GIOVANE VELLEDA DE MOURA

PRINCIPAIS PROTOCOLOS DE COMUNICAÇÃO UTILIZADOS EM REDES DE COMPUTADORES E INTERNET

Pelotas
2020

Trabalho de Conclusão de Curso apresentado à Anhanguera Pelotas, como requisito parcial para a obtenção do título de graduado em Engenharia da Computação.

Orientador: Gryco Araujo

PRINCIPAIS PROTOCOLOS DE COMUNICAÇÃO UTILIZADOS EM REDES DE COMPUTADORES E INTERNET

GIOVANE VELLEDA DE MOURA

GIOVANE VELLEDA DE MOURA

Pelotas
2020

PRINCIPAIS PROTOCOLOS DE COMUNICAÇÃO UTILIZADOS EM REDES DE COMPUTADORES E INTERNET

Trabalho de Conclusão de Curso apresentado à Anhanguera Pelotas, como requisito parcial para a obtenção do título de graduado em Engenharia da Computação.

BANCA EXAMINADORA

Prof. Me. Antônio Rogerio Ness

Prof. Me. Luthiano Venecian

Prof. Dr. Geórgia Rita Burck Duarte

Pelotas, 04 de Dezembro de 2020

Dedico este trabalho para a minha família, amigos e professores que me acompanharam e apoiaram durante esta jornada.

“Deixem que o futuro diga a verdade e avalie cada um de acordo com o seu trabalho e realizações. O presente pertence a eles, mas o futuro pelo qual eu sempre trabalhei pertence a mim.”

Nikola Tesla

MOURA, Giovane Velleda de. **Principais Protocolos de Comunicação utilizados em Redes de computadores e internet**. 2020. 32 páginas. Trabalho de Conclusão de Curso Engenharia da Computação – Anhanguera, Pelotas, 2020.

RESUMO

Redes de computadores podem ser ambientes onde recursos são compartilhados, tarefas executadas por qualquer sistema computacional, separados e também interligados, a interconexão entre redes apresenta um grau de complexidade proporcional a sua dimensão, a internet é composta de diversas destas redes conectadas entre si, esta interconexão só e possível pois existem protocolos que regem a comunicação e compartilhamento de recursos entre as diferentes redes. Este trabalho tera como objetivo principal demonstrar quais os principais protocolos de comunicação utilizados em Redes de computadores e internet, como também identificar, caracterizar e descrever os mesmos. A presente de pesquisa será realizado com base na revisão de bibliografia, assim sendo uma pesquisa qualitativa e descritiva, a literatura utilizada, abrangera alguns autores destacados mundialmente como Kurose e Ross, Tanenbaum, Comer dentre outros, nestas obras serão incluídos teses e dissertações e ainda documentos técnicos de órgãos certificadores. As obras escolhidas deveram ter uma abrangência de até 10 anos.

Palavras-chave: Protocolo; Redes de Computadores; Internet; OSI, TCP, UDP, IP.

MOURA, Giovane Velleda de. **Main Communication Protocols used in Computer Networks and the Internet**. 2020. 32 pages. Computer Engineering Course Conclusion Paper - Anhanguera, Pelotas, 2020.

ABSTRACT

Computer networks can be environments where resources are shared, tasks performed by any computer system, separate and also interconnected, the interconnection between networks presents a degree of complexity proportional to its size, the internet is composed of several of these networks connected together, this interconnection is only possible because there are protocols that govern communication and resource sharing between different networks. This work will have as main objective to demonstrate which are the main communication protocols used in Computer and internet networks, as well as to identify, characterize and describe them. The present research will be carried out based on the review of the bibliography, thus being a qualitative and descriptive research, the literature used, will cover some prominent authors worldwide such as Kurose and Ross, Tanenbaum, Comer among others, in these works will be included theses and dissertations and also technical documents from certifying bodies. The chosen works should have a coverage of up to 10 years.

***Key-words*:** Protocol; Computer network; Internet; OSI, TCP, UDP, IP.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ARP	Address Resolution Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
ICMP	Internet Control Message Protocol
HTTP	Hypertext Transfer Protocol
IEEE	Electric and Electronic Engineers
IP	Internet Protocol
ISO	International Organization for Standardization
LAN	Local Area Network
NDP	Neighbor Discovery Protocol
NIC	Network Interface Card
OSI	Open System Interconnection
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

SUMÁRIO

1 INTRODUÇÃO

A internet está presente no dia a dia das pessoas e instituições, sendo utilizada com uma infinidade de propósitos, dentre as quais podemos citar: comunicação, comércio, entretenimento, o IBGE, em 2017, aponta que o uso da internet nos domicílios brasileiros era aproximadamente em 74,9%, a internet nada mais é que a interligação de diversas redes de computadores em escala mundial.

Redes de computadores podem ser ambientes onde recursos são compartilhados, tarefas executadas por computadores ou qualquer outro sistema computacional, separados e também interligados, estas redes podem estar conectadas para criar redes maiores e mais complexas.

A interconexão de redes apresenta um grau de complexidade proporcional a sua dimensão, a internet sendo um emaranhado de diversas redes conectadas entre si, esta interconexão só e possível pois existem regras bem definidas que regem a comunicação e compartilhamento de recursos entre as diferentes redes e sistemas que a compõe internet, estas regras são chamadas de protocolos.

Este trabalho tera como objetivo principal demonstrar quais os principais protocolos de comunicação utilizados em Redes de computadores e na internet, como também identificar, caracterizar e descrever os mesmos.

