COLÉGIO ESTADUAL PROTÁSSIO ALVES
Curso Técnico Em Informática / Internet
Professor:Antônio Guimarães Neto

FUNDAMENTOS**D**E **R**EDES **E** **C**ONECTIVIDADE

Redes De Computadores I

MÓDULO 8 - ENDEREÇO IP

-2018-

Módulo 8 - Endereço IP

8.1 Conceito

Quando você deseja enviar uma carta a alguém... Ok, você não envia mais cartas; prefere WhatsApp ou deixar recado no Facebook. Vamos então melhorar o exemplo: quando você quer enviar um presente a alguém, basta contratar os Corrreios ou uma transportadora para fazer a entrega no endereço informado.Graças ao endereço, é possível encontrar exatamente a pessoa a ser presenteada. Também é graças ao seu endereço — único para cada residência ou estabelecimento — que você recebe contas de energia, boletos, aquele produto que você comprou em uma loja on-line, enfim.Na internet, o princípio é parecido. Para que seja encontrado, o seu computador precisa ter um endereço único. O mesmo vale para qualquer site, como o InfoWester: este fica hospedado em um servidor, que por sua vez precisa ter um endereço para ser localizado na internet. Isso é feito via endereço IP (*IP Address*), recurso também utilizado para redes locais, como a rede Wi-Fi da sua casa: o seu roteador atribui um IP a cada dispositivo conectado a ele.

O endereço IP é uma sequência de números composta por 32 bits. Esse valor consiste em um conjunto de quatro sequências de 8 bits. Cada uma é separada por um ponto e recebe o nome de octeto ou simplesmente byte, pois um byte é formado por 8 bits. O número 172.31.110.10 é um exemplo. Repare que cada octeto é formado por números que podem ir de 0 a 255, não mais do que isso.

A divisão de um IP em quatro partes facilita a organização da rede, da mesma forma que a divisão do seu endereço em cidade, bairro, CEP, número, etc, torna possível a organização das casas da região onde você mora.Nesse sentido, os dois primeiros octetos de um endereço IP podem ser usados para identificar a rede, por exemplo. Em uma escola que tem, vamos imaginar, uma rede para alunos e outra para professores, pode-se ter 172.31.x.x para a primeira rede e 172.32.x.x para a segunda, sendo que os dois últimos octetos são utilizados na identificação dos computadores.

8.2 Ip Estático x dinâmico

IP dinâmico

O IP dinâmico é o mais comum e se refere, principalmente, a um endereço que muda sempre, normalmente quando você liga o modem, ou em intervalos de tempo definidos pelo provedor. É o padrão ideal para uso doméstico, já que não requer equipamentos de melhor performance e não depende de conhecimentos um pouco mais avançados para configuração e manutenção.

Além disso, há um outro fator envolvido no IP dinâmico. Como o endereço é passível de mudança o tempo todo, é preciso que sua rede negocie o uso de um IP. Isso é feito por meio de um protocolo chamado DHCP. Ele funciona em segundo plano e permite que seu computador negocie e obtenha um endereço de IP dinâmico quando necessário.

IP fixos (Estáticos)

O IP fixo é mais raro e, em alguns casos, sua oferta pelo provedor está vinculada a taxas adicionais. Como é possível deduzir a partir da explicação sobre o dinâmico, o código fixo é um endereço de IP imutável. Ou seja, seu computador sempre terá o mesmo endereço, desde que conectado à rede com o fixo (se você levar o laptop para uma viagem e conectar de outro lugar, ele terá um IP diferente).

8.3 Endereços Físicos e Endereços Lógicos

Endereços físicos

O **endereço MAC** (*Media Access Control*) é definido como sendo um endereço físico de uma placa de rede, e é composto por 48 bits (12 caracteres hexadecimais). Os primeiros seis caracteres identificam o fabricante (ex. Intel, surecom, broadcom, etc) e os restantes seis identificam a placa em si. O endereço MAC é único no mundo para cada placa de rede (apesar de existirem ferramentas que possibilitam a alteração do mesmo), e é mantido na memória ROM , sendo posteriormente essa informação copiada para a memória RAM aquando da inicialização da placa. Há várias formas de representar um endereço MAC:

Endereços lógicos

Quando falamos em endereços na área das redes, é normal associarmos de imediato ao endereço IP configurado numa placa de rede. O endereço IP (versão 4) é um endereço lógico definido por 32 bits (4 octetos) e identifica um dispositivo numa determinada rede. Os endereços lógicos IPv6 são constituídos por 128 bits, sendo apresentados em 8 grupos de 4 dígitos hexadecimais (por ex1234:5678:90AB:CDEF:FEDC:BA09:8765:4321)

Mas qual é a vantagem desse modelo? O IP fixo é ideal para usuários que precisam ter absoluta certeza sobre o endereço de sua rede na Internet. Suponha que você tenha um servidor para sua empresa, ou precise criar um tipo de nuvem pessoal para arquivos, cujo acesso se dá via FTP: nesse caso, fixar o IP da rede é fundamental, já que você terá acesso a esses recursos sempre, bastando para isso acessá-los diretamente pelo número de IP fixo atribuído pelo seu provedor.

