

Capítulo

1

Multihop MAC: Desvendando o Padrão 802.11s

Débora Christina Muchaluat Saade, Arthur Guerrante Gomes,
Ricardo Campanha Carrano, Luiz Cláudio Schara Magalhães,
Célio Vinicius Neves Albuquerque, Liane Rockenbach Tarouco

Abstract

This chapter presents the IEEE standard for wireless multihop networks, 802.11s, discussing its uses and current implementations. The main innovation of the IEEE 802.11s standard is the creation of a layer-two mesh, by multihop forwarding at the MAC level, in contrast to traditional layer-three approaches. This chapter presents the main concepts of regular IEEE 802.11 wireless local area networks and briefly describes traditional layer-three multihop routing solutions. Then a detailed discussion of the mechanisms behind the 802.11s multihop MAC features is carried out. Pilot projects implementing mesh networks using both layer-two and layer-three approaches are also discussed.

Resumo

Este capítulo tem como objetivo principal apresentar o padrão emergente para redes sem fio com múltiplos saltos sendo proposto pelo IEEE 802.11s. O padrão IEEE 802.11s é inovador, pois propõe uma solução para encaminhamento através de múltiplos saltos no nível de enlace, o que difere das soluções tradicionais que operam no nível de rede. O capítulo aborda os principais conceitos de redes locais sem fio que seguem o padrão IEEE 802.11, apresenta brevemente as soluções tradicionais para comunicação com múltiplos saltos no nível de rede e discute em detalhes a proposta de padronização do IEEE 802.11s para comunicação em múltiplos saltos no nível MAC. Projetos piloto que implementam ambas as abordagens para comunicação sem fio através de múltiplos saltos também são comentados

1.1. Introdução

Redes locais sem fio (WLANs – *Wireless Local Area Networks*) que seguem o padrão IEEE 802.11, estão bastante difundidas devido a razões como facilidade de instalação e suporte a mobilidade. Mesmo assim, apesar dos padrões IEEE 802.11a, b e g serem extremamente populares e encontrados na maioria dos laptops, PDAs e outros equipamentos sem fio, ainda existem vários desafios em diversas áreas de pesquisa relacionadas que demandam novas soluções.

Um dos tópicos de interesse é a comunicação através de múltiplos saltos em redes sem fio baseada em soluções que estendam os padrões existentes. Esta área é bastante promissora, pois redes sem fio infra-estruturadas, apesar de oferecerem uma série de vantagens, podem ser expandidas se os nós forem capazes de encaminhar tráfego originado em outros nós de maneira ad-hoc e auto-configurável. Comunicação através de múltiplos saltos pode, por exemplo, estender o alcance dos pontos de acesso sem fio sem a necessidade de infra-estrutura adicional.

Roteadores sem fio de baixo custo também têm sido utilizados na instalação de backbones sem fio. Redes, onde o posicionamento de roteadores que formam um backbone sem fio é planejado para oferecer cobertura de acesso em certas áreas, ou para interconectar redes cabeadas distantes, são chamadas de redes em malha sem fio (WMNs – *Wireless Mesh Networks*). Assim sendo, por esta definição, redes em malha sem fio na verdade não são redes sem fio ad-hoc, pois são planejadas (ou projetadas), mas também podem se beneficiar das vantagens da tecnologia sem fio. Exemplos de projetos pilotos de WMNs são [Campista et al., 2008], [Bruno et al., 2005], [Akyildiz e Wang, 2005], [Akyildiz et al., 2005], [Aguayo et al., 2004] e [Couto et al., 2003].

Redes móveis ad-hoc (MANETs – *Mobile Ad Hoc Networks*) são redes auto-configuráveis compostas por nós móveis sem fio. Em uma MANET, os roteadores podem se mover e a topologia pode mudar rápida e drasticamente. Funções de roteamento são realizadas por alguns ou todos os nós sem fio. Redes em malha e redes ad-hoc sem fio utilizam comunicação em múltiplos saltos e, por isso, compartilham de um mesmo desafio: desenvolver protocolos de roteamento capazes de lidar com características de redes sem fio, tal como mobilidade, mudanças frequentes na qualidade dos enlaces sem fio e contenção no acesso ao meio. Depois de algumas décadas de pesquisa em protocolos e métricas de roteamento, existe uma tendência natural de basear novas propostas em mecanismos pré-existentes.

As soluções tradicionais para construção de redes sem fio com múltiplos saltos realizam a decisão de roteamento e o encaminhamento das informações transmitidas no nível de rede, o que tem a vantagem de ser independente da tecnologia de enlace e segue o modelo tradicional de arquitetura de rede que coloca comunicação inter-rede como responsabilidade da camada três.

Uma proposta mais recente para comunicação em múltiplos saltos em redes sem fio aborda a implementação de técnicas de encaminhamento através de múltiplos saltos no nível de enlace, como uma extensão das funcionalidades das redes locais sem fio [Camp e Knightly, 2008; Faccin et al, 2006]. Este tipo de solução pode popularizar rapidamente o uso de comunicação sem fio através de múltiplos saltos, pois as

implementações estarão disponíveis nos equipamentos dos usuários finais. Além disso, métricas que determinam a qualidade dos enlaces sem fio podem ser mais facilmente implementadas pela camada MAC, permitindo uma melhor utilização da rede sem fio.

O grupo de trabalho do IEEE 802.11s [IEEE, 2007] está desenvolvendo um padrão emergente para comunicação através de múltiplos saltos no nível dois. Esta nova proposta para a construção de redes sem fio faz com que a rede de múltiplos saltos pareça uma única rede local para o nível três. O futuro padrão IEEE 802.11s especifica funções de encaminhamento através de múltiplos saltos na camada MAC, utilizando um mecanismo de seleção de caminhos obrigatório chamado HWMP (*Hybrid Wireless Mesh Protocol*) e fornece um *framework* para seleção de caminhos que permite a utilização de mecanismos alternativos e futuras extensões. O padrão IEEE 802.11s amplia a definição do sistema de distribuição sem fio original do padrão IEEE 802.11, permitindo que a rede sem fio tenha uma área de cobertura que pode crescer à medida que novos nós se integram à rede adicionando um novo salto.

Este capítulo tem como objetivo principal apresentar o padrão emergente para redes sem fio com múltiplos saltos sendo proposto pelo IEEE 802.11s. O padrão IEEE 802.11s é inovador, pois propõe uma solução para encaminhamento através de múltiplos saltos no nível MAC, o que difere das soluções tradicionais que operam no nível de rede. A solução emergente IEEE 802.11s é comparada às soluções tradicionais de nível de rede para implementação de redes sem fio com múltiplos saltos, ressaltando suas vantagens e desvantagens. O texto também aborda projetos de pesquisa que envolvem investigações sobre redes sem fio com múltiplos saltos usando ambas as soluções discutidas. Como exemplo de solução no nível de rede, o Projeto ReMesh [Passos et al., 2006; Muchaluat-Saade et al., 2007] é brevemente apresentado e, como exemplo de solução que usa o padrão IEEE 802.11s, o projeto RUCA – Rede do Projeto Um Computador por Aluno [Carrano et al., 2007a; Carrano et al., 2007b], que avaliou a conectividade entre laptops XO, é discutido.

O restante do capítulo está estruturado como se segue. A Seção 1.2 aborda os conceitos principais do padrão IEEE 802.11 tradicional, discutindo as redes infra-estruturadas e ad-hoc e apresentando o protocolo de acesso ao meio CSMA/CA. A Seção 1.3 apresenta, de forma resumida, as soluções tradicionais para construção de redes sem fio com múltiplos saltos que realizam o encaminhamento das informações transmitidas no nível de rede. São discutidos os principais protocolos de roteamento ad-hoc, utilizados como base para o desenvolvimento de protocolos de seleção de caminhos padronizados na solução emergente 802.11s. A Seção 1.3 ainda apresenta o Projeto ReMesh como exemplo de uso de solução tradicional para redes sem fio de múltiplos saltos. A Seção 1.4 discute funcionalidades do padrão emergente 802.11s, os mecanismos de seleção de caminhos utilizados e o formato do novo quadro IEEE 802.11s, ressaltando o uso de vários endereços MAC para realizar o encaminhamento entre os nós origem e destino através de nós intermediários. A Seção 1.5 apresenta o Projeto OLPC (*One Laptop per Child*), que projetou um laptop popular de baixo custo a ser utilizado por crianças em fase escolar, como um exemplo real de implementação do último *draft* do futuro padrão. Finalmente a Seção 1.6 realiza as considerações finais.

1.2. Padrão IEEE 802.11

O padrão IEEE 802.11 é parte da família IEEE 802 que engloba padrões aplicados à construção de redes locais (LANs) e redes metropolitanas (MANs). Membros destacados desta família são, por exemplo, os padrões IEEE 802.3 (Ethernet) e IEEE 802.5 (*Token Ring*) assim como uma série de padrões mais recentes ou emergentes como o IEEE 802.15.1 (*Bluetooth*) ou IEEE 802.16 (WiMax) [Walke et al., 2006; Stallings, 2000].

O IEEE 802.11 é o padrão para montagem de redes locais sem fio (WLANs) e especifica as funções das camadas física (PHY) e de acesso ao meio (MAC – *Medium Access Control*), contendo uma série de emendas que ampliam ou aperfeiçoam suas capacidades. A Tabela 1.1 sumariza as principais emendas ao padrão existentes atualmente.

Tabela 1.1. Padrões e emendas IEEE 802.11

Padrão/emenda	Descrição
802.11-1997	Padrão original (de 1997) que descreve a camada MAC e técnica de modulação FHSS e DSSS (de 1 e 2Mbps)
802.11a	Emenda aprovada em 1999 e que introduz nova camada física (OFDM). Incorporada ao 802.11-2007.
802.11b	Emenda aprovada em 1999 e que introduz nova camada física (HR/DSS). Incorporada ao 802.11-2007.
802.11g	Emenda aprovada em 2003 e que introduz nova camada física (ERP). Incorporada ao 802.11-2007.
802.11d	Emenda aprovada em 2001 e que introduz suporte às questões regulatórias internacionais, permitindo que produtos 802.11 operem de forma compatível às diversas normas nacionais.
802.11e	Emenda aprovada em 2005 e que incorpora técnicas de qualidade de serviço (QoS) ao padrão 802.11.
802.11h	Emenda aprovada em 2004 e que adequa a emenda 802.11a às normas regulatórias da União Européia.
802.11i	Emenda aprovada em 2004 e que amplia os mecanismos de segurança das redes 802.11
802.11j	Emenda aprovada em 2004 que adequa o padrão 802.11 às normas regulatórias japonesas.
802.11-2007	Incorpora as emendas “a”, “b”, “d”, “e”, “g”, “h”, “i” e “j” ao padrão original de 1997.
802.11n (<i>draft</i>)	O Grupo de Trabalho “n” (TGn) propõe métodos para alcançar vazões superiores a 100Mbps. Muito associada ao IEEE 802.11n está a conhecida técnica de MIMO (<i>Multiple Input, Multiple Output</i>)
802.11r (<i>draft</i>)	O Grupo de Trabalho “r” (TGr) trabalha na criação de métodos de <i>handoff</i> mais rápidos, sobretudo para atender à dispositivos em rápido movimento (em veículos, por exemplo)
802.11s (<i>draft</i>)	O Grupo de Trabalho “s” (TGs) tem como objetivo ampliar o padrão para permitir a criação de redes em malha de múltiplos saltos formados por dispositivos 802.11.

Um dos objetivos principais do IEEE ao criar o padrão 802.11 foi permitir a interligação da rede sem fio com redes cabeadas que seguem o padrão Ethernet (802.3). A rede sem fio é vista como uma extensão de uma rede cabeada. Esta decisão resulta na necessidade de uma série de mecanismos apropriados para a compatibilização da parte com fio e sem fio de uma rede local. Ao mesmo tempo, com a popularização das redes sem fio, e seu uso cada vez mais intenso, a padronização segue na direção de propostas que aumentem a banda disponível (como as emendas b, a e g, e recentemente o *draft n*), tornem a rede mais segura (802.11i), auxiliem a mobilidade (*draft r*) e ofereçam qualidade de serviço (802.11e).

1.2.1. Padrões de Nível Físico IEEE 802.11

Redes 802.11 utilizam duas faixas do espectro de uso não licenciado na maior parte do mundo, inclusive no Brasil. Essas faixas são chamadas ISM (*Industrial, Scientific and Medical*) e como o nome indica são reservadas para uso industrial, médico e científico e podem ser usadas por qualquer dispositivo contanto que a potência transmitida não ultrapasse certos valores legais.

A primeira é a chamada banda S-ISM que abrange as frequências entre 2,4 e 2,5 GHz. Esta é a faixa utilizada pelas implementações 802.11b e 802.11g. Trata-se de uma porção do espectro com diversos dispositivos emissores, como fornos de microondas e alguns modelos de telefones sem fio (muitos utilizam a faixa de 400MHz). É também usada por dispositivos IEEE 802.15.1 (*Bluetooth*).

Os 83 MHz disponíveis na banda foram divididos em onze canais de 22 MHz. Apesar de existirem onze canais, só três canais independentes estão disponíveis, porque o espaçamento entre canais adjacentes é de 5MHz. Isto significa que o canal 3, por exemplo, interfere com os canais 1, 2, 4, 5, 6 e 7. Em instalações normais, para o melhor (re)uso da banda, é recomendada a utilização apenas dos canais 1, 6 e 11, por não interferirem entre si. No entanto, em casos especiais como por exemplo a existência de uma fonte de ruído que torne o uso dos canais recomendados inviável, os outros canais podem ser usados. Existe pesquisa também no uso proposital de canais sobrepostos, pois sob condições especiais é possível a comunicação mesmo quando as estações estão sintonizadas para frequências centrais diferentes [Rad e Wong, 2007]. A Figura 1.1 ilustra a tela de um analisador de espectro (software Chanalyzer), exibindo as faixas de frequência de três canais que não interferem entre si. Pode-se observar que a maior parte do tráfego está no canal 1.

Por conta de seu uso não licenciado e da extrema popularidade dos dispositivos que nela operam, a faixa do espectro de 2,4 GHz já se encontra extremamente disputada nas principais áreas urbanas do mundo. As características de propagação e o baixo poder de penetração destas frequências implicam na necessidade de visada direta para distâncias maiores do que algumas dezenas de metros, considerando as potências legalmente aceitáveis.

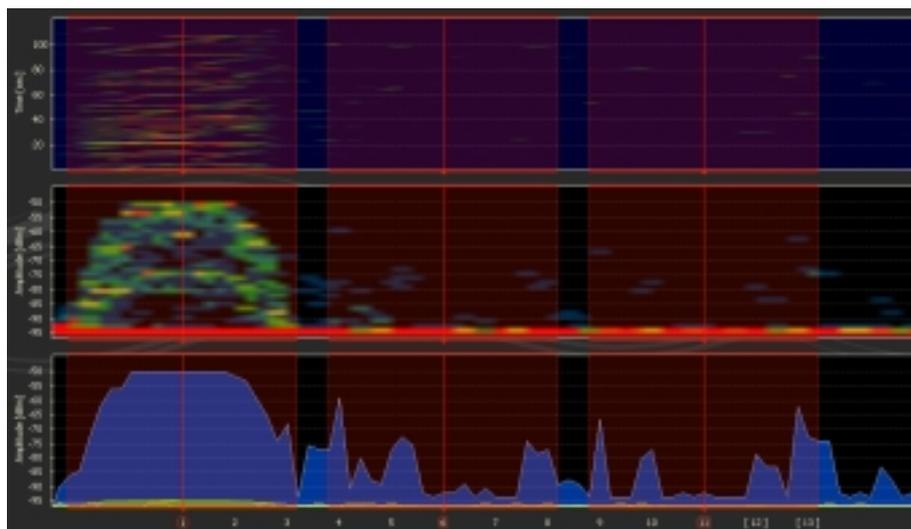


Figura 1.1. Tela do software Chanalyzer

A segunda faixa do espectro utilizada por dispositivos 802.11, no caso os que seguem a emenda “a”, é chamada banda C-ISM e abrange as frequências entre 5,725 e 5,875 GHz. Os dispositivos 802.11a não alcançaram a mesma popularidade dos dispositivos 802.11b ou 802.11g e também por isso sua operação está menos sujeita a interferência, apesar de a necessidade de visada ser ainda maior nestas frequências.

A versão original do padrão IEEE 802.11 incorporava duas taxas de codificação (1 e 2 Mbps) e foi projetada para operar na banda ISM de 2.4GHz. A camada física do padrão foi emendada pela primeira vez em 1999, com o lançamento do IEEE 802.11a, que introduzia taxas de até 54Mbps, no entanto, operando na faixa de 5GHz. Mais tarde, as emendas 802.11b (ainda em 1999) e 802.11g (em 2003), introduziram taxas de 5,5 e 11Mbps (emenda “b”) e taxas superiores, até 54Mbps (emenda “g”).

O padrão IEEE 802.11 original incorpora duas descrições de camada física, ambas provendo taxas de transmissão de 1 e 2 Mbps. A primeira chamada FHSS (*Frequency-Hopping Spread Spectrum*) foi a primeira técnica de espalhamento de espectro amplamente utilizada, e apesar de variantes da técnica estarem ainda em uso (em dispositivos Bluetooth, por exemplo), em relação ao IEEE 802.11 ela é hoje considerada obsoleta.

A segunda camada física proposta no padrão original é baseada na técnica de DSSS (*Direct Sequence Spread-Spectrum*) a acabou tendo maior sobrevida do que a técnica de FHSS por ser percebida como capaz de alcançar taxas maiores que esta em implementações futuras, o que de fato veio a acontecer.

Logo nos anos seguintes à edição do padrão IEEE 802.11 original, novas propostas de camadas físicas permitiram aumentar o desempenho das redes sem fio, através de taxas de transmissão maiores.

A técnica de modulação DSSS, em detrimento da FHSS, foi empregada para alcançar a taxa de 5,5 Mbps e uma variante sua chamada HR/DSSS (*High Rate Direct Spread Spectrum*) foi empregada para alcançar taxas de 11Mbps. Estas novas taxas compõem a proposta de camada física descrita na emenda “b”.