A presente de pesquisa será realizado com base na revisão de bibliografia, assim sendo uma pesquisa qualitativa e descritiva, a literatura utilizada, inicialmente, abrangera alguns autores destacados mundialmente como Kurose e Ross, Tanenbaum, Comer dentre outros, nestas obras serão incluídos teses e dissertações e ainda documentos técnicos de órgãos certificadores. As obras escolhidas deveram ter uma abrangência de até 10 anos.

A literatura atual foi encontrada no através, google acadêmico, Capes e Scielo, utilizando palavras chaves como protocolo, redes de computadores, internet, e posteriormente com modelo OSI, TCP, UDP, IP, também vieram como referência de outras obras na área como teses e dissertações, foi retirado, também, do material fornecido pela instituição de ensino em atividades relacionadas.

2 ARQUITETURA DE REDES E INTERNET

Uma rede de computadores é definida por Tanembaun(2011), como ambientes “que os trabalhos são realizados por um grande número de computadores separados, porém interconectados”, caracterizando o compartilhamento de recursos.

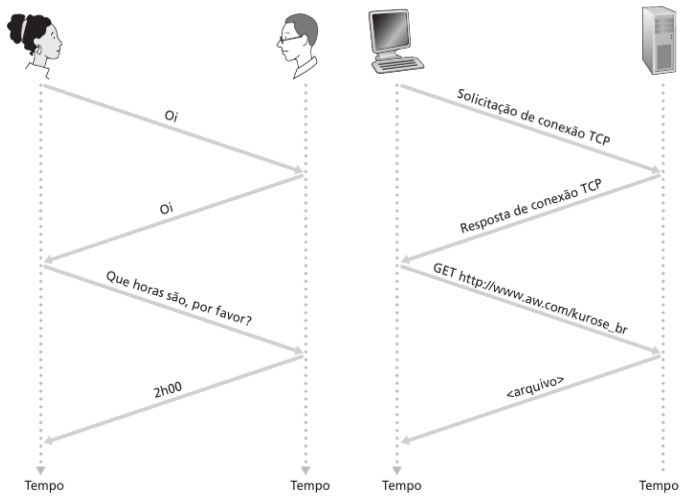
A internet sendo uma “rede de computadores que interconecta milhares de dispositivos computacionais ao redor do mundo” Kurose e Ross(2010), e Tanembaun(2011) relaciona a internet como a conexão de redes para criar redes maiores, e a internet sendo o exemplo mais claro de uma rede de redes. E Comer, afirma que a internet “embora pareça operar como uma rede unificada, não é composta de uma única tecnologia de rede, pois nenhuma tecnologia isolada é suficiente para todos os usos” (COMER, 2015)

Conforme Kurose e Ross (2010) existem duas abordagens fundamentais para o trafego de dados através de uma rede de enlaces, a comutação de circuitos e comutação de pacotes. Em redes de comutação de circuitos, os recursos necessários para a comunicação são alocados entre o transmissor e receptor, antes do início da comunicação, tornando-se exclusivo para esta seção. Em redes de comutação de pacotes, esses recursos não são reservados; as mensagens de uma sessão usam os recursos por demanda e, como consequência, poderão ter de esperar, entrar na fila se necessário, para conseguir acesso a um enlace de comunicação.

Os protocolos podem ser definidos como “o formato e a ordem das mensagens trocadas entre duas ou mais entidades comunicantes, bem como as ações realizadas na transmissão e/ou no recebimento de uma mensagem”, “os três protocolos fundamentais da internet que temos hoje - TCP, UDP e IP” Kurose e Ross(2010), e temos ainda que a “TCP/IP internet protocol suite e normalmente referenciada como TCP/IP, ela pode ser usada para comunicação entre qualquer conjunto de redes interconectadas” – (COMER 2015). Neste trabalho analisaremos estes protocolos fundamentais como o modelo de referência ISO OSI (Open Systems Interconnection).

Para melhor compreensão do funcionamento de um protocolo de comunicação, é possível fazer uma analogia em com duas pessoas conversando, conforme apresenta (KUROSE;ROSS, 2010)

***Figura 1**: Protocolo Humano e um protocolo de rede de computadores.*



***Fonte:** Kurose e Ross (2010), pg 6*

Um sistema dividido em camadas de protocolos, segundo Kurose e Ross (2010) tem vantagens conceituais e estruturais, esta divisão em camadas proporciona um modo estruturado de discutir componentes de sistemas e a modularidade facilita a atualização de componentes de sistema. E ainda “objetivo de cada camada é oferecer determinados serviços às camadas superiores, isolando essas camadas dos detalhes de implementação real desses recursos. Em certo sentido, cada camada é uma espécie de máquina virtual, oferecendo determinados serviços à camada situada acima dela” (TANEMBAUN, 2011).

Tendo em consideração o conceito de camadas de protocolos em termos abstratos, Kurose e Ross (2010) nos apresenta duas importantes arquiteturas de rede: os modelos de referência OSI e TCP/IP. “Embora os protocolos associados ao modelo OSI raramente sejam usados nos dias de hoje, o modelo em si é de fato bastante geral e ainda válido, e as características descritas em cada camada ainda são muito importantes. O modelo TCP/IP tem características opostas: o modelo propriamente dito não é muito utilizado, mas os protocolos são bastante utilizados” (KUROSE;ROSS, 2010).

O modelo OSI, segundo Tanembaun(2011), se baseia em uma proposta desenvolvida pela ISO (International Standards Organization) como um primeiro passo em direção à padronização internacional dos protocolos usados nas várias camadas, este modelo é denominado Modelo de Referência ISO OSI (Open Systems Interconnection), pois ele trata da interconexão de sistemas abertos. O modelo OSI tem sete camadas, com funcionamento bem definidos e cada camada executa alguns serviços para a camada acima dela, a interface de uma camada informa como os processos acima dela podem acessá-la e ainda especifica quais são os parâmetros e os resultados esperados, não revela o funcionamento interno da camada.

