Engenharia de Controle e Automação
Disciplina: Redes Industriais - 7º Período
Professor: José Maurício S. Pinheiro

AULA 3: Modelo TCP-IP

O padrão histórico e técnico da Internet é o modelo TCP/IP (*Transmission Control Protocol/Internet Protocol*), desenvolvido pelo Departamento de Defesa dos Estados Unidos (DoD) para ser uma rede que pudesse resistir em qualquer condição, mesmo na ocorrência de uma guerra nuclear. O TCP/IP foi projetado como um padrão aberto, o que ajudou muito no rápido desenvolvimento do TCP/IP como padrão.

1. Camadas do Modelo TCP-IP

O TCP/IP é organizado em quatro camadas conceituais construídas em uma quinta camada de hardware. Embora algumas das camadas no modelo TCP/IP tenham os mesmos nomes das camadas no modelo OSI, as camadas dos dois modelos não possuem uma correspondência exata.
O modelo TCP/IP tem as seguintes quatro camadas (Figura 1):

- A camada de Aplicação
- A camada de Transporte
- A camada de Internet
- A camada de acesso à rede

Figura 1 – Camadas do Modelo TCP-IP

- **CAMADA DE APLICAÇÃO** - Os protocolos de mais alto nível incluem os detalhes da camada de sessão e de apresentação do modelo OSI. A camada de aplicação trata de questões de representação, codificação e controle de diálogo. No nível mais alto, os usuários rodam programas aplicativos que acessam serviços disponíveis através de uma interligação em redes TCP/IP. Um aplicativo interage com um dos protocolos do nível de transporte para enviar ou receber dados. Cada programa aplicativo escolhe o estilo de transporte necessário, que tanto pode ser uma sequência de mensagens individuais ou um fluxo contínuo de bytes. O programa aplicativo passa, para a camada de transporte, os dados na forma adequada, para que possam, então, ser transmitidos;

- **CAMADA DE TRANSPORTE** - lida com questões de qualidade de serviços de confiabilidade, controle de fluxo e correção de erros. A primeira função da camada de transporte é prover a comunicação de um programa aplicativo para outro. Tal comunicação é sempre chamada fim-a-fim. A camada de transporte pode regular o fluxo de informações, fornece transporte confiável, assegurando que os dados cheguem sem erros e em sequência. Um de seus protocolos, o *Transmission Control Protocol* (TCP), fornece opções de comunicações de rede confiáveis com baixa taxa de erros e bom fluxo. O TCP é um protocolo orientado a conexões. Ele mantém um diálogo entre a origem e o destino enquanto empacota informações da camada de aplicação em unidades chamadas segmentos. O termo orientado a conexões não quer dizer que existe um circuito entre os computadores que se comunicam. Significa que segmentos da Camada 4 trafegam entre dois hosts para confirmar que a conexão existe logicamente durante um certo período;

- **CAMADA DE INTERNET** – trata das informações de uma máquina para outra. Aceita um pedido para enviar um pacote originário da camada de transporte juntamente com a identificação da máquina para a qual o pacote deve ser enviado. Seu propósito é dividir os segmentos TCP em pacotes e enviá-los a partir de qualquer rede. Os pacotes chegam à rede de destino independente do caminho para chegar até lá. O protocolo específico que governa essa camada é chamado *Internet Protocol* (IP). A determinação do melhor caminho e a comutação de pacotes ocorrem nesta camada. É muito importante a relação entre IP e TCP. Pode-se imaginar que o IP aponta o caminho para os pacotes, enquanto que o TCP proporciona um transporte confiável;

- **CAMADA DE ACESSO A REDE** - também conhecida como a camada host-para-rede. Esta camada lida com todos os componentes, tanto físico como lógico, que são necessários para fazer um link físico. Isso inclui os detalhes da tecnologia de redes, inclusive todos os detalhes nas camadas física e de enlace do OSI. Uma interface de rede pode consistir em um driver de dispositivo ou em um subsistema complexo que usa seu próprio protocolo de enlace de dados.

A Figura 2 mostra alguns dos protocolos comuns especificados pelo modelo de referência TCP/IP.

