UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
PROGRAMA DE PÓS-GRADUAÇÃO EM TECNOLOGIA
CURSO DE ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDE

CHRYSTIAN LUIZ MEGGER

ESTUDO E IMPLEMENTAÇÃO DE QoS EM REDES 802.11g SOB TOPOLOGIA MALHA

MONOGRAFIA

CURITIBA
2011

CHRYSTIAN LUIZ MEGGER

ESTUDO E IMPLEMENTAÇÃO DE QoS EM REDES 802.11g SOB TOPOLOGIA MALHA

Monografia apresentada como requisito parcial para a obtenção do grau de Especialista em Configuração e Gerenciamento de servidores e equipamentos de rede, do Programa de Pós-Graduação em Tecnologia. Universidade Tecnológica Federal do Paraná. Área de Concentração: Redes de Computadores
Orientador: Prof. MSc. Fabiano Scriptore de Carvalho

CURITIBA
2011

RESUMO

MEGGER, Chrystian L. **Estudo e implementação de QoS em redes 802.11g sob topologia malha.** 2011. 64 f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2011.

A presente monografia aborda o estudo para a implementação de técnicas de QoS (qualidade de serviço) em redes locais sem fio atuando em topologia malha. Apresenta as vantagens para utilização da topologia em malha e também a importância de engenhar a priorização do tráfego de dados, de modo que a implementação e aplicação de QoS não seja em vão e possibilite realmente uma melhora exponencial no tráfego priorizado. O projeto inicializa-se utilizando método bibliográfico, seguido de estudo em campo, configuração de equipamentos *wireless access points* e análise dos resultados obtidos. O resultado mostrará a eficácia de uma rede com QoS aplicado e funcionando de acordo com a necessidade de cada administrador da rede.

Palavras-chave: Redes. Qualidade de Serviço. Priorização de Tráfego. Topologia em malha. Redes sem fio.

ABSTRACT

MEGGER, Chrystian L. **Study and implementation of QoS on 802.11g in mesh topology.** 2011. 64 pages. Monograph (Specialization in Configuration and Management of Servers and Network Equipments) - Federal Technological University of Paraná. Curitiba, 2011.

This monograph deals with the study for implementation of QoS (quality of service) techniques on wireless LANs operating in mesh topology. Shows the advantages for using mesh topology and the importance of making the data traffic prioritization, so that the implementation and QoS application is not for nothing and really enables the exponential improvement in prioritized traffic. The project starts with bibliographic method, then will occur the laboratory study, after the *wireless access points* will be configured and then will be analyzed the results. The results going to show the data network working better after the QoS applied, according the network administrator wish.

Keywords: Network, Quality of Service, Traffic Priority, Mesh Topology. Wireless.

LISTA DE SIGLAS

AP – Access Point

ARPA - Advanced Research Projects Agency

BGP - Border Gateway Protocol

BSS - Basic Service Set

CIR - Commited Information Rate

CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance

DNS - Domain Name System

DHCP - Dynamic Host Configuration Protocol

DSCP - Differentiated Services Code Point

DSSS - Direct Sequence Spread Spectrum

ESS - Extended Service Set

FHSS - Frequency Hopping Spread Spectrum

FTP – File Transfer Protocol

GHz – Giga Hertz

GIF - Graphics Interchange Format

GLP - General Public Licence

HTTP - Hypertext Transfer Protocol

ICMP - Internet Control Message Protocol

IEEE - Institute of Electrical and Eletronics Engineers

IP – Internet Protocol

JPEG - Joint Photographic Experts Group

LAN – Local Area Network

LLC - Logical Link Control

MAC - Media Access Control

Mbps - Megabits por Segundo

MIMO - Multiple-Input Multiple-Output

MPEG - Motion Picture Experts Group

MPLS - Multi-Layer Protocol Label Switching

MPR - Multipoint Relays

NAT - Network Address Translation

OFDM - Orthogonal Frequency Division Multiplexing

OLSR - Optimized Link State Routing

OSI - Open Systems Interconnection

OSPF - Open Shortest Path First

PCI - Protocol Control Information

PDU - Protocol Data Unit

PHB - Per-Hop Behavior

QoS – Quality of Service

RFC - Request for Comments

RIP - Routing Information Protocol

RSVP - Resource Reservation Protocol

SDU - Service Data Unit

SIP - Session Initiation Protocol

SLA - Service Level Agreement

SNMP - Simple Network Management Protocol

TCP - Transmission Control Protocol

TCP/IP - Transmission Control Protocol over Internet Protocol

ToS – Type of Service

TTL – Time to Live

UDP - User Datagram Protocol

VoIP – Voice over Internet Protocol

WAN - Wide Area Network

WLAN – Wireless Local Area Network

LISTA DE ILUSTRAÇÕES

Figura 1 Camadas do modelo TCP/IP 18
Figura 2 Sinais da Camada Física 25
Figura 3 Padrões sem fio - Camada Física 25
Figura 4 Topologia em Barramento 26
Figura 5 Topologia em Anel 27
Figura 6 Topologia em Anel 28
Figura 7 Topologia em Anel 28
Figura 8 Topologia em Malha 30
Figura 9 Relação do 802.11 com modelo OSI 32
Figura 10 Canais de Radiofreqüência em 2,4 GHz 33
Figura 11 Cabeçalho IP 40
Figura 12 ToS 41
Figura 13 Marcação PHB-AF 44
Figura 14 Topologia de Estudo de Campo 48
Figura 15 JPerf 49
Figura 16 Configurações Básicas do *Access Point.* 50
Figura 17 Configurações do OLSR no *Access Point.* 51
Figura 18 Habilitando NAT no AP Gateway. 51
Figura 19 Configurando QoS 52
Figura 20 QoS por serviço 53
Figura 21 Testes iniciais 54
Figura 22 Teste Jperf - Destino 55
Figura 23 Teste Jperf - Origem 56
Figura 24 ICMP saturado 56
Figura 25 Pacotes sem QoS 57
Figura 26 QoS configurado 58
Figura 27 Pacotes com QoS 59
Figura 28 ICMP com rede saturada 59
Figura 29 Pacotes com QoS em rede saturada 60

SUMÀRIO

1 INTRODUÇÃO 10
1.1 TEMA 10
1.2 PROBLEMAS E PREMISSAS 11
1.3 OBJETIVOS 12
1.1.3.1 OBJETIVO GERAL 12
1.3.2 OBJETIVOS ESPECÍFICOS 12
1.4 JUSTIFICATIVA 12
1.5 PROCEDIMENTOS METODOLÓGICOS 13
1.6 EMBASAMENTO TEÓRICO 14
1.7 ESTRUTURA 15
2 REFERENCIAIS TEÓRICOS 16
2.1 REDES DE COMPUTADORES 16
2.1.1 MODELO DE REFERÊNCIA TCP/IP 17
2.1.2 MODELO DE REFERÊNCIA OSI 18
2.1.2.1 CAMADA DE APLICAÇÃO 19
2.1.2.2 CAMADA DE APRESENTAÇÃO 20
2.1.2.3 CAMADA DE SESSÃO 20
2.1.2.4 CAMADA DE TRANSPORTE 21
2.1.2.5 CAMADA DE REDE 22
2.1.2.6 CAMADA DE ENLACE 23
2.1.2.7 CAMADA DE FÍSICA 24
2.2 TOPOLOGIAS DE REDE 26
2.2.1 BARRAMENTO 26
2.2.2 ANEL 27
2.2.3 ESTRELA 27
2.2.4 PONTO A PONTO 28
2.2.5 MALHA 29
2.3 REDES SEM FIO 30
2.3.1 802:11: MÉTODOS DE MODULAÇÃO 32

2.3.1.1 FREQUENCY HOPPING SPREAD SPECTRUM (FHSS) 32
2.3.1.2 DIRECT SEQUENCE SPREAD SPECTRUM (DSSS) 33
2.3.1.3 ORTHOGONAL FREQUENCY DIVISION MULTIPLEXING (OFDM) .. 34
2.3.2 802:11: MODOS DE OPERAÇÕES 35
2.3.2.1 MODO AD-HOC 35
2.3.2.2 MODO INFRA-ESTRUTURA 36
2.3.3 802:11: PADRÕES DERIVADOS 36
2.3.3.1 PADRÃO 802.11A 36
2.3.3.2 PADRÃO 802.11B 37
2.3.3.3 PADRÃO 802.11G 37
2.4 QUALIDADE DE SERVIÇO (QOS) 38
2.4.1 TIPO DE SERVIÇO 40
2.4.2 SERVIÇOS INTEGRADOS 41
2.4.3 SERVIÇOS DIFERENCIADOS 42
2.4.4 QOS EM MPLS 45
2.5 FIRMWARE DD-WRT 45
2.5.1 QOS NO DD-WRT 46
3 ESTUDO DE CAMPO 48
3.1 CONFIGURANDO O ACCESS POINT 49
3.2 TESTES E RESULTADOS 53
4 CONSIDERAÇÕES FINAIS 61
REFERÊNCIAS 62

1 INTRODUÇÃO

Neste capítulo serão tratados os elementos introdutórios relacionados ao estudo e implementação de técnicas de qualidade de serviço em redes sem fio sob topologia malha.

1.1 TEMA

Com o crescimento e popularização da internet, a comunicação de dados tornou-se praticamente indispensável nos ambientes corporativo e residencial, sendo que o Brasil chegou a marca de 73,9 milhões de internautas (INSTITUTO BRASILEIRO DE OPINIÃO PÚBLICA E ESTATÍSTICA, 2011). Transações bancárias, acesso a banco de dados de filiais a uma matriz e voz sobre IP (VoIP) são exemplos de facilidades providas do crescimento da internet. Contudo, todo grande crescimento traz também algumas conseqüências, como questões de segurança e prioridade de tráfego na rede. Neste trabalho, abordar-se-á uma dessas conseqüências, a priorização e garantia de tráfego em redes, mas com um foco específico em redes sem fio, definida pelo Institute of Electrical and Eletronics Engineers (IEEE) padrão 802.11 (*wireless*). Este padrão tem, entre outras, as seguintes premissas: suportar diversos canais de comunicação; sobrepor diversas redes na mesma área de canal, apresentar robustez com relação à interferência, oferecer privacidade e controle de acesso ao meio (CÂMARA, DANIEL, 2000). Conforme a taxa de transferência de dados passou a atingir a faixa de Megabits por segundo (Mbps), as redes sem fio começaram a serem vistas como uma tecnologia promissora e com isto, a receber reais investimentos para a construção de equipamentos que possibilitassem a comunicação sem fio entre computadores (TELECO, 2006). Redes sem fio podem ser encontradas de diversas maneiras atualmente, seja em comunicação celular ou acesso a internet em redes domésticas com pontos de acesso (AP).

Em comunicação de dados, as informações necessitam de um meio para chegar ao seu destino, seja fibra ótica, cabos de cobre ou ar, como no *wireless*. Uma sequência de pacotes desde uma origem até um destino é chamada fluxo. Em uma rede orientada a conexão, todos os pacotes que pertencem a um fluxo seguem mesma rota; em uma rede não orientada a

conexão, eles podem seguir rotas diferentes. As necessidades podem ser caracterizadas por quatro parâmetros principais: confiabilidade, retardo, flutuação e largura de banda. Juntos, esses parâmetros definem a *Quality of Service* – Qualidade de Serviço (QoS) que o fluxo exige (TANENBAUM, ANDREW S., 2003, p.307).

1.2 PROBLEMAS E PREMISSAS

Com o padrão IEEE 802.11 definido, surgiram também suas derivações, 802.11a, 802.11b, 802.11g e 802.11n, nas quais são determinadas as faixas de freqüência de operação, taxas de transmissão, quantidade de canais e modulação. Cada administrador de rede deve escolher o melhor modelo que o atende, pois cada derivação tem seus prós e contras, como o custo de implantação e manutenção da rede ou propensão a interferência eletromagnética. Após a escolha do padrão adequado, deverá ser mapeado o tipo de informação que fará parte do fluxo de dados desta rede. Surgem então um dos problemas mais comuns vistos atualmente, a falta de QoS. Como os pacotes de voz não possuem possibilidade de retransmissão, devido utilizar em sua grande maioria o protocolo UDP (*User Datagram Protocol)* para comunicação, se um pacote contendo informações de voz é descartado ou há uma latência muito alta até o destino, a comunicação estará suscetível a falhas como picotamento, distorção na voz ou demora na recepção e estas são altamente perceptíveis ao ouvido humano. Mas este tipo de sintoma não afeta somente redes que utilizam VoIP. Por exemplo, em uma arquitetura de rede matriz-filiais, a banda disponível é disputada por pacotes contendo informações de vários tipos de aplicações (FTP, HTTP, etc). Entretanto, no final do mês, um fluxo maior de dados é enviado pelo departamento de recursos humanos para finalização das folhas de pagamento. Mas e se grande parte da rede estiver utilizada para acesso a internet ou acesso a banco de dados interno? Certamente o departamento de recursos humanos demorará mais para finalizar suas atividades. Essa é uma analogia que vale para demonstrar o real problema da falta de QoS em redes. Um agravante ainda é visto nas redes sem fio, pois interferência eletromagnética e barreiras entre a origem e o destino podem ocasionar a perda dos dados.

A implantação de QoS nas rede *wireless* permite a melhor utilização da mesma e a possibilita a engenharia de tráfego, sendo que assim será notada uma considerável diferença entre as redes com e sem aplicação de QoS.

1.3 OBJETIVOS

Nesta sessão serão trabalhados objetivo geral e objetivos específicos.

1.1.3.1 Objetivo Geral

O principal objetivo deste projeto é implemantar QoS em uma rede local *wireless* padrão IEEE 802.11g sob topologia malha.

1.3.2 Objetivos Específicos

- Identificar a necessidade da utilização de QoS em redes;
- Descrever as principais situações que dependem da aplicação da QoS para melhor funcionamento;
- Aplicar configurações de QoS em *Access Points;*
- Efetuar testes em topologia de rede *mesh* (malha);
- Analisar a rede após a inserção de configurações de QoS;
- Comparar a eficácia das redes antes e depois da configuração de QoS;
- Avaliar a viabilidade de inserção de QoS, baseado nos resultados obtidos;

1.4 JUSTIFICATIVA

Os administradores de redes em geral apresentam ainda alguma dificuldade em compatibilizar sua arquitetura de redes já existente com novos serviços ofertados. Apesar de existirem tutoriais passo a passo mostrando

como configurar equipamentos da maneira mais indicada, ainda encontram-se muitas redes subutilizadas devido à má projeção ou dimensionamento errôneo.

Com base nos resultados dos testes que serão realizados, este trabalho apresentará alguns motivos para a utilização da QoS em redes e também alguns cuidados que deve-se ter em projetar redes *wireless*, principalmente quando o fluxo de dados de uma determinada aplicação é prioritário em relação às demais.

Utilizando uma topologia de rede um pouco mais complexa, pretende-se demonstrar que um administrador pode ter o funcionamento adequado de sua rede apenas utilizando de recursos de configuração existentes nos próprios equipamentos e também a partir de pesquisas sobre aplicação de QoS nos diversos segmentos da rede.

1.5 PROCEDIMENTOS METODOLÓGICOS

Seguindo a linha de raciocínio de Gil (2002) sobre a classificação das pesquisas, levando em consideração os objetivos de cada uma, este trabalho de monografia estará seguindo os procedimentos técnicos de pesquisa bibliográfica e estudo de campo. Pesquisa bibliográfica, pois é desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos. A principal vantagem da pesquisa bibliográfica reside no fato de permitir ao investigador a cobertura de um gama de fenômenos muito mais ampla do que aquela que poderia pesquisar diretamente (GIL, Antônio Carlos, 2002, p. 44-45). Já o estudo de campo é definido, pois procura muito mais o aprofundamento das questões propostas do que a distribuição das características da população segundo determinadas variáveis. Como conseqüência, o planejamento do estudo de campo apresenta muito maior flexibilidade, podendo ocorrer mesmo que seus objetivos sejam reformulados ao longo da pesquisa. Outra distinção é que no levantamento das informações procura-se identificar as características dos componentes do universo pesquisado, possibilitando a caracterização precisa de seus segmentos (GIL, Antônio Carlos, 2002, p. 53).

1.6 EMBASAMENTO TEÓRICO

Seguindo a linha de pesquisa de Hamidian e Korner (2008, p.1), na atualidade, com as facilidades proporcionadas pelo *wireless* e com as novas tecnologias sem fio sendo padronizadas rapidamente, pode-se esperar uma grande procura por redes sem fio dos tipos ad hoc, malha ou redes de sensores. Todas essas redes operam independentemente de qualquer infra-estrutura. A utilização de QoS nestas redes é um tarefa desafiadora, mas torna-se altamente útil para a um melhor funcionamento da rede, apesar de aumentar a complexidade nas configurações dos equipamentos.

Mogre, Hollick e Steinmetz (2007, p.1) apresentaram um estudo mostrando os desafios e armadilhas para a realização da QoS em redes sem fio de grande porte também em topologia malha. Mencionaram a complexidade do desenvolvimento dos algoritmos para suportar QoS, mas também foi dito que a ausência deste acarretará em um desempenho ineficiente da rede. A base do estudo foi o padrão IEEE 802.16 e contou com estudo de caso onde a percepção do usuário final foi altamente relevante para a conclusão da pesquisa.

Como nas redes de pacotes a capacidade de processamentos de pacotes dos roteadores e a capacidade de tráfego nos canais de comunicação são compartilhados pelas diversas conexões simultâneas, e o tratamento de congestionamento é o simples descarte dos pacotes em excesso, o principal objetivo da QoS passa a ser priorizar o tráfego de pacotes das aplicações sensíveis a atrasos de propagação e perda de pacotes, como nas aplicações VoIP, em relação a outras aplicações menos sensíveis, como a comunicação e dados (BERNAU, PAULO SÉRGIO M., 2007, p.92). A priorização de pacotes é definida na QoS do fluxo e existe justamente para que os pacotes definidos pelo administrador da rede (voz, por exemplo) tenham prioridade em relação aos demais pacotes, sendo transmitidos e recebidos antes. Técnicas de qualidade de serviço são aplicadas em equipamentos como APs (Access Points) e roteadores, onde estes, por sua vez, saberão como tratar os pacotes recebidos.

1.7 ESTRUTURA

A monografia é composta por 4 capítulos. Primeiramente, o capítulo 1, tratará da parte introdutória, sendo apresentados o tema, os objetivos a serem atingidos, a justificativa da escolha e os problemas a serem resolvidos. Também nesta primeira parte, apresenta-se o embasamento teórico, procedimento metodológico e a estrutura da monografia.

