Aula 5 - Cálculo de máscara e de subredes

5.1 Conceitos

Quando um host se comunica com outro usa o endereço de enlace dele. Os endereços de hardware das placas de rede, ou MAC Address, são constituídos de 48 bits, sendo os primeiros 24 bits a referência ao fabricante da interface de rede, sendo representado por um número em hexadecimal pode ser visualizado executando-se os comandos "ifconfig" (Linux/UNIX) e "ipconfig" (Windows), por exemplo 00:50:56:C0:00:06.

Portanto quando a comunicação entre dois ou mais hosts é realizada coloca-se o endereço de hardware do destino no pacote, determinando que este pacote deve ser entregue ao host cujo endereço de placa de rede é o 00:50:56:C0:00:06.

O problema é que essa técnica só funciona dentro da rede local, pois a origem precisa antecipadamente conhecer o MAC Address do destino e é para isto que serve o protocolo ARP.

Mas e quando o destino não está na mesma rede que eu ou que não se pode colocar o MAC de destino no pacote? e é para isso que existe o roteamento IP.

Analisando o número IP do destino, o host de origem verifica que precisa repassá-lo ao gateway, porque o destino não se localiza na rede local. O gateway, por sua vez, compara o IP de destino com sua tabela de rotas para determinar para onde o pacote vai ser destinado, e assim sucessivamente, até que pacote chegar na rede local do destino, onde o último gateway irá enviar o pacote para o MAC Address de destino, sendo que cada etapa do roteamento envolve o MAC Address do gateway de saída.

Portanto conclui-se que o número IP não serve para que um host se comunique com outro, já que a comunicação é sempre de endereço MAC para endereço MAC e o número IP serve para determinar o próximo passo de roteamento, logo, entender o papel dos números IP em uma comunicação envolve compreender a tarefa de cada uma das quatro camadas do modelo TCP/IP.

5.2 IP e classes

Os números IPS são organizados através de uma técnica determinística, que permite saber onde está o destino ou pelo menos para que lado está. Os números IPs da

versão 4 (IPv4) são assim e a primeira organização de IPs foi a organização por classes.

Esse conceito já não importa mais para efeitos de roteamento, mas até 1993 era a forma usada para realizar roteamento IP. Nesta técnica os IPs foram catalogados em Classes, para determinar melhor o roteamento.

O objetivo do roteamento por classes era disponibilizar uma forma muito rápida (matematicamente) dos roteadores calcularem o destino. Basicamente determinou-se que dos 32 bits de um número IP, parte dele (alguns bits iniciais) diriam qual a rede de destino e outra parte dele (bits finais) diriam qual o número do host dentro desta rede. Se apenas 8 bits iniciais disserem qual rede é, um roteador só precisa analisar estes 8 bits para determinar o destino e não todos os 32, sempre visando o menor custo computacional, já que naquela época o hardware não tinha o poder de processamento da atualidade.

Portanto as classes foram divididas em 5 (A, B, C, D e E), porém apenas 3 são utilizados em endereçamento de hosts em redes (A, B e C).

Classe A:

Sempre que um número IP começar com 0, é classe A. Genericamente pode-se dizer que um classe A possui o formato:

0XXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX

Isto facilitava muito (embora não se usa mais isso) as operações de roteamento, por exemplo:

- se há roteador classe A e o primeiro bit do IP que deve-se rotear não for 0 (zero), pode-se concluir então que o destino não é o roteador classe A.

Como o primeiro bit será sempre ZERO, isto obriga o primeiro octeto do IP a ser 0XXXX XXXX, o que restringe as possibilidades deste octeto a ser de 0 a 127. Por isto que popularmente se diz que um IP Classe A é o que vai de 0.0.0.0 até 127.255.255.255.

Obs: os roteadores não fazem operações lógicas (AND, OR, XOR e etc.), mas operações bit a bit, ou seja, se primeiro bit for 0 (zero) é um classe A.

Sendo um Classe A, primeiro bit em zero, os próximos 7 bits dizem qual é a rede e os demais qual o host dentro desta rede:

0RRRRRRR HHHHHHHH HHHHHHHH HHHHHHHH

A definição da classe determina a quantidade de bits para rede, no caso de um classe A, tem-se sete bits para rede e 24 paro host.

