Centro Universitário de Brasília

Instituto CEUB de Pesquisa e Desenvolvimento – ICPD

RONALDO MARCIANO DA SILVA

ESTUDO DE CASO: AUTENTICAÇÃO IEEE 802.1x APLICADA À REDE ETHERNET DA CÂMARA LEGISLATIVA DO DISTRITO FEDERAL

Brasília

2012

RONALDO MARCIANO DA SILVA

ESTUDO DE CASO: AUTENTICAÇÃO IEEE 802.1x APLICADA À REDE ETHERNET DA CÂMARA LEGISLATIVA DO DISTRITO FEDERAL

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Senso*, na área de Rede Computadores.

Orientador: Prof. Msc. Rafael Sarres

Brasília

2012

RONALDO MARCIANO DA SILVA

ESTUDO DE CASO: AUTENTICAÇÃO IEEE 802.1x APLICADA À REDE ETHERNET DA CÂMARA LEGISLATIVA DO DISTRITO FEDERAL

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Senso*, na área de Rede Computadores.

Orientador: Prof. Msc. Rafael Sarres

Brasília, 3 de agosto de 2012.

Banca Examinadora

_____
Prof. Dr. Nome completo

_____
Prof. Dr. Nome completo

À minha esposa e filhos,

pelo apoio e carinho

a mim dedicados.

A meus pais,

pela educação e exemplo

que sempre me ofereceram.

AGRADECIMENTOS

Agradeço primeiramente a Deus pelo dom da vida e por permitir vivê-la com saúde.

A minha esposa Helda e meus filhos Eduardo e Fernando, pelo carinho e compreensão.

Aos meus familiares que sempre estiveram ao meu lado, me incentivando.

Ao professor Rafael Sarres pela orientação e conselhos.

Aos colegas da SEINF, pelo apoio e experiência profissional compartilhada.

Aos demais professores do curso de Rede de Computadores, pelos ensinamentos.

Ao ELEGIS por viabilizar a realização do curso de pós-graduação.

RESUMO

O objetivo deste trabalho é estudar o protocolo IEEE 802.1x e sua aplicação na rede ethernet da Câmara Legislativa do Distrito Federal - CLDF de forma a garantir que somente usuários pertencentes ao domínio tenham acesso físico aos segmentos lógicos da rede corporativa por meio de autenticação segura. Este protocolo de rede foi desenvolvido de maneira que o acesso dos usuários se realize somente após a validação por elementos ativos da rede, os quais podem ser switches para conexões com fio e também por acesso sem fio junto a um ponto de acesso. O 802.1x é um protocolo de segurança de rede criado pelo Institute of Eletrical and Eletronics - IEEE o qual estabelece padrões para o uso de autenticação baseada na porta de acesso da rede, que integrado com o servidor RADIUS e com o servidor Active Directory permite implantar a autenticação, autorização e *accounting* incorporando segurança necessária para o acesso à rede da CLDF. Este trabalho apresenta o resultado da avaliação de teste de conceito, que respaldou a decisão pela utilização do protocolo 802.1x, bem como a escolha do melhor método de autenticação a ser aplicado na rede da CLDF, visando diminuir os riscos dificultando acessos indevidos.

Palavras-chave: Autenticação. 802.1x. Rede. Radius.

ABSTRACT

The objective of this work is to study the IEEE 802.1x protocol and their application to the Câmara Legislativa do Distrito Federal - CLDF ethernet network to ensure that only users belonging to the domain have physical access to the logical segments of the corporate network through secure authentication. This network protocol was developed so that users access must happen only after validation by the active elements of the network, which can be switches for wired network and also wireless access at a hotspot. The 802.1x is a network security protocol created by the Institute of Electrical and Electronics - IEEE which sets standards for the use of port-based authentication for network access, which integrated with the RADIUS server and the server Active Directory allow deploy the authentication, authorization and accounting incorporating security required for access to the network of CLDF. This paper presents the outcome of the test concept, which supported the decision to use the 802.1x protocol, as well as choosing the best authentication method to be applied to Network CLDF order to decrease the risks hindering unauthorized access.

Key-words: Authentication. 802.1x. Network. Radius.

ÍNDICE DE FIGURAS

ABREVIAÇÕES

AAA - Authentication, Authorization, and *Accounting*
ACL - Acces Control List
CFTV - Circuito Fechado de TV
CGTI - Coordenadoria de Gestão de Tecnologia da Informação
CHAP - Challenge Handshake Authentication Protocol
CLDF - Câmara Legislativa do Distrito Federal
DES - Data Encryption Standard
DHCP - Dynamic Host Configuration Protocol DMZ
EAP - Extensible Authentication Protocol
EAPOL - Extensible Authentication Protocol over LAN
GDF - Governo do Distrito Federal
IAS - Internet Authentication Service
IEEE - Institute of Electrical and Electronic Engineers
IETF - Internet Engineering Task Force
IP - Internet Protocol
LACP - Link Aggregation Control Protocol
LAN - Local Area Network
LCP - Link Control Protocol
LDAP - Lightweight Directory Access Protocol
MAC - Media Access Control
NAP - Network Access Protection
NAS - Network Access Server
NPS - Network Policy Server
PAE - Port Access Entity
PAP - PAP - Password Authentication
PPP - Point-to-Point Protocol
RADIUS - Remote Authentication Dial-in User Service
SCA - Sistema de Controle de Acesso
SEINF - Setor de Infraestrutura
TI - Tecnologia da Informação
TLS - Transport Layer Security
TTLS - Tunneled Transport Layer Security
VLAN – Virtual Local Area Network
VPN - Virtual Private Network

SUMÁRIO

INTRODUÇÃO

A evolução da tecnologia da informação traz como consequência natural a larga dependência das organizações em relação aos sistemas de informação e demais serviços disponíveis na rede interna de computadores e na Internet.

No entanto, manter as informações que trafegam nessa rede seguras contra eventuais invasores, é um grande desafio enfrentado pelos gestores da segurança da informação de uma organização.

Nesse sentido, e diante da amplitude e complexidade do papel da segurança da informação, existe um modelo conceitual que divide estes desafios em camadas para tornar o entendimento mais claro. Essas divisões são chamadas de barreiras, e cada uma delas tem uma participação importante no objetivo maior de reduzir os riscos [1].

Este modelo conceitual implementa a teoria do perímetro, segmentando perímetros físicos ou lógicos, e oferecendo níveis de resistência e proteção complementares e tendenciosamente crescentes.

A restrição de acessos não autorizados aos segmentos lógicos de uma rede é um controle que exerce o papel de criar uma barreira para dificultar o acesso indevido às informações que trafegam na rede [1].

Sob esse aspecto, o protocolo IEEE 802.1x [2] apresenta-se como uma solução de segurança para evitar que dispositivos não autorizados tenham acesso físico aos segmentos lógicos de uma rede corporativa.

Este protocolo foi desenvolvido de forma que o acesso dos usuários se realize somente após a validação por elementos da rede, os quais podem ser

switches para conexões com fio e também por acesso sem fio junto a um ponto de acesso.

Desse modo, o objetivo deste trabalho estudar a utilização do protocolo 802.1x e sua aplicabilidade na rede ethernet da Câmara Legislativa do Distrito Federal – CLDF, de forma a garantir que somente usuários devidamente registrados tenham acesso à rede com fio, observando suas peculiaridades e os impactos no ambiente.

O 802.1x é um protocolo de segurança de redes criado pelo Institute of Eletrical and Eletronics - IEEE que estabelece padrões para o uso de autenticação baseada na porta de acesso da rede. O principal propósito para o uso deste protocolo é tornar o ambiente mais seguro impedindo que dispositivos de comunicação sem a devida autorização conectem-se à rede.

O capítulo 1 traz aspectos conceituais necessários para a compreensão do trabalho, apresentando conceitos de segurança, funcionamento do protocolo IEEE 802.1x e do protocolo RADIUS; o capítulo 2 apresenta o estudo de caso que analisa a autenticação 802.1x para aplicação na rede da Câmara Legislativa do Distrito Federal, contextualizando o problema e apresentando sua infraestrutura de tecnologia de informação, infraestrutura de rede, vulnerabilidade das portas dos switches e os principais riscos decorrentes, realização de teste de conceito apresentando resultados, considerações e problemas encontrados; por fim as conclusões finais sobre o trabalho que sugere a elaboração de trabalhos futuros para complementação da segurança da autenticação 802.1x.

1 ASPECTOS CONCEITUAIS

1.1 Segurança da Informação

A segurança da Informação tem como objetivo a preservação de três princípios básicos: Confidencialidade, Integridade e Disponibilidade [3].

Pelo princípio da confidencialidade, toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas.

A Integridade é preservada quando a informação é mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais.

Pelo princípio da disponibilidade toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitam para qualquer finalidade.

1.1.1 Ameaças

São agentes ou condições que causam incidentes, os quais comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade e, consequentemente, causando impactos aos negócios de uma organização [1].

1.1.2 Vulnerabilidades

Fragilidade presente ou associada aos ativos que manipulam e/ou processam informações e, ao ser explorada por uma ameaça, permite a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios da segurança da informação: confidencialidade, integridade e disponibilidade.

A vulnerabilidade é um ponto no qual o sistema fica suscetível a ataque [4]. Vulnerabilidades por si só não provocam incidentes, pois são elementos passivos, necessitam para tanto de um agente causador ou condição favorável, que são as ameaças [1].

1.1.3 Medidas de Segurança

São as práticas, os procedimentos e os mecanismos usados para a proteção da informação e seus ativos, que podem impedir que ameaças explorem as vulnerabilidades, a redução das vulnerabilidades, a limitação do impacto ou minimização do risco de qualquer outra forma. As medidas de segurança são consideradas controles que podem ter as seguintes características [1]:

- preventivas: são medidas de segurança que tem como objetivo evitar que incidentes venham a ocorrer. Visam manter a segurança já implementada por meio de mecanismos que estabeleçam a conduta e a ética da segurança da instituição. Como exemplos podemos citar as políticas de segurança, instruções e procedimentos de trabalho, especificação de segurança, campanhas e palestras de conscientização de usuários; e ferramentas para implementação de política de

segurança (firewall, antivírus, configurações adequadas de roteadores e dos sistemas operacionais etc).

- detectáveis: são medidas de segurança que visam identificar condições ou indivíduos causadores de ameaças, a fim de evitar que as mesmas explorem vulnerabilidades. Alguns exemplos são: análise de riscos, sistema de detecção de intrusão, alertas de segurança; câmeras de vigilância, alarmes, etc.

- corretivas: são ações voltadas à correção de uma estrutura tecnológica e humana para que as mesmas se adaptem às condições de segurança estabelecidas pela instituição, ou voltadas à redução dos impactos: equipes para emergências, restauração de backup, plano de continuidade operacional, plano de recuperação de desastres.

1.1.4 Riscos

Consiste na probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, causando, possivelmente, impactos nos negócios. [1]

1.1.5 Incidente

É um fato (evento) decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades, levando à perda de princípios da segurança da informação: confidencialidade, integridade e disponibilidade. [1]

Um incidente gera impactos aos processos de negócio da empresa, sendo ele o elemento a ser evitado em uma cadeia de gestão de processos e pessoas.

1.1.6 Teoria do Perímetro

No capítulo de Segurança Física, a Norma NBR ISO/IEC 17799 [3] faz a seguinte recomendação sobre perímetro de segurança:

> A proteção física pode ser alcançada através da criação de diversas barreiras físicas em torno da propriedade física do negócio e de suas instalações de processamento da informação. Cada barreira estabelece um perímetro de segurança, contribuindo para o aumento da proteção total fornecida.
>
> Convém que as organizações usem os perímetros de segurança para proteger as áreas que contêm os recursos e instalações de processamento de dados. Um perímetro de segurança é qualquer coisa que estabeleça uma barreira, por exemplo, uma parede, uma porta com controle de entrada baseado em cartão ou mesmo um balcão de controle de acesso com registro manual. A localização e a resistência de cada barreira dependem dos resultados da análise de risco.

