TEMA 2
Protocolo de Rede
Habilidades

- Compreensão de Protocolos em Camadas
- Análise de Pacotes
- Configuração de Protocolos de Rede
- Gerenciamento de Protocolos de Roteamento
- Segurança de Protocolos
- Resolução de Problemas de Protocolo

Introdução a Protocolos

Afinal, o que é um protocolo? O protocolo **é uma tecnologia que permite a comunicação entre os computadores**, ou seja, se tiver duas pessoas que falam em idiomas diferentes, não há possibilidade de ter uma comunicação nesse ambiente.

Para haver comunicação necessita ter um tradutor, para que possa estabelecer uma comunicação entre essas pessoas, a função do protocolo é a mesma do tradutor, ele possibilita a comunicação entre os computadores.
Protocolo é um **conjunto de regras, e métodos que devem ser seguidos para enviar e receber informações em uma rede**, é a forma que possibilita a comunicação entre os computadores.

Existem variados protocolos para executar distintas tarefas na rede como, para enviar e receber arquivos (FTP), testar a conectividade de rede (ICMP), acessando a internet para enviar e receber informações:

1. ARP (Address Resolution Protocol)
Função: Resolve endereços IP em endereços MAC.
Descrição: ARP é usado dentro de redes locais para mapear um endereço IP (que é usado na camada de rede) a um endereço MAC (que é usado na camada de enlace). Quando um dispositivo precisa enviar dados a outro dispositivo na mesma rede local, ele usa ARP para descobrir o endereço MAC correspondente ao endereço IP de destino.

2. HTTP (HyperText Transfer Protocol)
Função: Protocolo para transferência de hipertexto.
Descrição: HTTP é o protocolo usado na World Wide Web para transferir páginas web. Quando você acessa um site, o navegador envia uma solicitação HTTP ao servidor web, que responde com o conteúdo da página solicitada.

3. FTP (File Transfer Protocol)
Função: Transferência de arquivos entre sistemas.
Descrição: FTP é usado para transferir arquivos entre um cliente e um servidor na rede. Ele suporta autenticação e pode ser usado para baixar e enviar arquivos. FTP opera em duas conexões paralelas, uma para controle (porta 21) e outra para dados (porta 20).

4. TCP (Transmission Control Protocol)
Função: Protocolo de controle de transmissão.
Descrição: TCP é um protocolo de transporte que fornece uma conexão confiável e orientada a conexão entre dois dispositivos. Ele garante a entrega dos pacotes na ordem correta e sem perdas. TCP é usado por muitos protocolos de aplicação, como HTTP, FTP, e SMTP.

5. ICMP (Internet Control Message Protocol)
Função: Protocolo de mensagens de controle na Internet.
Descrição: ICMP é usado para enviar mensagens de erro e de controle na rede. Um dos usos mais comuns do ICMP é o comando "ping", que verifica a conectividade entre dois dispositivos na rede.

6. IP (Internet Protocol)
Função: Protocolo de endereçamento e roteamento na Internet.
Descrição: IP é responsável pelo endereçamento e roteamento dos pacotes de dados na rede. Cada dispositivo na rede possui um endereço IP único. Existem duas versões principais do IP: IPv4 e IPv6.

7. SMTP (Simple Mail Transfer Protocol)
Função: Protocolo para envio de e-mails.
Descrição: SMTP é usado para enviar e-mails de um cliente para um servidor de e-mails ou entre servidores de e-mail. Ele opera na porta 25 e é um dos principais protocolos para o envio de e-mails na Internet.

8. Telnet
Função: Protocolo para comunicação remota de texto.
Descrição: Telnet permite que um usuário se conecte a outro dispositivo na rede para gerenciamento remoto. Ele proporciona uma interface de linha de comando, mas não é seguro porque os dados, incluindo senhas, são transmitidos em texto claro.

9. UDP (User Datagram Protocol)
Função: Protocolo de datagramas de usuário.
Descrição: UDP é um protocolo de transporte que não garante entrega confiável, ordem, ou proteção contra duplicatas. Ele é mais rápido que o TCP e é usado em aplicações onde a velocidade é crítica e alguma perda de dados é tolerável, como streaming de vídeo e jogos online.

10. NNTP (Network News Transfer Protocol)
Função: Protocolo para transferência de artigos de Usenet.
Descrição: NNTP é usado para distribuir, postar, e ler artigos de grupos de discussão da Usenet. Ele opera na porta 119 e permite a comunicação entre servidores de notícias e clientes de notícias.

