CENTROWEG - SENAI

DESENVOLVIMENTO DE SISTEMAS

PABLO RUAN TZELIKS

TRABALHO DE ARQUITETURA DE REDES

Jaraguá do Sul

2025

PABLO RUAN TZELIKS

UMA VISÃO GERAL SOBRE O MODELO TCP/IP

Trabalho apresentado à unidade curricular de Arquitetura de Redes, do serviço nacional de aprendizagem industrial (SENAI) - CentroWEG.

Professor: Carlos Fabio Andrade

Jaraguá do Sul
2025

SUMÁRIO

1 INTRODUÇÃO

O TCP/IP é a base de toda a comunicação moderna na internet. Não se trata apenas de um protocolo, mas de um conjunto completo de regras que orquestram a forma como os dados são enviados e recebidos em redes de computadores.

A sua importância se deve à sua capacidade de ser um modelo aberto, confiável e flexível. No entanto, para que o modelo funcione, é importante entender as camadas que o compõem.

Diante disso, o presente trabalho busca oferecer uma visão geral sobre o Modelo TCP/IP, explorando seus conceitos fundamentais, sua arquitetura em camadas e o papel de cada protocolo na garantia de uma comunicação eficiente e segura na internet.

2 FUNDAMENTOS DO MODELO TCP/IP

2.1 O que é o modelo TCP/IP e como ele se relaciona com o modelo OSI?

O modelo TCP/IP é uma arquitetura em camadas que especifica métodos de comunicação para redes de computadores, definindo protocolos e responsabilidades em níveis distintos para que dados possam ser enviados e recebidos entre sistemas diferentes.

Ao contrário do modelo OSI (Open Systems Interconnection), que possui sete camadas e surgiu como um modelo de referência teórico e pedagógico, o TCP/IP foi desenvolvido a partir de implementação prática para atender às necessidades da ARPANET e da Internet emergente.

Em termos de mapeamento, o TCP/IP costuma ser apresentado com quatro camadas (Aplicação, Transporte, Internet, Acesso à Rede), que podem ser relacionadas às sete camadas do OSI, embora o alinhamento não seja estritamente um-para-um.

2.2 Quais são as camadas do modelo TCP/IP e quais são suas funções principais?

4. Camada de Aplicação: fornece serviços de rede diretamente às aplicações do usuário (HTTP, SMTP, DNS, FTP, etc.). É responsável pela sintaxe e semântica dos dados trocados entre aplicações.

3. Camada de Transporte: garante a comunicação fim-a-fim entre processos, oferecendo serviços como entrega confiável (TCP) ou entrega sem conexão e leve (UDP), controle de fluxo e multiplexação de aplicações via portas.

2. Camada de Internet: encarrega-se do endereçamento lógico (IP) e do encaminhamento de pacotes através de múltiplas redes, implementando princípios de roteamento e fragmentação.

1. Camada de Acesso à Rede (Link/Enlace + Física): trata do transporte físico de bits, formatação de quadros, endereçamento físico (MAC) e acesso ao meio (Ethernet, Wi-Fi, interfaces físicas).

2.3 Como o TCP/IP garante a comunicação confiável e sem erros entre sistemas diferentes?

A confiabilidade é alcançada principalmente através de protocolos da camada de transporte, em particular o TCP, que implementa:

1. Estabelecimento de conexão (handshake) para sincronizar estados entre emissor e receptor.

2. Numeração de sequência e acknowledgments (ACKs) para confirmar recepção e permitir remontagem ordenada.

3. Retransmissão de segmentos perdidos com temporizadores (timers).

4. Controle de fluxo (por exemplo, janelas deslizantes) para evitar que o receptor seja sobrecarregado.

5. Controle de erros por somas de verificação (checksums) em segmentos, que detectam corrupção de dados.

3 FUNCIONAMENTO DAS CAMADAS

3.1 Responsabilidades de cada camada

4. Aplicação: formata dados, negocia protocolos de nível superior, realiza tradução de nomes e fornece interfaces para o usuário. Exemplos são: navegadores (HTTP/HTTPS), clientes de e-mail (SMTP/IMAP), serviços de nomes (DNS).

3. Transporte: multiplexa várias aplicações (através de portas), garante entrega fim-a-fim, realiza controle de fluxo e congestionamento (TCP) ou entrega de baixa latência sem garantias (UDP).

2. Internet: encapsula segmentos em pacotes IP, insere nos mesmos cabeçalhos com endereços lógicos, realiza fragmentação ou remoção de fragmentos quando necessário, e determina roteamento entre redes.