No princípio das redes, adquiria-se uma faixa Classe A para grandes empresas, e podia suprir até 2^24 hosts, ou seja, 16.777.216 de hosts, porém existiam apenas 127 redes deste tipo no mundo.

Classe B:

Sempre que um número IP começar com 10, a classe é B e sendo desta classe, os próximos 14 bits é que dizem que rede é, sobrando os últimos 16 para determinar qual o host:

10RRRRRR RRRRRRRR HHHHHHHH HHHHHHHH

Com 16 bits paro host, cada rede poderia ter até 65.536 hosts e um total de 16384 redes classe B existem (2^14).

Classe C:

Sempre que um número IP começar com 110, é classe C e sendo desta classe, os próximos 21 bits é que dizem que rede é, sobrando os últimos 8 para determinar qual o host:

110RRRRR RRRRRRRR RRRRRRR HHHHHHHH

Com isto cada rede pode ter até 256 IPs e muitas redes deste tipo existiram, algo em torno de 2 milhões.

Classe D:

Ainda existe o Classe D (começa com 1110) reservado para tráfego multicast (ainda usado).

Classe E:

A Classe E (1111) é reservada para uso futuro. Como para uso normal, unicast, tem-se apenas o classe A, B e C, o último IP válido ainda hoje é o que começa com 223 (224

já é classe D).

5.3 Roteamento por classes de IP

A utilidade da divisão por classes (que já não se usa mais) com o número de bits, que determinam o que é rede, variava, logo a classe determinava quantos bits o roteador devia avaliar, já que o roteador necessitava saber a rede de destino para determinar a quem ele enviaria o pacote.

Desta forma, o roteador testava o primeiro bit, que se fosse zero, ou seja, Classe A, isolaria os próximos sete bits e jogaria em sua tabela de rotas, porém se os primeiros bits fossem 10, então são os próximos 14 bits que devem ser isolados e comparados com a tabela de rotas, neste caso, as operações binárias agilizam este tipo de operação.

Esta forma de roteamento era muito otimizada, tanto que foi ressuscitada no Ipv6, porém somente o conceito e não o modelo de classes, já que no padrão IPv6 não existem classes.

Essa técnica facilitava muito o trabalho dos roteadores, que sem muito esforço determinavam o que fazer com o pacote, porém causava um grande problema: a falta de números IPs.

O fato de uma faixa Classe C possibilitar apenas 256 IPs é pouco para a maioria das instituições que desejam entrar na Internet, já a classe A com seus 16 milhões de IPs é muito, logo preferia-se ficar com a classe B, que está se esgotou rapidamente.

Como exemplo pode-se citar o caso de uma instituição que tenha 300 computadores para conectar na Internet, neste caso uma rede da Classe C não serve, logo ele adquire um classe B, porém com 300 computadores em uma classe B, que pode ter 65.536 hosts, estaria sendo desperdiçado, portanto, mais de 65.000 endereços IP, sem citar uma rede Classe A que permite 16.000.000 de IPs.

Este fato gerou desorganização, pois esgotou rapidamente os números de IPs disponíveis, levando-se em conta ainda o desperdício IPs que não eram utilizados nas redes.

Este cenário caótico de endereçamento motivou a criação de uma nova técnica de classificação, e a CIDR se viu obrigada a reorganizar os endereçamento IP, sendo que nelas é que existem as máscaras de rede atuais.

5.4 Classificação CIDR

CIDR - Classless Inter-Domain Routing - Roteamento Inter-Domínio sem Classes, ou Roteamento Livre de Classes, veio para substiruir definitivamente o uso de classes e em 1993 este padrão substitui as classes.

Levando-se em conta que o IPv4 é dividido em duas partes:

- bits iniciais dizem qual rede é;

- bits finais dizem qual o host dentro desta rede.

Antes o conceito de Classe definia quantos bits eram a rede e quantos eram o host, porém o que o CIDR fez foi mudar este conceito, ou seja, não importa de qual classe o IP é, o número de bits de rede não é fixo, portanto pode-se ter agora um IP "CLASSE A", usando não sete, mas 24 bits para rede e os demais 8 paro host, como seria um classe C.

Esta mudança causou mudanças significantes pois o roteador já não consegue, através da análise do IP, avaliar quantos bits deve analisar para determinar a rede de destino, que provocouo fim da otimização dos cálculos, já que o roteador precisará efetuar mais cálculos, com custo mais onerosos, porém ganha-se um número consideravelmente maior de IPs.

