REDES WIRELESS MODO AD HOC TIPO MESH PARA ACESSO À INTERNET EM UMA INSTITUIÇÃO DE ENSINO SUPERIOR

NETWORKS WIRELESS MODE AD HOC MESH TYPE FOR INTERNET ACCESS IN AN HIGHER EDUCATION INSTITUTION

VIANELLO, Juliano Melquiades[1]
NEVES, Jailton Santos[2]

Resumo: Esse artigo apresenta uma proposta que pode ser facilmente implementada em qualquer instituição de ensino superior, que não possua rede cabeada e que desejar prover acesso gratuito à rede mundial de computadores para todo corpo de alunos, professores e funcionários da instituição, devidamente matriculados e cadastrados em sua base de dados, ou seja, acesso fornecido e custeado pela universidade que compartilhará o acesso em banda larga com segurança usando os protocolos 802.1X, RADIUS e LDAP. Além da metodologia apresentada, esse trabalho é uma proposta de solução para Universidade Santa Úrsula (USU), onde mostra-se as vantagens da utilização de uma rede em malha sem fio em modo *ad hoc* de baixo custo nesse campus em relação às redes sem fio infraestruturadas tradicionais. Analisar-se-á também qual protocolo de roteamento melhor se adapta a essa rede e serão apresentados os resultados obtidos a partir software de simulação Network Simulator 2.

Palavras chave: Ad hoc. 802.1X. Radius. Ldap. Roteamento

Abstract: This article presents a proposal that can be easily implemented in any higher education institution, that does not have a wired network and that wishes to provide free access to the worldwide computer network for all students, teachers and staff of the institution, duly enrolled and registered in its database, that is, access provided and funded by the university that will share secure broadband access using 802.1X, RADIUS and LDAP protocols. In addition to the methodology presented, this work is a proposal of solution to Santa Úrsula University (USU), where show the advantages of using a low cost wireless mesh in Ad hoc mode network on this campus in relation to traditional infrastructure networks. It will also be analyzed which routing protocol best fits this network and will present the results obtained from Network Simulator 2 simulation software.

Key Words: Ad hoc. 802.1X. Radius. Ldap. Routing

[1] Curso de Engenharia Elétrica - Universidade Santa Úrsula (USU), Rio de Janeiro, juliano.vianello@usu.edu.br
[2] MSc. Universidade Santa Úrsula, Rio de Janeiro, jaineves@gmail.com

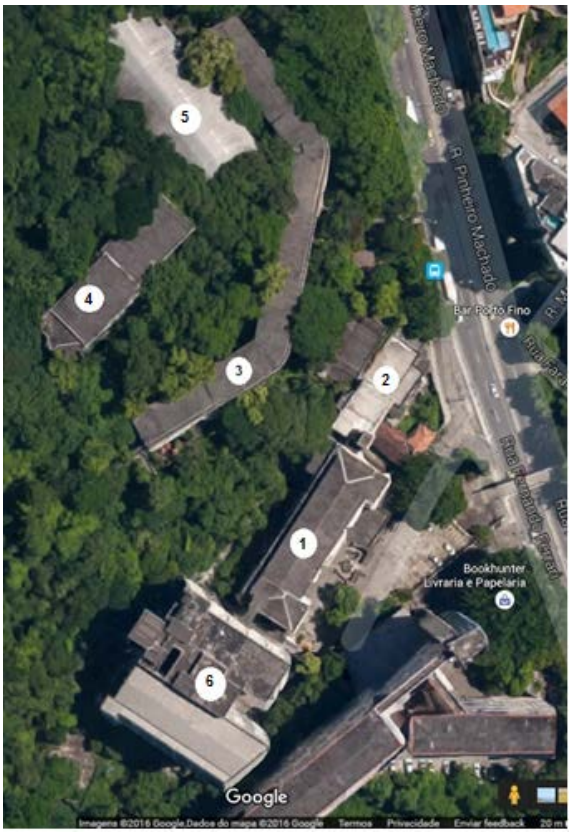
1. INTRODUÇÃO

A internet passou a ser essencial na vida das pessoas e, os acessos por meio das redes sem fio, que se tornaram muito comuns e estão disponíveis em residências, trabalhos, aeroportos, bares e universidades, facilitam a vida de quem depende da Internet para trabalhar, realizar pesquisas e ganhar dinheiro.

Diante do exposto, a implementação de redes desse tipo para alcançar usuários de todos os tipos e classes com qualidade é um grande desafio aos especialistas. Por outro lado, algumas dessas redes não fornecem o mínimo de segurança. Dessa forma, essa facilidade pode se tornar um problema para seus usuários que podem ser prejudicados se tiverem seus dados pessoais interceptados por *hackers* ou usuários mal-intencionados.

As redes em modo *ad hoc* tipo *mesh* são ideias para locais que disponibilizam pouca ou nenhuma infraestrutura de rede como é o caso da USU (Universidade Santa Úrsula). O campus da universidade é composto por 6 (seis) blocos e uma área de mata onde ficam o ginásio, os laboratórios e etc., conforme figura 1, a maioria não tem acesso à internet.

Figura 1 - Campus da Universidade Santa Úrsula



É importante também destacar que o perfil dos usuários das redes sem fio mudou com a evolução dos dispositivos finais utilizados pelos mesmos. Antes utilizavam laptops apoiados em mesas. Hoje os *smatphones* e *tablets* permitem o uso das redes enquanto nos movimentamos. Alguns protocolos utilizados em redes *ad hoc*, não previam essa mobilidade. Por esse motivo, serão

testados alguns protocolos e analisado o seu desempenho mediante esse comportamento, na rede proposta para a universidade.

O acesso à internet através de elementos móveis vem se tornando alvo de interesse corporativo e universitário em todo o mundo. Instituições de ensino oferecem acesso à internet em seu campus como atrativo para o ingresso de novos alunos. Novos padrões de acesso estão sendo estudados ou já entrando em produção, principalmente para a tecnologia celular. Além disso, é necessário também que seja oferecida o mínimo de segurança para os usuários dessas redes e um desempenho no mínimo razoável e adequado para o tamanho do campus e proporcional à quantidade de pessoas conectadas. Será apresentada uma solução que poderá ser implementada facilmente em qualquer instituição de ensino observando as características que foram citadas como fundamentais, e será utilizada o campus da USU como modelo.

O Campus da USU é composto pelo prédio I com quatro andares, prédio VI com 12 andares, um módulo com laboratórios, um ginásio que fica numa área cercada de mata, mas utilizada pelo corpo docente e discente da instituição, e mais dois módulos. A área é de aproximadamente 1000 metros quadrados e em alguns desses prédios/módulos, apesar de não haver nenhuma infraestrutura de rede, há energia elétrica, o que é suficiente para esse tipo de rede. Sendo assim, será possível implementar a rede em todo o campus permitindo acesso à internet a todos e em qualquer local do campus. Nesse momento, surge a questão da definição de qual seriam os melhores lugares para instalação dos roteadores?

As redes sem fio inicialmente eram utilizadas por usuários com *desktops* equipados com placas de rede *wireless* ou *laptops* que já possuíam essas placas de fábrica. A utilização desses equipamentos pelos usuários, normalmente é feita com os equipamentos apoiados em mesas, onde, embora eles estejam livres dos cabos de rede, o cabo de alimentação de energia elétrica ainda inibe em parte a mobilidade desses usuários. Como já foi mencionado, os modernos *smatphones* e *tablets* proporcionam maior mobilidade dos usuários, sem falar que o conteúdo das informações trafegadas na *internet* aumentou significativamente (LANÇA, 2016). Esses equipamentos permitem que os usuários conectados se movimentem a todo momento e continuem realizando atividades na rede como: *downloads*, pesquisas e jogos *on-line*. Alguns protocolos de roteamento para rede *ad hoc* podem ter o seu desempenho comprometido diante da mobilidade dos nós (Em redes de comunicação, um nodo ou nó (do latim nodus) é um ponto de conexão, seja um ponto de distribuição ou um terminal de comunicação), mas não sabemos como eles se comportam com a mobilidade dos usuários. Para essa nova realidade qual seria o melhor protocolo de roteamento a ser utilizado? São questões que serão abordadas por esta pesquisa.

Redes sem fio normalmente são implementadas com autenticação através de senhas compartilhadas. Isso pode ser um problema para a instituição que disponibiliza o acesso, pois se um

dos usuários acessar sites ou enviar conteúdo impróprio de pedofilia, por exemplo, a instituição que ofereceu o acesso poderá ser responsabilizada e terá que informar qual foi o usuário que realizou o acesso ou enviou o conteúdo ilícito. No entanto, com o uso de senhas compartilhadas não se pode distinguir um usuário do outro e o rastro do acesso fica comprometido caindo sobre a instituição a responsabilidade pela infração. Por fim, o controle de acesso dos usuários em uma rede tipo *mesh*, não funciona adequadamente se utilizarmos como premissa básica o MAC das máquinas dos usuários. Sendo assim, qual seria o método de autenticação mais adequado para redes desse tipo? São questões também abordadas por esta pesquisa.

Esse trabalho será uma proposta de solução para USU. Nele será descrito porque usar redes *ad hoc* na instituição ao invés das redes *wifi* tradicionais (no modo de operação "infraestrutura"). Na sequência será indicado o necessário para criação de uma rede *mesh* modo *ad hoc* de baixo custo, que poderá ser implementada na referida universidade ou qualquer outra instituição provendo o mínimo de segurança da informação, maior cobertura do acesso à rede no campus e, consequentemente, atendendo a um maior número de usuários, com melhor desempenho e controle de acesso.

Serão sugeridos os locais para instalação dos nós de roteamento *mesh*, o hardware e os sistemas operacionais, o protocolo de roteamento a ser utilizado com base nos resultados obtidos nas simulações realizadas com os protocolos pró-ativos, reativos e os híbridos, os softwares e programas utilizados para prover o mínimo de segurança, controle de acesso dos usuários e maior acessibilidade à internet por todos os usuários do campus (corpo docente, discente e funcionários).

Por fim, serão testados e analisados em ambientes de simulação (através do software Network Simulator 2) os desempenhos de alguns dos protocolos de roteamento pró-ativo, reativo e híbrido, para avaliar qual deles melhor se adapta ao cenário e topologia da universidade.

1.1 Relevância

O trabalho em redes em malha sem fios surgiu da constatação de que as redes sem fios poderiam ser aproveitadas para reduzir o custo da "última milha" no acesso à *Internet* e alcançar todas as classes de usuários. Através da colaboração entre os nós, um *link* com a rede fixa poderia ser compartilhado, permitindo o uso mais eficiente da banda, evitando o custo da passagem de fios até os usuários finais e beneficiando-se da economia em escala. O conceito foi estendido para o compartilhamento de outros recursos, além do *link* com a rede fixa.