Concluindo, “os protocolos utilizados em uma camada são de responsabilidade dessa camada. Esta pode usar os protocolos que quiser, desde que realize o trabalho (ou seja, forneça os serviços oferecidos). Ela também pode alterar esses protocolos sem influenciar o software das camadas superiores” (TANEMBAUN, 2011).

O modelo criado para ter “a capacidade para conectar várias redes de maneira uniforme. Essa arquitetura posteriormente ficou conhecida como modelo de referência TCP/IP, graças a seus dois principais protocolos” (TANEMBAUN, 2011).

O modelo que Kurose e Ross (2010) apresenta como protocolos de várias camadas, a pilha de protocolos TCP/IP, é formada por cinco camadas: física, de enlace, de rede, de transporte e de aplicação, descreveremos a seguir.

A camada de aplicação é onde residem aplicações de rede e seus protocolos, nela estãp incluidos muitos protocolos, tais como o protocolo HTTP (Hypertext Transfer Protocol), requisição e transferência de documentos pela Web, o SMTP (Simple Mail Transfer Protocol), correio eletrônico, o FTP (File Transfer Protocol), transferência de arquivos, DNS(Domain Name System), resolução de nomes de domínio, o pacote de informação na camada de aplicação denominado de mensagem.

Camada de transporte, “transporta” mensagens da camada de aplicação entre os lados do cliente e servidor de uma aplicação, segundo Kurose e Ross (2011), existem dois protocolos de transporte na Internet: TCP e UDP. O TCP provê serviços orientados para conexão, como a entrega garantida de mensagens ao destino e controle de fluxo, compatibilidade entre as velocidades do remetente e do

receptor, também fragmenta mensagens longas em segmentos mais curtos e provê mecanismo de controle de congestionamento. O protocolo UDP provê serviço não orientado para conexão a suas aplicações, é um serviço econômico que fornece segurança, sem controle de fluxo e de congestionamento, nem garantia de entrega de pacotes, um pacote desta camada é denominado segmento.

A camada de rede, por sua vez é responsável pela movimentação, de uma máquina para outra, de pacotes de camada de rede conhecidos como datagramas. O protocolo de camada de transporte da Internet (TCP ou UDP) em uma máquina de origem passa um segmento de camada de transporte e um endereço de destino à camada de rede. A camada de rede então provê o serviço de entrega do segmento à camada de transporte na máquina destinatária.

A camada de rede da Internet, segundo Kurose e Ross (2010), tem dois componentes principais, é um protocolo que define os campos no datagrama, bem como o modo como os sistemas finais e os roteadores agem nesses campos, protocolo IP, todos os componentes da Internet que têm uma camada de rede devem executar esse protocolo. O outro componente importante é o protocolo de roteamento que determina as rotas que os datagramas seguem entre origens e destinos. A Internet tem muitos protocolos de roteamento. Embora a camada de rede contenha o protocolo IP e também numerosos protocolos de roteamento, ela quase sempre é denominada simplesmente camada IP, refletindo o fato de que ele é o elemento fundamental que mantém a integridade da Internet.

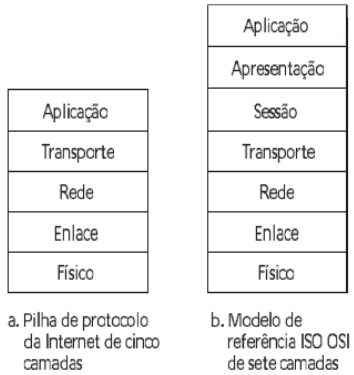
A camada de rede, segundo Kurose e Ross (2010), faz o roteamento de um datagrama por meio de uma série de roteadores entre a origem e o destino. Para levar um pacote de um nó, sistema final ou comutador de pacotes, ao nó seguinte na rota, a camada de rede depende dos serviços da camada de enlace. Em cada nó, a camada de rede passa o datagrama para a camada de enlace, que o entrega, ao nó seguinte, no qual o datagrama é passado da camada de enlace para a de rede.

Os serviços prestados pela camada de enlace dependem do protocolo específico empregado no enlace. Alguns protocolos de camada de enlace proveem entrega garantida entre enlaces, desde o nó transmissor, até o nó receptor. Esse serviço confiável de entrega é diferente do serviço de entrega garantida do TCP, que provê serviço de entrega garantida de um sistema final a outro. Exemplos mostrados por Kurose e Ross (2010), de alguns protocolos de camadas de enlace como

Ethernet, WiFi e PPP (point-to-point protocol — protocolo ponto-a-ponto). Como datagramas normalmente precisam transitar por diversos enlaces para irem da origem ao destino, serão manuseados por diferentes protocolos de camada de enlace em diferentes enlaces ao longo de sua rota, podendo ser manuseados por Ethernet em um enlace e por PPP no seguinte. A camada de rede receberá um serviço diferente de cada um dos variados protocolos de camada de enlace. Kurose e Ross (2010) nomeia pacotes de camada de enlace como quadros.

Camada física é o meio físico, como cabo de cobre, fibra óptica ou o ar, no caso de redes sem fio, Kurose e Ross (2010) aponta que tem por objetivo movimentar os bits individuais que estão dentro do quadro de um nó para o seguinte.

Figura 2: *Modelo referência TCP/IP e ISO/OSI*



Fonte: *Kurose e Ross (2010), pg 38*

3 PROTOCOLO DE INTERNET

O protocolo comumente referenciado como TCP/IP, é composto por um conjunto de protocolos trabalhando em conjunto, Tanenbaum(2011) apresenta que o “TCP e IP normalmente são implementados juntos (como ‘TCP/IP’)” e Comer(2015) cita que o “TCP/IP usa o termo host para se referir a um sistema terminal que se conecta à Internet”. Um host pode ser qualquer dispositivo conectado a internet, desde um grande e poderoso computador de uso geral ou um pequeno sistema para fins específicos.

