UNIDADE 2 – IPV4, IPV6, VLSM E CID
MÓDULO 1 – REDES CLASSFULL – REDES CLASSES A, B, C, D E E.

01

1 - ENDEREÇAMENTO IPV4

Um dos mais importantes tópicos na discussão do TCP/IP é o planejamento da atribuição do endereçamento IP (Internet Protocol) nos dispositivos que requerem esse identificador lógico (ETD-estações de trabalho desktops/notebooks, impressoras, telefones, roteadores. Mais recentemente SmartTV, wireless tablete, Smart devices, dentre outros).

Antes, recorde rapidamente alguns conceitos já vistos (se ainda não os aprendeu, a hora é agora!): o modelo ISO-OSI, Infra-estrutura-Tecnologias de rede: Ethernet (IEEE 802.3), Wi-Fi (IEEE 802.11), SONET/SDL, DSL, Cable Modem, WiMax; Redes Óticas. Saiba+

Com relação à Rede de tecnologia **Ethernet** (caso não se lembre, recorde!) ela utiliza:

- Acesso ao meio por contenção (Contention Media Access Method) quando utiliza mesma largura de banda;
- Meio de acesso Carrier Sense Multiple Access with Collision Detect (CSMA/CD);
- Half-Duplex de comunicação com somente um par de cabos com sinal em ambas as direções (colisão). Taxa de transmissão <= 10 Mbps;

Full-Duplex de comunicação com dois pares de cabos. Não há colisão. Taxa de transmissão <= 100 Mbps em ambas as direções. Taxa total de 200 Mbps.

- Padrão Ethernet na Camada Física (EIA/TIA (Eletronic Industry Association/Telecom Industry Association): [Taxa de transmissão] [Tipo de transmissão] [Comprimento máximo do cabo] = 10Base2.
- 10Base2, 10Base5 e 10BaseT: padrão 802.3 do IEEE (Institute of Electrical and Electronic Engineers).

Saiba+
Para melhor compreensão da "sopa de letrinhas" do nosso mundo de Redes de Computadores, tirar outras dúvidas e conhecer mais acerca do assunto acesse:

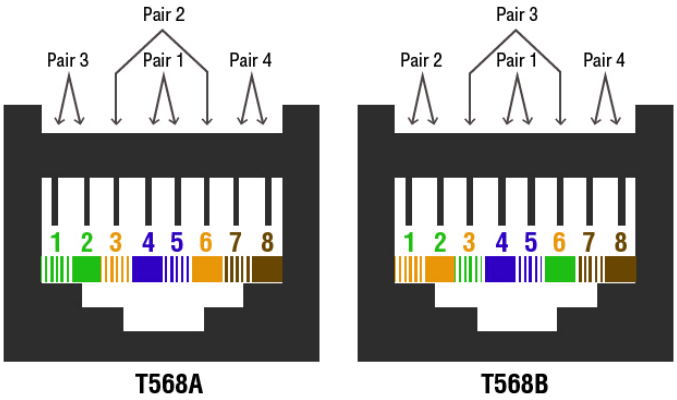
- http://www.extremenetworks.com.br/glossario.asp acessado em abril de 2015;
- Quer saber mais da Internet?
- Procure por: http://www.aisa.com.br/index1.html acessado em abril de 2015;
- http://www.aisa.com.br/mapa.html , acessado em abril de 2015 ou

http://navigators.com/internet_architecture.html acessado em abril de 2015.

02

Para a interligação entre dispositivos utilizamos o cabo ethernet par trançado. Para conectar dois componentes diferentes (um roteador e um PC), utiliza-se um cabo comum. Para conectar dois equipamentos iguais (equipamentos que trabalham em camadas iguais, como dois computadores), é necessário um cabo cross-over.

A diferença é que, no cabo comum, a ponta dos fios é igual no conector. O cabo cross-over tem um lado no modo 568A (tipo de cabo que serve para tráfego de dados na rede e normalmente é ligado em um Hub ou um Swtich) e o outro no modo 568B (tipo de cabo que serve para o tráfego de dados e voz pela rede e também é ligado em um hub ou um Swtich). Veja figura a seguir.



Tipos de Conectores
Fonte: Internet, acesso em abril 2015.

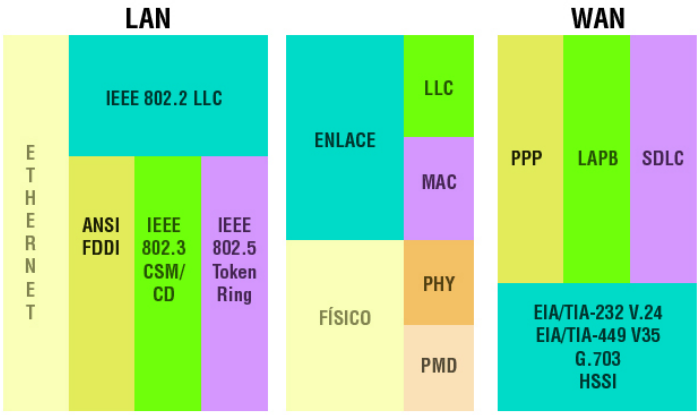
- **Cabos Straight-Through**;
- **Cabos Cross-Over**.

Cabos Straight-Through
Conexão entre um roteador e hub ou switch, um servidor a um hub ou switch, um Workstation a um hub ou switch, ou seja, conexões em equipamentos definidos em camadas diferentes.

Cabos Cross-Over
Uplinks entre swtiches, hubs a switches, hub a outro hub, roteador a outro roteador, dois computadores, ou seja, equipamentos definidos na mesma camada. Exceção: PC com roteador usa cabo Cross-Over, pois considera-se que estes trabalham nas mesmas camadas de rede, enlace e física.

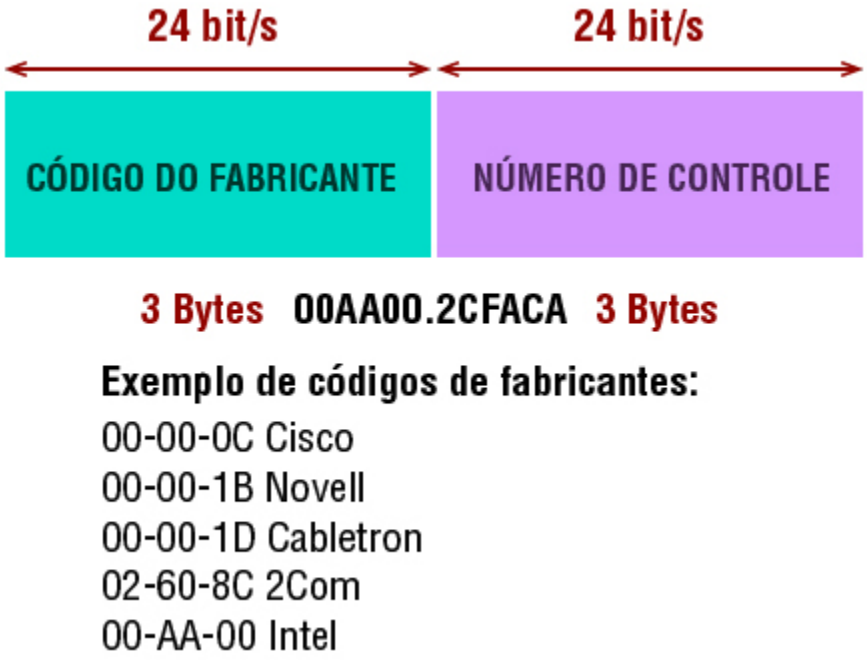
03

Veja abaixo as tecnologias existentes da camada física.



Tecnologias da camada física
Fonte: Internet, acesso em abril 2015.

Na figura abaixo o endereço físico MAC.



Endereço Físico
Fonte: Internet, acesso em abril 2015.

04

1.1 - Switches e Bridges na Camada de Enlace

Vamos recordar os pontos mais importantes da camada de enlace que abriga os switches e as bridges.

Switch é um ECD para fazer a comutação por meio da camada de enlace do protocolo TCP/IP com vários ETD e filtra a rede utilizando os endereços MAC. É um hardware-based bridges (ASICs – Application Specific Integrated Circuits) dedicado ao processamento de quadros.

a) O que caracteriza o switch?

1) Comutação (*switching*) na camada de enlace. A ligação é baseada no endereço MAC, para filtragem da rede.

2) Velocidade de transmissão limitada ao meio (*wire speed transmission*).

3) Baixa latência/espera (*low latency*).

4) Baixo custo.

5) Alta eficiência.

b) Para que serve o switch?

1) Utilizado para conectividade entre grupo de trabalho e segmentação da rede (quebra do domínio de colisão), em ambiente onde a maioria (80%?) dos usuários permanecem no segmento local.

2) Quebra o domínio de colisão em vários, mas um só domínio de broadcast.

c) Quais as funções do switch na camada de enlace?

1) Aprendizagem de endereços.

2) Decisões de filtragem/encaminhamento.

3) Esquema de inibição de loops (STP).

05

d) E em Nível da Rede?

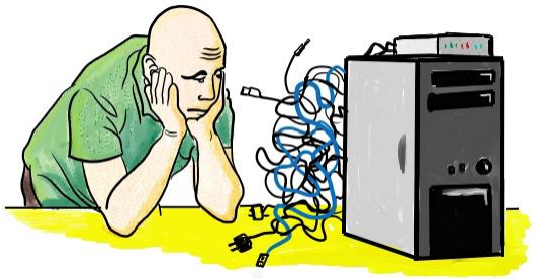
A camada de rede define e gerencia o endereçamento lógico da rede–IP. Roteia os dados pela internetwork por meio dos roteadores ou switch camada3. Os roteadores quebram o domínio de broadcast.

Os pontos mais importantes acerca dos **roteadores** são:

- Não propagam mensagens de broadcast ou de multicast;
- Utilizam endereço lógico no cabeçalho de camada de rede para determinar o roteador vizinho para o qual o pacote deve ser enviado;
- Podem prover funções de enlaces;

- Possibilitam a comunicação entre VLANs;
- Podem prover QoS para tipos específicos de tráfego de dados.

Por favor, **evite** essa cena:



Problemas
Fonte: Internet, acesso em abril 2015.

06

e) Mas o que é o endereço IP?

O endereço IP é um identificador numérico designado a cada dispositivo conectado a uma rede IP, que determina um local para o dispositivo de rede. É um endereço lógico (software) e não físico (hardware) como o MAC (Midia Access Control).

Foi criado para permitir que um dispositivo em uma rede possa se comunicar com um dispositivo em outra rede, independentemente dos tipos de LANs envolvidos (Ethernet, Token-Ring e outros).

Vale lembrar como tudo isso começou. A internet foi concebida por pesquisadores por volta de 1966 com financiamento da DARPA (Defense Advanced Reserarch Projects Agency) do Departamento de Defesa dos EUA (DoD).

Em 1969 foram instalados os primeiros quatro nós da rede, denominada de ARPANET. Os pontos interligavam a Universidade da Califórnia, em Los Angeles (UCLA), a Universidade da Califórnia em Santa Bárbara (UCSB), a Universidade de UTAH e a Universidade de Stanford (SRI). Veja figura a seguir.

ARPANET 1969
Fonte: Acesso à Internet, Abr. 2015.

Somente em 1983, com mais de 500 hosts na rede, que surgiu a Internet baseada no protocolo IP.

Host
Host é qualquer computador ou máquina conectado a uma rede, que conta com número de IP e nome definidos. Essas máquinas são responsáveis por oferecer recursos, informações e serviços aos usuários ou clientes. Por essa abrangência, a palavra pode ser utilizada como designação para diversos casos que envolvam uma máquina e uma rede, desde computadores pessoais a roteadores.

A Internet é baseada em padrões abertos onde toda tecnologia que a compõe é publicada pela IETF (Internet Engineering Task Force) em documentos públicos acessíveis a qualquer pessoa, denominados de RFC (Request For Comments).

07

O protocolo IP foi então definido na RFC 791 para prover duas funções básicas:

FRAGMENTAÇÃO	ENDEREÇAMENTO
Que permite o envio de pacotes maiores que o limite de tráfego estabelecido num enlace, dividindo-os em partes menores.	Que possibilita identificar o destino e a origem dos pacotes a partir dos endereços armazenados no cabeçalho do protocolo.

Sua versão de protocolo, utilizada desde aquela época até os dias atuais, é a 4, comumente referenciada com o nome do **protocolo de IPv4**. Entretanto, apesar dessa versão se mostrar muito robusta, e de fácil implantação e interoperabilidade, seu projeto original não previu alguns aspectos como:

- O crescimento das redes e um possível esgotamento dos endereços IP;
- O aumento da tabela de roteamento;
- Problemas relacionados à segurança dos dados transmitidos;
- Prioridade na entrega de determinados tipos de pacotes.

O endereço IPv4, por ser um identificador composto por 32 bits, separados por blocos de 8 bits (octeto) possibilitou 2^32 (ou 2^{32} = 2 elevado a 32), ou seja, 4.294.967.296 números.

Na época o número parecia grande para atender a toda demanda e ninguém imaginava que esses endereços um dia pudessem se esgotar. Mas em fevereiro de 2011 o último lote de IPv4 disponível foi distribuído.

Mundialmente, a ICANN (Internet Corporation Assigned Names and Numbers) é a autoridade responsável pela coordenação global do sistema de identificadores exclusivos da Internet por meio da IANA (Internet Assigned Numbers Authority).

IANA
IANA (Internet Assigned Number Authority) é responsável por alocar parte do espaço global de endereços IPV4 e os números de sistemas autônomos aos Registros Regionais de acordo com as necessidades estabelecidas.

08

Com a popularização comercial da Internet na década de 1990, esses endereços começaram a ser consumidos rapidamente. Diante disso, ampliou-se a estrutura organizacional para manter a governabilidade dos recursos da Internet. Daí surgiu a RIR (Regional Internet Registry) que apresenta a estrutura hierárquica no âmbito regional, conforme a figura abaixo:

Autoridades na governança da Internet no mundo
Fonte: Acesso à Internet, Abr. 2015.

09

Em 2012 foi publicado um estudo sobre o esgotamento dos IPv4 pelo cientista chefe do APNIC, Sr. Geoff Huston, autoridade da regional da Internet na Ásia e Pacífico. Abaixo um quadro resumo da conclusão do estudo feito por ele.

Tabela 1.1 – Projeção de esgotamento do IPv4 nas RIR

RIR	ATUAÇÃO	ESGOTAMENTO	BLOCOS/8
APNIC	Ásia e Pacífico	19/04/2011	1,2044
RIPNCC	Europa	29/02/2012	3,4683
LACNIC	América Latina	19/03/2014	4,4370
ARIN	América do Norte	26/05/2014	5,9743
AFRINIC	África	31/07/2020	4,3840

Fonte: Huston, 2012

O esgotamento era previsto pela academia desde 1990, quando a Internet se tornou comercial. Desde então foram direcionados esforços no sentido de amenizar esse esgotamento. As medidas paliativas responsáveis por manter a Internet funcionando até hoje foram **CIDR**, **DHCP** e o **NAT**.

Arquitetura TCP / IP propõe esquema de endereçamento universal, ou seja, **endereço IP**.

