Redes de Computadores e Sistemas Distribuídos

Prof. Me. Wallace Rodrigues de Santana

www.neutronica.com.br

Atribuição-NãoComercial-CompartilhaIgual 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.

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.

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.

Módulo Zero

Apresentação da Disciplina

Objetivo geral

- Apresentar aos alunos 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.
- Capacitar os alunos na compreensão dos principais serviços de redes e apresentar as características fundamentais da transmissão de dados em redes de computadores.
- Apresentar aos alunos os principais aspectos relacionados aos sistemas distribuídos para subsidiá-los na construção de aplicações distribuídas;
- Apresentar aos alunos os principais conceitos relacionados à arquitetura, processos, comunicação e sincronização, consistência e replicação, bem como tolerância a falhas em uma aplicação distribuída.

Objetivos específicos

- Identificar e compreender a funcionalidade dos elementos lógicos e físicos de redes de computadores;
- Compreender e aplicar os serviços ligados as redes de computadores e Internet, tais como DNS, Web, E-mail, FTP, entre outros;
- Compreender a arquitetura de sistemas distribuídos;
- Compreender o que são processos e chamada de procedimento remoto;
- Compreender a nomeação de identificadores e endereços;
- Compreender a sincronização de relógios e a consistência e replicação de dados;
- Compreender as técnicas de tolerância a faltas.

Módulos

PARTE I

1. Modelos de Referência OSI e TCP/IP
2. Protocolo IP
3. DHCP
4. DNS
5. FTP
6. Web
7. Correio Eletrônico
8. Camada de Transporte
9. Camada de Rede
10. Topologias e Tipos de Redes
11. Camada de Enlace
12. Camada Física

Módulos

PARTE II

1. Introdução a Sistemas Distribuídos
2. Arquitetura de Sistemas Distribuídos
3. Processos
4. Comunicação
5. Nomeação
6. Sincronização
7. Consistência e Replicação
8. Tolerância a Falhas

Ementa

- Histórico e evolução das Redes de Computadores;
- Modelo de Referência OSI e TCP/IP;
- Camada de Aplicação e Serviços;
- Camada de Transporte e Protocolos;
- Camada de Rede e Protocolos;
- Topologias e Tipos de Redes;
- Camadas de Enlace e Física;
- Introdução a Sistemas Distribuídos;
- Arquitetura de Sistemas Distribuídos;
- Processos;
- Comunicação;
- Nomeação e Sincronização em Sistemas Distribuídos;
- Consistência e Replicação;
- Tolerância a Falhas em Sistemas Distribuídos.

Referências

BÁSICAS

KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet: uma abordagem Top-Down.** 6ª ed. São Paulo: Pearson, 2013. E-book.

TANENBAUM, Andrew S.; WETHERALL David. **Redes de Computadores.** 5ª ed. São Paulo: Pearson Brasil, 2011. E-book.

TANENBAUM, Andrew S.; STEEN, Maarten Van. **Sistemas Distribuídos: Princípios e Paradigmas.** 2ª ed. São Paulo: Pearson Brasil, 2007.

COMPLEMENTARES

FOROUZAN B. **Comunicação de Dados e Redes de Computadores**. Mcgraw Hill. 2008.

MORIMOTO, C.E. **Redes - Guia Prático.** Porto Alegre: Sul Editores, 2010.

THOMPSON, M. A. **Windows Server 2012 - Instalação, Configuração e Administração de Redes.** São Paulo: Editora Érica, 2012.

TIBET, C.V. **Linux - Administração e Suporte.** 1ª ed. São Paulo: Novatec, 2001.

WHITE, Curt. **Redes de Computadores e Comunicação de Dados**. Cengage. 2012.

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

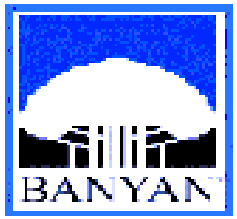
No inicio da década de 1980 a *International Organization for Standardization* (ISO) criou um modelo de referência para conexão de redes denominado *Open Systems Interconnection* (norma ISO 7498:1984), que ficou conhecido como modelo ISO/OSI ou simplesmente modelo OSI.

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.



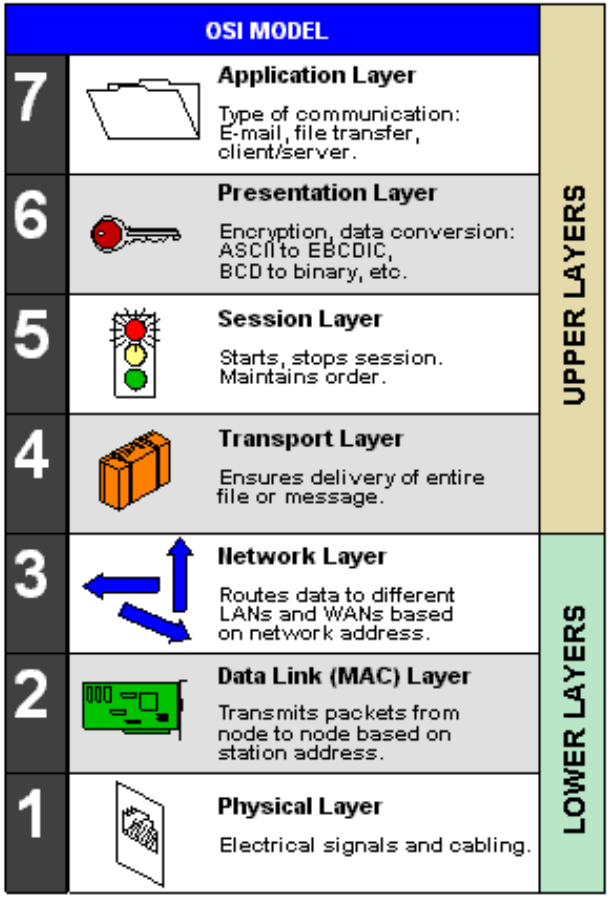
Modelo de referência OSI

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.

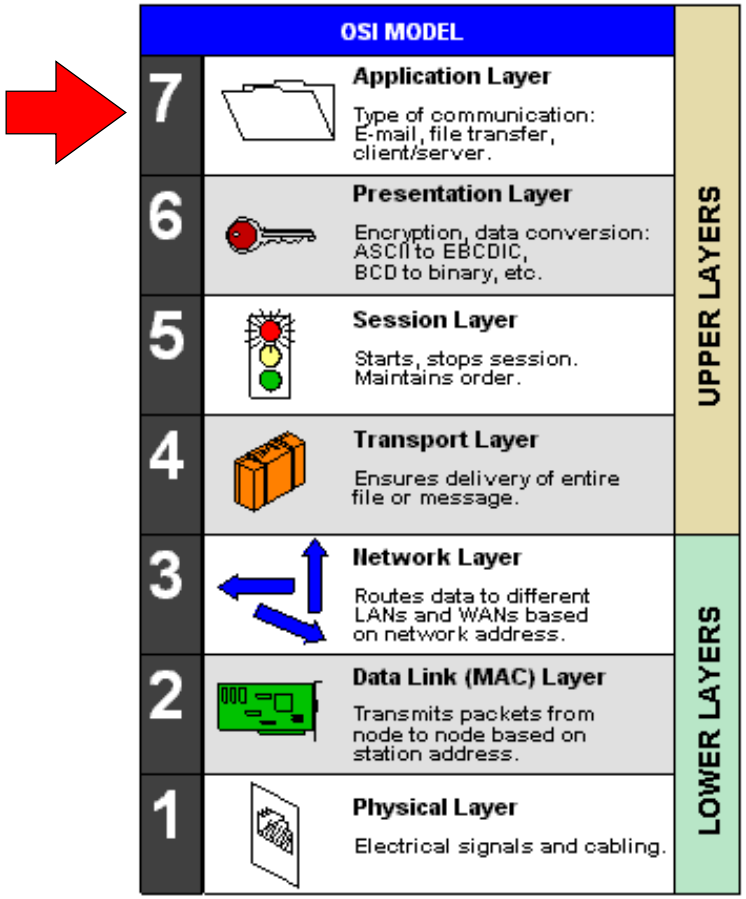


Fonte: Computer Desktop Encyclopedia

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.

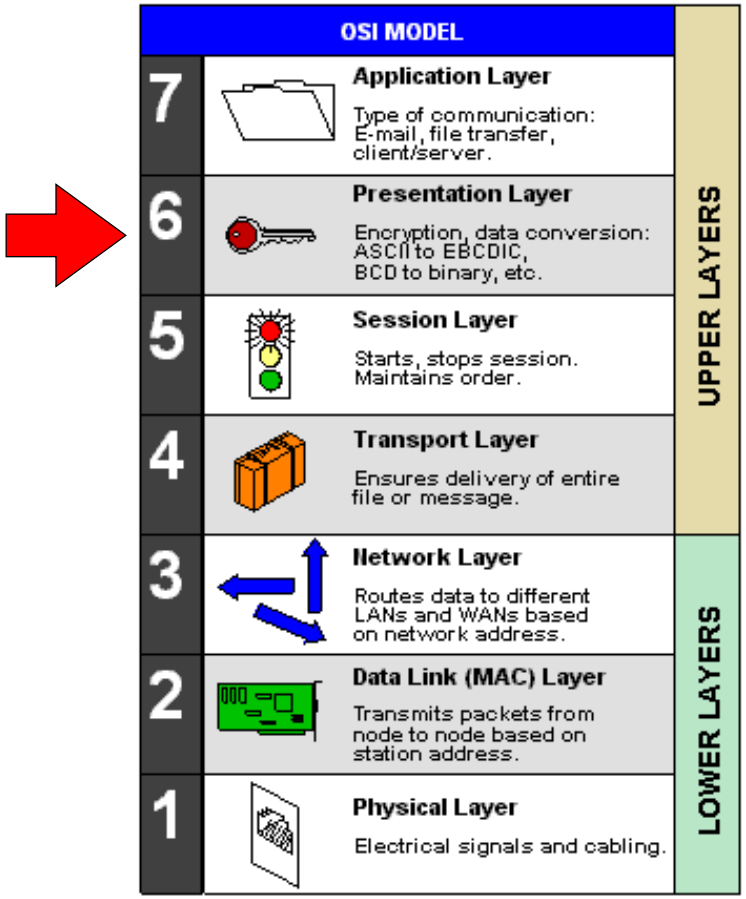


Fonte: Computer Desktop Encyclopedia

Camada de apresentação

Esta camada é responsável por converter os dados em um formato universal que possa ser interpretado por sistemas de plataformas diferentes.

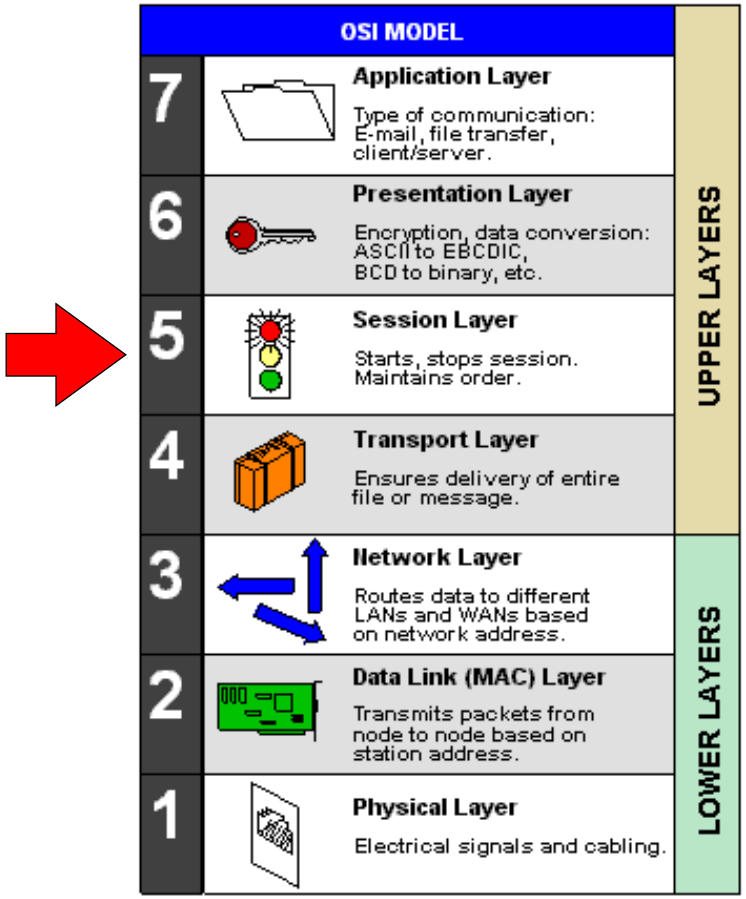
É nesta camada que as operações de criptografia e compactação de dados são executadas.



Fonte: Computer Desktop Encyclopedia

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.



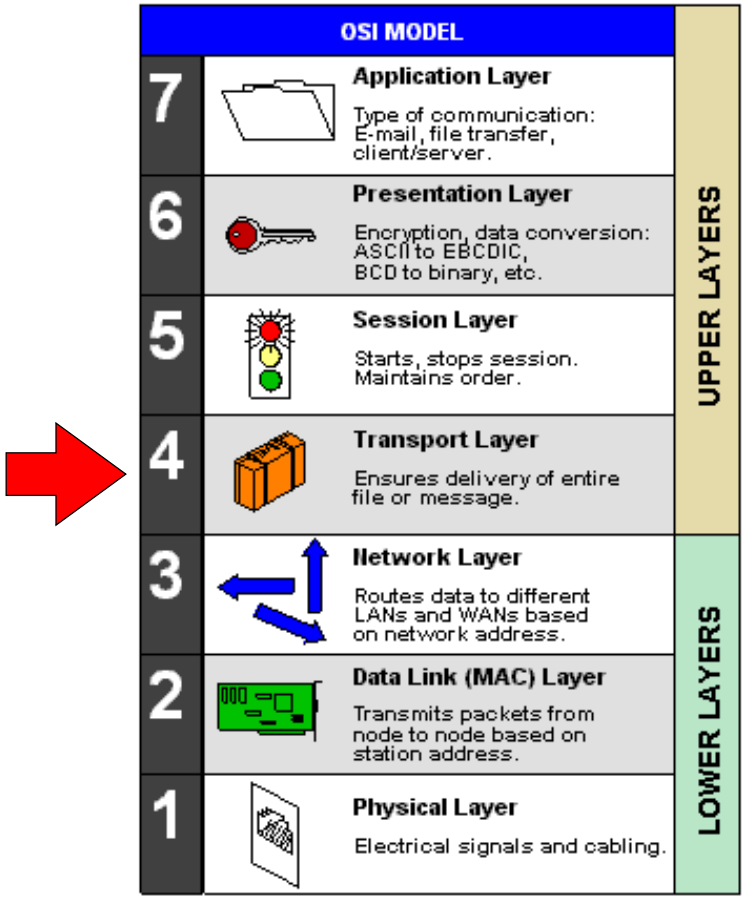
Fonte: Computer Desktop Encyclopedia

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).