8.4 Ipv4 x Ipv6

O IPv4 (Internet ProtocolVersion 4) é o protocolo de Internet mais utilizado e é capaz de cobrir uma quantidade exponencial de dispositivos.O IPv4 possui uma estrutura de 32 bits, sob a forma xxx :xxx : xxx : xxx, sendo que cada grupo xxx pode variar entre 0 e 255. Isto significa que este protocolo pode abranger 2^32 dispositivos, algo que era perfeitamente aceitável há alguns anos atrás. Assim surgiu o IPv6 Para conseguir responder à procura cada vez maior de novos IPs, foi criado o IPv6, que permite abranger um número muitas vezes maior que o IPv4.Para evitar problemas de compatibilidade, o IPv6 foi criado com a mesma estrutura do IPv4, apenas com um endereço mais longo.Assim, o IPv6 agora permite endereços com 128 bits de comprimento, permitindo agora 2^128 combinações de endereços diferentes. A sua estrutura é similar à do IPv4sendo que agora é xxxx :xxxx : xxxx : xxxx : xxxx : xxxx : xxxx : xxxx, em que cada X corresponde a um número hexadecimal (4 bits).

IPV4	IPV6
Endereço de 32bits	Endereço de 128bits
Suporte opcional de IPSec	Suporte obrigatório de IPSec
Nenhuma referência a capacidade de QoS (*Qualityof Service)*	Introduz capacidades de QoS utilizando para isso o campo FlowLabel
Processo de fragmentação realizada pelo router	A fragmentação deixa de ser realizada pelos routers e passa a ser processada pelos *host* emissores
O cabeçalho inclui os campos de opção	Todos os campos de opção foram mudados para dentro do campo *extension header*
O *AdressResolutionProtocol*(ARP), utiliza requisitos do tipo *Broadcast*	O ARP foi abandonado, sendo substituídos pelas mensagens *Neibhbor Discovery*
Internet Resolution Management Protocol(IGMP) é utilizado para gerir relações locais de sub-redes	O IGMP fio substituído por mensagens *MultcastListner Discovery*
Os Endereços de *Broadcast* são utilizados para enviar tráfego para todos os *host* de uma rede	Deixa de existir o endereço de *Broadcast,* para utilizar endereços *multicast*
O endereço tem de ser configurado manualmente	Adição de funcionalidades de autoconfiguração
Suporta pacotes de 576 bytes, passiveis de serem fragmentados	Suporta pacotes de 1280 bytes, sem fragmentação

8.5 As classes do Ipv4

Você já sabe que os endereços IP podem ser utilizados tanto para identificar o seu computador ou celular (ou qualquer outro dispositvo) dentro de uma rede quanto para identificá-lo na internet.Se na rede do trabalho o seu computador tem, como exemplo, o IP 172.31.100.10, uma máquina em outra rede pode ter o mesmo número, afinal, ambas as redes são distintas e não se comunicam — uma nem sabe da existência da outra.Mas, como a internet é uma rede global, cada dispositivo conectado nela precisa ter um endereço único. O mesmo vale para uma rede local: nesta, cada dispositivo conectado deve receber um endereço exclusivo. Se duas ou mais máquinas tiverem o mesmo IP, tem-se então um problema chamado "conflito de IP", que dificulta ou impede a comunicação desses dispositivos e pode inclusive atrapalhar toda a rede. Para que seja possível termos IPs para uso em redes locais e IPs para utilização na internet, contamos com um esquema de distribuição estabelecido pelas entidades IANA (*Internet AssignedNumbersAuthority*) e ICANN (*Internet Corporation for AssignedNamesandNumbers*) que, basicamente, divide os endereços em três classes principais e mais duas complementares. São elas:

Classe A: 0.0.0.0 até 127.255.255.255 — permite até 128 redes, cada uma com até 16.777.214 dispositivos conectados;

Classe B: 128.0.0.0 até 191.255.255.255 — permite até 16.384 redes, cada uma com até 65.536 dispositivos;

Classe C: 192.0.0.0 até 223.255.255.255 — permite até 2.097.152 redes, cada uma com até 254 dispositivos;

Classe D: 224.0.0.0 até 239.255.255.255 — *multicast*;

Classe E: 240.0.0.0 até 255.255.255.255 — *multicast reservado*

As três primeiras classes são assim divididas para atender às seguintes necessidades:
- Os endereços IP da classe A são usados em locais onde são necessárias poucas redes, mas uma grande quantidade de máquinas nelas. Para isso, o primeiro byte é utilizado como identificador da rede e os demais servem como identificador dos dispositivos conectados (notebooks, smartphones, impressoras, etc);

- Os IPs da classe B são usados nos casos em que a quantidade de redes é equivalente ou semelhante ao número de dispositivos. Para isso, usam-se os dois primeiros bytes do endereço IP para identificar a rede e os restantes para identificar os dispositivos;

- Os endereços IP da classe C são usados em locais que requerem grande quantidade de redes, mas com poucos dispositivos em cada uma. Assim, os três primeiros bytes são usados para identificar a rede e o último é utilizado para identificar as máquinas.

