



Revisão

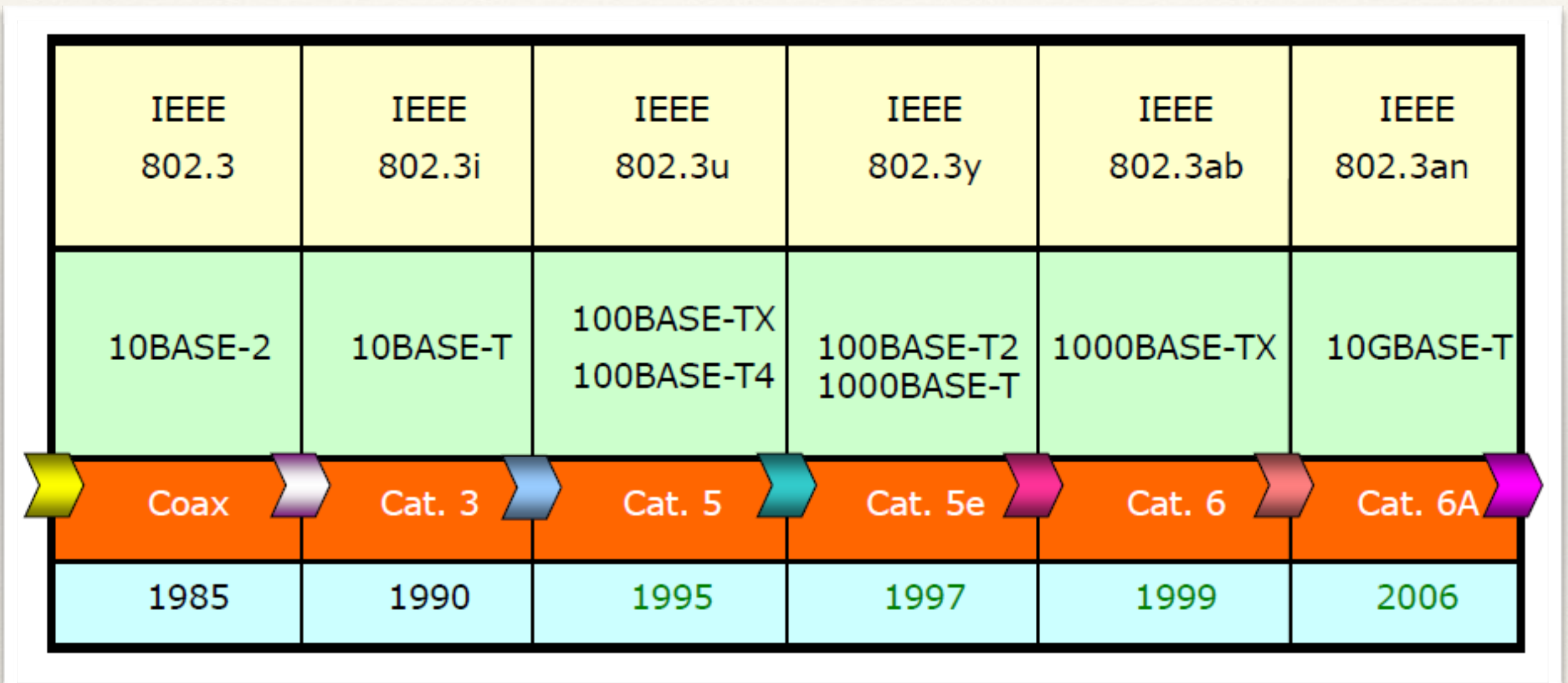
Professor
Wagner Gadêa Lorenz
wagnerlorenz@gmail.com

Disciplina: Redes de Computadores II
Curso de Sistemas de Informação

Categorias e classes de desempenho

Categoria de desempenho	Classe de aplicação	Frequência (largura de banda)	
Categoria 3	Classe C	16 MHz	10BASE-T (Ethernet
Categoria 5e	Classe D	100 MHz	10BASE-T e 100BASE-Tx (FastEthernet)
Categoria 6	Classe E	250MHz	1000BASE-T (Gigabit Ethernet)
Categoria 6A	Classe E Aumentada	500 MHz	
Categoria 7	Classe F	600 MHz	
Categoria 7A	Classe F Aumentada		

