

INTERCONEXÃO E PROTOCOLOS DE REDES MODELO TCP/IP

Autor: Me. Ramiro Sebastião Córdova Junior

Revisor: Luciana de Castro Lugli

INICIAR

introdução

Introdução

O modelo TCP/IP, assim como o modelo OSI, tem como objetivo estabelecer padrões para a comunicação em rede. A internet é o melhor exemplo de aplicação do modelo TCP/IP, tanto que, por vezes, as nomenclaturas se confundem e tornam comum referenciar o modelo TCP/IP como sendo o protocolo da internet. Isso se deve ao fato de que os serviços de rede utilizados em larga escala na internet utilizam os protocolos TCP e IP.

Sendo assim, ao longo desta unidade, serão apresentados os conceitos que permeiam o modelo TCP/IP e suas quatro camadas. Juntamente com a teoria referente às características das camadas, serão apresentados os protocolos mais usuais das camadas de aplicação, de rede e de transporte. Já os protocolos serão apresentados juntamente com exemplos que facilitam o entendimento de seu funcionamento.

Pilha de Protocolos TCP/IP

Na década de 1960, o Departamento de Defesa dos Estados Unidos iniciou o desenvolvimento de uma rede de comunicações que deveria ser à prova de ataques. Essa rede foi batizada com o nome de DARPANET (Defense Advanced Research Projects Agency). A ideia era basicamente ter um sistema que fosse descentralizado, em que, mesmo com o comprometimento de partes da rede de comunicação, ainda pudesse haver comunicação.

O modelo TCP/IP (Transmission Control Protocol/ Internet Protocol) teve sua origem a partir a evolução da DARPANET, que veio a ser batizada como ARPANET. Essa rede, além de interconectar bases militares, também interconecta algumas universidades americanas. Os conceitos do modelo OSI têm muitas aplicações do modelo TCP/IP, porém, como teve origem para fins militares, o modelo TCP/IP se tornou mais conhecido após o lançamento do modelo OSI. Pode-se dizer que o modelo TCP/IP é uma versão mais objetiva do modelo OSI, composto por quatro camadas, que formam a pilha de protocolos TCP/IP:

- Camada de Aplicação;
- Camada de Transporte;
- Camada de Rede;

- Camada Física.

Na Figura 3.1, é possível analisar uma comparação entre as camadas do modelo OSI e as camadas do modelo TCP/IP. Grande parte dos conceitos utilizados no modelo OSI são aplicados ao modelo TCP/IP, inclusive, durante a concepção dos dois modelos, houve interações entre os envolvidos.

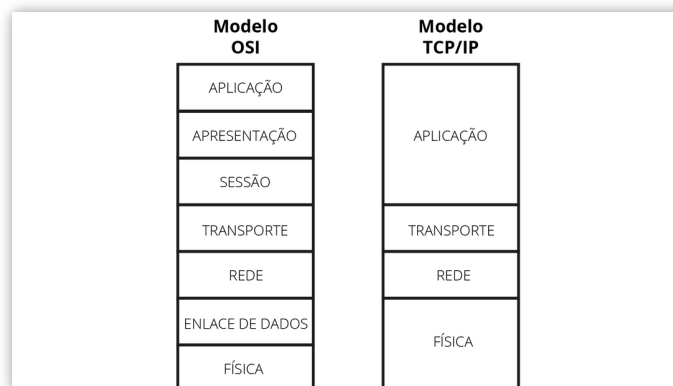


Figura 3.1 - Comparação entre Modelo OSI e o modelo TCP/IP

Fonte: Elaborada pelo autor.

O modelo TCP / IP especifica como os dados devem trafegar pela internet, como eles devem ser divididos em pacotes, endereçados, transmitidos, roteados e recebidos no destino. O TCP / IP requer pouco gerenciamento central e foi desenvolvido para tornar as transmissões confiáveis, com a capacidade de se recuperar automaticamente de eventuais falhas em qualquer dispositivo na rede. Isoladamente, TCP e IP são protocolos de rede e, para o funcionamento da internet, são os principais protocolos (COMER, 2016).

saiba mais

Saiba mais

Você sabia que é possível analisar o padrão de tráfego em uma rede TCP/IP e a partir de análises detectar alguma intrusão na rede? Para saber mais detalhes sobre o assunto, leia a dissertação de mestrado intitulada: “Análise de estado de tráfego de redes TCP/IP para aplicação em detecção de intrusão” para saber mais a respeito.

ACESSAR

O protocolo TCP define como as aplicações podem criar canais de comunicação em uma rede, além de gerenciar como uma mensagem é montada em pacotes menores antes de serem transmitidos pela internet e remontados na ordem certa no endereço de destino. O protocolo IP define como endereçar e rotear cada pacote para garantir que chegue ao destino correto. Cada roteador existente na rede verifica o endereço IP para determinar para onde encaminhar a mensagem.

O modelo de comunicação utilizado pelo TCP/IP é o cliente/servidor, em que um usuário ou computador (cliente) “recebe” um serviço (como, por exemplo, o envio de uma página da web) por outro computador (servidor) na rede.

Sendo assim, a seguir serão detalhadas as quatro camadas que compõem o modelo TCP/IP.

Camada de Aplicação

Essa camada interage com os softwares aplicativos utilizados pelos usuários. Por isso, é a camada de mais alto nível do modelo TCP/IP, pois é nela que são definidos os protocolos utilizados pelas aplicações. Ou seja, não existe um protocolo padrão para ela (KOZIEROK, 2005).

Por exemplo, quando a aplicação utilizada é um navegador WEB, o protocolo utilizado na camada de aplicação é o HTTP (Hyper Transport Text Protocol). No entanto, quando é utilizado um software de e-mails, o protocolo utilizado é o SMTP (Simple Mail Transfer Protocol). Sendo assim, é possível perceber que os serviços utilizados nos softwares aplicativos que se comunicam utilizam protocolos específicos. Vejamos a seguir alguns exemplos de protocolos da camada de aplicação:

- FTP (File Transfer Protocol);
- POP3 (Post Office Protocol);
- DNS (Domain Name System);
- SNMP (Simple Network Management System).

Camada de Transporte

A camada de transporte é responsável por manter as comunicações ponta a ponta na rede. O protocolo TCP lida com as comunicações entre hosts e fornece controle de fluxo, multiplexação e confiabilidade nas transmissões de dados. Essa camada fica localizada no modelo TCP/IP entre a camada de aplicação e a camada de internet. Na camada de transporte são definidos os níveis de serviço e o status da conexão durante o tráfego de dados.

