UNIVERSIDADE FEDERAL FLUMINENSE
CENTRO TECNOLÓGICO
MESTRADO EM ENGENHARIA DE TELECOMUNICAÇÕES

DOUGLAS VIDAL TEIXEIRA

APERFEIÇOANDO A OPERAÇÃO DE REDES EM MALHA SEM FIO

NITERÓI
2007

DOUGLAS VIDAL TEIXEIRA

APERFEIÇOANDO A OPERAÇÃO DE REDES EM MALHA SEM FIO

Dissertação apresentada ao Curso de Mestrado em Engenharia de Telecomunicações da Universidade Federal Fluminense, como requisito parcial para obtenção do Grau de Mestre. Área de Concentração: Comunicação de Dados Multimídia

Orientador: Prof^{o} Luiz Cláudio Schara Magalhães, Phd

Niterói

2007

Ficha Catalográfica elaborada pela Biblioteca da Escola de Engenharia e Instituto de Computação da UFF

T266 Teixeira, Douglas Vidal.
Aperfeiçoando a operação de redes em malha sem fio / Douglas Vidal Teixeira. – Niterói, RJ : [s.n.], 2007.

196 f.

Orientador: Luiz Cláudio Schara Magalhães.
Dissertação (Mestrado em Engenharia de Telecomunicações) - Universidade Federal Fluminense, 2007.

1.Comunicação de dados -otimização de redes. 2. Protocolos de roteamento. 3. Internet.. 4 .Análise de redes (planejamento).
5. Redes em malha sem fio. 6. Redes – gerência e acompanhamento.
I. Título.

DOUGLAS VIDAL TEIXEIRA

APERFEIÇOANDO A OPERAÇÃO DE REDES EM MALHA SEM FIO

Dissertação apresentada ao Curso de Mestrado em Engenharia de Telecomunicações da Universidade Federal Fluminense, como requisito parcial para obtenção do Grau de Mestre. Área de Concentração: Comunicação de Dados de Multimídia

Aprovada em _____de_____ de 2007

BANCA EXAMINADORA

_____

Prof^{o} Luiz Cláudio Schara Magalhães, Phd – Orientador
Universidade Federal Fluminense

_____

Prof^{a} Débora Christina Muchaluat Saade, D.Sc.
Universidade Federal Fluminense

_____

Prof^{o} Alexandre Sztajnberg, D.Sc.
Universidade Estadual do Rio de Janeiro

Niterói

2007

Dedico este trabalho à minha família, meus pais Carlos e Ilca, meu irmão Carlinhos e à minha namorada Renata. Meus alicerces.

Dedico também aos amigos do Projeto Remesh e do Laboratório Mídiacom da UFF.

AGRADECIMENTOS

Primeiramente a Deus por ter me permitido alcançar meus objetivos com saúde e paz.

À minha família por todo apoio, amor e compreensão.

.

Ao amigo Diego Passos, por toda a sua sapiência e ajuda ao longo de todo o projeto Remesh. Este trabalho não seria possível sem ele.

Aos amigos de mestrado Felipe Maya e Fábio Guerra, pela ajuda técnica e pelo apoio nos momentos de maior pressão.

Aos coordenadores do projeto, professores Célio Vinícius de Albuquerque e Débora Saade, por terem acreditado em mim e por todo o apoio técnico.

Ao meu orientador e também coordenador do projeto, professor Luiz Cláudio Schara Magalhães, pela paciência, amizade e pelo ótimo trabalho como orientador.

Finalmente, devo agradecer ao coordenador do curso de Mestrado em Engenharia de Telecomunicações da UFF, professor Andrés Pablo Barbero e ao secretário administrativo, Rafael Carvalho, por toda a ajuda dispensada.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS, SIGLAS E SÍMBOLOS

ABREVIATURA	INGLÊS	PORTUGUÊS
ANATEL	National Telecommunications Agency	Agência Nacional de Telecomunicações
AODV	Ad hoc On Demand Distance Vector	Vetor de distância *ad hoc* sob demanda
dB	Decibel	Decibel (unidade medida de magnitude)
dBi	dB isotropic	dB em relação ao irradiador isotrópico
dBm	dB milliwatt	dB milliwatt (unidade de medida de potência)
ETT	Expected Transmission Time	Tempo de Transmissão Esperado
ETX	Expected Transmission Count	Número de Transmissões Esperadas
GT	Workgroup	Grupo de Trabalho
IEEE	Institute of Electrical and Electronics Engineers	Instituto de Engenheiros Elétricos e Eletrônica
MB	Mega Byte	Mega Byte (2^{20} bytes)
Mbps	Mega bit per second	Mega bits por segundo
ML	Minimum Loss	Perda mínima
MPR	Multi-point Relay	Repetidor multiponto
OLSR	Optimized Link State Routing Protocol	Protocolo de Roteamento Otimizado baseado em estados de enlaces
PEII	EIRP – Equivalent Isotropic Radiated Power	Potência Equivalente Isotropicamente Irradiada
RFC	Request For Comments	Pedido para comentários
RNP	National Research Network	Rede Nacional de Pesquisa e Ensino
Rx	Reception	Recepção
Tx	Transmission	Transmissão
σ	Standard deviation	Desvio padrão

RESUMO

Redes em malha sem fio têm ganhado particular importância do mundo acadêmico e coorporativo nos últimos anos. Redes em malha, ou *mesh,* são redes sem fio baseadas no padrão IEEE 802.11, onde a comunicação entre os nós de acesso e roteamento é feita através de protocolos *ad-hoc*. Desta forma, as redes em malha são utilizadas para a criação de *backbones* sem fio, podendo fornecer acesso à Internet para usuários cabeados ou móveis.

Esta inversão do paradigma de estruturação de redes metropolitanas proporciona uma solução para o acesso na chamada última milha, além de novas formas de comunicação móvel e pessoal. Por utilizarem um padrão de acesso ao meio consolidado e amplamente difundido, podem ser construídas com baixos custos. Além disso, elas permitem a cobertura de grandes áreas sem a necessidade de projetos complexos de rádio-enlace por serem auto-configuráveis na presença de demais nós.

O presente trabalho apresenta a primeira fase do projeto acadêmico Remesh, financiado pela Rede Nacional de Pesquisa e Ensino, cujo objetivo foi a construção do primeiro protótipo de uma rede em malha acadêmica, fornecendo acesso em banda larga gratuito para alunos e funcionários da UFF.

Como assistente técnico do projeto, o autor apresenta a produção científica pessoal agregada à construção do protótipo: o esquema de endereçamento adotado, soluções de hardware, a metodologia empregada para o desenvolvimento dos enlaces de rádio, estudos para o aperfeiçoamento do protocolo de roteamento e de soluções para utilização de múltiplas antenas, desenvolvimento de aplicações de gerência e acompanhamento e diversas medições realizadas com objetivo de análise e comprovação da funcionalidade do protótipo.

Palavras chave: Redes em malha sem fio; Protocolos de roteamento ad-hoc; Métricas de qualificação de enlaces sem fio; Aplicações de gerência e acompanhamento de redes sem fio; OLSR, Optimized Link State Routing.

ABSTRACT

Mesh Networks have been attracting special attention from the academic and corporative communities over the last years. Mesh networks are wireless, IEEE 802.11 standard based networks, where access and routing nodes communicate with each other through ad-hoc protocols. Because of that, mesh networks are employed on the construction of wireless backbones, providing Internet access to cabled and mobile users.

This inversion of the metropolitan networks structure paradigm provides a solution to the last mile access, and also of alternative means of mobile and personal communication. By using a consolidated and successfully applied technology, they can be constructed with low costs. Besides, they allow large areas covering without complex radio-links projects due to its capability of auto configuring in the presence of other nodes.

This work presents the first part of an academic project called Remesh supported by the National Research and Education Network, which main objective was the construction of the first national academic mesh network prototype, providing wide band Internet access to students and employees of the academic community.

As the technical assistant of the project, the author of this work presents its personal scientific production added to the successful and functional construction of the prototype: the IP addressing scheme, hardware solutions, researches for the routing protocol improvement and radio link solutions (including the use of multiple antennas) and the development of the management and monitoring applications.

Keywords: Mesh networks; Ad-hoc routing protocols; Qualifying wireless link metrics; Managements and monitoring wireless applications; OLSR, Optimized Link State Routing Protocol.

1 INTRODUÇÃO

Nos últimos cinco anos, as tecnologias de acesso *wi-fi* têm sido utilizadas para o fornecimento de acesso às redes universitárias por parte de alunos residentes nas suas proximidades. Com o objetivo de expandir a área de cobertura e conseqüentemente o número de usuários, diversos projetos pilotos têm sido desenvolvidos. Os motivos são claros: a larga difusão da tecnologia *wi-fi,* os baixos custos dos equipamentos necessários e as altas taxas obtidas. Alguns exemplos são o RoofNet no MIT (BICKET *et al,* 2005), Vmesh (TSARMPOPOULOS, 2005) na Grécia, MeshNet na Universidade da Califónia em Santa Bárbara (CAMDEN *et al*, 2004), Microsoft *Community* Mesh (DRAVES *el al,* 2004 [a]; 2004 [b]), dentre outros (WEBER *et al*, 2003).

Nestes projetos, roteadores sem fio (geralmente de fácil acesso no mercado) são instalados no topo de edifícios e residências e comunicam-se entre si no modo *ad hoc* através de múltiplos saltos, encaminhando mensagens aos seus destinos. Usuários nos edifícios podem se conectar à rede em malha sem fio de forma cabeada, tipicamente via *Ethernet*, ou através do acesso sem fio, utilizando interfaces *wi-fi*. Tais projetos inspiraram o projeto Remesh, o primeiro piloto universitário brasileiro a implantar uma rede do tipo mesh (como são mais conhecidas as redes em malha sem fio) em ambiente externo, propiciando acesso à Internet em banda larga para participantes voluntários.

No presente trabalho será descrita a criação do protótipo de uma rede mesh de baixo custo, instalada em ambiente externo e utilizada por usuários em suas próprias residências. Serão descritos os procedimentos para a criação do nó de roteamento, levando-se em conta os *softwares* e os *hardwares* adotados. Será apresentado o esquema de endereçamento, o protocolo de roteamento, as escolhas de parâmetros de hardware, as soluções para o suprimento de energia e para a escolha das antenas mais apropriadas.

Uma discussão sobre a metodologia de montagem dos enlaces será apresentada utilizando modelos de propagação próprios (e simplificados) para a tecnologia de acesso em questão. Será apresentada uma nova proposta para o protocolo de roteamento utilizado na comunicação entre os nós. Medições do atraso, *jitter*¸ taxa de perda de pacotes e vazão, serão utilizadas para corroborar tanto o protocolo de roteamento como a validação funcional do protótipo. O trabalho realizado, em conjunto com os demais participantes[1], permitiu a construção de uma rede piloto e a geração de diversas pesquisas e medições no âmbito de tornar o protótipo funcional, escalável e reproduzível.

Como assistente técnico do projeto, o autor teve participação ativa em todas as fases do primeiro ano do projeto, tanto nas questões operacionais, desde a especificação e compra dos equipamentos até as instalações, quanto nas pesquisas e testes realizados. Destacam-se como contribuições próprias: a escolha dos parâmetros de funcionamento dos roteadores sem fio, o modelo de endereçamento; a solução para os acessos cabeado e sem fio simultâneamente através dos roteadores, a metodologia para a construção dos enlaces rádio, as edições realizadas, o modelo para a autenticação dos usuários, as ferramentas de gerência e acompanhamento da rede e algumas das soluções de hardware para montagem dos nós externos

1.1 MOTIVAÇÃO

O acesso à Internet através de elementos móveis vem se tornando alvo de interesse corporativo e universitário em todo o mundo. Novos padrões de acesso estão sendo estudados ou já entrando em produção, principalmente para a tecnologia celular. É inegável a tendência tecnológica e mercadológica para o desenvolvimento das comumente conhecidas "*Mobile Networks*". Neste escopo, uma tecnologia que já havia se consolidado e que ainda continua em desenvolvimento voltou a despertar interesse, as Redes Locais Sem fio, ou *Wireless Local Area Network (WLAN)*, ou ainda, o padrão comercial Wi-Fi (*Wireless Fidelity*) definido pela WECA – *Wireless Ethernet Compatibility Alliance*.

[1] Dentre os diversos participantes e colaboradores voluntários do projeto, destaca-se Diego Gimenez Passos, formado em Ciências da Computação pela UFF em 2007 e participante do primeiro e do segundo ano de realização do projeto Remesh. Diego Passos teve participação ativa em todas as pesquisas realizadas no projeto, devendo-se a ele a criação do protocolo OLSR-ML, que será detalhado no Capítulo 4 do presente trabalho (dpassos@ic.uff.br).

As redes locais sem fio são redes de comunicação de dados cujo acesso é baseado no padrão IEEE 802.11 (STALLINGS, 2002). Estas redes foram desenvolvidas utilizando as faixas de freqüências de 2,4 e 5 GHz, sendo que a segunda ainda está em processo de homologação pela ANATEL. A faixa de 2,4 GHz abrange as freqüências de 2,412 até 2,484 e é denominada de banda ISM – *Industrial, Scientific and Medical* (industrial, científica e médica). É uma banda de utilização livre em diversos países, o que permitiu o desenvolvimento de diversos equipamentos sem fio, como por exemplo, telefones, dispositivos de controle remoto e equipamentos para acesso local sem fio a computadores e pontos de acesso. Por ser uma faixa livre, não exige o pagamento das altas taxas praticadas pelos órgãos reguladores da utilização do espectro. No Brasil, este controle fica a cargo da ANATEL (Agência Nacional de Telecomunicações) e a utilização livre de encargos desta banda tem a ressalva de não ter objetivo comercial.

Desta forma, no final dos anos 90 até os dias atuais diversas empresas investiram na fabricação em escala industrial de dispositivos de acesso sem fio utilizando o padrão IEEE 802.11. Estes dispositivos abrangem interfaces de rede para *desktops* e *laptops* e pontos de acesso, que são os elementos que permitem a interligação de redes cabeadas tradicionais (padrão *Ethernet*) às redes sem fio, diretamente. Neste escopo, a utilização de redes locais sem fio, por oferecerem grande praticidade de conexão aos usuários, obteve uma grande expansão de utilização residencial e comercial. Desta forma, o padrão de acesso também evoluiu principalmente no que diz respeito às taxas de acesso: começando com 2 Mbps (padrão IEEE 801.11), depois alcançando 11 Mbps (802.11b, padrão que comprovou a eficácia comercial da tecnologia). Paralelamente surgia o padrão 802.11a que já conseguia alcançar taxas de 54 Mbps, porém utilizando uma outra faixa de freqüência, na faixa de 5 GHz. Em seguida, operando na faixa de 2.4 GHz, surgiram os roteadores 802.11g operando em 54 Mbps. Atualmente pode-se encontrar roteadores na faixa de 2.4 GHz operando nas taxas de 72 a 108 Mbps (EBERT *et al,* 2005) através de configurações que utilizam múltiplos rádios simultaneamente (padrão 802.11n). O padrão 802.11 é detalhado em ANSI/IEEE (2003).

Certamente, o acesso de dispositivos locais foi o principal objetivo do padrão. Isto significa a interconexão de diversos dispositivos móveis ao elemento de interligação das redes, o ponto de acesso. Esta arquitetura é chamada de modo "infraestrutura". Contudo, o padrão também especifica o modo de operação

denominado *ad hoc* que permite a comunicação dos elementos móveis diretamente, sem a necessidade da presença de um ponto de acesso, de maneira não-estruturada. Este modo de operação nasceu principalmente com o objetivo de ser empregado na computação ubíqua (GRISWOLD *et al,* 2004), permitindo o desenvolvimento de diversas aplicações distribuídas.

As redes *ad hoc* possibilitaram a abertura de um amplo conjunto de temas para serem estudados, destacando-se as redes de sensores e as redes mesh. As redes de sensores são constituídas por nós sem fio que se comunicam e trocam informações específicas para determinadas aplicações, como o monitoramento remoto de variáveis de ambiente (por exemplo, temperatura e umidade), ou como a localização de indivíduos ou animais dentro de uma área de interesse. As redes de sensores geralmente têm o objetivo de serem utilizadas em aplicações específicas e bem definidas e não serão abordadas neste trabalho (ESTRIN *et al,* 2000).

A grande diferença de uma rede em malha sem fio, ou rede mesh, para uma rede de sensores, é a finalidade para qual cada uma se propõe. As redes mesh têm como principal objetivo prover a interconexão dos nós participantes com outras redes estruturadas ou com a própria Internet. As redes mesh, também são constituídas por nós sem fio, móveis ou não, operando no modo *ad hoc.* Entretanto, nestas redes é desejável que haja uma baixa mobilidade dos nós participantes.

Contudo, mesmo que o requisito de baixa mobilidade seja satisfeito, os nós têm que ter a capacidade de se auto-configurarem de acordo com as características do meio. Cada novo nó, ao se associar à rede, permite que outros nós próximos a ele também se associem. Isto abrange não somente a inclusão, a movimentação ou a remoção de elementos, mas também a capacidade de escolha dos melhores caminhos entre eles. Por isto, a necessidade da atuação de protocolos de roteamento suficientemente "inteligentes", que possam atualizar as rotas de maneira a otimizar o encaminhamento dos pacotes, torna-se essencial.

O acesso a serviços de dados e/ou à Internet ainda é tema de grande interesse para estudos e investimentos. Dentre as diversas tecnologias podemos citar: *fiber-to-the-home* (acesso através de ramificações de fibras óticas chegando à casa do usuário final); o ADSL (*Asymmetric Digital Subscriber Line*) que permite o acesso à rede de dados através da linha telefônica; o acesso a cabo que utiliza a mesma estrutura física do serviço de canais de televisão por assinatura; a PLC (*Power Line Communication*) que

utiliza a rede elétrica; as tradicionais redes sem fio ponto-multiponto, que operam com a tecnologia MMDS (*Multichannel Multipoint Distribution Service*) e outras que, alternativamente, operam na faixa de 2,4 GHz; as tecnologias das gerações 2,5 e 3 da rede celular, como o GPRS (*General Packet Radio Service),* o EVDO (*Evolution Data Optimized)* e o WCDMA (*Wideband Code Division Multiple Access*), o *WiMax* (*"Worldwide Interoperability for Microwave Access"*, padrão IEEE 802.16, WIMAXFORUM; 2007), etc. Mais detalhes sobre tecnologias de acesso sem fio podem ser obtidos em STEELE *et al* (2001).

Cada nova tecnologia de acesso possui seus atrativos e suas fraquezas: as tecnologias que utilizam a rede celular ainda não possuem preços acessíveis para a grande parte da população brasileira; o acesso através da rede telefônica além de não ser tão acessível economicamente, também possui limitações de infra-estrutura (apesar da rede telefônica atingir quase a totalidade dos moradores de renda média dos grandes centros, nem todas as linhas disponíveis estão habilitadas para a rede de dados); a comunicação através da rede elétrica depende da qualidade de infra-estrutura e ainda é muito incipiente quanto às taxas de transferência obtidas (em torno de 2Mbps); o acesso através de fibra ótica é uma solução que provê alta performance, porém requer um alto investimento na instalação da infra-estrutura e está longe de atender a maior parte da população; o acesso via operadoras de TV por assinatura também depende de infra-estrutra; o acesso sem fio ponto-multiponto depende de projetos de rádio enlace bem estruturados e não atende a todas as localidades por questões geográficas.

As redes mesh possuem as seguintes características que as tornam uma solução atrativa:

- Baixo custo dos equipamentos;
- Utilizam uma faixa do espectro que é livre;
- Baixo custo na montagem de infra-estrutura, principalmente quanto ao cabeamento;
- Não necessitam de projetos complexos de rádio-enlace;
- Possibilitam altas taxas de transferência;

- Não estão sujeitas às limitações geográficas. Havendo a falta de conexão entre determinados pontos, simplesmente instalam-se novos nós para que a malha fique interligada;
- Instalação incremental de acordo com a demanda

Obviamente, existem diversos pontos fracos, dentre eles:

- Por utilizar uma faixa do espectro aberta, estão sujeitas a interferências;
- Necessitam de protocolos de roteamento eficientes e complexos;
- As taxas de transferência decaem exponencialmente com o número de saltos;
- A faixa de 2,4 GHz possui alcance limitado em comparação com as faixas de freqüência utilizadas nas redes celulares atuais (por exemplo, a tecnologia GSM que opera, no Brasil, na faixa de 1800 MHz);

Contudo, o principal fator que é o custo, ainda é baixo em comparação com todas as outras tecnologias. Além disso, a maior parte dos protocolos de roteamento é de código aberto, o que permite o avanço no desenvolvimento tecnológico, principalmente através dos meios acadêmicos. Por fim, o padrão IEEE 802.11 continua em evolução, resultando no desenvolvimento de equipamentos cada vez mais robustos quanto à taxa de erro de bits, mais eficientes quanto às taxas de transferências e, principalmente, mais baratos.

1.2 OBJETIVOS

Basicamente, a rede do projeto Remesh é uma rede do tipo mesh aonde os nós são fixos em localidades com acesso à energia elétrica. Desta forma, cada nó é roteador e ponto de acesso ao mesmo tempo. Os pacotes são encaminhados por um *backbone* sem fio (SHERESTHA e KO, 2006) com capacidade de adaptação em função das variações de qualidade dos enlaces. São utilizados roteadores comerciais, disponíveis no mercado nacional, alterando-se o sistema operacional original por uma distribuição particular do Linux. Esses roteadores passam a executar um protocolo de roteamento *ad hoc* e são instalados nos topos dos prédios de alunos e funcionários da Universidade Federal Fluminense (UFF). O *gateway* da rede mesh fica localizado no topo de um dos prédios da UFF, no Campus da Praia Vermelha, e está interligado à infra-estrutura

cabeada da universidade. Ele é o responsável pelo roteamento do tráfego dos voluntários para a Internet. Adicionalmente, o *gateway* juntamente com um desktop instalados na mesma rede local, tem a função de autenticar e gerenciar os acessos.

O presente trabalho tem a finalidade de relatar a experiência do primeiro ano de execução do projeto, durante o período de Outubro de 2005 até Outubro de 2006. Serão abordadas a construção, a instalação e a manutenção da rede mesh, tento em vista os detalhes técnicos dos enlaces, da infra-estrutura necessária, do protocolo de roteamento e dos aplicativos utilizados. O primeiro ano do projeto teve seu objetivo inicial alcançado com sucesso. Ele representou o início de uma seqüência de novos projetos de terceiros em parceria com a UFF, relacionados às redes em malha sem fio. Dentre eles podemos citar a própria renovação do Grupo de Trabalho (GT) Mesh por mais um ano pela RNP (2007); o projeto em parceria com a ANEEL (detalhes na página do PROJETO REMESH; 2007) para a construção de uma rede em malha para gerenciamento remoto em localidades de difícil acesso; o projeto RUCA (Rede para Um Computador por Aluno) onde a UFF foi a primeira universidade a ser escalada para os testes da interface de rede do XO, também conhecido publicamente como o "*laptop popular"* (CARRANO *et al,* 2007). Além dos novos projetos, a rede criada pelo projeto Remesh permitiu uma significativa contribuição à pesquisa e desenvolvimento através de palestras, minicursos e artigos publicados em congressos: PASSOS *et al,* 2006; ABELEM *et al,* 2007; MUCHALUAT-SAADE *et al,* 2007; PASSOS e ALBUQUERQUE, 2007; HIDEKI *et al*, 2007.

Outros projetos em redes mesh já foram implantados no Brasil e no exterior, principalmente partindo da iniciativa privada, como por exemplo pela CISCO (CISCO, 2007) na cidade de Tiradentes em Minas Gerais.

1.3 ESTRUTURA DA DISSERTAÇÃO

No Capítulo 2, mais projetos serão detalhados, bem como as métricas e os principais protocolos de roteamento *ad hoc* adotados para estas redes. Ainda no Capítulo 2, será feita uma breve explicação sobre o padrão de acesso adotado nestas redes, o IEEE 802.11, e suas extensões, dispensando uma atenção especial ao novo padrão IEEE 802.11s (padrão dedicado ao acesso para redes mesh). Em seguida, no Capítulo 3, o projeto Remesh será apresentado em detalhes: o procedimento de

construção do protótipo, a topologia, os esquemas de endereçamento, a nossa solução para prover simultaneamente o acesso e o roteamento na interface sem fio, as instalações externas e os problemas e soluções para a construção dos enlaces de rádio. No Capítulo 4, será discutido o protocolo de roteamento utilizado pelo projeto e as medições comparativas que foram realizadas para sua validação. O Capítulo 5 será dedicado à estrutura de controle de acesso e autenticação, bem como as ferramentas desenvolvidas e alteradas para a gerência do tráfego e da qualidade dos enlaces. Neste mesmo capítulo, medições na rede utilizada pelos voluntários (usuários da comunidade acadêmica) serão apresentadas visando a consolidação da funcionalidade do protótipo. Finalmente, no Capítulo 6 serão expostas nossas conclusões, comparações com demais projetos e propostas para trabalhos futuros. Propostas estas derivadas das avaliações e das dificuldades que foram encontradas ao longo do primeiro ano de execução do projeto.

Finalizando esta introdução, é importante ressaltar que o presente trabalho apresenta uma solução de baixo custo e de fácil implantação e disseminação para o provimento de acesso à Internet, mesmo em áreas geograficamente não propícias aos métodos tradicionais de instalação de infra-estrutura. Segundo MUCHALUAT-SAADE *et al* (2007), o Brasil é o sexagésimo segundo país no mundo em percentual da população com acesso à Internet, abrangendo somente 21% dos indivíduos acima de dez anos. A chamada "inclusão social", independentemente de posicionamentos filosóficos e políticos contra ou a favor, é um tema que merece atenção por parte da comunidade política, científica e empresarial. No Brasil, desde meados da década passada, vigorou um modelo social e educacional onde grande parte da população de baixa renda não tinha acesso à informação. Por mais que se defenda que esta situação esteja se revertendo, os custos a serviços básicos como telefonia e energia elétrica ainda são muito elevados em relação à renda média da população brasileira. A solução apresentada neste trabalho oferece uma alternativa viável para esta questão social.

2 TRABALHOS RELACIONADOS

Neste capítulo serão descritos os principais projetos em redes mesh, comerciais e universitários. Para uma melhor compreensão destes trabalhos, uma introdução à tecnologia de acesso IEEE 802.11 será feita. Em seguida, alguns protocolos de roteamento *ad hoc* mais pertinentes serão comentados.

2.1 O PADRÃO IEEE 802.11

O *Institute of Electrical and Electronic Engineers* (IEEE) realiza, dentre outras atividades, a elaboração de padrões para o setor de telecomunicações. O IEEE elaborou uma série dos padrões designados IEEE 802.x, que abrangem originalmente LANs (*"Local Area Networks"*) e MANs (*"Metropolitan Área Network"*), e mais recentemente passaram a incluir as PANs (*"Personal Area Networks"*). A família IEEE 802 é limitada a padronizar processos e procedimentos referentes às duas primeiras camadas do modelo da referência OSI (*Open System Interconnection*), a camada de enlace e a camada física. No modelo IEEE 802, a camada de enlace corresponde a duas subcamadas, a LLC ("*Logical Link Control"*) e a MAC ("*Medium Access Control*") (TANENBAUM, 2003).

No início da década de 1990, com o surgimento de diversas tecnologias proprietárias para WLANs, a *Federal Communications Comission* (órgão regulador dos EUA) solicitou ao IEEE que desenvolvesse um padrão que permitisse a fabricação de equipamentos que fossem capazes de interoperarem entre si, indepentendemente do fabricante. A partir desta demanda criou-se o grupo de trabalho IEEE 802.11 (IEEE 802.11; 2007), responsável por padrões que

especificam uma interface aérea entre um cliente sem fio e uma estação base ou ponto de acesso (Access Point) em redes de acesso local.

A subcamada MAC oferece dois tipos de controle de acesso, um assíncrono e outro síncrono, livre de contenção. Quando as estações se comunicam através de um ponto de acesso, o controle é dito síncrono (e não diretamente, umas com as outras). O controle síncrono é fornecido pela função de coordenação pontual (*Point Coordination Function* - PCF) que, basicamente, implementa o *polling* como método de acesso. O "coordenador pontual", normalmente o ponto de acesso, divide o tempo entre as estações participantes para que todas tenham a oportunidade de transmitir ciclicamente e sem colisões dentro de uma fatia do tempo.

Quando as estações se comunicam diretamente umas com as outras, o controle é dito assíncrono e a coordenação da rede acontece de forma distribuída. O controle assíncrono é realizado por um método de coordenação distribuída (*Distributed Coordination Function* - DCF). O DCF utiliza a técnica de acesso "*Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA)", na qual a estação que deseja transmitir ativa seu receptor para detectar a presença de portadora no meio antes de iniciar sua própria transmissão. Este método é semelhante ao CSMA/CD utilizado nas redes Ethernet que também se baseia na detecção de portadoras. Contudo, ao contrário do CSMA/CD, o CSMA/CA apenas evita as colisões no meio, ao invés de detectá-las, exatamente pela ausência da estrutura cabeada que permite a percepção de alterações nos níveis de tensão. Este método alternativo é utilizado porque os terminais do padrão 802.11 são *half-duplex* (por questões de custo e complexidade de construção), não podendo transmitir e receber simultaneamente (AKYILDIZ *et al,* 2005).

A detecção de portadora é feita de duas maneiras: utilizando o sinal de avaliação de canal livre (CCA - *Clear Channel Assessment*), de implementação obrigatória, ou utilizando pacotes RTS/CTS (*Request To Send/Clear To Send*) que utilizam um esquema de detecção de portadora virtual através de um vetor de alocação do meio (NAV – *Network Allocation Vector*), cuja implementação é opcional. O CCA funciona da seguinte maneira: se o meio estiver livre e permanecer neste estado por um tempo maior do que um intervalo de tempo bem definido (*Interframe Space*), a estação pode transmitir. Caso contrário, a transmissão é adiada por um de intervalo de espera aleatório, uniformemente distribuído, dentro de um período de tempo definido pela chamada "janela de contenção". O método com RTS/CTS utiliza o NAV. O NAV é um campo presente nos quadros CTS, RTS e de dados, que indica o tempo de duração da transmissão que está em andamento. Os elementos da rede, ao

identificarem o tempo do NAV, suspendem a detecção de portadora pelo período indicado (STALLINGS 2002).

A subcamada fisica do padrão IEEE 802.11 é dividida em duas subcamadas:

- Subcamada PLCP (*Physical Layer Convergence Procedure*), que mapeia os dados da subcamada MAC em quadros adequados à transmissão. O padrão IEEE 802.11 emprega três tipos diferentes de quadros: quadros de gerenciamento, de controle e de dados. O quadro de gerenciamento é utilizado para a associação e desassociação de uma estação com o ponto de acesso, para a sincronização e para procedimentos de autenticação. O quadro de controle é utilizado para o estabelecimento da conexão. O quadro de dados é utilizado para a transmissão. As estações são endereçadas conforme o padrão de endereçamento MAC de 48 bits. O campo de *payload* de dados é de tamanho variável (de 0 a 2312 bytes). O campo Type indica o tipo do quadro (gerenciamento, controle ou dados). O algoritmo CRC-32 (*Cyclic Redundancy Check* - 32 bits) é utilizado para detecção de erros.

- Subcamada PMD (*Physical Medium Dependent*), que recebe os quadros da camada PLCP e é responsável pela modulação, demodulação, detecção de portadora, transmissão e recepção.

Apesar do estabelecimento do padrão, a existência de três diferentes tecnologias de transmissão gerava problemas de interoperabilidade entre os dispositivos, o que provocava a insatisfação de fornecedores e clientes. Em 1997 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 garantindo a interoperabilidade. A ratificação da segunda geração do padrão IEEE 802.11, o 802.11b, foi concretizada em setembro de 1999. A WECA começou a testar e certificar os equipamentos de seus associados através do selo *Wireless Fidelity,* gerando o acrônimo *wi-fi*. Posteriormente a WECA mudou seu nome para Wi-Fi Alliance. Desde então, diversos grupos tarefa realizam pesquisas com o propósito de gerar novos complementos e melhorias ao padrão 802.11.

Atualmente, os padrões IEEE 802.11 *a*, *b* e *g* são os únicos que correspondem a diferentes implementações na camada física. O padrão 802.11h é uma versão do 802.11g padronizada para operar em conformidade com regulamentações específicas da Europa. O

padrão 802.11n permite taxas na ordem de 100 Mbps utilizando múltiplos rádios para recepção e transmissão em diferentes canais (MIMO – *Multiple Input Multiple Output*). O padrão 802.11a opera na faixa de 5GHz. No Brasil, a utilização desta faixa ainda está em fase de regulamentação. Nesta faixa, apesar do sinal se propagar por distâncias mais reduzidas, existem um total de 12 canais não sobrepostos, diferentemente dos padrões 802.11 b/g onde há somente 3.

O padrão 802.11b foi o primeiro a ser conhecido como Wi-Fi. Ele foi especificado para operar na banda ISM de 2,4 GHz utilizando DSSS (Direct Sequence Spread Spectrum) e permitindo atingir a taxa máxima de interface de 11 Mbps, com alcance típico em ambientes fechados de 50 a 100 metros, dependendo da quantidade de paredes e do número de obstruções. O sistema opera com 11 canais superpostos de 22 MHz cada. O padrão IEEE 802.11g foi também emitido em 2002 e ratificado em junho de 2003. Ele também opera na faixa de 2,4 GHz, porém com taxa máxima de interface de 54 Mbps. A mesma canalização do 802.11b é utilizada, permitindo que ambos os padrões sejam compatíveis. Desta forma, terminais de usuário 802.11b podem operar em redes servidas por pontos de acesso 802.11g e vice-versa. Entretanto, é preciso considerar que a presença de usuários 802.11b pode reduzir significativamente a vazão global em redes 802.11g, caso o transmissor não disponha de um sistema de ajuste dinâmico da taxa da interface. Existem outros padrões suplementares, abaixo listamos alguns que se destacam:

- IEEE 802.11e**:** responsável por desenvolver os mecanismos de qualidade de serviço (Quality of Service - QoS);

- IEEE 802.11f: Especifica o protocolo que permite o roaming entre APs de diferentes fabricantes;

- IEEE 802.11h**:** Esta extensão foi desenvolvida para resolver problemas de interferência de equipamentos 802.11a com equipamentos médicos e com os radares que utilizam a banda de 5 GHz;

- IEEE 802.11i**:** O padrão 802.11i, ratificado em Junho de 2004, fornece melhorias de segurança para redes Wi-Fi através de novos protocolos de cifragem denominados Temporal *Key Integrity Protocol* (TKIP) e *Advanced Encryption Standard* (AES);

- IEEE 802.11k**:** Proposta que estabelece regras para seleção de canais, roaming e controle de potência de transmissão, de modo a maximizar a taxa de transmissão da rede como um todo.

-IEEE 802.11r (STUART *et al*, 2004): Extensão que permite mobilidade com *hand-off* de clientes *wi-fi* entre diferentes pontos de acesso.

Recentemente um novo padrão de interesse ao presente trabalho surgiu. Trata-se do IEEE 802.11s (STUART *et al*, 2004), proposto para permitir o funcionamento de equipamentos dentro de uma estrutura de redes mesh, implementado no nível de enlace (camada 2).

2.1.1 O padrão 802.11s

O 802.11s especifica uma extensão à camada MAC do IEEE 802.11 para resolver o problema de interoperabilidade, definindo uma arquitetura e um protocolo que suporta envio de pacotes broadcast, multicast e unicast para realização de medidas rádio para a constituição de topologias em múltiplos saltos.

Os dispositivos em uma rede mesh 802.11s são denominados MP (*Mesh Point*). Os MP's da rede se intercomunicam, tal que cada trajeto pode ser estabelecido utilizando um protocolo de roteamento. O 802.11s define um protocolo imperativo de roteamento denominado HWMP (*Hybrid Wireless Mesh Protocol*), atuando na camada 2. O HWMP foi inspirado na combinação entre "*AODV*" (*Ad-hoc On-Demand Distance Vector;* PERKINGS, 2003) e "*tree-based routing*" (CLAUSEN *et al*, 2001 e 2003).

O MP pode ser um dispositivo individual que utiliza a rede mesh para se comunicar com os outros dispositivos na rede, como também pode ser um ponto de acesso, fornecendo acesso a outros clientes móveis. Ele pode ser um *gateway* para fornecer o acesso a uma rede *Ethernet* (ou IEEE 802.3) através de uma diretriz denominada "*Portal Mesh"*. Em ambos os casos, o 802.11s fornece um mecanismo de *proxy* que permite suporte ao endereçamento dos elementos participantes.

O padrão 802.11s também inclui mecanismos para o acesso determinístico à rede, para o controle do congestionamento e o para controle eficiente de energia. Desta maneira, é possível que os nós participantes definam a métrica mais adequada para a seleção dos melhores trajetos, baseado nas taxas exigidas pelas aplicações. A extensão utiliza mecanismos da segurança do padrão IEEE 802.11i, onde é possível a definição de uma única entidade administrativa para a segurança da rede. A extensão também permite o uso de mais de um rádio em cada nó.

O formato do cabeçalho MAC consiste de 24 bits que inclui campos como TTL (“*Time To Live”*) utilizado para prevenir seqüências infinitas de saltos entre os nós, número de seqüência fim-a-fim, utilizado para fluxos *broadcast* e outros serviços. Há dois tipos de quadros de controle propostos no IEEE 802.11s: *Request To Switch* (RTX) e *Clear To Switch* (CTX). Estes campos são necessários para permitir a troca do modo de operação, de acordo com as “informações elementares”. As informações elementares estão presentes em cada nó da rede mesh e podem ser consultadas por seus respectivos vizinhos. Ela consiste nos seguintes dados:

1. *Mesh ID*
2. *Mesh capability*
3. *Neighbor list*
4. *MPP reachability*
5. *Peer request*
6. *Peer response*
7. *Active profile announcement*

Estas informações são utilizadas por funções básicas da rede, tais como a descoberta de vizinho, roteamento HWMP, controle de congestionamento, *beaconing*, sincronização, acesso determinístico à rede e informações de controle do 802.11.

Uma topologia mesh pode ser composta por nós com mais de uma interface de rádio e pode utilizar um ou mais canais. Quando a opção de troca de canal não é suportada, cada nó opera sobre o mesmo canal ao mesmo tempo. Entretanto, o canal pode ser mudado ao longo do tempo, de acordo com os requisitos de controle de um mecanismo denominado DFS (“*Dynamic Frequency Selection*”). A seleção de um canal específico pode variar com diferentes requisitos da aplicação. A interface lógica de rádio estabelece um enlace com o vizinho para a obtenção do *mesh ID* (identificador mesh), do *mesh Profile* (perfil mesh) e para a seleção do canal.

O procedimento de geração do *beacon* é opcional no 802.11s e está baseado nos procedimentos e cláusulas do 802.11. A sincronização pode ser realizada nos modos síncrono ou assíncrono. No modo assíncrono, o nó pode escolher seu próprio intervalo de tempo para o envio do *beacon* e pode implementar um mecanismo de controle de colisão para evitar transmitir simultaneamente com seus vizinhos.

O MAC do IEEE 802.11 está baseado em contenção, e utiliza a função do mecanismo de coordenação distribuída (DCF-*"Distributed Coodination Function"*), como explicado anteriormente. Dois mecanismos são adaptados ao padrão 802.11 para estabelecer serviços wlan na rede mesh:

1. Multichannel MAC
2. MDA (Acesso determinístico)

No padrão 802.11, a camada MAC foi planejada para funcionar sobre um único canal. O *multichannel* MAC utiliza canais ortogonais para realizar transmissões simultâneas onde o desempenho agregado pode ser incrementado consideravelmente. Os benefícios sobre o uso de múltiplos canais são relatados em AGUAYO *et al* (2004) e DRAVES *et al* (2004[a]).

O *Mesh Deterministic Address* (MDA) é um método de acesso determinístico que permite a escolha dos canais com baixa contenção. O método configura o período de tempo nos vizinhos para evitar a interferência com as outras transmissões.

Quanto à descoberta da rede, o padrão requer que todos os integrantes da rede mesh forneçam suas próprias informações e de seus vizinhos diretos para permitir as conexões entres eles. Este processo utiliza a transmissão de *beacons* ou buscas diretas para a detecção dos integrantes. Em seguida, é realizada a troca de informações de rotas, que podem conter a informação do estado do enlace. A formação da rede mesh é realizada através de um processo contínuo que requer o monitoramento constante dos nós vizinhos. Cada nó é responsável pelas informações de conectividade dos seus vizinhos para poder reagir adequadamente às mudanças. Existem dois elementos essenciais na descoberta da rede. São eles:

1. Descoberta da topologia, composta por:
    a. Identificador Mesh
    b. Identificador do protocolo para a seleção das rotas
    c. Identificador de métricas para a seleção das rotas
2. Descoberta dos vizinhos: Depende da recepção do *beacon* com as informações dos identificadores da topologia mesh. Deve conter a informação de pelo menos um perfil de um nó e as capacidades da rede: versão e indicadores de atividade do nó.

Na Figura 1 estão ilustradas, esquematicamente, as entidades preconizadas pelo padrão para o estabelecimento da comunicação.

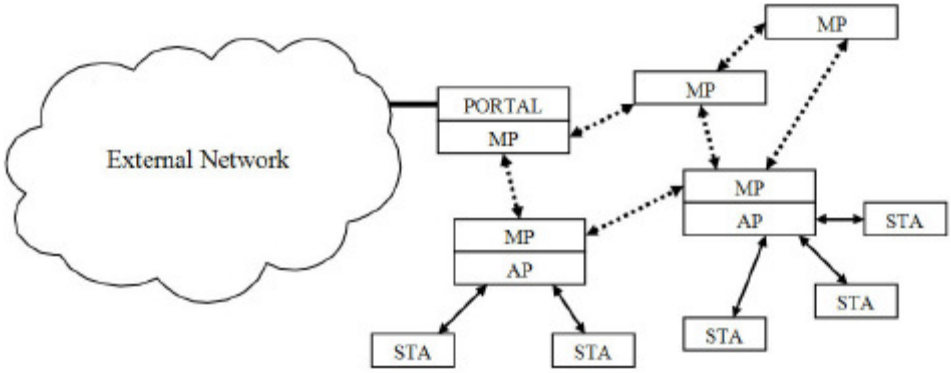


Figura 1: Arquitetura das entidades envolvidas no padrão 802.11s (fonte: HIDEKI *et al*, 2007)

Mais informações sobre o padrão IEEE 802.11s podem ser obtidas em HAUSER e BAKER (2003) e IEEE 802.11(2007). O projeto RUCA ("Rede para Um Computador por Aluno") financiado pela RNP (2007) trabalhou com o laptop de baixo custo, "XO", desenvolvido pelo projeto OLPC ("*One Laptop Per Child"*) no MIT. O XO utiliza uma interface sem fio que implementa parte das especificações do padrão IEEE 802.11s (LAPTOP.ORG 2007; CARRANO *et al,* 2007, HIDEKI *et al*, 2007).

2.2 MÉTRICAS DE ROTEAMENTO E PROTOCOLOS *AD HOC*

Nesta subseção serão abordadas as métricas e os protocolos de roteamento *ad hoc* mais conhecidos. As redes mesh e as redes *ad hoc* usam o mesmo mecanismo principal: comunicação entre nós através de múltiplos saltos sem fio em uma topologia em malha. Com a principal diferença de que as redes mesh são focadas em dispositivos estáticos, provendo maior confiabilidade. O roteamento deve prover o melhor caminho entre os nós da rede para uma comunicação eficiente, tendo que lidar com as dificuldades da interface rádio e suas freqüentes mudanças.

As redes mesh têm algumas funcionalidades em comum com redes ad hoc, os protocolos desenvolvidos para redes ad hoc são normalmente utilizados em redes mesh com algumas modificações. Esses protocolos estão em constante pesquisa devido a alguns aspectos:

- Na maioria dessas redes os nós são estáticos ou têm pouca mobilidade e não dependem de baterias. Logo o foco dos algoritmos de roteamento é aumentar a vazão e o desempenho da rede ao invés de mobilidade e uso de baterias;

- Novas métricas de roteamento são necessárias para aumentar o desempenho de redes mesh.

A principal tarefa dos protocolos de roteamento é a seleção do caminho entre o nó de origem e o nó de destino. Isso tem que ser feito de forma confiável, rápida, e com o mínimo "overhead". Em geral, os protocolos de roteamento podem ser classificados em: baseados na topologia e baseados na posição. Os protocolos baseados na topologia escolhem caminhos baseado nas informações de qualidade dos enlaces entre os nós. Os protocolos baseados na posição escolhem os caminhos baseados em informações geográficas através de algoritmos geométricos.

Os protocolos baseados na topologia são subdivididos entre reativos e pró-ativos. Os reativos computam uma rota apenas quando é necessário. Esse método reduz o controle de *overhead,* porém aumenta a latência devido ao tempo de configuração gasto para a montagem da rota sob demanda. Nos protocolos pró-ativos, todos os nós sabem todas as rotas para qualquer nó na rede. A latência de montagem das rotas diminui, entretanto um controle de *overhead* mais eficiente é necessário para a manutenção permanente. Ainda existem os protocolos híbridos, que combinam as vantagens dos dois protocolos acima mencionados.

Os protocolos de roteamento *ad hoc* calculam rotas com o menor custo entre os nós de origem e o nó de destino. Esse custo é calculado através de métricas de roteamento. Cada rota tem uma métrica que é usualmente a soma de todas as métricas dos enlaces contidos na rota.

As métricas de roteamento têm que satisfazer quatro requisitos:

- Assegurar estabilidade das rotas, isto é, alteração não freqüente de rotas;
- Determinar rotas com o menor custo eficientemente;
- Algoritmos eficientes para cálculos de rotas;
- Assegurar encaminhamento sem "loop".

De acordo com o protocolo de roteamento usado, algumas métricas são mais eficazes ou não. A seguir algumas métricas são descritas:

Número de saltos ("hop count") (CLAUSEN, 2001; AKYILDIZ *et al,* 2005)

Esta métrica tem como objetivo minimizar o número de nós em cada rota. De um outro ponto de vista, pode-se dizer que ela atribui a todos os enlaces o mesmo peso, sem

verificar qualquer característica dos mesmos. A única informação necessária para a sua implementação é a da vizinhança de cada nó, o que é facilmente obtido através do envio periódico de pacotes de broadcast.

Se por um lado esta abordagem é bastante simples, diminuindo o *overhead* do sistema e da rede, por outro lado ela claramente deixa de levar em consideração aspectos fundamentais na sua avaliação. Em redes sem fio, enlaces são afetados por vários fatores, como distância entre os nós, obstáculos e interferências. Desta forma, esta métrica em geral apresenta um desempenho ruim, já que tende a escolher enlaces longos demais, levando à altas taxas de perda de pacotes e baixa vazão. A métrica *hop count* é a utilizada na descrição do protocolo OLSR (CLAUSEN *et al*, 2003) e foi inicialmente utilizada na sua implementação (OLSR, 2006).

Expected Transmission Count (ETX) (COUTO *et al*, 2003)

A métrica ETX tem por objetivo aumentar a vazão conseguida na rede. Para isto, é utilizada a escolha de rotas que diminuam o número total de transmissões no nível de enlace (nível 2), ao longo do caminho. Dada a probabilidade "*Pab"* de sucesso na transmissão de um pacote pelo enlace entre dois nós *a* e *b*, o número de transmissões necessárias para que este envio ocorra é 1/ *Pab* . Assim, define-se o ETX de um enlace como o inverso da probabilidade de sucesso na transmissão de um pacote através deste enlace. Ou seja:

$$ETX_{ab} = \frac{1}{P_{ab}}$$

Seguindo este raciocínio, define-se o ETX de um caminho formado por *n* enlaces como o somatório de todos os valores de ETX:

$$ETX_n = \sum_{i=1}^{n} \frac{1}{P_i},$$

Onde *Pi* denota a probabilidade de sucesso no i-ésimo enlace do caminho.

Pelas definições, fica claro que é necessário obter as probabilidades de sucesso dos enlaces para calcular o ETX. Para inferir tais valores, os autores propõem a utilização de pacotes de broadcast. Pelo padrão 802.11, tais pacotes não sofrem retransmissão e são transmitidos na taxa mais baixa da interface (1 Mbps), fazendo com que seja possível estimar a probabilidade de sucesso através da seguinte fórmula:

$$P_{ab} = \frac{s}{w}$$

Na expressão, *w* é o tamanho de uma janela de transmissões considerada (por exemplo, dos últimos 10 pacotes), enquanto *s é* o número de sucessos obtidos.

Expected Transmission Time (ETT) (DRAVES *et al*, 2004[a])

A métrica ETT é uma modificação da métrica ETX para ajustar o cálculo das probabilidades de perdas dos enlaces. Ele utiliza a taxa de transmissão da interface, juntamente com a taxa de perda de pacotes:

$$\mathrm{ETT} = \mathrm{ETX} \times \frac{S}{B}$$

Onde S é o tamanho do quadro definido pelo próprio protocolo. A taxa de pacotes B pode ser estimada pela técnica de pares de pacotes (*packet pair probing*). Cada nó envia dois pacotes de investigação, ida e volta, para seus vizinhos periodicamente. O primeiro é pequeno e o segundo é maior. A diferença entre os tempos de recebimento dos dois pacotes é calculada. A taxa é obtida dividindo-se o tamanho dos pacotes pelo intervalo entre os recebimentos. Como não é possível garantir que os pacotes serão enviados sem atraso entre eles, é proposta a utilização de uma seqüência de 10 envios, onde o menor intervalo será contabilizado. Análogo ao ETX, a métrica total da rota é a soma de todos os ETT's dos enlaces contidos no caminho.

Weighted Cumulative Expected Transmission Time (WCETT) (DRAVES *et al,* 2004[a])

Trata-se da métrica implementada no projeto da Microsoft. É uma modificação da métrica ETT para redes em que são usados múltiplos rádios e diversidade de freqüências. Basicamente a métrica utiliza os múltiplos canais disponibilizados pela utilização de mais de um rádio (diversidade de freqüência) e, através de pesos, diferencia os que estão menos congestionados para o envio. Sem a utilização de múltiplos rádios, a métrica é semelhante à ETT.

Modified Expected Number of Transmissions (mETX) (KOKSAL e BALAKRISHNAN, 2006)

Esta métrica preconiza que o ETX, por ser baseado em sucessos na transmissão no nível de enlace, não consegue captar as variações do canal rádio que ocorram em intervalos de tempo menores do que o tempo de transmissão do quadro. A idéia proposta é avaliar a qualidade do canal através da quantidade de bits transmitidos com erro, dentro de cada quadro de nível de enlace. Desta forma, espera-se obter a qualificação do canal dentro de intervalos de tempo menores. A estimação é realizada através do envio de quadros com seqüências de bits conhecidas. O pacote recebido é comparado com o esperado e a probabilidade é calculada. Além de representar grande complexidade para o sistema, quadros de nível de enlace não recebidos corretamente são descartados sem nenhuma notificação para as camadas superiores. A métrica mETX, segundo os seus proponentes, obteve uma redução de 50% de perda de pacotes em comparação com a métrica ETX. Entretanto, os resultados são simplesmente analíticos, obtidos com parâmetros derivados de observações de redes mesh reais.

Effective Number of Transmissions (ENT) (KOKSAL e BALAKRISHNAN, 2006)

Proposto pelos mesmos autores da métrica mETX. Surgiu da idéia de que os erros nos enlaces sem fio ocorrem em rajadas. Desta forma, se um enlace é definido com 10% de taxa de perda, é esperado que de 100 pacotes transmitidos, os 10 erros ocorram em seqüência. O objetivo do ENT é realizar uma estimativa prévia de pacotes que possuam alta probabilidade de perda e impedir o seu envio, evitando o desgaste que as perdas ocasionam principalmente nas camadas mais altas (como ocorreria com o TCP, na camada de transporte). Este cálculo leva em consideração o número de retransmissões que ocorre no nível 2 antes do pacote ser descartado completamente (normalmente 7 vezes). Portanto, após a realização de uma medição, um enlace que possua uma alta taxa de perdas naquele instante, será desconsiderado (devido à característica proposta de que os erros ocorrem em rajadas) e não computado como uma possível rota. Desta forma, um benefício que o ENT pode trazer é a redução do número total de rotas presentes na topologia, diminuindo o gasto no processamento total da rede.

A métrica empregada na qualificação dos enlaces pode alterar por completo o funcionamento do protocolo. No Capítulo 4 será demonstrado como uma pequena alteração

na métrica utilizada na implementação do protocolo OLSR (ETX) resultou em medições completamente distintas.

Existem diversos protocolos *ad hoc* disponíveis atualmente. Abaixo serão apresentados os três protocolos *ad hoc* mais freqüentes nos projetos de redes mesh que serão abordados:

- DSR (Dynamic Source Routing; JOHNSON *et al,* 2001, 2002)

O DSR é um protocolo reativo. Ele é baseado em um algoritmo do tipo *source-routing*, isto é, o nó de origem determina qual a rota que o pacote deve seguir pela rede. Não são enviadas mensagens periódicas de troca de informações de roteamento, o que garante um melhor uso da banda disponível. Uma versão derivada do DSR é utilizada pela rede desenvolvida pelo projeto de redes mesh da Microsoft, juntamente com a métrica WCETT. A versão do protocolo é denominada MR-LQSR ("*Multi-radio Link-Quality Source Routing"*; DRAVES *et al,* 2004[b]).

No DSR, o nó de origem determina a rota completa que um pacote deverá seguir pela rede. Acrescentando esta informação ao cabeçalho do pacote, a origem inicia a transmissão, enviando o pacote para o primeiro nó indicado em uma lista. Cada nó armazena as rotas aprendidas, e, ao receber um pacote, verifica se possui uma rota para o nó de destino desejado. Se existir, o nó de origem emprega esta rota para enviar o pacote; caso contrário utiliza o protocolo de descobrimento de rotas para encontrar um caminho para o nó desejado. Cada rota armazenada possui um tempo de existência. Depois de expirado o tempo de existência da rota, o nó assume que ela não existe mais e a retira de sua tabela. Os nós sempre utilizam o protocolo de descobrimento de rotas quando ocorre um erro no roteamento, uma mudança de posição ou o desligamento de um nó.

Como a topologia em redes *ad hoc* é altamente dinâmica, o algoritmo contém um mecanismo para manutenção de rotas. Cada nó pode monitorar os pacotes de confirmação de outros nós ou ouvir todas as comunicações que passam por ele (modo promíscuo). Assim, cada nó pode observar a ocorrência de problemas com os nós vizinhos, procurando enviar um pacote com informação de erro para a origem. Para este caso, o nó de origem pode optar por utilizar uma rota que esteja armazenada ou iniciar um processo para seleção de uma nova rota.

- AODV (Ad hoc on-demand distance vector; PERKINS*,* 2003)

Utilizado no projeto Meshnet da universidade de Santa Bárbara (CAMDEM *et al,* 2004). Semelhante ao DSR, o protocolo AODV é um protocolo reativo. Ele funciona criando enlaces reversos para que o nó de destino saiba a seqüência de nós que os pacotes devem seguir até o nó de origem. Nesse protocolo, quando a origem precisa de uma rota para um determinado destino que não conste de sua tabela, inicia-se um processo para descobrimento de rota. Esse processo consiste da transmissão, usando *flooding*, de um pacote de requisição de rota "*RREQ"* a todos os seus nós vizinhos, que, por sua vez, propagam esta requisição aos demais nós. O processo se repete até que o destino seja alcançado ou até que um outro nó conhecedor da rota até o destino seja encontrado. Durante esse processo de descobrimento da rota, os nós que recebem o *RREQ* incluem entradas temporárias em suas tabelas, registrando a origem da mensagem de *RREQ*. Quando o destino ou um nó intermediário que conheça uma rota para o destino é encontrado, um pacote de *RREP* é enviado de volta à origem. Enquanto a mensagem *RREP* é propagada, cada nó intermediário que a recebe incrementa o campo correspondente à quantidade de saltos necessários para se alcançar o nó de destino.

No protocolo AODV, cada nó procura transmitir mensagens, denominadas "*hello",* periódicas aos seus nós vizinhos que possuam rotas que passem por ele. Desta forma, seus vizinhos podem manter-se atualizados sobre a existência ou não de uma rota. Caso as mensagens de *hello* de um determinado nó não sejam recebidas durante um período de tempo determinado, assume-se que ocorreu uma quebra em algum enlace, tornando-a inválida. Se a rota ainda estiver sendo usada, o nó pode realizar uma nova requisição - *RREQ* - para seleção de uma nova rota.

- OLSR (Optimized Link State Routing (CLAUSEN *et al*, 2001)

Utilizado no projeto VMesh (TSARMPOPOULOS *et al,* 2005) e no projeto Remesh (2007). É um protocolo pró-ativo. O protocolo OLSR destina-se a redes de alta escalabilidade. Baseia-se em uma técnica de *flooding* denominada *Multipoint Relaying* (MPR) para a disseminação dos pacotes de broadcast para controle. O método empregado pelo OLSR é o seguinte:

(1) Cada nó difunde, periodicamente, mensagens denominadas "*hello",* que contêm informações relacionadas aos seus vizinhos afastados em um salto. O campo TTL *(time to live)* da mensagem de *hello* é igual a '1', desta forma a mensagem não é reenviada

pelos seus vizinhos. Com o auxílio das mensagens de *hello*, os nós obtêm informações topológicas locais;

(2) Um nó denominado de *seletor* escolhe um conjunto de vizinhos para atuar como seus nós MPR. Um MPR é um nó intermediário através do qual a origem alcança os demais nós de destino, via múltiplos saltos. A informação do MPR e dos seus próprios vizinhos são enviadas nas próximas mensagens de *hello*;

(3) Os nós MPR desempenham dois papéis:

- São eles que retransmitem os pacotes de *broadcast* enviados por outros nós seletores;
- Os nós MPR, periodicamente, difundem sua lista de seletores presentes na rede (empregando *flooding*) através das suas mensagens de *hello*. Desta forma, cada nó da rede reconhece por qual MPR um determinado nó pode ser alcançado;
- Estas duas características acima reduzem, respectivamente: o número de retransmissões na rede de pacotes de *hello*; e o tamanho do pacote de *broadcast* que conterá um número menor de nós vizinhos.

(4) Com a informação da topologia global armazenada e atualizada em cada nó, o caminho mais curto entre o nó de origem e de destino é computado através do Algoritmo de *Dijkstra* (TANENBAUM, 2003).

Demais protocolos *ad hoc* desenvolvidos especificamente por projetos mesh serão abordados ao longo da próxima subseção.