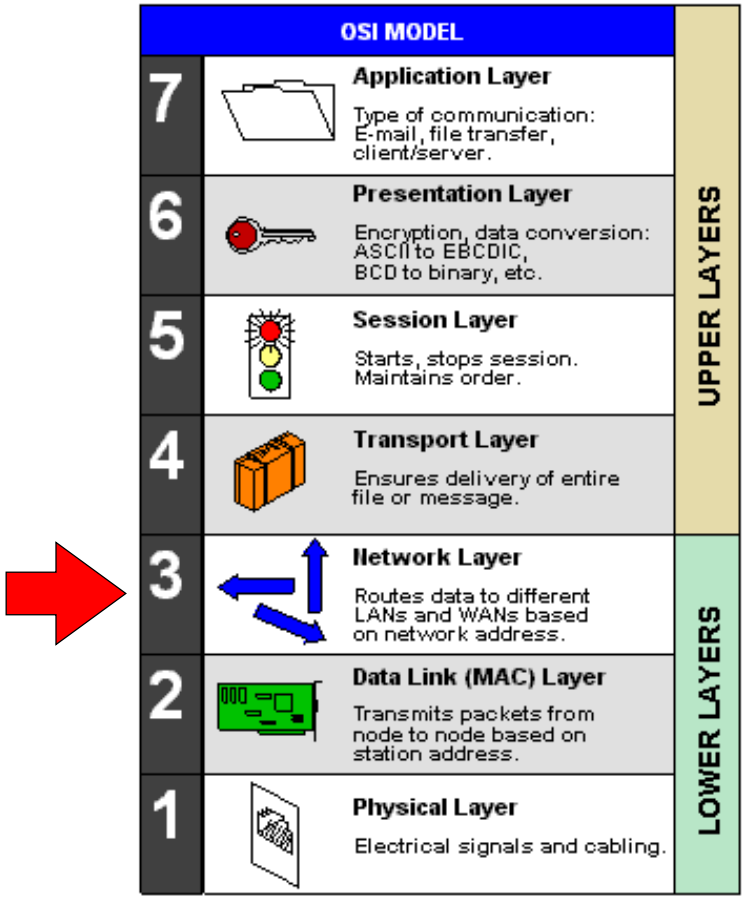


Fonte: Computer Desktop Encyclopedia

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.

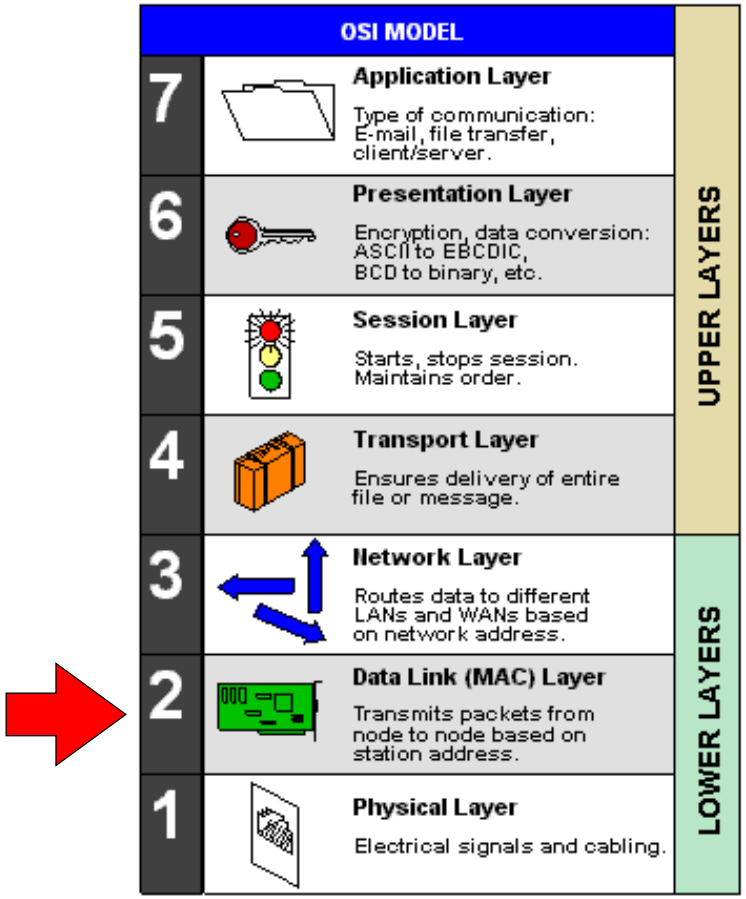


Fonte: Computer Desktop Encyclopedia

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.

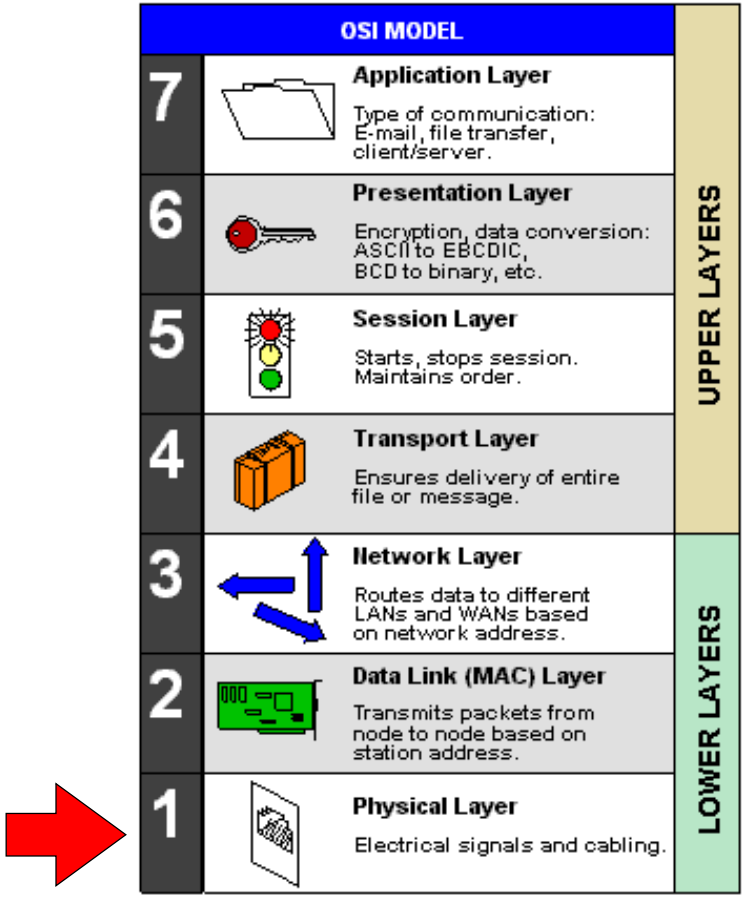


Fonte: Computer Desktop Encyclopedia

Camada física

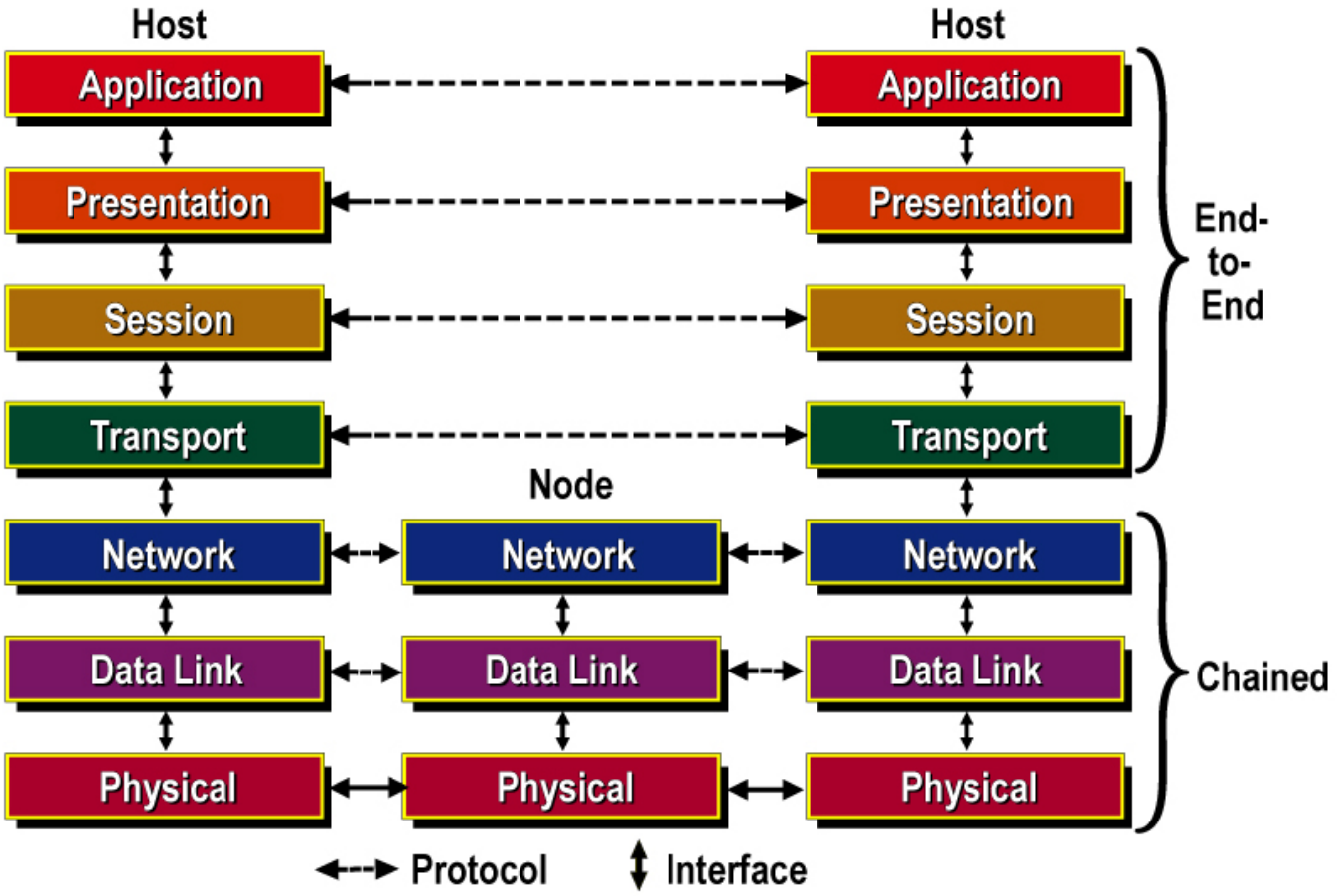
A camada física define as especificações elétricas, físicas e mecânicas dos meios físicos de transmissão.

Esta camada é responsável por enviar uma sequencia de bits entre a origem e o destino.

