



# **APOSTILA OFICIAL - REDES DE COMPUTADORES**

**Básico ao Intermediário**

**Capacitação Técnica Interna**



# **OBJETIVO DO CURSO**

Esta apostila foi desenvolvida para capacitar profissionais iniciantes e em atuação prática na área de redes de computadores, unindo fundamentos teóricos e aplicação real em ambientes residenciais, corporativos e de provedor de internet (ISP).

O material tem como finalidade:

- Apoiar o aluno durante as aulas e treinamentos
- Servir como material de consulta no dia a dia técnico
- Padronizar o conhecimento e as práticas técnicas adotadas pela Rede.com

# **SUMÁRIO**

- **Módulo 1 – Fundamentos de Redes**
- **Módulo 2 – Topologias de Rede**
- **Módulo 3 – Equipamentos e Rede Interna**
- **Módulo 4 – RouterBoard / MikroTik**
- **Módulo 5 – Protocolos de Rede**
- **Módulo 6 – Montagem e Diagnóstico de Rede**
- **Módulo 7 – Infraestrutura de Redes FTTH**

# **MÓDULO 1 – FUNDAMENTOS DE REDES**

## **Apresentação do Módulo**

Este módulo estabelece a base conceitual das redes de computadores. O objetivo é garantir que todos compreendam o que é uma rede, porque ela existe e como ela funciona, tanto do ponto de vista técnico quanto prático. É um módulo essencial para quem está iniciando e também para quem deseja consolidar conhecimentos.

### **1. O que é uma rede de computadores**

Uma rede de computadores é a interligação de dois ou mais dispositivos para trocar dados, compartilhar recursos e permitir comunicação eficiente.

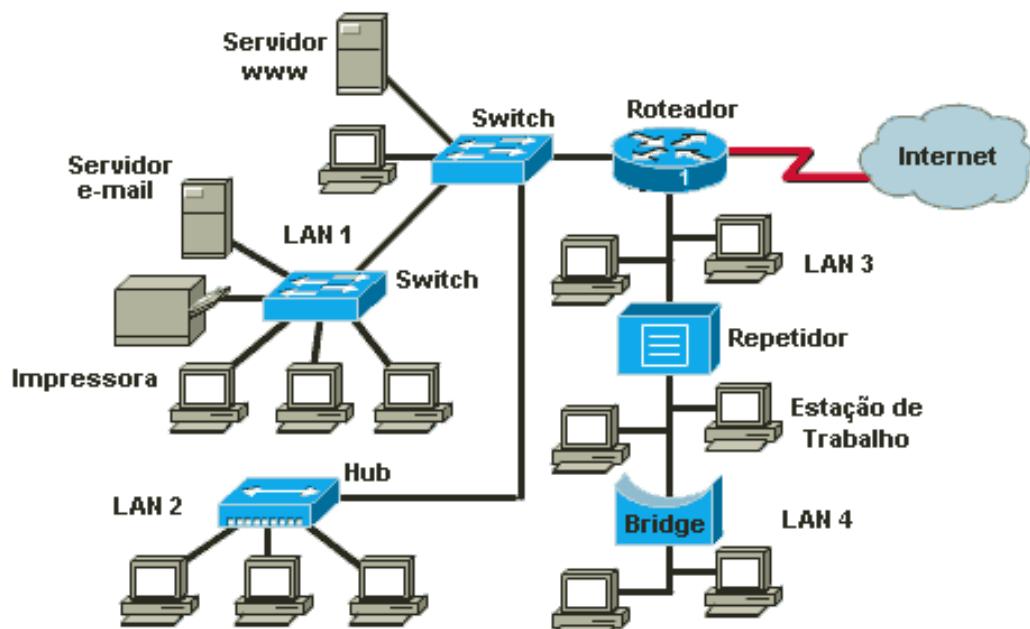
Esses dispositivos podem ser computadores, celulares, Smart TVs, servidores, impressoras e equipamentos de rede.

Exemplo prático:

Em uma residência, quando celular, TV e notebook acessam o Wi-Fi, todos fazem parte da mesma rede LAN. Em uma empresa, diversos computadores compartilham servidores e sistemas internos por meio da rede.

Camada estratégica:

Uma rede bem projetada reduz falhas, melhora desempenho, aumenta a segurança e diminui custos operacionais.