Os pontos de acesso permitem a interligação de redes cabeadas tradicionais às redes sem fio. A conexão de diversos dispositivos móveis com um elemento de interligação das redes é característica do modo infraestrutura. As redes *ad hoc* permitem a interconexão dos elementos móveis diretamente sem a necessidade de um ponto de acesso, num modo denominado "não

estruturado". Essa arquitetura permite o desenvolvimento de aplicações distribuídas (também conhecida como descentralizadas). As redes *mesh* têm como objetivo prover a interconexão dos nós participantes com outras redes estruturadas ou com a própria internet. Elas são também constituídas por nós sem fio, móveis ou não, operando em modo *ad hoc*, mas é desejável que haja baixa ou nenhuma mobilidade dos nós participantes.

A principal característica das redes do tipo *mesh* é o baixo custo comparado com as outras tecnologias. No modo infraestrutura, as redes podem alcançar taxas de transmissão bem altas, mas onde tiver um ponto de acesso à rede para os usuários, tem que ter estrutura de rede física para que o mesmo (ponto de acesso) se conecte, o que eleva muito o custo. Já nas redes *ad hoc* tipo *mesh*, os nós são instalados em locais que necessitam apenas de acesso à energia elétrica.

Desta forma, cada nó é um roteador e ponto de acesso ao mesmo tempo. Os pacotes são encaminhados por um *backbone* sem fio (SHERESTHA e KO, 2006) com capacidade de adaptação em função das variações de qualidade dos enlaces. São utilizados roteadores comerciais, disponíveis no mercado nacional, alterando-se o sistema operacional original por uma distribuição particular do Linux (O OpenWRT é uma distribuição do Linux que permite a configuração de alguns protocolos de roteamento nos roteadores, e por ser de código aberto, possibilita o melhoramento deles). Com esse sistema operacional os roteadores passam a executar um protocolo de roteamento *ad hoc* de código aberto, e permite melhoramentos e avanço no desenvolvimento tecnológico. O *gateway* da rede *mesh* fica interligado à infraestrutura cabeada da universidade ou a um link de saída para a rede mundial de computadores (*Internet*). Ele é o responsável pelo roteamento do tráfego para a Internet. Adicionalmente, o *gateway*, juntamente com um *desktop* com o RADIUS *(Remote Authentication Dial In User Service)* instalado na mesma rede local, tem a função de autenticar, gerenciar e controlar os acessos. Outro desktop ligado na rede com o LDAP *(Lightweight Directory Access Protocol)*, onde rodará o serviço de diretório, armazenará a base de dados dos usuários da rede a ser consultada pelo RADIUS com o mínimo de segurança. Nesse mesmo servidor funcionará um banco de dados para armazenamento dos *logs* de acesso. O custo fica por conta do link *internet*, roteadores e servidores (RADIUS e LDAP) todos usando *software free*.

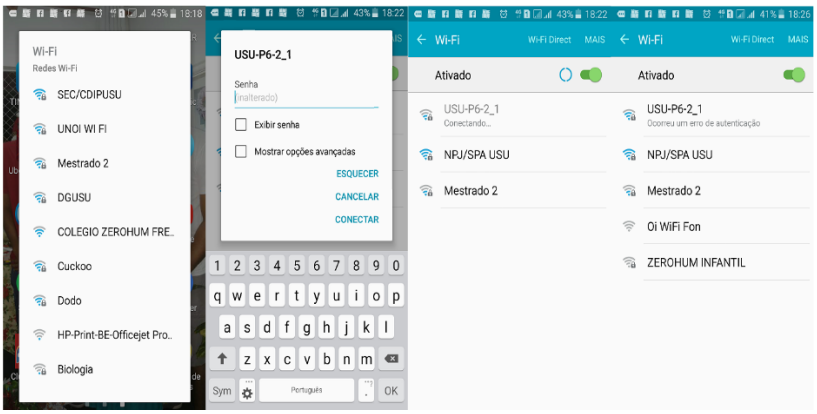
2. O PROJETO

Conforme foi mencionado anteriormente, a USU tem seis prédios e uma vasta área verde. Embora apenas dois prédios hoje sejam mais utilizados, a ideia é que a rede possa ter cobertura em todo o campus. O projeto pode ser dividido em fases e a primeira delas pode ser a cobertura dos prédios e áreas mais utilizadas para posteriormente a rede ser expandida.

Atualmente a universidade tem dois links de saída para a internet, um para rede corporativa e outro para os alunos. A velocidade desses links é de 30Mbps, mas o ideal seria que eles sofressem

um upgrade, pois a utilização do link tende a aumentar. Hoje já não é possível utilizar a rede por parte dos alunos, a dificuldade começa já na fase de conexão, apesar de colocar a senha corretamente, não é possível conectar e acessar a rede conforme pode ser visualizado na figura 2 e quando consegue conectar, é muito difícil navegar com eficiência devido à conexão lenta.

Figura 2 - Redes móveis disponíveis e falha na conexão



Para a primeira fase, os nós *mesh* podem ser instalados um por andar ou em andares alternados no prédio 6, cada um se comunicando com o gateway que fica no térreo na sala de TI da USU. Dessa forma, ele atenderia a demanda do prédio. No prédio I, onde fica a reitoria, como tem apenas 4 andares e a área é aberta, um ou dois nós *mesh* por andar e mais um nas proximidades da lanchonete seriam suficientes. Esses grupos de nós também se comunicariam com o gateway que ficaria no térreo e na sala de TI da USU. Na segunda fase, a rede pode ser expandida para os prédios que não possuem nenhuma infraestrutura de rede ou possuem cabeamento antigo que não servem mais, como é o caso do prédio onde estão os laboratórios e o ginásio. Em cenários como esse, as redes *mesh* são muito úteis.

2.1 O nó Mesh

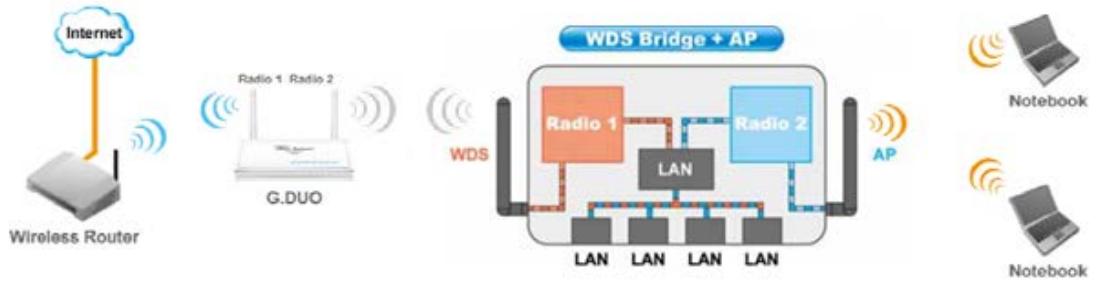
Existem diversos modelos de roteadores no mercado, que trabalham com protocolos diferentes. Os protocolos são uma forma de padronizar todos os dispositivos que utilizam as redes WiFi, porque se cada fabricante usasse sua própria tecnologia para transmissão de dados seria o caos e teriam problemas de interoperabilidade. A criação dos padrões foi a maneira que a indústria encontrou para que todos os aparelhos consigam se comunicar usando a mesma tecnologia. São gerenciados pelo IEEE (Instituto de Engenheiros e Eletricistas e Eletrônicos), que definem as normas e especificações que os fabricantes devem usar, não só para roteadores, mas também para qualquer outro aparelho que pretende usar WiFi, como televisores, smartphones ou dispositivos de internet das coisas. Para os nós da rede wireless tipo mesh no modo ad hoc da USU, podem ser utilizados roteadores sem fio comerciais de baixo custo, com dois rádios no mesmo equipamento ou

dois roteadores com um rádio cada, interligados para composição de um único nó da rede. A escolha vai depender do investimento que a instituição disponibilizará para o projeto, pois existem modelos e marcas diferentes com diferentes protocolos no mercado.

Hoje existem roteadores wireless padrão 802.11ac que alcançam velocidades acima de 1Gbps. Roteadores com esse padrão são ideais para o projeto da USU, pois um dos rádios seria configurado para utilizar esse padrão e compor o *backbone* ad hoc da rede, que transportará grande fluxo de dados. Para interface com os usuários, pode ser configurado outro padrão como o 802.11n ou 802.11g que alcançam velocidades de até 300Mbps e 54Mbps respectivamente, e que são os mais encontrados nos dispositivos finais como *laptops, iPads, tablets* e celulares. Nessa interface o SSID estará visível para todos e será configurada a opção de autenticação através do autenticador RADIUS que será discutido mais adiante.

O radio que será utilizado para compor o *backbon*e sem fio da rede no modo ad hoc, tem como objetivo rotear todo tráfego da rede, de nó em nó mesh até o que atua como *gateway*, permitindo a conexão da rede sem fio com a rede cabeada onde estão: o servidor de autenticação, o diretório de usuários LDAP e a saída para a internet. A figura 3 ilustra um exemplo de roteadore com dois rádios que poderão ser usados como nó mesh, conforme descrevemos.

Figura 3 - Roteador com dois rádios



A figura 4 ilustra um exemplo de rede montada com roteadores equipados com dois rádios, um usado para compor o backbone mesh e o outro para conexão dos usuários à rede.

Outra opção é a utilização de dois roteadores para composição de um nó *mesh*. A ideia é a mesma, pois configura-se um roteador para o modo ad hoc usando o padrão 802.11ac para compor o *backbone mesh* e o outro roteador padrão 802.11n para os usuários se conectarem à rede autenticando via RADIUS. Conecta um ao outro através de cabo de rede e configura o roteador de acesso à rede para utilizar o roteador do *backbone mesh* via endereçamento IP e rotas padrão. Assim, será possível chegar ao gateway de saída para a internet. A figura 5 ilustra o nó *mesh* com dois roteadores interligados.