O capítulo 2 trata do referencial teórico do projeto. Teoria sobre redes, modelos de referencia em camadas *Open System Connection* (OSI) e *Transmission Control Protocol over Internet Protocol* (TCP/IP), redes sem fio, padrão IEEE 802.11, topologia em malha e por fim a apresentação da QoS. Este capítulo trará de forma clara e objetiva os conceitos de rede que qualquer administrador deve conhecer antes de aplicar QoS em sua estrutura ou até mesmo antes de promover qualquer mudança na arquitetura de seu rede. Tratá também uma explicação sobre o funcionamento de QoS, como por exemplo, marcação dos pacotes por portas, por endereçamento IP e por aplicação utilizada.

Partindo para a parte prática do estudo, o capítulo 3 mostrará os passos seguidos para a configuração dos *Access Points*, bem como a aplicação das ferramentas de QoS disponíveis por padrão neste equipamento. Com isso, associa-se a parte teórica (marcação dos pacotes) com a parte prática (como marcar os pacotes).O estudo de campo será visto neste mesmo capitulo, onde pontos de acesso para redes sem fio serão instalados e será analisado o comportamento das redes com e sem QoS aplicado. A partir dos resultados obtidos, poder-se-á afirmar que a configuração de QoS é necessária e em quais situações torna-se praticamente obrigatória.

Finalizando a monografia, o capítulo 4 traz as conclusões sobre o estudo como um todo e também quesitos comumente vistos após esta sessão, como as referências.

2 REFERENCIAIS TEÓRICOS

2.1 REDES DE COMPUTADORES

O primeiro experimento conhecido de conexão de computadores em rede foi feito em 1965, nos Estados Unidos por obra de dois cientistas, Lawrence Roberts e Thomas Merril. A experiência foi realizada por meio de uma linha telefônica discada de baixa velocidade, fazendo a conexão entre dois centros de pesquisa um em Massachusetts e outro na Califórnia. Considera-se que naquela ocasião foi plantada a semente para o que hoje é a Internet. Contudo, o real nascimento das redes de computadores não foi por acaso e esta associado à corrida espacial, onde foi identificada a necessidade da criação de uma rede para conectar as bases militares americanas. As criação destas redes e boa parte dos elementos e aplicações essenciais para a comunicação entre computadores, como o protocolo TCP/IP, a tecnologia de comutação de pacotes de dados e correio eletrônico, estão relacionados ao desenvolvimento da Arpanet, a rede que deu origem a internet. Ela foi criada por um programa desenvolvido pela Advanced Research Projects Agency (ARPA) (CASTRO, JAIME J. DE, 2008, p.2).

Quando as primeiras redes de dados surgiram, somente computadores de um mesmo fabricante podiam comunicar-se entre si, por exemplo, empresas escolhiam ou uma solução IBM ou uma solução HP, mas nunca ambas, por uma questão de compatibilidade. Devido a isso, os usuários finais não estavam muito a vontade, pois, por exemplo, se uma empresa que adotava a IBM como fornecedora adquirisse outra empresa e esta utilizasse HP, não haveria possibilidade de integrar a parte adquirida à parte existente. Casos como este foram o suficiente para deixar muitos consumidores insatisfeitos a ponto de exigirem uma solução para esse impasse: que os fabricantes chegassem a um acordo, e que compatibilizassem de alguma forma suas tecnologias. Então, no inicio da década de 80 a International Organization for Standardization (ISO), juntamente com representantes de diversos fabricantes, criou um grupo de trabalho para resolver o problema. Em 1984, surgia o primeiro resultado desse esforço: o modelo de referência OSI. O modelo OSI foi criado com o intuito de padronizar a comunicação de dados e de permitir a interoperabilidade – independentemente de marca (fabricante) ou sistema utilizado, ou seja, compatibilizar *hardware* e *software* envolvidos, de alguma forma, com o

transporte de dados (FILIPPETTI, MARCO AURÉLIO, 2008, p. 33 e 34). Esse foi um passo muito importante para obtermos o que hoje é a poderosa internet, onde há a comunicação de dados, independentemente de fabricantes e que abrange ambientes diversificados, como os governamentais, corporativos, residenciais e um dos mais emergentes atualmente, o ambiente de usuários que utilizam a comunicação móvel, como acesso à internet via celular, *smartphones* e *modems* 3G.

Nos próximos subitens (2.1.1 e 2.1.2), apresentar-se-ão os dois modelos de referência OSI e TCP/IP e suas derivadas.

2.1.1 Modelo de referência TCP/IP

Com a difusão das redes Arpanet, pouco a pouco centenas de universidades e repartições públicas foram conectadas, usando linhas de telefones dedicadas, isto é, linhas com acesso sem depender da demanda de outros usuários. Quando foram criadas as redes de rádio e satélite, começaram a surgir problemas com os protocolos existentes, o que forçou a criação de uma nova arquitetura de referência. Desse modo, a habilidade para conectar várias redes de maneira uniforme foi um dos principais objetivos do projeto. Mais tarde, essa arquitetura ficou conhecida como Modelo de Referência TCP/IP, graças a seus dois principais protocolos TCP e IP (TANENBAUM, ANDREW S., 2003, p.48). Protocolos nada mais são do que padrões definidos para estabelecer logicamente a comunicação de dados entre dois ou mais pontos (computadores, roteadores etc). Em uma simples analogia, protocolos são comparados a idiomas, onde duas pessoas devem se comunicar na mesma linguagem para estabelecer um diálogo.

O modelo de referência TCP/IP foi o padrão adotado pela Arpanet e possui sua arquitetura dividida em quatro camadas distintas, cada uma responsável por determinada função durante o fluxo de dados. As camadas do modelo TCP/IP, em hierarquia decrescente, são: Camada de Aplicação, Camada de Transporte, Camada de Internet e Camada de Rede (também conhecida como Acesso a rede ou Interface de rede).

A figura 1 traz as camadas do modelo TCP/IP, bem como suas funções e exemplos de protocolos presentes em cada uma.

Camada	Descrição	Protocolos
Aplicação	Define os protocolos de aplicativos TCP/IP e como os programas host estabelecem uma interface com os serviços de camada de transporte para usar a rede.	HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP
Transporte	Fornece gerenciamento de sessão de comunicação entre computadores host. Define nível de serviço e o status da conexão usada durante o transporte de dados.	TCP, UDP, RTP
Internet	Empacota dados em datagramas IP, que contém informações de endereço de origem e de destino usadas para encaminhar datagramas entre hosts e redes. Executa o roteamento de datagramas IP.	IP, ICMP, ARP, RARP
Acesso a Rede	Específica detalhes de como os dados são enviados fisicamente pela rede, inclusive como os bits são assinalados eletricamente por dispositivos de hardware que estabelecem interface com um meio da rede, como cabo coaxial, fibra óptica ou fio de cobre de par trançado.	Ethernet, Token Ring, FDDI, X.25, RS-232, V.35

Figura 1 - Camadas do modelo TCP/IP
Fonte: Technet Microsoft – Modelo TCP/IP, 2011.

Contudo, o modelo TCP/IP não tinha um órgão de renome em seu controle acabou perdendo espaço para o modelo de referência OSI (*Open System Interconnection*), o qual foi criado pela Organização Internacional de Padronização - International Organization for Standardization, ISO.

2.1.2 Modelo de referência OSI

Como já mencionado, uma padronização viu-se necessária a fim de obter-se uma rede de computadores *multi-vendor*, ou seja, conexão entre equipamentos sem a obrigatoriedade de depender-se apenas de um fabricante. Foi justamente esta a causa abraçada por uma das principais organizações no que se refere à elaboração de padrões de comunicação de âmbito mundial, a ISO, onde no início da década de 80, definiu um modelo de arquitetura para

sistemas abertos, visando permitir a comunicação entre máquinas heterogêneas e definindo diretivas genéricas para a construção de redes de computadores independente da tecnologia de implementação. Este modelo foi denominado OSI, servindo de base para a implementação de qualquer tipo de rede, seja ela, curta, média ou longa distância (PINHEIRO, JOSÉ MAURICIO S., 2004).

Assim como o modelo TCP/IP, o modelo de referência OSI também foi definido em camadas, sete exatamente, onde cada uma possui sua função na pilha de protocolos. Cada camada interage com sua correspondente no equipamento remoto, ou seja, camada 3 de uma estação local só troca informações com camada 3 da estação remota. Contudo, não se deve confundir comunicação entre camadas correspondentes, com encapsulamento de dados, pois dados oriundos de aplicativos da camada sete são encapsulados dentro do formato oferecido pela camada imediatamente inferior, camada 6. As sete camadas mencionadas são nomeadas, da mais superior (camada 7) para a mais inferior (camada 1), da seguinte maneira: Aplicação, Apresentação, Sessão, Transporte, Rede, Enlace e Física. Nos próximos subitens serão apresentadas as principais características de cada camada do modelo OSI.

2.1.2.1 Camada de Aplicação

A camada de aplicação é a que mais se interage com o usuário. Nesta camada se encontram as principais aplicações (softwares / protocolos) utilizadas atualmente, como servidores de e-mail, navegador web, banco de dados, DNS, DHCP etc.

A transferência de um arquivo entre dois sistemas requer uma forma de trabalhar com as incompatibilidades existentes. A camada de aplicação tem grande importância na resolução deste problema. O dado entregue pelo usuário à camada de aplicação recebe a denominação *Service Data Unit* (SDU). A camada de aplicação, então, junta à SDU (dados do usuário) um cabeçalho chamado *Protocol Control Information* (PCI). O objetivo resultante desta junção é chamado de *Protocol Data Unit* (PDU), que corresponde à unidade de dados especificada de um certo protocolo da camada em questão (PINHEIRO, JOSÉ MAURICIO S., 2004).

2.1.2.2 Camada de Apresentação

A camada de apresentação responde às solicitações de serviço da camada de aplicação e envia solicitações de serviço para a camada imediatamente inferior (sessão). Diferentemente das camadas mais inferiores, preocupadas em mover bits de forma confiável de um ponto a outro, essa camada preocupa-se com a sintaxe e a semântica dos dados transmitidos. Por exemplo, após receber dados da camada de aplicação, pode ser necessário converter esses dados de seu formato original para um formato compreendido e aceitável por outras camadas do modelo, garantindo assim uma transmissão mais eficiente. Exemplos de formatações incluem PostScript, ASCII, EBCDIC e ASN.1 (FILIPPETTI, MARCO AURÉLIO, 2008, p. 43).

Criptografia e compressão também são funções, mas não exclusivas, da camada de apresentação. Formatos de compressão e codificação de imagem, como *Graphics Interchange Format* (GIF) e *Joint Photographic Experts Group* (JPEG), e vídeo, como QuickTime (empresa Apple™) e *Motion Picture Experts Group* (MPEG), são definidos na camada de apresentação.

2.1.2.3 Camada de Sessão

A Camada de sessão permite que usuários de diferentes máquinas estabeleçam sessões entre eles. Uma sessão oferece vários serviços, inclusive o controle de diálogo (mantendo o controle de quem deve transmitir em cada momento), o gerenciamento de símbolos (impedindo que duas partes tentem executar a mesma operação crítica ao mesmo tempo) e a sincronização (realizando a verificação periódica de transmissões longas para permitir que elas continuem a partir do ponto em que estavam ao ocorrer a falha) (TANENBAUM, ANDREW S., 2003, p.47).

2.1.2.4 Camada de Transporte

Responsável principalmente pela segmentação e controle de fluxo, a camada de transporte trabalha com os dois protocolos de comunicação mais comumente encontrados atualmente, o TCP e o UDP. Esta camada recebe os dados da camada superior (Sessão), divide-os em unidades menores e repassa esses segmentos para a camada de rede, assegurando que todas as informações chegarão ao destino na ordem correta e sem erros.

O controle de fluxo proporcionado pela camada de transporte garante uma conexão lógica ponto a ponto e gerencia o fluxo de dados fim a fim, onde o destino envia a confirmação dos dados recebidos e aguarda a chegada dos demais segmentos para fazer a reconstrução da informação. Uma vez que a origem não receba a confirmação, o segmento é retransmitido. Outra função do controle de fluxo é evitar congestionamento ou sobrecarga na rede, pois o poder de processamento das máquinas não é sempre idêntico e algumas informações podem chegar ao destino mais rapidamente do que ele possa processar, ocasionando assim o descarte de dados. Devido a isso, existe um mecanismo de memória chamado *buffer*, que armazena as informações por um certo período até que o destino possa processá-las. Caso o *buffer* do destino se esgote, um sinal (*not ready*) é enviado ao equipamento de origem, para que este aguarde um novo sinal (*ready*) antes de transmitir novos dados. Observa-se este tipo de situação de controle de fluxo quando utiliza-se o protocolo TCP, pois este é orientado a conexão e garante a confiabilidade e integridade na entrega dos dados. Contudo, perde-se em envio de informações e processamento, pois tem um *overhead* alto e ainda existem as mensagens de confirmação, que o torna muito utilizável em comunicação que não levem em consideração o fator tempo para funcionarem da melhor maneira. Exemplos clássicos de utilização do TCP navegadores web e e-mails.

Em contrapartida ao TCP, mas também definido na camada de transporte, encontra-se o protocolo UDP. Este protocolo possui *overhead* baixo, não é orientado a conexão e não oferece dispositivos de controle de fluxo sofisticados. Apesar de ser um protocolo simples e possuir apenas as funções básicas da camada de transporte, o UDP é mais rápido em relação ao TCP, o que o torna eficaz em transmissões de voz sobre IP (Voip) e gerenciamento de equipamentos (protocolo SNMP). Contudo, as transmissões estarão sujeitas a perdas, o que pode ser prejudicial em uma conversa Voip, por exemplo. Neste

quesito de definirem-se prioridades de tráfego na rede (engenharia de tráfego) é que se encaixa a aplicação de QoS, o qual será visto posteriormente.

Os serviços baseados em TCP e UDP rastreiam as várias aplicações que estão se comunicando. Para diferenciar os segmentos e datagramas para cada aplicação, o TCP e o UDP possuem campos de cabeçalho que podem identificar unicamente essas aplicações. Estes identificadores únicos são os números de porta. No cabeçalho de cada segmento ou datagrama, há uma porta de origem e destino. O número de origem é o número para essa comunicação associado à aplicação originada no *host* local. (CISCO, NETWORK ACADEMY, Módulo 1, Cap. 4, Slide 4.1.5.1, 2007). O número da porta de destino é a disponível para que se estabelece a comunicação. Portas como TCP 80 (HTTP), TCP 23 (Telnet), UDP 5060 (SIP) e UDP 53 (DNS) já são bem conhecidas de profissionais da área de TI.

2.1.2.5 Camada de Rede

Quando se fala em camada de rede ou camada 3 não de pode deixar de falar em roteamento, pois está é a camada responsável por enviar os pacotes aos seus destinos, sejam eles diretamente conectados ou em outras redes. Os dispositivos responsáveis por esse encaminhamento de pacotes são os roteadores, os quais tem papel fundamental no funcionamento da internet atualmente. Os roteadores recebem os pacotes em uma interface, analisam o endereço IP deste pacote e caso esse endereço faça parte de uma máquina (*host*, servidores) ou outro equipamento camada 3 diretamente conectada a ele, ou seja, na mesma rede que uma das interfaces, o roteador simplesmente encaminha (roteia) o pacote ao destino. Contudo, se o pacote recebido não for destinado ao roteador em questão este verificará se o endereço de destino se encontra em sua tabela de roteamento, uma base de dados que fica armazenada na memória do roteador RAM do roteador contendo as redes conhecidas pelo equipamento, e que pode ser estaticamente ou dinamicamente formada (FILIPPETTI, MARCO AURÉLIO, 2008, p. 48).

Existem basicamente dois tipos de pacotes definidos na camada de rede, os pacotes de dados e os pacotes de atualização. Os pacotes de dados são os utilizados para transporte dos dados pela rede, e os protocolos usados para suportar tal tráfego são conhecidos como protocolos roteados, como por exemplo, o IP e o IPX. Já os pacotes de atualização são utilizados justamente

para o transporte de atualização sobre roteadores vizinhos e os caminhos para alançá-los. Os protocolos usados para gerenciar esta tarefa são chamados de protocolos de roteamento, como OSPF (*Open Shortest Path First*), BGP (*Border Gateway Protocol*) e RIP (*Routing Information Protocol*).

Importante também salientar que os roteadores não propagam mensagens de *broadcast,* ou seja, mensagens enviadas para todos os endereços de uma mesma rede não atravessam o roteador, evitando assim lentidão na rede e customizando o processamento dos equipamentos. Roteadores também quebram os chamados domínios de colisão, ou seja, cada interface do roteador trabalha como se fosse uma rede isolada e utiliza de um endereço específico para ela.

A camada de rede também apresenta funções de controle de congestionamento e contabiliza o tráfego demandado pelo usuário para fins de tarifação.

2.1.2.6 Camada de Enlace

A camada de enlace assegura que os dados sejam transmitidos ao equipamento apropriado e converte os dados vindos da camada superior (Rede) m bits, tornando possível a transmissão através de meios físicos, como cabos, definidos na camada física. A camada de enlace formata a mensagem em frames e adiciona um cabeçalho customizado contendo o endereço de hardware (MAC *Address*) das máquinas transmissora e destinatária. È importante também entender que à camada de rede (onde os roteadores são definidos) não importa a localização física das máquinas, mas a localização lógica das redes. A camada de enlace (onde switches e *bridges* são definidos), sim, é responsável pela identificação de cada máquina (MAC *address*) em uma rede local (FILIPPETTI, MARCO AURÉLIO, 2008, p. 49). Nesta camada, também são feitos controle de fluxo, detecção de erros e possíveis correções.

A camada de enlace é dividida em duas subcamadas, LLC (*Logical Link Control*) e MAC (*Media Access Control*). A subcamada LLC é responsável pela identificação de protocolos de camada de rede e seu encapsulamento. Um cabeçalho LLC diz à camada de enlace o que fazer com um pacote uma vez que o frame é recebido. Por exemplo, assim que um host recebe um frame, ele analisa o cabeçalho LLC para entender para qual protocolo da camada de rede (IP, IPX) ele é destinado. A subcamada LLC também pode ajudar no controle

de fluxo e sequenciamento de bits. A subcamada MAC, por sua vez, define como os pacotes são alocados e transmitidos no meio físico. O endereçamento físico é definido nesta subcamada, assim como a topologia lógica. Disciplina da linha, notificação de erros, entrega ordenada de frames e controle de fluxo também podem ser utilizados nesta subcamada (FILIPPETTI, MARCO AURÉLIO, 2008, p. 50).

Como já mencionado, os switches são equipamentos definidos na camada em questão. A comunicação destes equipamentos é baseada no endereçamento físico (MAC) dos equipamentos conectados, onde estes são conhecidos pelos switches e armazenados em uma tabela e o frame será enviado apenas para a porta do switch que estiver mapeada com o endereço MAC do destino. Com isso, pode-se notar que cada porta do switch é um domínio de colisão próprio, diferentemente do hub, que é um grande domínio de colisão.

