N_COM_DAD_A5 - Texto de apoio

Site: EAD Mackenzie
Tema: COMUNICAÇÃO DE DADOS {TURMA 03B} 2023/1
Livro: N_COM_DAD_A5 - Texto de apoio

Impresso por: FELIPE BALDIM GUERRA .
Data: domingo, 30 abr 2023, 01:37

Índice

1. Introdução

Até o momento, em nossa disciplina de Comunicação de dados, conhecemos os principais serviços/ aplicações de redes e a forma como a camada de transporte oferece suporte para a camada de aplicação, auxiliando na comunicação entre processos em execução em sistemas finais distintos.

O estudo sobre a camada de Internet ou camada de redes (modelo OSI) é uma tarefa primordial e desafiadora, pois a camada de Internet é a responsável por implementar o serviço de entrega de pacotes entre sistemas finais, logo, o objetivo deste Texto de Apoio é compreender como se dá a transferência de pacotes entre sistemas finais por meio de uma infraestrutura composta por diversos dispositivos intermediários (também referidos como nós, hops ou saltos), bem como estudar os diversos protocolos desenvolvidos para a execução destas tarefas.

Nesta Aula 5, nossos estudos serão concentrados em apresentar os serviços oferecidos pela camada de rede, a versão 4 do protocolo da Internet (Internet Protocol – IPv4), os protocolos ICMP (Internet Control Message Protocol), DHCP (Dynamic Host Configuration Protocol) e o NAT (Network Address Translation).

2. Serviços da camada de Internet

A camada de Internet ou camada de rede é responsável por encapsular a chamada carga útil ou *payload* (Forouzan, 2010) e implementar um serviço de conexão de rede transparente para as camadas superiores que permite a entrega dos pacotes ao seu destino, independentemente da complexidade das redes utilizadas na execução da tarefa. Dentre as principais funções da camada de rede, podemos citar:

Encapsulamento – Na origem da mensagem, a camada de rede encapsulará os segmentos oriundos da camada de transporte com um cabeçalho contendo informações como endereços de origem e destino, bem como outros dados necessários para a entrega desse pacote. Quando um pacote chega a seu destino, a camada de rede desencapsulará o pacote e entregará o segmento à camada de transporte.

Roteamento – Denominamos roteamento a ação desempenhada por algoritmos que têm como objetivo encontrar a melhor rota entre dois sistemas finais conectados por meio de uma internet ou da Internet. Os algoritmos de roteamento serão discutidos na Aula 6 de nosso curso.

Encaminhamento – Durante o roteamento, cada dispositivo no núcleo da rede (roteadores) gerará uma tabela de repasse ou uma tabela de roteamento. Quando um pacote qualquer chegar a esse dispositivo, o roteador analisará as informações do cabeçalho da camada de rede, consultará a tabela de roteamento e encaminhará o pacote para uma interface de saída.

Além dos serviços básicos citados acima, a camada de rede **pode** oferecer os seguintes serviços:

Qualidade de serviço – Devido ao crescimento e à diversificação dos serviços disponíveis na Internet, oferecer tratamento preferencial a determinados tipos de tráfego em detrimento de outros tornou-se um recurso importante nas redes modernas. A qualidade dos serviços de rede (QoS – *Quality of Service*) pode ser implementada na camada de rede para dar suporte no encaminhamento de pacotes de serviços de voz e vídeo.

Segurança – Um problema gerado com o crescimento da Internet foi o aumento das vulnerabilidades de rede e o crescimento de ciberataques. Para mitigar as vulnerabilidades a nível da camada de rede, surgiu o IPsec (IP Security), que oferece uma comunicação segura (criptografada) entre dois ou mais hosts em uma rede.

Além das funções citadas acima, a camada de rede podo oferecer dois tipos de serviço: Rede de circuitos virtuais e rede de datagramas (comutação de pacotes).

