**FACULDADE DE TECNOLOGIA SENAC GOIÁS**

ALEXANDRE COSTA SANTOS

ALESSANDRO MIGUEL MANSO

DEUSAIR WELLIGNTON PEREIRA

**PROJETO INTEGRADOR**

**MODULO V**

**Gestão da Tecnologia da Informação**

**Projeto de Redes**

**Professor: Kelli**

Goiânia

2017

**Sumario**

DEFINIÇÃO..........................................................................03

CARACTERISTÍCAS............................................................03

SOLUÇÕES PARA REDE WARELESS...............................04

Sobre o FreeRADIUS.............................................................05

Instalar e configurar Freeradius no UBUNTU........................06

Bibliografia..............................................................................08

**DEFINIÇÃO**

IEEE 802.1X é um padrão IEEE para controle de acesso à rede com base em portas; faz parte do grupo IEEE 802.1 de protocolos de redes de computadores. Provê um mecanismo de autenticação para dispositivos que desejam juntar-se a uma porta na LAN, seja estabelecendo uma conexão ponto-a-ponto ou prevenindo acesso para esta porta se a autenticação falhar. É usado para a maioria dos Access points sem fio 802.11 e é baseado no Protocolo de Autenticação Extensiva (EAP).

**CARACTERISTÍCAS**

Um nó wireless precisa autenticar-se antes de poder ter acesso aos recursos da LAN. 802.1X provê autenticação baseada em portas, que envolve comunicação entre o requisitante, o autenticador e o servidor de autenticação. O requisitante é comumente o software em um dispositivo cliente, como um laptop, o autenticador é um Switch Ethernet ou Access Point sem fio, e a autenticação geralmente uma base de dados RADIUS. O autenticador atua como uma proteção secundária à rede. Não é permitido ao requisitante (ex.: dispositivo cliente) acesso através do autenticador ao lado protegido da rede até que a identidade do requisitante seja autorizada. Uma analogia a isso é prover um passaporte válido em um aeroporto antes de ser permitida a passagem pela segurança até o terminal. Com a autenticação baseada em portas 802.1X, o requisitante provê credenciais como nome de usuário / senha ou certificado digital, ao autenticador, e ele encaminha as credenciais até o servidor de autenticação para verificação. Se as credenciais são válidas (na base de dados do servidor de autenticação), o requisitante (dispositivo cliente) é permitido acessar os recursos localizados no lado protegido da rede.

Sob detecção do novo cliente (requisitante), a porta na switch (autenticador) é habilitada e mudada para o estado “não-autorizado”. Neste estado, apenas tráfego 802.1x é permitido; outros tráfegos, como DHCP e HTTP, são bloqueados na camada de enlace. O autenticador envia a identidade de autenticação EAP-request' ao requisitante, que por sua vez responde com o pacote EAP-response que o autenticador encaminha ao servidor de autenticação. Se o servidor de autenticação aceitar a requisição, o autenticador muda o estado da porta para o modo “autorizado” e o tráfego normal é autorizado. Quando o

requisitante efetua um logoff, envia uma mensagem EAP-logoff para o autenticador. O autenticador então, muda sua porta para o estado “não-autorizado”, bloqueando novamente todo o tráfego não-EAP.

implementa 802.1X para *access points wireless* para corrigir as vulnerabilidades de segurança encontradas em WEP. O papel do autenticador é realizado tanto pelo *Access point* em si via chave-pré-compartilhada (referida também como **WPA2-PSK**) ou para empresas maiores, por identidade terceira, como um servidor RADIUS. Ele provê autenticação apenas para o cliente ou, mais apropriadamente, autenticação forte e mútua utilizando protocolos como EAP-TLS.

**SOLUÇÕES PARA REDE WARELESS**

Para ajudar os usuários que estão enfrentando problemas de conectividade de rede, a Microsoft introduziu o Network Diagnostics Framework (NDF) no Windows Vista®. O NDF foi projetado para simplificar e automatizar muitas das etapas e soluções de solução de problemas comuns para problemas relacionados à rede.

O NDF é um conjunto de tecnologias que permite que uma coleção de solucionadores de problemas ajude os usuários a diagnosticar e, quando possível, corrigir automaticamente os problemas de rede. Quando um usuário experimenta um problema de rede, o NDF fornece a capacidade de diagnosticar e reparar muitos problemas comuns por meio da avaliação de diagnósticos. E nos casos em que não é possível fazer uma correção automática, o NDF é frequentemente capaz de fornecer ao usuário resolução para corrigir problemas.

No Windows Server® 2008 R2 e Windows® 7, a funcionalidade NDF é estendida pela integração com outros novos recursos do Windows 7, como o recurso Solução de problemas no Painel de Controle, rastreamento de rede usando o ETW (Event Tracing for Windows) e uma nova linha de comando Netsh contexto, Netsh Trace, que fornece recursos avançados de rastreamento.

