REDES DE COMPUTADORES

UNIDADE CURRICULAR 5-6-7

ÍNDICE

EMENTA

- História das Redes,
- Componentes de Rede, Arquiteturas Ponto-a-Ponto e Cliente-Servidor, Dispositivos Finais e Intermediários, Meios de Transmissão, Representações e Símbolos de Rede, Topologias Lógica e Física, Abrangência e Escopos, Intranet/Extranet, Tecnologias de Transmissão, Redes Confiáveis, Tendências, Ameaças;
- Protocolos e Modelos de Referência
- Camada Física
- Camada de Link/Enlace de Dados
- Camada de Rede, Resolução de Endereços, Endereços IPv4 e IPv6, Pacotes ICMP.
- Camada de Transporte
- Camada de Aplicação.
- Segurança

LABORATÓRIO

- Diagramas de Rede
- Estrutura de Comandos em Switch e Roteadores, plataforma CISCO, Huawei e Mikrotik.
- Configuração de Switches.
- Configuração de Roteadores.
- 3 Kahoot de Revisão.
- Montagem de Cabos de Rede cat6.
- Montagem de Tomadas (keystone).
- Cálculo de Redes.
- Virtualização de Rede com EVE-NG.
- Configuração de Rede LAN com Cisco Packet Tracer.
- Análise NIST.
- Ferramentas de Segurança.

BIBLIOGRAFIA RECOMENADA

Network Computers 6ª ed (Andrew S. Tanenbaum);

Redes de Computadores e a Internet (James Kurose);

Redes, Guia Prático (Carlos Morimoto);

Este material foi elaborado com base no CISCO CCNA (ITN, SWRE, ENSA)

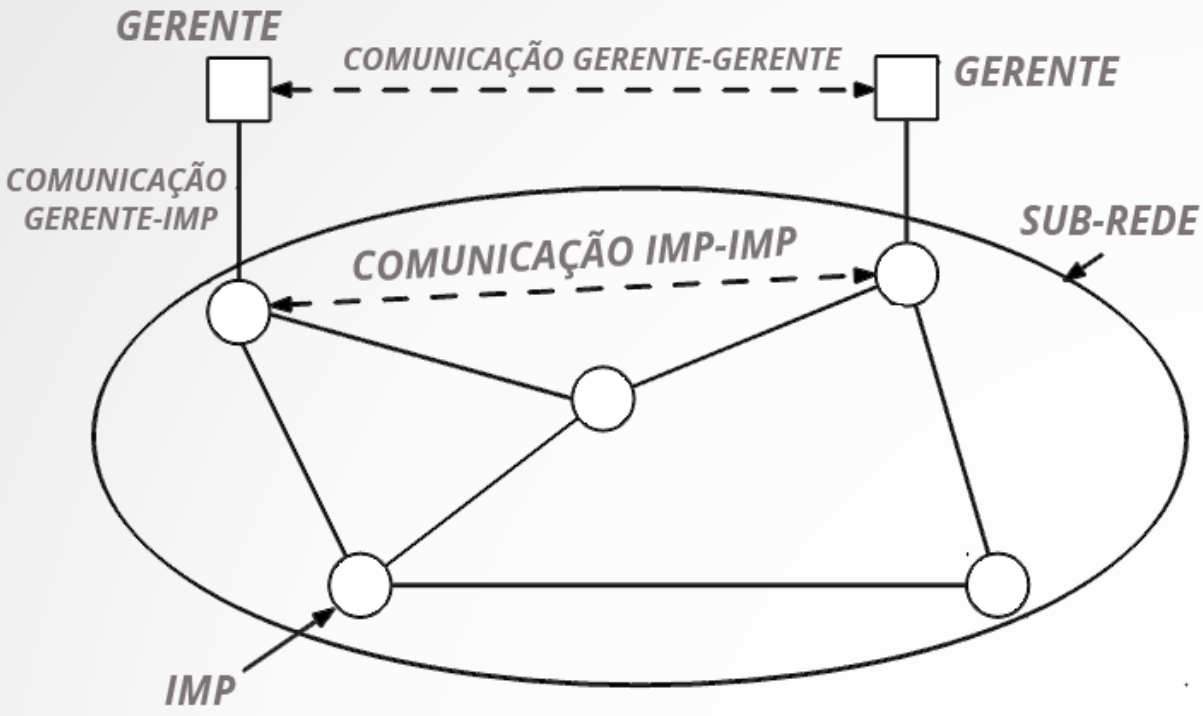
ARPANET

E SURGE UMA REDE...

Na década de 60, militares desejavam criar um meio de comunicação que fosse **robusto** e não tivesse **ponto central**, dificultando sua destruição. O objetivo era **facilitar a comunicação em tempos de guerra**.

Então a **ARPA** (*Advanced Research Projects Agency)* criou a ARPANET, logo após a União Soviética lançar o Sputnik (1957).

A ARPANET era constituída de uma sub-rede de minicomputadores chamados IMP, gerenciadas por outros computadores. Cada IMP era conectado a outros dois IMPs para garantir caminhos alternativos na transmissão.


GERENTE
COMUNICAÇÃO GERENTE-GERENTE
GERENTE
COMUNICAÇÃO GERENTE-IMP
SUB-REDE
COMUNICAÇÃO IMP-IMP
IMP

E FOI SE ESPALHANDO...

Em 1969 eram 4 IMPs, em 1970 eram 8, em 1971 aumentou para 15 e 1972 eram 34 IMPs. As sub-redes estavam espalhados nos principais polos americanos como o MIT, Havard, Utah, Illinois, UCSB e Stanford.

Em 1983, a ARPANET era uma rede estável e bem sucedida, com cerca de 200 IMPs.

Embora fosse crescendo rapidamente, o tipo de comunicação ARPANET **não era compatível com outras redes**. Começou então a pesquisar novos formas de comunicação entre redes. Em 1990, a ARPANET foi substituída por redes mais novas, criadas a partir da própria ARPANET.

E SURGE OUTRA REDE...

Era necessário um contrato de pesquisa com o DoD para fazer parte da ARPANET. Em 1984, a **NSF** começou a desenvolver um sucessor da ARPANET, aberto a todos os grupos de pesquisa, para fins civis. A **NSFNET** mantinha supercomputadores interconectados operando em San Diego, Boulder, Champaign, Pittsburgh, Ithaca e Princeton.

Cada supercomputador era conectado a um minicomputador (**fuzzball**). Os minicomputadores formavam as sub-redes.

O **encontro entre a ARPANET e a NSFNET** era realizado com a conexão entre um IMP e um fuzzball, em **Pittsburgh**.

OUTROS RUMOS

Depois da interconexão entre ARPANET e NSFNET, a rede cresceu muito rapidamente. Redes regionais foram integradas e conexões foram criadas entre Canadá, Europa e Pacífico. Em 1990, uma nova empresa, a ANS, assumiu a NSFNET, aumentando sua velocidade e alterando o nome para **ANSNET**. Neste momento eram 3 mil redes e 200 mil computadores.

Em 1992 foi conectado o milionésimo computador. Em 1995, a ANSNET foi desmembrada e vendida para a **AOL**. Outras regiões criaram redes semelhantes como a **EBONE** (pesquisa) e a **EuropaNET** (iniciativa privada).

O GRANDE BOOM

Até 1990, a rede era usada apenas para fins acadêmicos, com pesquisadores ligados ao governo, indústria e universidades. Foi quando **Tim Berners-lee** inventou o **WWW**, em que era possível trafegar hipertexto (códigos) e hipermídia (áudio, vídeo, imagens).

Milhares de usuários "comuns" foram atraídos para a rede, inicialmente com intuito apenas informativo. Podemos resumir a Internet como uma rede de redes, com bilhões de dispositivos conectados. Grande parte, constituída do que chamamos de **Internet Pública**, em contrapartida com a Internet Privada (chamada de Intranet);

GRANDE LEGADO

A Internet trouxe inúmeras aplicações e utilidades para a vida dos usuários e é há muitos anos a **ferramenta essencial que move o mundo**. Seus grandes legados podem ser vistos em várias partes como:

- **GPS** para mobilidade.
- **Documentos Eletrônicos** ante documentos físicos.
- **Ensino à Distância** para maior abrangência da educação.
- **Home Banking** para comodidade.
- **Correio Eletrônico** para comunicação.
- **Fóruns de Discussão** para debates e interação.
- **Transferência de Arquivos**.
- **Login Remoto** para agilidade em serviços.
- **Redes Sociais** para entretenimento.
- **Webmídia** para velocidade da informação.
- **Internet das Coisas**, a mais recente contribuição da Web.

PORQUE TANTAS REDES?

Porque existem tantas redes e quais as dependências de um mundo conectado?

- O mundo está demasiadamente **globalizado**.
- O acelerado **desenvolvimento tecnológico**.
- Expansão acentuada das redes de **comunicação**.
- Mudanças estratégicas em telecomunicações, transporte, negócios, etc.
- **Internacionalização** de mercados.
- Associações, fusões e programas cooperativos entre empresas.
- Ambiente de **competitividade**.

FACILIDADES E DESAFIOS

Podemos citar as facilidades trazidas pelas redes como:

- Facilitar a transferência de dados entre computadores.
- **Compartilhamento de recursos** com foco na economia.
- Segurança na duplicação de dados.
- Favorável às comunicações, com reuniões virtuais, videoconferências.
- Diversões interativas.

Mas também, há vários desafios:

- Planejamento e organização na implantação de uma rede.
- **Segurança** dos dados trafegados.
- Equilíbrio entre administração dos recursos e necessidade dos usuários.
- **Escalabilidade** de hardware e software, visando atualização.
- Integração.

COMPONENTES E CONCEITOS

HOST

Os computadores que participam de uma rede são chamados de ***host***. Alguns hosts são classificados como cliente e outros como servidores.

Os clientes contém softwares para solicitar e exibir informações obtidas de um servidor. Já os servidores contém softwares para fornecer serviços e informações, como correio eletrônico e páginas Web, podendo atender a muitos clientes simultâneos.

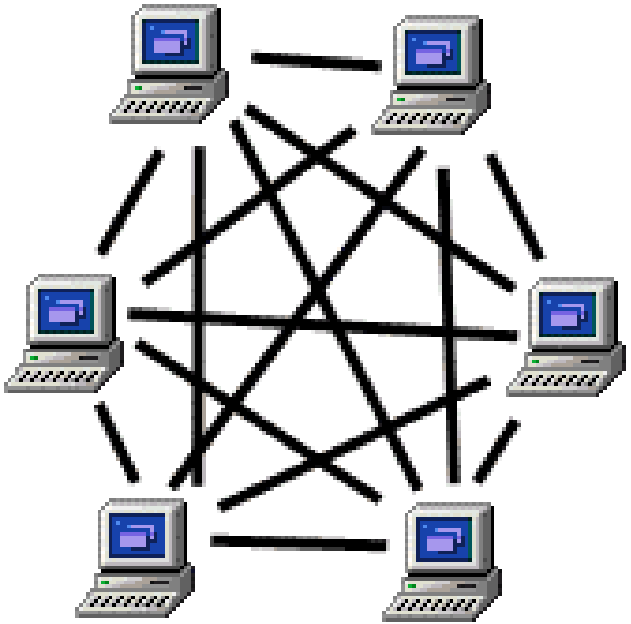
ARQUITETURAS

Quando os softwares de cliente e de servidores são executados no mesmo computador, este tipo de arquitetura é chamada de **PONTO-A-PONTO**. É bastante comum em pequenas empresas e residências.

As **vantagens** de uma rede ponto a ponto são a facilidade de configuração, a baixa complexidade, o baixo custo e o bom desempenho para tarefas simples.

Já as **desvantagens** ficam pelo fato da administração centralizada, não ser tão segura e confiável, não ser escalável e a possível lentidão gerada por sobrecarga na rede.

Peer to Peer Network



DESAFIOS

Em uma rede P2P, a arquitetura fica dependente da disponibilidade dos dispositivos, já que estes são livres para entrar ou sair da rede. Os participantes de P2P são de origens diversas. Com isso, há uma preocupação maior com a segurança e confiabilidade dos dados.

Participantes mais próximos tendem a ter um melhor tempo de resposta entre as interações. Otimizar a **latência** é um desafio;

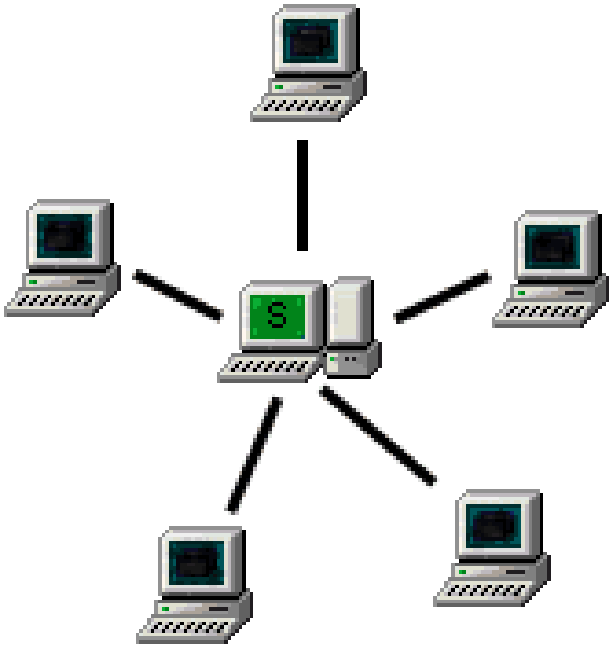
ARQUITETURAS

A arquitetura **CLIENTE-SERVIDOR** é a mais comum nas redes, inclusive na internet. Os papéis são bem definidos e exclusivos.

Tipos comuns de softwares de servidor são:

- **E-mail**, onde o servidor recebe e envia as mensagens e os clientes utilizam o navegador ou um programa para acessá-las.
- **Web**, onde o servidor armazena as páginas e scripts e os clientes utilizam o navegador para lê-las .
- **Arquivo**, onde o servidor armazena os arquivos e os clientes acessam, fazem download e upload.

Server Based Network



SEGURANÇA E CONTROLE

As maiores vantagens em relação ao uso de redes P2P, é com a segurança e confiabilidade das informações trafegadas.

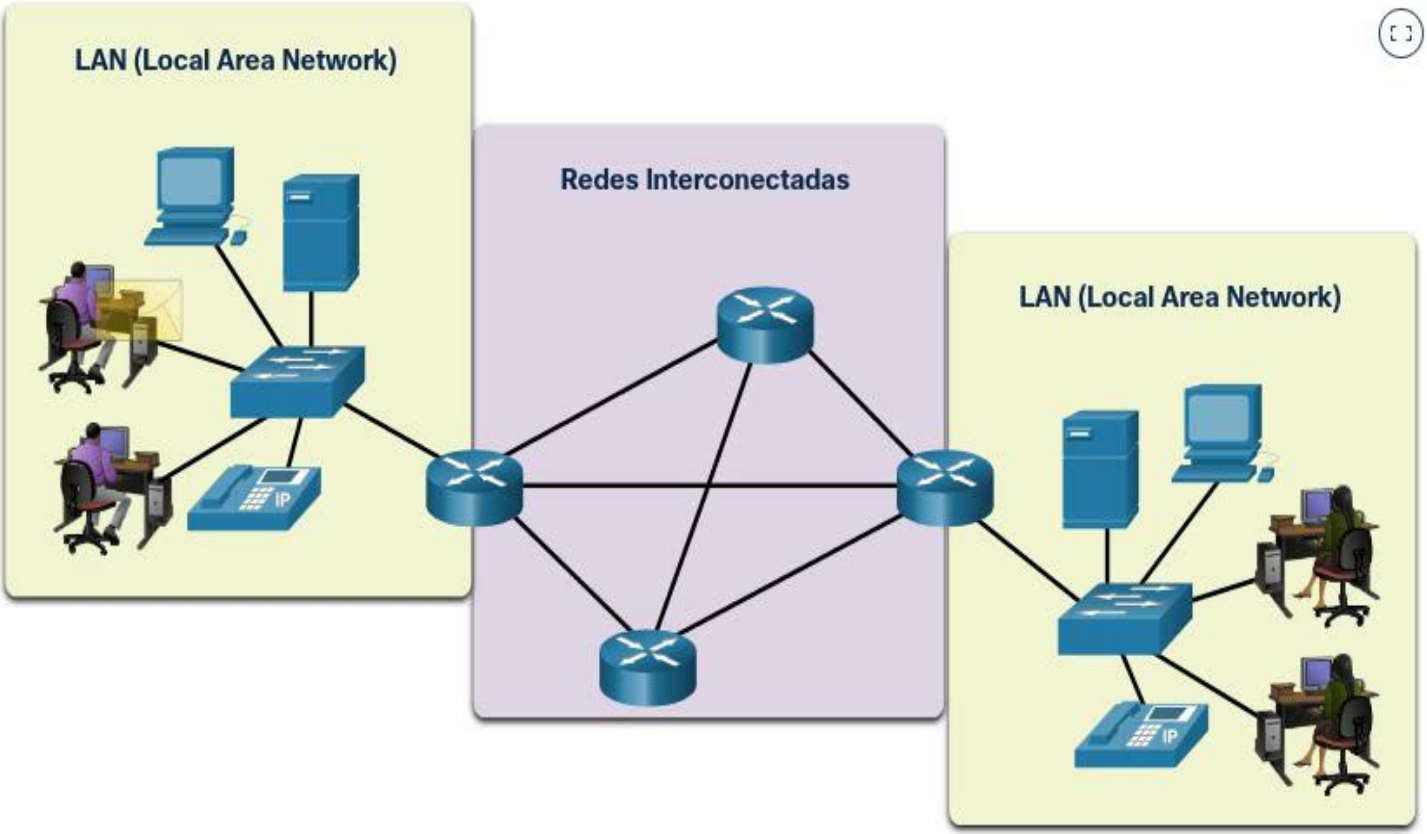
O servidor central pode controlar o tráfego, prevenir falhas é aumentar o tempo de resposta das tarefas.

Também pode evitar a duplicação de dados e sincronismo entre as máquinas.

DISPOSITIVOS FINAIS

A maioria dos dispositivos de rede que estamos familiarizados são classificados como dispositivos finais, e nós como, usuários finais de determinado serviço.

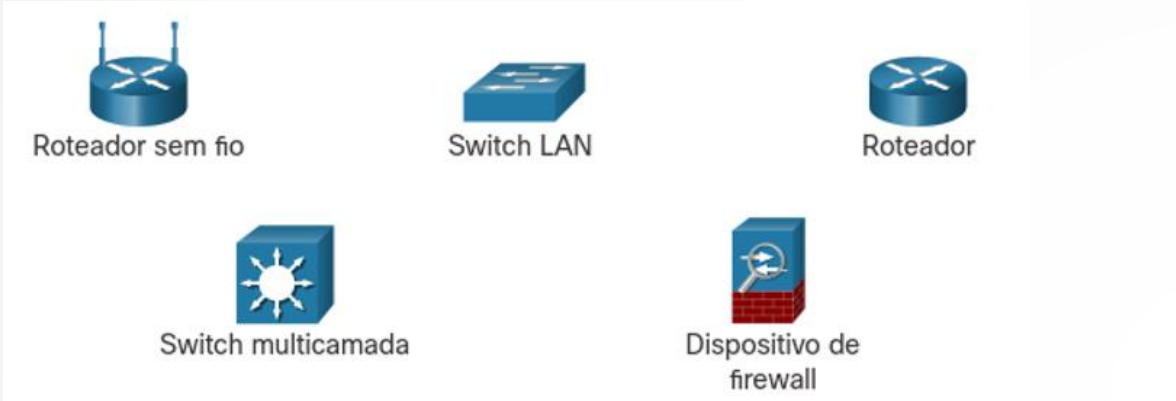
A comunicação nas redes ocorre com um dispositivo final originando uma mensagem, com destino a outro dispositivo final.


LAN (Local Area Network)
Redes Interconectadas
LAN (Local Area Network)
IP
IP

DISPOSITIVOS INTERMEDIÁRIOS

Os dispositivos estão no "**miolo**" da rede intermediários asseguram o fluxo dos dados, além de outras funções.

- Regeneram e retransmitem sinais de comunicação
- Notificam erros e falhas
- Mantém informações sobre os caminhos disponíveis
- Direcionam dados para caminhos alternativos
- Classificam mensagens de acordo com a prioridade
- Controlam a permissão do fluxo para segurança



E O HUB HERDADO?

O Hub era um dos principais equipamentos presentes nas redes, atuando como um concentrador e repetidor de múltiplas portas, controlando o fluxo;

Com o tempo foi caindo em desuso, reforçado pelo fato de, internamente, não fazer filtro dos dados, simplesmente transmitindo para todas as portas, o que gerava **tráfego desnecessário**.

MEIOS DE REDE

A comunicação na rede ocorre através de uma mídia, na qual a mensagem viaja por um determinado mecanismo. As redes modernas utilizam 3 mídias para transmissão.

- **Fios de metal**, onde os dados são codificados em **impulsos elétricos**.
- **Fibras de vidro ou plástico**, onde os dados são codificados em **impulsos de luz**.
- **Transmissão sem fio**, onde os dados são codificados através da modulação de frequências específicas de **ondas eletromagnéticas**.

Como escolher a mídia ideal? Varia, mas no geral devemos considerar:

- Distâncias percorridas;
- Ambiente de instalação;
- Custo;
- Quantidade de dados e velocidade requerida.

COMUNICAÇÃO HALF-DUPLEX E FULL DUPLEX

A base da comunicação é a troca de informação entre 2 agentes. Na comunicação half-duplex, o meio é compartilhado mas **não suporta transmissão e recepção simultânea**, ou seja, apenas um dispositivo pode utilizar a mídia por vez, para enviar ou receber. Tecnologia sem fio, o Hub herdado e topologias em barramento trabalham em half-duplex.

Já na comunicação full-duplex, ambos os dispositivos podem enviar e receber ao mesmo tempo, semelhante a uma linha telefônica.

CONTROLE DE ACESSO

Quando o meio de transmissão é compartilhado, as redes implementam métodos de controle de acesso para diminuir ocorrências de **colisões de pacotes**. São dois tipos:

- **Contenção**: todos os nós operam em half-duplex e há um processo quando dois dispositivos tentam transmitir ao mesmo tempo. As redes sem fio utilizam esse método.

- **Controlado**: no acesso controlado, cada nó tem seu próprio intervalo de tempo para utilizar o meio. Em antigas topologias chamadas de Token Ring, era utilizado uma espécie de **ficha** (*token*), onde quem a possuía era autorizado a utilizar o meio, liberando-a posteriormente.

TIPOS DE CONTENÇÃO

Os métodos baseados (CSMA) em contenção podem trabalhar de duas formas, por **detecção de colisão (CD)** ou por **prevenção de colisão (CA)**

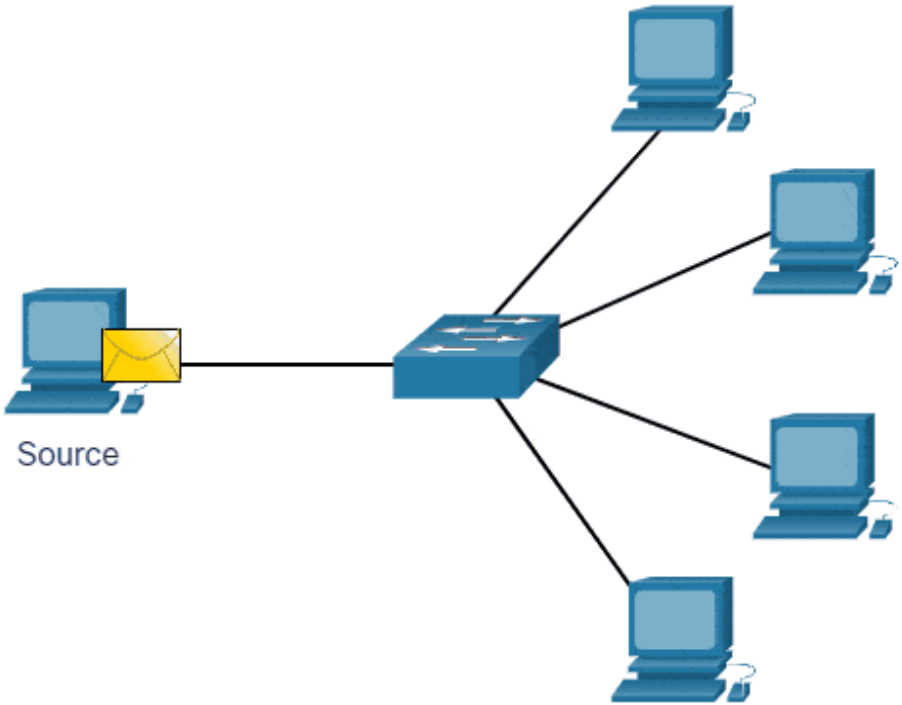
- **CSMA/CD**: quando dois nós tentam transmitir ao mesmo tempo ocorre uma colisão de pacotes que é detectada pelos dois dispositivos. Os dados enviados são corrompidos e precisão ser reenviados.

- **CSMA/CA**: não detecta colisões e sim tenta evitá-las, com um tempo de espera para cada dispositivo, antes de transmitir. Quando um dispositivo transmite, informa um tempo necessário para isso e todos os outros dispositivos recebem essa informação, estimando o período em que o meio está indisponível.

TIPOS DE COMUNICAÇÃO

As comunicações em rede de dados seguem 3 tipos semelhantes para entrega de mensagem

- **Unicast**: as informações são enviadas para um único dispositivo final.
- **Multicast:** as informações são enviadas para mais de um dispositivo final.
- **Broadcast** as informações são enviadas para todos os dispositivos finais da mesma rede.



Unicast

Multicast

Broadcast

TIPOS DE ABRANGÊNCIA

REDES DE VÁRIOS TAMANHOS

Uma rede pode conectar simplesmente dois computadores ou milhões de dispositivos.

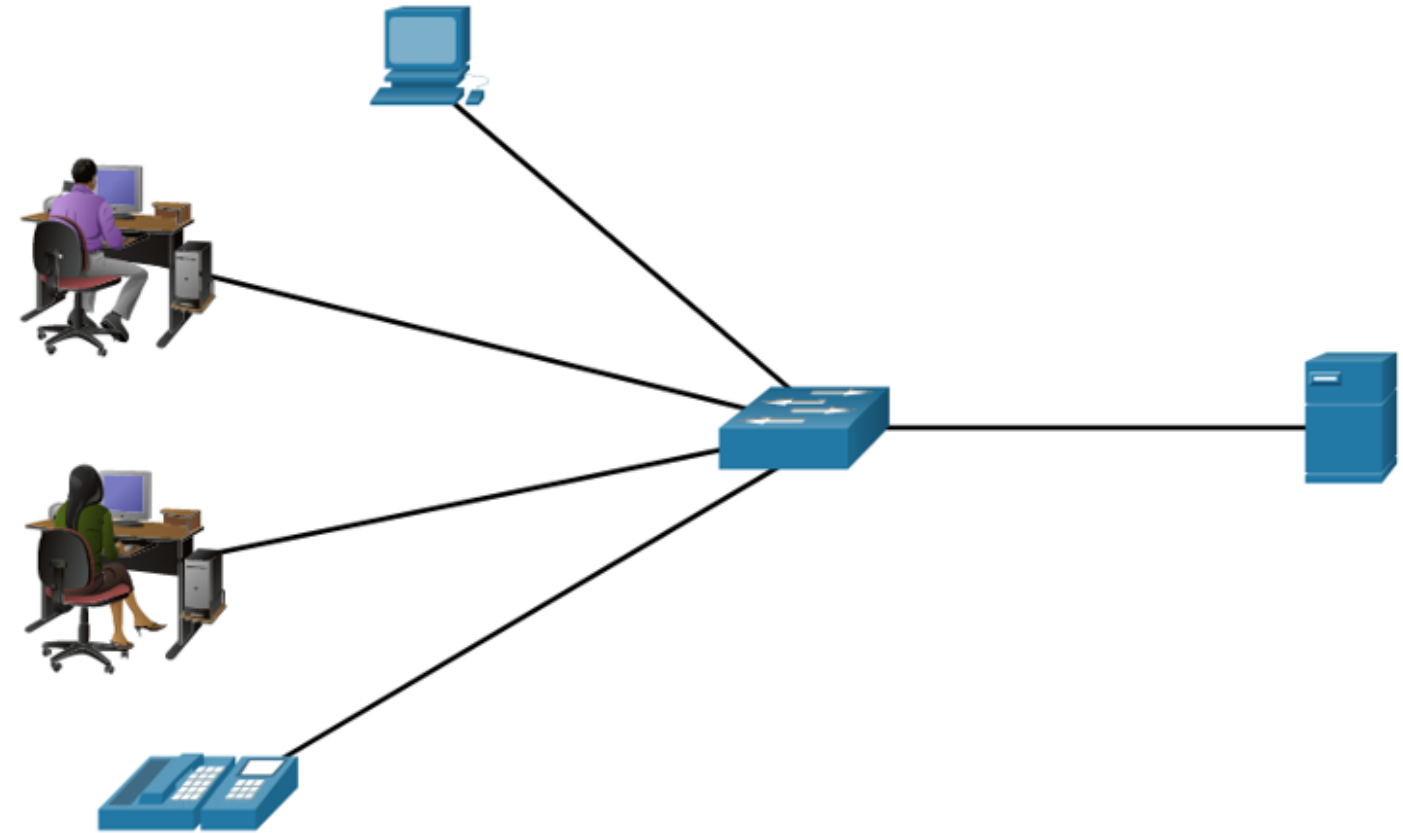
Uma **rede doméstica** pode compartilhar impressoras, documentos e outros recursos com dispositivos locais. Pode-se comportar também como uma **rede de escritório doméstico**, quando voltada ao trabalho.

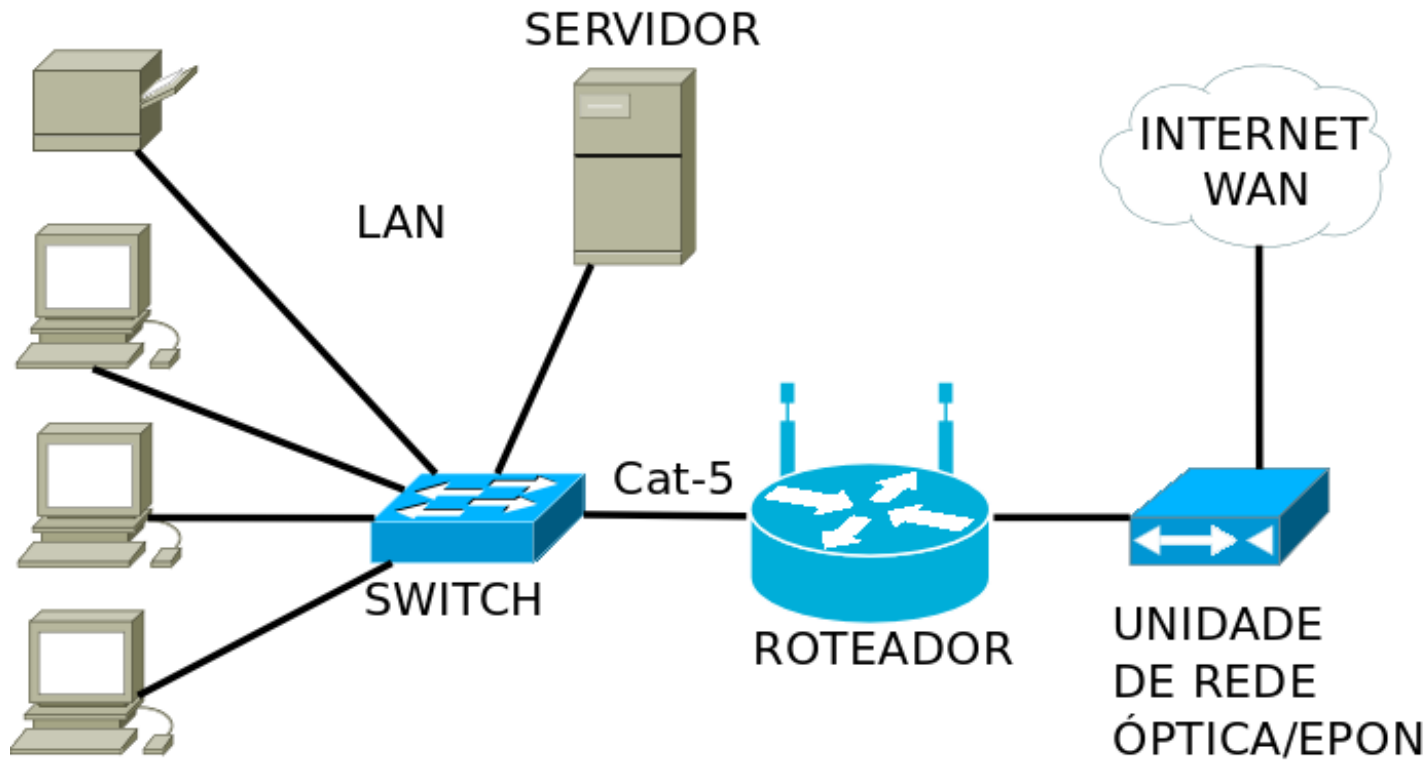
Já a **Internet** é a maior rede existente, sendo na verdade, formada por redes menores ao redor do mundo, todas interconectadas.

REDES LOCAIS (LAN)

Um abrangência bastante difundida é a rede LAN. Trata-se de uma **rede de pequeno alcance geográfico**, geralmente atribuída a um único operador, empresa, entidade jurídica ou acadêmica. **É uma rede privada**

- Velocidade geralmente alta entre os dispositivos, sendo geralmente de baixo custo.
- São ideais para conectar equipamentos em escolas, ambientes domésticos, escritórios e edifícios próximos.

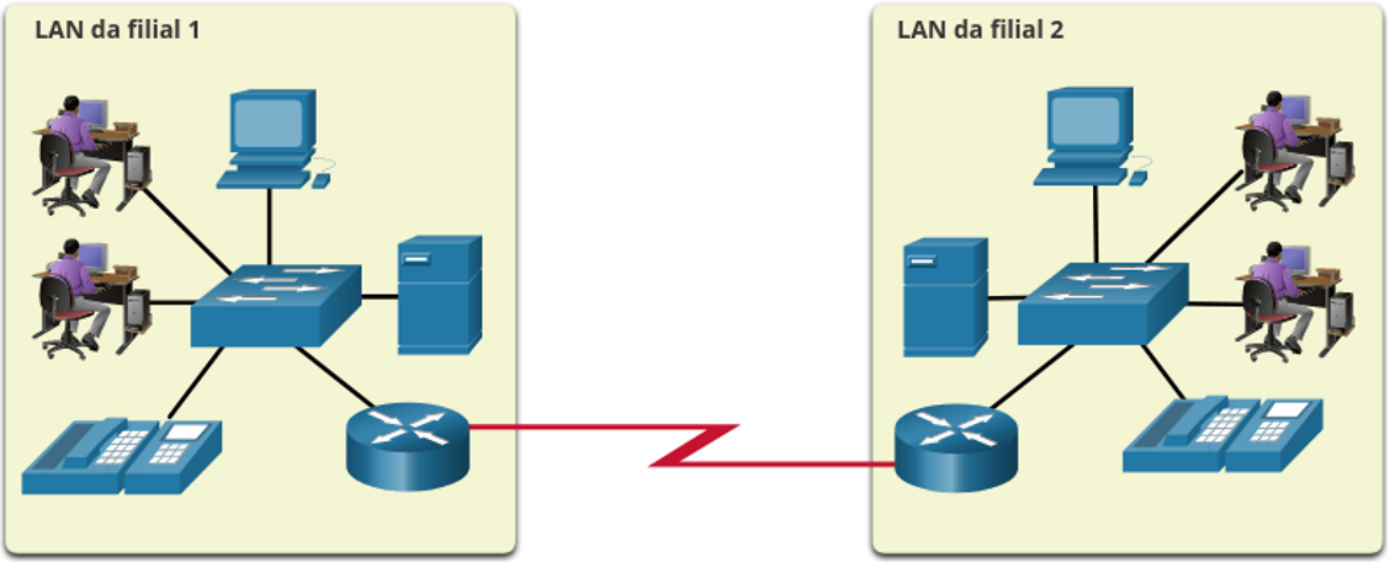



SERVIDOR
LAN
INTERNET
WAN
Cat-5
SWITCH
ROTEADOR
UNIDADE
DE REDE
ÓPTICA/EPON

REDES EXTENDIDAS (WAN)

Outra abrangência comum é a rede WAN. Trata-se de uma **rede de longo alcance geográfico**, geralmente referindo-se a Internet ou ao serviço de conexão de um provedor.

Fornece velocidade geralmente mais lenta, sendo mais cara quanto mais rápida. **É geralmente uma rede pública**.

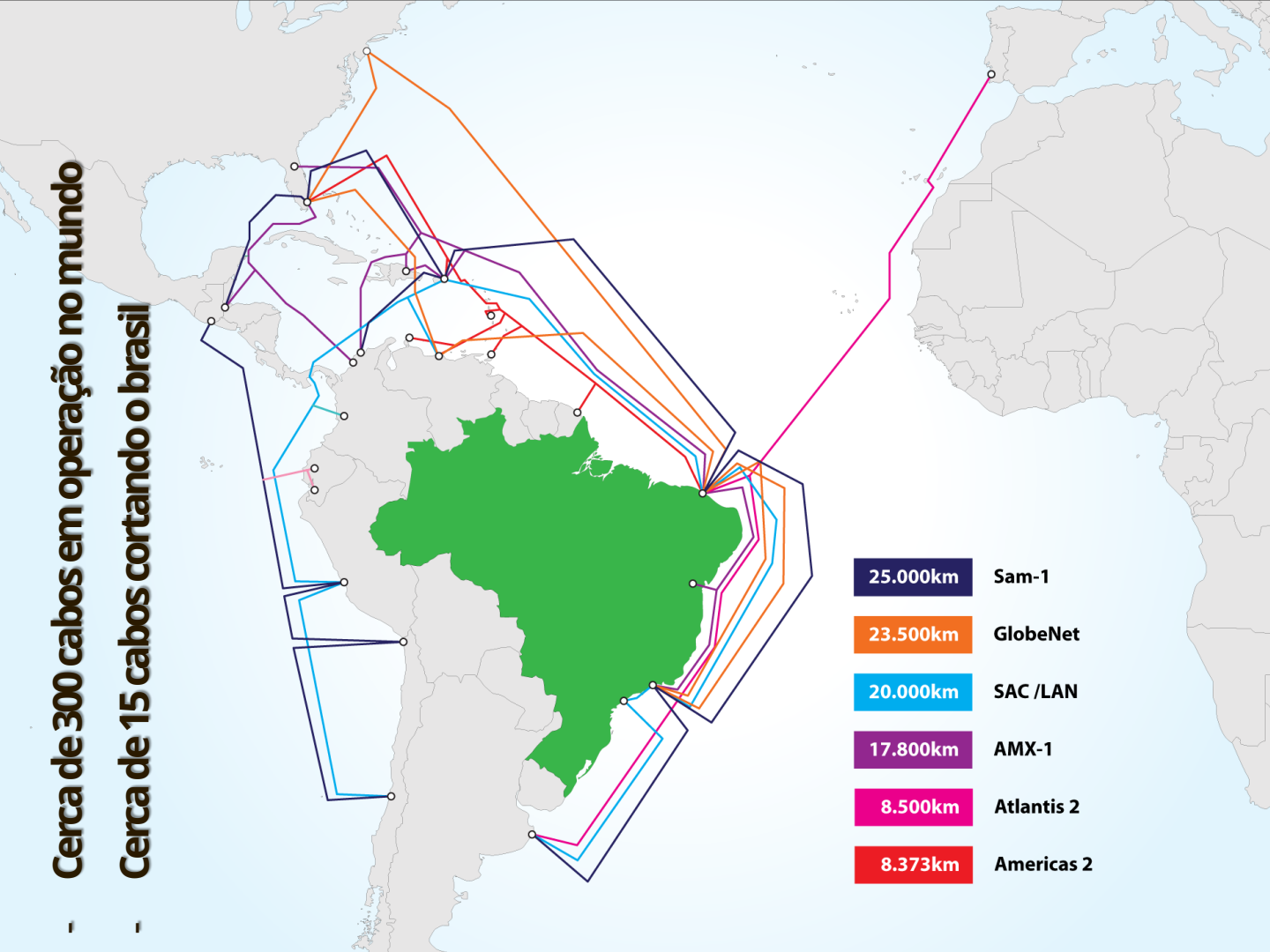

LAN da filial 1
LAN da filial 2

ENTENDENDO MELHOR A INTERNET

Como vimos, a Internet é uma rede WAN. É uma coleção mundial de redes interconectadas, entre LANs e WANs, podendo ainda ser composta de várias mídias. Não é de propriedade de nenhum indivíduo ou grupo. São interligadas por **cabos submarinos**.

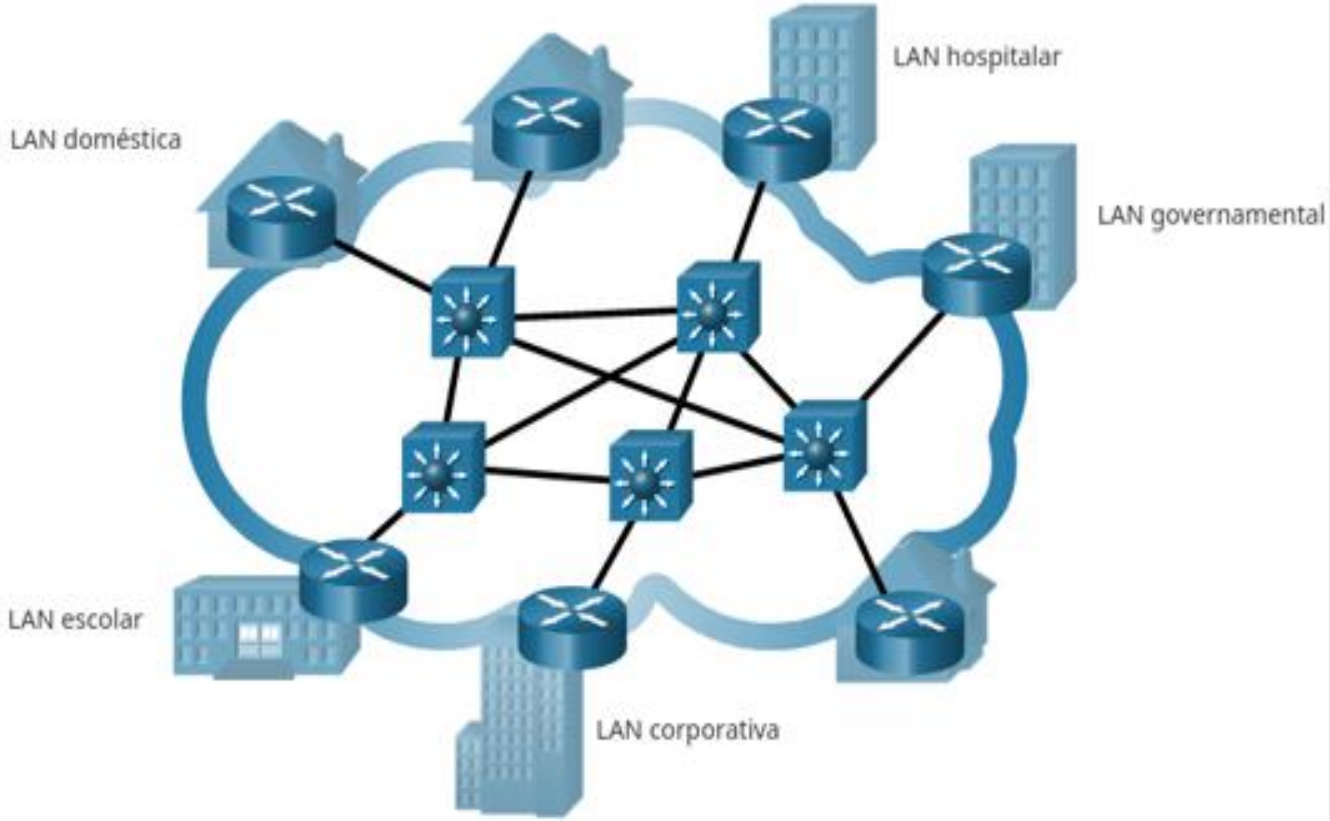
Garantir que tudo isso funcione exige cooperação de diversos órgãos na organização e uso, sendo alguns deles, o **IETF** (Internet Engineering Task Force), o **ICANN** (Internet Corporation for Assigned Names and Numbers) e a **IAB** (Internet Architecture Board).

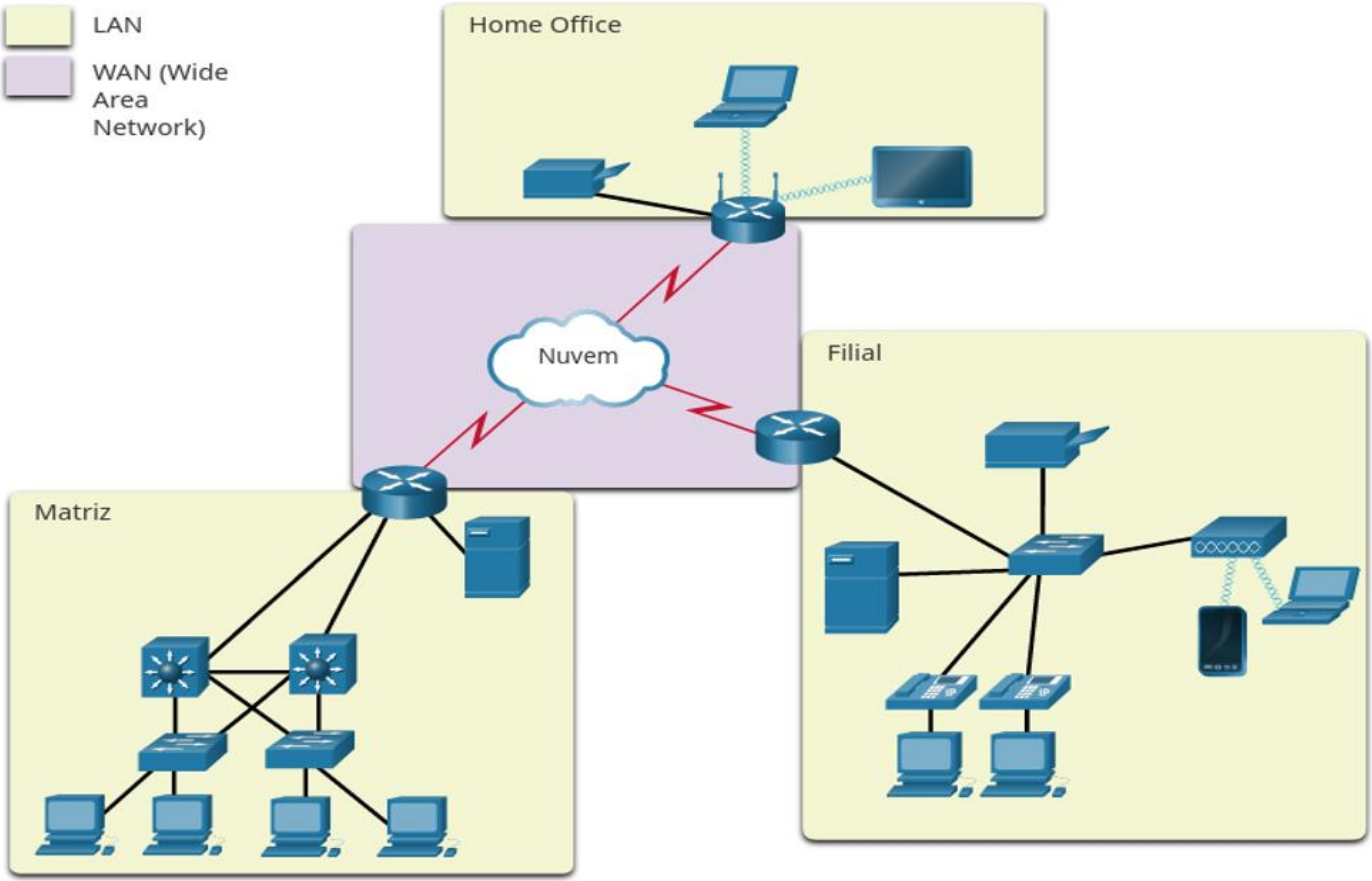
- Cerca de 300 cabos em operação no mundo
- Cerca de 15 cabos cortando o brasil



E QUANDO VOCÊ RECLAMA DA OPERADORA E DESCOBRE

QUE A SUA INTERNET CAIU PORQUE...


LAN hospitalar
LAN doméstica
LAN governamental
LAN escolar
LAN corporativa


LAN
WAN (Wide Area Network)
Home Office
Nuvem
Filial
Matriz

OUTRAS ABRANGÊNCIAS

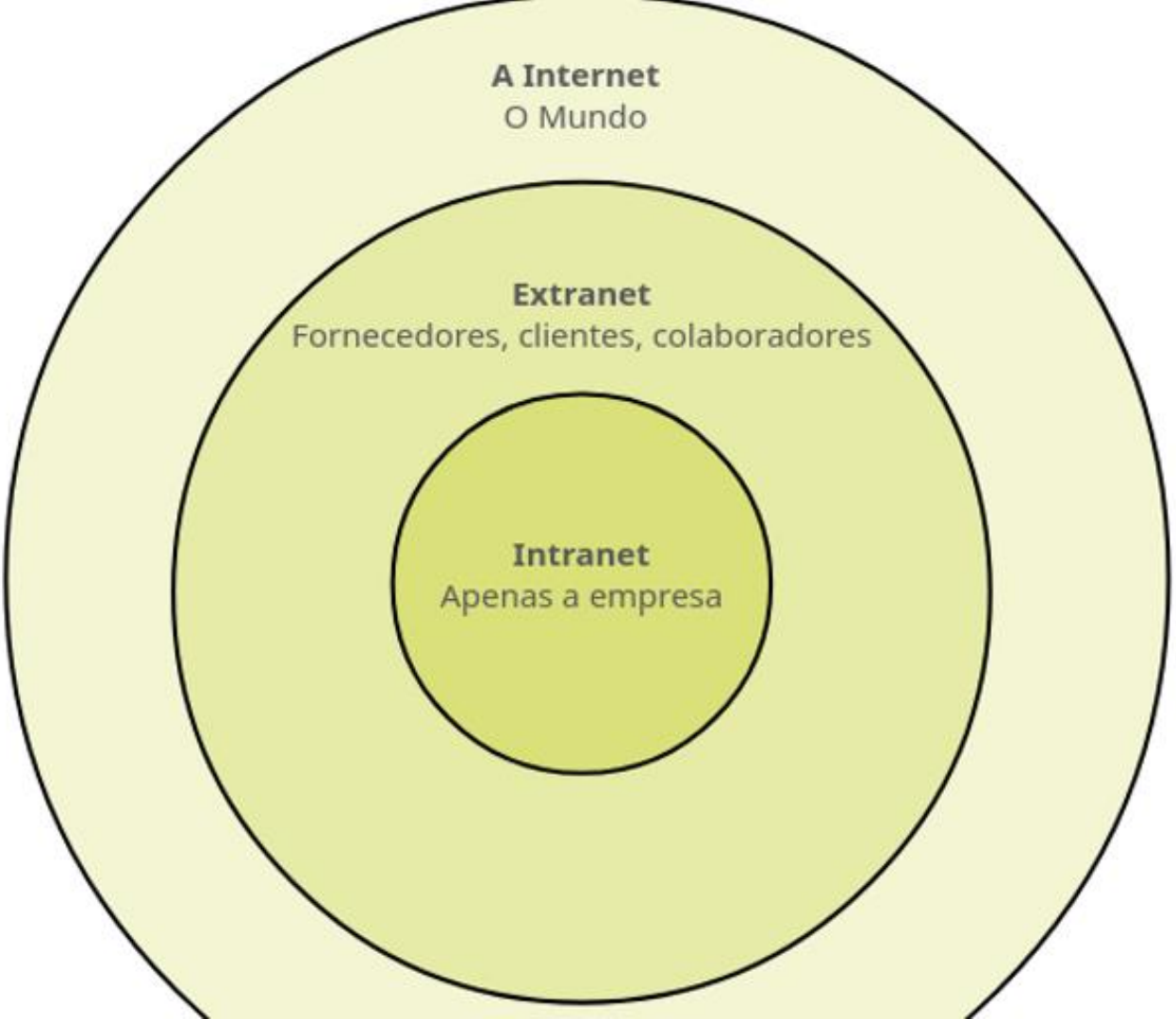
Existem outras abordagens menos comuns para o tamanho das redes, como:

- **MAN**, uma rede de abrangência metropolitana, podendo representar a infraestrutura de um provedor em determinada região.
- **GAN**, um conceito de rede global, de alcance ilimitado, englobando satélites e dispositivos móveis a nível mundial.
- **PAN**, rede de alcance pessoal, baseada nas tecnologias *bluetooth*, *Zigbee*, RFID e NFC, com melhor consumo de energia.
- **SAN**, rede voltada para sistemas de armazenamento (storages), com controle de versão e tolerância a falhas.

INTRANET E EXTRANET

A Intranet é uma junção **privada** de LAN e WAN, como se fosse uma internet particular, pertencente a uma única organização. Pode ser acessada somente por membros, funcionários ou outras pessoas autorizadas.

Quando a organização permite acesso externo a Intranet, ela o faz através de uma Extranet. A Extranet, obrigatoriamente deve oferecer um ambiente seguro e protegido para acesso, com **identificação** do visitante.


A Internet
O Mundo
Extranet
Fornecedores, clientes, colaboradores
Intranet
Apenas a empresa

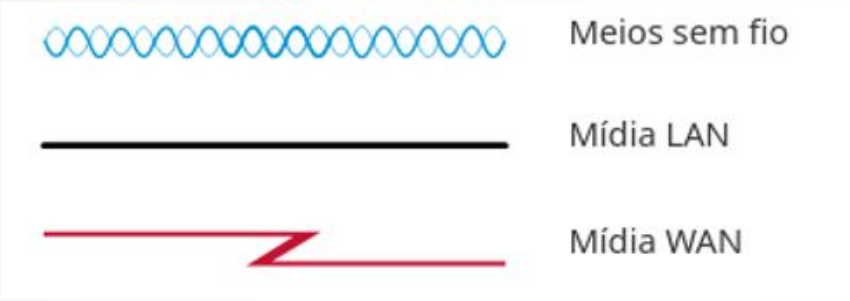
SIMBOLOGIAS E DIAGRAMA DE TOPOLOGIA

REPRESENTANDO A REDE

Demonstrar como a rede será pode ser um bom começo. É importante visualizar onde serão as conexões e como tudo ocorrerá, como num mapa visual.

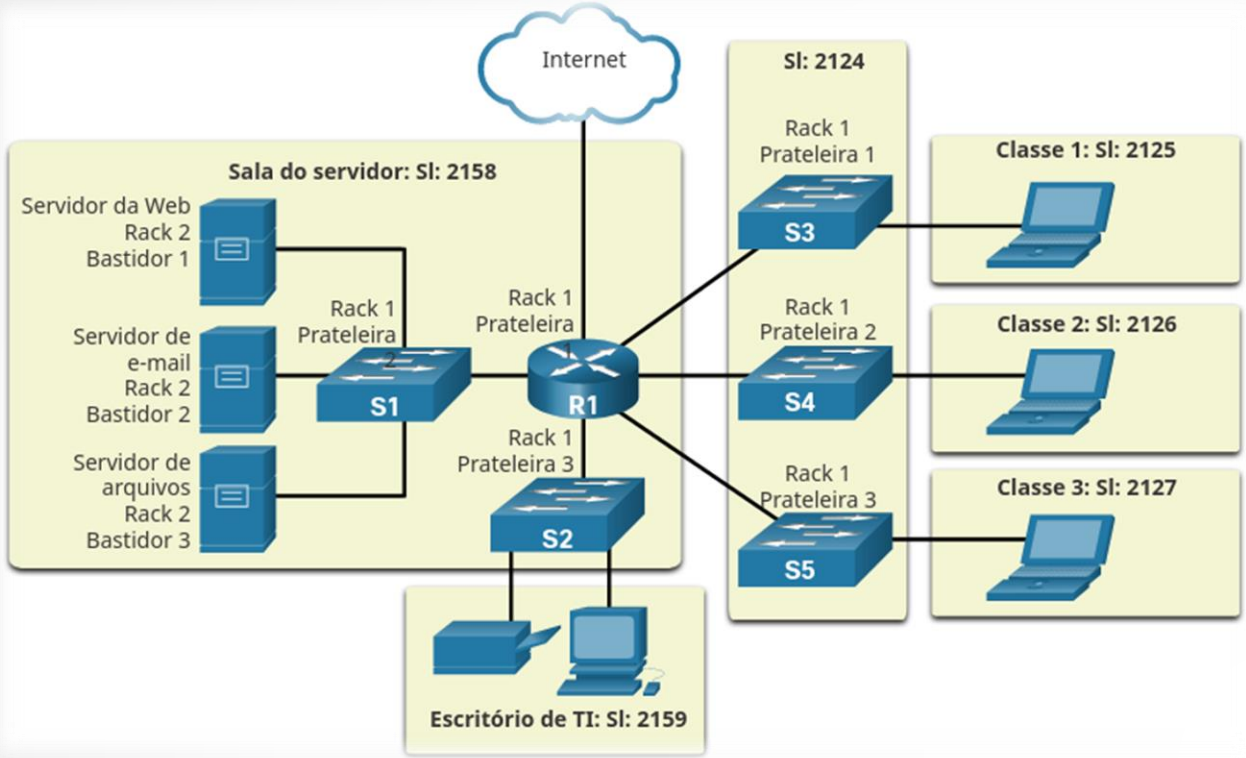
Um diagrama de topologia fornece uma “fotografia” da rede, facilitando a identificação de como os dispositivos se conectam, utilizando algumas terminologias próprias.

- **Porta Física**, é um **conector físico** em um dispositivo, onde é conectada uma mídia.
- **Interface ou Porta Lógica**, são **portas virtuais** em um dispositivo, para objetivos específicos.



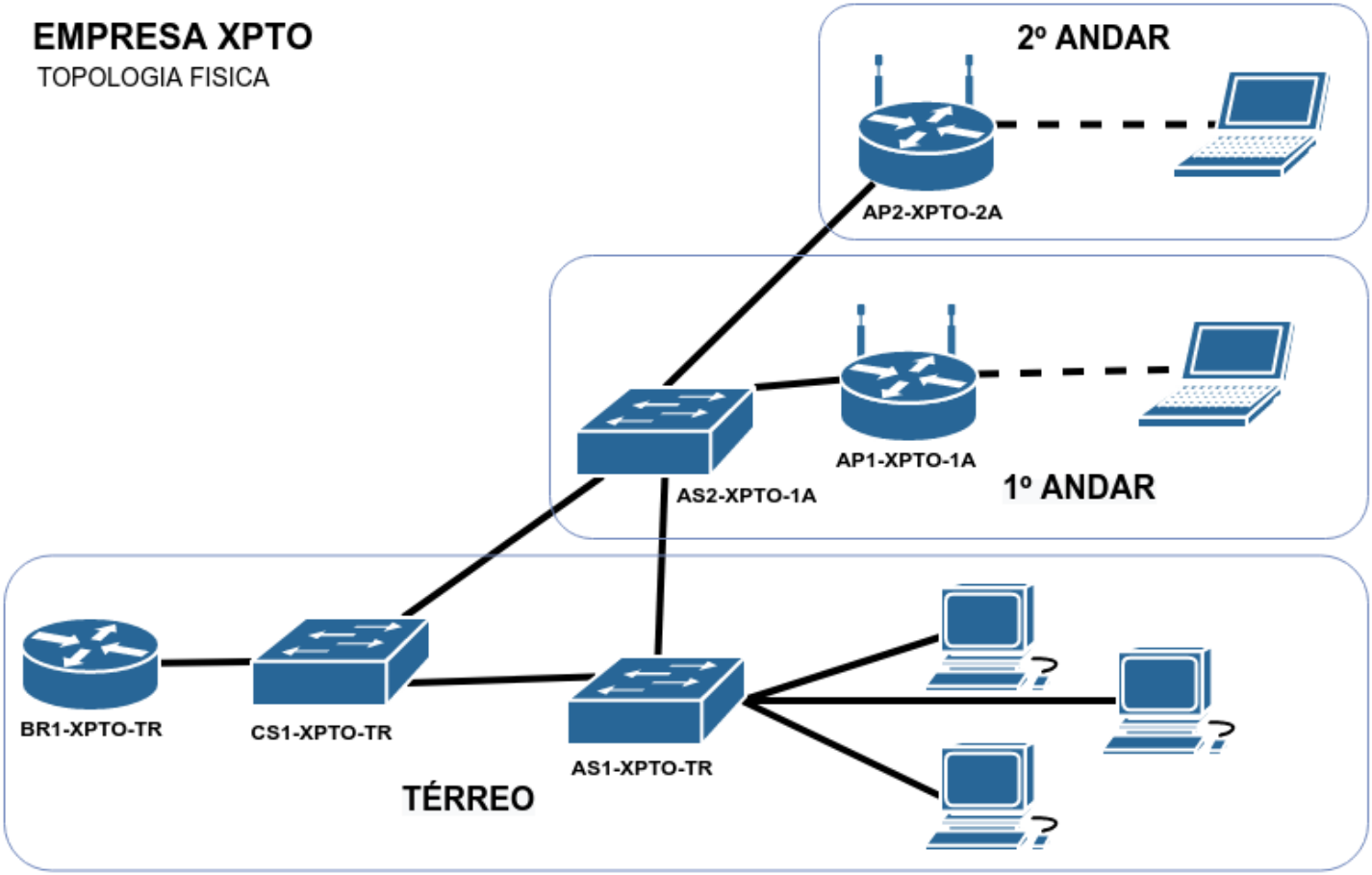
TOPOLOGIA FÍSICA

O diagrama de topologia física mostram apenas as localizações físicas, de forma rotulada, e as mídias utilizadas.



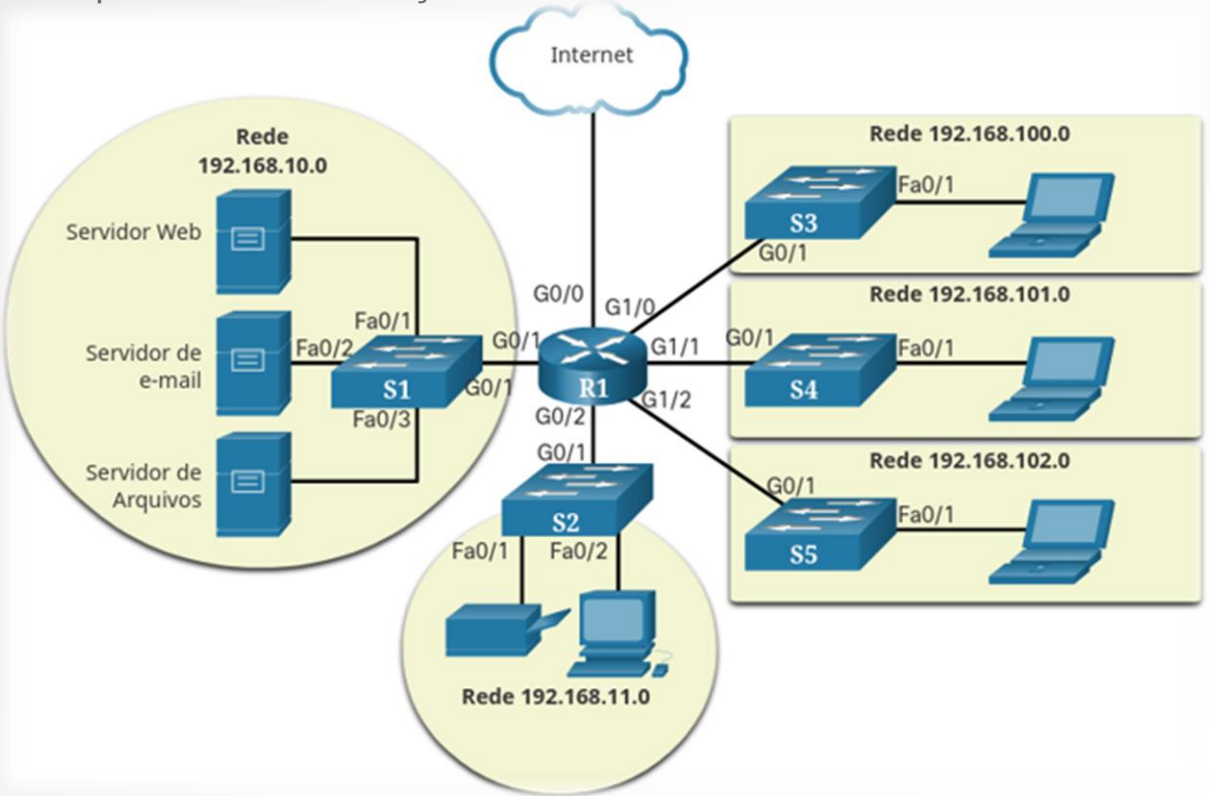
EMPRESA XPTO

TOPOLOGIA FISICA



TOPOLOGIA LÓGICA

O diagrama de topologia lógica ilustram os dispositivos, portas e o esquema de endereçamento utilizado.



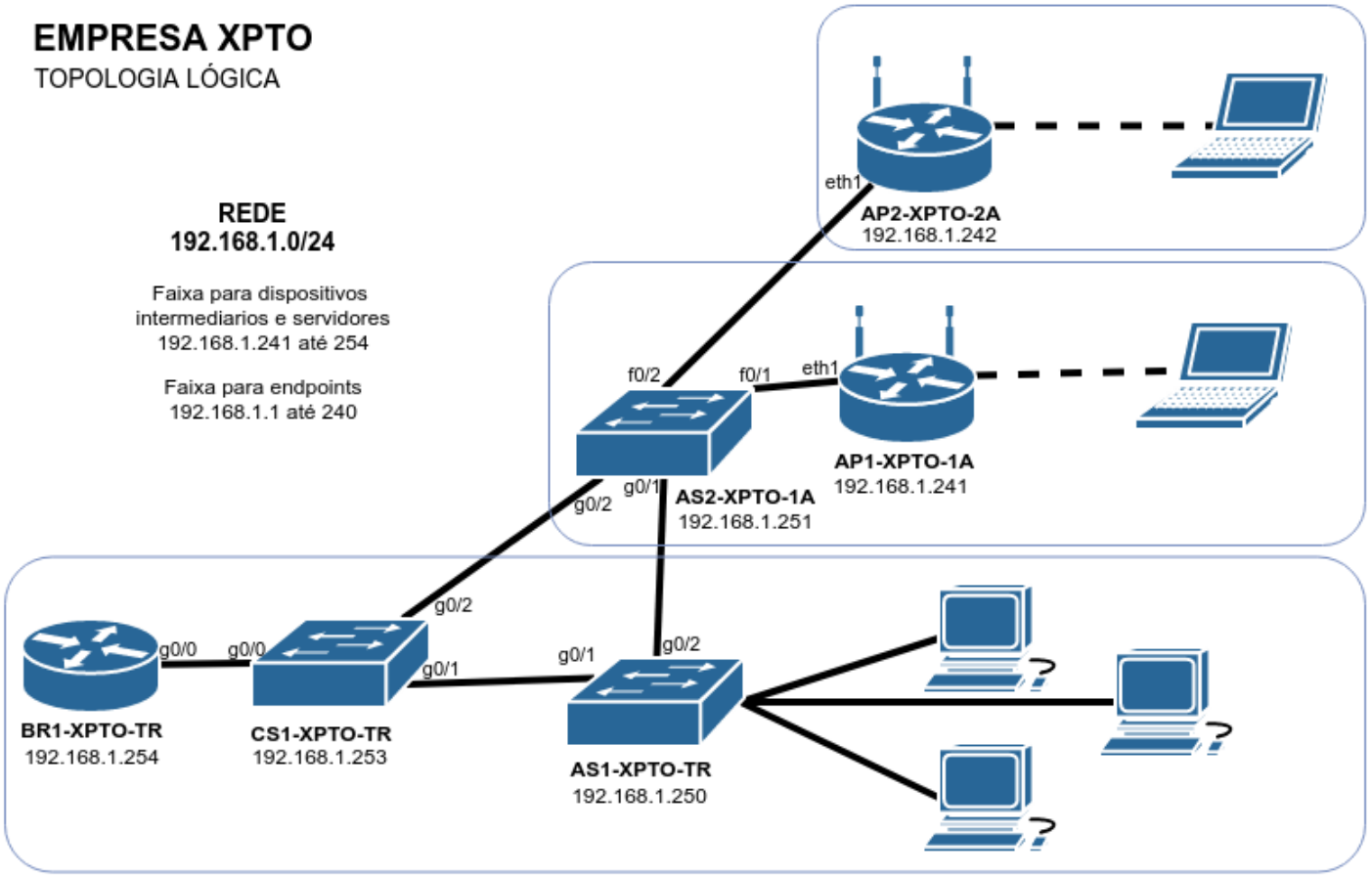
EMPRESA XPTO

TOPOLOGIA LÓGICA

REDE
192.168.1.0/24

Faixa para dispositivos intermediarios e servidores
192.168.1.241 até 254

Faixa para endpoints
192.168.1.1 até 240



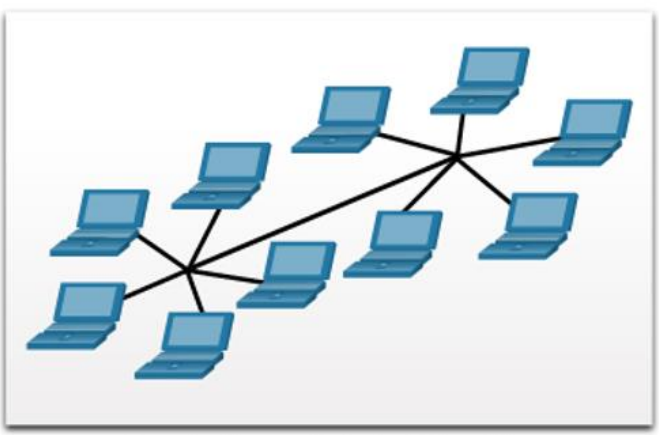
TOPOLOGIAS LAN

Nas redes locais, os dispositivos podem ser interligados em topologias chamadas **Estrela** ou **Estrelas Estendida**. Dessa forma, todos os dispositivos são conectados a um dispositivo intermediário central, com este podendo interconectar vários outros intermediários. São topologias **fáceis de instalar**, muito **escalonáveis** e fáceis de resolver problemas. Existem também topologias legadas, utilizadas nas primeiras redes:

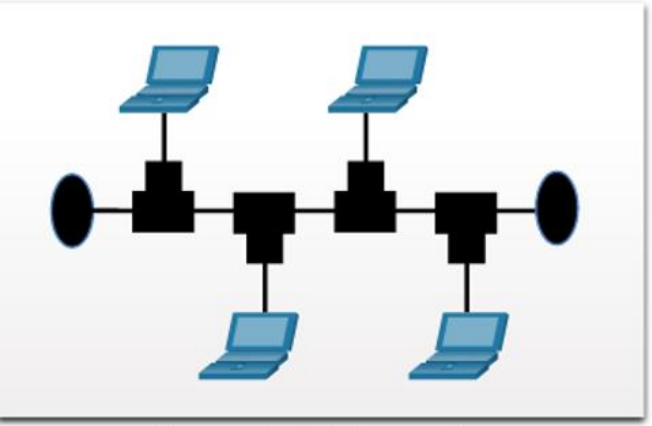
- **Barramento**: todos os dispositivos são encadeados, com **terminadores** nas extremidades. Usava cabos coaxiais, era barato e fácil de configurar. Como o meio era compartilhado, quanto mais computadores conectados, mais lenta é transmissão, uma vez que os dados passam por todas as máquinas.

- **Anel**: os dispositivos finais eram conectados ao vizinho, formando um anel, podendo ainda formar um anel duplo para redundância, numa técnica chamada **Beaconing**. Pode ser utilizado hoje em redes ópticas.

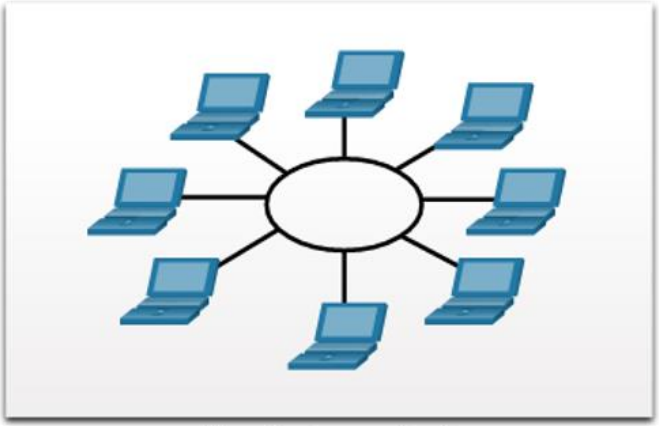
Topologia em Estrela



Topologia em Estrela Estendida



Topologia de Barramento



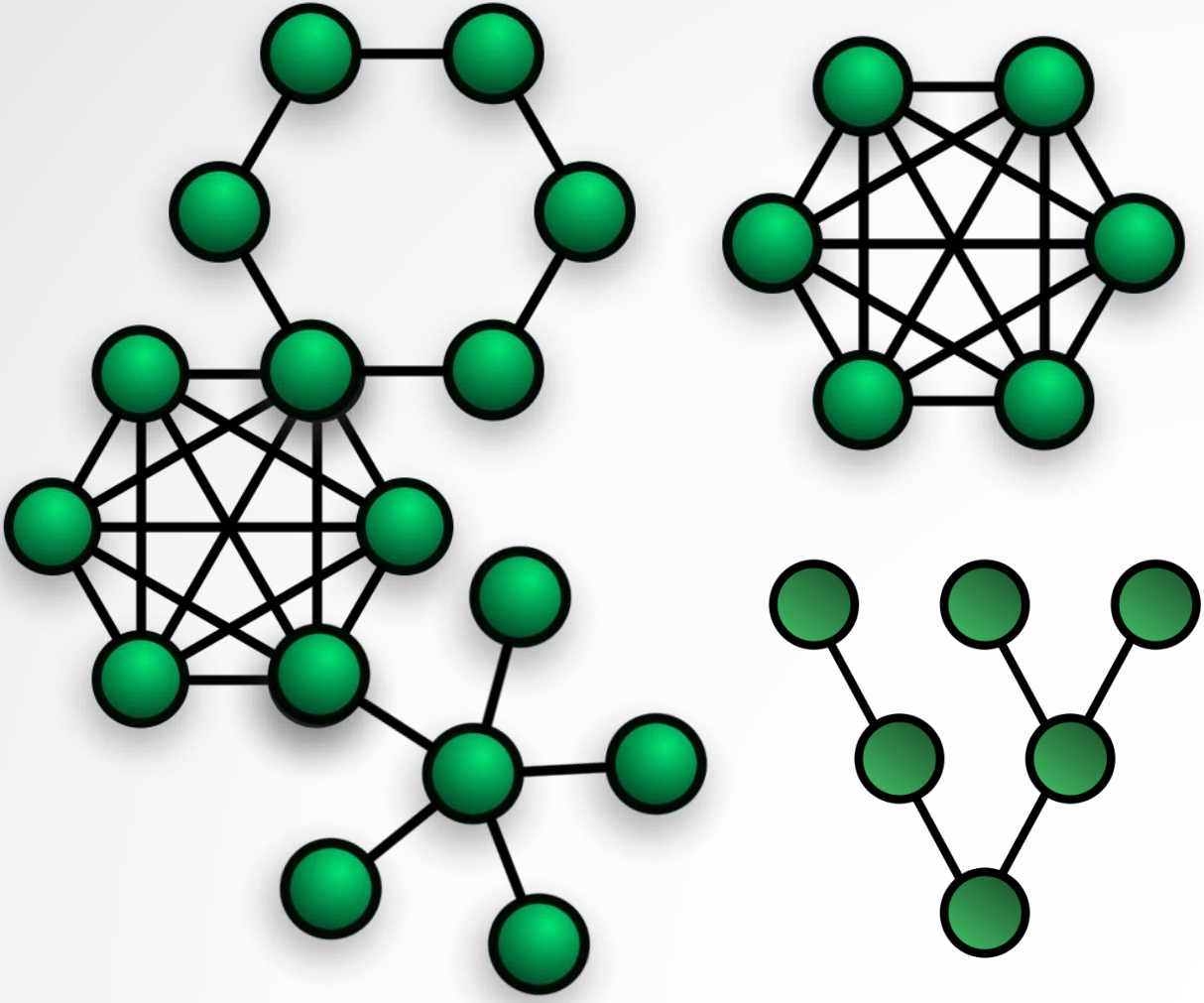
Topologia em Anel

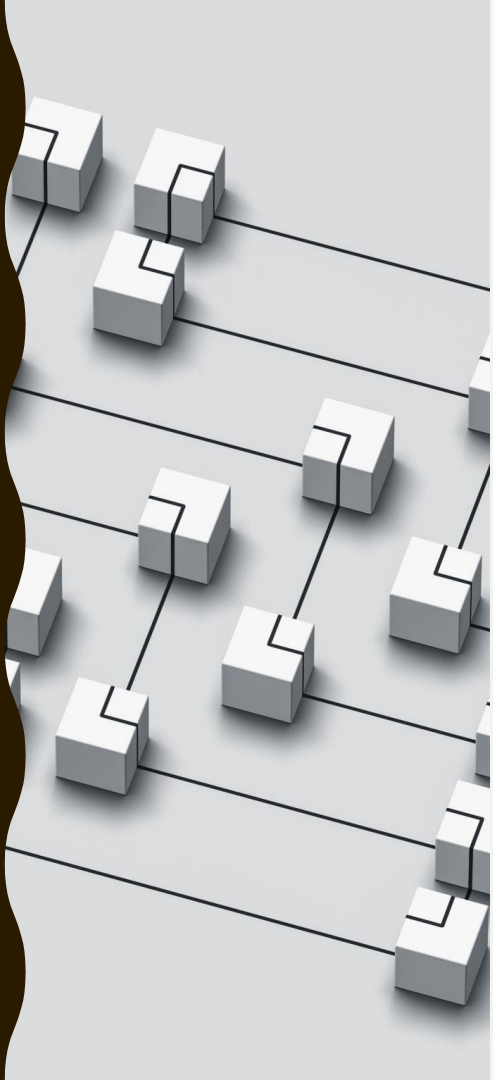
OUTRAS TOPOLOGIAS

- **Árvore (Tree)**: Variação da topologia estrela, onde as máquinas são dispostas de forma **hierárquica**, formando vários níveis, interligados por concentradores. A dependência passa a ser maior, pois se um concentrador falhar pode causar um "**efeito dominó**" nas redes inferiores. Facilidade de manutenção característica na topologia estrela também se aplica na árvore, porém em maior escala.

- **Malha (Mesh)**: Semelhante a topologia estrela, porém sem concentradores, com máquinas ligadas diretamente umas a outras (**ponto-a-ponto**). Apresenta excelente tolerância a falhas, porém de estrutura bastante complexa e cara, sendo pouco usadas em redes locais. Mais recentemente, passou-se a usar uma **arquitetura de transmissão sem fio** em malha.

- **Mista (Mixed)**: Reúnem características de dois ou mais topologias em uma única estrutura de rede. Implica alto custo de implantação e manutenção, sendo utilizada em casos bem específicos. Sua administração é descentralizada, geralmente sendo operada por topologias, isto é, não há um equipamento central de forma geral.





LABORATÓRIO

Construir um diagrama de topologia física simples da rede da sua casa.

- Cisco Packet Tracer
- DIA

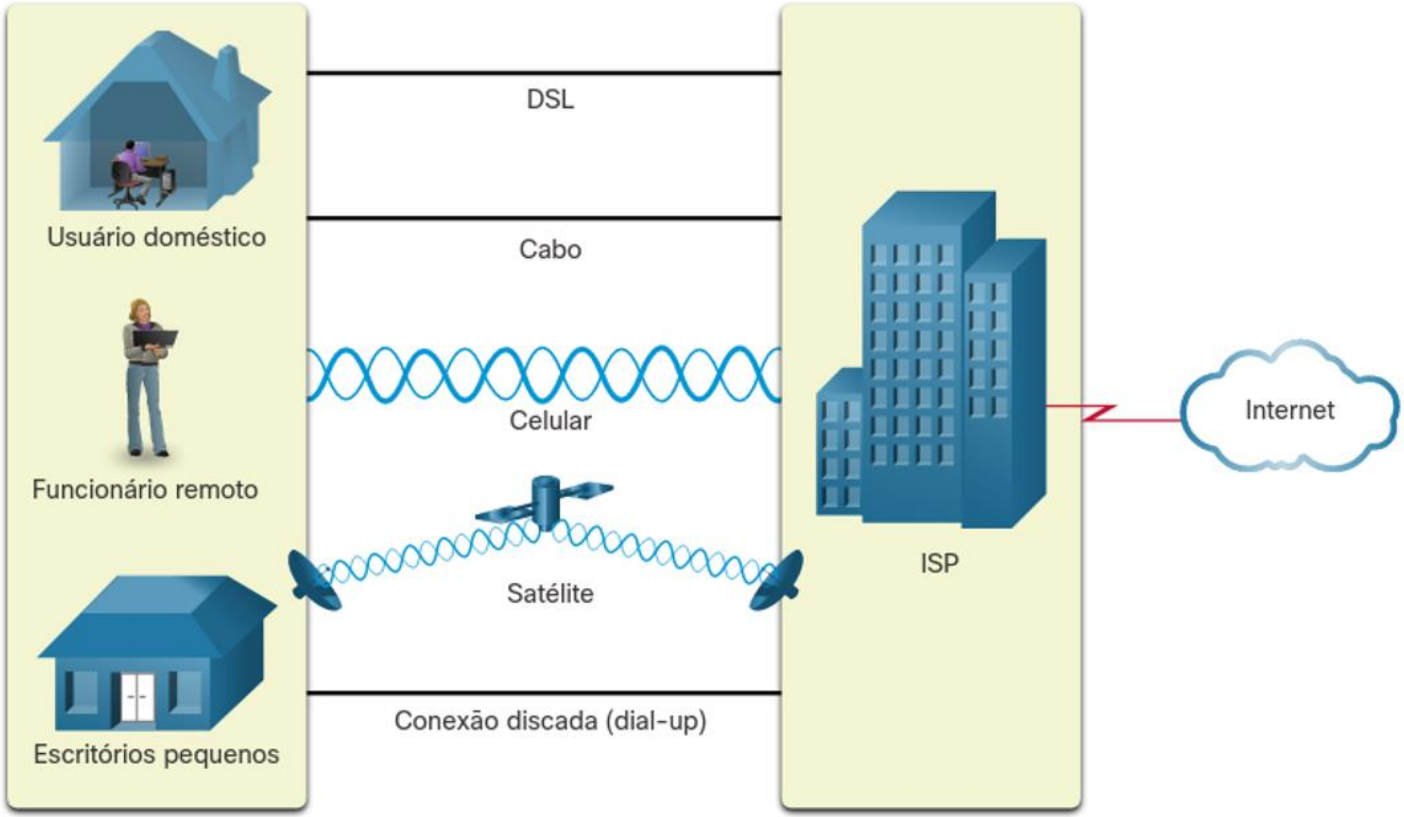
FORMAS DE CONEXÃO COM A INTERNET

TECNOLOGIAS DE ACESSO

Diferentemente de alguns anos atrás, hoje há diversas formas de se conectar a rede mundial, com cada vez mais qualidade e a um custo cada vez mais baixo.

