**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

Bibliografia....................................................................10

**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.

**Instalar e configurar Freeradius no CentOS**

**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

● Elaborar um documento com os conceitos e funcionalidades do protocolo 802.1x.

● Instalar e configurar um servidor de autenticação. Sugestão: FreeRadius

● Documentar a instalação e configuração através dos prints de telas