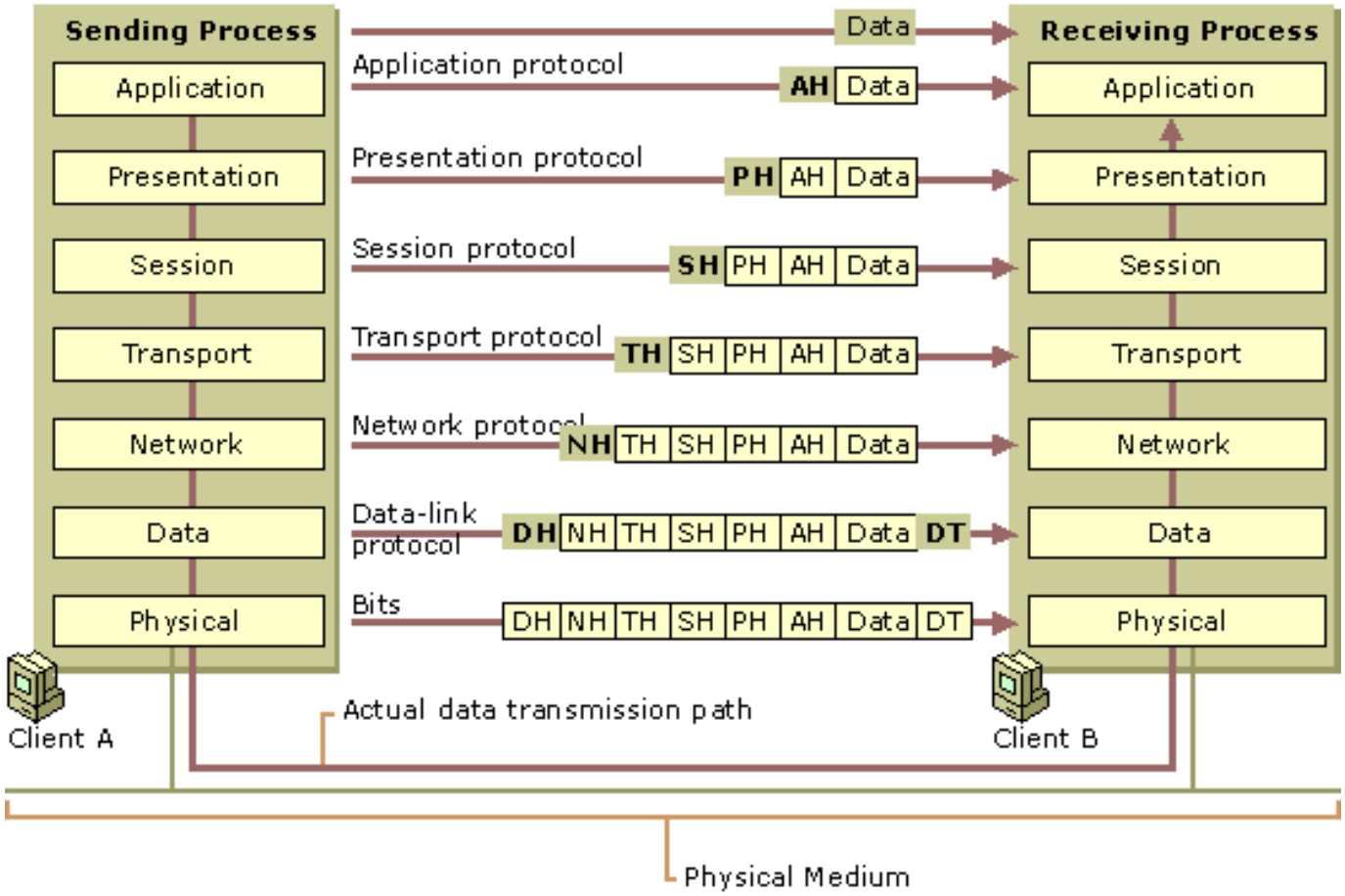


Fonte: Computer Desktop Encyclopedia

Relação entre as camadas



Fluxo de dados no modelo OSI



Modelo de referência TCP/IP

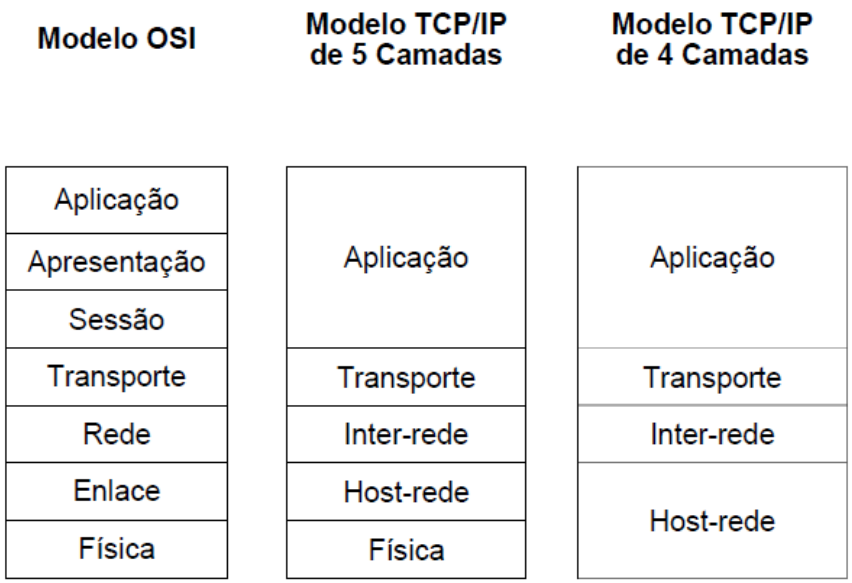
O modelo de referência TCP/IP surgiu de um projeto do exército dos Estados Unidos com o objetivo de criar uma rede que fosse tolerante à falhas.

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.

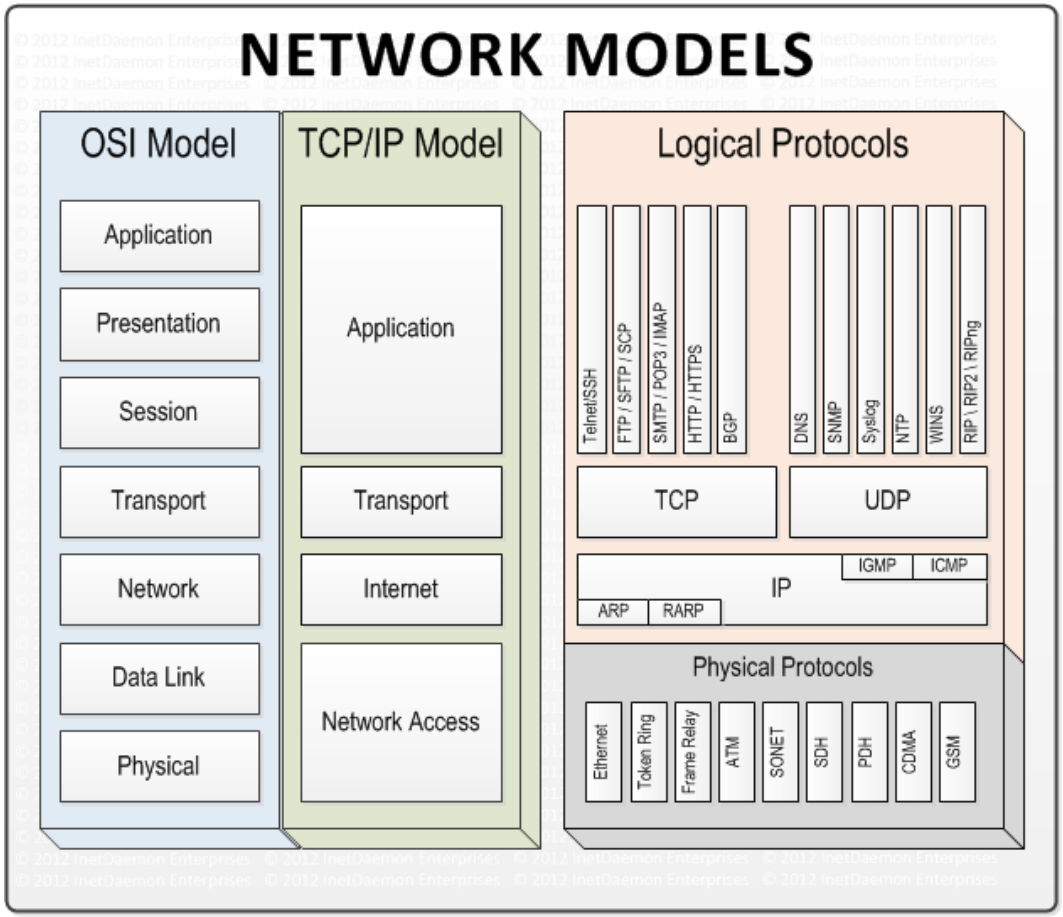
O Modelo de Referência não seguiu a mesma padronização do Modelo OSI, e por isso alguns autores adotam um modelo de 4 camadas, enquanto outros adotam o modelo de 5 camadas.

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

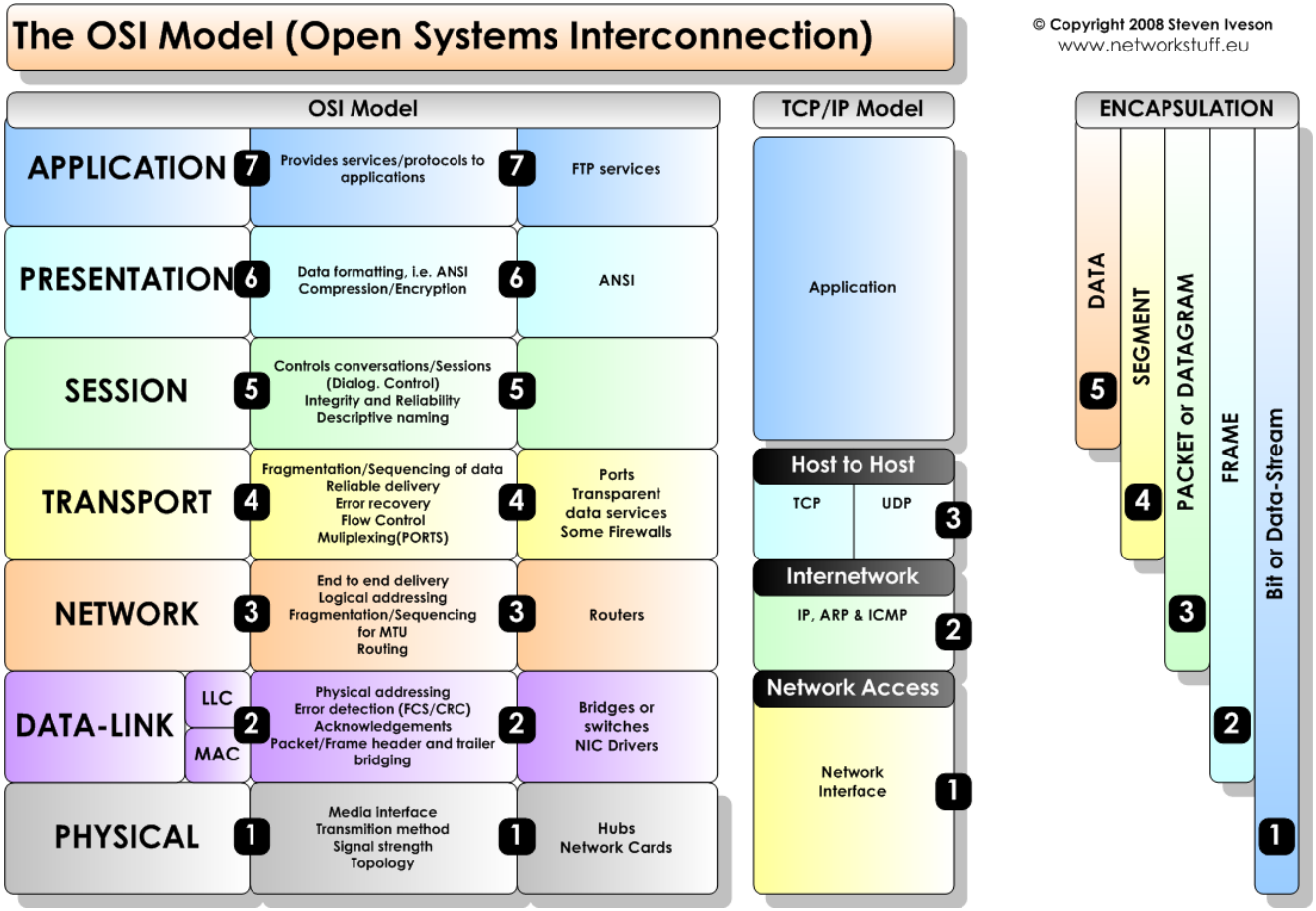
O Modelo de Referência TCP/IP recebe este nome porque seus dois principais protocolos são o de transporte (TCP) e o de rede (IP).



