ESTUDO DE CASO: AUTENTICAÇÃO IEEE 802.1X BASEADA NO PROTOCOLO RADIUS E SERVIÇO DE DIRETÓRIO LDAP APLICADO A REDE GIGAUFOPNET

Tiago R. Chaves

Orientador: Professor Ricardo Rabelo

8 de outubro de 2010

Sumário

O que é autenticação?

- **Autenticação** - Processo de verificação que exige do usuário uma prova de sua identidade.

1. Algo que o usuário sabe;
2. Algo que o usuário possui;
3. Algo que o usuário é.

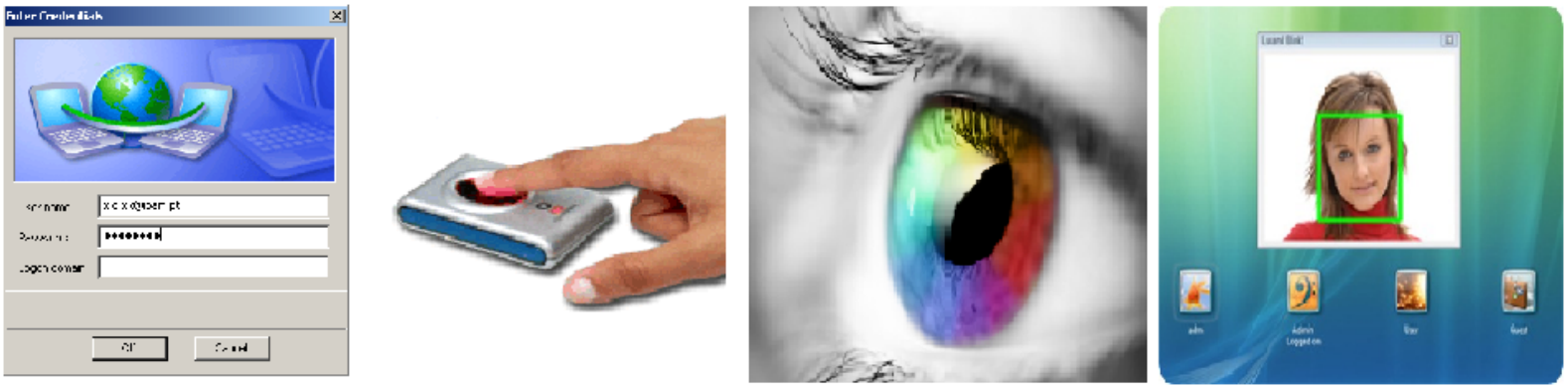

Figura: Tipos de Auntenticação

Por que utilizar autenticação?

"Durante os últimos anos as redes de computadores tiveram um grande crescimento." [1]

Por que utilizar autenticação?

"Durante os últimos anos as redes de computadores tiveram um grande crescimento." [1]

- Segurança;
- Confiabilidade;
- Integridade;

GigaUFOPnet

- Rede de computadores da UFOP, administrada pelo NTI - Núcleo de Tecnologia da Informação.

Figura: UFOP

Núcleo de Tecnologia da Informação

Figura: NTI

Unidades e Campi interligados pela GigaUFOPnet

Campus Ouro Preto

- Unidades do Morro do Cruzeiro
- IFAC - Instituto de Filosofia, Artes e Cultura
- EFAR - Escola de Farmácia Centro/REMOP
- EM - Escola de Minas Centro
- Centro de Convenções/Reitoria/PROEX/NAJOP/ASSUFOP

Unidades e Campi interligados pela GigaUFOPnet

Campus Ouro Preto

- Unidades do Morro do Cruzeiro
- IFAC - Instituto de Filosofia, Artes e Cultura
- EFAR - Escola de Farmácia Centro/REMOP
- EM - Escola de Minas Centro
- Centro de Convenções/Reitoria/PROEX/NAJOP/ASSUFOP

Campus Mariana

- ICHS - Instituto de Ciências Humanas e Sociais
- ICSA - Instituto de Ciências Sociais e Aplicadas

Unidades e Campi interligados pela GigaUFOPnet

Campus João Monlevade

- ICEA - Instituto de Ciências Exatas e Aplicadas

Usuários da GigaUFOPNet

Categoria	**Quantidade**
Professores	752
Técnicos administrativos	751
Alunos graduação *(presencial)*	8376
Alunos graduação *(distância)*	5195
Alunos pós-graduação *(em 2009)*	929
Total	**16003**

Tabela: Número de Usuários da GigaUFOPnet

Sem a impalantação do projeto

- Necessidade de pré-configuração de cada computador para acesso a rede;
- Problemas de acesso e segurança;
- Possibilidade de acesso indevido de algum ponto pré-configurado disponível;
- Problemas na identificação do usuário conectado a redes wireless;
- Distribuição estática de VLANs;
- Alta demanda de números de IP's.