As **redes de circuitos virtuais** oferecem um serviço de rede orientado a conexão em que todos os pacotes trafegarão por uma mesma rota pré-estabelecida entre origem e destino (Kurose, 2013). Esse tipo de serviço que permite estabelecer uma rota (circuito) entre dois pontos da rede, dependendo da tecnologia de circuito virtual utilizada, garante que os pacotes trafeguem por esse circuito com uma largura de banda constante (ou uma largura de banda mínima) e pode garantir, também, em alguns casos, que todos os pacotes transmitidos chegarão ao destino na ordem em que foram enviados. Embora as redes de circuitos virtuais ofereçam os benefícios citados acima, alocar (contratar) um circuito virtual é muito dispendioso.

As **redes de datagramas** ou **redes comutação de pacote** oferecem um serviço não orientado à conexão. Nesse serviço conhecido como "serviço do melhor esforço" (Kurose, 2013), não há a criação de um circuito entre origem e destino, logo, cada pacote pode seguir por uma rota distinta, pois os roteadores no núcleo da rede tratarão cada pacote recebido de forma independente (Forouzan, 2010). Apesar de não oferecer garantias na entrega dos pacotes nem uma taxa de transmissão constante, a adoção de redes de comutação de pacotes permite o uso mais eficiente dos recursos de infraestrutura, possibilitando o compartilhamento da largura de banda disponível com diversos usuários e, consequentemente, resultando na redução dos custos na contratação dos serviços de redes. Devido à possibilidade de escalabilidade e impondo exigência mínima sobre a camada de rede (Kurose, 2013), a rede de datagramas é o método de transmissão da Internet.

3. PROTOCOLO DA INTERNET – IP (INTERNET PROTOCOL)

Após apresentar, de maneira geral, as características da camada de rede, iniciaremos nossos estudos sobre o protocolo IP. Projetado para ser um protocolo de interligação de redes, o IP permite a entrega de datagramas para destinos na mesma rede ou em destinos que são acessados por meio de redes intermediárias (Tanenbaum, 2010). Como todo dispositivo de rede deve possuir um endereço fornecido pelo protocolo IP, o roteamento de datagramas inter-redes usa como base o campo do cabeçalho IP em que está contido o endereço de destino do datagrama.

Atualmente, há duas versões do protocolo IP: IPv4 e IPv6. Nesta aula, focaremos na versão 4 do protocolo (IPv4), apresentando informações como o formato do datagrama e o endereçamento. A versão 6 do protocolo IP (IPv6) será comentada somente na Aula 6.

4. Protocolo IPv4

O cabeçalho IPv4 possui 20 bytes de informações fixas (sem a adição de informações no campo opção), e os principais campos desse cabeçalho serão apresentados na sequência:

Versão – indica a versão do protocolo IP utilizado (neste caso, a versão IPv4).

Comprimento de cabeçalho – como o campo opções pode gerar um datagrama com tamanho superior a 20 bytes, esse campo refere-se ao número de palavras de 32 bits que constitui o cabeçalho.

Tipo do serviço – Atualmente chamado de serviços diferenciados, esse campo indica a maneira segundo a qual o datagrama deve ser tratado em função de seu serviço.

Comprimento do datagrama – esse campo apresenta o comprimento do datagrama (cabeçalho e dados) em bytes.

Identificador, flags e fragmentação offset – fragmentação IP é a operação que permite dividir um datagrama IP em datagramas de tamanho menor para atender a eventuais necessidades específicas no núcleo da rede. Os campos identificador, flag e fragmentação permitem controlar a divisão e a reconstrução de datagramas que precisaram ser fragmentados.

Tempo de vida (Time to live – TTL) – é o campo usado para controlar a vida útil de um datagrama. Implementado por meio de um número que será decrementado de uma unidade cada vez que o datagrama passar por um roteador, quando o valor do TTL chegar a 0, o pacote será descartado pelo roteador, evitando, assim, que um datagrama perdido fique circulando infinitamente pela rede.