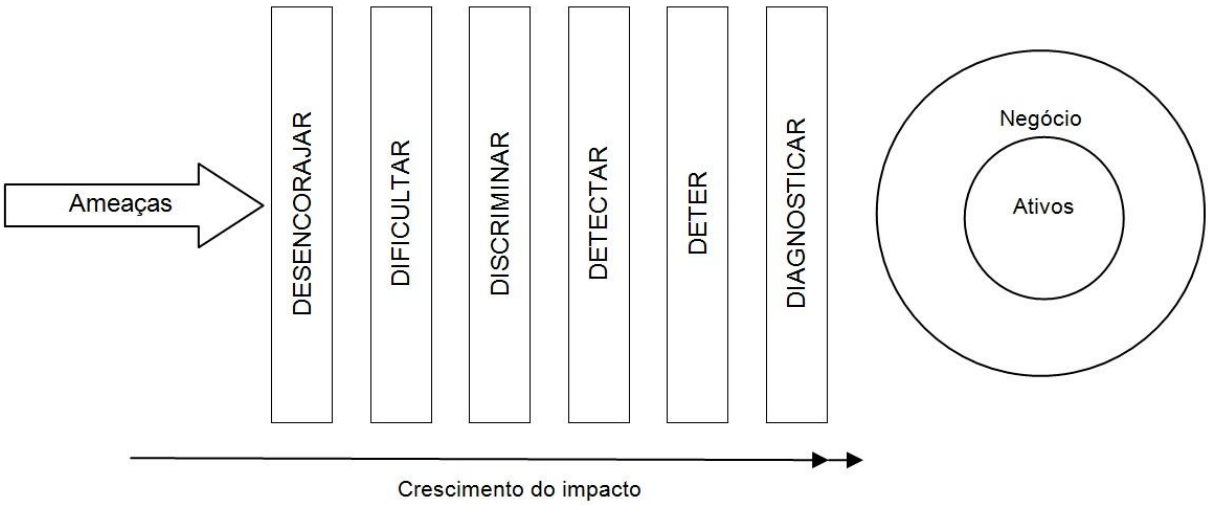
Uma maneira de se obter o melhor retorno dos mecanismos que garantam os níveis de proteção da informação é a segmentação inteligente dos ativos [1].

Desta forma é possível aplicar os controles de segurança com um nível previamente dosado de proteção, sem exceder os limites e nem ficar aquém das necessidades.

1.1.7 Barreiras da Segurança

Para Sêmola [1] as barreiras de segurança são divididas em seis tipos diferentes. Cada uma delas tem uma parcela de participação no objetivo de reduzir os riscos. Portanto deve ser dimensionada de forma a proporcionar uma interação e integração entre elas.

Figura 1 - Diagrama representativo das barreiras de segurança



Fonte – Sêmola (2003, p.53)

Este modelo conceitual implementa a teoria do perímetro, segmentando perímetros físicos ou lógicos, e oferecendo níveis de resistência e proteção complementares e tendenciosamente crescentes, conforme pode ser observado na figura 1 [1].

- barreira desencorajar: esta é a primeira das cinco barreiras de segurança e cumpre o papel importante de desencorajar as ameaças. Estas, por sua vez, podem ser desmotivadas ou podem perder o interesse e o estímulo pela tentativa de quebra de segurança por efeito de mecanismos físicos, tecnológicos ou

humanos. A simples presença de uma câmera de vídeo, mesmo falsa, de um aviso da existência de alarmes, capanhas de divulgação da política de segurança ou treinamento dos funcionários informando as práticas de auditoria e monitoramento de acesso aos sistemas, já são efetivos nesta fase.

- barreira dificultar: o papel desta barreira é complementar a anterior por meio da adoção efetiva dos controles que irão dificultar o acesso indevido. Como exemplo, podemos citar os dispositivos de autenticação para acesso físico, como roletas, detectores de metal e alarmes, ou lógicos, como leitores de cartão magnético, senhas, smartcards e certificados digitais, além da criptografia, firewall etc.

- barreira discriminar: aqui o importante é cercar-se de recursos que permitam identificar e gerir os acessos, definindo perfis e autorizando permissões. Os sistemas são largamente empregados para monitorar e estabelecer limites de acesso aos serviços de telefonia, perímetros físicos, aplicações de computador e banco de dados. Os processos de avaliação e gestão do volume de uso dos recursos, como email, impressora, ou até mesmo o fluxo de acesso físico aos ambientes, são bons exemplos das atividades desta barreira.

- barreira detectar: mais uma vez agindo de forma complementar às suas antecessoras, esta barreira deve munir a solução de segurança de dispositivos que sinalizem, alertem e instrumentem os gestores da segurança na detecção de situação de risco, seja em uma tentativa de invasão, uma possível contaminação por vírus, o descumprimento da política de segurança da empresa, ou a cópia e envio de informações sigilosas de forma inadequada. Entram aqui os sistemas de monitoramento e auditoria para auxiliar na identificação de atitudes de exposição,

como o antivírus e os sistemas de detecção de intruso, que reduzem o tempo de resposta a incidentes.

- barreira deter: esta quinta barreira tem o objetivo de impedir que a ameaça atinja os ativos que suportam o negócio. O acionamento desta barreira, ativando seus mecanismos de controle, é um sinal de que as barreiras anteriores não foram suficientes para conter a ação da ameaça. Neste momento, medidas de detenção, como ações administrativas, punitivas e bloqueios de acessos físicos e lógicos, respectivamente a ambiente e sistemas, são bons exemplos.

- barreira diagnosticar: apesar de figurar como a última barreira no diagrama, esta fase possui um sentido especial de representar a continuidade do processo de gestão de segurança da informação. Pode parecer o fim, mas é a ligação com a primeira barreira, criando um movimento cíclico e contínuo, e devido a esses fatores esta é a barreira de maior importância. Deve ser conduzida por atividades de análise de riscos que considerem tanto os aspectos tecnológicos quanto os físicos e humanos, sempre orientados às características e às necessidades específicas dos processos de negócio da empresa.

1.2 IEEE 802.1X

1.2.1 Introdução do protocolo 802.1x

Em um ambiente de rede onde o meio de acesso é compartilhado e aberto, como nas redes sem fio ou no caso das redes cabeadas, nas quais existem segmentos da rede que não podem ser verificados, a confiança nos hosts fica limitada. Para contornar esses aspectos que comprometem os pilares da segurança

conhecidos como: confiabilidade, integridade e disponibilidade dos ativos da rede [1], existem protocolos disponíveis para implementação.

O protocolo 802.1x provê autenticação entre os clientes da rede e o ativo no qual os mesmos estão conectados podendo este ser um switch ou um ponto de acesso (AP - Access Point) para acessos sem fio. Dessa forma, diminui os riscos às ameaças tornando os clientes da rede confiáveis.

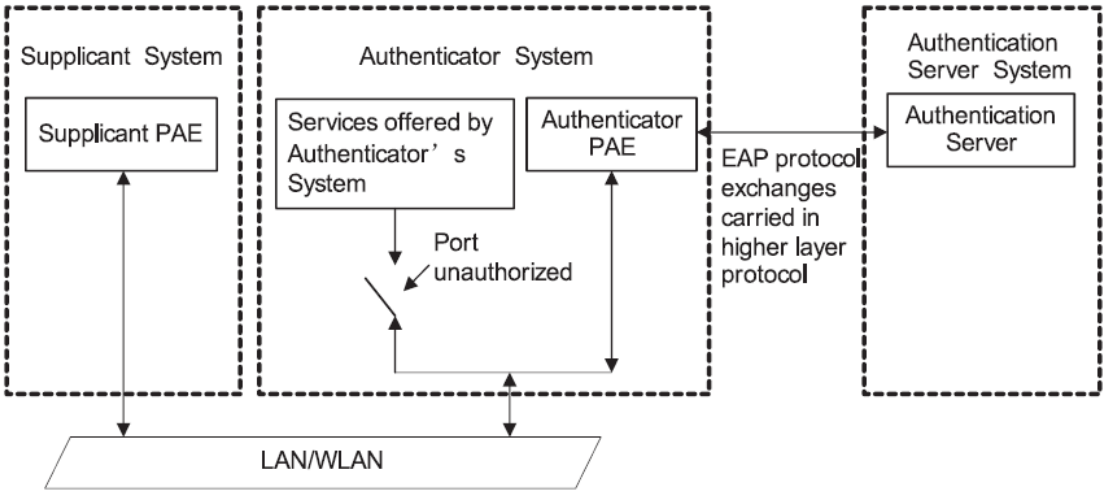
O protocolo 802.1X é um padrão do Institute of *Electrical and Electronic Engineers* – IEEE para controle de acesso à rede com base em portas. Faz parte do grupo IEEE 802.1, grupo de protocolos de redes. Nesse estudo trataremos dos mecanismos de autenticação em portas de redes LAN.

Para Brown [5], 802.1x é um protocolo que estende o *Extensible Authentication Protocol* - EAP sobre a *Local Area Network* - LAN por um processo chamado *Extensible Authentication Protocolo Over LANs* – EAPoL [2]. Esses protocolos são fundamentais para o funcionamento da autenticação 802.1x e serão apresentados nas próximas seções.

1.2.2 Arquitetura da autenticação 802.1x

Como mostrado na figura 2, o protocolo 801.1x adota uma arquitetura cliente servidor com três entidades: um sistema suplicante, um sistema autenticador e um sistema servidor de autenticação [6].

Figura 2 - Arquitetura de Autenticação 802.1x



Fonte – 3Com Switch 5500 Family Configuration Guide (2007, p.477)

O sistema suplicante é uma entidade localizada em uma ponta do enlace da LAN e é autenticado pelo sistema autenticador na outra ponta do enlace da LAN. Uma autenticação 802.1x é iniciada pelo programa cliente do sistema suplicante. O programa cliente deve suportar o protocolo EAPoL.

O sistema autenticador é a entidade localizada no outro lado do enlace da LAN. Ele autentica o sistema suplicante conectado. O sistema autenticador é geralmente um dispositivo de rede que suporta o protocolo 802.1x. Ele fornece uma porta física para o sistema suplicante acessar a LAN.

O sistema servidor de autenticação é uma entidade que fornece o serviço de autenticação para o sistema autenticador. Geralmente é implementado com o uso de um servidor RADIUS. O sistema servidor de autenticação oferece serviço que realiza a Autenticação, Autorização e Accouting – AAA para os usuários. Ele também armazena informações do usuário, como o nome de usuário, senha, a VLAN que pertence ao usuário, prioridade e Access Control List – ACL.

Segundo Brown [5], essas entidades fazem três diferentes comunicações para realizarem a autenticação, duas são trocas físicas e uma troca lógica.

Há uma comunicação física entre o suplicante e o autenticador e, também entre o autenticador e o servidor. Assim, o autenticador funciona como um tradutor entre o suplicante e o servidor de autenticação. A comunicação entre o suplicante e o servidor de autenticação é inteiramente lógica, já que não há nenhuma ligação física entre eles.

Quando o sistema autenticador e o sistema suplicante se comunicam utilizam o protocolo EAPoL na camada dois do modelo *Open Systems Interconnection* – OSI [7]. Qualquer coisa que o sistema suplicante tentar fazer fora do protocolo é ignorado pelo sistema autenticador. É possível configurar o processo de autenticação para permitir um tráfico específico oriundo da rede até o suplicante.

Assim que um dispositivo é conectado à porta, o sistema autenticador solicita a credencial de identificação. Nesse momento é utilizado um frame EAPoL chamado de *Request Identity*. Se existir um sistema suplicante na outra ponta do enlace, ele responderá com o pacote “Response”. O sistema autenticador aceitará o pacote de “Response” e encaminhará ao sistema servidor de autenticação utilizando o protocolo RADIUS. O sistema servidor de autenticação irá responder ao sistema autenticador usando o protocolo RADIUS. O sistema autenticador empacota esses dados do sistema servidor de autenticação e encaminha um *Request Identity* ao suplicante utilizando um pacote do protocolo EAPOL. Este tipo de comunicação continuará até que o processo de autenticação seja completado.

O sistema servidor de autenticação, que neste trabalho é o RADIUS, irá notificar ao sistema autenticador da validade ou não da credencial. O sistema autenticador passará essa informação para o suplicante, mas também tomará uma

ação, autorizando ou não o suplicante a ingressar na VLAN. É possível colocar suplicantes não autorizados dentro de VLANS especiais chamadas de *guest* VLAN.

Existem várias maneiras de atribuir VLAN a um dispositivo conectado. Uma delas é associar a VLAN para cada porta da rede por meio das configurações da própria porta. O sistema suplicante autenticado pode também possuir uma VLAN assinada pelo servidor RADIUS. Essa VLAN pode ser atribuída à porta da rede após uma autenticação ser realizada.

A *guest* (convidados) VLAN pode ser configurada na porta que tem o 802.1x habilitada. Assim, existem várias possibilidades de atribuir uma VLAN ao dispositivo que tentar se conectar a uma porta, que variam desde nenhuma VLAN a uma especifica a ser aplicada a um usuário em particular.

O conteúdo dos dados da comunicação lógica entre o sistema suplicante e o sistema servidor de autenticação, também está disponível ao sistema autenticador. Entretanto, ele nada faz até que a mensagem do sistema servidor de autenticação indicar uma validação ou não. Se a mensagem é de validação o sistema autenticador irá atribuir à porta uma específica VLAN. Se não for validada, o sistema autenticador irá manter o suplicante desconectado e colocará a porta em estado de *unauthorized*. Em algumas implementações é possível colocar suplicante que não pôde ser autenticado em uma *guest VLAN*.