Usando o Network Diagnostics Framework e o Network Tracing para solucionar problemas de conectividade

O guia, Usando o Network Diagnostics Framework e o Network Tracing para solucionar problemas de conectividade, fornece informações conceituais e exemplos de cenários que demonstram como você pode usar o NDF para identificar e reparar muitos problemas comuns de conectividade.

Aplica-se a: Windows 8.1, Windows Server 2012 R2

Este tópico fornece informações sobre os novos recursos do Acesso sem Fio Autenticado 802.1X no Windows Server 2012 R2 e no Windows 8.1.

A autenticação IEEE 802.1X fornece uma barreira de segurança adicional à sua intranet que você pode usar para impedir que computadores convidados, não autorizados ou não gerenciados que não podem realizar uma autenticação bem-sucedida se conectem à sua intranet.

Pelo mesmo motivo que os administradores implantam a autenticação IEEE 802.1X para redes com fio IEEE 802.3 - segurança aprimorada - os administradores de rede desejam implementar o padrão IEEE 802.1X para ajudar a proteger suas conexões de rede sem fio. Assim como um cliente com fio autenticado deve enviar um conjunto de credenciais para ser validado antes de poder enviar quadros pela intranet Ethernet com fio, um cliente sem fio IEEE 802.1X também deve executar a autenticação antes de poder enviar tráfego pelo seu ponto de acesso sem fio ( AP) e pela rede.

Se você implantou métodos de autenticação 802.1X com base em senha para conexões com fio e sem fio através de comutadores Ethernet e pontos de acesso sem fio, os usuários com computadores e dispositivos não associados ao domínio que executam o Windows 8.1 e o Windows Server 2012 R2 podem trazer seus próprios dispositivos para o organização e aproveitar as vantagens da reutilização de credenciais baseada em senha.

Quando métodos de autenticação EAP (Extensible Authentication Protocol) e EAP protegido (EAP) baseados em senha são implantados, os usuários finais podem fornecer suas credenciais na primeira vez que se conectam à rede da organização e se conectarem a todos os recursos desejados sem serem solicitados repetidamente para suas credenciais, porque as credenciais são armazenadas no computador local para reutilização.

Isso é especialmente útil para usuários que estão se conectando a vários recursos de rede, como sites de intranet corporativa, impressoras corporativas e aplicativos de linha de negócios.

Por motivos de segurança, quando o computador ou o dispositivo do usuário se desconecta da rede, as credenciais armazenadas são descartadas.

Esse recurso está disponível para computadores e dispositivos não associados ao domínio que executam o Windows 8.1 e o Windows Server 2012 R2 quando você implementou os seguintes métodos de autenticação em sua rede.

* EAP com o protocolo Microsoft Challenge Handshake versão 2 (EAP-MS-CHAP v2)
* PEAP-EAP-MS-CHAP v2
* EAP-TTLS com EAP-MS-CHAP v2

**Sobre o FreeRADIUS**

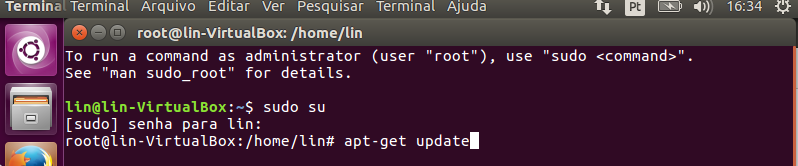
O FreeRADIUS foi fundado em junho de 1999 por Miquel van Smoorenburg e Alan DeKok. O primeiro lançamento "alfa" público do código foi em agosto de 1999, com 0,1 sendo lançado em maio de 2001. Desde então, novas versões foram lançadas a cada poucos meses.

Desde então, o projeto cresceu para incluir suporte a mais tipos de autenticação do que qualquer outro servidor de código aberto. É usado diariamente por [100 milhões de pessoas](https://freeradius.org/about/#usage_statistics) para acessar a Internet. Existem mais de 50 mil sites usando o FreeRADIUS, variando em tamanho de 10 usuários para mais de 10 milhões de usuários.

Desde a sua fundação, o projeto foi expandido para incluir vários outros [produtos relacionados ao RADIUS](https://freeradius.org/sub_projects/) , incluindo:

[freeradius-client](https://github.com/FreeRADIUS/freeradius-client) Uma biblioteca cliente RADIUS licenciada por BSD.   
[mod\_auth\_radius](https://github.com/FreeRADIUS/mod_auth_radius) Um módulo RADIUS para o Apache 1.xe 2.x.   
[pam\_radius\_auth](https://github.com/FreeRADIUS/pam_radius) Um Pluggable Authentication Module (PAM) para autenticação e contabilidade RADIUS.