O protocolo TCP/IP, conforme Comer(2015) tem a característica de tratar “todas as redes de forma igual”, seja uma rede de área local como uma Ethernet, uma rede de longa distância, uma rede wireless, um link ponto a ponto entre dois hosts, cada qual conta como uma rede.

Todo host possui um endereço físico, Comer(2015) explica que a IEEE (Electric and Electronic Engineers) “define um esquema de endereçamento 48-bit MAC que é usado com Ethernet e com outras tecnologias de rede”. A abreviação MAC significa Media Access Control, Controle de Acesso à Mídia em tradução livre. Ainda segundo Comer(2015) o “endereço MAC é atribuído a cada placa de interface de rede” e com o objetivo de garantir a unicidade, cada fornecedor de hardware de Ethernet deve comprar da IEEE um bloco de endereços MAC e assim atribuir um endereço a cada placa de interface de rede que for fabricada. A atribuição significa que não há dois hardwares de interfaces com o mesmo endereço Ethernet.

Comer (2015) fala que ao projetar o TCP/IP, escolhido um sistema análogo à rede de endereçamento físico, sendo que a host em uma internet é atribuído um endereço único inteiro chamado de endereço de Protocolo Internet ou endereço IP. Comer(2015) cita “a parte inteligente do endereçamento da internet é que os inteiros são cuidadosamente escolhidos para tornar eficiente o encaminhamento. Especificamente, um endereço de IP é dividido em duas partes: um prefixo do endereço identifica a rede a que o host está conectado e um sufixo identifica um host específico na rede”

Para Tanenbaum(2011) o “IP (Internet Protocol), que é a base para a Internet inteira, é um exemplo dominante de serviço de rede não orientado a conexões. Cada pacote transporta um endereço IP de destino que os roteadores utilizam para

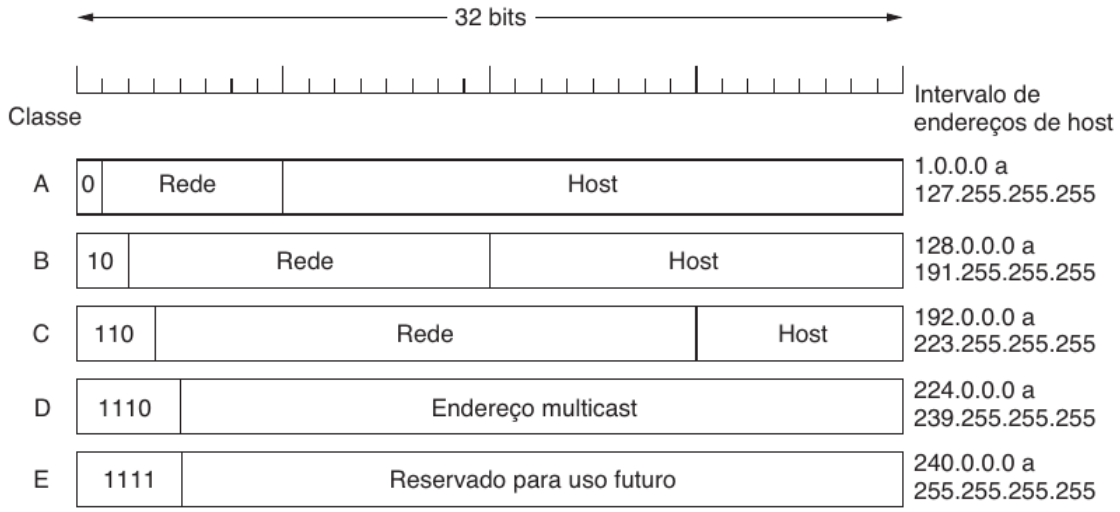
encaminhar cada pacote individualmente". Os endereços IP são formados por "32 bits nos pacotes IPv4 e 128 bits nos pacotes IPv6", como descreve Tanenbaum(2011) e Comer(2015) apresenta que "cada host em uma internet IPv4, é atribuído um endereço exclusivo que é utilizado em toda a comunicação com o host.", para um encaminhamento eficiente, um prefixo do endereço identifica uma rede e um sufixo identifica um host na rede.

Os endereços IP é um par composto por netid e hostid, no qual o netid identifica uma rede e o hostid identifica um host na rede. Tendo o endereço IP com tamanho fixo e dividir cada endereço em uma ID de rede e uma ID de host, Comer(2015) apresenta a seguinte pergunta: "que tamanho deve ter cada parte?" A resposta depende do tamanho das redes que esperamos na nossa internet. A explicação dada por Comer(2015) mostra que "alocação de muitos bits para o prefixo de rede permite que a nossa internet tenha muitas redes, mas limita o tamanho de cada rede. Alocação de muitos bits para um sufixo de host significa que uma determinada rede pode ser grande, mas limita o número de redes em nossa internet".

Para a acomodar o crescimento sem abandonar o esquema de endereçamento original, a resposta que nos mostra Comer(2015) foi uma técnica chamada endereçamento de sub-rede ou sub-rede, com ela um único prefixo de rede pode ser usado para várias redes físicas. Ao usar endereçamento sub-rede, temos em um endereço IPv4 de 32 bits como sendo uma parte de internet e uma parte local, onde a parte internet identifica um site, possivelmente com várias redes físicas, e a parte local identifica uma rede física e um host no site. Este método de endereçamento é dito autoidentificável, pois a fronteira entre o prefixo e o sufixo pode se identificada a partir do endereço, sem referência a informação externa.