## 2. Importância das redes no dia a dia

As redes são indispensáveis para:

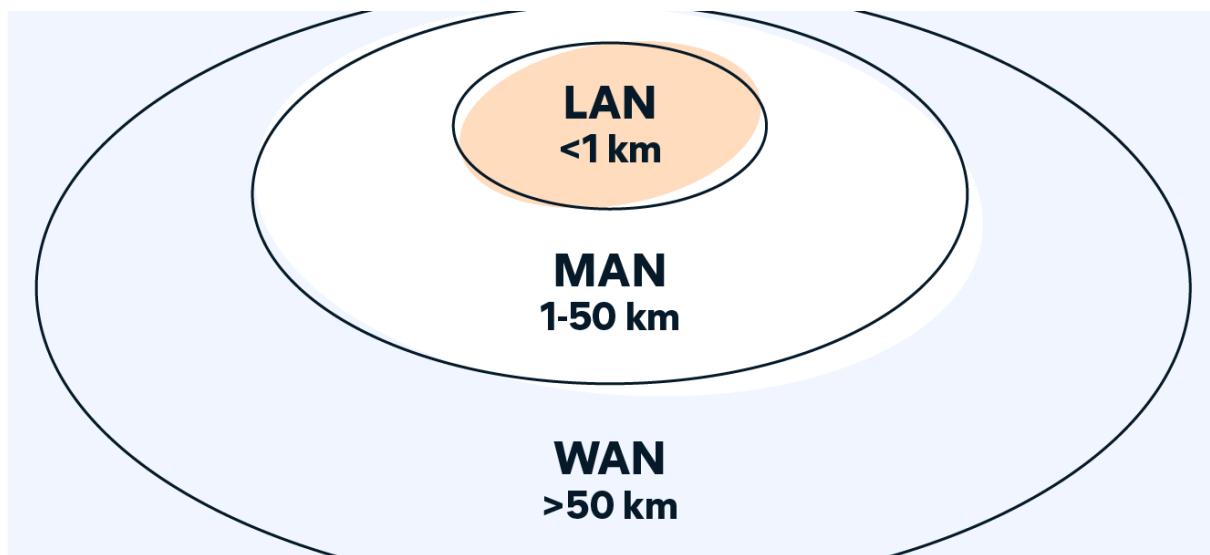
- Comunicação entre pessoas e empresas
- Funcionamento da internet e sistemas corporativos
- Serviços bancários, streaming, telefonia IP e nuvem
- Operações de provedores de internet (ISPs)

## 3. Tipos de redes

- LAN (Local Area Network): rede local, limitada a um ambiente físico pequeno.
- MAN (Metropolitan Area Network): cobre uma cidade ou região.
- WAN (Wide Area Network): grandes distâncias. Exemplo: Internet.
- WLAN: rede local sem fio (Wi-Fi).

*Resumo rápido:*

*LAN = casa/empresa | MAN = cidade | WAN = mundo*



## 4. Componentes básicos de uma rede

- Hosts: dispositivos finais (PCs, celulares, TVs)
- Switches: interligam dispositivos na LAN
- Roteadores: conectam redes diferentes

- Cabos de rede: meio físico de transmissão
- Interfaces de rede: placas de comunicação
- SFP / GBIC: módulos ópticos para fibra

### **Checklist – componentes essenciais de uma LAN:**

- Roteador
- Switch
- Cabos ou Wi-Fi
- Dispositivos finais

## **5. Conceitos fundamentais**

- IP: endereço lógico do dispositivo
- MAC Address: endereço físico da placa de rede
- Gateway: saída da rede local
- DNS: converte nomes em IPs

*Exemplo prático:*

*Quando digitamos um site, o DNS traduz o nome para um IP, e o gateway encaminha a solicitação para a internet.*

## **6. IPv4 e IPv6**

Os protocolos **IPv4** e **IPv6** são responsáveis pelo **endereçamento lógico dos dispositivos em uma rede**, permitindo que computadores, roteadores, servidores e outros equipamentos se identifiquem e se comuniquem corretamente.

O **IPv4** é a versão mais antiga e ainda amplamente utilizada do protocolo IP. Ele utiliza endereços de **32 bits**, representados em formato decimal separado por pontos, como no exemplo **192.168.1.10**. Esse padrão é comum em redes residenciais, empresariais e em grande parte da Internet atual. Devido à limitação de endereços disponíveis, o IPv4 normalmente opera em conjunto com tecnologias como **NAT** e **CGNAT**, especialmente em ambientes de provedores de internet.

O **IPv6**, por sua vez, foi desenvolvido para substituir o IPv4 e resolver a escassez de endereços. Ele utiliza endereços de **128 bits**, representados em formato hexadecimal e separados por dois pontos, como no exemplo **2001:db8:85a3::8a2e:370:7334**. O IPv6 permite uma quantidade praticamente

ilimitada de endereços e elimina a necessidade de NAT, possibilitando comunicação direta entre dispositivos.

Em termos de diagnóstico de redes, tanto o IPv4 quanto o IPv6 são utilizados para testes de conectividade, verificação de rotas e validação de configurações. O IPv6 ganha cada vez mais relevância em redes modernas, principalmente em ambientes FTTH e de provedores de internet.

