

Introdução às Redes e à Internet

Aula 02

<Módulo 01 />

Protocolos de comunicação em Redes



Introdução

Na vastidão do mundo digital, onde dispositivos e sistemas interagem para transmitir informações e dados, os protocolos de comunicação desempenham um papel essencial.

São os protocolos que, em muitos aspectos, possibilitam que nossa era de conectividade global seja tão dinâmica e eficiente.

Neste encontro, exploraremos o que são protocolos de comunicação e por que eles são elementos fundamentais na transmissão de dados.

Definição

Em essência, um protocolo de comunicação é um conjunto de regras e convenções que permitem a comunicação e a troca de informações entre dispositivos, sistemas e redes.

Essas regras estabelecem um padrão para a formatação de mensagens, a sequência de ações a serem seguidas e como os dispositivos devem responder às informações recebidas.

Por meio dos protocolos, diferentes partes podem entender-se, independentemente de suas origens, sistemas operacionais ou tecnologias subjacentes.

A metáfora mais simples para entender protocolos de comunicação é pensar neles como uma linguagem comum usada por dispositivos eletrônicos para "conversar".

Assim como a comunicação entre seres humanos requer um idioma compartilhado, a comunicação digital requer protocolos que definam como os dados são estruturados, transmitidos e interpretados.



Importância

A importância dos protocolos na transmissão de dados é difícil de ser subestimada.

Eles são o alicerce que sustenta o funcionamento da internet, redes locais, sistemas de telefonia, e uma ampla gama de tecnologias e aplicativos.

Eles garantem que, quando você envia um e-mail, navega na web, assiste a um vídeo em streaming ou faz uma chamada de voz pela internet, os dados sejam transmitidos corretamente e entendidos pelos dispositivos de destino.

Imagine a internet como um vasto sistema rodoviário, com inúmeros veículos (dados) viajando de um lugar para outro.

Protocolos de comunicação são como as regras de trânsito que garantem que esses veículos sigam rotas específicas, usem pistas apropriadas e respeitem semáforos e placas de sinalização para evitar colisões e garantir que a entrega dos dados ocorra de forma segura e eficaz.

Sem protocolos de comunicação, a comunicação digital seria caótica e ineficiente.

Dispositivos e sistemas não conseguiriam entender uns aos outros, levando a erros, perda de dados e desconexões.

Portanto, é a padronização proporcionada pelos protocolos que permite a interconexão contínua e a transmissão confiável de informações em nosso mundo digital.

Exploraremos os diferentes tipos de protocolos de comunicação, sua estrutura e funcionamento, e como eles desempenham papéis essenciais em nossas interações diárias com a tecnologia digital.

Protocolos de comunicação em Redes

Tipos

Protocolos de comunicação desempenham um papel crucial em possibilitar a transmissão eficiente de dados e informações em redes e sistemas digitais.

Eles se enquadram em várias categorias, dependendo de sua função e camada de atuação.

Dividem-se em 3 (três) tipos: Protocolos de Rede, Protocolos de Transporte e Protocolos de Aplicação.

Protocolos de Rede

Os protocolos de rede são fundamentais para a comunicação entre dispositivos em uma rede.

Eles operam na camada de rede e têm a responsabilidade de encaminhar pacotes de dados de um dispositivo de origem para um dispositivo de destino. Um dos protocolos de rede mais amplamente utilizados é o **TCP/IP** (*Transmission Control Protocol/Internet Protocol*), que é a espinha dorsal da Internet.

As principais funções e responsabilidades dos protocolos de rede incluem:

- **Roteamento de dados**
Determinar a melhor rota para os dados viajarem de um ponto a outro na rede.
- **Endereçamento**
Atribuir endereços IP únicos a cada dispositivo na rede para identificação.
- **Encapsulamento**
Incluir informações adicionais (cabeçalhos) em pacotes de dados para direcionar, verificar e proteger a transmissão.



Protocolos de Transporte

Os protocolos de transporte operam na camada de transporte e são responsáveis por gerenciar a comunicação ponto a ponto entre dispositivos finais. Dois protocolos de transporte amplamente utilizados são o **TCP** (*Transmission Control Protocol*) e o **UDP** (*User Datagram Protocol*).

