Redes de Computadores I

Aula 05 - Arquitetura Internet – Parte II

Apresentação

Na disciplina de Sistemas de Conectividade, você viu que a internet utiliza a pilha de protocolos TCP/IP e, além disso, estudamos superficialmente os protocolos de cada camada. Você deve lembrar que, na camada de rede, o principal protocolo é o protocolo IP (*Internet Protocol*). Nesta aula, você vai aprender como esse protocolo funciona e porque ele é a parte principal e fundamental da arquitetura da Internet.

Objetivos

- Entender o protocolo IPv4 e o formato de seu datagrama.
- Definir como é o esquema de endereçamento do protocolo IP.
- Entender como o IP pode ser utilizado para a divisão de uma rede em várias sub-redes.
- Entender o funcionamento das máscaras de sub-redes.

Características do Protocolo IP

O protocolo IP utiliza comutação de pacotes para realizar o encaminhamento das informações. Uma vez que você já estudou como funcionam as redes baseadas em comutação por pacotes, já deve compreender o funcionamento do IP. Sendo assim, vamos descrever, brevemente, algumas das características deste protocolo.

- As informações a serem transmitidas são divididas em partes e colocadas em pacotes, os quais contêm, entre outras informações de cabeçalho, o endereço lógico da máquina que gerou a informação e o endereço lógico da máquina para quem ela é destinada.

- Os pacotes destinados a uma máquina em uma rede diferente da máquina que o gerou são enviados, inicialmente, para o roteador da rede de origem. São transmitidos, então, de roteador em roteador, até atingirem a rede de destino, quando são entregues à máquina de destino. Esse processo se chama roteamento.

- O roteamento de cada pacote é feito independentemente dos demais pacotes. Portanto, caso uma máquina A envie 1.000 pacotes para uma máquina B, cada roteador no caminho entre A e B, ao receber o pacote para ser encaminhado, irá calcular a rota (próximo roteador no caminho) como se nenhum outro pacote entre A e B houvesse passado por ali antes. Como consequência disso, cada pacote pode seguir um caminho diferente.

- O protocolo IP não garante que os pacotes serão entregues, nem que os que forem entregues serão entregues na ordem em que foram transmitidos. Portanto, o protocolo IP passa os pacotes (apenas a parte de dados do pacote) para a camada de transporte na ordem em que são recebidos.

- Cada pacote transmitido pode demorar um tempo diferente do pacote anterior. Ou seja, o IP não oferece nenhuma garantia sobre o atraso que cada pacote sofre ao longo do caminho.

Formato do Quadro IP

Você sabe que cada camada da pilha de protocolos adiciona seus próprios cabeçalhos, e com o protocolo IP, que implementa a camada de rede, não seria diferente. O **Quadro 1** mostra os campos do cabeçalho de um pacote IP (ou datagrama IP). O pacote, evidentemente, ainda possui um campo de dados após esse cabeçalho que irá conter as informações recebidas da camada de transporte.

Vídeo 01 - Arquitetura Internet

<table>
<tr><td>Versão
4 bits</td><td>HLEN
4 bits</td><td>TOS
8 bits</td><td colspan="2">Tamanho
16 bits</td></tr>
<tr><td colspan="3">Identificação
16 bits</td><td>Flags
3 bits</td><td>Fragmentação
13 bits</td></tr>
<tr><td colspan="2">TTL
8 bits</td><td>Protocolo
8 bits</td><td colspan="2">Checksum do cabeçalho
16 bits</td></tr>
<tr><td colspan="5">Endereço IP de Origem
32 bits</td></tr>
<tr><td colspan="5">Endereço IP de Destin
32 bits</td></tr>
<tr><td colspan="5">Opções</td></tr>
</table>

Quadro 1 – Formato do cabeçalho do pacote IP

A seguir, veja uma breve descrição sobre cada um dos campos.

- **Versão**: indica a versão do protocolo IP sendo utilizado. Atualmente, a maioria das redes utiliza a versão 4 do protocolo, mas já existe a versão 6, que gradativamente vem substituindo a versão 4.

- **HLEN** (Header Length – **tamanho do cabeçalho**): conforme o nome já sugere, o campo opções pode ser utilizado para incluir campos opcionais no cabeçalho. Mas, muitas vezes, ele não é utilizado. Isso faz com que o tamanho do cabeçalho seja variável. Desse modo, o HLEN contém o tamanho do cabeçalho em palavras de 32 bits. Ou seja, multiplique o valor de HLEN por 4 para obter o tamanho do cabeçalho IP em bytes. O tamanho máximo do cabeçalho IP é 60 bytes, mas observe que sem as opções ele possui 20 bytes.

