Banco de Dados

LDAP

Rodrigo Rubira Branco - rodrigo@firewalls.com.br

O que é Serviço de Diretorio?

Banco de dados especializado em armazenar informações sobre objetos

Caracteristicas de Diretorio

Apesar de diretórios serem bancos de dados, eles não são banco de dados relacionais.

Diretórios:

- Tendem a conter informações descritivas;
- Armazena as informações em entradas organizadas em árvore;
- Informação estática – Geralmente mais lida do que escrita;
- Não implementam transações complexas;
- Conceito de transações se torna muito complicado;
- Possibilidade de réplica para otimizar tempo de resposta;
- Breves períodos de inconsistência são aceitos.

Arquitetura de Diretorios

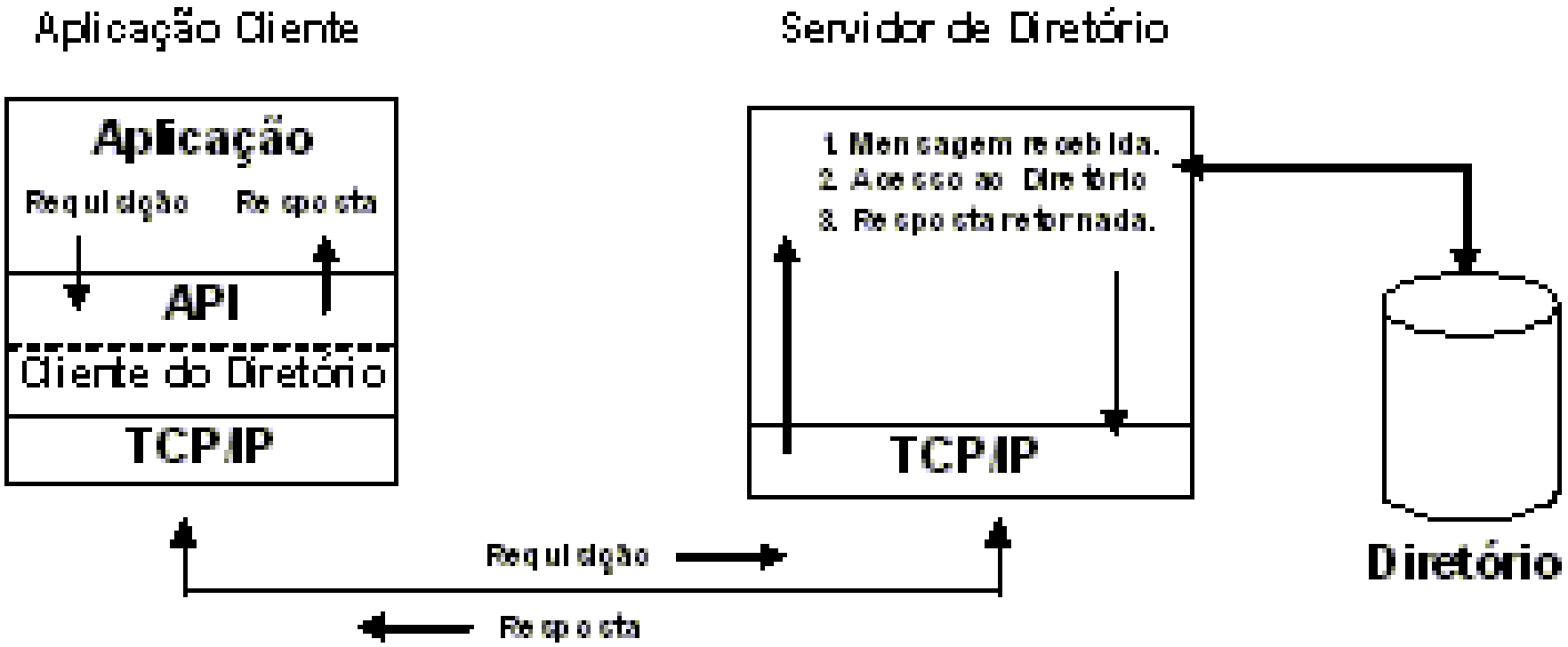


Figura 1. Interação Cliente/Servidor

Padrao X.500

X.500 (ano 1990)

Organiza as entradas em árvores hierárquicas;

Comunicação usando DAP (camada de aplicação);

Utiliza pilha de protocolos OSI completa;

Exigia muito recurso o que não era encontrado em pequenos ambientes.

