

FUNDAMENTOS E INFRAESTRUTURA DE REDES DE COMPUTADORES



Prof. Me. Wallace Rodrigues de Santana



www.neutronica.com.br

Versão 2.0 Preliminar

© 2014 neutronica.com.br



Atribuição-NãoComercial-Compartilhalgual 3.0 Brasil (CC BY-NC-SA 3.0)

Você tem a liberdade de:

Compartilhar — copiar, distribuir e transmitir a obra.

Remixar — criar obras derivadas.



Ficando claro que:

Renúncia — Qualquer das condições acima pode ser **renunciada** se você obtiver permissão do titular dos direitos autorais.

Domínio Público — Onde a obra ou qualquer de seus elementos estiver em **domínio público** sob o direito aplicável, esta condição não é, de maneira alguma, afetada pela licença.

Outros Direitos — Os seguintes direitos não são, de maneira alguma, afetados pela licença:

- Limitações e exceções aos direitos autorais ou quaisquer **usos livres** aplicáveis;
- Os **direitos morais** do autor;
- Direitos que outras pessoas podem ter sobre a obra ou sobre a utilização da obra, tais como **direitos de imagem** ou privacidade.

Aviso — Para qualquer reutilização ou distribuição, você deve deixar claro a terceiros os termos da licença a que se encontra submetida esta obra. A melhor maneira de fazer isso é com um link para esta página.

Sob as seguintes condições:



Atribuição — Você deve creditar a obra da forma especificada pelo autor ou licenciante (mas não de maneira que sugira que estes concedem qualquer aval a você ou ao seu uso da obra).



Uso não comercial — Você não pode usar esta obra para fins comerciais.



Compartilhamento pela mesma licença — Se você alterar, transformar ou criar em cima desta obra, você poderá distribuir a obra resultante apenas sob a mesma licença, ou sob uma licença similar à presente.

Fundamentos e Infraestrutura de Redes de Computadores

Apresentação da disciplina



Objetivo Geral

Apresentar ao aluno as características fundamentais de redes de computadores, em especial a Internet, bem como familiarizá-lo com sua arquitetura física e lógica e demonstrar as estratégias de aplicação e uso nas organizações.



Módulos

- Módulo 1 – Modelos de referência OSI e TCP/IP
- Módulo 2 – Camada de Rede e Protocolo IP
- Módulo 3 – Dynamic Host Configuration Protocol
- Módulo 4 – Network Address Translation
- Módulo 5 – Domain Name System
- Módulo 6 – File Transfer Protocol
- Módulo 7 – Hypertext Transfer Protocol
- Módulo 8 – Correio eletrônico
- Módulo 9 – Camada de transporte
- Módulo 10 – Camada de rede



Ementa

- Modelo de referência OSI e TCP/IP;
- Arquitetura de redes TCP/IP;
- Protocolos da camada de aplicação;
- Protocolos da camada de transporte;
- Protocolos da camada inter-redes;
- Serviços de rede da internet.



Referências

BÁSICAS

KUROSE, J. F. Redes de computadores e a Internet: uma abordagem top-down. Addison Wesley, 2007.

TANENBAUM, A. S. Redes de Computadores. Pearson. 2011.

DAVIE, Bruce. Redes de Computadores. Campus. 2013.

COMPLEMENTARES

BRITO, Samuel Henrique. Laboratórios de Tecnologias Cisco em Infraestrutura de Redes. Novatec. 2012.

SOUSA, Lindeberg. TCP/IP & Conectividade em Redes - Guia Prático. Erica. 2010.

FOROUZAN, B. Protocolo TCP/IP. Mcgraw Hill. 2009.

SOARES, Luiz Fernando Gomes. Redes de computadores: das LANs, MANs e WANs às redes ATM. Rio de Janeiro: Campus, 1995.

VELLOSO, Fernando de Castro. Informática: conceitos básicos. Campus, 2011.



Sistemática de Trabalho

- Aulas expositivas em sala de aula;
- Aulas no laboratório de informática;
- Listas de exercícios;
- Atividades;
- Avaliações.



Critérios de Avaliação

No decorrer de cada unidade são aplicadas atividades individuais, que devem ser entregues nas datas determinadas. Se entregues após esta data mas antes da data de aplicação da avaliação, a mesma valerá metade dos pontos.

Para compor as notas N1 e N2, faz-se a soma da atividade que vale 3 (três) com a primeira avaliação que vale 7 (sete):

$$N1 = \textit{Atividade} + \textit{Avaliação}$$

$$N2 = \textit{Atividade} + \textit{Avaliação}$$



Critérios de Avaliação

Ao final do semestre, será feita a média entre as notas N1 e N2, que deverá ser igual ou superior a 7 (sete) para que o aluno possa ser aprovado na disciplina sem a necessidade de realizar o exame final:

$$Média Final = \frac{N1 + N2}{2}$$



Critérios de Avaliação

Caso o aluno não atinja Média Final igual ou superior a 7 (sete), mas tenha obtido ao menos Média Final igual ou superior a 3 (três), poderá fazer um exame ao final do semestre.

O Exame Final é uma avaliação individual e sem consulta que vale de 0 (zero) a 10 (dez), onde será cobrado o conteúdo de todo o semestre.

A Nota Final será então a soma da Média Final mais a Nota do Exame divididos por 2 (dois).

O aluno para ser aprovado na disciplina deverá obter então Nota Final igual ou superior a 5 (cinco).

$$Nota\ Final = \frac{Média\ Final + Nota\ do\ Exame}{2}$$



Avaliações e exame

A avaliação é individual e sem consulta.

Datas previstas para entrega das atividades:

- Atividade 1: **verificar calendário acadêmico**
- Atividade 2: **verificar calendário acadêmico**

Datas previstas para aplicação das avaliações:

- Avaliação N1: **verificar calendário acadêmico**
- Avaliação N2: **verificar calendário acadêmico**

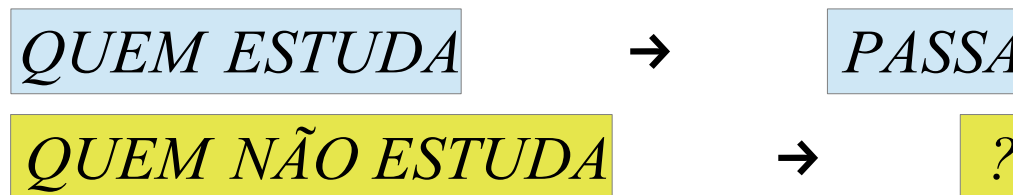
Data prevista para aplicação do exame:

- Exame: **verificar calendário acadêmico**



Regra de Três Simples

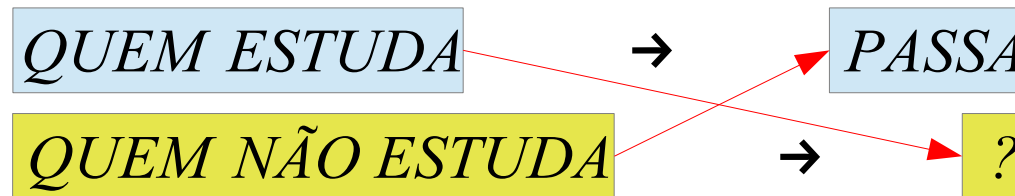
Não se esqueça:





Regra de Três Simples

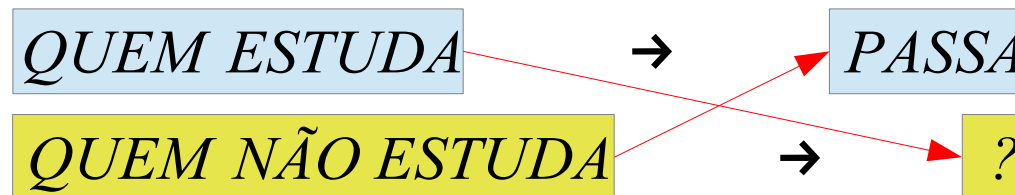
Não se esqueça:





Regra de Três Simples

Não se esqueça:

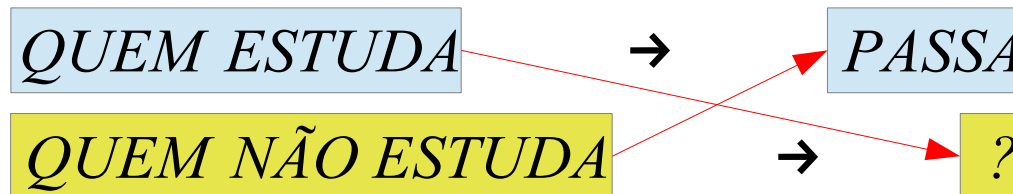


$$\boxed{QUEM\ ESTUDA} \times \boxed{?} = \boxed{QUEM\ NÃO\ ESTUDA} \times \boxed{PASSA}$$



Regra de Três Simples

Não se esqueça:



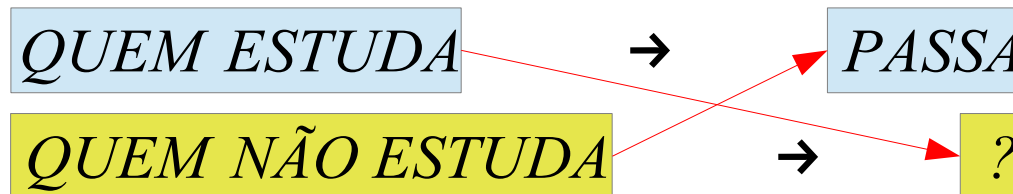
$$\boxed{QUEM\ ESTUDA} \times \boxed{?} = \boxed{QUEM\ NÃO\ ESTUDA} \times \boxed{PASSA}$$

$$\boxed{?} = \frac{\boxed{QUEM\ NÃO\ ESTUDA} \times \boxed{PASSA}}{\boxed{QUEM\ ESTUDA}}$$



Regra de Três Simples

Não se esqueça:



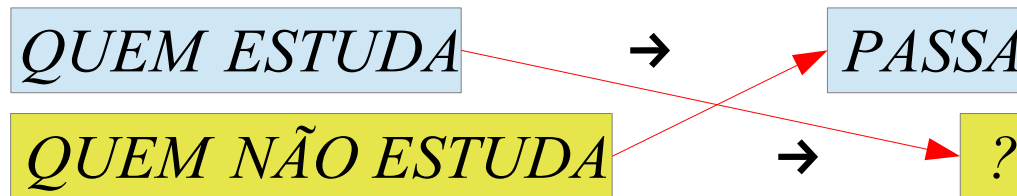
$$\boxed{QUEM ESTUDA} \times \boxed{?} = \boxed{QUEM NÃO ESTUDA} \times \boxed{PASSA}$$

$$\boxed{?} = \frac{\cancel{\boxed{QUEM NÃO ESTUDA}} \times \boxed{PASSA}}{\cancel{\boxed{QUEM ESTUDA}}}$$



Regra de Três Simples

Não se esqueça:



$$\text{QUEM ESTUDA} \times ? = \text{QUEM NÃO ESTUDA} \times \text{PASSA}$$

$$? = \frac{\cancel{\text{QUEM NÃO ESTUDA}} \times \text{PASSA}}{\cancel{\text{QUEM ESTUDA}}}$$

$$? = \text{NÃO PASSA}$$

Resposta

Módulo 1

Modelos de referência OSI e TCP/IP



Antecedentes

No início as redes eram proprietárias e a implementação de um fabricante era incompatível com a implementação de outro fabricante. Exemplos desta época são as redes SNA (Systems Network Architecture) da IBM, XNS (Xerox Network Services) da Xerox e DECnet da Digital.





Modelos de Referência

No início da década de 1980 a *International Organization for Standardization* (ISO) criou um modelo de referência para conexão de redes denominado *Open Systems Interconnection* (norma ISO 7498:1984), que ficou conhecido como modelo ISO/OSI ou simplesmente modelo OSI.

O modelo OSI aproveitou as boas práticas presentes nas implementações SNA e XNS.

No início da década de 1990, a *International Electrotechnical Commission* (IEC) juntou-se à ISO para reescrever a norma, que em 1994 foi publicada como norma ISO/IEC 7498-1 Segunda Edição.



Implementações pós OSI

As primeiras implementações pós OSI baseavam-se nas redes XNS na Xerox. Entre elas destacam-se as redes NetWare da Novell, VINES (*Virtual Integrated NETwork Service*) da Banyan e AppleTalk da Apple.

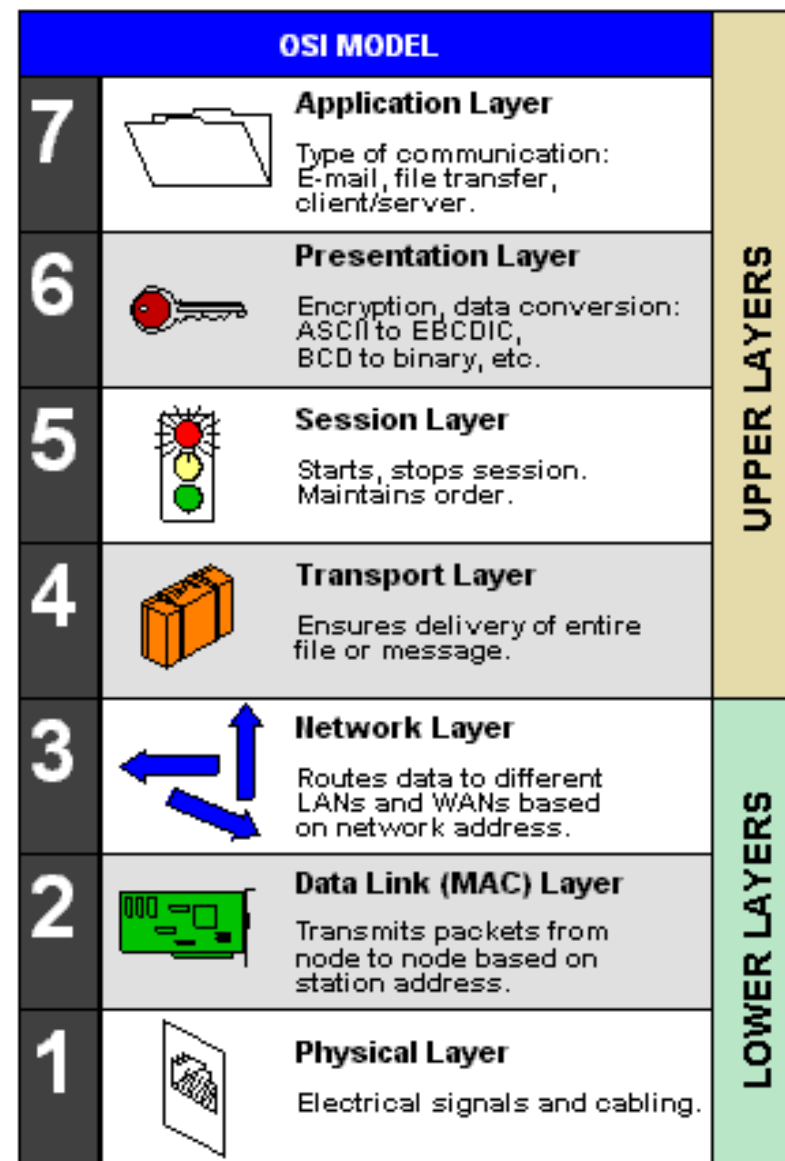
Novell.
NetWare





Modelo de Referência OSI

- O modelo de referência OSI é composto por sete camadas e representa um modelo base para a implementação da pilha de protocolos da rede, sem no entanto especificar exatamente os serviços e protocolos de cada camada.
- A transmissão de dados entre uma origem e um destino deve seguir uma sequência lógica de operações, desde a captura dos dados, passando por sua transformação até a transmissão dos mesmos.
- A ideia básica por trás do modelo OSI é que cada camada deve implementar apenas as operações e serviços necessários para abstrair cada etapa da transmissão de dados.
- Cada camada deve se comunicar apenas com as camadas adjacentes, ou seja, uma camada sempre recebe dados da camada anterior e depois repassa para a camada posterior.

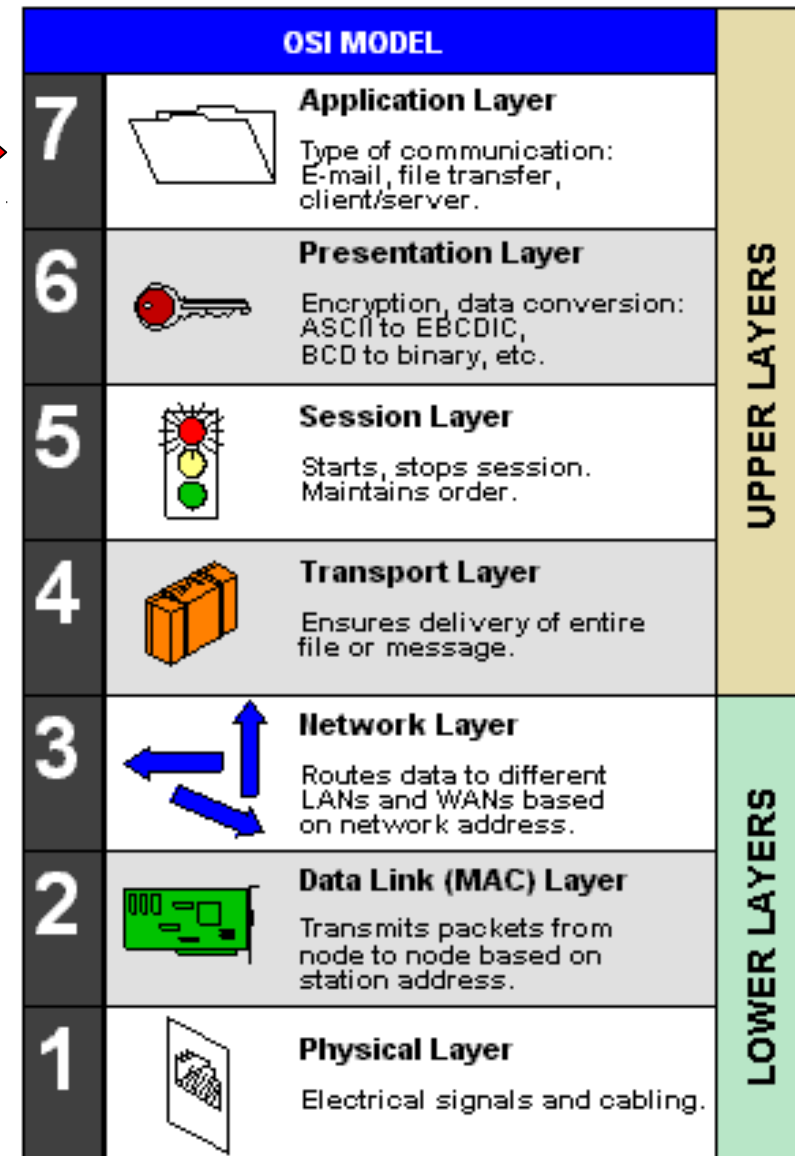
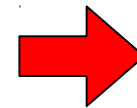


From Computer Desktop Encyclopedia
(c) 2004 The Computer Language Co. Inc.



Camada de Aplicação

- É nesta camada que residem as aplicações, tais como o navegador de Internet, cliente de correio eletrônico, transferência de arquivos, entre outros.
- Esta camada funciona como uma interface entre as aplicações do usuário e a pilha de protocolos das camadas mais baixas.

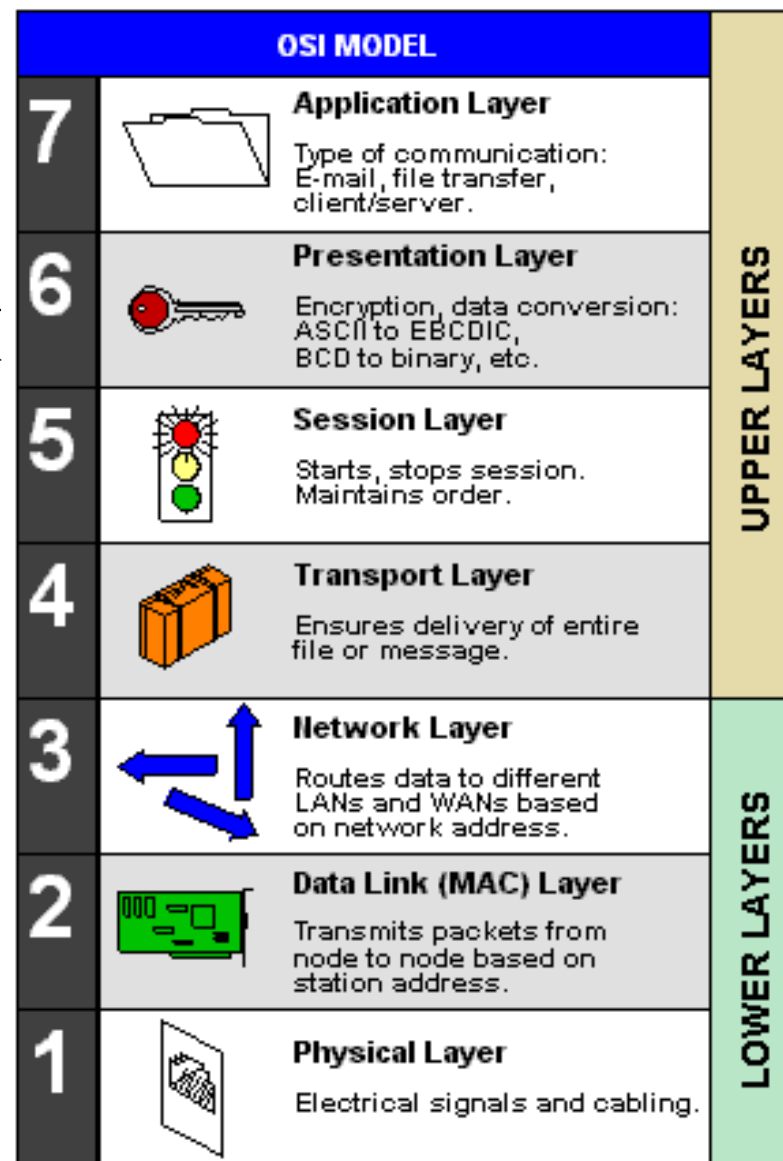
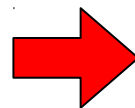


From Computer Desktop Encyclopedia
(c) 2004 The Computer Language Co. Inc.



Camada de Apresentação

- Esta camada é responsável por converter os dados em um formato universal que possa ser interpretado por sistemas de plataformas diferentes.
- É nesta camada que as operações de criptografia e compactação de dados são executadas.

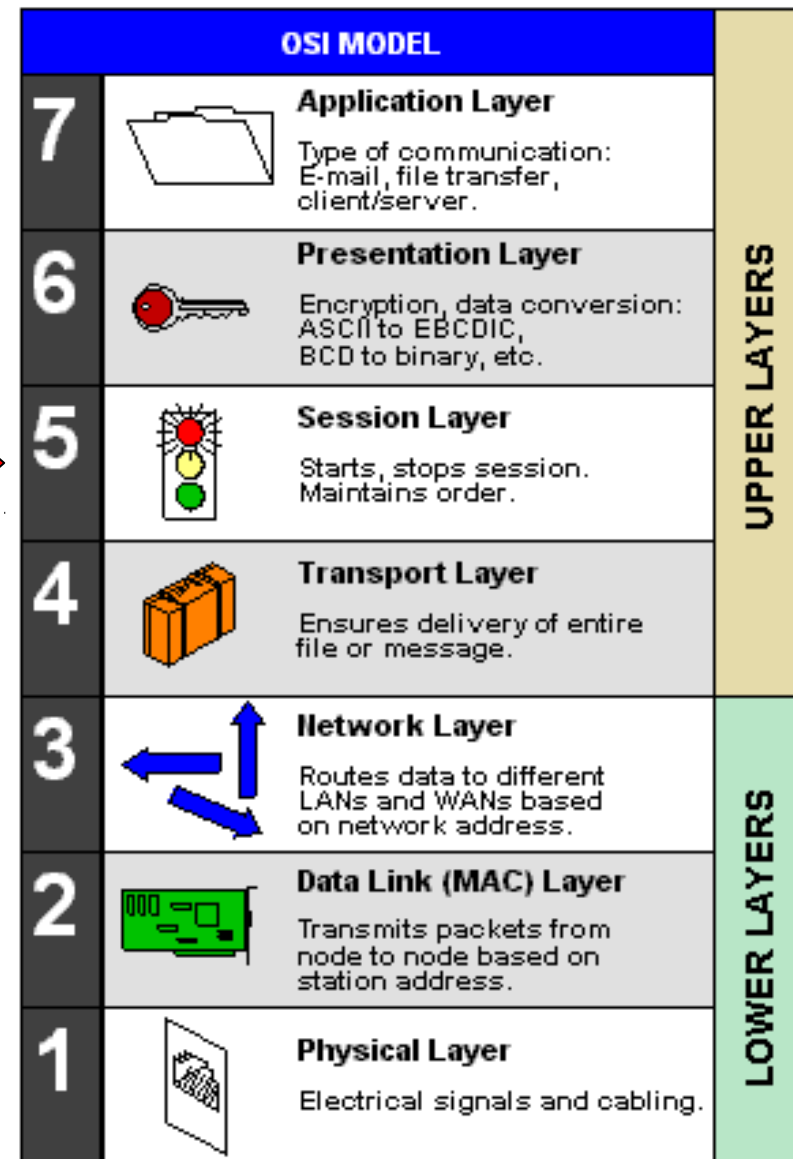
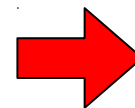


From Computer Desktop Encyclopedia
(c) 2004 The Computer Language Co. Inc.



Camada de Sessão

- A camada de sessão controla o estabelecimento da comunicação entre um par origem e destino. É responsável por iniciar e encerrar as sessões de comunicação.

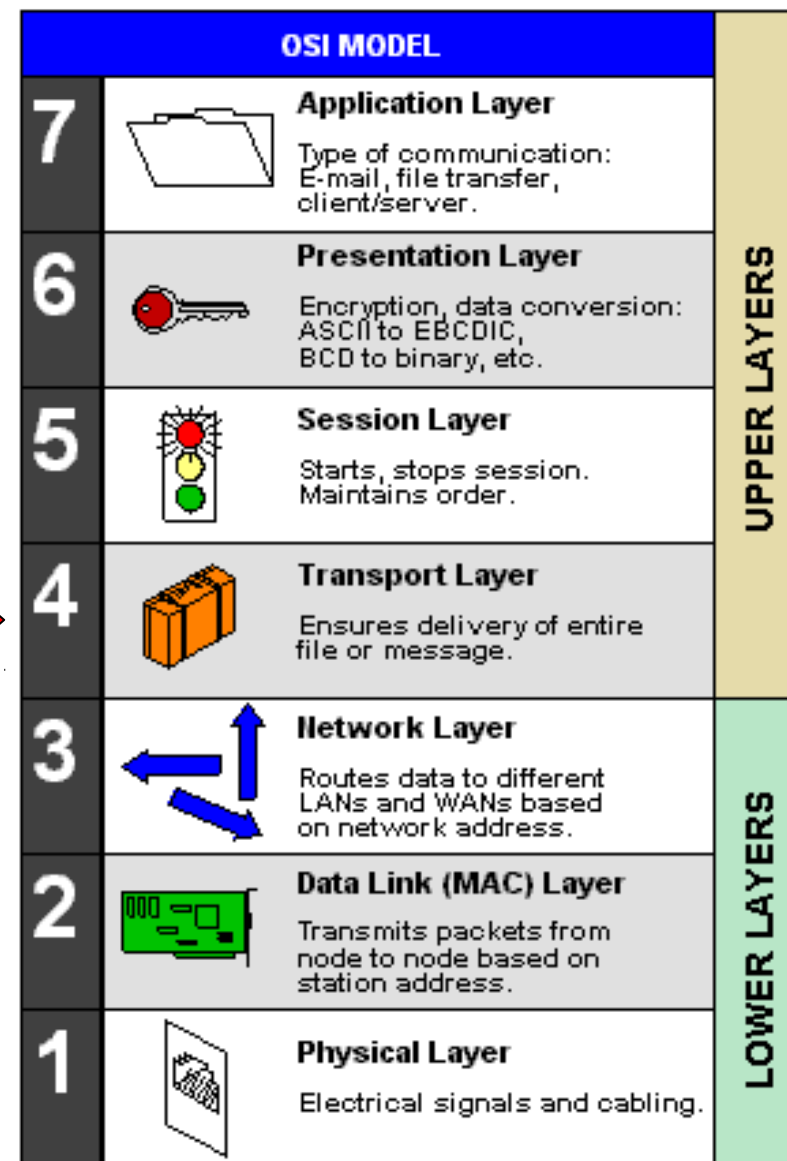
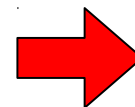


From Computer Desktop Encyclopedia
(c) 2004 The Computer Language Co. Inc.



Camada de Transporte

- Esta camada é responsável por segmentar os dados provenientes das camadas superiores e entregá-las da melhor maneira possível ao destinatário.
- Uma vez que os dados podem ser segmentados, a camada de transporte numera sequencialmente cada segmento, e estes deverão ser novamente juntados no destino.
- A entrega pode ser do tipo confiável (com confirmação de entrega) ou do tipo não confiável (sem confirmação).

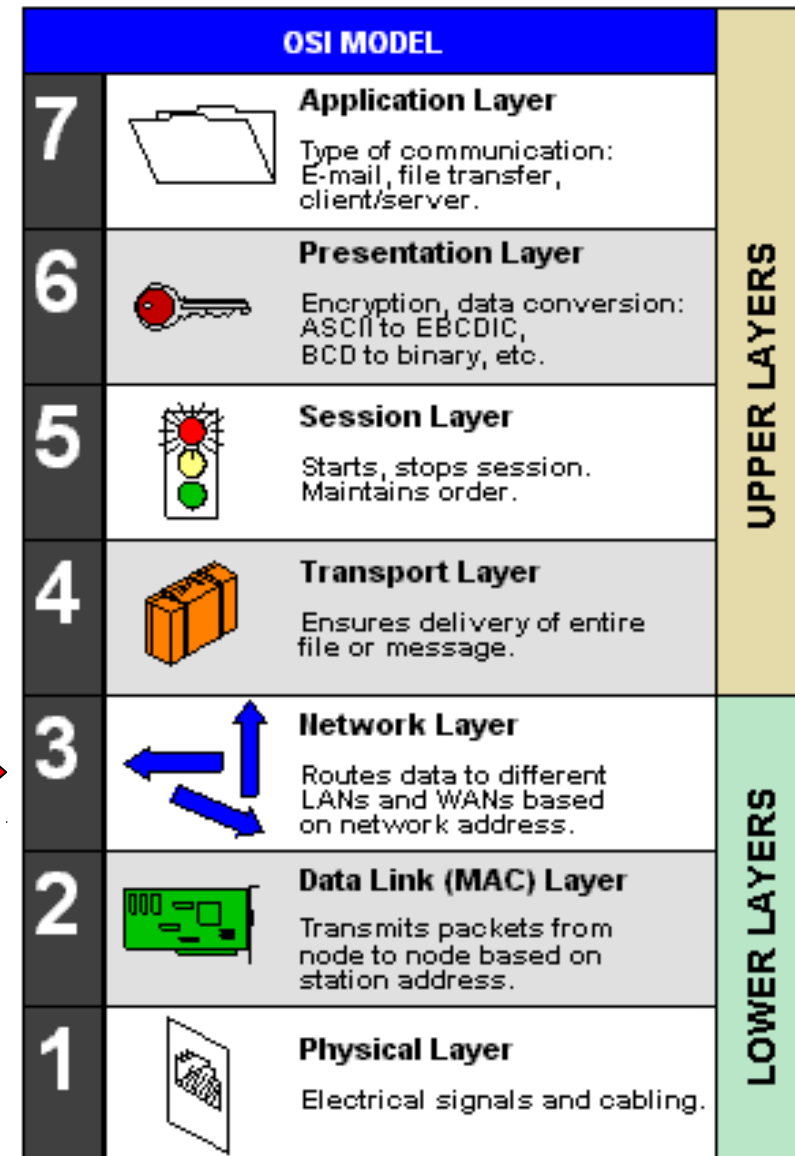
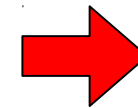


From Computer Desktop Encyclopedia
(c) 2004 The Computer Language Co. Inc.



Camada de Rede

- A camada de rede é responsável por fazer a entrega dos dados em redes distintas.
- Os protocolos da camada de rede usam o endereço de rede para identificar qual o melhor caminho para entregar dados entre a origem e o destino.