2.1.2.7 Camada de Física

A primeira camada do modelo de referência OSI é camada física e esta tem por seu principal objetivo a transmissão dos bits (sinal elétrico, óptico ou microondas) que formam os quadros (*frames*) da camada de enlace através dos meios cabos, fibras ópticas ou ar. Assim como a transmissão, é também de responsabilidade da camada física a recepção e organização dos sinais, de modo que estes, ao serem enviados para a camada superior, formem um *frame* completo. A figura 2 representa os sinais transmitidos na camada física.

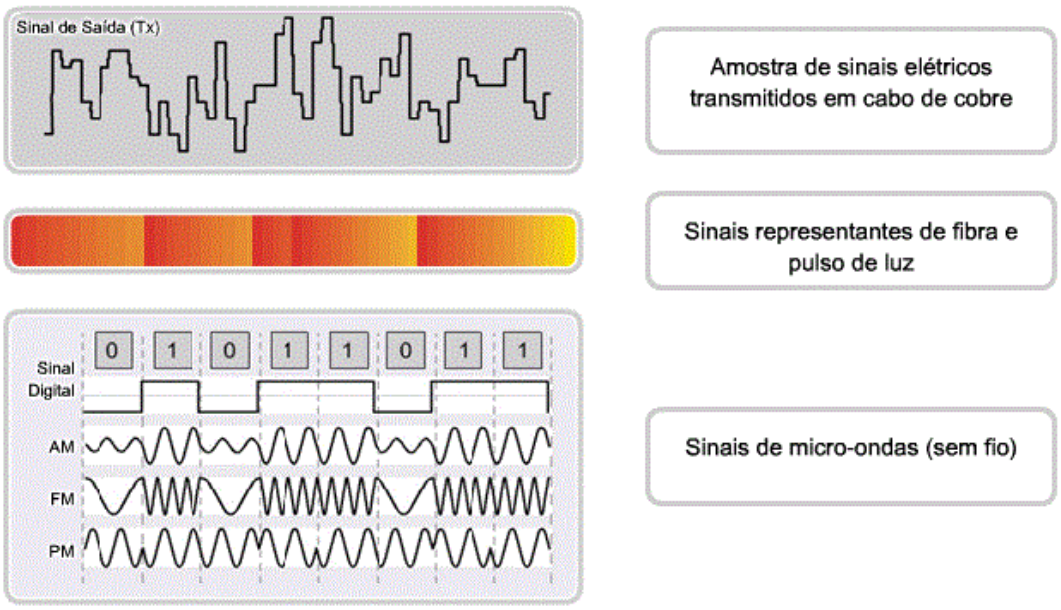

Figura 2 – Sinais da Camada Física
Fonte: Cisco Networking Academy – Fundamentos de Redes – Módulo1, Cap. 8, Slide 8.1.2.1, 2007.

Na camada física também são definidos os meios para a transmissão bem como seus conectores, caso necessário. Mídias Ethernet têm sua diferenciação baseada no tipo de cabo, categoria, quantidade de pares, diâmetro da fibra e conectores, mas naturalmente antes de se escolher a mídia o administrador da rede deve fazer um estudo e analisar se o tipo de cabo o atenderá nos quesitos distância e largura de banda suportada. Já para redes sem fio, os padrões de comunicação podem ser vistos na figura 3:

Padrões	Bluetooth 802.15	802.11(a,b,g,n), HiperLAN 2	802, 11, MMDS, LMDS	GSM, GPRS, CDMA, 2.5- 3G
Velocidade	<1 Mbps	1 - 54+ Mbps	22 Mbps+	10- 384 Kbps
Faixa	Curto	Médio	Médio - longo	Longo
Aplicações	Ponto-a-ponto dispositivo-a-dispositivo	Redes corporativas	Fixo, acesso "última milha"	PDAs, Telefones celulares, Acesso ao celular

Figura 3 – Padrões sem fio - Camada Física
Fonte: Cisco Networking Academy - Fundamentos de Redes – Módulo3, Cap. 7, Slide 7.1.1.2, 2007.

A comunicação sem fio será vista posteriormente com mais detalhes.

As transmissões de bits (sinais lógicos representados por 0 ou 1) dependem de codificação e sinalização. A codificação é um método de converter fluxo de bits de dados em um código predefinido. Os códigos são grupo de bits utilizados para fornecer um padrão previsível que possa ser reconhecido pelo remetente e pelo receptor. Já a sinalização consiste na

camada física gerar os sinais elétricos, ópticos ou sem fio que representem o “1” e “0” no meio físico (CISCO, NETWORK ACADEMY, Módulo 1, Cap. 8, Slide 8.3.2.2, 2007).

2.2 TOPOLOGIAS DE REDE

As topologias de redes nada mais são do que a disposição física em que os equipamentos se encontram conectados, ou seja, o *layout* da rede. As topologias encontradas atualmente são barramento, anel, estrela, ponto a ponto e malha.

2.2.1 Barramento

Na topologia em barramento, todos os equipamentos (mais de dois) encontram-se ligados a um mesmo segmento ou cabo. Não há a possibilidade de transmissão simultânea e a possibilidade de colisão é grande. Esta é uma topologia obsoleta e era utilizada em redes, por exemplo, onde um único cabo coaxial ia de uma extremidade à outra, mas quando havia uma maquina para ser conectada, o cabo era seccionado e nele encaixado um conector de três pontas em formato da letra T, onde uma das pontas se encaixava à máquina e as outras duas conectavam o cabo. A figura 4 traz uma topologia em barramento:

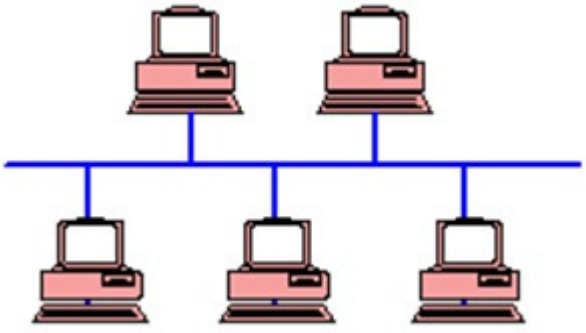

Figura 4 – Topologia em Barramento
Fonte: UFRGS – Redes e Telecomunicações, 2011

2.2.2 Anel

Na topologia em anel cada bit se propaga de modo independente, sem esperar pelo restante do pacote ao qual pertence. Em geral, cada bit percorre todo o anel no intervalo de tempo em que alguns bits são enviados, muitas vezes até mesmo antes de o pacote ter sido inteiramente transmitido (TANENBAUM, ANDREW S., 2003, p.30). Dispositivos para acesso simultâneo ao meio devem ser empregados para que não ocorram colisões neste tipo de topologia. Exemplo disso são as redes *Token Ring*, onde a transmissão dos dados deve partir apenas do equipamento que estiver habilitado para isso, muitas vezes mencionado também como o equipamento que estiver com a posse do "bastão" (*token*). A figura 5 mostra a topologia em anel:

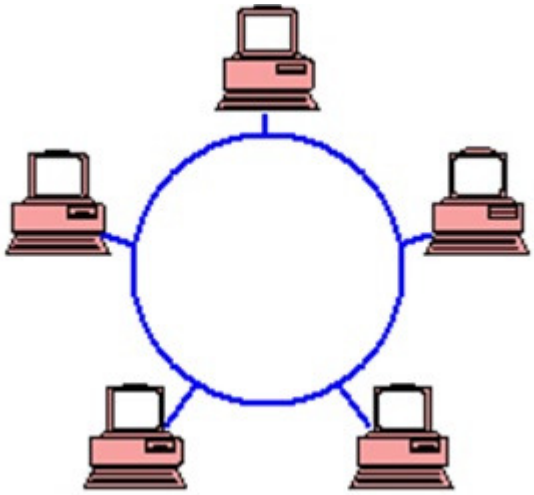

Figura 5 – Topologia em Anel
Fonte: UFRGS – Redes e Telecomunicações, 2011

2.2.3 Estrela

A topologia em estrela caracteriza-se em vários elementos da rede conectados a um elemento principal. Por ter um elemento centralizado, esta topologia é um pouco mais elaborada, tendo a necessidade de controle de fluxo e cuidando-se com o processamento do equipamento central e com sua operação e manutenção, pois caso haja falha com este equipamento toda a rede para. A topologia em estrela é demonstrada na figura 6.

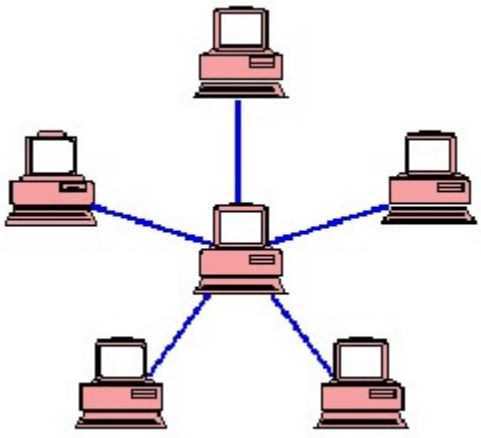

Figura 6 – Topologia em Anel
Fonte: UFRGS – Redes e Telecomunicações, 2011

2.2.4 Ponto a Ponto

A topologia ponto a ponto é a mais simples de todas, onde dois equipamentos são diretamente conectados e podem fazer a comunicação sem a intervenção de nenhum equipamento intermediário. Por definição, a conexão ponto a ponto em ethernet entre dois equipamentos de mesma camada, como por exemplo, roteador com roteador (elementos de camada 3), deve ser feita através de cabo *crossover* (cruzado), onde o fio TX (transmissor) de um lado corresponde ao RX (receptor) do outro lado e vice-versa. Contudo, atualmente muitos equipamentos já possuem "inteligência" suficiente para distinguir comunicação entre equipamentos de mesma camada ou camada distinta. A topologia ponto a ponto pode ser vista na figura 7:

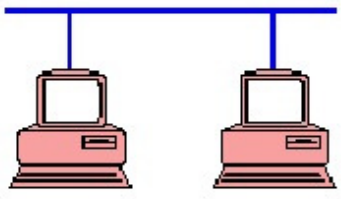

Figura 7 – Topologia em Anel
Fonte: UFRGS – Redes e Telecomunicações, 2011

2.2.5 Malha

Em contrapartida à topologia ponto a ponto, a topologia em malha (*mesh*) é a mais complexa de ser implantada. As redes em malha podem ser encontradas de duas maneiras, malha total ou malha parcial. Malha total (*full mesh*) consiste na comunicação total entre os equipamentos, ou seja, em uma rede com cinco elementos, cada um deles possuirá quatro conexões distintas. Malha parcial (*Partial Mesh*) consiste na conexão de alguns dos equipamentos da rede, mas estes considerados fundamentais na comunicação com o *gateway* de internet ou com a máquina de destino. Redes *mesh* possibilitam uma conexão mais rápida com o destino, visto que existem varias conexões que levam ao mesmo lugar e conseqüentemente usará o melhor caminho (através dos protocolos de roteamento) para alcançá-lo, redundância e tornam quase nula a possibilidade de falha de conectividade, pois em uma rede bem administrada raramente todos os pontos da rede em malha ficarão fora de serviço simultaneamente. Contudo, em redes cabeadas, o custo para a implantação das redes *mesh* torna-se um tanto elevado, devido ao custo de um bom cabeamento estruturado.

Em redes *wireless mesh,* um dos principais escopos desta pesquisa, as redes em malha necessitam apenas dos pontos de acesso (APs) e que estes se comuniquem entre si para encontrar o destino ou o *gateway* de internet através do melhor caminho. Em ambiente corporativo, as redes *wireless* em malha podem ser aplicadas em prédios comerciais, campus de uma universidade ou em espaços industriais em pavilhões. Isso ocasionará economia com cabeamento e facilidade de implantação, pois dependerá apenas de um bom profissional para a configuração dos APs. A topologia funciona com os APs operando no modo Ad-Hoc e seus protocolos de roteamento, como o OLSR (*Optimized Link State Routing*), o qual será utilizado na topologia de testes desta pesquisa. A explicação sobre as redes Ad-Hoc e protocolo OLSR serão vistos no tópico redes sem fio, no presente capítulo. Na figura 8 pode-se ver uma rede em malha parcial, mas possibilitando vários caminhos para se chegar ao roteador que faz o *gateway* com a internet.

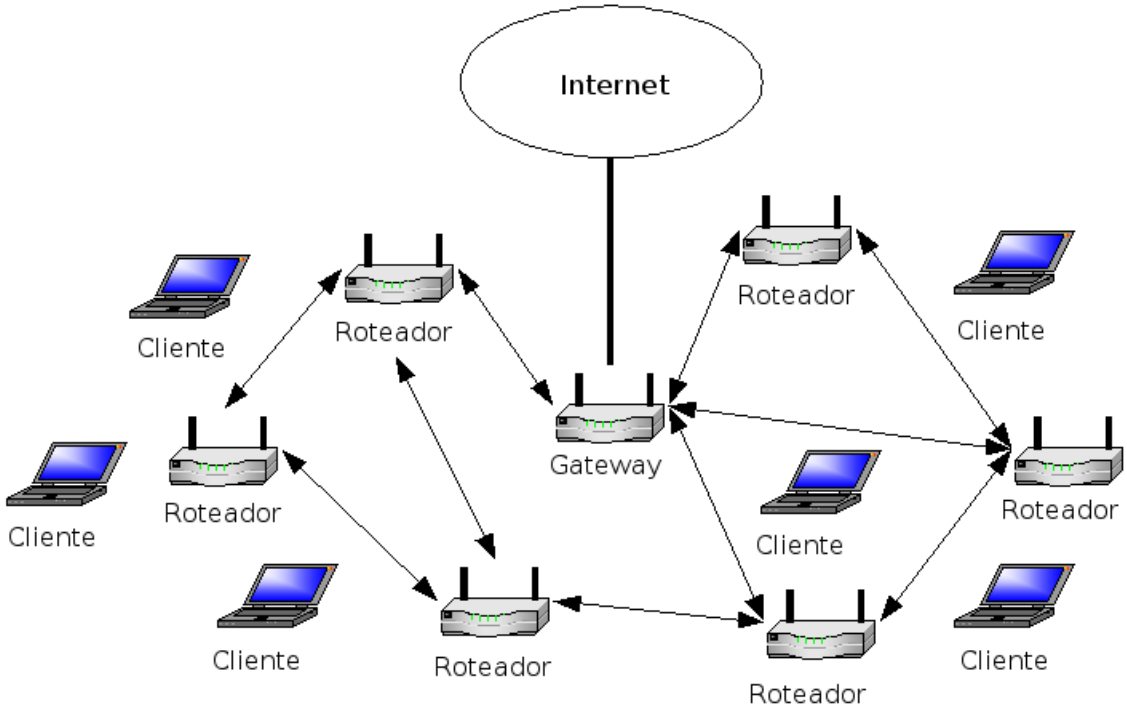

Figura 8 – Topologia em Malha
Fonte: Passos, Diego. Métricas de Roteamento para Redes em Malha Sem Fio, 2007, p.11.

2.3 REDES SEM FIO

Com o avanço da tecnologia e o surgimento de equipamentos como *notebooks*, viu-se uma nova necessidade aflorando, pois seria inviável ter um equipamento móvel (*notebook*) e ainda sim depender de rede cabeada para acesso à internet. Foi então que a idéia de comunicação sem fio surgiu. Contudo, o mesmo impasse de compatibilidade entre fabricantes veio a tona, pois como iriam fazer para um equipamento com placa de um determinado fabricante comunicar-se com a estação base de outro. Devido a isso, em meados da década de 90 o IEEE constituiu um grupo de pesquisa que recebeu a tarefa de padronizar a redes LANs sem fio. Em 1997 o padrão denomidado IEEE 802.11 teve sua primeira publicação em 1997 e nesta primeira oportunidade, as taxas de transmissão atingiam velocidades entre 1 e 2 Mbps.

Com o padrão 802.11 em funcionamento e operando nas velocidades de 1 e 2 Mbps, quase que imediatamente, a pessoas reclamaram da lentidão e a partir daí começaram os trabalhos para a definição de padrões mais rápidos. Uma divisão ocorreu dentro do comitê, resultando em mais dois novos padrões, publicados em 1999. O padrão 802.11a utiliza uma faixa de freqüências mais larga (5 GHz) e funcionava em velocidades de 54 Mbps. O padrão 802.11b

utilizava a mesma faixa de freqüências que o 802.11 (2,4 GHz), mas emprega uma técnica de modulação diferente, o que possibilitou alcançar 11 Mbps. Para tornar a questão ainda mais complicada do que já era, o comitê 802 apresentou ainda outra variante, o 802.11g, que utiliza a técnica de modulação do 802.11a, mas emprega a faixa de freqüência do 802.11b (TANENBAUM, ANDREW S., 2003, p.69). Atualmente o padrão que mais se ouve falar é o 802.11n, que emprega tanto as faixas de freqüências de 2,4 GHz (802.11b) ou 5 GHz (802.11a), mas sua técnica de modulação permite atingir velocidade de até 540 Mbps. No Brasil, os padrões mais utilizados são 802.11b e 802.11g, devido aos equipamentos (APs, telefones sem fio, etc) trabalharem em sua grande maioria na faixa de 2,4 GHz.

O padrão 802.11 é definido na camada de enlace e conseqüentemente camada física no modelo OSI. Na camada física são definidas as técnicas de modulação de cada padrão 802.11 (a,b,g e n) e o meio de transmissão é o próprio ar. As técnicas de modulação FHSS (*Frequency Hopping Spread Spectrum*), DSSS (*Direct Sequence Spread Spectrum*) e OFDM (*Orthogonal Frequency Division Multiplexing*) serão apresentadas posteriormente. Já na camada de enlace, ocorre a divisão de funções entre as duas subcamadas, MAC e LLC. A subcamada MAC determina como o canal é alocado, isto é, quem terá a oportunidade de transmitir os dados. Nela, apresenta-se o CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) que anula as colisões nas transmissões sem fio. Acima dela, encontra-se a subcamada LLC, cujo trabalho é ocultar as diferenças entre as diversas variações do 802 e torná-las indistinguíveis no que se refere à camada de rede (TANENBAUM, ANDREW S., 2003, p.232). A figura 9 mostra a comparação do *wireless* LAN com o modelo de referencia OSI:

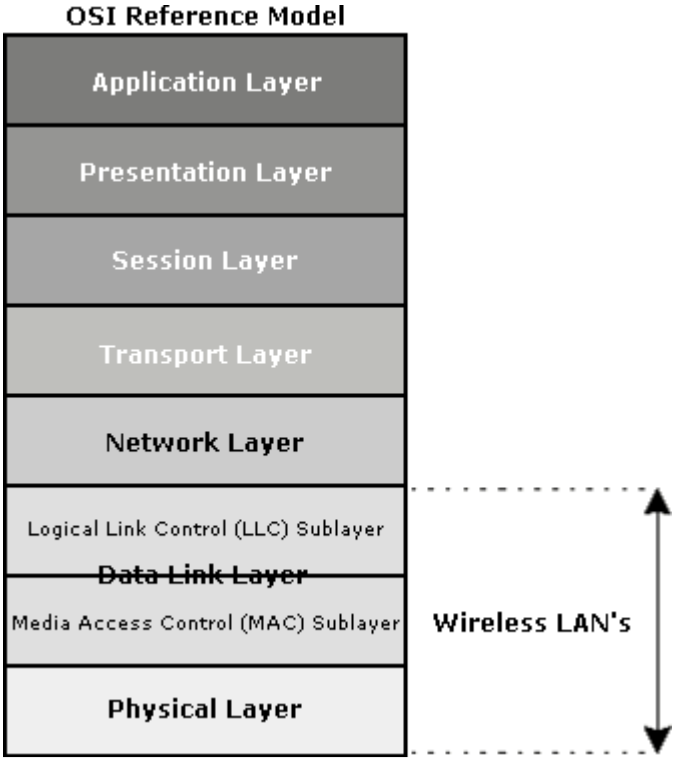

Figura 9 – Relação do 802.11 com modelo OSI
Fonte: Teleco – WLAN de Alta Velocidade II: Recomendações IEEE - 2006

2.3.1 802:11: Métodos de Modulação

Nesta sessão serão apresentados os três principais métodos de modulação do padrão 802.11 e suas derivadas (a,b,g,n), os métodos FHSS, DSSS e OFDM.