Figura 4 - Rede com roteador de dois rádios

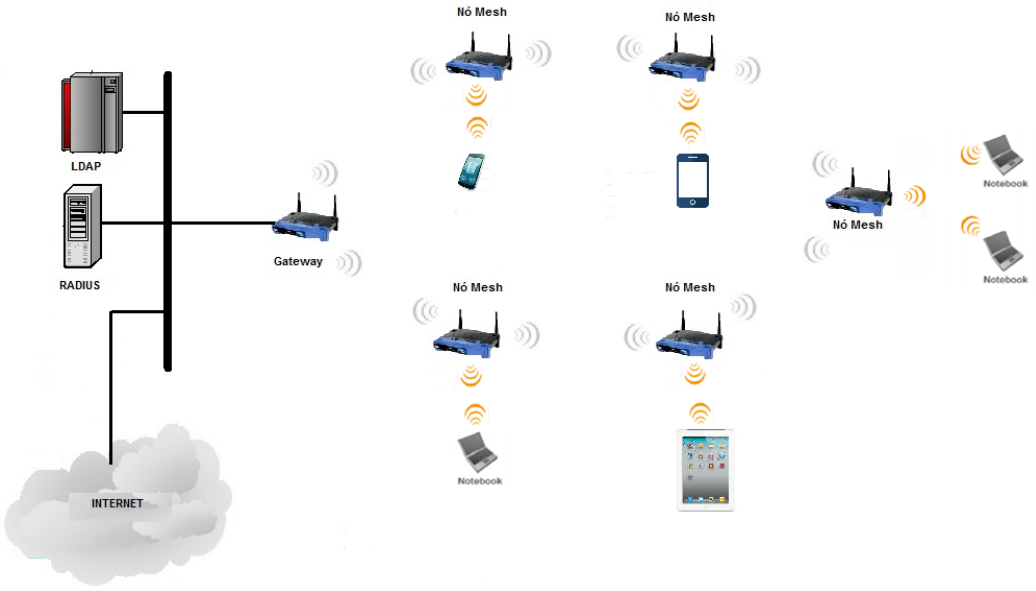


Figura 5 - Nó Mesh com dois roteadores

A figura 6 ilustra um exemplo de rede cujo nó mesh é composto por dois roteadores conforme figura 5.

Figura 6 - Rede composta por nós Mesh com dois roteadores

2.2. Autenticação e segurança da rede

Diferente das redes wireless padrão encontradas normalmente no nosso cotidiano, onde as senhas para conexão são compartilhadas, para autenticação dos usuários na rede será utilizado a integração do protocolo 802.1X com o RADIUS e o LDAP, que estabelece um padrão de segurança em redes sem fio alto, onde cada um terá seu *login* e senha pessoal. Será descrito cada um desses componentes e qual a função deles no processo de autenticação e segurança da rede.

O protocolo 802.1X (CONGDON, 2003) foi proposto tendo como foco as redes cabeadas, tendo em consideração os riscos associados às possibilidades de uma estação não autorizada, se conectar a uma porta de um switch e ter acesso à rede de uma instituição indevidamente. Em redes sem fio, o protocolo é muito utilizado para controlar quem acessa a rede usando uma porta lógica, que é a associação entre o dispositivo sem fio e o AP. Ele atende a dois requisitos básicos de segurança, a privacidade e a autenticação, por esse motivo será utilizado na proposta da solução, no entanto aqui será dado foco maior a autenticação, mais especificamente com a utilização do RADIUS que será discutido no tópico seguinte. O 802.1X pode ser configurado para exigir a autenticação entre o cliente e a rede e se não houver a autenticação, as comunicações não são permitidas.

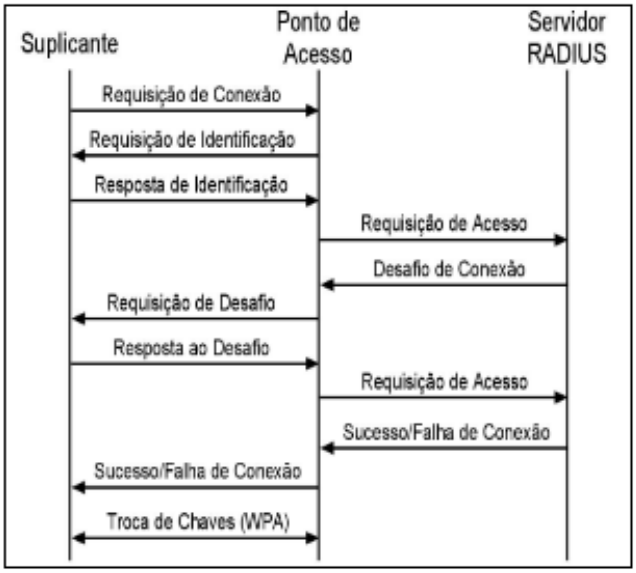
O IEEE 802.1X veio como solução para os problemas de autenticação encontrados no 802.11, ele fornece suporte à praticamente qualquer método de autenticação e manteve-se o suporte à infraestrutura existente como EAP (Protocolo de Autenticação Extensível), RADIUS e LDAP proporcionando benefícios com a sua utilização a custos muito baixos. A aplicabilidade do 802.1X alcança desde grandes empresas que necessitam de soluções escaláveis e robustas, até usuários domésticos e redes públicas que funcionam em aeroportos e universidades. Para a rede proposta na USU, o 802.1X fará o controle de acesso autenticando via RADIUS, somente alunos, professores e funcionários devidamente cadastrados na base de usuários (LDAP), evitando os riscos existentes em uma rede que usa senha compartilhada, como por exemplo, o consumo indevido da banda larga de uma instituição.

Os principais componentes do 802.1X são:

- O suplicante: o dispositivo do usuário que representa a entidade que deseja se autenticar e ter o acesso à rede, por exemplo, celular, *notebook*, *tablet* e etc.
- O Autenticador: o ponto de acesso sem fio que verifica o status do suplicante e quando adequado encaminha a requisição de autenticação para o servidor de autenticação (RADIUS) que verificar a validade das credenciais.
- O sistema de autenticação: o servidor LDAP que é a base de dados com as credenciais dos usuários cadastradas (usuário e senha).

Toda transação de autenticação é encapsulada em mensagens EAP. O processo de autenticação inicia-se quando o suplicante que é a estação sem fio (celular, *tablet, notebook*) tenta conectar-se à rede sem fio e envia uma mensagem de requisição para AP, esse por sua vez retorna com um pedido de identidade do suplicante. Ao receber a resposta do suplicante (*login*), o ponto de acesso a envia diretamente para o servidor RADIUS. Ele então cria um desafio pelo qual o suplicante deve passar com o uso da senha que ele possui. Caso a resposta esteja correta, terá acesso à rede sem fio, caso contrário receberá uma mensagem de falha de conexão. Se o protocolo para encriptação usado for o WPA ou WPA2 que utilizam TKIP e AES respectivamente, ocorre por fim, um acordo entre o suplicante e o ponto de acesso para decidir os valores de chaves temporais que serão usadas durante a comunicação. A figura 7 ilustra os passos nesse processo de autenticação.

Figura 7 - Processo de autenticação EAP com RADIUS



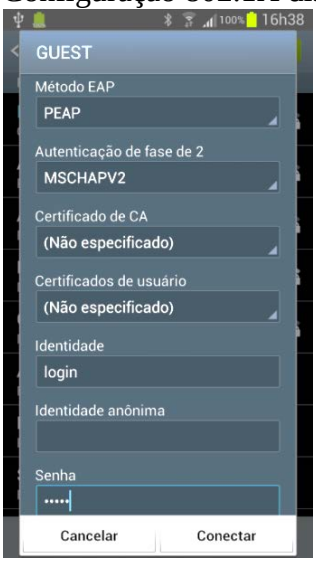
Na proposta de solução da Universidade Santa Úrsula, será utilizado o EAP-PEAP. PEAP que é o EAP Protegido, utiliza TLS (*Transport Layer Security*) para criar um canal criptografado entre o cliente PEAP de autenticação (o laptop ou celular), e um autenticador PEAP, por exemplo, o RADIUS. Esse canal TLS fornece proteção para a negociação do método EAP entre o cliente e o servidor e ajuda a impedir que um invasor insira pacotes entre eles para produzir a negociação de um tipo de EAP menos segura. O canal TLS criptografado também ajuda a impedir ataques de negação de serviço contra o RADIUS.

Depois que o canal TLS é criado entre o RADIUS e o cliente, o cliente passa as informações de credenciais (usuário e senha ou certificado de usuário ou computador) ao servidor pelo canal criptografado. O AP apenas encaminha a mensagem entre eles. O servidor autentica o usuário ou o computador com o tipo de autenticação selecionado, pode ser EAP-TLS com certificado digital ou

EAP-MSCHAPv2 (*Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol version 2*) com senha segura, que será adotado pela USU.

Ao se movimentar no campus da universidade, os usuários farão *handover* de um AP para o outro, a conexão rápida do PEAP permite que usuários sem fio se movimentem entre os APs, sem precisar de nova autenticação toda vez que se associarem a um novo ponto de acesso. A figura 8 ilustra um exemplo de configuração de um dispositivo *Android* para uso do 802.1X com EAP-PEAP, WPA2 e Mschapv2.

Figura 8 - Configuração 802.1X dispositivo Android



2.3. O RADIUS e o LDAP

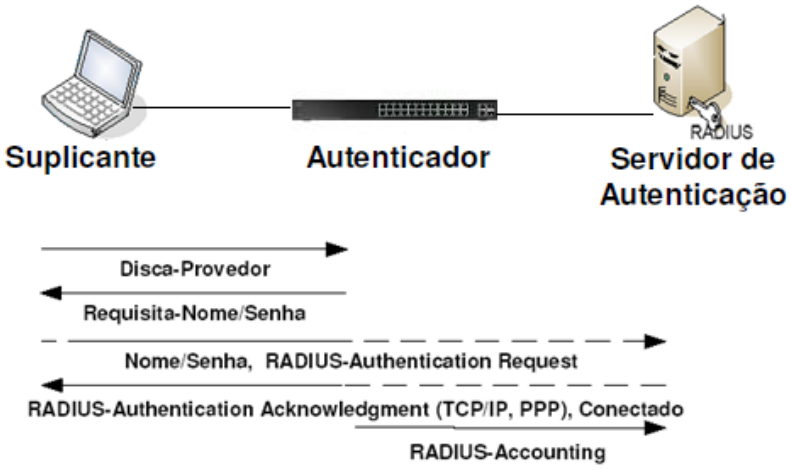
O RADIUS (RIGNEY, 2000) é um protocolo de rede que fornece gerenciamento centralizado de AAA (*Authentication*, *Authorization* e *Accounting*), na tradução Autenticação, Autorização e Contabilização, para usuários que conectam e utilizam um serviço de rede. Descrito pela RFC 2865 foi desenvolvido originalmente para uso de serviços de acesso discado pela sua simplicidade, eficiência e facilidade de implementação, hoje é suportado por servidores de VPN, *Access Points* e outros tipos de acesso a redes. O protocolo segue a arquitetura cliente/servidor e possui três funções básicas:

1. Autenticação de usuários ou dispositivos antes da concessão de acesso à rede.
2. Autorização de usuários ou dispositivos a usar determinados serviços providos pela rede.
3. Contabilização para informar sobre o uso dos serviços.