- **TOS** (Type of Service – **tipo de Serviço**): para compensar o fato de que o protocolo IP utiliza comutação de pacotes, e, portanto, não garante taxa constante de transmissão, esses bits indicam o tipo de dados contidos no pacote e com isso os roteadores podem dar prioridades na hora de encaminhá-los. Os pacotes podem, por exemplo, serem marcados solicitando prioridade, requerendo, assim, um baixo atraso, uma alta vazão ou maior confiabilidade durante sua transmissão.

- Tamanho: esse campo indica o tamanho em bytes do pacote IP (incluindo o cabeçalho e os dados) e, como possui 16 bits, significa que o tamanho máximo é 65.535 bytes. Na prática, o tamanho da maioria dos pacotes não ultrapassa os 1500 bytes.

- **Identificação** , Flags **e Fragmentação**: esses três campos são utilizados para realizarem a fragmentação dos pacotes IP, os quais estudaremos mais a frente nesta aula.TTL (Time To Live – Tempo de Vida): caso ocorra algum problema no roteamento, um pacote pode ficar circulando eternamente na rede. Para evitar que isso ocorra, esse campo contém um contador que vai sendo decrementado ao passar por cada roteador. Quando chega a zero, o roteador o descarta. Tipicamente, quem gera o pacote coloca o valor 255 nesse campo. Observe que não se utiliza, realmente, nenhuma medição de tempo para realizar essa função.

- **TTL** (Time To Live – **Tempo de Vida**): caso ocorra algum problema no roteamento, um pacote pode ficar circulando eternamente na rede. Para evitar que isso ocorra, esse campo contém um contador que vai sendo decrementado ao passar por cada roteador. Quando

chega a zero, o roteador o descarta. Tipicamente, quem gera o pacote coloca o valor 255 nesse campo. Observe que não se utiliza, realmente, nenhuma medição de tempo para realizar essa função.

- **Protocolo**: esse campo indica o protocolo da camada de transporte para o qual a parte de dados do pacote deve ser passada quando chegar ao destino. Evidentemente, o protocolo indicado será o mesmo utilizado na origem. Veja que esse código só é analisado na máquina de destino, pois não tem nenhuma utilidade para os roteadores no caminho. Existem códigos padronizados para cada protocolo de transporte. O do TCP é 6 e do UDP é 17. A função desse campo é a mesma do campo de tipo do quadro Ethernet: indicar o protocolo da camada superior (no caso rede), que deve receber a parte de dados do quadro.

- Checksum **do cabeçalho**: esse campo tem a mesma função do CRC (Cyclic Redundancy Check – Verificação de Redundância Cíclica) nas redes Ethernet, ou seja, identificar erros. Entretanto, existem duas diferenças principais em relação ao CRC. A primeira é que o cálculo do checksum é feito apenas sobre os bytes do cabeçalho, a parte de dados não é considerada. A segunda diferença é que o algoritmo utilizado aqui é muito mais simples. Basicamente, ele agrupa cada dois bytes do cabeçalho como um número e soma esses números utilizando complemen**TOS** aritméticos de 1. A razão para essas diferenças é acelerar o cálculo do checksum, uma vez que ele precisa ser recalculado em cada roteador do caminho, já que alguns campos do cabeçalho são alterados, como é o caso do TTL. Além disso, a parte de dados do pacote, normalmente, já é protegida contra erros pelos protocolos de transporte, que incluem seus próprios checksum.

- **Endereço IP de Origem**: contém o endereço IP da máquina que gerou o pacote. Esse campo não é alterado ao longo do caminho entre a origem e o destino.

- **Endereço IP de destino**: contém o endereço IP da máquina de destino. Esse campo não é alterado ao longo do caminho entre a origem e o destino.

- **Opções**: são campos opcionais com a finalidade de depuração e testes, mas que, normalmente, não são utilizados.

Veja que, embora o **Quadro 1** mostre o cabeçalho com várias linhas, lembre-se de que ele, na verdade, é uma sequência de bytes. Portanto, um pacote IP é composto pelos bytes de todos os campos do cabeçalho, seguidos pelos bytes da parte de dados.

No caso dos datagramas IP, para que um host destinatário possa reconstruir um datagrama original, ele faz uso de alguns campos do protocolo IP, como o campo identificação, flag e deslocamento. Quando um host remetente cria um datagrama, ele marca esse datagrama com um número de identificação e também acrescenta o endereço de origem e de destino. O host remetente incrementa o número de identificação para cada datagrama que envia. Sempre que um roteador precisar fragmentar um datagrama, cada novo datagrama resultante (datagrama de **TOS** menor – fragmento) recebe o endereço de origem, o endereço de destino e o número de identificação do datagrama original.