Usuários domésticos e pequenos escritórios geralmente contratam um ISP (*Internet Service Provider*) para a conexão, chamados de **provedores de acesso**.

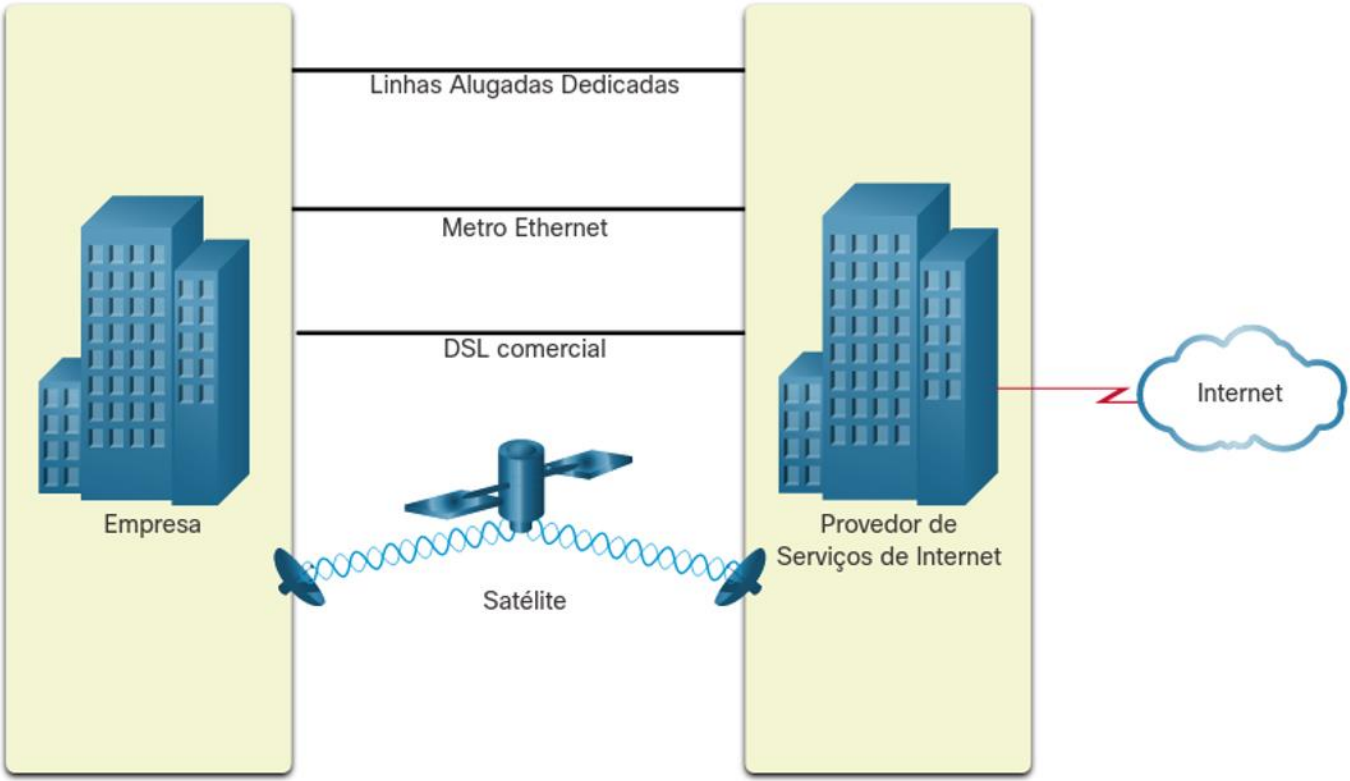
Já as organizações conectam-se a um ISP de nível empresarial, com maiores velocidades para dar suporte aos serviços comerciais como telefonia, videoconferência e armazenamento em nuvem. Os próprios provedores de acesso precisam de conexão, recorrendo a organizações maiores chamadas de **provedores de trânsito**.


DSL
Cabo
Celular
Satélite
Conexão discada (dial-up)
Usuário doméstico
Funcionário remoto
Escritórios pequenos
ISP
Internet

ACESSO DOMÉSTICO

As principais tecnologias de acesso doméstico são:

- **DSL**, oferecendo altas velocidades e disponibilidade, através da linha telefônica, geralmente utilizando assimetria (ADSL) no download e upload. Está caindo em desuso.
- **Cabo**, inicialmente operada por empresas de TV a cabo, onde o sinal de Internet é transmitido no mesmo cabo da TV. Vem sendo substituído pela fibra óptica (EPON/GPON).
- **Celular**, utiliza a rede celular para conexão e transmissão dos dados e tem alcance onde houver cobertura de sinal. Porém é limitada aos recursos do telefone e da torre.
- **Satélite**, utiliza um satélite na órbita baixa da Terra e uma antena na superfície. Tem alta disponibilidade, custo elevado e exige uma linha de visão sem obstáculos.
- **Dial-up (discada)**, opção de baixo custo, com uma linha telefônica e um modem. Tem baixíssimo desempenho.


Linhas Alugadas Dedicadas
Metro Ethernet
DSL comercial
Internet
Empresa
Provedor de
Serviços de Internet
Satélite

ACESSO EMPRESARIAL

As principais tecnologias de acesso a nível empresarial são:

- **Linhas Alugadas**, também chamada de LAN-TO-LAN ou L2L, são circuitos reservados dentro da rede do ISP para conexão entre pontos distantes, criando uma rede privada de dados.
- **Metro Ethernet**, é uma grande estrutura de rede metropolitana operada por ISP para conectar assinantes e empresas. Iremos entender a tecnologia Ethernet mais adiante.
- **DSL Comercial**, utiliza o mesmo princípio da conexão DSL doméstica, porém com simetria entre as velocidades.
- **Satélite**, também disponível como opção para empresas.

REDES CONFIÁVEIS

AXIOMAS DA CONFIABILIDADE

Com uma rede intensamente acessada como hoje, é fundamental que se tenha o mínimo de confiabilidade e segurança para um funcionamento eficiente.

Tudo isso funcionando com um gama de aplicativos e serviços, sobre muitos diferentes de tipos de cabos e dispositivos, num ambiente rico em mídia e interação.

Hoje há quatro características básicas alinhadas para atender as expectativas dos usuários:

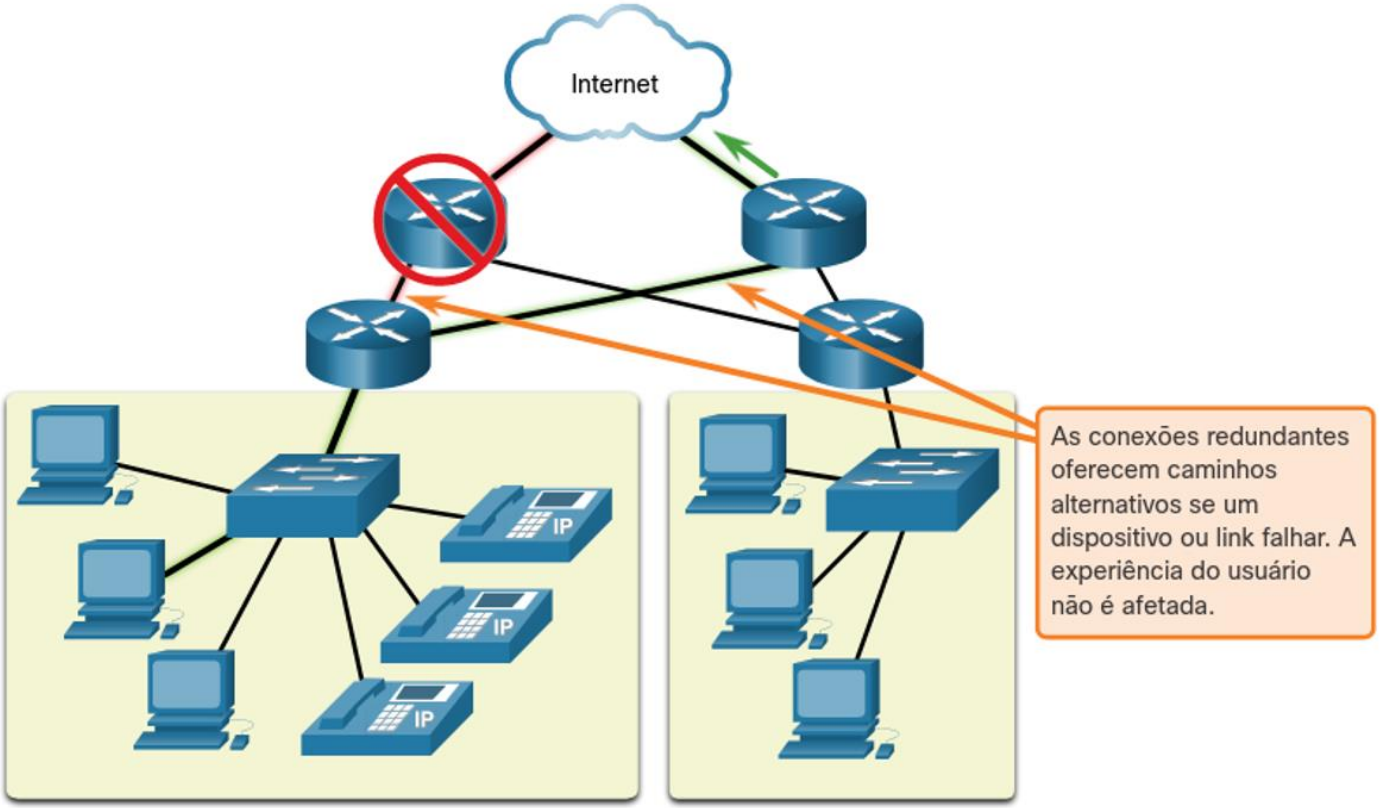
- **Tolerância a falhas;**
- **Escalabilidade;**
- **Qualidade de serviço (QoS);**
- **Segurança.**

TOLERÂNCIA A FALHAS

Quando há uma falha, a rede deve ser capaz de limitar o número de dispositivos afetados e permitir uma rápida recuperação.

A palavra chave para a tolerância a falhas é **redundância**, quando há vários caminhos entre a origem e o destino.

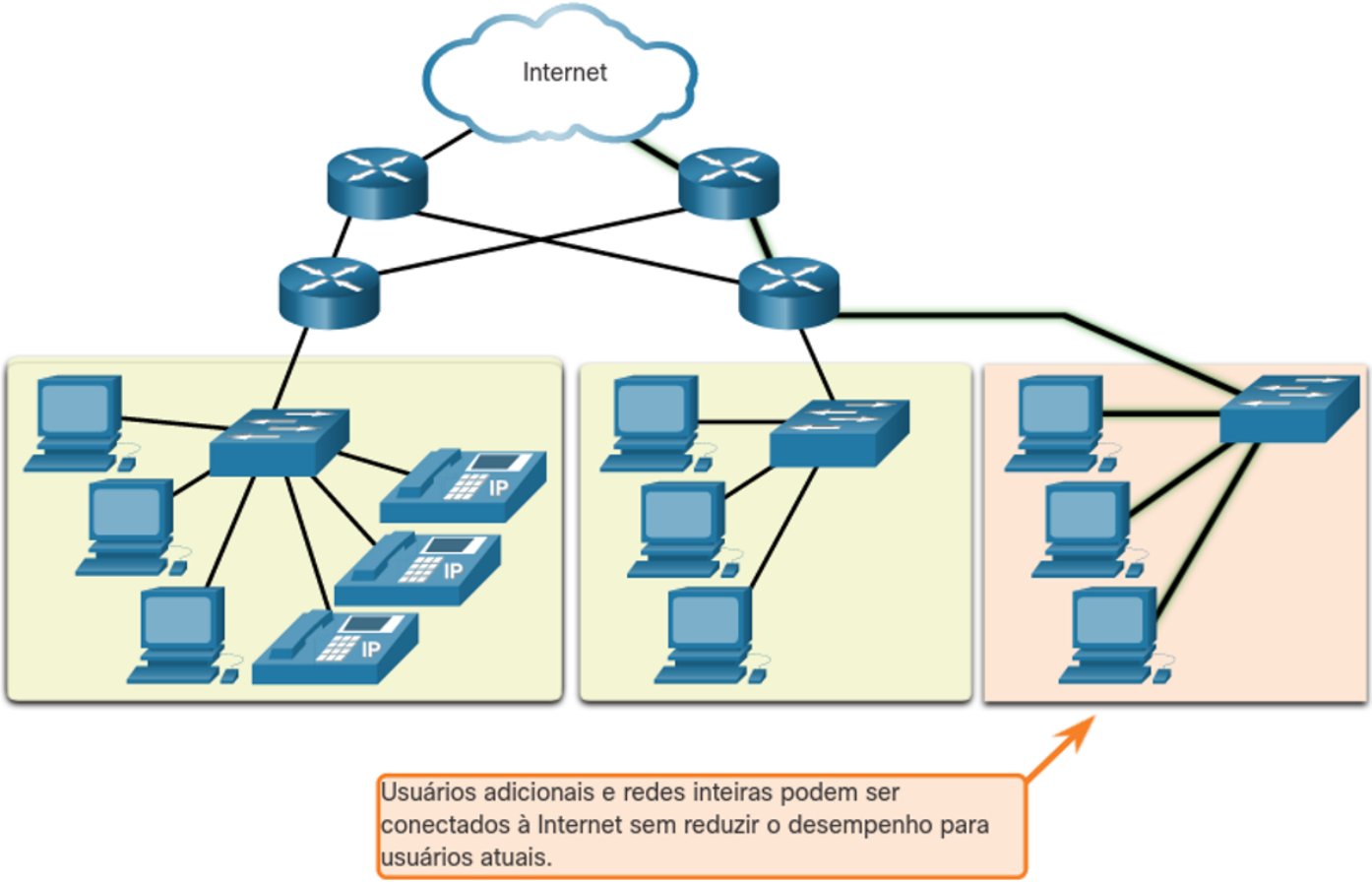
Outra palavra bem difundida é a **transparência**, que tem um conceito contrário ao que parece. A falha e a recuperação devem ser transparentes ao usuário, isto é, **despercebidas**.


Internet
IP
IP
IP
As conexões redundantes oferecem caminhos alternativos se um dispositivo ou link falhar. A experiência do usuário não é afetada.

ESCALABILIDADE

A rede também deve ser capaz de acomodar crescimento de usuários e serviços, sem degradar o desempenho.

Uma rede com **planejamento** e uso de padrões bem aceitos de hardware e software facilita o crescimento, sem que seja necessário criar um novo conjunto de regras para operação.

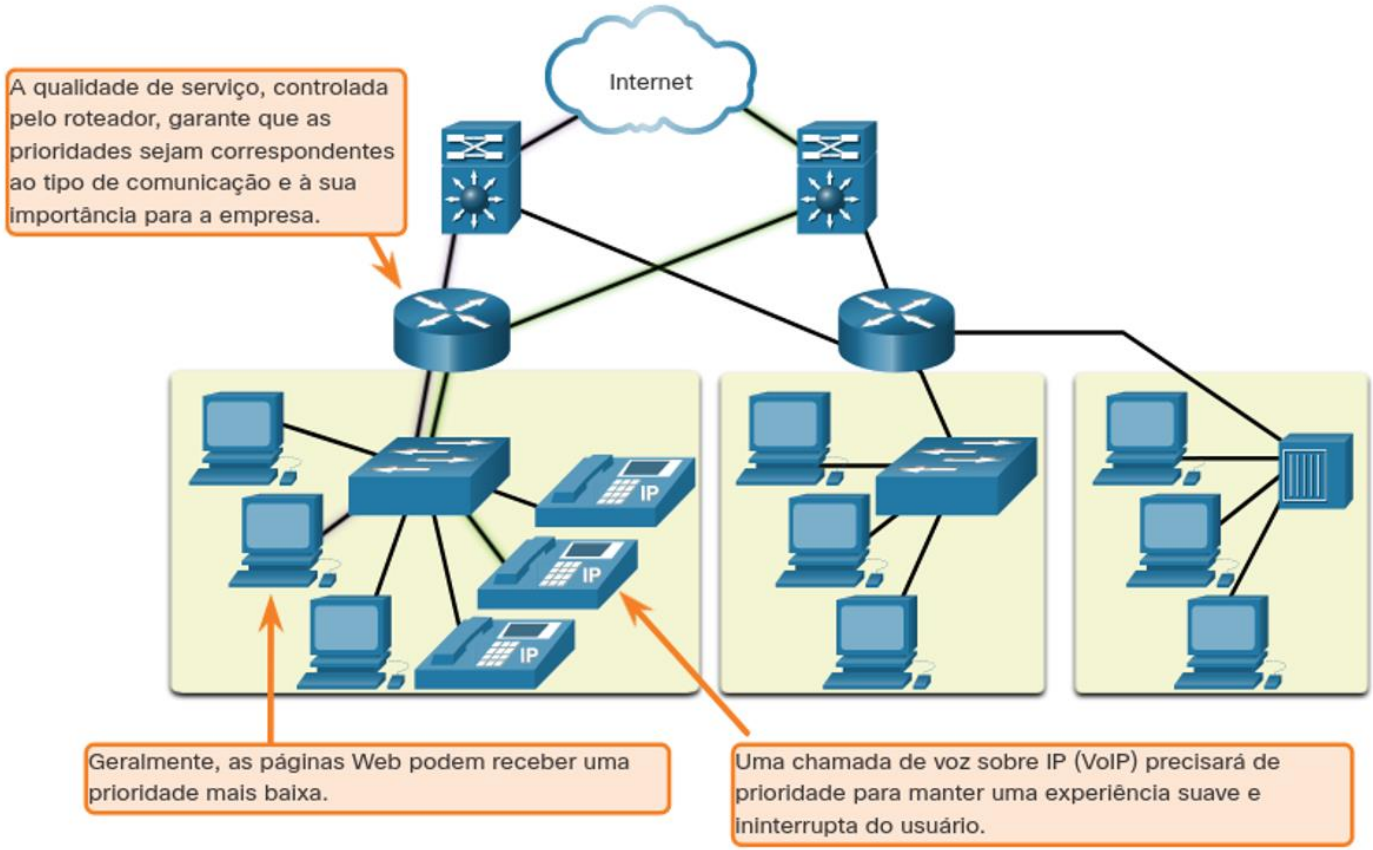

Internet
IP
IP
IP
Usuários adicionais e redes inteiras podem ser conectados à Internet sem reduzir o desempenho para usuários atuais.

QUALIDADE DO SERVIÇO

Dentre os serviços da rede, a transmissão de voz e vídeo de forma ao vivo (*streaming*) criam expectativas mais altas em relação a qualidade entregue.

Um congestionamento na rede, isto é, quando a demanda por banda excede a quantidade disponível, deve ser gerenciado de forma a **priorizar conteúdo**.

Se um usuário solicita uma página Web, enquanto outro está em um videoconferência, o roteador deve ter uma política de QoS aplicada para gerenciar o fluxo do tráfego por priorização.


A qualidade de serviço, controlada pelo roteador, garante que as prioridades sejam correspondentes ao tipo de comunicação e à sua importância para a empresa.
Internet
IP
IP
IP
Geralmente, as páginas Web podem receber uma prioridade mais baixa.
Uma chamada de voz sobre IP (VoIP) precisará de prioridade para manter uma experiência suave e ininterrupta do usuário.

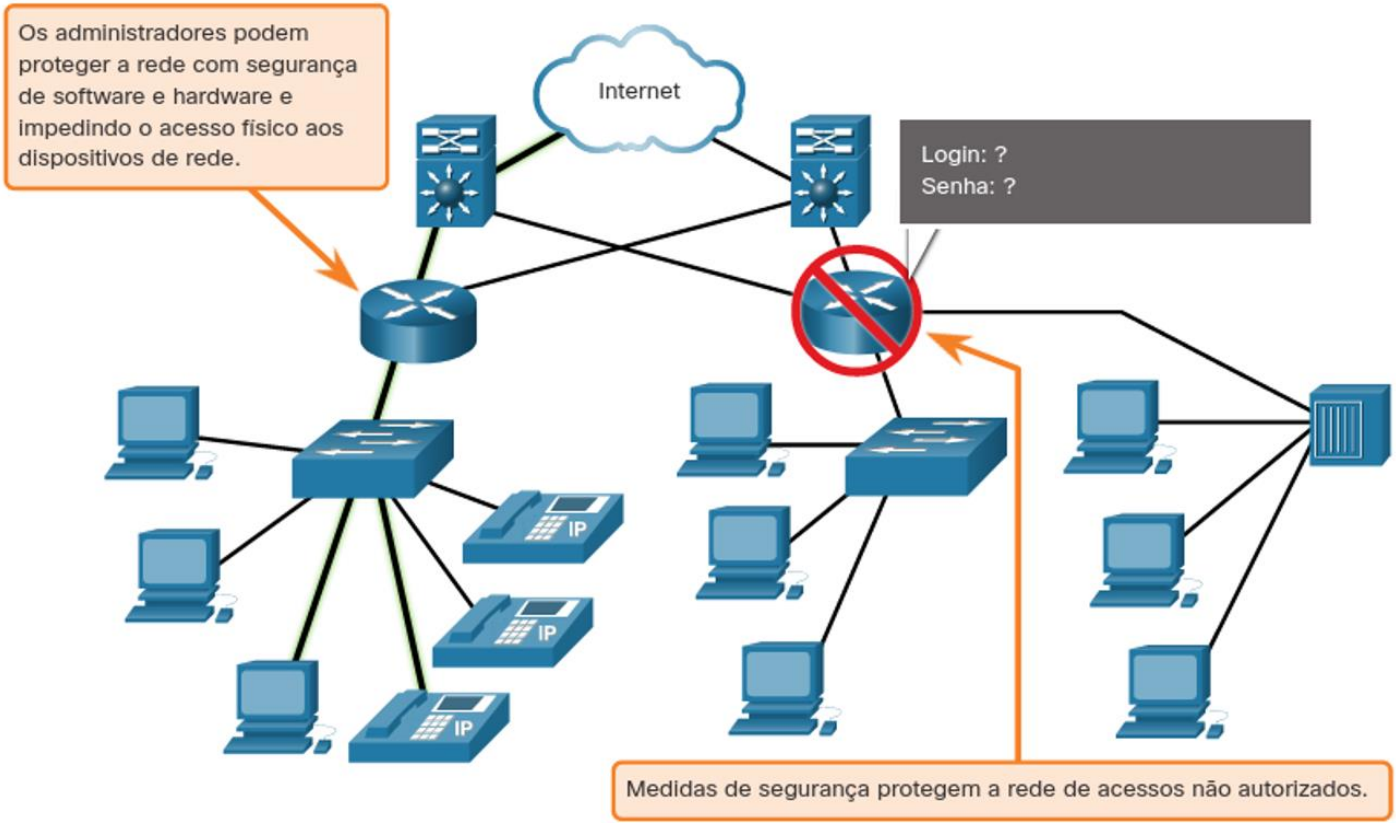
SEGURANÇA DA REDE

Uma rede sempre irá conter dados críticos, seja de caráter pessoal ou comercial. Duas vertentes de segurança devem ser observadas, a **segurança da infraestrutura** e a **segurança da informação**.

Na infraestrutura protegemos fisicamente os equipamentos e na informação, protegemos o acesso não autorizado com técnicas de ***Triple A*** *(authentication, authorization, accounting).*

Outro pilar da segurança é conceito **CID**:

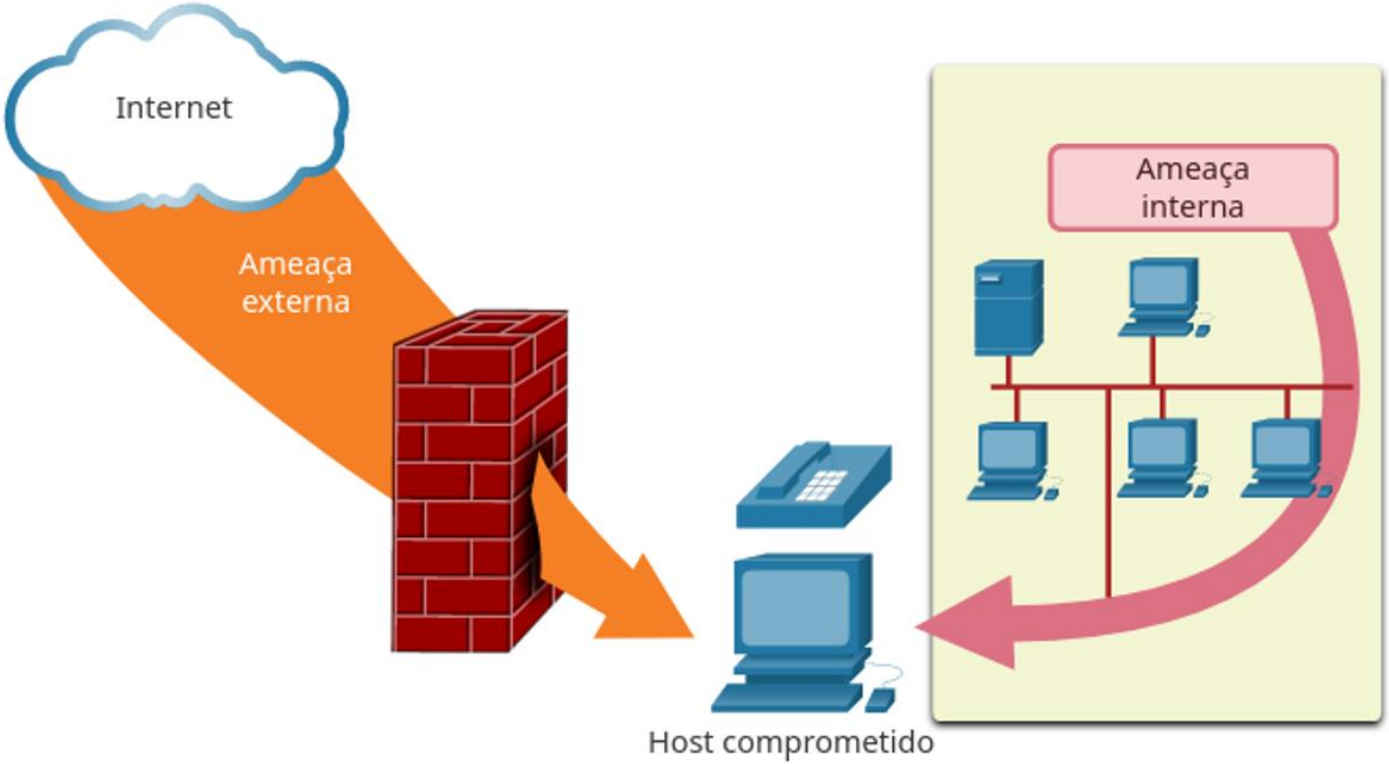
- **Confidencialidade**: a informação não é "vazada";
- **Integridade**: a informação é verdadeira;
- **Disponibilidade**: a informação pode ser oportunamente acessada.


Os administradores podem proteger a rede com segurança de software e hardware e impedindo o acesso físico aos dispositivos de rede.
Internet
Login: ?
Senha: ?
IP
IP
IP
Medidas de segurança protegem a rede de acessos não autorizados.

E AS AMEAÇAS?

A segurança da rede é integrante do estudo de redes, seja qual for o seu tamanho, deve proteger os dados e oferecer qualidade de serviço. A segurança sempre será prioridade máxima, pois muitas ameaças, internas e externas são presentes.

- **Vírus, Worms e Cavalos de Tróia**: softwares e códigos maliciosos em execução no dispositivo do usuário;
- **Spyware e adware**: softwares instalados no usuário e que coletam informações secretamente.
- **Ataques de dia zero**: ocorrem no primeiro dia em que uma vulnerabilidade se torna conhecida.
- **Negação de Serviço:** atrasam ou travam recursos na rede, tornando-os indisponíveis.
- **Homem no meio:** intercepta dados e roubam informações privadas da rede.
- **Engenharia social:** roubo de credenciais de login com base na confiança humana.


Internet
Ameaça externa
Ameaça interna
Host comprometido

QUAIS SOLUÇÕES?

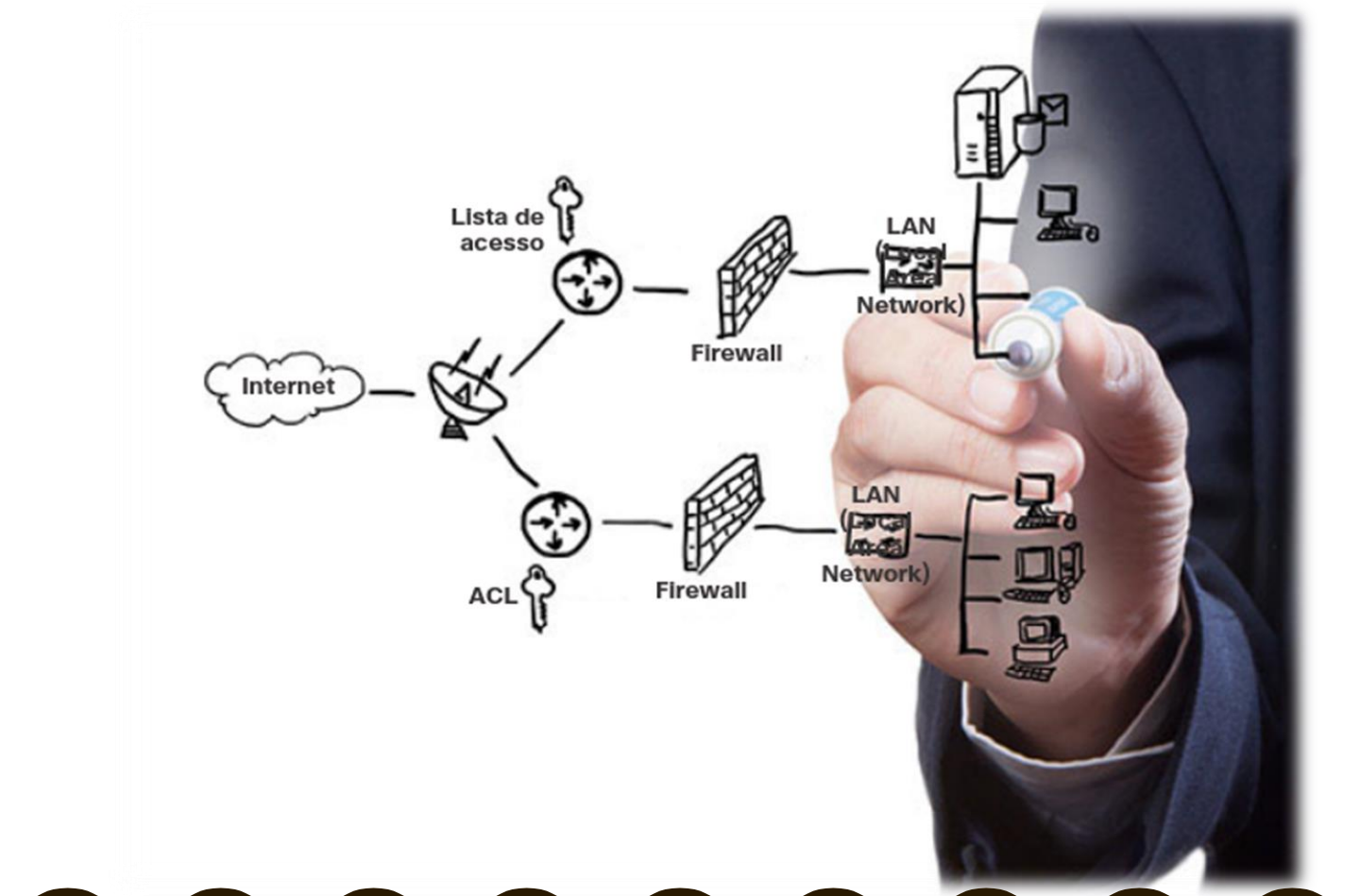
A solução para ameaças nunca é única, mas sim um conjunto delas, por isso a segurança deve ser implementada em várias camadas; se uma falhar, outra pode agir.

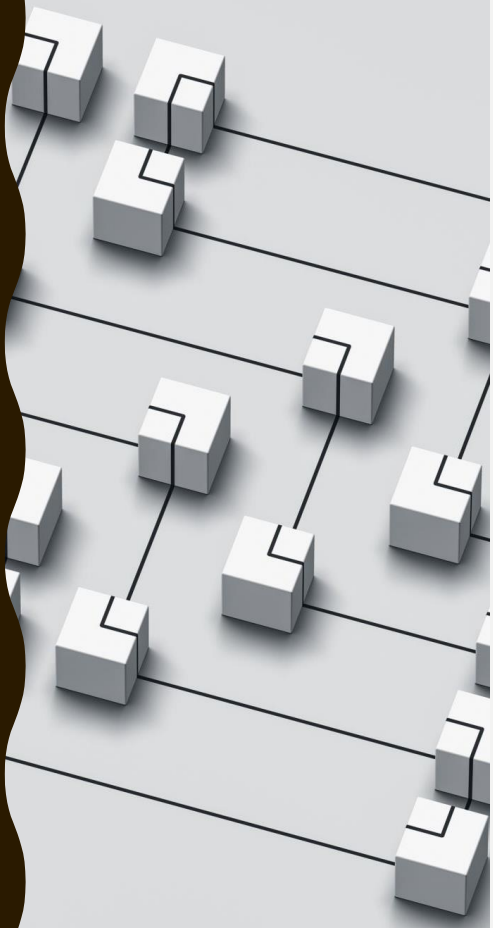
A segurança a nível doméstico pode ser:

- **Antivírus e Antispyware**: aplicativos pagos, gratuitos ou nativos que protegem contra infecção;
- **Firewall**: impede acesso a recursos de dentro ou fora da rede. Pode ser pago, gratuito ou nativo.

Já a nível corporativo há uma maior complexidade e opções:

- **Firewalls dedicados**: filtram grande quantidade de tráfego com mais detalhes.
- **ACL:** filtram mais tráfego ainda com base na origem e destino.
- **IDS/IPS:** detectam acesso não autorizados e bloqueia a conexão.
- **VPN:** acesso seguro a recursos, estando fora da rede.


Lista de acesso
LAN
Network)
Internet
Firewall
LAN
Network)
ACL
Firewall



LABORATÓRIO

Conhecer a estrutura de comandos dos principais equipamentos.

- Cisco
- Huawei
- Mikrotik

COMANDOS BÁSICOS

MÉTODOS DE ACESSO

Os equipamentos podem ser acessados remota ou localmente para configuração e manutenção, dependendo da necessidade. Os principais métodos de acesso são:

- **Console**: porta física especial em alguns equipamentos, utilizada em acessos locais, principalmente na **primeira configuração**. Utiliza um cabo específico de cada fabricante, sendo considerado um **acesso out-of-band**.

- **SSH**: serviço de rede para **acesso remoto in-band**, isto é, por dentro da rede, através de uma porta ou interface configurada. É o método mais recomendado para gerenciamento, por se **criptografado**.

- **Telnet**: opera da mesma forma que o SSH, porém **não criptografa** a conexão, ou seja, todos os comandos, senhas e autenticação são em texto plano.

MODOS DE COMANDOS

Após acessados, a maioria dos equipamentos, **exceto Mikotik**, permite dois modos de digitação dos comandos.

- **Visualização**: oferece poucos comandos para visualização de estatísticas, status, entre outros. Não permite nenhuma modificação no equipamento, variando de representação.
  - Na plataforma Cisco é chamado também de "**view-only ou exec usuário**" e aparece com o símbolo **>**
  - Na plataforma Huawei é chamado também de "**user-view**" e aparece com o símbolo **< >**

- **Configuração**: é o modo onde digitamos a maioria dos comandos de configuração, alteração e manutenção do equipamento. Também varia de representação.
  - Na plataforma Cisco é chamado também de "**exec privilegiado**" e aparece com o símbolo **#**
  - Na plataforma Huawei é chamado também de "**system-view**" e aparece com o símbolo **[ ]**

MODOS DE COMANDOS

A navegação entre os modos de visualização e configuração também varia para cada fabricante.

- **Cisco**: o modo padrão é visualização. Para acessar o modo configuração, digite o comando **enable**. Para retornar, use o comando **disable** ou as teclas **Ctrl + Z**.

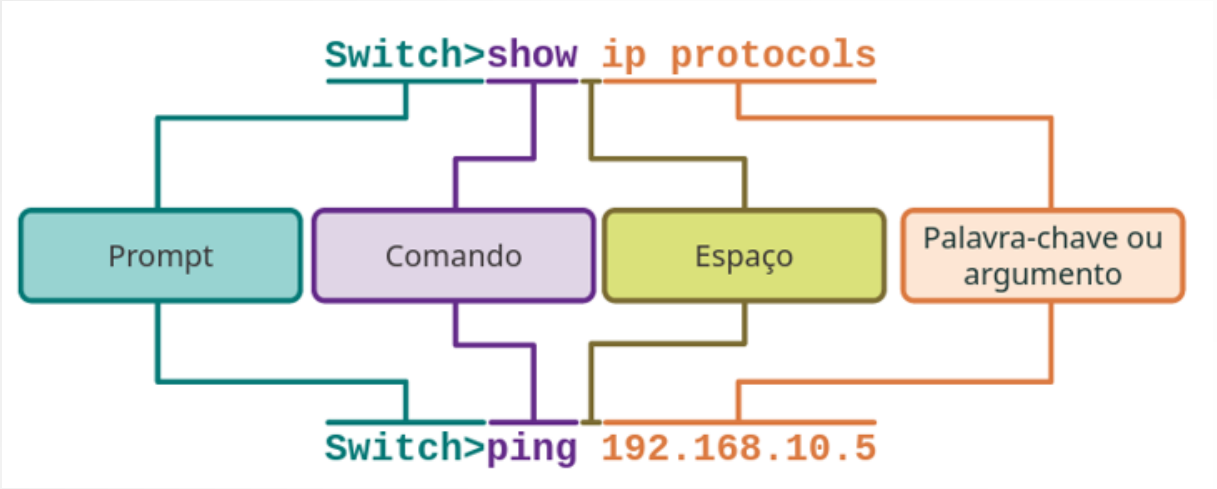
```
Switch>enable
Switch#
```

- **Huawei**: o modo padrão também é visualização. Para acessar o modo configuração, digite o comando **system-view**. Para retornar, use o comando **quit** ou as teclas **Ctrl + Z**.

```
<Huawei-Router> system-view
Enter system view, return user view with Ctrl+Z.
[Huawei-Router]
```

ESTRUTRA DE COMANDOS

O operador/administrador da rede deve conhecer a estrutura básica de comandos para utilizar o terminal. Para as plataformas Cisco e Huawei, a estrutura de comandos possui certa similaridade.

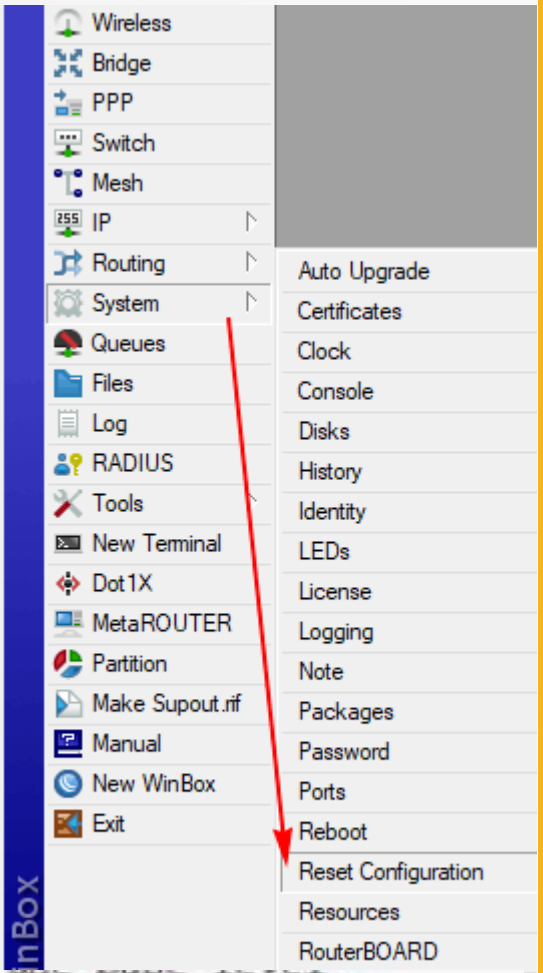


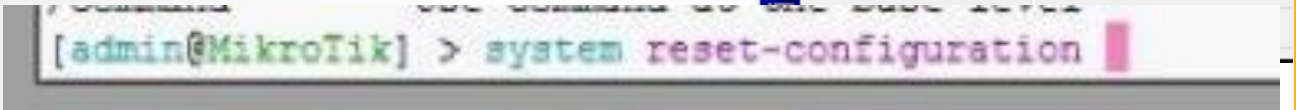
A palavra-chave é pré-definida, já o argumento é um valor variável.

ESTRUTRA DE COMANDOS

Nos equipamentos Mikrotik, a estrutura é semelhante ao terminal do Linux, sendo o diretório **/** como raiz, seguido pelas palavras-chaves de acordo com o menu do sistema operacional.

Dentro disso, são oferecidos opcionalmente os parâmetros de contexto e comandos baseados no conceito **CRUD/ABCD/LEIA/VEIA/BREAD**.





AJUDA DE CONTEXTO E AUTO-COMPLETE

Nas plataformas Cisco e Huawei, é possível acionar um comando de ajuda, que exibirá as possibilidades de ação, de acordo com o contexto atual do terminal. O comando é a **tecla ?**

Também há um auto-complete em ambas as plataformas, para auxílio na digitação de comandos no contexto atual e também visualização das possibilidades. Para isso, utiliza-se a **tecla TAB**

```
[SW_SHOWROOM]display ?
  aaa                       AAA
  aaa-quiet                 AAA quiet
  access-author             Access user author
  access-context            Access user context
  access-user               User access
  accounting-scheme         Accounting scheme
  acl                       Specify ACL configuration information
  alarm                     Alarm
  als                       Set automatic laser shutdown
  anti-attack               Specify anti-attack configurations
  arp                       Display ARP entries
  arp-limit                 Display the number of limitation
  arp-miss                  ARP Miss
  as                        Access switch
  assistant                 Assistant
  associate-user            Associate user
  authentication            Authentication unified-mode
  authentication-profile    Authentication profile
  authentication-scheme     Authentication scheme
  authorization-scheme      Display AAA authorization scheme
```

```
Switch#?
Exec commands:
  clear        Reset functions
  clock        Manage the system clock
  configure    Enter configuration mode
  connect      Open a terminal connection
  copy         Copy from one file to another
  debug        Debugging functions (see also 'undebug')
  delete       Delete a file
  dir          List files on a filesystem
  disable      Turn off privileged commands
  disconnect   Disconnect an existing network connection
  enable       Turn on privileged commands
  erase        Erase a filesystem
  exit         Exit from the EXEC
  logout       Exit from the EXEC
  more         Display the contents of a file
  no           Disable debugging informations
  ping         Send echo messages
  reload       Halt and perform a cold restart
  resume       Resume an active network connection
  setup        Run the SETUP command facility
  show         Show running system information
```

LABORATÓRIO

Comandos e configuração básica de equipamentos.

- Cisco
- Huawei
- Mikrotik

NOMES DE DISPOSITIVOS

É importante nomear os dispositivos para identificação durante um acesso remoto, evitando equívocos de configuração. É boa prática evitar espaços e caracteres especiais. O comando é feito no modo de configuração.

Nas plataformas CISCO, é adotado o nome padrão de “Switch” ou “Router”, dependendo do equipamento.

- Entre no modo de configuração com **enable**
- Entre na configuração global com **configure terminal**
- Nomeie com **hostname** seguido do nome escolhido.

```
Switch# configure terminal
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#
```

NOMES DE DISPOSITIVOS

Nas plataformas Huawei, é adotado sempre o nome “Huawei” como padrão.

- Entre no modo de configuração com **system-view**
- Nomeie com **sysname** seguido do nome escolhido.

```
[Huawei]sysname Huawei-Training

[Huawei-Training]
```

Nos equipamentos Mikrotik, é adotado sempre o nome “Mikrotik” como padrão.

- Entre no menu **/system identity**
- Nomeie com **set name=** seguido do nome escolhido.

```
[admin@RouterOS] > /system identity set name=ROTEADOR01
[admin@ROTEADOR01] >
```

CONFIGURAR SENHAS

É necessário proteger todos os modos de acesso (console visualização/configuração e Telnet/SSH), ao equipamento com senhas. As configurações são feitas no modo de configuração. Para proteger o console, siga abaixo.

- Entre no modo de configuração com **configure terminal**
- Entre na configuração do console com **line console 0**.
- Configure uma senha com **password**, seguido pela senha.
- Ative a configuração com o comando **login.**

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
```

CONFIGURAR SENHAS

Outro ponto de suma importância é proteger o modo de configuração, pois este dá acesso completo ao equipamento.

- Entre no modo de configuração com **configure terminal**
- Configure uma senha com **enable secret**, seguido pela senha.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# enable secret class
```

Para acesso SSH ou Telnet, utilizamos as linhas (line) VTY (Virtual Teletype), que permite até 16 conexões simultâneas. A configuração é semelhante a linha de console.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# 1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
```

CONFIGURAR SENHAS

Em equipamentos Huawei, as linhas são chamadas de user interface. Além disso, há algumas opções de autenticação. Vamos proteger o console da seguinte forma.

- Entre no modo de configuração com **system-view**
- Entre na configuração do console com **user-interface console 0**.
- Vamos escolher o modo de autenticação com senha (pode ser de outras formas) digitando **authentication-mode password**.
- Insira uma senha, criptografada com **set authentication password cipher** seguido pela senha.

```
<Quidway> system-view
[Quidway] user-interface console 0
[Quidway-ui-console0] authentication-mode password
[Quidway-ui-console0] set authentication password cipher Example@123
```

O modo de configuração é protegido por privilégios de usuários, iremos aprender mais adiante.

CONFIGURAR SENHAS

Para proteger as interfaces VTY, de acesso SSH ou Telnet, a configuração é bastante semelhante. O número máximo de conexões simultâneas por padrão é 5.

- Entre no modo de configuração com **system-view**
- Entre na configuração do console com **user-interface vty 0 4**.
- Vamos escolher o modo de autenticação com senha (pode ser de outras formas) digitando **authentication-mode password**.
- Insira uma senha, criptografada com **set authentication password cipher** seguido pela senha.

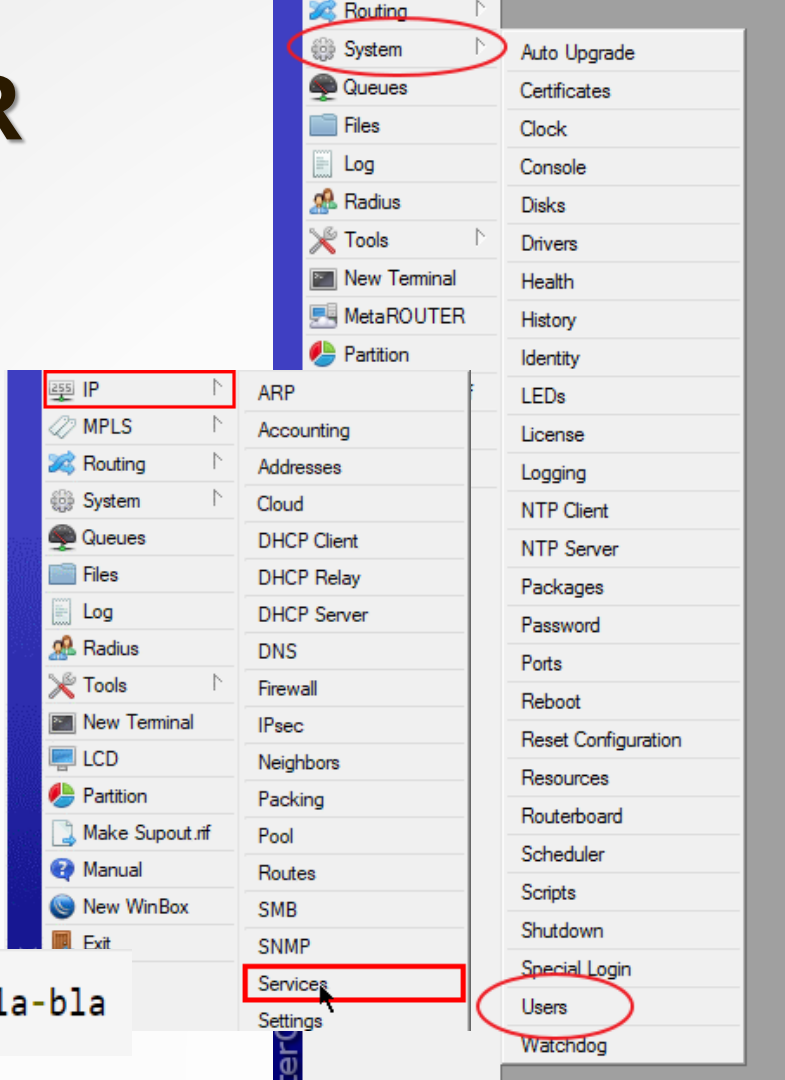
```
login as: netadmin
netadmin@192.168.95.145's password:

Info: The max number of VTY users is 5, and the number
      of current VTY users on line is 1.
      The current login time is 2017-06-02 21:13:19.
<Huawei>
```

Outra forma de autenticação é por login e senha, com os usuários locais do equipamento. Iremos aprender mais adiante como criar usuários.

CONFIGURAR SENHAS

Em equipamentos Mikrotik, as senhas são controladas separadamente por serviços e também pelo próprio acesso do usuário, dependendo de seu nível de permissão.
Lembrando que por padrão, o usuário **admin** não tem senha.




```
/user set admin password=bla-bla
```

BANNERS

Os banners são avisos em texto que geralmente aparecem ao entrar no equipamento. Embora não sejam obrigatórios, há um precedente legal para utilização de banners como aviso de acesso restrito, prevenindo para consequências em caso de violação. Em equipamentos Cisco, vamos configurar o motd (*message of the day*).

- Entre no modo de configuração com **configure terminal**
- Configure o banner com **banner motd** seguido da mensagem entre cerquilhas **#**.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# banner motd #a mensagem do dia#
```

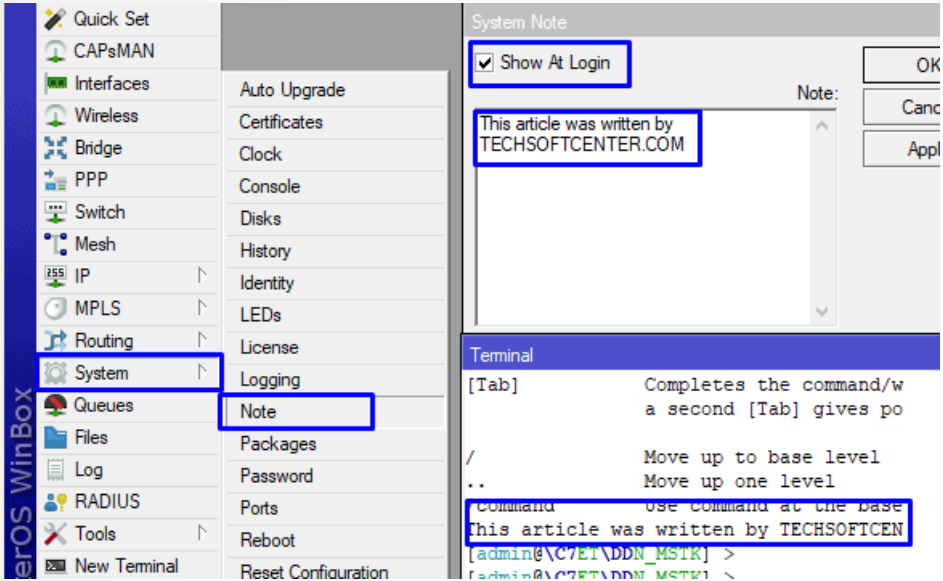
- A configuração para equipamentos Huawei é exatamente a mesma, apenas com a diferença de que o modo de configuração é acessado com **system-view.**

BANNERS

Em equipamentos Mikrotik, podemos também configurar os banners através do caminho **System - Note**, utilizando **set** ou **edit** com a mesma finalidade de Huawei e Cisco. Observe.

```
/ system note
set show-at-login=yes note="THIS IS NOT A PUBLIC ACCESS DEVICE!"
```

```
[admin@RB493G] /system note> edit note
```

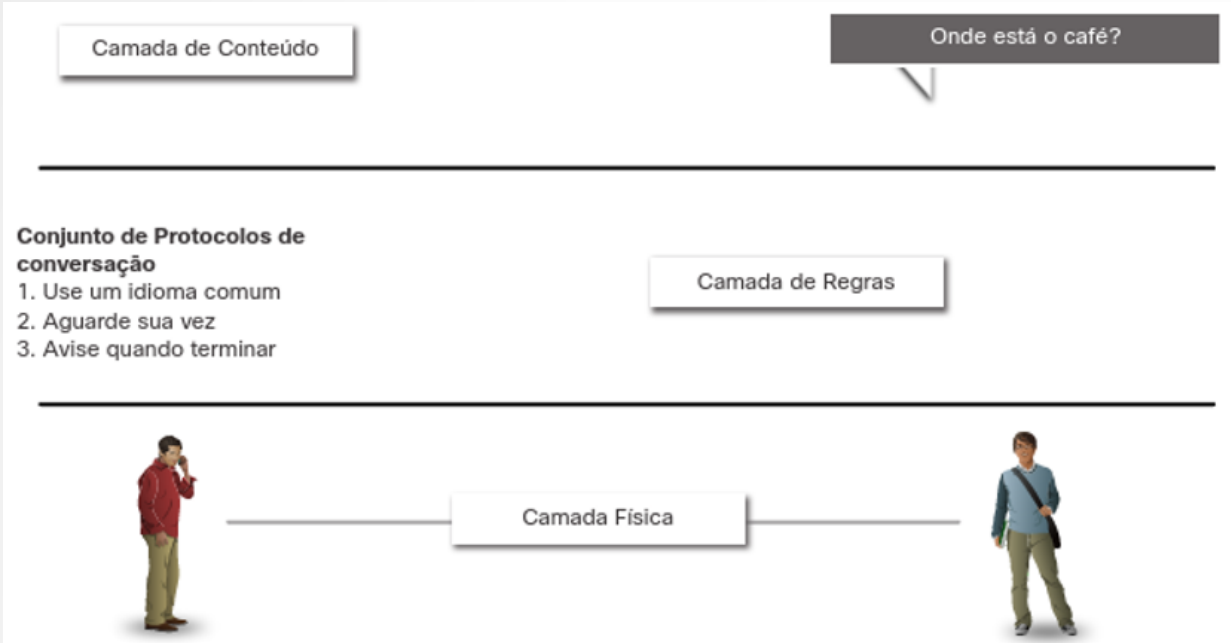


HUAWEI	CISCO
ping	ping
tracert	traceroute
display	show
display interface	show interfaces
display routing-table	Show ip route
Display ip interface	Show ip interface
Display version	Show version
Display bgp routing-table	Show ip bgp
Display clock	Show clock
Display port-mapping	Show port
dir flash: (on user view mode)	Show flash
Display logbuffer	Show logging
Display snmp-agent statistics	Show snmp
Display fr pvc-info	Show frame-relay pvc
Display users	Show users
Display lldp neighbor	Show cdp neigh
Display arp	Show arp
Display mac-address	Show mac-address
System-view	Conf t

PROTOCOLOS E PADRÕES

PROTOCOLOS

Os protocolos são como um conjunto de regras definindo e formatando o que deve ocorrer nas mensagens entre dispositivos. São descritos em **camadas ou pilha**, de modo que cada camada, das inferiores para as superiores, tem suas regras e seu trabalho bem definido. Pode ser comparado a um idioma.



PROTOCOLOS

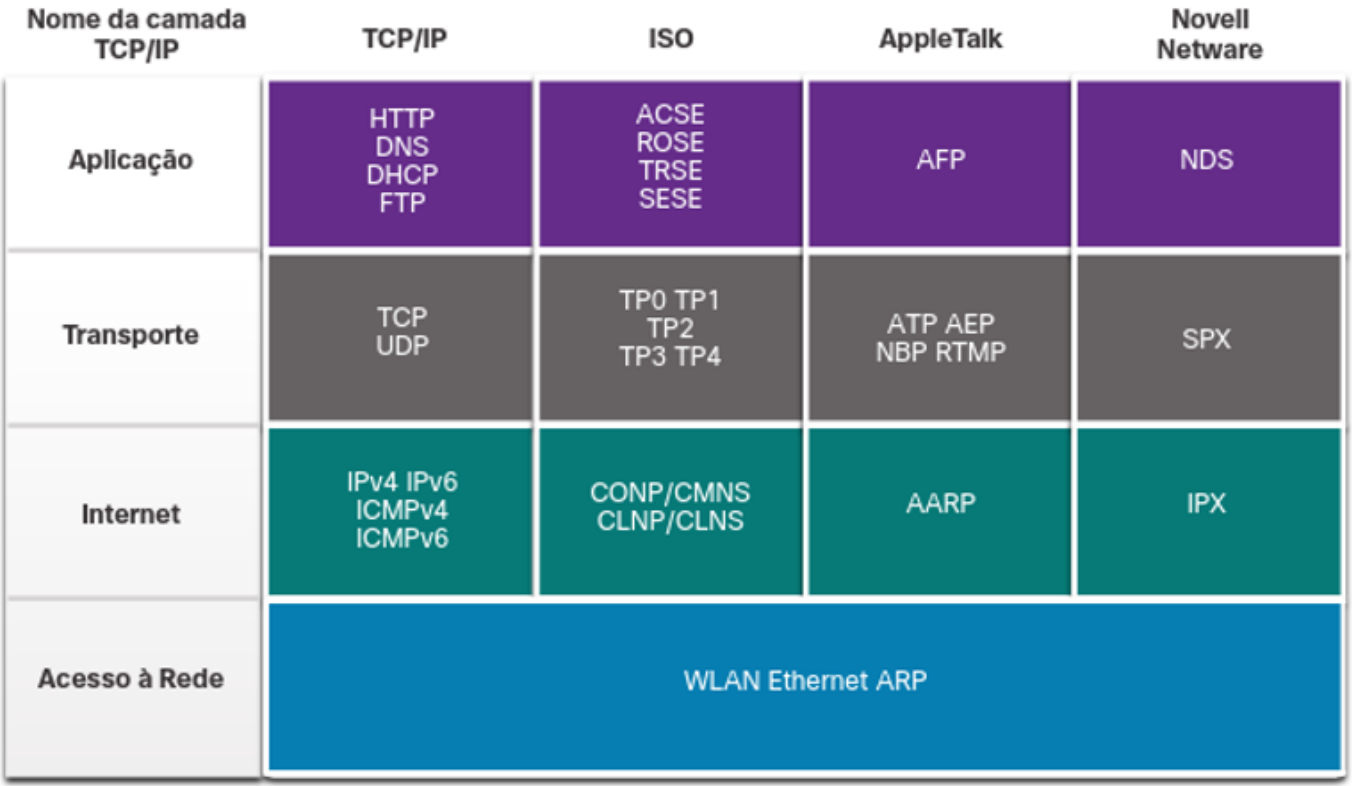
Vários foram os conjuntos de protocolos propostos ao longo da história, restando apenas um dominante.

- **TCP/IP**: é o mais comum e relevante usado atualmente. É mantido pela Internet Engineering Task Force (IETF).

- **OSI**: desenvolvida pela ISO e pela União Internacional de Telecomunicações em 1977, inclui um **modelo com 7 camadas**. Os protocolos OSI foram amplamente substituídos pelo TCP/IP.

- **AppleTalk**: lançado pela Apple Inc em 1985 para uso em seus dispositivos. Em 1995, a Apple substituiu-o pelo TCP/IP.

- **Novell NetWare**: lançado pela Novell Inc em 1983, juntamente com seu sistema operacional. Em 1995, a Novell também substituiu-o pelo TCP/IP.

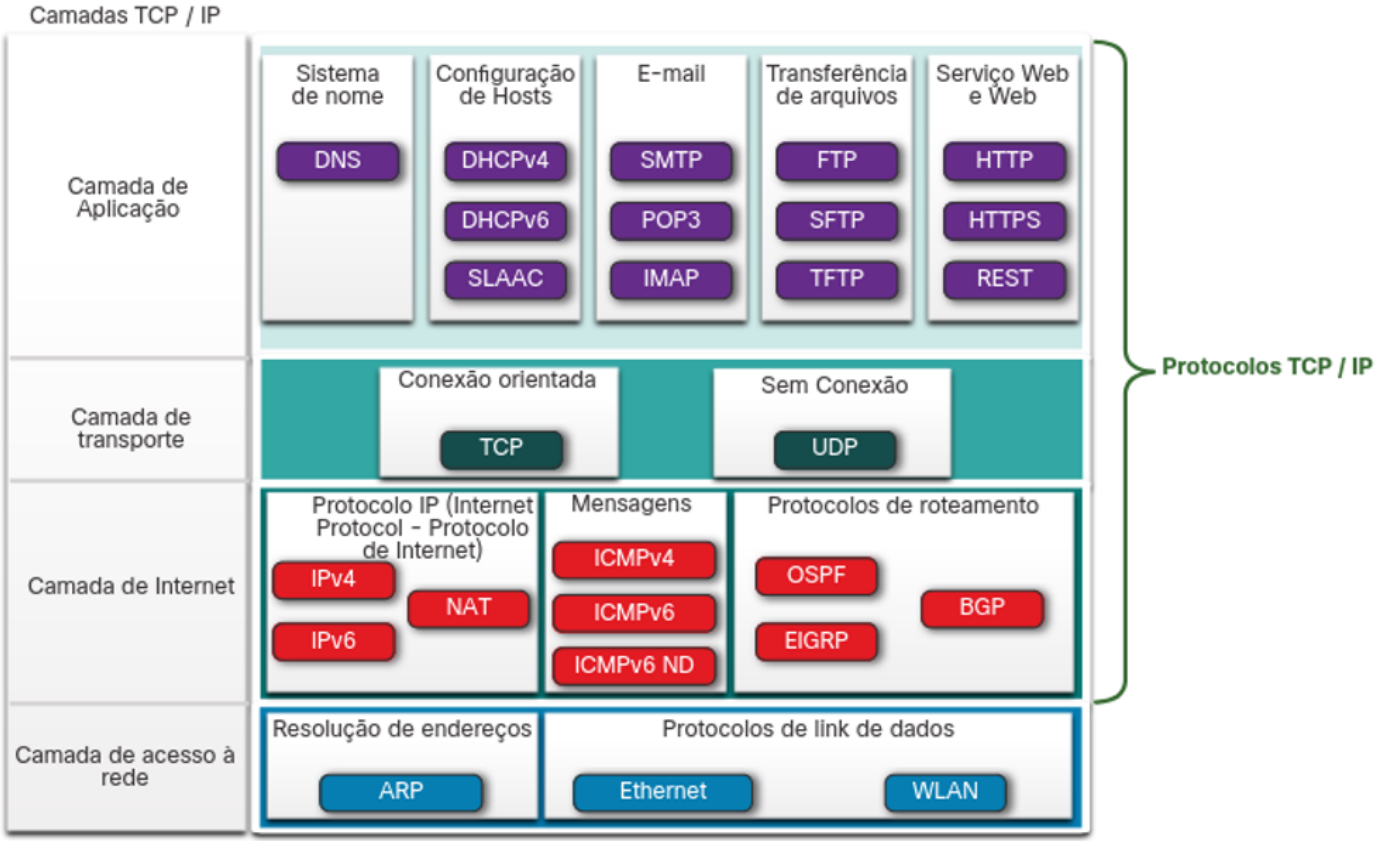

Nome da camada TCP/IP
TCP/IP
ISO
AppleTalk
Novell Netware
Aplicação
HTTP DNS DHCP FTP
ACSE ROSE TRSE SESE
AFP
NDS
Transporte
TCP UDP
TP0 TP1 TP2 TP3 TP4
ATP AEP NBP RTMP
SPX
Internet
IPv4 IPv6 ICMPv4 ICMPv6
CONP/CMNS CLNP/CLNS
AARP
IPX
Acesso à Rede
WLAN Ethernet ARP

PROTOCOLOS TCP/IP

Inclui hoje muitos protocolos e continua a evoluir, oferecendo suporte a novos serviços. É o conjunto utilizado na Internet e nas redes de hoje. Possui dois aspectos importantes.

- **Padrão aberto**: disponível gratuitamente e pode ser usado por qualquer fabricante em hardwares e softwares.

- **Base em padrões**: foi endossado e aprovado por empresas de padrões, significando que produtos de diferentes fabricantes conseguirão se comunicar com o conjunto sem problemas.


Camadas TCP / IP
Camada de Aplicação
Sistema de nome
DNS
Configuração de Hosts
DHCPv4
DHCPv6
SLAAC
E-mail
SMTP
POP3
IMAP
Transferência de arquivos
FTP
SFTP
TFTP
Serviço Web e Web
HTTP
HTTPS
REST
Camada de transporte
Conexão orientada
TCP
Sem Conexão
UDP
Camada de Internet
Protocolo IP (Internet Protocol - Protocolo de Internet)
IPv4
IPv6
NAT
Mensagens
ICMPv4
ICMPv6
ICMPv6 ND
Protocolos de roteamento
OSPF
EIGRP
BGP
Camada de acesso à rede
Resolução de endereços
ARP
Protocolos de link de dados
Ethernet
WLAN
Protocolos TCP / IP

CAMADA DE APLICAÇÃO

- **DNS**: converte nomes de domínios em endereços lógicos (IP).
- **DHCP**: gerencia e atribui endereços dinamicamente, realocando quando não utilizados.
- **SLAAC**: semelhante ao DHCP, porém sem controle e gerenciamento de endereços.

- **SMTP**: para envio de e-mails entre servidores e cliente-servidor.
- **POP3**: baixa e-mail do servidor, sem manter uma cópia lá.
- **IMAP**: baixa e-mail do servidor, porém mantendo uma cópia lá.

- **FTP**: para transferência de arquivos (download/upload).
- **SFTP**: transferência de arquivos com criptografia, usando SSH.
- **TFTP**: transferência de arquivos mais simples, com menos carga.

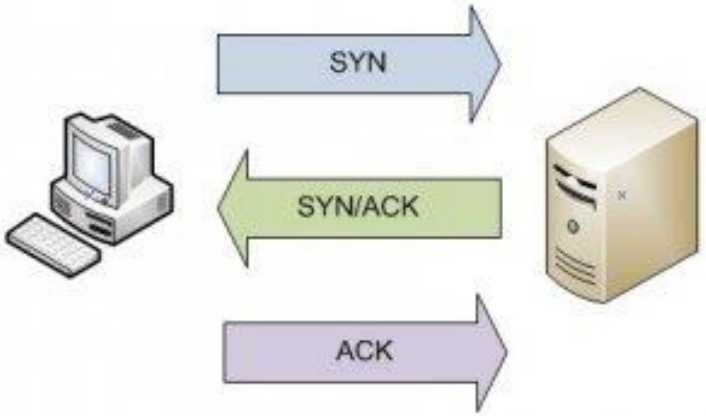
- **HTTP**: troca de texto, imagens, som e vídeo da Web.
- **HTTPS**: adiciona criptografia ao HTTP.

CAMADA DE TRANSPORTE

TCP: É um protocolo **orientado à conexão**, ou seja, é preciso estabelecer uma conexão antes do envio dos pacotes de rede. Se a conexão cair, o envio é interrompido; A grande vantagem é **garantir a entrega dos pacotes**. Se o pacote for perdido na transmissão, o protocolo reenvia um substituto.

UDP: **Não é orientado à conexão**, sendo por este motivo mais rápido que o TCP, pois não necessita estabelecer conexão ou verificar se o pacote chegou ao destino (melhor esforço);

É utilizado por aplicações de alta velocidade como streamings de áudio e vídeo.



CAMADA DE INTERNET

- **IP**: recebe segmentos da camada de transporte, empacota e endereça com **32 bits no IPv4 e 128 bits no IPv6** para entrega de ponta a ponta.
- **NAT**: associa endereços de uma **rede privada** a endereços de **rede pública** para navegação.
- **ICMP**: protocolo para mensagens entre hosts, para verificação da comunicação. Em redes IPv6, tem a funcionalidade também de descobrir vizinhos.

- **OSPF**: protocolo para distribuição de **rotas internas** dinamicamente.
- **EIGRP**: desenvolvido pelo Cisco para **roteamento interno**, usa uma métrica composta pela largura de banda, atraso, carga e confiabilidade para calcular o melhor caminho.
- **BGP**: protocolo de distribuição de **rotas externas**, geralmente entre provedores

CAMADA DE ACESSO A REDE

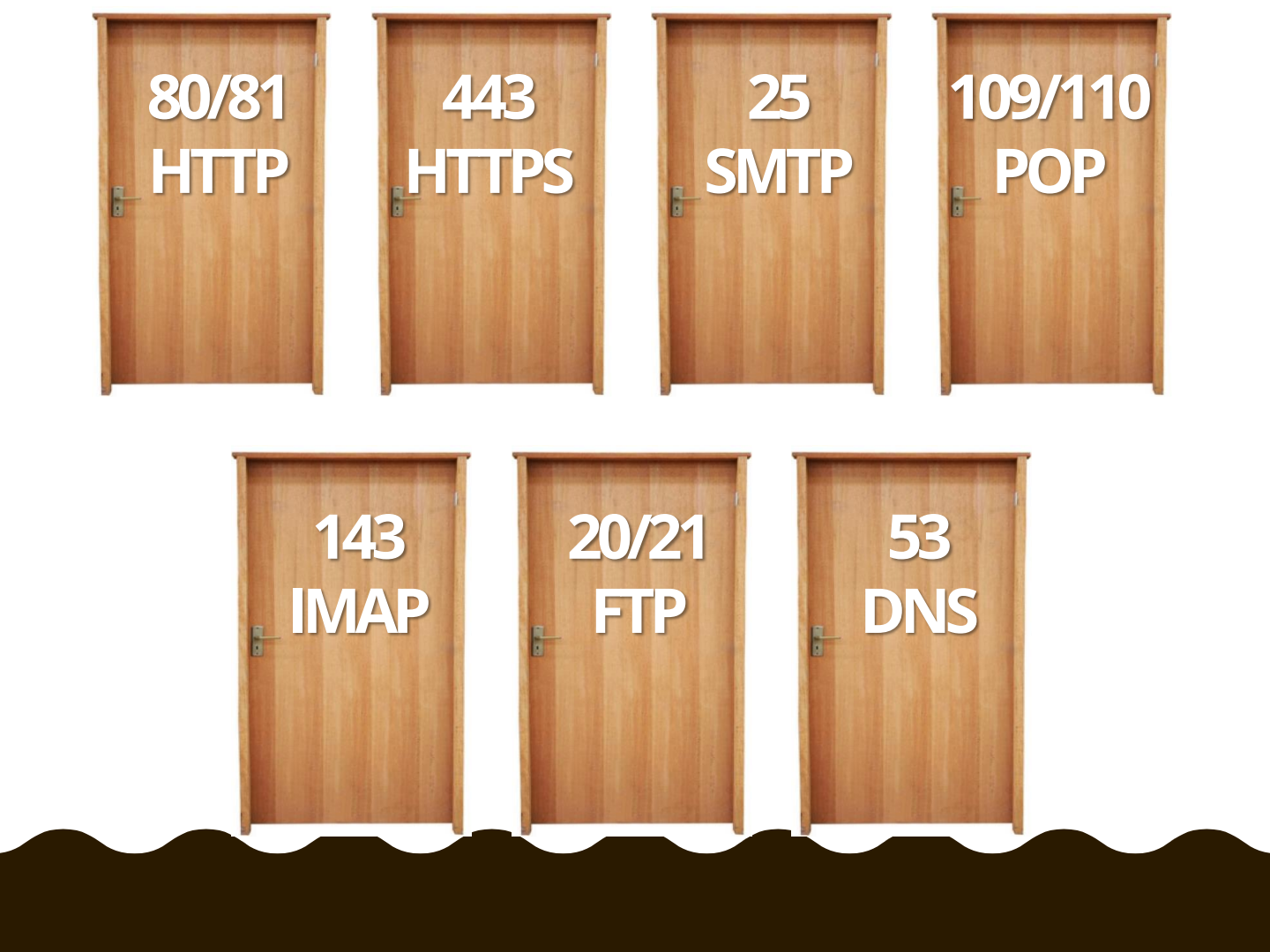
- **ARP**: mapeia dinamicamente um endereço lógico para um endereço físico. e segmentos da camada de transporte, empacota e endereça com **32 bits no IPv4 e 128 bits no IPv6** para entrega de ponta a ponta.

- **Ethernet**: define regras para padrão de fiação e sinalização da camada de acesso a rede.
- **WLAN**: rede local sem fio, opera nas frequências de rádio 2.4 e 5 GHz.

PORTAS LÓGICAS

Os diversos protocolos de aplicação podem ser executados de modo simultâneo nas máquinas graças as portas lógicas.

Imagine uma grande sala com milhares de portas. Cada protocolo atende numa porta específica (caso ela não esteja "trancada"). Existem ao todo, **65.536** portas. Vamos conhecer as principais.


80/81
HTTP
443
HTTPS
25
SMTP
109/110
POP
143
IMAP
20/21
FTP
53
DNS

OBSERVAÇÃO IMPORTANTE

Em 1º de Janeiro de 2013, o Brasil **trancou a porta 25** (SMTP) para reduzir o envio de ***spam*** (e-mail não solicitado). Todos os provedores e operadoras de Internet no país tiveram que reconfigurar seus servidores.

O protocolo passou então a atender na porta **587** ou **465**, considerada mais segura. A proposta surgiu em 2005, levando 8 anos para ser aprovada.

EMPRESAS DE PADRÕES

Se você for comprar um pneu para seu carro, pode escolher entre vários fabricantes, pois todos seguem um padrão. O mesmo acontece com os protocolos.

Os padrões são **desenvolvidos por organizações** em um esforço conjunto de estabelecer regras para toda a Internet e redes em geral. Isso permite que um usuário com sistema operacional Apple OSX baixe um arquivo de um site hospedado com servidor Linux.


IEEE

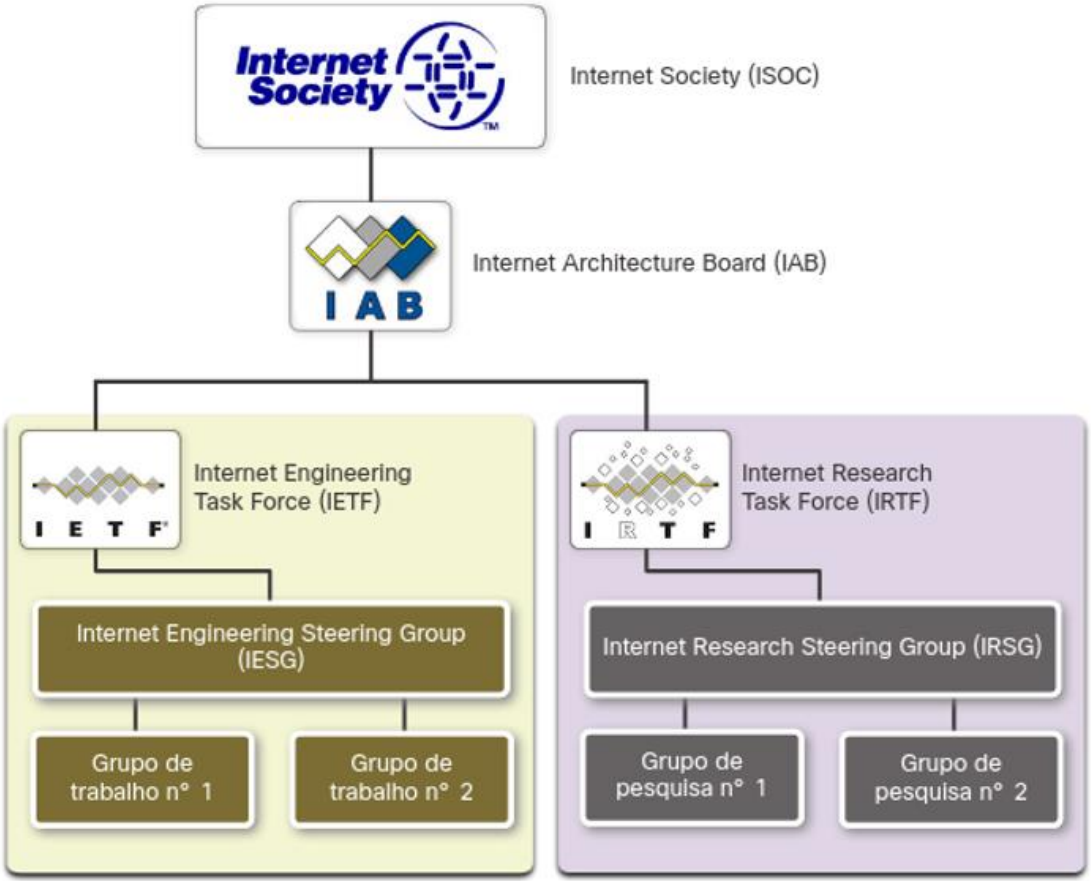
IETF®


iana
Internet Assigned Numbers Authority

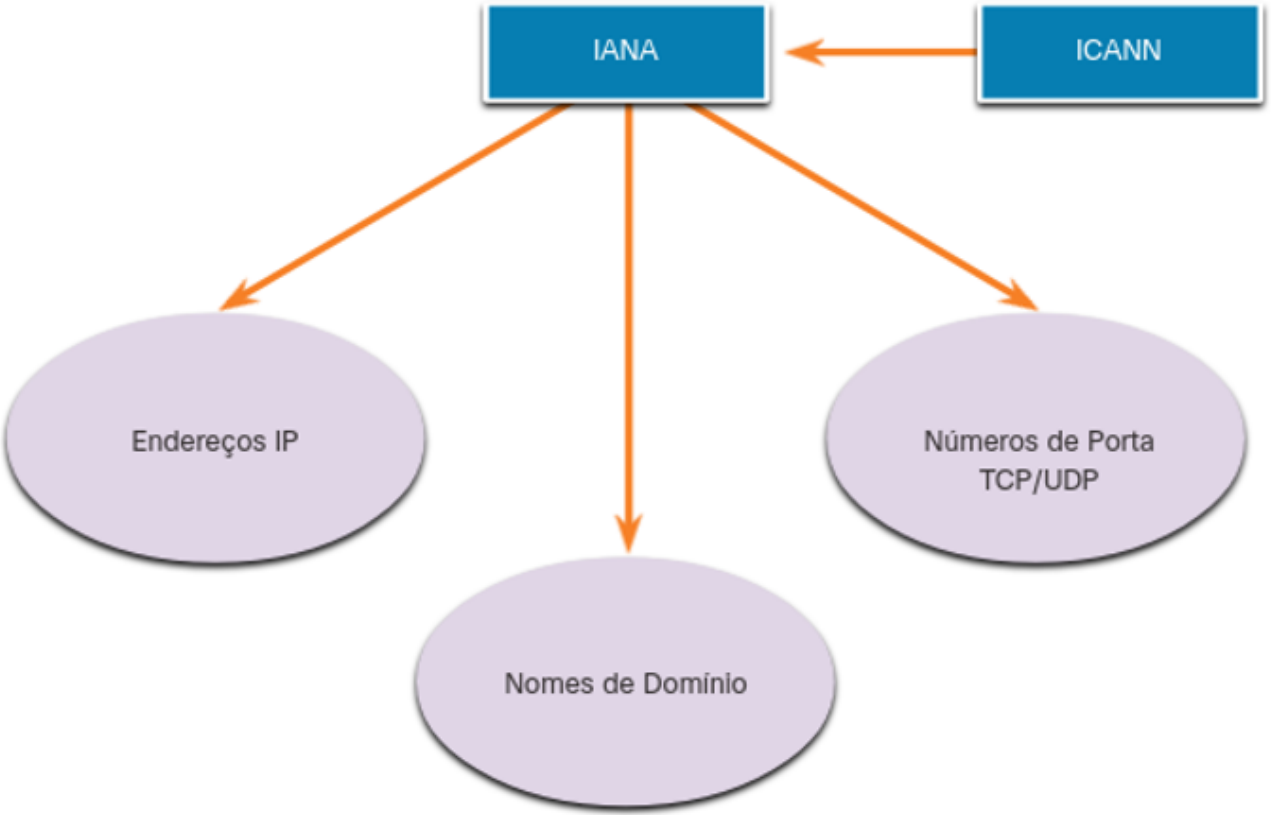

ICANN
The Internet Corporation for Assigned Names and Numbers


ITU


TIA



DESENVOLVIMENTO E SUPORTE DA INTERNET



DESENVOLVIMENTO E SUPORTE DO TCP/IP

PADRÕES ELETRÔNICOS

Outras empresas desenvolvem padrões de engenharia de comunicação entre meios físicos, como sinais eletrônicos.

- **IEEE**: padroniza a engenharia elétrica e eletrônica em vários setores, inclusive força e energia, saúde, telecomunicações e redes.

- **EIA**: estabelece padrões para fiação elétrica, conectores e racks usados para montar equipamentos de rede.

- **TIA**: desenvolve padrões para várias áreas, incluindo equipamentos de rádio, torres celulares, dispositivos de VoIP, comunicação via satélite, entre outros. O **cabo Ethernet** foi desenvolvido pela EIA e pela TIA de modo cooperativo.

- **ITU-T**: compactação de vídeo, IPTV e comunicações banda larga, como DSL.

MODELOS DE REFERÊNCIA

MODELOS DE CAMADAS

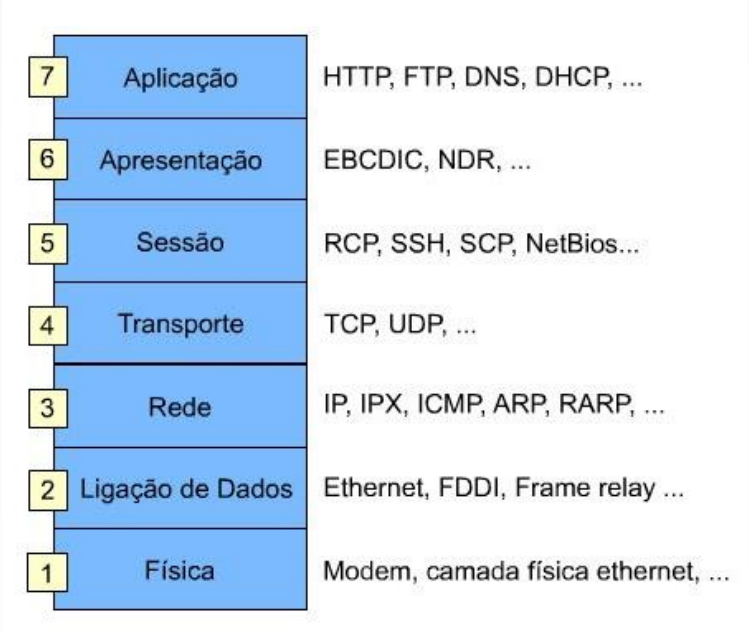
Um modelo de referência ajuda a entender como dois dispositivos interconectados se comunicam pela rede, independente de marcas de fabricantes.