1.2.3 PAE

O Port Access Entity – PAE é responsável pela implementação de algoritmos e também pela execução de operações relacionadas ao protocolo do mecanismo de autenticação [6].

O sistema do autenticador PAE autentica o sistema suplicante quando ele faz login na LAN e controla o status (autorizado/não autorizado) das portas controladas, de acordo com o resultado da autenticação.

O sistema suplicante PAE responde à requisição de autenticação recebida do sistema autenticador e submete a informação de autenticação do usuário ao sistema autenticador. Ele também envia a requisição da autenticação e requisição de desconexão para o sistema autenticado PAE.

1.2.4 Porta controlada e porta não controlada

O sistema autenticador fornece portas para o sistema suplicante acessar a LAN. Uma porta desse tipo é dividida em portas controlada e portas não controladas.

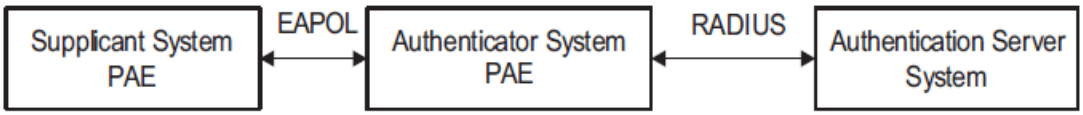
A porta controlada pode sempre enviar e receber pacotes. Elas, principalmente, servem para encaminhar pacotes EAPoL para garantir que um sistema suplicante possa enviar e receber requisições de autenticação.

A porta controlada pode ser usada para passar pacote de serviço quando ela está em estado autorizado. Ela é bloqueada quando não está em estado autorizado. Neste caso, nenhum pacote pode passar por ela.

1.2.5 Mecanismo do sistema de autenticação 802.1x

O sistema de autenticação IEEE 802.1x usa o Extensible Authentication Protocol – EAP para trocar informação entre o sistema suplicante e o servidor de autenticação, conforme figura 3 [6].

Figura 3 - Autenticação 802.1x



Fonte – 3Com Switch 5500 Family Configuration Guide (2007, p. 479)

Os pacotes do protocolo EAP transmitidos entre o sistema suplicante e o sistema autenticador são encapsulados como pacotes EAPoL.

Os pacotes do protocolo EAP transmitidos entre o sistema autenticador PAE e o servidor RADIUS podem ser encapsulados como EAP sobre pacotes RADIUS (EAPoR) ou serem finalizados no sistema PAEs. O sistema PAE então comunica com servidor RADIUS através dos pacotes do protocolo de *Password Authentication Protocol* – PAP ou *Password Challenge-Handshake* – CHAP [6].

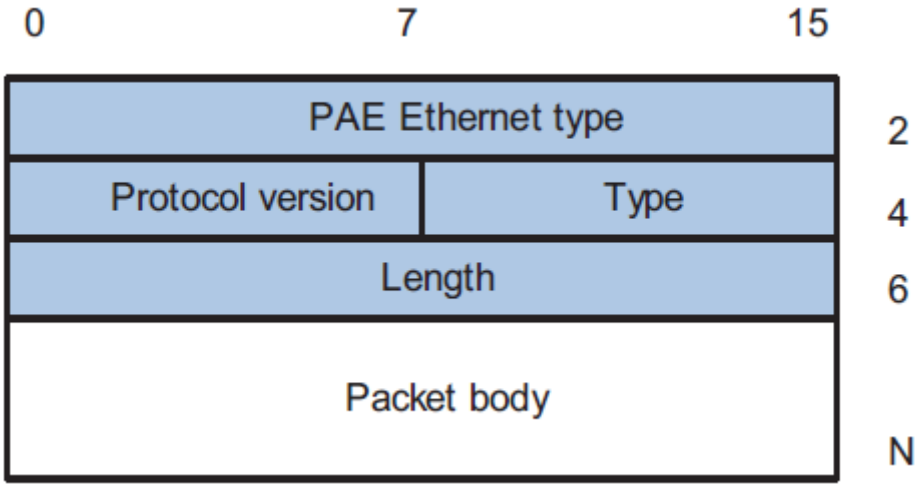
Quando um sistema suplicante passa a autenticação, o servidor de autenticação passa a informação sobre o sistema suplicante para o sistema autenticador. O sistema autenticador por sua vez determina o estado (autorizado ou não autorizado) da porta controlada segundo as instruções (*accept ou reject*) recebidas do servidor RADIUS.

1.2.6 Encapsulamento das mensagens EAPoL

1.2.6.1 O formado de um pacote EAPoL

EAPoL é um formato de encapsulamento de pacote definido na 802.1x para habilitar o pacote do protocolo EAP para ser transmitido entre o sistema suplicante e o sistema autenticador através da LAN. Os pacotes do protocolo EAP são encapsulado no formato EAPoL. A figura 4 [6] ilustra a estrutura de uma pacote EAPol.

Figura 4 - Pacote EAPoL



Fonte – 3Com Switch 5500 Family Configuration Guide (2007, p. 479)

Dentro de um pacote EAPoL:

a) O campo tipo ethernet PAE possui o identificador de protocolo. O identificador para o 802.1x é 0x888E.

b) O campo da versão do protocolo possui a versão do protocolo suportada pelo remetente do pacote EAPoL.

c) O campo Type pode ter um dos seguintes contéudo:

00 – indica que é um pacote EAP-packet, que carrega a informação da autenticação.

01 – indica que é um pacote EAPoL-start, que inicia a autenticação.

02 – indica que é um pacote EAPoL-logoff, que envia solicitações de de logging.

03 – indica que é um pacote EAPoL-key, que carrega informação da chave.

04 – indica que é um pacote EAPoL-encapsulated-ASF-Alert, que é usado para dar suporte às mensagens de alerta do Alerting Standards Forum – ASF.

d) O campo lenght indica o tamanho do campo do corpo do pacote. O valor “0” indica que o campo do corpo do pacote não existe.

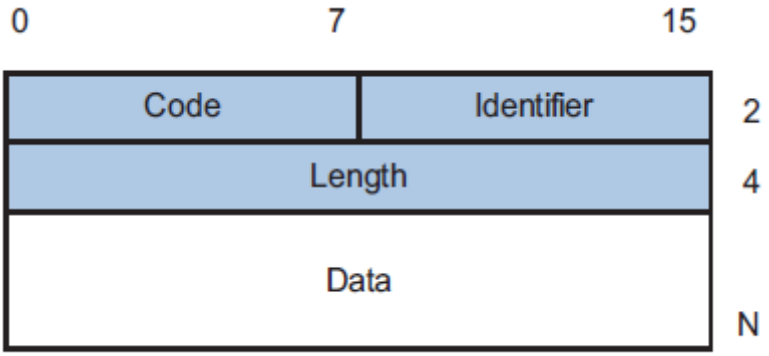
e) O campo do body packet difere do campo tipo.

Perceba que os pacotes EAPoL-Start, EAPoL-Logoff e EAPoL-Key são transmitidos apenas entre o sistema suplicante e o sistema autenticador. Os pacotes EAP são encapsulados pelo protocolo RADIUS para permitir sua chegada ao sistema servidor de autenticação. Informações de gerenciamento relacionada com a rede, como alarmes, são encapsulada no pacote EAPoL-Encapsulated-ASF-Alert, que é finalizado pelo sistema autenticador.

1.2.6.2 O formado de uma pacote EAP

Para um pacote EAPoL com valor do campo Type sendo EAP-packet, seu campo Packet body é uma pacote EAP, cujo formato é mostrado na figura 5 [6].

Figura 5 - Pacote EAP



Fonte – 3Com Switch 5500 Family Configuration Guide (2007, p. 480)

a) O campo *Code* indica o tipo de pacote EAP, que pode ser: um *Request*, um Response, um *Success* ou um *Failure*.

b) O campo identificador é usado para combinar o pacote Response com seu correspondente pacote *Request*.

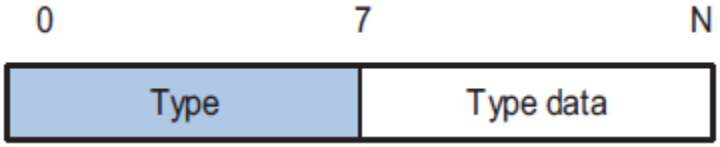
c) O campo Lenght indica o tamanho de um pacote EAP, que inclui os campos *Identifier*, *Leght* e *Data*.

d) O campo Data carrega um pacote EAP cujo formado difere do campo Code.

Um pacote *Success* ou *Failure* não contém o campo Data, por isso o campo *Lenght* é “4”.

A figura 6 [6] mostra o formado do campo Data de um pacote Request ou de um pacote Response.

Figura 6 - Campo Data



Fonte – 3Com Switch 5500 Family Configuration Guide (2007, p. 481)

a) O campo *Type* indica o tipo de autenticação EAP. O valor “1” indica a identidade e que o pacote é usado para perguntar a identidade do outro lado do enlace. O valor 4 representa MD5-Challenge (similar do PPP CHAP) e indica que o pacote inclui informação de pergunta.

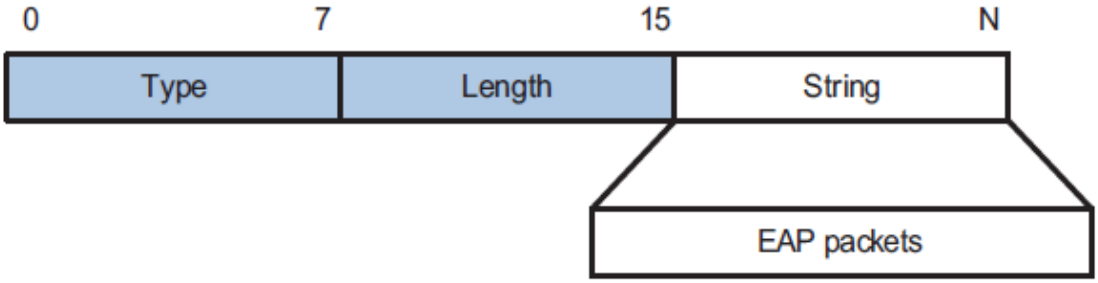
b) O campo *Type Date* diferencia os pacotes e *Request* e *Response*.

1.2.6.3 Campos adicionais para a autenticação EAP

Dois campos, EAP-message e *Messagem-authenticator*, são adicionados ao protocolo RADIUS para a autenticação EAP.

O campo EAP-message, formado como ilustrador na figura 7 [6], é usado para encapsular os pacotes EAP. O tamanho máximo da string do campo é 253 bytes. Pacotes EAP com seu tamanho maior que 253 são fragmentados e encapsulados em vários campos EAP-message. O código do tipo de EAP-message é 79.

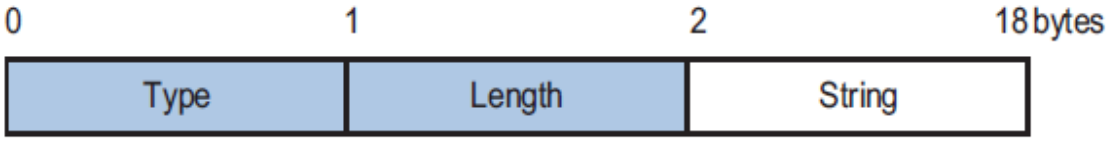
Figura 7 - Campo EAP-message



Fonte – 3Com Switch 5500 Family Configuration Guide (2007, p. 481)

O campo *Message-authenticator*, ilustrado na figura 8 [6], é usado para prevenir uma intercepção não autorizada para acessar pacotes durante uma autenticação CHAP, EAP, e assim por diante. Um pacote com o campo EAP-message também tem um campo *Message-authenticator*.

Figura 8 - Campo Message-authenticator



Fonte – 3Com Switch 5500 Family Configuration Guide (2007, p. 481)

1.2.6.4 Modo EAP relay

No modelo 802.1x, o EAP-PACKET é encapsulado no protocolo de nível mais alto (como EAPoR) para que alcancem com sucesso o servidor de autenticação. Geralmente, este modo requer que o servidor RADIUS suporte os dois

campos adicionais: o campo EAP message (com valor 79) e o campo *Message-authenticator* (com o valor 80).

Para formas de autenticação, EAP-MD5, EAP-TLS (T*ransport Layer Security*), EAP-TTLS (*Tunneled Transport Layer Security*), e *Protect Extensible Authentication Protocol* (PEAP), são disponíveis o EAP modo *relay*.

EAP-MD5 autentica o sistema suplicante. O servidor RADIUS envia chaves MD5 (contido dentro do EAP-*request*/MD5 *challenge packets*) para o sistema suplicante, que por sua vez criptografa as senhas usando chaves MD5.

