FACULDADES promove

Serviços de Diretórios - 02

Visão Geral do LDAP

Manassés Ferreira

21 de Agosto de 2017

Faculdades Promove - Sete Lagoas

Agenda

1. Protocolo Leve de Acesso a Diretório
2. O que é ?
3. Leve
4. Diretório
5. Protocolo de Acesso
6. Modelos LDAP
7. Resumo

Protocolo Leve de Acesso a Diretório

Protocolo Leve de Acesso a Diretório

Possibilidade de consolidar serviços existentes em um diretório simples que pode ser acessado por clientes LDAP a partir de vários fornecedores

Cinco características de um Serviço de Diretório

Leitura Eficaz para realizar leituras

Cinco características de um Serviço de Diretório

Leitura Eficaz para realizar leituras

Busca Possuir recursos de busca avançados

Cinco características de um Serviço de Diretório

Leitura	Eficaz para realizar leituras
Busca	Possuir recursos de busca avançados
Tipos	Permite aumentar/extender os tipos de informação armazenados

Cinco características de um Serviço de Diretório

Leitura	Eficaz para realizar leituras
Busca	Possuir recursos de busca avançados
Tipos	Permite aumentar/extender os tipos de informação armazenados
Distrib.	Implementar um modelo distribuído para armazenar informação

Cinco características de um Serviço de Diretório

Leitura	Eficaz para realizar leituras
Busca	Possuir recursos de busca avançados
Tipos	Permite aumentar/extender os tipos de informação armazenados
Distrib.	Implementar um modelo distribuído para armazenar informação
Consist.	Replicar de modo consistente a informação entre os servidores de diretório

O que é ?

LDAP: O que é ?

tools.ietf.org/html/rfc4510 [1]

Network Working Group K. Zeilenga, Ed.
Request for Comments: 4510 OpenLDAP Foundation
Obsoletes: 2251, 2252, 2253, 2254, 2255, June 2006
2256, 2829, 2830, 3377, 3771
Category: Standards Track

Lightweight Directory Access Protocol (LDAP):
Technical Specification Road Map

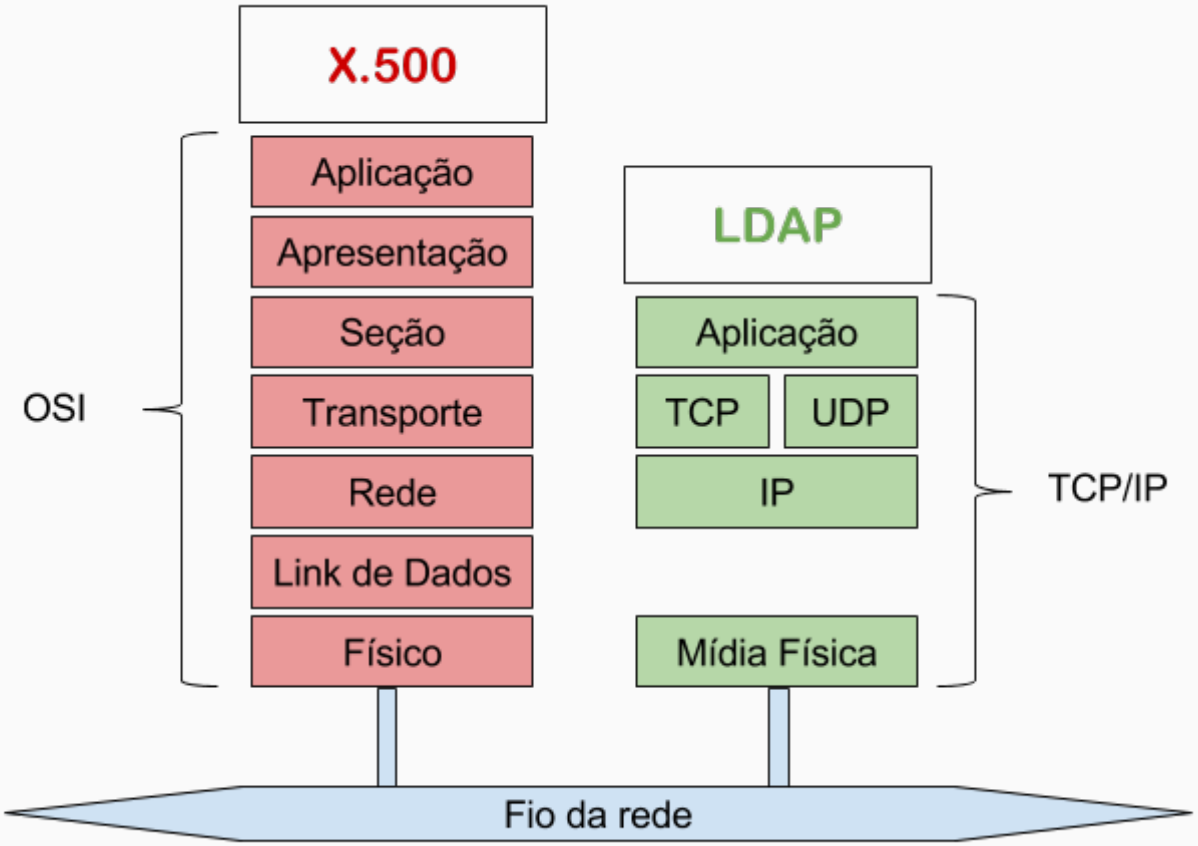
Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet

[1] Requests For Comments (RFC) is a type of publication from the Internet Engineering Task Force (IETF) and the Internet Society (ISOC), the principal technical development and standards-setting bodies for the Internet.

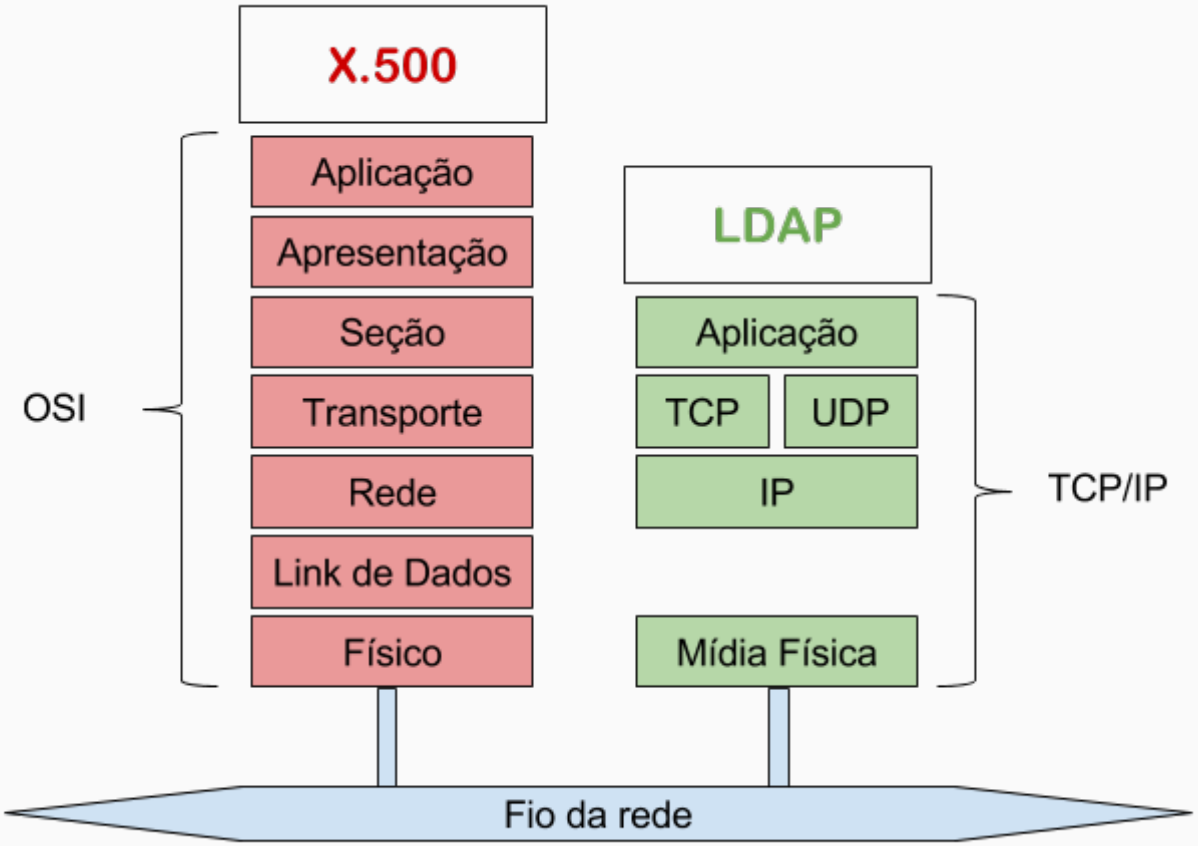
Leve

Leve



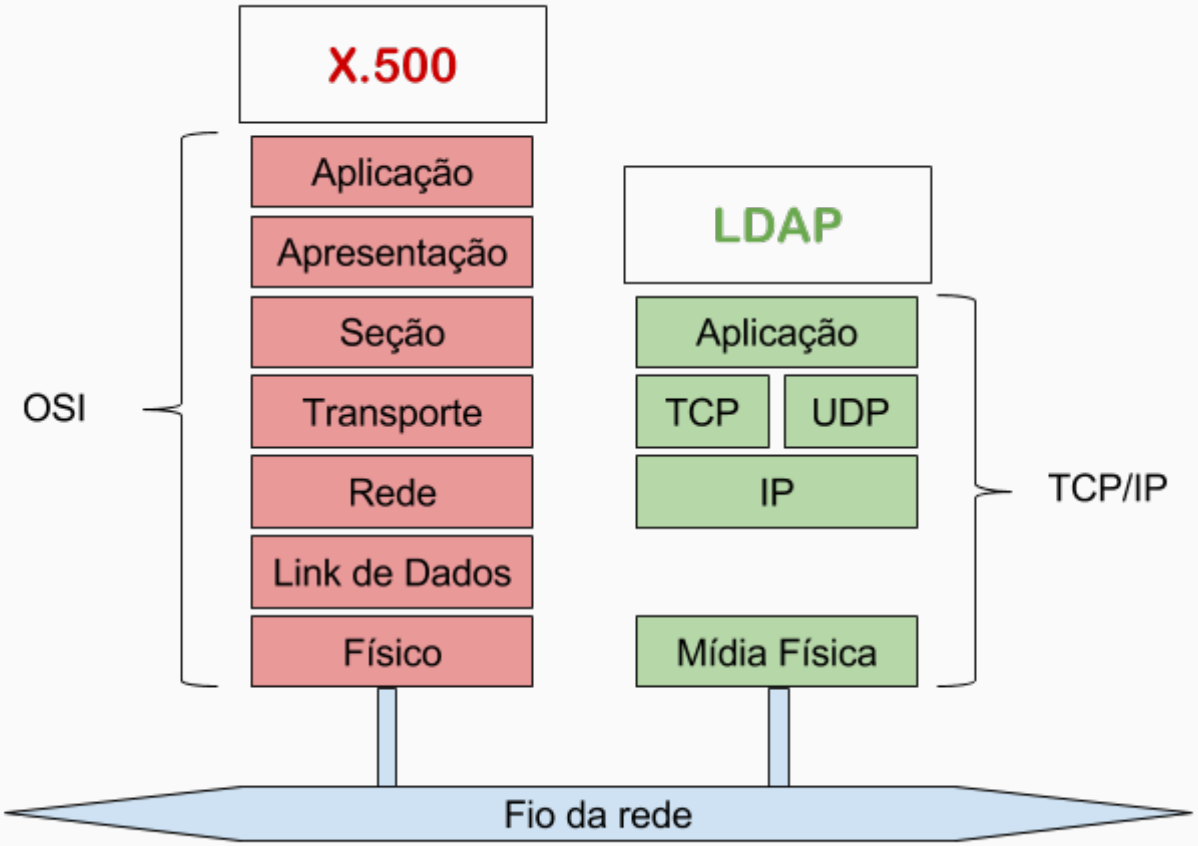
1. LDAP sobre TCP/IP (× X.500 sobre OSI)

Leve



1. LDAP sobre TCP/IP ($\times$ X.500 sobre OSI)
2. Modelo simples para programadores e administradores

Leve



1. LDAP sobre TCP/IP ($\times$ X.500 sobre OSI)
2. Modelo simples para programadores e administradores
3. Nove Operações (Quais ?)

Diretório

Diretório - Conceitos

https://tools.ietf.org/html/rfc4512

Directory is ”a collection of open systems cooperating to provide directory services”.

The information held in the Directory is collectively known as the Directory Information Base (DIB). A Directory user, which may be a human or other entity, accesses the Directory through a client (or Directory User Agent (DUA)). The client, on behalf of the directory user, interacts with one or more servers (or Directory System Agents (DSA)). A server holds a fragment of the DIB.

The DIB contains two classes of information:

1) user information (e.g., information provided and administrated by users). Section 2 describes the Model of User Information.

2) administrative and operational information (e.g., information used to administer and/or operate the directory). Section 3 describes the model of Directory Administrative and Operational Information.

Diretório - LDA não é ...

Não é uma substituição generalizada para serviços de ”diretórios especializados”(DNS, por exemplo).

