Ricardo Eleutério dos Santos

VLAN: Estudo, Teste e Análise desta Tecnologia

São José – SC

fevereiro / 2010

Ricardo Eleutério dos Santos

VLAN: Estudo, Teste e Análise desta Tecnologia

Monografia apresentada à Coordenação do Curso Superior de Tecnologia em Sistemas de Telecomunicações do Instituto Federal de Santa Catarina para a obtenção do diploma de Tecnólogo em Sistemas de Telecomunicações.

Orientador:
Prof. Odilson Tadeu Valle

Co-orientador:
Prof. Ederson Torresini

Curso Superior de Tecnologia em Sistemas de Telecomunicações
Instituto Federal de Santa Catarina

São José – SC

fevereiro / 2010

Monografia sob o título *"VLAN: Estudo, Teste e Análise desta Tecnologia"*, defendida por Ricardo Eleutério dos Santos e aprovada em fevereio de 2010, em São José, Santa Catarina, pela banca examinadora assim constituída:

Prof. Odilson Tadeu Valle
Orientador

Prof. Ederson Torresini
Co-orientador

Prof. Evandro Cantú
IFSC

Prof. Marcelo Maia Sobral
IFSC

Exige muito de ti e espera pouco dos outros.
Assim, evitarás muitos aborrecimentos.
Confúcio

Agradecimentos

Dedico este trabalho a minha família, sem a qual eu não teria o suporte para chegar até aqui. Principalmente a minha mãe por sempre me apoiar em todos os momentos.

Agradeço sinceramente a todos os professores que me ajudaram até este momento, durante todo o caminho da graduação até o dia de hoje. Agradeço especialmente o Odilson, pela orientação neste trabalho e por tirar diversas dúvidas quando tive dificuldate, também ao Ederson pela coorientação no trabalho e pelas várias horas que ele gastou me ajudando.

Aos meus amigos que me ajudaram nos momentos difíceis, a superar os obstáculos e criar motivação para concluir este trabalho.

Resumo

Este trabalho descreve detalhadamente a tecnologia de VLANs. Inicia pela descrição dos conceitos básicos e protocolos envolvidos e prosegue com o Padrão IEEE 802.1Q que suporta priorização de tráfego, objetivando a garantia de qualidade (QoS) para determinados serviços e/ou usuários. Em seguida é apresentado o Padrão IEEE 802.1X que define os serviços de autenticação, coibindo ou restringindo o acesso com mecanismos de controle de portas conveniados com o QoS. Baseado nas definições teóricas, o trabalho propõe alguns cenários para implantação de VLANs, diferenciados pelo tipo de ambiente e o tipo de aplicação pretendida. Culmina com uma proposta de implementação de VLANs no Campus São José do IFSC, mas que poderia ser adaptado à outras instituições.

Abstract

This paper describes in detail the technology of VLANs. It begins with the description of the basic concepts and protocols involved and proceeds with the IEEE 802.1Q standard which supports traffic priorization, aiming the Quality of Service (QoS) for certain services and/or users. Then its presented the IEEE 802.1X standard which defines the authentication services , restraining or restricting the access with port control mechanisms related with the QoS. Based in theoretical definitions, the paper proposes some VLAN implementation scenarios, distinguished by the type of enviroment and the type of desired application. It culminates with a VLAN implementation proposition on the Campus of São José IFSC, but that could be adapted to other institutions.

Conteúdo

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas

As seguintes abreviaturas são utilizadas neste trabalho:

AAA Authentication, Autorization, and Accounting

CFI Canonical Format Indicator

EAP Extensible Authentication Protocol

EAPOL EAP over LANs

EISS Enhanced Internal Sublayer Service

E-RIF Embedded Routing Information Field

FCS Frame Check Sequence

GARP Generic Attribute Registration Protocol

GID Garp Information Declaration

GIP GARP Information Propagation

GMRP GARP Multicast Registration Prococol

GVRP GARP VLAN Registration Protocol

IP Internet Protocol

ISS Internal Sublayer Service

IVL Independent VLAN Learning

LAN Local Area Network

MAC Medium Access Control

MAN Metropolitan Area Network

MPDU MAC Protocol Data Unit

MS Mac Service

MSDU MAC Service Data Unit

MST Multiple Spanning Tree

MSTP Multiple Spanning Tree Protocol

NCFI Non Canonical Format Indicator

OTP One Time Password

PACP Port Access Control Protocol

PAE Port Access Entity

PCP Priority Code Point

PDU Protocol Data Unit

PVID Port VID

RIF Routing Information Field

RSTP Rapid Spanning Tree Prococol

SST Single Spanning Tree

STP Spanning Tree Protocol

SVL Shared VLAN Learning

TCI Tag Control Information

TPID Tag Protocol Identifier

VID VLAN Identifier

VLAN Virtual Local Area Network

1 Introdução

Quando vamos estabelecer uma rede de comunicação de dados, sempre buscamos por melhorias como o aumento da segurança da rede para as informações dos usuários e do sistema. Quanto maior fica uma rede, mais árdua e complexa é a tarefa do gerente de rede para mantê-la organizada e completamente operante.

Uma tecnologia muito importante para melhorar estas questões dentro de uma rede é o estabelecimento de VLANs. Estas permitem melhorar muito as questões de segurança, organização lógica, escalabilidade, para facilitar a administração de uma rede.

Estaremos estudando os padrões IEEE 802.1Q, que define os padrões para o estabelecimento de VLANs, e IEEE 802.1X, que define os padrões de autenticação baseada em portas. O conhecimento destas normas nos permitirá a concepção de cenários de VLANs onde a autenticação do usuário irá definir a VLAN a qual ele pertence dentro de uma rede.

1.1 Organização do texto

O texto está organizado da seguinte forma:

- **Capítulo 2 - Virtual Local Area Network:** este capítulo descreve os conceitos fundamentais para a compreensão de VLANs e a autenticação de usuários;
- **Capítulo 3 - Padrão IEEE 802.1Q:** descreve o padrão IEEE 802.1Q que define vários conceitos e recomendações importantes para o estabelecimento de VLANs;
- **Capítulo 4 - Padrão IEEE 802.1X:** descrever o padrão IEEE 802.1X que define os princípios do controle de acesso baseado em portas e o protocolo de controle utilizado;
- **Capítulo 5 - Realização de cenários envolvendo VLANs e sugestões de**

implantação no IFSC: este capítulo irá mostrar alguns cenários de utilização de VLANs e sugestões para a implantação do serviço no campus SJ do IFSC;

- **Capítulo 6 - Conclusões:** apresenta as conclusões do trabalho;
- **Anexo A - Algumas configurações no Linux:** apresenta algumas configurações no Linux necessárias para estabelecer os cenários apresentados no Capítulo 5;
- **Anexo B - Configuração do switch DLINK DES-3526:** apresenta as configurações necessárias no *switch* utilizado neste trabalho;
- **Anexo C - DHCP:** descrição do protocolo DHCP, instalação e configuração do serviço;
- **Anexo D - RADIUS:** descrição do protocolo RADIUS, instação e configuração do serviço.

2 *Virtual Local Area Network*

Neste capítulo será descrito o princípio de funcionamento das *Virtual Local Area Networks* (VLANs), tal como alguns conceitos necessários para sua melhor compreensão. Passa-se por assuntos como as *Local Area Networks* e *Bridged Local Area Networks*, base principal para a implementação e funcionamento das VLANs. Será descrito um importante protocolo para o funcionamento de redes comutadas de dados, o *Spanning Tree Protocol* (STP), assim como, sua variação, muito importante dentro de um contexto VLAN, o *Multiple Spanning Tree Protocol* (MSTP).

2.1 Local Area Network

Local Area Network (LAN) são redes locais, possuindo dois ou mais terminais, que são interligados através de um barramento (historicamente HUB ou *Switch*[1]). A finalidade principal das LANs é a troca de dados entre terminais, permitindo também o compartilhamento de recursos de *software* e *hardware*. Quanto maiores forem as dimensões de uma LAN, maior será a degradação nos sinais até o recebimento por estações e assim poderão ocorrer erros. Redes locais definidas pelo padrão IEEE 802.3 devem se restringir a uma área de 10 quilômetros, quando a taxa de erro por degradação chega ao limite especificado, fazendo-se necessário o uso de equipamentos com suporte a outra tecnologia e passam a ser definidas pelo próprio padrão IEEE 802.3 como MAN (*Metropolitan Area Network*).

A aquitetura mais utilizada atualmente em Redes Locais é o TCP/IP, na versão IPv4, que já encontra-se com seu limite de endereços validos esgotado, e deverá migrar para o IPv6.

[1]Switch é um dispositivo interconectivo de rede que opera na camada 2 e pode operar também nas camadas 3, 4 e 7 do modelo OSI, ao contrário dos HUBs que operam na camada 1

2.2 Bridges

As *Bridges* são dispositivos que agem na camada de enlace, ao contrário dos hubs que são dispositivos de camada física e apenas funcionam como um barramento de dados. Elas repassam os quadros baseados no endereço de destino, ela examina o endereço de destino e procura em sua tabela de comutação qual interface que leva a este destino, repassando o quadro a devida interface.

Segundo KUROSE e ROSS(2006), as *Bridges* podem interconectar diferentes tecnologias de LAN, incluindo as *Ethernets 10BaseT*, *100BaseT* e *Gigabit Ethernet*.

As *Bridges* possuem importantes funções em uma rede. Elas separam o domínio de colisão[2] por portas, ao contrário de um hub que compreende um único domínio de colisão. Elas podem ser utilizadas para interligar diferentes LANs, formando as *Bridged* LANs (descritas em 2.3). Realizam a função de filtragem de quadros, onde a *Bridge* analisa se o quadro deve ser retransmitido ou apenas descartado.

As *Bridges* com suporte ao IEEE 802.1Q são fundamentais para a implementação de VLANs, são elas que tornam o processo possível. As *Bridges* podem oferecer também o serviço de roteamento(caso o *switch* possua suporte a serviço de camada 3), que somado ao serviço de VLAN poderá compreender grande parte da estrutura de uma rede.

2.3 Bridged Local Area Network

Por definição *Bridged* LAN é quando duas ou mais LANs são conectadas entre si através de uma ponte (*Switch*), agindo transparentemente como uma única LAN. Para ilustrar melhor o conceito de *Bridged* LAN, pega-se por exemplo uma empresa com diversos departamentos, cada qual com seus terminais interligados formando uma LAN, porém, há uma necessidade de interligar estes departamentos, com a adição de um *switch* entre as duas LANs, forma-se uma *Bridged* LAN. Uma *Bridged* LAN pode utilizar o algoritmo *spanning tree* (descrito em 2.5) para fazer a configuração das suas conexões. As *Bridged* LANs podem perder eficiência de acordo com seu tamanho, pois cada nó da LAN pode possuir dezenas de computadores ligados a ele, e mensagens de *broadcast* são encaminhadas por todos esses nós e podem chegar até ao ponto de congestionar os caminhos da rede.

[2]Domínio de colisão é uma área lógica que pode existir em uma rede, onde os pacotes podem colidir uns aos outros, gerando erros e diminuindo a eficiência da rede

Esta definição(*Bridged* LAN) caiu em desuso, pois atualmente com o barateamento dos equipamentos *Switch* e extinção dos HUBs, praticamente todas redes são interligadas por uma *Bridge*, então na sequência do estudo, todas LAN's devem ser consideradas como interligadas por meio de uma *Bridge*. Os padrões IEEE ainda fazem grande referência ao termo *Bridged* LAN.

2.4 VLAN

2.4.1 Definição de VLAN

Uma VLAN é um agrupamento lógico de estações, serviços e dispositivos de rede que não estão restritos a um segmento físico de uma rede local. Isto pode ser observado na Figura 1 (CISCO, 2003).

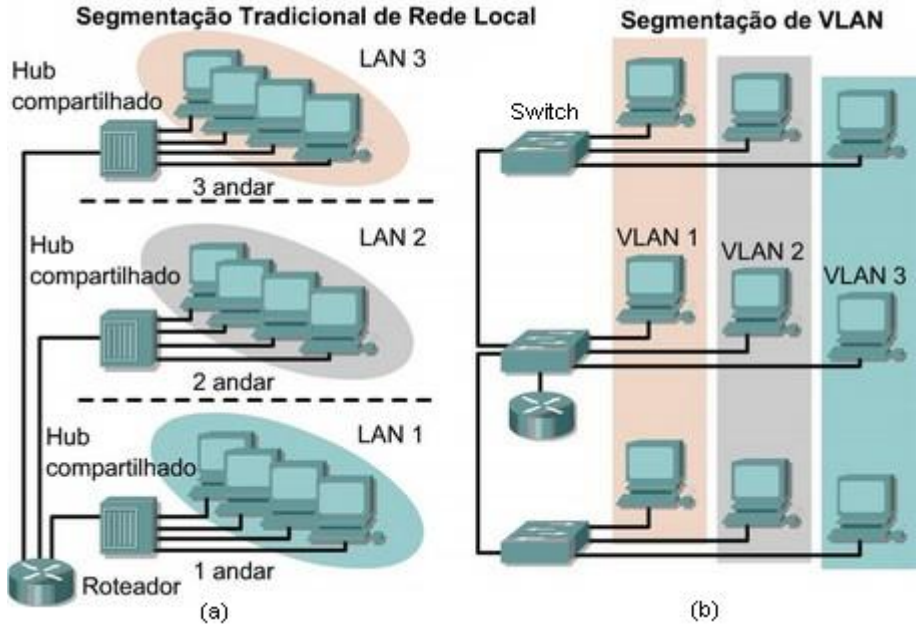

Figura 1: Comparação entre LAN e VLAN (CISCO, 2003)

Como pode ser observado na Figura 1, em (a), os terminais de um prédio estão limitadas a LAN do seu andar, limitação física que pode ser facilmente superada pela implementação de uma segmentação VLAN, mostrado em (b). Em uma LAN, todos terminais conectados a um HUB ou *switch* fazem parte da mesma LAN. Em uma VLAN, um *switch* pode atender diversas VLANs dependendo do tipo de identificação VLAN empregada, esta identificação será descrita em 2.4.3.

Faz-se necessário o uso de *switchs* para o estabelecimento das VLANs, ele que irá adicionar ou remover rótulos(será explicado a seguir) quando necessário. Cada VLAN

opera como uma LAN distinta, sendo necessário o uso de um roteador ou um *switch* com suporte a roteamento para estabelecer a conectividade entre diferentes VLANs.

As VLANs são configuradas nos *switchs* ou terminais de uma rede através da adição de um rótulo de 16 bits entre o cabeçalho *Ethernet* e o *Payload* de um quadro, ver a Figura 2. Com isto, apenas as portas do switch pertencentes a uma determinada VLAN irão receber os quadros destinados aquela VLAN. O quadro *Ethernet* aumenta em 4 octetos seu tamanho após a adição do rótulo. Uma descrição detalhada do rótulo VLAN está presente em 3.2.

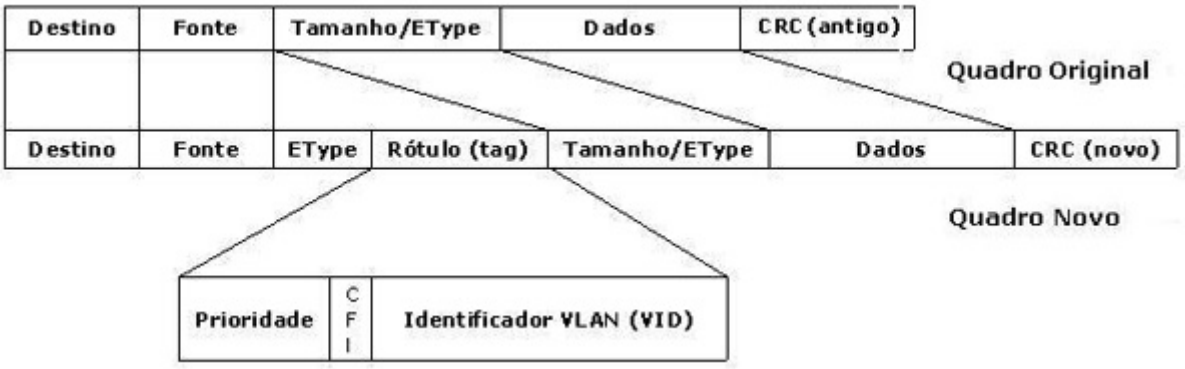

Figura 2: Quadro *Ethernet* antes e após adição do rótulo VLAN

Uma descrição maior das propriedades de uma VLAN, tais como regras e recomendações no seu estabelecimento, são previstas pelo padrão IEEE 802.1Q. No Capítulo 3 são citados alguns tópicos da norma.

2.4.2 Finalidade das VLANs

A função das VLANs é prover a segmentação lógica na rede, normalmente oferecida por roteadores em uma configuração LAN, permitindo a implementação serviços como: filtragem de *broadcast*, sumarização de endereços, segurança e controle de tráfego. São utilizadas para resolver problemas de escalabilidade, segurança e gerência de rede.

Uma VLAN pode ser definida como um domínio de *broadcast*[3] criado entre um ou mais *switchs*. O fato de filtrar os *broadcasts* e separar as redes adjacentes oferece segurança extra a uma rede, pois usuários de uma VLAN terão acesso somente ao tráfego que diz respeito a seu domínio, impossibilitando ações como, por exemplo, interceptação de quadros por um terminal não pertencente à mesma VLAN.

[3]Broadcasts são mensagens enviadas a todos os nós de uma rede, podendo ser mensagens de algum serviço na rede ou mensagens de requisição de estações

O processo de segmentação feito pelos roteadores é físico, cada interface do roteador irá representar um segmento da rede, enquanto a segmentação por VLAN é lógica, cada porta do *switch* pode fazer parte de um ou mais segmentos da rede, podendo ser alterada a qualquer momento por configuração

Por se tratarem de um agrupamento lógico na rede, diferentemente de uma LAN tradicional, as VLANs podem possuir terminais independentes de sua posição física na rede, estes terminais também podem ser adicionados ou removidos de diferentes VLANs a qualquer momento, bastando alterar a configuração no *switch* que liga o terminal em questão ao restante da rede, isto resolve diversos problemas de escalabilidade em uma rede, pois ela pode ser expandida ou dividida sem se preocupar com o espaço físico e estrutura do cabeamento já existente.

Toda a configuração das VLANs de uma rede pode ser feita remotamente pelo administrador, tornando desnecessário o acesso ou deslocamento até os armários de fiação. Isto, de forma geral, facilita muito a tarefa do administrador da rede ao custo de um maior planejamento e mais tempo investido na configuração da rede. Uma rede com VLANs mal configuradas podem também causar diversos problemas administrativos, como inoperabilidade da mesma ou quadros sendo filtrados de maneira incorreta.

Segundo PETERSON(2004) a principal limitação das VLANs é sua heterogeneidade, pois pelas *Bridges* se basearem no cabeçalho dos quadros de rede para fazer a divisão entre os quadros de VLAN, elas só poderão ser utilizadas para conectar *Ethernet* a *Ethernet*, 802.5[4] a 802.5 ou *Ethernet* a 802.5, por se tratarem de redes que admitem o mesmo formato de endereço de 48 bits.