Assim, quando um destinatário recebe vários datagramas de um mesmo remetente, ele examina os números de identificação dos datagramas, a fim de detectar quais deles são fragmen**TOS** de um mesmo datagrama de tamanho maior. O último datagrama resultante da fragmentação de um datagrama maior recebe um flag setado (marcado) para 0, a fim de indicar que esse é o último datagrama que forma o datagrama original, já os demais datagramas têm esse flag setado para 1. De posse dessas informações, o destinatário é capaz de remontar o datagrama original.

Quem Fornece os Endereços IP

Até agora, não dissemos quais endereços você deve colocar na sua empresa ou na sua casa. Nós não podemos colocar os endereços que desejarmos nas nossas máquinas porque os roteadores na internet precisam saber onde esses endereços estão, ou seja, o caminho para chegar a eles. Assim, grupos de endereços são distribuídos para cada país e ficam sob a responsabilidade de uma organização encarregada de fazer sua distribuição. Após isso, parte desses endereços é distribuída para as operadoras de *backbone* do país, que, por sua vez, distribuem

parte dos endereços recebidos para as empresas que se ligam a elas. Quando essa empresa é um provedor, ele repete o processo. Ou seja, distribui uma parte dos endereços dele para os seus clientes. Desse modo, quando você conecta no provedor, você recebe um dos endereços do provedor.

Atividade 01

---

1. Explique a função de todos os campos do cabeçalho dos pacotes IP.

Resposta

Resposta

1. O cabeçalho dos pacotes IP é composto pelos seguintes campos:
    - **Versão** – indica a versão (versão 4 ou versão 6) do protocolo IP em utilização.
    - **HLEN (***Header Len* **– tamanho do cabeçalho)** – contém o tamanho do cabeçalho em palavras de 32 *bits*. O tamanho máximo do cabeçalho IP é 60 *bytes*, mas esse tamanho pode variar de acordo com as opções setadas.
    - **TOS (***Type of Service* **– tipo de Serviço)** – para compensar o fato de que o protocolo IP utiliza comutação de pacotes, e, portanto, não garante taxa constante de transmissão, esses bits indicam o tipo de dados contidos no pacote e com isso os roteadores podem dar prioridades na hora de encaminhá-los.
    - **Tamanho** – esse campo indica o tamanho em *bytes* do pacote IP (incluindo o cabeçalho e os dados) e como possui 16 *bits* significa que o tamanho máximo é 65.535 bytes.
    - **Identificação,** *Flags* **e Fragmentação** – esses três campos são utilizados para realizarem a fragmentação dos pacotes IP.

- **TTL (***Time To Live* **– Tempo de Vida)** – caso ocorra algum problema no roteamento, um pacote pode ficar circulando eternamente na rede. Para evitar que isso ocorra, esse campo contém um contador que vai sendo decrementado ao passar por cada roteador. Quando chega a zero, o roteador o descarta.

- **Protocolo** – esse campo indica o protocolo da camada de transporte para o qual a parte de dados do pacote deve ser passada quando chegar ao destino. Evidentemente, o protocolo indicado será o mesmo utilizado na origem. Veja que esse código só é analisado na máquina de destino, pois não tem nenhuma utilidade para os roteadores no caminho. Existem códigos padronizados para cada protocolo de transporte. Por exemplo, o do TCP é 6 e do UDP é 17.

- *Checksum* **do cabeçalho** – esse campo tem a mesma função do CRC (*Cyclic Redundancy Check* – Verificação de Redundância Cíclica) nas redes Ethernet, ou seja, identificar erros. Entretanto, existem duas diferenças principais em relação ao CRC. A primeira é que o cálculo do *checksum* é feito apenas sobre os *bytes* do cabeçalho, a parte de dados não é considerada. A segunda diferença é que o algoritmo utilizado aqui é muito mais simples.

- **Endereço IP de Origem** – contém o endereço IP da máquina que gerou o pacote.

- **Endereço IP de destino** – contém o endereço IP da máquina de destino.

- **Opções** – são campos opcionais com a finalidade de depuração e testes, mas que normalmente não são utilizados.

Endereçamento

Continuando nossos estudos sobre a camada de rede, vamos falar agora de sua parte mais interessante, que é o endereçamento IP. Entender de endereçamento IP é fundamental porque quando se cria uma rede em uma empresa, normalmente se divide essa rede em várias redes menores, e é necessário decidir como distribuir os endereços. Além disso, a forma como os endereços são distribuídos tem um impacto direto em como o roteamento vai ser realizado. Um esquema de endereçamento bem feito simplifica muito a tarefa de configuração do roteamento e permite que essa tarefa seja feita de forma mais eficiente.