IPv4	IPv6
Implantado em 1981	Implantado em 1998
Endereço IP de 32-bit	Endereço IP de 128-bit
<b>4,3 bilhões de endereços</b> Endereços precisam ser reutilizados e mascarados	<b>340 undecilhões de endereços</b> Cada dispositivo tem um endereço exclusivo
Notação numérica decimal com ponto <b>192.168.5.18</b>	Notação hexadecimal alfanumérica <b>50b2:6400:0000:0000:6c3a:b17d:0000:10a9</b> (Simplificado - 50b2:6400::6c3a:b17d:0:10a9)
DHCP ou configuração manual	Compatível com configuração automática

## QUADRO RESUMO - IPv4 x IPv6

O **IPv4** utiliza endereços numéricos em formato decimal, é mais simples de identificar visualmente e ainda é amplamente adotado devido à compatibilidade com sistemas e equipamentos legados. No entanto, apresenta limitação de endereços, o que exige o uso de técnicas como NAT e CGNAT para viabilizar o crescimento das redes.

O **IPv6** utiliza endereços em formato hexadecimal, possui uma capacidade extremamente maior de endereços e foi projetado para atender à expansão da Internet. Ele melhora a escalabilidade das redes, reduz a complexidade do endereçamento e prepara a infraestrutura para tecnologias atuais e futuras, como redes FTTH, IoT e serviços em larga escala.

Do ponto de vista operacional, o IPv4 continua essencial no dia a dia, enquanto o IPv6 representa a evolução natural das redes e deve ser progressivamente incorporado às infraestruturas de provedores.

## 7. Comunicação em redes

Os dados são divididos em pacotes, encapsulados e enviados por protocolos. Cada etapa garante integridade, ordem e entrega correta.



## 8. Internet x Intranet

- Internet: rede pública global
- Intranet: rede privada corporativa

### Quadro Resumo do Módulo 1

- Redes conectam dispositivos
- IP identifica
- Gateway direciona
- DNS traduz

### Atividade prática

*Simular uma rede simples.*

# **MÓDULO 2 – TOPOLOGIAS DE REDE**

## **Apresentação do Módulo**

Este módulo aprofunda o entendimento sobre como as redes são estruturadas, mostrando como a escolha da topologia impacta diretamente desempenho, escalabilidade, custo e facilidade de manutenção.

### **1. Topologia física x topologia lógica**

- Topologia física: representa como cabos, racks, switches e roteadores estão fisicamente conectados.
- Topologia lógica: representa o caminho que os dados percorrem, independentemente da disposição física.

*Exemplo prático:*

*Uma rede pode ser fisicamente em estrela, mas logicamente segmentada por VLANs.*

### **2. Tipos clássicos de topologia**

- Barramento: todos compartilham o mesmo meio. Baixo custo, difícil diagnóstico.
- Anel: dados circulam em um único sentido. Pouco utilizada atualmente.
- Estrela: todos os dispositivos ligados a um ponto central. Fácil manutenção.
- Malha: múltiplos caminhos redundantes. Alta disponibilidade.
- Híbrida: combinação conforme necessidade.

*Camada estratégica:*

*Empresas e ISPs priorizam estrela e malha para reduzir pontos únicos de falha.*

### **3. Topologias em redes sem fio**

- Infraestrutura: AP central controlando acessos.
- Ad-hoc: comunicação direta entre dispositivos.
- Mesh: APs interligados, cobertura contínua.

#### 4. Critérios de escolha da topologia

- Custo de implantação
- Facilidade de expansão
- Nível de redundância
- Tipo de tráfego

### Quadro resumo do Módulo 2

*Topologia define desempenho, custo e confiabilidade da rede.*

#### 1. Topologia física x lógica

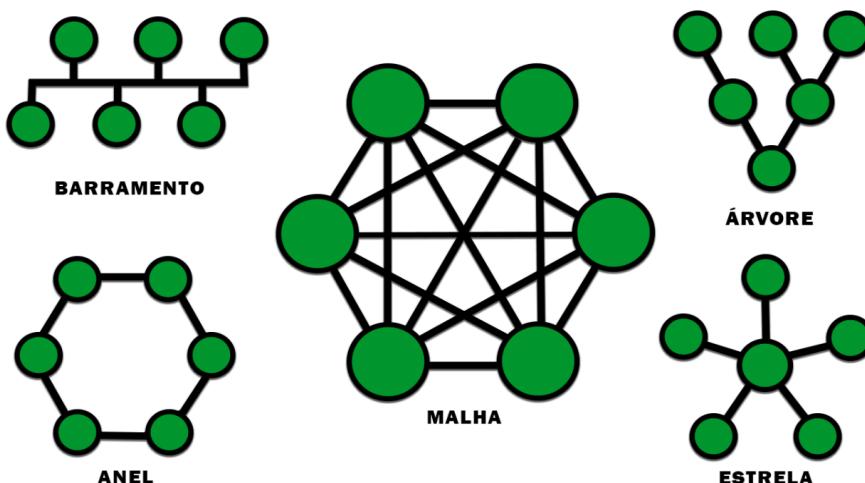
- Física: como os cabos estão conectados
- Lógica: como os dados circulam