2.4.3 Tipos de VLAN

É utilizado o termo VID(*VLAN Identifier* ou simplesmente Identificador VLAN para a identificação das VLANs, os segmentos que possuem o mesmo VID pertencem à mesma VLAN. De alguma forma os *switchs* devem reconhecer os VID's de cada quadro recebido, existem três métodos de reconhecimento:

- Baseado em porta;
- Baseado em endereço MAC;

[4]802.5 é o padrão IEEE que define as redes *Token Ring*, assim como o padrão IEEE que define a *Ethernet* é o 802.3.

- Baseado em protocolo da camada 3 ou endereço IP.

Nas VLANs baseadas em porta, cada porta da *Bridge* recebe uma ou mais VID's, fazendo com que todos os terminais que estiverem conectados na mesma porta pertençam à(s) mesma(s) VLAN(s). Este é o método mais utilizado para a implementação de VLANs. VLANs baseadas em porta são normalmente estáticas (2.4.4), mas podendo vir a se tornar dinâmicas com o uso de alguns artifícios extras na configuração da rede.

As VLANs baseadas em endereço MAC funcionam mantendo uma lista na *Bridge*, que contém o endereço MAC de cada máquina que está conectada a ela, fazendo com que a ponte extraia o endereço MAC dos pacotes recebidos e procure em sua lista para qual terminal deverá ser encaminhado. Este método permite atribuir diferentes cores a terminais ligados a uma mesma porta na rede. As vantagens deste tipo de abordagem é o fato de oferecer maior flexibilidade e certo nível de dinamicidade para as VLANs. As desvantagens deste método são o maior uso de recursos da rede para manter as tabelas sempre atualizadas e a necessidade da intervenção do administrador para incluir ou remover terminais da rede.

O terceiro tipo de VLAN é o baseado em protocolo de nível superior, ele analisa o campo de *Payload* dos quadros recebidos e os agrupa em uma determinada VLAN de acordo com alguma informação contida nele. Segundo TANENBAUM(2003) este método interfere na independência das camadas, pois o conteúdo do *Payload* não diz respeito à camada enlace, esta não deveria estar examinando seu conteúdo muito menos tomando decisões baseadas nele. Uma consequência possível desta técnica é que qualquer modificação no protocolo da camada 3 poderá fazer o *switch* falhar.

2.4.4 VLANs estáticas e dinâmicas

VLANs ditas estáticas se formam quando os terminais que pertencem a uma determinada VLAN possuem posição fixa na rede. Isto gera facilidade de administração da rede e elevação do nível de segurança.

VLANs ditas dinâmicas são quando os terminais que pertencem a uma determinada VLAN possuem posição variável na rede. Este tipo de abordagem pode ser implementada por meio do uso de VLANs baseadas em MAC ou então por meio da autenticação de usuários na rede(ver capítulo 4). VLANs dinâmicas geram um nível maior de complexidade na configuração e falhas de configuração podem vir a diminuir os níveis de segurança da rede. A vantagem é a flexibilidade, que pode ser desejável em determinadas

redes, como por exemplo acesso para visitantes em uma rede institucional.

2.4.5 Interfaces de acesso e de *trunking*

Interfaces de acesso são as interfaces da *Bridge* que encaminham os quadros sem rótulo VLAN ao seu destino, geralmente anexado a uma única VLAN. Nesta configuração, a existência da VLAN é transparente para o cliente que está conectado através desta interface, pois ele irá transmitir e receber quadros somente sem rótulo. Cabe a *Bridge* a função de adicionar o rótulo VLAN na recepção dos quadros e removê-lo no encaminhamento. Quadros com rótulo VLAN recebidos pela *Bridge* em uma interface de acesso serão descartados. Este tipo de interface é utilizada para fazer a ligação entre a *Bridge* e os clientes da rede.

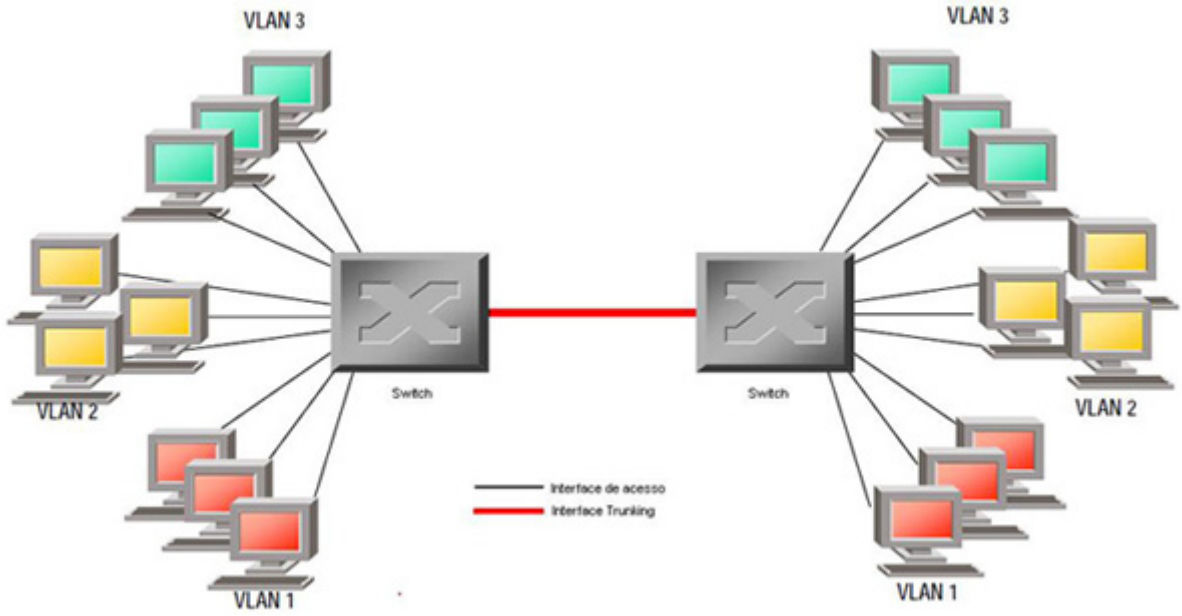

Figura 3: Interfaces de acesso e *trunking*

Interfaces de *trunking* são as interfaces da *Bridge* que encaminham os quadros com rótulo VLAN ao seu destino, geralmente anexado a mais de uma VLAN. Todos terminais, roteadores ou *switchs* conectados em uma interface de *trunking* são cientes de VLAN. Quadros sem rótulo VLAN recebidos por uma *Bridge* em uma interface *trunking* serão descartados. Este tipo de interface é utilizada para fazer a conexão entre dois *switchs* em uma rede, onde ambos necessitam das informações das VLANs que eles atendem, ou a conexão entre um *switch* e um servidor/provedor de serviço na rede.

A Figura 3 mostra o funcionamento dos dois tipos de interface. Os terminais de usuário possuem interface de acesso, e todo processo de VLAN está transparente para

eles, pois a informação do rótulo VLAN não lhes diz respeito. Já os *switchs* precisam trocar as informações de rótulo entre si, para saber para quais portas devem ou não ser encaminhados os quadros recebidos.

2.5 Spanning Tree Procotol

Em uma *Bridged* LAN pode ser desejável que exista um certo nível de redundância de caminhos na rede, isto para que a rede não se torne inoperante em caso de falha de algum segmento. A adição de caminhos redundantes na rede pode causar diversos problemas, como por exemplo, uma tempestade de *broadcast* se perdendo infinitamente em *loops*[5] da rede, causando congestionamento naquele segmento e fatalmente tornar a rede inoperante.

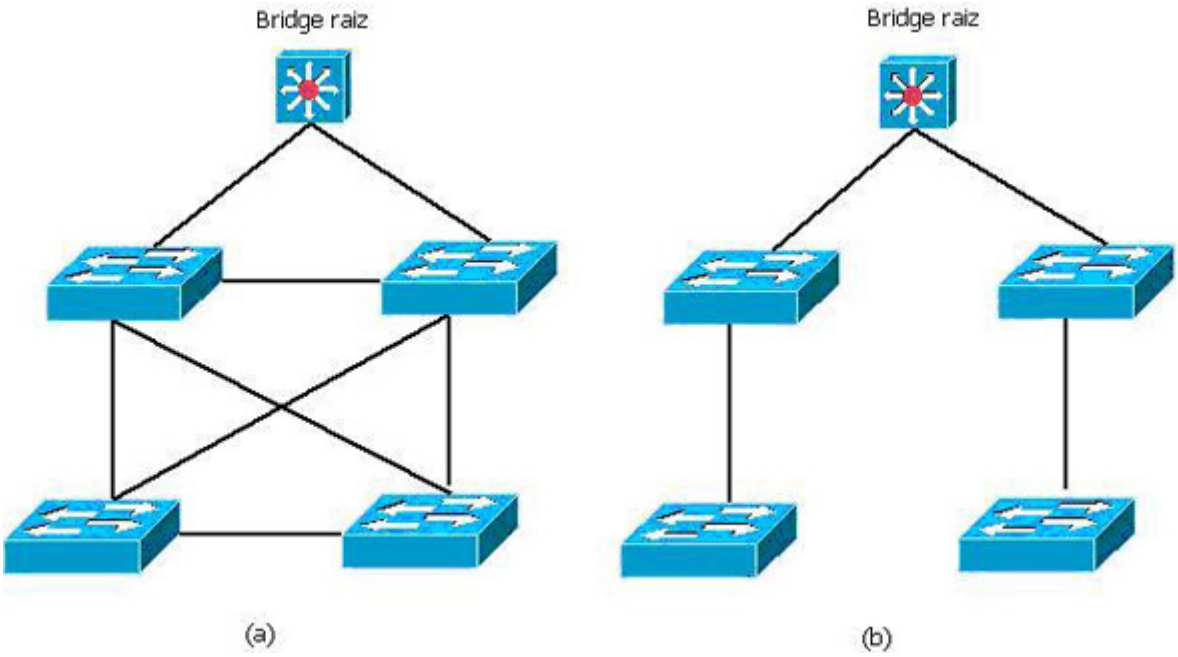

Figura 4: Exemplo simples do STP

Para resolver os problemas causados por *loops* nas redes, foi desenvolvido o *Spanning Tree Protocol* (STP). Ele calcula, através do algoritmo *spanning tree*, o custo dos diversos caminhos existentes na rede e estabelece qual caminho será utilizado. Com base neste cálculo ele então estabelece uma topologia lógica que será utilizada como base para o encaminhamento dos quadros na rede. Em caso de falha ou congestionamento de um segmento, ele recalcula os caminhos e atualiza a topologia lógica. Então em uma rede com diversos caminhos pela topologia física, o STP irá criar uma única topologia lógica e usá-la como ativa e colocar as outras topologias em estado de bloqueio.

[5]Loops são os circuitos fechados dentro de uma rede.

A Figura 4 mostra em (a) uma rede de quatro *switchs* ligados a uma *Bridge* raiz, contendo diversos loops. Em (b) mostra como poderia ficar a topologia lógica ativa da rede. Os demais caminhos ficam logicamente bloqueados na rede e poderão ser utilizados em uma outra topologia lógica pelo STP caso seja necessário.

Em um contexto VLAN, cada VLAN pode ter a necessidade de possuir uma instância própria dos caminhos redundantes para o seu funcionamento. Para lidar com estas múltiplas instâncias, foi desenvolvido o *Multiple Spanning Tree Protocol* (MSTP). Uma descrição detalhada do MSTP e suas características podem ser vistas no capítulo 13 da `IEEE Std 802.1Q`.

3 Padrão IEEE 802.1Q

Neste capítulo serão descritos alguns conceitos propostos pelo padrão, tais como regras e recomendações de uso, funcionalidades e compatibilidade de serviço, formato do rótulo VLAN nos quadros.

Neste capítulo será apresentado o resumo de alguns capítulo do padrão IEEE 802.1Q, que servem como base para o estudo.

3.1 Princípios da operação de redes

3.1.1 Visão geral da rede

A operação de uma *Virtual Bridged Local Area Network*, das *Bridges* e LANs, que compõem esta rede compreende:

- Uma topologia física compreendendo LANs, *Bridges* e portas de *Bridges*. Cada porta de *Bridge* liga uma LAN e é capaz de prover conectividade bidirecional para os quadros MAC de dados de usuário. Cada LAN é conectada com qualquer outra LAN através de uma *Bridge*.
- Cálculo de uma ou mais topologias ativas, cada uma sendo um subconjunto livre de *loops* da topologia física.
- Regras de classificação dos quadros MAC de dados de usuário que permitem a cada *Bridge* alocar, direta ou indiretamente, cada quadro a apenas uma topologia ativa.
- Gerência da conectividade provida por quadros de dados diferentemente classificados pela topologia ativa selecionada.
- Configuração implícita ou explicita da informação sobre a localização das estações finais, identificando LANs com estações finais ligadas que necessitam receber quadros de dados de usuário com um determinado endereço de destino.

- Comunicação sobre a localização das estações finais, para permitir que as *Bridges* restrinjam os quadros de dados de usuário às LANs que fazem parte do caminho provido até seus destinos.

3.1.2 Uso das VLANs

Virtual Local Area Networks (VLANs) e seus Identificadores VLAN (VIDs) proveem uma ampla, consistente e conveniente referência para que as *Bridges*:

- Identifiquem regras de classificação dos quadros de dados de usuário nas VLANs;
- Estendam efetivamente os endereços MAC de origem e destino, tratando os quadros e endereçando informações para diferentes VLANs independentemente;
- Identifiquem e selecionem entre diversas topologias ativas;
- Identifiquem a configuração dos parâmetros divididos em partes ou restringir acesso de uma das partes da rede à outra.

Juntando estas capacidades, torna-se possível as *Bridges* emular um número de *Bridged* LANs ou VLANs gerenciáveis. Um segmento de LAN que foi selecionado pela rede para receber quadros direcionados a uma determinada VLAN, é dito fazer parte, ou ser membro da VLAN. Similarmente, as estações finais que estão conectadas a estes segmentos de LAN e podem receber quadros direcionados a esta VLAN, são ditos fazer parte desta VLAN.

O rótulo VLAN permite aos quadros carregarem informações de prioridade, até mesmo se o quadro não foi classificado como parte de uma determinada VLAN.

3.1.3 Topologia VLAN

Cada *Bridge* coopera com as outras para operarem um STP para calcular uma ou mais topologias ativas, livres de *loop* e com total conectividade entre as estações finais. Este cálculo suporta a qualidade do Mac Service e provê uma recuperação rápida a rede causada pela falha de algum componente, utilizando uma conexão física alternativa, sem a necessidade de intervenção de gerência.

Todos os quadros de dados de usuário que estão classificados como pertencentes a uma determinada VLAN são forçados pelo processo de encaminhamento de cada *Bridge*

a fazerem parte de uma única topologia ativa. Toda VLAN é associada com uma *spanning tree*, embora, mais de uma VLAN pode ser associada à uma mesma *spanning tree*. Cada VLAN pode ocupar a extensão total da topologia ativa de sua *spanning tree* associada ou ser um subconjunto conectado desta topologia ativa. A extensão máxima de um subconjunto conectado pode ser limitada por gerência, através da exclusão explícita de certas portas da *Bridge* da conectividade da VLAN.

A qualquer momento, a extensão máxima de uma VLAN pode ser reduzida do seu valor máximo para incluir apenas os segmentos de LAN que proveem serviços de comunicação entre dispositivos conectados, pelo uso de um protocolo que permita as estações finais requisitar e liberar serviços que usam a VLAN. A determinação dinâmica da extensão da VLAN provê flexibilidade e conservação de largura de banda, ao custo de complexidade administrativa.

3.1.4 Localizando estações finais

Cada estação final anuncia implicitamente sua conexão a um segmento LAN e seu endereço MAC individual sempre que transmite um quadro. *Bridges* podem aprender o endereço de origem enquanto elas encaminham o quadro através da topologia ativa para seu destino ou destinos - ou através da VLAN se o local de destino ou destinos é desconhecido. A informação aprendida é armazenada na Base de Dados de Filtragem, utilizada para filtrar quadros com base nos seus endereços de destino.

A arquitetura da Base de Dados de Filtragem definida neste padrão reconhece que:

- Para algumas configurações, é necessário permitir que a informação de endereço aprendida em uma VLAN possa ser compartilhada com um certo número de outras VLANs. Isto é conhecido como *Shared VLAN Learning* (SVL);
- Para algumas configurações, é desejável que a informação de endereço aprendida por uma VLAN não seja compartilhada com outras VLANs. Isto é conhecido como *Independent VLAN Learning* (IVL);
- Para algumas configurações, é irrelevante se a informação aprendida é compartilhada entre as VLANs.

O Aprendizado de VLAN Compartilhada é alcançado através da inclusão da informação aprendida por um certo número de VLANs na mesma Base de Dados de Fil-

tragem; o Aprendizado de VLAN Individual é alcançado através da inclusão da informação aprendida por cada VLAN em uma Base de Dados de Filtragem distinta.

3.1.5 Regras de ingresso, encaminhamento e egresso

A função de retransmissão provida por cada *Bridge* controla:

- Classificação de cada quadro recebido como pertencente a uma e somente uma VLAN, e o descarte ou aceitação do quadro para processamento adicional baseado nesta classificação e no formato de quadro recebido, o qual pode ser uma das três possibilidades:

  1. Sem rótulo, e não identificado explicitamente o quadro como sendo pertencente a uma VLAN específica;
  2. Rótulo de prioridade, ou seja, incluir um rótulo de cabeçalho atribuindo informação explícita de prioridade, mas não identificando os quadros como pertencentes a uma VLAN específica;
  3. Rótulo de VLAN, ou seja, identificação explicita dos quadros como sendo pertencentes a uma VLAN específica.

  Este aspecto da retransmissão implementa as regras de ingresso.

- Implementação das decisões que definem para onde cada quadro deve ser encaminhado como determinado pela atual topologia VLAN (3.1.3), informação sobre a localização da estação (3.1.4). Este aspecto da retransmissão implementa as regras de encaminhamento.

- Fila de espera para a transmissão dos quadros através das portas selecionadas da *Bridge*, gerência dos quadros em espera, seleção dos quadros para transmissão, e a determinação do tipo apropriado de formato do quadro, com rotulo VLAN ou sem rótulo. Este aspecto da retransmissão implementa as regras de egresso.

3.2 Formato do quadro com rótulo

3.2.1 Propósito da rotulação

- Permite a veiculação de um VLAN *Identifier* (VID), facilitando uma classificação VLAN consistente do quadro através da rede e possibilitando a segregação dos

quadros atribuída a diferentes VLANs;

- Permite a veiculação da prioridade com o quadro quando estiver utilizando métodos de controle de acesso a mídia LAN IEEE 802, para não prover capacidade inerente a prioridade de sinalização;
- Pode suportar o uso de diferentes métodos de controle de acesso a mídia em uma única rede.

