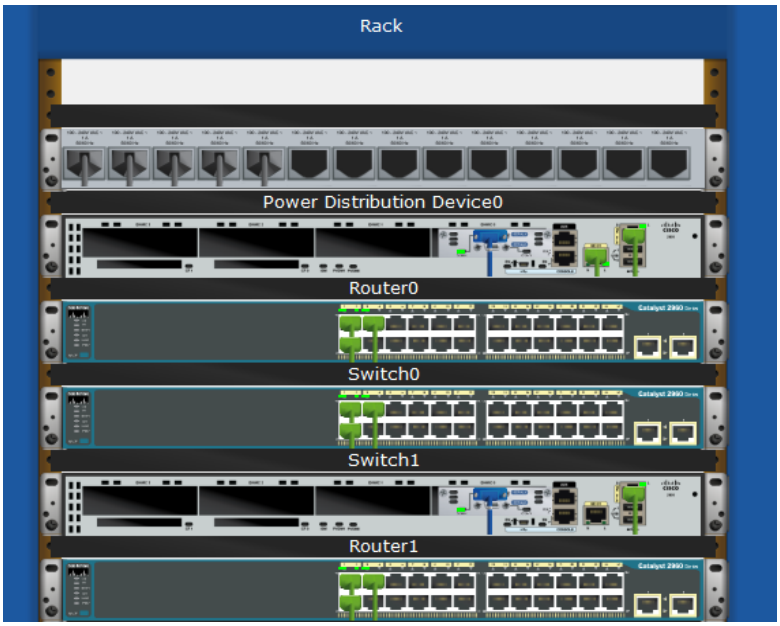
INSTITUTO TÉCNICO LUCRÉCIO DOS SANTOS

1º MANUAL DE APOIO AS AULAS DE REDES DE COMPUTADOR



Elaborado por: Hermelindo André Dias David

Luanda, 2021

SUMÁRIO

1. Histórico e evolução das Redes de Computadores

Para conhecer um pouco do avanço da tecnologia da área de redes, vamos pensar na definição do termo "Teleprocessamento". Teleprocessamento significa processamento à distância, ou seja, podemos gerar informações em um equipamento e transmiti-las para outro equipamento para serem processadas.

A necessidade da comunicação à distância levou, em 1838, a invenção do telégrafo por **Samuel F. B. Morse**. Esse evento deu origem a vários outros sistemas de comunicação como o telefone, o rádio e a televisão.

Na década de 1950, com a introdução de sistemas de computadores, houve um grande avanço na área de processamento e armazenamento de informações.

O maior avanço das redes de computadores aconteceu com a popularização da Internet. Essa grande rede mundial, onde hoje podemos ler nossos e-mails, acessar páginas Web, entrar em grupos de discussão, comprar os mais diversos artigos, ver vídeos, baixar músicas, etc., passou por vários processos até atingir este estágio e a sua tendência é evoluir cada vez mais.

Depois da Segunda Guerra, EUA e URSS começaram a ter seus desentendimentos, dando origem à **Guerra Fria** em 1949. Neste contexto, em que os dois blocos ideológicos e politicamente antagônicos exerciam enorme controlo e influência no mundo, qualquer mecanismo, qualquer inovação, qualquer ferramenta nova poderia contribuir nessa disputa liderada pela **União Soviética** e pelos **Estados Unidos**: as duas superpotências compreendiam a eficácia e a necessidade absoluta dos meios de comunicação.
Nessa perspectiva, o governo dos Estados Unidos temia um ataque russo às bases militares. Um ataque poderia trazer a público informações sigilosas, tornando os EUA vulneráveis. Então foi idealizado um modelo de troca e compartilhamento de informações que permitisse a descentralização das mesmas. Assim, se o Pentágono fosse atingido, as informações armazenadas ali não estariam perdidas. Era preciso, portanto, criar uma rede

Em 1969, iniciou-se uma conexão, com circuitos de 56 kbps, entre 4 localidades (Universidades da Califórnia, de Los Angeles e Santa Bárbara, Universidade de Utah e Instituto de Pesquisa de Stanford). Essa rede foi denominada ARPANET.

Várias universidades e empresas privadas foram envolvidas na pesquisa. Esse investimento foi devido ao receio do governo norte-americano de um ataque soviético a suas instalações, e a necessidade de distribuir suas bases de informação. Desde modo começaram a participar e contribuir com inúmeras pesquisas durante a década de 70, contribuições estas que deram origem ao protocolo TCP/IP.

A arquitetura denominada TCP/IP (Transmission Control Protocol / Internet Protocol) é uma tecnologia de conexão de redes resultante da pesquisa financiada pela Agência de Defesa dos Estados Unidos, DARPA (Defense Advanced Research Projects Agency).

Em 1980, a Universidade da Califórnia de Berkeley, que desenvolveu o sistema operacional UNIX, escolheu o protocolo TCP/IP como padrão. Como o protocolo não é proprietário, o crescimento da utilização do TCP/IP foi extraordinário entre universidades e centros de pesquisa.

Em **1985**, a NFS (National Science Foundation) interligou os supercomputadores de seus centros de pesquisa, a NFSNET. No ano seguinte, a NFSNET foi interligada a ARPANET, dando origem à Internet.

O cientista **Tim Berners-Lee**, do **CERN**, criou a **World Wide Web**, a linguagem **HTML** e o protocolo **HTTP** em 1992. Essa linguagem simples, mas eficiente, era usada para a criação dos sites com o conceito de hipertexto (documentos ligados entre si). A empresa norte-americana **Netscape** criou o protocolo HTTPS (HyperText Transfer Protocol Secure), possibilitando o envio de dados criptografados para transacções comercias pela internet.

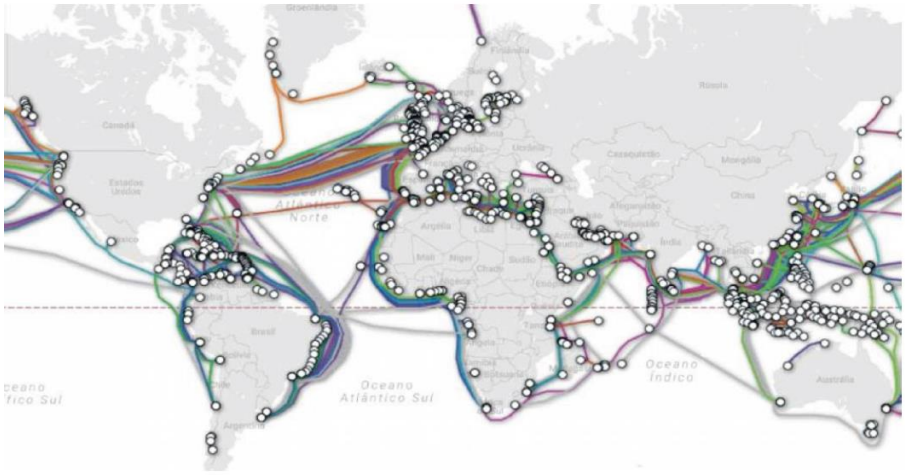


Ilustração 1-Mapa mundial ligação de fibra óptica

a) Detalhes de cada um dos cabos que estão representados acima? O site Submarine Cable Map cria um mapa interativo e você pode clicar em cada um deles. Acesse agora: https://www.submarinecablemap.com

b) Aprenda mais sobre os cabos submarinos? Assista esse vídeo de 9 minutos que explica mais detalhes. Dicionário de Informática: https://youtu.be/q-rBtDub3Hc

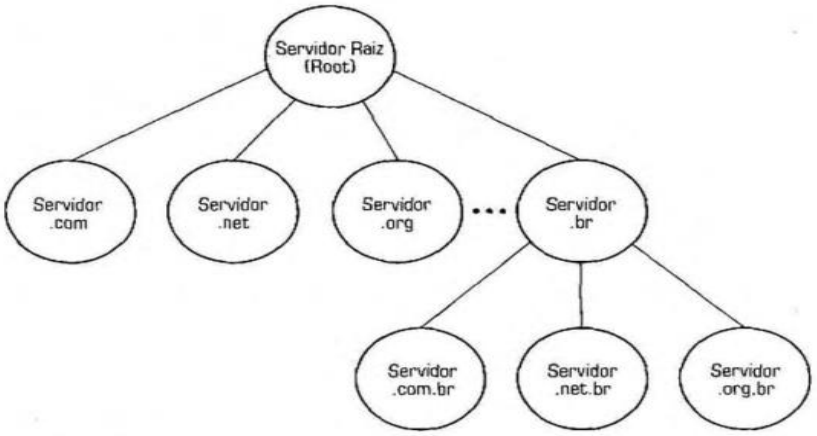


Ilustração 2-Estrutura hierárquica da Net

2. Conceitos Básicos de Redes de Computadores

2.1. Definição

Uma Rede de Computadores é um conjunto de computadores e dispositivos processadores capazes de trocar informações e compartilhar recursos, interligados por um sistema de comunicação.

2.2. Classificação segundo a extensão geográfica

2.2.1. Rede Local (LAN)

Rede de Área Local (LAN – Local Area Network), ou simplesmente Rede Local, é um grupo de computadores e dispositivos processadores interligados em uma rede em mesmo ambiente co-localizado.

Exemplo: A rede do ITLS

2.2.2. Rede de Longa Distância (WAN)

Rede de Longa Distância (WAN – Wide Area Network) é a rede de interligação de diversos sistemas de computadores, ou redes locais, localizados em regiões fisicamente distantes.

Exemplo: Uma rede que interliga serviço de emissão de cartas a nível nacional.

2.2.3. Rede Metropolitana (MAN)

Rede Metropolitana (MAN – Metropolitan Area Network) é uma rede dentro de uma determinada região, uma cidade, onde os dados são armazenados em uma base comum.

Exemplo: Uma rede de farmácias de uma mesma cidade.

2.2.4. Rede de Campus (CAN)

Rede de Campus (CAN – Campus Area Network) é uma rede que compreende uma área mais ampla que uma rede local, que pode conter vários edifícios próximos.

Exemplo: Um Campus Universitário.

2.2.5. Rede de Armazenamento (SAN)

Rede de Armazenamento (SAN - Storage Area Network) é uma rede que compartilha uma base de dados comum em um determinado ambiente.

Exemplo: Redes de um Minimercado.

2.3. Classificação de acordo a natureza

Do ponto de vista da maneira com que os dados de uma rede são compartilhados existem dois tipos básicos de rede: Ponto-a-ponto e Cliente/Servidor. O primeiro tipo é usado em redes pequenas, enquanto que o segundo tipo é largamente usado tanto em redes pequenas quanto em redes grandes. Note que essa classificação é independente da estrutura física usada pela rede, isto é, como a rede esta fisicamente montada, mas sim a maneira com que está configurada em software.