Além do protocolo TCP, em algumas situações, na camada de transporte é utilizado o protocolo UDP (User Datagram Protocol), ambos os protocolos são explicados detalhadamente nesta unidade.

Camada de Rede

A camada de rede, também chamada de camada da internet, trabalha com pacotes e conecta redes independentes para transportar os pacotes. Nessa camada são realizados endereçamento, roteamento e controle do envio e da recepção dos pacotes de dados.

A identificação dos dispositivos de rede que podem ser endereçados e da rede em que se encontram esses dispositivos é realizada por meio do endereço IP. O endereço IP é um método de identificação independente de outros métodos, como, por exemplo, o endereço físico de interfaces de rede (ou endereço MAC).

Também é comum do endereço IP ser chamado de endereço lógico de um equipamento. Esses dois métodos de identificação de equipamentos de rede (endereço MAC e endereço IP) são essenciais para a comunicação em redes de computadores. Os protocolos da camada de rede são o IP e o ICMP (Internet Control Message Protocol), que é usado para o relatório de erros.

Camada Física

Essa é a camada de nível mais baixo do modelo TCP/IP e corresponde à combinação da camada de enlace de dados e da camada física do modelo OSI. A camada física define detalhes de como os dados são fisicamente enviados pela rede, incluindo como os bits são sinalizados eletricamente ou opticamente por dispositivos de hardware que interagem diretamente com um meio físico, como cabo de par trançado, fibra ótica ou tecnologia wireless. Os protocolos utilizados nessa camada são o Ethernet para redes locais e o ARP (Address Resolution Protocol).

praticar

Vamos Praticar

Muito do conceito do modelo OSI é utilizado no modelo TCP/IP. Mesmo com menos camadas que o modelo OSI, o modelo TCP/IP é bastante completo para definição de transmissão de dados via internet. Algumas nomenclaturas também são iguais em ambos os modelos. Contudo, a camada de aplicação do modelo TCP/IP engloba três camadas do modelo OSI. Considerando as informações apresentadas, assinale a alternativa que apresenta quais são essas camadas.

- ☐ a) Transporte, enlace de dados e sessão.
- ☒ b) Aplicação, apresentação e sessão.

Feedback: alternativa **correta**, pois o modelo TCP/IP trabalha os protocolos dessas três camadas na camada de aplicação.

- ☐ **c)** Física, enlace de dados e apresentação.
- ☐ **d)** Camada de rede, transporte e aplicação.
- ☐ **e)** Camada de enlace de dados, física e transporte.

Protocolos da Camada de Aplicação

A camada de aplicação, por estar no topo da pilha TCP/IP, é a que interage diretamente com aplicações e requisições dos usuários. Por meio dessa camada, os usuários podem acessar a internet, por exemplo, além de outros vários serviços. Cada um desses chamados serviços de rede utiliza protocolos de comunicação específicos. Sendo assim, a seguir serão apresentados alguns detalhes dos protocolos mais comuns da camada de aplicação (ELIAS, 2013).

Protocolo HTTP

O HTTP (Hypertext Transfer Protocol) é um protocolo na camada de aplicação utilizado para sistemas de informações de hipermídia distribuídos e colaborativos. Essa é a base para a comunicação de dados para a World Wide Web (páginas publicadas na internet) desde 1990.

Basicamente, o HTTP é um protocolo utilizado para fornecer dados (arquivos HTML, arquivos de imagem, resultados de consultas, etc.) na internet. A porta de comunicação padrão é a TCP 80, mas outras portas também podem ser usadas, além disso, ele fornece uma maneira padronizada para os computadores se comunicarem. A

especificação HTTP define como os dados da solicitação dos clientes serão construídos e enviados ao servidor e como os servidores respondem a essas solicitações. A Figura 3.2 apresenta o fluxo de solicitações via protocolo HTTP.

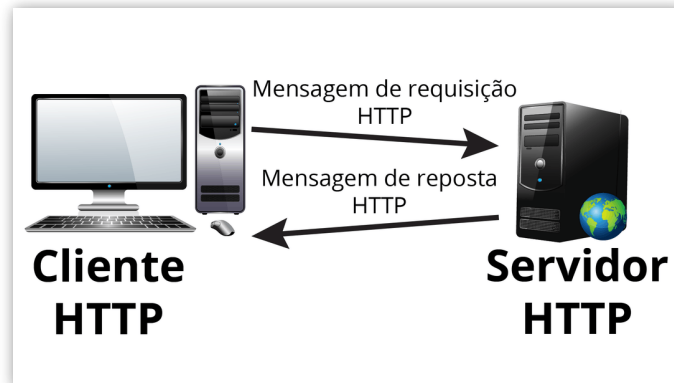


Figura 3.2 - Fluxo de mensagens HTTP

Fonte: Elaborada pelo autor.

Esse protocolo funciona baseado no modelo cliente (requisição) e servidor (resposta). Quando um navegador, por exemplo, faz uma requisição, é estabelecida uma conexão com o servidor (onde a página está hospedada). O cliente envia requisição contendo as seguintes informações:

- URI (Uniform Resource Locator), que é o endereço do servidor;
- Versão do protocolo HTTP que está sendo utilizado;
- Mensagem MIME (Multipurpose Internet Mail Extensions), que é o padrão que define a codificação dos dados para o formato ASCII, para transmissão via internet que contém os modificadores da requisição;
- Informações sobre o cliente;
- Conteúdo da mensagem.

A requisição é respondida pelo servidor por meio de uma linha de status com o seguinte conteúdo:

- Versão do protocolo HTTP utilizada no servidor;
- Código de operação bem-sucedida (ou de erro);
- Informações referentes ao servidor;
- Meta-informações;

- Conteúdo da mensagem.

Tanto o cliente como o servidor se comunicam através de troca de mensagens. Todas as requisições do cliente são feitas através de mensagens, e todas as respostas do servidor também. As mensagens são compostas por dois campos, o cabeçalho da mensagem e o corpo.

No cabeçalho da mensagem, são enviadas informações adicionais da conexão entre cliente e servidor. O corpo da mensagem é o que realmente foi requisitado pelo cliente, podendo também ser uma mensagem de erro, no caso de o recurso solicitado não estar acessível.