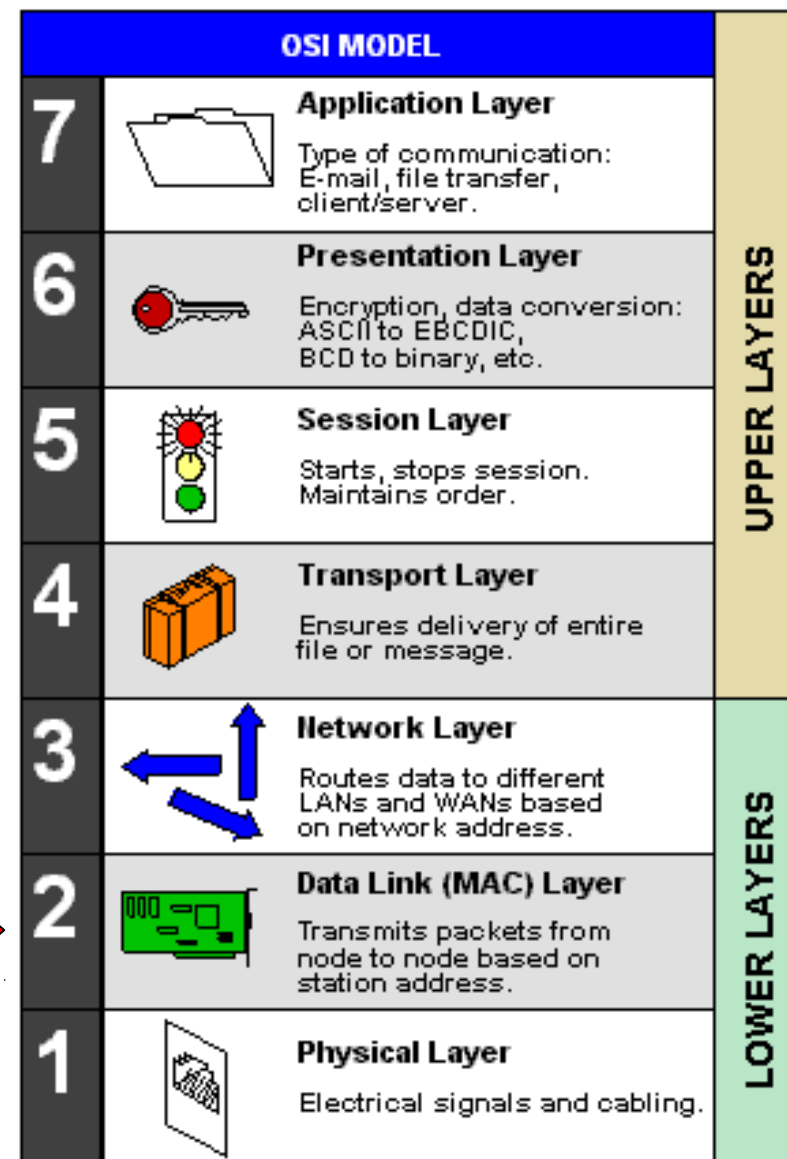
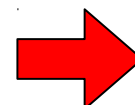


From Computer Desktop Encyclopedia
(c) 2004 The Computer Language Co. Inc.



Camada de Enlace

- A camada de enlace é responsável por fazer a entrega de dados em redes locais, ou ainda, entre máquinas que estejam no mesmo segmento de rede.
- Os protocolos da camada de enlace usam apenas o endereço local de cada estação, sem levar em conta o endereço de rede.

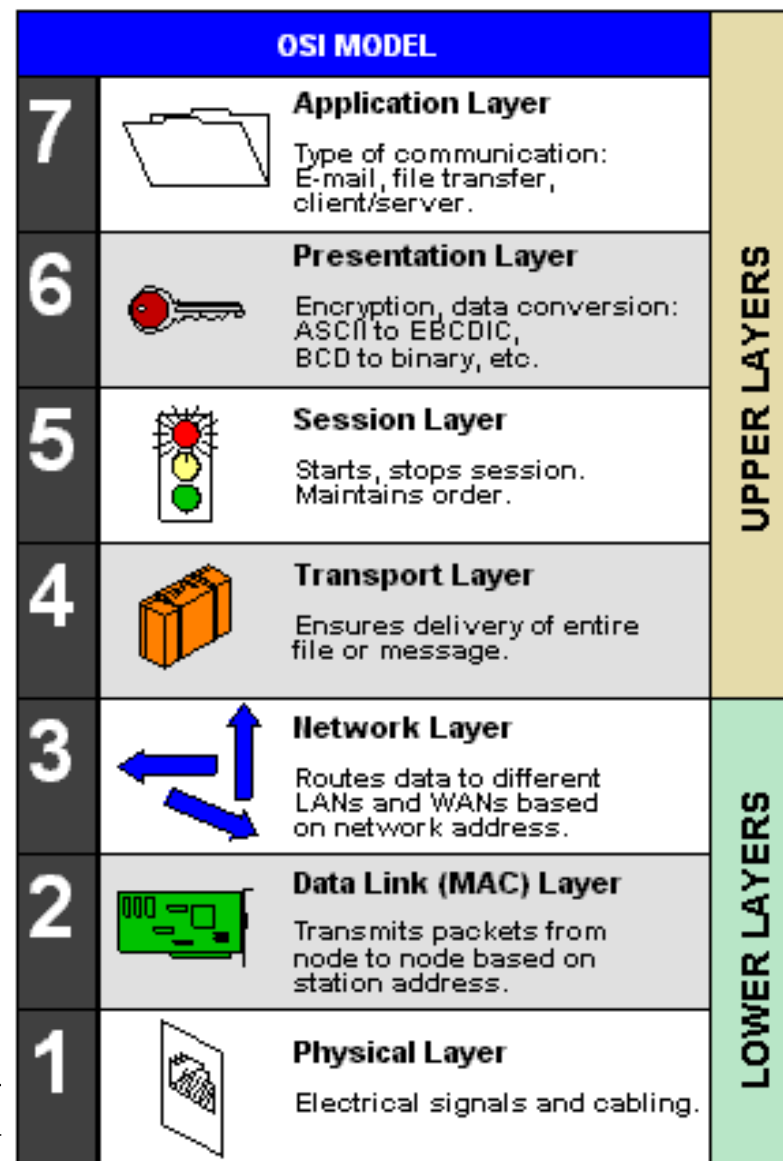
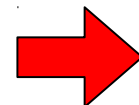


From Computer Desktop Encyclopedia
(c) 2004 The Computer Language Co. Inc.



Camada Física

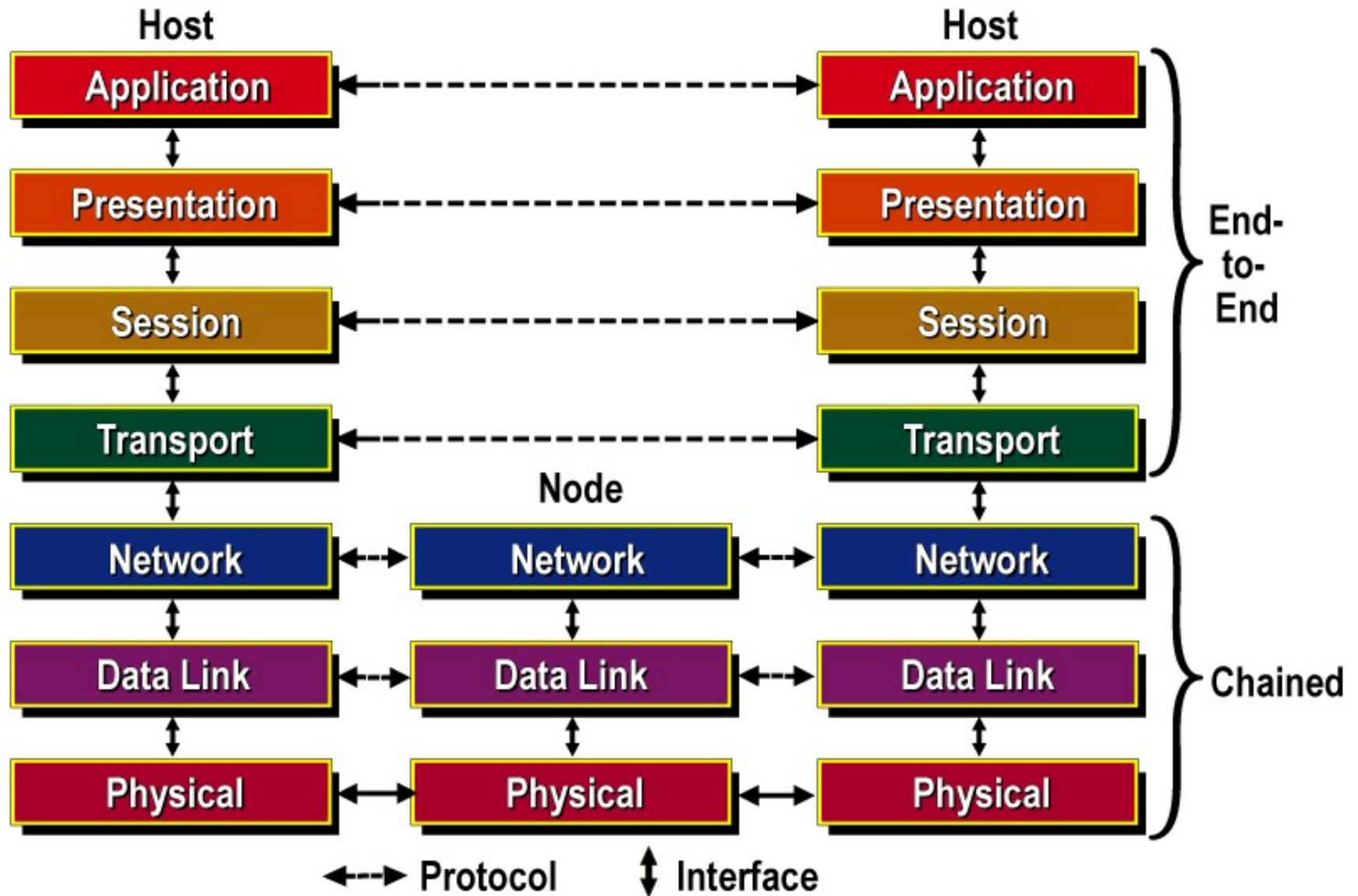
- A camada física define as especificações elétricas, físicas e mecânicas dos meios físicos de transmissão.
- Esta camada é responsável por enviar uma sequência de bits entre a origem e o destino.



From Computer Desktop Encyclopedia
(c) 2004 The Computer Language Co. Inc.

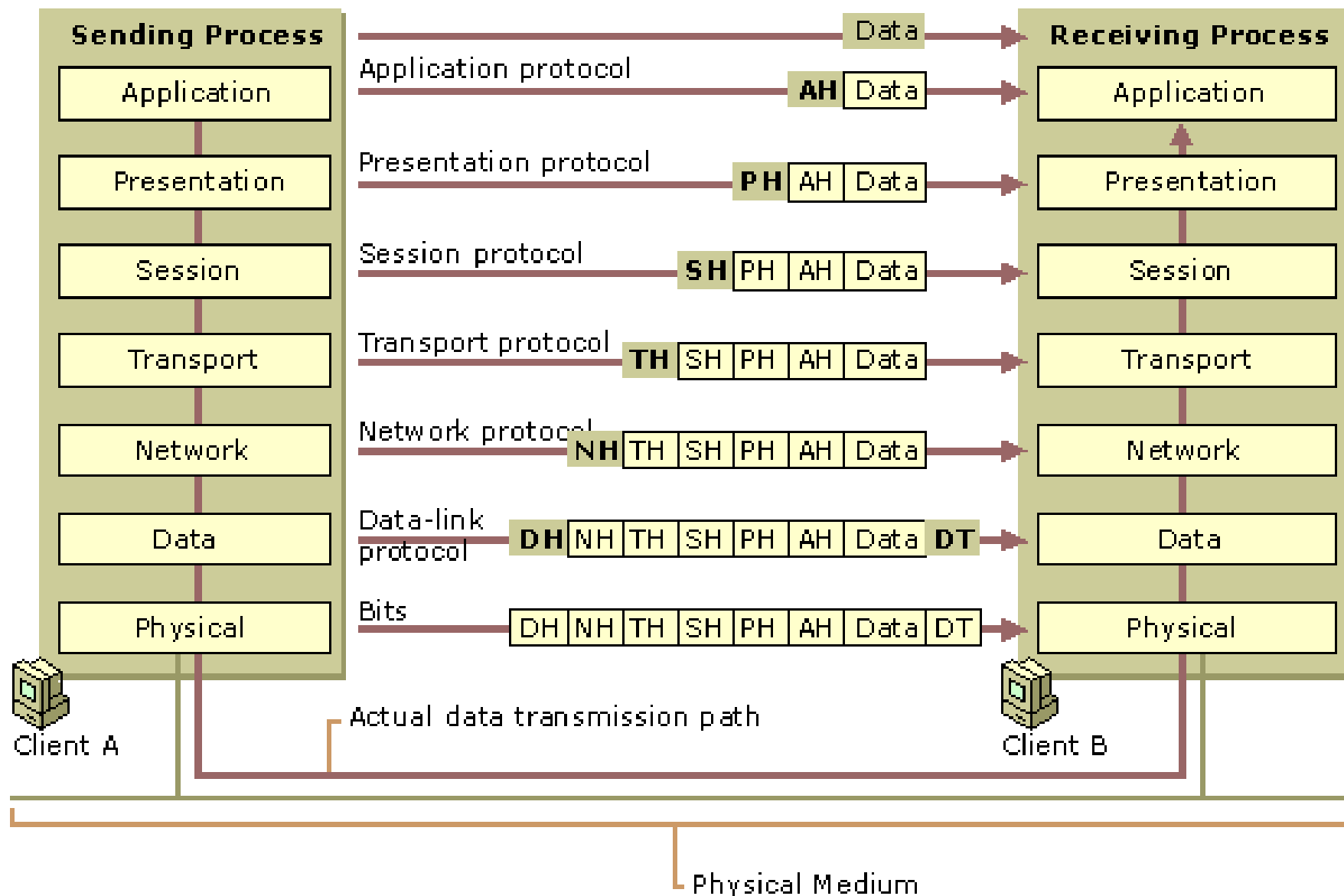


Relação entre as camadas





Fluxo de dados no modelo OSI





Modelo de Referência TCP/IP

- O modelo de referência TCP/IP surgiu de um projeto do exército dos Estados Unidos com o objetivo de criar uma rede que fosse tolerante à falhas.

- Houve a participação intensa de universidades e órgãos de pesquisa, e com o fim da Guerra Fria, a rede começou a aceitar que outras organizações pudessem se conectar à rede.

- O Modelo de Referência não seguiu a mesma padronização do Modelo OSI, e por isso alguns autores adotam um modelo de 4 camadas, enquanto outros adotam o modelo de 5 camadas.

- O modelo TCP/IP não é baseado no modelo OSI. A sua comparação destina-se apenas a facilitar o entendimento do modelo.

- O Modelo de Referência TCP/IP recebe este nome porque seus dois principais protocolos são o de transporte (TCP) e o de rede (IP).

Modelo OSI

Aplicação
Apresentação
Sessão
Transporte
Rede
Enlace
Física

**Modelo TCP/IP
de 5 Camadas**

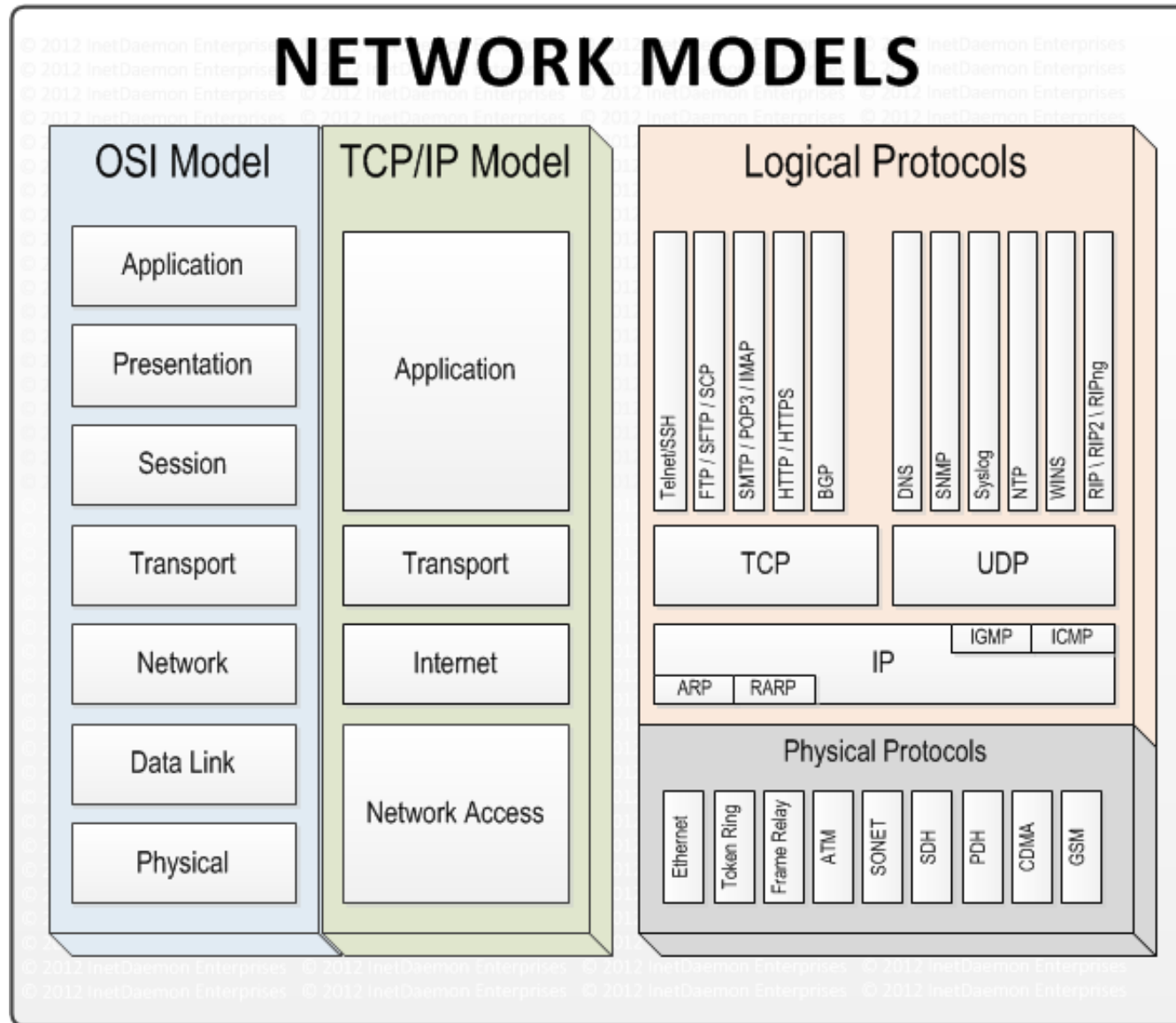
Aplicação
Transporte
Inter-rede
Host-rede
Física

**Modelo TCP/IP
de 4 Camadas**

Aplicação
Transporte
Inter-rede
Host-rede



Relação entre os modelos OSI e TCP/IP

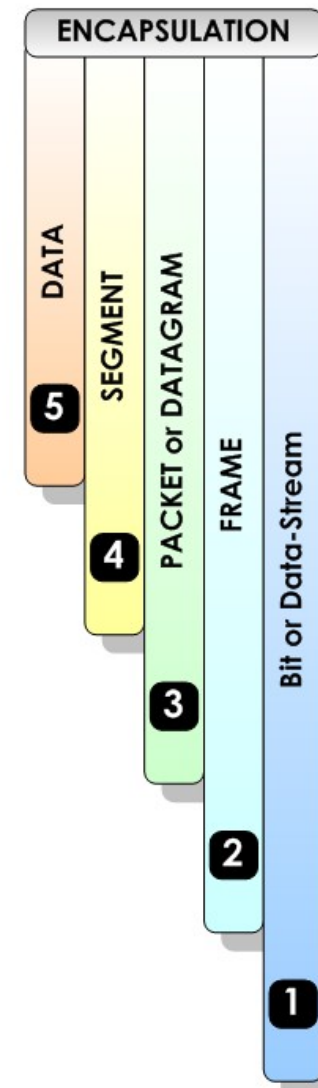
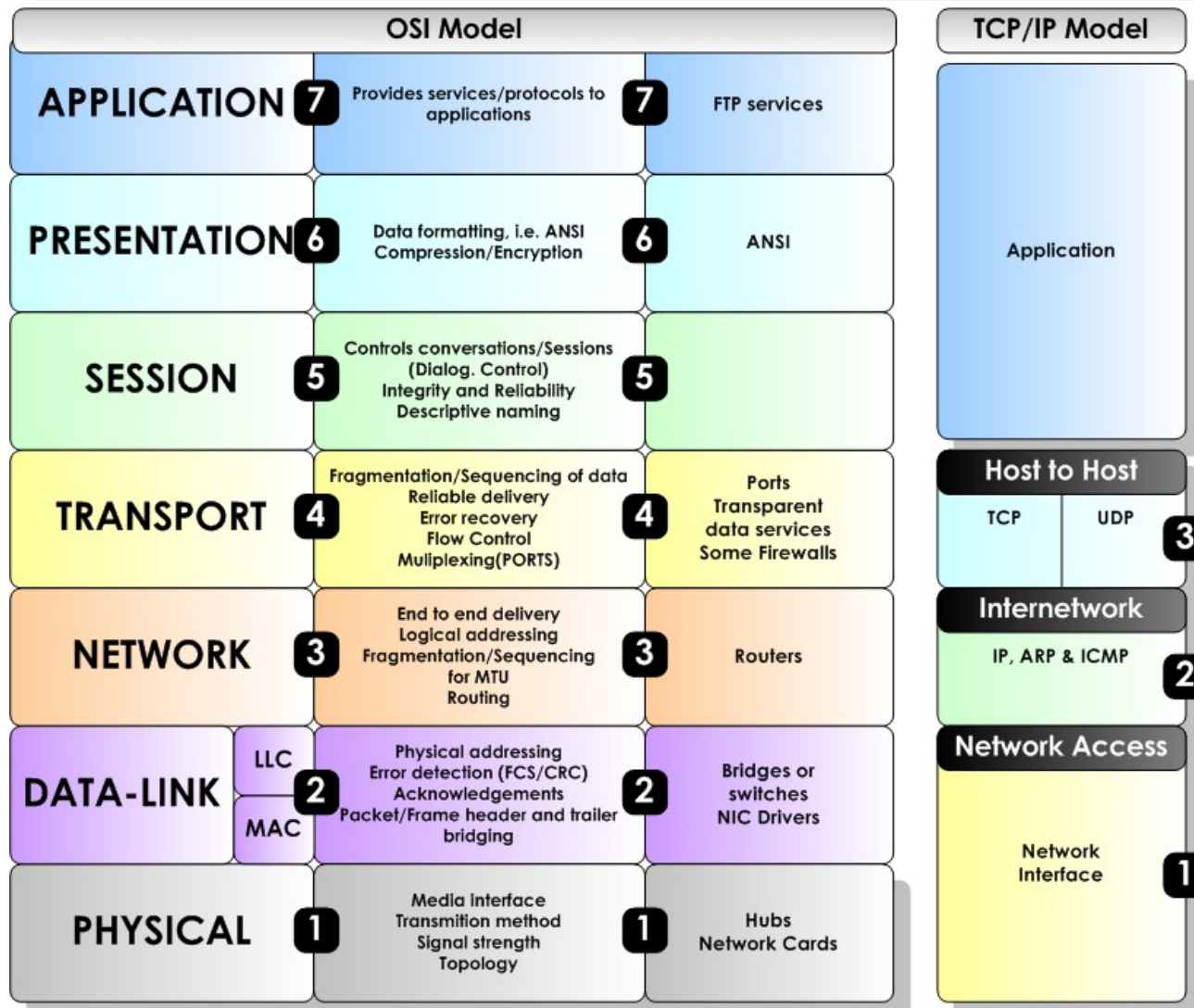




Relação entre os modelos OSI e TCP/IP

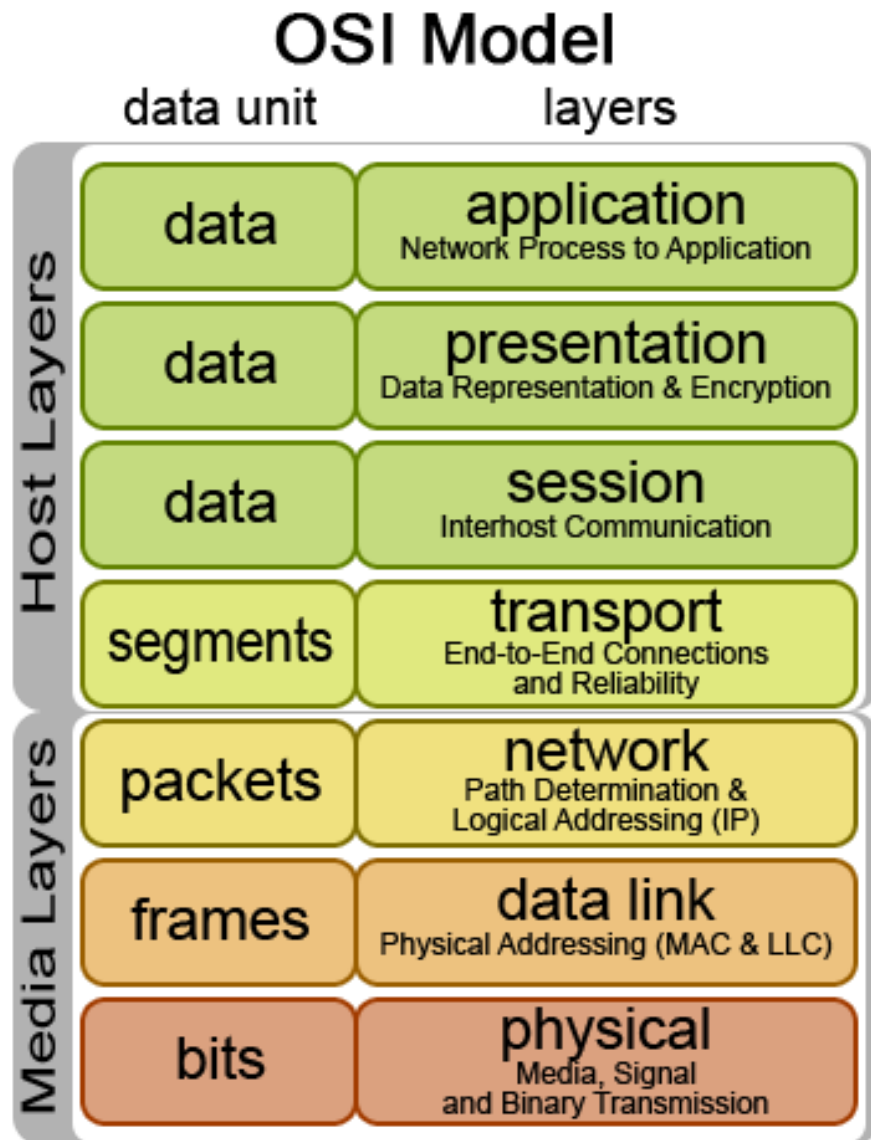
The OSI Model (Open Systems Interconnection)

© Copyright 2008 Steven Iveson
www.networkstuff.eu





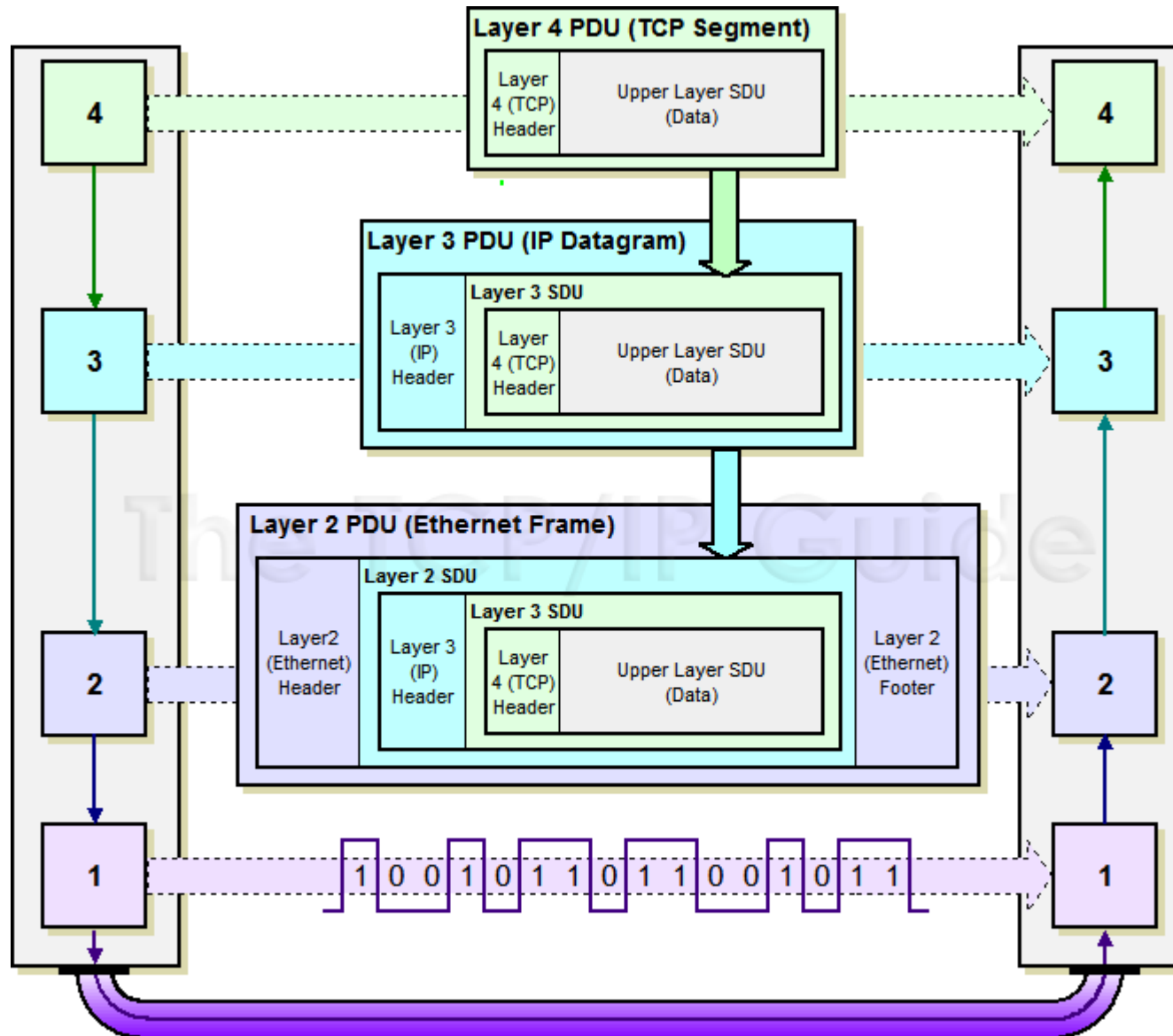
Unidades de informação



CAMADA	UNIDADE DE INFORMAÇÃO
Aplicação, Apresentação e Sessão	Mensagem ou Dados
Transporte	Segmento
Rede	Pacote ou Datagrama
Enlace	Quadro ou Frame
Física	Bits