Cabos Metálicos - Evolução dos protocolos de transmissão



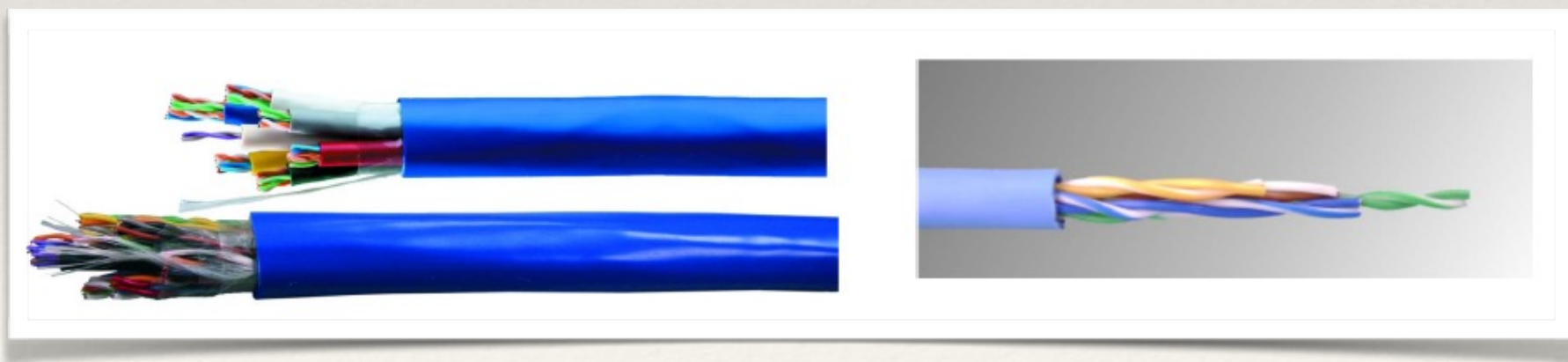
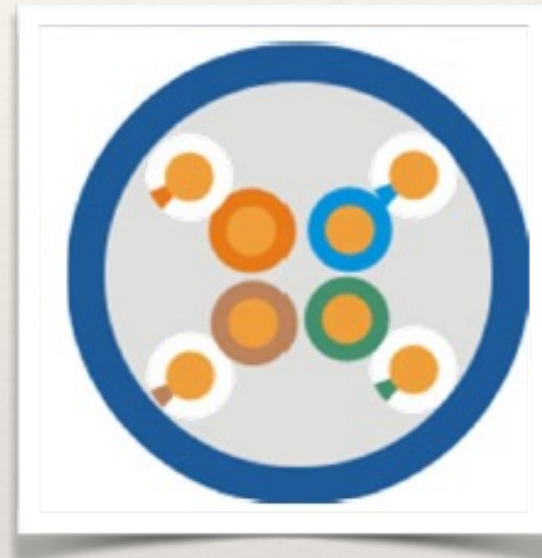
PARA VELOCIDADES DE 40GBPS E 100GBPS DEVE-SE USAR REDES ÓPTICAS COM FIBRA MMF OM3 E OM4.

Categoria 5e

Até 100 Mbps (Fast-ethernet)

Até 1 Gbps (Gigabit ethernet)

Até 100 MHz



Serviços de Rede - DNS e DHCP

Pessoal normalmente usam nomes para identificar umas as outras, porém computadores ligados em redes IP, como a Internet, usam endereços IP para identificar outras máquinas. No entanto, isso seria impossível se as pessoas tivessem que decorar os endereços IP dos sites. Seria inviável digitar endereços como `http://187.60.192.5` ao invés de `http://www.ulbra.edu.br`

Para facilitar o uso da internet é possível associar nomes, como `http://www.ulbra.edu.br`, aos endereços IP, para que as pessoas consigam decorar os endereços mais facilmente.

Serviços de Rede - DNS e DHCP

Para que isso seja possível, deve existir uma infraestrutura que traduz os nomes fictícios para os endereços reais das máquinas, o responsável por este serviço é o DNS (Domain Name System - Sistema de Nomes de Domínios).

Serviços de Rede - DNS

O DNS é dito descentralizado porque não está armazenado em uma única máquina, mas sim, em vários servidores espalhados pelo mundo. Os principais motivos para não centralizar o DNS são:

- **Ponto único de falha:** caso a tabela com todos os nomes e IPs estivessem armazenados em uma única máquina e essa máquina falhasse, toda a internet estaria comprometida.
- **Volume de tráfego:** se todas as traduções de nomes para IPs fossem realizadas em apenas uma máquina, o volume de tráfego e processamento seria tão grande que inviabilizaria o serviço.
- **Distância da base de dados:** caso toda a base de dados estivesse armazenada no Japão, nós, brasileiros, teríamos um serviço muito lento, pois teríamos que esperar um pacote ir e voltar de lá.
- **Manutenibilidade:** além disso, a máquina que hospedasse esse serviço não poderia sofrer atualizações e manutenção sem prejudicar toda a internet.