Foi idealizado para centralizar as atividades de AAA, uma vez que o crescente número de sistemas independentes, inviabiliza a administração descentralizada. Para facilitar o seu entendimento, a figura 9 ilustra o seu funcionamento onde um *host* faz uma requisição de acesso a um cliente RADIUS/autenticador, este por sua vez requisita as credenciais e os parâmetros de conexão ao suplicante e envia ao servidor RADIUS com os dados criptografados. O servidor, checa

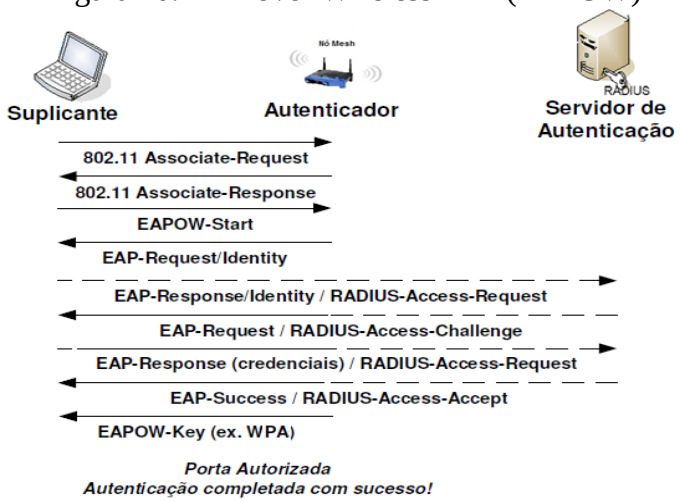
os dados enviados, autentica o usuário e repassa as credenciais relativas às autorizações daquele usuário. Sendo autorizado ou negado, uma mensagem é retornada ao cliente. Se autorizado, o autenticador libera o acesso à rede para o suplicante que fez a requisição e passa a transmitir mensagens de contabilização para o servidor RADIUS.

Figura 9 - Funcionamento do RADIUS



A integração entre o RADIUS e o 802.1X é tratada na RFC 3580 (CONGDON, 2003) de caráter informativo. Algumas modificações e especificações de autenticação e de contabilização do RADIUS são tratadas nesse documento (RFC 3580), definindo as alterações necessárias para seu correto funcionamento. Antes de implantar a solução IEEE 802.1X/RADIUS, uma série de considerações sobre segurança devem ser observadas. Para evitar diversas ameaças de segurança, é necessário suportar confiabilidade, autenticação na origem, integridade, proteção pacote a pacote e autenticação bi-direcional entre cliente e servidor RADIUS. A figura 10, ilustra a utilização do EAP sobre uma rede sem fio (*EAPOW – EAP over WirelessLAN*) e o RADIUS, nela podemos ver o passo a passo da negociação.

Figura 10. EAP over WirelessLAN (EAPOW)

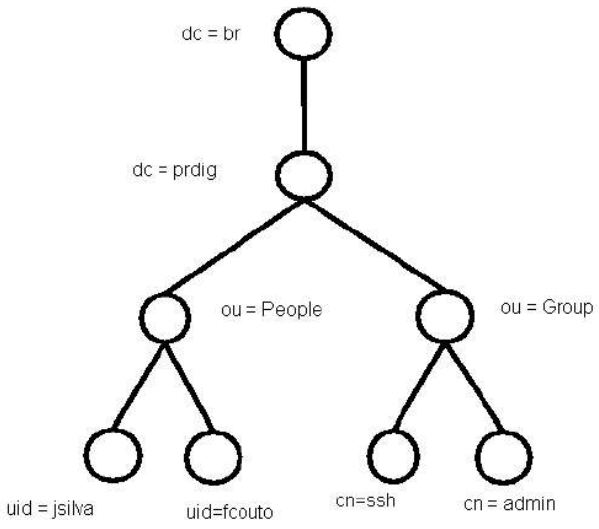


Para redes de grande porte, ter grandes números de usuários, grandes sedes ou cobrir extensa área territorial, o *login* remoto pode se tornar lento. Isso devido à grande quantidade de solicitações e consultas de usuários e sedes às bases ou também devido ao tempo de resposta do servidor. Nessas condições a melhor alternativa é usar uma estrutura em forma de árvore que agrupa as informações dos usuários em diretórios, possibilitando consultas mais rápidas, e essa é a ideia do LDAP (SERMERSHEIM. 2006).

Em um Diretório as informações são mais lidas do que escrita. Diretório é como um banco de dados, mas tende a conter mais informações descritivas, baseadas em atributo e é organizado em forma de árvore, não em tabela como os bancos *MySQL* e *PostgreSQL*. Por esse motivo, os diretórios normalmente não são usados para implementar transações complexas ou esquemas de consultas regulares em banco de dados. Diretórios são preparados para dar resposta rápida a grandes volumes de consultas ou operações de busca, como é o caso da autenticação. Eles podem replicar as informações extensamente acrescentando disponibilidade e confiabilidade, enquanto reduzem o tempo de resposta das aplicações.

O LDAP é um protocolo sobre o TCP/IP, ele permite a centralização de informações sobre usuários, senhas, diretórios home e etc., em um único lugar na rede. É utilizado para acessar um serviço de Diretório que pode apenas conter dados dos usuários como também regulamentar o acesso à rede e possui uma versão *open source*. As entradas são organizadas em uma hierarquia de árvore invertida onde o nó mais alto, chamado de raiz, é o componente nome de domínio “dc” de uma companhia, estado ou organização, conforme figura 11.

Figura 11 - Árvore Diretório LDAP

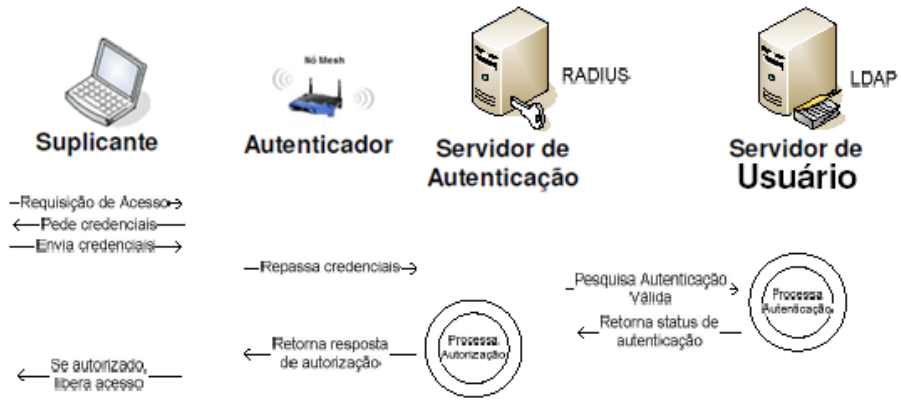


Além de ser mais rápido, oferece transações criptografadas usando SSL (*Secure Socket Layer)* que é mais segura que alguns mecanismos de transferência de senhas pela rede, ou *start* TLS *(Transport Layer Security)* na porta 389 ou LDAPS na porta 636.

Para acesso seguro, o LDAP suporta TLS, onde a comunicação entre o cliente e servidor é toda criptografada, no caso específico da USU, o servidor RADIUS tem a função de cliente do servidor LDAP.

No processo de autenticação, o LDAP suporta o SASL (*Simple Authentication and Security Layer*), que permite que o cliente e servidor negociem um método de autenticação. Para entender melhor a solução adotada, a figura 12 explica o funcionamento das tecnologias trabalhando em conjunto.

Figura 12 - Funcionamento da solução



O suplicante (usuário) envia uma requisição de acesso ao autenticador (nó *mesh*) que é um cliente RADIUS, esse por sua vez pede as credenciais (*login* e senha) para o suplicante, o suplicante envia as credenciais e o autenticador repassa as credenciais para o servidor RADIUS. O RADIUS usa as credenciais para fazer uma pesquisa no Diretório LDAP e verifica se a mesma é válida para autenticação, se for válida, o servidor RADIUS prossegue com a validação do *login* e senha, realizando a operação de autorização. Se o *login* e senha não tiver nenhuma restrição quanto à autorização, o servidor RADIUS autoriza a conexão e o autenticador (cliente RADIUS) libera a mesma para o suplicante que fez a requisição inicial.

Se o objetivo for possuir um banco de dados único para diversas aplicações em uma instituição, como por exemplo, utilizar esse mesmo diretório para autenticar os usuários da rede *wifi*, rede coorporativa e *outlook*, o LDAP é mais interessante por ser uma solução mais completa.

Podemos também usar um banco de dados como o *MySQL* ou o *PostgreSQL* com outro objetivo, o de armazenamento logs de autenticação e contabilização do servidor RADIUS. A versão *open source* do RADIUS (*FreeRADIUS*) vem originalmente com *plug-ins* próprios para essa integração. Para tal, o *plug-in* solicita o endereço IP do servidor do banco de dados, o nome da base de dados criada e permissão de leitura e escrita no banco. Uma vez que estabelecida a conexão e autorizada as permissões, através de scripts já prontos no RADIUS, são criadas as tabelas na base e os logs passam a ser armazenados para consultas e futuras auditorias.

3. PROTOCOLOS DE ROTEAMENTO

A camada de rede tem como função rotear os pacotes da origem até seu destino, o protocolo de roteamento, que atua nessa camada, decide qual linha de saída deve ser utilizada na transmissão do pacote. Para isso, os nós *mesh* que atuam como roteadores trocam informações entre si na tentativa de obter o conhecimento parcial ou total da rede e com isso selecionar a melhor rota. Quando obtém todas as informações, a rede atinge o estado de equilíbrio ou "converge" como é chamado este estágio. Como os enlaces entre um nó e outro podem deixar de funcionar, o equilíbrio na rede não é uma situação constante. O mecanismo do protocolo de roteamento deve restabelecer esse equilíbrio encontrando uma nova rota. A maneira que isso será feito depende do algoritmo utilizado por cada um. Nesse capítulo será descrito alguns deles.

O protocolo usado nos roteadores sem fio que compõe o *backbone mesh*, são protocolos próprios para redes Ad hoc. Os tipos mais utilizados são o AODV (*Ad Hoc On-Demand Distance Vector*) e o OLSR (*Optimized Link State Routing*). Esses protocolos não previam a atual mobilidade dos usuários, portanto, o desempenho da rede vai depender da topologia/particularidades da rede associada a essas características dos usuários. Um protocolo pode se adaptar melhor que outro na rede proposta da USU. Por esse motivo serão testados alguns deles através do simulador de rede NS2 (*Network Simulator*). Será realizada a comparação entre os protocolos e apresentar-se-á os resultados obtidos nas simulações. Com base nesses testes, será escolhido o protocolo a ser implementado na proposta de solução, lembrando que as características desejáveis para um algoritmo de roteamento são:

- Funcionamento correto
- Simplicidade
- Robustez
- Escalabilidade
- Convergência para rota ótima
- Aceitação de parâmetros QoS (*Quality of Service)*
- Adaptabilidade
- Independência da tecnologia de rede
- *Fairness* (justiça e equitatividade)

Antes de apresentar os protocolos de roteamento que serão testados, é importante deixar claro que a escolha do hardware para o nó *mesh* que será ponto de acesso e roteador da rede é muito importante. É desejável que o roteador *wireless* seja programável, de forma que os algoritmos de roteamento possam ser implementados. Alguns roteadores da *LINKSYS* são fáceis de encontrar no mercado brasileiro. Eles são compatíveis com o sistema operacional desejado, o *Openwrt* que é uma distribuição de software livre compacta do *LINUX* para roteadores, celulares e etc. Ele é flexível o

suficiente para desenvolvermos protocolos de roteamento, aplicativos e alterações do próprio hardware. Além disso, é compatível com alguns protocolos, como por exemplo, o AODV e OLSR.