Protocolo da camada superior – esse campo informa o protocolo que está encapsulado no datagrama. Representado por um número atribuído pela IANA (Internet Assigned Numbers Authority), podemos citar como exemplo os protocolos ICMP (1), IGMP (2), TCP (6) e UDP (17), nos quais o número entre parênteses representa os códigos atribuídos pela IANA aos respectivos protocolos citados.

Soma de verificação – a soma de verificação permite ao protocolo IP detectar erros e garantir que o cabeçalho IP não foi corrompido durante a transmissão (garante integridade). Esse campo tem função diferente da soma de verificação realizada na camada de transporte, pois a camada de rede não verifica a integridade dos dados transportados por ela, somente a integridade do cabeçalho IP.

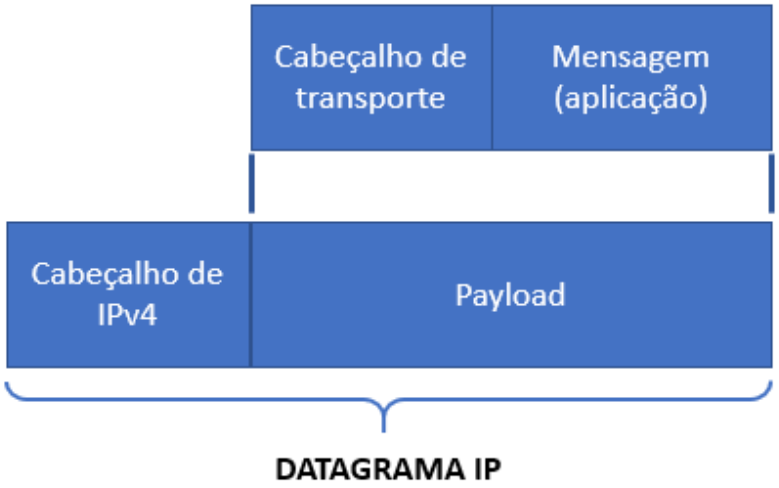
Endereço IP de origem e Endereço IP de destino – esses dois campos representam, respectivamente, o endereço do host que originou a mensagem e o endereço do host para o qual a mensagem será enviada. Detalhes sobre o endereçamento IP serão discutidos na sessão subsequente.

Opções – esse campo permite que o cabeçalho IP seja ampliado com informações inexistentes no projeto original do protocolo (Tanenbaum, 2010). Sua utilização não é recomendada devido à sobrecarga gerada no processamento dos datagramas.

Dados (das camadas superiores) – esse campo representa os dados encapsulados pelo datagrama IP oriundos da camada de transporte ou de outra natureza, como informações referentes ao protocolo ICMP (que serão discutidas em outro momento).