Serviços de Rede - DNS

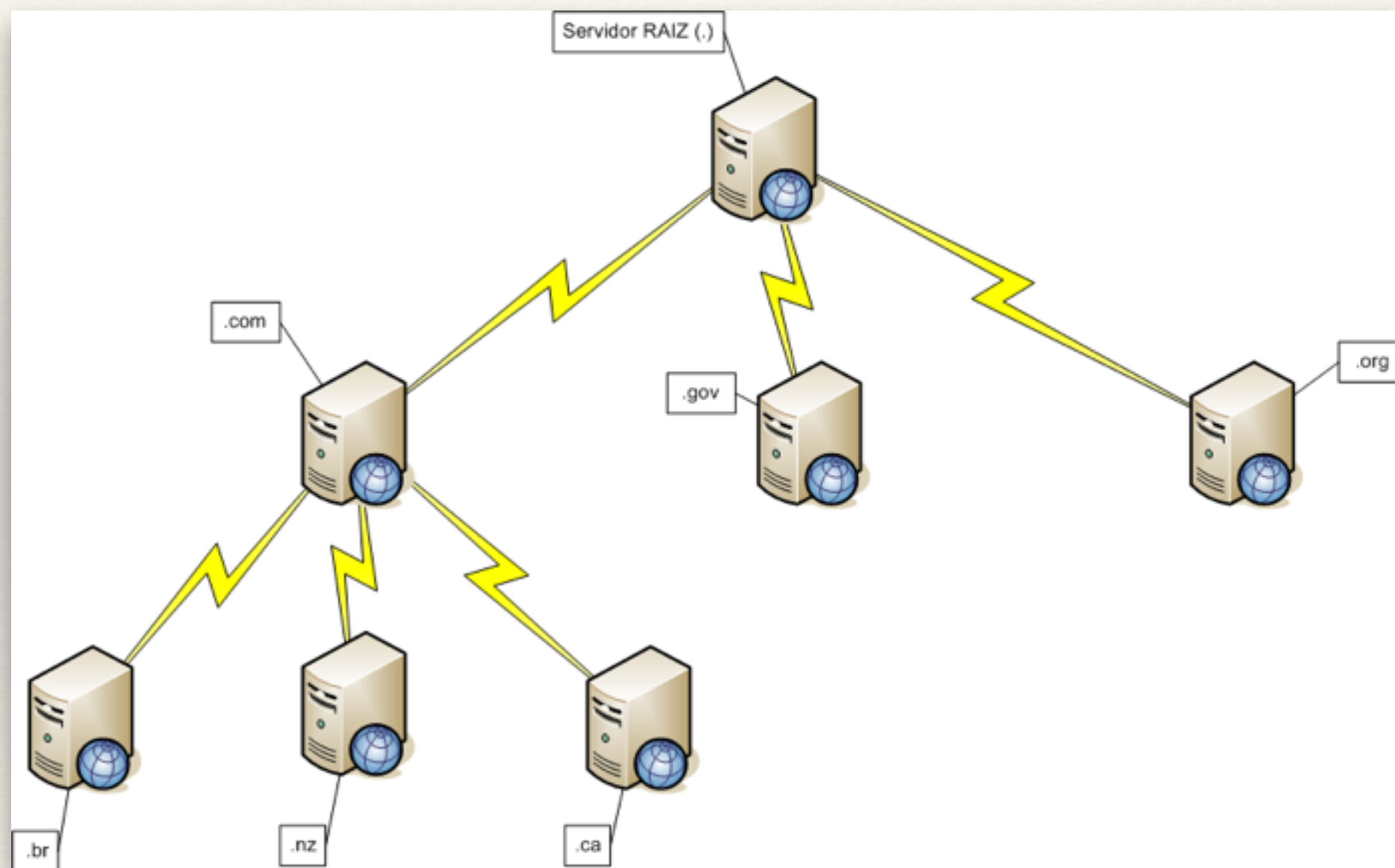
O DNS também é distribuído, não existe uma máquina que possua a tabela completa de todos os endereços e IPs da Internet, mas sim, várias máquinas cada uma com uma parte dessa tabela. Há dados replicados em máquinas diferentes, porém nenhuma possui a tabela completa.

A distribuição do DNS oferece vantagens como:

- Caso algum servidor pare de funcionar, apenas parte do DNS será comprometida.
- Além disso, como alguns dados estão duplicados, caso algum servidor pare de funcionar pode ser que alguns recursos ainda estejam acessíveis por nomes.

Serviços de Rede - DNS

Árvore de domínios do DNS:



<http://throberth.blogspot.com.br/2008/09/noes-de-dns.html>

Serviços de Rede - DNS

Construído dessa forma, o DNS pode ser gerenciado por organizações diferentes, por exemplo, todos os domínios que terminam em [.com.br](https://registro.br) são gerenciados pelo registro.br que é mantido pelo Comitê Gestor da Internet no Brasil.

Os principais serviços oferecidos pelo DNS são de três tipos: resolução de nomes, distribuição de carga e cache. A resolução de nomes pode ocorrer de duas formas:

- quando um cliente local, ou seja, de dentro do seu domínio, pergunta sobre um endereço externo ao seu domínio;
- quando um cliente externo ao seu domínio pergunta sobre endereços internos ao seu domínio local.

Serviços de Rede - DHCP

O serviço **DHCP** (Dynamic Host Configuration Protocol - Protocolo de Configuração Dinâmica de Hosts) serve para buscar configurações de rede, como IP, máscara, gateway e servidor DNS para um host, de forma que não seja necessária a configuração manual de cada um dos hosts de uma rede. Esse serviço é muito usado em redes de grande porte e é indispensável.

Serviços de Rede - DHCP

O funcionamento do DHCP é simples e inteligente. Um cliente DHCP não precisa nem saber o IP do servidor DHCP, pois manda uma mensagem DHCP em **broadcast** para a rede usando IP **255.255.255.255**, dessa forma todos os computadores irão receber essa requisição, inclusive o servidor DHCP.