São separados por camadas, onde cada camada representa uma etapa da interconectividade. Independente do modelo, as **camadas não se "conversam**", isto é, uma não conhece os dados da outra. Apenas recebe a informação, faz seu trabalho e repassa para a próxima camada. Isso vale tanto para o envio quanto para o recebimento, onde **cada camada tem acesso apenas às suas informações pertinentes**.

Já estudamos brevemente o modelo de camadas TCP/IP. Ele é usado para descrever as operações de rede, juntamente com outro modelo, o OSI.

MODELO OSI

O modelo OSI contém 7 camadas e foi proposto para melhor compreensão dos processos de rede, em detrimento ao modelo TCP/IP. É proposto para uso didático, inadequado para implementação, pois não contém detalhes de funcionamento, somente abstrações;



MODELO OSI

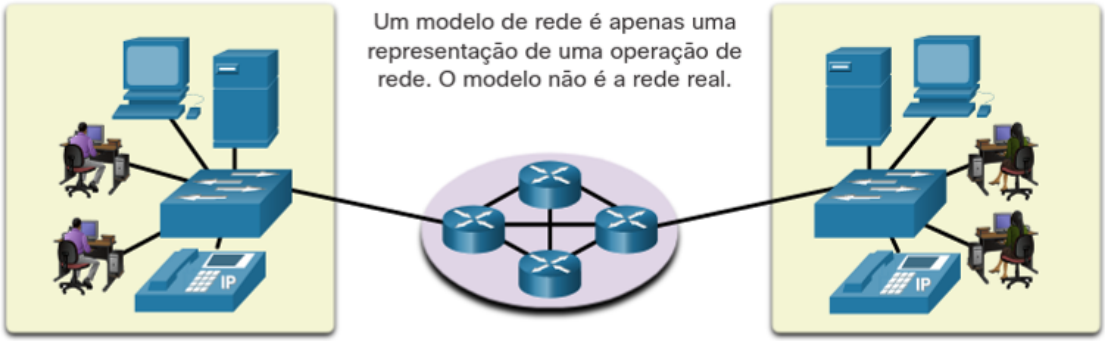
- **Física**: É a **interface com a rede**, propriamente dita, onde está especificado o tipo de mídia e a placa de rede. Trafega bit puro, seja no envio de dados (quando são transmitidos pela mídia) ou no recebimento (quando são "coletados" pela placa).
- **Dados**: Faz a **conferência dos dados** coletados pela camada física e a **correção de erros**, caso haja. Controla também o fluxo de dados que chegam/saem, evitando congestionamento.
- **Rede**: Após os dados serem corrigidos, **a camada de rede é responsável por endereçá-las**. Define também o caminho que as informações vão percorrer.
- **Transporte**: Transporta os pacotes endereçados pela rede. A camada de transporte também **controla o fluxo dos pacotes e os ordena**, a medida que vão saindo ou chegando. É uma camada especial, pois a comunicação é ponto-a-ponto, da origem diretamente com o destino.

MODELO OSI

- **Sessão**: É através da camada de sessão que as máquinas estabelecem comunicação entre seus processos. Com a sessão aberta, as máquinas controlam o início e fim de uma transmissão, bem como o reinício, caso seja necessário.

- **Apresentação**: Chamada também de tradução, essa camada faz a "**formatação**" dos dados que chegam ou saem para que sejam exibidos corretamente. Tem também o trabalho de comprimir ou criptografar os dados, conforme necessidade.

- **Aplicação**: Esta camada faz referência direta aos programas que fazem uso dos dados, propriamente ditos (e-mail, navegação Web, etc). **Aqui trabalham os protocolos das aplicações, mais próximos dos usuário final**.



Modelo OSI	Suíte de Protocolos TCP/IP	Modelo TCP/IP
Aplicação	HTTP, DNS, DHCP, FTP	Aplicação
Apresentação		
Sessão		
Transporte	TCP, UDP	Transporte
Rede	IPv4, IPv6, ICMPv4, ICMPv6	Internet
Enlace de Dados	Ethernet, WLAN, SONET, SDH	Acesso à Rede
Física		

COMPARAÇÃO OSI E TCP/IP

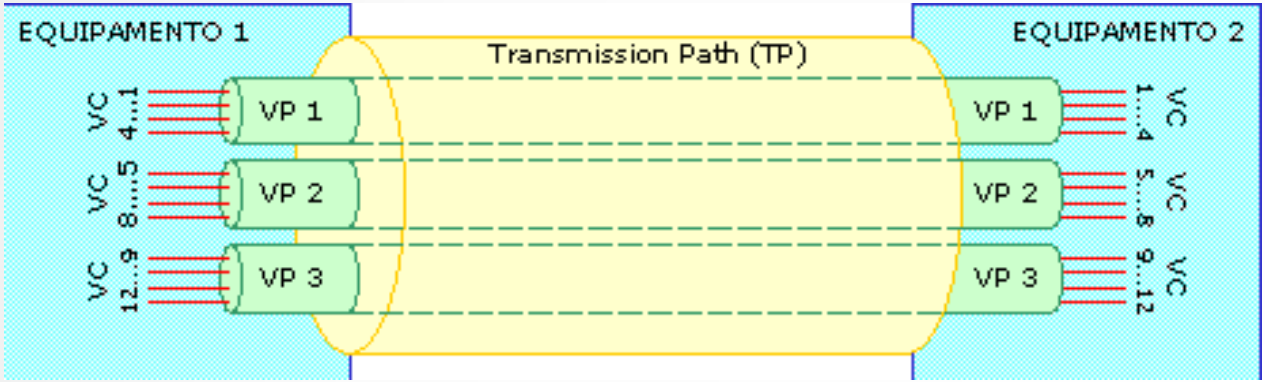
O PACOTE TCP/IP

Com tamanho máximo de 1.500 bytes (1,5 KB), trafega várias informações. Se os dados forem maiores, **o pacote é quebrado em partes menores** para o transporte.

<table>
<tr><td colspan="5">Porta origem</td><td colspan="4">Porta destino</td></tr>
<tr><td colspan="9">Número de sequência</td></tr>
<tr><td colspan="9">Número de confirmação</td></tr>
<tr><td>Header size</td><td colspan="2">Reservado</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td>Tamanho da janela</td></tr>
<tr><td colspan="5">Checksum</td><td colspan="4">Urgent pointer</td></tr>
<tr><td colspan="9">Opções (tamanho variável)</td></tr>
<tr><td colspan="9">Dados (tamanho variável)</td></tr>
</table>

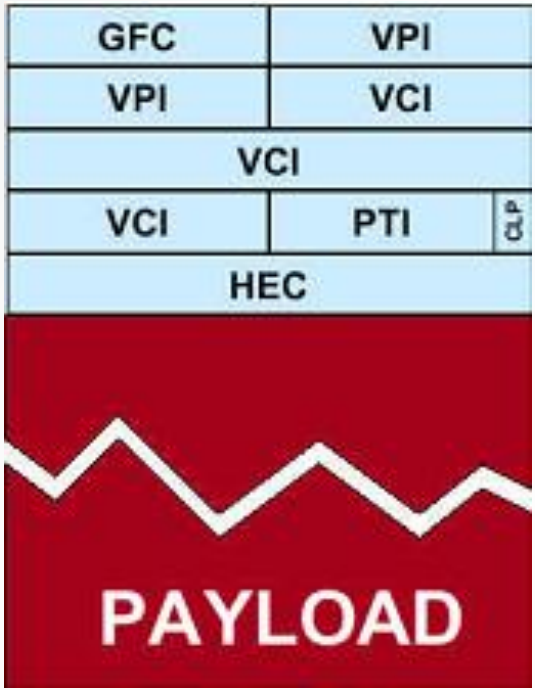
MODELO ATM

Modelo com 3 camadas, de alta velocidade orientado à conexão que não trafega pacotes e sim, **células**. É popular em telefonia de longa distância e serviços digitais integrados (o famoso "TV+Internet+Telefone"). A emissão de vários sinais é possível, pois na célula ATM existem as rotas virtuais, por onde trafegam os canais. Pode-se fazer uma analogia com uma rodovia que tem várias pistas para tráfego.



A CÉLULA ATM

Com 53 bytes (o pacote TCP/IP tem 1.500), a célula ATM trafega informações importantes para o fluxo.



SEGMENTAÇÃO DE DADOS

Quando a informação trafegada é maior que o *payload* da mídia, a informação é fragmentada em vários pedaços menores. Isso ajuda no gerenciamento do fluxo, onde, caso não ocorresse, gerariam atrasos, ocupação da mídia durante longo período, e pior resposta à falhas.

- **Velocidade**: com carga menor, grande quantidade de dados de diferentes tipos e origens podem ser trafegadas sem congestionar um link de comunicação (multiplexação).

- **Eficiência**: se algum conteúdo falhar no transporte, a rede se encarrega de retransmitir somente aquele segmento e não a mensagem toda.

SEQUENCIAMENTO

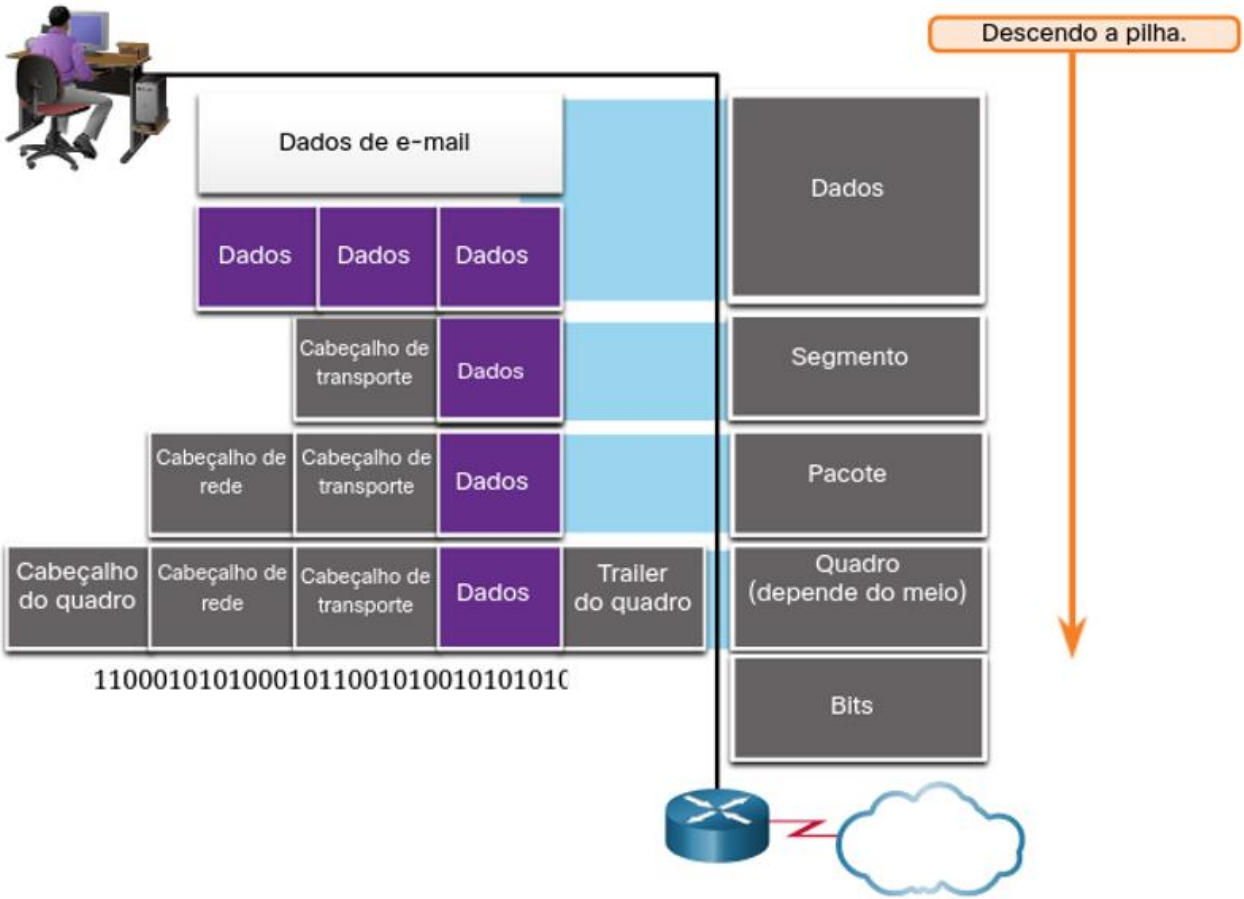
Imagina enviar pelos correios uma carta de 100 páginas, porém uma página em cada envelope. É possível que os envelopes cheguem fora de ordem, por isso deveria haver um número sequencial nas páginas para que a carta pudesse ser remontada mais tarde.

Nas comunicações em rede, o processo é semelhante com os segmentos da mensagem.

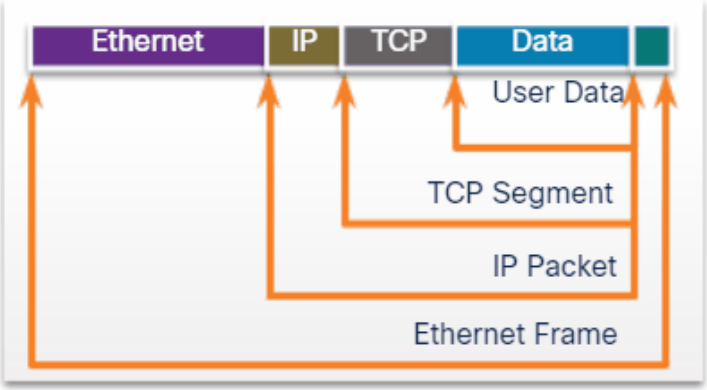
ENCAPSULAMENTO

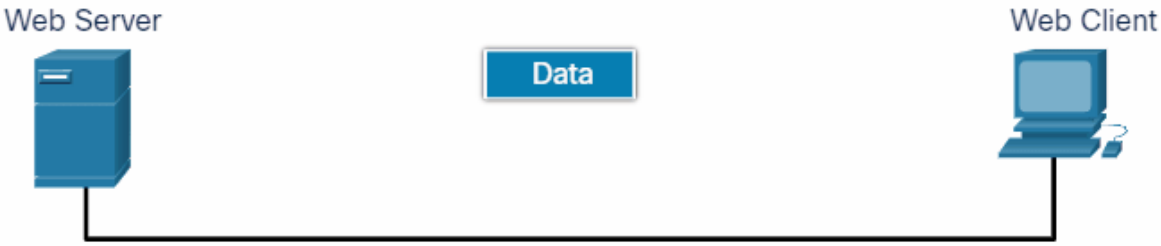
Ao passar pela pilha de protocolos, várias informações de protocolo vão sendo adicionadas a cada nível. A “cápsula” que cada camada recebe é chamada genericamente de **PDU**. Em cada etapa, a PDU recebe um nome específico para refletir as funções adquiridas.

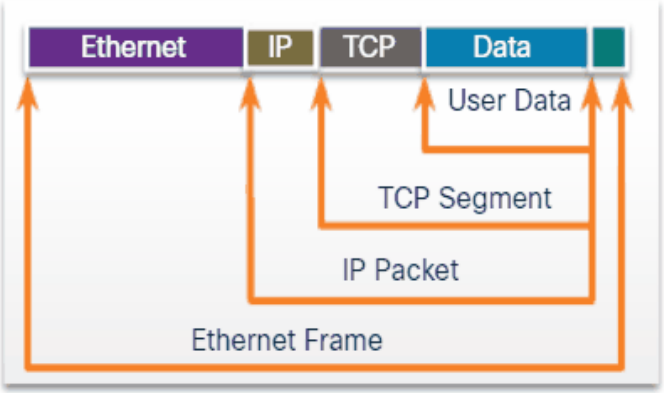
Lembre-se que **cada camada tem acesso apenas às suas informações** pertinentes. Ao receber o PDU, ela adiciona ou faz a leitura de suas própria informações e repassa para a próxima camada.



TCP = SEGMENTO / UDP = DATAGRAMA


Ethernet
IP
TCP
Data
User Data
TCP Segment
IP Packet
Ethernet Frame


Web Server
Data
Web Client


Ethernet
IP
TCP
Data
User Data
TCP Segment
IP Packet
Ethernet Frame


0101011010100101111011010100100101010110110

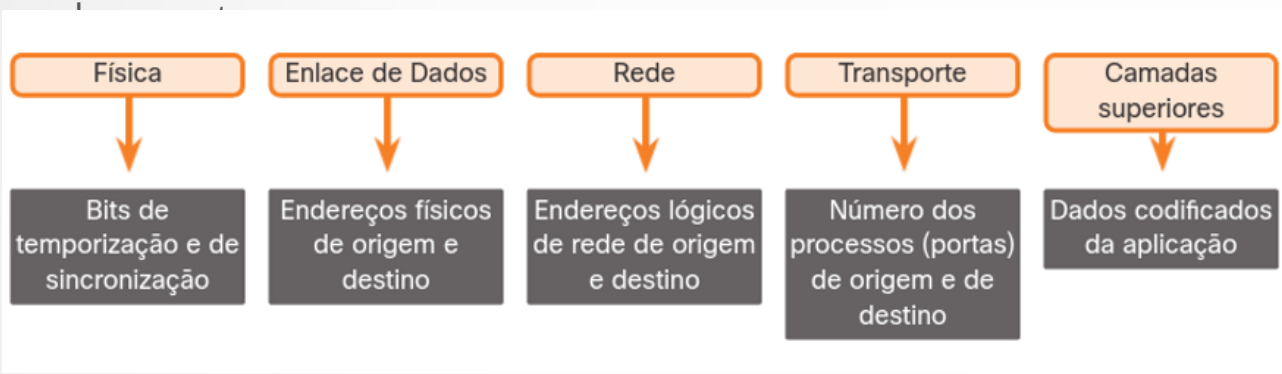
LABORATÓRIO

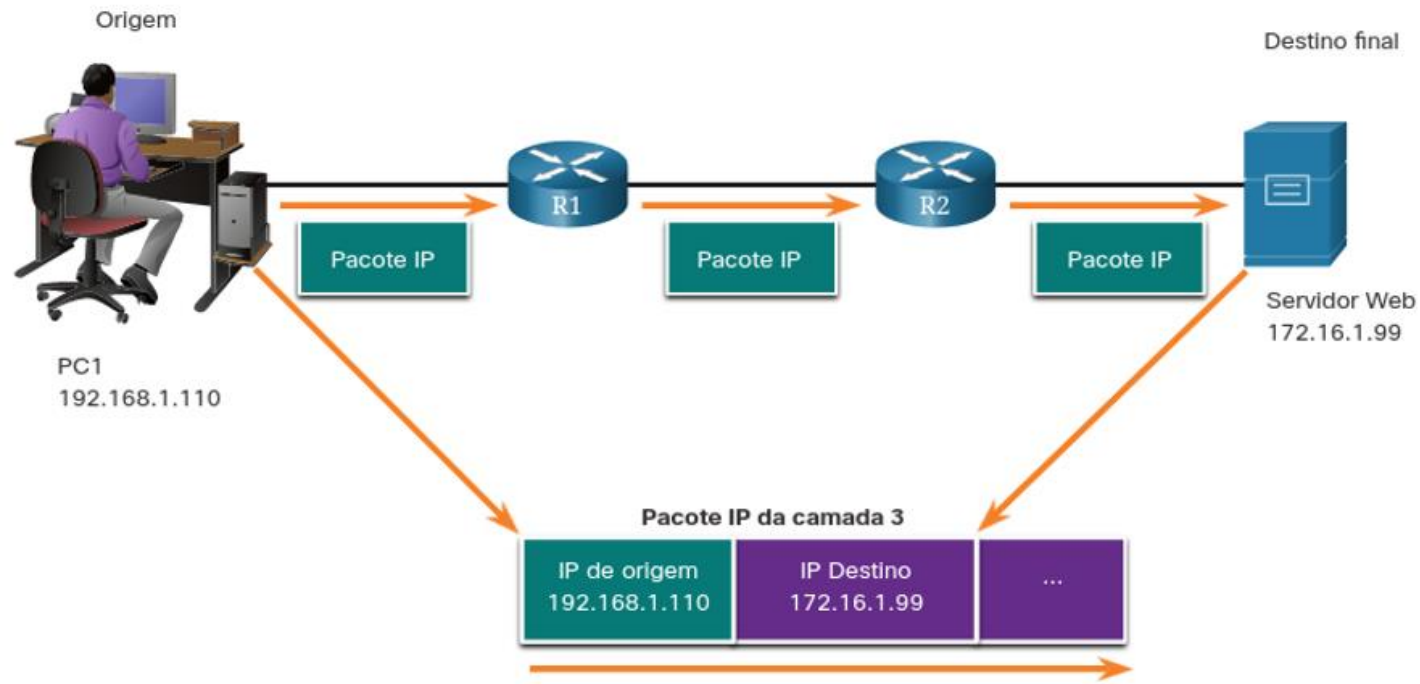
- Wireshark

Capturar um pacote de rede e estudar sua estrutura.

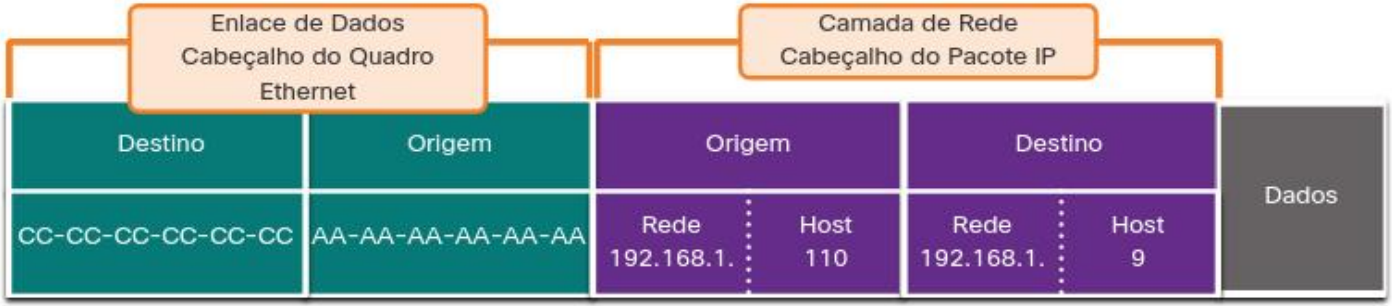
E COMO OS DADOS SÃO ACESSADOS?

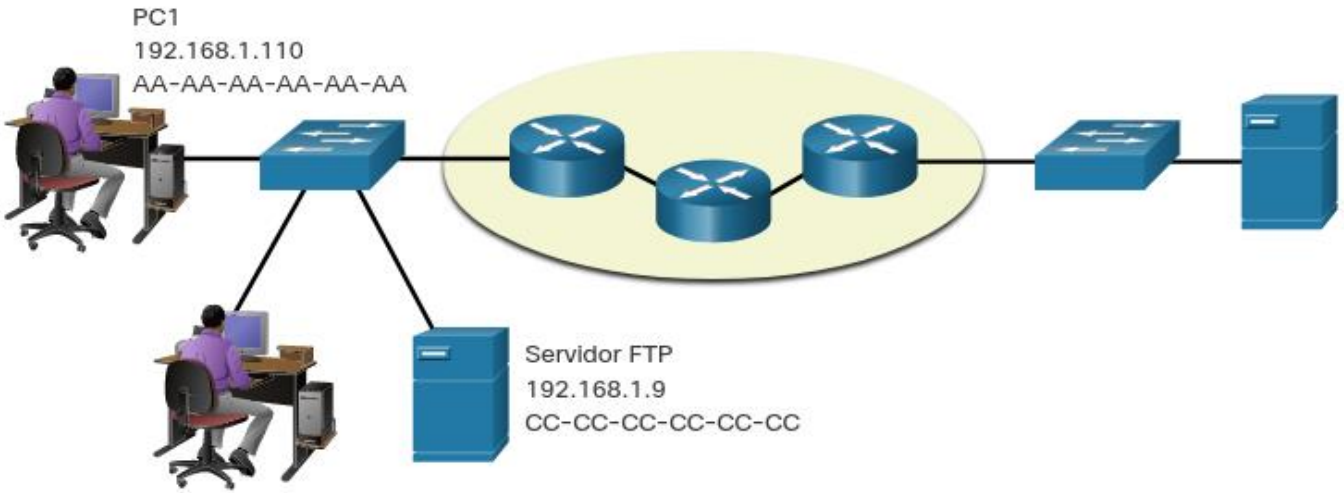
A PDU não vai a lugar nenhum se não for tratada corretamente. Por exemplo, as camadas 2 e 3 utilizam endereços para enviar e receber os dados segmentados, seja na mesma rede ou uma



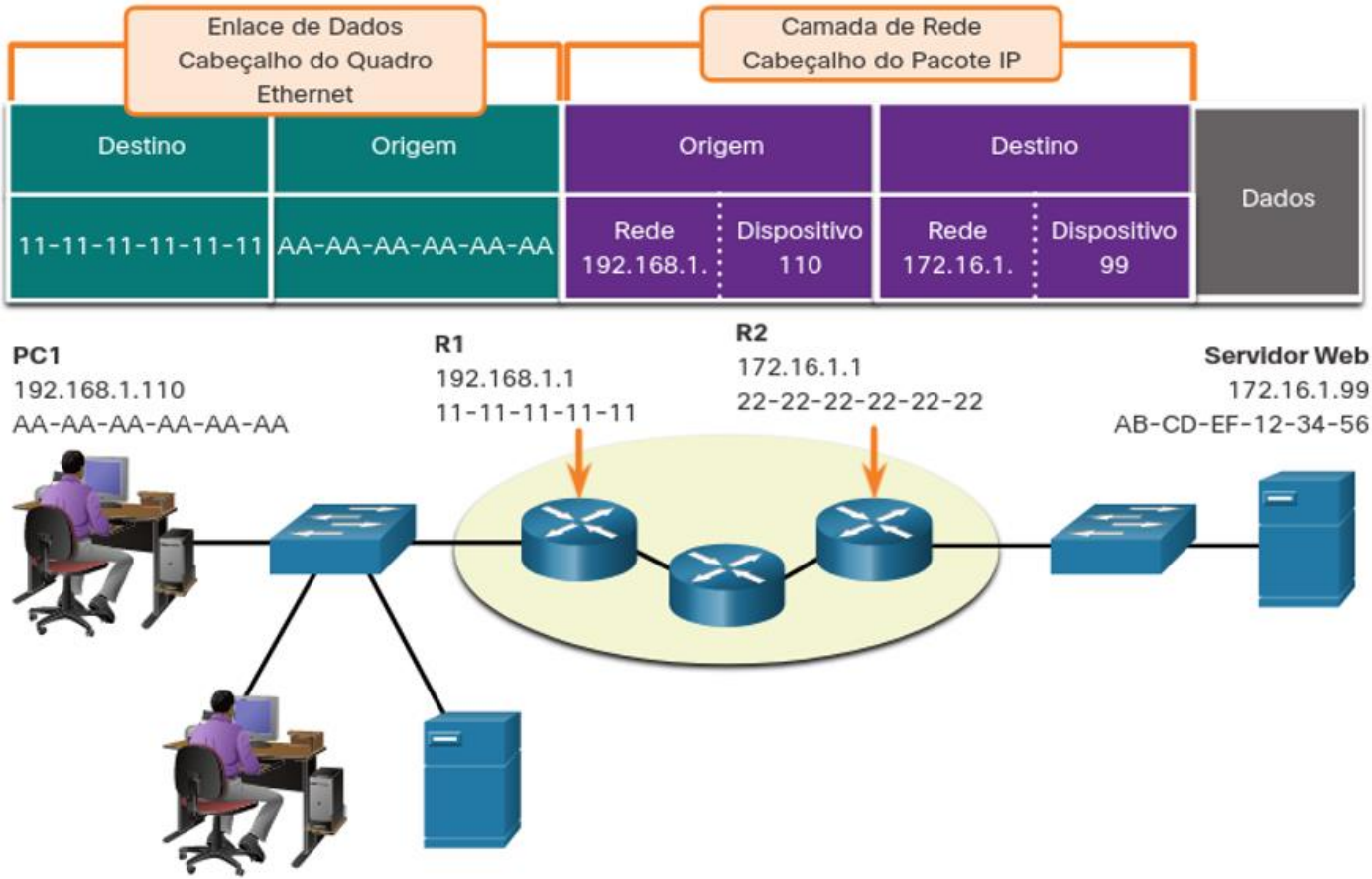


ENDEREÇOS DA CAMADA 3



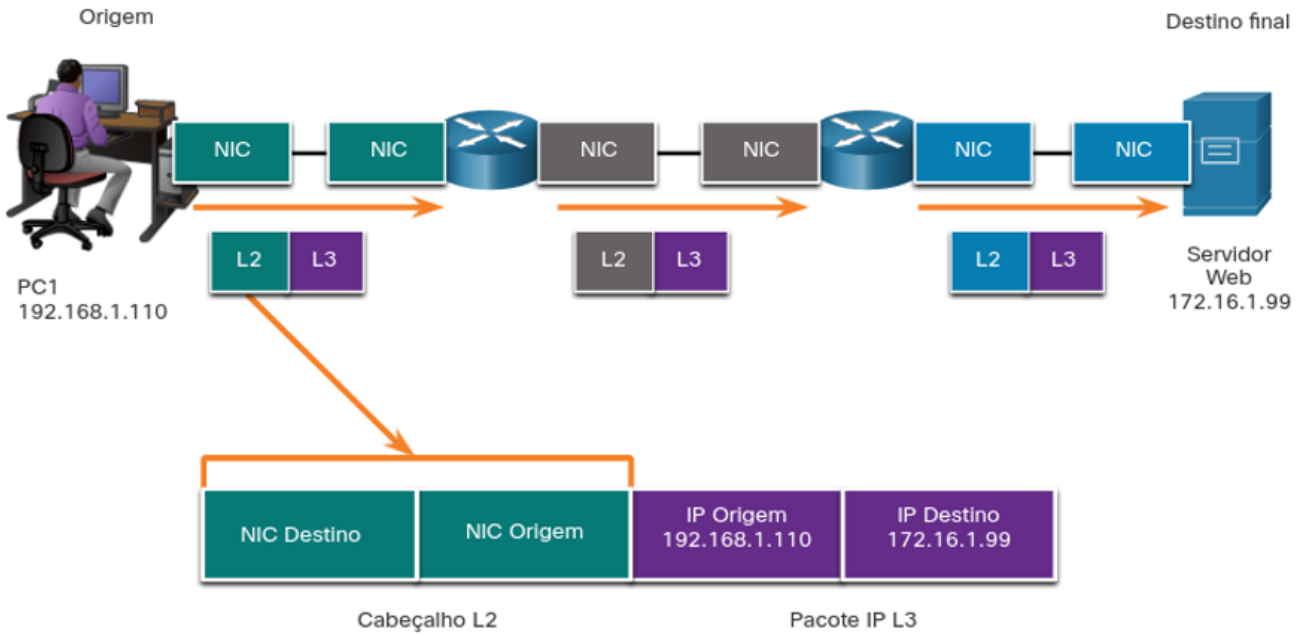


DISPOSITIVOS NA MESMA REDE – ENVIO DIRETO L2



DISPOSITIVOS EM REDE DIFERENTE – ROTEAMENTO L3

Host para Roteador



CAMINHO DO PACOTE NA REDE

CAMADA FÍSICA

A CONEXÃO FÍSICA

Antes de qualquer envio de comunicação de rede, **uma conexão física deve ser estabelecida**, ou por um cabo ou de modo sem fio.

A camada física do modelo OSI fornece os meios para transportar os bits, gerados a partir de um quadro da camada de enlace de dados. Ou então, receber os bits transmitidos pelo meio físico.

A PLACA DE REDE

A NIC (*Network Interface Card*) conecta o dispositivo a rede, seja final ou intermediário. junto a outros padrões de interface. A NIC comumente pode ser com fio, no padrão **Ethernet**, ou sem fio, no padrão **WLAN**, podendo haver os dois tipos presente no dispositivo.

PADRÕES DA CAMADA FÍSICA

Os protocolos e operações das camadas superiores são executados por softwares padronizados por engenheiros e cientistas da computação. Na camada física, trabalham **circuitos eletrônicos, meios físicos e conectores** desenvolvidos pelos engenheiros elétricos e de comunicações.

Várias organizações estão envolvidas no estabelecimento e manutenção de padrões da camada física como:

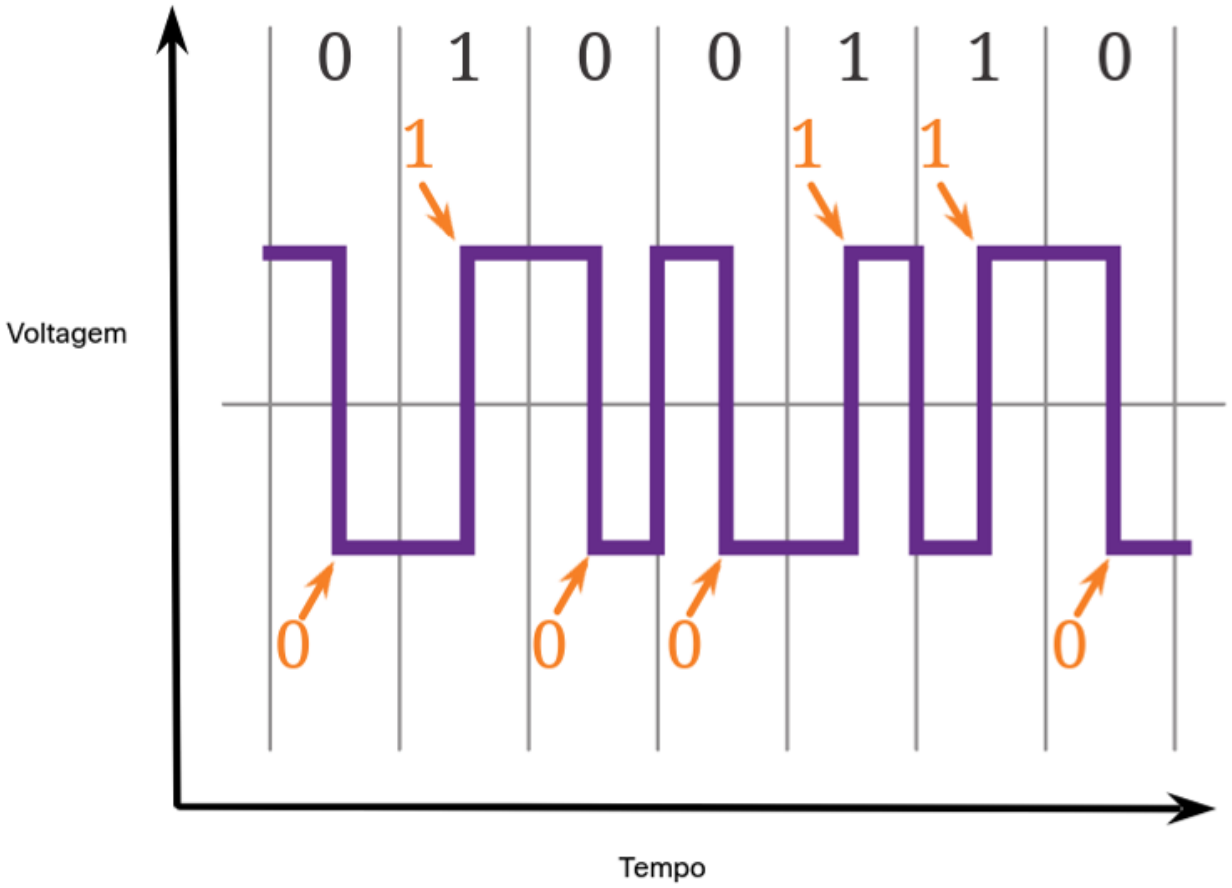
- ISO
- EIA/TIA
- ITU-T
- ANSI
- IEEE

Juntamente ainda com grupos regionais no Canadá, Japão e Europa.

PADRÕES DA CAMADA FÍSICA

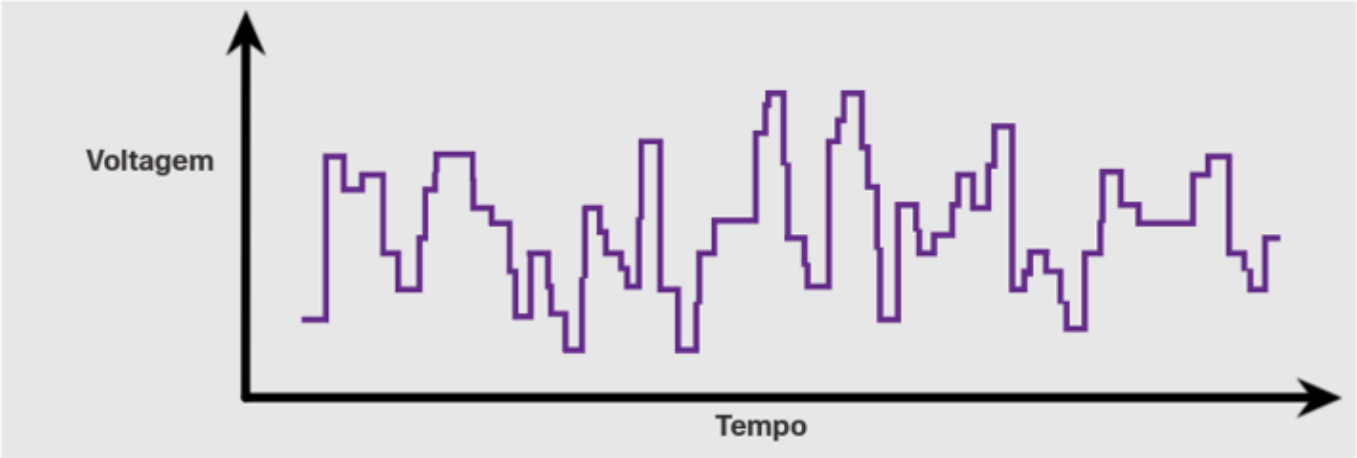
São 3 áreas funcionais abordadas por padrões na camada física, sendo:

- **Componentes Físicos**: são os dispositivos de hardware, componentes, mídia e conectores. As portas, interfaces, NICS, materiais e projetos de cabo são exemplos de especificações associados a camada Física.
- **Codificação**: é um método ou padrão de representação das informações digitais, semelhante ao código Morse. Por exemplo a codificação Manchester representa o bit 0 por uma transição de baixa voltagem e o bit por uma transição de alta voltagem.
- **Sinalização**: a camada física deve gerar o sinal (elétrico, óptico ou sem fio) no meio físico, definindo que tipo de sinal representa cada bit. Por exemplo, um pulso longo pode representar um 1, enquanto um pulso curto pode representar um 0.

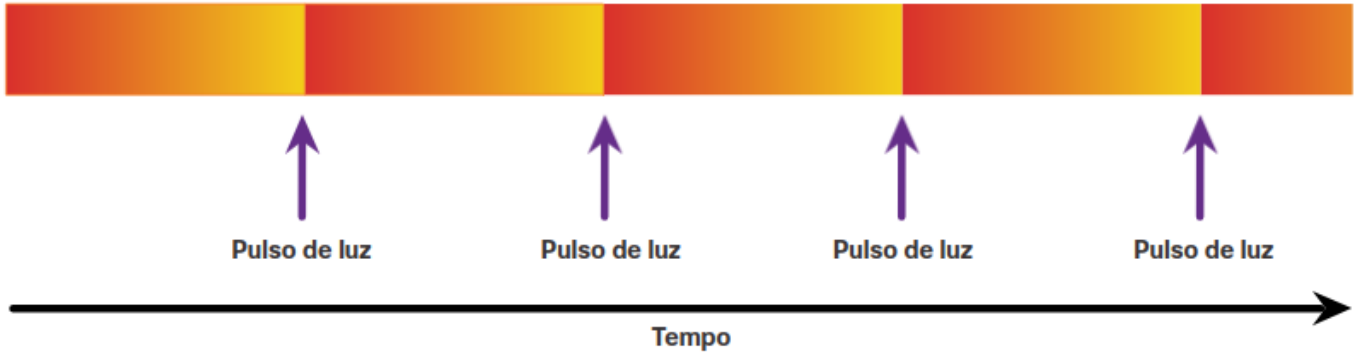


CODIFICAÇÃO MANCHESTER

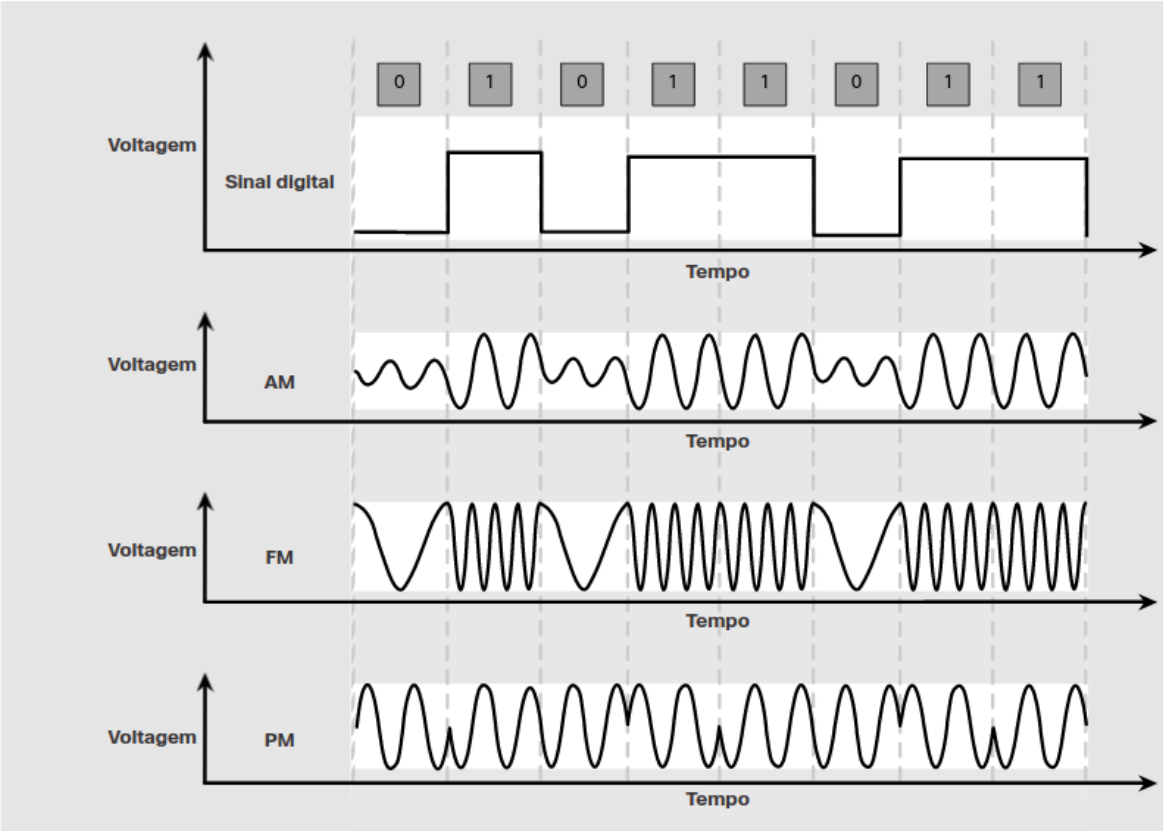
Sinais elétricos em Cabos de Cobre



Pulsos de Luz em Cabos Ópticos



Sinais em microondas sem Fio



LARGURA DE BANDA

A taxa de transferência de bits depende do meio físico, combinada a tecnologia de sinalização e detecção dos sinais. Geralmente medimos em termos de largura de banda, com a quantidade de dados transportadas em determinado período de tempo. A unidade padrão usada são **bits por segundo** (bps).

Unidades	Sigla	Equivalência
Bits por segundo	bps	1 bps (unidade fundamental)
Kilobits por segundo	Kbps	1 Kbps = 1.000 bps
Megabits por segundo	Mbps	1 Mbps = 1.000.000 bps
Gigabits por segundo	Gbps	1 Gbps = 1.000.000.000 bps
Terabits por segundo	Tbps	1 Tbps = 1.000.000.000.000

LARGURA DE BANDA

Há ainda outras terminologias para medir a qualidade da largura de banda.

- **Latência**: tempo necessário para os **dados viajarem de um lugar a outro**, incluindo atrasos. Pode ser afetada com a criação de 'gargalos' entre segmentos de uma mesma rede.

- **Taxa de Transferência**: a medida da transferência propriamente dita, geralmente menor do que a especificada nas implementações da camada física (**BW**). É influenciada pela quantidade de tráfego, tipo de tráfego e a latência.

- **Dados usáveis**: é a medida de dados usáveis transferidos em determinado período. Chamado também de **goodput**, é sempre menor que a taxa de transferência.

Velocidade de Transferência

80.78 Mbps

Velocidade de upload

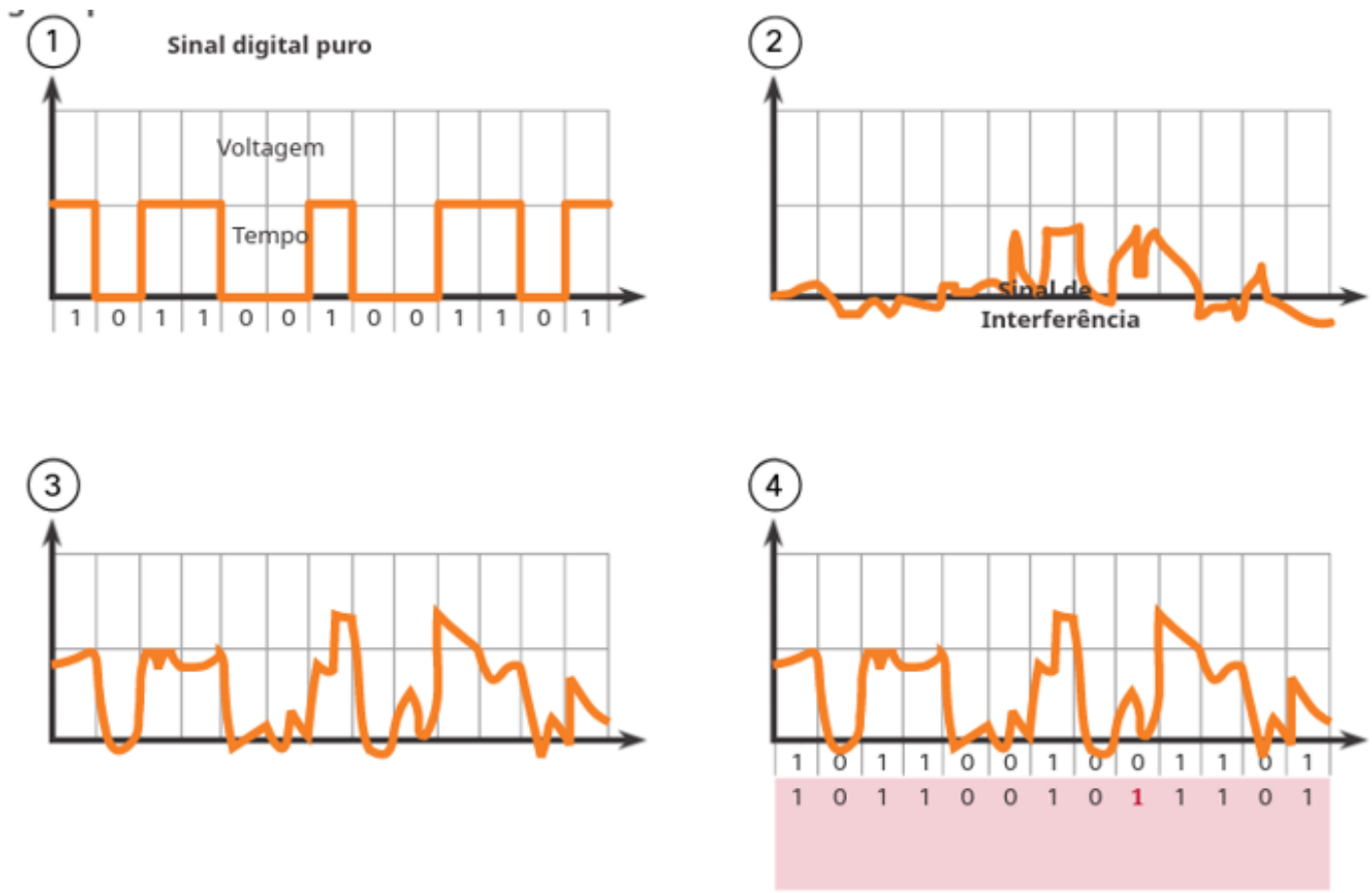
8.78 Mbps

CABEAMENTO DE COBRE

Tipo de cabeamento mais comum, sendo de 3 tipos, tem baixo custo, facilidade de instalação e baixa resistência a corrente elétrica. Porém é limitada pela distância e pela interferência de sinal.

Os dados são transmitidos como pulsos elétricos. Quanto maior a distância de viagem, mais o sinal se deteriora (**atenuação**). Além disso, ainda sofrem dois tipos de interferência.

- **EMI/RFI (Eletromagnética ou por Radiofrequência)**: sinais de ondas de rádio ou eletromagnéticos como luzes, motores e dispositivos domésticos podem distorcer ou corromper os sinais de dados transportados.
- **Diafonia**: interferência no campo magnético de um cabo por um outro cabo adjacente, captando o sinal do primeiro. É a causa da linha cruzada nos circuitos de telefone

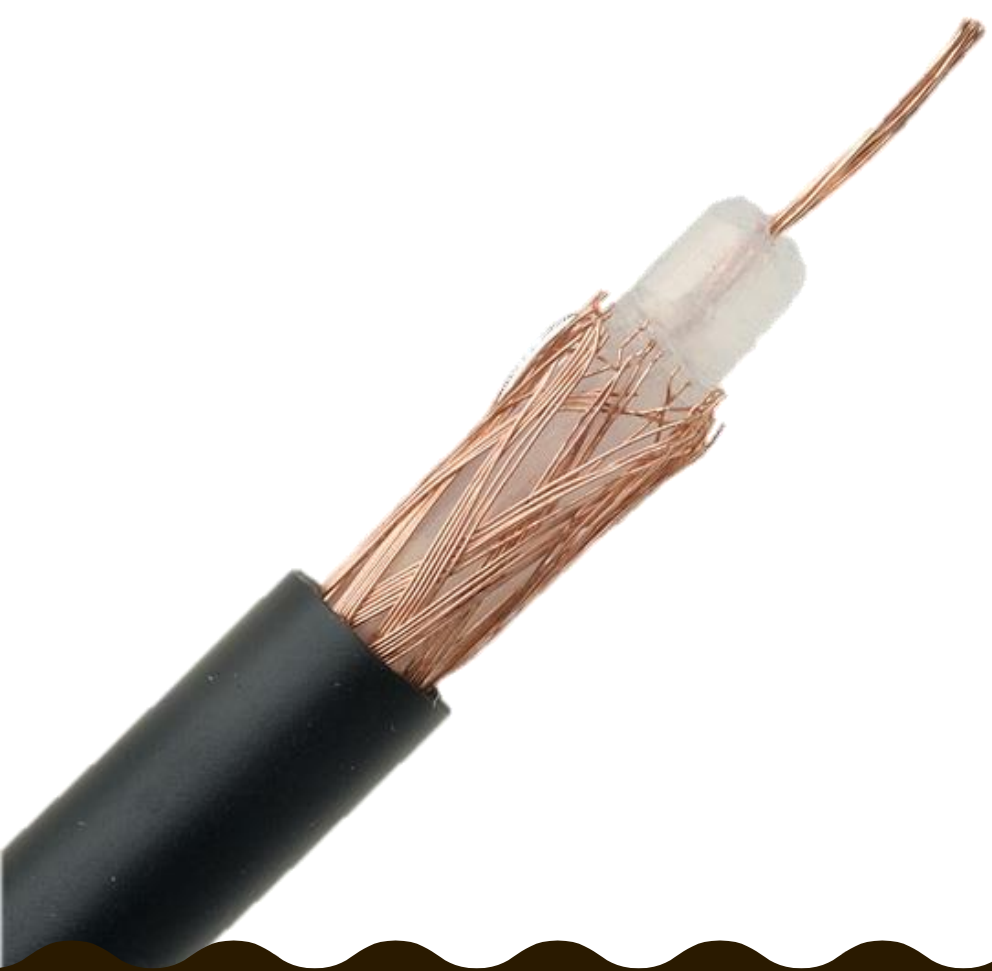

1
Sinal digital puro
Voltagem
Tempo
1 0 1 1 0 0 1 0 0 1 1 0 1
2
Sinal de
Interferência
3
4
1 0 1 1 0 0 1 0 0 1 1 0 1
1 0 1 1 0 0 1 0 1 1 1 0 1

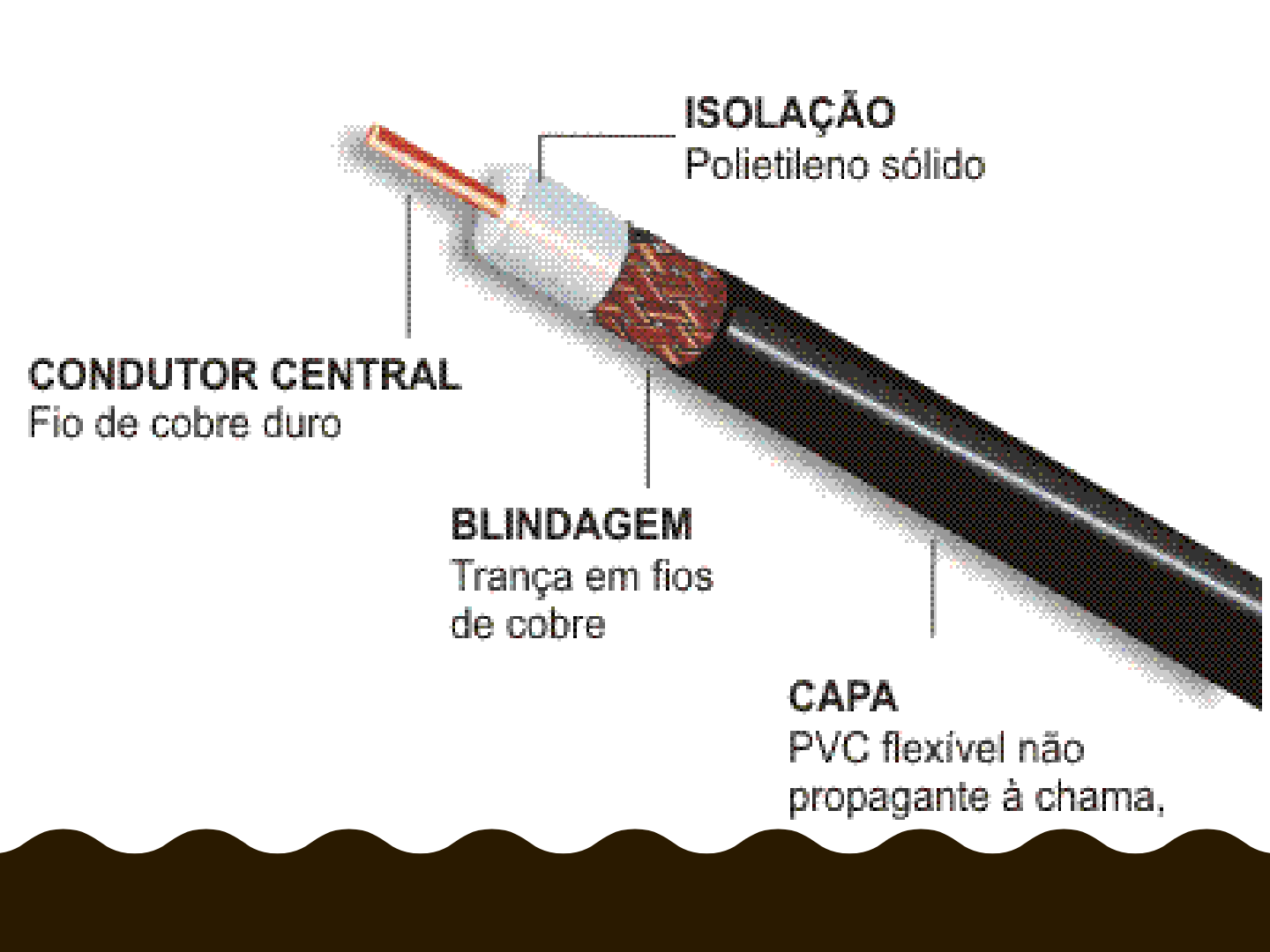
CABO COAXIAL

Uma das primeiras tecnologias de meio físico para redes, é formado por um **condutor de cobre** para transmissão dos sinais, com um camada isolante plástica envolvendo o condutor. Há ainda uma segunda camada de cobre envolvendo o material isolante, atuando como um segundo cabo no circuito e protegendo o condutor interno, reduzindo interferências. Por fim todo o cabo é coberto com um revestimento para proteção externa.

Embora tenha caído em desuso, ainda é utilizado em duas situações:

- **Instalações sem fio**: conecta a antena aos dispositivos, transportando a energia de radiofrequência.
- **TV/Internet a cabo**: nas instalações internas no cliente



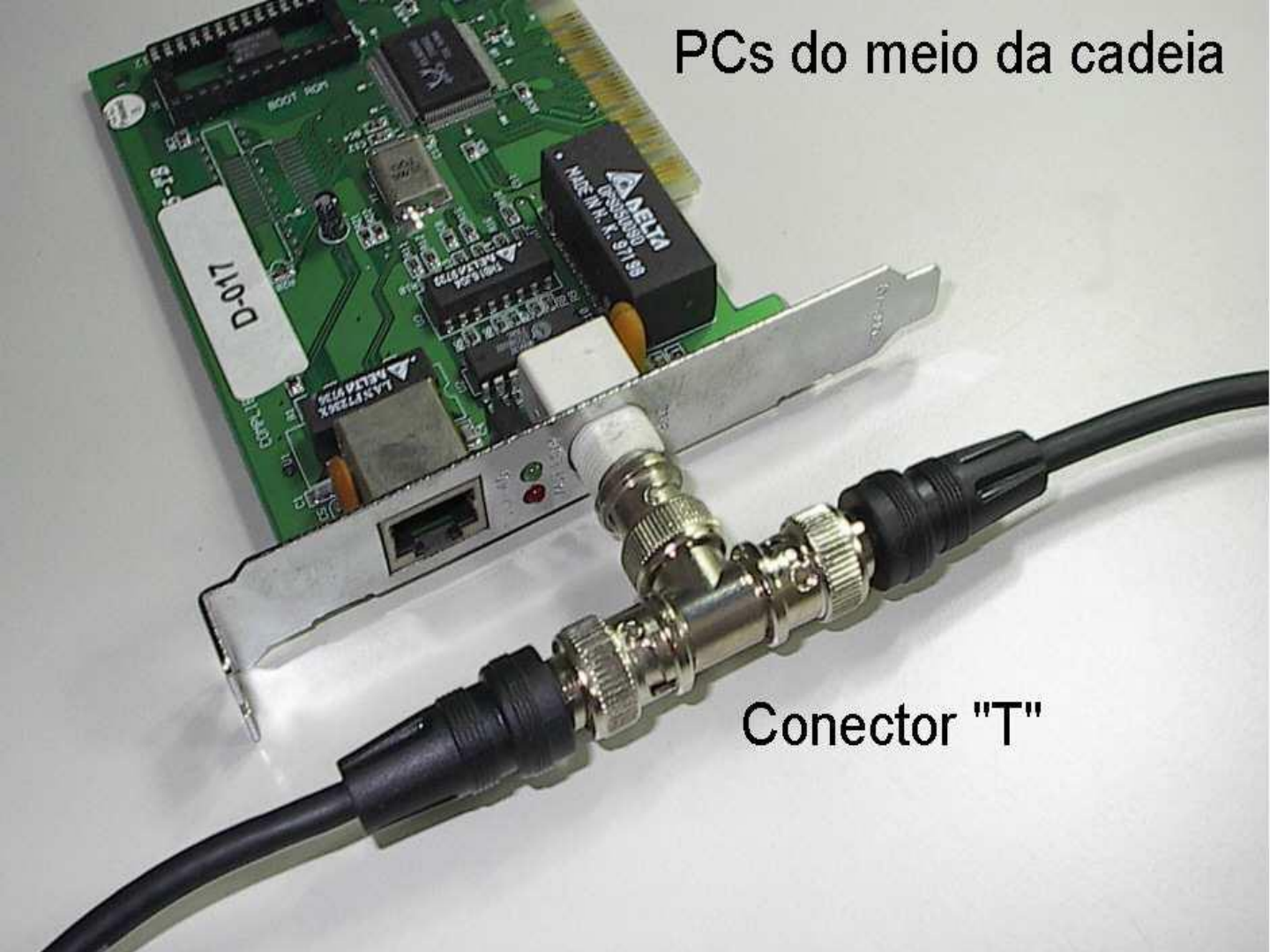

ISOLAÇÃO
Polietileno sólido
CONDUTOR CENTRAL
Fio de cobre duro
BLINDAGEM
Trança em fios
de cobre
CAPA
PVC flexível não
propagante à chama,

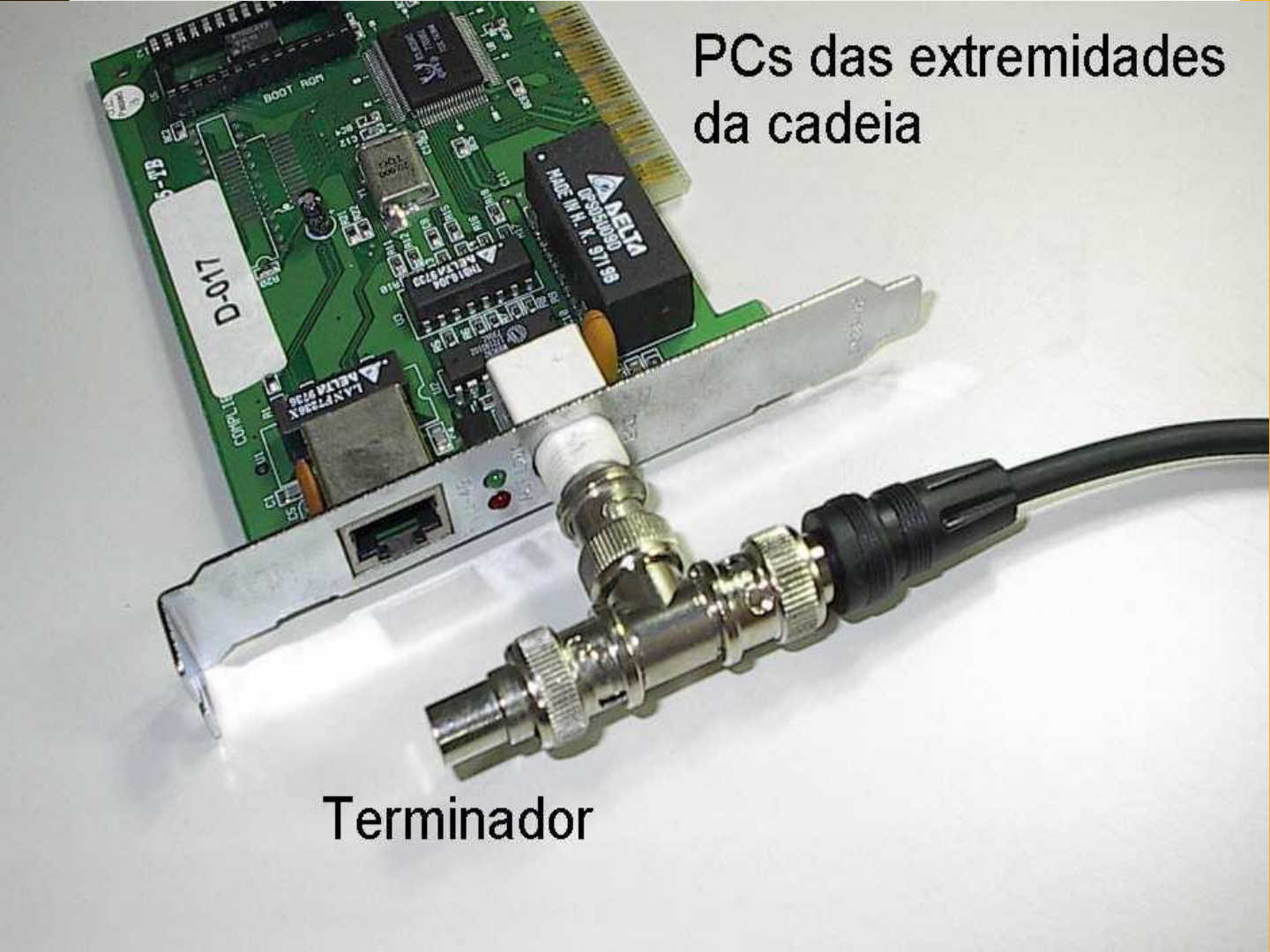
APLICAÇÃO E CONECTORES

Os cabos mais grossos (chamados 10BASE-5 ou *thicknet*) eram utilizados para formar a **base da rede**, geralmente interligando servidores e equipamentos, alcançando até 500m. Os cabos mais finos (chamados 10BASE-2 ou *thinnet*) são utilizados para interligar as **dispositivos**, alcançando até 185m.

Para realizar a conexão, eram utilizados conectores em T. Na ponta do cabo, eram fixados os conectores do tipo BNC, N ou F;

BNC Tipo N Tipo F


PCs do meio da cadeia
Conector "T"

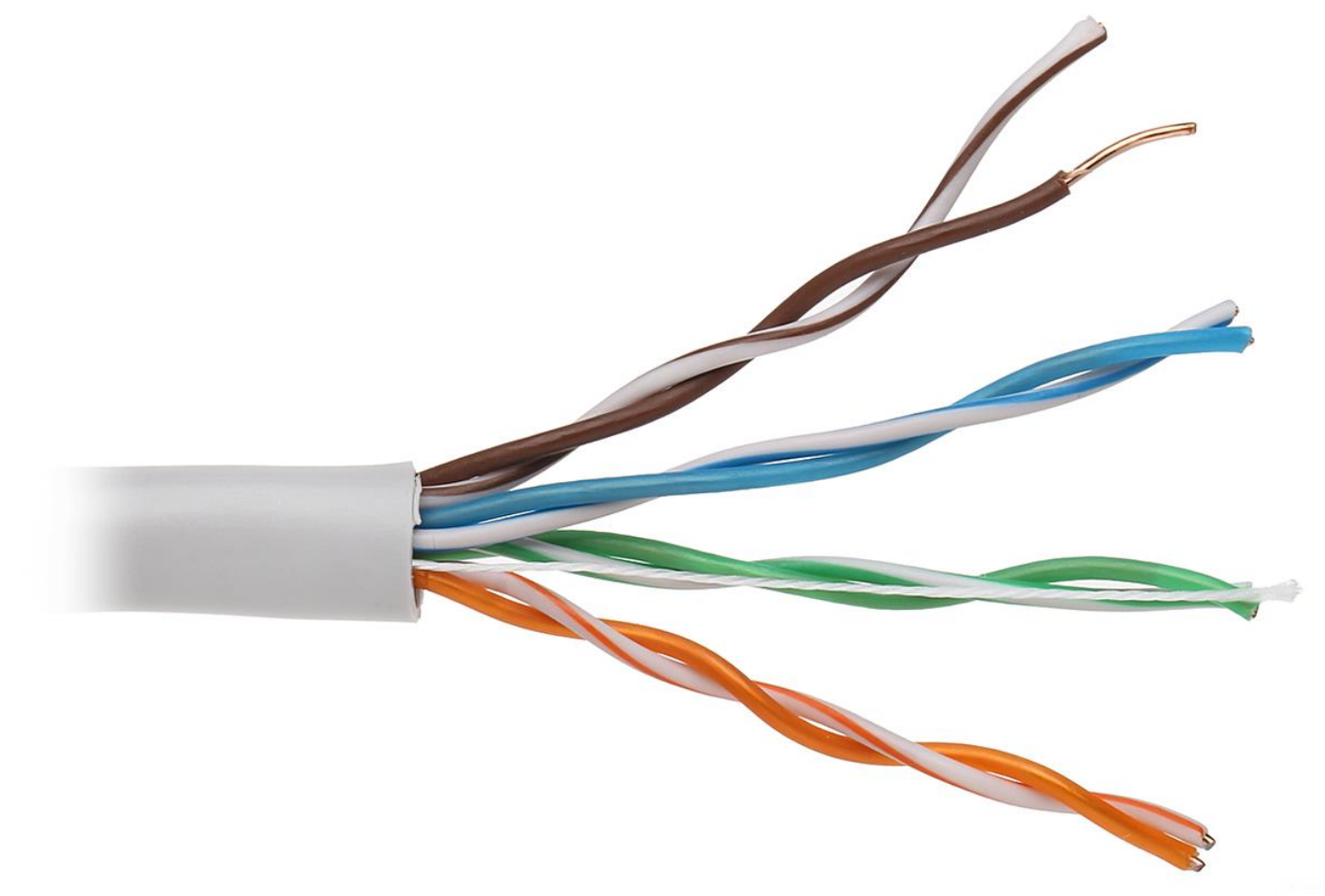

PCs das extremidades
da cadeia
Terminador

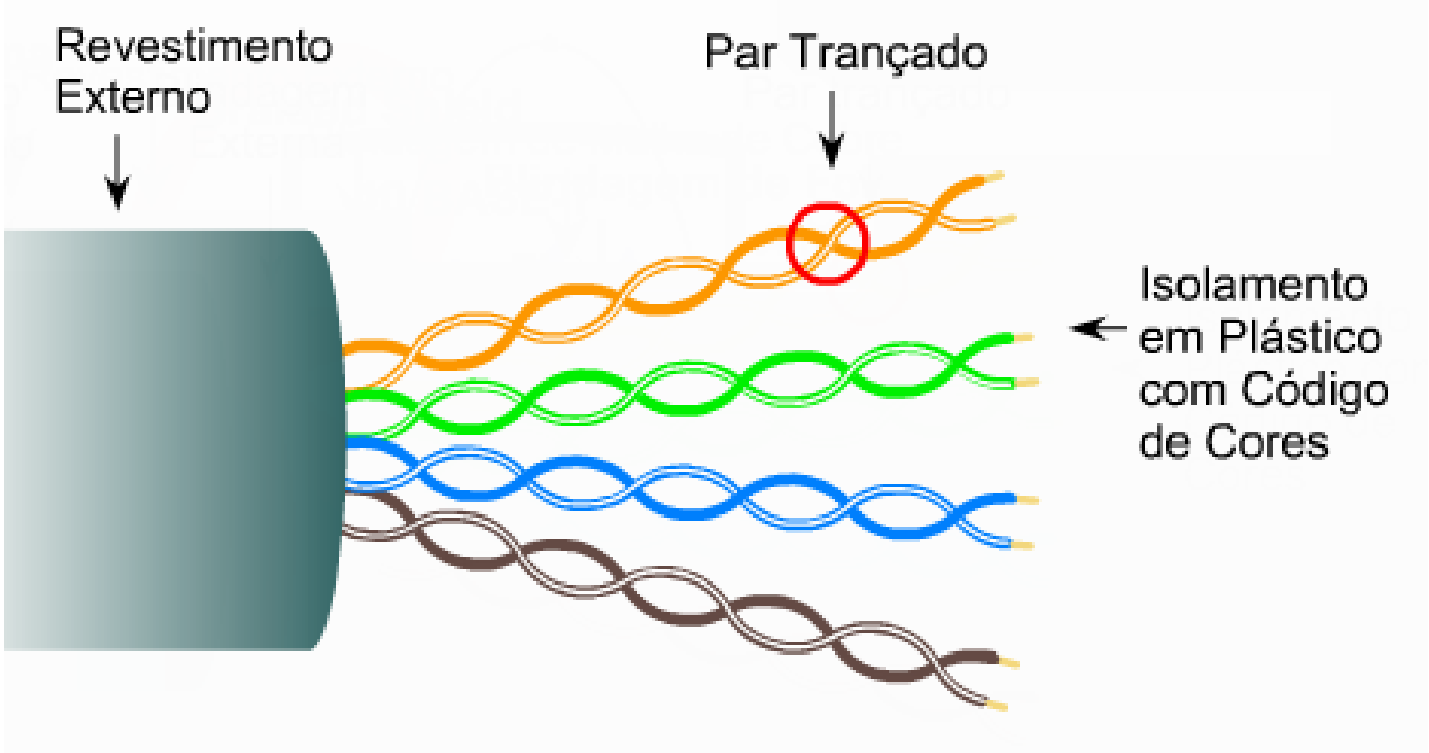
PAR TRANÇADO NÃO-BLINDADO

Era necessário levar informações com taxas de transmissão mais alta através de meios mais flexíveis do que os cabos coaxiais. O par trançado é tipo mais comum de meio físico atualmente, substituindo amplamente as redes coaxiais nas instalações modernas.

Nas LANs, o cabo UTP consiste em **4 pares de cabos codificados por cores**, trançados e protegidos por um capa plástica flexível.

Utilizado com conectores RJ45, conecta dispositivos finais e intermediários. A trança dos pares diminui ruídos e interferências, mas não os elimina. Além disso, potencializa os pulsos elétricos, mantendo-os constantes.




Revestimento Externo
Par Trançado
Isolamento em Plástico com Código de Cores

APLICAÇÃO E CONECTORES

Pares trançados podem ser usados em **redes domésticas e pequenas conexões**. São cabos **flexíveis**, **baratos** e fáceis de manusear e instalar. Suportam redes de até 1024 nós, alcançando até 100m de distância. As taxas de transmissão são até 100 vezes mais rápidas em comparação aos cabos coaxiais.

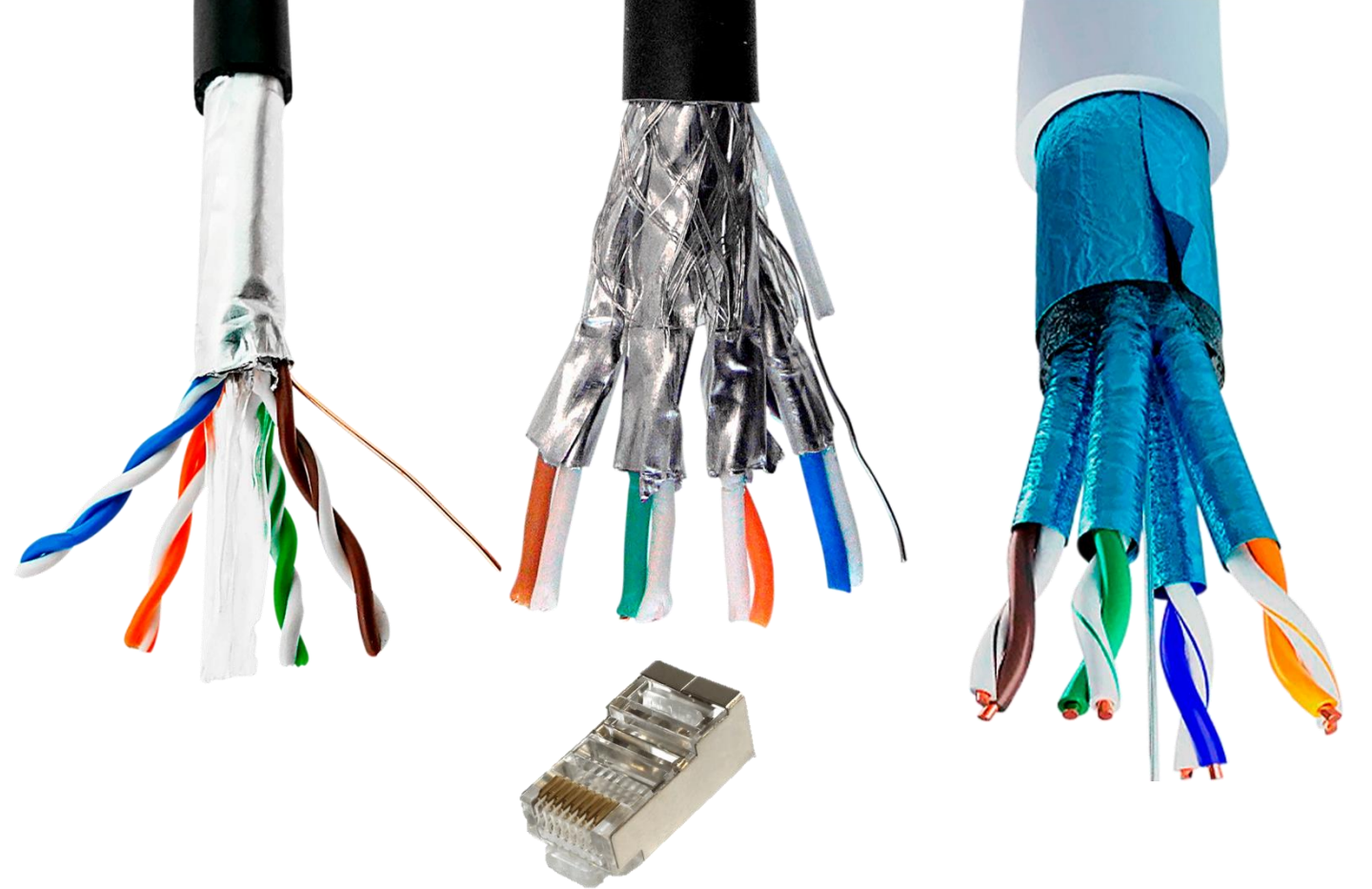
Na ponta do cabo é usado o conector RJ-45 Macho, enquanto nas placas e tomadas está o conector RJ-45 Fêmea ou Jack RJ - 45;

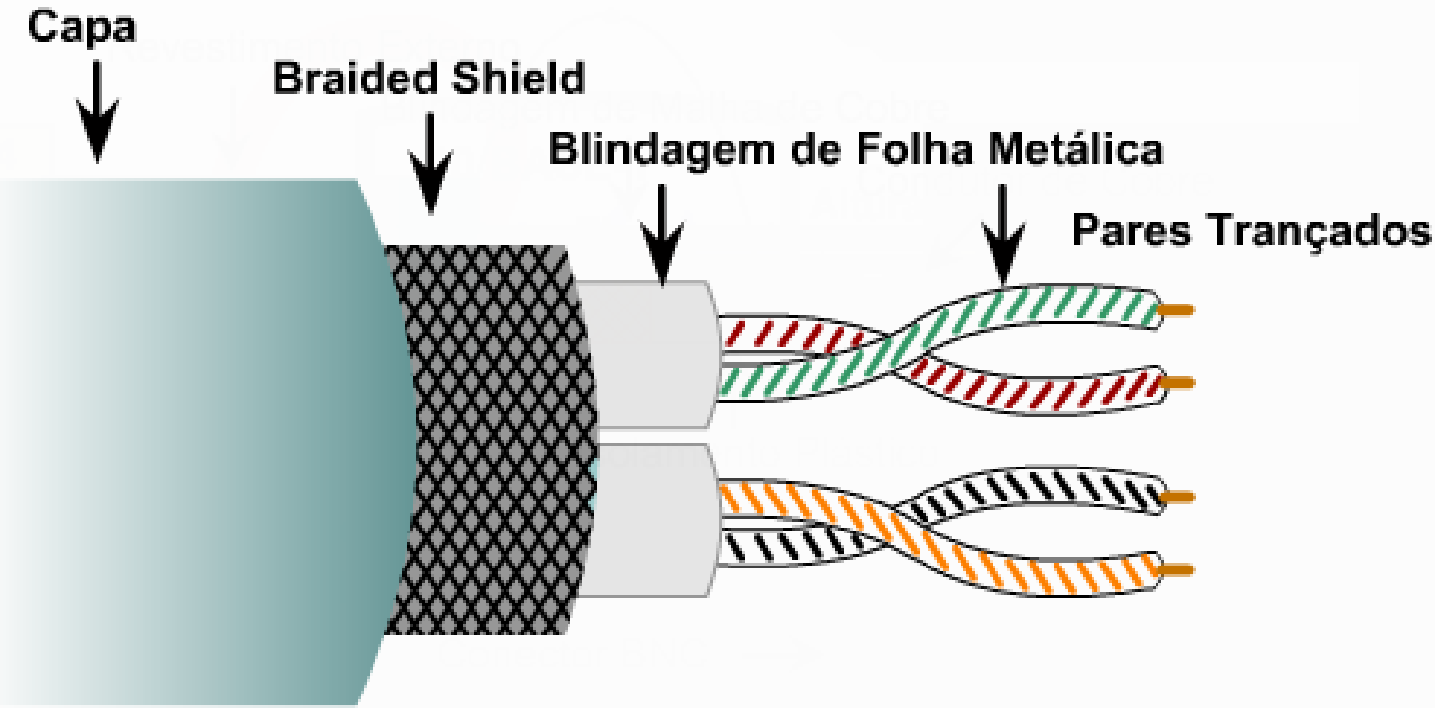
PAR TRANÇADO BLINDADO

A blindagem aplicada tem a função de **diminuir ruídos e interferências no cabo**, oferecendo maior proteção e desempenho, utilizando o mesmo conector RJ-45, porém também blindado. É mais caro e mais difícil sua instalação em comparação ao UTP.

Para aproveitar totalmente a blindagem, o **cabo deve ser aterrado**, para não gerar efeito contrário e captar sinais eletromagnéticos indesejados. Pode ser de 3 tipos:

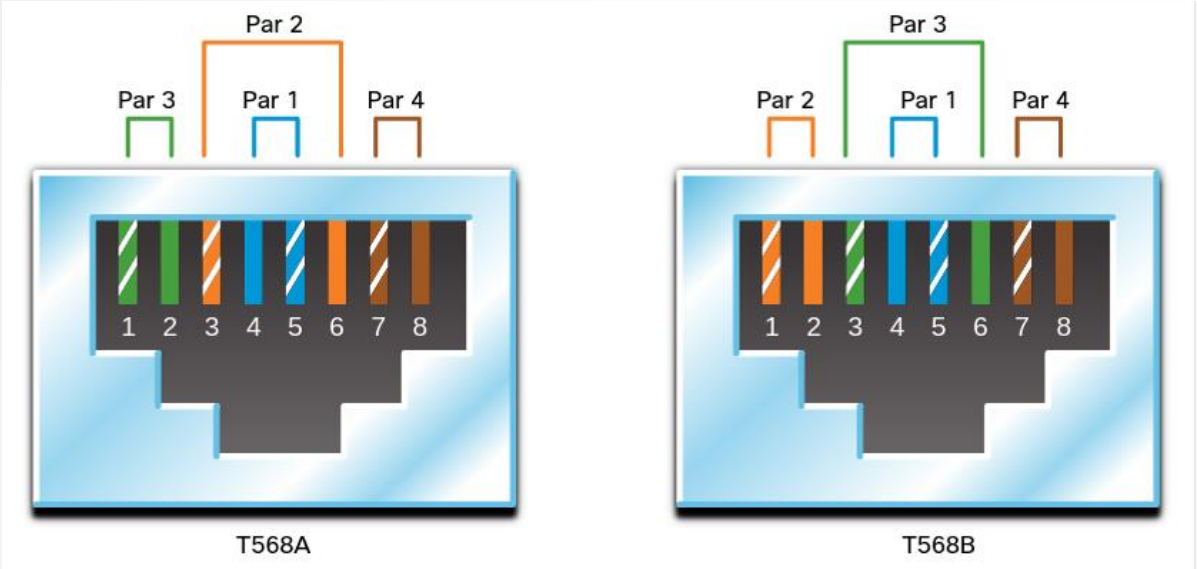
- **FTP**: blindagem simples, envolvendo todos os pares.
- **STP**: blindagem melhorada, envolvendo cada par separadamente.
- **SFTP ou SSTP**: blindagem robusta, envolvendo cada par separadamente adicionada a uma blindagem externa geral.