2.3.1. Redes Ponto-A-Ponto

Esse é o tipo de rede mais simples que ser montada. Praticamente todos os sistemas operacionais já vêm com suporte a rede ponto-a-ponto. Na rede ponto-a-ponto, os micros compartilham dados e periféricos sem muita burocracia. Qualquer micro pode facilmente ler e escrever arquivos armazenados em outros micros da rede bem como usar periféricos que estejam instalados em outros PCs. Obviamente tudo isso depende da configuração que é feita em cada micro individualmente, ou seja, não há o paple de um micro Servidor como nas redes cliente/servidor. Qualquer um dos micros da rede pode ser um servidor de dados e periféricos.

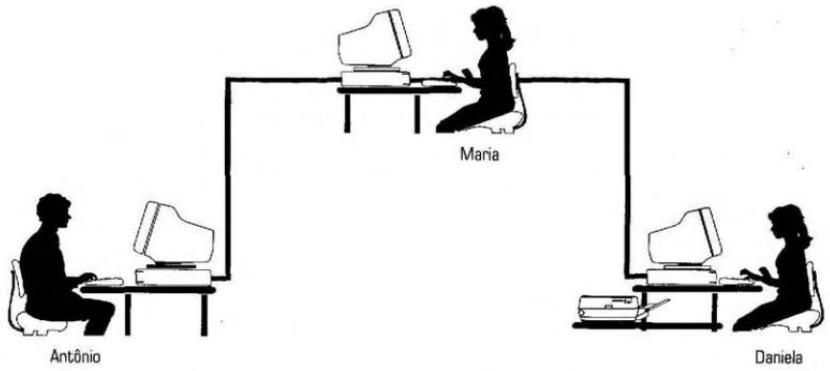


Ilustração 3- Redes Ponto-a-ponto

A figura mostra um escritório com três micros ligados em rede. Em um desses micros, há uma impressora instalada. Para que todos os micros possam ter acesso à impressora, basta o usuário daquele micro (Daniela) configurar o seu compartilhamento.

Características:

- Usado em redes pequenas (normalmente com até 10 micros).
- Baixo custo
- Fácil implementação
- Baixa segurança
- Sistema simples de cabeamento
- Todos os micros precisam necessariamente ser completos, isto é, funcionam normalmente sem estarem conectados à rede.
- Normalmente os micros estão instaldos em um mesmo ambiente de trabalho (um mesmo escritório, por exemplo)
- Não existem um administrador de rede, a rede é administrada por cada usuário.

- Cada micro na rede pode se comportar como cliente e servidor quando fornece um recurso.
- A rede terá problemas para crescer de tamanho.

2.3.2. Rede Cliente/Servidor

Se a rede estiver sendo planejada para ter mais de 10 micros instalados (ou no caso de redes pequenas onde a segurança for uma questão importante), então a escolha natural é uma rede do tipo cliente/servidor.

Nesse tipo de rede existe a figura do servidor, normalmente um micro que gera recursos para os demais micros da rede. O servidor é um micro especializado em um só tipo de tarefa, não sendo usado para outra finalidade como ocorre em redes ponto-a-ponto.

Com o servidor dedicado em a uma só tarefa, ele consegue responder rapidamente aos pedidos vindos dos demais micros da rede, não comprometendo o desempenho.

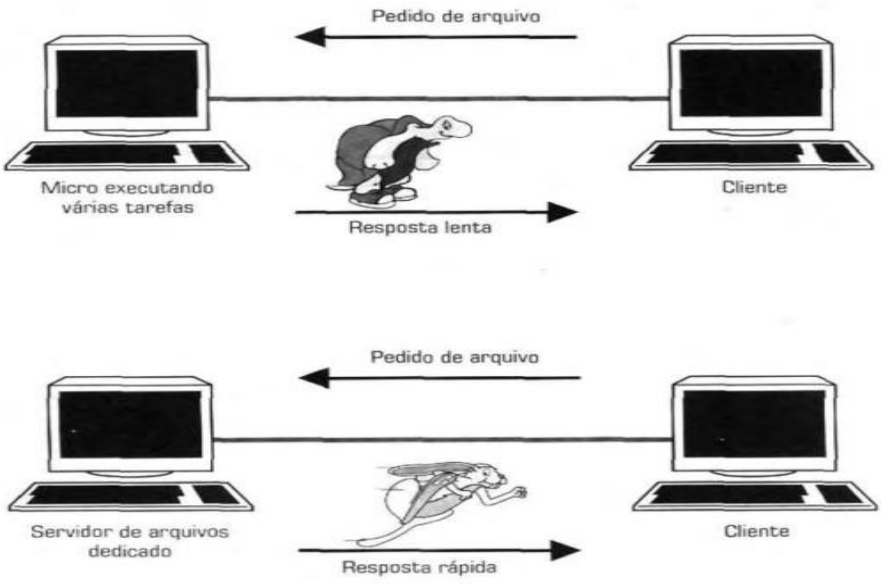


Ilustração 4- Rede ponto-a-ponto e cliente/servidor

A figura mostra uma comparação entre um pedido de um arquivo feito em rede ponto-a-ponto e em uma rede cliente/servidor, ou seja, um servidor dedicado oferece melhor desempenho para executar uma determinada tarefa porque, além de ser especializado na tarefa em questão, normalmente não executa outras tarefas ao mesmo tempo.

2.3.2.1. Tipos de servidores

Servidor de Arquivos: É um servidor responsável pelo armazenamento de arquivos de dados, como arquivos de texto, planilhas e gráficos que necessitam ser compartilhados com os usuários da rede. Note que o programa necessário para ler o arquivo (Processador de texto, por exemplo) é instalado e executado na máquina do usuário (Cliente) e não no servidor.

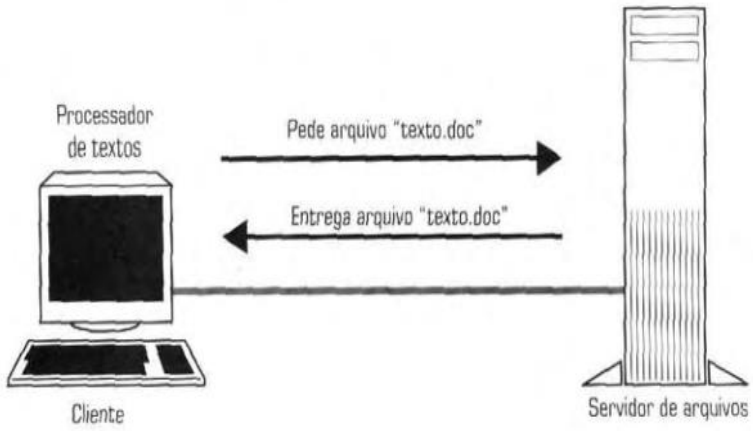


Ilustração 5-Servidor de Arquivos

Servidor de impressão: É um servidor responsável por processar os pedidos de impressão solicitados pelos micros da rede e enviá-los para as impressoras disponíveis.

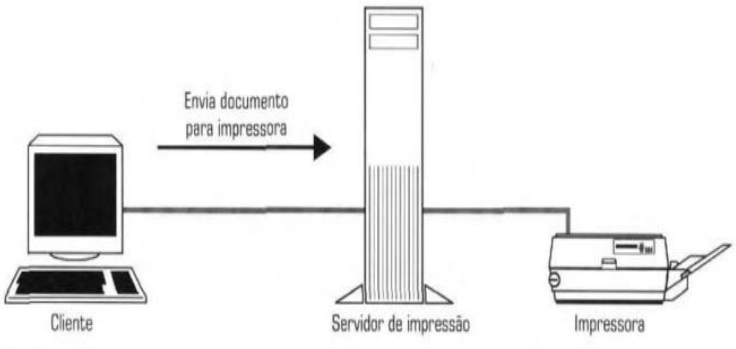


Ilustração 6- Servidor de impressão

Servidor de Aplicação: O servidor de aplicação é responsável por executar aplicações cliente/servidor, como por exemplo, um banco de dados. Ao contrário do servidor de arquivos, que somente armazena arquivos de dados e não os processa, o servidor de aplicação executa as aplicações e processa os arquivos de dados. Quando um micro faz

uma consulta em um banco de dados cliente/servidor, essa consulta será processada no servidor de aplicações e não no micro cliente, o micro cliente apenas mostrará o resultado enviado pelo servidor de aplicações. Com isso é possível que vários usuários acessem e manipulem ao mesmo tempo uma única aplicação, fazendo com que todos os dados fiquem sincronizados.

Ilustração 7- Servidor de Aplicação

Servidor de Correio Electrónico: Responsável pelo processamento e pela entrega de mensagens electrónicas. Se for um e-mail destinado a uma pessoa fora da rede, este será ao servidor de comunicação.

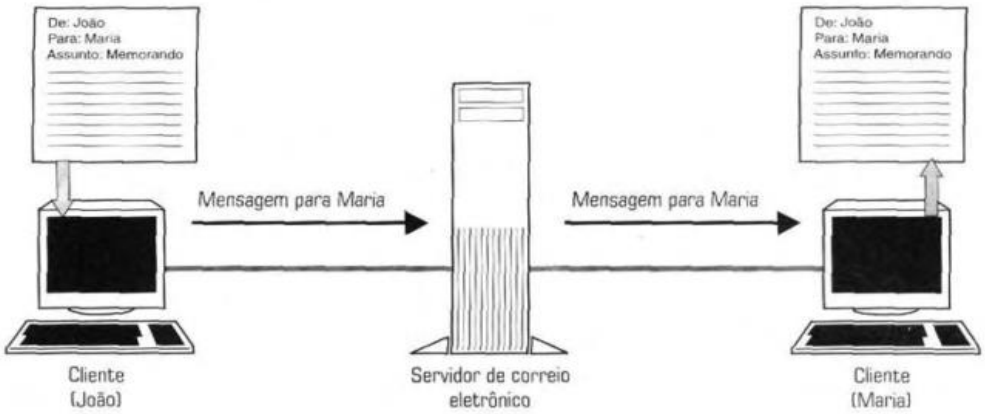


Ilustração 8- Servidor de Correio Electrónico

Servidor de Comunicação: Usado na comunicação entre a sua rede e outras redes, como a internet. Por exemplo, se você acessa a internet de uma linha telefônica convencional, o servidor de comunicação pode ser um micro com uma placa de modem que disca automaticamente para o provedor assim que alguém tenta cessar a internet.

