Universidade Federal Fluminense

Jairo Lino Duarte

Escalabilidade, Gerência e Mobilidade para Redes Mesh de Acesso à Internet

NITERÓI

2008

Universidade Federal Fluminense

Jairo Lino Duarte

Escalabilidade, Gerência e Mobilidade para Redes Mesh de Acesso à Internet

Dissertação de **Mestrado** *submetida* ao "Programa de Pós-Graduação em Computação"da Universidade Federal Fluminense como requisito parcial para a obtenção do título de Mestre. Área de concentração: Processamento Paralelo e Distribuído.

Orientador:
Prof. Célio Vinicius Neves Albuquerque, Ph.D.

NITERÓI

2008

Escalabilidade, Gerência e Mobilidade para Redes Mesh de Acesso à Internet

Jairo Lino Duarte

Dissertação de Mestrado submetida ao Programa de Pós-Graduação em Computação da Universidade Federal Fluminense como requisito parcial para a obtenção do título de Mestre. Área de concentração: Processamento Paralelo e Distribuído.

Aprovada por:

Prof. Célio Vinicius Neves Albuquerque, Ph.D. / IC-UFF
(Orientador)

Profa. Débora Christina Muchaluat Saade, D.Sc. /
TET-UFF

Prof. Luís Henrique Maciel Kosmalski Costa, Dr. / UFRJ

Niterói, 28 de Abril de 2008.

A resposta da pergunta “O que veio primeiro, o ovo ou a galinha ?” é bem simples, a galinha [Gênesis 1:20].

We proliferate the world, connected by strands of telephone and network cable. We communicate wirelessly through cellular, satellite and Wi-Fi networks. We collect comics, sports cards, and computers. We modify cars, build models, mix music and build our own toys. We are ravers, gamers, trekkies, programmers and techies. Do not fear us, but instead, embrace us. Listen to those who are passionate and accomplished in their pursuits no matter what they may be. Share your passions with them. There is a little geek in all of us.

What are you geek for?

(Adam & Terry Levinstein)

"Standing on the shoulders of giants"*. Since I know how small I am, my desire is to stand on God's shoulders. Which shoulder are you going to stand on?

(* Isaac Newton)

Agradecimentos

A primazia do meu agradecimento é dada a Deus, o primeiro e o mais importante dos quais me ajudaram até este momento.

Em seguida aos meus pais, que me proveram as condições, mais que necessárias, ao meu sucesso profissional e acadêmico.

Dedico também à minha companheira Juliana, que tanto me ajudou, incluindo a revisão lingüística deste trabalho.

Agradeço ao Professor Célio, o orientador, que fez mais do que o seu papel, durante a minha estadia como mestrando na UFF. Aos professores Débora e Schara agradeço por terem dado vida ao projeto Remesh, que foi a casa agradável onde a minha pesquisa se desenvolveu.

A porta do mestrado foi apresentada, a mim, pelo professor Vinod, durante o meu tempo de graduação, e sem esta contribuição dificilmente teria almejado o mestrado nesta época.

Aos meus colegas do projeto Remesh, como Douglas, Diego, Arthur, Rafael, Bruno, Clayton, agradeço por terem composto uma ótima equipe, certamente todos possuem contribuições nos resultados aqui apresentados. Em especial agradeço ao Douglas, com quem tive diversas conversas inspiradoras e ao Diego, cuja parceria foi de grande importância na realização de todas as atividades do projeto e dos resultados desta dissertação.

Agradeço as instituições que colaboraram no meu mestrado, como UFF, RNP, EATE e FEC.

Para os meus amigos do laboratório de pós-graduação dedico um grande abraço.

Resumo

Rede *mesh* é considerada uma evolução de rede IEEE 802.11, que adiciona alguns novos benefícios, como uma maior área de cobertura pelo uso de múltiplos saltos, e robustez pela capacidade de auto-configuração de rotas. Estes benefícios tornam possível o desenvolvimento de redes de acesso banda larga e de baixo custo. Portanto, rede *mesh* é uma boa opção para iniciativas de inclusão digital. O projeto Remesh, ao construir duas redes de acesso, com usuários da comunidade acadêmica da UFF, enfrentou diversas questões ligadas às áreas de escalabilidade, gerência e mobilidade. Apesar de considerável parte destas questões serem típicas às redes de acesso e às redes sem fio, no contexto de redes *mesh*, estas questões possuem implicações peculiares. Este trabalho tem sua abordagem focada sobre estas implicações e as correspondentes soluções adotadas. As contribuições apresentadas são, a investigação das questões e desenvolvimento de ferramentas de gerência; identificação de uma questão de escalabilidade, e a avaliação de uma nova solução; e a investigação de implicações nas questões de mobilidade.

Abstract

A Mesh network is considered an evolution of IEEE 802.11 type of network, that adds some new benefits, such as greater coverage area by the use of multiple hops, and robustness by the ability to automatically reconfigure its routes. These benefits make possible the development of networks for broadband access at a low cost. Therefore, a mesh network is a good option for initiatives of digital inclusion projects. The Remesh project, which built two access networks, with users from the academic community of UFF, faced several issues related to the areas of scalability, management and mobility. Despite a considerable part of these issues are typical for access networks and wireless networks, in the context of mesh networks, these issues have some peculiar implications. The focus of this work, is related to these issues and their corresponding solutions, for these issues. The main contributions are the investigation of such issues, their implications on mesh networks. The development of tools for management, the identification of a scalability limitation, and the evaluation of a new solution, and the research on mobility issues support over mesh networks.

Palavras-chave

1. Redes *mesh*;
2. Gerência;
3. Mobilidade;
4. Escalabilidade.

Abreviações

OLSR	:	Optimized Link State Routing
DHCP	:	Dynamic Host Configuration Protocol
HIP	:	Host Identity Protocol
SIP	:	Session Initiation Protocol
SNMP	:	Simple Network Management Protocol
HTML	:	Hyper Text Markup Language
HTTP	:	Hyper Text Transfer Protocol
SVG	:	Scalable Vector Graphics
CGI	:	Common Gateway Interface
URL	:	Uniform Resource Locator
CC-GNU GPL	:	Creative Commons GNU General Public License
IEEE	:	Institute of Electrical and Electronic Engineers
NAT	:	Network Address Translation
ISP	:	Internet Service Provider

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

Este trabalho aborda questões de pesquisa e desenvolvimento de redes sem fio no âmbito do Projeto Remesh. Este projeto utilizou redes *mesh* como resposta à questão de oferta de acesso à Internet. Esta questão é pertinente ao problema da popularização do acesso à Internet em várias comunidades brasileiras.

Apesar de no Brasil 99,6% da população possuir acesso à eletricidade, 55,2% à telefonia fixa e 93,1% à televisão em cores, apenas 21,55% tem acesso ao computador e, contudo, do total populacional, apenas 16,0% possuem acesso a Internet [IBGE 2008]. Isso mostra que ainda existe uma grande demanda que não foi atendida pela conectividade a Internet. Alguns fatores contribuem para a exclusão digital na sociedade brasileira, sendo o fator econômico o mais relevante.

Tendo-se em vista os dados estatísticos anteriores, aliados com a razoável suposição de que a telefonia fixa estaria ao alcance de quase todos os que possuem um computador, pode-se possivelmente concluir que todos os computadores poderiam estar conectados à Internet se a rede de telefonia fixa vier a ser utilizada como meio de acesso à Internet. Contudo, ao se analisar a diferença do percentual, entre os usuários que possuem acesso ao computador com os que têm acesso à Internet, resta evidente que existe algum problema com este tipo de acesso. Além da questão de custo necessário para se utilizar tal meio de acesso, um problema que ajuda a explicar o baixo uso está relacionado ao principal motivador do uso da Internet, o consumo de informações. Cada vez mais estas informações são representadas em formatos de tamanhos crescentes, como vídeos, imagens e arquivos diversos. De fato, a evolução do tamanho tem sido de tal modo que o desempenho alcançado, através do acesso discado em linhas telefônicas analógicas, é insuficiente para o consumo adequado das informações, da maneira que são atualmente disponibilizadas. Ou seja, mesmo quando o custo de utilização da telefonia fixa não é um problema, o fraco

desempenho pode ser considerado uma importante barreira.

Soluções de acesso alternativas, com um desempenho melhor do que a telefonia fixa em linhas analógicas, como linhas telefônicas digitais xDSL, redes de TV a cabo ou fibra ótpica possuem custos muito altos para a grande maioria da população. Este cenário faz com que o acesso à Internet com informações complexas seja um privilégio da população de maior renda. Tal cenário provoca a exclusão digital no país, o que em um futuro próximo pode resultar no grande dilema da exclusão sócio-econômica. Com isso, identifica-se a necessidade de criar algo que mude este cenário de exclusão, dando uma solução para o acesso à Internet de bom desempenho e de baixo custo, principalmente para as comunidades que moram em áreas sem infra-estrutura de comunicação adequada.

Redes em malha, ou *mesh*, são redes auto-configuráveis que utilizam comunicação sem fio de múltiplos saltos, formando um *backbone* que interconecta pontos de acesso tipicamente estacionários [Abelém et al. 2007] conectando seus usuários à Internet. Essa descrição de rede *mesh* a identificam como uma rede híbrida, que une conceitos de dois tipos de redes, a saber: o primeiro tipo é a rede infra-estruturada, de topologia fixa e planejada, que tem como meio de comunicação um cabo. Já o segundo tipo é a rede sem fio ad hoc, de topologia dinâmica e espontânea, e uso de comunicação por ondas eletromagnéticas.

Nos últimos anos, essas redes vêm ganhando cada vez mais atenção por parte da comunidade científica. Diversos projetos de pesquisa, geralmente com foco na inclusão digital, têm utilizado uma infra-estrutura em malha para a implantação de redes de acesso [Muchaluat-Saade et al. 2007, Tsarmpopoulos et al. 2005a]. Esta popularidade das chamadas redes *mesh* também é notória em termos comerciais. Grandes empresas do ramo, como Cisco e Nortel, já contam com soluções *mesh* em suas linhas de produtos [Cisco 2006, Roch 2005].

Em outubro de 2005, a Universidade Federal Fluminense,UFF, com o financiamento da Rede Nacional de Ensino e Pesquisa, RNP, criou um grupo de trabalho, chamado de Projeto Remesh, para desenvolver uma rede-protótipo do tipo *mesh*. Em março de 2006 a primeira rede *mesh* de acesso foi implantada em Niterói, RJ, e desde então seus usuários fizeram trafegar aproximadamente um Terabyte de dados. Em 2007 o Projeto Remesh foi multiplicado em três novas redes nas cidades de Brasília, Curitiba e Belém.

1.1 Desafios

O desenvolvimento de redes-protótipo cria novos tipos de problemas e necessidades em diversas áreas, sendo escalabilidade, gerência e mobilidade as três áreas que recebem maior atenção deste trabalho. O foco é dado às áreas mencionadas devido à experiência adquirida pelos administradores e usuários durante a operação da rede-protótipo, por serem as mais perceptíveis. Vale destacar que, no ponto de vista dos administradores, é desejável que a gerência seja a menos trabalhosa e, no ponto de vista dos usuários, a oferta de acesso a banda larga ao conteúdo na Internet e a capacitação de utilizar a Internet em um dispositivo portátil.

Gerenciar uma rede *mesh* cria vários desafios. Uma possível definição de gerenciamento é "O processo de controlar redes complexas de dados a fim de maximizar sua eficiência e produtividade" [Leinwand and Conroy 1996]. Este processo envolve coleta, processamento e análise de dados, assim como correção de problemas. Para realizar tal processo, o gerenciamento de redes pode ser funcionalmente dividido em cinco áreas, que serão denominadas de gerência de falhas, de configuração, de segurança, de desempenho e de contabilidade. Neste trabalho serão tratadas as áreas de configuração, segurança e contabilidade.

Por estas áreas de gerência não serem novas e, portanto, existem um farta quantidade material sobre esse assunto, como as técnicas descritas em artigos publicados e as ferramentas desenvolvidas. Entretanto, ao se iniciar uma busca do conjunto de material disponível com código aberto, verificou-se que as peculiaridades da rede *mesh* não são bem atendidas pelo acervo existente. Estas peculiaridades da rede *mesh* se devem por se tratar de uma rede híbrida e, mesmo sendo resultado da composição de características de outros tipos de redes, essa combinação impede que grande parte do material disponível possa ser utilizado de imediato. Outro fator que dificulta a procura de alguma ferramenta existente, se deve à falta de padronização de suas implementações, inclusive, a maior parte das ferramentas encontradas foram desenvolvidas exclusivamente para um determinada implementação de algum fabricante.

Outra área importante para o sucesso de uma rede sem fio é a mobilidade. Nesse sentido, o avanço dos sistemas de rádio, que melhoram o desempenho e diminuem o tamanho e o consumo de energia, têm possibilitado o desenvolvimento de dispositivos portáteis menores, capazes de trabalharem com informações mais complexas, como vídeos e animações. Tais equipamentos necessitam ter acesso as informações, a fim de serem úteis

a seus usuários. Tendo-se em vista a portabilidade, entende-se que a melhor forma de dar o acesso a informações é por meio de uma rede sem fio, uma vez que apenas dessa maneira tal característica seria plenamente explorada.

Ao se considerar a necessidade de se realizar, continuamente, a troca de dados com dispositivos móveis em uma rede sem fio, cujo alcance de cada ponto de acesso é limitado, impõe-se o uso de alguma técnica que possibilite a troca de pontos de acesso durante o evento da mobilidade. Contudo antes de escolher a técnica, cumpre entender o que é a mobilidade, seus desafios e seus objetivos. Para tal, devem ser definidas algumas questões, como: o nível do protocolo que dará suporte à mobilidade, o tipo de transparência dos problemas de mobilidade e os critérios de desempenho.

Tendo como análise o desenvolvimento das redes-protótipo e, ainda, a conseqüente expansão de suas topologias, já que redes em malha tipicamente estendem o alcance de redes *wifi* tradicionais através de saltos intermediários, foram detectados problemas de escalabilidade que limitavam a capacidade de crescimento da rede, tanto em número de usuários como em tamanho de sua topologia. Embora teoricamente seja possível abranger uma área de cobertura arbitrariamente grande e aumentar o número de usuários, na prática, foi demonstrado [Couto et al. 2003, Passos et al. 2006] que a partir de um determinado número de saltos, a capacidade de comunicação entre dois nós se torna inferior. No caso de uma rede de acesso, usuários localizados a um grande número de saltos do *gateway* ou em regiões com alta densidade de usuários ativos, seriam prejudicados, obtendo uma taxa de vazão consideravelmente inferior ao dos demais. São esses os problemas relativos a escalabilidade.

1.2 Objetivo

Como o Projeto Remesh é um projeto que visa a construir protótipos de redes reais, que se destinam ao uso dos clientes para acesso a Internet, os desafios nas áreas apresentadas de escalabilidade, gerência e mobilidade motivaram a elaboração de diversos trabalhos de pesquisa e desenvolvimento. O objetivo da presente dissertação é descrever as questões e soluções nas três áreas que tiveram a contribuição deste autor.

Conforme citado na seção anterior, não existe um conjunto de ferramentas disponíveis que possam ser imediatamente adaptadas ao trabalho de gerência das redes-protótipos. Desse modo, para o projeto Remesh, uma série de ferramentas criadas ou adaptadas por este autor. Tais ferramentas possuem a finalidade de atender as necessidades diárias do

gerenciamento da rede e, portanto, foram inspiradas ou estendidas de material existente que tivesse alguma similaridade com redes *mesh*, tipicamente as desenvolvidas para redes cabeadas ou para redes sem fio ad hoc.

Para atender as necessidades da área de mobilidade, foi realizado um estudo com fins de investigar soluções para a questão de mobilidade em diversos cenários, que servem para filtrar e classificar técnicas que são avaliadas com mais profundidade em um segundo momento. As técnicas existentes estudadas são amplas em seu modo de abordar o problema, já que as técnicas são implementadas em níveis diferentes, como de rede, de aplicação ou, ainda, um novo nível, que oferecem tipos diferentes de transparência e possuem suporte a diversos tipos de mobilidade.

Um dos objetivos do projeto Remesh, que possui contribuições deste autor, é remover ou atenuar os problemas que possam prejudicar a escalabilidade de rede *mesh* e, para tal, uma solução é apresentada para possibilitar a utilização de múltiplos *gateways* em conjunto com a técnica NAT. A sua implementação e avaliação demonstra a capacidade da solução em uma rede real. Os resultados dos testes de desempenho mostram que a solução DynTun resolve o problema de utilizar múltiplos *gateways* com NAT, permitindo assim aumentar o desempenho e a escalabilidade da rede *mesh*.

1.3 Organização do texto

Inicialmente o Capítulo 2 apresenta uma introdução ao tema, às redes sem fio, às redes em malha e ao Projeto Remesh. No seguinte, Capítulo 3, é descrito com detalhes um problema de escalabilidade, uma solução e a sua avaliação. As questões específicas de gerenciamento para redes *mesh* e as suas soluções são discutidas no Capítulo 4. Sobre a mobilidade de dispositivos em uma rede em malha, o Capítulo 5 esclarece o problema de mobilidade, sendo subdividido em tipos de mobilidade, seus problemas e possíveis soluções existentes, assim como algumas novas propostas para o Projeto Remesh. E finalmente como conclusão, o Capítulo 6 destaca o trabalho feito nas três áreas focadas que são a gerência, a mobilidade e a escalabilidade, assim como a descrição da contribuição do presente autor em cada uma.

Capítulo 2

Redes sem fio e em malha

2.1 Conceitos básicos

O padrão IEEE 802.11 [802.11 2007] pode ser utilizado para a construção de redes WLAN (*Wireless Local Acess Network*) e, por ser popular [Schmidt and Townsend 2003], possui inúmeros fornecedores de soluções, que dentre outros motivos, tornou os dispositivos deste padrão razoavelmente baratos.

As redes sem fio no padrão IEEE 802.11 podem funcionar em dois modos, infra-estruturado e ad hoc. O modo ad hoc, também conhecido como IBSS (*Independent Basic Service Set*), é o mais interessante para este trabalho, pois permite que dois dispositivos comuniquem-se diretamente, sem o uso de um dispositivo intermediário. As redes ad hoc utilizam o modo de mesmo nome. Este tipo de rede é comumente caracterizado por um conjunto de dispositivos que, através de uma conexão sem fio, se unem para estabelecer comunicações do tipo ponto-a-ponto. Nesta união, cada dispositivo pode cooperar com seus vizinhos, para o encaminhamento de mensagens a diversos destinos. Esta cooperação é útil, quando o destino não está ao alcance do rádio do dispositivo de origem. O encaminhamento forma uma rota, através de múltiplos vizinhos, entre os dispositivos de origem e de destino. Esta rota deve ser estabelecida por um protocolo de roteamento que, todavia, não é definido pelo padrão 802.11 e, portanto, a sua escolha é livre. Este protocolo é comumente otimizado para eficiência no consumo de energia e na disponibilidade de rotas alternativas.

Apesar do estabelecimento do padrão IEEE 802.11, a existência de diferenças na implementação do padrão impedia uma boa interoperabilidade entre os dispositivos existentes, o que afetava negativamente na adoção do padrão pelos clientes. Em 1997, empresas como a Lucent, a 3Com, a Aironet (Cisco), a Intersil, a Nokia e a Symbol uniram-se com

o objetivo de garantir a interoperabilidade entre produtos dentro do padrão IEEE 802.11. Esta união resultou na WECA (*Wireless Ethernet Compatibility Alliance*), cujo propósito é de certificar produtos WLAN, para garantir a interoperabilidade. Os equipamentos certificados poderiam ser reconhecidos pelos consumidores através do selo *Wireless Fidelity*, gerando o acrônimo Wi-Fi. Posteriormente a WECA mudou seu nome para Wi-Fi Alliance.

Neste trabalho, os equipamentos utilizados para a formação do *backbone*, que é a infra-estrutura fixa de comunicação, podem ser denominados de ponto de acesso, ponto da infra-estrutura, roteador, ponto, nó, ou *gateway*. Os dispositivos que utilizam esta infra-estrutura, para acessar a Internet, são denominados dispositivos móveis, dispositivos clientes, dispositivos portáteis ou simplesmente clientes. Usualmente os substantivos usuário e administrador são referentes às pessoas. Os termos Wi-Fi, 802.11 e sem fio podem ser considerados sinônimos.

2.2 Redes em malha

Redes em malha [Muchaluat-Saade et al. 2007], ou *mesh*, são redes auto-configuráveis que utilizam comunicação sem fio de múltiplos saltos, formando um *backbone* que interconecta pontos de acesso tipicamente estacionários [Abelém et al. 2007]. Por utilizar pontos estacionários e clientes sem fio, a rede *mesh* pode ser considerada uma rede híbrida. Nos últimos anos, estas redes vêm ganhando cada vez mais atenção por parte da comunidade científica. Diversos projetos de pesquisa, geralmente com foco na inclusão digital, têm utilizado uma infra-estrutura em malha para a implantação de redes de acesso [Tsarmpopoulos et al. 2005a]. Esta popularidade das chamadas redes *mesh* também é notória em termos comerciais. Grandes empresas do ramo, como Cisco e Nortel, já contam com soluções *mesh* em suas linhas de produtos [Cisco 2006, Roch 2005].

O tipo de rede *mesh* pode ser considerada uma evolução do tipo de redes ad hoc, contendo duas diferenças principais. A primeira é que existem dispositivos, dedicados a servir como parte da infra-estrutura de comunicação, onde estes são usualmente fixos e possuem acesso a fontes de energia permanente. A segunda diferença, é que os protocolos de roteamento são otimizados para oferecer a maior largura de banda, pela seleção de rota que recebe a melhor avaliação de desempenho.

Redes *mesh* tipicamente utilizam tecnologias padronizadas Wi-Fi, pois é considerado o padrão mais adotado para a construção de WLAN (*Wireless Local Area Network*),

todavia introduzindo um conceito de malha, com o objetivo de estender o alcance das redes Wi-Fi, pelo uso de múltiplos saltos em uma infra-estrutura. Esta infra-estrutura usualmente é fixa e dedicada à esta função.

2.3 Trabalhos relacionados

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 [Griswold et al. 2004]. Mais recentemente, a tecnologia 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 *mesh* (redes em malha sem fio) [Akyildiz et al. 2005]. Existem vários projetos pilotos de redes *mesh* ao redor do mundo. Exemplos são o RoofNet no MIT [Bicket et al. 2005, Couto et al. 2003], VMesh na Grécia [Tsarmpopoulos et al. 2005b], MeshNet na UCSB [Ho et al. 2004, Ramachandran et al. 2004], CUWin em Urbana [M. Lad and Kirstein 2005], Microsoft Mesh [Draves et al. 2004a, Draves et al. 2004b], Remesh em Niterói [Passos et al. 2006], entre outros [Weber et al. 2003].

Além de projetos acadêmicos, soluções comerciais já aparecem no mercado, oferecidas por grandes empresas, como Nortel [Roch 2005] e Cisco [Cisco 2006], e por pequenas empresas também [Bruno et al. 2005]. Diversos governos estão investindo na construção de cidades digitais usando redes *mesh* sem fio, como em Dublin [Weber et al. 2003], em Taipei onde os produtos da Nortel estão sendo usados e recentemente na cidade histórica de Tiradentes no Brasil, que utiliza a solução ofertada pela Cisco. Uma grande desvantagem dos roteadores mesh comerciais é o seu alto custo, impraticável para usuários finais comuns. A solução Remesh, como as de [Bicket et al. 2005, Tsarmpopoulos et al. 2005b, Ho et al. 2004, M. Lad and Kirstein 2005], é baseada no sistema operacional GNU/Linux, com código aberto e utiliza um roteador programável sem fio e de baixo custo.

Algumas soluções, incluindo as da Microsoft [Draves et al. 2004b], Nortel [Roch 2005] e Cisco [Cisco 2006], usam duas freqüências de transmissão diferentes, normalmente 802.11a em 5GHz para o *backbone* (enlaces entre os roteadores sem fio) e IEEE 802.11b/g em 2.4GHz para os enlaces de acesso (entre pontos de acesso e usuários). Já que no Brasil, a banda de 5Ghz ainda não está totalmente regulamentada, a solução Remesh utiliza somente a banda de 2.4GHz e, como RoofNet e VMesh, usuários finais são conectados aos pontos de acesso *mesh* através de Ethernet cabeada ou acesso Wi-Fi.

Em relação ao protocolo de roteamento, diferentes soluções são escolhidas em cada

projeto. VMesh e Remesh utilizam o protocolo OLSR (*Optimized Link State Routing*) [Clausen and Jacquet 2003b, Clausen and Jacquet 2003a], que é um protocolo de roteamento pró-ativo padronizado pelo IETF. 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. 2004b]. 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. 2004] utiliza o AODV (Ad hoc *On-Demand Distance Vector*) [Perkins et al. 2003], um protocolo reativo padronizado. A solução da Cisco utiliza um protocolo de roteamento proprietário chamado AWP (*Adaptive Wireless Path*) [Cisco 2006] 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 estado de enlace, 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 and Ramanathan 2003].

Os custos dos enlaces sem fio, usados para descoberta das melhoras rotas, podem ser calculados usando a contagem de saltos tradicional [Clausen and Jacquet 2003b], o tempo de ida e volta por salto, retardos entre pares de pacotes [Draves et al. 2004b], 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. 2004b]. A métrica ETX mede dinamicamente a qualidade dos enlaces sem fio e, como é usada pela solução Remesh. 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. O protocolo de roteamento usado por RoofNet escolhe a rota de menor ETT [Bicket et al. 2005]. 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. 2007, Draves et al. 2004a, Draves et al. 2004b]. Na maioria dos trabalhos relacionados, o custo de uma rota com múltiplos saltos é dado pela soma do custo de cada salto no caminho. Alguns autores [Bicket et al. 2005, Couto et al. 2003] afirmam que é melhor selecionar rotas com poucos enlaces sem fio com taxas de perda significativas do que favorecer rotas mais longas, por enlaces de baixa perda. Em testes iniciais foi utilizado essa abordagem, mas o desempenho da rede não foi satisfatório. A métrica ML (do protocolo OLSR-ML) desenvolvida pelo

projeto Remesh, baseada em ETX, mostra que a escolha oposta, ou seja, escolher rotas com enlaces, com taxas de perda menores, também leva a maior vazão, com o benefício adicional de manter as rotas mais estáveis e obter taxas de perda mais baixas.

Todos os trabalhos citados propõem o uso de protocolos de roteamento de nível de Rede para a implementação da rede em malha, entretanto um esforço recente do IEEE 802 está definindo um novo padrão para redes em malha no nível de Enlace, através da futura especificação IEEE 802.11s [802.11s 2006]. Uma implementação da proposta atual (*draft*) está sendo realizada pela OLPC (*One Laptop Per Child*) [OLPC 2005] para uso de redes em malha sem fio para conexão de laptops populares (XOs), no escopo do projeto UCA - Um Computador por Aluno, visando a inclusão digital de crianças em países em desenvolvimento. O Brasil participa do projeto UCA [Ricardo C. Carrano and Magalhães 2007] e o grupo de redes *mesh* da UFF coordenam os testes da rede dos laptops XOs.

2.4 Redes sem fio Comerciais e Comunitárias

Usuários de redes comunitárias sem fio tipicamente compartilham algumas poucas conexões à Internet [Netequality 2006]. Esses usuários podem estar espalhados por uma região urbana e as redes, por sua vez, não requerem muito planejamento para operação e para a implantação de novos pontos, além de não contarem com administração centralizada. De forma contrastante, redes comerciais constroem redes de múltiplos saltos, com pontos instalados em locais selecionados por um processo cuidadoso. Outra diferença é o tipo de antena mais utilizada em cada rede, uma vez que as redes comunitárias priorizam o uso de antenas omnidirecionais, com objetivo de aumentar a área de cobertura, enquanto as redes comerciais utilizam antenas direcionais, procurando criar enlaces de grande desempenho.

Uma visão mais ambiciosa para redes comunitárias sem fio é combinar as melhores características dos dois tipos de redes, onde é possível expandir a rede sem um exaustivo planejamento, mas com o suporte de gerenciamento central, provendo uma cobertura mais ampla e com desempenho de banda larga, considerando os seguintes critérios:

- **Expansão espontânea da rede**. A rede deve ser capaz de operar mesmo quando a topologia é determinada pelo local onde os usuários estão localizados;
- **Uso de antenas omnidirecionais**. Estas antenas aumentam a possibilidade de a rede crescer de modo espontâneo, ou seja, crescer conforme novos usuários ingressem

à rede.

- **Roteamento por múltiplos saltos**. Pois esta forma capacita a rede a cobrir uma maior área;
- **Otimizar o roteamento para maximizar vazão**. Ajustar o roteamento com o objetivo de melhorar a vazão, em uma rede com topologia estável, todavia com mudanças dinâmicas na qualidade dos enlaces.

Na seção seguinte, é descrito o projeto Remesh e a rede com mesmo nome. Esta rede pode ser considerada uma rede comunitária de acesso a Internet.

2.5 Projeto Remesh

Através de uma parceria entre o Instituto de Computação (IC) e o Departamento de Engenharia de Telecomunicações (DET), ambos da UFF, surgiu o projeto denominado Remesh. A principal proposta era a implantação de uma rede de acesso do tipo *mesh* para usuários universitários que residissem nas proximidades de suas universidades. Em particular, o projeto se comprometeu a desenvolver e testar o acesso via rede *mesh* nas comunidades situadas ao redor dos diversos *campi* da UFF.

Além do aspecto científico e tecnológico, o projeto visou a inclusão social e digital através das redes de comunicações das universidades brasileiras. Em particular, grande parte dos universitários da UFF é originalmente de cidades do interior do estado do Rio de Janeiro ou residentes locais de Niterói. Geralmente, a parcela oriunda de outros municípios se agrupa em "repúblicas" de estudantes que não possuem condições de arcar com os altos custos de uma conexão faixa larga tradicional do tipo ADSL ou cabo. O desenvolvimento e implantação de uma rede de acesso faixa larga sem fio do tipo *mesh* torna-se, neste contexto, uma alternativa altamente desejável de acesso de baixo custo para a comunidade universitária da UFF.

O projeto Remesh demonstra a viabilidade de uma rede de acesso universitária de banda larga sem fio. O projeto foi desenvolvido em duas fases. Na fase de desenvolvimento foram estudados e implementados os diversos componentes de um protótipo de roteador para a rede *mesh*. Estes componentes incluem o *hardware* do roteador, o sistema operacional, os algoritmos de roteamento, as antenas e os aplicativos necessários. Nesta fase, os protótipos foram testados nos laboratórios dentro das dependências da própria universidade. A primeira fase também englobou a construção de uma rede protótipo,

Figura 2.1: Arquitetura do projeto Remesh.

interna ao corredor do IC, onde haveria um ambiente relativamente controlado para a instalação dos protótipos. Simulações e análises foram usadas na fase de estudo e investigação, entretanto foi dispensada uma grande ênfase na implementação, desenvolvimento e testes dos diversos componentes de hardware e software do projeto. A segunda fase constituiu-se da formação de um grupo de voluntários, que são os usuários acadêmicos, que utilizam a Internet através da rede de acesso, construída em torno do *campi* da Praia Vermelha da UFF.

A arquitetura proposta, pelo projeto Remesh, para rede de acesso sem fio de banda larga está ilustrada na Figura 2.1.

Os roteadores *mesh* sem fio são instalados no topo dos edifícios ou casas dos usuários da comunidade. Através de conexão Ethernet (IEEE 802.3) ou Wi-Fi (IEEE 802.11), os usuários interligam suas estações pessoais ao roteador de sua residência, e através de uma malha sem fio em múltiplos saltos, os roteadores se comunicam com o(s) *gateways* 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*) [Lenczner 2005] realiza o controle de acesso à rede *mesh*. Somente os usuários cadastrados têm a capacidade de adquirir um acesso à rede, e este acesso, é adquirido por estes usuários depois de um processo de autenticação.

O projeto Remesh utiliza o protocolo OLSR [Clausen and Jacquet 2003b], que é um protocolo de roteamento do tipo estado de enlace, com medição pró-ativa. Este protocolo controla a inundação dos pacotes de controle ao utilizar o conceito de MPR (*MultiPoint Relays*). Este controle limita o número de nós responsáveis pela disseminação de in-

formações de roteamento, a fim de evitar transmissões redundantes. Portanto, cada nó seleciona o seu conjunto de MPRs, que é composto pelos nós responsáveis por encaminhar as informações de roteamento e os dados dos usuários. Cada nó preenche o seu conjunto MPR com o número mínimo de vizinhos, distantes a um salto, necessários para alcançar todos os vizinhos distantes de dois saltos. A implementação do OLSR é capaz de utilizar a métrica de contagem de saltos (*Hop Count*) ou a métrica ETX, para calcular a melhor rota. Contudo, o projeto Remesh desenvolveu uma nova métrica, denominada ML (*Minimum Loss*) [Passos et al. 2006], que seleciona a melhor rota baseados na menor taxa de perda de pacotes, ou seja, rotas em que sejam necessárias uma menor quantidade de retransmissões para que um pacote chegue até o destino.

A solução Remesh possui baixo reduzido e, esta característica, é devida ao custo baixo dos equipamentos necessários para montar a infra-estrutura (*backbone*) de rede de acesso. O custo atual de cada nó *mesh* é inferior a US$ 500, enquanto os seus concorrentes comerciais cobram alguns milhares de dólares por cada nó. O roteador utilizado é o WRT54G, da Linksys. Trata-se de um roteador IEEE 802.11g com 4 MB de memória flash (permanente) e 16 MB de memória RAM. Ele possui uma interface sem fio seguindo o padrão IEEE 802.11b/g e uma interface cabeada Ethernet. A interface cabeada é ligada a um *switch* lógico, que possui cinco portas físicas distintas. Além disso, ele vem equipado com duas antenas omni-direcionais de 2dB de ganho cada uma para explorar a diversidade espacial.

Além de ponto de acesso, ele roteia os clientes ligados a ele tanto pela interface sem fio como pelas suas cinco portas Ethernet presentes. O roteador vem de fábrica com um sistema operacional da própria Linksys que possui uma interface de administração via Web. A adaptação para capacitá-lo a operar como um roteador *mesh* é feita com a instalação do *firmware* modificado pelo Remesh, baseado na distribuição GNU/Linux denominada OpenWRT [OpenWrt 2007].