#### 2. Tipos de topologia

- Barramento: simples, pouco usada
- Anel: controle sequencial
- Estrela: padrão atual
- Malha: alta redundância
- Híbrida: combinação

*Camada estratégica:*

*Redes corporativas utilizam estrela ou malha para reduzir falhas.*



### **3. Redes sem fio**

- Infraestrutura
- Ad-hoc
- Mesh

#### **Quadro Resumo do Módulo 2**

*Estrela = fácil manutenção | Malha = alta disponibilidade*

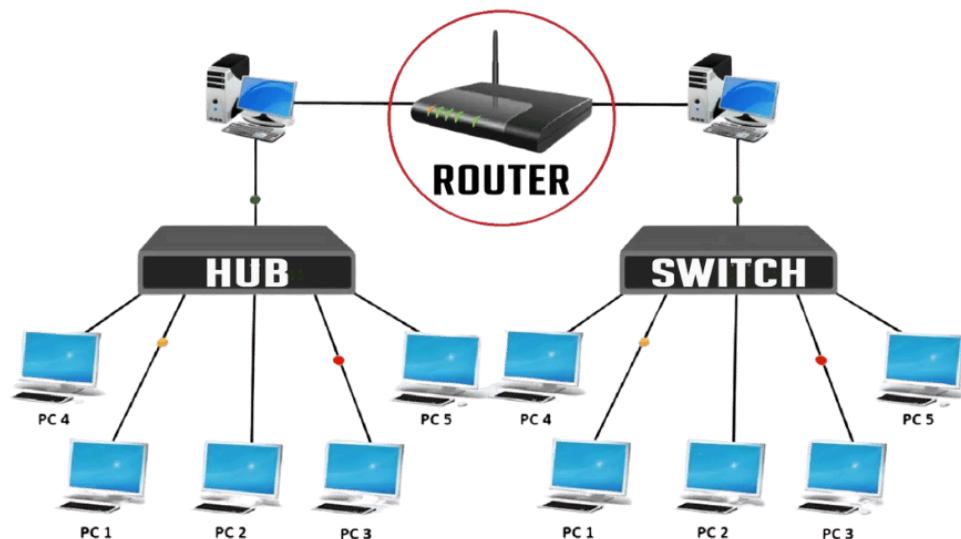
# **MÓDULO 3 – EQUIPAMENTOS E REDE INTERNA**

## **Apresentação do Módulo**

Este módulo detalha os principais equipamentos de rede, suas funções e como eles interagem dentro de uma LAN corporativa ou residencial.

### **1. Hub, Switch e Roteador**

- Hub: replica pacotes para todas as portas. Não possui inteligência.
- Switch: opera na camada 2, utiliza tabela MAC para direcionar tráfego.
- Roteador: opera na camada 3, conecta redes diferentes e aplica políticas.



### **2. Endereçamento IP na LAN**

- IP estático x IP dinâmico
- Máscara de rede
- Gateway padrão

*Exemplo prático:*

*Servidores utilizam IP fixo; estações usam DHCP.*

### **3. Segmentação de rede**

A segmentação melhora:

- Segurança
- Performance
- Organização

*Pode ser feita por sub-redes ou VLANs.*

### **4. Serviços de rede**

- DHCP: evita conflitos de IP
- NAT: permite múltiplos dispositivos acessarem a internet
- DNS: facilita navegação

### **5. Segurança em rede interna**

- Firewall
- Controle de acesso
- Separação de redes críticas

## **1. Hub, Switch e Roteador**

- Hub: obsoleto
- Switch: inteligência de encaminhamento
- Roteador: conexão entre redes

## **2. Segmentação de rede**

Uso de sub-redes e VLANs para:

- Segurança
- Organização
- Performance

### **3. Serviços de rede**

- DHCP
- NAT
- DNS

#### **Checklist – rede bem organizada**

- VLANs
- DHCP ativo
- Firewall configurado

# **MÓDULO 4 – ROUTERBOARD / MIKROTIK**

## **Apresentação do Módulo**

Este módulo aprofunda o uso de RouterBoards MikroTik, amplamente utilizadas em ambientes corporativos e provedores de internet.

### **1. RouterBoard e RouterOS**

- Hardware dedicado
- Sistema RouterOS
- Licenças e níveis

### **2. Métodos de acesso**

- WinBox
- WebFig
- Terminal (CLI)

### **3. Configuração essencial**

Nesta etapa realizamos a configuração básica do RouterOS, responsável por permitir o funcionamento correto da rede.