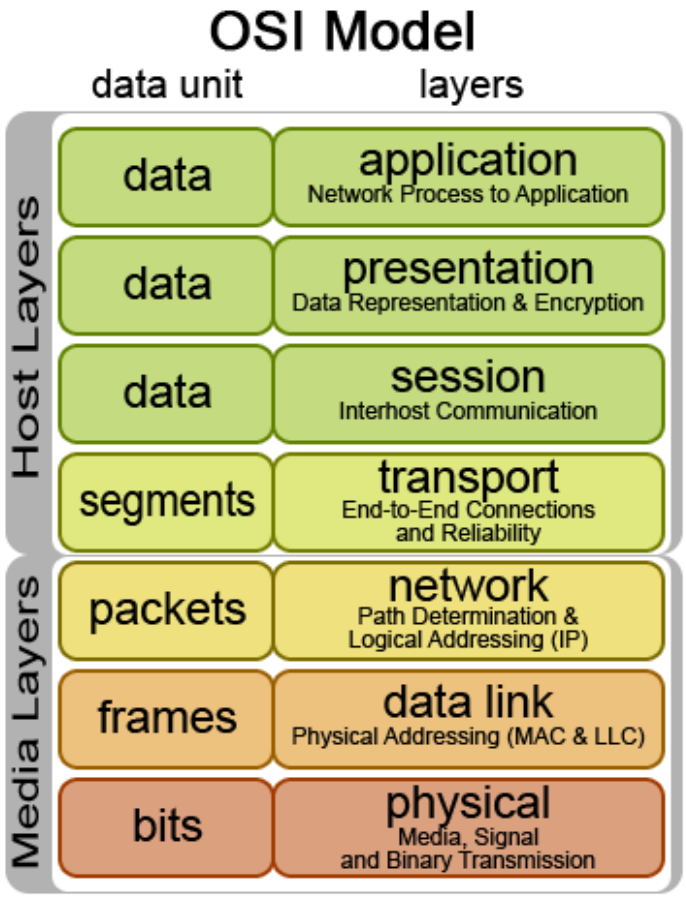
Relação entre os modelos OSI e TCP/IP



Relação entre os modelos OSI e TCP/IP

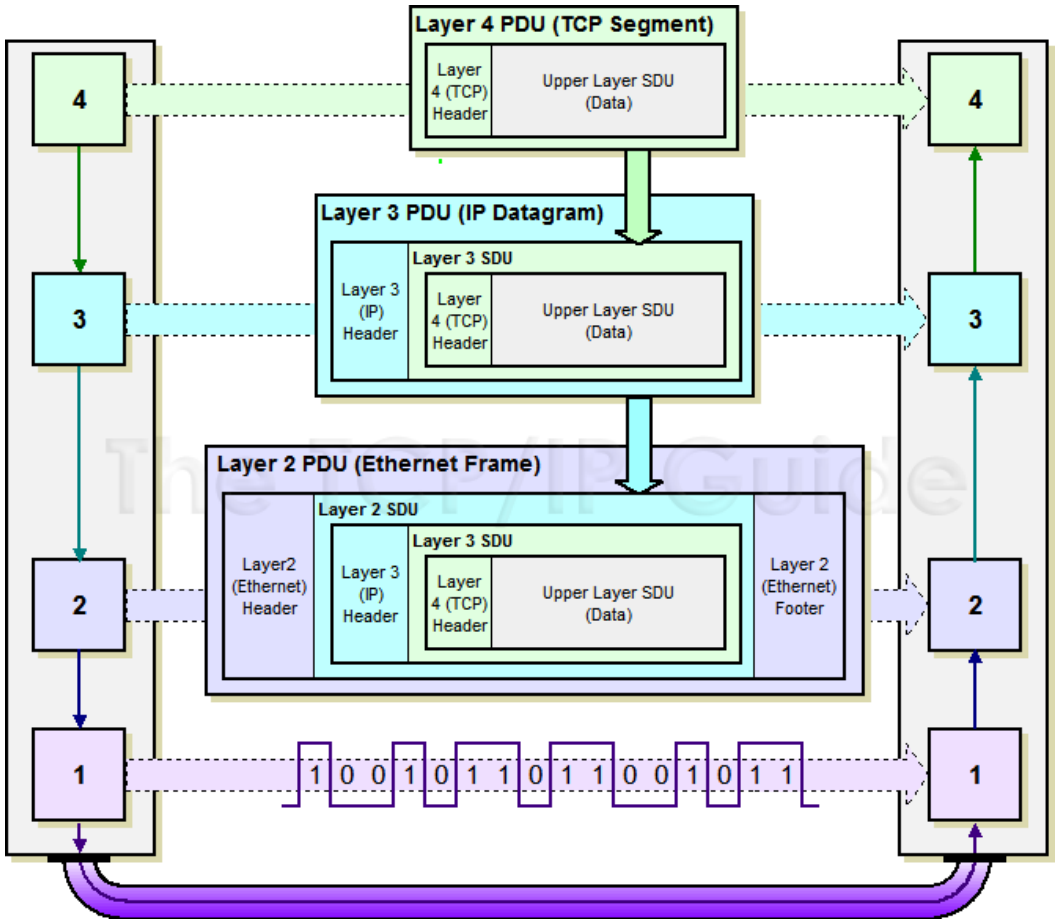


Unidades de informação



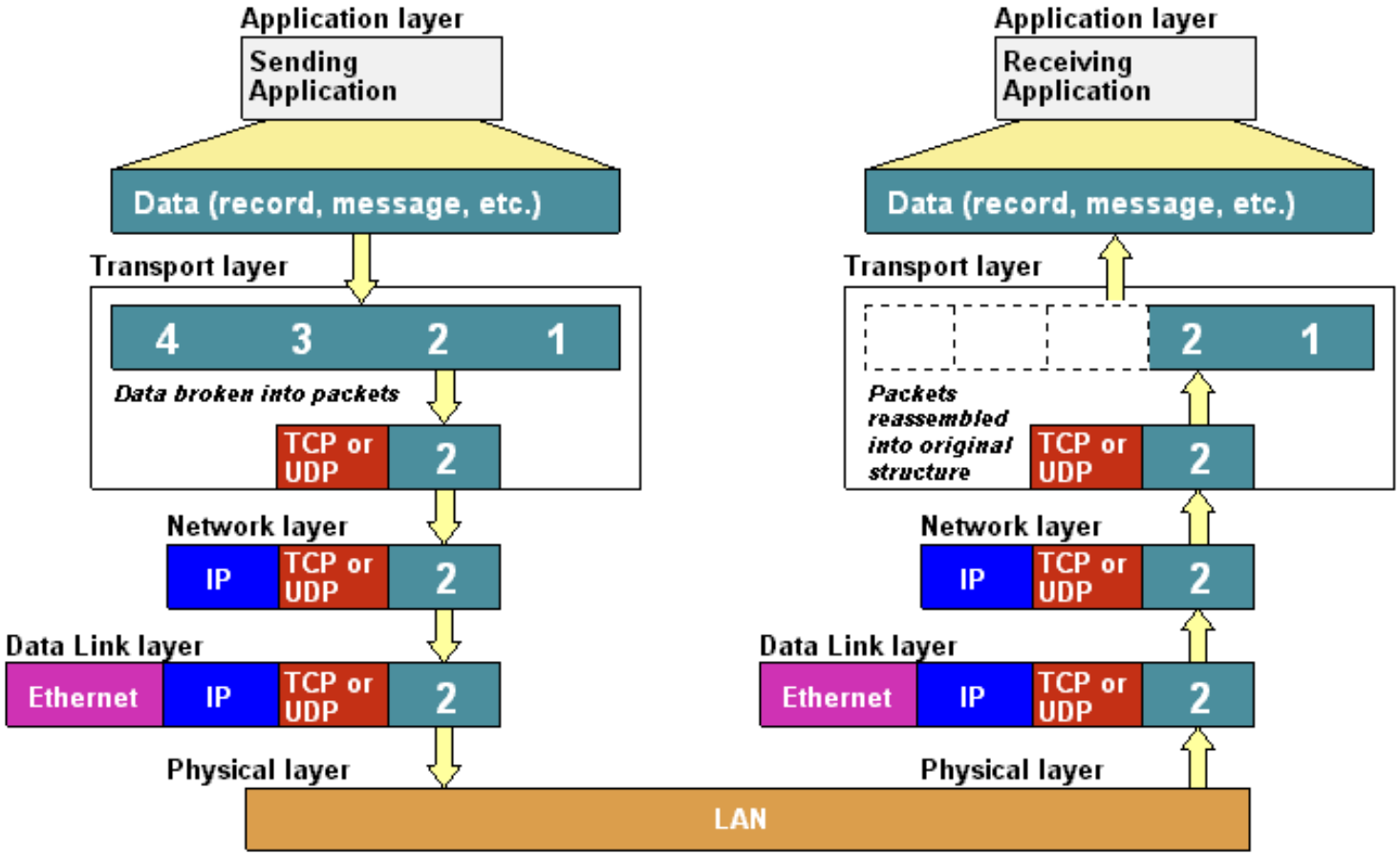
CAMADA	UNIDADE DE INFORMAÇÃO
Aplicação, Apresentação e Sessão	Mensagem ou Dados
Transporte	Segmento
Rede	Pacote ou Datagrama
Enlace	Quadro ou Frame
Física	Bits

Fluxo de dados no modelo TCP/IP

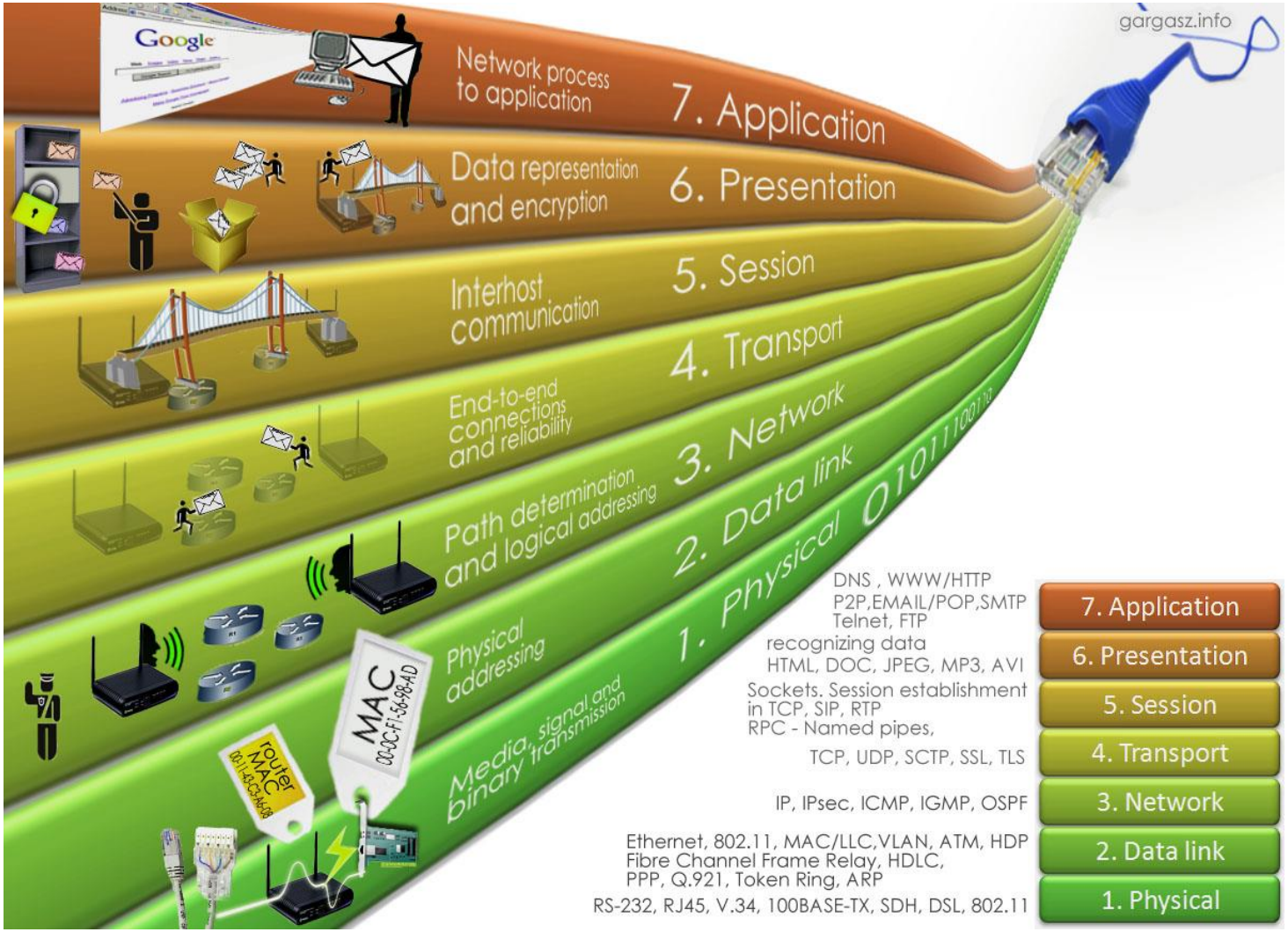


PDU – Protocol Data Unit
SDU – Service Data Unit

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.

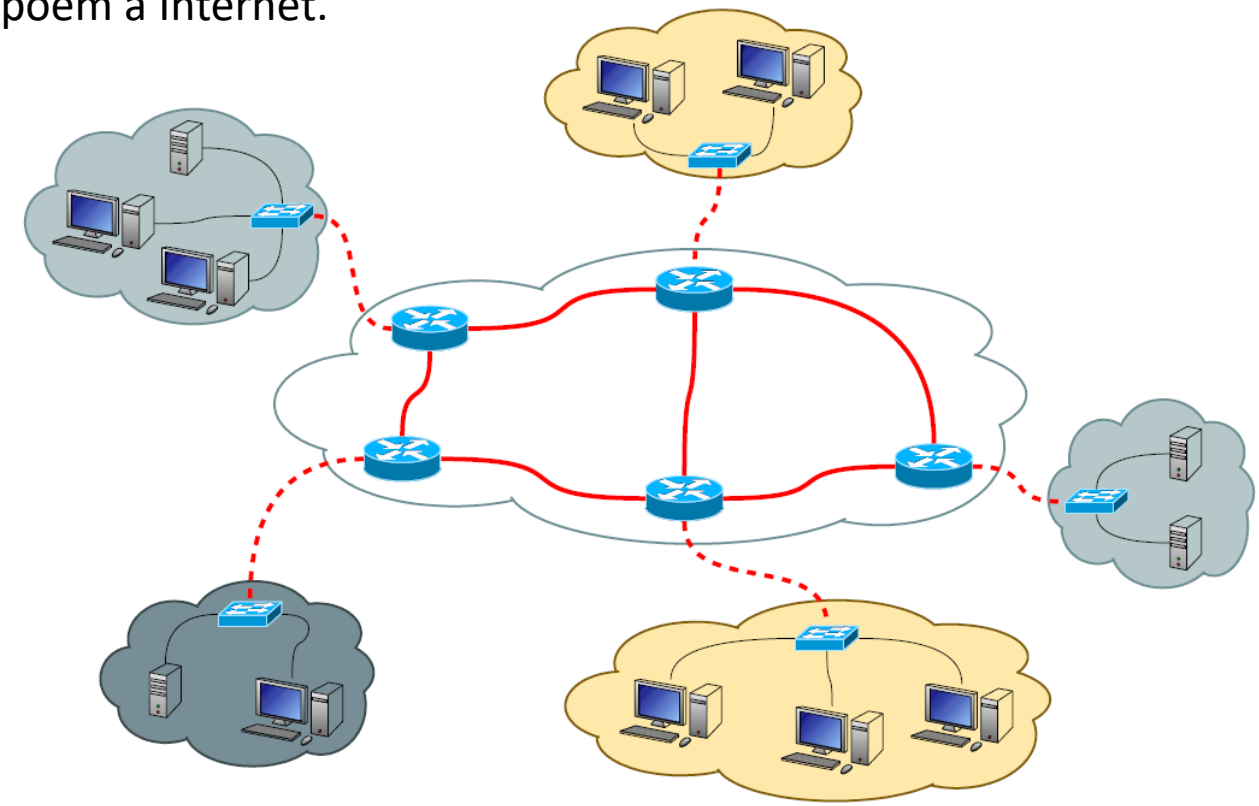
… acesse o artigo OSI Reference Model – The ISO Model of Architecture for Open Systems Interconnection, de Hubert Zimmermann.

Módulo 2

Camada de Rede e Protocolo IP

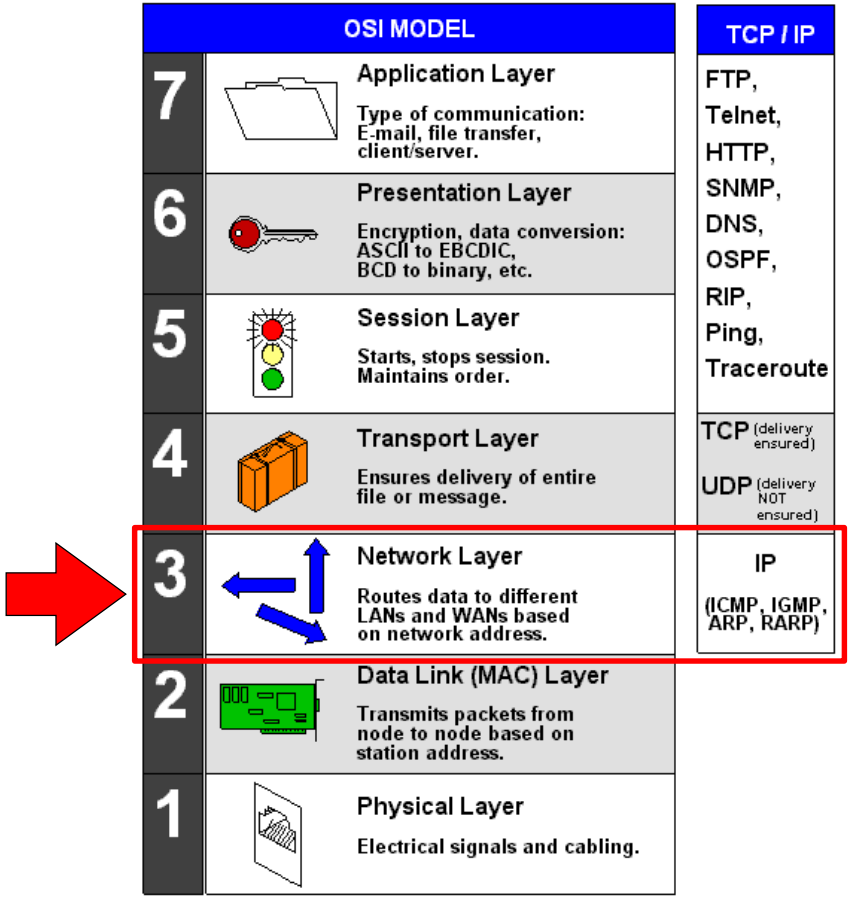
Introdução

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

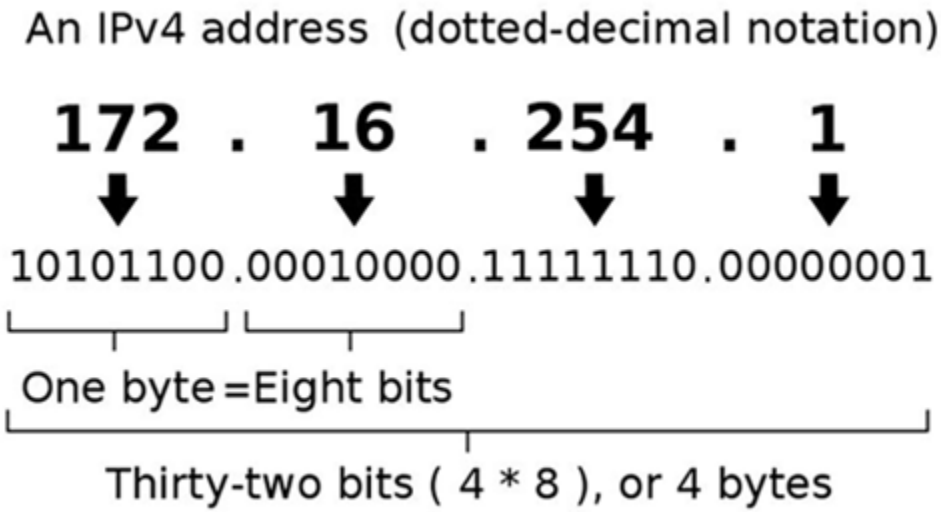
O Internet Protocol, ou simplesmente IP é um protocolo da camada de rede que tem por objetivo identificar unicamente um *host* na rede mundial de computadores e transmitir os datagramas (pacotes) da origem ao destino.