1. Acesso à Rede: converte pacotes em quadros físicos com endereçamento MAC, comanda transmissão real sobre mídias (seja par trançado, fibra, rádio), detecta e às vezes corrige erros de enlace.

3.2 Como o protocolo IP funciona para endereçamento e roteamento?

De maneira geral o IP (Internet Protocol) fornece duas funções centrais, são elas:

- Endereçamento lógico: cada interface de rede recebe um endereço IP (IPv4 ou IPv6) que identifica, de forma global (ou local, no caso de endereços privados), a origem e o destino de pacotes. O endereço IP é usado para determinar a rede de destino e, em algumas arquiteturas, a sub-rede e o host.

- Roteamento: ao enviar um pacote, o host coloca o endereço IP de destino no cabeçalho. Roteadores intermediários consultam suas tabelas de roteamento para decidir o próximo salto mais apropriado, encaminhando o pacote através de uma sequência de redes até alcançar a rede de destino. O comportamento

de roteadores é governado por protocolos de roteamento (estáticos ou dinâmicos) que constroem as tabelas com base em topologia e métricas.

Aspectos operacionais do IP incluem fragmentação (quando um pacote é maior que o MTU do enlace) e TTL (Time to Live) para evitar loops infinitos. O IP é, por design, um protocolo sem conexão e de "melhor esforço", a entrega confiável é delegada a camadas superiores.

3.3 Papel do protocolo TCP e como assegura a confiabilidade

O protocolo TCP tem como papel a transmissão de dados assegurando a entrega, diferentemente do UDP que não assegura sua entrega, porém busca maior velocidade. Dentre os principais pontos para assegurar a confiabilidade, são eles:

1. Handshake de três vias (SYN, SYN-ACK, ACK) para estabelecer uma conexão antes da transferência de dados.

2. Numeração de sequência de bytes e ACK cumulativo para rastrear quais dados foram recebidos.

3. Temporizadores e retransmissão quando ACKs não chegam a tempo.

4. Controle de fluxo (janela deslizante) para adaptar a taxa do transmissor à capacidade do receptor.

Mecanismos de controle de congestionamento (slow start, congestion avoidance, fast retransmit/fast recovery) para ajustar a taxa de envio à condição da rede. Checksum para detecção de corrupção no segmento.

Esses mecanismos combinados possibilitam uma comunicação confiável, ordenada e eficiente sobre uma rede que, em sua essência, não garante entrega.

4 PROTOCOLOS RELACIONADOS

4.1 Protocolos mais importantes associados ao TCP/IP

- IP (Internet Protocol) responsável pelo endereçamento lógico da internet.
- TCP (Transmission Control Protocol) realiza o transporte de dados, de maneira confiável.
- UDP (User Datagram Protocol) realiza transporte de dados, não assegura entrega, porém rapidez.
- HTTP / HTTPS relacionado a camada de Aplicação, protocolos da web, HTTPS em essência é mais segura, pela sua criptografia.
- FTP responsável por transferência de arquivos.
- DNS é quem faz a resolução de nomes, converte domínios em endereços de IP.
- ICMP (Internet Control Message Protocol) por esse protocolo que mensagens de diagnóstico e erro podem existir, pode ser observado ao executar o tracert no CMD.
- ARP (Address Resolution Protocol) resolve endereços IP para endereços MAC na rede local.
- DHCP é quem faz a atribuição dinâmica de endereços IP, automatizando esse processo para entre hosts e eliminando a necessidade de manipulação manual.
- TLS/SSL segurança na camada de transporte ou aplicação para criptografia.

4.2 Diferença entre TCP e UDP e situações de uso

- **TCP:** orientado à conexão. Fornece confiabilidade, ordenação e controle de fluxo. É adequado para aplicações que exigem precisão (transferência de arquivos, e-mail, páginas web com dados críticos).

- **UDP:** sem conexão. Possui baixo overhead, menor latência, não garante entrega nem ordenação é apropriado para aplicações sensíveis à latência que toleram perda de pacotes (streaming de áudio/vídeo em tempo real, jogos em tempo real, VoIP, DNS queries em muitos casos).

A escolha vai depender da necessidade de confiabilidade versus desempenho e latência.

4.3 Funcionamento do DNS no contexto do TCP/IP

O DNS (Domain Name System) traduz nomes legíveis (ex.: www.exemplo.com) em endereços IP. Seu funcionamento básico consiste em:

- Uma aplicação solicita resolução de nome ao resolvedor local (geralmente provedor ou cache do sistema operacional).