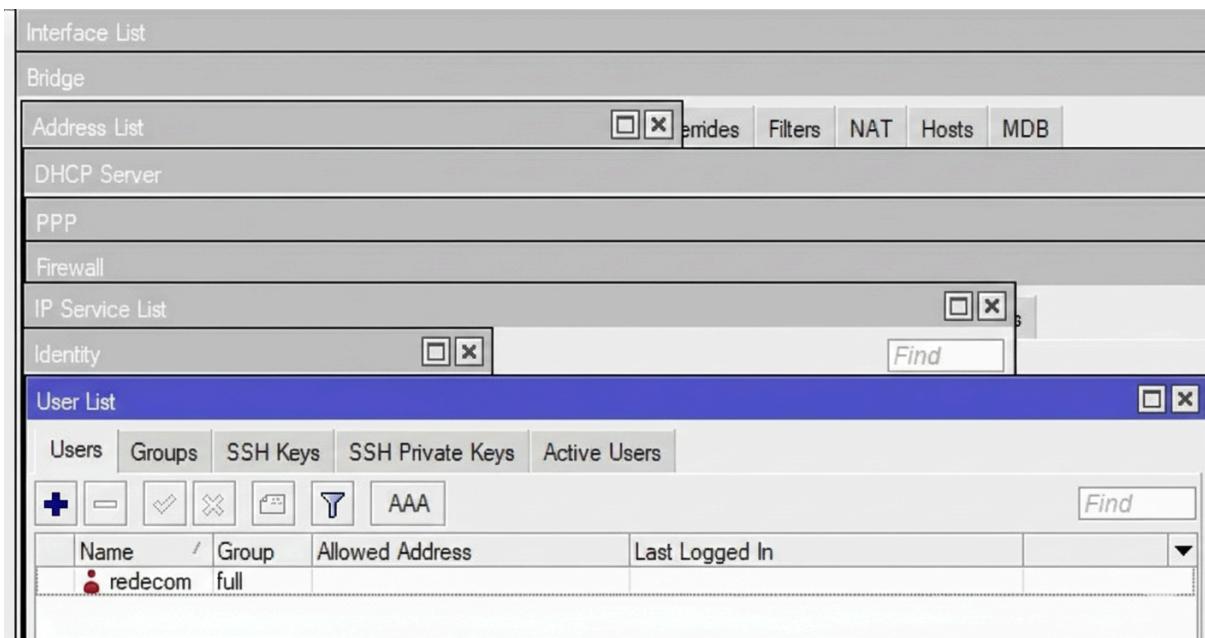
Itens configurados neste menu:

- Interface List
- Bridge
- Address List
- DHCP Server
- PPP
- Firewall
- IP Service List
- Identity
- User List

*Explicação didática:*

*Esse menu concentram praticamente toda a configuração inicial de uma RB*

*MikroTik. Um erro nessa etapa pode comprometer acesso, segurança ou conectividade.*



*Camada estratégica:*

*Padronizar essa configuração em todos os roteadores reduz falhas, facilita o suporte técnico e melhora a escalabilidade da rede.*

#### 4. PPP e autenticação

- PPPoE
- Hotspot

#### 5. Monitoramento e manutenção

- Ping
- Torch
- Traffic Flow
- Logs

# **FERRAMENTAS DE DIAGNÓSTICO DE REDE**

## **PING**

O Ping é uma das principais ferramentas de diagnóstico de rede e costuma ser o primeiro teste realizado por técnicos e profissionais de suporte ao identificar problemas de conectividade.

O Ping é uma ferramenta que verifica se existe comunicação entre dois dispositivos em uma rede.

Ele envia pequenos pacotes de dados utilizando o protocolo ICMP e aguarda a resposta do destino.

Através do Ping, é possível saber se um equipamento está acessível e se a comunicação ocorre de forma estável.

### **O Ping é utilizado para:**

- Verificar conectividade com a Internet
- Testar comunicação entre equipamentos da rede
- Identificar perda de pacotes
- Analisar o tempo de resposta da rede (latência)
- Auxiliar no diagnóstico inicial de falhas

### **Como o Ping funciona**

1. Um pacote ICMP é enviado para o destino
2. O destino responde ao pacote
3. O tempo entre envio e resposta é medido
4. Caso não haja resposta, ocorre falha de comunicação

## **Como realizar um Ping**

No Windows

1. Abra o Prompt de Comando (CMD)
2. Digite:

ping 8.8.8.8

ou

ping www.google.com

3. Pressione Enter

## **No Linux ou MikroTik (Terminal)**

ping 8.8.8.8

## **Como interpretar o resultado do Ping**

- Resposta com tempo baixo (ms): comunicação normal
- Tempo alto: possível lentidão ou rota longa
- Perda de pacotes: instabilidade na rede
- Request timed out: destino inacessível

## **Exemplo prático**

Ao receber uma reclamação de cliente sem acesso à internet:

1. Realize Ping no roteador do cliente
2. Realize Ping em um IP externo (ex: 8.8.8.8)
3. Se responde localmente, mas não externamente, o problema pode estar no link ou no roteamento

## **TORCH (MIKROTIK)**

O Torch é uma ferramenta avançada de monitoramento em tempo real presente nos equipamentos MikroTik, muito utilizada em ambientes de provedor de internet.