Para Tanenbaum(2011) os endereços IPv4 eram divididos em cinco categorias. Essa alocação passou a se chamar endereçamento em classes. As classes A, B e C permitem até 128 redes com 16 milhões de hosts cada uma, 16.384 redes com até 65.536 hosts cada uma e 2 milhões de redes com até 256 hosts cada uma, respectivamente, também há suporte para multicast (o formato da classe D), em que um datagrama é direcionado para vários hosts. A figura abaixo exemplifica a divisão das classes e os respectivos intervalos de endereço de hosts.

Figura 3: *Formatos de endereços IPv4*



Fonte: *Tanembaun (2011), pg 282*

Em particular, Comer(2015) ressalta que “a classe de um endereço pode ser determinada a partir dos três bits de ordem superior, com dois bits sendo suficientes para distinguir entre as três classes primárias”, e que os endereços IPv4 são escritos como quatro números inteiros decimais separados por pontos, em que cada inteiro dá o valor de um octeto do endereço. Assim, o endereço na internet de 32 bits: 10000000 00001010 00000010 00011110 é escrito como 128.10.2.30

O endereçamento IPv4 tem sido muito usado e para Tanembaun(2011) “tem funcionado extremamente bem, conforme demonstrado pelo crescimento exponencial da Internet. Infelizmente, ele tornou-se vítima de sua própria popularidade: está próximo de esgotar os endereços disponíveis”.

Foi então que surgiu o projeto do IPv6, segundo Tanembaun(2011), “que apresentou uma oportunidade importante para melhorar todos os recursos no IPv4 que ficaram aquém do que se deseja agora. Para chegar a um protocolo que atendesse a todos esses requisitos”. E Comer(2015) mostra que “devido ao IPv6 ter herdado muitos dos conceitos, princípios, e mecanismos encontrados no IPv4, não podemos entender o IPv6 sem ter entendido o IPv4”.

Relembrando que cada endereço IPv6 ocupa 128 bits, totalizando 16 octetos. Este espaço de endereço garante que o IPv6 possa tolerar qualquer esquema de atribuição de endereço. “Na verdade, se a comunidade decidir mudar o esquema de

endereçamento mais tarde, o espaço de endereçamento é suficientemente grande para acomodar uma mudança.” (COMER, 2015).

Para ajudar a compreender o tamanho de espaço do endereçamento IPv6, Comer(2015) relaciona o endereçamento IPv6 “com o espaço físico disponível: a superfície da Terra tem cerca de 5,1 × 10^8 quilômetros quadrados, o que significa que há mais de 1024 endereços por metro quadrado” e ainda com estimativa de utilização de endereços, com o exemplo, “se os endereços fossem atribuídos à taxa de um milhão de endereços a cada microssegundo, levaria mais de 10 anos para atribuir todos os endereços possíveis”.

Com o tamanho de endereço maior surgiu um novo problema, como deveria ser a leitura manipulação e edição de tais endereços. Para Comer(2015), a notação binária é inviável, notação decimal com pontos, usada para IPv4, também não faz endereços IPv6 suficientemente compactos.

Para tornar os endereços ligeiramente mais compactos e mais fáceis de manipular, os desenvolvedores do IPv6 criaram a notação hexadecimal colon (colon hexadecimal notation – abreviada como hex colon), em que o valor de cada quantidade de 16 bits é representado em hexadecimal separado por dois pontos. Por exemplo, quando o valor mostrado anteriormente em notação decimal é traduzido para a notação colon hex e impresso usando o mesmo espaçamento, torna-se: 68E6:8C64:FFFF:FFFF:0:1180:96A:FFFF.

A notação colon hex tem a vantagem óbvia de requerer menos dígitos e menos caracteres de separação do que a decimal com ponto. Além disso, a notação colon hex inclui duas técnicas que a tornam extremamente úteis. Em primeiro lugar, a notação colon hex permite a compressão de zeros, em que uma série de zeros repetidos é substituída por um par de dois-pontos. (COMER, 2015)

Para garantir que a compressão de zeros produza uma interpretação unica, as normas especificam que ela pode ser aplicada a qualquer endereço IPv6, uma única vez, e Comer(2015) explica que “a compressão de zeros é especialmente útil porque as atribuições IPv6 criarão muitos endereços que contêm sequências de zeros contíguas”, e também a notação hexadecimal colon pode incorporar sufixos decimais com ponto; “tais combinações se destinam a serem usadas durante a transição do IPv4 para o IPv6”, o exemplo, citado por Comer(2015) traz a seguinte

sequência de caracteres é uma notação colon hex como válida: 0:0:0:0:0:0:128.10.2.1

Deve-se tomar nota que os números separados por colons especificam cada um o valor de uma quantidade de 16 bits, os números na parte decimal com ponto o valor de um octeto, cada. A “compressão de zeros pode ser utilizada com o número anterior para produzir uma cadeia de caracteres hex colon equivalente que se assemelha bastante a um endereço IPv4: ::128.10.2.1” (COMER, 2015)

Finalmente, o IPv6 estende a notação tipo CIDR, permitindo que um endereço possa ser seguido por uma barra e um inteiro que especificam um número de bits. Por exemplo, 12AB::CD30:0:0:0:0/60, especifica os primeiros 60 bits do endereço, que é 12AB00000000CD3 em hexadecimal, (COMER, 2015)

O IPv6 usa o termo “vizinho” para descrever outro computador na mesma rede, o “IPv6’s Neighbor Discovery Protocol (NDP) e permite a um host mapear entre um endereço IPv6 e um endereço de hardware” (COMER, 2015). O NDP inclui muitas outras funções, como apresentado Comer(2015), permite a um host encontrar o conjunto de roteadores em uma rede; determinar se um determinado vizinho ainda esta ativo; aprender o prefixo da rede que está em uso; determinar as características do hardware de rede; configurar um endereço para cada interface e verificar que nenhum outro host na rede o está usando; e encontrar o melhor roteador para usar para um determinado destino.