Funções dos Protocolos?

Como sabemos o protocolo é um conjunto de regras, que se caracterizam ser mais regido por tópicos que os determinam, os tópicos são esses:

- **(Sintaxe):** É o padrão dos dados e a forma sequenciada em que os dados são demonstrados, ou seja, esses padrões que determinam a função do byte a byte, é como uma "gramática" do "idioma" utilizado na comunicação;
- **(Semântica):** Representa um padrão dos dados (Sintaxe), para dar um significado à mensagem;
- **(Timing):** Estabelece uma velocidade de transmissão dos "pacotes" (pedaços da mensagem), ele pretende definir uma rapidez/velocidade concebível de comunicação no qual possa ser sustentado em todas as partes que está se mantendo a comunicação.

O protocolo tem funções predeterminada para obter a comunicação entre os hosts:

1. **(Endereçamento):** Determina qual o destino da mensagem, para enviar uma carta necessita ter um destinatário para que a carta chega ao seu destino, o endereçamento tem o mesmo papel para qual seu host quer se comunicar;
2. **(Sequência e Numeração):** Identifica as mensagens por meio de um número sequencial;

3. **(Estabelecer a conexão):** Constitui um canal lógico entre as duas pontas (Túnel) para estabelecer a troca das mensagens;
4. **(Controle de erros):** Identifica e corrige os erros durante a comunicação;
5. **(Retransmissão):** Se o sinal (ACK) não é recebido no destinatário, ou quando a mensagem não é recebida em seu destino;
6. **(Confirmação de recebimento):** Envia uma confirmação para cada pacote recebido (ACK);
7. **(Conversão de Código):** Faz um ajuste dos códigos de acordo com as particularidades do destinatário.

A grande maioria dos hosts e hardware de rede não falam a mesma língua, ou seja, se não houver um protocolo para fazer a (tradução) entre os hosts, não haverá comunicação.

Cada protocolo é definido por um padrão, existem basicamente dois tipos de padrão:
- **Facto:** São padrões que são **usados pela comunidade**, principalmente por fabricantes quando lançam novos produtos, mas que ainda não foram aprovados por um comitê reconhecido, como ISO ou ANSI. Um exemplo é o protocolo IP;
- **Jure:** São **usadas pelos fabricantes** quando lançam novos produtos, porém ainda não tem aprovação pelos comitês reconhecidos.

Os protocolos são reconhecidos pelos comitês regularizadores, um exemplo claro é o modelo OSI, passam pelas especificações pelo comitê avaliador RFC (request for change).

CAMADAS OSI (Open Systems Interconnection):

As Sete Camadas do Modelo OSI:

1) Camada Física (Physical Layer)

Função: Trata da **transmissão e recepção dos dados brutos sob a forma de bits sobre um meio físico**. Inclui especificações elétricas, mecânicas e procedurais.
Exemplos: Cabos, conectores, hubs, repetidores, modems

2) Camada de Enlace de Dados (Data Link Layer)

Função: Fornece a **transferência de dados diretamente entre dois dispositivos na mesma rede local**. Garante a detecção e, opcionalmente, a correção de erros que possam ocorrer na camada física.
Subcamadas: LLC (Logical Link Control) e MAC (Media Access Control).
Exemplos: Switches, bridges, endereços MAC, Ethernet, Modem a Cabo (multiplexação)

3) Camada de Rede (Network Layer)

Função: Responsável pelo **roteamento de pacotes de dados entre redes diferentes e pela determinação do caminho mais eficiente para o envio dos dados**.
Exemplos: Roteadores, endereços IP, ICMP.

4) Camada de Transporte (Transport Layer)

Função: **Garante a entrega confiável de dados entre dois dispositivos finais**, independentemente da rede física. Inclui controle de fluxo, segmentação e reassembly, e controle de erro fim a fim.
Exemplos: TCP (Transmission Control Protocol), UDP (User Datagram Protocol).

5) Camada de Sessão (Session Layer)

Função: **Estabelece, gerencia e termina conexões entre aplicativos**. Coordena a troca de dados e controla o diálogo (half-duplex ou full-duplex).
Exemplos: RPC (Remote Procedure Call), sessões de gerenciamento.

6) Camada de Apresentação (Presentation Layer)

Função: Tradução, criptografia e compressão de dados. **Converte dados de um formato usado pela aplicação para um formato comum na rede e vice-versa**.
Exemplos: SSL/TLS (Secure Sockets Layer/Transport Layer Security), JPEG, ASCII, EBCDIC.