Protocolo SMTP

Esse é o protocolo utilizado para enviar mensagens de e-mail (correio eletrônico) por meio dos softwares conhecidos como clientes e e-mail. O cliente que deseja enviar o e-mail abre uma conexão TCP, com o servidor SMTP e envia o e-mail por essa conexão. O servidor SMTP utiliza um recurso chamado de spool para ficar sempre em modo de escuta. Assim que ele escuta uma conexão TCP de qualquer cliente, o processo SMTP inicia uma conexão nessa porta (que normalmente é a 25). Após estabelecer com êxito a conexão TCP, o processo do cliente envia a mensagem instantaneamente.

As conexões via protocolo SMTP podem ocorrer de cliente para servidor e de servidor para servidor. Na Figura 3.3 apresenta-se um exemplo de conexão, utilizando protocolo SMTP com as duas situações.

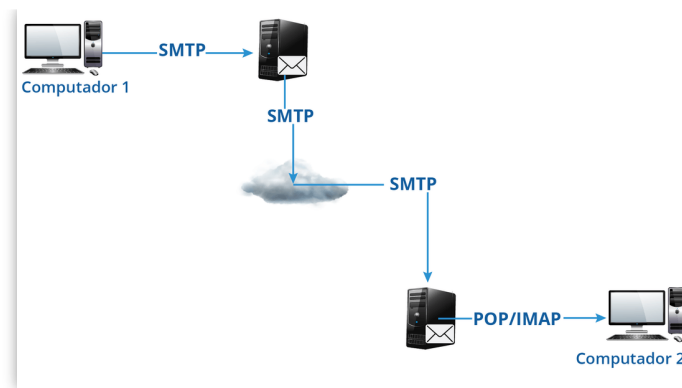


Figura 3.3 - Fluxo do protocolo SMTP

Fonte: Elaborada pelo autor.

Observe na Figura 3.3 que o computador 1 estabelece uma comunicação com um servidor SMTP, que estabelece uma conexão com outro servidor. Nesse servidor, é realizada uma conexão via protocolo POP com o computador 2 para entrega da mensagem.

Protocolo POP

O protocolo POP é utilizado para permitir que softwares clientes de e-mail possam receber mensagens. Os clientes de e-mail geralmente usam a conhecida porta TCP 110 para conectar-se a um servidor POP3. Sendo assim, na Figura 3.3, é possível observar o servidor POP com uma conexão estabelecida com um cliente que solicitou o recebimento de mensagens de e-mail.

Os servidores de e-mail hospedados pelos provedores de serviços da internet também usam o POP3 para receber os destinados a seus assinantes. Periodicamente, esses assinantes utilizam o software cliente de e-mail para verificar suas caixas de correio no servidor remoto e baixar os e-mails endereçados a eles.

Depois que o cliente de e-mail (por exemplo, o Outlook) faz o download dos e-mails, eles geralmente são excluídos do servidor, embora alguns deles possibilitem que os usuários especifiquem que os e-mails sejam copiados ou salvos no servidor por um período de tempo.

Protocolo IMAP

O IMAP (Internet Message Access Protocol) é um protocolo usado para acessar e-mail em um servidor web remoto, a partir de um cliente. Enquanto o protocolo POP pressupõe que os e-mails estão sendo acessados apenas em um software aplicativo, o protocolo IMAP permite o acesso simultâneo por vários clientes. Por isso, o IMAP é mais adequado para os usuários que desejam acessar seu e-mail de locais diferentes. Por padrão, esse protocolo utiliza as portas 143 e 993.

Protocolo FTP

O protocolo FTP (File Transfer Protocol) é um protocolo da camada de aplicação que permite mover arquivos entre sistemas de arquivos locais e remotos. Para transferir um arquivo, duas conexões TCP são usadas pelo FTP em paralelo: conexão de controle e conexão de dados.

Para enviar informações de controle, como identificação do usuário, senha, comandos para alterar o diretório remoto, comandos para recuperar e armazenar arquivos, etc., o protocolo FTP utiliza a conexão de controle através da porta 21.

Para enviar os dados (arquivos), o protocolo FTP utiliza a conexão de dados, que é iniciada na porta 20. O FTP envia as informações em outra porta, pois usa uma conexão de controle separada. Alguns protocolos enviam suas linhas de cabeçalho de solicitação e resposta e os dados na mesma conexão TCP, como, por exemplo, o protocolo HTTP. O protocolo FTP tem como característica a separação das conexões. A Figura 3.4 mostra como funciona essa separação.

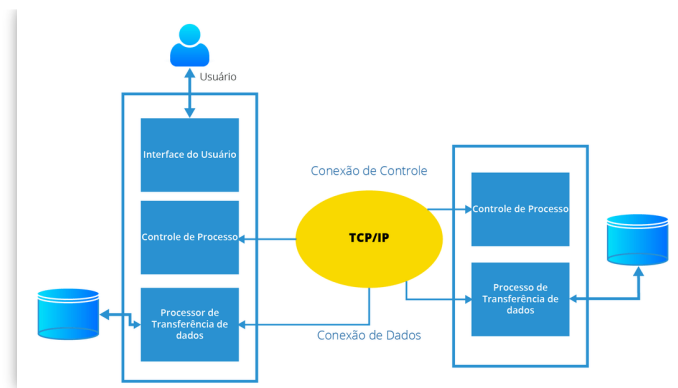


Figura 3.4 - Fluxo do protocolo FTP

Fonte: Elaborada pelo autor.

Protocolo DNS

O protocolo DNS (Domain Name System) auxilia os usuários a navegarem na internet na descoberta de sites, usando nomes de host legíveis por humanos, em vez de endereços IP numéricos. O serviço DNS consiste em um banco de dados distribuído implementado em uma hierarquia de servidores de nomes. É um protocolo da camada de aplicação para troca de mensagens entre clientes e servidores.

Cada host da internet é identificado pelo endereço IP, mas lembrar os números é muito difícil para as pessoas, portanto, é necessário um mapeamento para alterar o nome do domínio para o endereço IP. O protocolo DNS é usado para converter o nome de domínio dos sites em seu endereço IP numérico. Na Figura 3.5 é possível visualizar um host solicitando ao servidor de nomes DNS a resolução do nome do domínio. O servidor de nomes retorna o endereço IP correspondente a esse nome de domínio para o host solicitante para que ele possa se conectar futuramente a esse endereço IP.



