

**Faculdade de Tecnologia SENAC Goiás**

**Gestão da Tecnologia da Informação**

**Projeto de Redes de Computadores**

**PROTOCOLO 802.1X COM SERVIDOR DE AUTENTICAÇÃO**

**Alunos:** Antônio Bueno de Camargo  
Hudson Rodrigues

Iury Neres Santana  
Ivan Luís

**Junho - 2018**

**DEFINIÇÃO**

A IEEE 802.1X é um protocolo padrão de IEEE para controle de acesso de redes com base em portas (PNAC). Ele faz parte do grupo de protocolos de rede 802.1. Além disso, ele prevê mecanismos de autenticação para dispositivos que desejam se anexar a uma LAN ou WLAN. A IEEE 802.1X define o encapsulamento do Extensible Authentication Protocol (EAP) sobre o IEEE 802, que é conhecido como EAP over LAN ou EAPOL. Qualquer host que se conectar à rede deverá primeiro fornecer informações de autenticação, para receber permissões de acesso à rede.

A autenticação IEEE 802.1X normalmente é usada como uma forma de segurança avançada para redes com fio, mas alguns gestores de rede dos departamentos de TI estão buscando implementar o padrão IEEE 802.1X como uma forma de proteger suas conexões de rede sem fio. Isso porque da mesma forma que um cliente de rede com fio autenticado deve enviar algumas credenciais para serem validadas antes de poder enviar quadros pela intranet de Ethernet com fio, um cliente de uma rede wireless IEEE 802.1X também precisa executar a autenticação antes de poder enviar pacotes de dados pela sua porta do ponto de acesso (AP) sem fio e através da rede.

O padrão IEEE 802.1X define um protocolo cliente e um controle de acesso baseado em autenticação de servidor que restringe os clientes não autorizados de se conectarem a uma rede local por meio de portas de acesso público. O servidor de autenticação autentica cada cliente conectado a uma porta do switch e atribui a porta a uma VLAN antes de disponibilizar todos os serviços oferecidos pelo switch ou LAN. Até que o cliente esteja autenticado, o controle de acesso 802.1X permite apenas o tráfego do Protocolo de autenticação extensível sobre a LAN (EAPOL) através da porta a qual o cliente está conectado, depois do sucesso da autenticação, o tráfego normal também pode passar pela porta.

Com o 802.1X, você empacota mensagens EAP em quadros Ethernet e não usa PPP. É a autenticação e nada mais. Os gestores de TI buscam isso em situações nas quais o PPP não é necessário, quando eles usam protocolos diferentes de TCP/IP ou quando a sobrecarga e a complexidade de usar PPP é indesejável. O 802.1X usa três termos que você precisa saber. O usuário ou cliente que quer ser autenticado é chamado de “suplicante”. O servidor atual que faz a autenticação, geralmente um servidor RADIUS, é chamado de servidor de autenticação. E o dispositivo entre eles, tal como Access Point sem fio, é chamado de autenticador. Um dos pontos principais do 802.1X é que o autenticador. Um dos principais do 802.1X é que o autenticador pode ser simples e mudo, toda a inteligência tem que estar no suplicante e no servidor de autenticação. Isso faz com que o 802.1X seja ideal para Access Points sem fio, que são tipicamente pequenos e têm pouca memória e poder de processamento.

**CARACTERÍSTICAS**

|  |  |
| --- | --- |
| **Características** | **Descrição** |
| Camada Física | Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS) e infravermelho(IR). |
| Faixa de Frequência | 2,4 GHZ (11b, 11g) e 50 GHZ (11a). |
| Segurança de informação | 1Mbps, 2Mbps, 5.5Mbps, 11Mbps (11b), 54Mbps (11a11g) Autenticação, confidencialidade e integridade baseada no algoritmo de encriptação RC4, porém com gerenciamento da chave limitado |
| Throughput | Aproximadamente 50m (ambientes fechados) e 400m (ambientes abertos). |
| Aspectos Positivos | Velocidade de rede Ethernet, porém sem cabo, muitos produtos diferentes de empresas. Access Points e Wireless Cliente Cards estão diminuindo de preço. |
| Aspectos Negativos | Segurança baixa na configuração padrão, o throughput cai muito com a distância e a carga. |

O padrão IEEE 802.1x é uma solução para os problemas de autenticação encontrados no IEEE 802.11, pois o mesmo tem suporte a diversos métodos de autenticação existentes. Desta maneira, o IEEE 802.1x garante compatibilidade entre o Protocolo de Integridade Temporal de Chave (TKIP - Temporal Key Integrity Protocol), que foi desenvolvido para solucionar o problema de chave estática do WEP, e o Padrão de Criptografia Avançada (AES – Advanced Encryption Standard), que é um mecanismo forte de criptografia que vem sendo adotado recentemente.