Lightweight Directory Access Protocol

LDAP é um protocolo padrão para acesso a diretório.

Originalmente o LDAP foi concebido como uma alternativa ao protocolo DAP para acesso a diretórios baseados no modelo X.500.

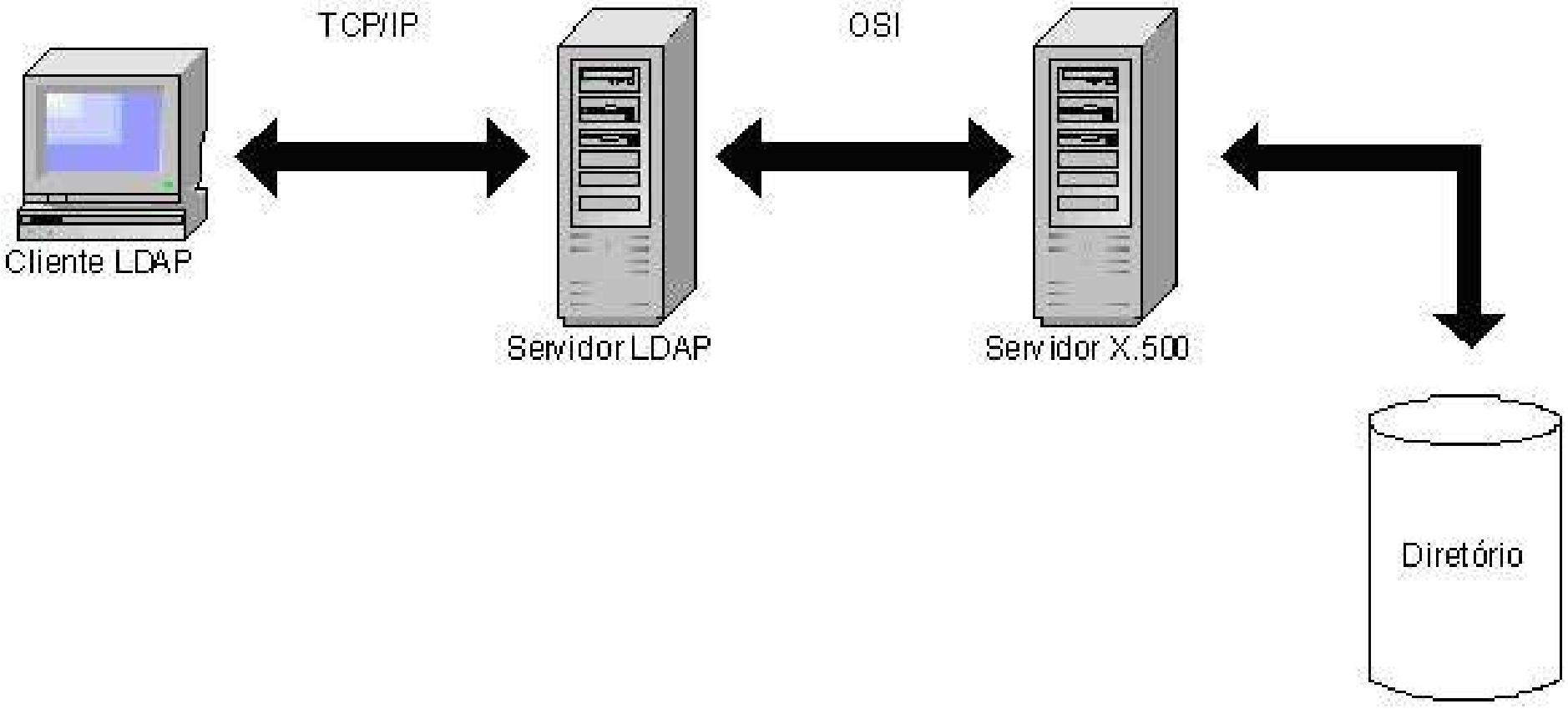
Surgiu baseado na pilha de protocolos TCP/IP;

Simplificou operações de acesso ao X.500;

Necessita de uma quantidade mínima de recursos de rede no lado cliente;

Se torna particularmente atrativa para aplicações baseadas em Internet.