3.2.2 Formato do rótulo

Cada rótulo VLAN compreende os seguintes elementos de informação sequencial:

- Um Tag Protocol Identifier (TPID) (3.2.3);
- Tag Control Information (TCI) que é dependente do tipo de rótulo (3.2.4, 3.2.5);
- Informação adicional, se e quando requisitada pelo tipo de rótulo e TCI.

3.2.3 Formatos do Tag Protocol Identifier (TPID)

O TPID inclui um valor *Ethernet Type* que é utilizado para identificar o quadro como quadro rotulado e para selecionar as funções de decodificação de rótulo corretas.

3.2.4 *Tag Protocol Identification*

Um único tipo de rótulo é especificado:

- Um RÓTULO VLAN, para uso geral das Bridges.

Um *Ethertype* distinto foi alocado para o uso no campo TPID de cada tipo de rótulo para que eles possam ser distintos um do outro, e de outros protocolos.

Tipo de Rótulo	**Nome**	**Valor**
Rótulo VLAN	IEEE Std 802.1Q Tag Protocol Type (802.1QTagType)	81 - 00

Tabela 1: IEEE 802.1Q Alocações *Ethernet Type*

3.2.5 VLAN Tag Control Information

O campo TCI do rótulo VLAN (Figura 5) tem comprimento de 2 octetos e codifica os parâmetros *vlan-identifier* e prioridade como números binários sem sinalização e um *Canonical Format Indicator* (CFI) como um único bit.

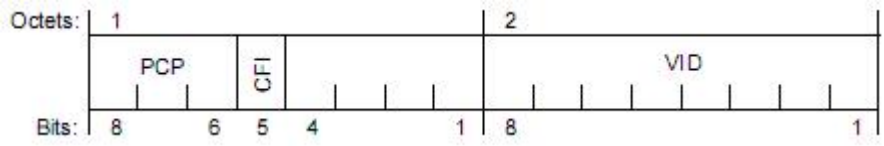

Figura 5: Formato do campo TCI do rótulo VLAN

O identificador VLAN é codificado em um campo de 12 bits. Uma *Bridge* ciente de VLAN pode não suportar uma faixa completa de valores de VID mas deve suportar o uso de todos valores VID na faixa de 0 até um máximo N, menor ou igual a 4094 e especificado para esta implementação. A Tabela 2 identifica valores de VID que possuem significados ou usos específicos.

Valor VID (hexadecimal)	**Significado / Uso**
0	O identificador VLAN nulo. Indica que o cabeçalho do rótulo possui apenas informação de prioridade; não existe identificador de VLAN presente no quadro. Este valor VID não deve ser configurado como um PVID ou como membro de um conjunto VID, ou configurado em qualquer entrada da Base de Dados de Filtragem, ou utilizado em qualquer operação de gerência.
1	O valor PVID padrão utilizado para classificar quadros que ingressam através de uma porta de uma *Bridge*. O valor PVID de uma porta pode ser modificado pela gerência.
FFF	Reservado para uso de implementação. Este valor VID não deve ser configurado como um PVID ou como membro de um conjunto VID, ou transmitido como rótulo de cabeçalho. Este valor VID pode ser usado para indicar uma combinação coringa para o VID em operações de gerência ou entradas na Base de Dados de Filtragem.

Tabela 2: Valores VID reservados

A prioridade é veiculada no 3-bit do campo *Priority Code Point* (PCP).

O bit CFI é usado para indicar que todos os endereços MAC presentes no campo de dados MAC (MAC data field) estão na forma canônica. Este campo é interpretado de forma diferente de acordo com a tecnologia utilizada (Ethernet, token ring, FDDI).

4 Padrão IEEE 802.1X

O objetivo deste capítulo é descrever alguns conceitos propostos pelo padrão, tais como regras e recomendações de uso, o princípio do controle de usuários e aplicações baseadas em porta, descrição do protocolo utilizado e algumas diretrizes de gerência.

Neste capítulo iremos apresentar um resumo de alguns capítulos do padrão IEEE 802.1X, que servem como base para o estudo.

4.1 Princípios da operação de Controle de Acesso a Portas

4.1.1 Função da operação de Controle de Acesso a Portas

O Controle de Acesso a Portas provê uma extensão opcional a funcionalidade de um Sistema (ver 4.1.3) que oferece um meio de prevenir acesso não autorizado de Suplicantes aos serviços oferecidos por este Sistema, e também prevenindo que uma Suplicante tente acessar um Sistema não autorizado. O Controle de Acesso a Portas também provê um meio pelo qual um sistema Suplicante pode prevenir que um sistema não autorizado se conecte a ele. Por exemplo, se o Sistema em questão é uma *Bridge* MAC, o controle sobre o acesso à *Bridge* e a LAN ao qual é conectado pode ser desejável para restringir o acesso a portas da *Bridge* acessíveis publicamente, ou dentro de uma organização, para restringir o acesso a uma LAN de departamento aos seus membros.

O controle de acesso é alcançado pelo Sistema forçando a autenticação de Suplicantes que se anexam as portas controladas pelo Sistema; do resultado do processo de autenticação, o Sistema pode determinar se uma Suplicante tem ou não autorização para acessar os serviços na porta controlada em questão. Se a Suplicante não é autorizada para o acesso, então ambos os Sistemas da Suplicante e do Autenticador configuram o estado das suas portas controladas para não autorizadas. No estado não autorizado, o uso da porta controlada é restrito de acordo com o valor do parâmetro *OperControlledDirections*

associado com a porta controlada (ver 4.1.5), prevenindo a transferência de dados não autorizada entre o Sistema Suplicante e os serviços oferecidos pelo Sistema Autenticador.

Os mecanismos definidos podem ser aplicados para permitir que qualquer Sistema autentique outro Sistema que está conectado em uma de suas portas controladas. Os Sistemas em questão incluem estações finais, servidores, roteadores e *Bridges* MAC.

4.1.2 Escopo da operação de Controle de Acesso a Portas

A operação do Controle de Acesso a Portas assume que as portas nas quais ele opera, oferecem uma conexão ponto a ponto entre uma única Suplicante e um único Autenticador. É esta suposição que permite as decisões de autenticação sejam feitas baseadas em portas. A autenticação de múltiplas PAEs Suplicantes anexadas a um único PAE Autenticador está fora do âmbito deste padrão.

Este padrão provê um protocolo para a comunicação de informação de autenticação entre uma Suplicante que esta anexada a porta de um Sistema Autenticador e um Servidor Autenticador, e para controlar o estado de porta do Autenticador e Sistema Suplicante, dependendo do resultado da troca de informações por protocolo. Este padrão não especifica a natureza da informação de autenticação que é trocada, nem em que base o Servidor de Autenticação toma suas decisões.

4.1.3 Sistemas, portas, e regras de sistema

Dispositivos que estão ligados a uma LAN, referenciados por este padrão como Sistemas, possuem um ou mais pontos de ligação com a LAN, referenciados por este padrão como portas de acesso a rede, ou portas.

As portas de um Sistema provêm meios para que ele possa acessar os serviços oferecidos por outros Sistemas alcançáveis através da LAN, e prover os meios pelos quais pode oferecer serviços para, ou acessar os serviços providos por, outros Sistemas alcançáveis através da LAN. O controle de acesso de rede baseado em portas permite que a operação de portas de Sistema sejam controladas de forma a garantir acesso aos seus serviços, e/ou acesso aos serviços de outros Sistemas, apenas permitido por Sistemas que estão autorizados a fazê-lo.

Para o propósito de descrever a operação do controle de acesso baseado em porta, uma porta de um Sistema (ou mais corretamente, um PAE associado com a porta; ver

4.1.6) é capaz de assumir um ou ambos os distintos papéis em uma interação do controle de acesso:

- Autenticador: A porta que deseja impor autenticação antes de permitir acesso a serviços que são acessíveis por ela adota o papel do Autenticador.
- Suplicante: A porta que deseja acessar os serviços oferecidos pelo sistema Autenticador adota o papel do Suplicante.

Um papel de Sistema adicional é descrito a seguir:

- Servidor de Autenticação: O Servidor de Autenticação realiza a função de autenticação necessária para conferir as credenciais de uma Suplicante para o Autenticador e indica se a Suplicante é autorizada para acessar os serviços do Autenticador.

Como pode ser visto nestas descrições, todos os três papéis são necessários para completar a troca de autenticação. Um dado Sistema pode ser capaz de adotar um ou mais destes papéis; por exemplo, um Autenticador e um Servidor de Autenticação podem ser co-alocados em um mesmo Sistema, permitindo que este Sistema realize a função de autenticação sem a necessidade de comunicar-se com um servidor externo. Similarmente, um PAE pode adotar o papel de Suplicante em algumas trocas de autenticação, e o papel de Autenticador em outras.

4.1.4 Acesso com controle e sem controle

A Figura 6 ilustra que a operação do Controle de Acesso a Portas tem o efeito de criar dois pontos distintos de acesso a um ponto de conexão do Sistema a LAN. Um ponto de acesso permite a troca sem controle de PDUs entre o Sistema e outros Sistemas da LAN, independentes do estado de autorização (*uncontrolled Port*); o outro ponto de acesso permite a troca de PDUs apenas se o atual estado da porta é Autorizado (*controlled Port*). As portas sem controle e com controle são consideradas fazerem parte do mesmo ponto de conexão com a LAN; qualquer quadro recebido na porta física é tornado disponível em ambas a portas com e sem controle, sujeitas ao estado de autorização na porta com controle.

O ponto de conexão com a LAN pode ser provido por qualquer porta física ou lógica que possa prover a conexão um a um com outro Sistema.

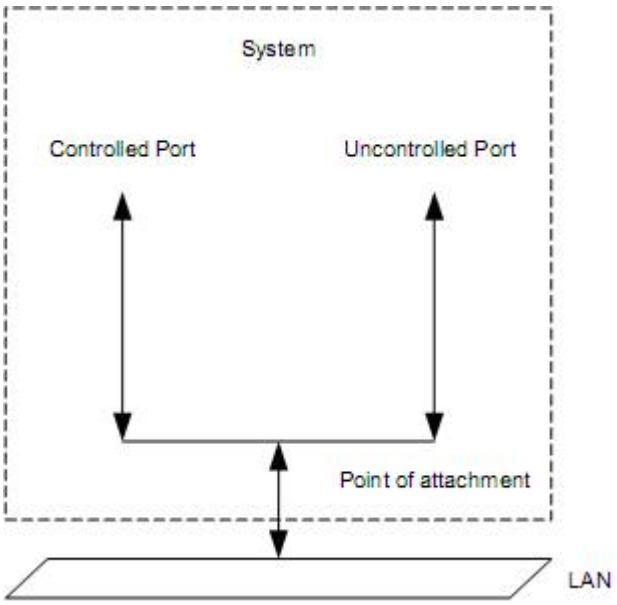

Figura 6: Portas com controle e sem controle

A Figura 7 ilustra o efeito do *AuthControllerPortStatus* associado com a porta controlada, representando este estado como um interruptor que pode ser ligado ou desligado, então permitindo ou prevenindo a inundação de PDUs através desta porta. A figura mostra dois sistemas, cada um com uma única porta; o parâmetro *OperControlledDirections* (ver 4.1.5) de cada porta é assumido como configurado para ambas. No Sistema 1, o *AuthControlledPortStatus* associado com a porta controlada é *unauthorized* e é portanto desabilitado (o "interruptor" é desligado); no Sistema 2, o *AuthControlledPortStatus* é *authorized* e é portanto habilitado (o "interruptor" é ligado).

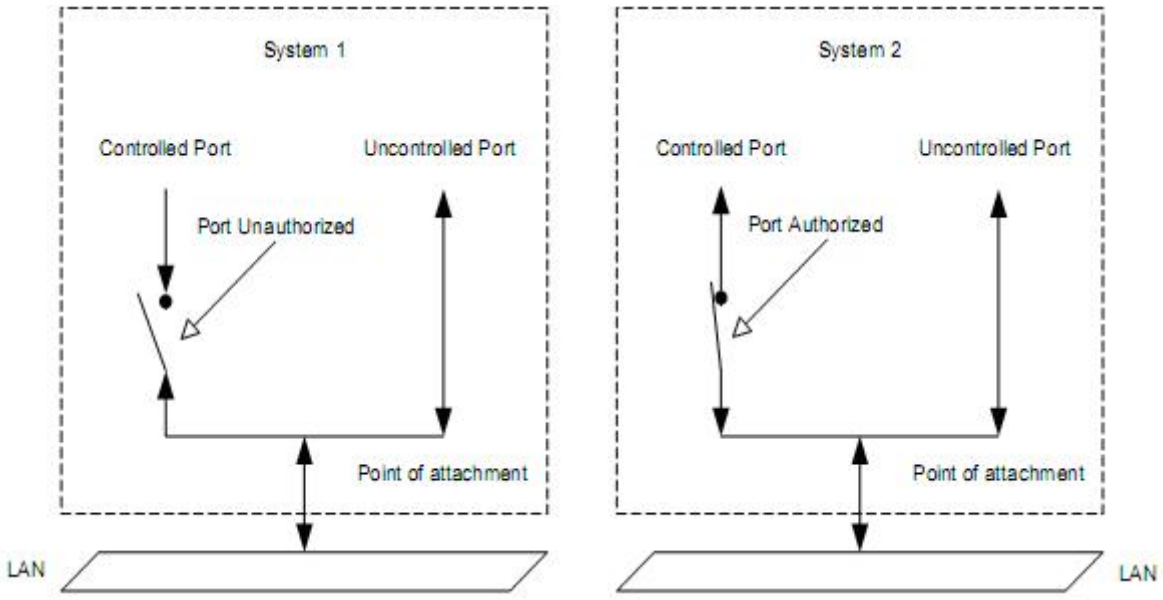

Figura 7: Efeito do estado de autorização nas portas com controle

Em adição ao *AuthControlledPortStatus*, um parâmetro *AuthControlledPortControl* é associado com a porta permitindo controle administrativo sobre o estado de autorização da porta. Este parâmetro pode receber os valores *ForceUnauthorized*, *Auto*, e *ForceAuthorized*; o valor padrão é *Auto*. A relação entre os parâmetros *AuthControlledPortStatus* e *AuthControlledPortControl* é:

- Um valor *ForceUnauthorized* no *AuthControlledPortControl* força o estado de máquina (ver 8.2.4 na IEEE Std 802.1X) do PAE Autenticador a configurar um valor de *AuthControlledPortStatus* para ser não autorizado; ou seja, A porta com controle é não autorizada incondicionalmente.
- Um valor *ForceAuthorized* no *AuthControlledPortControl* força o estado de máquina (ver 8.2.4 na IEEE Std 802.1X) do PAE Autenticador a configurar um valor de *AuthControlledPortStatus* pare ser autorizado; ou seja, A porta com controle é autorizada incondicionalmente.
- Um valor *Auto* no *AuthControlledPortControl* permite ao estado de máquina da PAE Autenticadora controlar o valor do *AuthControlledPortStatus* para refletir o resultado das trocas de autenticação entre a PAE Suplicante, PAE Autenticadora e Servidor de Autenticação.

Em todos os três casos, o valor de AuthControlledPortStatus reflete diretamente no valor da variável *portStatus* mantidas pelos estados de máquina da PAE Suplicante e Autenticadora (ver 8.2.2.2, 8.2.4, e 8.2.11 na IEEE Std 802.1X). Três fatores contribuem para o valor da variável *portStatus*:

- O estado de autorização do estado de máquina da PAE Autenticadora (assumido ser "autorizado" se o estado de máquina não é implementado para esta porta).
- O estado de autorização do estado de máquina da PAE Suplicante (assumido ser "autorizado" se o estado de máquina não é implementado para esta porta).
- O estado do *Supplicant Acess Control With Authenticator*, um parâmetro de controle administrativo. Este parâmetro possui dois valores possíveis, *active* e *inactive*. O valor padrão deste parâmetro de controle é *inactive*; o suporte ao valor *active* é opcional. O valor desde parâmetro tem efeito apenas de ambos os estados de máquina da PAE Autenticadora e PAE Suplicante forem implementados para aquela porta. Se o valor do parâmetro é *inactive*, então o parâmetro *portStatus* é determinado

apenas pelo estado de autorização do estado de máquina da PAE Autenticadora. Se o valor do parâmetro é *active*, então o parâmetro *portStatus* é determinado pelo estado de autorização de ambos estados de máquina da PAE Autorizadora e PAE Suplicante; se qualquer estado de máquina estiver em estado não autorizado, então o valor de *portStatus* é não autorizado.

O valor do parâmetro *AuthControlledPortControl* para cada porta do Sistema pode ser substituído por meio do parâmetro *SystemAuthControl* para o Sistema. Este parâmetro pode receber os valores *Enabled* e *Disabled*; seu valor padrão é *Disabled*. Se o *SystemAuthControl* é configurado como *Enabled*, então a autenticação é habilitada para o Sistema, e o estado de autenticação de cada porta é controlado de acordo com o valor do parâmetro *AuthControlledPortControl* da porta. Se o *SystemAuthControl* é configurado como *Disabled*, então todas as portas se comportam como se seu parâmetro *AuthControlledPortControl* esteja configurado como *ForceAuthorized*. Sob efeito, configurando o parâmetro *SystemAuthControl* como *Disabled* faz com que a autenticação seja desabilitada em todas as portas, e força todas portas com controle a serem Autorizadas.

Qualquer acesso a LAN é sujeita ao atual estado administrativo e operacional do MAC (ou MAC lógico) associado com a porta, em adição ao *AuthControlledPortStatus*. Se o MAC estiver física ou administrativamente inoperante, então não haverá trocas de protocolo de nenhum tipo usando este MAC nas portas com controle ou sem controle Isto é ilustrado na Figura 8; no Sistema 1, ambas as portas com e sem controle são capazes de acessar a LAN, pois a porta com controle é autorizada e o MAC que está provendo o ponto de conexão com a LAN está operante. No Sistema 2, nem a porta com controle nem a sem controle podem acessar a LAN, pois o MAC que está provendo o ponto de conexão com a LAN está inoperante. O estado inoperante do MAC também fez com que a PAE Autenticadora fizesse a transição da porta com controle para o estado não autorizado, como mostrado na Figura 8.

As PAEs do Suplicante e Autenticador usam as portas sem controle com objetivo de trocar informações de protocolo com outra PAE Suplicante ou Autenticadora.

Trocas de protocolo entre a PAE Autenticadora e o Servidor de Autenticação (se o servidor não for co-alocado com a PAE Autenticadora) podem ser conduzidos via uma ou mais portas sem controle do Sistema.