2.3 PROJETOS DE REDES MESH

As redes mesh estão sendo amplamente estudadas e diferentes soluções estão sendo propostas por grupos de pesquisa ou empresas. Atualmente, inúmeras iniciativas relacionadas à implantação de projetos utilizando redes mesh vêm sendo conduzidas. Nesta subseção apresentaremos os principais trabalhos em redes mesh, tanto os de caráter acadêmico e científico como as soluções comerciais que estão sendo propostas por empresas como NORTEL e CISCO.

2.3.1 Roofnet

O *Roofnet* (AGUAYO *et al*, 2004) é uma iniciativa do Laboratório de Ciência da Computação e Inteligência Artificial (CSAIL) do Instituto de Tecnologia de Massachusetts (MIT). Seu objetivo é estudar as questões envolvidas em redes sem fio de grande escala.

A rede do projeto Roofnet consiste de 20 nós (ROOFNET HOME PAGE, 2007) espalhados por uma área urbana próxima à universidade. O *hardware* de cada nó *Roofnet* é padronizado e fornecido pela equipe do MIT. São utilizados desktops com sistema operacional *Linux*, disponíveis em um gabinete compacto e resistente; cartão *wireless* padrão 802.11b, baseado no *Intersil Prism 2.5 chip-set,* uma antena omni-direcional (verticalmente, a antena possui um diagrama de irradiação com um feixe de cobertura de 20º), para instalação no topo dos edifícios de voluntários. A potência de saída dos rádios é de 200 mW, operando todos no mesmo canal 802.11b. Os desktops dos voluntários são ligados aos nós por meio de cabeamento *Ethernet*. O acesso à Internet é fornecido por voluntários que possuam outros meios de acesso particulares e estejam dispostos a compartilhar banda.

O roteamento é feito através de um protocolo desenvolvido pelo próprio projeto chamado *Srcr*. Trata-se de um protocolo híbrido, baseado no DSR. A diferença básica entre ambos reside na métrica utilizada para determinação das rotas. Enquanto o protocolo DSR utiliza o número de saltos, o *Srcr* utiliza a métrica "*Estimated Transmission Time" (ETT)*, que contabiliza a taxa de perda e envio de pacotes, estimando o atraso dos enlaces. O protocolo *Srcr* tenta encontrar a rota que forneça a maior vazão entre quaisquer pares de nós da rede, escolhendo a de menor valor de *ETT*. O protocolo *Srcr* considera que a rota escolhida reúne as condições mais favoráveis para trafegar a maior quantidade de pacotes por unidade de tempo. As retransmissões de nível de enlace necessárias são consideradas nos cálculos.

Quanto ao desempenho, a rede Roofnet apresenta valores típicos de vazão da ordem de 400 kbps em média e 627 kbps de pico. Para rotas com até 3 saltos, a taxa média obtida foi de 379 kbps e para rotas com até 7 saltos, 160 kbps. Segundo os autores, os valores obtidos são comparáveis às taxas encontradas em redes do tipo DSL tradicionais.

A rede Roofnet apresenta viabilidade de instalação em larga escala com valores razoáveis de utilização. Apesar disto, alguns pontos negativos são enumerados:

- O protocolo de roteamento *Srcr*, provavelmente, não seria escalável para valores em torno de algumas centenas de nós, em função da plataforma escolhida pelo *MIT* ser baseada no protocolo DSR;

- É preciso haver uma boa distribuição de nós com acesso fixo à Internet para que toda a rede obtenha acesso com taxas mínimas desejáveis;

- O custo do *hardware* é relativamente alto.

2.3.2 VMesh

Em TSARMPOPOULOS *et al* (2005) é apresentado o modelo da rede mesh que foi desenvolvida na Universidade de Thessaly, na cidade de Volos, na Grécia. O objetivo deste projeto é implantar uma rede mesh de baixo custo, utilizando roteadores 802.11b/g *off-theshelf* (fabricados na universidade). Os roteadores empregados são WRT54G da Linksys (LINKSYS, 2007) e executam uma distribuição peculiar do Linux, o OpenWrt (OPENWRT, 2006). A rede opera no modo *ad hoc*, utilizando o protocolo OLSR. Um ponto importante desse projeto é que os estudantes, funcionários e professores recebem acesso aos servidores da universidade e à Internet a partir de suas casas.

A arquitetura projetada pelo grupo da Universidade de Thessaly inclui vários elementos estacionários e nós móveis (Figura 2). Esses elementos fixos seriam os roteadores sem fio, instalados no topo dos prédios e telhados, equipados com antenas omni-direcionais de ganho entre 8 e 15 dBi. Sua principal função é de permitir que um ou mais dispositivos clientes se conectem localmente para ter acesso ao resto da rede. Entretanto, a rede do projeto VMesh também permite a presença de nós móveis que estejam executando o protocolo OLSR. O controle ao acesso é feito através de tunelamentos, permitido somente aos voluntários cadastrados.

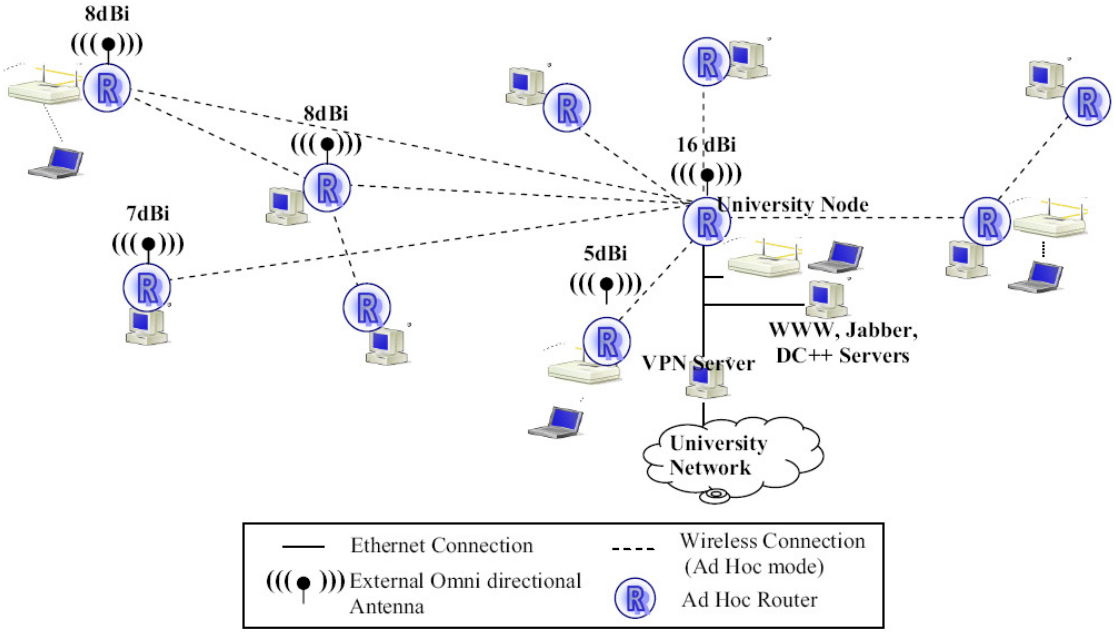


Figura 2: Arquitetura da rede do projeto VMesh

O projeto tem também como objetivo a criação de uma plataforma de testes para pesquisa e avaliação de algoritmos e *softwares,* na área de redes e de sistemas distribuídos. O endereçamento dos roteadores é estático e dos usuários é dinâmico. Cada roteador suporta até 29 dispositivos conectados a ele pela interface *Ethernet.* Eles são registrados em um servidor central e recebem um endereço IP pelo servidor DHCP do próprio roteador.

O *hardware* escolhido para implantação dos nós preconizou o custo, razão pela qual roteadores baseados em desktops (como no projeto Roofnet) foram descartados. Durante os estudos iniciais para determinação do *hardware* a ser empregado, preliminarmente foi encolhido um dispositivo denominado *Wireless Router Application Platform (WRAP).* A equipe do projeto desenvolveu, inicialmente, um roteador sem fio usando placas WRAP e duas interfaces *mini-pci (modelo 2.5 da Prism).* Entretanto, apesar do bom desempenho apresentado, o custo total do equipamento ficou inviável para o público-alvo formado por estudantes universitários.

Numa mudança de estratégia, os criadores do projeto procuraram por soluções comerciais disponíveis no mercado que atendessem aos requisitos de desempenho e custo definidos pelo projeto. O projeto então migrou para uma plataforma baseada nos roteadores WRT54G e sistema operacional embarcado Linux. O desempenho da plataforma final WRT54G/Linux apresentou valores típicos de vazão entre nós na ordem de 4400 kbps.

O projeto Vmesh permitiu um avanço significativo nas pesquisas relacionadas à área de redes mesh, pois foram os precursores da solução de mais baixo custo. Diversos fatores importantes devem ser ressaltados:

– A plataforma escolhida para o hardware, o sistema operacional e o esquema de endereçamento garantiram a flexibilidade necessária à implantação em larga escala da rede. Como será abordado no próximo capítulo, o projeto Remesh adotou estas mesmas características*;*

– O desempenho da rede mostrou-se satisfatório, considerando-se as limitações impostas pela tecnologia;

– O custo do conjunto *hardware/software* é baixo, o que permitiu a expansão da rede. Os voluntários adquiriam os equipamentos com recursos próprios e os administradores do projeto os preparavam para a implantação.

Numa rede comunitária é importante garantir que seus participantes não irão ser capazes de explorar e utilizar as informações que forem roteadas através dos nós de acesso. Usuários que não estiverem associados ao projeto não possuem acesso liberado à infra-estrutura da universidade. Desta forma, o controle de acesso à rede e a segurança são implementados através de VPN's ("Virtual Private Network"[2]).

O servidor VPN está instalado em um desktop que autentica e autoriza o acesso à rede da universidade. Ele é equipado com duas interfaces *Ethernet*. A primeira é conectada à rede local da universidade e à Internet. A segunda é conectada diretamente à interface *Ethernet* de um dos roteadores, fazendo a interligação da rede mesh comunitária. Desta maneira, todos os dispositivos que estiverem conectados à rede mesh precisarão passar pelo servidor VPN para utilizar os serviços fornecidos pela universidade.

2.3.3 Microsoft Research

A *Microsoft Research* possui uma equipe dedicada para pesquisar redes mesh comunitárias. O projeto é denominado "*Self-Organizing Neighborhood Wireless Mesh Networks"*. O objetivo é a pesquisa de tecnologias que viabilizem a implantação de redes do

[2] Uma VPN é uma rede de comunicação privada, utilizada para que entidades como empresas ou universidades, possam se comunicar através de uma rede pública utilizando protocolos de segurança e mecanismos de autenticação. (PETERSON E DAVIE, 1999)

tipo mesh a médio e longo prazo, de maneira escalável e confiável (DRAVES *et al,* 2004[a] e [b]).

Os experimentos realizados até agora pela *Microsoft Research* tiveram menor escala do que os do Roofnet, envolvendo poucas dezenas de nós em uma área muito menor. Um deles foi realizado em apartamentos de um condomínio localizado próximo à sede da empresa; outro, dentro das dependências da própria empresa. O *hardware* utilizado é o próprio *PC* dos usuários. O *software* consiste de um *driver* para o sistema operacional *Windows* que cria uma camada virtual entre as camadas de enlace e de rede.

O protocolo de roteamento utilizado pelo projeto é denominado *Multi-Radio Link-Quality Source Routing (MR-LQSR)*. O protocolo *MR-LQSR* é uma combinação do protocolo *Link-Quality Source Routing (LQSR)* (DRAVES *et al,* 2004 b) com a métrica *Weighted Cumulative Expected Transmission Time (WCETT)* (DRAVES *et al,* 2004 a). O protocolo *LQSR* é um protocolo do tipo *source-routed link-state* derivado do DSR, a exemplo do *Srcr*, diferindo deste nas métricas definidas. O *MR-LQSR* pretende ser um aperfeiçoamento do *Srcr*, levando em conta as taxas de transferência e de perda de pacotes obtidas com a utilização simultânea de múltiplos canais. Ele foi desenvolvido para o uso de nós que dispõem de mais de um rádio.

A equipe da *Microsoft Research* desenvolveu um *framework* de gerenciamento de falhas para redes *mesh*. Este gerenciamento consiste da detecção, isolamento e diagnóstico de falhas. A abordagem adotada consiste em reproduzir em um simulador os eventos ocorridos na rede a partir de dados coletados. Determinando, deste modo, o comportamento que a rede teria em diversas condições, permitindo o diagnóstico de problemas e das condições de tráfego da rede.

Os pesquisadores da *Microsoft* concluíram que as redes mesh são viáveis, mas as tecnologias existentes, atualmente, ainda são inadequadas. Eles crêem que será possível em médio prazo, ter redes deste tipo operando em situações reais considerando o trabalho que vem sendo desenvolvido pela empresa em paralelo ao desenvolvimento da indústria de *hardware* e dos organismos de padronização.

A Microsoft desenvolveu um conjunto de ferramentas para desenvolvimento de aplicativos para redes mesh, com objetivo de ser utilizado principalmente por instituições acadêmicas: "*Microsoft Mesh Toolkit"*. A solução presente neste kit foi implementada através de uma camada chamada *Mesh Connectivity Layer* ou simplesmente MCL. Estão presentes

neste kit alguns outros softwares como o *Venice*, que faz a instalação da MCL, e algumas ferramentas de medição de desempenho.

O MCL é um *driver* que implementa um adaptador virtual de rede. A rede mesh que estiver disponível para conexão, irá aparecer para o usuário através desta interface. Ele é implementado entre as camadas de enlace e de rede. Para as camadas mais altas, ele é visto como mais uma interface *Ethernet*, embora seja virtual. Para as camadas mais baixas, o MCL aparece como apenas um outro protocolo que está sendo executado acima do nível físico.

Três métricas são utilizadas para medição da qualidade dos enlaces: a primeira é o "*Expected Transmission Count"* (ETX), obtida através da medição da taxa de perda de pacotes *broadcast* entre pares de nós vizinhos, e apresentou melhor desempenho quando todos os nós da rede eram estacionários; a segunda métrica é a "*Per-hop Round Trip Time*" (RTT), que mede o atraso da transmissão, ida e volta, através de pacotes de sondagem unicast entre nós vizinhos; a terceira é chamada de "*Per-hop Packet Pair Delay*" (PktPair) e é baseada no atraso entre um par de pacotes enviados *back-to-back* para um nó vizinho (técnica de *packet pair*, semelhante ao utilizado pela métrica ETT).

A utilização de múltiplos rádios em cada nó permite o aumento da capacidade de transmissão global da rede. Cada nó utiliza dois ou mais rádios que irão trabalhar em canais com freqüências distintas. Isto possibilita que os nós possam receber e enviar pacotes simultaneamente. Em um sistema de apenas um rádio, cada nó precisa sincronizar suas transmissões e recepções de pacotes.

2.3.4 MeshNet

Desenvolvida na Universidade da California, o experimento *Santa Barbara Mesh* trata-se de uma rede sem fio instalada no campus da Universidade de Santa Bárbara, com um total de 25 nós equipados com rádios 802.11a/b/g. Os nós são distribuídos em cinco andares dentro do prédio do departamento de Engenharia (CAMDEN *et al,* 2004).

A rede está sendo utilizada para o desenvolvimento de protocolos e sistemas para operações robustas de redes sem fio com múltiplos saltos. Especificamente, a rede está sendo utilizada para conduzir pesquisas sobre protocolos de roteamento escalonáveis, gerenciamento eficiente de redes, *streaming* multimídia e soluções de QoS. Eles desenvolveram ferramentas de acompanhamento via web que permitem a visualização de parâmetros da rede em tempo real.

Os roteadores utilizados são dois Linksys WRT54G “amarrados” um ao outro (ilustrado na Figura 3). Um deles é nó da rede mesh, executando o protocolo de roteamento AODV. O outro é usado para gerenciamento fora da faixa de freqüência do canal da rede mesh. Este segundo roteador está conectado a uma rede sem fio, também localizada no mesmo prédio, permitindo o acesso por parte dos operadores. Ambos os roteadores estão interconectados um ao outro através de um segmento de cabo CAT5 nas suas portas *Ethernet*.

Figura 3: Dois roteadores WRT54G da Linksys ligados por suas portas *Ethernet* formando o nó da rede Meshnet

A rede possui ainda um *gateway* para o escoamento do tráfego da rede mesh para a Internet. O *gateway* é um desktop com sistema operacional Linux. Ele é equipado com uma interface de rede *pcmcia* sem fio padrão 802.11b e uma interface *Ethernet*. A interface sem fio é utilizada para interconectar o gateway à rede mesh, enquanto que a interface cabeada é utilizada para prover o acesso à Internet.

O principal objetivo do projeto Meshnet é o desenvolvimento de pesquisas. Alguns módulos específicos para monitoramento e gerenciamento de redes mesh foram desenvolvidos:

- **MeshViz** (UCSB MESHNET, 2007)**:** trata-se de uma ferramenta para visualização em tempo real das métricas da rede. Foi criado com ferramentas padrão de web como o *Adobe flash Player*, linguagem XML (*eXtensible Markup Language*) e gráficos em JPEG, possibilitando a portabilidade da plataforma. Ela foi desenvolvida com o objetivo de se tornar uma ferramenta de visualização aplicável a qualquer tipo de rede em mesh. Na Figura 4 está apresentado o diagrama de blocos dos módulos que compõem o aplicativo Meshviz.

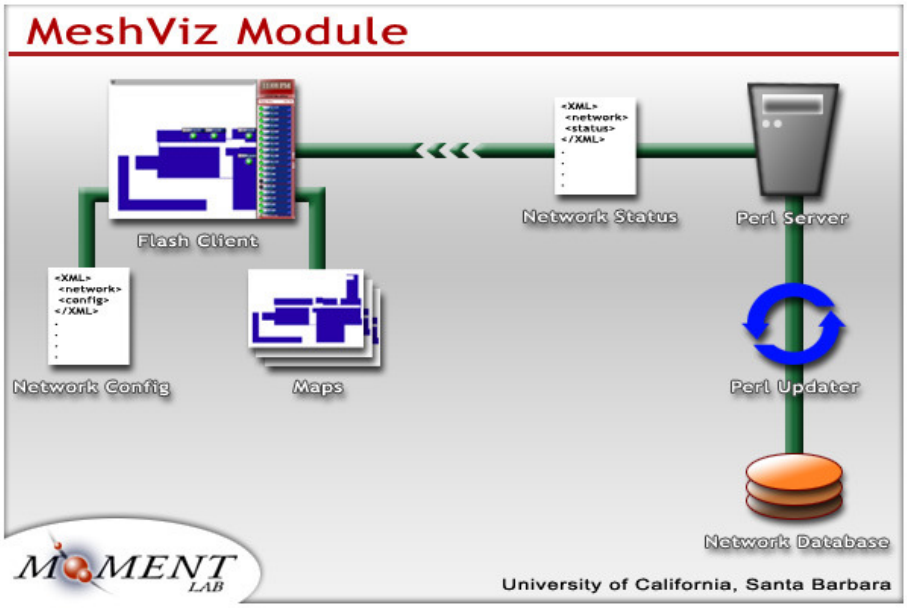


Figura 4: Diagrama do módulo Meshviz do projeto Meshnet

O cliente flash do *Perl Server* (na figura "*Flash Client"*) é um arquivo que deverá residir no servidor web – "MeshViz.swf" (o termo "client" se refere à funcionalidade do módulo dentro da arquitetura geral da aplicação). Este método permite a interação dos usuários, através de interface web, a cada um dos nós da rede. Existe também a possibilidade do usuário baixar o arquivo do servidor e executá-lo localmente. Através de um arquivo XML, o sistema pode ser configurado utilizando o módulo *Network Config*. O módulo permite ao usuário a escolha de qual servidor ele deseja se conectar para a coleta dos dados e de que maneira as informações serão apresentadas na tela. O usuário pode inserir no sistema o mapa da sua própria rede, através do módulo "*Maps*".

O módulo "*Network Status*" armazena a atualização dos dados enviados pelo servidor em um arquivo XML. Este arquivo fornece as informações correntes da rede em que o usuário está conectado. Essa informação é enviada pelo servidor no momento em que o usuário se conecta, podendo ser re-enviado com novas informações a qualquer instante. O primeiro envio de dados contém todas as informações da rede. Os pedidos consecutivos irão enviar apenas informações incrementais, evitando o desgaste de tempo de acesso, já que a quantidade de informações pode ser muito grande.

O servidor *Perl*[3] funciona juntamente com a máquina servidora, esperando conexões de clientes *flash*. Quando uma tentativa de conexão é detectada, o servidor adicionará este cliente em sua lista. De tempos em tempos, o servidor irá atender os clientes da lista ciclicamente, enviando um arquivo XML de status da rede. Desta forma, é possível manter um conjunto de informações consistentes e atualizadas das mudanças que ocorreram. O atualizador *perl* ("*Perl updater*") é a entidade que renova o processo. Ele funciona em um *loop* infinito. Na primeira iteração, o atualizador faz a requisição ao servidor, em seguida, cria um novo arquivo de status e, por fim, volta ao estado de espera por um segundo.

O banco de dados da rede ("*Network Database*") é quem fornece as informações aos clientes flash. O projeto Meshnet utiliza o banco de dados livre *mySQL*.

2.3.5 PROJETOS MESH PROPRIETÁRIOS

Atualmente, cada vez mais projetos comerciais estão surgindo com o objetivo de oferecer redes de acesso mesh com alta qualidade e confiabilidade. Eles diferem entre si em termos dos equipamentos empregados, dos protocolos de roteamento e das ferramentas de gerência e acompanhamento.

Nortel's Wireless Mesh Network (WMESH) (ROCH, 2005)

A solução WMESH da Nortel propõe uma nova arquitetura mesh para prover conectividade em grandes áreas outdoor com enfoque no mercado corporativo. A solução WMESH se apresenta com uma topologia de rede flexível e escalável o suficiente para suportar aplicações governamentais, empresariais e municipais. Ela utiliza o protocolo de roteamento tradicional OSPF (*"Open Shortest Path First"*; TANENBAUM, 2003).

Sua arquitetura é apresentada na Figura 5. Ela é composta por pontos de acesso para a formação de uma rede comunitária (CAN), fornecendo acesso para dispositivos móveis. Os pontos de acesso utilizam dois rádios para a constituição de duas redes distintas: uma interface 802.11a para o *backbone*; ou seja, comunicação entre os pontos de acesso; e outra 802.11b/g, para o provimento de acesso a dispositivos móveis.

[3] Perl é uma linguagem de programação estável e multiplataforma. É bem versátil para manipulação de *strings* e permite tempo de desenvolvimento curto. É amplamente utilizada para criação de aplicações *web* (WIKIPEDIA, 2007)

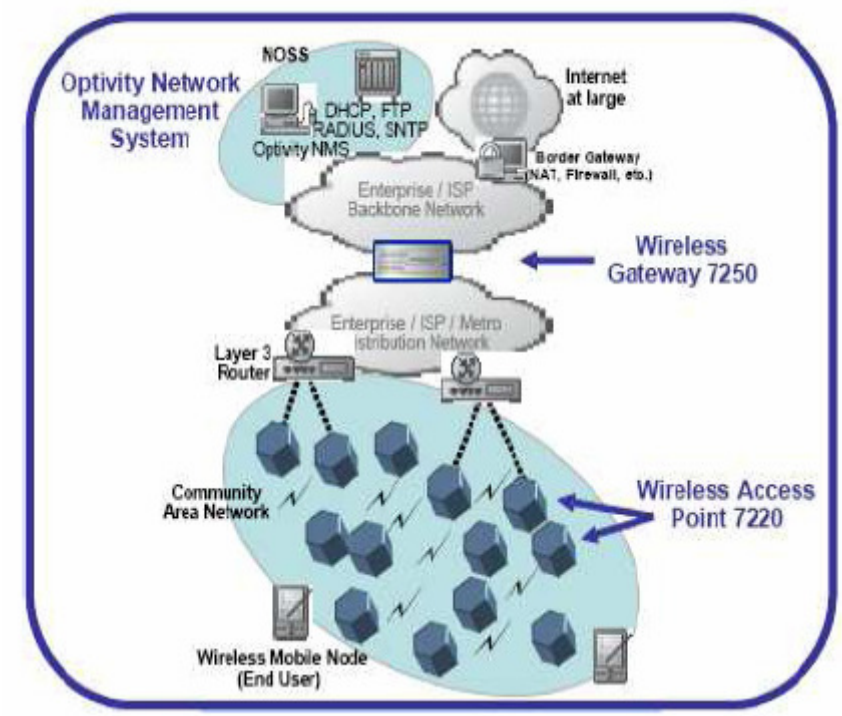


Figura 5: Arquitetura para redes mesh da Nortel (fonte: ROCH, 2005)

As CAN's estão conectadas a roteadores denominados NAP's ("*Network Access Points"*), que dão acesso à rede principal, combinando funções de *switch* e de ponto de acesso (AP) *wi fi*. Os NAP's fazem a conexão entre a rede distribuída e o *backbone* onde estão os *Wireless Gateways* (WG). Os WG's têm a responsabilidade de fazer o roteamento e fornecer a segurança dos dados no enlace principal.

Conectado ao *backbone*, o *Network Operations Support System* (NOSS) fornece facilidades centralizadas de monitoração e gerenciamento das operações da rede. O NOSS opera com um *framework* denominado *Nortel Optivity Network Management System* (ONMS). Ele é responsável pelo gerenciamento de falhas, desempenho e configuração. Além do ONMS, o NOSS também possui servidores de aplicações de redes (FTP, DHCP, SMTP, etc).

O endereçamento dos nós móveis é feito de forma dinâmica. Através da comunicação entre o AP e o WG, os nós recebem um endereço IP fornecido pelo servidor DHCP. A comunicação entre o AP e o WG é feita por IP Móvel (STALLINGS, 2002): o WG faz o papel do *Home Agent* enquanto que o AP é o *Foreign Agent*, criando o túnel entre eles.

Esta solução está sendo utilizada em diferentes cenários. Em Ottawa (Canadá), Taipei (China) e na Filadélfia (EUA). A solução da Nortel foi implantada para fornecer acesso banda

larga para regiões metropolitanas, sendo uma tecnologia concorrente ao WiMax (WIMAXFORUM, 2007). No Arkansas, EUA, a rede Mesh foi instalada em menor escala, em um campus universitário.

CISCO Mesh Network Solution (CISCO WIRELESS MESH, 2006):

A CISCO desenvolveu uma solução para redes mesh que também tem seu foco na implantação de redes *wi fi* em pólos empresariais e regiões metropolitanas. A solução da CISCO utiliza um protocolo de roteamento sem fio próprio e um sistema de gerenciamento baseado em software e hardware dentro de uma arquitetura unificada, apresentada na Figura 6:

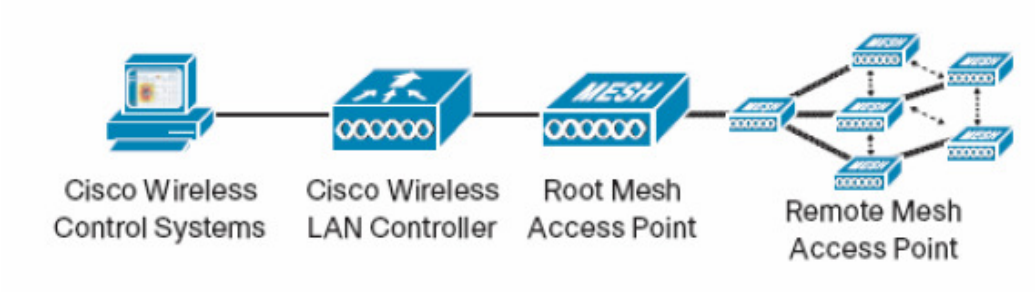


Figura 6: Componentes da solução para redes mesh da CISCO (fonte: CISCO WIRELESS MESH, 2006)

Os "*Cisco Wireless Control Systems"* permitem o gerenciamento da tecnologia para projetar, controlar e monitorar redes sem fio em ambientes abertos, a partir de um ponto centralizado, simplificando as operações e reduzindo o custo de implantação. A solução envolve a utilização do "*Cisco Aironet Series Access Points"*, que permitem aos provedores de serviços disponibilizarem as redes mesh de maneira escalável com fornecimento de segurança.

O "*Cisco Wireless LAN Controller*" faz a ligação entre os pontos de acesso e a parte cabeada da rede, além de centralizar algumas funções do padrão 802.11. O *Controller* provê o gerenciamento da configuração dos dispositivos da rede, das políticas de segurança e das freqüências de rádio através de algoritmos de otimização. Através da tecnologia IEEE 802.11e embutida no *Controller*, é fornecida QoS na camada MAC através de reserva de banda. O "*Root Mesh Access Point"* trabalha como *gateway* de ligação entre os pontos de acesso remotos e a rede. Tipicamente, são instalados no alto de telhados, postes ou prédios e utilizam o padrão IEEE 802.11a para comunicação (*backbone* da rede) . Já os "*Remote Mesh*

Access Points" fornecem acesso para clientes através do padrão IEEE 802.11b/g, porém se conectam ao *Root Mesh Access Point* via 802.11a (semelhante à solução da Nortel). Também possui portas *Ethernet* para conexão de dispositivos periféricos.

Com suporte simultâneo para os padrões IEEE 802.11a e 802.11b/g, o *Wireless Mesh Access Point* utiliza um protocolo de roteamento proprietário chamado *Adaptive Wireless Path Protocol* (AWP) para formar uma rede mesh dinâmica entre os pontos de acesso remotos, fornecendo acesso sem fio com requisitos de segurança para cliente móveis. O protocolo é baseado numa tecnologia de roteamento que responde dinamicamente às variações das condições de uso, propiciando a seleção de rotas ótimas para o caso de falhas nos enlaces ou mudanças no ambiente.

A CISCO espera que em curto prazo, o IETF conclua o processo de padronização de um protocolo para redes mesh, denominado *Lighweight Access Point Control Protocol* (LWAPP). O LWAPP é de autoria da *Airespace* (adquirida, em Março de 2005, pela *CISCO Systems*) e da *NTT DoCoMo* (empresa de telefonia celular japonesa), e pretende padronizar o protocolo de comunicação entre os pontos de acesso e os outros componentes do sistemas (*controllers, switches, routers* etc.).O objetivo desta iniciativa é de prover um mecanismo de encapsulamento e transporte genérico, que garanta a interoperabilidade entre os diversos fornecedores de equipamentos de infra-estrutura para acesso de nível 2, ou, ainda, de nível 3.

Vislumbram-se ainda as seguintes funcionalidades: (a) Reduzir o volume de processamento por um *AP*, permitindo a limitação dos recursos computacionais nestes dispositivos de modo a garantir o foco no acesso sem fio, eliminando as obrigações com respeito à filtragem e policiamento; (b) Viabilizar um esquema centralizado para todos os componentes do sistema do backbone, responsável pelo controle do tráfego de dados, autenticação, criptografia, segurança, *QoS* etc. (c) A especificação do *LWAPP* objetiva identificar estes pontos, através da definição das seguintes atividades principais: descobrimento, troca de informação e configuração dos *AP´s*, certificação e controle do *software* dos *AP´s*, encapsulamento, fragmentação e formatação dos pacotes de dados e· gerência e controle das comunicações entre os *AP´s*. A CISCO implantou um protótipo da sua solução mesh na cidade de Tiradentes (MG) para o fornecimento de acesso à Internet, cabeado e sem fio. Os pontos de acesso foram instalados em postes, cobrindo a região central. Esta iniciativa é decorrente do fato de Tiradentes ser uma cidade histórica, tombada como patrimônio histórico. Devido a isto, não é possível a realização de obras para a implantação de infra-estrutura de acesso tradicionais (passagem de cabeamento ótico subterrâneo, por

exemplo). Este é um exemplo da aplicabilidade das redes mesh fora do contexto da limitação de recursos financeiros.

Já existem diversas outras soluções comerciais de empresas de menor porte disponíveis no mercado mundial.

- *Mobile Mesh* (MOBILE MESH, 2007): utiliza um protocolo de acesso e roteamento proprietário que se divide em três instâncias. Cada uma realiza uma função específica: descoberta de enlaces, roteamento e descoberta de fronteiras. Desenvolvido pela empresa *Mitre*;

- Empresas de pequeno e médio porte como *LocustWorld* (LOCUSTWORLD, 2005) e a *4g MeshCube* (4G-SYSTEMS, 2005) vendem roteadores mesh *off-the-shelf*, similares aos do projeto *Roofnet*, consistindo de caixas com *PC's* pré-configurados com *softwares* específicos e interfaces sem fio.

- ROAMAD (2007) é outra empresa que disponibiliza uma solução completa proprietária para redes mesh.

2.3.6 OUTROS TRABALHOS

ORBIT

O ORBIT ("*Open Access Research Testbed for Next-Generation Wireless Networks*"; RAYCHAUDHURI *et al*, 2005; RAMACHANDRAN *et al,* 2004) é um projeto colaborativo entre diferentes fabricantes e centros tecnológicos tais como Rutgers, Columbia, Princeton, Lucent, Bell Labs, Thompson e IBM. O projeto tem o objetivo de obter resultados experimentais para redes sem fio de grande porte na área de protocolos, aplicações multimídia e de segurança da informação. O ORBIT é composto por dois laboratórios com o objetivo de emular, reproduzir e planejar redes sem fio que permitam a realização de novos experimentos. O laboratório é baseado em um *grid* sem fio de duas dimensões, composto por nós estáticos e móveis, que podem ser interconectados dinamicamente sobre topologias específicas. O laboratório permite realizar experimentos de redes celulares de alta velocidade (3G) e acesso a redes 802.11 em situações de mundo real (emulando condições de propagação). As medidas fornecidas pelos testes realizados permitem avaliar o tráfego das redes e a utilização do espectro de freqüência dos enlaces rádio.

DGP – RuralNet

O projeto DGP RuralNet ("*Digital Gangetic Plains*") pretende explorar o uso do padrão 802.11 como uma tecnologia de acesso de baixo custo e rápida distribuição em áreas rurais. O projeto consiste de uma rede 802.11 com enlaces direcionais em múltiplos saltos em zonas rurais, com pontos de acesso afastados em até 80 km. O propósito principal foi obter resultados de conectividade em ambientes externos de longas distâncias.

O projeto tem como objetivo estudar o aproveitamento de redes mesh em zonas rurais para determinar: metodologias de planejamento e distribuição, desenvolvimento de novos meios de acesso na camada MAC, administração e operação da rede, controle de energia, aplicações e serviços (QIU *et al*, 2006). Enlaces longos para redes mesh são possíveis em áreas rurais por oferecerem menos obstruções e interferências. Normalmente alcançam distâncias na ordem de dezenas de quilômetros. SAYANDEPP e RAMAN (2007) analisam as diferentes condições que estes ambientes configuram.

CUWin

O projeto CUWin ("*Community Wireless"*), localizado em Urbana *Champaign*, tem como principal contribuição um protocolo escalável de roteamento *ad hoc* próprio denominado HSLS ("*Hazy Sighted Link State";* SANTIVANEZ *et al,* 2002; SANTIVANEZ e RAMANATHAN, 2003). É um protocolo pró-ativo, baseado em estados de enlaces (*link-state*) que minimiza o custo, em termos de *overhead,* para a manutenção de uma visão consistente e atualizada da topologia da rede. Tem por objetivo realizar o roteamento eficiente mesmo em redes com um alto número de nós.

O projeto CUWin se associou à empresa GOOGLE (GOOGLE WIFI, 2006) para a implantação de uma rede mesh urbana com alto número de nós. Na página web é disponibilizado o mapa para a visualização da localização dos nós e dos estados dos enlaces.

Outras referências teóricas ainda serão citadas ao longo do trabalho. As referências relativas às questões de planejamento dos enlaces rádio serão apresentadas ao longo do Capítulo 3, quando a metodologia do projeto Remesh (2007) é explicada. O OLSR e a métrica ETX voltarão a ser discutidos em mais detalhes no Capítulo 4. Demais referências sobre programação e ferramentas de código aberto utilizadas pelo projeto Remesh serão citadas no Capítulo 5.

3 O PROJETO REMESH

Inspirado nos testes piloto de redes mesh ao redor do mundo (GRISWOLD *et al*, 2004; BICKET *et al,* 2005; TSARMPOPOULOS, 2005; CAMDEN *et al*, 2004; DRAVES *el al,* 2004 [a]; 2004 [b]) foi criado um Grupo de Trabalho (GT) financiado pela Rende Nacional de Pesquisa e Ensino (RNP) com a proposta de implantar uma experiência semelhante ao projeto VMesh (TSARMPOPOULOS, 2005) na Universidade Federal Fluminense (UFF).

Através de uma parceria entre o Instituto de Computação e o Departamento de Engenharia de Telecomunicações, ambos da UFF, surgiu o projeto denominado REMESH (2007). 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. A UFF possui seus *campi* integrados a diversas comunidades na cidade de Niterói, incluindo os bairros de Icaraí, Boa Viagem, Ingá, Santa Rosa, além do centro de Niterói (Figura 7). A topologia da cidade, a alta densidade populacional e a proximidade dos edifícios residenciais aos diversos *campi* da UFF propiciam um cenário perfeito para implantação de redes de acesso do tipo mesh (Figura 8).

Figura 7: Os diversos *campi* da UFF (áreas marcadas em vermelho) espalhados pela cidade de Niterói

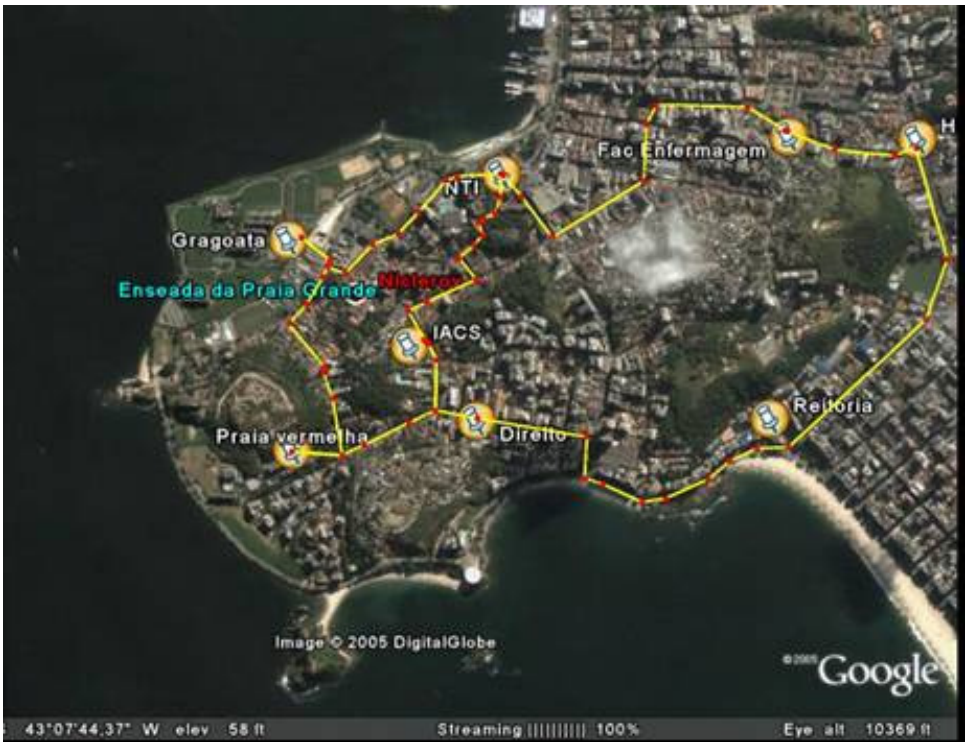


Figura 8: A alta densidade demográfica nas proximidades dos diversos *campi* da UFF (foto do GOOGLE EARTH, 2006).

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 atualmente se encontra em seu segundo ano de realização (2007) com artigos publicados, mini-cursos e palestras em congressos científicos (PASSOS *et al,* 2006; ABELEM *et al,* 2007; MUCHALUAT-SAADE *et al,* 2007; PASSOS e ALBUQUERQUE, 2007).

A seguir serão descritos, em detalhes, os procedimentos para a montagem do protótipo do roteador e da rede. Como assistente técnico, coube ao autor deste trabalho a iniciativa de gerar as soluções para a montagem do protótipo, os procedimentos e a metodologia de instalação e manutenção da rede.

3.1 OBJETIVOS, ESCOPO E METOLOGIA DO PROJETO

O projeto ReMesh teve como objetivo principal demonstrar a viabilidade de uma rede de acesso universitária faixa 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, o *firmware*, os algoritmos de roteamento, as antenas e os aplicativos necessários (incluindo a necessidade de haver um esquema de autenticação e ferramentas de gerência). Nesta fase, os protótipos foram testados nos laboratórios dentro das dependências da própria universidade. A primeira fase também englobou a construção da rede interna, 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 apresentassem as características desejadas (que serão discutidas neste capítulo) e a posterior instalação dos protótipos para a construção da rede externa.

A primeira escolha dentro da construção do protótipo foi o hardware para os nós de acesso e roteamento dentro da rede mesh. Seguindo a metodologia de outros projetos universitários (GRISWOLD *et al*, 2004; BICKET *et al,* 2005; TSARMPOPOULOS, 2005;

CAMDEN *et al*, 2004; DRAVES *el al,* 2004 [a]; 2004 [b]), percebe-se que é desejável para a escolha do nó mesh, um roteador sem fio programável de forma que os algoritmos de roteamento *ad hoc* e os aplicativos possam ser implementados. Tomando como base o projeto VMesh, foi escolhido os roteadores da família WRT54G da Linksys (LINKSYS, 2007), em suas versões 1 até 4, ilustrado na Figura 9, por duas razões básicas: facilidade de se encontrar no mercado brasileiro e compatibilidade com o sistema operacional desejado, o Openwrt (OPENWRT, 2006).

Figura 9: Roteador WRT54G da Linksys

O OpenWrt é uma distribuição de software livre compacta do sistema operacional Linux, criado especialmente para ser instalado em equipamentos com sistemas operacionais embarcados (por exemplo, roteadores, celulares, etc). Ele é flexível o suficiente para o desenvolvimento de aplicativos, protocolos de roteamento e alterações nas configurações do próprio hardware. Além disso, o OpenWrt é compatível com as implementações existentes dos protocolos de roteamento *ad hoc* AODV (PERKINS, 2003) e OLSR (CLAUSEN *et al*, 2003; OLSR, 2006), que foram testados no protótipo. Sua instalação requer cerca de 2MB de armazenamento e pode ser executado em processadores do tipo MIPS (PATTERSON e HENNESSY, 1998) de até 125 MHz e 4 MB de RAM. Ele possui um *framework* para a geração de imagens (igual ao utilizado para compilação de *kernel* no Linux) que pode ser baixado em qualquer *desktop* utilizando sistema operacional Linux. Durante o processo de geração, pode ser escolhido o processador alvo (*mipsel* ou *motorola*[4]), os pacotes que deverão estar presentes e o sistema de arquivos. Todas as ferramentas básicas do sistema operacional (comandos e aplicativos básicos) estão presentes em um grande arquivo binário executável chamado *busybox*. Cada comando é referenciado ao *busybox* por diferentes *links* lógicos[5]. O

[4] O primeiro é o utilizado pelos roteadores da Linksys e o segundo por equipamentos da própria empresa Morotola.

[5] Um link lógico é uma utilidade oferecida por sistemas UNIX e herdada ao sistema Linux. Um link lógico é um nome falso que referencia um arquivo real. O link lógico pode oferecer as mesmas propriedades do arquivo verdadeiro (execução, proteção, etc) dependendo de como foi criado.

restante das ferramentas é disponibilizado como arquivos independentes através de módulos a serem inseridos na memória e arquivos executáveis. Além disso, o OpenWrt possui uma coleção de variáveis de ambiente que acessam diretamente parâmetros do hardware como potência de saída, taxa de interface, ESSID, canal, etc. A efetividade do valor dado à uma determinada variável de ambiente depende da disponibilidade do hardware em permitir ou não a alteração do parâmetro em questão. A lista dessas variáveis e suas ações estão disponíveis em OPENWRT-NVRAM, 2007.

O WRT54G é um roteador sem fio com 4 MB de memória flash (permanente) e 8 MB de memória RAM. Ele possui uma interface sem fio seguindo o padrão IEEE 802.11G e uma interface *Ethernet* dividida em cinco portas distintas através de uma *bridge*[6] lógica. Além disso, ele vem equipado com duas antenas omni-direcionais de 2dB de ganho cada uma para implementar diversidade espacial[7] O roteador vem de fábrica com um sistema operacional da própria Linksys que possui uma interface de administração via web. Contudo, o roteador deve ser adaptado para ser um roteador mesh. Por isto a necessidade de ser compatível com o sistema operacional OpenWRT, tornando possível a substituição do *firmware* original por um sistema aberto. Nas versões mais atuais dos roteadores WRT54G (a partir da versão 5), o sistema operacional passou a ser desenvolvido pela VxWorks (WIND RIVER, 2007). O novo sistema impossibilitava o procedimento de inserção do *firmware* gerado pelo Openwrt. Além disso, eles passaram a ter metade do tamanho disponível tanto para a memória RAM como para a memória flash. Apesar da questão da inserção do firmware do Openwrt ter sido superada com a utilização de um *bootloader* da própria VxWorks (procedimento pode ser visto em FORUM.OPENWRT.ORG, 2007), o problema do tamanho ainda continuou. A solução adotada para esta questão foi a adoção do roteador WRT54GL também da Linksys.(L de Linux). O WRT54GL é equivalente ao WRT54G versão 4 (última versão com o sistema operacional da própria Linksys), porém mais caro.

A escolha do protocolo de roteamento foi uma questão importante na fase inicial do projeto. Como foi visto no Capítulo 2, redes do tipo mesh são redes comunitárias construídas com base em algoritmos de roteamento cooperativos, do tipo encontrado em redes sem fio e

[6] Uma bridge é uma ponte onde uma mesma interface Ethernet pode apresentar portas diferentes com endereços MAC distintos, fazendo com que elas possam ser acessadas independentemente.

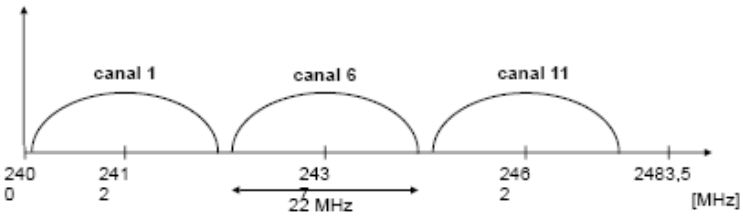
[7] Diversidade espacial é uma técnica utilizada na recepção de uma transmissão rádio para o aproveitamento dos raios provenientes de múltiplos percursos (RAPAPPORT, 1996). Utilizam-se duas ou mais antenas para a eleição do melhor sinal recebido. Se houverem demoduladores independentes para cada antena, os diferentes sinais dos múltiplos percursos podem ser combinados, gerando uma componente de maior potência (DIGAVVI *et al*, 2004).

sem infra-estrutura (redes *ad hoc*). Nessas redes, os algoritmos ou protocolos de roteamento podem ser divididos em duas categorias básicas: pró-ativos e reativos. A principal vantagem dos algoritmos pró-ativos é que todos os nós da rede têm sempre uma visão de qual é a topologia da rede em cada momento. Isso implica em rápido estabelecimento de rotas. Contudo, essa visão atualizada da topologia da rede implica que cada nó possua uma tabela que armazene todos os caminhos. Se a mobilidade dos nós for intensa, a troca de mensagens de controle entre eles será igualmente intensa. Em redes *ad hoc* tradicionais, os dispositivos possuem recursos limitados e são alimentados por bateria. A intensa troca de mensagens irá implicar em maior gasto energético. Já os algoritmos reativos, que estabelecem rotas por demanda, diminuindo o número de mensagens de controle, têm como principal desvantagem o atraso adicional para o estabelecimento da rota. Foram testados inicialmente os protocolos que já tinham versões disponíveis para o OpenWRT , o AODV, um protocolo reativo, e o OLSR, um pró-ativo. Devido às características inerentes à arquitetura do projeto (pouca mobilidade dos nós roteadores e sem restrições de energia), o OLSR foi o escolhido. Entretanto, por não ser um protocolo específico para redes do tipo mesh, o OLSR da forma como é apresentado na sua RFC (*Request For Comments;* CLAUSEN *et al,* 2003) não se apresentou como o mais adequado. O desenvolvimento de um protocolo mais próximo às características de rede do projeto foi uma questão de extrema importância e será detalhado no capítulo 4 do presente trabalho.

Uma questão que deve ser considerada é a escolha da taxa de operação da interface sem fio. O padrão IEEE 802.11g especifica como opcional ao fabricante, as taxas de dados que a interface poderá operar. A taxa máxima para interfaces que implementam o padrão é de 54 Mbps. Entretanto, para garantir interoperabilidade entre equipamentos de versões anteriores (802.11b e 802.11), torna-se necessário que a taxa seja ajustada de acordo com a capacidade dos participantes da rede sem fio. Particularmente, os roteadores da família WRT54G oferecem a opção da escolha do modo de operação. O sistema operacional OpenWRT pode acessar esse parâmetro do hardware através de uma variável de ambiente (*wl0_rate*). São disponibilizados pelo sistema diferentes valores de taxa de operação: 1, 2, 11, 22, 54 Mbps e modo automático. No modo automático a taxa da interface é negociada entre o transmissor e o receptor na taxa básica de 1Mbps antes de cada transmissão (STALLINGS, 2002).

Continuando, uma outra questão inerente à metodologia do projeto era o planejamento dos enlaces. Duas redes foram propostas, a rede interna e a rede externa. A primeira tinha o

propósito de desenvolvimento e aprimoramento do protótipo e das ferramentas necessárias para o seu funcionamento. A segunda (externa) tinha o propósito de validação e de realização de testes em condições mais realísticas de utilização. Para ambas as redes, o primeiro passo era a descoberta do melhor canal de utilização. O padrão 802.11 atua 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; como demonstrado na Figura 10. Através da ferramenta *iwlist,* disponível nos sistema Linux e também no OpenWrt (TOURRILHES, 2007), o ambiente escolhido era verificado e o canal menos utilizado era escolhido. Depois do primeiro nó instalado, a utilização de ferramentas que possibilitassem a inspeção das possíveis novas localizações era necessária. Neste caso foi escolhido o *Netstumbler* (NETSTUMBLER, 2007; ilustrado na Figura 11) executado em laptops. Trata-se de um aplicativo gratuito que inspeciona todas as redes operando na faixa de 2.4 GHz dentro do alcance da interface sem fio da máquina que o executa.



ID do canal	Freq. Central
1	2412 MHz
2	2417 MHz
3	2422 MHz
4	2427 MHz
5	2432 MHz
6	2437 MHz
7	2442 MHz
8	2447 MHz
9	2452 MHz
10	2457 MHz
11	2462 MHz

Figura 10: Espectro ocupado na faixa de 2.4 GHz definido pelo padrão IEEE 802.11

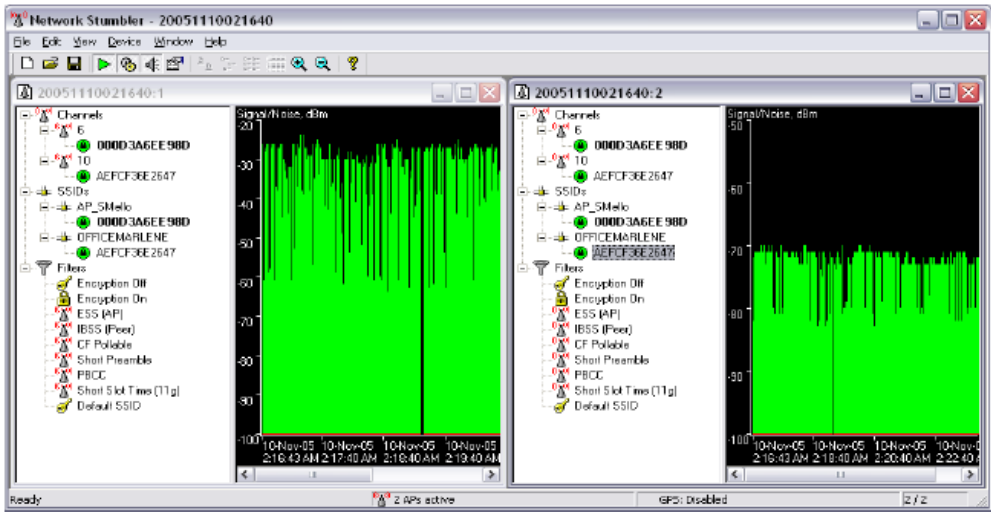


Figura 11: Ilustração da ferramenta *Netstumbler*

Quanto aos enlaces externos, em uma rede mesh é desejável que todos os nós participantes do roteamento possam transmitir e receber sinais provenientes de todas as direções. Para tanto, a escolha de antenas omni-direcionais para os nós externos era a melhor opção. A utilização de antenas omni-direcionais foi a escolha do projeto VMesh e também a do projeto Remesh, inicialmente. A grande vantagem da utilização de antenas omni-direcionais é o crescimento incremental que a rede irá dispor. Não limitando a cobertura do sinal irradiado, é possível instalar novos nós mesh em qualquer direção, desde que estejam em linha de visada. Para facilitar o projeto, os enlaces foram escolhidos de forma a sempre haver linha de visada entre os nós. Entretanto, a escolha dos nós era limitada pela presença de prédios com voluntários disponíveis e pela ausência de obstruções destrutivas dentro da região descrita pelo elipsóide de Fresnel (BOITHIAS, 1987; LAVERGNAT e SYLVAIN, 2000). De maneira simplificada, a equação utilizada para obtenção do raio da circunferência (em metros) descrita pela secção transversal do elipsóide de Fresnel na metade do percurso está descrita na Figura 12, junto com os parâmetros pertinentes. Na equação, f é a freqüência de operação em GHz e d é a distância (em km) entre os pontos. As distâncias eram inferidas com o auxílio do GOOGLE MAPS (2007). Geralmente, as transmissões nesta faixa começam a serem prejudicadas por obstáculos que ocupem 20% ou mais da zona de Fresnel (TERABEAM, 2006).

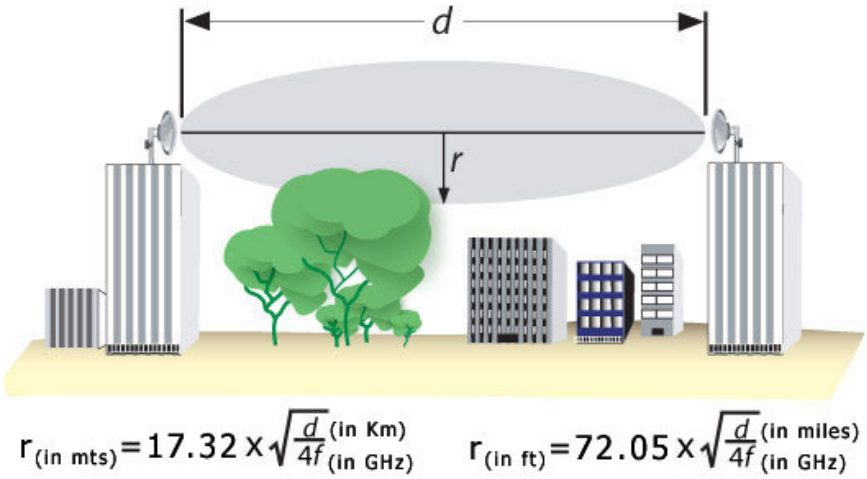


Figura 12: Zona de Fresnel (fonte: TERABEAM, 2006)

A aplicação da fórmula nos dá uma razão da distância com a altura dos nós: $r(m) = 5,59\sqrt{d(km)}$. Por exemplo, um enlace de 300 metros implica em um raio da zona de Fresnel de aproximadamente 3 metros e 2,45 metros de raio efetivo (o que equivale a 80% do comprimento total do raio, percentual que define o segmento mais importante em relação à taxa de perda de pacotes - TERABEAM, 2006). Isto implica na ausência de outros prédios com a mesma altura no percurso do enlace. Além disso, quanto menor for a altura dos prédios, menor deverá ser a distância. Este exemplo demonstra a dificuldade de se fazer um enlace longo sem obstruções na faixa de 2,4 GHz em uma área urbana, mesmo considerando apenas as obstruções diretas aos raios. A determinação do Elipsóide de Fresnel é apenas um requisito para o planejamento do enlace. As perdas de propagação ao longo do percurso devem ser estimadas para validar a viabilidade da distância planejada.

Existem modelos determinísticos e empíricos para o planejamento da perda de propagação de sistemas rádio operando na faixa de 2.4 GHz. Os modelos determinísticos são baseados na teoria de traçado de raios (RAPAPPORT, 1996) e são geralmente são insuficientes para a completa caracterização das diferentes situações de construção dos enlaces. Os modelos empíricos são baseados em campanhas de medidas e têm a finalidade de complementar os modelos determinísticos inserindo nas equações as perdas no sinal devido à propagação em ambientes com características definidas (descrição dos obstáculos, localização, alturas e materiais). Contudo, é muito difícil modelar as características externas, como por exemplo, definir o material da parede de um prédio ou de um poste (JADHAV *et al*, 2005; KIM e BOHACEK, 2005; SRIDHARA e BOHACEK, 2007). Dentre os modelos

empíricos disponíveis, destacamos os seguintes: Modelo Log-distance, Modelo ITU P. 1238-1, Modelo COST 231 Keenan e Motley e Modelo COST 231 Multi-wall.

Atualmente, dentre os modelos destacados, o mais completo para predição de sinais em ambientes interiores e exteriores na faixa de 2,4 GHz, em razão do número de parâmetros considerados, é o COST 231 Keenan e Motley ou COST 231 *Multi-Wall*:

$$L_{total} = L_0(d_0) + 10 \times n \times \log\left(\frac{d}{d_0}\right) + \sum_{i=1}^{I} k_{f,i} \times L_{f,i} + \sum_{j=1}^{J} k_{w,i} \times L_{w,i}$$

Onde:

L_0 – Perda de propagação a um metro da antena irradiante [dB] (para micro-células, d_0 = 1m). Alguns valores típicos estão na Tabela 1;

d – Distância ao transmissor [m];

n – Coeficiente de propagação (depende das características do ambiente, LU e RUTLEDGE, 2003);

$L_{f,i}$ – Perda de propagação do sinal através do piso i [dB];

$k_{f,i}$ – Número de pisos com a mesma característica;

$L_{w,i}$ – Perda de propagação do sinal através da parede j [dB];

$k_{w,i}$ – Número de paredes com a mesma característica;

I – Número de pisos atravessados pelo sinal;

J – Número de paredes atravessadas pelo sinal.