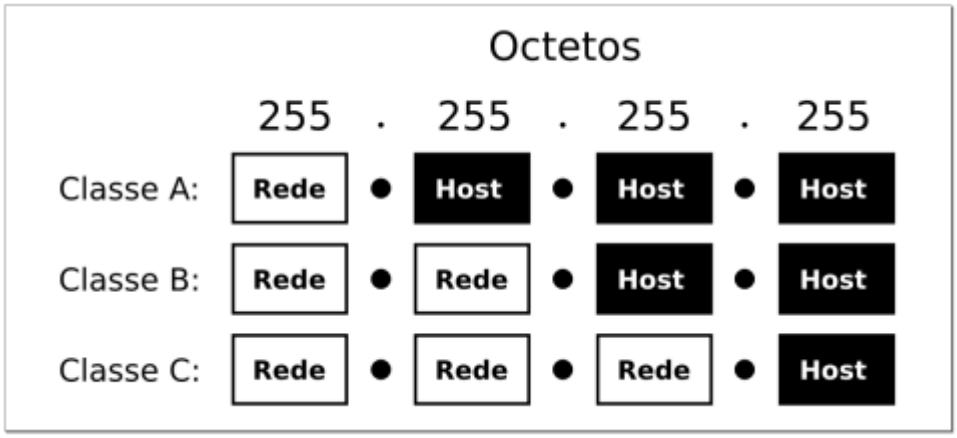
Endereços IP privados

-Há conjuntos de endereços das classes A, B e C que são privados. Isso significa que eles não podem ser usados na internet, pois foram reservados para aplicações locais. São, essencialmente, estes:

- Classe A: 10.0.0.0 à 10.255.255.255;
- **Classe B**: 172.16.0.0 à 172.31.255.255;
- **Classe C**: 192.168.0.0 à 192.168.255.255.

Suponha então que você tenha que gerenciar uma rede com cerca de 50 computadores. Você pode destinar a essas máquinas endereços de 192.168.0.1 até 192.168.0.50, por exemplo. Todas elas precisam de acesso à internet. O que fazer? Adicionar mais um IP para cada uma delas?Não. Na verdade, basta conectá-las a um servidor ou equipamento de rede — como um roteador Wi-Fi — que recebe a conexão à internet e a compartilha com todos os dispositivos conectados a ele. Com isso, somente este equipamento precisará de um endereço IP para acesso à internet.

Cada classe reserva um número diferente de octetos para o endereçamento da rede. Na classe A, apenas o primeiro octeto identifica a rede, na classe B são usados os dois primeiros octetos e na classe C temos os três primeiros octetos reservados para a rede e apenas o último reservado para a identificação dos hosts dentro dela.O que diferencia uma classe de endereços da outra é o valor do primeiro octeto. Se for um número entre 1 e 126 temos um endereço de classe A. Se o valor do primeiro octeto for um número entre 128 e 191, então temos um endereço de classe B e, finalmente, caso o primeiro octeto seja um número entre 192 e 223, temos um endereço de classe C.



Ao configurar uma rede local, você pode escolher a classe de endereços mais adequada. Para uma pequena rede, uma faixa de endereços de classe C (como a tradicional 192.168.0.x com máscara 255.255.255.0) é mais apropriada, pois você precisa se preocupar em configurar apenas o último octeto do endereço ao atribuir os endereços. Em uma rede de maior porte, com mais de 254 micros, passa a ser necessário usar um endereço de classe B (com máscara 255.255.0.0), onde podemos usar diferentes combinações de números nos dois últimos octetos, permitindo um total de 65.534 endereços.

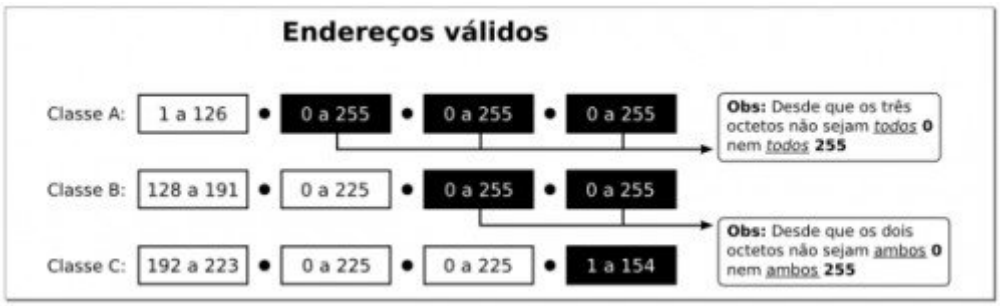
Continuando, temos a configuração das máscaras de sub-rede, que servem para indicar em que ponto termina a identificação da rede e começa a identificação do host. Ao usar a máscara "255.255.255.0", por exemplo, indicamos que os três primeiros números (ou octetos) do endereço servem para identificar a rede e apenas o último indica o endereço do host dentro dela.