X.500 x LDAP


TCP/IP
OSI
Cliente LDAP
Servidor LDAP
Servidor X.500
Diretório

X.500 x LDAP

Posteriormente, servidores que disponibilizavam serviço de diretório LDAP se tornaram comuns.

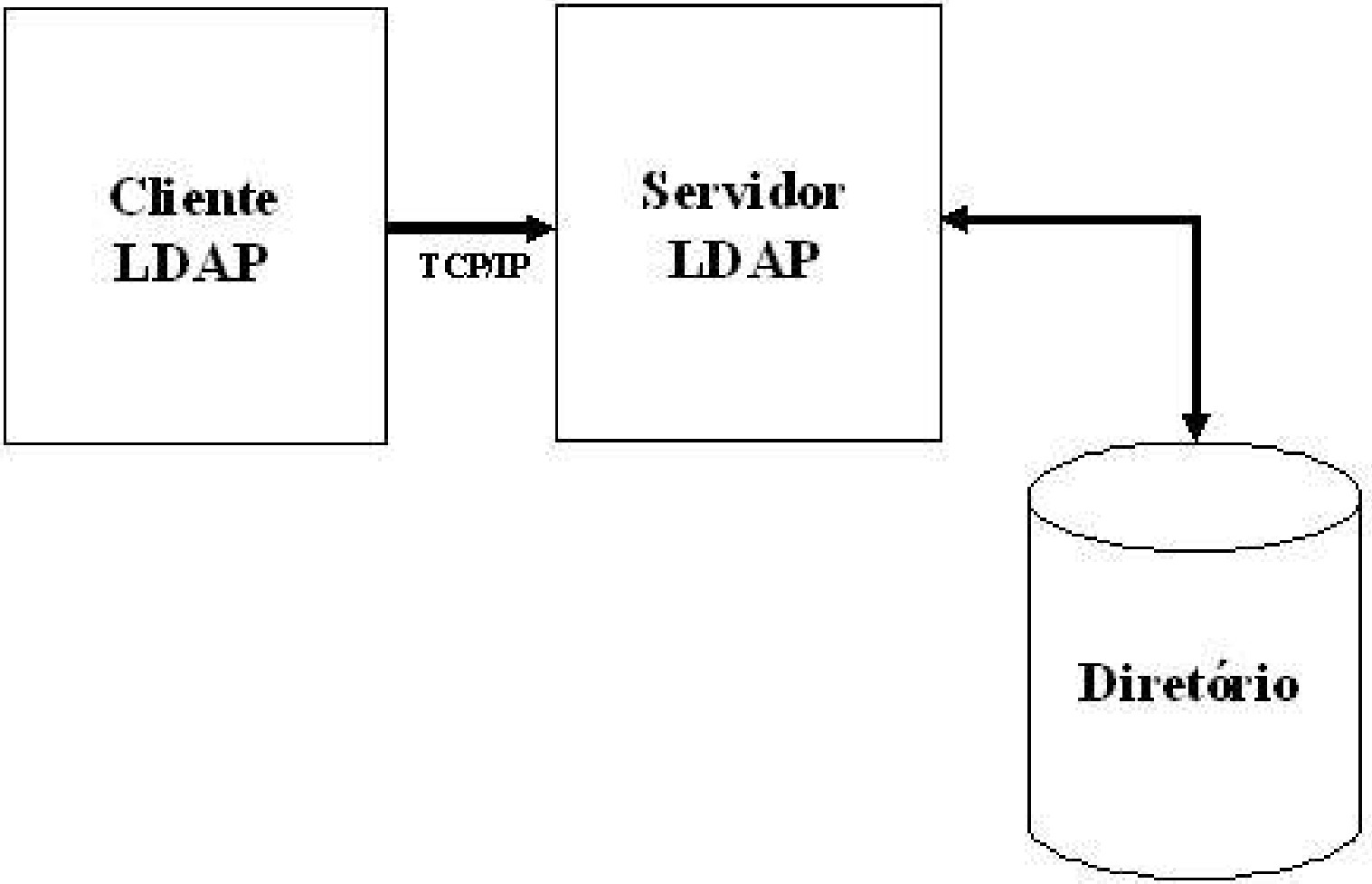
Algumas características que garantiram o sucesso do LDAP:

Utiliza a pilha de protocolos TCP/IP e não o OSI;

O modelo funcional é mais simples, o que o torna mais fácil de entender e implementar;

Utiliza strings para representar os dados e não estruturas complicadas de sintaxe.

Arquitetura Cliente/Servidor



Modelos LDAP

Os quatro modelos da arquitetura LDAP:

Modelo de Informação (Information Model) – *Descreve a estrutura da informação armazenada;*

Modelo de Nome (Naming Model) – *Descreve como as informações são organizadas e identificadas;*

Modelo Funcional (Funcional Model) – *Descreve quais operações podem ser efetuadas sobre as informações;*

Modelo de Segurança (Security Model) – *Descreve como a informação pode ser protegida contra acessos não autorizados.*

Conceitos

- SCHEMA ->

O esquema do diretório contém toda a informação sobre como os dados estão organizados na árvore (DIT – Directory Information Tree).

- OBJECT CLASS ->

Object Class consistem de um grupo de atributos referentes a uma entrada. Quando uma entrada é definida (instanciada), são atribuídas a esta um ou mais object class.

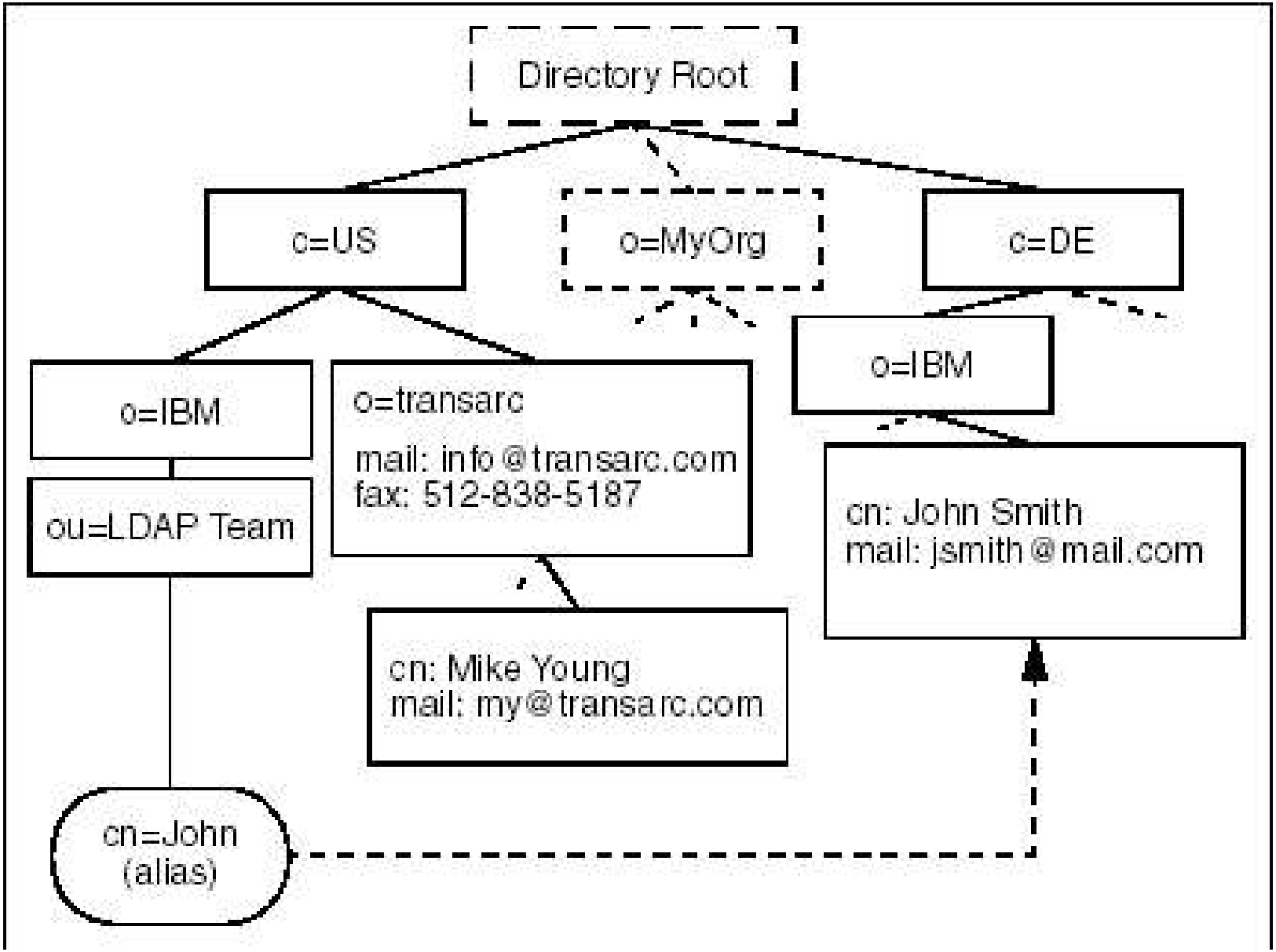
- Como na definição de orientação a objetos, uma object class (subclass) pode ser derivada de um outro objetc class (superclass); herdando todos os atributos do objeto pai.