- Se o cache não tem a entrada, o resolvedor consulta servidores DNS hierarquicamente (servidores raiz → TLD → autoritativos) até obter o IP.

- A comunicação de consulta normalmente usa UDP (porta 53) para consultas e TCP para transferências de zonas ou respostas longas.

O DNS é fundamental ao TCP/IP pois permite o uso de nomes amigáveis em vez de números de IP e constitui uma infraestrutura distribuída e replicada.

5. SEGURANÇA DO MODELO TCP/IP

5.1 Vulnerabilidades comuns e mitigações

- Sniffing: captura de tráfego em redes não criptografadas. Pode ser resolvido com criptografía de enlace (WPA2/3) e de camada superior (TLS).

- Ataques Man-in-the-Middle (MitM): interceptação ativa entre comunicantes. Pode ser resolvido com uso de TLS com verificação de certificados, HSTS e autenticação mútua quando necessário.

- IP Spoofing: falsificação de endereço de origem IP. Pode ser resolvido com filtros de ingress (anti-spoofing), verificações em roteadores, autenticação nas camadas superiores.

- DDoS/DoS: saturação de recursos na rede ou serviço. Pode ser resolvido com arquiteturas de defesa (CDNs, balanceadores, scrubbing centers), rate limiting, filtragem BGP e lists de bloqueio.

- Vulnerabilidades em serviços da camada de aplicação: Sendo eles injeção, XSS, CSRF. Pode ser resolvido com práticas seguras de desenvolvimento, WAFs (Web Application Firewalls).

- Ataques a protocolos (ex.: ARP Spoofing): manipulação de rede local. Pode ser resolvido com uso de switches com proteção (dynamic ARP inspection), segmentação de rede e segurança em camada 2.

5.2 Integração de TLS/SSL ao TCP/IP

TLS (Transport Layer Security) é o principal mecanismo para prover confidencialidade, integridade e autenticação nas comunicações TCP/IP. Opera entre as camadas de Aplicação e Transporte , encapsulando protocolos de aplicação (como HTTP) para formar HTTPS.

TLS usa criptografia simétrica e assimétrica, certificados X.509 e handshake para estabelecer chaves seguras e verificar identidade do servidor (e opcionalmente do cliente).

5.3 Melhores práticas para proteção contra DoS e MitM

- Arquitetura redundante: espalhar serviços por múltiplas regiões e servidores.

- Filtragem e rate limiting: bloquear tráfego malicioso no perímetro e aplicar limites por IP/porta.

- Criptografia padrão: usar TLS para todo o tráfego sensível; preferir práticas modernas (TLS 1.2/1.3).

- Monitoramento e detecção: IDS/IPS, logs centralizados e análise comportamental.

- Políticas BCP e hardening: atualizações regulares, remoção de serviços desnecessários, uso de redes privadas virtuais (VPNs) e segmentação de rede.

- Proteção contra ARP/NDP spoofing (em IPv6): usar mecanismos de segurança em switches, RA Guard, e protocolos de segurança adicionais.

6 EVOLUÇÃO E FUTURO DO TCP/IP

6.1 Evolução histórica

O TCP/IP evoluiu desde implementações experimentais (ARPANET) até o conjunto de protocolos formalizados que sustentam a Internet. Ao longo do tempo, protocolos foram padronizados, o modelo foi refinado, e extensões surgiram para suportar novas demandas (mobilidade, segurança, qualidade de serviço, escalabilidade).

A evolução incluiu melhorias em TCP (novos algoritmos de controle de congestionamento), adoção em massa de IPv4 e, mais recentemente, o desenvolvimento e implantação gradual do IPv6.

6.2 Limitações do modelo e adaptações

Entre limitações do modelo original estão a escassez de espaço de endereçamento IPv4, segurança limitada embutida no protocolo IP original, e dificuldades para mobilidade e endereçamento dinâmico em escala massiva.

Dentre as adaptações e mudanças, posso incluir:

- IPv6 para resolver escassez de endereços.

- Mecanismos de segurança adicionais (IPsec para encapsulamento e autenticação em IP).

- NAT (Network Address Translation) como solução intermediária para falta de endereços, com impactos sobre transparência de ponta a ponta.

6.3 Impacto do aumento de dispositivos IoT

A proliferação de dispositivos IoT amplia requisitos de escalabilidade, gerenciamento de dispositivos, segurança embutida e consumo de energia. Isso de maneira geral exige:

- Endereçamento massivo (onde IPv6 é essencial).