EAP-TLS permite que o sistema suplicante e o servidor RADIUS verifiquem certificado de segurança entre si e autentique a identidade de cada um, garantindo que os dados sejam transferidos para os destinatários verdadeiros e prevenindo de interceptação de dados.

EAP-TTLS é um tipo de extensão do EAP-TLS. EAP-TLS implementa autenticação bidirecional entre o cliente e o servidor de autenticação. EAP-TTLS transmite mensagem usando o fechamento de um túnel usando TLS.

PEAP cria canais de segurança TLS para garantir integridade dos dados e realizar nova negociação EAP para verificar sistemas suplicantes.

A figura 9 [6] descreve o procedimento da autenticação EAP-MD5.

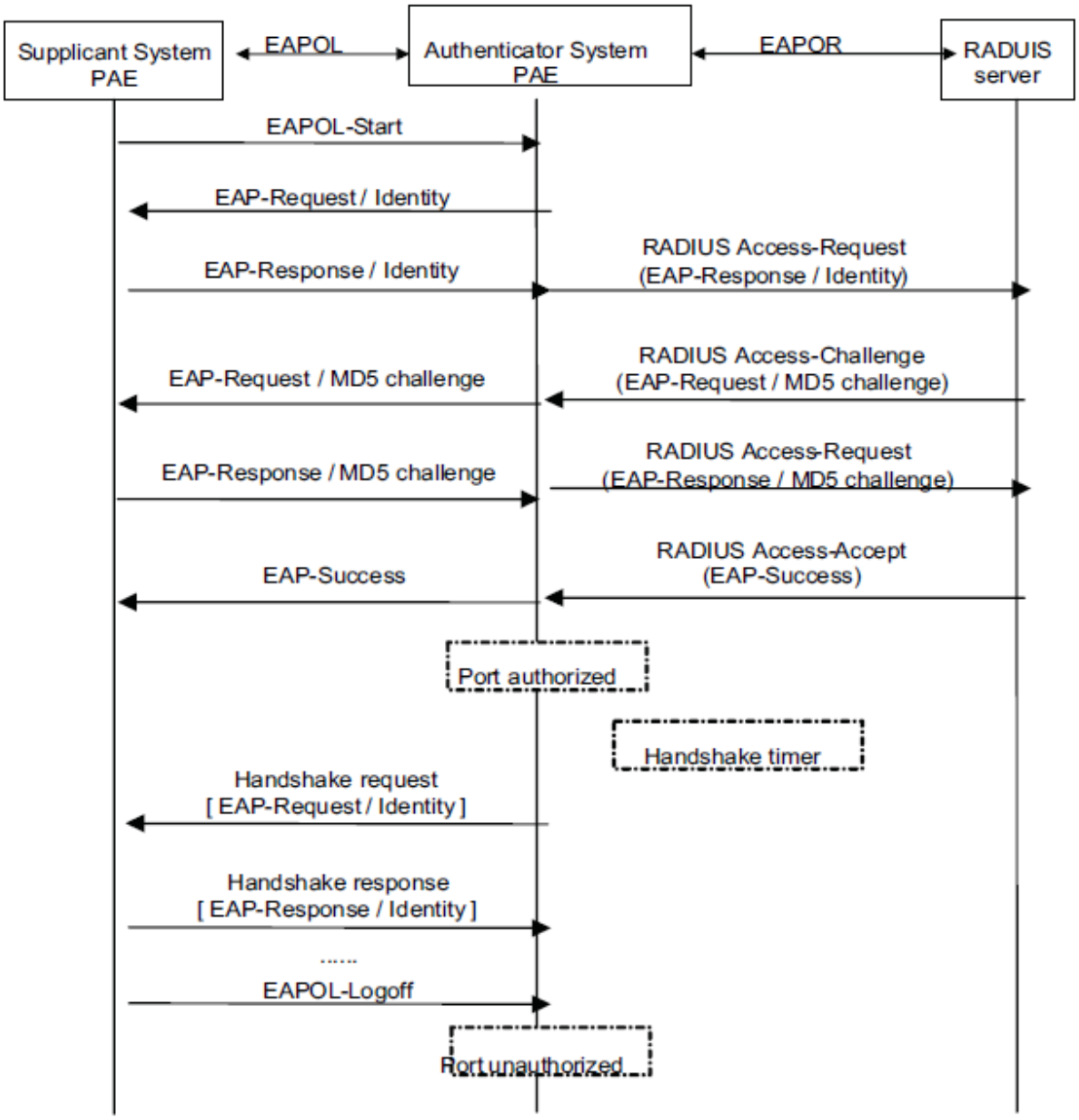
Detalhes do procedimento:

Um sistema suplicante inicia um cliente 802.1x para solicitar acesso enviando um pacote EAPoL-start para o switch, com seu nome de usuário e senha. O programa cliente 802.1x então envia o pacote para o switch para iniciar um processo de autenticação.

Ao receber o pacote de requisição de autenticação, o switch envia um EAP-request/identity para perguntar ao cliente 802.1x o nome do cliente.

O cliente 802.1x responde enviando um pacote EAP-response/identity para o switch com o nome do usuário nele contido. O switch então encapsula o pacote dentro de uma pacote RADIUS Access-Request e encaminha ao servidor RADIUS.

Figura 9 - Autenticação EAP-MD5 Fonte



3Com Switch 5500 Family Configuration Guide (2007, p. 482)

Ao receber o pacote do switch, o servidor RADIUS recupera o nome do usuário desse pacote, encontra a senha correspondente comparando o nome do

usuário armazenada dentro de seu bando de dados, criptografa a senha usando uma chave gerada randomicamente e envia a chave para o switch através de um pacote RADIUS *Access-challenge*. O switch então envia a chave para o cliente 802.1x.

Ao receber a chave (encapsulada dentro de um pacote EAP-*request*/MD5 challenge) do switch, o programa cliente criptografa a senha do sistema suplicante usando a chave e envia a senha criptografada (contida em um pacote EAP-*response*/MD5 *challenge*) para o servidor RADIUS através do switch. (Geralmente a criptografia é irreversível).

O servidor RADIUS compara a senha criptografada recebida (contida dentro de uma pacote RADIUS Access-request) com a senha local criptografada. Se os dois são iguais ele então retorna através de um pacote RADIUS *Access-accept* e um EAP-success) para o switch indicar que o sistema suplicante está autenticado.

O switch modifica o estado da porta correspondente para accepted state para permitir que o sistema suplicante tenha acesso à rede.

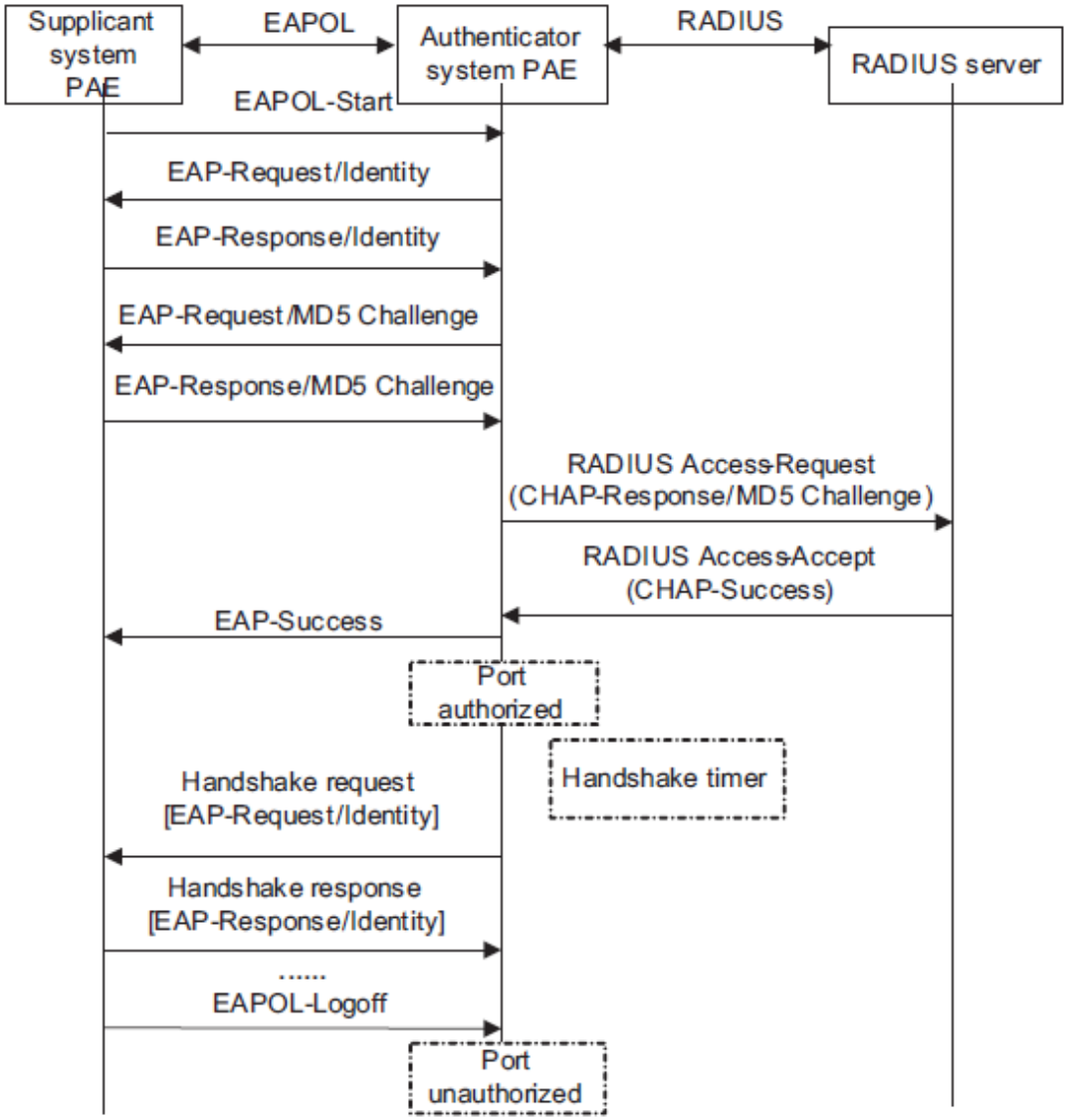
No modo *relay* EAP, pacotes não são modificados durante a transmissão se uma das formas PEAP, EAP-TLS, EAP-TTLS ou EAP-MD5, forem usadas para autenticar. Deve ser garantido que tanto o sistema suplicante e o servidor RADIUS utilizem a mesmo forma de autenticação.

1.2.6.5 Modo EAP teminating

Nesse modo, a transmissão do pacote EAP é encerrada pelo sistema autenticador e o pacote EAP é convertido para o pacote RADIUS. Autenticação e *accounting* são carregados por meio do protocolo RADIUS.

Nesse modo, PAP ou CHAP é empregado entre o switch e o servidor RADIUS. A figura 10 [6] ilustra o procedimento de autenticação.

Figura 10 - Autenticação EAP teminating



Fonte – 3Com Switch 5500 Family Configuration Guide (2007, p. 485)

O procedimento de autenticação no modo EAP *terminating* é o mesmo que no modo EAP relay, exceto a chave gerada randomicamente no modo EAP *terminating* é gerada pelo switch, e ele que envia o nome do usuário, a chave

randomicamente gerada e a senha criptografada do sistema suplicante para o servidor RADIUS realizar a autenticação.

1.3 RADIUS

O RADIUS é um protocolo de autenticação utilizado em praticamente todas as implementações do 802.1x [5]. As especificações do Radius são abrangidas pelas RFC 2564 [8] e RFC 3579 [9] da *Internet Engineering Task Force* – IETF. Ele é utilizado para disponibilizar acessos às redes utilizando a arquitetura AAA - Autenticação, Autorização e *Accounting* [11].

Inicialmente o protocolo RADIUS foi desenvolvido para uso em serviços de acesso discado [10]. Atualmente é implementado para autenticação de acesso à rede sem fio e outros tipos de dispositivos que permitem acesso autenticado às redes de computadores.

As especificações do EAP não descreve o RADIUS como um componente exigido, porém ele é, de fato, um componente essencial [5]. Qualquer servidor RADIUS atenderá as funções requeridas com capacidade para lidar com todos os métodos Extensible Authentication Protocol - EAP especificados. Porém se um novo método for desenvolvido, quase sempre um método proprietário, então é necessário o desenvolvimento um novo servidor proprietário para dar suporte o método. Isso significa que uma atenção particular deve se dar à escolha do EAP-Método e seu suporte pelo servidor RADIUS já implementado na rede. Como afirmado, um método proprietário pode requerer tanto a especificação do suplicante como a especificação de um servidor RADIUS de um vendedor particular.