7) Camada de Aplicação (Application Layer)

Função: Fornece serviços de rede diretamente aos aplicativos do usuário final. **Interage com software de aplicação para implementar funções de comunicação.**
Exemplos: HTTP (HyperText Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), DNS (Domain Name System).

Ferramentas de análise

- Como detetives digitais, precisamos de ferramentas para "espionar"os pacotes e entender o que está acontecendo na rede;
- Vamos explorar algumas **ferramentas de análise de pacotes** populares, como Wireshark. Essas ferramentas nos permitem ver o tráfego de dados em tempo real;
- Com essas ferramentas, podemos examinar pacotes individuais, entender seu conteúdo e identificar possíveis problemas na rede.

Rastreando a comunicação

- Às vezes, precisamos rastrear a comunicação entre dispositivos para entender como eles se comunicam;
- Imagine isso como seguir um caminho de migalhas de pão no famoso conto de João e Maria. Cada migalha nos leva a um novo pedaço da história;
- Da mesma forma, rastreamos os pacotes para entender como a informação flui de um dispositivo para outro;
- Isso nos ajuda a diagnosticar problemas, otimizar o tráfego e melhorar o desempenho da rede.

Compartilhamento de Recursos na rede?

Em uma rede de computadores seja ela local ou global, temos a possibilidade de compartilhar recursos entre os hosts que estão conectados na rede, mesmo que essa rede não tenha acesso a internet, temos a possibilidade de compartilhar impressoras, arquivos, pastas, etc.

Se a rede local estiver conectada com a internet, as possibilidades de compartilhamento nas redes de computadores aumentam, pois podemos trocar informações com qualquer host que esteja localizado no globo e conectado com a internet.

Compartilhar Internet e serviço entre os hosts, modificou a maneira do mundo em se comunicar, vai

de conversa on-line para videoconferência (envio de vídeo em tempo real), a internet nos possibilita resolver as nossas pendências do dia a dia, fazendo transações bancárias, compra e vendas de produtos ou serviços, utilizar as redes sociais para se conectar com as pessoas diferentes.

Tudo isso é possível, pois os protocolos permitem diferentes serviços nas redes de computadores, o importante é estudar e compreender como funciona os principais protocolos na rede.

O NAT (Network Address Translation): é um recurso utilizado em **roteadores e firewalls para traduzir endereços IP entre diferentes redes**. Sua função principal é **permitir que múltiplos dispositivos em uma rede privada compartilhem um único endereço IP público para acessar a Internet**. Isso é especialmente útil em redes domésticas ou empresariais, onde há mais dispositivos do que endereços IP públicos disponíveis.

O **NAT mantém uma tabela de tradução** que mapeia os endereços IP privados dos dispositivos internos para os endereços IP públicos do **roteador/firewall**. Isso permite que as respostas dos servidores na Internet sejam redirecionadas corretamente de volta para o dispositivo interno correto.

O protocolo **DHCP (Dynamic Host Configuration Protocol)** é um protocolo de rede utilizado para atribuir automaticamente endereços IP e outras configurações de rede a dispositivos em uma rede local.

Quando um dispositivo é conectado à rede local, ele procura por **um servidor DHCP para obter um endereço IP**. Isso é feito por meio de um processo de descoberta, no qual o dispositivo envia uma solicitação **DHCP Broadcast** (um pacote especial enviado a todos os dispositivos na rede local) para encontrar um servidor DHCP disponível.

Um **firewall** é um **dispositivo de segurança de rede ou software que monitora e controla o tráfego de rede com base em um conjunto de regras de segurança predefinidas**. Ele atua como uma barreira entre uma rede interna protegida e redes externas, como a Internet, filtrando o tráfego com base em políticas de segurança estabelecidas.

O **protocolo TLS/SSL** é fundamental para a segurança da comunicação em redes. Ele oferece criptografia para proteger os dados transmitidos, autenticação para garantir a identidade dos servidores e, opcionalmente, dos clientes, e verifica a integridade dos dados para garantir que não tenham sido alterados durante a transmissão. Isso protege contra espionagem, manipulação e ataques de intermediários maliciosos, garantindo uma comunicação segura e confiável.