Para a montagem de cada nó da rede, pronto para ser instalado em ambientes externos, utilizamos ainda os seguintes componentes: caixa hermética, base e haste de ferro galvanizado, antena omni-direcional de 18,5 dBi de ganho ou alternativamente antena direcional de 24 dBi de ganho, dependendo da localização do roteador, cabo RGC 213 de 1m, conectores RP-TNC para ligação do cabo com a saída RF do roteador, conectores N-macho para ligação do cabo com a antena omni-direcional e N-fêmea para ligação com a antena direcional, suporte metálico para fixar a caixa com o roteador na haste, adaptador POE (*Power Over Ethernet*) desenvolvido pelo projeto Remesh. Este POE evita a

passagem de cabo adicional, para levar a energia ao roteador, pois utiliza o cabo de rede UTP, de preferência com capa protetora, para ligação do roteador ao cliente.

2.6 Gerência, Mobilidade e Escalabilidade para redes em malha

O projeto Remesh teve, como maior motivador, o desenvolvimento de uma rede de acesso com algumas características de qualidade, desejáveis pela questão da inclusão digital, como oferta de banda larga, baixo custo (pelo uso de equipamentos IEEE 802.11b/g) e facilidade de administração.

O fruto de diversas pesquisas e conseqüentes desenvolvimentos, que atendem aos critérios, são apresentados neste trabalho.

Inicialmente no Capítulo 3 é descrita uma solução para o problema de escalabilidade de uma rede de acesso *mesh*, com nome DynTun, cuja motivação é a limitação de desempenho que uma rede *mesh* possui ao expandir sua área de cobertura, pois, clientes localizados em posições distantes, em número de saltos necessários até o único *gateway*, possuem uma conectividade à Internet com desempenho muito baixo. Esta limitação determina um limite ao crescimento da rede e, portanto, para que a rede Remesh não tenha sua utilidade severamente reduzida, a solução DynTun é proposta neste trabalho e implantada nas redes do projeto Remesh.

O segundo enfoque deste trabalho, descrito no Capítulo 4, é a área de gerência. Este enfoque é necessário para que a rede de acesso tenha sua qualidade melhorada, especificamente, a facilidade na administração cotidiana. Por ser uma rede de acesso, ferramentas e técnicas devem estar a disposição dos administradores, no evento de algum problema prejudicar a conectividade dos usuários, para que a origem do problema seja rapidamente identificada e as correções sejam imediatamente implantadas.

No Capítulo 5, são discutidas diversas questões sobre o suporte a capacidade de locomoção dos clientes, com seus dispositivos móveis, entre diversas áreas. Com relação à essa capacidade, vale atentar para um importante critério: a locomoção do cliente não deve impedir a conectividade do dispositivo, sendo, no caso de uma rede de acesso, a conectividade com outros dispositivos localizados na Internet. Um conjunto de questões e soluções existentes é apresentado.

Por fim, no Capítulo 6, são apresentadas as contribuições, as conclusões de cada área

abordada e os trabalhos futuros.

Capítulo 3

Escalabilidade de redes mesh

As redes *mesh* tipicamente possuem um maior alcance do que de redes *Wi-Fi* tradicionais, onde um ponto de acesso comunica-se diretamente com seus usuários. Entretanto, elas podem apresentar um gargalo ao estender o alcance, pois embora, teoricamente seja possível abranger uma área de cobertura arbitrariamente grande, na prática foi demonstrado [Couto et al. 2003, Passos et al. 2006] que a vazão obtida na comunicação entre dois pontos da rede degrada em forma exponencial, sendo o número de saltos entre eles a função da degradação. Desta forma, quanto maior a distância mais restrita é a comunicação entre dois pontos. Este gargalo é especialmente prejudicial às redes de acesso, pois seus usuários localizados a um grande número de saltos do *gateway* são prejudicados, uma vez que estes obtêm um desempenho consideravelmente inferior aos usuários mais próximos a um *gateway*.

Uma solução bastante imediata é a adoção de múltiplos *gateways* para a Internet, ou seja, implementar *multi-homing*. Se tais *gateways* forem bem posicionados, atendendo aos demais pontos da rede, de maneira uniforme, o gargalo irá diminuir, esta solução permitirá um crescimento escalável da rede. Define-se *multi-homing* [Guo et al. 2004], neste capítulo, como a utilização de mais de um ponto de conexão com a Internet (*gateway*) em uma rede de acesso.

No entanto, o simples aumento do número de conexões com a Internet não garante a melhora do desempenho. Sem os devidos cuidados, este procedimento pode trazer problemas de conectividade para alguns clientes, fazendo com que suas conexões sejam quebradas constantemente. Tais problemas são decorrentes da utilização da técnica tradicional de NAT [Egevang and Francis 1994] em conjunto com *multi-homing* na mesma rede de acesso.

A rede Remesh enfrentou o supracitado gargalo, sendo assim a motivação para o desen-

volvimento da solução proposta neste capítulo, denominada DynTun (*Dynamic Tunnels*) [Duarte et al. 2008].

A técnica DynTun é uma solução eficiente para o problema de *multi-homing* em redes *mesh* que utilizam a técnica NAT. Esta solução é baseada em criação dinâmica de túneis, marcação lógica de pacotes e políticas de roteamento. Neste capítulo, é apresentada também uma implementação concreta da proposta, que possibilitou a avaliação da solução em duas redes reais. Os resultados dos testes de desempenho mostram que a solução DynTun preserva a semântica das conexões dos usuários e tem o potencial de aumentar o desempenho e a escalabilidade da rede, assim como comprovam que o acréscimo de custo computacional no processamento dos pacotes é bastante baixo.

Apesar do DynTun ter sido desenvolvido para a rede Remesh, os critérios e mecanismos de implementação selecionados são comuns a diversas outras redes de acesso. Portanto, a solução é potencialmente aplicável a outras redes, que enfrentam o conflito entre NAT e *multi-homing*

O texto deste capítulo é organizado da seguinte forma: na Seção 3.1 o problema de violação da semântica das conexões dos usuários é detalhado. Na Seção 3.2 são apresentados alguns critérios utilizados para a definição de uma solução para suporte a *multi-homing*. Na Seção 3.3 são analisadas algumas propostas existentes para este suporte. Na Seção 3.4 a solução DynTun é apresentada em detalhes. Na Seção 3.5 são comentados aspectos de implementação da solução proposta. Finalmente, na Seção 3.6 são exibidos os resultados da avaliação realizada, seguidos pelas considerações finais sobre a escalabilidade de redes *mesh* na Seção 3.7.

3.1 Descrição do problema

Em uma rede *mesh* com mais de um ponto de conexão a Internet, o problema que pode prejudicar os clientes é a quebra das conexões de suas aplicações, que ocorre por causa da interação entre a escolha dinâmica de rotas e a utilização da técnica de NAT. A Figura 3.1 mostra um exemplo do comportamento desejável de um protocolo de roteamento no caso de problemas em um enlace. Nela, a rota, utilizada pelo cliente *mh* inicialmente, é a mais curta em número de saltos (destacada em negrito) até alcançar o *gateway*. Em um dado instante de tempo, ocorre uma falha em um dos enlaces que compõem a rota. Neste instante, o protocolo deve detectar esta falha e alterar o caminho escolhido para uma rota alternativa.

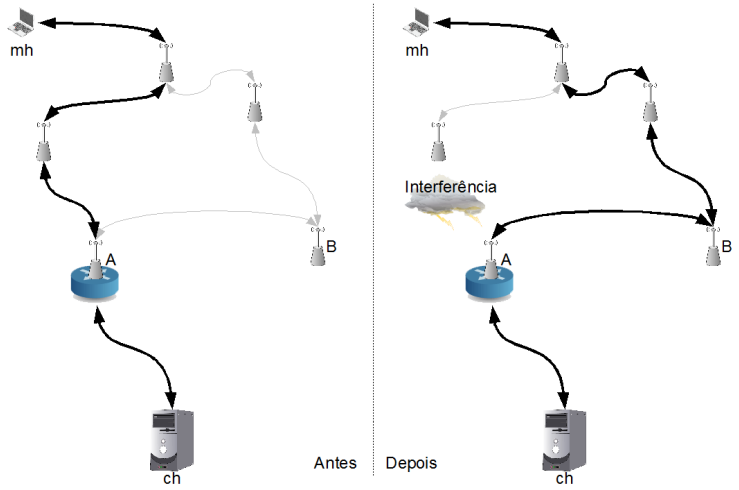


Figura 3.1: Exemplo de uma mudança de rota causada por problemas de conectividade.

Neste cenário, usualmente os efeitos sentidos pelo cliente são uma perda em rajada de alguns pacotes e um potencial breve aumento do atraso fim-a-fim. Isto se deve ao intervalo de tempo necessário para que o protocolo de roteamento perceba o problema e conclua a alteração de rota necessária. Pacotes enviados pelo cliente após a falha do enlace, porém antes do completo estabelecimento de uma rota alternativa, provavelmente serão perdidos. Dependendo do modo de operação do protocolo utilizado e de seus parâmetros de configuração, este intervalo pode durar vários segundos [Engelstad et al. 2004].

A situação ilustrada pela Figura 3.1, entretanto, é válida para uma rede com apenas um *gateway*. Porém, ao analisarmos uma topologia semelhante, mas composta por dois *gateways*, é possível entender o problema potencial. A Figura 3.2 ilustra um cenário muito parecido com o anterior. Agora, no entanto, o ponto B também trabalha como *gateway* para a Internet (e não apenas o ponto A).

Considerando novamente que uma falha ocorrerá em um dos enlaces da rota preferencial (em negrito) nesta última topologia, é razoável supor que o protocolo de roteamento irá agir para contornar o problema, utilizando como nova rota o caminho que passa pelo *gateway* B. Desta forma quando os pacotes de dados chegarem a B eles serão encaminhados para o servidor *ch* com o endereço de B, devido à técnica NAT, e não com o endereço de A como na antiga rota. Ao serem recebidos por *ch*, os pacotes poderão não ser corretamente associados à sua conexão, causando a quebra da comunicação.

Esta quebra de conexão se deve à maneira pela qual o protocolo de transporte TCP (*Transmission Control Protocol*) identifica os fluxos no destino. Uma conexão é identificada pela tupla contendo o endereço de origem, porta de origem, endereço de destino e

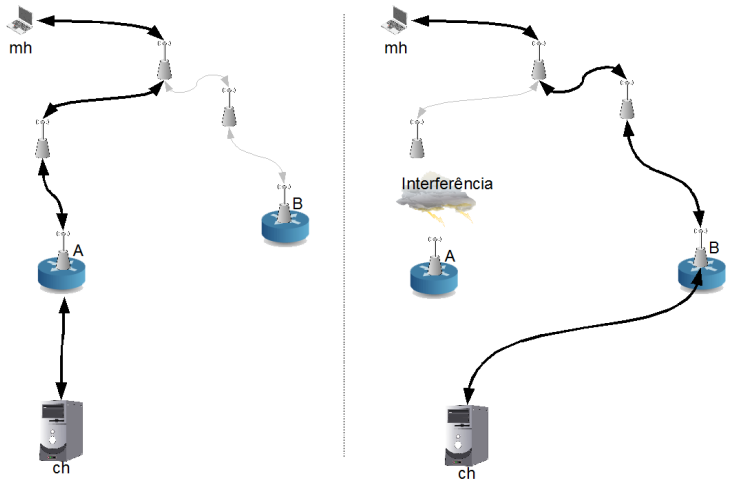


Figura 3.2: Utilização de diversos *gateways* e a técnica NAT em conjunto.

porta de destino. Desta forma, uma vez iniciada uma conexão, o endereço de origem deve se manter fixo. Do contrário, o destino não conseguirá identificar corretamente a conexão, levando à quebra da comunicação, conforme ilustrado na Figura 3.2.

Embora neste exemplo é utilizado o caso em que um enlace apresenta falhas, a troca de *gateways* pelo protocolo de roteamento pode ocorrer pela própria variação da qualidade dos enlaces sem fio.

Isto é especialmente verdadeiro em redes que trabalham com protocolos que realizam medidas ativas na rede. Diversas métricas de roteamento para redes *mesh* sem fio se valem deste expediente, enviando periodicamente pacotes de controle para avaliar a qualidade dos enlaces. Esta qualidade pode ser mensurada pela taxa de perda de pacotes ou atraso nos enlaces [Couto et al. 2003, Koksal and Balakrishnan 2006]. Portanto, em redes pró-ativas, os pacotes de controle do protocolo de roteamento competem com os pacotes de dados dos clientes. Como conseqüência, enlaces possuem a sua avaliação decrescente quanto maior for o nível de utilização pelos clientes.

Pode-se argumentar que uma solução trivial para o problema de conectividade é a não utilização do NAT. Entretanto, existem diversas vantagens técnicas [Ramakrishna 2001] no emprego do NAT, que são importantes diante os critérios descritos na Seção 3.2. Desta forma, a busca ou elaboração de outras soluções, que tornem possível utilizar NAT e *multi-homing*, se fazem necessárias.

3.2 Critérios

Uma boa solução para o problema apresentado na Seção 3.1 deve atender a determinadas restrições. Tais critérios visam garantir a manutenção das características das redes *mesh*, em especial a rede real Remesh. Desta forma, uma solução deve atender as seguintes características:

- **Ser transparente ao cliente**: nenhum componente da solução deve depender da cooperação explícita das aplicações ou protocolos de comunicação utilizados pelo cliente. A solução não deve introduzir novos problemas de desempenho ou interferir na conectividade do cliente. A decisão de usar múltiplos *gateways* em uma rede de acesso com NAT é dos administradores da rede, portanto é a rede de acesso que deve implementar as soluções necessárias.

- **Ter baixo custo**: a solução não deve necessitar de novos elementos de *hardware*. Desta forma, o conjunto de programas, que implementam a solução, deve compartilhar os recursos, dos pontos de acesso, com as demais funções, típicas de redes de acesso.

- **Ser escalável**: a solução não deve consumir recursos da rede em excesso, tanto em termos de banda, quanto em termos de processamento e memória.

- **Ser independente de ISP**: a solução não deve necessitar de suposições de existência de características ou recursos específicos no ISP (*Internet Service Provider*). Todavia deve supor questões impostas pelo ISP, como exemplo, a utilização da técnica *Ingress filtering* [Ferguson and Senie 1998].

- **Ser autônoma e dinâmica**: as decisões necessárias para o bom funcionamento da solução devem ser tomadas sem a necessidade de configurações pré-definidas ou intervenção de um operador humano. Elas devem ser tomadas pela própria solução, baseadas na situação momentânea da rede.

- **Otimizada para redes do tipo *mesh***: Idealmente a solução deve considerar questões típicas às redes *mesh*, como a variabilidade na qualidade dos enlaces.

- **Ser compatível com NAT**: como explicado na Seção 3.1, em geral não é desejável abdicar da utilização do NAT.

- **Ser baseada na camada de aplicação**: uma solução baseada em mecanismos na camada de aplicação tem características interessantes de portabilidade e independência de plataforma. Este interesse é devido ao desejo de facilitar a reutilização do solução em outros tipos de redes.

Todas estas características são levadas em consideração na elaboração da nova solução DynTun, como será apresentado na Seção 3.4. Pois, como descrito na seção a seguir, não foram encontradas soluções existentes que atendam, de forma satisfatória, aos critérios.

3.3 Trabalhos relacionados

O resultado de uma pesquisa bibliográfica é apresentado nesta seção, com o objetivo de demonstrar que o problema, de utilizar simultaneamente as técnicas *multi-homing* e NAT em uma rede *mesh* de acesso, é atual e ainda permanece em aberto.

Em redes que possuem endereços IP públicos independentes dos seus provedores de Internet (ISP), o balanceamento de carga por *multi-homing* pode ser obtido pela técnica de "BGP peering" [Bates and Rekhter 1998, Cisco 2006, RouteScience 2007]. Esta técnica, no entanto, requer que a rede de acesso possua uma identificação de sistema autônomo (*AS number*), além de requerer acordos de *peering* com os seus provedores, e o conseqüente gerenciamento necessário das tabelas BGP. Estes requisitos são perfeitamente adequados para grandes corporações, que são capazes de ter equipes e equipamentos especializados.

Contudo, em redes que utilizam endereços associados aos seus provedores de Internet (ISP), podem obter o balanceamento de carga pelo uso da técnica NAT. Algumas soluções comerciais [Radware 2007, Networks 2007a, Networks 2007b, Rether 2007, FatPipe 2007] utilizam mecanismos embarcados em equipamentos. Assim, a adoção de uma solução neste estilo forçaria a compra destes equipamentos, que por serem proprietários, não permitem a realização de adaptações aos critérios da rede Remesh.

As questões de custos monetários, em utilizar um enlace com cada ISP, levantadas por Goldenberg et al. [Goldenberg et al. 2004] são interessantes. Entretanto, nas redes *mesh* de acesso sem fio, o desempenho é a principal motivação, levando as otimizações relacionadas ao custo ou ao balanceamento de carga nos pontos de acesso para segundo plano.

Um estudo realizado por Akella et al. [Akella et al. 2003] quantifica o potencial benefício de desempenho trazido pelo uso de *multi-homing* pela análise de históricos de

tráfego da Internet. A conclusão dos testes apresentados é que o uso de múltiplos *gateways* pode melhorar em até 25% o desempenho em redes com dois provedores de acesso, e que boa parte desta melhora pode ser obtida com até quatro provedores. Contudo, este estudo foi realizado em uma rede com infra-estrutura de comunicação por cabo, que apresenta importantes diferenças no desempenho se comparada às redes sem fio. Entretanto, mesmo que os resultados apresentados possam não ser totalmente aplicáveis às redes *mesh* sem fio, servem como estímulo à utilização de *multi-homing*. No caso de uma rede *mesh* é esperado que o ganho de desempenho seja mais dependente da topologia do que o simples quantitativo do número de *gateways*, como é no caso da rede testada no estudo, que é do tipo cabeada.

Nas soluções apresentadas em [Suciu et al. 2005, Kniveton et al. 2002], túneis são criados para um agente permanente (*Home Agent*), o que requer o uso de equipamentos externos à rede com endereços IP fixos. Isto, entretanto, novamente vai de encontro às necessidades de baixo custo das redes *mesh*. Contudo, as soluções propostas ao utilizarem túneis apresentam desejadas qualidades, como a possibilidade do uso de diversos provedores de acesso e o suporte à redundância de forma simplificada.

Na solução apresentada por Shin et al. [Shin et al. 2004], a decisão de selecionar o melhor *gateway* é delegada ao dispositivo cliente. Assim, esta solução não é transparente ao cliente, pois este deve gerenciar o *multi-homing*. Outra questão está na forma conservadora adotada para evitar o problema de utilizar mais de um *gateway* durante uma mesma sessão. Os autores propõem que o mesmo *gateway* seja utilizado para todas as sessões, enquanto houver uma em atividade. Logo, *gateways* alternativos somente podem ser selecionados quando todas as sessões são fechadas.

Uma proposta mais próxima dos critérios apresentados na Seção 3.2 é apresentada em [Engelstad et al. 2004]. Os autores consideram uma rede com características similares às redes *mesh*, uso de NAT nos roteadores e uso de túneis até estes pontos de acesso. Contudo, a solução por ser instalada no dispositivo móvel não é transparente e, não vislumbra a seleção e gerenciamento dos túneis de forma dinâmica.

Nenhuma solução encontrada na pesquisa bibliográfica é plenamente adequada aos critérios da rede Remesh, portanto, a nova solução DynTun foi desenvolvida, contudo, esta nova solução aproveita o conhecimento adquirido na pesquisa realizada.

3.4 A solução DynTun

Como apresentado na Seção 3.1, uma vez aberta uma conexão TCP, os pacotes do cliente não podem chegar ao servidor com outro endereço IP de origem. Desta forma, tendo-se em vista os critérios apresentados na Seção 3.2, fica evidente que existem apenas duas classes de soluções desejáveis para o problema apresentado.

A primeira é composta por soluções em que todos os pacotes dos usuários são encaminhados para fora da rede com um mesmo endereço IP. Uma possível implementação deste método é através da centralização do NAT. Ou seja, o NAT não seria realizado pelos *gateways* da rede *mesh*, mas sim por um roteador central ao qual estes *gateways* estariam conectados. Esta solução ao centralizar a implementação do NAT, entretanto, traz implicações de escalabilidade e tolerância a falhas. Uma outra alternativa, seria fazer uma alteração na técnica de NAT, de forma que os pacotes de uma conexão sempre saiam da rede com o mesmo endereço IP. Em outras palavras, os *gateways* seriam obrigados a "forjar" um endereço IP. Esta solução, no entanto, pode conflitar com políticas de segurança de determinados ISPs, dado que muitos empregam a técnica *Ingress filtering* [Ferguson and Senie 1998]. Esta técnica de filtro verifica se o IP de origem dos pacotes pertence ao conjunto de sub-redes do ISP, com a finalidade de evitar ataques de negação de serviço e falsificação de identidade (*DoS - Denial of Service*).

A segunda classe de soluções engloba aquelas em que cada conexão utiliza apenas um *gateway* durante toda sua duração. A esta classe pertence, por exemplo, a solução apresentada em [Engelstad et al. 2004]. Este tipo de solução é caracterizada pelo uso de túneis, que garantam o envio dos pacotes ao *gateway* selecionado, outra característica deste tipo é de não sofrer dos problemas de escalabilidade enfrentados pelas soluções da primeira classe, adequando-se melhor aos critérios especificados na Seção 3.2. Desta forma, optou-se neste trabalho por seguir os conceitos da segunda classe.

A proposta, denominada DynTun (*Dynamic Tunnels*), consiste de um método no qual ao se iniciar uma nova conexão, seja escolhido um *gateway* pelo ponto ao qual o cliente está conectado, de forma que todos os pacotes referentes àquela conexão sejam encaminhados através deste mesmo *gateway*. Para isso, cada ponto da rede que atende diretamente aos usuários deve criar dinamicamente um túnel até cada *gateway* da rede de acesso. Quando um ponto recebe um pacote de dados oriundo de um dos seus usuários, ele verifica se é um pacote de uma conexão conhecida. No caso do pacote pertencer a uma nova conexão, o melhor *gateway* no momento é escolhido e associado à conexão. Por

outro lado, se o pacote recebido é de uma conexão já existente, ou seja, de uma conexão conhecida, o ponto simplesmente recupera a informação de qual *gateway* está associado àquela conexão. Com esta informação o pacote é encaminhado ao túnel respectivo. É interessante notar que conexões distintas de um mesmo usuário podem ser roteadas por *gateways* diferentes. Assim, o DynTun apresenta o potencial de explorar roteamento por múltiplos caminhos.

O uso de túneis cria uma topologia lógica, ligando cada ponto da rede a cada *gateway* da rede através de um enlace lógico, portanto, criando uma rede *overlay*, ilustrada pela Figura 3.3.

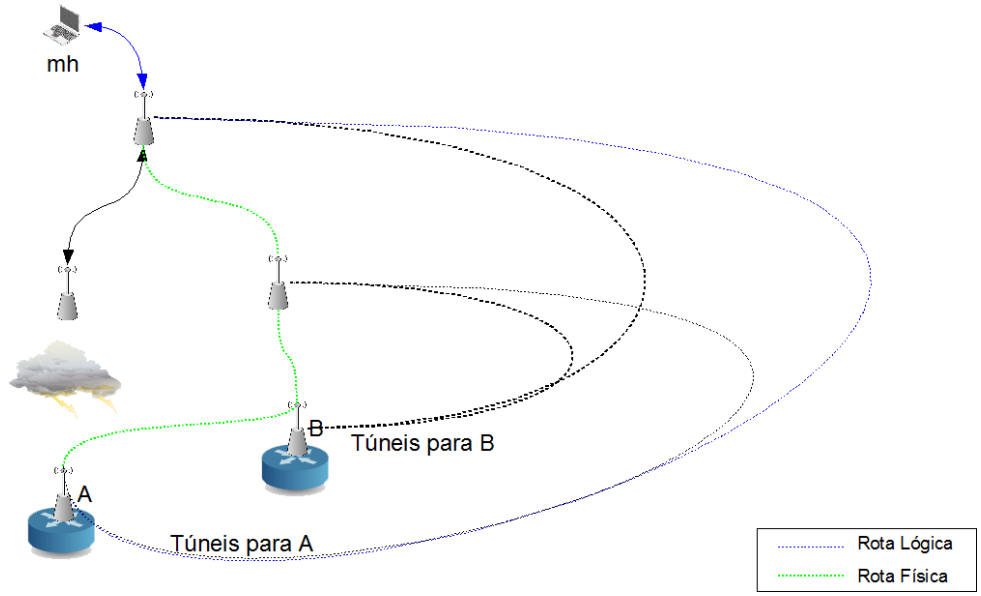


Figura 3.3: Nova topologia lógica, sobreposta a rede real.

A informação dos *gateways* disponíveis pode ser obtida através do protocolo de roteamento. Se o protocolo utilizado for baseado em estado de enlaces, a qualquer momento será possível obter essa informação, pois toda a topologia da rede é conhecida. Se, por outro lado, o protocolo adotado se baseia em vetor de distâncias, pode ser necessária a implementação de um sistema de anúncio de *gateways* [Shin et al. 2004], para que os pontos da rede saibam qual o melhor *gateway* em cada instante de tempo. A seleção do melhor *gateway*, em cada momento, é feita através dos critérios do próprio protocolo de roteamento. No caso da rede Remesh, o protocolo utilizado é o OLSR-ML (*Optimized Link State Routing - Minimum Loss*) [Passos and Albuquerque 2007], baseado em estado de enlaces. Assim, a implementação do sistema de anúncio de *gateways* não foi necessária.

É fácil perceber pela descrição apresentada que os pontos da rede precisam acompanhar o estado das conexões ativas. A princípio, isto pode parecer um problema de

escalabilidade. Na Seção 3.6 serão avaliados os impactos do aumento no processamento. Na Seção 3.5 é explicado como é atendido o critério de baixo consumo de memória da solução. Outra característica imediata é a transparência para os usuários. Toda a solução é implementada apenas nos pontos da rede, não necessitando de quaisquer modificações nos usuários.

Vale destacar que cada conexão tem a possibilidade de escolher o melhor *gateway* no momento de sua abertura. Para conexões de curta duração, existe uma grande probabilidade de que a escolha inicial se mantenha como a melhor durante toda a sua existência. Entretanto, para conexões mais longas, é razoável supor que eventualmente o melhor *gateway* passe a ser outro. Neste caso, o efeito negativo da solução tem um impacto no desempenho obtido, pois pode não manter a condição ótima ao longo de toda a duração da conexão. Este efeito negativo possui uma solução proposta para um trabalho futuro.

Pode-se verificar ainda um efeito colateral interessante. Como citado na Seção 3.1, a utilização de métricas de roteamento ativas por parte dos protocolos pode acentuar o problema de mudança de *gateways*, por causar constantes alterações nas rotas. Por outro lado, com a utilização da solução DynTun, o que ocorre é um balanceamento natural de carga na rede. À medida que conexões são roteadas através de um mesmo *gateway*, os enlaces que compõem a rota até ele receberão uma classificação pior por parte do protocolo de roteamento. Assim, o protocolo poderá eventualmente escolher um *gateway* alternativo, pelo qual as novas conexões serão abertas. Desta forma, um mesmo cliente poderá ter conexões estabelecidas através de vários *gateways* distintos.

3.5 Implementação

Além de propor a solução DynTun, também foi realizada uma implementação, para fins de avaliação e validação da proposta. Esta implementação foi realizada tomando-se por base as redes *mesh* de acesso implantadas pelo projeto Remesh [Muchaluat-Saade et al. 2007, Duarte et al. 2007]. O projeto conta com duas implementações de redes, sendo uma externa, construída ao redor de um dos *campi* da Universidade Federal Fluminense (UFF), e outra interna a um dos prédios da universidade. A rede externa, ilustrada na Figura 3.4, apresenta uma área de cobertura de cerca de 30 km^2, nas vizinhanças do *campus* localizado na cidade de Niterói, enquanto a rede interna (Figura 3.6) interconecta sete salas (como laboratórios e bibliotecas) em dois andares em um prédios da Escola de Engenharia.

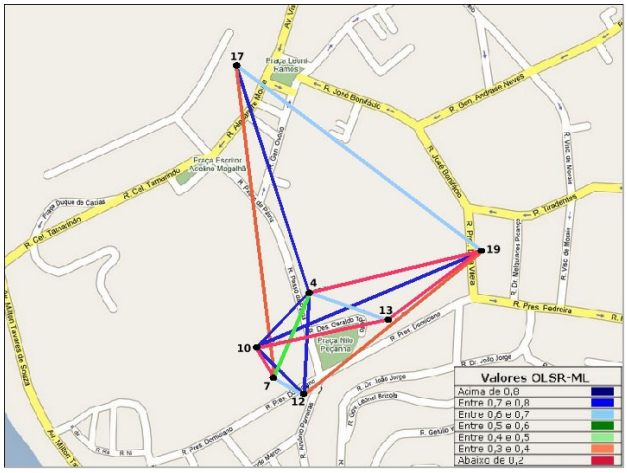


Figura 3.4: Visualização da topologia externa utilizada nos testes.

Em ambas redes de acesso, os pontos são compostos por equipamentos WRT54G do fabricante *Linksys*. Este tipo de *hardware* apresenta grandes restrições de processamento [Broadcom 2008] e memória, sendo assim um bom ambiente de testes para a avaliação do custo computacional da solução.

Optou-se neste trabalho por desenvolver o DynTun como um módulo do protocolo de roteamento OLSR, a partir da implementação de [Tønnesen 2007]. Esta decisão simplificou o processo de obtenção da lista de *gateways* da rede, necessária à solução. Ao integrar a solução ao protocolo de roteamento é atendido o critério de otimizar a solução para redes em malha, pois os dados utilizados na gerência dos túneis são provenientes de cálculos normalmente realizados pelo protocolo OLSR. Mesmo sendo um protocolo de roteamento, o OLSR é implementado na camada de aplicação e, portanto, o DynTun também esta localizado na mesma camada.

Ao ser iniciado, o DynTun carrega os módulos de Kernel (GNU/Linux) necessários, cria um túnel GRE (*Generic Routing Encapsulation*) [Farinacci et al. 2000] e uma interface de rede, que representa a entrada do túnel. Com os seguintes comandos:

```
# Carregar os módulos do kernel necessários
insmod ip_gre.o;
insmod ipt_CONNMARK;
#Criar a interface de rede do Túnel
ip tunnel add  NOME_TUNEL mode gre local ENDERECO_INTERFACE_SEMFIO ;
#Configurar o endereço da interface do túnel
ifconfig NOME_TUNEL ENDERECO_TUNEL netmask MASCARA_REDE ;
```

O túnel utilizado é do tipo NBMA (*Non-Broadcast Multi-Access*). Este tipo tem como característica a ausência de um endereço de destino na sua especificação, por tal cada ponto da rede *mesh* possui apenas uma interface de rede relacionada ao túnel, e este fato melhora a escalabilidade da solução. O destino de cada pacote, tunelado, é definido por uma regra de roteamento. Para os pontos que trabalham como *gateway* a interface do túnel serve como terminação de todos os túneis.

O GRE é um protocolo IP, identificado com o número 47 no cabeçalho dos pacotes IP, desenvolvido pela Cisco para permitir o tunelamento de pacotes, de qualquer protocolo de nível de rede, em uma rede com o protocolo IP. No caso da rede Remesh o tunelamento pode ser chamado de IPoIP (*IP over IP*). A capacidade de encapsulamento é freqüentemente utilizada para o desenvolvimento de redes *overlays* ou para implementar um protocolo de mobilidade. Usualmente o encapsulamento tem o custo de vinte bytes de sobrecarga, que corresponde ao tamanho do cabeçalho do protocolo GRE.

Além do túnel, são criadas algumas regras de marcação de pacotes utilizando o módulo *conntrack* da ferramenta *iptables* [Iptables and NetFilter 2007], freqüentemente encontrado em pontos de acesso baseados em GNU/Linux. Cada conexão dos usuários recebe uma marcação lógica interna ao *kernel* do roteador (ou seja, o conteúdo do pacote não é alterado) que será verificada para determinar o *gateway* utilizado. Estas regras são:

```
#Curto-circuito para não gerenciar pacotes destinados a rede local,
#pois não irão passar pelo NAT. (ex: pacotes já encapsulados pelo túnel)
iptables -A PREROUTING -t mangle --dest 10.0.0.0/8 -j RETURN;

#Retomar a marca do pacote dada a sua conexão, caso exista a marca.
iptables -A PREROUTING -t mangle -j CONNMARK --restore-mark;

#Caso o pacote tenha uma marca, não é necessário realizar mais nada
iptables -A PREROUTING -t mangle -m mark ! --mark 0 -j RETURN;

#Marcar os pacotes que ainda não possuem marcas.
#A marca 0 é para tratar as conexões criadas antes do DynTun ser ativado.
iptables -A PREROUTING -t mangle -j MARK --set-mark 0;

#Salvar a nova marca, para os próximos pacotes da mesma conexão.
iptables -A PREROUTING -t mangle -j CONNMARK --save-mark;
```

Depois da etapa de inicialização, o DynTun entra em um ciclo, que consiste em:

- buscar a lista de todos os *gateways* disponíveis na rede;
- identificar o melhor *gateway* naquele momento e;
- finalmente, alterar a regra de marcação das conexões para utilizar a marca referente ao *gateway* preferencial do momento. Todos os pacotes de uma conexão terão a mesma marca utilizada no primeiro.

Este ciclo tem um baixo impacto de processamento e de memória, pois reutiliza as informações calculadas pelo do protocolo OLSR.

A regra utilizada para alterar a marca para as novas conexão é descrita a seguir:

```
# Substituir a regra atual, que marca as novas conexões,
# para utilizar a marca correspondente ao melhor gateway det. pelo OLSR
iptables -t mangle -R PREROUTING 4 -j MARK --set-mark MARCA_GATEWAY
```

Periodicamente é realizada uma busca na lista completa dos *gateways*, com a finalidade de detectar novos elementos, e para que recursos do sistema (regras de roteamento) sejam liberados quando um *gateway* deixe de integrar a rede. Estes ajustes ajudam o DynTun a atender aos critérios de ser uma solução autônoma, dinâmica e adaptada a redes *mesh*.

O conjunto de regras utilizadas para cadastrar uma rota lógica, que passe pelo túnel, quando um novo *gateway* é detectado, são:

```
#Os pacotes com a marca do gateway serão encaminhados para uma tabela,
# com apenas a regra de roteamento adicionada abaixo
ip rule add fwmark MARCA_GATEWAY table N_SEQ_TAB ;

#Criar uma rota até o gateway, utilizando a interface do túnel.
ip route add default via END_GATEWAY dev NOME_TUNEL onlink table N_SEQ_TAB
```

A Figura 3.5, exemplifica os passos necessários para um pacote, transmitido do dispositivo cliente, ser encaminhado até um determinado *gateway*, no caso o A, e chegar ao servidor destinatário. No passo 1 o pacote é enviado do cliente até o seu primeiro ponto de acesso, no passo 2 o pacote é tratado por uma regra que determina a tabela de roteamento a ser utilizada, no passo 3 a tabela determina o endereço do *gateway* e a interface

de saída, no passo 4 o pacote é reempacotado com um pacote com destino ao *gateway A*, no passo 5 é selecionado o próximo salto, que é determinado pelo protocolo OLSR, nos passos entre 6 e $n-5$ o pacote do túnel é enviado até o *gateway*, no passo $n-4$ o pacote do usuário é desempacotado, no passo $n-3$ é selecionada a rota à Internet, no passo $n-2$ é realizado o NAT e, finalmente no passo n o pacote do usuário é enviado ao destinatário.