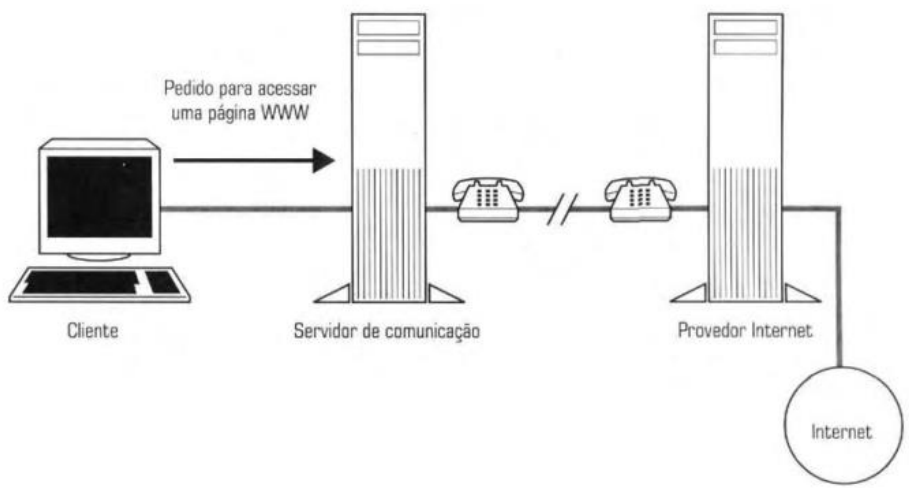


Ilustração 9- Servidor de Comunicação

Para além desses aqui abordados existem outros servidores que auxiliam as redes de computador a melhorar o seu desempenho, lembrar que a escolha de um em detrimento do outro depende da necessidade da rede.

Características:

- Usado normalmente em redes com mais de 10 micros ou redes pequenas que necessitam de um alto grau de segurança.
- Custo maior que o de redes ponto-a-ponto
- Maior desempenho do que redes ponto-a-ponto
- Implementação necessita de especialistas
- Alta segurança
- A manutenção e configuração da rede são feitas de maneira centralizada, pelo administrador da rede.
- Existência de servidores, que são micros ou equipamentos capazes de oferecer recursos aos demais micros da rede, como impressão, armazenamento de arquivos e envio de mensagens electrónicas.
- Possibilidade de uso de aplicações cliente/Servidor, como banco de dados.

2.4. Conceitos importantes

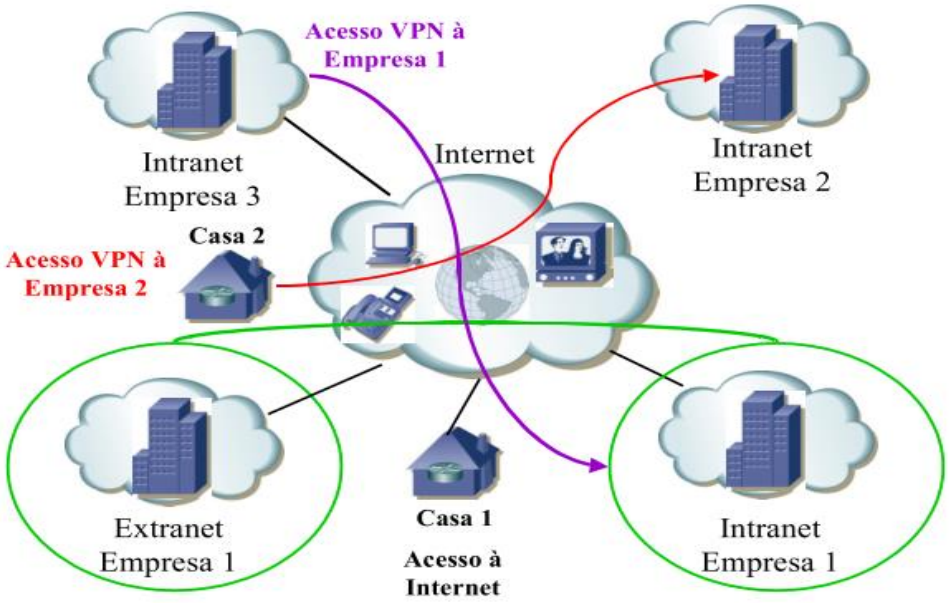


Ilustração 10- Conceitos gerais de Redes

2.4.1. Internet

É o conjunto de redes de computadores interligadas pelo mundo inteiro. Utiliza a arquitectura TCP/IP, e disponibiliza o acesso a serviços, permite a comunicação e troca de informação aos usuários do planeta.

2.4.2. Intranet

É a rede de computadores de uma determinada organização, baseada na arquitetura TCP/IP. Fornece serviços aos empregados, e permite a comunicação entre os mesmos e, de forma controlada, ao ambiente externo (à Internet). Também é conhecida como Rede Corporativa.

2.4.3. Extranet

É um conceito que permite o acesso, de funcionários e fornecedores de uma organização, aos recursos disponibilizados pela Intranet. Podemos dizer que é uma extensão da Intranet. Dessa maneira, podemos disponibilizar um padrão unificado entre as diversas empresas filiais do grupo.

2.4.4. VPN (Rede Privada Virtual)

VPN é uma rede virtual estabelecida entre dois ou mais pontos, que oferece um serviço que permite o acesso remoto, de funcionários ou fornecedores a uma determinada rede, a fim de executarem suas tarefas. Muito utilizada por funcionários, para terem acesso aos e-mails corporativos via Intranet, ou para as equipes de suporte técnico solucionarem problemas em seus sistemas de maneira remota.

2.5. Segurança em Redes

2.5.1. Redes confiáveis características:

Tolerância as falhas

Capacidade em manter a rede a funcionar mesmo quando aparece uma falha. Essa característica é implementada através da redundância de links e equipamentos.

Escalabilidade

Capacidade das redes em crescer face a necessidade organizacional sem afecto o rendimento da mesma e sem alterar por completo a sua topologia.

Qualidade de Serviço (QoS)

Capacidade em oferecer recursos ou serviços de qualidade de acordo com as exigências e necessidades actuais de comunicação. Ex: VOIP (serviço de voz IP), CCTV (vídeo vigilância por IP) e outros.

Segurança

Capacidade em manter a rede funcional e sem comprometimento dos seus dados e recursos a quando do surgimento de uma ameaça. A segurança pode ser: Física e lógica.

2.5.2. Tipos de Ameaças

Seja com ou sem fio, as redes de computadores são essenciais às actividades diárias. Pessoas e empresas dependem igualmente de seus computadores e redes. A intrusão por uma pessoa não autorizada pode resultar em custosas interrupções da rede e perda de trabalhos. Ataques a uma rede podem ser devastadores e resultar em perda de tempo e dinheiro, devido a danos ou roubo de informações e recursos importantes.

Invasores podem obter acesso a uma rede por meio de vulnerabilidades de softwares, ataques de hardware ou adivinhando o nome de usuário e senha de alguém. Os intrusos que obtêm acesso ao modificar o software ou ao explorar as vulnerabilidades do software são frequentemente chamados de hackers.

2.5.2.1. Ameaças Física

Uma vulnerabilidade igualmente importante é a segurança física dos dispositivos. Um invasor pode negar o uso de recursos da rede, se esses recursos estiverem fisicamente comprometidos.

As quatro classes de ameaças físicas são:

- **Ameaças ao hardware** - danos físicos aos servidores, roteadores, switches, cabeamento e estações de trabalho.
- **Danos ambientais** - extremos de temperatura (muito quente ou muito frio) ou extremos de umidade (muito úmido ou muito seco)
- **Ameaças elétricas** - picos de tensão, tensão de alimentação insuficiente (quedas de energia), energia não condicionada (ruído) e perda total de energia
- **Ameaças à manutenção** - manipulação inadequada de componentes eléctricos principais (descarga electrostática), falta de peças sobressalentes essenciais, cabeamento inadequado e identificação deficiente

2.5.2.2. Ameaças Lógicas (Malwares)

Malware ou código mal-intencionado (malcode) é uma abreviatura para software mal-intencionado. É um código ou software que é especificamente projetado para danificar, corromper, roubar ou causar ações "más" ou ilegítimas em dados, hosts ou redes. Vírus, worms e cavalos de Tróia são tipos de malware.

Vírus

Um vírus de computador é um tipo de malware que se propaga inserindo uma cópia de si mesmo dentro de outro programa e se tornando parte dele. Ele se dissemina de um computador para outro, deixando infecções por onde passa. A severidade dos vírus pode variar desde efeitos que causam pequenas perturbações até danos aos dados e software e condições de DoS (negação de serviço). Quase todos os vírus estão anexados a um arquivo executável, o que significa que o vírus pode existir em um sistema, mas não estar activo ou ser capaz de se disseminar até que o usuário execute ou abra o arquivo ou o programa hospedeiro mal-intencionado. Quando o código hospedeiro é executado, o código viral é executado também. Normalmente, o programa hospedeiro continua funcionando depois de ser infectado pelo vírus. No entanto, alguns vírus sobrescrevem outros programas com cópias deles mesmos, o que destrói todo o programa hospedeiro. Os vírus se disseminam quando o software ou documento ao qual estão anexados é transferido de um computador para outro, usando a rede, um disco, compartilhamento de arquivos ou anexos de e-mail infectados.

Worms

Os worms de computador são similares aos vírus na reprodução de cópias funcionais de si mesmos e podem causar o mesmo tipo de dano. Ao contrário dos vírus, que necessitam que um arquivo infectado se espalhe, worms são softwares independentes e não necessitam de um programa hospedeiro ou ajuda humana para se propagarem. Um worm não precisa estar anexado a um programa para infectar um hospedeiro e entrar em um computador usando uma vulnerabilidade no sistema. Os worms utilizam os recursos do sistema para viajar pela rede sem ajuda.

Cavalos de Tróia

Um cavalo de Troia é outro tipo de malware que recebeu o nome do cavalo de madeira usado pelos gregos para invadirem Troia. É uma parte perigosa do software que parece legítima. Os usuários são, em geral, enganados carregando e executando-os em seus sistemas. Após ser activado, ele pode realizar um grande número de ataques a um host, desde os que irritam o usuário (janelas pop-up ou alterações na área de trabalho) até danos no host (exclusão de arquivos, roubo de dados ou activação e disseminação de outro malware, como vírus). Cavalos de Tróia também são conhecidos por criarem portas dos fundos (back doors) que permitem o acesso de usuários mal-intencionados ao sistema.