Um endereço IP deve:

- Identificar unicamente uma rede na Internet;
- Identificar unicamente cada máquina de uma rede.

Um endereço IP compõe-se de uma quadra de números naturais na faixa de 0 (zero) a 255. Cada quadra tem um byte, normalmente representado por:

número . número . número . número

Exemplos de endereços IP:

100 . 101 . 102 . 103

150 . 165 . 166 . 0

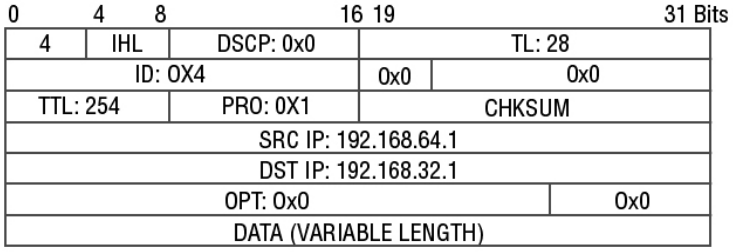
200 . 201 . 203 . 255

CIDR
CIDR (Classless Inter Domain Routing): pronuncia-se “sáider”, cuja tradução é Rota Interdomínios sem Classe, é um mecanismo de roteamento que permite sites publicarem múltiplas redes IPv4 de classe “C” com utilização de um único prefixo. CIDR sumariza (agrega) diversas redes em apenas uma, movendo-se a porção de rede (“1s”) da máscara original. O CIDR permitiu também a agregação de informação nas tabelas de roteamento, que cresciam exageradamente, fator que contribuiu para possibilitar a continuidade do crescimento da rede.

DHCP
DHCP (Dinamic Host Configuration Protocol) é um protocolo que configurado em um servidor atribui endereços IP automaticamente às estações de trabalho (ou outros dispositivos). Pode, também, configurar parâmetros TCP/IP nas estações, como os endereços de DNS, endereço default gateway da rede, wins servers e outros. O DHCP trouxe a possibilidade aos provedores de reutilizarem endereços de Internet fornecidos a seus clientes para conexões não permanentes, como as realizadas através de linhas discadas ou ADSL.

NAT
NAT (Network Address Translation), foi criado para protelar o esgotamento do espaço de endereçamento IPv4. Ele permite que uma rede privativa alcance a Internet. Resumidamente, o NAT encaminha os pacotes de dados para a Internet (rede externa) a pedido das máquinas que se encontram na rede local (privativa) para a qual está a executar as funções de tradução.

f) Formato dos pacotes IPv4:



Formato do Cabeçalho IPv4
Fonte: O autor, abril 2015.

Por enquanto não vamos nos preocupar com o significado de cada campo. O importante é saber que o **cabeçalho IPv4 tem 224 bits ou 28 bytes**.

Aqui vale lembrar a terminologia IP:

- **Bit** (digit binary);
- **Byte**;
- **Octeto**: sempre conjunto de 8 bits;
- **Endereço de Broadcast** (broadcast address);
- **Endereço Unicast** (unicast address).

Bit (digit binary)
Um dígito, 1 ou 0, representado pela letra minúscula “b” (esse será o nosso padrão. Outros poderão adotar outra convenção).

Byte
Conjunto com sequência de 8 bits.

Octeto
Sempre conjunto de 8 bits.

Endereço de Broadcast (broadcast address)
Endereço utilizado por aplicações e dispositivos para o envio de mensagens a todos os dispositivos de uma rede, simultaneamente (1 to all). Análogo à TV aberta onde todos os aparelhos de TV de uma região captam o sinal de uma emissora a partir de um ponto (antena transmissora).

Endereço Unicast (unicast address)
Comunicação de uma máquina para apenas outra máquina (1 to 1). Análogo ao pay-per-view, onde somente um assinante que solicitou o programa (e pagou por ele) o receberá.

11

g) Mudança de base de números

Antes de começar os cálculos acerca dos números IPs é importante dominar técnicas de conversão binário-decimal e vice-versa. Para isso vamos empregar o método posicional dos números. Os números binários utilizam 8 bits para definir um decimal, logo o número binário:

0	0	1	0	0	1	1	0

Em termos posicionais o octeto vale:

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Se todos os bits do octeto valerem “1” então cada octeto, em decimal, vale:

128+64+32+16+8+4+2+1=255. A posição que tiver valor “0” não será considerada.

No caso do nosso número temos:

$0*2^7+$	$0*2^6+$	$1*2^5+$	$0*2^4+$	$0*2^3+$	$1*2^2+$	$1*2^1+$	$0*2^1$

Logo:

0	0	32	0	0	4	2	0

Que nos fornece: 32+4+2=38, de acordo com as posições dos bits cada bit, em termos de sua respectiva posição, logo o número:

0	0	1	0	0	1	1	0

no sistema binário equivale a 38 no sistema decimal.

12

Assim, temos as 3 notações de IP que são aceitas e que representam o mesmo número:

1) **Decimal** (dotted decimal): 172.16.30.56
2) **Binário**: 10101100.00010000.00011110.00111000
3) **Hexadecimal**: AC 10 1E 38

Quando o IP (Internet Protocol) foi padronizado pelo IETF (Internet Engineering Task Force) em Setembro de 1981, a especificação requeria que cada dispositivo conectado a rede IP possuísse um endereço IP de 32 bits, chamado endereço IPv4 (IP versão 4), que permitia 2^{32} (4.294.967.296) endereços diferentes. Dispositivos como os roteadores, devem possuir dois endereços IPs diferentes, um para cada interface de rede.

Estes endereços são divididos em duas partes específicas:

A primeira parte de um endereço IP identifica a rede na qual o dispositivo está conectado (Número da rede ou Prefixo de rede).	A segunda parte identifica aquele dispositivo (host) na rede (Número do host).

Esta estrutura de endereçamento possui, portanto, dois níveis hierárquicos, conforme abaixo:

Nº da Rede	Nº do Host

13

Todos os hosts de uma mesma rede devem possuir um único número de host. Se dois hosts estão em diferentes redes (números de rede diferentes) então podem ter o mesmo número de host.

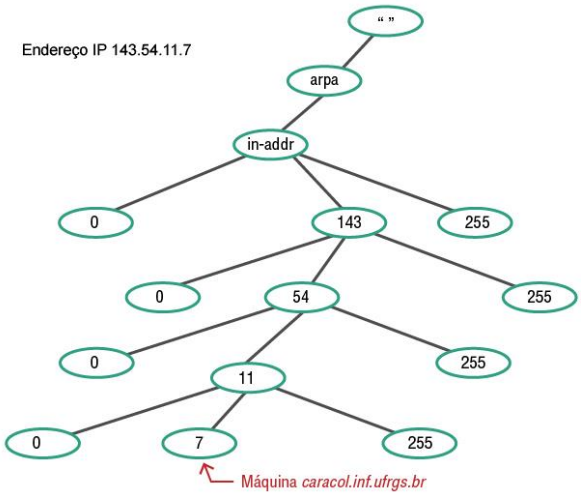
Essa estruturação adotada por alguns autores (devido à questão de que se cada endereço fosse único, todos os roteadores na Internet teriam que armazenar o endereço de cada um dos dispositivos conectado a ela) tornaria impossível um processo de roteamento eficaz, mesmo que apenas uma fração dos endereços viesse a ser utilizada.

A solução foi adotar de um esquema de endereçamento de três níveis: REDE. <SUBNET>.HOST. A porção REDE identifica a grande área, a porção SUBNET, mais específica, define a área de chamada e finalmente a porção HOST identifica o número do cliente. O padrão hierárquico segue o mesmo conceito do nosso número de telefone. Veja:

55-11-3344-1234, onde: 55: país; 11: cidade; 3344: central e 1234: assinante.

Assim teríamos: REDE CLASSFULL, que contém SUB-REDE, que contém HOST.

Veja a figura abaixo:

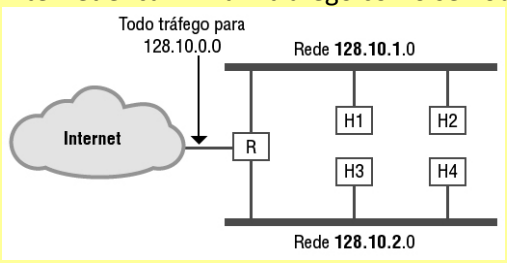


Hierarquia do número IPv4
Fonte: Acesso à Internet, abril 2015.

O endereço da rede identifica cada rede distintamente. Toda e qualquer máquina em uma rede divide o mesmo endereço de rede como parte de seu endereço IP. No exemplo dado acima, 172.16.30.56, a parte 172.16 identifica a rede, sendo o endereço da mesma. O endereço do nó (host) identifica individualmente cada dispositivo conectado à rede, logo, 30.56 é o dispositivo na rede.

Classful
No esquema de endereçamento IP original classful, cada rede física recebe um endereço de rede exclusivo; cada host em uma rede tem o endereço de rede como um prefixo do endereço individual do host.

Sub-rede
Um modo fácil de entender o endereçamento de sub-rede é imaginar que um site possui um único endereço de rede, porém duas ou mais redes físicas. Somente os roteadores locais sabem que existem várias redes físicas e como encaminhar o tráfego entre elas; todos os outros roteadores na internet encaminham tráfego como se houvesse uma única rede física no site.



Ao usar o endereço de sub-rede, pensamos em um endereço IP de 32 bits como tendo uma parte de Rede e uma parte de Rede Local, em que a parte de Rede identifica um site, possivelmente com várias redes físicas, e a parte local identifica uma rede física e um host neste site. O resultado é um endereçamento hierárquico que leva ao roteamento hierárquico correspondente.

2 - Formação das Classes de Rede

Endereços IP são organizados em classes. As classes determinam quantos bits são usados para identificar a rede e quantos são usados para codificar a máquina. A esse esquema de endereçamento chamamos **classful**.

Com o intuito de fornecer uma flexibilidade de endereçamento e suportar redes de tamanhos diferentes, o IPv4 foi criado com um espaço de endereços dividido em cinco diferentes categorias:

1) Endereços Classe A;

2) Endereços Classe B;

3) Endereços Classe C;

4) Endereços Classe D e

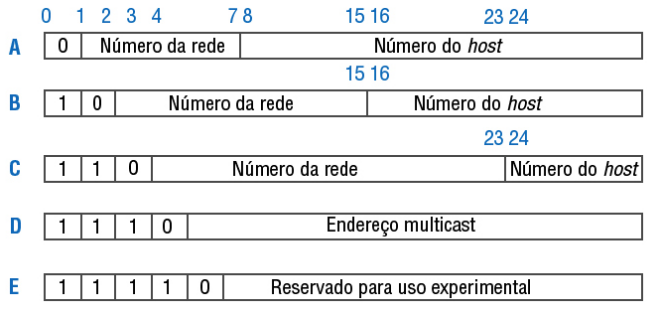
5) Endereços Classe E.

Cada classe fixa os limites entre o Número de rede e o Número do host em um local diferente do endereço de 32 bits. Os formatos das Classes Primárias de Endereços são ilustrados na figura a seguir.

Uma das características fundamentais do endereçamento IP é que cada endereço é fornecido com uma "chave" que identifica o ponto de divisão entre o Número de rede e o Número de host. Esta chave é conhecida como **Máscara de rede** ou simplesmente Máscara. Esta máscara fornece, portanto, o comprimento do Número de rede.

Por exemplo, se os primeiros dois bits de um endereço IP são 01, do LSB (bit menos significativo) para o MSB (bit mais significativo), o ponto de divisão situa-se entre os bits na posição 15 e 16. Este mecanismo simplifica o sistema de roteamento da Internet conforme veremos no decorrer do curso.

Temos então o quadro abaixo que resume as cinco classes de rede.



Formato das Classes Full (IPv4)
Fonte: Acesso à Internet, abril 2015.

2.1 – Critério utilizado na formação das classes de rede

Como eram formadas as Classes nos primórdios da Internet? Vejamos a seguir.

2.1.1 - Classe A de endereços

Em um endereço classe “A” o primeiro octeto sempre define o endereço de rede e os três restantes definem o endereço do dispositivo nessa rede:

REDE. host.host.host.

Os engenheiros do esquema de endereçamento definiram que o 1º bit do 1º octeto de um endereço pertencente à classe A deve estar “desligado”, ou seja, igual a “0”. Assim formalizou-se a regra de que a rede classe “A” começa com o número “0”, logo teríamos: 0xxxxxxx. host . host . host, ou seja, para a classe “A” teríamos 0+64+32+16+8+4+2+1 = 127 (se quiser: 255-128=127) redes. Lembre-se do octeto representado em binário e seu respectivo valor em decimal.

Rede classe A: 0.0.0.0 – 127.255.255.255, portanto a classe “A” tem redes definidas no intervalo 0 e 127.

A porção de rede dos endereços classe A tem o tamanho de 1 Byte, com o 1º bit deste Byte reservado de valor “0” e os 7 bits restantes disponíveis para manipulação. Como resultado o **número maior da rede da classe A é 127**.

Na classe “A” temos três **exceções**:

1) a rede de número 0.0.0.0: não é utilizada para endereçamento IP na Internet, pois, como veremos mais tarde, essa rede é utilizada para definir a rota padrão de roteamento;
2) a rede de número 127.0.0.0/8: não é utilizada, pois é usada para loopback interno (localhost) e
3) a rede 10.0.0.0/8 é de uso privativo. Na prática temos 128-3=125 redes classe “A”.

16

Cada uma dessas 125 redes tem 24 bits para a porção de host, logo obtém-se 2^{24} - 2 = 16.777.214 endereços únicos para cada endereço de rede pertencente à classe “A”. O menos 2 justifica-se pela retirada do 1º IP identificador da rede e o último o Broadcast da mesma.

A rede 10.0.0.0 não poderá ser utilizada para endereçamento Internet, pois a RFC-1918 (Request for Comments- padrão definido que normatizam as regras aplicadas na Internet) determina que seja não roteável na Internet por ser de uso específico. É dita **rede privativa**. Uma empresa pode utilizar essa rede internamente, porém para acessar a Internet com a mesma deverá utilizar o NAT-Network Address Translation, um artifício de tradução de endereços.

Na classe “A” temos como endereços válidos os do intervalo, por exemplo, 10.0.0.1 a 10.255.255.254, ou seja, entre o do endereço da rede e o endereço de Broadcast.

Os endereços Classe A correspondem a 50% do espaço total de endereços IP.

Classe A:

0	ID da rede – 7 bits	ID host – 8 bits	ID host – 8 bits	ID host – 8 bits

17

2.1.2 - Classe B de endereços

Nesta classe os primeiros 2 Bytes designam a porção de rede, enquanto os 2 Bytes seguintes designam a porção de host. O formato de um endereço classe “B” é:

REDE.REDE.host.host

Na classe “B” são fixos os dois primeiros bits do 1º octeto em 10, ou seja, um endereço classe “B” sempre começa com “10”. Assim temos: 10xxxxxx . xxxxxxxx . host . host

Ou seja, os endereços classe “B” vão até: 128+0+32+16+8+4+2+1 = 191. Logo, o intervalo da classe “B” começa com 128.0.0.0 e vai até 191.255.255.255.