Entre os passos 4 e $n-3$ o pacote do usuário é roteado por uma rota virtual, e entre os passos 6 e $n-4$ por uma rota física.

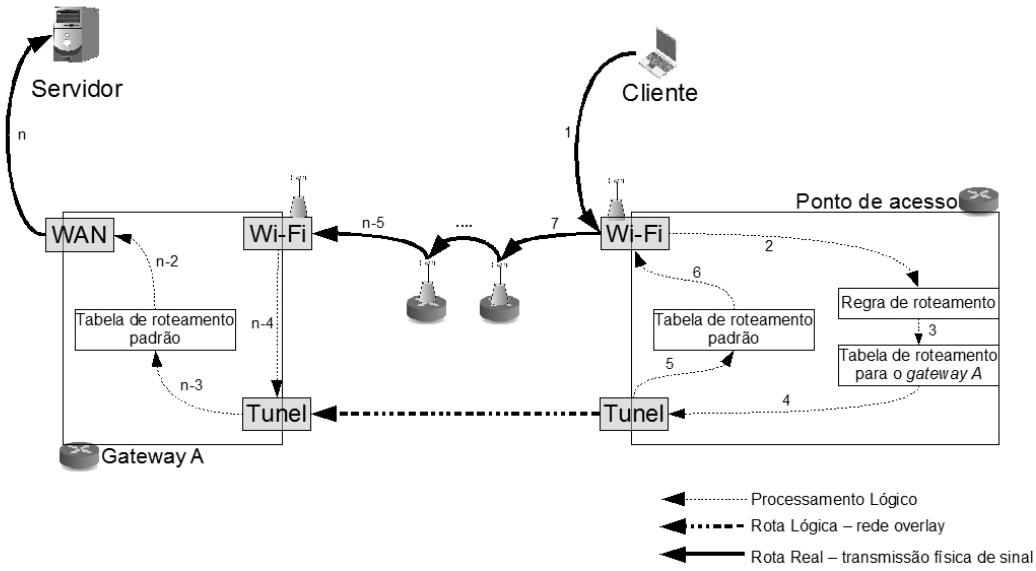


Figura 3.5: Roteamento com DynTun.

As regras apresentadas tiveram como alvo a *chain PREROUTING* do Iptables, que é utilizada no processamento dos pacotes provenientes dos clientes. Contudo, existe um conjunto similar, mas com o alvo a *chain OUTPUT*, que é utilizada para controlar os pacotes originados em processos do próprio ponto de acesso. A necessidade destas regras advém do fato de existirem algumas ferramentas, de gerência, que periodicamente criam conexões aos servidores externos. Este último conjunto foi omitido nesta seção, para evitar repetições.

Com relação ao custo da solução DynTun, três fatores reduzem a sobrecarga nos recursos limitados, de processamento e de memória, dos pontos de acesso.

O primeiro é ligado à lista de *gateways*, pois é extraída durante o usual processamento da topologia, realizado periodicamente pelo protocolo OLSR, ou seja, o módulo reutiliza artefatos produzidos por um processo existente.

O segundo fator é proveniente da solução DynTun utilizar o mecanismo do *conntrack*

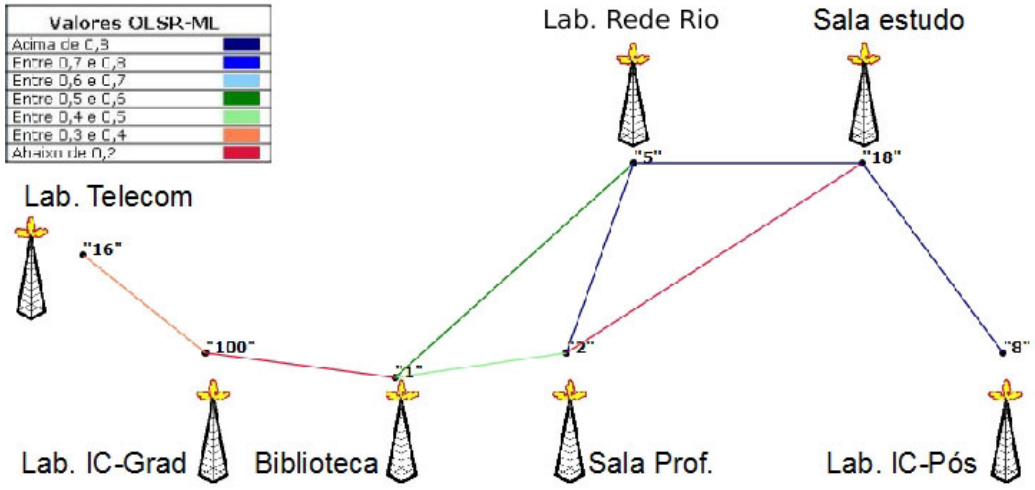


Figura 3.6: Visualização da topologia interna utilizada nos testes.

para a tarefa de classificar os pacotes de todas as conexões, pois esta tarefa é a que tem o maior custo de processamento. O uso do módulo *conntrack* não é considerado uma nova dependência, pois é necessário para outras tarefas já realizadas, como filtros com estado (*statefull firewall*) ou NAT e, portanto, o custo de determinar a qual conexão cada pacote pertence já é imposto por outras tarefas. Outra vantagem é que nenhum novo processo foi adicionado ao fluxo de processamento, que é o componente de roteamento do GNU/Linux. Desta forma, não foi adicionado atraso de processamento aos pacotes.

O terceiro fator, que contribui na redução do custo da solução DynTun, é relacionado às regras para marcação de pacotes. Existe uma regra inicial nos pontos de acesso que classifica, através dos endereços de origem, se os pacotes foram enviados diretamente por algum cliente ou se foram encaminhados por um ponto de acesso vizinho. Apenas os pacotes diretamente originados dos clientes irão passar pelas outras regras necessárias à solução. Portanto, para cada pacote, apenas um ponto de acesso realiza o processamento necessário ao DynTun. Desta forma a distribuição de carga, na gerência das conexões, é espontaneamente dividida de acordo com a distribuição de usuários e seus pontos de acesso.

3.6 Avaliação

Para avaliar o desempenho da solução DynTun, foram realizados testes comparativos em duas redes reais. As topologias utilizadas foram as das redes do projeto Remesh. Ambas apresentam dois pontos com a capacidade de atuarem como *gateways*. As Figuras 3.4 e 3.6 mostram a visão da topologia. Os pontos 7 e 17 representam os *gateways* da topologia

externa, enquanto os pontos 8 e 5 os *gateways* da rede interna. Nas sub-seções seguintes serão apresentados os testes realizados, seguidos dos seus respectivos resultados.

3.6.1 Semântica das conexões

O primeiro teste realizado teve como objetivo verificar a freqüência com que acontecem as quebras de conexões ocasionadas pelos problemas abordados na Seção 3.1. Para tanto, o ponto 18 da topologia interna foi utilizado como origem de vários fluxos de dados TCP em direção a um servidor externo à rede. A opção pelo ponto 18 se deve a expectativa de fluxos criados neste ponto troquem de *gateway* com freqüência. Isto devido a sua proximidade e da semelhança da qualidade dos enlaces dele com cada um dos dois *gateways* disponíveis na rede. Este cenário de um salto foi selecionado por ter a maior expectativa de ocorrência do evento de troca de *gateways*.

O experimento consistiu da abertura de 100 conexões TCP, iniciadas com intervalos de 1 minuto. A duração das conexões foi fixada em 900 segundos, totalizando 114 minutos de teste. A escolha destes parâmetros foi para simular o uso de conexões de aplicações do tipo P2P. Estas conexões possuem características de duração, quantidade de dados transferidos e paralelismo relativamente maiores do que outros tipos de aplicações e, portanto, é o tipo mais susceptível a sofrer quebras.

Ao longo do período testado, foram observados os tempos de duração de cada conexão e eventuais fechamentos causados pela troca de *gateway*. Pôde-se observar que 73 conexões foram concluídas com sucesso, enquanto as outras 27 foram quebradas. O tempo médio de duração das conexões quebradas foi de $178,9$ segundos, com um desvio padrão de 170 segundos. A Tabela 3.1 mostra a distribuição dos tempos de quebra das conexões.

Este resultado mostra a necessidade da utilização de algum esquema de gerenciamento de *multi-homing*, em redes com *multi-homing* e NAT, que preserve a semântica das conexões. Mais de um quarto das conexões foram quebradas ao longo do teste, um número certamente não desprezível. Destas, $33,3\%$ (9 conexões) tiveram duração de menos de 50 segundos. Este único ensaio é suficiênte, pois o objetivo principal é comprovar a ocorrência da quebra de conexões.

Outra possível conclusão deste teste, quando a solução DynTun for implementada, é que um quarto das conexões deixarão de usar o melhor *gateway*, em cada instante de tempo que cada conexão enviou pacotes ao servidor. Este problema constitui o principal ponto negativo da atual proposta do DynTun. Apesar de nenhum teste adicional demonstrar o

Tabela 3.1: Distribuição dos tempos de duração das conexões quebradas.

Intervalo (s)	Ocorrências
0 – 50	9
50 – 100	3
100 – 150	3
150 – 200	2
200 – 250	1
250 – 300	2
300 – 350	2
350 – 400	0
400 – 450	2
450 – 500	1
500 – 550	2

impacto deste ponto, sabe-se que o problema afeta apenas o mesma um quarta parte de conexões.

3.6.2 Aumento da capacidade

Esta sub-seção tem por objetivo avaliar o aumento na capacidade de escoamento do tráfego da rede, com a solução DynTun. Em outras palavras, deseja-se comparar a vazão obtida pelos usuários em conexões com servidores externos com e sem a utilização da solução.

Um novo experimento foi executado na topologia interna, com os pontos 2 e 18 sendo os criadores de conexões. Este experimento foi iniciado com uma medição da vazão de conexões TCP simultâneas, de cada ponto até um servidor localizado fora da rede, utilizando-se apenas o ponto 8 como *gateway*. Uma experiência similar foi realizada, com apenas o ponto 5 como *gateway*. Estes dois testes têm o objetivo de esclarecer a diferença do ganho de desempenho obtido por realocar o *gateway* para uma melhor posição física, com o ganho obtido pela solução DynTun.

A Tabela 3.2 mostra os resultados médios obtidos. Quando o único *gateway* disponível é o ponto 8, o ponto 2 necessita de três saltos para chegar ao servidor. Isso provoca uma substancial queda na vazão, especialmente no cenário avaliado, pois existe uma concorrência com o ponto 18. Esta concorrência é ainda mais acirrada, pois o ponto 2 depende do ponto 8 como salto intermediário até o servidor. Este teste demonstrou um uso injusto da rede, pois o teste demonstrou evidências de que o ponto 18 priorizou a própria conexão, em detrimento da conexão do ponto 2.

Por outro lado, na experiência seguinte, quando ponto 5 opera como único *gateway*,

Tabela 3.2: Vazão obtida na rede interna em cada um dos três cenários (em Mbps).

	Gateway 5 apenas	*Gateway* 8 apenas	DynTun
ponto 2	3,88	0,22	4,51
ponto 18	3,12	4,66	2,97
Agregado	7,00	4,88	7,48

os usuários (2 e 18) estão igualmente próximos ao *gateway*, permitindo uma competição no uso da rede mais justa e, portanto, ambos obtiveram bons resultados.

Quando os dois *gateways* são utilizados com a solução DynTun, cada fluxo TCP pôde ser encaminhado por um *gateway* diferente. Isto permitiu um aumento de cerca de 7% na vazão agregada obtida. É notavel perceber também que houve um aumento superior a vinte vezes na vazão obtida pelo ponto 2, em relação à situação em que apenas o ponto 8 foi utilizado como *gateway*. Ou seja, a solução DynTun permitiu um ganho maior do que é possível alcançar, apenas reposicionando o *gateway*. Este resultado é especialmente importante para redes de acesso sem fio, pois nem sempre é possível realocar o *gateway*.

Em um terceiro experimento, realizado na rede externa, um fluxo TCP de 20 minutos foi iniciado e, 10 minutos depois, enquanto a primeira conexão ainda estava ativa, um segundo fluxo foi criado. Ambos tiveram a mesma origem (o ponto 4 da topologia) e o mesmo destino (um servidor fora da rede). Entretanto, quando este experimento foi executado na rede com a solução DynTun (ou seja, com dois *gateways*), a primeira conexão foi aberta através ponto 7, enquanto a segunda foi forçada a utilizar o ponto 17 como *gateway*. A Figura 3.7 mostra os resultados obtidos.

Este experimento foi repetido 16 vezes, totalizando 8 horas de teste para cada cenário (com um *gateway* ou dois). Desta forma, o gráfico da Figura 3.7 mostra os resultados agregados dos fluxos 1 e 2 em cada cenário. Em ambos os casos, foi considerado o desvio padrão dos experimentos.

Os testes realizados na rede externa, como este último, têm uma duração mais longa, se comparada a rede interna, pois a externa possui uma maior variação na qualidade de seus enlaces, por diversos motivos como a interferência e a maior distância entre os pontos e, portanto, para diminuir o efeito destas variações nas conclusões do teste é necessário alongar a duração e aumentar o número de repetição dos testes.

Durante este teste houve uma clara tendência de aumento na capacidade da rede, quando dois *gateways* foram utilizados. Pode-se notar também que a variação verificada no cenário com dois *gateways* é consideravelmente menor em relação ao experimento com

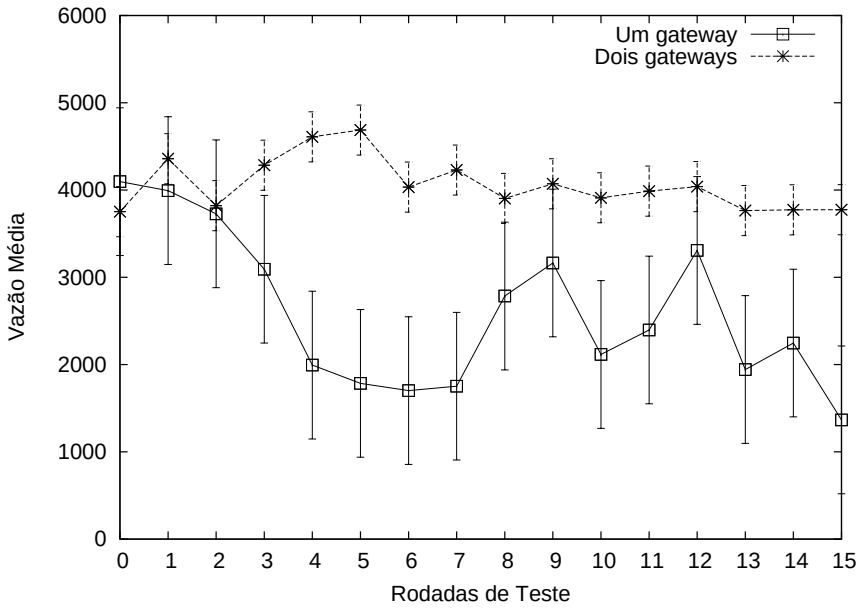


Figura 3.7: Vazão agregada de saída da rede utilizando um e dois *gateways*.

apenas um *gateway*. A Tabela 3.3 mostra os valores exatos de máximo, mínimo, média e desvio padrão dos pontos plotados na Figura 3.7.

Tabela 3.3: Máximo, mínimo, média e desvio padrão dos cenários (todos em Kbps).

Cenário	Máximo	Mínimo	Média	Desvio Padrão
Um gateway	4096	1366	2591,25	846,30
Dois gateways (DynTun)	4687	3752	4062,31	287,05

Os valores máximos foram relativamente próximos nos dois cenários, com uma diferença de menos de 600 Kbps. Entretanto, as diferenças entre os valores de mínimo (2386 Kbps) e média (1471, 06 Kbps) foram bastante acentuadas. Como efeito, o desvio padrão da amostra do cenário com dois *gateways* foi quase três vezes menor do que no cenário com apenas um *gateway*. Estes valores se apresentam como um indicativo de melhora no escoamento do tráfego da rede tanto em termos de banda oferecida (na média, o teste apontou uma melhora de 56, 77%), quanto em relação à estabilidade da mesma.

3.6.3 Impacto no desempenho da rede

Na Seção 3.4 foi discutido, de forma teórica, o impacto da solução DynTun no processamento. O requisito, imposto aos pontos, de rastrear o estado das conexões de seus

usuários poderia, a princípio, ter um custo de processamento, e como conseqüência, diminuir o desempenho da rede.

Com a finalidade de avaliar, de maneira prática, o real impacto da solução no desempenho da rede, foram realizados dois experimentos semelhantes, que avaliam o desempenho relativo à taxa de transmissão. No primeiro, um fluxo de dados TCP foi enviado a partir do ponto 4 da topologia até um servidor, localizado fora da rede. Para este teste, o ponto 17 foi desativado, fazendo com que a rede contasse com apenas um *gateway* (o ponto 7). Neste cenário, o experimento foi realizado com e sem a implementação do DynTun. Os resultados obtidos podem ser vistos no gráfico da Figura 3.8a. A média é referente a 12 repetições de 5 minutos para cada série.

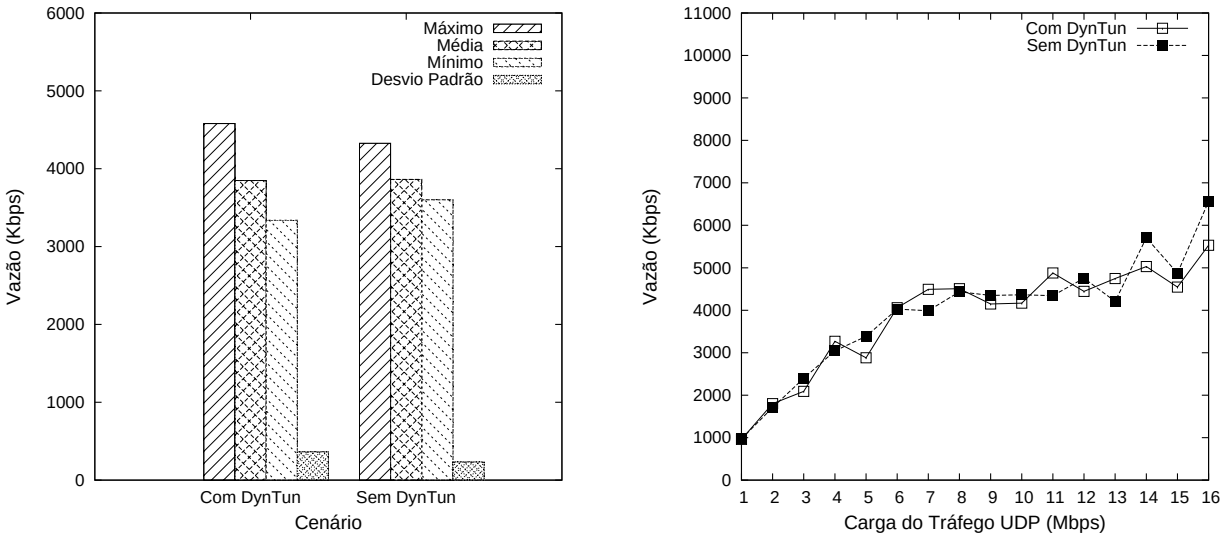
Claramente a utilização do DynTun não afetou o desempenho neste cenário. Em ambas as situações, as médias foram bastante próximas com uma ligeira desvantagem para o cenário em que a solução foi utilizada. Ao se considerar o desvio padrão das medidas, pode-se dizer que o impacto foi desprezível.

No segundo experimento, ao invés de utilizar fluxos TCP, optou-se por utilizar fluxos UDP, variando a taxa de transmissão de 1Mbps a 16Mbps. Neste caso, novamente os experimentos tiveram 5 minutos de duração, porém foram realizados apenas uma vez. A Figura 3.8b resume os resultados.

Novamente os dois cenários obtiveram resultados bastante próximos para todas as taxas avaliadas. Isso demonstra que, embora a solução proposta provoque um aumento no processamento realizado nos pontos de acesso, na topologia avaliada, este impacto não foi significativo diante do desempenho do canal de comunicação. Vale ressaltar ainda que as capacidades do *hardware* dos pontos de acesso utilizados neste experimento são bastante limitadas. O *clock* do processador é de 216 MHz e a memória RAM disponível é de apenas 16MB, valores bastante limitados.

3.7 Conclusão do capítulo

Para permitir um crescimento incremental, redes *mesh* podem utilizar a técnica *multi-homing*. Esta técnica contribui para combater a queda de desempenho, causada pelo aumento no número de saltos entre os usuários e um *gateway*. Como demonstrado no primeiro teste na Seção 3.6, a simples combinação das técnicas de *multi-homing* e NAT pode prejudicar os usuários. Tal prejuízo decorre da quebra de uma grande quantidade



(a) Fluxos TCP **(b) Fluxos UDP**

Figura 3.8: Demonstração do baixo impacto da solução sobre diferentes fluxos de dados.

das conexões dos usuários. Tal efeito negativo certamente prejudica a qualidade da rede percebida pelo usuário. Portanto, é requerido um mecanismo que evite este problema.

A solução DynTun é uma implementação real e funcional, que resolve o problema da interação entre as técnicas de *multi-homing* e NAT, preservando a semântica das conexões dos usuários. Apesar do DynTun ter como foco evitar as quebras nas conexões, os testes da Seção 3.6.2 demonstraram um real aumento na capacidade da rede, tanto no quesito banda agregada de seus usuários, quanto no significativo aumento, em uma ordem de magnitude, da taxa da vazão das conexões dos usuários que anteriormente se encontravam a mais saltos dos *gateways*.

As Seções 3.4 e 3.5 possuem vários itens que levantam a suspeita de que o DynTun poderia impactar negativamente no desempenho da rede, devido ao processamento adicional necessário ao gerenciamento dos túneis. Contudo, os dois últimos testes demonstraram o baixo impacto do DynTun no desempenho da rede.

A implementação do DynTun, apesar de ser moldada à rede Remesh, é também aplicável a outras redes, pois os critérios adotados são tão restritivos que facilitam sua adaptação às características de outras redes. Os dois itens que podem precisar de adaptação são a descoberta de *gateways* e a medição da qualidade das rotas.

Alguns trabalhos futuros incluem considerar a capacidade e carga de utilização de cada

gateway; oferecer suporte a *QoS*; evitar que conexões de uma mesma aplicação sejam tuneladas para *gateways* distintos, por causa de restrições que algumas aplicações possuem; investigar se o DynTun pode ser modificado para suportar à mobilidade do dispositivo cliente; adicionar mecanismos de criptografia nos túneis, com o objetivo de proteger os dados dos usuários e como último trabalho futuro, criar túneis que passem um por um *gateway* intermediário, com a finalidade de diminuir o uso de enlaces sem fio da rede *mesh*, ao utilizar o *backbone* cabeado que interconecta os *gateways*. Esta última modificação resolve o efeito negativo, da atual implementação, causado pela não utilização do melhor *gateway* em cada instante de tempo da vida de uma conexão. Portanto, esta modificação possui o potencial de melhorar, ainda mais, o aumento da capacidade, demonstrada pela Seção 3.6.2.

Este capítulo tratou de uma solução para área de escalabilidade, bem como apresentou uma solução que permite às redes *mesh* expandirem as suas topologias e, portanto, estenderem a sua área de cobertura. Este crescimento, com a solução, pode ter seu desempenho melhorado com o uso de *multi-homing*, mesmo quando o uso de NAT é desejável. No próximo capítulo será abordada a área de gerência, que é um tópico de relevância para as redes *mesh* que possuem uma topologia extensa.

Capítulo 4

Gerenciamento em redes mesh

Neste capítulo, são descritas inicialmente na Seção 4.1 algumas questões de gerência comuns em redes *mesh*. A partir de experiência do projeto Remesh, na Seção 4.2 são apresentadas algumas questões e suas soluções. Por fim, a Seção 4.3 sumariza os pontos abordados neste capítulo.

4.1 Questões de gerenciamento de redes *mesh*

O gerenciamento de redes *mesh* é uma tarefa significativamente mais complexa do que controlar redes com infra-estrutura cabeada, e também é diferente de gerenciar redes puramente do tipo ad hoc. A rede *mesh* por ser um tipo híbrido de rede, com atributos de redes infra-estruturadas e ad hoc, não é idealmente atendida por ferramentas existentes, pois estas são usualmente desenvolvidas frente a um conjunto de premissas pertencentes ao tipo de rede infra-estruturadas ou do tipo ad hoc. Como breves exemplos destas diferenças de atributos, as redes infra-estruturadas possuem topologia estaveis ou com enlaces de desempenho previsível, por outro lado, as redes ad hoc possuem forte limitação no fornecimento de energia e limitações ao acesso de infra-estrutura fixa. A seguir são destacadas algumas questões que dificultam a gerência de redes *mesh*.

Diferentemente de redes cabeadas, não existem padrões públicos e abertos, que tenham um número significativo de fornecedores. Como conseqüência, não existe uma grande quantidade de ferramentas voltadas para redes *mesh*. As ferramentas encontradas, são usualmente desenvolvidas pelo fornecedor de uma solução *mesh*, que é específica a sua implementação. Outro fator negativo, é que estas ferramentas, específicas a um fornecedor, não possuem código aberto, ou uma licença livre que permita a realização de adaptações necessárias a outras redes.

Um importante problema em redes *mesh*, relacionado ao processo de coleta de dados, é a sobrecarga (*overhead*) [Wenli Chen 1999][Badonnel et al. 2005]. Redes que utilizam enlaces segundo o padrão IEEE 802.11 [802.11 2007], possuem uma limitada largura de banda, que pode sofrer grandes variações e, portanto, as mensagens de gerência não devem consumir uma porção significativa do meio de comunicação, em qualquer momento.

A solução mais simplista para extrair as informações da rede, considerando que as ferramentas de gerência serão implementadas ao nível de aplicação, é acessar individualmente cada ponto da rede e, assim, recolher os dados desejados. Esta técnica pode resultar em uma utilização ineficiente dos recursos de comunicação da rede, levando a uma grande sobrecarga. A quantificação deste impacto negativo da troca de mensagens, ou seja, a sobrecarga, é difícil de predizer ou controlar, pois a qualidade dos enlaces de comunicação pode variar rapidamente. Portanto, simplesmente impor um limite de vazão e no tamanho das mensagens pode não ser razoável.

Outra solução, baseada no posicionamento de sondas passivas, que realizem o monitoramento, não pode ser considerada uma técnica adequada para redes de múltiplos saltos. Como exemplo, em uma rede Wi-Fi tradicional, é possível colocar uma sonda próxima ao ponto de acesso, pois este ponto de acesso comunica-se diretamente com todos seus clientes, portanto, a sonda seria capaz de coletar todas as informações relevantes de tráfego, ao monitorar o meio de comunicação sem fio. Contudo se este posicionamento for utilizado em redes de múltiplos saltos, a coleta de informações será parcial, levando a uma observação imprecisa do estado da rede. Isto porque pode não ser possível, a uma sonda passiva, detectar todo o tráfego da rede. Como conseqüência o monitoramento de redes de múltiplos saltos requer uma solução mais abrangente, onde seja possível distribuir as sondas, para coletar as informações do estado da rede e repassar o que foi coletado ao gerente da rede.

Uma rede *mesh* tem como vantagem possuir em sua topologia pontos fixos, que formam uma espinha dorsal (*backbone*), que é a infra-estrutura de comunicação utilizada pelos clientes. Ou seja, a maior parte da comunicação da rede passa por estes equipamentos. Outras características adicionais, destes pontos fixos, como exemplo são: alimentação irrestrita de energia, posicionamento fixo, características técnicas semelhantes e acesso de gerência por um terminal remoto. Estas características os tornam bons candidatos a desempenhar o papel de sonda.

Uma questão que deve ser levantada, para o gerenciamento de redes *mesh*, relativa à tarefa de monitoramento, é a propriedade temporal da informação a ser observada.

Esta propriedade é determinada pelos requisitos de gerência. Por exemplo, a tarefa de visualizar a topologia da rede, em tempo-real, necessita de que as informações sejam processadas em tempo hábil, caso contrário, a representação não será precisa. De forma oposta, um outro exemplo é a tarefa de obter o histórico de estatísticas de algum ponto fixo, que possui uma restrição de tempo muito baixa.

Com o objetivo de atender os requisitos de gerência, os mecanismos que implementam as funções de monitoramento devem responder os seguintes desafios:

- **Dispositivos com recursos limitados**. Os equipamentos que compõem a infraestrutura (*backbone*) da rede *mesh* possuem usualmente recursos limitados. Estes são caracterizados pela baixa capacidade de processamento e limitações de memória. Portanto, se for feita uma alocação inadequada de recursos ao monitoramento, podem ocorrer impactos negativos ao desempenho da rede;

- **Uso, quase exclusivo, do meio de comunicação sem fio**. Com apenas algumas exceções, os enlaces em uma rede *mesh* são feitos por rádio. Este fato determina o tipo de todas as mensagens de gerência, que é o tipo *in-band*. Este tipo é caracterizado pelo fato das mensagens, de controle ou de gerência, utilizarem o mesmo canal de comunicação que os clientes utilizam;

- **Variabilidade da qualidade dos enlaces**. Enlaces sem fio possuem características dinâmicas, como atenuações e interferências do ambiente, que podem resultar em grandes variações na qualidade do enlace. As variações no enlace podem provocar mudanças de rotas, e estas mudanças podem levar à quebra de conexões estabelecidas entre a sonda e o gerente da rede. Estas quebras podem interferir severamente na entrega das informações de monitoramento;

- **Equipamentos posicionados em locais de difícil acesso**. Os pontos fixos da rede, ou *backbone*, podem estar instalados em locais de difícil acesso. Portanto, qualquer interação física com o equipamento pode incorrer em um alto custo financeiro e de tempo.

Para todos os desafios apresentados, alguns objetivos adicionais devem ser considerados no desenvolvimento de ferramentas de gerência, como listado a seguir:

- **Baixa interação com o usuário**; As ferramentas devem simplificar ou reduzir a necessidade da interação com os administradores.

- **Baixa sobrecarga nos meios de comunicação**; As mensagens não devem ser limitadas no tamanho e na taxa, a que são transmitidas.

- **Confiabilidade**; As ferramentas devem ser capazes de realizar a configuração de múltiplos parâmetros, em uma única transação, ou voltar a um estado seguro, caso algo de errado ocorra durante algum processo de configuração.

- **Baixo consumo de memória**; As ferramentas devem depender em um conjunto mínimo de bibliotecas e aplicativos, a fim de minimizar o uso da memória permanente do ponto.

- **Baixo consumo em tempo de execução**; As ferramentas devem ser simples, leves, capazes de operar em baixa prioridade e realizar o mínimo de processamento nas informações, nos pontos da rede com baixa capacidade, com o objetivo de não esgotar a memória principal do ponto com dados de gerência. A importância deste objetivo é conseqüência da motivação econômica, de redução de custos, que simplificam os componentes do ponto ao mínimo razoável.

- **Resistência a falhas**. As ferramentas devem ser capazes de trabalhar com falhas intermitentes de comunicação.

4.1.1 Monitoramento de desempenho

Conforme a rede cresce em tamanho e complexidade, também cresce a necessidade de ferramentas que facilitem a tarefa de gerenciamento. Estas ferramentas podem ser utilizadas na tarefa de monitorar os equipamentos da infra-estrutura ou para acompanhar o nível de utilização do meio de comunicação. Usualmente estas ferramentas, possuem uma interface do tipo WEB, que simplifica o acesso por diversos tipos de equipamentos.

Para a tarefa de monitoramento a ferramenta Ntop [Deri and Suin 2000] foi selecionada. O Ntop é uma ferramenta que pode ser instalada no *gateway* e, neste caso, possui algumas características mais avançadas de monitoramento e análise do tráfego da rede, mostrando por exemplo qual protocolo, endereço de destino ou de origem que gerou maior carga nos enlaces com a Internet, e essas informações, juntamente com um histórico, ajudam a identificar usos abusivos por parte de um cliente ou até mesmo para o planejamento de crescimento da rede.

Esta ferramenta é utilizada em seu estado original, mesmo que este estado possua algumas questões negativas já identificadas, contudo, pelo tamanho das redes desenvolvi-

das estas questões não impõem impactos negativos importantes. Parte das questões são derivadas do método pelo qual esta ferramenta recolhem as informações dos pontos de rede, pois não consideram o impacto sobre o desempenho da rede, nem tão pouco a topologia da rede. Contudo, para redes de escala maiores que as desenvolvidas pelo projeto Remesh, é interessante desenvolver adaptações no mecanismo que agregue as informações nos pontos da rede *mesh* de forma ótima, e os enviem aos servidores que irão efetivamente armazenar, analisar e exibir os resultados aos administradores.

4.1.2 Sistema de controle de acesso

A rede Remesh por ser uma rede de acesso, que provê conectividade à Internet exclusivamente à comunidade acadêmica da UFF, necessita de um sistema de controle, que impeça a sua utilização por pessoas não autorizadas. Visto que, a infra-estrutura de comunicação é desenvolvida com o uso de redes sem fio, segundo o padrão IEEE 802.11, cujo sinal é transmitido por difusão, e portanto, cobrindo uma considerável área geográfica. Esta área é ocupada por diversos tipos de pessoas e, portanto, o sistema de controle deve discernir quais pessoas pertencem a comunidade acadêmica.

Os serviços de autenticação, controle de acesso e estatísticas de acesso dos usuários de rede Remesh são providos pelo sistema Wifidog [Lenczner 2005]. Este sistema é um *captive portal*, licenciado sob a licença CC-GNU GPL, que possui a capacidade de controlar o acesso de forma centralizada, contabilizar de consumo de banda dos usuários, e o mais interessante, não necessita que qualquer componente seja instalado nos dispositivos clientes.

Um *captive portal* é a junção de um sistema dinâmico de *firewall* com um conjunto de páginas HTML. Este sistema bloqueia todo tráfego dos usuários não autenticados, exceto o tráfego do protocolo HTTP que é redirecionado ao portal. Quando o usuário, através da página de *login*, informar a sua identificação, o servidor confere com a base de dados de usuários a autenticidade, e em caso de sucesso, reconfigura o *firewall* para permitir o acesso do usuário autenticado.