2.3.1.1 *Frequency Hopping Spread Spectrum* (FHSS)

O FHSS (Espectro de Dispersão de Saltos de Freqüência) utiliza 79 canais, cada um com 1MHz de largura, começando na extremidade baixa da banda de 2,4 Ghz. Um gerador de números pseudo-aleatórios é usado para produzir a seqüência de freqüência dos saltos (TANENBAUM, ANDREW S., 2003, p.232). É necessário garantir o sincronismo de todas as estações, para que elas mudem para as mesmas freqüências de forma simultânea, utilizando igualmente os canais de freqüência. Isso pode ser assegurado com a utilização de um mesmo gerador de números pseudo-aleatórios. Em um determinado momento, um canal desta seqüência é utilizado por curto período de tempo

para a transmissão dos dados. Com o sincronismo entre o receptor e o transmissor, considerando que a série de canais deste é conhecida pelo receptor, a informação será totalmente recuperada, fornecendo, além disso, maior segurança, já que um intruso não poderá espionar as transmissões se não conhecer a seqüência de saltos ou tempo de parada (período de tempo gasto em cada freqüência) (TELECO, 2006). Esta técnica de modulação é utilizada no padrão IEEE 802.11 original, mas não em seus derivados.

2.3.1.2 *Direct Sequence Spread Spectrum* (DSSS)

Igualmente à modulação FHSS, esta técnica de modulação também utiliza as freqüências na faixa de 2,4 GHz. Trabalha em uma largura de banda de 82 MHz (2,402 GHz à 2,483 GHz), sendo dividida em 11 canais de parcialmente sobrepostos. A figura 10 mostra a distribuição dos canais no espectro de freqüências:

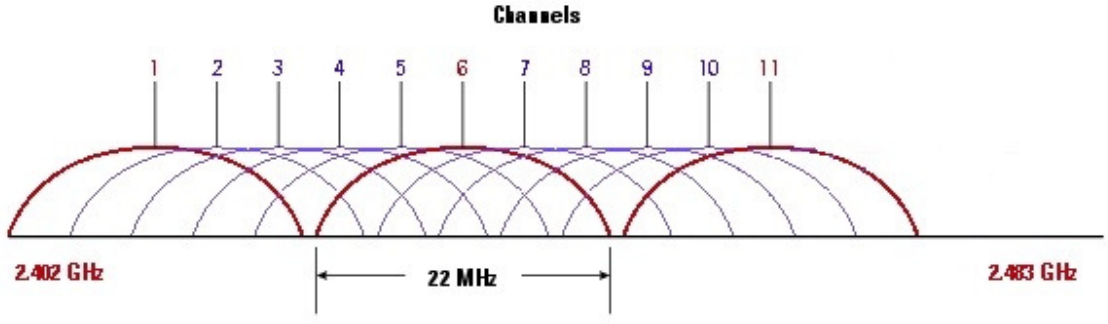

Figura 10 – Canais de Radiofreqüência em 2,4 GHz
Fonte: Air-Stream – *Community Wireless Network*, 2011.

Na técnica DSSS, os tempos de bit são divididos em número de intervalos de valor indefinido, os quais são chamados de chips. Cada transmissor possui uma seqüência aleatória de número de bits, esta conhecida como seqüência de chips. Uma determinada (mas não conhecida) seqüência de chips é utilizada para enviar um valor de bit “1” e para a transmissão do bit “0” o complemento da mesma seqüência, ou seja, se para a transmissão do bit “1” a seqüência de chips for 001100, para a transmissão do bit “0” a seqüência será 110011.

Segundo o padrão 802.11, o DSSS utiliza um sequencia de 11 bits para espalhar os dados antes de transmiti-los. Cada bit transmitido é modulado por

esta sequencia. Este processo espalha a energia de radiofreqüência em torno de uma banda de faixa larga que pode ser necessária para transmitir o dado. O receptor concentra o sinal de radiofreqüência recebido para recuperar o sinal (TELECO, 2006).

A técnicas de DSSS foram desenvolvidas para operada em largura de banda de 2 Mbps. Contudo, para o padrão 802.11b, foi desenvolvida a HR-DSSS (*High Rate Direct Sequence Spread Spectrum*), a qual utiliza maior quantidade de chips/s (11 milhões), o que possibilita largura de banda de 11 Mbps.

2.3.1.3 *Orthogonal Frequency Division Multiplexing* (OFDM)

A técnica de modulação OFDM opera tanto na faixa de 2,4 GHz quanto na faixa de 5 GHz. Utilização uma técnica de multiplexação por divisão de frequência ortogonal, ou seja, uma maneira de se modular o sinal através de múltiplas portadoras. Como isso, problemas na transmissão devido obstáculos, como parede, conseguem ser minimizados, o que não acontece no sistema HR-DSSS.

Em sua forma de implementação, o OFDM quebra uma portadora de dados de alta velocidade em várias portadoras de velocidades menores, e todas transmitem em paralelo. Cada portadora de alta velocidade é de 20 MHz e possui 52 subcanais, cada um com aproximadamente 320 KHz. Quatro subcanais são utilizados para a correção de erros e para manter a coerência do sinal de frequência. Os 48 subcanais restantes são para dados (TELECO, 2006).

O OFDM é utilizado nos padrões 802.11g e 802.11a, sendo que este opera na frequencia de 5 GHz e atinge velocidade de até 54 Mbps e aquele opera na faixa de 2,4 GHz e atinge a mesma velocidade de 54 Mbps. A vantagem do 802.11g é que atinge maior alcance e é compatível com o padrão 802.11b.

Outro padrão que utiliza o OFDM é o 802.11n. Contudo, o OFDM é implementado em conjunto com uma solução que permite a transmissão/recepção de dados através de múltiplos transmissores, receptores ou antenas paralelamente. Esta solução foi batizada de MIMO (*Multiple-Input Multiple-Output*). A velocidade a ser atingida pode chegar a 600 Mbps em quatro fluxos de MINO (4x4), ou seja, dois transmissores e dois receptores.

2.3.2 802:11: Modos de operações

Basicamente, existem dois modos de operações em WLANs, o modo Ad-Hoc e o modo infra-estrutura. A seguir, nos próximos dois subitens, eles serão apresentados.

2.3.2.1 Modo Ad-Hoc

Redes sem fio operando no modo Ad-Hoc podem operar sem a utilização de APs. Para o funcionamento das redes Ad-Hoc, os dispositivos devem ser configurados para operar neste modo e já conseguem trocar dados entre si. Contudo, os APs também podem ser configurados neste modo e uma aplicação para isso é a implementação das redes *wireless* em malha. Para que os pacotes saibam o melhor caminho em redes ad hoc em malha, o uso de um protocolo de roteamento é necessário. O OLSR será o protocolo ser configurado nos APs para a topologia futuramente apresentada na presente pesquisa.

O protocolo *Optimized Link State Routing* (OLSR) é um protocolo de roteamento proativo para redes Ad-Hoc móveis. Baseado em algoritmo para protocolos de roteamento *Link State* (Estado de Link), como o OSPF, por exemplo, o OLSR já possui as rotas definidas quando necessário, por isso chamado de protocolo proativo. Um equipamento operando com OLSR seleciona os nós vizinhos (equipamentos diretamente conectados), chamados de *Multipoint Relays* (MPR) e troca mensagens de controle apenas com esses equipamentos. As informações de melhor rota ou caminho mais curto para um destino também são trocadas somente entre MPRs. A idéia de MPRs é minimizar a quantidade de mensagens na rede, reduzindo retransmissões redundantes na mesma porção de rede.

O OLSR tem um número seqüencial em cada mensagem, portanto não requer a entrega seqüenciada dos pacotes. Definido para comunicar-se via protocolo UDP, porta 698, o OLSR também não exige transmissão confiável de mensagens de controle, pois cada nó envia as mensagens periodicamente e conseqüentemente pode suportar algumas perdas de mensagens.

A base desta visão geral sobre o protocolo OLSR foi retirada da RFC (*Request for Comments*) 3626, a qual descreve o funcionamento do OLSR. Informações mais detalhadas como, por exemplo, algoritmo utilizado, formato do pacote e troca de mensagens, podem ser encontradas na RFC 3626 e o caminho para tal encontra-se no presente projeto, sessão Referências.

2.3.2.2 Modo Infra-Estrutura

O modo infra-estrutura, por sua vez, implica na implementação de um ponto de acesso *wireless* conectado à rede ethernet por meio de um cabo metálico tradicional. Dispositivos configurados para este modo de operação não podem enviar *frames* diretamente um ao outro. Ao invés disso, eles enviam seus *frames* para um AP, e este os encaminha para o destinatário (FILIPPETTI, MARCO AURÉLIO, 2008, p. 79). A operação em modo infra-estrutura com a utilização de apenas um AP é chamada de *Basic Service Set* (BSS) e se forem utilizados dois ou mais APs para o mesmo modo de operação, os serviços são chamados de *Extended Service Set* (ESS).

2.3.3 802:11: Padrões derivados

Desde sua primeira publicação, em 1997, o padrão 802.11 vem passando por melhorias e inovações, geralmente acompanhando as novidades em tecnologia e a demanda dos usuários. Os padrões mais conhecidos em WLANs que derivaram do original 802.11 foram 802.11a, 802.11b, 802.11g e o 802.11n. Como as técnicas de modulação e larguras de banda de cada um já foram mencionadas anteriormente, será apresentado uma visão geral com as principais características de cada um.

2.3.3.1 Padrão 802.11a

O padrão 802.11a utiliza a modulação OFDM e opera na faixa de freqüências de 5 GHz, conseguindo velocidades de até 54 Mbps. A vantagem

em utilizar esta faixa de freqüências é que devido a maioria dos equipamentos operar na faixa de 2,4 GHz a ocorrência de interferência é menor. Por outro lado, a utilização de freqüências maiores gera ondas menores e facilmente bloqueadas por obstáculo, além disso, a distância que se consegue é menor.

Outro quesito para a faixa de freqüências de 5 GHz é que esta não é regulamentada pelos órgão responsáveis em alguns países.

2.3.3.2 Padrão 802.11b

Utilizando a técnica de modulação DSSS e operando na faixa de 2,4 GHz tornou o padrão 802.11b um dos principais padrões lançados pelo IEEE, em meados de 1999. A compatibilidade das freqüências com a grande maioria dos equipamentos e a possibilidade de atingir taxas de 11 Mbps também foram vantagens proporcionadas pela criação deste. Contudo, com o aumento do tráfego de dados, os 11 Mbps conseguidos pelo 802.11b não foi adequado.

Além da compatibilidade com os equipamentos que utilizam tecnologia *wireless*, as vantagens de se operar na faixa de 2,4 GHz são o alcance e o baixo custo de implantação.

2.3.3.3 Padrão 802.11g

Operando também na faixa de 2,4 GHz, mas com a escolha da técnica de modulação entre OFDM e DSSS tornou o padrão 802.11g o mais utilizado atualmente. Este padrão trouxe a possibilidade de se trabalhar na faixa de freqüência mais utilizada e com taxas de transmissão de dados podendo chegar à 54 Mbps (com modulação OFDM). A exemplo do padrão 802.11b, a operação na faixa de freqüências de 2,4 GHz traz os prós e os contras para o padrão 802.11g.

A compatibilidade entre o padrão 802.11g com o padrão 802.11b, sob modulação DSSS, também é um fator importante a ser mencionado, pois os usuários que já obtinham equipamentos com o 802.11b em funcionamento não precisaram redefinir sua rede para comunicar-se com equipamentos do novo padrão.

2.3.3.4 Padrão 802.11n

Aprovado em 2009, o padrão 802.11n veio para melhorar muito as taxas de transmissão atingidas nos padrões anteriores sem a necessidade de alocação de nova faixa de freqüência. Este padrão opera nas faixas de freqüências de 2,4 GHz e 5 GHz, o que possibilita a interoperabilidade com os padrões anteriores, mas tomando cuidado com questões de compatibilidade, pois, por exemplo, em uma rede com um AP que possibilita comunicação em 802.11n e dispositivos trabalhando em modo 802.11n e 802.11g, o padrão 802.11g prevalece e todos os equipamentos da redes farão suas transmissões no mesmo padrão.

Utilizando modulação OFDM, o padrão 802.11n conta agora com a adição da tecnologia MIMO o que possibilita a divisão de altas taxas de transmissão de dados em fluxos de transmissão menores, transmitindo-os simultaneamente através das múltiplas entradas e saída disponíveis nos equipamentos. Com isso, as taxas de dados podem chegar a 600 Mbps em canais de 40 MHz, na faixa de frequência de 5 GHz e com fluxo de MIMO 4X4, ou seja, quatro entradas e quatros saídas trabalhando simultaneamente.

Apesar de todas as vantagens, devido ao legado existente, este padrão ainda não é o mais utilizado atualmente.

2.4 QUALIDADE DE SERVIÇO (QoS)

Devido ao grande fluxo de informação nas comunicações de dados, o funcionamento das redes atuais exige alguma técnica que permita aos dispositivos saber quais os dados prioritários em um fluxo, ou seja, em possíveis descartes de pacotes os dados prioritários não sejam os primeiros a serem afetados. A função da técnica chamada de Qualidade de Serviço – *Quality of Service*, ou mais conhecida como QoS, surgiu justamente para tratar esse tipo de questão. Um exemplo da necessidade de implementação de QoS pode ser analisado comparando-se dois serviços muito utilizados, o Voip e o E-mail. O e-mail não necessita de entrega imediata (*on-line*) e caso haja algum descarte de pacotes com conteúdo do e-mail, o mesmo pode ser retransmitido e isso não ocasionará problemas ao destinatário, que receberá a mensagem da mesma maneira. Agora, analisando-se o Voip, caso haja algum problema na

transmissão e um pacote seja descartado, o áudio chegará ao destino com falhas de picotamento e por se tratar de uma conversação em tempo real, não existe a possibilidade de retransmissão. Em redes Voip, a qualidade da linha, a reserva de banda e o tempo de entrega dos pacotes são essenciais para uma boa comunicação. Através de marcação nos pacotes concorrentes ao mesmo fluxo de dados, a confiabilidade de uma comunicação Voip é possível. Claro que este foi apenas em exemplo dados, pois em cada ambiente o administrador da rede deverá saber o que é prioritário ou não.

Os principais fatores que determinam a utilização de técnicas de QoS em transmissões de dados são: Latência, perda de pacotes, *jitter* e largura de banda (*bandwidth*).

Latência é o tempo que os bits levam da origem ao destino ou caso haja necessidade de confirmação da entrega, é o tempo de chegada ao destino somado ao tempo de confirmação.

Perda de pacotes é o descarte de pacotes que por algum motivo não conseguiram alcançar o destino, onde as possíveis causas estão na saturação da banda disponível e erros encontrados na checagem feita pelo destino.

O *jitter*, segundo Tanembaum (2003, p.306), é a variação dos tempos de chegada dos pacotes até um destino. Em aplicações de áudio ou vídeo, não importa demoram 20 ms (milissegundos) ou 30 ms para serem entregues, desde que o tempo em trânsito seja constante. Um *jitter* elevado, no qual alguns pacotes demoram 20 ms e outros demoram 30 ms para chegar, resultará em qualidade irregular do som ou do vídeo.

Largura de banda é o link contratado para o tráfego do fluxo de dados, ou seja, a quantidade de bits por segundo que a rede suporta transportar. O protocolo Frame-Relay, por exemplo, permite a garantia banda mínima para determinado serviço através da configuração do CIR (*Commited Information Rate*).

Existem varias maneiras de se aplicar técnicas de QoS em uma rede, as quais podem ser chamadas de modalidades de QoS e sua aplicação dependerá da tecnologia utilizada na rede e da forma que o administrador achar viável de se tratar o fluxo de dados (priorizando os pacotes ou garantindo banda). De uma maneira geral, as principais modalidades de QoS são Tipo de Serviço (ToS), Serviços Integrados (IntServ), Serviços Diferenciados (DiffServ) e através do *Label* (Rótulo) em MPLS (*Multi-Layer Protocol Label Switching*). Nos quatro tópicos subseqüentes, serão descritas cada uma das modalidades.

2.4.1 Tipo de Serviço

Esta modalidade de QoS chamada de Tipo de Serviço (ToS), utiliza um campo de 8 bits do cabeçalho IP, chamado justamente de ToS, para prover os serviços. O cabeçalho IP pode ser visto na figura 11.

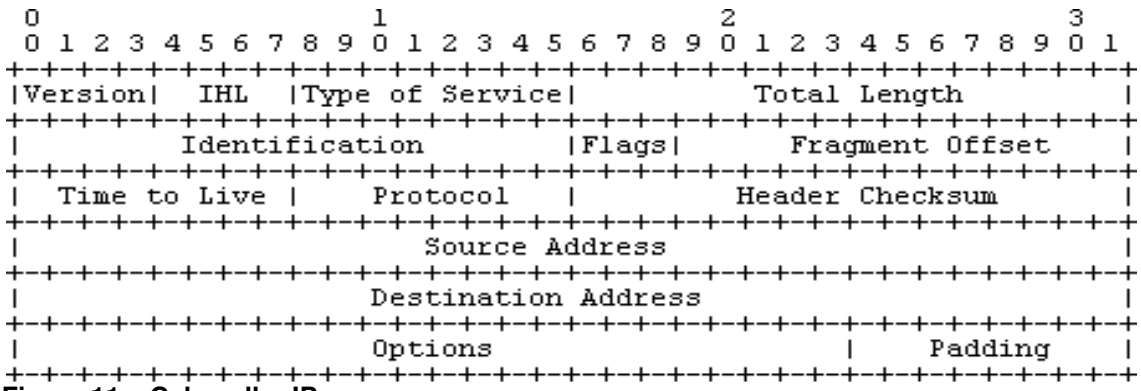

Figura 11 – Cabeçalho IP
Fonte: Teleco – PTT no Celular II – Protocolo IP, 2007.