- Protocolos leves (ex.: CoAP ou o MQTT em vez de HTTP para sensores).

- Soluções de gerenciamento e autenticação escaláveis.

- Proliferação de dados com novas tecnologias de radiofrequência, seja o Wi-Fi ou Bluetooth, porém hoje novos estão sendo usados, como o ProfiBus, LoraWAN, 5G, e etc.

- Novos desafios de segurança por dispositivos com recursos limitados e gestão de grandes volumes de tráfego telemetria.

Todas estas mudanças já estão sendo implementadas no mundo de hoje, já que a interconectividade e interoperabilidade são tópicos de grande importância atualmente, para cada vez mais computadores miniaturizados serem usado para diferentes propósitos.

7 IPV4 vs IPV6

7.1 Diferenças entre endereços IPv4 e IPv6 e como é feita a transição

1. Formato: IPv4 usa 32 bits (aproximadamente 4,3 bilhões de endereços). Já o IPv6 usa 128 bits (vastamente maior espaço de endereçamento).

2. Notação: IPv4 em decimal pontuado (ex.: 192.168.0.1); IPv6 em hexadecimal separado por dois pontos (ex.: 2001:0db8::1).

3. Funcionalidades: IPv6 inclui melhorias nativas (autoconfiguração, header simplificado para processamento eficiente, suporte obrigatório para IPsec em especificações originais, though use is optional).

4. Transição: realizada via técnicas como dual-stack (hosts e roteadores suportam ambos), tunneling (encapsulamento de IPv6 sobre IPv4) e tradução (NAT64/DNS64) para interoperabilidade.

7.2 Desafios e benefícios da adoção do IPv6

- Benefícios: espaço de endereços praticamente ilimitado, simplificação do roteamento em certas arquiteturas, autoconfiguração mais robusta e melhor suporte a mobilidade e hierarquias de endereçamento.

- Desafios: incompatibilidades com infraestruturas legadas, necessidade de atualizar equipamentos e software, complexidade operacional durante a fase de transição e barreiras organizacionais para migração.

7.3 Como a escassez de IPv4 impacta redes atuais

A falta de endereços IPv4 levou ao uso generalizado de NAT, que permite múltiplos hosts privados compartilharem um único endereço público. Isso introduz complexidade para aplicações P2P, quebra a transparência de ponta a ponta e

adiciona necessidade de traduções e soluções para traversal de NAT. A escassez motiva a adoção de IPv6 para evitar limitações de escala.

8. ROTEAMENTO E ARQUITETURA DE REDES

8.1 Como roteadores utilizam o modelo TCP/IP para encaminhar pacotes

Roteadores operam na camada de Internet, examinando o cabeçalho IP de cada pacote e consultando sua tabela de roteamento para identificar o próximo salto.

Eles não interpretam o conteúdo da camada de transporte (a não ser para NAT ou políticas), sua decisão baseia-se em prefixos de rede e métricas definidas por protocolos de roteamento.

O objetivo de roteadores é a comunicação entre diferentes redes, de maneira geral, roteadores precisam escolher a melhor rota até o IP final, e segui-la, roteador inicial faz o trabalho mais pesado, e depois os próximos roteadores, que são pontos de conexão de diferentes redes recebem o cabeçalho, e caso não sejam a rede final passam para a próxima mais perto.

Esse processo é iterado com o apoio das camadas L1, L2 e L3 até chegar no destino, sendo o IP final e seu MAC que será lido pelo Enlace, validado pela camada de Rede e assim a mensagem será transmitida. Tudo isso acontece em conjunto com a camada de Acesso a Rede e Internet no protocolo TCP/IP.

8.2 O que são tabelas de roteamento e como são usadas

Uma tabela de roteamento contém entradas do tipo: destino (prefixo de rede), máscara, próximo salto (next hop) e interface de saída. Estas entradas são preenchidas manualmente (roteamento estático) ou automaticamente via protocolos de roteamento dinâmico (ex.: OSPF, BGP, RIP). O roteador usa a melhor correspondência (longest prefix match) para escolher o caminho mais apropriado.

8.3 Protocolos de roteamento

- Interior Gateway Protocols (IGP): OSPF, IS-IS e RIP. Usados dentro de uma mesma rede administrativa.

- Exterior Gateway Protocol (EGP): BGP. Usado entre sistemas autônomos na Internet pública para troca de rotas.

Cada protocolo tem métricas e objetivos próprios (menor custo, política, escalabilidade) e influencia a forma como os pacotes trafegam entre domínios.