Algumas questões surgiram quando o sistema Wifidog foi inicialmente implantado. Esta questão tem como origem o foco dos desenvolvedores originais do Wifidog. A implementação original não suporta a conexão dos clientes por mais de uma interface de rede de um ponto de acesso e nem tão pouco suporta a topologia de múltiplos saltos de uma rede *mesh*. Devido a estas limitações o Wifidog utilizado no projeto Remesh possui algumas modificações [Teixeira 2007].

Como contribuição deste autor foi determinar o impacto, e conseqüentes problemas, que o uso de *multi-homing* tem sobre a arquitetura de autenticação. Também foram realizadas diversas contribuições ligadas à solução dos problemas encontrados, que são a proposta, a implantação, a validação e a implantação nas redes do projeto Remesh.

Esta solução foi necessária, pois com a adição de novos *gateways*, passou a ser necessário que a autenticação ocorra em todos os *gateways* da rede, pois se a topologia modificar-se de tal forma que o protocolo de roteamento escolha um outro *gateway*, o sistema de controle de acesso não deve solicitar uma nova autenticação, pois se o fizer, irá prejudicar gravemente a utilização da rede pelos clientes. Para solucionar tal problema, o servidor de autenticação deve informar, a autenticação do cliente, a todos os *gateways* cadastrados na base de dados, portanto, o usuário móvel, após a primeira autenticação, será pré-autenticado em todos os *gateways* e, assim, estaria prontamente habilitado a acessar a Internet pelo melhor *gateway*.

4.2 Ferramentas específicas do projeto Remesh

Para algumas questões de gerência, peculiares à rede Remesh, não foram encontradas boas ferramentas. Estas questões incluem a visualização da topologia, aquisição e armazenamento de estatísticas, instalação do sistema operacional e reconfiguração de parâmetros de operação. Por não encontrar adequadas ferramentas existentes, quatro novas ferramentas foram desenvolvidas, com o propósito de responder essas questões, que são apresentadas nas sub-seções seguintes.

4.2.1 Instalação da rede

No Projeto Remesh, a primeira ferramenta desenvolvida teve como foco os processos de instalação e configuração do sistema operacional, que é instalado no ponto da rede *mesh*. A instalação de um novo sistema é motivado pela utilização, e pelo projeto de equipamentos desenvolvidos para uso doméstico, cujos sistemas operacionais originais não permitem a instalação das ferramentas necessárias à operação de uma rede *mesh*. O processo de substituição realiza-se pela gravação de uma imagem de sistema, que é um único arquivo, que contém todo o sistema de arquivos. O sistema operacional gravado é o resultado de modificações do sistema OpenWRT [OpenWrt 2007], que por sua vez é um sistema baseado em GNU/Linux, e é voltado para operação em redes Wi-Fi.

Como primeiro passo, uma nova imagem do sistema deve ser compilada por uma

ferramenta, desenvolvida pelo projeto do OpenWRT, chamado *ImageBuild*. Cada arquivo de imagem criado é específico para cada rede e para cada tipo de *hardware* utilizado no ponto de acesso. Um conjunto de ferramentas utilitárias, de autoria do Projeto Remesh, são anexadas a esta imagem durante o processo de compilação. Após esta etapa, a imagem compilada é gravada na memória do ponto, em um estado parcialmente inativo e sem possuir uma identidade do ponto.

A fim de colocar o ponto de acesso em um estado ativo e, assim, servir como parte da infra-estrutura da rede *mesh*, dois programas utilitários, anexados a imagem, podem ser utilizados para a tarefa de configuração inicial. Estas duas ferramentas de configuração, "*Gateway node morph*" e "*Backhaul node morph*", executam diversas alterações nos arquivos configuração do sistema operacional, dando uma identidade única ao ponto em uma rede *mesh* e ativando seus componentes, portanto colocando o ponto de acesso em um estado operacional.

Antes de iniciar a compilação de uma imagem, alguns parâmetros específicos da rede *mesh* são definidos, como endereços IP dos servidores de gerência e "essid" que identifica uma rede sem fio. A identidade do ponto é um identificador único, em uma instância de rede *mesh*, e é o único parâmetro necessário na execução das ferramentas de configuração, dentro de cada ponto. Estas ferramentas operam de forma similar, contudo uma configura o ponto para operar com o papel de *gateway* e a outra configura o ponto a compor a infra-estrutura (*backhaul*).

Estas ferramentas de configuração possuem a desejada qualidade de necessitar de pouca interação com o usuário, pois todos os parâmetros de uma rede *mesh* são informados apenas na compilação da imagem, e esta imagem pode ser reutilizada em todos os pontos da rede, cujos equipamentos sejam similares. Finalmente para concluir a configuração de cada ponto, solicita-se apenas um parâmetro adicional, a identidade. Portanto, a tarefa de configuração pode ser bem realizada com pouco esforço. Outra qualidade interessante é o baixo consumo de memória, pois as ferramentas foram desenvolvidas com o que já é oferecido por padrão no sistema operacional OpenWRT, que são as ferramentas awk, sed, cat e comandos de "shell script" do *shell* ash. Portanto nenhuma biblioteca adicional foi incluída no arquivo de imagem. Estas ferramentas de configuração ainda podem ser apagadas após seu primeiro uso em cada ponto.

4.2.2 Configuração dos equipamentos

Durante a operação diária de uma rede *mesh*, é comum a realização de algumas tarefas em todos os pontos ativos, por exemplo, verificar se um determinado programa está em execução ou modificar um parâmetro da rede. Inicialmente, para realizar tal gerenciamento, era necessário acessar cada ponto, informando seu endereço IP, e enviando os comandos necessários, um ponto por vez. Esta repetição pode ser cansativa e sujeita a erros, se realizada de modo manual, por um administrador humano.

Com o objetivo de automatizar este processo de gerência, a ferramenta BShell (*Broadcast shell*) é proposta e ilustrada na Figura 4.1. De forma autônoma o BShell é capaz de descobrir os endereços IP de todos os pontos em atividade na rede, estabelecer um canal de comunicação com cada um, e por fim executar os comandos desejados.

O BShell requer apenas um parâmetro para operar, que é o texto que representa todos os comandos, que deve ser enviado e executado em todos os pontos da infra-estrutura da rede. Inicialmente o BShell através de uma técnica "cross-layer", consulta a tabela de rotas, e com uso de filtros, descobre os endereços IP dos pontos desejados. Para cada endereço encontrado, um terminal de gerência é criado, e o texto, com os comandos, passado como parâmetro ao BShell é enviado como entrada do terminal. Ao final da execução dos comandos enviados, o resultado da saída de cada terminal é redirecionado pelo BShell para arquivos de históricos, para futuras consultas.

Durante o desenvolvimento do BShell, duas qualidades foram priorizadas: baixo consumo de memória e resistência a falhas. A fim de diminuir o consumo de memória, todos os componentes utilizados pelo BShell estão disponíveis por padrão no sistema operacional e, portanto, nenhuma nova dependência foi criada. Para a segunda qualidade prioritária, resistência a falhas, em caso de falhas o BShell grava a mensagem de erro e continua a operação nos pontos restantes. Esta qualidade é de grande importância para operação em uma rede *mesh*, pois este tipo de rede pode sofrer freqüentes instabilidades, e portanto, um erro na execução dos comandos em um ponto não deve interromper a execução em outros.

Duas qualidades adicionais também foram alcançadas pelo BShell: baixa necessidade de interação com usuário e a disponibilidade. O BShell permite que a execução de uma mesma seqüência de comandos ocorra repetidas vezes nos pontos da rede, de forma autônoma e, assim também reduzindo falhas acidentais que poderiam ocorrer se a repetição fosse feita manualmente. A confiabilidade da ferramenta ocorre porque um

bloco de comandos pode ser executado em seqüência, mesmo que ocorra um evento de interrupção no canal de acesso. Este tipo de evento é comum, quando dentro do bloco de comandos, são realizadas reconfigurações de algum parâmetro de funcionamento da rede.

De forma similar, é proposta a ferramente Bcp (*broadcast CoPy*). O Bcp foi desenvolvido com os mesmos princípios do BShell. O objetivo desta nova ferramenta é permitir a cópia de arquivos para, ou de, todos os pontos ativos, com o uso do mecanismo de descoberta de endereços autônomo. Uma interessante interação entre o Bcp e o BShell, é quando se deseja executar uma seqüência tão grande de comandos que não possa ser passada como parâmetro ao BShell, sendo a solução escrever tal grande seqüência em um arquivo, enviá-lo aos pontos pelo Bcp, e por fim executá-lo em cada ponto pelo BShell.

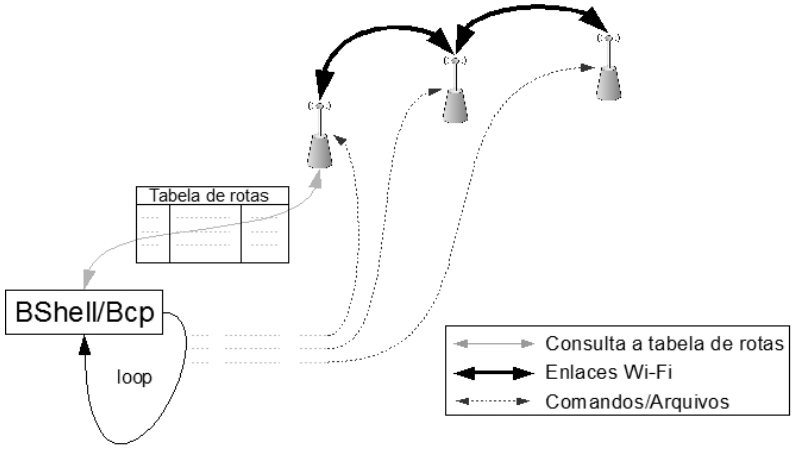


Figura 4.1: Ilustração do funcionamento das ferramentas autônomas.

Futuras versões destas ferramentas de disseminação podem utilizar informações internas ao OLSR [Clausen and Jacquet 2003b] usando, portanto, uma técnica *cross-layer*. O objetivo de usar tal tipo de técnica, é melhorar as tarefas de descoberta dos pontos da rede e de disseminação dos dados. Com esta integração com o OLSR, é possível descobrir a lista dos pontos pertencentes à rede que estão temporariamente desativados ou inalcançáveis no momento que as ferramentas são iniciadas.

Outra possível melhoria com o uso de informações contidas no protocolo de roteamento é a criação de *clusters* espontâneos, criados com o propósito de auxiliar a disseminação de arquivos ou comandos. Atualmente apenas um dos pontos da rede Remesh possui instalados as ferramentas BShell e Bcp, e por tal este ponto é considerado o gerente da rede. Este gerente, por cumprir tal função, possui toda responsabilidade de criar as conexões para cada ponto da rede, e por meio destas conexões executar a tarefa de forma seqüencial. Uma alternativa proposta mais escalável é a divisão em *clusters*, com a

finalidade de diluir a carga do ponto gerente, distribuindo as tarefas para outros pontos. Com as informações adicionais do protocolo de roteamento é possível descobrir quantos vizinhos cada ponto possui, e a qualidade de comunicação com cada um. Com essas informações, os *clusters* podem ser formados por setores de pontos, onde aquele que tiver a maior e melhor vizinhança será eleito como mestre do *cluster*. É de responsabilidade de cada mestre disseminar os dados para seus vizinhos e reportar para o ponto gerente o resultado da disseminação. Portanto o gerente terá de estabelecer comunicação apenas com estes mestres, ao invés de todos os pontos da infra-estrutura da rede.

4.2.3 Visualização da topologia

Uma das mais úteis e necessárias capacidades de um sistema de gerência é apresentar a topologia de uma rede aos seus administradores. Em redes com infra-estrutura cabeada, esta tarefa é considerada simples, pois as mudanças de topologia são infreqüentes. Em redes *mesh*, contudo, as características da topologia mudam com grande freqüência, por causa do ambiente volátil. Portanto, os equipamentos que possuem alguma tarefa de gerência precisam coletar informações de conectividade entre os pontos da rede, de forma periódica, a fim de que seja possível construir uma representação da topologia mais fiel às condições atuais da rede.

Por causa das características de redes sem fio, a qualidade do sinal de rádio pode variar muito ao longo do tempo. O enfraquecimento ou interferência no sinal pode resultar em quebras periódicas dos enlaces e, portanto, causar importantes alterações na topologia. A banda disponível e o atraso na transmissão dificilmente são considerados como atributos limitantes em redes cabeadas, contudo em redes do tipo *mesh*, é algo não desprezível. São estas características que tornam a tarefa de criar uma representação da topologia de uma rede *mesh* um desafio maior do que redes cabedas.

Adicionalmente, com o objetivo de facilitar as tarefas de administração e manutenção, a ferramenta de visualização de topologia para redes *mesh* deve exibir alguma métrica da qualidade de todos os enlaces sem fio da rede, a fim de que a administração, ao monitorar a qualidade de cada enlace, possa perceber os problemas de conectividade, caso existam. Como informações adicionais, a ferramenta pode prover informações sobre a configuração de cada ponto da rede e de algumas estatísticas de uso, integrando portanto, informações de diversas outras ferramentas.

Outros participantes do projeto Remesh desenvolveram uma nova ferramenta, Figura 4.2, para visualização de topologia. Com o novo objetivo de utilizar o posicionamento

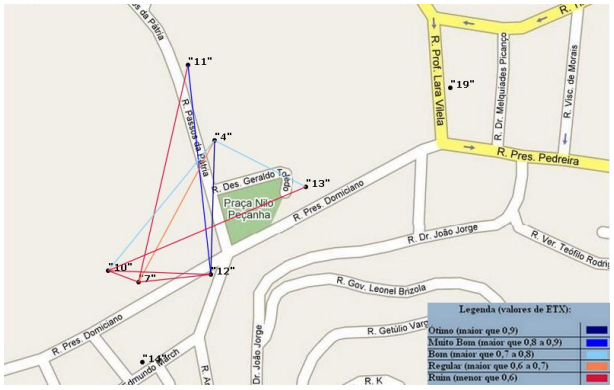


Figura 4.2: Imagem da topologia da rede Remesh produzida pela ferramenta.

geográfico dos pontos, como o objetivo de melhorar a usabilidade da figura. A nova ferramenta utiliza o padrão SVG, que é baseado em XML, para construir um mapa interativo, desenhando o grafo da topologia por cima de uma representação geográfica da rede, como um mapa ou foto aérea. Como a rede utiliza a métrica ML, a qualidade de cada enlace é representada por uma escala de cores no desenho do grafo. Por usar o padrão SVG, a ferramenta é compatível com vários navegadores modernos de páginas de Internet. Mais detalhes sobre a implementação desta ferramenta, podem ser vistos em [Valle et al. 2008].

Esta nova ferramenta oferece, aos administradores, a capacidade de identificar rapidamente as possíveis fontes de problemas. Quando algum usuário relata ter dificuldade no acesso à Internet ou algum desempenho anormal, os administradores, ao consultar as informações organizadas pela ferramenta, são capacitados a rapidamente oferecer uma resposta ao usuário, e iniciar ações corretivas.

4.2.4 Sistema de estatísticas

Para obter as estatísticas da rede Remesh, o projeto propôs uma solução alternativa para o protocolo SNMP [Case et al. 1990]. Apesar deste protocolo ser considerado um padrão estabelecido e amplamente utilizado para cumprir tal tarefa, apresentou contudo, alguns desafios ao projeto, que foram os motivadores da nova solução.

O primeiro desafio enfrentado é relativo às características específicas das redes *mesh*, pois o SNMP não é capaz de extrair todas as informações relevantes deste tipo de rede. Estatísticas interessantes como o *gateway* utilizado por cada ponto ou o número de saltos até ele, que são ambas relevantes, não podem ser obtidas pelas implementações tradicionais do SNMP. Outro exemplo de limitação é a informação sobre a largura de banda disponível, onde o SNMP é apenas capaz de descobrir a taxa utilizada em cada instante,

mas não é capaz de determinar a taxa máxima disponível, à camada de aplicação, na rota de um ponto até o atual e melhor *gateway*. Esta informação da taxa máxima disponível é útil para determinar se o baixo uso de cada enlace é devido a pouca demanda dos usuários, ou se algum outro fator está prejudicando o desempenho.

Como segundo desafio, é a grande proporção de recursos consumidos pela implementação do protocolo SNMP nos equipamentos utilizados como pontos da infra-estrutura da rede *mesh*. No caso da implementação fornecida pelo OpenWrt, o serviço SNMP consome mais de 10% da memória disponível, o que é mais do que duas vezes o tamanho ocupado pelo protocolo de roteamento OLSR (que fica próximo de 4,9%). Dada a quantidade de memória disponível neste tipo de equipamento, o consumo de recursos é uma forte restrição.

Considerando estes dois fatores, é proposto um sistema diferente para ser a solução dos problemas encontrados. O sistema é composto por três partes: um programa "shell script" utilizado para extrair as estatísticas, uma base de dados central para armazenar os dados coletados e um servidor de páginas para receber os dados dos pontos da rede, enviar, resgatar, e filtrar estas informações à base de dados e exibir, ao usuário, representações gráficas. Além de proposto, este sistema foi implementado e encontra-se em operação nas redes do projeto Remesh.

A primeira parte é instalada nos pontos da rede *mesh*. Por ser um "shell script", ocupa pouco espaço na memória permanente e pode possuir a capacidade de acessar as informações ofertadas por outras ferramentas. Em um intervalo de tempo ajustável, porém constante, as estatísticas são recolhidas e então repassadas para o servidor, por meio do protocolo HTTP, e este servidor recolhe as informações e as envia à base de dados.

Uma página HTML é o meio pelo qual os administradores da rede podem visualizar os dados históricos em forma de gráficos. É possível visualizar vinte e duas estatísticas de cada ponto, como atraso, banda disponível, perda de pacotes, número de saltos até o *gateway* padrão, taxa de uso da UCP (*CPU*), número de processos ativos, memória livre e ocupada e o número de bytes de entrada e saída das interfaces com e sem fio de cada ponto da rede. Os gráficos são construídos por até duas estatísticas, durante o intervalo de tempo. Estes parâmetros dos gráficos são selecionados pelo administrador. Outras informações adicionais são relacionadas ao usuários autenticados, assim como o tráfego gerado na rede por estes. A Figura 4.3 mostra um exemplo, com o atraso e banda disponível.

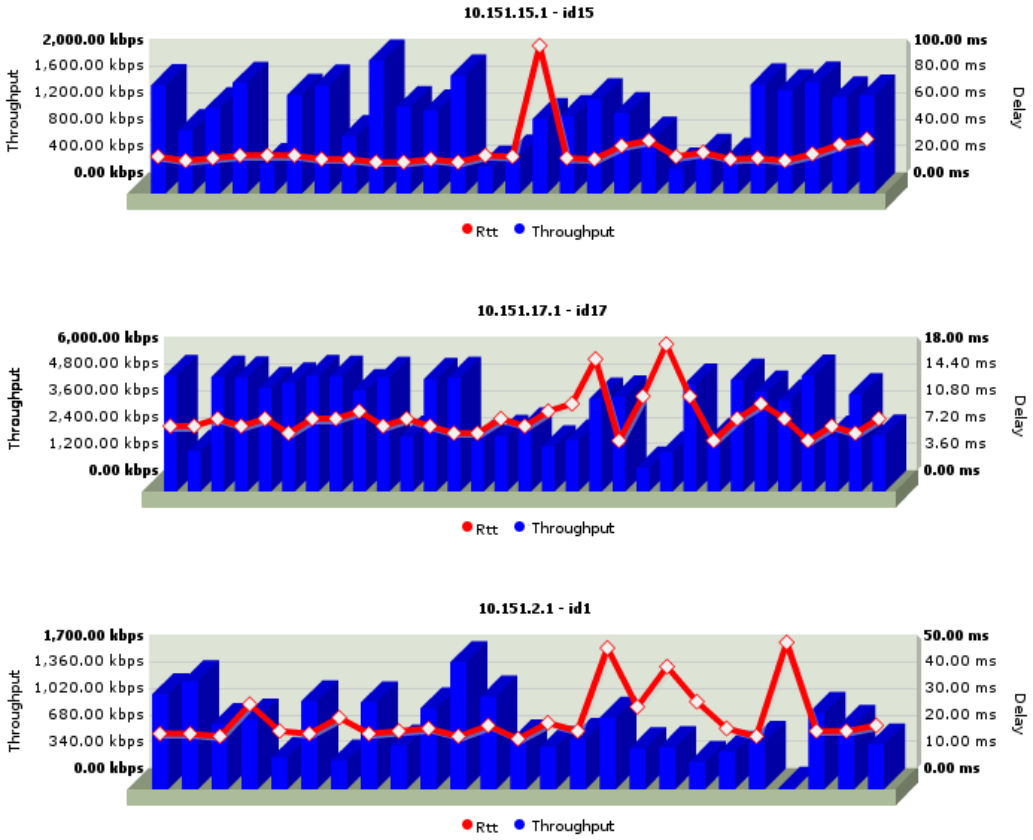


Figura 4.3: Exemplo de um gráfico gerado pela figura.

User (username)	Incoming	Outgoing	Total
pascoal	163,6G	207,1G	370,7G
jviana	76,5G	128,7G	205,3G
fidi	58G	50,7G	108,8G
wgramacho	26G	5,4G	31,4G
dvianna	18,9G	3,1G	22G
rtoso	18,5G	879,1M	19,4G
rcapua	12,3G	1,3G	13,5G
alvaro	8,8G	1,2G	10G
luciana	881M	4,4G	5,2G
ilima	4,1G	819,5M	4,9G

Figura 4.4: 10 maiores consumidores de banda.

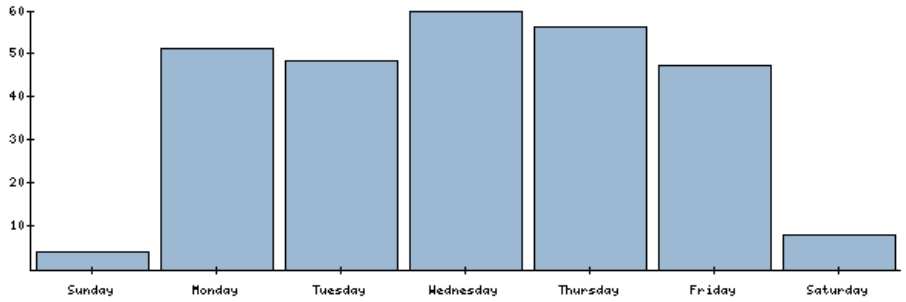


Figura 4.5: Número de usuários por dia da semana

Uma observação importante é que algumas informações capturadas pela ferramenta, como atraso, banda disponível e perda de pacotes, são obtidas por medições ativas, realizadas pelo uso de ferramentas auxiliares. Esta é uma característica da solução de monitoramento do Remesh que vai além do que o SNMP é capaz de oferecer, pois pelo uso de ferramentas consagradas como *ping* e *iperf* é possível agregar, com razoável facilidade, novos tipos de informações. Por outro lado, estas medidas ativas competem com os clientes pelo uso dos recursos da rede, e por tal poderiam interferir gravemente no desempenho da rede percebido pelos usuários, contudo o projeto limitou estes testes para ocorrerem durante curtos intervalos de tempo.

Estatísticas adicionais à esta ferramenta são coletadas pelo sistema WifiDog. Por ser um sistema de controle de acesso o Wifidog é capaz de coletar informações associadas ao

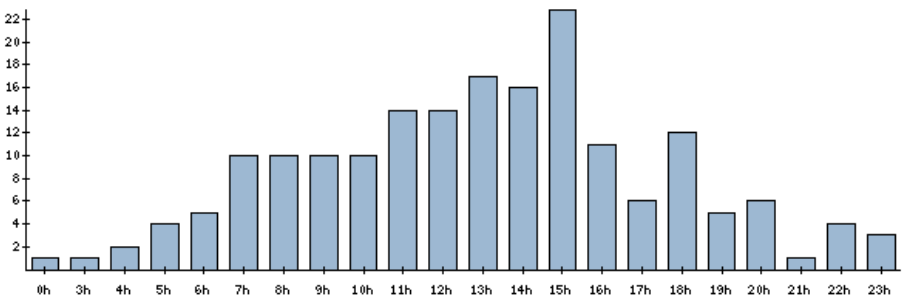


Figura 4.6: Número de conexões por hora do dia.

comportamento de cada usuário, que incluem:

- A lista dos dez maiores consumidores de banda da rede (Figura 4.4);
- O número de novas conexões por hora do dia (Figura 4.6);
- Número de usuários visitantes por dia da semana ou pelo dia do mês (Figura 4.5).

4.3 Conclusão do capítulo

Com o objetivo de facilitar a tarefa de gerenciar uma rede de acesso para seus administradores, é proposto um conjunto de ferramentas. Pois um importante objetivo da área de gerência, é permitir que a menor quantidade de esforço seja desempenhada nas tarefas de acompanhar o funcionamento da rede, detectar as falhas e suas origens, e efetuar as correções eventualmente necessárias. Contudo, as redes do tipo *mesh* impõem alguns novos desafios, como o uso de dispositivos com capacidade limitada, dependência do uso exclusivo de meio de comunicação sem fio, instabilidade causadas por variações na qualidade dos enlaces e barreiras sobre localização dos pontos de infra-estrutura em locais de difícil acesso.

Como conseqüência destes desafios, é definido neste trabalho, que o ferramental adotado no gerenciamento de redes *mesh* deve atender alguns critérios, como dependência mínima de interação com humanos, confiabilidade, baixo consumo de memória, baixo consumo em tempo de execução e resistência a falhas.

A fim de exemplificar como uma ferramenta é importante para diminuir o trabalho dos administradores, a Sub-seção 4.2.1 descreve um simples *shell script* que auxilia a configuração inicial dos equipamentos de rádio. Este *script* modifica um grande conjunto de configurações, que são necessárias para adicionar, a um ponto de acesso padrão, o suporte à rede *mesh*, tornando o processo de configuração inicial tão simples que pessoas, com um mínimo de treinamento, passaram a ser capazes de efetuar a operação, sem erros. Antes deste *script*, era necessário que um administrador experiente efetuasse a operação, porém, mesmo com uma grande experiência do administrador, o processo era demorado, e o mais negativo é que, em diversas ocasiões o resultado da operação não era adequado, na primeira tentativa. Outro exemplo de ferramente que facilita o gerenciamento é o sistema de estatística apresentada na Sub-seção 4.2.4, pois os administradores podem encontrar a origem de certos problemas ao observarem o histórico das estatísticas e, portanto, decidir qual é a correção necessária.

As ferramentas desenvolvidas ou modificadas, ao menos em parte, por este autor são descritas a seguir:

- A Ferramenta de configuração de *gateway*;
- A Ferramenta de configuração de ponto da infra-estrutura (*backhaul*);
- O BShell e o Bcp, que disseminam dados de forma autônoma aos pontos da rede;
- O sistema de controle de usuários baseado no Wifidog;
- Sistema de medição, coleta de estatísticas e visualização.

Capítulo 5

Mobilidade em redes mesh

O suporte à mobilidade é de suma importância para o sucesso de redes sem fio. Nos últimos anos têm-se constatado avanços em *hardware*, que possibilitaram o desenvolvimento de novos dispositivos portáteis, com um crescente potencial de trabalharem com informações complexas. Porém, parte do potencial destes dispositivos, em oferecer serviços úteis aos seus clientes, é dependente da disponibilidade de acesso a dados. Com o amadurecimento da Internet, esta passou a ser uma importante fonte de dados, sendo assim plausível concluir que diversos dispositivos portáteis terão sua utilidade explorada, se os mesmos forem capazes de acessar à Internet. Esta forma conveniente de acesso permite o deslocamento do usuário entre diferentes regiões geográficas e o acesso à rede, portanto, o uso de uma tecnologia de comunicação sem fio pode ser considerado necessário.

Apesar de existirem tecnologias de redes sem fio capazes de cobrir áreas com dezenas de quilômetros quadrados, nenhuma destas faz com o custo tão baixo ou com o desempenho semelhante ao tipo da rede mais popular, denominada Wi-Fi (IEEE 802.11). Contudo estas redes possuem uma limitada capacidade em atender uma grande região com eficiência, limitando, desse modo, a locomoção do usuário. Realizar continuamente a troca de dados com dispositivos móveis em uma rede sem fio, cujo alcance de cada ponto de acesso é limitado, impõe o uso de alguma técnica que possibilite a troca de pontos de acesso (*handoff*), durante a locomoção do usuário com seu dispositivo. Contudo, antes mesmo de escolher a técnica, é necessário entender o que é a mobilidade, os seus desafios e os seus objetivos.

O objetivo deste capítulo é explorar as questões ligadas à mobilidade. É apresentado um estudo das soluções existentes, com o ponto de vista relativo a redes *mesh*.

Inicialmente, este capítulo define alguns cenários típicos de mobilidade em redes *mesh*. Nas seções seguintes, as soluções são discutidas em cada nível distinto da pilha de proto-

colos. No nível de Rede, na Seção 5.1, é apresentada a solução IP Móvel [Perkins 2002] e a técnica MobileNAT [Buddhikot et al. 2005]. No nível de Transporte, na Seção 5.2, é descrito o protocolo Mobile-TCP (M-TCP) [Brown and Singh 1997] e outros. No nível de Aplicação, na Seção 5.3, é discutida uma solução existente que utiliza o protocolo SIP. A um novo nível, entre de Rede e de Transporte, é discutido, na Seção 5.4, a solução *Host Identity Protocol* (HIP) [Koponen et al. 2005]. Na Seção 5.5 são discutidos também algumas soluções de redes de acesso que oferecem suporte transparente ao dispositivo móvel. Na Seção 5.6, são descritas algumas questões e suas soluções relacionadas à mobilidade. Por fim, na Seção 5.7, é resumido o assunto apresentado neste capítulo.

Quatro cenários [Bondareva et al. 2006] são apresentados para demonstrar os problemas, em vários graus de complexidade, que devem ser tratados quando se deseja suportar a mobilidade de clientes sem fio, em uma rede de acesso *mesh*.

- **Cenário 1:** Cenário da rede sem fio mais simples é ilustrado pela Figura 5.1, onde apenas um *gateway* fornece acesso à Internet para todos os dispositivos móveis. Todos os clientes da rede sem fio estão a um salto do *gateway*, ou seja, sem qualquer intermediário. Portanto, as redes deste cenário não são consideradas redes *mesh*;

- **Cenário 2:** Com o suporte de protocolos de roteamento com múltiplos saltos, uma quantidade maior de clientes pode ser inserida na rede, pois estes passam a ter acesso ao *gateway*, pela colaboração de outros equipamentos. A Figura 5.2 ilustra o caso em que um único *gateway* conectado à Internet fornece acesso a todos os clientes da rede. Neste cenário pode ser encontrado o caso mais simples para redes *mesh*;

- **Cenário 3:** Redes *mesh* de grande escala, que utilizam protocolos de roteamento de múltiplos saltos, necessitam utilizar mais de um *gateway*. Como resultado, os clientes podem utilizar o *gateway* mais próximo, em busca de um melhor acesso à Internet, como visto na Figura 5.3, levando assim a diminuição da carga em cada *gateway*. Uma característica deste cenário, que simplifica ou evita diversos problemas de endereçamento e mobilidade, é que todos os *gateways* conectam-se à Internet por meio de um único nó controlador. Logo é possível classificar este tipo como micro-mobilidade ou intra-domínio, onde os usuários locomovem-se dentro do domínio de uma mesma rede. Providências devem ser tomadas para a manutenção das conexões ativas antes da troca de *gateways*;

- **Cenário 4:** A Figura 5.4 mostra o caso mais complexo de redes *mesh*, em que diferentes redes de acesso, cada qual com múltiplos saltos até cada *gateway*, interceptam-

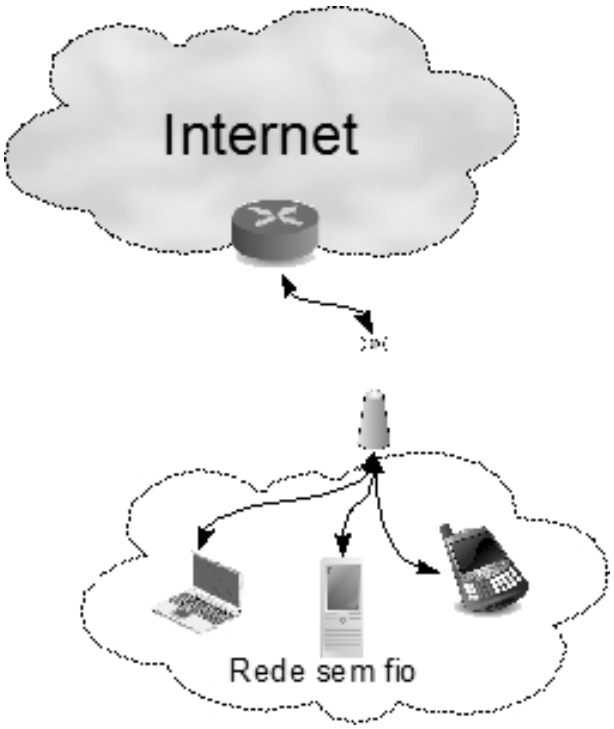


Figura 5.1: Rede com apenas um *gateway* e distantes a um salto.

se formando uma federação de redes *mesh*, onde os clientes irão migrar de rede de acesso, quando for necessário manter a conectividade com a Internet. Neste cenário, as novas conexões serão criadas na rede mais próxima, contudo, as conexões de transporte ativas, que o dispositivo móvel tinha com a outra rede de acesso, devem continuar em operação, após a mudança de rede de acesso. Este cenário determina o uso do tipo de mobilidade, conhecido como macro-mobilidade ou mobilidade inter-domínio, pois diferentes domínios, cada um relacionado a uma rede de acesso, devem trabalhar em conjunto, em favor do cliente em movimento.

Dentre os cenários apresentados, podemos destacar alguns critérios para analisar a capacidade dos métodos de suporte a alocação de endereço e de mobilidade em redes *mesh*:

- Endereços dos clientes serem topologicamente corretos em relação a rede de acesso;
- Suporte a múltiplos *gateways*;
- Suporte às conexões de transporte ativas quando houver migração entre redes ou *gateways* de acesso, à Internet;
- Nível de transparência e para qual ator é oferecida a transparência das questões de mobilidade.