Cenários comuns sem a impalantação do projeto

- Cenário 1: Usuário cadastrado e conectado a rede através de um computador da UFOP.

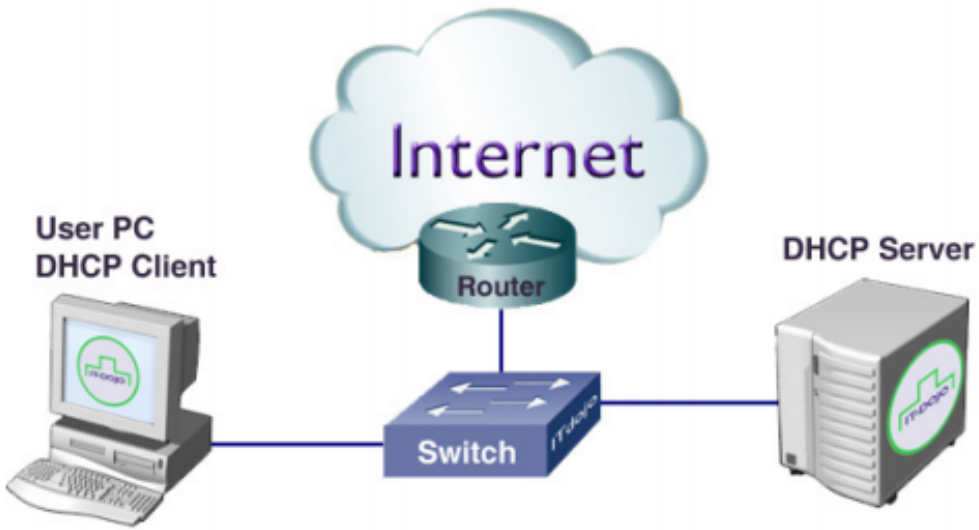

Figura: Cenário 1

Cenários comuns sem a impalantação do projeto

- Cenário 2: Usuário instala Hub/Switch para aumentar o número de pontos de acesso.