Capa
Braided Shield
Blindagem de Folha Metálica
Pares Trançados

PINAGEM PAR TRANÇADO

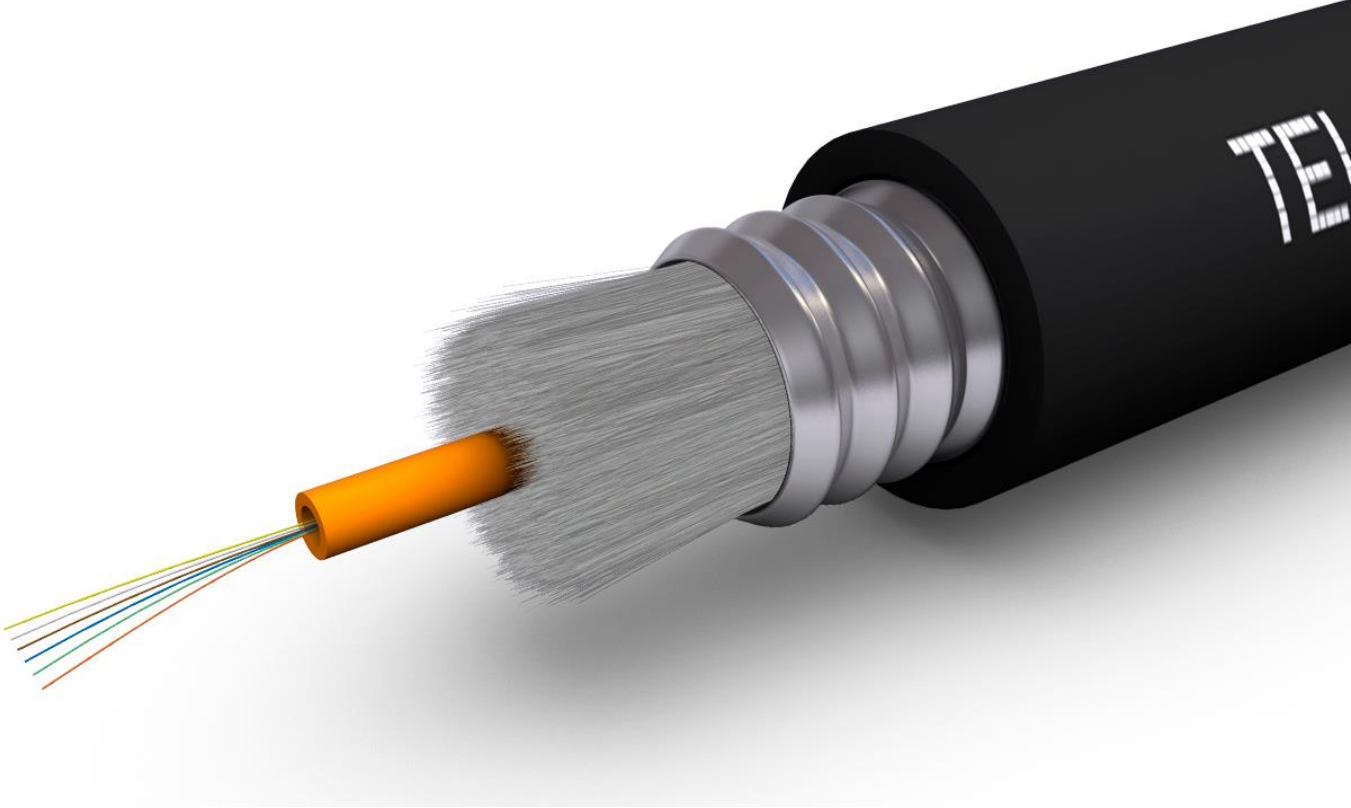
São dois tipos de cabos projetados para uso, o **direto**, mais comum, com **extremidades iguais**, que conecta dispositivos de camadas diferentes e o **cruzado**, com **extremidades diferentes**, que conecta dispositivos na mesma camada, porém é considerado legado, pois as tecnologias atuais de dispositivos detectam o tipo de cabo e autoconfigura a conexão.



FIBRA ÓPTICA

Tem alto custo, por isso é menos comum em redes do que cabeamento de cobre. Porém oferece **altas taxas de transferência**, **longas distâncias**, tem **menos atenuação** e é completamente **imune a interferências** EMI/RFI.

Fibras ópticas caracterizam-se por um filamento revestido internamento de vidro ou polímero formando um túnel espelhado com alta capacidade de transmissão de luz. A luz é emitida proveniente de laser ou LED e percorre toda a fibra refletindo na casca interna.

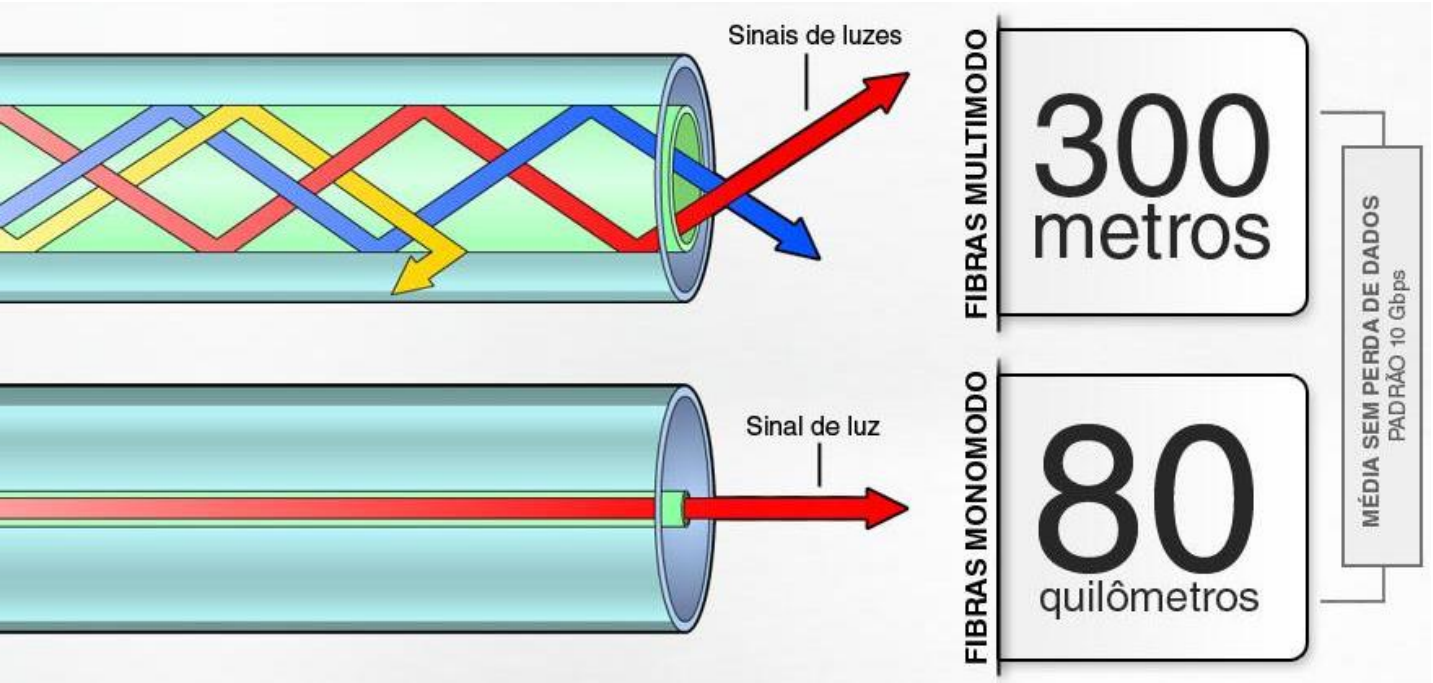

TE


Cabo
Revestimento
Camada de refração (125 µm)
Fibra ótica (62 µm)
Fibra de fortalecimento

MONOMODO E MULTIMODO

Fibras monomodo (SMF) tem um núcleo muito pequeno e utiliza tecnologia laser cara para emitir um só raio de luz na origem. São usadas em telefonia e serviços de TV por percorrerem **grandes distâncias**.

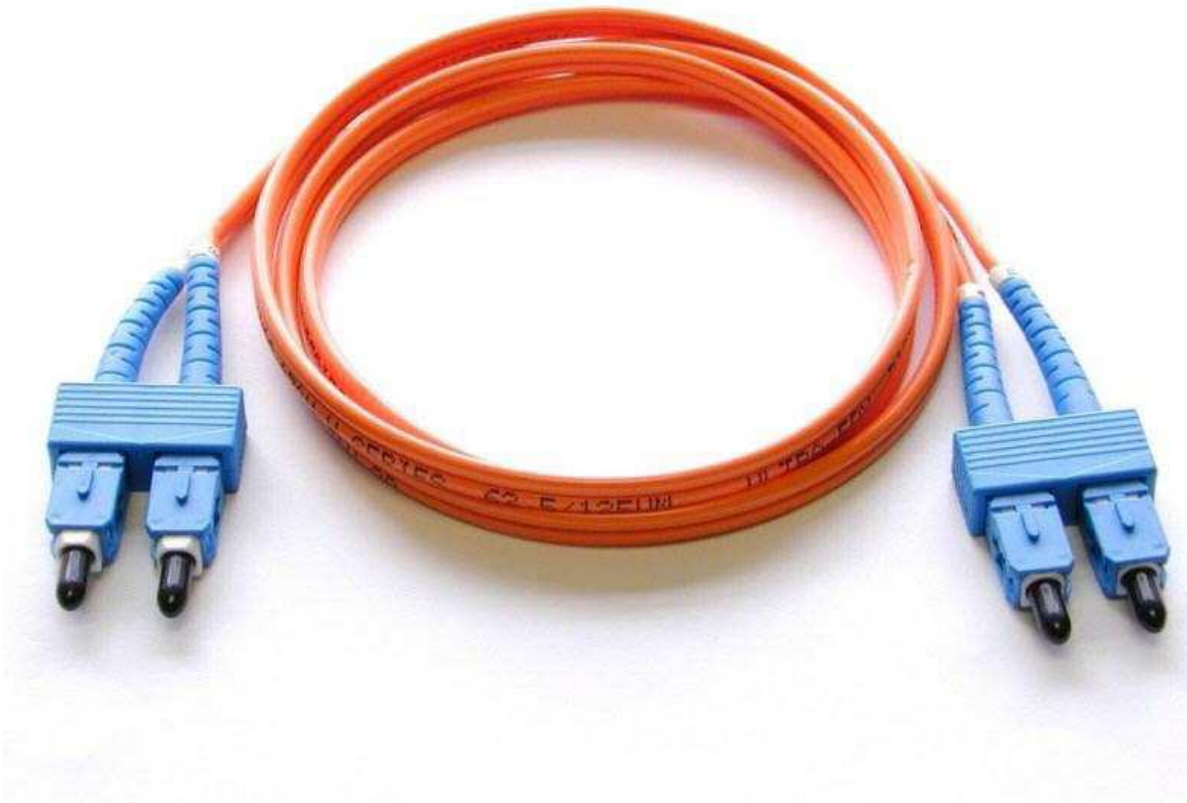
Já as **fibras multimodo** (MMF) aceitam vários feixes de luz (geralmente LED) em um núcleo maior, com dispersão maior e menores distâncias alcançadas. São populares nas LAN por serem acionadas com LED de **baixo custo**.


Sinais de luzes
Sinal de luz
FIBRAS MULTIMODO
300
metros
FIBRAS MONOMODO
80
quilômetros
MÉDIA SEM PERDA DE DADOS
PADRÃO 10 Gbps

APLICAÇÃO E CONECTORES

Fibras ópticas podem ser utilizadas em diversos setores como Redes Corporativas para interconexão de equipamentos pesados, **FTTH** para ambientes menores, Redes de Longo Curso para interconectar grandes distâncias e Cabos Submarinos para **distâncias transoceânicas**.

Possuem grandes variações de conectores, tanto macho quanto fêmea, variando para SMF e MMF. Alguns são o ST (formato cilíndrico para multimodo), SC (formato retangular, substituto do ST, para conexão em clientes), o LC (uma versão menor do SC) e o MT-RJ (derivado do RJ-45)

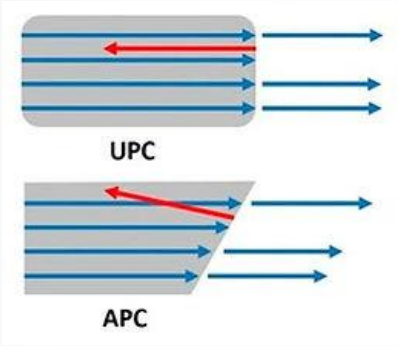



A
B

APLICAÇÃO E CONECTORES

Outra classificação é sobre conectores APC e UPC. Os conectores APC tem perda baixa de sinal (atenuação), transmitindo a grandes distâncias em alta velocidade, sendo também utilizados em instalações complexas. Tem maior custo e possui sempre a cor verde.

Já o conector UPC possui perda ligeiramente maior, mas ainda com boa taxa de transmissão, sendo utilizado em instalações simples. Tem menor custo e sempre será da cor azul



LCUPC LCAPC SCUPC SCAPC ST

E2000UPC E2000APC FCAPC FCUPC DINAPC

ESCOM - MM

ST - MM

SMA - MM

FC - MM

FC(PC) - SM

LC - MM

LC(PC) - SM

MTRJ - MM

SC(PC) - SM

SC - MM

ST - SM

E2000(APC) - SM

FC(APC) - SM

LC(APC) - SM

SC(APC) - SM

HMS - SM

COMPARAÇÃO FIBRA E UTP

Há muitas vantagens em usar fibra óptica, sendo atualmente a maioria dos ambiente empresarias com essa tecnologia, muito em função de não conduzirem eletricidade e possuírem **baixa atenuação**.

Implementação	Cabeamento UTP	Cabeamento Fibra Óptica
Largura de banda suportada	10Mbps – 10Gbps	10Mbps – 100Gbps
Distância	1 a 100 metros	1 a 100 KM
Imunidade a interferência	Baixa	Alto
Imunidade a perigos elétricos	Baixa	Alto
Custo da mídia e conectores	Baixo	Alto
Habilidades para instalação	Baixa	Alta

TRANSMISSÃO SEM FIO

Terceira maneira de se conectar a camada física, as redes sem fio oferecem mobilidade e comodidade no uso, transportando sinais eletromagnéticos representando os dígitos binários. Porém há algumas limitações:

- **Área de cobertura**: a transmissão funciona bem em ambientes abertos, mas alguns materiais de construção nos prédios e estruturas podem limitar a eficácia.
- **Interferência**: suscetível a interferência por dispositivos emissores de ondas e algumas luzes fluorescentes.
- **Segurança**: principal componente da administração da rede sem fio, pode sofrer com usuários não autorizados, captando sinal indevidamente.
- **Meio compartilhado**: opera em halfduplex, onde apenas um dispositivo transmite por vez, além do meio ser compartilhado com todos, comprometendo a largura de banda

PADRÕES SEM FIO

Os padrões sem fio abrangem a camada física e de enlace de dados, englobando a codificação dos dados para o **sinal de rádio**, frequência/potência da transmissão, recepção e decodificação do sinal e projeto/construção de antenas.

- **Wi-fi (IEEE 802.11)**: LAN sem fio (WLAN) utiliza um protocolo baseado em **contenção para colisões** e prover acesso múltiplo (CSMA/CA). A NIC sem fio deve ouvir primeiro antes de transmitir para determinar se o canal está limpo.
- **Bluetooth (IEEE 802.15)**: rede pessoal sem fio (WPAN), usa um processo de **emparelhamento** para comunicação de dispositivos entre 1 e 100 metros.
- **Zigbee (IEEE 802.15.4)**: semelhante ao Bluetooth, porém para baixa taxa de transferência, curto alcance e baixo consumo de energia, usado principalmente na **IoT**.
- **WiMAX (IEEE 802.16)**: acesso a banda larga sem fio, com topologia **multicast**.

LAN SEM FIO

O padrão WLAN é bastante comum nas redes e ambientes. Sua simplicidade de implementação é uma forte característica, já que requer poucos dispositivos:

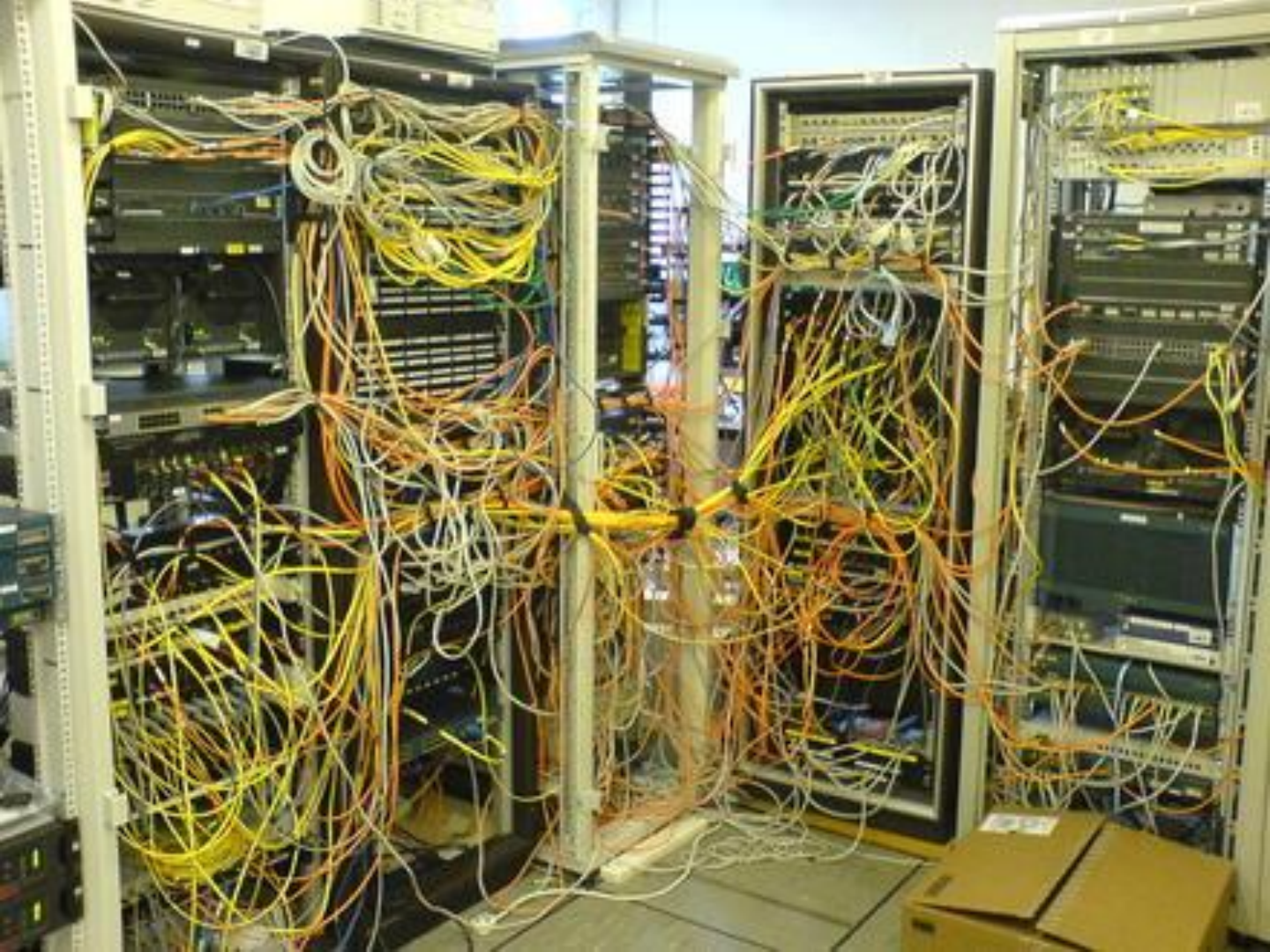
- **Ponto de Acesso (AP)**: emite o sinal sem fio, interconectando-se com a infraestrutura de rede existente. Alguns equipamentos, como roteadores domésticos fazem a função conjunta de AP, além das funções de roteamento.
- **NIC sem fio ou Adaptadores**: irão captar o sinal transmitido na faixa adequada. Algumas NICs trabalham apenas em 2.4 Ghz, outras captam também o sinal em 5Ghz.

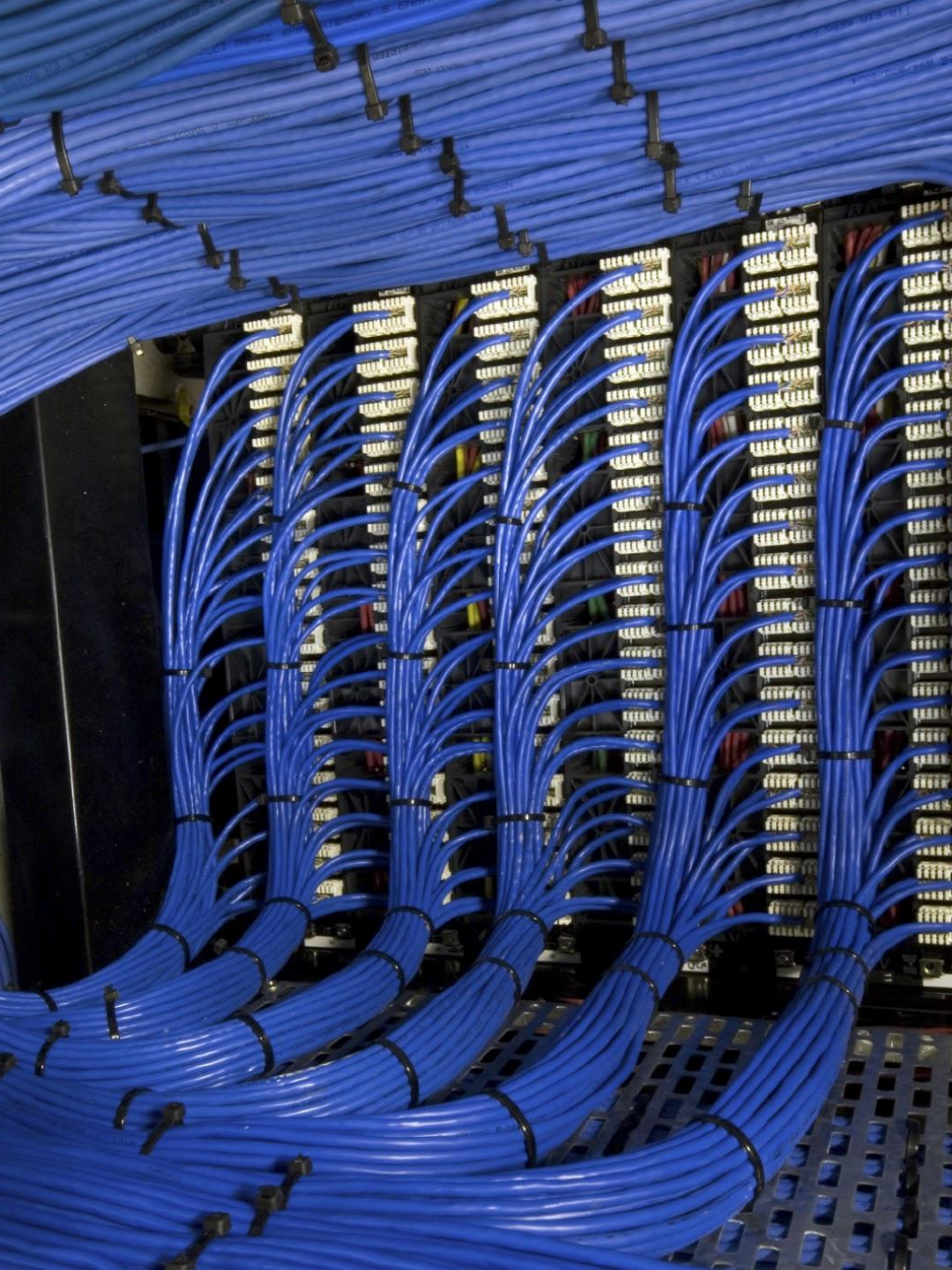
CABEAMENTO ESTRUTURADO

Cabeamento estruturado é um **conjunto de técnicas e procedimentos** para instalar uma rede cabeada de forma ideal, com organização e controle, considerando normas e padrões existentes em outras redes pelo mundo.

Facilita a manutenção, além de prevenir falhas e otimizar o desempenho. **Gerar documentação é essencial.**

Um bom cabeamento estruturado visa garantir que todo o projeto de infraestrutura seja plenamente capaz de operar por um período mínimo de 10 anos suportando, além dos processos, os servidores da rede local, a quantidade de switches, roteadores e sua extensão





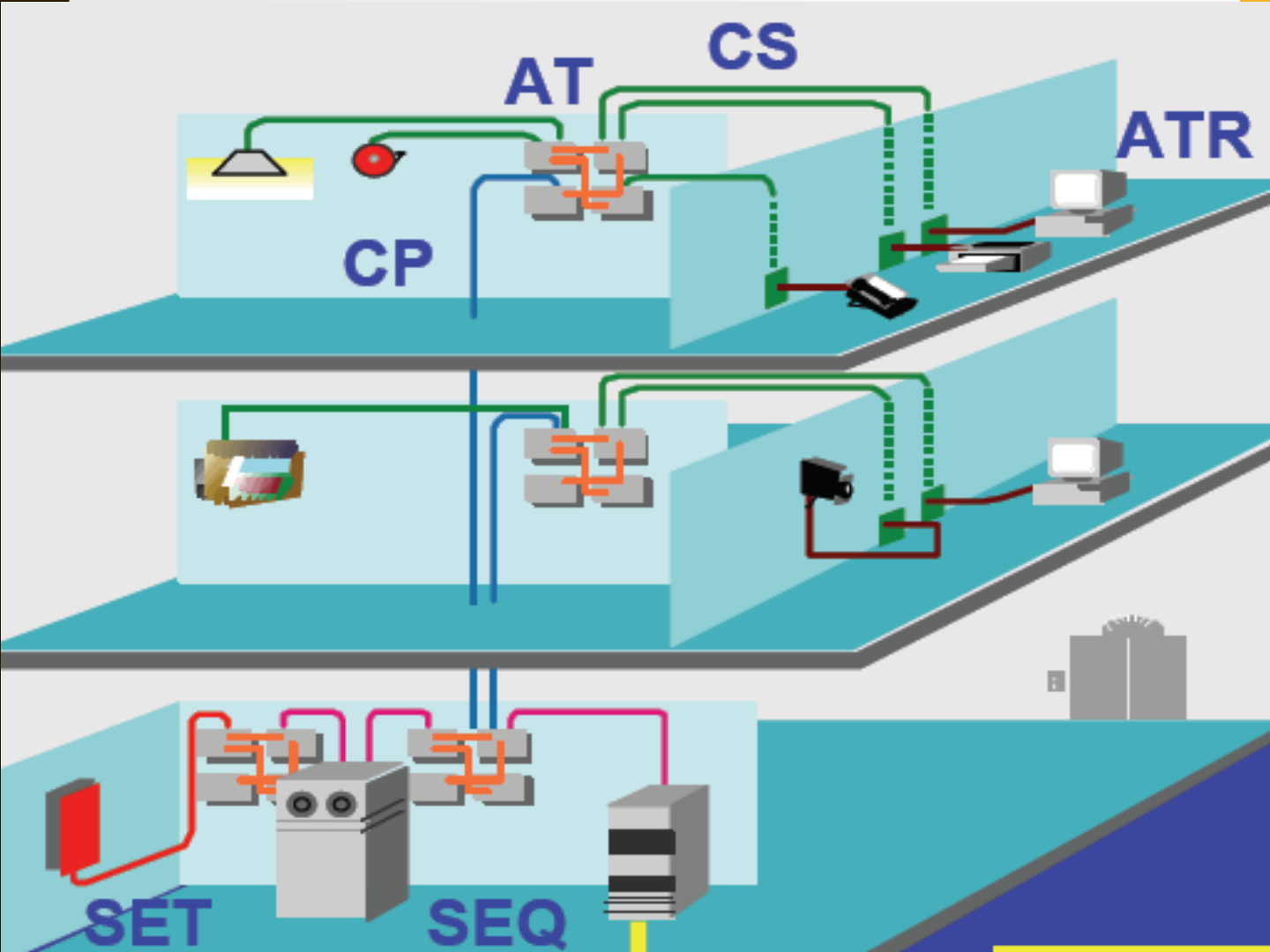
SUBSISTEMAS DE CABEAMENTO ESTRUTURADO

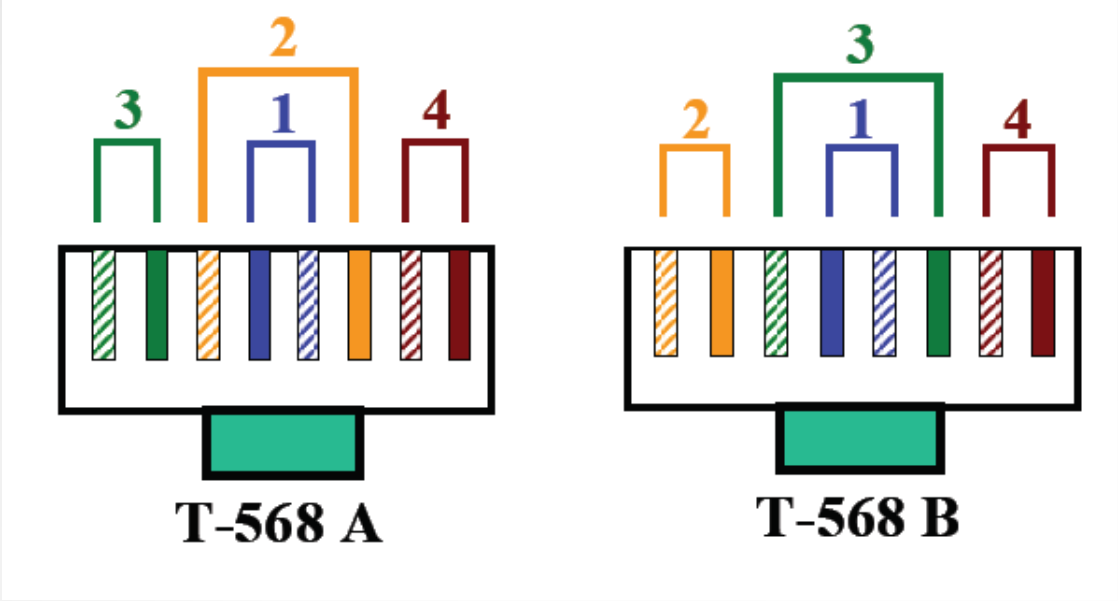
O estudo e aplicação de cabeamento estruturado se divide em partes chamadas **subsistemas**, com normas e orientações específicas para cada um deles.

- **SET**: sala de **chegada de cabos externos** como linhas de telefone, links de Internet, cabos ligando o prédio a outros prédios, etc. Sua sinalização é importante em projetos de cabeamento estruturado, pois trata-se de **onde começa a rede**.
- **SEQ**: É o "**cérebro**" da rede, onde ficam os principais equipamentos ativos, entre servidores, roteadores e switches. Deve ser protegida fisicamente, com acesso controlado de pessoas. As tarefas devem ser feitas, preferencialmente, de modo remoto.

SUBSISTEMAS DE CABEAMENTO ESTRUTURADO

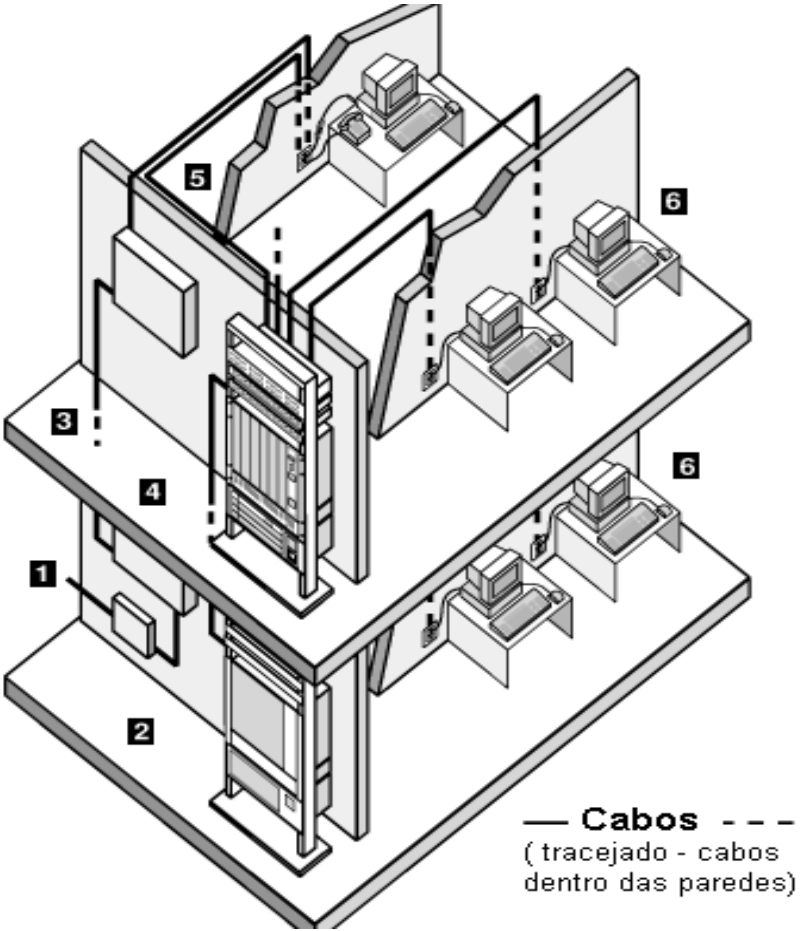
- **AT**: Funciona como uma **caixa de distribuição** do cabeamento de rede para os andares do prédio. Normalmente é acondicionado em um rack de rede. **Cada AT pode servir até 1000m² de área útil**.
- **ATR**: Destino final do cabeamento, **onde o usuário conecta seus serviços** de telecomunicação (TV, Telefone, FAX, PC, etc). Recomenda-se uma distância máxima de 10 metros da tomada (PT) até os equipamentos do usuário. Cada PT a 30 cm do chão.
- **CP**: Liga a **Sala de Equipamentos (SEQ) ao Armário de Telecomunicações (AT)**. Recomendada uma distância máxima de 90 metros
- **CS:** Liga o **Armário de Telecomunicações (AT) a Área de Trabalho (ATR)**. Recomendada uma distância máxima de 90 metros.

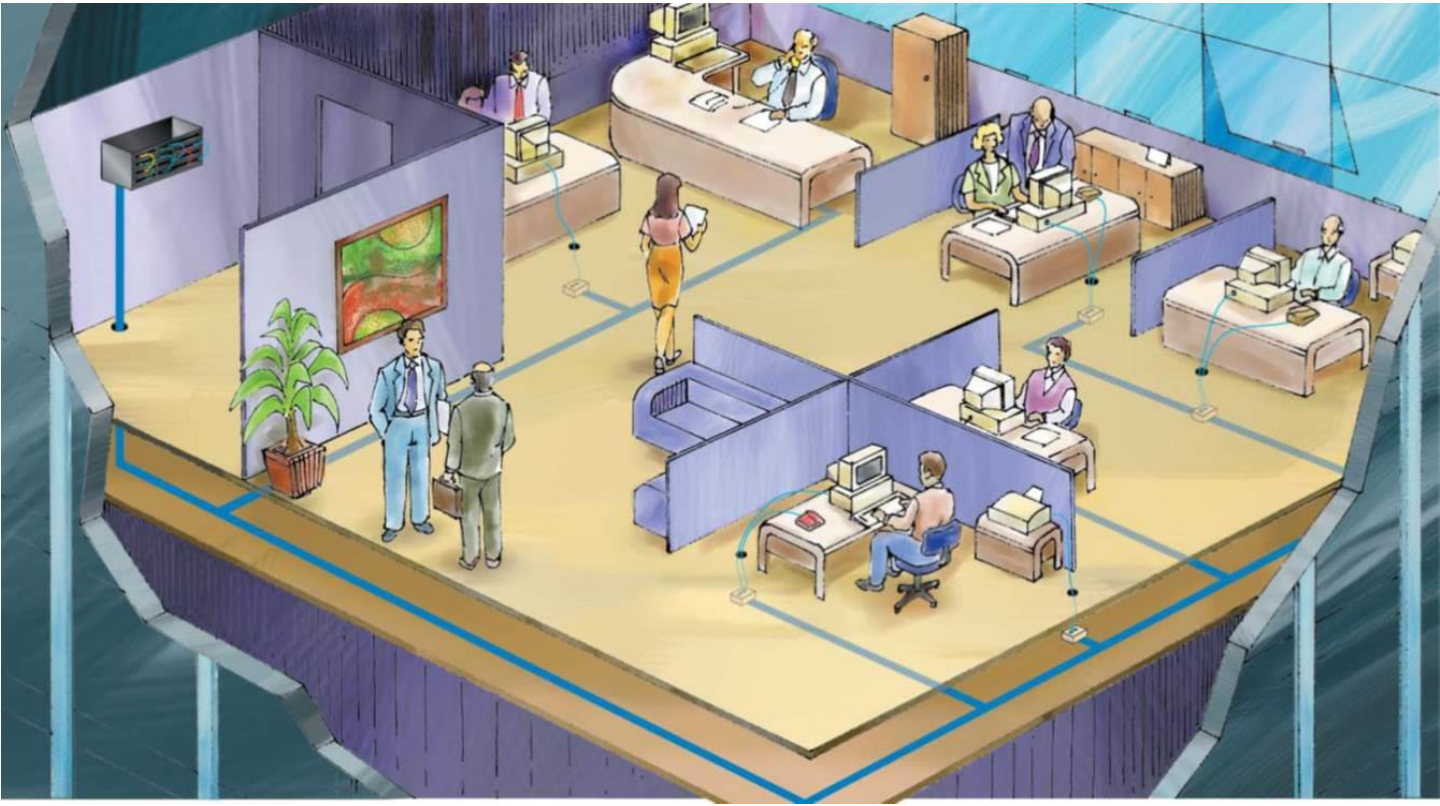

AT
CS
ATR
CP
SET
SEQ



MONTAGEM DE CABOS

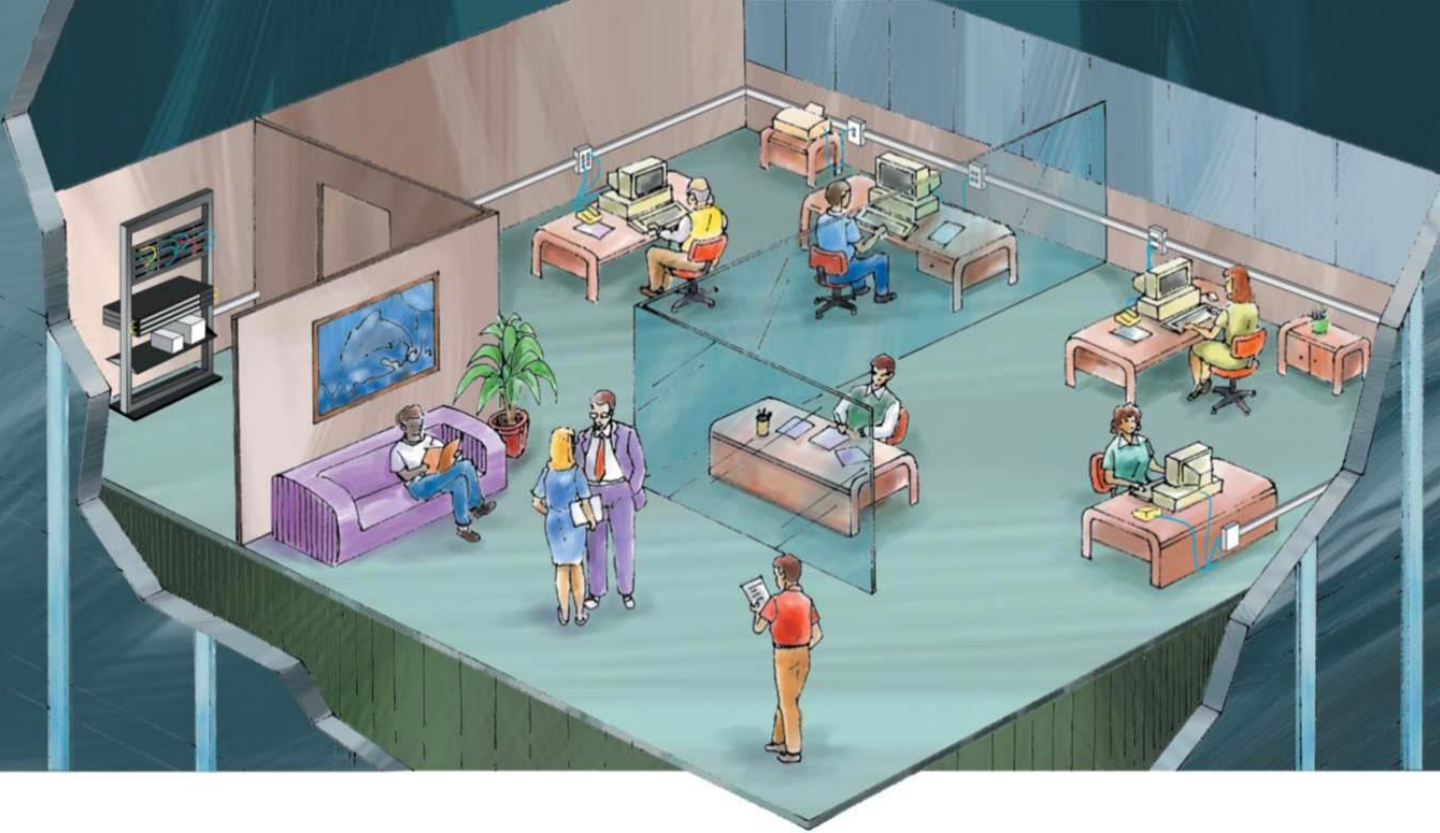
Devem ser preparados em um dos dois padrões EIA/TIA existentes. A ponta do cabo e a tomada de rede **devem ter o mesmo padrão**.


5
6
3
6
4
1
2
— Cabos - - -
(tracejado - cabos
dentro das paredes)



PISO FALSO

FORRO FALSO



CANALETAS APARENTES

NORMAS DE CABEAMENTO ESTRUTURADOS

- **ABNT/NBR 14565**: norma brasileira, de julho de 2000, baseada nas normas ANSI EIA/TIA 568B, 569 e 606. Trata de normas para montagem de cabos, estruturação e uso dos dispositivos de rede.
- **ANSI EIA/TIA 568B**: elaborada em Junho de 1991 e revisada em Outubro de 1995, trata de **cabeamento básico para edifícios comerciais**. Na revisão, incluiu-se normas para as tomadas, conexão entre prédios e cabeamento em *campus*. Além disso, atualizou as normas de cabos par trançado.
- **ANSI EIA/TIA 569**: elaborada em Fevereiro de 1998, trata de caminhos e espaços de telecomunicações para edifícios comerciais. Inclui também padrões de projeto para construção de rede, os **caminhos que a rede deve percorrer** e onde ficarão os equipamentos.

NORMAS DE CABEAMENTO ESTRUTURADOS

- **ANSI EIA/TIA 606**: elaborada em Maio de 2002, é uma norma para administração de **infraestrutura de redes**. Foco na documentação da rede.
- **ANSI EIA/TIA 607**: Elaborada em Outubro de 2002, especifica padrões de projeto para instalação de sistemas de **aterramento elétrico**.

NOTA: Temos ainda as **RFC, que embora não façam parte das normas de cabeamento estruturado,** funcionam como um manual para uma tecnologia de rede. Todos os documentos podem ser consultados em http://www.ietf.org/rfc.html

CAMADA DE ENLACE DE DADOS

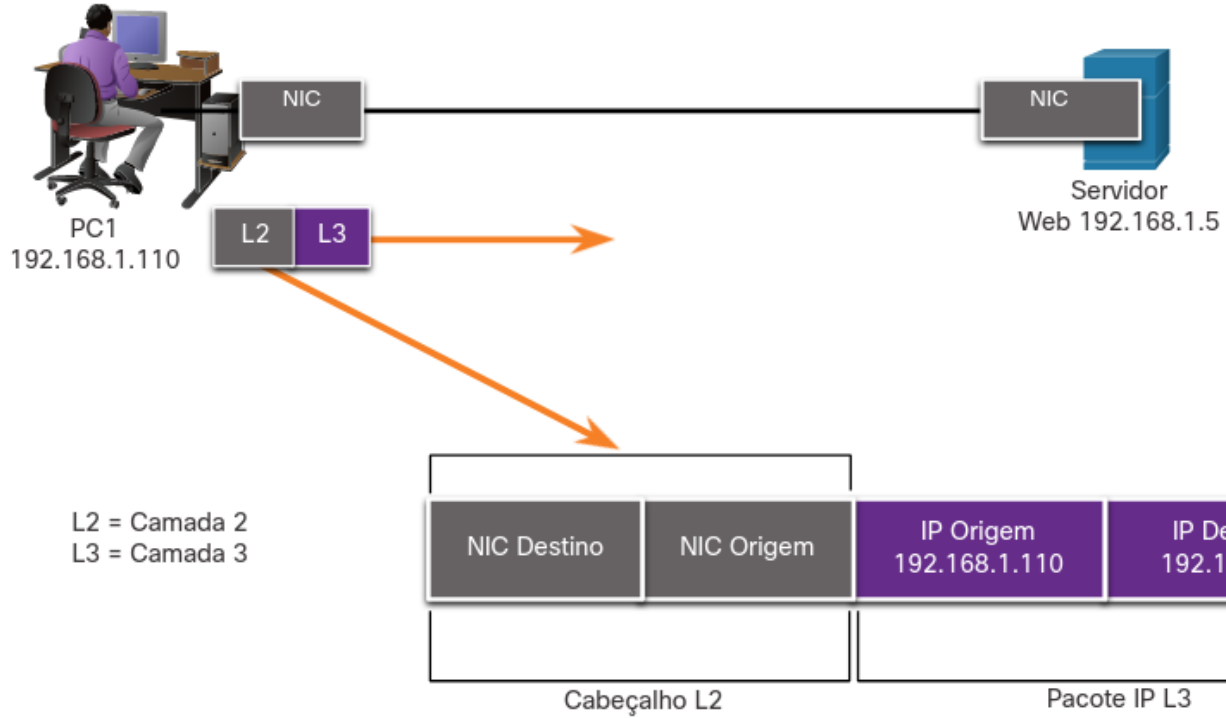

tyco
Electronics
AMP
NETCONNECT
24TP Auto
MDI-X Switch
Power
LK/ACT
LK/ACT
2 4 6 8 10 12 14 16 18 20 22 24
1 3 5 7 9 11 13 15 17 19 21 23

PROPÓSITOS

A camada de enlace de dados **prepara os dados da rede para serem enviados** pela camada física, entre outras tarefas:

- Permite que as camadas superiores acessem a mídia, já que elas não tem ciência do tipo de mídia que está sendo usada para encaminhar os dados.
- Aceita dados da camada 3 os encapsula em quadros da Camada 2.
- Executa detecção de erros e rejeita qualquer quadro corrompido.

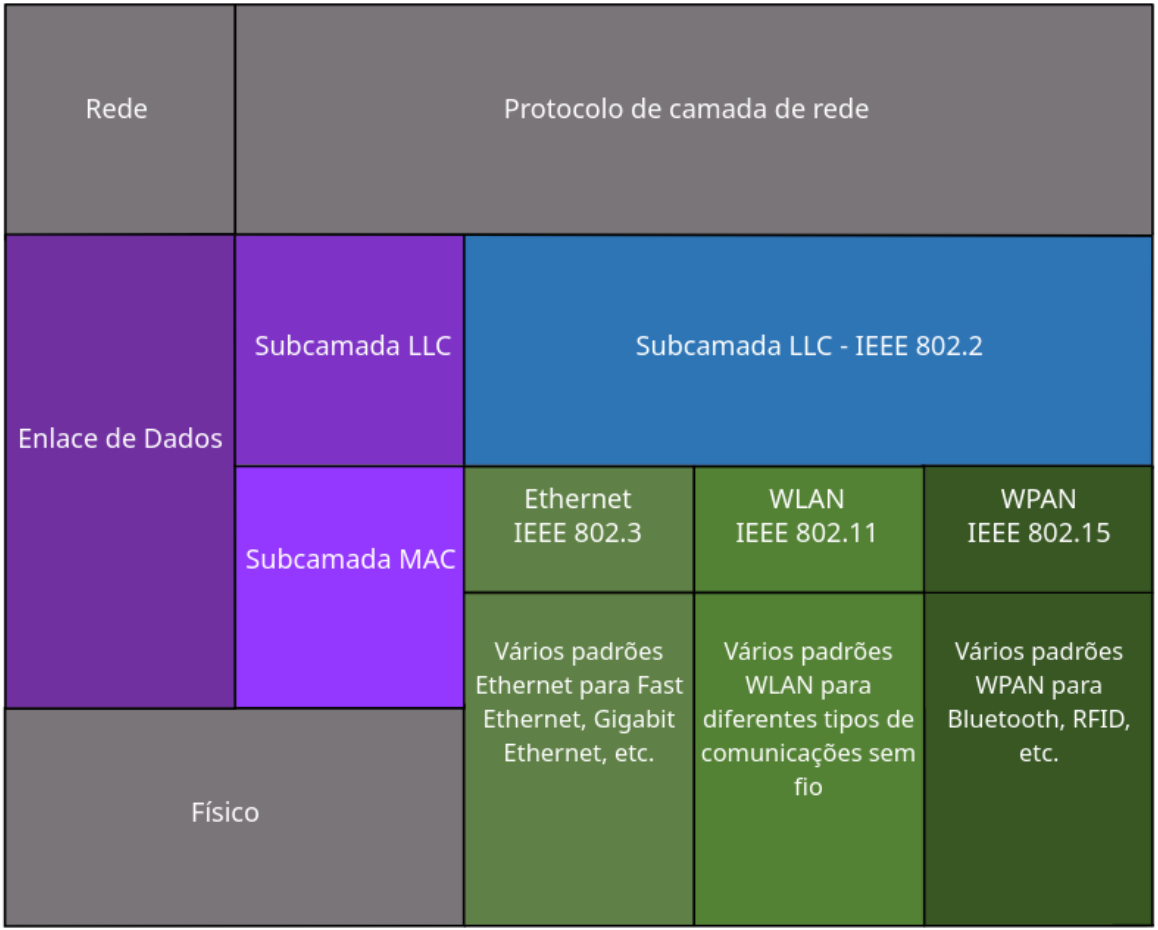
A camada de enlace de dados faz a interface entre a camada de rede e camada física, não importando as tecnologias e protocolos envolvidos. Ela simplesmente adiciona informações de destino em um pacote camada 3 e converte para um formato suportado pela camada 1.


NIC
NIC
Servidor
Web 192.168.1.5
PC1
192.168.1.110
L2
L3
L2 = Camada 2
L3 = Camada 3
NIC Destino
NIC Origem
IP Origem
192.168.1.110
IP Destino
192.168.1.5
Cabeçalho L2
Pacote IP L3

SUBCAMADAS

Os padrões IEEE 802 são específicos para LAN, MAN, WLAN e WPAN. A camada de enlace de dados tem outras duas subcamadas.

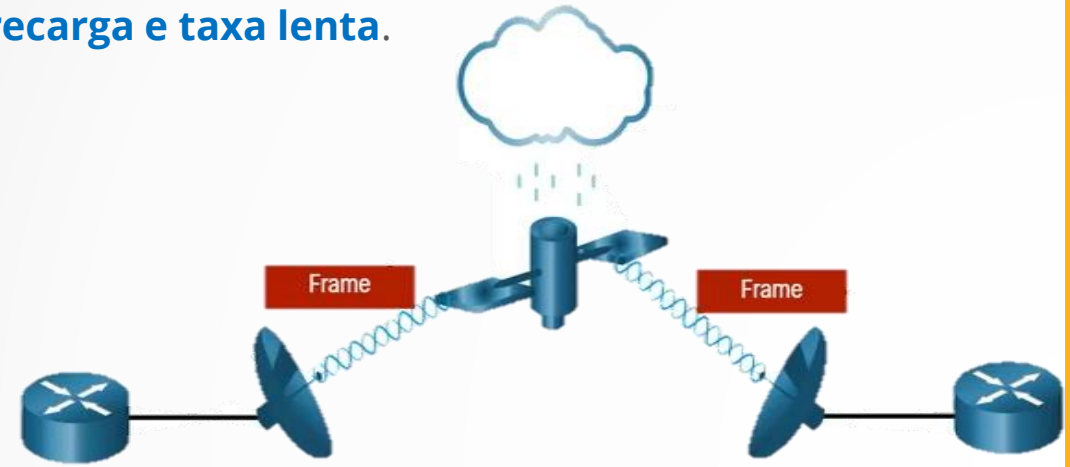
- **LLC**: esta subcamada que **faz efetivamente a comunicação** entre o software de rede (L3) e o hardware do dispositivo (L1), colocando no quadro qual o protocolo de rede utilizado, para interoperabilidade. Ao receber o pacote camada 3, adiciona informações de controle camada 2 para auxiliar na entrega ao destino.
- **MAC**: encapsula os dados recebidos da camada 3 e faz o **controle de acesso a mídia** para as comunicações half-duplex. Fornece também um **endereço de camada 2** e tem integração com várias tecnologias da camada física. Faz também a detecção de erros.


Rede
Protocolo de camada de rede
Enlace de Dados
Subcamada LLC
Subcamada LLC - IEEE 802.2
Subcamada MAC
Ethernet
IEEE 802.3
WLAN
IEEE 802.11
WPAN
IEEE 802.15
Vários padrões Ethernet para Fast Ethernet, Gigabit Ethernet, etc.
Vários padrões WLAN para diferentes tipos de comunicações sem fio
Vários padrões WPAN para Bluetooth, RFID, etc.
Físico

O QUADRO L2

O protocolo de enlace de dados é **responsável pela comunicação NIC-para-NIC na mesma rede**. O quadro gerado tem basicamente 3 partes, o **cabeçalho**, os **dados** e o **trailer**. A estrutura geral do quadro pode variar, conforme a rede, a tecnologia, topologia e protocolos envolvidos.

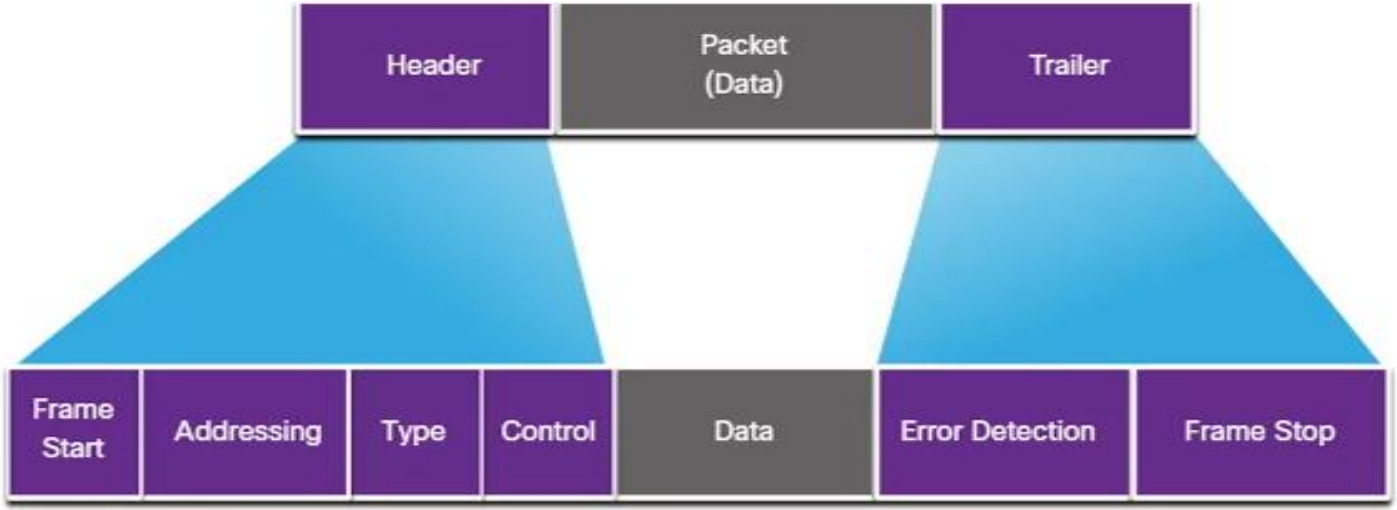
Em ambientes frágeis, mais controles são necessários para garantir a entrega, tornando o cabeçalho e o trailer maiores para acomodar mais informações. Quanto **mais esforço** na entrega, **mais sobrecarga e taxa lenta**.



O QUADRO L2

Apesar de protocolos diferentes poderem gerar quadros diferente, os campos de um quadro genérico incluem:

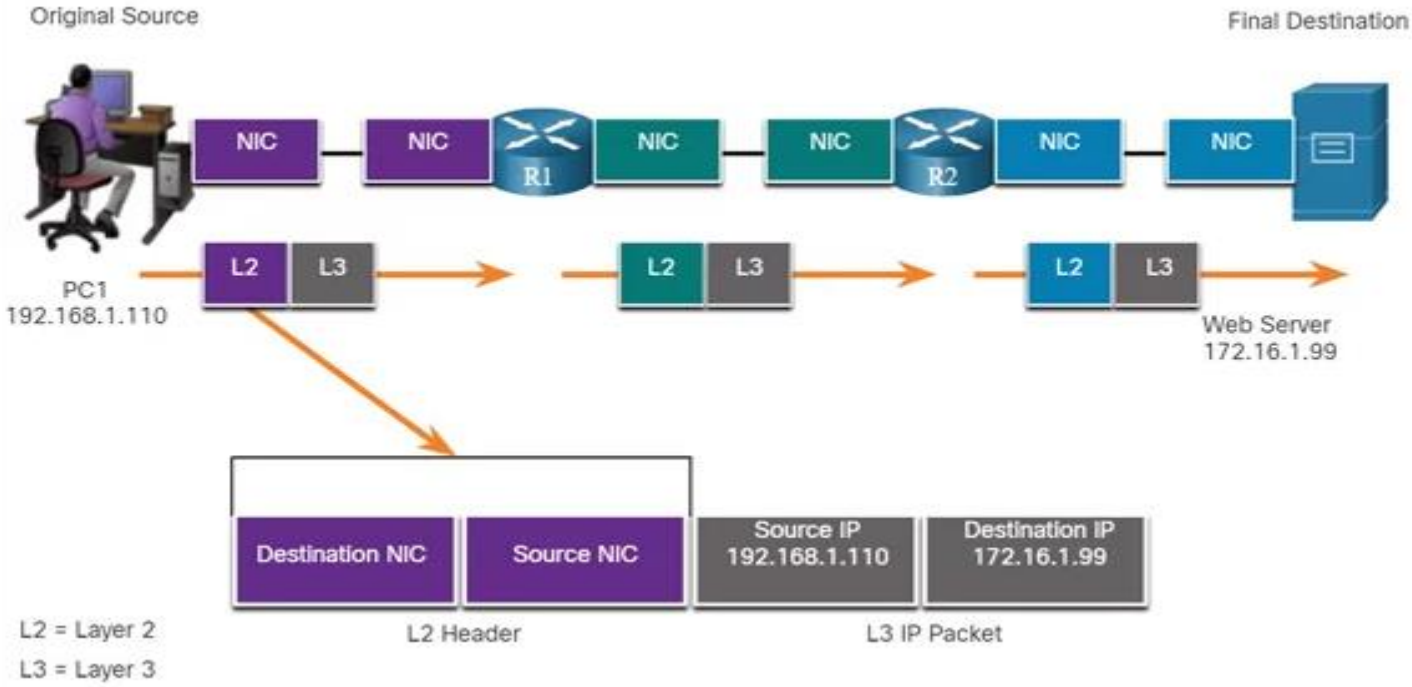
- **Início e Parada:** indicam os limites de início e fim do quadro.
- **Endereçamento**: endereços de camada 2 de origem e destino.
- **Tipo**: identifica o protocolo da camada 3.
- **Controle**: identifica serviços especiais de controle de fluxo, como o QoS, para receberem prioridade de transporte.
- **Dados**: contém a carga útil do quadro (incluindo as estrutura recebida das camadas superiores).
- **Detecção de erro**: incluído após os dados para formar o trailer, utiliza processos de comparação para determinar se o quadro está com erro.


Header
Packet
(Data)
Trailer
Frame
Start
Addressing
Type
Control
Data
Error Detection
Frame Stop

ENDEREÇAMENTO L2

Os endereços L2 são **apenas para entrega local**, isso porque não há uma hierarquia como os endereços de camada 3, de modo que não é possível o dispositivos encaminhar para uma rede remota.

Isso faz com que, **a cada salto, o quadro seja endereçado novamente** com a origem sendo quem envia o quadro e o destino sendo quem o recebe.

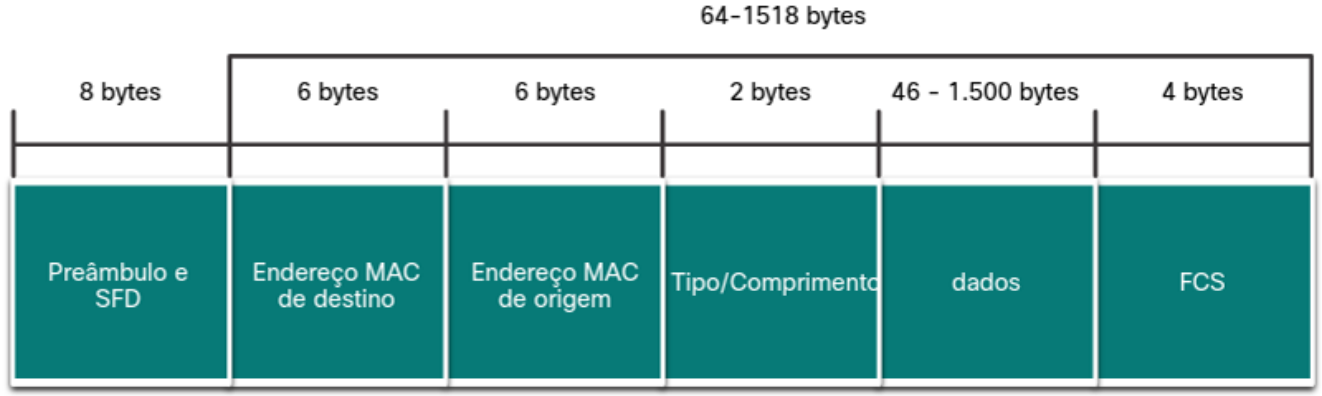

Original Source
Final Destination
NIC
NIC
R1
NIC
NIC
R2
NIC
NIC
L2
L3
L2
L3
L2
L3
PC1
192.168.1.110
Web Server
172.16.1.99
Destination NIC
Source NIC
Source IP
192.168.1.110
Destination IP
172.16.1.99
L2 Header
L3 IP Packet
L2 = Layer 2
L3 = Layer 3

QUADRO L2 ETHERNET

O tamanho **mínimo** do quadro é **64 bytes** e o **máximo 1518 bytes**, descartando o campo de preâmbulo e início do quadro. Quadros fora da faixa podem ser resultados de colisões e são descartados. Quadros com mais de 1500 bytes são chamados também de 'jumboframe' ou 'baby giant'.

- **Preâmbulo/SFD**: marca o início do quadro e lança um aviso ao receptor de que um novo quadro está chegando.
- **MAC**: endereço camada 2 de origem e destino
- **Tipo**: valor em hexadecimal que identifica o protocolo de camada superior, os valores comuns são 0x800 (IPv4), 0x86DD (IPv6) e 0x806 (ARP)
- **Dados**: geralmente um pacote IPv4 encapsulado.
- **FCS**: o dispositivo emissor faz um cálculo e envia junto ao quadro, o receptor faz o mesmo cálculo para comparação e detecção de erros.

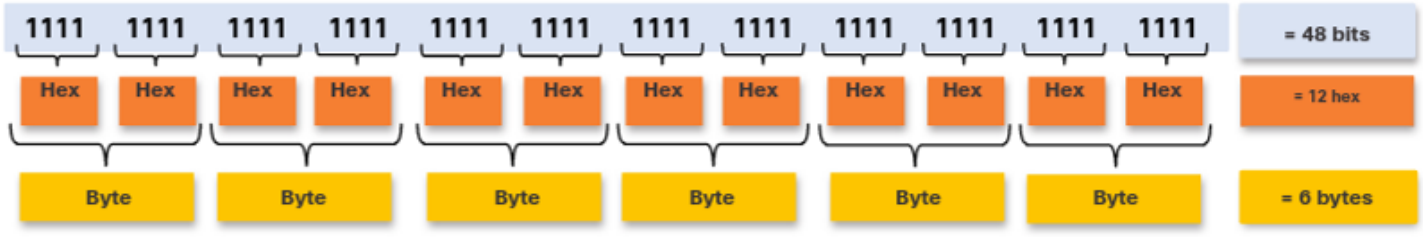
Campos do quadro Ethernet



O ENDEREÇO L2

O endereço de camada 2, chamado de **endereço MAC**, é composto por **48 bits**, expresso utilizando **12 valores hexadecimais**, ou seja, um tamanho de 6 bytes. No endereço, um grupo de zeros a esquerda é usado para completar o valor de 8 bits, dessa forma o valor 0A seria representado por 0000 1010.

Pode ser precedido também pela notação 0x (0x73) para diferenciar de valores decimais. Ou por subscript 16, com o número seguido de H (73H).

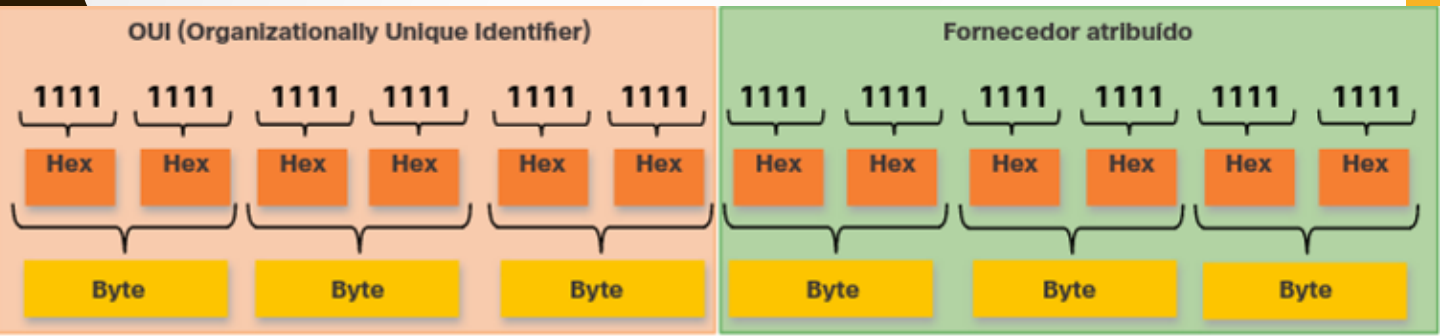


Decimal	Binário	Hexadecimal
0	0000 0000	00
1	0000 0001	01
2	0000 0010	02
3	0000 0011	03
4	0000 0100	04
5	0000 0101	05
6	0000 0110	06
7	0000 0111	07
8	0000 1000	08
10	0000 1010	0A
15	0000 1111	0F
16	0001 0000	10
32	0010 0000	20
64	0100 0000	40
128	1000 0000	80
192	1100 0000	C0
202	1100 1010	CA
240	1111 0000	F0
255	1111 1111	FF

O ENDEREÇO L2

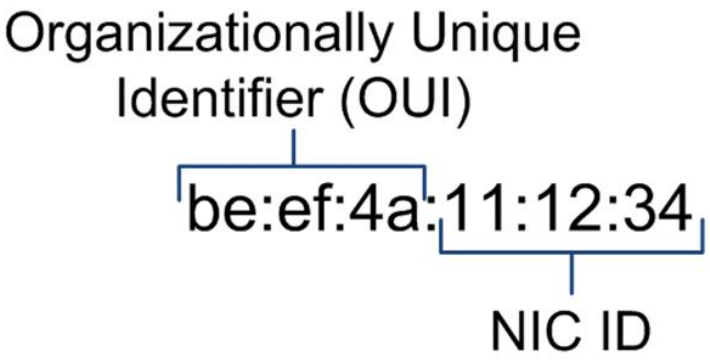
O endereço MAC é utilizado para **identificar o dispositivo dentro do mesmo segmento de rede local**. Eles devem ser exclusivos da NIC dentro do segmento, para isso há um regra de numeração.

Todos os fornecedores se registram no IEEE para obter uma numeração exclusiva de 3 bytes (24 bits) chamado de **OUI**. De modo que, ao fabricar uma nova NIC, o fornecedor define o endereço da seguinte forma.



Por exemplo, se a determinado fabricante possui o número OUI como BE-EF-4A, ao fabricar uma nova NIC, **é de sua responsabilidade garantir que não haja repetição** nos endereços, atribuindo um número exclusivo como 11-12-34.

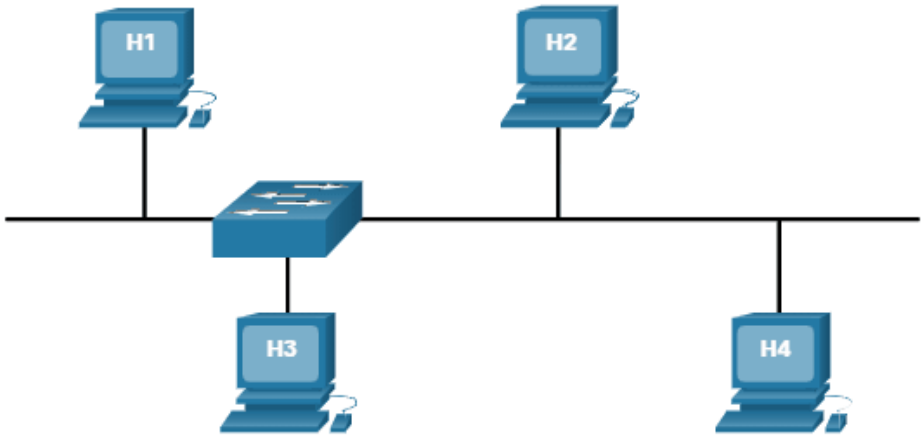
Embora isso possa acontecer, demandando uma troca de NIC ou modificação do endereço via software.



PROCESSAMENTO DE QUADROS

Nos modernos sistemas operacionais e NICs, **é possível alterar o endereço MAC via software**, para certas finalidades. Por isso, a filtragem ou controle de tráfego por MAC não é mais tão seguro e eficaz.

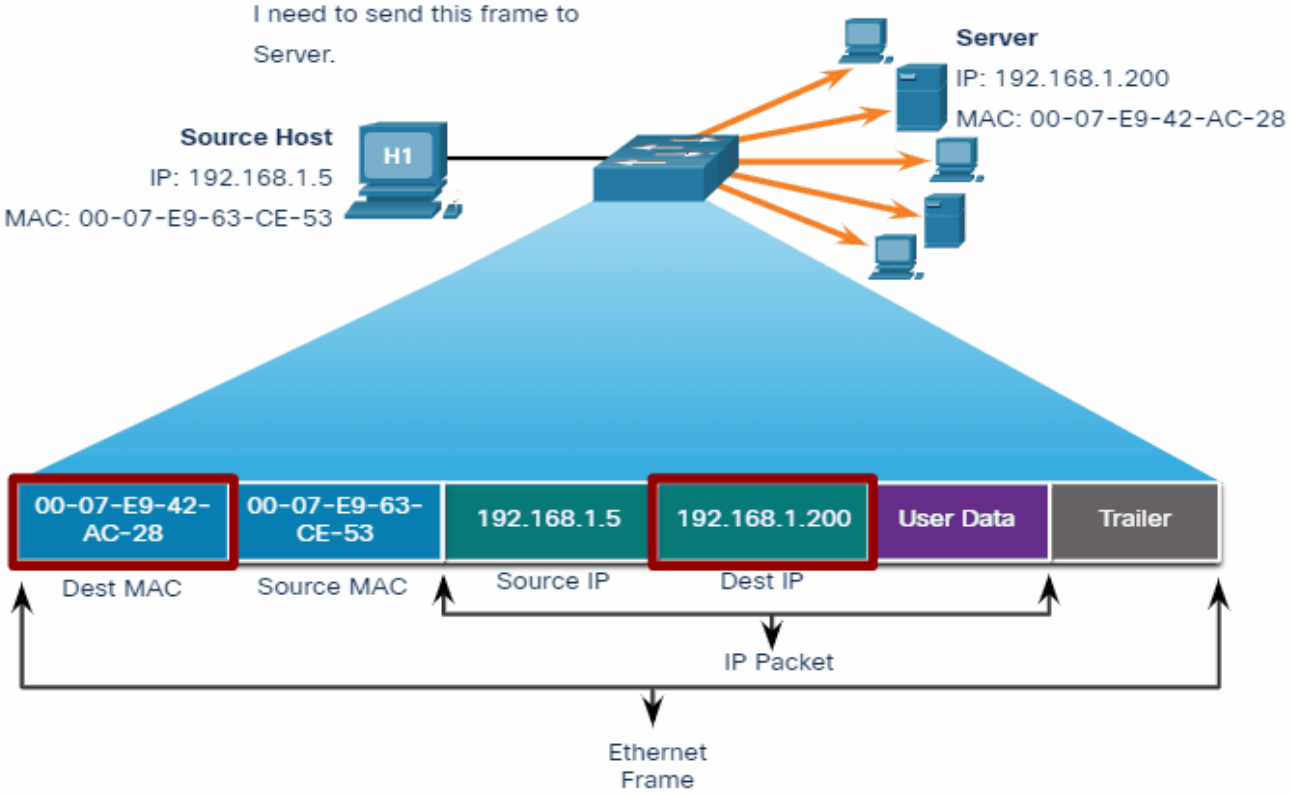
Quando uma NIC recebe um quadro, examina o endereço de destino para saber se o quadro lhe pertence, descartando o quadro em caso contrário. Em caso positivo, a NIC envia o quadro para as camadas superiores para desencapsulamento.

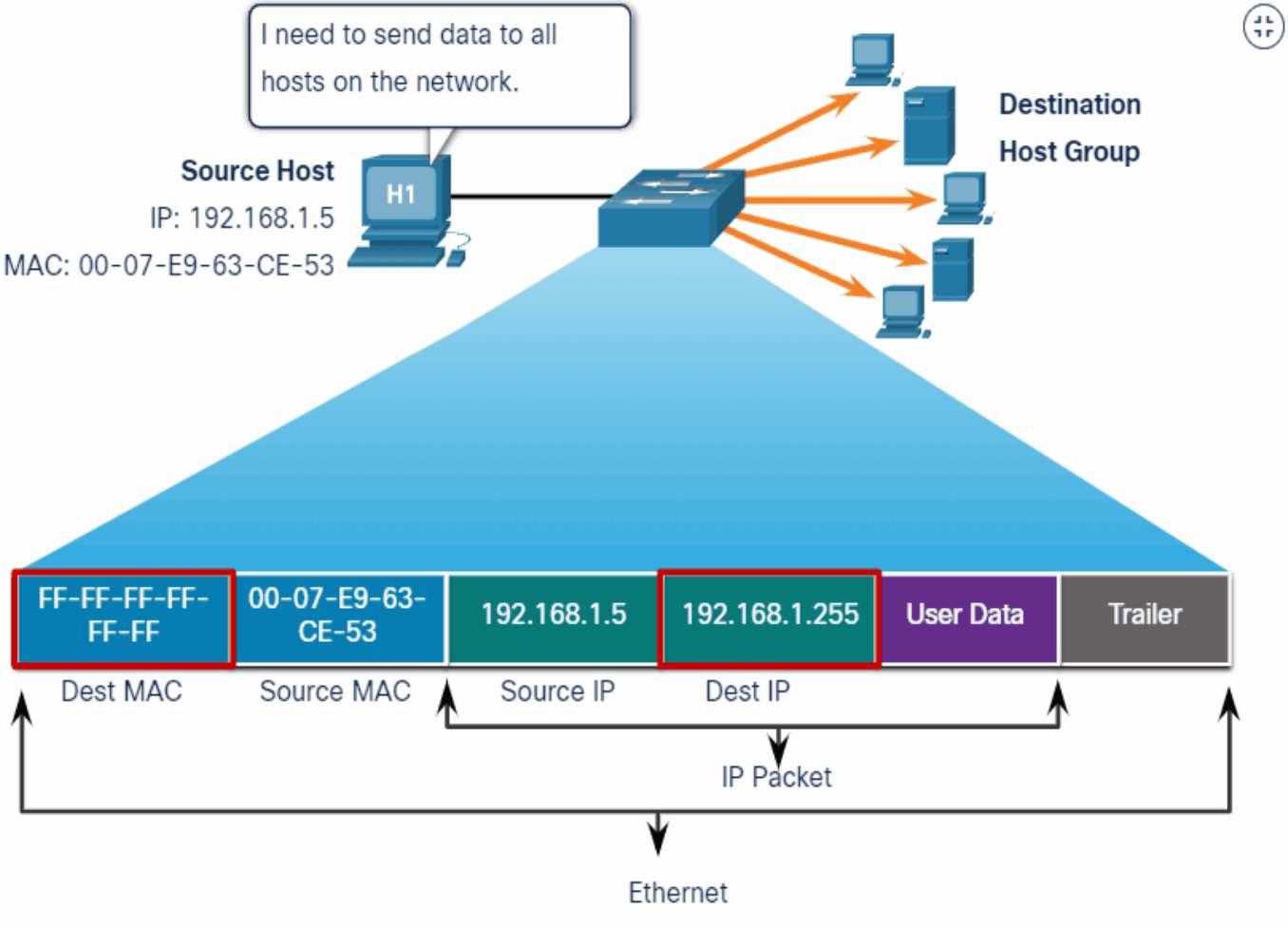

H1
H2
H3
H4

COMUNICAÇÕES L2

Os endereços de camada 2 para unicast, multicast e broadcast são diferentes.

- **Unicast**: é quando o quadro é enviado para um único dispositivo final de destino, com o endereço MAC deste. Um axioma é que o endereço MAC de origem deve ser sempre unicast.
- **Broadcast**: contém o endereço FF-FF-FF-FF-FF-FF e é distribuído por todas as portas do Switch, exceto a de entrada, sendo recebido e processado por todos os dispositivos daquela rede local. O roteador não encaminha pacotes broadcast.
- **Multicast**: são processados por um grupo de hosts específicos. O Switch distribui por todas as portas, exceto a de entrada. Um roteador só encaminhará pacotes multicast se estiver configurado pra isso.


I need to send this frame to Server.
Server
IP: 192.168.1.200
MAC: 00-07-E9-42-AC-28
Source Host
IP: 192.168.1.5
MAC: 00-07-E9-63-CE-53
H1
00-07-E9-42-AC-28
00-07-E9-63-CE-53
192.168.1.5
192.168.1.200
User Data
Trailer
Dest MAC
Source MAC
Source IP
Dest IP
IP Packet
Ethernet Frame


I need to send data to all hosts on the network.
Source Host
IP: 192.168.1.5
MAC: 00-07-E9-63-CE-53
H1
Destination Host Group
FF-FF-FF-FF-FF-FF
00-07-E9-63-CE-53
192.168.1.5
192.168.1.255
User Data
Trailer
Dest MAC
Source MAC
Source IP
Dest IP
IP Packet
Ethernet

O SWITCH

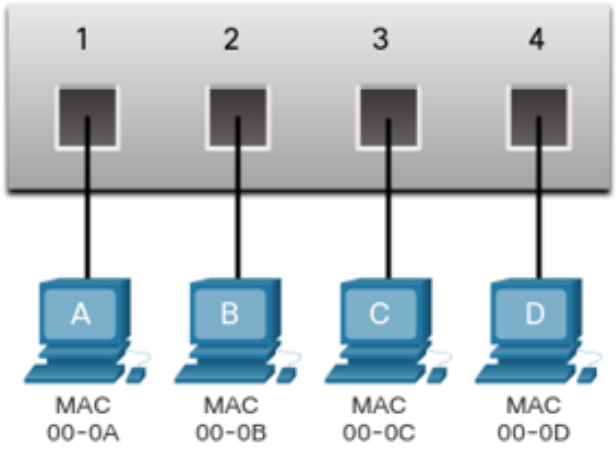
O switch é o **principal dispositivo** que trabalha na camada 2, filtrando e encaminhando pacotes, usando endereços MAC para tomada de decisão.

Não tem qualquer conhecimento da camada 3 ou dos dados do pacote, toma decisões apenas com base no endereço MAC.

O Switch examina sua tabela para definir o encaminhamento do quadro; a tabela inicialmente é vazia.

A tabela MAC também é chamada de “CAM”.

Tabela de endereços MAC	
Porta	**Endereço MAC**



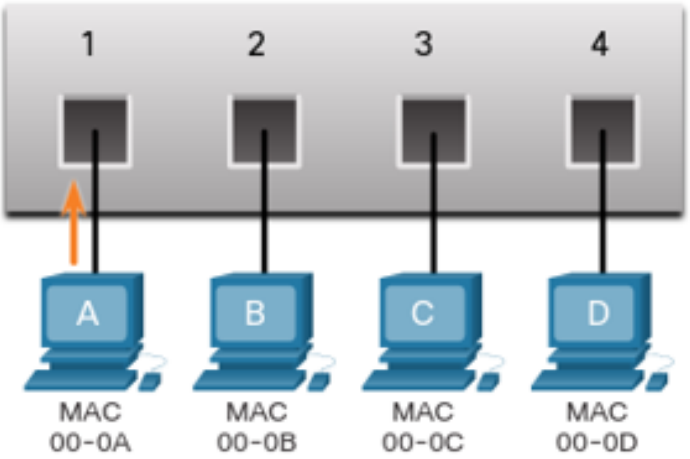
APRENDENDO MAC

Quando um **novo quadro** chega, o Switch examina o endereço de origem e a porta por onde o quadro entrou. Caso essas informações não existam na tabela MAC, o Switch as registra. Se o endereço MAC já existir, o Switch atualiza as informações de porta, se for necessário.

Em ambos os casos há um contador, geralmente de 5 minutos para manutenção da informação na tabela.

Por exemplo, um PC-A está enviando um quadro com destino ao PC-D. Como a tabela está vazia, o Switch adiciona as informações do PC-A na tabela.