O RADIUS opera no modelo cliente servidor onde o dispositivo de acesso à rede passa a informação da autenticação do cliente para o servidor. A segurança é

preservada neste modelo através do uso de uma senha compartilhada para o dispositivo de acesso e o servidor RADIUS. O servidor irá oferecer a autenticação necessária do suplicante e apenas quando o dispositivo de acesso fornecer credenciais válidas ao RADIUS.

O autenticador e o servidor de autenticação, RADIUS, se comunicam utilizando o protocolo RADIUS. Os pacotes RADIUS são basicamente formados de atributos. Cada atributo é um elemento de dado específico que é utilizado pelo autenticador ou é repassado para o suplicante. Existem mais de cem atributos reservados, porém apenas alguns são pertinentes na conversa 802.1x.

O dado do método EAP é encapsulado nos pacotes trocados entre o autenticador e o servidor de autenticação. Esse elemento é usado para trocar informações de autenticação entre o suplicante e o servidor de autenticação. O dado é criptografado entre o autenticador e o servidor RADIUS. O segredo compartilhado é uma parte da chave necessária para decriptografar os dados do método EAP.

Se a autenticação é bem sucedida, então o servidor RADIUS pode ser configurado para fornecer informação ao autenticador que será usada para modificar tanto a VLAN que será assinada como a lista de acesso. Essa informação está contida dentro de dois atributos específicos que são passados para o autenticador fora da troca do método EAP.

1.3.1 Arquitetura AAA

A estrutura em torno da qual o protocolo RADIUS foi desenvolvido é conhecida como arquitetura AAA, que consiste na autenticação, autorização e

accounting [11]. A autenticação verifica a identidade do usuário de um sistema, a autorização garante que o usuário autenticado somente tenha acesso aos recursos autorizados e a *accounting* coleta informações sobre a atividade do elemento autenticado e as envia ao servidor para armazenamento. A arquitetura AAA define uma forma estruturada para integração dessas três funcionalidades. Abaixo alguns exemplos de uso da arquitetura AAA [12]:

- controle de acesso em ambientes LAN: permite habilitar o acesso à porta física, objeto do estudo deste trabalho, ou ao segmento de uma rede sem fio.

- controle de acesso em ambientes VPN de acesso remoto: verifica-se inicialmente o direito de montar o túnel e, a seguir, são validadas as credenciais daquele usuário.

- controle de acesso através de firewalls: nesses casos, o firewall intercepta as requisições e aplica regras dinâmicas conforme permissões informadas pelo servidor AAA.

- Controle de acesso à Internet num ambiente corporativo, definindo políticas aceitáveis de uso conforme o grupo ao que o usuário pertença.

1.3.2 Funcionamento do RADIUS

O protocolo RADIUS, usado para fazer a comunicação entre o autenticador e o servidor de autenticação é muito similar ao esquema do EAP. Assim como o EAP, o RADIUS identifica a função a ser realizada por meio de um elemento chamado code e usa um processo sincronizador lock-step que utiliza um

elemento chamado identificador. A figura 11 [5] ilustra o esquema do pacote RADIUS.

Figura 11 - Pacote RADIUS

Code (1-byte)	Identifier (1-byte)	Length (2 bytes)	Authenticator (16 bytes)	Attributes (0-n bytes)

Code:	Message Type
Identifier:	Lock-step code to match requests to replies
Length:	Message length including header
Authenticator:	"Random unpredictable number" used to validate Information exchanges
Attributes:	Authentication information (EAP-Method)

Fonte – Brown (2007, p. 68)

A funcionalidade do code no RADIUS é a mesma executada no EAP. Existem seis valores pra este elemento pertinentes ao protocolo 802.1x. Quatro desses elementos são usados pelo servidor para transmissões ao autenticador, e duas são usados pelo autenticador para comunicar com o servidor. O autenticador enviará ao servidor de autenticação uma requisição de Access-request ou uma requisição de accounting-request. O servidor de autenticação possui algumas opções disponíveis. Elas podem responder para um Accountin-request, se declara bem sucedida ou mal sucedida com um Access-accept ou Access-reject, ou ele pode solicitar informação adicional com um Access-challenge. A conversação mais comum consiste do Access-request originado do autenticador, seguido pelo Access-challenge pelo servidor RADIUS. Os seis valores para o Code pertinente à autenticação 802.1x são demonstrados abaixo:

Quadro 1 – Valores para o campo Code

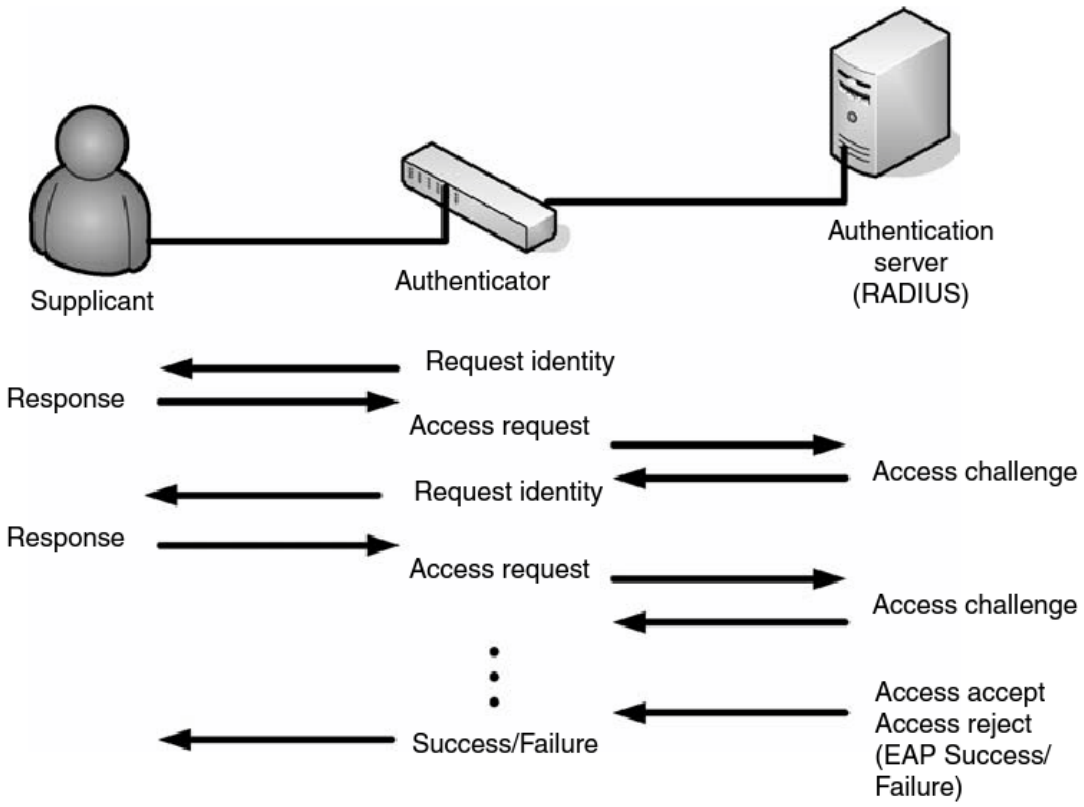
Code	Descrição
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
6	Access-Challenge

Fonte: Brown (2007)

O servidor RADIUS fará uma conversação “dual”. Ele conduzirá uma conversação com o autenticador usando RADIUS protocolo, e uma conversação método EAP com o suplicante. O fluxo aparentemente será o mesmo para os diversos métodos. Porém, a credencial ou outra informação de autenticação variará para cada método particular.

Lembrando que o autenticador fisicamente conversa com o servidor de autenticação enquanto o suplicante logicamente conversa com servidor de autenticação, conforme ilustrado na figura 12 [5].

Figura 12 – Conversação



RADIUS dual Fonte – Brown (2007, p. 69)

1.3.3 Processo Lock-Step

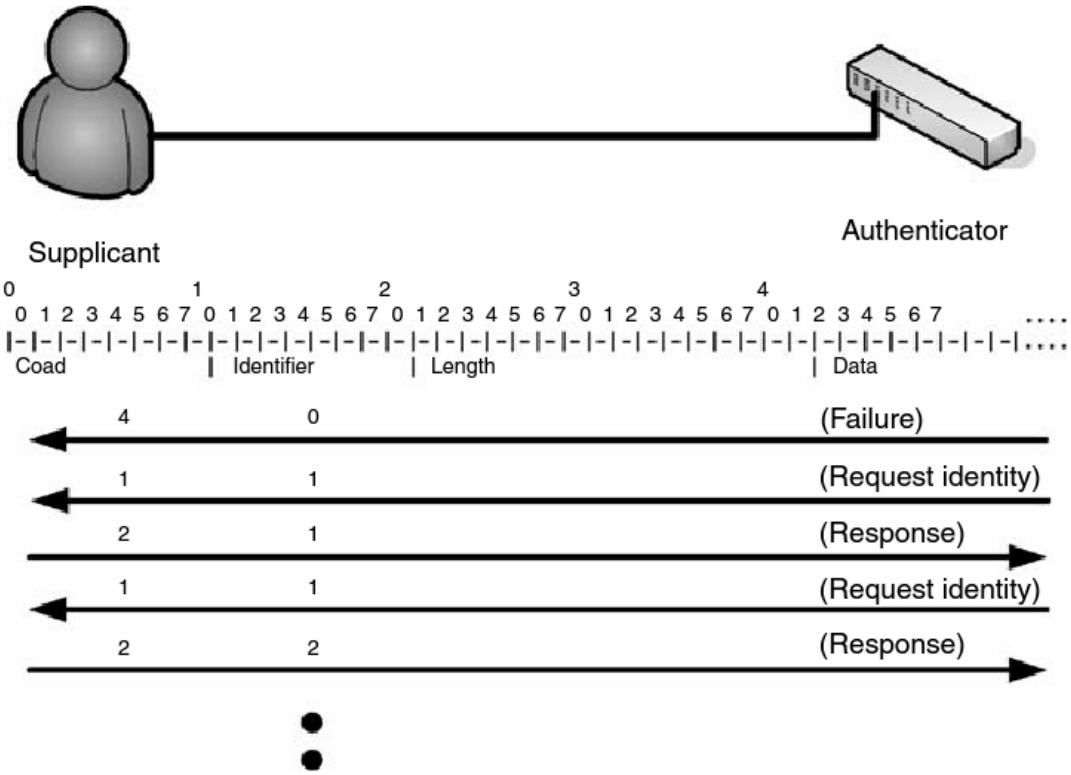
A responsabilidade do autenticador é garantir a resposta de cada requisição enviada. Isso é controlado com o processo lock-step, que é um método primitivo e garante um transporte confiável. O processo lock-step é um indicador que cada participante da conversa fala sobre a mesma informação. Por causa das requisições que originam do autenticador e das respostas que originam do suplicante, o autenticador sempre poderá ser quem indica a nova informação que

ocorre nessa troca, e o suplicante apenas responde para a requisição da informação atual.

O campo identificador é usado para implementar o lock-step. O autenticador irá configurar o identificador para um valor específico. O suplicante irá utilizar esse mesmo valor como resposta. O autenticador alterará esse valor do identificador para a próxima requisição e o suplicante, novamente, responderá com esse valor do identificador. O suplicante nunca saberá se a requisição foi recebida, baseado no valor do identificador, mas o autenticador sempre saberá.

Na figura 13 [5] apresenta o uso do identificador em uma típica conversa 802.1x entre o suplicante e o autenticador.

Figura 13 - Comunicação entre suplicante e autenticador



Fonte – Brown (2007, p. 54)

Nesse exemplo, o autenticador recebeu a resposta código “2” do suplicante. Ele então fará a tentativa de contatar o servidor de autenticação. Nessa tentativa vai conter os dados EAP inicialmente fornecidos pelo suplicante. Se a conversa é estabelecida com o servidor de autenticação com sucesso, o servidor enviará um *challenge*. Esse *challenge* é enviado pelo autenticador para o suplicante como um pacote *request-identity*. O autenticador modifica o identificador para um valor diferente daquele enviado no primeiro pacote. Assim, o autenticador está agindo apenas como um tradutor e guardião da porta. Durante as trocas com o suplicante, o autenticador controla a conversa no nível de transporte e não se interessa com o conteúdo que está sendo trocado no processo de autenticação.

Isso continua até o servidor de autenticação declarar bem sucedida ou mal sucedida a autenticação, e então o autenticador irá executar uma ação.

O autenticador se interessa no conteúdo do primeiro pacote da conversa originada do suplicante, a resposta do seu *request-identity*, e o último pacote, bem ou mal sucedido da resposta do servidor de autenticação.