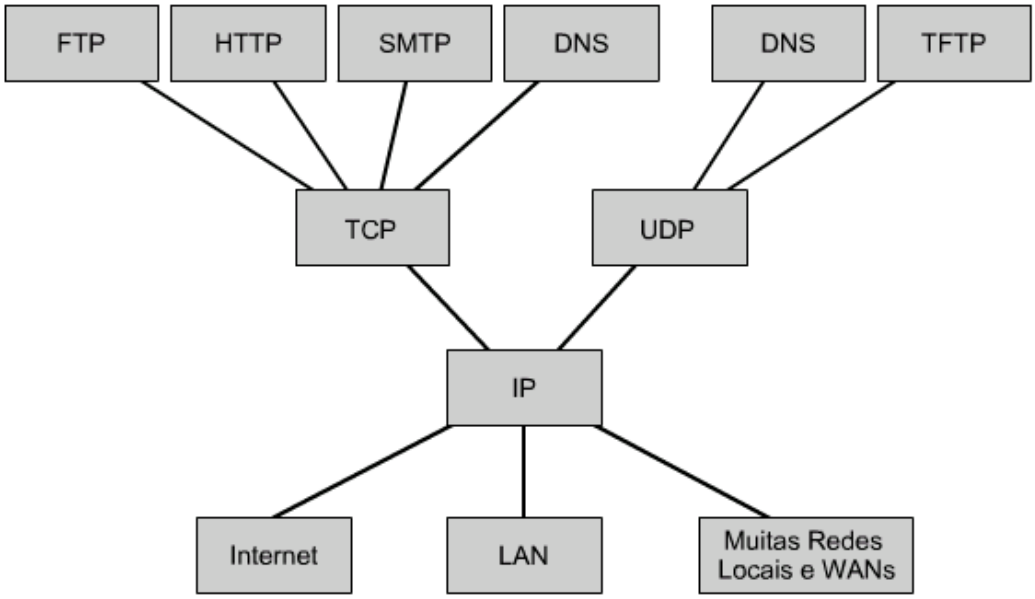


Figura 2 – Exemplos de protocolos do Modelo TCP-IP

Protocolos da camada de aplicação incluem os seguintes:

- FTP - File Transfer Protocol
- HTTP - Hypertext Transfer Protocol
- SMTP - Simple Mail Transfer Protocol
- DNS – Domain Name System
- TFTP - Trivial File Transfer Protocol

Os protocolos mais comuns da camada de transporte incluem:

- TCP - Transport Control Protocol
- UDP - User Datagram Protocol

O principal protocolo da camada de Internet é:

- IP - Internet Protocol

Protocolos da camada de acesso à rede:

A camada de acesso à rede se refere a qualquer tecnologia em particular usada em uma rede específica.

2. OSI versus TCP/IP

Os modelos de referência OSI e TCP/IP se baseiam no conceito de uma pilha de protocolos independentes. Nesses modelos, são oferecidos aos processos que desejam se comunicar um serviço de transporte fim a fim independentemente do tipo de rede que está sendo usado. Essas camadas formam o provedor de transporte. Em ambos os modelos, as camadas acima da camada de transporte dizem respeito aos usuários orientados à aplicação do serviço de transporte.
Apesar dessas semelhanças, os dois modelos também apresentam diferenças. Uma comparação entre o modelo OSI e o modelo TCP/IP realça semelhanças e diferenças (Figura 3).

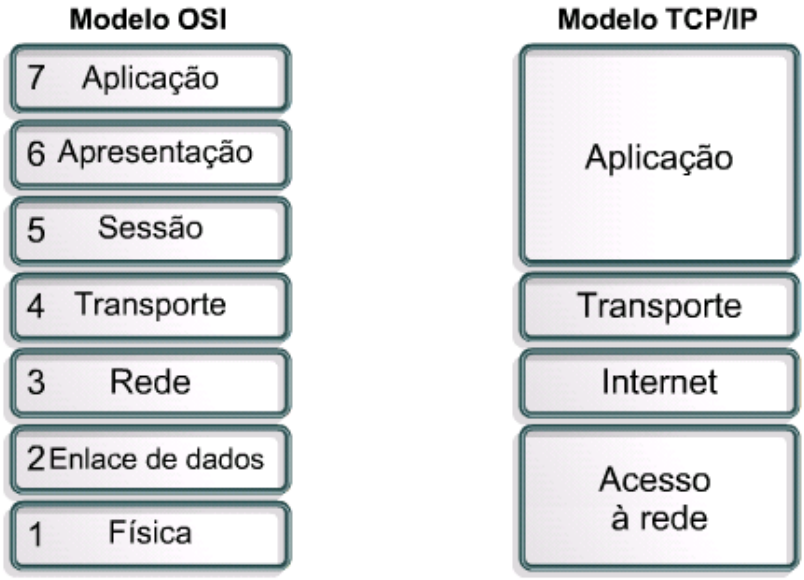


Figura 3 - Semelhanças e Diferenças entre OSI e TCP-IP

As semelhanças incluem:

- Ambos têm camadas.
- Ambos têm camadas de aplicação, embora incluam serviços diferentes.
- Ambos têm camadas de transporte e de rede comparáveis.
- Os dois modelos precisam ser conhecidos pelos profissionais de rede.
- Ambos supõem que os pacotes sejam comutados. Isto quer dizer que os pacotes individuais podem seguir caminhos diferentes para chegarem ao mesmo destino.

As diferenças incluem:

- O TCP/IP combina os aspectos das camadas de apresentação e de sessão dentro da sua camada de aplicação.
- O TCP/IP combina as camadas física e de enlace do OSI na camada de acesso à rede.
- O TCP/IP parece ser mais simples por ter menos camadas.

- Os protocolos TCP e IP são os padrões em torno dos quais a Internet se desenvolveu, portanto, o modelo TCP/IP ganha credibilidade apenas por causa dos seus protocolos. Ao contrário, geralmente as redes não são desenvolvidas de acordo com o protocolo OSI, embora o modelo OSI seja usado somente como um guia.

Na Figura 4 temos a comparação entre o modelo OSI e o modelo TCP/IP e Ethernet.