Tabela de endereços MAC	
Porta	**Endereço MAC**
1	00-0A

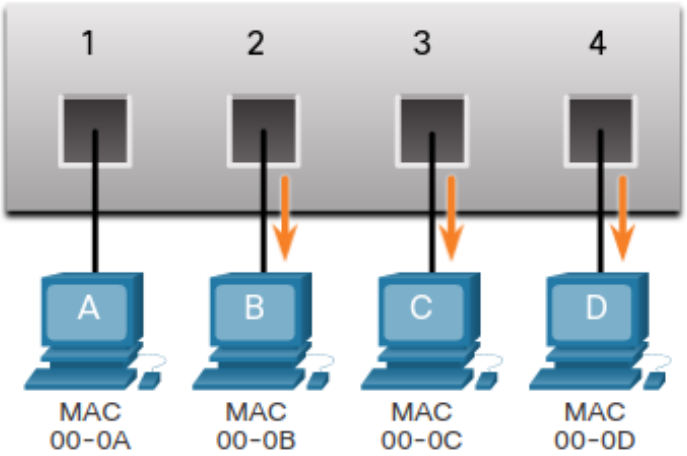


ENCAMINHANDO MAC

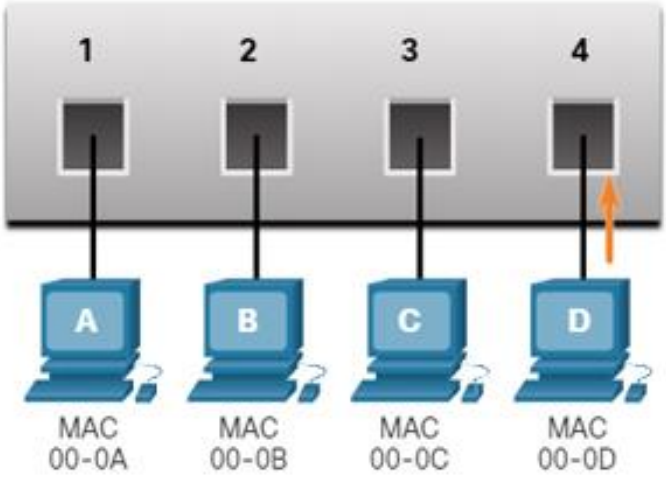
Se o endereço MAC de destino for **unicast** e corresponder a algum registro da tabela, o Switch **encaminha o quadro para a porta correspondente**. Se o endereço **MAC não existir**, o Switch **distribui por todas as portas**, exceto a de entrada, tratando como "unicast desconhecido".

A mesma ação acontece, isto é, o Switch distribui por todas as portas, exceto a de entrada, se o quadro for multicast ou broadcast.

Tabela de endereços MAC	
Porta	**Endereço MAC**
1	00-0A

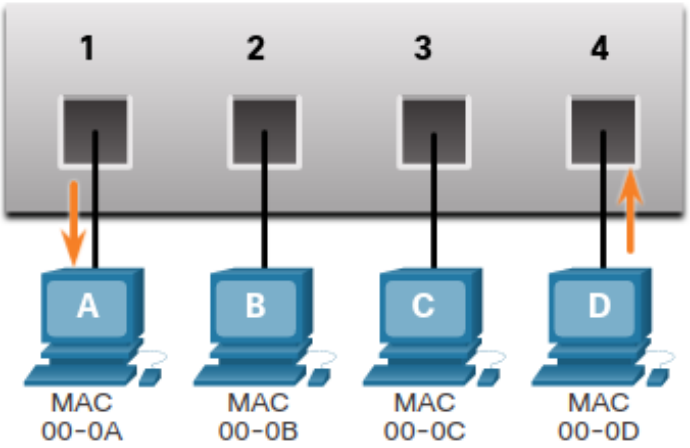


MAC Address Table	
Port	**MAC Address**
1	00-0A
4	00-0D



PC-D RESPONDENDO

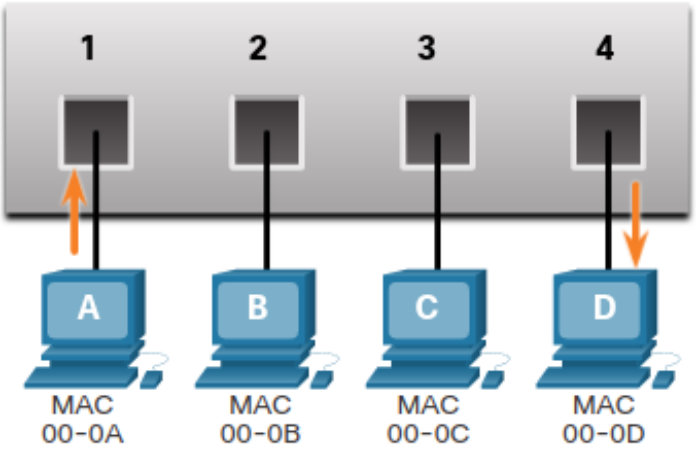
Tabela de endereços MAC	
Porta	**Endereço MAC**
1	00-0A
4	00-0D



MAC de Destino 00-0A	MAC de Origem 00-0D	Tipo	Dados	FCS

SWITCH ENCAMINHANDO

Tabela de endereços MAC	
Porta	**Endereço MAC**
1	00-0A
4	00-0D



PC-D RESPONDENDO

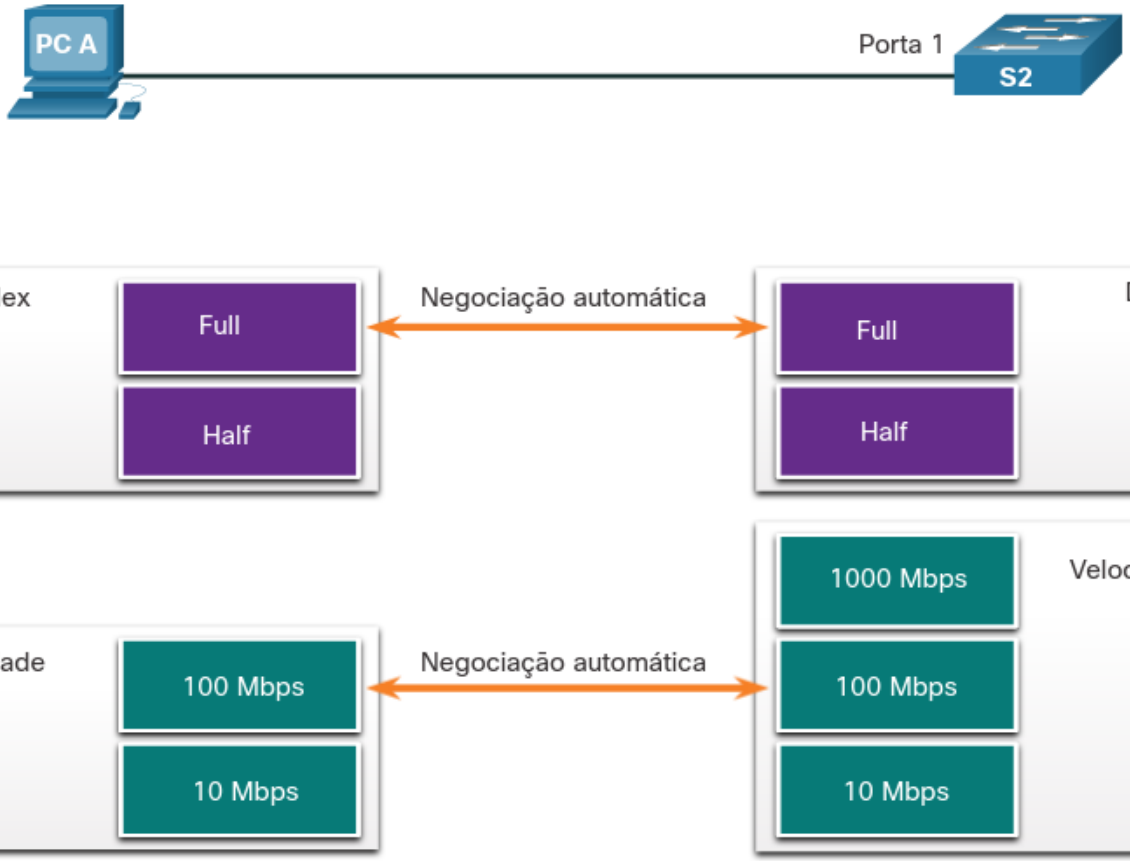
MÉTODOS DE ENCAMINHAMENTO

O Switch pode encaminhar pacotes de duas formas, dependendo de sua tecnologia.

- **Store-And-Forward**: o switch **recebe o quadro inteiro**, detecta erros e em caso de sucesso encaminha para a porta correta. É útil quando há análise de qualidade do serviço (QoS).
- **Cut-Through**: o switch **encaminha o quadro antes de recebê-lo completamente**, lendo pelo menos o endereço de destino. Não faz nenhuma verificação.

VELOCIDADES E NEGOCIAÇÃO

A **negociação automática** de velocidade é sempre recomendada, pois os dispositivos definirão entre si qual a largura de banda máxima, considerando a transmissão half e full duplex. A incompatibilidade duplex ou a má configuração pode comprometer o desempenho dos dispositivos.

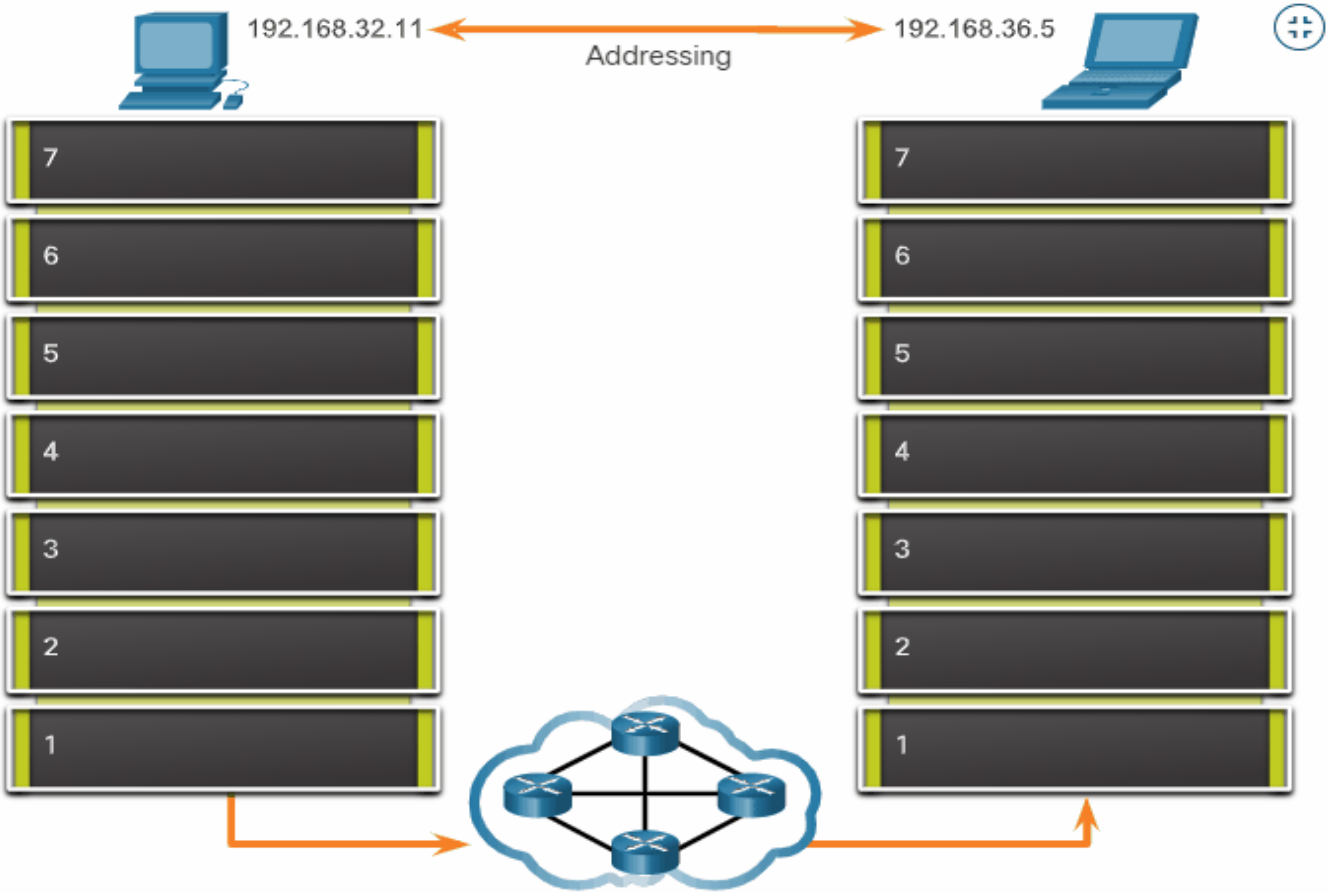

PC A
Porta 1
S2
Duplex
Full
Half
Negociação automática
Full
Half
Duplex
Velocidade
100 Mbps
10 Mbps
Negociação automática
1000 Mbps
100 Mbps
10 Mbps
Velocidade

CAMADA DE REDE

PROPÓSITOS

A camada de rede fornece serviços que permite os dispositivos trocarem dados entre si. Os principais protocolos são o IPv4 e o IPv6, além de outros para roteamento como o OSPF e o BGP e para mensagens como o ICMP. Também faz:

- **Endereçamento**: os dispositivos devem ser endereçados para **identificação exclusiva** na rede.
- **Encapsulamento**: encapsula na origem, o PDU da camada de transporte em um pacote, adicionando no cabeçalho os endereços de origem e destino.
- **Roteamento**: fornece serviços para direcionar o pacote para o **melhor caminho**, através do roteador.
- **Desencapsulamento**: desencapsula no destino, quando o endereço do cabeçalho corresponde a ele, o PDU vindo da camada de enlace, enviando-o a camada de transporte para continuação do processo.



Network layer protocols forward transport layer PDUs between hosts.

O PROTOCOLO IP

O IP é um protocolo de **baixa sobrecarga, de melhor esforço** (não garante entrega), **sem conexão** (“envia sem avisar”), apenas adicionando funções necessárias para enviar um pacote de uma origem a outra.

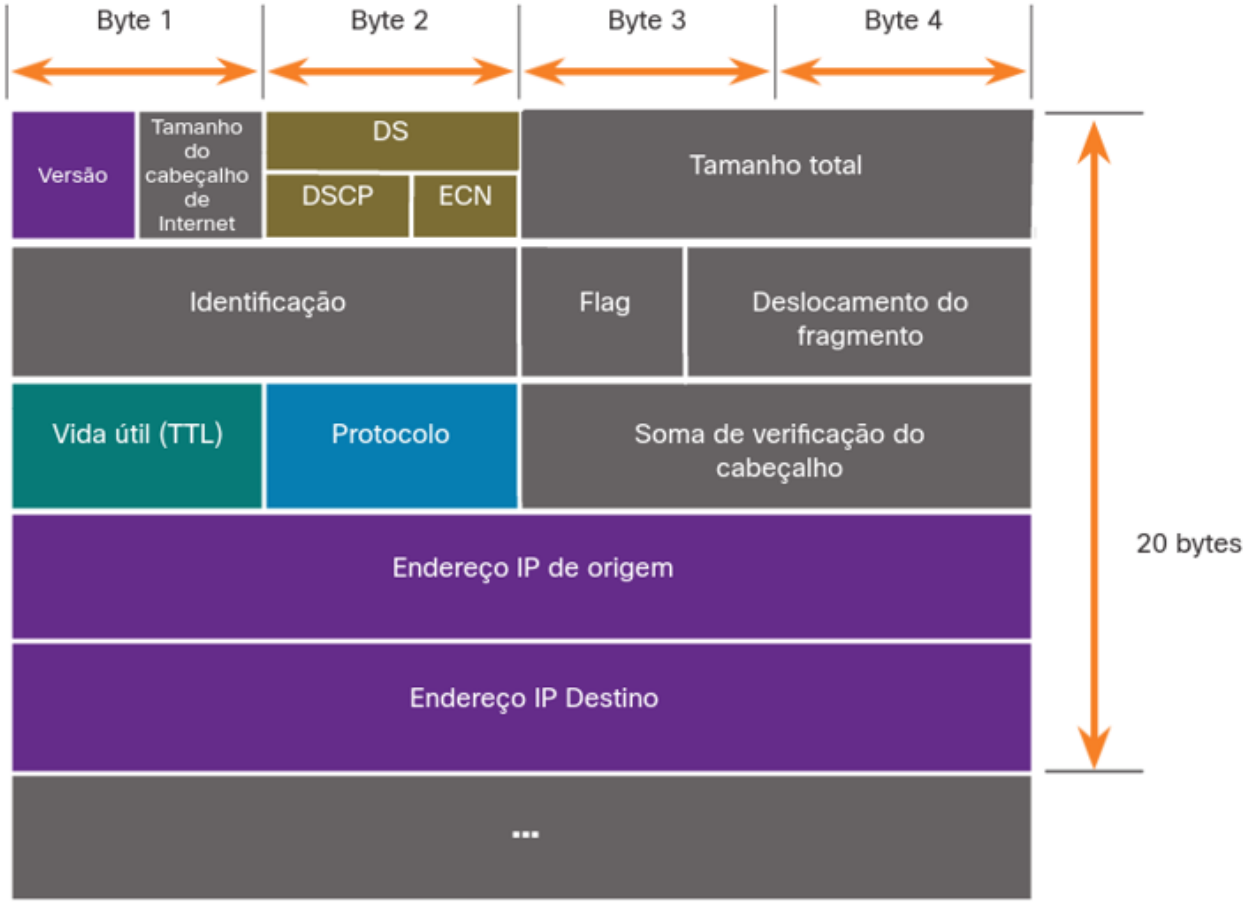
Uma característica importante é que o **cabeçalho IP não é alterado durante toda a trajetória do pacote**, exceto por um técnica descrita nos próximos slides chamada NAT.

O protocolo IP também opera em qualquer meio de transmissão, apenas observando o tamanho máximo que cada mídia consegue transmitir (**MTU**), lembrando que o tamanho do pacote TCP/IP é de 1518 bytes. Quando o MTU é menor, o **pacote é fragmentado causando latência**. Importante observar que o pacote IPv6 não pode ser fragmentado.

SOBRE O IPV4

O cabeçalho IP tem várias informações importantes, sendo lida da esquerda para a direita e de cima para baixo:

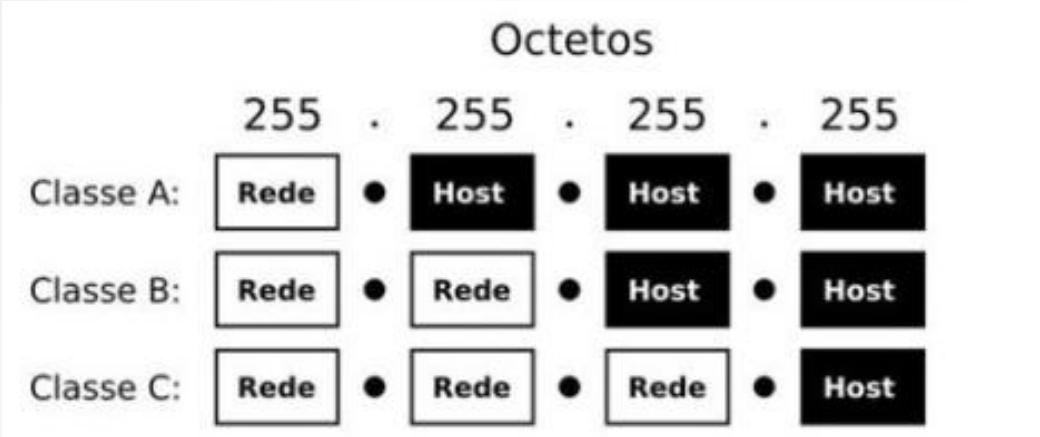
- **Versão**: com 4 bits 0100, identifica a versão 4 do IP
- **DS**: chamados anteriormente de Tipo de Serviço (ToS), são 8 bits que determinam a prioridade do pacote.
- **Checksum**: verificação de erros e corrupção do cabeçalho.
- **TTL**: valor de 8 bits definido na origem, é decrementado a cada roteador que o pacote passa. Se chegar a zero, o pacote é descartado, gerando mensagem de erro.
- **Protocolo**: 8 bits que identificam o protocolo de camada superior, sendo valores comuns 1 (ICMP), 6 (TCP) e 17 (UDP).
- **Endereço de origem**: 32 bits identificando a origem, sendo sempre unicast.
- **Endereço de destino**: 32 bits identificando o destino, podendo ser unicast, multicast ou broadcast.


Byte 1
Byte 2
Byte 3
Byte 4
Versão
Tamanho do cabeçalho de Internet
DS
DSCP
ECN
Tamanho total
Identificação
Flag
Deslocamento do fragmento
Vida útil (TTL)
Protocolo
Soma de verificação do cabeçalho
Endereço IP de origem
Endereço IP Destino
...
20 bytes

ENDEREÇOS IPV4

São **32 bits separados em 4 grupos com 8 bits** (octetos). Existem 5 classes para endereçamento, sendo 3 mais comuns, diferenciando-se pela quantidade de redes e equipamentos possíveis.

Os endereços podem ser representados na forma binária (0 e 1) ou decimal (de 0 a 255), para cada octeto.



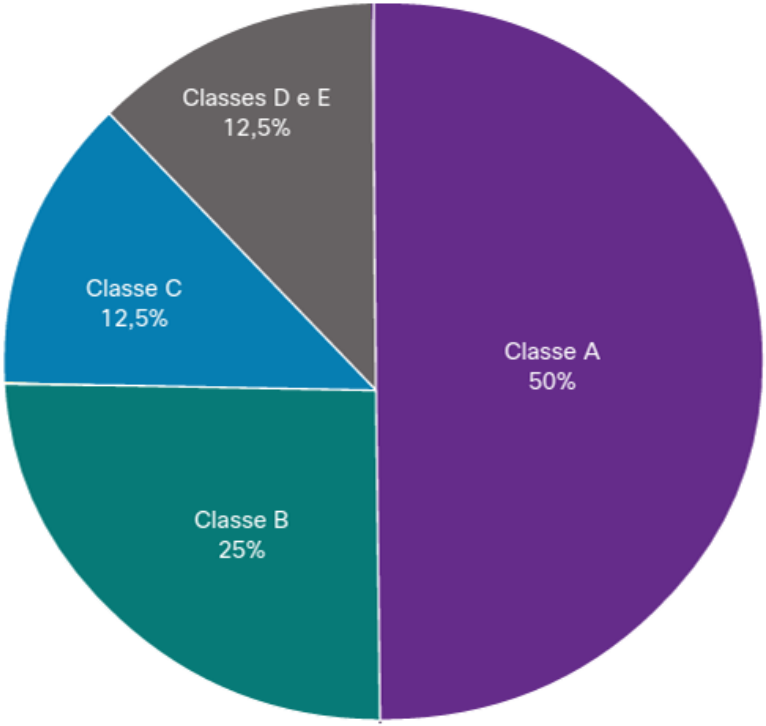
Seu endereço IP é:

23.128.42.244

CLASSES IPV4

Toda a faixa de endereçamento IPv4 foi dividida em classes na RFC 790 de 1981, afim de organizar a atribuição de endereços.

- **Classe A**: compreende endereços de **0.0.0.0 a 127.255.255.255**, projetados para redes com até 16 milhões de endereços (apenas o primeiro octeto para endereçar rede).
- **Classe B**: compreende endereços de **128.0.0.0 a 191.255.255.255**, projetados para redes com até 65 mil endereços (os dois primeiros octetos para endereçar rede).
- **Classe C**: compreende endereços de **192.0.0.0 a 223.255.255.255**, projetados para redes pequenas com 254 endereços (os três primeiros octetos para endereçar rede).
- **Classe D**: compreende endereços de **224.0.0.0 a 239.255.255.255**, utilizados para transmissões multicast.
- **Classe E**: compreende endereços de **240.0.0.0 a 255.255.255.255**, utilizados para experimentos pelo IETF.



Classe A

Total de Redes: 128
Total de Hosts/Redes: 16.777.214

Classe B

Total de redes: 16.384
Total de hosts/redes: 65.534

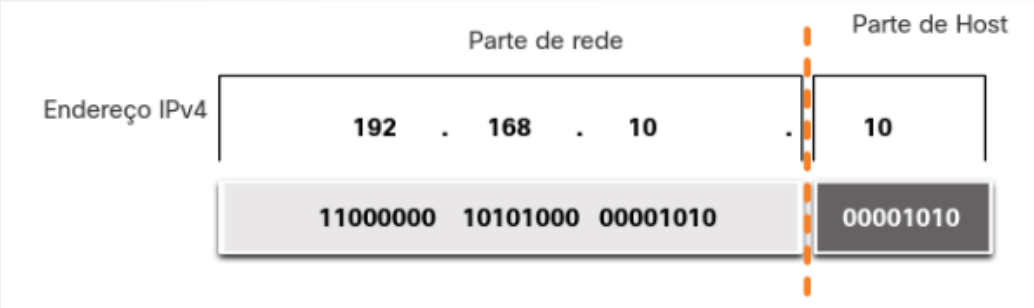
Classe C

Total de Redes: 2,097,152
Total de Hosts/Redes: 254

Com o grande desperdício das classes, a partir de 1990, com o advindo da Web, passou-se a utilizar endereços sem classe, ignorando a regra de tamanho de redes e hosts, melhorando o aproveitamento.

ESTRUTURA DE ENDEREÇOS IPV4

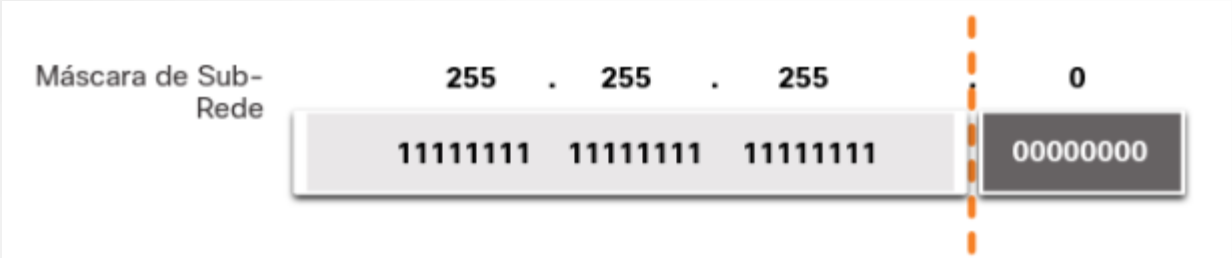
Em cada classe de endereçamento, há um tamanho definido para criar a rede e outro tamanho para endereçar um equipamento. Veja por exemplo um endereço de classe C.



Todos os bits da rede devem ser iguais nos dispositivos que fazem parte dela. Mas como saber exatamente o limite de endereço da rede e do host? Precisamos então de um novo parâmetro, a **máscara de rede**.

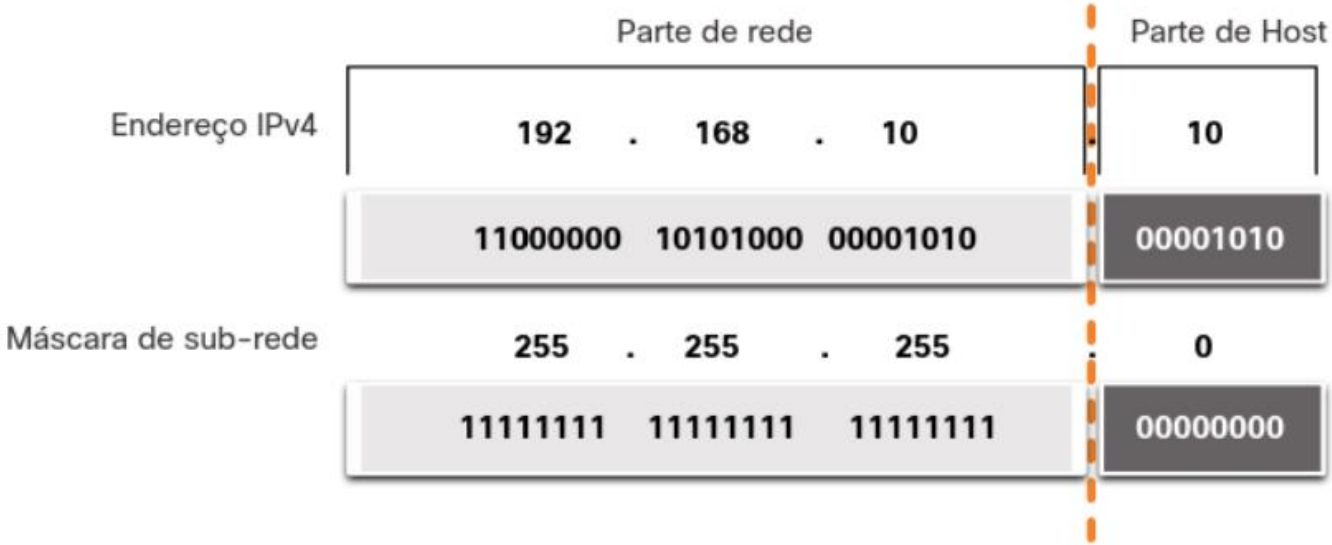
MÁSCARA DE REDE IPV4

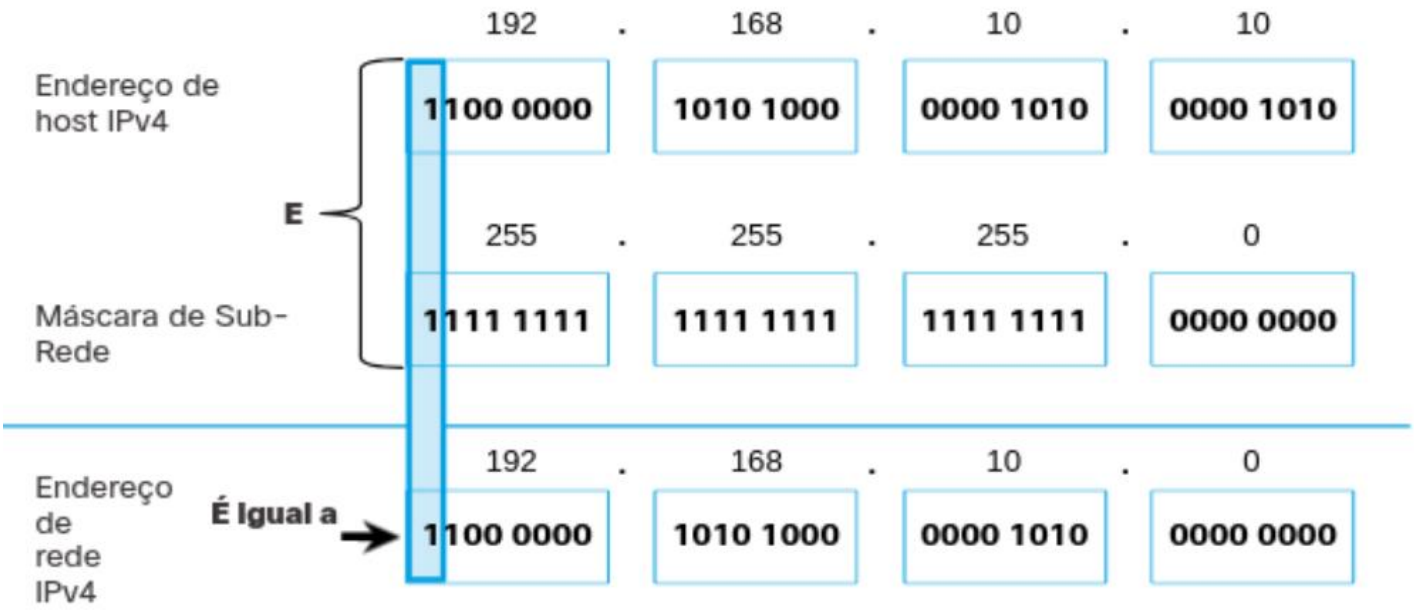
A máscara de rede tem a função de **limitar o tamanho da rede e a quantidade de equipamentos** que farão parte dela. Ela determina quantos bits estarão disponíveis para endereçar cada parte.



Para identificar cada parte, é comparada a máscara com o endereços IPv4 compara bit a bit, da esquerda para direita. O resultado encontrado identifica o primeiro endereço da rede.

A comparação é um **E lógico** (AND), onde o resultado 1 acontece somente quando ambos os bits (máscara e endereço).


Parte de rede
Parte de Host
Endereço IPv4
192 . 168 . 10 . 10
11000000 10101000 00001010 00001010
Máscara de sub-rede
255 . 255 . 255 . 0
11111111 11111111 11111111 00000000


192 . 168 . 10 . 10
Endereço de host IPv4
1100 0000 1010 1000 0000 1010 0000 1010
E
255 . 255 . 255 . 0
Máscara de Sub-Rede
1111 1111 1111 1111 1111 1111 0000 0000
192 . 168 . 10 . 0
Endereço de rede IPv4
É Igual a
1100 0000 1010 1000 0000 1010 0000 0000

REDE, HOST E BROADCAST

Há 3 tipos de endereços IPv4 em uma rede, uma para identificar o início dela, outro para o fim e outro para identificar um dispositivo específico.

- **Endereço de Rede**: é o **primeiro endereço da rede**, justamente para identificar seu início. Como vimos, é determinado com um AND lógico entre a máscara de rede e o endereço IPv4. Todos os bits da parte de host são 0 e não podem ser atribuídos a nenhum dispositivo.
- **Endereço de Broadcast**: é o **último endereço da rede**, utilizado para enviar mensagens a todos os dispositivos daquela rede. Todos os bits da parte de rede são 1e não podem ser atribuídos a nenhum dispositivo.
- **Endereço de Host**: são atribuídos a um **dispositivo** como computador, câmera, smartphones, impressora, roteador, etc. Pode ter qualquer combinação de bit na parte de host.

Por exemplo, para o endereço de rede 192.168.10.0/24 teríamos a seguinte tabela para Broadcast e Host.

Endereços de Broadcast, de Host e de Rede

	Parte de rede			Parte de host	Bits do host
Máscara de sub-rede **255.255.255.**0 ou **/24**	255 11111111	255 11111111	255 11111111	0 00000000	
Endereço de rede **192.168.10.**0 ou **/24**	192 11000000	168 10100000	10 00001010	0 00000000	Todos os 0
Primeiro endereço **192.168.10.**1 ou **/24**	192 11000000	168 10100000	10 00001010	1 00000001	Todos os 0s e um 1
Último endereço **192.168.10.**254 ou **/24**	192 11000000	168 10100000	10 00001010	254 11111110	Todos os 1s e um 0
Endereço de difusão **192.168.10.**255 ou **/24**	192 11000000	168 10100000	10 00001010	255 11111111	Todos os 1s

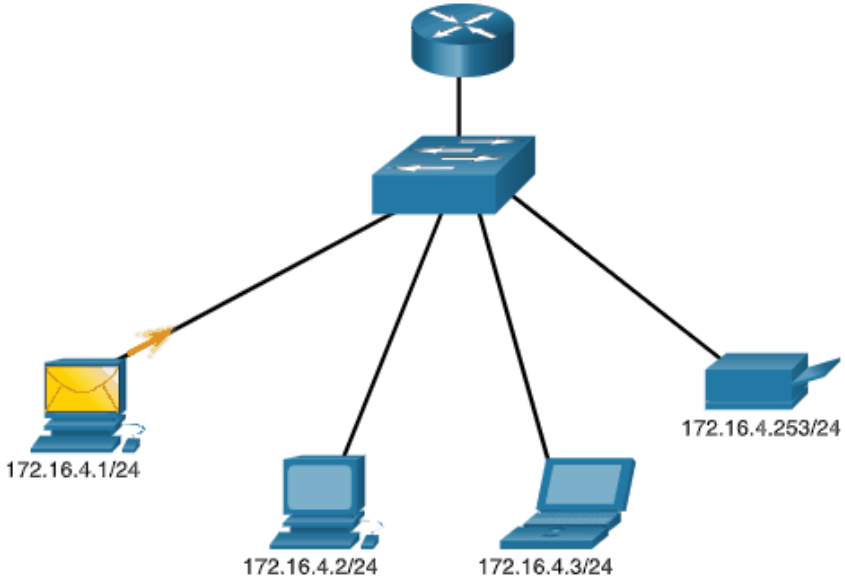
TRANSMISSÕES EM IPV4

As transmissões em IPv4 segue o padrão Unicast, Broadcast e Multicast estudados anteriormente.

- **Unicast**: direcionada a um **único endereço IPv4 de destino**, em comunicação do tipo Um-Para-Um. Um endereço de origem sempre será unicast, mesmo que o destino não seja.
- **Broadcast**: direcionada para o último endereço da rede, com o objetivo de atingir **todos os dispositivos daquela rede**, pois todos os bits de host são 1. Roteadores não encaminham pacotes broadcast.
- **Multicast**: direcionada a um **grupo de hosts**, utilizado em serviços como streaming de mídia. O IPv4 tem os endereços de 224.0.0.0 a 239.255.255.255 reservados para pacotes multicast.

Source: 172.16.4.1/24

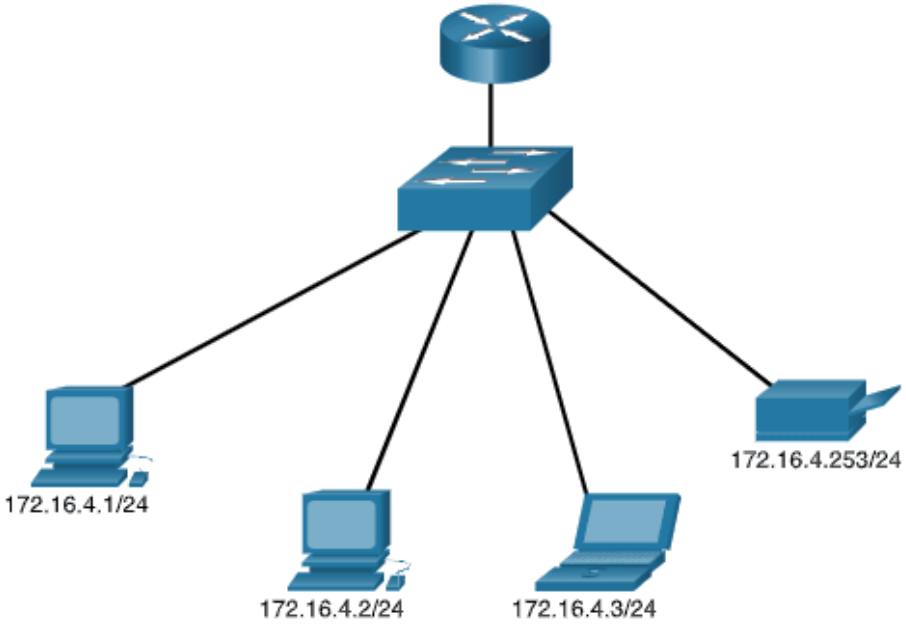
Destination: 172.16.4.253/24

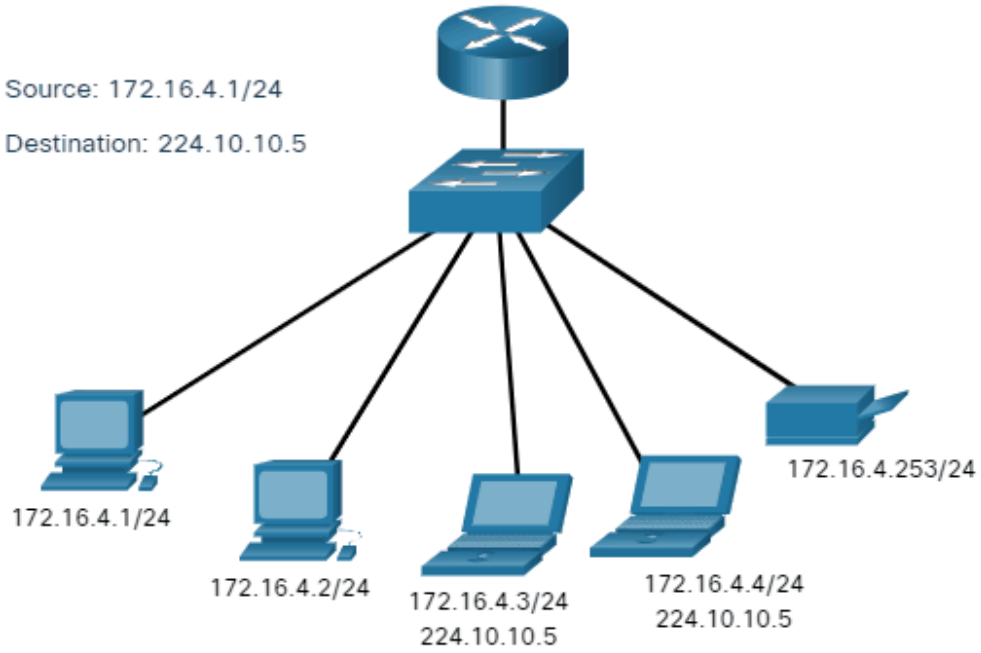


Limited Broadcast

Source: 172.16.4.1/24

Destination: 255.255.255.255




Source: 172.16.4.1/24
Destination: 224.10.10.5
172.16.4.1/24
172.16.4.2/24
172.16.4.3/24
224.10.10.5
172.16.4.4/24
224.10.10.5
172.16.4.253/24

ENDEREÇOS PÚBLICOS E PRIVADOS IPV4

Os endereços públicos são pacotes processados e roteados globalmente, porém nem todos os endereços são permitidos utilizar na Internet. Existem, pois, os endereços privados, utilizados em redes internas. Veja a tabela de endereços privados, definidas na **RFC 1918**.

Endereço de Rede e Máscara	Intervalo de Endereços
10.0.0.0/8	10.0.0.0 – 10.255.255.255
172.16.0.0/12	172.16.0.0 – 172.31.255.255
192.168.0.0/16	192.168.0.0 – 192.168.255.255

ENDEREÇOS ESPECIAIS IPV4

Algumas faixas de endereços IPv4, além das classificações de público e privado, foram reservadas para usos especiais.

- **Loopback**: são pacotes enviados por dispositivos com **destino a si mesmo**. Podem ser utilizados para teste da pilha de protocolos TCP/IP. Compreende a faixa 127.0.0.0/8.
- **Link Local**: são endereços atribuídos automaticamente a dispositivos que não conseguiram receber, por algum motivo, endereços automáticos de um servidor, num processo conhecido como **APIPA**. Podem ser roteados na rede local, embora seja uma prática incomum. Compreendem a faixa 169.254.0.0/16.
- **Documentação**: são endereços **reservados para produção de documentação, apostilas, livros, slides, etc**. Para evitar que sejam utilizados endereços reais, representando um risco de segurança. Compreende os blocos 192.0.2.0/24, 198.51.100.0/24 e 203.0.113.0/24. Foram definidas na RFC 5737

CLASSIFIQUE OS ENDEREÇOS COMO PÚBLICO OU PRIVADO.

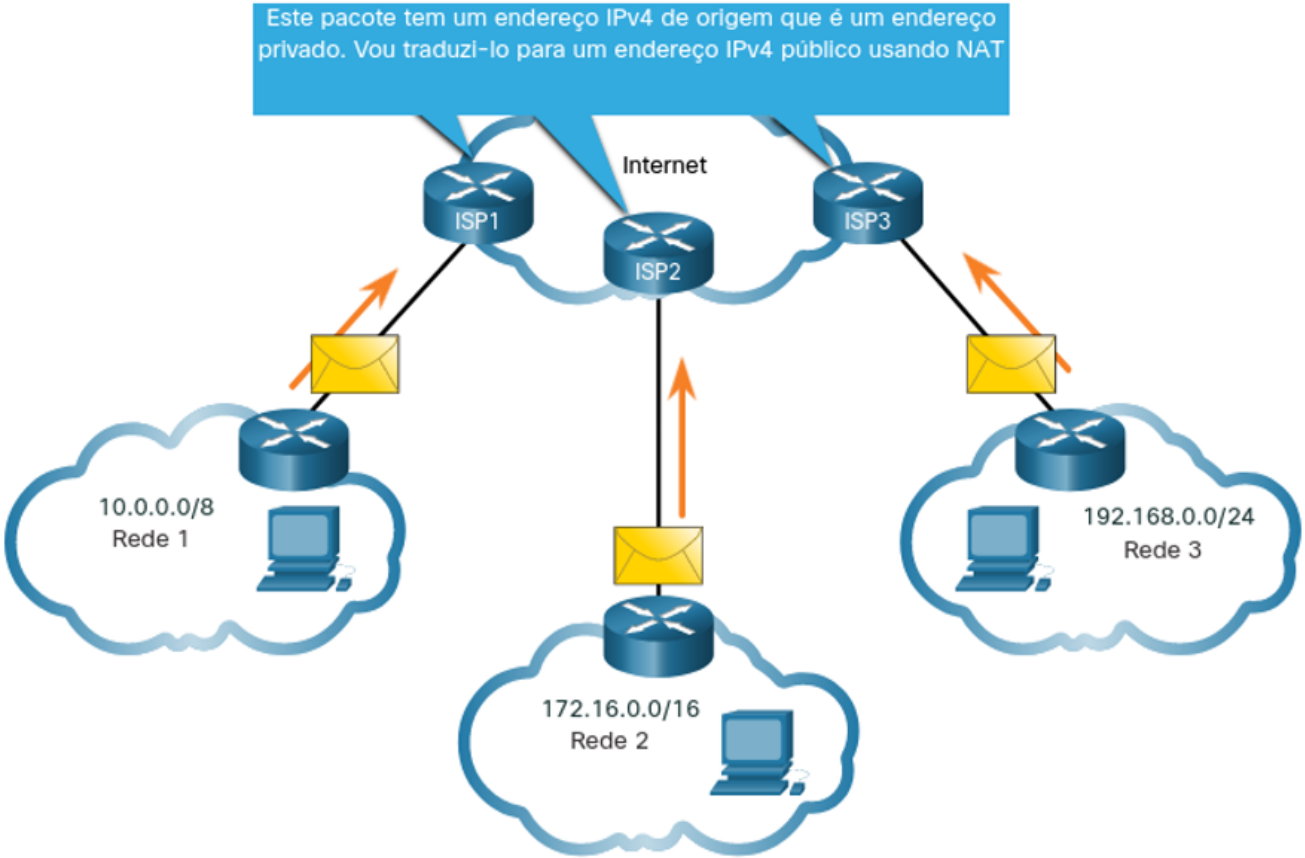
172.16.35.2	Pública	Privada
192.168.3.5	Pública	Privada
192.0.3.15	Pública	Privada
64.104.0.22	Pública	Privada
209.165.201.30	Pública	Privada
192.168.11.5	Pública	Privada
172.16.30.30	Pública	Privada
10.55.3.168	Pública	Privada

ROTEAMENTO, NAT E DMZ

Endereços privados não são roteados globalmente, isto é, os pacotes não devem ser processados por roteadores com destino a Internet. Porém, devido ao esgotamento de endereços públicos, implementou-se uma técnica chamada **NAT** (Network Address Translation).

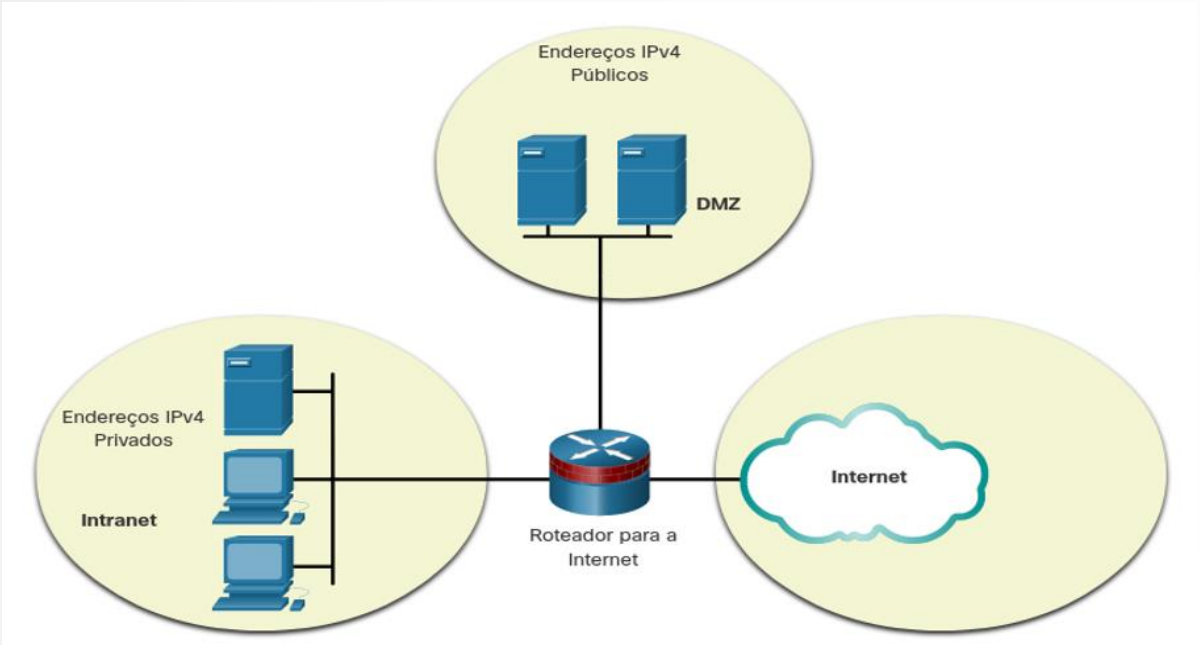
Essa técnica permite que um dispositivo interno que contém um endereço privado possa acessar a Internet sendo "**mascarado**" com um endereço público, geralmente pertencente ao gateway. Assim, **vários dispositivos internos podem acessar a Internet ao mesmo tempo**, compartilhando o endereço público do gateway.

O papel do gateway é "**traduzir**" os endereços privados para públicos e vice-versa na recepção, trocando o cabeçalho IP do pacote.


Este pacote tem um endereço IPv4 de origem que é um endereço privado. Vou traduzi-lo para um endereço IPv4 público usando NAT
Internet
ISP1
ISP2
ISP3
10.0.0.0/8
Rede 1
172.16.0.0/16
Rede 2
192.168.0.0/24
Rede 3

ROTEAMENTO, NAT E DMZ

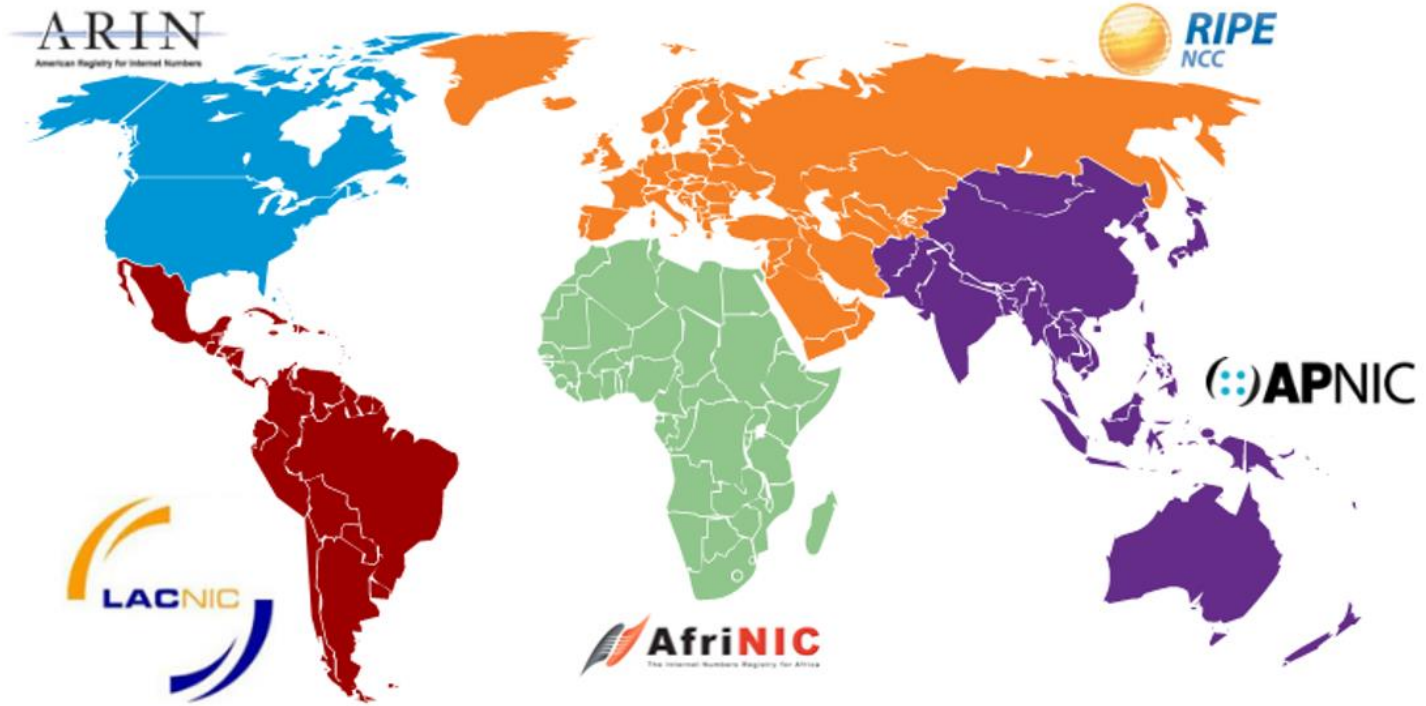
Além de dispositivos da rede interna e o gateway, as instituições também possui dispositivos com endereços públicos, isto é visíveis na Internet. Esses equipamentos ficam numa área da rede comumente chamada **DMZ (Demilitarized Zone),** com o roteador fazendo o trabalho de filtro de segurança.



ATRIBUIÇÃO DE ENDEREÇOS IP

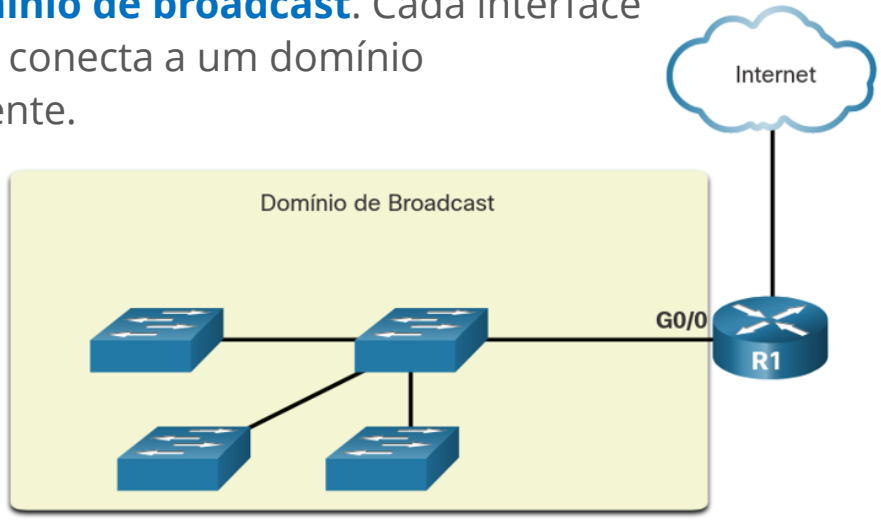
Os endereços IP são gerenciados pela IANA (Internet Assigned Numbers Authority) que determina a distribuição dos blocos pelo mundo, através das RIRs (Regional Internet Registry).

São **5 RIRs** pelo mundo, responsáveis por distribuir endereços para provedores (ISP), que por sua vez distribuem endereços para organizações e provedores menores.


ARIN
American Registry for Internet Numbers
RIPE
NCC
APNIC
LACNIC
AfriNIC

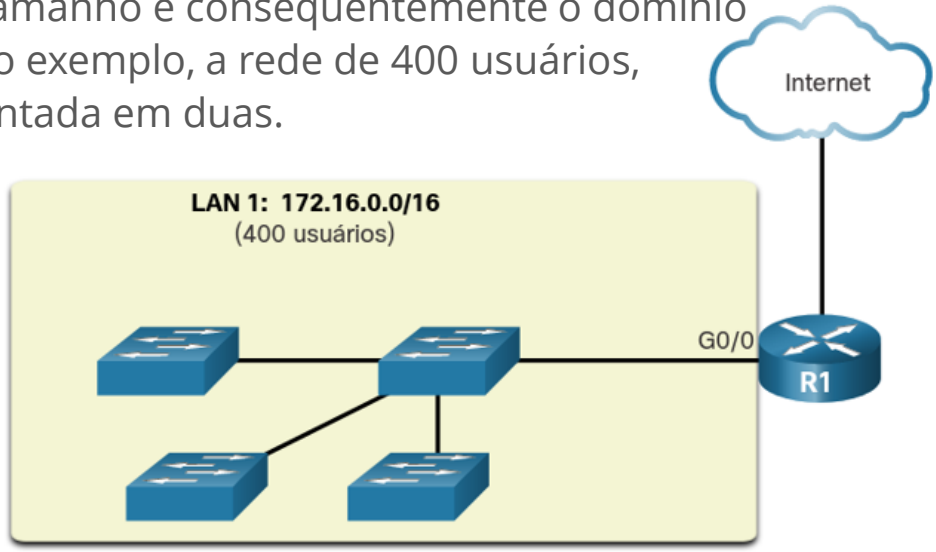
DOMÍNIOS E SEGMENTAÇÃO DE REDE

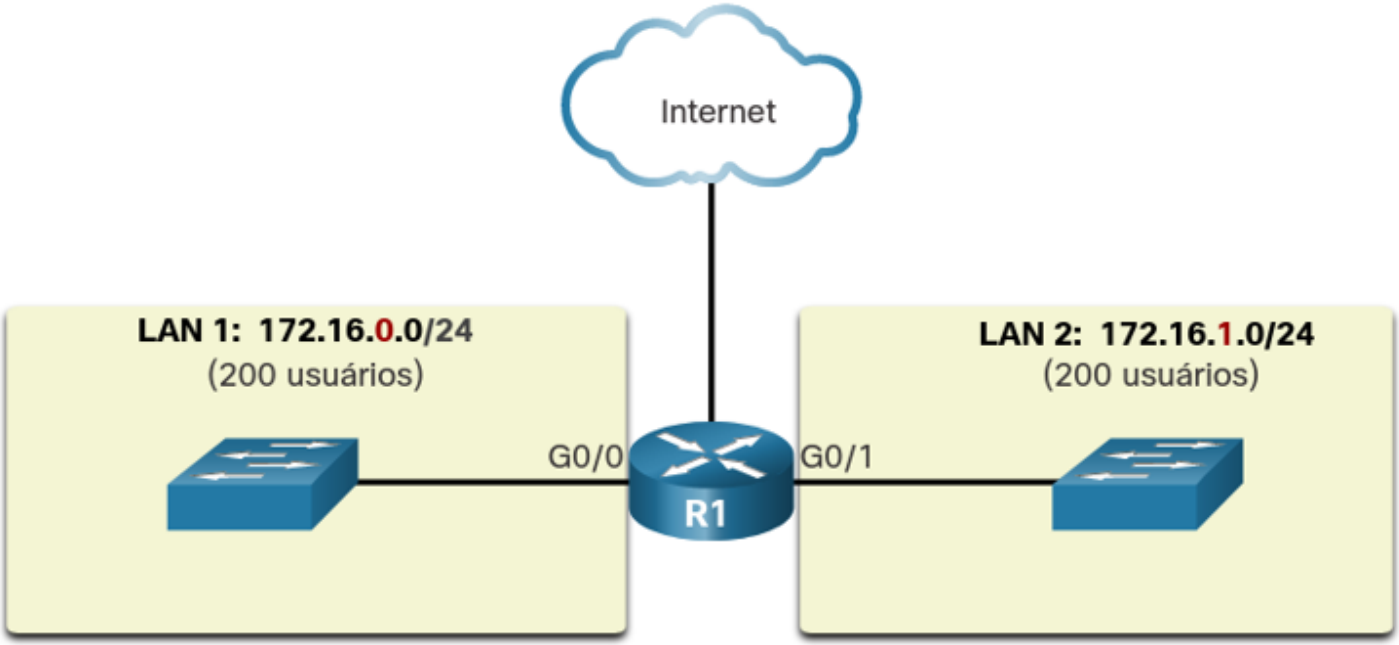
Os pacotes de broadcast são frequentemente enviados em uma rede, como por exemplo para ARP. Os switches difundem broadcast por todas as portas exceto a de entrada, mas roteadores não encaminham esse tipo de tráfego, criando o que chamamos de **domínio de broadcast**. Cada interface de um roteador se conecta a um domínio de broadcast diferente.



DOMÍNIOS E SEGMENTAÇÃO DE REDE

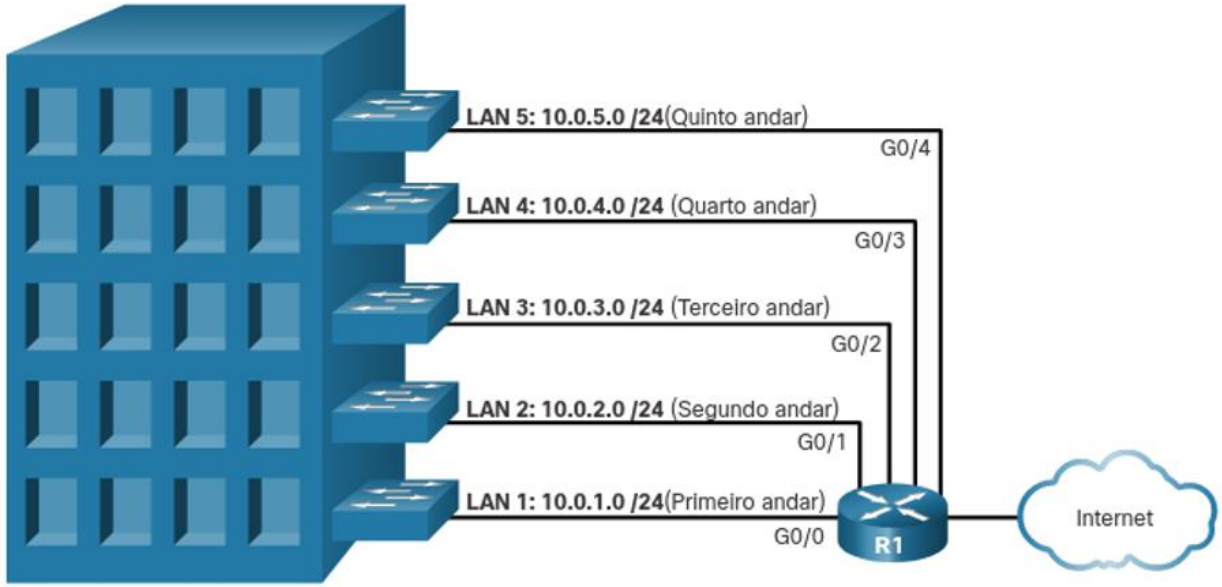
Quando temos grandes domínios de broadcast, a rede pode ser comprometida, pois o **tráfego excessivo** resulta em operações de rede lentas já que os dispositivos devem aceitar e processar cada pacote de difusão. A solução é segmentar a rede, reduzindo seu tamanho e consequentemente o domínio de broadcast. No exemplo, a rede de 400 usuários, pode ser segmentada em duas.



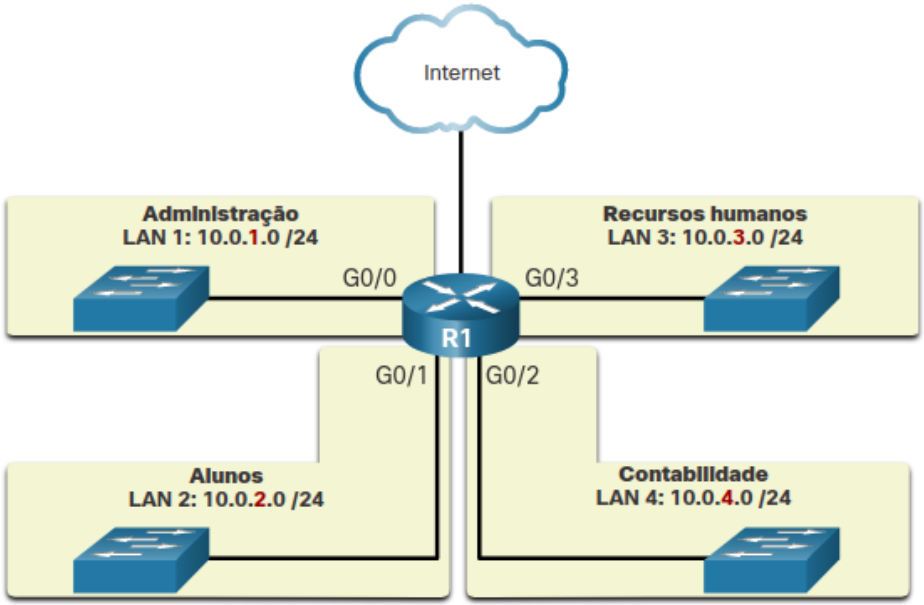


Observe que o prefixo da rede mudou de /16 para /24, ou seja, utilizou-se **bits de hosts para criar sub-redes**, interconectadas por um roteador, sendo essa a premissa de uma segmentação (“emprestar bits”). Há diversas maneiras de segmentar uma rede.

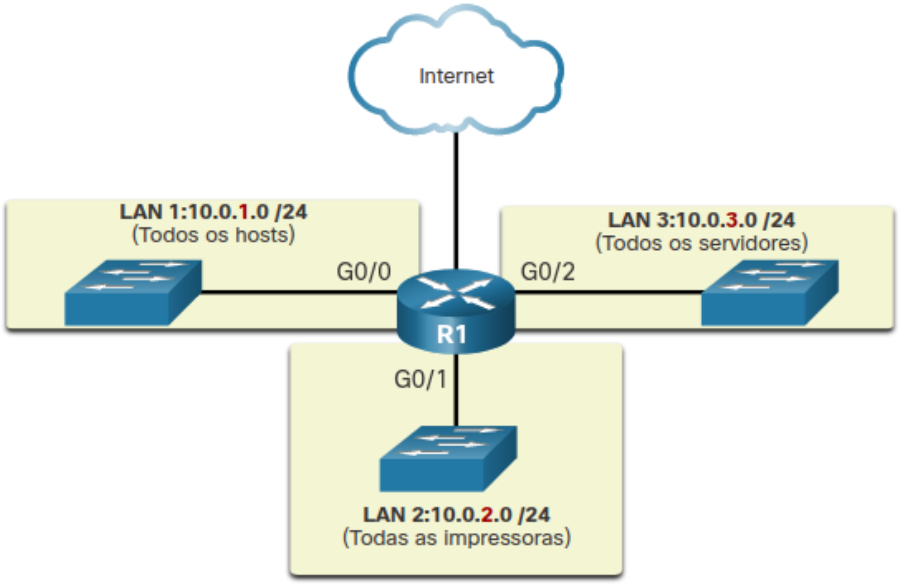
Divisão em Sub-Redes por Local



Sub-redes por grupo ou função



Sub-redes por tipo de dispositivo



COMO SEGMENTAR?

Já vimos os benefícios da segmentação. Quanto mais redes criamos, ou seja, quanto mais bits emprestamos, menor é o número de hosts, consequentemente menor é o tráfego.

Comprimento do Prefixo	Máscara de sub-rede	Máscara de sub-rede em binário (n = rede, h = host)	# de hosts
/8	255.0.0.0	nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh 11111111.00000000.00000000.00000000	16.777.214
/16	255.255.0.0	nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh 11111111.11111111.00000000.00000000	65.534
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.00000000	254

Veja no endereçamento das classes A, B e C. Vamos exemplificar um empresa que tenha escolhido trabalhar com o endereço classe A. Uma rede com 16 milhões de dispositivos é altamente inviável. A empresa então pode segmentar com o prefixo /16 ou /24.

Rede de sub-rede 10.0.0.0/8 usando um /16

Endereço da Sub-Rede (256 possíveis sub-redes)	**Intervalo de host (65,534 possíveis hosts por sub-rede)**	**Broadcast**
10.0.0.0**/16**	**10.0**.0.1 - **10.0**.255.254	**10.0**.255.255
10.1.0.0**/16**	**10.1**.0.1 - **10.1**.255.254	**10.1**.255.255
10.2.0.0**/16**	**10.2**.0.1 - **10.2**.255.254	**10.2**.255.255
10.3.0.0**/16**	**10.3**.0.1 - **10.3**.255.254	**10.3**.255.255
10.4.0.0**/16**	**10.4**.0.1 - **10.4**.255.254	**10.4**.255.255
10.5.0.0**/16**	**10.5**.0.1 - **10.5**.255.254	**10.5**.255.255
10.6.0.0**/16**	**10.6**.0.1 - **10.6**.255.254	**10.6**.255.255
10.7.0.0**/16**	**10.7**.0.1 - **10.7**.255.254	**10.7**.255.255
...	...	...
10.255.0.0**/16**	**10.255**.0.1 - **10.255**.255.254	**10.255**.255.255

Rede de sub-rede 10.0.0.0/8 usando um prefixo /24

Endereço da Sub-Rede (65,536 possíveis sub-redes)	Intervalo de host (254 possíveis hosts por sub-rede)	Broadcast
10.0.0.0/**24**	**10.0.0**.1 - **10.0.0**.254	**10.0.0**.255
10.0.1.0/**24**	**10.0.1**.1 - **10.0.1**.254	**10.0.1**.255
10.0.2.0/**24**	**10.0.2**.1 - **10.0.2**.254	**10.0.2**.255
...	...	...
10.0.255.0/**24**	**10.0.255**.1 - **10.0.255**.254	**10.0.255**.255
10.1.0.0/**24**	**10.1.0**.1 - **10.1.0**.254	**10.1.0**.255
10.1.1.0/**24**	**10.1.1**.1 - **10.1.1**.254	**10.1.1**.255
10.1.2.0/**24**	**10.1.2**.1 - **10.1.2**.254	**10.1.2**.255
...	...	...
10.100.0.0/**24**	**10.100.0**.1 - **10.100.0**.254	**10.100.0**.255
...	...	...
10.255.255.0/**24**	**10.255.255**.1 - **10.2255.255**.254	**10.255.255**.255

COMO SEGMENTAR?

Podemos segmentar qualquer prefixo de rede, **emprestando os bits de host**. Por exemplo uma rede /24 pode ser segmentada em redes cada vez menores.

Comprimento do Prefixo	Máscara de sub-rede	Máscara de sub-rede em binário (n = rede, h = host)	# de sub-redes	# de hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.**n**hhhhhhh 11111111.11111111.11111111.**1**0000000	**2**	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nn**hhhhhh 11111111.11111111.11111111.**11**000000	**4**	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnn**hhhhh 11111111.11111111.11111111.**111**00000	**8**	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnn**hhhh 11111111.11111111.11111111.**1111**0000	**16**	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnn**hhh 11111111.11111111.11111111.**11111**000	**32**	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnnn**hh 11111111.11111111.11111111.**111111**00	**64**	2

LABORATÓRIO

Criação de uma rede IPv4 básica com configuração de endereços nas interfaces.

- Cisco
- Huawei
- Mikrotik

PROBLEMAS COM IPV4

O IPv6 nasceu para sanar alguns problemas e limitações do IPv4. Ambos coexistem atualmente, mas em futuro próximo, o IPv6 substituirá completamente o IPv4.

- **Esgotamento**: com pouco mais de 4 bilhões de endereços IPv4, os **endereços sofrem de esgotamento**, visto a necessidade de conectar cada vez mais dispositivos advindos da Internet das Coisas (IoT).
- **Conectividade** Ponta a Ponta: com o esgotamento, criou-se uma técnica para "**mascaramento**" de endereço chamada NAT. A técnica consiste em vários dispositivos utilizarem o mesmo endereço IPv4. Isso dificulta a identificação do host de origem, causando problemas para tecnologias que exigem conectividade ponta a ponta, além de criar latência.

SOBRE O IPV6

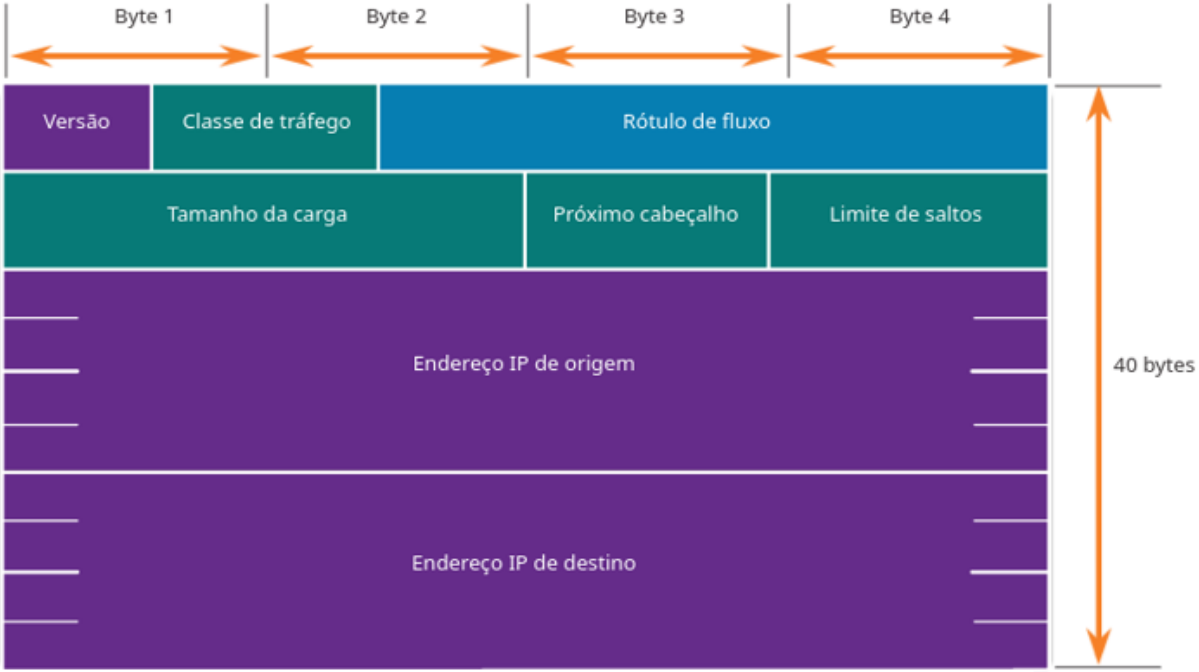
Com o advento do IPv6, alguns problemas do IPv4 foram solucionados:

- **Espaço aumentado**: endereços IPv6 são formados por 128 bits, ante a 32 bits do IPv4, o que resulta em pouco mais de 340 undecilhões de endereços (10^{36}), equivalente a cada grão de areia na Terra.
- **Manipulação aprimorada:** o cabeçalho foi simplificado, com menos campos.
- **NAT desnecessário**: com endereços numerosos, cada dispositivo pode utilizar uma identificação exclusiva, eliminado a necessidade de compartilhamento de endereço.

SOBRE O IPV6

Como dito, o cabeçalho foi simplificado, resultando em maior eficiência no processamento do pacote.

- **Versão**: com 4 bits 0110, identifica a versão 6 do IP
- **Classe de Tráfego**: são 8 bits que determinam a prioridade do pacote, equivalente ao DS do IPv4.
- **Rótulo de Fluxo**: com 20 bits, determina o tipo de manipulação que os roteadores devem fazer..
- **Comprimento de Carga**: valor com 16 bits que indica o tamanho da carga útil do pacote, excluindo o cabeçalho.
- **Próximo Cabeçalho**: 8 bits que identificam o protocolo de camada superior, semelhante ao campo Protocolo do IPv4.
- **Limite de Salto**: com 8 bits, substitui o campo TTL IPv4.
- **Endereços de origem e destino**: 128 bits que identificam o emissor e receptor, com regras semelhantes ao IPv4, excluindo broadcast.

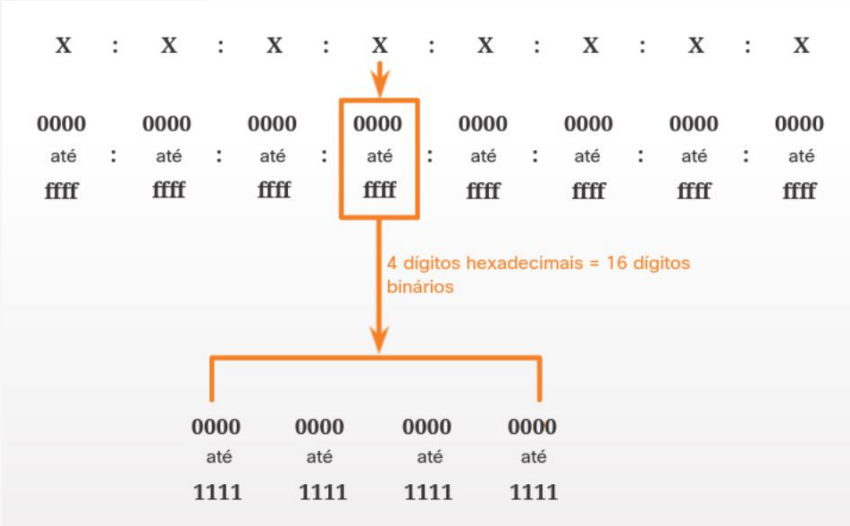


Legenda

- Nome dos campos mantido de IPv4 para IPv6
- Nome e posição alterados no IPv6
- Novo campo no IPv6

ENDEREÇOS IPV6

O endereço IPv6 tem estrutura diferente, sendo muito maior do que o IPv4, justamente para que o esgotamento seja improvável. São **128 bits** (ante 32 bits do IPv4) separados em **8 grupos de 16 bits** cada, representados por valores hexadecimais ao invés de decimais. São separados por dois pontos (:) e chamados de hexadecateto ou duplo-octeto. Hexteto é um termo informal.



ENDEREÇOS IPV6

Por serem bastante extensos, existem 2 regras que permitem **reduzir a escrita** do endereço.

- **Zeros À Esquerda**: podemos **omitir os zeros que aparece à esquerda** em qualquer um dos hexadecatetos.

Original	**2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200**
Reduzido	**2001 : db8 : 0 : 1111 : 0 : 0 : 0 : 200**

- **Grupos de Zeros**: quando houver uma **sequência de zeros**, pode-se representar por duplos dois-pontos (::), mas **somente uma vez**, para não gerar ambiguidade.

Original	**2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200**
Reduzido	**2001 : db8 : 0 : 1111 : 0 : : 200**

Original	**2001 : 0db8 : 0000 : 0000 : ab00 : 0000 : 0000 : 0000**
Reduzido	**2001 : db8 : 0 : 0 : ab00 : :**

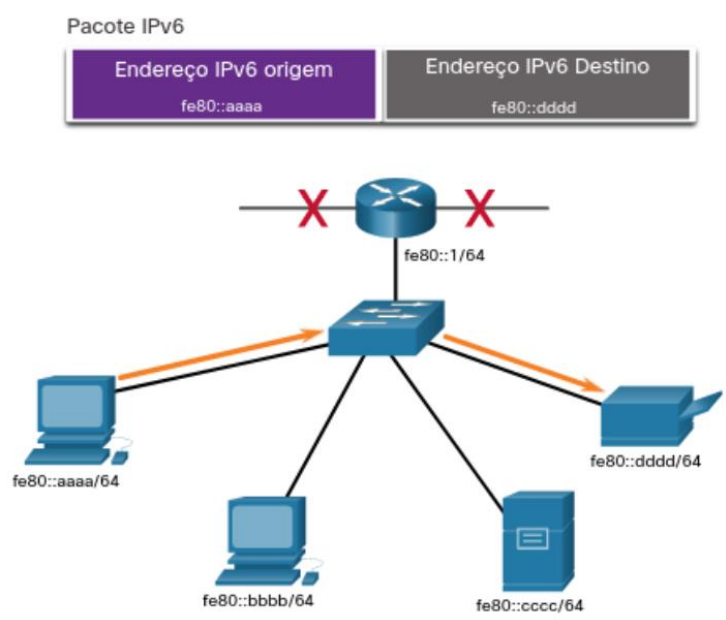
TRANSMISSÃO E TIPOS IPV6

As transmissões IPv6 são bastante parecidas com as transmissões IPv4, com unicast, multicast e também um transmissão anycast. A diferença é que não existe broadcast em IPv6,. Dentre os endereços unicast, temos:

- **Global (GUA)**: pode ser **roteado globalmente**, semelhante aos **endereços públicos** IPv4. A faixa global do IPv6 representa somente 13% do total possível. Compreende o espaço **2000::/3**

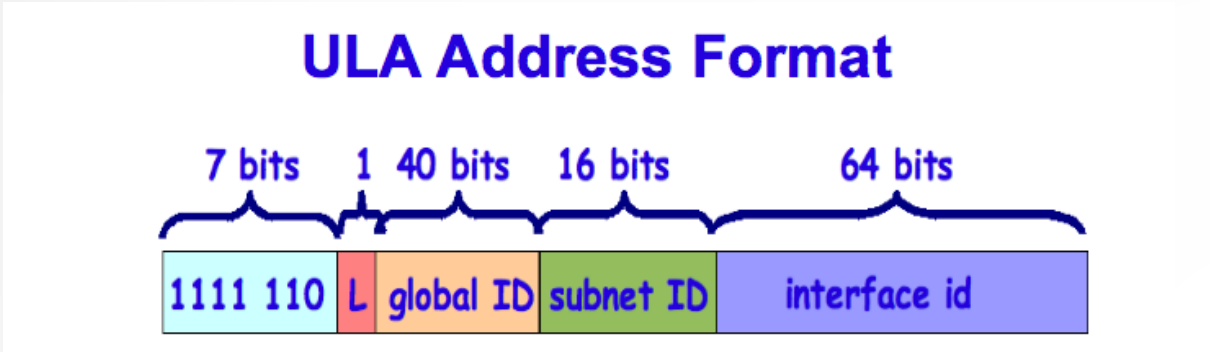
TRANSMISSÃO E TIPOS IPV6

- **Local (LLA)**: deve ser utilizado **apenas localmente, não sendo roteado** para nenhuma outra rede. É atribuído automaticamente por autoconfiguração, através de uma técnica conhecida como EUI, onde o endereço MAC é utilizado juntamente com bits adicionais. **Não são semelhantes ao endereços privados do IPv4** e compreende o espaço **FE80::/10**.



TRANSMISSÃO E TIPOS IPV6

- **Exclusivo (ULA)**: semelhante ao LLA, funcionam apenas na **rede local, mas é roteável**, embora não seja esperado que apareça na Internet. Possui alta probabilidade de ser **globalmente único, com 40 bits aleatórios** para formar o endereço, após o prefixo. São **semelhantes ao endereços privados do IPv4**, embora ainda sejam incomum. Está contido na **faixa FC00::/7**, definidos na RFC 4193.



ENDEREÇOS ESPECIAIS IPV6

Algumas faixas de endereços IPv4, além das classificações de público e privado, foram reservadas para usos especiais.

- **Loopback**: Mesmo conceito da faixa 127.0.0.0/8 no IPV4. A faixa IPv6 é ::1/128.
- **Documentação**: também reservados para produção de material audiovisual, como no IPv4. Compreende a faixa 2001:db8::/32.

DISTRIBUIÇÃO IPV6

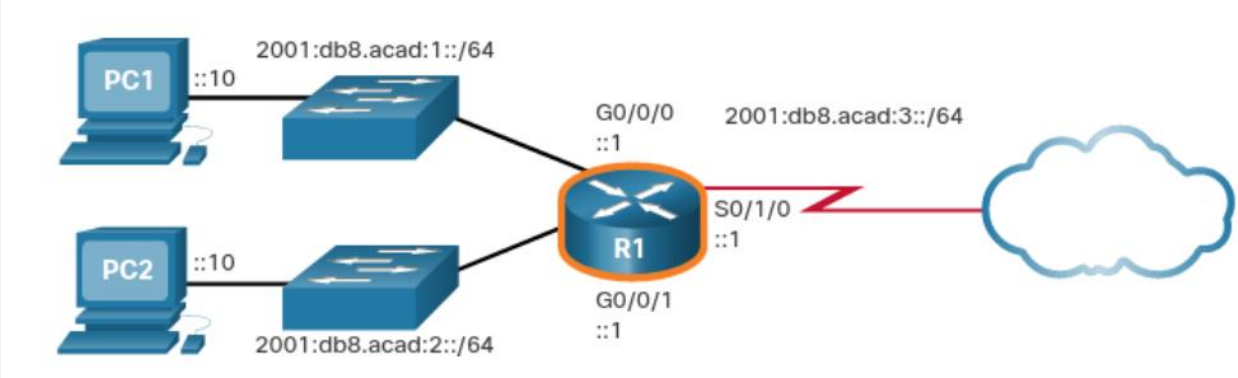
A IANA é responsável pelo gerenciamento dos blocos e distribuição pelos RIR. Cada **RIR recebe da IANA um bloco /12**. O **LACNIC** trabalha com o bloco **2800::/12** e o NIC.br trabalha com o /16 dentro desse bloco /12.