Conceitos

As entradas são organizadas na DIT com base no seu DN (***Distinguished Name***), que é o indentificador exclusivo de uma entrada.

Os DNs são compostos de uma sequência de RDNs (***Relative Distinguished Name***) e cada RDN corresponde a um ramo na DIT, desde a raiz até a entrada à qual o DN faz referência.

Visualizaçao



Comunicaçao Segura

O ***SASL*** foi implementado na versão 3 do LDAP e é um ***framework*** que permite diferentes métodos de autenticação dos clientes, como Kerberos e SSL.

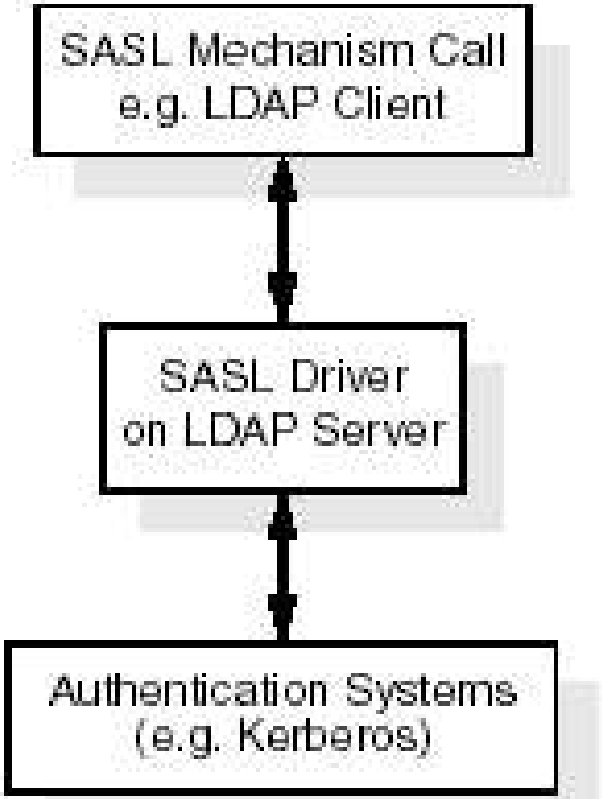
As três formas de obter acesso a um servidor LDAP são: sem autenticação, autenticação básica e SASL

Os clientes LDAP utilizam as funções SASL da API para fazer uma chamada ao driver SASL no servidor, que se conecta ao sistema de autenticação identificado pelo parâmetro *mechanism* para autenticar o usuário. É comum a utilização do SSL, ou o seu sucessor TLS.