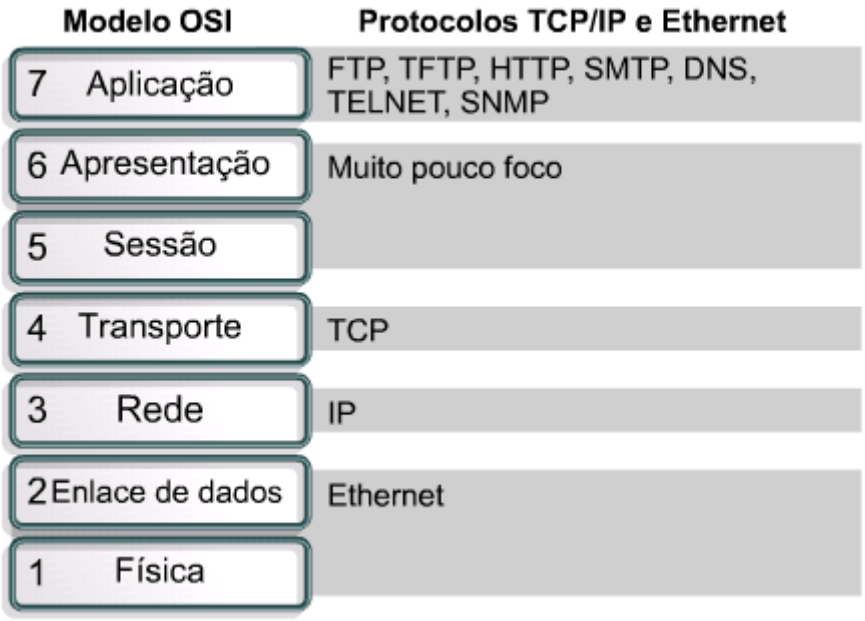


Figura 4 - Protocolos TCP/IP e Ethernet

3. Exemplos de Redes com Arquitetura TCP/IP

Alguns exemplos de aplicações de arquiteturas de redes baseadas em TCP/IP, como, por exemplo, redes internas de empresas baseadas em transporte TCP/IP, serviços de redes de empresas conectados à Internet, provedores de acesso à Internet.

- Redes internas à empresa utilizando protocolos TCP/IP para formar a estrutura de comunicação e a base das aplicações de rede tais como correio eletrônico, compartilhamento de arquivos, distribuição de informação via hipertexto, etc., conhecidas como intranet, na Figura 5.

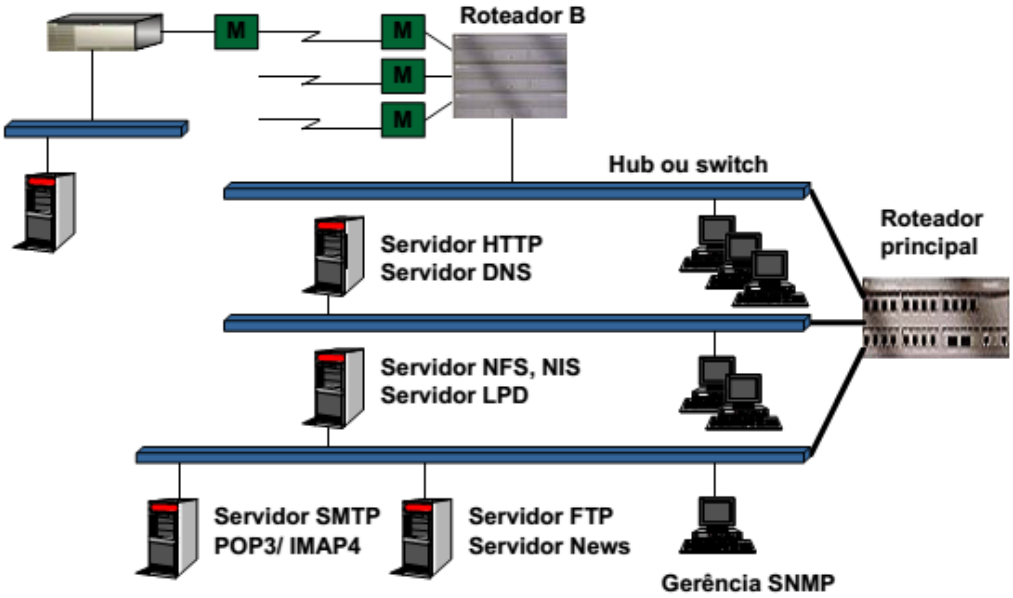


Figura 5 – Intranet

- Estrutura de rede TCP/IP conectada à Internet de forma segura, através da utilização de um firewall, que realiza o filtro de pacotes IP e o transporte de protocolo de aplicações por meio de um gateway (proxy), na Figura 6.