Não é feito para armazenar dados arbitrários.

Protocolo de Acesso

Protocolo de Acesso

tools.ietf.org/html/rfc4511

The general model adopted by this protocol is one of clients performing protocol operations against servers. In this model, a client transmits a protocol request describing the operation to be performed to a server. The server is then responsible for performing the necessary operation(s) in the Directory. Upon completion of an operation, the server typically returns a response containing appropriate data to the requesting client.

Protocol operations are generally independent of one another. Each operation is processed as an atomic action, leaving the directory in a consistent state.

Although servers are required to return responses whenever such responses are defined in the protocol, there is no requirement for synchronous behavior on the part of either clients or servers. Requests and responses for multiple operations generally may be exchanged between a client and server in any order. If required,

Protocolo de Acesso - Camadas

tools.ietf.org/html/rfc4511 The term ”transport connection”refers to the underlying transport services used to carry the protocol exchange, as well as associations established by these services.

The term ”TLS layer”refers to Transport Layer Security (TLS) services used in providing security services, as well as associations established by these services.

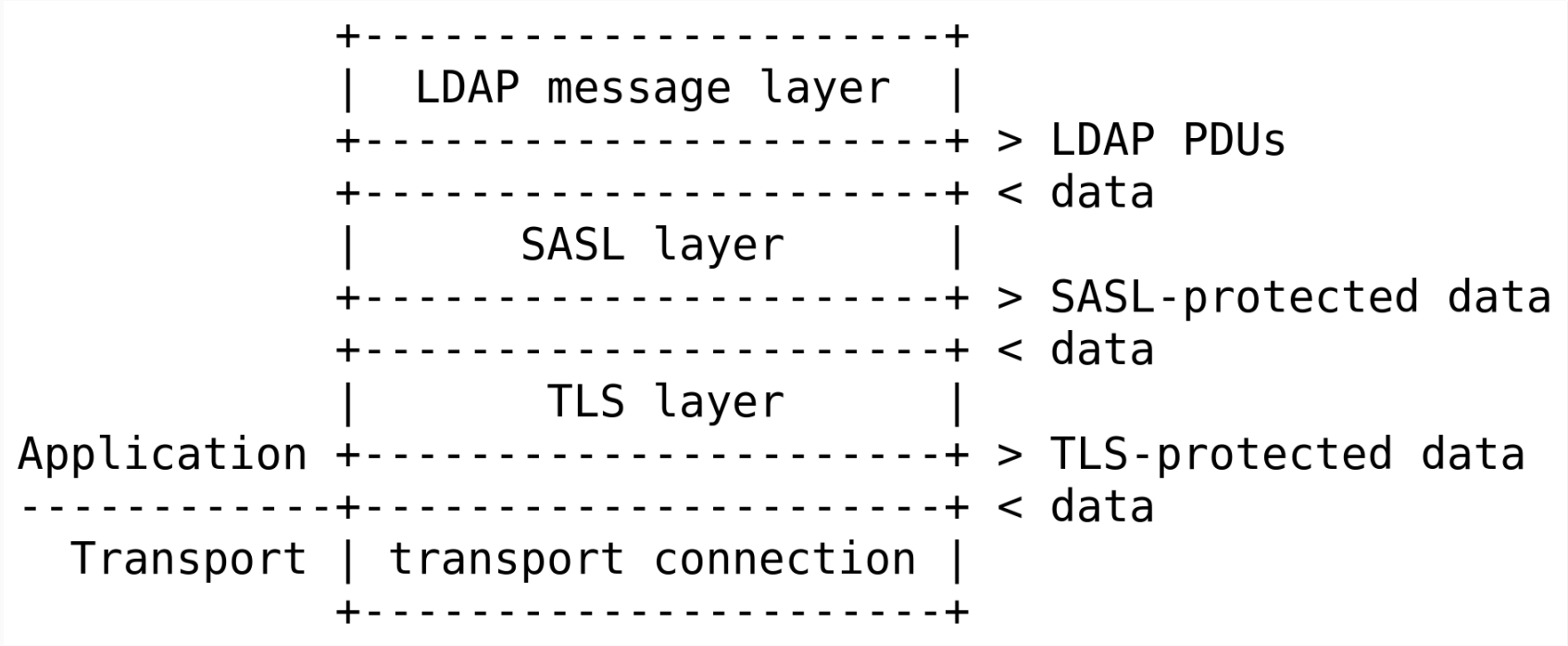
The term ”SASL layer”refers to Simply Authentication and Security Layer (SASL) services used in providing security services, as well as associations established by these services.