Como você viu na aula anterior, na Internet os hosts conseguem se comunicar graças aos endereços IPs atribuídos a cada host que fizer parte da rede. Esse endereço identifica individualmente cada host na rede. É importante mencionar que, na verdade, um endereço IP não se refere a um host, mas sim à uma interface de rede. Desse modo, um mesmo host pode fazer parte de duas redes distintas, bastando para isso que esse host tenha duas interfaces de rede, cada uma com um endereço IP adequado para cada uma destas redes.

Os endereços IP apresentam uma estrutura hierárquica, sendo dividido em duas partes distintas. A primeira parte, também chamada de prefixo, serve para identificar a rede a qual o host pertence, enquanto que a segunda parte, também chamada de sufixo, identifica o próprio host. Naturalmente, a parte de rede dos endereços de todas as máquinas de uma mesma rede IP é igual, fazendo com que uma rede corresponda a um bloco de endereços IP contínuos.

Vídeo 02 - Internet

Um endereço IP é representado no formato decimal com ponto, possuindo 32 bits de tamanho separado em 4 octetos de 8 bits cada. Desse modo, cada octeto pode assumir um valor entre 0 e 255, existindo portanto 2^{32} possíveis endereços

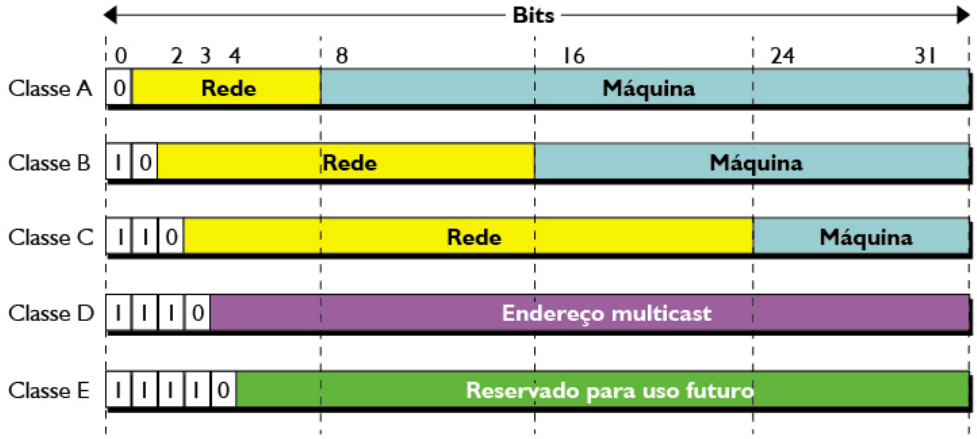
IPs. Alguns exemplos de endereços IPs são: 10.1.1.3, 173.10.10.21 e 200.241.100.10. Devemos salientar que os números IPs são representados nesse formato decimal para facilitar a nossa vida na hora de lembramos os endereços, mas na prática os computadores trabalham com todos esses números no formato binário. Assim, os endereços citados ficariam no formato binário mostrado na **Tabela 1**:

Decimal	Binário
10.1.1.3	00001010.00000001.00000001.00000011
173.10.10.21	10101101.00001010.00001010.00010101
200.241.100.10	11001000.11110001.01100100.00001010

Tabela 1 – Formatos de endereços IP (decimal e binário)

Como mencionamos anteriormente, o endereço IP tem uma parte que identifica a rede e uma parte que identifica a máquina. Quando se estava criando esse esquema de endereçamento, surgiu a seguinte questão: quantos bytes deixar para rede e quantos para as máquinas? Deixar muitos bytes para rede significa que poderiam existir muitas redes, mas que elas teriam poucas máquinas. Deixar muitos bytes para máquinas permite redes grandes, mas limita muito o número de redes existentes. A solução encontrada na época foi dividir todos os 2^{32} possíveis endereços em classes nas quais cada uma tivesse um número de bytes diferentes para a parte de rede. Assim, conforme mostra a **Figura 1**, foram criadas três classes de endereçamento chamadas de classe A, classe B e classe C. Além dessas, foi criada uma classe para utilização com aplicações multicast e outra classe que ficou reservada para uma utilização posterior.

Figura 01 - Classes de endereços IP



Fonte: Autoria própria.