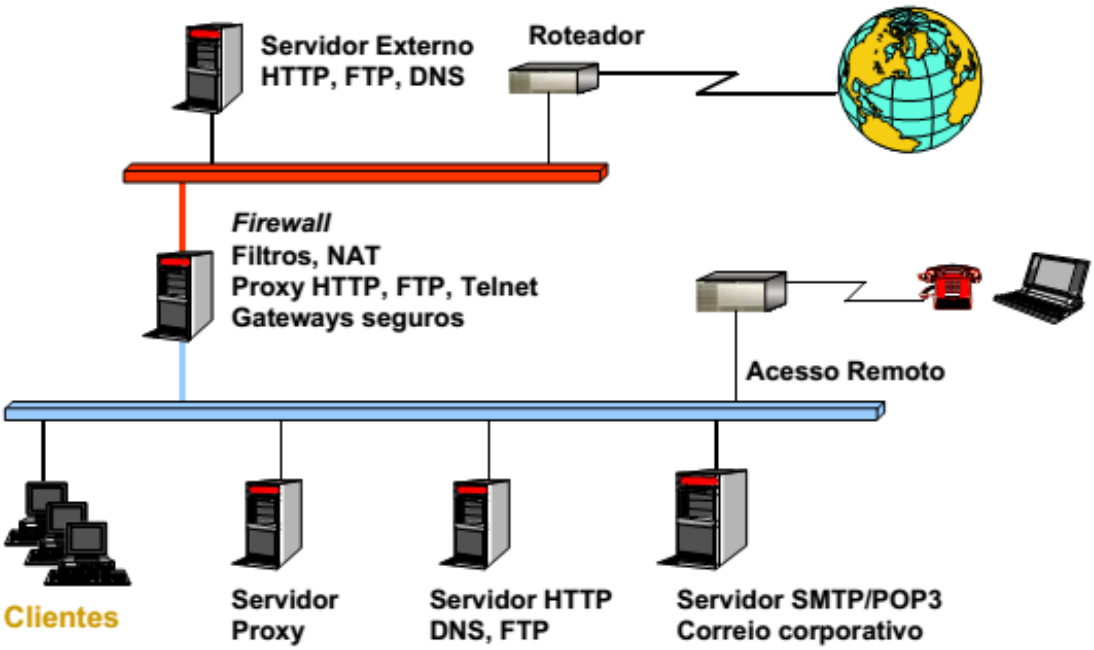


Figura 6 - Internet

- Provedor de Serviços de Internet, fornecendo serviços de conexão a usuários residenciais e empresas por meio de ligação dedicada, além de serviços básicos de Internet como HTTP, SMTP, POP3, FTP, etc., na Figura 7.

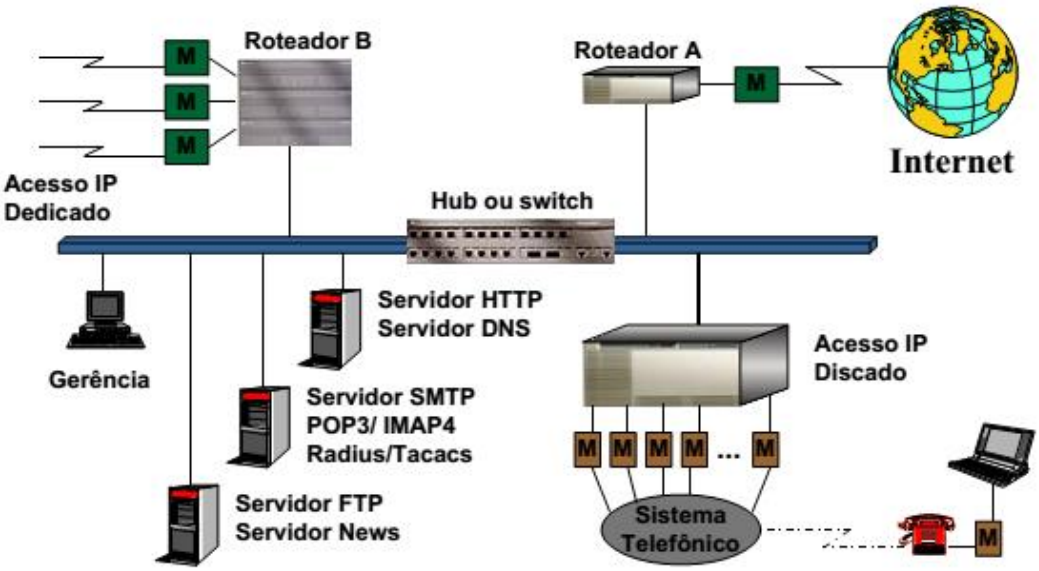


Figura 7 - Provedor de Serviços - ISP

4. IPv4

O protocolo IP foi projetado tendo como principal objetivo a ligação entre redes. Por isto ele é considerado como elemento integrador da Internet e através dele é possível a conexão de diversas sub-redes. A internet é composta de diversos backbones construídos através linhas de alta velocidades de diversos tipos de tecnologia. A cada um destes backbones estão conectadas várias redes locais de diferentes instituições, cada uma com suas características de sub-redes. Por exemplo, em muitas empresas é comum utilizar o IP e outros protocolos de sua família, para interligar computadores de tecnologia diferentes.
O protocolo IP providencia duas importantes definições de serviço. Uma define a unidade básica de transferência de dados chamada de datagrama IP. A outra define uma função de roteamento, preocupando-se como os pacotes são endereçados e quais caminhos terão que seguir para chegarem a seu destino.

4.1. Identificadores Universais

Diz-se que um sistema provê um serviço de comunicação universal quando é possível a quaisquer dos elementos deste sistema se comunicarem arbitrariamente. Para tornar um sistema de comunicação universal, devemos estabelecer um método globalmente aceito para identificação dos componentes a ele conectados. Nas redes TCP/IP, a entidade que atua como identificador universal é o endereço IP, um número de 32 dígitos binários.