No modelo CIDR a informação de quantos bits são usados para rede é simplesmente representada colocando-se este número ao lado do IP:

Exemplo:

10.1.0.5/24

Neste caso o /24 determina que são usados os primeiros 24 bits para rede, e que os últimos 8, o resto, são para definir o host.

Cada definição de uma rede IP possui ainda dois números especiais, que não podem ser usados:

- a definição do número da rede;

- e a definição do número de broadcast.

Isto já ocorria desta mesma forma no modelo de classes, porém estes números eram fixos, pois o número de bits para rede era preso a classe que ele pertencia, no CIDR, porém, estes dois números precisam ser calculados.

5.5 Cálculo do número de rede e de broadcast

Define-se como número de rede o primeiro endereço da faixa e como número de broadcast o último. Se tivermos, por exemplo, o IP 10.1.0.5/24 (24 bits para rede):

(10) (1) (0) (5)

0000 1010 0000 0001 0000 0000 0000 0101

<------ 24 bits para rede ----------> <- HOST->

O número de rede seria 00001010 00000001 00000000 00000000, ou 10.1.0.0, primeiro IP que seria paro host da seqüência.

O número de broadcast seria 0001010 00000001 00000000 11111111, ou 10.1.0.255, último número de host permitido.

Como calcular este número?

Usando operações binárias, pois elas são rápidas e eficientes. Para calcular o número da rede, faz-se um AND bit a bit do número IP com os números destinados a rede em 1. Se um IP é /24, quer dizer que devem ser usados 24 bits para rede, restando oito paro host. Para calcular a rede faz-se um AND com os primeiros 24 bits em 1 e os demais em zero:

(10) (1) (0) (5)

0000 1010 0000 0001 0000 0000 0000 0101

1111 1111 1111 1111 1111 1111 0000 0000 (24 bits em 1)

0000 1010 0000 0001 0000 0000 0000 0000 (resposta do AND)

Ao realizar este AND bit a bit, chega-se ao número 10.1.0.0 (número da rede).

Agora observe esta fato: caso seja lido de forma decimal estes bits que usados para o AND, que número será?

1111 1111 1111 1111 1111 1111 0000 0000

(255) (255) (255) (0)

255.255.255.0 soa mais familiar, por isto o nome “máscara de bits” pois é uma máscara que será usada em uma operação AND para determinar qual a rede.

Para determinar qual é o endereço de broadcast, se faz um OR bit a bit com a

máscara complementada (invertida, números destinados a rede em ZERO):

(10) (1) (0) (5)

0000 1010 0000 0001 0000 0000 0000 0101

0000 0000 0000 0000 0000 0000 1111 1111 (24 bits em 0)

0000 1010 0000 0001 0000 0000 1111 1111 (resposta do OR)

Sendo agora um OR, o resultado matemático disto será 10.1.0.255.

É isto que acontece em background, envolvendo a máscara para determinar a qual rede pertence e qual o endereço de broadcast. Uma máscara equívoca pode significar o isolamento de um host do resto do mundo, pois ela pode não rotear pacotes corretamente, não usando o gateway quando deveria, por exemplo.

5.6 Roteamento baseado em máscara

Cado host sabe seu IP, sua máscara e o IP do gateway. o host não sabe as máscaras e os ips de outras hosts, apenas a sua. Logo, ao necessitar comunicar-se com umo host cujo o IP é X.Y.W.Z o host não tem como saber qual rede este IP é, mas tem como saber se é a mesma rede sua. Isto é suficiente para ela saber se pode enviar diretamente (mesma rede) ou se precisa acionar o gateway para jogar para fora (estando no MS, pode-se não saber onde é um CEP que começa com "4", mas sabe-se que não é MS, pois no MS ele começa com "7", portanto, basta para enviar para outra agência de correio).

Exemplos:

Caso A: origem e destino estão na mesma rede. Maquina A com IP 10.1.0.5/25 deseja conversar com 10.1.0.120, pois não sabe a máscara do destino.