Fonte: Computer Desktop Encyclopedia

Endereço IPv4

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:



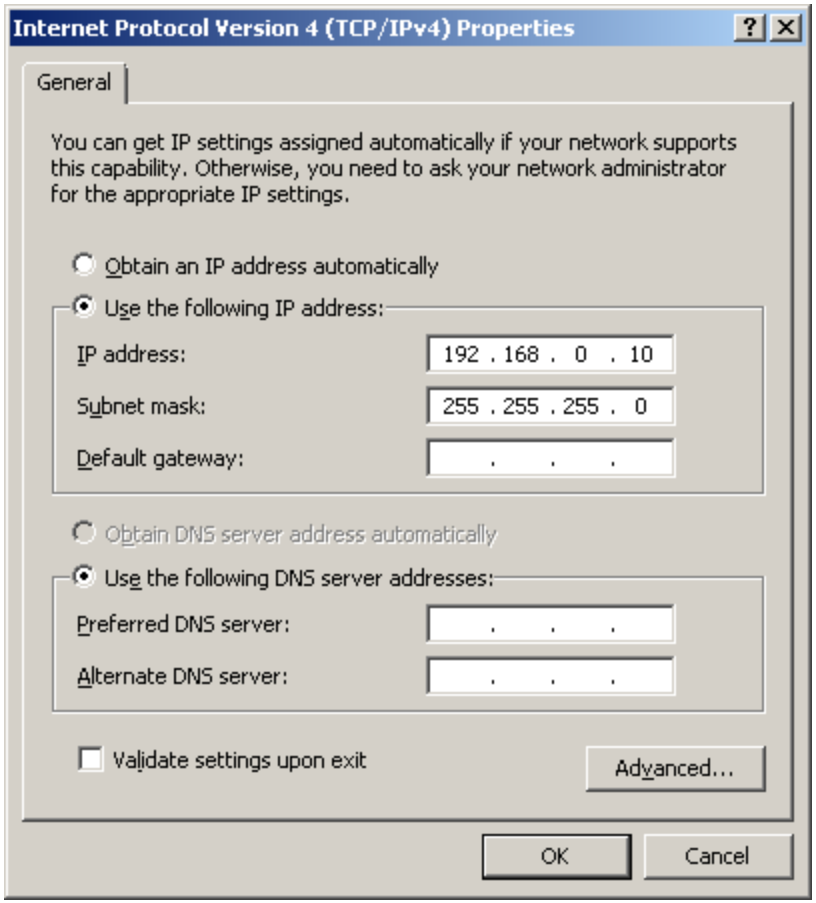
Máscara de rede

Todo *host* para funcionar na rede deve possuir um endereço IP, que o identifica unicamente na rede.

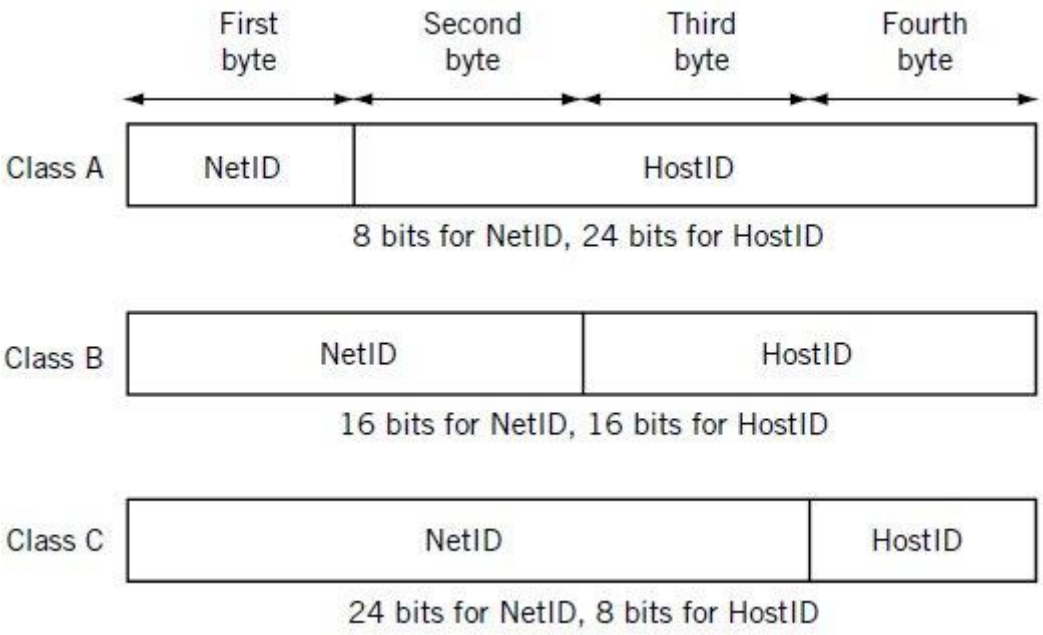
No entanto, o IP carrega duas informações: a rede onde o *host* está conectado e o próprio *host*.

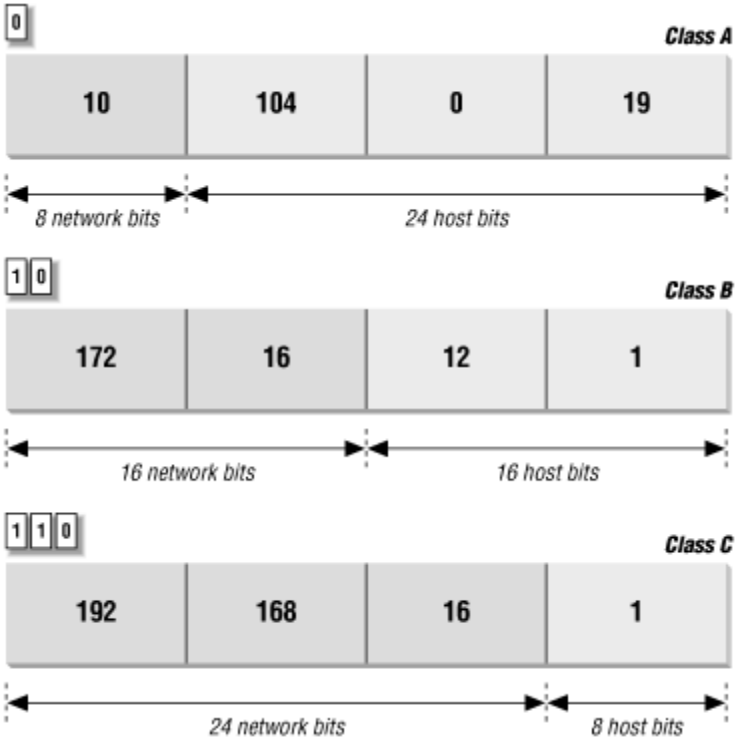
Estas duas informações são obtidas por meio da máscara de rede.