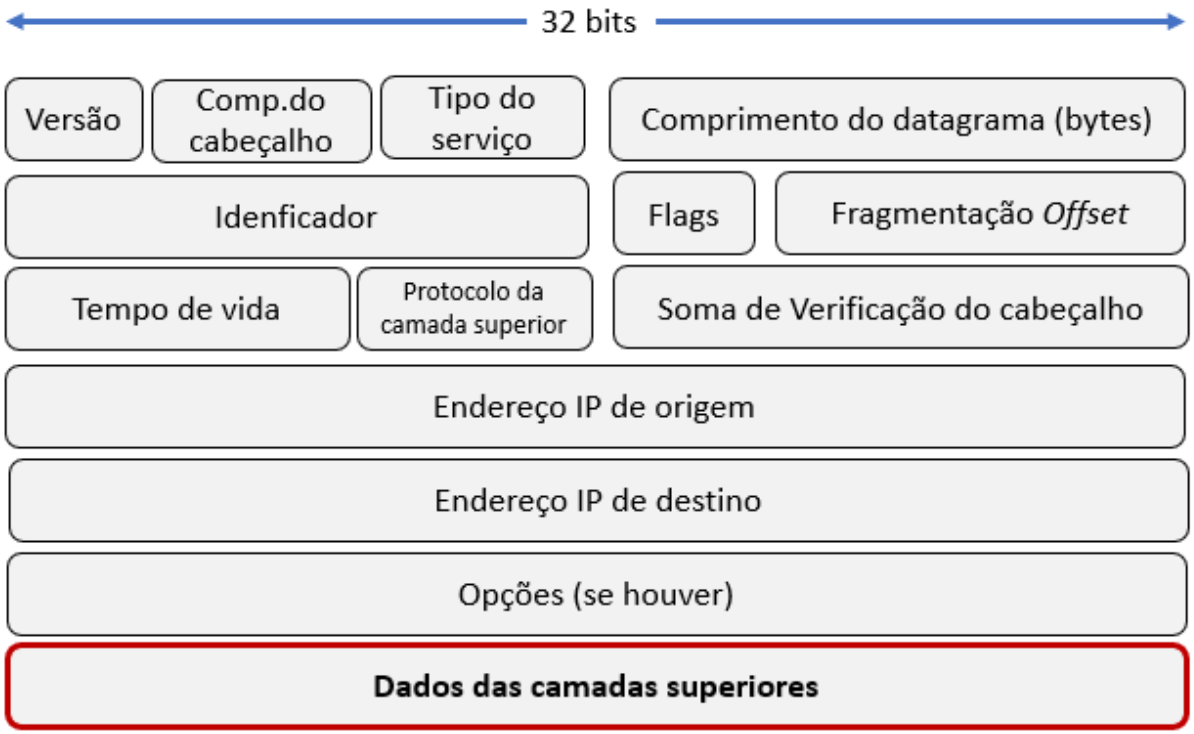
Iniciaremos nosso estudo sobre o Protocolo IPv4 pela estrutura do datagrama IP. Conforme apresentado na Figura 1, o datagrama IPv4 é composto pelos dados enviados pela camada de transporte e pelo cabeçalho IPv4 (Figura 2) que encapsulará esses dados.

Figura 1 – Datagrama IPv4



Fonte: Elaborada pelo autor.

Figura 2 – Formato do cabeçalho IPv4



Fonte: Elaborada pelo autor.

O cabeçalho IPv4 possui 20 bytes de informações fixas (sem a adição de informações no campo opção), e os principais campos desse cabeçalho serão apresentados na sequência:

Versão – indica a versão do protocolo IP utilizado (neste caso, a versão IPv4).

Comprimento de cabeçalho – como o campo opções pode gerar um datagrama com tamanho superior a 20 bytes, esse campo refere-se ao número de palavras de 32 bits que constitui o cabeçalho.

Tipo do serviço – Atualmente chamado de serviços diferenciados, esse campo indica a maneira segundo a qual o datagrama deve ser tratado em função de seu serviço.

Comprimento do datagrama – esse campo apresenta o comprimento do datagrama (cabeçalho e dados) em bytes.

Identificador, flags e fragmentação offset – fragmentação IP é a operação que permite dividir um datagrama IP em datagramas de tamanho menor para atender a eventuais necessidades específicas no núcleo da rede. Os campos identificador, flag e fragmentação permitem controlar a divisão e a reconstrução de datagramas que precisaram ser fragmentados.

Tempo de vida (Time to live – TTL) – é o campo usado para controlar a vida útil de um datagrama. Implementado por meio de um número que será decrementado de uma unidade cada vez que o datagrama passar por um roteador, quando o valor do TTL chegar a 0, o pacote será descartado pelo roteador, evitando, assim, que um datagrama perdido fique circulando infinitamente pela rede.

Protocolo da camada superior – esse campo informa o protocolo que está encapsulado no datagrama. Representado por um número atribuído pela IANA (Internet Assigned Numbers Authority), podemos citar como exemplo os protocolos ICMP (1), IGMP (2), TCP (6) e UDP (17), nos quais o número entre parênteses representa os códigos atribuídos pela IANA aos respectivos protocolos citados.