4 TCP E UDP

Para Comer(2015) o “TCP acrescenta funcionalidade substancial aos protocolos já discutidos, mas que sua implementação também é substancialmente mais complexa”. O TCP acrescenta o serviço transferência confiável garante a entrega de um fluxo de dados enviados de uma máquina para outra sem duplicação ou perda de dados, “a maioria dos protocolos confiáveis usa uma única técnica fundamental, conhecida como confirmação positiva com retransmissão (Positive Acknowledgement with Retransmition – PAR)”, nesta técnica o destinatário se comunica com a origem, enviando de volta uma mensagem de confirmação (ACK) cada vez que os dados chegam com sucesso, caso o remetente não receba a confirmação o dado é retransmitido.

O TCP é responsável por dividir o fluxo em pacotes, para tornar a transferência mais eficiente e minimizar o tráfego da rede, o “protocolo especifica o formato dos dados e as confirmações que dois computadores trocam para conseguir uma transferência confiável, bem como os procedimentos que os computadores usam para garantir que os dados chegaram corretamente”, e Comer(2015) mostra que o TCP “é tão significativo que todo o conjunto de protocolos da Internet é conhecido como TCP/IP”.

Como o TCP identifica uma conexão por um par de extremidades, um determinado número de porta TCP pode ser compartilhado por várias conexões na mesma máquina, como o TCP é um protocolo orientado a conexão, que exige que as duas extremidades concordem em participar antes de iniciar o tráfego TCP, os programas aplicativos nas duas extremidades da conexão precisam estabelecer uma conexão, (COMER, 2015).

Segundo Comer(2015) “para estabelecer uma conexão, o TCP usa um handshake de três vias, são trocadas três mensagens que permitem que cada lado concorde em formar uma conexão e saiba que o outro lado concordou”, o handshake são mensagens trocadas entre o transmissor e o receptor em uma ordem pre estabelecida.

O primeiro segmento de um handshake possui o bit SYN* marcado no campo de código. A segunda mensagem possui os bits SYN e ACK marcados, confirmando o primeiro segmento SYN, a mensagem de handshake final é apenas uma

confirmação, sendo simplesmente usada para informar ao destino que ambos os lados concordam que uma conexão foi estabelecida. Comer(2015) ressalta ainda que o “TCP em uma máquina espera passivamente pelo handshake, e o TCP em outra máquina o inicia. Porém, o handshake é cuidadosamente projetado para funcionar mesmo que as duas máquinas tentem iniciar uma conexão simultaneamente”. A conexão pode ser estabelecida de qualquer extremidade ou por ambas simultaneamente, após a conexão estabelecida, os dados podem fluir sem anormalidades.

Para terminar a conversação de modo controlado é utilizado a operação close. O TCP estabelece a importância que ambos os lados concordem em fechar a conexão e também saibam que ela está fechada, novamente o TCP utiliza o handshake de três vias para fechar a conexão.

O TCP usa uma combinação de números de porta de protocolo, de 16 bits, atribuída de forma estática e dinamica. Comer(2015) mostra que um conjunto de portas “foi atribuído por uma autoridade central para os serviços comumente acessados (por exemplo, servidores web e servidores de correio eletrônico). Outros números de porta estão disponíveis para que um sistema operacional aloque para aplicações locais, conforme necessário”. A seguir as mais comuns portas TCP utilizadas.

Quadro 1: *Principais portas atualmente atribuídos ao TCP*

Porta	Palavra-chave	Descrição
0	-	Reservado
7	echo	Eco
9	discard	Descartar
13	daytime	Hora do dia
19	chargen	Gerador de caracteres
20	ftp-data	File Transfer Protocol (dados)
21	ftp	File Transfer Protocol
22	ssh	Secure Shell
23	telnet	Conexão de Terminal
25	smtp	Simple Mail Transport Protocol
37	time	Hora
53	domain	Servidor de nome de domínio
80	www	World Wide Web
88	kerberos	Serviço de segurança Kerberos
110	pop3	Post Office Protocol versão 3
123	ntp	Network Time Protocol
161	snmp	Simple Network Management Protocol

179	bgp	Border Gateway Protocol
443	https	HTTP Seguro
860	iscsi	iSCSI (SCSI over IP)
993	imaps	IMAP Seguro
995	pop3s	POP3 Seguro
30301	bittorrent	Serviço BitTorrent

Fonte: *Comer (2015), pg 337*

As redes de comunicação por computador proveem entrega de pacote não confiável. Os pacotes podem ser perdidos quando os erros de transmissão interferem nos dados ou quando o hardware de rede falha e atrasam quando a rede fica muito carregada. Os sistemas de comutação de pacotes mudam de rotas dinamicamente, o que quer dizer que podem entregar pacotes fora de ordem, entregá-los após um atraso substancial ou entregar duplicatas. 286

O UDP (User Datagram Protocol), segundo Comer(2015) “não garante que as mensagens cheguem, nem que cheguem na mesma ordem em que foram enviadas, e também não fornece qualquer mecanismo para controlar a taxa com que a informação flui entre o par de hosts em comunicação”. As mensagens podem ser perdidas, duplicadas ou chegar fora de ordem ou ainda chegar mais rapidamente do que o destinatário é capaz de processá-los.