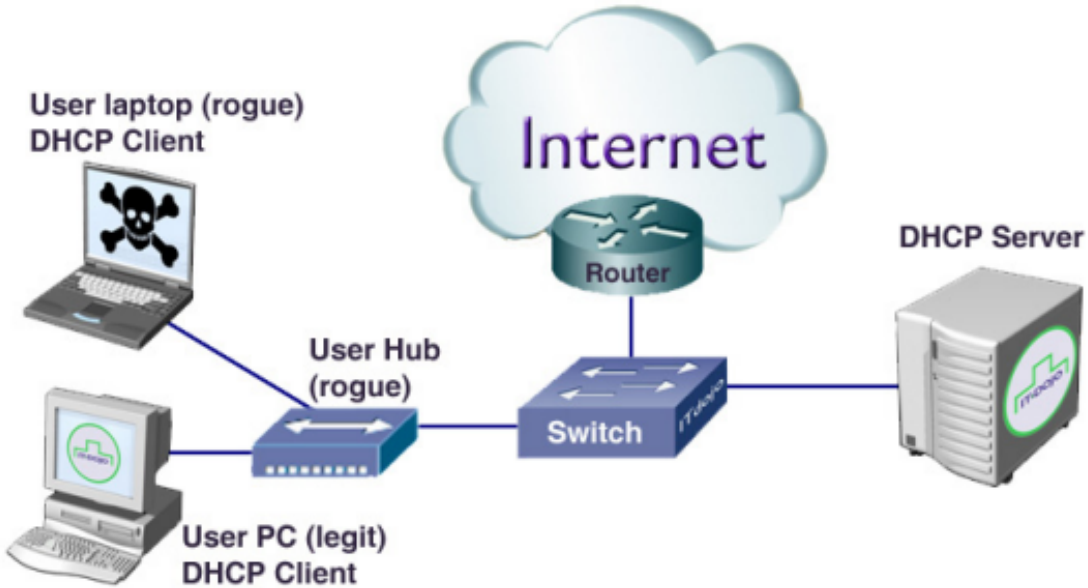

Figura: Cenário 2

Cenários comuns sem a impalantação do projeto

- Cenário 3 : Usuário isntala Acess Point

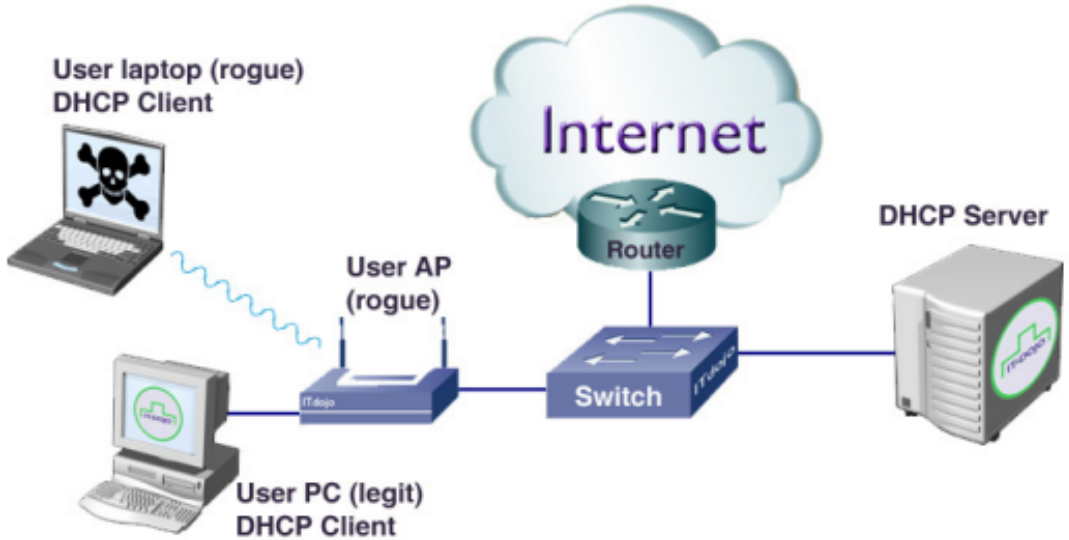

Figura: Cenário 3

Situação desejada

- Identificação e autenticação de todos os usuários da Rede GigaUFOPnet no momento da sua conexão;
- Implantação de políticas de acesso à rede de acordo com o papel de cada usuário;
- O usuário deve ter acesso a sua rede local e privilégios a partir de qualquer ponto da rede;
- Evitar a utilização não autorizada da rede;
- Controle de acesso dos usuários;
- Criação de uma rede wireless;
- VLANs dinâmicas.
- Melhor utilização das faixas de IP.

Objetivo geral

- Buscar um avanço na estrutura atual da GigaUFOPnet, acrescentando o serviço de autenticação.

Figura: Objetivo Geral

Objetivos específicos

- Garantir desempenho e confiabilidade do acesso a rede GigaUFOPnet;
- Autenticar todos os acessos a rede;
- Contabilizar todos os acessos e uso dos usuários;
- Identificar usuários mal intencionados utilizando a rede;
- Criar Login e Senha únicos para acesso a rede e outros serviços da UFOP;
- Disponibilizar acesso a rede para dispositivos móveis com segurança.

Etapas do Projeto

O desenvolvimento deste trabalho será dividido em quatro grandes etapas:

1. Primeira Etapa: Treinamento e pesquisa
2. Segunda Etapa: Experimentos
3. Terceira Etapa: Teste piloto (Fase atual)
4. Quarta Etapa: Implatação em todos os campi da UFOP

Primeira Etapa: Treinamentos e pesquisa

- Levantamento bibliográfico;
- Cursos.