A tabela 1, lista alguns protocolos de roteamento usados em redes *ad hoc*. Eles são divididos em três categorias: pró-ativo, reativo e híbridos, cujos algoritmos levam em consideração o critério de construção de rotas. Na sequência, serão descritos como eles funcionam e citados alguns exemplos, dentre eles alguns selecionados para as simulações da rede no NS2.

Tabela 1. Protocolos de roteamento de redes Ad Hoc

ABR	(Associativity-Based Routing)	IARP	(Intrazone Routing Protocol)
AODV	(Ad Hoc On Demand Distance Vector)	IERP	(Interzone Routing Protocol)
ARA	(Ant-Based Routing Algorithm)	LANMAR	(Landmark Routing)
BSR	(Backup Source Routing)	LAR	(Location-Aided Routing)
CBRP	(Cluster Based Routing Protocol)	LBR	(Link Life Based Routing)
CEDAR	(Core Extraction Distributed Ad Hoc Routing)	LCA	(Linked Cluster Architecture)
CHAMP	(Caching and Multipath Routing Protocol)	LMR	(Lightweight Mobile Routing)
CSGR	(Clusterhead Gateway Switch Routing)	LQSR	(Link Quality Source Routing)
DART	(Dynamic Address Routing)	LUNAR	(Lightweight Underlay Network Ad Hoc Routing)
DBF	(Distributed Bellman-Ford)	MMRP	(Mobile Mesh Routing Protocol)
DDR	(Distributed Dynamic Routing)	MOR	(Multipoint On-Demand Routing)
DNVR	(Dynamic Nix-Vector Routing)	MPRDV	(Multipoint Relay Distance Vector)
DREAM	(Distance Routing Effect Algorithm for Mobility)	OLSR	(Optimized Link State Routing)
DSDV	(Dynamic Destination-Sequenced Dist. Vector)	OORP	(OrderOne Routing Protocol)
DSR	(Dynamic Source Routing)	PLBR	(Preferred Link Based Routing)
DYMO	(Dynamic MANET On-Demand)	RDMAR	(Relative-Distance Micro-Discovery Ad Hoc Routing)
FSR	(Fisheye State Routing)	SSR	(Signal Stability Routing)
GLS	(Geographic Location Service)	STAR	(Source Tree Adaptive Routing)
GPSAL	(GPS Ant-Like)	TBRPF	(Topology Dissemination Based on Reverse Path Forwarding)
GPSR	(Greedy Perimeter Stateless Routing)	TORA	(Temporally-Ordered Routing Algorithm)
GSR	(Global State Routing)	WRP	(Wireless Routing Protocol)
HARP	(Hybrid Ad Hoc Routing Protocol)	ZHLS	(Zone-Based Hierarchical Link State)
HSLS	(Hazy Sighted Link State)	ZRP	(Zone Routing Protocol)
HSR	(Hierarchical State Routing)	...	

3.1. Protocolos Pró-ativos

Nos protocolos pró-ativos, o algoritmo avalia continuamente as rotas para que quando um pacote necessitar ser enviado, a rota já ser de conhecimento da rede e possa ser utilizada de imediato. Nesse tipo de protocolo são enviadas informações e atualizações sobre cada par de nós da rede em intervalos fixos para manter as tabelas de roteamento atualizadas. Os nós mantêm uma ou mais tabelas com informações referentes a todos os possíveis destinos e respondem a mudanças na sua topologia enviando atualizações iniciadas por meio de mecanismos de temporização, para manter a consistência da rede. Devido a essas atualizações, temos sempre um número constante de transmissões em andamento, mesmo quando a rede está em equilíbrio. A grande vantagem desses protocolos é o fato dos pacotes poderem ser enviados com um atraso mínimo porque os nós já

conhecem as rotas previamente. No entanto, é preciso que as redes possuam banda suficiente para evitar congestionamento e não possuam restrição de energia, isso porque a troca de mensagens de roteamento é elevada para garantir o conhecimento das rotas válidas. O DSDV (*Destination-Sequenced Distance-Vector)* e o OLSR (*Optimized Link State Routing*) são exemplos desses protocolos.

3.2. Protocolos Reativos

Esse protocolo utiliza algoritmos cuja rota só é determinada quando ela é requerida, ou seja, quando um nó deseja enviar um pacote para outro nó, ele só inicia o descobrimento da rota sob demanda. Dessa forma, os recursos como banda passante e energia podem ser utilizados de uma forma mais eficiente, porque somente serão gastos quando houver a necessidade de descoberta de rota para encaminhamento de um pacote e como essa necessidade é algo aleatório, esses protocolos não trocam mensagens regularmente o que corrobora para essa economia. Depois de descoberta, é utilizado algum procedimento de manutenção da rota para que ela continue ativa. A desvantagem desses protocolos é o maior atraso no encaminhamento da mensagem, pois se a rota do destino não for conhecida, o procedimento de descoberta de rota deve ser realizado. O DSR (*Dynamic Source Routing*) e o AODV (*Ad Hoc On-Demand Distance Vector*) são exemplos desses protocolos.

3.3. Protocolos Híbridos

Os protocolos híbridos como o próprio nome sugere, combina características dos protocolos pró-ativos e reativos para utilizar vantagens de ambos. Para redes maiores, uma solução possível seria a organização em grupos, dessa forma, a utilização de algoritmos diferentes para o roteamento dentro e entre os grupos seria muito interessante. Se os grupos forem bem divididos, apenas alguns nós sairão do grupo e as alterações de topologia serão passadas apenas para membros desse grupo, sendo transparentes para nós de outros grupos. Neste tipo de organização, atualizações entre grupos são menos frequentes que as que acontecem dentro do próprio grupo. Para os nós de fora, esses necessitam apenas saber como chegar ao grupo e geralmente fazem isso através de um nó apenas chamado *clusterhead,* por onde passam todos os dados de entrada e saída do grupo. Como exemplo de protocolos híbridos temos o ZRP e o FSR.

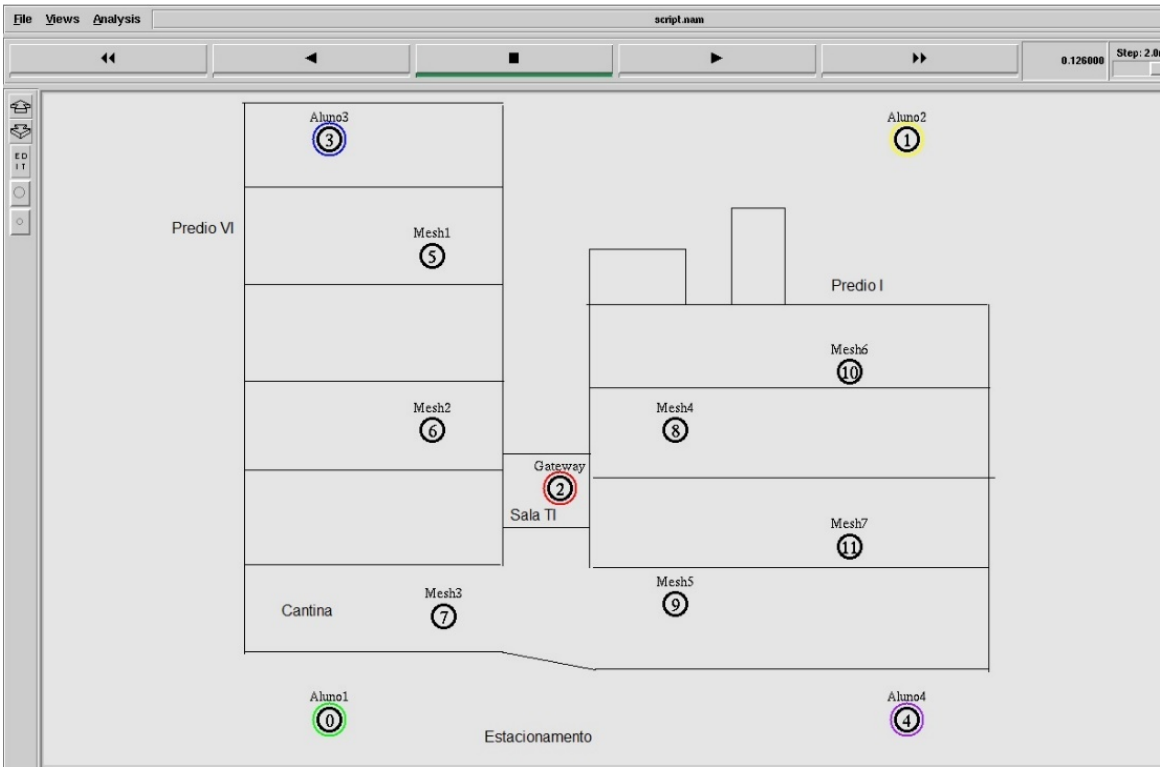
4. SIMULAÇÕES E RESULTDOS

Nesse capítulo, serão expostos os resultados dos testes realizados com os protocolos de roteamento, selecionados para a rede proposta utilizando o *Network Simulator 2* (NS2), que é um simulador de eventos discreto, resultante do projeto VINT *(Virtual Inter Network Testbed).*

4.1. O Cenário e script

Para simulação foi criado um *script* para um cenário com oito nós e quatro usuários conforme figura 13. Esses usuários utilizam protocolo UDP para transferência de dados entre eles e o *gateway* da rede que faz interface com a internet.

Figura 13 - Topologia usada no NS2 simulando USU



A topologia procurou retratar o ambiente da Universidade Santa Úrsula, contendo os prédios I e VI (os mais usados atualmente) para as simulações, os usuários sinalizados com o nome aluno nas cores amarelo, verde, azul e violeta, se movimentando entre os andares e prédios, em dois movimentos realizando transferência de dados numa simulação de conexão com a internet, conforme pode ser visto na figura 13.

Como o ambiente sem fio sofre diversas interferências e perdas por diversos fatores, procurou-se retratar esses ambientes nas simulações. No entanto como não é possível simular interferência, foi utilizada a mesma topologia e diferentes níveis de perdas de pacotes (com aplicação de taxa de erro) em 4 cenários para verificar como os protocolos se comportavam.