Figura 3.5 - Fluxo do protocolo DNS

Fonte: Elaborada pelo autor.

Para que seja possível garantir a disponibilidade desse serviço, existem diversos servidores DNS organizados em árvore. Por isso, os nomes possuem uma estrutura de nomeação que indica localização, finalidade e alguma referência à empresa ou ao dono do site.

Por exemplo, o endereço www.universidade.edu.br, se analisado, é possível perceber que está localizado no Brasil (.br), no subdomínio de entidades educacionais (.edu) no computador de nome universidade.

Protocolo SNMP

O protocolo SNMP (Simple Network Management Protocol) atua na camada de aplicação do modelo TCP/IP e é utilizado para troca de informações relacionadas ao gerenciamento de dispositivos de rede. Esse protocolo é amplamente utilizado para o gerenciamento e o monitoramento de elementos de uma rede.

Atualmente, a grande maioria dos equipamentos de rede possui suporte ao protocolo SNMP. Para que seja possível efetuar o monitoramento e/ou o gerenciamento de equipamentos de rede utilizando o protocolo SNMP, existe um software chamado de agente SNMP que deve estar presente nos equipamentos. Esse software atua na extração de informações dos equipamentos e na sequência realiza o envio das informações para o servidor de gerenciamento.

saiba mais
Saiba mais

O vídeo indicado realiza uma analogia entre o protocolo SNMP e o controle de tráfego aéreo, utilizando uma linguagem bem acessível para descrever o funcionamento do protocolo. Sendo assim, assista ao vídeo disponível em:

ASSISTIR

Protocolo DHCP

Esse protocolo é utilizado para atribuir de maneira dinâmica um endereço IP (Internet Protocol) a qualquer dispositivo ou nó em uma rede para que eles possam se comunicar usando IP. O protocolo DHCP automatiza e gerencia de maneira centralizada as configurações de endereçamento IP, em vez de exigir que os administradores de rede atribuam endereços IP manualmente a todos os dispositivos de rede, além disso, pode ser implementado em pequenas redes locais, bem como em grandes redes corporativas.

O DHCP é um protocolo cliente-servidor em que os servidores gerenciam um conjunto de endereços IP exclusivos, além de informações sobre parâmetros de configuração do cliente. O servidor DHCP atribui os endereços a partir desse conjunto de endereços disponíveis para serem ofertados. Os clientes configurados, como, por exemplo, impressoras, estações de trabalho, smartphones, telefones IP, etc., com DHCP enviam uma solicitação ao servidor DHCP e solicitam informações de configuração de rede, para a rede local em que estão conectados. Um cliente, normalmente, transmite uma consulta para essas informações imediatamente após a inicialização. O servidor DHCP responde à solicitação do cliente, fornecendo informações de configuração IP especificadas anteriormente por um administrador de rede. Isso inclui um endereço IP

específico, bem como um período de tempo, chamado período de concessão. Após encerrado o tempo de concessão, é realizado um teste que verifica se o cliente ainda está conectado à rede. Caso esteja, as configurações permanecem as mesmas, caso não esteja mais na rede, o servidor DHCP poderá atribuir as configurações para outro cliente quando solicitado. O protocolo DHCP possui três maneiras diferentes para definir o fornecimento dos endereços IP, que são:

- Concessão aleatória por tempo limitado (leasing): o endereço IP será alocado para um cliente que terá um tempo predefinido;
- Concessão aleatória por tempo ilimitado: o endereço será alocado para um cliente sempre que ele contatar o servidor;
- Concessão de endereço fixo: o endereço ofertado ao cliente é relacionado com o endereço MAC, podendo o administrador do servidor DHCP configurar qual endereço será utilizado (com base no endereço MAC).

A comunicação entre cliente e servidor DHCP é realizada por mensagens, e existem 8 tipos de mensagens diferentes no protocolo DHCP:

- Discover: é uma solicitação enviada pelo cliente que busca na rede por um servidor DHCP;
- Offer: representa a oferta de endereço IP do servidor para o cliente;
- Request: essa mensagem acontece quando o cliente aceita a oferta de endereço IP, comunicando ao servidor;
- Decline: mensagem que comunica algum parâmetro com erro;
- Ack: mensagem enviada do servidor para o cliente com o OK para atribuição de endereço;
- Nak: mensagem de rejeição de fornecimento de endereço do servidor para o cliente;
- Release: mensagem do cliente para o servidor informando a liberação do endereço IP utilizado;
- Inform: mensagem de um cliente que já possui endereço IP requisitando outras informações de endereçamento.

A Figura 3.6 apresenta o fluxo de mensagens entre cliente e servidor utilizando protocolo DHCP.

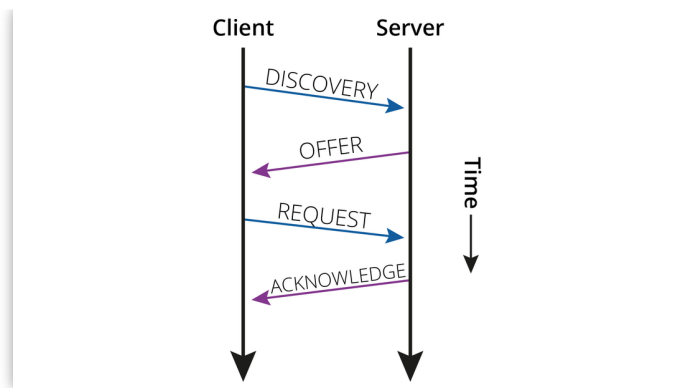


Figura 3.6 - Exemplo de fluxo do protocolo DHCP

Fonte: Gelmo96 / Wikimedia Commons.

Levando em consideração a finalidade do protocolo, podemos dizer que esse é um dos mais utilizados por gerentes de redes de computadores. Isso se deve à praticidade e à facilidade de configuração.

praticar

Vamos Praticar

Um servidor DHCP é um servidor de rede que atribui automaticamente endereços IP e outros parâmetros de rede aos dispositivos clientes. Sem um servidor DHCP, o administrador da rede precisa configurar manualmente todos os clientes que ingressam na rede, o que pode ser complicado, especialmente em redes grandes. O servidor se comunica com os clientes através de mensagens. Um dos tipos de mensagens enviadas pelo servidor é chamada de DHCP ACK.