Figura: Tecnologias utilizadas

Segunda Etapa: Experimentos

- Definição do nível de segurança adotado;
- Integração do banco de dados;
- Integração Samba e LDAP;
- Tentativas de eliminar a necessidade de utilização do Samba;
- Configuração de Switches;
- Configuração e definição de Access Points a ser utilizado no projeto;
- Testar o Schema BrEduPerson na LDAP;
- Definição de configurações dos clientes, usando a base de dados de usuários da UFOP;
- Avaliação das ferramentas de contabilidade do uso;
- Avaliação do comportamento dos switches;
- Avaliação do impacto de utilização de todos os serviços no servidor.

Terceira Etapa: Teste piloto

A infraestrutura testada será aplicada em uma unidade da UFOP para realização das seguintes tarefas:

- Configurações de todos os switches e clientes;
- Avaliação do funcionamento;
- Identificação das vulnerabilidades;
- Aplicação de possíveis melhorias.

Quarta Etapa: Implatação em todos os campi da UFOP

De maneira sistemática e coordenada todas as modificações necessárias serão aplicadas em todos os prédios da UFOP.

- Disponibilização de equipamentos;
- Disponibilização da equipe de implantação;
- Implantação definitiva após aprovação.

Padrão IEEE 802.1x

- O protocolo 802.1x é um padrão do IEEE (Institute of Electrical and Electronic Engineers);
- Controle de acesso à rede baseado em portas;
- Oferece autenticação, controle de acesso e gerência de redes locais com fio e sem fio;
- Pode utilizar certificados de cliente ou senhas e nomes de usuários;
- Separa a autenticação de usuário e de computador.

Figura: Access Point e Switch

Padrão IEEE 802.1x

- Utiliza um protocolo Extensible Authentication Protocol (EAP) para desempenhar a conversação de autenticação entre o usuário e o servidor;
- Os protocolos mais comuns usados nas redes sem fio são o TLS, PEAP, TTLS e LEAP.

Padrão IEEE 802.1x - Entidades

1. Suplicante (supplicant).
2. Autenticador (authenticator);
3. Servidor de autenticação (authentication server);

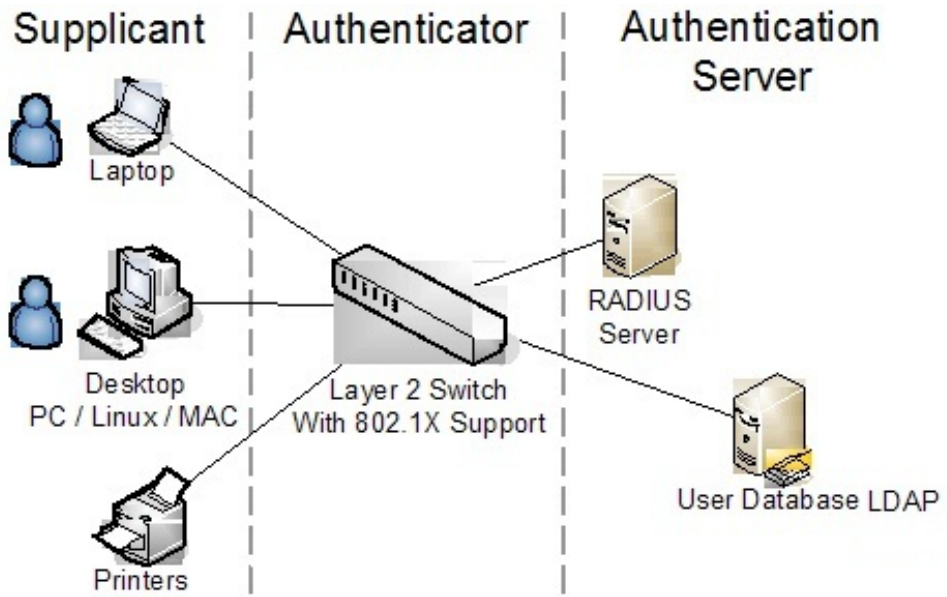

Figura: Entidades

Servidor de Autenticação Radius

- Remote Authentication Dial In User Service(Serviço Remoto de Autenticação da Discagem do Usuário);
- Define um padrão popular usado para manutenção e gerenciamento remoto Radius, autenticação usuário e validação;
- É um protocolo de controle de acesso de rede que utiliza recurso AAA (Authentication, Authorization, Accounting).