É esperado que a maioria das trocas de protocolo conduzidas pelas outras funções do Sistema façam uso de uma ou mais portas com controle do Sistema. No entanto, um

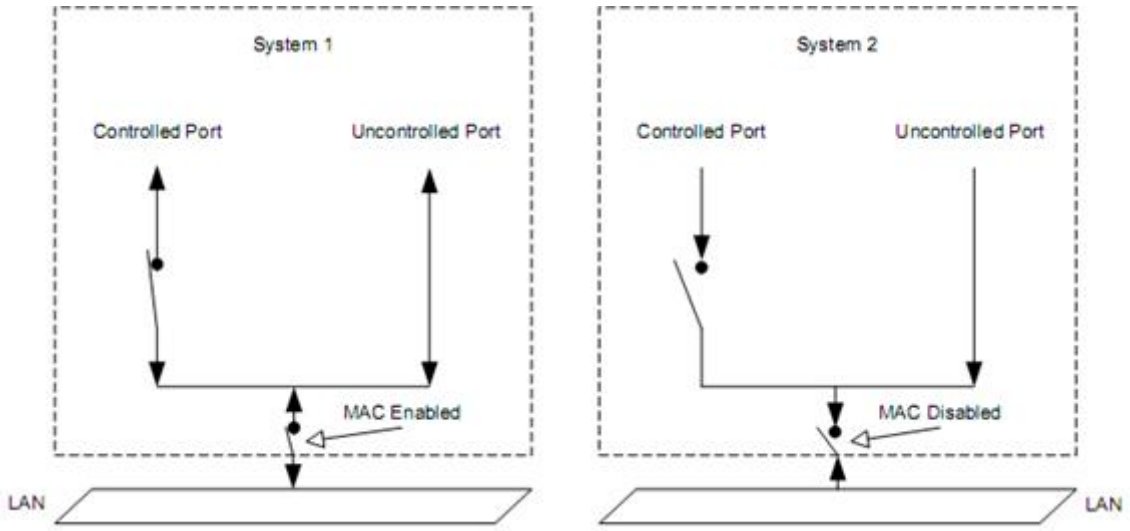

Figura 8: Efeito dos estados MAC Enabled/Disabled

determinado protocolo pode ter a necessidade de contornar a função de autorização e fazer uso da porta sem controle. A Figura 9 mostra os usos das portas com e sem controle em um Sistema Autenticador e um Sistema Suplicante, e a habilidade dos PAEs de mudar o estado de autorização da porta com controle de acordo com o resultado da troca de autenticação; a figura também mostra um exemplo das entidades de protocolo(as PAEs) que requerem o uso de uma porta sem controle para conduzir suas trocas de protocolo.

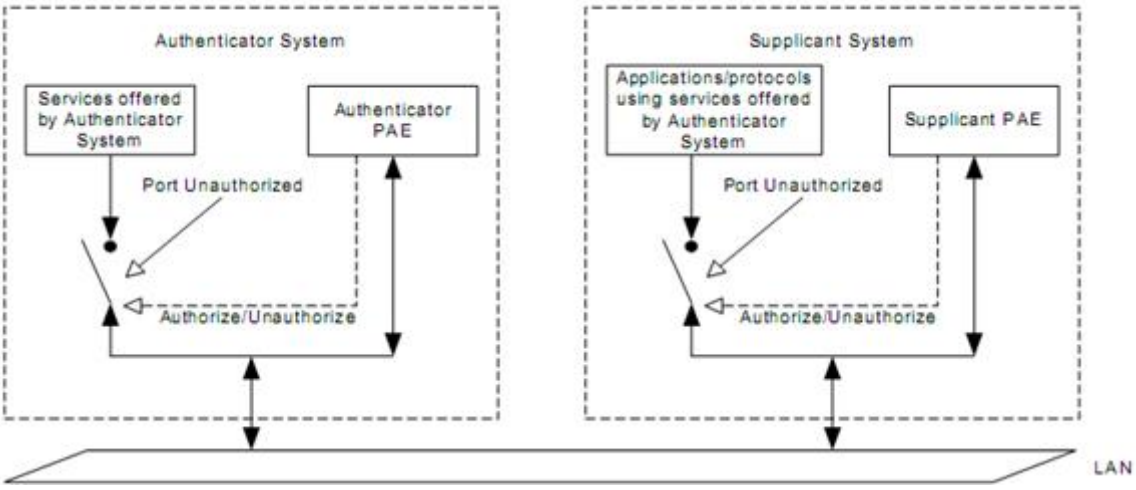

Figura 9: Uso das portas com e sem controle

A figura 10 ilustra a relação entre o Suplicante, Autenticador, e o Servidor de Autenticação, e a troca de informação entre eles. Nesta ilustração, ambas as portas do Suplicante e Autenticador estão no estado não autorizado e portando desabilitadas sob o ponto de vista do Sistema Suplicante, de acesso aos serviços do Sistema Autenticador. As duas PAEs fazem uso de suas portas sem controle para comunicar-se uma com a outra,

usando um protocolo de autenticação carregada na Camada Enlace, e a PAE Autenticadora se comunica com o Servidor de Autenticação usando um protocolo carregado por um protocolo de camada superior.

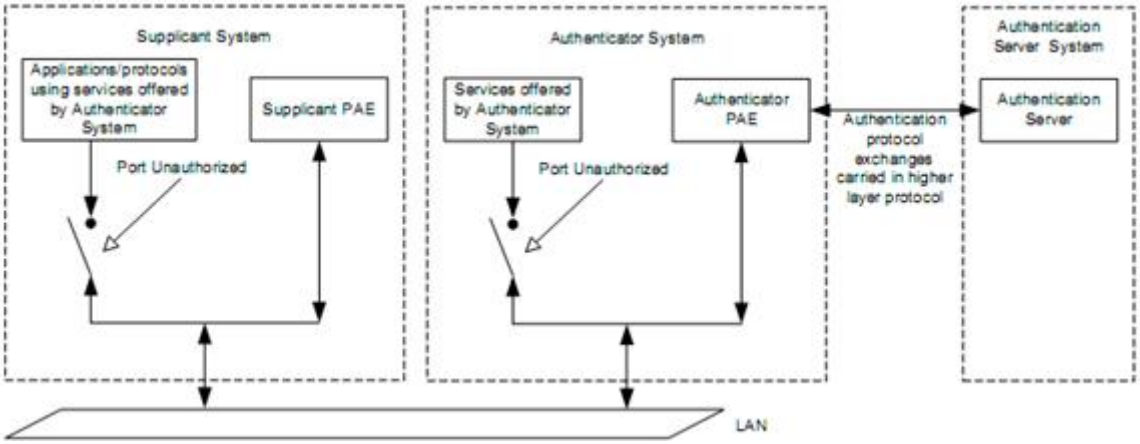

Figura 10: Papéis do Autenticador, Suplicante e Servidor de Autenticação

A comunicação entre o Autenticador e o Servidor de Autenticação pode fazer uso dos serviços de uma LAN, ou podem usar outro canal de comunicação. Nos casos nos quais o Servidor de Autenticação é co-alocado com o Autenticador, trocas de protocolos de autenticação entre estas duas entidades são desnecessárias.

Os serviços do Sistema B e a PAE do Sistema A, devem adotar o papel do Suplicante, e a PAE do Sistema B o papel do Autenticador. Para o Sistema B fazer uso dos serviços do Sistema A, os papéis são invertidos. Note que embora a função do Servidor de Autenticação é mostrada como residente em dois sistemas distintos neste exemplo, este não precisa ser o caso. Note também que, como o Sistema A e Sistema B implementam ambos as PAEs do Suplicante e Autenticador, para a porta controlada pelo Sistema se tornar autorizada, os estados de máquina do Suplicante e do Autenticador associados com esta porta devem estar ambos no estado autorizado.

No geral, a configuração mostrada na Figura 11 é destinada aonde não existe uma atribuição óbvia dos papéis de Autenticador e Suplicante (por exemplo, uma rede par a par IEEE 802.11) ou onde ambos sistemas desejam fazer uso de seu próprio Servidor de Autenticação para fazer controle de acesso a seus dispositivos.

4.1.5 Controle de recepção e transmissão

A medida a qual as trocas de protocolos que tomam lugar na porta com controle são afetadas pelo estado de autorização é determinada por dois parâmetros *controlled direc-*

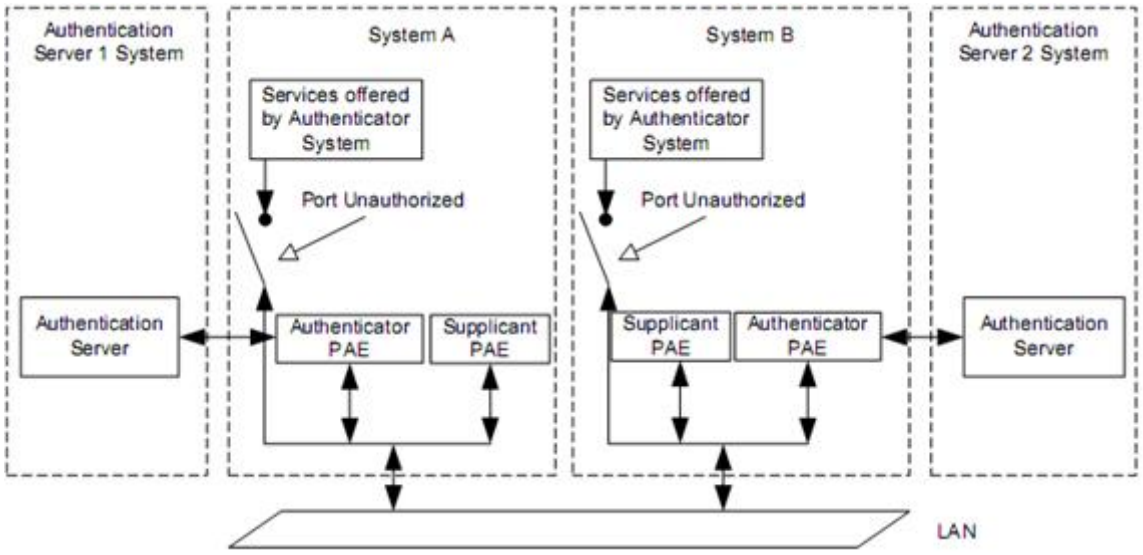

Figura 11: Sistemas adotando ambos papéis de Autenticador e Suplicante

tions associados com cada porta com controle: um parâmetro *AdminControlledDirections* e um parâmetro *OperationalControlledDirections*. Estes parâmetros determinam quando uma porta com controle que é não autorizada exerce controle sobre uma comunicação nas duas direções (desabilitando a recepção de quadros entrantes e a transmissão de quadros na saída), ou apenas na direção de entrada (desabilitando apenas a recepção de quadros entrantes). Os parâmetros *controlled directions* podem assumir um dos dois possíveis valores, *Both* e *In*. A relação entre estes dois parâmetros, e o significado de seus valores, é:

- ***AdminControlledDirections = Both***. Isto indica que é necessário exercer controle sobre ambos os tráfegos de entrada e saída através da porta com controle. O valor de *OperControlledDirections* é configurado incondicionalmente como *Both* se *AdminControlledDirections* estiver configurado como *Both*.

- ***AdminControlledDirections = In***. Isto indica que é necessário exercer controle apanas sobre o tráfego de entrada através da porta com controle. Se *AdminControlledDirections* é configurado como *In*, o valor de *OperControlledDirections* é configurado como *In* na inicialização e quando o MAC da porta se torna operável. No entanto, o valor de *OperControlledDirections* é configurado como *Both* se qualquer das seguintes condições for verdadeira:

  1. A porta é uma porta de *Bridge*, e o estado de máquina de Detecção de *Bridge* (ver Artigo 17 da IEEE Std 802.1D) detecta a presença de outra *Bridge* conectada a porta.

2. A porta é uma porta de *Bridge*, e o parâmetro *Edge Port* da porta é FALSO.
3. O MAC da porta se torna inoperante.

O valor do parâmetro *AdminControlledDirections* pode apenas ser modificado por gerência. Implementações de controle de acesso baseado em porta devem suportar a habilidade de configurar independentemente o parâmetro *AdminControlledDirections* de cada porta com controle para o valor *Both*. Implementações de controle de acesso baseado em porta podem suportar a habilidade de configurar independentemente o parâmetro *AdminControlledDirections* de cada porta com controle para o valor *In*.

4.1.6 Port Access Entity (PAE)

A *Port Access Entity* (PAE) opera os algoritmos e protocolos associados com o *Port Acess Control Protocol* definido no capítulo 4.2. A PAE existe para cada porta de um Sistema que suporta as funcionalidades do *Port Access Control* no papel de Suplicante, Auntenticador, ou ambos.

No papel de Suplicante, a PAE é responsável por prover informação a um Autenticador que irá estabelecer suas credenciais. A PAE que realiza o papel de Suplicante em uma troca de autenticação é conhecida como PAE Suplicante.

No papel de Autenticador, a PAE é responsável pela comunicação com a Suplicante, e por submeter a informação recebida de uma Suplicante para um Servidor de Autenticação para realizar a checagem das suas credenciais para seu estado de autorização ser definido em conseqüência disto. Uma PAE que realizar o papel de Autenticador em uma troca de autenticação é conhecida como PAE Autenticadora.

Ambos os papéis PAE controlam o estado de autorização da porta com controle (ver 4.1.4) dependendo do resultado do processo de autenticação. Se uma determinada porta com controle possui ambas as funcionalidades de PAE Suplicante e PAE Autenticadora associadas a ela, ambas as PAEs devem estar no estado autorizado para que a porta com controle se torne autorizada.

4.1.6.1 Papel do Autenticador

Uma PAE Autenticadora é responsável por forçar a autenticação de uma PAE Suplicante que se conecta a sua porta com controle e por controlar o estado de autorização da porta devidamente.

Para realizar a autenticação, a PAE Autenticadora faz uso de um Servidor de Autenticação. O Servidor de Autenticação pode ser co-alocado no mesmo Sistema que a PAE Autenticadora, ou pode ser localizada em outro lugar, sendo acessível via mecanismos de comunicação remota, baseados em LAN ou de outra forma.

4.1.6.2 Papel do Suplicante

A PAE Suplicante é responsável por enviar as credenciais da Suplicante à PAE Autenticadora em resposta aos pedidos da PAE Autenticadora, e de controlar o estado de autorização da porta com controle de acordo com o resultado da troca de autenticação enviada a ele pela PAE Autenticadora. A PAE Suplicante também pode iniciar trocas de autenticação e realizar trocas explícitas de *logoff*, como descrito adiante em 4.1.6.4.

4.1.6.3 Restrições de acesso a porta

A autenticação ocorre primariamente na inicialização de um Sistema, ou quando o Sistema Suplicante é conectado a uma porta do Sistema Autenticador. Até a autenticação ser concluída com sucesso, o Sistema Suplicante possui acesso ao Sistema Autenticador apenas para realizar trocas de autenticação, ou acesso a qualquer serviço de dispositivos oferecidos pelo Sistema Autenticador que não estão sujeitos a restrições de controle de acesso. Assim que a autenticação for finalizada com sucesso, ambos os Sistemas podem permitir acesso completo pelo Sistema Suplicante aos serviços oferecidos via porta com controle do Sistema Autenticador.

O estado operacional do MAC que suporta uma porta com controle pode ser habilitado ou desabilitado. Se o estado operacional do MAC é desabilitado, então o MAC não está disponível para uso, independente do estado de autorização associado à porta com controle.

Em um sistema que implementa uma PAE, a porta com controle é colocada no estado não autorizado até que a autenticação tome lugar, e é portanto desabilitada. Assim que a autenticação obtiver sucesso, e for determinado que o usuário autenticado é autorizado a acessar a porta com controle, a porta é colocada em estado autorizado; assumindo que não há outra razão para permanecer desabilitada (ex., o MAC foi desabilitado por motivos administrativos), a porta com controle está então disponível para uso.

A operação da PAE pode suportar um tempo de vida para o estado de autorização das portas com controle, e pode requisitar que a Suplicante autentique novamente a qual-

quer momento. Portas com controle permanecem autorizadas durante a reautenticação e mudam para o estado não autorizado apelas se o processo de reautenticação falhar.

A autenticação é configurada baseada em portas, pois é desejável em algumas configurações que certas portas não passem pelo processo de autenticação (ex., em portas ligando *Bridges* ou portas ligadas a servidores).

4.1.6.4 Mecanismos de logoff

Existem diversos mecanismos que podem resultar no estado da porta com controle mudar para não autorizado e portando controlando o acesso via esta porta de acordo com o parâmetro *OperControlledDirections* (ver 4.1.5):

- As trocas de autenticação entre a Suplicante e o Servidor de Autenticação podem resultar em falha ao autorizar a porta.
- Controles de gerencia podem prevenir que a porta seja autorizada, independente das credenciais do Suplicante.
- O MAC associado com a porta pode estar não operacional por qualquer motivo (incluindo falha de *hardware* ou questões de gerência).
- Falha de conexão entre a Suplicante e Autenticador podem fazer com que o Autenticador exceda o tempo limite de espera o estado de autenticação.
- Expiração do tempo de reautenticação pode ocorrer na falta de uma reautorização com sucesso.
- A PAE Suplicante falha em responder um pedido de informação de autenticação pelo PAE Autenticador.
- A PAE Suplicante pode realizar um pedido explícito de *logoff*.

Quando um usuário desconecta de uma estação final, é possível em alguns ambientes que o usuário (ou outro usuário) contorne uma nova requisição de *login* e, portanto ganhe acesso a estação final e a rede. Prover um mecanismo de *logoff* explícito garante que a sessão foi encerrada, não apenas a respeito do acesso do usuário a estação final, mas também em relação ao estado da estação final com a porta com controle do Sistema Autenticador a qual está conectada. Um *logoff* explícito portanto, causa que ambas as PAEs Suplicantes e Autenticadora configurem suas portas com controle para o estado não autorizado.

4.2 Port Access Control Protocol

4.2.1 Visão geral

A operação do processo de autenticação faz uso do *Extensible Authentication Protocol* (EAP, especificado na IETF RFC 3748) como meio de comunicação da informação de autenticação entre a Suplicante e o Servidor de Autenticação. O EAP é um protocolo genérico que suporta múltiplos mecanismos de autenticação. Por exemplo, através do uso do EAP, o suporte a um número de esquemas de autenticação podem ser adicionados, incluindo *smart cards*, *Kerberos*, Criptografia de Chave Pública, *One Time Passwords*, e outros.

A abordagem feita por este padrão é definir um formato de encapsulamento que permita que as Mensagens EAP possam ser carregadas diretamente pelo Serviço MAC da LAN. A forma encapsulada do EAP, conhecida como EAP *over* LANs, ou EAPOL, é usada para todas as comunicações entre a PAE Suplicante e a PAE Autenticadora.

Cada PAE possui duas componentes separadas, um conjunto de estados de máquina PACP, uma camada de alto nível com as quais estas máquinas se comunicam. No caso da PAE Suplicante, a camada de alto nível consiste da funcionalidade EAP, enquanto no caso da PAE Autenticadora, a camada de alto nível é uma combinação do EAP e funcionalidade do *authentication, authorization, and accounting* (AAA).

A Figura 12 mostra a interface entre os estados de máquina PACP e a camada de alto nível para a PAE Suplicante e PAE Autenticadora. Como mostrado, o sinal *portEnabled* do sistema indica que ambas a camada de alto nível e o PACP nesta porta estão ativos. O PACP passa mensagens EAP entre a porta física e camada de alto nível. O tráfego de mensagens na Suplicante é controlado usando o *eapResp/eapNoResp* do EAP para indicar se está pronto para uma outra mensagem, e um *eapReq* do PACP para indicar que uma mensagem esta disponível para que o EAP processe. O tráfego de mensagens no lado do Autenticador é controlado com um processo similar, com a camada de alto nível usando *eapReq/eapNoReq* para indicar quando está pronto para receber uma nova mensagem, e o *eapResp* para indicar que a mensagem está disponível para que a camada de alto nível processe.