Como podemos ver na **Figura 1**, cada classe aloca uma parte dos 32 bits para representar a rede e o restante para host (máquina). Essa quantidade de bits significará o total de redes e máquinas que poderemos ter em cada classe. O cálculo para descobrirmos a quantidade de redes e máquinas que teremos em cada classe é feito baseado no sistema binário. Assim, na classe A, temos 8 bits alocados para representar a rede (espaço em amarelo), porém, como visto na **Figura 1**, o primeiro bit é definido para zero, logo, restam sete bits, o que resulta em 128 redes possíveis (2^7 combinações que será igual a 128) e 24 bits para máquinas (2^{24} combinações que é igual a 16.777.216). A quantidade de redes e de hosts de cada classe está citada na tabela a seguir.

A **Tabela 2** mostra os intervalos dos IPs de cada classe:

Classe	Endereços	Núm. de redes	IPs por rede
A	0.0.0.0 até 127.255.255.255	128	16.777.216
B	128.0.0.0 até 191.255.255.255	16.384	65.534
C	192.168.0.0 até 223.255.255.255	2.091.150	256
D	224.0.0.0 até 239.255.255.255	Multicast	

Classe	Endereços	Núm. de redes	IPs por rede
E	240.0.0.0 até 247.255.255.255	Reservado	

Tabela 2 – Classes de endereços IP

Você acha que os quadros com endereços *multicast* e *broadcast* são repassados de modo diferente pelos swicthes? Se você respondeu sim, você acertou. Enquanto quadros com endereços unicast são encaminhados apenas na porta onde a estação de destino está conectada, quadros *multicast* e *broadcast* são encaminhados por todas as portas do switch. Portanto, mesmo que sua rede utilize apenas *switches*, lembre-se, um quadro enviado para um endereço de *broadcast* irá ocupar toda a rede, pois será retransmitido por todas as portas de todos os *switches*. Desse modo, embora os endereços *broadcast* sejam importantes para diversas aplicações, se utilizados em excesso, eles podem comprometer o desempenho da rede. Isso é um dos fatores que faz com que as pessoas evitem criar redes com um número muito alto de máquinas, preferindo dividir a rede em várias redes menores.

Endereços Reservados

Existem classes de endereços chamadas de classes especiais que não podem ser usadas em computadores na Internet e são reservadas. Como exemplo, temos a classe formada pelos endereços de 127.0.0.0 a 127.255.255.255, que é usada para testes na máquina local, e as redes 10.0.0.0 (classe A), 172.16.0.0 (classe B) e 192.168.0.0 (classe C), que são usadas em redes privadas (as redes das empresas ou que usamos em casa e que não são ligadas à Internet diretamente).

Como você viu, o endereço IP é capaz de identificar individualmente um host na rede. Desse modo, qualquer host que faça parte de uma rede precisa ter um endereço IP para poder se comunicar, seja essa rede do tipo Token Ring, Ethernet, Wireless etc.

A divisão de endereços IPs em endereços de rede e endereços de host simplifica o trabalho dos roteadores quando encaminhando pacotes para redes diferentes. Isso acontece porque os roteadores podem encaminhar pacotes com base apenas

na parte de rede de um endereço IP. Com isso, as tabelas mantidas pelos roteadores ficam menores, já que eles não precisam conhecer o endereço de todos os hosts que existem em uma determinada rede.

Atividade 02

1. Existem diversos endereços e classes de endereços que possuem um significado especial e não podem ser utilizados para identificar um *host*. Dizemos que esses endereços são reservados. Faça uma pesquisa sobre eles e em seguida liste-os, faça o mesmo com suas classes. Depois, explique para que eles foram reservados.

Resposta

Resposta

1. Os endereços em que os bits reservados para endereçar o *host* estão todos em zero são reservados para identificar a rede. Da mesma forma, os endereços em que os *bits* reservados para endereçar o host estão todos em um são reservados para identificar o endereço de *broadcast* daquela rede. Outro endereço reservado é conhecido como endereço de *loopback*, que endereça o próprio *host* (127.0.0.1).

Sub-Redes

Você já sabe que o endereço IP é dividido em uma parte para identificar a rede e outra para identificar a máquina, e que isso foi feito para permitir que os roteadores precisam ter rotas apenas para as redes e não para as máquinas individualmente. Desse modo, todos os endereços de uma rede IP precisam ser utilizados na mesma rede física. Ou seja, se você tiver duas redes físicas, você precisa de duas redes IP.

Antes de continuarmos, queremos saber se está claro para você o que é uma rede física. Para responder, lembre-se de que o roteador é o delimitador de uma rede, portanto, não importa quantos switches e hubs estejam interligados, todas as máquinas interligadas por eles formam uma única rede física. Agora, se você tiver dois laboratórios, cada um com 50 máquinas interligadas através de dois switches e dois hubs, e tiver um roteador interligando esses dois laboratórios, você terá duas redes físicas.