A emenda IEEE 802.11g surgiu em 2003 e passou a ser incorporada por dispositivos comerciais a partir de 2005. Sua grande vantagem foi elevar às taxas de transmissão até o patamar de 54Mbps utilizando codificação OFDM.

A rigor, o IEEE 802.11g oferece um conjunto de especificações de camada física agrupadas sobre o que se convencionou chamar ERP (*Extended-Rate PHY*). Estas se encontram sumarizadas na Tabela 1.2.

Tabela 1.2. ERP (*Extended-Rate PHY*)

Subcategorias do ERP	Descrição
ERP-DSSS e ERP-CCK	São duas técnicas de modulação retro compatíveis com as propostas no padrão 802.11 original e na emenda 802.11b. São empregadas quando o dispositivo opera nas taxas de 1, 2, 5,5 e 11 Mbps.
ERP-OFDM	É a técnica de modulação utilizada pela emenda 802.11a, mas operando na faixa de 2,4 GHz. É empregada pelo dispositivo para operar nas taxas de 6, 9, 12, 18, 24, 36, 48 e 54Mbps.
ERP-PBCC	Método opcional e não comumente implementado pelos dispositivos atualmente fabricados. Implementa taxas de 22 e 33 Mbps.
DSSS-OFDM	Método opcional e poucas vezes implementado cujo objetivo é também a retro compatibilidade. Trata-se de um esquema híbrido que utiliza DSSS para transmissão do cabeçalho e OFDM para o corpo do quadro (o que permite que estações 802.11b leiam o cabeçalho)

A Figura 1.2 apresenta todas as especificações de camada física atualmente descritas no padrão.

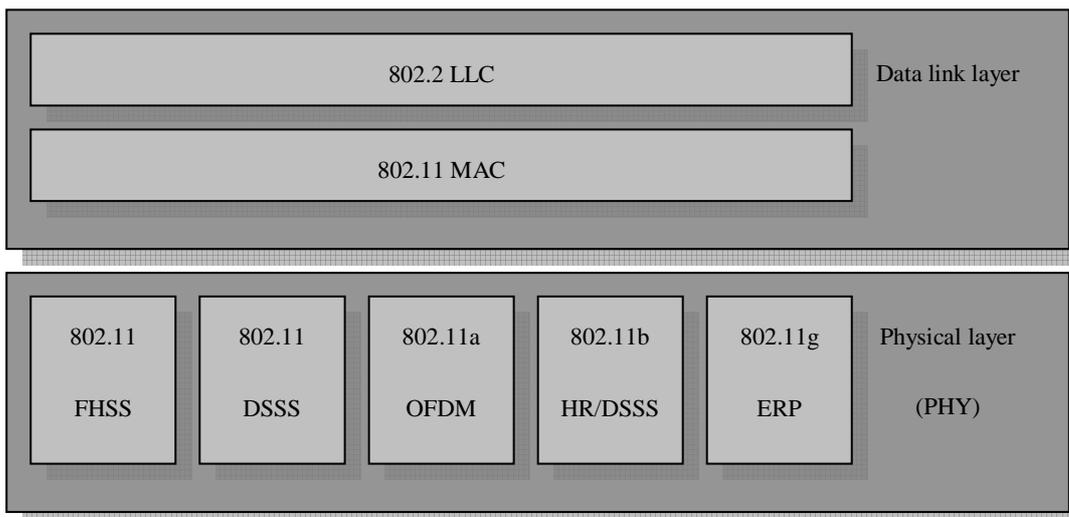


Figura 1.2. Padrões de nível físico IEEE 802.11

A possibilidade de estações operando com codificações diversas co-existirem na mesma rede aumenta a complexidade dos projetos práticos de redes sem fio. A

necessidade de todas as estações, seja qual for sua taxa de associação (isto é, a codificação sendo usada para comunicação entre dois pares), reconhecerem as informações de controle obriga o uso da codificação base nos dados de controle, como já foi citado acima. O resultado é que a taxa nominal é muito maior do que a efetivamente disponível como banda útil para dados, e os cálculos para disponibilidade de banda, conforme aumenta o número de estações são complexos, visto ser impossível definir, a priori, qual será a taxa de associação das estações.

Os pontos de acesso possuem mecanismos que permitem estabelecer uma taxa de associação mínima. Estes mecanismos são úteis porque não permitem que estações que estejam afastadas se associem a um ponto de acesso usando uma taxa baixa, que diminui a disponibilidade de banda para todas as estações associadas àquele ponto de acesso. A restrição do raio de associação (como efeito colateral de se usar apenas codificações mais complexas) também permite uma maior densidade de pontos de acesso. No entanto, isto pode gerar zonas de sombra e causar conexões intermitentes, já que flutuações do nível de sinal são norma para redes sem fio.

1.2.2. Controle de acesso ao meio

Apesar dos objetivos comuns, o controle de acesso ao meio descrito no padrão IEEE 802.11 difere do descrito na respectiva camada MAC do padrão IEEE 802.3 (Ethernet) justamente por conta das características do meio de propagação sem fio. A transmissão de rádio, em espaço livre, representa desafios que uma rede cabeada desconhece.

O mecanismo de acesso ao meio obrigatório para toda estação IEEE 802.11 é definido pela função de coordenação distribuída (DCF – *Distributed Coordination Function*) e é baseado no protocolo CSMA-CA (*Carrier Sense Multiple Access with Collision Avoidance*), que contrasta com o mecanismo de detecção de colisão CSMA-CD (*Carrier Sense Multiple Access with Collision Detection*) preconizado pelo padrão de redes Ethernet.

Transmissores de rádio não são capazes de escutar o meio ao mesmo tempo que transmitem, o que dificulta uma proposta de detecção de colisão (seria necessária uma segunda interface de rádio). Além disso, os custos de uma colisão em redes sem fio são altos se comparados aos mesmos custos em uma rede cabeada, onde as taxas de transmissão são usualmente maiores. Até porque a perda de quadros por corrupção na transmissão é um evento raro em redes cabeadas e relativamente comum nem redes sem fio.

Verificar a disponibilidade do meio de forma a evitar colisões é, por isso, o objetivo do MAC do 802.11. Um objetivo que não pode ser alcançado simplesmente através da escuta do meio. O fato de, em um determinado momento, uma estação não detectar em seu receptor a presença de outra transmissão não garante que ela poderá transmitir sem qualquer risco de colisão. Esta dificuldade inerente ao rádio pode ser ilustrada, por exemplo, pelo notório problema da estação escondida.

No cenário ilustrado na Figura 1.3, uma determinada estação A deseja transmitir para a estação C, mas ignora a existência concorrente de uma transmissão de B para C, pois B está muito distante de A. Se A transmitir neste ínterim causará a colisão e conseqüente perda de seu próprio quadro e do quadro originado em B.



Figura 1.3. Problema da estação escondida

Em resposta ao problema da estação escondida, o padrão IEEE 802.11 incorporou um mecanismo chamado de RTS/CTS. Segundo este esquema, quando um nó possui dados a transmitir, ele deve antes enviar um quadro RTS (*Request To Send*) com o objetivo de reservar o meio.

O quadro RTS inclui uma estimativa do tempo total necessário para a transmissão e confirmação de recebimento pelo destinatário (ACK). Assim, os nós que o recebem sabem por quanto tempo o meio ficará ocupado. O destinatário da transmissão deverá responder com um quadro CTS (*Clear To Send*) que também incorpora o tempo de reserva do meio. O ganho, neste caso, seria que os nós escondidos, apesar de não serem capazes de escutar o RTS receberiam o CTS e, uma vez que respeitem a reserva de tempo solicitada, a colisão será evitada.

O envio de quadros de controle RTS e CTS é opcional de acordo com o padrão e, tipicamente, só é aplicado na transmissões de quadros com tamanho maior que um determinado limiar (configurável pela implementação). A Figura 1.4 exibe um exemplo de transmissão de quadros entre duas estações em uma rede IEEE 802.11 usando RTS/CTS. Outras estações que desejam transmitir atualizam seus NAVs (*Network Allocation Vector*) com o tempo estimado da transmissão em andamento, indicando quando elas podem tentar o acesso ao meio oportunamente. O padrão indica diferentes intervalos de silêncio entre quadros, como DIFS (*DCF Interframe Space*) e SIFS (*Short Interframe Space*) por exemplo, dependendo do tipo de quadro que será transmitido [Walke et al., 2006].

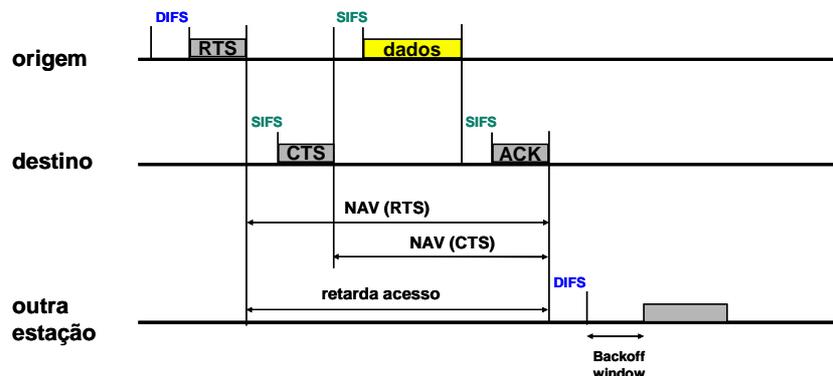


Figura 1.4. Transmissão usando RTS/CTS

O uso de RTS e CTS não é sempre benéfico por causa da possibilidade da existência de estações usando diferentes taxas de codificação. Para que todas as estações possam decodificar as mensagens de controle, estas têm que ser transmitidas na taxa

básica. Assim, os quadros RTS e CTS, apesar de conterem poucos dados, acabam ocupando o meio por um tempo desproporcional à informação carregada, principalmente se as estações estiverem utilizando taxas de codificação mais altas. A transmissão de RTS/CTS é vantajosa para envio de quadros cujo tempo de transmissão for maior que o tempo de troca de quadros RTS/CTS, caso contrário, não há ganho em usá-la.

1.2.3. Formato dos quadros 802.11

Na Figura 1.5 podemos ver o formato de um quadro IEEE 802.11. Uma das características mais importantes é a presença de quadro endereços MAC (ADDR1-4). Conforme mencionado acima, a rede sem fio foi projetada para ser uma extensão da Ethernet cabeada. Numa rede Ethernet, só são necessários dois endereços de 48 bits para enviar um pacote da origem para o destino. Numa rede sem fio, no entanto, um pacote indo para um destino pode ter que passar por intermediários (como pontos de acesso). Estes intermediários são o destino imediato do pacote, mas não seu destino final. Assim, é necessário identificá-los, bem como identificar o destino final para que o pacote chegue ao mesmo.

bytes:

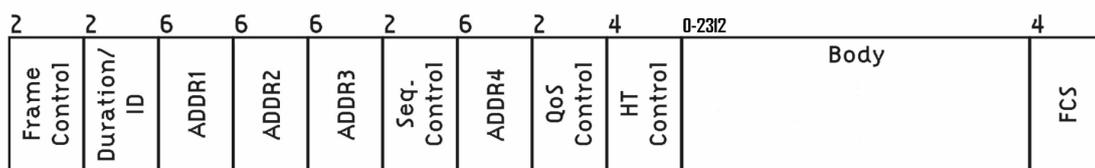


Figura 1.5. Estrutura geral de um quadro IEEE 802.11

Os endereços são numerados em vez de terem um nome porque sua função varia de acordo com tipo do quadro. Geralmente, o endereço 1 (ADDR1) é o destino imediato do pacote (isto é, identifica o receptor), o endereço 2 (ADDR2) identifica o transmissor e o endereço 3 é usado para filtragem no receptor.

Seguindo a convenção dos endereços MAC IEEE 802, se o primeiro bit de um endereço é zero, este é um endereço unicast. Se o bit for um, o endereço é multicast. Se todos os bits do endereço forem iguais a um, é um quadro de broadcast. Cada endereço pode ter uma das seguintes funções:

- Endereço de destino: destino final do quadro;
- Endereço de origem;
- Endereço do receptor: qual estação deve processar o quadro;
- Endereço do transmissor: qual estação enviou aquele quadro;
- Identificação do *Basic Service Set* (BSSID): como várias redes locais podem compartilhar a mesma área, este endereço permite identificar em que rede sem fio o quadro é transmitido.

A maior parte dos quadros usa 3 endereços (1-destino, 2-origem, 3-rede/BSSID). Casos onde quatros endereços são usados serão abordados na seção 1.4.4.

1.2.4. Tipos de Redes 802.11

O padrão IEEE 802.11 descreve dois tipos de redes sem fio em função da existência ou não de um nó especializado, chamado ponto de acesso (AP – *Access Point*). O primeiro tipo, a rede infra-estruturada, é aquele em que os nós se comunicam entre si por intermédio de um ponto de acesso que funciona como ponte, permitindo que as estações possam alcançar outras redes, cabeadas ou sem fio. A Figura 1.6 ilustra uma rede local sem fio infra-estrutura com APs interligados através de um sistema de distribuição cabeado. O conjunto de estações interligadas por um mesmo AP é chamado de BSS (*Basic Service Set*) e o conjunto de todas estações interligadas através de APs distintos que fazem parte de uma mesma rede no nível de enlace, graças a presença de um sistema de distribuição, é chamado ESS (*Extended Service Set*).

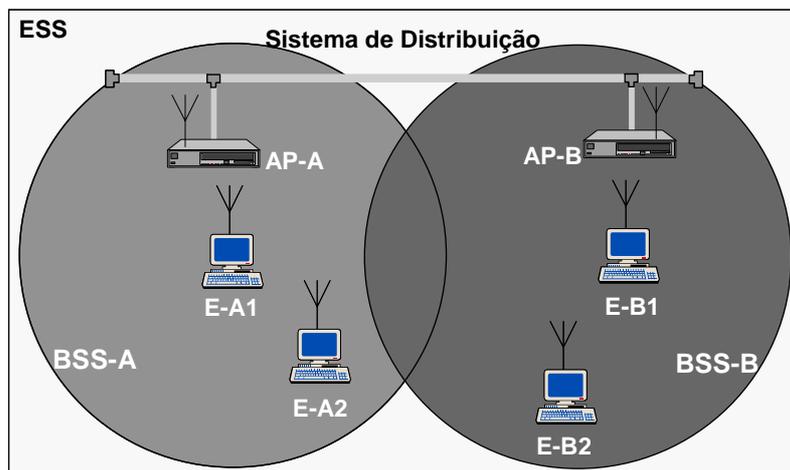


Figura 1.6. Rede local sem fio infra-estruturada

Para escolher o ponto de acesso, a estação segue quatro passos, repetidos após sintonizar cada canal de frequência:

- o nó envia um quadro de pergunta *Probe*;
- todos os pontos de acesso que escutam respondem com *Probe Response*;
- o nó escolhe um dos pontos de acesso, e envia para ele um quadro de associação *Association Request*;
- o ponto de acesso responde com um *Association Response*.

Uma estação escolhe um ponto de acesso cada vez que entra na rede e cada vez que o ponto de acesso não é considerado satisfatório. Quando um nó troca de um ponto de acesso para outro pertencendo a um mesmo ESS, o novo ponto de acesso avisa o antigo da troca.

Como o envio de *Probes* é custoso, foi criada uma nova forma de associação, chamada passiva. Os pontos de acesso enviam periodicamente um quadro de *Beacon*,

que avisa das capacidades daquele ponto de acesso. Para trocar de ponto de acesso, o nó pode, então, enviar um *Association Request* para o novo ponto.

Um segundo tipo de rede sem fio, formado apenas por estações, ou seja, sem pontos de acesso, consiste de uma coleção desestruturada de conexões ponto a ponto. Neste modo, chamado de ad-hoc, não está previsto a comunicação em múltiplos saltos entre os participantes. Trata-se, portanto, de uma rede local sem saltos intermediários. A Figura 1.7 ilustra uma rede sem fio ad-hoc.

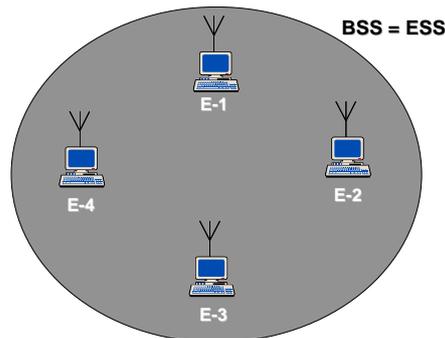


Figura 1.7. Rede sem fio ad-hoc

Partindo das redes ad-hoc sem fio, começaram a surgir várias propostas e soluções para oferecer comunicação em múltiplos saltos através de roteadores sem fio funcionando no modo ad-hoc, seguindo a abordagem tradicional de deixar as funções de roteamento e encaminhamento em múltiplos saltos para o nível de rede, como nas redes cabeadas. A Figura 1.8 ilustra uma rede sem fio com múltiplos saltos que segue a abordagem tradicional do nível de rede. É justamente o objetivo da emenda “s” a criação de uma rede ad-hoc onde operam protocolos de seleção de caminhos e encaminhamento de quadros através de múltiplos saltos na própria camada MAC 802.11. As próximas seções apresentam ambas as abordagens para comunicação em múltiplos saltos.