Diferente dos vírus e worms, os Cavalos de Tróia não se reproduzem infectando outros arquivos, tampouco se auto-reproduzem. Cavalos de Tróia se disseminam por meio da acção do usuário, quando o mesmo abre o anexo de um e-mail ou faz download e executa um arquivo da Internet, por exemplo.

3. Dispositivos de Rede

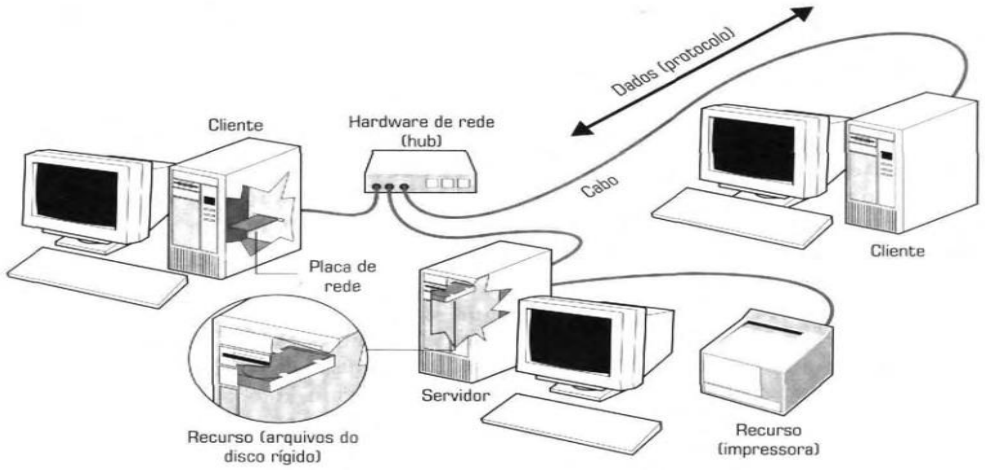


Ilustração 11- Dispositivos de rede

Servidor: È um micro ou dispositivo capaz de oferecer recursos para a rede. Em redes ponto-a-ponto não há a figura do servidor dedicado, nesse tipo de rede os micros ora funcionam como servidores, ora como clientes.

Cliente: É um micro ou dispositivo que acessa os recursos oferecidos pela rede.

Recurso: Qualquer coisa que possa ser oferecida e usada pelos clientes da rede, como impressores, arquivos, unidades de disco, acesso a internet, etc.

Protocolo: Para que todos os dispositivos de uma rede possam se entender independentemente do programa usado ou do fabricante dos componentes, eles precisam conversar usando uma mesma linguagem. Essa linguagem é genericamente chamada protocolo. Dessa forma, os dados de uma rede são trocados de acordo com um protocolo, como, por exemplo o TCP e o IP.

Cabeamento: Os cabos da rede transmitem os dados que serão trocados entre os diversos dispositivos que compõem uma rede.

Placa de Rede: A placa de rede, também chamada NIC (Network interface Card), permite que PCs consigam ser conectados em rede, já que internamente os PCs usam um sistema de comunicação totalmente diferente do utilizado em redes.

Hardware de Rede: São dispositivos intermédios usados na construção de uma rede de computadores, entre eles podemos encontrar:

3.1. Firewalls

Um firewall é uma das ferramentas de segurança disponíveis mais eficazes na protecção dos usuários contra ameaças externas. Os firewalls de rede estão localizados entre duas ou mais redes, e controlam o tráfego entre elas, além de ajudar a evitar o acesso não autorizado. Firewalls baseados em hosts ou firewalls pessoais são instalados nos sistemas finais. Produtos de firewall usam várias técnicas para determinar a permissão ou negação do acesso à rede. Essas técnicas são:

- **Filtragem de pacotes** - Impede ou permite o acesso com base em endereços IP ou MAC.

- **Filtragem de aplicações** - Impede ou permite o acesso de determinados tipos de aplicação com base nos números das portas.

- **Filtragem de URL** - Impede ou permite o acesso a sites com base em URLs específicas ou palavras-chave.

3.2. Repetidor (Repeater)

Os repetidores são dispositivos usados para estender as redes locais além dos limites especificados para o meio físico utilizado nos segmentos. Operam na camada 1 (Física) do modelo OSI e copiam bits de um segmento para outro, regenerando os seus sinais eléctricos.

Ilustração 12- Repetidor

3.3. Concentrador (Hub)

Os Hubs são os dispositivos actualmente usados na camada 1 (Física) e substituem os repetidores.

São repetidores com múltiplas portas.

Ilustração 13- HUB

3.4. Ponte (Bridge)

São dispositivos que operam na camada 2 (Enlace) do modelo OSI e servem para conectar duas ou mais redes formando uma única rede lógica e de forma transparente aos dispositivos da rede.

As redes originais passam a ser referenciadas por segmentos. As bridges foram criadas para resolver problemas de desempenho das redes. Elas resolveram os problemas de congestionamento nas redes de duas maneiras:

- Reduzindo o número de colisões na rede, com o domínio de colisão.
- Adicionando banda à rede.

Como as bridges operam na camada de enlace, elas "enxergam" a rede apenas em termos de endereços de dispositivos (MAC Address). As bridges são transparentes para os protocolos de nível superior. Isso significa que elas transmitem os "pacotes" de protocolos superiores sem transformá-los.

As bridges são dispositivos que utilizam a técnica de store-and-forward (armazena e envia). Ela armazena o quadro (frame) em sua memória, compara o endereço de destino em sua lista interna e direcciona o quadro (frame) para uma de suas portas.

Se o endereço de destino não consta em sua lista o quadro (frame) é enviado para todas as portas, excepto a que originou o quadro (frame), isto é o que chamamos de flooding.

Ilustração 14- Ponte (Bridge)

3.5. Comutador (Switch)

Os switches também operam na camada 2 (Enlace) do modelo OSI e executa as mesmas funções das bridges, com algumas melhorias.

Os switches possuem um número mais elevado de portas.

Ilustração 15- Comutador (Switch)

3.5.1. Princípio de Funcionamento

Os switches usam endereços MAC para direccionar as comunicações de rede para a porta apropriada em direcção ao destino. Um switch é composto de circuitos integrados e de um software que controla os caminhos dos dados através do switch. Para que um switch saiba qual porta usar para transmitir um quadro, primeiro ele deve saber quais dispositivos existem nas portas. À medida que aprende a relação das portas com os dispositivos, o switch cria uma tabela denominada tabela de endereços MAC ou tabela de memória endereçável de conteúdo (CAM). A CAM é um tipo especial de memória usado em aplicativos de pesquisa em alta velocidade.

Os switches determinam como lidar com quadros de dados de entrada mantendo a tabela de endereços MAC. Um switch cria sua tabela de endereços MAC gravando o endereço MAC de cada dispositivo conectado a cada uma de suas portas. O switch usa as informações da tabela de endereços MAC para enviar quadros destinados a um dispositivo específico para a porta atribuída a esse dispositivo.

O processo de duas etapas a seguir é executado em todos os quadros Ethernet que entram em um switch.

Passo 1. Aprendizagem – Exame do Endereço MAC de Origem

Todo quadro que entra em um switch é verificado quanto ao aprendizado de novas informações. Isso é feito examinando o endereço MAC de origem e o número da porta em que o quadro entrou no switch:

- Se o endereço MAC de origem não existe, é adicionado à tabela juntamente com o número da porta de entrada.

- Se o endereço MAC de origem existe, o switch actualiza o timer (temporizador) de actualização dessa entrada. Por padrão, a maioria dos switches Ethernet mantém uma entrada na tabela por cinco minutos.

Observação: se o endereço MAC de origem existe na tabela, mas em outra porta, o switch trata como uma nova entrada. A entrada é substituída usando o mesmo endereço MAC, mas com o número de porta mais actual.

Passo 2. Encaminhamento – Exame do Endereço MAC de Destino

Se o endereço MAC for um endereço unicast, o switch procurará uma correspondência entre o endereço MAC de destino do quadro e uma entrada na respectiva tabela de endereços MAC:

- Se o endereço MAC de destino estiver na tabela, ele encaminhará o quadro pela porta especificada.
- Se o endereço MAC de destino não estiver na tabela, o switch encaminhará o quadro por todas as portas, exceto a de entrada, de modos a descobrir a Porta de destino e mapear na tabela CAM com o endereço MAC (usando o protocolo ARP). Isso é chamado de unicast desconhecido.

Observação: se o endereço MAC de destino for um endereço de broadcast ou multicast, o quadro será enviado por todas as portas, excepto a de entrada.

3.5.2. Os Modos de envio de quadro de um switch

Os modos de envio de quadro ou frame utilizados por um switch são:

- Store-and-forward
- Cut-through
- Fragment Free

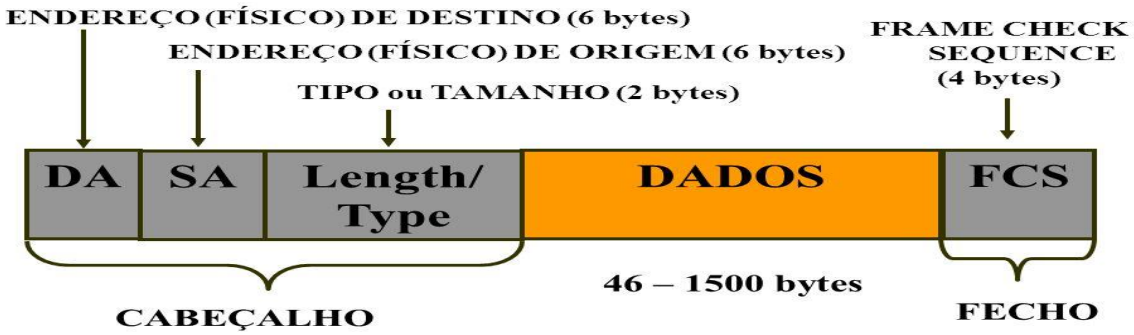
Store-and-forward todo quadro é armazenado e é analisada a integridade do dado, se correto é realizada a consulta à tabela de endereços MAC (MAC address table) para determinar a porta de destino. No caso de erro, o quadro é descartado.

Cut-through a consulta à tabela é iniciada no recebimento do quadro e o envio é imediato. O que pode causar o envio de quadros com erros, e retransmissões pela camada de transporte.

Fragment-free os primeiros 64 bytes são lidos (incluindo o cabeçalho do quadro) e a comutação se inicia antes que sejam lidos todo o campo de dados e o checksum. Este modo verifica a maioria dos erros e possui baixa latência.