Soma de verificação – a soma de verificação permite ao protocolo IP detectar erros e garantir que o cabeçalho IP não foi corrompido durante a transmissão (garante integridade). Esse campo tem função diferente da soma de verificação realizada na camada de transporte, pois a camada de rede não verifica a integridade dos dados transportados por ela, somente a integridade do cabeçalho IP.

Endereço IP de origem e Endereço IP de destino – esses dois campos representam, respectivamente, o endereço do host que originou a mensagem e o endereço do host para o qual a mensagem será enviada. Detalhes sobre o endereçamento IP serão discutidos na sessão subsequente.

Opções – esse campo permite que o cabeçalho IP seja ampliado com informações inexistentes no projeto original do protocolo (Tanenbaum, 2010). Sua utilização não é recomendada devido à sobrecarga gerada no processamento dos datagramas.

Dados (das camadas superiores) – esse campo representa os dados encapsulados pelo datagrama IP oriundos da camada de transporte ou de outra natureza, como informações referentes ao protocolo ICMP (que serão discutidas em outro momento).

5. Endereçamento IPv4

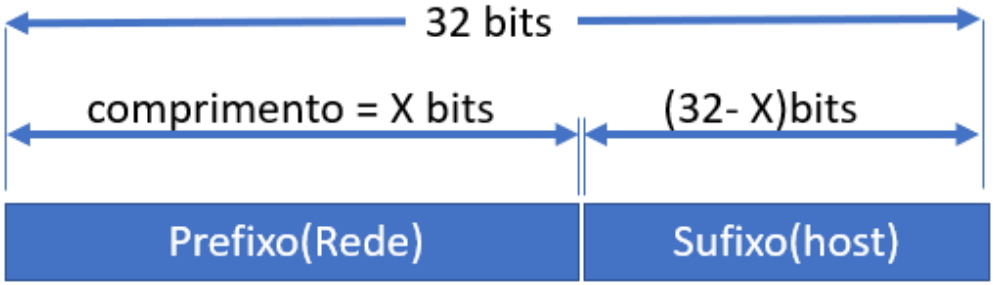
O endereçamento lógico IPv4 foi implementado utilizando um número de 32 bits, que permite endereçar aproximadamente 4,29 bilhões de equipamentos (2^{32} = 4,29x10^{9}). Esse endereçamento é representado por meio de quatro conjuntos de 8 bits (octetos), nos quais cada octeto é separado por ponto. A representação do endereço IP para usuário é realizada por um número decimal. Abaixo, temos um exemplo do endereço IPv4 em binário separado por octetos e seu equivalente em decimal:

Endereço binário	11000000.	10101000.	00000001.	00000101.
Endereço decimal	192 .	168 .	1 .	5

Conforme citado por Tanenbaum (2010), na prática, o endereço IP é associado a cada interface de rede, e não a um host específico, ou seja, se um host estiver conectado a duas redes, serão necessárias duas interfaces de rede distintas com dois endereços IP diferentes. Esse fato gera muita confusão, pois, quando pensamos em endereços IP, associamos que cada computador possui um endereço IP, o que, intuitivamente, não é errado, pois, em geral, os computadores domésticos pertencem a uma única rede. Esse fato leva muitas pessoas a associar que não só os computadores, mas todos os dispositivos de rede têm um único endereço IP – o que não é verdade, pois roteadores possuem várias interfaces (normalmente, ligadas a diferentes redes), o que demanda a atribuição de diferentes endereços IP, um endereço para cada interface do roteador.

Outra característica importante do endereçamento da camada de rede é o fato de o endereço IP ser hierárquico. Dividido em duas partes, o endereço IP possui uma parte chamada de prefixo, cuja sequência numérica define o endereço da rede, e uma segunda parte (sufixo) que determina o nó específico na rede. A Figura 3 apresenta um diagrama com o prefixo e o sufixo de um endereço IPv4 de 32 bits.