O número de redes na classe “B” é de: 6 bits+8 bits=14 bits (6 do 1º octeto e 8 do 2º octeto). Isso fornece um total de 2^{14} = 16.384 redes.

Tal como na classe “A”, nesta o endereço de rede 172.16.0.0/12 (total de 16 redes) é de uso privativo, ou seja, não roteável na Internet.

Os endereços válidos na classe “B” são: $2^{16} – 2$ = 65.534 endereços possíveis para dispositivos para cada endereço de rede classe “B” (O “menos 2” se justifica pelo mesmo motivo explicado na explanação da classe “A”).

Na classe “B” temos como endereços válidos os do intervalo, por exemplo, 172.16.0.1 a 172.16.255.254, ou seja, entre o do endereço da rede e o endereço de Broadcast.

Classe B:

1	0	ID da rede – 14 bits	ID host – 8 bits	ID host – 8 bits

18

2.13 - Classe C de endereços

Um endereço classe “C” tem os primeiros 3 Bytes designando a porção de rede, enquanto o Byte restante designa a porção do host. O formato de um endereço classe “C” é:

REDE.REDE.REDE.host.

Por exemplo, no endereço IP=192.168.30.56 a porção 192.168.30 determina o endereço da rede e o 56 é o dispositivo dessa rede.

Na classe “C” os primeiros 3 bits são fixos em 110xxxxx . xxxxxxxx . xxxxxxxx . host, ou seja, um endereço classe “C” sempre começa com “110”.

Os endereços classe “C” vão até: 128+64+0+16+8+4+2+1 = 223. Logo, o intervalo da classe “C” começa com 192.0.0.0 e vai até 223.255.255.255.

Assim, na classe “C” temos 5bits do 1º octeto + 8 bits do 2º octecto + 8 bits do 3º octeto = 21 bits que designam redes. Isso fornece um total de 2^{21}=2.097.152 endereços de rede. Similarmente às redes classes “A” e “B”, a “C” tem a rede 192.168.0.0/16 como rede privativa.

Classe C:

1	1	0	ID da rede – 21 bits	ID host – 8 bits

19

2.1.4 – Classe D de endereços

Esta classe foi definida como tendo os 4 primeiros bits do número IP como sendo sempre iguais a 1, 1, 1 e 0.

A classe D é uma classe especial, reservada para os chamados endereços de **Multicast**. Os endereços IPs desta classe não são roteáveis na Internet.

Os endereços classe “D” vão até: 128+64+32+0+8+4+2+1 = 239. Logo, o intervalo da classe “D” começa com 224.0.0.0 e vai até 239.255.255.255.

Classe D:

1	1	1	0	ID Multicast – 28 bits

20

2.1.5 – Classe E de endereços

Esta classe foi definida como tendo os 5 primeiros bits do número IP como sendo sempre iguais a 1, 1, 1, 1 e 0.

A classe E é uma classe especial, reservada para **pesquisa** somente. Os endereços IPs desta classe não são roteáveis na Internet.

Os endereços classe "E" vão até: 128+64+32+16+0+4+2+1 = 247. Logo, o intervalo da classe "E" começa com 240.0.0.0 e vai até 247.255.255.255.

Classe E:

1	1	1	1	0	Uso Futuro - 27 bits

21

A tabela a seguir resume as classes de rede.

Tabela 1.2: ClassFull – Resumo

Classe	1º Octeto	Netw. e Host	Máscara	Nº redes	Nº hosts
A	1-127	N.H.H.H	255.0.0.0	124(2^7-4)	16.777.214 (2^{24}-2)
B	128-191	N.N.H.H	255.255.0.0	16.382 (2^{14}-2)	65.534 (2^{16}-2)
C	192-223	N.N.N.H	255.255.255.0	2.097.150 (2^{21}-2)	254 (2^{8}-2)
D	224-239	Multicast	NA	NA	NA
E	240-247	Pesquisa	NA	NA	NA

Fonte: O Autor, 2015.

Alguns IPs especiais:

Este host:

Tudo igual a "0"

Host nesta rede:

Tudo igual a “0”	ID do host

Broadcast limitado:

Tudo igual a “1”

Broadcast dirigido à rede:

ID da Rede	Tudo igual a “1”

22

Endereços Broadcast (difusão) servem para endereçar simultaneamente todas as máquinas da rede (vale, em geral, somente para máquinas de uma mesma rede local).

São formados colocando-se todos os bits da parte de endereçamento de máquina de um endereço IP com valor 1.

Exemplo:

Endereço IP	**Endereço de difusão**
200.237.190.21	200.237.190.255
150.165.166.21	150.165.255.255
26.27.28.21	26.255.255.255

Endereço de **Loopback**:

127	Qualquer combinação (normalmente 0.0.1)

O endereço 127.0.0.0 da classe A é reservado. É usado para testes do TCP/IP e para comunicação Inter processos em uma máquina local. Quando uma aplicação usa o endereço de “loopback” como destino, o software do protocolo TCP/IP devolve os dados sem gerar tráfego na rede. É a forma simples de fazer com que um cliente local fale com o servidor local correspondente, sem que se tenha de alterar o programa cliente e/ou o programa servidor.

23

2.1.6 – Máscara da rede

A **máscara de rede** padrão serve para separar, do endereço IP, a porção do número que designa a rede da porção que designa os hosts.

Em um endereço de classe A, a máscara será 255.0.0.0, indicando que o primeiro octeto se refere à rede e os três últimos ao host. Em um endereço classe B, a máscara padrão será 255.255.0.0, onde os dois primeiros octetos referem-se à rede e os dois últimos ao host e, em um endereço classe C, a máscara padrão será 255.255.255.0, onde apenas o último octeto refere-se ao host.

Para que serve a máscara da rede?

Serve para "extrair" a identificação de rede de um endereço IP através de uma operação simples de AND binário, ou seja, IP & Msc = Rede.

Exemplo:

Endereço IP:	**200.237.190.21**
Máscara da rede:	255.255.255. 0
Endereço da rede:	200.237.190. 0

Imagine que exista a rede XYZ e esta possui a máscara 255.255.255.0. Pode-se ter 3 máquinas: um computador com IP 192.168.0.1, outro com IP 192.168.0.101 e outro com IP 192.168.0.250, todos pertencentes à mesma rede XYZ, pois usam a mesma máscara.

Como todos possuem a mesma máscara, logo estão na mesma rede, logicamente conectados, e podendo compartilhar dados entre si.

24

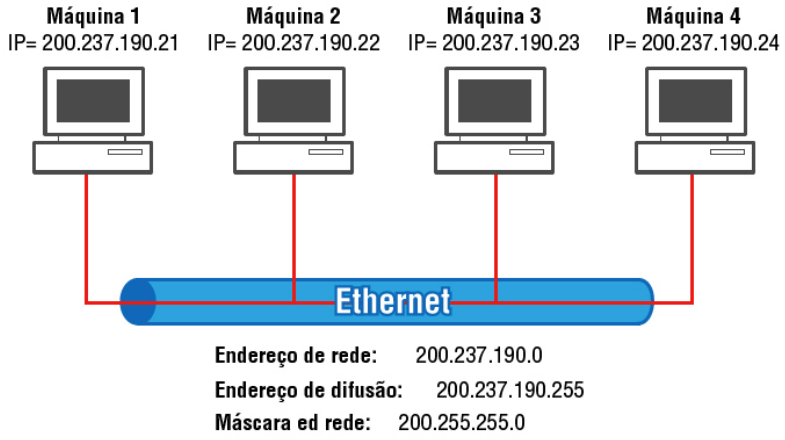
O cálculo inverso também pode ser feito, ou seja, para obter o endereço de máquina faz-se uma operação binária AND com o complemento da máscara de rede.

Endereço IP:	**200.237.190.21**
Máscara da rede:	0. 0. 0.255
Endereço da máquina:	0. 0. 0.21

Outro exemplo:

Endereço IP	Máscara Rede	Endereço Rede	Endereço Máquina	Broadcast
200. 237.190.21	255.255.255.0	200.237.190.0	0.0.0.21	200.237.190.255
150.165.166.21	255.255.0.0	150.165.0.0	0.0.166.21	150.165.255.255
26.27.28.21	255.0.0.0	26.0.0.0	0.27.28.21	26.255.255.255

Mais um exemplo:



Endereços da rede e máscara
Fonte: Dantas(2002).

25

3 - Endereços IP e Atribuição de nomes (DNS)

3.1 – O que faz o DNS?

Um equipamento na rede XYZ pode ser um notebook, PC ou Tablet e para acessar a Internet (outra rede) basta atribuir o endereço IP do seu modem para o gateway e o DNS de cada equipamento.

Ele simplesmente pega os nomes dos sites que você coloca no navegador e os converte em endereço IP para buscar na Internet. Por exemplo, quando é digitado www.google.com.br é a mesma coisa que digitar, no meu caso, 216.58.222.3 (obs.: para verificar em seu equipamento com sistema operacional Windows: Iniciar -> cmd<enter> -> na tela do cmd.exe comande “ping google.com.br” sem os aspas).

O que é mais fácil gravar: esse endereço IP ou o nome do site?

Com certeza os nomes dos sites. Faça o teste e digite o endereço obtido em sua máquina no seu navegador e veja o resultado. Para encontrar o IP de um site qualquer, utilize o prompt digitando o comando nslookup <site>.

26

3.2 – O que é o DNS?

O Domain Name System (DNS) é um sistema de gerenciamento de nomes hierárquico e distribuído para computadores, serviços ou qualquer recurso conectado à Internet ou em uma rede privada.

O DNS baseia-se em nomes hierárquicos e permite a inscrição de vários dados digitados além do nome do host e seu IP.

Em virtude do banco de dados de DNS ser distribuído, seu tamanho é ilimitado e o desempenho não degrada tanto quando se adiciona mais servidores nele. Este tipo de servidor usa como porta padrão a de número 53.

A implementação do DNS-Berkeley foi desenvolvido originalmente para o sistema operacional BSD UNIX 4.3.

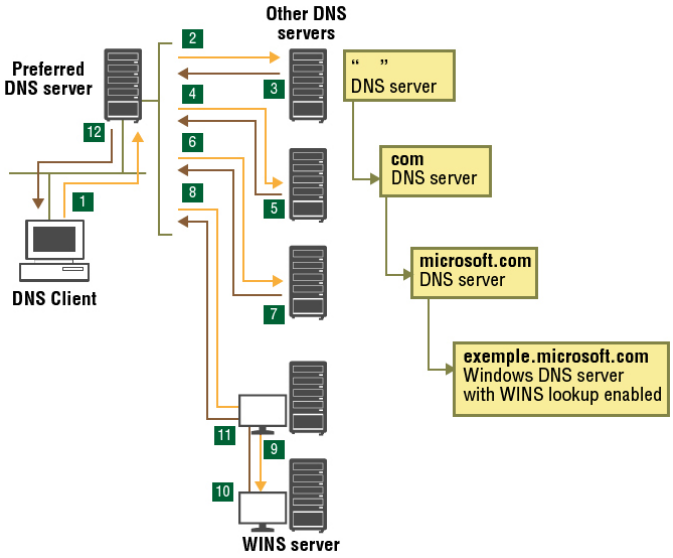
27

3.3 - Qual a função principal do DNS?

O DNS é um mecanismo para traduzir um nome de domínio em um endereço IP. Vimos que um recurso da internet, por exemplo, um site da Web, pode ser identificado de duas maneiras: pelo seu nome de domínio, por exemplo, “www.wikipedia.org” ou pelo endereço de IP dos equipamentos que o hospedam (por exemplo, 208.80.152.130 é o IP associado ao domínio www.wikipedia.org). Endereços de IP são usados pela camada de rede para determinar a localização física e virtual do equipamento. Nomes de domínio, porém, são mais mnemônicos para o usuário e empresas.

Presume-se que o DNS sirva apenas ao objetivo de mapear nomes de hosts da Internet a dados e mapear endereços para nomes de host. Isso não é correto, o DNS é um banco de dados hierárquico (ainda que limitado), e pode armazenar quase qualquer tipo de dados, para praticamente qualquer finalidade.

Veja figura a seguir:



Funcionamento do DNS.
Fonte: acesso à Internet, abril 2015.

28

3.4 - DNS reverso

Normalmente o DNS atua resolvendo o nome do domínio de um host qualquer para seu endereço IP correspondente. O DNS Reverso resolve o endereço IP, buscando o nome de domínio associado ao host. Ou seja, quando temos disponível o endereço IP de um host e não sabemos o endereço do domínio (nome dado à máquina ou outro equipamento que acesse uma rede), tentamos resolver o endereço IP através do DNS reverso que procura qual nome de domínio está associado aquele endereço.

Os servidores que utilizam o DNS Reverso conseguem verificar a autenticidade de endereços, verificando se o endereço IP atual corresponde ao endereço IP informado pelo servidor DNS. Isto evita que alguém utilize um domínio que não lhe pertence para enviar spam.

29

Resumo

Foi visto neste módulo que um dos mais importantes tópicos na discussão do TCP/IP é o planejamento da atribuição do endereçamento IP nos dispositivos que requerem esse identificador lógico (ETD-estações de trabalho desktops/notebooks, impressoras, telefones, roteadores. Mais recentemente SmartTV, wireless tablete, Smart devices, dentre outros)

Para tanto, o entendimento do modelo ISO-OSI, Infra-estrutura-Tecnologias de rede: Ethernet (IEEE 802.3), Wi-Fi (IEEE 802.11), SONET/SDL, DSL, Cable Modem, WiMax; Redes Óticas é fundamental para que se entenda o processo.

A rede Ethernet é a mais importante para nós, pois mais de 90% de nossas LANs e WANs estão sob a tecnologia da mesma.

A ICANN (Internet Corporation Assigned Names and Numbers) é a autoridade responsável pela coordenação global do sistema de identificadores exclusivos da Internet por meio da IANA (Internet Assigned Numbers Authority).

Vale lembrar que um endereço IP deve: 1) Identificar unicamente uma rede na Internet; 2) Identificar unicamente cada máquina de uma rede; 3) Um endereço IP compõe-se de uma quadra de números naturais na faixa de 0 (zero) a 255. Cada quadra tem um byte, normalmente representado por: **número . número . número . número.**

Não esquecer o conceito das mudanças de base de números feitas por meio do método posicional dos números.

Depois recordar a formação das classes de rede com os respectivos bits fixos identificadores de cada classe “A”, “B” e “C” endereçáveis na Internet e critérios próprios de formação.

Outro ponto a lembrar é acerca da máscara da rede que serve para separar, do endereço IP, a porção do número que designa a rede da porção que designa os hosts, ou seja, ela serve para “extrair” a identificação de rede de um endereço IP através de uma operação simples de AND binário, ou seja, IP & Msc = Rede.

UNIDADE 2 – IPV4, IPV6, VLSM E CID

MÓDULO 2 – ENDEREÇAMENTO IPV6 E REDES CLASSLESS – REDES SEM CLASSE.

01

1- ENDEREÇAMENTO IPV6

O protocolo IPv6 apresenta como principal característica e justificativa para o seu desenvolvimento o **aumento no espaço** para endereçamento.

O IPv6 possui um espaço para endereçamento de 128 bits, sendo possível obter 340.282.366.920.938.463.463.374.607.431.768.211.456 endereços (2^{128}).