O campo ToS é usado para especificar o tratamento do datagrama durante sua transmissão através da rede. Segundo a RFC 791, que descreve o protocolo IP, no campo ToS os três primeiros bits (0, 1 e 2) são chamados de bits de precedência e indicam a importância do datagrama, sendo possíveis oito combinações distintas. Os bits 3, 4 e 5 representam *Delay* (Atraso), *Throughput* (rendimento) e *Reliability* (Confiabilidade), respectivamente. Os bits definidos em “0” representam a operação normal e os bits “1” representam a melhoria de cada quesito, onde a seqüência 111 representa baixo atraso, alto rendimento e alta confiabilidade. Por fim, os bits 6 e 7 são destinados para uso futuro.

A figura 12 mostra com mais detalhes o campo ToS e o significado das combinações dos bits de precedência:

```
Bits 0-2:  Precedence.
Bit    3:  0 = Normal Delay,      1 = Low Delay.
Bits   4:  0 = Normal Throughput, 1 = High Throughput.
Bits   5:  0 = Normal Relibility, 1 = High Relibility.
Bit  6-7:  Reserved for Future Use.

   0     1     2     3     4     5     6     7
+-----+-----+-----+-----+-----+-----+-----+-----+
|                 |     |     |     |     |     |
|   PRECEDENCE    |  D  |  T  |  R  |  0  |  0  |
|                 |     |     |     |     |     |
+-----+-----+-----+-----+-----+-----+-----+-----+

  Precedence

    111 - Network Control
    110 - Internetwork Control
    101 - CRITIC/ECP
    100 - Flash Override
    011 - Flash
    010 - Immediate
    001 - Priority
    000 - Routine
```

Figura 12 – ToS
Fonte: IETF – RFC 791 – *Internet Protocol Specification*, 1981.

2.4.2 Serviços Integrados

A modalidade de QoS chamada IntSev foi desenvolvido para a garantia de fluxos de dados individuais, onde o caminho fim a fim é definido e ocorre a reserva dos recursos necessários para a comunicação (banda, tamanho de *buffer* e tempo da sessão). Todos os equipamentos da rede até o destino devem saber a quantidade de recursos a ser reservada. Para isso, o transmissor deve estabelecer uma comunicação com o receptor e informá-lo a quantidade de recursos necessários. O responsável por estabelecer esta comunicação, bem como a alocação dos recursos, é o protocolo RSVP (*Resource Reservation Protocol*)

O protocolo RSVP é empregado para fazer as reservas, apenas operando com mensagens de controle, diferentemente de outros protocolos utilizados para a transmissão de dados. Basicamente, o funcionamento do RSVP consiste em um emissor solicitar uma QoS específica para o receptor que envia uma mensagem de reserva RSVP de volta com a QoS que deveria ser reservada para o fluxo do emissor para o receptor. O emissor não precisa saber quais são as características de todos os possíveis receptores para estruturar as reservas (BRUN , ALTAMIR. VOGT, EIDE., 2002, p.45).

O RSVP permite que vários transmissores enviem os dados para os vários grupos de receptores, torna possível receptores individuais mudarem livremente de canais e otimiza o uso da largura de banda ao mesmo tempo que elimina o congestionamento. Ao fazer uma reserva, um receptor pode (opcionalmente) especificar uma ou mais origens a partir da quais deseja receber informações. Ele também pode especificar se essas opções serão fixas durante o período da reserva, ou se o receptor deseja manter em aberto a opção de alterar as origens mais tarde. Os roteadores utilizam essas informações para otimizar o planejamento para a largura de banda. Em particular, dois receptores só serão configurados para compartilhar um caminho se ambos concordarem em não alterar as origens posteriormente (TANENBAUM, ANDREW S., 2003, p.318).

Apesar da reserva de recursos para um funcionamento adequado das aplicações, a utilização de Intserv torna-se inviável em uma rede mais robusta, pois deverá manter as informações de sessão (fluxo) em cada roteador participante do caminho fim a fim, efetuar atualizações periódicas para que a sessão não seja encerrada. Outra desvantagem em se reserva antecipadamente a banda pode ser analisada em um vídeo conferência, por exemplo, onde casa haja necessidade de mais participantes e a banda saturaria e a aplicação da QoS não resultaria em melhorias.

2.4.3 Serviços Diferenciados

Este modalidade de QoS denominada Serviços Diferenciado ou mais conhecido com DiffServ, baseia-se na qualidade de serviço em classe, ou seja, cada pacote em um fluxo de dados é analisado e encaminhado de acordo com sua devida prioridade ou garantia de serviço.

A idéia fundamental dos Serviços Diferenciados é definir em conjunto de pequeno de mecanismos que possam ser implementados nos nós da rede e que suportem uma grande variedade de serviços. Os Serviços Diferenciados são oferecidos no interior de um domínio de diferenciação de serviços (domínio DS), o qual é composto por um conjunto de nós que compartilham uma mesma política de serviços. Um domínio DS provê a diferenciação de serviços somente em uma direção, sendo assim assimétrico (LIMA, CARLOS EDUARDO, 2001).

Assim como ocorre em QoS baseado no tipo de serviço, o DiffServ também utiliza o campo ToS do cabeçalho IP, mas nesta modalidade o ToS

chama-se campo DS e é inserido nos equipamentos de borda. São analisados pelos nós da rede os seis primeiros bits como um todo e continua-se ignorando a utilização dos dois últimos bits. Os seis bits mencionados formam um código diferenciador de serviços, chamado DSCP (*Differentiated Services Code Point*). Através destes seis bits consegue-se 64 possibilidades de tratamento dos pacotes nos nós de rede em um domínio DS. Este tratamento é chamado de *Per-Hop Behavior* (PHB). O tratamento baseado em PHB (classe), define-se principalmente em três categorias: PHB Padrão, Encaminhamento Expresso (PHB-EF) e Encaminhamento Assegurado (PHB-AF).

O PHB padrão utiliza melhor esforço para o fluxo de dados marcados com esta classificação de DSCP, ou seja, pacotes marcados com PHB padrão não tem prioridade no domínio DS e seguem o fluxo normalmente desde que haja banda para isso. Em caso de congestionamento, se pacotes com PHB padrão forem comparados com outras classes, serão os primeiros a serem descartados.

O PHB-AF é aplicado em pacotes com necessidade de priorização em momentos de congestionamento, mas sem a necessidade de garantia de fazendo. Neste serviço, a utilização da banda é feita através de demanda de cada pacote, onde, por exemplo, marcação com PHB AF-13 tem maior prioridade no fluxo do que pacotes marcados com PHB AF-22. Contudo, se a banda estiver disponível, qualquer pacote poderá seguir o fluxo normalmente. Os serviços prestados por este tipo de PHB são chamados de serviços olímpicos, pois marcações do tipo PHB-AF são definidas como ouro, prata e bronze, onde ouro tem maior prioridade que as demais, seguindo uma lógica relacionada à preciosidade dos metais. Para melhor entendimento, é possível fazer uma analogia com uma fila de banco, na qual existe a prioridade para idosos. Se tiverem dez pessoas e chegar uma pessoa idosa, esta pessoa passará a frente dos demais e seguirá ao caixa de idosos. Contudo, se o caixa de idosos estiver livre, as demais pessoas da fila poderão ser atendidas. A figura 13 apresenta as marcações de PHB-AF em um DSCP:

DROP Precedence	Class #1	Class #2	Class #3	Class #4
Low Drop Precedence	(AF11) 001010	(AF21) 010010	(AF31) 011010	(AF41) 100010
Medium Drop Precedence	(AF12) 001100	(AF22) 010100	(AF32) 011100	(AF42) 100100
High Drop Precedence	(AF13) 001110	(AF23) 010110	(AF33) 011110	(AF43) 100110

Figura 13 – Marcação PHB-AF
Fonte: Cisco Systems – *Quality of Service – The Differentiated Services Model*, 2008.

O último modelo de PHB é o de encaminhamento expresso ou PHB-EF. Esta marcação tem como principal característica diminuir o tempo dos pacotes em transito, evitando que seu fluxo seja atrapalhado por possíveis congestionamentos e possibilitar a entrega de uma maneira mais confiável. Esta técnica consiste em alocar uma porcentagem do total da banda para tráfego de pacotes marcados com PHB-EF e descartá-los caso esta porcentagem seja excedida. Devido a isso, deve analisar-se muito bem a rede antes de fazer qualquer configuração de QoS deste tipo, pois se a banda garantida for muito baixa, em aplicações de VoiP, por exemplo, a possibilidade de falhas de áudio será maior. Em contrapartida, se a banda garantida for muito alta, poderá afetar o tráfego das demais aplicações na rede.

Serviços que utilizam marcação PHB-EF podem ser classificados com *Premium*. Geralmente os pacotes excedentes às porcentagens defefinidas são tratados de duas maneiras, sendo uma o descarte de pacotes acima da taxa e a outra é retardá-los o maior tempo possível.

A QoS de serviços diferenciados tem sua definição contratual (cliente e operadora) baseado em um acordo de serviço entre ambas as partes, onde são definidos quesitos como os tempos de atraso dos pacotes, tempo de disponibilidade do enlace, tempo para resolução de problemas, ou seja, métricas relacionadas diretamente ao funcionamento do *link.* O acordo é chamado de SLA (*Service Level Agreement*) e caso não seja cumprido o responsável estará sujeito ao pagamento de multas contratuais.

2.4.4 QoS em MPLS

Quando um roteador recebe um pacote e precisa encaminhá-lo para uma interface de saída, ele deve analisar toda a tabela de roteamento para encontrar o melhor caminho. Visando diminuir o processamento dos roteadores, bem como o tempo de entrega do pacote ao destino, foi desenvolvida uma técnica para comutação de pacotes baseada em rótulos (*labels*). O rotulo foi inserido entre o cabeçalho do protocolo de camada 2 e o cabeçalho IP. Este protocolo foi chamado de MPLS (*Multi-Layer Protocol Label Switching*) e ficou conhecido como protocolo de camada dois e meio. Antes da transmissão dos pacotes há um mapeamento dos rótulos na rede, onde cada nó armazena em uma tabela o rótulo e a porta de saída. Após a rede convergida, cabe aos roteadores apenas analisar o rótulo e fazer a comutação dos pacotes até o destino.

O rótulo MPLS contém 32 bits, sendo 20 deles para a identificação do rótulo (campo *label*), 3 bits que possibilitam classificação dos pacotes baseado no rótulo (campo QoS ou EXP), 1 bit no campo *stack* ou S, o qual possibilita um pacote receber mais de um *label*, fazendo assim um empilhamento de *labels* e quando este bit estiver em “1”, significa que o *label* anterior é o último da pilha e por fim um campo 8 bits indicando o TTL (*Time to Live*) o qual determina a quantidade de saltos que um pacote poderá percorrer antes de ser descartado.

2.5 FIRMWARE DD-WRT

O DD-WRT é um firmware baseado em Linux e liberado sob os termos de publicação de softwares GLP (*General Public Licence*) para a utlização em roteadores *wireless* IEEE 802.11 a/b/g/n (DD-WRT, 2011). A documentação necessária para instalação do firmware e demais informações para as configurações básicas (IP, SSID, senhas, etc) estão disponíveis na página oficial da comunidade DD-WRT (www.dd-wrt.com).

A configuração do AP com DD-WRT para operar em malha e também para a configuração da QoS está disponível no capítulo Estudo de Campo, subitem Configurando o *Access Point*.

2.5.1 QoS no DD-WRT

A QoS do DD-WRT pode ser configurado para a saídas/entradas WAN (que utilizam a internet) ou internamente no AP para a rede local e é baseado em regras de *iptables*. O *iptables* é uma aplicação que permite criar regras no tráfego em uma rede e na grande maioria das vezes é utilizado em servidores de borda com sistema operacional Linux. As regras e comandos do *iptables* são assuntos um tanto quanto extensos e fogem um pouco do espoco da pesquisa, mas o importante é entender como a QoS é feita no DD-WRT. A marcação dos pacotes para QoS no DD-WRT ocorre na tabela *mangle* do *iptables* e prevê cinco classificações de serviço, sendo elas, *Exempt, Premium, Express, Standard e Bulk*.

A classe *Exempt* é a dominante e utiliza 100% da banda disponível caso marcado em algum pacote. Se aplicações que utilizarem está classe e necessitarem de muita largura de banda, pode interferir no funcionamento dos demais dados passantes pela rede. Devido a isso, a utilização dessa classe deve ser cuidadosamente analisada, aplicada em casos extremos e com a divisão da banda total sendo feita da maneira correta. O pacote participante da classe *Exempt* recebe marcação 100.

A classe *Premium* é a classe que prevê maior largura de banda para priorização (75% de 100%) e é bem utilizada em serviços VoIP. A pacote desta classe é marcado com valor 10.

A classe *Express* é geralmente é utilizada para serviços que não demandem muita banda, mas que quando forem requeridas as aplicações, exista banda suficiente para o correto funcionamento. Utiliza 15% de 100% da banda e Telnet e SSH são exemplos que se encaixam nessa classe. O pacote com marcação 20 representa esta classe.

A classe *Standard* é a classe considerada padrão nos pacotes que utilizam a QoS. São os tráfegos que possivelmente podem ter retransmissão (no caso de TCP) ou passíveis de perdas. A banda alocada para esta classe é 10% de 100% e o pacote recebe marcação 30.

A classe *Bulk* é a classe inferior a todas com apenas 1,5% de 100% da banda e é utilizada somente se houve banda disponível, ou seja, se as demais classes estiverem com suas transmissões ociosas. Os pacotes da classe *Bulk* são marcados com valor 40 e geralmente aplicações *Peer to Peer* (P2P) se encaixam nesta classe.

Os pacotes que não estiverem com seus serviços especificados na configuração da QoS recebem valor de marcação 0.

A QoS no DD-WRT pode ser aplicada em endereços MAC, endereços IP, aplicações/protocolos(UDP, TCP, ICMP) e portas ethernet do AP. A escolha ou desempate para a aplicação da QoS segue o mesmo critério, MAC, IP, aplicação/porta e porta ethernet.

3 ESTUDO DE CAMPO

Este capítulo apresentará a configuração do *Access Point* para operar com e sem a configuração de QoS aplicada. Serão realizados testes e posteriormente publicados os resultados a fim demonstrar o funcionamento das técnicas de QoS .

Serão espalhados quatro APs, operando com o protocolo OLSR. O firmware utilizado é o DD-WRT, que é um firmware livre, baseado em Linux, como já mencionado.

Primeiramente, será feito o teste sem a utilização de QoS aplicado, onde o link será saturado e poderá notar-se o tempo de resposta de um pacote ICMP ou em downloads via FTP.

Na sequência, será aplicado QoS em determinadas portas, como por exemplo na faixa UDP 5000, muito utilizada em VoIP. Os resultados também serão visualizados nos tempos de resposta, mas agora comparando-se dados transmitidos com QoS e sem QoS.

A saturação do link será feita com a utilização de uma ferramenta para mediação de desempenho, chamada JPerf. Esta ferramenta é de uso gratuito e com ela consegue abrir várias sessões para trafego de pacotes UDP ou TCP, possibilitando a escolha de porta de destino, largura de banda, tamanho do segmento e tamanho do *buffer*. Opera no modo cliente/servidor, onde para o presente projeto, os clientes serão os *hosts* conectados aos APs e o servidor será uma maquina a qual será conectada ao *gateway* com saída para internet.

A topologia de testes pode ser vista na figura 14:

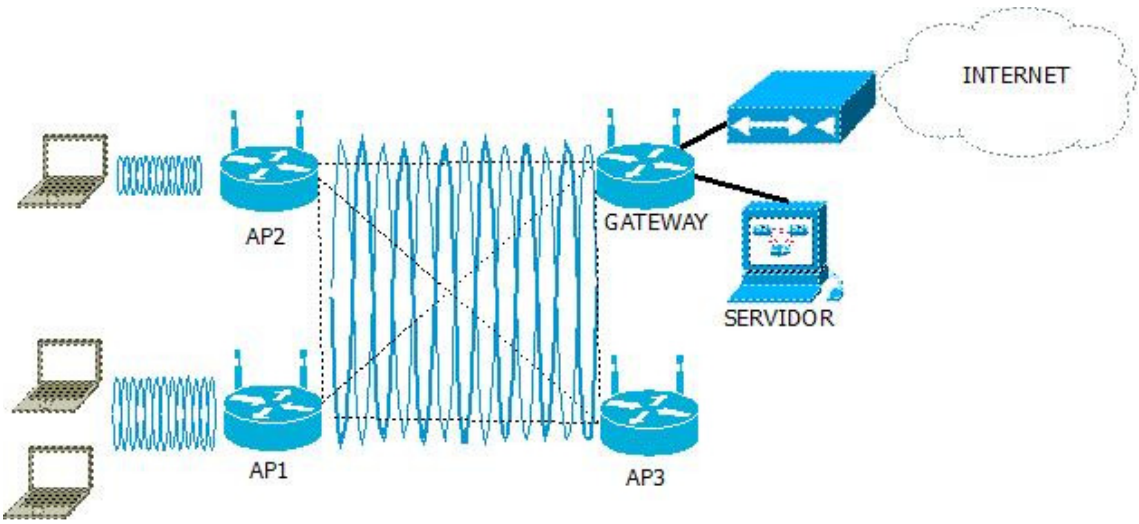

Figura 14 – Topologia de Estudo de Campo
Fonte: Autoria Própria.

Para familiarização, a figura 15 apresenta a interface gráfica do software gerador de tráfego, JPerf.