Então o servidor DHCP responde a requisição para o endereço **0.0.0.0**, pois o cliente ainda não possui um IP válido na rede. Essa mensagem também será recebida por todos os computadores da rede, porém a mensagem é endereçada ao endereço MAC do cliente que fez a requisição, assim, os outros computadores irão ignorar a mensagem.

Serviços de Rede - DHCP

Nessa mensagem enviada pelo servidor DHCP estão especificadas algumas informações que serão usadas pelo cliente para configurar sua rede. Entre as informações estão: endereço de IP válido para a rede; máscara de subrede; gateway da rede e servidores DNS da rede.

Serviços de Rede - DHCP

Servidores DHCP podem atribuir endereços de rede de três formas:

- **Configuração Manual:** nesse modo, o servidor DHCP associa um IP a um determinado equipamento de rede, dessa forma, apenas esse equipamento irá receber um certo endereço e possuirá um endereço fixo (será sempre o mesmo endereço).
- **Configuração Automática:** nesse modo, quando um equipamento de rede requisitar um endereço, ele receberá um que não necessariamente será fixo, ou seja, poderá variar. Esse endereço poderá ser usado por tempo indeterminado.
- **Configuração Dinâmica:** nessa forma de operação o servidor DHCP oferece um endereço para um equipamento de rede por um determinado tempo. Quando o tempo terminar, o equipamento que o solicitou precisa renovar o porte do endereço ou o servidor DHCP poderá realocar esse endereço para outro equipamento (economizando endereços e evitando que os endereços disponíveis acabem).

Protocolo ARP

O ***Address Resolution Protocol*** ou ARP é um protocolo utilizado para encontrar endereço da camada de enlace (Ethernet, por exemplo) a partir do endereço da camada de rede (como um endereço IP). O emissor difunde em broadcast um pacote ARP contendo o endereço IP de outro host e espera uma resposta como um endereço MAC respectivo.

Cada máquina mantém uma tabela de resolução em cache para reduzir a latência e carga na rede. O ARP permite que o endereço IP seja independente do endereço Ethernet, mas apenas funciona se todas as máquinas o suportarem.

Protocolo ARP

Como visto anteriormente os protocolos são organizados em camadas.

Aplicações	SMTP; Telnet, FTP, etc.			
Transporte	TCP		UDP	
Redes	IP	ICMP	ARP	RARP
Enlace	Ethernet, sem fio			

Endereçamento IP

O **IP** é um **protocolo**, da camada de rede, de entrega de pacote não confiável, de melhor esforço e sem conexão. Melhor esforço significa que os pacotes pelo IP podem ser perdidos, ficarem fora de ordem ou mesmo serem duplicados, mas o IP não se responsabilizará por essas situações, pois tratar dessas situações fica a cargo dos protocolos de camada mais alta (**transporte**).

Endereçamento IP

Para ser capaz de identificar um dispositivo na Internet, cada computador recebe uma atribuição de um endereço, o endereço IP, ou endereço da Internet. O endereço IP são números que identificam seu computador em uma rede (<endereço da rede><número do computador nessa rede>).

Inicialmente você pode imaginar o IP como um número de telefone. O IP é composto por quatro bytes e a convenção de escrita dos números é chamada de **notação decimal pontuada**. Por convenção, cada interface do computador ou roteador tem um endereço IP, também é permitido que o mesmo endereço IP seja usado em mais de uma interface de uma mesma máquina, mas normalmente cada interface tem seu próprio endereço IP.

Endereçamento IP

Considere o endereço IP **128.2.7.9**, internamente, esse número é convertido para um número binário onde:

128 = 10000000

2 = 00000010

7 = 00000111

9 = 00001001

Mas apenas esse número não nos indica muita coisa. Como o endereçamento IP indica o endereço da rede e o computador dentro dela, precisamos saber qual a sua máscara de rede (**netmask**) para identificar a rede, e, na sequência, o computador dentro dessa rede.

Endereçamento IP

A máscara da rede indica quantos bits serão utilizados para identificar a rede, o que sobrar será utilizado para identificar o computador (**host**) dentro dessa rede.

Considere a máscara de rede **255.255.0.0**, internamente, este número é convertido para um número binário onde:

255 = 11111111

255 = 11111111

0 = 00000000

0 = 00000000

Endereçamento IP

Considere o número IP **128.2.7.9**. Se dissermos que sua máscara de rede é **255.255.255.0**, estamos indicando que os três primeiros bytes (24 bits) será utilizados para identificar a rede e o último byte (8 bits) será utilizado para identificar o número do computador.

De forma análoga, considerando o número IP **128.2.7.9**, se dissermos que sua máscara de rede é **255.255.0.0**, estamos indicando então que os dois primeiros bytes (16 bits) serão utilizados para identificar a rede e os dois últimos bytes (16 bits) serão utilizados para identificar o número do computador. O endereço de rede é conhecido pela porção zero indicada na máscara.