Este valor representa aproximadamente 79 octilhões (7,9×1028) de vezes a quantidade de endereços IPv4 e representa, também, mais de 56 octilhões (5,6×1028) de endereços por ser humano na Terra, considerando-se a população estimada em 6 bilhões de habitantes.

O IPv6 já vem habilitado por padrão nos sistemas operacionais atuais. Se você tem uma versão atualizada de Windows, Linux, MacOS ou BSD, o IPv6 estará ativado.

Uma vez que o IPv6 esteja ativo, caso seu provedor de acesso Internet já suporte IPv6, a configuração do seu computador provavelmente se dará de forma automática. Consulte seu provedor e pergunte se ele já tem IPv6. Se não tiver, pergunte quando terá!

A maior parte dos provedores de acesso no Brasil até 2012 ainda não tinham ativado o IPv6 para usuários domésticos. Para saber como ativar o IPv6 em seu sistema operacional, clique aqui.

Clique aqui
Acesse o site http://ipv6.br/entenda/ative/ e lá você encontrará informações para habilitar o IPv6 em seu sistema operacional.

02

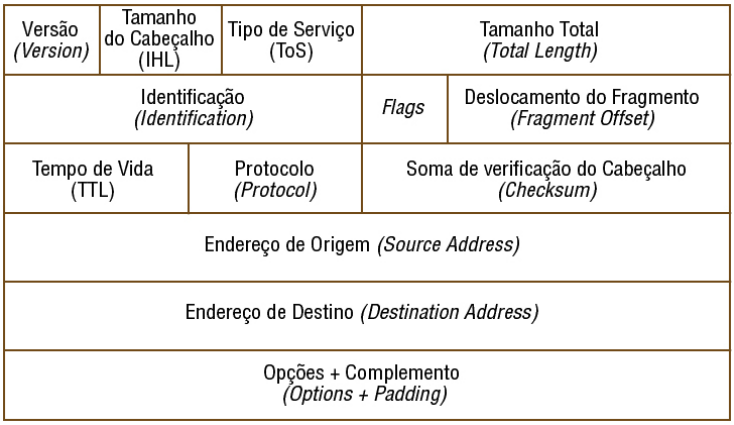
1.1- Cabeçalhos IPv4 e IPv6

Apresentaremos a seguir as principais características do **IPv6** a começar pela análise das mudanças ocorridas na estrutura de seu cabeçalho, as diferenças entre os cabeçalhos de ambas as versões, ressaltando o que foi aprimorado no funcionamento do protocolo.

a) Cabeçalho IPv4

O cabeçalho IPv4 possui 12 campos fixos, que podem ou não conter opções responsáveis por fazer com que o tamanho varie de 20 a 60 Bytes. Estes campos são destinados transmitir informações sobre:

- a versão do protocolo;
- os tamanhos do cabeçalho e dos dados;
- a fragmentação dos pacotes;
- o tipo dos dados sendo enviados;
- o tempo de vida do pacote;
- o protocolo da camada seguinte (TCP, UDP, ICMP);
- a integridade dos dados e
- a origem e destino do pacote.



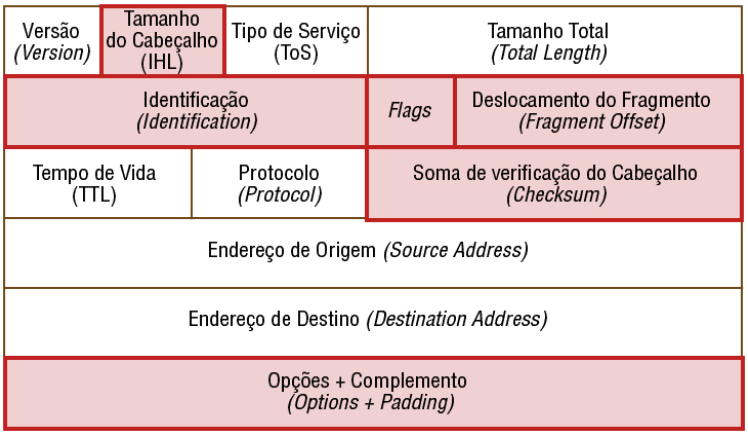
Cabeçalho IPV4

Fonte: http://ipv6.br/entenda/cabecalho/, acesso abril 2015.

03

b) Cabeçalho IPv6

Algumas mudanças foram realizadas no formato do cabeçalho base do IPv6 de modo a torná-lo mais simples. Dentre as mudanças, destaca-se a remoção de seis dos campos existentes no cabeçalho IPv4, como resultado tanto da inutilização de suas funções quanto de sua reimplantação com o uso de cabeçalhos de extensão. A figura a seguir identifica esses campos.



Campos removidos do cabeçalho IPv6 em destaque.

Fonte: acesso à Internet, abril 2015.

Removeu-se o campo “Tamanho do Cabeçalho” uma vez que seu valor foi fixado, portando desnecessário. Os campos “Identificação”, “Flags”, “Deslocamento do Fragmento” e “Opções e Complementos” passaram a ter suas informações indicadas em cabeçalhos de extensão apropriados. O campo “Soma de Verificação” foi descartado para deixar o protocolo mais eficiente já que outras validações são realizadas pelos protocolos das camadas superiores da rede.

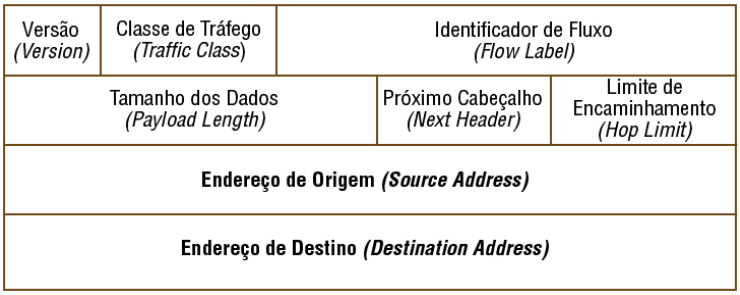
04

Conforme observamos, o número de campos foi reduzido para apenas oito e o tamanho foi fixado de 40 Bytes. Além disso, ele ficou mais flexível e eficiente com a adição de cabeçalhos de extensão que não precisam ser processados por roteadores intermediários. Tais alterações permitiram que, mesmo com um espaço de endereçamento quatro vezes maior que o do IPv4, o tamanho total do cabeçalho IPv6 fosse apenas duas vezes.

O campo "Identificador de Fluxo" foi adicionado para possibilitar o funcionamento de um mecanismo extra de suporte a QoS (Quality of Service). Mais detalhes sobre este campo e mecanismo serão apresentados nas próximas seções.

Por fim, os campos "Versão", "Endereço de Origem" e "Endereço de Destino" foram mantidos e apenas tiveram seus tamanhos alterados.

Veja abaixo como ficou o cabeçalho IPv6.



Cabeçalho IPV6.
Fonte: http://ipv6.br/entenda/cabecalho/, acesso abril 2015.

Conforme observado na figura acima, o cabeçalho do IPv6 está dividido nos seguintes campos:

1) Versão (4 bits);
2) Classe de Tráfego (8 bits);
3) Identificador de Fluxo (20 bits);
4) Tamanho do Dados (16 bits);
5) Próximo Cabeçalho (8 bits);
6) Limite de Encaminhamento (8 bits);
7) Endereço de origem (128 bits);
8) Endereço de Destino (128 bits).

Versão (4 bits)

Identifica a versão do protocolo utilizado. No caso, o valor desse campo é 6.

Classe de Tráfego (8 bits)
Identifica os pacotes por classes de serviços ou prioridade. Ele provê as mesmas funcionalidades e definições do campo “Tipo de Serviço do IPv4”.

Identificador de Fluxo (20 bits)
Identifica pacotes do mesmo fluxo de comunicação. Idealmente esse campo é configurado pelo endereço de destino para separar os fluxos de cada uma das aplicações e os nós intermediários de rede podem utiliza-lo de forma agregada com os endereços de origem e destino para realização de tratamento específico dos pacotes.

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 indicava o tamanho do cabeçalho mais o tamanho dos dados transmitidos. O tamanho dos cabeçalhos de extensão também é somado nesse novo campo.

Próximo Cabeçalho (8 bits)
Identifica o cabeçalho de extensão que segue o atual. Ele foi renomeado (no IPv4 chamava-se Protocolo) para refletir a nova organização dos pacotes IPv6, uma vez que ele deixou de conter os valores referentes a outros protocolos, para indicar os tipos dos cabeçalhos de extensão.

Limite de Encaminhamento (8 bits)
Esse campo é decrementado a cada salto de roteamento e indica o número máximo de roteadores pelos quais o pacote pode passar antes de ser descartado. Padronizou o modo como o campo Tempo de Vida (TTL) do IPv4 é utilizado, o qual diferia da descrição original que o definia como o tempo, em segundos, para o pacote ser descartado caso não chegasse à 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.

05

Além das remoções de campos, ainda se renomeou o reposicionamento de quatro campos conforme a tabela a seguir.

Diferença IPv4 x IPv6

IPv4	IPv6
Tipo de Serviço	Classe de Serviço
Tamanho Total	Tamanho dos Dados
Tempo de Vida (TTL)	Limite de encaminhamento
Protocolo	Próximo Cabeçalho

Fonte: Brito, 2013.

A Norma que rege o IPv6 é a RFC 4291.

06

1.2 – Representação dos endereços

1.2.1- Abreviação

Podem ser aplicadas para facilitar a escrita de alguns endereços muito extensos: 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. Observa-se que a abreviação do grupo de zeros só pode ser realizada uma única vez, caso contrário haverá ambiguidades na representação do endereço. A 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::.

1.2.2- Prefixos de rede

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. Saiba+

Prefixo 2001:db8:3003:2::/64

Prefixo global 2001:db8::/32

ID da sub-rede 3003:2

Saiba+
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 e outros. Com isso, é possível diminuir o tamanho da tabela de roteamento e agilizar o encaminhamento dos pacotes.

07

1.2.3- Representação dos endereços IPv6 em URLs (Uniform Resource Locators)

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.

Observe os exemplos a seguir:

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

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

a) **Forma preferida** (endereço completo em formato hexadecimal):

b) **Forma comprimida** (substituição de sequência de zeros):

c) **Forma mista** (adequada para ambientes IPv4 e IPv6);

d) **Representação textual completa.**

Forma preferida
Esta é a forma preferida de representação:

FEA0 : 2A5F : 709C : AEBC : 97 : 3154 : 3D12
1030 : 2A9C : 0 : 0 : 0 : 500 : 200C : 3A4

Forma comprimida
Exemplo de representação de forma comprimida:

FF08 : 0 : 0 : 0 : 0 : 0 : 209A : 61 → FF08 : : 209A : 61
1030 : 2A9C : 0 : 0 : 0 : 500 : 200C : 3A4 → 1030: 2ª9C : : 500 : 200C : 3A4
0 : 0 : 0 : 0 : 0 : 0 : 0 : 1 → : : 1 (endereço de loopback)
0 : 0 : 0 : 0 : 0 : 0 : 0 : 0 → : : (endereço unspecified)

Forma mista
Exemplo de representação de forma mista:

0 : 0 : 0 : 0 : 0 : 0 : 193.136.239.163 (endereço IPv6 compatível com IPv4)
0 : 0 : 0 : 0 : 0 : FFFF: 129.145.34.10 (endereço IPv4 mapeado em IPv6)

Ou

: : 193.126.239.163 (endereço IPv6 compatível com Ipv4)
: : FFFF: 129.145.34.10 (endereço Ipv4 mapeado em Ipv6)

Representação textual completa
Exemplo de representação textual completa:

FE80 : : ABC : DEF / 10
2001 : 810 : 260 : : / 56
2001 : 810 : 260 : 1B81 : 7FBC : 98DC : 1223 / 64

08

1.3. Endereços IPv6

Há três tipos de endereços IPv6: Unicast, Anycast e Multicast.

1.3.1 Unicast

Identificam uma única interface de uma máquina, de forma que um pacote enviado a um endereço unicast é entregue a uma única interface.

Formas de endereçar Unicast:

- endereços globais, permitem agregação de endereços com base em máscaras semelhante ao CIDR.

- **endereços sites-locais**, endereçamento dentro de um site. Prefixo “1111 1110 11”

- **endereços links-locais**, usado dentro de um dado “link”, para autoconfiguração. Prefixo “1111 1110 10”

A tabela a seguir fornece alguns tipos de prefixos.

Tipos de Prefixo

Tipo	Prefixo
Não especificado	00 ... 00 (128 bits)
Loopback	00 ... 01 (128 bits)
Multicast	11111111
Link-local unicast	11111111 10
Global unicast	Restantes prefixos

Fonte: Brito, 2013.

09

Os endereços unicast são utilizados para comunicação entre dois nós, por exemplo, telefones VoIPv6, computadores em uma rede privada. A estrutura do unicast foi definida para permitir agregações com prefixos de tamanho flexível, similar ao CIDR do IPv4.

Alguns exemplos de tipos de endereços unicast IPv6: Global Unicast, Unique-Local e Link-Local.

- **Global Unicast** – é equivalente aos endereços públicos IPv4 e globalmente roteável e acessível na Internet IPv6. Ele é constituído por três partes:

    a) o **prefixo de roteamento global**, utilizado para identificar o tamanho do bloco atribuído a uma rede;

    b) a **identificação da sub-rede**, utilizada para identificar um enlace em uma rede;

    c) e a **identificação da interface**, que deve identificar de forma única uma interface dentro de um enlace.

Saiba+ sobre o endereço Global unicast

- **Link Local** – usado apenas no enlace específico onde a interface está conectada. O endereço link local é atribuído automaticamente pelo prefixo FE80::/64. Os 64 bits reservados para a identificação da interface são configurados utilizando o formato IEEE EUI-64. Vale ressaltar que os roteadores não devem encaminhar para outros enlaces, pacotes que possuam como origem ou destino um endereço link-local.

- **Unique Local Address (ULA)** – utilizado apenas para comunicações locais, geralmente dentro de um mesmo enlace ou conjunto de enlaces. Um endereço ULA é composto de quatro partes e não deve ser roteável na Internet global. Sua utilização permite que qualquer enlace possua um prefixo /48 privado e único globalmente. Deste modo, caso duas redes, de empresas distintas, por exemplo, sejam interconectadas, provavelmente não haverá conflito de endereços ou

necessidade de renumerar a interface que o esteja usando. Além disso, o endereço ULA é independente de provedor, podendo ser utilizado na comunicação dentro do enlace mesmo que não haja uma conexão com a Internet. Seu prefixo pode ser facilmente bloqueado, e caso um endereço ULA seja anunciado acidentalmente para fora do enlace, através de um roteador ou via DNS, não haverá conflito com outros endereços.

Identificação da interface
Os identificadores de interface (IID) são utilizados para distinguir as interfaces dentro de um enlace. Devem ser únicos dentro do mesmo prefixo de sub-rede. O mesmo IID pode ser usado em múltiplas interfaces em um único nó, porém, elas dever estar associadas a deferentes sub-redes. Normalmente utiliza-se um IID de 64 bits, que pode ser obtido de diversas formas.