9. COMPARAÇÃO COM OUTROS MODELOS DE REDES

9.1 Principais diferenças e semelhanças entre TCP/IP e OSI

- Abordagem: OSI é um modelo de referência de sete camadas mais didático; TCP/IP é uma arquitetura prática de quatro camadas baseada em protocolos reais.

- Granularidade: OSI separa mais funções (ex.: sessão e apresentação) que no TCP/IP estão frequentemente agrupadas na camada de aplicação.

- Adoção: TCP/IP tornou-se padrão de fato para a Internet por sua implementação prática; OSI é usado para ensino e padronização conceitual.

- Semelhanças: ambos usam conceito em camadas, encapsulamento e interfaces bem definidas entre níveis.

9.2 Eficiência do TCP/IP para implementação e Internet moderna

O TCP/IP provou ser eficiente por sua simplicidade e por ter sido projetado e testado em implementações reais, o que facilitou a adoção massiva. Sua flexibilidade (permitir múltiplos protocolos de aplicação, transporte e roteamento) e filosofia de “camadas mínimas” contribuíram para robustez, extensibilidade e interoperabilidade.

10. DESEMPENHO E EFICIÊNCIA

10.1 Como o modelo lida com congestionamento e controle de fluxo

O controle de fluxo (fim-a-fim) evita que um receptor mais lento seja inundado por um transmissor rápido, é implementado por TCP via janelas deslizantes.

Controle de congestionamento (rede) são algoritmos TCP que ajustam a taxa de envio conforme a percepção de congestionamento (perda de pacotes ou sinais explícitos).

10.2 Técnicas de otimização: algoritmos de controle de congestionamento

- TCP Reno: introduziu fast retransmit e fast recovery; base para muitos outros.

- TCP Cubic: algoritmo padrão em muitos sistemas modernos (ex.: Linux) projetado para comportamento adequado em redes de alta largura de banda e alta latência.

- BBR (Bandwidth-Delay Product based), variantes que tentam modelar capacidade disponível em vez de reagir apenas a perdas.

11. IMPACTO DO TCP/IP NO MUNDO DIGITAL

11.1 Impacto na popularização da Internet

O modelo TCP/IP, por permitir a interconexão de redes heterogêneas com um conjunto de protocolos padrão, foi decisivo para a rápida expansão e adoção da Internet global. Ele permitiu interoperabilidade entre sistemas diversos, facilitou inovação em camadas superiores (aplicações web, e-mail, VoIP) e estabeleceu fundamentos para serviços distribuídos e economia digital.

11.2 Contribuição para interconectividade entre LANs, WANs e Internet

TCP/IP funciona como uma linguagem comum para redes locais (LANs), metropolitano (MAN) e ampla (WAN), abstraindo diferenças físicas e permitindo que roteadores e gateways façam a tradução de meios e encaminhamento. A modularidade do modelo possibilita que novas tecnologias de enlace e novos serviços sejam integrados sem reescrever todo o conjunto protocolar.

REFERÊNCIAS

FORTINET. O que é TCP/IP?. Disponível em: https://www.fortinet.com/resources/cyberglossary/tcp-ip. Acesso em: 15 set. 2025.

CLOUDFLARE. O que é TCP/IP?. Disponível em: https://www.cloudflare.com/pt-br/learning/ddos/glossary/tcp-ip/. Acesso em: 15 set. 2025.

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO (UFRJ). Introdução ao IP Security. Disponível em: https://www.gta.ufrj.br/grad/03_1/ip-security/paginas/introducao.html. Acesso em: 15 set. 2025.

IBM. Protocolos TCP/IP. Disponível em: https://www.ibm.com/docs/pt-br/aix/7.3.0?topic=protocol-tcpip-protocols. Acesso em: 15 set. 2025.

KUROSE, James F.; ROSS, Keith W. Computer Networking: A Top-Down Approach. (Livro-referência clássico para entendimento de camadas, protocolos e aplicações.)

TANENBAUM, Andrew S.; WETHERALL, David J. Computer Networks. (Aborda princípios, protocolos e arquitetura de redes.)

RFC 791 — Internet Protocol (IP). (Especificação original do IPv4.)

RFC 8200 — Internet Protocol, Version 6 (IPv6) Specification. (Especificação do IPv6.)

Documentação IETF e publicações sobre TCP (TCP RFCs históricas) e sobre algoritmos de congestionamento (publicações e RFCs pertinentes).

Manuais e guias práticos: Wireshark User Guide; material de laboratórios de redes (cursos e tutoriais).