O UDP prove o serviço por melhor esforço não confiável de entrega sem conexão, usando IP para transportar mensagens entre máquinas. O UDP usa o IP para levar mensagens, mas adiciona a capacidade de distinguir entre os vários destinos dentro de um determinado computador host, (COMER, 2015).

O UDP como o TCP, distingue vários processos dentro de determinada máquina permitindo que os emissores e receptores atribuam um número de porta de protocolo a cada aplicativo. Uma mensagem UDP inclui dois números de porta de protocolo que identificam uma aplicação no computador remetente e um aplicativo no computador de destino. Comer(2015) cita que, “alguns números de porta UDP são bem conhecidos, sendo atribuídos permanentemente por uma autoridade central e honrados na Internet. Outros números de porta estão disponíveis para quaisquer programas aplicativos utilizarem”. Abaixo está relacionado as portas mais utilizadas do UDP.

Quadro 2: *Principais portas atualmente atribuídos ao UDP*

Porta	Palavra-chave	Descrição
0	-	Reserved
7	echo	Eco
9	discard	Descarte
11	systat	Usuários ativos
13	daytime	Hora do dia
15	netstat	Programa de status da rede
17	qotd	Citação do dia
19	chargen	Gerador de caracteres
37	time	Hora
42	name	Servidor de nome de host
43	whois	Quem é
53	nameserver	Domain Name Server
67	bootps	Servidor BOOTP or DHCP
68	bootpc	Cliente BOOTP or DHCP
69	tftp	Trivial File Transfer
88	kerberos	Serviço de segurança Kerberos
111	sunrpc	ONC Remote Procedure Call (Sun RPC)
123	ntp	Network Time Protocol
161	snmp	Simple Network Management Protocol
162	snmp-trap	Traps SNMP
264	bgmp	Border Gateway Multicast Protocol (BGMP)
389	idap	Lightweight Directory Access Protocol (LDAP)
512	biff	Comsat do UNIX
514	syslog	Log do System
520	rip	Routing Information Protocol (RIP)
525	timed	Daemon de hora
546	dhcpv6-c	Cliente DHCPv6
547	dhcpv6-s	Servidor DHCPv6
944	nsf	Service Network File System (NFS)
973	nfsv6	Network File System (NFS) overIPv6

Fonte: *Comer (2015), pg 280*

UDP é um protocolo “enxuto” pelo fato de que não aumenta muita coisa à semântica do IP. Ele simplesmente oferece aos programas aplicativos a capacidade de se comunicar usando o serviço de remessa de pacote em conexão e não confiável do IP.

Assim, as mensagens UDP podem ser perdidas, duplicadas, adiadas ou entregues fora da ordem, um par de programas aplicativos que utiliza UDP deve estar preparado para lidar com erros. Se um aplicativo UDP não resolve os erros, ele pode funcionar corretamente em uma LAN confiável, mas não em uma internet de

longa distância na quais problemas de atraso e perda são mais comuns, (COMER, 2015).

No esquema de camadas de protocolo, o UDP se encontra na camada de transporte, acima da camada 3, a camada de internet, e abaixo da camada 5, a camada de aplicação. Conceitualmente, a camada de transporte é independente da camada de internet, mas, na prática, elas interagem fortemente. O checksum UDP inclui os pseudo endereços com os endereços IP da origem e do destino, significando que o software UDP precisa interagir com o software IP para encontrar endereços IP antes de enviar datagramas, (COMER, 2015).

A camada IP é responsável só pela transferência de dados entre um par de hosts em uma internet, enquanto a camada UDP é responsável só pela diferenciação entre múltiplas fontes ou destinos dentro de um host.

Dentre outros protocolos importantes que podem ser citado temos o DHCP (Dynamic Host Configuration Protocol),ou protocolo de configuração dinâmica de host, que permite aos hosts serem “configurados com alguma informação básica, como seus próprios endereços IP”,(TANEMBAUN, 2011) e para Comer(2015) “o DHCP permite que um computador obtenha todas as informações necessárias para se comunicar em uma determinada rede (incluindo endereço IPv4, máscara de sub-rede e endereço de um roteador padrão) quando o computador inicia”.

Em uma rede precisa ter um servidor DHCP responsável pela configuração, “quando um computador é iniciado, ele tem um endereço Ethernet ou outro endereço da camada de enlace embutido na NIC(network interface card)”, mas não possui um endereço IP. O host envia uma solicitação de broadcast solicitando um endereço IP em sua rede, usando um pacote DHCP DISCOVER, esse pacote precisa alcançar o servidor DHCP. “Quando o servidor recebe a solicitação, ele aloca um endereço IP livre e o envia ao host em um pacote DHCP OFFER” (TANEMBAUN, 2011).

Para Tanembaun(2011) “um problema que surge com a atribuição automática de endereços IP a partir de um pool é por quanto tempo um endereço IP deve ser alocado”, se determinado host sair da rede e não retornar seu endereço IP ao servidor DHCP, esse endereço será permanentemente perdido, “para impedir que isso aconteça, a atribuição de endereço IP pode ser por um período de tempo fixo”.

As mensagens trocadas entre os hosts incluem mensagens de controle, os eventos inesperados são tradados pelo Internet Control Message Protocol ou ICMP, este protocolo também é usado para testar as conexões de rede e a internet. “Cerca de 12 tipos de mensagens ICMP são definidos. Cada tipo de mensagem ICMP é transportada encapsulada dentro de um pacote IP” (TANEMBAUN, 2011).

O ICMP é “uma parte integrante do IP que manipula mensagens de erro e controle”. Os equipamentos e hosts usam ICMP para enviar relatórios de problemas sobre datagramas de volta à origem que enviou o datagrama, uma mensagem ICMP sempre vai voltar para a fonte original do datagrama que causou o erro, (COMER, 2015).