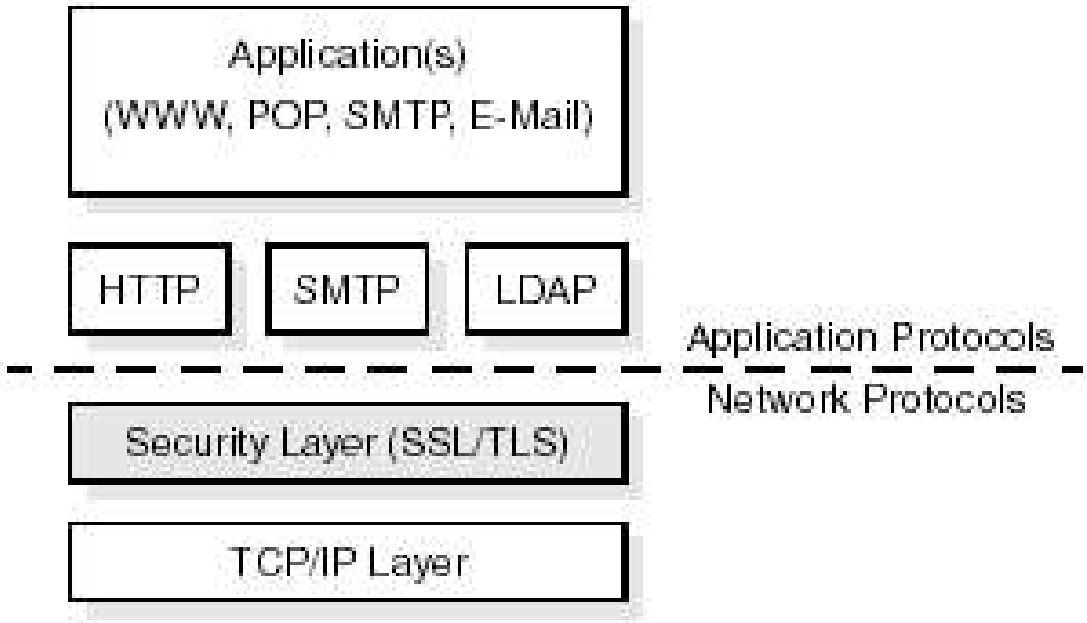
Apesar de conceitualmente aceitar múltiplos mecanismos de autenticação, alguns fornecedores não disponibilizam todos, preferindo disponibilizar apenas os mecanismos mais utilizados, como SSL/TLS e Kerberos.

O Kerberos costuma ser executado em um servidor independente para prover as funções de autenticação e utiliza um padrão amplamente aceito para criptografia dos dados, o DES.

Visualizando...