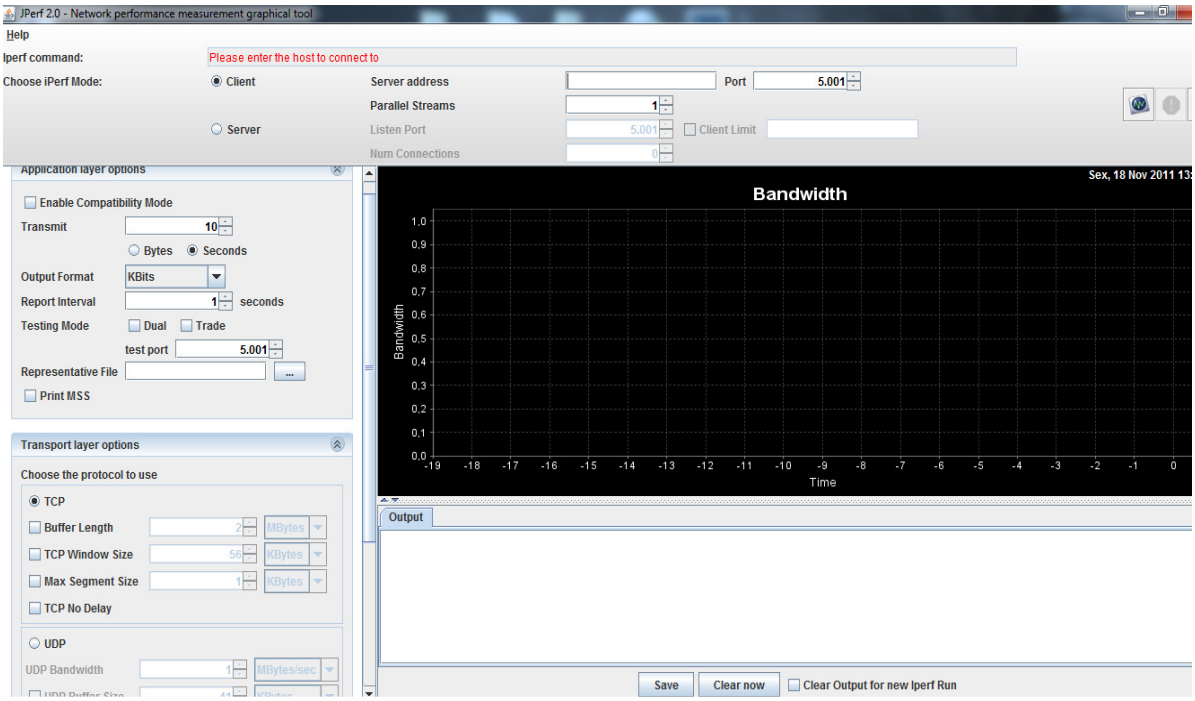

Figura 15 – JPerf
Fonte: Autoria Própria.

Depois de gerado o tráfego de dados para saturação do link, deve-se analisar se realmente há a marcação dos pacotes conforme previsto. Para este fim, com o firmware DD-WRT faz a marcação baseada em regras de *iptables* utilizar-se-á o próprio AP na verificação de marcação. Posteriormente, será informado o comando para tal.

3.1 CONFIGURANDO O *ACCESS POINT*

Para a configuração dos APs para operar em modo *mesh*, primeiramente deve-se escolher as opções básicas. Para isso, deve-se ir até as abas *Wireless > Basic Settings.* Escolher o modo de operação Ad Hoc, o padrão de operação sem fio (b,g,misto), escolher o canal (escolhido canal 6), marcar a opção *unbridge de wlan* e colocar um IP (201.1.1.1/24) . Como o modo de operação *wireless* escolhido para a pesquisa foi o IEEE 802.11g,

todos os equipamentos *wireless* da rede devem suportar este padrão. A figura 16 demonstra as opções escolhidas para o estudo:

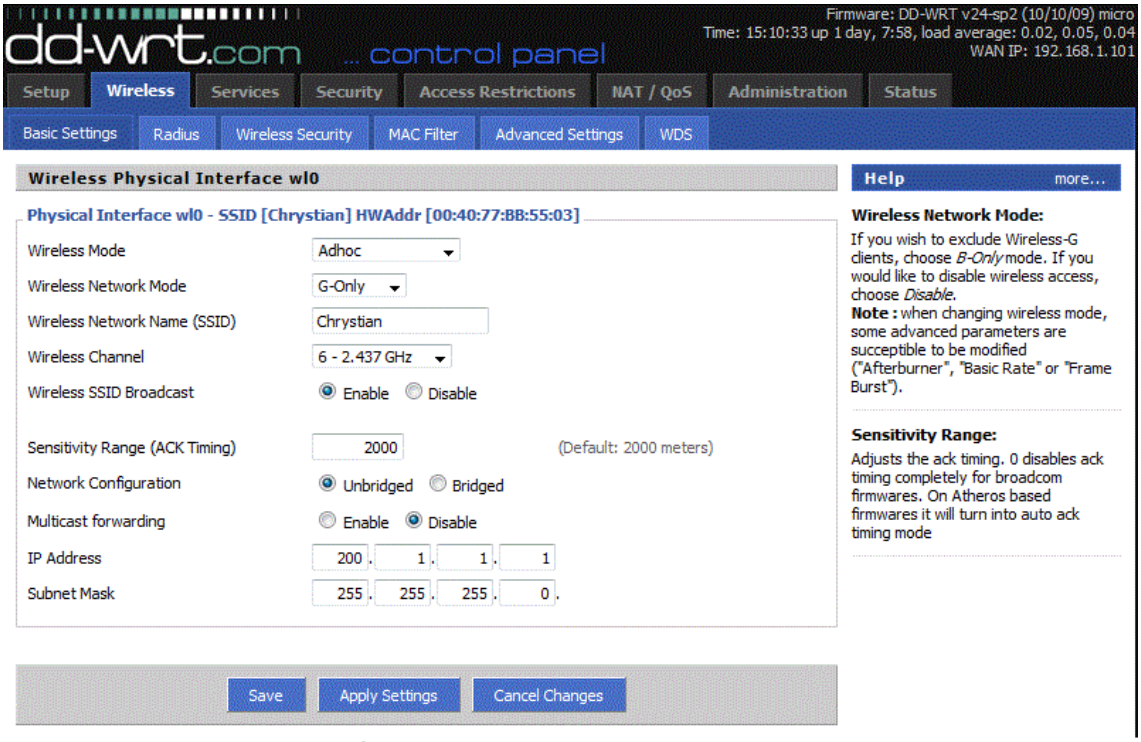

Figura 16 - Configurações Básicas do *Access Point.*
Fonte: Autoria Própria.

Após as configurações básicas, deve-se configurar o modo de roteamento para o protocolo OLSR. Para tal, deve ir até a opção *Setup*, selecionar a opção *Advanced Routing* e logo pode-se ver a opção *Operating Mode.* Ao lado desta opção há uma caixa, na qual deve ser colocada a opção OLSR Router. As demais opções são para limiares que influenciam no algoritmo de roteamento e podem ser deixadas com os valores padrão. A figura 17 mostra a configuração do OLSR no AP:

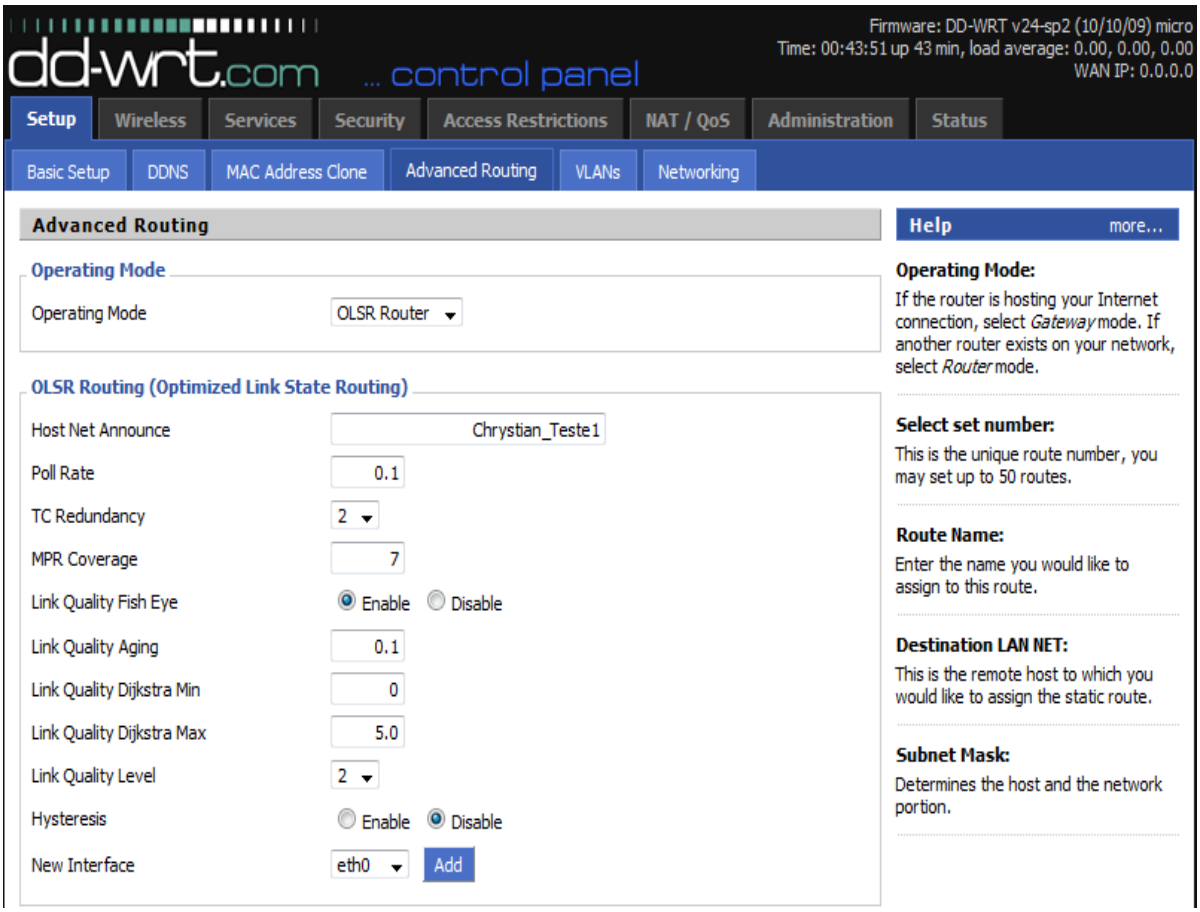

Figura 17 - Configurações do OLSR no *Access Point.*
Fonte: Autoria Própria.

Quando se habilita o OLSR, automaticamente é desabilitada a função de tradução de endereços, NAT (Network Address Translation), então, para se poder continuar com acesso à internet, no AP que será o *gateway* deve-se habilitar o NAT e para tal, conforme a comunidade do firmware DD-WRT (http://www.dd-wrt.com/wiki/index.php/Mesh_Networking_with_OLSR), as linhas de comando apresentadas na figura 18 devem ser digitadas após entrar nas opções *Administration > Commands*, no modo de configuração do AP:

```
iptables -t nat -A POSTROUTING -o $(nvram get wan_ifname) -j MASQUERADE

iptables -t nat -A POSTROUTING -o $(nvram get wl0_ifname) -s $(nvram get
eth1_ipaddr)/$(nvram get eth1_netmask) -d $(nvram get eth1_ipaddr)/$(nvram get
eth1_netmask) -j MASQUERADE

iptables -t nat -A POSTROUTING -o $(nvram get lan_ifname) -s $(nvram get
lan_ipaddr)/$(nvram get lan_netmask) -d $(nvram get lan_ipaddr)/$(nvram get
lan_netmask) -j MASQUERADE
```

Figura 18 – Habilitando NAT no AP Gateway.
Fonte: Autoria Própria (Baseado em DD-WRT, 2011).

Seguindo os passos mencionados para as configurações dos APs, podem-se realizar os testes de conectividade e acesso à internet, bem como os testes sem a aplicação da QoS.

A configuração de QoS no AP são feitas acessando as opções *NAT/QoS > QoS*, conforme figura 19:

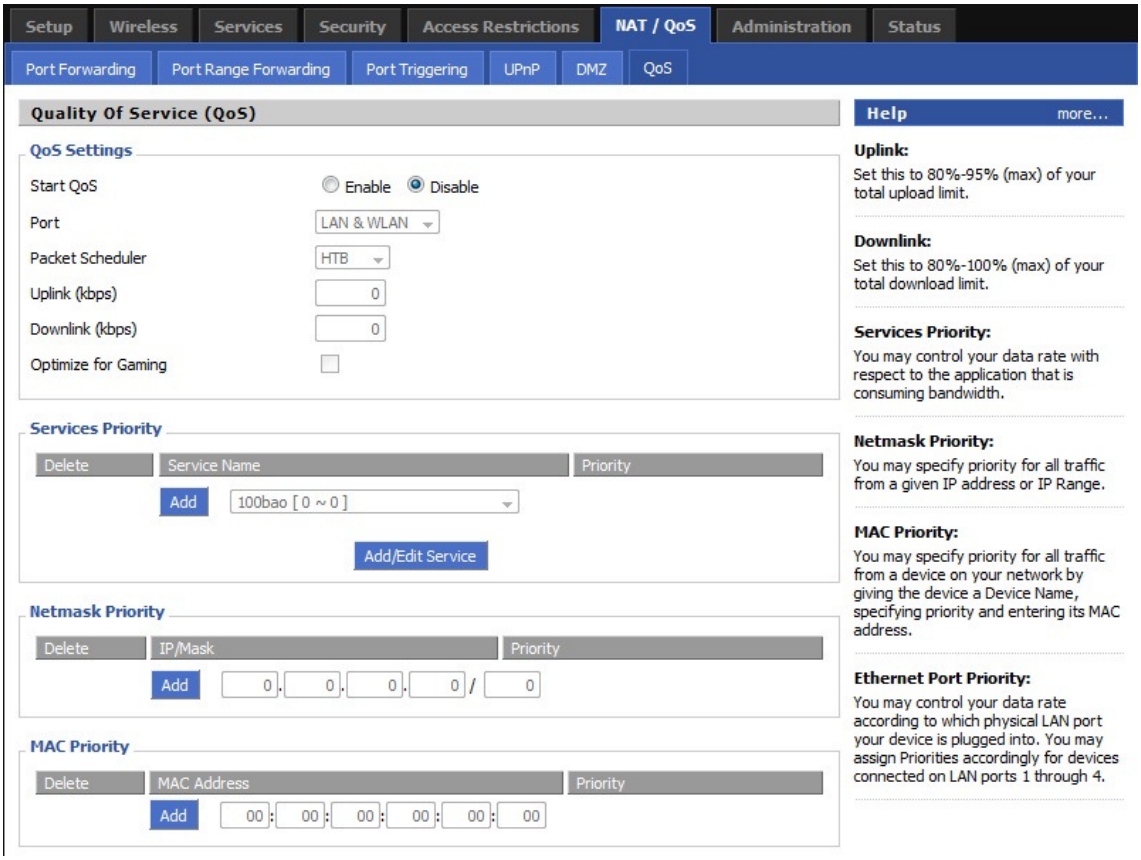

Figura 19 – Configurando QoS
Fonte: Autoria Própria.

Para configurar QoS baseado em endereço MAC, basta ir na opção *MAC Priority*, inserir o endereço conhecido e clicar em *ADD*. Para priorizar determinado endereço IP a opção é *Netmask Priority*, insere-se o endereço IP e máscara (se for uma máquina apenas insere-se máscara /32, se for range insere-se a mascara da rede) e clica-se em *ADD.* Para marcação por serviço (portas lógicas), primeiramente clica-se na opção *ADD/Edit Service*. Abrirá uma nova janela, conforme figura 20, onde define-se um nome para o serviço, o protocolo e o range de portas.

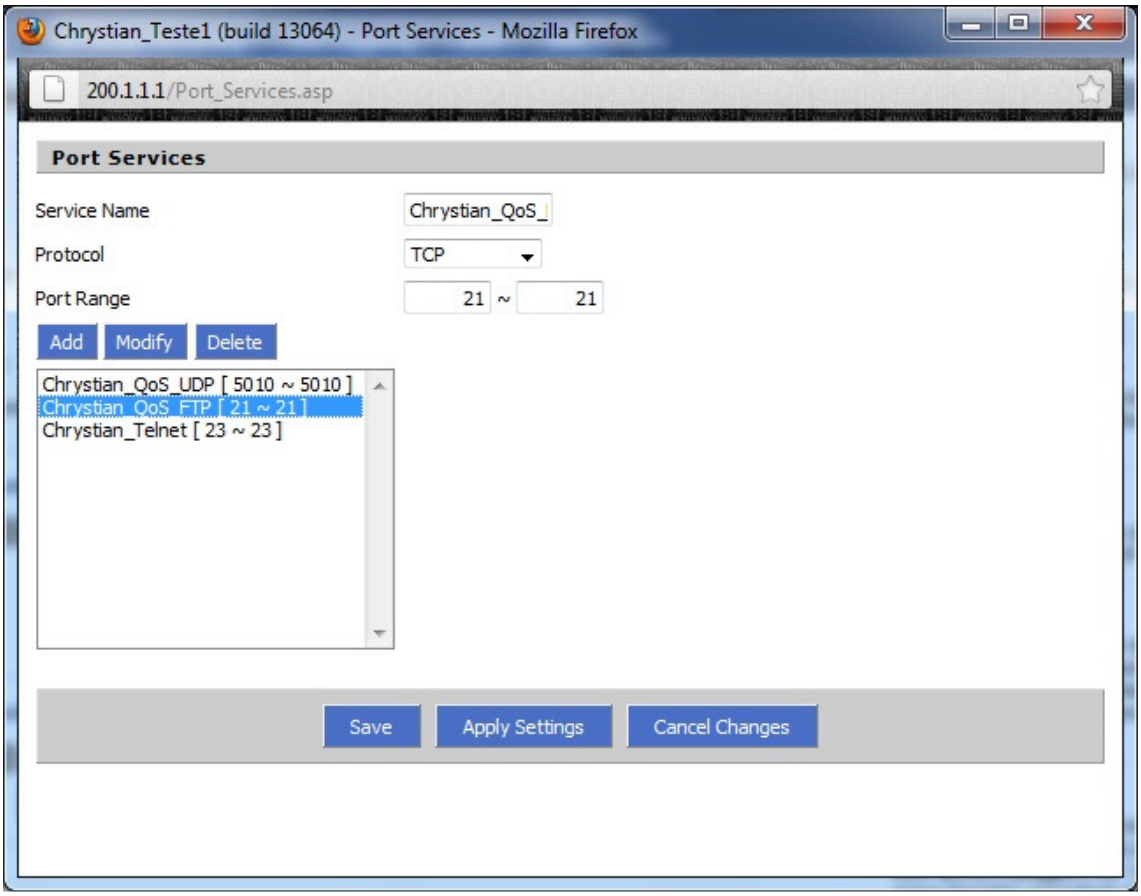

Figura 20 – QoS por serviço
Fonte: Autoria Própria.