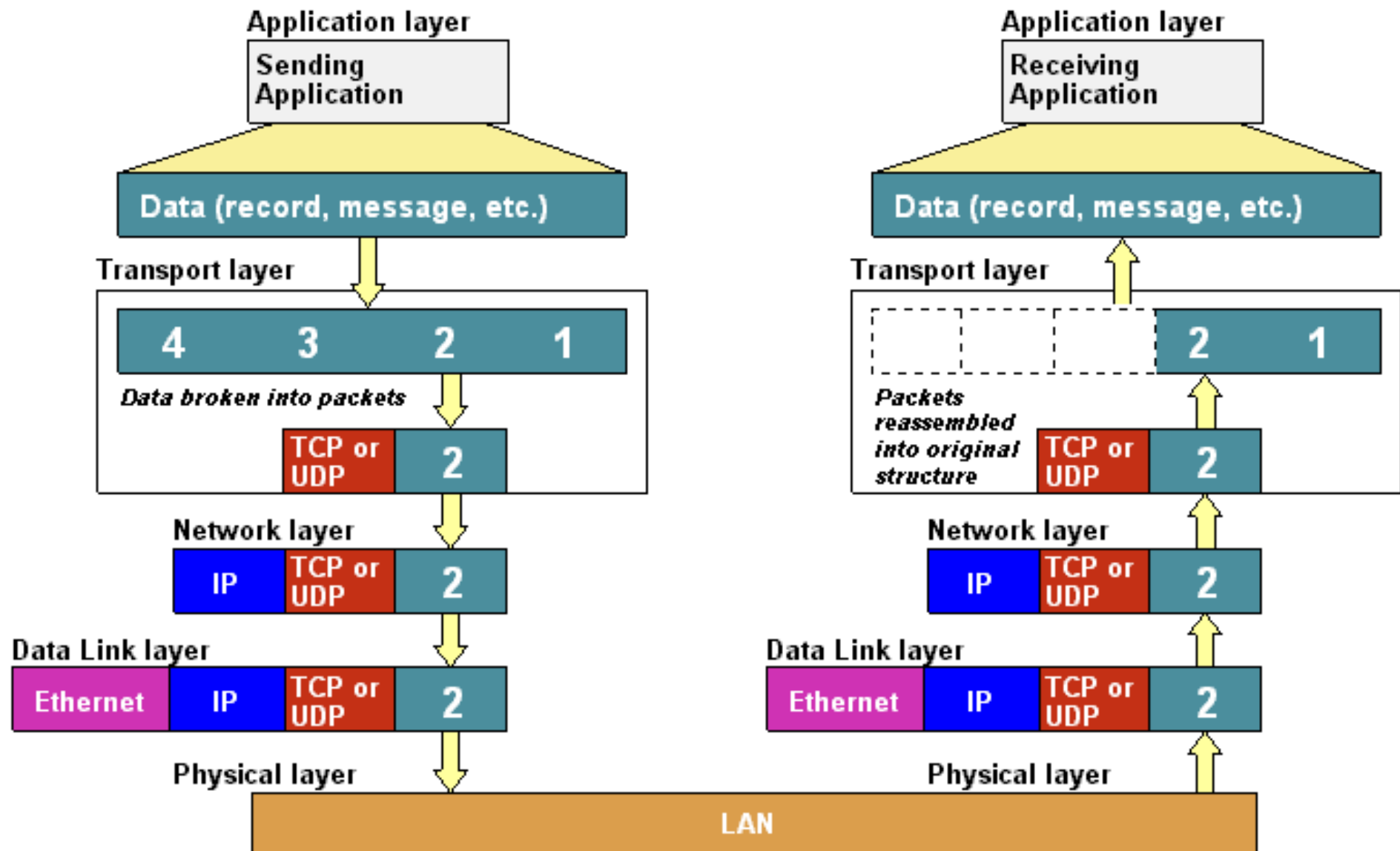


Fluxo de dados no modelo TCP/IP



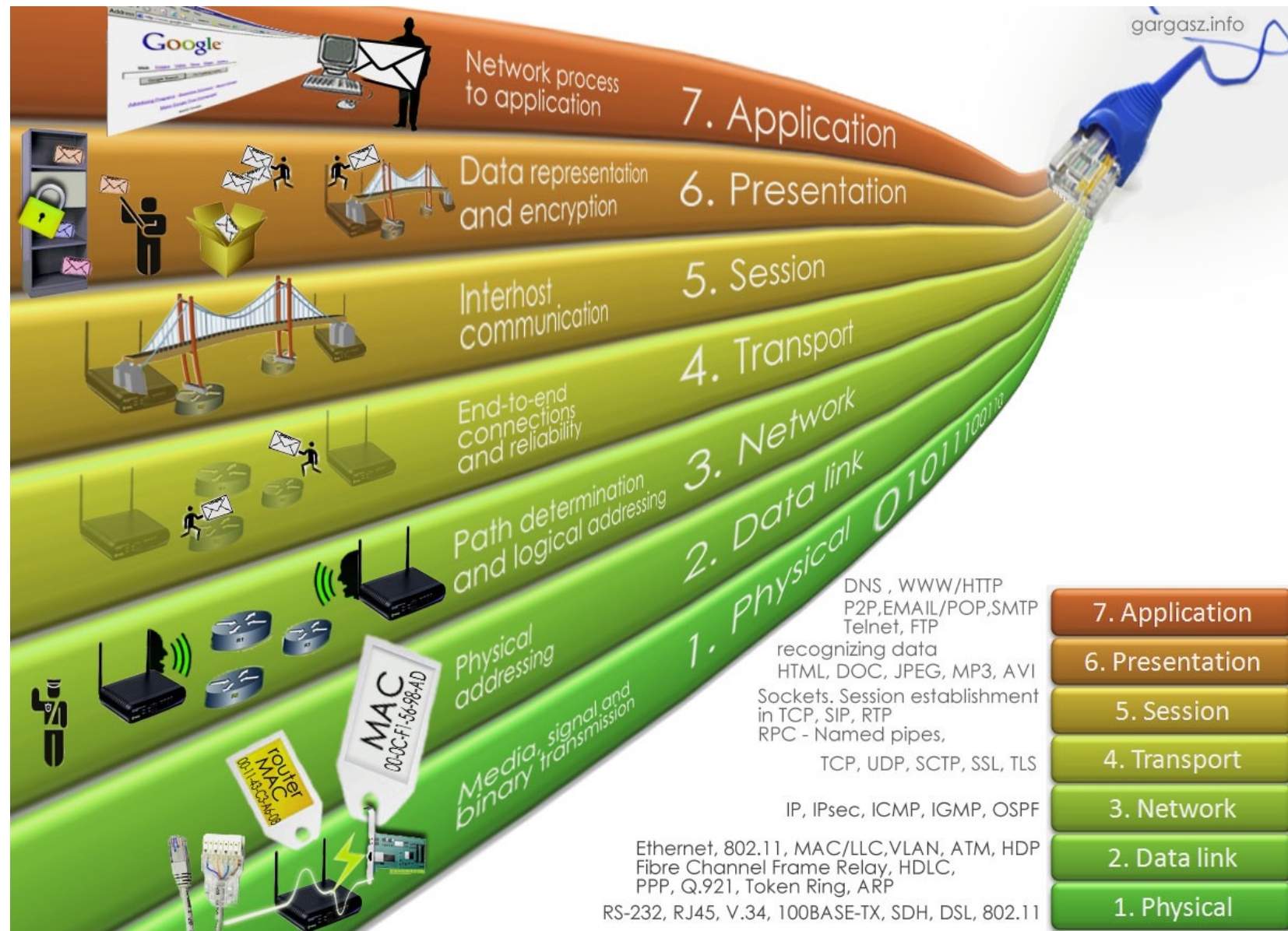


Fluxo de dados no modelo TCP/IP





Protocolos TCP/IP





Para saber mais...

- ... acesse a norma ISO/IEC 7498-1 OSI – Basic Reference Model, da International Organization for Standardization (ISO) e da International Electrotechnical Commission (IEC).
- ... acesse o material online sobre o Modelo de Referência ISO/OSI, do Prof. Dr. Nilton Alves Jr., do Centro de Pesquisas Físicas, Brasil.
- ... acesse o artigo OSI Reference Model – The ISO Model of Architecture for Open Systems Interconnection, de Hubert Zimmermann.

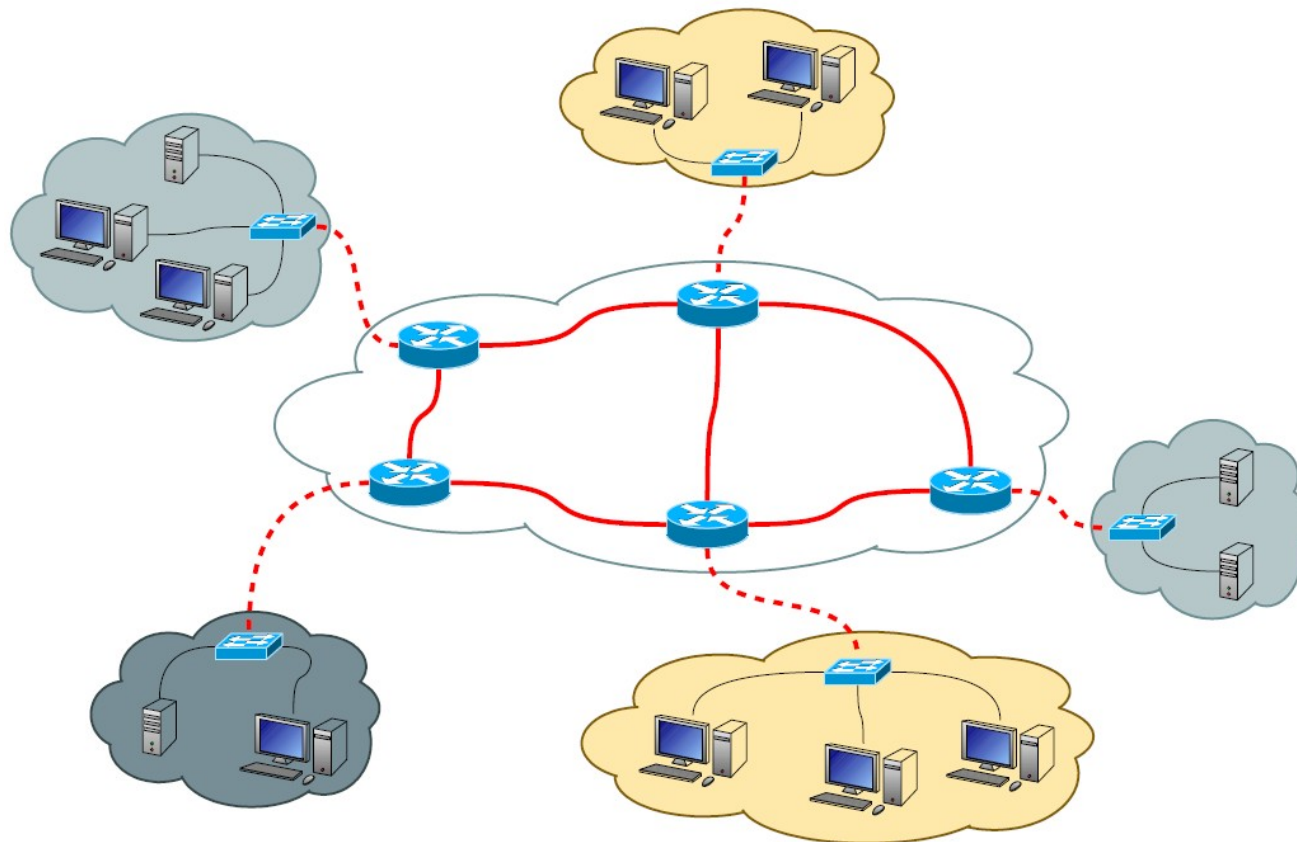
Módulo 2

Camada de Rede e Protocolo IP



Introdução – Camada de Rede



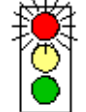




A camada de rede é responsável por enviar informações entre a origem e o destino da transmissão de dados pelas diferentes redes e caminhos alternativos que compõem a Internet.





O Protocolo IP

O Internet Protocol, ou simplesmente IP é um protocolo da camada de rede que tem por objetivo identificar unicamente um *host* na rede mundial de computadores e transmitir os datagramas (pacotes) da origem ao destino.

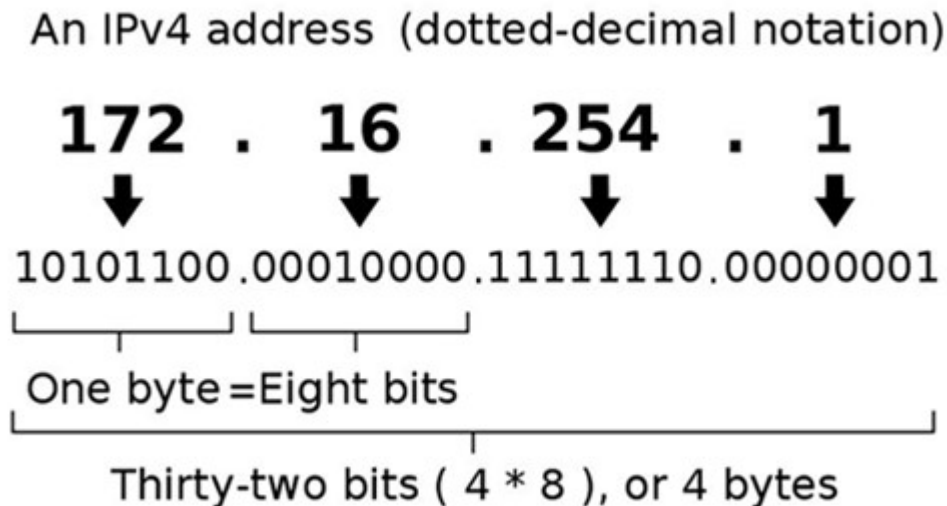
OSI MODEL			TCP / IP
7		Application Layer Type of communication: E-mail, file transfer, client/server.	FTP, Telnet, HTTP, SNMP, DNS, OSPF, RIP, Ping, Traceroute
6		Presentation Layer Encryption, data conversion: ASCII to EBCDIC, BCD to binary, etc.	
5		Session Layer Starts, stops session. Maintains order.	
4		Transport Layer Ensures delivery of entire file or message.	TCP (delivery ensured) UDP (delivery NOT ensured)
3		Network Layer Routes data to different LANs and WANs based on network address.	IP (ICMP, IGMP, ARP, RARP)
2		Data Link (MAC) Layer Transmits packets from node to node based on station address.	
1		Physical Layer Electrical signals and cabling.	

From Computer Desktop Encyclopedia
(c) 2004 The Computer Language Co. Inc.



Endereço IP

O endereço IP é um número binário composto por 32 bits. Cada grupo de 8 bits é conhecido como octeto, de modo que um endereço possui 4 octetos. O endereço IP pode ser escrito na notação binária ou decimal, conforme exemplo abaixo:





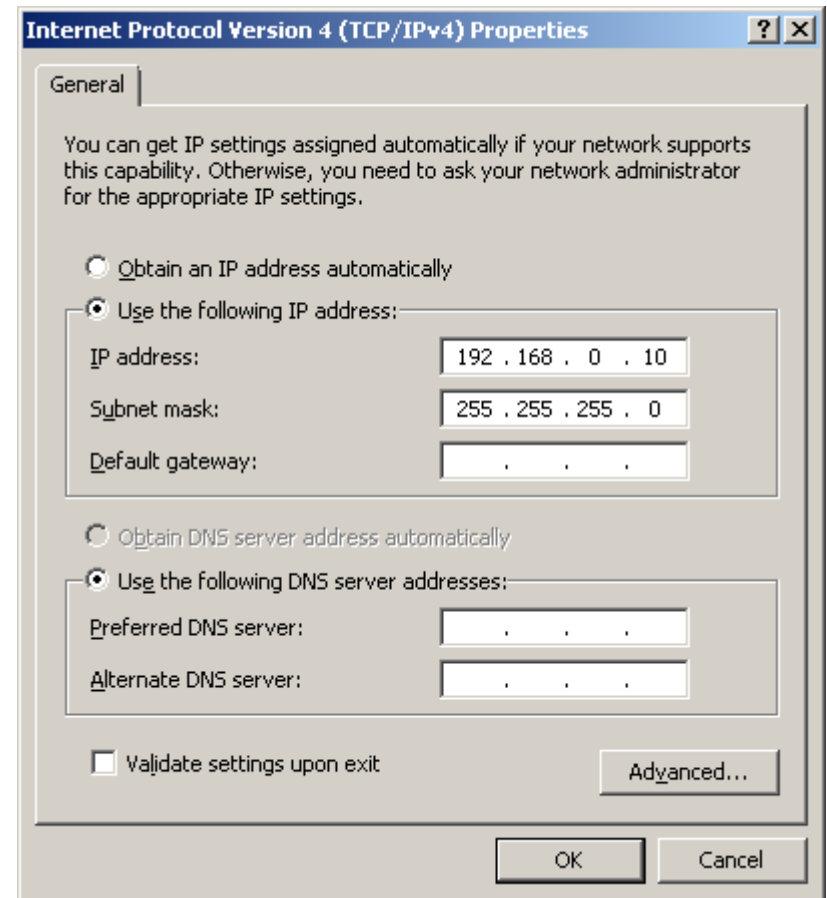
Máscara de rede

Todo *host* para funcionar na rede deve possuir um endereço IP, que o identifica unicamente na rede. No entanto, o IP carrega duas informações: a rede onde o *host* está conectado e o próprio *host*. Estas duas informações são obtidas por meio da máscara de rede.

Class A 11111111.00000000.00000000.00000000
255.0.0.0

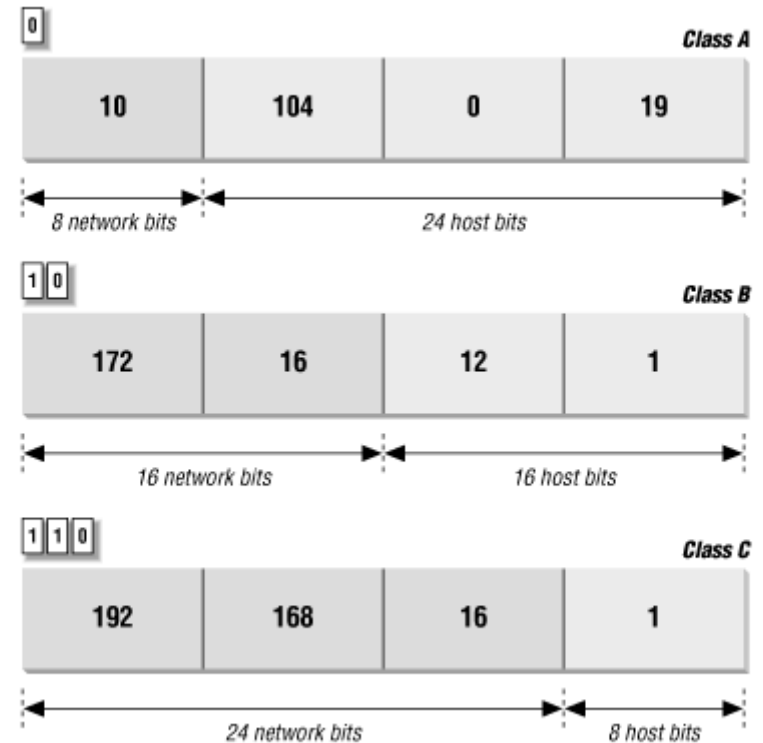
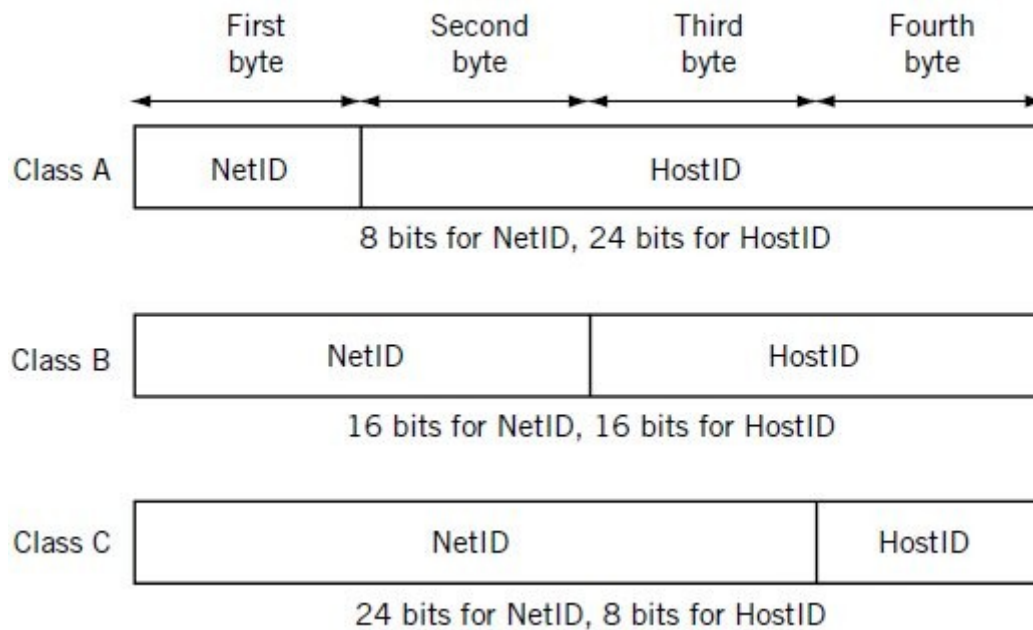
Class B 11111111.11111111.00000000.00000000
255.255.0.0

Class C 11111111.11111111.11111111.00000000
255.255.255.0



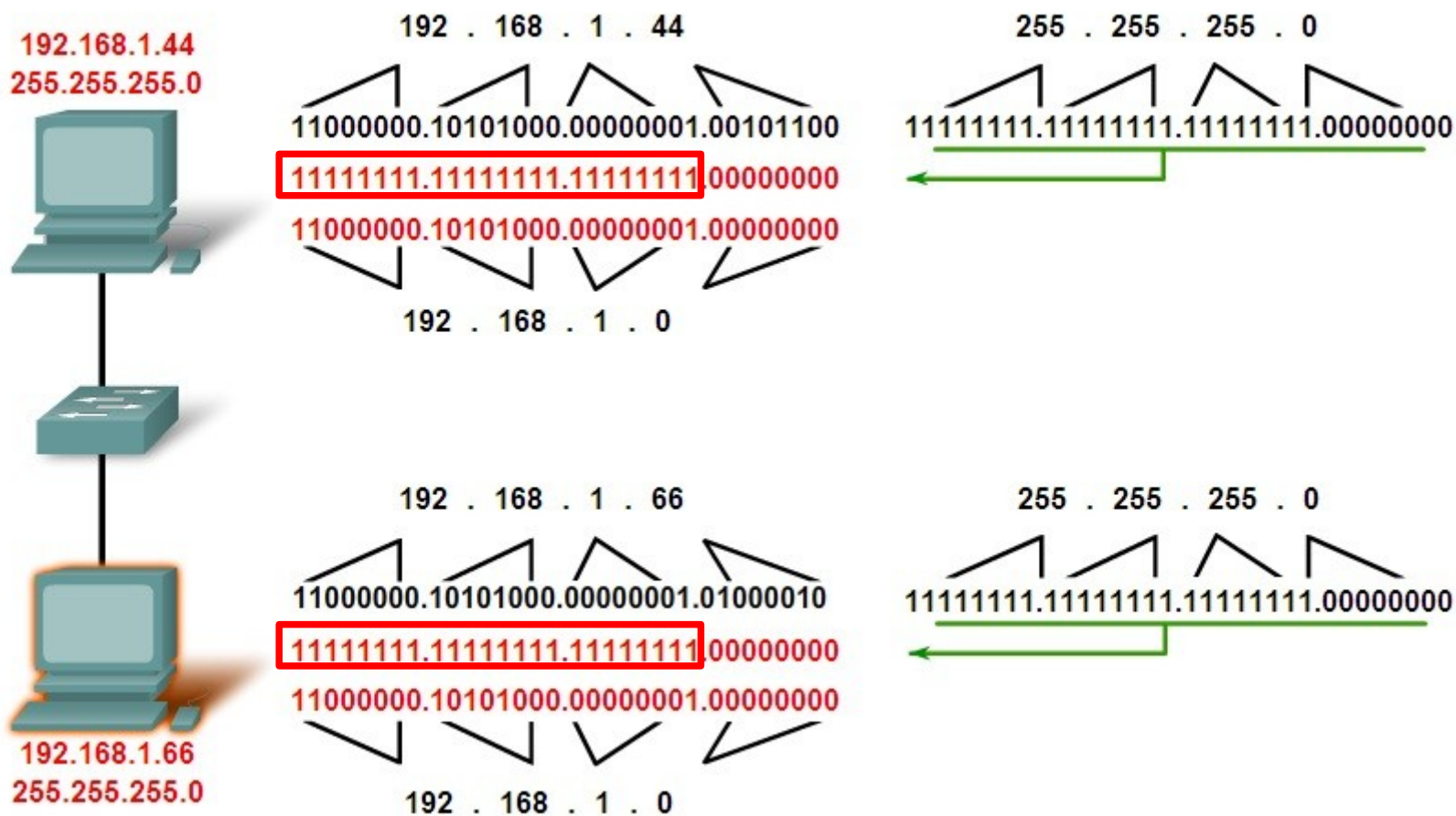


Máscara de rede





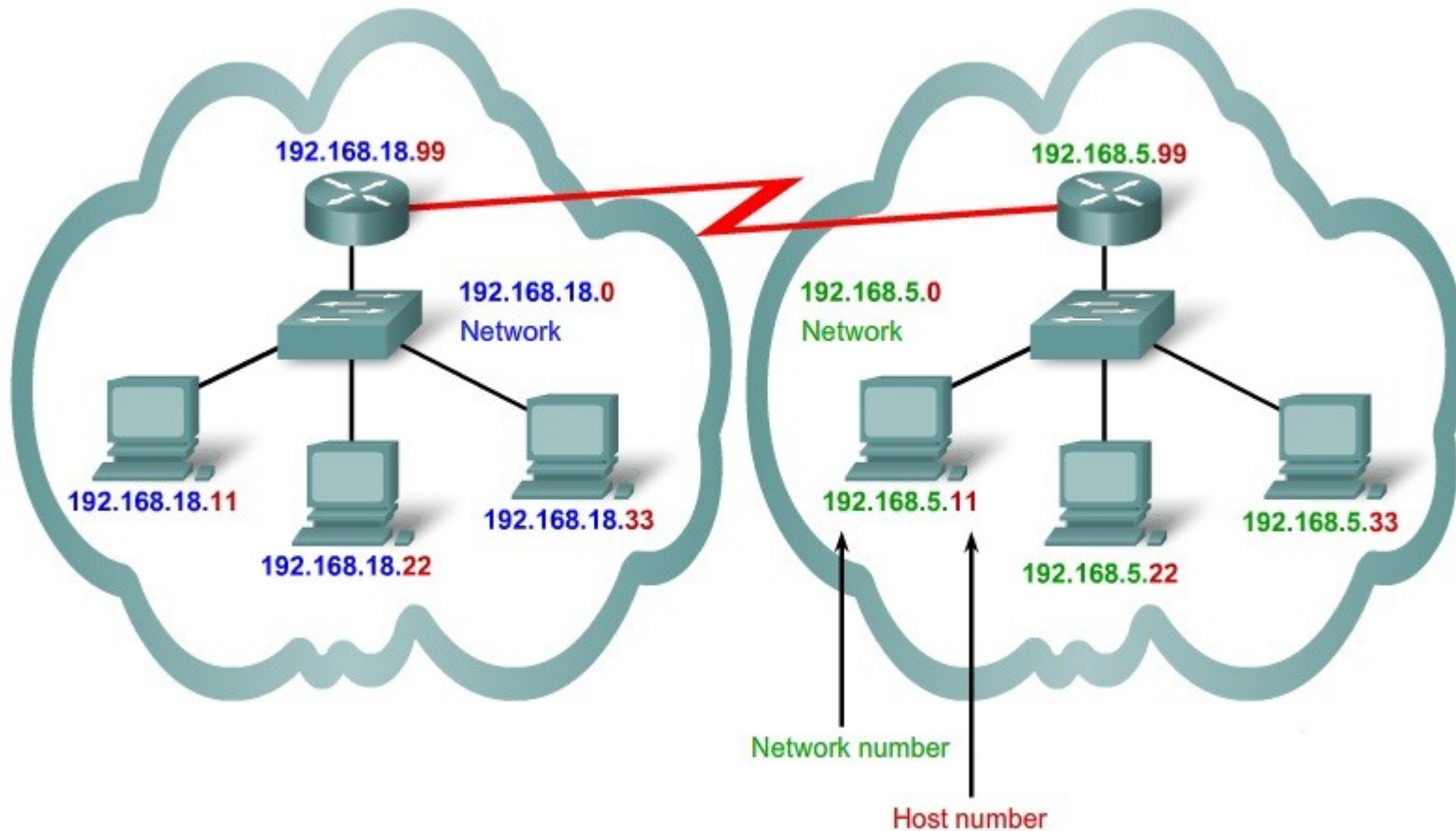
Operação “E” lógico



Entradas		Saída
0	0	0
0	1	0
1	0	0
1	1	1



Redes distintas





Máximo de *hosts* por classe

Class	First Octet Range	Default Subnet Mask	Max Hosts	Format
A	1-126	255.0.0.0	16M	<div>NETID</div> <div>Network</div> <div>1 Octet</div> <div>HOSTID</div> <div>Host</div> <div>Host</div> <div>Host</div> <div>3 Octet</div>
B	128-191	255.255.0.0	64K	<div>NETID</div> <div>Network</div> <div>2 Octet</div> <div>HOSTID</div> <div>Host</div> <div>Host</div> <div>2 Octet</div>
C	192-223	255.255.255.0	254	<div>NETID</div> <div>Network</div> <div>3 Octet</div> <div>HOSTID</div> <div>Host</div> <div>1 Octet</div>
D	224-239	N/A	N/A	<div>Multicast Address</div> <div></div> <div></div> <div></div> <div></div>
E	240-255	N/A	N/A	<div>Experimental</div> <div></div> <div></div> <div></div> <div></div>



Criando sub-redes

0	8	16	24	32			
200				13	94	Host ID (8 bits)	Class C Network 200.13.94.0
1 1 1 1 1 1 1 1				1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	0 0 0 0 0 0 0 0	0 Subnet ID Bits 8 Host ID Bits (1 Subnet, 254 Hosts)
255				255	255	0	
1 1 1 1 1 1 1 1				1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 0 0 0 0 0 0 0	1 Subnet ID Bit 7 Host ID Bits (2 Subnets, 126 Hosts Each)
255				255	255	128	
1 1 1 1 1 1 1 1				1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 0 0 0 0 0 0	2 Subnet ID Bits 6 Host ID Bits (4 Subnets, 62 Hosts Each)
255				255	255	192	
1 1 1 1 1 1 1 1				1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 0 0 0 0 0	3 Subnet ID Bit 5 Host ID Bits (8 Subnets, 30 Hosts Each)
255				255	255	224	
1 1 1 1 1 1 1 1				1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 0 0 0 0	4 Subnet ID Bit 4 Host ID Bits (16 Subnets, 14 Hosts Each)
255				255	255	240	
1 1 1 1 1 1 1 1				1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 0 0 0	5 Subnet ID Bit 3 Host ID Bits (32 Subnets, 6 Hosts Each)
255				255	255	248	
1 1 1 1 1 1 1 1				1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 0 0	6 Subnet ID Bit 2 Host ID Bits (64 Subnets, 2 Hosts Each)
255				255	255	252	



Máscara de rede - Notação

A máscara de rede pode ser escrita na notação decimal ou na notação CIDR (*Classless Inter-Domain Routing*):

Máscara	CIDR	Máscara	CIDR	Máscara	CIDR	Máscara	CIDR
0.0.0.0	/0	255.0.0.0	/8	255.255.0.0	/16	255.255.255.0	/24
128.0.0.0	/1	255.128.0.0	/9	255.255.128.0	/17	255.255.255.128	/25
192.0.0.0	/2	255.192.0.0	/10	255.255.192.0	/18	255.255.255.192	/26
224.0.0.0	/3	255.224.0.0	/11	255.255.224.0	/19	255.255.255.224	/27
240.0.0.0	/4	255.240.0.0	/12	255.255.240.0	/20	255.255.255.240	/28
248.0.0.0	/5	255.248.0.0	/13	255.255.248.0	/21	255.255.255.248	/29
252.0.0.0	/6	255.252.0.0	/14	255.255.252.0	/22	255.255.255.252	/30
254.0.0.0	/7	255.254.0.0	/15	255.255.254.0	/23	255.255.255.254	/31

→ **Classe A** → **Classe B** → **Classe C**



IP público e privado

IP público é todo aquele que pode ser usado na Internet e é visível em toda a rede mundial de computadores. Já o IP privado é visível apenas dentro de uma rede particular, e não pode ser acessado por outros computadores da Internet. Além destes, existem ainda endereços IP reservados para fins específicos.

CIDR address block	Description	Reference
0.0.0.0/8	Current network (only valid as source address)	RFC 1700
10.0.0.0/8	Private network	RFC 1918
14.0.0.0/8	Public data networks	RFC 1700
127.0.0.0/8	Loopback	RFC 3330
128.0.0.0/16	Reserved (IANA)	RFC 3330
169.254.0.0/16	Link-Local	RFC 3927
172.16.0.0/12	Private network	RFC 1918
191.255.0.0/16	Reserved (IANA)	RFC 3330
192.0.0.0/24	Reserved (IANA)	RFC 3330
192.0.2.0/24	Documentation and example code	RFC 3330
192.88.99.0/24	IPv6 to IPv4 relay	RFC 3068
192.168.0.0/16	Private network	RFC 1918
198.18.0.0/15	Network benchmark tests	RFC 2544
223.255.255.0/24	Reserved (IANA)	RFC 3330
224.0.0.0/4	Multicasts (former Class D network)	RFC 3171
240.0.0.0/4	Reserved (former Class E network)	RFC 1700
255.255.255.255	Broadcast	

► Faixa de endereços IP privados.



Para saber mais...