Funcionamento do SASL

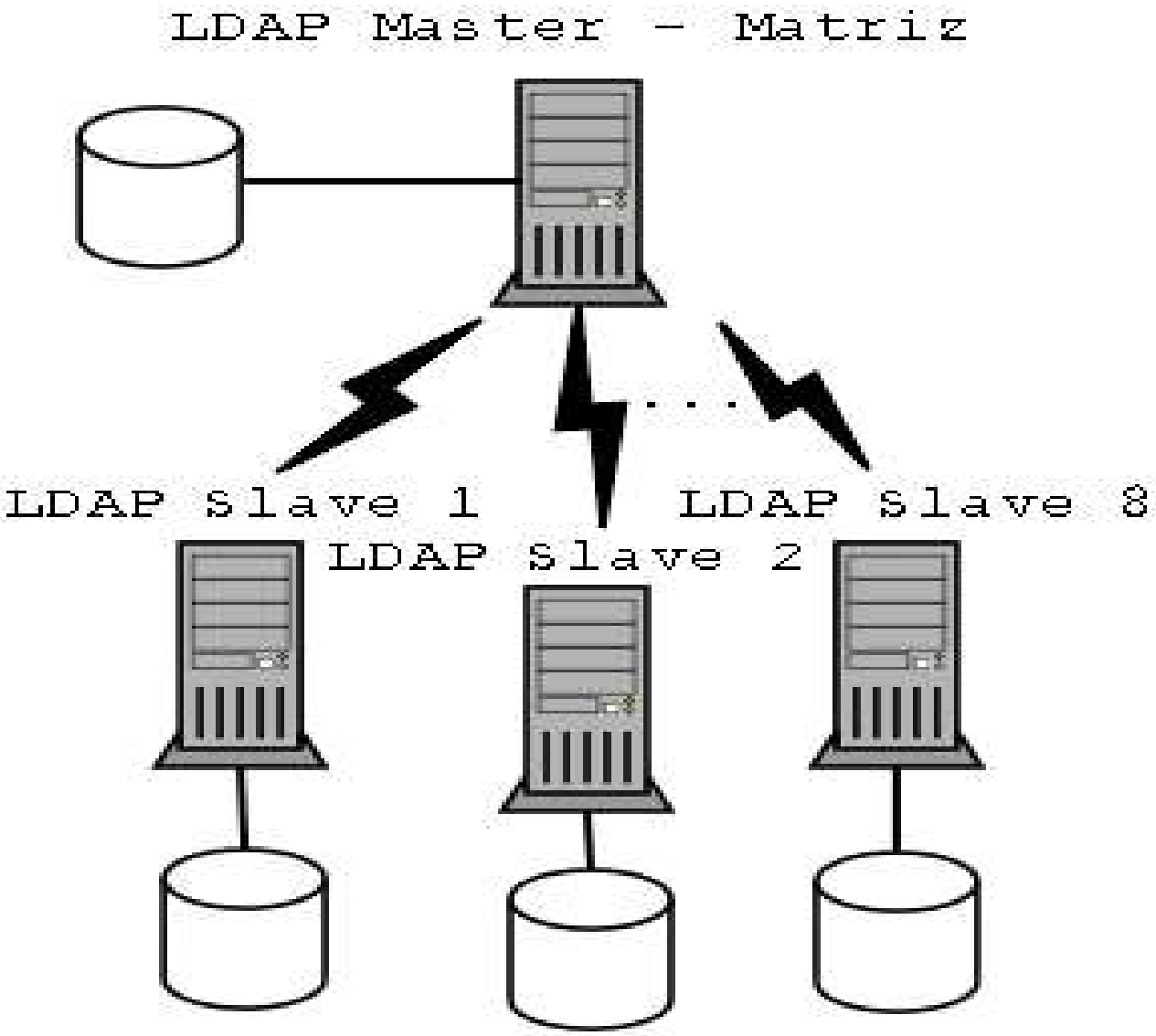


Camada SSL/TLS

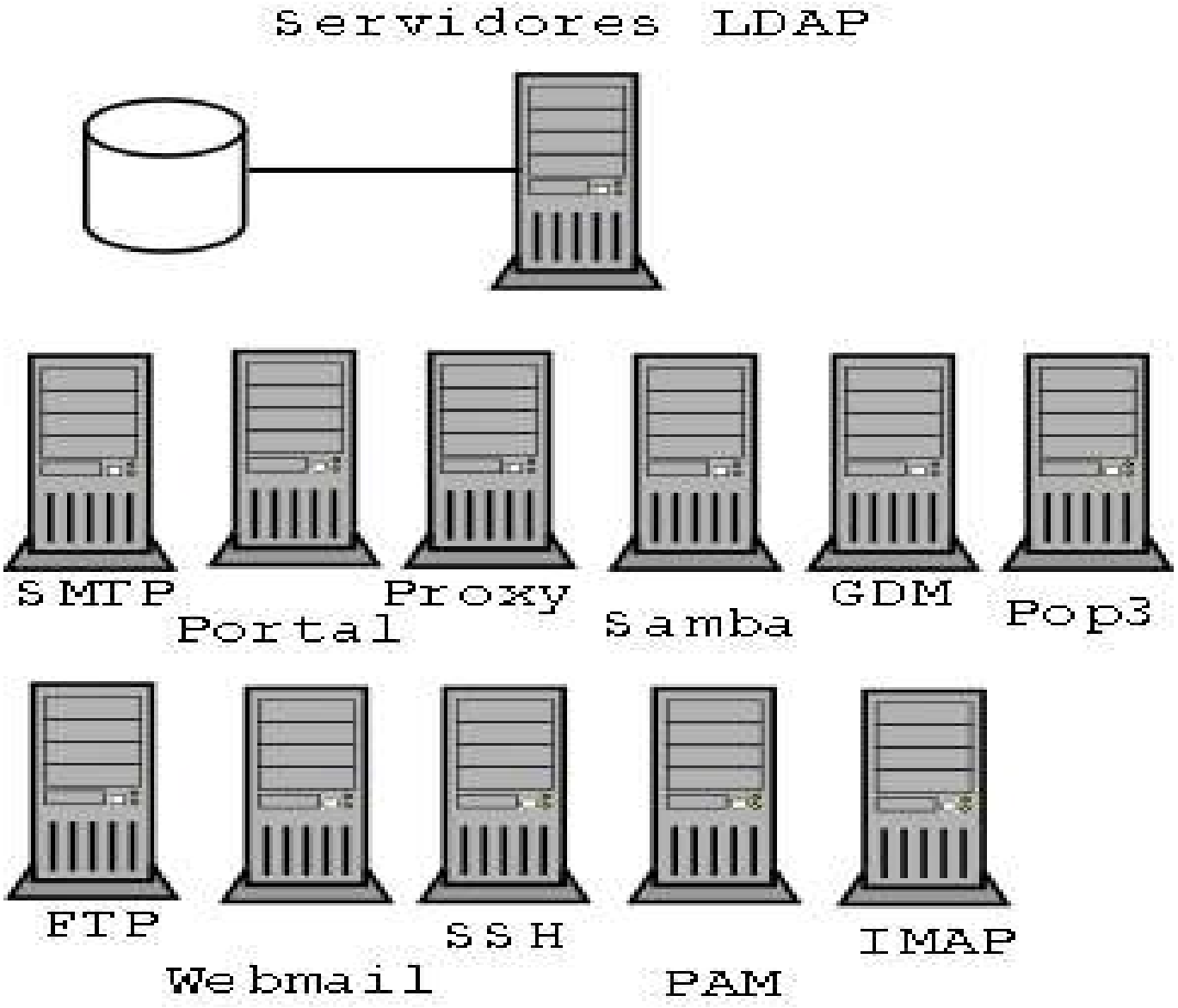
CASE – O Cliente

- + de 30 anos no mercado
- + de 2000 empregados
- 4 fabricas e 2 empresas coligadas
- Trabalha no mercado de exportaçao
- Certificada ISO 9002
- Slaves LDAP com Conectiva Linux
- Master e demais servidores com Slackware Linux

Replicaçao



Ambiente em Questão



Referencias

Understanding LDAP - IBM redbook
http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg244986.pdf

Sys Admin Guide for Directory Services
ftp://docs-pdf.sun.com/816-4856/816-4856.pdf

Introduction to OpenLDAP Directory
http://www.openldap.org/doc/admin21/intro.html

Uma Introduçàо ao LDAP
http://geocities.yahoo.com.br/cesarakg/introlda-ptbr.html

Documentaçao de Soluçao
Autor: Rodrigo Rubira Branco

FIM! Será mesmo?

DÚVIDAS?!?

Rodrigo Rubira Branco

rodrigo@firewalls.com.br