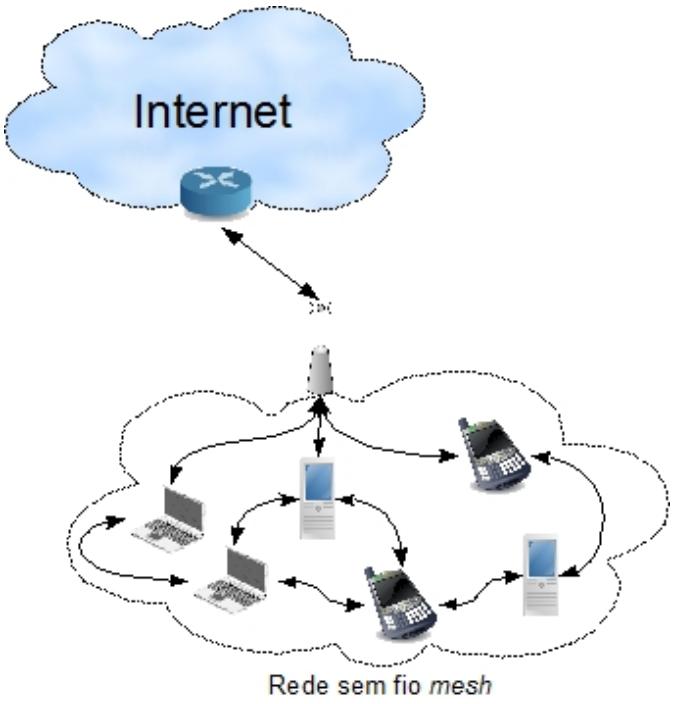


Figura 5.2: *gateway* oferece serviço a maiores distâncias pelo uso de múltiplos saltos.

O endereço IP impõe uma dificuldade com relação à mobilidade, uma vez que este endereço empenha duas funções distintas. A primeira função é utilizada pelo nível de Transporte para identificar o dispositivo. O segundo, utilizado pelo nível de Rede, serve para localizar em qual rede o dispositivo está conectado. A deficiência fica evidente pelo evento de mobilidade, pois apesar de o dispositivo continuar sendo o mesmo, mas em outra rede de acesso, a sua localização é diferente, gerando assim um conflito das funções, já que uma função precisa da alteração do endereço e a outra não.

No quarto cenário, o mais desafiante, a alocação de endereços torna-se mais difícil. Isto porque, nos cenários anteriores, a necessidade do endereço ser topologicamente correto, era mais fácil de gerenciar, pois era considerado apenas o domínio de uma rede de acesso. Esta necessidade cria alguns problemas no evento de mobilidade entre diferentes redes de acesso, tendo em vista que endereços de dois domínios devem ser considerados. Como conseqüência da mobilidade, o antigo endereço deixará de ser topologicamente correto. O problema fica evidente quando o cliente móvel, que está realizando a migração de rede de acesso, muda de endereço IP, com o objetivo de adquirir um endereço correto à nova topologia, que causa quebra nas conexões em andamento. Esta perda de conexão cria um efeito muito negativo, do ponto de vista do usuário, que prejudica a qualidade do serviço que o dispositivo portátil provê ao cliente.

Para que um endereço do cliente seja topologicamente correto, é necessário que este

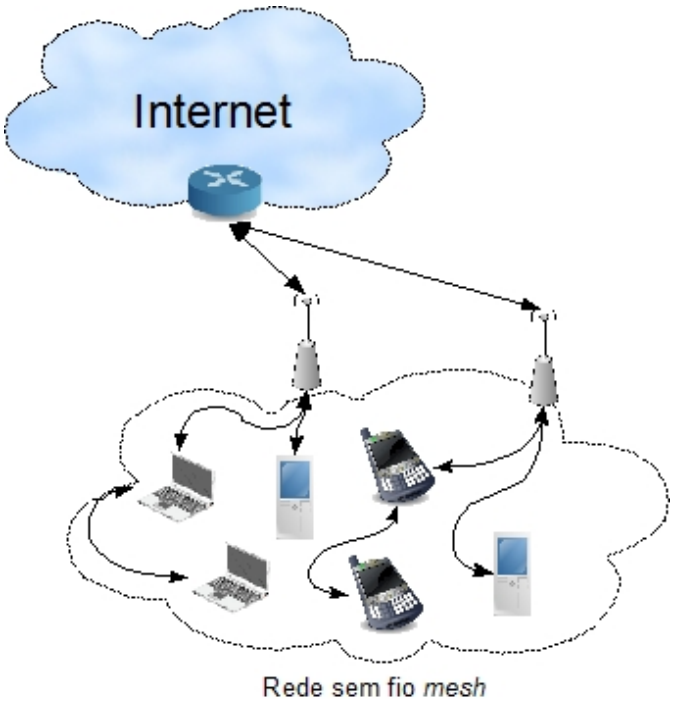


Figura 5.3: Rede com múltiplos *gateways* e por múltiplos saltos

pertença à sub-rede de acesso, ou seja, o prefixo do endereço deve pertencer à rede. Um prefixo é pertencente a uma rede quando seus roteadores de borda anunciam, aos seus vizinhos, que são a rota de encaminhamento dos endereços com o determinado prefixo.

Esta necessidade de alocar os endereços, segundo a topologia do cliente e a sua rede de acesso, precisa ser considerada, pois o roteamento na Internet é dito hierárquico. Caso o endereço do cliente não seja correspondente à sub-rede do *gateway*, seria necessário a divulgação da rota deste endereço nos roteadores de núcleo da Internet, o que por questão de escalabilidade e segurança, não é viável.

Em relação ao critério de transparência, é descrito a seguir o ponto de vista adotado. Na comunicação entre dois pontos na Internet podem ser identificados cinco atores: os dois pontos finais da comunicação, as duas redes de acesso, que cada ponto utiliza, e um conjunto de redes, que é simplesmente abstraído como a Internet, que interconecta as redes de acesso. Todas as soluções são transparentes ao ator Internet, contudo, todas diferem em relação aos outros atores. Estas diferenças são boas candidatas para determinar se uma solução é adequada a um cenário. De forma similar, as técnicas adotadas diferem-se quanto aos atores envolvidos na implementação, que pode ser outro item classificatório.

Antes de iniciar a apresentação das técnicas de suporte a mobilidade, na próxima seção são apresentadas algumas questões relacionadas ao endereçamento em redes sem fio

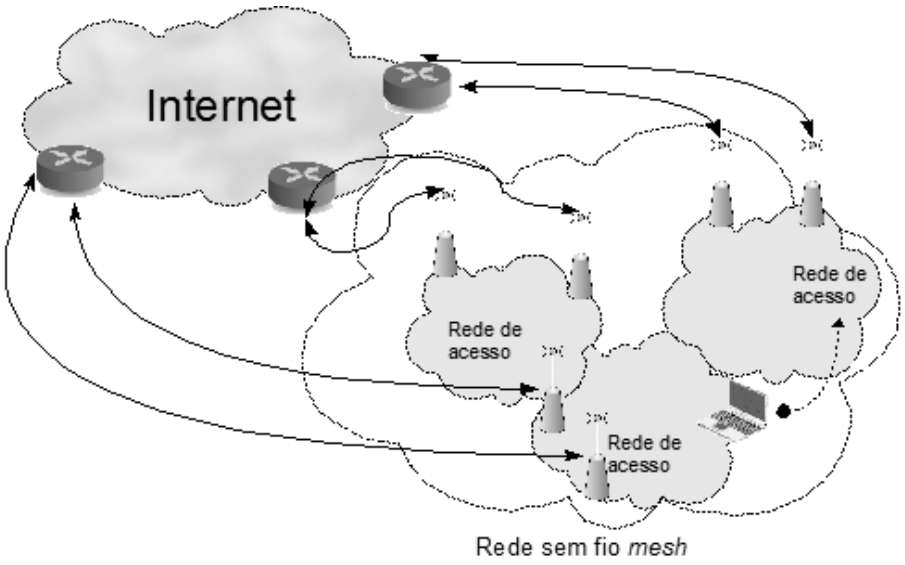


Figura 5.4: Interação entre múltiplas redes de acesso.

e à detecção de mobilidade.

5.1 Suporte a mobilidade no nível de Rede

Em seguida é brevemente descrito o padrão IP Móvel, que foi desenvolvido com o objetivo de dar suporte à mobilidade em redes IP e, em seguida, a descrição da técnica MobileNAT [Buddhikot et al. 2005].

5.1.1 IP Móvel

A técnica IP Móvel [Perkins et al. 2002] foi desenvolvida pela Internet Engineering Task Force (IETF), com o objetivo de permitir que dispositivos móveis, ao realizar movimentação entre diferentes redes de acesso, mantenham um endereço IP permanente. No IP Móvel, cada cliente móvel possui dois endereços: um permanente (*home address*), e outro dinâmico (*care-of-address*), este último é relativo à rede de acesso que o cliente está visitando, que é modificado quando o cliente associa-se a uma nova rede de acesso.

Existem dois tipos de entidades no IP Móvel:

- Um agente externo (*Foreign Agent*) que é responsável por divulgar o endereço dinâmico (*care-of-address*) usado pelo IP Móvel, gerenciando informações sobre os dispositivos móveis associados a sua rede. Os dispositivos devem entrar em contato com o agente externo para registro e aquisição de um endereço dinâmico, que é

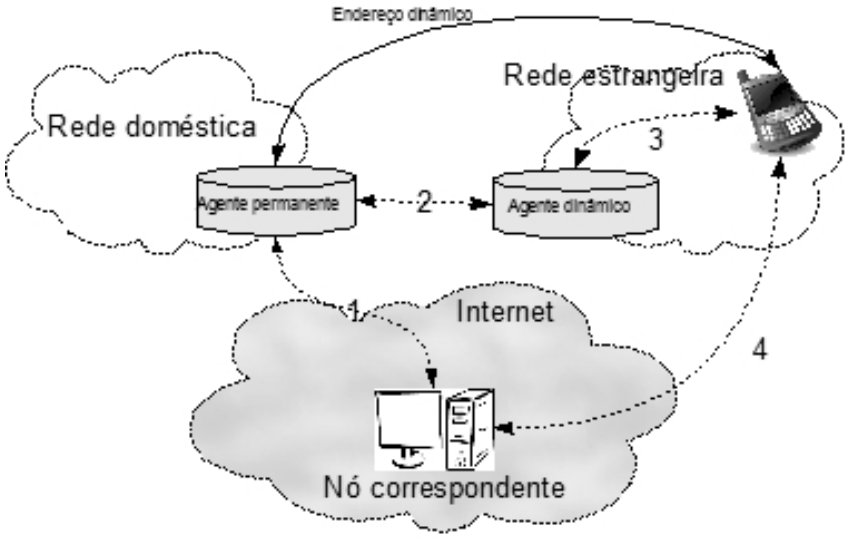


Figura 5.5: IP Móvel.

topologicamente relacionado à rede do agente externo;

- Um agente permanente (*Home Agent*) que é um dispositivo com endereço fixo, conectado a uma rede que possui o endereço permanente (*Home address*) do cliente e, portanto, pode ser visto como representante do cliente. O agente tem o papel de gerenciar as informações sobre o cliente móvel ao qual representa.

A Figura 5.5 exibe o fluxo de comunicação do protocolo IP Móvel. Inicialmente um dispositivo na Internet, com o objetivo de se comunicar com o cliente móvel, envia pacotes de dados ao agente permanente (*Home Agent*), que os redireciona ao cliente móvel. O redirecionamento utiliza o último endereço dinâmico (*care-of-address*) conhecido do cliente móvel, encapsulando o cabeçalho dos pacotes IP enviado pelo destinatário. Se o cliente móvel mudar de rede de acesso e, por conseqüência, alterar também o agente externo (*Foreign Agent*), este deve enviar, ao agente permanente, o novo endereço obtido depois da migração entre redes de acesso.

O IP Móvel suporta o uso de múltiplos *gateways*. Também é capaz de manter as conexões abertas do nível de Transporte em funcionamento, durante as migrações de rede de acesso e agentes externos, portanto, o protocolo IP Móvel é apropriado para ser usado em todos os cenários apresentados. Contudo, este protocolo possui algumas deficiências destacadas a seguir:

- Os dispositivos móveis devem sempre informar sobre a sua movimentação ao seu agente permanente, que pode provocar um significativo aumento na latência do

restabelecimento do fluxo de dados [Fikouras et al. 1999], quando o cliente móvel muda de ponto de acesso freqüentemente;

- Cada dispositivo móvel deve possuir um agente permanente, que por sua vez deve ter um endereço globalmente roteável. Este agente deve estar sempre disponível, para que o dispositivo móvel seja alcançável, criando assim um novo ponto de falha;

- O agente permanente e a sua rede de acesso são recursos necessários ao cliente móvel, para que este seja capaz de migrar entre diferentes redes de acesso e, por serem necessários, portanto, aumentam o risco de alguma falha de equipamento interromper a comunicação do cliente móvel;

- O filtro de ingresso [Ferguson and Senie 1998] é uma técnica que dificulta alguns tipos de acesso maliciosos a Internet, onde, em cada domínio administrativo, os roteadores de borda só retransmitem pacotes em direção à Internet, somente se estes pacotes tiverem o endereço de origem IP pertencente a sub-rede do roteador. Este filtro prejudica o funcionamento normal do IP Móvel, que passa a ser obrigado utilizar uma adaptação, como encontrada em [Montenegro et al. 1998];

- Em redes *mesh*, os pacotes enviados em *broadcast* podem causar um grande impacto no desempenho da rede, pois, o agente externo (*foreign agent*) pode não ter acesso direto ao dispositivo móvel. Tal impacto é ocasionado pelo risco de uma inundação de pacotes, por toda a rede;

- O fato de redes *mesh* realizarem comunicação em múltiplos saltos, dificulta ou impede o correto funcionamento dos mecanismos de detecção de movimentos encontrados no padrão original do IP Móvel, pois o mecanismo de sinalização utilizado pelo dispositivo móvel e pelo agente externo não é adequado no cenário que é utilizado multiplos saltos;

- Como o nível de Rede não pode comunicar ao protocolo TCP, no nível acima, este sofre de questões que prejudicam seu desempenho. Estas questão são descritas, com mais detalhes, na Sub-seção 5.6.3.

Além do IP Móvel, os seus pesquisadores criaram outros dois protocolos para Internet, Celular IP [Valkó 1999] e Hawaii [Ramjee et al. 2002] para oferecer suporte a micro-mobilidade. O Celular IP é uma solução hierárquica, que busca minimizar os registros, nos agentes permanentes (*Home Agents*), feitos pelos dispositivos móveis, quanto é realizada uma troca de ponto de acesso. Ao se organizar os agentes externos (*Foreign*

Agent), de modo que cada agente seja responsável por várias estações de acesso, que controlam um conjunto de células de rádio, tem-se como resultado deste arranjo hierárquico, que o dispositivo, enquanto usar as células gerenciadas pelo mesmo agente, não precisa realizar nenhum novo registro. Todavia, existe a desvantagem de que o Celular IP utiliza um conjunto de protocolos específicos, o que dificulta a sua ampla implementação em diferentes tipos de redes de acesso.

Já o protocolo Hawaii [Ramjee et al. 2002], por sua vez, adota uma solução baseada em domínios, que organiza as estações de acesso sob forma de árvores, realizando uma configuração especializada de rotas, instalando desvios por clientes, em roteadores específicos que suportam a micro-mobilidade. Além disso, apresenta vantagem sobre o Celular IP, por separar os agentes externos (*Foreign Agents*) dos *gateways*, o que simplificou as funções dos *gateways*, tornando-os assim mais resistente às falhas do mesmo. Entretanto, possui a desvantagem de obrigar a modificação dos roteadores pertencentes à topologia de árvore, que suporta a micro-mobilidade.

Outras pesquisas adicionais [Perkins 1996a, Lei and Perkins 1997] adaptaram o IP Móvel, de modo a permitir seu uso em redes ad hoc. Neste sentido, ao se incluir uma extensão ao IP Móvel, passa-se a permitir que os dispositivos móveis usem o endereço dinâmico (*care-of-address*) mesmo que estejam a mais de um salto do agente externo (*Foreign Agent*). Resolve-se ainda o conflito na manipulação de tabela de rotas, pois tanto a rede *mesh* quanto o IP Móvel tentam manipular a tabela de roteamento. Uma solução para tal conflito é instalar um terceiro gerente para coordenar as manipulações.

Uma solução alternativa, MIPANET [Jönsson et al. 2000], os clientes móveis de uma rede ad hoc que desejam ter acesso à Internet, realizam um registro no agente externo e passam a utilizar o seu endereço permanente (*home address*) para todas as comunicações. O cliente móvel cria um túnel com o agente externo, para encaminhar todos os pacotes com destino à Internet que, ao chegar no agente externo, são desencapsulados e enviados em seguida ao destinatário. Dentro da rede sem fio o protocolo de roteamento ad hoc é responsável por rotear o pacote do cliente móvel ao agente externo. Adicionalmente o MIPMANET utiliza um novo algoritmo, chamado MIPMANET *Cell Switching* (MMCS), que indica ao cliente a necessidade de realizar um novo registro em outro novo agente externo.

5.1.2 MobileNAT

Examina-se, a seguir, uma adaptação da técnica NAT que adiciona o suporte de mobilidade, tanto de micro e macro mobilidade, entre diversos espaços de endereçamento heterogêneos (domínios de rede). As três principais características desta técnica são:

1. **Uso de dois endereços**, um virtual e outro globalmente roteável;
2. **Extensão do protocolo DHCP**, para gerenciar os dois endereços;
3. **O uso de um gerente de Mobilidade**, que altera as regras NAT em resposta aos eventos de mobilidade.

MobileNAT [Buddhikot et al. 2005] possui dois componentes que realizam tradução de endereço, uma é realizada em um roteador chamado de nó âncora (*archor node*) e possui um comportamento similar anteriormente visto com *gateway* NAT. A segunda tradução é feita em um novo nível chamado *shim* que é colocado no dispositivo móvel. Com essas traduções, o MobileNAT é capaz de influenciar na rota do pacote, que é utilizada entre o nó âncora e dispositivo móvel. Este roteamento possibilita que sejam realizadas adaptações de rotas sob os eventos de mobilidade.

O endereço IP impõe uma dificuldade com relação à mobilidade, pois este endereço desempenha duas funções distintas. Uma é identificar o dispositivo no nível de Transporte e segundo servir como referência a sua localização física no nível de Rede. A deficiência fica evidente pelo evento de mobilidade, pois apesar do dispositivo continuar sendo o mesmo, mas em outra rede de acesso, a sua localização é diferente, gerando assim um conflito das funções, uma ez que, uma precisa da alteração do endereço e a outra não.

Com fins de resolver tal conflito, a técnica MobileNAT utiliza dois endereços para cada dispositivo, como se verifica a seguir:

- **Endereço Virtual** E_v (*Virtual* IP): Endereço fixo, cuja função é dar uma identificação que não se altera no evento de mobilidade, que é utilizado pelos níveis de transporte e nos acima;
- **Endereço Físico** E_f (*Physical* IP): Endereço que identifica a localização corrente do dispositivo móvel, utilizado para rotear os pacotes para o Nó Móvel dentro de um domínio (espaço de endereçamento ou sub-rede) ou pela Internet. Claramente o E_f deve ser modificado sempre que o evento de mobilidade levar o dispositivo a uma nova sub-rede.

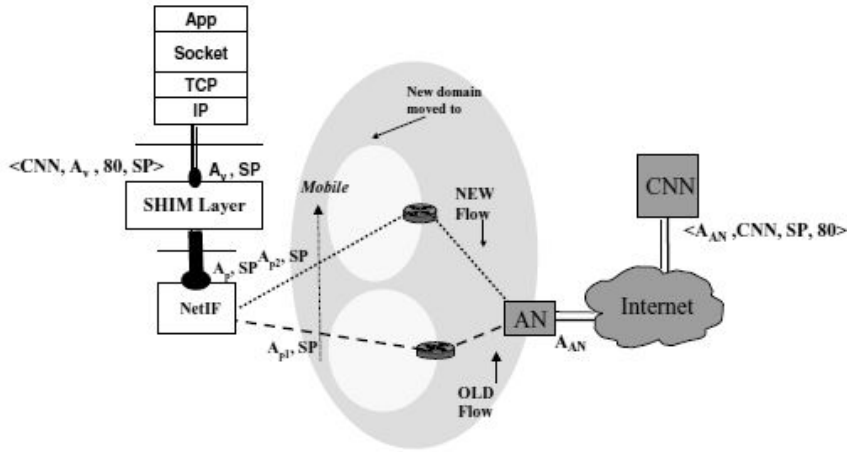


Figura 5.6: Suporte a mobilidade intra-domínio. (fonte: [Buddhikot et al. 2005])

Como ambos os endereços podem ser públicos ou privados, existem quatro combinações possíveis e o MobileNAT oferece suporte a todas. A seguir, é descrita a combinação com ocorrência mais provável em redes *mesh*, onde ambos endereços são privados.

Na Figura 5.6 é exemplificada a mobilidade intra-domínio, com sessões TCP ao serviço da página de notícias CNN na porta destino 80 e de origem SP. O dispositivo móvel possui a tupla de endereços (E_f,E_v), na camada de transporte esta sessão possui a tupla de identificação (TCP, E_v, CNN, SP, 80). Como o E_v é o endereço de origem e não pode ser usado no roteamento do pacote, deve ser substituído pelo E_f na técnica NAT de origem (*Source* NAT ou SNAT). O mesmo ocorre quando o pacote de resposta chega ao dispositivo móvel com a técnica NAT de destino (*Destination* NAT ou DNAT). Estas substituições são realizadas entre nível de Rede e de Enlace, em um nível chamado *Shim*.

Quando o pacote chega ao nó âncora, é realizada a técnica NAT convencional, o E_f é substituído pelo endereço público do nó âncora (E_{nat}), pois o E_f, por ser privado, somente pode ser utilizado dentro do domínio controlado pelo nó âncora. No caso do E_f ser público, não será necessário realizar NAT, mas o endereço deve ser o da sub-rede, no qual o nó âncora é responsável por realizar o roteamento. O nó âncora mantém o mapeamento de endereços realizado na tradução. Por fim, o pacote é encaminhado ao destinatário, que é o servidor CNN. O servidor CNN mantém a sessão no nível de Transporte com a tupla (TCP, CNN, E_{nat}, 80, SP). Quando a resposta é enviada, o pacote que a contém sofre as mesmas traduções do pacote de requisição, mas em ordem inversa.

Quando o cliente realiza algum movimento, para a sessão não ser invalidada quando o cliente migrar de rede de acesso, as tuplas de identificação, no nível de Transporte, não devem ser alteradas. Neste momento, a utilidade do E_v fica clara, pois como não é

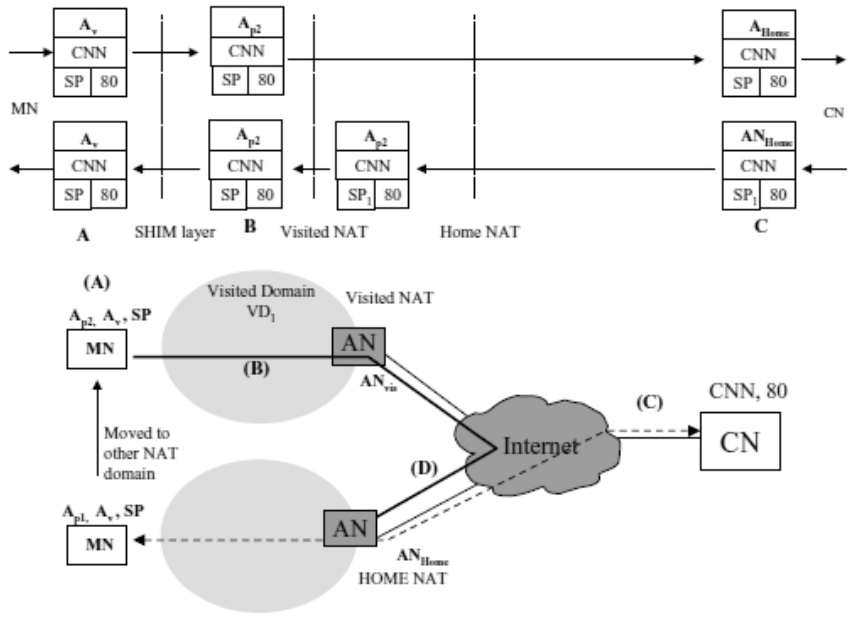


Figura 5.7: Mobilidade entre diferentes domínios, preservando as conexões no nível de Transporte. (fonte: [Buddhikot et al. 2005])

alterada, no evento de mobilidade, permite-se que a tupla no lado do cliente móvel não necessite de modificações. No outro extremo da sessão, no destinatário (CNN), a tupla utiliza o endereço do nó de âncora, que igualmente não é alterado no mesmo evento de mobilidade. Somente o E_f deve ser atualizado para refletir a nova localização física. O nó âncora e o dispositivo móvel, quando informados da mobilidade, atualizam o mapeamento com o novo E_f. Sendo assim, o destinatário não precisa realizar qualquer ação, pois este é protegido de qualquer alteração causada pela mobilidade, somente o nó âncora e o dispositivo móvel precisam ser modificados para suportar o MobileNAT.

Acima foi mencionado apenas um exemplo de mobilidade intra-domínio. Apresenta-se, a seguir, um exemplo de mobilidade inter-domínio, conforme ilustrado pela Figura 5.7.

No caso de mobilidade inter-domínio, diferentes nós âncoras serão envolvidos, pois cada domínio possui um nó responsável. O primeiro e antigo domínio é chamado de NAT nativo (*home* NAT) e o novo de NAT visitado (*visited* NAT). Os dois nós âncoras devem cooperar, para a manutenção das conexões existentes ativas do cliente que realizou a movimentação. Quando o cliente entra em um novo domínio e, portanto, adquire outro E_f, o nó âncora do domínio nativo deve ser informado do novo E_f, assim como do endereço do nó âncora do domínio visitado.

Todo tráfego das conexões antigas continua sendo enviado ao nó âncora nativo (*home* NAT), pois os destinatários (como o servidor CNN) não participam da gerência das questões de mobilidade. O nó âncora nativo repassa todos os pacotes destinados ao antigo E_f do cliente, pertencentes às conexões iniciadas durante a presença do cliente em seu domínio, ao novo do domínio visitado, utilizando o nó âncora visitado como intermediário. Após chegar ao nó âncora visitado, os pacotes seguem o caminho para a nova localização do cliente.

O MobileNAT pode ser comparado com as variações do IP Móvel:

- **IPv6** móvel cria a possibilidade do destinatário enviar respostas a um endereço diferente de quem enviou o pacote, pelo uso da opção IP de destino (*destination IP*). Portanto, os pacotes podem ser enviados diretamente ao último endereço conhecido do dispositivo móvel e, por tal, não precisa utilizar a rota menos eficiente que passe pelo agente permanente *Home Agent*. Como a implementação deste padrão requer mudanças, em larga escala, que ainda não foram realizadas na infra-estrutura da Internet, não é, portanto, uma opção viável.

- IP Móvel com NAT exige o uso de túneis e de adaptações no agente permanente, pois tanto o cliente móvel, quanto o agente externo (*foreign agent*), passam a possuir endereços privados. O agente permanente é capaz de perceber que o cliente móvel e o agente externo estão sob NAT, ao verificar que o endereço anunciado no pacote de comunicação entre os agentes difere do endereço do pacote, pois o endereço do pacote que chega ao agente permanente é do *gateway* que realizou o NAT.

Uma técnica similar ao MobileNAT é o Virtual-NAT [Su and Nieh 2002], que é uma proposta de migração de conexões TCP, ao evento de mobilidade. Esta proposta usa uma abordagem fim-a-fim [Saltzer et al. 1984], onde a tradução é realizada nos dois extremos, ou seja nos dispositivos que usam uma conexão. É utilizada uma sinalização explícita entre estes dispositivos, que obriga a implementação desta técnica em ambos dispositivos, mesmo se um destes não for móvel.

A seguir, passa-se a examinar o nível de Transporte e as implicações provocadas pelo uso das redes sem fio e da mobilidade, tendo-se como foco o protocolo TCP, que foi escolhido pela sua importância e pela especial fragilidade das implicações de mobilidade. Inicialmente, são apresentadas algumas questões que influenciam o funcionamento deste protocolo na implementação clássica e, ao final, algumas evoluções como M-TCP e WTCP, seguido do protocolo de apoio ao TCP chamado SNOOP.

5.2 Suporte a mobilidade ao nível de Transporte

5.2.1 M-TCP: TCP para redes celulares móveis

Uma forma de modificar o TCP, com a finalidade de melhorar o desempenho em redes *mesh*, é colocar um intermediário, *proxy*, no ponto de divisão entre a rede com e sem fio. Grande parte das soluções baseadas em *proxy* tentam encobrir o efeito da perda de pacotes nas redes sem fio sobre o protocolo TCP. Esse objetivo pode ser alcançado, ao evitar eventos de *timeout* e retransmissão rápida (e a conseqüente diminuição da janela de transmissão) no dispositivo remetente, ou evitar incrementos no temporizador de *timeout*. Uma técnica empregada é o bloqueio de pacotes ACK duplicados, resultantes de perdas do canal sem fio, para evitar a retransmissão rápida. Outra técnica, também útil, é manipular o campo tamanho de janela do protocolo TCP para zero, por meio do anuncio ZWA (*Zero Window Advertisement*) nos pacotes ACK a fim de, temporariamente, suspender as transmissões do TCP e, assim evitar o evento *timeout*.

M-TCP [Brown and Singh 1997] é baseado na abordagem de inserir um elemento entre os dois pontos que realizam uma comunicação, dividindo a conexão em duas partes, para permitir a introdução de técnicas que respondam melhor às desconexões e a largura de banda variável das redes sem fio. O ponto de divisão ocorre em um ponto especial chamado nó supervisor (*Supervisor Host*), que está na fronteira entre as redes com e sem fio, responsável por um número de estações de suporte móveis, com conjunto de células, ao quais os clientes móveis terão conectividade à rede.

O TCP no ponto destinatário da conexão, que pode estar na Internet, não precisa ser alterado, pois não precisa ter o conhecimento da mobilidade ou das características da rede sem fio, que suporta o cliente móvel no outro extremo da conexão. Somente no ponto supervisor e no cliente móvel é implementado o M-TCP. No cliente móvel, o M-TCP apenas adiciona ao TCP clássico um mecanismo de notificação sobre o estado do enlace. É no supervisor que as técnicas de migração de endereço do M-TCP são implementadas.

5.2.2 WTCP e SNOOP

Acima foi apresentado uma variação do TCP adaptada à mobilidade, contudo existem outras alternativas que visam melhorar o desempenho do TCP em redes sem fio, como o WTCP [Ratnam and Matta 1998] e a técnica de apoio SNOOP [Balakrishnan et al. 1995].

O WTCP busca tornar transparente o tempo gasto por cada segmento no *buffer*

do ponto adicional, que no caso do M-TCP foi chamado de supervisor e no WTCP é chamado de estação base, com o efeito de eliminar interferências sobre a estimativa de RTT de perdas provocadas pelo meio de comunicação das redes sem fio. O WTCP possui algumas otimizações no enlace criado entre a estação base e o cliente móvel, como exemplo, a diminuição da janela de transmissão no caso de perda, com a finalidade de evitar a provável perda em rajada, que são costumeiras em redes sem fio, para retomar a situação operação normal quando um ACK é recebido, indicando o restabelecimento do enlace sem fio, sem passar pela fase de início lento (*slow start*) ou *timeout*.

A técnica SNOOP [Balakrishnan et al. 1995], implementada no nível de Enlace, pode ser vista como um apoio transparente ao TCP clássico, a ser instalado nos pontos de suporte de redes sem fio. O funcionamento da técnica consiste em instalar no *gateway* da rede sem fio um processo que analise todos tráfego TCP que ingressam a rede sem fio, armazenando os segmentos TCP em um *buffer*. Estes segmentos serão utilizados se o mesmo processo observar algum ACK duplicado originado do cliente Móvel, em direção a alguma outra rede. No caso de encontrar uma mensagem de ACK duplicado, esta mensagem será barrada, para em seguida, o mesmo processo, pela retransmissão do segmento armazenado no *buffer*, corrigir a perda detectada pela mensagem ACK duplicada. Como resultado, a técnica SNOOP consegue assim deixar livre o destinatário, na rede externa, os problemas causados por perdas da rede sem fio. A técnica SNOOP possui limitações relacionadas ao tamanho e ao gerenciamento do *buffer*, assim como perdas em longas rajadas.

Estas técnicas, ao tentarem esconder os problemas de perda em redes sem fio dos dispositivos na Internet, possuem algumas limitações de quanto podem melhorar o desempenho do TCP [Tsaoussidis and Matta 2002].

5.3 Suporte a mobilidade ao nível de Aplicação

Poucas propostas foram criadas no intuito de criar suporte à mobilidade que utilizem soluções ao nível de aplicação. Uma proposta conhecida, que é totalmente baseada em mecanismos deste nível, é o protocolo SIP. Este protocolo cria o suporte à reconfiguração após o evento de mobilidade, por meio do uso de mensagens, sinais, servidores *proxy* e *relay* entre os dispositivos que realizam uma conexão.

Entre as vantagens de se utilizar soluções baseadas em mecanismos implementados no nível de aplicação, tem-se a possibilidade de adequar as necessidades de cada tipo de

aplicação, facilitar a implantação de modificações nas implementações e depender menos da capacidade da rede em oferecer as facilidades requeridas. Todavia, tem-se um ponto negativo, que consiste no custo de todas aplicações serem modificadas com estes mecanismos, não podendo usar a abstração de alguns problemas, caso a implementação fosse oferecida por níveis inferiores.

Existe ao menos uma opção que diminui o custo de adoção de soluções a nível de Aplicação, que seria a instalação de uma aplicação especialista no dispositivo móvel, que irá interceptar todo tráfego gerado por outras aplicações e realizar o tratamento adequado. Adicionalmente, a aplicação especialista em mobilidade pode oferecer ao usuário uma interface para o gerenciamento de perfis para as aplicações clientes.

Outra solução é instalar uma aplicação no *gateway* da rede sem fio, conferindo à rede sem fio a capacidade de oferecer uma facilidade de suporte a mobilidade de grau mais amplo, com mecanismos que atendam de forma geral a todos os tipos de aplicações existentes utilizados pelos usuários dos dispositivos atendidos pela rede sem fio. Como última opção apresentada, tem-se a própria aplicação cliente, pelo uso de uma biblioteca de apoio, a dar o suporte necessário. Desta forma, existe beneficio da aplicação cliente poder controlar e responder, de forma dinâmica, os eventos de mobilidade e as variações da qualidade do meio de comunicação.

5.3.1 SIP

Um exemplo de técnica baseada no nível de aplicação, é o protocolo SIP (*Session Initiation Protocol*), que possui uma proposta [Wedlund and Schulzrinne 1999] de um mecanismo de suporte a mobilidade fim-a-fim (*end-to-end*) e, portanto, utiliza exclusivamente os mecanismos de sinalização e de troca de mensagens do protocolo SIP para dar suporte a mobilidade.