Como vimos, na divisão original (que não é mais usada hoje em dia, como veremos a seguir) os endereços das três faixas eram diferenciados pelo número usado no primeiro octeto. Os endereços de classe A começavam com números de 1 a 126 (como, por exemplo, "62.34.32.1"), com máscara 255.0.0.0. Cada faixa de endereços classe A era composta de mais de 16 milhões de endereços mas, como existiam apenas 126 delas, elas eram reservadas para o uso de grandes empresas e órgãos governamentais.

Em seguida tínhamos os endereços de classe B, que englobavam os endereços iniciados com de 128 a 191, com máscara 255.255.0.0 (criando faixas compostas por 65 mil endereços) e o "terceiro mundo", que eram as faixas de endereços classe C. Elas abrangiam os endereços que começam com números de 192 a 223. As faixas de endereços de classe C eram mais numerosas, pois utilizavam máscara 255.255.255.0, mas, em compensação, cada faixa de classe C era composta por apenas 254 endereços. Veja alguns exemplos:

Ex. de endereço IP	Classe do endereço	Parte referente à rede	Parte referente ao host	Máscara de sub-rede padrão
98.158.201.128	Classe A	98.	158.201.128	255.0.0.0 (rede.host.host.host)
158.208.189.45	Classe B	158.208.	189.45	255.255.0.0 (rede.rede.host.host)
208.183.34.89	Classe C	208.183.34.	89	255.255.255.0 (rede.rede.rede.host)

Ao alugar um backbone vinculado a uma faixa de endereços classe C, por exemplo, você receberia uma faixa de endereços como "203.107.171.x", onde o "203.107.171" é o endereço de sua rede dentro da Internet, e o "x" é a faixa de 254 endereços que você pode usar para identificar seus servidores e os hosts dentro da rede. Na ilustração temos um resumo das regras para endereços TCP/IP válidos:



Como você pode notar no diagrama, nem todas as combinações de endereços são permitidas, pois o primeiro endereço (0) é reservado à identificação da rede, enquanto o último (255) é reservado ao endereço de broadcast, que é usado quando alguma estação precisa enviar um pacote simultaneamente para todos os micros dentro do segmento de rede.

Os pacotes de broadcast são usados para, por exemplo, configurar a rede via DHCP e localizar os compartilhamentos de arquivos dentro de uma rede Windows (usando o antigo protocolo NetBIOS). Mesmo os switches e hub-switches detectam os pacotes de broadcast e os transmitem simultaneamente para todas as portas. A desvantagem é que, se usados extensivamente, eles prejudicam o desempenho da rede.

8.6Endereços válidos x inválidos

Ip's Válidos: são ips que podem ser usados na rede:
Ip's Não Válidos: São ip's que não podem ser usados na redes ou setados em maquinas por ex:
Outro tipo de ip que não pode ser usados são os ip’s de redes!
Os ip's de redes variam de acordo com a mascara!

Como você pode notar no diagrama acima , nem todas as combinações de endereços são permitidas, pois o primeiro endereço (0) é reservado à identificação da rede, enquanto o último (255) é reservado ao endereço de broadcast, que é usado quando alguma estação precisa enviar um pacote simultaneamente para todos os micros dentro do segmento de rede.Os pacotes de broadcast são usados para, por exemplo, configurar a rede via DHCP e localizar os compartilhamentos de arquivos dentro de uma rede Windows (usando o antigo protocolo NetBIOS). Mesmo os switches e hub-switches detectam os pacotes de broadcast e os transmitem simultaneamente para todas as portas. A desvantagem é que, se usados extensivamente, eles prejudicam o desempenho da rede.

Veja alguns exemplos de endereços inválidos:

127.xxx.xxx.xxx: Nenhum endereço IP pode começar com o número 127, pois essa faixa de endereços é reservada para testes e para a interface de loopback. Se por exemplo você tiver um servidor de SMTP e configurar seu programa de e-mail para usar o servidor 127.0.0.1, ele acabará usando o servidor instalado na sua própria máquina. O mesmo acontece ao tentar acessar o endereço 127.0.0.1 no navegador: você vai cair em um servidor web habilitado na sua máquina. Além de testes em geral, a interface de loopback é usada para comunicação entre diversos programas, sobretudo no Linux e outros sistemas Unix.