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

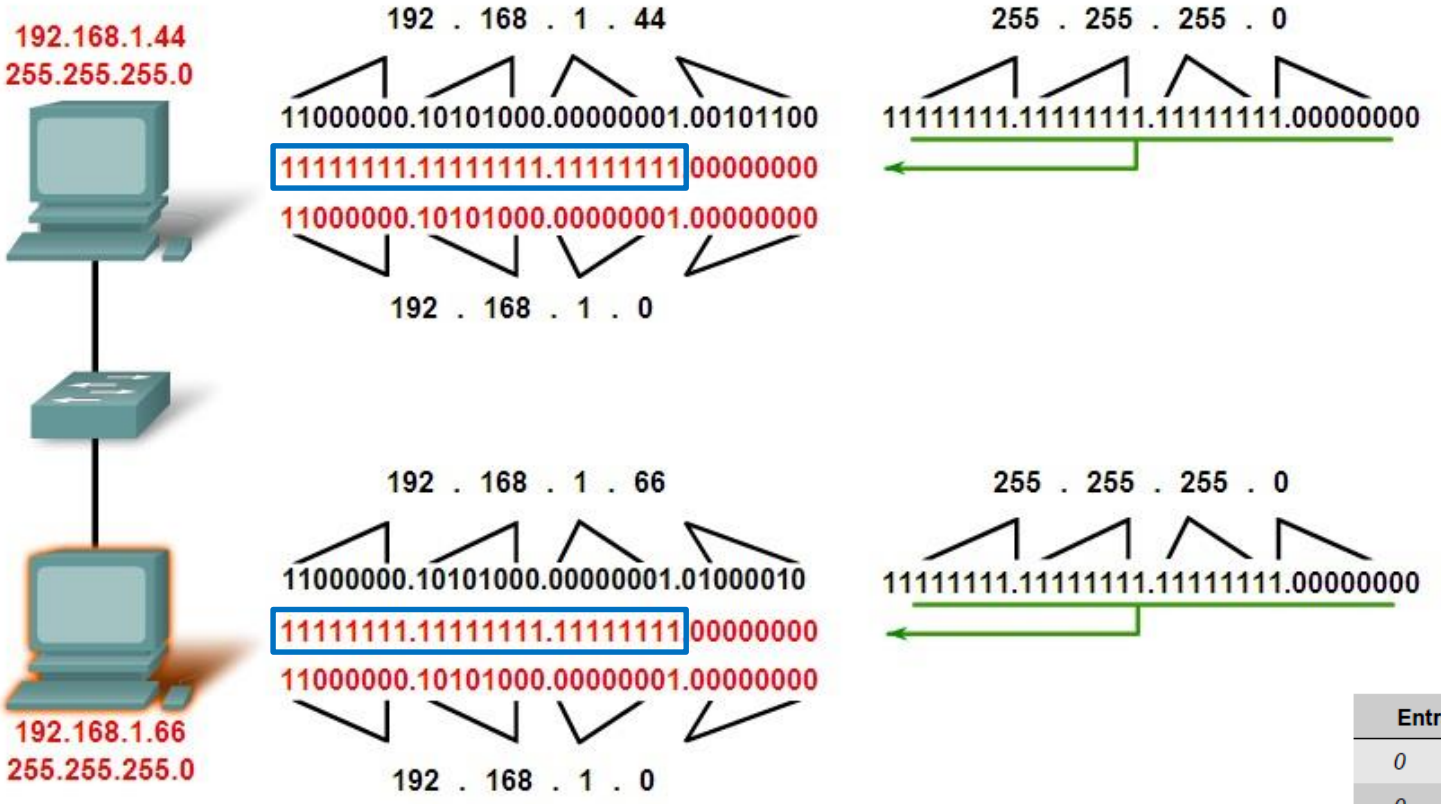


Máscara de rede



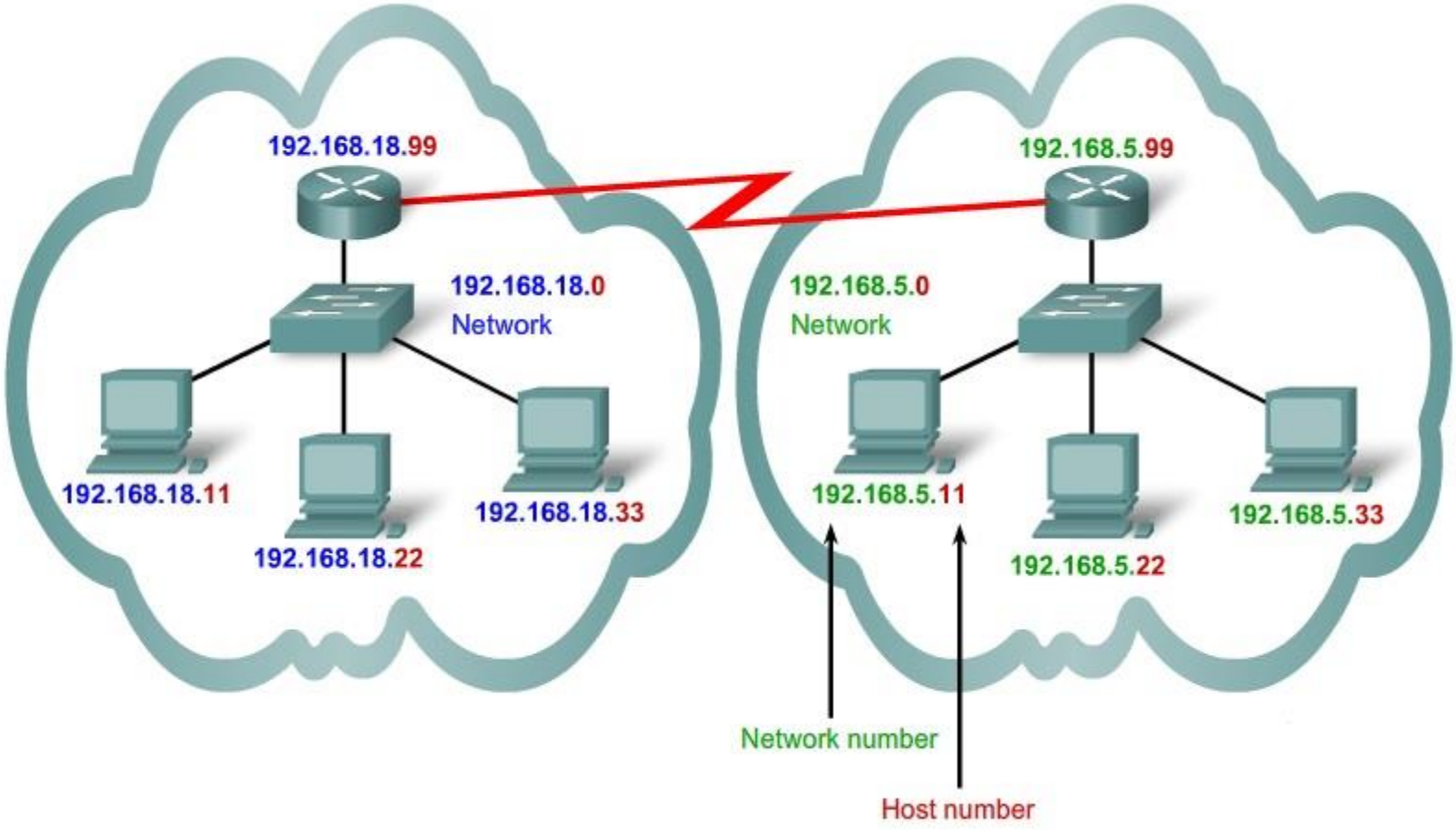


Operação “E” lógico

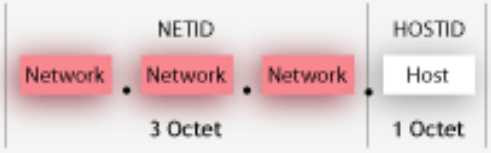


Entradas		Saída
0	0	0
0	1	0
1	0	0
1	1	1

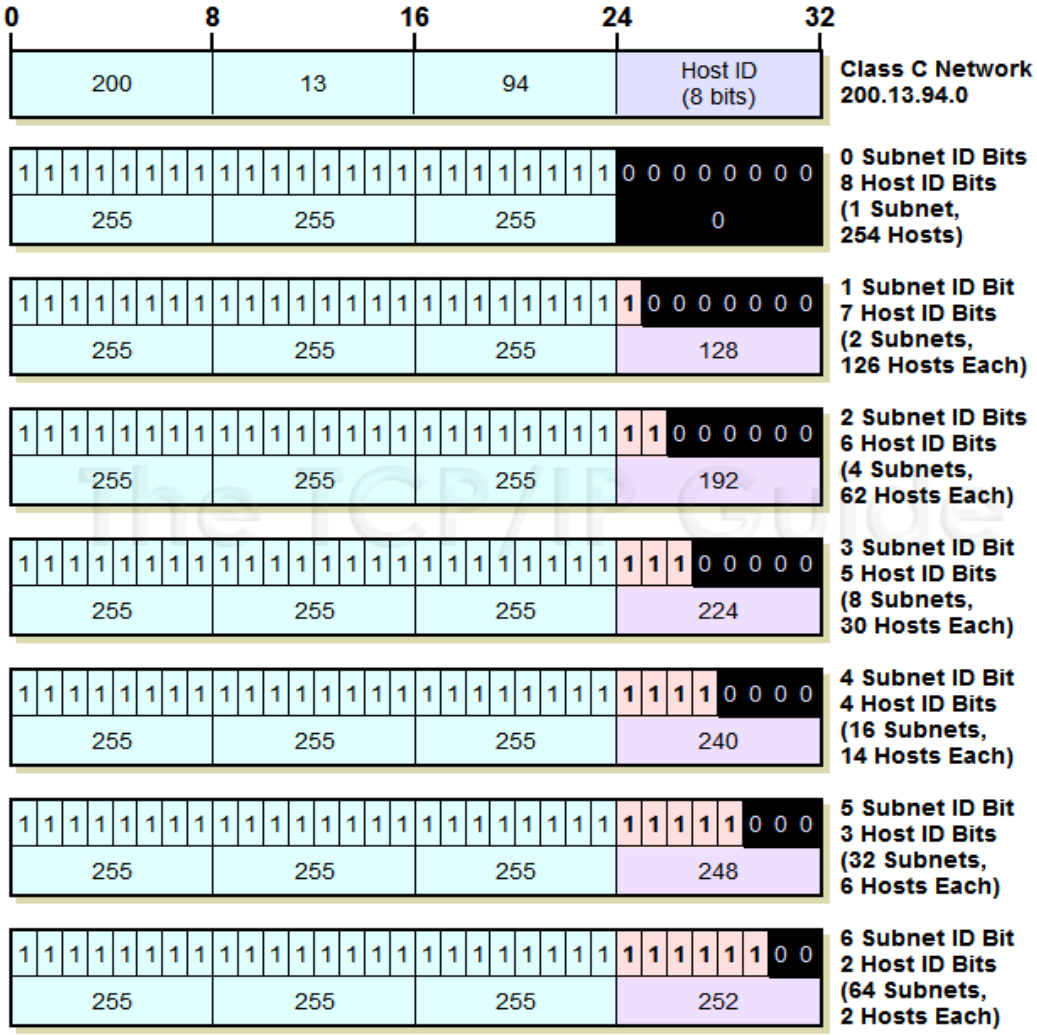
Redes distintas



Máximo de hosts por classe

CLass	First Octet Range	Default Subnet Mask	Max Hosts	Format
A	1-126	255.0.0.0	16M	
B	128-191	255.255.0.0	64K	
C	192-223	255.255.255.0	254	
D	224-239	N/A	N/A	
E	240-255	N/A	N/A	

Criando subredes



Máscara de rede – notação

Máscara	CIDR
0.0.0.0	/0
128.0.0.0	/1
192.0.0.0	/2
224.0.0.0	/3
240.0.0.0	/4
248.0.0.0	/5
252.0.0.0	/6
254.0.0.0	/7

Máscara	CIDR
255.0.0.0	/8
255.128.0.0	/9
255.192.0.0	/10
255.224.0.0	/11
255.240.0.0	/12
255.248.0.0	/13
255.252.0.0	/14
255.254.0.0	/15

Classe A

Máscara	CIDR
255.255.0.0	/16
255.255.128.0	/17
255.255.192.0	/18
255.255.224.0	/19
255.255.240.0	/20
255.255.248.0	/21
255.255.252.0	/22
255.255.254.0	/23

Classe B

Máscara	CIDR
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30
255.255.255.254	/31

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.

IP público e privado

A IANA (Internet Assigned Numbers Authority) reservou três blocos do espaço de endereço IP para redes privadas:

- 10.0.0.0 - 10.255.255.255 (prefixo 10/8);
- 172.16.0.0 - 172.31.255.255 (prefixo 172.16/12);
- 192.168.0.0 - 192.168.255.255 (prefixo 192.168/16).

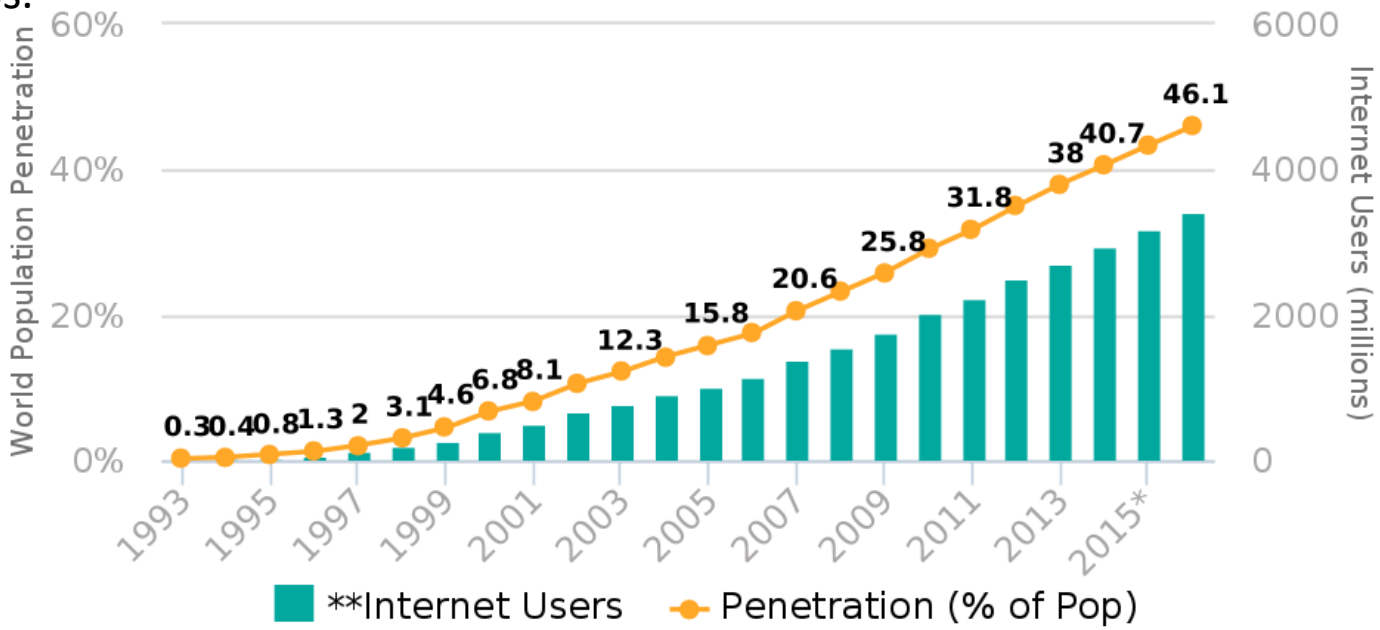
CIDR address block	Description	Reference
0.0.0.0/8	Current network (only valid as source address)	RFC 1700
10.0.0.0/8	Private network	RFC 1918
14.0.0.0/8	Public data networks	RFC 1700
127.0.0.0/8	Loopback	RFC 3330
128.0.0.0/16	Reserved (IANA)	RFC 3330
169.254.0.0/16	Link-Local	RFC 3927
172.16.0.0/12	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.

Esgotamento do IPv4

Como o IPv4 possui de 32 bits de tamanho, isso dá um total de aproximadamente 4 bilhões de endereços distintos possíveis.

Quando a pilha TCP/IP entrou em operação em 1983, acreditava-se que este número seria mais do que suficiente para endereçar os dispositivos existentes e futuros.



Fonte: statpedia.com com dados extraídos de internetlivestats.com

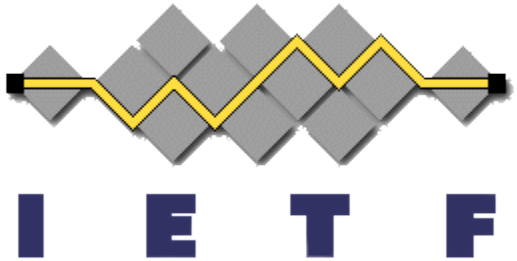
Esgotamento do IPv4

No entanto, passado mais três décadas, dada a popularização da Internet, o número de usuários tem crescido cada vez mais e mais, e se cada um dos 7 bilhões de habitantes da Terra precisa-se de um endereço IPv4, não haveria como atender a tal demanda.

Esgotamento do IPv4 – Alternativas CIDR

Diante do cenário de esgotamento dos endereços IPv4, a IETF (Internet Engineering Task Force) passou a discutir estratégias para solucionar a questão do esgotamento dos endereços IP e o problema do aumento da tabela de roteamento.

Para isso, em novembro de 1991, é formado um grupo de trabalho denominado ROAD (ROuting and Addressing), que apresentou como solução a estes problemas a utilização do CIDR (Classless Interdomain Routing).

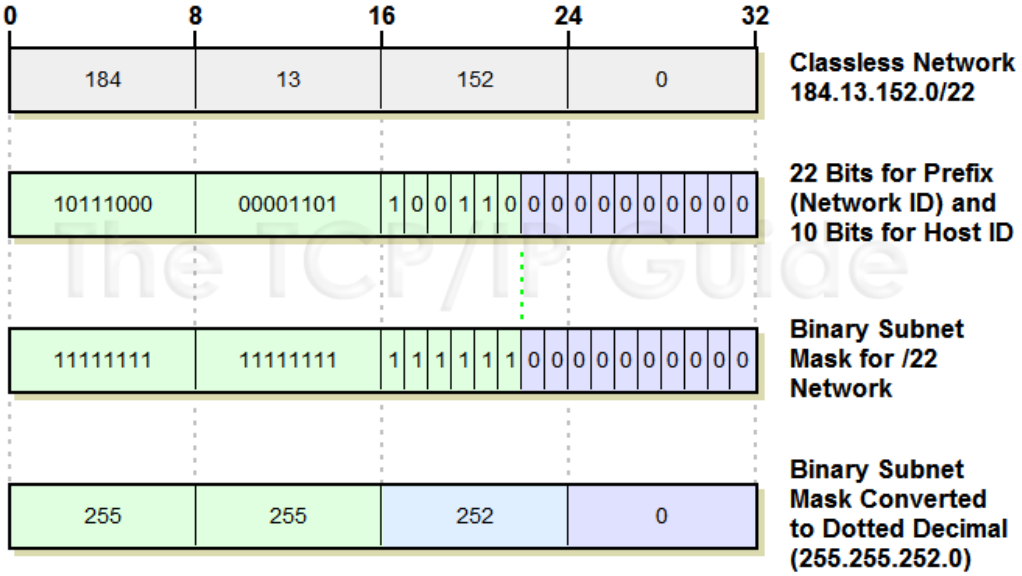


Fonte: ipv6.br

Esgotamento do IPv4 – Alternativas CIDR

Definido na RFC 4632 (tornou obsoleta a RFC 1519), o CIDR tem como ideia básica o fim do uso de classes de endereços, permitindo a alocação de blocos de tamanho apropriado a real necessidade de cada rede; e a agregação de rotas, reduzindo o tamanho da tabela de roteamento.

Com o CIDR os blocos são referenciados como prefixo de redes.

