O Active Directory

Active directory

- Serviço de diretório extensível para gerenciar recursos da rede de modo eficiente
- Armazena informações detalhadas sobre cada recurso na rede
- Possibilidade de armazenar grandes quantidades de informações
- Uso de login único para os diversos serviços em uma rede

Elementos

- Cada recurso do AD é representado como um **objeto**.
- É possível restringir as permissões por meio de diretivas de grupo;
- A infraestrutura de segurança do AD usa as diretivas para impor modelos de segurança sobre vários objetos agrupados em um contexto lógico. Ex.:
  - Setores, departamentos, diretorias etc.

Permissões

- A gerência de permissões é feita de modo centralizado
- A autenticação também é centralizada
- Em uma rede podem haver vários servidores como controladores de domínio, mesmo com um único domínio
- Uma vez autenticados as configurações do servidor indicam a que recursos da rede este usuário tem acesso

LDAP

- O active directory é baseado no modelo LDAP (Lightweight Directory Access Protocol)
- Foi desenvolvido pelas empresas de telefonia ainda na década de 80 para armazenar informação sobre os usuário de telefones
- Dentro do diretório é possível armazenar informações no formato <tipo>:<valor>
- Ex.:
  - `telephoneNumber: +1 888 555 1232`
  - `mail: john@example.com`
  - `manager: cn=Barbara Doe,dc=example,dc=com`

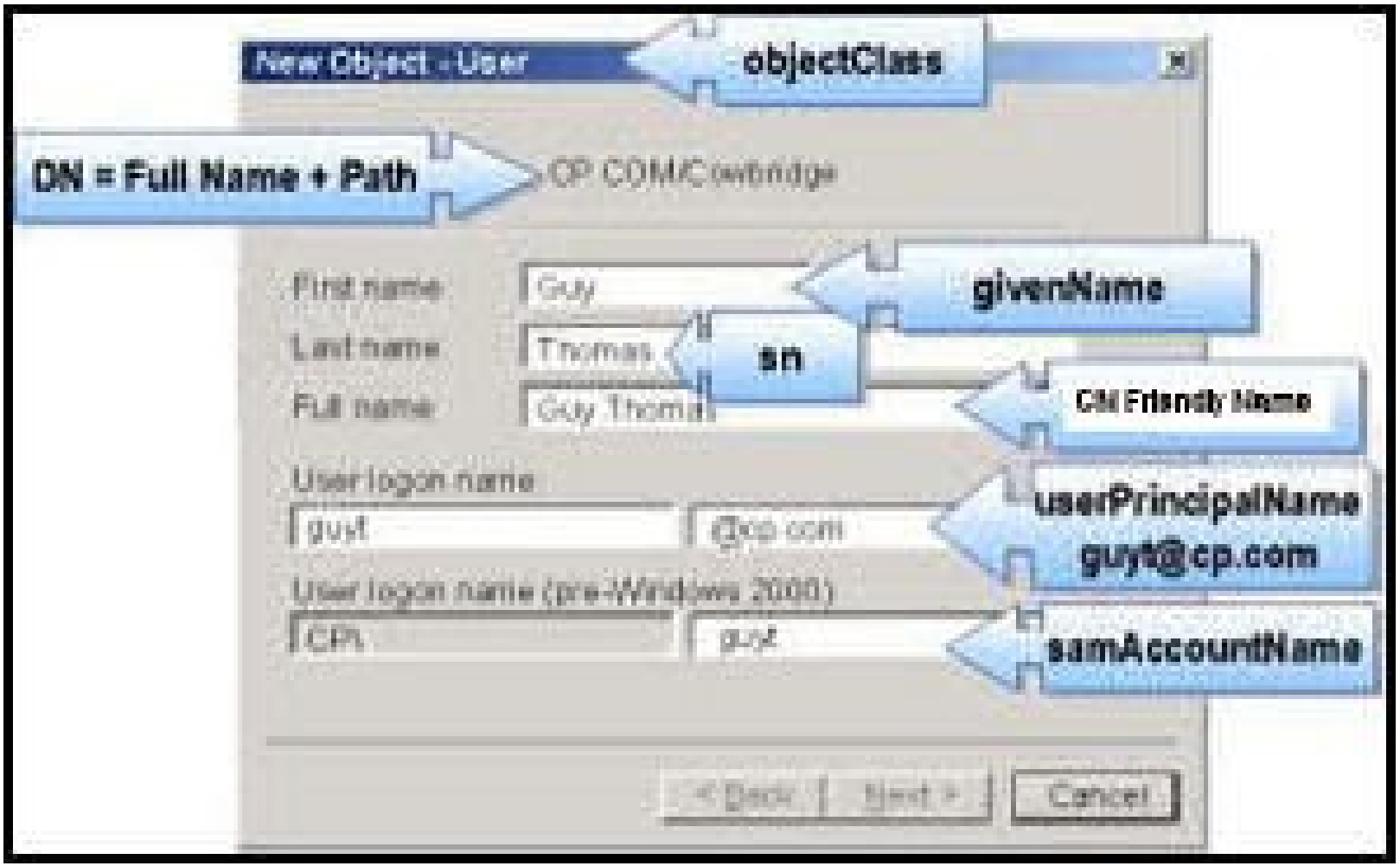
LDAP

- Assim o active directory pode armazenar qualquer tipo de informação sobre os usuários em questão
  - Ex.:
    - Nome do setor
    - Telefone
    - E-mail
    - Nome do chefe
    - etc.

Objetos do LDAP

- No active directory objetos podem ter vários atributos
- Atributos mais importantes:
  - DN = distinguished name
    - Nome único no diretório é composto do CN e OU e DC
  - CN = common name
    - Nome real do usuário
  - OU = Organizational Unit
    - Departamento ou setor que o usuário faz parte
- Ex.: Um usuário chamado: CSantana em um domínio Company.com teria seu DN:
  - `cn=CSantana, cn=Users, dc=Company, dc=com.`

Objetos LDAP



Arquitetura lógica do AD

- Objetos
- Domínios, árvores e florestas;
- Relações de confiança;
- Namespaces;
- Distribuição de dados;

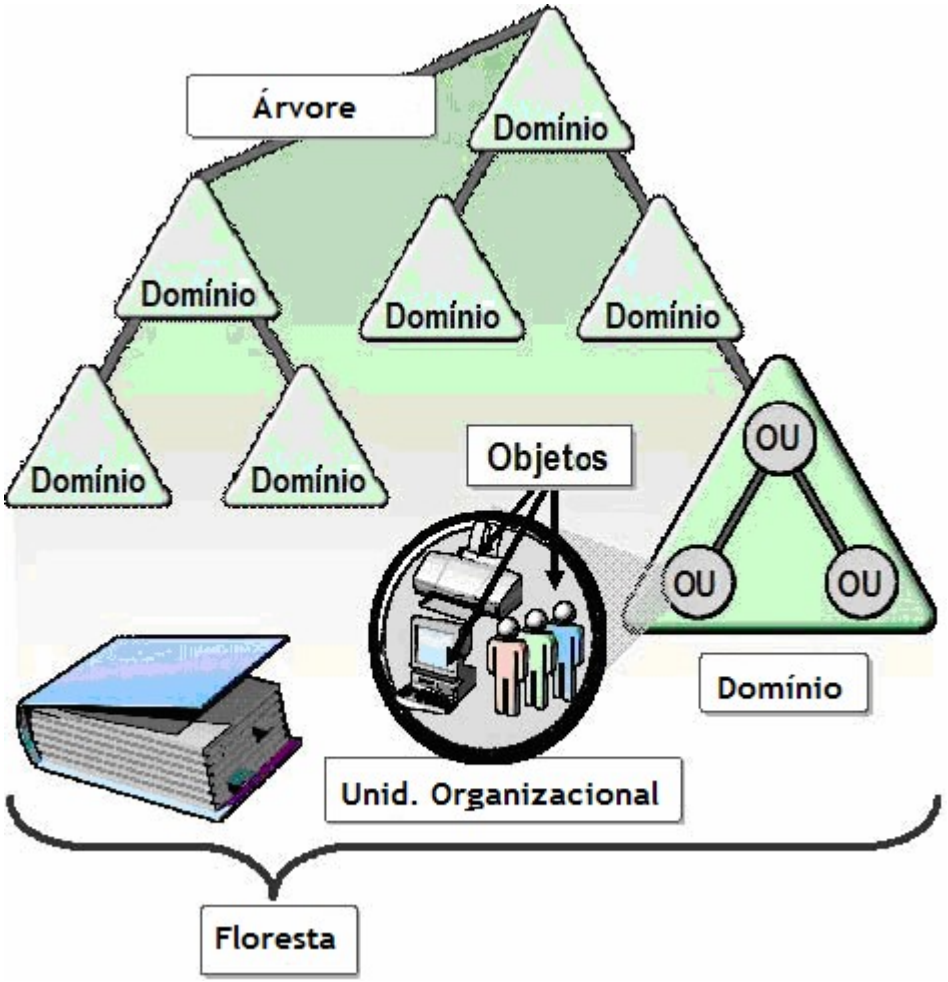
Objetos no AD

- Todo objeto é classificado em uma classe:
  - Usuário
  - Grupo
  - Computador
  - Impressora
  - Unidade organizacional
- Cada classe carrega consigo um conjunto de atributos e diretivas do que pode ser feito, nos objetos desta classe

Domínios Árvores e Florestas

- Domínio: o agrupamento lógico de objetos que permite o gerenciamento central dos mesmos.
- Árvore: agrupamento lógico de domínios em um namespace exclusivo ou grupo de domínios que compartilham o mesmo namespace.
- Floresta: agrupamento lógico de árvores de domínio ou grupo de árvores de domínios para compartilhar os recursos.

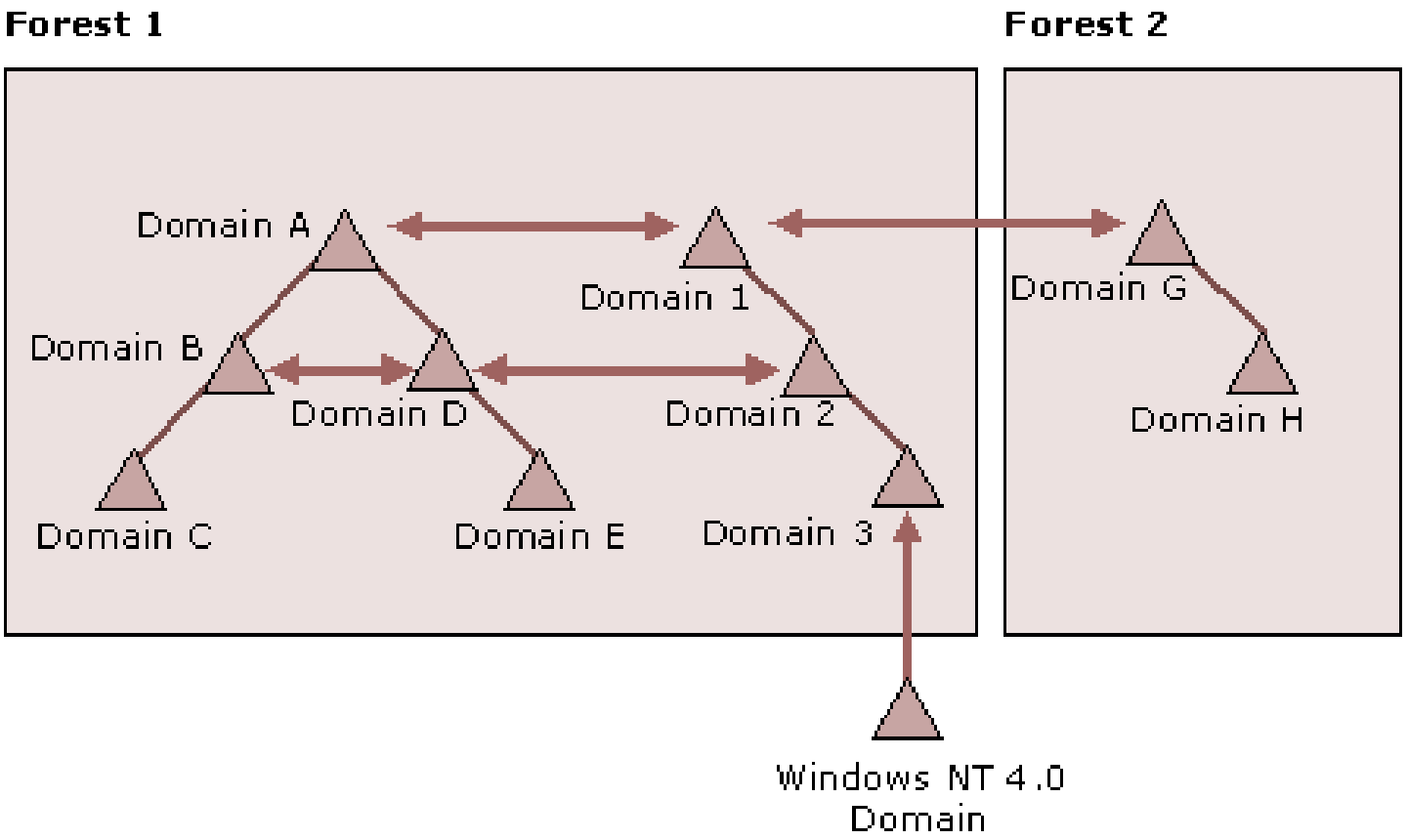
Domínios árvores e florestas



Relações de confiança

- Implicam em transferências de informações entre os vários domínios
- Se domínio ***A*** confia no domínio ***B*** isso implica que domínio ***B*** confia em domínio ***A***
- As relações também são passadas a diante, se ***A*** confia em ***B*** e ***B*** confia em ***C*** isso implica que ***A*** confia em ***C***

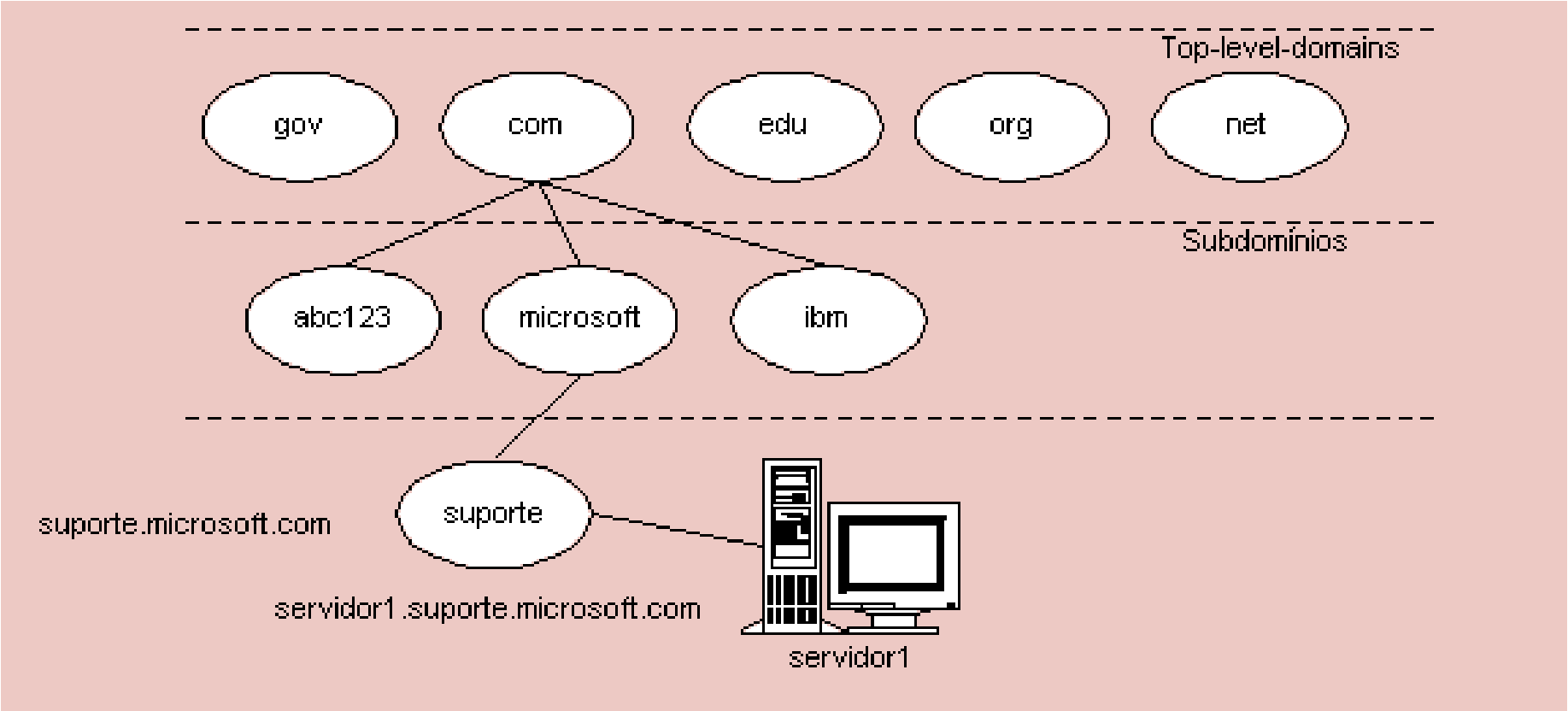
Relações de Confiança



Namespace

- Um namespace é o conjunto de nomes usados em um domínio.
- Não poderá haver dois equipamentos com o mesmo nome em um mesmo namespace.
- Associado à hierarquia de DNS

Namespace


Top-level-domains
gov
com
edu
org
net
Subdomínios
abc123
microsoft
ibm
suporte.microsoft.com
suporte
servidor1.suporte.microsoft.com
servidor1

Distribuição de dados;

- Dependentes das configurações de site da árvore de domínios
- Os sites descrevem a estrutura física da rede enquanto os domínios descrevem a estrutura lógica
- Um domínio pode ter vários sites e um site pode conter vários domínios
- Dentro de um domínio há ainda as unidades organizacionais, comumente usada para separar setores em um domínio

Grupos de usuários

- Grupos de segurança:
  - Podem ser usados para diferenciar usuários de uma mesma Unidade Organizacional
  - Um usuário pode participar de vários grupos
  - Políticas de segurança podem ser definidas por grupo de usuário
  - Facilitam a gerência de recursos na rede
- Grupos de distribuição:
  - São usados para propagação de e-mails usando o exchange

Grupos de usuários