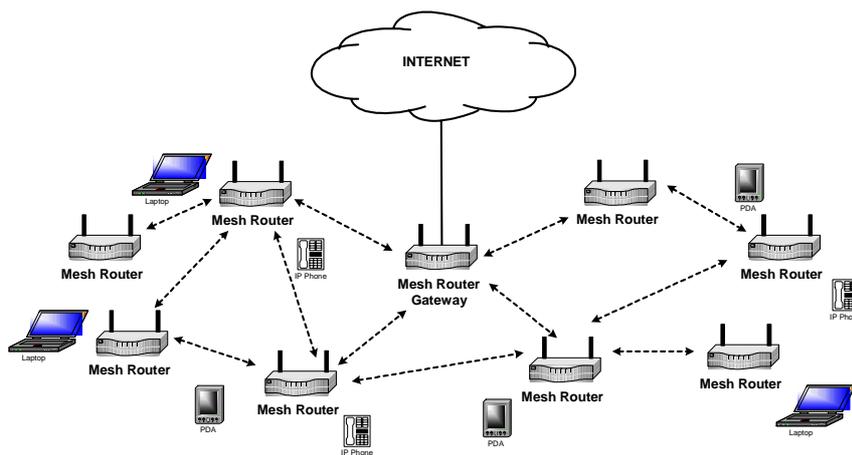


Figura 1.8. Rede sem fio com múltiplos saltos

1.3. Soluções Tradicionais para Redes sem Fio com Múltiplos Saltos no Nível de Rede

As soluções tradicionais para redes sem fio com múltiplos saltos utilizam as funções de roteamento do nível de rede para encaminhar pacotes através de roteadores sem fio intermediários até o destino correspondente.

Os algoritmos de roteamento tradicionais, desenvolvidos para redes cabeadas, trabalham em um cenário onde os nós são fixos, com enlaces simétricos, estáveis e com alta banda disponível. Em uma rede sem fio com múltiplos saltos os nós podem ser móveis, há uma variação das condições do meio de transmissão, assimetria dos enlaces, baixa taxa de transmissão e, em alguns casos, limitação de energia dos nós. Essas condições tornam a rede muito mais dinâmica e impossibilitam o uso eficiente dos protocolos de roteamento tradicionais. Nas soluções tradicionais para redes sem fio com múltiplos saltos, normalmente são utilizados protocolos de roteamento para redes móveis ad-hoc [Murthy e Manoj, 2004; Cordeiro e Agrawal, 2002].

As rápidas e freqüentes mudanças na topologia das redes sem fio com múltiplos saltos exigem uma atualização das tabelas de roteamento com a mesma agilidade. Isto resultaria num aumento do overhead que exigiria banda e energia, recursos escassos neste tipo de rede. A dificuldade é agravada quando os nós acumulam as funções de clientes e roteadores, o que é o caso de redes ad-hoc de múltiplos saltos usando laptops. Neste cenário, é inconveniente que o processo de trocas de mensagens de roteamento roube muito do poder de processamento dos laptops. Então, um protocolo ideal para esse tipo de rede também deve exigir pouco processamento.

Não é adequado escolher um único protocolo ideal para redes sem fio com múltiplos saltos, já que como observado anteriormente, os nós podem possuir características diferentes, assim como a topologia da rede. Nas redes em malha, por exemplo, como será mostrado na subseção 1.3.3 com a apresentação do projeto ReMesh, os nós são fixos, possuem alimentação constante e seu processamento é restrito a função de roteador.

Quanto à construção de rotas, os protocolos de roteamento unicast para redes ad-hoc podem ser classificados como pró-ativos ou reativos (sob demanda). Há também protocolos híbridos que reúnem características das duas classes.

Nos protocolos pró-ativos, cada nó mantém em sua tabela de roteamento informações atualizadas sobre a topologia completa da rede adquirida através de trocas periódicas de mensagens de roteamento. Estas informações são muitas vezes difundidas por toda a rede através de inundação (*flooding*). Quando um nó precisa de um caminho até um destino, ele já possui localmente uma base de dados que com o uso de algum algoritmo, como o de Dijkstra [Tanenbaum, 2003], possibilita que a escolha do melhor caminho seja feita localmente e imediatamente pelo próprio nó.

Os protocolos reativos não trocam mensagens periodicamente para manter a tabela de roteamento atualizada. Em lugar disto, o caminho para determinado destino só é descoberto quando houver necessidade de transmissão de dados para o nó correspondente.

Os mecanismos pró-ativos se adaptam melhor às redes com menor número de nós e disponibilidade de banda, já que o overhead de controle do protocolo para manutenção das tabelas de rotas é alto. Já os protocolos reativos possuem menor overhead, por outro lado exigem procedimentos custosos para descoberta de rotas através do envio de mensagens por difusão e procedimentos específicos para manutenção de rotas. Os protocolos de roteamento híbridos tentam aproveitar as vantagens e minimizar as desvantagens de cada um dos dois grupos.

1.3.1. Protocolos de Roteamento Ad-hoc

Esta seção aborda o funcionamento de protocolos de roteamento ad-hoc que serviram de base para a elaboração dos protocolos de seleção de caminho usados nas primeiras versões do IEEE 802.11s: o AODV (*Ad hoc On-demand Distance Vector*) [Perkins et al., 2003], representante da classe dos reativos ou sob demanda e o OLSR (*Optimized Link State Routing*) [Clausen e Jacquet, 2003], protocolo pró-ativo.

1.3.1.1. AODV

O AODV (*Ad hoc On-demand Distance Vector*) [Perkins et al., 2003] é um protocolo com alta escalabilidade, funcionando bem tanto para redes pequenas como para redes com milhares de nós móveis. Como a descoberta de rota é feita sob demanda, só quando a rota for realmente necessária, isto permite que caminhos sejam descobertos em redes muito maiores sem que haja uma troca periódica de informações de roteamento, característica dos protocolos pró-ativos. Esta estratégia também evita o desperdício de banda, energia e minimiza o uso de memória e processamento nos nós.

Ao contrário dos protocolos pró-ativos que mantêm informações sobre rotas disponíveis na rede em cada nó, os protocolos reativos, como o AODV, necessitam, para cada envio de pacote a determinado destino, iniciar um procedimento de descoberta de rota. Este processo provoca uma latência maior até o início da transmissão dos dados. Depois de descoberta, a rota é marcada como ativa e fica armazenada na tabela de roteamento da fonte e de todos os nós do percurso que participaram do procedimento de descoberta da rota durante um tempo. Enquanto ativa, os nós que participaram desse processo podem utilizar a rota para encaminhar pacotes. Depois de expirado o tempo, ou se for observada alguma quebra de enlace, uma nova descoberta de rota é necessária.

O AODV pode detectar a quebra de algum enlace de duas maneiras distintas. O primeiro modo é com o uso de mensagens enviadas periodicamente chamadas de *hello*. Estas mensagens são enviadas em broadcast por um nó, mas com TTL configurado para 1, e servem para anunciar ou reiterar a sua presença aos nós vizinhos. Quando os vizinhos notam que o envio do *hello* foi cessado, isto é um indicativo de que o nó não está mais ali ou está impossibilitado de se comunicar, o que indica que o enlace está quebrado. A segunda maneira de se detectar a quebra de um enlace é através das informações provenientes da camada de enlace, o que proporciona economia de banda, energia e processamento. Assim que um nó detecta a quebra de um enlace, essa informação deve ser difundida para todos os nós que se utilizam dele para encaminhamento de alguma rota.

Os nós no AODV usam, em seus pacotes de roteamento, e armazenam em suas tabelas números de seqüência que servem para verificar o quão recente é a informação e

assim evitar *loops* de roteamento, prevenindo-se assim de um problema característico dos protocolos de vetor de distância, a contagem para infinito [Tanenbaum, 2003].

Descoberta de Rotas

Para a descoberta de rotas, os nós do AODV utilizam dois pacotes, um de requisição de rota, o RREQ (*Route Request*) e outro de resposta à requisição da rota, o RREP (*Route Reply*).

Quando um nó fonte deseja transmitir dados para um destino, ele realiza uma inundação na rede com mensagens RREQ com informações que denunciam a intenção da fonte em estabelecer uma rota para determinado destino. Os pacotes RREQ possuem o formato mostrado na Figura 1.9.

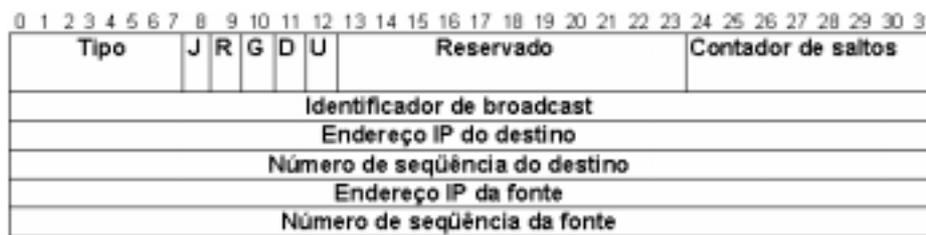


Figura 1.9. O formato da mensagem RREQ

O campo Tipo indica que o pacote é um RREQ. Os campos J (*Join*) e R (*Repair*) são reservados para comunicação multicast. O G indica se um gratuitous RREP deve ser enviado ao destino por um nó intermediário. O D (*Destination Only*), quando ativado, determina que a resposta a esta requisição só pode ser dada pelo destino. O campo contador de saltos contém o número de saltos desde a fonte até o nó em que o RREQ está sendo processado.

O identificador de broadcast é um número seqüencial que identifica o pedido de requisição de rota. Como a requisição é feita em broadcast, a mesma requisição pode chegar por caminhos diferentes aos nós intermediários. Este identificador serve então para que estes nós, ao analisar o RREQ juntamente com o endereço da fonte, saibam se esta requisição já foi atendida. Os 32 bits seguintes correspondem ao endereço IP do destino para o qual se deseja construir uma rota. O campo Número de seqüência do destino registra o último número de seqüência que a fonte recebeu relativo a alguma rota para o destino desejado. O RREQ ainda contém o endereço do nó que originou a requisição e seu respectivo número de seqüência.

Quando um nó recebe um RREQ, se ele não for o destino requerido, ele checa na sua tabela de roteamento se há alguma rota válida para o destino. Se não houver, ele então repassa para os seus vizinhos, e este processo se repete até atingir o destino ou algum nó que conheça a rota até ele. A cada retransmissão, o campo contador de saltos é incrementado e os nós registram em uma entrada de suas tabelas de roteamento o endereço do vizinho de quem recebeu o primeiro RREQ e seu respectivo número de seqüência, além do seu tempo de expiração. Durante este procedimento, os nós intermediários aprendem o caminho reverso até a fonte e podem utilizar esta rota para transmitir dados. O aprendizado da rota reversa possibilita também que a resposta de requisição de rota possa ser transmitida em unicast diretamente para a fonte.

Se algum nó intermediário tiver em sua tabela de roteamento alguma rota ativa para o destino com o número de seqüência maior ou igual ao último recebido pela fonte, e se o RREQ não possuir o bit D ativado, ele poderá responder a requisição. Tanto para este caso como quando o destino responde a requisição, um pacote RREP é enviado para o nó fonte com o número de seqüência atualizado para um valor maior que o valor atual contido no RREQ.

A cada nó percorrido pelo RREP as tabelas de roteamento são preenchidas ou atualizadas com a informação do endereço do próximo salto para chegar ao destino, isto é, o endereço do nó de quem recebeu o RREP e o novo número de seqüência do destino. O pacote RREP possui o formato mostrado na Figura 1.10.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Tipo								R	A	Reservado								Tamanho do Prefixo				Contador de saltos									
Endereço IP do destino																															
Número de seqüência do destino																															
Endereço IP da fonte																															
Tempo de vida																															

Figura 1.10. O formato da mensagem RREP

O campo Tipo diz que esta mensagem é um RREP. O bit R (*Repair*) é apenas usado para comunicação multicast. O bit A (*Acknowledgement required*) é utilizado quando se deseja que a fonte confirme o recebimento da resposta RREP. O campo de Tamanho do Prefixo especifica que o próximo salto indicado pode ser usado por qualquer nó com o mesmo prefixo de endereço de roteamento (definido pelo tamanho do prefixo) que o do destino requisitado. O Contador de saltos indica quantos saltos há do destino até a fonte que fez a requisição da rota.

Os próximos campos informam o IP do destino, que neste caso representa o nó que fez a requisição da rota. Há a informação também do número de seqüência do destino, do endereço IP da fonte e tempo de vida da rota.

Se um nó encaminha uma resposta por um enlace que tenha uma probabilidade de erro alta ou que seja unidirecional, ele pode ativar o bit A. Isto força o nó que fez a requisição da rota a confirmar o recebimento do RREP.

Se uma rota não for utilizada por um determinado período, seu tempo de vida expira e ela é eliminada da tabela de rotas.

Manutenção de Rotas

Quando um nó detecta uma quebra de enlace, ou através da análise das informações da camada de enlace, ou pelo cessar do envio de mensagens *hello* por parte de algum vizinho, ele deverá avisar a todos os nós que se utilizam desta rota sobre a indisponibilidade da mesma. Como cada nó mantém em sua tabela de roteamento uma lista de todos os nós predecessores de cada rota, quando detectada a quebra de algum enlace, o nó detector sabe os nós que utilizam este enlace no encaminhamento de seus dados e são eles que devem ser notificados.

Para notificar a invalidez de uma rota, os nós utilizam uma mensagem de erro chamada de RERR (*Route Error*). O formato da mensagem RERR é mostrado na Figura 1.11.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Tipo								N	Reservado												DestCount (1...i)										
Endereço IP do destino inalcançável (1)																															
Número de seqüência do destino inalcançável (1)																															
.																															
.																															
Endereço IP do destino inalcançável (i)																															
Número de seqüência do destino inalcançável (i)																															

Figura 1.11. O formato da mensagem RERR

O campo Tipo indica que a mensagem é uma RERR. O bit N (*No Delete*) indica quando o nó está reparando algum enlace em que houve problema e que as entradas que utilizam este enlace não devem ser apagadas. O campo *DestCount* diz quantos destinos estão inalcançáveis. Os campos seguintes listam os endereços de IP dos destinos inalcançáveis e os respectivos números de seqüência das rotas que levam até eles.

Esta mensagem é geralmente enviada em broadcast, porém se apenas um nó for atingido pela quebra de algum enlace, o nó que detectou pode enviar o RERR em unicast para o nó prejudicado.

Assim que os nós receberem o RERR, a rota para o destino dito como inalcançável é apagada da tabela de roteamento e um novo processo de descobrimento de rota é iniciado.

1.3.1.2 OLSR

O OLSR (*Optimized Link State Routing*) [Clausen e Jacquet, 2003], como o nome sugere, é uma otimização dos clássicos protocolos de roteamento de estado de enlace projetada para redes ad-hoc. Através da escolha de nós para exercerem funções especiais, os MPRs (*Multipoint Relays*), ele utiliza uma técnica que diminui substancialmente o overhead causado pelas trocas de mensagens de roteamento característico de protocolos pró-ativos. Ao mesmo tempo o OLSR se beneficia da rápida atualização das informações topológicas da rede, muito importante em redes dinâmicas como as ad-hoc, e da pouca latência no estabelecimento de rotas.

Cada nó da rede, chamado de nó seletor, deve selecionar um conjunto de nós para atuarem como MPR. Quando o nó seletor pretende disseminar uma informação pela rede (broadcast), apenas os nós MPR irão repassar os pacotes. A diminuição do overhead se dá por conta do menor número de retransmissões. O processo de seleção de nós MPR deve se preocupar em escolher um conjunto de MPRs que possam cobrir todos os seus vizinhos de 2 saltos, com isto ele assegura que nenhum nó irá deixar de receber os pacotes (veja a Figura 1.12, retirada de [Zhang et al., 2007]).

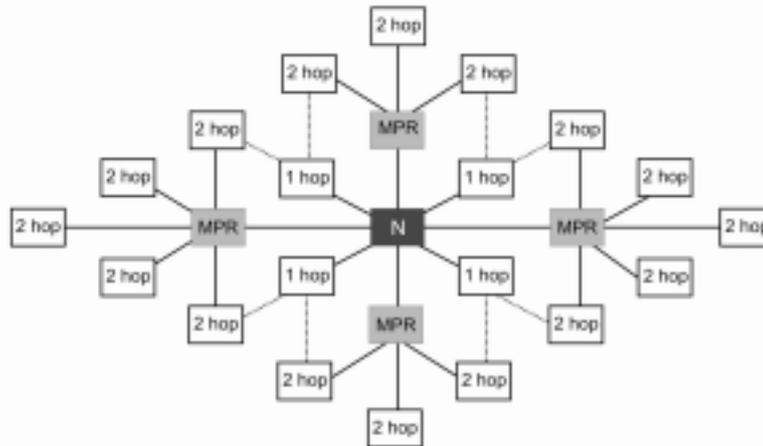


Figura 1.12. Exemplo de escolha de MPRs

Como em todos os protocolos pró-ativos, os nós OLSR trocam mensagens periódicas com os outros nós da rede. Estas informações abastecem bancos de dados armazenados localmente em cada nó chamado de repositórios e estes guardam informações sobre os vizinhos de um e dois saltos e os respectivos enlaces com eles, nós MPRs, nós seletores e informações sobre a topologia da rede inteira. Dois tipos de pacote são usados para disseminar estas informações: *hello* e TC (*Topology Control*). Há também os pacotes MID (*Multiple Interfaces Declaration*), que servem para correlacionar os endereços das múltiplas interfaces de um nó com o seu endereço principal [Clausen e Jacquet, 2003].

O OLSR usa um formato de pacote único para transportar todos os tipos de mensagens, ilustrado na Figura 1.13. Por outro lado, cada mensagem possui seu formato próprio, como será mostrado nas seções seguintes. A utilização de um formato de pacote único facilita a criação de extensões para o protocolo sem causar problemas de compatibilidade. Isto possibilita também o envio de diferentes tipos de mensagem em uma transmissão única. E por último, é vantajoso utilizar o tamanho máximo de pacote permitido pela rede para otimizar a utilização do canal.

Tamanho do pacote		Número de Seqüência do pacote	
Tipo	Vtime	Tamanho da mensagem	
Endereço de Origem			
TTL	Cortador de saltos	Número de Seqüência da mensagem	
Mensagem			
Tipo	Vtime	Tamanho da mensagem	
Endereço de Origem			
TTL	Cortador de saltos	Número de Seqüência da mensagem	
Mensagem			

Figura 1.13. Formato do Pacote OLSR

Dentro do cabeçalho do pacote há a informação do tamanho do pacote (em bytes) e o número de seqüência do mesmo, que é incrementado sempre que um novo pacote é transmitido. Este número serve para identificar o quão recente é o pacote e evita que haja a retransmissão de um mesmo pacote mais de uma vez.