3.5.3. Quadro Ethernet (Frame)

- O quadro (frame) é a menor estrutura de informação transmitida através de uma rede local.



3.6. Roteador (Router)

O Roteador é o equipamento que opera na camada 3 (Rede) do modelo OSI, e permite a conexão entre redes locais ou entre redes locais e de longa distância.

Suas principais características são:

- Filtram e encaminham pacotes;
- Determinam rotas;
- Segmentam pacotes;
- Realizam a notificação à origem.

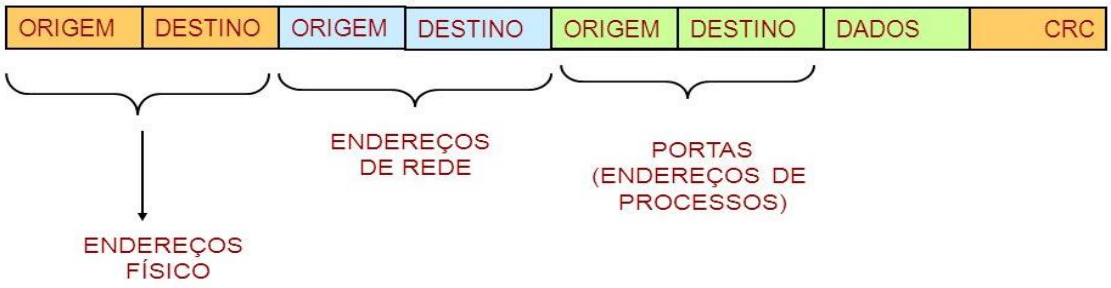
Quanto a sua forma de operação, as rotas são determinadas a partir do endereço de rede da estação de destino e da consulta às tabelas de roteamento.

Essas tabelas são actualizadas utilizando-se informações de roteamento e por meio de algoritmos de roteamento.

Tais informações são transmitidas por meio de um protocolo de roteamento (RIP, OSPF e EIGRP)

Ilustração 16- Roteador (Router)

3.6.1. Quadro de Pacote



3.7. Modem

Dispositivo electrónico utilizado para a conversão entre sinais analógicos e digitais. A palavra tem como origem as funções de modulação e demodulação. São geralmente utilizados para estabelecer a conexão entre computadores e redes de acesso.

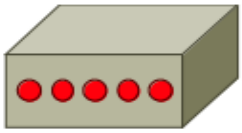


Ilustração 17- Modem

4. Tipo de meios físicos usados para transportar dados pela rede

4.1. Especificações de cabos

Existem várias organizações, grupos empresariais e entidades governamentais que constituem institutos para especificar e regulamentar os tipos de cabos usados em redes.

Podemos citar entre tais organizações internacionais a EIA/TIA (Electronic Industry Association e Telecommunications Industries Association), o IEEE (Institute of Electrical and Electronic Engineers), a UL (Underwriters Laboratories), ISO/IEC (International Standards Organization / International Electrotechnical Commission). Além de criar os códigos e gerar as especificações dos materiais utilizados no cabeamento, também definem os padrões de instalação.

4.2. Cabo coaxial

O cabo coaxial tem melhor blindagem que os cabos de par trançado, com isso pode se estender por distâncias maiores em velocidades mais altas. Dois tipos de cabo coaxial são muito usados:

- Cabo de 50 ohms.
- Cabo de 75 ohms.

O cabo de 50 ohms, é muito utilizado em transmissões digitais, já o cabo de 75 ohms, é usado em transmissões analógicas e, principalmente, em ambientes de televisão.

Um cabo coaxial é formado por um fio de cobre colocado na parte central, envolvido por um material isolante. O isolante é envolvido por uma malha sólida entrelaçada. O condutor externo, que tem a função de diminuir o efeito de ruídos sobre o sinal transmitido, é coberto por uma camada plástica protetora.

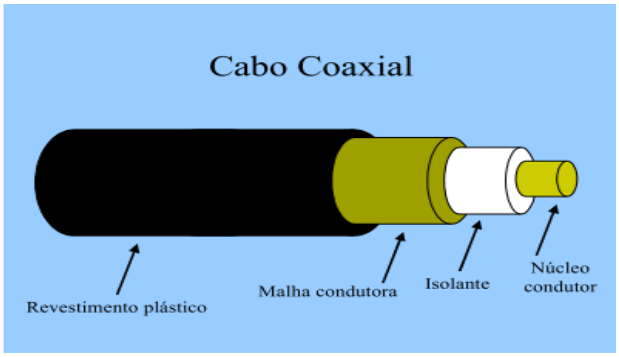


Ilustração 18- Cabo Coaxial

4.3. Cabos de par-trançado (STP e UTP)

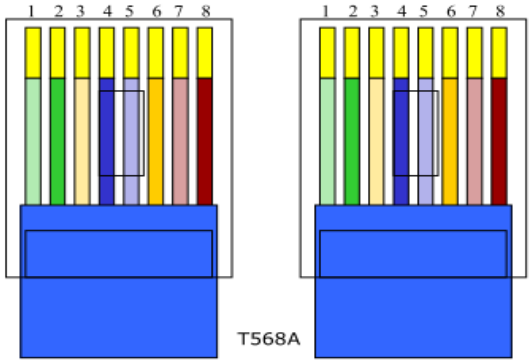
São amplamente utilizados nas redes ethernet. Possuem 8 fios fixados a um conector RJ-45, em cada uma das suas extremidades.

Os pares trançados podem ser utilizados na transmissão de sinais analógicos ou digitais. A largura de banda e a taxa de transmissão dependem da espessura do fio e da distância percorrida mas, em muitos casos, é possível alcançar taxas altas, na ordem de alguns Mbps por alguns quilómetros. Muitas interferências podem ser provocadas se os pares não forem trançados. Devido ao custo e ao desempenho obtidos, os pares trançados são usados em larga escala e é provável que assim permaneçam nos próximos anos.

Denominamos de UTP (Unshielded Twisted Pair) os cabos que não possuem blindagem e STP (Shielded Twisted Pair) os que possuem blindagem.

4.3.1. Cabo Directo (Straight-Through)

O cabo directo possui este nome devido a sua pinagem, interliga o pino 1 de uma extremidade ao pino 1 da outra, e assim sucessivamente. Conforme figura abaixo:



Pinagem:

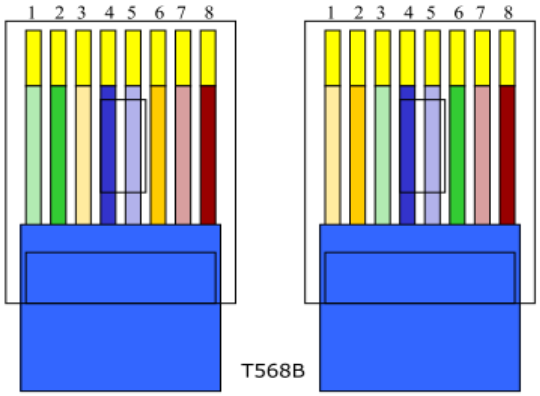
Extremidade A	Extremidade B
Pino 1 – Verde e Branco	Pino 1 – Verde e Branco
Pino 2 – Verde	Pino 2 – Verde
Pino 3 – Laranja e Branco	Pino 3 – Laranja e Branco
Pino 4 – Azul	Pino 4 – Azul
Pino 5 – Azul e Branco	Pino 5 – Azul e Branco
Pino 6 – Laranja	Pino 6 – Laranja
Pino 7 – Marrom e Branco	Pino 7 – Marrom e Branco
Pino 8 – Marrom	Pino 8 – Marrom

Ilustração 19- Cabo UTP Ref. T568A

Ele é utilizado para interligar os seguintes equipamentos:

- Roteador ao Switch ou Hub.
- Computador ao Switch ou Hub.

4.3.2. Cabo Cruzado (Crossover)



Pinagem:

Extremidade A	Extremidade B
Pino 1 – Verde e Branco	Pino 1 – Laranja e Branco
Pino 2 – Verde	Pino 2 – Laranja
Pino 3 – Laranja e Branco	Pino 3 – Verde e Branco
Pino 4 – Azul	Pino 4 – Azul
Pino 5 – Azul e Branco	Pino 5 – Azul e Branco
Pino 6 – Laranja	Pino 6 – Verde
Pino 7 – Marrom e Branco	Pino 7 – Marrom e Branco
Pino 8 – Marrom	Pino 8 – Marrom

Ilustração 20- Cabo UTP Ref. T568B

O cabo Crossover é utilizado para interligar os seguintes equipamentos:

• Roteador ao Roteador.

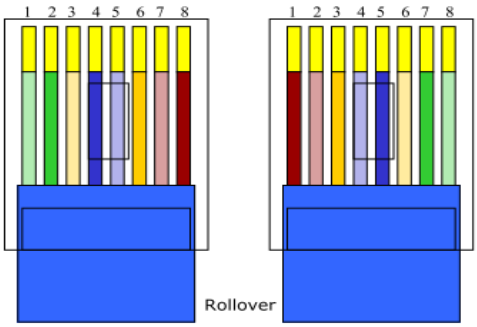
• Computador ao Computador.

• Switch ao Switch.(*)

• Hub ao Hub.(*)

(*) Para esses dispositivos existem, em alguns modelos, a opção de uma porta especial que aceita o cabo directo.

4.3.3. Cabo Rollover



Pinagem:

Extremidade A	Extremidade B
Pino 1 – Verde e Branco	Pino 1 – Marrom
Pino 2 – Verde	Pino 2 – Marrom e Branco
Pino 3 – Laranja e Branco	Pino 3 – Laranja
Pino 4 – Azul	Pino 4 – Azul e Branco
Pino 5 – Azul e Branco	Pino 5 – Azul
Pino 6 – Laranja	Pino 6 – Laranja e Branco
Pino 7 – Marrom e Branco	Pino 7 – Verde
Pino 8 – Marrom	Pino 8 – Verde e Branco

Ilustração 21- Cabo Rollover ou cabo Console

O cabo Rollover é utilizado na porta console dos dispositivos, quando queremos realizar uma configuração ou manutenção local no equipamento (roteadores, switches, computadores, etc.).

Abaixo podemos verificar a divisão dos cabos por categoria e sua aplicação:

Tipo	Aplicação
Categoria 1	Voz (cabo telefônico)
Categoria 2	Dados a 4 Mbps (LocalTalk)
Categoria 3	Transmissão de até 16 MHz. Dados a 10 Mbps (Ethernet)
Categoria 4	Transmissão de até 20 MHz. Dados a 20 Mbps (16 Mbps Token Ring)
Categoria 5	Transmissão de até 100 MHz. Dados a 100 Mbps (Fast Ethernet)
Categoria 6	Utilizado em ISDN, cabos para modem e TV a cabo.
Categoria 7	Ethernet 1000BaseT, ATM com transmissão de até 500MHz.