Os ISPs recebem no mínimo um /32, distribuindo então /48 e /64 para clientes, dependendo do escopo e do tamanho do cliente.

CONFIGURAÇÃO IPV6

A configuração de endereços IPv6 é muito semelhante a configuração de IPv4. Vamos ver nas principais plataformas a configuração de um endereço GUA, globalmente exclusivos e roteáveis na Internet.

Tomaremos como exemplo a seguinte topologia lógica, com os endereços indicados.



A configuração está nas portas 0/0/0 e 0/0/1 do roteador e na interface serial 0/1/0 do mesmo.

CONFIGURAÇÃO IPV6

Na plataforma Cisco, a configuração é feita com os seguintes comandos (roteadores e switches multicamadas). Quando for utilizado o endereço LLA, adicionar a palavra **link-local**

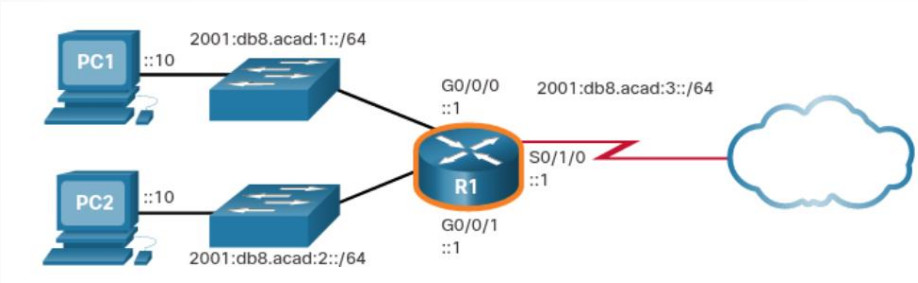
```
R1(config)# interface GigabitEthernet 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface GigabitEthernet 0/0/1
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/1/0
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# no shutdown
```

```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ipv6 address fe80::1:1 link-local
R1(config-if)# exit
```

CONFIGURAÇÃO IPV6

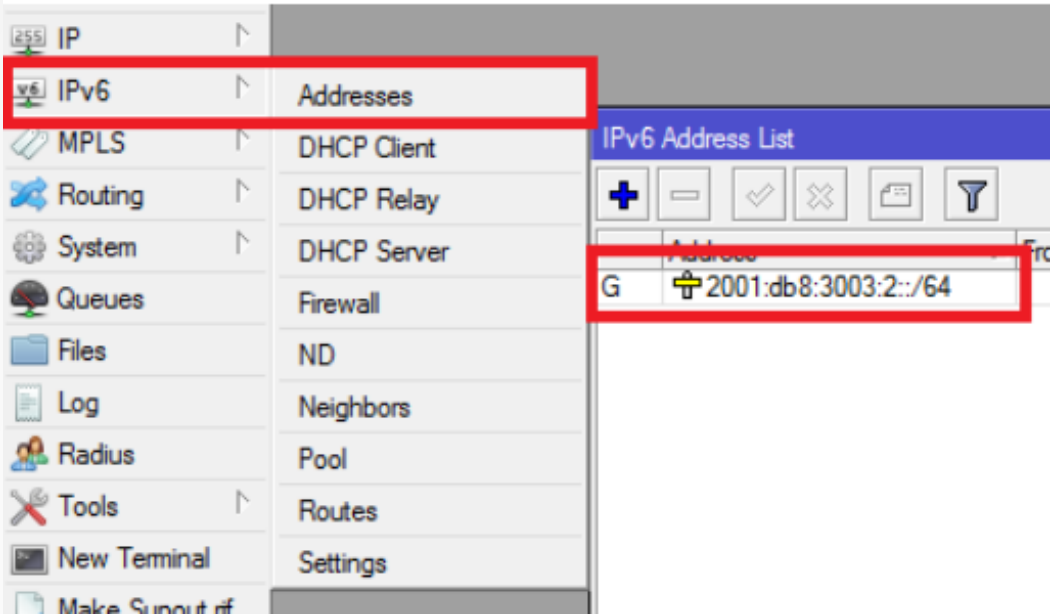
Observe o mesmo cenário construído em plataforma Huawei. Alguns preceitos mudam, por exemplo, é necessário ativar o IPv6 no system-view primeiramente para que seja possível endereçar as interfaces. Após isso, ativar o IPv6 também na interface para endereçá-la.

```
[R1]ipv6
[R1]interface gigabitethernet 0/0/0
[R1-GigabitEthernet0/0/0]ipv6 enable
[R1-GigabitEthernet0/0/0]ipv6 address 2001:db8:acad:1::1/64
[R1-GigabitEthernet0/0/0]ipv6 address fe80::1:1 link-local
[R1-GigabitEthernet0/0/0]undo shutdown
```



CONFIGURAÇÃO IPV6

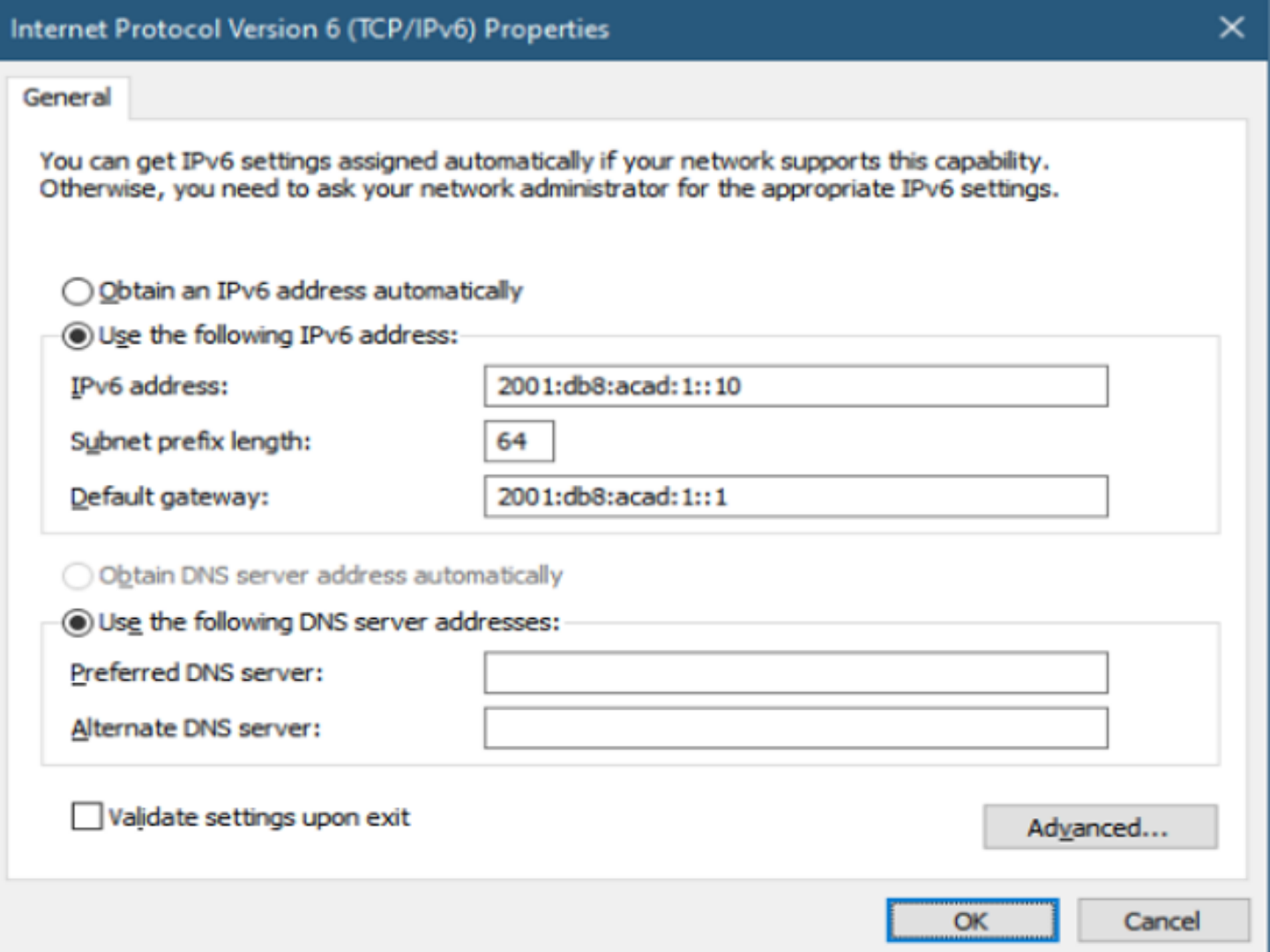
Em plataforma Mikrotik, podemos usar o menu **IPv6 > Addresses** e inserir o IP através do botão + que aparece na janela, escolhendo algumas opções. Ou pelo comando **/ipv6 address add address=2001:db8:b::2/64 interface=ether1 comment=INTERNET**



CONFIGURAÇÃO IPV6 EM HOSTS

A configuração IPv6 em Windows se dá por janela semelhante a configuração IPv4.

A configuração IPv6 em hosts Linux irá depender do Kernel e da versão do Sistema Operacional.


Internet Protocol Version 6 (TCP/IPv6) Properties
General
You can get IPv6 settings assigned automatically if your network supports this capability.
Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.
Obtain an IPv6 address automatically
Use the following IPv6 address:
IPv6 address:
2001:db8:acad:1::10
Subnet prefix length:
64
Default gateway:
2001:db8:acad:1::1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

Primeiro deve-se carregar o módulo IPv6 com o comando **modprobe ipv6**. Então adicionar a linha **alias net-PF-10 ipv6,** no arquivo correspondente a versão e depois executar a configuração.

- RedHat/Fedora/Mandriva/SuSE: /etc/modprobe.conf
- Ubuntu - Debian - Slackware: /etc/modprobe.d/aliases
- Outras versões ou se o arquivo não for encontrado:/etc/modules.conf

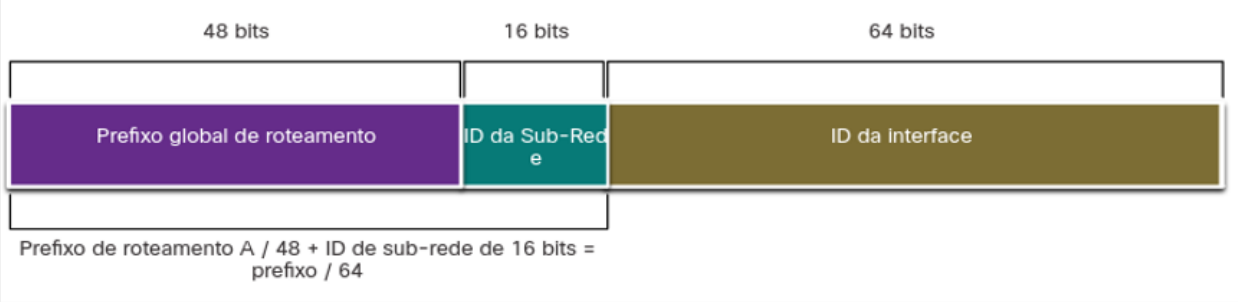

No arquivo etc/sysconfig/network adicionar:
NETWORKING_IPV6=yes
IPV6_DEFAULTGW='endereço IPv6 do gateway'
No arquivo /etc/sysconfig/network/ifcfg-'nome da interface' adicionar:
IPV6INIT=yes
IP6ADDR='endereço IPv6/prefixo'
Reiniciar a rede:
service network restart ou
/etc/init.d/network restart


No arquivo /etc/network/interfaces adicionar:
iface eth0 inet6 static

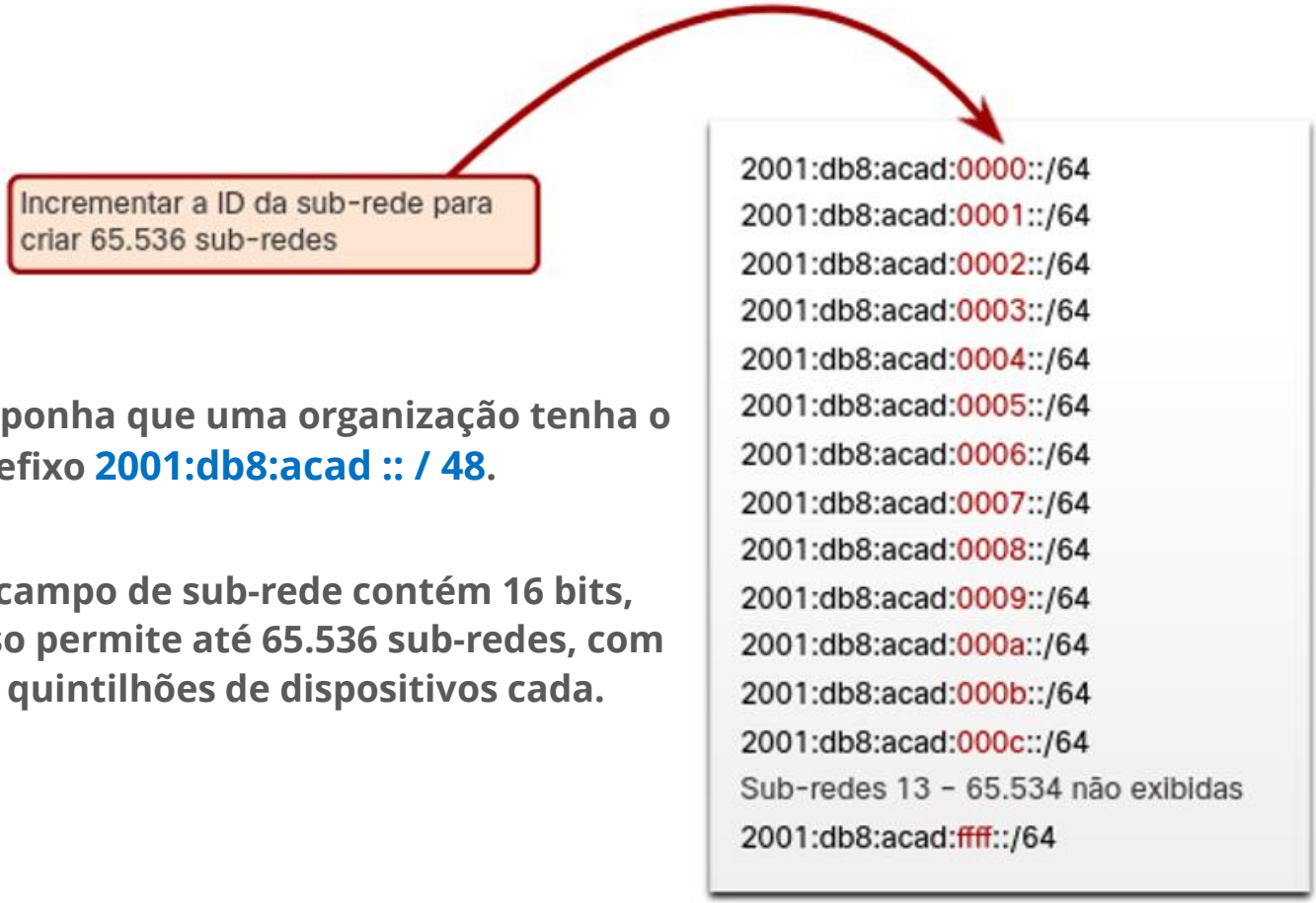
pre-up modprobe ipv6
address 'endereço IPv6'
netmask 64
gateway 'endereço IPv6 do gateway'
Reiniciar a rede:
ifup –force eth0

SEGMENTAÇÃO IPV6

Aprendemos anteriormente como criar subredes e segmentar uma rede IPv4. No IPv6 tem algumas facilidade, pois existe um campo próprio para isso na estrutura do endereço, entre o prefixo e o ID da interface.

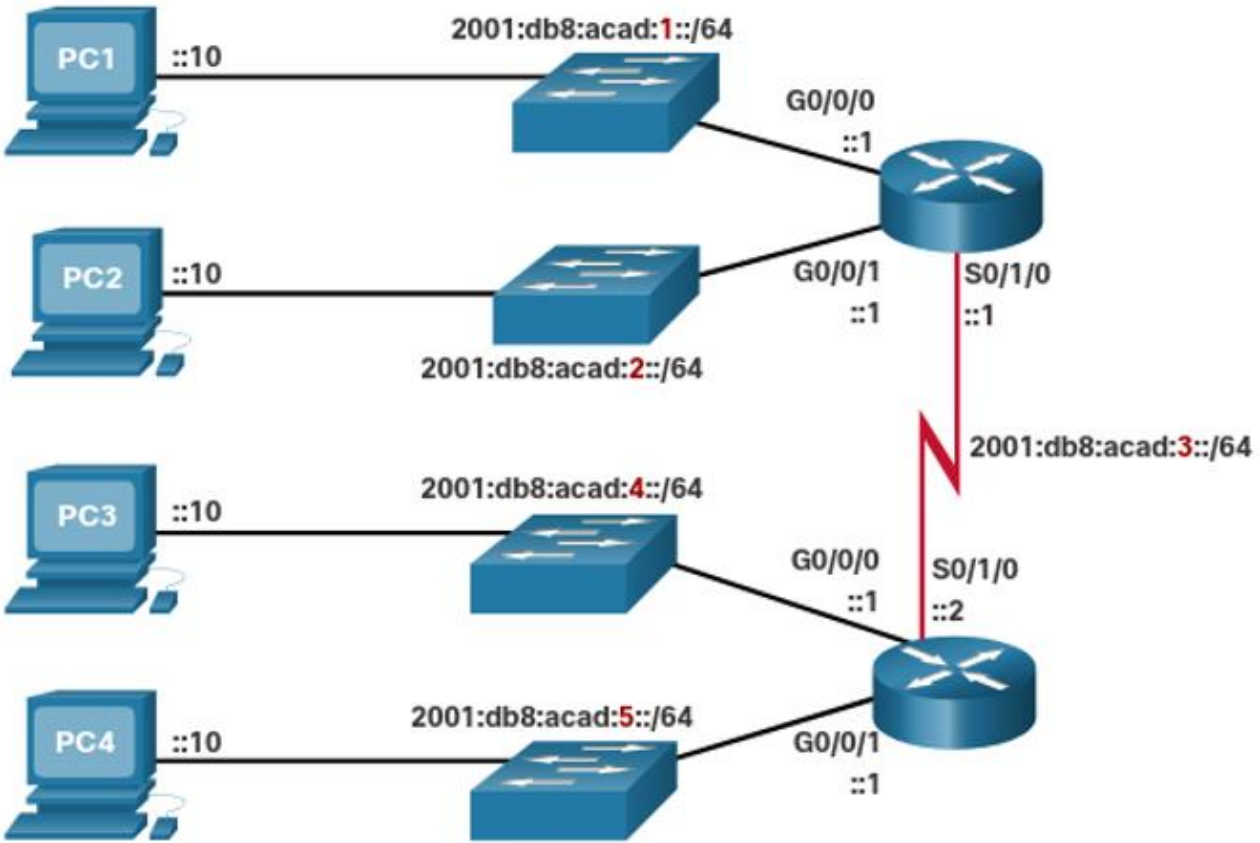


Por exemplo, com um prefixo /48 e um ID com 64 bits, sobram 16 bits para o campo da sub-rede. Não é necessário converter em binário para criar a sub-rede como no IPV4, **basta acrescentar uma unidade hexadecimal no campo**.



Suponha que uma organização tenha o prefixo 2001:db8:acad :: / 48.

O campo de sub-rede contém 16 bits, isso permite até 65.536 sub-redes, com 18 quintilhões de dispositivos cada.



EXEMPLO DE TOPOLOGIA COM ALOCAÇÃO DE SUB-REDE

```
R1(config)# interface GigabitEthernet 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface GigabitEthernet 0/0/1
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/1/0
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# no shutdown
```

EXEMPLO DE CONFIGURAÇÃO DE SUB-REDE NA INTERFACES

LABORATÓRIO

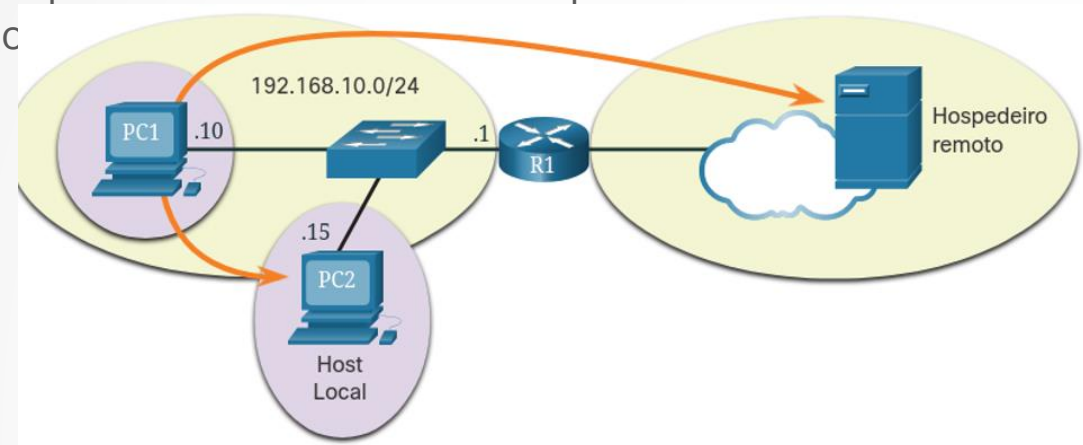
Criação de uma rede IPv6 básica com configuração de endereços nas interfaces.

- Cisco
- Huawei
- Mikrotik

ROTEAMENTO

Os pacotes, sejam IPv4 ou IPv6, são criados na origem e os dispositivos possuem uma **tabela de roteamento própria** ao enviar mensagens. Um host pode enviar pacotes para três destinos:

- **Próprio**: pacote enviado a ele mesmo, com endereços especiais IPv4 e IPv6, os quais veremos mais adiante.
- **Local**: pacote enviado a um host que está na mesma rede.
- **Remoto**: pacote enviado a um host que está em rede diferente ou remo



GATEWAY

Quando o pacote é enviado para **outra rede diferente da origem**, ou seja, quando acontece o roteamento, o dispositivo acionado é o gateway. Este nome é dado ao dispositivo responsável por processar pacotes que irão para redes remotas, comumente sendo um Switch ou um Roteador.

O gateway **se conecta a rede local**, servindo de "porta de saída" e possuindo um endereço no mesmo intervalo dessa rede local.

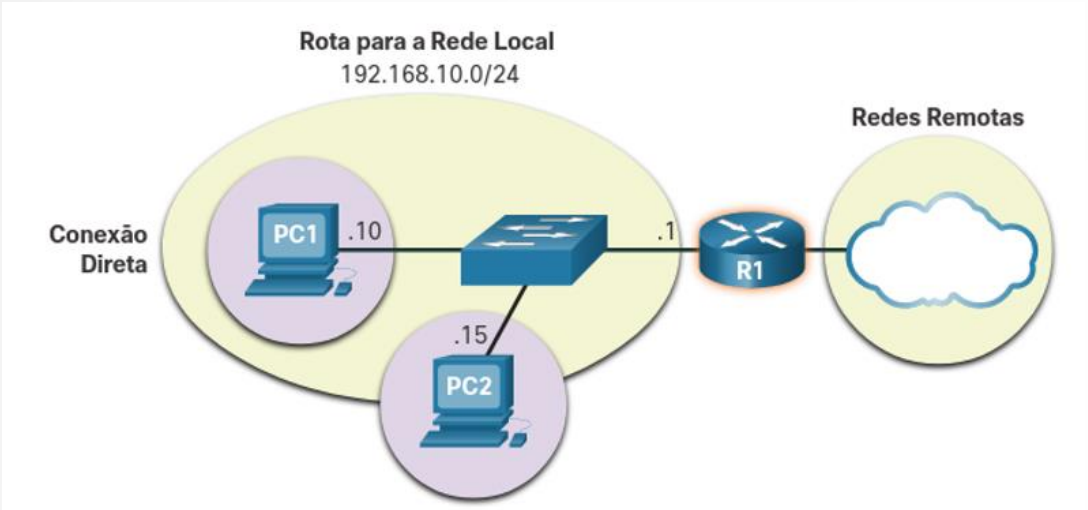


TABELA DE ROTEAMENTO

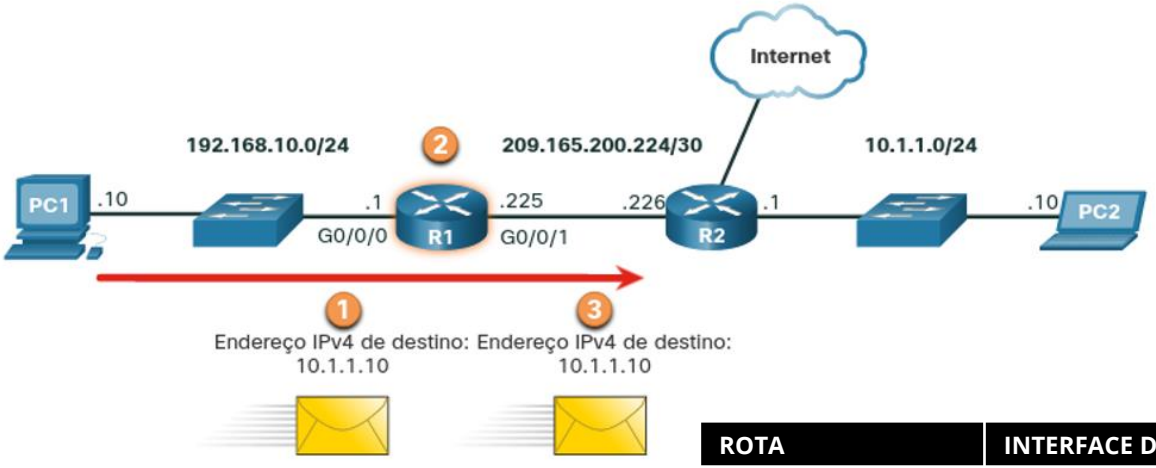
Para dispositivos finais, se inserirmos o comando **netstat –r / route print** para sistemas Windows, ou **netstat –rn / ip route** para sistemas Linux/Mac, iremos visualizar a tabela de roteamento do dispositivo. As informações parecem confusas mas são simples. Os resultados podem vir em 3 seções distintas:

- **Lista de interfaces**: lista o endereço da camada 2 e o número de interface atribuído de todas as interfaces de rede do dispositivo.
- **Tabela IPv4**: lista todas as rotas IPv4 conhecidas, entre conexões diretas, rede local e rotas padrão.
- **Tabela IPv6**: lista todas as rotas IPv6 conhecidas, entre conexões diretas, rede local e rotas padrão.


```
C:\Users\PC1 > netstat -r
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination Netmask Gateway Interface Metric
          0.0.0.0 0.0.0 192.168.10.1 192.168.10.10 25
        127.0.0.0 255.0.0.0 No link 127.0.0.1 306
        127.0.0.1 255.255.255.255 On-Link 127.0.0.1 306
  127.255.255.255 255.255.255 On-Link 127.0.0.1 306
     192.168.10.0 255.255.255.0 No link 192.168.10.10 281
    192.168.10.10 255.255.255.255 On-Link 192.168.10.10 281
   192.168.10.255 255.255.255.255 On-Link 192.168.10.10 281
        224.0.0.0 240.0.0.0 No link 127.0.0.1 306
        224.0.0.0 240.0.0.0 No link 192.168.10.10 281
  255.255.255.255 255.255.255.255 On-link 127.0.0.1 306
  255.255.255.255 255.255.255 On-Link 192.168.10.10 281
```

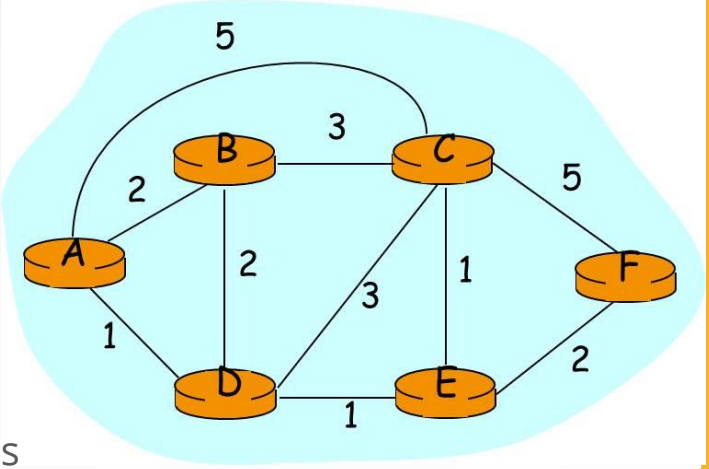
DECISÕES DO ROTEADOR

Os pacotes para redes remotas são encaminhados ao gateway, quase sempre um roteador. Ele irá examinar o pacote e consultar sua própria tabela de roteamento para determinar o melhor caminho (rota). No exemplo, temos a tabela de roteamento de R1



ROTA	INTERFACE DE SAÍDA
192.168.10.0/24	G0/0/0
209.165.200.224/30	G0/0/1
10.1.1.0/24	via R2
0.0.0.0/0	Via R2

QUAL O MELHOR CAMINHO?



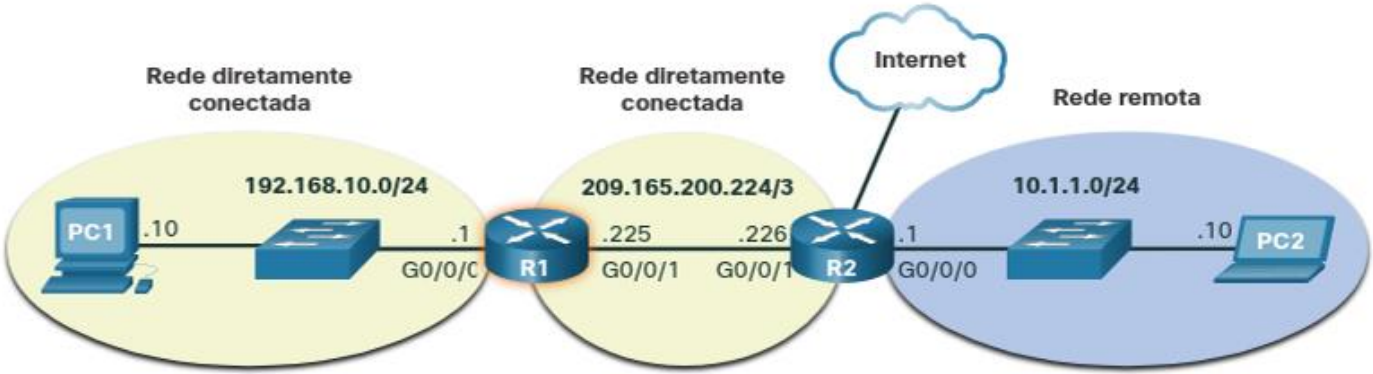
Roteadores utilizam algoritmos que calculam o melhor caminho baseado em algumas características como tráfego e colisões. Os algoritmos podem ser do tipo **Link-State** (“dirigir com um mapa”) ou **Distance-Vector** (“dirigir pedindo informações”) . Alguns algoritmos são:

- **RIP**: calcula com base no número de saltos até o destino.
- **OSPF**: além do número de saltos, analisa a condição de tráfego.
- **EIGRP**: protocolo proprietário da CISCO, idêntico ao OSPF, porém mais otimizado.
- **BGP**: utilizado nos *backbones* da Internet, na troca de rotas entre ISPs, sendo otimizado para grandes estruturas;

TABELA DE ROTEAMENTO DO ROTEADOR

Os roteadores podem armazenar 3 tipos de rotas em sua tabela:

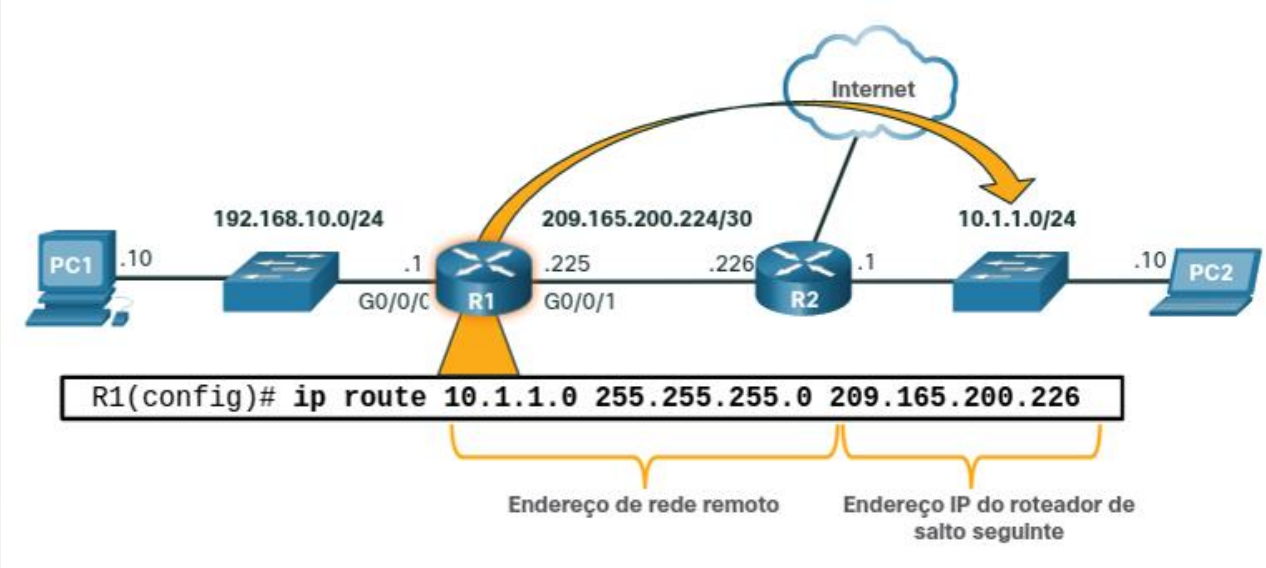
- **Conectadas Diretamente**: são adicionadas a partir das **interfaces ativas** do próprio roteador.
- **Remotas**: estão conectadas nas **interfaces de outros roteadores** e são adicionadas explicitamente por um administrador ou dinamicamente por protocolos específicos.
- **Rotas Padrão**: funciona como **gateway de último recurso**, isto é, quando não outra correspondência melhor na tabela de roteamento. Se não houver configuração de rota padrão, o roteador pode descartar pacotes indevidamente.



ROTA	INTERFACE DE SAÍDA
192.168.10.0/24	G0/0/0
209.165.200.224/30	G0/0/1
10.1.1.0/24	via R2
0.0.0.0/0	Via R2

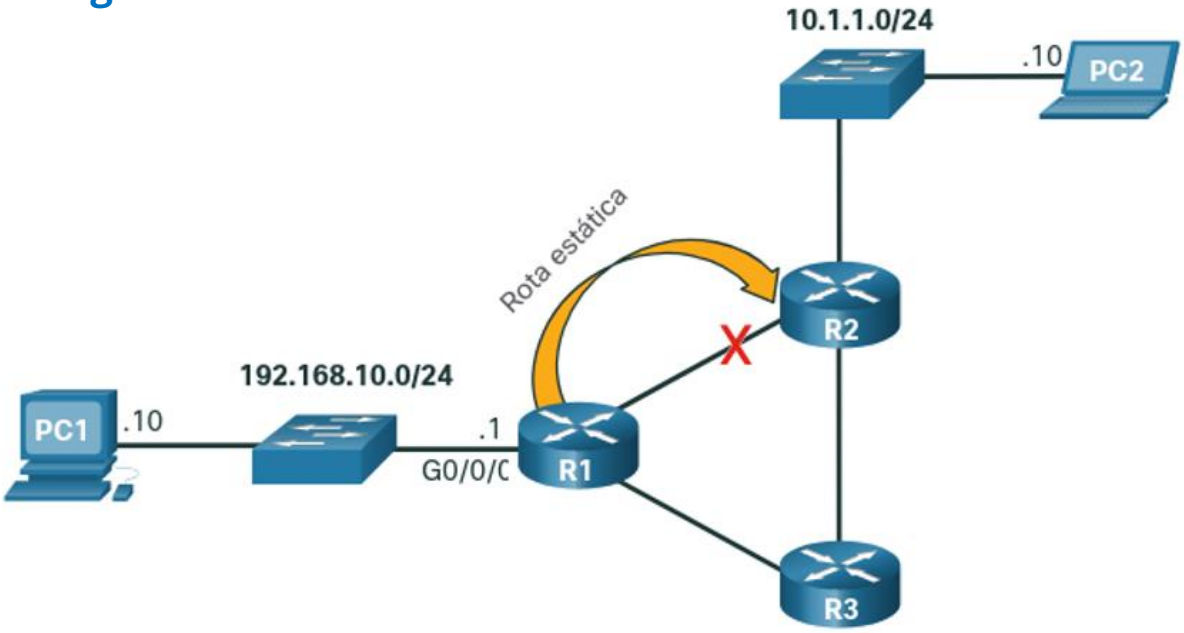
ROTAS ESTÁTICAS

Rotas estáticas são entradas de rotas, sejam de qualquer tipo, **configuradas manualmente**. Deve indicar o endereço da rede de destino e o endereço do roteador do próximo salto. Veja o exemplo de comando para adicionar uma rota estática em dispositivos Cisco.



ROTAS ESTÁTICAS

O grande problema em rotas estáticas é que **se o caminho mudar**, por exemplo com adição de novos roteadores ou indisponibilidade de uma interface, a **rota precisa ser reconfigurada**.



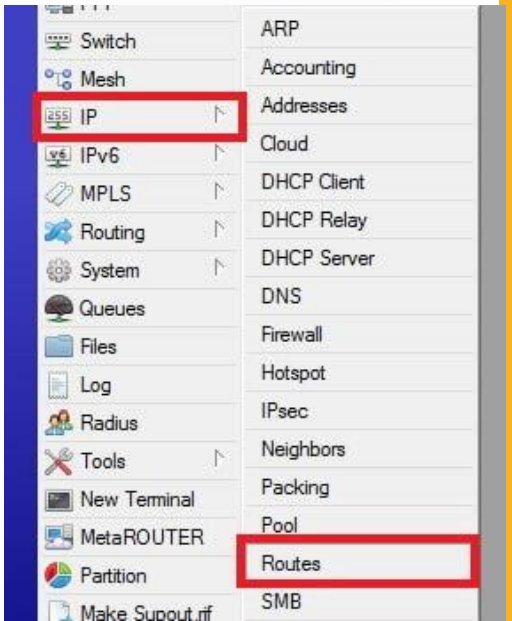
ROTAS ESTÁTICAS

Para equipamentos da plataforma Huawei/3COM, o comando básico para adicionar uma rota estática, com o mesmo exemplo anterior é:

ip route-static 10.1.1.0 255.255.255.0 209.165.200.226

Para equipamentos da plataforma Mikrotik, o comando básico para adicionar uma rota estática, com o mesmo exemplo anterior é:

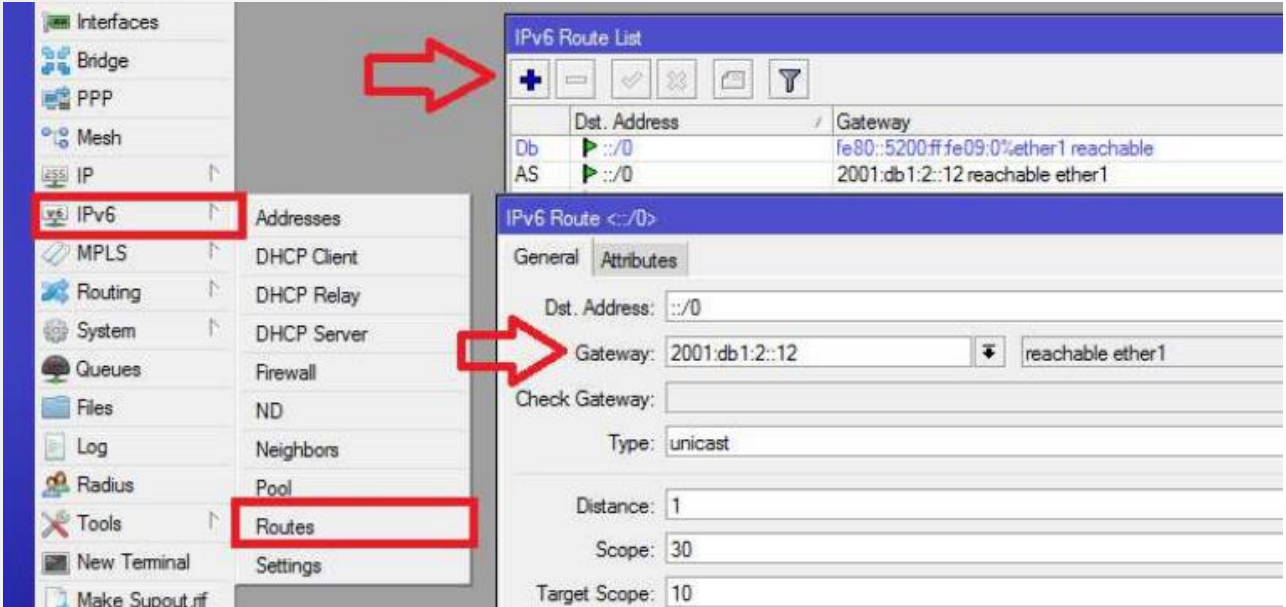
/ip route add
dst-address=192.168.2.0/24
gateway=172.16.1.2



ROTAS ESTÁTICAS

A rota estática em IPv6 para plataforma Huawei ficaria **ipv6 route-static ::0 2001:db8:2::12**

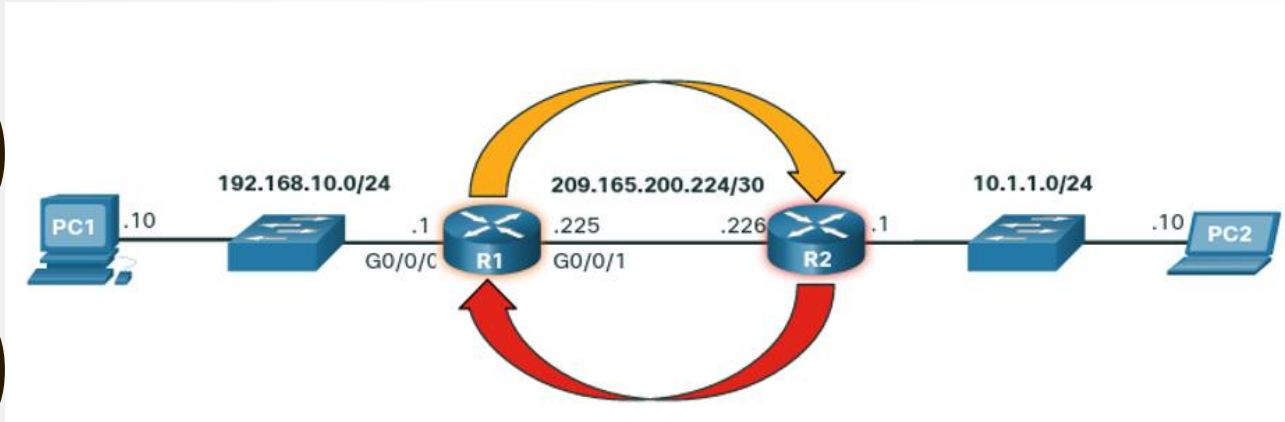
A rota estática IPv6 no Mikrotik pode ser pelo caminho conforme imagem ou pelo comando **/ipv6 route add dst-address==::/0 gateway=2001:db1:2::12**



ROTAS DINÂMICAS

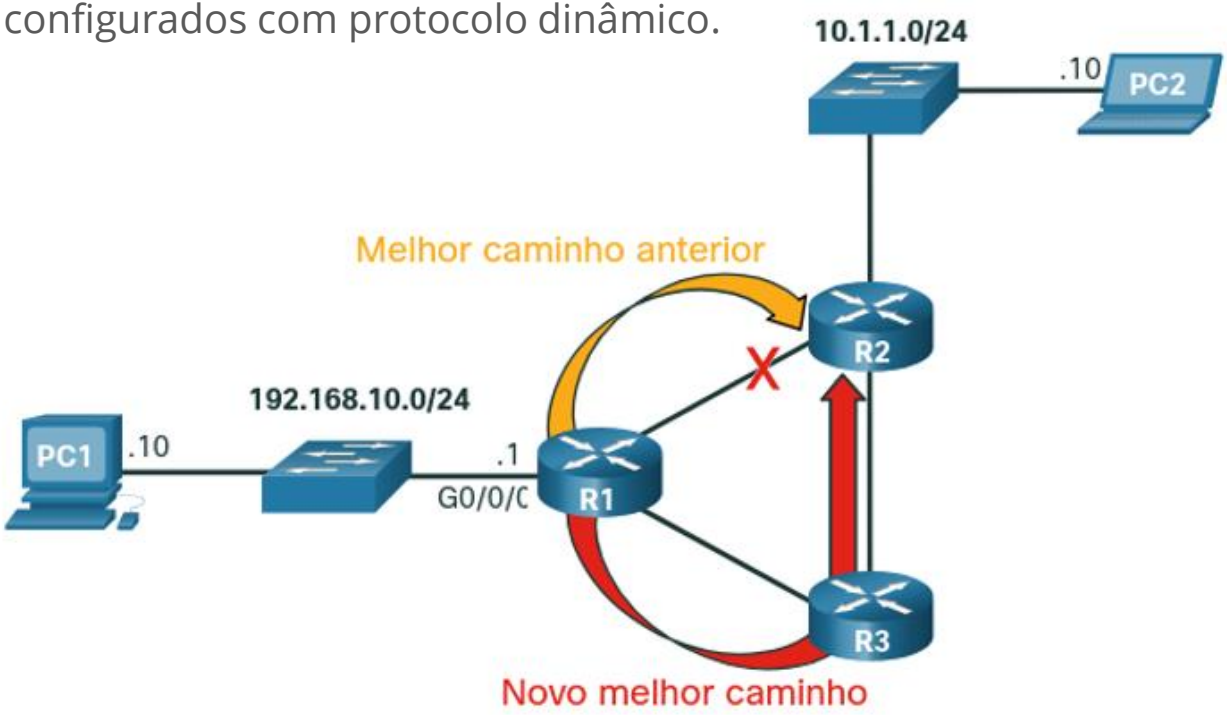
Rotas dinâmicas são entradas de rotas, sejam de qualquer tipo, **configuradas automaticamente** a partir de **trocas de informações entre roteadores**, através de um protocolo de roteamento dinâmico.

Qualquer alteração no caminho ou na topologia faz com que a tabela de roteamento seja atualizada automaticamente. Dois exemplos de protocolos são o OSPF e o EIGRP.



ROTAS DINÂMICAS

Como dito, qualquer alteração na rede atualiza automaticamente as tabelas de roteamento dos dispositivos configurados com protocolo dinâmico.

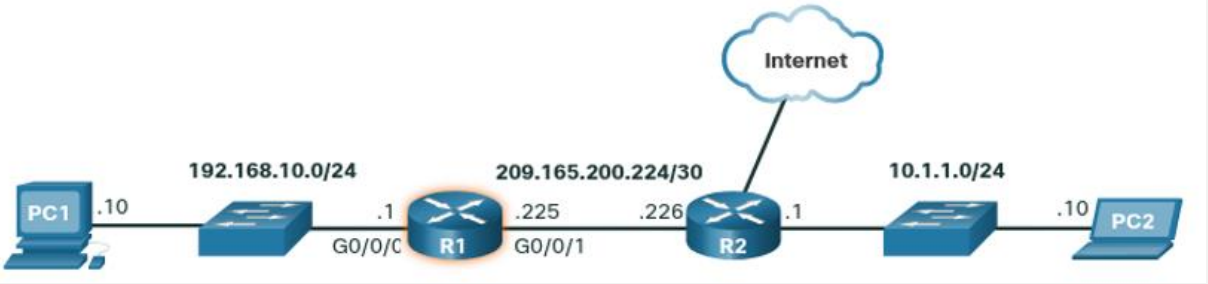


EXIBINDO A TABELA DE ROTAS

Ao exibir a tabela de rotas, seja em qualquer plataforma, o resultado será bastante parecido quanto as informações exibidas para a classificação da rota, sendo:

L: rota local da própria interface
C: rota diretamente conectada
S: rota estática, configurada manualmente
O: rota dinâmica aprendida via protocolo OSPF
D: rota dinâmica aprendida via protocolo EIGRP

Em plataformas Cisco, o comando para exibição da tabela de rotas é **show ip route**. Em plataformas Huawei/3COM, o comando é **display ip routing-table**. Em plataformas Mikrotik, o comando é **/ip route print**.



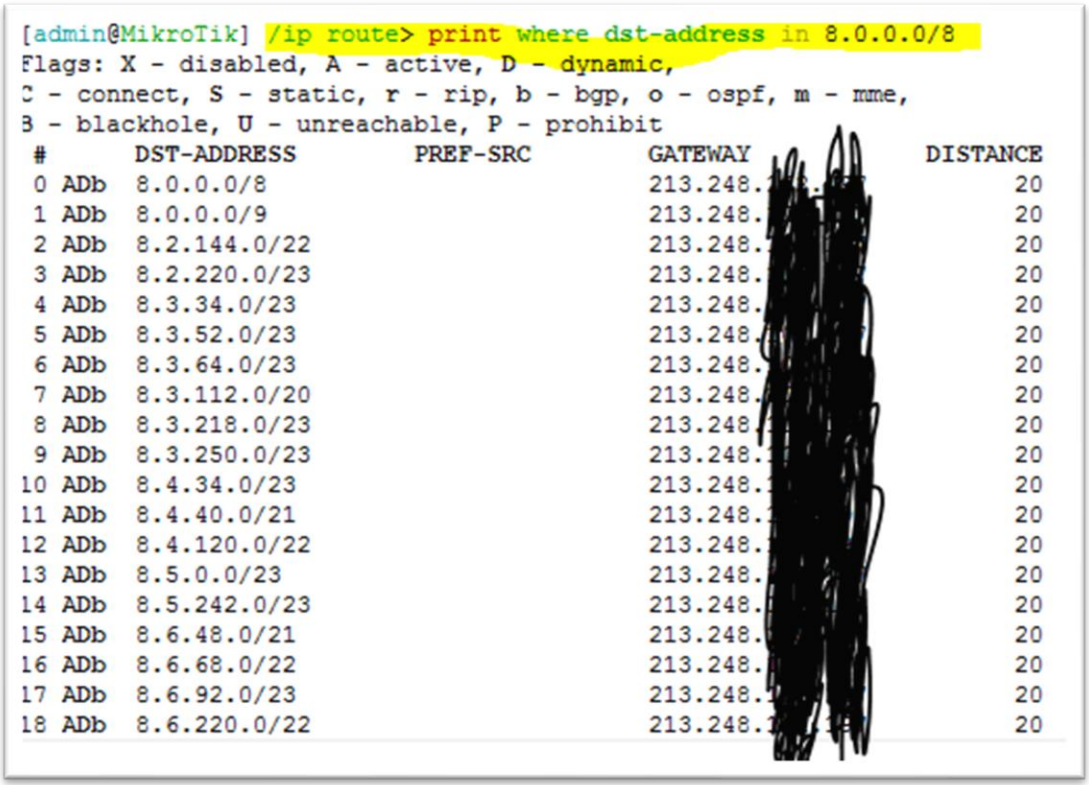

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 209.165.200.226 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 209.165.200.226, GigabitEthernet0/0/1
      10.0.0.0/24 is subnetted, 1 subnets
O        10.1.1.0 [110/2] via 209.165.200.226, 00:02:45, GigabitEthernet0/0/1
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, GigabitEthernet0/0/1
```

[Huawei] display ip routing-table
Route Flags: R - relay, D - download to fib

Routing Tables: Public Destinations : 2 Routes : 2

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
0.0.0.0/0	Static	60	0	D	120.0.0.2	Serial1/0/0
8.0.0.0/8	RIP	100	3	D	120.0.0.2	Serial1/0/0
9.0.0.0/8	OSPF	10	50	D	20.0.0.2	Ethernet2/0/0
9.1.0.0/16	RIP	100	4	D	120.0.0.2	Serial1/0/0
11.0.0.0/8	Static	60	0	D	120.0.0.2	Serial1/0/0
20.0.0.0/8	Direct	0	0	D	20.0.0.1	Ethernet2/0/0
20.0.0.1/32	Direct	0	0	D	127.0.0.1	Loopback0

Em plataformas Huawei/3COM, a classificação da rota é pela coluna **Proto**. A coluna **NextHop** indica o gateway de saída e a coluna **Interface** indica a porta ou interface lógica do dispositivo pelo qual o pacote será enviado.

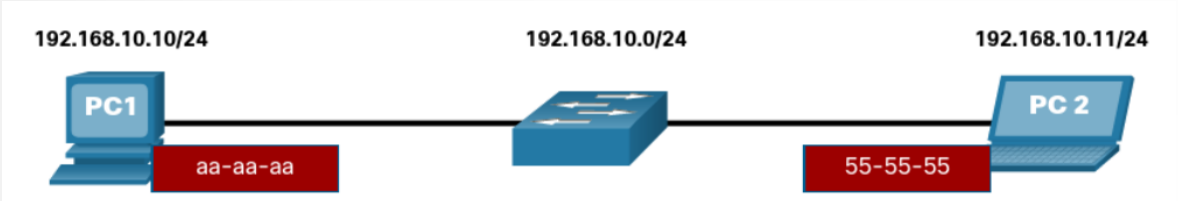


```
[admin@MikroTik] /ip route> print where dst-address in 8.0.0.0/8
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY                 DISTANCE
 0 ADb  8.0.0.0/8                          213.248.[redacted]             20
 1 ADb  8.0.0.0/9                          213.248.[redacted]             20
 2 ADb  8.2.144.0/22                       213.248.[redacted]             20
 3 ADb  8.2.220.0/23                       213.248.[redacted]             20
 4 ADb  8.3.34.0/23                        213.248.[redacted]             20
 5 ADb  8.3.52.0/23                        213.248.[redacted]             20
 6 ADb  8.3.64.0/23                        213.248.[redacted]             20
 7 ADb  8.3.112.0/20                       213.248.[redacted]             20
 8 ADb  8.3.218.0/23                       213.248.[redacted]             20
 9 ADb  8.3.250.0/23                       213.248.[redacted]             20
10 ADb  8.4.34.0/23                        213.248.[redacted]             20
11 ADb  8.4.40.0/21                        213.248.[redacted]             20
12 ADb  8.4.120.0/22                       213.248.[redacted]             20
13 ADb  8.5.0.0/23                         213.248.[redacted]             20
14 ADb  8.5.242.0/23                       213.248.[redacted]             20
15 ADb  8.6.48.0/21                        213.248.[redacted]             20
16 ADb  8.6.68.0/22                        213.248.[redacted]             20
17 ADb  8.6.92.0/23                        213.248.[redacted]             20
18 ADb  8.6.220.0/22                       213.248.[redacted]             20
```

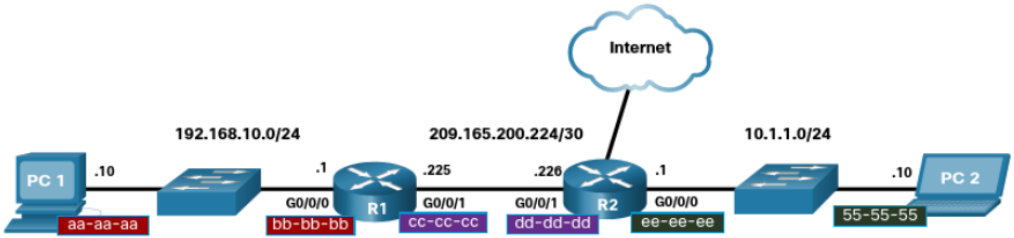
Em plataformas Mikrotik, a rota ainda vem sinalizada se está ativa e se está alcançável.

RELACIONAMENTO L2 E L3

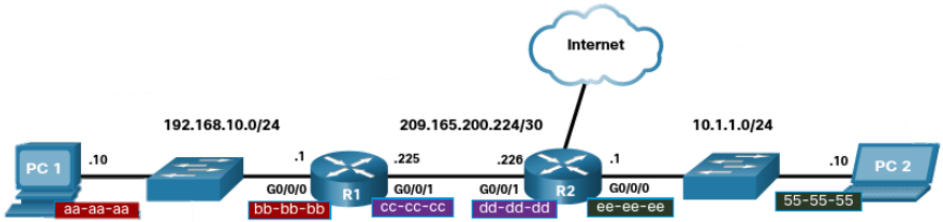
Na entrega de mensagens em uma rede, são utilizados os endereços da camada de enlace de dados e da camada de rede. Quando a entrega é local, ou seja, na mesma rede, o endereço L2 de destino é o próprio host de destino. Quando a entrega é remota, o endereço L2 de destino é o do próximo salto. A determinação do tipo de entrega é via endereço L3.

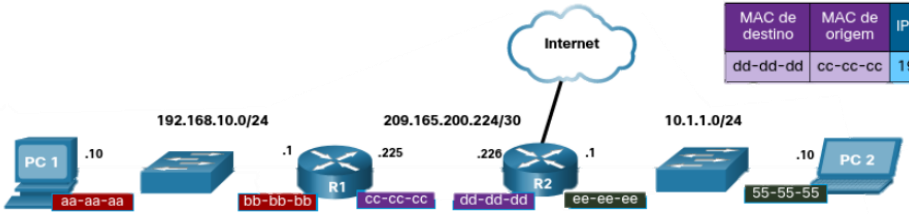


MAC de destino	MAC de origem	IPv4 de origem	IPv4 de destino
55-55-55	aa-aa-aa	192.168.10.10	192.168.10.11



MAC de destino	MAC de origem	IPv4 de origem	IPv4 de destino
bb-bb-bb	aa-aa-aa	192.168.10.10	10.1.1.10



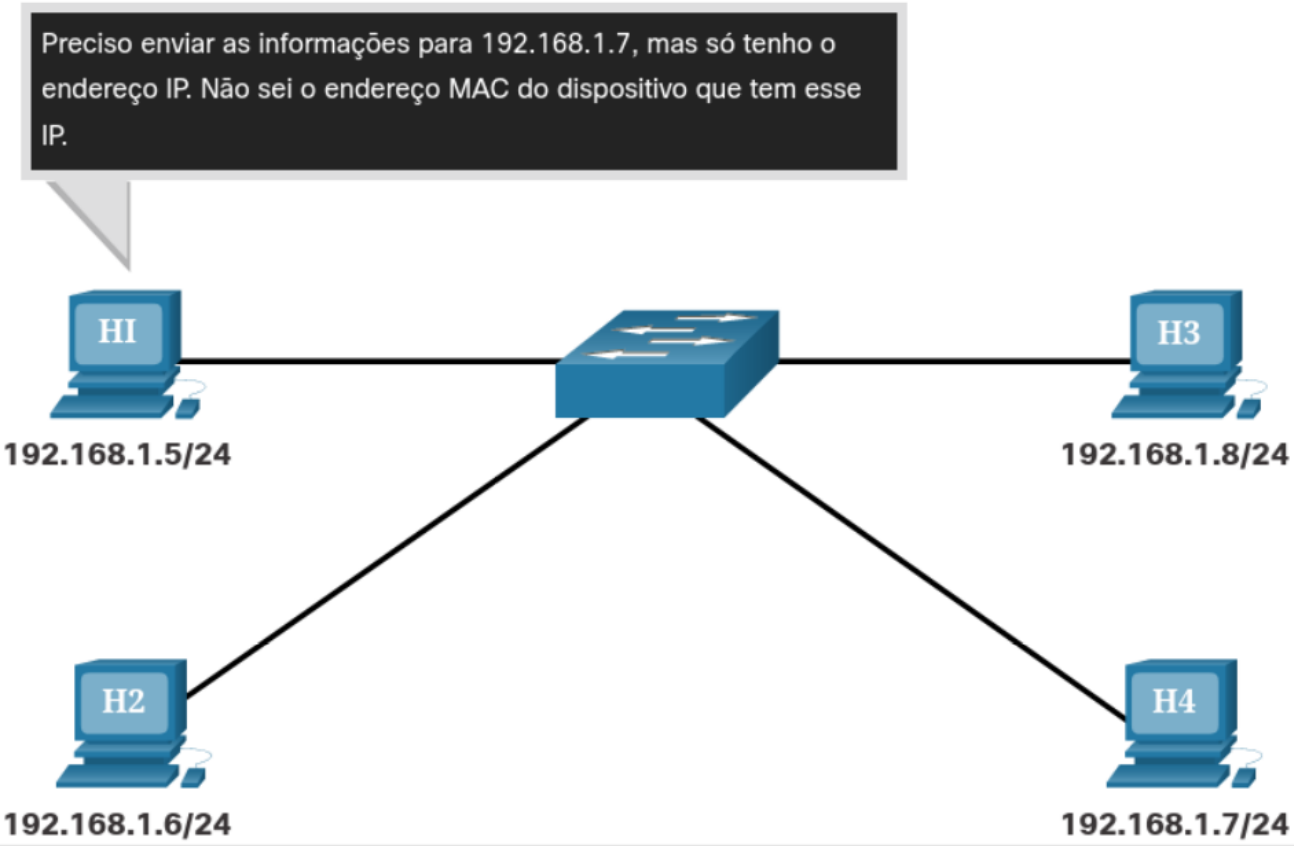


MAC de destino	MAC de origem	IPv4 de origem	IPv4 de destino
dd-dd-dd	cc-cc-cc	192.168.10.10	10.1.1.10

MAC de destino	MAC de origem	IPv4 de origem	IPv4 de destino
55-55-55	ee-ee-ee	192.168.10.10	10.1.1.10

DESCOBERTA DE L2

Como visto, as mensagens contém o endereço L2 (para entrega NIC-a-NIC) e o endereço L3 (para determinação remoto/local). Quando o dispositivo possui apenas o endereço L3, faz uso do protocolo **ARP** para descobrir o endereço L2. O processo contrário é feito pelo protocolo **RARP**. O ARP funciona apenas em redes IPv4. Em redes IPv6, esse processo é o **ICMPv6 ND**.


Preciso enviar as informações para 192.168.1.7, mas só tenho o endereço IP. Não sei o endereço MAC do dispositivo que tem esse IP.
HI
H3
192.168.1.5/24
192.168.1.8/24
H2
H4
192.168.1.6/24
192.168.1.7/24

PROTOCOLO ARP

O ARP tem duas funções principais, a **resolução de endereços IPv4 em endereços MAC** e **administrar o mapeamento entre os endereços**, chamada tabela **ARP**.

Quando um dispositivo precisa descobrir o endereço MAC de outro a partir do IPv4, ele pesquisa em sua própria tabela ARP. Se a **entrega for local**, ele pesquisará o endereço **MAC do host de destino**, se a **entrega for remota**, ele pesquisará o endereço **MAC do gateway**.

Se a pesquisa não trouxer resultados, o dispositivo envia na rede uma **requisição ARP**.

REQUISIÇÃO ARP

Uma solicitação/requisição ARP é enviada quando o dispositivo emissor precisa **determinar o endereço MAC do destino**. A mensagem enviada não tem cabeçalho IP, sendo apenas um quadro Ethernet, com as seguintes características:

- **Endereço L2 de destino**: sai como endereço de broadcast FF-FF-FF-FF-FF-FF, de modo que todos os hosts recebam e processem a requisição.
- **Endereço L2 de origem**: o endereço MAC do solicitante.
- **Tipo**: o campo tipo do quadro Ethernet recebe o valor 0x806

Somente um dispositivo responderá a requisição com o endereço MAC correspondente.

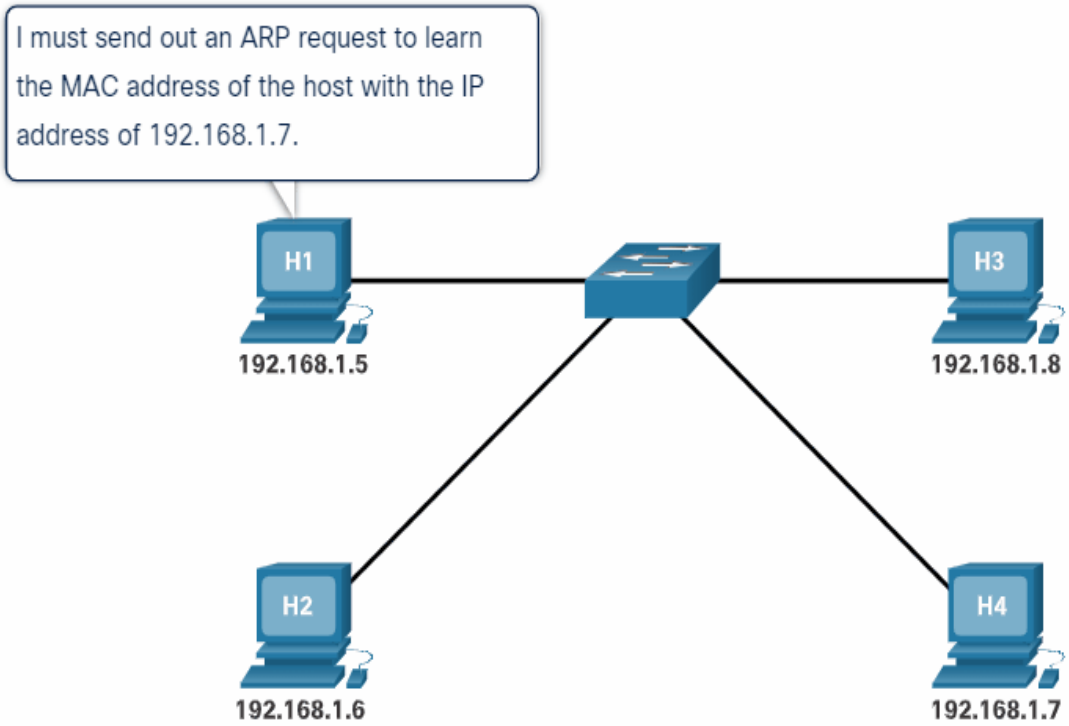
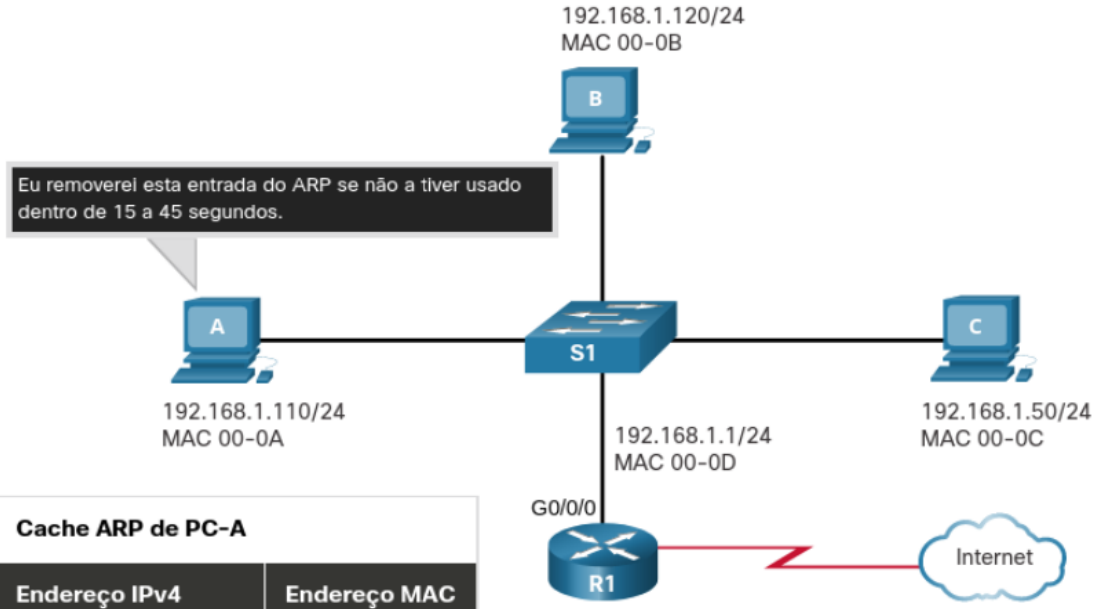

I must send out an ARP request to learn the MAC address of the host with the IP address of 192.168.1.7.
H1
192.168.1.5
H3
192.168.1.8
H2
192.168.1.6
H4
192.168.1.7

TABELA ARP

Os hosts guardam as resoluções ARP numa tabela, como um cache, contendo um **temporizador** para cada entrada, geralmente de **15 a 45 segundos**. A entrada também pode ser removida ou inserida com comandos.



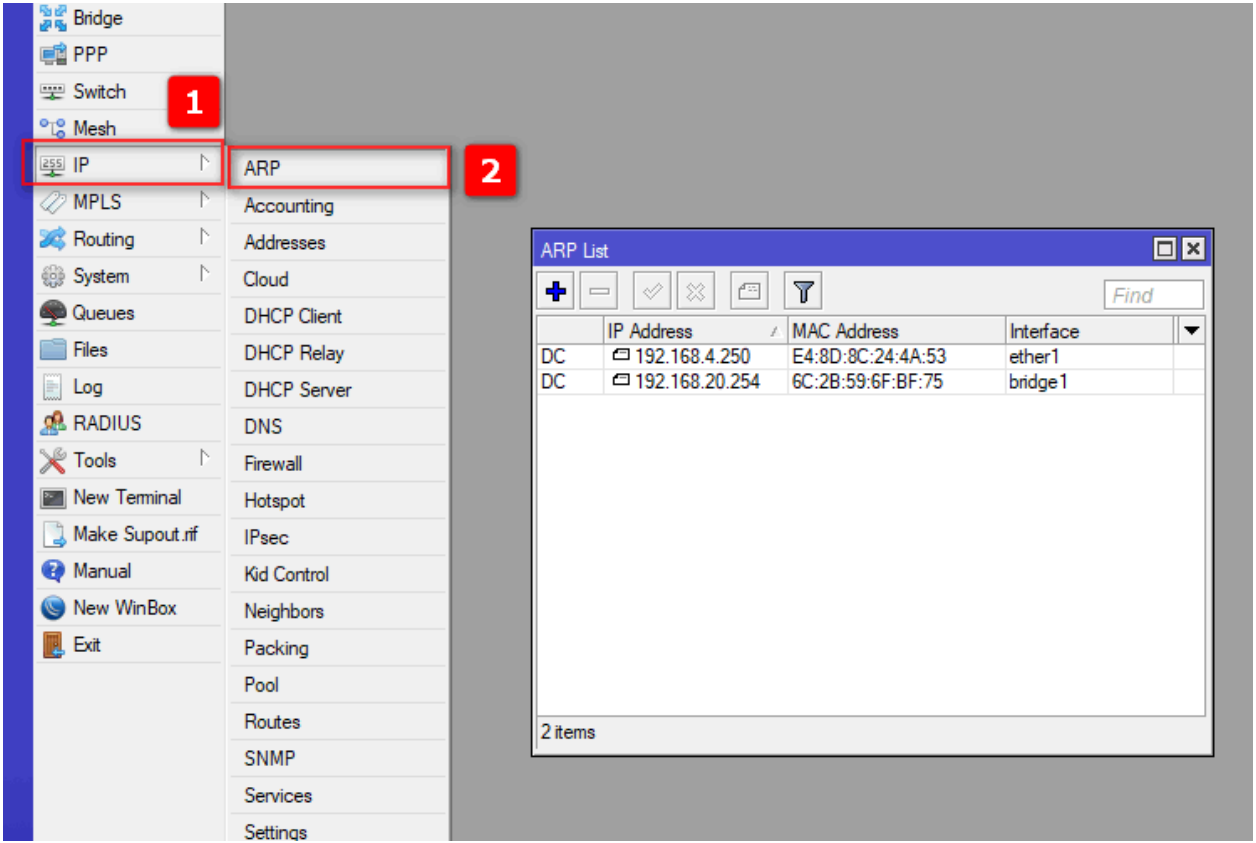
Cache ARP de PC-A	
Endereço IPv4	**Endereço MAC**
192.168.1.1	00:0 D

```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.10.1            -   a0e0.af0d.e140  ARPA   GigabitEthernet0/0/0
Internet  209.165.200.225          -   a0e0.af0d.e141  ARPA   GigabitEthernet0/0/1
Internet  209.165.200.226          1   a03d.6fe1.9d91  ARPA   GigabitEthernet0/0/1
R1#
```

Em plataforma Cisco, podemos visualizar a tabela ARP com o comando **show ip arp**