Logo a seguir há os campos de cabeçalho da mensagem. O campo Tipo indica que tipo de mensagem está sendo anexada (*hello* ou TC). O *Vtime* indica por quanto tempo a informação contida nesta mensagem deve ser considerada como válida nos repositórios. O próximo campo diz o tamanho desta mensagem. O Endereço de Origem representa o endereço do nó que criou a mensagem. O TTL (*Time To Live*) indica o número de saltos que a mensagem pode dar até ser descartada. O contador de saltos é incrementado a cada retransmissão. O número de seqüência da mensagem serve para o nó receptor verificar se a mensagem é atualizada. O campo mensagem aloca a mensagem de *hello* ou TC.

Outros tipos de mensagens podem ser usados nas extensões propostas para o OLSR. Algumas das extensões possibilitam modo de conservação de energia (*sleep mode*), roteamento multicast, suporte para enlaces unidirecionais, métricas especiais de roteamento, entre outras.

Mensagem *hello*

As mensagens *hello* são usadas para disseminar informações locais sobre a condição dos enlaces, presença de vizinhos e sinalização para os MPRs. Como elas são enviadas periodicamente aos vizinhos de um salto (TTL igual a 1), não é necessário nenhum mecanismo de retransmissão da mensagem. As mensagens de *hello* não são retransmitidas.

As informações oriundas do *hello* irão povoar os repositórios correspondentes aos enlaces ativos do nó, vizinhos de um ou dois saltos, MPRs e seletores. Através das informações armazenadas nestes repositórios os nós são capazes de selecionar e gerenciar corretamente seu conjunto de nós MPRs. O formato da mensagem *hello* é mostrado na Figura 1.14.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Reservado										Htime										Willingness											
Link Code					Reservado					Tamanho da mensagem de link																					
Endereço do vizinho																															
Endereço do vizinho																															
Link Code					Reservado					Tamanho da mensagem de link																					
Endereço do vizinho																															
Endereço do vizinho																															

Figura 1.14. Formato da mensagem *hello*

O campo *Htime* especifica o intervalo de emissão da mensagem de *hello*. Se a rede deseja tornar-se mais sensível às mudanças topológicas, este intervalo pode ser reduzido, com o ônus de congestionar mais a rede com pacotes de controle. O *Willingness* representa a disponibilidade do nó para o repasse de dados, se o *Willingness* estiver marcado como *WILL_NEVER*, o nó não será capaz de retransmitir pacotes. Caso esteja marcado como *WILL_ALWAYS*, ele sempre poderá repassar, e assim terá grande potencial de ser escolhido como MPR.

A seguir são listados os endereços do vizinho do nó emissor do *hello* e as características dos enlaces para estes vizinhos. Para cada conjunto de vizinhos um cabeçalho é acrescentado com os campos *Link Code* e o tamanho desta mensagem (de um *Link Code* até o próximo). O *Link Code* é dividido ainda em dois outros campos: Tipo de Enlace e Tipo de Vizinho.

Os Tipos de Enlace são classificados como:

- UNSPEC_LINK – indica que nenhuma informação sobre os enlaces é dada.
- ASYM_LINK – indica que os enlaces para os vizinhos listados são simétricos.
- SYM_LINK – indica que os enlaces para os vizinhos listados são assimétricos.
- LOST_LINK – indica que os enlaces para os vizinhos listados foram perdidos.

Os Tipos de Vizinhos são os seguintes:

- SYM_NEIGH – indica que os vizinhos listados possuem um enlace simétrico com este nó.
- MPR_NEIGH – indica que os vizinhos listados possuem um enlace simétrico com este nó e foram selecionados como MPR pelo emissor.
- NOT_NEIGH – indica que os nós não são mais vizinhos ou que os enlaces até eles são assimétricos.

Sempre que um nó recebe um *hello*, ele atualiza seus repositórios e estas informações serão de suma importância no processo de seleção dos nós MPR. Com elas é possível que o nó detecte todos os seus vizinhos e seus respectivos vizinhos (vizinhos de dois saltos) e as condições dos enlaces entre eles, possibilitando a escolha de MPRs que satisfaçam os requisitos apresentados anteriormente. Como todos os enlaces onde o MPR está envolvido devem ser simétricos, isto garante que todo repasse de pacotes no OLSR ocorra em enlaces simétricos, o que evita problemas causados por enlaces unidirecionais.

Mensagem TC

Através das mensagens *hello*, as características dos enlaces e a detecção de vizinhança, dão uma noção de como cada nó pode se comunicar com seus vizinhos. As mensagens TC lançam mão de algumas dessas informações armazenadas nos repositórios que servem como base para a disseminação de informações topológicas por toda a rede e que serão usadas na construção das rotas.

Como apenas os nós MPR repassam dados numa rede OLSR, para os nós obterem informações suficientes sobre o posicionamento de cada nó na rede, os nós MPR devem disseminar a lista de seus nós seletores através das mensagens TC. Desta forma, cada nó da rede reconhece por qual MPR um determinado nó pode ser alcançado. Essas mensagens, assim como o *hello*, também são enviadas periodicamente. A Figura 1.15 ilustra o formato das mensagens TC.

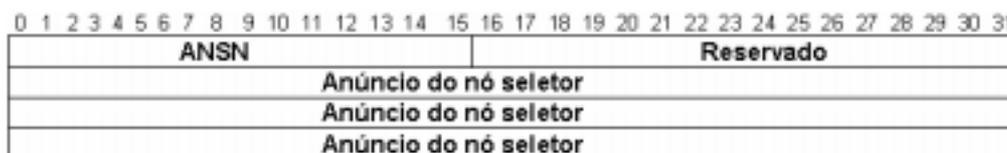


Figura 1.15. Formato da mensagem TC

O campo ANSN é o número de seqüência associado ao anúncio dos nós seletores. Com ele, o nó receptor saberá se a mensagem é recente e deve ser considerada

ou não. A seguir são listados todos os nós seletores deste nó MPR que está disseminando o TC.

Com estas informações, cada nó se torna capaz de calcular as rotas localmente através do algoritmo de Dijkstra [Tanenbaum, 2003]. O protocolo OLSR, por conta de sua técnica que reduz o overhead, apresenta uma grande melhora em eficiência frente aos protocolos clássicos de estado de enlace. E quanto maior e mais densa for a rede, maior será a eficiência deste protocolo comparada aos outros.

1.3.2. Projetos de Redes que Adotam Soluções Tradicionais para Múltiplos Saltos

Nos últimos anos, várias universidades e centros de pesquisa ao redor do mundo têm desenvolvido e instalado redes sem fio para comunicação ubíqua dentro de seus campi. Mais recentemente, a tecnologia de rede sem fio tem sido usada para prover acesso às redes universitárias para usuários que moram nas proximidades de seus campi, usando o conceito de redes sem fio de múltiplos saltos através de soluções tradicionais no nível de rede. Existem vários projetos ao redor do mundo, como por exemplo, RoofNet no MIT [Bicket et al., 2005, Couto et al., 2003], VMesh na Grécia [Tsarmpopoulos et al., 2005], MeshNet na UCSB [Ho et al., 2004; Ramachandran et al., 2005], CUWin em Urbana [Lad et al., 2005], Microsoft Mesh [Draves et al., 2004a; Draves et al., 2004b], ReMesh em Niterói [Passos et al. 2006; Muchaluat-Saade et al., 2007], entre outros.

Além de projetos acadêmicos, soluções comerciais também aparecem no mercado, oferecidas por grandes empresas, como Nortel [Roch, 2005] e Cisco [Cisco, 2008], e por pequenas empresas também [Bruno et al., 2005]. Diversos governos estão investindo na construção de cidades digitais usando redes sem fio de múltiplos saltos, como em Dublin [Weber et al., 2003], em Taipei onde os produtos da Nortel estão sendo usados e na cidade histórica de Tiradentes no Brasil, que utiliza a solução da Cisco.

Algumas soluções, incluindo as da Microsoft [Draves et al., 2004a], Nortel e Cisco, usam duas frequências de transmissão diferentes, normalmente 802.11a em 5GHz para o backhaul (enlaces entre os roteadores sem fio) e 802.11b/g em 2.4GHz para os enlaces de acesso (entre pontos de acesso e usuários).

Em relação ao protocolo de roteamento, diferentes soluções são escolhidas em cada projeto. VMesh e ReMesh utilizam OLSR. Microsoft Mesh usa um protocolo reativo com roteamento na origem derivado do DSR (*Dynamic Source Routing*) [Johnson et al., 2001], chamado MR-LQSR (*Multi-Radio Link-Quality Source Routing*) [Draves et al., 2004a]. RoofNet desenvolveu uma proposta híbrida, combinando a técnica de estado de enlace e a descoberta sob demanda no estilo DSR, criando um protocolo chamado Srcr [Bicket et al., 2005]. O trabalho da UCSB apresentado em [Ramachandran et al., 2005] utiliza o AODV. A solução da Cisco utiliza um protocolo de roteamento proprietário chamado AWP (*Adaptive Wireless Path*) [Cisco, 2008] e a Nortel utiliza o OSPF (*Open Shortest Path First*) [Roch, 2005], tradicionalmente usado em redes cabeadas. O projeto CUWin está desenvolvendo um protocolo de roteamento escalável, baseado em *link state*, que minimiza o custo de manter um visão consistente da rede, chamado HSLs (*Hazy Sighted Link State*) [Bruno et al., 2005; Santivanez et al., 2002; Santivanez e Ramanathan, 2003].

Os custos dos enlaces sem fio, usados para descoberta das melhores rotas, podem ser calculados usando a contagem de saltos tradicional [Clausen e Jacquet, 2003; Santivanez et al., 2002], o tempo de ida e volta por salto, retardos entre pares de pacotes [Draves et al 2004a], a métrica ETX (*Expected Transmission Count*) [Couto et al., 2003] ou métricas similares derivadas, tal como ETT (*Expected Transmission Time*) [Bicket et al., 2005] e WCETT (*Weighted Cumulative Expected Transmission Time*) [Draves et al., 2004a]. A métrica ETX mede dinamicamente a qualidade dos enlaces sem fio, tentando encontrar caminhos com o menor número de transmissões necessárias para entregar um pacote ao seu destino final. A métrica ETT prevê o tempo total para enviar um pacote ao longo de uma rota, considerando a taxa de transmissão máxima de cada enlace e a probabilidade de recepção usando essa taxa. WCETT leva em consideração a interferência entre enlaces que utilizam o mesmo canal. Uma discussão detalhada sobre métricas para qualidade de enlaces pode ser encontrada em [Campista et al., 2008]

1.3.3. Um Caso Real: Projeto ReMesh

O projeto ReMesh iniciou em 2005 como um grupo de trabalho da RNP (Rede Nacional de Pesquisa) constituído por professores e alunos do Instituto de Computação (IC) e do Departamento de Engenharia de Telecomunicações (TET) da Universidade Federal Fluminense (UFF). O seu intuito foi oferecer uma alternativa altamente desejável de acesso banda larga de baixo custo para a comunidade universitária da UFF e de diversas universidades brasileiras. A arquitetura proposta pela solução ReMesh para rede de acesso sem fio banda larga está ilustrada na Figura 1.16.

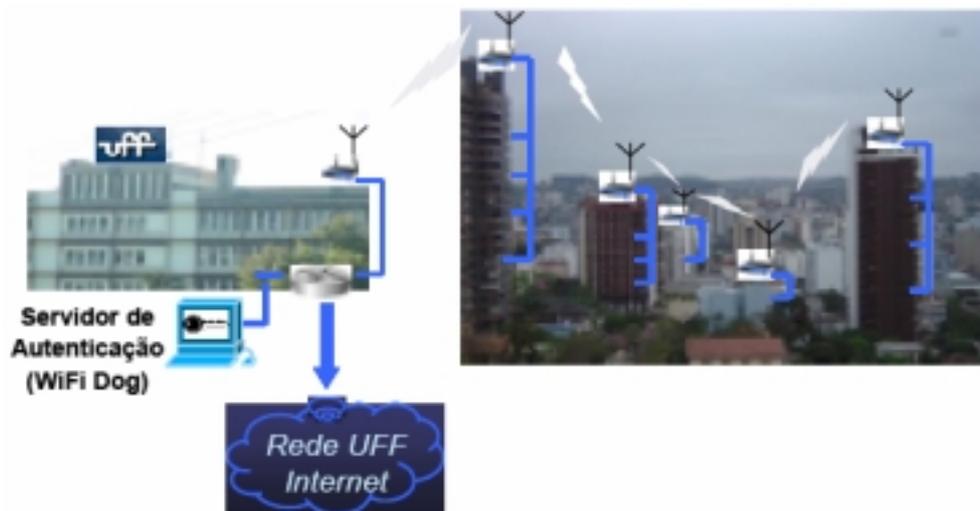


Figura 1.16. Arquitetura do ReMesh

Os roteadores que compõem a malha sem fio são instalados no topo dos edifícios ou casas dos usuários da comunidade. Através de conexão Ethernet ou WiFi, os usuários interligam suas estações pessoais ao roteador de sua residência, e através de uma rede sem fio em múltiplos saltos, os roteadores se comunicam como(s) *gateway(s)* para Internet, sendo este(s) instalado(s) no topo de um dos prédios da instituição que possui acesso à Internet. O *gateway* se comunica com um servidor de autenticação, que através do software aberto Wifidog (*captive portal*) [Wifidog, 2008], realiza o controle

de acesso à rede em malha. Só os usuários cadastrados têm acesso à rede, depois de se autenticarem.

Como solução de roteamento, o Projeto ReMesh utiliza uma implementação do protocolo pró-ativo OLSR estendida com uma métrica que mede a qualidade dos enlaces, chamada ML (*Minimum Loss*) [Passos et al., 2006], derivada da métrica ETX. O protocolo OLSR-ML tenta encontrar caminhos de menor perda para entregar um pacote ao seu destino final.

A rede em malhas sem fio da UFF está em funcionamento desde abril de 2006, tendo hoje mais de 70 usuários cadastrados, que já transferiram mais de 700GB de informação através da rede.

1.4. Padrão Emergente IEEE 802.11s

Em setembro de 2003, o IEEE formou um grupo de estudos para pesquisar a criação de redes em malha sem fio de múltiplos saltos. Um ano mais tarde, este grupo deu origem ao *Task Group “s”* (TGs), que posteriormente, em março de 2006, publicou seu primeiro *draft*. Até o momento da escrita deste capítulo, IEEE 802.11s ainda está na fase de *draft* (atualmente na versão 1.08) [IEEE, 2007], por isto algumas mudanças devem ser esperadas até que IEEE 802.11s se torne um padrão. De fato, muitos melhoramentos foram feitos no *draft* atual, considerando versões anteriores do documento, e o leitor deve sempre ter em mente que este trabalho ainda está em andamento. Não obstante, implementações comerciais deste *draft* já estão disponíveis em alguns dispositivos sem fio [OLPC, 2008; Open802.11s, 2008].

Devido a limitações de recursos dos dispositivos sem fio portáteis, tais como alimentação, processamento e memória, existe uma demanda de soluções para esse tipo de equipamentos que possam ser facilmente embutidas em cartões de rede (*Network Interface Cards* – NICs) e em SoCs (*systems-on-chip*). Por isso, uma solução para comunicação em múltiplos saltos implementada na camada de enlace, sendo leve em contraste com uma implementação tradicional de roteamento no nível de rede, se encaixa perfeitamente neste propósito.

A proposta de padrão introduz novos formatos de quadros, trata de questões como segurança e gerenciamento, assim como uma série de otimizações necessárias para a montagem de redes em malha de múltiplos saltos no nível de enlace. Além disso, boa parte de seu conteúdo é dedicada à descrição de protocolos para encaminhamento de quadros na rede em malha.

Originalmente, dois mecanismos de seleção de caminho foram propostos em versões anteriores do *draft*. RA-OLSR (*Radio-Aware Optimized Link State Routing*) [Zhang et al., 2007], que é um protocolo pró-ativo com um mecanismo de controle de inundação baseado no OLSR [Clausen e Jacquet, 2003], porém adaptado para trabalhar em nível dois ao invés do três. E um protocolo híbrido, chamado HWMP (*Hybrid Wireless Mesh Protocol*), baseado no AODV [Perkins et al., 2003] e na sua extensão AODV-ST [Ramachandran et al., 2005]. O HWMP é atualmente o protocolo obrigatório e o único restante na proposta atual (versão 1.08). RA-OLSR foi removido em favor de um framework de seleção de caminhos extensível que possibilita implementações alternativas de protocolos e métricas para seleção de caminhos.

Antes de discutirmos os mecanismos de seleção de caminhos iremos apresentar brevemente os mecanismos de criação da rede em malha e descrever a arquitetura proposta pelo padrão emergente.

1.4.1. Arquitetura da Rede sem Fio com Múltiplos Saltos no Nível de Enlace

De acordo com o proposto pelo futuro padrão IEEE 802.11s, os nós em uma rede em malha podem ser classificados da seguinte forma (ver Figura 1.17):

- Cliente ou estação (STA) é um nó que utiliza serviços da rede, mas não encaminha pacotes de outros nós e também não participa dos mecanismos de descoberta de caminhos.
- Nó mesh (MP – *Mesh Point*) é um nó que participa da formação e da operação da rede em malha. O conjunto de MPs que participa da mesma rede em malha forma a nuvem mesh (*mesh cloud*).
- Ponto de acesso mesh (MAP – *Mesh Access Point*) é um MP que incorpora também funcionalidades de um ponto de acesso (AP) e, através destas, oferece serviços às estações (STA).
- Portal mesh (MPP – *Mesh Portal Point*) é um MP que incorpora as funcionalidades adicionais de um *gateway*, conectando a nuvem em malha a uma rede externa, como a Internet, por exemplo.