Na camada de alto nível, o EAP e métodos EAP associados realizam o diálogo de autenticação, mas para completar, a camada de alto nível irá receber uma interpretação do AAA para sinalizar sucesso ou falha ao PACP, usando os sinais *eapSuccess* e *eapFail*.

O método EAP no Autenticador encaminha as mensagens EAP para frente e para trás, ao Servidor de Autenticação, utilizando o protocolo AAA como transporte. A camada de alto nível coordena as componentes EAP e AAA. O RADIUS é um protocolo de transporte que pode ser utilizado como uma camada de baixo nível para este mecanismo de encaminhamento.

Ao invés de apenas permitir um método de autenticação pré-determinado, o EAP permite que a PAE Autenticadora requisite mais informação antes de determinar o mecanismo de autenticação específico. No EAP, a PAE Autenticadora envia uma ou mais requisições para autenticar a PAE Suplicante. A requisição possui um campo de tipo para determinar o que está sendo requisitado. Tipicamente, o Autenticador irá enviar uma requisição inicial de Identidade, seguida de uma ou mais requisições de informação de autenticação. No entanto, uma requisição inicial de Identidade não é necessária, e poderá ser ignorada em casos nos quais a identidade é presumida ou pode ser determinada por outros meios (como um método especifico para troca de identidade). A PAE Suplicante envia um pacote de resposta a cada requisição. Como no pacote de requisição, o pacote de resposta possui um campo de tipo correspondente ao campo de tipo da requisição.

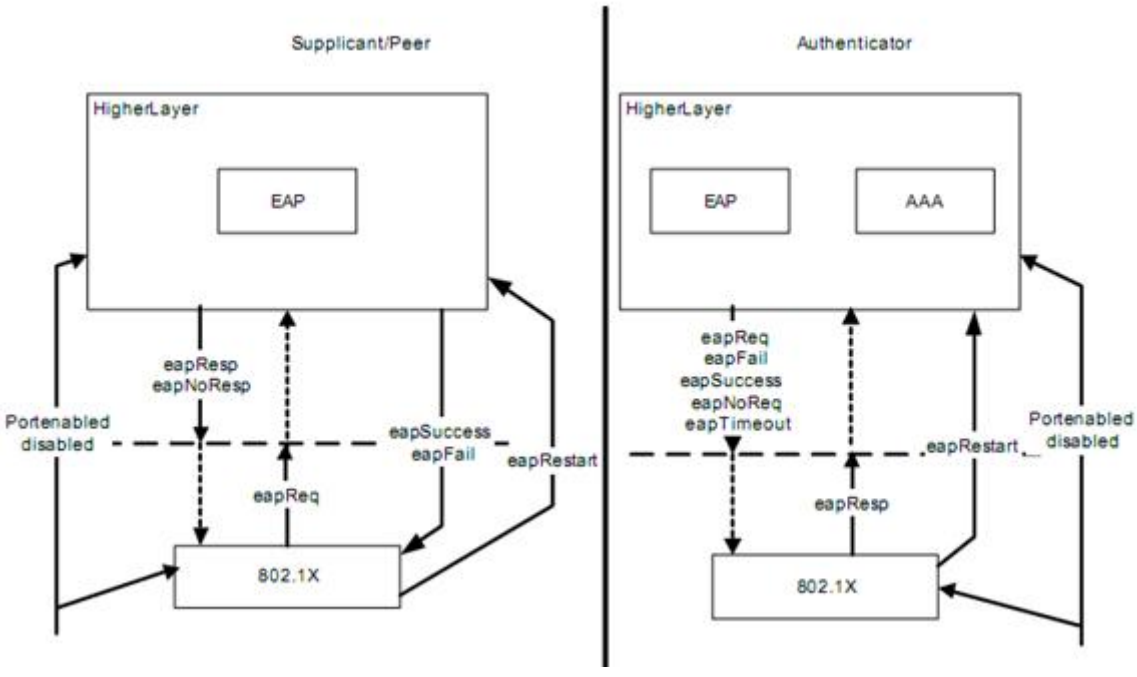

Figura 12: Diagrama de interface da camada de alto nível

A troca de autenticação finaliza com uma indicação de *Accept* ou *Reject* do Servidor de Autenticação. O Autenticador encaminha o pacote EAP com a indicação de *Accept* ou *Reject*, enquanto o cliente AAA operando como uma camada abaixo do EAP interpreta a indicação e indica sucesso ou falha ao Autenticador, que irá configurar a porta com

controle para autorizada ou não autorizada adequadamente.

4.2.2 Inicio da autenticação

A autenticação pode ser iniciada tanto pela PAE Suplicante quanto pela PAE Autenticadora. Se a autenticação é habilitada em uma determinada porta, a autenticação é iniciada pela PAE Autenticadora ao perceber que o estado operacional do MAC associado a porta foi alterado de desabilitado para habilitado.

A PAE Suplicante pode iniciar uma seqüência de autenticação enviando um quadro *EAPOL-Start* (ver 7.5.4 da IEEE Std 802.1X).

4.2.3 EAPOL-*Logoff*

Quando a Suplicante deseja que a PAE Autenticadora realize um *logoff* (ou seja, configurar o estado a porta para não autorizada), a PAE suplicante uma mensagem *EAPOL-Logoff* (ver 7.5.4 da IEEE Std 802.1X) para a PAE Autenticadora. Como resultado, a PAE Autenticadora muda imediatamente o estado da porta com controle para não autorizado.

4.2.4 Retransmissão

A PAE Autenticadora é responsável pela retransmissão de mensagens entre ela e a PAE Suplicante. Em particular, o EAP é a componente da PAE Autenticadora que lida com a retransmissão, não os estados de máquina IEEE 802.1X. Então, se um pacote EAP é perdido em transito entre a PAE Suplicante e PAE Autenticadora (ou vice versa), a PAE Autenticadora irá retransmitir. As exceções são as mensagens *EAPOL-Start*, que são retransmitidas se necessário pela PAE Suplicante, e qualquer mensagem EAP entregue durante os estados FAIL e SUCCESS.

Em implementações aonde a função de autenticação é realizada por um Servidor de Autenticação remoto, podem ser necessárias retransmissões entre a PAE Autenticadora e o Servidor de Autenticação. Neste caso, pode ser necessário que a camada de alto nível adote uma estratégia de retransmissão que seja mais apropriada as características de transmissão do caminho de comunicação envolvido.

4.2.5 Retransmitindo quadros EAP

A PAE Autenticadora é responsável por retransmitir quadros EAP entre a Suplicante e o Servidor de Autenticação via camada de alto nível. Deve também realizar qualquer alteração dos quadros EAP que sejam necessárias para converter quadros EAP transportados como EAPOL entre a PAE Suplicante e PAE Autenticadora. É responsabilidade da camada de alto nível realizar qualquer alteração necessária nos quadros EAP entre o Autenticador e o Servidor de Autenticação. Para realizar a função de retransmissão, a informação contida nos quadros EAP não deve ser modificada além do necessário para converter o formato de quadro para/do formato EAPOL.

4.2.6 Exemplos de trocas EAP

Nestes exemplos, a troca de quadros EAPOL é mostrada como uma linha contínua; a troca de quadros transportados em uma camada de alto nível como o RADIUS é mostrada como uma linha pontilhada. Os diagramas mostram quais trocas de PDU envolvem a PAE Autenticadora modificando quadros EAP para poder realizar a tradução de protocolo.

O exemplo na Figura 13 mostra a conversação do Autenticador iniciado no caso de uma autenticação *One Time Password* (OTP). O OTP é utilizado por motivos ilustrativos; outros protocolos de autenticação poderiam ser utilizados, apesar de poderem mostrar certa diferença de comportamento.

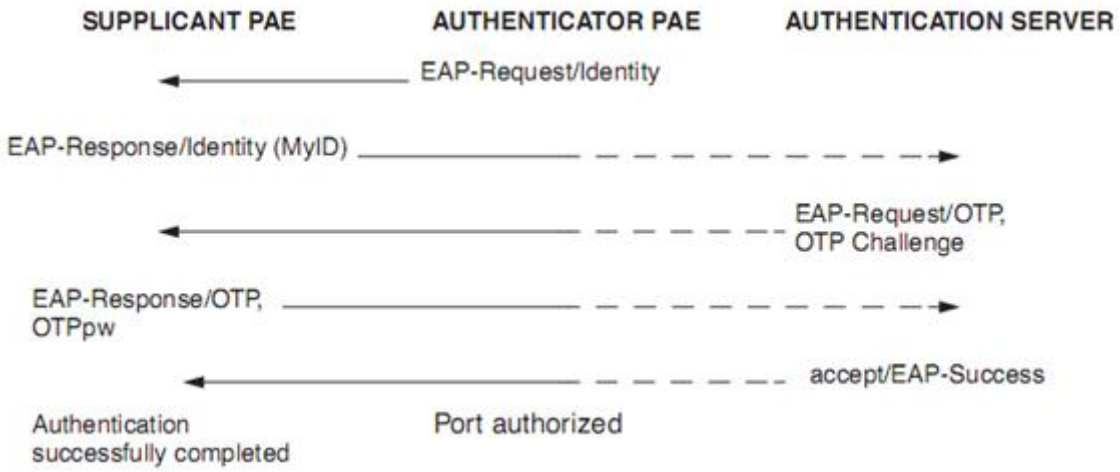

Figura 13: Autenticador iniciado, troca OTP (sucesso)

Caso a Suplicante falhe a autenticação EAP, a conversação iria parecer como ilustrado na Figura 14.

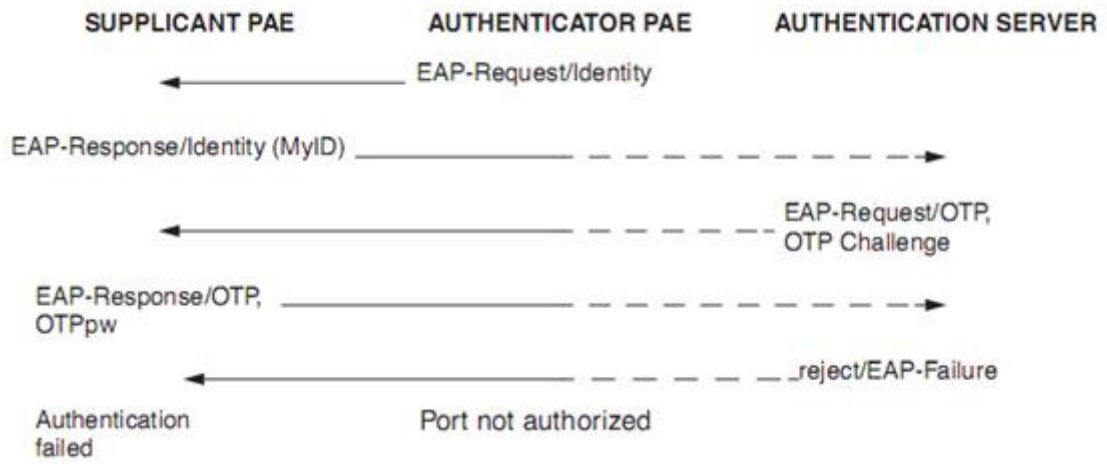

Figura 14: Autenticador iniciado, troca OTP (falha)

A Figura 15 ilustra uma troca de autenticação com sucesso, seguida de um *logoff* explícito requisitado pela Suplicante.

Uma conversação de autenticação com Suplicante iniciado será ilustrada pela Figura 16.

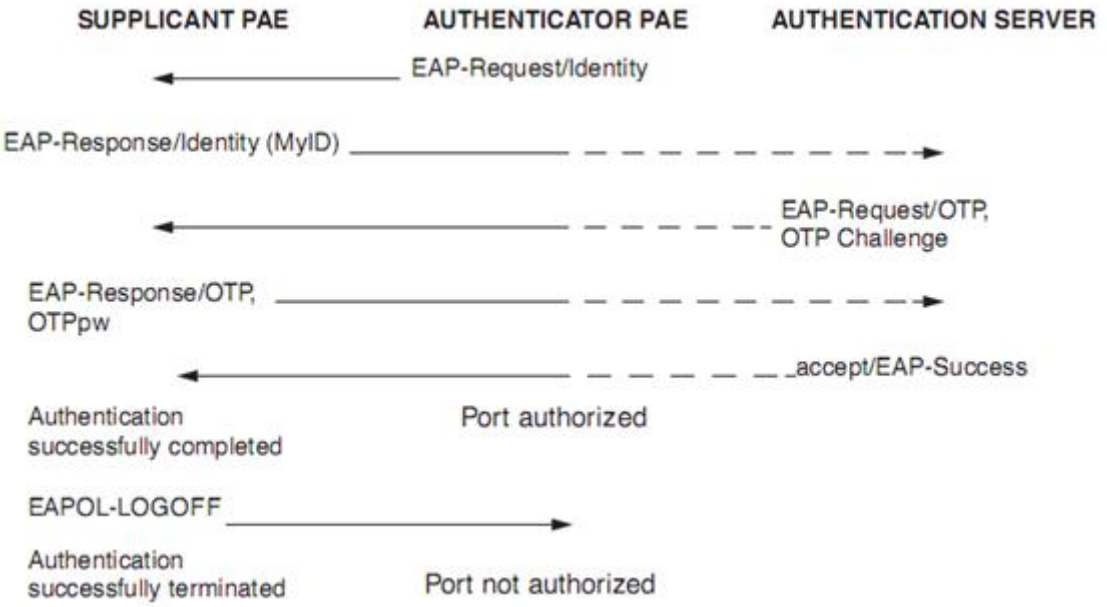

Figura 15: Autenticação com sucesso seguida de um logoff

No caso em que a Suplicante não suporte a autenticação, mas a autenticação é habilitada no Autenticador, a conversa vai parecer como a ilustrada na Figura 17.

No caso em que o Autenticador não suporte a autenticação, mas a autenticação é habilitada na Suplicante, a conversa vai parecer como a ilustrada na Figura 18.

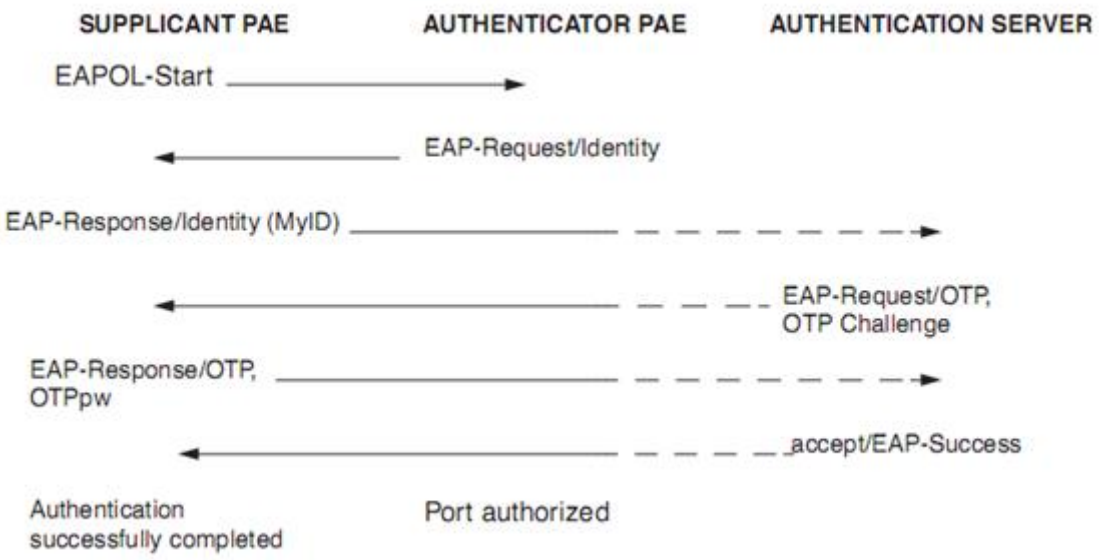

Figura 16: Suplicante iniciada, troca OTP (sucesso)

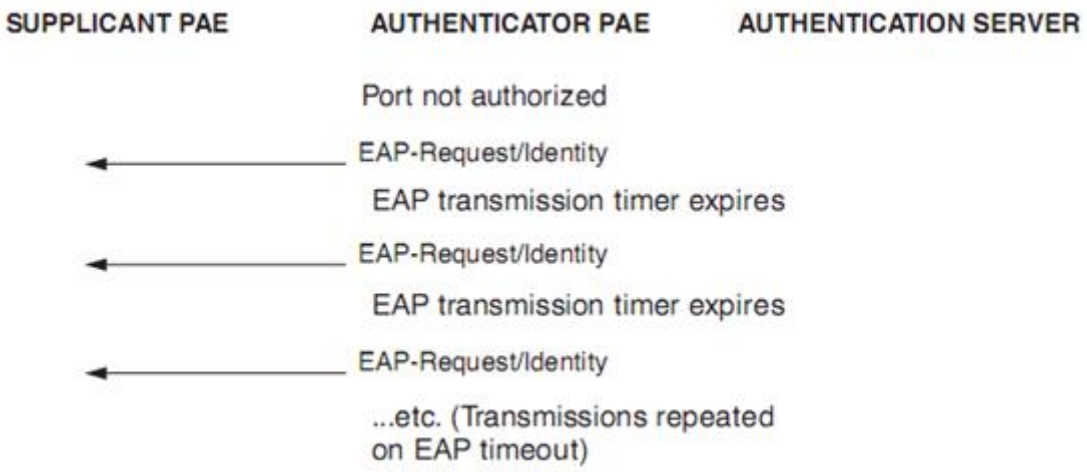

Figura 17: Suplicante não suporta a autenticação

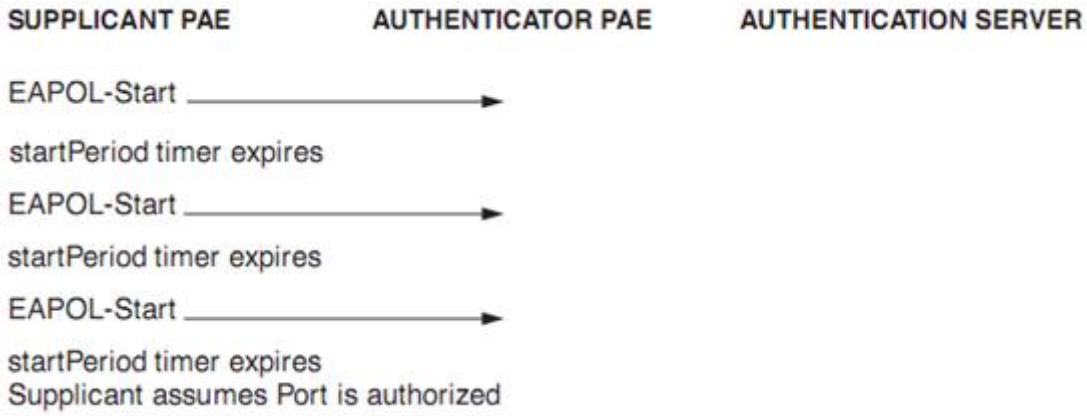

Figura 18: Autenticador não suporta a autenticação

4.2.7 Transmissão da informação de chave

O protocolo EAPOL suporta opcionalmente a transmissão da informação de chave doAutenticador para a Suplicante, ou da Suplicante para o Autenticador, seguido de uma troca de autenticação com sucesso, em circunstâncias nas quais a criptografia é disponível entre os sistemas Suplicante e Autenticador (ex., onde a encriptação é usada em uma associação IEEE 802.11 entre a estação e um *access point*).