Ilustração 22- Categorias de Cabos UTP

4.4. Fibra Óptica

Um sistema de transmissão óptica possui 3 componentes fundamentais: o gerador de luz, o meio de transmissão e o receptor. Seu funcionamento consiste na instalação de um gerador de luz em uma das extremidades e o receptor na outra. O gerador, ou fonte, de luz recebe um pulso eléctrico e envia o sinal de luz através do meio de transmissão para o receptor. O receptor, ao entrar em contacto com a luz, emite um pulso eléctrico. Adopta-se por convenção que a presença de luz equivale a um bit 1, e o bit 0 representa a ausência de luz.

As fibras ópticas são constituídas por três camadas: o núcleo, a casca e o revestimento externo. O núcleo e a casca são produzidos a partir do vidro, ou de materiais a base de sílica ou plástico, e possuem diferentes índices de refracção.

A atenuação da luz através do meio depende do comprimento de onda da luz. As principais vantagens da fibra óptica são:

- Baixa atenuação
- Elevada largura de banda
- Imunidade à interferência electromagnética
- Baixo peso
- Pequena dimensão

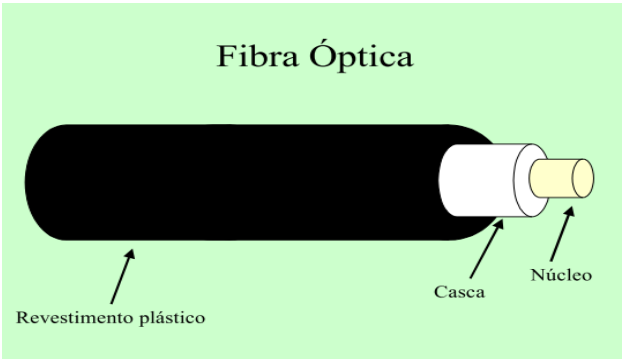


Ilustração 23- Cabo de Fibra óptica

4.4.1. Fibras Multimodo e Monomodo

A diferença está no modo de operação entre elas. A fibra monomodo possui um modo de propagação enquanto as multimodos podem ter vários modos de propagação.

Entre as fibras multimodo a diferença está na composição do material e os respectivos índices de refracção. Enquanto na gradual temos uma variação gradativa no índice de refracção, devido a várias camadas de materiais, na fibra de índice degrau temos uma única composição de forma que temos um índice de refracção constante.

4.4.2. Atenuação

Chamamos de atenuação a perda da potência de um sinal luminoso em uma fibra óptica. Sua unidade de medida é em decibéis por quilómetro (dB/km).

Essa perda depende do comprimento de onda da luz e do material usado e ocorre por causa da limitação de distância entre a origem e o término da transmissão. Os principais factores que geram a atenuação são: a absorção, o espalhamento e a curvatura.

5. Modelo OSI e TCP/IP

Conforme vimos no início da apostila, a arquitetura TCP/IP (Transmission Control Protocol /Internet Protocol) é nasceu da pesquisa financiada pela Agência de Defesa dos Estados Unidos, DARPA (Defense Advanced Research Projects Agency), e evoluiu muito com o desenvolvimento do sistema operacional UNIX.

A Internet expandiu devido aos fatos do protocolo TCP/IP não ser proprietário e ser de fácil implementação.

As regras de implementação da arquitectura TCP/IP são normalizadas pelas RFCs (Requests for Comments).

A tendência é evoluir ainda mais, provendo serviços cada vez mais interactivos.

5.1. Camada de Aplicação

A camada de Aplicação tem a função de prover uma interface entre os programas de usuários (aplicativos) e as redes de comunicação de dados

A camada de Aplicação é equivalente às camadas 5, 6 e 7 do Modelo OSI. Os protocolos mais conhecidos são:

● HTTP – HyperText Transfer Protocol - protocolo responsável pela comunicação via páginas WWW (World Wide Web) ou, simplesmente, Web. Por um programa navegador (browser), usando o protocolo HTTP, um usuário pode acessar informações contidas em um servidor Web.

● FTP – File Transfer Protocol – protocolo responsável pela transferência de arquivos entre computadores.

● Telnet – Terminal de acesso remoto – protocolo que permite o acesso a um equipamento distante. Permite que possamos dar comando e rodar aplicações remotamente.

● DNS – Domain Name System – aplicação responsável pela tradução de endereços IP em nomes e vice-versa.

● SMTP – Simple Mail Transfer Protocol – protocolo responsável pelo armazenamento e envio de e-mails (Eletronic Mail - Correio Electrónico).

5.2. Camada de Transporte

A principal função da camada de transporte é prover uma comunicação fim-a-fim entre as aplicações de origem e destino, de forma transparente para as camadas adjacentes.

O nome dado à PDU (Protocol Data Unit) desta camada é segmento. Ela é equivalente à camada 4 do Modelo OSI. Seus dois principais protocolos são o TCP e o UDP.

O TCP (Transmission Control Protocol) é um protocolo orientado a conexão. Fornece um serviço confiável, com garantia de entrega dos dados.

O UDP (User Datagram Protocol) é um protocolo não orientado a conexão. Fornece um serviço, não confiável, sem garantia de entrega dos dados. Um datagrama pode se perder, sofrer atrasos, ser duplicado ou ser entregue fora de sequência. Não executa nenhum mecanismo de controlo e nem envia mensagens de erro.

5.3. Camada Internet

A função da camada Internet é prover a conectividade lógica realizando a comutação de pacotes, ou roteamento, de forma a encontrar o melhor caminho para a transmitir pacotes através da rede.

Como vimos, a camada Internet, pode ser chamada de Rede ou Internetwork, é equivalente a camada 3, de Rede, do Modelo OSI.

Os protocolos principais desta camada são:

● IP (Internet Protocol): O protocolo IP é um protocolo não orientado à conexão, ele é transmitido pela rede pelos roteadores, que decidem o melhor caminho analisando a sua tabela de roteamento.

● ICMP (Internet Control Message Protocol) (popular ping)

● ARP (Address Resolution Protocol)

● RARP (Reverse Address Resolution Protocol)

5.4. Camada de Acesso à Rede

A função da camada Acesso à Rede é prover uma interface entre a camada Internet e os elementos físicos da rede. A camada inferior da arquitectura TCP/IP tem as funcionalidades referentes às camadas 1 e 2 do Modelo OSI.

5.5. Comparação do modelo OSI com o modelo TCP/IP

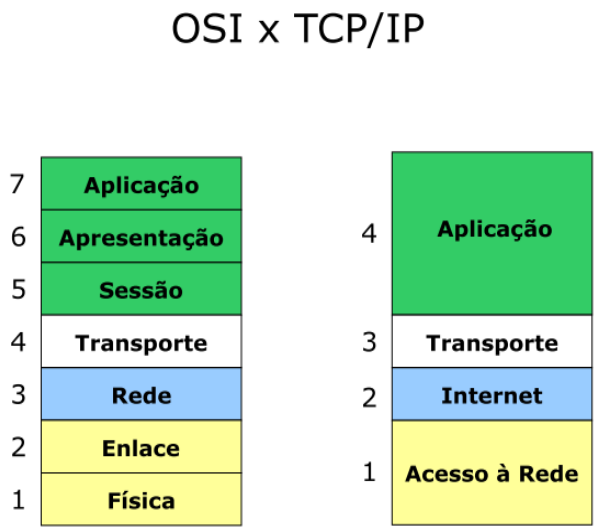


Ilustração 24- Modelo OSI/ TCP

Principais pontos de comparação:

- OSI é um modelo de referência, TCP/IP é uma arquitectura de implementação
- Ambos são divididos em camadas.
- As camadas de Transporte são equivalentes.
- A camada de Rede do Modelo OSI equivalente à camada Internet do TCP/IP.
- As camadas de Aplicação, Apresentação e Sessão do Modelo OSI são equivalentes à camada de Aplicação do TCP/IP.
- As camadas de Enlace e Física do Modelo OSI são equivalentes à camada Acesso à Rede do TCP/IP.

6. Endereçamento de Rede

6.1. Endereçamento IP

O endereçamento IP é o endereço lógico da arquitectura TCP/IP, e amplamente utilizado na Internet. Cada host da Internet possui, pelo menos, um endereço IP.

Actualmente, a grande maioria das redes que compõem a Internet utilizam a versão 4 do protocolo IP (IPv4), porém devido a limitação dos endereços utilizados nesta versão foi desenvolvida a versão 6 (IPv6) que, entre outras vantagens, resolve este problema.

6.1.1. Endereçamento IPv4

O endereço IP, na versão 4, é formado por 32 bits, divididos em 4 blocos de 8 bits, representados no sistema decimal (0- 255).

0-255.0-255.0-255.0-255

Exemplo: 10.235.18.129, 172.29.2 44.5 e 200.20 7.10.188.

O endereço IP é constituído por dois componentes: a identificação da rede (netid) e a identificação do host dentro da rede (hostid).