Obstáculo	Perda [dB]
Espaço livre	0
Janela (tinta não metálica)	3
Janela (tinta metálica)	5 a 8
Parede fina (madeira)	5 a 8
Parede média (madeira)	10
Parede espessa (aprox. 15 cm)	15 a 20
Parede muito espessa (aprox. 30 cm)	20 a 25
Piso/Teto espesso	15 a 20
Piso/Teto muito espesso	20 a 25

Tabela 1: Valores típicos de perda de propagação (COST 231, 1999)

A formula de COST 231 assume, através de diversas medições realizadas em campo, que a perda de propagação segue uma distribuição *log-normal* (LEON-GARCIA, 1994). O valor L_{total} é a mediana da distribuição. Segundo o modelo, a perda poderia ser calculada em qualquer ponto do percurso ($L_{total}(d)$) como uma função da mediana L_{total} mais uma variável aleatória gaussiana de média 0 e desvio padrão igual a 1 (RAPAPPORT, 1996). Para o cálculo de enlaces, o valor da perda média de percurso é suficiente, pois define o raio máximo da área de cobertura onde pelo menos 50% da energia do sinal estará presente.

O parâmetro L_0 está relacionado às perdas de espaço livre nas proximidades da antena. Ele incorpora na fórmula os parâmetros dos efeitos de borda da propagação (BALANIS, 2005). Para micro-células (células de raio de até 500m de comprimento, aproximadamente), as distâncias utilizadas são da ordem de 1 metro (COST 231, 1999). No caso de células maiores (raio entre 1 a 5 km), L_0 é calculado para distâncias da ordem de 1 km (SKLAR, 1997). No projeto, L_0 foi utilizado segundo modelos propostos em COST 231 (1999), com o valor de 45 dB.

A constante de propagação n está relacionada especificamente com o ambiente de propagação (LU e RUTLEDGE, 2003). Também é um valor empírico. A Tabela 2 apresenta alguns valores típicos de n:

Ambiente	Constante de propagação n
Espaço livre	2
Área urbana para cobertura rádio celular	2,7 a 3,5
Área urbana com sombreamentos para cobertura rádio celular	3 a 5
Construções compactas (prédios), em linha de visada	1,6 até 1,8
Construções compactas (prédios) sem linha de visada	4 a 6
Construções amplas (fábricas, universidades)	2 a 3

Tabela 2: Valores de n para diferentes tipos de ambientes (fonte: BARSOCCHI, 2006)

Uma análise mais completa sobre os mecanismos de propagação para sistemas de comunicação sem fio de micro-ondas pode ser encontrada em BARSOCCHI (2006) e DE LA ROCHE *et al* (2007). A descrição dos demais modelos foge ao escopo do presente trabalho e não foram considerados no planejamento das redes do projeto Remesh (tanto a rede interna como a externa).

Para cada uma das redes desenvolvidas pelo projeto houve um planejamento distinto para a montagem dos enlaces. Os nós na rede interna estão separados por distâncias mais curtas, não estão em linha de visada e possuem em seu percurso obstáculos conhecidos, como paredes, pisos e redes interferentes, bem como parâmetros desconhecidos, como presença aleatória de pessoas, o funcionamento do elevador, geradores de energia próximos aos locais de instalação de alguns roteadores e redes interferentes esporádicas.

Na rede externa, os nós estão separados por distâncias maiores e possuem visada direta para pelo menos um nó vizinho, entretanto, o número de obstáculos presentes na zona de Fresnel é bem maior e não é possível determinar com precisão o material que os compõem. Isto significa diretamente no aumento da interferência causada pelos múltiplos percursos do sinal (desvanecimento rápido) e na perda de potência ocasionada pelos efeitos da difração. Além disto, o ambiente externo está sujeito ao desvanecimento de propagação causado pela chuva, fenômeno que não ocorre no ambiente interno. Obstáculos aleatórios como a presença de pessoas e, neste caso de carros também, são mais freqüentes, bem como um número muito

maior de redes externas, esporádicas ou não, atuando na mesma freqüência. Ainda, existe também a perda de propagação causada pela refração, resultado das diferentes camadas que se formam na atmosfera devido às variações de umidade e temperatura. Para mitigar esses fenômenos de propagação, o projeto optou pela utilização de antenas de alto ganho direcionais e omni-direcionais, acopladas aos roteadores através de guias de onda (cabos) de baixa perda. Neste capítulo, as questões inerentes aos enlaces externos voltarão a ser tratadas quando a rede externa for detalhada.

No restante do capítulo será detalhado o processo de construção do protótipo, em seguida o esquema de endereçamento adotado, a descrição da rede interna e sua topologia. Por fim, será descrita a rede externa, onde serão apresentados mais detalhes sobre a construção dos enlaces externos, bem como os problemas e as soluções encontradas.

3.2 MONTAGEM DO PROTÓTIPO

A primeira etapa é a aquisição do sistema operacional OpenWrt em um desktop com sistema operacional Linux. Após executado, uma tela para a escolha dos pacotes desejados. Uma vez decidido quais serão os componentes do sistema operacional, basta escolher o sistema de arquivos para a geração da imagem. Atualmente são gerados dois tipos: *jffs ("Journaling Flash File System*") e *squashfs ("Squash File System").* A diferença prática entre os dois é o desempenho e o tamanho ocupado. O *jffs* ocupa mais espaço, porém é mais rápido e foi o escolhido para a geração da imagem utilizada no protótipo. O *squashfs* é mais compacto e mais lento. A inserção da imagem no roteador é simples e pode ser feita através da interface web original do roteador na seção "*Upgrade Firmware*". Após a inserção do sistema Openwrt, o roteador continuará respondendo pelo mesmo endereço IP original proveniente do fabricante e também terá uma interface web de gerência do novo *firmware*. Existe uma alternativa para a inserção da imagem utilizando o aplicativo *tftp*[8]. O procedimento passo a passo é descrito no site do OpenWrt e também pode ser obtido no site do projeto (PROJETO REMESH, 2007).

Além do sistema operacional, o protótipo utiliza ferramentas adicionais como a nossa versão do protocolo OLSR (Capítulo 4) e o módulo binário do agente de autenticação *wifidog* (Capítulo 5). Aplicativos diversos desenvolvidos para sistemas Linux para desktops podem

[8] TFTP – Trivial File Transfer Protocol. É baseado no protocolo FTP (File Transfer Protocol; TANENBAUM, 2003) porém realiza apenas a trasferência direta do arquivo desejado (não tem interface para controle).

ser executados dentro do roteador, entretanto eles devem ser gerados utilizando o compilador e o *linker*[9] (SILBERSCHATZ *et al,* 2002) do OpenWRT, presentes no pacote de sua distribuição. Entretanto, este trabalho está se tornando cada vez mais desnecessário à medida que novos pacotes estão sendo incorporados diretamente no OpenWrt.

Para a montagem do protótipo para ser instalado em ambientes externos, são utilizados os seguintes componentes:

- Caixa hermética plástica (Figura 13)
- Base de ferro galvanizado (Figura 14)
- Haste de ferro galvanizado de 2 metros (Figura 14)
- Suporte metálico para encaixe da caixa na haste (Figura 14)
- Antena omni-direcional de 18,5 dbi de ganho ou alternativamente antena direcional de 24 dbi de ganho, dependendo do enlace (Figura 15)
- Cabo RGC 213 de 1m (Figura 16)
- Conectores RP-TNC (*Reverse Polarity - Threaded Neill-Concelman*) para ligação do cabo com a saída de RF do roteador (Figura 16)
- Conectores N-Macho para ligação do cabo com a antena omni-direcional e N-Fêmea para ligação com a antena direcional (Figura 16)
- Módulo POE (fora do padrão) desenvolvido pelo próprio projeto (Figura 17), cuja montagem é detalhada na próxima seção.
- Cabo de rede (CAT5), de preferência com capa protetora, para ligação do roteador aos usuários.

[9] Um *linker* atua junto ao compilador para a geração do arquivo executável. Ele apenas grava quais bibliotecas são necessárias para o executável e seus nomes ou números em um índice.

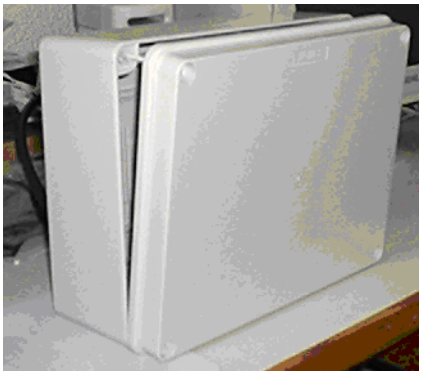


Figura 13: Caixa hermética para proteção do roteador

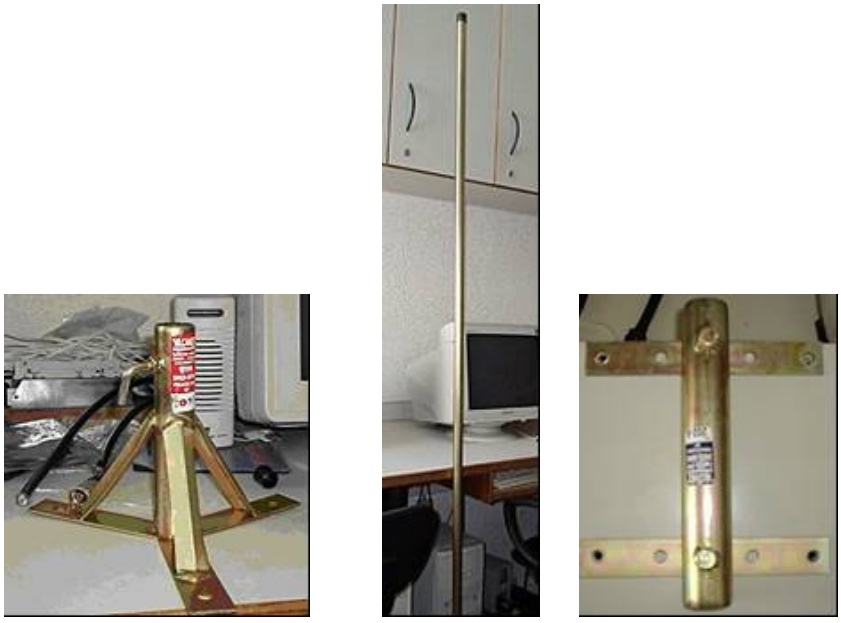


Figura 14: Da esquerda para a direita: base para a haste da antena, haste de 2 metros para suporte da antena e do roteador e suporte metálico para prender a caixa ao suporte

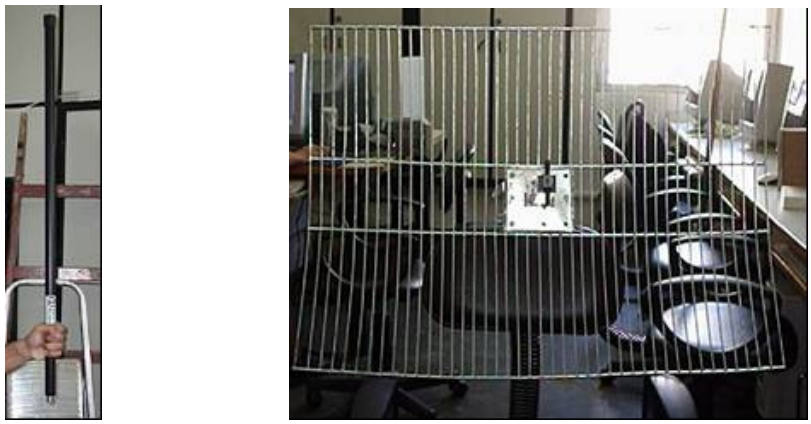


Figura 15: Antenas omni-direcional e puramente direcional


Figura 16: Da esquerda para a direita: cabo RGC 213 e conectores RP-TNC e N-Macho

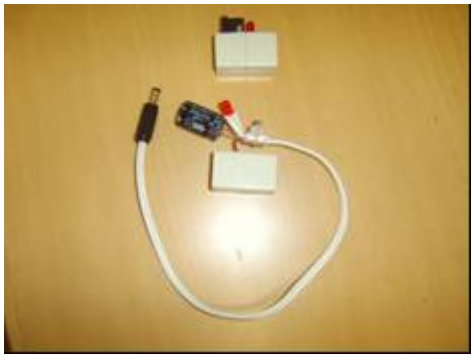


Figura 17: Módulo POE

Finalmente, o protótipo completo para ambientes externos pode ser visto na Figura 18.

Figura 18: Protótipo completo para ambientes externos

Além do roteador e das peças de montagem para o ambiente externo, é necessária uma máquina para fazer o serviço de autenticação e coleta de estatísticas de acesso (servidor de

autenticação instalado com uma instância do *wifidog*). A mesma máquina também é encarregada de ser servidor web, onde são executadas ferramentas de gerência dos nós e de acompanhamento dos enlaces.

3.2.1 Suprimento de Energia

O suprimento de energia elétrica foi outra solução de baixo custo desenvolvida pelo projeto, em particular pelo professor SCHARA[10]. Segundo LINKSYS WRT54G POWER SUPPLY (2007), o WRT54G possui um conversor DC/DC que converte 12V para 3.3V necessário para o roteador. O conversor funciona com uma voltagem de entrada de 4.75 a 40.0V, saindo 3.3V e 3A de corrente. Isso significa que o limite inferior de voltagem fornecida é de 5V mas o limite superior é menos de 40V, não sendo recomendado usar mais de 20V por causa do capacitor de entrada que possui um valor nominal de voltagem de 25V. A conversão é realizada através de um chip regulador de tensão, AC1501-03 (ANACHIP CORP, 2007), localizado conforme ilustrado na Figura 19.

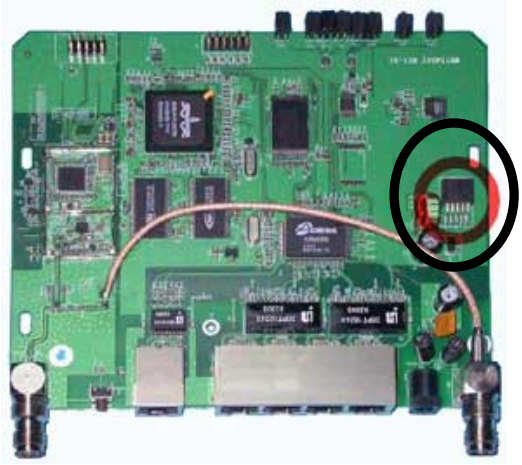


Figura 19: Chip AC1501-3 (marcado pelas circunferências) presente no roteador WRT54G da Linksys que permite o seu funcionamento com diferentes valores de tensão de entrada

A Tabela 3 é o resultado de testes no aparelho usando uma fonte variável:

[10] Magalhães, Luiz Cláudio SCHARA. Engenheiro de Sistemas pela Pontifícia Universidade Católica do Rio de Janeiro e PhD em Ciência da Computação pela universidade de Illinois (Urbana Champaign, UIUC). Atualmente é professor titular da UFF, é o orientador do presente trabalho e um dos coordenadores do projeto Remesh. Página pessoal: http://www.midiacom.uff.br/~schara.

Voltagem na Entrada (Volts)	Corrente na Entrada (Amperes)	Potência fornecida (Watts)
6.0	0.932	5.592
6.5	0.851	5.5315
7.0	0.784	5.488
7.5	0.727	5.4525
8.0	0.677	5.416
8.5	0.635	5.3975
9.0	0.598	5.382
9.5	0.565	5.3675
10.0	0.535	5.35
10.5	0.509	5.3445
11.0	0.485	5.335
11.5	0.465	5.3475
12.0	0.445	5.34
12.5	0.426	5.325
13.0	0.410	5.33
13.5	0.395	5.3325
14.0	0.381	5.334
14.5	0.368	5.336
15.0	0.356	5.34

Tabela 3: Diferentes valores de potência na entrada do roteador WRT54G (fonte: LINKSYS WRT54G POWER SUPPLY, 2007)

Em vista disto, percebe-se que não há necessidade de um kit de *Power over Ethernet* padrão (capaz de fornecer alimentação adicional). Se for utilizado 100m de cabo *Ethernet* (CAT5) indo para o roteador com uma voltagem de entrada de 12V, há uma perda de 5V, sobrando 7V que são suficientes para o roteador trabalhar.

O módulo de POE (*Power Over Ethernet)* utilizado no projeto não é padrão, pois não há injetores de tensão para medir o comportamento do equipamento remoto e desligar a tensão se o equipamento não for capaz de receber alimentação via POE. O módulo desenvolvido simplesmente usa os fios "ociosos" do padrão *Ethernet* (4,5,7 e 8, conforme a Figura 20) para levar tensão DC da casa do usuário até o equipamento localizado no topo do prédio. Além de ser uma solução barata, diminui o trabalho adicional da passagem de um cabo somente para energia e dos transtornos que poderiam ser ocasionados se a alimentação fosse suprida pelas dependências do prédio, onerando os condôminos.

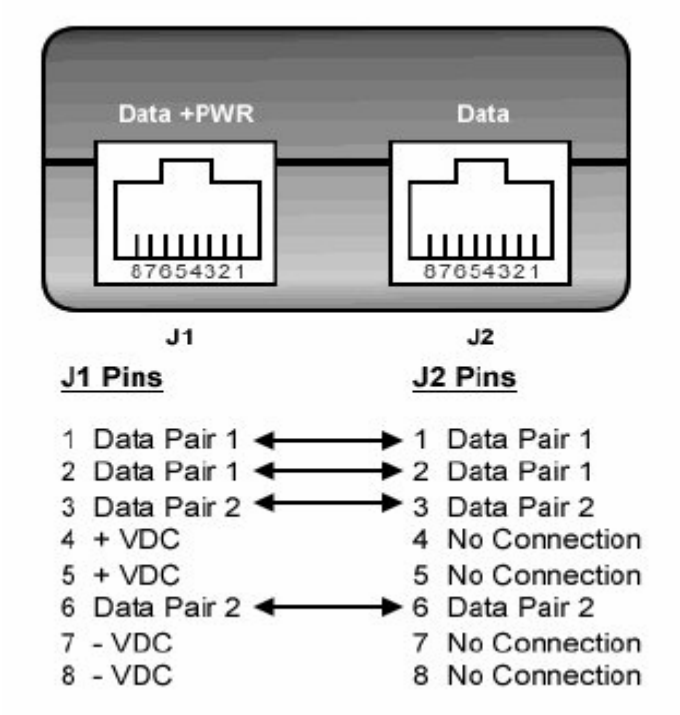


Figura 20: Conector RJ45. O POE utiliza os fios 4 e 5 para um malha do fio de energia e os fios 7 e 8 para a outra

O POE para ser montado utiliza dois extensores RJ45 e conectores de energia macho (plug tipo P4) e fêmea (jack tipo P4), conforme o padrão utilizado pelo WRT54G[11]. Cada extensor RJ45 recebe um dos conectores de energia. Abrindo-se o extensor em duas partes, podem-se separar os fios ociosos que serão utilizados, cortando-os. Apenas uma metade dos fios cortados será utilizada, a outra metade restante dos fios não é utilizada e deve ser isolada. Juntando os fios dois a dois, forma-se em cada extensor um único par, permitindo uma maior condutância. Fazendo-se um pequeno furo no extensor, pode-se fixar o seu respectivo conector. O extensor que recebe o conector fêmea fica localizado na casa do usuário e será ligado diretamente na fonte de energia. Das duas partes que formam o extensor, a que recebe o conector será a parte que levará a energia até o topo do prédio através do cabo CAT5. A outra metade simplesmente liga mais um cabo CAT5 à máquina do usuário. O outro extensor será análogo. A primeira metade é responsável por receber a energia. Com o auxílio de mais um par de fios (pode-se usar o mesmo fio do CAT5 de aproximadamente 10cm), solda-se os fios do extensor que trazem a energia. Na outra extremidade do fio adicional, solda-se o conector macho que será ligado no roteador. A outra metade do extensor fica com quatro fios cortados que não são utilizados e também devem ser isolados. Nesta metade (a que não traz

energia da casa do usuário) outro segmento de cabo CAT5 deverá ser ligado para fazer a conexão com a porta do roteador e pode ser bem curto (20 cm aproximadamente). Os dois extensores estão ilustrados na Figura 17. No POE da figura ainda foi adicionado um capacitor eletrolítico de voltagem apropriada (por exemplo, 470KμF 16V, para fontes de 12V) para diminuir a indutância e dois led's para indicar a atividade. Esses dois itens são extras e o módulo pode funcionar sem eles, conforme foi descrito acima.

3.2.2 Esquema de endereçamento

Para conexão da rede *mesh* à Internet, é necessária a escolha de um nó para ser o *gateway* da rede. O nó *gateway* é ligado na mesma rede onde está o servidor web e de autenticação. Obviamente, os nós que são instalados nos prédios dos usuários são os que não precisam estar ligados por cabo à rede que fornece acesso à Internet. Todo o tráfego para a Internet é "escoado" até o gateway, passando pelos múltiplos saltos dos diferentes percursos possíveis.

Os roteadores possuem duas interfaces, a Ethernet e a sem fio (802.11g). A rede utiliza um esquema de endereçamento que basicamente divide a rede em duas: a rede cabeada (fornecida pela interface "LAN") e a rede sem fio. Cada roteador define duas sub-redes próprias: uma para os usuários com fio e outra para os clientes sem fio.

A interface sem fio é definida pelo ESSID e pelo canal, operando no modo *ad hoc*. No caso do *gateway*, existe ainda uma outra interface de rede lógica Ethernet para a interligação com a Internet (identificada como interface WAN). Os usuários, cabeados ou sem fio, recebem a configuração de rede por servidores DHCP (*Dynamic Host Configuration Protocol*; PETERSON e DAVIE, 1999) operando em cada um dos roteadores.

Mesmo operando no modo *ad hoc*, a configuração das máscaras dos endereços juntamente com o protocolo de roteamento possibilitam aos usuários sem fio que se conectem aos roteadores da mesma forma que se conectariam em uma rede operando no modo estruturado (modo "*Managed*"; STALLINGS, 2002). Isto é feito através da utilização de máscaras diferentes para as interfaces sem fio do roteador e do usuário, aliado à disseminação da informação das topologias realizada pelo protocolo OLSR. Esta informação é especificada no campo HNA (*Host and Network Association*) do cabeçalho do pacote de anunciação do OLSR (pacote "*HELLO"*).

---

[11] Aqui, torna-se necessário fazer uma ressalva. Os conectores de energia (plug e jack P4) seguem o padrão do roteador WRT54G da Linksys que é vendido no Brasil e nos EUA, podendo ser diferente nas versões vendidas em outros países.

. A adoção de máscaras diferentes é necessária porque se a máscara dos usuários não for igual ou maior do que “255.255.255.224” (redes que permitem no máximo 32 endereços válidos ou, em outras palavras, 30 máquinas), o protocolo de roteamento não exportará para os demais nós da rede sem fio a informação sobre quem são *gateways* de cada sub-rede. Cada nó é, portanto, responsável por duas sub-redes: a cabeada e a sem fio.

Se as máscaras forem iguais às dos roteadores (“255.255.0.0”), mesmo que o usuário envie pedidos à rede através do roteador local que está agindo como *gateway* para ele, os pacotes não voltariam necessariamente pela mesma rota, pois o usuário não está executando nenhum tipo de protocolo de roteamento *ad hoc*. Se o protocolo de roteamento não informar aos demais nós da rede que uma determinada sub-rede (sem fio) só poderá ser alcançada através do nó que a anunciou, os pacotes não terão como ser roteados de fora para dentro da rede mesh. Experimentos comprovaram que esta anunciação só é realizada para máscaras com o 4° byte do endereço IP igual ou maior do que 224, por exemplo, 240, 248 ou 253. Isto é um fato particular à implementação do OLSR e ao modelo de endereçamento adotado pelo projeto.

Por outro lado, se os roteadores não utilizarem máscaras do tipo “255.255.0.0”, eles não poderão se comunicar entre si, pois eles são identificados exatamente pelo terceiro byte do endereço IP. Em vista disto, foi adotada uma nomenclatura específica para a geração dos endereços. Cada roteador é chamado por um número inteiro na faixa de 0 até 253 (“*ID*” do roteador). A interface sem fio recebe os parâmetros de configuração através de valores especificados em variáveis de ambiente (*nvram*). Estes valores são configurados automaticamente através da execução de script (“*Configure_manet*”, ANEXO 1) com o “*ID”* do roteador. O script fornece também o endereço das interfaces sem fio e da interface Ethernet LAN (NESARGI e PRAKASH, 2002). No caso do *gateway* para a Internet, um endereço para a interface Ethernet WAN também é fornecido.

O endereço da interface sem fio do nó é dado pelo esquema: 10.151.*ID+1*.1 com máscara 255.255.0.0. Por exemplo, o nó de “ID” 0 terá o endereço 10.151.1.1. A interface LAN terá o endereço dado o seguinte esquema:

10.152.Y.Z onde

Y ={(*ID**32)}mod(256)

Z = {(*ID**32)mod (256)} + 2, com máscara 255.255.255.224

O termo *mod* se refere à operação matemática “módulo”.

Esses serão os endereços entregues às interfaces LAN dos roteadores. Os usuários serão identificados pela interface à qual eles pedem acesso ao servidor DHCP de cada roteador. Os usuários sem fio receberão endereços dentro do seguinte escopo:

Início → 10.151.*ID*+1.2

Final da faixa→ 10.151.*ID* +1.28

Máscara → 255.255.255.224

E os usuários com fio (acesso pela interface LAN) receberão:

Início →10.152.Y.Z , onde

Y = {(*ID**32) mod 65536} mod 256

Z = {(*ID**32) mod 256} + 2

Final da faixa → 10.152.Y.Z , onde

Y = {(*ID**32) mod 65536} div 256

Z = {(*ID**32) mod 256}+30

Máscara → 255.255.255.224

Onde "*div"* é o resultado da divisão inteira.

As faixas das sub-redes entregues pelos roteadores também terão que ser exportadas pelo protocolo de roteamento exigindo, portanto, que elas sejam especificadas na sua configuração (o ANEXO 2 contém, a título de exemplificação, o arquivo utilizado pelo projeto para configurar o OLSR). Este esquema de endereçamento é baseado pelo proposto por TSARMPOPOULOS *et al* (2005). MIHSIN e PRAKASH (2002) analisam métodos de endereçamentos funcionais em redes *ad hoc* com alto número de nós.

Entretanto, ao longo do projeto, os roteadores passaram a ser identificados diretamente pelo terceiro byte do endereço IP (*ID + 1*), pela facilidade cognitiva na associação do roteador ao seu endereço.

3.3 REDE INTERNA

A rede interna está localizada dentro das dependências do campus da Praia Vermelha da UFF (campus dos cursos de Engenharia e Ciência da Computação) constituída por sete nós

mesh (até o fim do ano de 2006) com suas antenas originais. A rede interna é muito útil para desenvolvimento e realizações de testes em um ambiente protegido e de fácil acesso.

A rede interna foi instalada segundo a viabilidade de localização em termos de segurança, energia e qualidade dos enlaces. Procurou-se montar uma topologia com enlaces adjacentes de alta qualidade e pouca interferência de sinais provenientes de outros nós. Devido a isto, na maior parte do tempo os nós se comunicam pelas rotas esperadas, demonstradas na Figura 21. A rede interna consiste em um total de 7 roteadores, incluindo o *gateway*.

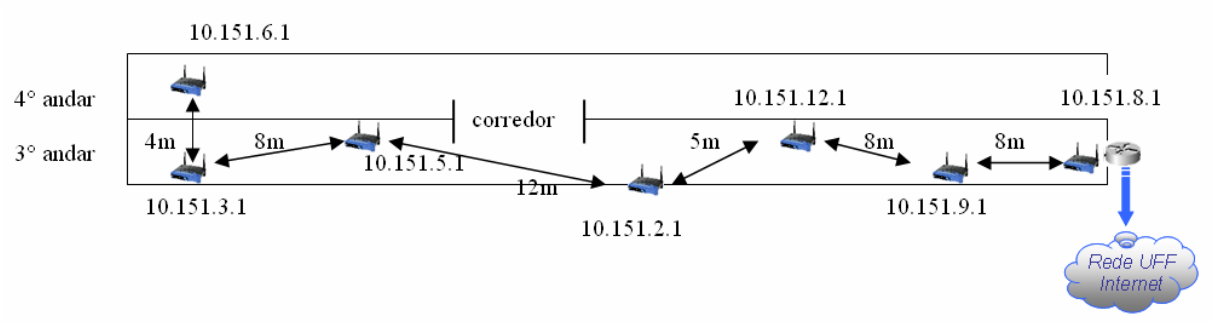


Figura 21: Topologia da rede interna

As configurações dos nós da rede interna são:

- Potência de saída: 255mW (aproximadamente 24 dBm). Este é o valor de potência máximo obtido com a utilização do OpenWrt. Nominalmente, os roteadores WRT54G da Linksys trabalham com uma potência de saída máxima de 79mW (19 dBm);
- Duas antenas de 5dBi cada, operando simultaneamente para recepção, porém só uma é utilizada para transmissão em um modo denominado "automático" pelo fabricante;
- Canal 1, canal menos utilizado por outras redes;
- ESSID: gt_mesh_interna;
- Limiar de RSR (Relação Sinal Ruído) na recepção: -94dBm para 1 Mbps, -88dBm para 2 Mbps; -87 dBm para 5.5 Mbps e -84dBm para 11 Mbps (BÜTTRICH, 2005);
- Altura aproximada entre o chão e a antena: entre 1 e 1,5m;

- Controle de taxa no modo automático (modo possibilitado pela interface sem fio).

A taxa de interface foi definida após algumas medições de vazão, utilizando os seis saltos existentes.

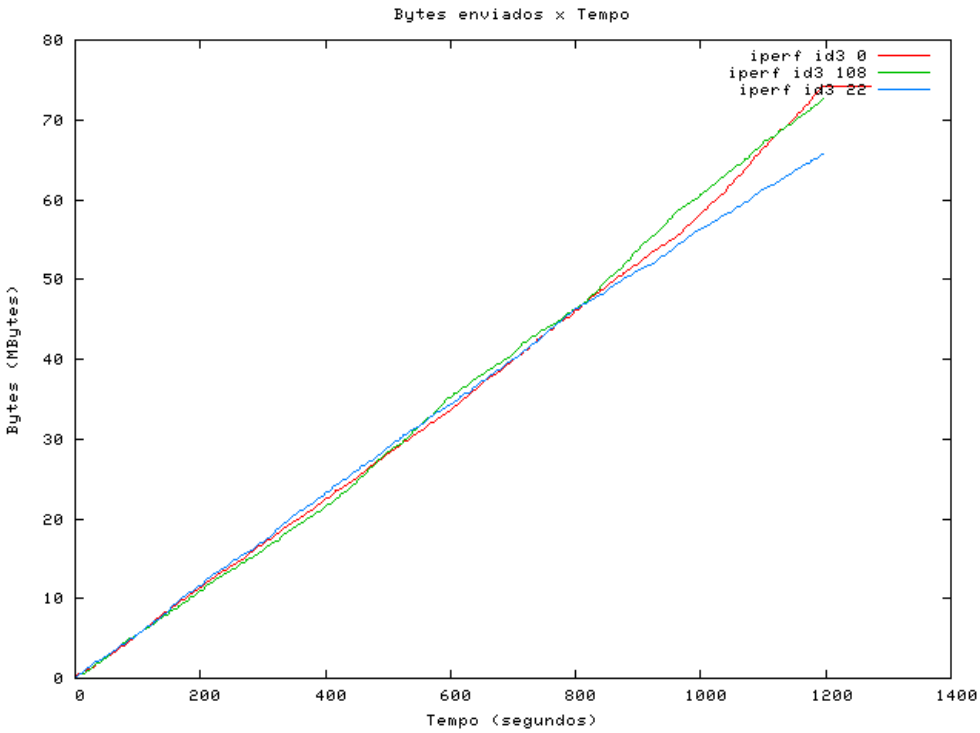


Figura 22: Quantidade de bytes enviados por tempo para diferentes valores de taxa da interface

Na Figura 22, a legenda indica a ferramenta utilizada para a medição, a identificação do nó de origem das medições e o valor da variável *wl0_rate*, respectivamente. No momento da medição, o roteador 10.151.4.1 (*ID 3*) estava na ponta esquerda da seqüência dos nós. Este roteador na topologia atual está na rede externa e foi substituído pelo de *ID* 5 (10.151.6.1). A ferramenta utilizada foi o *iperf* (TIRUMALA *et al,* 2005) transmitindo tráfego TCP ("*Traffic Control Protocol*", PETERSON e DAVIE, 1999).

O *iperf* consiste em uma ferramenta que pode operar tanto com TCP como com UDP. Ele atua com um módulo cliente e um módulo servidor. Utilizando o TCP, o módulo cliente tenta ocupar o máximo da banda disponível e recebe do módulo servidor a quantidade de dados foram entregues. Utilizando UDP ("*User Datagram Protocol*"; PETERSON e DAVIE, 1999), a banda que se deseja medir tem que ser utilizada como parâmetro de entrada.

Entretanto, o interesse no momento é apenas demonstrar o motivo da escolha do valor de operação da taxa da interface.

Os diferentes valores da variável *wl0_rate* são interpretados como o dobro da taxa da interface: 22 equivale a 11 Mbps, 108 equivale a 54 Mbps e 0 se refere ao modo automático. Para cada um dos três testes, os sete roteadores que constituem a rota de seis saltos devem ter suas respectivas variáveis configuradas adequadamente. Os testes foram realizados consecutivamente, com rotas estáticas (sem o protocolo de roteamento em funcionamento) e cada um durou 20 minutos.

Como pode ser observado, o valor *automático* do modo de operação teve um resultado muito próximo ao valor limite da interface. CHEBROLU *et al* (2006) mostra como a taxa da interface pode influenciar na taxa de perda de pacotes. Isto ocorre principalmente porque o limiar da RSR na recepção aumenta. Em vista das variações que os enlaces sem fio podem sofrer e pelo resultado obtido no teste da Figura 22, decidiu-se adotar o modo de operação automático.

Com os dados dos equipamentos, é possível realizar um cálculo de enlace (*Link Budget,* RAPAPPORT, 1996) entre dois nós para o pior caso de taxa de operação da interface, 1 Mbps, e para o caso de 11Mbps (Tabela 4).

Taxa da Interface: Nó → Nó	1 Mbps	11 Mbps	unidade
Potência de Tx	24	24	dBm
Perda nos cabos e conectores (Tx)	0	0	dB
Ganho de Antena (Tx)	5	5	dBi
PEII (Potência Equivalente Isotrópicamente Irradiada)	24 + 5 =27	24 + 5 =27	dBm
Limiar de potência de recepção (Prlimiar)	-94	-84	dBm
Perda nos cabos e conectores (Rx)	0	0	dB
Ganho de Antena (Rx)	5	5	dBi
Nível de Sinal Recebido mínimo	-94 - 5 = -99	-84 - 5 = -89	dBm
Perda Máxima de Percurso	**27 – (- 99) = 126**	**27 – (- 89) = 116**	dBm

Tabela 4: Cálculo da perda máxima no enlace sem fio para a rede interna

Considerando a topologia da rede interna da UFF, o pior caso dos enlaces inclui a passagem por um piso e duas paredes, representando duas salas distintas com dois roteadores instalados (enlace entre 10.151.6.1 e 10.151.3.1). Estimando o piso como “muito espesso” e

as paredes como “espessas” (aproximadamente 15 cm), utilizando os valores da Tabela 1 e utilizando a expressão de COST 231 Keenan e Motley, pode-se escrever:

1 Mbps: $L_{total} = L_0 + 10 \times n \times \log(d) + 2 \times 15 + 25 < 126$

11 Mbps: $L_{total} = L_0 + 10 \times n \times \log(d) + 2 \times 15 + 25 < 116$

Valores típicos podem ser obtidos em COST 231 (1999). Seguindo a Tabela 2, para ambientes confinados, porém mais amplos do que prédios e sem linha de visada, um valor usual para n é 2,3 (COST 231, 1999; RAPAPPORT, 1996). O valor adotado para L_0 foi de 45 dB, tanto para ambientes internos como externos. Para esses valores e uma distância de 4 metros, L_{total} vale:

$$L_{total} = 45 + 10 \times 2,3 \times \log(4) + 2 \times 15 + 25$$
$$L_{total} \cong 114$$

A perda de propagação calculada ficou 2 dBm abaixo do limite permitido pelo equipamento à 11 Mbps (116 dBm pelo *Link Budget)* e 12 dBm para 1 Mbps (126 dBm). Neste caso, o enlace é viável para ambas as taxas. Entretanto, se a distância entre eles aumentasse para 5 metros, L_{max} seria igual a 116 dBm. A qualidade da transmissão seria severamente afetada para a taxa de 11 Mbps, tornando necessária a operação da interface em taxas mais baixas.

Para os outros enlaces, sabendo-se que não atravessam pisos (Figura 21) e inferindo as mesmas características para todas as paredes que abrigam os roteadores, teoricamente poderiam alcançar distâncias de até 164,8 metros na taxa de 1 Mbps e 60 metros na taxa de 11 Mbps (considerando uma parede “espessa” por sala). Porém, além dos outros fenômenos não cobertos pela fórmula como obstáculos adicionais no percurso (mesas, cadeiras, etc), pessoas transitando e redes interferentes, uma grande dificuldade existente na rede interna da UFF é a presença do vão que o corredor representa no meio do percurso de propagação (enlace entre os nós 10.151.5.1 e 10.151.2.1). O corredor poderia ser interpretado como uma fenda em um guia de microondas retangular, por exemplo, se a fenda for transversal às linhas de corrente geradas no guia, boa parte da energia de propagação é dissipada para o seu exterior. Inclusive, este mecanismo é utilizado por alguns tipos de antenas (BALANIS, 2005). Obviamente, isto é apenas uma analogia para ilustrar o efeito singular que ocorre na rede interna neste local: o enlace que passa pelo corredor é o que tem a pior qualidade de sinal (baixa RSR), limitando a taxa de interface dos seus nós e, conseqüentemente, a vazão total nos seis saltos.

3.4 REDE EXTERNA

A rede externa foi criada para a validação do protótipo como um produto funcional e em condições de ser utilizado em situações fora de um ambiente controlado. O planejamento foi feito ao longo dos seis primeiros meses do projeto onde diversos anúncios foram colocados através de diferentes meios (painéis, panfletos, internet e comunicados aos professores).

Em resposta à divulgação, foi montado um banco de voluntários que foram mapeados e analisados através de visitas nos locais. Nas visitas eram avaliados: a viabilidade de espaço para instalação, presença de pára-raios menores do que a haste do protótipo, presença de visada direta para algum outro nó da rede, condições dos dutos para passagem de cabos, viabilidade de passagem do cabo pelo lado de fora e autorização do síndico e condôminos (Figura 23).

Figura 23: Vistoria da viabilidade de instalação do protótipo externo em diferentes prédios: 1. Presença de antenas interferentes; 2. Acesso até o apartamento do voluntário; 3. Viabilidade de passagem dos cabos; 4. Presença de linha de visada para outro ponto; 5. Espaço físico com condições de perfuração do chão

Na Figura 24, os círculos representam os voluntários próximos ao campus da UFF. Os voluntários que apresentavam condições de instalação foram numerados na ordem em que foram que visitados.

Figura 24: Mapeamento inicial da rede externa (GOOGLE MAPS, 2007)

A segunda fase consistiu na instalação do protótipo. Os protótipos foram instalados nos seguintes números da Figura 24: UFF, 1, 3, 6, 7 e 8. Obviamente, eventos não esperados ocorreram durante o processo: danos nos cabos de RF (RGC 213) devido a ventos fortes; falta de comunicação entre o nós desejados e usuários que desligavam eventualmente o módulo POE. Através de freqüentes supervisões, esses eventos foram mantidos sob controle do projeto.

Até o final de 2006, a rede externa contava com um total de seis roteadores, incluindo o *gateway* localizado no topo do Bloco E do campus da UFF, que foi primeiro ponto a ser instalado. Em seguida, os outros pontos foram instalados, começando pelos nós 10.151.1.1 e 10.151.4.1 (vide Figura 25), que são os principais pontos de saída da UFF (responsáveis para que os outros nós alcancem o *gateway*). Todos os nós conseguem alcançar o *gateway* com boa qualidade, permitindo aos usuários acesso à Internet com altas taxas (comprovado no Capítulo 5, através de medições de vazão nos enlaces e de utilização da rede por parte dos usuários).

Na Figura 25, os balões representam os pontos instalados. Junto a eles, estão os seus respectivos endereços IP's e alturas aproximadas ("h") em relação ao solo. As linhas sólidas representam os enlaces mais freqüentes e as tracejadas representam os enlaces esporádicos. Os comprimentos aproximados dos enlaces, de antena a antena, também estão representados. As duas circunferências indicam um morro e um prédio, dois obstáculos que limitam a conectividade direta dos nós 10.151.11.1 e 10.151.14.1 ao *gateway*.

Figura 25: Topologia da rede externa com identificação dos nós, suas alturas e comprimento dos enlaces principais e secundários (GOOGLE MAPS, 2007)

As características dos nós são:

- Potência de saída: 255mW (aproximadamente 24 dBm).

- 1 Antena omni-direcionais de 18,5 dBi de ganho da marca HYPERTEC (2007)
- ESSID: gt_mesh_externa;
- Limiar de RSR (Relação Sinal Ruído) na recepção: -94dBm para 1 Mbps, -88dBm para 2 Mbps; -87 dBm para 5.5 Mbps e -84dBm para 11 Mbps (BÜTTRICH, 2005);
- Altura aproximada entre o chão e a antena: variando de acordo com o local de instalação (Figura 25):
    - 10.151.1.1 → 23 metros, possui obstrução do próprio prédio nas laterais, não permitindo conectividade com dois nós adjacentes 10.151.14.1 e 10.151.13.1. Localizado com enlace direto ao *gateway*. Geralmente faz a interconexão do nó 10.151.11.1 à UFF.
    - 10.151.4.1 → 60 metros. Ligado diretamente ao *gateway*. Faz a interconexão dos nós 10.151.13.1 e 10.151.14.1 à UFF.
    - 10.151.11.1 → 23 metros. Não se conecta à UFF através do nó 10.151.4.1 devido à obstrução no elipsóide de Fresnel causada pela posição da antena (Figura 26). Geralmente está a dois saltos da UFF. O enlace direto é comprometido por uma montanha (circunferência maior na Figura 25).
    - 10.151.14.1 → 30 metros. Não se conecta com freqüência diretamente à UFF devido à obstrução causada por um prédio (circunferência menor na Figura 25). Utiliza o nó 10.151.4.1, estando geralmente a dois saltos.
    - 10.151.13.1 → 60 metros. Utiliza o nó 10.151.4.1 e está a dois saltos da UFF.
- Controle de taxa no modo automático
- Opera no canal 2. Apesar de ser um canal sobreposto ao canal 1, apresentou menos interferência com relação aos canais 1, 3 e 4 através de medições utilizando o analisador de espectro do *Netstumbler*. Os canais 6 e 11 apresentavam alto grau de ocupação. As redes interna e externa estão fisicamente isoladas.

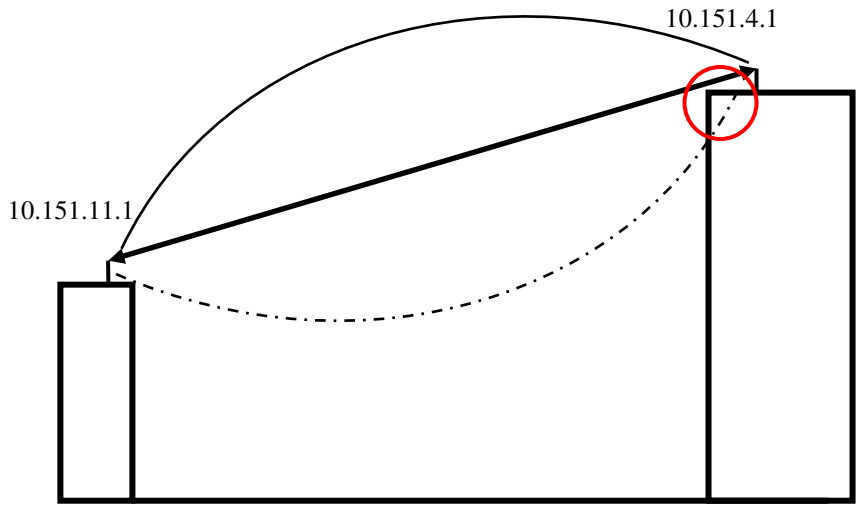


Figura 26: Ilustração do enlace entre os nós 10.151.11.1 e 10.151.4.1 com obstrução no elipsóide de Fresnel

Para as especificações acima, temos na Tabela 5 o cálculo de perda máxima de enlace (*Link Budget*) para dois nós e para duas taxas de interface: 1 e 11 Mbps.

Taxa da Interface: Nó → Nó	1 Mbps	11 Mbps	unidade
Potência de Tx	24	24	dBm
Perda nos cabos e conectores (Tx) – valor médio	2	2	dB
Ganho de Antena (Tx)	18,5	18,5	dBi
PEII (Potência Equivalente Isotropicamente Irradiada)	24 + 18,5 -2 = 40,5	24 + 18,5 -2 = 40,5	dBm
Prlimiar	-94	-84	dBm
Perda nos cabos e conectores (Rx)	2	2	dB
Ganho de Antena (Rx)	18,5	18,5	dBi
Nível de Sinal Recebido mínimo	-94 – 18,5 + 2 = - 110,5	-84 – 18,5 + 2 = - 100,5	dBm
Perda Máxima de Percurso	**40,5 – (- 110,5) = 151**	**40,5 – (- 100,5) = 141**	dBm

Tabela 5: Cálculo da perda máxima no enlace sem fio para a rede interna

Utilizando a expressão de COST 231 Keenan e Motley, pode-se escrever:

1 Mbps: $L_{total} = L_0 + 10 \times n \times \log(d) < 151$

11 Mbps: $L_{total} = L_0 + 10 \times n \times \log(d) < 141$

Utilizando a Tabela 2, para espaço livre, em ambiente urbano e em linha de visada pode-se utilizar **n** (constante de propagação) igual a 3 (COST 231, 1999; RAPAPPORT,

1996). O valor adotado para L_0 foi de 45 dB. Substituindo L_{total} por 151 dBm e 141 dBm, pode-se calcular a distância máxima dos enlaces para ambos os casos:

1 Mbps: $45 + 10 \times 3 \times \log(d) < 151$ $\quad d < 3411$

11 Mbps: $45 + 10 \times 3 \times \log(d) < 141$ $\quad d < 1585$

Em teoria, os enlaces nestas condições podem alcançar mais de 3 km na taxa de 1 Mbps e mais de 1 km na taxa de 11 Mbps, o que certamente atendia às necessidades do projeto. Entretanto, os enlaces que tinham uma grande diferença de altura não conseguiam se comunicar, mesmo em presença de visada direta. Especificamente entre o *gateway* e o nó 10.151.4.1 e entre os nós 10.151.14.1 e 10.151.4.1. Isto é explicado pelo lóbulo de irradiação da antena adotada (BOITHIAS, 1987), apresentado na figura abaixo:

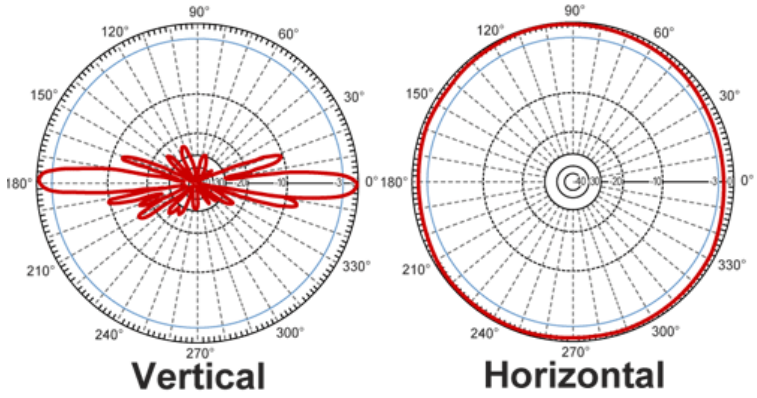


Figura 27: Lóbulos de irradiação da antena omni-direcional adotada no projeto (fonte: HYPERTEC, 2007)

Verticalmente, a irradiação de energia da antena é muito bem definida para baixo e para cima. Desta forma, a componente diagonal eletromagnética é fraca, tornando a diretividade da antena limitada para enlaces cujos nós estejam localizados em alturas próximas.

Em vista destes fenômenos, o projeto que antes contava com um modelo utilizando apenas antenas omni-direcionais com 18,5 dBi de ganho passou a usar antenas direcionais do tipo parábola 24 dBi. Para não diminuir a capacidade de crescimento incremental da rede (pontos com visada para todos os lados), as antenas direcionais foram colocadas em apenas um dos nós de cada enlace deficiente. No caso, foi colocada uma antena direcional no *gateway* (Figura 28) e uma no nó 10.151.14.1.

Figura 28: Nó da UFF com as duas antenas instaladas (direcional e omni)

A princípio, pensou-se em trabalhar com as duas antenas simultaneamente. Desta forma, seria possível instalar antenas direcionais para mitigar o problema de conectividade nos dois nós dos enlaces deficientes, sem perder a área de abrangência. Em outras palavras, “o melhor dos dois mundos”.

Para isto, seria utilizado o modo de operação de diversidade de antenas (diversidade espacial), disponibilizado pelo WRT54G. Através de uma variável da *nvram* disponibilizada pelo OpenWRT (*wl0_antdiv),* pode configurar o roteador para operar em três diferentes modos: apenas uma das antenas, apenas a outra ou as duas simultaneamente. Segundo OPENWRT-NVRAM (2007), o modo de diversidade funciona da seguinte forma: o rádio quando está em fase de recepção do sinal, consegue captar o sinal em ambas as antenas. Para transmitir, ele utiliza a antena que por último recebeu e decodificou com sucesso um quadro de dados. Uma característica das redes mesh é o encaminhamento de pacotes. Isto significa que um nó pode receber pacotes do vizinho de um lado e ter que encaminhá-lo para um outro que pode estar localizado no lado oposto. Devido a isto, a última antena que recebeu com sucesso um datagrama não será necessariamente a antena a ser utilizada para a próxima transmissão. Por isto, o modelo de diversidade empregado pelos equipamentos WRT54G apresentou baixa eficiência. Nas Figura 29, Figura 30 e Figura 31 estão ilustrados três curtos testes de vazão. Cada um dos três testes foi realizado durante 20 segundos utilizando a ferramenta *iperf*, gerando tráfego UDP. As medições foram feitas com tráfego sendo

originado a partir do nó *gateway* (com as duas antenas instaladas) e recebido pelo nó adjacente 10.151.1.1, sem a presença do protocolo de roteamento.

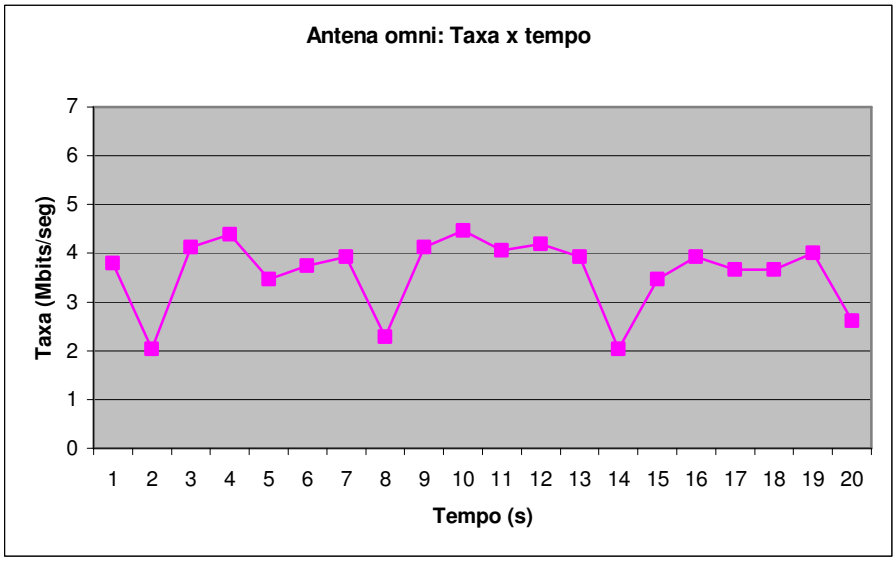


Figura 29: Desempenho da antena omni-direcional - Média de 3.53 Mbps

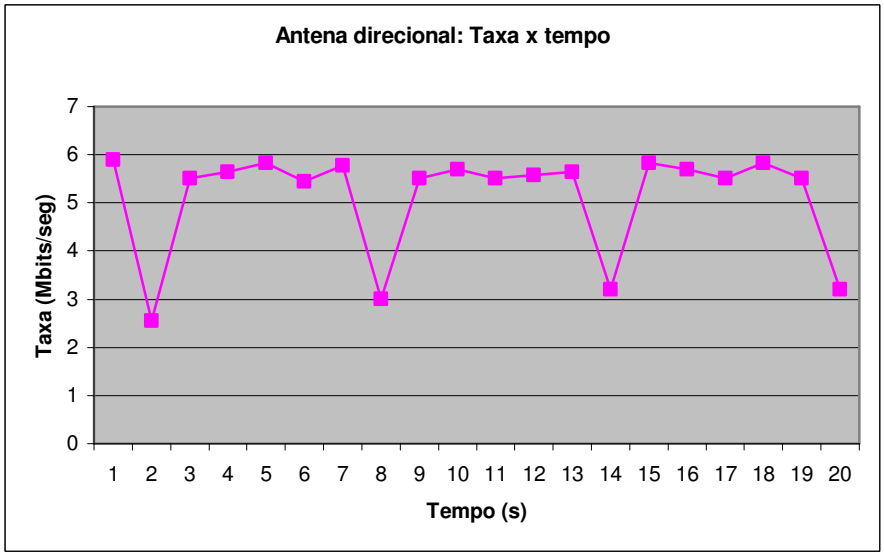


Figura 30: Desempenho da antena direcional - Média de 5.09 Mbps

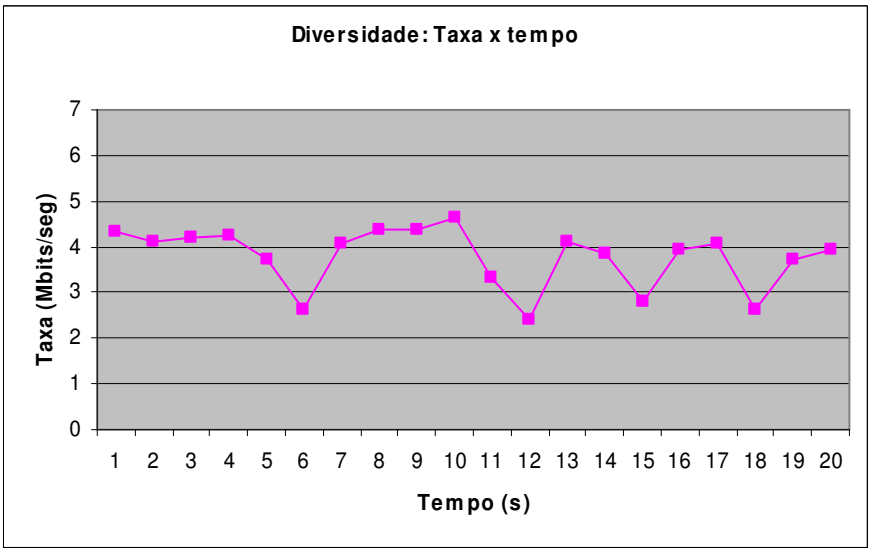


Figura 31: Desempenho do modo de diversidade - Média de 3.77 Mbps

Pelos resultados obtidos, percebe-se que a antena direcional apresentou maiores valores de taxa do que os outros dois modos. Os outros dois modos apresentaram valores bastante semelhantes. Os três testes foram realizados consecutivamente, na ordem como foram apresentados nas figuras. Isto significa que a semelhança encontrada entre os valores dos dois testes (antena omni-direcional e diversidade) tem baixa probabilidade de ter sido influenciada por algum fenômeno de propagação (formação de uma área com vapor d'água alterando o índice de refração do percurso ou a ocorrência de chuva, por exemplo).

O modo de diversidade apresentou uma ligeira melhora na taxa média em relação à antena a omni-direcional, entretanto, ficou abaixo do resultado obtido com a direcional. Logo, atuando com ambas as antenas, era esperado que o modo de diversidade obtivesse algum valor próximo ao obtido com o uso da melhor antena. O resultado demonstrou que ocorreu o contrário, nos levando a abandonar o modo de operação de diversidade do equipamento. Cabe ressaltar que cada teste foi realizado alterando-se somente o valor da variável *wl0_antdiv*, mantendo-se as características físicas (ambas as antenas fixadas na haste). Adicionalmente, como o tráfego gerado foi UDP (sem controle de fluxo e de congestionamento), as medições se referem apenas a um sentido do fluxo.

Em vista disto, começou-se a desenvolver um módulo para o *driver* da interface sem fio dos roteadores. O modelo da interface é uma Broadcom, *chipset* 4707 (FORUM OPENWRT.ORG, 2007). O objetivo era a utilização eficiente e inteligente de ambas as antenas. A idéia seria criar, em cada roteador, uma tabela em sua memória contendo os seus

vizinhos diretos e a melhor antena que a ser utilizada para realizar a transmissão. No momento da transmissão de um determinado pacote, o módulo escolheria a antena adequada. Para a recepção, manter-se-ia o esquema original da interface que opera com ambas as antenas simultaneamente. Para a manutenção da tabela de vizinhos, dois procedimentos para iniciar as medições seriam adotados: 1. Com o objetivo de captar as variações aleatórias das condições de propagação dos enlaces, a primeira medição seria realizada periodicamente e durante um curto espaço de tempo. 2. A outra medição iniciaria toda vez que um novo vizinho fosse adicionado à tabela ARP[12] do roteador. O procedimento seria válido tanto para um novo nó mesh na rede como para um usuário pedindo acesso.

Para realizar as medições, o roteador alocaria cada uma das antenas separadamente. Ao final da medição, os resultados seriam avaliados e a antena que obtivesse o melhor desempenho seria eleita. As medições utilizariam as ferramentas já presentes nos roteadores: *ping* (ICMP – "Internet Control Message Protocol"), extraindo-se o tempo de ida e volta do pacote (RTT- "Round Trip Time") e *iperf*, fazendo uma rápida transmissão UDP quando o alvo da medição fosse um outro nó mesh (esta restrição é devida à estrutura de funcionamento cliente-servidor do *iperf*, exigindo que os nós de origem e destino o executem ao mesmo tempo).