O uso desta facilidade é controlado pelo parâmetro *keyTxEnabled*, que pode ser modificado por gerência. Um valor de *TRUE* permite que a informação de chave seja transmitida assim que *keyAvailable* e *keyRun* forem configurados como *TRUE*.

O *keyAvailable* pode ser configurado como *TRUE* por gerência, ou pela camada de alto nível durante a autenticação. A Figura 19 mostra a interface entre a camada de alto nível e a camada de chave IEEE 802.1X que suporta a transmissão da chave e sinaliza *keyAvailable*. No que se *keyTxEnabled* é *TRUE*, então o diálogo de autenticação EAP deve resultar na chave ser disponível tanto no Suplicante quanto no Autenticador para o processo ter sucesso, então os únicos métodos EAP que suportam este processo podem ser utilizados em ambientes aonde é esperado que o EAP provenha as chaves. O PACP também suporta a variável *portValid* que está disponível a camada de nível superior (isto não é utilizado por implementações existentes mas está disponível para futuras implementações). O *portValid* tem influência quando uma porta autenticada se torna autorizada. Isto permite que o PACP exija duas condições antes de autorizar uma porta: *Authenticated* e *data channel secure* (ou seja, criptografada).

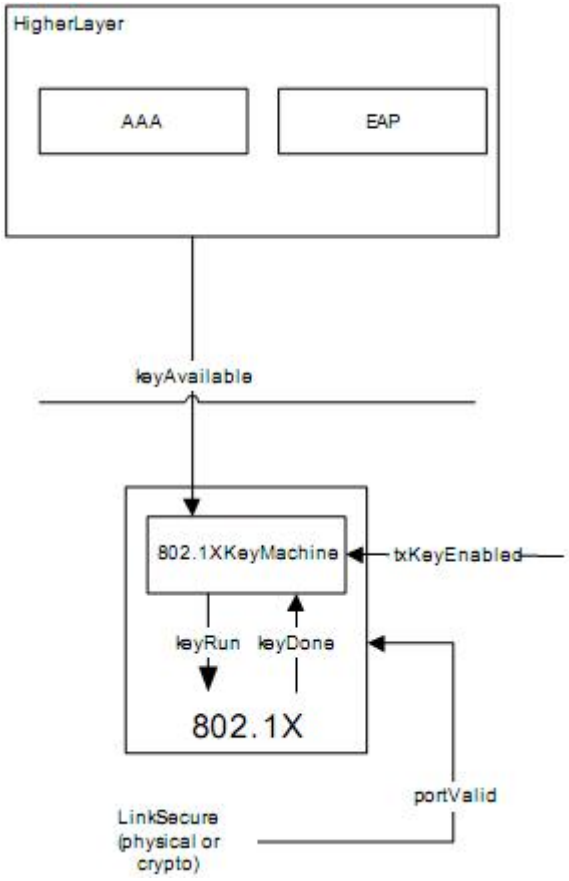

Figura 19: Interface entre camada de alto nível e Máquina de Chave

5 *Realização de cenários envolvendo VLANs e sugestões de implantação no IFSC*

Neste capítulo serão apresentados alguns cenários práticos idealizados para ilustrar o funcionamento das VLANs. Eles buscam mostrar alguns conceitos importantes, como interfaces de acesso e interface *trunking*, roteamento entre VLANs distintas, atribuição dinâmica de faixa de endereçamento IP para as VLANs através de um servidor DHCP, atribuição de VLANs baseado na autenticação do usuário na rede. Por fim serão apresentadas duas sugestões para a implantação do serviço de VLAN no IFSC.

5.1 Configuração de VLANs em estações

A Figura 20 ilustra uma configuração simples realizada. O objetivo deste cenário é a configuração de VLANs entre estações finais pertencentes a mesma rede, com a configuração de VLANs feita somente nas estações. O *switch* contém apenas a VLAN padrão configurada. Nesta configuração, o terminal A possui ligação com as VLANs 10 e 20, enquanto o terminal B possui ligação com a VLAN 10 e o terminal C com a VLAN 20.

Para realizar os testes de conectividade, usa-se o comando *ping* apenas as interfaces lógicas das estações, pois fisicamente elas são capazes de comunicar-se sem problemas por estarem na mesma rede. A estação A possui ambas interfaces de VLAN configuradas, logo ela poderá enviar e receber quadros de B e C. As estações B e C por sua vez, poderão comunicar-se apenas com A. Se B e C tentarem comunicar-se entre si, eles irão receber uma mensagem de erro declarando que o destino não é acessível.

No experimento percebe-se que todos os quadros enviados e recebidos possuem o rótulo VLAN, quadros sem estes rótulos seriam descartados no destino. Como o switch possui uma configuração passiva neste cenário, ele apenas retransmite os quadros como

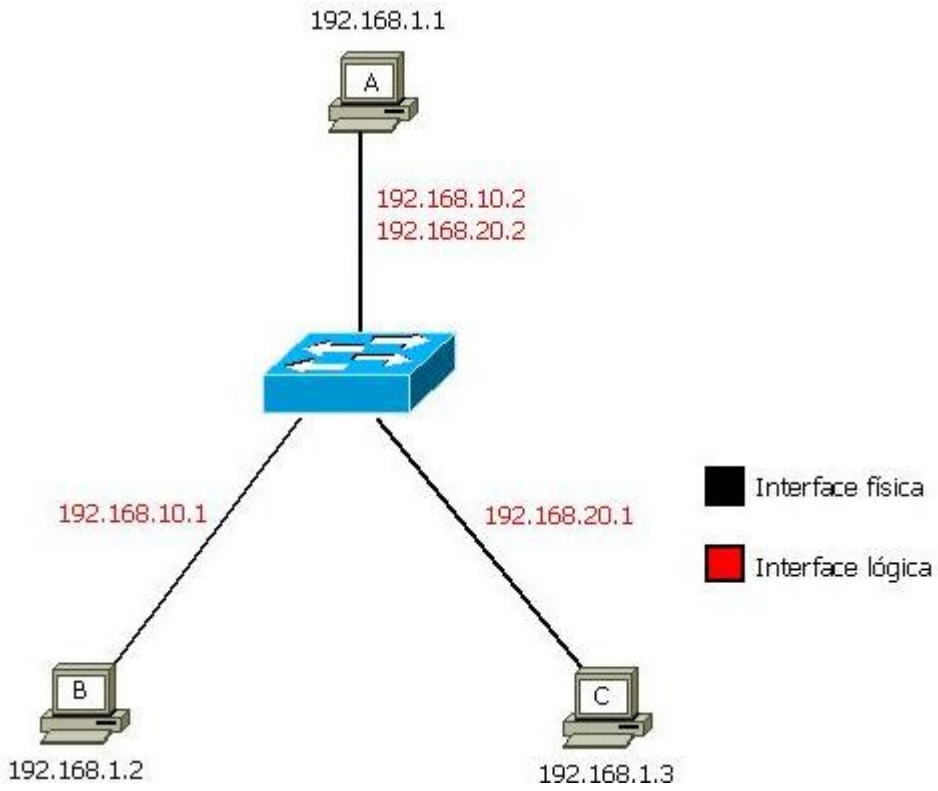

Figura 20: Configuração de VLANs apenas nos terminais

ele recebeu, neste caso com o rótulo. No caso de receber um quadro sem rótulo, o *switch* irá retransmiti-lo sem rótulo.

Uma descrição da configuração de interfaces no Linux pode ser vista no Anexo A.

5.2 Interfaces trunking em VLANs

A Figura 21 ilustra a configuração das VLANs no *switch* e a aplicação do conceito de interfaces de acesso e interface *trunking*. Foram criadas no *switch* as VLANS 10 e 20. Considera-se que a estação A está ligada a porta 1 do *switch*, a estação B ligada a porta 2 e a estação C ligada a porta 3.

Todos os quadros enviados e recebidos pelas estações A e B possuem rótulo de VLAN, isto caracteriza a interface que as liga com o *switch* como interface *trunking*. Para esta configuração é necessário que exista a configuração das VLANs tanto no *switch* como nos terminais, se o terminal não possuir a configuração de VLAN ele irá descartar os quadros que ele receber com o rótulo. As portas do *switch* devem estar configuradas para retransmitir os quadros com o rótulo neste tipo de interface.

Todos os quadros enviados e recebidos pela estação C não possuem rótulo de VLAN,

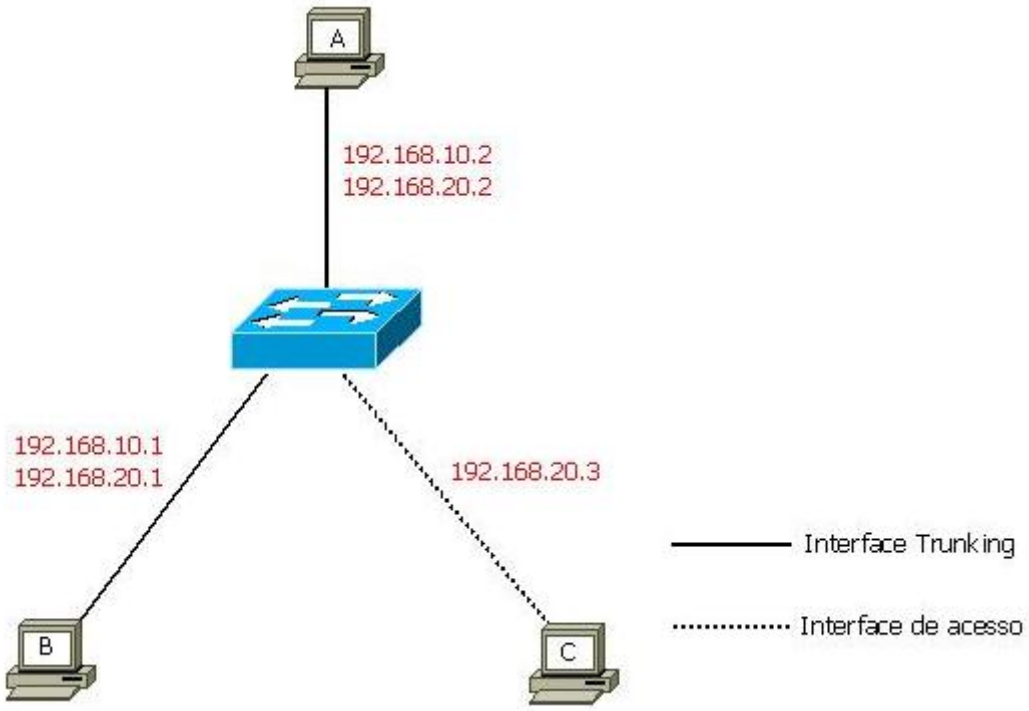

Figura 21: Interfaces *trunking* e de acesso

isto caracteriza a interface que a liga com o *switch* como interface de acesso. Nesta configuração, não é necessário aplicar qualquer configuração de interface lógica no terminal, ele irá receber normalmente os quadros destinados a sua VLAN diretamente na sua interface física. A existência da VLAN é transparente a este usuário. Cabe ao *switch* a tarefa de inserir o rótulo de VLAN nos quadros que ele receber de uma interface de acesso e retransmitir para as outras portas da VLAN correspondente, e também a tarefa de receber os quadros destinados a esta VLAN (originados de outros terminais) e remover o rótulo VLAN antes de retransmiti-los a outras interfaces de acesso.

Uma descrição da configuração do *switch* DLINK DES-3526 pode ser vista no Anexo B.

5.3 Roteamento e DHCP em VLANs

A Figura 22 ilustra o roteamento entre diferentes VLANs e também a distribuição dinâmica de endereços IP para as estações de uma VLAN. Foram criadas nos *switchs* as VLANs 10, 20 e 30. As interfaces ligando o *switch* com o roteador e servidor DHCP devem ser de *trunking*, enquanto as interfaces entre o *switch* e os terminais devem ser de acesso.

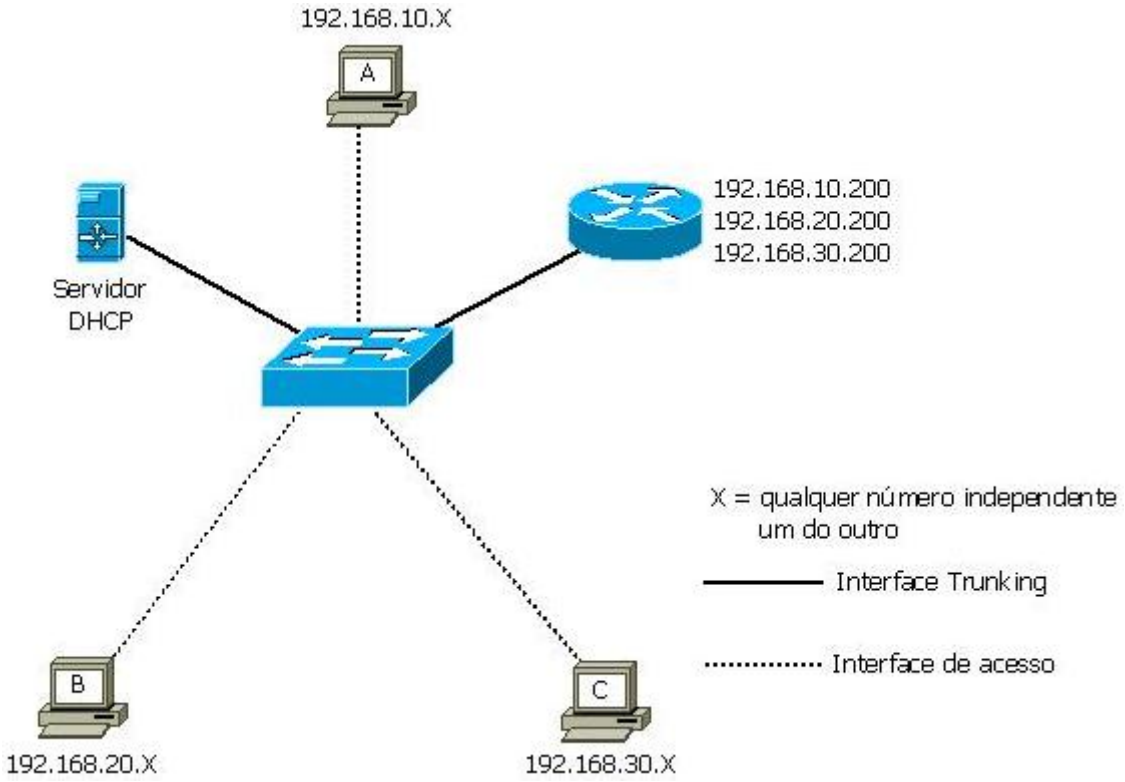

Figura 22: Roteamento entre VLANs e servidor DHCP

Os terminais A, B e C, devem requisitar um endereço IP ao servidor DHCP, que irá atribuir uma faixa diferente de endereços para cada VLAN, como ele possui interface *trunking* com o *switch*, ele irá identificar qual interface requisitou o endereço e fazer uma oferta com base nesta informação.

A função do roteador é permitir a comunicação entre as diferentes VLANs. Sua interface com o *switch* deve fazer parte de todas as VLANs as quais se deseja que ele forneça o serviço de roteamento. O roteador pode ser substituído nesta configuração por um terminal Linux, habilitado para rotear os quadros recebidos. Também será necessário configurar as interfaces de cada VLAN no roteador. No lado dos clientes, deverão ser configuradas as rotas de acesso as outras VLANs. No caso do terminal A, ele deve possuir uma configuração de rota, dizendo que os pacotes a serem transmitidos para B e C devem ser encaminhados para 192.168.30.200 (ou seja, o endereço do roteador padrão).

No caso de um terminal Linux fazendo a função de roteador, o servidor DHCP pode estar alocado no mesmo terminal.

Uma descrição da configuração do servidor DHCP pode ser vista no Anexo C. A configuração de um terminal Linux como roteador pode ser vista no Anexo A.

5.4 Autenticação e VLANs

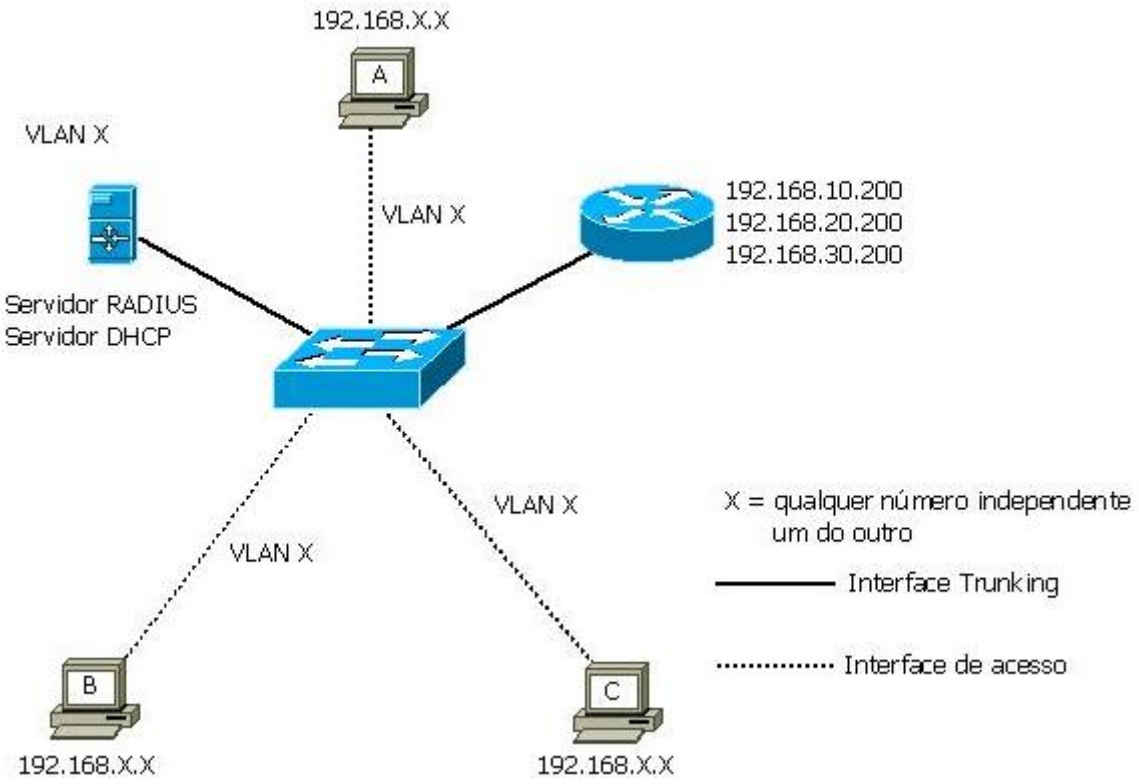

Figura 23: Atribuição de VLANs baseado em autenticação de usuário

A figura 23 ilustra o funcionamento de VLANs baseadas em autenticação, usando um servidor RADIUS como base de dados de autenticação.