O host A primeiro determina a sua rede aplicando um AND do seu IP com sua máscara, sendo que ela agora é 255.255.255.128, pois um /25 significa 25 bits em 1:

1111 1111 1111 1111 1111 1111 1000 0000

(255) (255) (255) (128)

Chega-se a conclusão que pertence a rede 10.1.0.0, e faz o mesmo com o IP de destino, aplicando um AND do IP de destino COM A SUA MÁSCARA (única que ela tem):

(10) (1) (0) (120)
0000 1010 0000 0001 0000 0000 0111 1000
1111 1111 1111 1111 1111 1111 1000 0000 (25 bits em 1)

Como resultado deste AND, chega-se ao cálculo de 10.1.0.0. Como o número calculado para rede é o mesmo, a conclusão é que o destino está aqui, local, basta realizar um ARP e endereçar diretamente o MAC do destino e, portanto não há a necessidade de usar o gateway.

Caso B: origem e destino não estão na mesma rede, o host A com IP 10.1.0.5/25 deseja conversar com 10.1.0.129. Já sabemos que a rede que o host A pertence é 10.1.0.0 (pode não ser se o host A estiver com a máscara errada)

Ela faz o mesmo com o IP de destino, aplicando um AND do IP de destino COM A SUA MÁSCARA (única que ela tem):

(10) (1) (0) (129)
0000 1010 0000 0001 0000 0000 1000 0001
1111 1111 1111 1111 1111 1111 1000 0000 (25 bits em 1)
0000 1010 0000 0001 0000 0000 1000 0000 (RESULTADO AND)

Como resultado deste AND, chega-se ao cálculo de 10.1.0.128, que não é mesma rede do host A. A conclusão é que o destino não o local e precisa repassar o pacote para o gateway.

Se o host A estiver com a máscara errada (um /24 quando deveria ser um /25) ela pode ficar isolada de parte da rede, por achar que o destino é rede local quando não é (deveria ter usado o gateway). Da mesma forma se ela é um /25, quando deveria ser na realidade um /24, poderá usar o gateway quando não era necessário. A correta configuração de máscara é extremamente importante.

5.7 Cálculo máscara, sub-rede e de hosts

Para definir qual é a máscara de sub-rede ideal ao dividir uma rede, devemos levar em conta alguns fatores como como a quantidade de sub-redes ou de hosts que se

deseja obter.

Como exemplo para ilustração tem-se a subdivisão de uma rede classe B: 172.25.0.0

A máscara de rede original é 255.255.0.0 – sendo que os bytes 172.25 identificam a rede, restam, portanto 2 bytes, ou 16 bits, que deverão identificar as sub-redes e também os hosts dentro de cada sub-rede, ou seja, se forem utilizados muitos bits do restante para designar sub-redes, sobrarão poucos bits para designar os hosts dentro das sub-redes

Exemplo:

Se forem utilizados 12 bits dos 16 restantes para designar sub-redes, pode-se dividir a rede 172.25.0.0 em até 4.096 sub-redes, ou seja 2^12 , porém em cada sub-rede pode-se ter somente 14 hosts (2^4 = 16 - 2 inválidos = 14), pois restarão apenas 4 bits para identificar os hosts dentro das sub-redes.

A máscara de sub-rede neste caso seria:

255 . 255 . 255 . 240

11111111.11111111.11111111.1111 0000

Nota-se que há 12 bits (1) que representam a rede.

Por outro lado, caso se quira utilizar 12 bits para designar os hosts da rede, possibilitando assim 4094 hosts por sub-rede, pode-se ter somente 16 sub-redes, já que restarão somente 4 bits para designar a rede.

A máscara de sub-rede nesse caso seria:

255 . 255 . 255 . 240

11111111.11111111.1111 0000.00000000

Exemplo:

Em uma rede deseja-se ter uma sub-rede com 30 hosts. Qual a melhor máscara de sub-rede?

R:

2^5 – 2 = 30

Logo permanecem 5 zeros na parte de host:

11111111.11111111.11111111.11100000

255 . 255 . 255 . 224

Na notação CIDR, a máscara será:

255.255.255.224/27

Exercício

Calcular a máscara de um rede com 200 hosts.

R:

200 hosts = 2^8 – 2 = 254

Portanto tem-se 8 zeros na parte de host do endereço.

A máscara de rede será então:

11111111.11111111.11111111.00000000

255 . 255 . 255 . 0

ou na notação CIDR seria /24

Obs: lembrar que este sempre temos de reservar 2 endereços IP, 0 para a rede e 255 para o broadcast, portanto em um endereçamento de hosts sempre estes 2 endereços serão reservados e não poderão ser utilizados para endereços de hots para cada subrede.