The term ”LDAP message layer”refers to the LDAP Message Protocol Data Unit (PDU) services used in providing directory services, as well as associations established by these services.

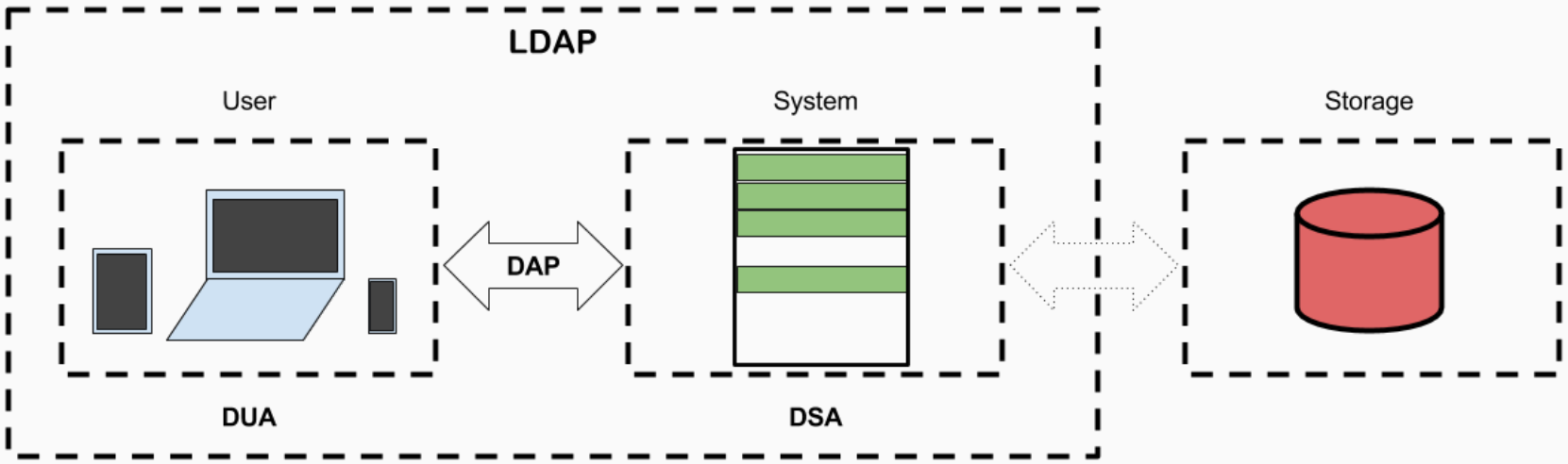
The term ”LDAP session”refers to combined services (transport connection, TLS layer, SASL layer, LDAP message layer) and their associations.