Todas as VLANs são criadas no *switch*, sem se atribuir nenhuma porta a elas inicialmente. É criada uma *guest* VLAN, a qual todas as portas de usuário estão ligadas inicialmente. Os terminais ligados a esta *guest* VLAN não terão acesso aos recursos de rede, ela funciona como uma porta de controle, como descrito pelo padrão IEEE 802.1X, e apenas permite troca de mensagens entre PAE suplicante e PAE autenticador(podendo também ser o servidor de autenticação).

Um terminal se conecta na rede, ganha acesso a *guest* VLAN, após isso ela será requisitada um login e senha. Caso o processo de autenticação seja um sucesso, o servidor RADIUS(atuando como servidor de autenticação) irá alterar a configuração da porta do *switch* em questão, e ela fará parte da VLAN que diz respeito ao usuário ou processo autenticado. Em caso de falha de autenticação, o usuário ou processo permanece conectado apenas na *guest* VLAN, sem recursos de rede.

Após o processo de autenticação ter sucesso, o terminal poderá fazer uma requisição de endereço ao servidor DHCP e receber um endereço dentro da VLAN que faz parte.

5.5 Sugestões de uso de VLANs no IFSC

O campus SJ do IFSC, hoje, não usa VLANs em sua estrutura de rede. Existe hoje a necessidade da implantação de VLANs neste ambiente, por questões organizacionais e de segurança. Com base nisto, foi decidido sugerir dois perfis de implantação do serviço no campus SJ do IFSC, cada um atendendo diferentes necessidades. Estes perfis serão mostrados a seguir.

5.5.1 Primeiro perfil

Todas VLANs sofrerão autenticação pelo servidor RADIUS, exceto as citadas. Neste caso, todos os usuários se conectarão em suas respectivas VLANs, independente do local de acesso. IPs fornecidos por DHCP (exceto as citadas como estáticas). Este perfil permite um controle melhor dos usuários e suas ações, e garante maior dinamicidade no acesso a rede.

VLAN 10: Servidores (estática) (sem RADIUS) (alta prioridade)

VLAN 20: VLAN com a RNP (estática) (sem RADIUS) (alta prioridade)

VLAN 90: VLAN geral de alunos (acesso a WEB e rede local) (baixa prioridade)

VLAN 100: VLAN geral de visitantes (apenas acesso WEB) (baixa prioridade)

VLAN 110: VLAN geral de funcionários (acesso a WEB) (rede local, prioridade normal)

VLAN 120: VLAN de administração (alta prioridade)

VLANs 31-50: Reservadas para coordenadorias e setores administrativos (mesmo perfil da VLAN de funcionários)

VLANs 60-80: Reservadas para laboratórios que requerem IPs estáticos. Para os laboratórios utilizados em aulas práticas, que possuem terminais Linux onde não há autenticação com o servidor.

5.5.2 Segundo perfil

Apenas alguns locais do Campus sofrem autenticação pelo servidor RADIUS. Enquanto o restante dos locais possui VLAN fixa e IPs estáticos. Este perfil garante os IPs estáticos para os setores administrativos do Campus, porém se perde a dinamicidade e o

controle de usuários.

VLAN 10: Servidores (alta prioridade).

VLAN 20: VLAN com a RNP (alta prioridade).

VLAN 90: VLAN de laboratórios de uso comum (RADIUS + IP estático) (acesso a WEB e rede local) (prioridade varia com perfil de usuário: aluno = baixa, funcionário = normal)

VLAN 100: VLAN de visitantes por wifi (RADIUS + DHCP) (acesso a WEB) (baixa prioridade)

VLAN 110: VLAN geral de funcionários (acesso a WEB e rede local) (prioridade normal)

VLAN 120: VLAN *wifi* para alunos (RADIUS + DHCP) (acesso a WEB e rede local) (prioridada baixa)

VLAN 130: VLAN *wifi* para funcionários (RADIUS + DHCP) (acesso a WEB e rede local) (prioridade normal)

VLANS 31-50: Reservadas para coordenadorias e setores administrativos (mesmo perfil da VLAN de funcionários)

VLANs 60-80: Reservadas para laboratórios. (perfil pode variar de acordo com necessidades do laboratório)

5.5.3 Diagrama dos perfis

A figura 24 mostra um diagrama representando os perfis sugeridos anteriormente, mostrando a disposição das faixas de IP com as VLANs em funcionamento. Este diagrama não leva em conta a localização física dos equipamentos.

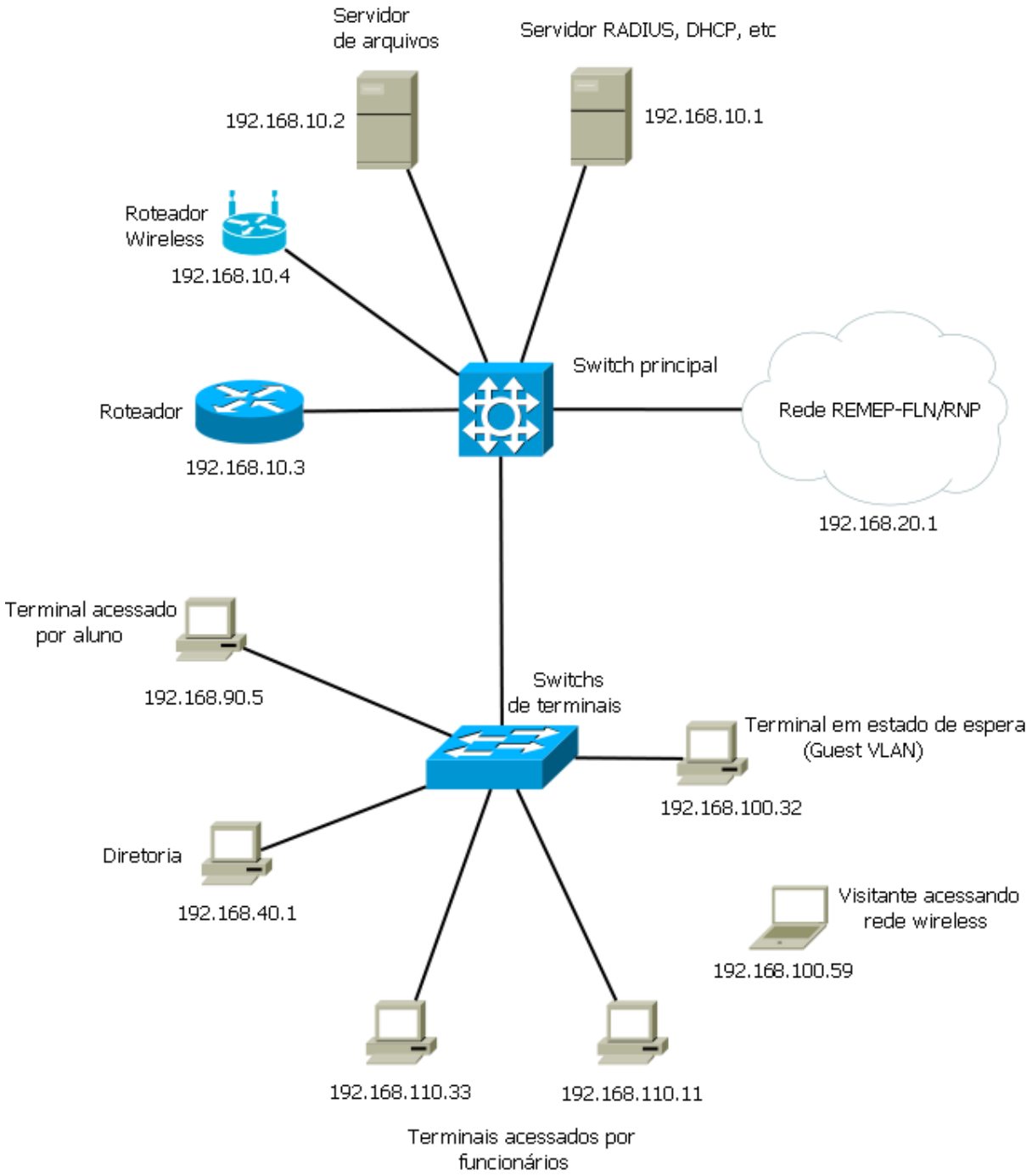

Figura 24: Diagrama de VLANs dos perfis sugeridos para o IFSC

6 Conclusões

Este trabalho teve como objetivo compreender o uso das VLANs, passar por cenários práticos de utilização e chegar a um cenário que poderia ser implantado no Campus SJ do IFSC, mas que pode ser adaptado à outras instituições.

Foram estudados os conceitos básicos para a compreensão de VLANs e diferenciação com as LANs, passando pelos padrões IEEE 802.1Q, que define as VLANs, e 802.1X com seu controle de acesso. Paralelamente ao estudo de VLANs foi estudado a autenticação de usuário e protocolos de rede como o DHCP e RADIUS, que, junto com VLANs, permitem a criação de redes locais com bom grau de segurança e autonomia da rede.

O serviço de VLAN juntamente com um servidor de autenticação RADIUS pode suprir diversas necessidades presentes hoje no ambiente do Campus SJ do IFSC. Se vê a necessidade de um maior controle de acesso dos usuários, principalmente por parte dos alunos, assim como a adoção de critérios de prioridade de serviços baseada no perfil dos usuários e serviços. Uma melhor organização lógica da rede, assim como deixa-la melhor preparada para futuras expansões e alterações na sua estrutura.

Com o barateamaneto de custos dos equipamentos que implementam VLANs, chega-se a conclusão que é desejável o uso de VLANs em qualquer ambiente de rede de médio a grande porte que tenha necessidade de uma segmentação, e o uso de um servidor RADIUS em conjunto pode criar inúmeras possibilidades de utilização. A tendência é que esta técnica seja cada vez mais difundida no ambiente de redes, e já é muito utilizada para diversas soluções.

6.1 Sugestões para trabalhos futuros

- Implantação do serviço de VLAN no IFSC;
- Estudo de VLANs aplicadas a redes sem fio e VoIP;

ANEXO A – Algumas configurações no Linux

O objetivo deste anexo é mostrar os comandos necessários para realizar os cenários descritos no Capítulo 5 deste trabalho.

A.1 Configuração de interfaces lógicas

Para adicionar uma interface lógica no Linux, utilizamos os seguintes comandos:

vconfig add eth0 10

ifconfig eth0.10 192.168.2.1/24 up

```
auto eth0
iface eth0 inet static
        address 192.168.1.12
        netmask 255.255.255.0
        gateway 192.168.1.254

auto vlan10
iface vlan10 inet static
        address 192.168.10.200
        netmask 255.255.255.0
        vlan-raw-device eth0

auto vlan20
iface vlan20 inet static
        address 192.168.20.200
        netmask 255.255.255.0
        vlan-raw-device eth0
```

Figura 25: Configuração de inferfaces lógicas

Existe também outra forma de configurar as interfaces lógicas que é através da configuração do arquivo /etc/network/interfaces. A figura 25 mostra um exemplo de configuração deste arquivo.

Após a configuração de interfaces no arquivo /etc/network/interfaces, é necessário que se reinicie o serviço de interfaces de rede do Linux através do comando:

```
/etc/init.d/networking restart
```

A.2 Configurando Linux como roteador

Para configurar um terminal Linux como roteador, podemos simplesmente usar o seguinte comando:

```
sysctl -w netipv4 ip-forward=1
```

ANEXO B – Configuração do switch DLINK DES-3526

Este anexo tem como objetivo mostrar como são feitas as configurações necessárias no switch DLINK DES-3526 para realizar os cenários mostrados no Capítulo 5.

B.1 Configuração de VLANs estáticas

Na interface WEB do switch DLINK, abrimos a pasta *configuration*, depois a pasta VLAN e selecionamos *Static VLAN Entry*, como mostra a Figura 26. Clicamos em *Add New 802.1Q VLAN*.

A seguir iremos encontrar a interface de configuração de uma nova VLAN, mostrada na Figura 27.

O significado dos campos da interface de configuração a seguir:

VID: O VLAN ID da VLAN a ser criada.

VLAN Name: O nome da VLAN a ser criada.

Advertisement: Habilitando esta função irá permitir que o *switch* envie pacotes GVRP as estações notificando que elas poderão entrar na VLAN existente.

Tag: Esta opção define se o rótulo VLAN será retransmitido pelo switch para esta porta.

None: Nenhuma configuração para esta porta em questão.

Egress: A porta faz parte da VLAN.

Forbidden: Especifica que a porta não faz parte da VLAN e está dinamicamente proibida de fazer parte da VLAN.

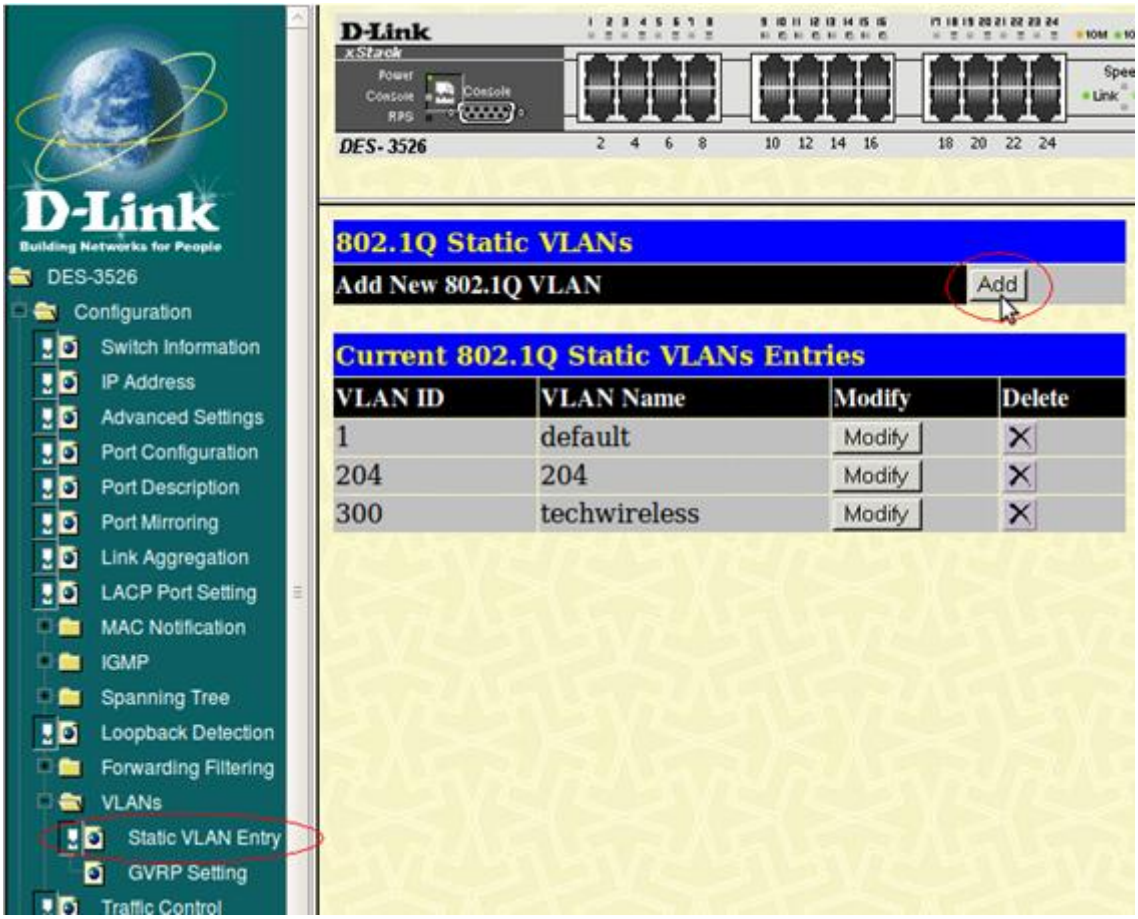

Figura 26: Adicionar VLAN estática

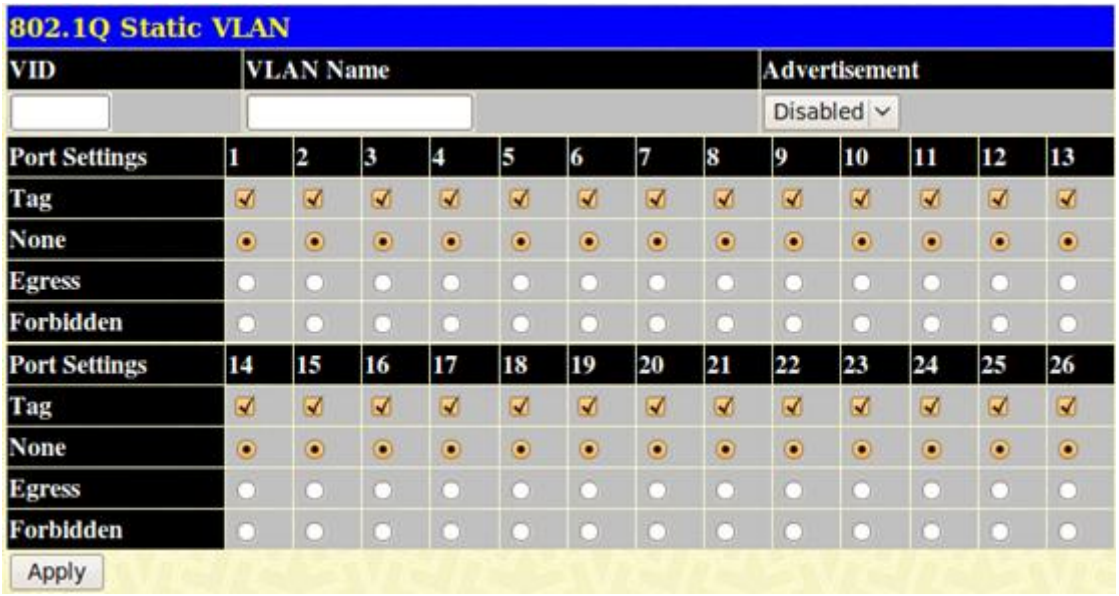

Figura 27: Interface de configuração de VLAN

Após todas configurações serem defidamente feitas, clica-se em *Apply* para confirmar a nova entrada de VLAN no *switch*.

B.2 Configuração de VLAN de visitante

Para o uso de autenticação através do RADIUS, é necessário a configuração de uma VLAN de visitantes no switch. A Figura 28 mostra como acessar a interface de configuração de VLAN de visitantes no *switch*.