Após isso, aplicar a alteração (*Apply Setting*) e depois salvar (*Save*). Após salvar a configuração, retorna-se à tela anterior (figura 19) e escolhe-se a opção configurada que se encontrará disponível na caixa seletora em *Service Name* e clica-se em *ADD.*

A configuração de QoS se aplicará ao AP somente após clicar na opção *Apply Settings*, no modo de configuração global do equipamento. Para evitar perdas de informação devido a uma eventual reinicialização do AP, deve-se salvar a configuração na opção *Save.*

3.2 TESTES E RESULTADOS

Os testes para chegar-se ao objetivo da presente pesquisa, iniciaram-se configurando os quatro APs para operar em Ad Hoc, com roteamento OLSR e com IPs fixos na faixa de 200.1.1.0/24. Após isso, deve-se configurar os *hosts* com IPs fixos (pois desabilitou-se o DHCP para o *wireless*), máscara /24 e *gateway* para o IP 200.1.1.1 (Ap com conexão com a internet e servidor). No

AP que atua como *gateway*, as portas ethernet foram definidas para operar na rede 192.168.0.0/24 e o servidor foi conectado à porta 1 do AP e recebeu o IP 182.168.0.102. Um *host* foi emulado no servidor através do software Virtual Box e recebeu o IP 192.168.0.122.

Para verificar o funcionamento da rede em malha, o teste foi realizado a partir da configuração de um laptop com o IP 200.1.1.100 e que não alcançasse diretamente o *gateway*, apenas um dos APs intermediários. Conectando-se ao ID da rede OLSR (deve ser o mesmo em todos os APs da *mesh*), foi possível chegar à internet e ao servidor normalmente. Em seguida, colocou-se outro AP intermediário na mesma disposição do anterior, de modo que os mesmos funcionem simultaneamente. Desligou-se o primeiro AP e notou-se que a conexão do laptop com o servidor e com a internet permaneceu ativa, concluindo-se com êxito o teste que previa o funcionamento da rede em malha (*mesh).*

Após concluir o funcionamento da rede, passou a analisar o tráfego para aplicação da QoS. Com a rede sem uso, efetuou-se um teste de *ping* de um *host* (200.1.1.102) para o *gateway*. O resultado foi o melhor possível (1milisegundo de tempo de resposta) e demonstra-se na figura 21:

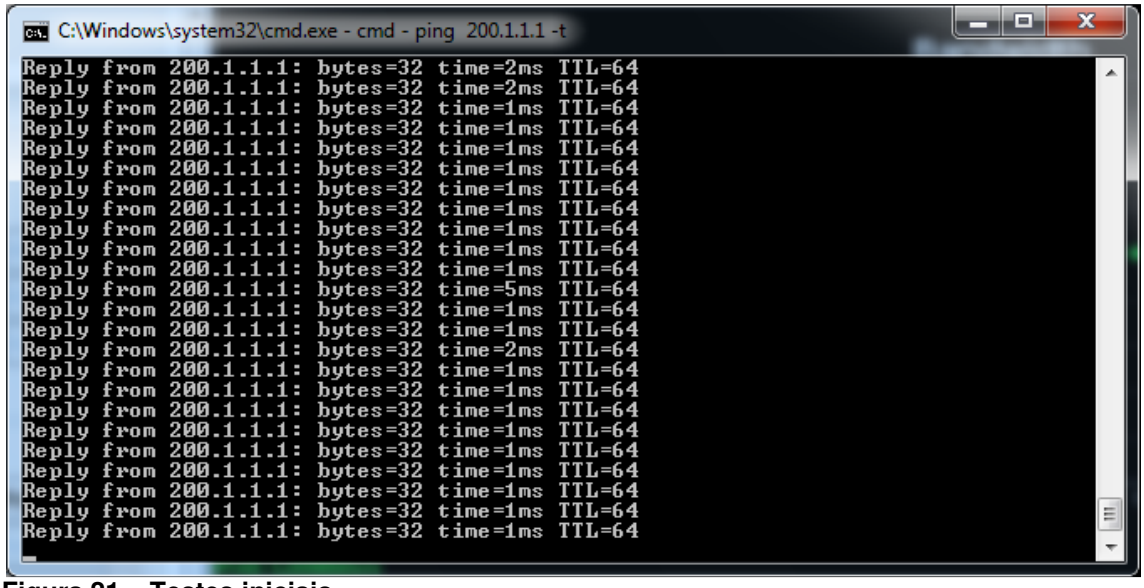

Figura 21 – Testes iniciais
Fonte: Autoria Própria.

Observando-se que a rede estava ok, foi gerado tráfego de várias origens e com serviços distintos, como internet (redes sociais, P2P, páginas em geral), tráfego com Jperf (3 sessões x 30Mbps e 4 sessões x 5Mbps) de um

host na rede 200.1.1.0/24 para o *host* (192.168.0.122). Foram abertas sessões FTP dos laptops para o servidor 192.168.0.102. Notou-se que o *led* WLAN (*wireless*) no *gateway* piscava extremamente rápido, o que indicou tráfego excessivo no mesmo. A figura 22 mostra uma das sessões aberta via Jperf, com tráfego de 30M, utilizado a porta UDP 5000 como destino e visualizada a partir do destino:

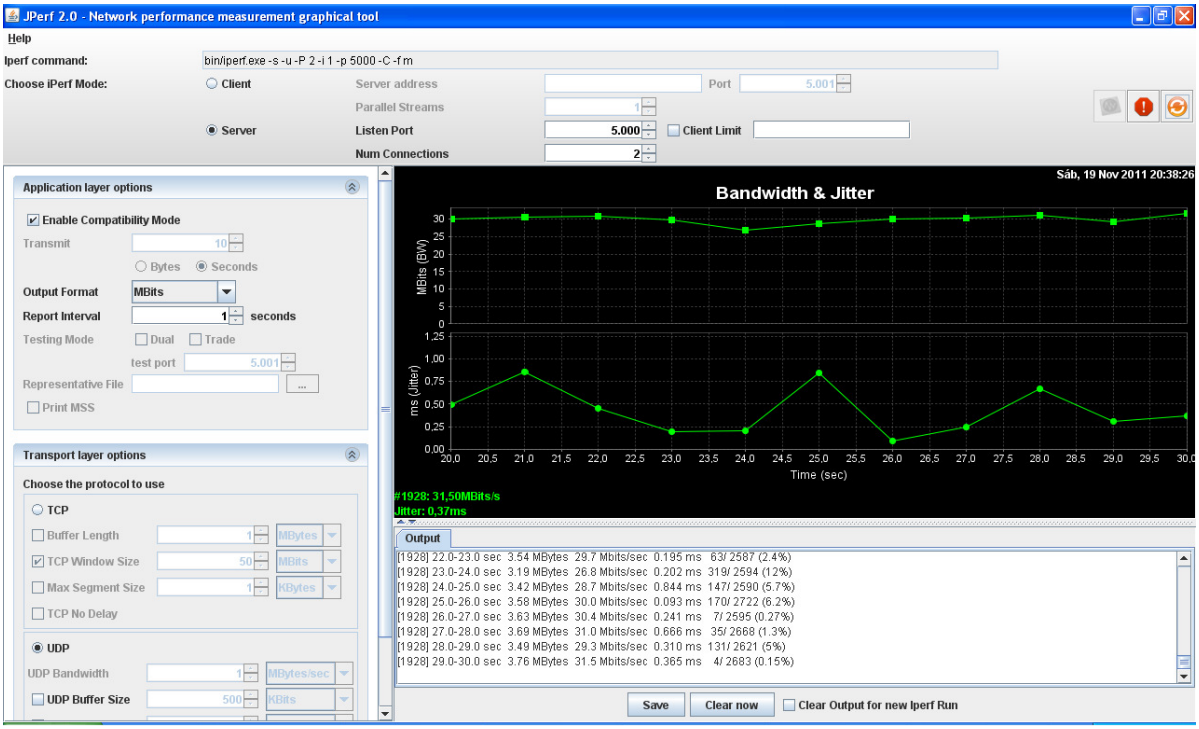

Figura 22 – Teste Jperf - Destino
Fonte: Autoria Própria

A figura 23 mostra o teste com Jperf a partir da origem, das quatro sessões de 5Mbps, sendo três delas para a porta UDP 5000 e uma delas para a porta UDP 5010:

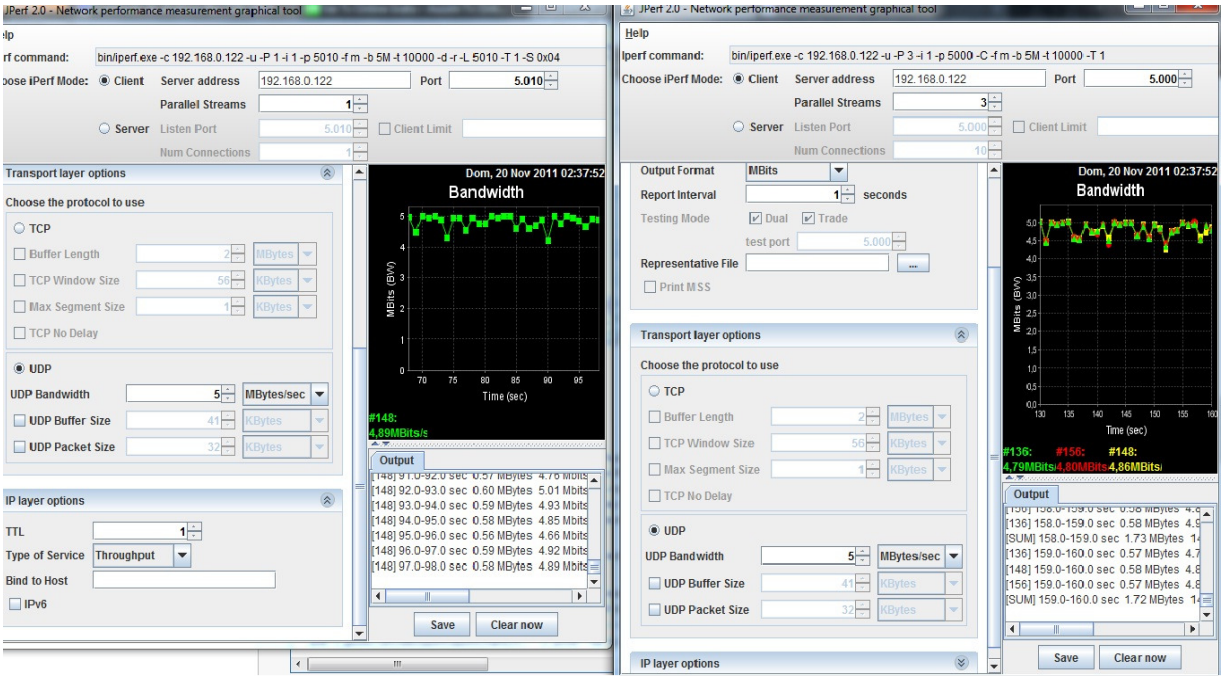

Figura 23 – Teste Jperf - Origem
Fonte: Autoria Própria

Com a rede saturada, o mesmo teste de *ping* foi realizado do *host* (200.1.1.102) para o *gateway* e obteve-se tempo de resposta de 3 segundos, além de pacotes descartados, conforme figura 24:

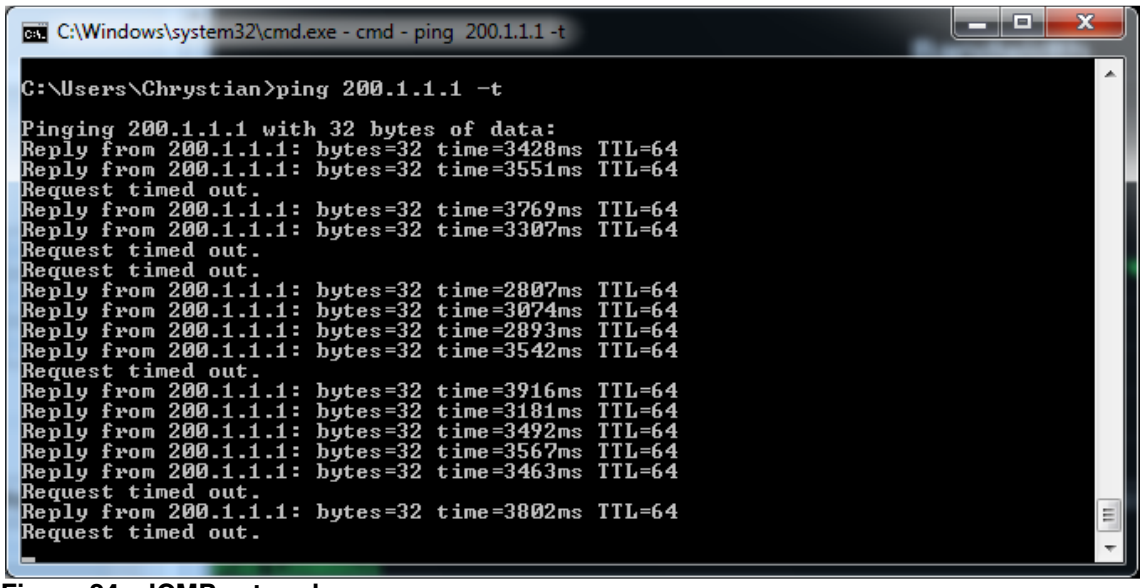

Figura 24 – ICMP saturado
Fonte: Autoria Própria.

Conforme mencionado anteriormente, consegue-se observar a marcação dos pacotes no AP, para verificar se há ou não a aplicação da QoS. Deve-se acessar o AP via telnet e no terminal digitar o comando *cat /proc/net/ip_conntrack*. Aparecerão todas as conexões ativas no AP. Como geralmente são muitas e o resultado fica um tanto bagunçado, pode-se utilizar do filtro */grep* para melhor busca. Para demonstração, eliminaram-se as conexões de 30M (devido lentidão) e aplicou-se o comando para buscar os resultados da porta UDP 5000, UDP 5010 e TCP 21. Analisando-se a figura 25, observa-se que ao final de cada resposta existe uma opção *mark=0* e é exatamente nesta opção que pode-se ver a aplicação ou não da QoS, somente lembrando que 0 é o padrão sem QoS e os valores de QoS são 100, 10, 20, 30 e 40, dependendo da classe de priorização.

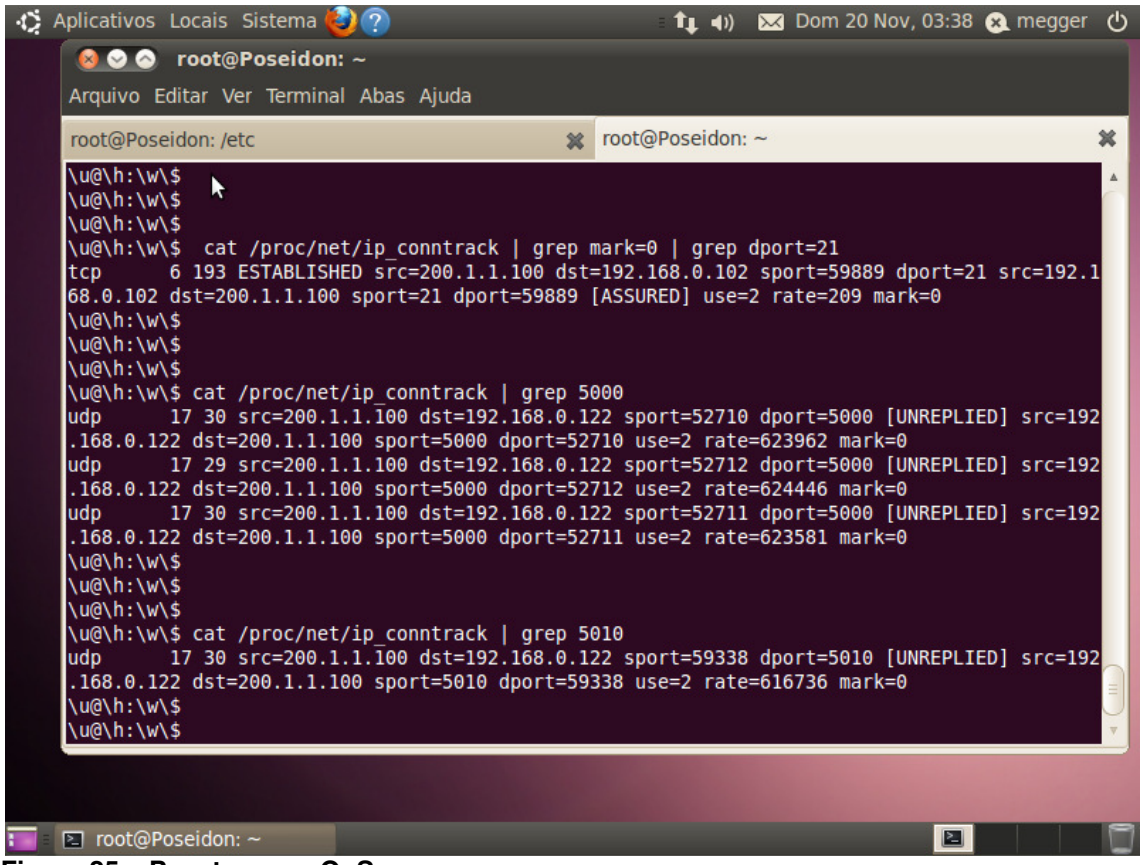

Figura 25 – Pacotes sem QoS
Fonte: Autoria Própria.

Com o resultado deste teste, observou-se que realmente existe a competição por banda e com aumento das requisições para o *gateway*, os tempos de resposta aumentam e existe a possibilidade de descarte de pacotes aleatoriamente, pois como não existem nenhum prioridade, em caso de saturação os pacotes recebidos são descartados.