- ... acesse o material online sobre Camada de Rede, do Prof. Dr. Romildo Martins da Silva Bezerra, do Instituto Federal de Educação, Ciência e Tecnologia da Bahia, Brasil
- ... acesse o material online sobre o Protocolo TCP/IP, do Prof. Dr. Nilton Alves Jr., do Centro de Pesquisas Físicas, Brasil.
- ... acesse o material online sobre TCP, UDP e Portas de Comunicação, de Júlio Battisti.

Módulo 3

Dynamic Host Configuration Protocol



Protocolo DHCP

O protocolo DHCP é usado para atribuir endereços IP e outras informações de conectividade de forma automática para os clientes de uma rede.

O DHCP é sucessor do protocolo BOOTP.



Requisitos para o servidor DHCP

O servidor DHCP, assim como qualquer outro servidor da rede, sempre deverá ter um IP fixo.

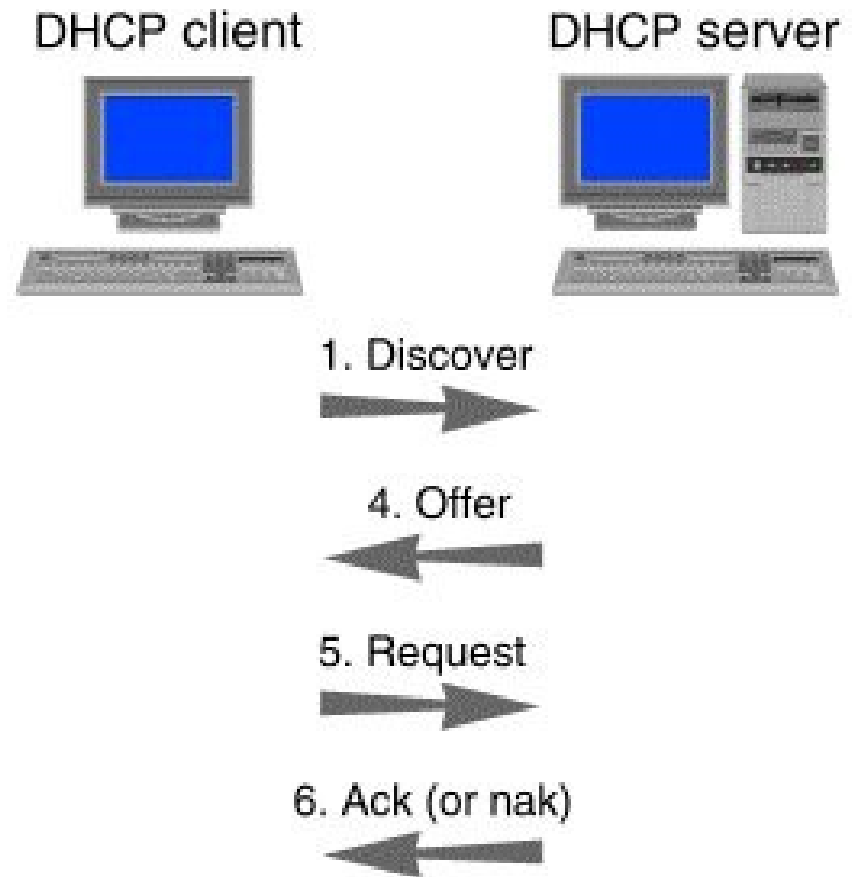
Para que os clientes possam obter configurações do servidor DHCP, é necessário que neste seja configurado o Escopo, que nada mais é que faixas de endereços IP's previamente planejadas que serão distribuídos aos clientes da rede.

Dentro de cada escopo, além da faixa de endereços IP, pode-se configurar também as exclusões, as reservas e as opções de escopo, como por exemplo o endereço do *default gateway* e dos servidores de nome.



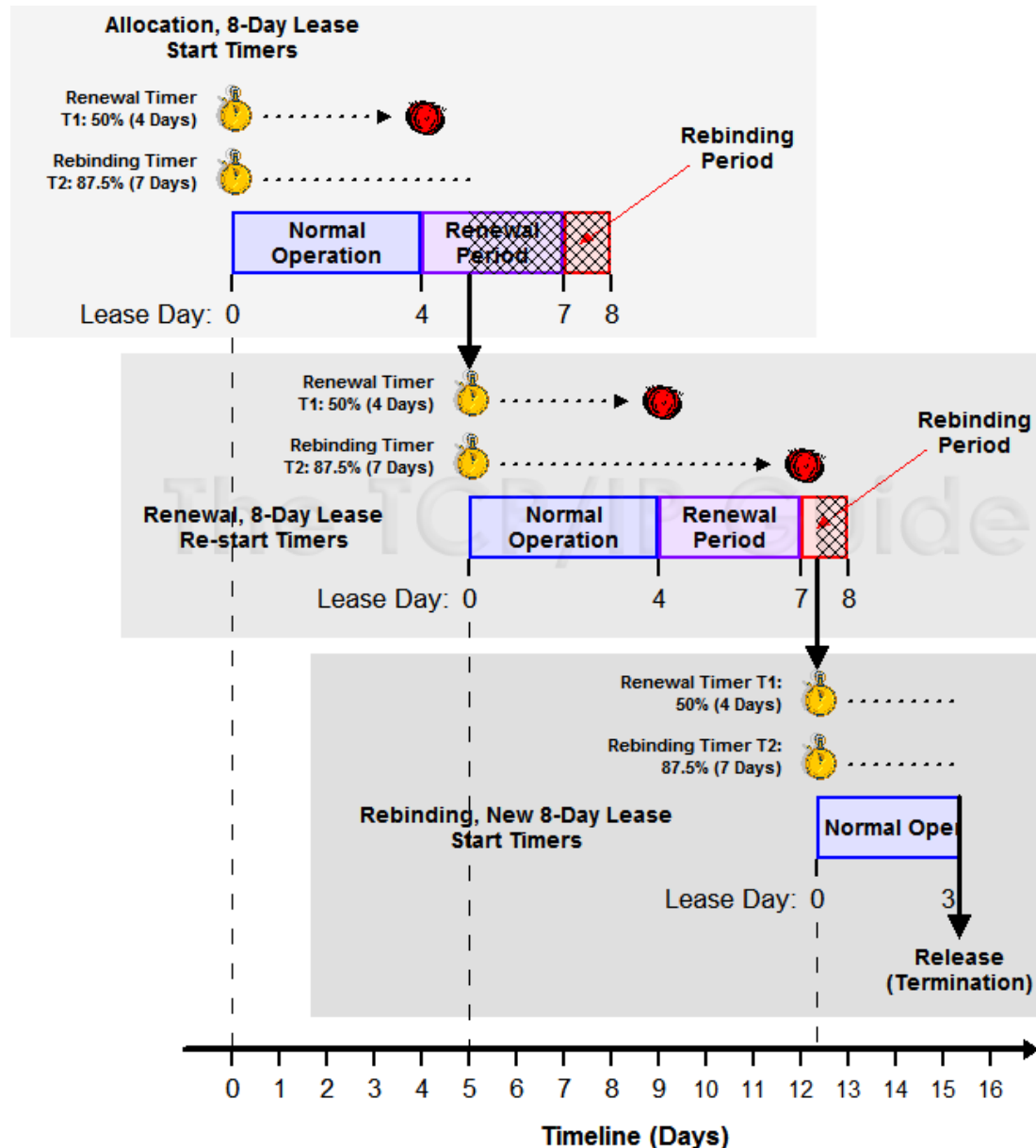
Passos na comunicação DHCP

- 1)O cliente envia para a rede uma mensagem DHCPDISCOVER;
- 2)O servidor DHCP da rede responde com a mensagem DHCPOFFER;
- 3)O cliente envia para a rede uma mensagem DHCPREQUEST;
- 4)O servidor DHCP responde com uma mensagem DHCPACK, que contém as configurações de IP, máscara, *default gateway*, etc.;
- 5)O cliente recebe a mensagem DHCPACK e usa os parâmetros contidos nela para configurar a conexão de rede;
- 6)Se o cliente receber uma mensagem DHCPNAK, todo o processo é reiniciado;
- 7)Caso o cliente não necessite mais das configurações, ele envia uma mensagem DHCPRELEASE para o servidor DHCP.





Ciclo de vida da alocação do DHCP





Para saber mais...

... acesse o material online sobre Dynamic Host Configuration Protocol, de Júlio Battisti.

... veja a animação online do funcionamento do protocolo DHCP, da RAD University.

Módulo 4

Network Address Translation



NAT

O mecanismo *Network Address Translation* foi criado para permitir que redes locais pudessem acessar a Internet sem a necessidade de ter um IP público para cada máquina, pois a quantidade de endereços IPv4 disponíveis estava esgotando-se rapidamente.

O NAT permite que uma rede local possa navegar na Internet usando uma quantidade de IP's públicos menor que a quantidade de máquinas.

O que o NAT faz é ocultar os endereços IP internos privados, convertendo-os em um ou mais endereços IP públicos do *firewall* ou do roteador de borda.

Os dados desta conversão ficam armazenados na tabela NAT.

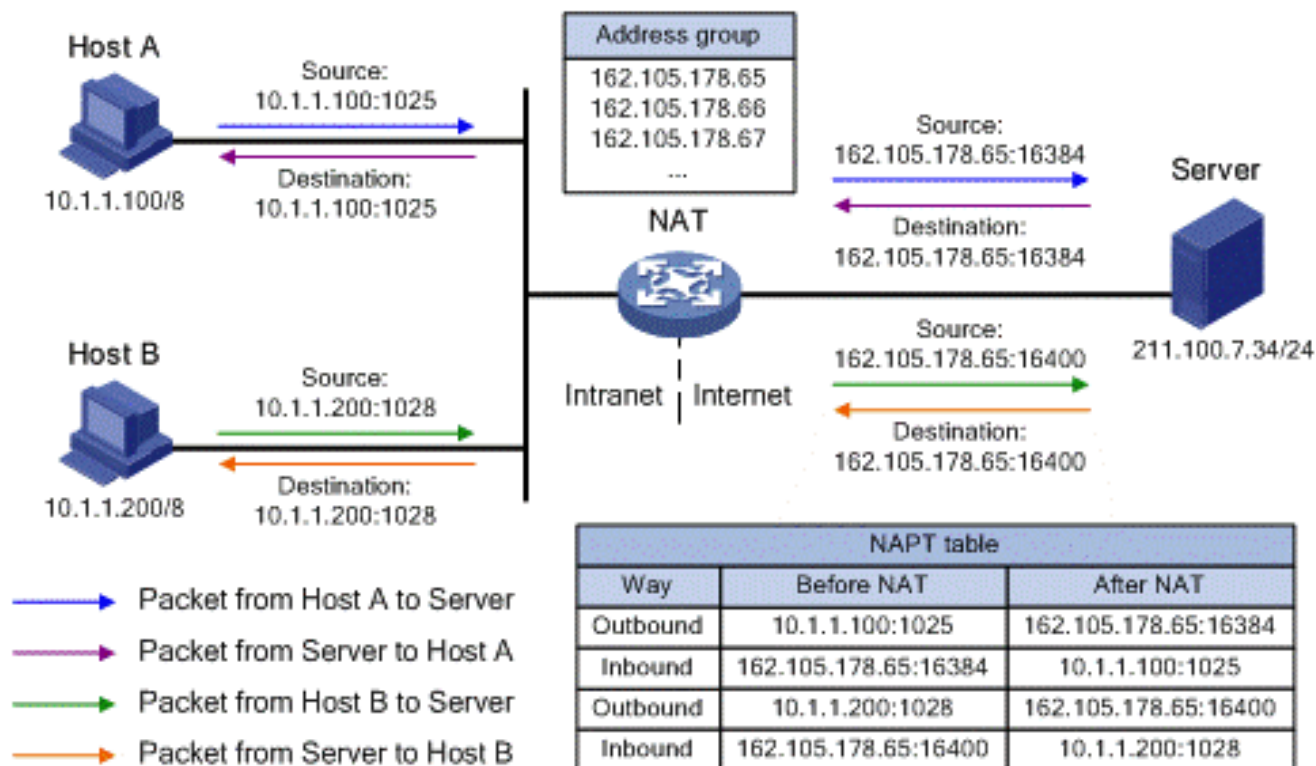


NAT

No exemplo abaixo, o Host A e o Host B possuem IP's privados, com os quais não é possível navegar na Internet.

Quando estas máquinas desejam acessar o IP público de um servidor externo, o roteador NAT faz a conversão dos IP's privados internos para o IP público 162.105.178.65.

Para que seja possível encaminhar corretamente os pacotes, o NAT mantém uma tabela associando o IP e a porta da máquina de origem com o IP e porta do roteador NAT.





Para saber mais...

... veja a animação online do funcionamento do NAT, da Cisco Systems, Inc.

... veja a animação online do funcionamento do NAT, de Greg Tomsho e Angela Poland

Módulo 5

Domain Name System



DNS

O Domain Name System é um banco de dados hierárquico que oferece o serviço de resolução de nomes URL (*Uniform Resource Locator*) usados para identificar um domínio.

Toda comunicação na Internet é feita por meio dos endereços IP, mas é muito mais fácil memorizar URL's do que endereços IP.

Assim, o que o serviço de DNS faz é converter as URL's em endereços IP:

`www.brasil.gov.br` → 161.148.172.106

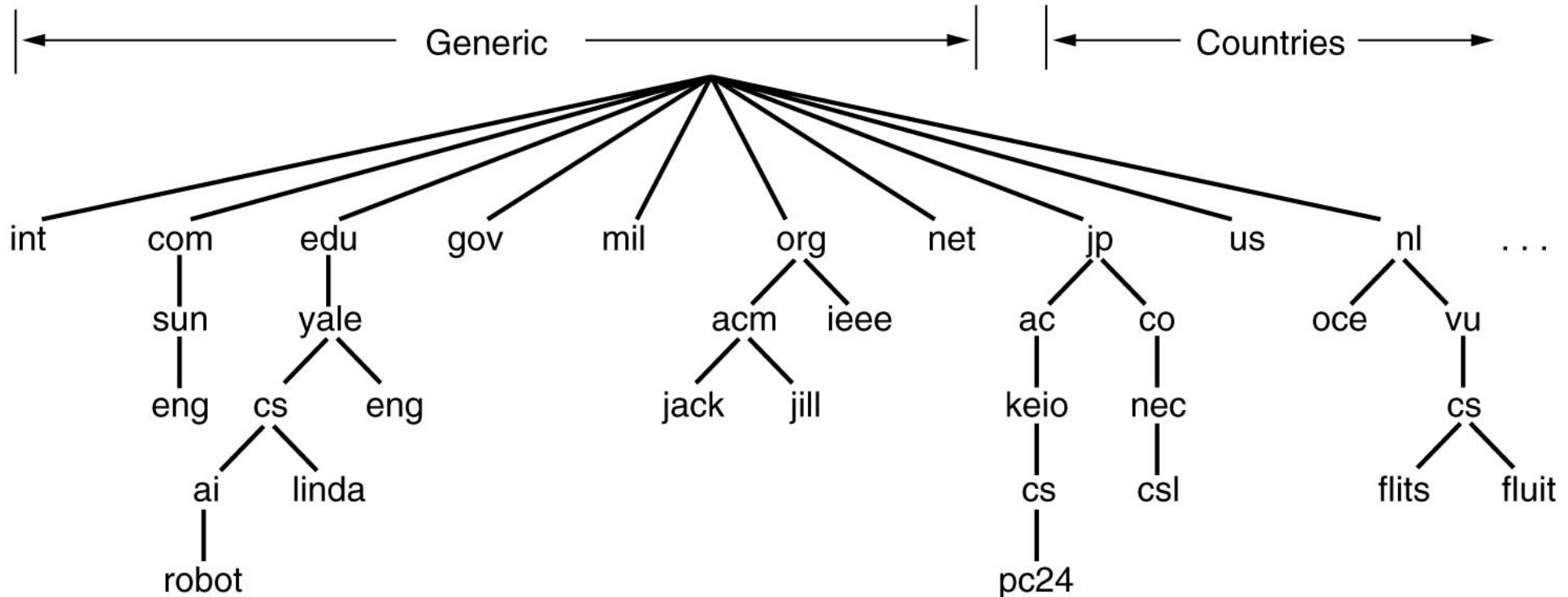
`www.tj.sp.gov.br` → 200.142.86.230

`www.google.com` → 190.98.170.103



DNS

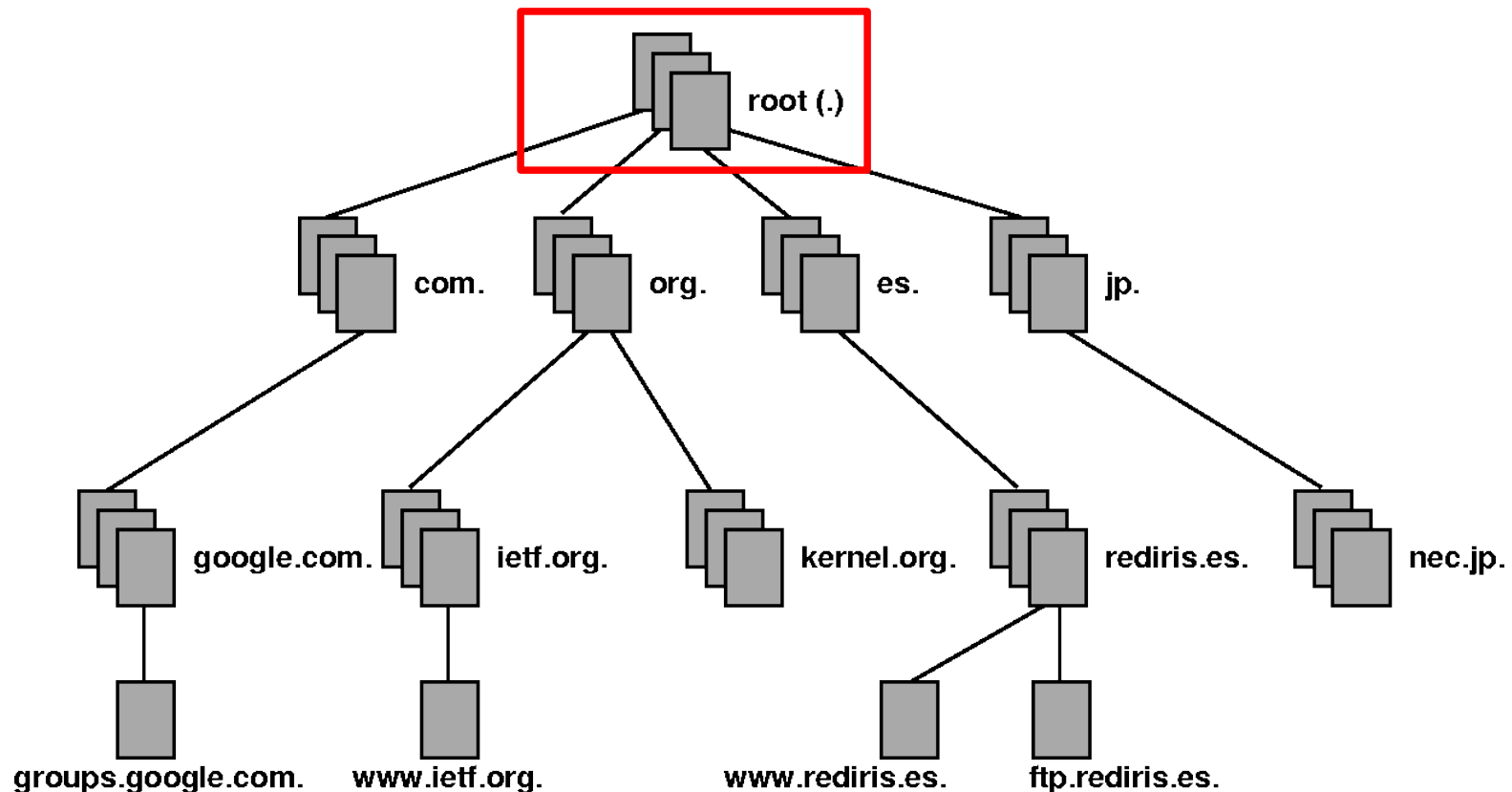
Os nomes de domínio servem para identificar uma rede ou grupo de computadores. Estão dispostos de forma hierárquica e geralmente possuem um ou mais servidores DNS responsáveis por mapear todos os nomes abaixo daquele domínio (ou subdomínio) em endereços IP.





DNS – root server

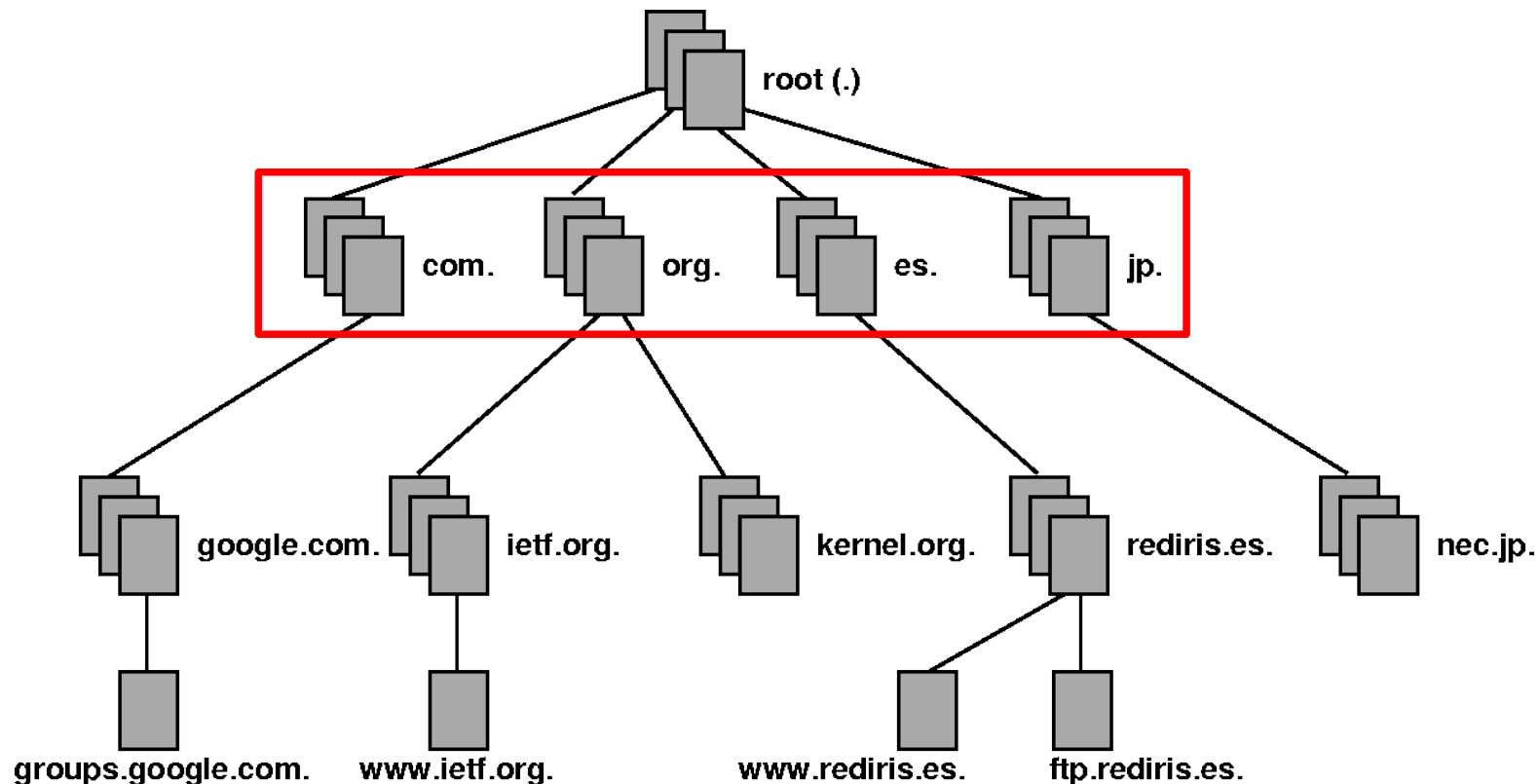
O ponto mais alto da cadeia é denominado *root*. O servidor DNS responsável por este ponto é o *root server*. Este servidor possui todas as entradas para os servidores imediatamente abaixo dele.





DNS – top-level domain

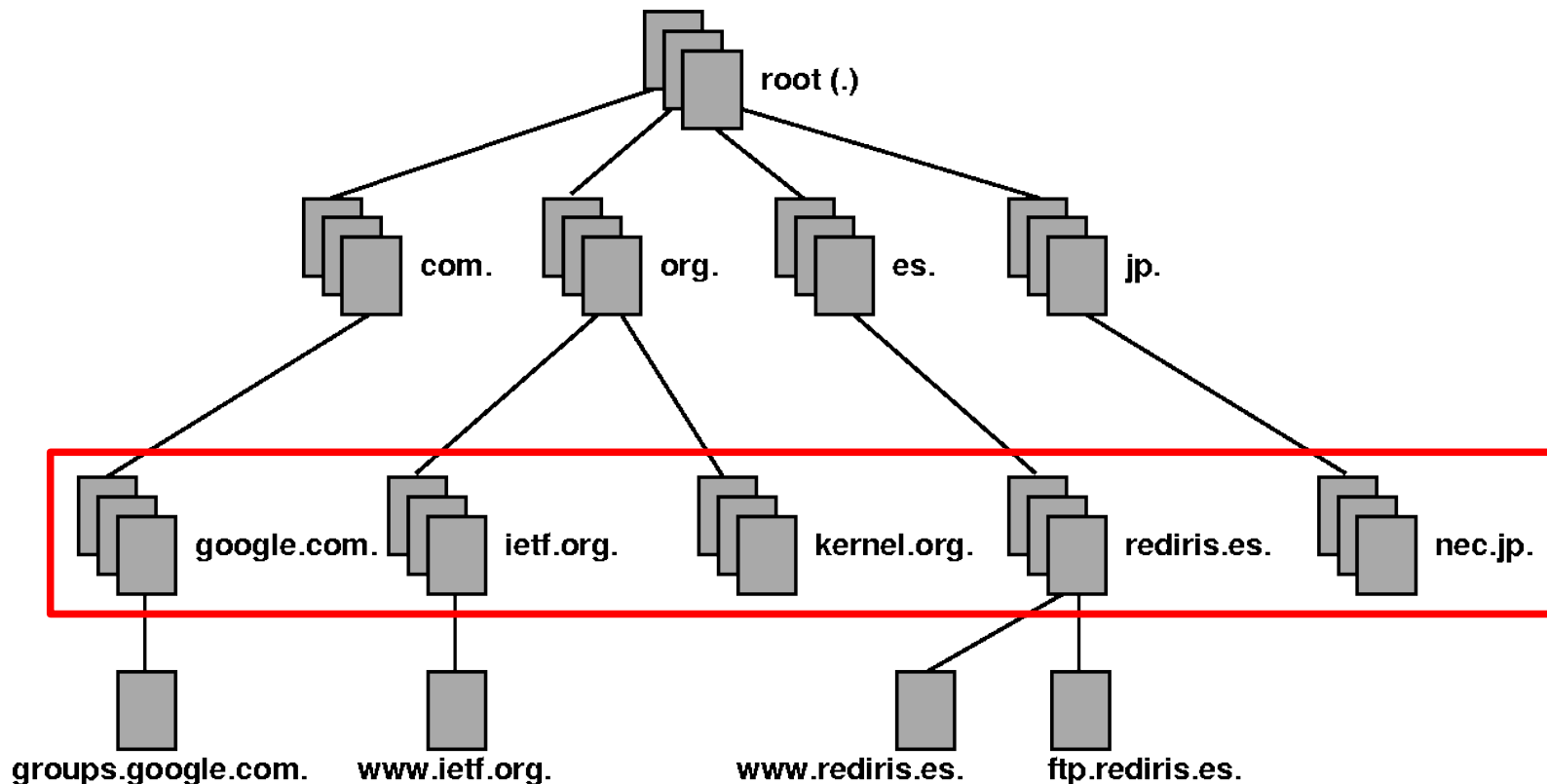
Os *Top-level Domain* identificam domínios genéricos, como .com ou .gov, e domínios de países, como .br, .jp, .it, etc. O servidor DNS responsável por este ponto é o *TLD server*. Este servidor possui todas as entradas para os servidores imediatamente abaixo dele.





DNS – authoritative server

Os servidores autoritativos são responsáveis pelas empresas ou organizações que representam. O servidor DNS responsável por este ponto é o *authorative server*. Este servidor possui todas as entradas para os servidores e demais *hosts* dentro da organização.





Root server

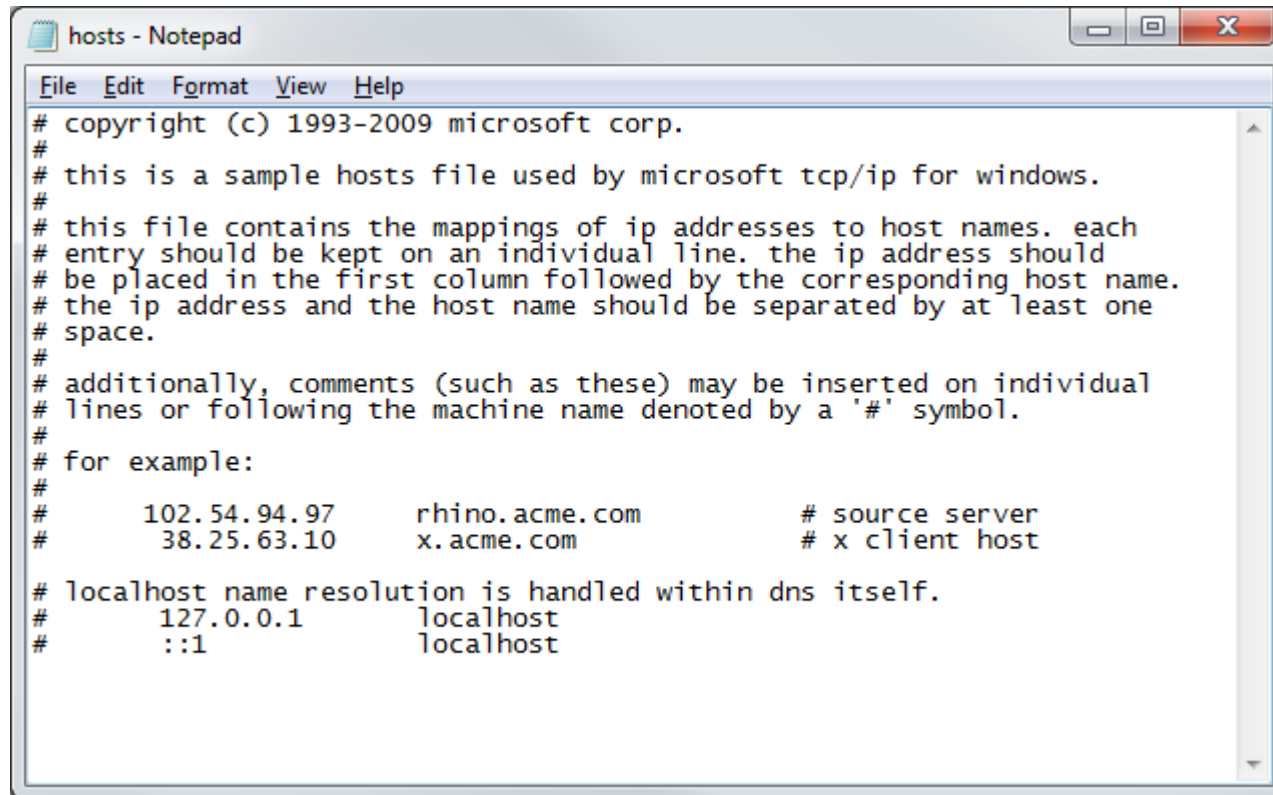
Os *root servers* são servidores DNS que possuem informações sobre os servidores *top-level domain*. São os primeiros a serem consultados. Ao todo são treze servidores.