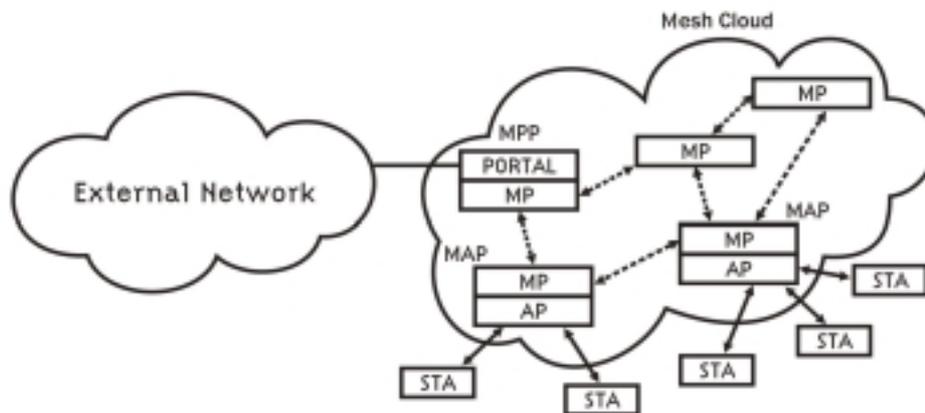


Figura 1.17. Topologia de uma rede sem fio IEEE 802.11s com múltiplos saltos

A Figura 1.17 ilustra uma possível topologia ad-hoc para a arquitetura proposta. Observa-se que as linhas pontilhadas representam a rede em malha propriamente dita à qual estações compatíveis com o padrão 802.11 (mas sem capacidades de MP, isto é, STAs) participam indiretamente, por intermédio de nós mesh (MPs) estendidos com funcionalidades de ponto de acesso (AP).

Nesta topologia apenas um MPP (PORTAL/MP) está presente, mas cabe ressaltar que nada impede a presença de múltiplos desses nós especializados, ficando a seleção de um deles por conta de cada estação.

A Figura 1.17 deve ser vista como um instantâneo para o que seria uma topologia dinâmica, onde os nós podem se movimentar em padrões imprevisíveis e

variados e enlaces podem se formar (ou ser interrompidos) não apenas em função destes movimentos, mas também como consequência das condições mutáveis do espectro. Neste sentido, a função de MPP pode ser oportunista e anunciada sempre que possível através dos protocolos e mecanismos aplicáveis, que serão analisados adiante.

1.4.2. Criação da Nuvem Mesh

Em redes sem fio infra-estruturadas, um identificador (SSID) é usado para distinguir os grupos de pontos de acesso, que mantêm uma correlação funcional e pertencem a uma mesma rede.

Da mesma maneira, uma rede mesh precisa de um identificador de rede, mas ao invés de sobrecarregar a definição e função do SSID, o *draft* propõe um identificador Mesh ou Mesh ID. Similarmente ao padrão IEEE 802.11, quadros de controle (*beacons*) são usados para anunciar um Mesh ID, que não deve ser confundido com o SSID padrão empregado nas redes sem fio infra-estruturadas tradicionais. Para evitar confundir um nó não-mesh que tente se associar a uma rede mesh por engano, nós mesh (MPs) enviam *beacons* em broadcast com o SSID setado com um valor especial.

O Mesh ID é um dos três elementos que caracterizam a rede mesh. Os outros dois são o protocolo de seleção de caminho e a métrica de seleção de caminho. Juntos, estes três elementos definem um perfil. Um nó mesh pode suportar diferentes perfis, mas todos os nós da nuvem mesh, num dado momento, devem compartilhar o mesmo perfil.

O IEEE 802.11s define como perfil obrigatório o HWMP como mecanismo de descoberta de caminho e a métrica *Airtime Link Metric* para seleção de caminho, como serão apresentados nas seções seguintes. O *draft* não impede que outros protocolos ou métricas sejam usados na nuvem mesh. Pelo contrário, define *frameworks* para estes mecanismos alternativos, mas adverte que a rede mesh não pode usar mais de um perfil ao mesmo tempo. Essa recomendação pode ser interpretada como uma tentativa de evitar a complexidade da renegociação de perfis que pode ser muito dispendiosa para um dispositivo simples implementar. Se a nuvem mesh é formada por elementos não obrigatórios (protocolo e métrica), não é necessário voltar a configuração original para acomodar um novo membro mesh que só dê suporte ao perfil obrigatório.

Uma rede mesh é formada por MPs e vizinhos que compartilham o mesmo perfil. O mecanismo de descoberta de vizinhança é similar ao o que é atualmente proposto pelo padrão 802.11 – escaneamento ativo e passivo. Para conseguir isto, os já conhecidos quadros de *beacon* e *probe* são estendidos para incluir campos relacionados a rede mesh. Como será mostrado nas seções seguintes, o *draft* não introduz novos quadros mas estende os já existentes.

Para concluir nossa análise sobre o procedimento de criação da nuvem mesh, devemos comentar sobre o estabelecimento dos *peer links* – arestas do grafo mesh. Um nó mesh deve criar e manter *peer links* com seus vizinhos que compartilham o mesmo perfil ativo (um MP pode manter vários perfis, mas somente um está ativo num dado momento). Uma vez que um candidato a vizinho é encontrado, através de escaneamento ativo ou passivo, um MP usa o protocolo *Mesh Peer Link Management* [IEEE, 2007] para abrir um *peer link*.

Um *peer link* é univocamente identificado pelo endereço MAC de ambos os participantes e por um par de identificadores de enlaces, gerados por cada um dos MPs para minimizar reuso em intervalos de tempo pequenos.

Para estabelecer um *peer link*, ambos os MPs trocam quadros *Peer Link Open* e *Peer Link Confirm*, como retratado na Figura 1.18. Sempre que um MP quer fechar um *peer link*, ele deve mandar um quadro *Peer Link Close* para o MP par.

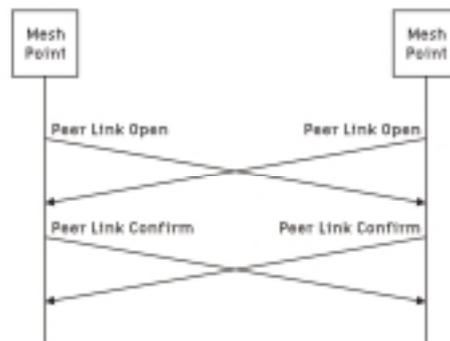


Figura 1.18. Criação de um *peer link* entre nós mesh no IEEE 802.11s

1.4.3. Mecanismos de seleção de caminho

IEEE 802.11s propõe um protocolo de seleção de caminho mandatório: um protocolo híbrido (reativo e pró-ativo) chamado HWMP (*Hybrid Wireless Mesh Protocol*). Apesar de o padrão assegurar compatibilidade entre dispositivos de diferentes fabricantes ditando um mecanismo mandatório (HWMP e *Air Link Metric*), ele também inclui um framework extensível que pode ser usado para dar suporte a aplicações específicas.

Para possibilitar a troca desses parâmetros de configuração, um elemento de configuração mesh (*Mesh Configuration element*) é transportado pelos quadros de *beacon*, quadros *Peer Link Open* e *Peer Link Confirm*. O elemento de configuração mesh contém, dentre outros campos, um identificador do protocolo de seleção de caminho (*Active Path Selection Protocol Identifier*) e um identificador da métrica de seleção de caminho (*Active Path Selection Metric Identifier*).

1.4.3.1. HWMP e *Air Link Metric*

O protocolo híbrido HWMP, inspirado no protocolo AODV (*Ad Hoc On Demand Distance Vector*) [Perkins et al., 2003], pretende mesclar as vantagens das abordagens pró-ativa e reativa para seleção de caminhos.

O HWMP pode, portanto, ser configurado para operar em dois modos: modo reativo sob demanda (*on-demand reactive mode*) ou modo pró-ativo baseado em árvore (*tree-based proactive mode*).

O primeiro – modo de operação sob demanda – é apropriado para estabelecimento de caminhos entre nós mesh (MPs) em um esquema *peer-to-peer*, ao passo que no segundo – modelo pró-ativo – cada nó calcula antecipadamente uma topologia em árvore onde a raiz é um determinado nó que se anuncia com tal (MP raiz). Esta abordagem que, como veremos adiante, pode ser implementada através de dois mecanismos distintos, pode aumentar a eficiência no encaminhamento de quadros

quando existe uma tendência de concentração de tráfego no nó raiz, que pode, por exemplo, estar atuando como portal mesh (MPP).

O que faz o HWMP realmente híbrido é o fato de que ambos os modos (pró-ativo e reativo) podem ser usados concomitantemente. A principal vantagem desta abordagem é que, em certas circunstâncias, apesar de disponível de antemão, o caminho entre dois nós em uma topologia em árvore pode não ser o caminho ótimo e, neste momento, a descoberta sob demanda pode ser empregada, fornecendo um caminho alternativo mais apropriado. Um exemplo de tal circunstância é o caso onde dois nós, que não são MP raiz, são capazes de trocar dados através de um caminho de custo mínimo (diretamente por um simples enlace mesh), mas são forçados a fazer com que seus quadros subam e desçam a árvore para alcançar um nó raiz.

Na especificação atual do IEEE 802.11s, a métrica obrigatória para definir a qualidade de um enlace sem fio é a chamada *Airtime Link Metric*. Ela representa a quantidade de tempo necessária para a transmissão de um quadro levando em consideração a taxa de transmissão, o overhead imposto pela camada física e a probabilidade de retransmissão do quadro (inferida da taxa de erros do enlace em questão). A forma de cálculo desta taxa de erros, no entanto é deixada a cargo da implementação, ou seja, não é descrita pela norma. Nós transmitindo em uma taxa baixa podem usar toda a banda do canal com suas longas transmissões da mesma maneira que um enlace com alta probabilidade de erro pode ocupar o meio por um longo tempo devido às retransmissões. A métrica *Airtime Link Metric* foi desenvolvida para evitar ambos os casos. De acordo com o padrão, a métrica é calculada como:

$$c_a = \left[O + \frac{B_t}{r} \right] \frac{1}{1 - e_f}$$

Onde O é uma latência constante de overhead que varia de acordo com a implementação da camada física, B_t é tamanho do quadro de teste (1024 bytes), r é a taxa de transmissão em Mbps com que o MP transmite o quadro de teste e e_f é a probabilidade de erro medida no envio do quadro de teste.

Durante o processo de descoberta de um caminho (*path discovery*), cada nó participante irá contribuir com seus cálculos de métrica acrescentando ou atualizando dados nos quadros de gerenciamento dedicados à troca de informações de encaminhamento. Independente do modo de operação (pró-ativo ou reativo) as funções do HWMP são implementadas pelos seguintes quadros de gerenciamento:

- *Path Request* (PREQ) – requisição de caminho – estes quadros são enviados em difusão (broadcast) por um MP que deseja encontrar um caminho para outro MP.
- *Path Reply* (PREP) – resposta de caminho – estes quadros são enviados pelo MP de destino, em resposta ao recebimento de uma requisição de caminho (PREQ).
- *Path Error* (PERR) – erro no caminho – estes quadros são usados para notificação de que um caminho não está mais disponível.
- *Root Announcement* (RANN) – anúncio de nó raiz – estes quadros são utilizados pelo nó que se anuncia como nó raiz (MP raiz). Conforme antecipamos, existem

dois mecanismos para implementação do modo pró-ativo no HWMP, sendo o quadro RANN usado em um deles.

Os quadros que acabamos de mencionar serão empregados em todos os três (dois pró-ativos e um reativo) mecanismos providos pelo HWMP, como colocado na Figura 1.19. O primeiro deles, reativo, é chamado de seleção de caminho sob demanda. Os outros dois pró-ativos são batizados de “mecanismo PREQ” e “mecanismo RANN”, em função dos quadros utilizados para o anúncio do nó raiz.



Figura 1.19. Variações do protocolo de seleção de caminho HWMP

A Figura 1.20 representa um exemplo de topologia para o mecanismo de descoberta de caminho sob demanda. Neste caso, um nó designado como origem S-MP deseja encontrar um caminho para um nó de destino D-MP e, para tal, precisará da colaboração dos nós intermediários I-MPs.

O mecanismo opera da seguinte maneira. O nó S-MP envia, por difusão, um quadro PREQ contendo o endereço MAC de D-MP, o nó de destino. Um nó mesh que receba esse quadro deverá checar suas tabelas e verificar se conhece um caminho para D-MP. Em caso afirmativo, deverá enviar um quadro de resposta (PREP) de volta para S-MP. Em caso negativo, o nó mesh intermediário (I-MP) deverá retransmitir o quadro, novamente usando o endereço MAC de difusão (FF:FF:FF:FF:FF:FF).

O nó de origem S-MP, no entanto, pode evitar que nós intermediários respondam à requisição PREQ setando o *flag* DO (*Destination Only* – destino apenas) no cabeçalho do quadro PREQ. Neste caso, apenas o nó de destino poderá responder a requisição original emitindo um quadro PREP. Desta forma, ao receber uma requisição (PREQ) onde DO tenha sido ativado, um nó intermediário irá forçosamente retransmitir o quadro PREQ e o processo se repetirá até que a requisição alcance seu destino. Na Figura 1.20, as setas em linha cheia representam PREQs.

Outro *flag* RF (*Reply and Forward* – resposta e encaminhe) também pode ser empregado para controlar o comportamento dos nós intermediários. Se RF for setado e DO não, um nó intermediário poderá responder a requisição, isto é, enviar um PREP (contanto, é claro, que conheça um caminho para o nó de destino), mas ainda assim deverá retransmitir o quadro de requisição adiante.

Se, por outro lado, DO e RF estiverem desativados, um nó intermediário está autorizado a responder a requisição, mas uma vez que o faça, não deverá mais retransmitir o quadro PREQ. Observa-se, portanto, que os *flags* DO e RF determinam a quantidade de respostas (PREPs) recebidas pela origem S-MP.

A cada vez que manipula um quadro PREQ, um nó mesh intermediário aprende um caminho reverso para o nó de origem S-MP. Este poderá ser útil mais tarde para o encaminhamento dos quadros de resposta (PREPs), no caso do nó intermediário em questão participar do caminho selecionado. Justamente por conta da formação deste caminho reverso, os quadros de resposta (PREPs) poderão ser encaminhados em unicast para o nó de origem S-MP.

Os quadros PREQ e PREP carregam um campo de métrica que é incrementado por cada nó intermediário, refletindo os tempos de transmissão de cada enlace no caminho. É através desta métrica que o nó de destino D-MP é capaz de selecionar um caminho reverso dentre os múltiplos caminhos eventualmente existentes (dado um cenário de nuvem densa). Analogamente o nó de origem S-MP poderá escolher entre vários caminhos diretos, caso existam, através da métrica contida nos quadros de resposta, encerrando, desta forma, o ciclo de descoberta de caminho.

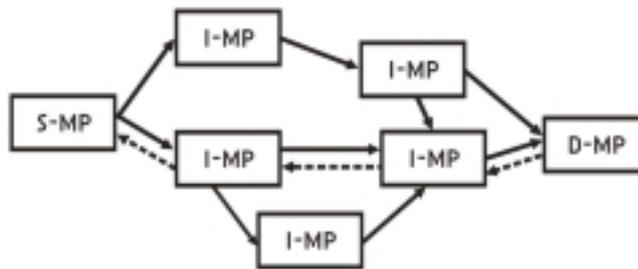


Figura 1.20. Exemplo do mecanismo de descoberta de caminho sob demanda

No que diz respeito à densidade da nuvem mesh, devemos notar que, em um meio sem fio, grande cobertura e alta taxa de transmissão são objetivos conflitantes, pois aumentado um, diminui o outro. Quadros broadcast e multicast são normalmente transmitidos a baixas taxas para atingir o maior número de nós possíveis. Nós distantes terão maior chance de receber os quadros, se eles foram transmitidos a uma taxa baixa. Por outro lado, esses quadros levarão um maior tempo para se propagar através da nuvem, o que pode ser problemático em uma ambiente denso.

Como dissemos antes, além do mecanismo de descoberta de caminho por demanda, o protocolo HWMP provê dois diferentes métodos pró-ativos para construção de tabelas de encaminhamento. O primeiro deles é baseado no emprego de quadros PREQ e por isso chamado de “mecanismo pró-ativo PREQ”. O segundo utiliza um quadro especial, chamado RANN e, da mesma forma, fica designado como “mecanismo pró-ativo RANN”.

No mecanismo baseado em PREQs, uma vez configurado para operar como MP raiz, um nó mesh difunde periodicamente um quadro PREQ com os *flags* DO e RF ativados, o que configura um quadro “PREQ pró-ativo”. Cada nó que receba este quadro irá atualizar seu cabeçalho com os valores de métrica e contagem de saltos e retransmiti-lo. Com o tempo, todos os nós da nuvem mesh serão notificados.

Ao receber um PREQ pró-ativo um nó responde ou não com um PREP em função do valor de um terceiro *flag* no cabeçalho do quadro de requisição. Se setado, este *flag* chamado “PREP pró ativo” (*Proactive PREP*) faz com que os nós enviem um PREP de volta ao nó raiz. Na verdade, mesmo que “PREP pró-ativo” esteja desativado,

um nó pode responder ao nó raiz com um PREP se desejar estabelecer um caminho no esquema *peer-to-peer* com o nó raiz. Por exemplo, ele pode ter dados para enviar ao nó raiz.

No segundo mecanismo pró-ativo previsto pelo IEEE 802.11s, ao invés de utilizar quadros PREQs o nó raiz inunda a nuvem mesh com quadros RANN (*Root Announcement*). Neste caso, os nós que eventualmente desejem formar caminhos para o nó raiz enviam, para este, um quadro PREQ.

Desta vez, a requisição PREQ será enviada em unicast, mas será processada pelos nós intermediários através das mesmas regras aplicadas aos quadros PREQ difundidos pelo mecanismo reativo do protocolo. O nó raiz, ao receber a requisição responderá com o respectivo quadro PREP, estabelecendo assim, um caminho entre o nó requisitante e o nó raiz. Por fim, o mecanismo RANN introduz um passo adicional e pode ser vantajoso se comparado com o mecanismo PREQ apenas se uma pequena porção dos MPs deseja estabelecer caminhos com o nó raiz.

