



Aplicações TCP/IP parte II

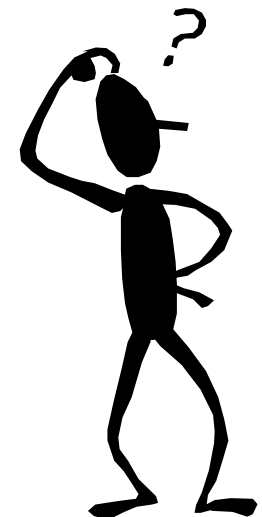
Prof. Walter Cunha

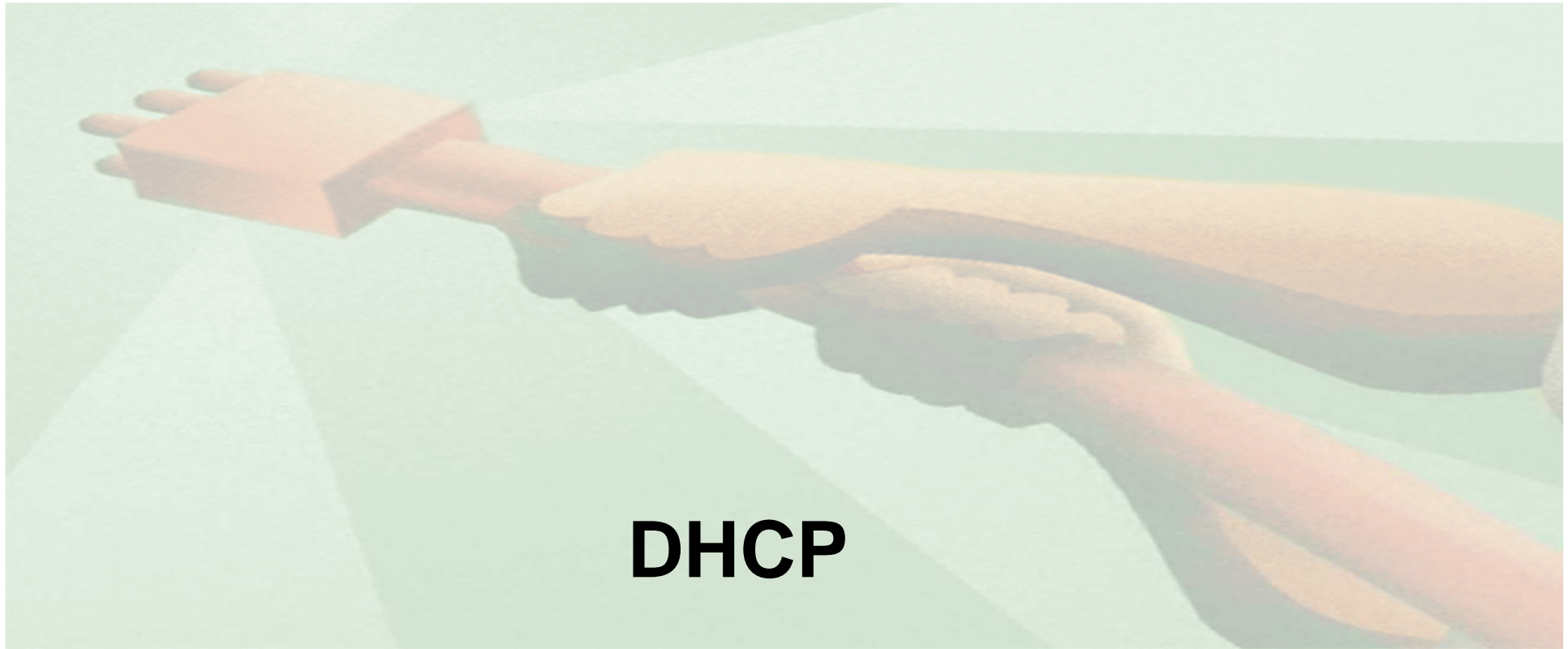
<http://www.itnerante.com.br/profile/WalterCunha>



Roteiro

1. DHCP
2. DNS
3. LDAP





DHCP

Dynamic Host Configuration Protocol

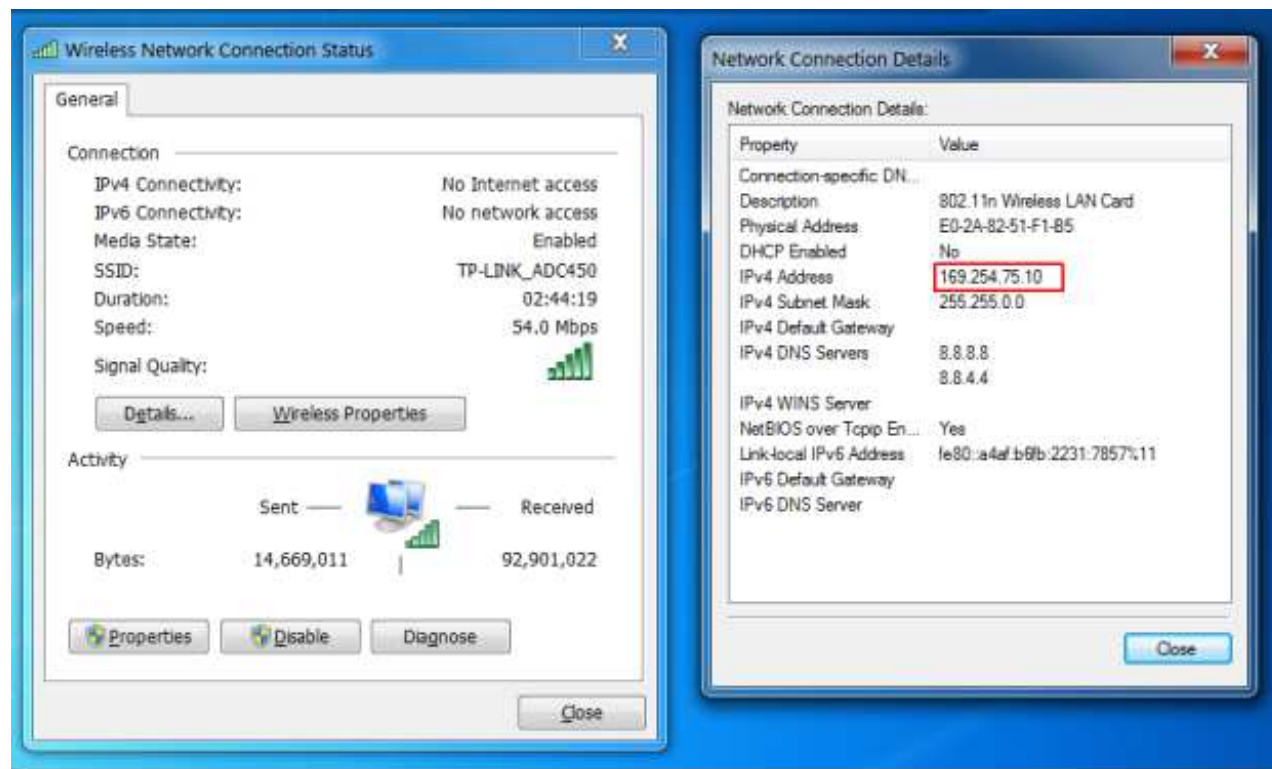
Serviços: DHCP - Definição

- O DHCP permite que todos os micros da rede recebam suas configurações de rede automaticamente a partir de um servidor central, sem que você precise ficar configurando os endereços manualmente em cada um.
- O objetivo principal é a simplificação da administração de uma rede.

Serviços: DHCP - Histórico

- RARP
 - Camada Baixa, Subutiliza o Quadro e Sem locação Dinâmica
- BOOTP
 - Mesma Porta do DHCP, Resolve em Parte a Subutilização, Sem locação Dinâmica
- DHCP
 - Todas as informações de inicialização necessárias, locação rápida e dinâmica de um endereço IP

Serviços: DHCP - APIPA



Autocofiguração: A Microsoft criou uma aplicação chamada de IP privado automático (APIPA), que foi implantado em milhões de máquinas e tornou-se de fato padrão (RFC 5735, 169.254.0.0/16).

Serviços: DHCP - Características

Servidor DHCP possui tabela pré configurada com parâmetros dos clientes e um conjunto de endereços IP a serem fornecidos aos clientes

- Portas UDP 67 e 68
- IP dinâmico ou fixo
- Máscaras de rede
- Mais info. de configuração das estações, como:
 - servidores de nome, roteadores default
 - rotas estáticas
 - servidores SMTP
 - ...

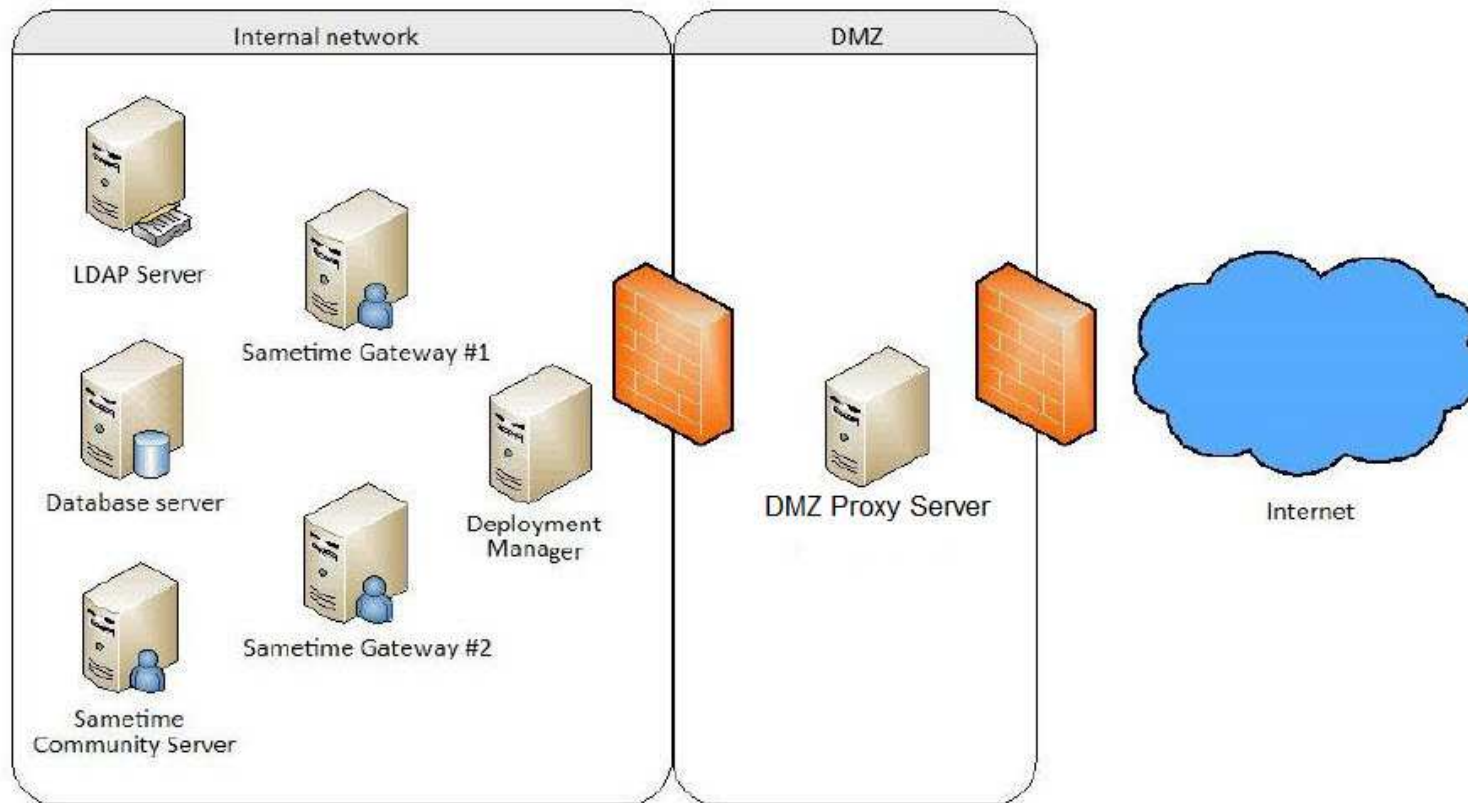
Serviços: DHCP

- Empréstimo pode ser do tipo:
 - **Manual**, amarrado ao MAC da estação (igual ao BOOTP)
 - **Automático**, quando este conecta-se pela primeira vez na rede, lhe é atribuído um endereço permanente.
 - **Dinâmico**, o IP é locado temporariamente a um equipamento e periodicamente, é necessária a atualização dessa locação

Serviços: DHCP

- O RARP é usado quando uma estação precisa obter sua configuração de rede via DHCP.
- DHCP é protocolo (statefull) de camada de aplicação (tem porta), embora opere na camada de Redes e de Enlace.
- O servidor DHCP pode publicar o par (nome da estação, endereço IP) em um servidor de DNS dinâmico (DDNS)

Serviços: DHCP – IP Fixo



É importante deixar claro que, em uma rede, o administrador deverá deixar fixo em algumas máquinas os seus endereços IP.

Questões

(Indefinida) “O DHCP (Dynamic Host Configuration Protocol) é um _____ de serviço _____ que oferece configuração dinâmica de terminais, com concessão de _____ de host e outros parâmetros de configuração para clientes de rede.” Assinale a alternativa que completa corretamente a afirmativa anterior:

- A) protocolo, TCP/IP, direitos D) endereço, IP, site
- B) protocolo, TCP/IP, endereços IP E) endereço, TCP/IP, direitos
- C) portal, IP, direitos

Questões

(Indefinida) “O DHCP (Dynamic Host Configuration Protocol) é um _____ de serviço _____ que oferece configuração dinâmica de terminais, com concessão de _____ de host e outros parâmetros de configuração para clientes de rede.” Assinale a alternativa que completa corretamente a afirmativa anterior:

- A) protocolo, TCP/IP, direitos D) endereço, IP, site
- B) protocolo, TCP/IP, endereços IP** E) endereço, TCP/IP, direitos
- C) portal, IP, direitos

Questões

(Consulplan) Que protocolo é utilizado por uma estação cliente DHCP para detectar um conflito de endereço?

A) DCCP B) SCTP C) NDP D) UDP E) ARP

(ESAG/TCE-RR 2006 ADAP) DHCP usa como padrão portas diferentes do protocolo BOOTP.

Questões

(Consulplan) Que protocolo é utilizado por uma estação cliente DHCP para detectar um conflito de endereço?

A) DCCP B) SCTP C) NDP D) UDP E) ARP

E (ESAG/TCE-RR 2006 ADAP) DHCP usa como padrão portas diferentes do protocolo BOOTP.

Questões

Na configuração e na administração de redes TCP/IP, em especial em redes locais, a distribuição de endereços IP e de informações de configuração da rede e do roteamento torna-se rapidamente um problema de difícil tratamento, à medida que tais ambientes vêm passando de uma situação relativamente estática para uma situação em que vários computadores necessitam se conectar às redes apenas temporariamente. Esse problema se agrava com o advento das tecnologias de rede sem fio e com a utilização cada vez maior de computadores portáteis, pois os computadores podem ser movidos de um lugar para outro rápida e facilmente. No que se refere ao protocolo DHCP (*dynamic host configuration protocol*), que permite a atribuição de parâmetros de configuração de maneira dinâmica em uma rede TCP/IP, assinale a opção correta.

Questões

- a) DHCP é um protocolo stateless, no qual o cliente simplesmente envia uma solicitação de informações de configuração ao servidor e fica esperando uma resposta. Se uma resposta chegar, o cliente começa a utilizar as informações de configuração nela fornecidas. Se não houver resposta, o cliente limita-se a repetir a solicitação até obter as informações desejadas.
- b) Para utilizar DHCP, o cliente necessita, no mínimo, conhecer a priori o endereço IP de um dos servidores DHCP presentes na rede.
- c) O servidor DHCP decide acerca da alocação de endereços IP somente com base na quantidade de endereços IP disponíveis.
- d) DHCP permite configuração completamente dinâmica, modo de operação em que um servidor aloca um endereço para um computador por um período de tempo limitado. Nesse caso, o computador não poderá terminar a alocação do endereço antes da expiração do prazo definido pelo servidor.
- e) A utilização de DHCP permite configurar redes TCP/IP em que a quantidade de computadores pode exceder a quantidade de endereços IP disponíveis. Nessa situação, caso a quantidade de computadores ativos simultaneamente exceda a quantidade de endereços IP disponíveis, os computadores do grupo excedente não receberão informações de configuração para utilizar a rede.

Questões

- a) DHCP é um protocolo **stateless**, no qual o cliente simplesmente envia uma solicitação de informações de configuração ao servidor e fica esperando uma resposta. Se uma resposta chegar, o cliente começa a utilizar as informações de configuração nela fornecidas. Se não houver resposta, o cliente limita-se a repetir a solicitação até obter as informações desejadas.
- b) Para utilizar DHCP, o cliente necessita, no mínimo, **conhecer a priori o endereço IP de um dos servidores DHCP presentes na rede**.
- c) O servidor DHCP decide acerca da alocação de endereços IP **somente** com base na quantidade de endereços IP disponíveis.
- d) DHCP permite configuração completamente dinâmica, modo de operação em que um servidor aloca um endereço para um computador por um período de tempo limitado. **Nesse caso, o computador não poderá terminar a alocação do endereço antes da expiração do prazo definido pelo servidor.**
- e) A utilização de DHCP permite configurar redes TCP/IP em que a quantidade de computadores pode exceder a quantidade de endereços IP disponíveis. Nessa situação, caso a quantidade de computadores ativos simultaneamente exceda a quantidade de endereços IP disponíveis, os computadores do grupo excedente não receberão informações de configuração para utilizar a rede.

Questões

(ESAF/CGU-TI 2006) 44- O DHCP possibilita a distribuição de endereços IP para máquinas na rede.

Com relação aos tipos de distribuição possíveis com o uso do DHCP é correto afirmar que

- a) na distribuição automática é definido um tempo de validade, possibilitando o reaproveitamento de endereços IP. Nesses casos, os endereços IP são desvinculados dos respectivos endereços MAC.
- b) na distribuição manual, um endereço IP é associado de forma estática a um endereço MAC.
- c) na distribuição dinâmica, os endereços são distribuídos à medida que novas máquinas são inseridas na rede. Neste caso, os endereços IP são associados de forma estática a endereços MAC, não permitindo o reaproveitamento de endereços IP.
- d) para impedir a alta rotatividade dos endereços IP quando se utiliza a distribuição automática, faixas de endereços MAC e IP são especificados no servidor DHCP.
- e) para gerenciar a alta rotatividade dos endereços IP quando se utiliza a distribuição dinâmica, faixas de endereços MAC e IP são especificadas e vinculadas manualmente no servidor DHCP.

Questões

(ESAF/CGU-TI 2006) 44- O DHCP possibilita a distribuição de endereços IP para máquinas na rede.

Com relação aos tipos de distribuição possíveis com o uso do DHCP é correto afirmar que

- a) na distribuição **automática** (dinâmica) é definido um tempo de validade, possibilitando o reaproveitamento de endereços IP. Nesses casos, os endereços IP são desvinculados dos respectivos endereços MAC.
- b) na distribuição manual, um endereço IP é associado de forma estática a um endereço MAC.
- c) na distribuição **dinâmica** (automática), os endereços são distribuídos à medida que novas máquinas são inseridas na rede. Neste caso, os endereços IP são associados de forma estática a endereços MAC, não permitindo o reaproveitamento de endereços IP.
- d) para impedir a alta rotatividade dos endereços IP quando se utiliza a distribuição **automática**, faixas de endereços MAC e IP são especificados no servidor DHCP.
- e) para gerenciar a alta rotatividade dos endereços IP quando se utiliza a distribuição dinâmica, faixas de endereços MAC e IP são especificadas e **vinculadas manualmente no servidor DHCP**.

Serviços: DHCP - Cliente

- Quando o dhclient, o cliente DHCP, é executado na máquina cliente, ele começa a transmissão por difusão de requisições de informações de configuração.
 - Por padrão, estas solicitações são na porta UDP 68.
 - O servidor responde na UDP 67
- Um cliente DHCP pode passar por seis estados de aquisição:
 - INICIALIZA
 - SELECIONA
 - SOLICITA
 - LIMITE
 - RENOVA
 - VINCULA NOVAMENTE

Serviços: DHCP - Mensagens

DHCP DISCOVER - Broadcast para localização de servidor DHCP

DHCP OFFER - Oferta de endereço IP para um cliente

DHCP REQUEST - Requisição do endereço IP oferecido (bcast)

DHCP DECLINE - Informa que houve um erro na oferta

DHCP ACK - Confirmação do servidor sobre a atribuição do end.

DHCP NAK - Negativa de fornecimento do endereço (raro)

DHCP RELEASE - Cliente libera o endereço IP utilizado (raro)

DHCP INFORM - Cliente que já possui endereço IP pode requisitar outras informações de configuração respectivas àquele endereço

Serviços: DHCP - Início do Lease



DHCP DISCOVER (broadcast, UDP 67)



DHCP OFFER (IP, tempo, params) de A



DHCP OFFER (IP, tempo, params) de B



DHCP REQUEST para A (broadcast)



ou

DHCP DECLINE para A (parâmetros errados)



DHCP ACK de A

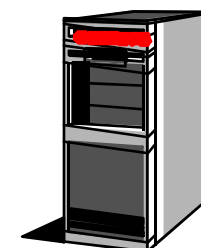


ou

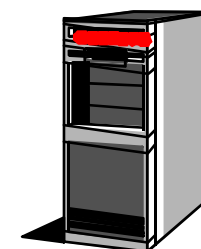
DHCP NACK de A



A



B



Serviços: DHCP - Renovação

... Após 50% do tempo de Empréstimo



DHCP REQUEST para A (broadcast)



DHCP ACK de A



...

ou

DHCP NACK de A



DHCP DISCOVER para A (broadcast)



A



B



Serviços – DHCP Formato PDU

| | | | | |
|------------------------------------|----------|----------|----------|----|
| 0 | 7 | 15 | 23 | 31 |
| Octeto 1 | Octeto 2 | Octeto 3 | Octeto 4 | |
| OP | HTYPE | HLEN | HOPS | |
| TRANSACTION ID | | | | |
| SECONDS | | FLAGS | | |
| CLIENT IP ADDRESS | | | | |
| YOUR IP ADDRESS | | | | |
| SERVER IP ADDRESS | | | | |
| ROUTER IP ADDRESS | | | | |
| CLIENT HARDWARE ADDRESS (16 bytes) | | | | |
| SERVER HOST NAME (64 bytes) | | | | |
| BOOT FILE NAME (128 bytes) | | | | |
| OPTIONS (Variavel) | | | | |

Serviços – DHCP Formato PDU

| CAMPO | INFORMAÇÕES |
|------------------------|---|
| OP | Numa mensagem DHCP, uma solicitação e uma resposta possuem os mesmos campos. O que as diferenciam é o conteúdo deste campo. A informação um indica uma solicitação, a informação dois indica uma resposta |
| HTYPE | Informa o padrão de rede utilizado pelo adaptador de rede |
| HLEN | Informa o tamanho do endereço MAC do adaptador de rede |
| HOPS | Quantidade de roteadores pelos quais a mensagem deverá passar |
| ID DE TRANSAÇÕES | Número de identificação da mensagem |
| SEGUNDOS | Quantidade de tempo em segundos desde que o cliente fez a inicialização |
| FLAGS | Utilizado para "setar" opções especiais de resposta às solicitações |
| ENDEREÇO IP DO CLIENTE | Em uma solicitação o cliente informa o seu endereço IP (possível quando o cliente conhece o seu endereço) |

Serviços – DHCP Formato PDU

| | |
|-----------------------------|---|
| ENDEREÇO IP DO CLIENTE | Em uma solicitação o cliente informa o seu endereço IP (possível quando o cliente conhece o seu endereço) |
| SEU ENDEREÇO IP | Utilizado pelo servidor para enviar informação do endereço IP disponível para o cliente que solicitou. |
| ENDEREÇO IP DO SERVIDOR | Preenchido pelo cliente quando ele quer obter uma informação de um servidor específico. |
| ENDEREÇO IP DO ROTEADOR | Preenchido pelo servidor para informar ao cliente o endereço IP do roteador da rede local |
| END. DE HARDWARE DO CLIENTE | Informação do endereço MAC do cliente |
| NOME DO HOST DO SERVIDOR | Quando esses campos não são utilizados para enviar as informações pertinentes a cada um (nome do servidor e informação do sistema operacional que será inicializado no cliente) o DHCP utiliza-o remetendo informações adicionais transformando-os em campo de OPÇÕES, otimizando assim a utilização da mensagem. |
| NOME DO ARQUIVO DE PARTIDA | Nome do arquivo que contém a imagem de memória da(s) estação (ões) correspondente(s) |
| OPÇÕES | Esse campo é utilizado para informar que tipo de resposta ou solicitação DHCP (DHCPDISCOVER, DHCPPOFFER etc.) está sendo enviada para o cliente ou para o servidor. |

Questões

(FCC/TRT-RR 2011) No modelo *TCP/IP*, são protocolos respectivamente atuantes nas camadas de aplicação, transporte e rede:

- (A) SMTP, TCP e DHCP.
- (B) UDP, TCP e DNS.
- (C) DHCP, ICMP e IPv6.
- (D) DNS, SMTP e IPSec.
- (E) SMTP, HTTPS e RTP.

Questões

(FCC/TRT-RR 2011) No modelo *TCP/IP*, são protocolos respectivamente atuantes nas camadas de aplicação, transporte e rede:

- (A) SMTP, TCP e DHCP.
- (B) UDP, TCP e DNS.
- (C) DHCP, ICMP e IPv6.
- (D) DNS, SMTP e IPSec.
- (E) SMTP, HTTPS e RTP.

Questões

(FCC/TRF-1 2011) Em redes locais baseadas em TCP/IP, o protocolo DHCP atua tipicamente entre as camadas:

- (A) Aplicação e Transporte.
- (B) Transporte e Rede.
- (C) Rede e Enlace.
- (D) Transporte e Enlace.
- (E) Enlace e Física.

Questões

(FCC/TRF-1 2011) Em redes locais baseadas em TCP/IP, o protocolo DHCP atua tipicamente entre as camadas:

- (A) Aplicação e Transporte.
- (B) Transporte e Rede.
- (C) Rede e Enlace.
- (D) Transporte e Enlace.
- (E) Enlace e Física.

Questões

(CESPE/TCU 2008) O administrador da rede reclamou eventual ocorrência de conflitos de endereçamento IP entre computadores da rede. Nessa situação, o analista deve orientá-lo no sentido de que, em uma rede com mais de um servidor DHCP, os escopos dos servidores podem se sobrepor, e que, se for esse o caso, podem acontecer situações nas quais os servidores aloquem endereços a partir de um mesmo conjunto de endereços. Em decorrência disso, diferentes clientes podem receber um mesmo endereço, se não houver um mecanismo que detecte conflitos.

(CGU/SEFAZ-CE 2007) Uma mensagem de oferta DHCP (Dynamic Host Configuration Protocol) contém um identificador da transação da mensagem de descoberta recebido, o endereço IP proposto para a máquina cliente, a máscara de rede e o intervalo de tempo de aluguel do endereço IP. A mensagem de descoberta DHCP é enviada por um cliente dentro de um pacote UDP.

Questões

- C (CESPE/TCU 2008) O administrador da rede reclamou eventual ocorrência de conflitos de endereçamento IP entre computadores da rede. Nessa situação, o analista deve orientá-lo no sentido de que, em uma rede com mais de um servidor DHCP, os escopos dos servidores podem se sobrepor, e que, se for esse o caso, podem acontecer situações nas quais os servidores aloquem endereços a partir de um mesmo conjunto de endereços. Em decorrência disso, diferentes clientes podem receber um mesmo endereço, se não houver um mecanismo que detecte conflitos.
- C (CGU/SEFAZ-CE 2007) Uma mensagem de oferta DHCP (Dynamic Host Configuration Protocol) contém um identificador da transação da mensagem de descoberta recebido, o endereço IP proposto para a máquina cliente, a máscara de rede e o intervalo de tempo de aluguel do endereço IP. A mensagem de descoberta DHCP é enviada por um cliente dentro de um pacote UDP.

Questões

(ESAF/ANA 2009) Se um cliente interrompe imediatamente o uso de um endereço IP e retorna ao estado INICIALIZA, ele recebeu do servidor DHCP, a mensagem

- a) DHCPNACK
- b) DHCPREQUEST
- c) DHCPACK
- d) DHCPOFFER
- e) DHCPDISCOVER

Questões

(ESAF/ANA 2009) Se um cliente interrompe imediatamente o uso de um endereço IP e retorna ao estado INICIALIZA, ele recebeu do servidor DHCP, a mensagem

- a) **DHCPNACK**
- b) DHCPREQUEST
- c) DHCPACK
- d) DHCPOFFER
- e) DHCPDISCOVER

Questões

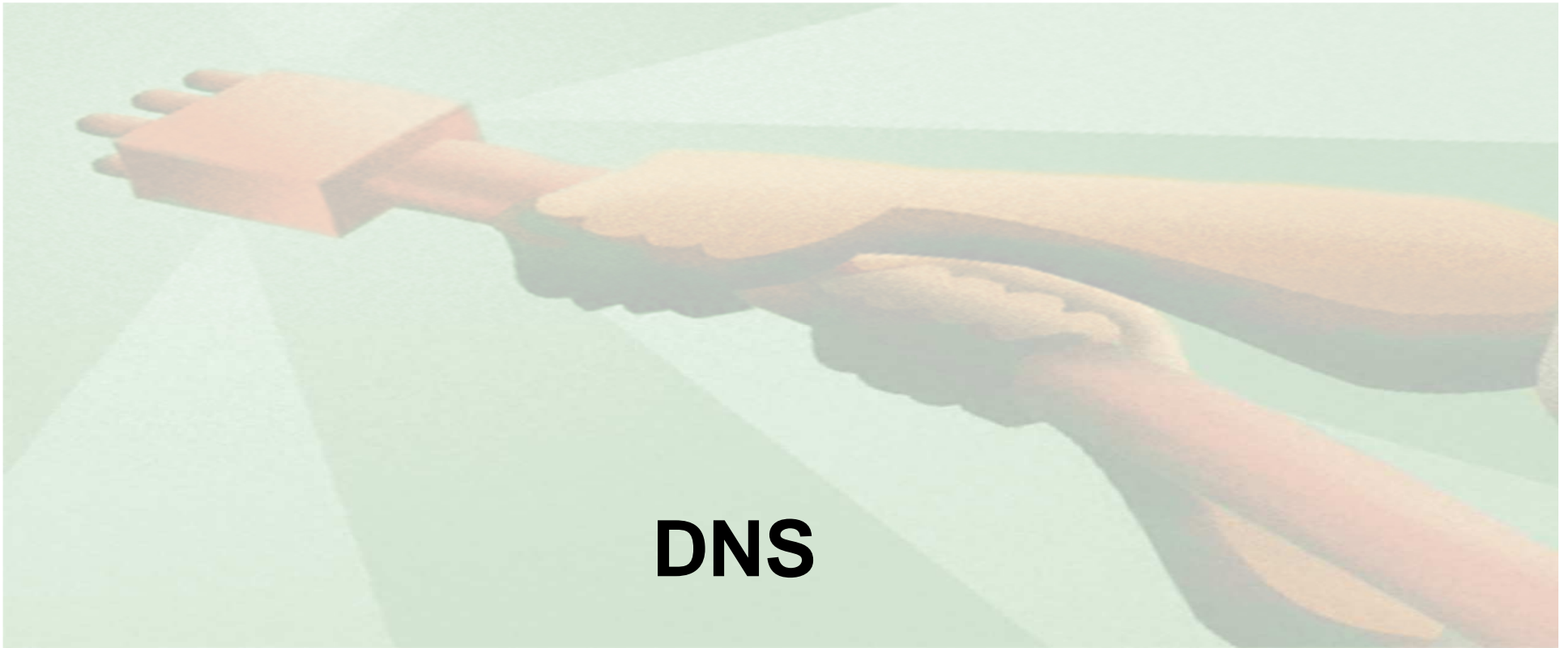
(FGV/MEC 2009) Um cliente DHCP é um equipamento que está configurado para solicitar a um servidor DHCP um endereço IP. Nesse processo, um cliente DHCP pode passar por seis estados de aquisição. O que define em que estado se encontra o cliente é a mensagem que ele envia para um dos servidores DHCP da sua rede. No estado *inicializa*, quando um cliente inicializa pela primeira vez, ele difunde uma mensagem para todos os servidores DHCP da rede local a fim de adquirir as configurações de inicialização na rede. Para tanto ele manda um determinado tipo de mensagem, enviado em um datagrama UDP da mesma forma que no BOOTP. Após o envio dessa mensagem, o cliente passa para o estado *seleciona*. A mensagem é:

- (A) DHCPACK (B) DHCPSEND
- (C) DHCPQUERY (D) DHCPREQUEST
- (E) DHCPDISCOVER

Questões

(FGV/MEC 2009) Um cliente DHCP é um equipamento que está configurado para solicitar a um servidor DHCP um endereço IP. Nesse processo, um cliente DHCP pode passar por seis estados de aquisição. O que define em que estado se encontra o cliente é a mensagem que ele envia para um dos servidores DHCP da sua rede. No estado *inicializa*, quando um cliente inicializa pela primeira vez, ele difunde uma mensagem para todos os servidores DHCP da rede local a fim de adquirir as configurações de inicialização na rede. Para tanto ele manda um determinado tipo de mensagem, enviado em um datagrama UDP da mesma forma que no BOOTP. Após o envio dessa mensagem, o cliente passa para o estado *seleciona*. A mensagem é:

- (A) DHCPACK (B) DHCPSEND
- (C) DHCPQUERY (D) DHCPREQUEST
- (E) DHCPDISCOVER



DNS

Domain Name System

Serviços: DNS

- Mapeamento de endereços IP em nomes
- Banco de dados distribuídos, contendo informações sobre um conjunto de nomes
- Como mapear nomes em IP?
 - plano (tabela) ou hierárquico
- DNS usa a abordagem hierárquica
 - `www.cursos.telemidia.puc-rio.br`
 - `ftp.nasa.gov`
 - `serv1.acme.com.br`
- Mapeamento Plano: tabelas de *hosts* (`/etc/hosts` ou `C:\WINDOWS\HOSTS`).

Serviços: DNS - Definições

- Domínio é um nome de fácil memorização e que serve para localizar e identificar computadores na Internet
 - Domínios possuem servidores autoritários para responder pelas máquinas e sub-domínios
- Zonas são regiões hierárquicas de um domínio gerenciadas de forma distinta (em servidores distintos)
- Árvore Invertida

Serviços: DNS

- Mecanismo descentralizado* (não a gerência)
- A responsabilidade pelas partes do espaço de nomes é delegada
 - Por exemplo, os hosts que são autoritativos para a zona “br” nada sabem sobre a zona “com.br”, exceto quem são os servidores DNS para essa zona, ou seja, quais servidores DNS receberam a delegação de autoridade para a zona.

Serviços: DNS

- Protocolo híbrido (Porta 53)
 - Utiliza a camada de transporte UDP para recebimento de pedidos de consultas de resolução de hosts/ip (vice-versa) ATÉ um tamanho de 512 bytes
 - Se o tamanho da mensagem for maior que 512 bytes o protocolo TCP é utilizado mesmo para consultas ao servidor.
 - E, por fim, utiliza TCP para troca de informações de zonas com os servidores DNS vizinhos.

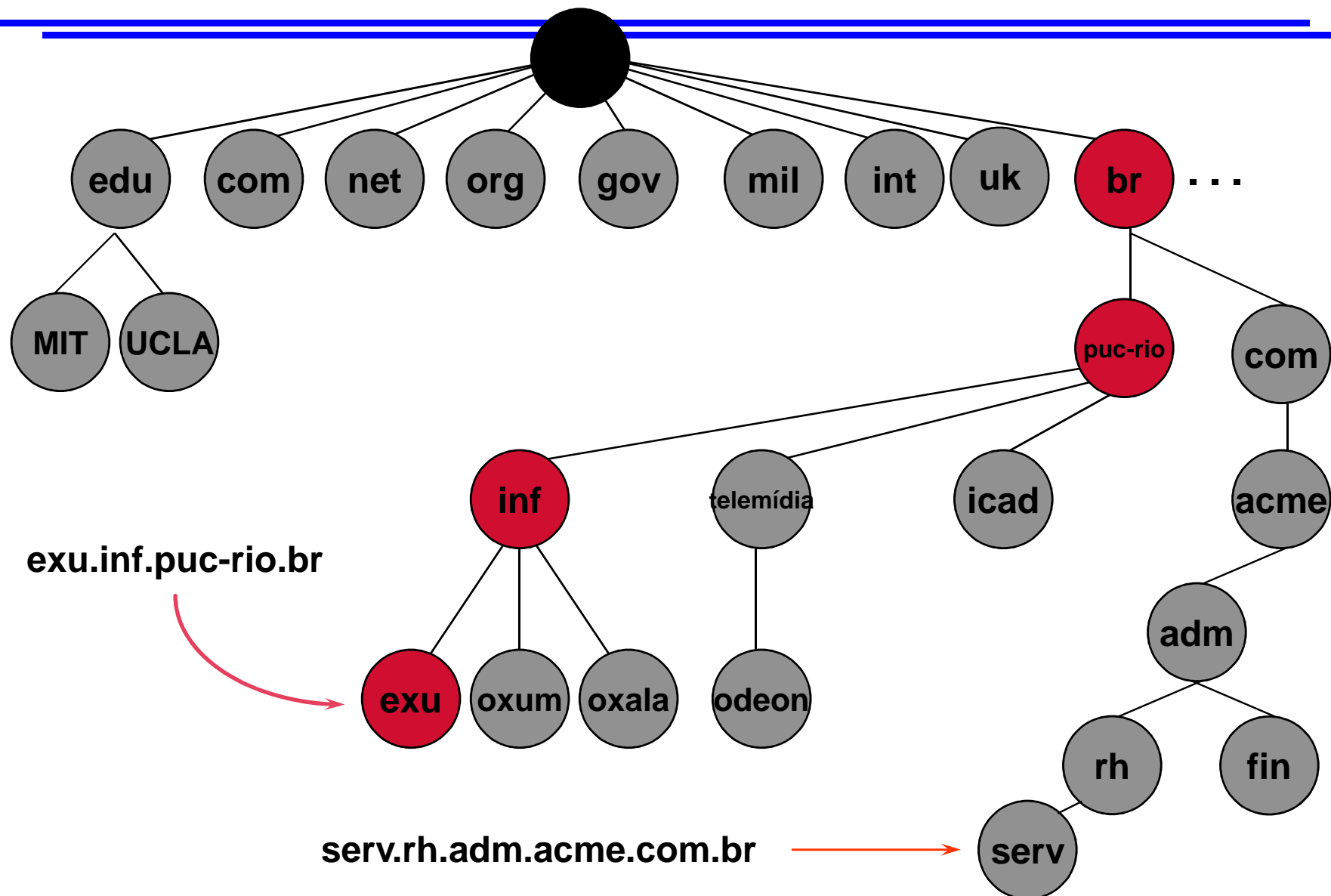
Serviços: DNS

- DNS é todo o sistema e também é um protocolo.
 - Especifica os protocolos para o mapeamento de nomes em endereços IP
 - Especifica as regras de sintaxe para os nomes de domínio e a delegação
- Nomes são completamente independentes da organização da rede física e endereços IP
 - Um domínio com mais de uma rede
 - Uma rede com máquinas em domínios diferentes
 - Uma máquina em dois domínios diferentes

Serviços: DNS

- O nome completo de um host – FQDN = Full Qualified Domain Name – é composto de duas partes:
 - * A primeira parte identifica o host dentro do domínio e
 - * A segunda parte identifica o domínio.
 - Em `www.provasdeti.com.br`, `www` é o nome do host, e `provasdeti.com.br` é o domínio.
 - Domínio principal: " " (branco)
 - Domínios secundários: `com`, `gov`, `net`, `br`, `fr`,
 - Domínios terciários: `nasa.gov`, `puc-rio.br`, `com.br`, `net.br`, `co.uk`, `co.jp`, ...

Serviços: DNS



Serviços: DNS

- br , com , edu , gov , uk , são Top Level Domain Names

TLD), cujo registro é feito pelo Internic.

- Generic Top Level Domain Names
 - .com, .net, .org
- “Novos” GTLDs:
 - .firm, .store, .web, .arts, .rec, .infor, .nom

Serviços: DNS

- A organização responsável por atribuir nomes de domínio e endereços IP em nível global é a ICANN (*Internet Corporation for Assigned Names and Numbers*)
- No Brasil, o registro de domínios fica a cargo do Registro.br

O Registro.br é o departamento do NIC.br responsável pelas atividades de registro e manutenção dos nomes de domínios que usam o .br. Também executamos o serviço de distribuição de endereços IPv4 e IPv6 e de números de Sistemas Autônomos (ASN) no país.

Serviços: DNS

- Domínios DPN (Domínios de Primeiro Nível) .br:
 - .com.br, .edu.br, .g12.br, .gov.br, .mil.br, .net.br., org.br, .br
- As categorias podem ser divididas em 3 tipos.
 - Os domínios de pessoa física e profissionais liberais só podem ser registrados por um titular com CPF.
 - Os domínios de pessoa jurídica devem ser associados a um CNPJ.
 - Já os domínios genéricos podem ser registrados por CPF ou CNPJ.

Questões

(FCC/Metro-SP 2010) Responsável pela “tradução” do endereço IP do site pelo domínio (nome) do mesmo. O acrônimo DNS significa:

- (A) Data Name Service.
- (B) Domain Name Service.
- (C) Domain Name Sector.
- (D) Data Name Sector.
- (E) Domain Navigator Service.

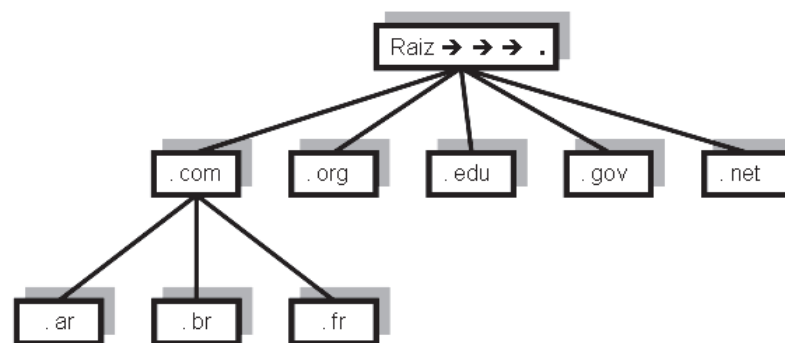
Questões

(FCC/Metro-SP 2010) Responsável pela “tradução” do endereço IP do site pelo domínio (nome) do mesmo. O acrônimo DNS significa:

- (A) Data Name Service.
- (B) Domain Name Service. (System!)**
- (C) Domain Name Sector.
- (D) Data Name Sector.
- (E) Domain Navigator Service.

Questões

(FGV/MEC-2009) A figura a seguir refere-se a um recurso usado em redes TCP/IP que permite acessar computadores sem que o usuário ou sem que o próprio computador tenha conhecimento de seu endereço IP. Esse recurso permite o uso de nomes ou domínios, como *www.mec.gov.br* para acessar o site do MEC em vez do correspondente IP. Na Internet, ele é representado por um conjunto de grandes bancos de dados distribuídos em servidores de todo o mundo que indicam qual IP é associado a um nome. (cont...)



Questões

(cont...) Na comunicação no âmbito da pilha de protocolos TCP/IP, esse recurso se comunica com o TCP da camada de transporte por meio de uma porta conhecida. Esse recurso e a porta são, respectivamente:

- (A) DNS e 53
- (B) NFS e 53
- (C) DNS e 80
- (D) NFS e 67
- (E) DNS e 67

Questões

(cont...) Na comunicação no âmbito da pilha de protocolos TCP/IP, esse recurso se comunica com o TCP da camada de transporte por meio de uma porta conhecida. Esse recurso e a porta são, respectivamente:

- (A) DNS e 53
- (B) NFS e 53
- (C) DNS e 80
- (D) NFS e 67
- (E) DNS e 67

Questões

(FCC/TRE-PI 2010) O DNS é um protocolo da camada de I e suas requisições são feitas usando a porta 53 do protocolo _ II na camada de III .

As lacunas I, II e III devem ser preenchidas, respectivamente, por

- (A) transporte, UDP e rede.
- (B) transporte, TCP e rede.
- (C) aplicação, UDP e enlace.
- (D) aplicação, UDP e transporte.
- (E) aplicação, TCP e transporte.

Questões

(FCC/TRE-PI 2010) O DNS é um protocolo da camada de I e suas requisições são feitas usando a porta 53 do protocolo _ II na camada de III .

As lacunas I, II e III devem ser preenchidas, respectivamente, por

- (A) transporte, UDP e rede.
- (B) transporte, TCP e rede.
- (C) aplicação, UDP e enlace.
- (D) aplicação, UDP e transporte.**
- (E) aplicação, TCP e transporte.

Questões

(FCC/MPE-RN 2010) Uma pequena rede TCP/IP que não tenha um servidor DNS

- (A) exigirá que cada estação tenha um arquivo de hosts para a localização do servidor Web.
- (B) funcionará normalmente porque uma rede pequena não exige qualquer outra alternativa.
- (C) funcionará normalmente, caso tenha na rede um servidor DHCP instalado.
- (D) exigirá obrigatoriamente a instalação do servidor.
- (E) funcionará apesar do servidor Web não ser localizado.

Questões

(FCC/MPE-RN 2010) Uma pequena rede TCP/IP que não tenha um servidor DNS

- (A) exigirá que cada estação tenha um arquivo de hosts para a localização do servidor Web.
- (B) funcionará normalmente porque uma rede pequena não exige qualquer outra alternativa.
- (C) funcionará normalmente, caso tenha na rede um servidor DHCP instalado.
- (D) exigirá obrigatoriamente a instalação do servidor.
- (E) funcionará apesar do servidor Web não ser localizado.

Questões

(CESPE/ Correios 2011) Os serviços DNS são imprescindíveis para a comunicação em redes TCP/IP, já que, sem eles, a camada de rede se torna totalmente inoperante, fazendo que, em nenhuma situação, ocorra comunicação IP.

(CESPE/MPU 20100 A hierarquia de atribuição de nomes de domínios na Internet é dependente da topologia física das redes que constituem a Web.

(ESAF/SEFAZ-CE ADAP) As entidades registradoras, ou seja, entidades comerciais que verificam nomes de domínios, registram esses nomes nos bancos de dados DNS, são credenciadas pela ICANN (Internet Corporation for Assigned Names and Numbers).

Questões

- E (CESPE/ Correios 2011) Os serviços DNS são **imprescindíveis** para a comunicação em redes TCP/IP, já que, sem eles, **a camada de rede se torna totalmente inoperante**, fazendo que, em nenhuma situação, ocorra comunicação IP.
- E (CESPE/MPU 20100 A hierarquia de atribuição de nomes de domínios na Internet é **dependente** da topologia física das redes que constituem a Web.
- C (ESAF/SEFAZ-CE ADAP) As entidades registradoras, ou seja, entidades comerciais que verificam nomes de domínios, registram esses nomes nos bancos de dados DNS, são credenciadas pela ICANN (Internet Corporation for Assigned Names and Numbers).

Serviços: DNS - Tipos

- Existem 3 tipos de servidores básicos de DNS
 - **Primário:** mantém as tabelas de configuração de DNS localmente
 - **Secundário:** recebe atualização do primário com informação sobre a zona
 - **Caching-only:** Somente realiza cache dos domínios consultados, sem nenhuma informação local

Serviços: DNS - Tipos

- Servidor fornece dois tipos de resposta:
 - **autoritativa**: quando é o servidor primário ou secundário para o domínio
 - **não-autoritativa**: quando sabe a resposta por meio de uma informação residente em cache
- Por exemplo, os hosts que são autoritativos para a zona “**br**” nada sabem sobre a zona “**com.br**”, exceto quem são os servidores DNS para essa zona, ou seja, quais servidores DNS receberam a delegação de autoridade para a zona.

Serviços: DNS - Tipos

- Sub-tipos de servidores:
 - **forwarders** - se não possui a informação no cache, consulta outro servidor de nomes, esperando um tempo máximo pela resposta.
 - **slave** - depende completamente de outros servidores, nunca tentando realizar uma consulta

Serviços: DNS - Tipos

- Entre 2 DNS, podem haver zonas sincronizadas, um DNS sendo o **Master** que contém a zona original, e os outros seus slaves, que contém cópias da zona original.
- Para manterem-se sincronizados automaticamente, eles usam essa "consulta" especial, o AXFR (transferência "full" ou integral da zona) ou IXFR (transferência incremental, ou apenas alterações, da zona).
- Ambos acontecem via TCP ao invés de UDP como é o normal de DNS.

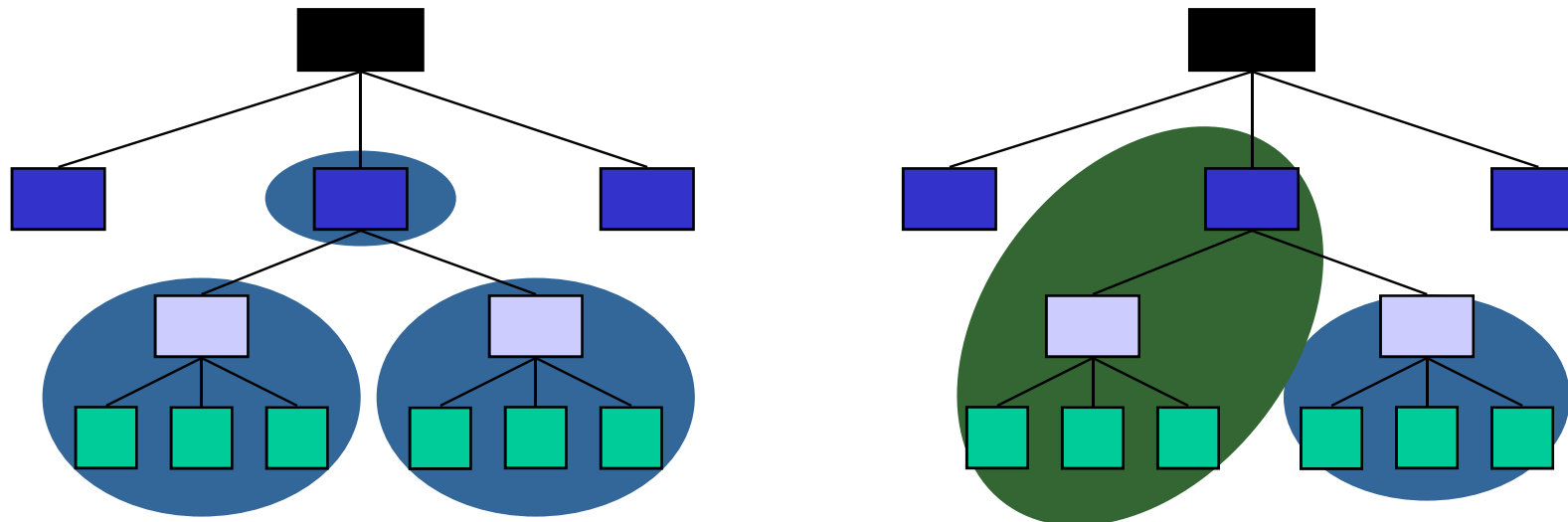
Serviços: DNS - Tipos

- **bind** é a implementação (Linux) padrão do servidor de DNS
- **resolver** é um conjunto de funções no cliente que executam os pedidos de consulta para um servidor DNS

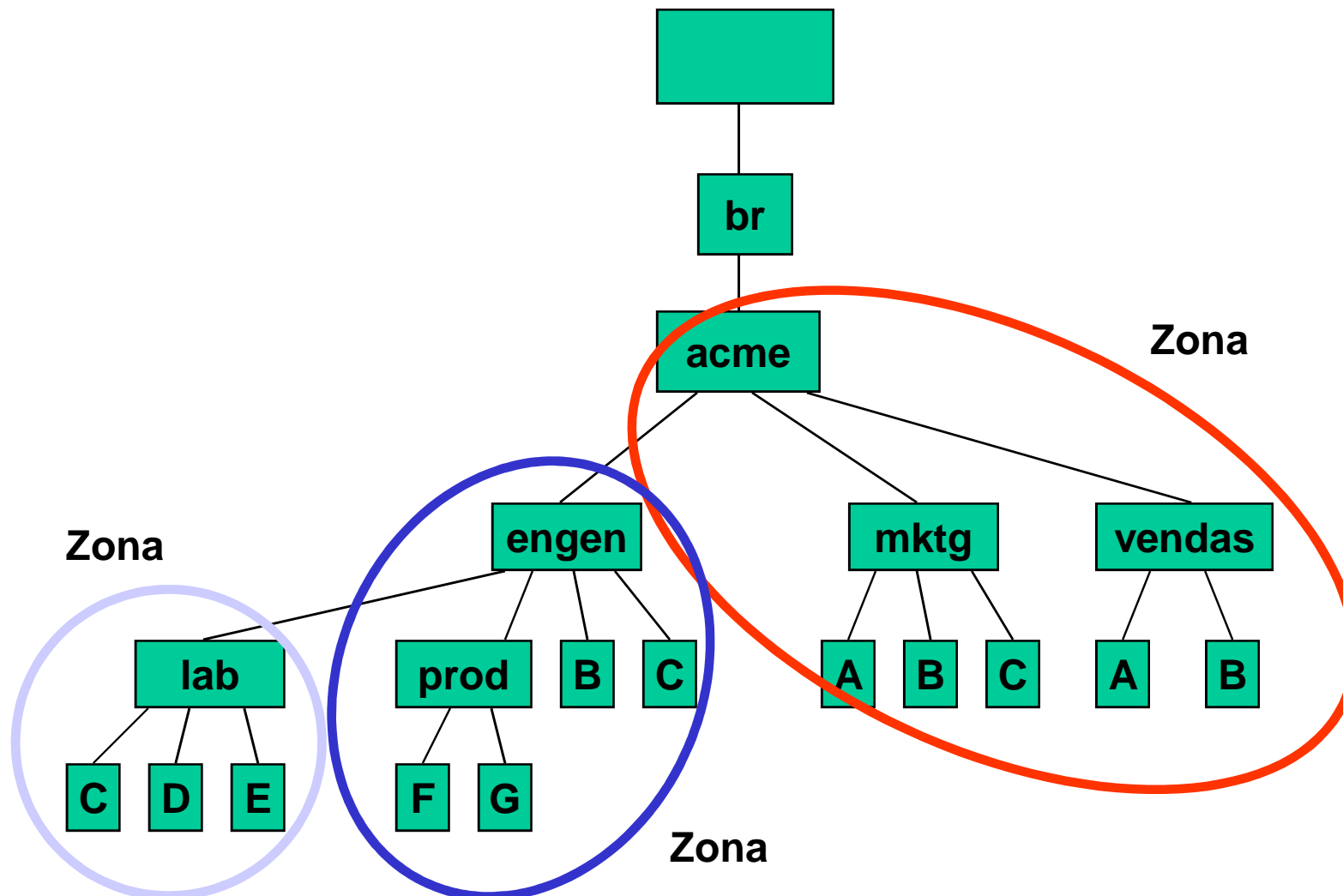
```
/etc/resolv.conf:  
domain enge.acme.com.br  
search lab.enge.acme.com.br fabrica.acme.com.br  
nameserver 200.18.2.1  
nameserver 200.18.100.1
```

Serviços: DNS - Consultas

- Domínios possuem servidores autoritários para responder pelas máquinas e sub-domínios
- Zonas são regiões hierárquicas de um domínio gerenciadas de forma distinta (em servidores distintos)

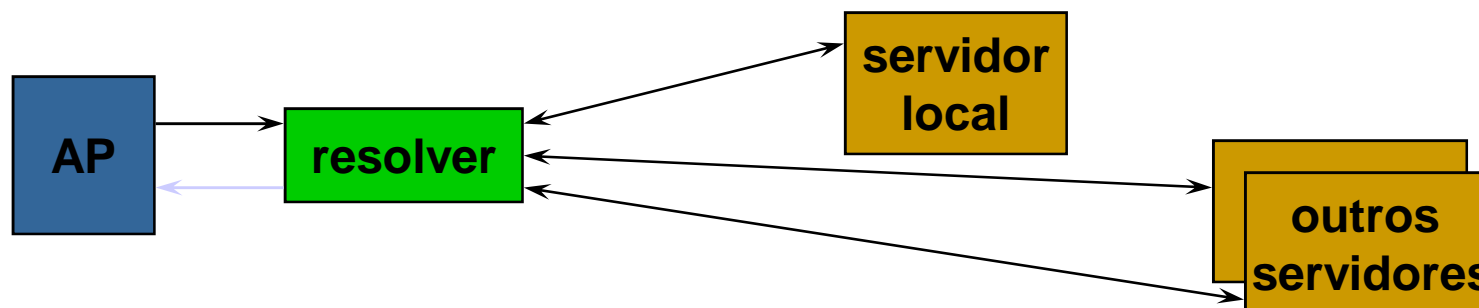
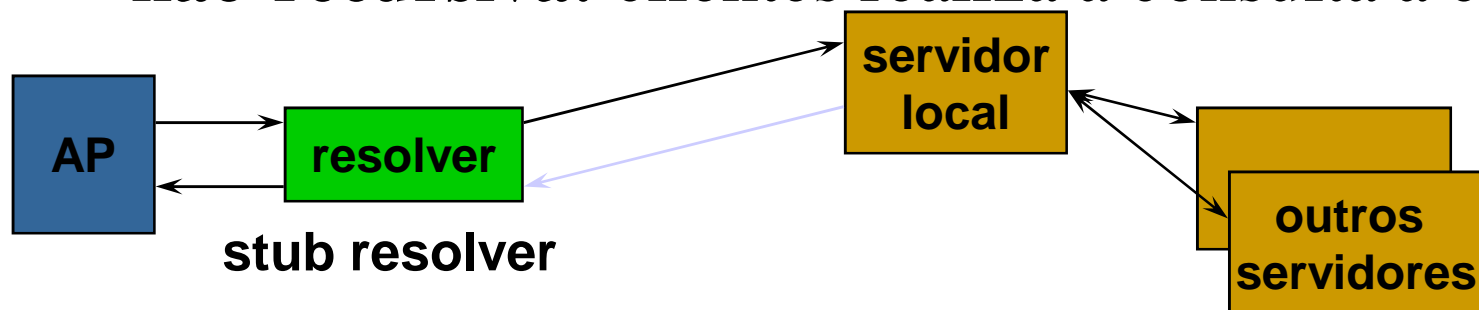


Serviços: DNS - Consultas



Serviços: DNS - Consultas

- Duas opções para consulta:
 - **recursiva:** servidor de nomes se encarrega da consulta
 - **não-recursiva:** clientes realiza a consulta a cada NS



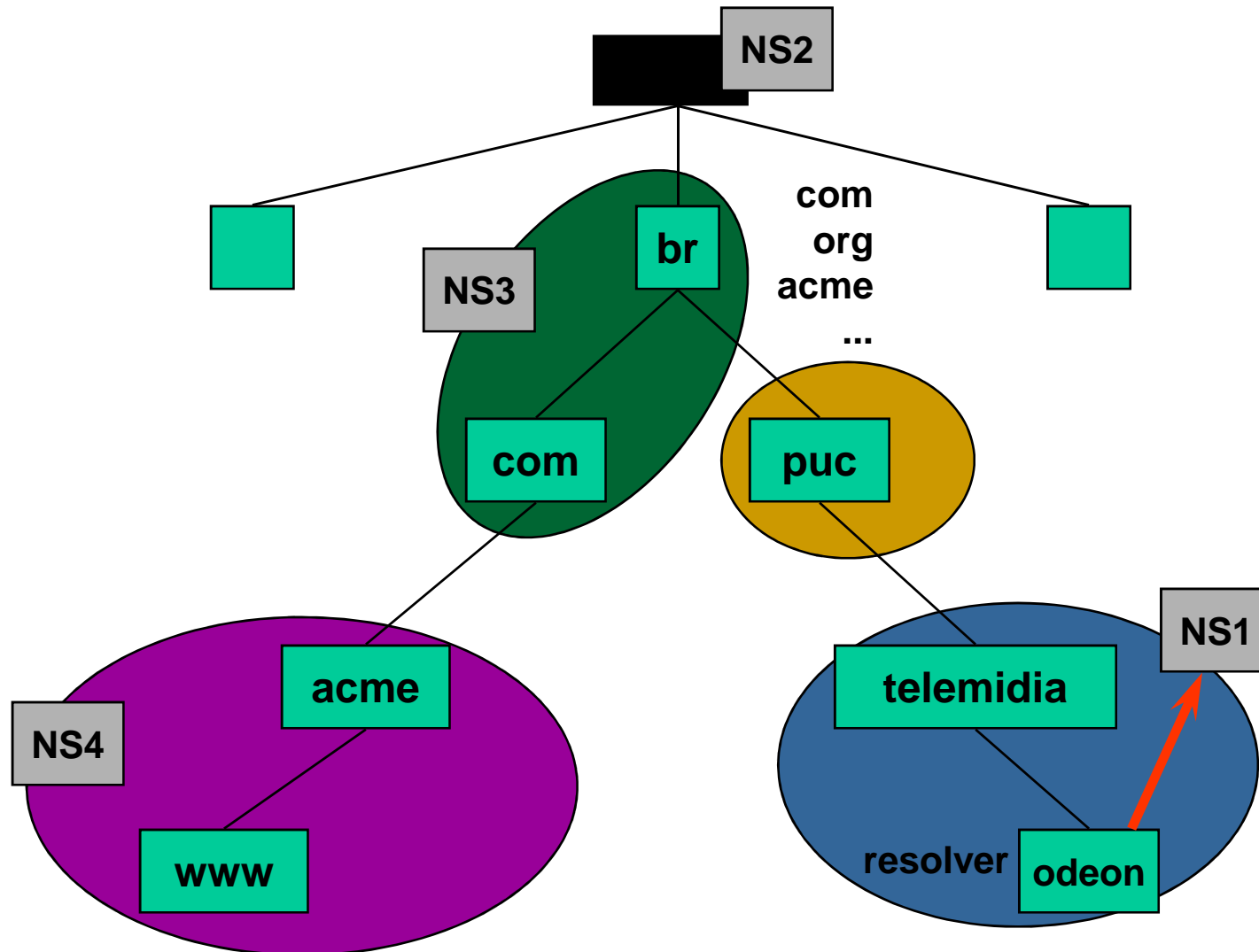
Serviços: DNS - Consultas

- Servidores e resolvers possuem cache para armazenar as respostas efetuadas
- Cache pode ser também de domínios inteiros
- Resolvers podem armazenar também todo o conteúdo do servidor local em cache

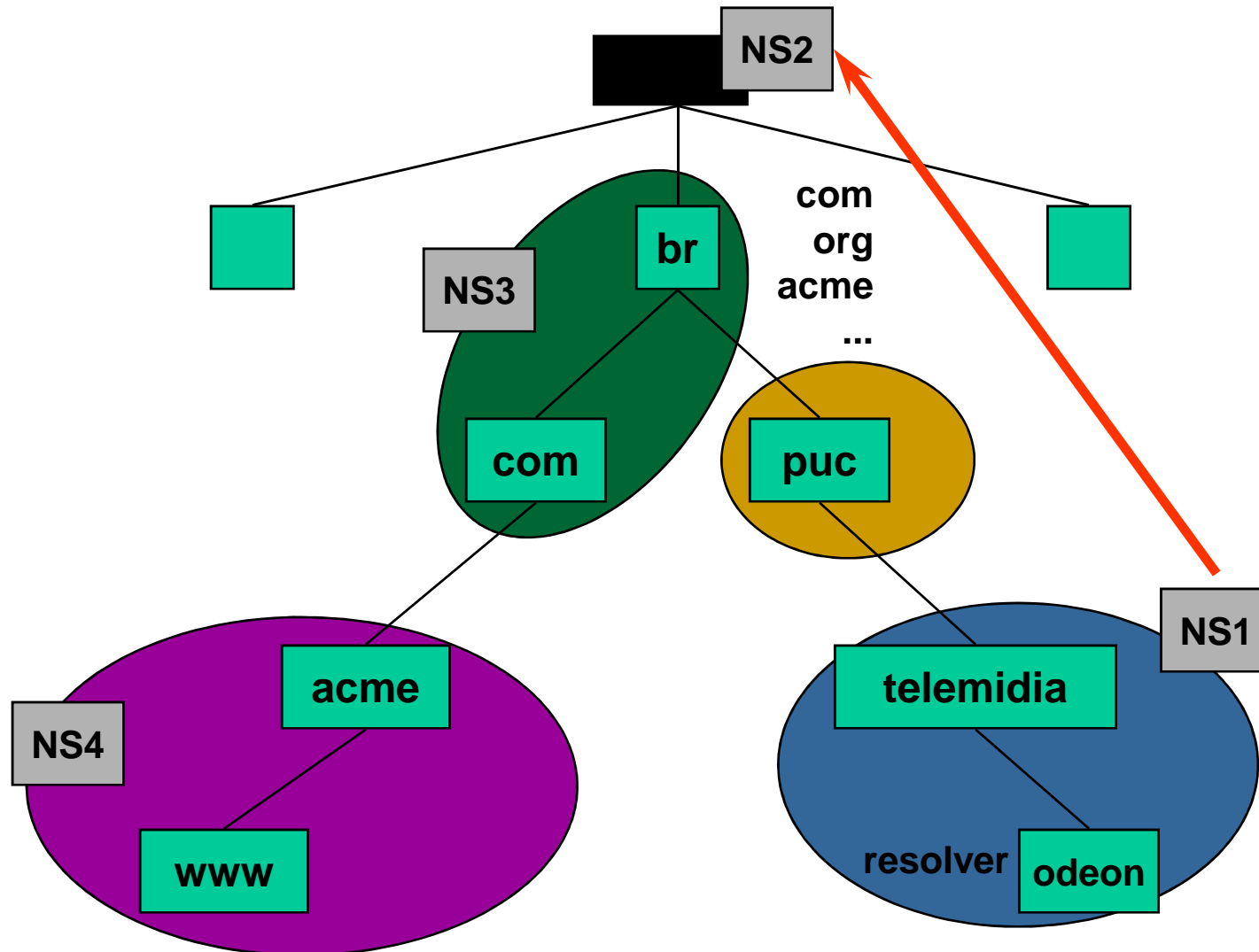
Serviços: DNS - Consultas

- Cliente (resolver) consulta servidor de DNS
- Ex. resolução de `www.acme.com.br` da máquina `odeon.telemidia.puc-rio.br`
- Consulta um servidor de nomes próximo (geralmente o do domínio `telemidia.puc-rio.br`)
- Servidor não possui informação e consulta o servidor do domínio (ou o NS pode já saber o servidor de `.br`)
- Servidor `.br` informa ao servidor inicial o servidor do domínio `.com.br`, ou se for o servidor autoritário para `.com.br`, já informa o endereço do servidor de `acme.com.br`
- Servidor consulta servidor de `acme.com.br` e retorna ao cliente o end. IP de `www.acme.com.br` (guarda no cache)

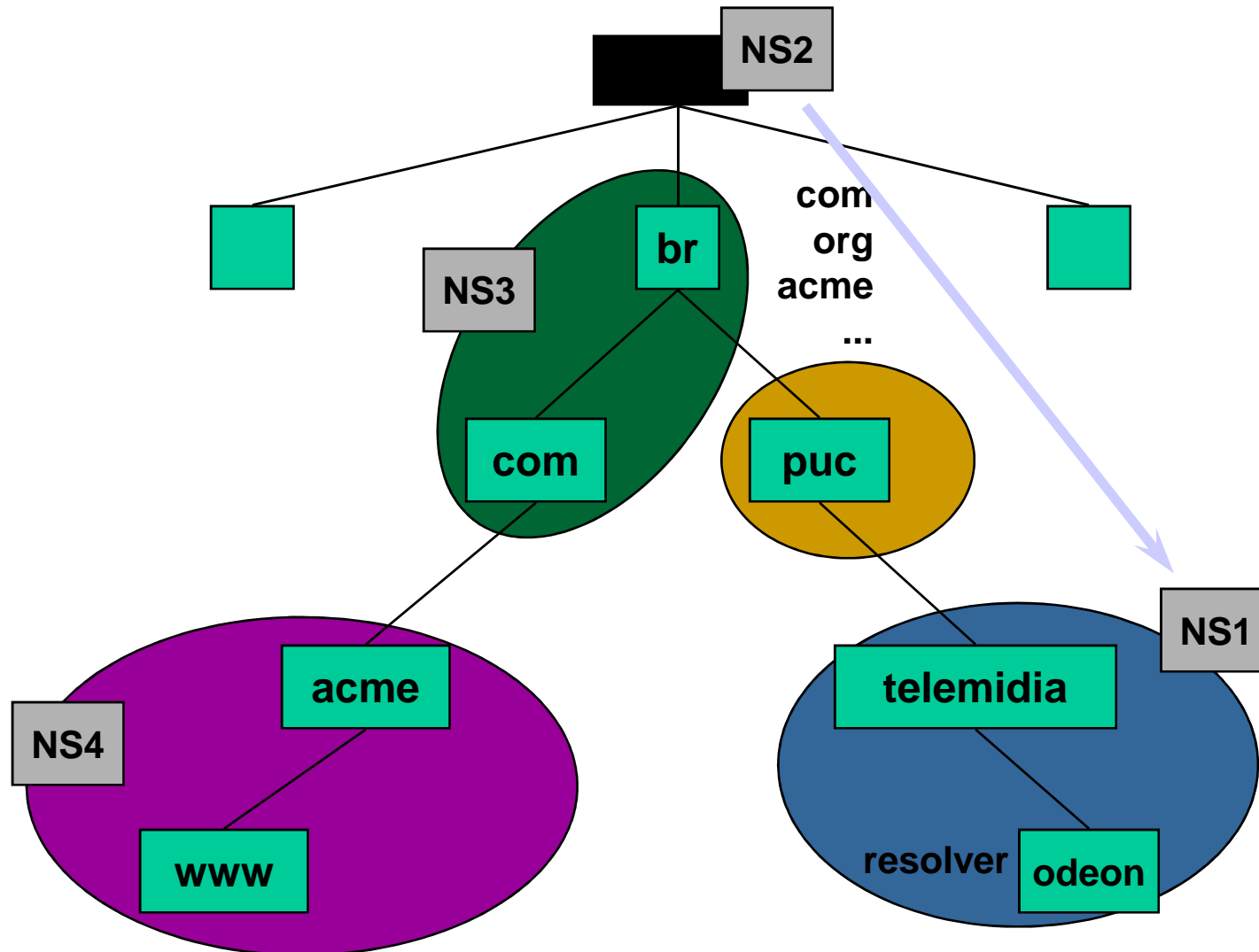
Serviços: DNS - Consultas



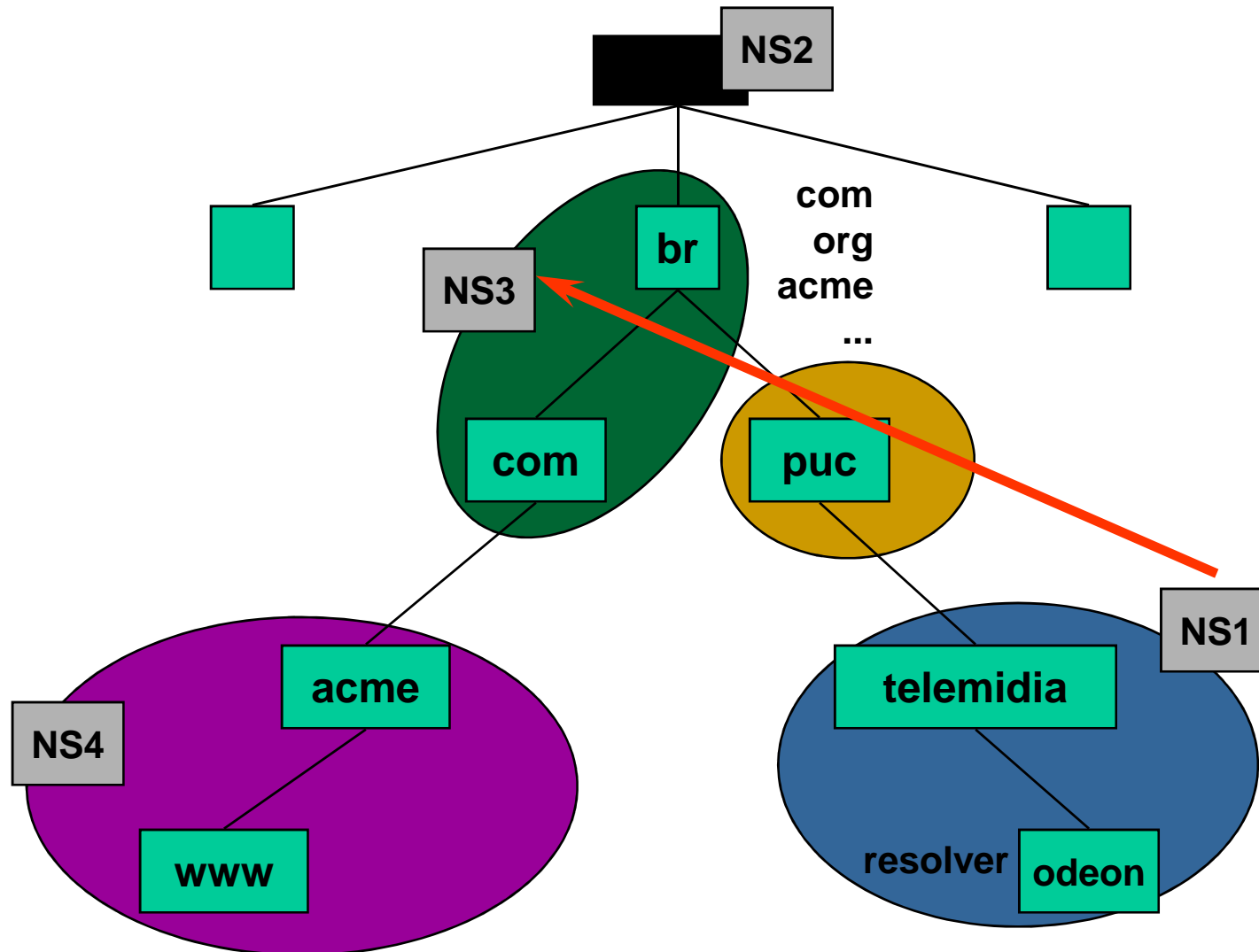
Serviços: DNS - Consultas



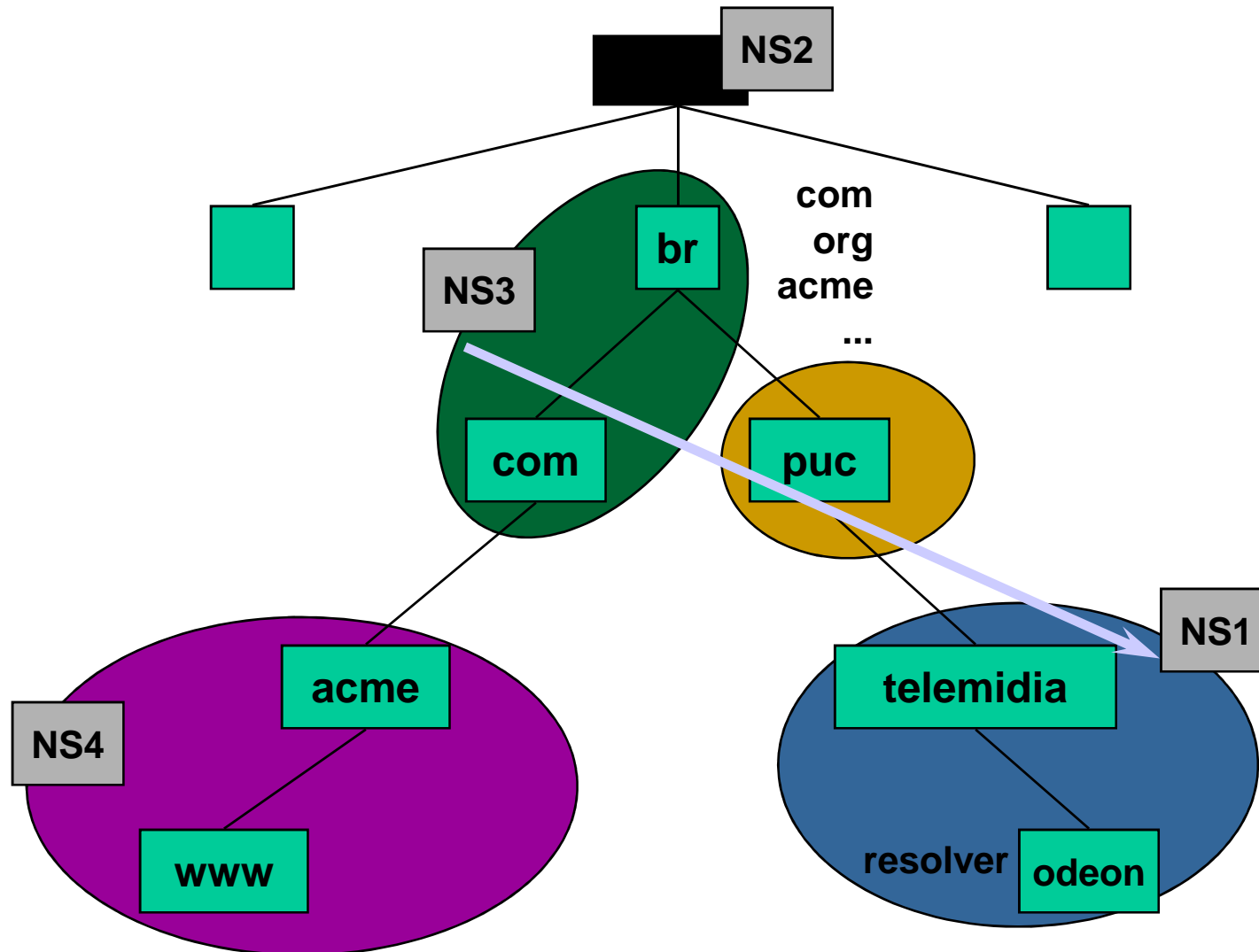
Serviços: DNS - Consultas



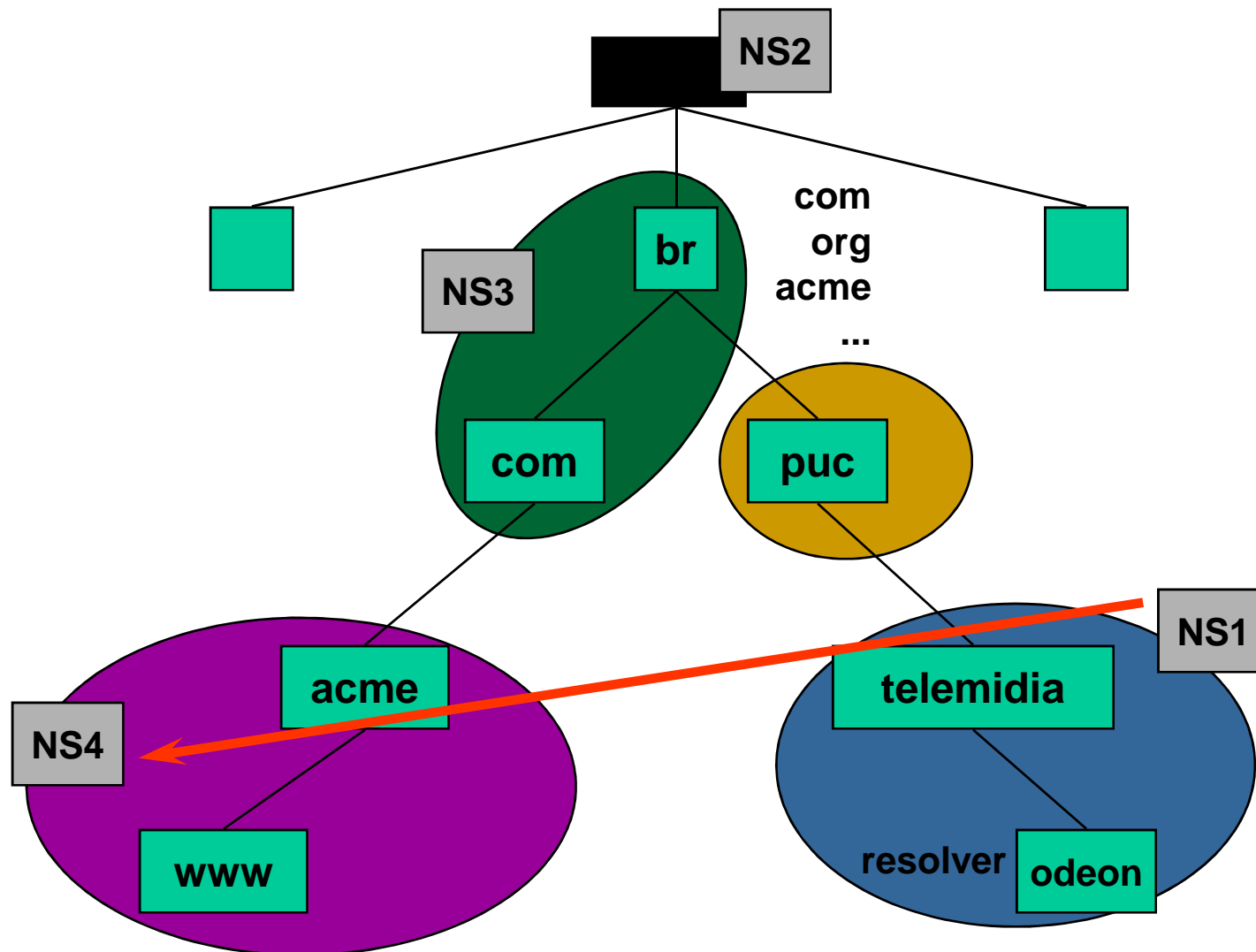
Serviços: DNS - Consultas



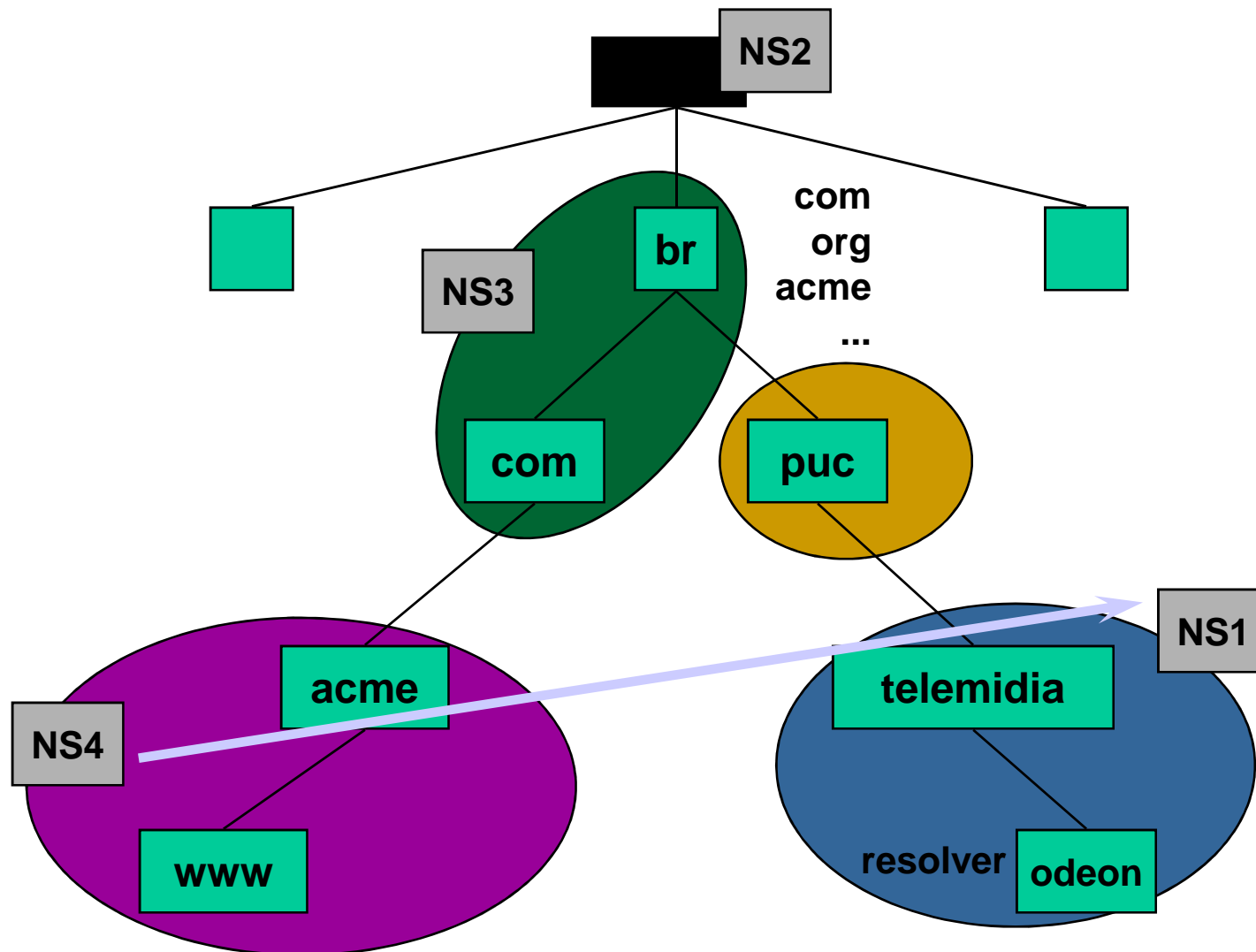
Serviços: DNS - Consultas



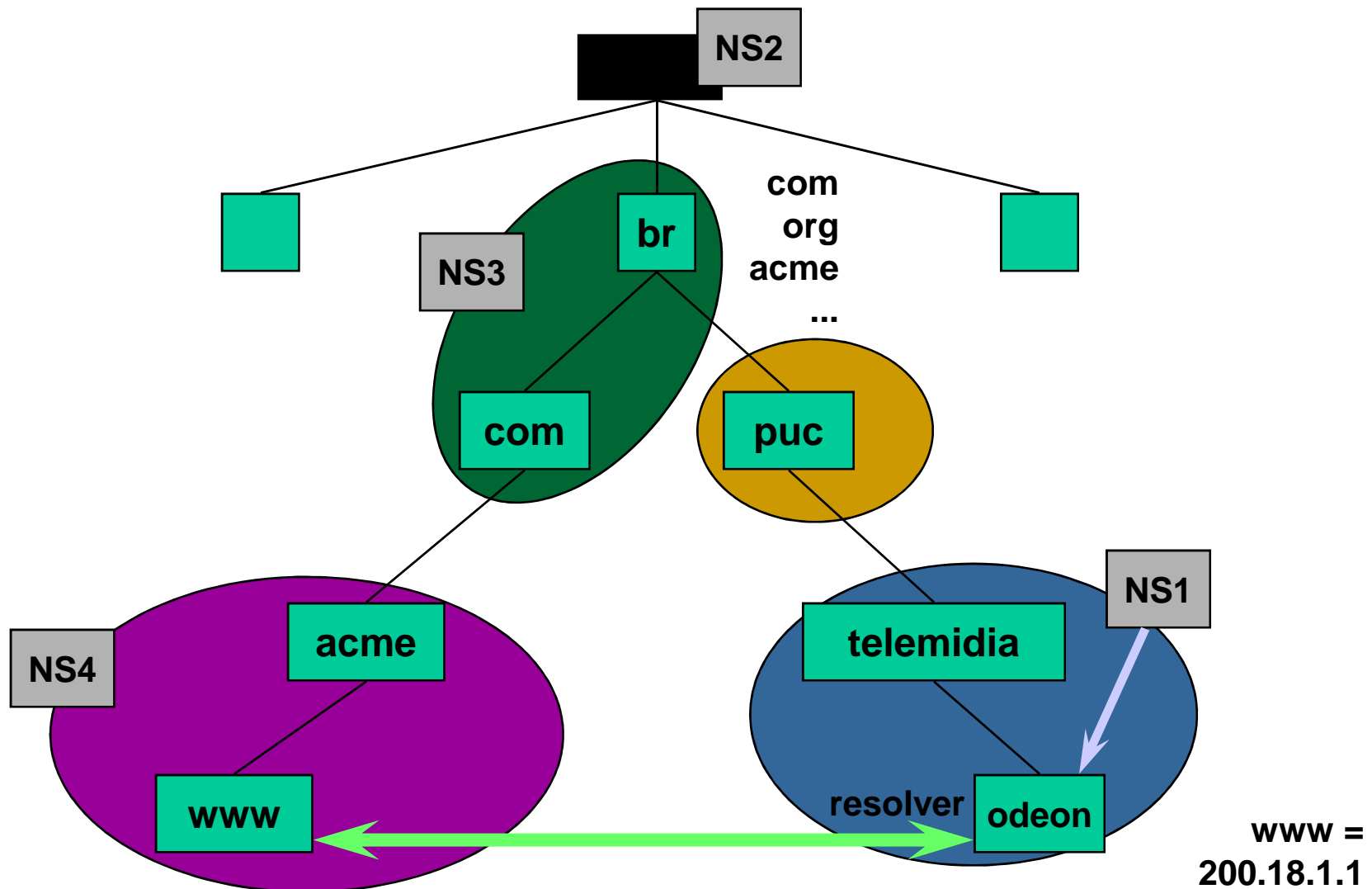
Serviços: DNS - Consultas



Serviços: DNS - Consultas



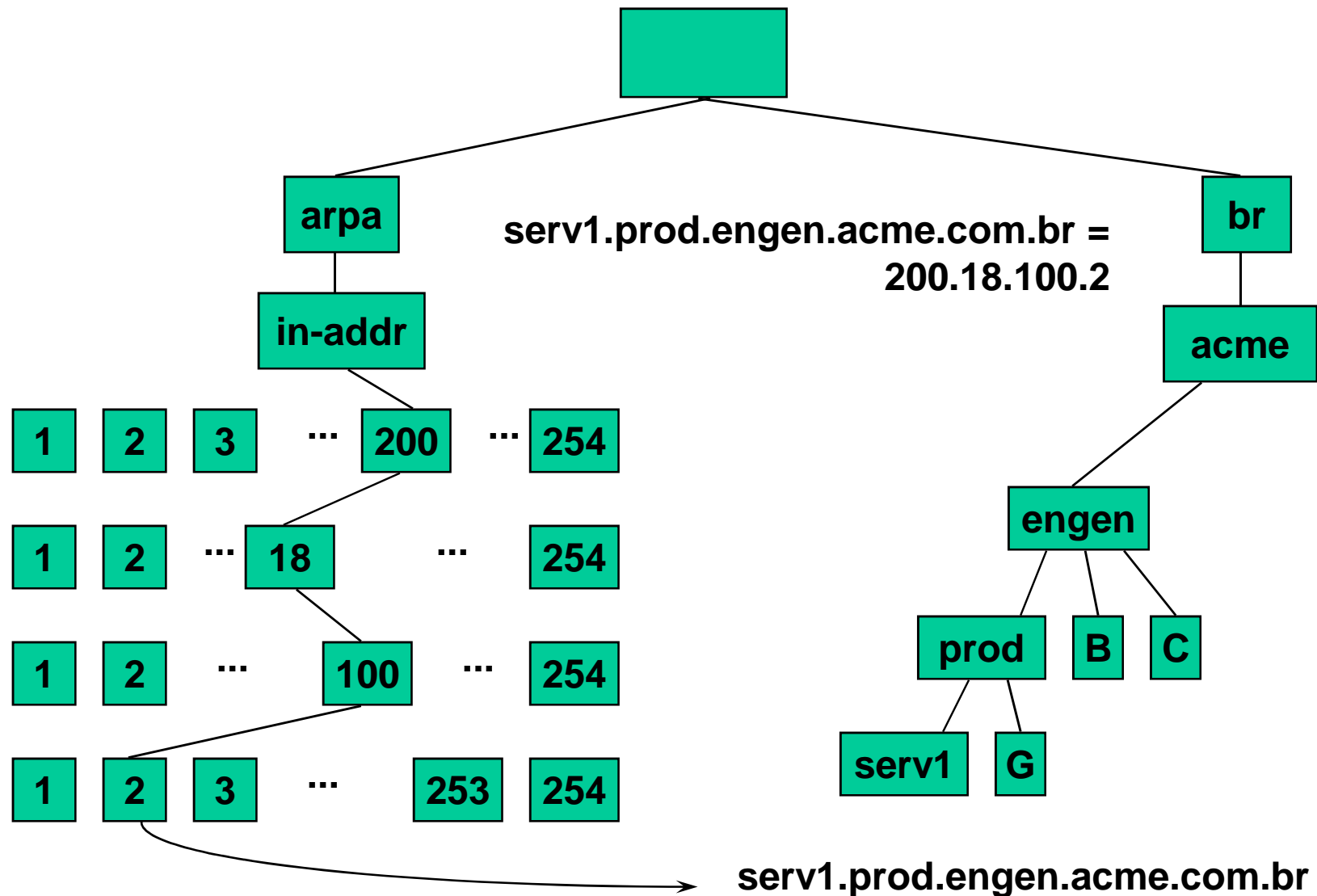
Serviços: DNS - Consultas



Serviços: DNS Reverso

- DNS possui também uma organização paralela para mapear endereços IP em nomes
- Utiliza como domínio raiz o `in-addr.arpa`
- O endereço 200.18.1.2 é resolvido pelo domínio `2.1.18.200.in-addr.arpa`

Serviços: DNS Reverso



Serviços: DNS – Dinâmico (DDNS)



Serviços: DNS – Dinâmico (DDNS)

- Por meio do DNS Dinâmico (Dynamic DNS), você pode registrar um endereço de acesso como "meu-nome.no-ip.org" ou "fulano.dyndns.com", que passa a apontar para seu endereço IP corrente.
- Normalmente, para registrar um domínio é necessário ter um servidor com dois IPs fixos (ou dois servidores, com um IP cada), de forma a configurar os dois servidores DNS necessários.
- Os servidores do registro.br ou da entidade responsável pelo seu domínio passam então a redirecionar as requisições para o seu servidor DNS primário, que responde com o endereço IP do servidor.

Serviços: DNS – Privado

- Endereços reservados não devem estar associados a nomes em servidores DNS públicos. Se você utilizá-los em redes privadas e quiser usar nomes para as máquinas, configure um servidor DNS privado ou utilize tabelas de *hosts* (/etc/hosts ou C:\WINDOWS\HOSTS).

Questões

(FCC/TRT-RJ 2011) O cliente DNS faz solicitação a um servidor DNS utilizando nome completo do host, como, por exemplo, www.algo.com.br.

O servidor DNS responde ao cliente o endereço IP do host ou um código de erro, caso o endereço não seja resolvido. Trata-se da resolução de nome DNS do tipo

- (A) intercâmbio.
- (B) interativa.
- (C) reversa.
- (D) recursiva.
- (E) de domínio.

Questões

(FCC/TRT-RJ 2011) O cliente DNS faz solicitação a um servidor DNS utilizando nome completo do host, como, por exemplo, www.algo.com.br.

O servidor DNS responde ao cliente o endereço IP do host ou um código de erro, caso o endereço não seja resolvido. Trata-se da resolução de nome DNS do tipo

- (A) intercâmbio.
- (B) interativa.
- (C) reversa.
- (D) recursiva.**
- (E) de domínio.

Questões

(Consulplan/TCE-RR 2006) uma das características mais comuns no serviço de DNS é o uso de cachês.

(CESPE/Petrobras 2007) Para traduzir um nome de máquina em um endereço IP, independentemente do modo como a consulta seja feita aos servidores Domain Name System (DNS), uma aplicação que seja cliente desse serviço de tradução tem que percorrer a hierarquia de nomes enviando consultas para vários servidores ao longo da hierarquia.

Questões

C (Consulplan/TCE-RR 2006) uma das características mais comuns no serviço de DNS é o uso de cachês.

E (CESPE/Petrobras 2007) Para traduzir um nome de máquina em um endereço IP, **independentemente do modo como a consulta seja feita aos servidores Domain Name System (DNS)**, uma aplicação que seja cliente desse serviço de tradução tem que percorrer a hierarquia de nomes enviando consultas para vários servidores ao longo da hierarquia.

Questões

(CESPE/TJ-DF 2008) No contexto do DNS (domain name system), um servidor de nomes com autoridade deve ser usado por qualquer organização que tenha hospedeiros que possam ser acessados publicamente na Internet, de modo a fornecer registros DNS acessíveis publicamente que mapeiem os nomes desses hospedeiros para endereços IP.

(CESPE/Pref. Vitória 2007) Ao se configurar o TCP/IP, pode-se listar os endereços de vários servidores domain name system (DNS). Nesse caso, para traduzir um nome em endereço, o primeiro servidor na lista será consultado. Se a resposta desse servidor for referente a impossibilidade de se realizar a tradução, o servidor seguinte na lista será consultado.

Questões

- A (CESPE/TJ-DF 2008) No contexto do DNS (domain name system), um servidor de nomes com autoridade deve ser usado por qualquer organização que tenha hospedeiros que possam ser acessados publicamente na Internet, de modo a fornecer registros DNS acessíveis publicamente que mapeiem os nomes desses hospedeiros para endereços IP.
- E (CESPE/Pref. Vitória 2007) Ao se configurar o TCP/IP, pode-se listar os endereços de vários servidores domain name system (DNS). Nesse caso, para traduzir um nome em endereço, o primeiro servidor na lista será consultado. Se a resposta desse servidor for referente a impossibilidade de se realizar a tradução, o servidor seguinte na lista será consultado.

Questões

(CESPE/UNIPAMPA 2013) Ao se acrescentar um servidor novo à Internet em um novo domínio, deve-se registrar o domínio e o endereço IP em um servidor DNS autoritativo primário e em um secundário.

(CESPE/Correios 2011) O serviço DNS (domain name server) é necessário para o funcionamento do serviço de email de uma organização, pois o DNS mantém registros que descrevem o endereço do servidor de email responsável pelo domínio.

Questões

- C (CESPE/UNIPAMPA 2013) Ao se acrescentar um servidor novo à Internet em um novo domínio, deve-se registrar o domínio e o endereço IP em um servidor DNS autoritativo primário e em um secundário.
- A (CESPE/Correios 2011) O serviço DNS (*domain name server*) é necessário para o funcionamento do serviço de *email* de uma organização, pois o DNS mantém registros que descrevem o endereço do servidor de *email* responsável pelo domínio.

Questões

(UFF – Técnico de Lab.) No tocante ao DNS, é um servidor de DNS amplamente utilizado:

- a) BIND;
- b) SSH;
- c) DMZ;
- d) GOPHER;
- e) SAM.

Questões

(UFF – Técnico de Lab.) No tocante ao DNS, é um servidor de DNS amplamente utilizado:

- a) BIND;
- b) SSH;
- c) DMZ;
- d) GOPHER;
- e) SAM.

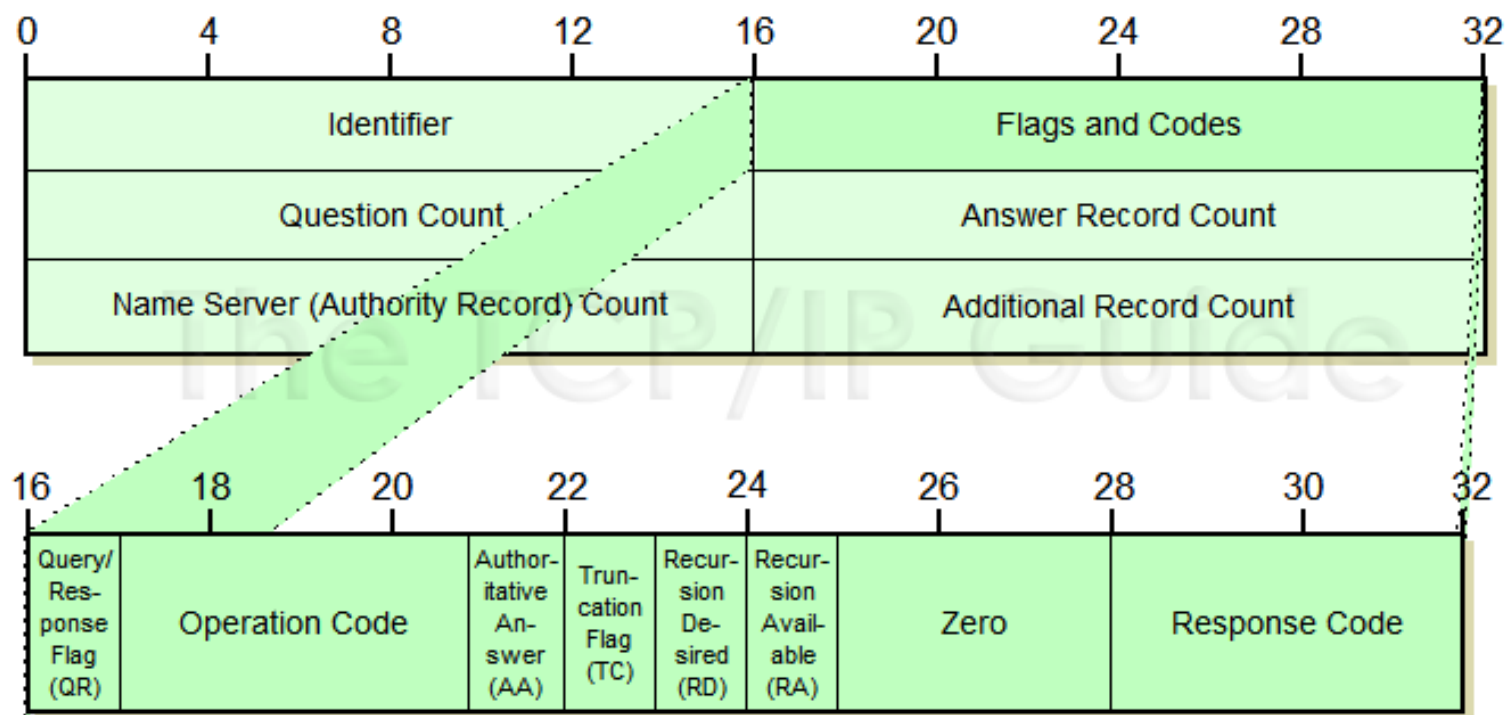
Serviços: DNS – Tipos de Registros

- **A** - O **A**, também conhecido por hostname, é o registro central de um DNS, ele vincula um domínio ou subdomínio a um endereço IP direto.
- **AAAA** - Executa a mesma função de **A**, porém, para um endereço IPv6.
- **NS** - Name Server (Servidor de Domínio), especifica servidores DNS para o domínio ou subdomínio. Pelo menos, dois registros NS devem ser definidos para cada domínio: um principal e outro secundário.
- **CNAME** - Significa Canonical NAME. Especifica um apelido (alias) para o hostname (A). É uma forma de redirecionamento.
- **MX** - Sigla para Mail eXchanger. Aponta o servidor de e-mails. Pode-se especificar mais de um endereço, formando-se assim uma lista em ordem de prioridade para que haja alternativas no caso de algum e-mail não puder ser entregue.

Serviços: DNS – Tipos de Registros

- **PTR** - PoinTeR, aponta o domínio reverso a partir de um endereço IP.
- **SOA** - Start Of Authority. Indica o responsável por respostas autoritárias a um domínio, ou seja, o responsável pelo domínio. Também indica outras informações úteis como número serial da zona, replicação, etc.
- **TXT** - Refere-se a TeXT, o qual permite incluir um texto curto em um hostname. Técnica usada para implementar o SPF.
- **SPF** - Sender Policy Framework, é uma tentativa de controle de falsos e-mails. Permite ao administrador de um domínio definir os endereços das máquinas autorizadas a enviar mensagens neste domínio.
- **SRV** - Abreviação de SeRVice, permite definir localização de serviços disponíveis em um domínio, inclusive seus protocolos e portas.

Serviços: DNS – Mensagem



Definições: [https://technet.microsoft.com/pt-br/library/dd197470\(v=ws.10\).aspx](https://technet.microsoft.com/pt-br/library/dd197470(v=ws.10).aspx)

Serviços: DNS – NSLOOKUP

- O nslookup é uma ferramenta administrativa de linha de comando para testar e solucionar problemas de servidores DNS.
- Essa ferramenta é instalada junto ao protocolo TCP/IP, ou seja, é comum aos sistemas operacionais que implementam a pilha.
- Para iniciar o Nslookup.exe no modo interativo, digite "nslookup" no prompt de comando:

C:\> nslookup

Servidor padrão: nome_do_servidor1.domínio.com

Endereço: 10.0.0.1

>

Serviços: DNS – NSLOOKUP

Existem 3 formas básicas de resolução via resolvedor (o cliente DN, que faz as solicitações):

- **Recursiva** - o cliente espera que o servidor envie a resposta final completa, caso não a tenha (não seja a autoridade), solicita recursivamente aos outros servidores até que obtê-la.
- **Iterativa** (cuidado não é INterativa) : o cliente solicita e se o servidor não tiver ele envia para o cliente o endereço IP do servidor que provavelmente tenha, aqui o cliente faz diretamente a segunda solicitação e iterativamente até obter o endereço.
- **Inversa** - para obter o nome a partir do IP, o resolvedor pode utilizar a solicitação inversa, nesse caso ele utiliza a classe PTR (ponteiro), para um solicitação desse tipo é necessário montar um mensagem com o ip invertido + in-addr + arpa 172.30.0.20 >" 20.0.30.172.in-addr.arpa"

Serviços: DNS – Pharming

- *Pharming* é um tipo específico de *phishing* que envolve a redireção da navegação do usuário para sites falsos, por meio de alterações no serviço de DNS (*Domain Name System*).
- Neste caso, quando você tenta acessar um *site* legítimo, o seu navegador *Web* é redirecionado, de forma transparente, para uma página falsa. Esta redireção pode ocorrer:
 - por meio do comprometimento do servidor de DNS do provedor que você utiliza;
 - pela ação de códigos maliciosos projetados para alterar o comportamento do serviço de DNS do seu computador;
 - Pela ação direta de um invasor, que venha a ter acesso às configurações do serviço de DNS do seu computador ou *modem* de banda larga.

<http://cartilha.cert.br/golpes/>

Questões

(FCC/TRT-RJ 2011) O cabeçalho da mensagem DNS possui um tamanho de

- (A) 12 bytes.
- (B) 12 bits.
- (C) 16 bytes.
- (D) 16 bits.
- (E) 32 bytes

Questões

(FCC/TRT-RJ 2011) O cabeçalho da mensagem DNS possui um tamanho de

(A) 12 bytes.

(B) 12 bits.

(C) 16 bytes.

(D) 16 bits.

(E) 32 bytes

Questões

(FCC/TRT-RJ 2011) O campo da mensagem do servidor DNS que especifica a operação solicitada e um código de resposta associado é denominado

- a) identificação.
- b) parâmetro.
- c) seção de perguntas.
- d) seção de respostas.
- e) seção de autoridades.

Questões

(FCC/TRT-RJ 2011) O campo da mensagem do servidor DNS que especifica a operação solicitada e um código de resposta associado é denominado

- a) identificação.
- b) parâmetro.
- c) seção de perguntas.
- d) seção de respostas.
- e) seção de autoridades.

Questões

(ESAF/ANA 2009) Um registro de recurso DNS é uma tupla composta pelos campos

- a) Name, Value, TTL.
- b) Name, Value, Type.
- c) Name, Type, TTL.
- d) Name, Value, Type, Cache.
- e) Name, Value, Type, TTL.

Questões

(ESAF/ANA 2009) Um registro de recurso DNS é uma tupla composta pelos campos

- a) Name, Value, TTL.
- b) Name, Value, Type.
- c) Name, Type, TTL.
- d) Name, Value, Type, Cache.
- e) Name, Value, Type, TTL.

Questões

(FCC/TER-PE 2011 ADAP) Dentre os tipos de registros de recursos do DNS, o CNAME tem como função especificar o nome do host preparado para aceitar mensagens de correio eletrônico para o domínio especificado.

(CESPE/Pref. Vitória 2007) Os registros de recurso PTR identificam os domínios pelos quais os servidores DNS são responsáveis. Um servidor DNS pode ser responsável por mais de um domínio na hierarquia DNS.

Questões

- E** (FCC/TER-PE 2011 ADAP) Dentre os tipos de registros de recursos do DNS, o **CNAME** tem como função especificar o nome do host preparado para aceitar mensagens de correio eletrônico para o domínio especificado.

- E** (CESPE/Pref. Vitória 2007) Os registros de recurso **PTR** identificam os domínios pelos quais os servidores DNS são responsáveis. Um servidor DNS pode ser responsável por mais de um domínio na hierarquia DNS.



LDAP

Lightweight Directory Access Protocol

LDAP – Serviço de Diretório

- É aquele que armazena informações de forma hierárquica, obedecendo aos critérios que regem seu princípio de organização, possibilitando buscas e consultas, podendo ser ou não distribuídos, disponibilizando suas informações para auxiliar outros serviços, protocolos e aplicativos.
- Traduzindo, **Diretórios são Bancos de dados especializados.**
 - Por esse prisma, o LDAP é similar ao SQL no sentido que é uma linguagem para interagir com bancos de dados sem especificar um banco de dados particular
- De fato, o banco de dados de suporte ao LDAP é quase sempre um sistema RDBMS geral, como o LDBM ou o Oracle.

LDAP – Histórico

- O **X.500** é um padrão de protocolos de serviços de diretórios, utilizados em redes de computadores, e foi elaborado para trabalhar sobre modelo OSI e incorporado ao pacote de protocolos ISO/IEC 9594. Designado para dar suporte ao padrão **X.400**, que define a troca de mensagens eletrônicas entre os usuários da rede local, a função do X.500 é prover serviços de diretórios para rede, centralizando a base de dados dos usuários da rede em um servidor X.500.
- O protocolo de acesso a diretórios **DAP** (*Directory Access Protocol*) faz parte das especificações do padrão X.500, e foi desenvolvido para trabalhar junto a todas as camadas do modelo OSI, com o objetivo definir o acesso de usuários aos serviços de diretórios que seu padrão provia.

LDAP – Histórico

- O LDAP foi criado como uma alternativa ao DAP, para prover acesso aos serviços de diretórios do X.500 pelos protocolos da pilha TCP/IP. O LDAP é mais fácil de ser implementado do que o DAP, além de exigir menos recursos da rede e de memória. Por esses motivos recebeu o nome *Lightweight Directory Access Protocol* (protocolo leve de acesso a diretórios).
- Posteriormente foram criados servidores de diretórios voltados para o TCP/IP e o LDAP. O Slapd (*stand-alone LDAP daemon* - servidor) foi escolhido como a melhor opção e consolidado. Com sua utilização, passa-se a colocar em prática um software provedor de serviços de diretórios específicos para o TCP/IP e o LDAP, deixando de lado o X.500 que é uma mera adaptação de um padrão desenvolvido para o modelo OSI. Com isso há um ganho em performance e funcionalidades e melhor integração com o LDAP.

LDAP – Definição

- Protocolo aberto (de camada de aplicação, TCP 389) para acessar e gerenciar informações de diretório, permitindo localizar quaisquer recursos existentes na rede, incluindo usuários.
- Usando serviços baseados em LDAP, o administrador não precisa criar um conta de usuário por host (Autenticação).
 - É necessário apenas incluir 1 registro desse usuário no banco de dados do LDAP e esse usuário pode efetuar login em qualquer host dessa rede.
- As implementação mais conhecidas são o **Active Directoy e o OpenLDAP.**

LDAP – Versões

***1993 primeira versão**

Problema de Segurança

***1996 LDAP v2**

Autenticação forte com Kerberos v4.

***1997 LDAP v3 (atual)**

Esta última foi desenvolvida para solucionar uma série de limitações existentes na anterior, incluindo aspectos de segurança, passando a suportar protocolos de autenticação forte como o Simple Authentication Security Layer(SASL) e o Transport Layer Security(TLS)

LDAP – Vantagens

- **Facilidade em organizar e localizar informações e arquivos disponibilizados.** Cada funcionário pode ter uma conta de acesso no servidor LDAP, para que possa cadastrar informações sobre si e compartilhar arquivos.
- **Grande escalabilidade.** É possível replicar servidores (para backup ou balanceamento de carga) e incluir novos servidores de uma forma hierárquica, interligando departamentos e filiais de uma grande multinacional por exemplo.
- **Padrão aberto.** Pode ser usado em qualquer tipo de rede TCP/IP, permitindo que existam produtos para várias plataformas.

LDAP – Active Directory

- O AD (Active Directory) é uma implementação de serviço de diretório no protocolo LDAP (Lightweight Directory Access Protocol) e é um software da Microsoft utilizado em ambientes Windows.
- O AD representa todo recurso de rede, por exemplo as máquinas, como **Objetos**, os quais possuem propriedades chamadas atributos dos objetos.
- **Domínio**
- **Floresta**
- **Domain Controller**
- **Group Policy**

LDAP – OpenLDAP

- É uma das suítes mais usadas. Uma vez instalado, pode ser configurado através do arquivo **/etc/sldap.conf**.
- O servidor é o ***daemon sldapd*** e o cliente o **ldapsearch**, que é originalmente um utilitário de modo texto mas que pode trabalhar em conjunto com vários *front-ends* gráficos.
- O OpenLDAP pode ser usado em conjunto com vários clientes comerciais e permite estabelecer vários níveis de permissões e controle de acesso para os dados compartilhados, além de suportar criptografia.
- Note que embora seja possível ter acesso à base de dados remotamente, **o LDAP não é um protocolo na Internet, apenas em Intranets.**

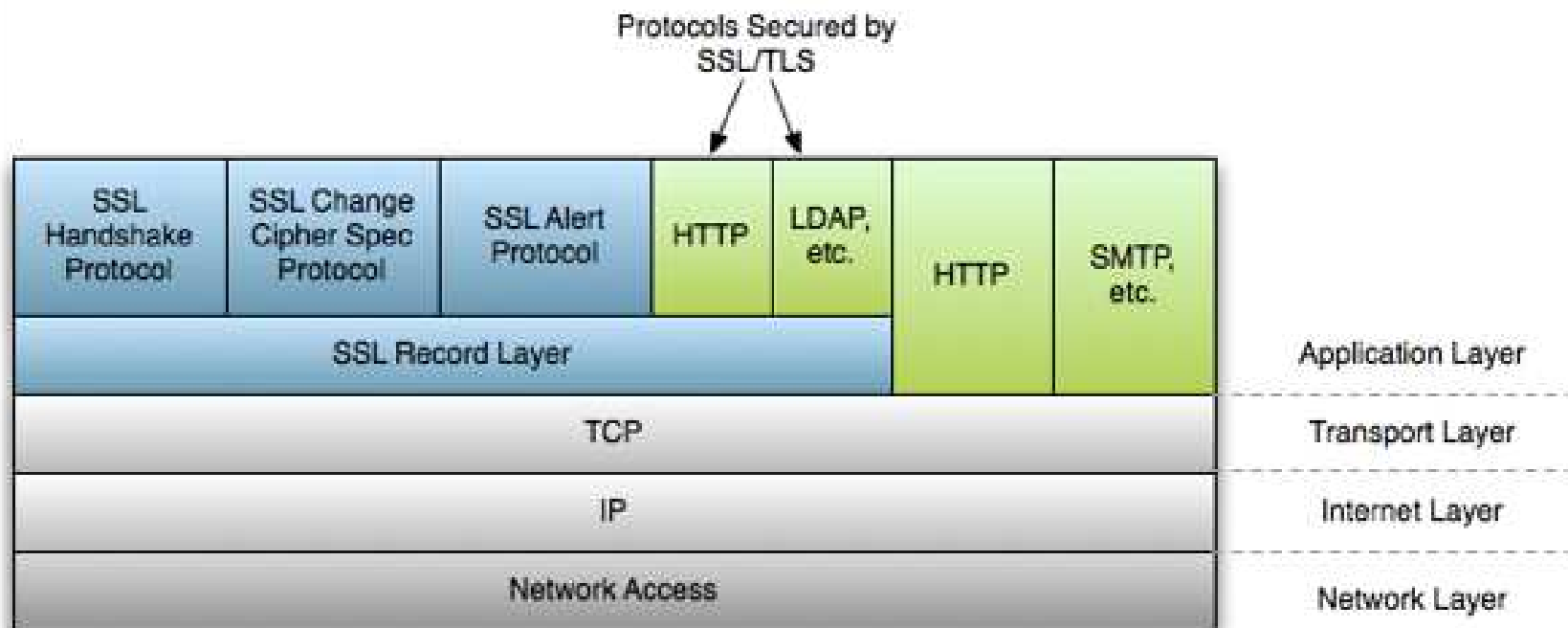
LDAP – OpenLDAP

A suíte é composta pelos softwares:

- **Slapd** - *stand-alone LDAP daemon* (servidor);
- **Slurpd** - *stand-alone LDAP update replication daemon*;
- **Syncrepl** – Replicação de base é mais flexível e tem mais recursos que o slurpd, mas só funciona nas versões mais novas do OpenLDAP;
- Bibliotecas de implementação do protocolo LDAP;
- Utilitários, ferramentas e amostras clientes.

LDAP – Seguro (LDAPS)

Porta TCP 686



Questões

(CESPE/ABIN 2010) O LDAP permite que a estrutura hierárquica da organização esteja representada no serviço de diretório e que o processo de autenticação de usuários seja distribuído entre um servidor mestre e vários servidores escravos.

(CESPE/ABIN 2010) Um serviço de diretório embasado no LDAP possibilita que haja um controle centralizado de usuários e que seja armazenado e acessível por métodos padronizados.

(CESPE/ABIN 2010) O LDAP versão 3 suporta tanto a autenticação por meio de certificados quanto o uso de TLS.

Questões

C (CESPE/ABIN 2010) O LDAP permite que a estrutura hierárquica da organização esteja representada no serviço de diretório e que o processo de autenticação de usuários seja distribuído entre um servidor mestre e vários servidores escravos.

C (CESPE/ABIN 2010) Um serviço de diretório embasado no LDAP possibilita que haja um controle centralizado de usuários e que seja armazenado e acessível por métodos padronizados.

C (CESPE/ABIN 2010) O LDAP versão 3 suporta tanto a autenticação por meio de certificados quanto o uso de TLS.

Questões

(FCC/MPE-RN 2010) NÃO se trata de uma característica do LDAP:

- a) Organização de servidores de forma hierárquica.
- b) Substituição dos bancos de dados relacionais.
- c) Multiplataforma.
- d) Padrão aberto.
- e) Grande escalabilidade.

Questões

(FCC/MPE-RN 2010) NÃO se trata de uma característica do LDAP:

- a) Organização de servidores de forma hierárquica.
- b) Substituição dos bancos de dados relacionais.
- c) Multiplataforma.
- d) Padrão aberto.
- e) Grande escalabilidade.

Questões

(FCC/MPE-RN 2010) NÃO se trata de uma característica do LDAP:

- a) Organização de servidores de forma hierárquica.
- b) Substituição dos bancos de dados relacionais.
- c) Multiplataforma.
- d) Padrão aberto.
- e) Grande escalabilidade.

Questões

(FCC/MPE-RN 2010) Em relação ao LDAP é INCORRETO afirmar que

- a) serve como base para uma solução DNS (Domain Name System).
- b) toda informação de um item pode ser colocada em um único registro.
- c) permite a obtenção de informações de apenas um ramo da hierarquia.
- d) possibilita implantar segurança em ramos diferentes da árvore.
- e) localiza e gerencia usuários e recursos na rede.

Questões

(FCC/MPE-RN 2010) Em relação ao LDAP é INCORRETO afirmar que

- a) serve como base para uma solução DNS (Domain Name System).
- b) toda informação de um item pode ser colocada em um único registro.
- c) permite a obtenção de informações de apenas um ramo da hierarquia.
- d) possibilita implantar segurança em ramos diferentes da árvore.
- e) localiza e gerencia usuários e recursos na rede.

Questões

(CESPE/TCU 2008) Os analistas de um dos grupos constataram que havia, nessa infra-estrutura, computadores agrupados em vários domínios distintos e que, em cada domínio, havia um banco de dados comum, compartilhado pelos computadores que formam cada um desses domínios. Com base nessas constatações, o grupo inferiu preliminarmente que a forma de organização da infra-estrutura era compatível com a tecnologia Microsoft Active Directory, o que foi confirmado posteriormente. Nessa situação, será possível ao administrador definir diretivas de segurança para cada domínio, bem como estabelecer relacionamentos entre esses domínios. Além disso, será possível a instalação de mais de um controlador de domínio em cada domínio.

Questões

C (CESPE/TCU 2008) Os analistas de um dos grupos constataram que havia, nessa infra-estrutura, computadores agrupados em vários domínios distintos e que, em cada domínio, havia um banco de dados comum, compartilhado pelos computadores que formam cada um desses domínios. Com base nessas constatações, o grupo inferiu preliminarmente que a forma de organização da infra-estrutura era compatível com a tecnologia Microsoft Active Directory, o que foi confirmado posteriormente. Nessa situação, será possível ao administrador definir diretivas de segurança para cada domínio, bem como estabelecer relacionamentos entre esses domínios. Além disso, será possível a instalação de mais de um controlador de domínio em cada domínio.

LDAP – Estrutura

- O LDAP permite que a estrutura hierárquica da organização esteja representada no serviço de diretório e que o processo de autenticação de usuários seja distribuído entre um servidor mestre e vários servidores escravos.
- A representação hierárquica pode refletir limites políticos ou geográficos das organizações ou se basear nos nomes usados no DNS.
- **A organização dos servidores neste caso é similar ao DNS:** é especificado um servidor raiz e a partir daí é possível ter vários níveis de servidores, além de *mirrors* do servidor principal.

LDAP – Esquema e Objeto

- **uid** (userid) – Trata-se de um identificador único obrigatório
- **cn** (common name) – O nome da pessoa
- **givenname** – O nome da pessoa
- **Sn** (surname) – O sobrenome da pessoa
- **o** (organization) – O nome da empresa
- **ou** (organizational unit) – Departamento da empresa onde a pessoa trabalha
- **mail** – O endereço de correio eletrônico da pessoa
- **dc** (domain component)
- **dn** (distinguished name) – Identifica uma entrada de forma não ambígua num serviço de diretório

LDAP – Esquema e Objeto

um *Distinguished Name* terá a forma:

- uid=jeapil,cn=pillou,givenname=jean-francois

um *Relative Distinguished Name* aqui é

- “uid=jeapil”.
- O **esquema** possibilita a manutenção da consistência dos dados do diretório, por exemplo, definir se um atributo poder possuir um ou vários valores.
- Uma **object class** apenas informa quais atributos são obrigatórios e quais são opcionais para certo registro.

LDAP – Modelos

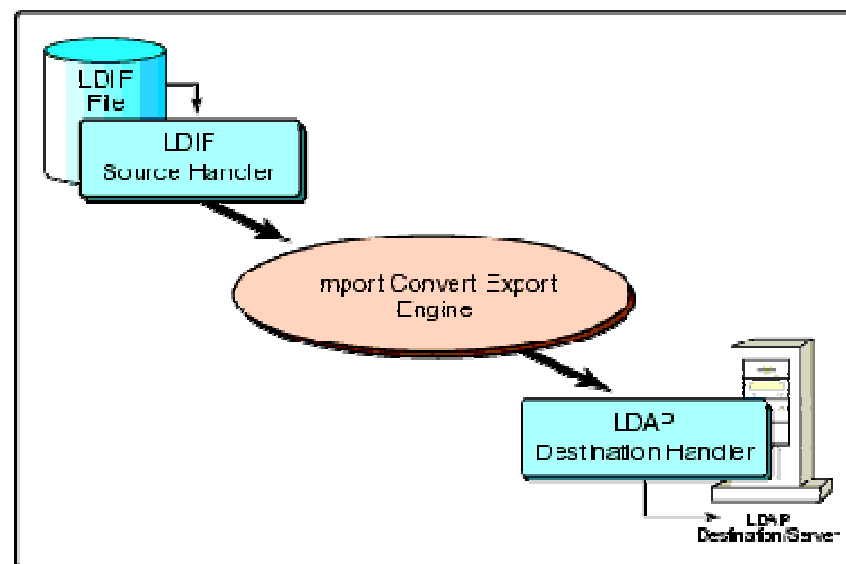
- **Modelo de Informação** – Define o tipo de informação que pode ser armazenada em um diretório LDAP
- **Modelo de Nomes** – Define como a informação no diretório LDAP pode ser organizada e referenciada
- **Modelo Funcional** – Define o que pode ser feito, ou seja as operações que podem ser executadas com a informação no diretório LDAP e como ela pode ser acessada e alterada
- **Modelo de Segurança** – Define como a informação no diretório LDAP pode ser protegida de acessos ou modificações não autorizadas.

LDAP – Object Class

- **Estrutural** – Indica os atributos que uma entrada pode ter e onde ela se encontra na estrutura da árvore.
- **Auxiliar** – Indica os atributos que a entrada pode ter.
- **Abstrata** – Indica uma especificação parcial na hierarquia da object class hierarchy; somente subclasses estruturais e auxiliaries podem aparecer como entrada no diretório.

LDAP – LDIF

- O LDAP fornece um formato de troca (**LDIF**, *Lightweight Data Interchange Format*) que permite importar e exportar os dados de um anuário com um simples arquivo texto.
- A maioria dos servidores LDAP suporta este formato, que permite uma grande interoperabilidade entre eles.



LDAP – Operações Básicas

- Bind – autentica e especifica a versão do protocolo LDAP;
- Search – procura por e/ou recupera entradas dos diretórios;
- Compare – testa se uma entrada tem determinado valor como atributo;
- ADD – adiciona uma nova entrada;
- Delete – apaga uma entrada;
- Modify – modifica uma entrada;
- Modify DN – move ou renomeia uma entrada;
- Start TLS – protege a conexão com a Transport Layer Security (TLS);
- Abandon – aborta uma requisição prévia;
- Extended Operation – operação genérica para definir outras operações;
- Unbind – fecha a conexão, não o inverso de Bind.

Questões

(FCC/TRT-4 2011) No âmbito de LDAP, Bind

- a) autentica e especifica a versão do protocolo LDAP.
- b) adiciona uma nova entrada.
- c) protege a conexão com a Transport Layer Security.
- d) aborta uma requisição prévia.
- e) testa se uma entrada tem determinado valor como atributo.

Questões

(FCC/TRT-4 2011) No âmbito de LDAP, Bind

- a) autentica e especifica a versão do protocolo LDAP.
- b) adiciona uma nova entrada. (ADD)
- c) protege a conexão com a Transport Layer Security. (Start TLS)
- d) aborta uma requisição prévia. (Abandon)
- e) testa se uma entrada tem determinado valor como atributo. (Compare)

Questões

(FCC/TRT-24 2011) Em relação ao LDAP, é INCORRETO afirmar:

- a) As entradas são organizadas em uma estrutura em árvore chamada Directory Information Tree (DIT).
- b) As entradas são organizadas na DIT, segundo o seu Relative Distinguished Names (RDN).
- c) O Distinguished Name (DN) é um nome único que identifica sem ambiguidades cada entrada.
- d) Os Distinguished Names (DN) são constituídos por uma sequência de Relative Distinguished Names (RDN).
- e) Cada Relative Distinguished Name (RDN) corresponde a um ramo da árvore.

Questões

(FCC/TRT-24 2011) Em relação ao LDAP, é INCORRETO afirmar:

- a) As entradas são organizadas em uma estrutura em árvore chamada Directory Information Tree (DIT).
- b) As entradas são organizadas na DIT, segundo o seu Relative Distinguished Names (RDN).
- c) O Distinguished Name (DN) é um nome único que identifica sem ambiguidades cada entrada.
- d) Os Distinguished Names (DN) são constituídos por uma sequência de Relative Distinguished Names (RDN).
- e) Cada Relative Distinguished Name (RDN) corresponde a um ramo da árvore.

Questões

(FCC/TRT-14 2011) Em relação ao LDAP, é INCORRETO afirmar:

- a) É derivado do sistema de diretórios X.500.
- b) É basicamente um sistema de diretórios que engloba o diretório em si e um protocolo denominado DAP.
- c) Normalmente um cliente conecta-se ao servidor LDAP, através da porta padrão 389 (TCP).
- d) A operação Compare tem como função testar se uma entrada tem determinado valor como atributo.
- e) Extended Operation é uma operação genérica para definir outras operações.

Questões

(FCC/TRT-14 2011) Em relação ao LDAP, é INCORRETO afirmar:

- a) É derivado do sistema de diretórios X.500.
- b) É basicamente um sistema de diretórios que engloba o diretório em si e um protocolo denominado DAP.
- c) Normalmente um cliente conecta-se ao servidor LDAP, através da porta padrão 389 (TCP).
- d) A operação Compare tem como função testar se uma entrada tem determinado valor como atributo.
- e) Extended Operation é uma operação genérica para definir outras operações.

Questões

(FGV/MEC 2009) *Lightweight Directory Access Protocol* (LDAP) é um *protocol* destinado à comunicação entre servidores LDAP e *clients* LDAP. Nesse processo, *clients* LDAP acessam diretórios armazenados por servidores LDAP. O “L” de LDAP significa *lightweight* porque ele é um protocolo pequeno e fácil, derivado do *X.500 Directory Access Protocol* (DAP) definido na arquitetura *OSI/ISO*. Servidores LDAP armazenam informação em diretórios no formato hierárquico, existindo quatro modelos, dos quais dois são descritos a seguir:

- I. Descreve as operações que podem ser executadas na informação armazenada no diretório LDAP.
- II. Descreve como a informação no diretório LDAP pode ser protegida de acesso não autorizado.

Os modelos descritos são denominados, respectivamente:

- (A) FUNCTIONAL e INFORMATION
- (B) FUNCTIONAL e OPERATIONAL
- (C) FUNCTIONAL e SECURITY
- (D) NAMING e INFORMATION
- (E) NAMING e SECURITY

Questões

(FGV/MEC 2009) *Lightweight Directory Access Protocol* (LDAP) é um *protocol* destinado à comunicação entre servidores LDAP e *clients* LDAP. Nesse processo, *clients* LDAP acessam diretórios armazenados por servidores LDAP. O “L” de LDAP significa *lightweight* porque ele é um protocolo pequeno e fácil, derivado do *X.500 Directory Access Protocol* (DAP) definido na arquitetura *OSI/ISO*. Servidores LDAP armazenam informação em diretórios no formato hierárquico, existindo quatro modelos, dos quais dois são descritos a seguir:

- I. Descreve as operações que podem ser executadas na informação armazenada no diretório LDAP.
- II. Descreve como a informação no diretório LDAP pode ser protegida de acesso não autorizado.

Os modelos descritos são denominados, respectivamente:

- (A) FUNCTIONAL e INFORMATION
- (B) FUNCTIONAL e OPERATIONAL
- (C) FUNCTIONAL e SECURITY
- (D) NAMING e INFORMATION
- (E) NAMING e SECURITY



Dúvidas?

Prof. Walter Cunha

falecomigo@waltercunha.com