Para demonstrar como a utilização inteligente de ambas as antenas faria diferença no desempenho da rede externa, foi instalado no nó *gateway* um script que realiza a mesma medição que o módulo proposto faria. O script faz uso do comando "*wl*" (WL COMMAND, 2007) que é um arquivo executável que acessa diversas opções disponíveis da interface sem fio (equivalendo à atuação na variável *wl0_antdiv*). O aplicativo *wl* também é distribuído juntamente com o *driver* da interface da Broadcom,

O script foi executado a partir do nó *gateway* durante cinco dias distintos: **22**, **23**, **25** e **27** do mês de Dezembro de 2006. Para cada dia, foram escolhidos quatro horários diferentes no intuito de captar a variabilidade diária: **4**, **10**, **16** e **22** horas. Os resultados estão na **Tabela 6**. O script encontra-se no ANEXO 3.

[12] ARP, "Address Resolution Protocol"; é um protocolo utilizado para descobrir um endereço Ethernet através do endereço IP. No OpenWrt (assim como em outros sistemas operacionais) os endereços Ethernet das máquinas pertencentes à mesma rede são armazenados em uma tabela, denominada tabela ARP (PETERSON e DAVIE, 1999).

Hora	**04**					**10**					**16**					**22**				
Dia	**22**	**23**	**25**	**26**	**27**	**22**	**23**	**25**	**26**	**27**	**22**	**23**	**25**	**26**	**27**	**22**	**23**	**25**	**26**	**27**
NÓ	**MELHOR ANTENA**																			
10.151.1.1	D	O	O	D	D	D	D	*	D	D	D	D	*	O	O	D	O	D	O	O
10.151.4.1	O	D	O	O	D	D	*	*	D	D	*	D	*	D	O	D	D	D	*	O
10.151.11.1	*	*	*	*	*	*	*	*	*	*	*	*	*	*	O	*	*	*	*	*
10.151.14.1	D	*	*	O	D	O	O	O	O	D	O	O	O	*	*	O	*	O	*	*
Legenda:	D → Antena Direcional O → Antena Omni-direcional * → Sem conectividade com nenhuma antena																			

Tabela 6: Melhor antena a partir do nó gateway por hora, dia e nó de destino

A primeira observação a ser feita sobre os resultados obtidos é relacionada ao enlace para o nó 10.151.11.1. Durante as medições, este enlace apareceu somente uma única vez com a antena omni-direcional no dia 27 às 16 horas. Como foi visto, este enlace sofre com a obstrução causada por um morro (Figura 25). O segundo enlace menos freqüente é até o nó 10.151.14.1 que também sofre com uma obstrução. Entretanto, percebe-se que este enlace pode estar ativo esporadicamente com a utilização da antena omni-direcional. Foram obtidas 10 medições captadas pela antena omni contra apenas 3 utilizando a direcional e 7 onde não houve conectividade alguma. Somente no dia 22 não houve perda de conectividade em nenhum horário, observando que por 3 vezes a antena omni direcional foi melhor. O período em que não houve falta de conectividade foi às 10 horas.

Os enlaces para os nós 10.151.1.1 e 10.151.4.1 foram os que obtiveram melhor distribuição nas observações. Para o nó 10.151.1.1, 7 horários apresentaram melhor resultado com a antena omni-direcional contra 11 com a antena direcional. Em dois horários não foi observada conectividade no mesmo dia (25): às 10 e 16 horas. No dia 22 o enlace obteve melhor performance com a antena direcional em todos os horários de medição. Dias 23, 26, e 27 houve 50% de distribuição entre as antenas para diferentes horários. No dia 23 os resultados foram alternados. Já nos dias 26 e 27, a antena direcional teve melhor resultado às 4 e 10 horas perdendo para a omni nos outros dois horários.

Para o nó 10.151.4.1, por 5 vezes a antena omni-direcional obteve melhor resultado contra 10 vezes com a direcional. Por cinco vezes não foi observada nenhuma conexão, sendo que duas vezes no dia 25, da mesma forma que o nó 10.151.1.1. O único período em que não houve perda de conectividade em nenhum dia foi às 4 horas. O único dia que não houve perda

de conectividade em nenhum horário foi dia 27. Da mesma forma que o nó 10.151.1.1, a antena direcional foi melhor nos horários de 4 e 10 horas.

Não foi observada nenhuma correlação entre dias e horários quanto ao uso das antenas. Evidenciando que para a obtenção de uma distribuição estatística do uso das antenas por dia ou horário, mais medições seriam necessárias. Contudo, o objetivo desta medição foi exatamente demonstrar a alta variabilidade da utilização das antenas. Tanto para um determinado dia, como para um determinado horário, os resultados com as antenas tiveram alta variabilidade. Com exceção do enlace 10.151.11.1, nenhum dos outros apresentou um resultado conclusivo sobre a utilização de uma única antena. O resultado indica que a operação simultânea e inteligente das antenas poderia trazer melhoras significativas na qualidade da rede externa.

Apesar de a medição ter indicado a necessidade do desenvolvimento do módulo para diversidade, o projeto não foi concluído. O módulo da interface sem fio do WRT54G é proprietário. Ele é distribuído como um arquivo binário presente na instalação do OpenWrt. Isto dificultou bastante o desenvolvimento que necessitava acessar diretamente as funções da interface, ficando para um trabalho futuro. As referências deste trabalho para programação em nível de módulos de *kernel* para sistemas baseados em Linux são COBERT *et al* (2005) e RUSSEL (2002).

Através do site da loja WIRELESS&CIA (2007), pode-se obter os preços dos itens que compõem o protótipo, estimando-se (até a data deste trabalho) que o preço de um protótipo mesh não ultrapassa a quantia de R$1.000,00, sem contabilizar o desktop e o preço do serviço de conexão à Internet. Este valor é bastante razoável se for considerado que cada nó mesh pode fornecer acesso a múltiplos usuários, permitindo a divisão do custo. O valor do protótipo é o resultado de um esforço conjunto do projeto em minimizar os custos. As soluções propostas possuem suas vulnerabilidades e dependências. O POE, por exemplo, depende da estabilidade do fornecimento de energia de um determinado usuário. O protótipo não incorporou na sua construção proteção contra raios (o que certamente aumentaria em muito o custo), tornando-o dependente das condições da instalação do local. As vulnerabilidades exigem uma manutenção constante da rede, porém este fato não invalida a capacidade de produção comercial do protótipo. Além disto, as medições que serão demonstradas no Capítulo 5 consolidam o protótipo como uma experiência universitária bem sucedida e utilizável.

Finalizando, o modelo inicial do projeto não tinha o objetivo de prover acesso sem fio aos usuários. O que se pretendia era uma réplica do modelo realizado em TSARMPOPOULOS (2005), onde o acesso dos usuários seria realizado apenas pela interface cabeada. Desta maneira, não foi feito um estudo mais detalhado da cobertura para os usuários sem fio. Certamente, a complexidade dos modelos demonstrados aumentaria muito. Os enlaces não seriam apenas diretos (em linha de visada), exigindo um estudo das condições de urbanização da região para os cálculos de perda por difração. O sombreamento e a interferência entre símbolos (interferência co-canal) na recepção dos usuários passariam a ter participação significativa nas perdas dos enlaces. O cálculo da perda máxima suportada pelo enlace em função dos equipamentos (*Link Budget*) apresentaria um valor menor devido à ausência de antenas de alto ganho nos usuários. A ausência deste planejamento não impediu que houvesse usuários sem fio pedindo acesso ao projeto.

No próximo capítulo será discutido o protocolo de roteamento. Para redes mesh baseadas no protocolo IEEE 802.11 nas extensões a/b/g, os protocolos de roteamento *ad hoc* têm fundamental importância na estrutura de funcionamento por múltiplos saltos. Baseado no projeto VMesh (TSARMPOPOULOS, 2005), a princípio adotou-se a utilização do protocolo OLSR, principalmente pelo fato de já existir uma implementação presente na distribuição atual do OpenWrt. Entretanto a versão original do OLSR não funcionou satisfatoriamente na rede de desenvolvimento do projeto (rede interna), apresentando alta variabilidade no estabelecimento das rotas e conseqüentemente alta taxa de perda de pacotes. Esta característica levou o projeto a empenhar grande energia no desenvolvimento de uma solução que estabilizasse o funcionamento da rede. Tal esforço ocasionou no desenvolvimento de uma nova extensão do protocolo, denominada OLSR - *Minimum Loss*.

4 PROTOCOLO DE ROTEAMENTO

Neste capítulo serão descritos os protocolos de roteamento *ad hoc* adotados ao longo do projeto Remesh (2006). Uma revisão dos principais protocolos existentes e suas métricas já foi feita no Capítulo 2 deste trabalho. O objetivo agora é detalhar os protocolos que foram efetivamente utilizados para a intercomunicação dos clientes e dos roteadores.

O desenvolvimento de um protocolo de roteamento deve ser baseado em alguns princípios básicos, incluindo a transparência, de tal forma que as aplicações possam ser isoladas da complexidade das especificações e gerenciamento de recursos, a integração entre as diversas camadas de protocolos, de forma que a banda disponibilizada seja configurável ou ao menos previsível fim-a-fim. Em vista disso, alguns requisitos devem ser observados e controlados, como o atraso, o *jitter* e a taxa de perda na entrega de pacotes, de forma a garantir uma boa estimativa da largura de banda disponível, dentro das características de uma rede.

O protocolo de roteamento foi uma das principais vertentes de pesquisa do projeto. Ao longo da utilização das redes, tanto a interna como a externa, diversas questões de desempenho e de perda de pacotes foram levantadas tomando-se como base a questão do roteamento. Diversas pesquisas sobre métricas e formas de roteamento foram feitas, motivando a realização de medições e alterações.

As primeiras experiências do projeto utilizaram o protocolo OLSR (CLAUSEN *et al,* 2001), através de sua implementação em código livre disponível na Internet (OLSR, 2006). O OLSR é um protocolo pró-ativo (STALLINGS, 2002) que mantém uma visão consistente da rede atualizando constantemente a tabela de rotas. Isto é feito através do envio periódico de pacotes de controle denominados “HELLO”, em regime de broadcast. Cada nó deve informar

no pacote de HELLO quais são os seus nós vizinhos (nós que estão a um salto). A partir desta informação, os nós montam a sua própria lista de MPR's ("*Multipoint Relay"*). Um determinado nó é eleito como MPR para o seu vizinho quando ele é o intermediário para demais nós da rede. Segundo os proponentes do OLSR, a utilização de MPR's torna o "*flooding*" na rede mais eficiente. À medida que um nó recebe as informações dos MPR's dos demais nós da rede, o protocolo utiliza o algoritmo de Dijkstra (PETERSON e DAVIE, 1999) para montar a sua própria tabela de rotas.

Para o compartilhamento das tabelas de rotas, o OLSR utiliza um outro pacote de controle denominado TC ("*Topology Control*"). No pacote de TC são transmitidas todas as informações sobre as rotas de cada nó incluindo os valores de ETX para cada enlace. Através dos pacotes de TC os roteadores conseguem montar uma visão global da rede e não apenas dos seus próprios MPR's.

Segundo a RFC do OLSR (CLAUSEN *et al*, 2003), a métrica originalmente utilizada é a de contagem do número mínimo de saltos. Isto significa que a melhor rota é aquela que apresenta o menor número de roteadores no caminho entre a origem e o destino. Esta métrica torna-se insuficiente para estimar uma rota na medida em que a topologia começa a se tornar mais densa. Isto porque pode haver mais de um MPR que possa levar um determinado pacote para o mesmo destino.

Em ambientes sem fio, as condições dos enlaces são bastante variáveis dependendo de diversos fatores climáticos (umidade, temperatura, salinidade, chuvas, etc) e aleatórios (obstruções físicas, interferências de sinais espúrios, etc). Isto significa que um mesmo nó pode se comunicar com mais de um nó vizinho de maneiras completamente diferentes. Isto levou à necessidade da utilização de uma outra métrica para a utilização do OLSR. Em sua implementação, as primeiras versões do OLSR utilizavam somente a métrica de contagem de saltos. A partir da versão 0.4.8 esta implementação passou a utilizar uma métrica denominada ETX – *Expected Transmission Count* (COUTO *et al*, 2003), detalhada na subseção **2.2**.

No decorrer do projeto, viu-se que o ETX não estava sendo suficientemente satisfatório para uma transmissão contínua. Por diversas vezes as rotas se alteravam e o tempo de sincronização dos nós não era suficiente para evitar a excessiva perda de pacotes e o longo atraso. A partir da necessidade de aumentar a estabilidade da transmissão de pacotes na nossa rede, criamos uma pequena variação da extensão ETX a qual denominamos de ML – *Minimum Loss* (PASSOS *et al,* 2006). Nas próximas subseções explicaremos o

funcionamento de cada uma das métricas e demonstraremos testes comparativos referentes à perda de pacotes, atraso, jitter, estabilidade das rotas e vazão.

4.1 EXTENSÕES DO OLSR

Antes de explicarmos o funcionamento das métricas do OLSR, alguns conceitos devem ser explicitados. Segundo o padrão IEEE 802.11 (KOKSAL, JAMIESON, *et al*, 2006; KOKSAL e BALAKRISHNAN, 2006; STALLINGS, 2002), para o envio de pacotes de dados, a camada de enlace deve retransmitir o quadro até um número determinado de vezes, para que este seja entregue com sucesso. O padrão indica até sete vezes, realizado de maneira transparente para as camadas superiores.

Entretanto, para pacotes de broadcast, não deve haver retransmissões de nível 2. Também é padronizado pelo IEEE 802.11, que o envio de pacotes de broadcast deva ser feito na taxa mais baixa da interface, 1Mbps. A utilização de taxas mais baixas, diminui o nível da codificação dos dados, tornando a codificação mais robusta e menos sujeita a falhas no percurso (DRAVES *et al,* 2004 [a])

A partir deste conceito, pode-se estimar que o envio com sucesso de um pacote de broadcast representa uma transmissão perfeita em nível 2. A métrica ETX visa qualificar um determinado enlace através do número de retransmissões de nível 2 para que se consiga enviar um pacote de dados com sucesso. A implementação do OLSR utiliza os próprios pacotes de "HELLO" modificados, para fazer a estimativa do ETX. A cada intervalo de tempo t (padrão da implementação é $t = 2$ segundos), um nó transmite um pacote de HELLO. Cada nó gera uma janela deslizante de tempo w, referente ao nó que envia, preenchendo a cada t segundos com 1 ou 0, referente ao sucesso ou a falha no envio, respectivamente. Desta forma, após w segundos, uma janela já está totalmente preenchida. Dados r pacotes que efetivamente foram enviados com sucesso, a probabilidade de entrega p é dada por:

$$p = r/w.$$

O valor do ETX do entre os nós será dado pelo inverso de p:

$$\text{ETX} = 1/p \text{ ou } w/r.$$

Desta forma, estima-se que para a entrega de um pacote com sucesso, seja necessário o número de vezes representado por ETX de retransmissões de nível 2. Analogamente, um valor de ETX igual ou maior do que 1 representa um enlace onde a probabilidade de entrega de um

pacote sem retransmissões de nível 2 seja de 1/ETX. Percebe-se que o ETX irá variar de 1 até infinito, porém para a probabilidade de entrega nula ($p = 0$), o ETX recebe o valor 0, representando a ausência de enlace.

4.1.1 Métrica original

Em uma rota com múltiplos enlaces, o protocolo irá estimar o ETX total fazendo a soma dos ETX's de cada enlace. Por exemplo, considerando uma rota formada por três nós consecutivos, A, B e C, respectivamente, teremos o seguinte valor de ETX entre A e C:

$$ETX_{AC} = ETX_{AB} + ETX_{BC}$$

O protocolo irá eleger a rota que apresentar o menor valor do somatório dos ETX's. Este valor significa o número de retransmissões de nível 2 necessárias para que um pacote seja entregue com sucesso entre A e C. No caso de rotas que possuam o somatório com o mesmo valor, o critério de desempate é o menor número de saltos.

Contudo, após o projeto ter colocado a rede interna em funcionamento (primeira rede de testes), observou-se que as rotas mudavam com uma freqüência muito alta. Tal instabilidade ocasionava em uma alta taxa de perda de pacotes.

Para ilustrar este problema, tomemos, por exemplo, uma janela de tamanho $w = 22$ segundos, sendo preenchida a cada 2 segundos com a estimativa de entrega dos pacotes de HELLO. Suponha a existência de três nós N1, N2 e N3, onde todos se comunicam. Considere duas possíveis rotas entre N1 e N3: a primeira passando por dois enlaces perfeitos N1→N2→N3 (ETX igual a 1 para cada enlace, somando em um ETX igual a 2 para a rota ao longo de todo o intervalo de tempo da janela); a segunda, uma rota direta (N1→N3) passando por um enlace com 50% de probabilidade de perda de pacotes (a cada intervalo de $2t$ segundos um pacote é perdido). A Figura 32 representa uma abstração do estado das janelas de cálculo do ETX ao longo do tempo.

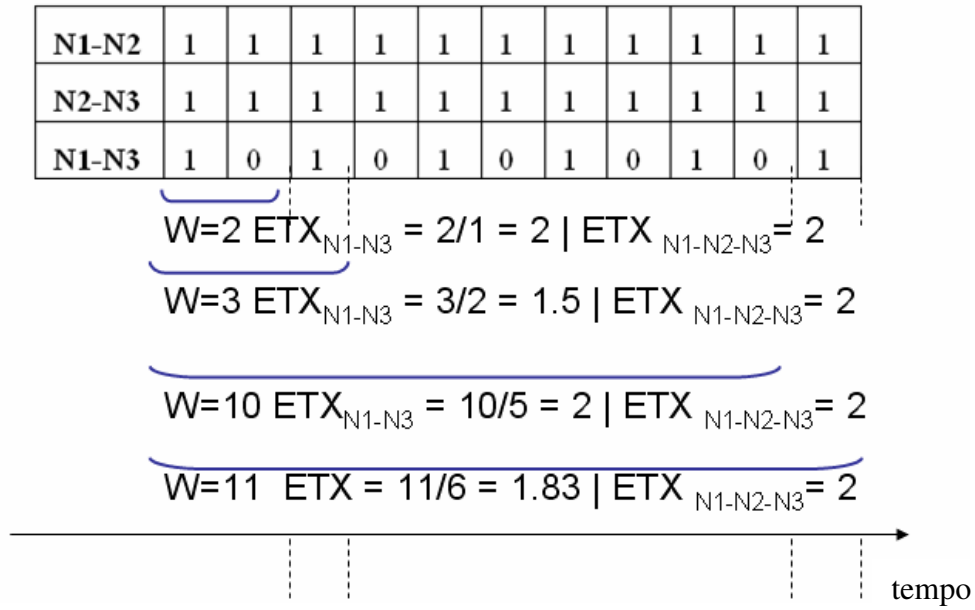


Figura 32: Exemplo de janela de cálculo de ETX para três nós ao longo do tempo (PASSOS *et al, 2006)*

Como pode ser observado, à medida que a janela é preenchida, diferentes valores de ETX vão sendo computados. Considerando *r* o número de pacotes que são entregues com sucesso e que o ETX do enlace é igual a *w/r,* vemos que o menor ETX sempre fica com o enlace direto (50 % de perda de pacotes). Mesmo quando os valores são iguais (ETX = 2), pelo critério de desempate do menor número de saltos, a rota direta sempre será a escolhida.

Os proponentes do ETX (COUTO *et al,* 2003*)* argumentam que a vazão é maximizada para rotas com um menor número de saltos, mesmo que esta apresente perda de pacotes, devido ao fato dos nós próximos estarem compartilhando o mesmo meio, aumentando o tempo de contenção de acesso ao meio. Esta mesma argumentação também é utilizada na proposta do projeto Roofnet (BICKET *et al,* 2005). Certamente, o número total de transmissões de nível 2 ao longo de toda a rota é minimizado. Entretanto, como uma rota com uma alta taxa de perda de pacotes é utilizada, o número de retransmissões de nível 2 decorrentes das tentativas falhas de envio de pacotes é maior, porém não é computada. Se, no enlace com perdas, fossem adicionados ao valor do ETX o número de retransmissões de nível 2 que ocorreram para cada pacote perdido, a rota N1→N3 apresentaria um valor de ETX muito maior.

Isto pode ser inferido observando-se o incremento que ocorre no valor do ETX para cada pacote perdido. Considere uma janela de tamanho *w* com *r* pacotes recebidos com sucesso:

$$ETX_t = \frac{w}{r}$$

Em seguida, a janela irá deslizar para a chegada de um novo pacote que, na realidade, foi perdido:

$$ETX_{t+1} = \frac{w}{r-1}$$

Considerando δ o incremento, temos:

$$\delta = ETX_{t+1} - ETX_t$$

$$\delta = \frac{w}{r} - \frac{w}{r-1} = \frac{w}{r(r-1)}$$

Este incremento é bem pequeno para enlaces com baixa perda de pacotes e chega a valores próximos de 1 quando a perda de pacotes é próxima de metade da janela. Como mencionado anteriormente, o valor do ETX para um enlace perfeito é igual a 1 (vide Figura 33), fazendo com que o incremento aditivo seja 1 para cada salto adicional que surge na rota. Em resumo, o OLSR com a extensão ETX tende a selecionar rotas mais curtas com maior taxa de perda de pacotes do que rotas com maior número de saltos e com menor perda de pacotes.

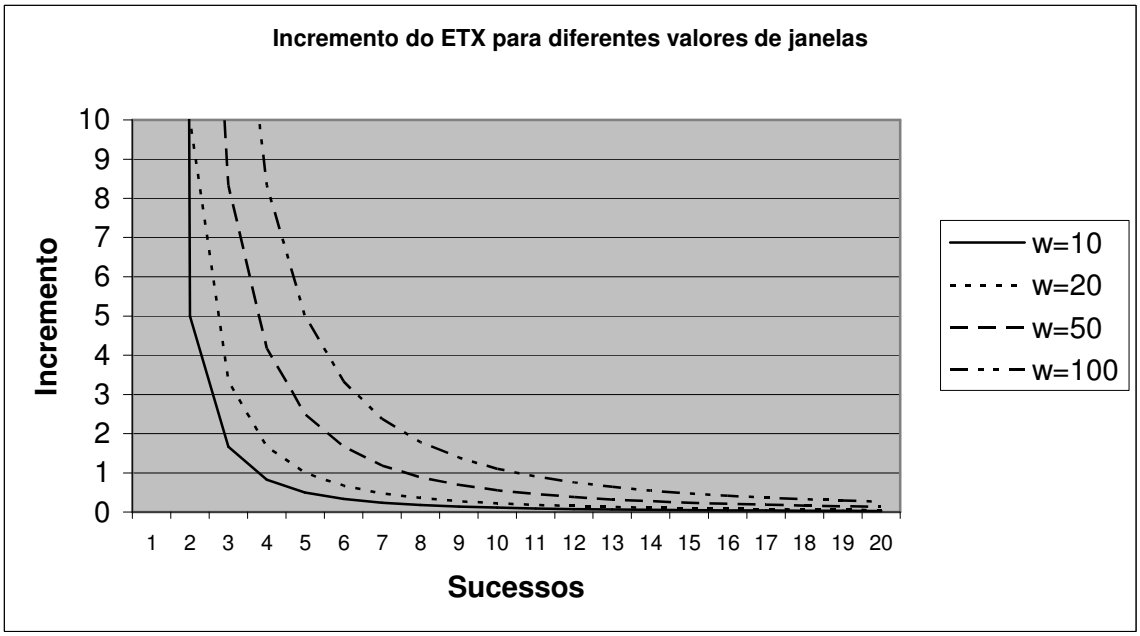


Figura 33: Variação do incremento para diferentes valores de janelas

4.1.2 Métrica proposta

Em vista dos problemas de altas taxas de perdas e instabilidade de rotas que ocorriam com a utilização do OLSR com métrica ETX, foi proposta uma pequena alteração no protocolo para que a rede se tornasse mais estável. Como o objetivo era a diminuição da taxa de perda de pacotes, a nova extensão foi denominada de ML – *Minimum Loss* (PASSOS *et al*, 2006).

A idéia do OLSR-ML é utilizar a probabilidade de entrega com sucesso de pacotes ao invés do número de retransmissões esperadas no nível 2, o ETX. Ou seja, dada uma rota com múltiplos saltos (A → B → C), nós estimamos a probabilidade de sucesso fim a fim através do produto das probabilidades de sucesso de cada enlace. No caso, a rota A para C passando por B seria dada por:

$P_{AC} = P_{AB} \; x \; P_{BC}$

Como a probabilidade de sucesso é o inverso do ETX, temos:

$P_{AB} = 1/ ETX_{AB}$

$P_{AC} = 1/ ETX_{AB} \text{ x } 1/ETX_{BC}$

Utilizando o produto e não a soma, passamos a escolher a rota com a maior probabilidade de sucesso na entrega de um pacote. Sendo assim, uma rota constituída por dois enlaces perfeitos (cada enlace com probabilidade igual a 1) teria a probabilidade de sucesso fim a fim igual a 1. Levando-se em conta que a probabilidade de sucesso de entrega de um pacote está diretamente ligada com a taxa de perda de pacotes do enlace, desta maneira estamos privilegiando caminhos com maior número de saltos e com menos perdas do que caminhos com menor número de saltos porém com maior taxa de perdas. No caso da situação onde, para um caminho existem duas rotas, uma passando por dois enlaces perfeitos e outra direta, porém também perfeita, o critério de desempate do OLSR original elegerá a rota com menor número de saltos.

4.2 MEDIÇÕES NA REDE INTERNA

Uma seqüência de testes foi realizada na nossa rede interna (Figura 34) visando a comparação dos dois protocolos quanto à variação dos valores de ETX, estabilidade de rotas, perda de pacotes, atraso e vazão. Como mencionado no Capítulo 3, a rede interna é

constituída de 7 nós espalhados ao longo de dois andares adjacentes de um prédio do campus da UFF, instalados em diferentes salas (ou seja, separados por paredes ao longo de todo o percurso), cobrindo uma extensão de aproximadamente 50 metros. Os roteadores da rede interna mantêm as suas antenas originais (omni-direcionais de 5 dBi de ganho). Nas próximas subseções adotaremos os nomes OLSR-ETX e OLSR-ML para diferenciarmos o protocolo original e o proposto, respectivamente.

4.2.1 Variação do ETX na rede interna

A Figura 34 representa os nós da rede interna com enlaces nomeados. Os nós estão classificados de acordo com o terceiro byte do seu endereço IP (ID + 1) e pelas diferentes salas onde eles foram instalados. Por exemplo, o nó 6 está localizado no Midiacom (laboratório da pós-graduação da Engenharia de Telecomunicações da UFF). As linhas contínuas representam enlaces de boa qualidade (baixa taxa de perda de pacotes) enquanto que as linhas pontilhadas representam enlaces piores. Os enlaces L1 a L20 (L provém de "Link") foram monitorados utilizando o *plugin dot-draw* (OLSR, 2006) da implementação do OLSR, representado na Figura 35. Na mesma figura podemos ver que os enlaces principais da rede interna possuem boa qualidade com valores de ETX em torno de 1,5, com exceção do enlace entre os nós 10.151.2.1 e 10.151.3.1 (marcado pela elipse na figura). Este enlace não é preferencial e pouco freqüente na construção das rotas. Na mesma figura, é possível ver dois enlaces com ETX igual a zero. A explicação para este fato é que a implementação do OLSR do projeto foi configurada para trabalhar com um alto tempo de desistência do nó. Isto significa que o enlace em algum momento existiu (por questões de propagação diversas). Os nós armazenaram a informação, porém, no momento da captura da imagem, já não existia mais.

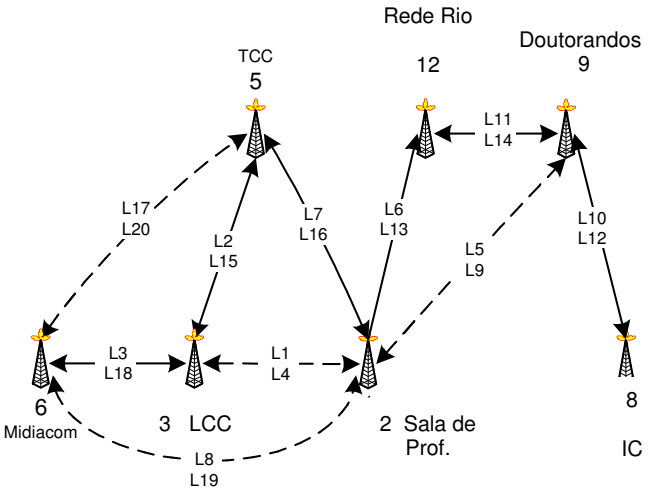


Figura 34: Nós da rede interna com enlaces nomeados (PASSOS *et al,* 2006*)*

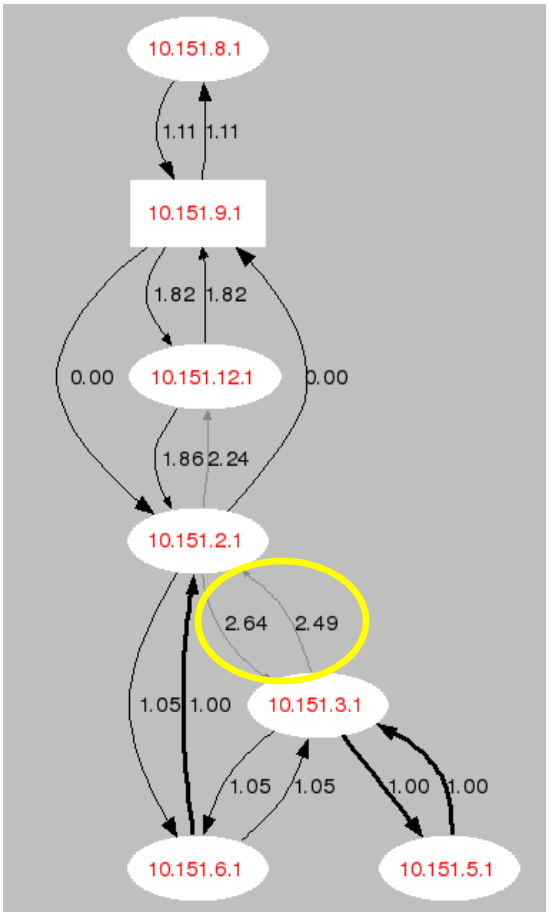


Figura 35: “Retrato” dos nós da rede interna representados por seus valores de ETX

O teste durou 24 horas e as informações dos diferentes valores de ETX foram armazenadas. Na Tabela 7 estão representados, para cada um dos 20 enlaces, os nós de Origem, Destino, os valores médio, mínimo, máximo e o desvio padrão do ETX (σ). As linhas em negrito representam os enlaces de boa qualidade e que possuem valor médio de ETX abaixo de 1,20.

L	O	D	Méd	Mín	Max	σ
L1	3	2	9,40	1,05	71,30	7,03
L2	**3**	**5**	**1,06**	**1,00**	**1,97**	**0,07**
L3	**3**	**6**	**1,12**	**1,00**	**51,00**	**2,07**
L4	2	3	10,09	1,00	53,12	8,02
L5	2	9	90,91	1,00	451,56	72,11
L6	**2**	**12**	**1,07**	**1,00**	**2,21**	**0,09**
L7	**2**	**5**	**1,13**	**1,00**	**13,42**	**0,17**
L8	2	6	2,40	1,00	104,04	4,08
L9	9	2	199,60	1,00	451,56	180,58
L10	**9**	**8**	**1,02**	**1,00**	**1,32**	**0,03**
L11	**9**	**12**	**1,07**	**1,00**	**1,39**	**0,06**
L12	**8**	**9**	**1,01**	**1,00**	**1,24**	**0,03**
L13	**12**	**2**	**1,06**	**1,00**	**2,28**	**0,09**
L14	**12**	**9**	**1,05**	**1,00**	**68,45**	**0,42**
L15	**5**	**3**	**1,04**	**1,00**	**30,44**	**0,19**
L16	**5**	**2**	**1,20**	**1,00**	**451,56**	**4,19**
L17	5	6	6,10	1,00	51,00	3,54
L18	**6**	**3**	**1,10**	**1,00**	**141,67**	**2,16**
L19	6	2	2,25	1,00	106,25	2,17
L20	6	5	8,21	1,05	425,00	6,58

Tabela 7: Valores de ETX monitorados na rede interna (PASSOS *et al,* 2006)

Percebe-se que, mesmo enlaces considerados de boa qualidade como L3 e L18 (ETX máximo de 141,67), podem apresentar valores extremamente altos para o ETX, o que representa períodos ocasionais de alta taxa de perda de pacotes. O mesmo fenômeno pode ser visto no enlaces L7, L14, L15 e L16. O contrário também é observado nos enlaces L4, L5, L9 e L17, que são considerados ruins. Estes apresentam valores médios de ETX altos, porém ocasionalmente não sofrem perdas (ETX mínimo igual a 1).

Observando o valor do desvio padrão, percebe-se a alta variabilidade do ETX, o que resulta em constantes mudanças de rotas. Considere uma transmissão entre os nós 2 e 6. Existe um enlace direto L8 com ETX médio de 2,40. Existe também uma rota alternativa passando por três enlaces, L7, L15 e L3 (nós 2→5→3→6) com um ETX médio de 3,29 (= 1,13 + 1,04 + 1,12). Pequenas flutuações na qualidade do enlace L8 podem resultar na mudança para a rota alternativa (σ_{L8} = 4,08). Deve-se observar também que os enlaces L7, L15 e L3 são enlaces mais estáveis e de menor perda (resultam em uma rota com 24% de probabilidade de perda) do que L8 (58,3% de probabilidade de perda).

4.2.2 Estabilidade de rotas na rede interna

Para verificarmos o número de vezes que as rotas se alteravam ao longo dos nós da rede interna, enviamos 18.000 pacotes de ping entre os nós das extremidades da rede (nós 8 e 6), registrando as rotas ao longo do percurso. O teste foi realizado durante um período de 5 horas entre 10 às 15 horas em um dia útil. OLSR-ETX registrou um total de **426** mudanças de rotas enquanto que o OLSR-ML não registrou **nenhuma** mudança de rota durante o mesmo período em outro dia útil.

4.2.3 Taxa de perda de pacotes na rede interna

O objetivo deste experimento é comparar a perda de pacotes entre os dois protocolos. Foram disparados 43.200 pings entre os nós das pontas (8 e 6). O teste durou um período de 12 horas para cada protocolo, no mesmo período, durante dois dias úteis. Como era esperado, a Figura 36 demonstra uma queda significativa na perda de taxa de perda de pacotes para o OLSR-ML, com reduções variando entre 59,8% e 97,0%.

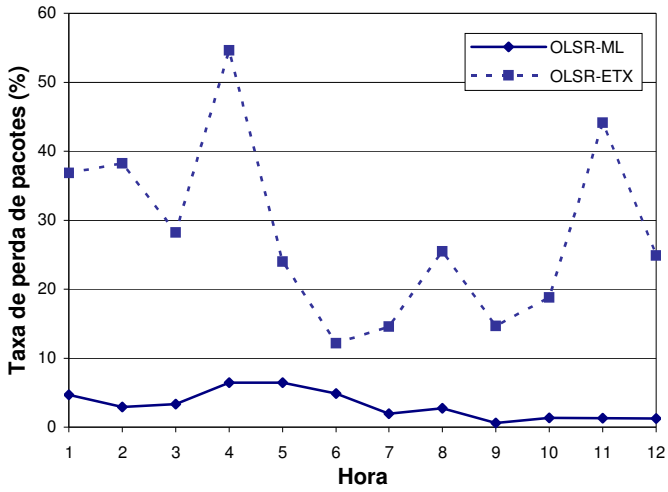


Figura 36: Taxa de perda de pacotes na rede interna para os dois protocolos (PASSOS *et al,* 2006)

4.2.4 Atraso e Jitter da rede interna

A medição com os envios dos pings também possibilitou a análise dos atrasos (vide Figura 37). Eles foram obtidos através do tempo de ida e volta (RTT - "*Round Trip Time*") de cada pacote de ping.

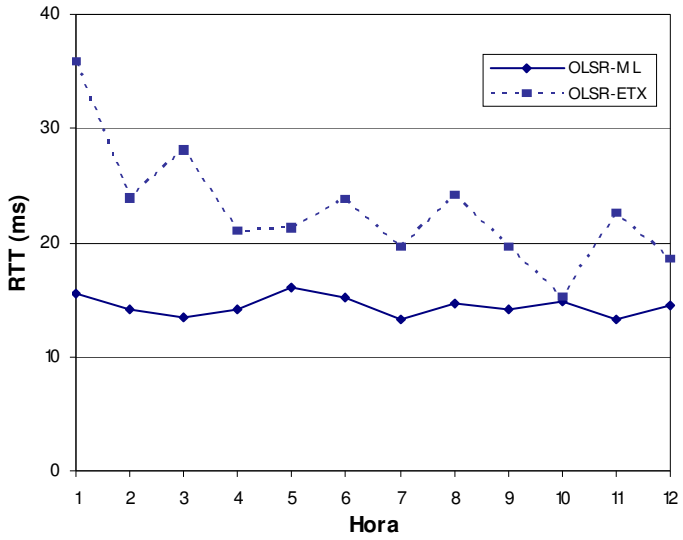


Figura 37: Tempo de ida e volta (RTT) dos pacotes ICMP para os dois protocolos (PASSOS *et al,* 2006)

Com o objetivo de selecionar caminhos de menor perda, o OLSR-ML tende a escolher rotas com um maior número de saltos e enlaces mais confiáveis comparado ao OLSR-ETX. O aumento do número de saltos poderia resultar em um atraso na rede maior. Certamente, aumentando o número de nós tentando transmitir no mesmo meio, aumenta-se o tempo de contenção devido ao protocolo de acesso ao meio CSMA-CA (*Carrier Sense Multiple Access – Colision Avoidance*; STALLINGS, 2002). Entretanto, a Figura 37 demonstrou que o atraso com o OLSR-ML diminuiu de 1,34% a 56,3% em relação ao OLSR-ETX durante todo o período da medição. Este ganho ocorre porque durante a transmissão de pacotes que atuam em camadas superiores à camada de enlace (camada 2), cada perda significa que sete retransmissões de nível 2 ocorreram e falharam. No nosso caso, o ICMP é um protocolo que atua no nível 3.

Escolhendo rotas mais confiáveis, estamos aumentando o número de retransmissões de nível 2 que possuem maior probabilidade de sucesso e diminuindo as que possuem maior probabilidade de falha. Esta situação é ainda pior para aplicações fim a fim que utilizam como protocolo de transporte o TCP. Uma perda em um enlace qualquer em um caminho com múltiplos saltos ocasionará na necessidade da retransmissão do pacote inteiro desde a origem. Neste caso, além do tempo gasto para a retransmissão, existe o tempo de *timeout* e o *backoff* exponencial da janela de transmissão do TCP (PETERSON e DAVIE, 1999).

Através de dois outros dias de medição utilizando o envio de pings, realizamos a medição do desempenho da rede quanto ao jitter. O procedimento foi o mesmo da medição

para perdas e atraso realizado anteriormente. Em cada dia foi testado um protocolo durante 12 horas ininterruptas, durante o mesmo horário.

O jitter da rede foi calculado pela diferença dos RTT's dos pacotes ICMP consecutivos. Para realizar a comparação dos protocolos, foram selecionados os valores em intervalos por hora (Figura 38).

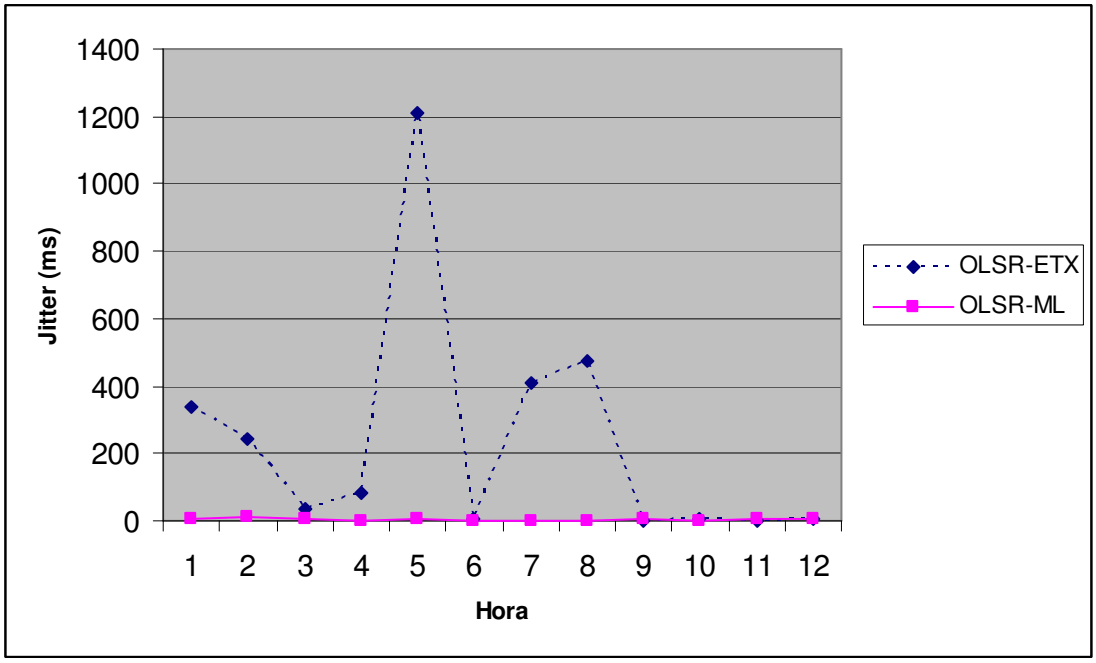


Figura 38: Jitter da rede interna para os dois protocolos

Percebe-se que o jitter permaneceu em torno de zero para o OLSR-ML, demonstrando uma alta estabilidade na variação do atraso durante a transmissão. A estabilidade da variação do jitter ao longo do tempo comprova que o OLSR-ML está preparado para suportar tráfegos que demandam cadência na entrega de dados, como fluxos multimídia e voz. Com o OLSR-ETX, o jitter apresentou variações bruscas até as quatro últimas horas de medição. O pico ocorrendo às 5 horas com o OLSR-ETX, precedendo uma seqüência de pacotes perdidos. Neste período, o OLSR-ML apresentou jitter 99,6% menor do que o OLSR-ETX.

4.2.5 Vazão da rede interna

Como mencionado na subseção anterior, COUTO *et al* (2003) argumenta que, minimizando o número de nós que compartilham o mesmo meio, a vazão é maximizada. Certamente, aumentando o número de nós tentando transmitir no mesmo meio, aumenta-se o

tempo de contenção e a probabilidade de colisão, resultando em uma queda significativa na vazão ao longo de uma rota com mais de um salto.

Para a medição da vazão, foi realizado um teste utilizando a ferramenta *iperf* (TIRUMALA *et al,* 2005). O *iperf* pode ser instalado facilmente dentro do Openwrt, nos permitindo, que os testes sejam executados a partir do próprio roteador (da mesma forma que são realizados os testes com o "ping"). Este teste consistiu no disparo de pacotes a partir do nó 8 (nó de borda da rede) para cada um dos outros nós participantes. O *iperf* mediu a vazão para cada nó enviando tráfego TCP unidirecional.

No total, foram realizadas 300 medições de 1 segundo para cada nó da rede, como pode ser visto na Figura 39.

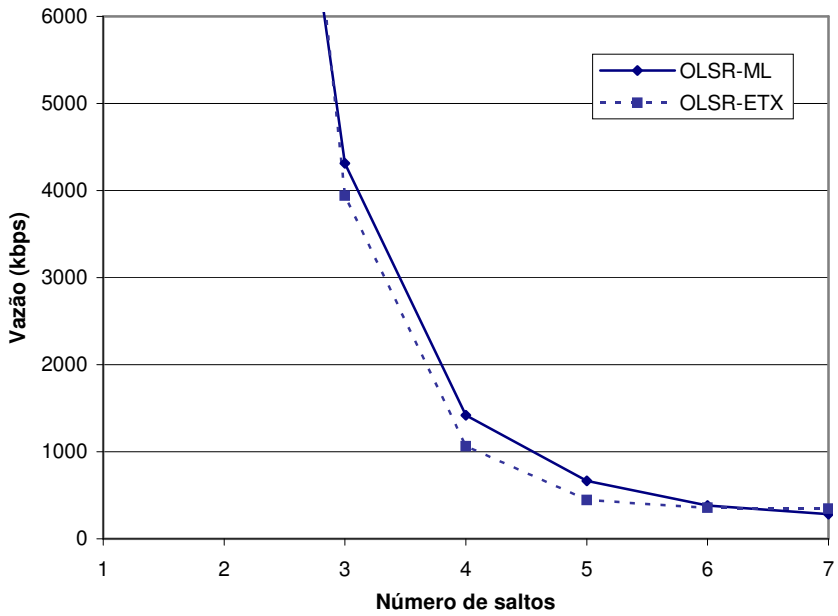


Figura 39: Vazão pelo número de saltos na rede interna para os dois protocolos (PASSOS *et al,* 2006)

Diferentemente do que era esperado, o OLSR-ML não apresentou queda na vazão. Ao contrário, para 3, 4 e 5 saltos apresentou uma leve melhora. A queda exponencial em função do número de saltos é consistente com o comportamento de outras redes em malha (BICKET *et al,* 2005; DRAVES *et al,* 2004 [a]). Isto ocorre pelo fato de que nós adjacentes, compartilhando o mesmo meio de colisão, precisam esperar o término da transmissão de cada um para que possam iniciar as suas próprias.

4.3 MEDIÇÕES NA REDE EXTERNA

A rede externa do projeto Remesh foi instalada gradativamente ao longo do ano de 2006 e tem expectativa de término apenas no ano de 2007. Até o momento de conclusão deste trabalho, seis nós foram instalados em topos de prédios das vizinhanças do campus da Praia Vermelha da UFF, sendo o *gateway* instalado no próprio prédio do campus.

As medições na rede externa foram mais difíceis de serem feitas devido a alguns fatores abaixo relacionados:

- Alta imprevisibilidade devido aos fatores de propagação inerentes ao ambiente externo. A aleatoriedade na rede externa é maior e mais complexa do que na rede interna onde possuímos algum controle da localização e monitoramento. Por exemplo, em dias de chuva as medições ficavam comprometidas, não possibilitando comparações.
- A formação de uma topologia onde os nós não se encontram em uma mesma seqüência. A partir do gateway, dois nós geralmente são alcançados com um salto e os outros três através de dois ou mais saltos, por rotas diferentes. Diferentemente da rede interna, onde os testes puderam ser realizados por toda a estrutura através dos nós das extremidades, na rede externa as medições tiveram que ser realizadas nó a nó.
- Cada nó da rede externa encontra-se no topo de algum prédio nas proximidades do campus. Isto significa que, em caso de problemas onde a atuação remota nos roteadores não funcionava mais, era necessário acessar o roteador diretamente. O que nos tomava bastante tempo não só pelo deslocamento, mas também pela necessidade do voluntário morador do prédio em questão estar presente.
- A rede externa é a nossa rede de produção. Existe tráfego real e pessoas que a utilizam. Apesar do cunho acadêmico do projeto, o protótipo tinha que operar com um mínimo de qualidade e disponibilidade para os usuários. Desta forma, medições como obtenção da vazão máxima da rede, requeriam que não houvesse nenhum outro tráfego coexistindo com o do teste. Isto tornava obrigatória a retirada dos usuários, porém com o provimento de aviso prévio.
- As antenas de alto ganho (18 e 24 dBi) aumentaram o alcance do nosso sinal, porém também aumentaram a área de interferência. Determinadas localidades abrangiam mais de dez redes operando na faixa de 2,4 GHz. Através de um "*wardrive*"

(procedimento para descobrir redes sem fio em uma determinada localidade, através da locomoção com um *laptop* com interface sem fio) descobrimos mais de 37 pontos de acesso na região de interesse, não havendo nenhum canal totalmente livre.

Na Figura 40 está demonstrada uma visão esquemática da topologia da rede externa evidenciando as rotas preferenciais, ou seja, aquelas que ocorrem com maior freqüência.

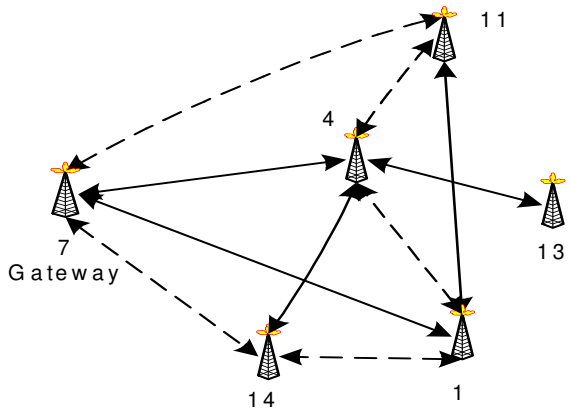


Figura 40: Topologia esquemática da rede externa do projeto Remesh

De acordo com a figura, os nós 4 e 1 são os que, na maior parte do tempo, estão a um salto do *gateway* (nó 7). Os demais nós (11, 13 e 14) estão geralmente a dois saltos. Na Figura 40, os nós estão sendo representados diretamente pelo terceiro byte do endereço IP (*ID* + 1)

4.3.1 Variação do ETX na rede externa

A Tabela 8 demonstra os valores de ETX médio, mínimo, máximo e o desvio padrão σ para os enlaces mais freqüentes (coluna L de *link*) entre os nós da rede externa (Figura 40). A informação foi coletada em um período de 24 horas. A medição apresentou seis enlaces com valores médios de ETX entre 1,3 e 1,7 e com baixo desvio padrão (enlaces L1, L2, L3, L8, L9 e L10). Apesar dos valores médios de ETX serem razoavelmente bons, o fato deles não apresentarem valores próximos e as freqüentes variações nas qualidades dos enlaces demonstradas por seus valores de desvio padrão, faz com que o número de troca de rotas torne-se mais freqüente, como será visto a seguir.

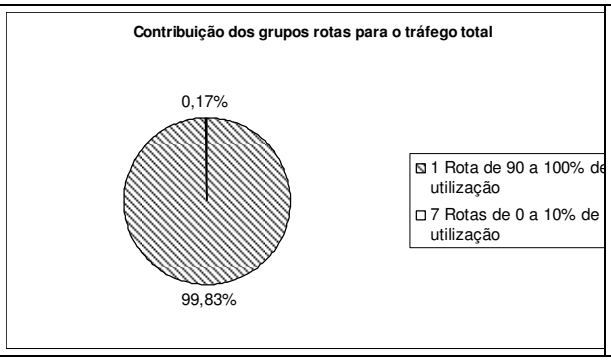
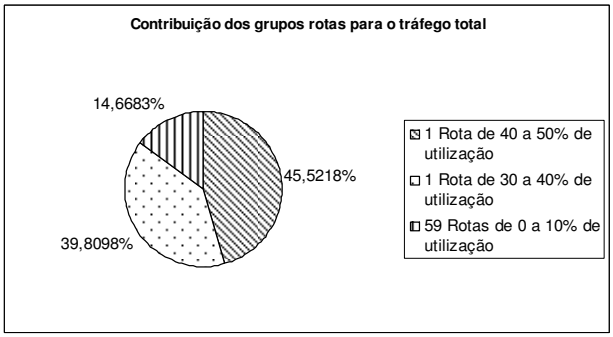
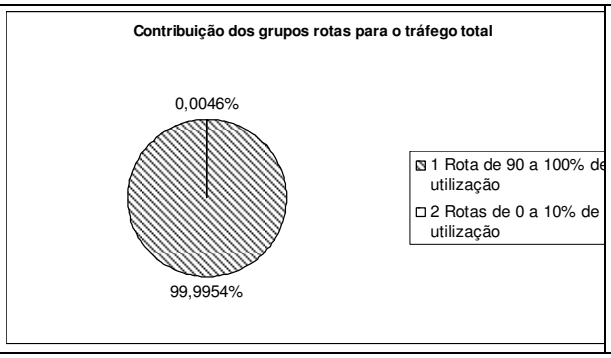
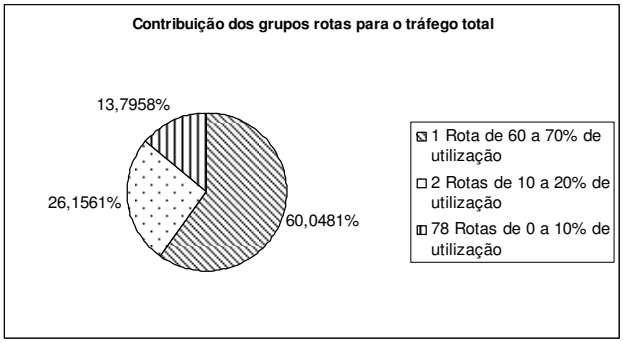
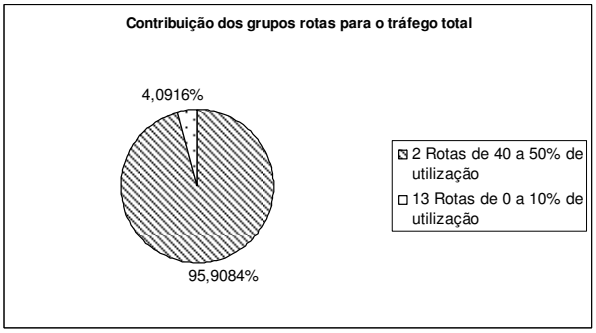
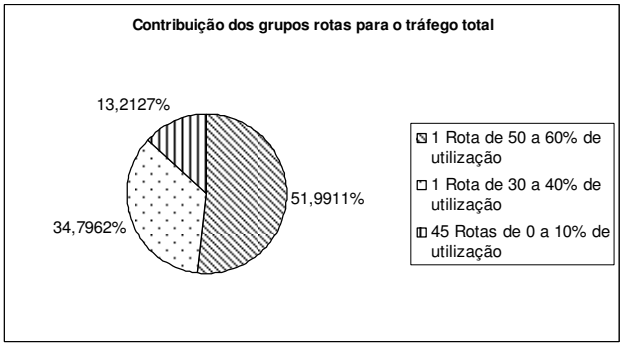
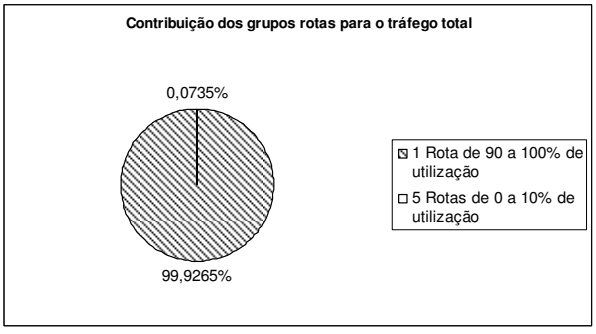
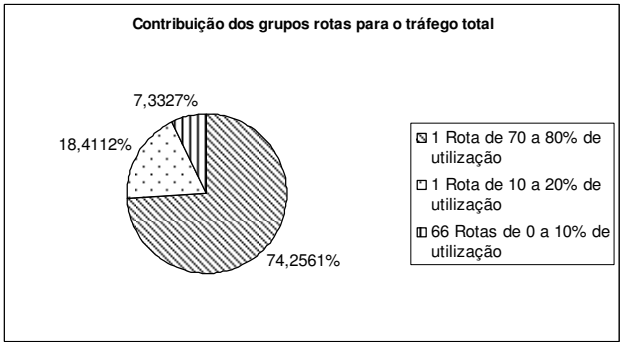
L	O	D	Méd	Mín	Max	σ
L1	7	11	1,55	1,00	12,75	0,59
L2	7	4	1,69	1,00	6,39	0,41
L3	7	1	1,41	1,00	4,72	0,31
L4	7	14	38,65	2,02	425	55,97
L5	14	1	6,70	1,00	106,25	8,92
L6	4	14	33,17	2,81	451,56	31,74
L7	4	1	13,88	1,32	71,3	13,51
L8	1	11	1,30	1,00	7,92	0,28
L9	4	11	1,70	1,05	13,62	0,50
L10	4	13	1,50	1,00	3,58	0,28

Tabela 8: Variação do ETX na rede externa

4.3.2 Estabilidade de rotas na rede externa

Para a verificação da estabilidade de rotas, foi realizado um teste de ping, onde os pacotes eram disparados a partir do *gateway* (nó 7 na Figura 40), durante um período de 24 horas, resultando em um total de 86.400 pacotes de ping, para os outros nós da rede e para cada um dos dois protocolos (OLSR-ETX e OLSR-ML). O objetivo do teste era a verificação da variação das rotas em relação ao *gateway*.

Utilizando a opção –R da ferramenta ping no Linux, foi possível evidenciar as rotas trafegadas. As rotas obtidas foram separadas em grupos de acordo com o percentual de utilização (número de pacotes trafegados). Porém, mais de uma rota na mesma faixa percentual de utilização foram encontradas. Portanto, para uma melhor compreensão dos resultados, na Tabela 9 uma série de gráficos em forma de pizza é apresentada para cada nó (com exceção do *gateway*) e para cada protocolo. Os gráficos representam o quanto cada grupo de rotas contribuiu para o tráfego total.

OLSR-ETX	OLSR-ML
Nó 1	
	
Nó 4	
	
Nó 11	
	
Nó 13	
	
Nó 14	

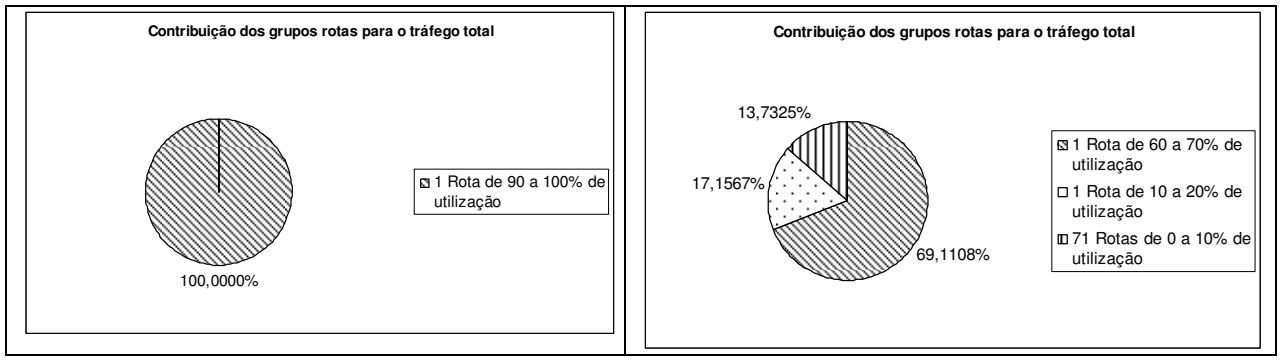


Tabela 9: Variação de rotas na rede externa por protocolo e nó

Cada rota é diferenciada pelo caminho de ida e de volta, isto explica o alto número de diferentes rotas encontradas principalmente para o protocolo OLSR-ML. Diferentemente dos resultados obtidos na rede interna, em termos de estabilidades de rotas, o OLSR-ETX obteve resultados melhores do que OLSR-ML para todos os nós.