```
<FW>display arp
2017-11-07 17:27:54.130 +02:00
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE INTERFACE      VPN-INS
                                          VLAN
------------------------------------------------------------------------
192.168.1.1     48fd-8e10-4680            I -  GE0/0/0        default
1.1.1.1         48fd-8e10-4681            I -  GE0/0/1
1.1.1.5         2047-47af-f37f  6         D-0  GE0/0/1
```

Em plataforma Huawei, podemos visualizar a tabela ARP com o comando **display arp**. Em hosts com Windows ou Linux, o comando para visualizar a tabela ARP é **arp -a**

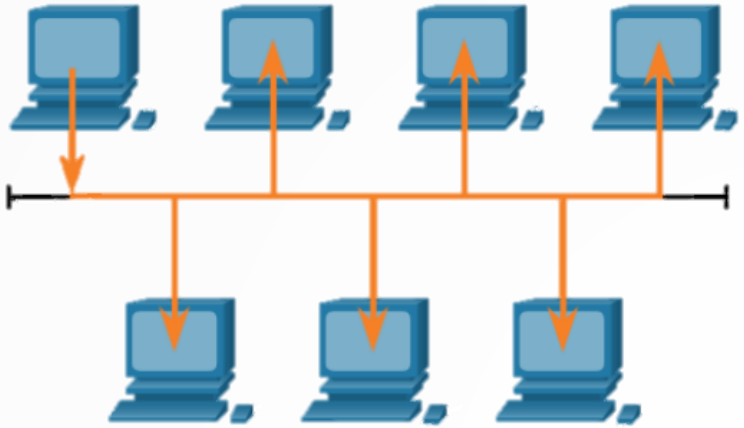


Em equipamentos Mikrotik, o comando é /ip arp print

PROBLEMAS DO ARP

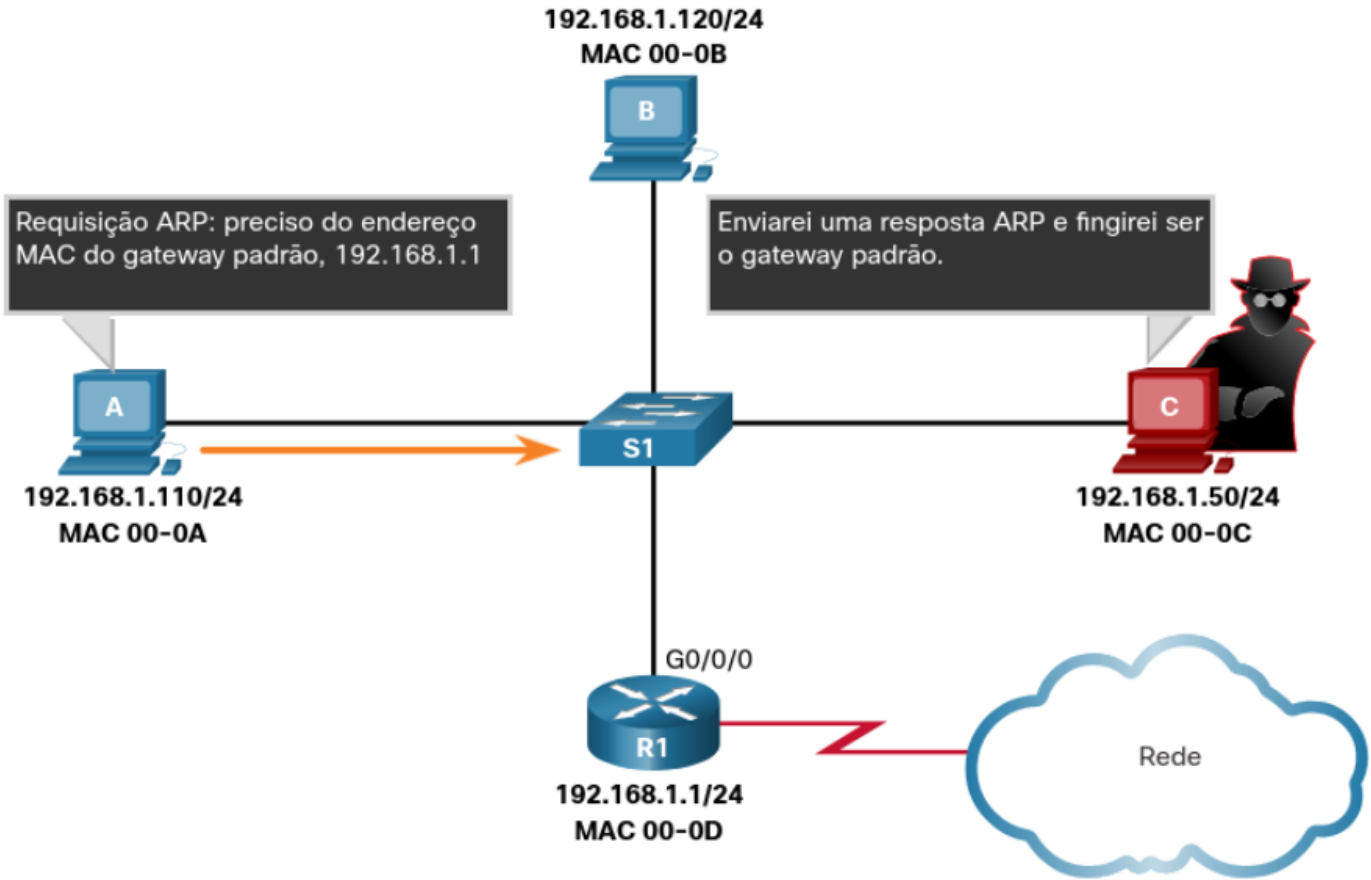
Como as requisições ARP são do tipo broadcast, isto é, a mensagem é inundada na rede, e elas são frequentes, se houver muitos equipamentos conectados, o desempenho pode ser comprometido.

Broadcasts ARP podem inundar a mídia local.



ARP POISON/SPOOFING

As requisições ARP podem sofrer ataque de envenenamento / falsificação. Acontece quando um **atacante responde falsamente uma requisição ARP** se passando por outro dispositivo, como um gateway. O solicitante então adicionará o MAC do atacante na tabela ARP e enviar pacotes para ele.


192.168.1.120/24
MAC 00-0B
B
Requisição ARP: preciso do endereço MAC do gateway padrão, 192.168.1.1
Enviarei uma resposta ARP e fingirei ser o gateway padrão.
A
S1
C
192.168.1.110/24
MAC 00-0A
192.168.1.50/24
MAC 00-0C
G0/0/0
R1
192.168.1.1/24
MAC 00-0D
Rede

DESCOBERTAS IPV6

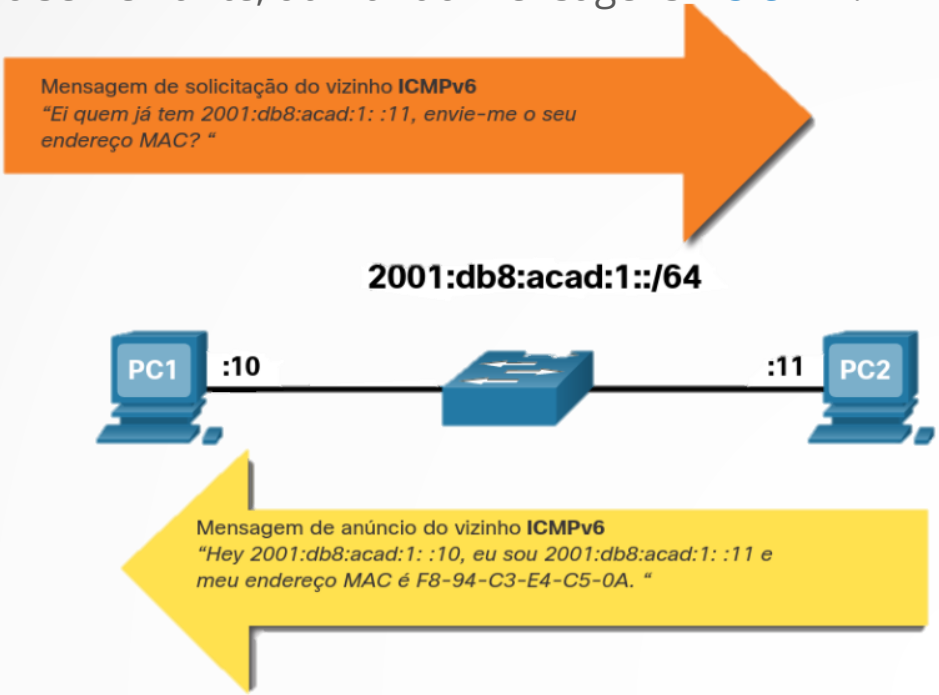
Em uma rede IPv6, o protocolo ND ou NDP faz o trabalho delegado ao ARP numa rede IPv4. Ele fornece serviços de resolução de endereços, descoberta de vizinhos e entrega de mensagens ICMPv6. São 5 tipos de mensagens utilizadas:

- **Solicitação de Vizinho** (Neighbor Solicitation)
- **Anúncio de Vizinho** (Neighbor Advertisement)
- **Solicitação de Roteador** (Router Solicitation)
- **Anúncio de Roteador** (Neighboor Solicitation)
- **Redirecionar Mensagem** (Redirect)

As mensagens de vizinho são utilizadas entre dispositivos finais (como o ARP), enquanto as mensagens de roteador são utilizadas entre dispositivos finais e roteadores. O redirecionamento é utilizado para determinar o próximo salto do pacote.

VIZINHOS IPV6

No protocolo ARP, para descobrir o endereço MAC, os dispositivos enviam uma mensagem **broadcast** para obter uma resposta do dispositivo com o IPv4 correspondente. No IPv6, o protocolo ND faz um processo semelhante, utilizando mensagens **NS e NA**.



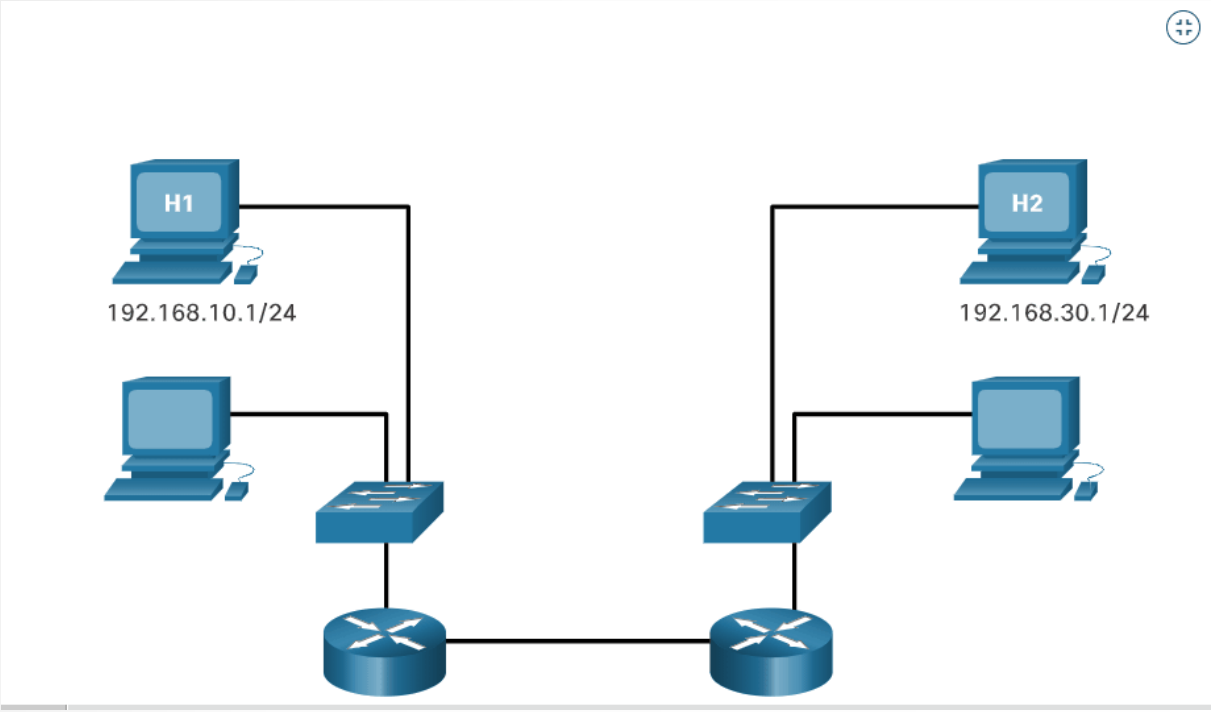
O PROTOCOLO ICMP

O protocolo ICMP é de grande utilidade em redes, pois podem fornecer serviços de **mensagem sobre o processamento** de pacotes sob certas condições. Porém por questões de segurança são por vezes desabilitadas. Alguns exemplos de serviços ICMP são:

- **Informar sobre acessibilidade do host**: podemos utilizar ICMP para testar a **capacidade de acesso** a um host em uma rede IP.
- **Informar se o destino está alcançável**: quando um **pacote não pode ser entregue**, o emissor recebe uma mensagem que o destino está inalcançável.
- **Informar se a mensagem está chegando ao destino a tempo**: usado para informar que o pacote **chegou ao fim da vida útil** antes da chegada ao destino.

ACESSIBILIDADE DO HOST

O host emissor envia uma solicitação ICMP (**Echo Request**). Se o destino estiver disponível, enviará uma resposta (**Echo Reply**). Esta é a base do utilitário **ping**.



DESTINO INACESSÍVEL

Quando um pacote não pode ser entregue ao próximo destino, uma mensagem é enviada a origem para informar a inacessibilidade, junto a um **código** com o motivo. Alguns dos códigos ICMPv4 são os seguintes:

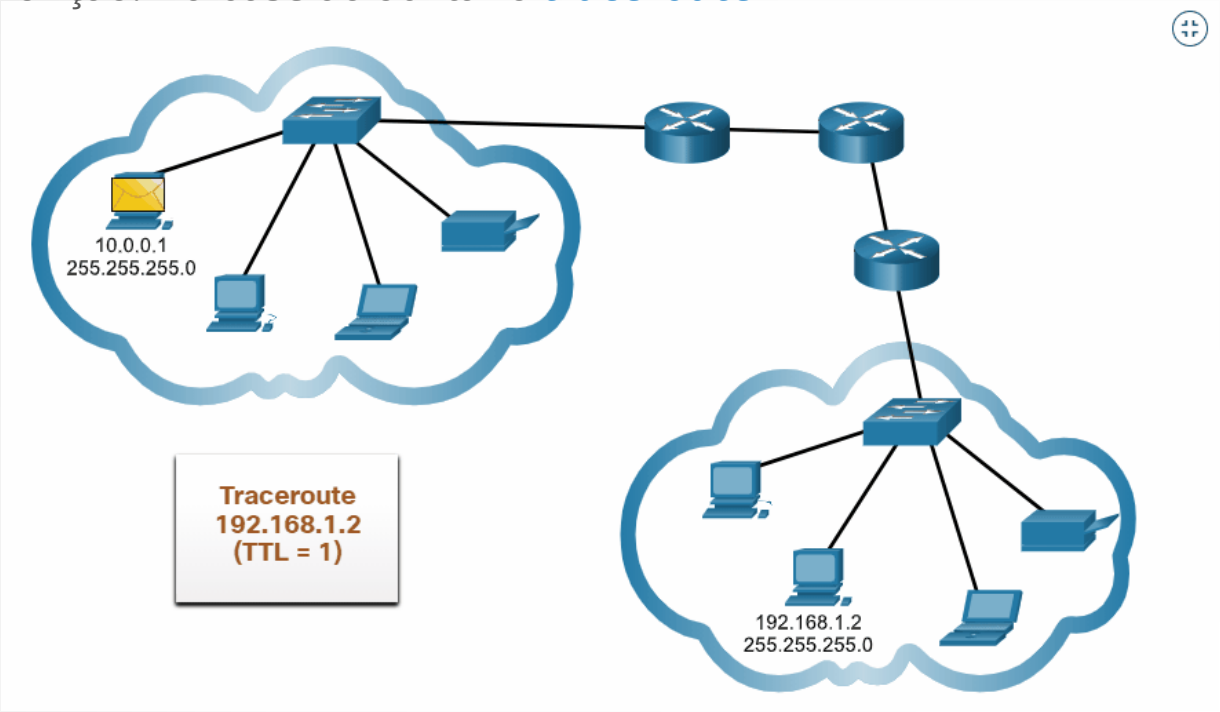
0 – Rede inacessível
1 – Host inacessível
2 – Protocolo inacessível
3 – Porta inacessível

Alguns dos códigos para ICMPv6 são os seguintes:

0 – Sem rota para o destino
1 – A comunicação com o destino é proibida administrativamente
2 – Além do escopo do endereço de origem
3 – Endereço inacessível
4 – Porta inacessível

TEMPO DE VIDA ÚTIL

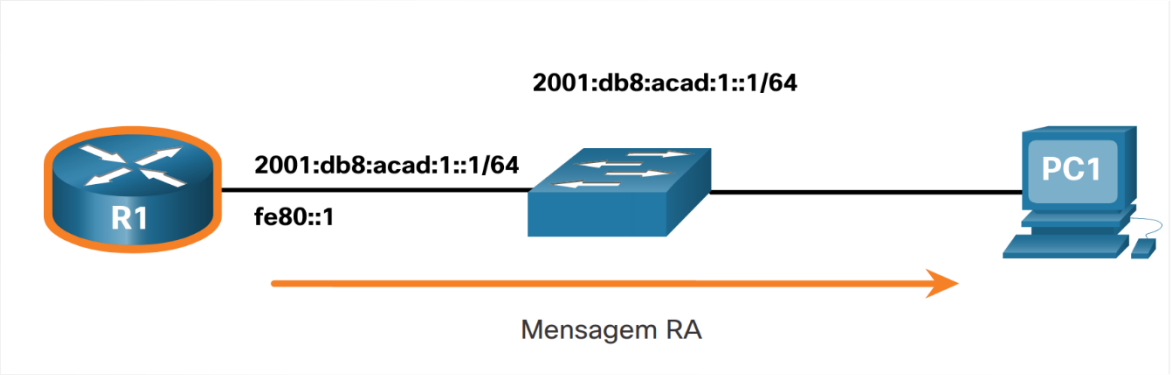
Se um pacote é recebido e seu campo de tempo de vida (**TTL**) é decrementado pra zero, o pacote é descartado e a origem é notificada. O IPv6 utiliza o campo **Limite de Salto** para essa função. É a base do utilitário **traceroute**



MENSAGENS ICMPV6

As mensagens ICMPv6 incluem comumente serviços de descoberta, alocação de endereços e anúncios.

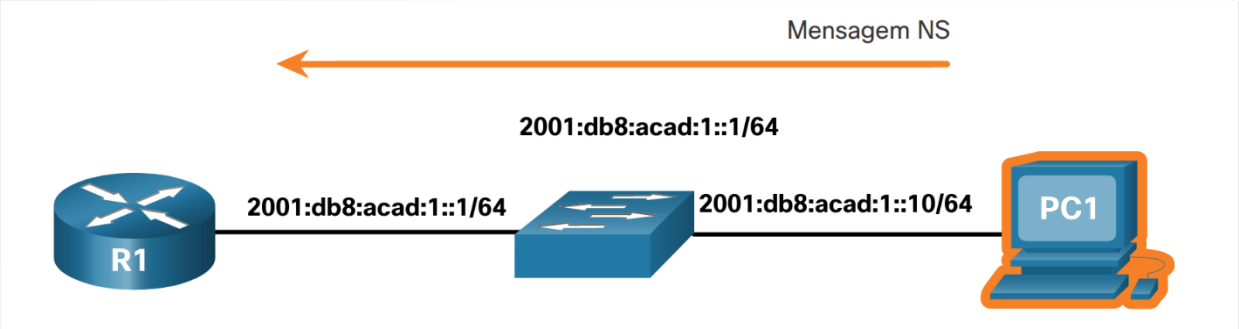
- **Mensagens RA:** são enviadas por roteadores a **cada 200 segundos** para fornecer informações de endereçamento para hosts, como prefixo, DNS, nome de domínio, etc.



R1 envia uma mensagem RA, "Olá, dispositivos habilitados para IPv6. Eu sou R1 e você pode criar um endereço GUA IPv6. O prefixo é 2001: db8: acad: 1 :: / 64. A propósito, use meu endereço local de link fe80 :: 1 como seu gateway padrão. "

MENSAGENS ICMPV6

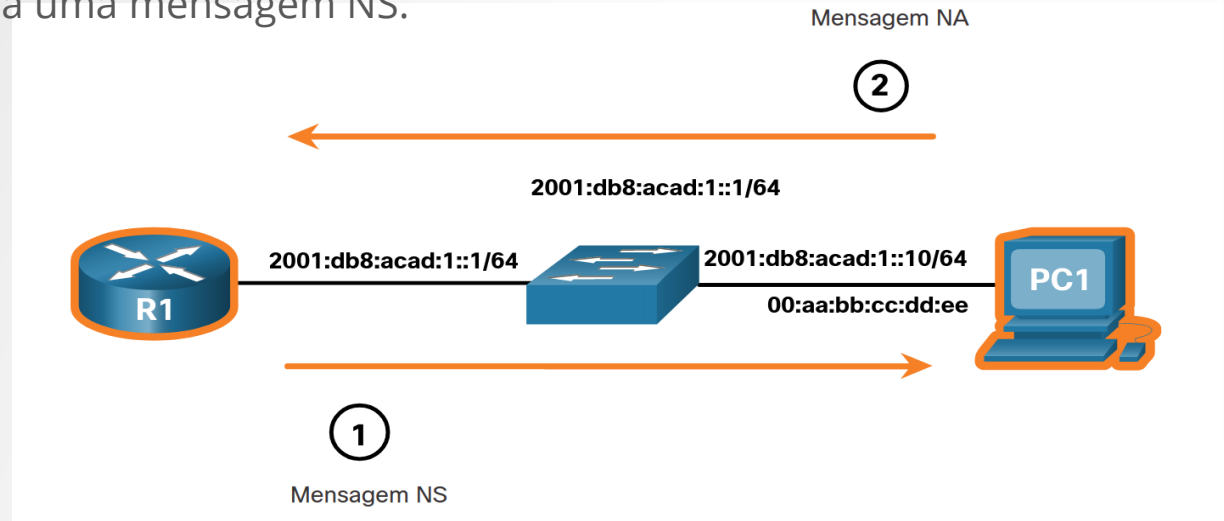
- Mensagens NS: são enviadas por hosts, como uma "**pergunta**", para consultar a exclusividade de um endereço IPv6 na rede. Se não houver resposta dentro de determinado período de tempo, o endereço será aceito para uso. Usado também na **resolução de endereços**, semelhante ao ARP no IPv4



PC1 envia uma mensagem NS para verificar a exclusividade de um endereço, "Quem tiver o endereço IPv6 2001: db8: acad: 1 :: 10, envie-me seu endereço MAC?"

MENSAGENS ICMPV6

- Mensagens NA: são enviadas por hosts, como uma "**resposta**", a uma mensagem NS.



R1 envia uma mensagem NS de resolução de endereço. "Quem tiver o endereço IPv6 2001: db8: acad: 1 :: 10, envie-me seu endereço MAC?"

PC1 responde com uma mensagem NA. "Eu sou 2001: db8: acad: 1 :: 10 e meu endereço MAC é 00: aa: bb: cc: dd: ee."

LABORATÓRIO

Teste de Ping e Traceroute e observação das mensagens ICMP.

- Ping no loopback
- Ping no host local
- Ping no gateway
- Ping no host remoto

CAMADA DE TRANSPORTE

PROPÓSITOS

No modelo TCP/IP, a camada de transporte faz o link entre a aplicação e as camadas inferiores, fazendo a **transmissão dos pacotes**.

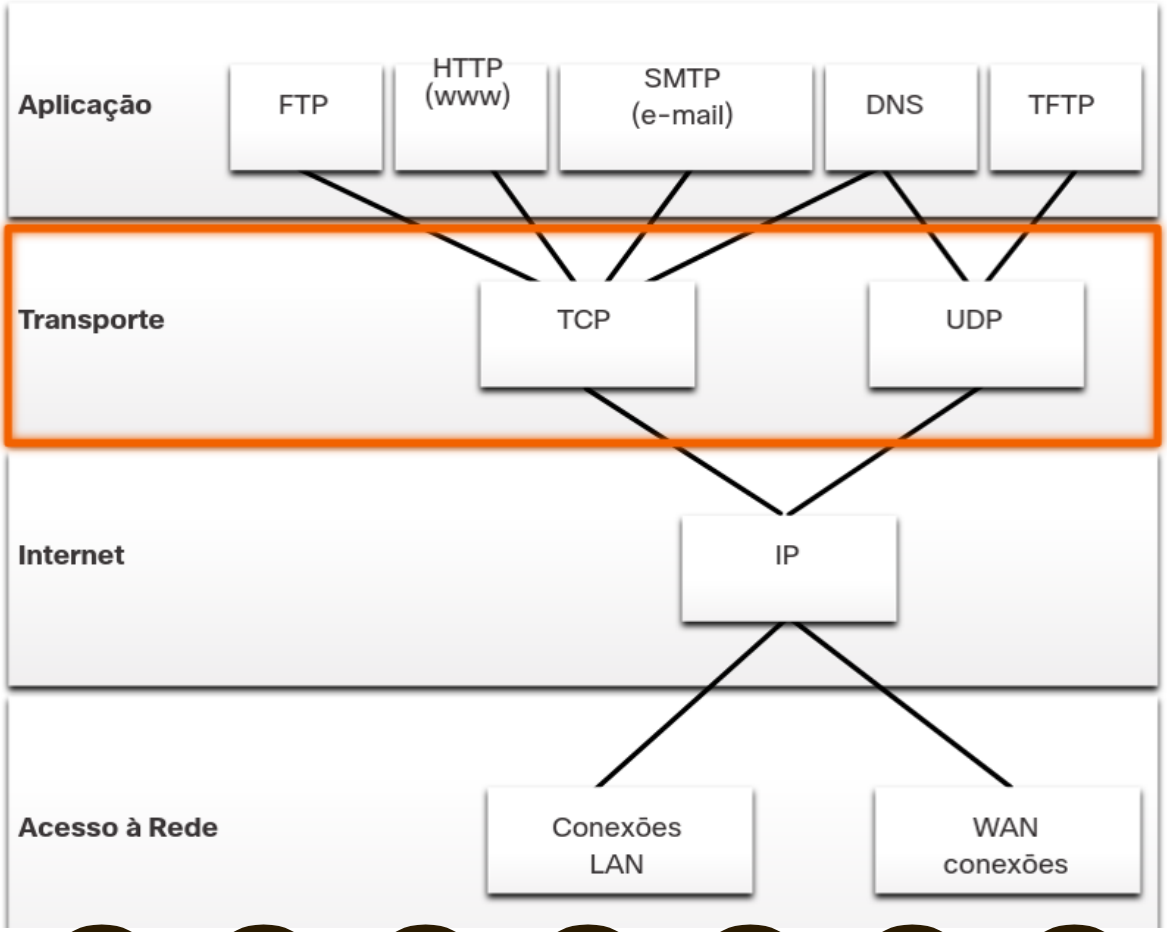
Não tem conhecimento sobre o tipo de mídia, congestionamento do link, tamanho da rede, caminho dos pacotes ou tipo de host de destino.

Ela recebe a carga, divide ou não em tamanhos menores para facilitar o transporte/gerenciamento, identifica o aplicativo e adiciona as informações de cabeçalho.

PROTOCOLOS DE TRANSPORTE

Os protocolos da camada de transporte especificam **como transferir mensagens** entre hosts e são responsáveis por gerenciar os requisitos de confiabilidade de uma conversa.

Diferentes aplicações têm diferentes requisitos de confiabilidade de transporte. Portanto, o TCP/IP fornece dois protocolos da camada de transporte, conforme mostrado na figura.

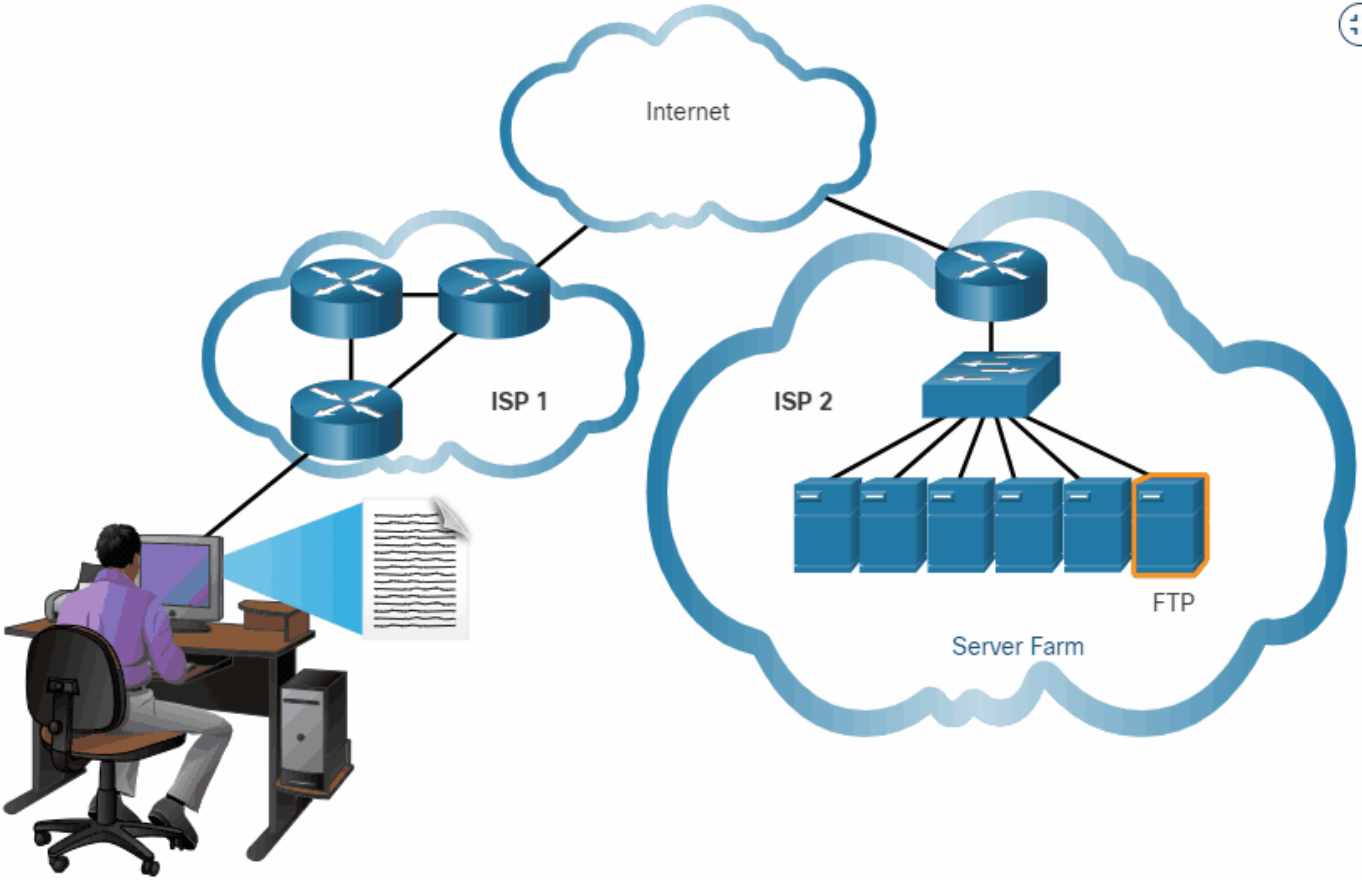

Aplicação
FTP
HTTP (www)
SMTP (e-mail)
DNS
TFTP
Transporte
TCP
UDP
Internet
IP
Acesso à Rede
Conexões LAN
WAN conexões

PROTOCOLO TCP

Definido na RFC 793, o TCP é considerado um **protocolo confiável**, que **garante a entrega** do pacote ou a chegada de todos os dados ao destino, incluindo campos no cabeçalho para isso. É como se enviássemos algo pelo correio com a garantia ou notificação de entrega.

- o protocolo TCP **rastreia** os dados enviados.
- **confirma** os dados recebidos.
- **retransmite** todos os dados não confirmados
- envia dados na sequência e escolhe uma taxa aceitável.

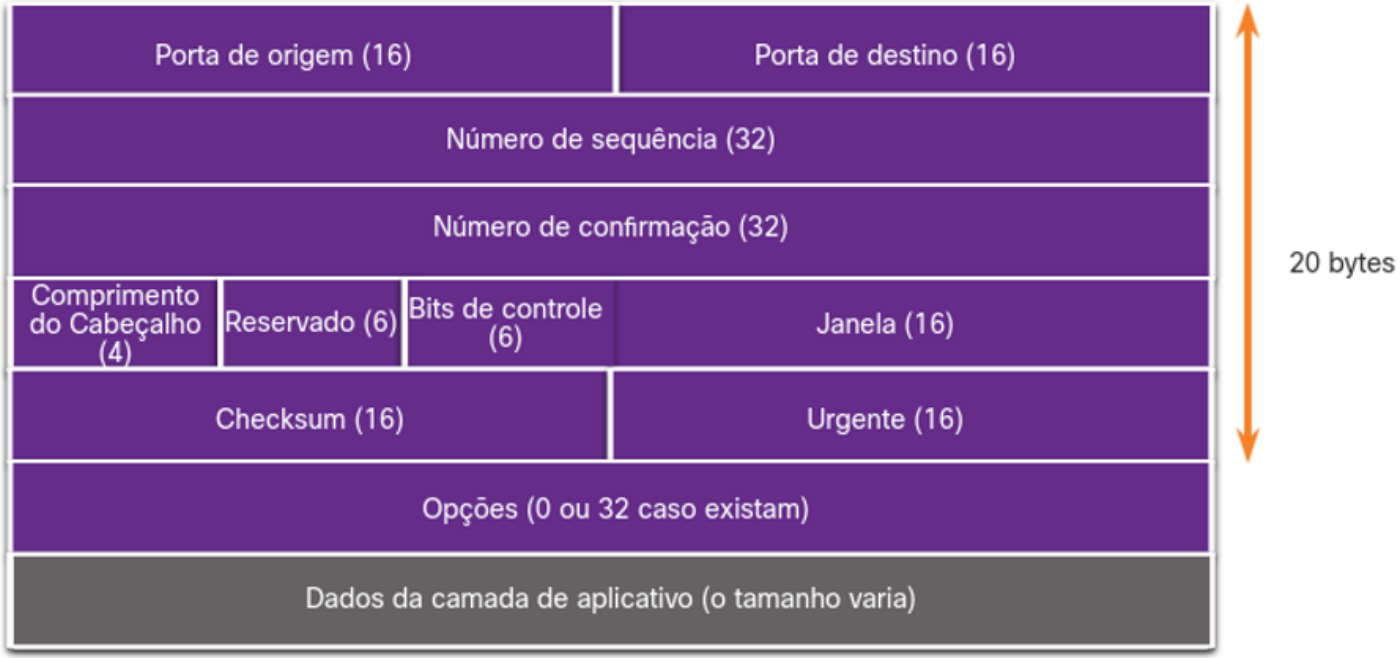
Para o trabalho, é necessário estabelecer uma conexão prévia, por isso dizemos que é um protocolo **orientado a conexão**.


Internet
ISP 1
ISP 2
FTP
Server Farm

CABEÇALHO TCP

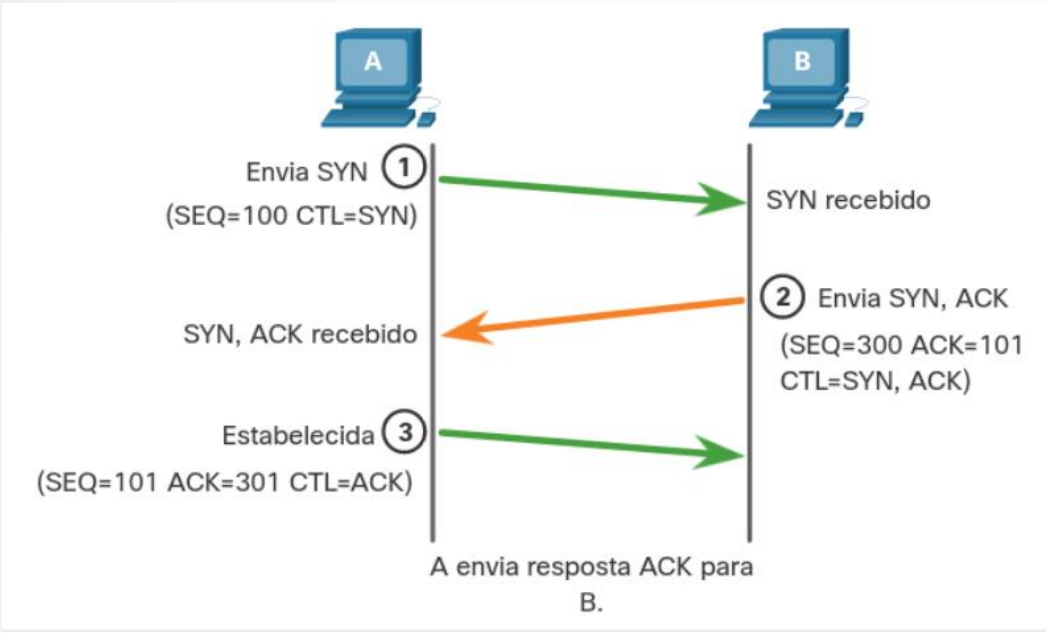
O TCP é um protocolo **stateful**, o que significa que controla o estado da sessão de comunicação, utilizando campos de controle. Tem um tamanho de 20 bytes.

- **Porta de origem e destino**: campo de 16 bits cada para identificar o aplicativo de origem e destino.
- **Nº sequencial**: campo de 32 bits para remontagem de dados.
- **Nº de confirmação**: 32 bits para indicar que os dados foram recebidos.
- **Comprimento**: 4 bits que indicam o comprimento do cabeçalho.
- **Reservado**: 6 bits, campo ainda sem uso, reservado para o futuro.
- **Bits de Controle**: 6 bits que indicam a finalidade/função do pacote.
- **Tamanho da janela**: 16 bits para indicar quantos bytes podem ser aceitos de uma só vez.
- **Checksum**: 16 bits para verificação de erros do cabeçalho e dados.
- **Urgente**: 16 bits para indicar se os dados contidos são urgentes.


Porta de origem (16)
Porta de destino (16)
Número de sequência (32)
Número de confirmação (32)
Comprimento do Cabeçalho (4)
Reservado (6)
Bits de controle (6)
Janela (16)
Checksum (16)
Urgente (16)
Opções (0 ou 32 caso existam)
Dados da camada de aplicativo (o tamanho varia)
20 bytes

A CONEXÃO TCP

O protocolo TCP tem um processo de conexão chamado **Three-Way Handshake**, onde o dispositivo de origem sinaliza o desejo de conexão (**SYN**), o destino sinaliza o aceite (**SYN/ACK**) e a origem faz o aceite final (**ACK**). Os bits de controle do cabeçalho também indicam o progresso e o status da conexão.



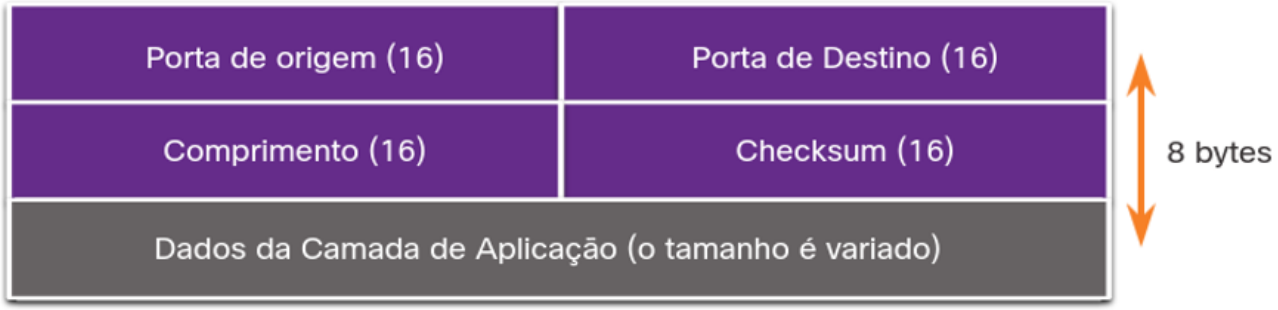
PROTOCOLO UDP

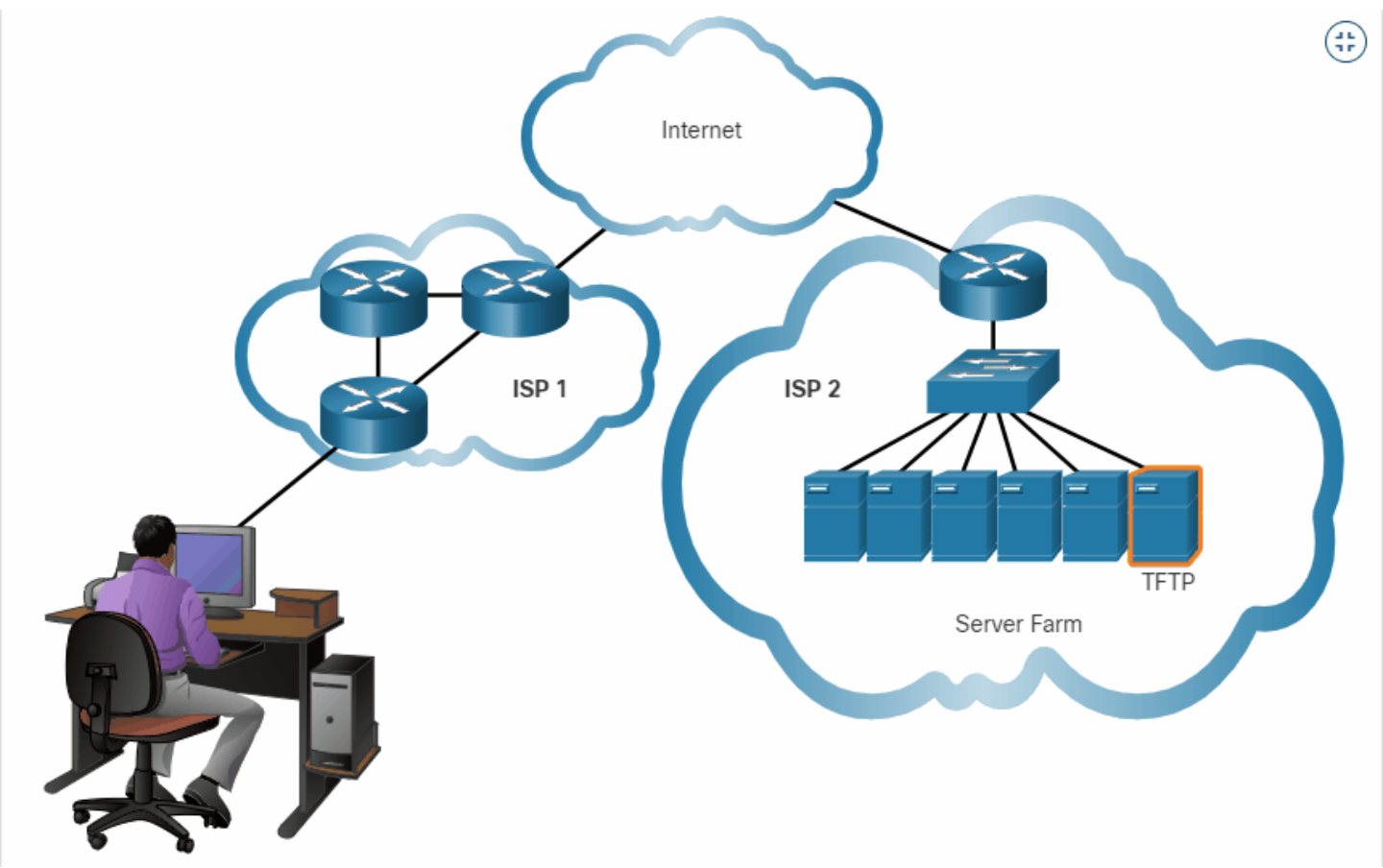
O UDP é considerado mais simples, pois **não faz controle de fluxo** e **não tem confiabilidade**, o que gera menos campos no cabeçalho e mais velocidade. Por isso dizemos que é uma protocolo **sem estado ou entrega de melhor esforço**. É como enviar uma carta não registrada, sem avisar ao remetente e sem rastreamento.

CABEÇALHO UDP

Como o protocolo UDP não fornece confiabilidade, não necessita de campos de controle, o que torna o cabeçalho apenas com 4 campos e tamanho de 8 bytes.

- **Porta de origem e destino**: campo de 16 bits cada para identificar o aplicativo de origem e destino.
- **Comprimento**: 4 bits que indicam o comprimento do cabeçalho.
- **Checksum**: 16 bits para verificação de erros geral.




Internet
ISP 1
ISP 2
TFTP
Server Farm

USAR TCP OU UDP?

Algumas aplicações suportam perda de dados, mas **não suportam atrasos** na transmissão. Para esses casos, o **UDP** é a melhor escolha. Pode ser usado também em mensagens de dados mínimos, onde a retransmissão pode ser feita de modo rápido.

Para outras aplicações, é importante o **controle dos dados**, onde **perdas são inaceitáveis**, e a chegada e sequenciamento precisam ser acompanhadas e rastreadas. Nestes casos, o **TCP** é o mais adequado.

Os desenvolvedores escolhem o protocolo de transporte com base nas necessidades da aplicação. Geralmente **streaming utilizam UDP**, enquanto aplicações tradicionais e **conteúdo sob demanda pode utilizar TCP**. Algumas aplicações também podem usar ambos protocolos, para driblar bloqueios de firewall por exemplo.

UDP

VoIP
(telefonia IP)

DNS
(resolução de nomes de domínio)

Propriedades necessárias para escolha do protocolo:

- Rápido
- Baixa sobrecarga
- Não exige confirmações
- Não reenvia dados perdidos
- Entrega os dados assim que chegam

TCP

SMTP/IMAP
(E-mail)

HTTP/HTTPS
(World Wide Web

Propriedades necessárias para escolha do protocolo:

- Confiável
- Confirma a chegada dos dados
- Reenvia dados perdidos
- Entrega os dados em sequência

NÚMEROS DE PORTAS

A camada de transporte utiliza números de porta para identificar o aplicativo de origem e destino da transmissão, sendo ao todo **65536** portas (0 - 65535). A IANA separou em 3 grupos.

- **Portas Bem Conhecidas**: de 0 a 1023, são **portas reservadas** para serviços comuns ou populares, permitindo identificar rapidamente o aplicativo associado. São geralmente **bloqueadas** por diversos motivos e também por segurança.
- **Portas Registradas**: de 1024 a 49.151, são atribuídas a entidades para processos ou aplicativos específicos. Por exemplo a porta 1863 era a porta do antigo MSN Messenger e a porta 3306 é a porta do banco de dados MySQL.
- **Portas Particulares/Dinâmicas**: atribuída dinamicamente pelo sistemas operacional, quando determinando serviço ou aplicativo é iniciado.

PORTAS BEM CONHECIDAS

Número da Porta	Protocolo	Aplicação
20	TCP	Protocolo de transferência de arquivos (FTP) - Dados
21	TCP	Protocolo de transferência de arquivos (FTP) - Controle
22	TCP	Secure Shell (SSH)
23	TCP	Telnet
25	TCP	Protocolo SMTP
53	UDP, TCP	Protocolo DNS
67	UDP	Protocolo de Configuração Dinâmica de Host (DHCP) - Servidor
68	UDP	Protocolo de configuração dinâmica de host - cliente
69	UDP	Protocolo de Transferência Trivial de Arquivo (TFTP)
80	TCP	Protocolo HTTP
110	TCP	Protocolo POP3 (Post Office Protocol - Protocolo dos Correios)
143	TCP	Protocolo IMAP
161	UDP	Protocolo de Gerenciamento Simples de Rede (SNMP)
443	TCP	HTTPS (Secure Hypertext Transfer Protocol - Protocolo de Transferência de Hipertexto Seguro)

COMANDO NETSTAT

O comando **netstat** simples exibe as conexões de portas estabelecidas e pode ser útil para diagnóstico de rede. É o mesmo comando para sistemas Windows e Linux, e pode adicionar alguns parâmetros, inclusive combinados.

- **r**: exibe a tabela de roteamento.
- **p**: exibe conexões por algum protocolo especificado, por exemplo **–p IP**.
- **s**: estatísticas sobre as conexões TCP/UDP.
- **n**: exibição numérica de endereços e portas.
- **q**: exibição geral das portas TCP e seus status.
- **a**: exibe todas as portas ativas.
- **v**: exibe a versão do comando netsat instalado no momento.
- **t**: exibe todas as conexões TCP.
- **u**: exibe todas as conexões UDP.

```
aqsa@aqsa-VirtualBox:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:mysql         0.0.0.0:*               LISTEN
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:db-lsp          0.0.0.0:*               LISTEN
tcp       54      0 aqsa-VirtualBox:50536   guestportal.hec.go:8443 CLOSE_WAIT
tcp       54      0 aqsa-VirtualBox:50550   guestportal.hec.go:8443 CLOSE_WAIT
tcp        0      0 aqsa-VirtualBox:34674   162.125.35.134:https    ESTABLISHED
tcp        0      0 aqsa-VirtualBox:54964   162.125.19.130:https    ESTABLISHED
tcp       54      0 aqsa-VirtualBox:50546   guestportal.hec.go:8443 CLOSE_WAIT
tcp6       0      0 [::]:http               [::]:*                  LISTEN
tcp6       0      0 [::]:ftp                [::]:*                  LISTEN
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
tcp6       0      0 [::]:db-lsp             [::]:*                  LISTEN
```

```
aqsa@aqsa-VirtualBox:~$ netstat -au
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp        0      0 0.0.0.0:17500           0.0.0.0:*
udp        0      0 0.0.0.0:42123           0.0.0.0:*
udp        0      0 0.0.0.0:mdns            0.0.0.0:*
udp        0      0 localhost:domain        0.0.0.0:*
udp        0      0 aqsa-VirtualBox:bootpc  _gateway:bootps         ESTABLISHED
udp6       0      0 [::]:41827              [::]:*
udp6       0      0 [::]:mdns               [::]:*
aqsa@aqsa-VirtualBox:~$
```

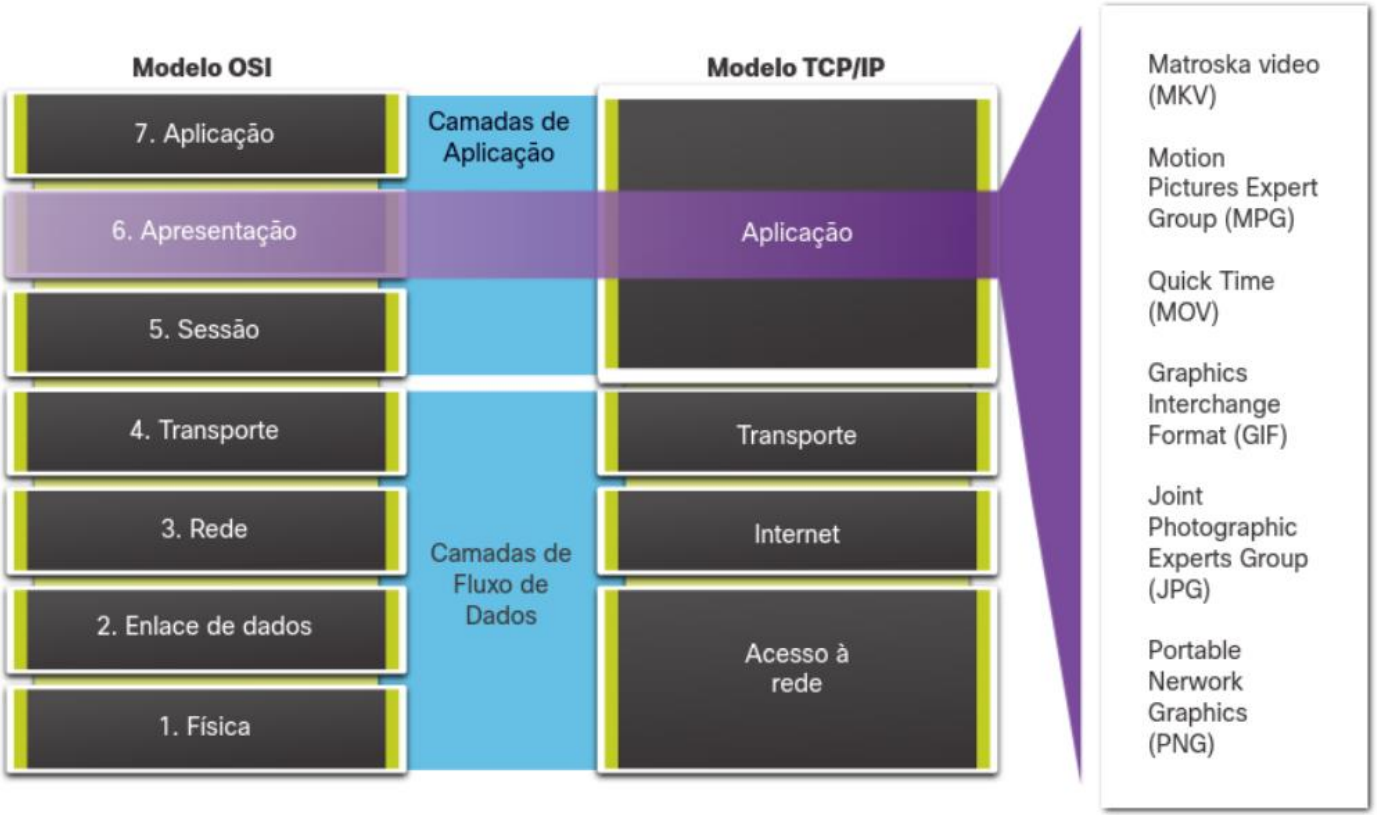
CAMADA DE SESSÃO, APRESENTAÇÃO E APLICAÇÃO

SESSÃO E APRESENTAÇÃO

A camada de sessão tem a função de **criar e gerenciar as sessões** e diálogos entre aplicações de origem e destino, mantendo sessões ativas ou reiniciando as interrompidas ou ociosas.

Já a camada de apresentação tem as funções de:

- **Formatar** e apresentar os dados para o destino de maneira compatível.
- **Comprimir** dados se necessário, para ser descomprimido pela próxima camada.
- **Criptografar** dados para transmissão e descriptografar após o recebimento.



FORMATOS PADRÃO DE ARQUIVOS

PROPÓSITOS DA CAMADA DE APLICAÇÃO

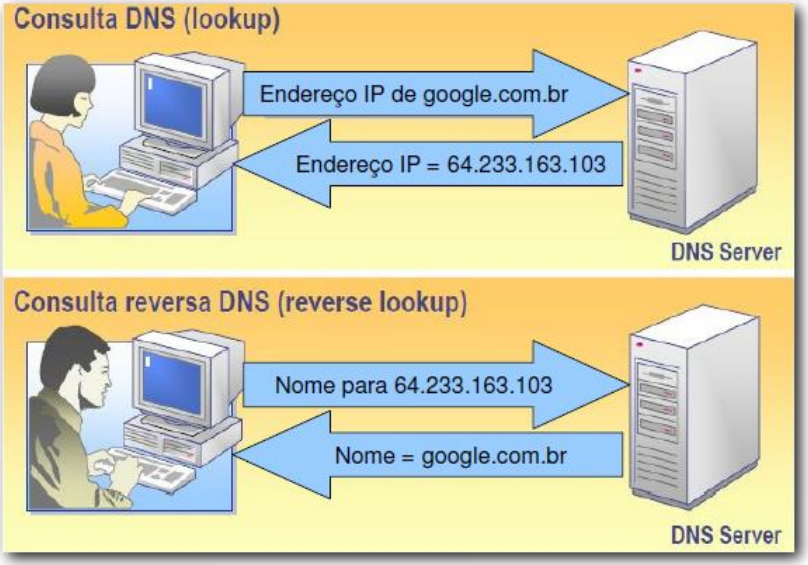
É a camada mais próxima do usuário, que fornece a interface entre os aplicativos usados para se comunicar. Há muitos protocolos ali e outros novos sempre estão em desenvolvimento. Alguns deles são:

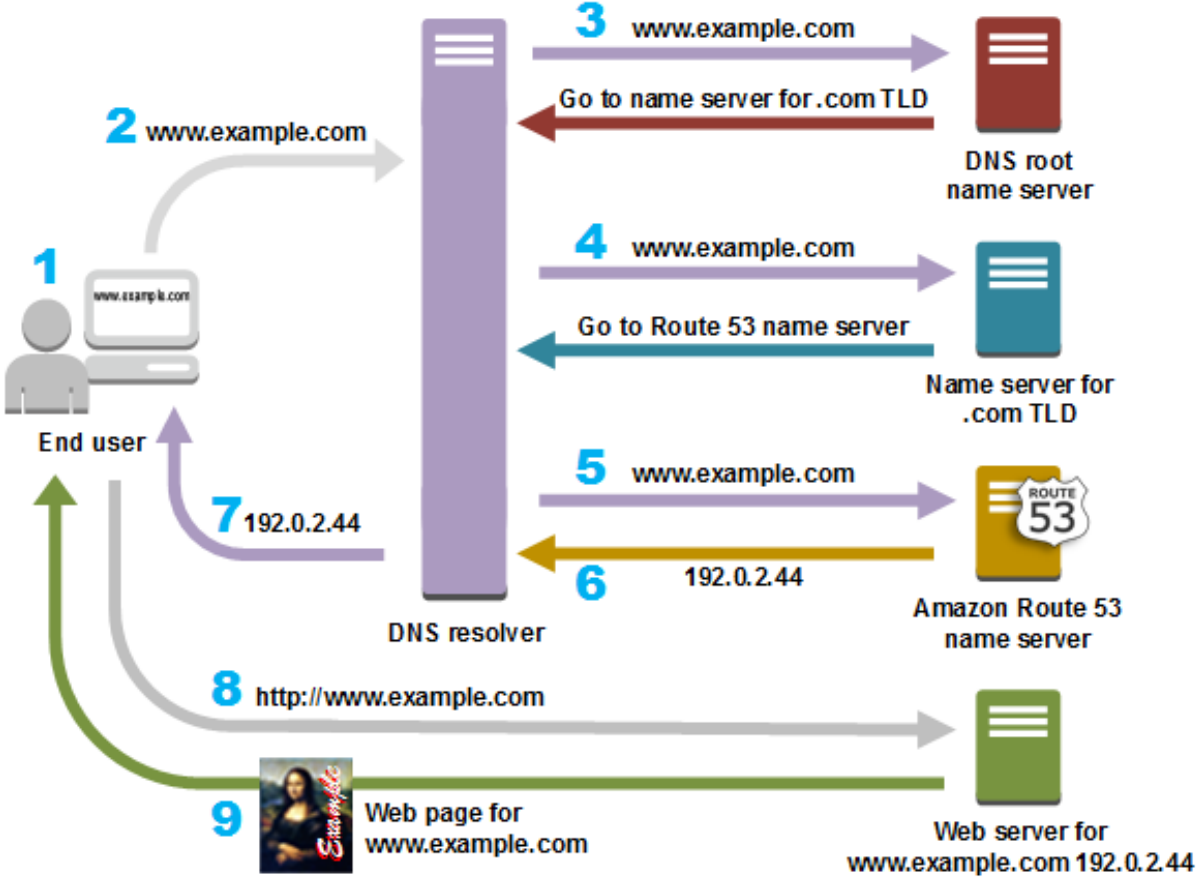
- DNS
- DHCP
- POP/IMAP/SMTP
- FTP
- HTTP/HTTPS

PROTOCOLO DNS

É um protocolo de resolução de endereços, baseado em um nome de domínio. Faz a importante tarefa de **associar nomes a IP**. Quando digitamos www.sorjonas.com.br na Internet, na verdade estamos procurando um servidor com um IP que hospeda este site.

Para não precisarmos decorar este IP, digitamos apenas o nome do site (no caso, sorjonas.com.br) e o DNS "procura" o IP correspondente para nós. O DNS utiliza protocolo **UDP** e opera na **porta 53**.




1
End user
2 www.example.com
DNS resolver
3 www.example.com
Go to name server for .com TLD
DNS root name server
4 www.example.com
Go to Route 53 name server
Name server for .com TLD
5 www.example.com
6 192.0.2.44
ROUTE 53
Amazon Route 53 name server
7 192.0.2.44
8 http://www.example.com
9 Web page for www.example.com
Web server for www.example.com 192.0.2.44

ESQUEMA DNS

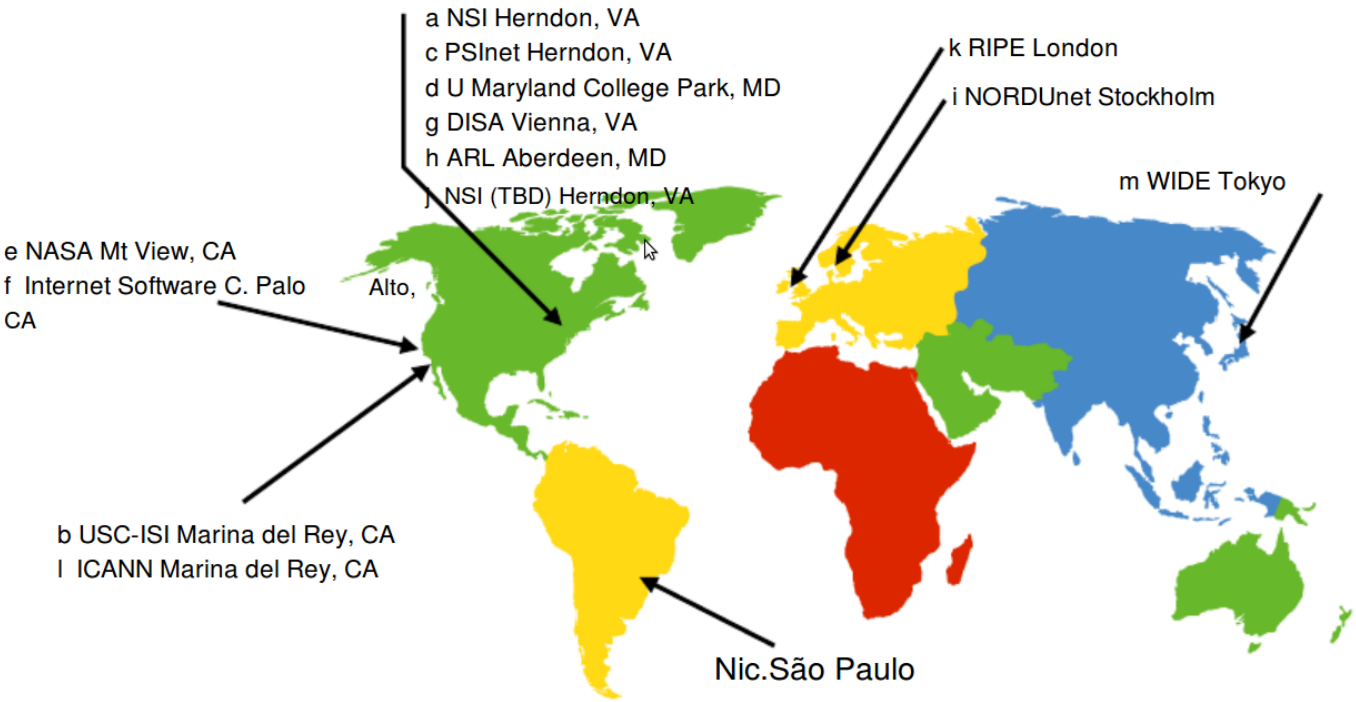
REGISTROS DNS

O DNS faz uso de diferentes tipos de registros/entradas para resolver nomes. Alguns tipos de registros são:

- **A**: endereço IPv4 do dispositivo final.
- **NS**: servidor de nomes com autoridade
- **AAAA**: endereço IPv6 do dispositivo final.
- **MX**: registro de endereço de correio eletrônico.

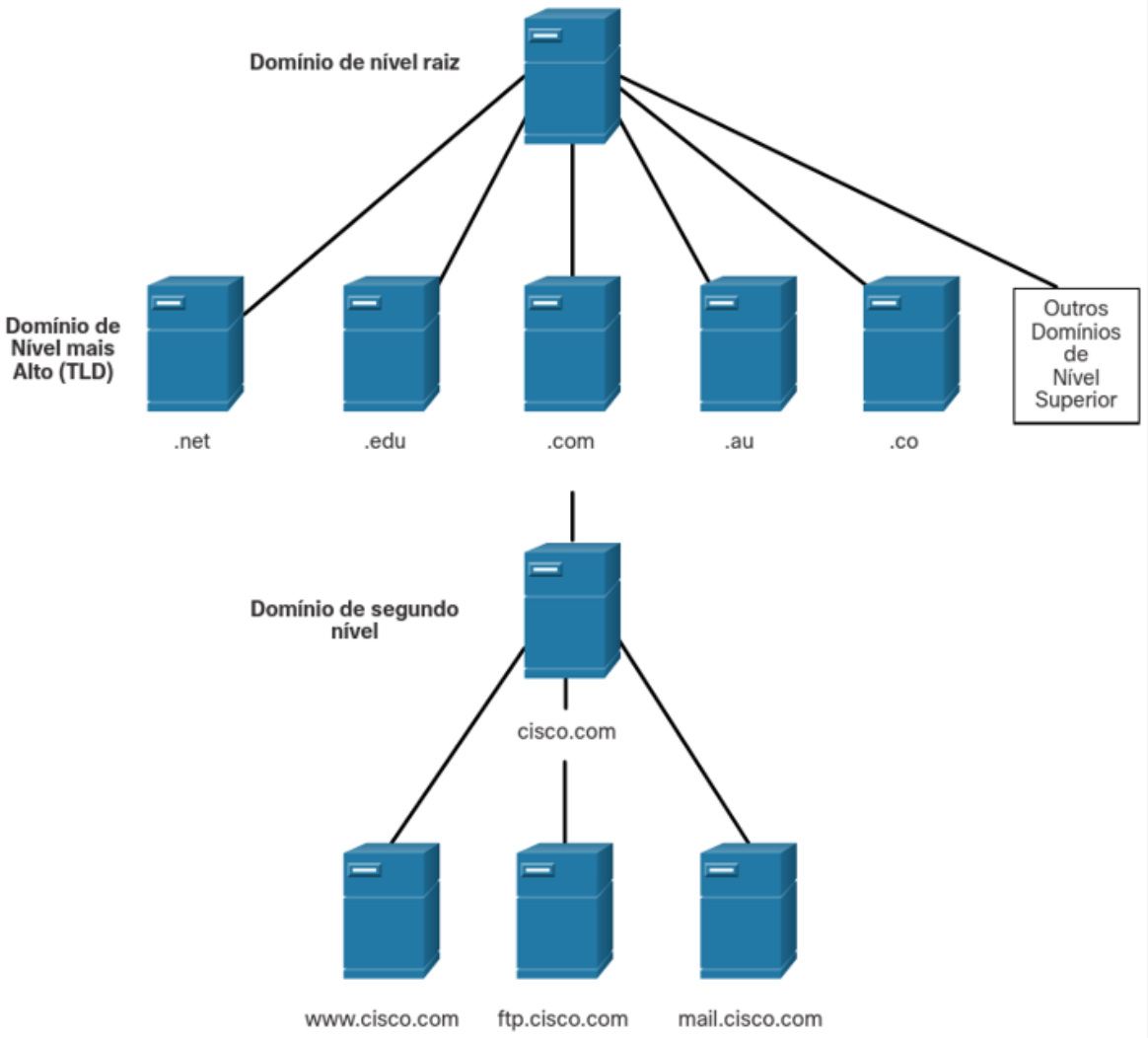
O serviço DNS é **hierárquico**. Quando um dispositivo faz uma consulta DNS, o servidor consulta seus próprios registros para resolver o nome. Caso não consiga, ele entra em contato, com outros servidores para resolver, escalando para servidores maiores conforme a estrutura do endereço até conseguir a resolução.

No topo da estrutura estão os **servidores raiz**, são 14 deles espalhados pelo mundo.



São **10 nos EUA, 1 na Ásia, 1 na Europa** e recentemente foi ativado um servidor raiz em **São Paulo**, servindo toda a América Latina, melhorando a latência de 160ms para cerca de 20ms.

DNS ROOT SERVERS NO MUNDO


Domínio de nível raiz
Domínio de Nível mais Alto (TLD)
.net
.edu
.com
.au
.co
Outros Domínios de Nível Superior
Domínio de segundo nível
cisco.com
www.cisco.com
ftp.cisco.com
mail.cisco.com

COMANDOS DNS

Em dispositivos Windows, o comando **ipconfig /displaydns** exibe o cache de resoluções DNS feitas até o momento. O sistema Linux não guarda cache DNS por padrão, mas podemos visualizar o servidor configurado com o comando **cat /etc/resolv.conf** ou com o comando **service nscd status**.

A consulta DNS é automática pelo servidor, porém o usuário final também pode consultar manualmente uma resolução de nomes através do comando **nslookup**, disponível em Windows ou Linux. Ele traz qual é o servidor padrão do dispositivo (o servidor que respondeu a consulta), qual a porta de comunicação e as informações da consulta. É possível também utilizar a **consulta reserva**, isto é, pesquisar pelo IP para obter o nome.

```
C:\Users> nslookup
Default Server:  dns-sj.cisco.com
Address:  171.70.168.183
> www.cisco.com
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:    origin-www.cisco.com
Addresses:  2001:420:1101:1::a
          173.37.145.84
Aliases:  www.cisco.com
> cisco.netacad.net
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:    cisco.netacad.net
Address:  72.163.6.223
>
```

```
nslookup microsoft.com
```

```
Servidor: 8.8.8.8
Endereço: 8.8.8.8 # 53
Resposta não autorizada:
Nome: microsoft.com
Endereço: 134.170.185.46
Nome: microsoft.com
Endereço: 134.170.188.221
```