CIDR
Conforme visto anteriormente, com o CIDR (Classless Inter-Domain Routing), o tamanho dos blocos alocados para cada rede passou a corresponder à real necessidade das mesmas.

Saiba+ Global Unicast
O Global Unicast utiliza os 64 bits mais a esquerda para identificação da rede e os 64 bits mais a direita para identificação da interface. Portanto, exceto casos específicos, todas as sub-redes em IPv6 tem o mesmo tamanho de prefixo, 64 bits (/64), o que possibilita 2^64 = 18.446.744.073.709.551.616 dispositivos por sub-rede. Atualmente, está reservada para atribuição de endereços a faixa 2000::/3 (001), que corresponde aos endereços de 2000:: a 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff. Isto representa 13% do total de endereços possíveis com IPv6, o que permite criar 2^(64−3) = 2.305.843.009.213.693.952 (2,3×1018) sub-redes (/64) diferentes ou 2^(48−3) = 35.184.372.088.832 (3,5×1013) redes /48.

Quatro partes
Um endereço ULA, com um ID global é composto de 4 partes:

a) **Prefixo**: FC00::/7.
b) **Flag Local** (L): se o valor for 1 (FD) o prefixo é atribuído localmente. Se o valor for 0 (FC), o prefixo deve ser atribuído por uma organização central (ainda a definir).
c) **Identificador global**: identificador de 40 bits usado para criar um prefixo globalmente único.
d) **Identificador da Interface**: identificador da interface de 64 bits.

Deste modo, a estrutura de um endereço ULA é FDUU:UUUU:UUUU:: onde U são os bits do identificador único, gerado aleatoriamente por um algoritmo específico.

10

1.3.2 – Endereço Anycast

Um endereço IPv6 anycast é utilizado para identificar um grupo de interfaces. Um pacote enviado a um endereço anycast é encaminhado apenas à interface do grupo mais próxima da origem do pacote.

Os endereços anycast são atribuídos a partir da faixa de endereços unicast e não há diferenças sintáticas entre eles. Portanto, um endereço unicast atribuído a mais de uma interface transforma-se em um endereço anycast, devendo-se neste caso, configurar explicitamente os nós para que saibam que lhes foi atribuído um endereço anycast. Além disso, este endereço deve ser configurado nos roteadores como uma entrada separada (prefixo /128 – host route).

Para que serve o endereço anycast?

Este esquema de endereçamento pode ser utilizado para descobrir serviços na rede, como servidores DNS e proxies HTTP, garantindo a redundância desses serviços. Utilizado, também, para fazer balanceamento de carga em situações onde múltiplos hosts ou roteadores provem o mesmo serviço, para localizar roteadores que forneçam acesso a uma determinada sub-rede ou para localizar os Agentes de Origem em redes com suporte a mobilidade IPv6.

Todos os roteadores devem ter suporte ao endereço anycast Subnet-Router. Este tipo de endereço é formado pelo prefixo da sub-rede e pelo IID preenchido com zeros (ex.: 2001:db8:cafe:dad0::/64). Um pacote enviado para o endereço Subnet-Router será entregue para o roteador mais próximo da origem dentro da mesma sub-rede.

Pode ser utilizado no suporte a mobilidade IPv6. Este tipo de endereço é formado pelo prefixo da sub-rede seguido pelo ID dfff:ffff:ffff:fffe (ex.: 2001:db8::dfff:ffff: ffff:fffe). Ele é utilizado pelo Nó Móvel, quando este precisar localizar um Agente Origem em sua Rede Original.

11

1.3.3 – Endereços Multicast

Endereços multicast também são utilizados para identificar grupos de interfaces, sendo que cada interface pode pertencer a mais de um grupo. Diferentemente da unicast, os pacotes enviados para esses endereços são entregues a todas as interfaces que compõem o grupo. São usados por apenas uma máquina para alcançar um grupo definido de máquinas, análogo à TV por assinatura.

No IPv6 é requerido que todos os nós suportem multicast, visto que muitas funcionalidades da nova versão do protocolo IP utilizam esse tipo de endereço.

Para que serve o endereço multicast?

Funciona como o broadcast, dado que um único pacote é enviado a vários hosts. No broadcast o pacote é enviado a todos os hosts da rede, sem exceção, enquanto que no multicast apenas um grupo de hosts receberá esse pacote. Isso reduz a utilização de recurso de uma rede, bem como otimiza a entrega de dados aos hosts receptores. Aplicações como videoconferência, distribuição de

vídeo sob demanda, atualizações de *softwares* e jogos on-line, são exemplos de serviços que vêm ganhando notoriedade e podem utilizar as vantagens apresentadas pelo multicast.

Os endereços multicast não devem ser utilizados como endereço de origem de um pacote. Esses endereços derivam do bloco FF00::/8, onde o prefixo FF, que identifica um endereço multicast, é precedido por quatro bits, que representam quatro flags, e um valor de quatro bits que define o escopo do grupo multicast.

13

1.3.4- Endereços IPv6 especiais para fins específicos

Existem alguns endereços IPv6 especiais utilizados para fins específicos. São eles:

a) Endereço Não-Especificado (Unspecified)

É representado pelo endereço 0:0:0:0:0:0:0:0 ou ::0 (equivalente ao endereço IPv4 unspecified 0.0.0.0). Ele nunca deve ser atribuído a nenhum nó, indicando apenas a ausência de um endereço. O endereço unspecified não deve ser utilizado como endereço de destino de pacotes IPv6.

b) Endereço Loopback

Representado pelo endereço unicast 0:0:0:0:0:0:0:1 ou ::1 (equivalente ao endereço IPv4 loopback 127.0.0.1). Este endereço é utilizado para referenciar a própria máquina, sendo muito utilizado para teste internos. Este tipo de endereço não deve ser atribuído a nenhuma interface física, nem usado como endereço de origem em pacotes IPv6 enviados para outros nós.

c) Endereços IPv4-mapeado

Representado por 0:0:0:0:0:FFFF:wxyz ou ::FFFF:wxyz, é usado para mapear um endereço IPv4 em um endereço IPv6 de 128-bit, onde wxyz representa os 32 bits do endereço IPv4, utilizando dígitos decimais. É aplicado em técnicas de transição para que nós IPv6 e IPv4 se comuniquem. Ex. ::FFFF:192.168.100.1.

d) Faixas de endereços reservadas para usos específicos:

- 2002::/16: prefixo utilizado no mecanismo de transição 6to4;

- 2001:0000::/32: prefixo utilizado no mecanismo de transição TEREDO;
- 2001:db8::/32: prefixo utilizado para representar endereços IPv6 em textos e documentações.

Outros endereços utilizados no início do desenvolvimento do IPv6 tornaram-se obsoletos e não devem mais ser utilizados. Veja quais são.

Veja quais são

Endereços que não devem mais ser utilizados:

- **FEC0::/10**: prefixo utilizado pelos endereços do tipo site local, desenvolvidos para serem utilizados dentro de uma rede específica sem a necessidade de um prefixo global, equivalente aos endereços privados do IPv4. Sua utilização foi substituída pelos endereços ULA;
- **::wxyz**: utilizado para representar o endereço IPv4-compatível. Sua função é a mesma do endereço IPv4-mapeado, tornando-se obsoleto por desuso;

3FFE::/16: prefixo utilizado para representar os endereços da rede de teste 6Bone. Criada para ajudar na implantação do IPv6, está rede foi desativada em 6 de junho de 2006 (06/06/06).

14

1.4 – Transição entre o IPv4 e o IPv6

O IPv4 e o IPv6 não são compatíveis entre si. O IPv6 não foi projetado como complemento do IPv4, mas sim, um substituto que resolve o problema do esgotamento de endereços. Apesar disso, ambos os protocolos funcionam simultaneamente nos mesmos equipamentos.

Para esse funcionamento simultâneo foi implementada a pilha dupla ou dual stack. A ideia é que, quando o IPv6 estivesse implantado em todos os dispositivos, o IPv4 deixaria de ser realmente útil e poderia ser abandonado paulatinamente.

Atualmente temos ilhas IPv6 em uma Internet majoritariamente IPv4, mas depois de algum tempo, teremos o contrário.

As **técnicas de transição**, em aplicação, segundo sua **funcionalidade**, são:

a) Pilha dupla	b) Túneis	c) Tradução
• Consiste na convivência do IPv4 e do IPv6 nos mesmos equipamentos, de forma nativa, simultaneamente. Essa técnica é a técnica padrão escolhida para a transição para IPv6 na Internet e deve ser usada sempre que possível.	• Permitem que diferentes redes IPv4 comuniquem-se através de uma rede IPv6, ou vice-versa.	• Permitem que equipamentos usando IPv6 comuniquem-se com outros que usam IPv4, por meio da conversão dos pacotes.

15

Tanto a técnica de túneis quanto as técnicas de tradução podem ser **stateful** ou **stateless**.

Técnicas stateful são aquelas em que é necessário manter tabelas de estado com informações sobre os endereços ou pacotes para processá-los.	**Técnicas stateless** não é necessário guardar informações, cada pacote é tratado de forma independente.

De forma geral técnicas stateful são mais caras: gastam mais CPU e memória, por isso não escalam bem. Sempre que possível deve-se dar preferência a técnicas stateless.

Há casos em que é necessária a comunicação entre IPv4 e IPv6 para apenas um, ou poucos tipos de aplicações. Ou ainda, quando é usada uma técnica de tradução e ela funciona para quase todas as aplicações, mas falha para algumas poucas, nomeadamente aquelas que carregam endereços IP literais no protocolo, na camada de aplicação. Para esses casos podem ser usados gateways específicos, na camada de aplicação. São chamados de Application Level Gateways, ou ALGs.

De forma geral, os **critérios** que devem ser considerados na escolha da técnica a ser utilizada são:

1) deve-se preferir técnicas que impliquem na utilização de IPv6 nativo pelos usuários finais, de forma que túneis IPv4 dentro de IPv6 devem ser preferidos em detrimento de túneis IPv6 sobre IPv4;
2) deve-se preferir técnicas stateless em detrimento de técnicas statefull;
3) deve-se evitar técnicas para prolongar o uso do protocolo IPv4, sem a adoção concomitante do IPv6;
4) deve-se analisar a adequação da técnica à topologia da rede onde será aplicada e

5) deve-se analisar a maturidade da técnica e as opções de implantação, como por exemplo suporte à mesma nos equipamentos de rede e em softwares.

16

1.5 – Endereços de conhecimento obrigatório pelos dispositivos

Qualquer **máquina** precisa reconhecer como seus, os 6 seguintes endereços:

1) endereço link-local de cada uma das interfaces;
2) endereços unicast e anycast que foram configurados;
3) endereço loopback;
4) endereços multicast que designam todos os nós, nomeadamente, FF01 : 0 : 0 : 0 : 0 : 0 : 0 : 1 e FF02 : 0 : 0 : 0 : 0 : 0 : 0 : 1
5) endereços multicast do tipo solicited-node;
6) endereços multicast de cada um dos grupos de mulicast a que pertence.

Os **roteadores**, além desses acima, devem reconhecer como seus, os 3 endereços abaixo listados:

1) endereços anycast correspondentes aos roteadores da sub-rede em que se encontram;
2) qualquer outro endereço anycast configurados no roteador;
3) endereços multicast de todos os roteadores, nomeadamente, FF01 : 0 : 0 : 0 : 0 : 0 : 0 : 2; FF02 : 0 : 0 : 0 : 0 : 0 : 0 : 2 e FF05 : 0 : 0 : 0 : 0 : 0 : 0 : 2.

17

1.6 – Autoridades da Internet

Até 1998 a coordenação dos IP era feita pela IANA (Internet Assigned Number Authority). Em 1998, foi formada a ICANN (Internet Corporation for Assigned Names and Numbers)

A RIR (Regional Internet Registries), RFC 1174, define:

- APNIC (Asia Pacific Network Information Center);
- ARIN (American Registry for Internet Numbers),
- RIPE-NCC (Réseaux IP Européens Network Coordination Centre);
- AfriNIC (The Internet Numbers Registry for Africa);

- LACNIC (Latin American and Caribbean Internet Address Registry,).

Os RIR são associações fornecedoras de serviços de Internet (Internet Services Providers - ISP).

Assistir vídeo no material online

IANA
http://www.iana.org

ICANN
http://www.icann.org

APNIC
http://www.apnic.net

ARIN
http://www.arin.net

RIPE-NCC
http://www.ripe.net

AFRINIC
http://www.afrinic.net

LACNIC
http://www.lacnic.net

18

2 - Conceitos de Classless

À medida que a Internet começou a crescer exponencialmente, problemas surgiram com o esquema classful de endereçamento IP. Essas dificuldades foram minimizadas parcialmente por meio do conceito de **endereçamento de sub-rede**. Essa forma proporciona maior flexibilidade para os administradores de redes individuais em uma Internet.

As sub-redes, no entanto, não resolvem os problemas em termos gerais. Algumas destas questões permanecem devido ao uso de classes mesmo com as sub-redes.

Embora o desenvolvimento do IPv6 tenha começado em meados da década de 1990 com seu sistema de endereçamento de 128 bits, reconheceu-se que seriam necessários muitos anos para que a implantação generalizada do IPv6 fosse possível.

A fim de prolongar a vida do IPv4 até que a recente versão do IPv6 pudesse ser concluída, foi necessário implementar nova solução para tratar dispositivos IPv4. Este novo sistema para eliminar a noção de classes inteira de endereços, criando um novo esquema de endereçamento sem classes, foi chamado de **Classless Inter-Domain Routing** (CIDR).

De forma simples, podemos dizer que os protocolos de roteamento que respeitam as regras de classes são chamados de classful (“com classe”) e os protocolos que não respeitam essa regra são chamados de protocolos de roteamento classless (“sem classe”).

19

2.1. Qual é o problema central da rede "Classful"?

A principal fraqueza da rede regular é **baixa "granularidade**". Um bloco de endereço de classe B contém 65.534 endereços de hosts, mas um bloco Classe C tem um número relativamente pequeno 254. Há milhares de organizações "médias" que precisam de mais de 254 endereços IP, mas uma pequena percentagem destas precisa de 65.534 endereços ou próximo desse número. Ao criar suas redes, estas empresas tendem a solicitar blocos de endereços classe B e não blocos classe C, porque precisam mais de 254.

Devido à forma como as classes do sistema antigo foram projetados, existem mais de 2 milhões de blocos de endereços de classe C, mas apenas 16.384 Classe B. Enquanto 16.384 parece muito à primeira vista, como há milhões de organizações e empresas ao redor do mundo, as alocações de Classe B foram consumidas rapidamente, enquanto as rede menores de classe C foram pouco utilizadas.

As autoridades que distribuíam os endereços da Internet precisavam de uma maneira de utilizar melhor o espaço de endereço para que não se recorresse a outras redes antes da transição para IP versão 6.

Você acha que subnetting seria a solução? Veja **aqui** a resposta.

A única solução para este problema seria convencer ou, no pior caso, forçar a empresa a utilizar muitos blocos Classe C, de menor tamanho, em vez de "perder" a maior parte dos IPs de classe B. Muitas organizações resistiram a essa à ideia devido à complexidade envolvida e isso fez com que o outro problema principal surgisse sem que fosse corrigido: o **crescimento das tabelas de roteamento Internet**. Substituindo uma rede Classe B com 10 Classe C significaria dez vezes mais entradas para roteadores para acompanhar.