Protocolo de Acesso - Camadas

tools.ietf.org/html/rfc4511

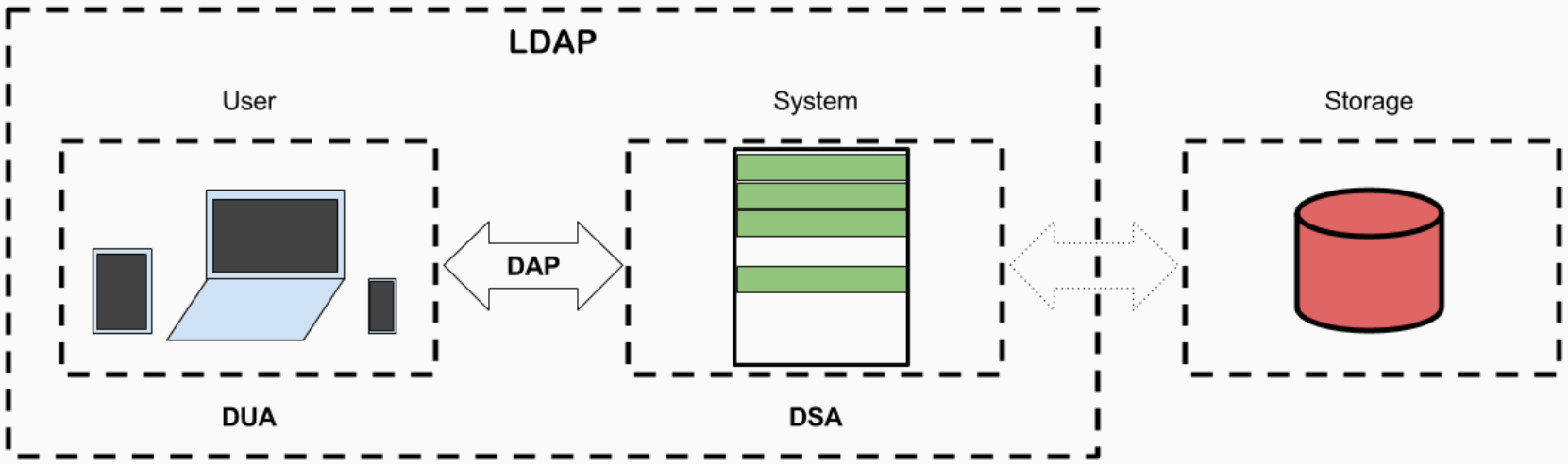


Protocolo de Acesso - Cliente/Servidor



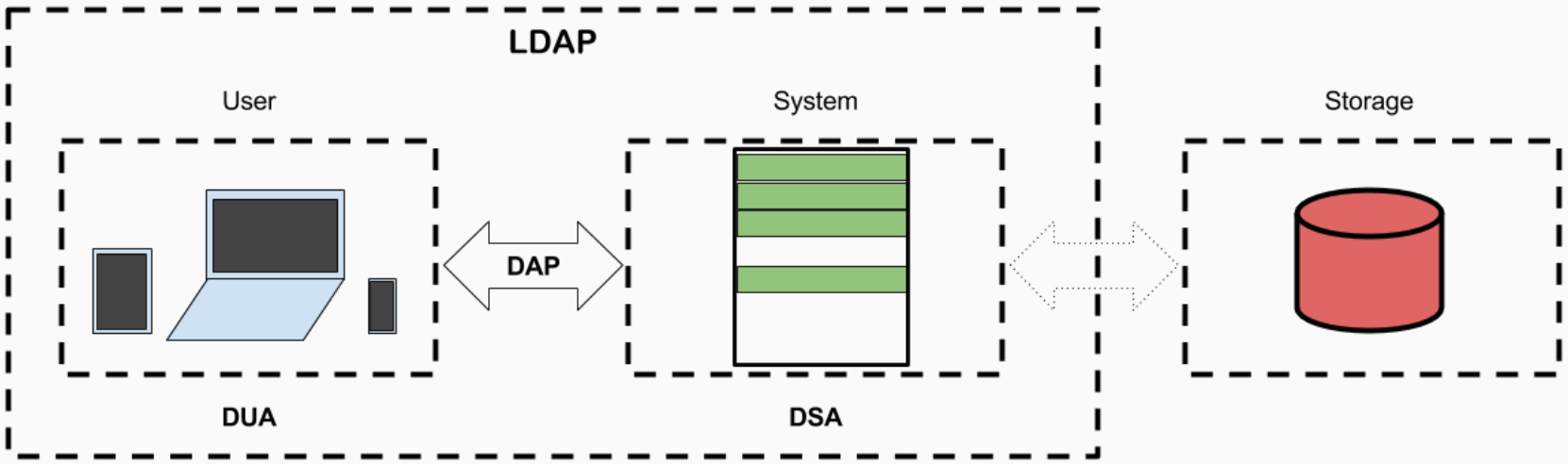
1. User: human or entity (thing! IoT)

Protocolo de Acesso - Cliente/Servidor



1. User: human or entity (thing! IoT)
2. System: server

Protocolo de Acesso - Cliente/Servidor



1. User: human or entity (thing! IoT)
2. System: server
3. Storage: LDAP não diz respeito à como implementar persistência. (vide próximo slide)

(Serviços de Diretórios $\times$ Banco de Dados)