```
nslookup 134.170.185.46
```

```
Servidor: 8.8.8.8
Endereço: 8.8.8.8 # 53
Resposta não autorizada:
46.185.170.134.in-addr.arpa name = grv.microsoft.com.
Respostas autorizadas podem ser encontradas em:
```

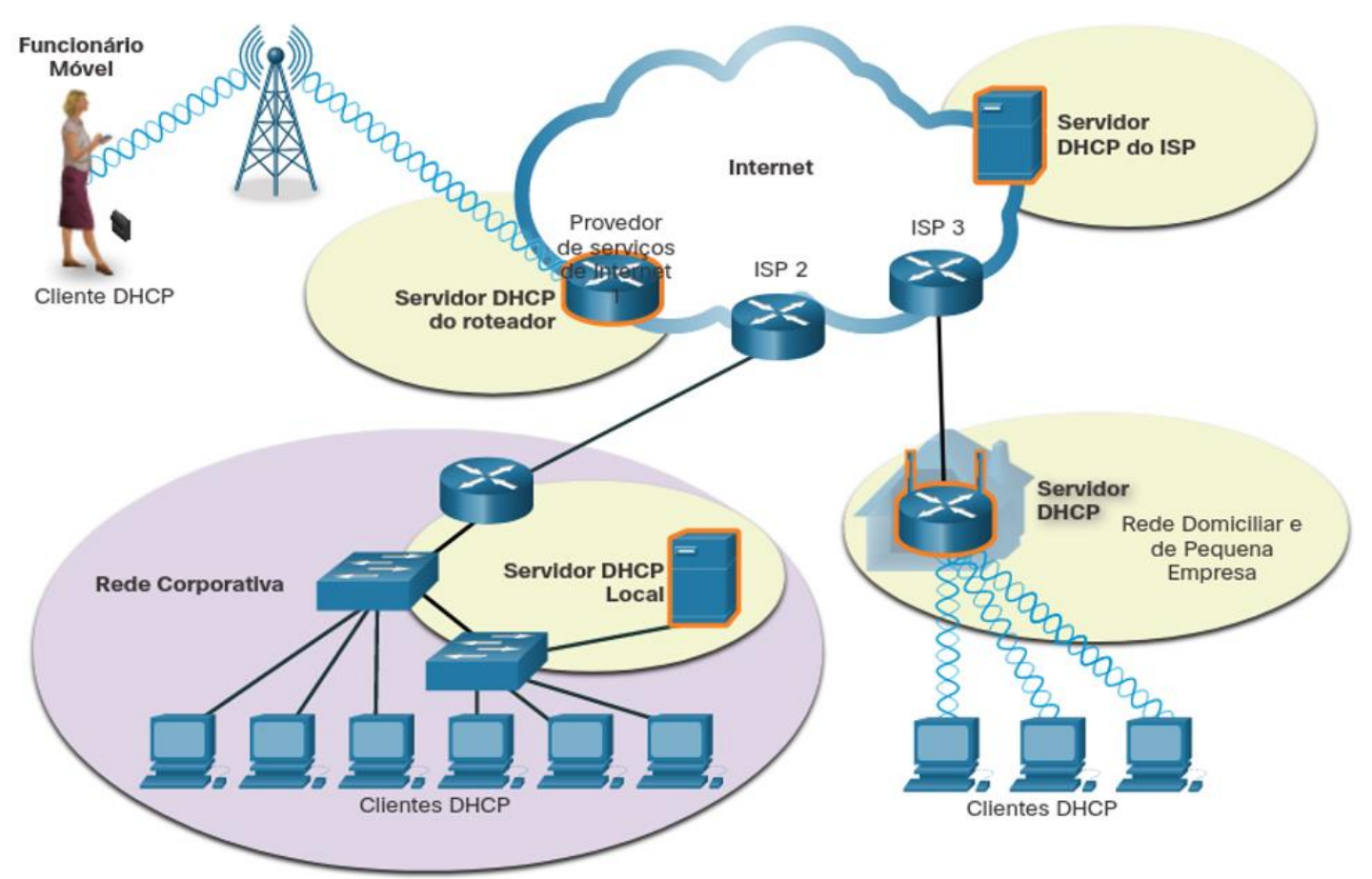
TIPOS DE CONSULTA NSLOOKUP

PROTOCOLO DHCP

O protocolo DHCP carrega informações de conectividade do servidor para o cliente, isto é, o **servidor envia parâmetros de rede** (endereço IP, gateway, máscara, etc) automaticamente para o cliente, de modo que este possa se conectar, sem nenhuma configuração manual.

Muito utilizado nas redes atuais, oferece comodidade (principalmente em redes WLAN) quando há um ambiente com rotatividade de conexão (usuários/dispositivos entrando e saindo), mas pode ser visto como uma **brecha de segurança**, dependendo do nível adotado na organização.

Em redes médias, o servidor DHCP pode ser um PC com uma aplicação exclusiva para tal. Já em redes domésticas, o servidor DHCP normalmente está localizado no roteador doméstico.



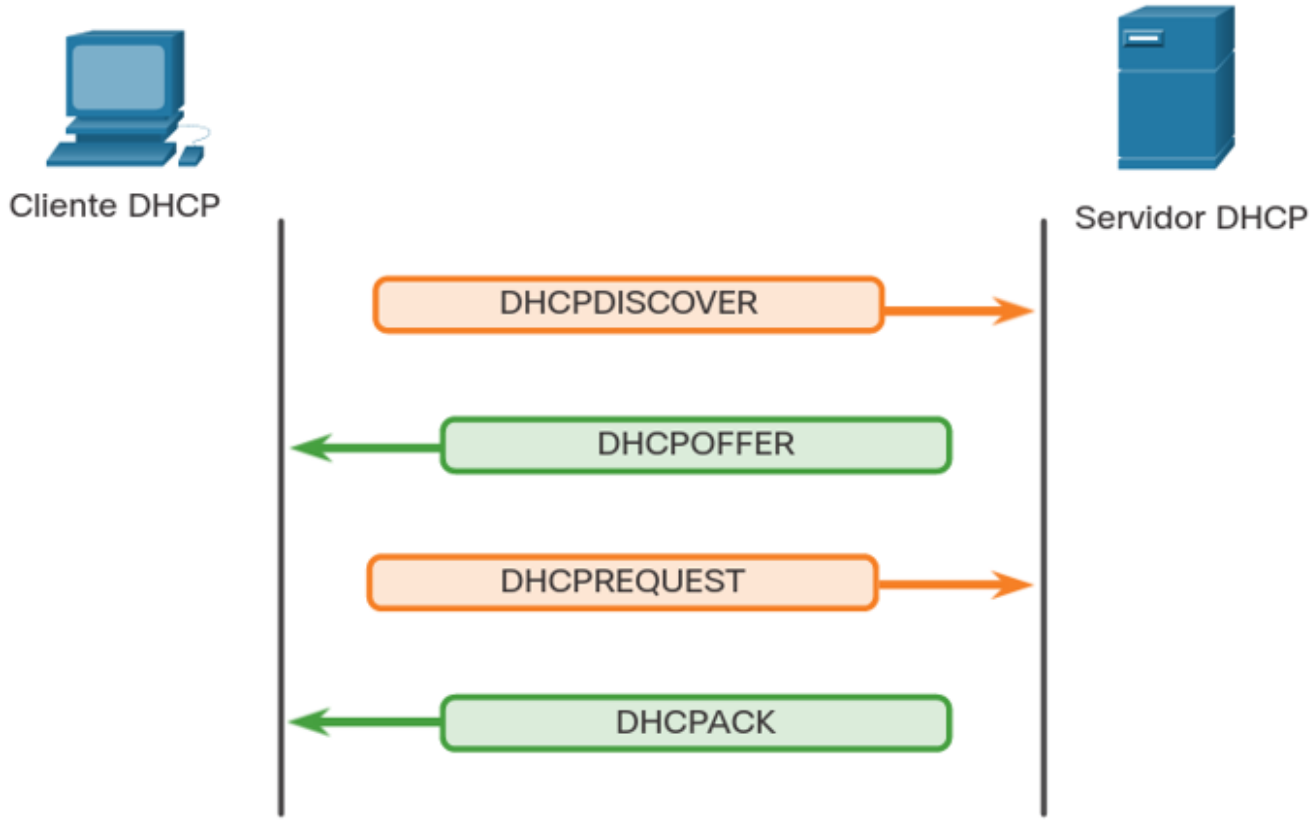
SERVIÇO DHCP EM VÁRIOS AMBIENTES

MENSAGENS DHCP

Quando um dispositivo configurado para receber conectividade dinâmica se conecta à rede, ele envia uma mensagem de descoberta para encontrar algum servidor DHCP disponível (**DHCPDISCOVER**). Um ou mais servidores pode responder a mensagem, oferecendo alocação de conexão e enviando os parâmetros de rede (**DHCPOFFER**).

O dispositivo então escolhe qual oferta aceitar e enviar uma mensagem de requisição ao servidor (**DHCPREQUEST**). O servidor então envia a mensagem que a alocação está completa e finalizada (**DHCPACK**). Ou pode negar, caso haja alguma falha no processo (**DHCPNAK**), sendo necessário reiniciá-lo.

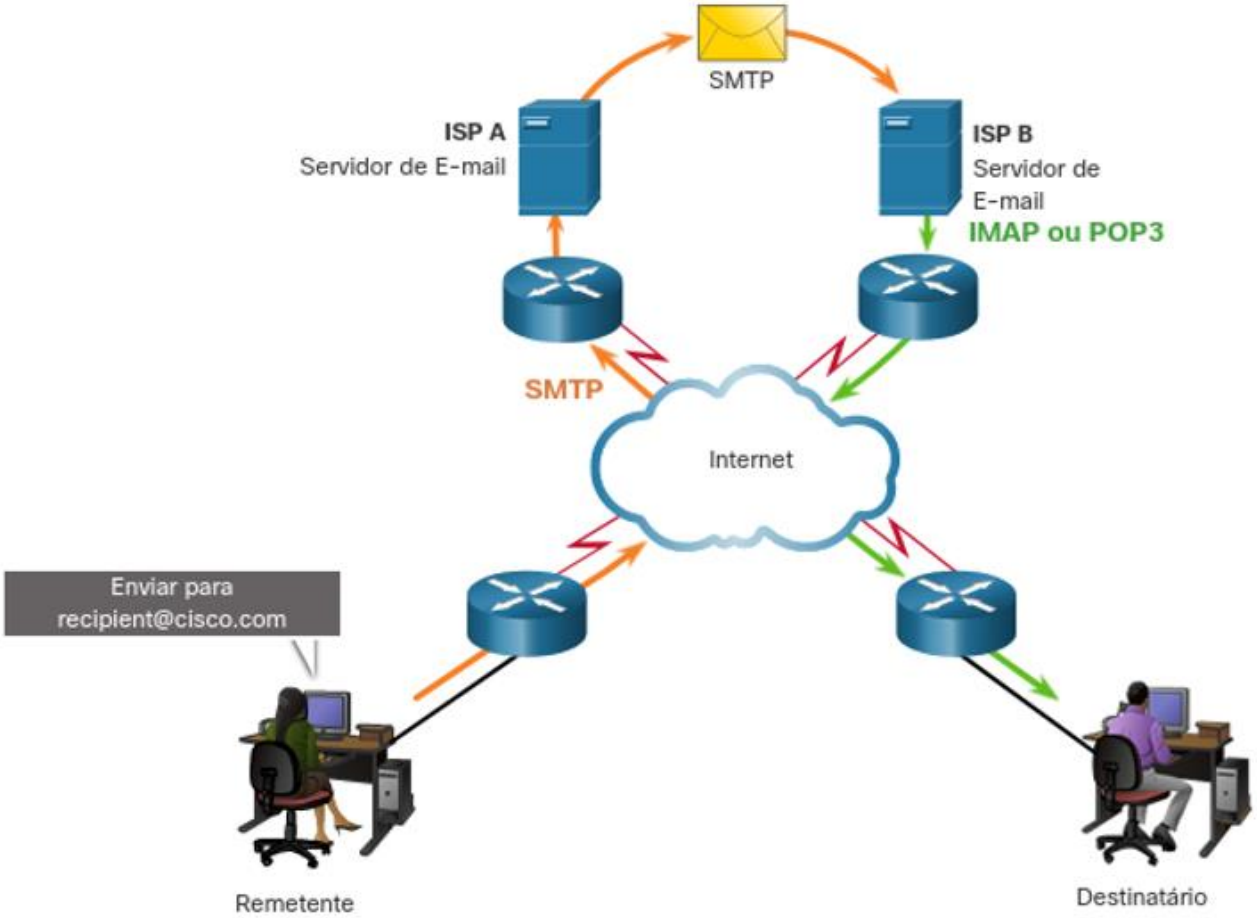
Quanto ao IPv6, o serviço e parecido, exceto pelo servidor não enviar a configuração de gateway, sendo esta obtida através de mensagem RA. As mensagens **DHCPv6** são **SOLICIT, ADVERTISE, INFORMATION REQUEST e REPLY**.


Cliente DHCP
Servidor DHCP
DHCPDISCOVER
DHCPOFFER
DHCPREQUEST
DHCPACK

SERVIÇO DE E-MAIL

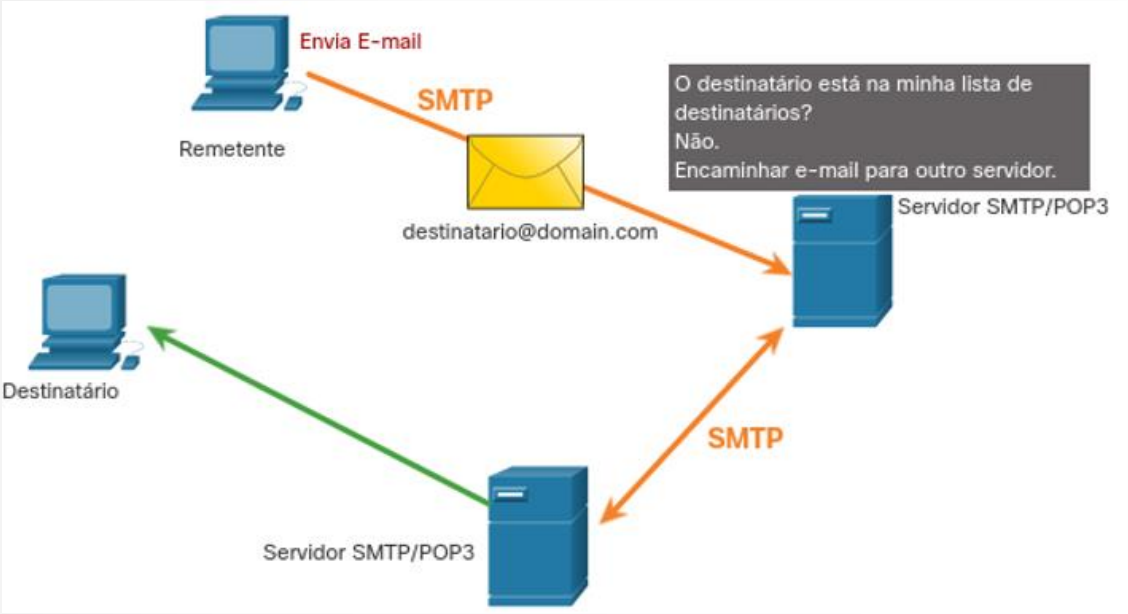
Um dos serviços mais básicos de uma rede é a troca de e-mail através de armazenamento, encaminhamento, envio e recuperação de mensagens eletrônicas.

Os clientes de e-mail se conectam com os servidores, que por sua vez se comunicam com outros servidores para envios e recepção, utilizados **MTA** (Mail Transfer Agent). Para a transmissão, utilizam o protocolo SMTP, para recuperação utilizam POP ou IMAP


SMTP
ISP A
Servidor de E-mail
ISP B
Servidor de
E-mail
IMAP ou POP3
SMTP
Internet
Enviar para
recipient@cisco.com
Remetente
Destinatário

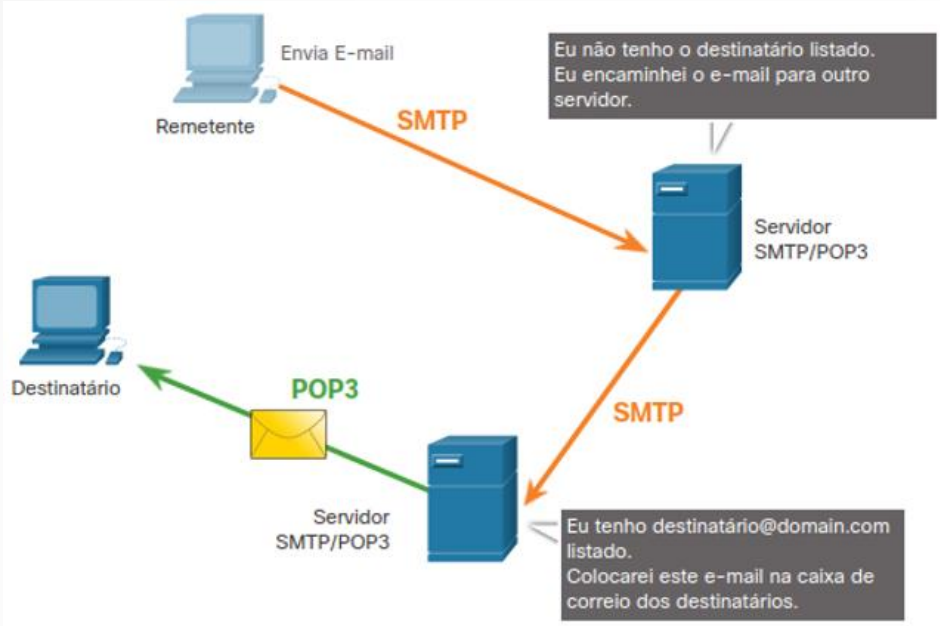
PROTOCOLO SMTP

O protocolo SMTP é utilizado para envio de e-mail. Quando um dispositivo envia um e-mail, ele encaminha uma mensagem SMTP para o servidor, que por sua vez, encaminha ao servidor de destino, através de outro processo SMTP. O protocolo utiliza **TCP** e opera na **porta 25**.



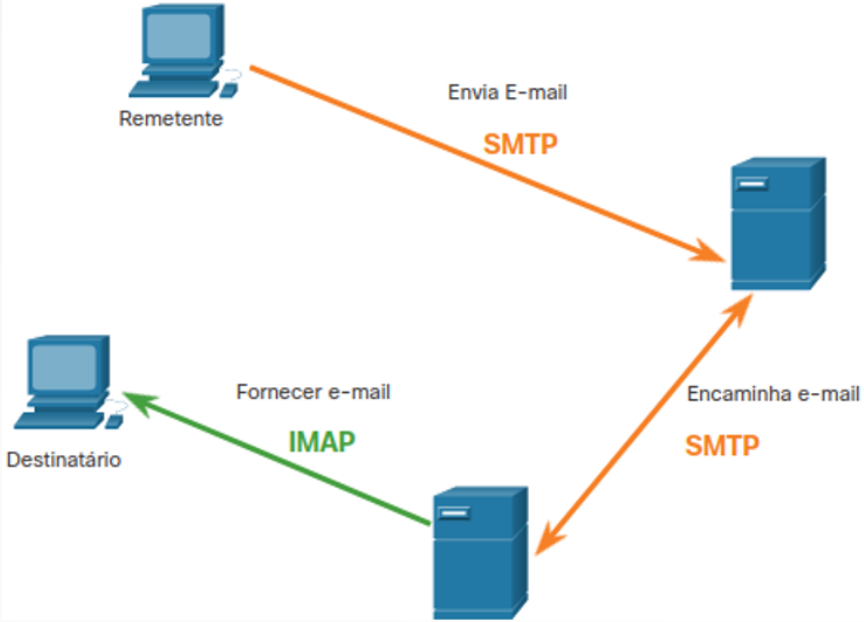
PROTOCOLO POP

O protocolo POP é utilizado pelo cliente para recepção/recuperação de um e-mail recebido pelo servidor. Quando um dispositivo solicita conexão POP, o e-mail é transferido para o cliente e **excluído do servidor**, por isso não é de uso recomendado para pequenas empresas. Opera com **TCP** na **porta 110**.



PROTOCOLO IMAP

O protocolo IMAP também é utilizado pelo cliente para recepção/recuperação de um e-mail recebido pelo servidor. Mas diferentemente do protocolo POP, apenas uma **cópia do e-mail** é transferida para o cliente, permanecendo a mensagem original no servidor. Opera com **TCP** na **porta 143**.



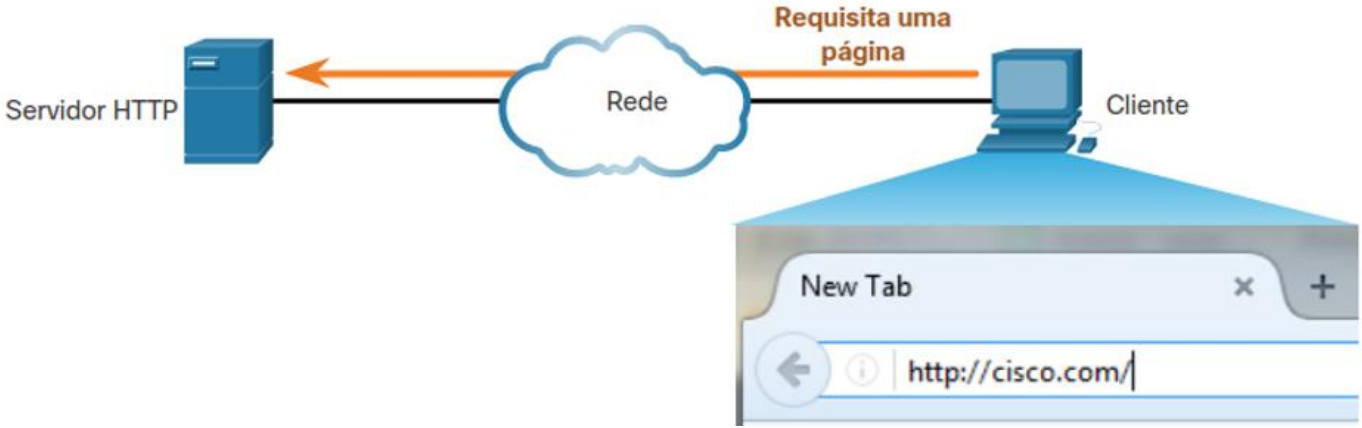
PROTOCOLO HTTP

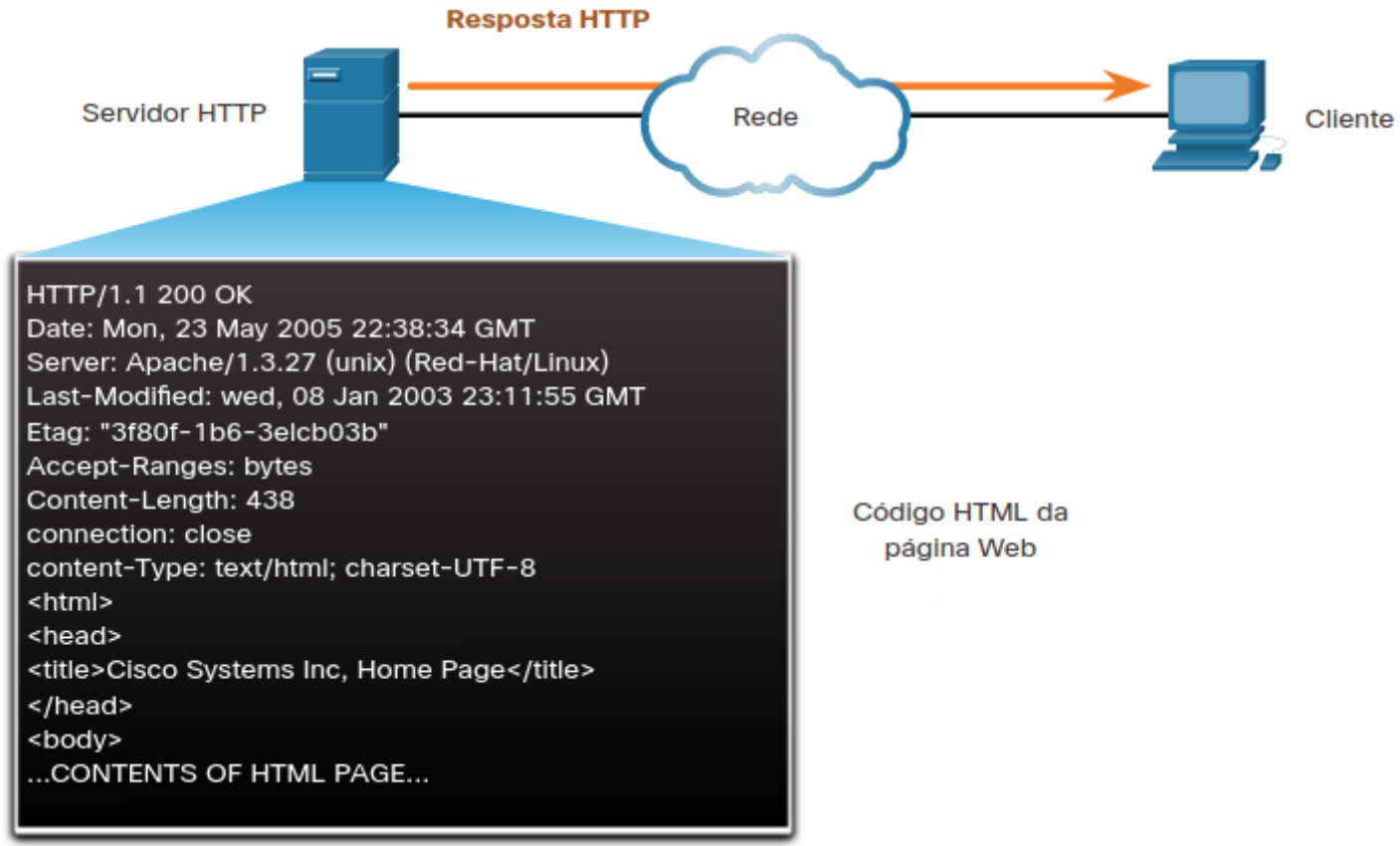
O protocolo HTTP é utilizado para **navegação Web**, utilizando **TCP** e operando na **porta 80**. Ele é operado por um servidor Web para processar uma requisição de um cliente tentando acessar um endereço Web (URL/URI) utilizado pelo cliente, que também está utilizando o protocolo. Por exemplo, considerando como URL o endereço abaixo: http://www.cisco.com/index.html

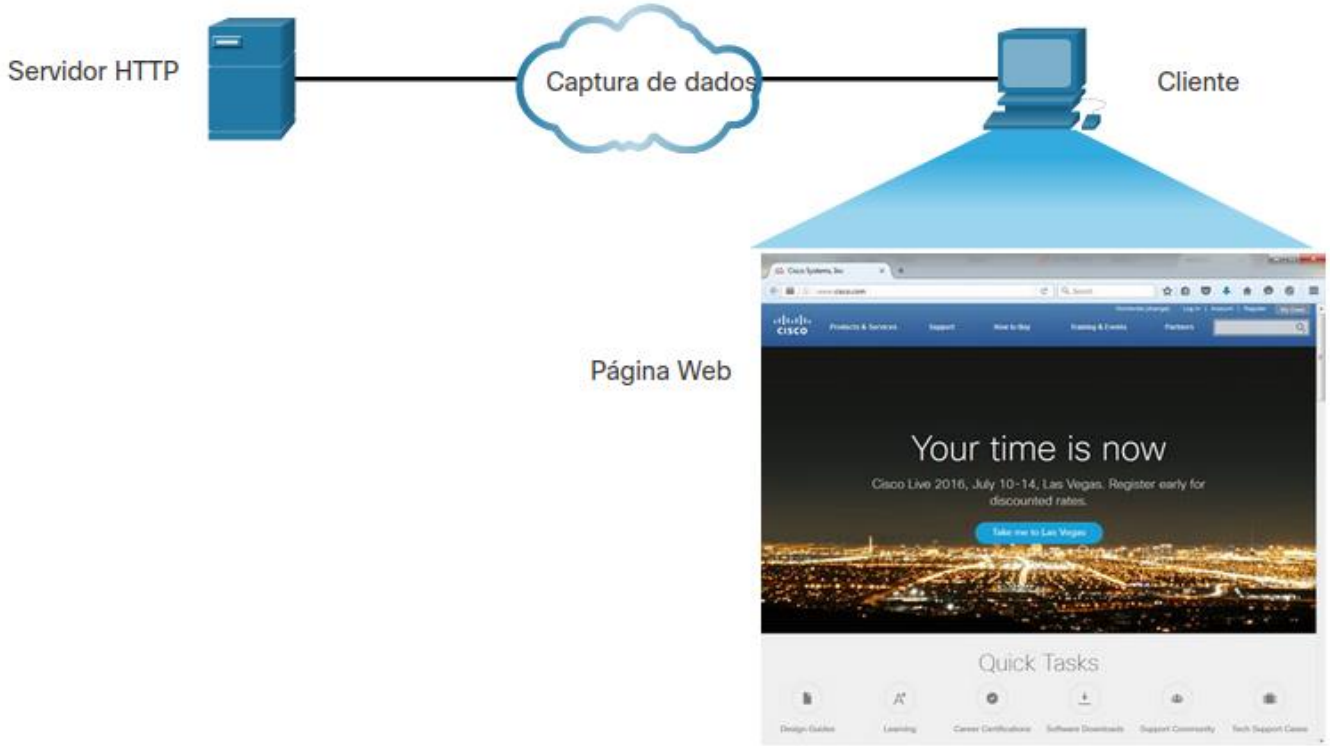
- Na primeira etapa, a **URL é separada em 3 partes**, o http que é o **protocolo**, o www.cisco.com que é o **servidor** de destino e o index.html que é **recurso** desejado, no caso uma página.
- Na segunda etapa, o navegador Web aciona o serviço **DNS** para obter o IP da URL e então o cliente envia a requisição para o servidor (GET).
- Na terceira etapa, o servidor então responde enviando o recurso codificado para o cliente.
- Por último, o navegador interpreta a resposta e exibe corretamente para o cliente.

O navegador interpreta como três partes da URL:

- http (o protocolo ou esquema)
- www.cisco.com (o nome do servidor)
- index.html (o nome do arquivo específico solicitado)




Resposta HTTP
Servidor HTTP
Rede
Cliente
HTTP/1.1 200 OK
Date: Mon, 23 May 2005 22:38:34 GMT
Server: Apache/1.3.27 (unix) (Red-Hat/Linux)
Last-Modified: wed, 08 Jan 2003 23:11:55 GMT
Etag: "3f80f-1b6-3elcb03b"
Accept-Ranges: bytes
Content-Length: 438
connection: close
content-Type: text/html; charset-UTF-8
<html>
<head>
<title>Cisco Systems Inc, Home Page</title>
</head>
<body>
...CONTENTS OF HTML PAGE...
Código HTML da
página Web


Servidor HTTP
Captura de dados
Cliente
Página Web
Your time is now
Cisco Live 2016, July 10-14, Las Vegas. Register early for discounted rates.
Quick Tasks

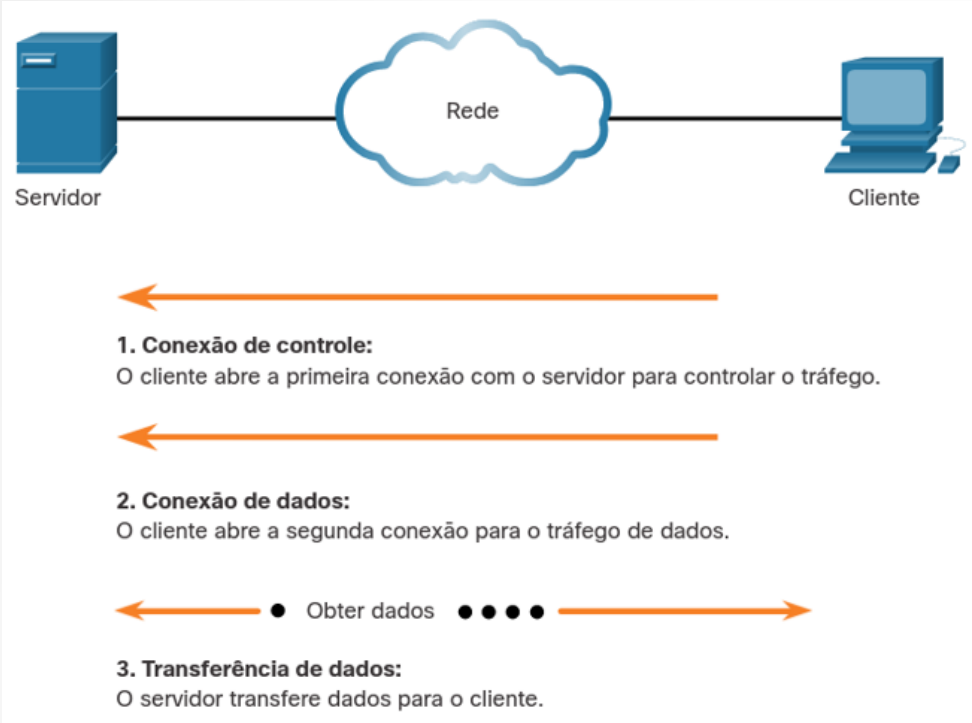
MENSAGENS E MÉTODOS

O protocolo HTTP utiliza tipos de mensagens e alguns métodos para organizar a comunicação entre cliente e servidor.

- **HTTP REQUEST** (Requisição): é um pedido do cliente para o servidor. Por exemplo que trocamos de página ou acessamos um endereço é enviada uma requisição. Uma requisição contém métodos, por exemplo o método **GET** para obter algum recurso do servidor (página, música, etc) ou um método **POST** para enviar dados para processamento.
- **HTTP RESPONSE** (Resposta): é a reposta do servidor para uma requisição, juntamente a um **código** (status) que representa o tipo de resposta. Por exemplo, **200** significa que tudo ocorreu sem erros, **301** significa um redirecionamento da requisição, **401** significa que o cliente não tem permissão para tal requisição, **404** significa que o recurso solicitado não existe no servidor, **500** significa que houve algum erro do servidor no processamento.

PROTOCOLO FTP

O protocolo FTP foi desenvolvido para possibilitar a **troca de arquivos** entre cliente e servidor. Utiliza TCP e opera nas portas 20/21, onde faz o controle da sessão e o envio dos dados.



LABORATÓRIO

Simulação de serviços L7 com o Packet Tracer

- HTTP/HTTPS
- DHCP
- DNS
- SMTP/POP

LABORATÓRIO

Instalação de servidores Web e DNS em ambiente Linux

- Apache
- Bind9

SEGURANÇA DE REDES


I'm not a
Hacker
I'm a
"SECURITY

ASPECTOS DO AMBIENTE E DA SEGURANÇA

A segurança das redes sempre foi e sempre será um ponto crítico, pois a informação é um dos bens mais valiosos de uma organização. Desde um **ataque cibernético a Estônia** em 2007, passou-se também a temer uma espécie de guerra virtual entre nações, sendo mais barata, menos arriscada e podendo realizar ataques a distância.

O conceito **CID** de segurança vem abranger minimamente aspectos de proteção para uma informação. Se a informação não é "vazada" (**confidencialidade**), não é modificada (**integridade**) e está a disposição quando necessária (**disponibilidade**) é altamente provável que esteja segura.

Uma tarefa importante é identificar as ameaças e vulnerabilidades de uma rede ou ambiente.


Módulo © Copyright 2004
Módulo © Copyright 2004
Minha Senha é DUDU
ESPORTES
Senha: TOTO
Nome: Tonho
VISITA
DADOS PRIVADOS
BACKUP
BACKUP
GAME
OFF
Word
PwPoint
Excel
Excel
WORD
OFICIAL
OFICIAL
Módulo © Copyright 2004

VULNERABILIDADES

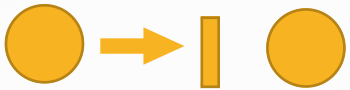
Vulnerabilidade pode ser vista como o **grau de fraqueza** em uma rede ou dispositivo, sendo todos sujeitos a tal. Os três principais grupos ou fontes de vulnerabilidade são a tecnologia, a configuração da rede/equipamentos e a política.

- **Tecnologia**: o próprio protocolo TCP/IP contém vulnerabilidades como o HTTP, FTP e ICMP, além do envio de SMTP. Os sistemas operacionais também contém problemas de segurança que devem ser tratados.
- **Configuração**: senhas frágeis ou **sem criptografia**, contas de usuários não protegidas, serviços de Internet mal configurados, **permissões indevidas**, roteamentos mal feitos, etc.
- **Política**: controles de acessados não aplicados, **política de segurança não implementada**, alterações ou instalações não autorizadas, plano de recuperação inexistente, treinamentos, etc.

MODELOS DE ATAQUES

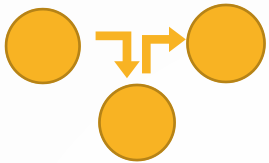
Um ataque cibernético pode ser feito de várias formas, cujas podemos classificar em algumas categorias.

- **Interrupção**: o serviço ou recurso **para** de ser fornecido por ação voluntária de terceiros.

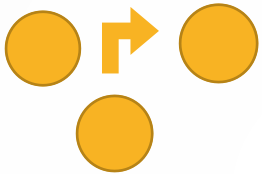


- **Interceptação**: a informação é acessada por **terceiros**, sem autorização para tal ação.

- **Modificação**: a informação é **alterada** sem autorização, a fim de parecer original.



- **Fabricação**: quando a fonte de um recurso ou serviço é **falso**, mas aparenta ser verdadeiro.



AMEAÇAS E ATAQUES

Em cada modelo, pode-se encontrar algum ataque realizado por invasores e malfeitores.

- **Roubo de informações**: o serviço ou recurso é invadido para obtenção de dados que são **vendidos ou utilizados de modo indevido**.
- **Perda/manipulação**: o serviço ou recurso é invadido e os dados são **destruídos ou alterados**, como a mudança de um preço do item ou um vírus reformatando um disco rígido.
- **Roubo de identidade**: informações pessoais são roubadas para **falsificação de identidade** afim de obter documentos, fazer compras não autorizadas, etc.
- **Interrupção de serviço**: conhecido como **DoS**, quando usuários legítimos são impedidos de acessar um serviço ou recurso os quais tem direito.

ATAQUES DE VÍRUS, WORM E TROJANS

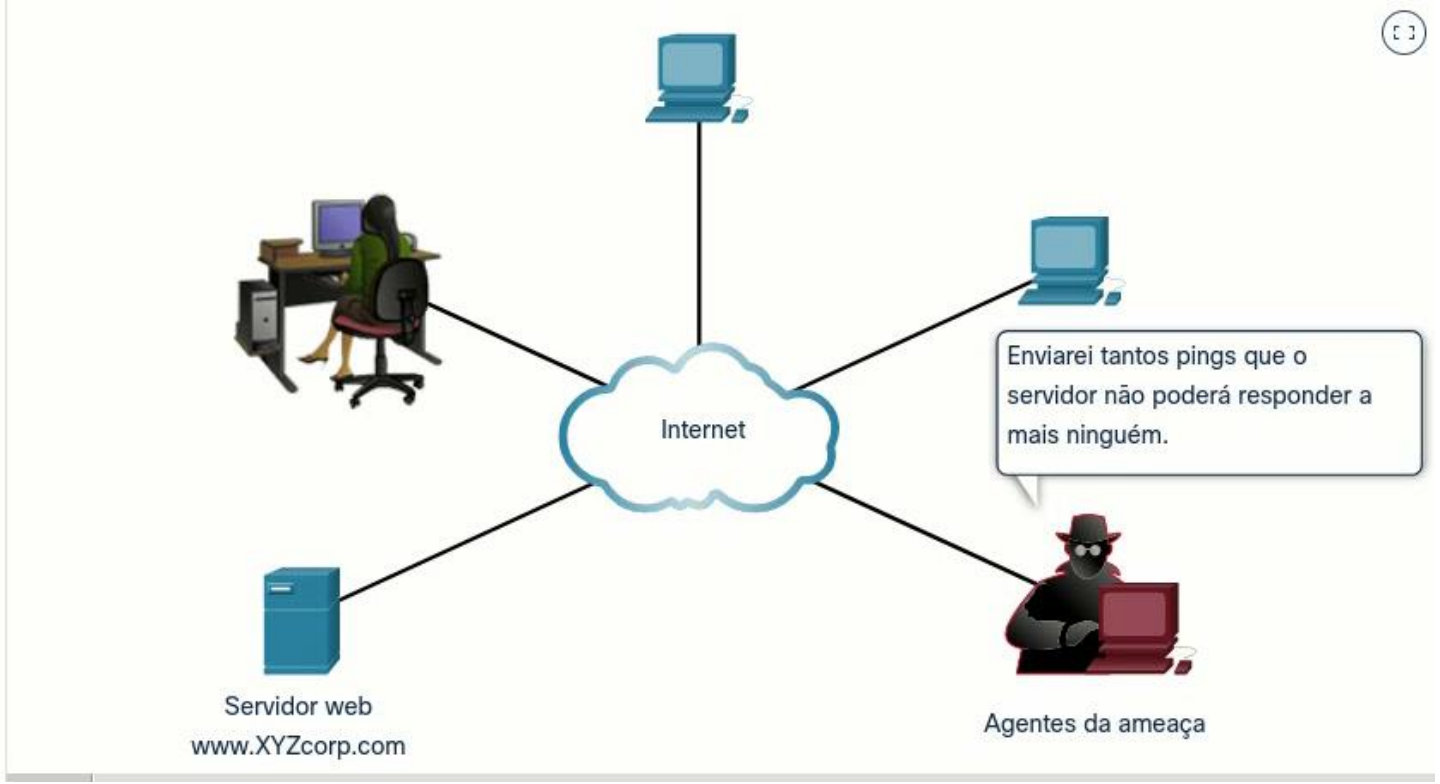

Dispositivo de clonagem sendo preparado para instalação.
BDN
Rede de Auto-Atendimento
Instruções de uso


Dispositivo instalado de forma
a não perceber a anormalidade.
Leitura do código de barras
Instruções de uso


Bradesco
Tarifas de
Serviços Bancários.
Pessoa Física
Micro câmera para visualizar tela do equipamento (Letras de Acesso)
Micro câmera para visualizar o teclado (senha de seis dígitos)

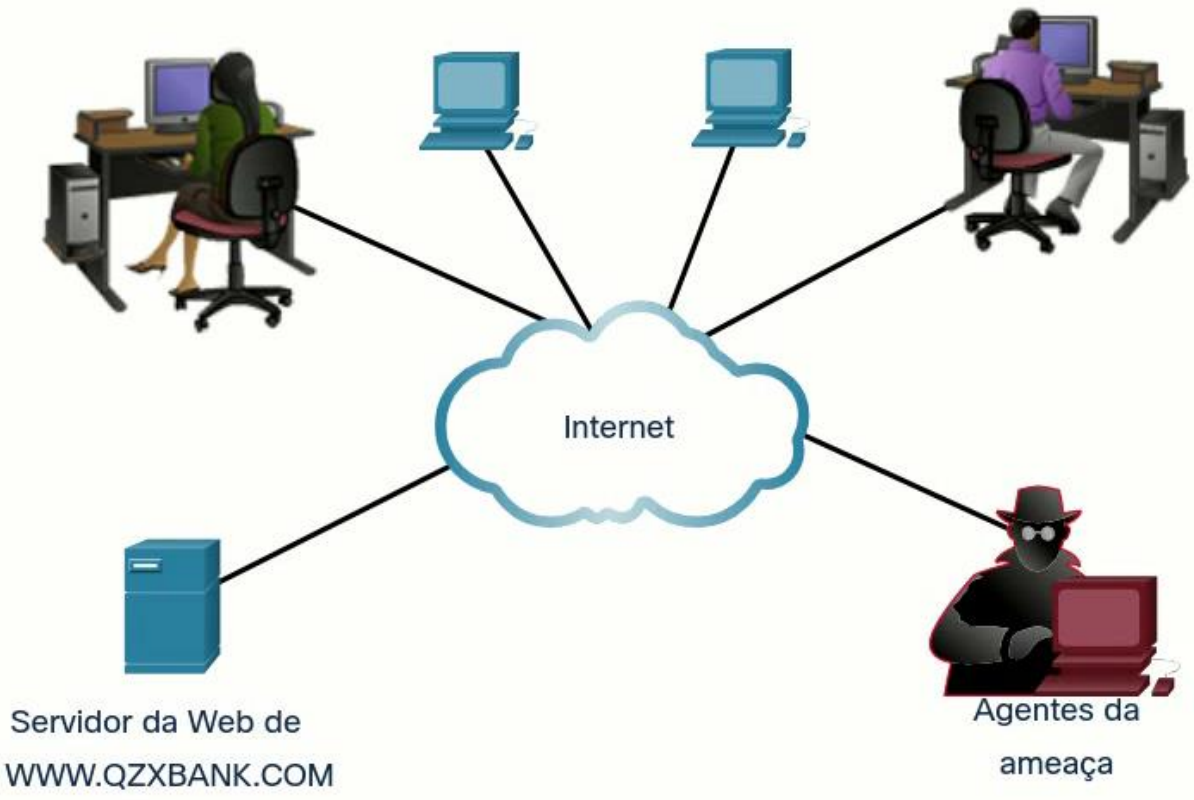

Bradesco
Tarifas de
Serviços Bancários.
Pessoa Física
Multi Expresso
Bradesco

Panasonic
PV-BP50
60
ALL BATTERY
GENUINE CAMCODER PART
U.S.A CONSUMER
BATTERY MUST BE RECYCLED.
CALL 1-800-SAY-LEAD
IN THE U.S.A.
NONSPILLABLE
Matsushita Electric Industrial Co.,Ltd. Made in Japan



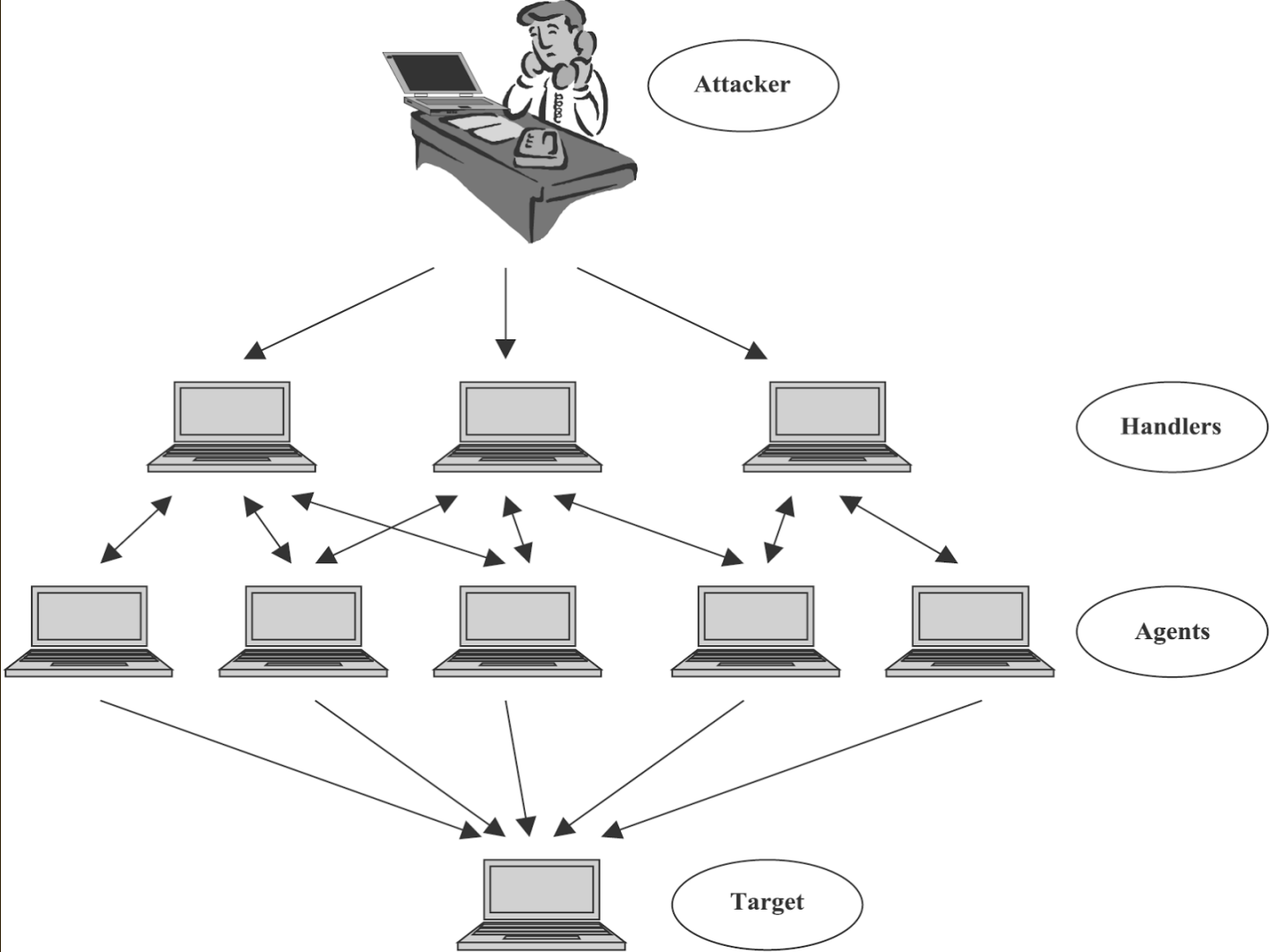
O ataque de negação de serviço não é uma técnica de invasão e sim de interrupção do alvo, por meio de sobrecarga de solicitações (**flood**).

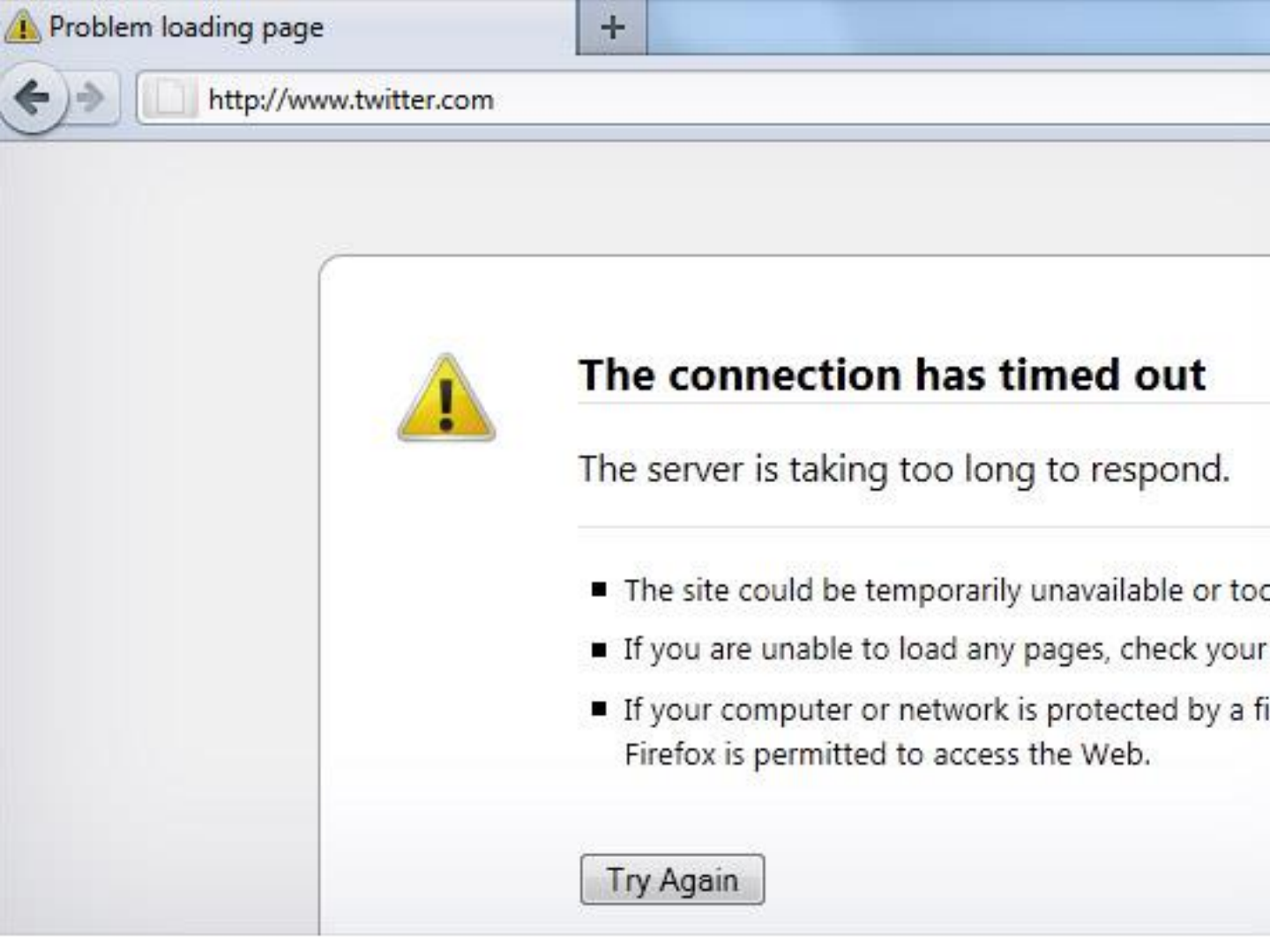
ATAQUE DOS (DENIAL OF SERVICE)



O ataque de negação de serviço distribuído é feito por máquinas infectadas, comandadas a distância.

ATAQUE DDOS (DISTRIBUTED DENIAL OF SERVICE)

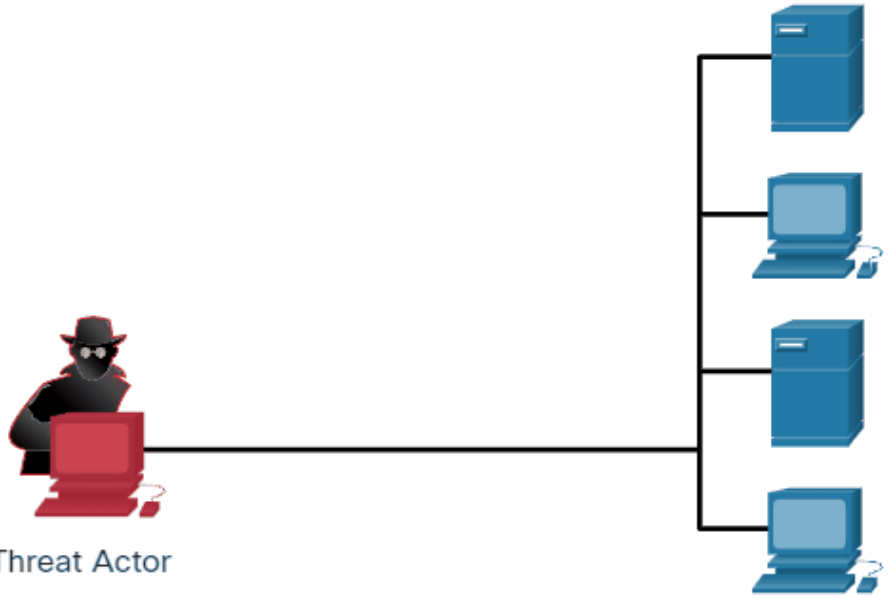

Attacker
Handlers
Agents
Target


Problem loading page
http://www.twitter.com
The connection has timed out
The server is taking too long to respond.
The site could be temporarily unavailable or too
If you are unable to load any pages, check your
If your computer or network is protected by a fi
Firefox is permitted to access the Web.
Try Again

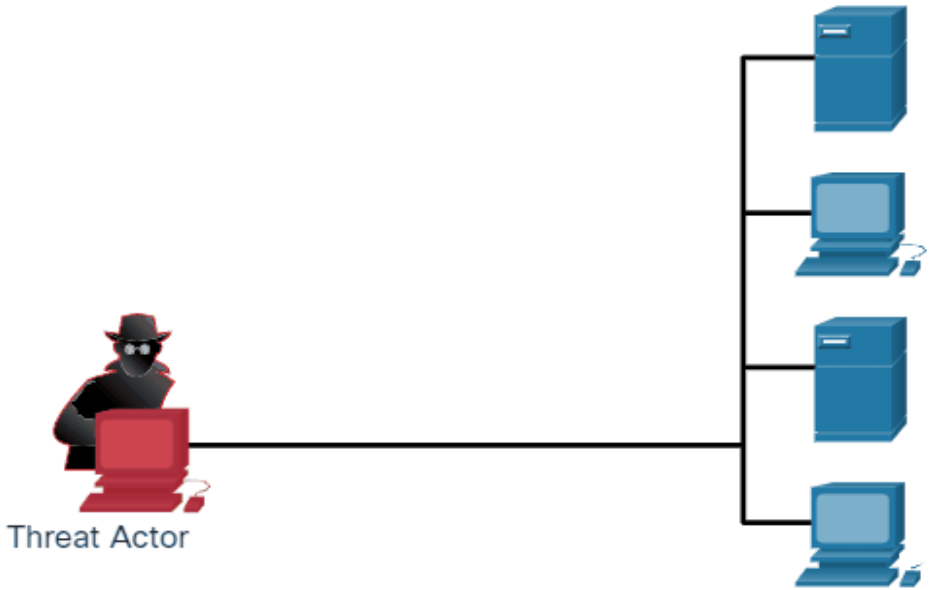
ATAQUE DE RECONHECIMENTO

Combinado em 2 técnicas chamada **footprint** e **fingerprint**, buscam levantar informações sobre o alvo para mapear possível vulnerabilidades, sendo bastante difícil detectar.

- **Consultas à bases da Internet**: reconhece o alvo por registros na Internet como **nslookup** ou **whois**.
- **Varredura de ping** : utiliza dos utilitários ping, fping, gping etc para **mapear** quais alvos estão ativos.
- **Verificações de porta**: ferramentas como o **Nmap** podem mostrar quais serviços ou portas estão ativas no alvo.



BUSCANDO EM BASES DA INTERNET

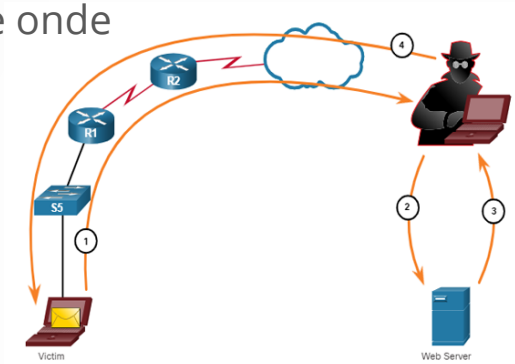


REALIZANDO VARREDURAS EM PORTAS

ATAQUE DE ACESSO

Busca obter acesso a contas da Web, banco de dados e outras informações confidenciais, utilizando vulnerabilidades em serviços de autenticação, FTP e HTTP.

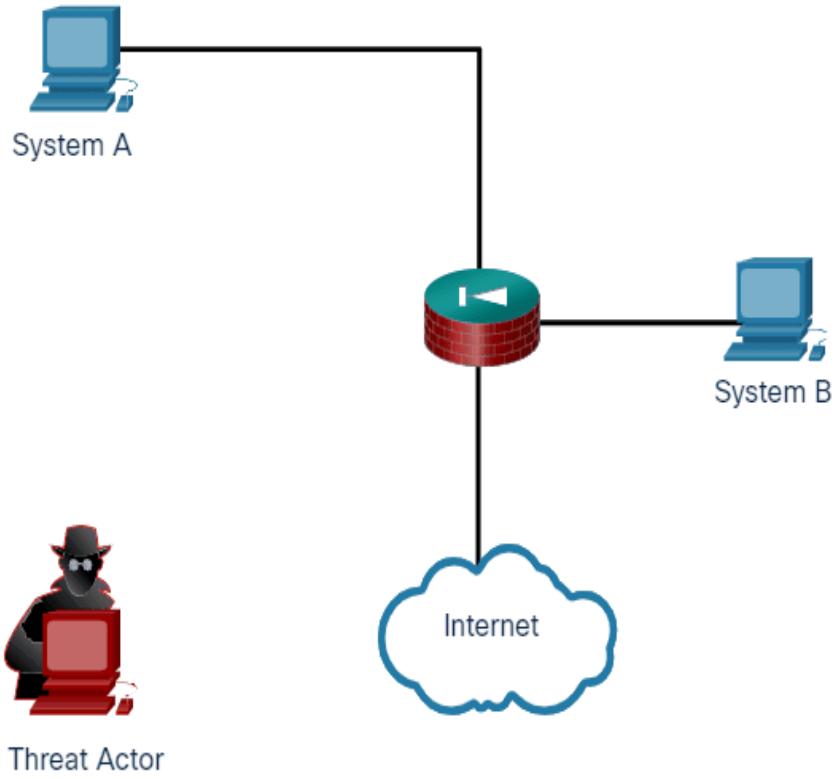
- **Captura de senha**: pode utilizar ataques de força bruta, cavalos de Tróia ou **sniffers** de pacotes.
- **Exploração de confiança**: o atacante utiliza privilégios não autorizados para obter **acesso a um sistema a partir de outro.**
- **Homem no meio**: cenário de ataque onde um agente de ameaça é posicionado entre duas entidades legítimas para ler ou modificar os dados que passam entre as duas partes.



PASSWORD CRACKER

É a quebra de senha de acesso por técnicas e softwares, como a força bruta, com tentativas sucessivas até o acerto, utilizando dicionários **próprios** na Internet. Alguns softwares populares são:

- OPHCrack;
- Cain and Abel;
- John the Ripper;
- Air Crack;
- Air Snort;
- Brutus;
- Unsecure;
- NetKeyView;
- Ppa;
- CowPatty



ATAQUE DE CONFIANÇA

ENGENHARIA SOCIAL

Uma das mais poderosas formas de ataque, **explora as fraquezas humanas** para obter acesso a informações e recursos exclusivos. Com os sistemas de segurança cada vez mais sofisticados, percebeu-se facilmente que o ser humano era o alvo mais vulnerável.

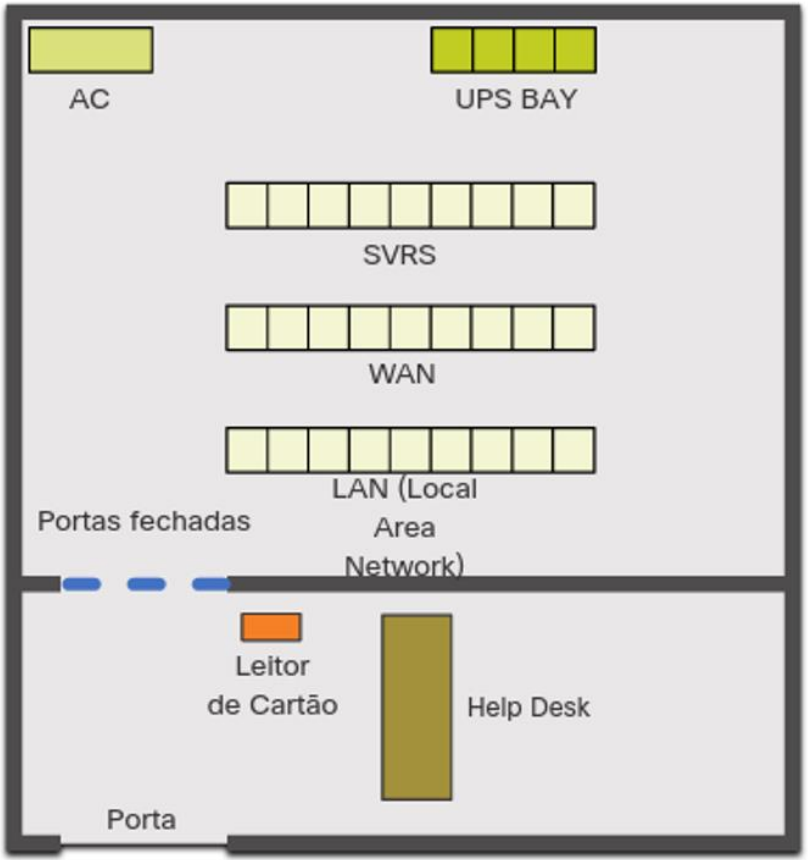
Algumas técnicas são **falsidade ideológica**, analisar documentos na mesa de **pessoas distraídas**, namorar alguém da organização, etc.

SEGURANÇA FÍSICA

A estrutura física de uma rede pode ser tão vulnerável quanto softwares ou sistemas operacionais, pois se comprometidos, podem afetar seriamente o funcionamento da rede.

- **Ameaça de hardware**: servidores, roteadores, switches, cabeamento e estações de trabalho.
- **Ameaça ambiental**: extremos de temperatura e extremos de umidade devem ser monitorados e controlados.
- **Ameaça elétrica**: picos de tensão, tensão de alimentação insuficiente ruídos ou falta de energia sem contingência.
- **Ameaça de manutenção**: descarga eletrostática, falta de peças de reposição críticas, cabeamento incorreto, rotulagem inadequada.

Um bom plano de segurança física deve abranger a **proteção aos ativos** como um todo.



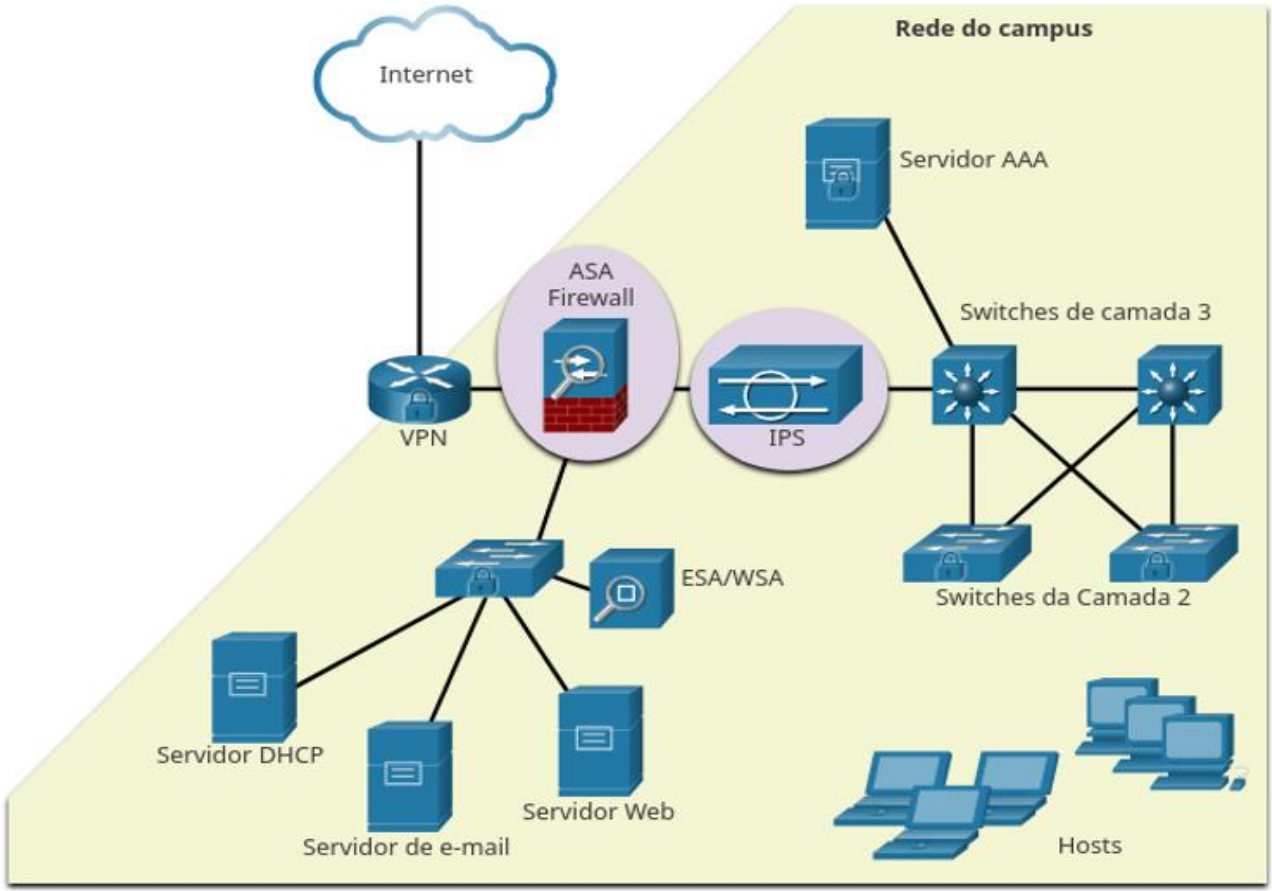
O **acesso físico** aos equipamentos deve ser bloqueado e controlado. Impedir acesso por portas, janelas, piso elevado, teto e canais de ventilação.

O uso de **logs eletrônicos** também é válido, assim como **câmeras de segurança**.

FERRAMENTAS DE SEGURANÇA

Para mitigar ameaças, várias técnicas e procedimentos de segurança podem ser implementados, via hardware, software e pessoas. O ideal é proteger roteadores, switches, servidores e hosts, abordando uma segurança por camadas.

- **VPN**: cria **túneis seguros** para acesso remoto autenticados e fornece serviços de localização para sites seguros.
- **Firewall**: barra **conexões externas indevidas** aos hosts internos.
- **IPS**: previne **intrusões** monitorando o tráfego de entrada e saída procurando anormalidades.
- **ESA/WSA**: **filtros** para e-mail e navegação Web contra malwares, spam, spoofing e phishing.
- **Servidor AAA**: servidor de **autenticação**



AMBIENTE INTEGRADO DE SEGURANÇA

MEDIDAS DE PREVENÇÃO

Além de softwares e sistemas de segurança, algumas medidas podem prevenir danos mais severos.

- **Backup**: backups de ativos de rede são importantes contra perda de dados, podendo ser guardado em uma mídia removível ou em um servidor FTP local/em nuvem. Considerar sempre a **frequência**, conforme política de TI, **integridade** de armazenamento e recuperação, **segurança** da cópia e validação no acesso e restauração. Considerar também backup de hosts
- **Atualização/Patch**: pode corrigir bugs e vulnerabilidades, aumentando a eficácia contra ataques conexões externas indevidas aos hosts internos. Nos hosts, manter versões atualizadas de **patches de segurança**.
- **AAA**: igualmente importante é implementar a **autenticação, autorização e controle** em todos os dispositivos de rede.

MONITORAMENTO

O monitoramento de redes podem ser essencial para antecipar falhas, detectar ataques, manter recursos, entre outros. A atividade de monitorar deve ser feita com um **NMS** para alguns benefícios.

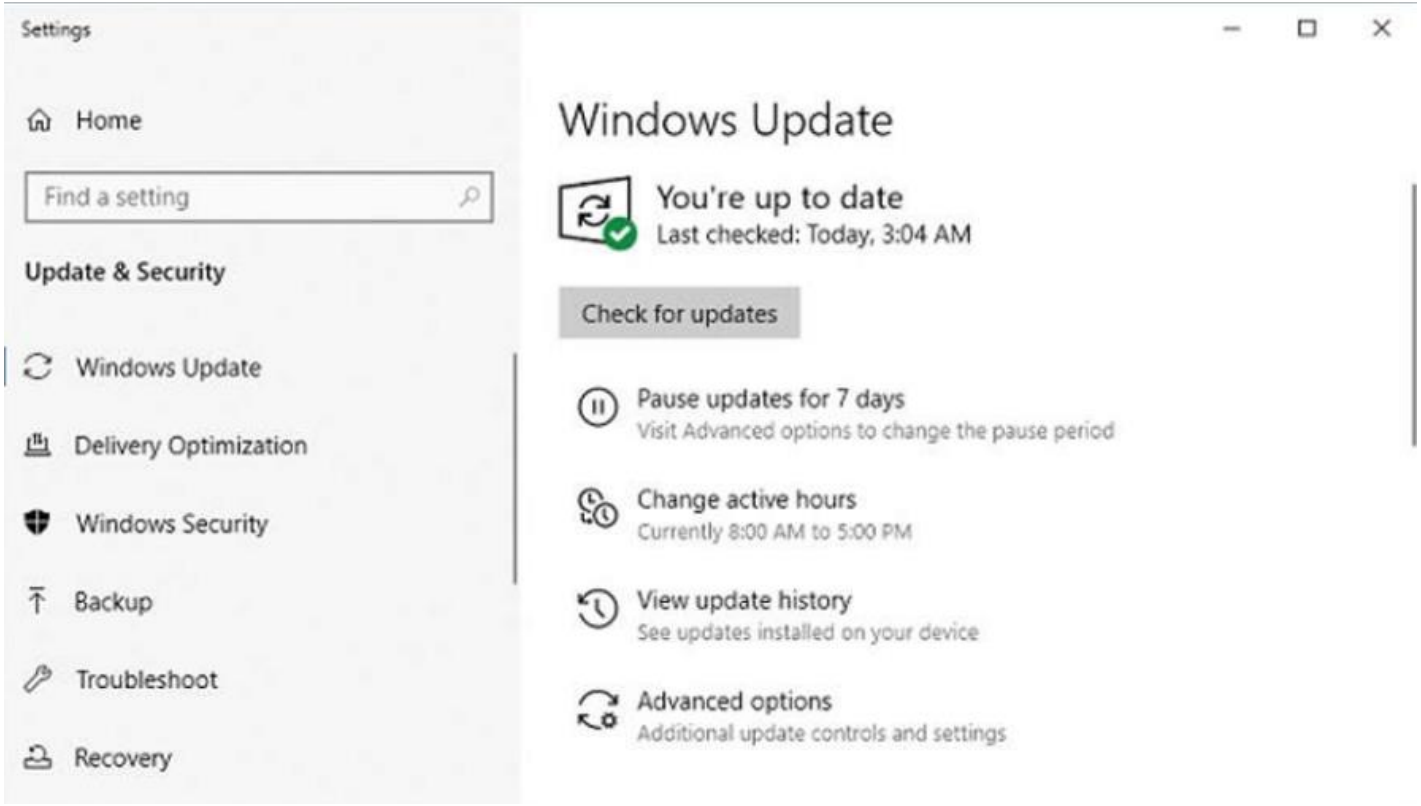
- monitorar de forma automatizada, evitando falhas humanas.
- visualizar eventos em tempo real, para mais rápida atuação.
- auxiliar no inventário de hardware e planejar novos investimentos.
- Concentrar o gerenciamento de falhas, configuração, contas, desempenho e segurança em um recurso.

Várias opções de NMS estão disponíveis, tanto em softwares livres (Cacti, Nagios, Zabbix, PRTG, OpenNMS) quanto em soluções comerciais (CA Unicenter, HP OpenView, IBM Tivoli).

LABORATÓRIO

Instalação e Configuração de um NMS

- Zabbix
- Grafana


Settings
Home
Find a setting
Update & Security
Windows Update
Delivery Optimization
Windows Security
Backup
Troubleshoot
Recovery
Windows Update
You're up to date
Last checked: Today, 3:04 AM
Check for updates
Pause updates for 7 days
Visit Advanced options to change the pause period
Change active hours
Currently 8:00 AM to 5:00 PM
View update history
See updates installed on your device
Advanced options
Additional update controls and settings

Autenticação

Quem é você?

Autorização

Quanto você pode gastar?

Contabilização

Em que você gastou?

Account Number	Statement Closing Date	Current Amount Due
1234-567-890	01-31-01	$278.50

JOE EMPLOYEE
456 SKYVIEW DRIVE
HOMETOWN, USA 99900-1234

MAIL PAYMENT TO :
THE BANK
132 VINE STREET
ANYTOWN, USA 67500-0010

872919345 00178255000000003

Detach here and return upper portion with check or money order. Do not staple or fold.

Statement of Personal Credit Card Account

Retain this portion for your files.

THE BANK

Cardmember Name	Account Number	Statement Closing Date
JOE EMPLOYEE	1234-456-890	01-31-01

Statement Date:	02-01-01	Payment Due Date:	03-01-01
Closing Date:	01-31-01		
Credit Limit	$1,500.00	Credit Available:	$1221.50
New Balance:	$278.50	Minimum Payment Due:	$20.00

Account Summary

Previous Balance:	+74.24	Transaction Fees:	+3.00
Purchases:	+250.50	Annual Fees:	+25.00
Cash Advances:	+0	Current Amount Due:	+250.50
Payments:	-74.25	Amount Past Due:	+0
Finance Charge:	+0	Amount Over Credit Line:	+0
Late Charge:	+0	NEW BALANCE:	$278.50

Reference Number	Sold	Posted	Activity Since Last Statement		Amount
43210987	01-03	01-13	Payment, Thank You		-$74.25
01234567	01-12	01-13	Wings 'N' Things	Anytown, USA	$25.25
78901234	01-14	01-17	Record Release	Anytown, USA	$40.00
45678901	01-14	01-17	Sports Stadium	Anytown, USA	$75.25
3210987	01-22	01-23	Tie Tack	Anytown, USA	$20.75
76543210	01-29	01-30	Electronic World	Anytown, USA	$89.25
23455678		01-30	Transaction Fees		$3.00
34567890		01-01	Annual Fee		$25.00

PAGE 1 OF 1

TÉCNICAS DE SENHAS

Um senha deve ser forte o suficiente de modo a ser difícil de adivinhar e fácil de lembrar. Senhas mais longas são mais seguras, mas a principal característica deve ser a **complexidade**.

- Use senhas de 8 a 10 caracteres.
- Torne sua senha complexa, com iniciais de uma frase ou misturando caracteres especiais com alfanuméricos, inclusive espaço, se permitido.
- Altere senhas periodicamente para limitar danos por perdas.

Senhas consideradas fracas: “secret”, “oliveira”, “toyota”, “joao1995”, “folhaazul23”.

Senhas consideradas fortes: “j0n4s@2023”, “dhaqmecp_pcg”

OUTRAS TÉCNICAS

- **Criptografia**: embaralhar o conteúdo da mensagem para **ocultar seu significado**.
- **Esteganografia**: visa esconder não o conteúdo, mas sim a **existência** da mensagem.
- **Biometria**: avanço em relação a autenticação, deixando de ser por algo que o usuário tem (cartão) ou sabe (senha) para considerar **características físicas e biológicas**.

TBMDJ GVGV!


BANCO CENTRAL DO BRASIL
100
100
REAIS
A 1026069479 A


Fibras Coloridas
Linhas Multidirecionais
MicroImpressões
Marca D'Água
Registro Coincidente
BANCO CENTRAL DO BRASIL
MODELO 100
100
REAIS
A 0000000000 A
Marca Tátil
Imagem Latente
Fio de Segurança
A 0000000000 A
Numeração

Cor
Azul-turqueza

156mm — **Tamanho** — 70mm

Faixa holográfica mostra número cem, a palavra reais, a garoupa colorida e diversas cores em movimento

Pode-se ver o **valor da nota escondido** dentro do retângulo à direita, quando ela está em posição horizontal

Marca d´água revela um peixe e um número cem, contra a luz

Alto relevo pode ser sentido nas legendas, números, figuras e laterais da nota

Oreja

Geometría de la mano

Estructura venosa

Retina

Termografía facial

Huella Dactilar

Iris

Voz

Firma

Cara

CONFIGURAÇÕES DE SEGURANÇA

A configuração de segurança de ativos de rede é um dos pontos mais críticos e importantes da operação. Dispositivos Cisco vem com um assistente denominado **Auto Secure** que irá guiar o usuário e fazer ajustes quando ativado.

```
Router# auto secure
                --- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of
the router but it will not make router absolutely secure
from all security attacks ***
```

Além disso, podemos configurar outros parâmetros, como **criptografar** todas as senhas, definir um **tamanho mínimo** para elas, detectar ataques de **força bruta** e desativar o modo de configuração após um **período inativo**.

```
R1(config)# service password-encryption
R1(config)# security passwords min-length 8
R1(config)# login block-for 120 attempts 3 within 60
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# exec-timeout 5 30
R1(config-line)# transport input ssh
R1(config-line)# end
```

Na configuração de exemplo acima, estamos definindo um tamanho **mínimo** de senha de **8 caracteres**. Também estamos **bloqueando** o login por **2 minutos**, caso a senha seja digitada **3 vezes incorretamente dentro de 60 segundos**. Por fim, estamos definindo um tempo **ocioso** de no **máximo 5 minutos e 30 segundos** antes de **desconectar** o usuário.

CONFIGURAÇÕES DE SEGURANÇA

Outra configuração importante em equipamentos Cisco é desativar os serviços e portas não utilizados. Com o comando **show ip ports all** podemos visualizar todos os serviços ativos. Por exemplo, o acesso web ao equipamento pode ser desativado com no **ip http server**.

```
Router# show ip ports all
Proto Local Address              Foreign Address            State       PID/Program Name
TCB       Local Address              Foreign Address            (state)
tcp    :::443                    :::*                       LISTEN      309/[IOS]HTTP CORE
tcp    *:443                     *:*                        LISTEN      309/[IOS]HTTP CORE
udp    *:67                       0.0.0.0:0                              387/[IOS]DHCPD
Receive
```

E por último, vem a configuração do acesso remoto, via SSH. Configure um **nome de domínio IP** para identificação, gere uma chave para criptografar os dados trafegados de **até 2048 bits**, crie o usuário e vincule o acesso SSH ao banco de dados local.

```
Router# configure terminal
Router(config)# hostname R1
R1(config)# ip domain name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com % The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
```

No exemplo acima, a chave de criptografia foi definida para **1024 bits**, dessa forma podemos até usar a versão mais nova do protocolo SSH. O comando **login local** faz com que os usuários do próprio equipamentos sejam credenciais para acesso via SSH.

CONFIGURAÇÕES DE SEGURANÇA

Na plataforma Huawei, a segurança mínima tem os aspectos:

- A criptografia se dá pela palavra-chave **cipher** antes das senhas, ou ainda **irreversible-cipher**.
- O tamanho mínimo da senha pode ser configurado com o **comando set password min-length**, seguido da quantidade de caracteres desejada.
- O desligamento do login pode ser forçado após um período de inatividade com o comando **idle-timeout**, seguido pela quantidade em minutos.
- A força bruta pode ser evitada configurando o bloqueio automático do login após erros de senha com **wrong password**, seguido pelo intervalo de tentativas com **retry-interval,** seguido pela quantidade com **retry-time,** seguido pelo período de bloqueio em minutos com **block-time**

```
<HUAWEI> system-view
[~HUAWEI] aaa
[~HUAWEI-aaa] local-user hello@163.net password irreversible-cipher Hello@163
```

```
[Base] set password min-length 10
```

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] idle-timeout 10
```

```
<AC6605> system-view
[AC6605] aaa
[AC6605-aaa] local-aaa-user wrong-password retry-interval 5 retry-time 3 block-time 5
```

METODOLOGIA NIST

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

O NIST é um instituto americano de padrões, sendo um dos mais antigos laboratórios de ciências físicas do país. Trabalham, além de padrões, com tecnologia em geral, inclusive segurança cibernética. Define 4 etapas para resposta a incidentes de segurança:

- **Preparação**: **liste os ativos de rede** e classifique-os por importância. Então tenha uma base de tráfego para comparações e um plano de **quem deve ser comunicado** baseado em cada equipamento e incidente. Em seguida, determine quais eventos devem ser investigados e crie um **plano de resposta** para cada um deles.
- **Detecção e Análise**: aqui um incidente foi detectado. **Reúna informações sobre o incidente** e analise o impacto.
- **Contenção, Erradicação e Recuperação**: estancar as perdas, **remover a ameaça** e voltar ao normal.
- **Atividade Pós-Incidente**: relatórios, pesquisa, aprendizagem, possíveis cenários futuros, etc

ANÁLISE DE SEGURANÇA

Vamos exercitar uma análise de segurança, com os seguintes aspectos.

- **Sistema**: identificação de equipamentos, dados, softwares, hardwares, pessoas e processos.
- **Ameaças**: naturais (inundação, enchente, deslizamento de terra, etc), ambientais (queda de energia, poluição, produtos químicos, vazamentos, etc) e humanas.
- **Vulnerabilidades**: Falhas ou fraquezas que podem ser exploradas (falta de treinamento/atualizações, etc).
- **Controles**: O que o sistema possui atualmente para controle de vulnerabilidades e ameaças?
- **Probabilidades x Impactos x Riscos**: Possibilidade de acontecimento, efeitos e fator de risco numérico.
- **Recomendações**: O que pode ser melhorado? Quais as soluções propostas para redução de riscos?
- **Documentação dos Resultados**: produção do documento final.

LABORATÓRIO

Instalação e Configuração de Ferramentas de Segurança

- Firewall do Windows
- IPTables
- Valhala Honeypot
- Nmap
- Cain & Abel

SERVIDORES – WINDOWS SERVER

WINDOWS SERVER

O Windows Server é o sistema operacional da Microsoft para servidores, que se difere de sua linha para estações de trabalho. Foram várias edições e sub-edições:

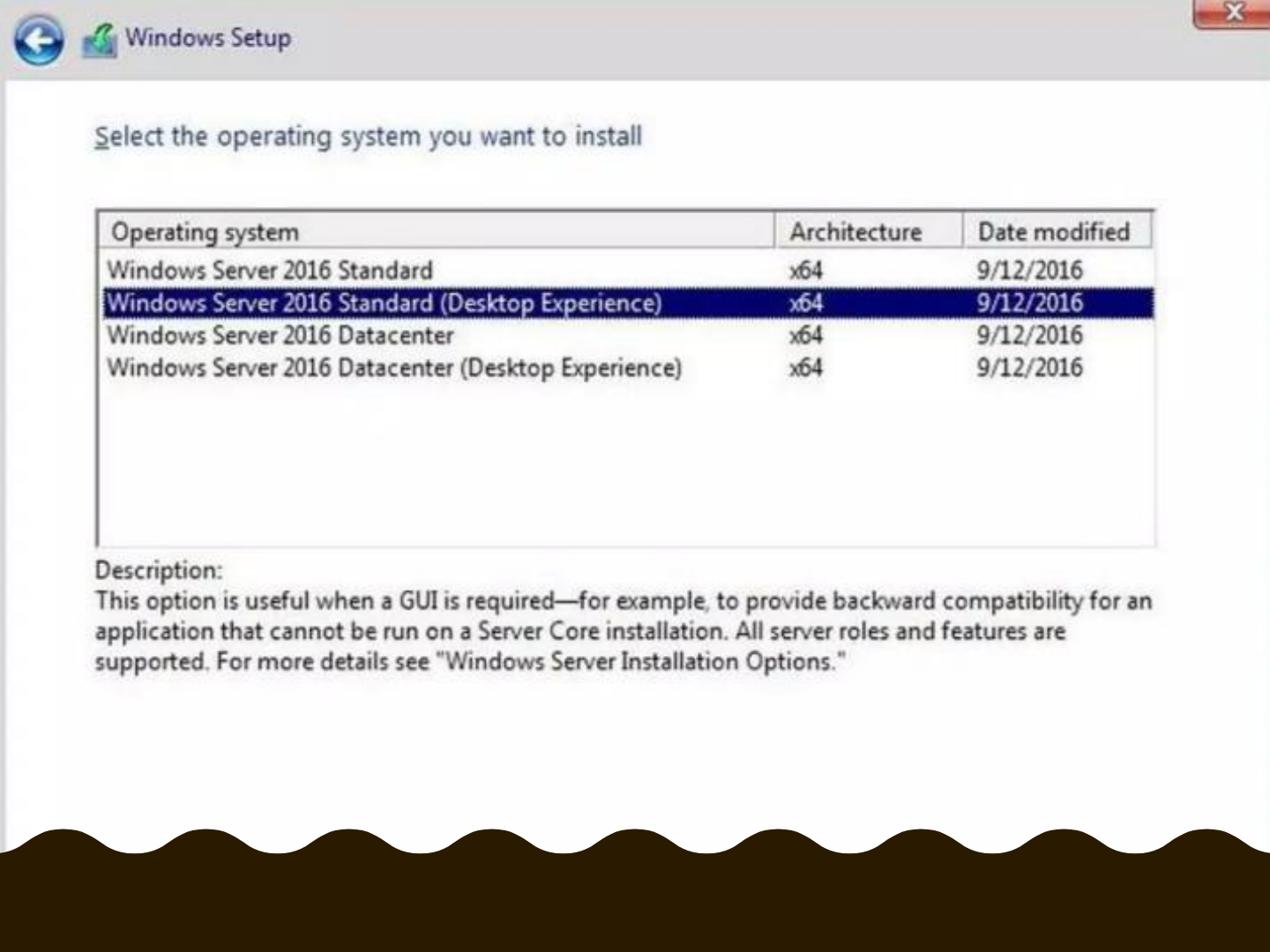
- **Windows NT Server**: primeira versão, idealizada em 2003.
- **Windows 2000 Server Edition**: mesma interface do Windows Professional 2000, foi o primeiro com o Active Directory, o Kerberos para autenticação, .
- **WS 2003**: melhorias gerais nos serviços de rede, no AD, no servidor Web IIS
- **WS 2008**: melhorias gerais.
- **WS 2012**: o primeiro com a interface Metro, com melhorias gerais no AD e no IIS
- **WS 2016**: melhorias gerais.
- **WS 2019**: além das melhorias gerais, veio preparado para funções em nuvem e com suporte ao protocolo HTTP/2 .

CATEGORIAS WINDOWS SERVER

As principais edições para Windows Server, incluem:

- **Datacenter**: para ambientes virtualizados ou datacenters por software. Essa categoria suporta no máximo 24 TB da RAM. Instâncias ilimitadas de máquinas virtuais por licença.
- **Standard**: para ambientes físicos e com baixa carga/densidade. Também suporta 24 TB de RAM, número de cores ilimitado, mas apenas 2 máquinas por licença.
- **Essentials**: voltado para pequenos negócios, com até 25 usuários e 50 dispositivos conectados. Apenas uma instância pode ser executada na licença.

É possível ainda obter uma instalação chamada de “Nano Server”, mais leve, sem GUI, sendo otimizada para nuvem. Neste material, iremos tratar da versão **Windows Server 2016, na edição Standard**.


Windows Setup
Select the operating system you want to install
Operating system
Architecture
Date modified
Windows Server 2016 Standard
x64
9/12/2016
Windows Server 2016 Standard (Desktop Experience)
x64
9/12/2016
Windows Server 2016 Datacenter
x64
9/12/2016
Windows Server 2016 Datacenter (Desktop Experience)
x64
9/12/2016
Description:
This option is useful when a GUI is required—for example, to provide backward compatibility for an application that cannot be run on a Server Core installation. All server roles and features are supported. For more details see "Windows Server Installation Options."

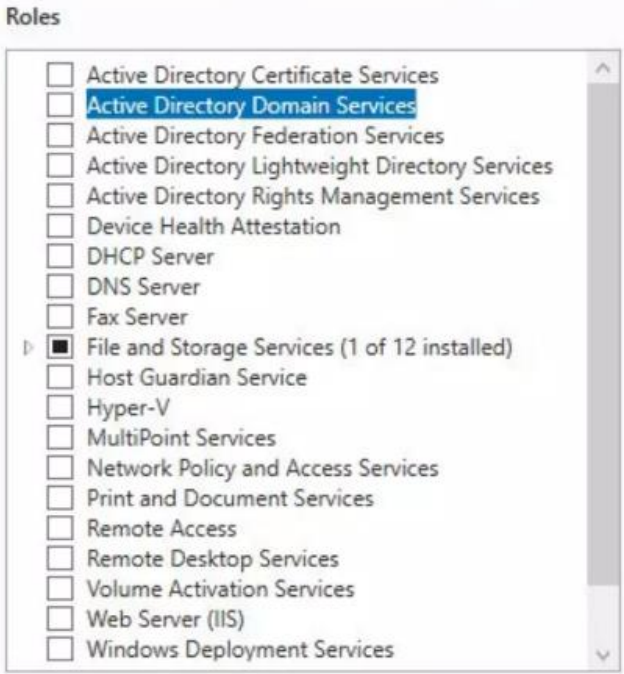
ESCALA COMPARATIVA WINDOWS SERVER 2012 X 2016

Descrição dos recursos	Windows Server 2012/2012 R2 Standard e Datacenter	Windows Server 2016 Standard e Datacenter
Suporte a memória física (host)	Até 4 TB por servidor físico	Até 24 TB por servidor físico (6x)
Suporte a processador lógico físico (host)	Até 320 LPs	Até 512 LPs
Suporte a memória de máquina virtual	Até 1 TB por máquina virtual	Até 12 TB por máquina virtual (12x)
Suporte a processador virtual de máquina virtual	Até 64 VPs por máquina virtual	Até 240 VPs por máquina virtual (3,75x)

RECURSOS DISPONÍVEIS

No Windows Server 2016, os recursos disponíveis vieram melhorados em relação a versão 2012, mesmo os recursos padrão.

- Active Directory com melhorias.
- DHCP Server
- DNS Server
- Servidor de Arquivos
- Servidor de Impressão
- Containers
- Hyper-V
- Power Shell 5.1
- Servidor Web IIS



ACTIVE DIRECTORY

É o enorme banco de dados de **serviço de diretório**, presente na linha Windows Server, que contém informações sobre todas as contas de usuário de uma rede, permitindo uma administração bastante abrangente. Permite autenticar e autorizar usuários e computadores em uma rede, atribuindo diretivas de segurança e outras diversas configurações a eles.

Permite também armazenar e gerenciar as informações trafegadas na rede. **É baseado no protocolo LDAP**, apesar de não ser o único protocolo utilizado no AD.

Fazendo uma analogia, se o AD é uma grande biblioteca, o LDAP é um excelente bibliotecário.

SERVIDOR DE ARQUIVOS E IMPRESSÃO

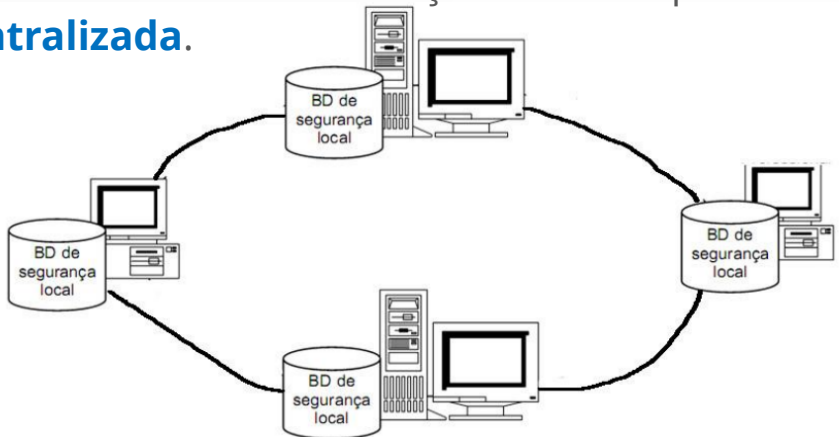
O serviço de arquivos do Windows Server, permite o armazenamento local e remoto de arquivos dos usuários, com controle de permissão de acesso. Contém opções de aplicação de **cotas de discos** por usuário e **filtro de tipos de arquivos para o armazenamento**. Também é possível fazer redundância do armazenamento, como um backup sincronizado.

O serviço de impressão permite controlar as impressoras presentes na rede, de forma centralizada, facilitando o compartilhamento. Permite realizar **um diagnóstico remoto de toners, filas de impressão, carga de papel**, etc. Também faz controle por permissão de cada usuário.

O GRUPO DE TRABALHO

Máquinas com sistema Windows vem por padrão aninhada em um grupo de trabalho, denominado também por WORKGROUP. Trata-se de um agrupamento de dispositivos em rede, compartilhando recursos, mas **sem um servidor central** para gerenciamento.

Cada estação no grupo de trabalho mantém um relação de dados de forma local, como contas de usuários e informações de segurança , tornando a administração deste tipo de arquitetura, **descentralizada**.



DOMÍNIO, ÁRVORE E FLORESTA

Diferentemente do grupo de trabalho, o domínio é uma coleção de dispositivos em rede, mas que compartilha um banco de dados centralizado. É a **principal unidade na estrutura do Active Directory**, abrigando máquinas locais e remotas, onde as regras de segurança, permissões e configurações administrativas são únicas para cada domínio.

Em cada domínio também há os gerentes (Domain Controller). Sempre que um dispositivo é adicionado a um domínio, ele recebe um FQDN que especifica o local daquele equipamento dentro da estrutura, numa organização hierárquica parecida com o DNS.

A árvore é simplesmente uma coleção de domínios, com um domínio raiz. A floresta... você já deve imaginar o que é!

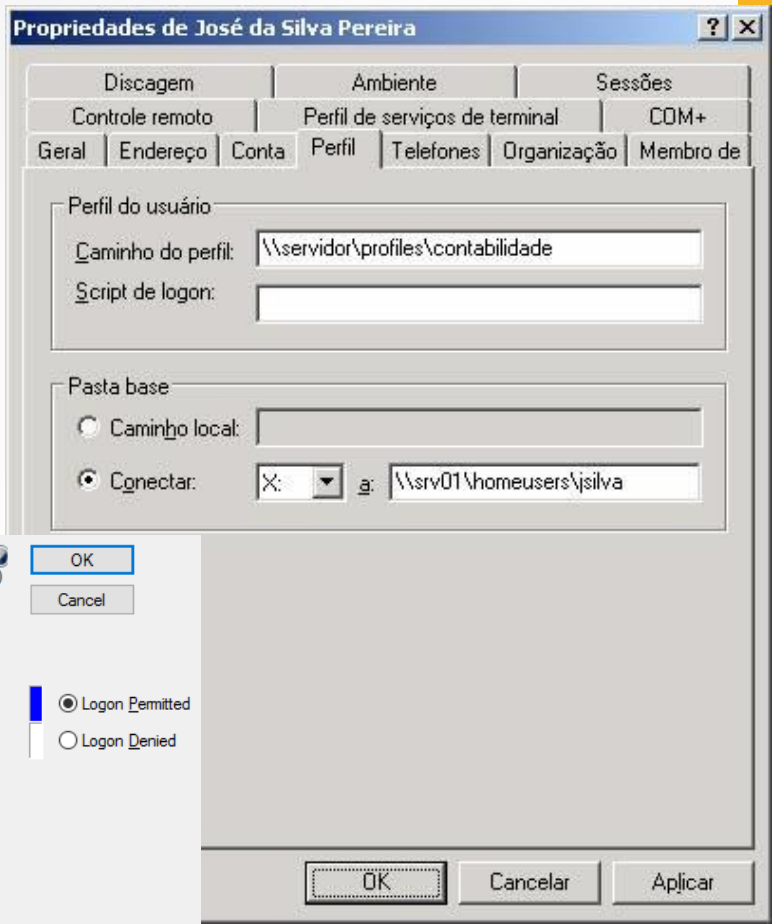
LABORATÓRIO

Primeiros Passos com o Windows Server

- Instalação
- Instalação do AD
- Controlador de Domínio
- Criação de Usuário
- Criação de Grupo

ADMINISTRAÇÃO DE USUÁRIOS

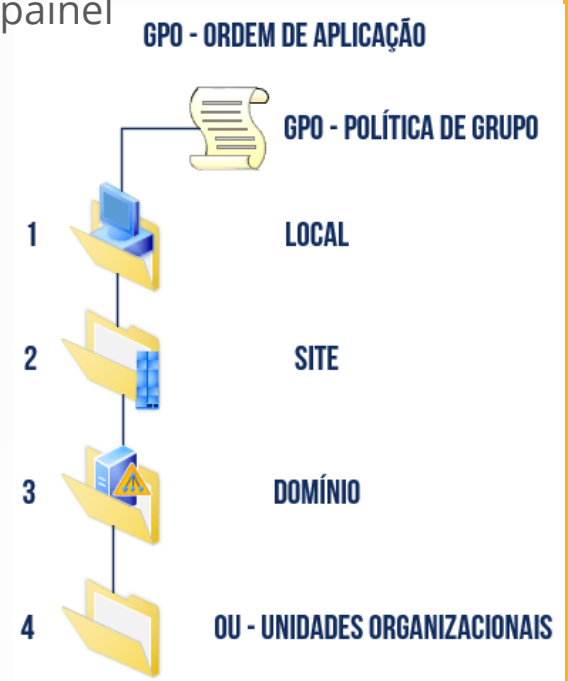
Usuários cadastrados no Active Directory podem ser configurados em diversos aspectos, desde um política de senha, até controle de logon por horário.



GPO

Uma GPO é uma política de grupo com diretrizes e regras para diversos recursos dos usuários e computadores. Pode ser aplicada **localmente** (num único usuário ou computador) ou no **domínio** como um todo. Com uma GPO, é possível, por exemplo, bloquear o menu executar, painel de controle, definir aspectos de configuração do Internet Explorer como página inicial, sites confiáveis, favoritos e outros.

São mais de **3000 GPOs** que podem ser aplicadas no Windows Server 2016. Há um ordem de **precedência** para aplicação de uma GPO.



BOAS PRÁTICAS DE GPO

A maioria das GPOs dizem respeitos a segurança de forma geral, mas há também GPOs para personalização, acessos e administração de privilégios. Algumas boas práticas de GPO são:

Limitar ou Bloquear o Painel de Controle: através do Painel de Controle , pode-se **controlar todos os aspectos do computador**. Limitar o acesso permite que as organizações mantenham dados e outros recursos íntegros.

Desativar o prompt de comando: Por ele pode-se executar comandos que dão **privilégios aos usuários** e ignoram outras restrições do sistema. Por isso, é prudente desabilitar o Prompt de Comando para garantir a segurança dos recursos do sistema.

Impedir instalações de software: com isso, impedimos que os usuários instalem **aplicativos ou malware indesejados** que possam comprometer o sistema.

LABORATÓRIO

GPO e Administração de Usuário

- Limitar Logon
- Forçar Troca de Senha
- GPO de Segurança
- GPO de Personalização
- GPO de Firewall

DNS E DHCP

O serviço DNS vem disponível para instalação no pacote de recursos do Windows Server 2016, bastando configurar a Zona de Pesquisa Direta e a Zona de Pesquisa Inversa e testar com o comando **nslookup**.

O mesmo ocorre com o serviço de DHCP, bastando instalar através do assistente e configurar as faixas de IP para distribuição, as faixas de IP para exclusão, e os demais parâmetros de rede como máscara, gateway, DNS e Leasing. A configuração pode ser feita tanto em IPv4 quanto em IPv6.

LABORATÓRIO

DNS e DHCP

- Instalação e Configuração DNS
- nslookup
- Instalação e Configuração DHCP

SERVIDORES – LINUX SERVER

LINUX SERVER

As distribuições Linux para servidores caracterizam-se por não conter por padrão uma interface gráfica, além de um melhor aproveitamento do hardware em geral. Algumas distribuições são:

- **Debian Server**: tem excelente estabilidade desde 1996, sendo um dos melhores no quesito segurança pela sua maturidade.
- **Ubuntu Server**: uma das mais conhecidas distribuições, é derivada do Debian, contendo as mesmas funcionalidades, lidando bem com arquivos, jogos, web, e-mail e proxy.
- **CentOS**: derivado da RHEL, é extremamente poderoso, com perfil mais empresarial, com gerenciador de pacotes rpm.
- **Slackware**: bastante estável e já contém diversas aplicações na instalação completa. Para usuários mais experientes, por não ser tão popular.
- **Fedora**: também derivado da RHEL, com aplicações já inclusas.
- **OpenSUSE**: bastante estável, para usuários mais experientes.

AMBIENTE LAMP

Um servidor WEB em plataforma Linux deve reunir um ambiente completo, com as ferramentas mínimas necessárias para a execução de uma aplicação Web. Este ambiente chamamos de LAMP que é um acrônimo para **L**inux, **A**pache, **M**ySQL e **P**HP.

- **Apache**: é o servidor web propriamente dito, de código aberto, parte da Apache Foundation, presente desde 1995 e responsável por boa parte do crescimento inicial da Internet.
- **MySQL**: É um dos mais populares e utilizados gerenciador de banco de dados, mantido atualmente pela Oracle.
- **PHP**: É uma linguagem de programação dinâmica, processada do lado do servidor, por este motivo, sendo necessário instalar seu interpretador para execução do código PHP.

Adicionalmente, podemos ter uma ferramenta de FTP no servidor para transferência de arquivos e uma administração gráfica do banco de dados, evitando a linha de comando.

LABORATÓRIO

Ambiente LAMP com algumas funcionalidades

- Instalação Apache
- Instalação MySQL
- Instalação PHP
- Instalação FTP Server
- Instalação PHPMYADMIN

DNS

Dependendo da distribuição, o serviço DNS terá de ser instalado separadamente, sendo que alguns Linux já contém um serviço DNS incluso. Duas opções bem populares são o **Unbound** e o **Bind9**. Para o exemplo, iremos considerar o Bind9 na distribuição Ubuntu.

Como em qualquer serviço DNS, é necessário configurar a zona direta e a zona reversa. No Bind9 os arquivos de configuração ficam em /etc/bind.

Para testes podemos usar os comandos **nslookup**, **host** e **dig**. Basta observar as respostas dos comandos para que o servidor DNS está resolvendo corretamente os endereços.

LABORATÓRIO

Servidor DNS Bind9

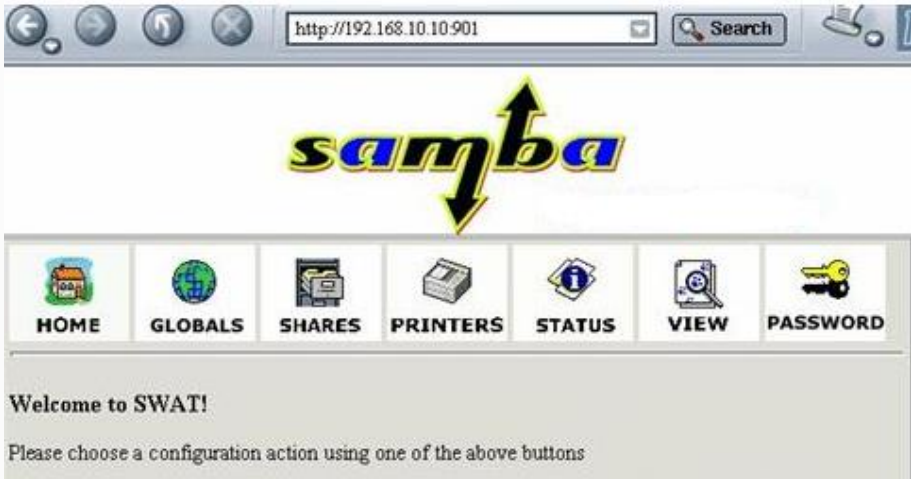
- Instalação e configuração do BIND9
- Testes com dig
- Testes com nslookup
- Testes com host

SERVIDOR DE ARQUIVOS

Um software popular para Linux no tocante a compartilhamento de arquivos é o SAMBA. Um servidor SAMBA permite compartilhar **arquivos do servidor Linux em um rede de computadores Windows**, utilizando o protocolo SMB.

A configuração do servidor SAMBA é feita em um **único arquivo** e de maneira bem simples, o que não significa que seja desprovido de segurança, pelo contrário.

O SAMBA também pode ser configurado através de uma interface gráfica, sendo bastante eficiente. A ferramenta mais popular para isso é o SWAT, sendo acessado pela porta padrão **901**



LABORATÓRIO

Servidor de Arquivos

- Instalação e configuração do SAMBA
- Testes de Acesso
- Instalação SWAT