NOME	IP	OPERADOR
a.root-servers.net	198.41.0.4	Verisign
b.root-servers.net	192.228.79.201	USC-ISI
c.root-servers.net	192.33.4.12	Cogent Communications
d.root-servers.net	199.7.91.13	University of Maryland
e.root-servers.net	192.203.230.10	NASA
f.root-servers.net	192.5.5.241	Internet Systems Consortium
g.root-servers.net	192.112.36.4	Defense Information Systems Agency
h.root-servers.net	128.63.2.53	U.S. Army Research Lab
i.root-servers.net	192.36.148.17	Netnod
j.root-servers.net	192.58.128.30	Verisign
k.root-servers.net	193.0.14.129	RIPE NCC
l.root-servers.net	199.7.83.42	ICANN
m.root-servers.net	202.12.27.33	WIDE Project



Arquivo hosts

O arquivo hosts c:\windows\system32\drivers\etc



```
hosts - Notepad
File Edit Format View Help
# copyright (c) 1993-2009 microsoft corp.
#
# this is a sample hosts file used by microsoft tcp/ip for windows.
#
# this file contains the mappings of ip addresses to host names. each
# entry should be kept on an individual line. the ip address should
# be placed in the first column followed by the corresponding host name.
# the ip address and the host name should be separated by at least one
# space.
#
# additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# for example:
#
#      102.54.94.97      rhino.acme.com      # source server
#      38.25.63.10      x.acme.com         # x client host
#
# localhost name resolution is handled within dns itself.
#      127.0.0.1        localhost
#      ::1              localhost
```

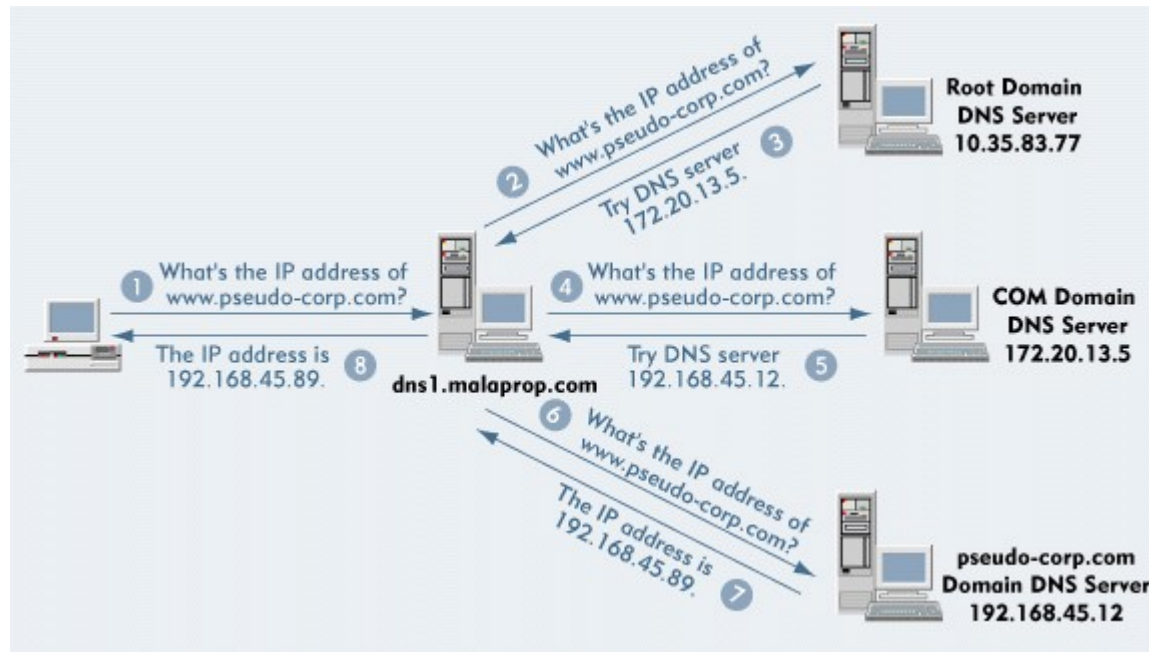



DNS – resolução de nomes

O Domain Name System é um banco de dados hierárquico que oferece o serviço de resolução de nomes URL (*Uniform Resource Locator*).

Toda comunicação na Internet é feita por meio dos endereços IP, mas é muito mais fácil memorizar URL's do que endereços IP.

Assim, o que o serviço de DNS faz é converter as URL's em endereços IP:





DNS – Ferramentas

Nslookup.....



Para saber mais...

- ... leia o material online sobre Domain Name System, de Júlio Battisti.
- ... veja a animação online do funcionamento do protocolo DNS, da RAD University.
- ... leia o tutorial DNS apresentado no 3º PTT Fórum, do registro.br.
- ... veja a lista de Top-Level Domains, da Internet Assigned Numbers Authority (IANA).
- ... veja a lista de Domínios de Segundo Nível do Brasil, do registro.br.

Módulo 6

File Transfer Protocol



Introdução

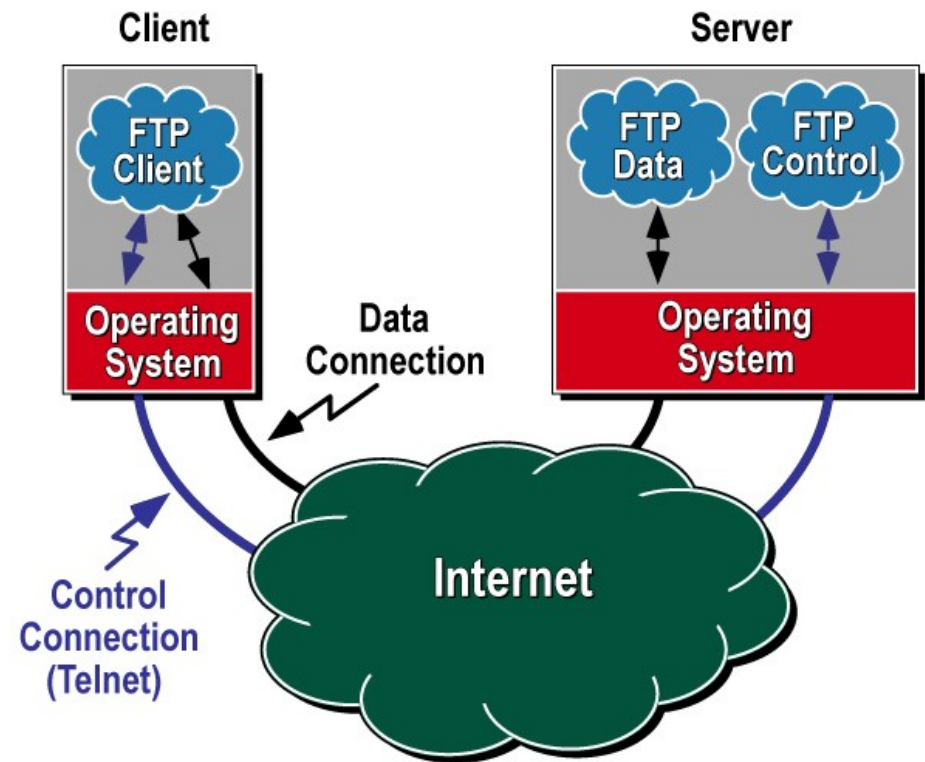
O protocolo FTP (File Transfer Protocol) é usado para transferir arquivos usando como método de transporte o protocolo TCP. É baseado no modelo cliente/servidor e usa duas conexões, uma para dados e outra para controle.



FTP

Quando o cliente FTP deseja conectar-se ao servidor FTP, é realizada uma conexão TCP na porta 21 do servidor, denominada conexão de controle. É por esta conexão que serão enviados e recebidos os comandos de listagem e cópias de arquivos, por exemplo.

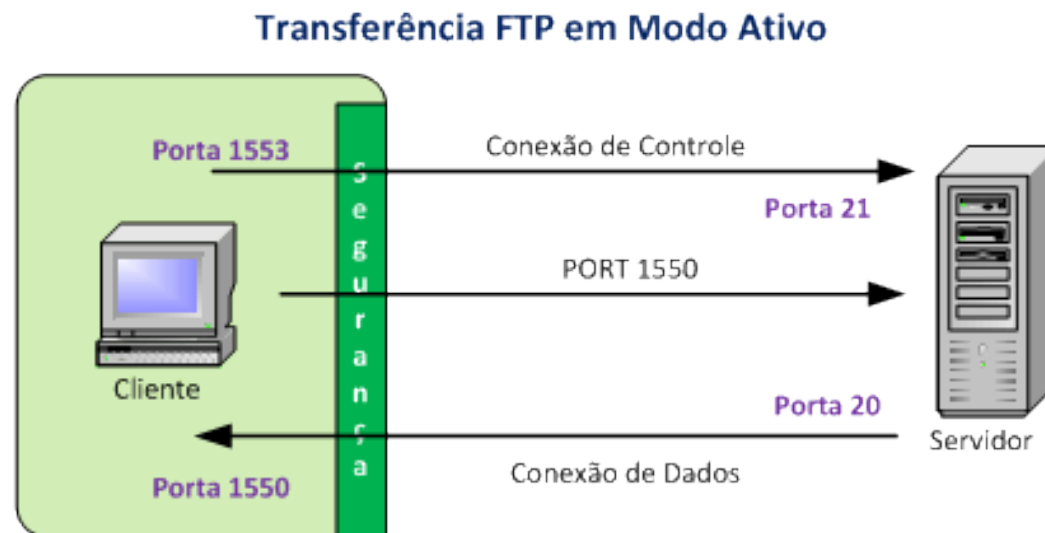
Quando o cliente realiza uma cópia ou envio de arquivo, uma nova conexão TCP é aberta, desta vez na porta 20 do servidor, por onde irão trafegar os arquivos.





FTP – Modo ativo

No modo ativo a conexão é gerenciada pelo cliente FTP. Neste caso, após estabelecer uma conexão TCP na porta 21 do servidor, o cliente envia um comando PORT seguido do número da porta onde o servidor deverá estabelecer a conexão de dados.



Cliente se conecta à porta 21 do Servidor usando a porta 1553 (conexão de Controle)

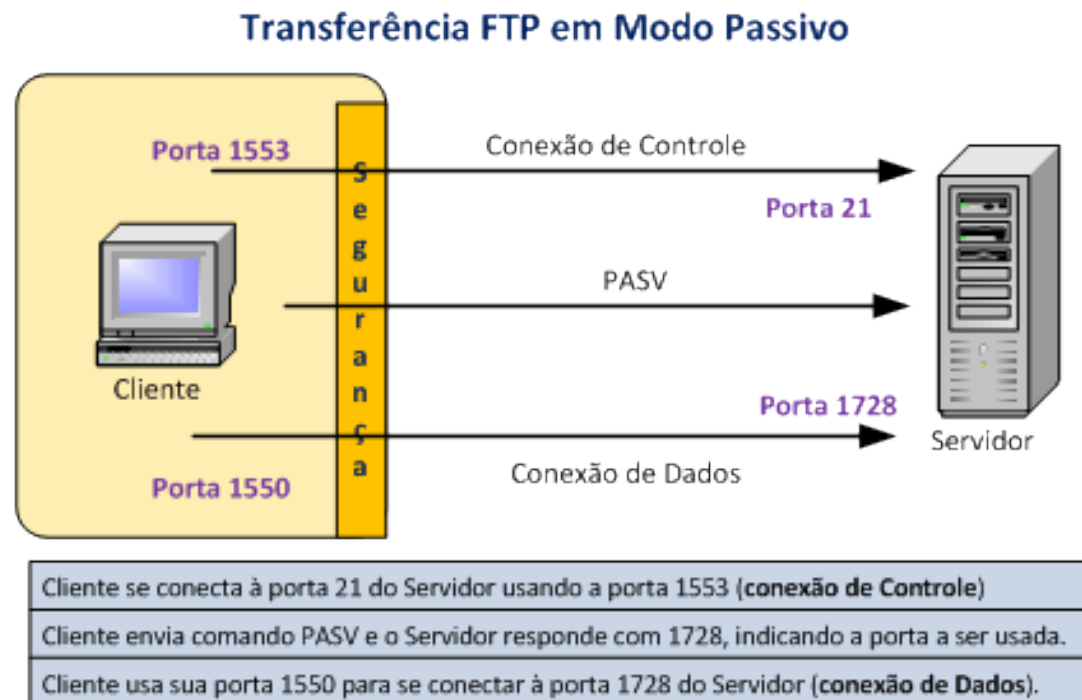
Cliente envia comando PORT 1550, notificando ao Servidor qual porta deve ser usada

Servidor usa sua porta 20 para se conectar à porta 1550 do Cliente (conexão de Dados).



FTP – Modo passivo

No modo passivo a conexão é gerenciada pelo servidor FTP. Neste caso, após estabelecer uma conexão TCP na porta 21 do servidor, o cliente envia um comando PASV e espera uma resposta do servidor indicando qual porta deverá ser usada para transmissão de dados.





FTP – Ferramentas

No modo passivo a conexão é gerenciada pelo servidor FTP. Neste caso, após estabelecer uma conexão TCP na porta 21 do servidor, o cliente envia um comando PASV e espera uma resposta do servidor indicando qual porta deverá ser usada para transmissão de dados.



Para saber mais...

... leia o tutorial Serviço de FTP, de Gerson Konnus.

... leia o tutorial How to set up an FTP Server in Windows 2000, da Microsoft Corporation.

Módulo 7

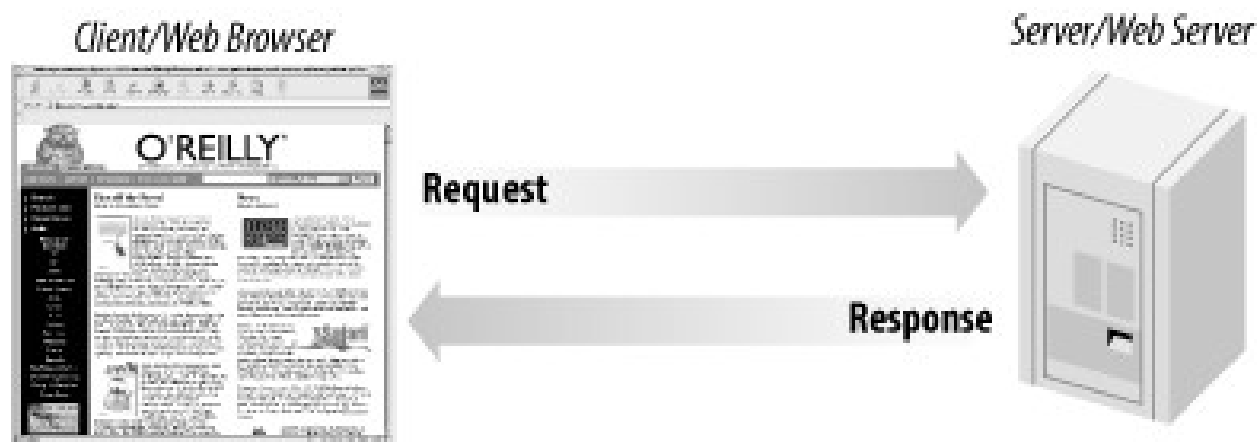
Hypertext Transfer Protocol



HTTP

O Hypertext Transfer Protocol, ou Protocolo de Transferência de Hipertexto, é usado para transferência de dados do tipo hipertexto, que nada mais é que um texto estruturado que pode conter elementos de multimídia como som e imagem e que utiliza ligações lógicas para outros textos.

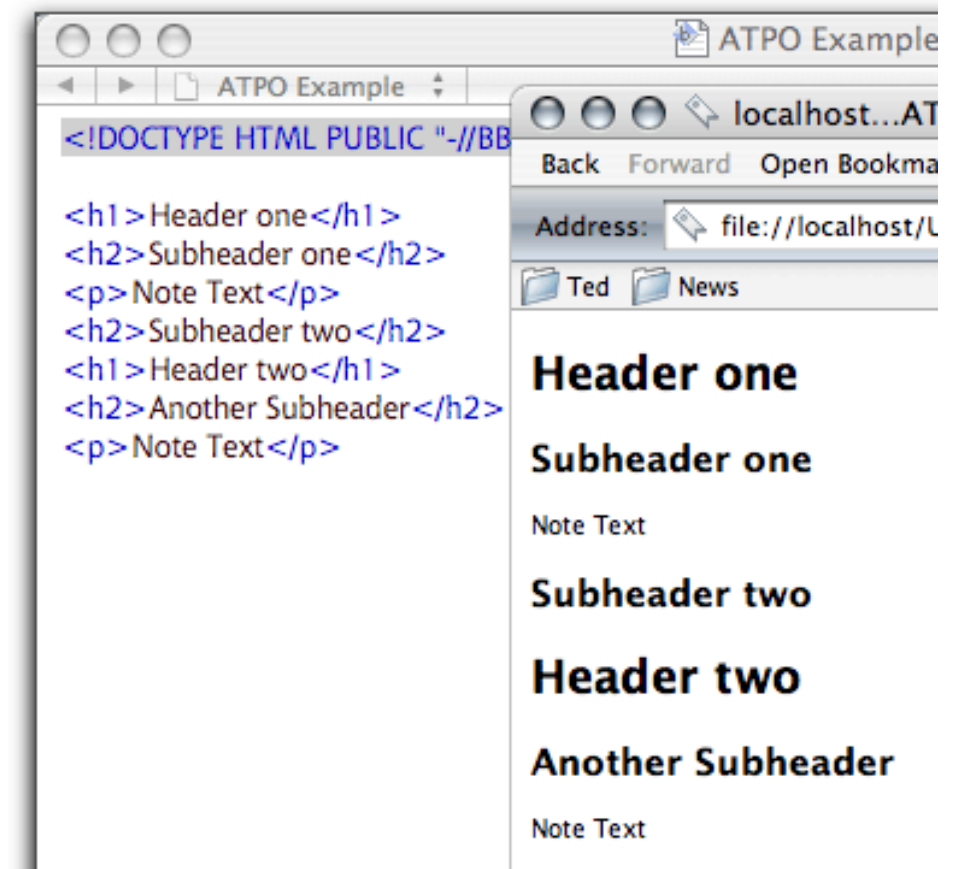
O protocolo HTTP trabalha no modelo cliente/servidor, e podem ser transferidos dados do tipo texto claro, HTML, som, imagens, entre outros.





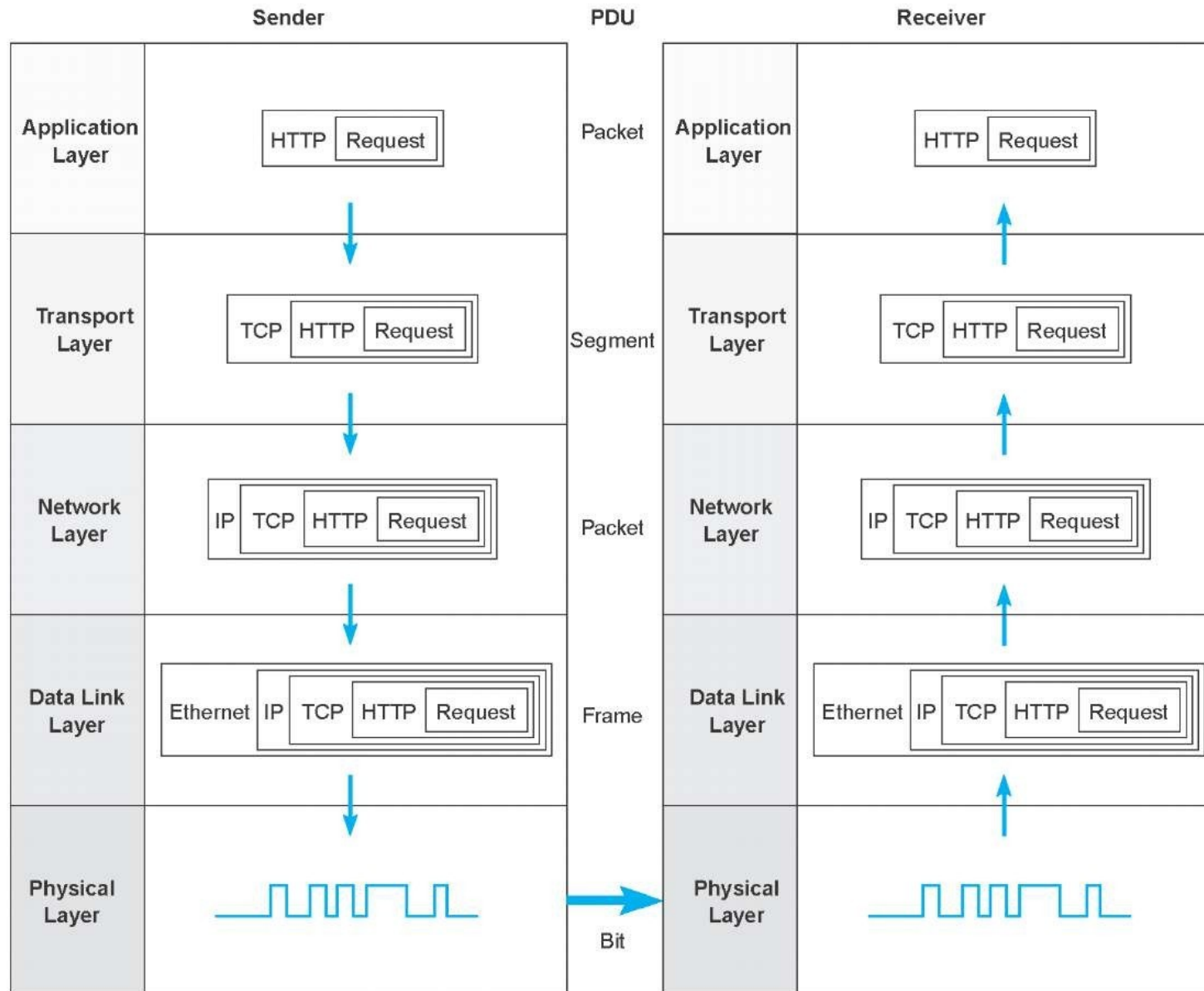
HTML

O HyperText Markup Language, ou Linguagem de Marcação de Hipertexto é usado para formatar páginas Web. A linguagem HTML é interpretada pelos navegadores Web.





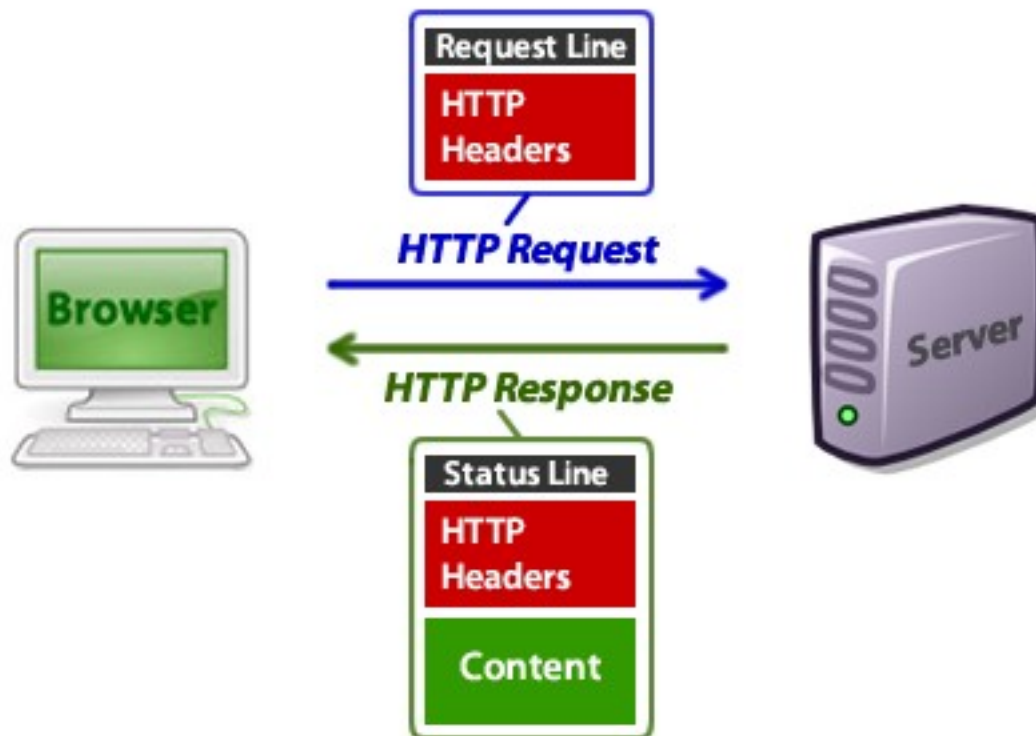
HTTP – PDU





HTTP

Uma sessão HTTP inicia com a requisição do cliente, que envia uma mensagem HTTP Request. O servidor Web configurado por padrão na porta 80 captura a requisição e envia uma mensagem HTTP Response, que contém o cabeçalho da resposta e os dados do recurso requisitado.





HTTP – Estrutura de requisição

A estrutura do pedido de requisição pode ser dividida em quatro partes:

- O método (method) indica o tipo de requisição. Os mais comuns são GET, POST e HEAD;
- O caminho (path) é a localização do recurso que se deseja recuperar. Pode ser uma página HTML, uma imagem, arquivo de áudio, etc;
- O protocolo (protocol) contém a versão do protocolo HTTP que o navegador está usando;
- O cabeçalho (header) HTTP contém várias informações sobre a requisição e o navegador Web.

method	path	protocol
GET	/tutorials/other/top-20-mysql-best-practices/	HTTP/1.1

```
Host: net.tutsplus.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: PHPSESSID=r2t5uvjq435r4q7ib3vtdjq120
Pragma: no-cache
Cache-Control: no-cache
```

HTTP headers as Name: Value



HTTP – Métodos

O método usado pelo protocolo HTTP para o pedido de requisição pode ser do tipo:

- GET – método usado para recuperar as informações sobre um determinado recurso e o próprio recurso;
- POST – método usado para recuperar apenas as informações sobre um determinado recurso;
- HEAD – método usado para enviar informações do cliente para o servidor. Usado em preenchimento de formulário, por exemplo.



HTTP – Estrutura de Resposta

A estrutura do pedido de resposta pode ser dividida em três partes:

- O protocol (protocol) contém a versão do protocolo HTTP que o servidor está usando;
- O código de estado (status code) indica, entre outras coisas, se a requisição foi ou não atendida com sucesso;
- O cabeçalho (header) HTTP contém várias informações sobre a resposta e o servidor Web.

```
protocol      status code
HTTP/1.1      200 OK
Transfer-Encoding: chunked
Date: Sat, 28 Nov 2009 04:36:25 GMT
Server: LiteSpeed
Connection: close
X-Powered-By: W3 Total Cache/0.8
Pragma: public
Expires: Sat, 28 Nov 2009 05:36:25 GMT
Etag: "pub1259380237;gz"
Cache-Control: max-age=3600, public
Content-Type: text/html; charset=UTF-8
Last-Modified: Sat, 28 Nov 2009 03:50:37 GMT
X-Pingback: http://net.tutsplus.com/xmlrpc.php
Content-Encoding: gzip
Vary: Accept-Encoding, Cookie, User-Agent
```

HTTP headers as Name: Value



HTTP – Códigos de estado

HTTP Status Codes				
For great REST services the correct usage of the correct HTTP status code in a response is vital.				
1xx – Informational	2xx – Successful	3xx – Redirection	4xx – Client Error	5xx – Server Error
This class of status code indicates a provisional response, consisting only of the Status-Line and optional headers, and is terminated by an empty line	This class of status code indicates that the client's request was successfully received, understood, and accepted.	This class of status code indicates that further action needs to be taken by the user agent in order to fulfill the request.	The 4xx class of status code is intended for cases in which the client seems to have erred.	Response status codes beginning with the digit "5" indicate cases in which the server is aware that it has erred or is incapable of performing the request.
100 – Continue 101 – Switching Protocols 102 – Processing	200 – OK 201 – Created 202 – Accepted 203 – Non-Authoritative Information 204 – No Content 205 – Reset Content 206 – Partial Content 207 – Multi-Status	300 – Multiple Choices 301 – Moved Permanently 302 – Found 303 – See Other 304 – Not Modified 305 – Use Proxy 307 – Temporary Redirect	400 – Bad Request 401 – Unauthorised 402 – Payment Required 403 – Forbidden 404 – Not Found 405 – Method Not Allowed 406 – Not Acceptable 407 – Proxy Authentication Required 408 – Request Timeout 409 – Conflict 410 – Gone 411 – Length Required 412 – Precondition Failed 413 – Request Entity Too Large 414 – Request URI Too Long 415 – Unsupported Media Type 416 – Requested Range Not Satisfiable 417 – Expectation Failed 422 – Unprocessable Entity 423 – Locked 424 – Failed Dependency 425 – Unordered Collection 426 – Upgrade Required	500 – Internal Server Error 501 – Not Implemented 502 – Bad Gateway 503 – Service Unavailable 504 – Gateway Timeout 505 – HTTP Version Not Supported 506 – Variant Also Negotiates 507 – Insufficient Storage 510 – Not Extended

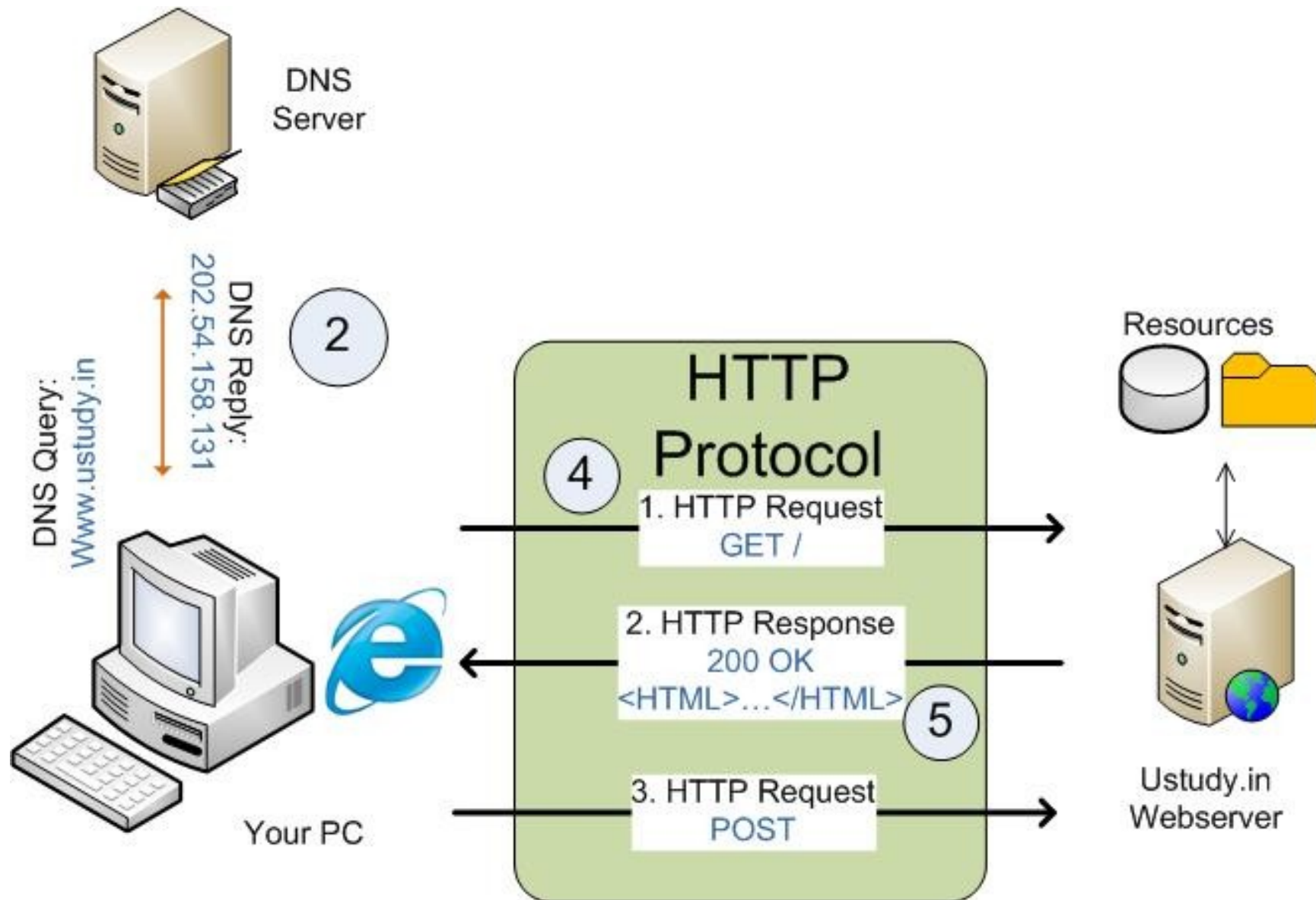
Examples of using HTTP Status Codes in REST	
201 – When doing a POST to create a new resource it is best to return 201 and not 200.	
204 – When deleting a resources it is best to return 204, which indicates it succeeded but there is no body to return.	
301 – If a 301 is returned the client should update any cached URI's to point to the new URI.	
302 – This is often used for temporary redirect's, however 303 and 307 are better choices.	
409 – This provides a great way to deal with conflicts caused by multiple updates.	
501 – This implies that the feature will be implemented in the future.	

Special Cases	
306 – This status code is no longer used. It used to be for switch proxy.	
418 – This status code from RFC 2324. However RFC 2324 was submitted as an April Fools' Joke. The message is <i>I am a teapot</i> .	