Diversos tipos de mobilidade são suportados pela proposta, como exemplo a mobilidade de dispositivo, de sessão e de serviços. Um tipo adicional de mobilidade que é pouco explorado ou sequer cogitado é a mobilidade dos usuários, como no exemplo do usuário trocar de dispositivo, entre um computador de mesa para um *smartphone*, carregando consigo todas as atividades que envolvem o uso de rede para o novo dispositivo. A proposta estende o SIP para permitir mobilidade dentro do mesmo domínio ou entre diversos domínios administrativos, permitindo assim ao usuário utilizar as redes de acesso a fim de obter acesso a serviços de rede a partir do seu dispositivo móvel com mínimo de interrupção ao evento de mobilidade. O protocolo SIP utiliza outros protocolos comuns do

IETF como DHCP, AAA, Diffserv entre outros para prover as funcionalidades requeridas.

As principais motivações desta proposta de extensão do SIP são:

- Solução baseada no argumento fim-a-fim [Saltzer et al. 1984], dando ao nível de aplicação a responsabilidade de manipular a mobilidade sem utilizar ou conhecer recursos específicos dos níveis inferiores.
- Permite otimização de rotas e melhoria no desempenho em serviços de tempo real pelo uso dos mecanismos do SIP.
- Utiliza identificador de alto nível SIP URI (*Uniform Resource Identifier*), que é superior e independente das identificações dos níveis de transporte e de rede.

Os três principais componentes que formam o protocolo SIP são o agente de usuário, o *proxy* e os servidores de redirecionamento. Cada usuário é identificado por uma URI (*Uniform Resource Identifier*). O agente é instalado no dispositivo que o usuário utiliza, sendo o agente responsável por enviar mensagens SIP para inicializar uma sessão e por receber futuras mensagens. Para a sessão ser estabelecida entre o cliente móvel e o destinatário, o agente envia mensagens de INVITE contendo a URI do destinatário ao servidor *proxy*. Este servidor deve possuir o mapeamento da URI do destinatário com a sua atual localização, em alguma rede de acesso. O servidor então repassa a mensagem de INVITE ao destinatário. Por fim, o destinatário, quanto receber o INVITE, entra em contato com o dispositivo móvel, enviando a sua atual localização, para o estabelecimento da sessão.

Ao evento de mobilidade, o dispositivo móvel deve informar a todos os participantes das sessões existentes de sua nova localização, por meio do reenvio de mensagens INVITE, contendo o novo endereço. O servidor de redirecionamento pode ser utilizado pelo dispositivo móvel, a fim de criar uma forma permanente de contato com outros destinatários, pois ao mesmo evento de mobilidade, apenas o servidor de redirecionamento precisa ser notificado da nova localização, para atualizar todas as sessões estabelecidas.

O SIP possui a vantagem de ser implementado ao mais alto nível, que é o nível de Aplicação. Pelo argumento fim-a-fim, é o nível mais capacitado para tratar, de forma adequada um problema, ao tipo de uso que a aplicação demanda. Outra vantagem de ter o suporte ao nível de Aplicação é a independência dos outros nível e, portanto, pode ser rapidamente adotada pelas aplicações que teriam o maior beneficio com o suporte, como exemplo aplicações de conversação por áudio.

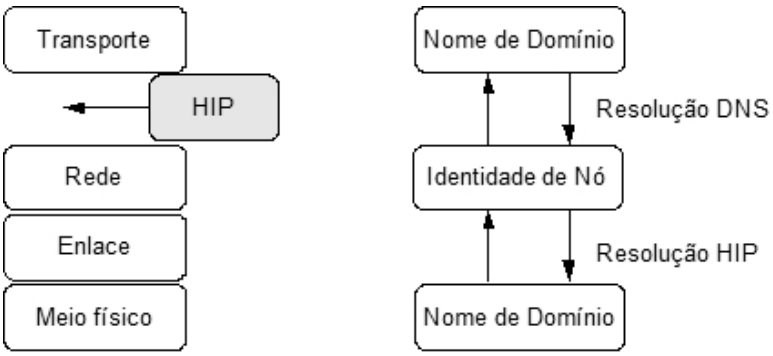


Figura 5.8: A esquerda a nova camada e a direita a resolução de identificações.

A desvantagem do SIP é o tempo necessário para migração (*handoff*) ser considerado alto para aplicações de tempo real [Nakajima et al. 2003]. Como o SIP não depende de nenhum mecanismo especial dos níveis inferiores, possui poucas oportunidades de otimizar o tempo necessário de migração, a não ser que técnicas, do tipo *cross-layer*, sejam utilizadas.

5.4 Suporte a mobilidade no nível intermediário entre Rede e Transporte: HIP

As soluções anteriormente apresentadas possuem como centro de atuação algum nível existente da pilha protocolo de rede, contudo, é possível desenvolver uma solução que não seja restrita à estrutura existente, como é o caso do protocolo *Host Identity Protocol* (HIP) [Koponen et al. 2005]. Este protocolo propõe um nível intermediário, a ser inserido entre os níveis de rede e de transporte. Com o objetivo de prover um método de identificação de dispositivos, que separa a identificação e a localização hierárquica do endereço IP. Para tal, o protocolo introduz um novo espaço de nomes, com o objetivo de identificar uma entidade (HI, *Host Identiy*), entre os níveis de rede e de transporte (Figura 5.8). Esta identificação é utilizada para o estabelecimento e atualização das conexões, ativas durante um evento de mobilidade, e suas conseqüentes reconfigurações de endereço, no nível de Rede.

A necessidade da separação, entre a identificação e a localização de uma entidade, ocorre pela sobrecarga semântica existente no endereço IP. A camada de transporte (TCP) pode utilizar este endereço como identificação da entidade, correspondente a uma conexão. A camada de rede, por sua vez, utiliza o mesmo endereço para determinar a localização da entidade correspondente.

Um cliente móvel usualmente estabelece um contato inicial com um destino, através da procura do endereço IP a partir de uma identificação (*Domain name*) pertencente ao destino, por meio de uma requisição ao DNS. Quando o evento de mobilidade é considerado, é possível que ocorra o problema que o servidor DNS não possuir a informação correta da localização do destino, ou seja, o servidor pode não ser notificado, a tempo, sobre o endereço IP atual, e acabar por responder com o endereço IP de uma antiga localização. Este problema ocorre quando o destino migra de rede de acesso, e por tal, com a nova localização um novo endereço IP.

O mesmo problema de falta de atualização da localização, pode ocorrer mesmo quando o DNS responsável pela identificação é atualizado com o novo endereço. Isto se deve a possibilidade do servidor DNS, utilizado pelo outro participante da comunicação, guardar em sua memória *cache* a antiga localização da identificação. Um problema típico de base de dados distribuídos escaláveis. No modelo não móvel, em que as entidades raramente realizam trocas de endereço, o uso de *cache* permite grandes ganhos de desempenho e escalabilidade, porém torna-se inconveniente quando a identidade é de um dispositivo móvel, o qual pode sofrer constantes atualizações.

A proposta do protocolo HIP alivia o problema relacionado ao DNS, pois através de extensões *rendenzvous* (*rendezvous extensions*), em que um dispositivo, com identificação HI, pode ser alcançado pelo IP de uma entidade intermediária, chamado servidor *Rendezvous*. Este servidor possui uma localização estável e fixa, para ser sempre alcançável. Com HIP, a configuração DNS, para um dispositivo, consiste nos dois itens anteriores, a identificação HI e a localização do servidor *Rendezvous*, de tal forma que, quando um dispositivo iniciar uma nova conexão com um outro qualquer, a primeira mensagem será enviada ao servidor fixo, que a reenvia ao destinatário pela última localização conhecida (Figura 5.9). O restante das mensagens são trocadas diretamente entre os dispositivos finais, sem passar pelo servidor, portanto, não possui o efeito do roteamento triangular do MIP. Quando o dispositivo móvel muda de rede de acesso, este informa ao servidor a sua nova localização. O comportamento do servidor *Rendezvous* é similar ao agente permanente (*home agent*) da arquitetura IP Móvel.

HIP permite a mobilidade IP fim-a-fim de forma transparente para a camada de transporte, logo HIP é uma solução para todos os quatro cenários apresentados, possuindo duas importantes limitações:

- O uso do HIP iria obrigar a modificação da pilha de camadas de rede nos dispositivos e a introdução de um serviço global *Rendezvous*;

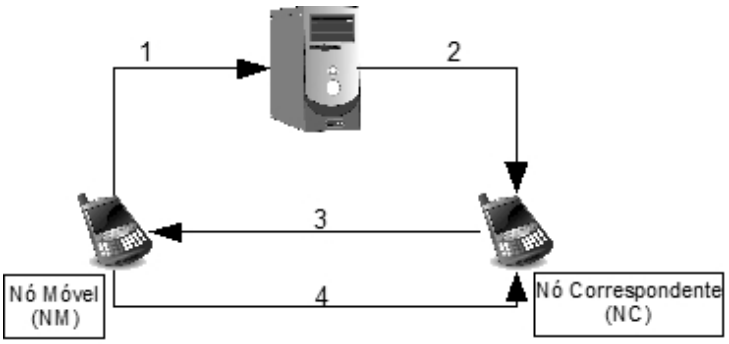


Figura 5.9: Estabelecimento da associação em HIP.

- Algumas limitações de desempenho [Henderson et al. 2003], como o tempo necessário a retomada de atividade das conexões após uma troca da rede de acesso, dificultam o bom funcionamento de aplicações interativas ou com restrições de tempo real.

5.5 Suporte a mobilidade transparente, dada pela rede de acesso

Uma outra abordagem, mais restrita, apresenta soluções em que as próprias redes de acesso oferecem o suporte à mobilidade, com algum grau de transparência ao dispositivo móvel. Este tipo é mais limitado, uma vez que a mobilidade é suportada apenas dentro do domínio de uma rede ou, em casos especiais, através de domínios de redes vizinhas, se estas adotarem solução semelhante.

Um bom exemplo deste tipo de rede *mesh* é a solução SMesh [Amir et al. 2007]. Esta solução utiliza mecanismos de *multicast* com a finalidade de aumentar a taxa de entrega de pacotes ao usuário, quando estes transitam entre regiões cobertas por diferentes pontos de acesso. Duas boas características desta solução são o modo de operação da rede, ad hoc, e a transparência ao dispositivo móvel, já que não precisa executar nenhum processo adicional para realizar a mobilidade. Por operar no modo ad hoc, o SMesh, não sofre com o problema de silêncio por *hand-over*, tendo em vista que em outras soluções, baseadas em modo infra-estruturado [Meraki 2007, Roch 2005, Navda et al. 2005, Ganguly et al. 2006], não é possível realizar a transmissão ao cliente, durante o período correspondente ao processo de desassociação do antigo ponto de acesso e da seguinte associação ao novo ponto.

A contribuição do SMesh é oferecer suporte transparente em modo ad hoc. Uma das questões que muito favorecia a escolha do modo infra-estruturado, em detrimento

do modo ad hoc, é sua falta de mecanismos, especificados no padrão IEEE 802.11, que ajudassem na detecção da movimentação do cliente. Em contrapartida, o modo infraestruturado permite tal detecção pelo processo de reassociação do cliente a um novo ponto de acesso. Tal processo pode ser utilizado para iniciar na reconfiguração da rede, que se ajusta ao novo ponto de contato do dispositivo móvel. A solução do Smesh consistem em utilizar o protocolo DHCP, amplamente implementado em praticamente todos os dispositivos móveis. O campo da resposta, do ponto de acesso ao cliente, T_2, determina o instante em que devem ser reenviados requisições DHCP, em disseminação (*broadcast*). Como conseqüência da disseminação do pedido, todos os pontos de acesso próximos ao dispositivo móvel são capazes de detectar a sua presença.

Outros tipos de rede, que também suportam mobilidade dos usuários, são as redes que utilizam enlaces WDS [802.11 2007] em conjunto com o protocolo Bridge [802.1D 2004]. Contudo, este tipo de rede, apesar de utilizar múltiplos saltos, como fazem as redes *mesh*, não utilizam protocolos de roteamento sensíveis a alguma métrica de enlace, que determine a qualidade das rotas até o destino e, desse modo, são redes pouco escaláveis.

As soluções desta seção possuem duas características, a primeira é o escopo de suporte reduzido, que se restringe apenas a um domínio de rede e, a segunda, é a permissão oferecida aos dispositivos móveis, que apenas implementem corretamente o padrão IEEE 802.11, para realizarem a mobilidade. Como conseqüência, tendo-se em vista essas características, passa a ser potencialmente viável a rápida adoção dessas soluções, uma vez que todo o custo de investimento e o esforço de suporte à mobilidade fica restrito à rede de acesso. Ainda que essa solução se mostre limitada, essa pode ser suficiente para o desenvolvimento de aplicações que atendem determinados nichos de mercado e, assim, desencadear a implementação das soluções mencionadas em outras seções deste capítulo.

Os cenários 1, 2 e 3, que não requerem o suporte a mobilidade inter-domínio, ou macro-mobilidade, são adequadamente atendidos pelas soluções desta seção.

5.6 Questões adicionais de mobilidade

5.6.1 Alocação de endereços

Para um esquema de alocação de endereços em redes *mesh*, é importante identificar cada dispositivo cliente por um endereço localmente único. Para tal, algumas estratégias podem ser adotadas. Na alocação sem estado (*stateless*) não existe um mecanismo centralizado

para distribuir os endereços, portanto os dispositivos atribuem, a si mesmos, endereços únicos, através de três possibilidades:

- Cada dispositivo cliente cria um endereço de forma aleatória, para posteriormente verificar, pelo protocolo de detecção de endereço duplicado (*Duplicate Address Detection*- DAD [Perkins et al. 2001]), a unicidade do endereço criado;
- Uso do mecanismo de configuração de endereço automático definido pelo IPv6 em conjunto com os mecanismos One-hop-DAD [Yunlong et al. 2004] e Weak DAD [Vaidya 2002];
- Utilizar somente os mecanismos do IPv6 como sugerido por [Bechler et al. 2003].

A fim de obter endereços válidos na Internet, cada dispositivo pode usar o prefixo da rede que é periodicamente anunciado pelo *gateway*, ou de forma pró-ativa, enviar um pedido ao *gateway* [Sun et al. 2002]. Outra possibilidade é deixar o prefixo ser automaticamente incluído pelo *gateway*, quando este for encaminhar algum pacote em um enlace externo à rede de acesso. Na alocação com estado (*statefull*), um mecanismo de controle central gerencia a alocação de endereços únicos, através do protocolo DHCP.

5.6.2 Detecção de mobilidade

As técnicas que suportam a mobilidade usualmente necessitam detectar que houve tal evento. A detecção deste evento pode ser classificada em relação a transparência ou sob o ator responsável por implementá-la.

Definimos duas classes de detecção de mobilidade:

1. **Classe I.** O dispositivo é envolvido na gerência das questões de mobilidade;
    - **A - O dispositivo portátil conhece o *gateway* que deve utilizar**, neste caso o equipamento cliente controla de forma explícita a seleção de *gateway*. Este é o caso mais comum da detecção de mobilidade, o que é razoável em redes cujo protocolo de roteamento permite aos clientes conhecerem toda a rota necessária até o *gateway*, permitindo portanto, ao próprio dispositivo cliente gerenciar sua mobilidade;
    - **B - O *gateway* informa ao dispositivo de sua mobilidade**, quando o dispositivo desconhece a rota até o *gateway*, fato comum em redes *mesh*. Este

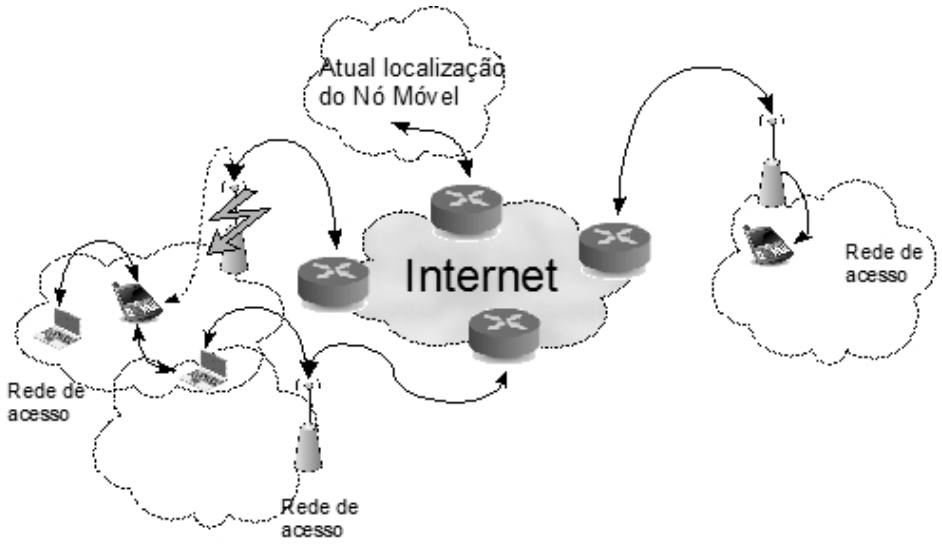


Figura 5.10: Problema de detecção de mobilidade: Por causa da auto-reparação da rede *mesh* em algum salto o cliente Móvel tem alterado o seu *gateway*.

cenário ocorre em redes de múltiplos saltos, que permite a cada salto decidir sobre o encaminhamento do pacote, portanto o dispositivo móvel não é capaz, utilizando seus próprios recursos, de detectar a mudança de *gateway*. Contudo, o *gateway*, ao receber os pacotes, é capaz de identificar a presença de novos clientes e, assim, enviar uma notificação ao dispositivo sobre a sua mobilidade. Ao ser informado, o cliente pode realizar os ajustes necessários. Ilustra-se tal situação na Figura 5.10;

- **C - Controle parcial do cliente**, é quando o cliente utiliza os mecanismos de detecção de pontos de acesso, que analisam a intensidade do sinal proveniente de cada ponto. O próprio dispositivo móvel pode mudar para um novo ponto e, esta decisão pode usar com base na diferença da intensidade do sinal.

2. **Classe II**, O dispositivo não gerencia sua mobilidade. Em diversas situações, pode ser desejável que os protocolos de roteamento de uma sub-rede sem fio ou os clientes móveis não precisem cuidar das questões de mobilidade. Uma opção, que atende este objetivo, é delegar esta função ao *gateway*, que passará a dar o suporte pleno à mobilidade. Neste caso, toda sobrecarga necessária ao suporte do serviço de mobilidade é transferida na sua totalidade ao *gateway*.

5.6.3 Questões de desempenho

A seguir, passa-se a examinar no protocolo TCP as implicações de desempenho que o uso de redes sem fio e mobilidade provocam.

O desempenho do protocolo TCP degrada de forma significativa em redes sem fio. Um motivo bem conhecido da degradação, nas implementações clássicas do protocolo, é a não diferenciação entre perda por congestionamento ou perda causada pela má qualidade do canal de comunicação [Xylomenos et al. 2001]. Como resultado, quando perdas ocorrem por problemas no canal, a vazão da rede decai rapidamente e, quando o canal sem fio volta ao estado de operação normal, o TCP clássico não recupera de forma apropriada o nível de vazão normal. Isto porque, o TCP clássico utiliza mecanismos de contenção de congestionamento, mediante a detecção de perdas. Pelo fato da perda não ter sido causada por congestionamento, estes mecanismos são empregados de modo inadequado.

O bom funcionamento do TCP, em parte, depende do recebimento de pacotes com mensagens ACKs, logo o seu desempenho é severamente influenciado pela assimetria da rede, situação onde as características do caminho de ida e volta diferenciam-se nas medidas de largura de banda, taxa de perda e latência. Em redes *mesh*, os pacotes de dados TCP e de ACK podem tomar rotas muito diferentes, causando assim a assimetria, contudo, mesmo quando o caminho utilizado pelos dois pacotes é o mesmo, as condições do canal de comunicação sem fio podem mudar freqüentemente, novamente causando uma assimetria. Conseqüentemente, o protocolo clássico TCP, projetado para operar em meios de comunicação com qualidade pouco variável, possui um baixo desempenho em redes ad hoc [Petrovic and Aboelaze 2003], e por conseqüência, também em redes *mesh*.

Em redes *mesh*, os roteadores, que formam a sua infra-estrutura, operam no modo ad hoc, onde eventos dinâmicos que alteram as rotas são freqüentes. Considerando diversos fatores como a mobilidade, a qualidade do canal, a carga de utilização e outros, as rotas podem sofrer mudanças com grande freqüência e, conseqüentemente, grandes variações podem ocorrer na medida do RTT (*round trip time*), o que irá degradar o desempenho do TCP, pois este protocolo depende de medições homogêneas do RTT.

Em resumo, os principais problemas do TCP ao ser utilizado em redes ad hoc sem fio são:

- Falta de capacidade de diferenciar perdas de pacotes por congestionamento ou por problemas no canal de comunicação;

- Em caso de mobilidade, breves desconexões podem causar eventos de *timeout* que podem paralisar o envio de dados por um tempo muito maior que o necessário;
- Sensibilidade à assimetria de rotas e flutuações nas medições do RTT.

5.6.4 Impacto da técnica NAT na mobilidade

Assim como no Capítulo 3, a técnica NAT por ser comumente utilizada em redes de acesso, deve também ser considerada na área de mobilidade, pois tal técnica introduz um conjunto de questões, apresentadas a seguir, que dificultam a implementação de algumas técnicas de mobilidade, portanto, é necessário entender estas questões, antes de avaliar as soluções para o problema de mobilidade. Note que o foco é dado as implementações padrões do NAT [Egevang and Francis 1994], e não as implementações especialmente adaptadas à mobilidade, como MobileNAT e VNAT.

O cenário mais simples para interação da mobilidade e da técnica NAT, ocorre tão-somente quando apenas um roteador da rede de acesso realiza a função NAT (Figura 5.11). Neste caso, o suporte a mobilidade é mais simples, pois, basta apenas que o protocolo de roteamento da rede de acesso suporte à mobilidade. Contudo, a proteção, de mudança de endereço, que o NAT oferece ao destinatário não pode ser utilizada se ambos estão estão dentro na mesma rede de acesso, ou seja, a comunicação entre os clientes não passa sobre o *gateway*. Uma solução é capacitar os clientes a utilizar o mesmo protocolo de roteamento de sua rede de acesso.

Em alguns cenários, utilizar NAT em um único roteador pode não ser possível, ou impor um desempenho inadequado. Usualmente, apenas topologias onde todos os *gateways* são suportados por uma única infra-estrutura (*backbone*), e o *gateway* que realiza o NAT está neste *backbone*, mostram-se capazes de suportar, com qualidade, a demanda de roteamento.

Para tornar possível o uso de múltiplos *gateways* com NAT, fora das topologias com as peculiaridades acima, deve-se usar redirecionamentos [Amir et al. 2007]. Uma forma de implementar a troca de pacotes entre *gateways* é pelo uso de túneis, como ilustrado na Figura 5.12. O cliente móvel deve selecionar ao início de cada nova conexão algum *gateway* com NAT e então criar o túnel. Tal túnel cria um enlace virtual direto entre o cliente e o *gateway* selecionado, por meio de encapsulamento IP-over-IP [Perkins 1996b], encapsulamento mínimo (*Minimal Encapsulation*) IP ou *Generic Routing Encapsulation* (GRE) [Farinacci et al. 2000].

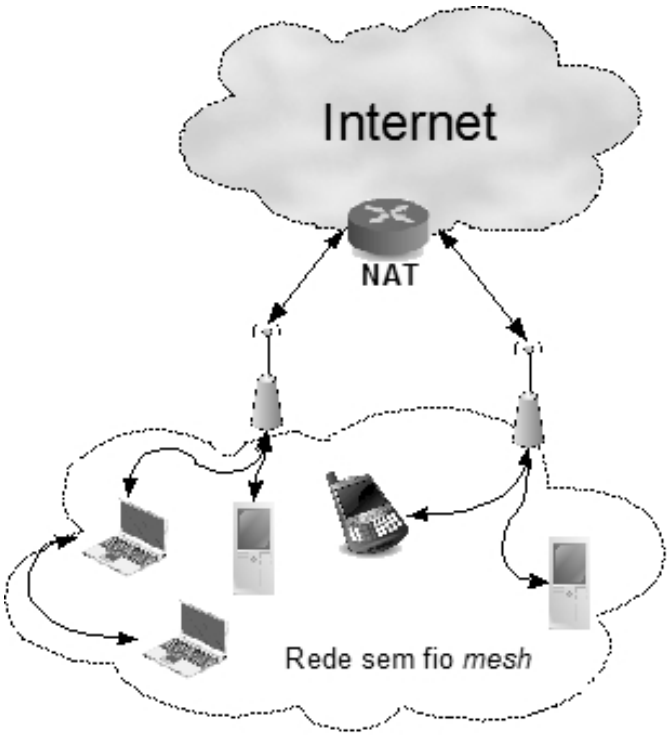


Figura 5.11: Um único *gateway* com NAT atende a todos os *gateways* da rede mesh

Tais técnicas são maneiras de encapsular um pacote original, em um novo pacote, cuja principal diferença é o destino, que passa a ser um *gateway*. O novo pacote ao ser recebido pelo *gateway*, é desfeito para obter o pacote original, que sofre então o processamento pela técnica NAT, e finalmente é encaminhado até o destinatário original. O objetivo do túnel é tornar transparente a rota (*gateways* intermediários) que foi utilizada pela rede, para assegurar que o pacote do dispositivo móvel seja enviado a um determinado *gateway*, que está no final do túnel. Contudo, isso pode obrigar uma implementação específica tanto no *gateway* que está no fim do túnel quanto no cliente móvel, a fim de tratar o encapsulamento e desencapsulamento necessários ao funcionamento do túnel.

A combinação dos termos túnel, *gateway* e NAT também apareceram no Capítulo 3, contudo, agora é o próprio cliente que gerencia as conexões com seus *gateway*, e anteriormente, a rede de acesso esconde qualquer troca de *gateway* ocorrido. Um dos trabalhos futuros do DynTun, é relativo a este cenário, onde é proposto instalar a solução DynTun no dispositivo cliente para a obtenção do suporte à mobilidade.

Outra solução que suporte múltiplos *gateways* com o emprego do NAT, é o uso de dois endereços IP, entre o *gateway* NAT destino do túnel e outros *gateways* NAT intermediários, o que iria tornar NAT similar ao Mobile IPv4 e ao MobileNAT, o que adiciona a possibilidade de macro-mobilidade, que não é possível pelo simples uso do túnel descrito

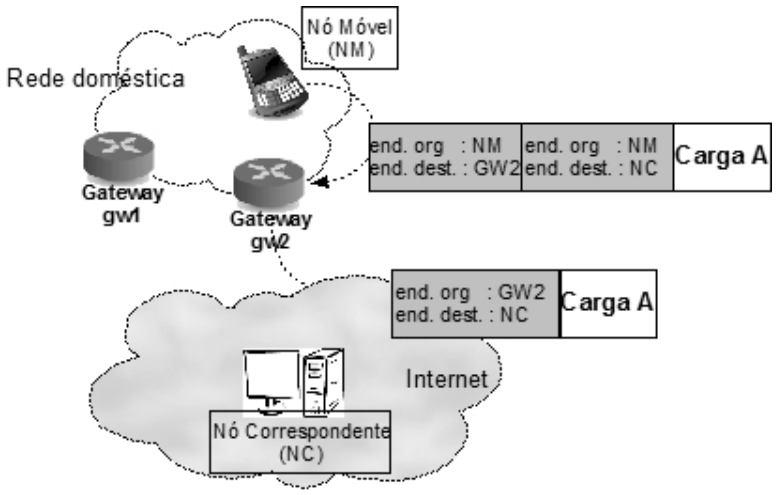


Figura 5.12: Todos os *gateways* realizam NAT; Técnica de tunelamento é necessária.

anteriormente.

Por fim, o uso de NAT é suficiente nos três primeiros cenários, quando o suporte a macro-mobilidade não é necessário, e o emprego da técnica NAT é realizado somente em um equipamento (*gateway*) central. Desta forma, o NAT possui algumas vantagens em relação ao IP Móvel, como a de não necessitar de um endereço adicional, como o endereço fixo (*Home Address*) ou de algum processo de registro no *gateway*. Contudo, no quarto cenário que oferece macro-mobilidade, encontram-se as grandes deficiências desta solução, por causa do grande custo associado a operação de túneis, prejudicando a aplicabilidade do NAT neste cenário mais complexo. Em linhas gerais, as seguintes limitações do NAT em redes *mesh* são:

- A técnica NAT originalmente não possui suporte a mobilidade entre diferentes redes, pois, o cliente precisa estar sob o mesmo *gateway* NAT para não invalidar as conexões. Com a modificação da técnica NAT, ao adicionar uso de túneis entre o primeiro *gateway* NAT e o cliente, este túnel será estendido por um ou mais *gateways* intermediários, conforme a movimentação do cliente em diferentes redes de acesso;

- Cooperação com o padrão IP Móvel requer mecanismos adicionais, como técnicas NAT transverso [Hu 2005] sobre *gateways* com NAT, solução que criaria uma sobrecarga adicional.

- É razoavelmente mais difícil suportar conexões iniciadas por dispositivos, na Internet, para um cliente da rede de acesso que utilize NAT. Existem dois tipos de soluções que são comumente implementadas, o primeiro é a técnica estática de

	Na Rede de Acesso	Nível de Rede	Nível de Transporte	Nível de Aplicação
Dispositivo Adicional	☺	☹	😐	😐
Transparência	☺	😐	☹	😐
Latência	☺	☹	😐	😐
Macro-Mobilidade	☹	☺	😐	☺
Custo	☺	😐	😐	☹
Time To Market	☺	☹	☹	☺

Figura 5.13: Comparação dos tipos de soluções à mobilidade.

encaminhamento por porta (*Port Forwarding*), ou sua variação dinâmica UPnP [Jeronimo and Weast 2003].

5.7 Conclusão do capítulo

Para o aspecto de mobilidade, este trabalho inicialmente descreve quatro cenários de mobilidade, assim como alguns critérios relevantes ao projeto, para auxiliarem na compreensão da existência de diversos tipos mobilidade. No primeiro cenário, o mais simples, cujos desafios já são bem atendidos pelo padrão IEEE 802.11, existe apenas um ponto de acesso e seus clientes. No segundo cenário é adicionado, em relação ao primeiro, a importante característica do uso de múltiplos saltos, a caracterizar, desse modo, uma pequena rede *mesh*. No terceiro cenário se utilizam múltiplos *gateways*, a representar, assim, uma rede *mesh* de larga escala. No quarto e último cenário contemplado, é apresentado uma federação de redes, que permitiria aos usuários um alto grau de liberdade, possibilitando a realização de movimentações por áreas cobertas por redes distintas. Desse modo, as soluções são classificadas de acordo com esses cenários, em razão da existência de desafios diferenciados em cada um deles.

A Figura 5.13 classifica as soluções em quatro tipos, exibidas em colunas, e as avalia segundo seis critérios, em cada linha, sob ponto de vista do usuário.

O primeiro critério corresponde à necessidade de utilizar dispositivos adicionais que sirvam de apoios à solução, como é o caso do *home agent* no IP Móvel. As soluções que envolvem apenas a rede de acesso usualmente reutilizam a infraestrutura de acesso para o suporte à mobilidade, enquanto as soluções de nível de Rede necessitam que equipamentos

externos à rede de acesso sejam utilizados como ponto de apoio. Os demais tipos de soluções podem ou não utilizar um ponto de apoio.

A segundo critério refere-se a transparência dos problemas de mobilidade aos seus clientes. Neste critério as redes de acesso possuem a melhor capacidade de proteger o usuário dos problemas da mobilidade, sem terem de modificar o dispositivo portátil. As soluções do nível de Aplicação podem ser adotadas de forma gradual, iniciando-se pelas aplicações que teriam o maior benefício de suportar a mobilidade, como as aplicações VOIP. Os outros tipos de soluções necessitam que o sistema operacional, ou suas bibliotecas, sejam modificados.

O critério de latência corresponde ao tempo necessário para a retomada das conexões ativas quando é realizada uma troca de ponto de acesso. As soluções de redes de acesso, por envolverem o meio de transmissão, são capazes de detectar e reagir ao evento de mobilidade mais rapidamente. Já, as soluções do Nível de Rede possuem sérias dificuldades em detectar o evento de mobilidade sem prejudicar o desempenho da camada de transporte. Contudo, as soluções baseadas no nível de Transporte podem ser adaptadas para tolerarem e reagirem adequadamente aos eventos de mobilidade. Por fim, as soluções no nível de Aplicação podem adaptar o serviço que oferecem ao usuário para tratar as modificações nas conexões provocadas pela mobilidade.

O quarto critério, de macro-mobilidade, é o ponto chave para atender o quarto cenário. Este é o pior critério para as redes de acesso, pois soluções deste tipo são usualmente específicas para cada rede de acesso. Contudo como redes *mesh* de acesso podem cobrir extensas áreas, esta limitação não necessariamente restringe a mobilidade do usuário. De forma contrastante, as soluções do nível de Rede possuem esta capacidade como ponto mais forte.

O critério de custo, relacionado ao critério de transparência, é melhor atendido pelas soluções nas redes de acesso, visto que usualmente não é necessário qualquer modificação nos dispositivos clientes. As outras soluções necessitam que os sistemas operacionais, ou suas bibliotecas, sejam modificados e, desse modo, as soluções devem suportar as diversas combinações de sistemas operacionais e arquiteturas. O pior tipo neste critério é das soluções no nível de Aplicação, uma vez que estas soluções devem ser replicadas para cada aplicação.

O sexto e último critério, o termo *time to market*, é referente ao tempo necessário para que as soluções sejam implementadas e postas em atividade. As soluções de redes de acesso, por tratarem apenas de micro-mobilidade e pela proximidade do dispositivo

usuário, podem ser rapidamente adotadas. As soluções no nível de Aplicação podem ser utilizadas nas aplicações que possuem o maior benefício no suporte à mobilidade e, portanto, podem ser específicas a um tipo de serviço dado ao usuário.

Uma consideração final é a conclusão desta avaliação, que classifica as melhores soluções a serem adotadas por uma rede *mesh*. Primeiramente as soluções baseadas em redes de acesso são interessantes pois permitem que dispositivos e aplicações existentes possam ser utilizados durante a movimentação do usuário entre área cobertas por diversos pontos de acesso. As soluções no nível de Aplicação são adequadas pois não necessitam de suporte específico à mobilidade na rede de acesso, no sistema operacional ou nas bibliotecas de comunicação, outra vantagem é a proximidade com o usuário e, portanto, é melhor capacitado a modificar o serviço prestado ao usuário.

Com o fim deste capítulo, é completada a apresentação sobre as três áreas chaves desta dissertação, que são as áreas de: gerência, mobilidade e escalabilidade. A seguir, no Capítulo de conclusão, são revistos os pontos mais importantes.