Considerando o OLSR-ML, o maior número de rotas diferentes ficou concentrado dentro da faixa de 0 a 10% de utilização para todos os nós. Por exemplo, o nó 1 apresentou 59 diferentes rotas nesta faixa, ocupando 14,6683% do tráfego total. O maior número de diferentes rotas é observado no nó 4. Foram observadas 81 rotas diferentes, com apenas uma ocupando 60,0481% e duas ocupando 26,1561% do tráfego total. Este mesmo nó apresentou apenas 1 rota para praticamente 100% do tráfego total com o OLSR-ETX. Esta disparidade pode ser explicada utilizando a Figura 41.

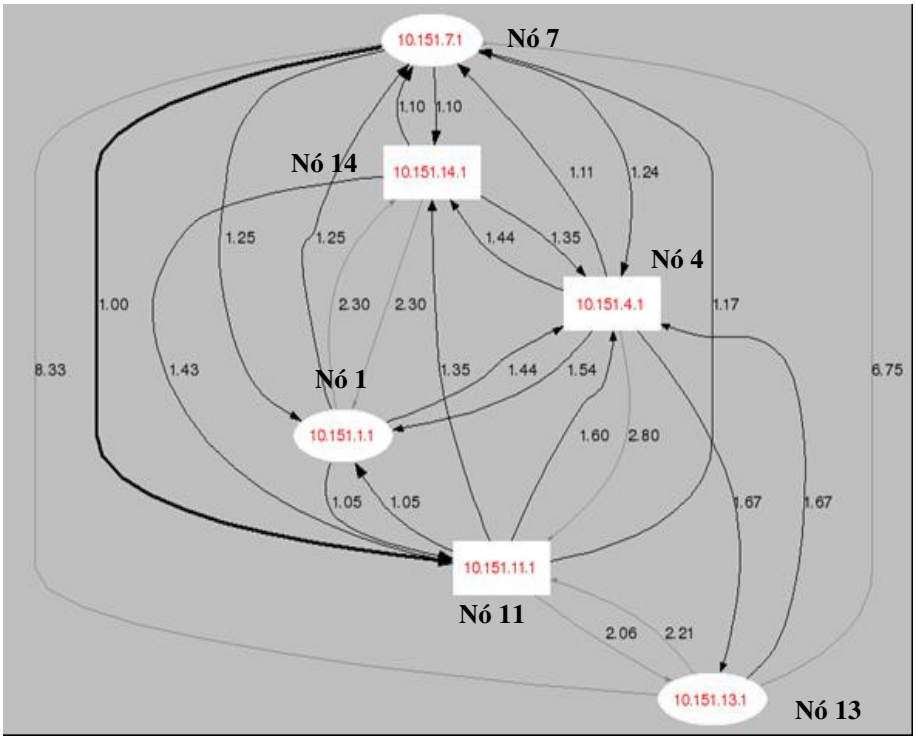


Figura 41: “Retrato” dos enlaces da rede externa representados por seus valores de ETX

Comparando os valores de ETX para os enlaces da rede externa (Figura 41) com os valores dos enlaces da rede interna (Figura 35), podemos distinguir dois tipos de situações. Na rede interna, cada nó possui enlaces de alta qualidade com seus nós adjacentes e muito ruins com os que estão a mais de um salto. Tal situação pode ser considerada como uma topologia de “enlaces bem definidos”. Nesta situação, o OLSR-ML apresentou um resultado muito superior ao OLSR-ETX (subseção **4.2.2**).

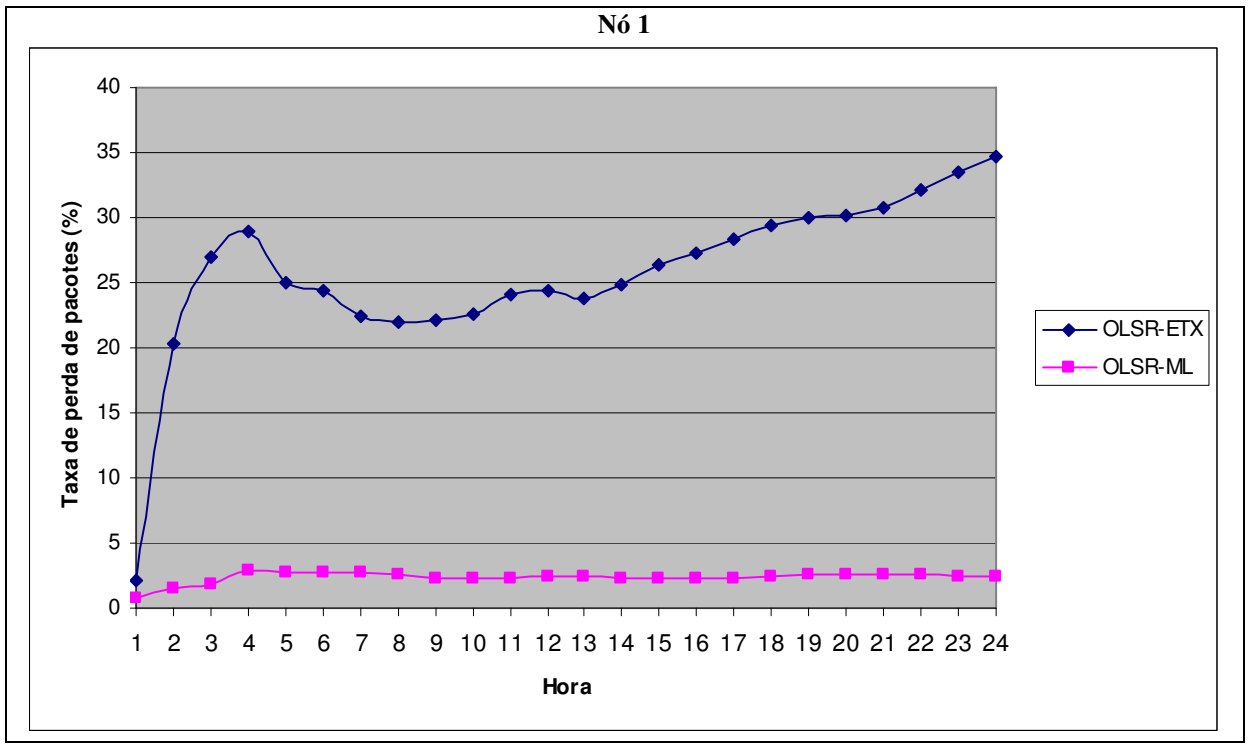
Na rede externa, praticamente todos os nós possuem enlaces diretos para os outros nós da rede, adjacentes ou não, com valores de ETX médios bem próximos e baixo desvio padrão (Tabela 7). Podemos definir esta situação como uma topologia de enlaces não bem definidos. Nesta situação o OLSR-ETX apresentou um resultado melhor em termos de estabilidade de rotas.

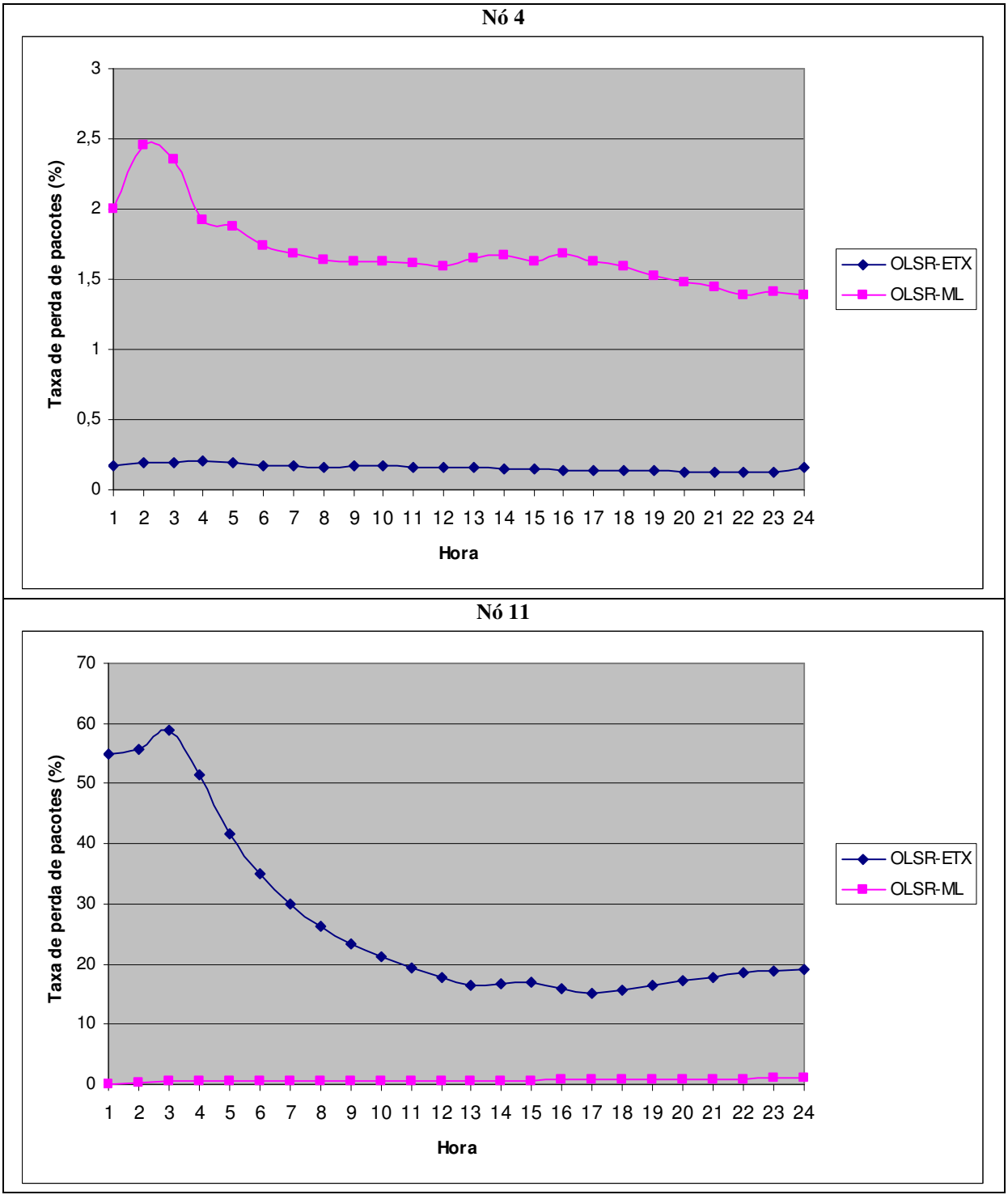
No protocolo OLSR-ETX, cada novo nó que é adicionado em uma rota composta de múltiplos saltos significa um incremento de no mínimo 1 no valor do ETX total da rota. Em contrapartida, o OLSR-ML adiciona um novo nó em uma rota de múltiplos saltos sem nenhum incremento no valor do ETX total, a não ser as perdas inerentes ao enlace adicionado. No melhor caso, um enlace com valor de ETX igual a 1, não haverá nenhum incremento no valor do ETX total da rota. Como explicado anteriormente, o OLSR-ML tende a escolher

rotas mais longas e com menos perdas. Porém, em uma situação de enlaces não bem definidos, a taxa de inclusão e exclusão de novos nós aumenta, conseqüentemente aumentando a instabilidade de rotas.

4.3.3 Taxa de perda de pacotes na rede externa

A informação da taxa de perdas de pacotes foi retirada da mesma medição utilizada no item anterior: disparo de pings a partir do *gateway*, durante 24 horas para cada nó utilizando ambos protocolos. Na Tabela 10, um gráfico com a variação da taxa de perda de pacotes em intervalos de horas.é apresentado para cada nó.




Nó 4
Taxa de perda de pacotes (%)
3
2,5
2
1,5
1
0,5
0
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Hora
OLSR-ETX
OLSR-ML
Nó 11
Taxa de perda de pacotes (%)
70
60
50
40
30
20
10
0
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Hora
OLSR-ETX
OLSR-ML

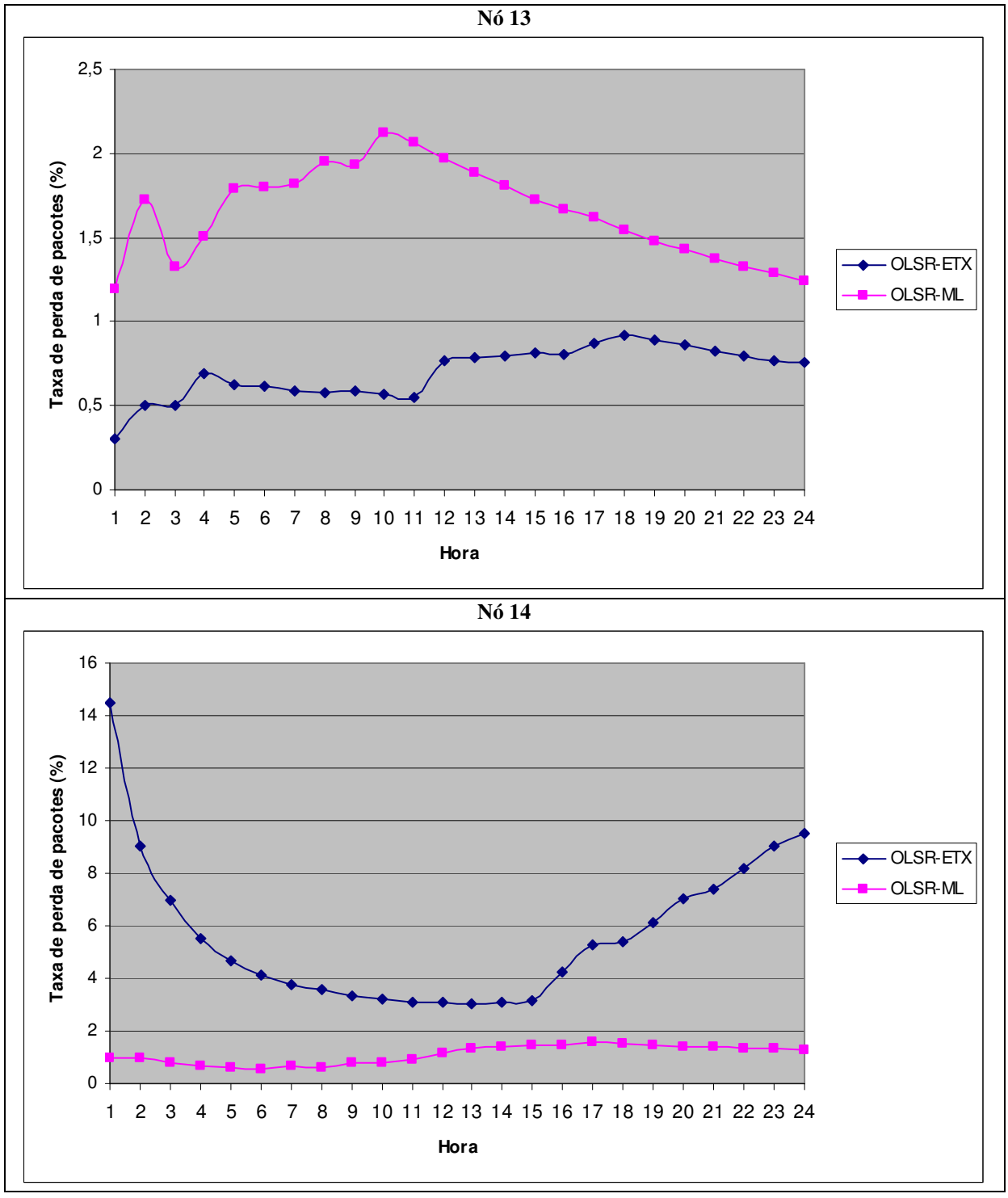


Tabela 10: Comparação da taxa de perda de pacotes na rede externa entre ambos os protocolos para cada nó

Sendo o OLSR um protocolo distribuído, variações nas rotas estabelecidas requerem tempo para que os nós se sincronizem suas tabelas de roteamento. Durante este período de tempo, pacotes que estiverem em tráfego são perdidos. Contudo, observando os gráficos da

Tabela 10, os nós 1, 11 e 14 obtiveram uma taxa de perda de pacotes menor para o OLSR-ML, ao contrário dos nós 4 e 13.

Esperava-se que para todos os nós, o OLSR-ETX apresentasse um resultado melhor devido à alta instabilidade das rotas. Contudo, mesmo com as perdas devido às mudanças de rotas, o fato do OLSR-ML escolher caminhos com menos perdas continua a proporcionar, pelo menos para alguns nós, uma taxa de perda de pacotes menor. Ainda, deve-se observar que para os casos onde o OLSR-ETX obteve um melhor desempenho, a diferença máxima na taxa de perdas de pacotes foi de 2% tanto para o nó 4 como para o nó 13. Nos casos onde o OLSR-ML obteve melhor desempenho, as diferenças máximas nas taxas de perda de pacotes entre os protocolos foram maiores: nó 1 com 31%, nó 11 com 60% e nó 14 com 13%. Em nenhum nó, o OLSR-ML apresentou taxa de perda de pacotes maior do que 2,5%, enquanto que o OLSR-ETX alcançou um valor próximo a 60% de taxa de perda de pacotes para o nó 11.

4.3.4 Atraso e Jitter da rede externa

O mesmo teste da seção anterior permitiu a obtenção do atraso e do jitter da rede externa através do RTT de cada pacote de ping. O jitter foi retirado pela subtração do RTT do pacote de ping no instante de amostragem com o valor do RTT do pacote imediatamente anterior. Os valores foram separados em intervalos de hora para melhor compreensão.

Na Figura 42, pode-se comparar os valores dos atrasos médios e na Tabela 11 exibimos os gráficos comparativos para o atraso e o jitter entre os dois protocolos e para cada nó.

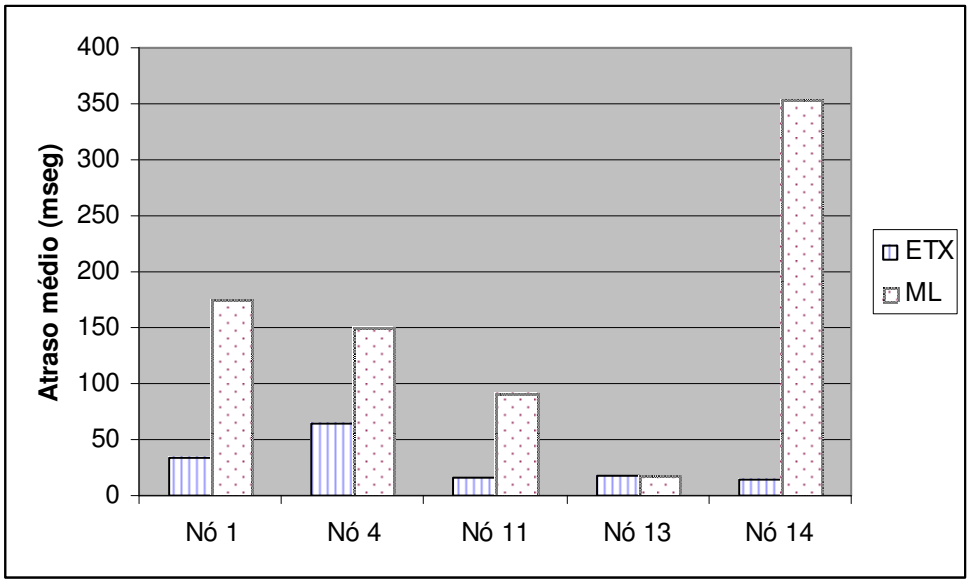
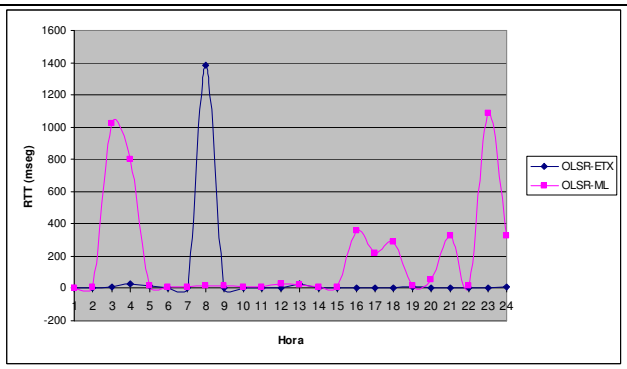
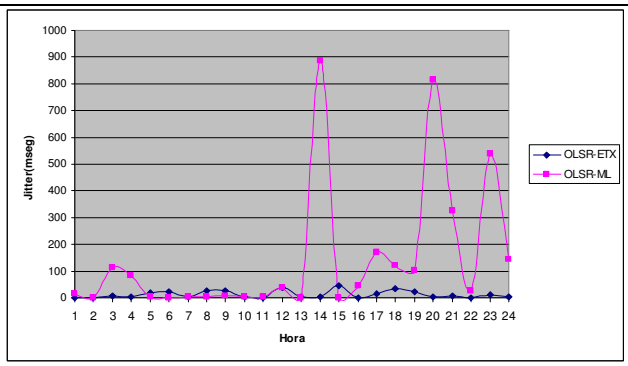
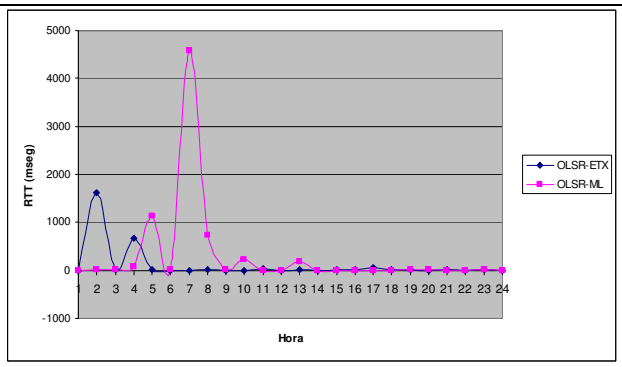
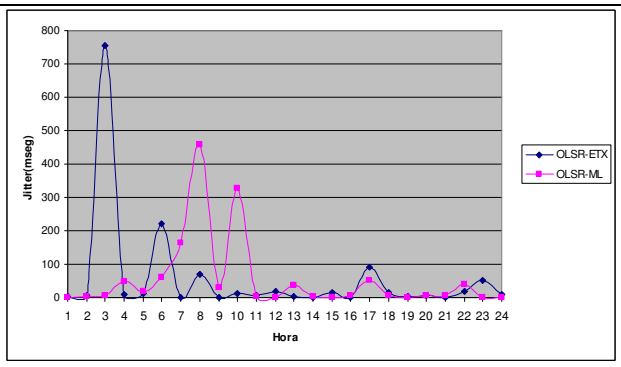


Figura 42: Atraso médio para cada nó e protocolo

Atraso	Jitter
Nó 1	
	
Nó 4	
	
Nó 11	

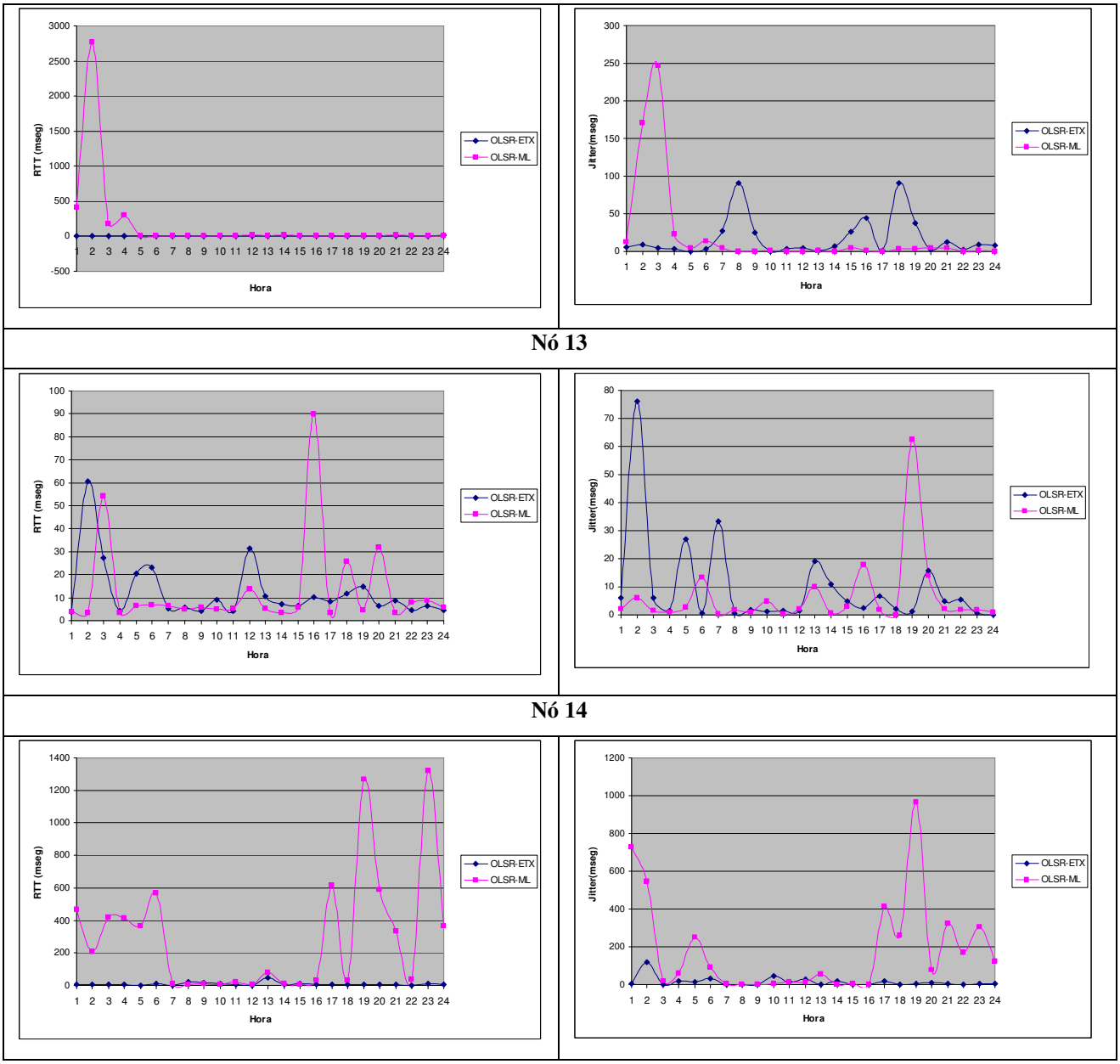


Tabela 11: Comparação do atraso e do jitter na rede externa entre ambos os protocolos para cada nó

Analisando a Figura 42, percebe-se que o nó 13 foi o único que teve performance semelhante para ambos os protocolos (em torno de 18 milisegundos). Em todos os outros nós, o OLSR-ML obteve um valor de atraso médio maior do que o OLSR-ETX, alcançando 352,858 contra 13,775 milisegundos no nó 14. Como a rede apresentou uma alta variação de rotas com o OLSR-ML, o alto valor no atraso médio reflete o tempo que é gasto em *loops* que surgem durante a sincronização dos nós. Com o OLSR-ETX, as rotas se mantém mais estáveis, mesmo que sejam para enlaces que possuam maior taxa de perda de pacotes. Por isto as perdas são maiores (como demonstrado na subseção anterior), mas o atraso dos pacotes bem sucedidos torna-se, em média, menor.

Os gráficos presentes na Tabela 11 demonstram que a rede apresentou uma variação maior ao longo do tempo para os valores dos atrasos e do jitter com o OLSR-ML para todos os nós. Os momentos de pico refletem os instantes de loop na rede

Quanto ao jitter, os nós 4, 11 e 13 apresentaram variações parecidas para ambos os protocolos ao longo do tempo. Entretanto, para os nós 1 e 14 o OLSR-ETX apresentou valores praticamente constantes para o jitter contra picos em torno de 900 milisegundos para o OLSR-ML.

4.3.5 Vazão da rede externa

O teste realizado para a obtenção dos valores de vazão na rede externa consistiu na execução de um *script* em três horas distintas do dia (04, 11 e 18), ao longo de 12 dias, separando 6 dias para cada protocolo. O teste consistiu na execução da ferramenta *iperf* durante 10 minutos, a partir do *gateway*, para cada outro nó da rede, após a retirada dos usuários ativos e da permissão de acesso. Os fluxos gerados foram bidirecionais simultâneos, usando o TCP como protocolo de transporte. Após a finalização do teste para o último nó, os usuários reaviam suas permissões de acesso.

A cada execução do *iperf*, um valor médio era obtido para cada situação (protocolo, hora do dia e nó). Na Figura 43 estão as médias totais dos valores obtidos. O termo “ida” se refere aos fluxos gerados do *gateway* em direção ao nó (*upstream*) *e* o termo “volta” para a situação oposta (*downstream*).

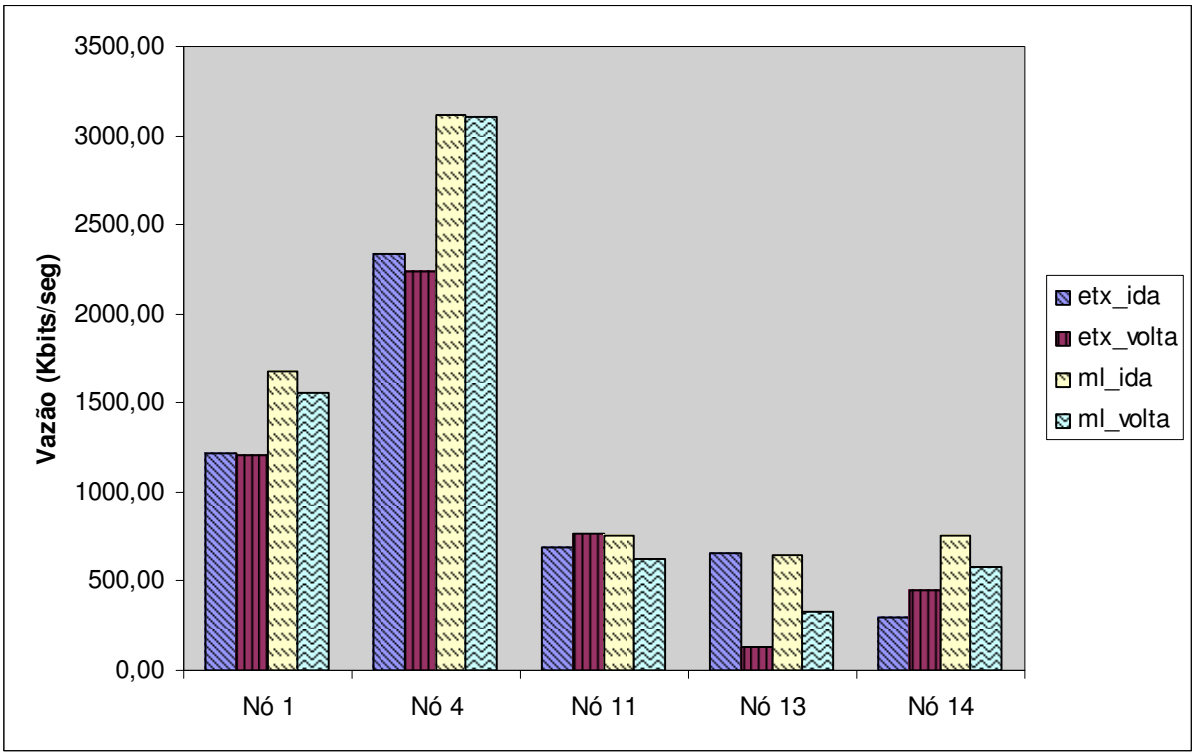


Figura 43: Vazão na rede externa para cada nó e protocolo

Como pode ser visto, o OLSR-ML obteve melhor desempenho em comparação com o OLSR-ETX para os nós 1, 4, 13 e 14. Em ambos os protocolos, os nós mais distantes do *gateway* (11, 13 e 14) apresentam uma queda considerável na vazão por estarem, geralmente, a dois saltos de distância enquanto que os nós 1 e 4 são nós diretos.

Nó 11 apresentou um resultado próximo para ambos os protocolos. Neste nó o OLSR-ETX obteve vazão média de 690 kbps para *upstream* (“ida” no gráfico) e 762 kbps para *downstream* (“volta” no gráfico), enquanto que o OLSR-ML obteve 761 kbps para *upstream* e 625 kbps para *downstream*.

No nó 4 a diferença entre os protocolos alcançou mais de 500 kbps em ambos os sentidos. Nó 13 teve um desempenho semelhante para *upstream* em ambos os protocolos (662 e 643 kbps para OLSR-ETX e OLSR-ML, respectivamente), porém uma diferença de 193 kbps para *downstream* a favor do OLSR-ML: 131 kbps para o OLSR-ETX e 324 kbps para o OLSR-ML. Estes últimos valores foram as menores taxas médias obtidas, demonstrando que o OLSR-ML não passou a marca de 300 kbps, fornecendo conexão à taxas satisfatórias.

4.4 CONCLUSÕES

Neste capítulo foi apresentado o protocolo de roteamento *ad hoc* OLSR de maneira um pouco mais detalhada. O principal objetivo foi demonstrar os mecanismos do seu funcionamento, bem como as dinâmicas de construção das rotas a partir da métrica utilizada. A partir de sua utilização na rede interna, a rede de testes, foi percebida a deficiência do protocolo e o porquê foi realizada a modificação que gerou o protocolo OLSR-ML. O OLSR-ML comprovou sua a eficácia através de testes comparativos na rede interna, com resultados bastante satisfatórios.

O OLSR-ML foi desenvolvido através de pequenas alterações no código fonte da implementação do OLSR original. A compilação para a arquitetura do roteador (MIPS) é realizada através dos utilitários disponibilizados pelo pacote do OpenWRT. Após a compilação, é gerado um novo binário. Sua instalação nos roteadores é realizada com a cópia do arquivo binário e dos módulos do sistema operacional que utiliza (os módulos não são alterados). O OLSR-ML foi projetado para permitir que que possa ser chaveado para o OLSR-ETX simplesmente alterando-se o parâmetro "LinkQualityLevel" no arquivo de configuração *olsrd.conf* (vide **ANEXO 2**). Entretanto, para que a configuração entre em vigor, é necessário reiniciar o protocolo.

Em seguida, quando os testes foram realizados na rede externa, a rede de produção, os resultados não apresentaram as mesmas tendências. Ambos os protocolos, OLSR-ETX e OLSR-ML, obtiveram resultados melhores em alguns aspectos e piores em outros. O OLSR-ETX apresentou melhor estabilidade de rotas e menor atraso e variação do jitter. Por outro lado, o OLSR-ML obteve melhor performance quanto à taxa de perda de pacotes e vazão.

A rede externa apresenta uma topologia mais complexa do que a rede interna, quanto às rotas a serem seguidas entre os nós e o *gateway*. Enquanto que a rede interna possui enlaces bem definidos, com valores de ETX bem diferenciados (por exemplo, 1 e 2 para dois possíveis enlaces de um caminho de mesma origem e fim) e com baixo desvio padrão, entre os nós e seus vizinhos diretos. Por outro lado, a rede externa apresenta enlaces com valores de ETX muito próximos entre praticamente todos os nós participantes. Esta situação é decorrente do fato da rede externa estar sujeita a um número maior de efeitos de propagação que afetam muito mais as condições da comunicação rádio. Além disso, na rede externa não existe situações ideais de localização dos nós. A instalação dos nós depende da existência de algum voluntário e da presença de condições mínimas para instalação (espaço físico, possibilidade de passagem ou lançamento dos cabos, etc).

Contudo, o objetivo de uma rede em malha sem fio é o seu crescimento não estruturado através da capacidade dos nós se auto-configurarem. Uma situação como a que foi apresentada na rede externa do projeto Remesh, possivelmente é um caso comum em outras redes em malha (instaladas em ambientes externos e urbanos). Os resultados dos testes demonstraram uma deficiência do OLSR-ML em lidar com topologias deste tipo. Entretando, como não houve resultados conclusivos para se eleger um dos dois protocolos como o melhor, pode-se concluir que existe uma deficiência na métrica utilizada. Como relatado em diversos trabalhos, (BICKET, *et al,* 2005; DRAVES *et al,* 2004 [a] e [b]; KOKSAL e BALAKRISHNAN, 2006; KOKSAL, JAMIESON, *et al*, 2006; RAMACHANDRAN *et al*, 2005) o ETX já pode ser considerada uma métrica ultrapassada, que não representa inteiramente a qualidade de um enlace por considerar apenas uma variável, o número esperado de retransmissões de nível 2.

Avaliando os resultados dos testes, conclui-se que o protocolo OLSR-ML é superior ao OLSR-ETX em topologias simplificadas, com poucas alterações de rotas preferenciais. Porém, em topologias mais complexas, torna-se necessária a implementação de outras métricas que representem, com maior precisão e menor tempo de atualização, a qualidade dos enlaces. Uma métrica que estime as qualidades de transmissão dos enlaces com maior diferenciação poderia diminuir o número de alterações de rotas em intervalos de tempo curtos. Essa estabilidade poderia não refletir as variações rápidas das condições de propagação, entretanto, diminuiria o número de troca de rotas e, possivelmente, a latência no tráfego dos pacotes. Neste sentido, uma solução simples seria a utilização de histerese, entretanto, seria necessária uma avaliação para a definição dos valores dos limiares de trocas de rotas.

No próximo capítulo a rede externa será avaliada quanto a sua utilização. Serão explicadas a técnica e a ferramenta utilizadas para a autenticação, os aplicativos desenvolvidos para o acompanhamento e gerência da rede, outras medições e estatísticas de utilização. As ferramentas e os resultados das medições serão utilizados para a validação do protótipo como um produto funcional do ponto de vista do usuário final.

5 GERÊNCIA E UTILIZAÇÃO DA REDE

Este capítulo tratará com maior ênfase da rede externa. Ela é a “rede de produção”, onde está localizado o maior número de usuários. A rede externa é destinada principalmente para fins acadêmicos, contudo, fornecer o serviço de conexão com a maior disponibilidade e qualidade possíveis constitui um estudo de caso de extremo valor. Os usuários participantes do projeto são alunos e funcionários da UFF que geram tráfego real. A rede provê o acesso dos usuários à rede da UFF, que os conecta à Internet. Por este motivo, não foi possível realizar testes com tráfegos de características corporativas.

Neste capítulo serão abordados os aspectos referentes à interação dos usuários com a rede e a qualidade com que eles estão obtendo acesso à Internet. Iniciaremos com a explicação do processo de autenticação. Em seguida, serão abordadas as ferramentas que foram geradas para a gerência e o acompanhamento do uso da rede. Finalmente, através de medições, demonstraremos parâmetros técnicos da qualidade da rede, como perda de pacotes, atraso, jitter e vazão.

5.1 PROCESSO DE AUTENTICAÇÃO DOS USUÁRIOS

O projeto Remesh teve como um dos seus objetivos o fornecimento de acesso à Internet em banda larga a alunos e funcionários da UFF, fora das dependências da universidade. A UFF fornece acesso à Internet para seus funcionários e alunos gratuitamente, através de sua estrutura cabeada interna. Os professores possuem acesso em suas salas e os alunos desfrutam de diversos laboratórios. Entretanto, este acesso possui um custo que é

coberto pela Universidade e, em vista disso, torna-se imprescindível que este acesso seja exclusivo apenas àqueles que possuam este direito.

Levar o projeto para fora das dependências físicas do campus implica na necessidade de que este acesso seja controlado. Um outro problema está na questão de uma política adotada pelo projeto. Com o objetivo de alcançar um número crescente de voluntários que possibilitem uma quantidade maior de locais para a instalação de novos nós, adotou-se uma política de usar a rede sem fio sem nenhum tipo de criptografia (WEP, WPA, WPA2, etc; STALLINGS, 2002). Desta forma, à medida que novos nós eram adicionados, indivíduos que dispusessem de interfaces de conexão padrão 802.11 e morassem nas redondezas dos nós, poderiam se associar e experimentar a qualidade do acesso. O usuário que acessa a rede sem fio, além de divulgar o projeto, torna-se um voluntário em potencial para a instalação do nó em seu prédio, ou de sua residência, por desejar obter o acesso também pela estrutura cabeada (por exemplo, para se conectar à Internet através de um desktop sem interface sem fio). O surgimento de novas localidades para a instalação de novos nós propicia o conseqüente crescimento da rede externa.

Obviamente, não é permitido que o acesso da universidade seja oferecido indiscriminadamente a todas as pessoas que morem nas proximidades dos nós externos. Para manter a política de acesso sem "ferir" as regulamentações internas da UFF, adotou-se a técnica de *Captive Portal*. Esta técnica consiste na inserção de um *firewall* entre o usuário e o *gateway* de acesso. Toda vez que um pacote é encaminhado para o *gateway*, ele passa pela barreira. Um usuário não autenticado terá o seu pacote bloqueado pelo *firewall*.

Para que os pacotes do usuário possam fluir livremente até o *gateway*, ele deverá executar um *browser* (aplicativo de acesso a páginas e serviços da Internet) e fazer uma requisição a uma URL (*Universal Resource Locator*; PETERSON e DAVIE, 1999) qualquer. O pacote da requisição será bloqueado no *gateway* que redireciona o cliente ao servidor de autenticação. Neste momento o usuário visualiza a página de entrada que contém as informações dos requisitos necessários para que o acesso seja permitido (Figura 44). Ao mesmo tempo, são encaminhados o endereço IP e o MAC ("*Media Access Control"*, endereço físico da interface de rede) do usuário que está fazendo a requisição ao servidor de autenticação.

Figura 44: Página de entrada para o acesso à rede do projeto Remesh

O servidor de autenticação é uma estação independente, localizada na mesma rede do *gateway* da rede externa. Este servidor é encarregado de manter um banco de dados de todos os clientes cadastrados. Assim que o usuário chega à página inicial do servidor de autenticação, ele deverá entrar com um *login* e senha autorizados. O servidor liberará ou não o acesso deste cliente encaminhando uma mensagem ao *gateway* de acesso. Esta mensagem irá conter a informação para abrir as portas do *firewall* (PETERSON e DAVIE, 1999) para o determinado endereço IP e MAC. Com o *firewall* do *gateway* liberado, o cliente pode navegar sem interrupções em seu acesso. Em caso de inatividade por mais de duas horas, o servidor envia uma mensagem para o *gateway* retirando a permissão do usuário.

Além da funcionalidade de segurança, o módulo de autenticação pode ainda armazenar dados sobre o acesso do determinado cliente, o que o torna uma ferramenta de administração dos usuários e do tráfego da rede.

Atualmente, existem disponíveis diversas soluções para implantação de um esquema de *captive portal*: *NoCatAuth*, *MonoWall*, etc. Uma lista mais completa de ferramentas de *captive portal* pode ser encontrada na página web da PERSONAL TELCO WIKI (2007). Na rede do projeto Remesh optou-se por utilizar o *Wifidog* (WIFIDOG, 2006) por ser um software aberto (licença GPL – “General Public License") e de fácil customização. Ele é dividido em dois módulos: um binário, escrito em C (JAMSA e KLANDER, 1998) e presente no *gateway* e nos nós da rede externa, que é inicializado durante o *boot* de cada nó; e o outro

que consiste em uma página dinâmica, escrita em PHP[13], presente no servidor de autenticação. O funcionamento do *wifidog* é ilustrado a seguir, nas Figura 45, 46 e 47.

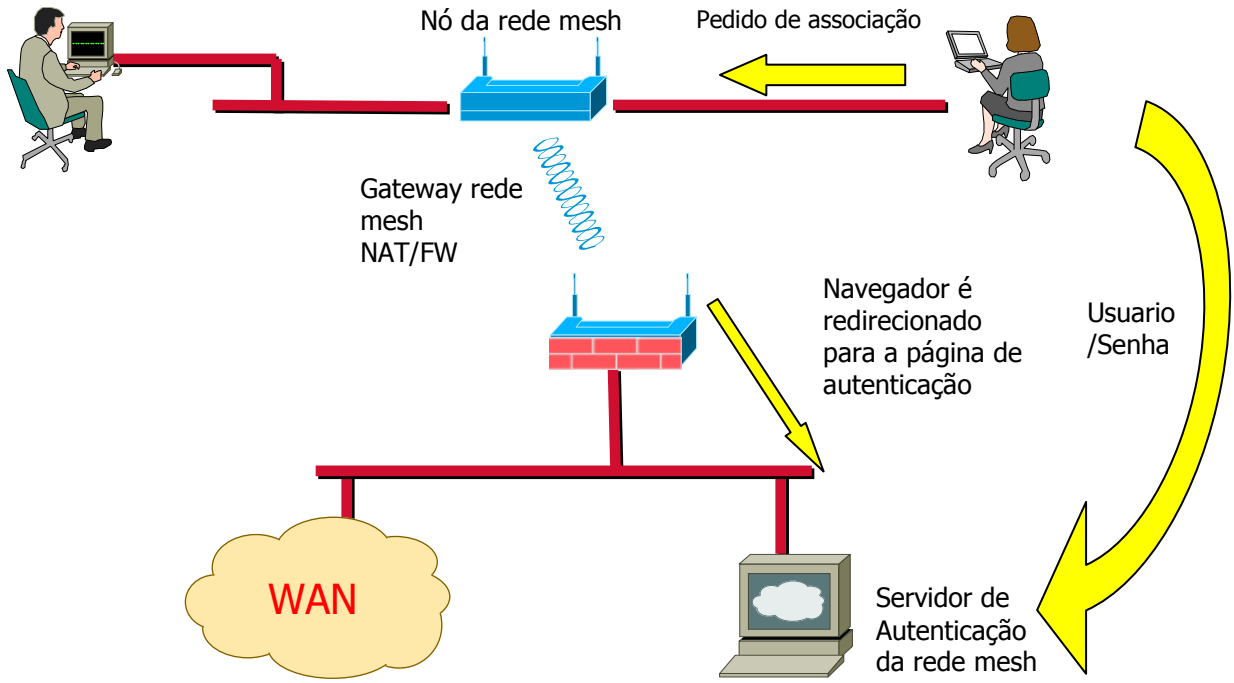


Figura 45: *Wifidog* – cliente inicia uma conexão

[13] PHP é um acrônimo recursivo para *Hypertext Preprocessor*. É uma linguagem de programação interpretada, livre e amplamente utilizada para a criação de páginas dinâmicas na *web*.

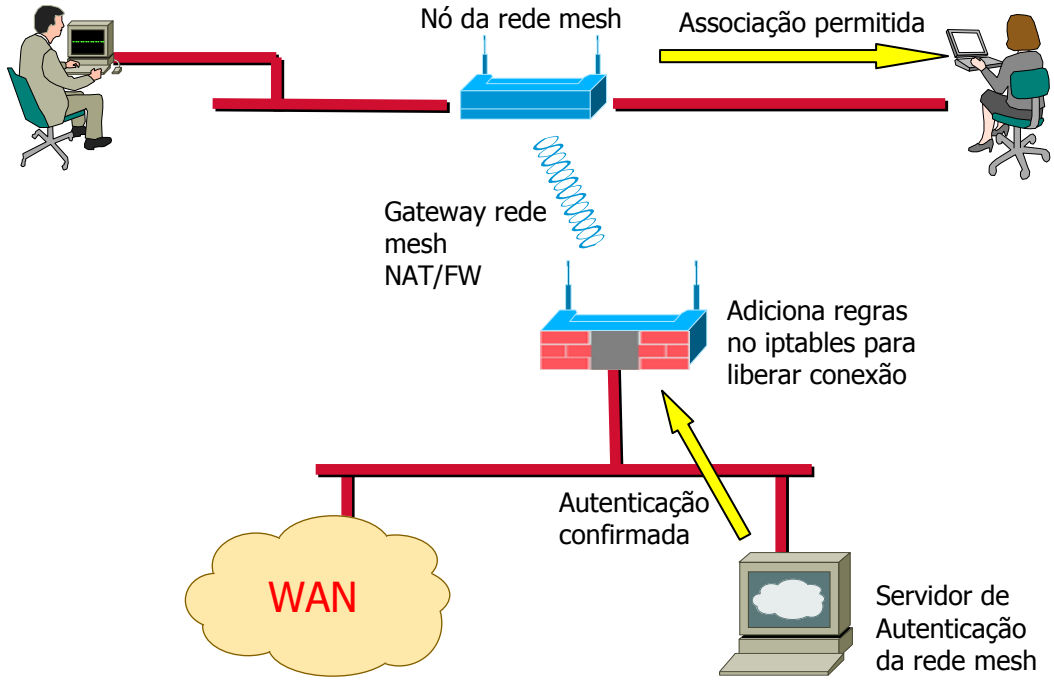


Figura 46: *Wifidog* - Processo de autenticação e liberação

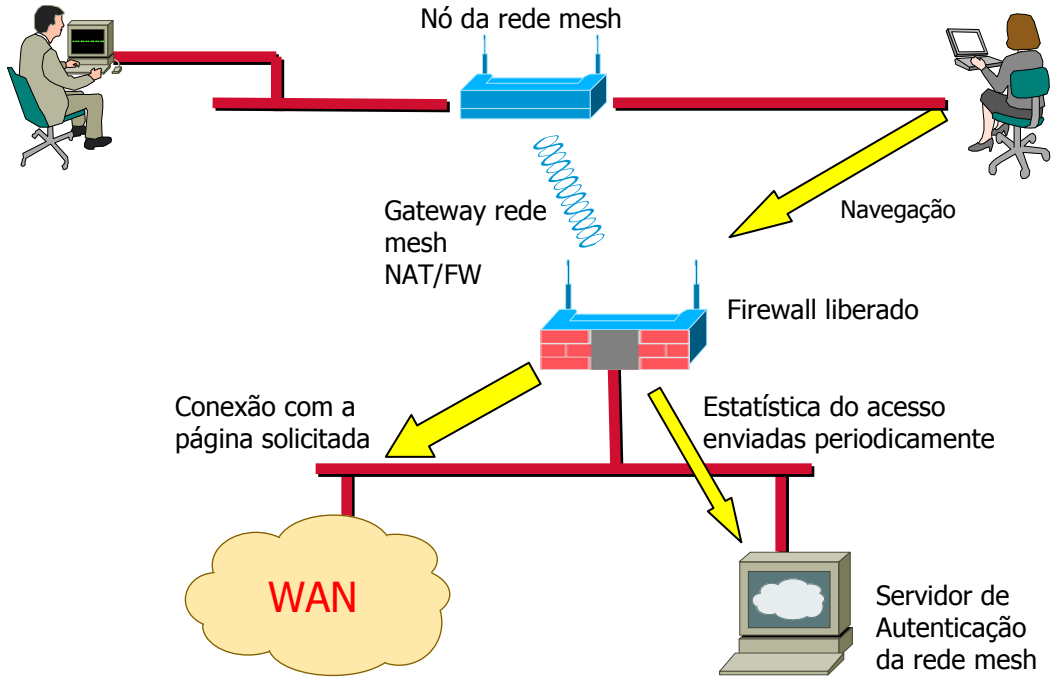


Figura 47: *Wifidog* - cliente autenticado e navegação liberada

Na Figura 45 pode ser visto o início do processo. Um cliente recebe o endereço por DHCP. Neste momento, qualquer outro serviço diferente do acesso http (*Hypertext Transport Protocol*; PETERSON e DAVIE, 1999) ao servidor de autenticação está bloqueado. Assim que o usuário executa um *browser* e tenta navegar para qualquer URL, ele será direcionado ao servidor de autenticação. Assim que é autenticado (Figura 46), o servidor de autenticação envia ao *gateway* a informação de que aquele endereço IP e MAC possui acesso a todas as portas. O usuário recebe a notificação e pode navegar diretamente na Internet sem ser bloqueado (Figura 47). Ao longo da conexão, o módulo binário do *wifidog* envia dados do acesso para que estatísticas do uso da rede possam ser geradas. Esse envio de informação é transparente para o usuário.

No protótipo desenvolvido, era necessário conseguir autenticar não somente os usuários que estão ligados à rede por fio (voluntários que moram em prédios que possuem nós instalados), mas também possibilitar a autenticação dos clientes que se ligam à rede sem fio. O *wifidog* autentica apenas uma interface de entrada para uma interface de saída, ou seja, se o sistema está autenticando clientes que se ligam ao roteador pela interface *Ethernet*, não será possível autenticar os que se conectam pela interface sem fio. Para resolver isto, foi proposta uma arquitetura particular ao projeto.

Primeiramente devemos dividir os nós da rede entre nós clientes e o nó *gateway*. Os nós clientes são aqueles que serão instalados nos apartamentos possibilitando a ligação por fio dos computadores dos usuários através das portas *Ethernet* do roteador. O nó *gateway* é o que encaminha todo o tráfego da rede mesh para a Internet, ou seja, é o que deve ter a sua porta *Ethernet* ligada à WAN (*Wide Area Network*), fornecida pela estrutura da universidade. Nele não ligamos computadores clientes nas portas *Ethernet*, não exigindo, portanto, a realização de autenticação para esta interface. Desta forma, pode-se eleger o *gateway* como o nó que fará a autenticação dos clientes sem fio enquanto que os outros nós farão a autenticação dos clientes por fio.

O processo é feito da seguinte maneira: cada nó cliente possui uma instalação do módulo binário original do *wifidog*, configurado para autenticar a porta de entrada *Ethernet* para a porta de saída sem fio; o nó *gateway* possui uma versão alterada do módulo binário do *wifidog* configurado para autenticar a interface de entrada sem fio para a interface de saída *Ethernet* WAN. A alteração do módulo não filtra os clientes pelo MAC de origem, pois um cliente sem fio que se autentica em um nó cliente (não *gateway*) da rede, não terá o seu MAC estampado no pacote roteado. Além disso, o nó *gateway* terá que ter regras específicas para

não barrar os pacotes provenientes de clientes da rede com fio que já foram autenticados nos seus nós de origem. A Figura 48 representa esquematicamente a arquitetura.

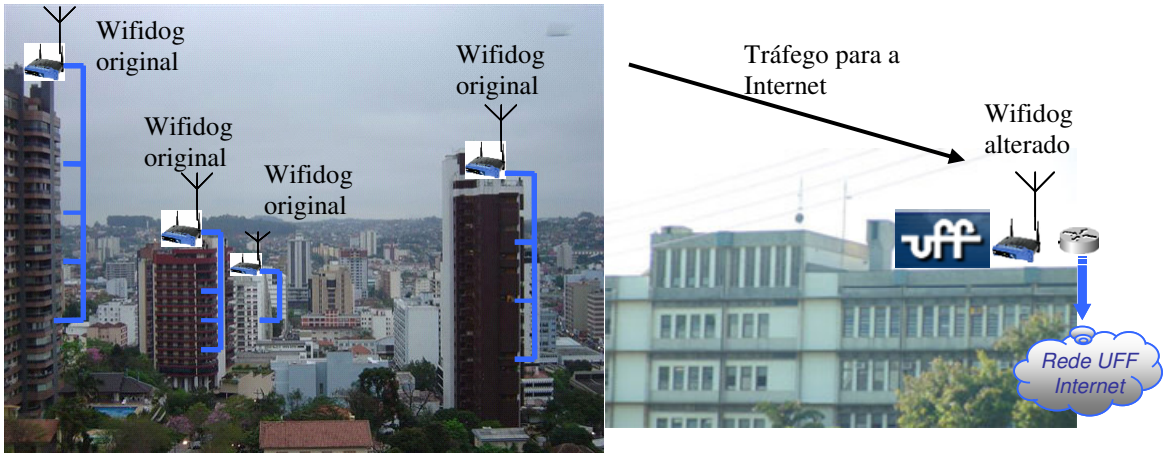


Figura 48: Esquema da instalação do wifidog na rede Mesh da UFF

Para um cliente sem fio, o esquema representado na Figura 45 é um pouco diferente. Ao pedir um IP para um nó próximo por DHCP, ele estará habilitado a trafegar dentro da rede externa do projeto, ou seja, ele pode ter acesso a qualquer máquina da rede, pois não foi necessária qualquer autenticação ou chave para isto. Contudo, ao sair da rede mesh para a Internet (com exceção ao acesso do serviço de DNS – *Domain Name System;* PETERSON e DAVIE, 1999), ele deverá passar pelo *gateway*. Neste momento ele será encaminhado para o servidor de autenticação conforme a Figura 49.

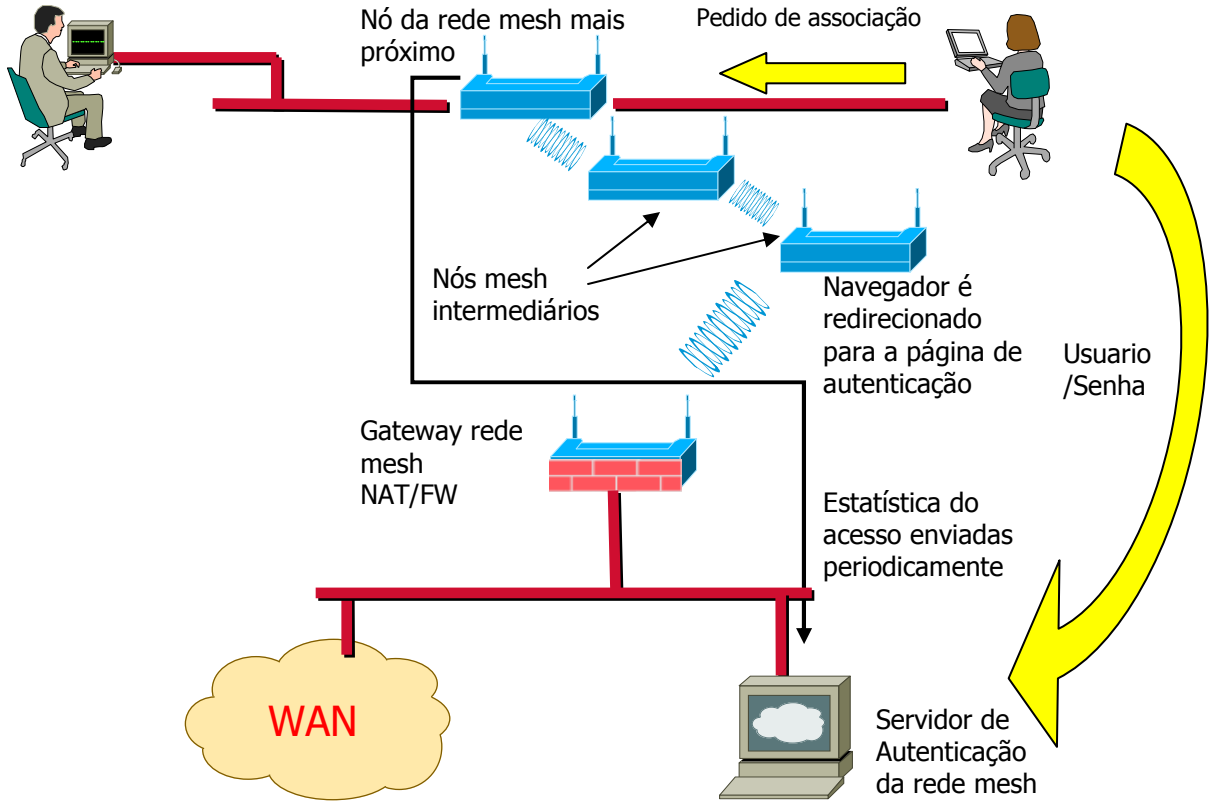


Figura 49: Wifidog - Autenticação de um cliente sem fio

O módulo binário instalado nos nós da rede mesh consiste em:

- Binário executável: /usr/bin/wifidog
- Scripts de inicialização: /etc/init.d/S65wifidog e /usr/bin/wifidog-init
- Arquivo de configuração: /etc/wifidog.conf onde a interface de entrada é a *Ethernet* LAN e a de saída é a sem fio
- Bibliotecas necessárias: /lib/libpthread.so.0; /usr/lib/libhttpd.so.0.0.0; /usr/lib/stdc++.so.6.