4.2. Classes Primarias de Endereços

A Internet é uma grande rede de computadores como qualquer outra rede física. A grande diferença, entretanto, está no fato de que a Internet é uma estrutura virtual, concebida e implementada inteiramente em software. Assim, os projetistas tiveram liberdade de arbitrar o tamanho e formato dos pacotes, endereços, técnicas de roteamento, etc. Nada é ditado pelo hardware. Na questão do endereçamento, optou-se por um esquema análogo ao das redes convencionais, onde a cada host é atribuído um número inteiro que será seu endereço, neste caso, o endereço IP.
A grande vantagem no esquema de endereçamento da Internet é que ele foi concebido para simplificar a tarefa de roteamento. Cada máquina ligada à Internet possui um endereço de 32 bits, que se divide em duas partes: uma primeira que identifica a rede a qual esse computador está fisicamente conectado e uma segunda parte que identifica o computador (host) propriamente dito.
Importante observar que todas as máquinas conectadas a uma mesma rede irão compartilhar essa primeira parte, que se convencionou chamar net id (identificador da rede). Analogamente, à segunda porção do endereço IP chamamos host id (identificação da máquina). Em termos práticos, cada endereço IP deverá estar contido em uma das cinco categorias representadas na Figura 8.
A classe de um endereço pode ser identificada através do exame dos quatro bits de mais alta ordem, sendo que as três classes básicas (A, B e C) podem ser distinguidas apenas pelos dois primeiros.

- **Classe A** - usada para um pequeno número de redes que contêm mais de 65.535 hosts, reserva 7 bits para o net id e 24 bits para o host id.
- **Classe B** – os endereços se destinam a redes de tamanho intermediário (entre 256 e 65535 máquinas) e reservam 14 bits para o net id e 16 bits para o host id.
- **Classe C** - apropriada para pequenas redes, aloca 21 bits para o net id e apenas 8 bits para o host id.

Observar que os endereços IP são estruturados de forma a permitir uma rápida extração da identificação da rede (net id) e da máquina a ela conectada (host id). Os gateways dependem da extração eficiente do net id para realizar o roteamento dos pacotes IP.
O endereço 127.0.0.0 é reservado à aplicação de loopback. Isto é, qualquer pacote enviado a este endereço não deve trafegar na rede, mas retornar ao próprio remetente (isto equivale a dizer que o pacote retornará da própria interface de rede do host). O endereço de loopback se presta a testes e comunicação entre processos que rodam numa mesma máquina.

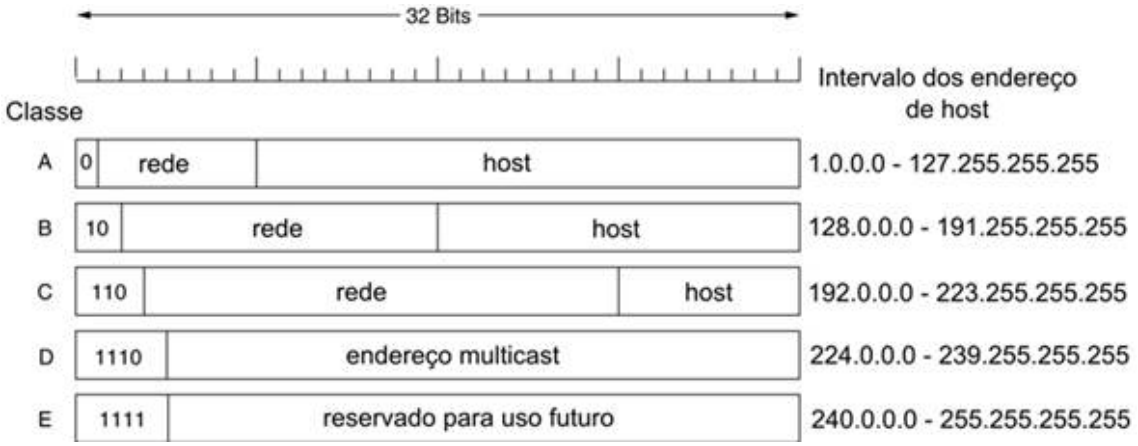


Figura 8 - Classes IPV4

Uma das desvantagens desse esquema de endereçamento é que, como um endereço IP se refere a uma conexão de rede (e não a um host), quando uma máquina muda de uma rede para outra, ela deve mudar de endereço IP. Isso traz uma grande barreira à conexão de hosts móveis (como computadores portáteis) que necessitem de IP's fixos à Internet.

4.3. CIDR

A IETF (*Internet Engineering Task Force*) passou a discutir estratégias para solucionar a questão do esgotamento dos endereços IPv4 e o problema do aumento da tabela de roteamento. Para isso, em novembro de 1991, foi formado um grupo de trabalho que apresentou como solução a utilização do CIDR (*Classless Interdomain Routing*).
Definido na RFC 4632, 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. 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.

4.4. DHCP

Outra solução, apresentada na RFC 2131, 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 sub-rede, endereço do roteador padrão e o endereço do servidor DNS local. O DHCP tem sido muito utilizado por parte dos ISP's 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 à rede, lhe será designado um desses endereço de forma arbitrária, e no momento que o cliente se desconecta, o endereço é devolvido.

4.5. NAT

A NAT (*Network Address Translation*), foi outra técnica paliativa desenvolvida para resolver o problema do esgotamento dos endereços IPv4. Definida na RFC 3022, 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.
A utilização da NAT mostrou-se eficiente no que diz respeito a economia de endereços IP, além de apresentar alguns outros aspectos positivos, como facilitar a numeração interna das redes, ocultar a topologia das redes e só permitir a entrada de pacotes gerados em resposta a um pedido da rede. No entanto, o uso da NAT apresenta inconvenientes que não compensam as vantagens oferecidas:

- Quebra o modelo fim-a-fim da Internet, não permitindo conexões diretas entre dois hosts, o que dificulta o funcionamento de uma série de aplicações, como P2P, VoIP e VPN;
- Baixa escalabilidade, pois o número de conexões simultâneas é limitado, além de exigir um grande poder de processamento do dispositivo tradutor;
- Impossibilita rastrear o caminho de pacote, através de ferramentas como traceroute, por exemplo, e dificulta a utilização de algumas técnicas de segurança como IPSec.
- Seu uso passa uma falsa sensação de segurança, pois, apesar de não permitir a entrada de pacotes não autorizados, a NAT não realiza nenhum tipo de filtragem ou verificação nos pacotes que passa por ela.