Capítulo 6

Conclusão

É notório que algumas características inerentes à rede *mesh* simplificam a sua operação, como a capacidade de auto-configuração e o baixo custo dos equipamentos. Contudo, essas qualidades não são suficientes para o uso eficiente em redes de larga escala. Para que as redes *mesh* possam efetivamente prover acesso de boa qualidade à população, torna-se imprescindível a investigação de algumas questões nas áreas de escalabilidade, gerência e mobilidade [Muchaluat-Saade et al. 2007].

Conforme descrito no Capítulo 3, os problemas relacionados à escalabilidade são os que causam os maiores impactos no desenvolvimento de uma rede de acesso de larga escala, ao afetar, desse modo, a capacidade de escoamento dos dados entre a Internet e seus usuários. Dentro do conjunto de empecilhos existentes, parte considerável se origina na tecnologia de transmissão de dados em redes sem fio Wi-Fi, que utiliza a comunicação por rádio que compartilha o meio de comunicação com outras entidades, o que causa inúmeras dificuldades. Tal situação impede o uso contínuo da rede pelos seus usuários, tendo em vista as interferências causadas pelos demais clientes de redes sem fio, bem como as resultantes de diversas outras fontes, valendo mencionar: os telefones sem fio e os fornos de microondas. Como última limitação, foi destacada a atenuação do sinal de rádio, cuja intensidade varia conforme a distância existente entre o emissor e o receptor, reduzindo o seu desempenho e, conseqüentemente, também afetando negativamente o desempenho da rede. Convém ressaltar que a característica de múltiplos saltos de redes *mesh* amplia a dimensão desses obstáculos, uma vez que os efeitos negativos acumulam-se a cada salto, que um pacote de dados dá em direção ao *gateway*.

Diante dos problemas impostos pela tecnologia sem fio Wi-Fi, verifica-se a possibilidade de abrandar as suas influências no desempenho de redes *mesh*. Nesse sentido, tem-se uma solução proposta intitulada DynTun [Duarte et al. 2008], que visa a distribuir e diminuir o uso dos enlaces sem fio, reduzindo os prejudiciais eventos de colisões e de

interferências. Isso porque, apesar do tráfego de dados ser distribuído a diversos *gateways*, ainda assim, a simples combinação das técnicas de *multi-homing* e NAT pode ter como resultado um indesejável efeito negativo, a saber, a quebra de uma grande quantidade de conexões, como demonstrado no primeiro teste na Seção 3.6. Essa conseqüência, que evidentemente prejudica a qualidade percebida pelo usuário, pode ser evitada através dos mecanismos oferecidos pelo DynTun.

É constatado, na Subseção 3.6.2, que a implementação da solução DynTun melhora consideravelmente o acesso dos clientes à Internet. Inclusive a Tabela 3.2 demonstra que DynTun é capaz de tornar mais justa a competição, pelo uso da rede de acesso, entre os dois dispositivos clientes utilizados.F

Observa-se que a implementação do DynTun, apesar de ter sido feita no âmbito do Projeto Remesh, é também aplicável a outras redes sem fio, uma vez que os critérios descritos na Seção 3.2 são tão restritivos que facilitam a sua adaptação às características de outras redes. Salienta-se que o mecanismo de descoberta de *gateways*, assim como a técnica de medição da qualidade das rotas, correspondem aos dois itens que possivelmente sofreriam alguma adaptação em outros tipos de redes mesh. No caso do DynTun, ambos os itens foram reutilizados do protocolo OLSR.

A tarefa de gerenciar uma rede de acesso, de modo a torná-la menos trabalhosa aos operadores humanos, requer o uso de um conjunto de ferramentas. O gerenciamento desejável usualmente consiste na possibilidade de se dispender a menor quantidade de esforço para acompanhar o funcionamento da rede, detectar as falhas e suas origens, assim como efetuar as correções eventualmente necessárias. Conforme descrito no Capítulo 4, as redes do tipo *mesh* impõem alguns desafios, como o uso de dispositivos com capacidade limitada, a dependência de uso exclusivo do meio de comunicação sem fio, a instabilidade causada por variações na qualidade dos enlaces e as barreiras sobre localização dos pontos de infra-estrutura em locais de difícil acesso.

Como conseqüência destes desafios, é definido neste trabalho que as ferramentas adotadas no gerenciamento de redes *mesh* devem atender alguns critérios, como a dependência mínima de interação com seres humanos, a confiabilidade, a resistência a falhas e, por fim, o baixo consumo de espaço na memória permanente e de processamento.

A fim de exemplificar como uma ferramenta é importante para diminuir o trabalho dos administradores, na Subseção 4.2.1, é proposto um simples *shell script*, que auxilia a configuração inicial dos equipamentos de rádio. Esse *script* modifica um grande conjunto de configurações indispensáveis, a fim de possibilitar que um ponto de acesso

padrão passe a operar como um ponto da rede *mesh*. Tal ferramenta torna o processo de configuração inicial tão simples, a permitir que pessoas com um treinamento básico, tornem-se capazes de efetuar a operação sem erros. Sem este *script*, era necessário que um experiente administrador efetuasse a operação e, ainda assim, o processo era demorado, valendo mencionar que em diversas ocasiões o resultado da operação não era adequado na primeira tentativa. Outro exemplo é a medição da banda disponível às aplicações clientes, que com o sistema de estatísticas, passou a ser realizado de forma periódica e automática [Duarte et al. 2007].

Para o aspecto de mobilidade, este trabalho inicialmente descreve quatro cenários de mobilidade, assim como alguns critérios relevantes ao projeto, para auxiliarem na compreensão da existência de diversos tipos mobilidade. No primeiro cenário, o mais simples, cujos desafios já são bem atendidos pelo padrão IEEE 802.11, existe apenas um ponto de acesso e seus clientes. No segundo cenário é adicionado, em relação ao primeiro, a importante característica do uso de múltiplos saltos, a caracterizar, desse modo, uma pequena rede *mesh*. No terceiro cenário se utilizam múltiplos *gateways*, a representar, assim, uma rede *mesh* de larga escala. No quarto e último cenário contemplado, é apresentada uma federação de redes, que permitiria aos usuários um alto grau de liberdade, possibilitando a realização de movimentações por áreas cobertas por redes distintas [Abelém et al. 2007].

Como cada cenário possui desafios diferenciados, as soluções são descritas de acordo com as suas particularidades. Outra forma de classificação das soluções é com relação ao item de transparência, uma vez que algumas opções oferecem transparência a entidades diferentes, como exemplo a rede de acesso ou ao dispositivo móvel.

É importante não confundir o critério de suporte a múltiplos *gateways* das soluções do Capítulo 5 com o DynTun, já que no caso do DynTun o problema a ser resolvido é de total responsabilidade da rede de acesso, pois este critério resulta de uma decisão dos administradores da rede de acesso, não do usuário e, por isso, todo o suporte a múltiplos *gateways* deve ser implementado sem qualquer participação do dispositivo móvel ou do usuário. Entretanto, em relação ao suporte à mobilidade de dispositivos portáteis, é razoável supor que a responsabilidade de resolver os problemas relacionados ao suporte venham a ser compartilhados entre o dispositivo e a rede, posto que ambos visam a possibilidade de uso, pelo usuário, dos serviços da rede durante a movimentação pelas áreas cobertas por vários pontos de acesso.

Outra classificação das soluções de mobilidade é com relação à entidade que deverá ser modificada para o seu suporte.

O primeiro tipo oferece as melhores características de suporte, caracterizado quando ambos, a rede de acesso e o dispositivo móvel, devem sofrer modificações. Este primeiro tipo é melhor representado pela solução IP Móvel. Existe uma grande expectativa nessa solução, no sentido de tornar o uso de dispositivos móveis bastante atrativo, caso seja adotada de forma ampla. A principal vantagem oferecida pelo IP Móvel é permitir o uso de diversas redes de acesso, de alto desempenho e de curto alcance, uma rede por vez, mudando sempre que uma nova rede de acesso for considerada melhor por qualquer motivo. O potencial do IP Móvel é plenamente explorado se utilizado em conjunto com IPv6, contudo, a adoção do IPv6 não ocorrerá no curto prazo.

Uma solução alternativa é o MobileNAT, que não possui o mesmo problema de adoção do IP Móvel, pois ao contrário da solução anterior, o MobileNAT afasta a exigência de modificar toda a infra-estrutura da Internet para funcionar de forma ótima, necessitando apenas da introdução de um equipamento, com finalidade de ser um ponto de apoio de uma extensão do protocolo DHCP, e a adição de um nível na pilha de protocolos de rede, para realizar as traduções de endereços necessários. Contudo, se o dispositivo móvel transitar apenas em redes onde seus *gateways* tenham a infra-estrutura do MobileNat, é dispensável qualquer modificação no dispositivo móvel. Em qualquer situação, os dispositivos na Internet, que estabelecem alguma comunicação com o equipamento portátil, não precisam ser modificados, assim como a infra-estrutura da Internet. Por esses motivos, a adoção do MobileNAT pode ocorrer com menos esforço, se comparado à solução mais indicada, o IP Móvel.

Assim como o MobileNAT, existe um outro tipo de solução à mobilidade que introduz um nível adicional na pilha de protocolos de rede, o HIP. Como o MobileNAT, a solução HIP acrescenta uma nova camada para tratar as questões de mobilidade e também utiliza um equipamento na Internet para auxiliar na comunicação. Todavia, diferentemente, utiliza uma abordagem par-a-par (p2p), diminuindo, desse modo, a carga de uso do equipamento auxiliador. O HIP e o IP Móvel possuem bom desempenho, contudo, em situações de grande freqüência de mudança de endereço, essas soluções demonstram problemas de desempenho [Henderson et al. 2003].

O terceiro tipo de solução, que utiliza mecanismos no nível de Aplicação, é o que possui o maior potencial para um rápida adoção. Pode ser considerado que uma das principais motivações que leva o usuário a utilizar um dispositivo portátil são os serviços de dados, oferecidos pelas aplicações. Para que estas aplicações sejam capazes de oferecer serviços atrativos, é necessário que estes tenham acesso aos dados requisitados. Caso

os recursos oferecidos pela rede não se mostrarem suficientes ou adequados aos requisitos das aplicações, alguns mecanismos de compensação podem ser implementados diretamente pela aplicação. Essa adaptação faz com que, em um segundo momento, a demanda dos usuários pelas aplicações adaptadas justifique a alteração na infra-estrutura de rede, a fim de generalizar o suporte necessário.

Uma abordagem mais restrita criou o quarto tipo de solução, em que as próprias redes de acesso oferecem o suporte à mobilidade, com algum grau de transparência ao dispositivo do usuário. Este tipo é o mais limitado, visto que a mobilidade é suportada apenas dentro do domínio de uma rede ou, em casos especiais, através de domínios de redes vizinhas, se estas adotarem solução semelhante. Exemplos desse tipo de rede *mesh* são relatados em [Roch 2005, Meraki 2007, Amir et al. 2007] ou por uma rede de múltiplos saltos, similar a *mesh*, que utiliza um conjunto de enlaces WDS [802.11 2007] com bridge [802.1D 2004]. Por ser o escopo mais restrito e por permitir que dispositivos realizem mobilidade, com a simples implementação correta do padrão IEEE 802.11, essa abordagem possui o melhor potencial de rápida adoção, uma vez que todo custo de investimento e esforço de suporte à mobilidade fica restrita à rede de acesso e, ainda assim, pode ser suficiente para que aplicações que atendam certos nichos de mercado possam se desenvolver.

6.1 Contribuições

Para o problema de escalabilidade e a solução DynTun, o autor desda dissertação divide a autoria com um outro colega de projeto. As contribuições mais significativas deste autor são:

- Planejamento dos testes, que demonstram o problema de escalabilidade;
- Pesquisa bibliográfica, e a conseqüente avaliação das técnicas encontradas;
- Projeto da solução;
- Pesquisa dos mecanismos de implementação;
- Determinação do impacto do DynTun nos mecanismos anteriormente utilizados na rede Remesh.
- Planejamento dos testes de avaliação da solução.

As contribuições deste autor na área de gerência, resumidamente, são:

- Identificar e descrever as questões relacionadas a rede *mesh*;
- Determinar os critérios para a seleção e o desenvolvimento de ferramentas;
- Idealização do conceito das ferramentas BShell e BCP;
- Projeto da ferramenta de estatísticas;
- Adaptação do Wifidog, para o suporte a múltiplos *gateways*;
- Definição dos problemas em aberto.

Na área de suporte à mobilidade, pode-se destacar as contribuições seguintes:

- Pesquisa bibliográfica;
- Determinar os cenários de mobilidade, relevantes a rede *mesh*;
- Classificar as técnicas encontradas nos quesitos de transparência e o nível, da pilha de protocolos de rede, a que pertencem;
- Identificação, nas técnicas existentes, questões relacionadas a rede *mesh*.

6.2 Publicações

Esta dissertação é o resultado de um conjunto de pesquisas e de desenvolvimento de soluções, realizados no projeto Remesh e, dentre os frutos destes esforços, quatro trabalhos foram publicados pelo autor desta dissertação.

O primeiro artigo, com o título de "DynTun: Túneis Dinâmicos e a Escalabilidade de Redes em Malha", foi aceito no SBRC de 2008, e serviu de base do Capítulo 3.

O Capítulo 4, sobre gerência, é baseado no artigo, intitulado de "Management Issues on Wireless Mesh Networks", que foi publicado no evento LANOMS de 2007,

O terceiro trabalho, denominado "Redes Mesh: Mobilidade, Qualidade de Serviço e Comunicação em Grupo", é um minicurso de SBRC 2007. A parte relacionada à mobilidade serviu como base ao Capítulo 5.

O projeto Remesh foi apresentado em "Redes em Malha: Solução de Baixo Custo para Popularização do Acesso à Internet no Brasil", no SBRT de 2007.

6.3 Trabalhos futuros

Em relação a solução DynTun é possível adicionar melhorias que considerem a capacidade, o custo e o nível de utilização de cada *gateway*, aplicando alguns conceitos de balanceamento de custo, como visto em [Goldenberg et al. 2004]. Conforme aplicativos com características interativas, como VoIP, são utilizadas na rede Remesh algumas questões ligadas a QoS, que devem influenciar na escolha do *gateway*. Adicionalmente, nenhum cuidado foi empregado para atender a restrição das aplicações, que empregam múltiplas conexões paralelas, que demandam que todas as conexões tenham endereço de origem iguais. Essa restrição não é atendida pelo DynTun, uma vez que este apenas providencia que os pacotes de uma conexão sejam roteados à Internet pelo mesmo *gateway* com NAT, entretanto, não cuida que todas as conexões de uma aplicação sejam roteadas por um único *gateway*, como seria necessário, a fim de atender à citada restrição.

Para a questão do suporte a mobilidade é indispensável dar prosseguimento ao desenvolvimento de técnicas baseadas no nível de Aplicação, até o momento em que alguma solução, ao nível de Rede, venha a ser amplamente implantada. Uma proposta como apresentada por [Wedlund and Schulzrinne 1999] que utiliza os mecanismos de sinalização do SIP pode ser adotada como ponto inicial de desenvolvimento, visto que inúmeras questões de desempenho ainda precisam ser trabalhadas.

Uma interessante proposta é investigar se a instalação do DynTun, que atualmente é uma técnica de melhora na escalabilidade, no dispositivo cliente é suficiente para a implementação de uma técnica de suporte a mobilidade em redes *mesh* que operem com o mesmo protocolo de roteamento, o OLSR-ML.

6.4 Últimas ponderações

As redes de acesso à Internet, baseadas na tecnologia sem fio Wi-Fi, podem aumentar suas capacidades ao adotar as técnicas de redes *mesh*. Esta melhoria consiste na capacidade de expansão da área cobertura, capacidade de provimento de acesso por banda larga, capacidade de gerenciar a rede de acesso e a capacidade de suportar a mobilidade dos dispositivos clientes.

As técnicas apresentadas nestes trabalho, cobrindo três importantes áreas de uma rede de acesso sem fio, podem ser utilizadas no desenvolvimento de redes de acesso a Internet bem sucedida, com baixo custo e, portanto, redes *mesh* são um meio adequado para a

inclusão digital.

Referências

[802.11 2007] 802.11, I. (2007). Ieee standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements - part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications. *IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999)*, pages C1–1184.

[802.11s 2006] 802.11s, I. (2006). IEEE P802.11s/D0.02, Draft Amendment to Standard for Information Technology - Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Amendment: ESS Mesh Networking. Junho 2006.

[802.1D 2004] 802.1D, I. (2004). Ieee standard for local and metropolitan area networks media access control (mac) bridges. *IEEE Std 802.1D-2004 (Revision of IEEE Std 802.1D-1998)*, pages 1–269.

[Abelém et al. 2007] Abelém, A. J. G., de Albuquerque, C. V. N., Muchaluat-Saade, D. C., Aguiar, E. S., Duarte, J. L., da Fonseca, J. E. M., and Magalhães, L. C. S. (2007). Redes mesh: Mobilidade, qualidade de serviço e comunicação em grupo. *Minicurso do SBRC 2007, capítulo 2.*

[Akella et al. 2003] Akella, A., Maggs, B., Seshan, S., Shaikh, A., and Sitaraman, R. (2003). A measurement-based analysis of multihoming. In *SIGCOMM '03: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 353–364, New York, NY, USA. ACM.

[Akyildiz et al. 2005] Akyildiz, I. F., Wang, X., and Wang, W. (2005). Wireless mesh networks: a survey. *Comput. Netw. ISDN Syst.*, 47(4):445–487.

[Amir et al. 2007] Amir, Y., Danilov, C., Musaloiu-Elefteri, R., and Rivera, N. (2007). An inter-domain routing protocol for multi-homed wireless mesh networks. *World of Wireless, Mobile and Multimedia Networks, 2007. WoWMoM 2007. IEEE International Symposium on a*, pages 1–10.

[Badonnel et al. 2005] Badonnel, R., State, R., and Festor, O. (2005). Management of mobile ad hoc networks: information model and probe-based architecture. *Int. J. Netw. Manag.*, 15(5):335–347.

[Balakrishnan et al. 1995] Balakrishnan, H., Seshan, S., Amir, E., and Katz, R. (1995). Improving tcp/ip performance over wireless networks. *Proc. 1st ACM Conf. on Mobile Computing and Networking.*

[Bates and Rekhter 1998] Bates, T. and Rekhter, Y. (1998). Scalable support for multi-homed multi-provider connectivity. RFC Experimental 2260, Internet Engineering Task Force.

[Bechler et al. 2003] Bechler, M., Franz, W., and Wolf, L. (2003). Mobile Internet Access in FleetNet. *13. Fachtagung Kommunikation in verteilten Systemen, Leipzig, Germany.*

[Bicket et al. 2005] Bicket, J., Aguayo, D., Biswas, S., and Morris, R. (2005). Architecture and evaluation of an unplanned 802.11b mesh network. In *MobiCom '05: Proceedings of the 11th annual international conference on Mobile computing and networking*, pages 31–42.

[Bondareva et al. 2006] Bondareva, O., Baumann, R., and ETH-Zentrum, S. (2006). Handling addressing and mobility in hybrid wireless mesh networks. Technical report, Swiss Federal Institute of Technology.

[Broadcom 2008] Broadcom (2008). Especificação do hardware bcm4712 - http://www.broadcom.com/products/Wireless-LAN/802.11-Wireless-LAN-Solutions/BCM4712. Acessado em 22-03-2008.

[Brown and Singh 1997] Brown, K. and Singh, S. (1997). M-tcp: Tcp for mobile cellular networks. *SIGCOMM Comput. Commun. Rev.*, 27(5):19–43.

[Bruno et al. 2005] Bruno, R., Conti, M., and Gregori, E. (2005). Mesh networks: Commodity multihop ad hoc networks. *IEEE Communications Magazine*, pages 123–131.

[Buddhikot et al. 2005] Buddhikot, M., Hari, A., Singh, K., and Miller, S. (2005). MobileNAT: A New Technique for Mobility Across Heterogeneous Address Spaces. *Mobile Networks and Applications*, 10(3):289–302.

[Campista et al. 2007] Campista, M. E. M., Passos, D. G., Esposito, P. M., Moraes, I. M., de Albuquerque, C. V. N., Muchaluat-Saade, D., Rubinstein, M. G., Costa, L. H. M. K., and Duarte, O. C. M. B. (2007). Routing metrics and protocols for wireless mesh networks. *IEEE Network Magazine*. Aceito para publicação em 2007.

[Case et al. 1990] Case, J. D., Fedor, M., Schoffstall, M. L., and Davin, J. (1990). Simple network management protocol (SNMP). RFC Experimental 1157, Internet Engineering Task Force.

[Cisco 2006] Cisco (2006). Cisco wireless mesh networking solution. http://www.cisco.com/go/wirelessmesh Acessado em 01/04/2008.

[Clausen and Jacquet 2003a] Clausen, T. and Jacquet, P. (2003a). Optimized link state routing protocol (olsr). RFC Experimental 3626, Internet Engineering Task Force.

[Clausen and Jacquet 2003b] Clausen, T. and Jacquet, P. (2003b). Optimized link state routing protocol (OLSR). RFC Experimental 3626, Internet Engineering Task Force.

[Couto et al. 2003] Couto, D. S. J. D., Aguayo, D., Bicket, J., and Morris, R. (2003). A high-throughput path metric for multi-hop wireless routing. In *MobiCom '03: Proceedings of the 9th annual international conference on Mobile computing and networking*, pages 134–146, New York, NY, USA. ACM Press.

[Deri and Suin 2000] Deri, L. and Suin, S. (2000). Effective traffic measurement using ntop. *IEEE Communications Magazine*, 38(5):138–143.

[Draves et al. 2004a] Draves, R., Padhye, J., and Zill, B. (2004a). Comparison of routing metrics for static multi-hop wireless networks. In *ACM SIGCOMM*.

[Draves et al. 2004b] Draves, R., Padhye, J., and Zill, B. (2004b). Routing in multi-radio, multi-hop wireless mesh networks. In *MobiCom '04: Proceedings of the 10th annual international conference on Mobile computing and networking*, pages 114–128, New York, NY, USA. ACM Press.

[Duarte et al. 2008] Duarte, J., Passos, D., and Albuquerque, C. (2008). "dyntun: Túneis dinâmicos e a escalabilidade de redes em malha". *Simpósio Brasileiro de Redes de Computadores (SBRC 2008)*.

[Duarte et al. 2007] Duarte, J., Passos, D., Valle, R., Oliveira, E., Muchaluat-Saade, D. C., and Albuquerque, C. (2007). Management issues on wireless mesh networks. In *5th Latin American Network Operations and Management Symposium (LANOMS 2007)*.

[Egevang and Francis 1994] Egevang, K. and Francis, P. (1994). The IP network address translator (NAT). RFC Experimental 1631, Internet Engineering Task Force.

[ElBatt et al. 2000] ElBatt, T. A., Krishnamurthy, S. V., Connors, D., and Dao, S. K. (2000). Power management for throughput enhancement in wireless ad-hoc networks. In *ICC (3)*, pages 1506–1513.

[Engelstad et al. 2004] Engelstad, P. E., Tonnesen, A., Hafslund, A., and G.Egeland (2004). Internet connectivity for multi-homed proactive ad hoc networks. *2004 IEEE International Conference on Communications*, 7:4050–4056.

[Farinacci et al. 2000] Farinacci, D., Li, T., Hanks, S., Meyer, D., and Traina, P. (2000). Generic routing encapsulation (GRE). RFC Experimental 2784, Internet Engineering Task Force.

[FatPipe 2007] FatPipe, N. I. (2007). http://www.fatpipeinc.com/. Acessado em 03-02-2007.

[Ferguson and Senie 1998] Ferguson, P. and Senie, D. (1998). RFC2267: Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. *Internet RFCs*.

[Fikouras et al. 1999] Fikouras, N., El Malki, K., Cvetkovic, S., and Smythe, C. (1999). Performance of tcp and udp during mobile ip handoffs in single-agent subnetworks. *Wireless Communications and Networking Conference, 1999. WCNC. 1999 IEEE*, pages 1258–1262 vol.3.

[Ganguly et al. 2006] Ganguly, S., Navda, V., Kim, K., Kashyap, A., Niculescu, D., Izmailov, R., Hong, S., and Das, S. (2006). Performance Optimizations for Deploying VoIP Services in Mesh Networks. *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, 24(11):2147.

[Goldenberg et al. 2004] Goldenberg, D. K., Qiuy, L., Xie, H., Yang, Y. R., and Zhang, Y. (2004). Optimizing cost and performance for multihoming. In *SIGCOMM '04: Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 79–92, New York, NY, USA. ACM.

[Griswold et al. 2004] Griswold, W. G., Shanahan, P., Brown, S. W., Boyer, R., Ratto, M., Shapiro, R. B., and Truong, T. M. (2004). Activecampus - experiments in community-oriented ubiquitous computing. *IEEE Computer*.

[Guo et al. 2004] Guo, F., Chen, J., Li, W., and cker Chiueh, T. (2004). Experiences in building a multihoming load balancing system. *INFOCOM 2004: Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, 2:1241–1251.

[Henderson et al. 2003] Henderson, T., Ahrenholz, J., and Kim, J. (2003). Experience with the host identity protocol for secure host mobility and multihoming. *Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE*, 3:2120–2125 vol.3.

[Ho et al. 2004] Ho, C., Ramachandran, K., Almeroth, K. C., and Belding-Royer, E. M. (2004). A scalable framework for wireless network monitoring. In *ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots*.

[Hu 2005] Hu, Z. (2005). NAT Traversal Techniques and Peer-to-Peer Applications. *Seminar on Internetworking*.

[IBGE 2008] IBGE (2008). Pnad 2006, síntese de indicadores www.ibge.gov.br/home/estatistica/populacao/trabalhoerendimento/pnad2006. Acessado em 10/Março/2008.

[Iptables and NetFilter 2007] Iptables and NetFilter (2007). http://www.iptables.org/. Acessado em 03-02-2007.

[Jeronimo and Weast 2003] Jeronimo, M. and Weast, J. (2003). *UPnP Design by Example: A Software Developer's Guide to Universal Plug and Play*. Intel Press.

[Johnson et al. 2004] Johnson, D., Perkins, C., and Arkko, J. (2004). RFC3775 Mobility Support in IPv6. *Mobility Support in IPv6. Network Working Group. June*.

[Johnson et al. 2001] Johnson, D. B., Maltz, D. A., and Broch, J. (2001). DSR: the dynamic source routing protocol for multihop wireless ad hoc networks.

[Jönsson et al. 2000] Jönsson, U., Alriksson, F., Larsson, T., Johansson, P., and Maguire Jr, G. (2000). MIPMANET: mobile IP for mobile ad hoc networks. *Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing*, pages 75–85.

[Justin and Nelson 1994] Justin, C. and Nelson, S. (1994). Performance of autonomous dynamic channel assignment and power control for tdma/fdma wireless access. *IEEE Journal On Selected Areas In Communications*, 12(8):1314–1323.

[Kniveton et al. 2002] Kniveton, T. J., Malinen, J., Devarapalli, V., and C.Perkins (2002). Mobile router tunneling protocol. Internet draft, Internet Engineering Task Force.

[Koksal and Balakrishnan 2006] Koksal, C. E. and Balakrishnan, H. (2006). Quality-aware routing metrics for time-varying wireless mesh networks. *IEEE Journal On Selected Areas In Communications*, 24(11):1984–1994.

[Koponen et al. 2005] Koponen, T., Gurtov, A., and Nikander, P. (2005). Application mobility with hip. In *Proceedings of ICT*.

[Kyasanur and Vaidya 2005] Kyasanur, P. and Vaidya, N. (2005). Routing and interface assignment in multi-channel multi-interface wireless networks. In *Wireless Communications and Networking Conference*, volume 4, pages 2051– 2056.

[Leech et al. 1996] Leech, M., Ganis, M., Lee, Y., Kuris, R., Koblas, D., and Jones, L. (1996). RFC1928: SOCKS Protocol Version 5. *Internet RFCs*.

[Lei and Perkins 1997] Lei, H. and Perkins, C. (1997). Ad Hoc Networking with Mobile IP. *Proceedings of the 2nd European Personal Mobile Communications Conference*, pages 197–202.

[Leinwand and Conroy 1996] Leinwand, A. and Conroy, K. F. (1996). *Network management (2nd ed.): a practical perspective*. Addison Wesley Longman Publishing Co., Inc., Redwood City, CA, USA.

[Lenczner 2005] Lenczner, M. (2005). Wireless portals with wifidog. *Linux J.*, 2005(140):8.

[M. Lad and Kirstein 2005] M. Lad, S. Bhatti, S. H. and Kirstein, P. (2005). Enabling coalition-based community networking. In *The London Communications Symposium (LCS)*.

[Meraki 2007] Meraki (2007). http://meraki.com/. Acessado em 5/Julho/2007.

[Montenegro et al. 1998] Montenegro, G. et al. (1998). Reverse Tunneling for Mobile IP. Technical report, RFC 2344, May 1998.

[Muchaluat-Saade et al. 2007] Muchaluat-Saade, D. C., Albuquerque, C., Magalhães, L. C. S., Passos, D., Duarte, J., and Valle, R. (2007). Redes em malha: Solução de baixo custo para popularização do acesso à internet no brasil. In *Simpósio Brasileiro de Telecomunicações (SBrT 2007)*.

[Nakajima et al. 2003] Nakajima, N., Dutta, A., Das, S., and Schulzrinne, H. (2003). Handoff delay analysis and measurement for SIP based mobility in IPv6. *Communications, 2003. ICC'03. IEEE International Conference on*, 2:1085–1089.

[Navda et al. 2005] Navda, V., Kashyap, A., and Das, S. R. (2005). Design and evaluation of imesh: An infrastructure-mode wireless mesh network. *wowmom*, 1:164–170.

[Netequality 2006] Netequality, P. (2006). http://www.netequality.com/. Acessado em 5/Julho/2007.

[Networks 2007a] Networks, F. (2007a). http://www.f5.com/. Acessado em 03-02-2007.

[Networks 2007b] Networks, N. (2007b). http://www.nortelnetworks.com/. Acessado em 03-02-2007.

[OLPC 2005] OLPC (2005). http://laptop.org. Acessado em Março/2007.

[OpenWrt 2007] OpenWrt (2007). http://openwrt.org/. Acessado em 03-03-2008.

[Passos and Albuquerque 2007] Passos, D. and Albuquerque, C. (2007). Proposta, implementação e análise de uma métrica de roteamento multiplicativa para redes em malha sem fio. *Revista Eletrônica de Iniciação Científica (REIC)*.

[Passos et al. 2006] Passos, D., Teixeira, D., Muchaluat-Saade, D., Magalhães, L. S., and Albuquerque, C. (2006). Mesh network performance measurements. In *5th International Information and Telecommunicatios Technologies Symposium*.

[Perkins 1996a] Perkins, C. (1996a). Mobile-IP, ad-hoc networking, and nomadicity. *Computer Software and Applications Conference, 1996. COMPSAC'96., Proceedings of 20th International*, pages 472–476.

[Perkins 1996b] Perkins, C. (1996b). RFC2003: IP Encapsulation within IP. *Internet RFCs*.

[Perkins 2002] Perkins, C. (2002). Ip mobility support for ipv4.

[Perkins et al. 2002] Perkins, C. et al. (2002). IP Mobility Support for IPv4.

[Perkins et al. 2001] Perkins, C., Malinen, J., Wakikawa, R., Belding-Royer, E., and Sun, Y. (2001). IP Address Autoconfiguration for Ad Hoc Networks. *IETF Draft*.

[Perkins et al. 2003] Perkins, C. E., Belding-Royer, E. M., and Das, S. R. (2003). Ad hoc on-demand distance vector (AODV) routing. RFC Experimental 3561, Internet Engineering Task Force.

[Petrovic and Aboelaze 2003] Petrovic, M. and Aboelaze, M. (2003). Performance of tcp/udp under ad hoc ieee802.11. *Telecommunications, 2003. ICT 2003. 10th International Conference on*, 1:700–708 vol.1.

[Radware 2007] Radware (2007). http://www.radware.com/. Acessado em 03-02-2007.

[Ramachandran et al. 2004] Ramachandran, K., Belding-Royer, E., and Almeroth, K. (2004). Damon: a distributed architecture for monitoring multi-hop mobile networks. In *IEEE International Conference on Sensor and Ad hoc Communications and Networks*.

[Ramakrishna 2001] Ramakrishna, P. F. (2001). Ipnl: A NAT-extended internet architecture. In *the 2001 SIGCOMM conference*, pages 69–80. ACM.

[Ramanathan and Hain 2000] Ramanathan, R. and Hain, R. (2000). Topology control of multihop wireless networks using transmit power adjustment. In *INFOCOM (2)*, pages 404–413.

[Ramjee et al. 2002] Ramjee, R., Varadhan, K., Salgarelli, L., Thuel, S., Wang, S., and La Porta, T. (2002). HAWAII: a domain-based approach for supporting mobility in wide-area wireless networks. *IEEE/ACM Transactions on Networking (TON)*, 10(3):396–410.

[Raniwala et al. 2004] Raniwala, A., Gopalan, K., and cker Chiueh, T. (2004). Centralized channel assignment and routing algorithms for multi-channel wireless mesh networks. *SIGMOBILE Mob. Comput. Commun. Rev.*, 8(2):50–65.

[Ratnam and Matta 1998] Ratnam, K. and Matta, I. (1998). Wtcp: an efficient mechanism for improving tcp performance over wireless links. *Computers and Communications, 1998. ISCC '98. Proceedings. Third IEEE Symposium on*, pages 74–78.

[Rether 2007] Rether, N. I. (2007). http://www.rether.com/. Acessado em 03-02-2007.

[Ricardo C. Carrano and Magalhães 2007] Ricardo C. Carrano, M. B. and Magalhães, L. C. S. (2007). Mesh networks for digital inclusion - testing olpc's xo mesh implementation. In *8o Forum Internacional de Software Livre*.

[Roch 2005] Roch, S. (2005). Nortel's wireless mesh network solution: Pushing the boundaries of traditional wlan technology. Technical Report Issue 2, Nortel Technical Journal.

[RouteScience 2007] RouteScience (2007). http://www.routescience.com. Acessado em 03-10-2007.

[Saltzer et al. 1984] Saltzer, J., REED, D., and CLARK, D. (1984). End-to-end arguments in system design. *Technology*, 100:0661.

[Santivanez et al. 2002] Santivanez, C., McDonald, B., Stavrakakis, I., and Ramanathan, R. (2002). On the scalability of ad hoc routing protocols. In *IEEE INFOCOM*.

[Santivanez and Ramanathan 2003] Santivanez, C. and Ramanathan, R. (2003). Hazy sighted link state (HSLS) routing: A scalable link state algorihm. In BBN Technical Memorandum, No. 1301.