6.1.1.1. Endereços IP classes A, B, C, D e E

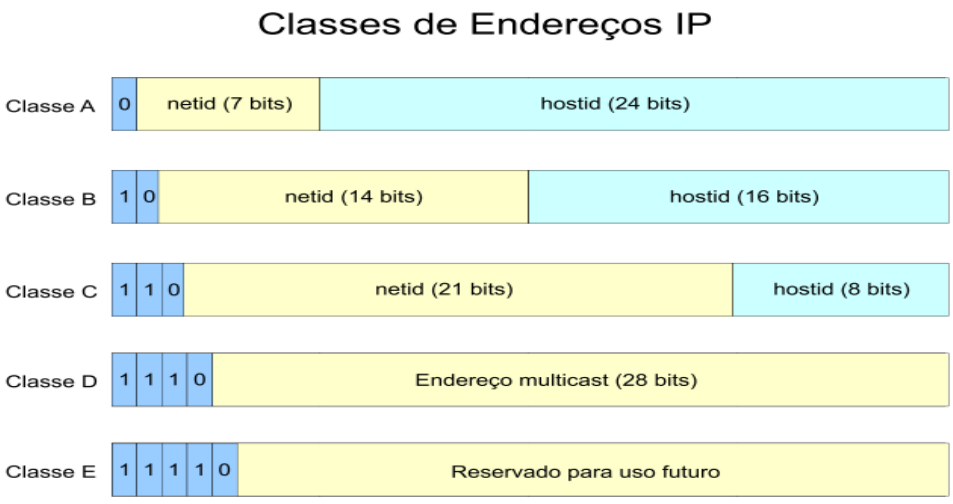


Ilustração 25- Classes de Endereço IPV4

Faixa de Endereços:

Classe	Início da faixa de endereços	Término da faixa de endereços
A	1.0.0.0 (00000001.00000000.00000000.00000000)	126.0.0.0* (01111110.00000000.00000000.00000000)
B	128.0.0.0 (10000000.00000000.00000000.00000000)	191.255.0.0 (10111111.11111111.00000000.00000000)
C	192.0.0.0 (11000000.00000000.00000000.00000000)	223.255.255.0 (11011111.11111111.11111111.00000000)
D	224.0.0.0 (11100000.00000000.00000000.00000000)	239.255.255.255 (11101111.11111111.11111111.11111111)
E	240.0.0.0 (11110000.00000000.00000000.00000000)	255.255.255.255 (11111111.11111111.11111111.11111111)

O endereço 127.0.0.0 é reservado

Classe A: é destinada uma faixa de endereços para empresas com um grande número de hosts, onde o primeiro octeto representa a parte da rede e os demais octetos representam a parte do host. O primeiro bit de um endereço classe A deve ser 0.

Classe B: é destinada uma faixa de endereços para empresas com número intermediário de hosts, onde os dois primeiros octetos representam a parte da rede e os dois últimos octetos representam a parte do host. Os primeiros dois bits de um endereço classe B devem ser 10.

Classe C: é destinada uma faixa de endereços para empresas com um número pequeno de hosts, onde os três primeiros octetos representam a parte da rede e o último octeto representa a parte do host. Os primeiros três bits de um endereço classe C devem ser 110.

Classe D: é a faixa destinada ao serviço de multicast, onde o endereço de rede direcciona os pacotes de destino para grupos específicos.

Classe E: a IETF reserva os endereços dessa faixa para pesquisas.

Comparação do número de redes e hosts das classes A, B e C.

Classe	Número de bits para redes	Número de redes reais disponíveis nas classes	Número de bits para hosts	Número de hosts por rede
A	7	$2^7 - 2 = 126$	24	$2^{24} - 2 = 16.777.214$
B	14	$2^{14} = 16.384$	16	$2^{16} - 2 = 65.534$
C	21	$2^{21} = 2.097.152$	8	$2^8 - 2 = 254$

6.1.1.2. Endereços IP reservados

Existem endereços reservados que não podem ser utilizados em nenhum host ou dispositivo de rede.

Para cada bloco de endereços IP, são reservados o primeiro endereço (Endereço da rede) e o último (endereço de broadcast).

- O endereço 127.0.0.1 é o endereço de localhost (endereço da própria máquina).
- O endereço 0.0.0.0 não é usado.

6.1.1.3. Endereços IP públicos e privados

Os endereços IPs utilizados na Internet são denominados públicos ou válidos e são administrados por determinadas entidades. O controlo central cabe ao IANA, já o bloco de endereços destinados a Angola é controlado pela Angola Telecom e seus colaboradores.

Existem alguns blocos de endereçamento que foram reservados para utilização dentro de redes privadas, muito usados em Intranets ou redes de gerenciamento. A esses blocos damos o nome de endereços privados ou inválidos. São eles:

Endereços Privados

Classe	Início da faixa	Término da faixa
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

Os Endereços IP Privados auxiliam no contorno do problema de escassez de IPs, pois as redes privadas não conectadas directamente à Internet podem usar qualquer endereço. E para obter o acesso à Internet usamos a técnica de NAT (Network Address Translation) para converter endereços privados em públicos.

6.2. Noções de IPv6

O IPv6 foi desenvolvido principalmente para equacionar o problema da escassez de endereçamento IP. Possui 128 bits, formado por oito blocos de 16 bits, sendo representados por quatro dígitos hexadecimais.

8.2.9. Comparação entre IPv4 e IPv6

Característica	IPv4	IPv6
Tamanho do endereço	32 bits (4 octetos)	128 bits (16 octetos)
Exemplo de endereço IP	10.1.2.3	0000:0000:0000:0000:FFFF:FFFF:0A01:0203
Abreviação	-	::FFFF:FFFF:0A01:0203
Número de endereços	2^{32}	2^{128}

6.3. Endereço MAC (Media Access Control)

Endereço único para representação de todas as máquinas ligadas a rede, é um endereço associado a placa de redes e permite com que o dispositivo possa ser associado a uma rede.

Composto por 48 bits de comprimento, sendo expresso por 12 digitos hexadecimais agrupados em dois (2), refazendo um total de 6 grupos.

EX: 00-60-2F-3A-07-BC e 00-60-2F-3A-07-BC

Tipos de Endereço MAC

MAC Unicast: Representação específica, ou seja, representa uma única máquina.

MAC Broadcast: Usado para direccional todas as redes em mesmo domínio de broadcast, ou seja, na mesma rede. Representação: FF-FF-FF-FF-FF-FF.

MAC Multicast: Destina-se a representar um grupo na rede, é um endereço especial que começa com 01-00-5E em hexadecimal.

6.4. Obtenção de um endereço IP

6.4.1. Atribuição estática do endereço IP

Podemos atribuir manualmente um endereço IP a um host. Vários tipos de equipamentos suportam esta configuração, a diferença está na forma de executar a entrada dos dados.

Alguns sistemas operacionais permitem a configuração gráfica e outros através de linha de comando.

Normalmente, os parâmetros mais comuns a serem configurados são:

- Endereço IP
- Máscara
- Default Gateway
- Servidor de DNS

Para o sistema operacional Windows temos:

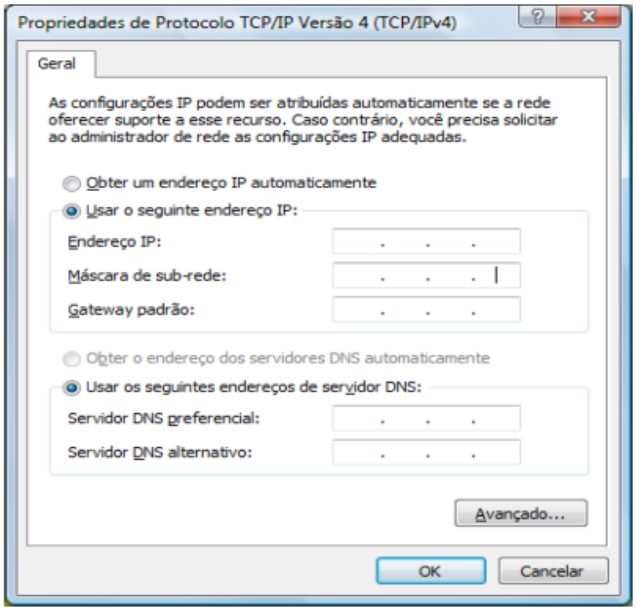


Ilustração 26- Atribuição de endereço IP no PC

6.4.2. Atribuição de Endereços IP com uso de DHCP Automaticamente

O protocolo DHCP (Dynamic Host Configuration Protocol) é utilizado para prover as configurações básicas de endereçamento IP e proporcionar o controlo da utilização dos endereços.

Facilita a configuração das estações de trabalho, principalmente em redes com grande número de hosts.

6.4.2.1. Princípio de funcionamento DHCP

Quando o cliente inicializa (ou quer ingressar em uma rede), ele começa um processo de quatro etapas para obter um aluguel de endereço. Um cliente inicia o processo com uma mensagem de broadcast DHCPDISCOVER com seu próprio endereço MAC para descobrir os servidores DHCPv4 disponíveis.

Descoberta do DHCP (DHCPDISCOVER)

A mensagem de broadcast DHCPDISCOVER encontra os servidores DHCPv4 na rede. Como o cliente não tem informações válidas de IPv4 durante a inicialização, ele usa endereços de broadcast de Camada 2 e Camada 3 para se comunicar com o servidor.

Pacote de DHCP Offer (DHCPOFFER)

Quando o servidor DHCPv4 recebe uma mensagem DHCPDISCOVER, reserva o endereço IPv4 disponível para alugar para o cliente. O servidor também cria uma entrada ARP que consiste no endereço MAC do cliente solicitante e o endereço IPv4 alugado do cliente. O servidor DHCPv4 envia mensagem de vinculação DHCPOFFER ao cliente solicitante a mensagem de DHCPOFFER é enviada como unicast, usando o endereço MAC de Camada 2 do servidor como o endereço origem e o endereço MAC de Camada 2 do cliente como destino.

Solicitação de DHCP (DHCPREQUEST)

Quando o cliente receber o DHCPOFFER do servidor, enviará uma mensagem DHCPREQUEST. Esta mensagem é usada para geração e renovação do aluguel. Quando usado para geração de aluguel, DHCPREQUEST actua como um aviso de aceitação de vinculação para o servidor seleccionado para os parâmetros que oferecia e

uma recusa implícita a todos os outros servidores que possam ter fornecido ao cliente uma oferta de vinculação.

Muitas redes corporativas usam vários servidores DHCPv4. A mensagem DHCPREQUEST é enviada na forma de um broadcast para informar esse servidor DHCPv4 e todos os outros servidores DHCPv4 sobre a oferta aceita.

Reconhecimento de DHCP (DHCPACK)

Ao receber a mensagem DHCPREQUEST, o servidor verifica as informações de aluguel com um ping do ICMP para esse endereço para garantir que ele não esteja sendo usado actualmente, cria uma nova entrada ARP para o aluguel do cliente e envia uma mensagem unicast DHCPACK. A mensagem DHCPACK é uma cópia de DHCPOFFER, excepto por uma mudança no campo do tipo de mensagem. Quando o cliente recebe a mensagem DHCPACK, regista informações sobre configuração e realiza uma pesquisa ARP para o endereço atribuído. Se não houver resposta ao ARP, o cliente sabe que o endereço IPv4 é válido e começa a usá-lo como seu próprio.

7. Criação de Sub-redes

No endereço IPv4 original, há dois níveis de hierarquia: Uma rede e um host. Esses dois níveis de endereçamento permitem agrupamentos básicos de rede que facilitam o roteamento de pacotes para uma rede de destino. Um roteador encaminha pacotes com base na parte de rede de um endereço IP. Quando a rede é localizada, a parte de host do endereço permite a identificação do dispositivo de destino.