Subnetting
Subnetting é fazer a divisão de uma rede em sub-redes. Significa utilizar a máscara de sub-rede para dividir a rede em segmentos menores ou sub-redes.

aqui
Subnetting não ajudaria muito nesta questão. Por quê? Porque ele só funciona dentro dos blocos de endereços das redes classful. Se uma organização precisasse de 2.000 endereços IP iria solicitar um bloco de rede Classe B, porém poderiam usar a sub-rede para gerenciar de forma mais eficiente o seu bloco. No entanto, as sub-redes nada poderiam fazer sobre o fato de que esta organização nunca iria usar mais de 62.000 dos endereços em seu bloco, ou seja, cerca de 97% do seu espaço de endereçamento alocado.

20

Qual seria, então, a solução?

A criação do VLSM – Variable Length Subnet Mask, ou seja, máscara de tamanho variável.

O objetivo da criação do VLSM foi economizar o uso do IPv4. Vimos que os endereços IP são projetados para serem divididos em um identificador de rede e um identificador de host. Com o conceito de sub-rede foram introduzidos alguns bits “roubados" da identificação do host para criar uma ID de sub-rede, dando ao endereço IP um total de três níveis hierárquicos. Com VLSM, nós são divididos em redes e em sub-rede, tendo mais bits a partir da identificação de host para nos dar uma hierarquia de nível múltiplo com "sub-sub-redes", "sub-sub-sub-redes" e assim por diante.

Existem dois **critérios para a aplicação do VLSM** para a divisão de uma rede em sub-redes:

1) RFC-950, com Nº SR = 2^n - 2 e Nº Hosts = 2^n - 2;
2) RFC-1812, com Nº SR = 2^n e Nº Hosts = 2^n - 2.

O RFC 950 é o menos econômico dos dois. Ele despreza a 1ª sub-rede, por ter o identificador dessa faixa (IP da 1ª sub-rede) coincidente com o identificador da rede mãe e a última sub-rede por esta ter o mesmo IP broadcast da rede mãe. Já o RCF-1812, mais recente, não despreza sub-rede alguma. A diferenciação é feita por meio da máscara atribuída ás sub-redes.

Se a divisão da rede em sub-redes for feita função do número de usuários em cada sub-rede então a fórmula é idêntica para os dois RFCs: Nº Hosts = 2^n – 2.

A situação particular de cada cenário é que definirá o emprego de cada uma das fórmulas citadas.

VLSM
VLSM (Variable Lenght Subnet Mask) é um método de cálculo de sub-redes mais eficiente que o tradicional, você pode alocar somente os bits necessários da sub-rede utilizando máscaras de tamanho variáveis. Com o VLSM você pode segmentar uma sub-rede já segmentada anteriormente,

não sendo necessário que os blocos de endereços tenham o mesmo tamanho, ou seja, podemos dizer que é possível dividir aquilo que já foi dividido.

21

Em um ambiente sem classes, alteramos a forma como olhamos para endereços IP, através da aplicação de conceitos VLSM, não só a uma rede, mas a toda a Internet. Em essência, a Internet que é uma rede gigante, torna-a um grande número de blocos. Alguns desses grandes blocos são divididos em blocos menores, que por sua vez podem ser subdivididos. Esta quebra pode ocorrer várias vezes, o que nos permite dividir o "bolo" de endereços da Internet em fatias de diversos tamanhos, para atender às necessidades das organizações.

Tratando-se da aplicação VLSM, a norma que rege as regras da divisão é o RFC-1812.

Com a utilização de sub-redes nós dividimos uma rede (classe A, B ou C) em várias sub-redes, cada uma delas com um tamanho fixo.

Exemplo:

Como dividir a rede classe C de domínio 200.200.10.0 em 08 sub-redes com a máscara /27?

Considere o RFC-1812 uma das normas que regulamenta a aplicação do VLSM, pois a outra regra é dada pelo RFC-950, mais antiga, e que desperdiça mais IPs que a considerada.

Vejamos a seguir qual seria a solução para o exemplo citado.

22

Solução:

1) Número de bits necessários para representar as 8 sub-redes citadas:

No SR = 2ˆn → 8 = 2^n → n = 3, logo, precisamos “roubar” 3 bits da porção destinada aos hosts.

2) Nova máscara resultante:

255.255.255.11100000, ou seja, 255.255.255.224

3) A variação das sub-redes:

pelo complemento de 224, temos: 256-224 = 32.

pelo bit LSB dos bits “roubados” temos o valor decimal igual a 32.

Logo, a variação é de 32 em 32.

4) Listagem das sub-redes:

Listas das sub-redes obtidas.

Id SR	1º IP válido	Último IP válido	Broadcast
200.200.10.0	200.200.10.1	200.200.20.30	200.200.10.31
200.200.10.32	200.200.10.33	200.200.10.62	200.200.10.63
200.200.10.64	200.200.10.65	200.200.10.94	200.200.10.95
200.200.10.96	200.200.10.97	200.200.10.126	200.200.10.127
200.200.10.128	200.200.10.129	200.200.10.158	200.200.10.159
.....	.....	.....	.....
200.200.10.192	200.200.10.193	200.200.10.254	200.200.10.255

Fonte: O Autor, 2015.

Com o conceito de VLSM o que se faz é dividir as sub-redes em outras sub-redes, cada uma com o tamanho necessário para satisfazer os requisitos de projeto. Simplificadamente, fazemos sub-redes das sub-redes. Podemos pegar uma das sub-redes geradas na tabela acima e dividi-la em outras sub-redes, cada uma delas com um tamanho específico. Por isso o termo **VLSM** (Variable Length Subnet Masking), ou seja, **Sub-Redes de Tamanhos Variáveis**.

23

3. Emprego das redes Classless

No início IPs não podiam receber máscaras “quebradas”, elas sempre terminavam em octetos e eram separadas em classes:

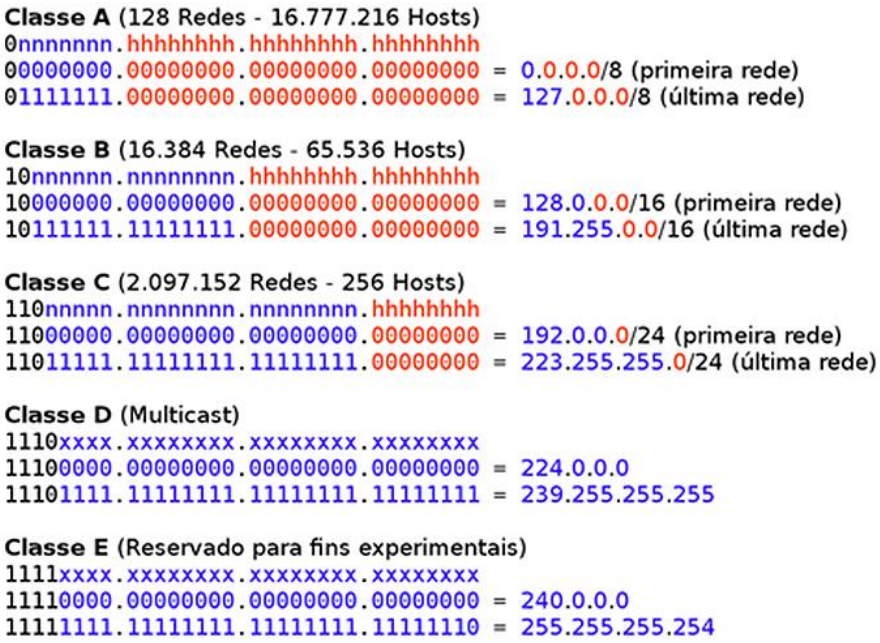


Figura 2.1: Classes de redes IPv4
Fonte: Acesso à Internet, 2015.

Essa divisão em classes é chamada de **Classful** e acarreta um enorme desperdício, pois caso precise de 2 endereços irá ser atribuído no mínimo uma Classe C que contém 254 endereços válidos para designação de ETD.

Entretanto, era muito fácil para o computador definir o que era rede e o que era host, pois se o primeiro bit fosse 0 já era possível saber que os primeiros 8 bits eram rede e o restante host. Se o primeiro bit fosse 1 e o segundo 0 sabíamos que o prefixo era /16 e assim em diante.

Nos dias atuais, classes cheias não são mais usadas, mas ainda há muitas referências verbais a elas por uma questão de legado, então devemos atentar para o fato que uma classe de IP não é definida pelo tamanho do prefixo e sim pela faixa em que ele está e o prefixo. Por exemplo, ao escrever 128.0.0.1/8 isso não é um endereço Classe A, provavelmente é uma “supernetting”. O endereço 120.0.0.1/16 não é um endereço Classe B, provavelmente uma “subnetting”.

Hoje utilizamos somente endereços Classless, pois não adotamos mais a definição de classes cheias, pela questão de que os últimos lotes classe “C” IPv4 disponíveis já foram distribuídos.

24

Resumo

O IPv6 possui um espaço para endereçamento de 128 bits, sendo possível obter 340.282.366.920.938.463.463.374.607.431.768.211.456 endereços (2^{128}). Este valor representa aproximadamente 79 octilhões (7,9×1028) de vezes a quantidade de endereços IPv4 e representa,

também, mais de 56 octilhões (5,6×1028) de endereços por ser humano na Terra, considerando-se a população estimada em 6 bilhões de habitantes.

As redes classless são as redes sem classe, ou seja, diferentemente das redes que possuem máscara /8; /16 ou /24.

Surgiu como solução a três problemas do esquema "classful" de endereçamento IP estudado no módulo anterior. Os mesmos foram minimizados parcialmente por meio do conceito de endereçamento de sub-rede. Essa forma proporciona maior flexibilidade para os administradores de redes individuais em uma Internet. Sub-redes, no entanto, não resolvem os problemas em termos gerais. Algumas destas questões permanecem devido ao uso de classes mesmo com as sub-redes.

O problema central da rede "Classful" é a baixa "granularidade". Um bloco de endereço de classe B contém 65.534 endereços de hosts, mas um bloco Classe C tem um número relativamente pequeno 254. Há milhares de organizações "médias" que precisam de mais de 254 endereços IP, mas uma pequena percentagem destas precisa de 65.534 endereços ou próximo desse número. Ao criar suas redes, estas empresas tendem a solicitar blocos de endereços classe B e não blocos classe C, porque precisam mais de 254.

A solução obtida foi com a criação do VLSM – Variable Length Sub Mask, ou seja, máscara de tamanho variável. O objetivo principal da criação foi economizar o uso do IPv4. Vimos que os endereços IP são projetados para serem divididos em um identificador de rede e um identificador de host. Ao introduzir o conceito de sub-rede foram introduzidos alguns bits “roubados" da identificação do host para criar uma ID de sub-rede, dando o endereço IP de um total de três níveis hierárquicos. Com VLSM, nós são divididos em redes e em sub-rede, tendo mais bits a partir da identificação de host para nos dar uma hierarquia de nível múltiplo com "sub-sub-redes", "sub-sub-sub-redes" e assim por diante.

Existem dois critérios para a aplicação do VLSM para a divisão de uma rede em sub-redes:

1) RFC-950, com Nº SR = 2^n - 2 e Nº Hosts = 2^n - 2;

2) RFC-1812, com Nº SR = 2^n e Nº Hosts = 2^n - 2.

O RFC 950 é o menos econômico dos dois. Ele despreza a 1ª sub-rede, por ter o identificador dessa faixa (IP da 1ª sub-rede) coincidente com o identificador da rede mãe e a última sub-rede pelo fato desta ter o mesmo IP broadcast da rede mãe. Já o RCF-1812, mais recente, não despreza sub-rede alguma. A diferenciação é feita por meio da máscara atribuída às sub-redes.

Se a divisão da rede em sub-redes for feita em função do número de usuários em cada sub-rede, então a fórmula é idêntica para os dois RFCs: Nº Hosts = 2n – 2.

A situação particular de cada cenário é que definirá o emprego de cada uma das fórmulas citadas.

UNIDADE 2 – IPV4, IPV6, VLSM E CID

MÓDULO 3 – REDES VLSM – VARIABLE LENGTH SUBNET MASK

01

1 - CONCEITOS DE VLSM

VLSM - Variable Lenght Subnet Mask é um método de cálculo de sub-redes mais eficiente que o tradicional, você pode alocar somente os bits necessários da sub-rede utilizando máscaras de tamanho variáveis.

No cálculo de sub-redes tradicional é utilizada uma máscara de sub-rede única para todos os blocos, o que não é muito eficiente quando se tem uma topologia de rede com uma quantidade variável de hosts por sub-rede.

Em redes que utilizam VLSMs é necessário implementar protocolos de roteamento classless como o RIPv2, EIGRP, OSPF, IS-IS e BGP pois é preciso que a máscara de sub-rede seja encaminhada nas atualizações de roteamento, já que a mesma varia a cada bloco.

Protocolos de roteamento como RIPv1 e IGRP já não suportam redes com VLSMs, pois são classful e não encaminham a máscara de sub-rede nas atualizações.

02

1.2 - Vantagens da utilização do VLSM

São três as vantagens da utilização do VLSMs:

a) Menos desperdício de endereços IPs	b) Maior flexibilidade na distribuição de endereços	c) Possibilidade de sumarização de rotas (agregação de rotas)
•É possível fazer uso mais eficiente da divisão de sub-redes alocando mascaras de sub-redes diferentes a cada bloco.	•É possível redimensionar sub-redes dentro de uma sub-rede calculada. Quando houver uma alteração na topologia da rede não é necessário alterar o endereçamento de toda a rede.	•É possível você sumarizar diversas rotas em um único endereço de rede com máscara específica, diminuindo assim o tamanho das tabelas de roteamento.

03

1.3 - Aplicação do VLSM

Inicialmente abordaremos somente a primeira vantagem "Menos desperdício de endereços IPs", por meio de dois exemplos simples.

> Para fazer uso de VLSM é preciso que você tenha conhecimento pleno das sub-redes.

Para a aplicação do VLSM temos dois **critérios**:

a) Critério preconizado pelo RFC-950

nº SR = 2^n – 2, onde n é o nº de bits necessários para designar a quantidade de sub-redes necessárias. O "menos 2" significa que a 1ª sub-rede é desprezada por ter o ID coincidente com o ID da rede mãe e a última sub-rede tem o mesmo broadcast da rede mãe. Portanto, duas sub-redes são desprezadas.

nº Host = 2^n -2, onde n é o nº de bits necessários para designar os hosts de cada sub-rede. O "menos 2" significa que o 1º IP nomeia a sub-rede e o último IP é o broadcast da faixa considerada. Portanto, dois números IPs são desconsiderados para nomeação dos hosts.

b) Critério preconizado pelo RFC-1812

nº SR = 2^n, onde n é o nº de bits necessários para representar as sub-redes necessárias. Aqui não tem o "menos dois", pois a diferenciação das faixas de redes será feita por meio das máscaras das sub-redes originárias da rede mãe.

nº Host = 2^n -2, onde n é o nº de bits necessários para designar os hosts de cada sub-rede. O "menos 2" significa que o 1º IP nomeia a sub-rede e o último IP é o broadcast da faixa considerada. Portanto, dois números IPs são desconsiderados para nomeação dos hosts.