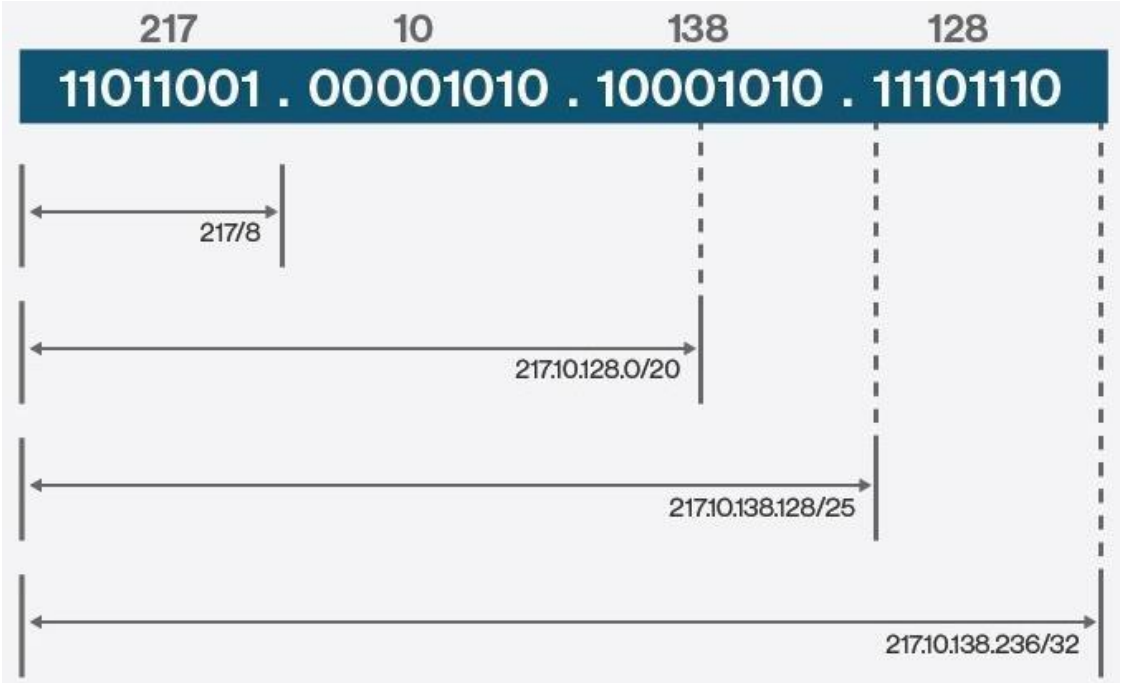


Fonte: ipv6.br

Esgotamento do IPv4 – Alternativas CIDR

Por exemplo, no endereço A.B.C.D/X, os X bits mais significativos indicam o prefixo da rede.

Outra forma de indicar o prefixo é através de máscaras, onde a máscara 255.0.0.0 indica um prefixo /8, 255.255.0.0 indica um /16, e assim sucessivamente.



Fonte: ipv6.br

Esgotamento do IPv4 – Alternativas DHCP

Outra solução, apresentada na RFC 2131 (tornou obsoleta a RFC 1541), foi o protocolo DHCP (Dynamic Host Configuration Protocol).

Através do DHCP um host é capaz de obter um endereço IP automaticamente e adquirir informações adicionais como máscara de rede, endereço do gateway (roteador padrão) e o endereço do servidor DNS local.

O DHCP tem sido muito utilizado por parte dos ISPs (Internet Service Provider) por permitir a atribuição de endereços IP temporários a seus clientes conectados.

Desta forma, torna-se desnecessário obter um endereço para cada cliente, devendo-se apenas designar endereços dinamicamente, através de seu servidor DHCP.

Este servidor terá uma lista de endereços IP disponíveis, e toda vez que um novo cliente se conectar a rede, lhe será designado um desses endereços de forma arbitrária, e no momento que o cliente se desconecta, o endereço é devolvido.

Fonte: ipv6.br

Esgotamento do IPv4 – Alternativas
NAT

O NAT (Network Address Translation) foi outra técnica paliativa desenvolvida para resolver o problema do esgotamento dos endereços IPv4.

Definida na RFC 3022 (tornou obsoleta a RFC 1631), tem como ideia básica permitir que, com um único endereço IP, ou um pequeno número deles, vários hosts possam trafegar na Internet.

Dentro de uma rede, cada computador recebe um endereço IP privado único, que é utilizado para o roteamento do tráfego interno.

No entanto, quando um pacote precisa ser roteado para fora da rede, uma tradução de endereço é realizada, convertendo endereços IP privados em endereços IP públicos globalmente únicos.

Para tornar possível este esquema, utiliza-se os três intervalos de endereços IP declarados como privados na RFC 1918, sendo que a única regra de utilização é que nenhum pacote contendo estes endereços pode trafegar na Internet pública.

Fonte: ipv6.br

IPv6 – especificações

As especificações da IPv6 foram apresentadas inicialmente na RFC 1883 de dezembro de 1995, no entanto, em dezembro de 1998, esta RFC foi substituída pela RFC 2460.

Como principais mudanças em relação ao IPv4 destacam-se:

• **Maior capacidade para endereçamento:** no IPv6 o espaço para endereçamento aumentou de 32 bits para 128 bits, permitindo: níveis mais específicos de agregação de endereços; identificar uma quantidade muito maior de dispositivos na rede; e implementar mecanismos de autoconfiguração;

• **Simplificação do formato do cabeçalho:** alguns campos do cabeçalho IPv4 foram removidos ou tornaram-se opcionais, com o intuito de reduzir o custo do processamento dos pacotes nos roteadores;

Fonte: ipv6.br

IPv6 – especificações

• **Suporte a cabeçalhos de extensão:** as opções não fazem mais parte do cabeçalho base, permitindo um roteamento mais eficaz, limites menos rigorosos em relação ao tamanho e a quantidade de opções, e uma maior flexibilidade para a introdução de novas opções no futuro;

• **Capacidade de identificar fluxos de dados:** foi adicionado um novo recurso que permite identificar de pacotes que pertençam a determinados tráfegos de fluxos, para os quais podem ser requeridos tratamentos especiais;

• **Suporte a autenticação e privacidade:** foram especificados cabeçalhos de extensão capazes de fornecer mecanismos de autenticação e garantir a integridade e a confidencialidade dos dados transmitidos.

Fonte: ipv6.br

IPv6 – distribuição de endereços

Como não pode haver repetição de endereços, eles são um recurso que tem de ser gerenciado de forma centralizada na Internet.

O autoridade responsável por este controle é a IANA (Internet Assigned Numbers Authority).

Fonte: ipv6.br

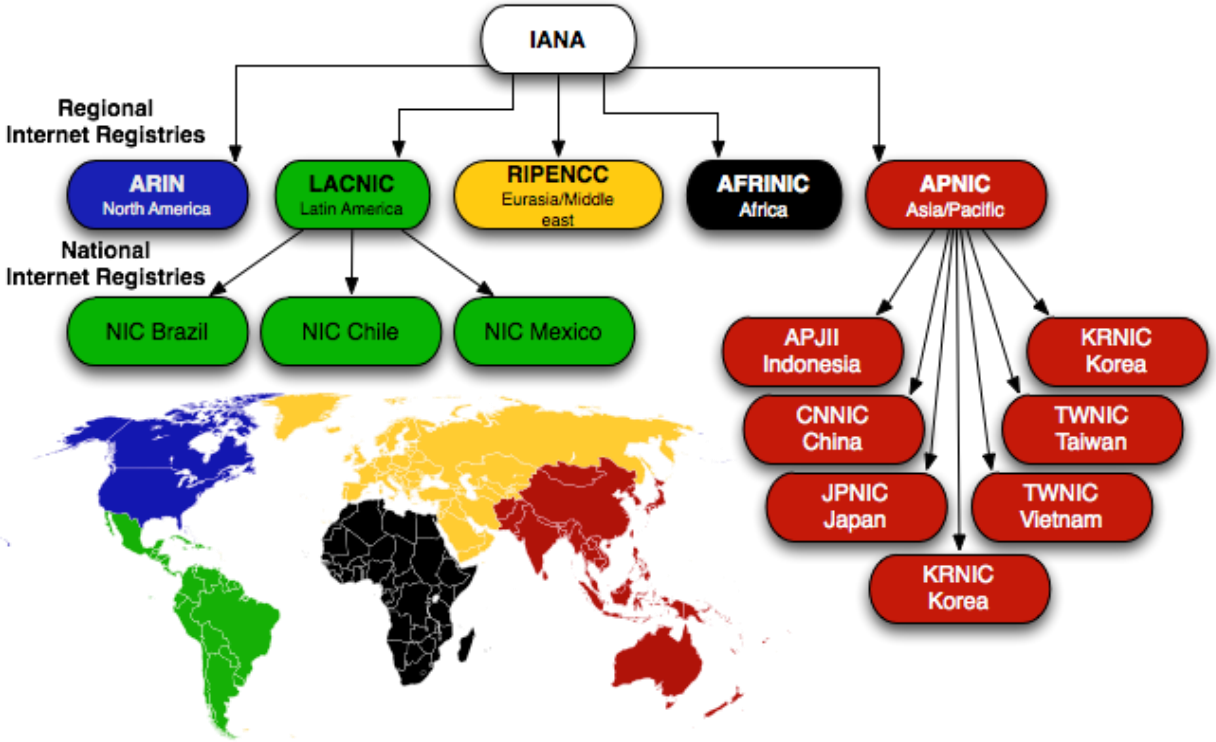
IPv6 – distribuição de endereços

Atualmente a função da IANA é realizada pela ICANN (Internet Corporation for Assigned Names and Numbers), e a estrutura de distribuição de IPs é hierárquica, contando também com organizações regionais, chamadas de RIR (Regional Internet Registries) e em alguns casos, estruturas nacionais, chamadas de NIR (National Internet Registries).

Fonte: ipv6.br

IPv6 – distribuição de endereços

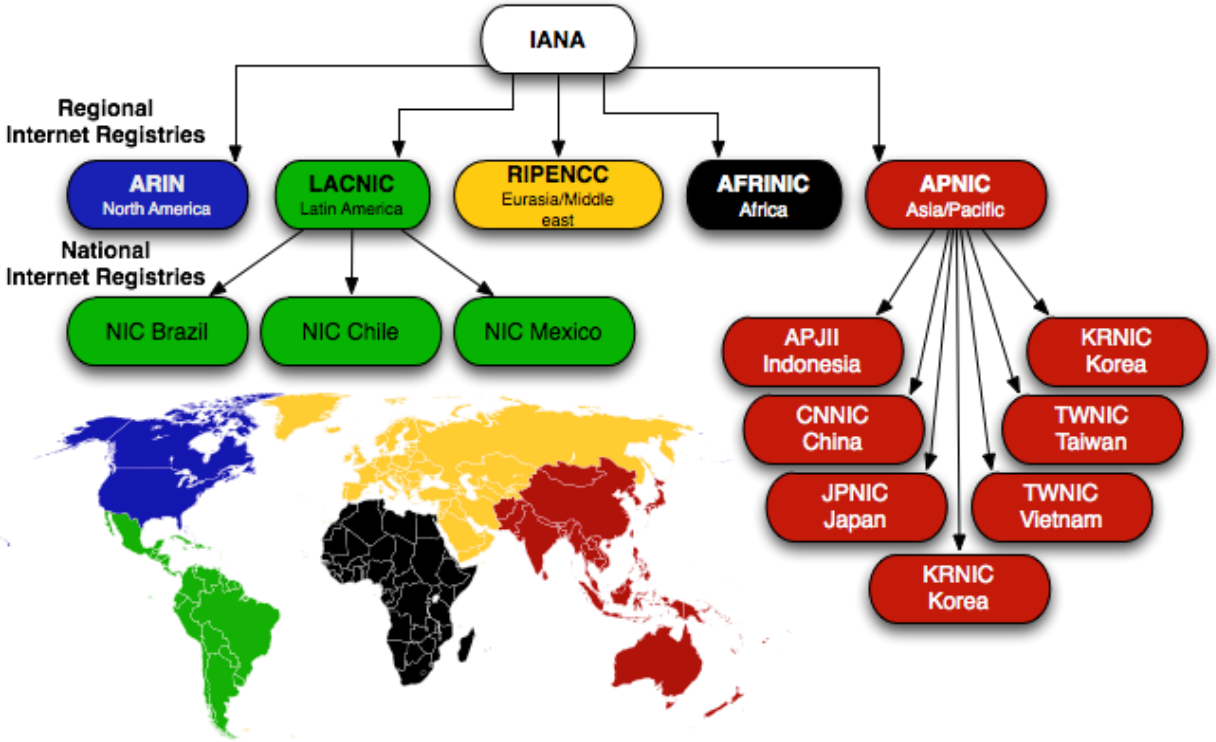
Há cinco RIRs: o ARIN, na América do Norte, o LACNIC, na América Latina e Caribe, o RIPENCC, abrangendo a Europa e parte da Ásia, o AFRINIC, na África e o APNIC, na região da Ásia e Oceania.



Fonte: ipv6.br

IPv6 – distribuição de endereços

Cada uma dessas organizações é responsável por definir as regras de distribuição dos endereços em sua respectiva área de atuação, bem como implementa-las.



Fonte: ipv6.br

IPv6 – distribuição de endereços

Em alguns países há entidades nacionais para a distribuição dos IPs.

É o caso do Brasil, por exemplo, onde o NIC.br é quem gerencia esse recurso.

lacnic

nic.br

NIC CHILE
somos el punto CL

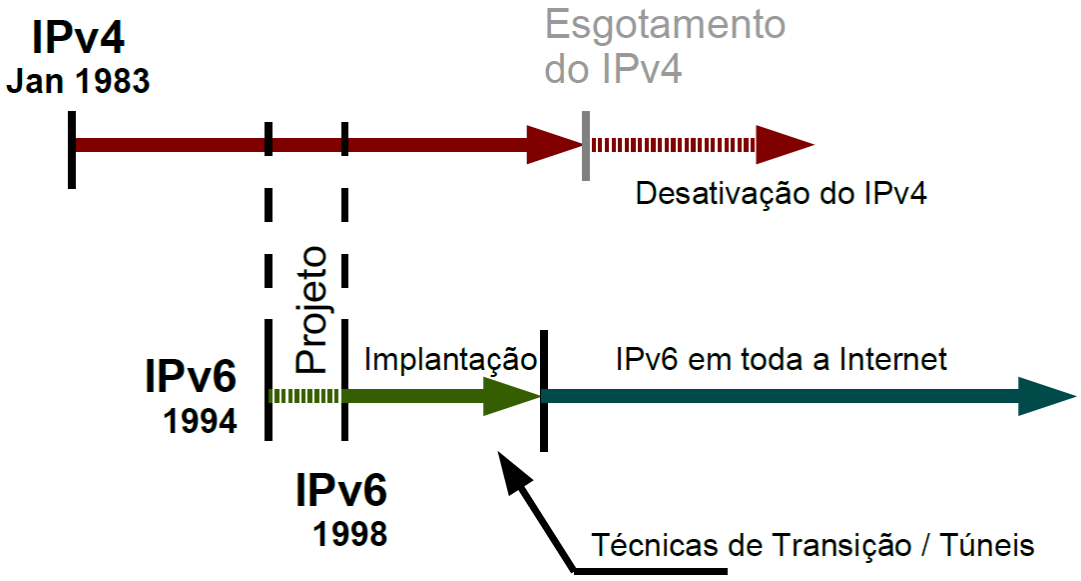
NIC MÉXICO

Fonte: ipv6.br

IPv6 – transição

O IPv6 foi projetado de tal forma que não é compatível com o IPv4. Eles não podem interoperar diretamente.