Entretanto, conforme as redes crescem, com muitas organizações adicionando centenas e até milhares de hosts à sua rede, a hierarquia de dois níveis não é suficiente.

Subdividir uma rede acrescenta um nível à hierarquia da rede, criando basicamente três níveis: Uma rede, uma sub-rede e um host. A inserção de mais um nível à hierarquia cria outros subgrupos em uma rede IP que agiliza a entrega de pacotes e adiciona filtragem, ajudando a minimizar o tráfego “local”.

7.1. Domínios de Broadcast

Em uma LAN Ethernet, os dispositivos usam broadcasts para localizar:

- **Outros dispositivos** – Um dispositivo usa o protocolo ARP (Address Resolution Protocol), que envia broadcasts de Camada 2 para um endereço IPv4 conhecido na rede local para descobrir o endereço MAC associado.

- **Serviços –** Geralmente, um host adquire sua configuração de endereço IP usando o protocolo DHCP (Dynamic Host Configuration Protocol), que envia broadcasts na rede local para localizar um servidor DHCP.

Roteadores não propagam broadcasts. Quando um roteador recebe um broadcast, ele não o encaminha por outras interfaces. Portanto, cada interface de um roteador se conecta a um *domínio de broadcast* e os broadcasts são propagados apenas no domínio de broadcast específico.

7.1.1. Problemas com Grandes Domínios de Broadcast

Um grande domínio de broadcast é uma rede que conecta vários hosts. Um problema desse tipo de domínio é que os hosts podem gerar broadcasts em excesso e afetar a rede de forma negativa. A solução é reduzir o tamanho da rede para criar domínios de broadcast menores em um processo denominado *divisão em sub-redes*. Os espaços de rede menores são chamados de *sub-redes*.

7.2. Motivo para Divisão em Sub-Redes

A divisão em sub-redes reduz o tráfego total da rede e melhora seu desempenho. Além disso, permite que o administrador implemente políticas de segurança como, por exemplo, quais sub-redes podem ou não se comunicar com quais sub-redes.

As sub-redes IPv4 são criadas com um ou mais bits de host sendo usados como bits de rede. Isso é feito estendendo-se a máscara de sub-rede para pegar emprestado alguns dos bits da parte de host do endereço e criar bits de rede adicionais. Quanto mais bits de host forem emprestados, mais sub-redes poderão ser definidas.
OBS: o uso de prefixos mais longos diminui o número de hosts por sub-rede.

7.3. Fórmula para criação de Sub-rede:

Use: 2^n >= Número de Sub-redes

Aonde: n - Número de bits emprestados

Para determinar o número de hosts disponível na sub-rede deve-se usar a seguinte formula:

$2^h - 2$ = Número de hosts disponível

Aonde: h - Número de bits restantes para host

7.4. Criando Sub-redes em redes /24

Exemplo:

Criar **duas** sub-redes a partir do Endereço de rede 192.168.1.0/24

Passo 1

Determinar a quantidade de bits que será emprestado na porção de host para a criação da sub-rede, com a fórmula 2^n>= Número de sub-redes.

Então teremos:

2^n>=2, n = 1 aonde: 2^1>=2 , ou seja, 2=2.

A nossa nova máscara será: 24+1=25 (/25 ou 255.255.255.128)

Sabendo o número de bits a empresta na parte de rede, nesse exemplo n=1, vamos para o passo 2.

Passo 2

Transformamos o endereço de rede em binário e de acordo com a máscara dada, no caso /24, que em decimal é representado: 255.255.255.0, apenas fazemos as alterações na porção destinada para a rede de modos a criar as sub-redes:

1) 192.168.1.0|0000000
2) 192.168.1.1|0000000

Fizemos as combinações nos bits emprestados de modos a criar as sub-redes, que serão:

192.168.1.0 e 192.168.1.128, ambos com a máscara de sub-rede 255.255.255.128, em decimal.

Passo 3

O Endereço de Broadcast e o último endereço valido para cada sub-rede, ou seja, ativando todas as combinações de host nos endereços de rede:

1) 192.168.1.0|1111111 = 192.168.1.127
2) 192.168.1.1|1111111 = 192.168.1.255

Passo 4

Para se saber o número de hosts que pode suportar a sub-rede, utilizamos a seguinte fórmula: $2^h - 2$ = Número de hosts

Teremos: $2^7 - 2$ = Número de host, 128 – 2 = Número de host, então Número de hosts =126.

Nota: O máximo de bits que podemos emprestar nessa classe de endereço é 6 bits, deixando os outros 2 para representar os host da rede, é muito usual em redes ponto-a-ponto.

Exercícios:

1) Criar 4 sub-redes com o seguinte endereço: 192.168.128.0/24?
2) Criar 10 sub-redes com o seguinte endereço: 192.168.2.0/24?

7.5. Criando Sub-redes em redes /16 e /8

Exemplo:

Criar **quatro** sub-redes a partir do Endereço de rede 172.16.0.0/16

Passo 1

Determinar a quantidade de bits que será emprestado na porção de host para a criação da sub-rede, com a fórmula $2^n >=$ Número de sub-redes.

Então teremos:

$2^n >= 4$, n = 2 aonde: $2^2 >= 4$, ou seja, 4=4.

A nossa nova máscara será: 16+2=18 (/18 ou 255.255.192.0)

Sabendo o número de bits a empresta na parte de rede, nesse exemplo n=2, vamos para o passo 2.

Passo 2

Transformamos o endereço de rede em binário e de acordo com a máscara dada, no caso /16, que em decimal é representado: 255.255.0.0, apenas fazemos as alterações na porção destinada para a rede de modos a criar as sub-redes:

1) 172.16.00|000000.00000000
2) 172.16.01|000000.00000000
3) 172.16.10|000000.00000000
4) 172.16.11|000000.00000000

Fizemos as combinações nos bits emprestados de modos a criar as sub-redes, que serão:

172.16.0.0, 172.16.64.0, 172.16.128.0 e 172.16.192.0, ambos com a máscara de sub-rede 255.255.192.0, em decimal.

Passo 3

O Endereço de Broadcast é o último endereço valido para cada sub-rede, ou seja, activando todas as combinações de host nos endereços de rede:

1) 172.16.00|111111.11111111 = 172.16.63.255
2) 172.16.01|111111.11111111 = 172.16.127.255
3) 172.16.10|111111.11111111 = 172.16.191.255
4) 172.16.11|111111.11111111 = 172.16.255.255

Passo 4

Para se saber o número de hosts que pode suportar a sub-rede, utilizamos a seguinte fórmula: $2^h - 2$ = Número de hosts

Teremos: $2^{14} - 2$ = Número de host, 16.384 – 2 = Número de host, então Número de hosts =16.382.

Nota: O máximo de bits que podemos emprestar nessa classe de endereço é 14 bits, deixando os outros 2 para representar os host da rede, é muito usual em redes ponto-a-ponto.

Exercícios:

1) Criar 7 sub-redes com o seguinte endereço: 172.17.0.0/16?
2) Criar 10 sub-redes com o seguinte endereço: 172.30.0.0/16?
3) Criar 10 sub-redes com o seguinte endereço: 10.0.0.0/8?
4) Criar 4 sub-redes com o seguinte endereço: 10.0.0.0/8?

7.6. Divisão de sub-redes com base ao número de hosts

Exemplo:

Criar sub-redes a partir do Endereço de rede 192.168.1.0/24, que suportam 120 hosts para cada sub-rede

Passo 1

Determinar a quantidade de bits que será usado na porção de host para criar sub-redes que satisfaçam a condição, com a fórmula, $2^h - 2$ = Número de hosts.

Então teremos:

$2^h - 2$ >= Número de hosts

$2^h - 2$ >= 120 hosts

$2^7 - 2$ >= 120 hosts, Verdade!

A partir desse momento já sabemos que não haver desperdício de endereços devemos apenas usar 7 (sete) bits para a parte de host, consequentemente teremos a nossa nova máscara alterada para:

255.255.255.0|0000000 = 255.255.255.128

Passo 2

Transformamos o endereço de rede em binário e de acordo com a nova máscara dada, no caso 255.255.255.128, fazemos as alterações na porção destinada para a rede de modos a criar as sub-redes:

3) 192.168.1.0|0000000
4) 192.168.1.1|0000000

Fizemos as combinações nos bits emprestados de modos a criar as sub-redes, que serão:

192.168.1.0 e 192.168.1.128, ambos com a máscara de sub-rede 255.255.255.128, em decimal.

Passo 3

O Endereço de Broadcast e o último endereço valido para cada sub-rede, ou seja, ativando todas as combinações de host nos endereços de rede:

1) 192.168.1.0|1111111 = 192.168.1.127
2) 192.168.1.1|1111111 = 192.168.1.255

Passo 4

Para se saber o número de sub-redes que podem ser formadas, utilizamos a seguinte fórmula: 2^n = Número de sub-redes

Teremos: 2^1 = Número de sub-redes, 2 = Número de sub-redes.

Exercícios:

1. Criar sub-redes com o seguinte endereço de redes: 192.168.5.0/24, que suporta 20 hosts?
2. Criar sub-redes com o seguinte endereço de redes: 172.16.32.0/16, que suporta 100 hosts?
3. Criar sub-redes com o seguinte endereço de redes: 10.0.0.0/8, que suporta 200 hosts?

8. Criação de Redes LANs Pequenas

O crescimento é um processo natural para muitas empresas de pequeno porte, e suas redes devem acompanhá-lo. O ideal é que o administrador de redes tenha experiência suficiente para tomar decisões inteligentes sobre como ampliar a rede de acordo com o crescimento da empresa.

Para projectar ou escalar uma rede, são necessários alguns elementos:

- **Documentação da rede** - topologia física e lógica
- **Inventário de dispositivos** - lista de dispositivos que usam ou compõem a rede
- **Orçamento** - orçamento de TI discriminado, incluindo o orçamento de compra de equipamentos do ano fiscal
- **Análise de tráfego** - protocolos, aplicações e serviços, e seus respectivos requisitos de tráfego, devem ser documentados

OBS: Esses elementos são usados para subsidiar a tomada de decisão que acompanha o crescimento de uma rede pequena.

REFERÊNCIAS BIBLIOGRÁFICAS

- Manual Curso CCNA1,2 e 3. 2018.
- TORRES, Gabriel. Redes de Computador curso completo. Ed. Axel Books Brasil, 2001.
- TORRES, Gabriel. Hardware Completo Curso. 3ª ed. Rio de Janeiro, Axel, 1999.
- WEBBER, Carlos. Apostila de Redes de Computador. Centro Universitário Sant` Ana, 2009