**Instalar e configurar Freeradius no UBUNTU**

**Primeiro passo e mandar um comando de update para atualizar repositorio e evitar falhas na instalação**

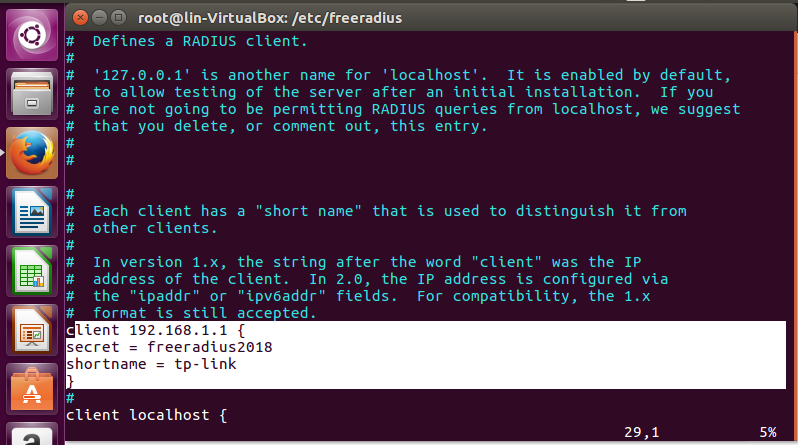
**Agora instalar o servidor FreeRADIUS com comando apt-get:**

****

**Acessar a pasta do arquivo:**

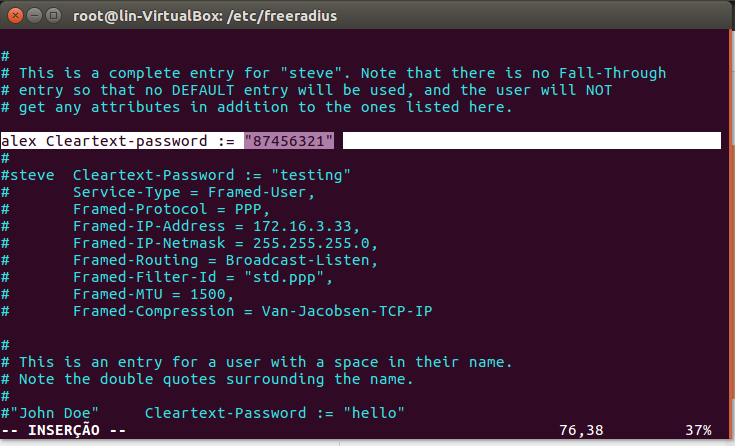
****

Acessar arquivo e configurando cliente /AP



Entrar na pasta users e configurar cliente:

Conforme mostrado abaixo deve-se inserir uma linha conforme modelo abaixo:

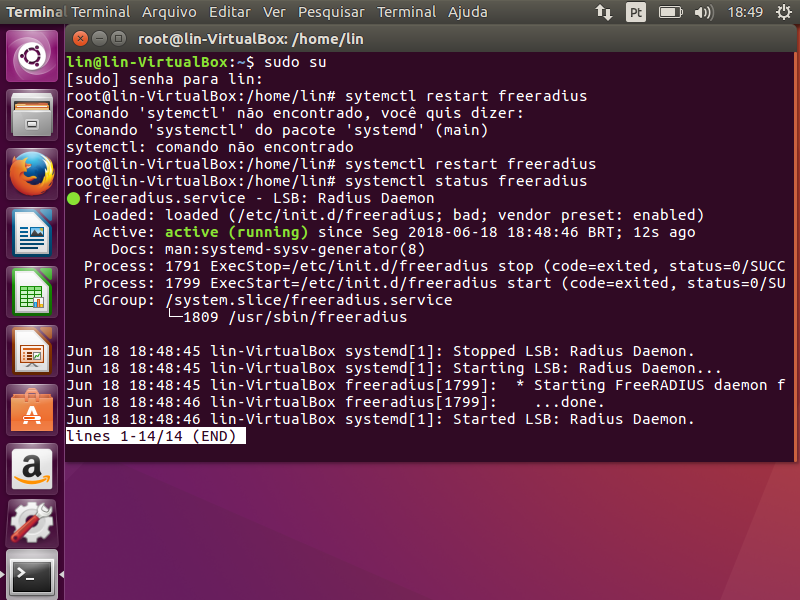
“nome do usuário” Cleartext-Password := “senha”

**Com cliente já configurado reiniciar o FreeRADUIS**

****

**Verifique a situação para ver se a configuração está ok**





**Bibliografia:**

https://pt.wikipedia.org/wiki/IEEE\_802.1X

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ee731908(v=ws.10)

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn452409(v=ws.11)

Projeto de Redes de Computadores

Professor(es) responsável(is) : Kelly Alves Martins de Lima

Implementar o protocolo 802.1x utilizando um servidor de autenticação