[Schmidt and Townsend 2003] Schmidt, T. and Townsend, A. (2003). Why wi-fi wants to be free. *Commun. ACM*, 46(5):47–52.

[Shin et al. 2004] Shin, J., Lee;, H., Na, J., Park, A., and Kim, S. (2004). Gateway discovery and routing in ad hoc networks with NAT-based internet connectivity. In *Vehicular Technology Conference*, pages 2883–2886.

[Su and Nieh 2002] Su, G. and Nieh, J. (2002). Mobile Communication with Virtual Network Address Translation. *Department of Computer Science, Columbia University*, pages 003–2.

[Suciu et al. 2005] Suciu, L., Bonnin, J., Guillouard, K., and Ernst, T. (2005). Multiple Network Interfaces Management for Mobile Routers. *Proceedings of the International Conference on Intelligent Transportation Systems Telecomunications (ITST), Brest, Junho*.

[Sun et al. 2002] Sun, Y., Belding-Royer, E., and Perkins, C. (2002). Internet Connectivity for Ad Hoc Mobile Networks. *International Journal of Wireless Information Networks*, 9(2):75–88.

[Teixeira 2007] Teixeira, D. V. (2007). Aperfeiçoando a operação de redes em malha sem fio. Master's thesis, Universidade Federal Fluminense.

[Tønnesen 2007] Tønnesen, A. (2007). http://www.olsr.org/. Acessado em 03-02-2007.

[Tsaoussidis and Matta 2002] Tsaoussidis, V. and Matta, I. (2002). Open issues on TCP for mobile computing. *Wireless Communications and Mobile Computing*, 2(1):3–20.

[Tsarmpopoulos et al. 2005a] Tsarmpopoulos, N., Kalavros, I., and Lalis, S. (2005a). A low-cost and simple-to-deploy peer-to-peer wireless network based on open source linux routers. In *Proceedings of TRIDENTCOM'05*, pages 92–97.

[Tsarmpopoulos et al. 2005b] Tsarmpopoulos, N., Kalavros, I., and Lalis, S. (2005b). A low-cost and simple-to-deploy peer-to-peer wireless network based on open source linux routers. In *International Conference on Testbeds and Research Infrastructures for the DEvelopment of NeTworks and COMmunities (TRIDENTCOM'05)*, pages 92–97. IEEE Computer Society.

[Vaidya 2002] Vaidya, N. (2002). Weak duplicate address detection in mobile ad hoc networks. *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*, pages 206–216.

[Valkó 1999] Valkó, A. (1999). Cellular IP: a new approach to Internet host mobility. *ACM SIGCOMM Computer Communication Review*, 29(1):50–65.

[Valle et al. 2008] Valle, R., Passos, D., Muchaluat-Saade, D. C., and Albuquerque, C. (2008). "mesh topology viewer (mtv): an svg-based interactive mesh network topology visualization tool". *IEEE Symposium on Computers and Communications, (ISCC'08)*.

[Wakeman et al. 1992] Wakeman, I., Crowcroft, J., Wang, Z., and Sirovica, D. (1992). Layering considered harmful. In *IEEE Network*, pages 20–24.

[Weber et al. 2003] Weber, S., Cahill, V., Clarke, S., and Haahr, M. (2003). Wireless ad hoc network for dublin: A large-scale ad hoc network test-bed. *ERCIM News*.

[Wedlund and Schulzrinne 1999] Wedlund, E. and Schulzrinne, H. (1999). Mobility support using sip. In *WOWMOM '99: Proceedings of the 2nd ACM international workshop on Wireless mobile multimedia*, pages 76–82, New York, NY, USA. ACM.

[Wenli Chen 1999] Wenli Chen, Nitin Jain, S. S. (1999). ANMP: Ad hoc network network management protocol. *IEEE Journal on Selected Areas in Communications*, 17(8):1506–1531.

[Xu and Saadawi 2001] Xu, S. and Saadawi, T. (2001). Does the ieee 802.11 mac protocol work well in multihop wireless ad hoc networks? In *Communications Magazine*, volume 39, pages 130–137.

[Xylomenos et al. 2001] Xylomenos, G., Polyzos, G., Mahonen, P., and Saaranen, M. (2001). Tcp performance issues over wireless links. *Communications Magazine, IEEE*, 39(4):52–58.

[Yunlong et al. 2004] Yunlong, Z., Rui, S., and Xiaozong, Y. (2004). One hop-DAD based address autoconfiguration in MANET. *Lecture notes in computer science*, pages 674–680.

Apêndice

Com a finalidade de manter os capítulos principais da dissertação mais concisos, algumas questões de menor importância foram movidas para o apêndice.

A1 - Mobilidade

A sub-seção a seguir é referente ao assunto de detecção de mobilidade, descrito na Subseção 5.6.2

A1.1 Implementação da detecção de mobilidade na classe I

- As soluções baseadas em nível de Rede ou superior, como IP Móvel e HIP, usualmente trabalham com detecção de mobilidade apenas da Classe 1A. Esta classe implica que o dispositivo móvel estabelece e mantém a sua conexão padrão para o mesmo *gateway*. Somente no caso do *gateway* padrão ficar fora de alcance, o dispositivo móvel deve descobrir e estabelecer uma nova rota à um novo *gateway* e, se necessário, reconfigurar seu endereço. Nesta classe de detecção de mobilidade, o próprio dispositivo que realizou a movimentação deve tomar as ações necessárias, como informar ao dispositivo correspondente ou ao agente permanente (*Home Agent*) o novo endereço, caso tenham ocorrido alterações do mesmo. Um exemplo é ilustrado na Figura 6.1;

- Para a Classe 1B, o dispositivo móvel não tem controle sobre qual *gateway* o pacote será realmente entregue, logo as técnicas baseadas na classe anterior são incapazes de detectar a mobilidade, utilizando mecanismos próprios. Contudo o *gateway* pode auxiliar o cliente móvel, pois, o *gateway* possui a capacidade de perceber a mobilidade ao analisar o endereço de origem de cada pacote. O *gateway* ao perceber algum novo endereço de origem, informa ao cliente a mudança ocorrida. O cliente, ao ser notificado da alteração, pode cuidar dos ajustes necessários. Um desses exemplos é ilustrado na Figura 6.2.

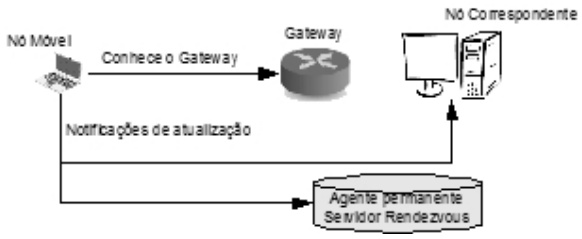


Figura 6.1: Classe Ia: O dispositivo móvel controla a sua mobilidade.

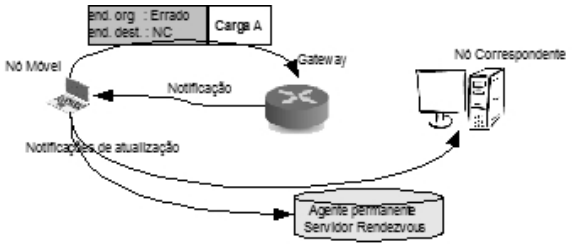


Figura 6.2: Classe Ib: *gateway* notifica o dispositivo sobre sua mobilidade.

- Para a Classe 1C, o mecanismo de detecção de sinais dos pontos de acesso é implementado no *driver* do dispositivo sem fio, no dispositivo móvel. Neste caso o procedimento de troca de ponto utiliza os mecanismos dos processos de desassociação no antigo ponto e de associação no novo ponto. Cabe, portanto, a rede realizar as adaptações necessárias, quando esta receber as mensagens de reassociação. Este tipo de implementação é tipicamente encontrada em redes que ofereçam suporte transparente à mobilidade, como o caso de [Meraki 2007, Roch 2005, Amir et al. 2007, Navda et al. 2005, Ganguly et al. 2006]

A1.2 Implementação da detecção de mobilidade na classe 2

Em alguns casos, é interessante remover da rede sem fio ou do dispositivo móvel a responsabilidade de gerenciar a mobilidade, delegando ao *gateway*, a sobrecarga da resolução das questões relacionadas à mobilidade. Em tal situação, a classe 2, de detecção de mobilidade pode ser mais adequada.

Nos protocolos IP Móvel e HIP, o cliente possui a responsabilidade de informar, aos outros dispositivos participantes dos protocolos, o evento de mobilidade e as suas conseqüentes reconfigurações. O próprio *gateway* é candidato a tomar esta responsabilidade, absorvendo a carga de gerenciar a reconfiguração, necessária no evento de mobilidade. Assim, pode-se utilizar qualquer protocolo de roteamento no domínio da rede sem fio, para controlar as rotas do cliente até o *gateway*. Este protocolo de roteamento pode ser otimizado para utilizar o melhor caminho até qualquer *gateway* (*anycast*).

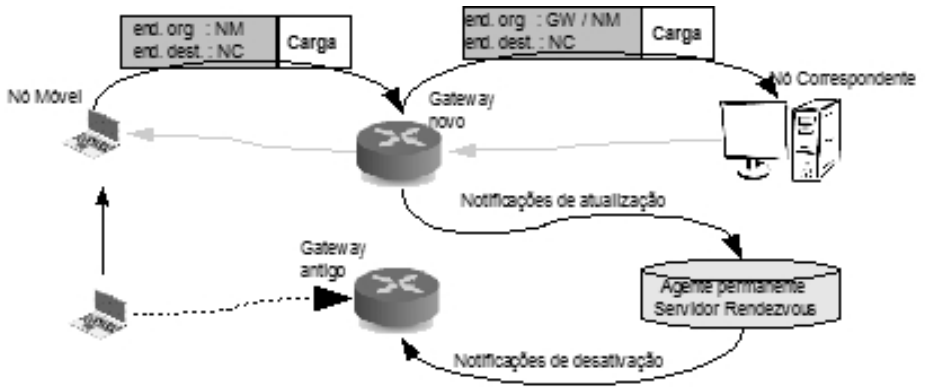


Figura 6.3: Classe II: *gateway* gerencia completamente a mobilidade.

A classe 2, ao permitir a livre seleção de protocolo de roteamento para uma sub-rede sem fio, torna-se interessante às redes *mesh*, pois este tipo usualmente emprega protocolos auto-gerenciáveis, com medidas de reparação de rotas em cada salto.

Para o IP Móvel, uma solução pode ser vista na Figura 6.3. Quando o dispositivo móvel tenta enviar um pacote pelo *gateway*, este percebe o ingresso de um novo cliente, pela análise do campo endereço de origem (*Home Address*) contido no pacote. Então extrai-se o endereço do agente permanente (*Home Agent*), para em seguida informar ao agente sobre o novo endereço do cliente. O *gateway* modifica diversos campos do pacote, incluindo o endereço de origem usando o próprio endereço (do *gateway*), bem como colocando o endereço permanente (*Home Address*) na opção de agente permanente do cabeçalho móvel [Johnson et al. 2004]. Depois destas modificações no pacote, o *gateway* encaminha o pacote atualizado à Internet. Quando o pacote chega ao dispositivo destinatário, o endereço IP de origem (do *gateway*) é trocado pelo endereço permanente do cliente móvel e vice versa. Logo o nível de Transporte, do destinatário, não percebe que houve qualquer movimentação do cliente. Para Mobile IPv4, é possível usar encapsulamento UDP a partir do *gateway*, em vez do cabeçalho móvel opcional do IPv6.

Uma solução similar pode ser utilizada no HIP, utilizando-se do encapsulamento UDP, no caso de IPv4, ou do cabeçalho móvel, para IPv6. Após a notificação realizada pelo *gateway* aos dispositivos que participam dos protocolos, como o *Home Agent*, o *Rendezvous Server* ou os destinatários, o agente móvel ou servidor Rendezvous pode notificar ao antigo *gateway*, para que desative o controle do cliente que o deixou.

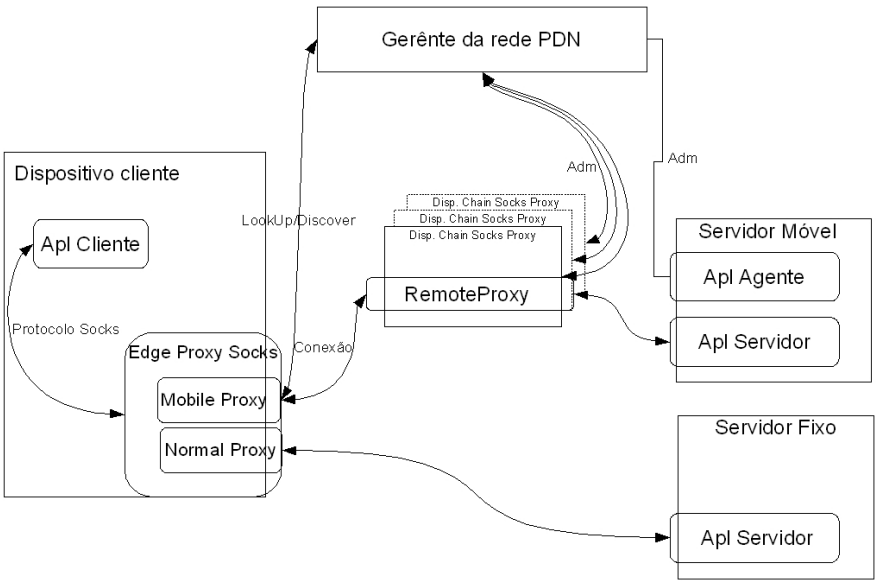


Figura 6.4: Arquiterura do Mproxy

A1.3 Proposta de suporte a mobilidade

Uma solução a ser proposta, denominada Mproxy, tem o potencial de oferecer suporte à mobilidade, com o uso de mecanismos provenientes, principalmente, do nível de Aplicação e com algum suporte no nível de Rede.

O objetivo do Mproxy é adicionar alguns mecanismos de suporte à mobilidade nas aplicações existentes, sem as modificar. Esta adição pode ser dada de duas formas. A primeira corresponde a uma configuração na versão V4 ou V5, se a aplicação suportar o protocolo proxy socks [Leech et al. 1996]. A segunda pelo uso do único mecanismo necessário no nível de Rede, que é um mecanismo que realiza a interceptação das conexões da aplicação cliente.

A finalidade destas formas é encaminhar todas as conexões de uma determinada aplicação para um servidor proxy. É este o servidor proxy que gerencia as questões ligadas à mobilidade.

O centro da arquitetura desta solução é formado por três componentes, ilustrado na Figura 6.4, o mencionado servidor proxy, um servidor de gerência e um servidor de apoio.

O nível de Aplicação pode ser considerado como base do Mproxy, pois o componente servidor proxy é uma aplicação instalada no dispositivo móvel. Este servidor é responsável por intermediar as conexões das aplicações clientes com os servidores de apoio. Os ser-

vidores de apoio irão redirecionar as conexões aos destinatários originais. O servidor de gerência coordena a cooperação dos outros componentes.

O objetivo desta arquitetura é dividir a conexão original em duas, a primeira, entre o dispositivo móvel e o ponto de apoio, é denominada de conexão móvel. A segunda conexão corresponde à ligação entre este ponto de apoio e o destinatário original da conexão. Esta divisão procura delimitar as questões relacionadas à mobilidade na conexão móvel, pois em seus dois extremos estão as aplicações da solução.

Devido à conexão móvel absorver os problemas relacionados à mobilidade, a solução Mproxy utiliza algumas técnicas vistas na Seção 5.2, que descreve soluções no nível de Transporte que combatem os problemas causados pelos eventos de mobilidade. Contudo, o Mproxy utiliza tais técnicas no nível de Aplicação, por cima do protocolo UDP, pois desta forma o Mproxy não é atingido pelos problemas do TCP. Se a aplicação cliente utilizar uma conexão do protocolo TCP, o Mproxy implementará os mecanismos do TCP que o UDP não têm, contudo, estes mecanismos são adaptados para trabalharem com as características de atraso e perda de enlaces sem fio. Outro fator que contribui para seleção do UDP é que este protocolo não possui o controle de estado como o TCP. Este controle de estado é fonte de diversos problemas relacionados à quebra de conexões, em eventos de mobilidade ou de reconfiguração de endereço.

O papel do servidor de gerência é de controlar o comportamento e o estado dos servidores de apoio e de determinar quais os pontos de apoio que os servidores *proxies* utilizam. Inicialmente os servidores *proxies* conhecem apenas o servidor de gerência, pois este possui um endereço de IP fixo. O servidor de gerência é responsável por encontrar o ponto de apoio mais adequado para o dispositivo móvel. Nesta questão, diversas técnicas são reaproveitadas do conceito de CDN (*Content Delivery Network*), como a distribuição de carga e a distribuição geográfica destes pontos, no gerenciamento, no custo de operação da infraestrutura, na tarefa de determinar o melhor ponto de apoio em relação a um cliente e na manutenção do estado destes pontos. Desta forma o conceito PDN (*Proxy Distribution Network*) é criado.

Com a finalidade de diminuir os problemas causados por falhas na infraestrutura da solução, a tarefa do servidor de gerência é distribuída em um conjunto de servidores, que de forma cooperativa, cumprem as tarefas gerenciais. Adicionalmente, as informações sobre o estado das conexões móveis são guardadas em seus servidores *proxies* e algum nível de replicação é realizada nos pontos de apoio.

O uso de pelos menos dois novos dispositivos pode ser visto como ponto negativo,

assim como ocorre na seção de conclusão do Capítulo 5, contudo, estes dispositivos podem ser reutilizados para realizar algum processamento nos dados das conexões que passam pelos pontos de apoio. Um exemplo de processamento é realizar a transcodificação, no ponto de apoio, que adapte um vídeo aos recursos do dispositivo móvel, que usualmente possui uma reduzida capacidade de tela. A vantagem existe, uma vez que o dispositivo móvel, usualmente, não tem em si próprio a capacidade de processamento adequado para realizar a adaptação necessária e, portanto, o ponto de apoio poderia fornecer os recursos computacionais necessários para a transcodificação.

Como evidenciado na descrição desta proposta, as áreas de atuação são tão amplas que são assuntos que podem ser tratados por diversos artigos ou trabalhos futuros.

A2 Gerência

Uma pesquisa inicial realizada na área de gerência não teve um conteúdo maduro o suficiente a ser inserido no Capítulo 4, portanto, o resultado da pesquisa é apresentado a seguir, com a finalidade de servir de inspiração a trabalhos futuros.

A2.1 Questões em aberto para redes em Malha

A2.2 Técnica cross-layer

Algumas questões, que foram enfrentadas pelo Projeto Remesh, continuam sem solução satisfatória, pois inicialmente foram tratadas por métodos temporários ou podiam ser ignoradas. Isto era possível pois a rede tinha um pequena escala e, portanto as questões também são de baixo impacto.

Contudo, conforme a rede Remesh cresceu em tamanho e escala, algumas destas questões que inicialmente eram ignoradas, passaram a ter uma maior visibilidade, impedindo de alguma forma a evolução da rede. Por uma recente experiência do projeto no trabalho relacionado a questões de roteamento (DynTun), técnicas *cross-layer* mostraram-se ser uma interessante fonte de soluções.

As técnicas *cross-layer* são baseadas em troca de informações entre diferentes camadas da pilha de protocolos. Inicialmente a pilha de protocolos foi construída com o objetivo de separar melhor as responsabilidades de comunicação, tornado possível alterar a implementação de alguma camada sem afetar as demais, fazendo com que cada camada fosse independente das superiores. Apesar desta separação ter contribuído com a popula-

rização da Internet, por tornar mais simples desenvolver implementações de cada camada, tornou-se um impecilho [Wakeman et al. 1992] no atual nível de desenvolvimento da Internet, pois informações interessantes são escondidas em camadas inferiores, o que impede o uso de técnicas mais adaptadas e com maior complexidade, nas camadas superiores, que poderiam melhorar o desempenho das redes.

Nas próximas cinco sessões são esclarecidas algumas das questões encontradas pelo projeto, que ainda não foram satisfatoriamente resolvidas, onde técnicas *cross-layer* podem ser úteis.

A2.3 Seleção dinâmica de canal

As versões 802.11b de 1997 e 802.11g de 2003 atuam especificamente entre as freqüências de 2412 a 2462 MHz. Cada canal do padrão ocupa uma banda de 22 MHz, entretanto, a faixa na qual o padrão atua está dividida em 11 canais sobrepostos, cada um ocupando 5 MHz de banda. Isto significa que na faixa disponível, apenas três canais não se interferem: 1, 6 e 11.

Com o aumento da popularidade de produtos de redes sem fio para consumidores finais, que implementam os padrões IEEE 802.11b/g, estes três canais são utilizados com crescente intensidade.

Com o objetivo de resolver esta limitação, a seleção de canal, principalmente em redes *mesh* que utilizam apenas um rádio, deve escolher o canal com a menor intensidade de interferência, em toda a rede.

Usualmente esta seleção de canal ocorre de forma estática, no momento que a rede começa a ser instalada e, portanto, o canal escolhido é possivelmente o melhor apenas neste momento. Conforme o crescimento da rede, outros canais podem passar a ser melhores, portanto, o desafio é criar um mecanismo de seleção autônoma que dinamicamente selecione o melhor canal, avaliando constantemente a condição de todos os canais [Justin and Nelson 1994]. Tal mecanismo consiste em verificar a situação de cada canal na vizinhança de cada ponto da rede, e usar as informações adquiridas para escolher um canal que melhore o desempenho da rede como um todo.

Um critério possível é atribuir valores a cada canal, que reflitam o nível de interferência observado em cada ponto. Portanto quanto mais livre de interferência um canal estiver, melhor será o seu valor. Contudo o peso do valor das observações em cada ponto pode ser diferenciado, de tal forma, a privilegiar os pontos que estão com maior carga de uso

pelos usuários. Outro fator adicional, que pode alterar o valor, é o nível de conectividade que cada canal pode proporcionar a rede, pois o número de bons enlaces sem fio pode ser influenciado pelo canal escolhido, e como uma rede *mesh* usualmente é beneficiada pelo aumento de enlaces disponíveis, os canais com maior quantidade de enlaces terá seu valor melhorado.

Entretanto, um cuidado especial deve ser tomado a fim de evitar grandes ou rápidas oscilações na seleção de canais, pois a cada troca, podem surgir problemas de sincronização, que causam particionamento da rede. Mesmo quando toda a rede altera o canal de forma bem sucedida, perdas de pacotes, devido a atrasos, podem ocorrer. Estes problemas podem prejudicar o desempenho da rede.

A contribuição do *cross-layer* neste assunto é permitir que dados, correspondentes da camada de rede, influenciem na configuração da camada física ou de enlace, sendo que o processo de pesquisa e reconfiguração pode ser executado por mecanismos baseados na camada de aplicação. Esta mesma contribuição pode ser encontrada nas próximas sub-seções.

A2.4 Utilização de múltiplos rádios

Quando redes de múltiplos saltos, que implementam o padrão IEEE 802.11, utilizam apenas uma única interface de rede sem fio, estas redes possuem uma grande limitação [Xu and Saadawi 2001]. Esta limitação tem impacto na capacidade da rede em explorar o potencial de cada enlace sem fio. Esta limitação é causada, dentre outros motivos, pelo compartilhamento do meio de comunicação e o uso de rádios que operem no modo *half-duplex*. Os eventos de colisões de mensagens é um tipo muito comum de problema, tão comum que pode impactar severamente a vazão máxima útil do enlace. A vazão pode decair rapidamente a cada novo salto [Passos et al. 2006] e, portanto, limitando o área de cobertura que uma rede *mesh* pode cobrir com eficiência.

Uma possível solução a esta questão limitante é utilizar interfaces adicionais de rede Wi-Fi [Kyasanur and Vaidya 2005, Raniwala et al. 2004]. Esta solução pode manter o uso exclusivo de rádios relativamente baratos e simples, que implementem o padrão IEEE 802.11, desde que as interfaces de um mesmo ponto da rede *mesh* operem em canais distintos e não interferentes entre si. Como benefício desta solução, é a possibilidade de transformar o ponto, que operava em modo *half-duplex*, que não pode transmitir e receber dados ao mesmo tempo, para uma solução *full-duplex*, que é capaz transmitir e receber dados simultaneamente, realizado qualquer umas das duas operações em cada interface.

Outro beneficio potencial é a redução de interferência e das colisões de mensagens entre pontos vizinhos da rede *mesh*, por reduzir a intensidade de uso de cada canal. Estas vantagens podem contribuir na melhora da escalabilidade da rede.

Um desafio, para utilizar de forma eficiente múltiplas interfaces de rádio, é criar uma técnica de seleção que utilize a diversidade de canais como uma vantagem. Ao menos três técnicas podem ser facilmente consideradas. A primeira é uma estratégia estática, ao qual em um evento de reconfiguração da rede, é analisado o estado da rede, para então selecionar o melhor canal para cada enlace, e por fim, configurar os rádios baseados nesta seleção [Raniwala et al. 2004]. Esta configuração permanecerá estática até o próximo evento de reconfiguração. A segunda estratégia é dinâmica, que de forma similar a primeira, realiza uma análise seguida de reconfiguração, contudo, esta o faz em um ciclo contínuo, com o objetivo de manter a rede sempre ajustada a mudanças no meio de comunicação. A terceira pode ser considerada uma forma híbrida das anteriores, onde uma das interfaces será configurada pelo método estático e, assim, aumentando a conectividade e estabilidade da rede, e as outras interfaces configuradas pelo método dinâmico, para que a rede tenha capacidade de rapidamente responder às mudanças nas condições no meio de comunicação.

O mesmo cuidado deve ser tomado na seleção de canal da sub-seção anterior, que é de evitar instabilidades, com o nível de freqüência que impacte na capacidade de funcionamento de rede ou que possam criar partições na rede.

A2.5 Seleção dinâmica de potência de transmissão

Um dos parâmetros que possui uma grande importância na operação e desempenho do rádio, é a potência de transmissão. Um aumento na potência de transmissão usualmente capacita, a um ponto da rede *mesh*, a cobrir uma área maior com seu sinal de rádio. Além desta vantagem, existe um possível benefício na taxa máxima de transmissão, que um enlace pode sustentar. Contudo, quanto maior a potência de transmissão, maior será a interferência em pontos vizinhos, e este problema, mesmo que algum enlace, individualmente, melhore significativamente com o aumento da potência, pode diminuir o desempenho da rede como um todo.

Atualmente na rede Remesh, o parâmetro que regula a potência de transmissão é ajustada de forma manual, pelo uso de conhecimento empírico do local ao qual o ponto da rede está instalado ou simplesmente é justado de forma ambiciosa, para o nível mais alto suportado pela interface.

Uma forma de corrigir estes métodos simplistas, de regulação de potência, é criar uma técnica de ajuste inteligente no controle de potência [Ramanathan and Hain 2000, ElBatt et al. 2000]. Esta técnica pode fazer bom uso de informações disponíveis em outros níveis. Neste caso, utilizar informações contidas no nível de Rede, pois o protocolo de roteamento utilizado pelo Projeto Remesh, OLSR, é do tipo estado de enlace, portanto, cada ponto da rede não apenas conhece o estado dos enlaces com seus vizinhos próximos, mas tem também uma visão global da rede. Um técnica sugerida é modificar o potência nos enlaces, observar o resultado da alteração, consultando as informações dos estados dos enlaces, fornecidas pelo protocolo de roteamento. As alterações deve atender dois objetivos, o primeiro é maximizar a qualidade dos enlaces que cada ponto tem com seus vizinhos classificados como MPR, e o segundo é minimizar com os outros vizinhos. Estes dois objetivos são contraditórios, pois o primeiro tende a aumentar a potência, enquanto o que tenta minimizar tende a diminuir a potência.

São duas as razões que explicam a diferença entre ambos objetivos. O primeiro tenta priorizar os enlaces com os vizinhos MPR, pois são estes os vizinhos que podem ser utilizados como primeiro salto, no reencaminhamento dos pacotes provenientes dos clientes, até a Internet. Enquanto o segundo, tenta minimizar o impacto em outros enlaces, que poderão ser utilizados como segundo ou mais saltos do mesmo encaminhamento. Diminuir a interferência na rede é uma questão muito importante, pois se esta interferência for suficientemente intensa, os mecanismos de recuperação de perdas do nível de enlace podem falhar, assim, forçando o de nível de transporte, quando existe, a recuperar a perda com o uso de mecanismos mais lentos, do tipo fim-a-fim.

Alguns cuidados devem ser providenciados, pois uma redução exagerada da potência pode prejudicar a capacidade do protocolo de roteamento em descobrir a topologia real da rede e, portanto, reduz a quantidade de enlaces úteis. O nível de ajuste na potência de transmissão deve maximizar uma função utilitária, que considera o peso de ganho, ao melhorar os enlaces com vizinhos MPR, com o peso da perda do desempenho no restante da rede, por causa de interferência em vizinhos distantes, a alguns saltos.

Alem da função de utilidade, outras questões podem ser consideradas no controle da potência, como exemplo, o evento de transmissão de pacotes de controle do protocolo de roteamento, para disseminação de informações ao restante da rede. Este evento é fundamental para descoberta e manutenção da topologia da rede, que pode ser beneficiada por uma aumento temporário da potência. Outros exemplos de eventos são os que ocorrem quando a topologia sofre uma severa alteração, como a perda de um ponto ou

particionamento da rede. Estes eventos podem também ser beneficiados por um aumento momentâneo da potência, a fim de diminuir os impactos negativos.

A2.6 Configuração autonômica de rede

Conforme a rede *mesh* cresce em tamanho, várias tarefas de gerência, que inicialmente eram fáceis de realizar manualmente, passaram a ser consideradas fonte de grande volume de trabalho indesejado aos administradores. Conforme as tecnologias evoluem e conquistam novos mercados, o número e qualidade de recursos humanos, que possuem alto nível de capacitação, se torna limitado. Portanto, aumenta a pressão pelo desenvolvimento de ferramentas autônomas, que simplifiquem e ampliem as capacidades de gerência.

Atualmente, cada ponto da rede *mesh*, impõem no mínimo um processo de configuração manual aos usuários. Cada usuário responsável, por realizar tais processos, deve ter um bom conhecimento nas áreas de redes sem fio e nas questões especificas às redes *mesh*. Cada parâmetro de operação, como "essid", canal do rádio e identificação do ponto devem ser inseridos nos arquivos de configuração antes da instalação. Contudo, seria mais prático se no processo de instalação, fosse possível implantar o ponto no local desejado e deixar o restante da rede realizar o processo de configuração do novo ponto, com pouca ou nenhuma interação dos usuários, portanto, diminuindo a obrigação do usuário em dominar todos os aspectos ligados a redes *mesh*.

O mecanismo de gerência autonômica, que pode dar à rede *mesh* esta capacidade de auto ajustar-se, deve ser capaz de alterar diversos parâmetros de operação de forma adequada, para que a rede mantenha sempre um estado funcional. Esta capacidade não deve ficar limitada somente no momento de instalação de novos pontos, mas também permitir que pontos da rede sejam realocados a um outro setor da rede, sem que qualquer preparativo, anterior a realocação, seja necessário.

Alguns objetivos devem ser almejados por tal mecanismo, como o de segurança, que por exemplo, deve evitar que o ponto seja erroneamente configurado a fazer parte de uma rede estrangeira. Esta segurança também deve possuir alguma resistência a ataques do tipo DoS (*Denial of Service*) ou aceitar comandos de entidades não autorizadas. Outro cuidado é em relação ao tempo de inatividade da rede, que cada processo de reconfiguração provoca, de ser menor do que o tempo que os usuários podem esperar para a retomada da atividade. Estas alterações também devem evitar prejudicar o desempenho da rede ou aumentar demasiadamente a sobrecarga nos equipamentos dos pontos com funções de gerência.

Cada componente implantado, deste mecanismo de configuração autônoma, deve servir como infra-estrutura para que outras ferramentas possam ser desenvolvidas, promovendo extensibilidade da capacidade de gerência, com por exemplo, adicionar soluções as questões em aberto na rede Remesh, como seleção dinâmica de canal e controle inteligente na potência de transmissão. Tal infra-estrutura deve simplificar o desenvolvimento destas ferramentas ao fornecer métodos de acesso, configuração e informações da rede, por meio de simples métodos de acesso.

A2.7 Integração de ferramentas

Com o desenvolvimento de várias ferramentas, cada qual focada em um conjunto restrito de problemas, a tarefa de gerenciar a rede *mesh* envolve o trabalho de coletar informações dispersas em diversas ferramentas, cada qual com sua forma de acesso. Uma nova, e mais centralizada, ferramenta deve oferecer uma visualização dos dados em um formato mais integrado, como por exemplo, ao exibir a representação, do estado da rede, enriquecida com informações de diferentes ferramentas. Esta ferramenta deve filtrar e combinar dados dispersos em poucas representações.

Seguindo o exemplo de outras soluções proprietárias [Meraki 2007, Netequality 2006], a ferramenta de visualização de topologia pode ser utilizada como ponto de agregação de dados de outras ferramentas, como demonstrado na Figura 6.5, pois pode ser espacialmente organizado pela disposição da topologia da rede. Portanto a ferramenta de topologia pode combinar informações da rede, a fim de construir um mapa rico de informações visuais aos administradores. Portanto, oferecendo a possibilidade de um acesso mais rápido e abrangente da situação da rede. Por exemplo, a qualidade de todos os enlaces e o número de usuários autenticados, em cada ponto, podem ser representados por simples artefatos visuais no mapa. Informações mais detalhadas, em cada ponto, podem ser solicitadas com uma simples interação com o mapa.

O mair objetivo da integração de ferramentas de gerência é oferecer um novo canal de acesso aos administradores de rede, para que estes sejam capazes de coletar dados de diversas ferramentas, por um mecanismo mais fácil e rápido. Tais ferramentas de integração devem permitir aos administradores decidirem o nível de detalhe das informações, a fim de evitar uma possível esmagadora inundação de informações.

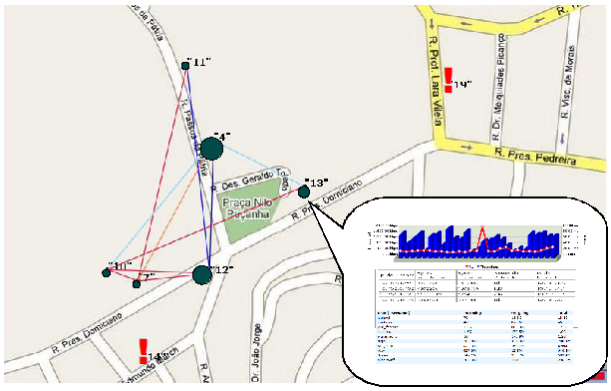


Figura 6.5: Simulação de uma ferramenta de integração.