5. IPV6

Em dezembro de 1993, a IETF formalizou, através da RFC 1550, as pesquisas a respeito da nova versão do protocolo IP, solicitando o envio de projetos e propostas para o novo protocolo através do grupo de trabalho da IETF denominado *Internet Protocol next generation* (IPng). A nova versão do Protocolo Internet passou a ser chamada oficialmente de IPv6 com a RFC 2460, em dezembro de 1998. 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 e identificando uma quantidade muito maior de dispositivos na rede, além de implementar mecanismos de autoconfiguração. A escalabilidade do roteamento multicast também foi melhorada através da adição do campo "escopo"

no endereço multicast. E um novo tipo de endereço, o anycast, foi definido;

- **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;
- **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.

Enquanto no IPv4 o espaço para endereçamento possui 32 bits, o que possibilita um máximo de 4.294.967.296 (2^{32}) endereços distintos, no IPv6 o espaço para endereçamento é de 128 bits, sendo possível obter 340.282.366.920.938.463.463.374.607.431.768.211.456 (2^{128}) endereços. Isto representa aproximadamente 79 octilhões ($7{,}9 \times 10^{28}$) de vezes a quantidade de endereços IPv4 e representa, também, mais de 56 octilhões ($5{,}6 \times 10^{28}$) de endereços por ser humano na Terra, considerando-se uma população estimada em 6 bilhões de habitantes.

Tecnicamente, o IPv6 também apresentou mudanças no tratamento da fragmentação dos pacotes, que passou a ser realizada apenas na origem. Ele permite o uso de conexões fim-a-fim, princípio que havia sido quebrado com o IPv4 devido à grande utilização de NAT. Além disso, trouxe recursos que facilitam a configuração de redes, além de outros aspectos que foram melhorados em relação ao IPv4.

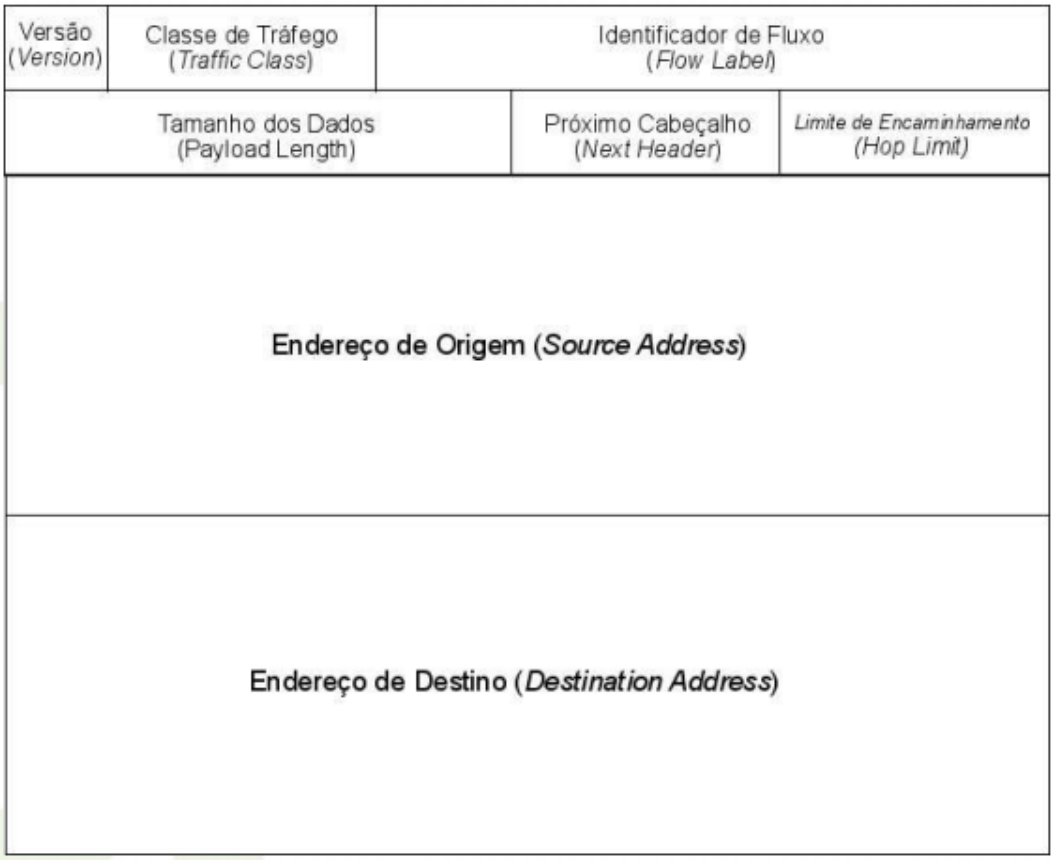


Figura 9 - Cabeçalho IPV6

Sobre os campos do cabeçalho IPV6 (Figura 9) temos:

- **Versão (4 bits)** - Identifica a versão do protocolo IP utilizado. No caso do IPv6 o valor desse campo é 6;
- **Classe de Tráfego (8 bits)** - Identifica e diferencia os pacotes por classes de serviços ou prioridade. Ele continua provendo as mesmas funcionalidades e definições do campo Tipo de Serviço do IPv4.
- **Identificador de Fluxo (20 bits)** - Identifica e diferencia pacotes do mesmo fluxo na camada de rede. Esse campo permite ao roteador identificar o tipo de fluxo de cada pacote, sem a necessidade de verificar sua aplicação.
- **Tamanho do Dados (16 bits)** - Indica o tamanho, em Bytes, apenas dos dados enviados junto ao cabeçalho IPv6. Substituiu o campo Tamanho Total do IPv4, que indica o tamanho do cabeçalho mais o tamanho dos dados transmitidos. Os cabeçalhos de extensão também são incluídos no cálculo do tamanho.
- **Próximo Cabeçalho (8 bits)** - Identifica cabeçalho que se segue ao cabeçalho IPv6. Este campo foi renomeado (no IPv4 chamava-se Protocolo) refletindo a nova organização dos pacotes IPv6, pois agora este campo não contém apenas valores referentes a outros protocolos, mas também indica os valores dos cabeçalhos de extensão.
- **Limite de Encaminhamento (8 bits)** - Indica o número máximo de roteadores que o pacote IPv6 pode passar antes de ser descartado,

sendo decrementado a cada salto. Padronizou o modo como o campo Tempo de Vida (TTL) do IPv4 tem sido utilizado, apesar da definição original do campo TTL, dizer que este deveria indicar, em segundos, quanto tempo o pacote levaria para ser descartado caso não chegasse ao seu destino.

- **Endereço de origem (128 bits)** - Indica o endereço de origem do pacote.
- **Endereço de Destino (128 bits)** - Indica o endereço de destino do pacote.

5.1. Estrutura de Endereçamento IPv6

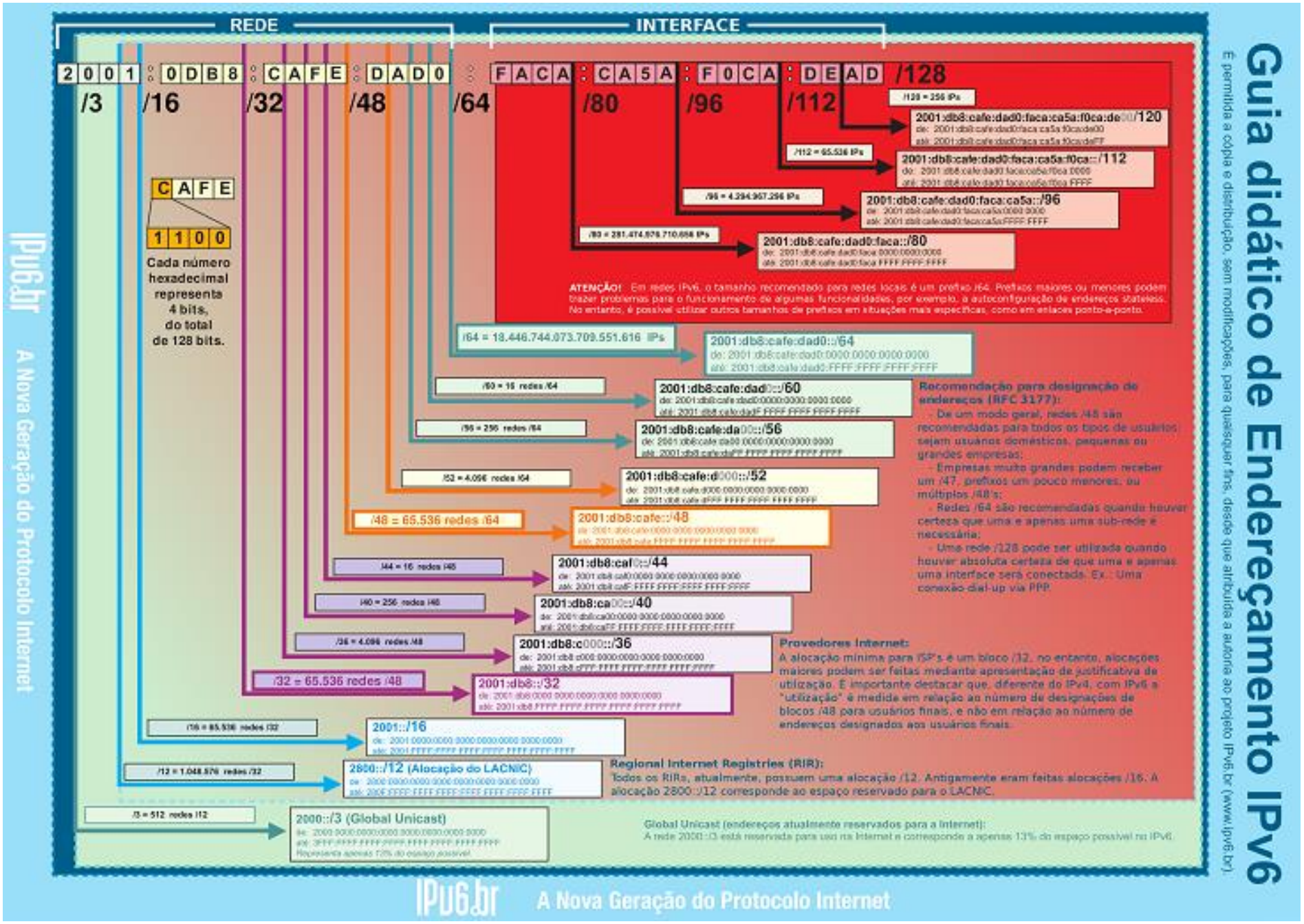
Enquanto os 32 bits dos endereços IPv4 são divididos em quatro grupos de 8 bits cada, separados por ".", escritos com dígitos decimais. Por exemplo: 192.168.0.10, a representação dos endereços IPv6, divide o endereço em oito grupos de 16 bits, separando-os por "**:**", escritos com dígitos hexadecimais (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. 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:DB8:0:0:130F::140B** ou **2001:DB8::130F:0:0:140B**. Neste exemplo é possível observar que a abreviação do grupo de zeros só pode ser realizada uma única vez, caso contrário poderá haver ambiguidades na representação do endereço.
Se o endereço acima fosse escrito como 2001:DB8::130F::140B, não seria possível determinar se ele corresponde a **2001:DB8:0:0:130F:0:0:140B**, a **2001:DB8:0:0:0:130F:0:140B** ou **2001:DB8:0:130F:0:0:0:140B**. Esta abreviação pode ser feita também no fim 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::**.
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 sub-rede apresentado a seguir indica que dos 128 bits do endereço, 64 bits são utilizados para identificar a sub-rede.