Seguindo o mesmo teste anterior para demonstrar a marcação dos pacotes, ainda sem as sessões de 30M, configurou-se a porta UDP 5010 com classe *Express*, a requisição FTP (TCP 21) com classe *Premium* e para não ocorrer problemas de acesso, configurou-se o telnet como *Exempt*. A configuração é vista na figura 26:

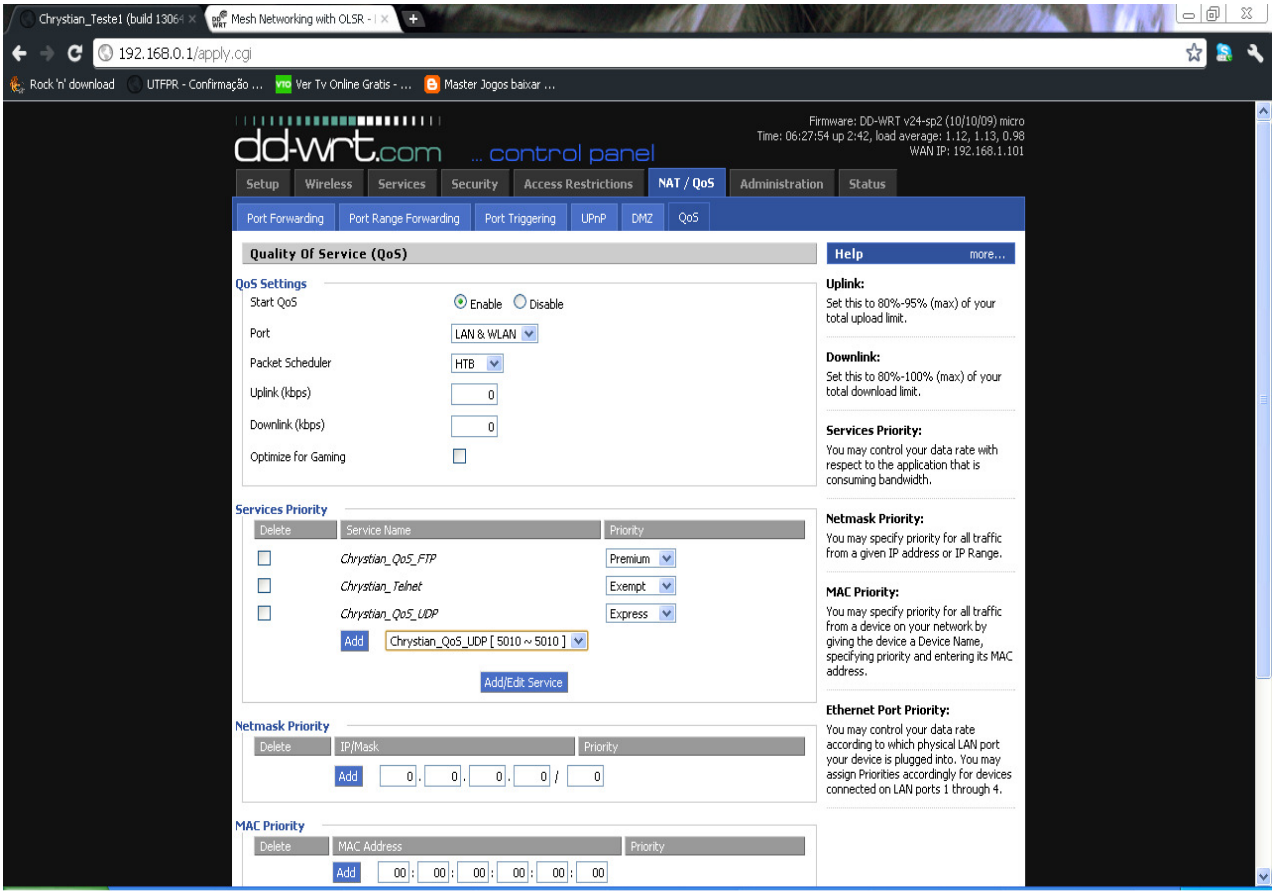

Figura 26 – QoS configurado
Fonte: Autoria Própria.

O resultado obtido pode ser visto na figura 27, onde o tráfego FTP teve marcação 10 (*Premium*), o tráfego gerado para a porta UDP 5010 teve marcação 20 (*Express*) e o tráfego gerado para a porta UDP 5000 teve marcação 0.

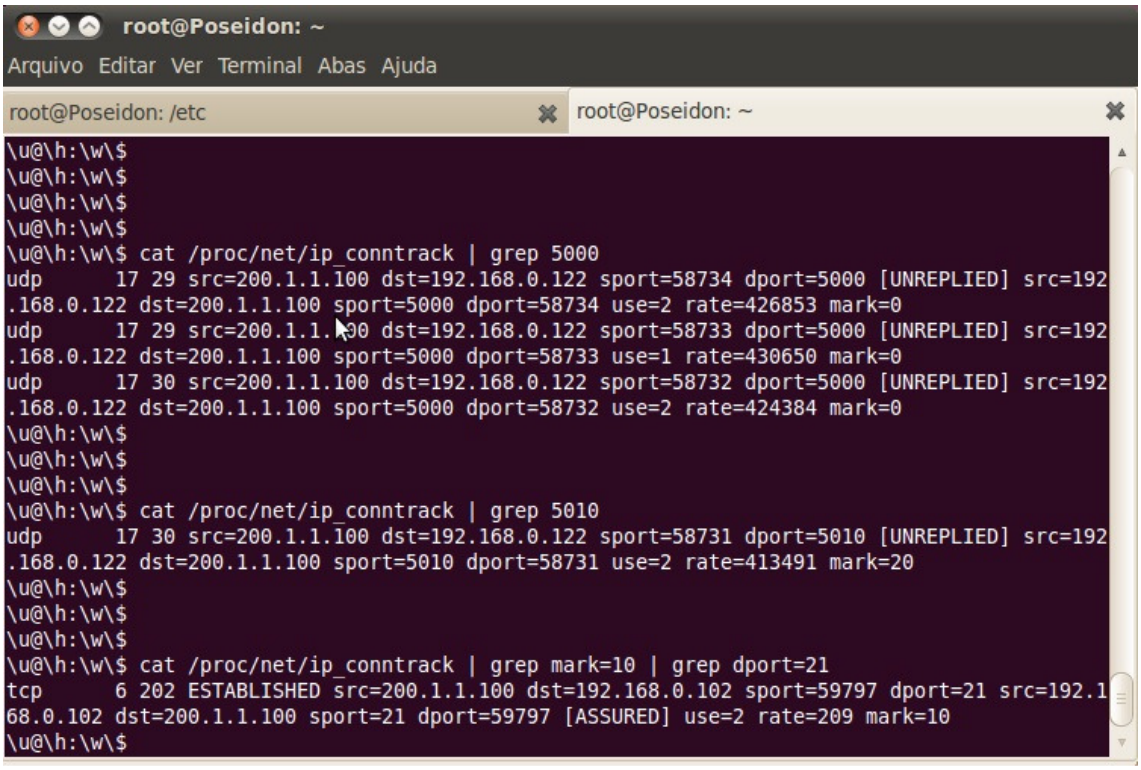

Figura 27 – Pacotes com QoS
Fonte: Autoria Própria.

Visto que realmente existe a marcação dos pacotes, para a conclusão do estudo de campo, saturou-se a rede novamente e configurou-se o mesmo QoS. O acesso ao AP via HTTP tornou-se impossível de se trabalhar e o AP voltou a descartar pacotes pequenos como ICMP de 32 bytes, mas agora com mais frequência, conforme figurar 28:

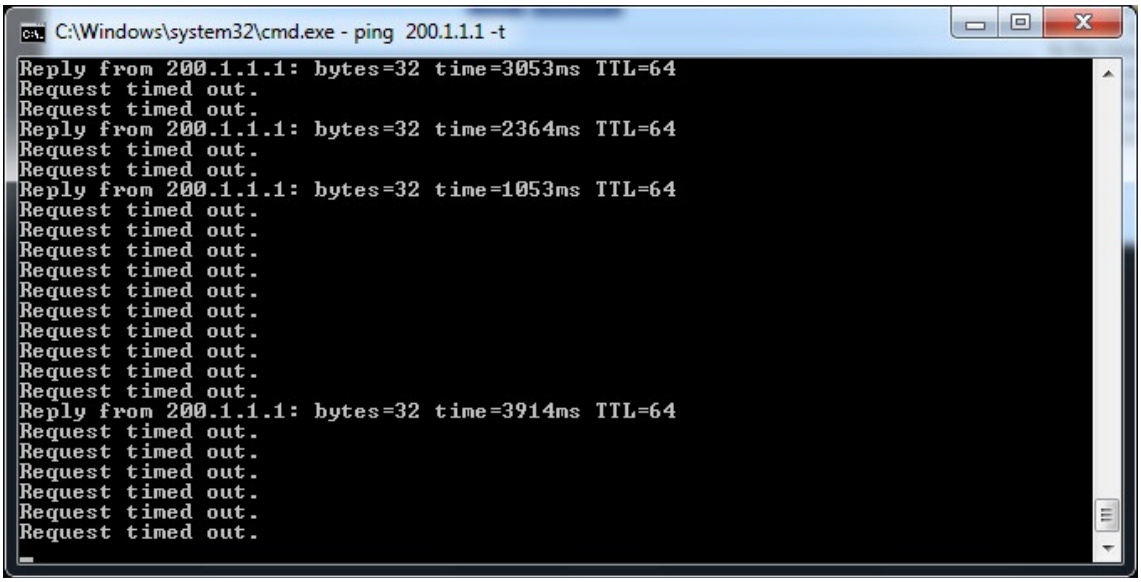

Figura 28 – ICMP com rede saturada
Fonte: Autoria Própria.

Em contrapartida, a conexão telnet funcionou normalmente e sem travamento, sem possível executar comandos no AP. O tráfego gerado para a porta UDP 5010 bem como o FTP receberam tratamento diferenciado e suas tarefas não tiveram quaisquer problemas. A figura 29 mostra a QoS aplicada com a rede saturada e as devidas marcações, inclusive na conexão telnet que foi estabelecida como *Exempt* e recebeu valor 100.

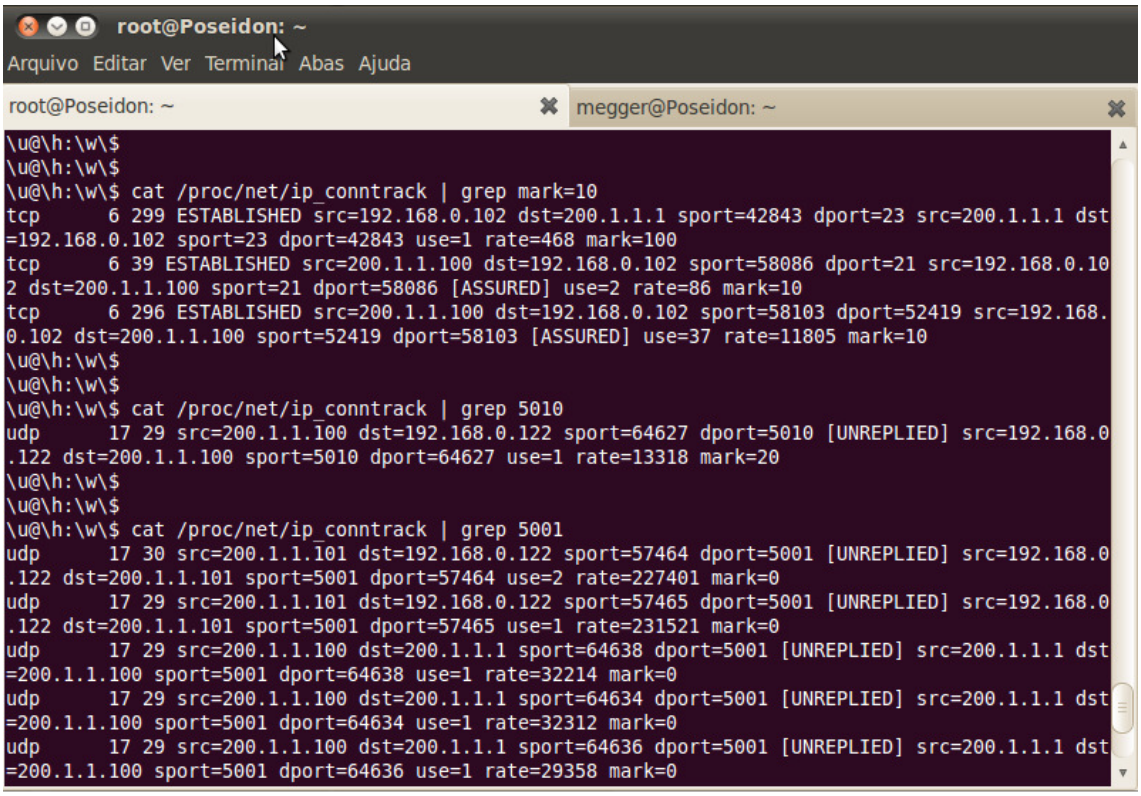

Figura 29 – Pacotes com QoS em rede saturada
Fonte: Autoria Própria.

4 CONSIDERAÇÕES FINAIS

As redes estão em constate crescimento e as empresas tendem a acompanhar tal fato, onde praticamente tudo gira em torno da TI de uma empresa, como transações bancárias, telefonia, sistemas internos de controle, contabilidade e muitas outras funções. Incorreto para um administrador de empresas é pensar que sua rede está ok e nunca mais precisará atuar sobre ela, mesmo com roteadores modernos, APs operando na última tecnologia e portas de switches vagas. Pensando assim, em caso de possível expansão, muitos problemas serão encontrados. Agora, imaginando-se uma rede sem qualquer cuidado, não relacionados à segurança mas sim com o tráfego gerado dentro da própria LAN, onde por exemplo uma transferência bancária estará competido com o simples download de um filme. Em questões como esta, não basta apenas ter uma rede fisicamente ok, mas também cuidar do tráfego de dados. Uma QoS aplicada nesta rede resolveria este tipo de problema.

Com a pesquisa bibliográfica e o estudo de campo concluídos, pode-se afirmar que o uso de QoS realmente é necessário nas redes das corporações. Independentemente da rede, sempre haverá dados prioritários e uma má engenharia pode ocasionar no descarte dos mesmos. Além disso, a pesquisa trouxe a configuração de QoS aplicado em redes sem fio atuando em topologia malha. Através da experiência em campo e dados obtidos nos testes, notou-se uma enorme diferença em uma rede com as prioridades determinadas.

Recomenda-se a utilização das técnicas de QoS, principalmente em aplicações sensíveis a atraso e sem possibilidade de descarte ou retransmissão de dados, prevenindo-se proativamente a ocorrência de possíveis problemas.

REFERÊNCIAS

AIR-STREAM, *Community Wireless Network*. ***Channels for 802.11b*.** Disponível em < http://www.air-stream.org.au/book/export/html/147> Acesso em 08/10/11, 12:39

BERNAU, Paulo Sérgio M. **Voz sobre protocolo IP - A nova realidade da telefonia.** 1ª ed., São Paulo: Editora Érica, 2007

CÂMARA, Daniel. **Proposta para cobertura de áreas de sombra em redes wireless.** Disponível em <http://www.eurecom.fr/~camara/redes/Seminario.html> Acesso em 02/08/11, 20:48

CASTRO, Jaime J. de. **Como nasceu a idéia de rede entre computadores.** Disponível em <http://www.apostilando.com/download.php?cod=2963&categoria= > Acesso em 07/09/2011, 19:38.

CISCO, Networking Academy. **CCNA Exploration – Fundamentos de Rede.** Cisco Systems, Inc., 2007-2009.

CISCO, Systems. **Quality of Service – The Differentiated Services Model.** Cisco Systems, Inc., 2008. Disponível em < http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6558/ps6610/product_data_sheet0900aecd8031b36d.html> Acesso em 13/10/11, 18:07.

DD-WRT, Official Webpage. **Mesh Network with OLSR.** 2011. Disponível em < http://www.dd-wrt.com/wiki/index.php/Mesh_Networking_with_OLSR> Acesso em 30/10/2011, 21:32.

DD-WRT, Official Webpage. **What is DD-WRT.** 2011. Disponível em < http://www.dd-wrt.com/wiki/index.php/What_is_DD-WRT%3F> Acesso em 30/10/2011, 20:10.

FILIPPETTI, Marco Aurélio. **CCNA 4.1 – Guia Completo de Estudos.** Florianópolis: Editora Visual Books, 2008.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa.** 4ª. ed. São Paulo: Atlas, 2002.

HAMIDIAN, Ali; KORNER, Ulf. **QoS Provisioning in Wireless Mesh Network**. Department of Electrical and Information Technology of Lund University. Lund – Sweden, 2008.

INTERNET ENGINEERING TASK FORCE (IETF). **RFC 791 – *Internet Protocol – Protocol Specification***. Disponível em <http://www.ietf.org/rfc/rfc791.txt> Acesso em 13/10/11, 11:20

INTERNET ENGINEERING TASK FORCE (IETF). **RFC 3626 – OLSR Protocol**. Disponível em <http://www.ietf.org/rfc/rfc3626.txt> Acesso em 10/10/11, 13:20

INSTITUTO BRASILEIRO DE OPINIÃO PÚBLICA E ESTATÍSTICA (IBOPE). **Notícias**. Disponível em <http://www.ibope.com.br/calandraWeb/servlet/CalandraRedirect?temp=6&proj=PortalIBOPE&pub=T&nome=home_materia&db=caldb&docid=EA0526673CE1740D832578570054B23B> Acesso em 23/06/11, 11:23.

LIMA, Carlos Eduardo Parag; HOLLICK Matthias; STEINMETZ Ralf. **Diferenciação de Serviços na Internet - DiffServ.** Universidade Federal do Rio de Janeiro – Rio de Janero, 2001. Disponível em < http://www.gta.ufrj.br/grad/01_2/diffserv/index.html> Acesso em 13/10/11, 16:20.

MOGRE, Parag; HOLLICK Matthias; STEINMETZ Ralf. **QoS in Wireless Mesh Networks: Challenges, Pitfalls and Roadmap to its Realization.** Department of Electrical Engineering and Information Technology. Darmstadt University. Darmstadt – Germany, 2007.

PASSOS, Diego. **Métricas de Roteamento para Redes em Malha Sem Fio**. Universidade Federal Fluminense. Departamento da Ciência da Computação, Niterói, 2003.

PINHEIRO, José Mauricio S. **Modelo OSI**. Disponível em <http://www.projetoderedes.com.br/artigos/artigo_modelo_osi.php>. Acesso em 04/10/11, 14:33.

TANENBAUM, Andrew. S. **Redes de Computadores**. 4ª ed. Rio de Janeiro: Editora Campus (Elsevier), 2003.

TELECO, Inteligências em Telecomunicações. **LAN/WAN Wireless I: Introdução.** 2006. Disponível em <http://www.teleco.com.br/tutoriais/tutorialrwlanman1/pagina_1.asp> Acesso em 23/06/11, 13:48.

MICROSOFT, Technet. **Modelo TCP/IP.** Microsoft, Biblioteca., 2011. Disponível em <http://technet.microsoft.com/pt-br/library/cc786900%28WS.10%29.aspx> Acesso em 19/09/11, 22:32.

TELECO, Inteligências em Telecomunicações. **PTT no Celular II – Protocolo IP.** 2007. Disponível em < http://www.teleco.com.br/tutoriais/tutorialpushtotalk2/pagina_2.asp> Acesso em 13/10/11, 10:48.

TELECO, Inteligências em Telecomunicações. **WLAN de Alta Velocidade I: Protocolos.** 2006 Disponível em < http://www.teleco.com.br/tutoriais/tutorialredeswlanI/pagina_5.asp> Acesso em 08/10/11, 12:04.

TELECO, Inteligências em Telecomunicações. **WLAN de Alta Velocidade II: Recomendações IEEE** 2006. Disponível em < http://www.teleco.com.br/tutoriais/tutorialredeswlanII/pagina_2.asp> Acesso em 07/10/11, 18:56.

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL. **Teoria da Comunicação.** Disponível em < http://chasqueweb.ufrgs.br/~paul.fisher/apostilas/redes/redes.htm> Acesso em 07/10/11, 20:17.