Key	Description
Black	HTTP version 1.0
Blue	HTTP version 1.1
Aqua	Extension RFC 2295
Green	Extension RFC 2518
Yellow	Extension RFC 2774
Orange	Extension RFC 2817
Purple	Extension RFC 3648
Red	Extension RFC 4918



HTTP – Exemplo



```
josh@blackbox:~$ telnet en.wikipedia.org 80
```

```
Trying 208.80.152.2...
```

```
Connected to rr.pmtpa.wikimedia.org.
```

```
Escape character is '^['.
```

```
GET /wiki/Main_Page http/1.1
```

```
Host: en.wikipedia.org
```

```
HTTP/1.0 200 OK
```

```
Date: Thu, 03 Jul 2008 11:12:06 GMT
```

```
Server: Apache
```

```
X-Powered-By: PHP/5.2.5
```

```
Cache-Control: private, s-maxage=0, max-age=0, must-revalidate
```

```
Content-Language: en
```

```
Vary: Accept-Encoding, Cookie
```

```
X-Vary-Options: Accept-Encoding;list-contains=gzip, Cookie;string-contains=enwikiToken;string-contains=enwikiLoggedOut;string-contains=enwikiToken;string-contains=centralauth_Token;string-contains=centralauth_Session;string-contains=centralauth_LoggedOut
```

```
Last-Modified: Thu, 03 Jul 2008 10:44:34 GMT
```

```
Content-Length: 54218
```

```
Content-Type: text/html; charset=utf-8
```

```
X-Cache: HIT from sq39.wikimedia.org
```

```
X-Cache-Lookup: HIT from sq39.wikimedia.org:3128
```

```
Age: 3
```

```
X-Cache: HIT from sq38.wikimedia.org
```

```
X-Cache-Lookup: HIT from sq38.wikimedia.org:80
```

```
Via: 1.0 sq39.wikimedia.org:3128 (squid/2.6.STABLE18), 1.0 sq38.wikimedia.org:80 (squid/2.6.STABLE18)
```

```
Connection: close
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

```
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en" dir="ltr">
```

```
<head>
```

```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
```

```
<meta name="keywords" content="Main Page,1778,1844,1863,1938,1980 Summer Olympics,2008,2008 Guizhou riot,2008
```

```
...
```

```
... This content has been removed to save space
```

```
...
```

```
"Non-profit organization">nonprofit</a> <a href="http://en.wikipedia.org/wiki/Charitable_organization" title="Charitable organization">charitable organization</a></li>
```

```
<li id="privacy"><a href="http://wikimediafoundation.org/wiki/Privacy_policy" title="wikimedia:Privacy policy">Privacy policy</a></li>
```

```
<li id="about"><a href="/wiki/Wikipedia:About" title="Wikipedia:About">About Wikipedia</a></li>
```

```
<li id="disclaimer"><a href="/wiki/Wikipedia:General_disclaimer" title="Wikipedia:General disclaimer">Disclaimer</a></li>
```

```
</li>
```

```
</ul>
```

```
</div>
```

```
</div>
```

```
<script type="text/javascript">if (window.runOnloadHook) runOnloadHook();</script>
```

```
<!-- Served by srv93 in 0.050 secs. --></body></html>
```

```
Connection closed by foreign host.
```

```
josh@blackbox:~$
```

Response h

Respons



HTTP – Exemplo

No exemplo a seguir é demonstrado como acessar um site usando o TELNET ao invés de um cliente Web comum.

```
josh@blackbox:~$ telnet en.wikipedia.org 80
Trying 208.80.152.2...
Connected to rr.pmtpa.wikimedia.org.
Escape character is '^J'.
GET /wiki/Main_Page http/1.1
Host: en.wikipedia.org

HTTP/1.0 200 OK
Date: Thu, 03 Jul 2008 11:12:06 GMT
Server: Apache
X-Powered-By: PHP/5.2.5
Cache-Control: private, s-maxage=0, max-age=0, must-revalidate
Content-Language: en
Vary: Accept-Encoding, Cookie
X-Vary-Options: Accept-Encoding;list-contains=gzip, Cookie;string-contains=enwikiToken;string-contains=enwikiLoggedOut;string-contains=enwiki_session;string-contains=centralauth_Token;string-contains=centralauth_Session;string-contains=centralauth_LoggedOut
Last-Modified: Thu, 03 Jul 2008 10:44:34 GMT
Content-Length: 54218
Content-Type: text/html; charset=utf-8
X-Cache: HIT from sq39.wikimedia.org
X-Cache-Lookup: HIT from sq39.wikimedia.org:3128
Age: 3
X-Cache: HIT from sq38.wikimedia.org
X-Cache-Lookup: HIT from sq38.wikimedia.org:80
Via: 1.0 sq39.wikimedia.org:3128 (squid/2.6.STABLE18), 1.0 sq38.wikimedia.org:80 (squid/2.6.STABLE18)
Connection: close

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en" dir="ltr">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <meta name="keywords" content="Main Page,1778,1844,1863,1938,1980 Summer Olympics,2008,2008 Guizhou riot,2008 Jerusal
    ...
    ... This content has been removed to save space
    ...
    "Non-profit organization">nonprofit</a> <a href="http://en.wikipedia.org/wiki/Charitable_organization" title="Charitable organization">charity</a>.<b
    r /></li>
      <li id="privacy"><a href="http://wikimediafoundation.org/wiki/Privacy_policy" title="wikimedia:Privacy policy">Privac
    y policy</a></li>
      <li id="about"><a href="/wiki/Wikipedia:About" title="Wikipedia:About">About Wikipedia</a></li>
      <li id="disclaimer"><a href="/wiki/Wikipedia:General_disclaimer" title="Wikipedia:General disclaimer">Disclaimers</a>
    </li>
    </ul>
  </div>
</div>

  <script type="text/javascript">if (window.runOnLoadHook) runOnLoadHook();</script>
<!-- Served by srv93 in 0.050 secs. --></body></html>
Connection closed by foreign host.
josh@blackbox:~$
```




HTTP – Exemplo

O usuário conecta-se ao site Web usando o comando TELNET no console por meio do comando:

```
telnet en.wikipedia.org 80
```

```
josh@blackbox:~$ telnet en.wikipedia.org 80
Trying 208.80.152.2...
Connected to rr.pmtpa.wikimedia.org.
Escape character is '^]'.
```



HTTP – Exemplo

O usuário deseja recuperar o recurso `/wiki/Main_Page` por meio dos comandos:

```
GET /wiki/Main_Page http/1.1
```

```
Host: en.wikipedia.org
```

```
GET /wiki/Main_Page http/1.1  
Host: en.wikipedia.org
```

Request



HTTP – Exemplo

O servidor responde com um código de estado 200 OK, indicando que a página existe, bem como o cabeçalho de resposta.

```
HTTP/1.0 200 OK
Date: Thu, 03 Jul 2008 11:12:06 GMT
Server: Apache
X-Powered-By: PHP/5.2.5
Cache-Control: private, s-maxage=0, max-age=0, must-revalidate
Content-Language: en
Vary: Accept-Encoding, Cookie
X-Vary-Options: Accept-Encoding;list-contains=gzip, Cookie;string-contains=enwikiToken;string-contains=enwikiLoggedOut;string-contains=enwiki_session;string-contains=centralauth_Token;string-contains=centralauth_Session;string-contains=centralauth_LoggedOut
Last-Modified: Thu, 03 Jul 2008 10:44:34 GMT
Content-Length: 54218
Content-Type: text/html; charset=utf-8
X-Cache: HIT from sq39.wikimedia.org
X-Cache-Lookup: HIT from sq39.wikimedia.org:3128
Age: 3
X-Cache: HIT from sq38.wikimedia.org
X-Cache-Lookup: HIT from sq38.wikimedia.org:80
Via: 1.0 sq39.wikimedia.org:3128 (squid/2.6.STABLE18), 1.0 sq38.wikimedia.org:80 (squid/2.6.STABLE18)
Connection: close
```

Response headers



HTTP – Exemplo

O servidor responde com o conteúdo do recurso solicitado no formato HTML.

Response body

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en" dir="ltr">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <meta name="keywords" content="Main Page,1778,1844,1863,1938,1980 Summer Olympics,2008,2008 Guizhou riot,2008 Jerusal
  ...
  ... This content has been removed to save space
  ...
  "Non-profit organization">nonprofit</a> <a href="http://en.wikipedia.org/wiki/Charitable_organization" title="Charitable organization">charity</a>.<b
r /></li>
    <li id="privacy"><a href="http://wikimediafoundation.org/wiki/Privacy_policy" title="wikimedia:Privacy policy">Privac
y policy</a></li>
    <li id="about"><a href="/wiki/Wikipedia:About" title="Wikipedia:About">About Wikipedia</a></li>
    <li id="disclaimer"><a href="/wiki/Wikipedia:General_disclaimer" title="Wikipedia:General disclaimer">Disclaimers</a>
  </li>
  </ul>
</div>
</div>
  <script type="text/javascript">if (window.runOnloadHook) runOnloadHook();</script>
<!-- Served by srv93 in 0.050 secs. --></body></html>
```



HTTP – Exemplo

O servidor encerra a conexão.

```
Connection closed by foreign host.  
josh@blackbox:~$
```



Para saber mais...

... acesse o visualizador de Cabeçalho de Requisição e Resposta HTTP web-sniffer.net.

... acesse o visualizador de Cabeçalho de Requisição e Resposta HTTP web-sniffer.me.

Módulo 8

Correio Eletrônico



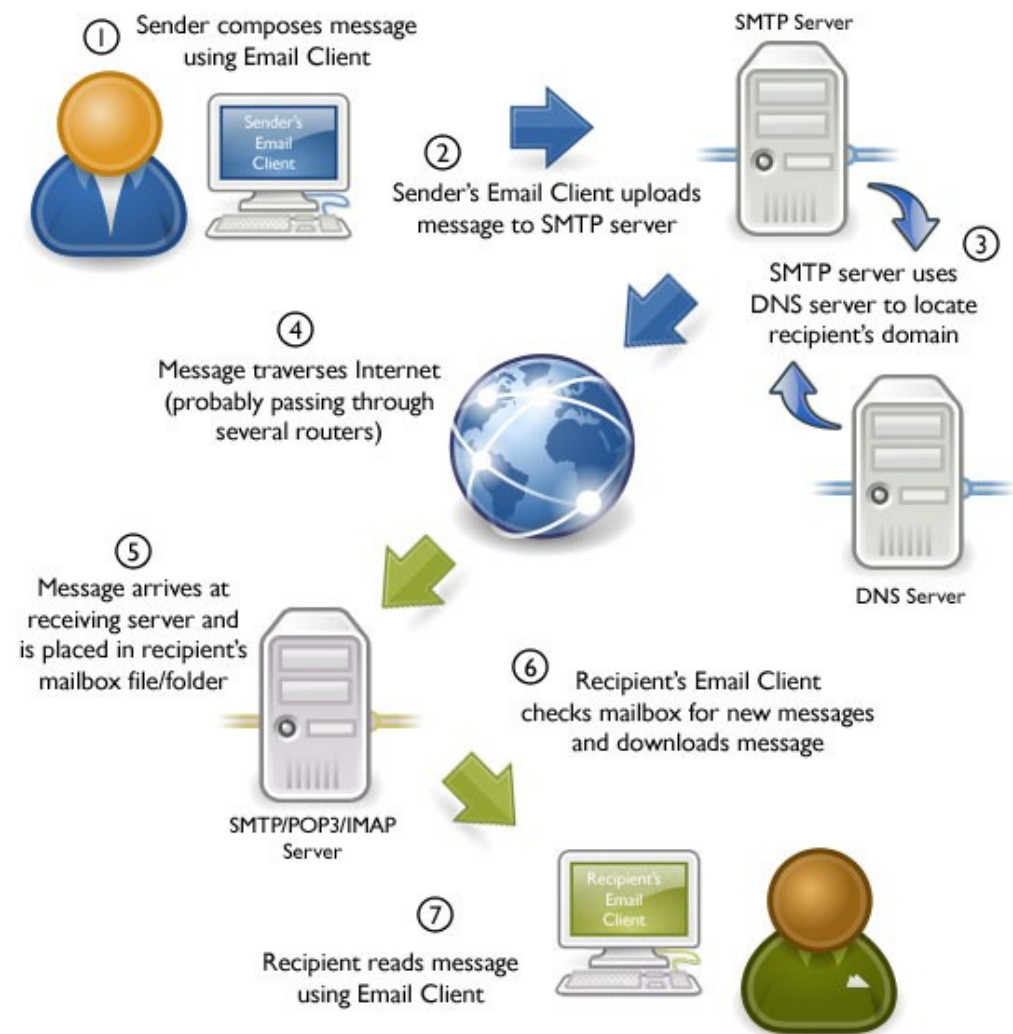
Introdução

Correio eletrônico é um método digital para troca de mensagens entre um remetente e um ou vários destinatários.



Correio Eletrônico

O sistema de correio eletrônico é composto por servidores de correio, que contêm as caixas postais dos usuários, e por clientes de correio, que permitem que os usuários possam interagir com o sistema, ou seja, lendo e postando mensagens.



©2010 OnlyMyEmail Inc. (www.OnlyMyEmail.com) with many thanks to the Gnome project (www.gnome.org) for the images

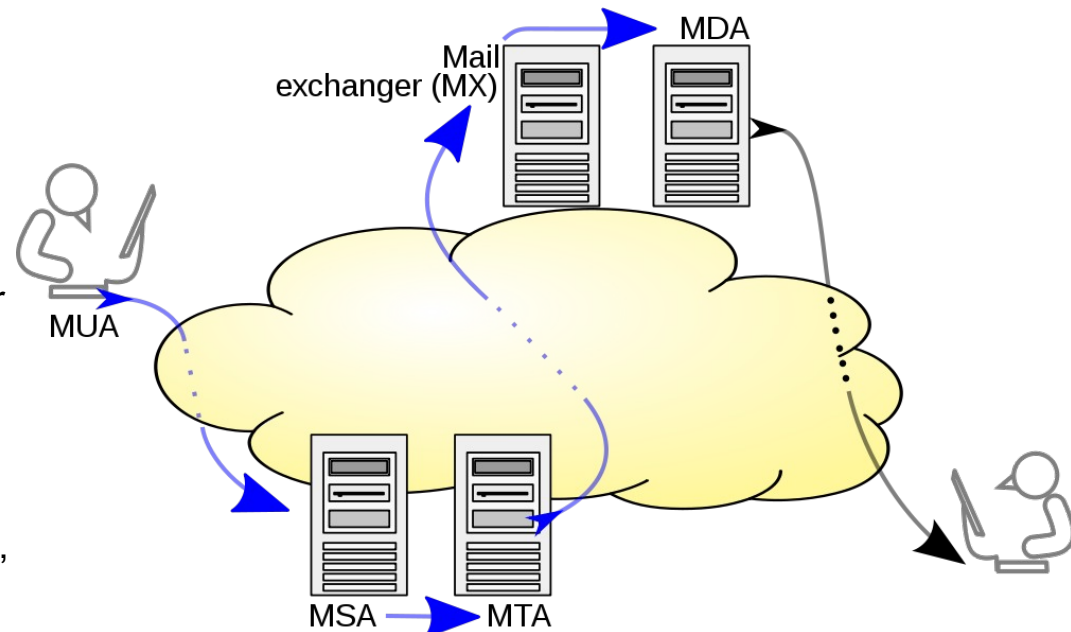


Correio Eletrônico - Componentes

O cliente de correio é também conhecido como MUA (*Mail User Agent*). O MUA permite que o usuário possa criar, enviar e receber mensagens.

Quando o cliente cria uma mensagem, o próximo passo é enviá-la para o MSA (*Mail Submission Agent*), que é responsável por tratar e enviar a mensagem para o MTA (*Mail Transfer Agent*), responsável por enviar a mensagem pela Internet, por meio do protocolo SMTP (*Simple Mail Transfer Protocol*), para o MX (Mail Exchanger) do destinatário. O MSA e o MTA trabalham em conjunto e geralmente estão instalados e configurados no mesmo servidor de correio.

Quando o MX do destinatário recebe a mensagem, este direciona para o MDA (*Mail Delivery Agent*), que é responsável por disponibilizar a mensagem para o destinatário por meio de serviços de Webmail, ou por meio dos protocolos POP (*Post Office Protocol*) ou IMAP (*Internet Message Access Protocol*). O MX e o MDA trabalham em conjunto e também podem estar instalados e configurados no mesmo servidor.





SMTP

O protocolo SMTP (*Simple Mail Transfer Protocol*) é usado para transferir mensagens de correio entre o cliente (MUA) e o servidor de correio ou ainda entre servidores de correio de diferentes organizações.

Opera na porta TCP 25 (envio de mensagens entre servidores de correio) ou na porta TCP 587 (envio de mensagens entre cliente e servidor de correio).





SMTP - Exemplo

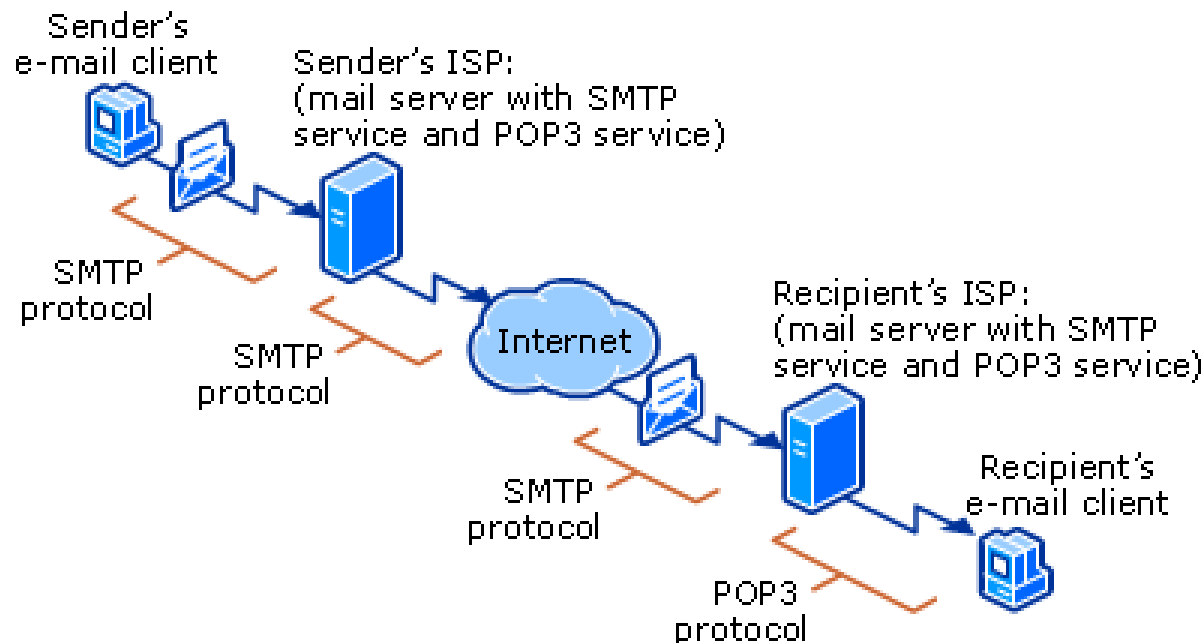
Usando o Telnet como MUA, o usuário Mickey deseja enviar uma mensagem para dois destinatários: Mônica e Magali. O quadro abaixo mostra a sequencia de comandos. Linhas em negrito são mensagens do servidor.

```
helo disney.com
250 OK
mail from:mickey@disney.com
250 OK - mail from <mickey@disney.com>
rcpt to:monica@panini.com.br
250 OK - Recipient <monica@panini.com.br>
rcpt to:magali@panini.com.br
250 OK - Recipient <magali@panini.com.br>
data
354 Senda data. End with CRLF.CRLF
subject:Ferias
Viaje pra Disney nestas ferias!
.
250 OK
quit
221 closing connection
Connection close by foreign host.
```



POP

O protocolo POP (*Post Office Protocol*) é usado para baixar todas as mensagens da caixa postal do usuário, armazená-las localmente e em seguida apagá-las do servidor de correio, ainda que seja possível manter uma cópia da mensagem no servidor. O protocolo POP está na versão 3 (POP3) e é indicado para conexões *off-line*. Ele opera na porta TCP 110.





POP - Exemplo

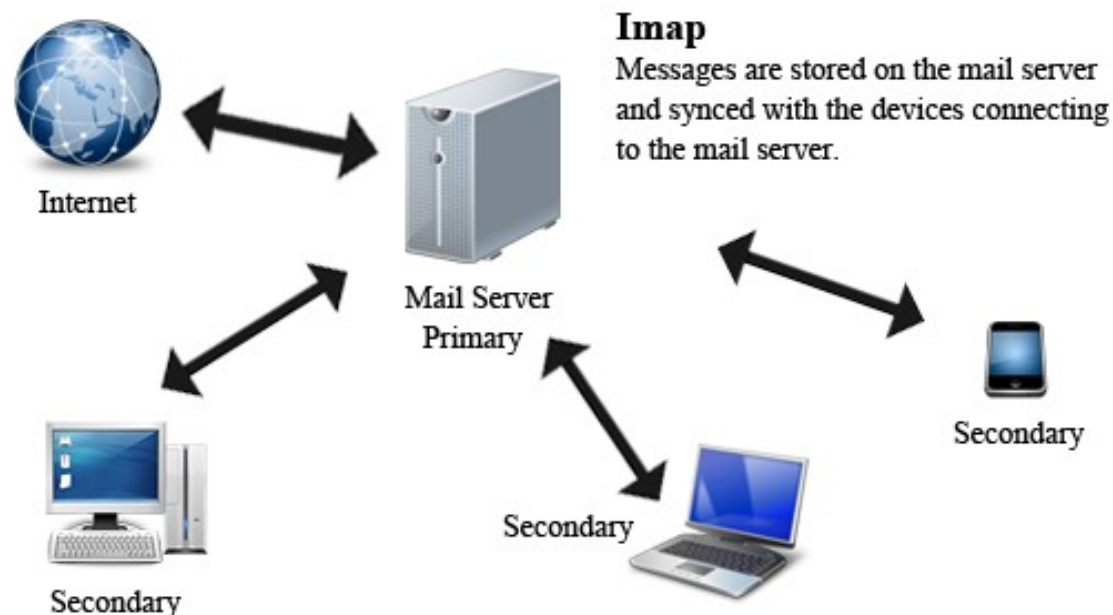
Usando o Telnet como MUA, a usuária Mônica visualiza uma mensagem de sua caixa postal e em seguida a apaga. O quadro abaixo mostra a sequencia de comandos. Linhas em negrito são mensagens do servidor.

```
user monica
+OK
pass 1234
+OK User successfully logged on
list
1 264
.
retr 1
Received:      from      disney.com      (192.168.0.10      [192.168.0.10])      by
MAIL.panini.com.br with SMTP (Microsoft Exchange Internet Mail Service
Version 5.5.2653.13)
      id LN8FJSQ1: Tue, 22 May 2012 08:29:55 -0700
subject:Ferias
Viaje pra Disney nestas ferias!
.
dele 1
+OK
quit
+OK Microsoft Exchange POP3 server version 5.5.2653.23 signing off
Connection close by foreign host.
```



IMAP

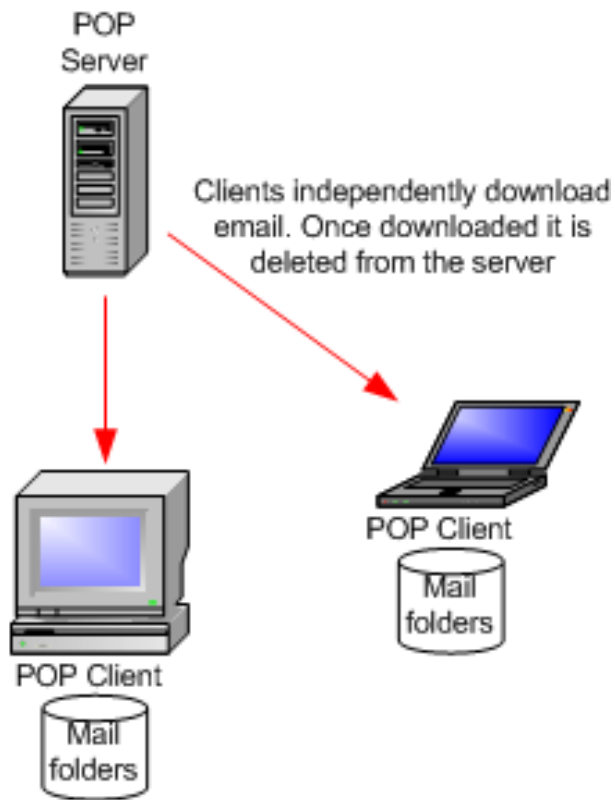
O protocolo IMAP (*Internet Message Access Protocol*) sincroniza o cliente com o servidor de correio, de modo que as mensagens não precisam ser copiadas do servidor para a máquina local. Permite ainda que vários clientes possam conectar-se a mesma caixa postal. O protocolo IMAP está na versão 4 (IMAP4) e é indicado para conexões *on-line*. Ele opera na porta TCP 143.



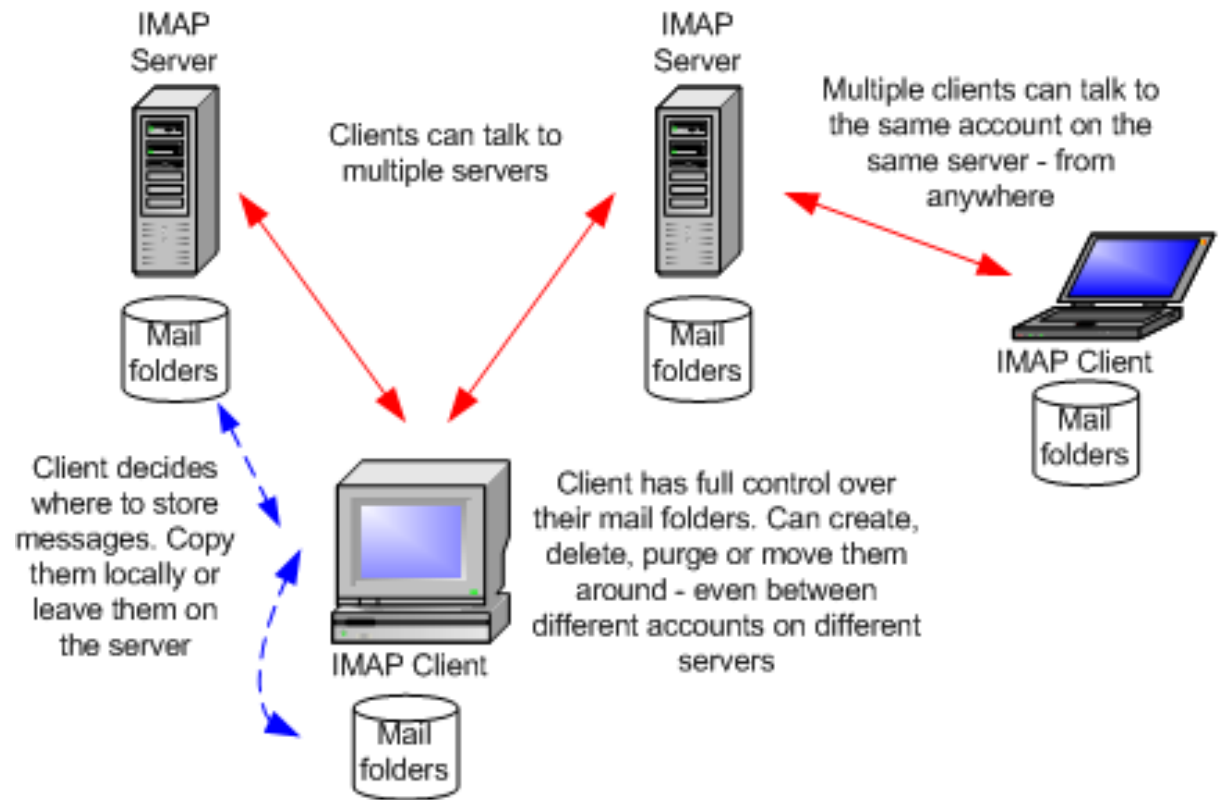


POP vs. IMAP

POP



IMAP

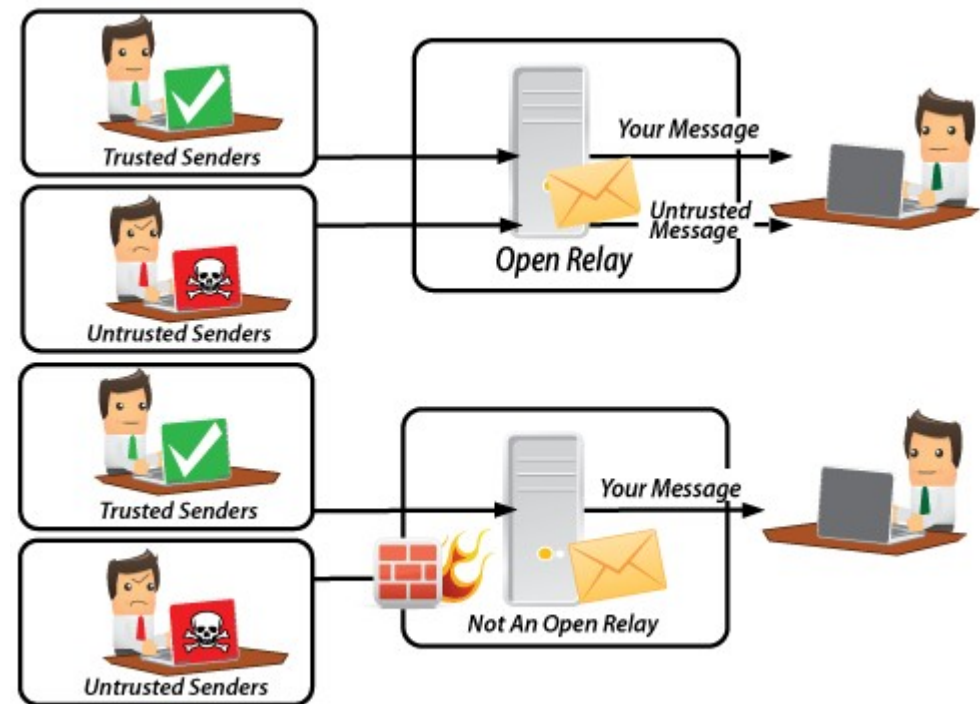




Relay (Retransmitir)

U servidor de correio pode ser configurado de duas formas: com retransmissão ativada (*Open Relay*) ou desativada (*Not Open Relay*). No primeiro caso, qualquer usuário pode conectar-se ao servidor de correio e enviar mensagens, mesmo que ele não possua uma caixa postal ou autorização para tal. No segundo caso, somente usuários que possuem caixas postais ou autorização podem enviar mensagens.

Vírus e *spammers* procuram usar servidores de correio que estejam operando no modo *Open Relay*.

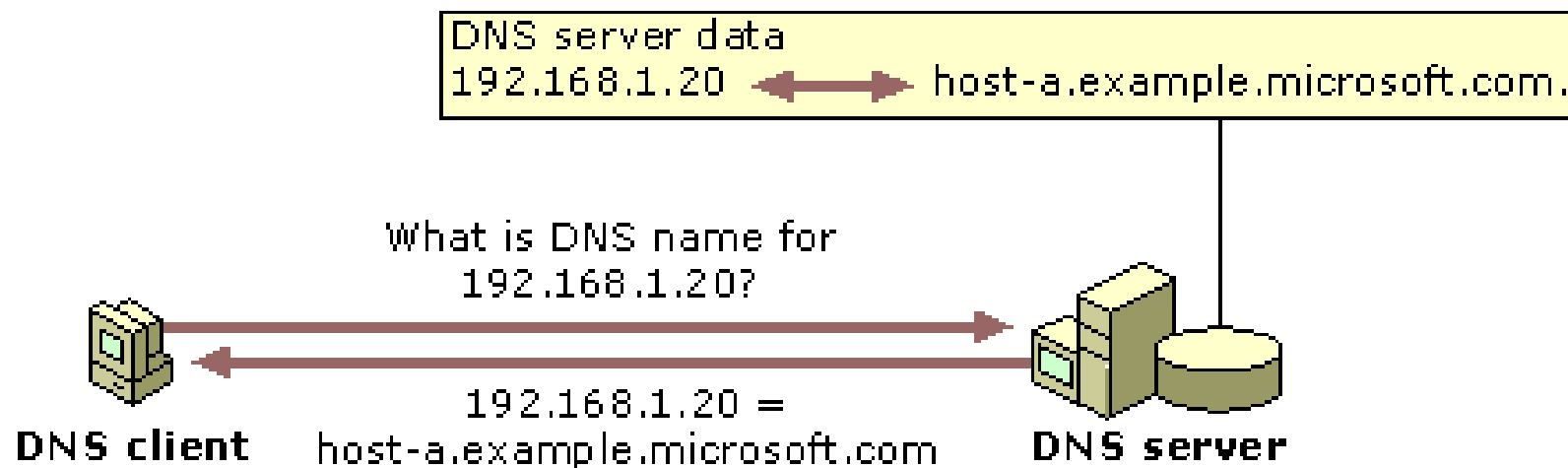




DNS Reverso

Ao contrário da pesquisa DNS direta, onde dado um nome de domínio retorna-se com um endereço IP, na pesquisa DNS reversa é dado um endereço IP e como resultado obtêm-se um nome de domínio.