255.xxx.xxx.xxx, xxx.255.255.255, xxx.xxx.255.255: Nenhum identificador de rede pode ser 255 e nenhum identificador de host pode ser composto apenas de endereços 255, seja qual for a classe do endereço, pois estes endereços são usados para enviar pacotes de broadcast. Outras combinações são permitidas, como em 65.34.255.197 (em um endereço de classe A) ou em 165.32.255.78 (endereço de classe B).

xxx.0.0.0, xxx.xxx.0.0: Nenhum identificador de host pode ser composto apenas de zeros, seja qual for a classe do endereço, pois estes endereços são reservados para o endereço da rede. Como no exemplo anterior, são permitidas outras combinações como 69.89.0.129 (classe A) ou 149.34.0.95 (classe B).

xxx.xxx.xxx.255, xxx.xxx.xxx.0: Nenhum endereço de classe C pode terminar com 0 ou com 255, pois, como já vimos, um host não pode ser representado apenas por valores 0 ou 255, já que eles são usados para o envio de pacotes de broadcast.

Dentro de redes locais, é possível usar máscaras diferentes para utilizar os endereços IP disponíveis de formas diferentes das padrão. O importante neste caso é que todos os micros da rede sejam configurados com a mesma máscara, caso contrário você terá problemas de conectividade, já que tecnicamente os micros estarão em redes diferentes.

Um exemplo comum é o uso da faixa de endereços 192.168.0.x para redes locais. Originalmente, esta é uma faixa de endereços classe C e por isso a máscara padrão é 255.255.255.0. Mesmo assim, muita gente prefere usar a máscara 255.255.0.0, o que permite mudar os dois últimos octetos (192.168.x.x). Neste caso, você poderia ter dois micros, um com o IP "192.168.2.45" e o outro com o IP "192.168.34.65" e ambos se enxergariam perfeitamente, pois entenderiam que fazem parte da mesma rede. Não existe problema em fazer isso, desde que você use a mesma máscara em todos os micros da rede.

No caso dos endereços válidos na Internet, as regras são mais estritas. A entidade global responsável pelo registro e atribuição dos endereços é a IANA (http://www.iana.org/), que delega faixas de endereços às RIRs (Regional Internet Registries), entidades menores, que ficam responsáveis por delegar os endereços regionalmente. Nos EUA, por exemplo, a entidade responsável é a ARIN (http://www.arin.net/) e no Brasil é a LACNIC (http://www.lacnic.net/pt/). Estas entidades são diferentes das responsáveis pelo registro de domínios, como o Registro.br.

8.6 Conflito de endereço Ip

As faixas de endereços começadas com "10", "192.168" ou de "172.16" até "172.31" são reservadas para uso em redes locais e por isso não são usadas na Internet. Os roteadores que compõe a grande rede são configurados para ignorar pacotes provenientes destas faixas de endereços, de forma que as inúmeras redes locais que utilizam endereços na faixa "192.168.0.x" (por exemplo) podem conviver pacificamente, sem entrar em conflito.

8.7 CIDR e Máscara de subrede , exemplos de máscara e endereços

Uma máscara de sub-rede, também conhecida como subnetmask ou netmask, é um número de 32 bits usado em um IP para separar a parte correspondente à rede pública, à sub-rede e aos hosts.Uma sub-rede é uma divisão de uma rede de computadores. A divisão de uma rede grande em menores resulta num tráfego de rede reduzido, administração simplificada e melhor performance de rede. No IPv4 uma sub-rede é identificada por seu endereço base e sua máscara de sub-rede.

Máscara de rede padrão acompanha a classe do endereço IP: num 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. Num 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 num endereço classe C, a máscara padrão será 255.255.255.0 onde apenas o último octeto refere-se ao host.

O termo endereço de rede pode tanto significar o endereço lógico, ou seja o endereço da camada de rede – tal como o endereço IP, como o primeiro endereço (endereço base) de uma faixa de endereços reservada a uma organização.Os computadores e dispositivos que compõem uma rede (tal como a Internet) possuem um endereço lógico. O endereço de rede é único e pode ser dinâmico ou estático. Este endereço permite ao dispositivo se comunicar com outros dispositivos conectados à rede. Para facilitar o roteamento os endereços são divididos em duas partes:

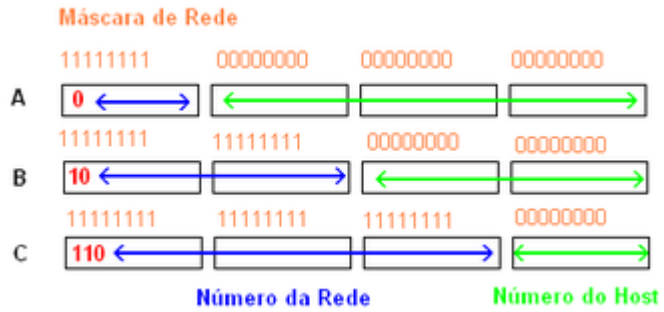
- O endereço (número) da rede que identifica toda a rede/sub-rede: o endereço de todos os nós de uma sub-rede começam com a mesma sequência.
- O endereço (número) do host que identifica uma ligação a uma máquina em particular ou uma interface desta rede.

Isto funciona de maneira semelhante a um endereço postal onde o endereço de rede representa a cidade e o endereço do host representa a rua. A máscara de sub-rede é usada para determinar que parte do IP é o endereço da rede e qual parte é o endereço do host.