O Torch permite visualizar o tráfego de dados que passa por uma interface de rede, exibindo informações como IP de origem, IP de destino, protocolo e volume de dados transmitidos.

Ele mostra quem está consumindo banda e como esse consumo acontece.

### **O Torch é utilizado para:**

- Identificar consumo excessivo de banda
- Detectar lentidão causada por uso intenso
- Monitorar tráfego por IP, porta ou protocolo
- Auxiliar no diagnóstico de problemas de desempenho

### **Como utilizar o Torch no MikroTik**

Acesso pelo WinBox

1. Acesse o MikroTik pelo WinBox
2. Vá em Tools → Torch
3. Selecione a Interface desejada (WAN ou LAN)
4. (Opcional) Configure filtros:
  - IP Address
  - Port
  - Protocol
5. Clique em Start

### **Informações exibidas pelo Torch**

- Src. Address: endereço IP de origem

- Dst. Address: endereço IP de destino
- Tx: dados enviados
- Rx: dados recebidos
- Protocol: protocolo utilizado

## **Exemplo prático**

Se um cliente relata internet lenta:

1. Execute o Torch na interface correspondente
2. Observe se algum IP apresenta alto consumo
3. Identifique aplicações ou dispositivos responsáveis
4. Com base nisso, aplique orientação ou controle de banda

### *Atenções importantes*

- *Utilize filtros para evitar sobrecarga*
- *Evite uso prolongado em equipamentos muito carregados*
- *O Torch deve ser usado como ferramenta de análise pontual*

### *Camada estratégica:*

*Padronizar configurações reduz falhas e facilita suporte.*

## **TRACEROUTE**

O Traceroute é uma ferramenta de diagnóstico utilizada para identificar o caminho que os dados percorrem entre a origem e o destino dentro de uma rede ou pela Internet.

Ela é essencial para localizar **onde ocorrem atrasos ou falhas de comunicação.**

O **Traceroute** mostra todos os “saltos” (hops) que um pacote de dados realiza até chegar ao destino final.

Cada salto representa um equipamento intermediário, como roteadores e gateways.

Com essa ferramenta, é possível visualizar **em que ponto da rede o tráfego está passando ou parando**.

## Para que serve o Traceroute

- Identificar onde ocorre lentidão na comunicação
- Localizar falhas de rota
- Verificar caminhos até servidores externos
- Apoiar diagnósticos de perda de conectividade
- Entender a rota entre o cliente e a Internet

## Como o Traceroute funciona

1. O dispositivo envia pacotes com limite de tempo (TTL)
2. A cada salto, o TTL é reduzido
3. Cada roteador responde informando sua presença
4. O processo continua até alcançar o destino final

## Como realizar um Traceroute

### No Windows

1. Abra o **Prompt de Comando (CMD)**
2. Digite:

tracert 8.8.8.8

ou

tracert www.google.com

3. Pressione **Enter**

## No Linux ou MikroTik (Terminal)

traceroute 8.8.8.8

## Como interpretar o resultado do Traceroute

- **Cada linha:** representa um salto da rota
- **Tempo baixo:** comunicação normal
- **Tempo alto em um salto específico:** possível gargalo
- Asteriscos ( \* ): ausência de resposta naquele ponto
- **Falha antes do destino:** possível problema de rota

## Exemplo prático

Se um cliente relata lentidão apenas em determinados sites:

1. Execute o Traceroute até o site informado
2. Identifique em qual salto ocorre aumento de latência
3. Verifique se o problema está na rede interna, no provedor ou fora da rede

## Atenções importantes

- Nem todos os equipamentos respondem ao Traceroute
- A ausência de resposta não significa necessariamente falha
- Sempre analise o conjunto dos saltos, não apenas um ponto isolado

# **MÓDULO 5 – PROTOCOLOS DE REDE**

## **Apresentação do Módulo**

Este módulo aprofunda o entendimento dos protocolos responsáveis pela comunicação, confiabilidade e segurança das redes.

### **1. Modelo OSI e TCP/IP**

O **Modelo OSI (Open Systems Interconnection)** é um modelo conceitual dividido em **7 camadas**, criado para **padronizar a comunicação em redes de computadores**.

Ele não é um protocolo, mas uma **referência técnica** usada para projeto, estudo e principalmente diagnóstico de problemas de rede.

### **Visão geral**

- Ajuda a entender **onde ocorre um problema**
- Facilita a comunicação entre técnicos
- Permite isolar falhas por camada

### **Camada 1 – Física**

#### **Função:**

Responsável pela **transmissão física dos dados**, em forma de sinais elétricos, ópticos ou rádio.