Uma forma de utilizar os recursos que o padrão IEEE 802.1x oferece, é implementar o protocolo EAP (BLUNK, 1998), proposto para ampliar a funcionalidade de autenticação do protocolo ponto-a-ponto (PPP - Point-to-Point Protocol) (SIMPSON 1994), antes limitada aos mecanismos providos pelo Protocolo para Controle de Link (LCP - Link Control Protocol), que eram o Protocolo de Autenticação por Senha (PAP - Password Authentication Protocol) e o Protocolo de Autenticação por Negociação de Desafio (CHAP – Challenge Handshake Authentication Protocol) (SIMPSON, 1996). O PAP é um protocolo utilizado principalmente para autenticação em redes discadas, no qual o login e a senha trafegam em texto claro. O CHAP provê criptografia somente do usuário e senha, porém os dados também trafegam em texto claro.

Utilizando o EAP é possível ter independência de mecanismos de autenticação PPP, sendo assim uma alternativa interessante para interligação de redes visto a sua capacidade de adaptação a novos mecanismos. Neste trabalho será utilizado o EAP em conjunto com o protocolo TLS utilizando certificados digitais para autenticação dos usuários.

Uma vantagem do uso do protocolo EAP é o aumento de vida útil dos equipamentos que possuem suporte ao protocolo IEEE 802.1x, pois os mesmos passam a funcionar como intermediários entre o host cliente e o servidor de autenticação, não sendo necessário implementar mecanismos adicionais de segurança no próprio equipamento.

**CENÁRIOS DE IMPLEMENTAÇÃO**

Para implementar este protocolo é necessário que todas as portas de rede corporativa precisam ter autenticação 802.1x habilitadas para obter segurança, com exceção de lugares onde a segurança física é exclusivamente restrita. Para os hosts que não suportam o protocolo é necessário identificar as portas e colocá-las em VLAN’s inseguras, isoladas via firewall das VLAN’s seguras. É recomendado utilizar autenticação por equipamento mesmo que também faça autenticação por usuário. É recomendado que se habilite a autenticação por equipamento usando senha no AD, para que quando a senha no AD expirar seja possível a autenticação.

**SOLUÇÕES PARA REDE WIRELESS**

O protocolo IEEE 802.1x garante compatibilidade entre o protocolo Temporal Key Integrity Protocol que faz criptografia de pacotes e o protocolo Advanced Encryption Standard que é o padrão norte americano de criptografia. Esse protocolo faz a autenticação baseado em servidor e cliente que restringe clientes não autorizados a se conectarem na rede, barrando invasores ou dispositivos não gerenciados.

As redes sem fio apresentam as seguintes vantagens:

* **Flexibilidade:** dentro da área de cobertura, uma determinada estação pode se comunicar sem nenhuma restrição. Além disso, permite que a rede alcance lugares onde os fios não poderiam chegar.
* **Facilidade**: a instalação pode ser rápida, evitando a passagem de cabos através de paredes, canaletas e forros, portanto uso mais eficiente do espaço físico.
* **Redução do custo agregado**: mesmo mais dispendiosa que uma rede cabeada, estão agregadas vantagens como: melhor utilização dos investimentos em tecnologias existentes como laptops, rede de dados e voz, aplicativos, agilidade nas respostas aos clientes.
* **Diversas topologias**: podem ser configuradas em uma variedade de topologias para atender a aplicações específicas. As configurações são facilmente alteradas, facilidade de expansão, manutenção reduzida.

Em contrapartida, apresentam as seguintes desvantagens:

* **Flexibilidade:** dentro da área de cobertura, uma determinada estação pode se comunicar sem nenhuma restrição. Além disso, permite que a rede alcance lugares onde os fios não poderiam chegar.
* **Qualidade de serviço:** a qualidade do serviço provido ainda é menor que a das redes cabeadas. Tendo como principais razões para isso a pequena banda passante devido às limitações da radio transmissão e a alta taxa de erro devido à interferência.
* **Custo:** o preço dos equipamentos de Redes sem Fio é mais alto que os equivalentes em redes cabeadas.
* **Segurança:** intrinsecamente, os canais sem fio são mais suscetíveis a interceptores não desejados. O uso de ondas de rádio na transmissão de dados também pode interferir em outros equipamentos de alta tecnologia, como por exemplo, equipamentos utilizados em hospitais. Além disso, equipamentos elétricos são capazes de interferir na transmissão acarretando em perdas de dados e alta taxa de erros na transmissão.
* **Baixa transferência de dados:** embora a taxa de transmissão das Redes sem Fio esteja crescendo rapidamente, ela ainda é muito baixa se comparada com as redes cabeadas.