O TLS/SSL criptografa os dados usando algoritmos de criptografia fortes, garantindo que apenas o remetente e o destinatário legítimos possam acessar e entender as informações transmitidas.
O TLS/SSL usa hashes criptográficos para verificar a integridade dos dados. Isso significa que, se os dados forem alterados durante a transmissão, os hashes não corresponderão mais, alertando os usuários sobre a adulteração dos dados.

Os protocolos de roteamento, como **OSPF (Open Shortest Path First) e BGP (Border Gateway**

Protocol), desempenham um papel fundamental no encaminhamento e direcionamento eficiente do tráfego de dados em redes. Aqui está como eles influenciam o tráfego de dados:

OSPF (Open Shortest Path First):

- **Roteamento Interno:**
- O OSPF é um protocolo de roteamento interno usado em redes locais, como LANs (Local Area Networks) e intranets corporativas. Ele é projetado para determinar o melhor caminho dentro de uma única organização ou domínio de roteamento.

- **Influência no Tráfego:**
- O OSPF avalia a topologia da rede e calcula o caminho mais curto (menor custo) entre os dispositivos usando o algoritmo de Dijkstra. Ele compartilha informações de roteamento entre os roteadores dentro do mesmo domínio OSPF para garantir que todos os dispositivos tenham uma visão consistente da rede. Isso influencia diretamente o tráfego de dados, direcionando-o pelos caminhos mais eficientes dentro da rede local.

BGP (Border Gateway Protocol):

- **Roteamento Externo:**
- O BGP é um protocolo de roteamento externo usado para trocar informações de roteamento entre sistemas autônomos (AS - Autonomous Systems). Ele é usado principalmente na Internet, onde diferentes ASs estão interconectados para fornecer conectividade global.

- **Influência no Tráfego:**
- O BGP permite que os roteadores troquem informações de roteamento sobre redes externas e determinem os melhores caminhos para alcançar destinos fora de sua rede local. Ele influencia o tráfego de dados ao tomar decisões de roteamento com base em métricas como caminho mais curto, largura de banda, políticas de roteamento e outras considerações específicas do AS.

Diferença entre Roteamento Interno e Externo:

- **Roteamento Interno:**
- Refere-se ao processo de troca de informações de roteamento dentro de uma única rede ou domínio de roteamento. É usado para determinar o melhor caminho entre dispositivos dentro da mesma organização ou rede local. Exemplos incluem OSPF, EIGRP (Enhanced Interior Gateway Routing Protocol), RIP (Routing Information Protocol) interno, entre outros.

- **Roteamento Externo:**
- Refere-se ao processo de troca de informações de roteamento entre diferentes sistemas autônomos (ASs) na Internet ou em outras redes públicas. É usado para determinar os melhores caminhos para alcançar destinos fora da rede local. Exemplos incluem BGP e EGP (Exterior Gateway Protocol).

Conclusão:
Os protocolos de roteamento, como OSPF e BGP, desempenham papéis distintos no direcionamento do tráfego de dados em redes**. Enquanto o OSPF influencia o tráfego dentro de uma rede local, o BGP determina os melhores caminhos para alcançar destinos fora da rede local, como na Internet.** A diferença fundamental entre roteamento interno e externo reside na escala e no escopo das redes envolvidas.

ATIVIDADES:

1. O que são protocolos de rede e por que são essenciais para a comunicação entre dispositivos em uma rede de computadores?

2. Explique o que é um modelo de referência em camadas, como o modelo OSI, e como ele auxilia na compreensão dos protocolos de rede.

3. Descreva o funcionamento básico do Protocolo de Controle de Transmissão (TCP) e do Protocolo de Internet (IP). Como esses protocolos trabalham juntos para fornecer comunicação confiável?

4. O que é o DNS (Sistema de Nomes de Domínio) e como ele funciona para traduzir nomes de domínio em endereços IP?

5. Explique a diferença entre os protocolos UDP (User Datagram Protocol) e TCP em termos de confiabilidade de transmissão de dados. Em que situações cada um é mais adequado?

6. Qual é a função do protocolo ARP (Address Resolution Protocol) em uma rede? Como ele permite que dispositivos encontrem o endereço MAC correspondente a um endereço IP?

7. O que é NAT (Network Address Translation) e qual é o seu papel na conservação de endereços IP em redes privadas?

8. Descreva como o protocolo DHCP (Dynamic Host Configuration Protocol) funciona para atribuir automaticamente endereços IP e outras configurações de rede a dispositivos em uma rede local.

9. Quais são os benefícios da implementação do protocolo de segurança TLS/SSL em uma conexão de rede? Como ele ajuda a proteger a confidencialidade e a integridade dos dados transmitidos?