O módulo binário instalado no nó *gateway* da rede consistem em:

- Binário executável alterado: /usr/bin/wifidog
- Scripts de inicialização: /etc/init.d/S65wifidog e /usr/bin/wifidog-init; o primeiro é alterado e o segundo é o original que vem no pacote do *wifidog*
- Arquivo de configuração: /etc/wifidog.conf onde a interface de entrada é a sem fio e a de saída é a *Ethernet* WAN

- Bibliotecas necessárias (iguais): /lib/libpthread.so.0; /usr/lib/libhttpd.so.0.0.0; /usr/lib/stdc++.so.6.
- Arquivo /etc/wifidog_extra; este arquivo é executado pelo S65wifidog e escreve nas tabelas do *firewall* (*iptables*) as devidas permissões para que os clientes com fio não sejam bloqueados. Os clientes com fio são diferenciados facilmente pela sub-rede que pertencem (10.152.0.0 para clientes com fio e 10.151.0.0 para a sub-rede sem fio).
- Arquivo /etc/init.d/S45firewall devidamente configurado. Este arquivo adiciona regras extras no *firewall* do *gateway* para que dados necessários às ferramentas de gerência da rede não sejam bloqueadas. Porém as ferramentas de gerência têm acesso somente às portas requeridas e somente para a máquina que as executa.

O módulo PHP deverá ser instalado em uma máquina comum com sistema operacional Linux. Para o seu funcionamento ele depende dos seguintes itens:

- PHP versão 5.xx
- Banco de dados "Postgres"
- Servidor Apache, versão 2.xx , de preferência com SSL (*Secure Socketse Layer)* para criptografar a senha e *login* através de https (*secure http*).
- Módulo php_xml para suporte a dialetos XML (RSS)
- Módulo php_gettext para suporte a múltiplas línguas
- Módulo php_mbstring para suporte a diferentes tipos de caracteres
- Módulo php_mcrypt, php_xml e php_mhash para suporte a servidor RADIUS[14] (opcional)
- Módulo php_radius para utilização de RADIUS (opcional)

[14] RADIUS – "Remote Authentication Dial In User Service". O servidor RADIUS, definido pela RFC 2865, é usado por provedores de serviços de Internet (ISP — *Internet Service Providers)* para executar tarefas de Autenticação, Autorização e Contabilidade. Quando utilizado em redes sem fio, opera em conjunto com o ponto de acesso (PA), que é configurado como um "cliente" RADIUS. Nesse caso, cada pedido que passa pelo PA, é repassado ao servidor RADIUS. Quando o usuário solicita conexão ao PA, ele deve informar um *login* e senha para efetuar a autenticação. Depois de receber o nome do usuário e a senha, o AP cria um pacote com essas informações. Este pacote é enviado para o servidor RADIUS criptografado. O servidor RADIUS recebe a requisição e valida o nome do usuário e senha. Se o nome e senha conferirem, o RADIUS devolve ao PA uma autorização que inclui informações da rede do cliente e serviços que ele está autorizado a utilizar (STALLINGS, 2002).

- Módulo php_gd, php_png e php_jpg para construção dos gráficos (opcional)
- Conjunto das páginas fornecidas pelo módulo com as alterações realizadas pelo projeto
- Configuração das páginas para definição do banco de dados e da senha de administração.

O módulo do *wifidog* em PHP consiste em um conjunto de páginas dinâmicas que devem ser instaladas no servidor de autenticação. Elas não somente permitem a autenticação dos usuários, mas também a gerência dos mesmos e dos diversos nós instalados.

Uma vez instalado no servidor com todas as aplicações em funcionamento, os nós da rede devem ser cadastrados para que a gerência da rede possa diferenciar os usuários de acordo com os nós de acesso (Figura 50).

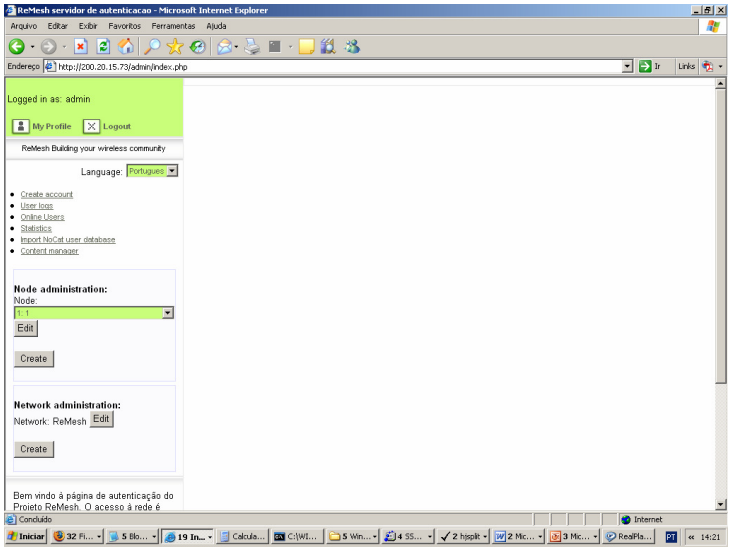


Figura 50: Página de gerência com as opções à esquerda

Ao se autenticar como administrador, dentre as opções disponíveis está a criação de nós. Cada nó da rede deverá ser cadastrado. O projeto utiliza como identificador o terceiro *byte* do endereço do nó, por exemplo, o nó 10.151.20.1 será identificado como "*ID* 20" (Figura 51). Esta identificação é importante, pois é o primeiro parâmetro a ser configurado no arquivo *wifidog.conf* do módulo binário que é executado dentro dos roteadores (Figura 52). Assim que o nó é criado, ele pode ser alterado na mesma página. O cadastro de usuários também é feito nesta página e as informações necessárias são o *login*, a senha e uma conta de email.

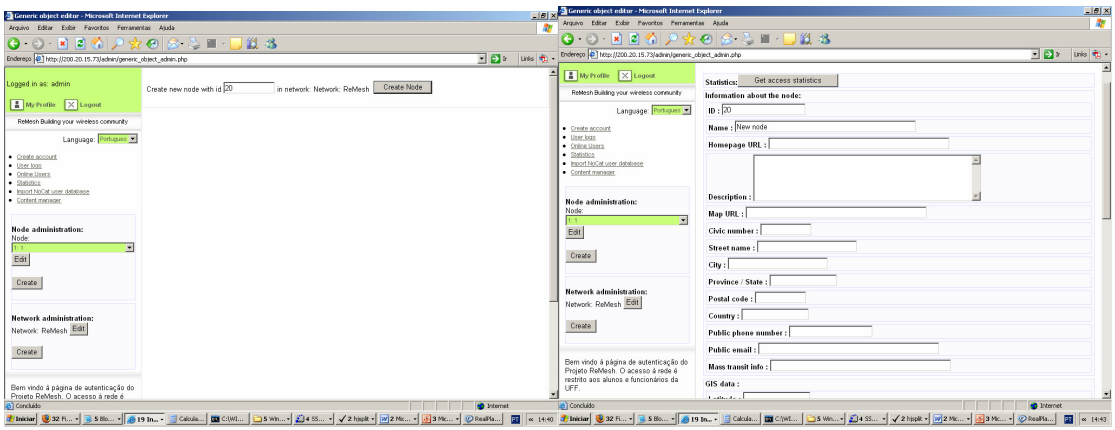


Figura 51: Wifidog - Criação de um novo nó

```
# WiFiDog Configuration file

# Parameter: GatewayID
# Default: default
# Optional but essential for monitoring purposes
#
# Set this to the template ID on the auth server
# this is used to give a customized login page to the clients
# If none is supplied, the default login page will be used.

GatewayID 20

# Parameter: ExternalInterface
# Default: NONE
# Optional
#
# Set this to the external interface.  Typically vlan1 for OpenWrt, and eth0 or ppp0 otherwise

ExternalInterface vlan1

# Parameter: GatewayInterface
# Default: NONE
# Mandatory
#
# Set this to the internal interface.    Typically br0 for OpenWrt, and eth1 otherwise

GatewayInterface eth1

# Parameter: GatewayAddress
# Default: Find it from GatewayInterface
# Optional
#
```

Figura 52: Wifidog - Arquivo de configuração *wifidog.conf* localizado dentro dos roteadores no diretório /etc

Originalmente, as páginas do módulo em PHP do *wifidog* possuem uma dinâmica diferente da que fora adotada na construção da rede do projeto Remesh. Abaixo listamos nossas modificações:

- Logo de exibição foi trocado para exibirmos o do projeto (Figura 53)
- Qualquer indivíduo cadastrado pode cadastrar novos usuários. Na nossa versão somente o administrador pode fazer isto.

- Cada novo usuário ao ser cadastrado tem 20 minutos para acessar o seu correio eletrônico e validar o email cadastrado. Na nossa versão o usuário cadastrado não recebe email é está plenamente autorizado para utilização da rede assim que recebe um *login* e senha de acesso
- Um mesmo *login* pode ser usado em diferentes máquinas ao mesmo tempo. Na nossa versão, o usuário que entra com um *login* que já está em utilização, desabilita o anterior e recebe uma notificação na página de entrada (Figura 54).
- Dados sobre estatísticas dos usuários podem ser visualizados somente pelo administrador. Na nossa versão nós criamos uma página em PHP que age em conjunto com o servidor web do projeto para que algumas informações possam ser disponibilizadas livremente.

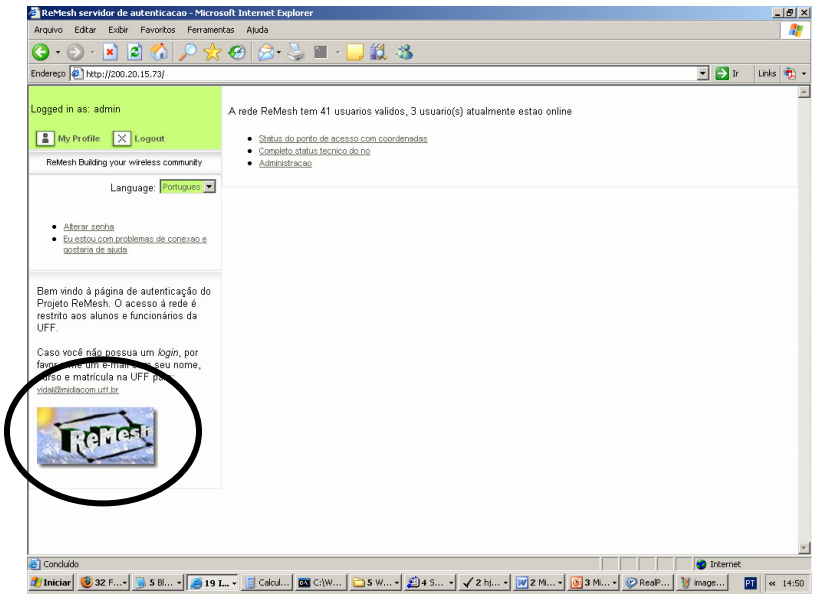


Figura 53: Wifidog - A página de abertura foi personalizada para exibir o logo do projeto

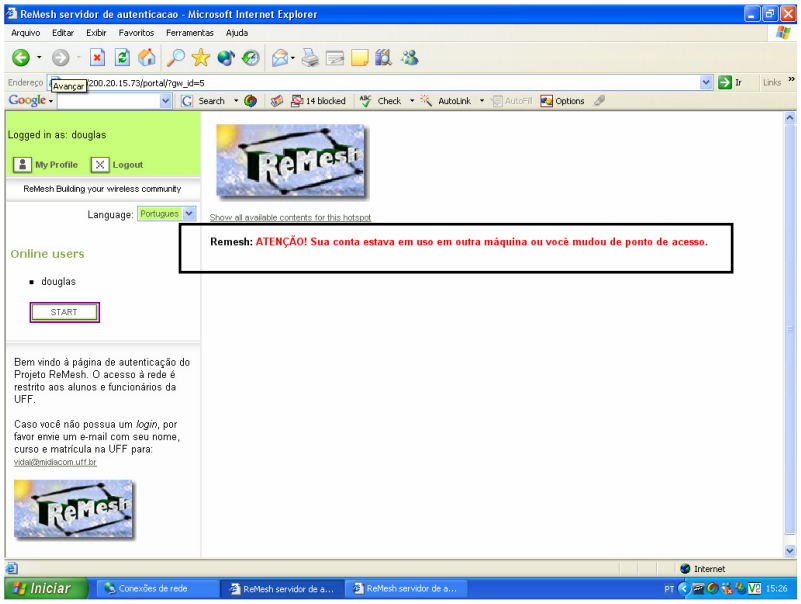


Figura 54: Usuário entrando com o mesmo login em duas máquinas diferentes. A máquina anterior será desabilitada.

A arquitetura proposta para o procedimento de autenticação pode ser invertida. Os clientes sem fio podem ser autenticados nos nós clientes e os clientes com fio no nó *gateway*. Contudo, para que esta configuração funcione, o nó *gateway* teria que manter suas portas abertas para todos os endereços da sub-rede sem fio (10.151.0.0/16), pois agora ele autenticaria apenas os endereços da sub-rede cabeada (10.152.0.0/16). Isto aumentaria muito a vulnerabilidade porque qualquer indivíduo utilizando um endereço IP da rede sem fio poderia ser roteado diretamente à Internet, desde que se conectasse no nó *gateway* como ponto de acesso.

Da maneira atual, o *gateway* está aberto para endereços da sub-rede cabeada, que só podem chegar até ele de duas maneiras: roteado por um elemento (roteador, estação, etc) que tenha uma interface sem fio, devidamente configurada na sub-rede, ou se conectando diretamente no roteador que representa o nó *gateway*. A primeira opção é possível, porém aumenta a dificuldade da invasão. A segunda opção não representa problema, pois o *gateway* possui proteção física por estar dentro das dependências da universidade (modelo que deve ser seguido no caso da reprodução da rede).

Além disso, com o nó usando o *wifidog* para bloquear os clientes sem fio, seria necessária a adição de múltiplas regras adicionais de *firewall* para permitir o encaminhamento dos pacotes provenientes de outros nós. Aumentar as regras nas tabelas de *firewall* de um

roteador significa no aumento do uso da memória RAM dos equipamentos. Isto não é desejado já que os roteadores utilizados no projeto atualmente dispõem apenas de 16 Mbytes.

Obviamente, a técnica de *captive portal* pode ser quebrada através da escuta na rede por endereços que estejam liberados (*packet sniffing*). Com isto, enquanto um usuário está autenticado, os seus endereços IP e MAC (no caso de clientes cabeados) podem ser utilizados por um invasor (*spoofing)*, porém, ao terminar suas atividades, o usuário é orientado a fechar a sua sessão. Isto é realizado através de uma pequena janela do *browser* que o *wifidog* mantém aberta com a opção de *"logout"*. Sabendo-se que políticas de uso como estas não podem ser exigidas dos usuários, utiliza-se um outro aspecto do nosso modelo que é a validação de um único endereço IP por *login* e senha. Na nossa atual estrutura, os endereços concedidos pelo servidor de DHCP são renovados com certa freqüência. Um novo endereço IP que seja identificado com o mesmo *login* e senha que foram utilizados para autenticar o endereço que foi "roubado" removerá o acesso do invasor, que será obrigado a buscar um novo endereço validado.

O projeto em sua primeira fase não teve como objetivo de alta prioridade a segurança do acesso. Apesar das dificuldades impostas à invasão, como o processo de autenticação, o próprio esquema de roteamento que exige um pouco de conhecimento da estrutura da rede e do serviço *https* para a entrada do *login* e senha, a solução possui deficiências nesta questão. Além das que já foram tratadas no parágrafo anterior, todo o tráfego dos usuários está aberto e passando por uma rede sem fio. Futuramente, o projeto pode propor novos esquemas de segurança. Contudo, por ser um projeto acadêmico e prioritariamente com fins de pesquisa nas áreas de novos aplicativos, gerência e métricas de roteamento, o esforço a ser gasto em uma estrutura mais confiável neste sentido foge ao escopo inicialmente proposto. Obviamente, levando este serviço para fins corporativos, a questão da segurança terá que ser seriamente revista.

Além do arcabouço de autenticação, o *wifidog* permite a visualização dos *logs* dos acessos dos usuários, da quantidade de dados que estão trafegando e das estatísticas de uso. Na próxima subseção, serão demonstrados os aspectos administrativos do *wifdog*, bem como a descrição das demais ferramentas desenvolvidas pelo projeto para o acompanhamento e gerência da rede.

5.2 FERRAMENTAS DE ACOMPANHAMENTO E GERÊNCIA

Nesta subseção serão demonstradas as ferramentas utilizadas pelo projeto para a gerência e manutenção dos nós e dos usuários. O principal objetivo desta subseção é a demonstração das ferramentas que foram geradas a partir da customização e aproveitamento de aplicativos livres (GPL). As ferramentas foram adaptadas não somente à estrutura da rede do projeto Remesh, mas também para serem utilizadas de maneira simplificada através da web.

5.2.1 Gerência dos usuários

A ferramenta *wifidog* possui uma interface de gerência de acesso exclusivo ao administrador do servidor de autenticação. Esta interface permite a visualização de estatísticas sobre os acessos bem como a criação e exclusão dos nós da rede (Figura 55). O *wifidog* é o responsável pela coleta das estatísticas dos acessos e pela gerência dos nós participantes. Em sua interface administrativa, o *wifidog* permite a adição, a exclusão e a edição dos nós participantes da rede. Nela também é possível a adição de novos usuários e o acesso às estatísticas de acesso filtradas por usuário, nó e/ou data. Além disso, é possível obter informações extras, como os usuários que estão *online* e a quantidade de dados trafegados na conexão atual. É possível também acessar o *log* de todas as outras conexões realizadas, fornecendo o usuário, data e duração do acesso e a quantidade de dados trafegados.

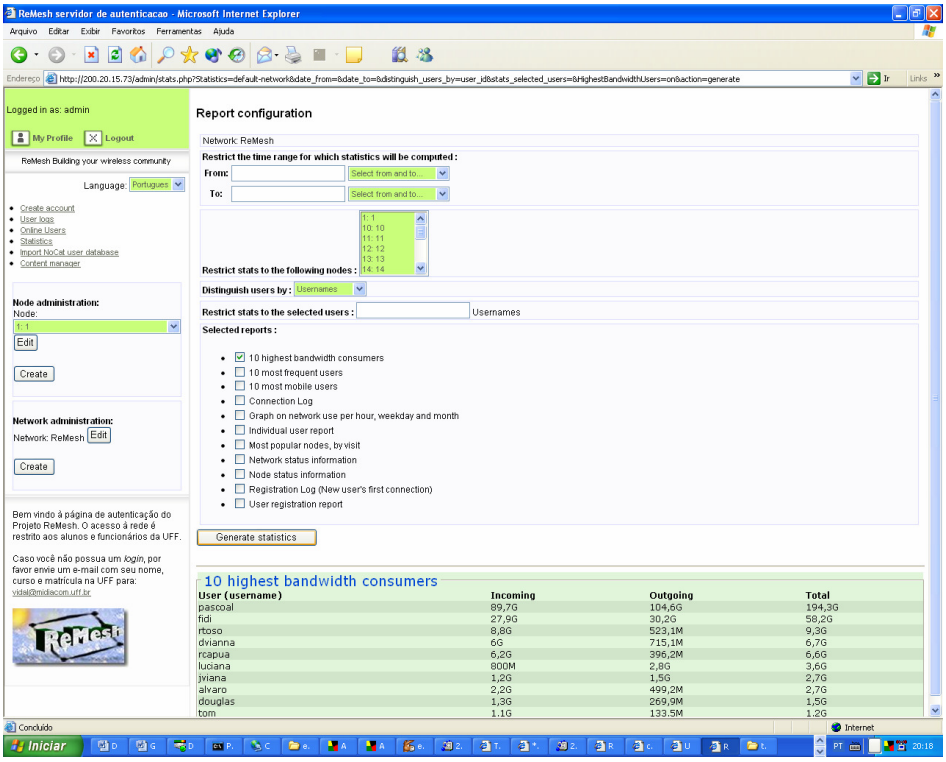


Figura 55: Interface de gerência do Wifidog

Com o objetivo de tornar determinadas informações públicas e de fácil acesso, foi criada uma pequena página em PHP dentro do servidor de web que fornece somente os dados que desejamos informar. Para tanto, quando a página é acessada diretamente, nenhuma informação é disponibilizada, porém, dentro do servidor web, uma URL é montada com as variáveis PHP associadas aos valores das informações a serem exibidas.

A construção da página foi feita a partir do código fonte da página original que é exibida na interface administrativa, removendo as funções que restringiam o seu acesso e mantendo somente as funções que exibem as informações desejadas. A página recebe a URL com os parâmetros desejados e monta as *strings* a serem exibidas. Se os parâmetros são enviados incorretamente, a página não exibe nada, protegendo informações confidenciais como nomes e quantidade de dados trafegados por usuários.

As informações disponibilizadas são diferenciadas entre a redes interna e externa e podem ser exibidas na página do projeto (PROJETO REMESH, 2007) Elas são:

- Os 10 usuários que mais consomem banda
- Os 10 usuários mais freqüentes
- Os 10 usuários que mais acessaram a rede por nós distintos

- Gráficos da quantidade de acessos por hora, dia da semana e mês
- Os nós mais visitados
- Gráficos do número de novos usuários registrados por mês e acumulativo
- Número de novos usuários por nó de acesso

Na Figura 56 está a página com as estatísticas sobre usuários e acessos à rede do projeto:

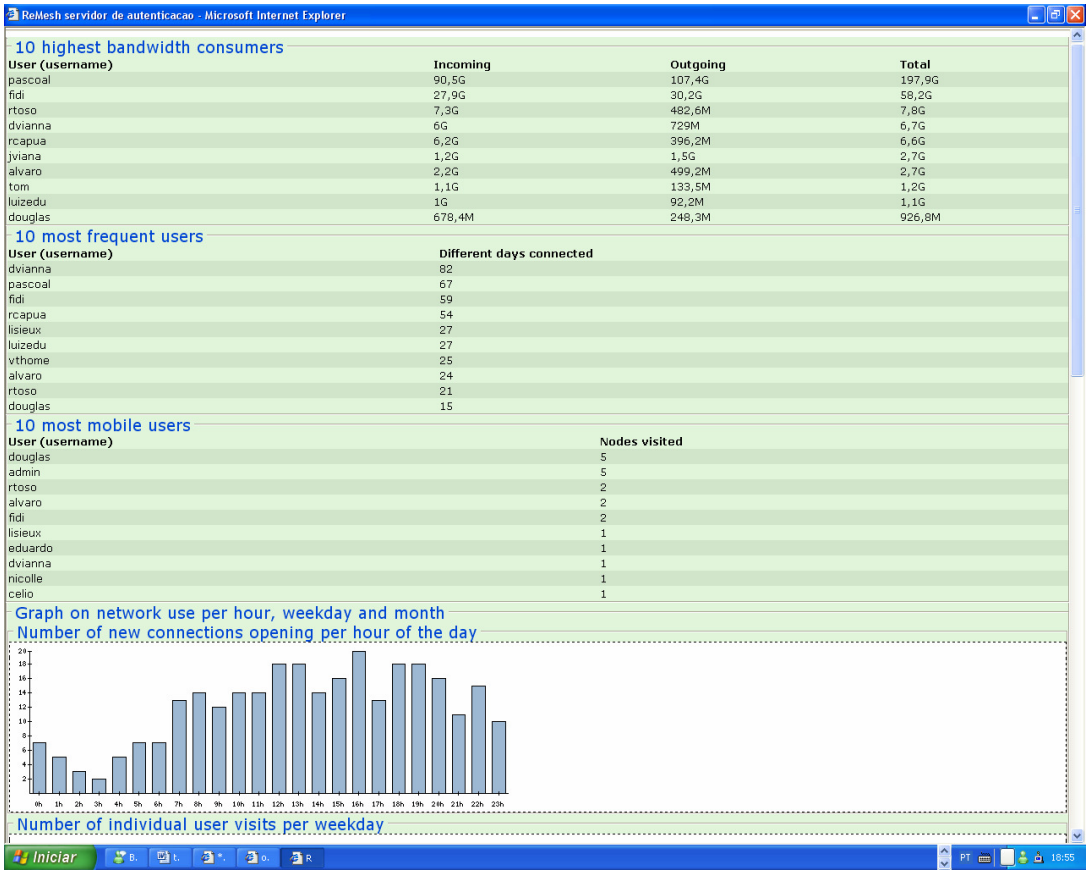


Figura 56: Visualização de estatísticas de acessos disponíveis na página do projeto Remesh

Quanto ao controle do acesso dos usuários, como exclusão ou suspensão de uma dada conexão, o módulo do *wifidog* não fornece uma interface *web* direta para a realização destas ações. Para tanto, torna-se necessária a ação direta ao banco de dados utilizado pelo módulo. As duas ações mais freqüentes são: suspensão temporária de usuários (útil para a realização

de testes e medições) e de conexões ativas. Elas são feitas através dos seguintes comandos SQL[15]:

1. Primeiro, deve-se acessar o banco no servidor de autenticação: "*/usr/local/pgsql/bin/psql wifidog"*. Onde "*wifidog*" é o nome do banco criado pelo módulo.
2. Dentro do banco digite:
    a. " UPDATE USERS SET ACCOUNT_STATUS=0 WHERE USERNAME!='admin'; ". Este comando, por exemplo, desabilita todos os usuários diferentes de admin. Para habilitar novamente basta executar o mesmo comando mudando o valor da coluna ACCOUNT_STATUS para 1.
    b. " UPDATE CONNECTIONS SET TOKEN_STATUS='USED' WHERE TOKEN_STATUS='IN_USE' AND USER_ID=(SELECT USER_ID FROM USERS WHERE USERNAME!='admin'); ". Este comando irá desabilitar todas as conexões ativas que não estejam sendo realizadas pelo usuário "admin".
3. O módulo do *wifidog* foi customizado para que, quando um usuário for apenas desabilitado, porém não excluído, ele visualize a tela exibida na Figura 57 ao tentar se conectar.

[15] SQL - *Structured Query Language,* ou Linguagem de Consulta Estruturada, é uma linguagem de pesquisa declarativa para bancos de dados relacionais e é um grande padrão para a operação banco de dados devido à sua simplicidade e facilidade de uso (WIKIPEDIA, 2007).

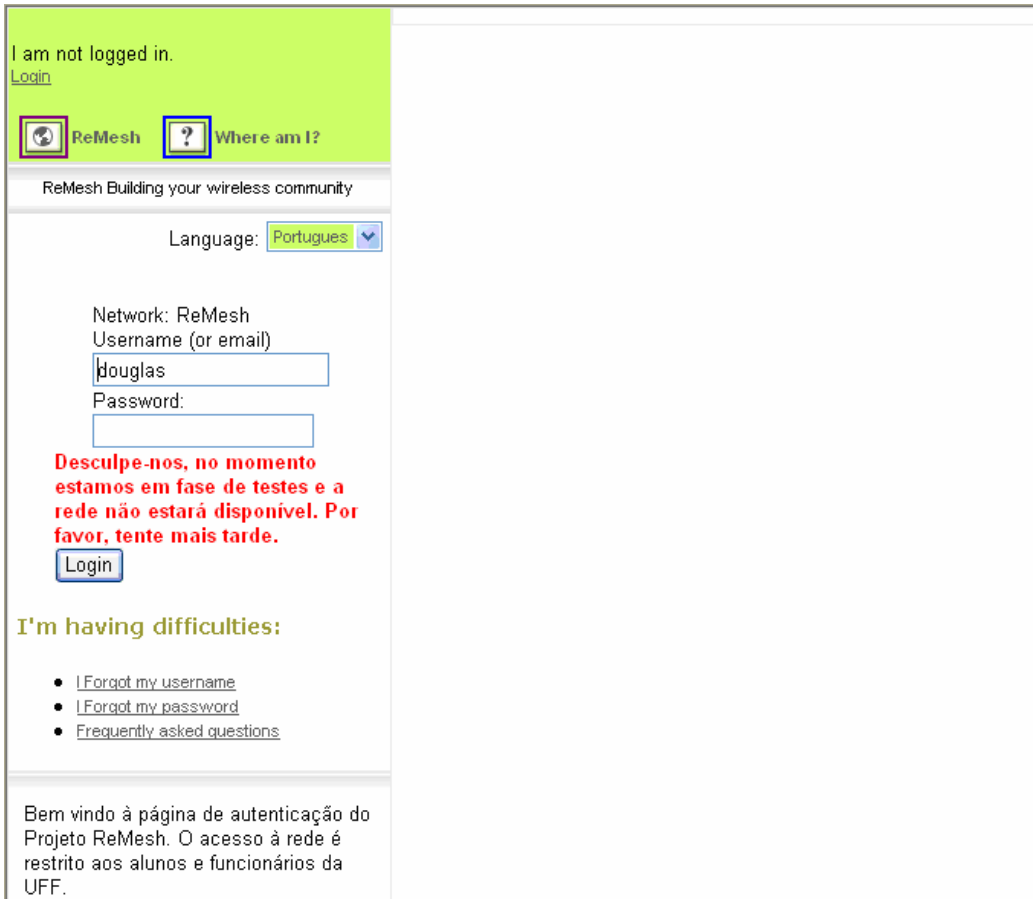


Figura 57: Tela de entrada do *wifidog* para usuários que foram desabilitados temporariamente.

Obviamente, demais ações, como exclusão permanente de usuários, podem ser feitas através de simples comandos SQL diretamente no banco de dados do servidor. Os dados obtidos pela ferramenta serão demonstrados no final deste capítulo.

5.2.2 Visualização da topologia e dos enlaces

A implementação do OLSR utilizada no projeto possui diversos *plugins* para ações diversas. Os *plugins* são módulos, escritos em C, que podem ser carregados ou não durante a inicialização do protocolo. A sua ativação e os parâmetros requeridos são informados no arquivo de configuração do olsr (*olsr.conf*).

Um destes plugins é o "*olsrd_dot_draw*". Este *plugin* age abrindo uma porta de acesso no nó que o executa. Esta porta aceita acessos via telnet e realiza a transferência de dados relativos à qualidade dos enlaces e das sub-redes exportadas por cada roteador mesh.

O plugin realiza apenas a abertura da porta e o envio das informações para uma determinada máquina, especificada no arquivo de configuração do *olsr (olsrd.conf)*. O plugin

envia as informações no formato "*dot*"[16] (GRAPHVIZ, 2006) através de uma conexão *telnet*[17]. Ele pode ser executado em qualquer nó da rede que possua o *olsr* e o módulo compilado. No caso da rede do projeto, ele está sendo executado nos gateways, tanto da rede interna como da rede externa. O *plugin* é acionado no arquivo de configuração segundo as diretivas abaixo:

```
LoadPlugin "olsrd_dot_draw.so.0.3"
{
PlParam     "accept"     "200.20.15.73"
PlParam     "port"       "2004"
}
```

O primeiro parâmetro indica a máquina que está habilitada para fazer a conexão *telnet* com o roteador. A porta padrão, caso não seja especificada, é a 2004.

Para ser utilizado com plugin, foi disponibilizado um programa em linguagem *perl* chamado "olsr-topology-view.pl". Tratas-se de um programa simples e de código aberto que pode ser obtido na Internet (MESHCUBE, 2007). Este programa age juntamente com os aplicativos Linux *GraphViz* (2006) e *ImageMagick* (2006), ambos de código aberto e também disponíveis na Internet. O programa em *perl* recebe os dados dos enlaces de todos os nós da rede a partir do roteador que executa o plugin. Utilizando o aplicativo *Graphviz,* o programa monta o gráfico da topologia da rede. O *plugin* envia as informações na taxa em que recebe os pacotes de HELLO (Capítulo 4) do *olsr.* Diversos gráficos são gerados ao longo do tempo e exibidos através do aplicativo *Imagemagick*. Desta forma consegue-se manter uma visão atualizada das condições dos enlaces entre os nós.

O programa em *perl* foi customizado para exibir as informações dos enlaces sem as suas sub-redes (informação originalmente disponibilizada, porém desnecessária, pois todas as sub-redes dos nós são conhecidas e estáticas), além de alterações visuais na geração dos elementos gráficos (formato e cores dos nós e setas). Outra alteração realizada foi a remoção do comando que executa o *Imagemagick* (comando "*composite"*), pois o objetivo era apenas a geração da imagem da topologia para ser exibida em uma página *web* estática.

---

[16] Fomato de arquivo que relaciona diferentes pontos com valores entre eles. Comumente utilizado em Ciência da computação para geração de gráficos de topologias e de grafos.

[17] Telnet é um protocolo de aplicação cliente-servidor , que funciona sobre o TCP, utilizado para *chats* e acesso remoto. Por não apresentar nenhum tipo de segurança aos dados trafegados, gradualmente vem sendo substituído por outro protocolo de aplicação, o SSH.

Um exemplo da imagem que é gerada pelo programa com a configuração padrão pode ser visto na Figura 58. A figura apresenta a imagem que é gerada pela aplicação original. Como pode ser observada, a qualidade visual é bem baixa (fontes pequenas e fundo preto), demonstrando a necessidade de alterações nos parâmetros de exibição. Com este propóstio, foi desenvolvido um programa escrito em C++, utilizando *cgi* (*Common Gateway Interface;* DWIGHT, ERWIN e NILES, 1997)*,* para que os gráficos pudessem ser apresentados em *html* de maneira mais compreensível (Figura 59).

O programa desenvolvido, denominado *topology.cgi,* é executado pelo servidor web quando um usuário o resquisita. Ele utiliza o programa em *perl* para fazer as requisições para os gateways da rede interna e externa. Com as informações obtidas, são gerados dois gráficos. Em seguida, o programa escreve uma página em *html* (*Hypertext Markup Language*) para exibi-los. A página é atualizada em um intervalo constante de tempo, gerando uma coleção de imagens. Desta forma, tem-se uma visão consistente da topologia de ambas as redes (interna e externa) e da qualidade dos seus respectivos enlaces.

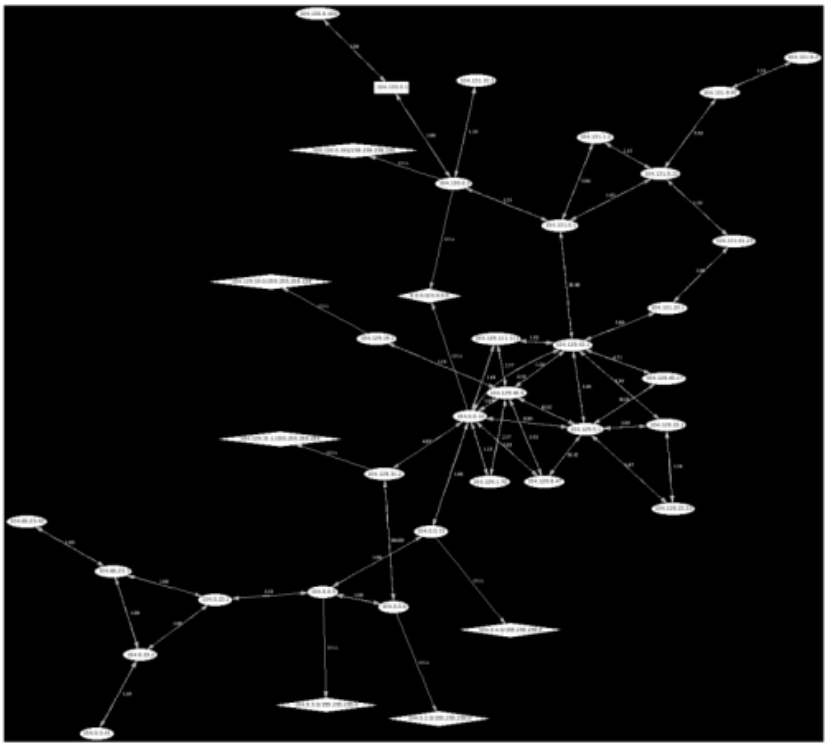


Figura 58: Gráfico gerado pelo programa *olsr-topology-view.pl* com as configuração padrão

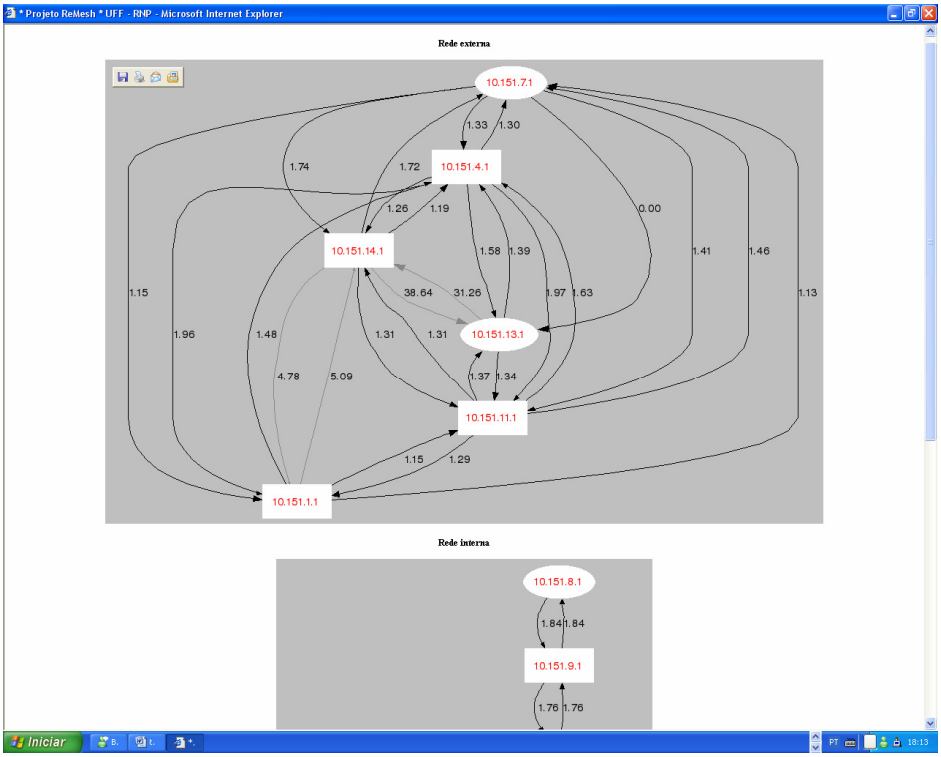


Figura 59: Ferramenta desenvolvida para a visualização via *web* da topologia da rede em tempo real

Através desta ferramenta, é possível um acompanhamento em tempo real das redes interna e externa. Pode-se saber se o nó está ativo, com quais nós ele está se comunicando e a qualidade dos enlaces. Além disso, é muito útil no momento de novas instalações. Quando um nó é ativado, ele entra automaticamente no gráfico da topologia, permitindo a verificação do estado do novo enlace.

Com o objetivo de tornar a visualização mais intuitiva e fácil para os usuários, os enlaces que antes eram representados por seus respectivos valores de ETX (Figura 41), passaram a ser representados por suas probabilidades de sucesso (Figura 60). Esta alteração foi realizada alterando-se o código do próprio módulo (“*olsrd_dot_draw.c*”) e recopilando-o (probabilidade de sucesso é o inverso do valor do ETX). Os nós são normalmente representados por elipses. Quando são MPR’s (*Multipoint Relay*, vide Capítulo 4), são representados por quadrados. A topologia pode ser visualiza na página do projeto (PROJETO REMESH, 2007).

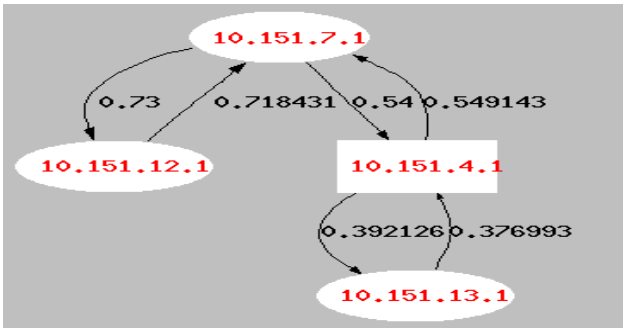


Figura 60: Gráfico da topologia da rede com enlaces representados por suas probabilidades de sucesso

5.2.3 Visualização de parâmetros internos dos nós

Através de um outro *plugin* do olsr, o *"olsrd_http_info"*, cada nó exibe suas informações via *web*. O acesso à informação é obtido por portas específicas (portas altas, não reservadas a serviços básicos). As informações disponibilizadas são: sub-redes que o nó exporta, seus vizinhos, seus MPR's, a qualidade da comunicação dele com os outros nós (valor do ETX em ambos os sentidos), os endereços de suas interfaces (sem fio e *Ethernet*) e a sua tabela de rotas (Figura 61).

Originalmente, o *plugin* faz com que o roteador execute um servidor *http* em uma determinada porta para exibir as informações. Ele é ativado no arquivo de configuração do *olsr* através dos parâmetros abaixo:

```
LoadPlugin "olsrd_httpinfo.so.0.1"        →Nome do plugin
{
PlParam      "Port"  "8087"               →Porta associada ao serviço http
PlParam      "Net"   "0.0.0.0 0.0.0.0"    →Parâmetro que especifica a rede
}                                          pode acessá-lo
```

Pelo fato da rede do projeto realizar NAT (*Network Address Translation),* não seria possível visualizar as informações fora da universidade. Para permitir que tais informações se tornassem acessíveis via *web* em qualquer lugar, duas medidas foram tomadas: primeiramente criamos uma série de regras de roteamento através da ferramenta *iptables* dentro do nó gateway (nó que realiza o NAT e que está dentro da rede da universidade com um endereço IP classe B; PETERSON e DAVIE, 1999) para que os roteadores pudessem ser acessados fora da rede em malha. Cada nó é mapeado a uma porta alta diferente. Em seguida, como o acesso

deveria ser feito através de portas altas, não era possível que um usuário conseguisse visualizar a página a partir de sua casa, por exemplo, devido ao *firewall* da universidade. Para contornar isto, foi criada outra aplicação *cgi*, atuando dentro do servidor web, ou seja, dentro da universidade e, portanto, não bloqueado.

A aplicação *cgi*, escrita em C (*httpinfo.cgi)*, abre uma conexão *http* na porta utilizada pelo plugin (porta alta), em seguida, pega os dados enviados e re-monta a página para exibi-la através do servidor *web* do projeto na porta 80 (porta padrão para http). Para cada nó, criamos um *hyperlink* na página do projeto. No *hyperlink*, está contida a porta que está associada ao determinado nó. A aplicação *cgi* utiliza a porta como parâmetro para acessar o roteador correto:

http://mesh.ic.uff.br/cgi-bin/httpinfo.cgi?8084

No exemplo acima, o usuário irá visualizar a página relativa ao roteador **10.151.4.1**.

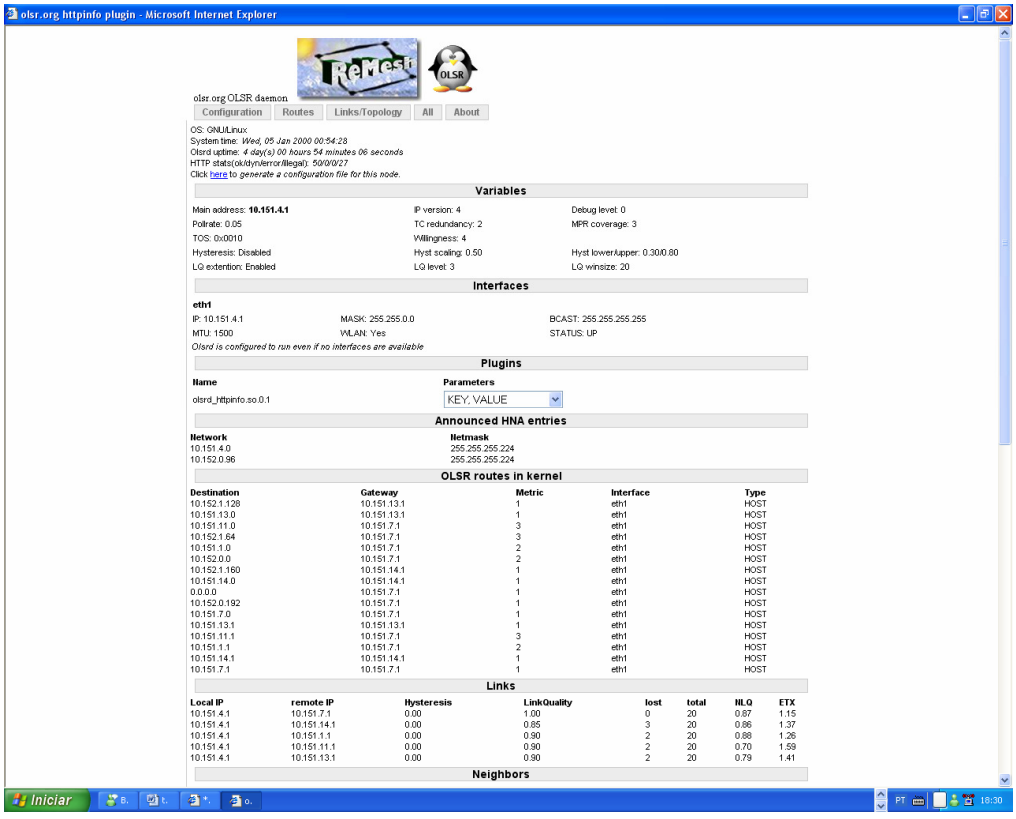


Figura 61: Informações de cada um dos nós disponíveis através do servidor *web*

5.2.4 MRTG *(Multi Router Traffic Grapher)* da rede externa

O MRTG (MRTG, 2007) é uma ferramenta que utiliza o protocolo SNMP (*Simple Network Management Protocol*)[18] e, adicionalmente, scripts para a automatização da geração de páginas *html* contendo os gráficos com as informações de monitoramento. Ele vem sendo utilizado amplamente para monitoração do tráfego das redes do projeto.

Na rede em malha do projeto Remesh, ele foi instalado no servidor *web* que está na mesma rede do gateway. Através de regras de *iptables* presentes no gateway, o servidor é encaminhado para obter as informações de cada nó da rede. Em cada nó da rede externa, foi instalado um cliente SNMP, disponibilizado pela distribuição do OPENWRT (OPENWRT, 2006).

A montagem das páginas com os gráficos funciona de maneira simples. O servidor *web* faz requisições periódicas aos nós da rede que estão executando os clientes SNMP. Os nós enviam as informações coletadas dos tráfegos que estão vindo de fora para eles (entrantes) e vice-versa (tráfego do nó para fora), para cada interface disponível. Como já foi mencionado, os nós possuem três interfaces: a sem fio (*wifi)*, a *Ethernet* WAN e a *Ethernet* LAN. Nos nós repetidores, somente as interfaces sem fio e LAN possuem tráfego. A interface sem fio do roteador, além de servir de ponto de acesso para os usuários, também faz o encaminhamento de pacotes que estão trafegando via múltiplos saltos. A LAN recebe os usuários cabeados e, portanto, disponível apenas para os voluntários do projeto que permitiram a instalação de roteadores em seus prédios. No gateway a situação é inversa. A interface sem fio funciona da mesma maneira, porém como ele não provê acesso aos usuários cabeados, a interface LAN não possui tráfego. Em contrapartida, no gateway, a interface WAN é a que recebe todo tráfego que liga a rede em malha com a Internet.

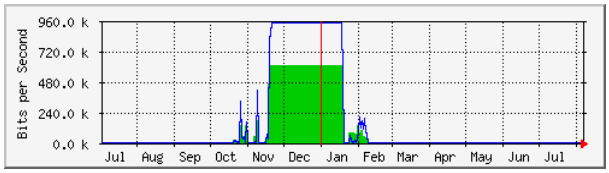
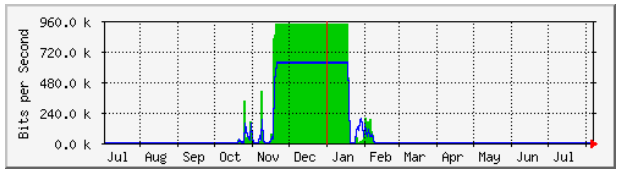
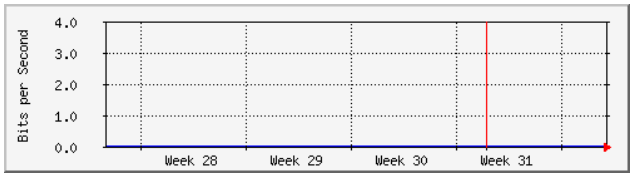
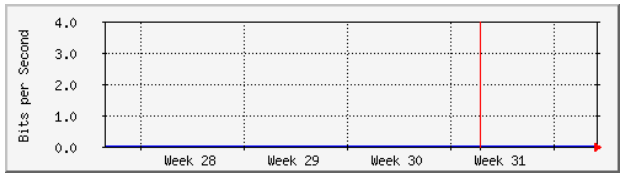
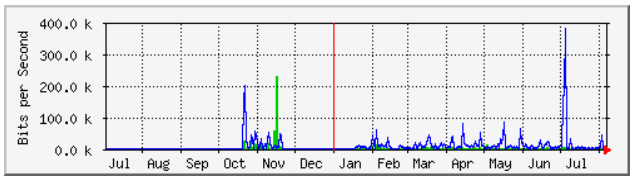
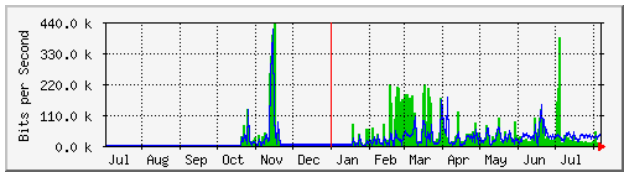
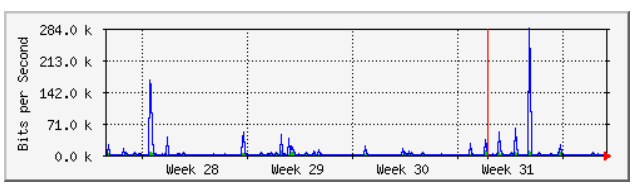
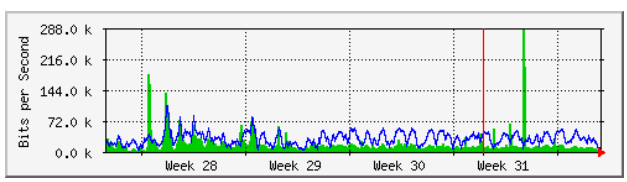
A granularidade de tempo disponibilizada pelo MRTG pode ser diária (cada valor é obtido pela média de 5 minutos), semanal (média de cada 30 minutos), mensal (média de cada par de horas) ou anual (média diária). Como cada nó da rede dispõe de duas interfaces ativas, o MRTG foi configurado para gerar os dois tipos de gráficos, referentes a cada uma delas. A escolha por esta separação possibilita a discriminação de duas informações úteis: total de tráfego gerado por usuários cabeados e o total de tráfego sem fio (encaminhados e de acesso

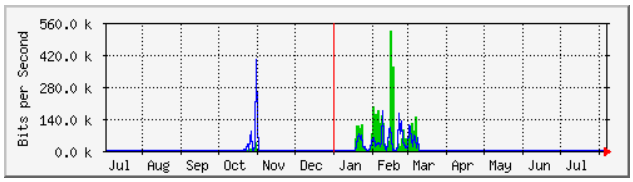
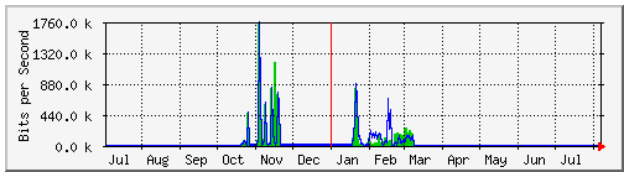
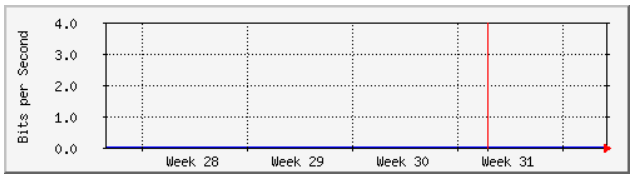
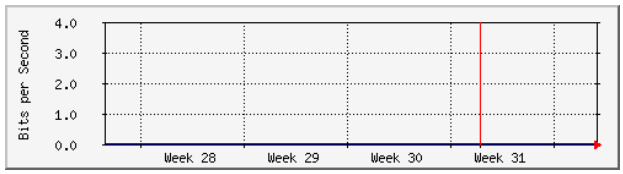
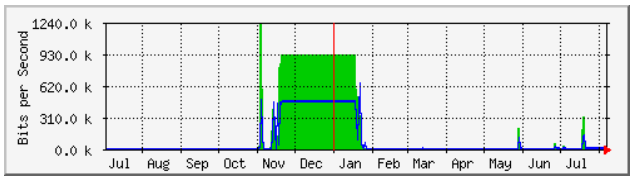
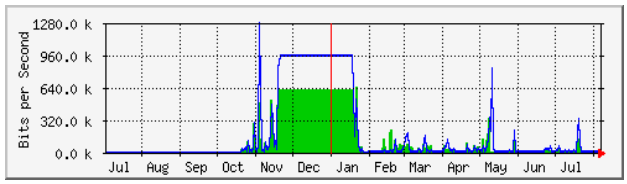
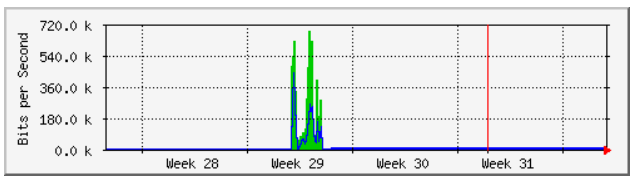
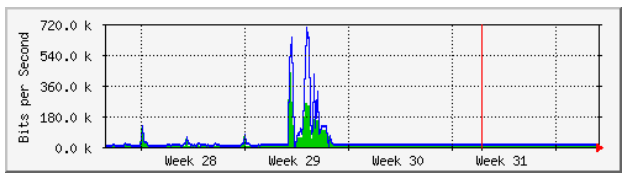
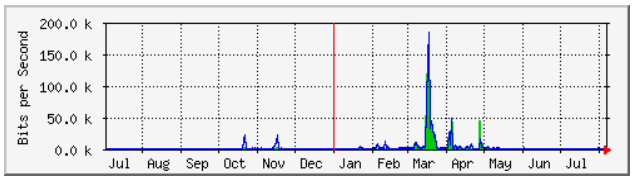
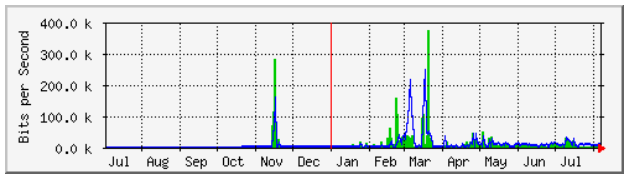
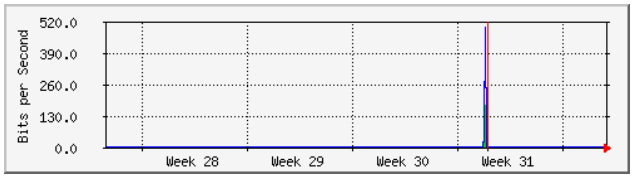
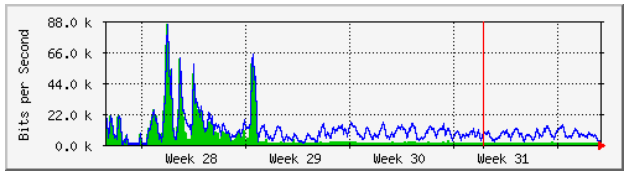
[18] SNMP – *Simple Network Management Protocol*- Protocolo de Gerência Simples de Redes é um protocolo de gerência típica de redes TCP/IP, da camada de aplicação que facilita o intercâmbio de informação entre os dispositivos de rede. O SNMP possibilita aos administradores de rede gerenciar o desempenho da rede, encontrar e resolver problemas e planejar o crescimento desta (WIKIPEDIA, 2007).

local). Supondo que os usuários não gerem tráfego entre eles, a informação da interface sem fio pode ser considerada como o total que sai da rede em malha com destino à Internet.

Na Tabela 12 estão exibidos os gráficos anuais e mensais respectivamente. Eles estão separados por nó (incluindo o gateway) e por suas respectivas interfaces. A notação utilizada é de linhas mais escuras (azuis), com a parte interior não preenchida, para o tráfego que sai e linhas mais claras (verdes), com a parte interior preenchida, para o tráfego entrante. Os nós podem ser identificados através da Figura 40. As imagens foram obtidas no início do mês de Março de 2007. Portanto, os gráficos mensais representam as quatro últimas semanas do mês de Fevereiro e a primeira semana de Março de 2007.

O conjunto completo dos gráficos está disponibilizado na página do projeto (PROJETO REMESH, 2007).