**O QUE É RADIUS?**

**RADIUS** (Remote Authentication Dial In User Service) é um protocolo de rede que fornece gerenciamento centralizado de autenticação, autorização e contabilização para usuários que se conectam-se a e utilizam um serviço de rede. Radius foi desenvolvido pela Livingston Enterprises Ic. em 1991 como um protocolo de autenticação e contabilização de servidor de acesso, sendo mais tarde introduzido como padrão do **IETF(**Internet Engineering Task Force).

RADIUS é um protocolo do tipo cliente/servidor que roda como um protocolo da camada de aplicação, usa como apoio o protocolo de transferência UDP. Tanto Servidores de Acesso Remoto (RAS), como servidores de Redes Virtuais Privadas (VPNs) e Servidores de Acesso à Rede (NAS), e todos os gateways que controlam o acesso a rede possuem um componente cliente do protocolo RADIUS que se comunica com o servidor RADIUS. Este servidor normalmente é um processo de background rodando no UNIX ou Microsoft Windows server.

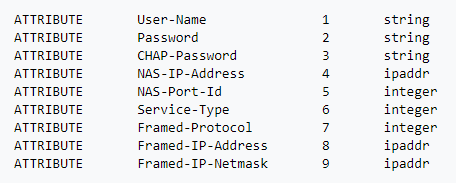
Um servidor **RADIUS** possui três funções básicas:

* Autenticação de usuários ou dispositivos antes da concessão de acesso à rede.
* Autorização de outros usuários ou dispositivos a usar determinados serviço providos pela rede.
* Para informar sobre o uso de serviços.

O protocolo RADIUS é resumidamente, um serviço baseado em UDP de pergunta e resposta. As requisições e respostas seguem um padrão de tabelas (variável=valor).

A variável não possui um nome e sim um número. A relação entre este número e seu nome é obtida através de dicionários.

Exemplo de dicionário padrão:



**O QUE É O FREERADIUS?**

FreeRADIUS é a mais popular e o mais amplo servidor de RADIUS em código livre do mundo. FreeRADIUS provê autenticação, autorização e contabilidade (accounting) para muitas das empresas da Fortune 500, esse padrão é conhecido como AAA. FreeRADIUS é utilizado no mundo acadêmico, em instituições de pesquisa e educacionais. Criado a partir de 1999 por Alan DeKok e Miquel Van Smoorendburg, possui um desenho modular que encoraja o desenvolvimento comunitário de extensões.

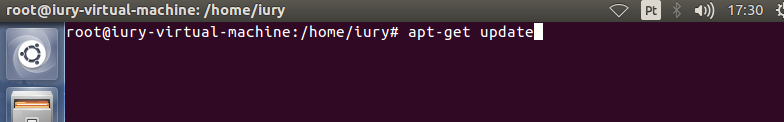
FreeRADIUS é o servidor (em software livre) que suporta o maior número de tipos de autenticação e, atualmente, é o único servidor RADIUS de código livre que suporta o protocolo EAP - Extensible Authentication Protocol. Além disto, FreeRADIUS é o único que suporta virtualização, mantendo os custos de implantação e manutenção baixos. Seu desenho modular é fácil de entender, permitindo facilmente a inclusão ou remoção de módulos sem, contudo, afetar o desempenho, os requisitos de hardware, de memória ou a segurança do sistema. A modularidade permite executar FreeRADIUS em sistemas embarcados ou em servidores com vários núcleos e com gigabytes de memória RAM.

Um servidor RADIUS pode manipular de poucas até milhares de requisições por segundo. Estudos de caso registram organizações que possuem 10 milhões de usuários cadastrados no sistema. Servidores comerciais normalmente vendem suas soluções como aditivos e nunca são completas. FreeRADIUS é um pacote completo com todas as soluções em um único produto, sem necessidade de softwares ou licenças adicionais.