As diferenças entre esses dois protocolos são fundamentais e podem ser resumidas da seguinte maneira:

- **TCP** (*Transmission Control Protocol*)
Este protocolo é conhecido por sua confiabilidade. Ele estabelece uma conexão entre os dispositivos de origem e destino e garante que os dados sejam entregues sem erros e na ordem correta. É amplamente utilizado em aplicativos que requerem transferência segura de dados, como navegação na web, e-mails e transferência de arquivos.
- **UDP** (*User Datagram Protocol*)
O UDP, por outro lado, é mais focado na velocidade. Ele não estabelece uma conexão permanente e não garante a entrega de dados. É usado em aplicativos que priorizam a velocidade sobre a confiabilidade, como videoconferências e transmissões em tempo real.



Protocolos de comunicação em Redes

Protocolos de Aplicação

Os protocolos de aplicação são voltados para a interação entre aplicativos e serviços na camada de aplicação. Eles são projetados para facilitar tarefas específicas, como a transferência de páginas da web, o envio de e-mails ou o compartilhamento de arquivos. Alguns exemplos notáveis de protocolos de aplicação incluem:

- **HTTP** (*Hypertext Transfer Protocol*)
Usado para a transferência de páginas da web, o HTTP permite que navegadores se comuniquem com servidores da web para solicitar e receber conteúdo.
- **SMTP** (*Simple Mail Transfer Protocol*)
Responsável pelo envio de e-mails, o SMTP é fundamental para a comunicação por e-mail e a entrega de mensagens.
- **FTP** (*File Transfer Protocol*)
O FTP é usado para transferir arquivos de um computador para um servidor ou vice-versa.
É amplamente utilizado para gerenciar o armazenamento de arquivos e o compartilhamento de dados.



RFC (*Request for Comments*)

Um **RFC**, que significa "*Request for Comments*" (Solicitação de Comentários), é um tipo de documento técnico que descreve padrões, protocolos, procedimentos e informações relevantes para a comunidade da Internet.

Embora o nome possa sugerir que sejam documentos sujeitos a revisões ou comentários, os **RFCs** têm um status especial.

Eles são criados, mantidos e publicados pela *Internet Engineering Task Force* (**IETF**), uma organização responsável por estabelecer padrões técnicos para a Internet.

Os **RFCs** desempenham um papel crítico na evolução e funcionamento da Internet e das redes de computadores em geral.

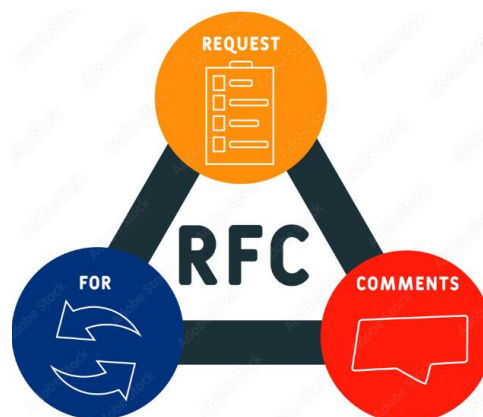
- **Padronização**
 - Os RFCs estabelecem padrões técnicos que garantem a interoperabilidade e compatibilidade entre dispositivos e sistemas em todo o mundo.
 - Eles servem como referência para a implementação de tecnologias e protocolos.
- **Inovação e Evolução**
 - A Internet é um ambiente em constante evolução, com novas tecnologias e protocolos sendo desenvolvidos regularmente.
 - Os RFCs fornecem um meio de documentar e compartilhar essas inovações, permitindo que a comunidade global de tecnologia as adote e construa sobre elas.
- **Resolução de Problemas**
 - Os RFCs frequentemente abordam desafios técnicos específicos e oferecem soluções para problemas que surgem na operação da Internet.
 - Eles servem como valiosos recursos de solução de problemas para profissionais de TI.
- **Referência Autoritária**
 - Quando há dúvidas ou debates sobre como uma tecnologia ou protocolo deve ser implementado, os RFCs servem como fontes autoritárias que podem ser consultadas para esclarecimento.