Figura 3 – Diagrama com o prefixo e o sufixo de um endereço IPv2 de 32 bits

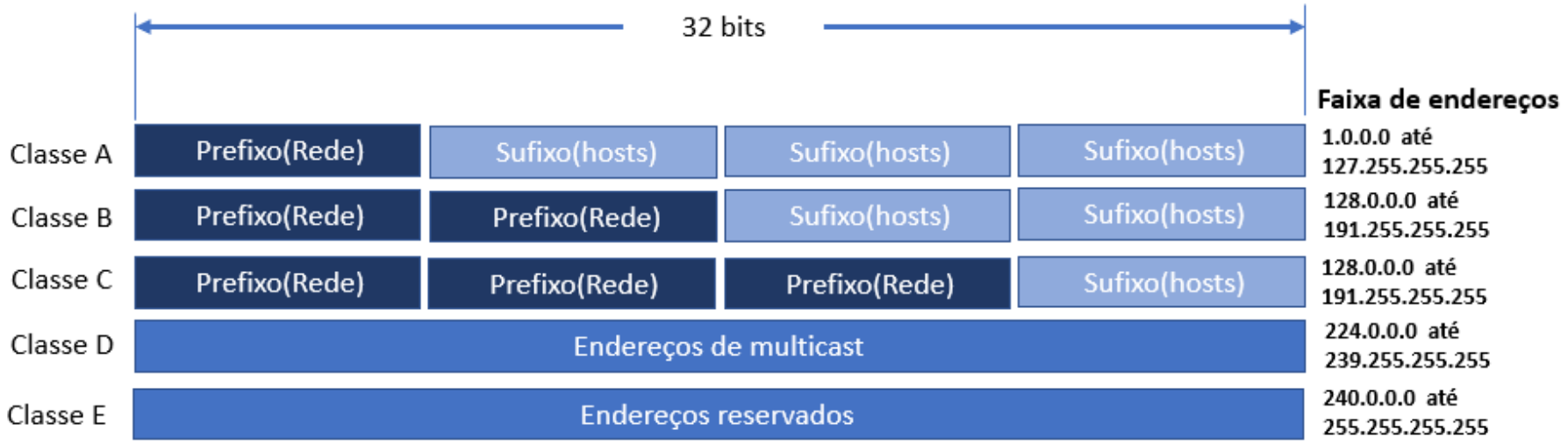


Fonte: Elaborada pelo autor.

Na Figura 3, temos uma representação do endereço IPv4 com seu tamanho de 32 bits dividido em prefixo de rede e sufixo. Se o prefixo de rede possui X bits, o sufixo de rede será a diferença do total de bits (32 bits) do endereço e o número de bits utilizados no prefixo de rede.

Para facilitar a manipulação dos endereços IPv4, incialmente, as redes foram projetadas para usar endereços IP com prefixos de comprimento fixo. Esse tipo de endereçamento ficou conhecido como endereçamento de classes ou classful. No sistema classful, os endereçamentos IP disponíveis são divididos em cinco classes (classe A, B, C, D e E), conforme mostra a Figura 4.

Figura 4 – Formato dos endereços IPv4 Classful



Fonte: Elaborada pelo autor.

O uso do endereçamento de diferentes classes de redes com tamanhos diferentes, onde foi determinada uma faixa de endereçamento específica para cada classe. Essas faixas de endereçamento foram criadas de modo a facilitar a extração das informações, como prefixo e sufixo de rede. Em resumo das informações da Figura 4 temos:

Endereços da classe A – usados por redes grandes, dedicam um octeto do endereçamento IP como sufixo de rede e os demais octetos para endereçar hosts na rede.

Endereços da classe B – usados em redes de porte médio, alocam dois octetos do endereçamento IP como sufixo de rede e os outros dois octetos para endereçar hosts na rede.

Endereços da classe C – usados para redes de porte pequeno. As redes classe C dedicam três octetos do endereçamento IP como sufixo de rede e somente um octeto para endereçar hosts na rede.

Endereços da classe D – não é dividida em prefixo e sufixo, pois essa faixa de endereçamento é usada para comunicação multicast.