Foram testados quatro protocolos de roteamento, um reativo, dois pró-ativos e um híbrido. Nas simulações, que duram 7 minutos ou 420 segundos cada, foi verificado a vazão/*throughput* da rede, *delay* fim-a-fim dos pacotes, quantidade de pacotes enviados, quantidade de pacotes recebidos, número de pacotes perdidos e etc.

O script utilizado nas simulações do NS2, sofreu pequenas alterações de um cenário para outro para possibilitar que o ambiente fosse retratado, valor da taxa de erro, por exemplo. Nas partes fixas dele, temos, por exemplo, a velocidade de deslocamento utilizada pelos usuários (10km/h), tamanho dos pacotes (500 bytes). Na sequência, além das configurações padrão para construção de uma rede *Wireless Ad hoc*, foi configurado que a área da simulação seria de 500X500, que a conexão dos usuários com o *gateway* usaria o protocolo UDP (*User Datagram Protocol*) para uma aplicação CBR (*Constant Bit Rate*) com velocidade padrão de 448Kbps e etc. Foi configurada também um módulo para inserir erro no cenário, simulando um ambiente igual ao que uma rede sem fio encontra diariamente. A unidade de erro pode ser especificada em termos de pacotes, bits ou baseados no tempo, foi utilizado taxa de erro de pacote e configurado cenários para erro a 1, 5, 10 e 15%.

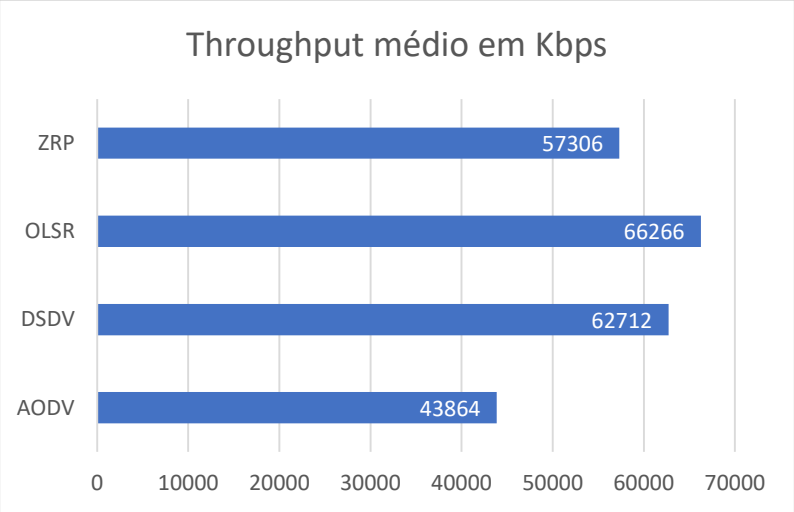
4.2. Testes e resultados

Após construção do *script*, foram testados quatro protocolos de roteamento na rede proposta, um reativo (AODV), dois pró-ativos (DSDV e OLSR) e um híbrido (ZRP). Para os testes foram medidos *Throughput* (taxa de transferência) da rede, o *delay* mínimo, máximo e médio, quantidade de pacotes enviados, recebidos, perdidos e o percentual de pacotes entregue ao final das simulações. Os testes foram realizados simulando ambiente normal e ambiente com erro de pacote em diferentes percentuais.

Os resultados das simulações foram coletados após 7 minutos ou 420 segundos para os quatro protocolos. As performances foram analisadas a partir do arquivo trace gerado ao final de cada simulação no NS-2 com o auxílio de outro script que utiliza a linguagem de programação AWK (Aho, Weinberger e Kernighan - A linguagem AWK foi criada em 1977 pelos cientistas Alfred Aho, Peter J. Weinberger e Brian Kernighan e a palavra AWK é uma abreviatura dos sobrenomes dos criadores. Essa linguagem é baseada na linguagem C e utilizada frequentemente por desenvolvedores para processar textos e manipular arquivos. É interpretada por linha e tem como principal objetivo deixar os scripts de Shell mais poderosos e com muito mais recursos sem utilizar muitas linhas de comando, podendo resolver infinidades de problemas do dia-a-dia.), assim foram extraídos os dados que seriam analisados.

Primeiramente foi verificada a vazão da rede, também conhecido como *Throughput* da rede ou taxa de transferência efetiva da rede, que é o número de bits que podem ser transferidos sobre uma rede num determinado tempo. Esta vazão foi medida em um cenário sem erro e depois em outros quatro cenários que apresentavam erro de pacote com percentuais diferentes (1, 5, 10 e 15% de erro). A figura 14 apresenta o *Throughput* médio da rede para o cenário sem erro de pacotes.

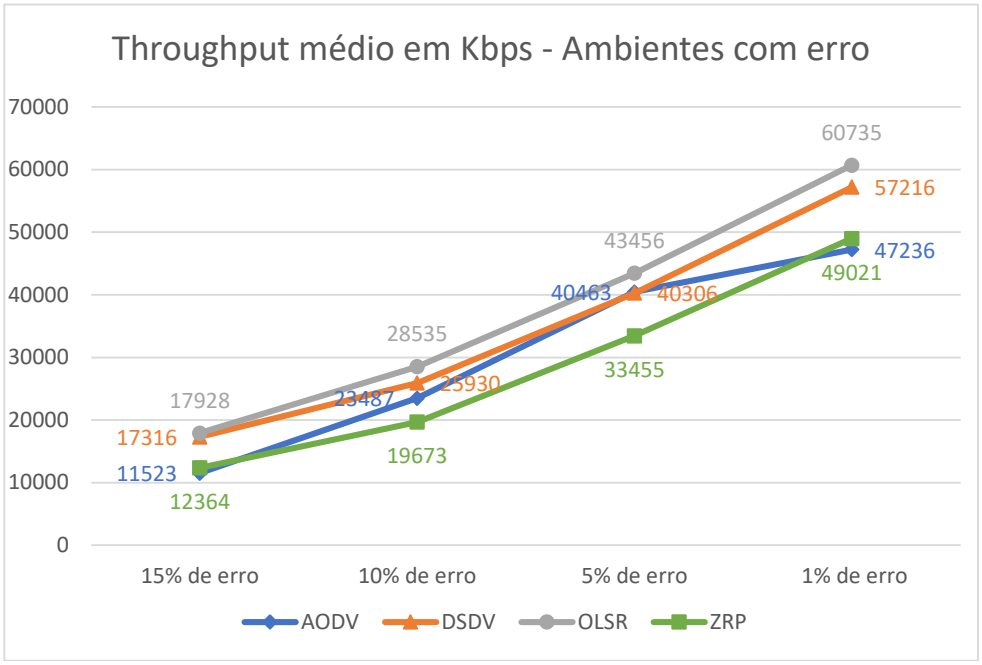
Figura 14 - Throughput da rede em cenário sem erro



Nesse cenário foi verificado que o protocolo OLSR obteve o melhor desempenho entre os demais atingindo 66,2 Mbps de *throughput* médio.

Na sequência foram realizados testes nos cenários com diferentes percentuais de erro de pacotes, simulando os diversos problemas que uma rede sem fio pode encontrar, como por exemplo, obstáculos físicos (paredes), interferências eletromagnéticas provenientes de eletrodomésticos e etc. A figura 15 ilustra o resultado obtido.

Figura 15 - Throughput médio da rede em cenário com erro de pacotes



O protocolo OLSR também obteve melhor resultado no ambiente que apresentava erro. Na medida que o percentual de erro diminuía, foi observado que a taxa de transferência aumentava. O segundo melhor resultado foi do protocolo DSDV, ambos protocolos pró-ativos.

Em seguida foi analisado o atraso ou *delay* da rede, que é o tempo em que o pacote leva para atravessar uma rede desde a origem até o destino. Foram analisados os atrasos mínimos, médio e máximo para cada protocolo. Assim como no *throughput*, as medições foram realizadas primeiramente num cenário sem erro, onde foram verificados os valores de *delay* mínimo e médio para cada protocolo (figura 16) e *delay* máximo alcançado para cada um deles (figura 17). Posteriormente, os protocolos foram testados em quatro cenários com percentuais de erro de pacote diferentes, onde os mesmos parâmetros foram analisados: *delay* mínimo e médio (conforme figura 18) e *delay* máximo (conforme figura 19).