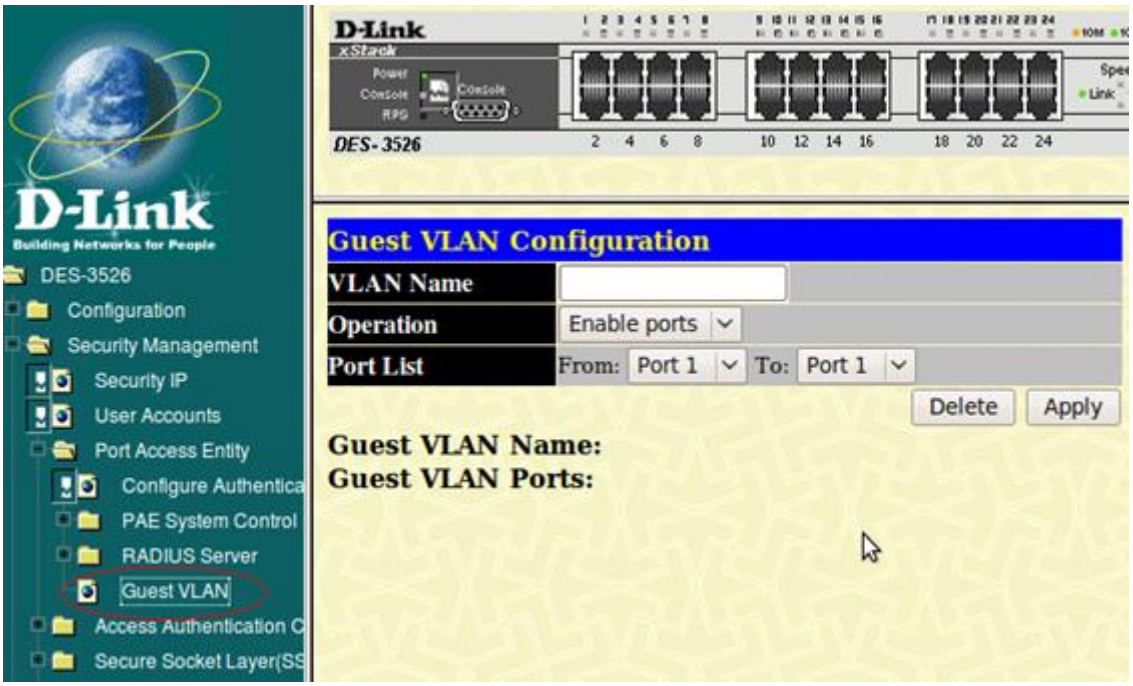

Figura 28: Interface de configuração de VLAN de visitantes

O significado dos campos da interface de configuração a seguir:

VLAN Name: Nome da VLAN que possui as portas que farão parte da VLAN de visitantes. Esta VLAN deve estar criada como visto em B.1, e todas as portas que se deseja incluir na VLAN de visitantes devem fazer parte somente desta VLAN.

Operation: Definir se irá habilitar ou desabilitar as portas na VLAN de visitantes.

Port List: Definir a faixa de portas que irão fazer parte da configuração.

Guest VLAN Name: Nome da atual VLAN de visitantes.

Guest VLAN Ports: Listagem das portas que fazem parte da atual VLAN de visitantes.

Após todas configurações serem defidamente feitas, clica-se em *Apply* para confirmar

a configuração da VLAN de visitantes no *switch*.

B.3 Configuração do RADIUS

O switch suporta a configuração de até três servidores de autenticação RADIUS. A Figura 29 mostra como ter acesso a interface de configuração do servidor RADIUS no switch.

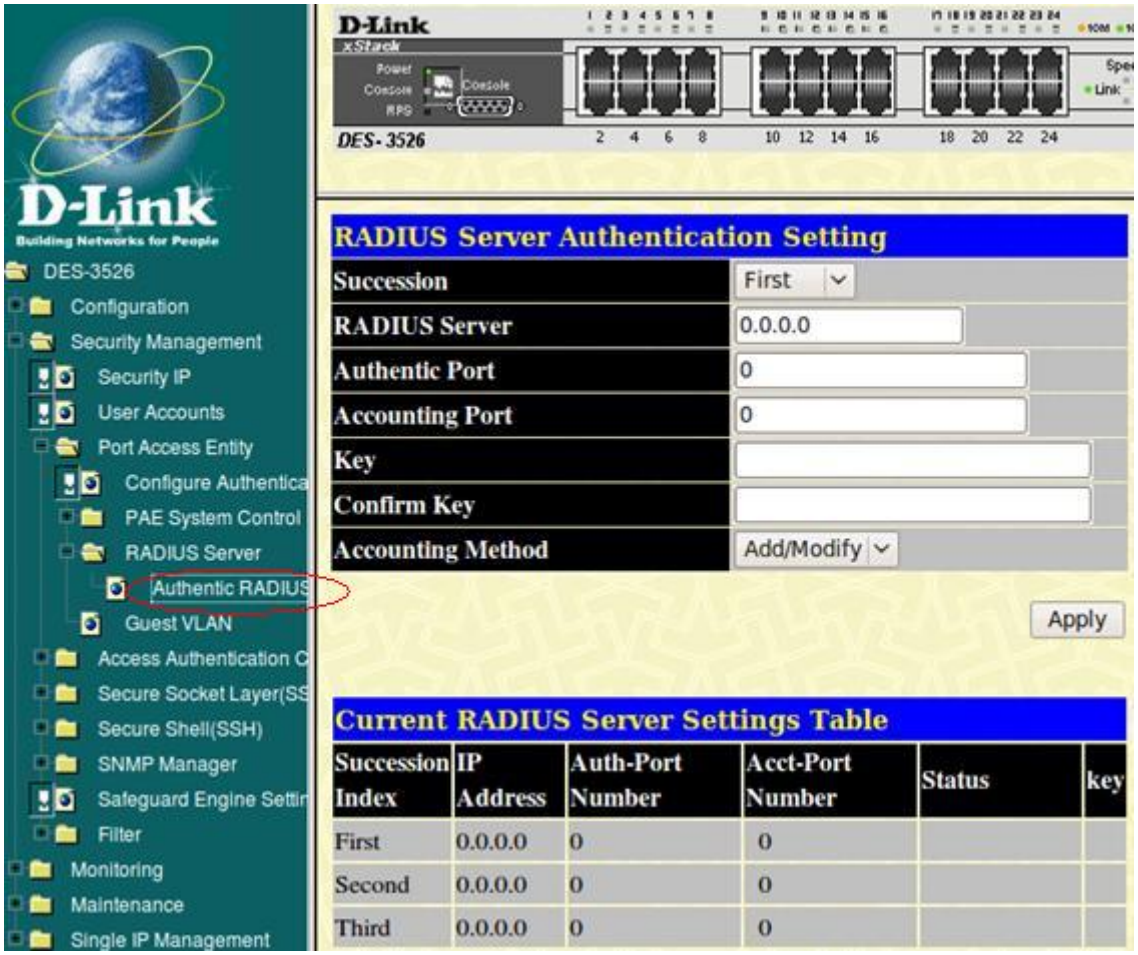

Figura 29: Interface de configuração do servidor RADIUS no switch

O significado dos campos da interface de configuração a seguir:

Succession: A ordem de sucessão na qual o servidor é utilizado.

RADIUS Server: Endereço IP do servidor RADIUS.

Authentic Port: Porta de autenticação, normalmente 1812.

Accounting Port: Port de contas, normalmente 1813.

Key: Senha para acesso ao servidor RADIUS pelo switch.

Confirm Key: Confirmação da senha.

Accounting Method: Adicionar/modificar ou remover a configuração.

Após todas configurações serem defidamente feitas, clica-se em *Apply* para confirmar a configuração do servidor RADIUS no *switch*.

ANEXO C – DHCP

Segundo (COMER, 2006) o *Dynamic Host Configuration Protocol* (DHCP) permite que um computador obtenha informações na inicialização, incluindo o endereço de um roteador padrão, o endereço de um servidor de nome de domínio e um endereço IP. O DHCP permite que um servidor aloque endereços IP automática ou dinamicamente. A alocação dinâmica é necessária para ambientes como uma rede sem fio, em que os computadores podem se conectar ou desconectar rapidamente.

O protocolo DHCP se dá por trocas de mensagens entre o cliente e um servidor DHCP. O cliente, na inicialização do sistema, envia um pacote UDP em *broadcast*, este pacote é chamado de "DHCP Discover". A figura 30 ilustra o envio desta mensagem.

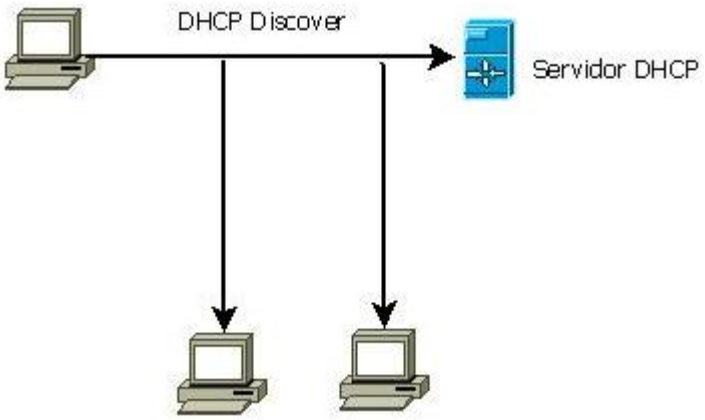

Figura 30: DHCP Discover

A Figura 31 mostra a resposta do servidor DHCP, que ao receber o pedido do cliente, irá enviar um pacote a ele contendo uma oferta de um endereço disponível em sua tabela. Esta mensagem é chamada de "DHCP Offer".

A Figura 32 ilustra a requisição do cliente ao endereço IP oferecido anteriormente, caso ele não aceite o endereço, poderá receber outras ofertas. Esta mensagem de requisição do cliente ao servidor é chamada de "DHCP Request".

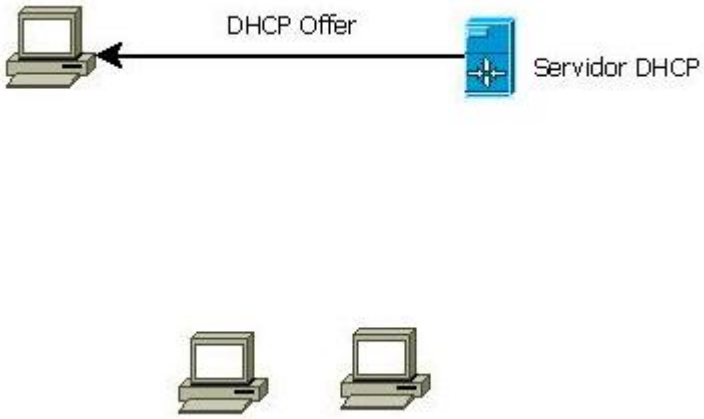

Figura 31: DHCP Offer

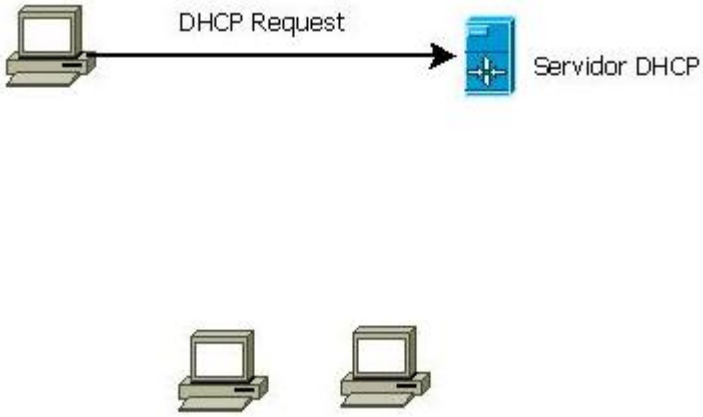

Figura 32: DHCP Request

A Figura 33 mostra a confirmação final do servidor, caso finalize positivamente o aluguel do endereço, para o cliente, que então poderá passar a fazer uso do endereço recebido. Esta mensagem é chamada de "DHCP Ack".

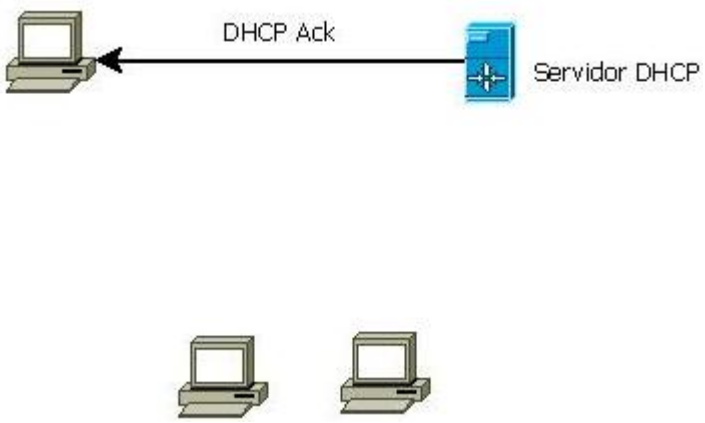

Figura 33: DHCP Ack

O protocolo ainda possui as mensagens: "DHCP Nack" (caso o servidor não valide o aluguel do endereço), "DHCP Decline" (caso o cliente não aceite o endereço oferecido), "DHCP Release" (quanto o cliente encerra o aluguel de um endereço do qual fazia uso).

Os endereços alugados pelo servidor DHCP possuem um "período de aluguel". Quando este tempo expirar, o cliente deverá requisitar outro endereço ao servidor.

C.1 Instalação e configuração

Para instarmos o servidor DHCP, utilizamos o seguinte comando (no Ubuntu):

apt-get install dhcp3-server

A configuração do servidor DHCP é feita através do arquivo /etc/dhcp3/dhcpd.conf.

A Figura 34 mostra um exemplo de configuração do arquivo /etc/dhcp3/dhcpd.conf.

No lado do cliente, deve ser usado o seguinte comando pra requisitar um endereço para o servidor DHCP:

dhclient

```
#/etc/dhcp3/dhcpd.conf

authoritative;
ddns-update-style none;

default-lease-time 600;
max-lease-time 7200;

log-facility local7;

subnet 192.168.1.0 netmask 255.255.255.0 {
        range 192.168.1.200 192.168.1.201;
}

subnet 192.168.10.0 netmask 255.255.255.0 {
option routers 192.168.10.200;
option subnet-mask 255.255.255.0;
range 192.168.10.10 192.168.10.100;
}

subnet 192.168.20.0 netmask 255.255.255.0 {
option routers 192.168.20.200;
option subnet-mask 255.255.255.0;
range 192.168.20.10 192.168.20.100;
}
```

Figura 34: Exemplo de configuração do servidor DHCP

ANEXO D – RADIUS

O *Remote Authentication Dial In User Service* (RADIUS) é um protocolo de rede que provê um serviço centralizado de gerência pelo método *Authentication, Authorization, and Accounting* (AAA), para conectar computadores usando o serviço de rede.

O RADIUS é um protocolo cliente/servidor que roda na camada de aplicação e utiliza o protocolo UDP como transporte. Pode ser utilizado para controlar meios de acesso a Internet, rede local e redes sem fio. Pode prover diversos serviços integrados, como por exemplo um *log* de ações de usuário.

As principais funções de um servidor RADIUS:

- Autenticar usuários ou dispositivos antes de conceder acesso a rede;
- Autorizar estes usuários ou dispositivos para determinados serviços de rede, e;
- Auditar o uso destes serviços.

D.1 Instalação

Neste trabalho é utilizado o servidor FreeRADIUS. Ele é instalado da seguinte forma:

Download do código fonte da aplicação:

cd /usr/local/src

wget ftp://ftp.freeradius.org/pub/freeradius/freeradius-server-2.1.7.tar.gz

Descompactação do código:

tar xzf freeradius-server-2.1.7.tar.gz

É necessário possuir a biblioteca *libssl-dev* instalada para utilizar o RADIUS:

apt-get install libssl-dev

Compilação (usando o diretório /usr/local/freeradius-server-2.1.7 como destino):

cd freeradius-server-2.1.7

./configure –prefix=/usr/local/freeradius-server-2.1.7 –exec-prefix=/usr/local/freeradius-server-2.1.7

make clean

make install

Para executá-lo, devemos usar o seguinte comando como *root*:

radiusd -X

D.2 Configuração

O RADIUS possui dois arquivos que devem ser configurados, o users e o clients.conf.

A seguir a Figura 35 mostra um exemplo de configuração do arquivo users:

```
aluno  Cleartext-Password := "aluno"
Tunnel-Type = "VLAN",
Tunnel-Medium-Type = "IEEE-802",
Tunnel-Private-Group-ID = "5"
```

Figura 35: Exemplo de configuração do arquivo users

A seguir a Figura 36 mostra um exemplo de configuração do arquivo clients.conf:

```
client proxy {
        ipaddr = 192.168.10.200
        secret = admin
        shortname = admin
        nastype = other
}
```

Figura 36: Exemplo de configuração do arquivo clients.conf

D.3 WPA Supplicant

O programa WPA *Supplicant* é utilizado para autenticar o cliente com um servidor RADIUS, ele deve ser instalado e configurado no lado do cliente.

Para instalá-lo no sistema:

apt-get install wpa-supplicant

Seu arquivo de configuração é o /etc/wpa-supplicant.conf.

Um exemplo de configuração do arquivo pode ser visto na Figura 37:

```
network={
        key_mgmt=IEEE8021X
        eap=TTLS MD5
        identity="myloginname"
        anonymous_identity="myloginname"
        password="mypassword"
        phase1="auth=MD5"
        phase2="auth=PAP password=mypassword"
        eapol_flags=0
}
```

Figura 37: Exemplo de configuração do arquivo wpa-supplicant.conf

Referências

CISCO. *CCNA3: Conceitos Básicos de Switching e Roteamento Intermediário*. [S.l.]: CISCO SYSTEMS, 2003.

COMER, D. E. *Interligação de Redes com TCP/IP*. [S.l.]: Campus, 2006.

CONGDON, P. *IEEE Std 802.1X - Port-Based Network Access Control*. [S.l.]: The Institute of Electrical and Electronics Engineers, Inc., 2004.

CRIANDO Redes Locais Virtuais (VLANs) com Linux. In: . [s.n.], 2009. Disponível em: <http://www.linuxabordo.com.br/wiki/index.php?title=VLAN>. Acesso em: out. 2009.

FOROUZAN, B. A. *Data Communications and Networking*. [S.l.]: McGraw-Hill, 2007.

PETERSON, L. *Redes de Computadores: Uma Abordagem de Sistemas*. [S.l.]: Elsevier, 2004.

PRESCHER, C. H. *Estudo e projeto para o provimento seguro de uma infra-estrutura de rede sem fio 802.11*. [S.l.]: IFSC, 2009.

SEAMAN, M. *IEEE Std 802.1Q - Virtual Local Area Networks*. [S.l.]: The Institute of Electrical and Electronics Engineers, Inc., 2005.

TANENBAUM, A. S. *Computer Networks*. [S.l.]: Prentice Hall, New Jersey, 2003.

VALLE, O. T. *Linux: Básico, Gerência, Segurança e Monitoramento de Redes*. [S.l.: s.n.], 2009.