Endereçamento IP

Um último exemplo, considerando o número IP **128.2.7.9**, se dissermos que sua máscara de rede é **255.255.192.0**, estamos indicando que 18 bits serão utilizados para identificar a rede e o restante para identificar o host, pois:

255 = 11111111
255 = 11111111
192 = 11000000
0 = 00000000

Endereçamento IP

No exemplo anterior, os bits em **vermelho** indicam o endereço de rede e os bits em **azul** o endereço do host, isso significa que uma rede com essa máscara de rede poderá ter aproximadamente 16 mil computadores na mesma rede.

Para se obter o número de computadores em uma rede, basta utilizar o cálculo 2^n (2 elevado a n), sendo que n o número de bits.

Nesse caso, $2^{14} = 16384$.

Endereçamento IP

Originalmente, o espaço do endereço IP foi dividido em poucas estruturas de tamanho fixo chamados de “classes de endereço”. As três principais são a classe A, classe B e classe C. Examinando os primeiros bits de um endereço, o software do IP consegue determinar rapidamente qual a classe e, logo, a estrutura do endereço.

Classe A: Primeiro bit é 0 (zero).

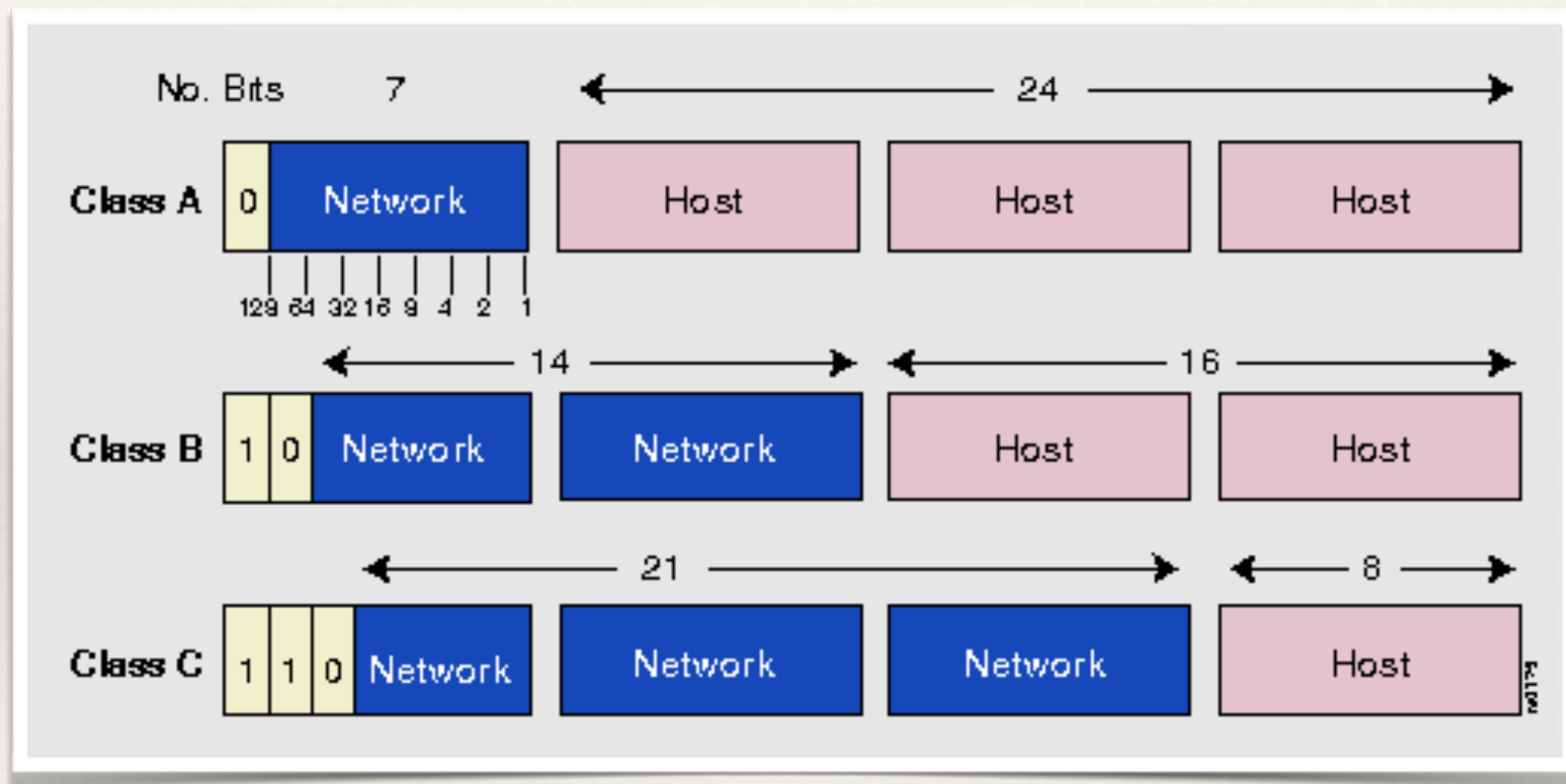
Classe B: Primeiros dois bits são 10 (um, zero).