Figura 16 - Delay mínimo e médio em cenário sem erro

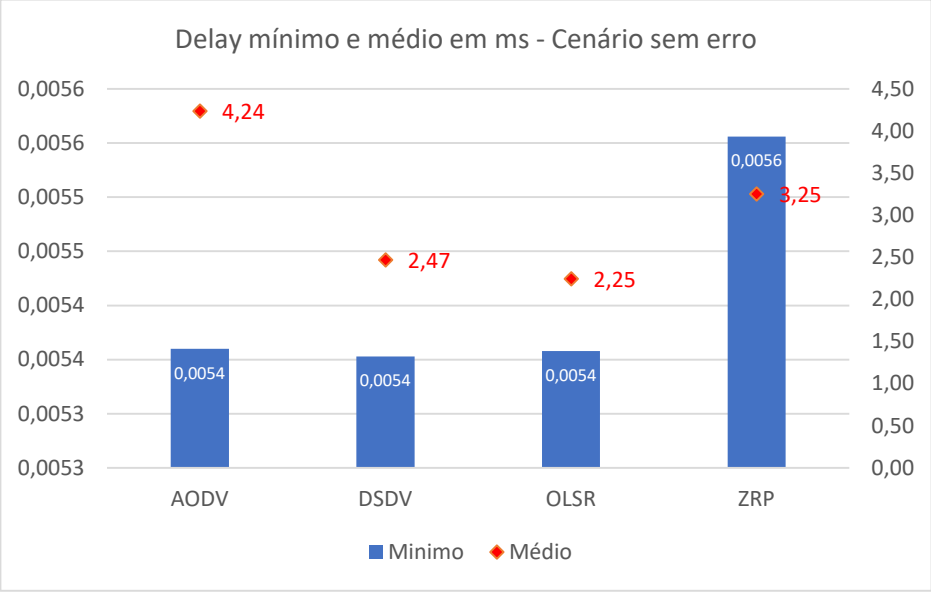
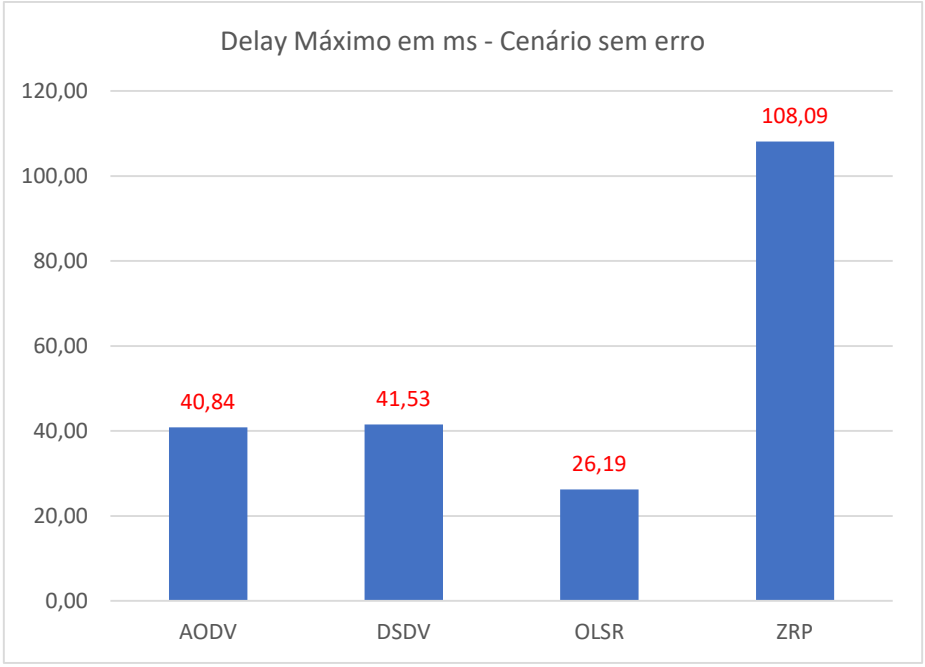
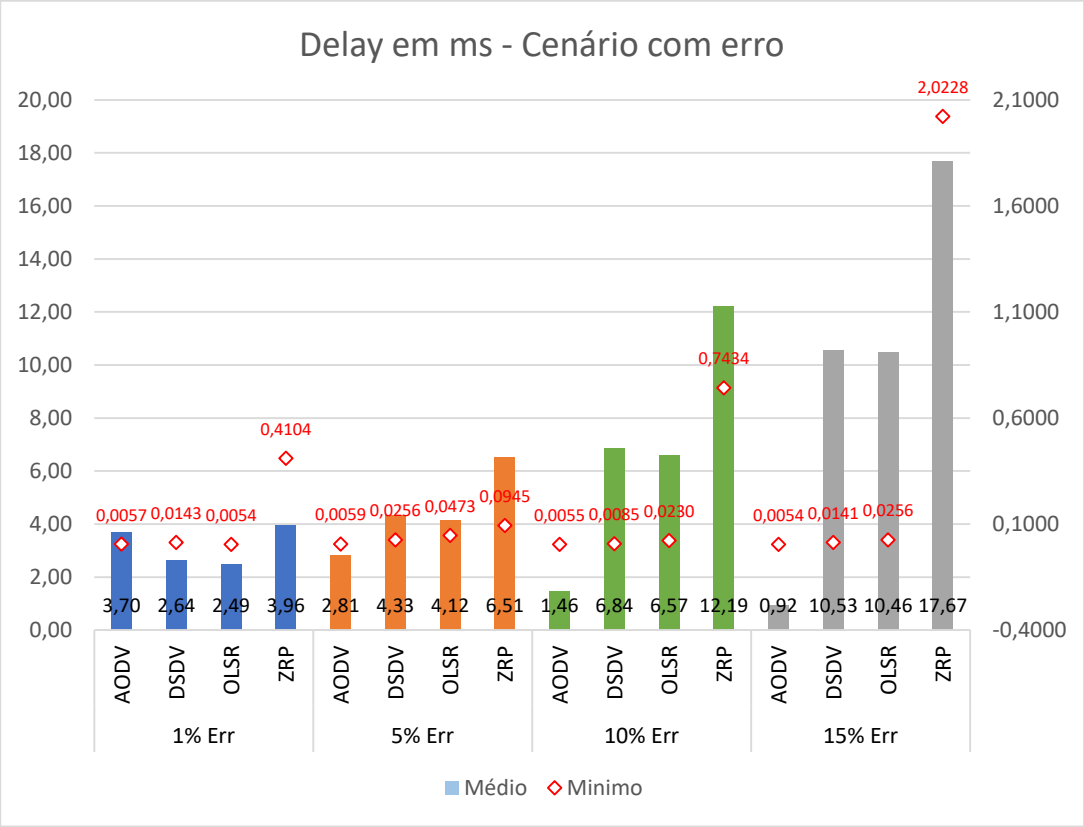


Figura 17 - Delay máximo em cenário sem erro



Para decidir qual dos protocolos obteve melhor desempenho nesse quesito, foi levado em consideração o *delay* médio e mais uma vez o protocolo OLSR foi o melhor com a média de 2,25 ms por pacote enviado conforme figura 16. O *delay* máximo dele também foi o menor entre os demais protocolos conforme figura 17.

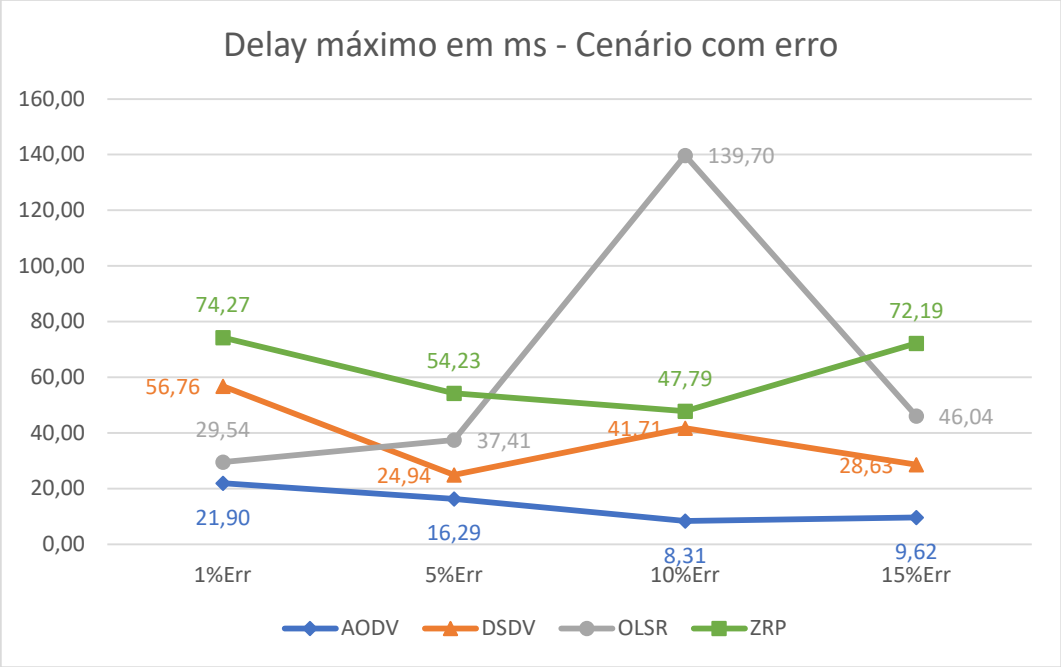
Figura 18 - Delay mínimo e médio em cenário com erro



Nos testes executados para os cenários com erro, levando em consideração os valores de *delay* médio, foi observado que o protocolo reativo AODV obteve melhor desempenho. Na medida que o percentual de erro aumentava, o *delay* fim-a-fim do protocolo diminuía conforme pode ser visto na figura 18.

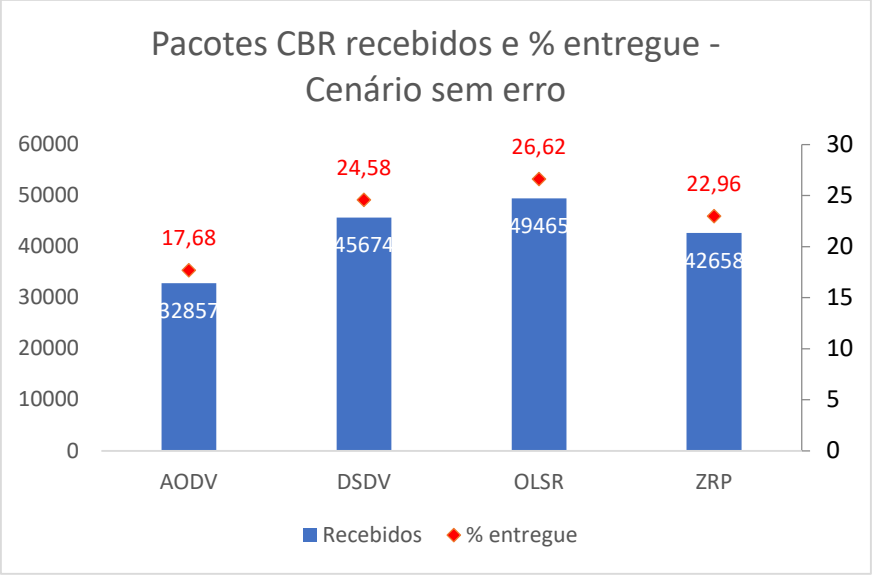
Para análise do *delay* máximo dos protocolos, foi utilizada a figura 19, onde pode ser observado que o protocolo AODV obteve melhor desempenho em todos os cenários de erro, inclusive no que apresenta maior percentual de erro. Lembrando que quanto menor o *delay*, melhor para a aplicação, principalmente para aplicações que funcionam em real time. Com o AODV, quanto maior o percentual de erro, menor o *delay* máximo, médio e mínimo apresentado pelo protocolo.

Figura 19 - Delay máximo em cenário com erro



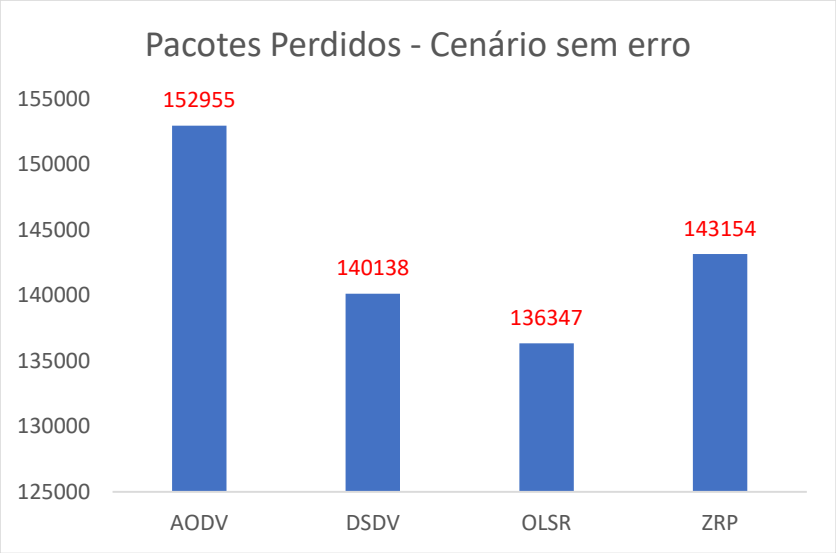
Por fim, foi verificado a quantidade de pacotes recebidos, percentual de pacotes entregues e pacotes perdidos nos mesmos cenários. Os resultados podem ser observados nas figuras 20 e 21 para o cenário sem erro e na figura 22 para os cenários com erro.