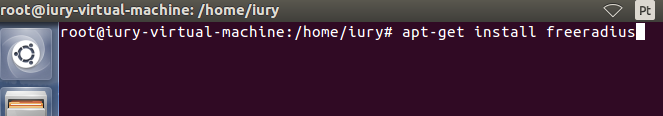
Um cliente FreeRADIUS foi projetado como um esquema de consultas SQL. O uso de consultas SQL pode otimizar as políticas AAA. O projeto de implantação do sistema é uma fase importante e, não é raro, que alguns clientes encontrem limitações sérias após alguns meses de funcionamento. Essas falhas são causadas por seus próprios erros de projeto. O correto uso de tabelas, índices e consultas SQL são fatores primordiais na implementação de um sistema FreeRADIUS.

**INSTALANDO O SERVIDOR FREERAIUS**

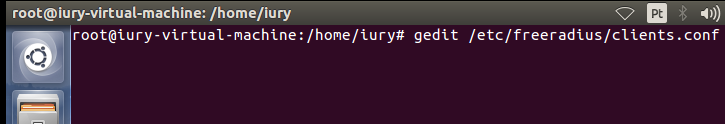
1. Primeiramente vamos atualizar nosso repositório do UBUNTU 16.04.



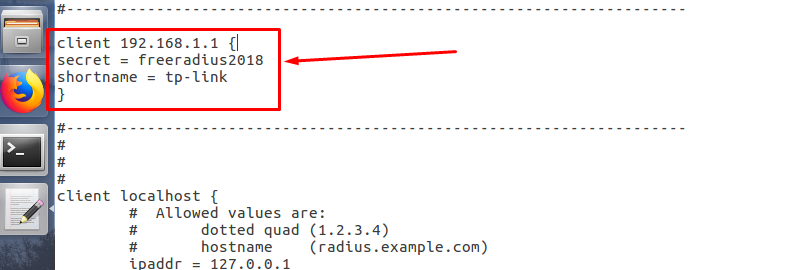
1. Após realizar a atualização do repositório, vamos instalar o servidor FreeRADIUS.



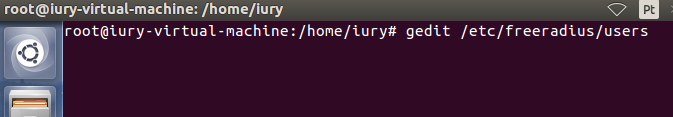
1. O diretório onde ficam os arquivos de configuração do freeRADIUS fica /etc/freeradius.
2. Primeiramente vamos configurar o cliente/AP.



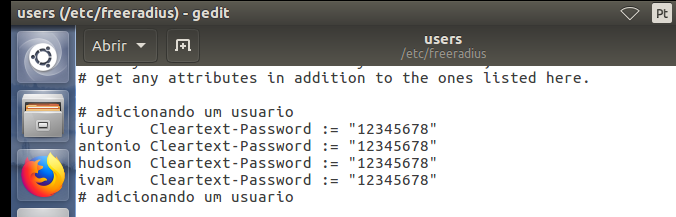
1. Adicionar a seguinte linha.



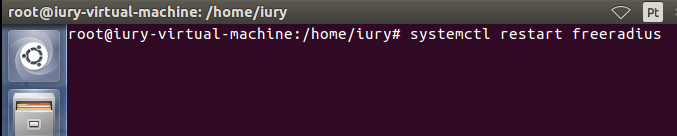
1. Posteriormente vamos adicionar os clientes que vão estar autorizados a adentrar em nossa rede.



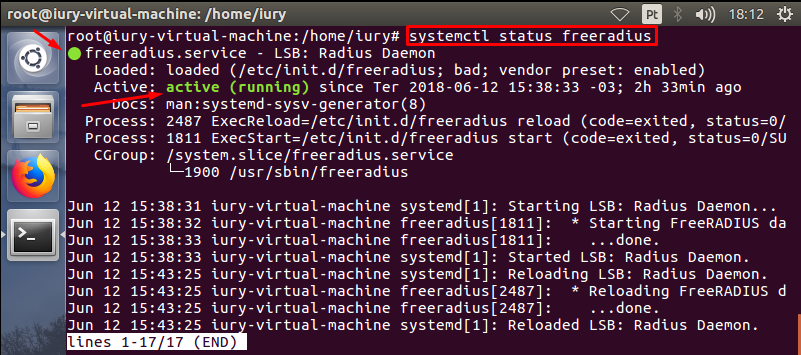
1. Adicionar a seguinte linha.