04

2 - Cálculo de VLSM

Dividir a seguinte rede classe C: 193.45.32.0/255.255.255.0 em, pelo menos, 10 sub-redes, conforme preconizado pelo RFC-950. Determinar o seguinte:

a) Quantos bits serão necessários para fazer a divisão e obter pelo menos 10 sub-redes?
b) Quantos números IP (hosts) estarão disponíveis em cada sub-rede?
c) Qual a nova máscara de sub-rede?
d) Listar a faixa de endereços de cada sub-rede.

Solução

a) Número de bits necessários para fazer a divisão em 10 sub-redes.

Conforme o RFC-950, nº SR => **10 = 2^n-2 → 12 = 2^n**

Para n=2, a fórmula resulta em 4;

Para n=3, a fórmula resulta em 8;

Para n=4 a fórmula resulta em 16.

Logo, quantos bits serão necessários para fazer a divisão e obter pelo menos 10 sub-redes? Resposta: 4 bits, pois 3 bits nos fornece somente 8 SR e precisamos de 12.

b) Quantos números IP (hosts) estarão disponíveis em cada sub-rede?
Pela máscara: 255.255.255.11110000, temos que foram utilizados quatro bits do último octeto (além dos 24 bits dos três primeiros octetos, os quais já faziam parte da máscara original), sobraram apenas 4 bits para os endereços IP, ou seja, para os endereços de hosts em cada sub-rede. Lembre-se da fórmula: **nº Hosts = 2^n-2**

Logo, substituindo n por 4, vou obter um valor de 14. Com isso, já estou em condições de responder questão b, ou seja, 14 hosts estarão disponíveis em cada sub-rede.

05

c) Qual a nova máscara de sub-rede?

255.255.255.0 → 255.255.255.11110000, portanto:

128+64+32+16 = 240. Com os quatro primeiros bits do quarto octeto sendo iguais a 1, o valor do quarto octeto passa para 240, com isso já temos condições de responder a questão c. Lembrar que esta será a máscara de sub-rede utilizada por todas as 16 sub-redes.

Logo, a nova máscara de sub-rede é 255.255.255.240

d) Listar a faixa de endereços de cada sub-rede.

Ao listar as faixas, consideramos os 16 hosts, apenas é importante salientar que o primeiro (ID da sub-rede) e o último (broadcast) não são utilizados para designar conexões (hosts). Com isso a primeira sub-rede vai do host 0 até o 15, a segunda sub-rede do 16 até o 31, a terceira do 32 até o 47 e assim por diante, conforme indicado no esquema da tabela a seguir:

Listagem das sub-redes obtidas no cálculo

ID SR	1º IP válido	Último IP válido	Broadcast

193.45.32.0	193.45.32.1	193.45.32.14	193.45.32.15
193.45.32.16	193.45.32.17	193.45.32.30	193.45.32.31
193.45.32.32	193.45.32.33	193.45.32.46	193.45.32.47
193.45.32.48	193.45.32.49	193.45.32.62	193.45.32.63
193.45.32.64	193.45.32.65	193.45.32.78	193.45.32.79
.....	.....	.....	.....
193.45.32.240	193.45.32.241	193.45.32.254	193.45.32.255

Conforme preconiza o RFC-950 a faixa do ID 193.45.32.0 e a faixa do ID 193.45.32.240 não são utilizadas, pois a 1ª faixa de sub-rede possui o mesmo ID da rede mãe e a última faixa possui o mesmo broadcast da rede mãe.

A RFC-950 determina que não pode haver apenas 1 bit para definição de sub-redes, uma vez que esse bit teria de estar sempre "ligado" ou "desligado", o que seria "ilegal".

06

Vamos a outro exemplo. Dividir a rede classe B: 150.100.0.0/255.255.0.0 em, pelo menos, 20 sub-redes, conforme o que preconiza o RFC-950. Determinar:

a) Quantos bits serão necessários para fazer a divisão e obter pelo menos 20 sub-redes?
b) Quantos números IP (hosts) estarão disponíveis em cada sub-rede?
c) Qual a nova máscara de sub-rede?
d) Listar a faixa de endereços de cada sub-rede.

Solução:

a) Fórmula → **nº SR = 2^n-2**, portanto: 20 = 2^n-2 → 22 = 2^n. Para n=2, a fórmula resulta em 4. Para n=3, a fórmula resulta em 8. Para n=4 a fórmula resulta em 16. Para n=5 a fórmula resulta em 32.

Se utilizarmos apenas 4 bits, obteremos somente 16 sub-redes e precisamos de pelo menos 20. Com 5 bits, obteremos um número de sub-redes bem maior do que o necessário, mas fazer o quê? Não podemos pegar fração de bits.

Resposta: 5 bits.

Logo, são necessários 5 bits para fazer a divisão e obter pelo menos 20 sub-redes.

b) Quantos números IP (hosts) estarão disponíveis em cada sub-rede?

150.100.0.0/255.255.0.0, logo temos a máscara: 255.255.11111000.00000000

Sobraram apenas 11 bits (os três restantes do terceiro octeto mais os 8 bits do quarto octeto) para os endereços IP para hosts em cada sub-rede.

Nº Host = 2^n-2. Substituindo n por 11 (número de bits que restaram para a parte de host), obtém-se o valor de 2048, descontados o 1º IP (ID da 1ª faixa) e o último IP (broadcast), temos: 2046.

Resposta: 2046.

Logo, 2046 IP (hosts) estarão disponíveis em cada sub-rede.

07

c) Qual a nova máscara de sub-rede?

255.255.11111000.00000000 -> basta somar os respectivos valores, ou seja: 128+64+32+16+8 = 248. Com os cinco primeiros bits do terceiro octeto sendo iguais a 1, o valor do terceiro octeto passa para 248, com isso já temos condições de responder a alternativa c. É importante lembrar, mais uma vez, que esta será a máscara de sub-rede utilizada por todas as 32 sub-redes.

Resposta: 255.255.248.0.

Logo, a nova máscara de sub-rede é 255.255.248.0.

d) Listar a faixa de endereços de cada sub-rede.

Qual o valor decimal do quinto bit (de qualquer octeto), ou seja, o bit menos significativo (LSB-Least Significant Bit)? É igual a 8 (o primeiro é 128, o segundo 64, o terceiro 32, o quarto é 16 e o quinto é 8). O valor do último bit é um indicativo das faixas de variação para este exemplo. Ou seja, na prática temos 2048 hosts em cada sub-rede, embora o primeiro e o último não devam ser utilizados, pois o primeiro é o endereço da própria sub-rede e o último é o endereço de broadcast da sub-rede. Por isso que ficam 2046 hosts por sub-rede, devido ao '-2' na fórmula, o '-2' significa: menos o primeiro e menos o último. Ao listar as faixas, consideramos o valor do último bit da máscara. No nosso exemplo é o 8. A primeira faixa vai do zero até um número anterior ao valor do último bit, no caso do 0 a 7.

Importante: Observe que os valores de 0 a 7 são definidos no terceiro octeto, que é onde estamos utilizando cinco bits a mais para fazer a divisão em sub-redes.

08

Dando continuidade à solução do item d, qual seria a faixa de endereços IP da próxima sub-rede? Se a primeira foi de 0 até 7, a segunda sub-rede terá valores de 8 a 15 no terceiro octeto, a terceira sub-rede terá valores de 16 a 23 e assim por diante.

Pelo RFC-950, na divisão da rede em 32 sub-redes, onde cada sub-rede fica com 2048 endereços IP, a primeira e a última sub-rede não são utilizadas e o primeiro e o último número IP, dentro de cada sub-rede (ID da SR e o Broadcast), também não são utilizados conforme tabela a seguir.

Listagem das sub-redes obtidas no cálculo.

Nº	ID SR	1º IP válido	Último IP válido	Broadcast
1	150.100.0.0	150.100.0.1	150.100.7.254	150.100.7.255
2	150.100.8.8	150.100.8.1	150.100.15.254	150.100.15.255
3	150.100.16.0	150.100.16.1	150.100.23.254	150.100.23.255
4	150.100.24.0	150.100.24.1	150.100.31.254	150.100.31.255
5	150.100.32.0	150.100.32.1	150.100.39.254	150.100.39.255
6	150.100.40.0	150.100.40.1	150.100.47.254	150.100.47.255
7	150.100.48.0	150.100.48.1	150.100.63.254	150.100.63.255
8	150.100.64.0	150.100.64.1	150.100.71.254	150.100.71.255
....	.....	.....	.....	.....
17	150.100.128.0	150.100.128.1	150.100.135.254	150.100.135.255
.....	.....	.....	.....	.....
32	150.100.248.0	150.100.248.1	150.100.255.254	150.100.255.255

Fonte: O Autor, 2015.

Com base na tabela apresentada, é fácil responder qual sub-rede contém um determinado número IP. Por exemplo, considere o número IP 150.100.130.222. Primeiro você observa o terceiro octeto do número IP (terceiro, porque é neste octeto que estão os últimos bits que foram utilizados para a máscara de sub-rede). Consultando a tabela anterior, você observa o valor de 130 para o terceiro octeto corresponde a sub-rede 17, na qual o terceiro octeto varia entre 128 e 135, conforme tabela acima.

09

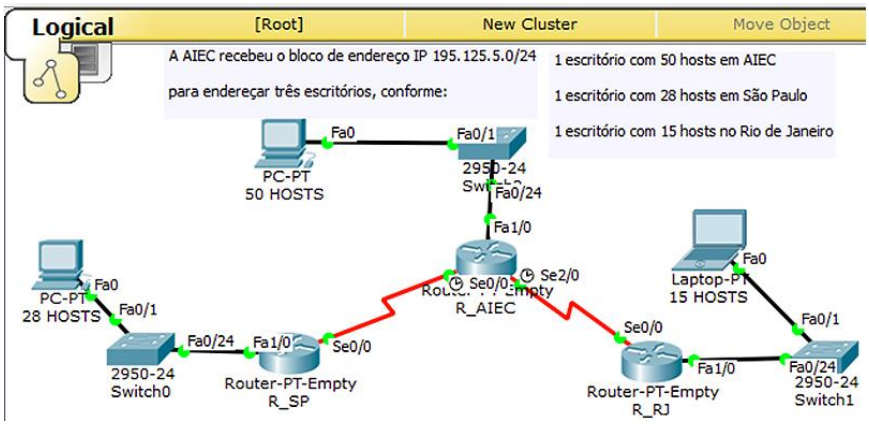
3 - Emprego do VLSM

Para fixarmos o conceito de VLSM, um exemplo prático. Suponha que você trabalhe como administrador de rede em uma empresa que tenha recebido o bloco de endereço IP 195.125.5.0/24 para meta é endereçar três escritórios, conforme abaixo.

1 escritório com 50 hosts na AIEC

1 escritório com 28 hosts em São Paulo

1 escritório com 15 hosts no Rio de Janeiro



Cenário do estudo de caso.
Fonte: O Autor, 2015.

Tente solucionar este problema e, depois, verifique se você acertou. A solução pode ser conferida a seguir.

10

Solução:

Cálculo das faixas de endereços para cada escritório.

Veja que nos dois exemplos anteriores começamos por calcular pelo nº de sub-redes necessário. Aqui vamos calcular pelo nº de hosts de cada sub-rede.

a) Inicie pela AIEC, por ser o maior.

Dica: como precisamos de 50 hosts, temos que utilizar 6 bits para hosts (2^6=64 > 50). Veja a solução

b) Procedimento para São Paulo, com 28 hosts.

Dica: precisamos de 28 hosts (2^5=32 > 28). Veja a solução

c) Procedimento para o Rio de Janeiro onde teremos 15 hosts.

Dica: 5 bits para hosts (2^5=32 > 15) e 3 bits para rede. Como já utilizamos a rede 195.125.5.64/27 para São Paulo, utilizaremos a próxima para o Rio de Janeiro, ficando para o Rio de Janeiro:

195.125.5.96/27. Veja a solução

a) Escritório com 50 hosts na AIEC

Como precisamos de 50 hosts, temos que utilizar 6 bits para hosts (2^6=64 > 50). Utilizando 6 bits para hosts temos 2 bits para sub-rede, ou seja, teremos: 255.255.255.11000000 → uma máscara /26. Neste caso o LSB tem valor decimal igual a 64, logo as sub-redes variarão de 64 em 64 no último octeto. Então: 195.125.5.0 –> 195.125.5.1 (1º IP) – 195.125.5.62 (último IP) – 195.125.5.63 (broadcast).

Variação das sub-redes:
192.125.5.0
192.125.5.64
192.125.5.128
192.125.5.192
Como tínhamos 2 bits para sub-redes, eles proporcionam somente 4 redes.

AIEC:
195.125.5.0/26 onde,
Endereço de rede é 195.125.5.0
Endereço de broadcast é 195.125.5.63
Endereço de hosts 195.125.5.1 a 195.125.5.62

b) Escritório com 28 hosts em São Paulo

Precisamos de 28 hosts (2^5=32 > 28). Utilizamos 5 bits para hosts e 3 para rede, ficando uma máscara /27. Vamos pegar a próxima sub-rede das que sobraram, ou seja, 195.125.5.64 e transformá-la em /27 = 255.255.255.11100000 → variação de 32 em 32.
192.125.5.64 → para São Paulo.
192.125.5.96
192.125.5.128.
Logo temos para São Paulo:
195.125.5.64 → 195.125.5.65 – 192.125.5.94 – 195.125.5.95 onde,
Endereço de rede é 195.125.5.64
Endereço de broadcast é 195.125.5.95
Endereço de hosts 195.125.5.65 a 195.125.5.94

c) escritório com 15 hosts no Rio de Janeiro

Endereço de rede é 195.125.5.96
Endereço de broadcast é 195.125.5.127
Endereço de hosts 195.125.5.97 a 195.125.5.126
Pronto. O cálculo das sub-redes para a LAN de cada escritório está terminado. Há uma questão, em nossa topologia exemplo estamos utilizando enlaces seriais, precisaremos também de sub-redes para endereçar os links ponto-a-ponto entre as unidades, pois requerem somente dois IPs.

Vamos calcular os endereços do enlace entre AIEC-São Paulo. Precisamos apenas de 2 endereços de hosts (um para cada interface serial de cada roteador). Logo, 2 bits para hosts é o suficiente e ficamos uma máscara /30, ficando da seguinte forma:

Enlace AIEC-São Paulo pega-se a rede seguinte (sub-rede utilizada é desprezada), ou seja, a 195.125.5.128/27.