1. SD é mais lido do que gravado

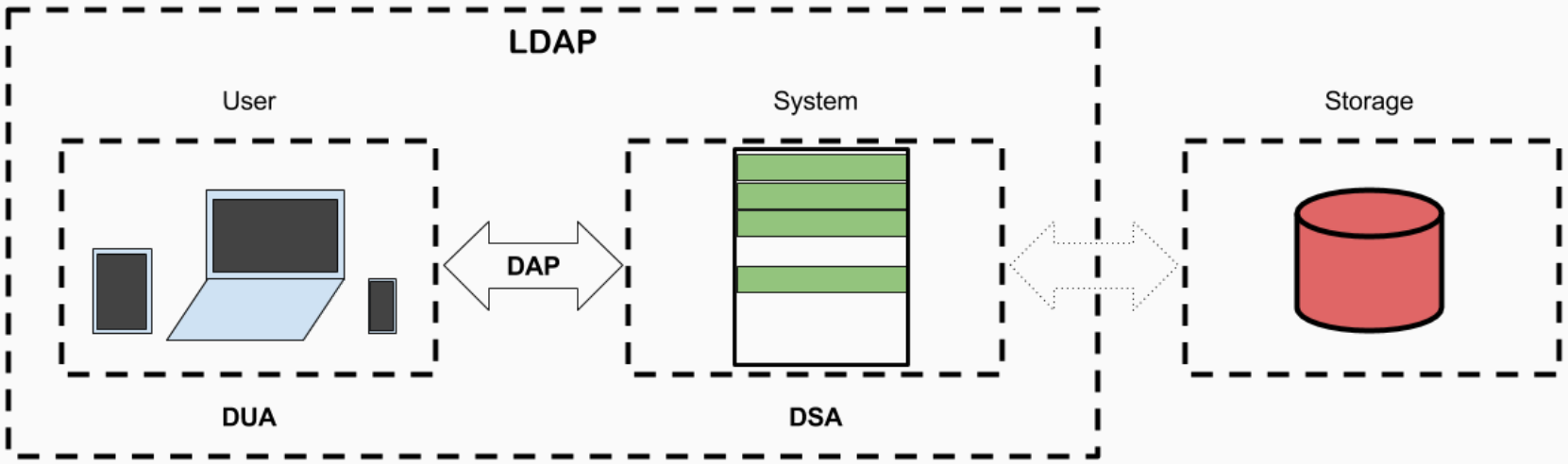
(Serviços de Diretórios $\times$ Banco de Dados)

1. SD é mais lido do que gravado
2. Em BD, transações e travas de escrita são essenciais

(Serviços de Diretórios $\times$ Banco de Dados)

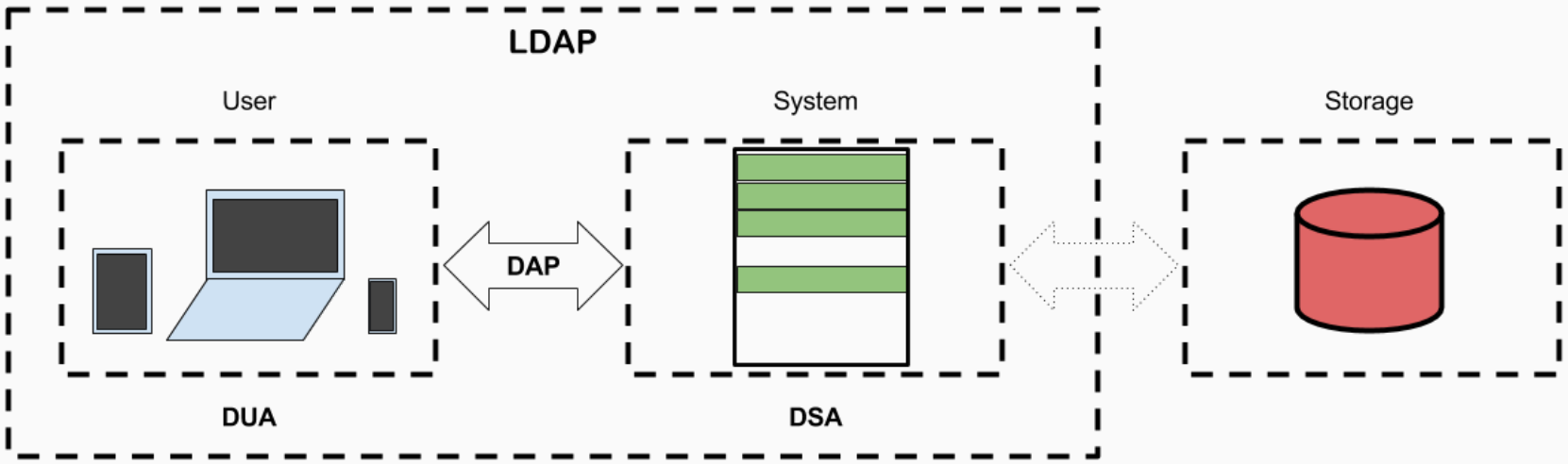
1. SD é mais lido do que gravado
2. Em BD, transações e travas de escrita são essenciais
3. Persistência do LDAP pode ser feita usando BD

Protocolo de Acesso - Semântica



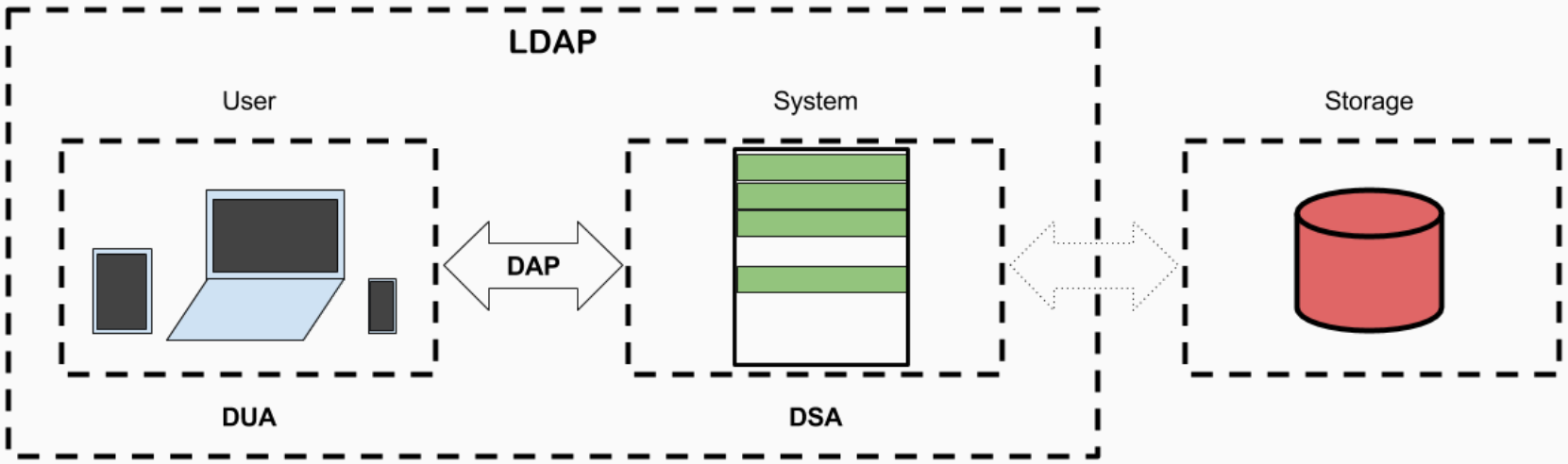
1. User: human or entity (thing! IoT)

Protocolo de Acesso - Semântica



1. User: human or entity (thing! IoT)
2. System: server

Protocolo de Acesso - Semântica

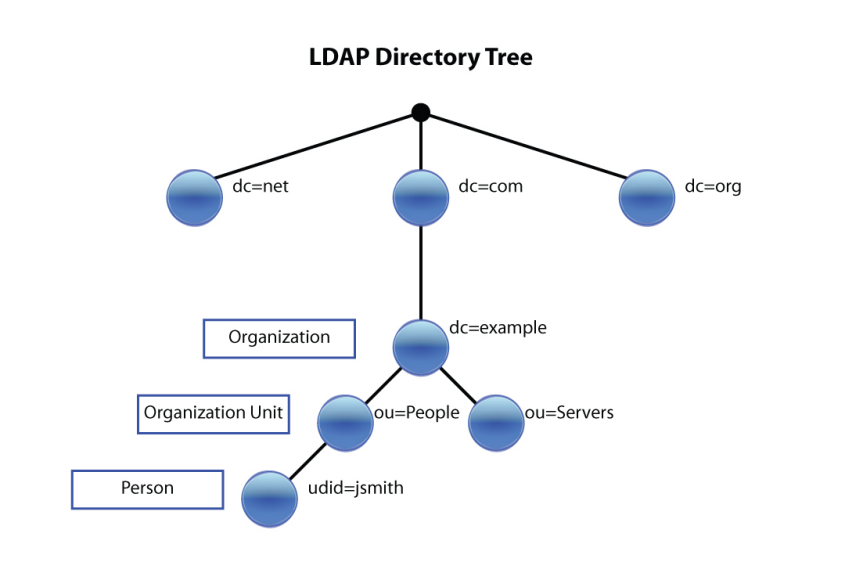


1. User: human or entity (thing! IoT)
2. System: server
3. Storage: LDAP não diz respeito à como implementar persistência. (vide próximo slide)

Modelos LDAP

Modelos LDAP

Modelo de informação
Modelo de nomes
Modelo funcional



Resumo

Resumo

LDAP is not just for user validation, any task that has the following properties might be a good use case for LDAP:

1. You need to locate ONE piece of data many times and you want it fast
2. You don’t care about the logic and relations between different data
3. You don’t update, add, or delete the data very often
4. The size of each data entry is small
5. You don’t mind having all these small pieces of data at a centralized place

Perguntas?