2 ESTUDO DE CASO

2.1 Contextualização

A Câmara Legislativa do Distrito Federal - CLDF, no cumprimento de sua missão, busca sempre a melhoria da qualidade do atendimento, exigindo grandes esforços e uma postura pró ativa na obtenção de resultados práticos e objetivos. Por esta razão, em fevereiro de 2007 a Direção da Casa aprovou o Ato da Mesa Diretora nº 15 [13], que dispõe sobre a informatização da Câmara Legislativa do Distrito Federal.

Neste documento também foram estabelecidos critérios de segurança e privacidade, “Os equipamentos, sistemas e programas de informática devem ser protegidos contra fraude, violação, acesso indevido ou desautorizado, erro, acidente, contaminação por vírus, spam, spyware e outras ameaças” [13].

As atividades da CLDF são fortemente amparadas no uso intensivo de informação e de conhecimento. Por isso, a ampliação do uso e da disponibilidade de recursos de tecnologia da informação faz parte da estratégia institucional adotada para aumentar a capacidade de resposta da casa e melhorar os processos gerenciais.

A eventual indisponibilidade de sistemas corporativos produz impacto direto sobre a produtividade dos servidores e, consequentemente, sobre o desempenho institucional. Além disso, impactam também sobre os clientes externos, parceiros, e usuários do portal da CLDF na Internet, interessados nas informações e nos serviços direcionados aos órgãos públicos e à sociedade.

A disponibilidade das informações, para ser garantida, necessita de suporte proativo e reativo a eventuais falhas. A Coordenadoria de Gestão da Tecnologia da Informação – CGTI, atua fortemente no cumprimento dessas determinações a fim de aumentar a proteção dessas informações dos diversos tipos de ameaças para minimizar danos ao negócio e garantir sua continuidade.

Nesse sentido, a chefia do Setor de Infraestrutura - SEINF solicitou um estudo técnico para a implantação do protocolo 802.1x na rede ethernet da CLDF, com os seguintes objetivos específicos:

- autenticar todos os usuários da CLDF no momento de sua conexão sem comprometer o nível atual de desempenho e de confiabilidade da rede da CLDF;

- implantar políticas de acesso à rede de acordo com o papel de cada usuário;

- permitir ao usuário acesso a sua rede local e privilégios a partir de qualquer ponto da rede;

- identificar após a conexão, usuários mal intencionados utilizando a rede.

2.2 Infraestrutura de Tecnologia de Informação da CLDF

A Tecnologia da Informação pode ser definida como um conjunto de todas as atividades e soluções providas por recursos de computação.

Sendo a informação um bem que agrega valor a uma empresa ou a um indivíduo, é necessário usar os recursos de Tecnologia da Informação - TI de forma eficaz, utilizando ferramentas, sistemas ou outros meios que façam das informações um diferencial competitivo. Além disso, é necessário buscar soluções que tragam bons resultados, mas que tenham o menor custo possível.

A principal finalidade da infraestrutura de TI é a de disponibilizar em tempo integral o suporte aos serviços de informática da CLDF. Para tanto, se faz necessária a execução de planejamento que garanta o bom funcionamento dos componentes desta infraestrutura, dentre eles as máquinas servidoras, os softwares básicos, os equipamentos ativos de rede, o cabeamento físico, a estabilização da rede elétrica, o sistema ininterrupto de energia, o condicionamento de ar, etc.

A infraestrutura de Tecnologia da Informação da CLDF é administrada pelo Setor de Infraestrutura – SEINF, subordinado à Coordenadoria de Gestão da Tecnologia da Informação – CGTI, que é um órgão consultivo da Mesa Diretora da Câmara Legislativa do Distrito Federal.

Abaixo são apresentados os serviços de infraestrutura e recursos físicos necessários ao funcionamento dos serviços de informática da CLDF.

1) Armazenamento de arquivos: Serviço de armazenamento dos arquivos criados nas unidades.

2) Banco de dados: Serviço de armazenamento dos dados dos sistemas corporativos.

3) Backup: Serviço de cópia de segurança dos dados armazenados;

4) Acesso à Internet: Serviço que possibilita o acesso à Internet;

5) E-mail: Serviço de Correio Eletrônico;

6) Servidor de aplicativos: Serviço de hospedagem de sistemas de informação;

7) Equipamentos ativos da rede (backbone): Equipamentos que viabilizam a troca de dados entre os computadores da rede;

8) Instalações elétricas: Rede elétrica para uso dos equipamentos de informática;

9) Rede Elétrica estabilizada: Sistema ininterrupto de fornecimento de energia (no-break);

10) Rede física: Cabeamento e pontos de rede;

11) Ar condicionado: Sistema de refrigeração da sala dos equipamentos centrais.

2.3 Infraestrutura de rede da CLDF

Para atender a necessidade das diversas unidades da CLDF de conectar seus equipamentos de informática à rede da CLDF foram distribuídas 19 salas no prédio destinadas à instalação de switches de acesso à rede.

A conexão física entre esses switches de acesso e os switches do núcleo da rede é feita por meio de enlaces de fibra ótica com velocidade de 1 GBS ou de 10 GBS conforme necessidade de uso de banda.

Para a conexão entre os switches de acesso e o switch do núcleo foi configurado o *Link Aggregation Control Protocol* – LACP com dois enlaces de fibra, que oferece maior velocidade e/ou redundância do canal. Aumentado assim a disponibilidade.

2.3.1 Mapa da rede da CLDF

A rede da CLDF é composta por switches empilhados do fabricante 3Com modelo 5500, conforme topologia apresentada na figura 14:

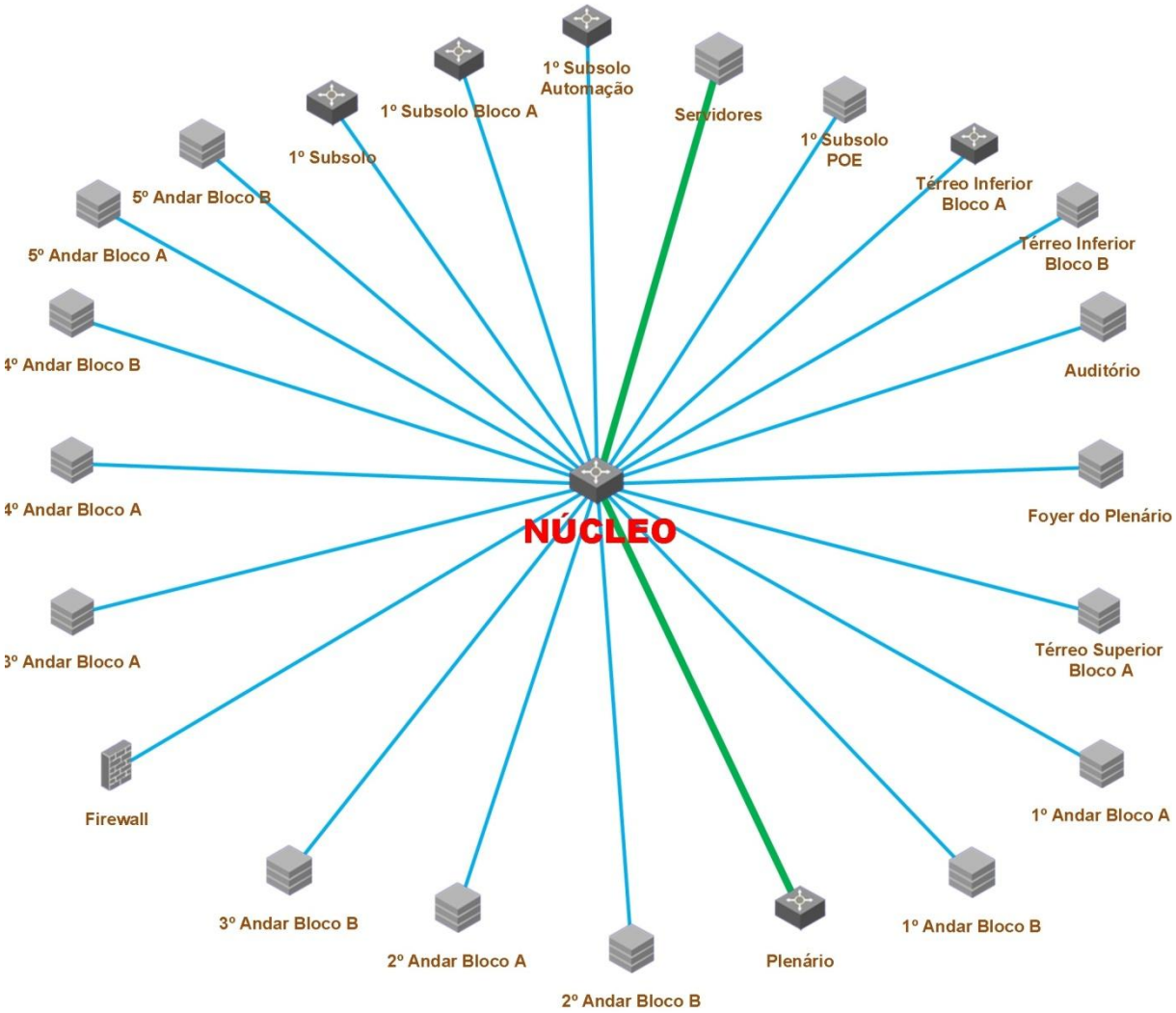


Figura 14 - Topologia da rede da CLDF
Fonte – Programa de Gerenciamento IMC

2.3.2 Segmentação da rede

Para atender alguns serviços que necessitam utilizar uma rede lógica independente, foram implementadas as seguintes VLANs na rede da CLDF:

- Interna;
– Áudio;
– Automação Predial;
– Circuito Fechado de TV - CFTV;
– Controle de Acesso - SCA;
– DMZ;
– GDFNet;
– Interlegis;
– Internet link1;
– Internet link 2;
– PABX;
– Terceiros.

2.3.3 Equipamentos nas unidades da CLDF

A CGTI tem como responsabilidade fornecer às unidades da Casa os recursos computacionais necessários ao andamento dos processos operacionais e decisórios.

Nos quadros a seguir são apresentados os microcomputadores, notebooks e impressoras existentes na CLDF.

Quadro 2 – Quantitativo de Microcomputadores

Microcomputadores

Tipo	**Descrição**	**Sistema Operacional**	**Quantidade**
Microcomputador	Lenovo Pentium D	Windows Vista	800
Microcomputador	Hp	Windows 7	250
Total			**1050**

Fonte: Inventário de rede da CLDF

Quadro 3 – Quantitativo de notebook

Notebooks

Tipo	**Descrição**	**Sistema Operacional**	**Quantidade**
Notebook	Lenovo	Windows Vista	40

Fonte: Inventário de rede da CLDF

2.3.4 Rede sem fio

Ainda não foi implantada na rede da CLDF uma solução corporativa de rede fio.

Existe um ponto de acesso sem fio instalado na rede para atender uma necessidade pontual do setor do Plenário. Somente notebooks de propriedade da

CLDF, com endereços MACs previamente cadastrados, acessam a rede através desse ponto de acesso.

O projeto para aquisição de uma solução de rede sem fio corporativa para a CLDF está em fase de elaboração de projeto de especificação técnica.

A nova rede sem fio está prevista para entrar em funcionamento a partir do início do ano de 2013.

2.4 Vulnerabilidade das portas dos switches

Para Brown [5], originalmente a rede de computadores não foi concebida tendo segurança como premissa. Ela não foi desenvolvida para oferecer proteção, mas para disponibilizar acesso.

Se for conectado um dispositivo, como um capturador de pacotes, a uma porta da rede, normalmente ele terá acesso a tudo que estiver trafegando. Algumas informações mais sensíveis provavelmente estarão protegidas no local que estão armazenadas, como exemplo em um servidor, mas no transporte da informação através da rede ela não estará protegida.

A comunicação entre os diversos dispositivos da rede podem ser feita para ocorrer de forma criptografada, porém não é um cenário geralmente implementado haja vista o alto custo dos investimentos demandados. Nesse sentido há uma solução oferecida pela empresa Microsoft conhecida como isolamento de domínio com uso do IPsec [14], que exige alto poder de processamento entre o dispositivos de comunicação envolvidos.

Um exemplo de ataque bem sucedido e, que causou impactos negativos à MIT - *Massachusetts Institute of Technology* foi realizado no ano de 2010 pelo

hacker Aaron Swartz, que teve acesso a uma sala reservada do MIT, e com um laptop conectado a uma porta da rede baixou mais de 4 milhões de trabalhos do acervo da JSTOR, uma biblioteca de artigos científicos digitalizados da MIT. Esse ataque poderia ter sido evitado caso as portas de acesso à rede tivessem com protocolo 802.1x habilitado [26].