Finalmente, é importante comentar o papel do quadro PERR dentro do esquema recém descrito. Sempre que um quadro não puder ser encaminhado por um nó pertencente ao caminho, este deverá notificar o remetente sobre a quebra do enlace e, conseqüente inviabilidade daquele caminho. Esta informação deverá ser encaminhada de volta a todos os participantes anteriores alcançando finalmente o remetente original que, assim, deverá iniciar um novo ciclo de descoberta de caminho.

1.4.3.2. MPPs – Portais Mesh

A capacidade de encaminhamento de tráfego através de múltiplos saltos em uma rede mesh não seria tão útil sem um mecanismo que possibilitasse conectar a nuvem mesh a outras redes como, por exemplo, a Internet cabeada. A Figura 1.21 mostra dois exemplos de interconexão de redes mesh. Como mencionado anteriormente, o IEEE 802.11s chama os nós *gateways* de portais mesh MPPs (*Mesh Portal Points*).

Na Figura 1.21a, está ilustrado o uso dos MPPs para interconectar nuvens mesh a outras redes locais. Nesse cenário os portais mesh atuam como pontes e todos os nós interconectados pertencem a mesma sub-rede de nível três. A Figura 1.21b retrata outro cenário onde os MPPs atuam como *gateways* para outras sub-redes de nível três. Em uma rede em malha ad hoc, onde cada nó é um potencial roteador, ele se torna também um potencial *gateway* entre a nuvem mesh e a infra-estrutura cabeada.

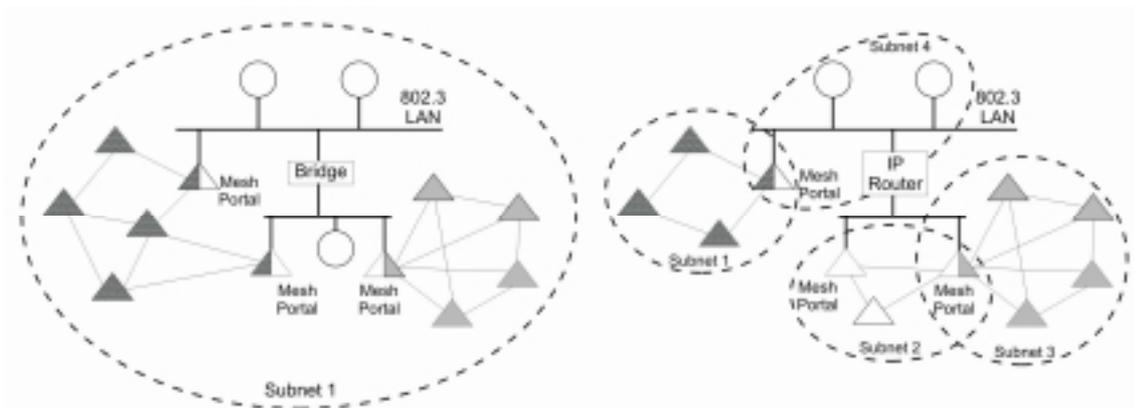


Figura 1.21. Exemplos de interconexão através de portais mesh.
(a) Bridging na camada 2; (b) Roteamento na camada 3

A característica básica de um MPP é o fato de ser um nó que participa da nuvem mesh, isto é um nó mesh, ao mesmo tempo em que mantém conexão com uma outra rede. Esta capacidade deve ser de alguma forma propagada pela nuvem, permitindo que outros MPs se beneficiem desta dupla conectividade. Por isso, uma vez configurado como MPP um nó irá anunciar seu status através da transmissão em difusão de quadros de anúncio de portal chamados de PANNs (*Portal Announcements*).

Um MP que receba o anúncio, isto é o quadro PANN, irá registrar o endereço MAC do portal associado à métrica do caminho até ele e, em seguida retransmitir, por difusão, o quadro de anúncio. Cada nó da nuvem mesh irá manter uma lista dos MPPs disponíveis e escolherá um dentre eles para encaminhar seu tráfego destinado para fora dos limites da nuvem.

Um portal mesh (MPP) também pode ser usado para interconectar redes mesh que usam diferentes protocolos de seleção de caminho, como ilustrado na Figura 1.21b. O projeto de interconexão de várias redes cabeadas IEEE 802.3 e nuvens mesh através de uma grande inter-rede de camada dois, como apresentado na Figura 1.21a, pode ser facilmente implementado por pontes que seguem o padrão 802.1D [IEEE, 1998].

1.4.4. Sintaxe do Padrão IEEE 802.11s

Esta seção apresenta como o IEEE 802.11s estende o formato dos quadros IEEE 802.11 de forma a suportar seus objetivos, isto é, uma rede sem fio de múltiplos saltos implementada no nível de enlace (camada MAC). Inicialmente é apresentado o uso de seis endereços MAC em um mesmo quadro e, logo em seguida, o formato dos quadros IEEE 802.11s é detalhado.

1.4.4.1. Formato dos Quadros IEEE 802.11s

Inicialmente, recordamos que os dois primeiros bytes de um quadro 802.11 contêm o chamado campo de controle do quadro (*frame control field*), sendo que dois bits deste campo (o terceiro e o quarto) identificam o tipo de quadro, conforme a Figura 1.22.

00 = quadro de gerenciamento	01 = quadro de controle
10 = quadro de dados	11 = reservado

Figura 1.22. Tipos de quadros 802.11

Além do campo tipo, outros quatro bits são reservados para definir subtipos dentro de uma categoria. Assim, um *beacon*, por exemplo, é definido como tipo gerenciamento (0x0) e subtipo *beacon* (0x8), ao passo que um ACK (*acknowledgement*) pertence ao tipo controle (0x1) e subtipo (0xD).

Por se tratar de uma extensão ao padrão IEEE 802.11, os quadros mesh introduzidos pelo 802.11s devem ser classificados dentro dos quatro tipos existentes. Inicialmente, pretendia-se utilizar o tipo reservado, ainda disponível (0x3), mas em versões mais recentes da proposta definiu-se que:

- Os dados trocados por MPs são transportados por quadros de dados mesh (*Mesh Data Frames*), definidos como quadros de dados (tipo 0x2) com um cabeçalho mesh pré-posto ao corpo do quadro 802.11, similar ao que está ilustrado na Figura 1.24.
- Quadros de gerência da rede mesh, como por exemplo os quadros PREQ, PREP, etc, são definidos como pertencentes ao tipo 0x0 (*management frames*) e subtipo 0xF, até então reservado. Estes quadros foram batizados como *Multihop Action frames*.

Outra característica dos novos quadros é a utilização dos *flags FromDS* e *ToDS*. Estes bits são utilizados, em uma rede IEEE 802.11, para marcar pacotes que sejam destinados a um sistema de distribuição (*ToDS*) ou sejam oriundos deste (*FromDS*). O sistema de distribuição, em uma rede sem fio, é a infra-estrutura que pode interligar diversos pontos de acesso ou mesmo conectar a rede sem fio à Internet. Assim, por exemplo, um quadro oriundo de uma estação IEEE 802.11 em modo infra-estrutura que seja destinado a outra estação IEEE 802.11 tem os flags *FromDS* = 0 e *ToDS* = 1. A Figura 1.23 representa um sistema de distribuição sem fio (WDS – *Wireless Distribution System*) [IEEE, 1999] que interliga dois pontos de acesso (AP1 e AP2), permitindo a troca de quadros entre duas estações (STA1 e STA2) sem que haja participação da camada de rede. Em outras palavras, o sistema de distribuição provê uma ponte para o ESS (*Extended Service Set*).

Um sistema de distribuição sem fio (*Wireless Distribution System*), ou WDS, é aquele em que diversos pontos de acesso permitem a troca de dados entre estações a eles associadas através de quadros IEEE 802.11, ou seja, por intermédio de um backbone sem fio, e não através de quadros IEEE 802.3 como em uma rede cabeada. Chama-se de quadro WDS aquele que possui ambos os *flags fromDS* e *ToDS* setados. Sua função original é, portanto, a de permitir a troca de dados entre estações associadas a diferentes pontos de acesso dentro de uma mesma rede local sem fio. O que o IEEE 802.11s propõe é que quadros trocados pelos MPs em um nuvem mesh sejam também marcados com ambos esses *flags*.

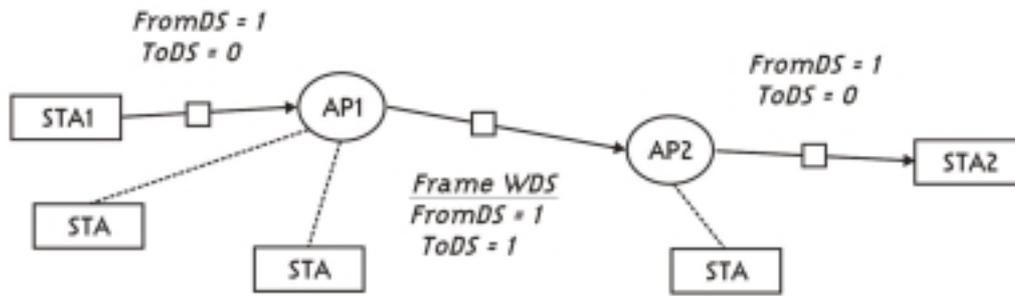


Figura 1.23. Exemplo de uso dos flags *FromDS* e *ToDS* em uma rede local sem fio

Antes da extensão “s” o padrão 802.11 classificava os quadros onde os *flags FromDS* e *ToDS* estavam ativados como “quadro de dados usando o formato de quatro endereços”. Com a proposta do IEEE 802.11s a redação na atual versão do draft passa a ser “quadros de dados usando o formato de cabeçalho MAC de quatro endereços, que incluem mas não se limitam a quadros de dados mesh”.

Como não foi padronizada, diversas implementações proprietárias e não documentadas de WDS podem ser encontradas em modelos variados de pontos de acesso, algumas potencialmente conflitantes com o padrão emergente. Isso aponta para um futuro de ajustes não apenas na proposta do IEEE 802.11s, mas destas implementações, de forma a evitar problemas de compatibilidade.

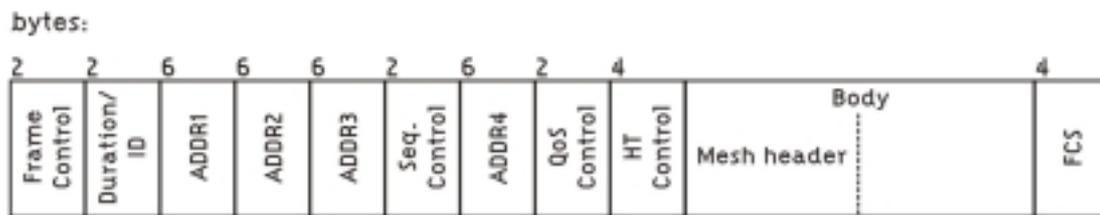


Figura 1.24. Estrutura geral de um quadro IEEE 802.11s

É oportuno observar que em uma rede IEEE 802.11 no modo ad-hoc, cada quadro traz ambos os *flags (FromDS e ToDS)* desmarcados (zerados). Isto evidencia uma importante diferença. Uma rede ad-hoc IEEE 802.11 é aquela em que conexões oportunistas podem ser formadas entre estações IEEE 802.11, mas onde não há múltiplos saltos ou, em outras palavras, encaminhamentos de quadros, e não deve ser confundida com uma rede mesh.

A Figura 1.24 mostra a estrutura geral de um quadro IEEE 802.11 estendido pelo cabeçalho mesh, pré-posto ao corpo do quadro. O cabeçalho mesh é, por sua vez, representado na Figura 1.25 e contém quatro campos. O primeiro é o *Mesh Flags*, que atualmente só define o uso dos primeiros dois bits, ficando os outros 6 reservados.

Os primeiros dois bits determinam a quantidade de endereços MAC presentes no último campo, *Mesh Address Extension*, o que pode variar entre 0 e 3, indicando um campo de 0, 6, 12 ou 18 bytes, onde cada endereço possui 6 bytes.

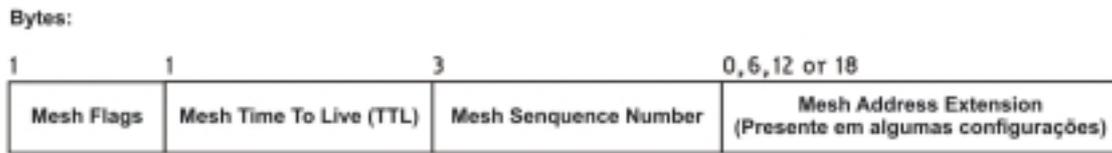


Figura 1.25. Formato do cabeçalho mesh (*mesh header*)

O campo Mesh TTL indica a quantidade máxima de saltos que um quadro poderá realizar na nuvem mesh e é decrementado por cada nó que retransmitir o quadro. Seu objetivo é evitar que quadros sejam eternamente retransmitidos na nuvem por conta de algum *loop* de encaminhamento.

O número de seqüência mesh (*Mesh Sequence Number*) é um identificador do quadro que permite a uma estação detectar o recebimento de duplicatas prevenindo retransmissões desnecessárias dentro da nuvem mesh. E, finalmente, o já mencionado campo *Mesh Address Extension* que carrega endereços MAC extras, já que a rede mesh pode precisar de até seis endereços como será discutido na próxima seção.

1.4.4.2. Conectividade de STAs e Endereçamento de Quadros

De acordo com o IEEE 802.11s, nós não-mesh (STAs) podem participar da rede mesh através de um nó mesh (MP) com capacidades de ponto de acesso (nós MAP na Figura 1.17). STAs se comunicando pela nuvem mesh são intermediados pelos seus respectivos MAPs e este cenário constitui um exemplo de como é usado o formato de quadro com seis endereços.

O formato de quadro IEEE 802.11 usual, com quatro endereços, pode ser usado tanto para transmissão de dados como para quadros de controle. Os quatro endereços MAC nesse caso são:

- SA (*Source Address*) é o endereço MAC da fonte do quadro, ou seja, o nó que gerou o quadro original.
- DA (*Destination Address*) é o endereço MAC do nó que é o destino final do quadro.
- TA (*Transmitter Address*) é o endereço MAC do nó que transmite um quadro. Será igual à SA quando o quadro for originado e transmitido pela primeira vez. Será diferente de SA toda vez que for transmitido por um nó intermediário.
- RA (*Receiver Address*) é o endereço MAC do próximo nó que irá receber o quadro e pode ser o mesmo que DA quando o quadro está para alcançar seu destino final.

Em resumo, SA e DA estão associados aos nós extremos em um caminho completo pela nuvem mesh, ao passo que TA e RA estão associados aos nós participantes de uma transmissão em um enlace. Mas, como será discutido a seguir, quadros com quatro endereços, utilizados no padrão IEEE 802.11 original para transmissão usando um sistema de distribuição sem fio, não são suficientes para implementar todas as funcionalidades propostas pela emenda “s”.

Como exemplificamos acima, se dois nós não-mesh estão se comunicando através da nuvem mesh, dois endereços adicionais são necessários – o Mesh SA (*Mesh Source Address*) e o Mesh DA (*Mesh Destination Address*). Para entendê-los, as entidades DA e SA são definidas de uma forma mais geral:

- Mesh SA – Em um quadro de seis endereços, o SA (*Source Address*) é o nó originador da comunicação fim-a-fim e esta fora da nuvem mesh, enquanto o Mesh SA é o endereço do nó que introduz o quadro na nuvem mesh (em nome de SA).
- Mesh DA – Da mesma forma, DA (*Destination Address*) define o endereço final do quadro, ao passo que Mesh DA é o endereço da última estação que recebe o quadro na nuvem (e faz isso em nome de DA).

A Figura 1.26 representa um cenário onde STA1 deseja se comunicar com STA2 associada a um MAP distinto do seu. Durante esta transmissão, se analisarmos um quadro enquanto este é encaminhado do nó MP1 para o nó MP2, observamos o esquema de seis endereços em ação. Os vários endereços são mostrados na própria figura.

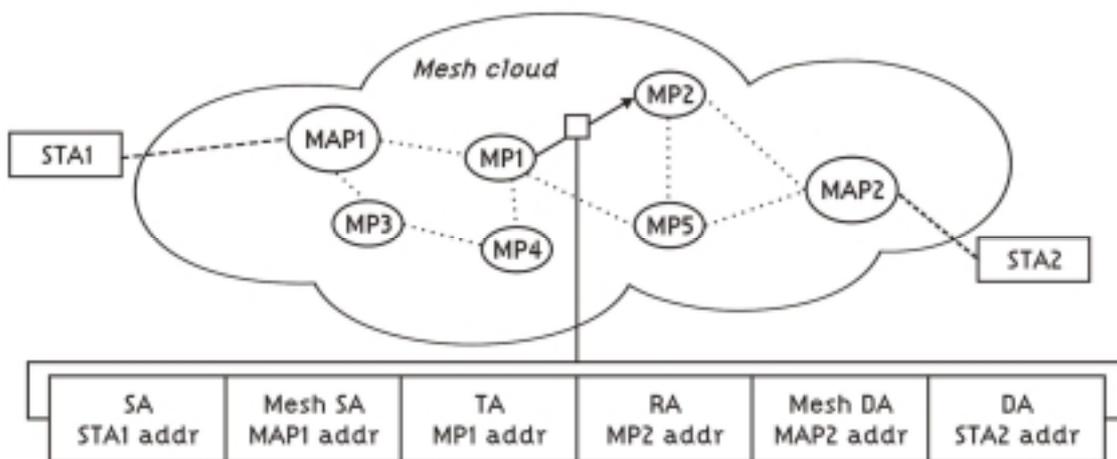


Figura 1.26. Cenário em que 6 endereços MAC são utilizados na transmissão entre duas STAs

Um outro caso onde o formato com seis endereços é usado é no modo pró-ativo do HWMP (baseado em árvore), onde dois nós conseguem se comunicar através de um MP raiz. Neste cenário, o caminho completo inclui dois sub-caminhos – um do MP fonte até o MP raiz e outro deste até o MP de destino. Finalmente, MPs conseguem também se comunicar com o “mundo exterior” através de portais mesh (MPPs). Em todos esses casos, mais de quatro endereços são necessários.