Endereços da classe E – assim como os endereços de classe D, essa classe não é dividida em prefixo e sufixo e seus endereços foram reservados para uso futuro.

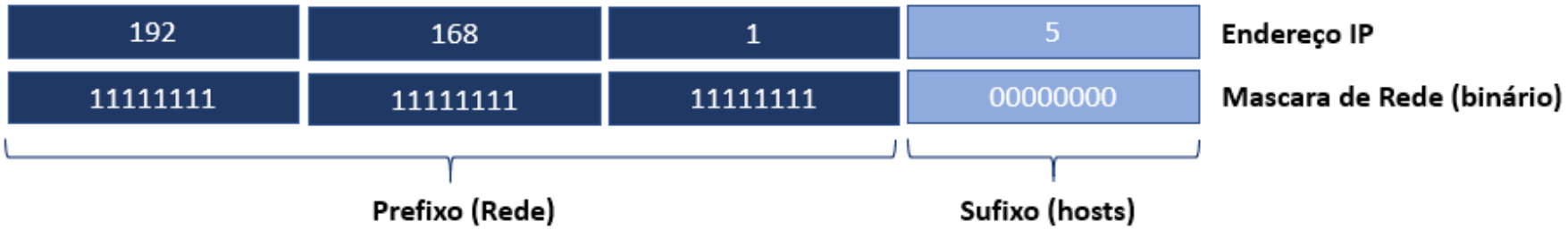
Devido à falta de flexibilidade na alocação dos endereços e, principalmente, no tamanho das redes (só era possível criar redes de três tamanhos), o padrão conhecido como **classful** se tornou obsoleto (Forouzan, 2010), dando lugar ao padrão de endereçamento sem classes (**classless**).

Ao contrário do **classful**, o padrão **classless** utiliza prefixos de rede de comprimento variável que podem melhor atender às demandas dos projetistas de redes.

6. Máscara de rede

Para determinar o tamanho do prefixo e, consequentemente, do sufixo implícito no endereço IPv4, foi necessária a criação da máscara de rede (ou máscara de sub-rede). Assim como o endereço IP, a máscara de rede também é um número inteiro com 32 bits (separada por octetos) no qual o prefixo de rede é representado pelo bit “1” e o sufixo pelo bit “0”. A Figura 5 mostra um exemplo em que o prefixo e o sufixo da rede serão determinados pela sequência de bits da máscara de rede:

Figura 5 – Determinação de Prefixo de rede por meio de uma máscara de rede



Fonte: Elaborada pelo autor.

Notamos na Figura 5 que a máscara está em binário e que os octetos preenchidos com o bit 1 indicam o prefixo de rede. Apesar da Figura 5 mostrar uma representação da máscara em binário, assim como já ocorre com o endereço IPv4, quando vamos configurar a máscara de rede em nossos dispositivos, usamos a notação em decimal.

Usando a numeração decimal, as redes das classes A, B, e C possuem as seguintes máscaras:

Classe A	255.0.0.0
Classe B	255.255.0.0
Classe C	255.255.255.0

Outra maneira de representar as máscaras de rede é simplesmente descrever o tamanho do prefixo de rede no seguinte formato “/nº de bit do prefixo” logo após o endereço IP. Usando essa notação para representar o endereço e a máscara de rede presente na Figura 5, teríamos o seguinte endereço “**192.168.1.5/24**”. Essa notação é conhecida como notação CIDR (Classless Inter-Domain Routing).

Uma rede IP pode ser dividida em unidades menores chamadas sub-redes. As sub-redes oferecem uma flexibilidade adicional ao administrador de redes devido à possibilidade de criar várias redes lógicas dentro de uma rede única de classe A, B ou C.