Classe C: Primeiros três bits são 110 (um, um, zero).

Classe D: (endereço multicast): Primeiros quatro bits são 1110 (um, um, um, zero).

Classe E: (endereço especial reservado) Primeiros cinco bits são 11110 (um, um, um, um, zero).

Endereçamento IP



Endereçamento IP

Classe	Gama de Endereços	Nº de Endereços por Rede
A	1.0.0.0 até 127.255.255.255	16.777.216
B	128.0.0.0 até 191.255.255.255	65.536
C	192.168.0.0 até 255.255.255.255	256
D	224.0.0.0 até 239.255.255.255	Multicast
E	240.0.0.0 até 247.255.255.255	Uso futuro; atualmente reservada a testes pela IETF

Gateway

Em uma rede de computadores, o gateway ou “porta de entrada”, é um computador intermediário ou um dispositivo dedicado, responsável por fornecer determinados tipos de serviços.

Entre suas principais funcionalidades, podemos destacar a interligação de duas redes que possuem protocolos diferentes, compartilhamento da conexão de internet, roteadores, proxy, firewalls, etc.

Para configurá-lo como cliente, é necessário informar o endereço gateway do serviço nas propriedades de rede de seu sistema operacional.

Gateway

De acordo com Tanenbaum (2011), “o nome geral para uma máquina que faz uma conexão entre duas ou mais redes e oferece a conversão necessária, tanto em termos de hardware e software, é um gateway”.

Os gateways são distinguidos pela camada em que operam na hierarquia de protocolos.

Gateway

Quando estamos conectados à internet por meio de um roteador, ele é a porta de ligação com esse serviço.

Para que uma máquina tenha acesso a ele, é necessário configurar o endereço gateway do roteador no computador que terá acesso à internet.

Esse serviço pode ser configurado, automaticamente, ou manualmente.

Com esses procedimentos, estamos indicando a porta de entrada da internet.

Proxy

Ao acessar um computador em que a página da internet solicitada está bloqueada, normalmente, o proxy é o responsável por não permitir o acesso.

Então, o proxy bloqueia as páginas da internet? Também.

O servidor proxy possui várias funcionalidades e uma delas é bloquear as páginas da internet.

Proxy

O proxy funciona de forma intermediária entre o usuário e a internet.

Pode-se observar na Figura 1 a atuação do proxy desempenhando a conexão da estação de trabalho com a rede externa.

Ao solicitarmos um endereço web, o endereço da URL é enviado para o servidor proxy, que, por sua vez, filtra as informações que podem ser acessadas ou não.