Processo de identificação do RADIUS

1. Cliente envia solicitação de serviço para o servidor de acesso à rede.
2. Servidor de Acesso à Rede responde solicitando nome do usuário e senha
3. Cliente fornece as credenciais.
4. Servidor de Acesso à Rede envia a solicitação para o servidor RADIUS.
5. Servidor RADIUS primeiro verifica se a comunicação está vindo de um Servidor de Acesso à Rede autorizado, e se for, ele verifica as credenciais com aquelas em seu banco de dados, depois envia a resposta para o Servidor de Acesso à Rede.
6. O Servidor de Acesso à Rede recebe um comando access_accept (acesso aceito) ou access_reject (acesso negado) do servidor do RADIUS e usa este resultado para definir se permite ou rejeita a tentativa de acesso do cliente.

Figura: Tecnologias utilizadas

LDAP

- Lightweight Directory Access Protocol, ou Protocolo Leve de Acesso a Diretórios, ou apenas LDAP, é um protocolo utilizado para atualizar e pesquisar diretórios, rodando sobre o protocolo de rede TCP/IP. [5]

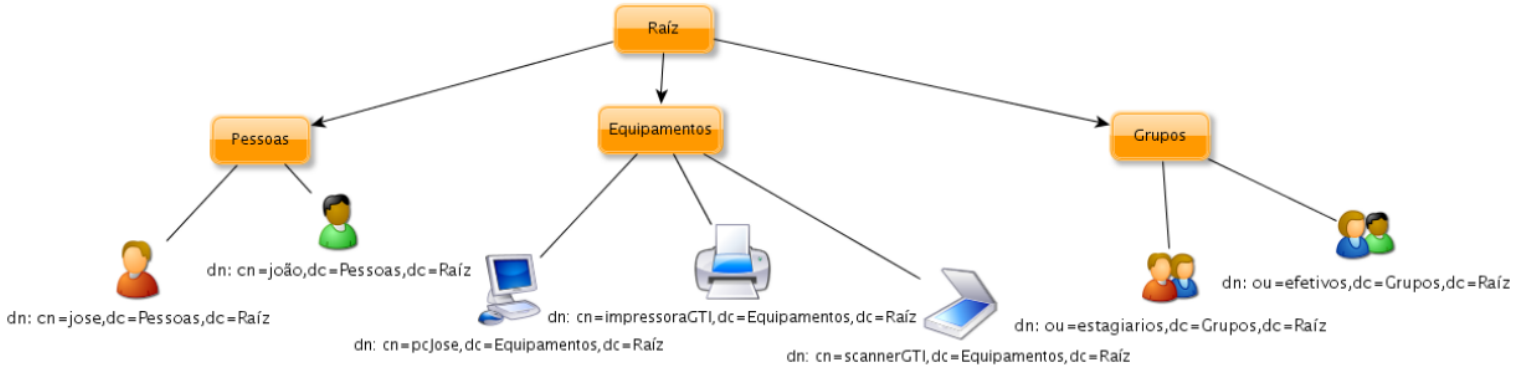

Figura: Exemplo de uma estrutura em diretórios

Vantagens do LDAP

- É um padrão aberto;
- É otimizado para realizar pesquisas e leitura;
- Centraliza toda a informacão;
- Suporta mecanismos de segurança para autenticação e para a troca de dados (TLS);
- Muitas aplicações e serviços possuem suporte ao LDAP.

Desvantagens do LDAP

- Em alguns casos não substitui as bases de dados relacionais;
- Pouco eficiente para operacões de escrita e atualização;
- Integração com outros serviços e aplicações torna a implantação complexa.