7. Tipos de endereços IPv4

Devido ao número crescente de pessoas e dispositivos conectados à Internet, os analistas e projetistas de redes perceberam que, apesar dos mais de 4 bilhões de endereços IPv4 disponíveis, seria necessário atribuir faixas de IPs que só poderiam ser usadas em funções específicas, como as que só podem ser usadas em redes privadas. Uma visão geral sobre a designação das diferentes faixas de IPs, bem como os diferentes tipos de endereços serão discutidos em uma videoaula do Professor Resolve.

8. OUTROS PROTOCOLOS E SERVIÇOS RELACIONADOS À CAMADA DE INTERNET

a

8.1. Protocolo ICMP

O Protocolo ICMP (Internet Control Message Protocol) é responsável por testar e reportar erros por meio do envio de mensagens para o endereço IP de origem. Cerca de 12 tipos de mensagens ICMP podem ser encapsuladas em um datagrama IP, dentre as quais podemos citar: Destination Unreachable – mensagem recebida quando um host não pode localizar o destino especificado no datagrama. Time Exceeded – mensagem recebida pelo emissor do datagrama quando um pacote é descartado em função do contador TTL chegar a zero. Esse recurso é utilizado de maneira muito inteligente pelo utilitário Traceroute. Parameter Problem – indica que um valor ilegal foi detectado no cabeçalho IP. Echo e Echo Reply – solicitação de uma resposta (eco) de determinado host para verificar se este está ativo (ligado e conectado à rede). Esses tipos de mensagens são usados pelo utilitário ping que, além de informar se o host está ativo ou não, indica o tempo necessário para enviar e receber uma mensagem a esse host. Além das mensagens citadas, uma lista completa dos recursos do protocolo ICMP podem ser estudadas na RFC 792.

8.2. Protocolo DHCP

O DHCP (Dynamic Host Configuration Protocol) é um protocolo da camada de aplicação que permite a um hospedeiro obter dinamicamente seu IP do servidor de rede quando se conectar à rede. Para executar essa operação, é necessário um servidor DHCP (muitas vezes, essa função de roteador DHCP é realizada por um roteador) que mantém uma base de endereços IP. Toda vez que um host se conectar à rede e não tiver um endereço IP configurado, o protocolo DHCP solicitará ao servidor um endereço IP válido que permita ao host usufruir dos serviços da rede.

8.3. Network Address Translation – NAT

O rápido crescimento da Internet impôs diversos desafios para os arquitetos de redes, pois, à medida que novos usuários ou serviços eram adicionados à Internet, o número de endereços IPv4 disponíveis para conectar esses novos usuários ou serviços iam se extinguindo. O problema da rápida atribuição e esgotamento dos mais de 4 bilhões de endereços IPv4 não é algo teórico nem um problema para se preocupar no futuro, é um problema atual e já demandou o desenvolvimento de soluções que diminuíssem a atribuição de endereços IPv4. Dentre as soluções propostas, podemos citar o NAT. Essa solução descrita na RFC 3022 permite que todos os sistemas finais de uma rede local que usam endereços privados acessem a Internet usando um único endereço público, fornecido pelo provedor de Internet (ISP). Para que isso seja possível, quando um computador de uma rede local que possui um endereço IP privado for acessar a Internet, o NAT converterá o endereço IP privado dos pacotes que serão enviados para a Internet no endereço IP público da rede. O processo inverso de conversão ocorre quando um pacote vindo da rede pública chega ao NAT com destino a um host da rede local.

9. REFERÊNCIAS

FOROUZAN, B. A. Comunicação de dados e Redes de computadores. 3. ed. Porto Alegre: Bookman, 2010.

KUROSE, J. F.; ROSS, K. W. Redes de computadores e a internet: uma abordagem top-down. 6. ed. São Paulo: Pearson, 2013 | Biblioteca Virtual Universitária — Pearson.

SILBERSCHATZ, A.; GALVIN, P. B.; GAGNE, G. Fundamentos de Sistemas Operacionais: princípios básicos. São Paulo: LTC, 2015.

TANENBAUM, A. Redes de computadores. 5. ed. São Paulo: Pearson, 2010 | Biblioteca Virtual Universitária — Pearson.