Proxy

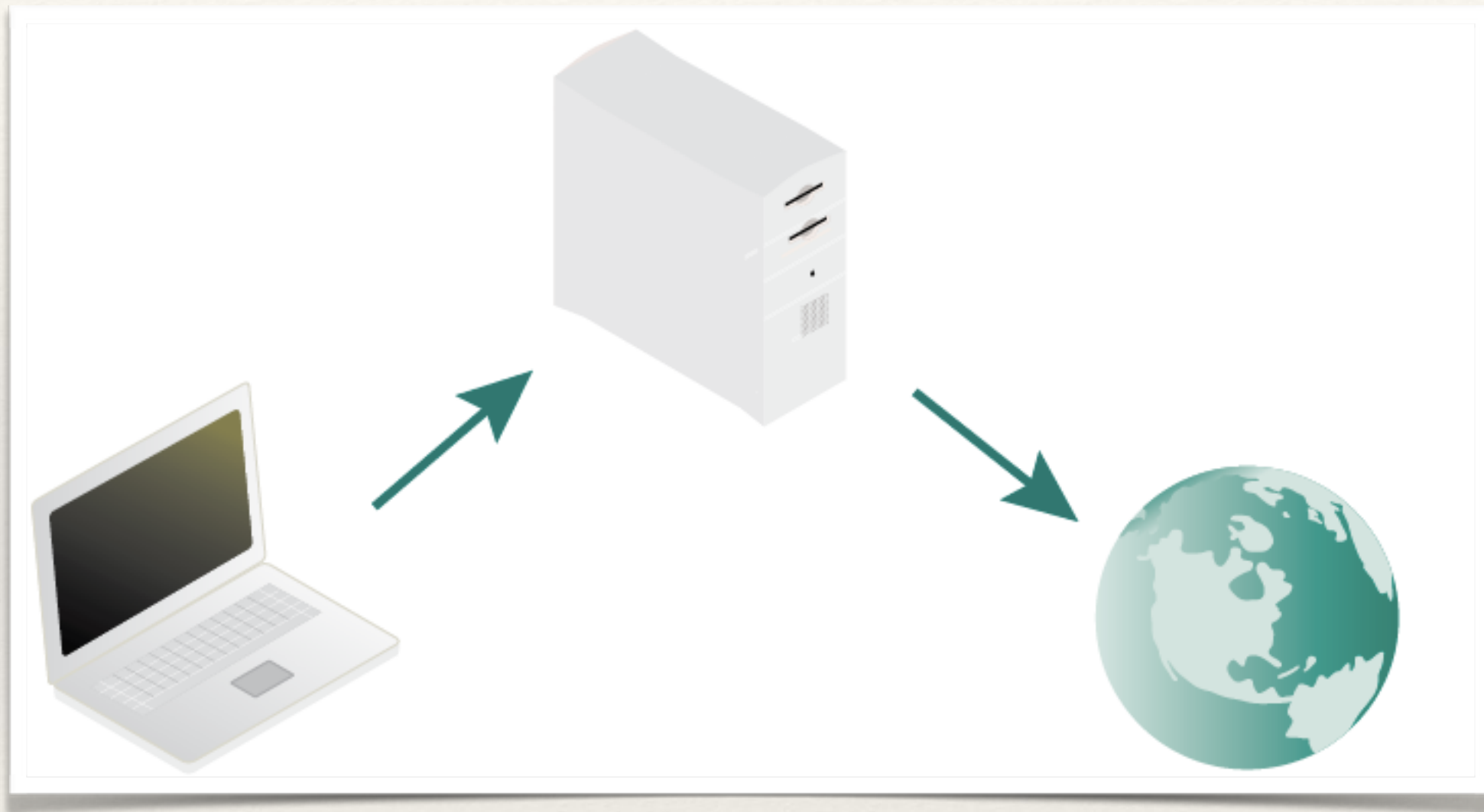


Figura 1. O Proxy atua entre o usuário e a internet

Proxy

Existem vários programas de proxy grátis no mercado, o administrador da rede é responsável por gerenciar o conteúdo que será acessado.

Muitas empresas do Brasil e do mundo bloqueiam sites como Facebook, Orkut e entre outros. Alguns especialistas dizem que os funcionários perdem muito tempo de trabalho diante de sites que os distraiam.

Outros dizem que o bom funcionário sabe a hora certa de navegar. Opiniões à parte, o profissional de TI é o responsável por detectar a necessidade de colocar o proxy dentro de uma empresa e viabilizar o seu correto funcionamento.

Proxy

Outra importante função do proxy é manter uma área de acesso rápido às informações já acessadas por outros usuários, evitando a retransmissão das mesmas informações pela rede.

Ao solicitar uma página como `www.ulbra.edu.br`, o servidor Proxy captura os dados da página web solicitada, guardando-os em um espaço em disco.

Se outro usuário da rede solicitar a mesma página, ela será apresentada em seu navegador de forma rápida, diminuindo o tempo de requisição ao servidor web.

Proxy

Ao solicitar uma página web em uma rede que possui o serviço de Proxy, o navegador fará primeiro uma procura do conteúdo em cache, isto é, na memória que foi utilizada para guardar as informações de acesso.

Caso não encontrar, o acesso será feito diretamente no site web solicitado.

Proxy

Dentre as várias funcionalidades do proxy, é importante ressaltar que a configuração do serviço varia muito de administrador para administrador de rede.

Um proxy bem configurado permite saber quais páginas da web o funcionário está acessando, e por quanto tempo.

Pode-se criar políticas que permitam aos funcionários acessarem páginas como Myspace, blog, etc., durante o horário de almoço.

Firewall

O firewall ou “Muro antichamas” é o serviço responsável por aplicar uma política de segurança nas informações que trafegam na rede.

Ele é responsável por bloquear qualquer tentativa de acesso ao seu computador sem autorização.

Pode-se observar na Figura 2 a demonstração do firewall atuando entre a rede e a internet.