Considerando as informações apresentadas, assinale a alternativa que apresenta a função dessa mensagem.

- ☐ a) Informar ao cliente que a conexão com o servidor foi estabelecida.
- ☐ b) Informar ao cliente que irá ofertar um endereço IP.

Feedback: alternativa **incorreta**, pois a mensagem de DHCP ACK só é enviada pelo servidor em caso de sucesso na atribuição de endereço IP.

- ☐ **c)** Informar ao cliente que não irá ofertar um endereço IP.
- ☒ **d)** Informar ao cliente que a atribuição de endereço foi realizada com sucesso.

Feedback: alternativa **correta**, pois essa mensagem é a última enviada ao cliente quando o fluxo ocorre normalmente no protocolo DHCP.

- ☐ **e)** Informar ao cliente que as configurações de IP estão erradas.

Protocolos na Camada de Rede

Na camada de rede, é possível realizar a comunicação entre diversos roteadores de rede, a fim de estabelecer os melhores caminhos para o tráfego de dados. Sendo assim, apresentaremos os principais protocolos utilizados na camada de rede.

Protocolo IP

O Internet Protocol (IP) é um protocolo ou um conjunto de regras utilizadas para rotear e endereçar pacotes de dados para que eles possam trafegar pelas redes e chegar ao destino adequado. Os dados que trafegam na internet são divididos em partes menores, chamadas pacotes. As informações de IP são anexadas a cada pacote, e essas informações ajudam os roteadores a enviar pacotes para o destino correto. Quando os pacotes chegam ao seu destino, eles são tratados de maneira diferente, dependendo do protocolo de transporte usado em combinação com o IP (normalmente o TCP). O destino dos pacotes é definido pelo protocolo IP, com a utilização de três campos:

- Endereço IP de origem: endereço atribuído ao dispositivo que inicia o envio de dados ou alguma requisição de serviço;

- Endereço IP de destino: endereço atribuído ao dispositivo que receberá o pacote de dados;
- Máscara de sub-rede: esse campo permite ao protocolo verificar qual a parte do endereço referente à rede.

Os pacotes IP são criados adicionando um cabeçalho IP a cada pacote de dados, antes que ele seja enviado. Um cabeçalho IP é uma série de bits que registra várias informações sobre o pacote, incluindo o endereço IP de envio e recebimento. Nesse contexto, a Figura 3.7 apresenta um pacote IP e seus campos com uma descrição de cada campo do pacote.

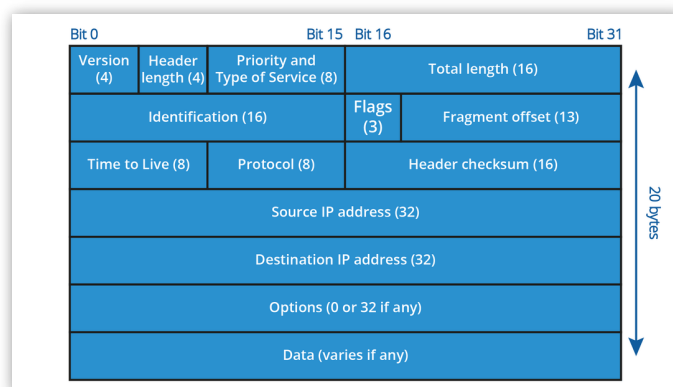


Figura 3.7 - Estrutura do pacote IP

Fonte: Adaptado de Wikimedia Commons.

São muitos os campos que compõem um cabeçalho IP. A seguir é apresentada uma descrição dos campos que compõem o cabeçalho IP.

- Versão: versão do protocolo IP;
- HL (Header Length): comprimento do cabeçalho IP;
- TOS (Type of Service): define como o pacote deve ser tratado em relação à sua prioridade;
- Identificação: identificação única do pacote transmitido pelo equipamento;
- Flags: este campo é composto por dois bits. O MF (More Fragments) define se o pacote é um fragmento, ou se é o último fragmento de um pacote IP. O bit DF (Do not fragment) indica que o pacote não deve ser fragmentado (pelos roteadores);

- Offset: indica qual o posicionamento do fragmento em relação ao pacote de que ele faz parte;
- TTL (Time to Live): limita o tempo de duração de um pacote, evitando que ele fique para sempre na rede;
- Protocolo: define a camada de aplicação na qual o protocolo será utilizado;
- Checksum: campo que ajuda a garantir a integridade do pacote através de uma checagem;
- Endereço de origem: endereço IP do dispositivo onde se originou o pacote;
- Endereço de destino: endereço IP do dispositivo de destino do pacote;
- Padding: campo utilizado para garantir que o pacote tenha o tamanho de 32 bits (padrão do protocolo IP);
- Opções: informações adicionais para o protocolo IP, como, por exemplo, a rota de origem.

Um endereço IP na versão 4 (IPv4) tem o tamanho de 32 bits (ou 4 bytes). Sendo assim, existem 2^{32} endereços de IP na versão 4 disponíveis, o que resulta em torno de 4 bilhões de dispositivos que podem ser endereçados na internet. Com o risco de esgotamento de endereços IP para internet, foi desenvolvido o protocolo IP versão 6 (IPv6). O protocolo IPv6 possui 128 bits no campo de endereçamento do pacote, possibilitando, assim, o endereçamento de muito mais dispositivos.

reflita
Reflita

O endereçamento de equipamentos de rede vem ao longo dos anos migrando da versão 4 (ou sendo usado em paralelo) para a versão 6. O chamado ipv6 permitirá que qualquer dispositivo possa ser conectado à internet, como, por exemplo, equipamentos domésticos como geladeira e cafeteira. A ideia é que, associado ao conceito de internet das coisas, o protocolo ipv6 venha sendo cada vez mais utilizado. Qual será o limite de endereçamento de dispositivos de rede? Será que o protocolo Ipv6 será suficiente?

O cálculo seria algo em torno de 256×10^{27} trilhões de dispositivos que poderiam ser endereçados, além disso, o protocolo IPv6 garante que conceitos como o de Internet das Coisas sejam aplicáveis.

Protocolo ICMP

Como o protocolo IP não possui um mecanismo para envio de mensagens de erro e de controle, o protocolo ICMP (Internet Control Message Protocol) se encarrega dessas tarefas. Ele é utilizado para relatar erros ou para comunicação entre dispositivos.