Nó 7 (Gateway da rede externa)	
Interface WAN	Interface sem fio
	
	
Nó 4	
Interface LAN	Interface sem fio
	
	

Nó 1	
Interface LAN	Interface sem fio
	
	
Nó 11	
Interface LAN	Interface sem fio
	
	
Nó 13	
Interface LAN	Interface sem fio
	
	

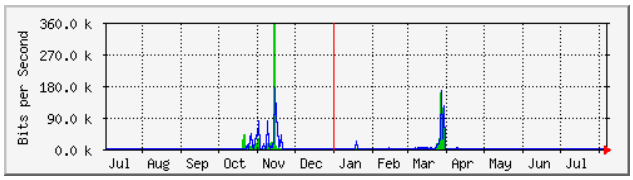
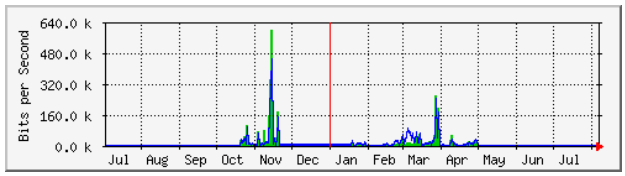
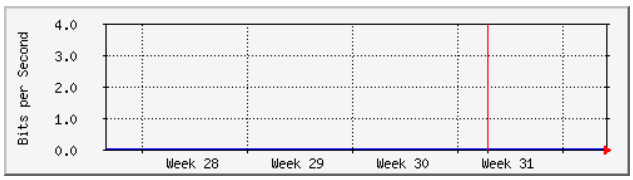
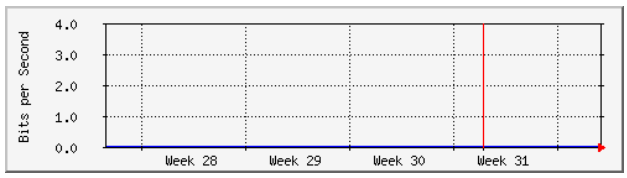
Nó 14	
Interface LAN	Interface sem fio
	
	

Tabela 12: MRTG da Rede Externa – gráficos separados por nó e interface ativa

As medições passaram a ser contabilizadas a partir de Outubro de 2006, como pode ser visualizado. No nó 7, pode ser percebido que todo o tráfego que chegou pela interface sem fio foi direcionado para a Internet, ou seja, não ocorreu nenhum tráfego com origem e destino dentro da rede que tivessem o gateway como nó intermediário (por isto podemos assumir que os usuários não geram tráfego entre si). Os gráficos entre as interfaces sem fio e WAN não seriam análogos se estivessem contabilizando os períodos onde houve medições de capacidade de vazão entre os nós (para tais medições é gerado tráfego a partir do nó com a ferramenta *iperf*). Nos gráficos com granularidade mensal, percebe-se que nas últimas semanas não houve tráfego significante, principalmente por coincidir com o período de férias e de carnaval na universidade.

O nó 4 tem uma característica interessante nos gráficos anual e mensal para ambas as interfaces. O tráfego foi bem maior na interface sem fio do que na LAN. Isto é bem razoável pelo fato do nó 4 ser um nó de ligação (na maior parte do tempo) entre os nós 13 e 14 com o gateway. O nó 1, apesar de ser repetidor na maior parte do tempo para o nó 11, apresentou um tráfego bem similar entre as interfaces (melhor observado na granularidade mensal). Contudo, na interface sem fio, existem picos de até 2920 kbps, enquanto que na interface LAN, durante o mesmo período, os picos foram menores (de até 2400 kbps).

O nó 11 apresentou uma quantidade bem maior de tráfego na interface sem fio do que na interface LAN (praticamente nulo após o mês de Janeiro). Além disso, o tráfego entrante é bem maior do que o que sai, demonstrando que o nó está sendo utilizado como nó de acesso para algum usuário. Quando os tráfegos que entram e saem estão na mesma proporção, é uma

indicação de que o nó está sendo utilizado como elemento intermediário para o encaminhamento de pacotes de outros nós da rede. O nó 13 foi pouco utilizado para os usuários cabeados (baixo tráfego na interface LAN), porém existe tráfego saindo na interface sem fio, chegando ao valor máximo de 1399 kbps, representado a utilização por usuários sem fio. Finalmente, nó 14 foi bem utilizado por algum usuário cabeado nos meses de Outubro e Novembro de 2006 (gráfico anual). Após este período, pode-se observar nos gráficos mensais, a ausência de utilização na interface LAN e baixo tráfego na interface sem fio (média de 10 kbps de tráfego entrante e 36 kbps de tráfego saindo), o que pode representar pacotes sendo encaminhados ou simplesmente tráfego de controle (a taxa máxima foi de 390 kbps neste período).

O MRTG demonstrou ser uma ferramenta muito útil e de fácil utilização. Contudo, devido a pouca quantidade de memória disponível nos roteadores, o excesso de processos sendo executados ao mesmo tempo ocasiona na finalização forçada do cliente SNMP. O projeto vem contornando isto removendo processos menos utilizados ou transferindo alguns serviços para os servidores (estações com alta capacidade de processamento e grande quantidade de memória). A gerência de rede pode obter muito mais informações através do MRTG, como por exemplo, tráfego de usuários não autorizados. A partir dos dados provenientes do MRTG, pode-se cruzar com as estatísticas de uso dos usuários cadastrados (através do *wifidog*) e descobrir se a rede está sendo invadida. Outra utilização do MRTG é a definição de nós que estão sendo subutilizados, viabilizando a recolocação destes em áreas de maior interesse.

5.3 QUALIDADE DA REDE EXTERNA

Nesta subseção serão apresentadas medições na rede externa com o objetivo de demonstrar a qualidade de sua utilização. Diferentemente do Capítulo 4 onde as medições tiveram caráter comparativo, o objetivo agora será a qualificação da usabilidade da rede externa, rede onde há tráfego com perfil mais próximo de uma rede de produção. Isto significa que os resultados que serão apresentados demonstram as condições de acesso à Internet que os usuários efetivamente estão experimentando.

Vale ressaltar que no momento das medições, a rede externa estava em plena utilização utilizando o protocolo de roteamento OLSR-ML, com a antena direcional no gateway e com taxa de interface no modo “automático” (parâmetros que foram discutidos e

comparados em capítulos anteriores). Serão demonstradas medições mais detalhadas de vazão, de atraso correlacionando com a perda de pacotes e do jitter. Finalizaremos esta subseção com as estatísticas de uso obtidas pela ferramenta *wifidog*.

5.3.1 Vazão

O objetivo dos testes de vazão era de demonstrar a real capacidade do sistema para os usuários, ou seja, o que eles realmente têm de capacidade de *upload* e de *dowload*. Para tanto, foi criado um *script* em *bash* que faz a retirada dos usuários ativos e bloqueia qualquer outro que não seja permitido de entrar na rede. A medição utilizou a ferramenta *iperf* sobre TCP e com fluxo bidirecional. Os testes eram gerados a partir do gateway para cada outro nó da rede externa, durante 10 minutos. As medições foram realizadas durante três horários distintos, 4, 11 e 18 horas, durante seis dias consecutivos. As médias finais deste teste já foram demonstradas na Figura 43.

Na Figura 62 estão os mesmos resultados, porém com os valores separados por hora do dia, nó, e direção do fluxo (up de *uplink* ou *upstream*, do gateway para o nó, e down para *downlink* ou *downstream*, do nó para o gateway), além da inclusão dos valores de desvio padrão.

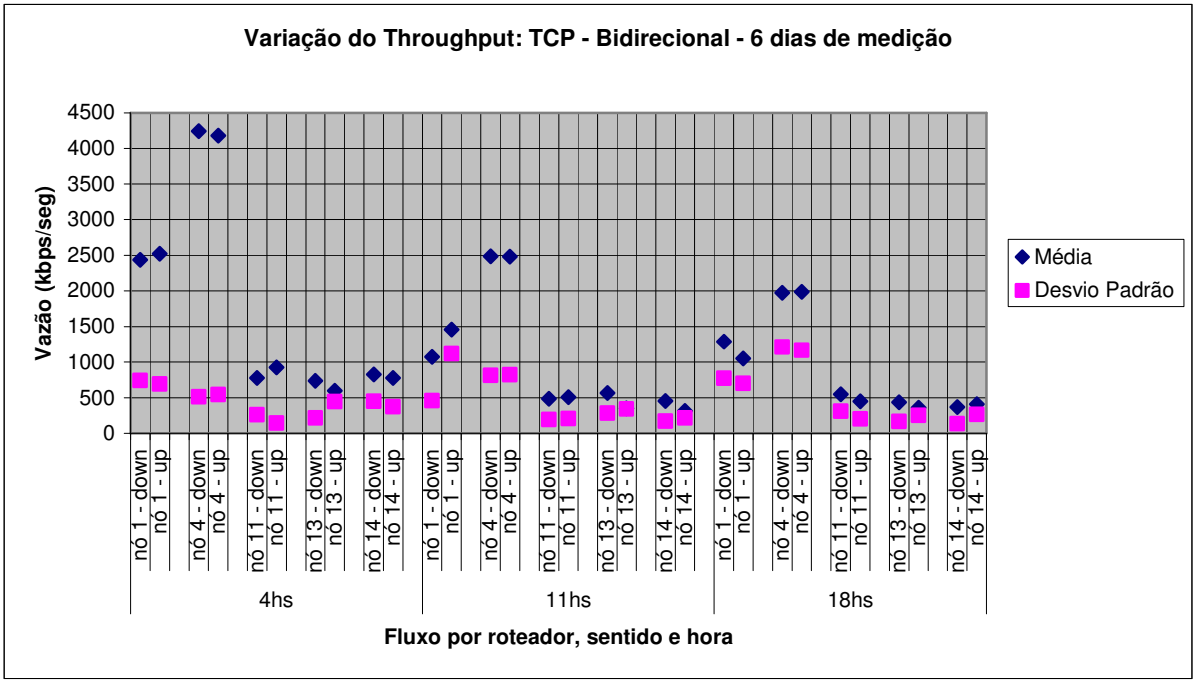


Figura 62: Vazão da rede externa para cada roteador em três horários distintos de medição

Todos os nós obtiveram valores mais altos no período de 4 horas. Durante este horário, a baixa densidade de carros e pessoas presentes no espaço do rádio-enlace permite que as interferências oriundas de múltiplos percursos sejam diminuídas (BOITHIAS, 1987), melhorando a qualidade do sinal recebido. Os horários de 11 e 18 horas obtiveram resultados similares, sendo que, pelo mesmo motivo descrito para as 4 horas, o horário de 11 horas teve uma leve vantagem.

O nó 4 foi o que teve as maiores taxas (em torno de 4250 kbps) nos dois sentidos com baixo valor de desvio padrão. Isto era esperado pelo fato do nó 4 estar próximo ao gateway e, portanto, um dos principais nós de ligação entre outros nós da rede à Internet. Seguindo estes resultados está o nó 1, que também possui enlace direto ao gateway. O nó 1, apesar de estar próximo, não está na direção do feixe principal da antena do gateway. Isto implica também em uma diferença menor entre as médias e os valores de desvio padrão (em torno de 1750 kbps) em comparação com o nó 4 (em torno de 3750 kbps).

O nó 4, mesmo no horário mais crítico (18 horas), obteve valores de desvio padrão razoáveis (em torno de 1250 kbps) em comparação com os outros nós. Contudo, para os outros nós, os valores foram altos em comparação com as respectivas médias. O alto valor do desvio padrão indica a intensa variabilidade na qualidade do enlace e era esperado devido à taxa de mudança de rotas (vide Tabela 9). Porém não é um resultado satisfatório.

Os outros nós obtiveram desempenho semelhante por estarem mais distantes do gateway e, na maior parte do tempo, serem alcançados através de dois ou mais saltos. Durante o período das 4 horas, os nós 1, 13 e 14 obtiveram taxas entre 500 e 1000 kbps. Nos outros horários obtiveram médias entre 300 e 500 kbps. Apesar das taxas serem consideradas altas para os padrões de acesso no Brasil (com base em observações realizadas no ano 2006, obviamente a tendência da tecnologia é aumentar este patamar), os valores de desvio padrão estão muito próximos das médias. Por exemplo, o nós 13 e 14, nos horários de 11 e 18 horas, obtiveram valores de desvio padrão muito próximos dos valores de médias em ambos os sentidos. Um caso crítico é o nó 14, no sentido *upstream* no horário das 11 horas. A média foi de 312,6 kbps e o desvio padrão foi de 213,2 kbps.

Os valores das médias indicam que, pelo menos na maior parte do tempo, os usuários têm conseguido experimentar valores de vazão bem razoáveis. Os valores mais elevados (nó 4) alcançaram patamares de taxa de 4246 kbps, no sentido de *downstream* e 4183 kbps no sentido contrário.

Para uma melhor análise, outro teste para a vazão foi realizado, considerando fluxos diferenciados: TCP bidirecional e unidirecional e UDP, somente unidirecional e com carga de 10 Mbps. Para cada um destes três tipos de fluxos propostos, foram realizadas medições de 10 minutos para cada nó. O objetivo deste resultado é a avaliação das diferenças de vazão que são obtidas diferenciando o modelo de medição realizado. As medições deste teste (Figura 63) são independentes das medições realizadas na Figura 62 (dias e horários diferentes).

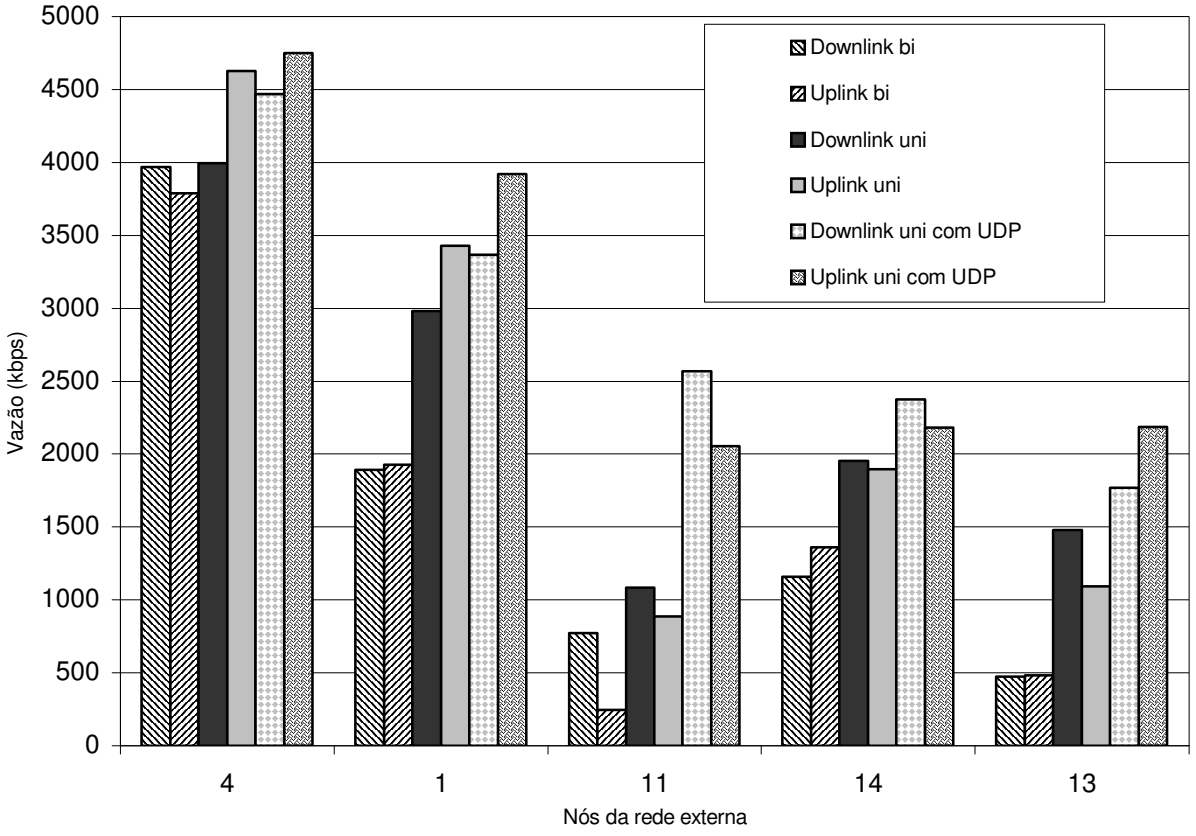


Figura 63: Medições de vazão com diferentes tipos de fluxo (PASSOS *et al,* 2006)

As medições unidirecionais são realizadas separadamente, ou seja, para a obtenção dos valores de *uplink*, o *iperf* é executado no gateway em direção ao nó. Para *downlink,* o *iperf* é executado no nó em direção ao gateway. Obviamente, ocupando o canal de transmissão com apenas um fluxo, os valores obtidos são iguais ou maiores. Utilizando UDP, os valores obtidos tornam-se maiores ainda, chegando a 4700 kbps para o nó 4 no sentido de *uplink*. Isto ocorre devido à ausência de fluxo contrário gerado pelo controle de congestionamento da arquitetura do TCP (envio de ACK's).

A medição com UDP tenta colocar na rede a carga configurada (no caso, 10Mbps). O *iperf* vai reportar o quanto ele conseguiu alcançar de dados enviados no lado cliente (lado que recebe o fluxo), gerando o valor da taxa obtida. Com o UDP, a taxas obtidas alcançaram em média valores 20% superiores em comparação com os fluxos unidirecionais do TCP, destacando-se o nó 11 onde os fluxos UDP alcançaram o dobro.

5.3.2 Atraso e perda de pacotes

O objetivo desta subseção é avaliar a qualidade da rede em relação aos valores dos atrasos. O teste realizado foi o mesmo da subseção **4.3.4**. Ele consiste no disparo de pacotes de ping a partir do gateway para todos os outros nós da rede, em um período de tempo de 24 horas para cada um (total de 86400 pacotes). Os gráficos relacionam os valores dos atrasos com a quantidade de pacotes perdidos e excedidos, acumulados ao longo do tempo.

Pacotes excedidos são os que expiram o TTL (*Time To Live)* e retornam para a origem. Eles representam momentos onde as variações nas rotas da rede foram altas, criando *loops* entre os roteadores, até que os nós "desistem" de entregar o pacote ao destino. Os pacotes perdidos englobam os que foram excedidos, os que não foram entregues por falhas na transmissão e os que entraram em *loop* mas não obtiveram uma rota de retorno para serem "devolvidos" à origem. Para o valor dos pacotes perdidos, pode-se utilizar a mesma numeração do eixo das ordenadas (vertical).

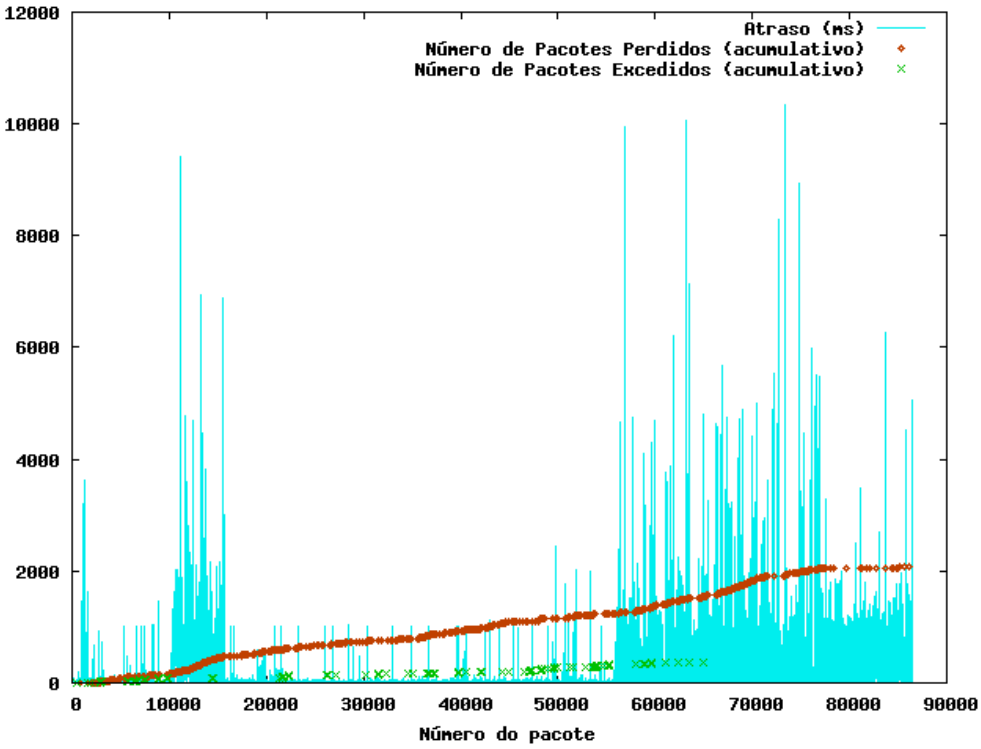


Figura 64: Atraso e perda de pacotes acumulados para o nó 1

Nó 1 (Figura 64) obteve perda relativamente linear ao longo de toda a transmissão, tendo leve aumento nos períodos de picos nos valores de atraso (chegando a até 10 segundos de atraso). A partir dos pacotes de número 70000 os pacotes excedidos pararam de ser reportados. Neste mesmo período ocorrem altos valores de atraso consecutivos, demonstrando instabilidade de rotas. É interessante observar que, mesmo nos períodos onde os valores de atraso não excederam 2 segundos (entre os pacotes 20000 e 50000), as perdas continuaram a ocorrer, chegando a 1728 pacotes perdidos (2 % de perda).

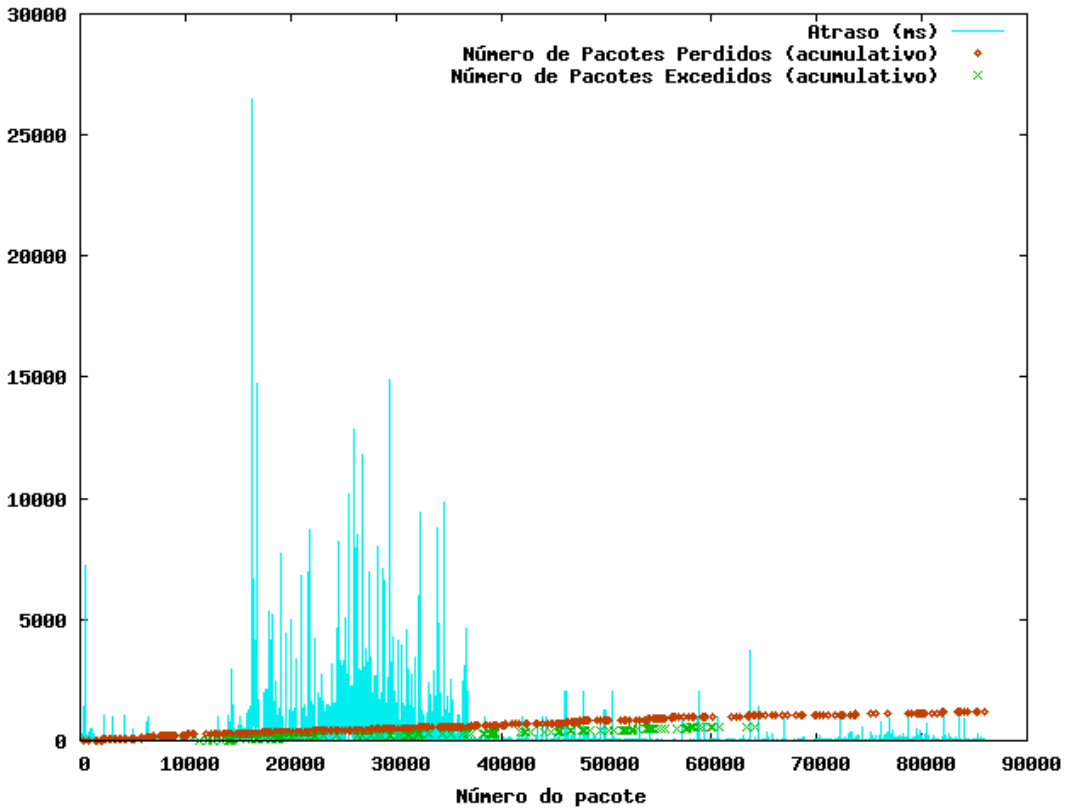


Figura 65: Atraso e perda de pacotes acumulados para o nó 4

O nó 4 (Figura 65) obteve melhor desempenho quanto a variação do atraso em relação ao nó 1 pois ocorreu somente um período de alta instabilidade. Entretanto, o nó 4 alcançou um pico de 25 segundos, mais de duas vezes superior ao pico do nó 1, mantendo-se relativamente estável após este valor. As perdas acumuladas foram lineares ao longo do tempo e bem próximas do número de pacotes excedidos: aproximadamente 2%.

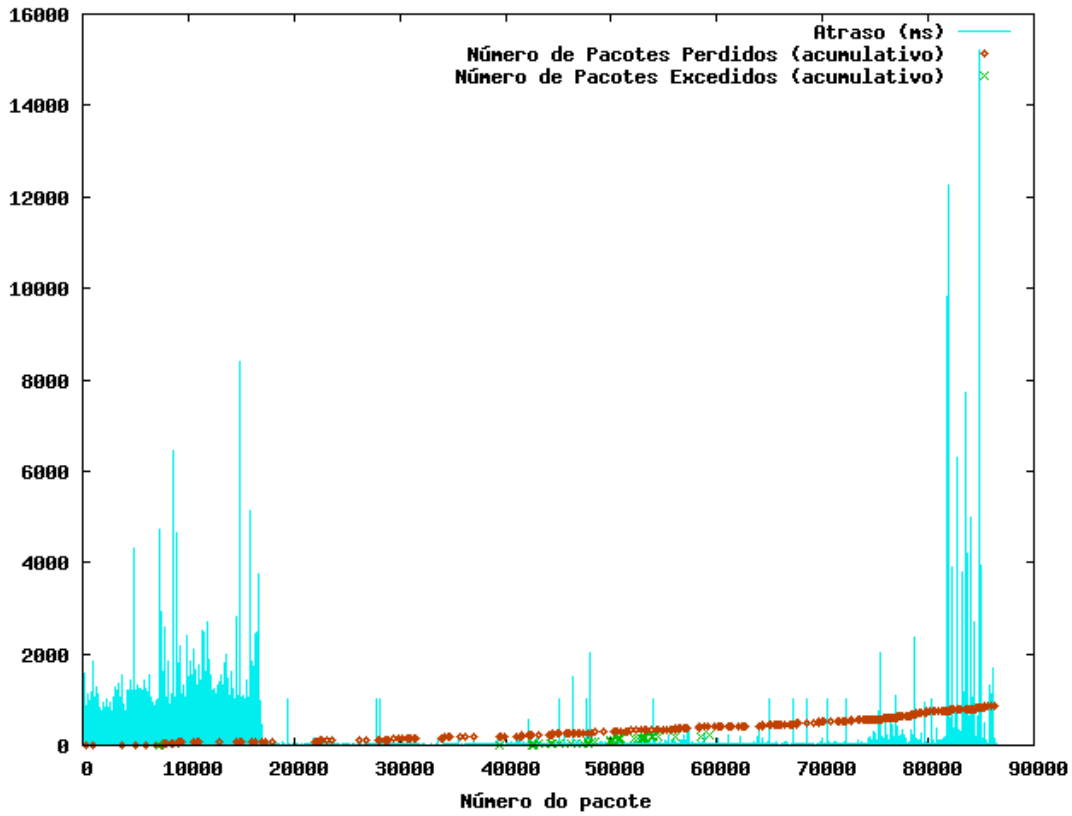


Figura 66: Atraso e perda de pacotes acumulados para o nó 11

Nó 11 (Figura 66) apresentou dois períodos de alta variação no atraso, chegando a um pouco mais de 8 segundos no primeiro e até 15 segundos no segundo. Entretanto foram períodos de curta duração. O aumento na taxa de perdas foi linear a partir dos 40000 pacotes, tendo antes obtido algumas perdas esporádicas, variando com períodos de nenhuma perda. O valor final de pacotes perdidos foi de 1247 (aproximadamente 1% de perda).

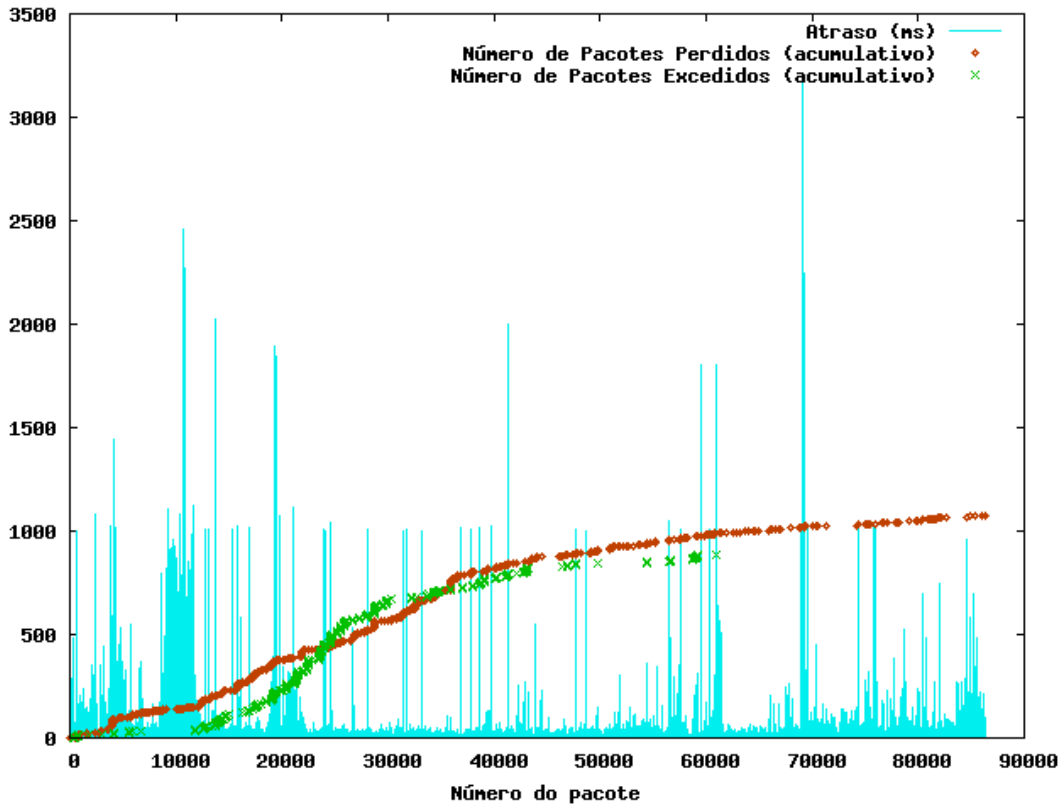


Figura 67: Atraso e perda de pacotes acumulados para o nó 13

Nó 13 (Figura 67) apresentou bons valores de atraso ao longo de todo o período de transmissão. À primeira vista, parece que ocorreu instabilidade ao longo de todo o período de transmissão. O que não está incorreto devido aos altos e baixos dos picos, porém percebe-se que valor máximo de atraso obtido foi de 3,2 segundos, ou seja, no nó 13, devido à ausência de picos fora da média, os valores dos atrasos mantiveram-se em torno do mesmo intervalo (entre 0 e 3500 milisegundos). As perdas de pacotes tiveram aumento linear separadas por dois períodos de diferentes angulações: do pacote 0 ao pacote 35000 (aproximadamente), com maior angulação, e depois entre os pacotes 35000 até o final da transmissão, com menor angulação. Um total de 2120 pacotes foram perdidos, representando 2% de perda.

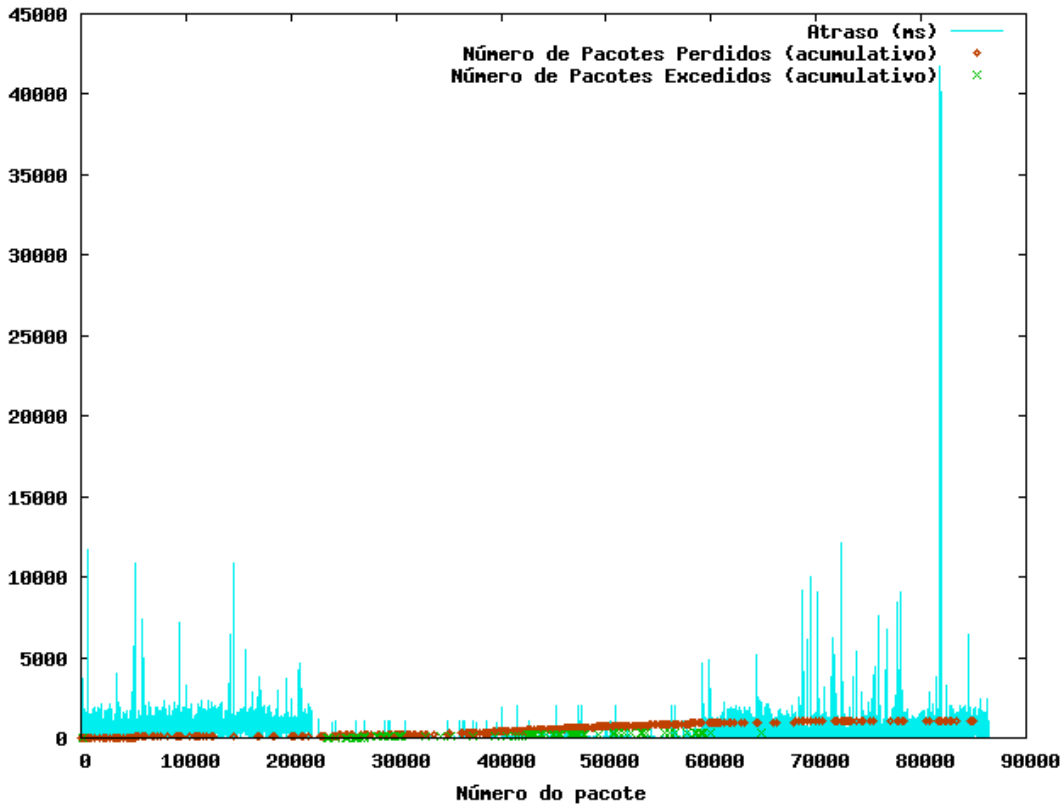


Figura 68: Atraso e perda de pacotes acumulados para o nó 14

Nó 14 (Figura 68) apresentou alta instabilidade nos valores de variação de atraso, piorando nos períodos entre o pacote de número 80000, quando ocorreram picos em torno de até 40 segundos. Apesar do alto valor, nos outros períodos o máximo obtido foi de 12 segundos. As perdas de pacotes também tiveram aumento linear alcançando 1448 pacotes perdidos (aproximadamente 1% de perda).

A rede demonstrou certa estabilidade quanto à taxa de pacotes perdidos, não superando os patamares de 2% de perda. Entretanto, os valores de atraso variaram muito, passando por períodos de alta instabilidade alcançando valores intoleráveis (até 40 segundos). A rede é confiável, porém em determinados períodos pode se tornar de difícil utilização, principalmente em nós mais críticos como os nós 11e 14.

Uma análise mais detalhada das variações do atraso ao longo do tempo resultaria em um processo estocástico (LEON-GARCIA, 1994), que poderia ser modelado para a obtenção um possível padrão. A princípio, pode-se concluir que uma métrica baseada na perda de pacotes, como é o caso do ETX, não resulta em valores acurados da real qualidade dos enlaces. A perda de pacotes possui uma taxa de aumento praticamente linear, ou seja, as

perdas ocorrem na mesma proporção ao longo de todo o período de transmissão. O mesmo não é observado para o atraso. Uma métrica baseada em atraso, como o ETT (*Expected Transmission Time*; DRAVES *et al,* 2004[a]*)* poderia resultar em uma avaliação mais próxima da realidade dos enlaces.

Entretanto, pode-se concluir que uma métrica com uma variabilidade maior poderia aumentar a instabilidade da rede, aumentando a taxa de alteração das rotas ao longo do tempo. Porém, as medições poderiam gerar médias que apresentariam diferenças maiores entre os diferentes enlaces, resultando em enlaces definidos como "bons" e "ruins", sem qualificações intermediárias. Desta forma, mesmo que os valores das estimativas tivessem uma maior taxa de variação, a troca das rotas seria menos freqüente.

5.3.3 Jitter

A importância do jitter como parâmetro de qualificação é a verificação da condição da rede para aplicações que são sensíveis à variações do atraso, como por exemplo: voz e vídeo. Para tais aplicações, variações no tempo de envio dos pacotes podem gerar falhas na sincronização do fluxo. Uma rede que com boa capacidade para esses tipos de fluxo tem que apresentar jitter estável e próximo de zero.

A partir dos resultados obtidos na subseção anterior, pode-se prever que o jitter na rede externa apresentará grandes variações. O teste realizado foi o mesmo da subseção **4.3.4,** disparo de pings a partir do gateway para os demais nós da rede. Os valores foram obtidos através do módulo da diferença do atraso de um pacote com o atraso do pacote anterior.

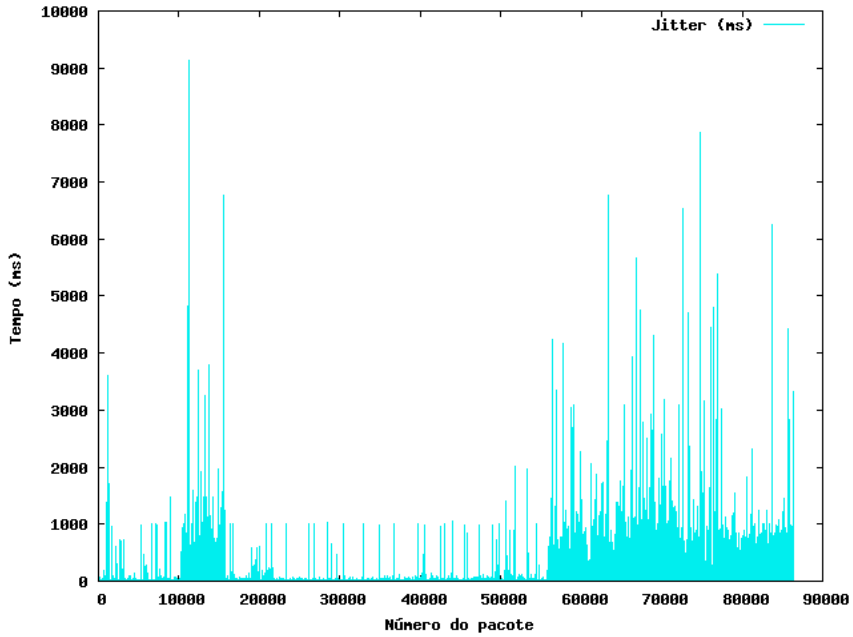


Figura 69: Valores do jitter para o nó 1

O nó 1 (Figura 69) apresentou alto valor de jitter entre os pacotes 10000 e 15000, chegando a 9 segundos. Entre os pacotes de números 15000 e 55000 existe um período de baixa variação, chegando a picos em torno de 1 segundo. Porém, a partir do pacote de número 55000 as altas variações tornam-se freqüentes e se mantêm até a finalização do teste, alcançando picos de até 8 segundos.

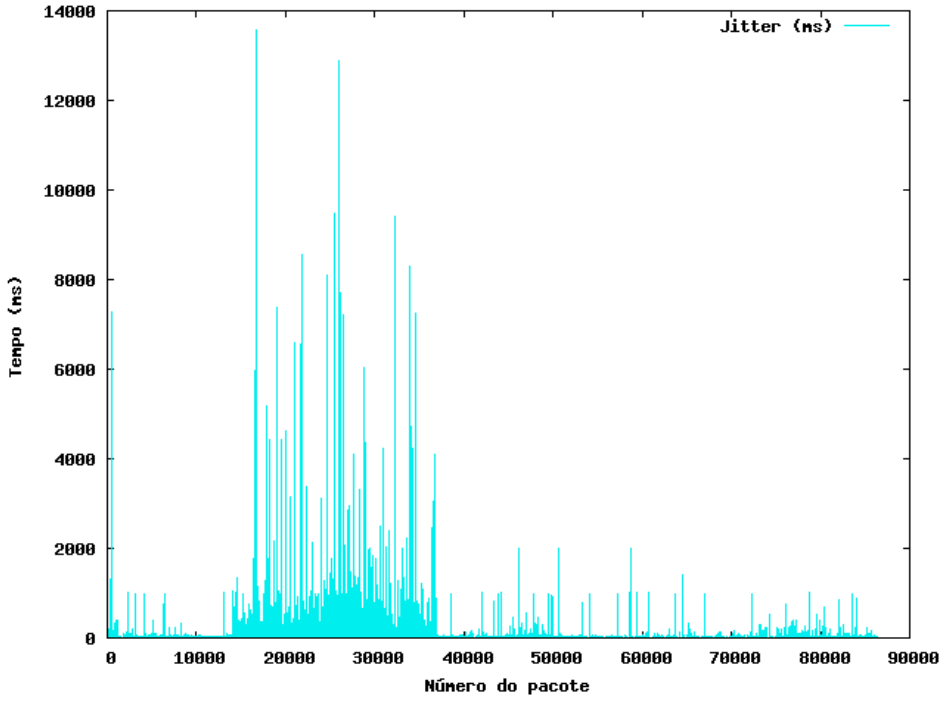


Figura 70: Valores do jitter para o nó 4

Nó 4 (Figura 70) possui períodos mais longos de estabilidade em comparação com o nó 1, entretanto, no período entre os pacotes de números 15000 e 38000, aproximadamente, existe um período de alta instabilidade com picos na faixa de 13,5 segundos. No restante do tempo, o nó 4 apresentou instabilidade tolerável. Entretanto, picos na ordem de 12 segundos, como os que foram apresentados, finalizariam uma transmissão de voz, por exemplo.

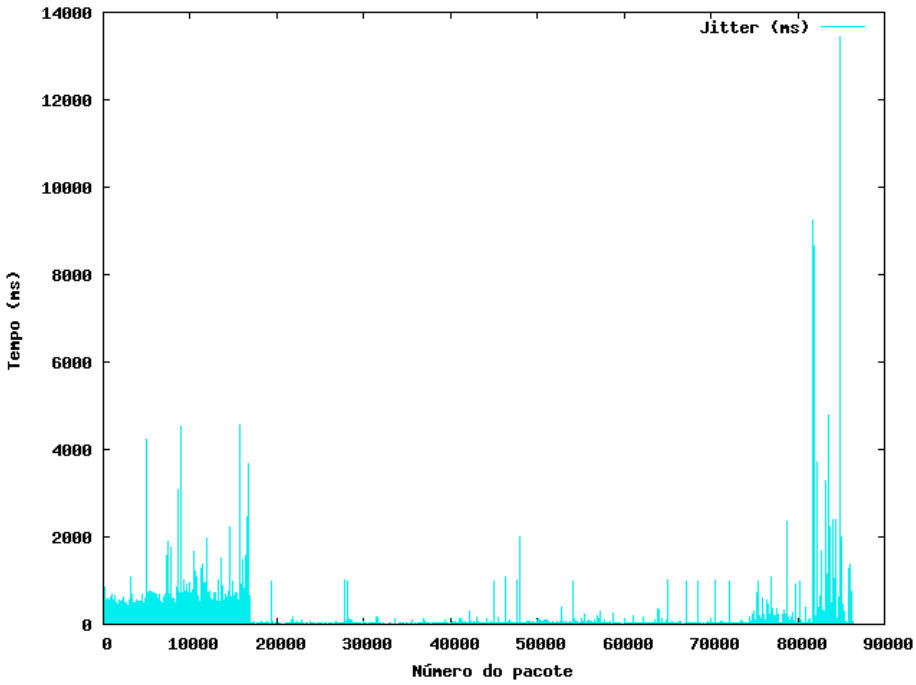


Figura 71: Valores do jitter para o nó 11

Nó 11 (Figura 71) apresentou valores de jitter bem razoáveis entre os pacotes de número 20000 até o de 80000, aproximadamente. Neste período aplicações sensíveis às variações do atraso funcionariam muito bem. O máximo valor obtido foi de 13,5 segundos, apenas no período final.

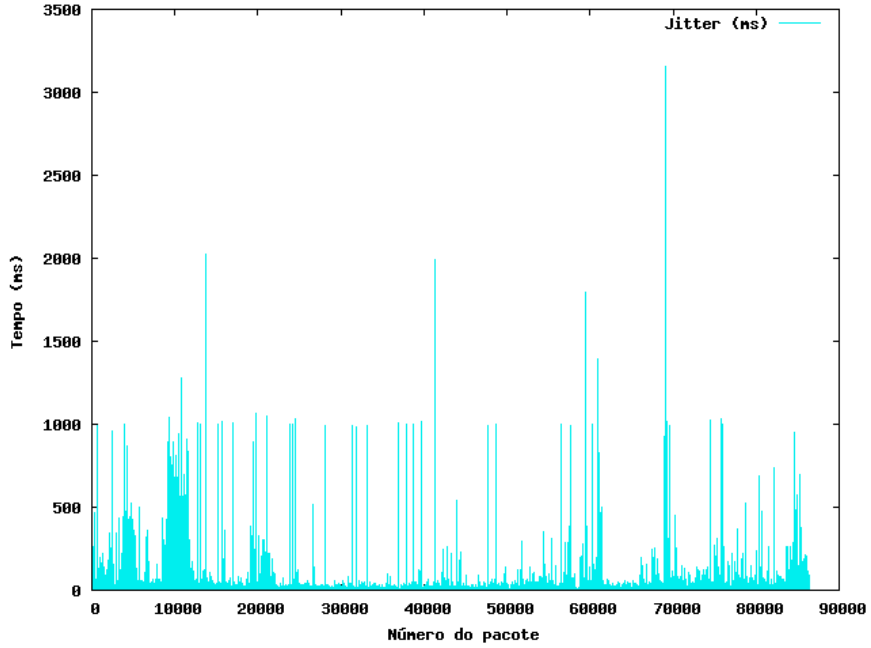


Figura 72: Valores do jitter para o nó 13

O nó 13 (Figura 72) apresentou uma maior estabilidade com o jitter na média de 500 milissegundos. É interessante observar que o nó 13 é acessível a partir do gateway, na maior parte do tempo, através do nó 4. A estabilidade do nó 13 é devido ao fato dele estar isolado do meio onde todos os nós se comunicam com qualidades próximas. Ele possui um enlace bem definido com o nó 4 e enlaces praticamente inexistentes com os demais nós da rede (vide Figura 40).

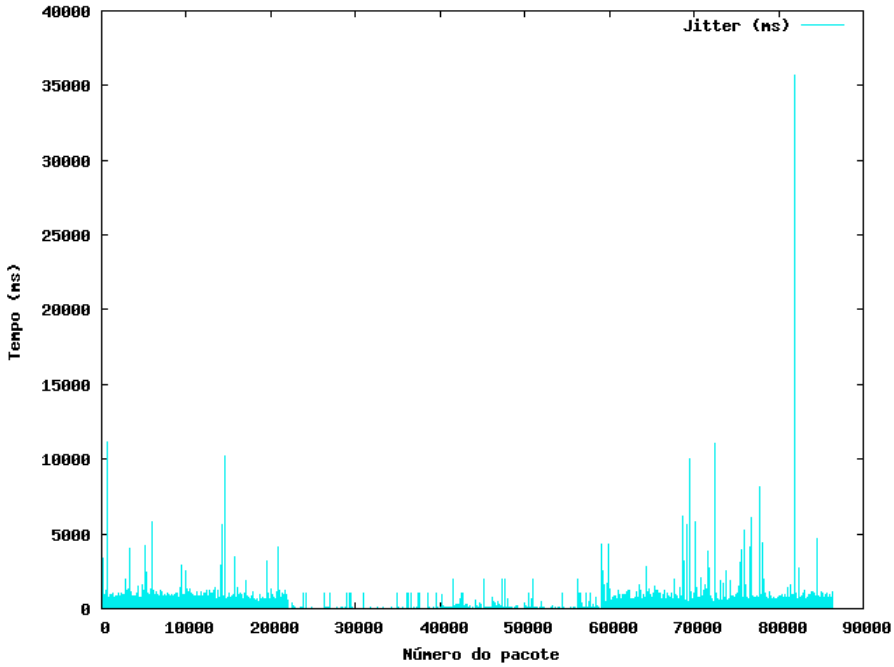


Figura 73: Valores do jitter para o nó 14

O nó 14 (Figura 73) apresentou os piores valores, chegando a obter picos de 35 segundos. Entretanto, até o pacote de número 70000 as variações se mantiveram em torno de 1,5 segundos. Em caso de uma transmissão sensível a estas variações, ela seria razoavelmente bem sucedida no intervalo entre os pacotes de número 20000 até o pacote de número 60000.

A observação dos gráficos implica que existem períodos de estabilidade e períodos de alta instabilidade para todos os nós. Um estudo mais detalhado das condições de propagação entre os nós da rede externa poderia esclarecer se existem fenômenos esporádicos ocorrendo no período de 24 horas ou se estas variações são resultados unicamente de uma falha do protocolo e da métrica de roteamento. De qualquer maneira, mais uma vez pode-se prever que uma métrica baseada no atraso poderia definir com maior precisão os estados dos enlaces. Entretanto, se ocorrem fenômenos fora do controle como um enlace de alta potência operando em determinados horários ou algum equipamento com alta capacidade de geração de ruído sendo esporadicamente ligado, apenas o aprimoramento da métrica não seria suficiente.

5.3.4 Estatísticas de uso

Tendo em vista parâmetros técnicos de qualificação da rede vistos nas subseções anteriores, neste momento será demonstrado o quanto a rede tem sido efetivamente utilizada. Os resultados que serão demonstrados foram obtidos a partir do módulo de autenticação *wifidog*. Os valores apresentados foram obtidos até Setembro 2006, observando que a rede externa passou a operar a partir de Abril deste mesmo ano, com a instalação dos primeiros nós da rede externa.

Apesar do principal objetivo do projeto Remesh ser a pesquisa acadêmica, a utilização da rede depende de usuários reais, exigindo uma determinada qualidade na manutenção da rede. Como a rede em malha do projeto não é um serviço comercial, não se dispõem de técnicos disponíveis 24 horas para a manutenção. Entretanto, a rede foi bem utilizada trazendo resultados bem satisfatórios (Figura 74). A obtenção de novas estatísticas de utilização irá reportar valores ainda mais elevados de utilização.

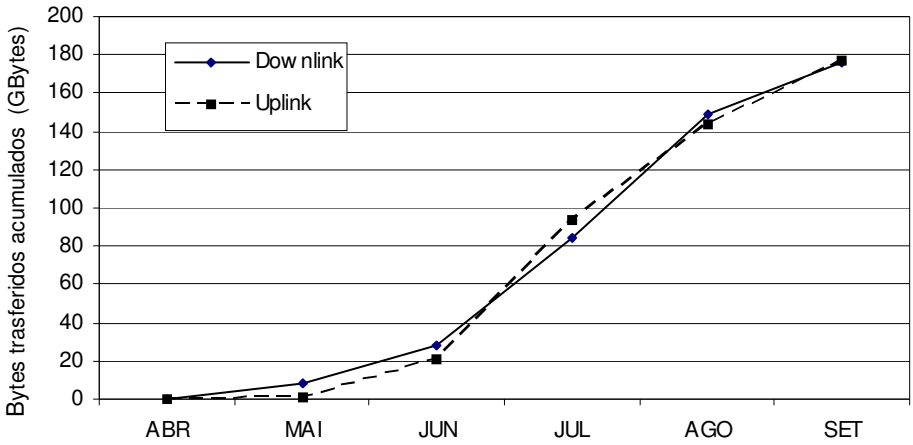


Figura 74: Quantidade de bytes transferidos na rede do projeto Remesh

Em apenas 6 meses de utilização a rede alcançou patamares de utilização bem altos. Isto é devido ao alto grau de utilização dos voluntários, que são, na maior parte, estudantes e também ao fato da rede disponibilizar utilização de todos os serviços disponíveis na Internet, incluindo aplicações P2P (*Peer to Peer).* A seguir será apresentada uma seqüência de estatísticas de uso da rede externa, obtidas pelo *wifidog*.

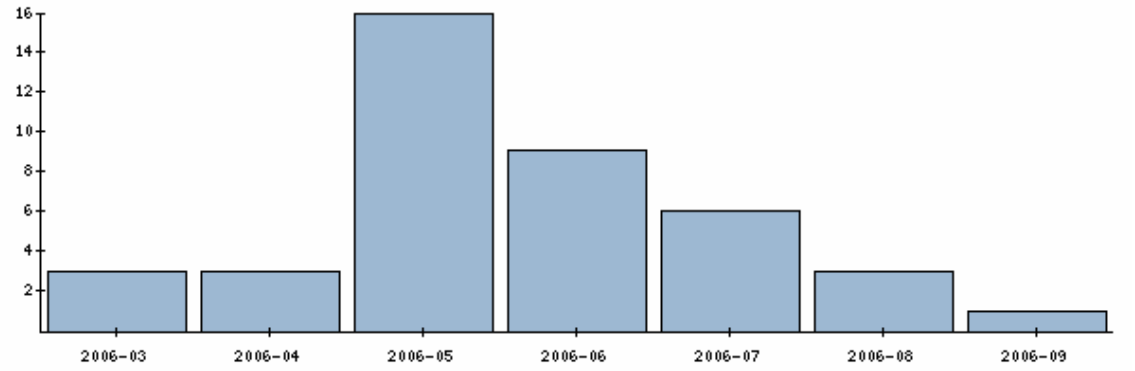


Figura 75: Número de novos usuários cadastrados por mês

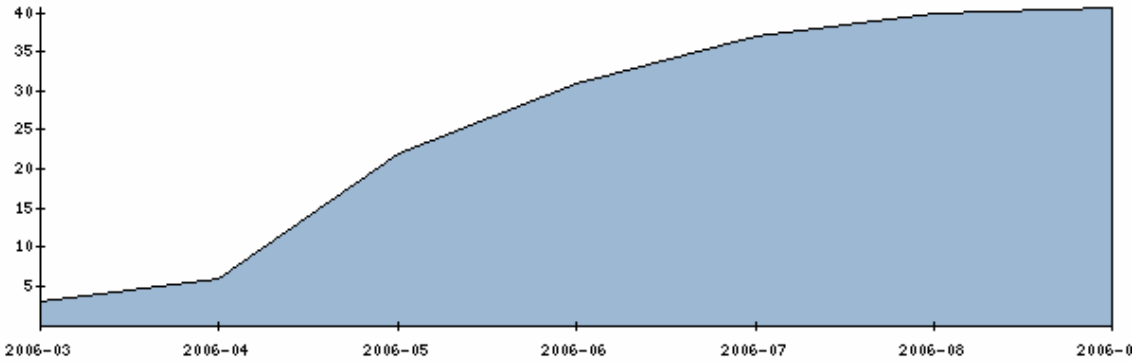


Figura 76: Número acumulativo de novos usuários cadastrados

Na medida em que a rede aumentou o número de roteadores externos, novos usuários começaram a surgir, além dos voluntários (Figura 75 e76).

Usuário	***Incoming***	***Outgoing***	**Total**
pascoal	90,6G	107,6G	198,1G
fidi	27,9G	30,2G	58,2G
rtoso	7,3G	482,6M	7,8G
dvianna	6G	729,9M	6,7G
rcapua	6,2G	396,2M	6,6G
jviana	1,2G	1,5G	2,7G
alvaro	2,2G	499,2M	2,7G
tom	1,1G	133,5M	1,2G
luizedu	1,1G	93,1M	1,2G
douglas	678,4M	248,3M	926,8M

Tabela 13: 10 usuários que mais consomem banda

Usuário	**Dias diferentes conectados**
dvianna	82
pascoal	67
fidi	59
rcapua	54
luizedu	28
lisieux	27
vthome	25
alvaro	24
rtoso	21
douglas	15

Tabela 14: 10 usuários mais freqüentes

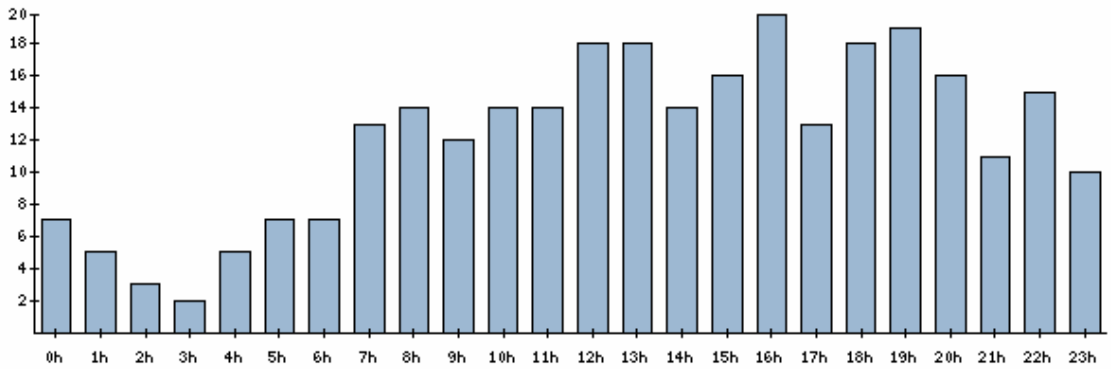


Figura 77: Número de novas conexões abertas por hora do dia

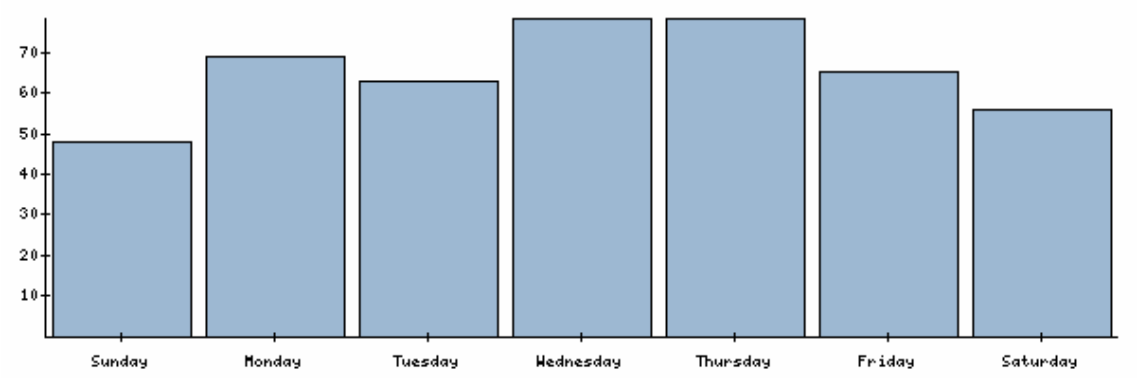


Figura 78: Número de visitas individuais dos usuários por dia da semana

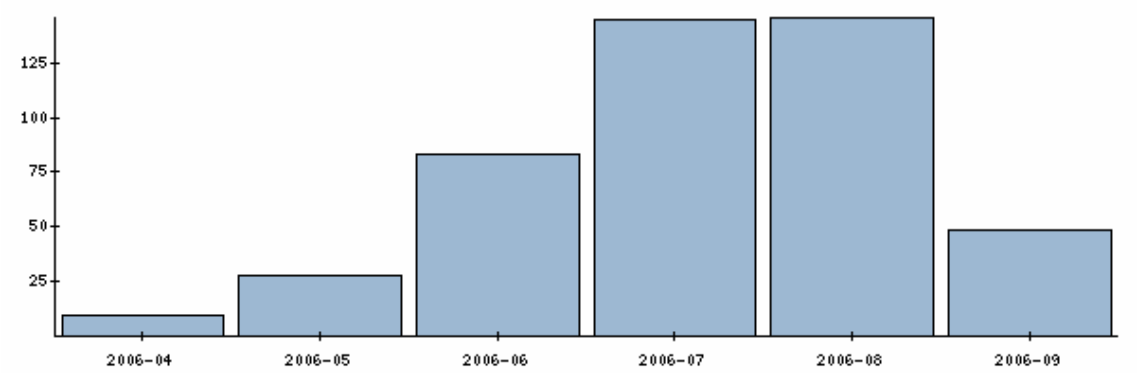


Figura 79: Número de visitas individuais dos usuários por mês

Nó	Visitas
4	157
7	149
1	78
14	54
11	16
13	3
Total:	**457**

Tabela 15: Nós mais populares por visita

Observação: Uma visita é uma contagem de conexões, porém considerando apenas uma conexão por dia para cada usuário em um determinado nó.