Suponha então que você tem à sua disposição a rede de classe B 150.1.0.0 para utilizar nos laboratórios. Como a classe B utiliza dois bytes para a parte de máquinas, você tem 2^{16} endereços disponíveis, ou seja, 65.535 endereços. Se você tem apenas 100 máquinas, parece que o problema é simples. Acontece que todos os seus endereços IP são da mesma rede IP e precisam ser utilizados na mesma rede física. Ou seja, dos 65.535, você vai utilizar 50 endereços em um laboratório e vai deixar sem uso todos os outros. Mesmo que sua rede fosse classe C, você ainda desperdiçaria aproximadamente 200 endereços.

Como você pôde observar, mesmo o esquema de classes A, B e C não foi suficiente para evitar o desperdício de endereços. Para reduzir esse problema, foi criado o conceito de **máscara de rede**, que permite dividir uma faixa de endereços IP (endereços de uma rede IP) em várias sub-redes menores. De modo geral, a **máscara de rede** permite utilizarmos quantos bits desejarmos para a parte de rede (e consequentemente para a parte de máquina), aumentando a flexibilidade na divisão de redes em sub-redes.

Vídeo 03 - Internet

Máscara de Rede

Uma máscara de rede ou como também pode ser chamada, net mask, é um número de 32 bits separados em quatro octetos, em geral, representado no formato decimal pontilhado (quatro conjuntos de números que variam entre 0 e 255) e que é

usada para que possamos identificar a porção de rede e de host de um endereço IP da rede. A máscara possui 1 nos bits da parte de rede e 0 nos bits da parte de máquina. Cada classe tem sua máscara padrão, conforme mostrado na **Tabela 3**.

Classe	Representação em Decimal	Representação em Binário
A	255.0.0.0	11111111.00000000.00000000.00000000
B	255.255.0.0	11111111.11111111.00000000.00000000
C	255.255.255.0	11111111.11111111.11111111.00000000

Tabela 3 – Classes de rede com as máscaras padrão

A máscara permite identificar a que rede um endereço IP pertence. Para isso, basta realizar a operação AND binário entre o endereço IP e a máscara. O resultado, que terá 4 bytes, é o endereço de rede. Observe que tudo que essa operação faz é colocar 0 em todos os bits na parte de máquina do endereço IP e manter os valores dos bits relativos à parte da rede.

Veja um exemplo utilizando o endereço IP 200.241.100.10 com máscara 255.255.255.0:

Endereço IP:	200.241.100.10	11001000.11110001.01100100.00001010
Máscara de rede	255.255.255.0	11111111.11111111.11111111.00000000
Endereço de rede	200.241.100.0	11001000.11110001.01100100.00000000

Observe agora como funciona a máscara de rede na prática.

Máscara de Sub-rede

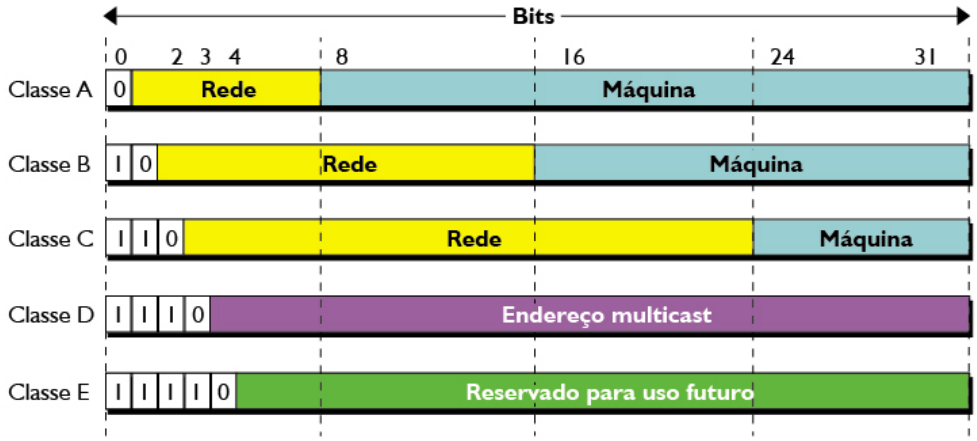
Muitas vezes, podemos querer dividir a nossa rede (de uma empresa, por exemplo) em várias redes menores (lembre-se do problema dos dois laboratórios que citamos anteriormente). Esse processo é denominado criação de sub-redes, que trará como benefício um tráfego de rede reduzido, administração simplificada e melhor desempenho da rede, além de diminuir o desperdício de endereços IP.