Existem dois comandos implementados em diferentes sistemas operacionais que são bons exemplos de utilização do protocolo ICMP, que são os comandos: PING e o TRACEROUTE.

O comando conhecido como PING permite a realização de um teste de conectividade entre dois hosts. Ou seja, se existe uma rota para que um dispositivo esteja conectado à internet. Caso, na realização desse teste, ocorra alguma perda de pacotes, ou até mesmo o equipamento de destino não esteja acessível, o comando PING apresenta o retorno com a porcentagem de pacotes perdidos.

Para que seja possível identificar a rota que um pacote faz para alcançar o seu destino, é possível utilizar o comando TRACEROUTE, além disso, esse comando irá listar todos os roteadores por onde o pacote irá passar para que consiga alcançar o destino definido.

O campo TTL que compõe um pacote IP será apresentado em ambos os comandos. Esse campo é decrementado a cada salto de roteador que o pacote dá ao longo do caminho. Nesse contexto, a Figura 3.8 apresenta um exemplo de comando TRACEROUTE.

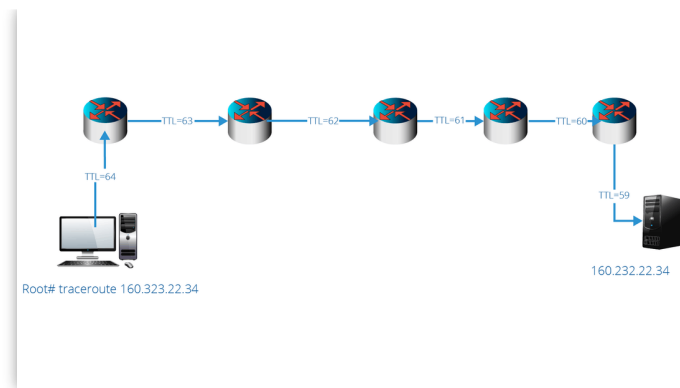


Figura 3.8 - Comando Traceroute

Fonte: Elaborada pelo autor.

Protocolo RIP

O RIP (Routing Information Protocol) é um protocolo de roteamento dinâmico que utiliza a contagem de saltos como uma métrica de roteamento para encontrar o melhor caminho entre a origem e a rede de destino, é considerado um protocolo de roteamento de vetor de distância e utiliza porta 520.

Um roteador trabalhando com o protocolo RIP envia o conteúdo de sua tabela de roteamento para cada um dos roteadores adjacentes a cada 30 segundos. Quando uma rota é removida da tabela de roteamento, ela é sinalizada como inutilizável pelos roteadores receptores após 180 segundos e removida de suas tabelas após 120 segundos adicionais. A Figura 3.9 exemplifica o funcionamento do protocolo RIP.

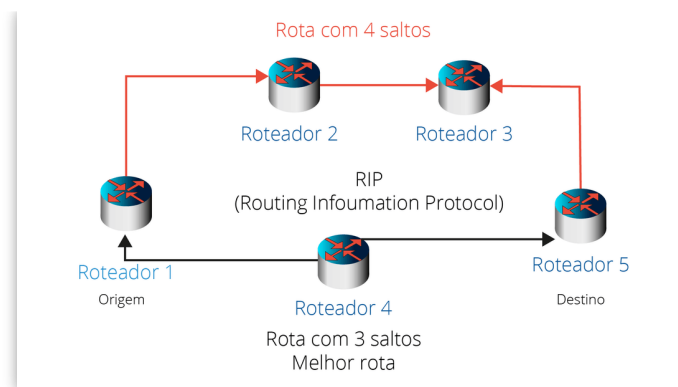


Figura 3.9 - Exemplo de seleção de rota com protocolo RIP

Fonte: Elaborada pelo autor.

A contagem de saltos é o número de roteadores existentes entre a rede de origem e o destino. O caminho com a menor contagem de saltos é considerado o melhor caminho para alcançar uma rede e, portanto, colocado na tabela de roteamento. O protocolo RIP impede loops de roteamento, limitando o número de saltos permitidos em uma rota entre a origem e o destino. A contagem máxima de saltos permitida para o protocolo RIP é 15, quando a contagem chegar a 16, o protocolo considera como inacessível à rede.

praticar

Vamos Praticar

O protocolo ICMP (Internet Control Message Protocol) é usado na camada de rede para diagnóstico e gerenciamento de redes. Dois bons exemplos de utilização desse protocolo são os comandos PING e TRACERT, implementados em diferentes sistemas operacionais. Considerando as informações apresentadas, assinale a alternativa que apresenta a função desses dois comandos, respectivamente.

- ☐ **a)** Apresentar o caminho realizado pelo pacote para chegar ao seu destino / Testar a conectividade entre dois dispositivos.
- ☐ **b)** Calcular o tempo que o usuário leva para se conectar à internet / Calcular o tempo de retorno de um pacote de rede
- ☒ **c)** Testar a conectividade entre dois dispositivos / Apresentar o caminho realizado pelo pacote para chegar ao seu destino.

Feedback: alternativa **correta**, pois o comando PING retorna estatísticas da conexão e o comando TRACERT apresenta os roteadores que existem entre origem e destino.

- ☐ **d)** Calcular o tempo de retorno de um pacote de rede / Calcular o tempo que o usuário leva para se conectar à internet.
- ☐ **e)** Informar o modelo do roteador utilizado na rede / Informar o modelo do switch utilizado na rede (se houver).

Protocolos da Camada de Transporte

No modelo TCP/IP existem dois protocolos da camada de transporte que se destacam, o protocolo TCP e o UDP. Nesta seção serão apresentados detalhes desses dois protocolos.

Protocolo TCP

O protocolo TCP (Transmission Control Protocol) atua na comunicação orientada à conexão facilitando a troca de mensagens entre dispositivos em uma rede, além de ser mais comum em redes que usam o Internet Protocol (IP).

Esse protocolo recebe as mensagens de um aplicativo/serviço e as divide em pacotes, que podem ser encaminhados pelos dispositivos da rede para o destino, numerando cada pacote e os remonta antes de entregá-los ao destinatário do aplicativo/serviço. Por ser orientado à conexão, garante que uma conexão seja estabelecida e mantida até que a troca de mensagens seja concluída.