Este recurso é bastante usado pelos servidores de correio para verificar se as mensagens recebidas provem de domínios reais ou forjados.





Cabeçalho da mensagem

Toda mensagem de correio possui um cabeçalho que contém informações importantes sobre remetente e destinatário, bem como por quais servidores a mensagem passou e por quais filtros (antivírus e *antispam*) foi submetida.

```
Return-Path: <melody@covingtoninnovations.com>
Received: from spgw1.servdns.com [65.163.13.5] by smail4.servdns.com with SMTP;
Sun, 13 Jan 2008 19:59:57 -0500
Received: from fmailhost02.isp.att.net (fmailhost02.isp.att.net [204.127.217.102])
by spgw1.servdns.com (Sectorlink) with ESMTP id AA8DB300097
for <mc@covingtoninnovations.com>; Sun, 13 Jan 2008 19:58:13 -0500 (EST)
Received: from hokusai (adsl-224-168-165.asm.bellsouth.net[74.224.168.165])
by isp.att.net (frfwmlhc02) with SMTP
id <20080114005830H0200af55e>; Mon, 14 Jan 2008 00:58:30 +0000
X-Originating-IP: [74.224.168.165]
From: "Melody Covington" <melody@covingtoninnovations.com>
To: <melody@maxcharge.com>,
"Michael A. Covington" <mc@covingtoninnovations.com>
Subject: Appointments for the coming week
Date: Sun, 13 Jan 2008 19:58:29 -0500
Organization: Covington Innovations
Message-ID: <001101c85648$94774e60$6801a8c0@Hokusai>
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="====_NextPart_000_0012_01C8561E_ABA14660"
X-Mailer: Microsoft Office Outlook 11
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.3198
Thread-Index: AchWSJPQySP0K1HFSwLo/S9GWHQA==
X-servdns-MailScanner-Information: Please contact the ISP for more information
X-servdns-MailScanner: Found to be clean
X-servdns-MailScanner-From: melody@covingtoninnovations.com
```

"RECEIVED" LINES show how message entered the Internet. Last one or two are most informative. Some may be fake.

"FROM" LINE is address given by the sender; may be totally false.

LINES THAT START WITH X are comments added by software; may be true or false.

```
Return-Path: <bogdan@fx.ro>
Received: from srv01.advenzia.com (root@localhost)
by emailaddressmanager.com (8.11.6/8.11.6) with ESMTP id i2OApwQ14083
for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 10:51:58 GMT
X-ClientAddr: 193.231.208.29
Received: from corporate.fx.ro (corporate.fx.ro [193.231.208.29])
by srv01.advenzia.com (8.11.6/8.11.6) with ESMTP id i2OApvs14078
for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 10:51:57 GMT
Received: from mail.fx.ro (mail3.fx.ro [193.231.208.3])
by corporate.fx.ro (8.12.11/8.12.7) with ESMTP id i2OAtxBr025924
for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 12:55:59 +0200
Received: from localhost.localdomain (corporate2.fx.ro [193.231.208.28])
by mail.fx.ro (8.12.11/8.12.3) with ESMTP id i2OAtQe006624
for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 12:55:50 +0200
Date: Wed, 24 Mar 2004 12:55:50 +0200
Message-Id: <200403241055.i2OAtQe006624@mail.fx.ro>
Content-Disposition: inline
Content-Transfer-Encoding: binary
MIME-Version: 1.0
To: support@emailaddressmanager.com
Subject: How to read email headers
From: bogdan@fx.ro
Reply-To: bogdan@fx.ro
Content-Type: text/plain; charset=us-ascii
X-Originating-IP: [80.97.5.101]
X-Mailer: FX Webmail webmail.fx.ro
X-RAVMilter-Version: 8.4.3(snapshot 20030212) (mail)
Status:
```



Mensagem forjada

Muitos vírus e *spammers* usam a técnica de mensagem forjada (*email spoofing*) para enviar mensagens falsas. Esta técnica consiste em

When an SMTP email is sent, the initial connection provides two pieces of address information:

MAIL FROM: - generally presented to the recipient as the Return-path: header but not normally visible to the end user.[5] and by default no checks are done that the sending system is authorized to send on behalf of that address.

RCPT TO: - specifies which email address the email is delivered to, is not normally visible to the end user but may be present in the headers as part of the "Received:" header.

Together these are sometimes referred to as the "envelope" addressing, by analogy with a traditional paper envelope.[6]

Once the receiving mail server signals that it accepted these two items, the sending system sends the "DATA" command, and typically sends several header items, including:

From: Joe Q Doe <joeqdoe@example.com> - the address visible to the recipient; but again, by default no checks are done that the sending system is authorized to send on behalf of that address.

Reply-to: Jane Roe <Jane.Roe@example.mil> - similarly not checked

The result is that the email recipient sees the email as having come from the address in the From: header; they may sometimes be able to find the MAIL FROM address; and if they reply to the email it will go to either the address presented in the MAIL FROM: or Reply-to: header - but none of these addresses are typically reliable.[7]

```
Delivered-To: [REDACTED]
Received: by 10.100.254.20 with SMTP id b20cs98801ani;
        Fri, 24 Jul 2009 21:30:52 -0700 (PDT)
MIME-Version: 1.0
Sender: marycollins4me@gmail.com
Received: by 10.239.163.136 with SMTP id p8mr522319hbd.141.1248496252081; Fri,
        24 Jul 2009 21:30:52 -0700 (PDT)
Date: Sat, 25 Jul 2009 05:30:52 +0100
X-Google-Sender-Auth: 2dab84a987bf6d9a
Message-ID: <c3688cd60907242130t212cedd112dc4687e1dcc002d@mail.gmail.com>
Subject: CONFIRMATION OF FUND (Reference Number: PP-278-686-296)RESPONSE
        NEEDED FOR FINA VERIFICATION
From: "service@paypal.com" <paypalonlinefundteam@mail2world.com>
To: [REDACTED]
Content-Type: multipart/alternative; boundary=001485f1d8989bd63f046f802fffb

--001485f1d8989bd63f046f802fffb
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: quoted-printable

[image: PayPal] <https://www.paypal.com/us>
```

Dear Valued Customer

[REDACTED] The payment have been made to your paypal account for an auction item: (ACER LAPTOP{Like New!} + FREE SOFTWARE!! + =3D) the money have been transferred to your paypal account by one of our client (alexjohnsoncole02@gmail.com) and it has also been Approved and confirmed here with us but we just need the shipment confirmation from you so that we may credit and release the money to your account immediately. Go ahead with the shipment of the item now to it's destination address and get back to us with the shipment tracking number of the item being sent to our client and we used this NEW POLICY of ours to protect both the BUYER and the SELLER from any internet fraud activities.



Para saber mais...

... acesse o documento sobre Noções básicas sobre a pesquisa inversa, da Microsoft.

... acesse o Analizador de Cabeçalho de e-mail, da MX Toolbox.

Módulo 9

Camada de transporte



Introdução

A camada de transporte é responsável por transferir dados entre a máquina de origem e a máquina de destino.

Esta transferência poder ser feita de duas formas: com confirmação de entrega de dados, por meio do protocolo TCP, ou sem confirmação de entrega de dados, por meio do protocolo UDP.



Protocolo TCP

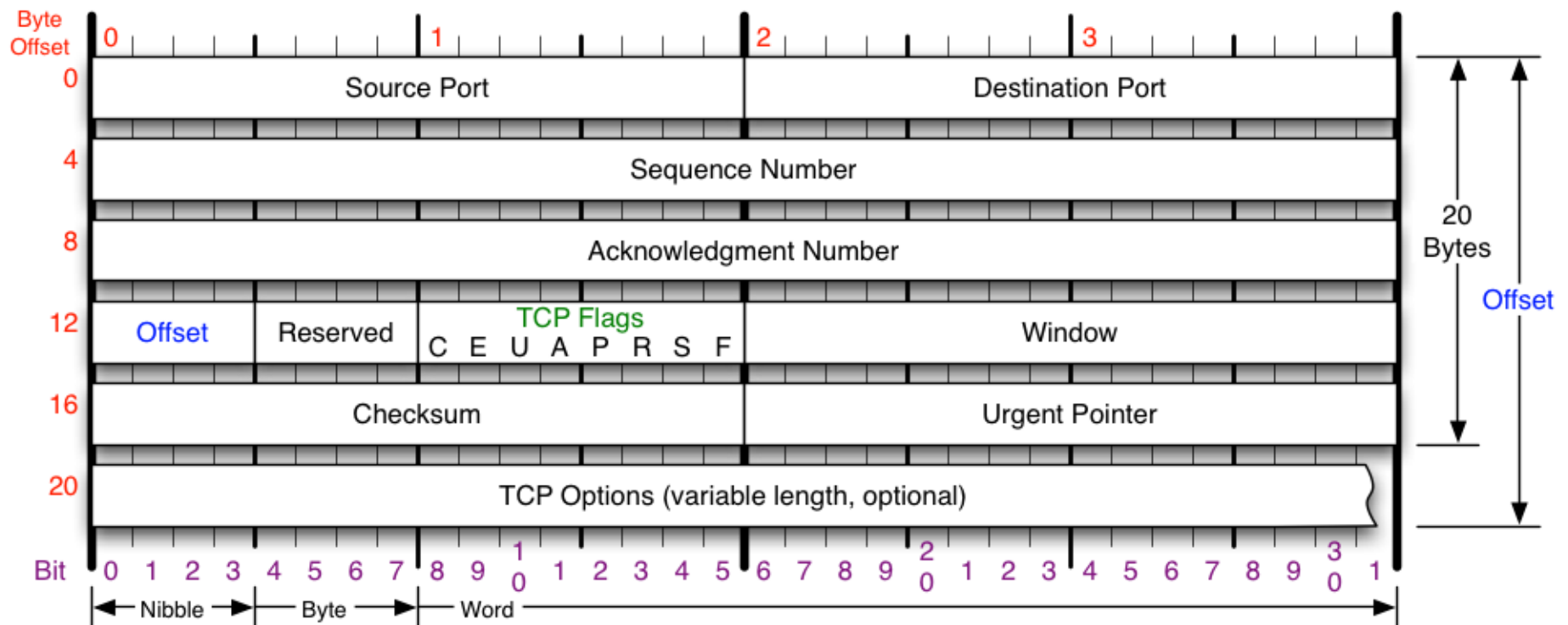
O protocolo TCP (Transmission Control Protocol)



Protocolo TCP - Cabeçalho

O cabeçalho do protocolo TCP possui 20 bytes de tamanho, e possui informações sobre as portas origem e destino, número de sequência, número de reconhecimento, entre outros.

TCP Header





Protocolo TCP - Cabeçalho

TCP Flags

C E U A P R S F

Congestion Window

C 0x80 Reduced (CWR)
E 0x40 ECN Echo (ECE)
U 0x20 Urgent
A 0x10 Ack
P 0x08 Push
R 0x04 Reset
S 0x02 Syn
F 0x01 Fin

Congestion Notification

ECN (Explicit Congestion Notification). See RFC 3168 for full details, valid states below.

Packet State	DSB	ECN bits
Syn	0 0	1 1
Syn-Ack	0 0	0 1
Ack	0 1	0 0
No Congestion	0 1	0 0
No Congestion	1 0	0 0
Congestion	1 1	0 0
Receiver Response	1 1	0 1
Sender Response	1 1	1 1

TCP Options

0 End of Options List
1 No Operation (NOP, Pad)
2 Maximum segment size
3 Window Scale
4 Selective ACK ok
8 Timestamp

Checksum

Checksum of entire TCP segment and pseudo header (parts of IP header)

Offset

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

RFC 793

Please refer to RFC 793 for the complete Transmission Control Protocol (TCP) Specification.

Copyright 2008 - Matt Baxter - mjb@fatpipe.org - www.fatpipe.org/~mjb/Drawings/



Protocolo TCP - MSS

O MSS ou Maximum Segment Size (Tamanho Máximo do Segmento) é a quantidade máxima de bytes que um segmento TCP pode transportar. Em redes Ethernet este valor é de 1460 bytes, enquanto que para redes seriais (linhas discadas, por exemplo), este valor é de 536 bytes.

```

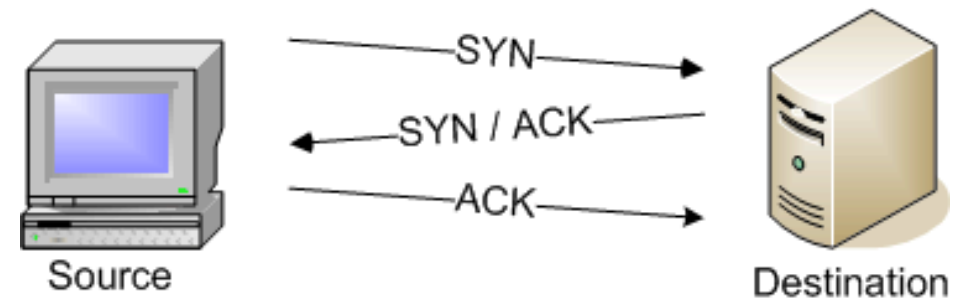
> Ethernet II, Src: AsustekC_b3:01:84 (00:1d:60:b3:01:84), Dst: Cisco_ca:85:69
> Internet Protocol, Src: 192.168.1.16 (192.168.1.16), Dst: 209.20.64.81 (209.20.64.81)
▽ Transmission Control Protocol, Src Port: 49214 (49214), Dst Port: http (80), S
    Source port: 49214 (49214)
    Destination port: http (80)
    Sequence number: 0 (relative sequence number)
    Header length: 40 bytes
    > Flags: 0x02 (SYN)
        Window size: 5840
    > Checksum: 0xb1df [validation disabled]
    ▾ Options: (20 bytes)
        Maximum segment size: 1460 bytes
        SACK permitted
        Timestamps: TSval 5356733, TSecr 0
        NOP
        Window scale: 7 (multiply by 128)
```



Protocolo TCP - Handshake - Open

Antes do início de uma transmissão de dados, deve-se proceder com a abertura da sessão, por meio do Handshake de três vias.

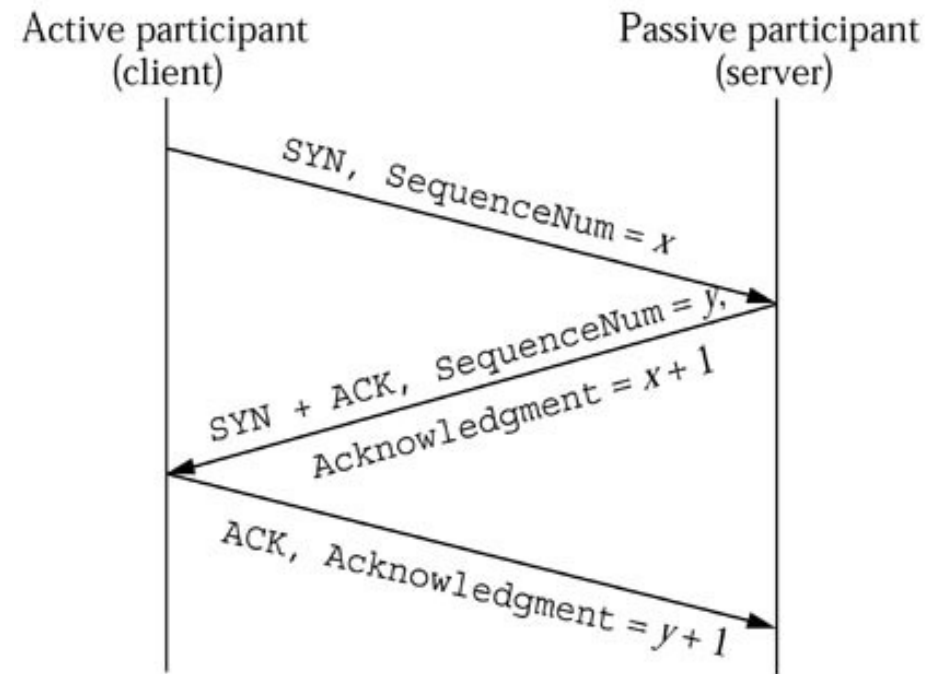
O computador origem envia ao destinatário um sinal SYN. Se o computador destino aceitar a conexão, envia um sinal SYN+ACK para o computador origem, que responderá com um sinal ACK.





Protocolo TCP - Handshake - Open

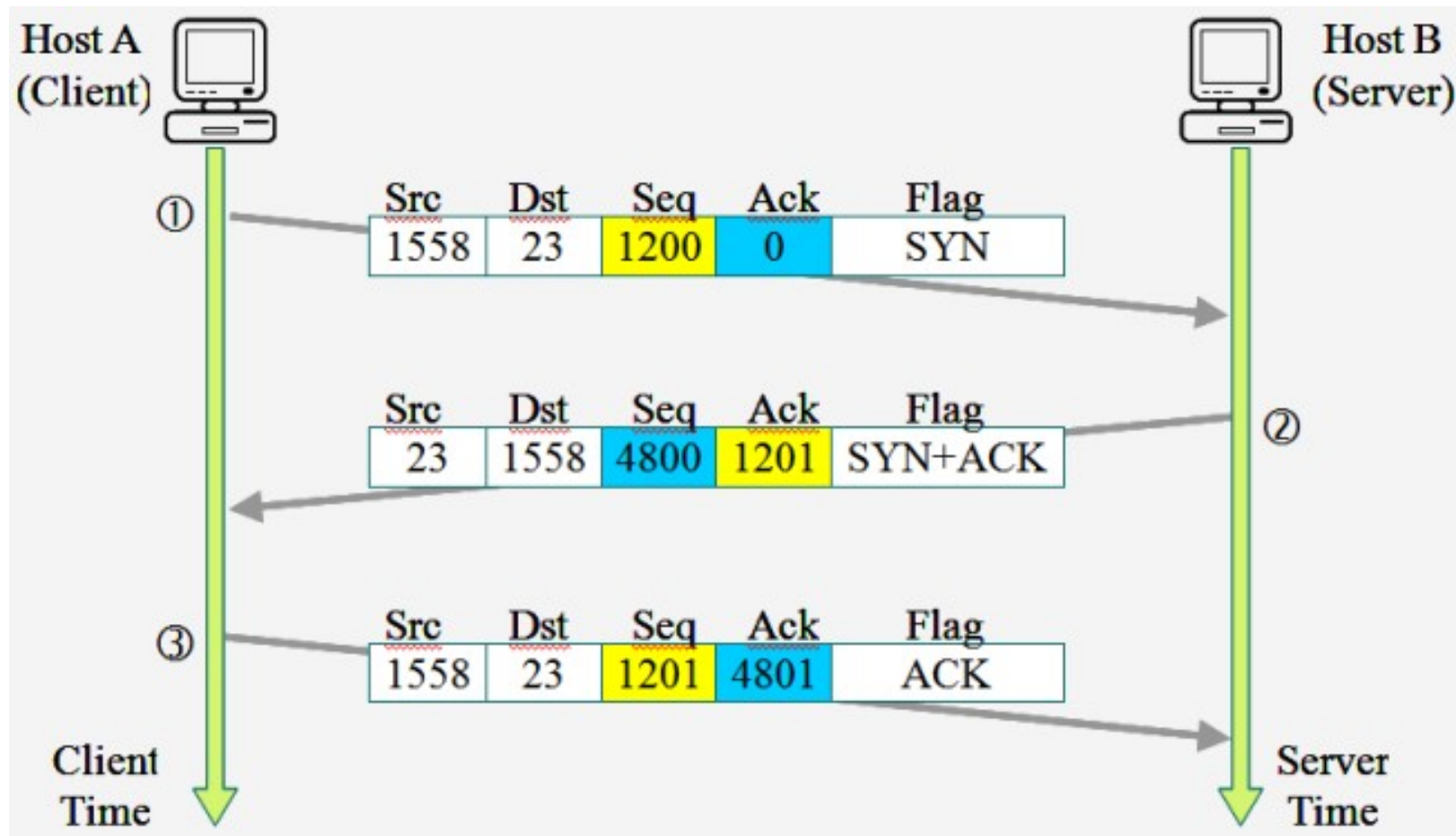
Quando o computador origem envia ao destinatário um sinal SYN, este recebe um número sequencial x . Quando o computador destino responde, este envia um novo número sequencial y e um número de reconhecimento que será igual a $x+1$. Por fim, o computador origem responde com um número sequencial $x+1$ (que não aparece na figura) e um número de reconhecimento $y+1$.





Protocolo TCP - Exemplo

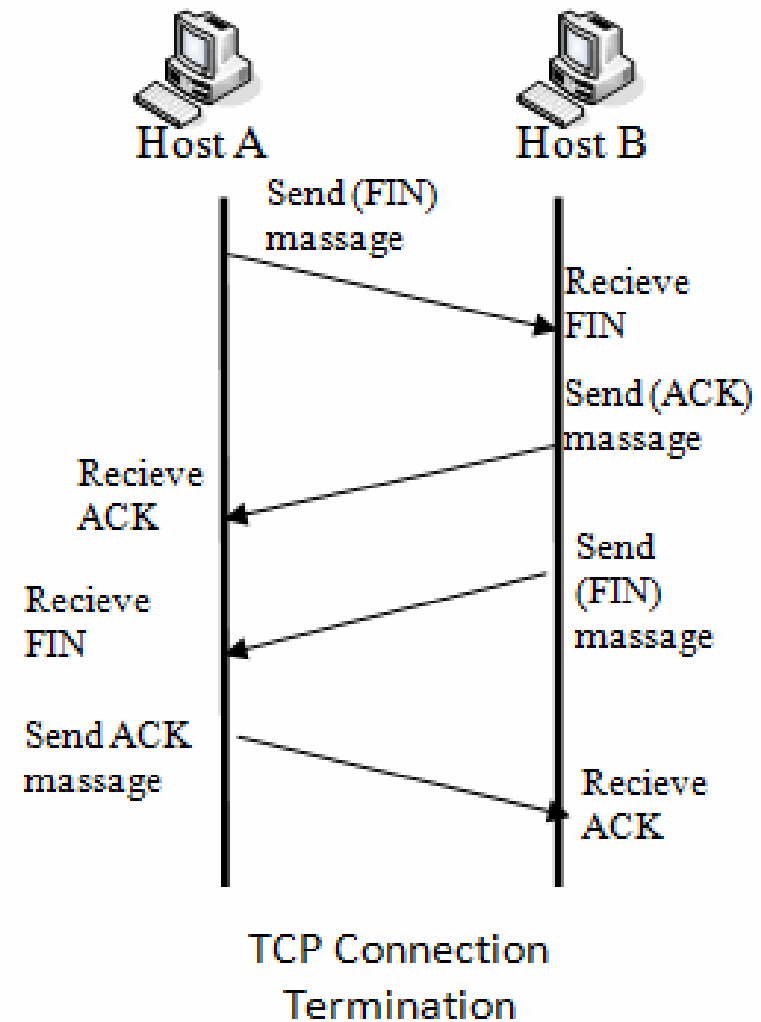
No exemplo abaixo, pode-se ver o handshake de três vias entre um computador cliente (Host A) e um servidor (Host B).





Protocolo TCP - Handshake - Close

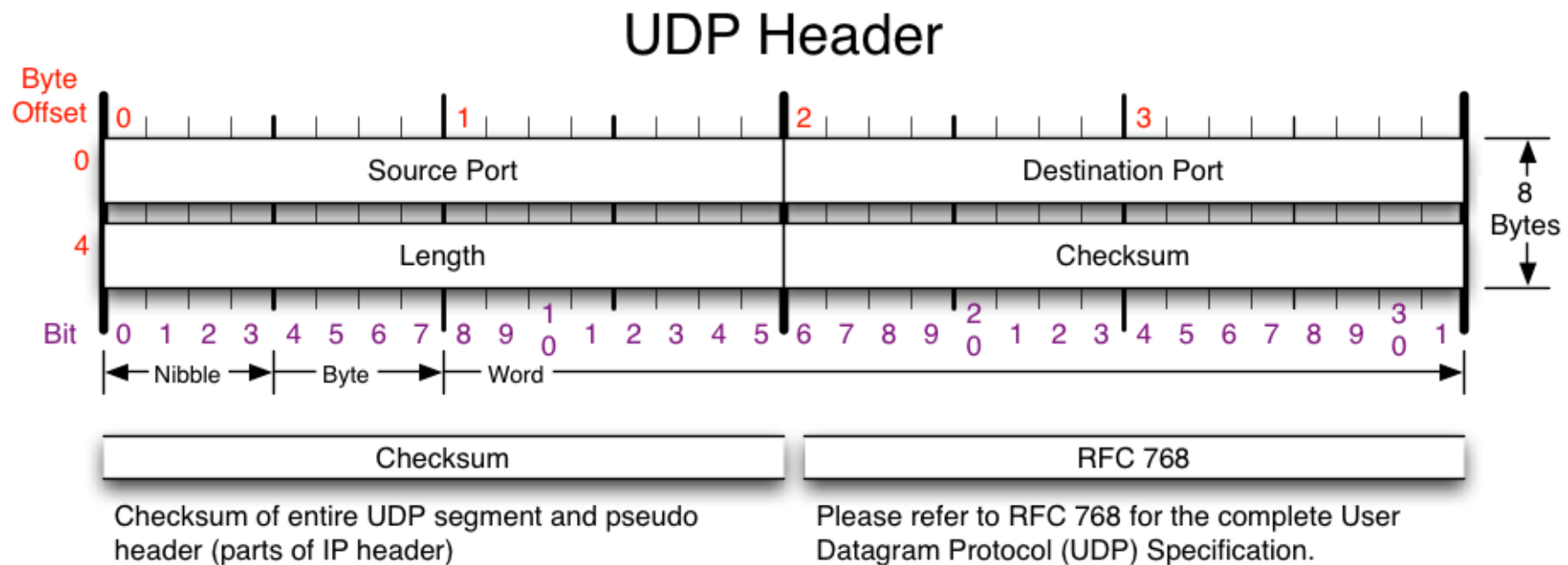
Quando o computador origem deseja encerrar a conexão, o mesmo envia ao destinatário um sinal FIN. O computador destino responde enviando um sinal ACK e na sequência um sinal FIN solicitando também o encerramento da conexão. Por fim, o computador origem responde com um sinal ACK.





Protocolo UCP - Cabeçalho

Por não oferecer o serviço de confirmação de entrega, o cabeçalho do protocolo UCP é mais simples e possui apenas 8 bytes de tamanho. Contém apenas informações sobre as portas origem e destino, tamanho e código de checagem.



Copyright 2008 - Matt Baxter - mjb@fatpipe.org - www.fatpipe.org/~mjb/Drawings/



Para saber mais...

... acesse o material online sobre Camada de Transporte, do Prof. Dr. Romildo Martins da Silva Bezerra, do Instituto Federal de Educação, Ciência e Tecnologia da Bahia, Brasil.

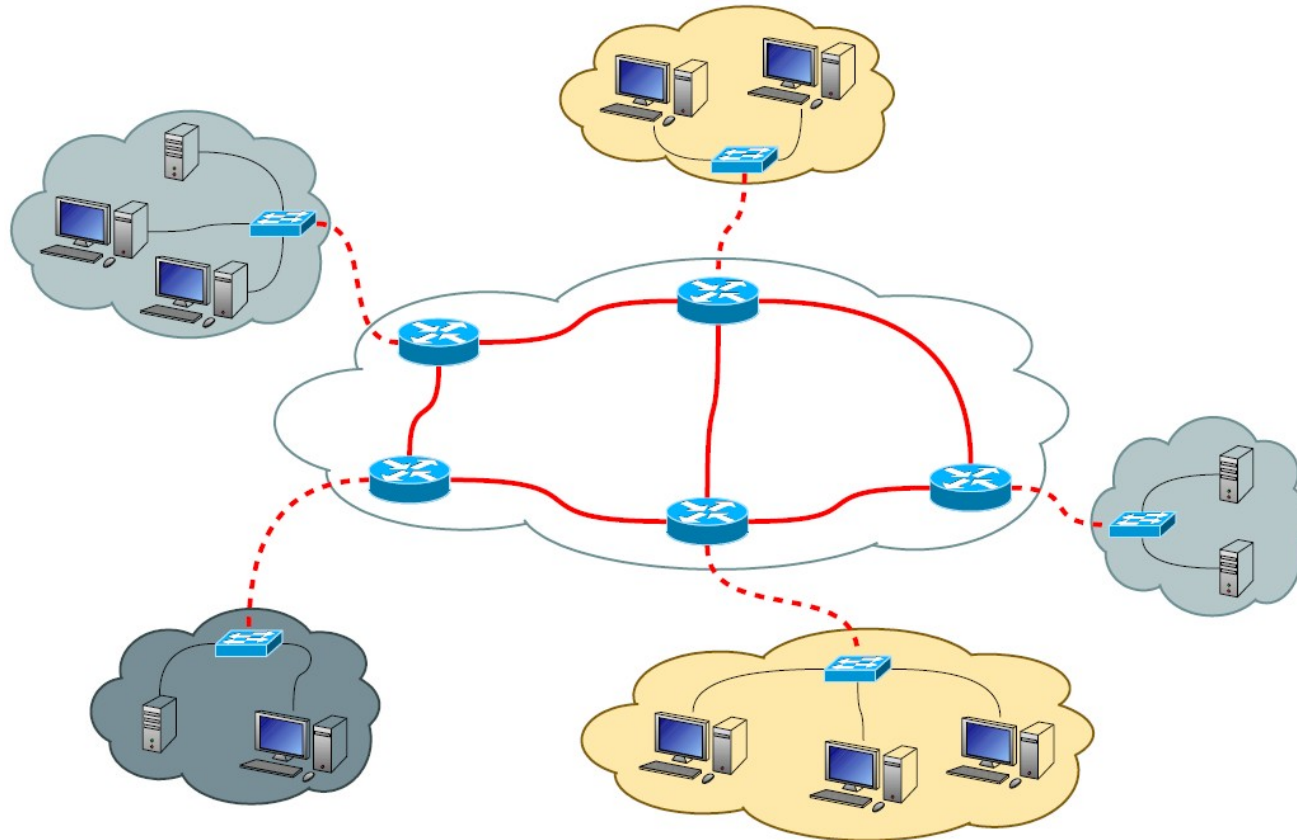
Módulo 10

Camada de rede



Introdução

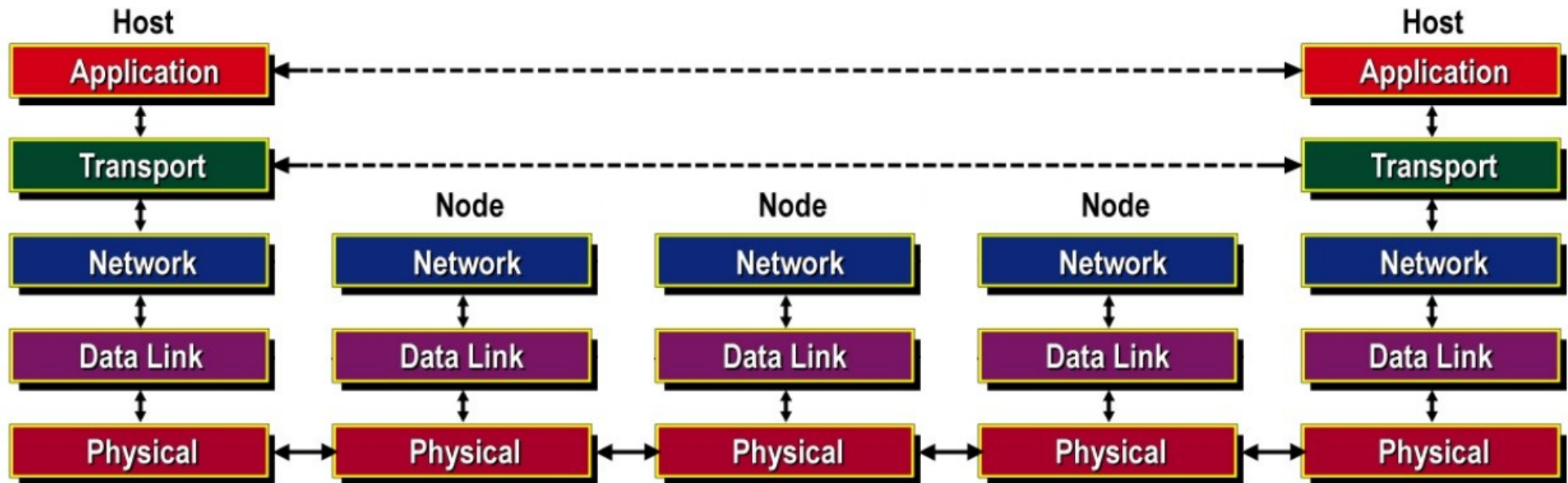
A camada de rede é responsável por rotear os pacotes de dados entre as diferentes redes que se interpõem entre a origem e o destino.