#### **Exemplos:**

- Cabos de rede (UTP, fibra óptica)
- Conectores RJ45
- Sinal Wi-Fi
- LEDs de portas

#### **Importância no diagnóstico:**

*Problemas nessa camada indicam que não há comunicação nenhuma.*

#### **Falhas comuns:**

- Cabo rompido ou mal crimpado

- Porta queimada
- Equipamento desligado

## Camada 2 – Enlace (Data Link)

### Função:

Garante a comunicação **entre dispositivos da mesma rede local**, usando endereços MAC.

### Exemplos:

- Switches
- Bridge
- ARP
- VLAN

### Importância no diagnóstico:

*Quando há link físico, mas os dispositivos não se enxergam corretamente na rede local.*

### Falhas comuns:

- Conflito de MAC
- VLAN configurada incorretamente
- Loop de rede

## Camada 3 – Rede

### Função:

Responsável pelo **endereçamento lógico e roteamento** dos pacotes.

### Exemplos:

- IP (IPv4 / IPv6)
- Roteadores
- Gateway
- ICMP (ping)

### Importância no diagnóstico:

*Se o dispositivo se conecta à rede, mas não acessa outros destinos, geralmente o problema está aqui.*

### **Falhas comuns:**

- IP incorreto
- Gateway errado
- Rota inexistente

## **Camada 4 – Transporte**

### **Função:**

Controla a **entrega dos dados**, garantindo confiabilidade ou velocidade.

### **Protocolos principais:**

- **TCP** – confiável, com controle de erro
- **UDP** – rápido, sem controle de erro

### **Importância no diagnóstico:**

Quando a conexão existe, mas **aplicações falham ou ficam instáveis**.

### **Falhas comuns:**

- Porta bloqueada
- Serviço não escutando
- Perda excessiva de pacotes

## **Camada 5 – Sessão**

### **Função:**

Gerencia **sessões de comunicação** entre dispositivos.

### **Exemplos:**

- Sessões PPP
- Login remoto persistente

### **Importância no diagnóstico:**

Problemas de **queda de conexão após autenticação**.

## **Camada 6 – Apresentação**

### **Função:**

Responsável pela **formatação, criptografia e compressão dos dados**.

### **Exemplos:**

- SSL/TLS
- Criptografia
- Codificação de dados

### **Importância no diagnóstico:**

*Falhas de certificado ou erro de compatibilidade de dados.*

## **Camada 7 – Aplicação**

### **Função:**

Interface direta com o usuário e as aplicações.

### **Exemplos:**

- HTTP / HTTPS
- FTP
- DNS
- SMTP

### **Importância no diagnóstico:**

*Quando a rede funciona, mas o serviço não abre.*

### **Falhas comuns:**

- Serviço fora do ar
- DNS não respondendo
- Aplicação mal configurada

## **MODELO TCP/IP**

O Modelo TCP/IP é o modelo **real e prático**, usado na Internet e em redes de provedores (ISP).

Ele possui **4 camadas**, que agrupam o modelo OSI.

### **Camada 1 – Acesso à Rede**

**Equivale às camadas 1 e 2 do OSI**

**Função:**

- Comunicação física
- Endereçamento MAC
- Enlace local

**Diagnóstico típico:**

- Cabo
- Wi-Fi
- Porta de switch

### **Camada 2 – Internet**

**Equivale à camada 3 do OSI**

**Função:**

- Endereçamento IP
- Roteamento entre redes

**Protocolos:**

- IP
- ICMP

**Diagnóstico típico:**

- Ping não responde
- Gateway incorreto

## **Camada 3 – Transporte**

**Equivale à camada 4 do OSI**

**Função:**

- Controle de portas
- Confiabilidade ou velocidade

**Protocolos:**

- TCP
- UDP

**Diagnóstico típico:**

- Serviço conecta e cai
- Porta bloqueada no firewall

## **Camada 4 – Aplicação**

**Equivale às camadas 5, 6 e 7 do OSI**

**Função:**

- Serviços finais
- Comunicação com o usuário

**Protocolos:**

- HTTP / HTTPS
- DNS
- FTP
- SMTP

**Diagnóstico típico:**

- Internet funciona, mas site não abre
- DNS não resolve nomes

## **IMPORTÂNCIA PRÁTICA NO DIAGNÓSTICO (VISÃO ISP)**

A lógica correta de diagnóstico é sempre **de baixo para cima**:

1. Tem sinal físico?
2. Está na rede local?
3. Tem IP e gateway?
4. O transporte responde?
5. A aplicação funciona?

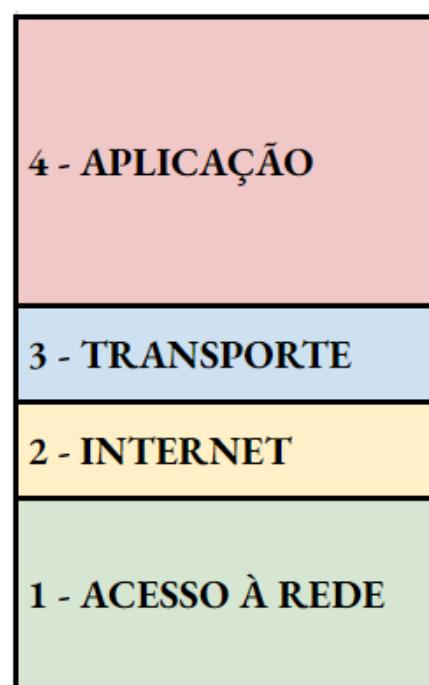
Essa abordagem:

- Reduz tempo de atendimento
- Evita trocas desnecessárias de equipamento
- Padroniza o suporte técnico

**Modelo OSI**



**Arquitetura TCP/IP**



### **Protocolos de aplicação**

HTTP, HTTPS, FTP, SFTP, DNS, DHCP

## Protocolos de transporte

- TCP: confiável
- UDP: rápido

## Protocolos de rede e roteamento

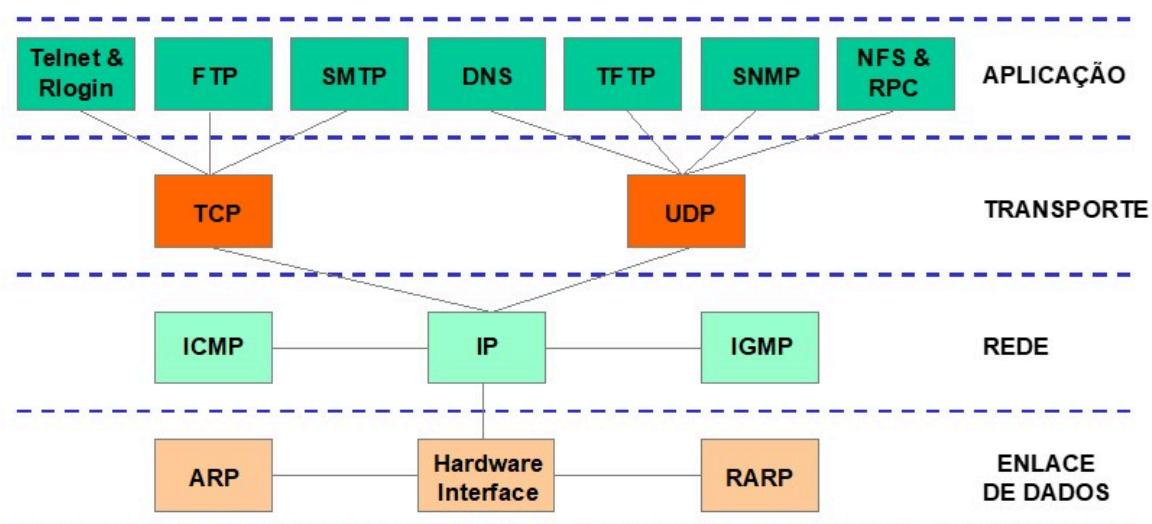
- IP
- ICMP
- ARP
- OSPF
- RIP

## Protocolos de segurança

- SSH
- TLS
- IPSec
- VPN

## Protocolos

- Aplicação: HTTP, DNS
- Transporte: TCP, UDP
- Rede: IP, ICMP
- Segurança: VPN, IPSec



# **MÓDULO 6 – MONTAGEM E DIAGNÓSTICO DE REDES**

## **Apresentação do Módulo**

Aplicação prática dos conhecimentos adquiridos ao longo do curso.

### **1. Planejamento de rede**

- Levantamento de necessidades
- Definição de topologia
- Endereçamento IP

### **2. Implementação**

- Instalação física
- Configuração lógica

### **3. Testes de conectividade**

- Ping
- Traceroute
- Testes de velocidade

### **4. Diagnóstico e solução de problemas**

- Falhas físicas
- Falhas lógicas
- Análise de logs

#### **Checklist diagnóstico:**

- IP válido
- Gateway correto
- DNS funcionando

# **MÓDULO 7 – INFRAESTRUTURA DE REDES**

## **FTTH**

### **Apresentação do Módulo**

Este módulo apresenta os fundamentos técnicos da infraestrutura de fibra óptica utilizada por provedores de internet.

#### **1. Conceito FTTH**

Fibra até a casa do cliente, alta velocidade e baixa latência.

#### **2. Tecnologia GPON**

- OLT
- ONT/ONU
- Downstream e Upstream

#### **3. Cabos de fibra óptica**

- Monomodo
- Multimodo
- Padrões de cores

#### **4. Splitters e cálculo de perda**

- Atenuação
- Orçamento óptico

#### **5. Projetos FTTH**

- Leitura de mapas
- CTO e CEO
- Padrões de instalação