Devido ao comportamento imprevisível das redes, os pacotes IP podem ser perdidos ou entregues fora de ordem. O protocolo TCP detecta e minimiza esses problemas reordenando os dados do pacote ou solicitando um novo envio. Essa precisão afeta a

velocidade de tráfego, além disso, é famosa pela confiabilidade, porém essa confiabilidade tem relação direta com a taxa de transmissão.

No início de cada conexão, o protocolo TCP cria uma máquina de estados conhecida como 3-way handshake, um mecanismo confiável de conexão em 3 vias capaz de oferecer o estabelecimento de comunicação confiável e sincronizada entre os equipamentos. Nesse contexto, a Figura 3.10 apresenta a sequência para estabelecimento da conexão.

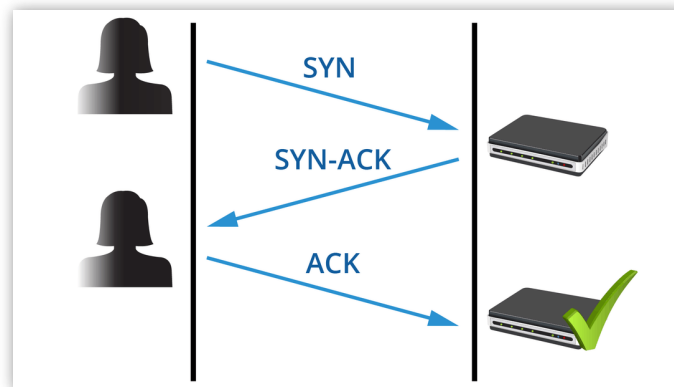


Figura 3.10 - Estabelecimento de conexão TCP

Fonte: Dake / Wikimedia Commons.

A popularização do protocolo TCP no transporte de dados se dá devido ao fato de ser um protocolo confiável, que permite retransmissão de pacotes perdidos, duplicados ou atrasados (KUROSE; ROSS, 2010). A Figura 3.11 apresenta o cabeçalho TCP e seus campos.

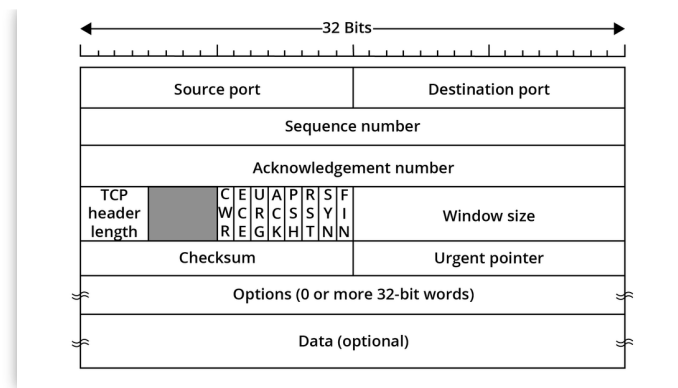


Figura 3.1 1 - Cabeçalho TCP

Fonte: Quliyevferman / Wikimedia Commons.

O cabeçalho TCP, assim como o cabeçalho IP, possui diferentes campos com informações distintas. A seguir, é apresentada uma breve descrição dos campos apresentando os tópicos a seguir.

- Porta de Origem: porta de conexão utilizada na origem;
- Porta de Destino: porta de conexão utilizada no destino;
- Número de Sequência: indica o número de sequência dos dados que estão sendo transmitidos;
- Número de Confirmação (ACK): este campo possui um número que indica a confirmação de recebimento dos dados. Essas informações são trocadas em ambos os sentidos, informando também o próximo conjunto de bytes a ser recebido;
- Tamanho do cabeçalho: indica o número de palavras de 32 bits contidas no cabeçalho TCP;
- Reservado: normalmente possui a sequência 000;
- Bit de controle CWR (Congestion Window Reduced): é um bit utilizado para o controle de congestionamento.
- Bit de controle ECE (ECN Echo): bit utilizado pelo dispositivo receptor para informar ao emissor que foi recebido um pacote com indicação de congestionamento;
- Bit de Controle URG (Urgent Pointer): indica que o segmento que está sendo transportado possui dados urgentes;
- Bit de Controle ACK (Acknowledge): este bit sinaliza que o valor do campo de reconhecimento é válido;

- Bit de Controle PSH (Push): este bit pode informar a origem e ao destino a necessidade de transmissão rápida dos dados;
- Bit de Controle RST (Reset): informa que a conexão foi abortada;
- Bit de Controle SYN (Synchronism): este bit atua no estabelecimento da conexão;
- Bit de Controle FIN (Finishing): indica a finalização de um pacote;
- Tamanho da Janela: informa a quantidade de bytes disponíveis para recepção do pacote;
- Checksum: armazena o resultado de um cálculo que verifica a integridade do pacote;
- Urgent Pointer: caso o bit de controle URG seja ativado, este campo indica onde termina o conjunto de dados urgentes;
- Opções: informa várias opções que o TCP pode transmitir;
- Padding: campo utilizado para garantir, através da inserção de zeros, que o cabeçalho TCP tem o comprimento de 32 bits.

É importante salientar que uma conexão TCP pode ser encerrada a qualquer momento. O encerramento da conexão se dá quando o cliente ou servidor envia o valor 1 no bit de controle RST.

Protocolo UDP

O protocolo UDP (User Datagram Protocol) é um protocolo de camada de transporte. Ao contrário do TCP, é um protocolo não confiável e sem conexão. Portanto, não há necessidade de estabelecer conexão antes da transferência de dados (FOROUZAN, 2009).

Embora o TCP (Transmission Control Protocol) seja o protocolo dominante da camada de transporte, é utilizado na maioria dos serviços da internet por fornecer entrega garantida, confiabilidade e outras vantagens. Porém, todas essas vantagens custam sobrecarga e latência adicionais. Nesse contexto, o protocolo UDP é mais interessante para os serviços em tempo real, como jogos de computador, comunicação por voz ou vídeo, conferências ao vivo. Como é para esses serviços, é necessário alto desempenho, o UDP permite que pacotes sejam descartados em vez de processar pacotes atrasados. Não há verificação de erro no UDP, portanto, ele também economiza largura de banda.

O cabeçalho UDP é menos complexo que o cabeçalho TCP. A Figura 3.12 apresenta os campos do cabeçalho UDP com descrições das funções dos campos.