Vamos ver um exemplo do uso de máscara de rede e também de criação de sub-redes. Suponha que você tenha uma empresa formada por quatro setores (atendimento, suporte, financeiro e gerência) e que lá exista uma única rede de computadores que usa uma das faixas de endereços reservadas para rede privada: a rede 192.168.1.0/24 (uma rede de classe C). O /24 é outra forma de representar a máscara 255.255.255.0, pois ele indica o numero de bits 1 na máscara. Essa rede, com essa máscara, é composta dos seguintes endereços: 192.168.1.0 até o 192.168.1.255, ou seja, 256 IPs. Porém, não poderemos usar nem o primeiro nem o último endereço (192.168.1.0 e o 192.168.1.255), pois eles são usados para representar a própria rede e o endereço de broadcast, respectivamente. Mas o que isso significa? Bem, o endereço de rede identifica toda a rede, conforme já falamos anteriormente, ou seja, todos os hosts da rede, e o endereço de broadcast é usado quando se deseja enviar informações para todos os hosts na rede. Desse modo, temos na verdade 254 endereços disponíveis.

Com o passar do tempo, você decide separar a sua rede por setor, fazendo com que cada setor tenha sua própria rede. Então, como faremos essa divisão? Bem, nós precisaremos modificar a máscara de rede. Como você viu na Tabela 3, uma rede de classe C, tem na sua máscara padrão, 24 bits definidos como 1 em binário, o que em decimal seria: 255.255.255.0. Para criarmos as sub-redes, precisaremos pegar alguns bits da parte de host e colocarmos na parte de rede. Na literatura, é comum usar o termo “pegar emprestado” bits para criarmos as sub-redes. Mas, como saberemos quantos bits são necessários? Veja, se pegarmos um bit faremos 2^1 = 2 sub-redes, se pegarmos 2 bits faremos 2^2 = 4 e se pegarmos 3 bits teremos 2^3 = 8 sub-redes e assim por diante.

No nosso exemplo, como queremos criar 4 sub-redes, devemos pegar emprestado 2 bits da parte de host, que antes tinha 8 bits para endereçar os hosts, dando um total de 256 endereços, e agora ficará apenas com 6 bits e um total de 64 endereços (26). Desse modo, a máscara de rede que tinha 24 bits definidos em 1 ficará agora com 26 bits em 1. Na **Figura 2**, a parte na cor cinza representa a parte de rede do endereço IP, a parte verde representa as 4 sub-redes possíveis usando dois bits e a parte amarela é a parte usada para endereçar os hosts de cada sub-rede. Como temos 6 bits, teremos um total de 2^6 IPs por sub-rede, mas lembre-se de que não podemos usar nem o primeiro nem o último IP de cada sub-rede, conforme mostramos antes, por se tratarem do endereço de rede e de broadcast. Deixando 62 endereços disponíveis $(2^6 - 2)$

Figura 02 - Sub-redes (representação em binário e em decimal).



Fonte: Autoria própria.

A **Tabela 4** mostra as variações de IPs possíveis, representados em decimal, para cada sub-rede. Lembre-se de que cada endereço de rede tem 4 bytes, de modo que os endereços das sub-redes são: 192.168.1.0, 192.168.1.64, 192.168.1.128 e 192.168.1.192. Observe também que cada rede agora tem apenas 64 endereços (incluindo os de rede e broadcast). Isso é natural, pois criar as sub-redes não aumenta os endereços disponíveis.

Endereço de rede (reservado)	Primeiro endereço disponível	Último endereço disponível	Endereço de broadcast (reservado)
192.168.1.0	192.168.1.1	192.168.1.62	192.168.1.63
192.168.1.64	192.168.1.65	192.168.1.126	192.168.1.127
192.168.1.128	192.168.1.129	192.168.1.190	192.168.1.191
192.168.1.192	192.168.1.193	192.168.1.254	192.168.1.255

Tabela 4 – Endereços das 4 sub-redes em decimal

É importante observar que a máscara de sub-redes funciona de maneira hierárquica e é normalmente aplicada internamente em uma organização. Isso quer dizer que para o exterior, a rede continua sendo vista como uma rede /24, mas internamente é vista como várias sub-redes /26. Com isso, os roteadores de fora da organização só precisam saber para onde enviar pacotes para a rede 192.168.1.0/24, enquanto que os roteadores de dentro da organização tomam conhecimento dos outros 2 bits que foram emprestados para a criação das 4 sub-redes e encaminham o pacote para sua rede final. Dessa maneira, roteadores diferentes consideram um número de bits diferentes para a parte de rede.