Firewall

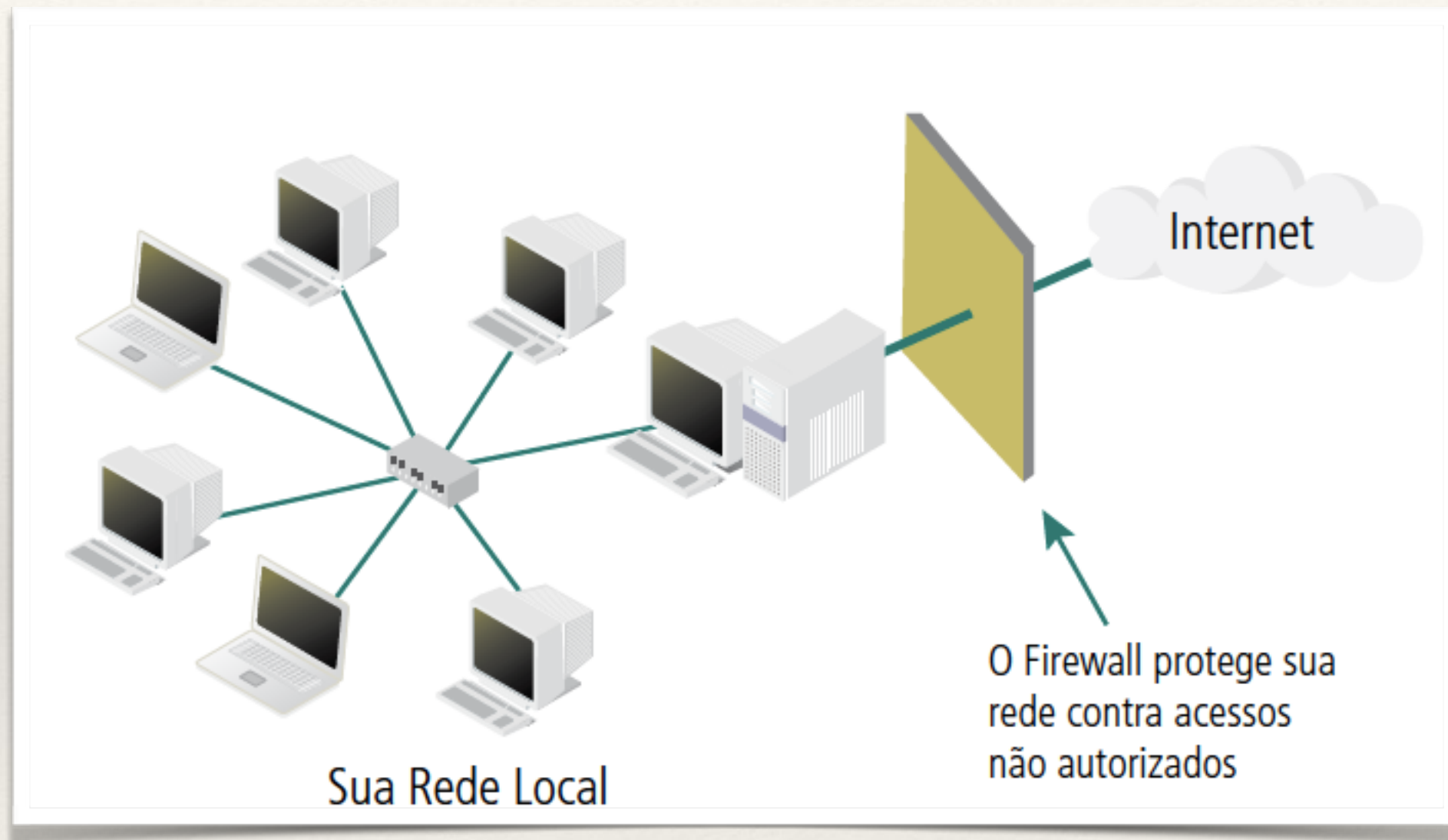


Figura 2. Firewall atuando entre a rede e a internet

Firewall

Assim como o proxy, um mesmo firewall pode ser configurado por maneiras diferentes, e a configuração depende do grau de conhecimento do administrador da rede.

Firewall

Através do firewall é possível bloquear portas de programas, IPs, etc.; com ele, o administrador da rede configura o que é permitido entrar através da internet.

Podemos perceber que, ao contrário do proxy, o **firewall bloqueia o que entra na rede pela internet.**

Já o proxy, bloqueia o que o usuário vai acessar na internet.

Uma empresa que possui esses dois serviços, tem um antivírus atualizado em suas máquinas, está menos sujeita a ataques de crackers, menos problemas relacionados a vírus e maior segurança nas informações que estão trafegando na rede.

Firewall

A importância do firewall fica evidente na afirmação de Comer (2006): uma organização que possui várias conexões externas precisa instalar um firewall em cada uma delas e precisa coordenar todos os firewalls. Deixar de restringir o acesso de forma idêntica em todos os firewalls pode deixar a organização vulnerável.

Resumo

Dentre diversos serviços fornecidos pelos servidores, podemos destacar que eles proporcionam ao administrador da rede: segurança, flexibilidade e principalmente autonomia.

O gateway é um computador intermediário ou um dispositivo dedicado, responsável por fornecer determinados tipos de serviços, como conectar à internet.

O protocolo DHCP é um serviço de rede que fornece as configurações TCP/IP aos computadores clientes da rede.

O serviço de proxy permite ao profissional de TI criar uma política de privacidade dentro de empresas, universidades, etc., bloqueando diversos acessos externos na internet. A outra função do proxy é fazer cache das páginas recentemente acessadas pelo usuário, permitindo abrir as páginas com maior velocidade.

A necessidade de instalação do serviço de firewalls em uma empresa cresce a cada dia. Esse serviço bem configurado permite controlar o que entra na rede, assim como prevenir contra ataque de crackers.

Dúvidas

- Conteúdo
 - Moodle
 - (<http://wagnerglorenz.com/moodle/>)
- Dúvidas
 - wagnerglorenz@gmail.com



Referências Bibliográficas

- Tanenbaum, A. S. Redes de Computadores, Tradução da 4ª Edição. Rio de Janeiro: Campus, 2003.
- Tanenbaum, A. S. Redes de Computadores, Tradução da 5ª Edição. Rio de Janeiro: Pearson, 2011. <http://ulbra.bv3.digitalpages.com.br/users/publications/9788576059240/pages/-18>
- Material Prof. Henrique Tamiosso Machado