Os endereços IPv4 consistem de endereços de 32 bits divididos em 4 octetos e uma máscara de sub-rede do mesmo tamanho. Há três tipos de redes "*classful*"

Classe	Bits iniciais	Início	Fim	Máscara de sub-rede padrão	Notação CIDR
A	0	1.0.0.1	126.255.255.254	255.0.0.0	/8
B	10	128.0.0.1	191.255.255.254	255.255.0.0	/16
C	110	192.0.0.1	223.255.255.254	255.255.255.0	/24

Os 32 bits das máscaras de sub-rede são divididos em duas partes: um primeiro bloco de 1s, indicando a parte do endereço IP que pertence à rede, seguido por um bloco de 0s, indicando a parte que pertence ao host.Normalmente, as máscaras de sub-rede são representadas com quatro números de 0 a 255 separados por pontos. A máscara 255.255.255.0 (ou, em binário, 11111111.11111111.11111111.00000000).



Máscaras de Rede para as classes A, B e C classfull.

Embora normalmente as máscaras de sub-rede sejam representadas em notação decimal, é mais fácil entender seu funcionamento usando a notação binária. Para determinar qual parte de um endereço é o da rede e qual é o do host, um dispositivo deve realizar a operação AND.

Exemplo classfull

	Endereço Decimal	Binário
Endereço completo	192.168.5.10	11000000.10101000.00000101.00001010
Máscara da sub-rede	255.255.255.0	11111111.11111111.11111111.00000000
Porção da rede	192.168.5.0	11000000.10101000.00000101.00000000

As máscaras de sub-rede não precisam preencher um octeto ("byte"). Isto permite que uma rede “classfull” seja subdividida em sub-redes. Para criar uma sub-rede reserva-se alguns bits do host para a rede.

O exemplo a seguir mostra como os bits podem ser "emprestados" para converter uma rede classfull em uma sub-rede.

Exemplo CIDR

	Endereço Decimal	Binário
Endereço completo	192.168.5.130	11000000.10101000.00000101.10000010
Máscara de sub-rede	255.255.255.192	11111111.11111111.11111111.11000000
Porção da sub-rede	192.168.5.128	11000000.10101000.00000101.10000000

No exemplo dois bits foram emprestados da porção do host e usados para identificar a sub-rede.

IP	Prefixo da Rede	Número da sub-rede	Número do Host
11000000.10101000.00000101.10000010	11000000.10101000.00000101	10	000010

Para determinar o número de hosts/sub-redes disponíveis a partir de certa máscara de sub-rede devemos verificar o número de bits emprestados. No exemplo anterior, por exemplo, há 2 bits emprestados, logo há:

CIDR e Máscaras de tamanho variável

Muito do que vimos até aqui já foi abordado nos capítulos anteriores. Optei por começar com um resumo geral para chamá-lo de volta ao tema, já que esta questão dos endereçamentos é um assunto complicado. Vamos então às novidades.

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 ou 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 (abreviação de "ClasslessInter-DomainRouting", que pronunciamos como "cider"), a partir de 1993 (leia o RCF no http://tools.ietf.org/html/rfc1519).

Entender as classes de endereços A, B e C é importante para compreender o uso das máscaras de sub-rede e por isso elas ainda são muito estudadas, mas é importante ter em mente que, na prática, elas são uma designação obsoleta. Naturalmente, ainda existem muitas redes que utilizam faixas de endereços de classe A, B e C (já que as faixas alocadas no passado não podem ser simplesmente revogadas de uma hora para a outra), mas as faixas alocadas atualmente utilizam quase sempre o novo sistema.

No CIDR são utilizadas máscaras de tamanho variável (o termo em inglês é VLSM, ou Variable-LengthSubnetMask), que permitem uma flexibilidade muito maior na criação das faixas de endereços. 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.

Outra mudança é que 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.O CIDR permite também que várias faixas de endereços contínuas sejam agrupadas em faixas maiores, de forma a simplificar a configuração. É possível agrupar 8 faixas de endereços com máscara 255.255.255.0 (classe C) contínuas em uma única faixa com máscara /21, por exemplo, que oferece um total de 2045 endereços utilizáveis (descontando o endereço da rede, endereço de broadcast e o endereço do gateway).As faixas de endereços são originalmente atribuídas pela IANA às entidades regionais. Elas dividem os endereços em faixas menores e as atribuem aos carriers (as operadoras responsáveis pelos links), empresas de hospedagem, provedores de acesso e outras instituições. Estas, por sua vez, quebram os endereços em faixas ainda menores, que são atribuídas aos consumidores finais.