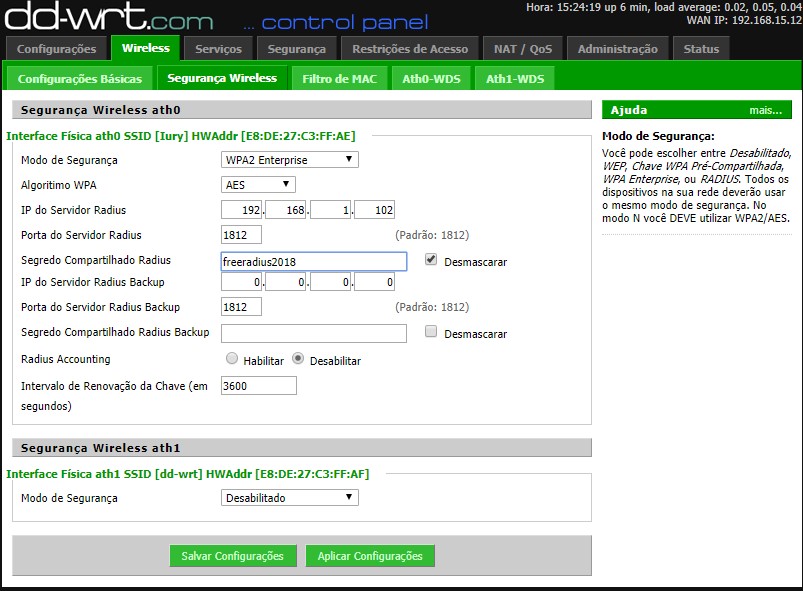
1. Feito isso vamos reiniciar o servidor FreeRADIUS.



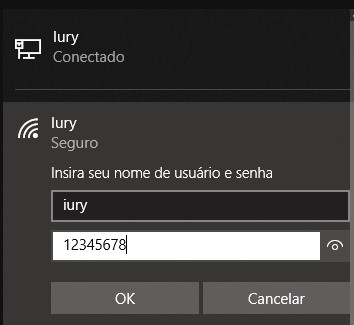
1. Posteriormente vamos verificar o status do nosso servidor.



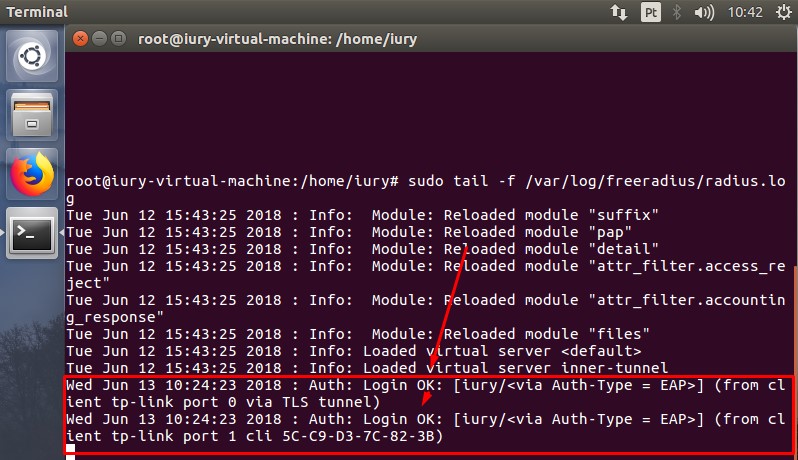
1. Depois de reiniciar o serviço do FreeRADIUS, basta configurar o AP com o usuário e senha do servidor para que o mesmo possa autenticar ou não seus usuários à rede.
2. Após configurar o servidor vamos configurar o AP para que o mesmo se comunique com o servidor de autenticação.



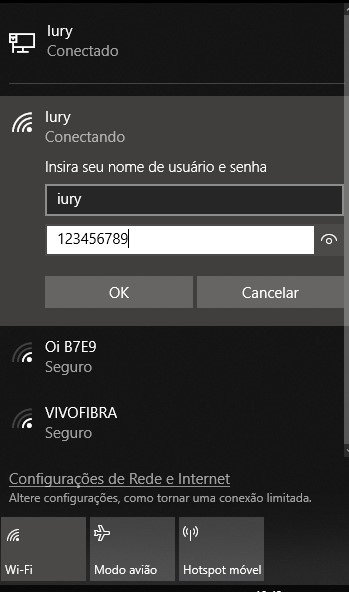
1. Realizando a autenticação na rede. Observe que solicita um usuário e senha. Deverá colocar usuários cadastrados no servidor FreeRadius.



1. Visualizando o log do servidor FreeRADIUS quando o acesso à rede é permitido.



1. Forçando um acesso indevido a rede.



1. Visualizando o log do servidor quando o mesmo não permite acesso à rede.