O ICMP tem mensagens como destino inalcançável, informa que um datagrama não pode ser encaminhado para o seu destino; mensagens de redirecionar mensagens, informam a um host para que mude o primeiro salto em sua tabela de encaminhamento; mensagens de tempo excedido, para quando um limite de salto ou tempos de reconstituição expiram; mensagens de problema de parâmetro, para outros problemas de cabeçalho, (COMER, 2015).

Outras mensagens como de “requisição/resposta de eco (echo request/reply menssages) ICMP podem ser usadas para testar se um destino está acessível. Um conjunto de mensagens mais antigas ICMPv4 que foram destinadas a fornecer informações para inicialização de um host não é mais usado”(COMER, 2015).

Uma mensagem ICMP viaja na área de dados de um datagrama IP e tem três campos de comprimento fixo no início da mensagem: um campo de mensagem ICMP tipo, um campo código e um campo ICMP checksum. O tipo de mensagem determina o formato do restante da mensagem, bem como o seu significado, (COMER, 2015).

Quadro 3: Os principais tipos de mensagem ICMP

Tipo de mensagem	Descrição
Destination unreachable	O pacote não pôde ser entregue
Time exceeded	O campo TTL atingiu 0
Parameter problem	Campo de cabeçalho inválido
Source quench	Restringe o envio de pacotes
Redirect	Ensina uma rota a um roteador
Echo e Echo reply	Verificam se uma máquina está ativa

Timestamp request/reply	O mesmo que Echo, mas com registro de tempo
Router advertisement/solicitation	Encontra um roteador próximo

Fonte: *Tanenbaum (2011), pg 292*

O Address Resolution Protocol, (ARP), “permite que um host encontre endereço físico de um host alvo na mesma rede física, a partir somente do endereço IP do host alvo”(COMER, 2015) e para Tanembaun(2011) “a vantagem de usar o ARP sobre os arquivos de configuração é a simplicidade. O gerenciador do sistema não precisa fazer muito, exceto atribuir a cada máquina um endereço IP e decidir sobre as máscaras de sub-rede. O ARP faz o restante”

ARP é um protocolo de baixo nível que mascara o endereçamento utilizado pelo hardware de rede, que nos permite atribuir um endereço IP arbitrário para cada máquina, podemos pensar “em ARP como associado com o sistema de rede física, e não como parte dos protocolos da Internet”, e ainda o ARP pode “mapear um protocolo de endereço de alto nível arbitrário para um endereço de hardware de rede arbitrária. Na prática, a ARP só é usado para mapear os endereços IPv4 de 32 bits para endereços Ethernet de 48 bits” (COMER, 2015).

Para fazer o com que o ARP funcionar de forma mais eficiente, Tanenbaum(2011), cita as otimizações como “quando uma máquina executa o ARP, ela coloca o resultado em cache caso precise entrar em contato com a mesma máquina em breve. Da próxima vez, ela encontrará o mapeamento em seu próprio cache”, eliminando a necessidade de uma segunda mensagem de controle.

As entradas no cache ARP devem ter um tempo limite para permitir que os mapeamentos mudem, quando um host é configurado para usar um novo endereço IP, “Um modo mais inteligente de ajudar a manter atualizada a informação em cache e otimizar o desempenho é fazer com que cada máquina envie seu mapeamento por broadcast quando for configurada” (TANENBAUM, 2011).

Esta mensagem geralmente é feito na forma de um ARP procurando seu próprio endereço IP. Não pode haver resposta, mas como efeito colateral é possível criar ou atualizar uma entrada no cache ARP de cada host. “Isso é conhecido como ARP gratuito. Se uma resposta chegar (inesperadamente), duas máquinas receberam o mesmo endereço IP” (TANENBAUM, 2011).

5 CONSIDERAÇÕES FINAIS

Este trabalho foi desenvolvido com objetivo a apresentar os principais protocolos de comunicação para internet e redes de computadores bem como algumas de suas características, o trabalho foi fundamentado em pesquisas bibliográficas, os autores selecionados são referencia na área, tem como finalidade demonstrar a importância, os princípios e características dos mesmos.

Os protocolos e modelos apresentados neste trabalho incluem apenas alguns dos mais utilizados para o perfeito funcionamento da internet e rede de computadores, existem ainda muitos protocolos que não foram abordados neste trabalho, e estão presentes no nosso dia-a-dia, como exemplo temos o correio eletrônico ou e-mail, o carregamento de documentos da web, transferência de arquivos entre hosts dentre muitos outros.

A pesquisa demonstrou que os protocolos não só trabalham em conjunto como também são complementares e alguns ainda são interdependentes, ou ainda no caso de TCP e UDP tem o mesmo propósito geral, neste caso o transporte de dados entre hosts, mas apresentam funcionamentos distintos. O entendimento sobre o funcionamento e arquitetura dos protocolos apresentados serve de base para o estudo mais aprofundado do tema rede de computadores.

REFERÊNCIAS

COMER, D. E. **Interligação em Redes com TCP/IP**. Trad. 6. Rio de Janeiro: Campus, 2015

IBGE – Instituto Brasileiro de Geografia e Estatística. **Pesquisa Nacional por Amostra de Domicílios Contínua** - PNAD Contínua. Rio de Janeiro. 2018.

KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet: Uma abordagem top-down**. Trad. 7 ed. São Paulo: Addison Wesley, 2010.

PETERSON, L. L.; DAVIE, B. S. **Redes de Computadores: Uma abordagem de sistemas**. Trad. 5 ed. Rio de Janeiro: Campus, 2013.

TANENBAUM, A. S. **Redes de Computadores**. trad. 5 ed. Rio de Janeiro: Elsevier, 2011.