Uma rede, sem a implementação de algum controle de restrição de acesso na porta do switch, está propensa a falhas que podem comprometer a confidencialidade, integridade e disponibilidade das informações. Abaixo alguns incidentes com maior risco de ocorrer considerando esse cenário:

- um usuário poderá cometer incidentes de segurança sem ser identificado;

- um dispositivo não autorizado, infectado por vírus, poderá disseminar esse vírus na rede;

- um dispositivo não autorizado poderá compartilhar programas não licenciados na rede e promover a “pirataria”;

- um dispositivo não autorizado poderá usar protocolos e/ou programas que estão em violação direta com as normas de segurança corporativa;

- um dispositivo não autorizado poderá provocar negação de serviço;

- um dispositivo não autorizado poderá interagir com dispositivos da rede e torna-los indisponíveis na rede.

3 TESTE DE CONCEITO

Para realização dos testes de implantação do IEEE 802.1x é necessária a configuração das seguintes entidades:

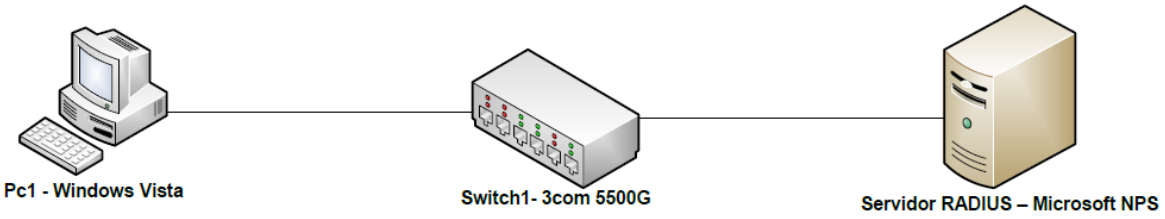
- servidor RADIUS;

- switches de rede que suportem o protocolo 802.1x;

- clientes da rede que suportem o protocolo 802.1x.

Na figura 15 é apresentado o esquema que as entidades serão configuradas no ambiente de teste:

Figura 15 - Esquema de entidades



Fonte: Ilustração nossa

3.1 Configuração do Servidor RADIUS

Dentre as soluções de servidores RADIUS disponíveis no mercado destacamos o FreeRadius [15] utilizado pelos sistemas operacionais Linux e o Network Policy Server utilizado pelos sistemas Windows Microsoft [16].

A solução RADIUS escolhida para ser utilizada como sistema servidor de autenticação para os clientes 802.1x foi o NPS da Microsoft, já que o serviço de

diretório utilizado pela CLDF é Active Directory Windows Server 2008 desenvolvido pela própria Microsoft. Assim, configurar o NPS no ambiente atual é mais simples que configurar demais soluções RADIUS disponíveis.

3.1.1 Servidor NPS

Network Policy Server – NPS é uma implementação RADIUS da Microsoft para sistemas operacionais Windows Server 2008 e Windows Server 2008-R2 que substituiu a implementação Internet Authentication Service – IAS nativa do sistema operacional Windows Server 2003 [16].

O NPS realiza de forma centralizada a autenticação, autorização e *accounting* das conexões de vários tipos de acessos à rede, incluindo conexões de rede sem fio e Virtual Private Network – VPN.

3.1.2 Configuração

O NPS é instalado utilizando o assistente de instalação Roles do Windows 2008. O NPS é um serviço do *role Network and Access Service*.

Uma vez que o NPS foi instalado e reiniciado, o servidor Radius pode começar a ser configurado.

O NPS deve ser iniciado a partir da opção do menu *Network Policy Server* localizado no grupo de Ferramentas Administrativas.

A criação da política Radius pode ser feita com o assistente do Network Access Protection (NAP). Basta selecionar servidor RADIUS 802.1X para redes sem

fio ou conexões com fio na tela inicial do NPS e clique em Configure NAP. Neste estudo foi selecionada a opção Secure Wired (Ethernet) Connections.

Os parâmetros utilizados para a configuração do servidor RADIUS estão descritos no Apêndice A.

3.2 Configuração dos switches

O switch utilizado para realização dos testes foi o modelo 5500G do fabricante 3COM, que atende os requisitos para ser configurado como um autenticador 802.1x [6].

Este switch possui uma interface de comando de linha para que o usuário interaja com o dispositivo. Por meio dessa interface o usuário configura o switch e visualiza as informações de saída para verificar as configurações e o estado de funcionamento.

As configurações básicas do protocolo 802.1x no switch 5500G da 3com estão descritas no Anexo A [6].

3.3 Configuração dos clientes

Como já apresentado anteriormente as estações de trabalho da rede da CLDF são formadas por clientes Microsoft Windows Vista e Windows 7.

Para a instalação do protocolo 802.1x, a estação de trabalho do cliente deve ser previamente configurada como membro do domínio da rede. Isso deve ser feito utilizando uma porta do switch sem o protocolo 802.1x ativo.

Com o cliente conectado a uma porta do switch com o 802.1x ativo, deve ser habilitado o serviço de Configuração Automática de Rede com Fio, que é desativado por padrão.

Demais configurações de rede devem ser feitas utilizando os seguintes parâmetros:

- habilitar a obtenção automática de endereço IP.

- habilitar a autenticação IEEE 802.1x para a rede.

- escolher o método de autenticação de rede: Microsoft EAP protegido (PEAP)

- verificar e validar o certificado do servidor NPS (RADIUS).

3.4 Resultados

Com a implementação do protocolo 802.1X no ambiente simulado, foi verificado que é possível aumentar a segurança contra acesso físico não autorizado a um segmento da rede da CLDF.

Com a restrição dos acessos indevidos, providos a partir dos segmentos da rede local, é possível garantir que um dispositivo não consiga se conectar fisicamente aos segmentos da rede, protegendo assim os seus serviços.

O protocolo 802.1X tem a função de garantir que todas as portas físicas disponíveis para acesso à rede com fio, sejam monitoradas pelo servidor RADIUS, forçando dessa forma que todos os usuários da rede estejam com a conta da rede e senhas válidas para que a solicitação de acesso à rede seja atendida.

Os métodos disponíveis no ambiente, o EAP-TLS e o PEAP-MS-CHAPv2, proporcionam um nível de segurança elevado para garantir os acessos aos segmentos de rede, o padrão adotado foi o método PEAP-MS-CHAPv2.

Para a adoção do método EAP-TLS é necessário um certificado digital para cada conta de computador do domínio. Neste caso, uma Infraestrutura de Chave Pública - ICP deve ser implantada no ambiente da rede da CLDF para emissão e gerenciamento de Certificados Digitais.

Para Brown [5], embora o método EAP-TLS torne o ambiente de segurança mais robusto, possui a grande desvantagem do custo financeiro exigido para a administração ou para a aquisição de certificados. Se os certificados não são comprados a partir de uma autoridade reconhecida pelos dispositivos na rede, então uma Infraestrutura de Chave Pública deve ser estabelecida dentro da rede. Em ambos os casos, o custo da execução, em dinheiro ou experiência, pode ser significativo. O ambiente que implementa a autenticação baseada em certificados se torna mais complexo e requer um maior nível de administração.

O método PEAP-MS-CHAPv2 possui a garantia de que somente usuários previamente registrados tenham acesso ao segmento de rede de serviço, porém esse método, diferentemente do EAP-TLS, atende apenas à política de validação da conta de usuário e do computador no domínio, através de um canal protegido para verificação e validação das informações da conta e senha do usuário, juntamente

com a conta do computador e verifica se a mesma possui permissão de acesso no domínio.

O processo de autenticação do PEAP-MS-CHAPv2 ocorre em duas partes. A primeira parte é usada para estabelecer um túnel entre o suplicante e o servidor de autenticação, e a segunda parte é a autenticação da credencial. Uma vez estabelecido o túnel, outro método EAP é usado para a autenticação das credenciais dos usuários.

O fluxo do PEAP é também similar aos outros métodos 802.1x. O autenticador envia um *request-identity* e o suplicante responde. O autenticador encaminha para o servidor de autenticação, o servidor responde com um *challenge* para início do PEAP. Nesse ponto é iniciado um túnel TLS.

O PEAP aproveita o TLS para criar um túnel seguro que é usado para transportar as credenciais. Um método inteiramente diferente é encapsulado dentro do túnel TLS. O método mais popular é o EAP MS-CHAP2-V2. Como as credenciais trocadas estão dentro de um túnel não há possibilidades dessas informações serem vistas por meio de *snooping*.

A implementação do método sem a utilização de um túnel TLS deixará a autenticação vulnerável a um ataque para roubo de senha de usuário durante a troca de credenciais. Apesar do protocolo MSCHAPv2 parecer complexo, ele utiliza o algoritmo MD4 para gerar o hash da senha do usuário, que cria três chaves Data Encryption Standard – DES. Por causa da fraqueza na construção do DES, é possível que um atacante consiga facilmente recuperar estas chaves em qualquer método MS-CHAPv2 independente do tamanho e da complexidade da senha [17].

A autenticação e autorização de acesso ficam sob a responsabilidade do servidor RADIUS, onde todas as requisições da rede serão encaminhadas por seus clientes RADIUS para validação. O servidor possui as políticas de acesso determinando os métodos de autenticação que são solicitados às estações de trabalho. O servidor RADIUS ainda é capaz de auditar a utilização de banda, períodos de conexão entre outras informações através do RADIUS *accounting*.

Todos os eventos de acesso foram registrados pelo NPS (RADIUS). Para isso foi feita a configuração da opção "accounting" para salvar os logs de acesso na pasta c:\windows\system32\LogsFile. Assim foi possível exibir os logs de acesso de todos os usuários, por nome de usuário, IP, mac address, data e horário de acesso. Portanto os usuários mal intencionados poderão ser identificados.

3.5 Considerações e Problemas encontrados

Para diminuir os riscos de acessos não autorizados é desejável que todas as portas de rede tenham autenticação 802.1x habilitadas, com a exceção de lugares onde a segurança física é estritamente mantida, como por exemplo o CPD.

Manter em um mesmo segmento de rede portas autenticadas e portas sem autenticação é deixar vulnerabilidade para ser explorada por um atacante. Isso significa que todos os equipamentos de rede deverão suportar e estar configurado com autenticação, o que implica em um custo para fazer upgrade do equipamento de rede atual.

Todavia, se não for viável a substituição dos equipamentos de rede, como as impressoras que não suportem autenticação 802.1x, as portas por eles utilizadas

terão que ser identificadas e colocadas em VLANs "inseguras", isoladas via firewall das VLANs "seguras" que exigem autenticação de porta [19].

A rede da CLDF possui, ainda em produção, dois modelos de impressoras que não suportam a autenticação 802.1x: Lexmark T520 e Xerox P8E.

Enquanto não forem substituídas, essas impressoras deverão ser instaladas em VLANS dedicadas somente para serviço de impressão e configuradas com autenticação por mac address para acessarem a rede. Entre essa rede e a rede interna deve ser instalado um servidor de impressão com duas interfaces de rede – uma para a rede de impressoras e outra para a rede interna.

Além das impressoras, existem outros equipamentos que não suportam a autenticação 802.1x. Estes equipamentos estão instalados em VLANS isoladas, destinadas à diferentes serviços oferecidos pela rede:

– Áudio;

– Automação Predial;

– Circuito Fechado de TV - CFTV;

– Controle de Acesso - SCA;

– Interlegis;

– PABX;

A comunicação dessas redes com a rede interna é realizada por meio de um firewall que só permite o tráfego de dados de monitoramento e de gerência.

Dessa forma teremos um ambiente seguro com controle de acesso à porta somente na rede interna. Isso não é uma solução ideal haja vista que os dispositivos pertencentes a cada VLAN continuarão vulneráveis a determinados

tipos de ameaças. Uma solução seria que todos os equipamentos que não suportem autenticação fossem gradativamente substituídos por equipamentos com suplicantes 802.1x.

Conforme relatado no site da Microsoft [18], existe uma fraqueza importante no protocolo 802.1x. Ele autentica apenas no momento de estabelecimento de uma conexão. Assim que o suplicante autentica e a porta do switch é aberta, as demais comunicações entre o suplicante e o switch não são autenticadas. Isto cria uma situação na qual é possível para um invasor fazer parte da rede.

A falta de autenticação sucessiva por pacote do 802.1X cria a situação de um ataque *man-in-the-middle*. O 802.1X autentica apenas a conexão, depois ele assume que todo o tráfego que passa pela conexão é legítimo. Esta seria a principal falha do 802.1X, que para ser explorada requer acesso físico à porta do switch. Esse acesso físico que pode ser feito com o uso de um dispositivo como um hub, que expande a porta do switch. Alem disso, é necessário que o atacante conheça informações do endereço IP e do endereço MAC *Address* do dispositivo conectado na porta a ser atacada. Essas informações dos dispositivos serão utilizadas para fazer *spoofing* dos endereços IP e mac-address, necessárias para que um computador não autorizado ingresse na rede pela mesma porta do switch.