255.255.255.11111100 → 255.255.255.252, ou seja:
192.125.5.128
192.125.5.132
192.125.5.136
.....
192.125.5.252

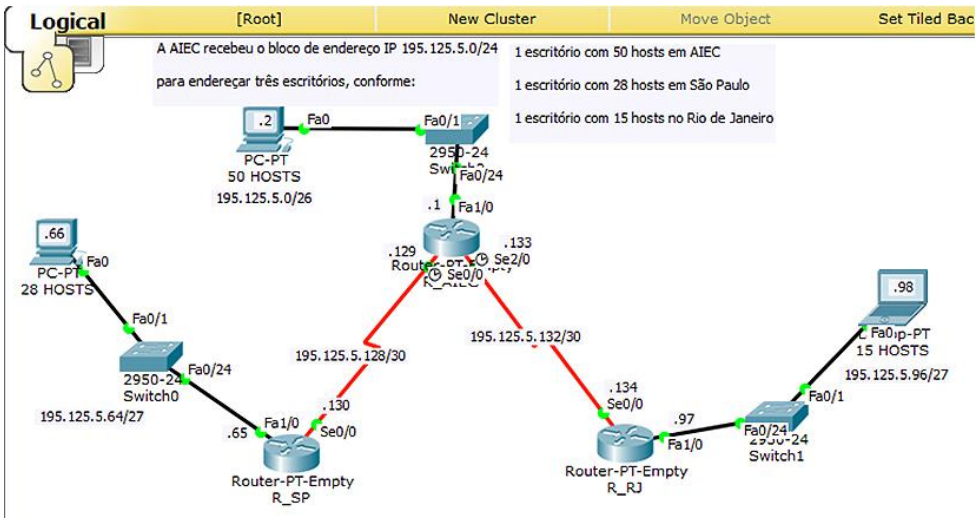
Adotamos para esse enlace a 1ª faixa: 195.125.5.128/30, onde:
Endereço de rede é 195.125.5.128
Endereço de broadcast é 195.125.5.131
Endereço de hosts 195.125.5.129 e 195.125.5.130

Idem para o enlace AIEC-Rio de Janeiro. Será utilizada uma máscara /30.
Enlace AIEC-Rio de Janeiro
195.125.5.132/30, onde:
Endereço de rede é 195.125.5.132
Endereço de broadcast é 195.125.5.135
Endereço de hosts 195.125.5.133 e 195.125.5.134.

11

Terminamos o nosso planejamento do esquema de endereçamento. Perceba que a partir de um bloco contínuo de endereços classe C padrão (195.125.5.0) conseguiu-se fazer a divisão em blocos de endereços variáveis, com a utilização mais econômica dos endereços IP.

Isso ocorreu graças ao conceito de VLSM. Veja abaixo a figura completa, com os endereços calculados.



Cenário do Estudo de Caso com o plano de endereçamento IPv4.
Fonte: O Autor, 2015.

12

RESUMO

VLSM - Variable Lenght Subnet Mask é um método de cálculo de sub-redes mais eficiente que o tradicional, você pode alocar somente os bits necessários da sub-rede utilizando máscaras de tamanho variáveis.

No cálculo de sub-redes tradicional é utilizada uma máscara de sub-rede única para todos os blocos, o que não é muito eficiente quando se tem uma topologia de rede com uma quantidade variável de hosts por sub-rede.

As vantagens da utilização do VLSM são:

a) Menos desperdício de endereços IPs: é possível fazer uso mais eficiente da divisão de sub-redes alocando mascaras de sub-redes diferentes a cada bloco;

b) Maior flexibilidade na distribuição de endereços: é possível redimensionar sub-redes dentro de uma sub-rede calculada. Quando houver uma alteração na topologia da rede não é necessário alterar o endereçamento de toda a rede;

c) Possibilidade de sumarização de rotas (agregação de rotas).

É possível você sumarizar diversas rotas em um único endereço de rede com máscara específica, diminuindo assim o tamanho das tabelas de roteamento.

MÓDULO 4 – REDES CIDR – CLASSLESS INTER-DOMAIN ROUTING.

01

1 - CONCEITO DO CIDR

Como o nome indica, CIDR - Classless Inter-Domain Routing, são redes sem classes que eliminam completamente as noções anteriores de classes.

Vale fazermos um pequeno resumo para lembrarmos como surgiu o CIDR: a divisão tradicional, com as classes A, B e C de endereços IP fazia com que um grande número de endereços fossem desperdiçados. Um provedor de acesso que precisasse de 10.000 endereços IP, por exemplo, precisaria utilizar uma faixa de endereços classe B inteira (65 mil endereços), o que geraria um grande desperdício, ou utilizar 40 faixas de endereços classe C separadas, o que complicaria a configuração. Existia ainda o problema com as faixas de endereços classe A, que geravam um brutal desperdício de endereços, já que nenhuma empresa ou organização sozinha chega a utilizar 16 milhões de endereços IP. A solução para o problema foi a implantação do sistema CIDR - Classless Inter-Domain Routing.

Com o CIDR, não há mais as classe A, B e C, as quais eram divididas e identificadas pelos primeiros bits do endereço. Em vez disso, todos os blocos de Internet podem ser de tamanho arbitrário. Em vez de termos todas as redes usando 8 (Classe A), 16 (Classe B) ou 24 (Classe C) bits para a identificação de rede, podemos ter grandes redes com, digamos, 13 bits para a identificação de rede (deixando 19 bits para o ID acolhimento), ou muito pequenas que utilizam 28 bits para a identificação de rede (apenas 4 bits para a identificação de host). O tamanho da rede ainda se baseia no poder de binário o número de bits de ID do hospedeiro, do curso.

02

Basicamente, o conceito por trás do padrão de endereçamento CIDR é o contrário da proposta das sub-redes (VLSM). Enquanto nessa última movemos os bits de hosts (“0s”) para criar um número maior de redes, com CIDR a ideia básica é **sumarizar** diversas redes em apenas uma, movendo-se a porção de rede (“1s”) da máscara original. Esse processo é conhecido como **supernetting** ou prefix routing.

Lembre-se de que, ao usarmos sub-redes, há um problema: a sub-rede pode ser feita através de qualquer número de bits da identificação do host disponível, assim, como seria possível saber onde é o limite entre a ID de sub-rede e ID de acolhimento? O mesmo problema ocorre em CIDR.

No CIDR, como o ponto de divisão entre ID anfitrião e ID de rede podem ocorrer em qualquer lugar, precisamos de informações adicionais, a fim de interpretar endereços IP corretamente. De acordo com CIDR, é claro, isso afeta não apenas os endereços dentro de uma organização, mas em toda a Internet, uma vez que não há padrão e cada rede pode de ser um tamanho diferente.

O CIDR usa o prefixo de rede, em vez dos três primeiros bits do endereço IP, para determinar o ponto de divisão entre o NetID e o HostID, daí o nome “prefix routing”. O prefixo é a maneira de se especificar o número de bits contíguos mais à esquerda na porção “rede” de cada entrada na tabela de roteamento.

03

2 - Funcionamento do CIDR

O CIDR - Classless Inter-Domain Routing foi introduzido em 1993 (RFC 1517), substituindo a geração anterior de sintaxe de endereço IP - redes classful. CIDR permitiu um uso mais eficiente do espaço de endereços IPv4 e agregação de prefixo, conhecida como **sumarização de rotas** ou **supernet**.

Essa foi a técnica encontrada para combater o desperdício de endereços. Agora não importa a classe para se determinar o número de endereços necessários, importa sim a quantidade necessária.

O CIDR trabalha da direita para a esquerda e o VLSM da esquerda para a direita.

O CIDR tem como objetivo:
1- Uso mais eficiente do espaço de endereços IPv4;
2- Prefixo de agregação, o que reduziu o tamanho das tabelas de encaminhamento.

O CIDR permite que os roteadores agrupem rotas para reduzir o volume de informações de roteamento realizado pelos roteadores.

Os endereços IP e as máscaras de sub-rede são escritos com quatro octetos, separados por pontos, seguido por uma barra e um número de dois dígitos que representa a máscara de sub-rede, por exemplo:

10.1.1.0/30

172.16.1.16/28

192.168.1.32/27

CIDR / VLSM Rede:

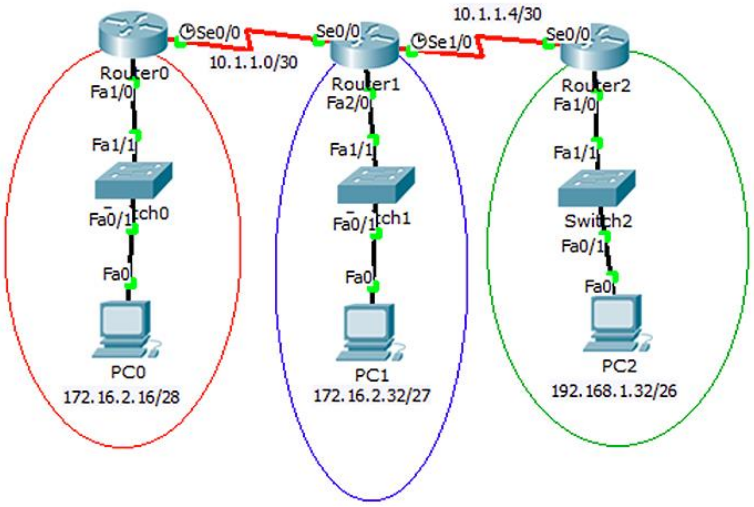


Figura 4.1: Cenário do Estudo de caso.
Fonte: O Autor, 2015.

octeto
Octeto é o conjunto de quatro números, uma vez que eles na verdade representam um número binário de 8 bits ou 1 byte. Consequentemente, o valor decimal máximo para cada um dos quatro números em um endereço IP é 255 e não 999.

04

Com o CIDR, classes de endereços (Classe A, B, e C) tornaram-se sem sentido. O endereço de rede não é mais determinado pelo valor do primeiro octeto, mas atribuído pela máscara de sub-rede. O número de hosts em uma rede pode, agora, ser atribuído por um prefixo específico, dependendo do número de servidores necessários para essa rede. Em suma, as faixas de endereços não precisam mais iniciar com determinados números. Uma faixa com máscara /24 (equivalente a uma faixa de endereços de classe C) pode começar com qualquer dígito e não apenas com de 192 a 223.

CIDR usa VLSM (Variable Length Sub Mask – máscaras de tamanho variável) para alocar endereços IP para sub-redes de acordo com a necessidade, em vez de uma classe, o que permite uma flexibilidade muito maior na criação das faixas de endereços. Como já visto, VLSM permite dividir em sub-redes e por sua vez dividir novamente.

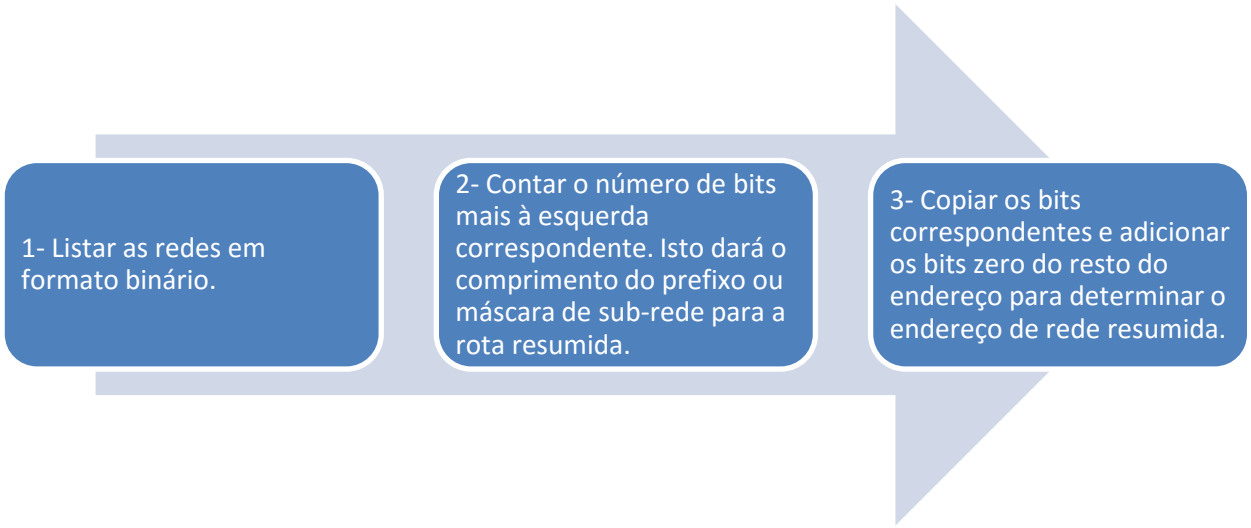
Se são necessários apenas 1000 endereços, por exemplo, poderia ser usada uma máscara /22 (que permite o uso de 1022 endereços), em vez de uma faixa de classe B inteira, como seria necessário antigamente.

Propagar supernets CIDR ou sub-redes VLSM requer um protocolo de roteamento sem classes. Um protocolo de roteamento sem classes inclui a máscara de sub-rede, juntamente com o endereço de rede na atualização de roteamento.

05

Resumo da determinação de rotas

A determinação do resumo do percurso e a máscara de sub-rede, para um grupo de redes, pode ser feita em três passos:



O endereço resumido de rede e máscara de sub-rede pode agora ser usado como rota de síntese para este grupo de redes. Rotas sumarizadas podem ser usadas tanto por rotas estáticas quanto por protocolos de roteamento sem classes. Os protocolos de roteamento classful só podem resumir rotas para a máscara classful padrão.

As máscaras de sub-redes limitadas a 255.0.0.0 ou **/8;** 255.255.0.0 ou **/16** e 255.255.255.0 ou **/24**, que antes do advento do CIDR eram conhecidas como endereços de rede classful agora não mais existem.

Uma grande **vantagem** do CIDR é que, com a introdução do CIDR e VLSM, os ISP (Internet Service Provider) podem atribuir uma parte de uma rede classful para um cliente e uma parte diferente para outro cliente.

06

Resumo

As redes CIDR - Classless Interdomain Routing, como o nome indica, são redes sem classes que eliminam completamente as noções anteriores de classes. Não há mais classe A, B e C, as quais eram divididas e identificadas pelos primeiros bits do endereço. Em vez disso, todos os blocos de Internet podem ser de tamanho arbitrário. Em vez de termos todas as redes usando 8 (Classe A), 16 (Classe B) ou 24 (Classe C) bits para a identificação de rede, podemos ter grandes redes com, digamos, 13 bits para a identificação de rede (deixando 19 bits para o ID acolhimento), ou muito pequenas que utilizam 28 bits para a identificação de rede (apenas 4 bits para a identificação de host).

Basicamente, o conceito por trás deste padrão de endereçamento é o contrário da proposta das sub-redes (VLSM). Enquanto nessa última movemos os bits de hosts (“0s”) para criar um número maior de redes, com CIDR a ideia básica é sumarizar diversas redes em apenas uma, movendo-se a porção de rede (“1s”) da máscara original. Esse processo é conhecido como “supernetting” ou “prefix routing”.

O CIDR foi introduzido em 1993 (RFC 1517), substituindo a geração anterior de sintaxe de endereço IP - redes classful. CIDR permitiu um uso mais eficiente do espaço de endereços IPv4 e agregação de prefixo, conhecida como sumarização de rotas ou supernet.

O CIDR trabalha da direita para a esquerda e o VLSM da esquerda para a direita**.**

Técnica encontrada para se combater o desperdício de endereços. Não importa a classe para se determinar o número de endereços necessários. Importa sim a *quantidade* necessária*.*

Com a introdução do CIDR e VLSM, os ISPs podem atribuir uma parte de uma rede classful para um cliente e uma parte diferente para outro cliente.