Revisando, a máscara de subrede determina qual parte do endereço IP é usada para endereçar a rede e qual é usada para endereçar os hosts dentro dela. No endereço 200.232.211.54, com máscara 255.255.255.0 (/24), por exemplo, os primeiros 24 bits (200.232.211.) endereçam a rede e os 8 últimos (54) endereçam o host. Quando usamos máscaras simples, podemos trabalhar com os endereços em decimais, pois são sempre reservados 1, 2 ou 3 octetos inteiros para a rede e o que sobra fica reservado ao host. Esta é a idéia usada nas faixas de endereços classe A, B e C. Quando falamos em máscaras de tamanho variável, entretanto, precisamos começar a trabalhar com endereços binários, pois a divisão pode ser feita em qualquer ponto. Imagine, por exemplo, o endereço "72.232.35.108". Originalmente, ele seria um endereço de classe A e utilizaria máscara "255.0.0.0". Mas, utilizando máscaras de tamanho variável, ele poderia utilizar a máscara "255.255.255.248", por exemplo.

Nesse caso, teríamos 29 bits do endereço dedicados à endereçar a rede e apenas os 3 últimos bits destinados ao host. Convertendo o endereço para binário teríamos o endereço "01001000.11101000.01100000.01101100", onde o "01001000.11101000.01100000.01101" é o endereço da rede e o "100" é o endereço do host dentro dela. Como temos 29 bits dedicados à rede, é comum o uso de um "/29" como máscara, no lugar de "255.255.255.248".À primeira vista, esse conceito parece bastante complicado, mas na prática não é tão difícil assim. A primeira coisa a ter em mente é que as máscaras de tamanho variável só fazem sentido quando você converte o endereço IP para binário.Para converter um número decimal em um número binário, você pode usar a calculadora do Windows ou o Kcalc no Linux. Configure a calculadora para o modo científico (exibir/científica) e verá que do lado esquerdo aparecerá um menu de seleção permitindo (entre outras opções) escolher entre decimal (dec) e binário (bin)

255.255.255.0 (/24)	nenhum	00000000	nenhuma	254 endereços (do 1 ao 254)
255.255.255.192 (/26)	11	000000	2 endereços (2 e 3)	62 endereços (de 1 a 62)
255.255.255.224 (/27)	111	00000	6 endereços (de 1 a 6)	30 endereços (de 1 a 30)
255.255.255.240 (/28)	1111	0000	14 endereços (de 1 a 14)	14 endereços (de 1 a 14)
255.255.255.248 (/29)	11111	000	30 endereços (de 1 a 30)	6 endereços (de 1 a 6)
255.255.255.252 (/30)	111111	00	62 endereços (de 1 a 62)	2 endereços (2 e 3)

Obs: A divisão de classes tradicional fazia com que um grande numero de endereços fosses desperdiçados por exemplo , um provedor de acesso que precisasse de 1.000 endereços , utilizaria a classe B inteira , 65 mil endereços , **classer inter domain routing ,onde** são usadas máscara de tamanho variável , que permitem uma

flexibilidade muito maior na criação de faizas de endereços., se são necessários 1000 endereços usaríamos a máscara /22 que permite o usp de 1022 endereços. O **Iana** controla as fixas de IP. A máscaras de subredes indicam qual parte do endereço indoca a rede e o host dentro dela.

Classe A: 255.0.0.0 10.10.10.1 /8
Classe B: 255.255.0.0 172.12.13/16
Classe C: 255.255.255.0 192.168.1.4/24

As máscaras além de identificarem o Ip , servem para mascarar um endereços mudando as faixas, ex: se se, 192.168.6.7 usassemos a máscara 25.255.0.0 da Classe B os dois primeiros octetos representam a rede e o host os dois últimos

1 2 4 8 16 32 64 128 = 255

8.8 Comandos básicos de rede Windows

1. Ipconfig: Esse comando não vai resolver os possíveis erros da rede, mas você consegue obter detalhes sobre endereço IPv4, máscara da sub-rede, gateway, DNS, IPv6 e outros tantos. Uma vez executado o comando, é possível conferir se o seu roteador está distribuindo o IP correto, se o DNS atribuído é o correto e assim por diante.

2. Ping: Basta digitar "ping", o endereço do site (pode ser o IP ou o endereço completo) e pressionar Enter. O Windows envia alguns pacotes para a página indicada e aguarda a resposta. Em poucos segundos, você poderá saber se os pacotes foram devidamente entregues e o tempo que foi necessário para tal tarefa.
3.Tracert: Outro comando semelhante ao "ping" é o "tracert". O nome desse recurso vem de "traçar rota", justamente porque ele serve para verificar se todos os servidores envolvidos na comunicação entre seu computador e uma determinada página estão operando conforme o esperado. Ao executar esse comando, o Windows confere o tempo necessário, em milissegundos, para se conectar a cada um dos computadores intermediários no processo de acesso até a página solicitada. O último rastreado na rota é a página que você quer visitar.