Camada de rede

Quando existe a transmissão de dados entre dois *hosts*, todas as camadas do modelo TCP/IP estarão envolvidas na comunicação apenas nos *hosts* origem e destino. No nós intermediários apenas as camadas de rede, enlace e física serão usadas.





Protocolo IP

O protocolo IP (Internet Protocol) é responsável por rotear os pacotes – também conhecidos como datagramas – pela Internet.

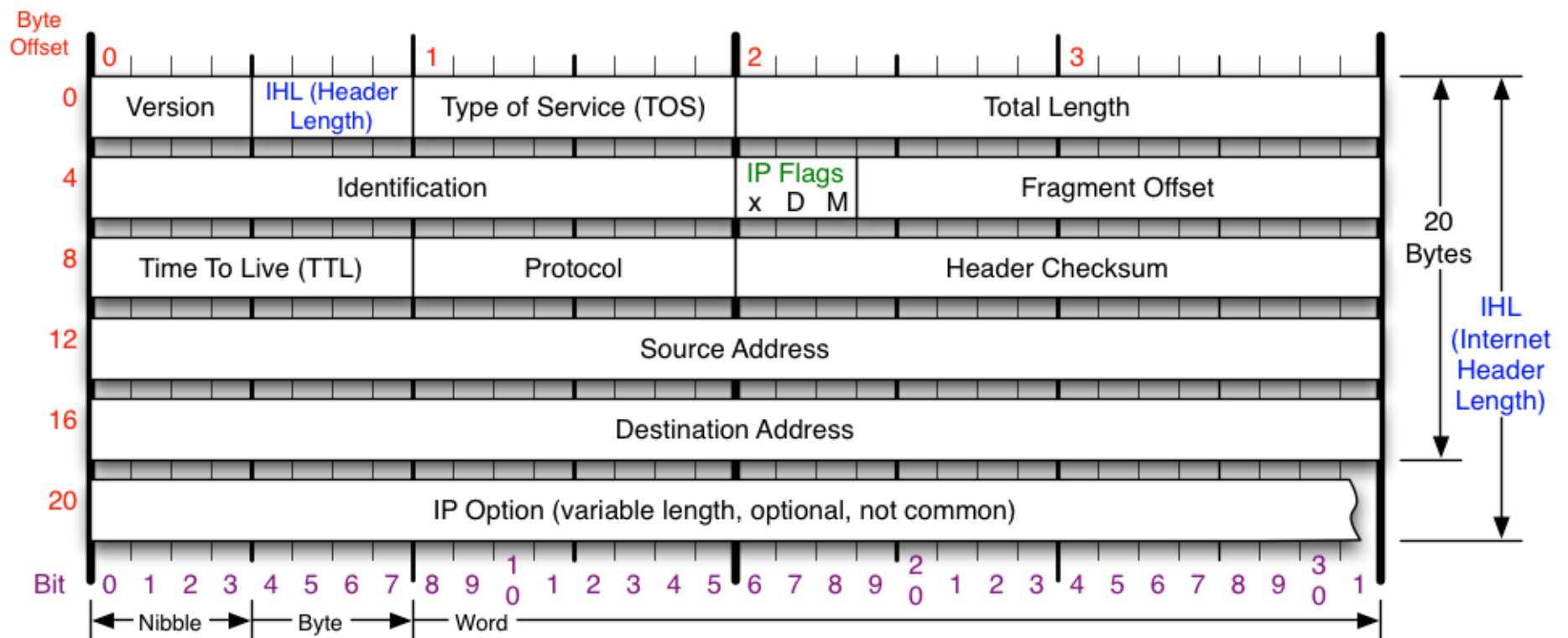
Sua função é transportar e entregar os pacotes entre origem e destino escolhendo os melhores caminhos baseados no menor custo. Deve ser capaz também de selecionar caminhos alternativos quando houver falhas nos caminhos principais.



Protocolo IP - Cabeçalho

O cabeçalho do protocolo IP possui 20 bytes de tamanho, e possui informações sobre os endereços IP origem e destino, dados sobre fragmentação, tempo de vida, entre outros.

IPv4 Header





Protocolo IP - Cabeçalho

Version

Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.

Header Length

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

Protocol

IP Protocol ID. Including (but not limited to):

1 ICMP	17 UDP	57 SKIP
2 IGMP	47 GRE	88 EIGRP
6 TCP	50 ESP	89 OSPF
9 IGRP	51 AH	115 L2TP

Total Length

Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.

Fragment Offset

Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.

Header Checksum

Checksum of entire IP header

IP Flags

x D M

x 0x80 reserved (evil bit)
D 0x40 Do Not Fragment
M 0x20 More Fragments follow

RFC 791

Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

Copyright 2008 - Matt Baxter - mjb@fatpipe.org - www.fatpipe.org/~mjb/Drawings/



Protocolo IP - Fragmentação

A fragmentação ocorre sempre que a camada de rede precisar enviar pacotes maiores do que a camada de enlace é capaz de transportar. Para isso o cabeçalho IP possui os campos *Identification*, *IP Flags* e *Fragment Offset*. O primeiro campo identifica o conjunto de fragmentos, de modo que possam ser remontados no destino. O segundo campo indica se aquele fragmento é ou não o último da sequência, e o terceiro campo indica a posição do fragmento em relação ao pacote original.

Example

- ❑ 4000 byte datagram
- ❑ MTU = 1500 bytes

1480 bytes in data field

offset = $1480/8$

length	ID	fragflag	offset
=4000	=x	=0	=0

One large datagram becomes several smaller datagrams

length	ID	fragflag	offset
=1500	=x	=1	=0

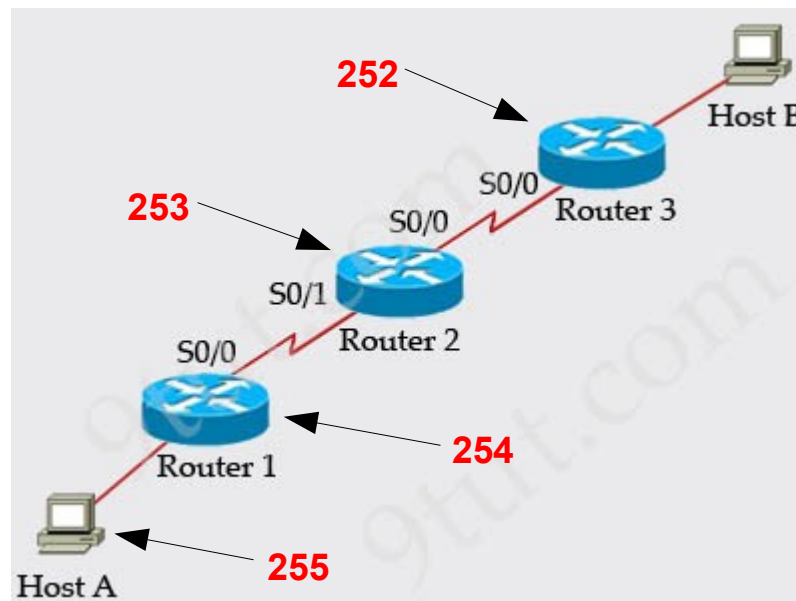
length	ID	fragflag	offset
=1500	=x	=1	=185

length	ID	fragflag	offset
=1040	=x	=0	=370



Protocolo IP - Tempo de vida

O tempo de vida ou TTL (Time to Live) é um parâmetro do cabeçalho IP que indica por quantos roteadores – ou saltos (*hops*) – um pacote pode “viajar” antes de ser descartado. Para cada roteador por onde o pacote passa, este campo é decrementado de 1.

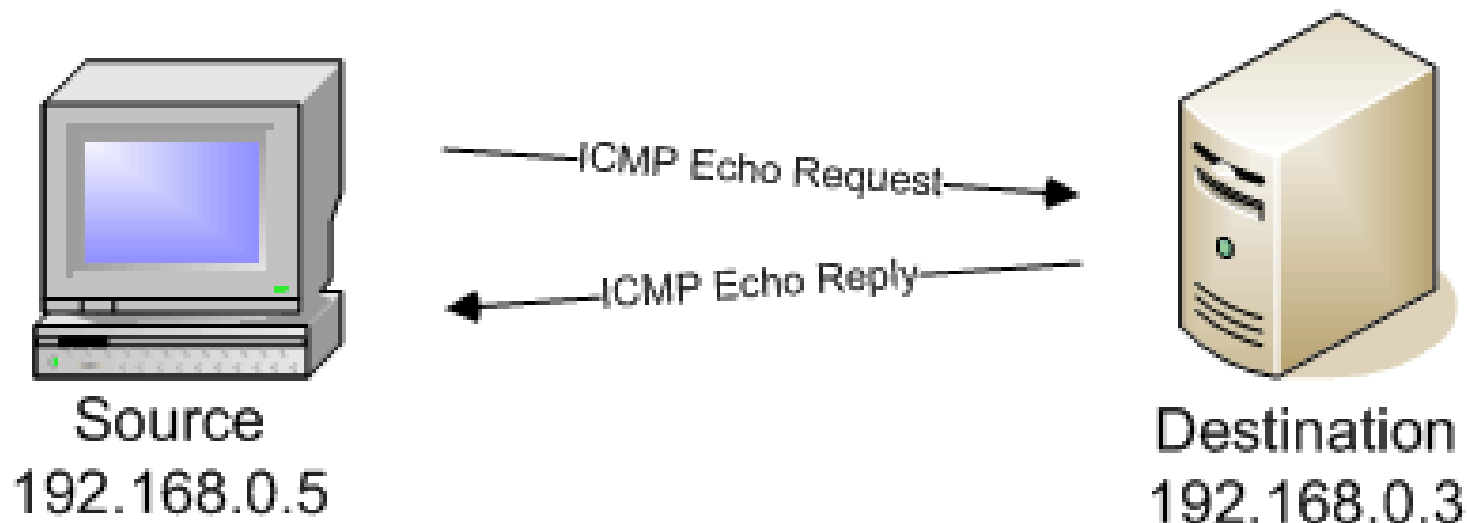




Protocolo ICMP

O protocolo ICMP (Internet Control Message Protocol) é usado para enviar pela rede mensagens de diagnóstico e de erro.

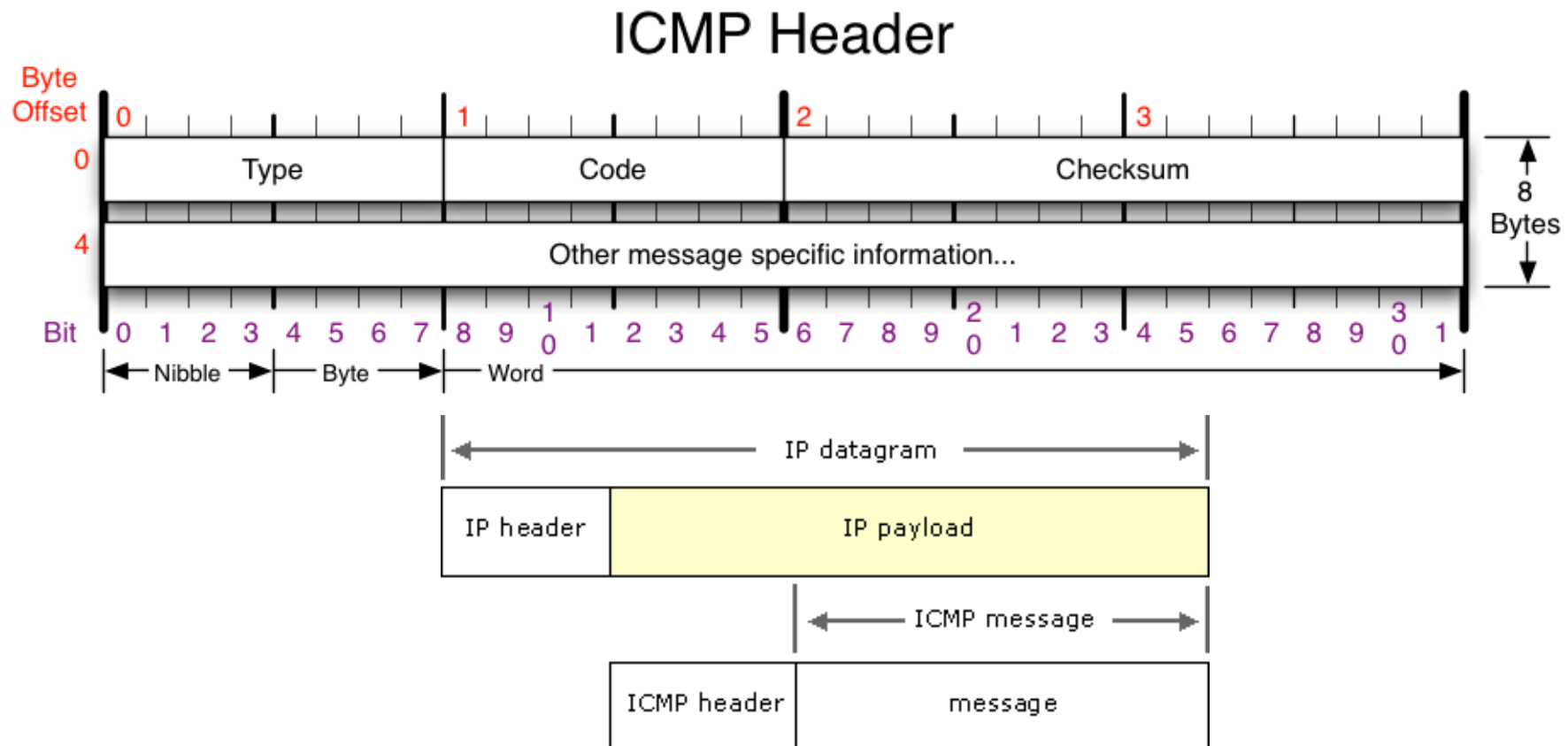
Um exemplo do uso deste protocolo é o comando PING, usado para diagnóstico básico de rede. Este comando envia uma solicitação de Echo Request a um determinado *host*, que estando ativo e acessível, responde com uma resposta Echo Reply.





Protocolo ICMP - Cabeçalho

O cabeçalho do protocolo ICMP possui 8 bytes de tamanho, e é transportado dentro de um pacote IP.



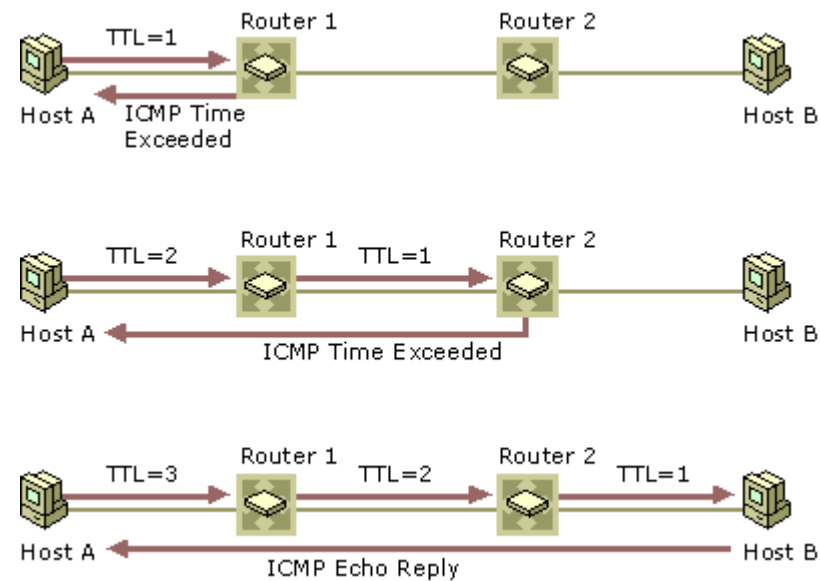
Protocolo ICMP - Cabeçalho

ICMP Message Types		Checksum	
Type	Code/Name	Type	Code/Name
0	Echo Reply	3	Destination Unreachable (continued)
3	Destination Unreachable	12	Host Unreachable for TOS
0	Net Unreachable	13	Communication Administratively Prohibited
1	Host Unreachable	4	Source Quench
2	Protocol Unreachable	5	Redirect
3	Port Unreachable	0	Redirect Datagram for the Network
4	Fragmentation required, and DF set	1	Redirect Datagram for the Host
5	Source Route Failed	2	Redirect Datagram for the TOS & Network
6	Destination Network Unknown	3	Redirect Datagram for the TOS & Host
7	Destination Host Unknown	8	Echo
8	Source Host Isolated	9	Router Advertisement
9	Network Administratively Prohibited	10	Router Selection
10	Host Administratively Prohibited	11	Time Exceeded
11	Network Unreachable for TOS	0	TTL Exceeded
		1	Fragment Reassembly Time Exceeded
		12	Parameter Problem
		0	Pointer Problem
		1	Missing a Required Operand
		2	Bad Length
		13	Timestamp
		14	Timestamp Reply
		15	Information Request
		16	Information Reply
		17	Address Mask Request
		18	Address Mask Reply
		30	Traceroute
		Checksum of ICMP header	
		RFC 792	
		Please refer to RFC 792 for the Internet Control Message protocol (ICMP) specification.	

Copyright 2008 - Matt Baxter - mjb@fatpipe.org - www.fatpipe.org/~mjb/Drawings/



Tracert





Protocolo ARP

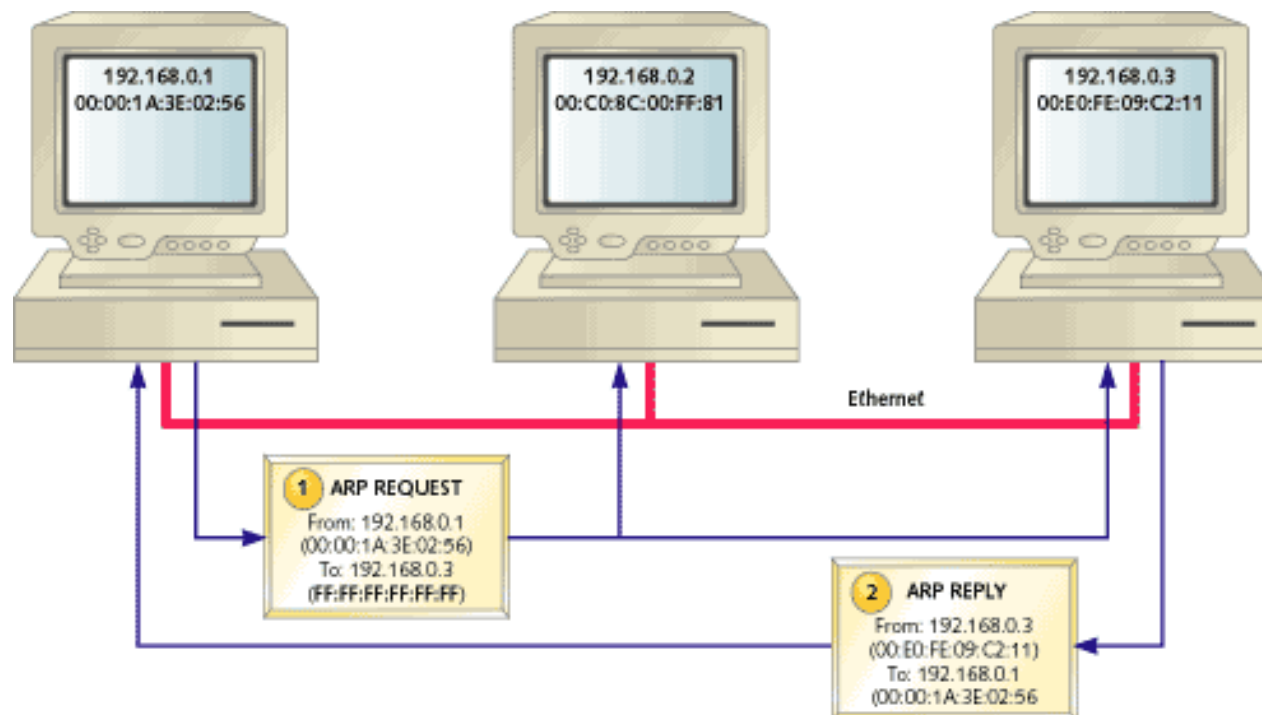
O protocolo ARP (Address Resolution Protocol) é responsável por fazer a resolução de endereços IP lógicos em endereços físicos conhecidos como MAC (Media Access Control), que já vem gravados na placa de rede pelo fabricante.





Protocolo ARP

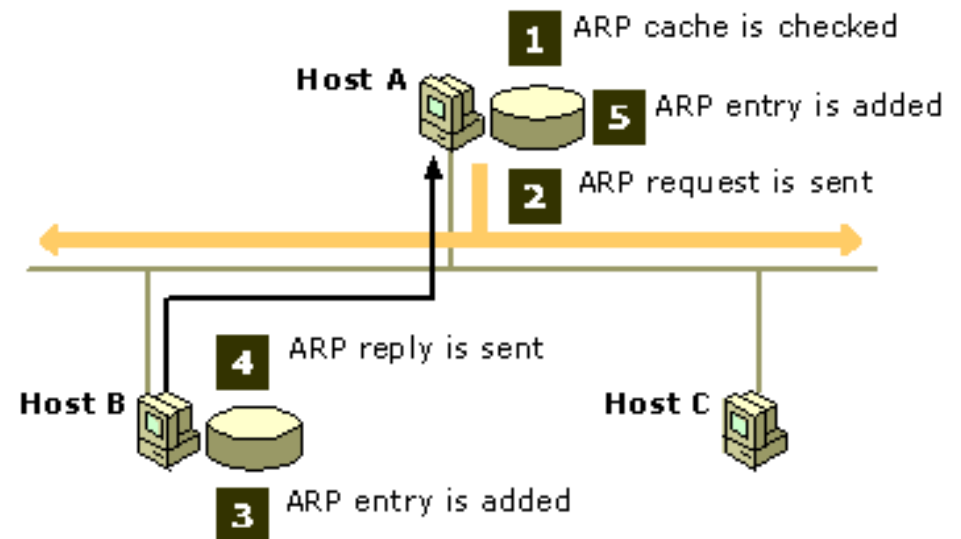
Na figura abaixo, o *host* cujo IP é 192.168.0.1 deseja comunicar-se com o *host* de IP 192.168.0.3. Como na camada de enlace a comunicação é feita via endereço MAC, e o primeiro *host* não conhece o MAC do destino, ele então envia um pacote ARP para o endereço especial FF-FF-FF-FF-FF-FF, de modo que todos os *hosts* deste segmento recebam a mensagem. Neste caso, somente o destinatário irá responder a mensagem com seu endereço MAC, e então o emissor poderá criar uma nova mensagem com o MAC destino.





Protocolo ARP - exemplo

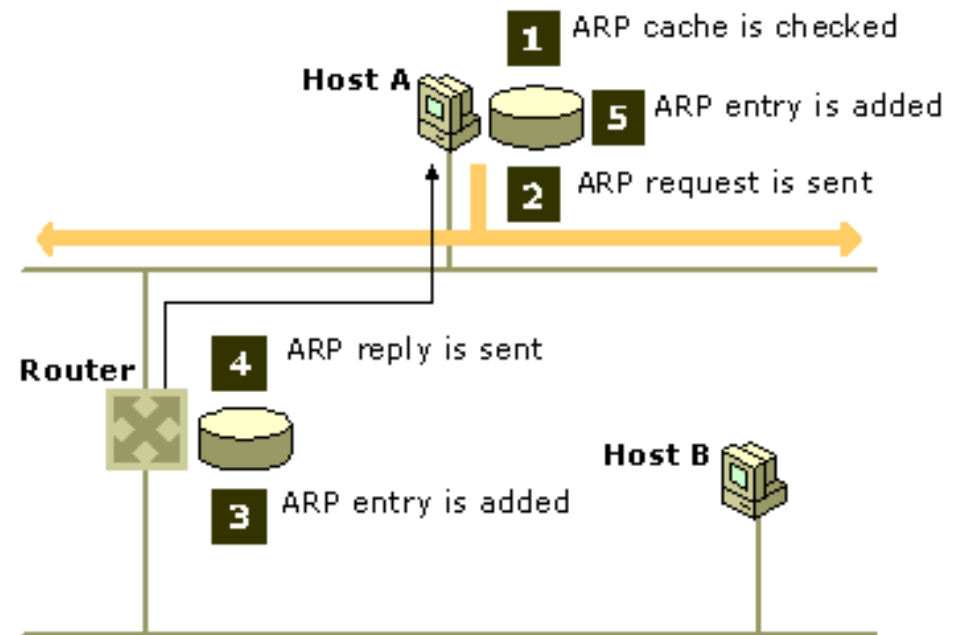
Na figura ao lado, o Host A deseja comunicar-se com o Host B, e verifica no cache se o endereço MAC do destino é conhecido [1]. Em caso negativo, um pacote ARP Request é disparado na rede [2]. Quando o Host B recebe o pacote, este armazena no cache o endereço MAC do Host A [3] e envia um pacote ARP Reply na rede [4], que é recebido pelo Host A e que armazena o endereço MAC aprendido no cache [5].





Protocolo ARP - exemplo

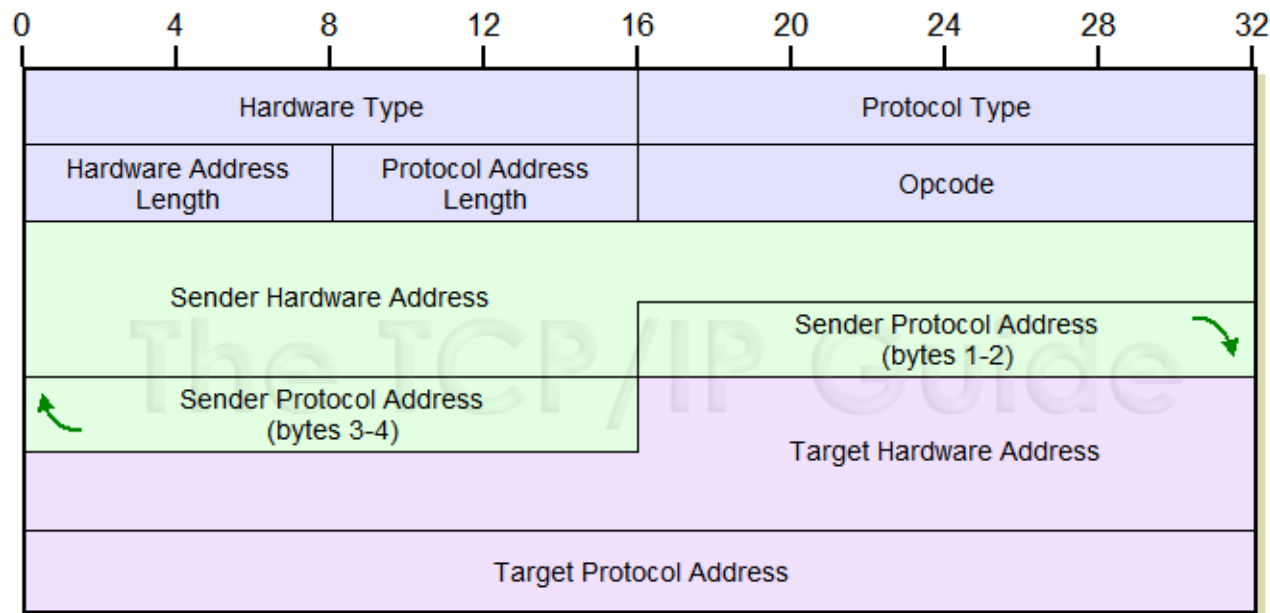
Na figura ao lado, o Host A deseja comunicar-se com o Host B, e determina que para tal precisa enviar sua solicitação para o roteador. Então, o Host A verifica no cache se o endereço MAC do roteador é conhecido [1]. Em caso negativo, um pacote ARP Request é disparado na rede [2]. Quando o roteador recebe o pacote, este armazena no cache o endereço MAC do Host A [3] e envia um pacote ARP Reply na rede [4], que é recebido pelo Host A e que armazena o endereço MAC aprendido no cache [5].





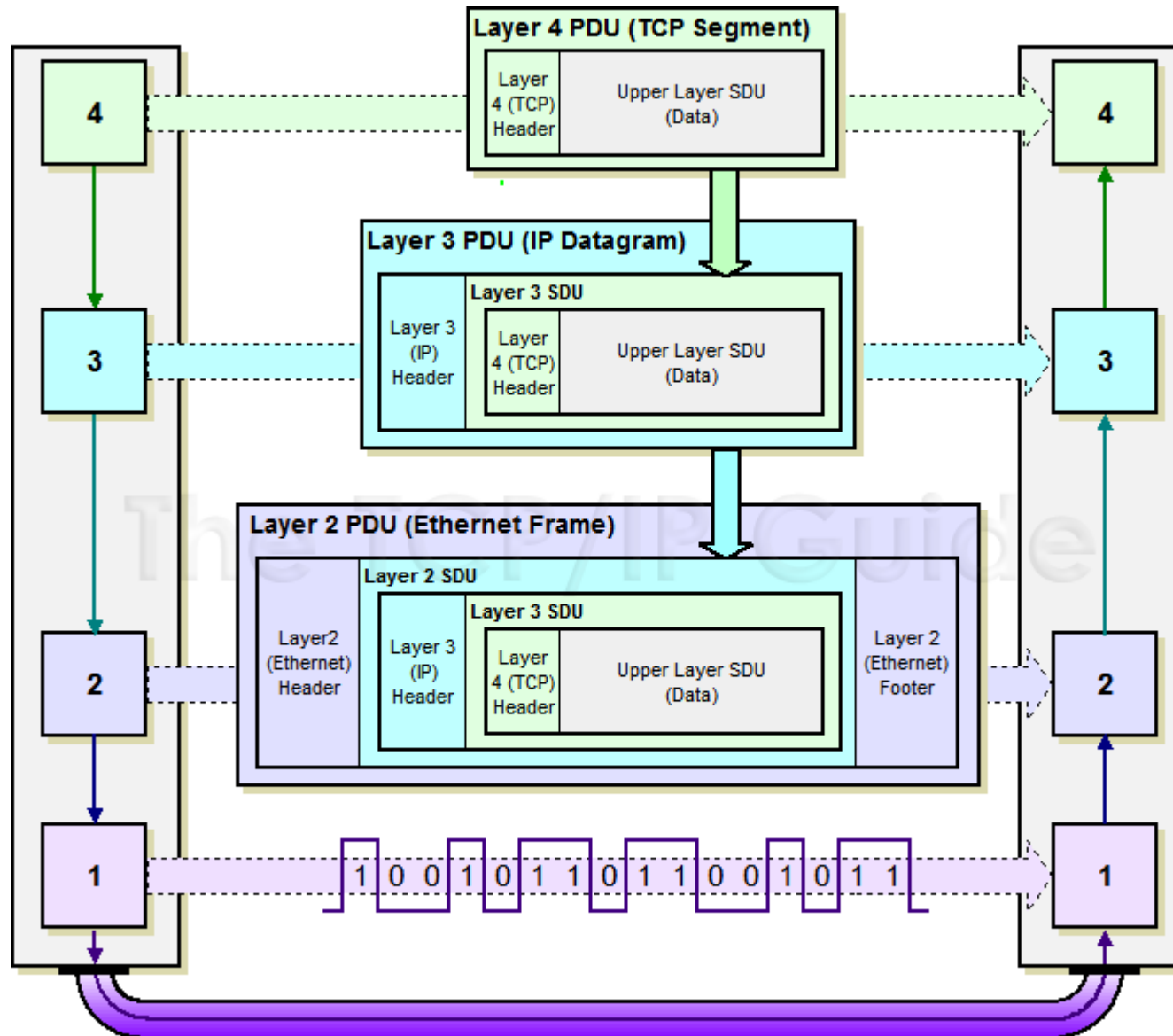
Protocolo ARP - Cabeçalho

O cabeçalho do protocolo ARP possui 28 bytes de tamanho, e possui informações sobre o endereço MAC físico e IP lógico da origem e do destino.





Fluxo de dados no modelo TCP/IP





Para saber mais...

- ... acesse o simulador de Fragmentação IP, de Ryan Gilbert.
- ... acesse o simulador de Roteamento IP, de Gil Messerman, Gilad Karni e Uri Braun.
- ... leia o documento sobre Protocolo ARP, da Microsoft.

FIM