Assim, o plano inicial era fazer uma transição gradual, mantendo o IPv4 e adicionando o IPv6 em todos os dispositivos da Internet ao longo do tempo, de forma que, antes dos endereços livres IPv4 esgotaram-se, o IPv6 estivesse instalado em toda a Internet.

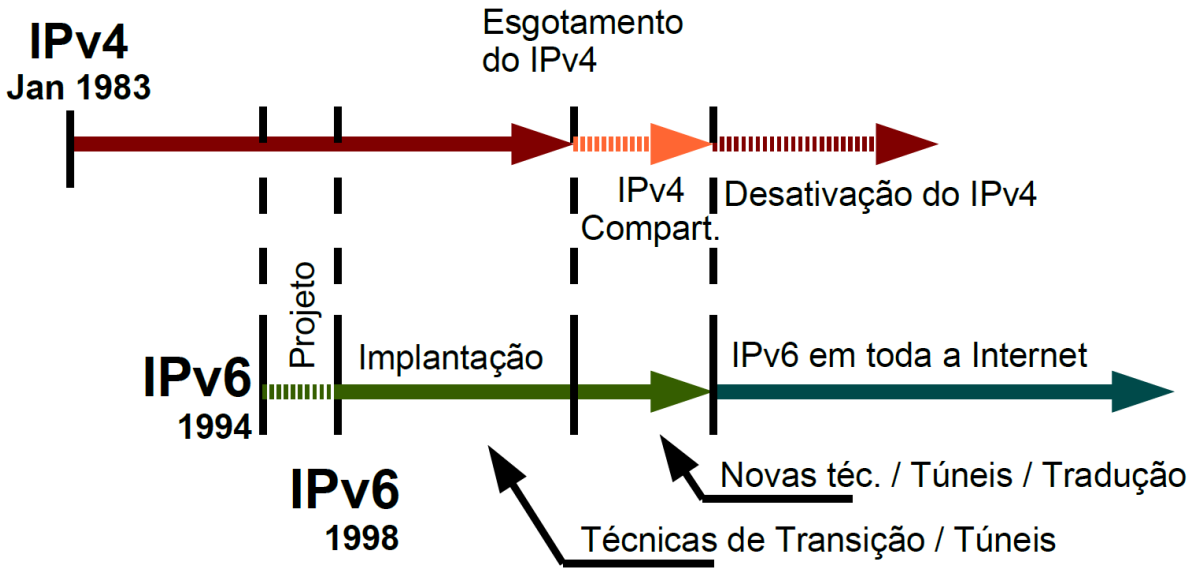


Fonte: ipv6.br

IPv6 – transição

No Brasil, construiu-se o cronograma abaixo como referência para a implantação do protocolo no país.

Ele foi construído com base no diálogo com diversos provedores de acesso, de serviços e operadoras de telecomunicações, em diversas reuniões de coordenação ao longo dos anos de 2011 e 2012.



Fonte: ipv6.br

IPv4 e IPv6

O IPv4 é um protocolo de rede com tamanho de 32 bits, o que significa que ele possui 2^{32} combinações possíveis, ou seja:

$$2^{32} = 4.294.967.296\ endereços$$

Já o protocolo IPv6 tem o tamanho de 128 bits, o significa que ele possui 2^{128} combinações possíveis, ou seja:

$$2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456\ endereços$$

Fonte: ipv6.br

Endereço IPv6

Os 32 bits dos endereços IPv4 são divididos em quatro grupos de 8 bits cada, separados por ".", escritos com dígitos **decimais**. Por exemplo:

192.168.0.10

A representação dos endereços IPv6 divide o endereço em oito grupos de 16 bits, separando-os por ":", escritos com dígitos **hexadecimais** (0-F). Por exemplo:

2001:0DB8:AD1F:25E2:CADE:CAFE:F0CA:84C1

Na representação de um endereço IPv6, é permitido utilizar tanto caracteres maiúsculos quanto minúsculos.

Fonte: ipv6.br

Endereço IPv6 – regras de abreviação

Além disso, regras de abreviação podem ser aplicadas para facilitar a escrita de alguns endereços muito extensos. É permitido omitir os zeros a esquerda de cada bloco de 16 bits, além de substituir uma sequência longa de zeros por "::".

Por exemplo, o endereço:

2001:0DB8:0000:0000:130F:0000:0000:140B

pode ser escrito como:

2001:DB8::130F:0:0:140B

--ou--

2001:DB8:0:0:130F::140B

Neste caso a abreviação do grupo de zeros só pode ser realizada uma única vez, caso contrário poderá haver ambiguidade na representação do endereço.

Fonte: ipv6.br

Endereço IPv6 – regras de abreviação

Se o endereço:

2001:0DB8:0000:0000:130F:0000:0000:140B

fosse escrito como:

2001:DB8::130F::140B

não seria possível determinar se ele corresponde a:

2001:DB8:0:0:130F:0:0:140B

--ou--

2001:DB8:0:0:0:130F:0:140B

--ou--

2001:DB8:0:130F:0:0:0:140B

Fonte: ipv6.br

Endereço IPv6 – regras de abreviação

Esta abreviação também pode ser feita no final ou no início do endereço, como ocorre em:

2001:DB8:0:54:0:0:0:0

que pode ser escrito da forma:

2001:DB8:0:54::

Fonte: ipv6.br

Endereço IPv6 – prefixos de rede

Outra representação importante é a dos prefixos de rede. Em endereços IPv6 ela continua sendo escrita do mesmo modo que no IPv4, utilizando a notação CIDR.

Esta notação é representada da forma “endereço-IPv6/tamanho do prefixo”, onde “tamanho do prefixo” é um valor decimal que especifica a quantidade de bits contíguos à esquerda do endereço que compreendem o prefixo.

O exemplo de prefixo de subrede apresentado a seguir indica que dos 128 bits do endereço, 64 bits são utilizados para identificar a subrede:

- Prefixo **2001:db8:3003:2::/64**
- Prefixo global **2001:db8::/32**
- ID da subrede **3003:2**

Esta representação também possibilita a agregação dos endereços de forma hierárquica, identificando a topologia da rede através de parâmetros como posição geográfica, provedor de acesso, identificação da rede, divisão da subrede, etc. Com isso, é possível diminuir o tamanho da tabela de roteamento e agilizar o encaminhamento dos pacotes.

Fonte: ipv6.br

Endereço IPv6 – URLs

Com relação a representação dos endereços IPv6 em URLs (Uniform Resource Locators), estes agora passam a ser representados entre colchetes.

Deste modo, não haverá ambiguidades caso seja necessário indicar o número de uma porta juntamente com a URL.

Exemplos:

http://[**2001:12ff:0:4::22**]/index.html

http://[**2001:12ff:0:4::22**]:8080

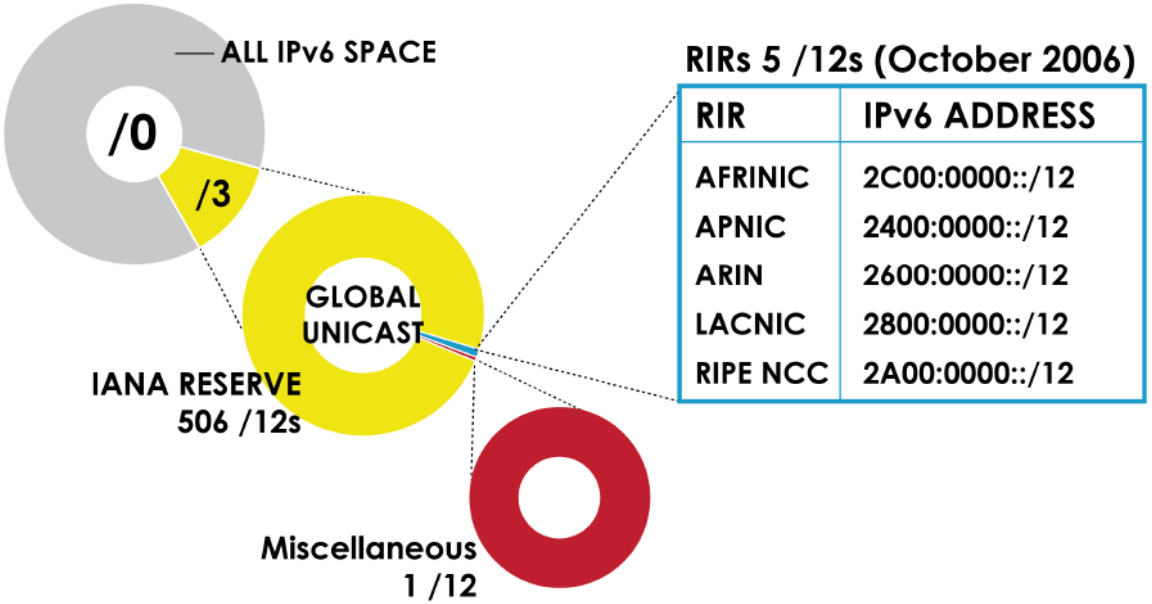
Fonte: ipv6.br

Endereço IPv6 – alocação e designação

Na hierarquia das políticas de atribuição, alocação e designação de endereços, cada RIR recebe da IANA um bloco /12 IPv6.

O bloco **2800::/12** corresponde ao espaço reservado para o LACNIC alocar na América Latina.

O NIC.br por sua vez, trabalha com a subrede **2801::/16** que faz parte deste /12.



RIRs 5 /12s (October 2006)

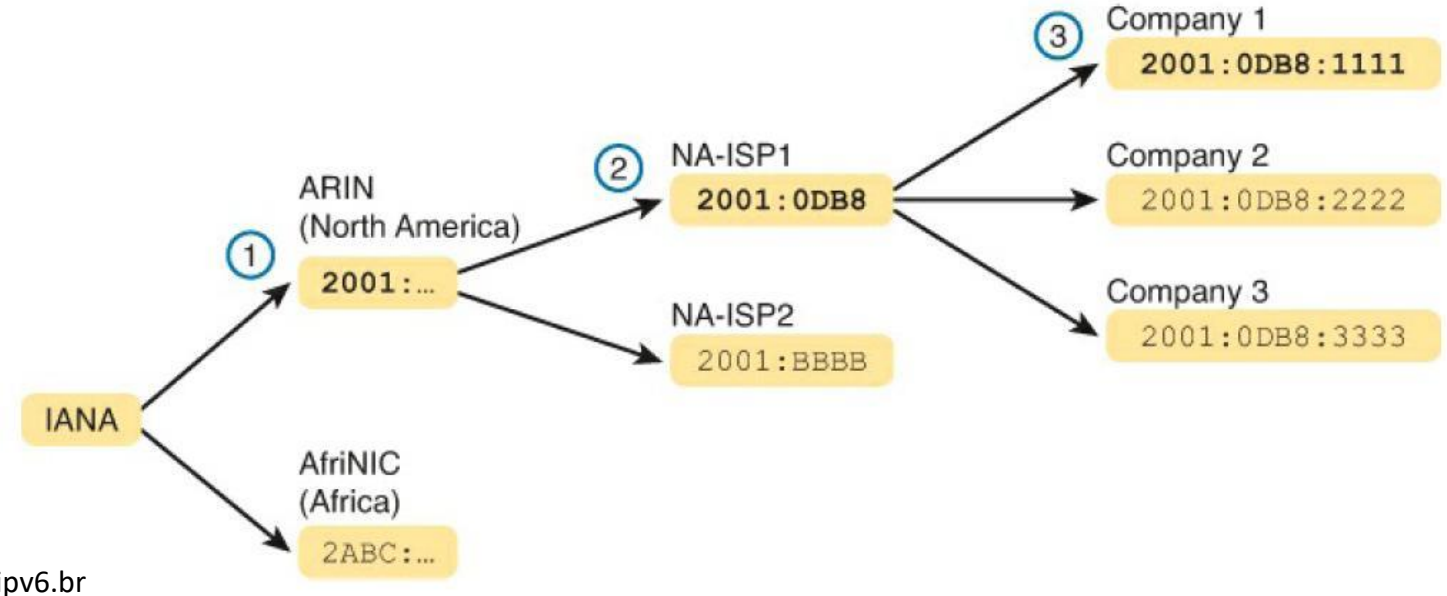
RIR	IPv6 ADDRESS
AFRINIC	2C00:0000::/12
APNIC	2400:0000::/12
ARIN	2600:0000::/12
LACNIC	2800:0000::/12
RIPE NCC	2A00:0000::/12

Fonte: ipv6.br

Endereço IPv6 – alocação e designação

A alocação mínima para ISPs é um bloco /32, no entanto, alocações maiores podem ser feitas mediante apresentação de justificativa de utilização.

Um aspecto importante que merece destaque é que diferente do IPv4, com IPv6 a utilização é medida em relação ao número de designações de blocos de endereços para usuários finais, e não em relação ao número de endereços designados aos usuários finais.



Fonte: ipv6.br

Endereço IPv6 – recomendação do NIC.br

O NIC.br recomenda utilizar:

• **/64 a /56 para usuários domésticos:** Para usuários móveis pode-se utilizar /64, pois normalmente apenas uma rede é suficiente. Para usuários residenciais recomenda-se redes maiores. Se o provedor optar por, num primeiro momento, oferecer apenas /64 para usuários residenciais, ainda assim recomenda-se que no plano de numeração se reserve um /56.

• **/48 para usuários corporativos:** Empresas muito grandes podem receber mais de um bloco /48. Para planejar a rede é preciso considerar que para cada rede física ou VLAN com IPv6 é preciso reservar um /64. Esse é o tamanho padrão e algumas funcionalidades, como a autoconfiguração dependem dele. É preciso considerar também a necessidade de expansão futura, assim como a necessidade de agregação nos protocolos de roteamento.

Fonte: ipv6.br

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.

... acesse os diversos materiais disponíveis em www.ipv6.br.

FIM