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

rede, etc. Com isso, é possível diminuir o tamanho da tabela de roteamento e agilizar o encaminhamento dos pacotes.
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. Por exemplo:

- http://[**2001:12ff:0:4::22**]/index.html
- http://[**2001:12ff:0:4::22**]:8080


Guia didático de Endereçamento IPv6
É permitida a cópia e distribuição, sem modificações, para quaisquer fins, desde que atribuída a autoria ao projeto IPv6.br (www.ipv6.br).
IPv6.br A Nova Geração do Protocolo Internet
REDE
INTERFACE
2001 : 0DB8 : CAFE : DAD0 : FACA : CA5A : F0CA : DEAD /128
/3 /16 /32 /48 /64 /80 /96 /112
CAFE
1100
Cada número hexadecimal representa 4 bits, do total de 128 bits.
/128 = 256 IPs
2001:db8:cafe:dad0:faca:ca5a:f0ca:de00/120
/112 = 65.536 IPs
2001:db8:cafe:dad0:faca:ca5a:f0ca::/112
/96 = 4.294.967.296 IPs
2001:db8:cafe:dad0:faca:ca5a::/96
/80 = 281.474.976.710.656 IPs
2001:db8:cafe:dad0:faca::/80
ATENÇÃO! Em redes IPv6, o tamanho recomendado para redes locais é um prefixo /64. Prefixos maiores ou menores podem trazer problemas para o funcionamento de algumas funcionalidades, por exemplo, a autoconfiguração de endereços stateless. No entanto, é possível utilizar outros tamanhos de prefixos em situações mais específicas, como em enlaces ponto-a-ponto.
/64 = 18.446.744.073.709.551.616 IPs
2001:db8:cafe:dad0::/64
/60 = 16 redes /64
2001:db8:cafe:dad0::/60
/56 = 256 redes /64
2001:db8:cafe:da00::/56
/52 = 4.096 redes /64
2001:db8:cafe:d000::/52
/48 = 65.536 redes /64
2001:db8:cafe::/48
/44 = 16 redes /48
2001:db8:caf0::/44
/40 = 256 redes /48
2001:db8:ca00::/40
/36 = 4.096 redes /48
2001:db8:c000::/36
/32 = 65.536 redes /48
2001:db8::/32
/16 = 65.536 redes /32
2001::/16
/12 = 1.048.576 redes /32
2800::/12 (Alocação do LACNIC)
/3 = 512 redes /12
2000::/3 (Global Unicast)
Recomendação para designação de endereços (RFC 3177):
- De um modo geral, redes /48 são recomendadas para todos os tipos de usuários sejam usuários domésticos, pequenas ou grandes empresas;
- Empresas muito grandes podem receber um /47, prefixos um pouco menores, ou múltiplos /48's;
- Redes /64 são recomendadas quando houver certeza que uma e apenas uma sub-rede é necessária;
- Uma rede /128 pode ser utilizada quando houver absoluta certeza de que uma e apenas uma interface será conectada. Ex.: Uma conexão dial-up via PPP
Provedores Internet:
A alocação mínima para ISP's é um bloco /12, no entanto, alocações maiores podem ser feitas mediante apresentação de justificativa de utilização. É importante destacar que, diferente do IPv4, com IPv6 a "utilização" é medida em relação ao número de designações de blocos /48 para usuários finais, e não em relação ao número de endereços designados aos usuários finais.
Regional Internet Registries (RIR):
Todos os RIRs, atualmente, possuem uma alocação /12. Antigamente eram feitas alocações /16. A alocação 2800::/12 corresponde ao espaço reservado para o LACNIC.
Global Unicast (endereços atualmente reservados para a Internet):
A rede 2000::/3 está reservada para uso na Internet e corresponde a apenas 13% do espaço possível no IPv6.
IPv6.br A Nova Geração do Protocolo Internet