [Online]. Available: <http://www.ietf.org/rfc/rfc4862.txt>
- [15] Z. Shelby, S. Chakrabarti, E. Nordmark, and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)," RFC 6775 (Proposed Standard), Internet Engineering Task Force, Nov. 2012. [Online]. Available: <http://www.ietf.org/rfc/rfc6775.txt>
- [16] E. Kim, D. Kaspar, C. Gomez, and C. Bormann, "Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing," RFC 6606 (Informational), Internet Engineering Task Force, May 2012. [Online]. Available: <http://www.ietf.org/rfc/rfc6606.txt>
- [17] "IETF Working Group - Routing Over Low power and Lossy networks (roll)." [Online]. Available: <http://datatracker.ietf.org/wg/roll/charter/>
- [18] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," RFC 6550 (Proposed Standard), Internet Engineering Task Force, Mar. 2012. [Online]. Available: <http://www.ietf.org/rfc/rfc6550.txt>
- [19] "IETF Working Group - Constrained RESTful Environments (CoRE)." [Online]. Available: <http://datatracker.ietf.org/wg/core/charter/>
- [20] Z. Shelby, K. Hartke, and C. Bormann, "The Constrained Application Protocol (CoAP)," RFC 7252 (Proposed Standard), Internet Engineering Task Force, Jun. 2014. [Online]. Available: <http://www.ietf.org/rfc/rfc7252.txt>
- [21] E. Rescorla and N. Modadugu, "Datagram Transport Layer Security Version 1.2," RFC 6347 (Proposed Standard), Internet Engineering Task Force, Jan. 2012. [Online]. Available: <http://www.ietf.org/rfc/rfc6347.txt>
- [22] "IETF Working Group - IPv6 over Networks of Resource-constrained Nodes (6lo)." [Online]. Available: <https://datatracker.ietf.org/wg/6lo/charter/>
- [23] "IETF Working Group - IPv6 over the TSCH mode of IEEE 802.15.4e (6tisch)." [Online]. Available: <https://datatracker.ietf.org/wg/6tisch/charter/>