A Figura 1.27 representa um cenário similar, substituindo MAP2 por um MPP. Neste caso, cinco endereços MAC distintos são necessários e o esquema de seis endereços é também empregado, sendo que tanto o Mesh DA quanto o DA contém o endereço MAC do MPP. É tarefa deste MPP agir como *gateway* e encaminhar o tráfego oriundo de STA para fora da nuvem mesh, possivelmente através do emprego de roteamento na camada três.

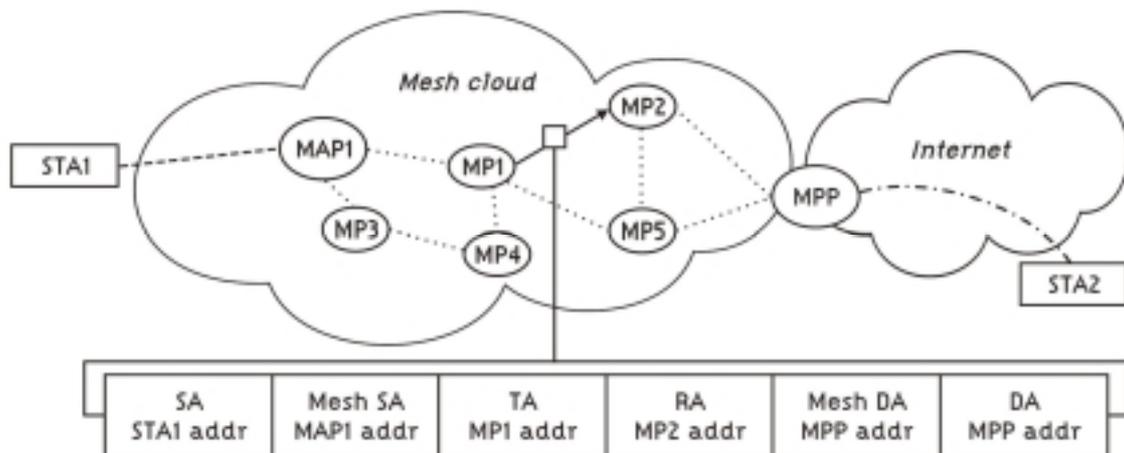


Figura 1.27. Cenário em que 5 endereços MAC são utilizados na transmissão entre um STA e um MPP

1.4.5. Características Adicionais

O Padrão IEEE 802.11s cobre muito mais do que podemos registrar neste capítulo de livro. Tentamos apresentar os pontos mais importantes para o entendimento do funcionamento de uma rede mesh, mas há ainda muitos outros aspectos interessantes [Camp e Knightly, 2008].

O IEEE 802.11s introduz um método de acesso ao meio chamado MDA (*Mesh Deterministic Access*), que ajuda a reduzir a contenção com o uso de uma nova função de coordenação. O mecanismo é opcional e pode ser implementado por um sub-grupo de MPs presentes na nuvem mesh. Como consequência, MPs com o MDA ativado devem ser capazes de interoperar com MPs com o MDA desativado, mesmo que isso prejudique a eficácia do esquema.

A idéia central do MDA é introdução de períodos de tempo, chamados MDAOPs (*MDA Opportunities*), período pelo qual o nó com o MDA ativado tem a oportunidade de acessar o meio com o mínimo de contenção (pode ainda haver contenção devido a presença de nós com o MDA desativado). MDA é implementado através da ação de cinco novos quadros: *MDA Setup Request*, *MDA Setup Reply*, *MDAOP Advertisement Request*, *MDAOP Advertisements*, *MDAOP Set Teardown* [IEEE, 2007].

Controle de congestionamento é brevemente citado na proposta do padrão. Um mecanismo de controle de congestionamento deve ser selecionado para toda a rede e também será anunciado pelo elemento de configuração mesh, junto com o protocolo de seleção de caminho e métrica. O *draft* descreve o formato do quadro de notificação de congestionamento (*Congestion Control Notification*) enviado pelo MP para seu MP par (ou MPs) a fim de indicar seu status de congestionamento. Contudo, detalhes sobre como o congestionamento é detectado ou o que provoca a notificação de congestionamento são considerados além do escopo do futuro padrão.

Economia de energia, por outro lado, recebe maior atenção no *draft*. A idéia principal é que alguns nós escolhidos, chamados de *Power Save Supporting MPs*, irão armazenar quadros de outros nós, chamados de *Power Saving MPs*, e os transmitir

apenas em tempos negociados. Este é um serviço similar ao que um ponto de acesso deve prover aos nós que estão associados a ele nas redes IEEE 802.11.

Em termos de segurança, IEEE 802.11s descreve mecanismos que provêm tanto autenticação e privacidade. A segurança é baseada no mecanismo MSA (*Mesh Security Association*), que garante segurança no enlace entre dois MPs e pode operar mesmo que não haja nenhum autenticador central, isto é, existe suporte para autenticação distribuída.

Uma vez configurado para oferecer segurança, um MP só deve estabelecer *peer links* seguros com outros MPs e renegociar *peer links* pré-existentes que ainda sejam inseguros. O estabelecimento de um *peer link* envolve a troca de quadros extras (como um *four-way handshake*) que começa imediatamente após a troca inicial de quadros *Peer Link Open* e *Peer Link Confirm*.

O padrão IEEE 802.1X [IEEE, 2001] é colocado como núcleo do mecanismo MSA, entretanto chaves PSKs (*Pre-Shared Keys*) também podem ser utilizadas, o que parece viável somente para redes mesh com administração centralizada.

1.5. Um Caso Real: Projeto OLPC

A OLPC (*One Laptop Per Child*) [OLPC, 2008] é uma organização não governamental (ONG) sem fins lucrativos que se propôs a projetar e fornecer computadores, especialmente projetados para fins pedagógicos e de inclusão digital. A OLPC realizou o projeto de um laptop de baixo custo, batizado de XO, que oferece uma interface de comunicação sem fio que implementa o *draft* do futuro padrão IEEE 802.11s. A rede em malha sem fio de nível dois da OLPC consiste em uma implementação simplificada de versões iniciais do *draft*, o que na prática preservou a consistência com a proposta em evolução. O XO foi o primeiro dispositivo a adotar o 802.11s como base para implantação de uma rede sem fio com comunicação em múltiplos saltos implementada na camada MAC. A Figura 1.28 ilustra o laptop XO.



Figura 1.28. Laptop XO

Os laptops foram projetados para uso educacional e para operar em condições encontradas nos países em desenvolvimento. Assim, a resistência mecânica e o baixo consumo de energia, por exemplo, são foram diretivas fundamentais no projeto da OLPC.

A premissa é que os laptops, além de seu emprego em sala de aula e nas demais atividades escolares, farão também parte da vida extra-classe de cada aluno, podendo ser utilizados em suas residências. Por isso, o computador pode servir como instrumento de inclusão digital da família e da comunidade onde está inserida cada criança.

A OLPC prevê a utilização do laptop XO em dois cenários: dentro da escola e na casa do estudante. Em ambos os casos, uma máquina servidora na escola (*School Server*) deverá ser capaz de compartilhar recursos com todos os nós da rede sem fio estendendo a capacidade e utilidade dos XOs. Os servidores da escola podem oferecer vários serviços para os nós da rede como, por exemplo, extensão da memória do XO, ponto de acesso a Internet, *cache*, biblioteca da escola, hospedagem de sites e plataforma para aplicativos como *Instant Messenger* e Voz sobre IP (VoIP).

O cenário, em que alunos estão utilizando o laptop na escola, corresponde a uma rede sem fio densa, onde os alunos associam-se ao ponto de acesso ou chegam a ele através de saltos intermediários para ter acesso à Internet, como ilustrado na Figura 1.29. Os XOs que estão associados ao ponto de acesso funcionam como *gateways* para os outros que não têm acesso direto a ele, o que oferece escalabilidade para a rede.

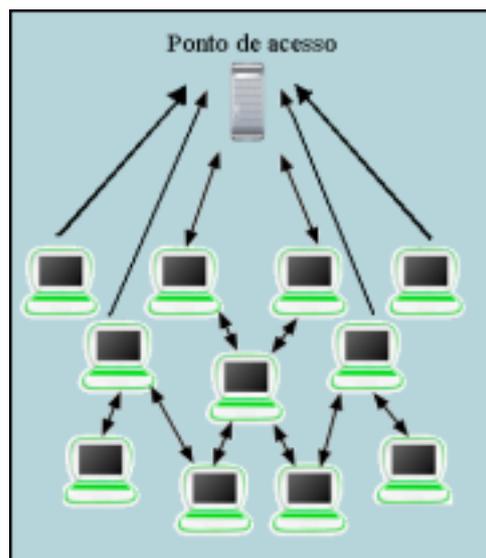


Figura 1.29. Rede sem fio densa (uso dos laptops na escola)

Um ponto de acesso sem fio normalmente não suporta muitos nós associados simultaneamente. Com o uso da topologia densa, cada ponto de acesso associa apenas os XOs mais próximos, e estes podem dar acesso a mais uma gama de outros laptops, possibilitando o aumento de oferta de acesso.

O outro cenário em que a utilização dos laptops é distribuída na comunidade caracteriza uma rede sem fio esparsa. Neste caso, a conectividade pode ser realizada em dois níveis distintos. No primeiro, pode-se permitir a interconexão de XOs presentes na vizinhança através da formação de uma rede ad-hoc. Essa rede permite diversas possibilidades de comunicação entre os participantes, podendo suportar aplicações *peer-to-peer* (P2P) como voz sobre IP, conversações (*chats*) em texto, compartilhamento de conteúdo e aplicativos, dentre outras.

Em um segundo nível, a escola é colocada como ponto de acesso a Internet. A nuvem *mesh* comunitária se conectará a escola e poderá usufruir de seus serviços tais como acesso a conteúdos e aplicativos disponíveis nos servidores da escola e conectividade à Internet. A rede em malha sem fio é, portanto, vista como uma possibilidade de ampliar o alcance dos laptops à rede da escola e, por conseqüência, à Internet. Para permitir a conectividade de XOs mais distantes, antenas externas podem ser instaladas na escola. A Figura 1.30 apresenta o cenário esparso.

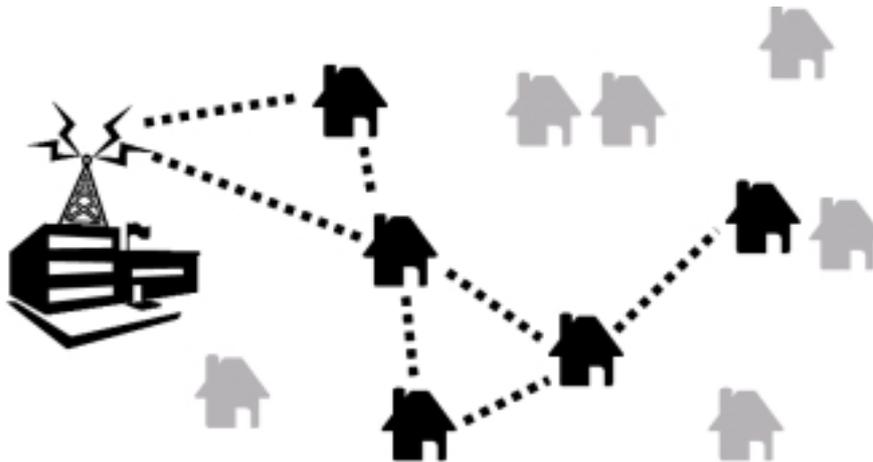


Figura 1.30. Rede sem fio esparsa (uso dos laptops em casa)

1.5.1. A Arquitetura do Laptop XO

O laptop XO possui arquitetura compatível com a plataforma x86. Seus componentes eletrônicos são fabricados em escala industrial, o que permite manter os custos baixos. Além disso, a plataforma x86 é a de mais ampla adoção e a melhor conhecida, o que simplifica a tarefa de desenvolvimento de software.

O laptop já foi desenvolvido nos modelos B1, B2 e B3. O processador do modelo B1 é o AMD Geode GX-500, que foi substituído pelo LX-700 a partir do modelo B3. O XO é equipado com 128 MB de memória no modelo B2-1 e 256 MB nos demais modelos (B1 e nos modelos mais recentes).

O sistema operacional escolhido foi o Linux. Novamente, a escolha vai ao encontro dos objetivos de baixo custo, estabilidade e ampla base de desenvolvedores. O Linux utilizado é baseado na distribuição Fedora Core.

Naturalmente, um *kernel* Linux específico, enxuto e otimizado, foi construído para o XO e a seleção criteriosa de pacotes da distribuição permitiu sua instalação no sistema de arquivos montado sobre um NAND flash de 512 MB (os modelos mais recentes já possuem 1GB de capacidade de armazenamento).

Quando nos referimos ao software do XO, podemos identificar três componentes distintos de *firmware*/BIOS, imagem e *firmware* do rádio. O *firmware* do XO reside em chip *flash* tipo SPI de 1MB, juntamente com a BIOS e informações de identificação da unidade (número serial e outro identificador único, o UUID). A imagem do sistema operacional é a distribuição do GNU/Linux, incluindo o *kernel*, *drivers* e demais componentes a serem instalados no dispositivo de armazenagem do XO (o chip flash do

tipo NAND). Finalmente, o *firmware* do rádio é o componente de software que controla o subsistema de rádio na interface de rede sem fio.

O subsistema de rádio do XO é composto por um chip controlador Marvell 88W8388, que contém um processador ARM9 e memórias RAM e ROM, e um rádio Marvell 88W8015, com interface IEEE 802.11b/g. O sistema de rádio está conectado à CPU principal através de um barramento USB (*Universal Serial Bus*) e continua sendo alimentado de energia mesmo que a CPU principal não esteja. O processamento de quadros MAC é realizado pelo controlador Marvell 8838 e não utiliza a CPU principal, necessária apenas para o processamento de informações de nível de rede e camadas superiores. A Figura 1.31 ilustra a arquitetura do subsistema de rádio do XO.

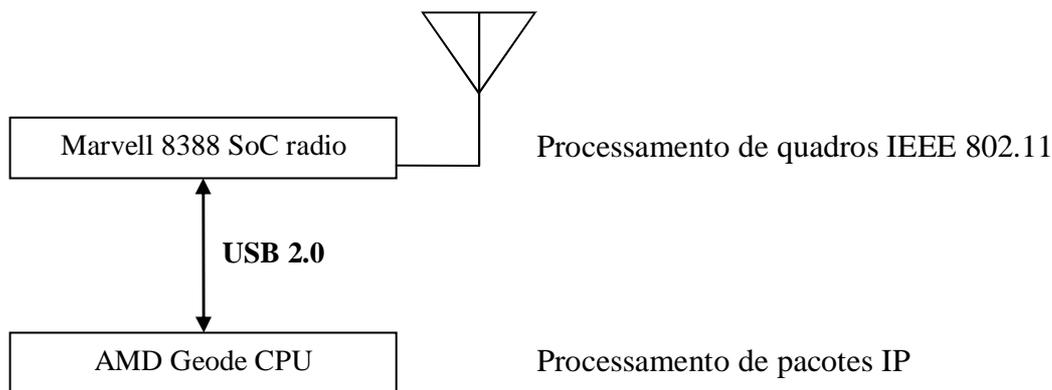


Figura 1.31. Subsistema de rádio do XO

A segregação do subsistema de rádio traz uma vantagem interessante decorrente do fato deste poder operar ainda que a CPU principal se encontre em modo inativo. A possibilidade do SoC implementado pelo Marvell 8838 processar quadros IEEE 802.11 sem a necessidade de intervenção da CPU principal permite que um XO opere como nó intermediário de uma nuvem *mesh* ainda que esteja desligado e com um consumo da ordem de apenas 0,5 watt. A CPU principal é solicitada apenas no processamento de pacotes IP. Portanto, é importante salientar que a implementação do IEEE 802.11s reside no subsistema de rádio e, com isso, um laptop XO pode participar ativamente da rede *mesh* e encaminhar quadros de outros nós da rede mesmo sem o uso da CPU principal ou de uma pilha de protocolos TCP/IP.

Na implementação das funções especificadas pelo *draft* IEEE 802.11s no laptop XO, não há nenhum mecanismo pró-ativo de seleção de caminhos, e apenas a versão reativa, sob-demanda, do HWMP encontra-se implementada. MPPs não são anunciados periodicamente na rede, e portanto MPs devem descobri-los através de buscas por um endereço MAC anycast reservado.

1.5.2. O Projeto RUCA

A OLPC idealizou o uso de seus laptops em escolas de países em desenvolvimento como ferramenta de aprendizado, inclusão social e digital. O Brasil já mostrou interesse na compra de milhões de XOs para serem distribuídos nas escolas públicas. Desta forma, foi lançado o Projeto UCA (Um Computador por Aluno) vinculado à Presidência

da República onde vários centros de Pesquisas estão fazendo o estudo de viabilidade do uso do laptop dentro da escola e na casa do estudante.

O Projeto UCA dividiu-se em diversos projetos paralelos. Alguns centros focaram o aspecto pedagógico, como LSI (Laboratório de Sistemas Integráveis – USP) e o LEC (Laboratório de Estudos Cognitivos - UFRGS) onde foram iniciados os trabalhos de introdução do uso do XO em escolas. Os institutos propõem atividades, desenvolvem softwares educativos, preparam professores, avaliam a adaptação das crianças aos laptops, e o quanto estes estão colaborando para o aprendizado. O LIA (Laboratório de Interação Avançada) da UFSCar (Universidade Federal de São Carlos) também vem desenvolvendo softwares educativos.

Outros projetos dedicam-se a questões mais técnicas. O CERTI (Centros de Referência em Tecnologias Inovadoras) juntamente com o CenPRA (Centro de Pesquisa Renato Archer) trabalham na adaptação do navegador Opera para o XO. O SERPRO (Serviço Federal de Processamento de Dados) está incumbido de realizar testes de hardware e software.