Uma opção para mitigar essa falha seria habilitar a funcionalidade de *reauntenticação* do 802.1x no sistema autenticador, bem como definir um intervalo de tempo entre cada *reauntenticação* em um valor mínimo possível. No caso do switch utilizado em laboratório o tempo padrão de *reauntenticação* foi de 3600 segundos [6].

A comunicação entre os diversos dispositivos da rede poderia ser implementada para ocorrer de forma criptografada, porém não é um cenário viável para implementação haja vista o alto custo dos investimentos demandados. Nesse sentido há uma solução oferecida pela empresa Microsoft conhecida como isolamento de domínio com uso do IPsec [19], que exige alto poder de processamento entre os dispositivos de comunicação envolvidos.

Alguma soluções tecnológicas de segurança propõem cumprir o papel de verificação e atualização do sistema antes de seu ingresso efetivo na rede. Estas soluções são conhecidas como *Network Access Control* – NAC e se apresentam como solução de segurança de acesso à rede que utilizam o protocolo 802.1x como parte da implementação da segurança.

Dentre as soluções NAC mais conhecida podemos citar:

Network Admission Control *[20]*: Conjunto de tecnologias (software e hardware) que utilizam a rede para aplicar políticas de segurança e verificar conformidade dos dispositivos.

Trusted Network Connect [21]: O acesso à rede ocorre através de dispositivos que aplicam as políticas de acesso. Permite múltiplos fabricantes e garante interoperabilidade a todos os dispositivos da rede.

Network Access Protection *[22]*: Provê acesso protegido a recursos da rede, restringindo o acesso baseado na avaliação do usuário do ambiente Windows. O NAP necessita interação com os dispositivos de rede.

CONCLUSÃO

Os resultados obtidos durante a realização dos testes demonstram que a autenticação 802.1x, utilizando o método PEAP-MS-CHAPv2, pode ser realizada na rede da CLDF. A autenticação é feita com o uso das mesmas credenciais dos usuários utilizadas para fazer *login*, ocorrendo de forma transparente.

Esse método facilita a implantação desse tipo de solução, já que o usuário com conta válida cadastrada no domínio não terá seu procedimento de acesso à rede alterado. Assim os usuários continuarão a ter acesso à rede com mesmos privilégios a partir de qualquer ponto da mesma.

Os testes comprovaram também que a solução utilizando um controlador de domínio integrado ao suplicante nativo do sistema operacional para o processo de autenticação no momento do *logon*, mostrou-se efetivo para o acesso à rede. Esse cenário é o encontrado em toda rede da CLDF, onde todo o serviço de diretório da rede é realizado pelo Active Directory Windows 2008 da Microsoft e os sistemas operacionais instalados nas estações de trabalho são nativos do Microsoft Windows, sendo eles Windows Vista e Windows 7.

A utilização do método EAP-TLS permite uma autenticação mais confiável, porém sua utilização no momento não se mostra viável, pois não existe disponibilidade financeira da CLDF para investir em aquisição de certificados digitais, nem recursos humanos para a implantação de uma Infraestrutura de Chave Pública da própria CLDF.

A implementação da solução na rede da CLDF, no mesmo modelo que foi realizado no ambiente teste, não demandará custo financeiro adicional com

aquisição de software e hardware, porém será necessário investimento financeiro em treinamento e contratação de serviços de terceiros para implementar a solução.

Os testes realizados em laboratório não demonstraram nenhuma falha de autenticação utilizando o protocolo 802.1x, porém há estudos que relatam a existência de vulnerabilidade pela falta de autenticação sucessiva por pacote do protocolo, que cria a situação de um ataque *man-in-the-middle*.

Para a implementação do 802.1x é necessário que os dispositivos sem suplicante 802.1x sejam colocados em VLAN "insegura" isoladas da VLAN “segura” e que utilizem a autenticação por mac address para acessarem a rede.

Embora o protocolo 802.1x não tenha resolvido por completo os problemas de segurança relacionados ao controle de acesso à porta do switch, ele ainda permanece como uma solução importante que torna muito mais difícil um intruso explorar as informações que trafegam em uma rede.

Diante do exposto, concluímos que a autenticação 802.1x é um protocolo que deve ser implantado na rede da CLDF. Ele oferece nível de resistência e proteção que complementa outros controles de segurança já implementados na CLDF, sendo assim cumprirá o objetivo de diminuir os riscos dificultando acessos indevidos.

Para estudos futuros deverá ser realizado trabalho técnico para levantamento de solução de segurança que resolva os problemas de vulnerabilidades a ameaças, como um *man-in-the-middle* e, também solucione questões como a autenticação de dispositivos que não possuem clientes suplicantes.

REFERÊNCIAS

[1] SÊMOLA, Marcos. *Gestão da Segurança da Informação*. Rio de Janeiro: Campus, 2003. 156 p.

[2] IEEE - Institute of Electrical and Electronics Engineers. *Port-Based Nerwork Access Control. Padrão IEEE 802.1x*. New York, 2010.

[3] ABNT. *ISO/IEC 17799: Código de Prática para a Gestão da Segurança da Informação*. Rio de Janeiro: 2001.

[4] MORAES, Alexandre Fernandes de. *Redes Sem Fio – Instalação, Configuração e Segurança*. São Paulo. Érica, 2010. 284 p.

[5] BROWN, Edwin Lyle*. 802.1x Port-Base Authentication*. United States of America: Taylor & Francis Group, 2007. 254 p.

[6] *3COM SWITCH 5500 FAMILY CONFIGURATION GUIDE*. Marlborough, 2007.1049 p.

[7] TANENBAUM, Andrew S. *Redes de Computadores*. Rio de Janeiro: Campus, 2003. 945 p.

[8] INTERNET ENGINEERING TASK FORCE. *RFC 2865: Remote Authentication Dial In User Service. California*, 2000. 77 p.

[9] INTERNET ENGINEERING TASK FORCE. *RFC 3579: Remote Authentication Dial In User Service*. California, 2003. 46 p.

[10] CHAVES, Rodrigues Alves. *Estudo de Caso: Autenticação IEEE 802.1x Baseada no Protocolo Radius e Serviço de Diretório LDAP Aplicado a Rede GIGAFOPNET*. Ouro Preto, 2010. 110 p.

[11] HASSELL, Jonathan. *RADIUS*. United States of America: O'Reilly, 2002.

[12] Moraes, Alexandre M. S. P. *Autenticação, Autorização e Accounting: Conceitos Fundamentais*. Disponível em: <http://alexandremspmoraes.wordpress .com/2013/02/15/autenticacao-autorizacao-e-accounting-conceitos-fundamentais>. Acesso em: 23 abr. 2013.

[13] BRASIL. *ATO DA MESA DIRETORA n. 15, de 7 fevereiro de 2007*. Dispõe sobre a informatização da Câmara Legislativa do Distrito Federal. Lex: Diário Oficial da Câmara Legislativa do Distrito Federal, Brasília. Legislação Distrital.

[14] MICROSOFT TECHNET. *Segurança na Microsoft*. Disponível em: <http://blogs.technet. com/b/fcima/archive/2006/10/30/o-que-voc-precisa-saber-antes-de-implementar-802-1x-em-redes-com-fio.aspx >. Acesso em: 08 jul. 2012.

[15] *Freeradius*. Disponível em: <http://www.freeradius.org/ Acesso em: 18 abr 2013.

[16] MICROSOFT TECHNET. *Network Policy Server*. Disponível em: <http://technet. microsoft.com/en-us/network/bb629414.aspx>. Acesso em: 23 jun. 2012.

[17] THE RUCKUS ROOM*. Another Wi-Fi Crack UP*. Disponível em: <http://www. theruckusroom.net/2012/08/the-annual-defcon-event-is-notorious-for-introducing-new-cracks-attacks-and-hijacks-to-the-computer-and-network-security-in.html>. Acesso em: 27 ago. 2012.

[18] MICROSOFT TECHNET. *Network Policy Server*. Gerenciamento de Segurança. Disponível em: <http://www.microsoft.com/brasil/technet/seguranca /colunas/sm0805. mspx>. Acesso em 08 jul. 2012.

[19] MICROSOFT TECHNET. *Segurança na Microsoft*. Disponível em: <http://blogs.technet. com/b/fcima/archive/2006/10/30/o-que-voc-precisa-saber-antes-de-implementar-802-1x-em-redes-com-fio.aspx >. Acesso em: 08 jul. 2012.

[20] *NAC Solution And Technology Overview*. Disponível em <http://www.inf ormit .com/content/images/ 1587052253 /samp lechapter/1587052253ch1.pdf> Acesso em 18 abr. 2013.

[21] *Trusted Network Connect* . Disponível em <http://www.trustedcomput inggroup.org/developers/trusted_network_connect.> Acesso em 18 abr. 2013.

[22] MICROSOFT TECHNET. *Network Access Protection for Windows Server 2008*. Disponível em <http://www.microsoft.com/ brasil/servidores/windows server2008/net work-access-protection.mspx>. Acesso em 18 abr. 2013.

[23] PALMA, Luciano; PRATES, Rubens. *TCP/IP* – Guia de Consulta Rápida. São Paulo: Novatec, 128 p.

[24] MICROSOFT CORPORATION. *Deployment of IEEE 802.1X for Wired Networks Using Microsoft Windows*. California, 2005. 36p.

[25] BRASIL. *RESOLUÇÃO n. 34, de 24 de fevereiro de 1992*. Dispõe sobre... Lex: Diário Oficial da Câmara Legislativa do Distrito Federal, Brasília. Legislação Distrital.

[26] O Globo Tecnologia. <http://oglobo.globo.com/tecnologia/aaron-swartz-hacker-fundador-do-reddit-comete-suicidio-aos-26-anos-7278368>. Acesso em 24 abr. 2013.

APÊNDICE A – Parâmetros para configuração do servidor RADIUS NPS

- Tipo de conexão 802.1x: Secure Wired (Ethernet) Connections;
- Nome do cliente (switch) : switch1;
- Endereço Ip do Cliente: 192.168.1.10;
- Segredo compartilhado: passwd****;
- Tipo de EAP: Secured password (EAP-MSCHAP v2);
- Grupo de usuários para aplicar políticas: cldf\Teste-8021x;
- Nome do fabricante do switch: RADIUS Standard.

ANEXO A – Parâmetros para configuração do switch 3com 5500G

Habilitar o 802.1x como configuração global:

- <5500> system-view

- [5500] dot1x

Habilitar o 802.1x na porta Ethernet 1/0/1:

- [5500] dot1x interface Ethernet 1/0/1

Configurar o método de controle de acesso para MAC-based:

- [5500] dot1x port-method macbased interface Ethernet 1/0/1

Criar um scheme RADIUS com o nome radius1:

- [5500] radius scheme radius1

Definir endereço do servidor RADIUS primário de autenticação e “accounting”.

- [5500-radius-radius1] primary authentication 192.168.1.100

- [5500-radius-radius1] primary accounting 192.168.1.100

Definir endereço do servidor RADIUS secundário de autenticação e *accounting*.

- [5500-radius-radius1] secondary authentication 192.168.1.100

- [5500-radius-radius1] secondary accounting 192.168.1.100

Configurar a senha para que o switch e o servidor RADIUS de autenticação troquem mensagens.

- [5500-radius-radius1] key authentication passwd1234

Configurar a senha para que o switch e o servidor RADIUS “accouting” troquem mensagens.

- [5500-radius-radius1] key accounting passwd1234

Configurar o intervalo e o número de tentativas para o switch enviar pacotes para o servidor RADIUS.

- [5500-radius-radius1] timer 5

- [5500-radius-radius1] retry 5

Configurar o interval que o switch envia real-time accounting packets para o servidor RADIUS:

- [5500-radius-radius1] timer realtime-accounting 15

Configurar para enviar o nome de usuário para o servidor RADIUS com o nome de domínio truncado:

- [5500-radius-radius1] user-name-format without-domain

- [5500-radius-radius1] quit

Criar o domínio com o nome cl.df.gov.br:

- [5500] domain enable cl.df.gov.br

Especificar para que o radius1 seja adotado com um esquema RADIUS do domínio do usuário. Se o servidor RADIUS for inválido, especificar para adotar esquema de autenticação local.

-[5500-isp-aabbcc.net] scheme radius-scheme radius1 local

Especificar o número máximo de números de usuário que o domínio pode acomodar (30):

- [5500-isp-aabbcc.net] access-limit enable 30

Habilitar a função desconectar se ocioso e definir os parâmetros relacionados:

-[5500-isp-aabbcc.net] idle-cut enable 20 2000

- [5500-isp-aabbcc.net] quit

Definir o domínio de usuário padrão para ser cl.df.gov.br

- [5500] domain default enable cl.df.gov.br

Criar conta de usuário de acesso local

- [5500] local-user localuser

- [5500-luser-localuser] service-type lan-access

- [5500-luser-localuser] password simple localpass