Para entender melhor, faça uma analogia com o sistema de entrega de cartas e encomendas por correio. As cartas são normalmente encaminhadas para uma central de processamento no estado de destino e de lá encaminhadas para a cidade de destino. Para centrais de processamento em outros estados, a única informação relevante é o estado de destino (os primeiros 24 bits usados), enquanto que para centrais dentro do estado de destino, a informação relevante é a cidade de destino (os 2 bits que foram emprestados da parte de host).

Atividade 03

1. Identifique o endereço de rede do IP 201.85.27.190 com máscara de sub-rede 255.255.240.0. Para ajudar, fornecemos os equivalentes em binário.

201.85.27.190	11001001.01010101.00011011.10111110
255.255.240.0	11111111.11111111.11110000.00000000

2. Suponha que você tenha a seguinte rede classe C: 192.168.100.0/24 e quer dividi-la em 8 sub-redes. Sendo assim, responda as questões a seguir.
    a. Quantos bits você precisará usar para criar as sub-redes?
    b. Qual o endereço de rede e de broadcast de cada sub-rede?
    c. Qual é a nova máscara de sub-rede?
    d. Quantos hosts poderão ser endereçados em cada nova sub-rede?

Respostas

Respostas

1. | | |
   |---|---|
   | 201.85.27.190 | 11001001.01010101.00011011.10111110 |
   | 255.255.240.0 | 11111111.11111111.11110000.00000000 |

   Aplicando a regra do AND, o endereço de rede do IP 201.85.27.190 é 201.85.16.0.

2. a. Dois bits para criar as quatro sub-redes.

   b.
   - Sub-rede 1: broadcast = 192.168.100.63 e sub-rede = 192.168.100.0
   - Sub-rede 2: broadcast = 192.168.100.127 e sub-rede = 192.168.100.64
   - Sub-rede 3: broadcast = 192.168.100.191 e sub-rede = 192.168.100.128
   - Sub-rede 4: broadcast = 192.168.100.255 e sub-rede = 192.168.100.192

   c. 255.255.255.192

   d. 62

Leitura complementar

- <http://www.juliobattisti.com.br/artigos/windows/tcpip_p7.asp> - Nesse site, você encontrará como fazer a divisão de uma rede em sub-redes.

- <http://pt.wikipedia.org/wiki/Endereço_IP> - Nesse site, você encontrará uma boa definição de endereçamento, classes de endereços IPs, além de outras informações.

- <http://www.juliobattisti.com.br/artigos/windows/tcpip_p3.asp> - Esse site faz uma introdução ao endereçamento IP e mostra como são feitos os cálculos em binário.

- <http://www.subnet-calculator.com/>

- <http://jodies.de/ipcalc> - Nesses dois endereços, você acessará ferramentas que auxiliarão nos cálculos para criação de sub-redes.

Resumo

Estudamos nesta aula a definição do principal protocolo da Internet, o protocolo IP. Estudamos também o esquema de endereçamento IP e vimos que um endereço IP possui uma parte que identifica a rede e outra que identifica as máquinas da rede. Outro ponto importante foi o gerenciamento e criação de sub-redes através de máscaras de sub-redes.

Autoavaliação

1. Para que serve uma máscara de rede?

2. Quantos *hosts* uma rede classe C com sua máscara padrão poderá endereçar?

3. Suponha que você tem a seguinte rede: 19.168.100.0/24 e queira dividi-la em 6 sub-redes, responda:

    a. Qual será a nova máscara de rede?

    b. Qual o endereço de *broadcast* da primeira e da última sub-rede?

    c. Quantos bits da parte de *host* você usou para criar as sub-redes?

    d. Como fica a nova máscara de rede no formato decimal?

Respostas

Respostas

1. A mascara de sub rede serve para separar em um IP a parte correspondente à rede, às sub redes e aos hosts das sub redes.
2. 254 hosts pois ainda existem o endereço de rede e o de broadcast.
3.

    a. 11111111.11111111.11111111.11100000

    b. 19.168.100.32 e 19.168.100.255 (na verdade são criadas 8 sub-redes e não 6 sub-redes pois são necessários 3 bit para criar as subredes.

    c. 3 bits

    d. 255.255.255.224

Referências

KUROSE, J.; ROSS, K. **Redes de computadores e a internet.** 5. ed. São Paulo: Addison Wesley, 2010.

TANENBAUM, Andrew S. **Redes de computadores e a internet.**. 4 ed. Rio de Janeiro: Editora Elsevier, 2003.

SOARES, l. F. G. **Redes de computadores das LANs, MANs e WANs às redes ATM**. 2. ed. São Paulo: Editora Campus, 1995.

FOROUZAN, B. **Comunicação de Dados e Redes de Computadores.** 3. ed. Porto Alegre: Bookman, 2006.