Figura 20 - Pacotes recebidos e percentual entregue cenário sem erro



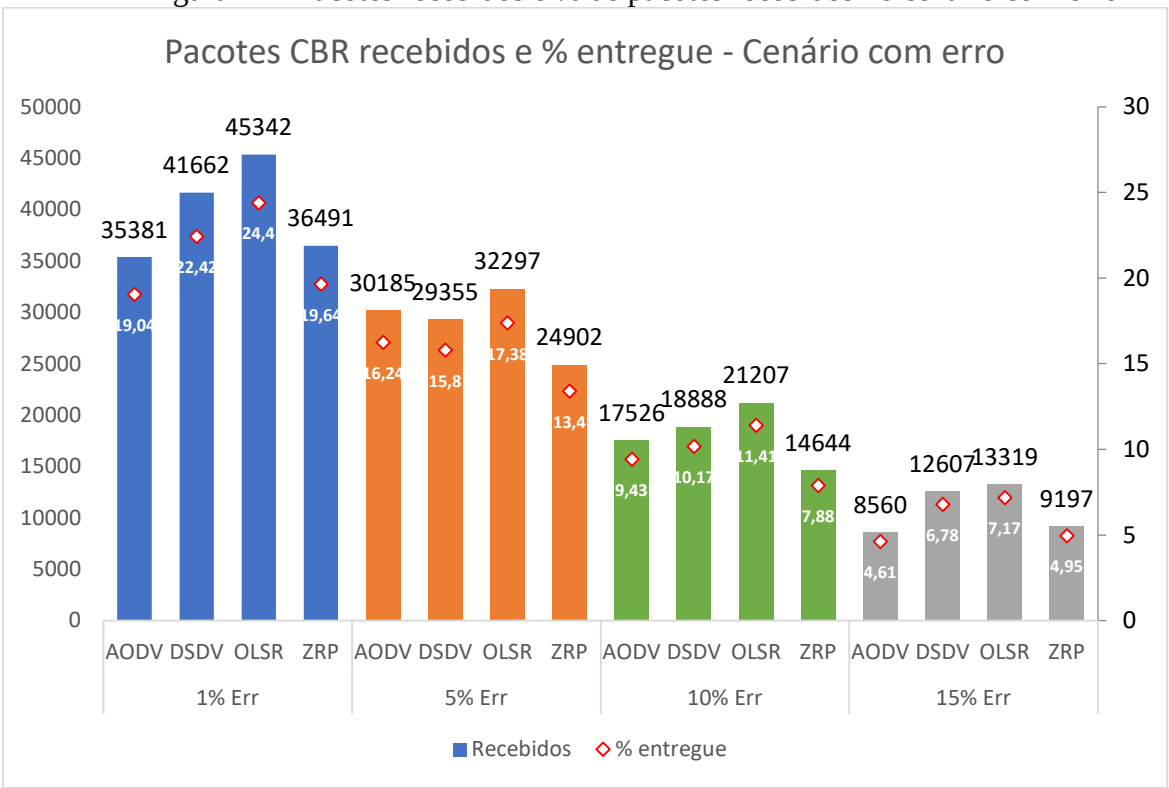
A figura 20, mostra que o protocolo OLSR mais uma vez obteve melhor desempenho, entregando 26,62% dos pacotes transmitidos. A figura 21, mostra também que o protocolo OLSR perdeu menos pacotes que os demais protocolos.

Figura 21 - Pacotes perdidos cenário sem erro



Para os cenários que apresentam erro de pacote, o protocolo OLSR apresentou melhor desempenho em todos como pode ser visto na figura 22, tanto na quantidade de pacotes recebidos quanto no percentual de pacotes entregues no receptor.

Figura 22 - Pacotes recebidos e % de pacotes recebidos no cenário com erro



5. CONCLUSÃO

A solução aqui apresentada, utilizando redes em malha sem fio no modo *ad hoc* tipo *mesh* é totalmente viável, de baixo custo e não se aplica somente a uma Instituição de Ensino Superior

(IES), mas em qualquer instituição que não possua rede cabeada disponível, ou em lugares que não é possível chegar nenhuma ou o mínimo de infraestrutura de rede, mas que dispõe de energia elétrica.

No caso da USU, como a estrutura de rede cabeada é muito antiga e em alguns prédios sequer existe, a utilização de redes desse tipo se encaixa perfeitamente para atender a demanda da instituição com rapidez e eficiência. Importante lembrar que o link de saída para internet contratado da operadora, será compartilhado com todos, por esse motivo, ele deve acompanhar a demanda da instituição e ser de velocidade que suporte à conexão simultânea dos usuários.

A configuração dos servidores que serão utilizados como RADIUS e LDAP também é muito simples, ambos utilizam softwares gratuitos e de fácil instalação, desde o sistema operacional até o software da aplicação. Com o RADIUS, diversas aplicações da instituição poderão utilizá-lo para autenticação e autorização de usuários, como por exemplo, *login* em rede coorporativa, *login* em dispositivos de rede e sistemas diversos. Depois de conectado, toda atividade realizada é armazenada para consultas e futuras auditorias.

O LDAP também pode ser muito útil na instituição. Ele poderá ser utilizado como diretório único para cadastro de todos os usuários. Com ele a instituição terá uma base centralizada que poderá ser utilizada para consultas de autenticação realizada por aplicações e dispositivos diversos, como por exemplo, *outlook*, sistemas de catracas eletrônicas, RADIUS e etc.

A rede proposta para à Universidade Santa Úrsula, foi utilizada nos testes como um estudo de caso de aplicação da metodologia. Nos resultados, o protocolo de roteamento OLSR obteve o melhor desempenho na maioria absoluta dos testes *(throughput*/vazão da rede, pacotes recebidos, percentual de pacotes entregues, *delay* mínimo, médio e máximo em cenário sem erro). Isso acontece devido ao fato dele ser um protocolo pró-ativo e já possuir em sua tabela de roteamento caminho otimizado para todos os nós destinos da rede, utilizando a técnica MPR.

O protocolo OLSR não apresentou melhor desempenho nos testes realizados em cenário com erro, para os tempos de *delay* mínimo, médio e alto. Nesse cenário, o protocolo AODV por ser um protocolo reativo, programado para ser adaptativo a cenários de alta mobilidade como no caso das simulações (alunos movimentando-se a 10km/h), foi o melhor. O AODV descobre o melhor caminho no momento que necessita enviar os dados. Se os enlaces apresentam taxa de erro, é verificado qual o melhor deles para ser utilizado na transmissão. Como esse procedimento é realizado nó a nó, ele se adapta mais rapidamente ao cenário, assim ele obtém melhores tempos em redes com taxa de erro.

A escolha do protocolo a ser utilizado na rede, vai depender do tipo de aplicação mais comum na instituição. Pensando nisso, os tempos de *delay* podem ser levados em consideração na hora da escolha. Se a rede for utilizada na maior parte do tempo para aplicações sensíveis à variação

do *delay* (mais conhecida como *jitter*), aplicações como voz e vídeo em tempo real, o AODV seria o mais indicado. O fato do protocolo AODV, apresentar melhores tempos em relação ao *delay* para ambientes que apresentam altas taxas de erro (muito comum em redes sem fio), é muito importante e são fatores que pesam na hora da escolha, principalmente se a diferença entre a vazão dos protocolos não for muito diferente.

Mas se a rede não apresentar alta taxa de erro e de interferência, e o objetivo final for acesso à internet por parte dos usuários, com maior vazão e tráfego de dados, independentemente do tipo de aplicação utilizada, como é o caso da USU, o protocolo OLSR seria a melhor escolha. Ele obteve melhores resultados para vazão nos cenários com erro e sem erro, inclusive de *delay* mínimo, médio e máximo no cenário normal (sem erro), seguido do protocolo DSDV que é outro protocolo pró-ativo.

Como no ambiente de testes foram utilizados poucos nós, o protocolo ZRP não apresentou bom desempenho, uma vez que o mesmo é mais apropriado para redes maiores e com muitos nós. Se a rede for expandida para os outros blocos/edifícios da instituição, seria muito interessante realização de novas simulações, pois os protocolos podem apresentar resultados diferentes em uma rede com um número elevado de nós. Isso porque, quanto mais saltos entre a origem (usuário) e o destino (gateway), menor tende a ser a vazão da rede, principalmente se a aplicação utilizar o protocolo TCP que faz controle de erro, fluxo e congestionamento.

REFERÊNCIAS

AD HOC. "*Redes Ad Hoc – Protocolos DSR, AODV, OLSR e DSDV*", GTA UFRJ. 2009. Disponível em: https://www.gta.ufrj.br/grad/09_1/versao-final/adhoc/intro.html. Acessado em março de 2017.

AIR LIVE. *"G.DUO Dual 11g Access Point"* – User´s Manual Powered by OvisLink Corp. Air Live, 2009.

CHELLA, R. V. *"Administração de usuários em um Sistema Linux utilizando LDAP e PostgreSQL"* – Monografia do curso de Especialização em Software Livre. UFPR, 2004.

CONGDON. P.; ABOBA. B.; SMITH. A.; ZORN. G.; ROESE. J.; RFC 3580 – *IEEE 802.1X Remote Autenthication Dial In User Service (RADIUS), usage guidelines*. IETF, 2003. Disponível em: https://tools.ietf.org/html/rfc3580. Acessado em abril de 2017.

DUARTE, O. C. M. B. ; SILVA, L. A. F. *"RADIUS em Redes sem Fio"*. Grupo de Teleinformática e Automação – PEE-COPPE/DEL-POLI, UFRJ, 2003.

LANÇA, H.C. *"A regulação dos conteúdos disponíveis na Internet "*, editora Chiado. Primeira edição dezembro de 2016.

RIGNEY. C.; WILLENS. S.; RUBENS. A.; SIMPSON. W. RFC 2868 – *Remote Authentication Dial In User Service (RADIUS)*. IETF, 2000. Disponível em: https://tools.ietf.org/html/rfc2865. Acessado em fevereiro de 2017.

SERMERSHEIM, J. RFC 4511 – Lightweight Diretory Access Protocol (LDAP). IETF, 2006. Disponível em: https://tools.ietf.org/html/rfc4511. Acessado em março de 2017.

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

TEIXEIRA, D. V. "Aperfeiçoando a Operação de Redes em Malha sem Fio" – Dissertação de Mestrado em Engenharia de Telecomunicações. UFF, 2007.