10. Como os protocolos de roteamento, como OSPF (Open Shortest Path First) e BGP (Border Gateway Protocol), influenciam o tráfego de dados em uma rede? Qual é a diferença entre roteamento interno e roteamento externo?

11. O que é um Firewall e como ele utiliza protocolos para filtrar e controlar o tráfego de rede?

RESPOSTAS:

1. Os protocolos de rede são conjuntos de regras e convenções que regulam a comunicação entre dispositivos em uma rede de computadores. Eles são essenciais para permitir que dispositivos diferentes se comuniquem de forma eficiente, estabelecendo padrões para formatos de dados, endereçamento, transmissão e recebimento de informações.

2. Um modelo de referência em camadas, como o modelo OSI (Open Systems Interconnection), divide o processo de comunicação em redes em várias camadas funcionais. Cada camada tem uma responsabilidade específica e se comunica com as camadas adjacentes por meio de interfaces padronizadas. Isso ajuda na compreensão e no projeto de redes, permitindo a separação de preocupações e a interoperabilidade entre diferentes sistemas.

3. O Protocolo de Controle de Transmissão (TCP) é responsável por garantir a entrega confiável de dados em uma rede, estabelecendo e mantendo uma conexão entre dispositivos e controlando o fluxo de dados. O Protocolo de Internet (IP) é responsável pelo endereçamento e roteamento dos

pacotes de dados na rede. Ambos os protocolos trabalham juntos: o IP roteia os pacotes entre dispositivos e o TCP gerencia a comunicação entre aplicativos, garantindo que os dados sejam entregues de forma confiável e na ordem correta.

4. O DNS (Sistema de Nomes de Domínio) é responsável por traduzir nomes de domínio legíveis por humanos em endereços IP utilizados pelos computadores para localizar recursos na Internet. Funciona como uma espécie de "catálogo telefônico" da Internet, permitindo que os usuários acessem sites usando nomes de domínio em vez de endereços IP numéricos.

5. A principal diferença entre os protocolos UDP (User Datagram Protocol) e TCP (Transmission Control Protocol) está na confiabilidade da transmissão de dados. O TCP garante a entrega confiável dos dados, garantindo que todas as informações sejam recebidas e na ordem correta, enquanto o UDP não garante a entrega confiável, sendo mais rápido e adequado para aplicações onde a perda de alguns dados é tolerável, como streaming de vídeo e jogos online.

6. O protocolo ARP (Address Resolution Protocol) é utilizado em redes locais para mapear endereços IP em endereços MAC. Ele permite que dispositivos encontrem o endereço MAC correspondente a um endereço IP, facilitando a comunicação dentro da rede local.

7. O NAT (Network Address Translation) é um recurso utilizado em roteadores e firewalls para traduzir endereços IP entre diferentes redes. Seu papel principal é permitir que múltiplos dispositivos em uma rede privada compartilhem um único endereço IP público para acessar a Internet, conservando assim endereços IP em redes privadas.

8. O protocolo DHCP (Dynamic Host Configuration Protocol) funciona para atribuir automaticamente endereços IP e outras configurações de rede a dispositivos em uma rede local. Quando um dispositivo se conecta à rede, ele envia uma solicitação DHCP para encontrar um servidor DHCP disponível, que então fornece ao dispositivo um endereço IP e outras configurações de rede necessárias.

9. Os benefícios da implementação do protocolo de segurança TLS/SSL em uma conexão de rede incluem a proteção da confidencialidade e integridade dos dados transmitidos. Ele oferece criptografia para proteger os dados contra espionagem, autenticação para garantir a identidade dos remetentes e destinatários, e verifica a integridade dos dados para garantir que não tenham sido alterados durante a transmissão.

10. Os protocolos de roteamento, como OSPF (Open Shortest Path First) e BGP (Border Gateway Protocol), influenciam o tráfego de dados em uma rede ao determinar os melhores caminhos para enviar pacotes de dados entre dispositivos. O roteamento interno ocorre dentro de uma única rede, enquanto o roteamento externo ocorre entre diferentes redes ou sistemas autônomos.

11. Um firewall é um dispositivo de segurança de rede ou software que monitora e controla o tráfego de rede com base em um conjunto de regras de segurança predefinidas. Ele utiliza protocolos para filtrar e controlar o tráfego de rede, bloqueando ou permitindo o acesso a determinados recursos com base em políticas de segurança estabelecidas.