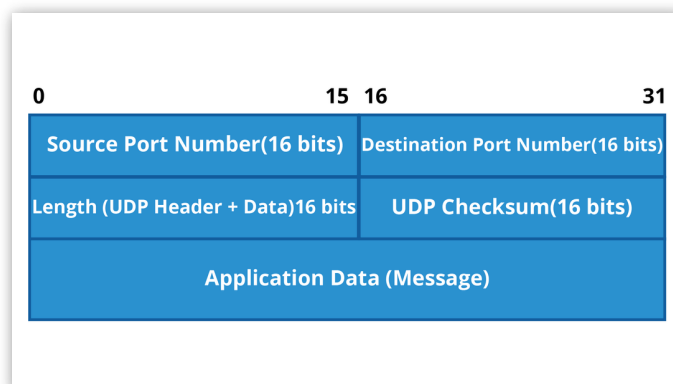


Figura 3.12 - Cabeçalho TCP

Fonte: Devarshi / Wikimedia Commons.

Logo abaixo são descritas as funções dos campos.

- Número de Porta de Origem: porta utilizada no emissor;
- Número de Porta de Destino: porta utilizada no receptor;
- Comprimento: este campo informa o tamanho do pacote UDP;
- Checksum: campo específico para checagem;

O UDP funciona encapsulando dados em um pacote UDP e adicionando suas próprias informações de cabeçalho ao pacote. Depois que os pacotes UDP são encapsulados em um pacote IP, eles são enviados para seus destinos.

praticar
Vamos Praticar

Os protocolos TCP (Transmission Control Protocol) e UDP (User Datagram Protocol) são utilizados na camada de transporte. Podemos dizer que o protocolo TCP é mais utilizado que o UDP, porém o protocolo TCP possui lentidão maior na velocidade de transmissão.

O que faz com que o protocolo TCP seja mais lento que o UDP?

- ☒ **a)** O fato de realizar o controle de erros nos pacotes transmitidos.

Feedback: alternativa **correta**, pois o protocolo TCP permite a retransmissão de pacotes perdidos.

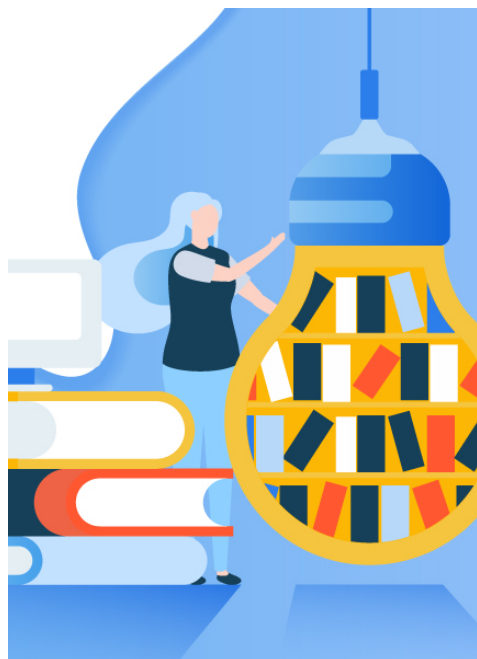
- ☐ **b)** O fato de não estabelecer uma conexão antes da transferência.
- ☐ **c)** Apresenta um cabeçalho menos complexo.

Feedback: alternativa **incorreta**, pois o protocolo TCP fornece entrega garantida dos pacotes, confiabilidade e outras vantagens.

- ☐ **d)** O fato de não realizar o controle de erros de transmissão.
- ☐ **e)** Por ser um protocolo não confiável.

indicações

Material Complementar



LIVRO

Interligação de redes com TCP/IP - Volume 1: Princípios, Protocolos e Arquitetura

Douglas E. Comer

Editora: Campus

Ano: 2015

Comentário: No capítulo 5 deste livro é realizada uma explicação sobre as características do endereçamento de equipamentos na internet, apresentando os detalhes técnicos de como funciona o endereçamento IPv4.

WEB

O que são os protocolos e número de portas TCP e UDP

Ano: 2013

Comentário: O vídeo indicado apresenta recursos visuais e como funcionam as portas TCP e UDP.

Para conhecer mais sobre o filme, acesse o link disponível em:

ACESSAR

conclusão

Conclusão

Nesta unidade estudamos os conceitos do modelo TCP/IP (e suas camadas) e os protocolos utilizados no modelo TCP/IP. Foi possível observar que os protocolos estão presentes em muitas aplicações utilizadas no nosso cotidiano. Ou seja, mesmo que os usuários não tenham noção dos detalhes técnicos referentes ao funcionamento dos protocolos, eles têm um contato constante com eles através das camadas de aplicação.

A internet é estruturada em cima do modelo TCP/IP e, a partir do estudo do modelo, é possível entender melhor os fluxos de comunicação referentes aos protocolos. Juntamente a isso, é possível associar os protocolos às aplicações mais convencionais como o acesso a um website, até aplicações como o gerenciamento de equipamentos de rede. Ou seja, tudo que acontece na internet tem como base o modelo TCP/IP.

referências

Referências Bibliográficas

4LINUX. O Que é SNMP [Online] 2017. Disponível em: <https://www.4linux.com.br/o-que-e-snmip>. Acesso em: 10 dez. 2019.

COMER, D. E. **Redes de Computadores e Internet-6**. Porto Alegre: Bookman Editora, 2016.

ELIAS, G. **Arquitetura e protocolo de rede TCP-IP**. 2. ed. Rio de Janeiro: RNP/ESR, 2013. Disponível em: <http://www.lest5.com.br/lest/attachments/article/3/ArquiteturaeProtocolosdeRedeTCPIP.pdf>. Acesso em: 10 jan. 2020.

FOROUZAN, B. A. **Comunicação de dados e redes de computadores**. Porto Alegre: AMGH Editora, 2009.

KOZIEROK, C. M. **The TCP/IP guide**: a comprehensive, illustrated Internet protocols reference. São Paulo: No Starch Press, 2005.

KUROSE, J. F.; ROSS, K. W.; ZUCCHI, W. L. **Redes de Computadores e a Internet**: uma abordagem top-down. São Paulo: Pearson Addison Wesley, 2007.

KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet**: uma abordagem top-down. 5. ed. São Paulo: Pearson, 2010.

TANENBAUM, A. S. **Redes de computadores**. 4. ed. Rio de Janeiro: Editora Campus, 2003.