Protocolos de comunicação em Redes

RFC de protocolos importantes

Para aprofundar seus estudos, recomendamos a leitura dos RFCs relativos aos protocolos apresentados neste encontro:

- **RFC 793 (TCP)**
<https://www.rfc-editor.org/info/rfc793>
- **RFC 768 (UDP)**
<https://www.rfc-editor.org/info/rfc768>
- **RFC 7231 (HTTP)**
<https://www.rfc-editor.org/info/rfc7231>
- **RFC 768 (HTTPS)**
<https://www.rfc-editor.org/info/rfc2818>
- **RFC 5321 (SMTP)**
<https://www.rfc-editor.org/info/rfc5321>
- **RFC 959 (FTP)**
<https://www.rfc-editor.org/info/rfc959>



Estrutura de um Protocolo de Comunicações

Os protocolos de comunicação são essenciais para a transmissão de dados e informações em sistemas digitais, como redes de computadores.

Eles são estruturados de forma organizada e padronizada para garantir que os dados sejam transmitidos de forma correta e eficaz.

A estrutura de um protocolo de comunicação inclui diversos componentes, cada um com funções específicas que desempenham um papel fundamental na comunicação entre dispositivos.

Vamos explorar os componentes comuns em um protocolo e como essas estruturas garantem a transmissão precisa dos dados.

• Cabeçalhos

O cabeçalho é a parte inicial de um pacote de dados transmitido por um protocolo. Ele contém informações críticas que os dispositivos e sistemas usam para processar os dados.

Os elementos típicos encontrados em um cabeçalho incluem:

• Endereçamento

Os endereços de origem e destino, que indicam de onde os dados vêm e para onde estão indo.

• Controle de Fluxo

Informações sobre como o fluxo de dados deve ser gerenciado, evitando sobrecargas ou congestionamentos na rede.

• Identificação de Protocolo

Indica qual protocolo está sendo usado para que o receptor saiba como interpretar os dados.

• Mensagens

As mensagens constituem a parte principal dos dados transmitidos por um protocolo.

Elas contêm as informações reais que estão sendo enviadas de um dispositivo para outro.

As mensagens podem ser divididas em várias partes ou segmentos, dependendo da complexidade da comunicação.

A estrutura de mensagens é projetada de acordo com a finalidade do protocolo, e a organização das informações pode variar amplamente.

• Campos de Dados

Os campos de dados são segmentos específicos das mensagens que contêm informações de interesse.

Eles são organizados em uma estrutura definida e têm formatos previsíveis.

Os campos de dados contêm informações que são cruciais para a aplicação de destino, e a maneira como esses campos são estruturados e codificados é especificada no protocolo.

Protocolos de comunicação em Redes

Garantindo a Transmissão Correta

A estrutura de um protocolo é projetada para garantir que os dados sejam transmitidos corretamente. Isso é alcançado por meio de várias técnicas e verificações:

- **Integridade de Dados**

Muitos protocolos incluem verificação de integridade para garantir que os dados não foram corrompidos durante a transmissão.

Isso é frequentemente feito usando somas de verificação ou códigos de detecção de erros.

- **Sequenciamento**

- Protocolos de transporte, como o TCP, garantem que os dados sejam transmitidos na ordem correta e que todos os pacotes sejam entregues.

- **Confirmação e Retransmissão**

- Protocolos como o TCP incorporam mecanismos para confirmar a recepção de dados e retransmiti-los em caso de perda ou erro.

- **Gerenciamento de Erros**

- Protocolos podem incluir medidas para corrigir erros ou solicitar a retransmissão de dados em caso de problemas.



A estrutura organizada dos protocolos, incluindo cabeçalhos, mensagens e campos de dados, bem como as verificações de integridade e o gerenciamento de erros, são projetadas para garantir que os dados sejam transmitidos de forma confiável, independentemente do ambiente de rede.

Isso é essencial para a transmissão bem-sucedida de informações em sistemas digitais complexos, onde a precisão e a confiabilidade são imperativos.

Protocolos de Segurança na Comunicação Online

A comunicação online desempenha um papel crucial em nossa sociedade digital, facilitando transações financeiras, troca de informações confidenciais e muito mais. No entanto, com a crescente ameaça de ataques cibernéticos e interceptações não autorizadas, a segurança da comunicação se tornou uma prioridade.

É aí que entram os protocolos de segurança, como **SSL/TLS** (*Secure Sockets Layer/Transport Layer Security*), que desempenham um papel vital na proteção de informações sensíveis durante a transmissão.

SSL/TLS para Criptografia de Dados

O SSL/TLS é um conjunto de protocolos de segurança projetados para criar uma camada segura de comunicação entre um cliente e um servidor.