Outra vertente do UCA foi o projeto RUCA (Rede do Projeto Um Computador por Aluno) [Carrano et al., 2007a; Carrano et al., 2007b], administrado pela RNP (Rede Nacional de Pesquisa) e desenvolvido no ano de 2007. Sob a coordenação da Universidade Federal Fluminense (UFF), a Universidade Federal de Brasília (UnB), Universidade de São Paulo (USP), Universidade Federal do Amazonas (UFAM), Universidade Federal da Paraíba (UFPB) e Universidade Federal do Rio Grande do Sul (UFRGS) testaram a interface de rede sem fio dos laptops e sua capacidade de formação de redes de múltiplos saltos no nível MAC nos dois cenários propostos pela OLPC:

- Modo denso – Ambiente de sala de aula, com muitos laptops, como ilustrado na Figura 1.29.
- Modo esparsos – Alunos acessando a Internet de suas casas através do servidor da escola, como ilustrado na Figura 1.30.

O uso concorrente de muitos laptops em um ambiente de alta densidade precisou ser atestado pelo RUCA. E uma grande preocupação do projeto foi saber como um laptop se comporta neste ambiente, onde o nível de interferência é muito alto, e a disputa pelo acesso ao meio pode causar uma significativa degradação na qualidade da rede.

Para que modo esparsos fosse tecnicamente viável era preciso que os laptops (hardware e software) alcançassem determinados níveis de desempenho, em termos de distância, vazão e latência. Em termos práticos, foi preciso determinar se, por exemplo, laptops em casas vizinhas se comunicavam de forma efetiva e a que distância máxima uma criança deveria residir para poder, a partir de seu dispositivo, conectar-se à escola. Estas e outras questões foram respondidas pelo Projeto RUCA.

Os testes realizados no âmbito do projeto RUCA foram divididos em três partes principais: teste de capacidade do laptop, funcionamento do laptop no modo denso e no modo esparsos. A idéia central dos testes foi o levantamento dos limites superiores de operação dos laptops. Para isto foram criadas situações artificiais nas quais se teria o melhor desempenho possível. Por exemplo, para a medição do alcance máximo dos

laptops foi definido como área de testes um local plano de pelo menos um quilômetro de extensão, sem obstruções e sem interferência eletromagnética na faixa de 2.4 GHz, e os laptops foram colocados a 1,20 metros do solo, de forma que o chão não limitasse a zona de Fresnel [Carrano et al., 2007a] nesta faixa de frequência (para distâncias de um quilômetro).

Os testes revelaram que a vazão máxima do XO é limitada a 13 Mbps. Como o XO possui apenas o barramento USB, toda comunicação dos periféricos, inclusive da placa de rede residente na placa mãe, é feita através deste barramento. Apesar da velocidade do barramento USB ser adequada para a taxa máxima da comunicação via rede sem fio IEEE 802.11g, que é de 54 Mbps, a CPU da placa de rede não consegue gerenciar o barramento USB e a comunicação sem fio na taxa máxima, gerando um gargalo. Este gargalo não deve causar problemas, já que 13 Mbps é uma taxa respeitável para uma única máquina, e isto não influencia a comunicação em malha, já que no esquema usado no XO apenas as máquinas de origem e destino fazem o processamento TCP/IP que necessita da CPU principal (e assim requer passagem pelo barramento USB). O encaminhamento dos pacotes nas máquinas intermediárias não requer o uso da CPU principal, e pode ser feito na taxa máxima negociada entre as máquinas, chegando a 54 Mbps se as máquinas estiverem próximas uma da outra.

Os testes em ambientes densos indicaram uma incapacidade dos pontos de acesso de prover comunicação de forma justa para todas as máquinas. Infelizmente, acreditamos que esta seja resultante do padrão de redes sem fio. O método de acesso ao meio CSMA-CA é aleatório, e não justo. Numa condição onde muitas máquinas tentam se comunicar, parte da banda do meio é perdida por colisões. Este tipo de acesso ao meio é bom para redes com baixa utilização, mas tende a ser ineficiente quando a utilização ultrapassa metade da capacidade.

A última série de testes teve por objetivo analisar a rede em malha do XO. Os testes mediram a vazão e latência dependendo do número de saltos. Uma rede em malha no nível de enlace não pode ser muito grande por definição, pois utiliza endereços físicos MAC e não endereços IP, o que impede o agrupamento de endereços nas tabelas de encaminhamento.

Redes em malha que utilizam um único rádio têm restrições de desempenho devido a interferência entre as estações. Enquanto uma estação está transmitindo, as estações que estão na sua área de interferência não podem receber pacotes de outras estações. E a área de interferência é, de modo geral, maior que a área de transmissão. Assim, se estações estão dispostas em uma linha reta, é esperado que o desempenho caia pela metade a cada salto, até que se saia da área de interferência da primeira estação, o que permite então o reuso do canal (transmissão simultânea de dois quadros).

Os testes comprovaram a operação da rede em malha do XO. O encaminhamento de pacotes por estações que não tinham sido configuradas com endereços IP demonstra o uso do encaminhamento em nível de enlace. Devido ao modo usado para o desenvolvimento do software do XO espelhar o modelo de software livre, sendo parte do desenvolvimento feito por voluntários, a UFF acabou tendo um papel importante no desenvolvimento da rede em malha do XO, encontrando várias anomalias que foram sanadas pela OLPC.

Conforme mencionado, redes em malha com um único rádio têm seu desempenho limitado pela impossibilidade de reuso do canal. No entanto, foi observada uma vazão de 2 Mbps em redes com cinco saltos, o que pode ser considerado um bom resultado já que 2 Mbps é mais vazão do que é oferecido pela maior parte das conexões consideradas de banda larga no país atualmente. É interessante notar que os testes foram feitos usando o encaminhamento de nível dois, e isto foi comparado com o roteamento de nível três no mesmo hardware. Na média, como era de se esperar, o encaminhamento de nível dois foi melhor do que o roteamento de nível três, já que neste último caso os pacotes têm que ser enviados da placa de rede para a memória central do XO via USB, enquanto que no primeiro caso isto só acontece nas máquinas de origem e destino.

1.6. Considerações Finais

Dispositivos de comunicação portáteis tais como PDAs, telefones celulares, iPods, entre outros encontram-se atualmente presentes e amplamente difundidos na sociedade mundial. O potencial de comunicação sem fio destes dispositivos será em um futuro próximo responsável por um grande volume de tráfego de dados nas redes metropolitanas.

Apesar da pilha de protocolos TCP/IP ser o padrão de fato em uso em redes convencionais, nem todos os dispositivos de comunicação portáteis são, nem precisam ser, dispositivos IP. Além disso, mesmo com os avanços tecnológicos dos anos recentes, dispositivos móveis ainda são limitados em muitos aspectos. O preço da mobilidade tipicamente implica em reduzidos poder de processamento, armazenamento e memória, principalmente devido a questões de peso e conservação de energia destes.

Com isso, o uso de redes auto-suficientes em termos de encaminhamento de dados no nível 2, ou seja redes do tipo multihop MAC, parece ser bastante atrativo. Estas redes suportam naturalmente dispositivos não-IP, e podem ser implementadas mais facilmente em dispositivos de menor capacidade. Estima-se que seja mais simples e barato implementar as funcionalidades de uma rede em malha nível-2 em uma interface de rede que incluir, no sistema do dispositivo sem fio, a pilha de protocolos TCP/IP sobre os mecanismos de camada 2 convencionais.

Em termos de desempenho, ressalta-se ainda que informações do subsistema de rádio estão naturalmente disponíveis à camada 2. Tais informações são de extrema relevância para redes sem fio onde o canal de comunicação é sujeito a interferências complexas e variações freqüentes. Métricas de qualidade de enlace precisas são vitais para o pleno funcionamento de algoritmos de escolha de melhor caminho. Uma grande dificuldade de protocolos de roteamento de camada 3 é a estimativa acurada da qualidade dos enlaces.

Por essas razões principais, iniciativas de padronização e implementação de redes sem fio com comunicação de múltiplos saltos no nível de enlace, como a proposta do IEEE 802.11s que foi discutida neste capítulo, são de extremo valor e têm potencial para uso prático largamente difundido.

Outra facilidade prevista no futuro padrão IEEE 802.11s é a possibilidade de existência de dispositivos heterogêneos interconectados a rede em malha sem fio, onde os de maior capacidade podem oferecer serviços adicionais ou mesmo auxiliar na

comunicação entre dispositivos de menor capacidade. Pontos de acesso mesh (MAPs) são exemplos de tais dispositivos.

Optando por flexibilizar a composição dos mecanismos da rede mesh, o futuro padrão visa prover interoperabilidade em ambientes heterogêneos e ainda em evolução. Com isso, é especificado um *framework* extensível para seleção de caminhos e para mecanismos de controle de congestionamento, que prevê a existência de diferentes implementações de mecanismos, protocolos e métricas.

A primeira implementação do *draft* do IEEE 802.11s nasceu da iniciativa da ONG *One Laptop Per Child* [OLPC, 2008] através da produção do laptop popular XO. A rede mesh de nível dois da OLPC consiste em uma implementação simplificada de versões iniciais do *draft*, o que na prática preservou a consistência com a proposta em evolução. Na implementação da OLPC, não há nenhum mecanismo pró-ativo de seleção de caminhos, e apenas a versão reativa, sob-demanda, do HWMP encontra-se implementada. Como a implementação do IEEE 802.11s é feita por um subsistema de rádio independente da CPU principal do laptop, o XO pode participar de uma rede em malha mesmo se estiver desligado. Este é um exemplo de dispositivo que não precisa implementar a pilha TCP/IP para oferecer comunicação de múltiplos saltos.

A OLPC tem também desenvolvido antenas ativas que hospedam o mesmo subsistema de rádio do XO. Tais antenas ajudam a melhorar a cobertura de redes mesh e consistem em um interessante exemplo de dispositivo não-IP de comunicação em malha.

Além da implementação do futuro padrão em laptops de baixo custo, como oferecido pela OLPC, uma outra significativa iniciativa de implementação do futuro padrão vem sendo desenvolvida através do Projeto Open802.11s [Open80211s, 2008], cujo objetivo é a criação de uma implementação completamente aberta e gratuita do padrão IEEE 802.11s.

Finalmente é esperado que o padrão IEEE 802.11s seja, através de sua capacidade de encaminhamento de quadros MAC em múltiplos saltos, uma relevante emenda à família de padrões IEEE 802.11.

Referências

- Aguayo, D., Bicket, J., Biswas, S., Judd, G. e Morris, R. (2004). Link-level measurements from an 802.11b mesh network, in ACM SIGCOMM, pp. 121-132.
- Aguayo, D., Bicket, J. e Morris, R. (2005). SrcRR: A high throughput routing protocol for 802.11 mesh networks (DRAFT), Tech. rep., MIT.
- Akyildiz, I. F. e Wang, X. (2005). A survey on wireless mesh networks, IEEE Communications Magazine 43, 9, pp. S23-S30.
- Akyildiz, I. F., Wang, X. e Wang, W. (2005). Wireless mesh networks: A survey, Computer Networks 47, 4, pp. 445-487.
- Bicket, J., Aguayo, D., Biswas, S., e Morris, R. (2005). Architecture and Evaluation of an Unplanned 802.11b Mesh Network, ACM MobiCom.

- Bruno, R., Conti, M. e Gregori, E. (2005). Mesh networks: Commodity multihop ad hoc networks, *IEEE Communications Magazine* 43, 3, pp. 123-131.
- Camp, J. e Knightly, E. (2008). The IEEE 802.11s extended service set mesh networking standard, *IEEE Communications Magazine* (to appear).
- Campista, M. E. M., Esposito, P. M., Moraes, I. M., Costa, L. H. M. K., Duarte, O. C. M. B., Passos, D. G., Albuquerque, C. V. N., Muchaluat-Saade, D. C. and Rubinstein, M. G. (2008). Routing metrics and protocols for wireless mesh networks, *IEEE Network* 22, 1, pp. 6-12.
- Carrano, R., Bletsas, M., Magalhães, L. C. S. (2007a). Mesh Networks for Digital Inclusion - Testing OLPC's XO Mesh Implementation. 8o Fórum Internacional de Software Livre. Anais da Trilha Internacional do Workshop do 8 Fórum Internacional de Software Livre, Porto Alegre, RS.
- Carrano, R., Martins, R., Magalhães, L. C. S. (2007b). The RUCA Project and Digital Inclusion. 5th Latin American Network Operations and Management Symposium – LANOMS 2007, Petrópolis, RJ.
- Cisco Wireless Mesh Networking Solution (2008), <http://www.cisco.com/go/wirelessmesh>.
- Clausen, T., Jacquet, P. (2003). Optimized Link State Routing Protocol (OLSR), IETF RFC 3626.
- Cordeiro, C., Agrawal, D. (2002). Mobile Ad Hoc Networking; Livro texto dos minicursos do Simpósio Brasileiro de Redes de Computadores. Búzios, RJ.
- Couto, D. S. J. D., Aguayo, D., Bicket, J. and Morris, R. (2003). A high-throughput path metric for multi-hop wireless routing, in ACM International Conference on Mobile Computing and Networking (MobiCom), pp. 134-146.
- Draves, R., Padhye, J. e Zill, B. (2004a). Comparison of routing metrics for static multi-hop wireless networks, in ACM SIGCOMM, pp. 133-144.
- Draves, R., Padhye, J. e Zill, B. (2004b). Routing in multi-radio, multi-hop wireless mesh networks, in ACM International Conference on Mobile Computing and Networking (MobiCom), pp. 114-128.
- Faccin, S. M., Wijting, C., Kenck, J. e Damle, A. (2006). Mesh WLAN networks: concept and system design, *IEEE Wireless Communications Magazine* 13(2), pp. 10-17.
- Ho, C., Ramachandran, K., Almeroth, K. C. e Belding-Royer, E. M. (2004). A Scalable Framework for Wireless Network Monitoring, 2nd ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots (WMASH), Philadelphia, PA.
- IEEE (1998). IEEE 802.1d. media access control (MAC) bridges, Standard.
- IEEE (1999). IEEE 802.11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Standard.
- IEEE (2001). IEEE p802.1x.port-based network access control, Standard.

- IEEE (2007). IEEE p802.11s/d1.08, draft amendment to standard IEEE 802.11: ESS mesh networking, work in progress.
- Johnson, D., Maltz, D., e Broch, J. (2001). DSR: the dynamic source routing protocol for multihop wireless ad hoc networks, Ad Hoc Networking, Addison-Wesley Longman Publishing Co., Boston, MA.
- Lad, M., Bhatti, S., Hailes, S. e Kirstein, P. (2005). Enabling Coalition-Based Community Networking, The London Communications Symposium (LCS).
- Muchaluat-Saade, D. C., Albuquerque, C. V. N., Magalhães, L. C. S., Passos, D., Duarte, J., Valle, R. (2007). Redes em Malha: Solução de Baixo Custo para Popularização do Acesso à Internet no Brasil. XXV Simpósio Brasileiro de Telecomunicações – SBRT 2007, Recife, PE.
- Murthy, C. Siva Ram, Manoj B. S. (2004). Ad Hoc Wireless Networks: Architectures and Protocols. 2. ed. New Jersey: Prentice Hall.
- OLPC (2008). One Laptop Per Child project, URL <http://laptop.org/>.
- Open802.11s (2008). Open 802.11s project, URL <http://open80211s.org>.
- Passos, D., Teixeira, D. V., Muchaluat-Saade, D. C., Magalhães, L. C. S. e Albuquerque, C. V. N. (2006). Mesh network performance measurements, in International Information and Telecommunications Technologies Symposium (I2TS), pp. 48-55.
- Perkins, C. E., Belding-Royer, E. M., e Das, S. R. (2003) Ad hoc On-Demand Distance Vector (AODV) Routing. IETF RFC 3561.
- Rad, A. H. M.; Wong, V. W. S. (2007) Partially Overlapped Channel Assignment for Multi-Channel Wireless Mesh Networks. ICC '07. IEEE International Conference on Communications, 2007, pp.3770-3775.
- Ramachandran, K. N., Buddhikot, M. M., Chandranmenon, G., Miller, S., Belding-Royer, E. M. e Almeroth, K. C. (2005). On the design and implementation of infrastructure mesh networks, in IEEE Workshop on Wireless Mesh Networks (WiMesh).
- Roch, S. (2005). Nortel's Wireless Mesh Network solution: Pushing the boundaries of traditional WLAN technology, Nortel Technical Journal, Issue 2. disponível em http://www.nortel.com/solutions/ntj/collateral/ntj2_wireless_mesh.pdf
- Santivanez, C., McDonald, Stavrakakis, Ramanathan (2002). On the Scalability of Ad Hoc Routing Protocols, IEEE INFOCOM, New York, NY, vol. 3, pp. 1688–1697.
- Santivanez, C., Ramanathan, R. (2003). Hazy Sighted Link State (HSLs) Routing: A Scalable Link State Algorithm, BBN Technical Memorandum, No. 1301.
- Stallings, W. (2000) Local and Metropolitan Area Networks, 6a. ed., Prentice Hall.
- Tanenbaum, Andrew. S. (2003) Redes de Computadores. São Paulo: Ed. Campus..
- Tsarpapoulos, N., Kalavros, I. e Lalis, S. (2005). A Low Cost and Simple-to-Deploy Peer-to-Peer Wireless Network based on Open Source LinuxRouters, IEEE First

- International Conference on Testbeds and Research Infrastructures for the DEvelopment of NeTworks and COMmunities (TRIDENTCOM), pp. 92-97.
- Walke, B., Mangold, S., Berlemann, L. (2006). IEEE 802 Wireless Systems – Protocols, Multi-hop Mesh/Relaying, Performance and Spectrum Coexistence, John Wiley & Sons.
- Weber, S., Cahill, V., Clarke, S. e Haahr, M. (2003). Wireless Ad Hoc Network for Dublin: A Large-Scale Ad Hoc Network Test-Bed, ERCIM News, vol. 54.
- WiFiDog (2008), A Captive Portal Suite, <http://dev.wifidog.org>
- Zhang, Y., Luo, J. e Hu, H. (2007). Wireless Mesh Networking Architectures, Protocols and Standards, chap. 12, Wireless Networks and Mobile Communications Series (Auerbach Publications, Taylor & Francis Group), pp. 391-423.