As estatísticas exibidas nas Figuras 77, 78 e 79 e nas Tabelas 11, 12 e 13, demonstram que a rede externa tem sido amplamente utilizada. Uma avaliação mais acurada poderia

incluir a estes resultados entrevistas com os usuários mais freqüentes. Pode-se concluir que o objetivo de oferecer Internet com taxas altas para os voluntários tem sido alcançado com êxito.

6 CONCLUSÕES

O projeto Remesh foi a primeira experiência universitária brasileira na implantação de uma rede do tipo mesh em um ambiente externo urbano, propiciando acesso à Internet para voluntários a partir de suas residências. Este trabalho relatou o primeiro ano de execução do projeto realizado na UFF e financiado pela RNP, com ênfase nas realizações do autor deste trabalho: desenvolvimento do protótipo, abrangendo os equipamentos escolhidos, o sistema operacional, os parâmetros de configuração, o modelo de endereçamento e os aplicativos para autenticação de usuários e gerenciamento. Outra contribuição descrita foi a metodologia desenvolvida para a montagem e resolução de problemas que surgiram nos enlaces externos ao longo tempo. Questões referentes à propagação foram pertinentes para a manutenção e a construção da topologia da rede. Em vista disto, foram utilizados modelos de propagação simplificados e empíricos, aliados aos resultados de diversas medições comparativas. O protocolo de roteamento foi um elemento de grande esforço de pesquisas e análises para a melhoria do desempenho da rede. O resultado deste esforço foi a proposta de uma pequena alteração, porém com grande diferença nos resultados, na implementação original do protocolo OLSR. Por fim, diversas medições tomando-se o usuário final como referência, corroboraram a funcionalidade do protótipo.

As redes mesh são aquelas onde os nós de encaminhamento da rede são equipados com interfaces sem fio do padrão *wi fi* (padrão IEEE 802.11), proporcionando o roteamento e o acesso aos usuários simultaneamente. Elas operam em faixas de freqüências livres (ISM), não exigindo outorga ou licenciamento por parte de órgãos reguladores (até o presente momento). Elas utilizam o modo de acesso *ad hoc,* preconizado pelo padrão IEEE 802.11 nas extensões a/b/g. Neste modo, os nós comunicam-se diretamente entre si, sem a necessidade de um elemento de coordenação, disputando o meio.

A tecnologia IEEE 802.11 tem evoluído rapidamente nos últimos. Desde meados da década de 90, quando efetivamente surgiu, diversas novas extensões vêm sendo agregadas ao padrão. Tal evolução é um reflexo da ampla aceitação da tecnologia por parte dos mercados e das comunidades científicas. A padronização e a interoperabilidade dos diferentes equipamentos têm grande influência nesta disseminação.

Paralelamente, o desenvolvimento de protocolos na camada de rede que aproveitam as características da tecnologia também vem evoluindo. Técnicas inteligentes e eficientes de qualificação dos enlaces e de descobrimento das topologias propiciam aos desenvolvedores e pesquisadores um excelente campo de pesquisa, extremamente desafiador e atraente. Tais métricas e técnicas, através de protocolos de roteamento colaborativos, proporcionam o encaminhamento de pacotes por rotas selecionadas dinamicamente. Criando-se desta forma *backbones* sem fio para o tráfego de pacotes através de múltiplos saltos.

Neste ponto, torna-se necessária uma distinção entre as redes *ad hoc* e as redes mesh. As redes mesh são redes *ad hoc* onde se espera uma baixa mobilidade dos nós encarregados do encaminhamento dos pacotes e, normalmente, a ausência de questões como o consumo de energia (BRUNO *et al,* 2005). Estas características são necessárias à finalidade que as redes mesh se propõem: o fornecimento de intercomunicação e de acesso comunitário, estendendo as áreas de abrangência, tipicamente curtas, que as tradicionais redes locais sem fio (WLANS) proporcionam.

Aliada a estas características, tem-se o baixo custo inerente das redes mesh. Operando em uma faixa do espectro livre, utilizando equipamentos cada vez mais baratos e com o crescente desenvolvimento de protocolos de roteamento e aplicativos de código aberto, os gastos necessários à montagem das redes tornam-se irrelevantes quando comparados com outras tecnologias de acesso sem fio (redes celulares e *WiMax*, por exemplo). O baixo custo ocasiona na facilidade e rapidez na montagem dos equipamentos e na implantação da rede.

No Brasil, os custos aos serviços de acesso à Internet com altas taxas ainda são muito elevados. Uma situação comum dentro das universidades é a presença de diversos alunos provenientes de outros estados e municípios, que saem de suas cidades de origem para morarem próximos aos *campi*. No caso da UFF, muitas vezes estes alunos procuram morar em *repúblicas,* dividindo os custos de habitação. Geralmente, a baixa renda não os possibilita de arcarem com os custos de um acesso à Internet em suas residências. Foi neste escopo que o projeto Remesh surgiu. Baseado em experiências de redes mesh universitárias em outros

países, o projeto se dispôs a construir um protótipo próprio para o provimento de acesso à alunos e funcionários voluntários da UFF.

Por meio de muitas pesquisas e esforços na busca de soluções que barateassem os custos, o protótipo foi construído (durante o ano de 2006) com um valor médio de R$500,00 e máximo de R$1.000,00. Esta variação no preço é decorrente dos seguintes fatores: gastos adicionais resultantes das condições de instalação, exigindo cabos CAT-5 com proteção externa e *hardwares* de montagem mais robustos; modelos e marcas dos elementos que compõem o protótipo, incluindo o próprio roteador; presença de equipamentos de aterramento; contratação de mão-de-obra auxiliar para a instalação; utilização de múltiplas antenas; dentre outros.

Utilizando uma rede de testes dentro das dependências da universidade, as dificuldades puderam ser superadas e novas soluções foram propostas antes das instalações externas serem realizadas. Este modelo de prototipagem foi fundamental para os bons resultados alcançados e para a repercussão do projeto. Resultados estes refletidos na publicação de vários artigos, na realização de cursos e de palestras. Abaixo, estão listados os principais resultados obtidos por este trabalho:

- Participação ativa na construção de uma rede mesh externa, utilizando antenas de alto ganho, cabos de baixas perdas e caixas herméticas plásticas, provendo acesso gratuito à Internet para os voluntários moradores próximos às redondezas do *campus* da UFF;
- Construção de um protótipo de um roteador mesh, escalável, facilmente reproduzível e com soluções de baixo custo:
  - Sistema operacional embarcado de código aberto, o OpenWrt (herança do projeto VMesh; TSARMPOPOULOS *et al,* 2005); que oferece um bom grau de liberdade para desenvolvimento e alterações dos aplicativos, além de um grande número de ferramentas prontas;
  - Utilização de um roteador de fácil acesso e de custo relativamente acessível no mercado nacional (WRT54G), outra herança do projeto VMesh;
  - Desenvolvimento de um módulo não padrão, porém funcional, para o fornecimento de energia a partir da residência do usuário (módulo POE descrito no Capítulo 3);
  - Utilização de um protocolo de código aberto, o OLSR (herança do VMesh);

  - Adaptação de ferramentas de código aberto para a autenticação, segurança e acompanhamento dos acessos e do tráfego (*wifidog* e o MRTG);
  - Desenvolvimento de ferramentas próprias em código aberto para acompanhamento via *web* de informações sobre as qualidades dos enlaces e configurações internas, disponibilizadas através de *plugins* já presentes no protocolo de roteamento (*olsrd topology-view* e *http-info*). Tais ferramentas foram influenciadas pelas que foram desenvolvidas no projeto Meshnet (CANDEM *et al,* 2004);
  - Utilização de aplicativos de código livre para a realização das medições (*ping,* scripts em *bash* e *Iperf*), destacando as que foram realizadas na rede externa;

- Desenvolvimento de um esquema de endereçamento que, atuando em conjunto com o protocolo de roteamento, fornece acesso cabeado e sem fio, simultaneamente ao encaminhamento de pacotes (partindo de modelo original herdado do projeto VMesh);
- Participação no desenvolvimento de uma extensão na métrica de roteamento do protocolo OLSR, capaz de apresentar um alto ganho no desempenho, dependendo do tipo da topologia da rede (PASSOS *et al,* 2006).

. Dentre os projetos em redes mesh pesquisados, muitas são as semelhanças entre os projetos Remesh e o VMesh. Os motivos são explicitados no Capítulo 2, através de duas características do projeto Vmesh: (1) o objetivo do projeto VMesh é fornecimento de acesso à Internet para a comunidade acadêmica, onerando o usuário apenas com o custo da compra do equipamento; (2) a busca de uma solução para um protótipo de custo mais acessível. O projeto VMesh, na sua fase preliminar, procurou adotar o mesmo modelo utilizado no projeto Roofnet empregando PC's, devidamente adaptados, como roteadores da rede. Este paradigma demonstrou ser excessivamente custoso e levou os pesquisadores do projeto a adotarem roteadores comerciais alterando o *firmware* original.

Contudo, em termos de vazão, o projeto Remesh teve melhores resultados. Embora muito pouca informação acerca do desempenho esteja disponível na referência do projeto VMesh, é relatado que na rede interna, a taxa de quadros de nível de enlace alcançada é da ordem de 4400 kbps. No projeto Remesh, taxas típicas com fluxos TCP entre dois nós vizinhos na rede interna alcançam valores acima de 8000 kbps (vide Figura 39).

Quanto ao projeto Roofnet, as taxas de vazão TCP entre dois nós vizinhos na rede externa ficam em torno de 2451 kbps (BICKET *et al,* 2005), utilizando roteadores dentro do

padrão 802.11b. No projeto Remesh, as taxas entre dois nós vizinhos ficam acima de 3 Mbps (vide Figura 63) utilizando roteadores no padrão 802.11g. Entretanto, vale ressaltar que a rede externa, apesar de operar no modo automático para a seleção da taxa de interface, apresentou como valor médio de operação 11 Mbps durante o período das medições (mantendo a validade da comparação). Ainda, no projeto Roofnet, a média para dois saltos ficou em torno de 771 kbps com fluxo TCP unidirecional. Utilizando novamente a Figura 63, pode ser verificado que para fluxos TCP unidirecionais, os valores de vazão para os nós que tipicamente estão a dois saltos do *gateway* (nós 11, 14 e 13) as taxas de vazão ficam acima de 1 Mbps. Para fluxos TCP bidirecionais concorrentes, as taxas de vazão para estes mesmos nós ficam em torno de 500 a 700 kbps. Entretanto, em termos do número de nós participantes, o projeto Remesh é bem menor do que o Roofnet que possui atualmente um total de 20 nós externos ativos (ROOFNET HOME PAGE, 2007). Deve-se ressaltar que as condições financeiras para a aquisição dos equipamentos são muito melhores nos EUA (especificamente em Cambridge, Massachusetts, onde está localizada a rede do Roofnet) em comparação com o Brasil. Isto é fundamental, pois no Roofnet muitos voluntários disponibilizaram os equipamentos a partir dos seus próprios recursos.

Em termos de qualidade de acesso à Internet para o usuário final, a rede do projeto Remesh apresentou valores bastante razoáveis em comparação com os padrões vigentes no Brasil. Como pode ser visto na Figura 62, nos enlaces da rede externa tipicamente a dois saltos do *gateway* (nós 11, 13 e 14), as taxas médias obtidas com fluxos TCP bidirecionais concorrentes ficaram em torno de 500 kbps ao longo de três diferentes momentos do dia. Os enlaces diretos ao *gateway* obtiveram valores bem superiores, variando de 1 Mbps até a 4,250 Mbps (nó 4). Entretanto, como pode ser visto na mesma figura, os valores de desvio padrão não foram baixos para os nós 11 e 14, alcançando patamares próximos às médias. Isto indica que estes nós sofrem de uma flutuação muito grande na qualidade da navegação. Para tráfego *web,* geralmente caracterizado por rajadas de acessos, estas flutuações podem não representar desconfortos significativos para os usuários. Contudo, para aplicações que exigem fluxos contínuos, isto passa a ser um problema. Ainda utilizando o nó 14 como exemplo, pode ser visto na Figura 68 e na Figura 73 os altos valores de atraso e de *jitter*, respectivamente. Para tráfego TCP, estes resultados tornam-se ainda mais agravantes. Devido ao controle de congestionamento, os altos valores de atraso são “compreendidos” pelo protocolo como perdas de fragmentos, exigindo muitas vezes a retransmissão do pacote inteiro. Este comportamento pode ser o motivo para a alta variabilidade que o nó 14 obteve na vazão. A

mesma explicação pode ser aplicada para o nó 11. Os demais nós não obtiveram variâncias significativas em comparação com as médias.

Em termos de aplicativos, a primeira fase do projeto se preocupou em desenvolver aqueles que eram essenciais para que houvesse os mecanismos básicos para o controle, acesso e manutenção da rede. Sem as ferramentas desenvolvidas, as visitas nos locais onde os nós estão fisicamente instalados teriam que ser feitas com freqüência quase diária, ocasionando em atrasos significativos no andamento das demais metas do projeto. Em sua segunda fase, novas ferramentas de gerência baseadas em XML estão sendo desenvolvidas (MUCHALUAT-SAADE *et al,* 2007), de maneira semelhante à ferramenta MeshViz do projeto Meshnet. As novas ferramentas proporcionam um conforto maior na administração da rede, pois automatizam a realização de medições que antes que eram obtidas apenas manualmente com a execução de scripts em linhas de comando (interface de interação do usuário com o roteador disponibilizada pelo OpenWrt).

6.1 TRABALHOS FUTUROS

Apesar dos bons resultados obtidos, problemas que surgiram ao longo do projeto demonstram algumas deficiências e merecem atenção para trabalhos futuros:

- A desigualdade na banda disponível quando há geração e encaminhamento de tráfegos simultâneos no mesmo nó *wi-fi* (BENSAOU *et al,* 2000). Considere uma topologia de dois saltos com três nós adjacentes onde dois nós desejam transmitir para o mesmo nó de destino, o nó de uma das pontas e o nó intermediário. Diferentemente do que é preconizado pelo padrão IEEE 802.11 (IEEE 802.11), a banda total disponível entre o nó intermediário e o de destino não é dividida igualmente entre os dois fluxos transmitidos. O nó intermediário dá preferência para o seu próprio fluxo de pacotes, deixando os que deveriam ser encaminhados com uma parcela abaixo da metade da banda total disponível. Este problema também é conhecido como a questão da "injustiça" ou desigualdade no acesso ao meio com o padrão IEEE 802.11. Medições utilizando rotas estáticas na rede interna, onde a topologia apresenta nós fisicamente adjacentes, foram realizadas e comprovaram o problema (HIDEKI, 2006).
- Em DIGGAVI *et al* (2004) é apresentado um trabalho que demonstra o quanto as taxas de transmissões podem aumentar com a utilização de diversidade espacial em

rádios 802.11 a/b/g. No Capítulo 3, foi demonstrado através de medições de vazão, que o mecanismo de diversidade espacial do roteador WRT54G é deficiente (Figura 29, Figura 30 e Figura 31). No mesmo capítulo, também foi demonstrado que duas antenas totalmente distintas (omni e direcional) podem alternar entre si no melhor desempenho dos enlaces ao longo do dia (Tabela 6). O presente trabalho propôs um modelo para a construção de um módulo que escolha a melhor antena dinamicamente no momento de cada transmissão, de acordo com as condições do meio. O projeto foi iniciado, porém não concluído, ficando para um trabalho futuro;

- A rede interna obteve valores bem melhores para as taxas de perda de pacotes, latência a estabilidade das rotas com a utilização do OLSR-ML, em comparação com o OLSR-ETX (Figura 36, Figura 37 e Figura 38). Entretanto, os resultados não foram semelhantes na rede externa, aonde ambos os protocolos (OLSR ML e ETX) apresentaram quesitos com melhor e pior desempenhos. Este resultado exige que estudos sobre métricas mais acuradas (que definam melhor a qualidade dos enlaces) sejam feitos. Em PASSOS e ALBUQUERQUE (2007) novas métricas foram propostas com melhores resultados em comparação com OLSR-ML e ETX. Contudo elas ainda não foram testadas na rede externa;
- A rede apresenta deficiências na segurança no tráfego dos dados por não haver criptografia na camada de enlace (como WPA – "*Wi-Fi Protected Access*", por exemplo).

As deficiências encontradas ao longo do projeto resultaram na proposta de um conjunto de trabalhos futuros. Além dos que já foram mencionados, outros trabalhos podem ser propostos:

- Trabalhos, como o descrito em KOKSAL *et al* (2006), demonstram como a utilização de múltiplos canais pode aumentar a vazão total da rede, mesmo utilizando apenas um rádio. A escolha sincronizada entre os canais disponíveis pode melhorar o desempenho global da rede, elegendo os menos congestionados. Além disto, esta técnica pode permitir que os nós proporcionem acesso para duas ou mais sub-redes distintas de usuários sem fio, sem que elas interfiram entre si;

- Técnicas mais eficientes de acesso ao meio do padrão IEEE 802.11 podem ser estudadas, alterando-se parâmetros do modo básico (CSMA-CA) ou do modo com utilização de RTS/CTS (CHEBROLU *et al,* 2006 e BIANCHI, 2000). Entretanto, analogamente ao projeto de diversidade de antenas, seria necessária a atuação direta no *driver* da interface sem fio. Outro obstáculo neste esforço é que determinados parâmetros de acesso do padrão, como o tamanho inicial da janela de contenção e o número de vezes que o *backoff* exponencial ocorre, são *hardcoded,* ou seja, estão implementados diretamente no hardware (BIANCHI, 2000);
- Construção de protótipos próprios, utilizando dispositivos *wi fi* com *drivers* totalmente programáveis (disponíveis, por exemplo, em DEFACTO WIRELESS, 2007), eliminando alguns problemas de acesso a parâmetros do hardware. Outra proposta nesta direção é a criação de dispositivos com múltiplos rádios, como é utilizado na solução da CISCO (CISCO WIRELESS MESH, 2006).

6.2 CONSIDERAÇÕES FINAIS

As redes mesh propõem um conjunto de novos temas para pesquisas. As propostas mencionadas se referem às camadas de enlace e de rede. Entretanto, inúmeras outras idéias podem ser propostas nas outras camadas. Por exemplo, adaptação do TCP para transmissões mais eficientes na interface sem fio. Aplicativos distribuídos para determinados serviços em ambientes com infra-estrutura mesh, dentre outros.

Diferentemente do que é preconizado por alguns autores (STEELE *et al,* 2002), as redes IEEE 802.11, modo *ad hoc* ou estruturado, não atuam somente como tecnologias de acesso complementares às redes WiMax. Tomando como exemplo as soluções da CISCO (CISCO WIRELESS MESH, 2006) e da Nortel (ROCH, 2005), redes mesh podem ser montadas para cobrirem áreas metropolitanas com alto grau de qualidade e escalabilidade. Entretanto, ambas as soluções apresentam custos muito altos, na ordem de alguns milhares de reais para apenas um nó roteador (MUCHALUAT-SAADE *et al*, 2007), além de exigirem a implantação de outros equipamentos adicionais (como pode ser visto na Figura 5 e na Figura 6, no Capítulo 2), o que dificulta a implantação em larga escala.

Existem vários campos de atuação comercial para as redes mesh. Elas podem ser utilizadas como redes de "emenda", interligando duas regiões distintas através de uma área onde não se podem realizar obras de infra-estrutura (como por exemplo, reservas florestais ou regiões tombadas como patrimônio histórico). Outra utilidade é que elas oferecem uma solução de fácil implantação e de baixo custo para o provimento de acesso na chamada "última milha". Este termo se refere à parte que interliga o acesso do usuário final à estrutura do serviço (*backbones* e centrais de distribuição, por exemplo). Muitas pesquisas são feitas no esforço de se obter novas tecnologias menos custosas (que exijam menos obras de infra-estrutura) e que proporcionem facilidades de gerência e de tolerância a falhas. Além disso, no momento em que a TV Digital for efetivamente implantada no Brasil, as redes mesh (dependendo da topologia e da quantidade de nós instalados) podem fornecer uma solução para o canal de retorno proveniente dos tráfegos individuais dos usuários.

Finalizando, as redes mesh possuem a vantagem de poderem fornecer uma infra-estrutura de acesso de baixo custo, de fácil planejamento e com capacidade de implantação incremental sob demanda. Tais características possuem um impacto direto para a cobertura de regiões como as favelas. Na cidade do Rio de Janeiro, por exemplo, a maior parte das favelas estão localizadas em regiões montanhosas, onde os custos das obras para implantação de infra-estruturas de acesso tradicionais são muito altos e, provavelmente, sem a perspectiva de obtenção do retorno financeiro necessário. Soluções de enlaces rádios ponto-a-ponto ou ponto-multiponto também sofreriam dos mesmos problemas de custo, pois, nas favelas, a maior parte das habitações são casas ou conjuntos habitacionais, exigindo a instalação de enlaces distintos para cada localidade e, eventualmente, de repetidores para superar os obstáculos geográficos. Neste âmbito, as redes mesh fornecem uma solução imediata para a questão da inclusão digital, atualmente tão discutida em debates políticos e sociais no Brasil.

REFERÊNCIAS

4G-SYSTEMS. *4g-systems solution*.Site da empresa que vende uma solução mesh proprietária. Disponível em: http://www.4g-systems.biz/. Acessada em Fevereiro de 2007.

ABELEM, ALBUQUERQUE, MUCHALUAT-SAADE, AGUIAR, DUARTE, FONSECA, MAGALHÃES. "*Redes Mesh: Mobilidade, Qualidade de Serviço e Comunicação em Grupo*", publicado no Livro de Minicursos do SBRC 2007, Belém, PA, maio de 2007.

AGUAYO, D.; BICKET, J; BISWAS, S; JUDD, G.; MORRIS, R. "*Link level Measurements from an 802.11b Mesh Network*", SIGCOMM 2004. Agosto de 2004.

AKYILDIZ, I. F.; WANG, X.; WANG, W. "*Wireless Mesh Networks: a survey*", IEEE Communications Magazine, Volume: 43, Issue: 9. Setembro de 2005.

ANACHIP CORP. Fabricante do chip AC1501-03 presente nos roteadores. Página:http://www.anachip.com.tw. Último acesso realizado em Fevereiro de 2007.

ANSI/IEEE Std 802.11, 1999 Edition (R2003), 802.11: Part 11: *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE, LAN/MAN Standard, 1999 (Reaff: 2003).

BALANIS, C. A. "*Antenna Theory: Analysis and Design"*. 3ª edição, John Willey & Sons, Inc. 2005.

BARSOCCHI, P. "*Channel Models for Terrestrial Wireless Communications: A Survey*". Relatório Técnico do Ministério Italiano de Pesquisa e Universidades para o *framework*

"IS-MANET". Abril de 2006. Disponível em: http://dienst.isti.cnr.it/Dienst/UI/2.0/Describe/ercim.cnr.isti/2006-TR-16?tiposearch=cnr&langver= .

BENSAOU, B.; WANG, Y.; KO, C.C. "*Fair medium Access in 802.11 based Wireless Ad-hoc Networks"*. IEEE/ACM - The First Annual Workshop on Mobile Ad Hoc Networking &Computing (MobiHoc'00), Boston, EUA, Agosto de 2000.

BIANCHI, G. "*Performance Analysis of the IEEE 802.11 Distributed Coordination Function*". IEEE Journal on Selected Areas in Communications, vol. 18, n° 3. Março de 2000.

BICKET, J.; AGUAYO, D.; BISWAS, S.; MORRIS, R. "*Architecture and Evaluation of an Unplanned 802.11b Mesh Network*", Mobicom. Agosto de 2005. Disponível em: http://pdos.csail.mit.edu/roofnet/

BOITHIAS, L. "*Radio Wave Propagation"*. Editora McGraw-Hill. Capítulo 6, pp. 144-171. 1987.

BRUNO, R.; CONTI, M.; GREGORI, E. "*Mesh Networks: Commodity Multihop Ad Hoc Networks*", in IEEE Communications Magazine, March 2005.

BÜTTRICH, S. *"Wifi Hardware*". ICTP – School on Radio Based Networking, Trieste, Itália. 2005. Apresentação técnica disponível em: http://wire.less.dk.

CAMDEN, C. HO; RAMACHANDRAN, K.; ALMEROTH, K.; BELDING-ROYER, E. M. "*A Scalable Framework for Wireless Network Monitoring*.", 2o ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots (WMASH), Philadelphia, PA, setembro de 2004. Disponível em: http://moment.cs.ucsb.edu/meshnet/.

CARRANO, R. C.; MARTINS, R. R.; MAGALHÃES, L.C.S. "*The RUCA Project and Digital Inclusion".* In: 5th Latin American Network Operations and Management Symposium, Petrópolis, 2007. Anais do 5th Latin American Network Operations and Management Symposium, Petrópolis, 2007

CHEBROLU, K.; RAMAN, B.; SEM, S. "*Long-Distance 802.11b Links: Performance Measurements and Experience"*.MobiCom'06. Los Angeles, CA. Setembro de 2006.

CISCO WIRELESS MESH. Disponível em http://www.cisco.com/go/wirelessmesh. Acessada em Março de 2006;

CLAUSEN, T.; JACQUET, P. "*Optimized Link State Routing Protocol (OLSR)*", IETF RFC 3626, 2003.

CLAUSEN, T.; JACQUET, P.; MUHLETALER, P.; QAYYUM, A.; LAOUITI, A.; VIENNOT, L."*Optimized Link State Routing Protocol*". IEEE INMIC, Pakistão, 2001.

CORBET, J.; RUBINI, A.; KROAH-HARTMAN, G. "*Linux Device Drivers"*. Editora O' Reilly, 3ª edição, 2005.

COST 231. Página com os relatórios atualizados: http://www.lx.it.pt/cost231/. Última atualização:1999.

COUTO, D.; AGUAYO, D.; BICKET, J.; MORRIS, R. *"A High-Throughput Path Metric for Multi-Hop Wireless Routing",* em ACM MobiCom, San Diego, CA, Setembro de 2003.

DE LA ROCHE, G.; JAFFRÈS-RUNSER, K.; GORCE, J.M. *"On predicting in-building WiFi coverage with a fast discrete approach"*. Mobile Network Design and Innovation, Vol. 2, No. 1, 2007. Disponível em: "http://perso.citi.insa-lyon.fr/gdelaroc//articles/IJMNDI2007.pdf".

DEFACTO WIRELESS. Página da empresa que vende peças para montagem de dispositivos sem fio. http://www.defactowireless.com/. Acessada em Janeiro de 2007.

DIGGAVI, S.N.; AL-DHAHIR, N.; STAMOULIS, A.; CALDERBANK, A.R." *Great expectations: the value of spatial diversity in wireless networks"***.**Proceedings of the IEEE. Volume 92, Issue 2, Fevereiro de 2004. Páginas: 219 – 270

DRAVES, R.; PADHYE J.; ZILL, B. "*Routing in Multi-radio, Multi-hop Wireless Mesh Networks*", in ACM MobiCom, Philadelphia, PA, Setembro de 2004 [a].

DRAVES, R.; PADHYE J.; ZILL, B."*Comparison of Routing Metrics for Static Multi-Hop Wireless Networks*", in ACM SIGCOMM, Portland, OR. Agosto de 2004 [b].

DWIGHT, J.; ERWIN, M; NILES, R. *"Using CGI"*. Segunda Edição. Editora QUE. 1997.

EBERT, J.; GRASS, E.; IRMER, R.; KRAEMER, R.; FETTWEIS, G.; STROM, K.; TRANKLE, G.; WIRNITZER, W.; WITMANN, R.; REUMERMAN, H.; SCHULZ, E.; WECKERLE, M.; EGNER, P.; BARTH, U. "*Paving the Way for Gigabit Networking"*. Communications Newsletter. Abril de 2005.

ESTRIN, D; GONVINDAN, R.; INTANAGONWIWAT, C. "*Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks"*. In *Proc. of the Sixth Annual International Conference on Mobile Computing and Networks (MobiCOM 2000)*, Boston, MA, Agosto de 2000.

FORUM.OPENWRT.ORG. Página: http://forum.openwrt.org/viewtopic.php?id=6140. Acessada em Julho de 2007.

GOOGLE EARTH. Página: http://earth.google.com. Último acesso realizado em Janeiro de 2006.

GOOGLE MAPS. Página: http://maps.google.com. Último acesso realizado em Junho de 2007.

GOOGLE WIFI. Projeto de acesso sem fio da empresa "GOOGLE". Disponível em http://wifi.google.com. Acessado em Dezembro de 2006.

GRAPHVIZ; Página da aplicação que monta gráficos de topologias a partir de dados no formato *dot*: http://www.graphviz.org. Acessada em Julho de 2006.

GRISWOLD, W. G.; SHANABAN, P.; BROWN, S. W.; BOYER, R.; RATTO, M.; SHAPIRO, R. B.; TRUONG, T. M. "*ActiveCampus -Experiments in Community-Oriented Ubiquitous Computing*", IEEE Computer. Outubro de 2004.

HAUSER, J.; BAKER D.; *IEEE P802.11, Wireless LANs*. Draft PAR for IEEE 802.11 ESS Mesh. 2003.

HIDEKI, L. "*Medição de throughput nas redes em malha sem fio*". Projeto final de graduação em Engenharia de Telecomunicações. Universidade Federal Fluminenese, Dezembro de 2006. Disponível em http://www.midiacom.uff.br/~schara/alunos/leonardo-mt.pdf.

HIDEKI, L. MARTINS, R.R. GUERRANTE, A. CARRANO, R. MAGALHÃES, L.C.S." *Evaluating the impact of RTS-CTS in OLPC's XOs' Mesh Networks*". In: XXV Simpósio Brasileiro de Telecomunicações (SBrT'07), 2007, Recife. Anais do XXV Simpósio Brasileiro de Telecomunicações (SBrT'07), 2007.

HYPERTEC. Fabricante das antenas utilizadas no projeto Remesh. Página: http://www.hypertec.com.br/. Último acesso: Fevereiro de 2007.

IEEE 802.11. Página oficial do grupo: http://grouper.ieee.org/groups/802/11/main.html. Último acesso realizado em Juno de 2007.

IMAGEMAGICK; Página do utilitário que constrói animações a paritr de seqüências de imagens: http://www.imagemagick.org. Acessada em Julho de 2006.

JADHAV, S. BROWN, T. X. DOSHI, S. HENKEL, D. THEKKEKUNNEL, R. G. "*Lessons learned constructing a wireless ad hoc network test bed*" 1st International Workshop on Wireless Network Measurements, 2005.

JAMSA, K.; KLANDER, L. *Programando em C/C++ - A Bíblia*. Editora MakronBooks, 1998.

JOHNSON D.; MALTZ, D.; BROCH J. "*DSR: the dynamic source routing protocol for multihop wireless ad hoc networks*", Ad Hoc Networking, Addison-Wesley Longman Publishing Co., Boston, MA, pp. 139-172, 2001.

JOHNSON, D; MALTZ, D.; HU, U.; JETCHEVA, J. "*The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)",* draft-ietfmanet-dsr-07.txt, RFC 4728. Disponível em: http://www.rfc-editor.org/rfc/rfc4728.txt. Fevereiro 2002.

KIM, J. BOHACEK, S. "*A survey-based mobility model of people for simulation of urban mesh networks*," in *MeshNets*, 2005 (disponível em http://www.eecis.udel.edu/ bohacek).

KOKSAL, C. E.; BALAKRISHNAN, H. "*Quality-Aware Routing Metrics for Time-Varying Wireless Mesh Networks*". IEEE Journal on Selected Areas In Communications,Vol. 24, No. 11. Nov. de 2006. Disponível em: http:// www.ece.osu.edu/~koksal/papers/routing_ent.pdf.

KOKSAL, C. E.; JAMIESON, K.; TELATAR, E. THIRAN, P. "*Impacts of Channel Variability on LinkLevel Throughput in Wireless Networks*". SIGMETRICS Perform. Eval. Junho de 2006. Disponível em http://icapeople.epfl.ch/koksal/papers/paper_chan.pdf.

LAPTOP.ORG. Página oficial do laptop XO desenvolvido pelo MIT: http://laptop.org/laptop/. Último acesso realizado em Julho de 2007.

LAVERGNAT, J. SYLVAIN, M. "*Radio Wave Propagation – Principles and Techinques"*. Johm Wiley & Sons., pp 1-22; 27-121. 2000.

LEON-GARCIA, A. "*Probability and Random Processes for Electrical Engineering"*. Addison-Wesley, 2a Edição; pp. 329-389. Maio de 1994.

LINKSYS – Site da empresa fabricante dos roteadores da família WRT54G utilizados no projeto Remesh: http://www.linksys.com. Acessada em Junho de 2007.

LINKSYS WRT54G POWER SUPPLY. Página: http://kioan.users.uth.gr/wireless/wrt54g/supply.html. Último acesso: Janeiro de 2007.

LOCUSTWORLD site *http://locustworld.com/index.php.* Acessado em Janeiro de 2007.

LU, D. e RUTLEDGE, D. "*Investigation of indoor radio channels from 2.4GHz to 24GHz*", IEEE Antennas and Propagation Symposium (APS/URSI), pp. 134-137. Junho de 2003.

MESHCUBE; Página para download do aplicativo que permite a construção de gráficos de topologias a partir do plugin *olsr_dot_draw* do OLSR e dos utilitários Graphviz e Imagemagik: http://meshcube.org/meshwiki/OlsrTopologyVisualization. Acessada em Agosto de 2006.

MIHSIN, M.; PRAKASH, M. "*IP Address Assignment in a Mobile Ad Hoc Network*", MILCOM 2002.

MOBILE MESH. Solução proprietária de rede mesh da empresa *Mitre.* Página: http://www.mitre.org/work/tech_transfer/mobilemesh/. Último acesso realizado em Julho de 2007.

MRTG; Tobi Oetiker's MRTG - The Multi Router Traffic Grapher. Página da ferramenta - http://oss.oetiker.ch/mrtg/. Acessada em Fevereiro de 2007.

MUCHALUAT-SAADE, D. C.; ALBUQUERQUE, C. V. N.; MAGALHÃES, L. C. S.; PASSOS, D.; DUARTE, J.; VALLE, R. "*Redes em Malha: Solução de Baixo Custo para Popularização do Acesso à Internet no Brasil"*. Recife, SBrT, Setembro de 2007.

NESARGI, S.; PRAKASH, R. "*MANETconf: Configuration of hosts in a mobile ad hoc network*", INFOCOM 2002.

NETSTUMBLER. "*Network Stumbler"*. Página da ferramenta: http://www.netstumbler.com. Acessada em Fevereiro de 2007.

OLSR. Site com a implementação do protocolo OLSR : http://www.olsr.org, acessada em Novembro de 2006.

OPENWRT. Site do sistema operacional Openwrt: http://openwrt.org/, acessada em dezembro de 2006.

OPENWRT-NVRAM; Fórum com uma lista de parâmetros de configuração do sistema operacional OpenWrt. http://wiki.openwrt.org/OpenWrtNVRAM. Acessada em Junho de 2007.

PASSOS, D. G.; TEIXEIRA, D. V.; MUCHALUAT-SAADE, D. C.; MAGALHÃES, L. C. S.; ALBUQUERQUE, C. V. N. "*Mesh Network Performance Measurements"*. I2TS – 5th International Information and Telecommunication Technologies Symposium. Cuiabá, MT, Brasil. Dezembro de 2006.

PASSOS, D.; ALBUQUERQUE, C. V. N. "*Proposta, Implementação e Análise de uma Métrica de Roteamento Multiplicativa para Redes em Malha Sem Fio"*.XXVII Congresso da Sociedade Brasileira de Computação- CTIC. 2007.

PATTERSON, D. A.; HENNESSY, J. L. "*Computer organization and design: the hardware/software interface*". Morgan Kaufmann Publishers, Inc. San Mateo, CA, 964p. 2ª Edição, 1998.

PERKINS, C. E. "*Ad hoc On-Demand Distance Vector (AODV) Routing*", IETF RFC 3561, Disponível em: http://www.ietf.org/rfc/rfc3561.txt. Julho de 2003.

PERSONAL TELCO WIKI. Site com listagem de ferramentas abertas para autenticação de usuários com *Captive e Active Portal*: http://wiki.personaltelco.net/index.cgi/PortalSoftware. Acessada em janeiro de 2007.

PETERSON, L. L.; DAVIE, B. S. "*Computer Networks: A system Approach"*. Morgan Kaufman Publishers; 2ª edição; 1999.

PROJETO REMESH, Rede Mesh de Acesso Universitário Faixa Larga. Site oficial do Grupo de Trabalho Mesh da RNP. http://mesh.ic.uff.br. Acessada em Julho de 2007.

QIU, L. BAHL P. RAO, A.. *Troubleshooting Wireless Mesh Networks***.** Computer Communications Review. 2006.

RAMACHANDRAN, K.; BELDING-ROYER E.; ALMEROTH K. *DAMON: A Distributed Architecture for Monitoring Multi-hop Mobile Networks*, IEEE International Conference on Sensor and Ad hoc Communications and Networks (SECON), Santa Clara, CA, 2004

RAMACHANDRAN, K.; BUDDHIKOT, M. M.; CHANDRANMENON, G.; BELDING-ROYER, E.; ALMEROTH, K.; MILLER, S. "*On the Design and Implementation of Infrastructure Mesh Networks"*. WiMesh, First IEEE Workshop on Wireless Mesh Networks, em conjunto com SECON-2005.

RAPAPPORT, T. "*Wireless Communications"*. Prentice-Hall, 1ª Edição.1996.

RAYCHAUDHURI D., SESKAR I., OTT M., GANU S., RAMACHANDRAN K., KREMO H., SIRACUSA R., LIU H. E SINGH M., *Overview of the ORBIT Radio Grid Testbed for Evaluation of Next-Generation Wireless Network Protocols,* WCNC'05. 2005.

RNP – Rede Nacional de Ensino e Pesquisa: http://www.rnp.br. Acessada em Fevereiro de 2007.

ROAMAD site http:// www.roamad.com/roamad/company. Acessado em Janeiro de 2007.

ROCH, S. "*Nortel's Wireless Mesh Network solution: Pushing the boundaries of traditional WLAN technology*". Nortel Technical Journal, Issue 2, Outbro de 2005. Disponível em: http://www.nortel.com/solutions/ntj/collateral/ntj2_wireless_mesh.pdf

ROOFNET HOME PAGE. Página do projeto Roofnet. Acessada em Setembro de 2007. Disponível em: http://pdos.csail.mit.edu/roofnet/doku.php.

RUSSEL, P. *Unreliable Guide To Hacking The Linux Kernel*. GNU General Public License. 2002.

SANTIVANEZ, C.; CESAR, A.; MCDONALD, B.; STAVRAKAKIS, I.; RAMANATHAN, R. "*On the Scalability of Ad Hoc Routing Protocols*". IEEE INFOCOM, Junho de 2002.

SANTIVANEZ, C.; RAMANATHAN, R. "*Hazy Sighted Link State (HSLS) Routing: A Scalable Link State Algorihm*". BBN Technical Memorandum, No. 1301. Março de 2003.

SAYANDEEP SEN; BHASKARAN RAMAN. *Long Distance Wireless Mesh Network Planning: Problem Formulation and Solution*, Accepted for publication, The 16th Annual International World Wide Web Conference (WWW 2007) Canada, 2007.

SHERESTHA, D. M.; KO, Y. B. "*On Construction of the Virtual backbone in Wireless Mesh Networks".* ICACT2006, Fevereiro de 2006.

SILBERSCHATZ, A. GAGNE, G. GALVIN, P. B."*Operating Systems Concepts"*. Editora Wiley, 6ª edição. 2002.

SKLAR, B. "*Rayleigh fading channels in mobile digital communication systems*" IEEE Communications Magazine, Volume 35, Issue 7, pp. 90-100. Julho de 1997.

SRIDHARA, V. BOHACEK, S. "*Realistic Propagation Simulation of Urban Mesh Networks*". *Department of Electrical and Computer Engineering,* universidade de Delaware, DE 19716. Computer Networks: The International Journal of Computer and Telecommunications Networking. 2007.

STALLINGS, W. "*Wireless Communications and Networks".* Prentice Hall; 1ª edição, 2002.

STEELE, R. LEE C. GOULD, P. "*GSM, cdmaOne and 3G Systems*". John Wiley & Sons. 2001.

STUART J. KERRY, BRIAN MATHEWS. *Fast Roaming Standard to Support Mobile, Voice-Over IP Services; Mesh Standard to Extend Range of WLAN Access Points*. IEEE 802.11r.2004.

TANENBAUM, Andrew S., "*Redes de Computadores*". 4ª. ed. Rio de Janeiro: Elsevier, 2003

TERABEAM. Página com ferramentas de auxílio para o cálculo da zona de fresnel. Disponível em http://www.terabeam.com/support/calculations/fresnel-zone.php. Acessada em Março de 2006.

TIRUMALA, A.; QIN, F.; DUGAN, J.; FERGUSON, J.; GIBBS, K. "*Iperf-The TCP/UDP bandwidth measurement tool*", http://dast.nlanr.net/Projects/Iperf/, 2005.

TOURRILHES, J. "*Wireless LAN Resources for Linux*". Página: http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/. Acessada em Fevereiro de 2007.

TSARMPOPOULOS, N.; KALAVROS, Y.; LALIS, S. "*A Low Cost and Simple-to-Deploy Peer-to-Peer Wireless Network based on Open Source Linux Routers*", Simpósio Brasileiro de Redes de Computadores, Fortaleza, CE, Maio de 2005.

USCB MESHNET. Página do projeto MeshNet da Universidade de Santa Bárbara Califórnia. Página: http://moment.cs.ucsb.edu/meshnet/. Acessada em Setembro de 2007.

WEBER, S.; CAHILL, V. CLARKE, S. HAAHR, M. "*Wireless Ad Hoc Network for Dublin: A Large-Scale Ad Hoc Network Test-Bed*", ERCIM News, vol. 54, 2003. Disponível em http://www.ercim.org/publication/Ercim_News/enw54/weber.html.

WIFIDOG. Página oficial da ferramenta: http://www.wifidog.org. Acessada em agosto de 2006.

WIKIPEDIA; Enciclopédia web livre: http://www.wikipedia.org. Acessada em Janeiro de 2007.

WIMAXFORUM. Página com diversas informações sobre o estado da arte da tecnologia WiMax: http://www.wimaxforum.org/technology/. Acessada em Junho de 2007.

WIND RIVER, página da empresa que desenvolve o sistema operacional VxWorks: http://www.windriver.com/. Acessada em Junho de 2007.

WIRELESS&CIA. Loja virtual de equipamentos sem fio. Página: http://www.wirelessecia.com.br. Último acesso: Julho de 2007.

WL COMMAND – Página com a lista das funcionalidades do arquivo executável “wl” proprietário da Broadcom: http://www.dd-wrt.com/wiki/index.php?title=Wl_command. Último acesso: Fevereiro de 2007.

ANEXOS

ANEXO 1: *Configure_Manet.sh* - Script de configuração de portas

```
#!/bin/ash

if [ $# -ne 1 ]
then
  echo "usage: configure_manet.sh id"
  exit 0
fi

# configuration variables

LAN_IPADDR=10.$((152+($1/2048))).$((($1*32)%65536)/256)).$((($1*32)%256+1))

LAN_NETMASK=255.255.255.224
WIFI_IPADDR=10.151.$(((1+$1)%256)).1
WIFI_NETMASK=255.255.0.0
#coloque aqui o ssid da sua rede!
WIFI_SSID="mesh"
WAN_IPADDR=
WAN_NETMASK=
WAN_GW=
WAN_DNS=
DHCP_FROM=10.$((152+($1/2048))).$((($1*32)%65536)/256)).$((($1*32)%256+2))
DHCP_TO=10.$((152+($1/2048))).$((($1*32)%65536)/256)).$((($1*32)%256+30))
DNSMASQ_FILE=/etc/dnsmasq.conf

# configure lan interface
nvram set lan_ifnames=vlan0
nvram set lan_ifname=vlan0
nvram set lan_proto=static
nvram set lan_ipaddr=$LAN_IPADDR
nvram set lan_netmask=$LAN_NETMASK
nvram unset lan_gateway
nvram unset lan_dns

# configure wifi interface
nvram set wifi_ifname=eth1
nvram set wifi_proto=static
nvram set wifi_ipaddr=$WIFI_IPADDR
nvram set wifi_netmask=$WIFI_NETMASK
nvram unset wifi_gateway
nvram unset wifi_dns
nvram set wl0_mode=sta
nvram set wl0_infra=0
nvram set wl0_ssid=$WIFI_SSID

# configure wan interface
nvram unset wan_ifnames
nvram set wan_proto=static
nvram set wan_ipaddr=$WAN_IPADDR
nvram set wan_netmask=$WAN_NETMASK

#nvram set wan_gateway=$WAN_GW
nvram unset wan_gateway
nvram set wan_dns=$WAN_DNS
nvram set wan_hostname="id"$1
```

```
#DHCP
nvram set dhcp_start=3
nvram set dhcp_num=20

# display settings
echo "LAN Address: "$LAN_IPADDR
echo "LAN NetMask: "$LAN_NETMASK
echo "DHCP LAN: "$DHCP_FROM"-"$DHCP_TO
echo "---"
echo "Wifi Address: "$WIFI_IPADDR
echo "Wifi NetMask: "$WIFI_NETMASK
echo "---"
echo "WAN Address: "$WAN_IPADDR
echo "WAN NetMask: "$WAN_NETMASK
echo "WAN Interface: disabled"
echo "---"
echo "Firewall: disabled"

# commit changes
echo "Writing changes..."
nvram commit
# generate dnsmasq configuration file
echo "domain-needed" > $DNSMASQ_FILE
echo "bogus-priv" >> $DNSMASQ_FILE
echo "filterwin2k" >> $DNSMASQ_FILE
echo "local=/lan/" >> $DNSMASQ_FILE
echo "domain=$WIFI_SSID" >> $DNSMASQ_FILE
echo "except-interface=vlan1" >> $DNSMASQ_FILE
echo "dhcp-authoritative" >> $DNSMASQ_FILE
echo "dhcp-range=$DHCP_FROM,$DHCP_TO,$LAN_NETMASK,12h" >> $DNSMASQ_FILE
echo "dhcp-leasefile=/tmp/dhcp.leases" >> $DNSMASQ_FILE

echo "read-ethers" >> $DNSMASQ_FILE
echo "dhcp-lease-max=30" >> $DNSMASQ_FILE

# turn off firewall
if [ -f /etc/init.d/S45firewall ]
then
   mv /etc/init.d/S45firewall /etc/init.d/s45firewall
fi
# turn on olsrd
if [ -f /etc/init.d/olsrd]
then
    cp /etc/init.d/olsrd /etc/init.d/S53olsrd
fi
```

ANEXO 2: *olsrd.conf* – Arquivo de configuração do OLSR

```
 #
# olsr.org OLSR daemon config file
#
# Lines starting with a # are discarded
#
# This file was shipped with olsrd 0.4.9
#

# Debug level(0-9)
# If set to 0 the daemon runs in the background

DebugLevel      0

# IP version to use (4 or 6)

IpVersion       4

# Clear the screen each time the internal state changes

ClearScreen     no

# HNA IPv4 routes
# syntax: netaddr netmask
# Example Internet gateway:
# 0.0.0.0 0.0.0.0

Hna4
{
#   Internet gateway:
   0.0.0.0      0.0.0.0
#   more entries can be added:
#   192.168.1.0  255.255.255.0
10.152.0.192 255.255.255.224
10.151.7.0 255.255.255.224
}

# HNA IPv6 routes
# syntax: netaddr prefix
# Example Internet gateway:
Hna6
{
#   Internet gateway:
#   ::              0
#   more entries can be added:
#   fec0:2200:106:: 48
}


# Should olsrd keep on running even if there are
# no interfaces available? This is a good idea
# for a PCMCIA/USB hotswap environment.
# "yes" OR "no"

AllowNoInt      yes

# TOS(type of service) value for
# the IP header of control traffic.
# If not set it will default to 16
```

```
#TosValue       16

# The fixed willingness to use(0-7)
# If not set willingness will be calculated
# dynamically based on battery/power status
# if such information is available

Willingness     4

# Allow processes like the GUI front-end
# to connect to the daemon.

IpcConnect
{
    # Determines how many simultaneously
    # IPC connections that will be allowed
    # Setting this to 0 disables IPC

    MaxConnections  0

    # By default only 127.0.0.1 is allowed
    # to connect. Here allowed hosts can
    # be added

    Host            127.0.0.1
    #Host            10.0.0.5

    # You can also specify entire net-ranges
    # that are allowed to connect. Multiple
    # entries are allowed

    #Net             192.168.1.0 255.255.255.0
}

# Wether to use hysteresis or not
# Hysteresis adds more robustness to the
# link sensing but delays neighbor registration.
# Used by default. 'yes' or 'no'

UseHysteresis   no

# Hysteresis parameters
# Do not alter these unless you know
# what you are doing!
# Set to auto by default. Allowed
# values are floating point values
# in the interval 0,1
# THR_LOW must always be lower than
# THR_HIGH.

HystScaling     0.50
HystThrHigh     0.80
HystThrLow      0.30


# Link quality level
# 0 = do not use link quality
# 1 = use link quality for MPR selection
# 2 = use link quality for MPR selection and routing (OLSR-ETX)
```

```
# 3 = use probabilities (OLSR-ML)
# Defaults to 0

LinkQualityLevel        3

# Link quality window size
# Defaults to 10

LinkQualityWinSize      100

# Polling rate in seconds(float).
# Default value 0.05 sec

Pollrate   0.05
#0.05

# TC redundancy
# Specifies how much neighbor info should
# be sent in TC messages
# Possible values are:
# 0 - only send MPR selectors
# 1 - send MPR selectors and MPRs
# 2 - send all neighbors
#
# defaults to 0

TcRedundancy    2

#
# MPR coverage
# Specifies how many MPRs a node should
# try select to reach every 2 hop neighbor
#
# Can be set to any integer >0
#
# defaults to 1

MprCoverage     3

# Olsrd plugins to load
# This must be the absolute path to the file
# or the loader will use the following scheme:
# - Try the paths in the LD_LIBRARY_PATH
#   environment variable.
# - The list of libraries cached in /etc/ld.so.cache
# - /lib, followed by /usr/lib

# Example plugin entry with parameters:

#LoadPlugin "olsrd_dyn_gw.so.0.3"
#{
    # Here parameters are set to be sent to the
    # plugin. Theese are on the form "key" "value".
    # Parameters ofcause, differs from plugin to plugin.
    # Consult the documentation of your plugin for details.

    # Example: dyn_gw params

    # how often to check for Internet connectivity
    # defaults to 5 secs
```

```
#   PlParam     "Interval"   "40"

    # if one or more IPv4 addresses are given, do a ping on these in
    # descending order to validate that there is not only an entry in
    # routing table, but also a real internet connection. If any of
    # these addresses could be pinged successfully, the test was
    # succesful, i.e. if the ping on the 1st address was successful,the
    # 2nd won't be pinged
#   PlParam     "Ping"       "141.1.1.1"
#   PlParam     "Ping"       "194.25.2.129"
#}

LoadPlugin "olsrd_httpinfo.so.0.1"
{
PlParam         "Port"  "8087"
PlParam         "Net"   "0.0.0.0 0.0.0.0"
}

LoadPlugin "olsrd_dot_draw.so.0.3"
{
PlParam         "accept"        "200.20.15.217"
}

# Interfaces and their rules
# Omitted options will be set to the
# default values. Multiple interfaces
# can be specified in the same block
# and multiple blocks can be set.

# !!CHANGE THE INTERFACE LABEL(s) TO MATCH YOUR INTERFACE(s)!!
# (eg. wlan0 or eth1):

Interface "eth1"
{

    # IPv4 broadcast address to use. The
    # one usefull example would be 255.255.255.255
    # If not defined the broadcastaddress
    # every card is configured with is used

    # Ip4Broadcast              255.255.255.255

    # IPv6 address scope to use.
    # Must be 'site-local' or 'global'

    # Ip6AddrType               site-local

    # IPv6 multicast address to use when
    # using site-local addresses.
    # If not defined, ff05::15 is used

    # Ip6MulticastSite          ff05::11

    # IPv6 multicast address to use when
    # using global addresses
    # If not defined, ff0e::1 is used

    # Ip6MulticastGlobal        ff0e::1

    # Emission intervals.
```

```
    # If not defined, RFC proposed values will
    # be used in most cases.

    # Hello interval in seconds(float)
    HelloInterval    2.0
#    HelloInterval    2.0

    # HELLO validity time
     HelloValidityTime  60.0
#     HelloValidityTime 6.0

    # TC interval in seconds(float)
    TcInterval        5.0
#    TcInterval        5.0

    # TC validity time
     TcValidityTime     90.0
#     TcValidityTime    10.0

    # MID interval in seconds(float)
    MidInterval 5.0
#    MidInterval        5.0

    # MID validity time
     MidValidityTime    90.0
#     MidValidityTime   10.0

    # HNA interval in seconds(float)
    HnaInterval 5.0
#    HnaInterval        5.0

    # HNA validity time
     HnaValidityTime    90.0
#     HnaValidityTime   10.0

    # When multiple links exist between hosts
    # the weight of interface is used to determine
    # the link to use. Normally the weight is
    # automatically calculated by olsrd based
    # on the characteristics of the interface,
    # but here you can specify a fixed value.
    # Olsrd will choose links with the lowest value.

    Weight 0


}
```

ANEXO 3: Script medição para o uso de diversidade de antenas

```
#!/bin/sh
data=$(date +%m-%d-%Y-%Hhs)
if [ -f /tmp/ant ];
        then rm /tmp/ant*
fi
touch /tmp/ant
touch /tmp/ant_1
touch /tmp/ant_1_ping
touch /tmp/ant_2
touch /tmp/ant_2_ping
a=0;
tx_ant=$( wl txant | awk '{print $3}')
printf $tx_ant > /tmp/tx_ant

for count in $(seq 2);
do

wl antdiv $a;
wl txant $a;
sleep 4;
flag=0;
ping -c 4 -q 255.255.255.255 -b;
for i in $(cat /proc/net/arp | awk '{if ($6=="eth1") print $1"@"$4}'); do ip=$(echo $i | awk -F @ '{print $1}');
ip_num=$(printf $ip | awk -F . '{ print $4 }'); if [ "$ip_num" = "1" ]; then
echo $a"@"$ip;

mac=$(printf $i | awk -F @ '{print $2}');tempo=0;iperf -c $ip -t 5 -f Mbytes -C -b 5M| awk -F "MBytes"
'{cont=0}{if (cont==0) print $2; cont++}' | awk '{print $1}' > /tmp/b;tempo=$(awk '{if ($0!="") print $0}'
/tmp/b);
rm /tmp/b; if [ "$tempo" != "" ]; then printf "\n"$mac" "$a" "$tempo"\n" >> /tmp/ant_1; fi;
echo $a"@"$ip;

else

mac=$(printf $i | awk -F @ '{print $2}');tempo=0;ping -c 10 $ip | awk -F "time=" '{print $2}' | awk '{print $1}' >
/tmp/c; tempo=$(awk 'BEGIN{t1=0}{t1=t1+$1}END{if ((t1==0)||(t1==""")) print 10000; else print t1}' /tmp/c);
   rm /tmp/c; if [ "$tempo" != "10000" ]; then printf $mac" "$a" "$tempo"\n" >> /tmp/ant_1_ping;fi;

fi;
done;
a=$(expr $a + 1);
done
sort /tmp/ant_1 > /tmp/ant_2_t
sort /tmp/ant_1_ping > /tmp/ant_2_ping_t

#preparo o arquivo para o ultimo awk

awk 'BEGIN{ip="";cont=0;linha=""}{if (($0!="")&&(ip!=$1)&&(ip!="")&&(cont<2)) {print ip" "5" "0; print
$0;cont=1;} else {if ($0!=""){if (cont>1) cont=1; else cont++; print $0;}}ip=$1}END{if (cont<2) print $1" 5
0"}' /tmp/ant_2_t > /tmp/ant_2
awk 'BEGIN{ip="";cont=0;linha=""}{if (($0!="")&&(ip!=$1)&&(ip!="")&&(cont<2)) {print ip" "5" "10000;
print $0;cont=1;} else {if ($0!=""){if (cont>1) cont=1; else cont++; print $0;}}ip=$1}END{if (cont<2) print $1"
5 10000"}' /tmp/ant_2_ping_t > /tmp/ant_2_ping

awk 'BEGIN{ip="";tempo=0; ant=0}{if (ip==$1){if (tempo<$3) {print $1"@"$2} else print ip"@"ant}else
{ip=$1;tempo=$3;ant=$2}}END {print "ff:ff:ff:ff:ff:ff@3"}' /tmp/ant_2 >>/tmp/ant;
```

```
awk 'BEGIN{ip="";tempo=0; ant=0}{if (ip==$1){if (tempo>$3) {print $1"@"$2} else print ip"@"ant}else
{ip=$1;tempo=$3;ant=$2}}' /tmp/ant_2_ping >>/tmp/ant;

rm /tmp/ant_2

tx_ant=$(cat /tmp/tx_ant)
rm /tmp/tx_ant

 wl antdiv 3
 wl txant $txant

cp /tmp/ant /shared/testes/externos/antena/ant_$data
cat /proc/net/arp | grep "eth1"  > /shared/testes/externos/antena/arp_$data
```

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo