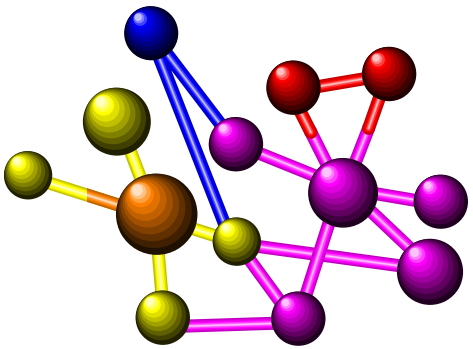
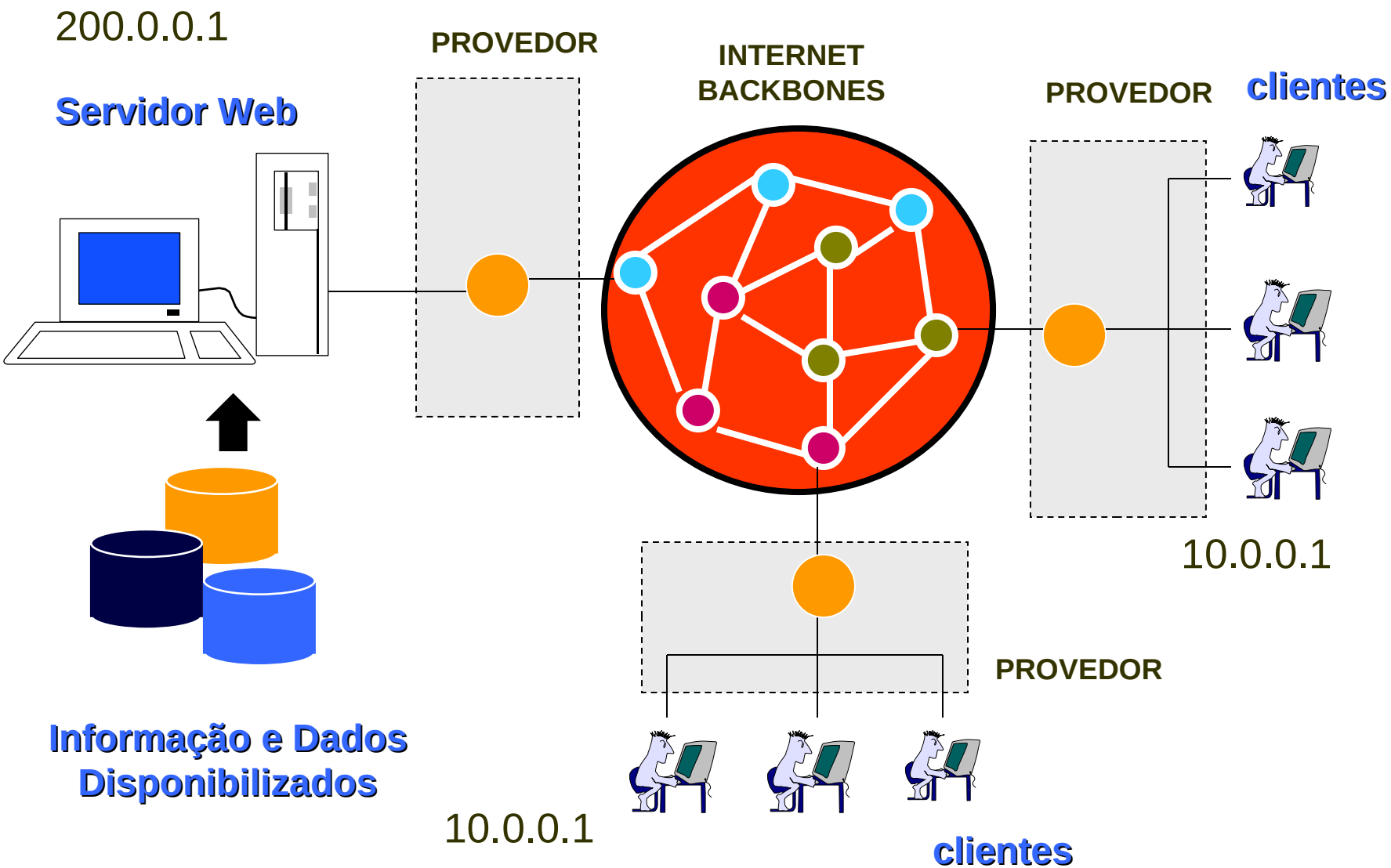


Endereçamento Internet e Intranet

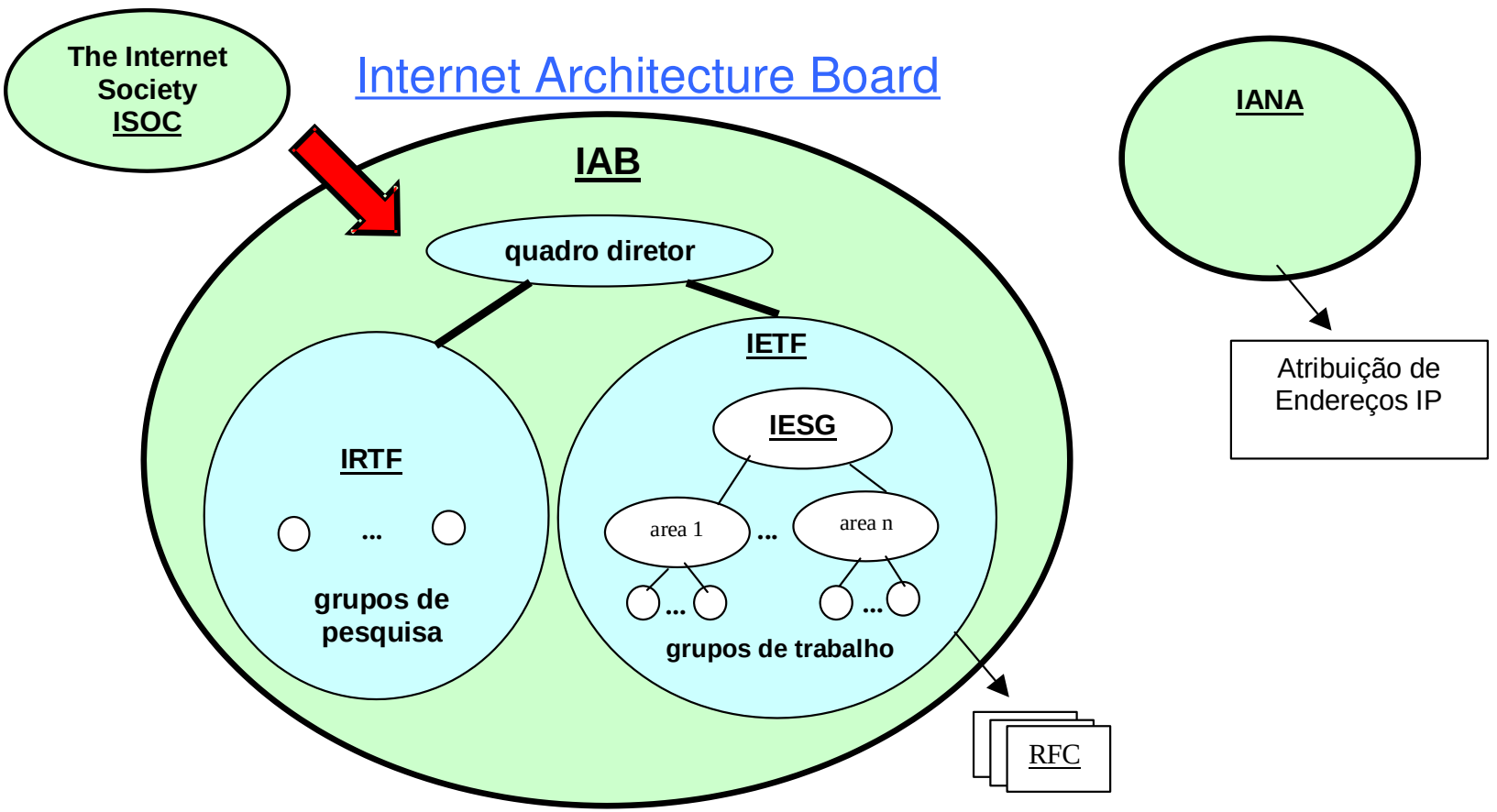
Redes TCP/IP

Infra-estrutura de Comunicação



Padrões da Internet

- **<u>Conceito:</u> Documentação referentes a protocolos, padrões e políticas, publicadas para permitir que diferentes fabricantes forneçam produtos compatíveis com a internet.**

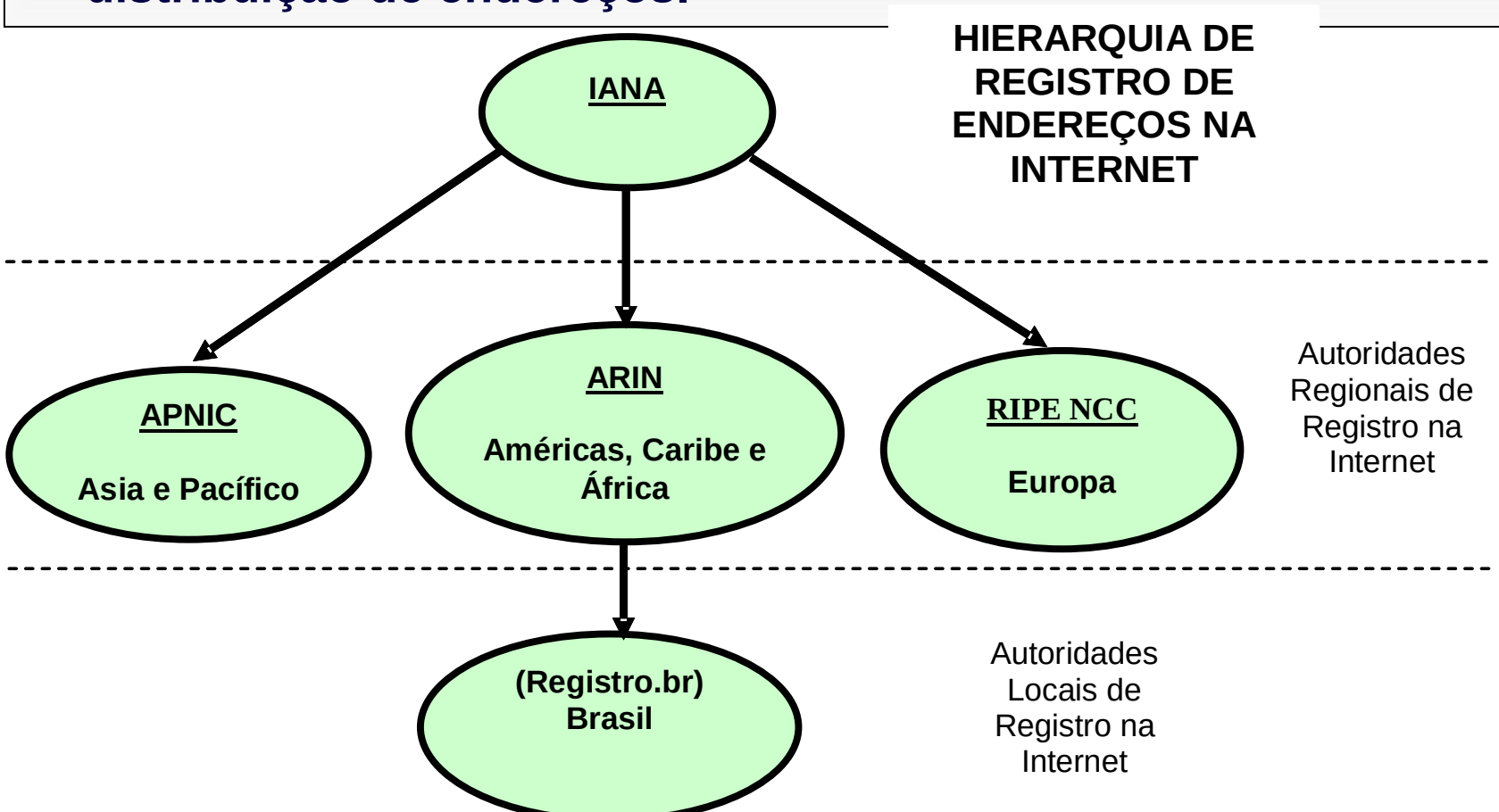


Padrões na Internet

- IAB: (***The Internet Architecture Board***).
- IETF: (***The Internet Engineering Task Force***). **Grupo de trabalho que identifica, prioriza e endereça assuntos considerados de curto prazo, incluindo protocolos, arquitetura e operações de serviços.**
- RFC: (***Request for Comments***). **Denominação dada aos documentos que especificam padrões e serviços para Internet e para a arquitetura TCP/IP.**
- IANA (***The Internet Assigned Numbers Authority***). **Organização internacional responsável por coordenar a distribuição de endereços IP entre as diversas redes de computadores que se conectam a Internet.**
- ISOC (***The Internet Society***).

Endereços na Internet

- Conceito: **A atribuição de endereços IP para os computadores que se conectam a Internet é coordenada por autoridades de abrangência mundial, de maneira a evitar a duplicação e a má distribuição de endereços.**



Conexão de Intranets com a Internet

- **Tipos de hosts numa empresa:**
  - **Hosts acessíveis** apenas internamente**.**
  - **Hosts acessíveis tanto** internamente quanto externamente**.**

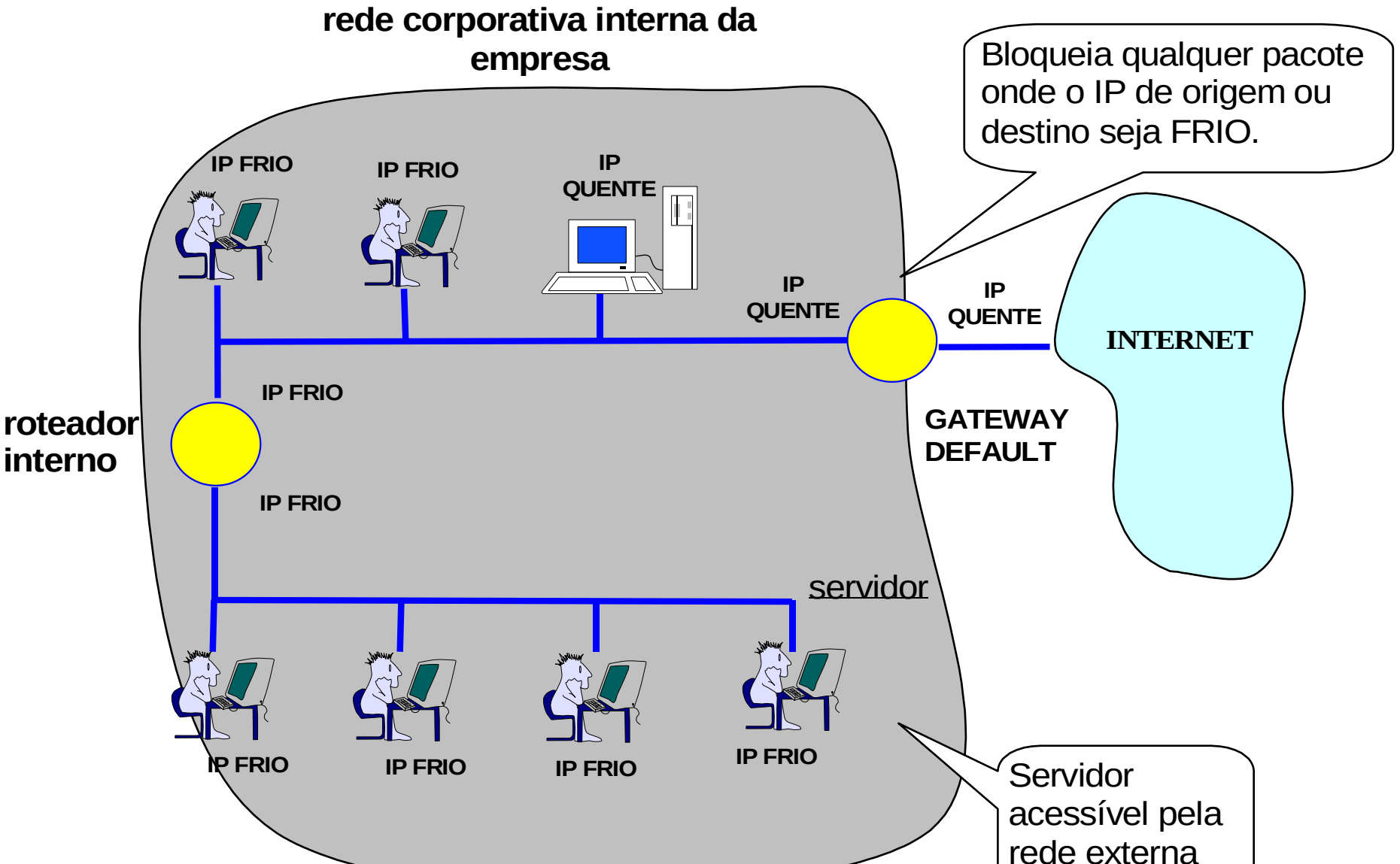
- **As regras para atribuições de endereços IPs com diferentes graus de conectividade com o mundo externo são definidas pela RFC 1918.**

  - Hosts categoria 1:
    - **Hosts que se comunicam APENAS INTERNAMENTE.**
  - Hosts categoria 2:
    - **Hosts que se comunicam INDIRETAMENTE com o mundo externo**.
  - Hosts categoria 3:
    - **Hosts que se comunicam DIRETAMENTE com o mundo externo.**

Motivação – Falta de IP's e Segurança

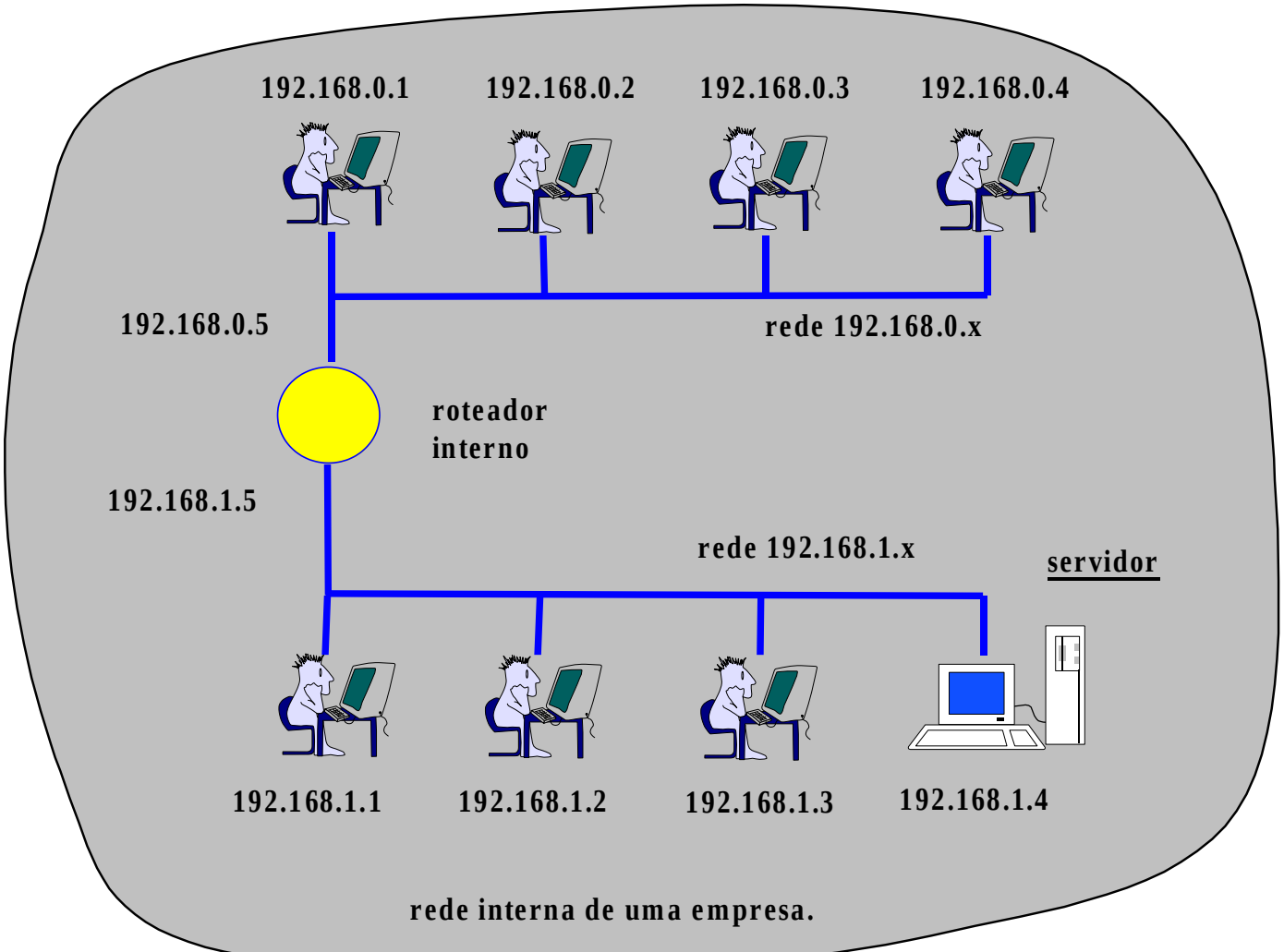
- Desperdício de IP's:
  - MIT tem 16,843,008.
  - General Electric tem 17,206,528.
  - IBM tem 17,542,656.
  - AT&T tem 19,800,320

Roteador Interno e Gateway Default



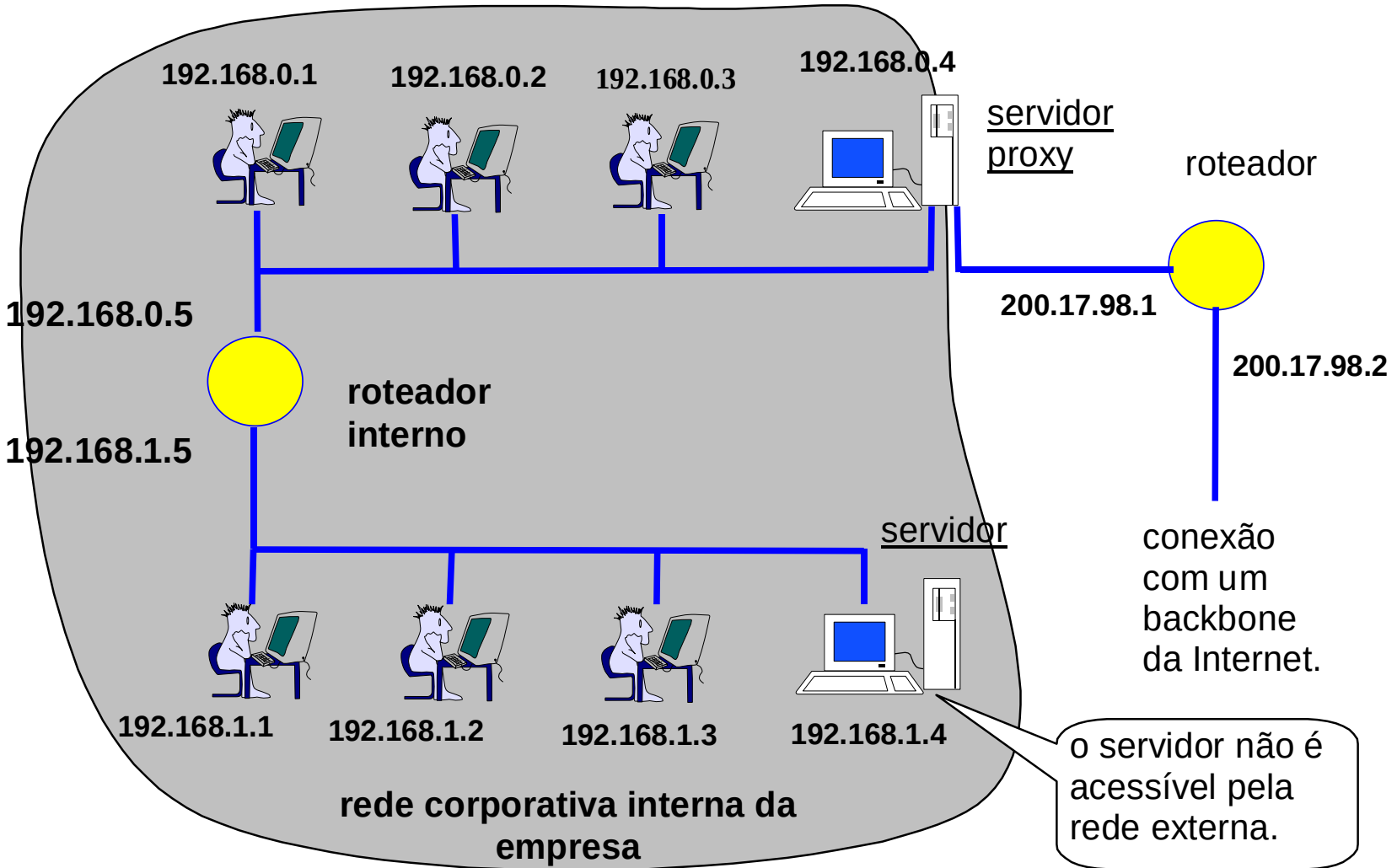
Hosts categoria 1 - Exemplo 1

Exemplo de uma rede Intranet constituída de duas redes físicas conectadas por um roteador.



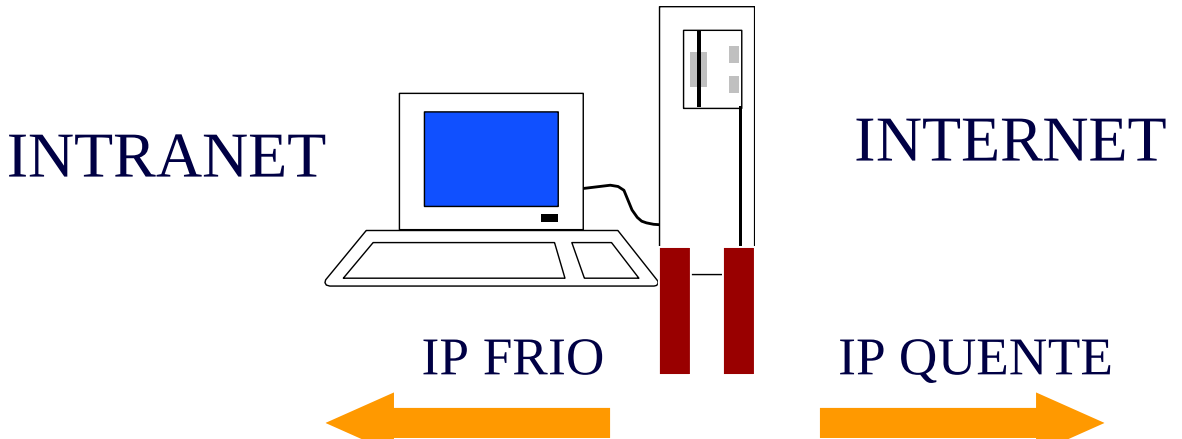
Hosts Categoria 2

Exemplo de uma rede Intranet interligada a Internet através de um servidor proxy. Nessa rede, os hosts estão na categoria 2.



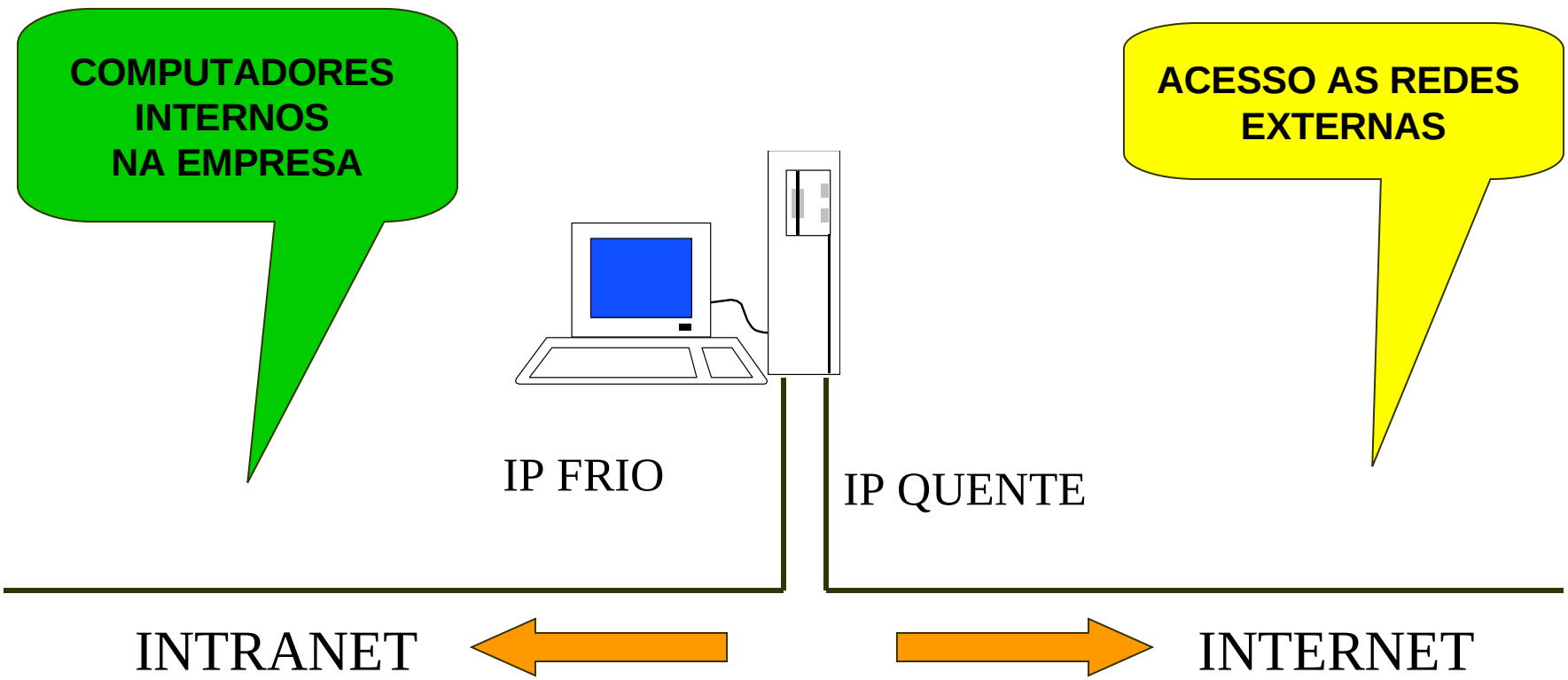
Servidor Proxy

- O Proxy é geralmente implementado através de um computador com duas interfaces de rede, uma conectada a rede interna e a outra a rede externa.
  - Quando uma aplicação cliente necessita acessar informações de um servidor externo, ele efetua o pedido ao servidor proxy.
  - O servidor proxy contata o servidor externo e retorna o resultado ao cliente.



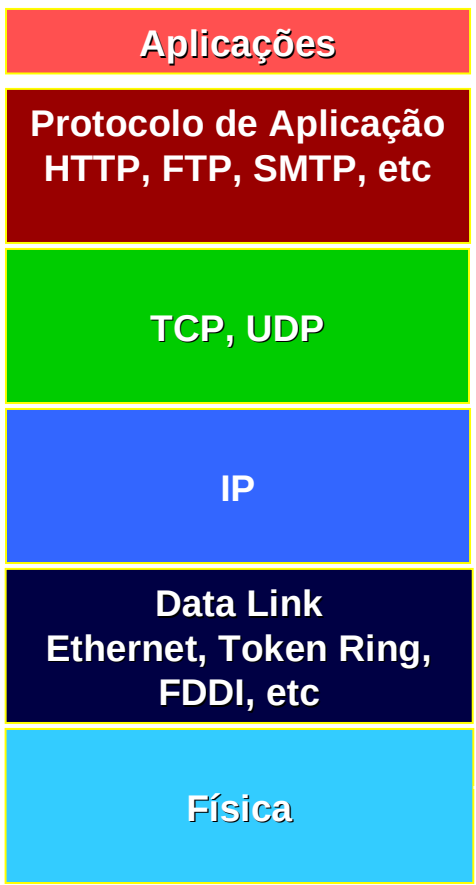
Servidor Proxy

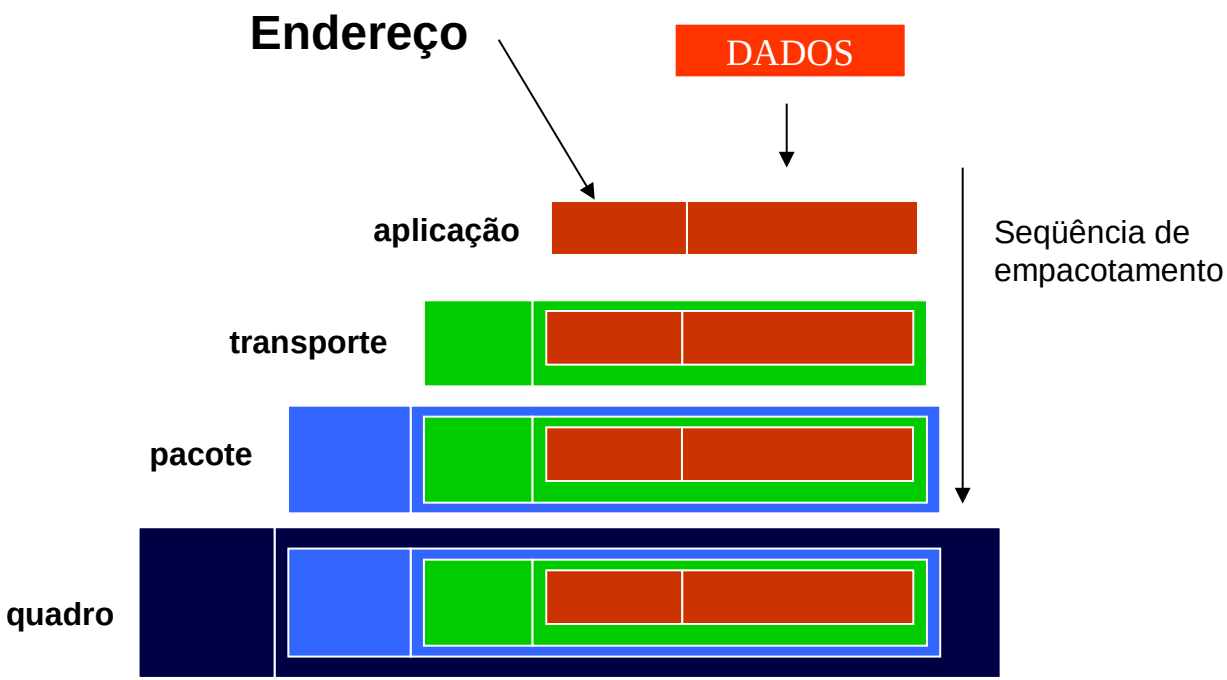
- **O Proxy = Gateway de aplicação**
  - **Para funcionar o proxy analisa o conteúdo do protocolo da aplicação.**



Proxy depende da Aplicação

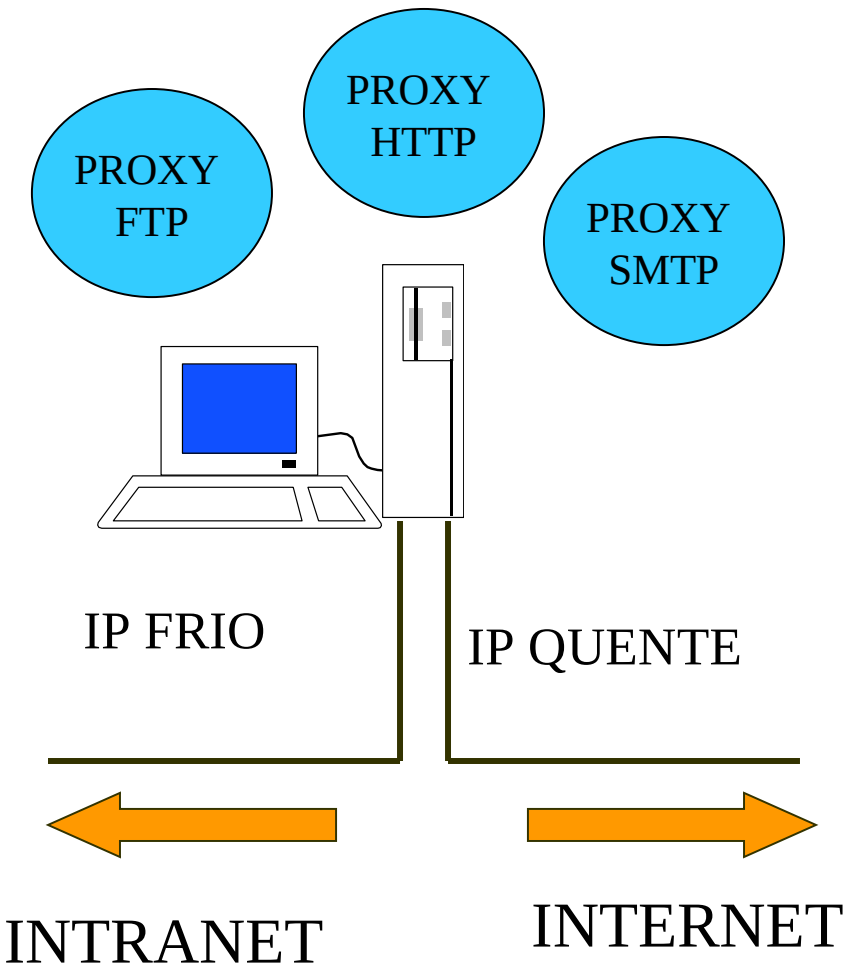
Cada protocolo da camada de aplicação formada seu cabeçalho de maneira diferente.





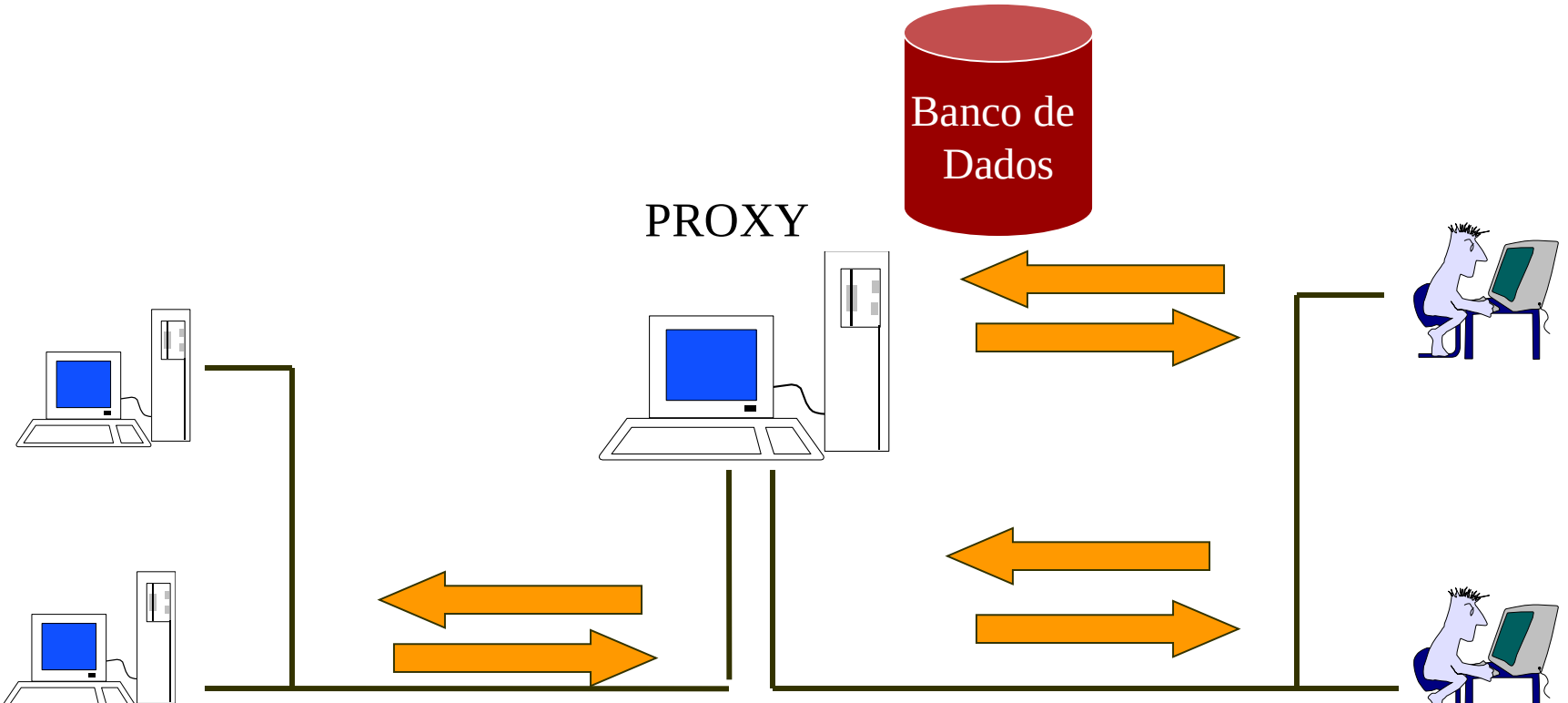
O Proxy Depende da Aplicação

- Numa rede conectada através de Proxy, os serviços disponibilizados pelos usuários são limitados aos serviços que o Proxy é capaz de compreender.



Outras Funções do Proxy

- Os proxys podem executar ainda as funções de:
  - Autenticação
  - Cache
  - Restrição de Acesso: Por conteúdo, IP, Hora do Dia, etc.

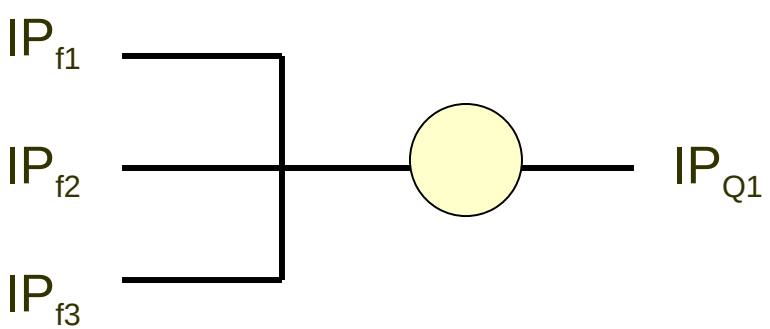


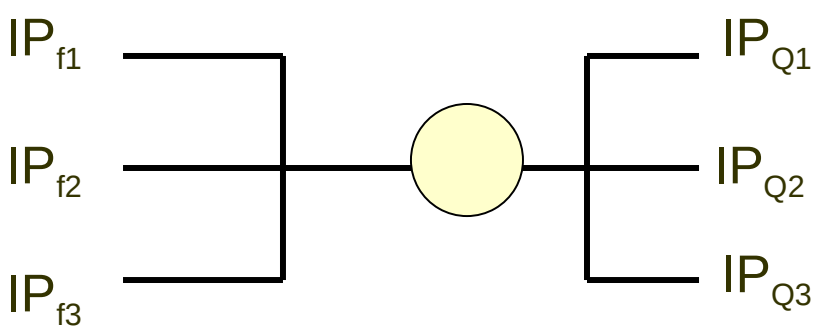
NAT: Network Address Translation

- Permite traduzir endereços privados em endereços registrados.
  - Seu funcionamento é definido pela RFC 1631
- A função de NAT é geralmente executada por:
  - ROTEADORES, FIREWALLS OU APLICATIVOS INSTALADOS EM COMPUTADORES COM DUAS PLACAS DE REDE
    - EM TODOS OS CASOS, OS CLIENTES SÃO CONFIGURADOS PARA UTILIZAR O DISPOSITIVO DE NAT COMO ROTEADOR.

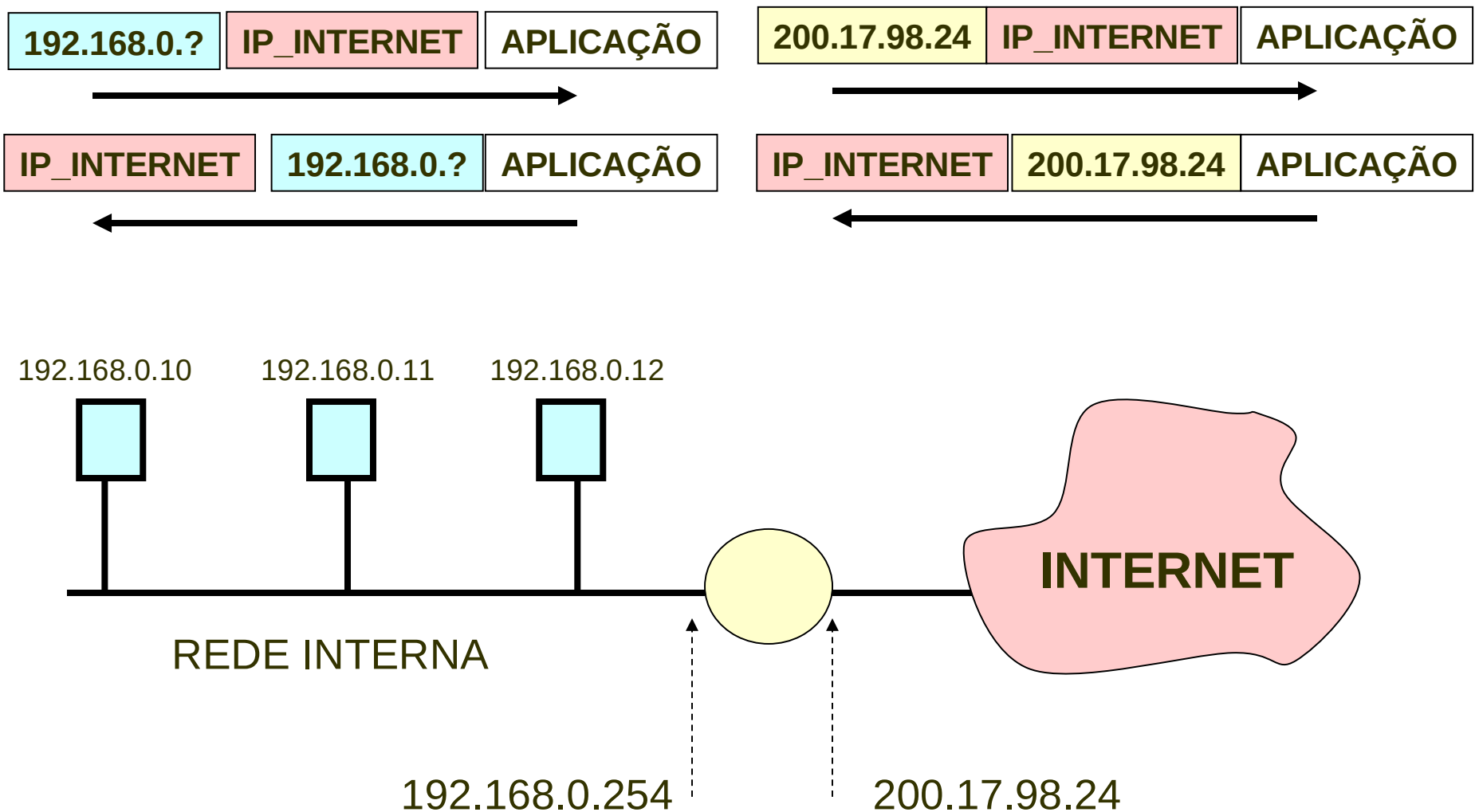
Tipos de NAT

- Traduções:
  - One-TO-Many (Dinâmico)
    - Traduzir vários IP's para um único
    - Funcionamento similar ao Proxy (mais usual)
  - Many-TO-Many (Estático)
    - Traduzir um grupo de IP's para outro grupo de IP's





NAT: Implementado em Roteadores ou Firewalls



LIMITAÇÕES DO NAT

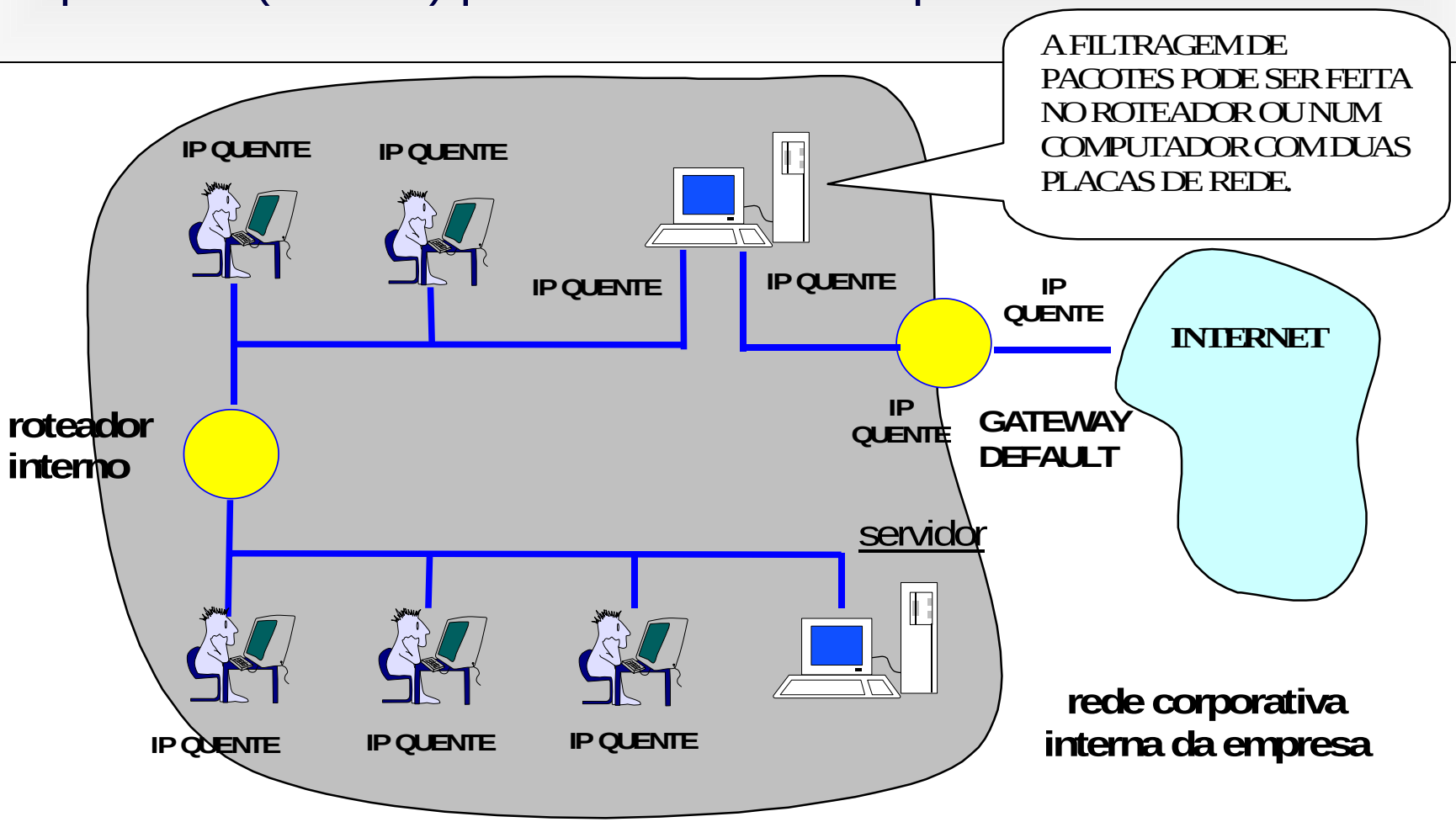
- NAT permite apenas que clientes internos acessem servidores externos:
  - Um computador com IP privado funcionará apenas como cliente.
- Além da troca dos IPs, muitos parâmetros precisam ser recalculados:
  - Estas operações diminuem a velocidade do roteador.

TIPOS DE NAT

- NAT Estático
  - Mapeia um Endereço IP em Outro
  - O número de Endereços Privados é igual ao Número de endereços Públicos
  - Converte apenas endereços IP
- NAT Dinâmico
  - Mapeia um Endereço IP público em vários endereços Privados
  - Utiliza informação das portas UDP e TCP para fazer o mapeamento.
  - Usualmente chamado de
    - PAT: Port Address Translation (PAT) ou
    - NAPT: Networ and Address Port Translation

Host Categoria 3

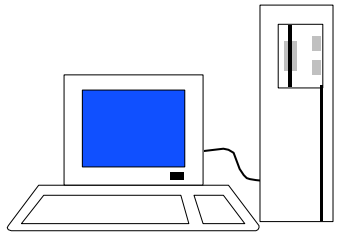
- Hosts categoria 3 precisam ser protegidos por filtros de pacotes (firewall) para não ficarem expostos a rede externa.



PORTAS

a comunicação entre o cliente e o servidor se dá através de protocolos de aplicação padronizados

Cliente



Dados armazenados

FTP — Porta 21 — programa servidor de transferência de arquivos

TELNET — Porta 23 — programa servidor de terminal remoto

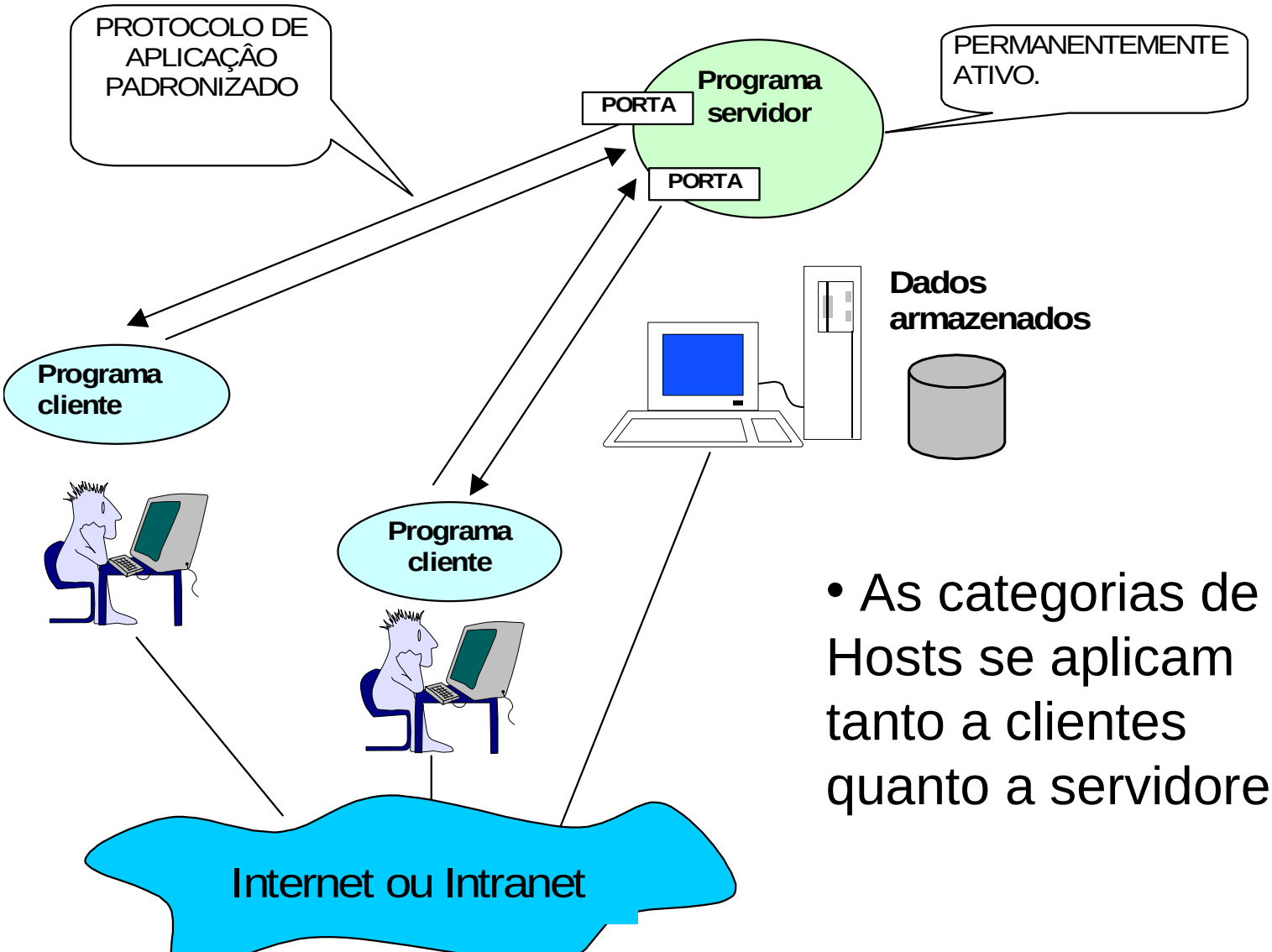
SMTP — Porta 25 — programa servidor de correio eletrônico

Porta 80 — HTTP — programa servidor de hipertexto e outros serviços WWW

Porta 161 — SNMP — programa gerência Rede

Porta 53 — DNS — programa servidor de nomes

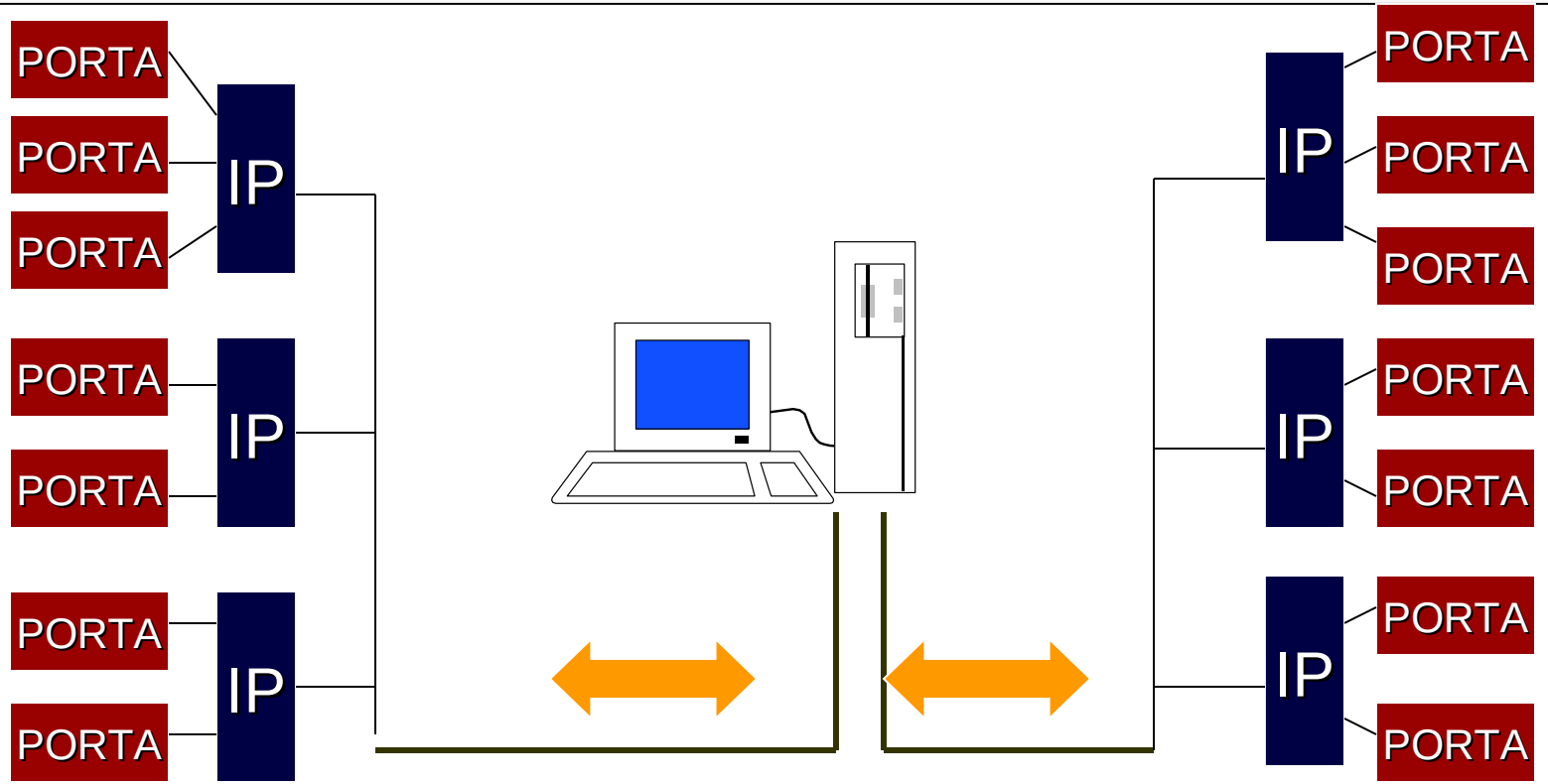
Arquitetura Cliente-Servidor



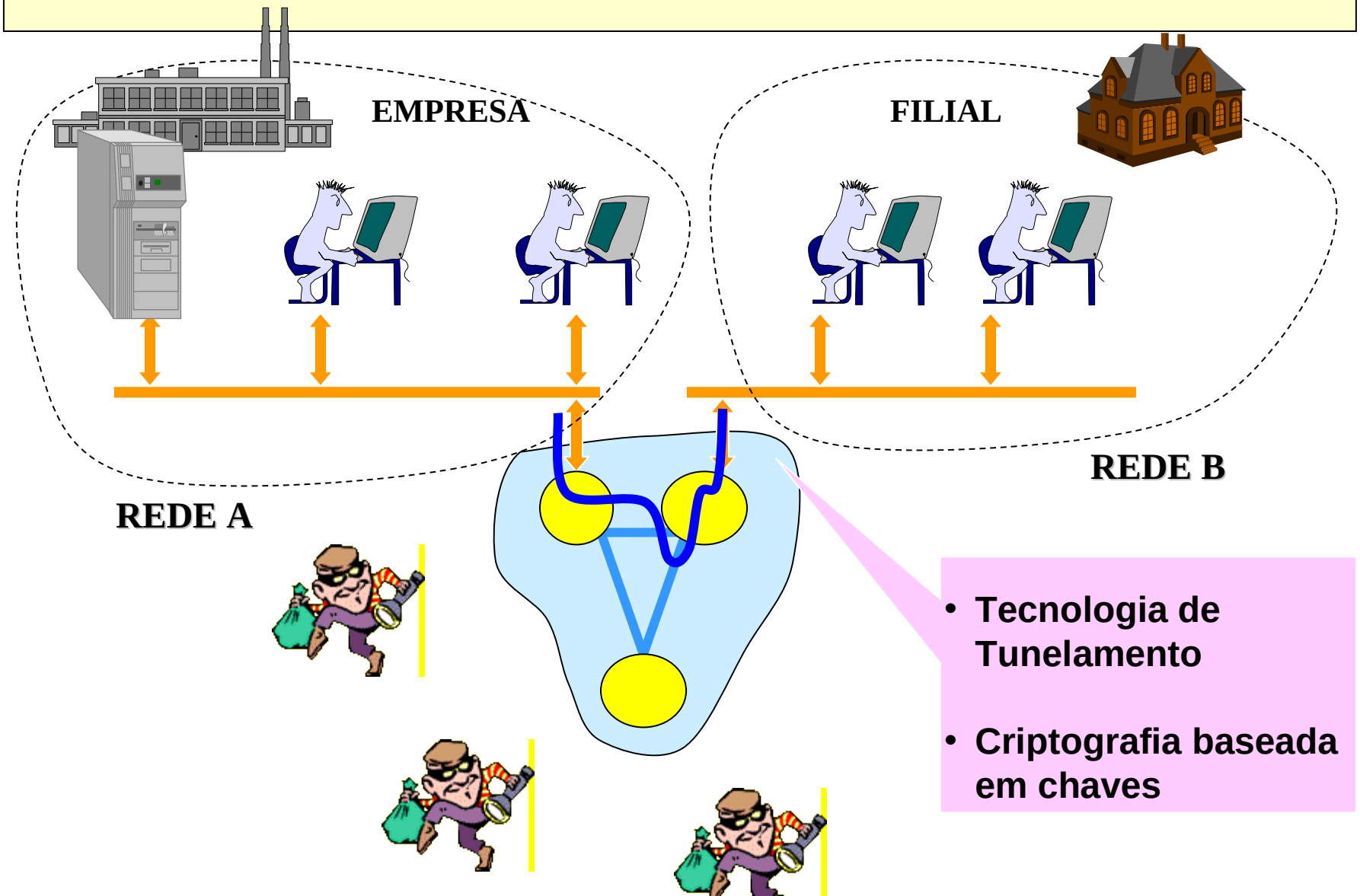
- As categorias de Hosts se aplicam tanto a clientes quanto a servidores.

Filtragem de Pacotes

- A filtragem de pacotes é feita com base nas informações contidas no cabeçalho do pacotes e das informações sobre as portas.



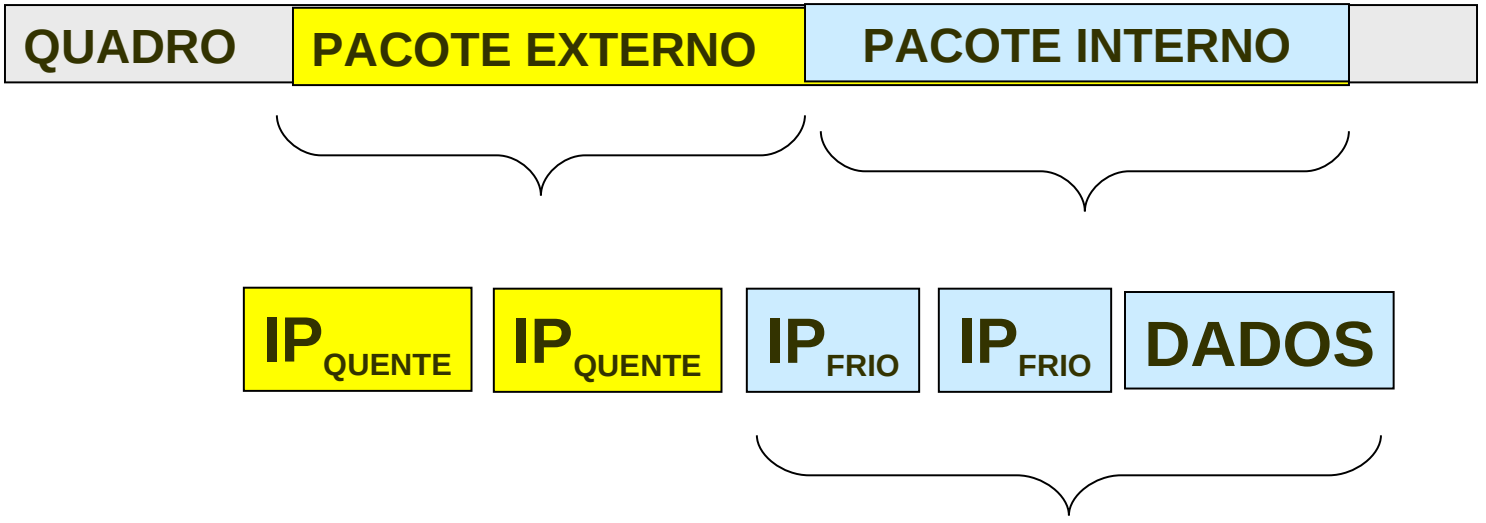
Extranets = VPN (Virtual Private Networks)



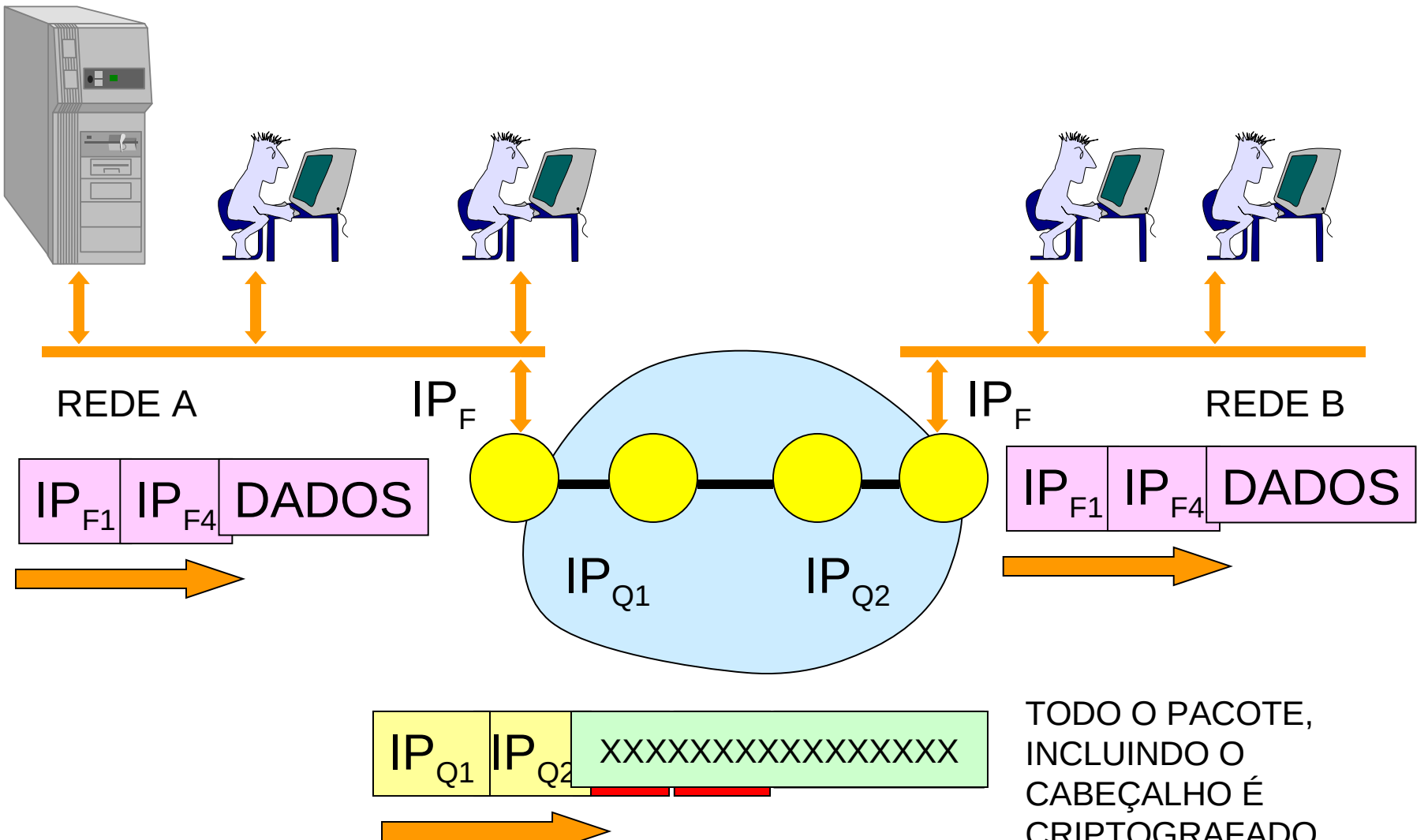
- Tecnologia de Tunelamento
- Criptografia baseada em chaves

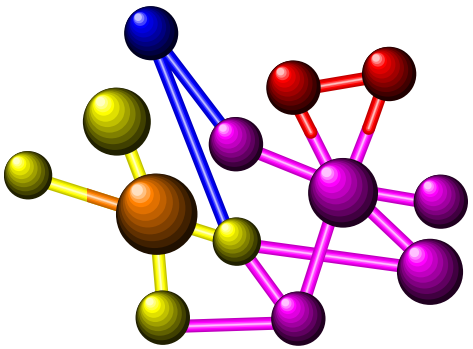
TUNELAMENTO

- Tunelamento é o princípio de colocar uma estrutura de informação dentro da outra.
- Por exemplo, o tunelamento nível 3 consiste em colocar um pacote dento do outro.



Exemplo


REDE A
IP F
IP F
REDE B
IP F1 IP F4 DADOS
IP Q1
IP Q2
IP F1 IP F4 DADOS
IP Q1 IP Q2 XXXXXXXXXXXXXXX
TODO O PACOTE, INCLUINDO O CABEÇALHO É CRIPTOGRAFADO.



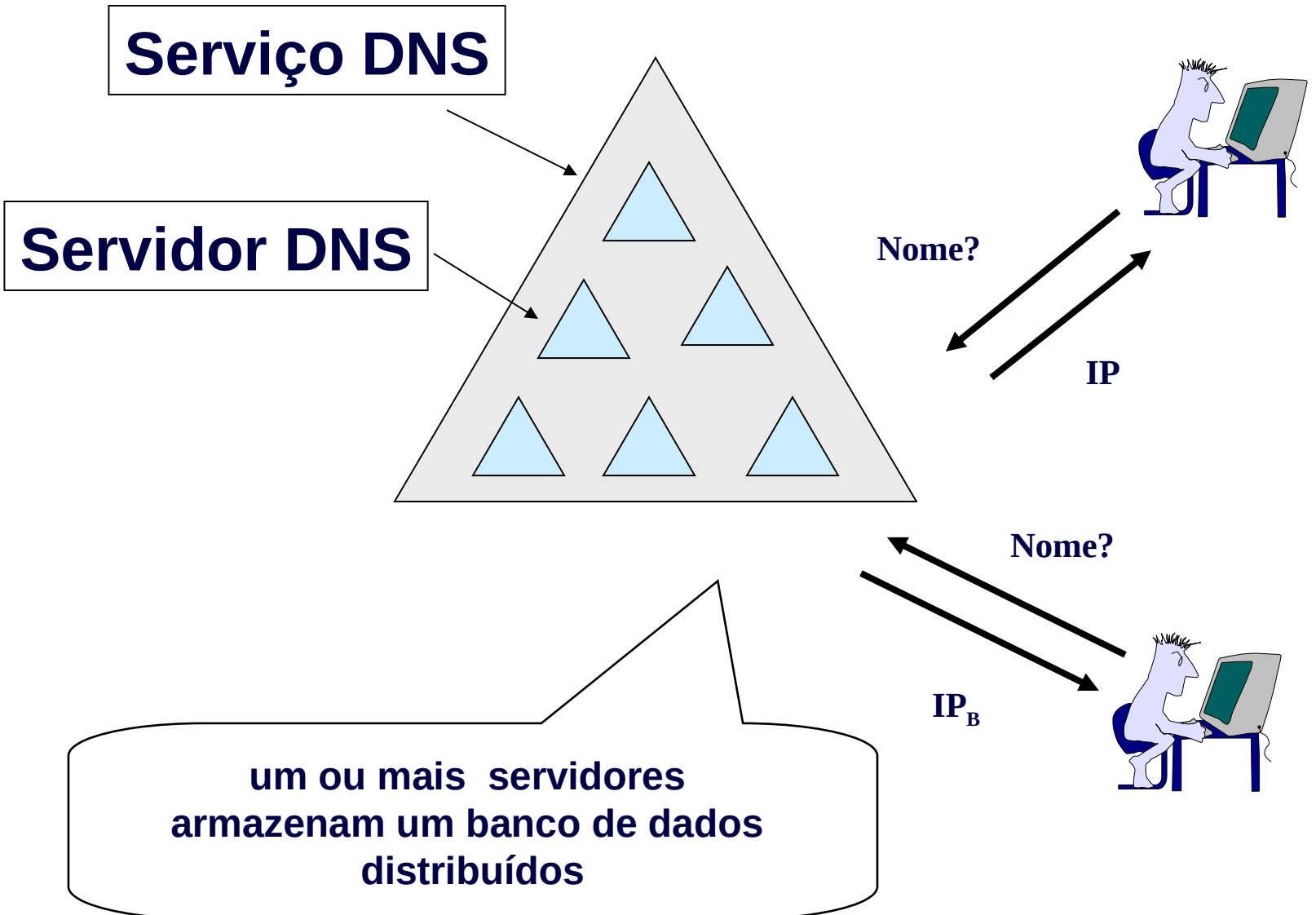
A) DNS

Redes TCP/IP

DNS - Domain Name Service

- Padrão Aberto para Resolução de Nomes Hierárquicos
  - Agrupa nomes em domínios.
  - A árvore de nomes é armazenada num **banco de dados distribuído**.
- Especificações do DNS
  - RFCs 1033, 1034, 1034, 1101, 1123, 1183 e 1536.
    - Expecificações da Internet Task Force

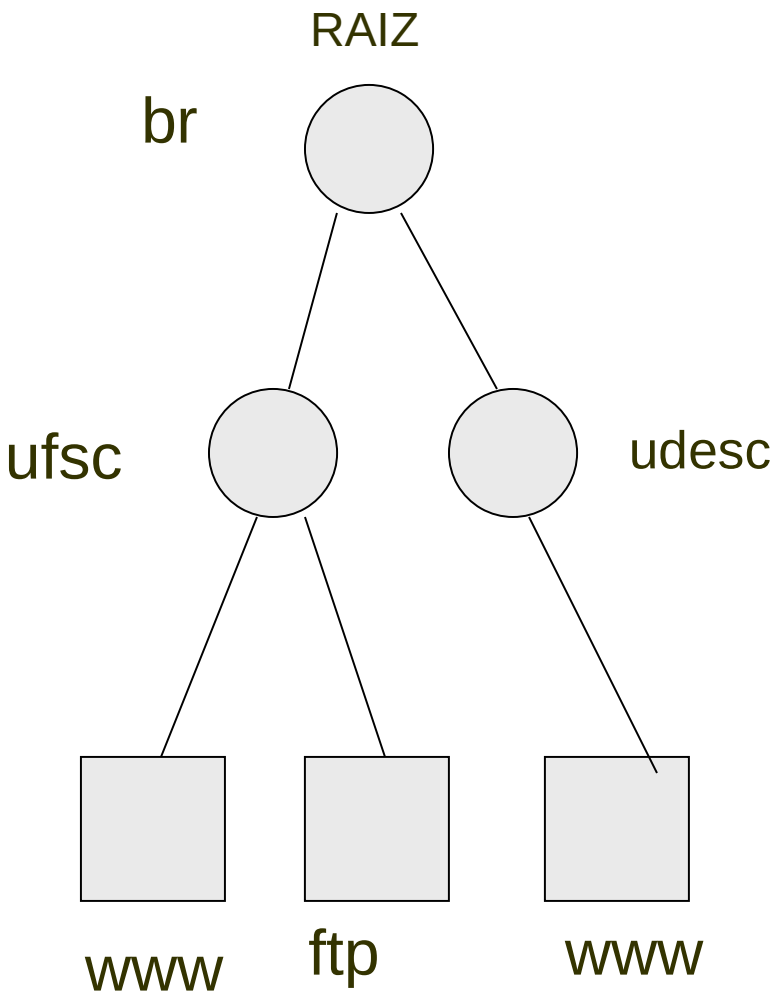
Serviço DNS

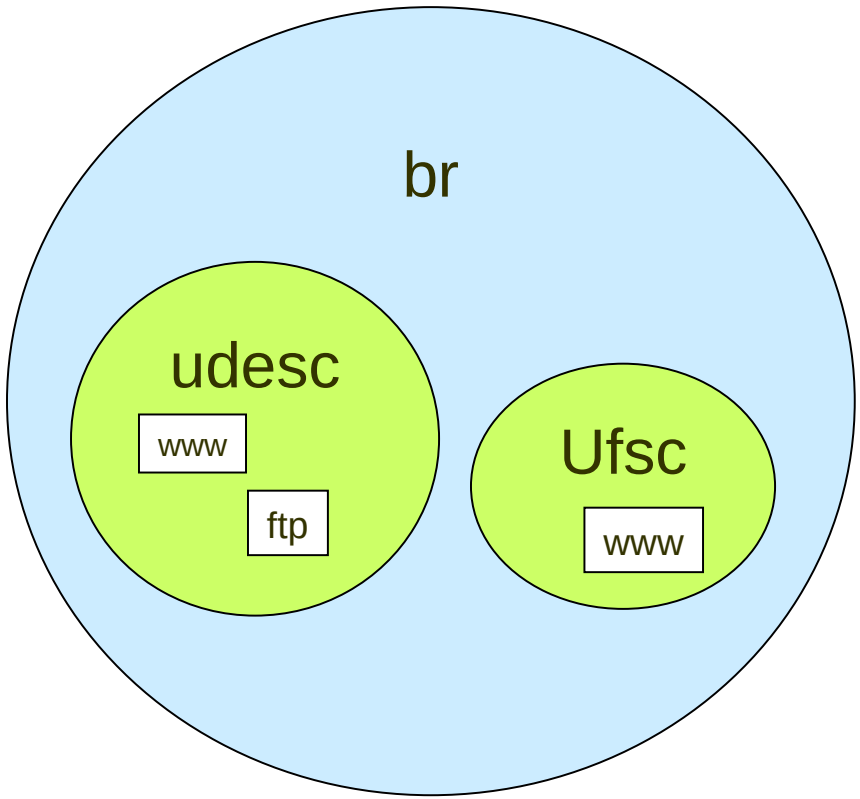

Serviço DNS
Servidor DNS
Nome?
IP
Nome?
IP$_B$
um ou mais servidores
armazenam um banco de dados
distribuídos

Nome de Domínio

- Os nomes Hierárquicos utilizados pelo DNS são chamados FQDN:
  - Fully Qualified Domain Name
- Exemplo:
  - www.unesc.net
  - www: nome do host
  - unesc: nome de domínio
  - net: nome de domínio
- Nome de domínio:
  - Coleção de HOSTS ou de outros domínios.

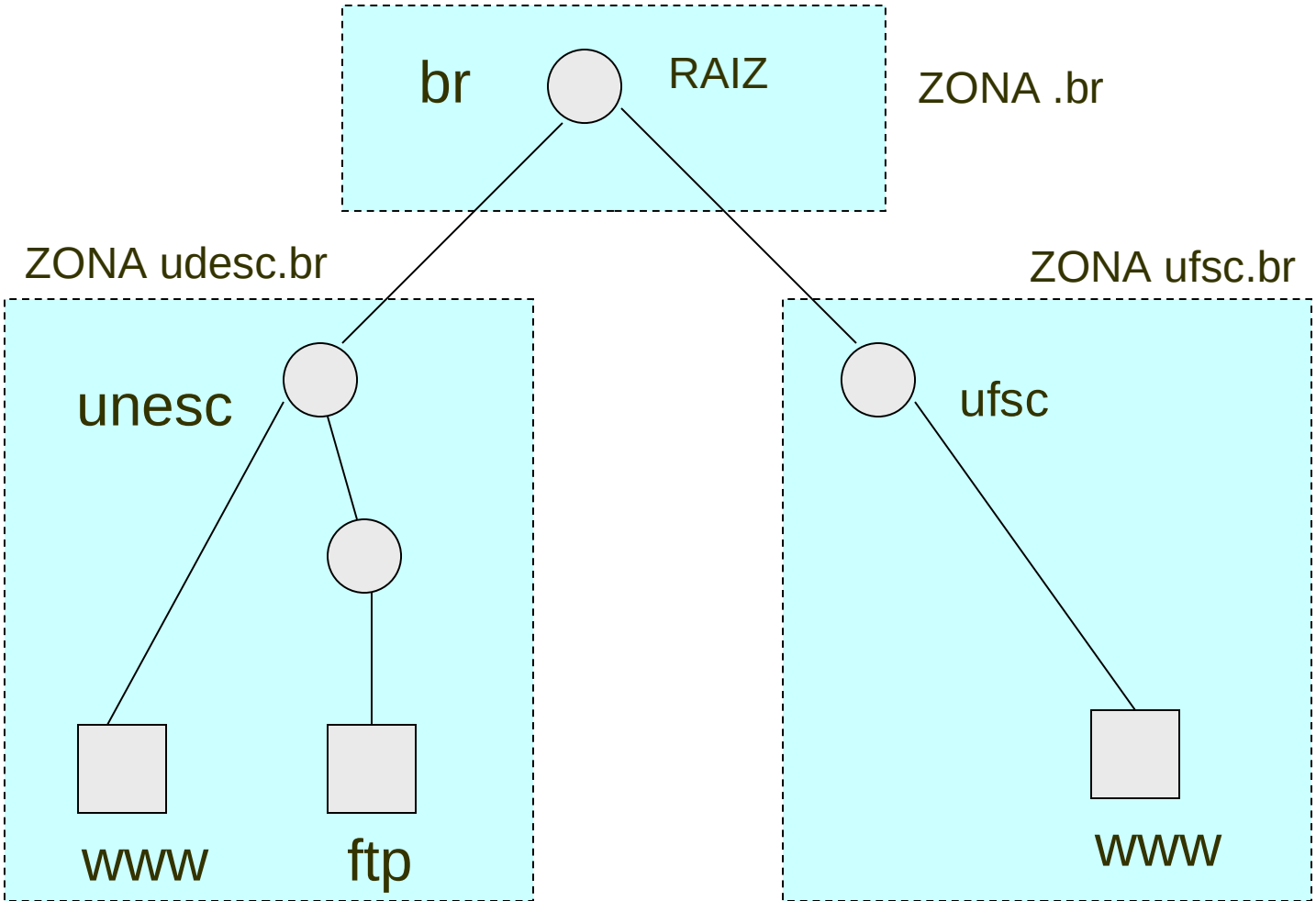
Árvore de nomes





Banco de Dados Distribuídos

- No serviço DNS, os nomes estão armazenados em ZONAS. Zonas são arquivos textos que contém os nomes de um ou mais domínios.



Tipos de Registros no DNS

- **A:** Host Adress
  - associa um nome a um endereço IP: **nome ⇒ IP.**
- **PTR:** Point Resource Record
  - associa um endereço IP a um nome: **IP ⇒ nome.**
- **NS:** Name Server
  - identifica o servidor DNS no domínio.
- **SOA:** Start of Authority
  - indica que o servidor de DNS é a autoridade para fornecer informações no domínio (**authoritative**).

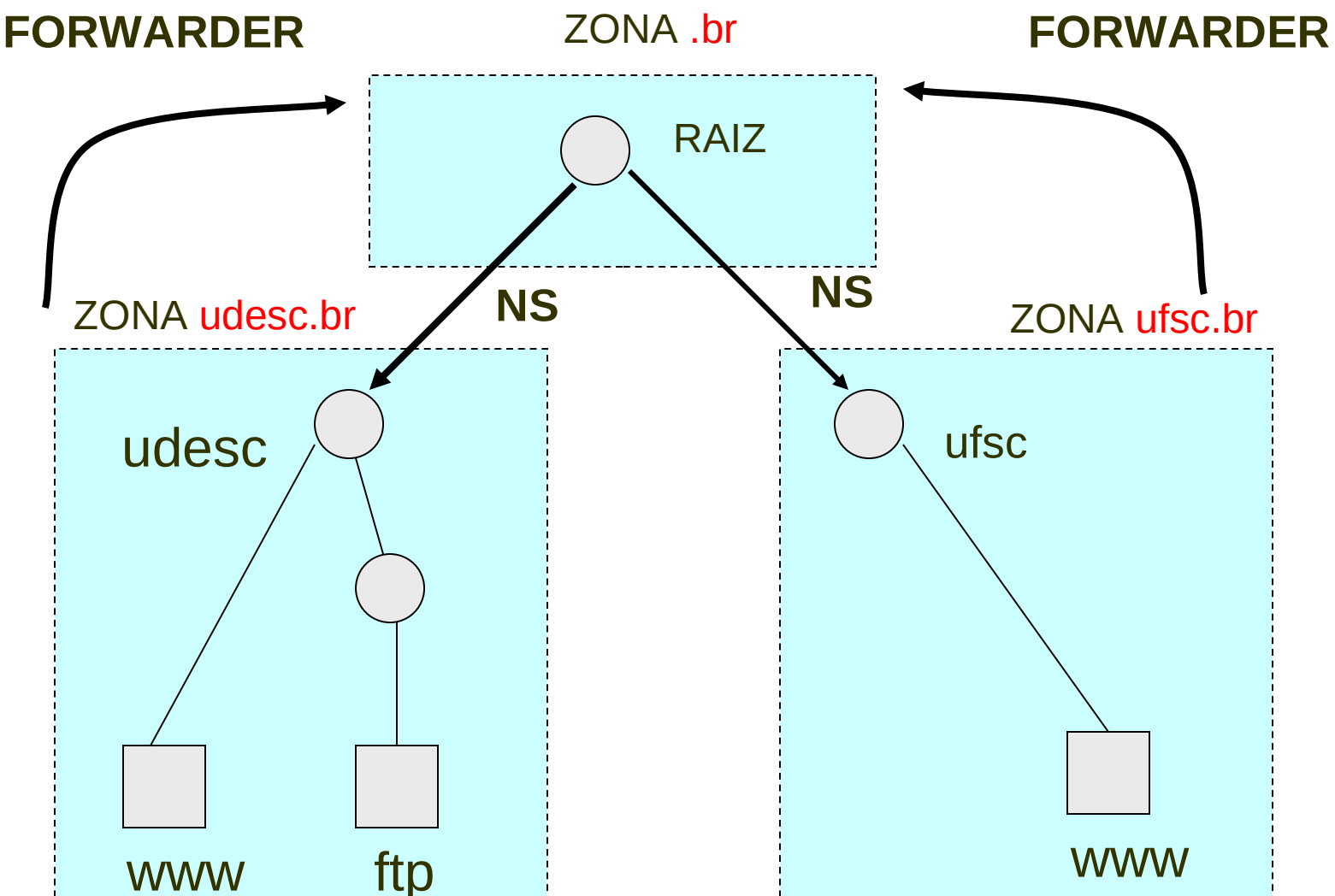
Consulta Reversa

- O cliente fornece um número IP e requisita o nome correspondente.
- Os registros que relacionam IPs aos nomes são do tipo PTR.
  - Por exemplo, um registro para o endereço IP 10.17.98.31 corresponde a uma entrada DNS no seguinte formato:
    - 31.98.17.10.in-addr.arpa
- Se o endereço IP não estiver contido no domínio local (aquele controlado pelo servidor DNS consultado), o servidor DNS contata o servidor DNS situado num nó superior da árvore.
  - Este mecanismo de procura seqüencial consultando os nós superiores é chamado “walking the tree”.

Forwarder

- Cada servidor DNS possui um arquivo de configuração que diz:
  - Lista de zonas que ele armazena
  - Lista de servidores forwarders
- Lista de zonas
  - Indica a localização física do arquivo correpondente a cada ZONA.
- Lista de forwarders
  - Um forwarder é um servidor DNS hierarquicamente superior ao servidor corrente.
  - Esse servidor recebe as consultas de domínios não armazenados pelo servidor DNS.

Ponteiros NS e Forwarders



Consulta Recursiva

- Graças ao ponteiros NS e FORWARDER qualquer servidor DNS pode responder por toda a árvore de nomínios.
- A resposta pode ser:
  - O mapeamento nome-IP requisitado
  - Uma mensagem de erro dizendo que o domínio ou host não foi encontrado.

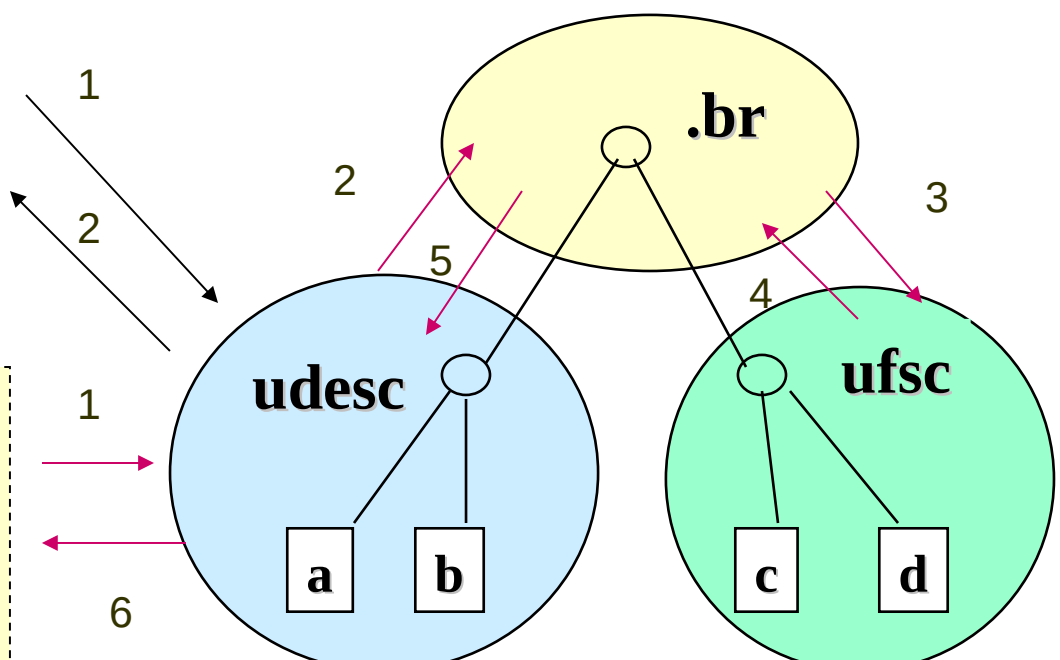
RESPOSTA AUTORITÁRIA

a.udesc.br?

IP = 10.17.98.31

d.ufsc.br?

IP = 200.17.98.174



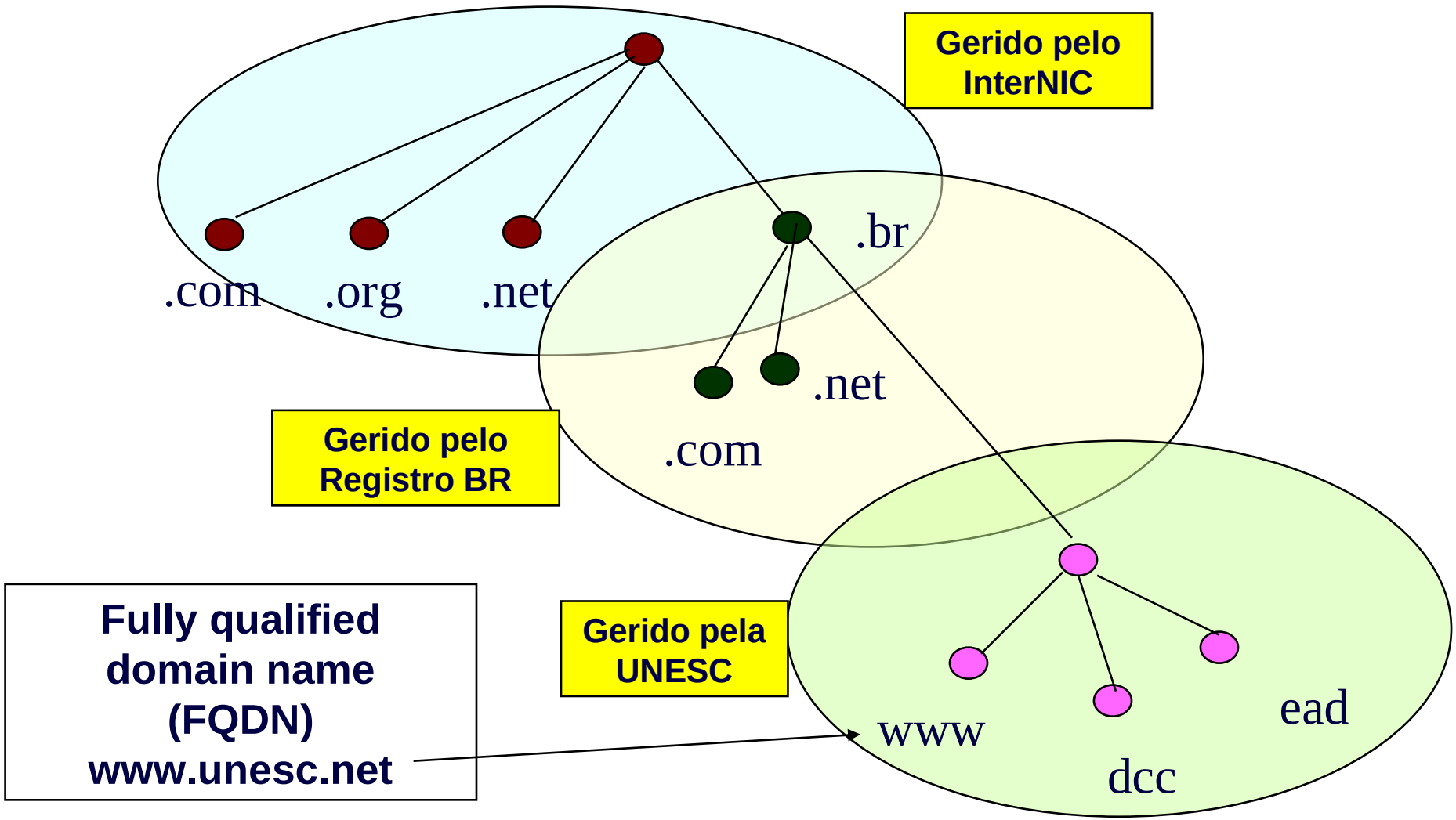
DNS e a Internet

- O “root” da árvore de nomes da Internet é gerenciado pelo Internet Network Information Center (InterNIC)
- InterNIC é o nome dado a um projeto criado num acordo entre a National Science Foundation (NSF) e a Network Solutions, Inc.
  - Provê um serviço de registro de nomes para os domínios .com, .net, .org, .edu...;
  - http://www.internic.net
- O InterNIC delega a responsabilidade de administrar partes do domínio de nomes para as empresas e organizações conectadas na Internet.