Arquitetura final da GigaUFOPnet

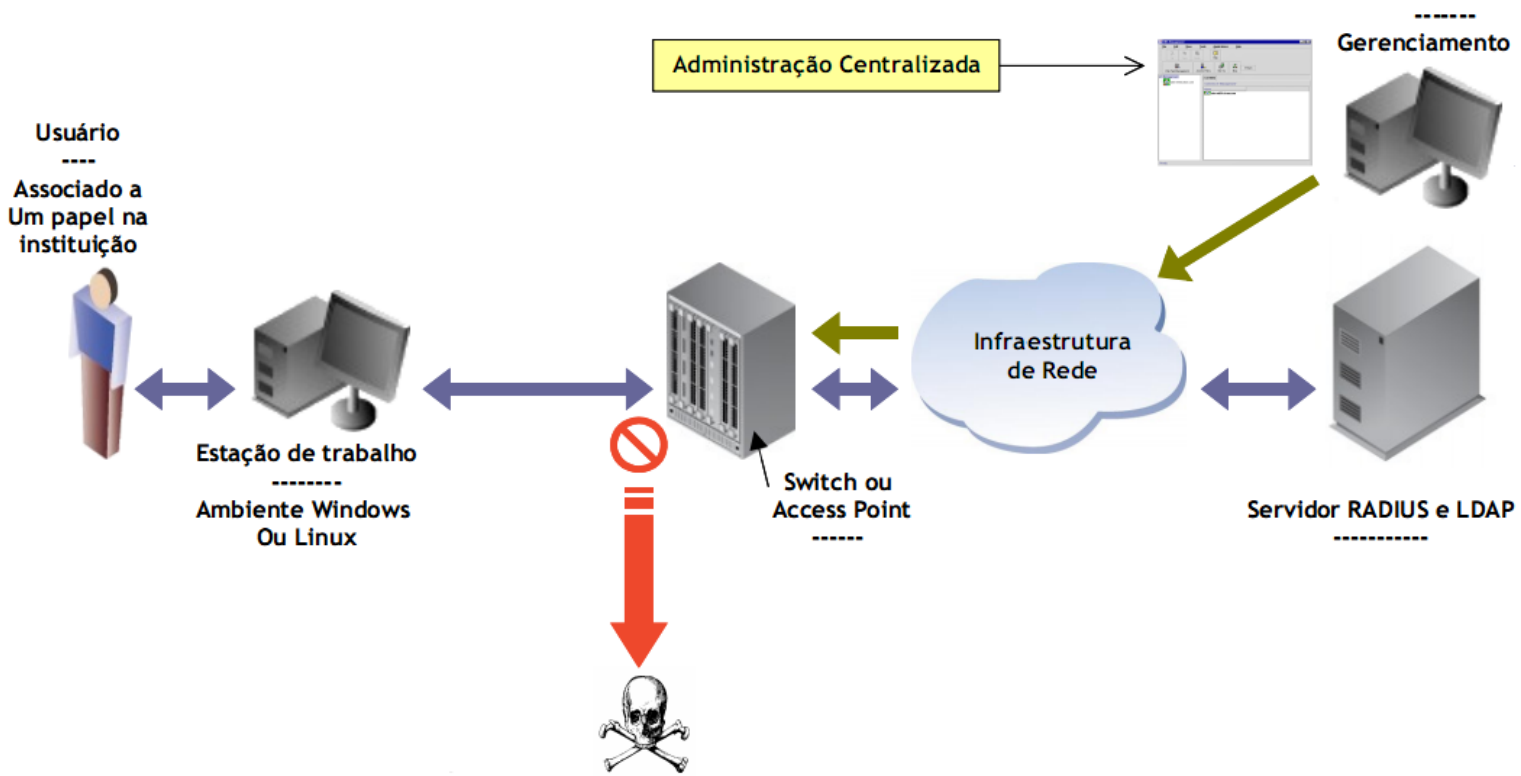

Figura: Situação Desejada

Referências


M. Balbonil.
Nic.br anuncia resultados da pesquisa sobre o uso da internet no brasil.
Technical report, Núcleo de Informação e Coordenação (NIC.br), 2006.


Luiz Gustavo Barrosi and Dierone César Foltran Junior.
Autenticação ieee 802.1x em redes de computadores utilizando tls e eap.
IEEE 4º Encontro de Engenharia e Tecnologia dos Campos Gerais, August 2008.


T. Chaves et al.
Projeto network login.
Technical report, Núcleo de Tecnologia da Informação, Universidade Federal de Ouro Preto, 2009.


J. VOLLBRECHT et all.
Aaa authorization framework.
RFC 2904, Internet Engineering Task Force, 2000.


Felipe Bartholo Favilla.
Autenticação centralizada utilizando o protocolo ldap.

Dúvidas ???

Obrigado!

Referências

[2] [3] [4]