A criptografia é o pilar desses protocolos e garante que os dados transmitidos sejam ilegíveis para qualquer pessoa que tente interceptá-los.



Protocolos de comunicação em Redes

Importância do SSL/TLS

- **Criptografia de Dados**
 - Quando você acessa um site que usa SSL/TLS (geralmente reconhecido pelo "https://" na barra de endereços), seus dados são criptografados antes de serem transmitidos pela Internet.
 - Isso significa que, mesmo se alguém interceptar as informações, elas aparecerão como texto ilegível, a menos que possuam a chave de descryptografia correta.
- **Proteção da Privacidade**
 - A criptografia SSL/TLS protege a privacidade do usuário, garantindo que informações sensíveis, como senhas, informações de pagamento e mensagens pessoais, permaneçam confidenciais.
- **Autenticidade e Integridade**
 - Além da criptografia, o SSL/TLS verifica a autenticidade dos sites, garantindo que você está se comunicando com o servidor legítimo, e também protege a integridade dos dados, impedindo que sejam alterados durante a transmissão.
- **Proteção Contra Intercepção e Ataques**
 - O SSL/TLS é uma defesa eficaz contra intercepções de dados por hackers e ataques de homem no meio, em que terceiros tentam roubar informações durante a comunicação.

Importância da Proteção de Informações Sensíveis

A proteção de informações sensíveis na comunicação online é fundamental por várias razões:

- **Roubo de Identidade**
 - Dados pessoais, como números de seguro social e informações de cartão de crédito, podem ser usados para roubo de identidade se caírem nas mãos erradas.
 - A criptografia SSL/TLS ajuda a evitar o acesso não autorizado a esses dados.
- **Segurança Financeira**
 - Transações financeiras, como compras online e transações bancárias, envolvem informações de pagamento.
 - A segurança dessas transações é vital para evitar fraudes e perdas financeiras.
- **Confidencialidade Empresarial**
 - Empresas precisam proteger informações confidenciais, como planos estratégicos, propriedade intelectual e comunicações internas, para evitar vazamentos de dados e espionagem industrial.
- **Conformidade Regulatória**
 - Muitas regulamentações governamentais e padrões do setor exigem a proteção de informações sensíveis, e o não cumprimento dessas normas pode resultar em penalidades legais.

Em resumo, os protocolos de segurança, como SSL/TLS, são elementos fundamentais na proteção de informações sensíveis durante a comunicação online.

Eles desempenham um papel crucial na manutenção da privacidade, autenticidade e integridade dos dados, contribuindo para um ambiente digital mais seguro e confiável.

É fundamental que empresas e usuários adotem esses protocolos para proteger seus dados e manter a segurança online.

Protocolos de comunicação em Redes

Lei Geral de Proteção de Dados

- **Lei nº 13.709/2018**

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

A Lei Geral de Proteção de Dados, ou LGPD, é uma legislação brasileira que regula a coleta, o armazenamento, o tratamento e a transferência de dados pessoais.

A LGPD foi sancionada em setembro de 2020 e entrou em vigor em setembro de 2021.

Ela é inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia e visa proteger os direitos de privacidade e autodeterminação das pessoas em relação aos seus dados pessoais.



Importância da LGPD

- **Proteção da Privacidade**

Ela fortalece a proteção da privacidade e da integridade dos dados pessoais, garantindo que as empresas colem e processem informações pessoais de maneira legal, justa e transparente.

- **Direitos dos Indivíduos**

A LGPD concede aos indivíduos maior controle sobre seus dados, permitindo que eles acessem, corrijam, excluam ou restrinjam o processamento de suas informações pessoais.

- **Transparência**

As organizações são obrigadas a informar aos titulares dos dados como suas informações são coletadas e processadas, promovendo maior transparência.

- **Responsabilidade Empresarial**

A LGPD impõe responsabilidades às empresas que coletam e processam dados pessoais, incentivando a implementação de medidas de segurança para proteger esses dados.

- **Consentimento Informado**

Requer que as organizações obtenham o consentimento explícito dos titulares dos dados antes de coletar e processar informações pessoais.

- **Sanções por Não Conformidade**

A lei prevê multas substanciais para organizações que não cumprem suas disposições, incentivando a conformidade.

- **Relevância Internacional**

A LGPD alinha o Brasil com as regulamentações internacionais de privacidade, facilitando a transferência de dados pessoais entre o Brasil e outras jurisdições.