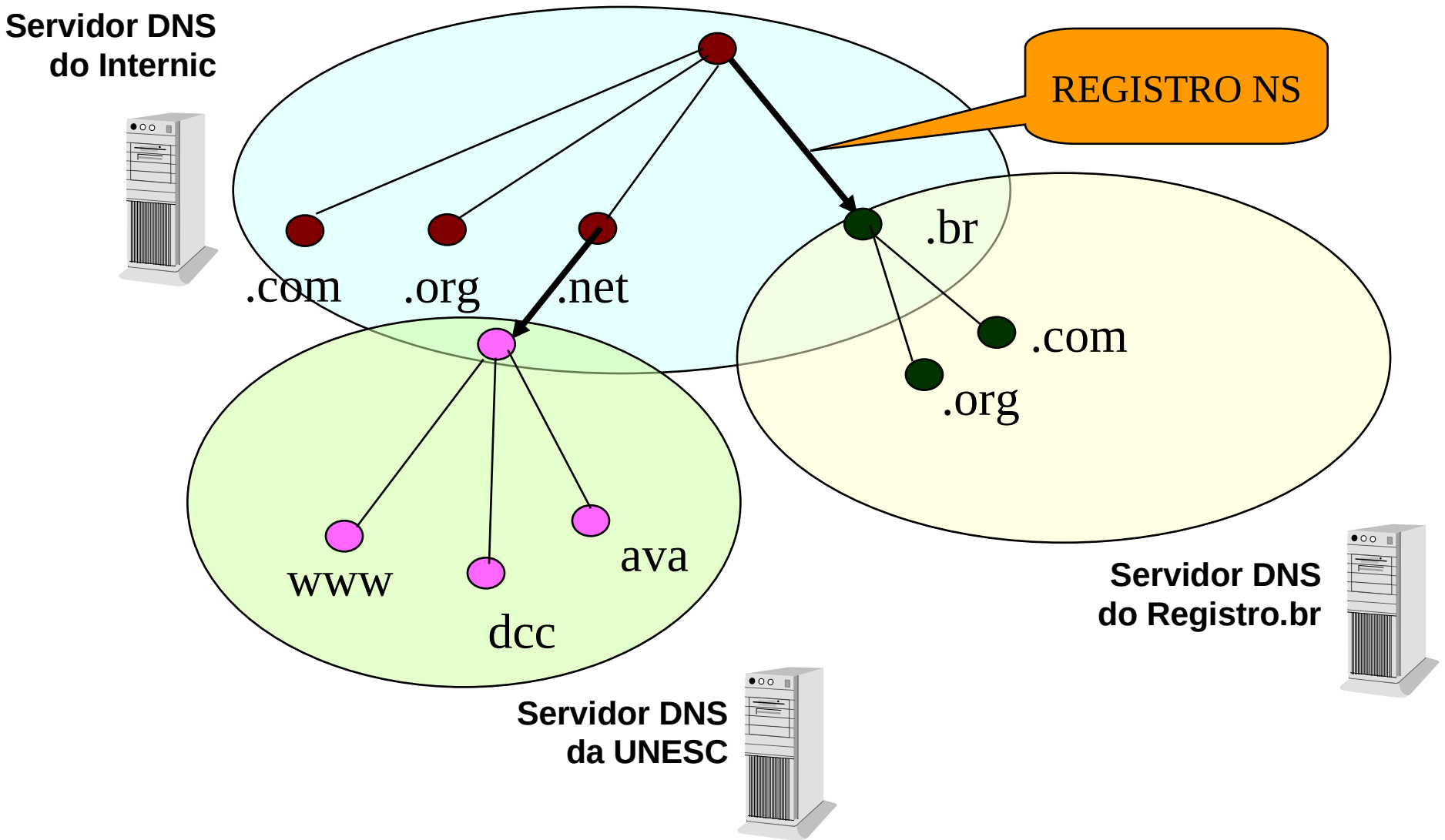
Domínios Gerenciados pelo InterNIC

- Segundo a nomenclatura adotada na Internet, o "*Domain Name Space*" é dividido em três áreas principais:
  - Organization Domains:
    - 3 caracteres para indicar a atividade da empresa.
      - .com, .edu, .gov, .int, .mil, .net, .org
      - .int: organizações internacionais
      - .mil: organizações militares
      - .org: organizações não comerciais
  - Geographical Domains:
    - 2 caracteres para identificar o país.
      - .br, .fr, .jp, etc.
  - Reverse domain:
    - domínio especial utilizado para associar endereços IP aos nomes.

Exemplo


Gerido pelo InterNIC
.com
.org
.net
.br
.net
.com
Gerido pelo Registro BR
Gerido pela UNESC
www
dcc
ead
Fully qualified domain name (FQDN)
www.unesc.net

Zonas

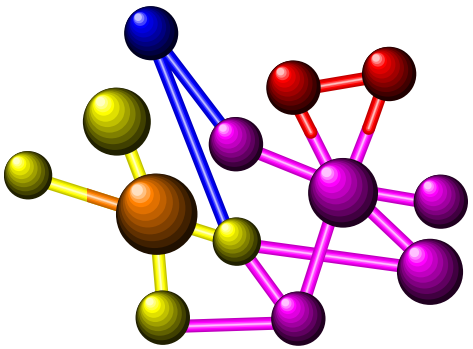

Servidor DNS
do Internic
REGISTRO NS
.com
.org
.net
.br
.com
.org
www
dcc
ava
Servidor DNS
do Registro.br
Servidor DNS
da UNESC

Tipos de Servidores

- **Primário**
  - É o servidor autoritário para zona. A inclusão, alterações ou exclusão dos registros da zona são feitas através deste servidor.
  - O servidor primário envia uma cópia dos seus arquivos de dados para o servidor secundário através de um processo denominado **“zone transfer”**
- **Secundário**
  - Funciona como backup. Apenas lê os arquivos de dados do servidor primário, e responde as requisições dos clientes quando requisitado.
- **Caching-Only**
  - São servidores DNS que apenas efetuam consultas e guardam o resultado numa cache e retornam os resultados.
  - Um servidor DNS realiza consulta a outros servidores sempre que tiver que localizar um nome externo as zonas que controla.

DNS - Resumo

- **Vantagens:**
  - Implementa um mecanismo de nomes hierárquico.
    - Isto facilita a organização dos nomes em redes de grande porte.
  - O banco de dados que armazena os nomes é distribuído.
    - Cada servidor DNS contém informações de zonas específicas, e pode ser administrado separadamente.
  - É o mecanismo de nomes adotado na Internet.
    - Pode ser utilizado para resolver nomes na rede local (intranet) e na rede Internet.
- **Desvantagem:**
  - Não é dinâmico.
    - É responsabilidade do administrador manter as entradas do arquivo de nomes atualizada.



C) DHCP

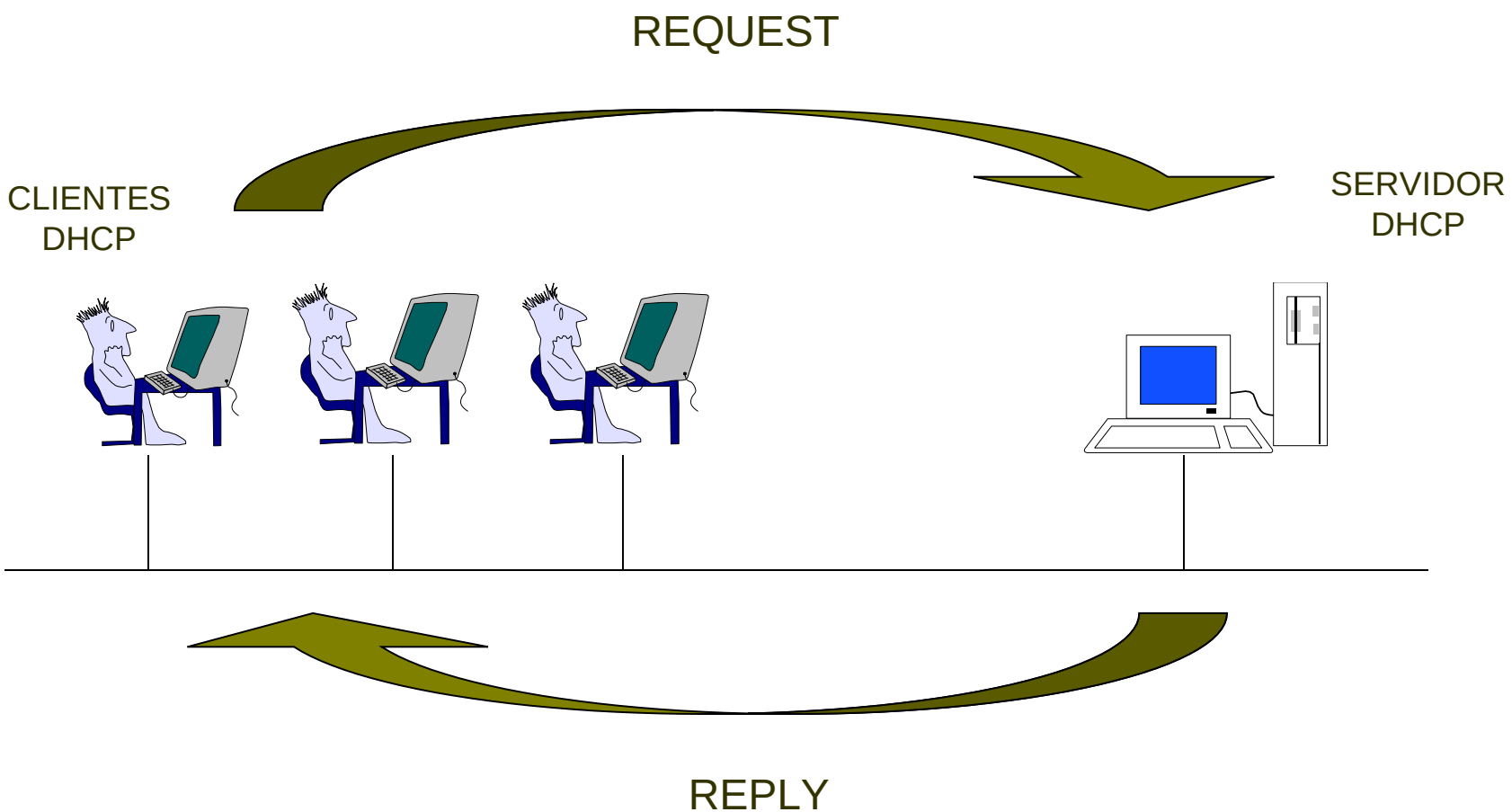
Redes TCP/IP

DHCP

- Dynamic Host Configuration Protocol
  - Padrão Industrial Aberto
    - IETF RFC 1533, 1534, 1541 e 1542.
      - IETF: Internet Engineering Task Force
      - RFC: Request for Comments
  - Utilizado para centralizar a administração e configuração de parâmetros TCP/IP numa rede.
  - Elimina a necessidade de configurar manualmente os clientes numa rede TCP/IP.

DHCP - Arquitetura Cliente-Servidor

- Um computador da rede deve funcionar como servidor DHCP.



Administração de Endereços IP

- Cada computador numa rede TCP/IP deve ter um endereço IP único.
  - O endereço IP identifica a estação e a rede ao qual a estação pertence.
  - Quando o computador é movido para outra rede, seu endereço IP deve refletir esta mudança.
- DHCP especifica os seguintes serviços (RFC 1541):
  - um protocolo para que o servidor DHCP e seus clientes se comuniquem.
    - PROTOCOLO BOOTP
  - Um método para configura os parâmetros de rede de um host IP:
    - IP, máscara, gateway default, servidores de nomes, etc.

ESCOPO DHCP

- Quando se utiliza DHCP, cada rede local é caracterizada por um ESCOPO:

PARTE FIXA

MASCARA
GATEWAY
SERVIDOR DE NOMES
OUTRAS ROTAS
PERÍODO DE EMPRÉSTIMO

MESMO VALOR
PARA TODOS OS HOSTS
DO ESCOPO

PARTE DINÂMICA

RANGE DE IP'S

UM VALOR DIFERENTE
PARA CADA HOST DO
ESCOPO

Processo de Atribuição

ESCOPO

255.255.255.0 200.17.98.23 72 horas
200.17.98.1 ... 200.17.98.254

Cliente DHCP

Dhcpdiscover

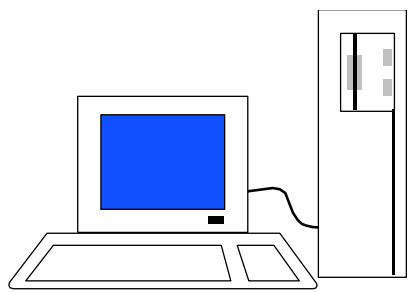
Dhcpoffer 200.17.98.1

Dhcprequest 200.17.98.1

Dhcpack 200.17.98.1

...

Dhcprelease 200.17.98.1



Servidor DHCP

Todas as mensagens são enviadas em broadcast

Processo de Atribuição

- **1) O cliente envia a mensagem Dhcpdiscover em broadcast.**
  - O endereço IP de origem do pacote é 0.0.0.0 pois o cliente ainda não tem um endereço IP.
- **2) Quando o servidor recebe o pacote, ele seleciona um endereço IP disponível na sua lista e oferece ao cliente.**
  - O servidor responde ao cliente com a mensagem **Dhcpoffer**
- **3) Quando o cliente recebe a oferta ele pode:**
  - aceitar enviando a mensagem **Dhcprequest** (incluindo o IP) em broadcast
  - recusar enviando a mensagem **Dhcpdecline** em broadcast
- **4) Quando o servidor recebe o Dhcprequest ele pode:**
  - confirmar para o cliente com a mensagem **Dhcpack**
  - recusar, se o endereço foi usado por outro, com a mensagem **Dhcpnack**
- **5) O cliente pode liberar um endereço com a mensagem Dhcprelease.**

Observações

- 1) O cliente aceita a primeira oferta que receber.
  - Se houver mais de um servidor DHCP distribuindo endereços IP, não haverá como selecionar apenas um deles.
- 2) O direito do cliente de usar o endereço IP recebido pelo servidor DHCP é temporário.
  - Quando o prazo de validade do IP expira, o servidor pode atribuí-lo a outra estação na rede.
  - O cliente pode liberá-lo antecipadamente com a mensagem **Dhcprelease**

Observações

- 3) Se o cliente não receber a oferta do servidor:
  - Ele repete o pedido em intervalos de 2, 4, 8, 16 segundos.
  - Se as 4 tentativas fracassarem, ele tenta novamente em intervalos de 5 minutos.
- 4) Quando o cliente é reinicializado, ele tenta utilizar o mesmo IP que tinha anteriormente.
  - Ele envia o pacote **Dhcprequest** com o endereço IP antigo ao invés do **Dhcpdiscover**.
  - Se o pedido é negado, então o cliente envia um **Dhcpdiscover**.

Considerações sobre o Planejamento da Implementação do DHCP

- Para redes não segmentadas:
  - Um único servidor DHCP pode atender até 10000 clientes (estimativa).
- Para redes segmentadas:
  - Se os roteadores são compatíveis com a RFC1542
    - Um único servidor DHCP é suficiente.
  - Se os roteadores não são compatíveis com a RFC1542
    - Deve-se utilizar um servidor DHCP para cada rede.
- Computadores que se ligam temporariamente na rede (notebooks, por exemplo) devem receber IPs com tempo de “leasing” curto.