4. netstat -na: Ainda falando sobre problemas de rede, há mais um comando que pode ser útil para conferir se o seu computador não está se comportando de forma anormal. O "netstat" é um comando bem simples, mas que pode ser bem esclarecedor. Para usá-lo, digite o seguinte no Prompt de Comando:

5.Telnet:Permite Acessar, No Modo Terminal (Tela Passiva), Um Host Remoto:

```
telnet <IP ou host>
```

```
telnet <IP ou host><porta TCP>
```

Este comando também permite ver se um serviço TCP funciona em um servidor distante especificado pelo endereço IP e o número da porta TCP. Deste modo, podemos verificar se o serviço SMTP, por exemplo, roda em um servidor Microsoft Exchange utilizando o endereço IP do conector SMTP e na porta número 25. As portas mais comuns são:

Protocolo	Porta
FTP	21
TELNET	23
SMTP	25
WWW	80
POP3	110

6. Hostname: Mostra O Nome Da Máquina

8.9 Outros Protocolos

Serviço	TCP	UDP	Observações
FTP	21	21	Transferência de arquivos
SSH	22	22	Protocolo de login remoto encriptado
Telnet	23	23	Protocolo de login remoto
SMTP	25	25	Para envio de email
DNS	53	53	Resolução de nomes para IP
HTTP	80	80	Para web browser
POP3	110	110	Para recepção de email
IMAP	143	143	Para recepção/envio de email
TLS/SSL	443	443	Protocolo de camada de sockets segura
IRC	6667	6667	Para conversação/chat
Pichat	9009	9009	Protocolo de conversação/chat

8.10 Gateway: o que é e como funciona?

Com a popularização da internet e das telecomunicações em geral, as pessoas passaram a utilizar os recursos de rede, como o gateway, de forma automática e natural. São raros os casos de usuários que buscam entender o funcionamento e o que acontece “por trás” dos navegadores e computadores pessoais.No entanto, é interessante conhecer um pouco sobre como a coisa toda funciona, até mesmo para identificar possíveis anomalias que possam comprometer a estrutura de TI utilizada.Neste post, vamos falar sobre um recurso pouco comentado, ainda que esteja presente em todas as topologias de acesso à internet: o gateway. Continue a leitura para saber do que se trata, como funciona e para que serve essa ferramenta!

O que é um gateway?

Em uma tradução livre do inglês, um *gateway* poderia ser classificado como “portal” ou “portão”. Em resumo, uma passagem entre dois ambientes distintos.A tradução do termo é exatamente o que ele significa: um equipamento encarregado de estabelecer a comunicação entre duas redes, respeitando protocolos específicos e tomando determinadas ações necessárias para o correto funcionamento da comunicação entre as duas pontas.Grosso modo, o funcionamento do dispositivo é bastante simples. Ele **faz o papel de ponte entre as redes**, analisando e tratando as informações de acordo com as definições preestabelecidas e o tipo de função a que se destina.Uma das funções centrais de um *gateway* é organizar o tráfego de informações entre um equipamento final (computador, notebook, smartphone, tablet, etc) e a internet.
Naturalmente, o dispositivo é utilizado também para prover recursos de segurança, controlando as informações que entram e saem da rede interna.Outra atribuição dos *gateways* é “traduzir” as informações entre redes heterogêneas. Isto é, permitir a comunicação entre diferentes ambientes e arquiteturas. Assim, a ferramenta é capaz de converter os dados entre sistemas diferentes, de modo que cada lado seja capaz de “entender” o outro.

8.11 Cálculo de sub rede

Como o IPV 4 está escasso é impressionante , devemos fazer cálculos para evitar desperdícios, exemplo: se temos uma rede onde 100 usuários irão se conectar , não usaremos a mascara clássica , 255.255.25.0 /24, que usaria 256 endreços, deixando 156 is vagos. Vermos como aproveirar ndreços , descobrir numero de ips , broadcast , primeiro e último endereço IP.

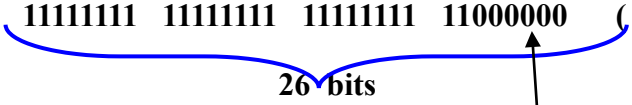
Cálculo do IP : 10.20.12.45 /26

- Endereço de rede:10.20.12.0
- Endereços de Broadcast:10.20.12.63
- Máscara: 255.255.255.192
- Primeiro IP:10.20.12.1
- Ùltimo IP: 10.20.12.62
- Nº total de IPS: 64
- Nº de IPS válidos: 62 (hosts)

- Converter em binário: Divisão ou tabela : 128 64 32 16 8 4 2 1 = 255 Endereços
8ª 7ª 6ª 5ª 4ª 3ª 2ª 1ª

10 20 12 45
00001010 00010100 00001100 0101101

11111111 11111111 11111111 11000000 (nº de hosts)



26 bits

Máscara : 255 255 255 192

2 ^ b – 2 (b= número de bits , 2 ^6= 64 : nº de IPS , 64 -2 : 62 (nº de ips válidos,hosts)

Endereço de rede: 00001010 00010100 00001100 *00*00000 /26
10 20 12 0

Endereço de broad: 00001010 00010100 00001100 00111111 /26 (troca os hosts)
10 20 12 63