CLASSIFICAÇÃO DE REDES DE COMPUTADORES

Introdução

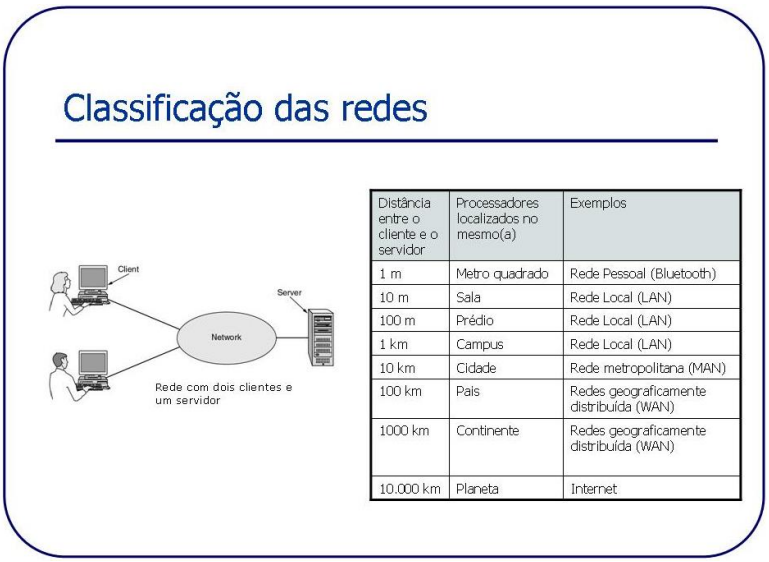
A classificação de redes em categorias pode ser realizada segundo diversos critérios, alguns dos mais comuns são:

- **Dimensão / alcance ou área geográfica ocupada**
  Redes Pessoais / Redes Locais / Redes Metropolitanas / Redes de área alargada /
- **Capacidade de transferência de informação**
  Redes de baixo débito / Redes de médio débito / Redes de alto débito / ...
- **Topologia** ("a forma da rede")
  Redes em estrela / Redes em "bus" / Redes em anel / ...
- **Meios físicos de suporte ao envio de dados**
  Redes de cobre / Redes de fibra óptica / Redes rádio / Redes por satélite / ...
- **Ambiente em que se inserem**
  Redes de industriais / Redes de coorporativas / ...
- **Método de transferência dos dados**
  Redes de "broadcast" / Redes de comutação de pacotes / Redes de comutação de circuitos / Redes ponto-a-ponto / ...
- **Tecnologia de transmissão**
  Redes "ethernet" / Redes "token-ring" / Redes FDDI / Redes ATM / Redes ISDN / ...

Como todas as classificações, tem um valor relativo, por exemplo o significado de "alto débito" varia com a evolução da "tecnologia corrente". Por outro lado, aos diferentes critérios de classificação geram sobreposições entre si.

CLASSIFICAÇÃO QUANTO AO ALCANCE

Uma rede de computadores é formada por um conjunto de módulos processados (e.g. microcomputadores) capazes de trocar informações e compartilhar recursos, através de um sistema de comunicação.



Distância entre o cliente e o servidor	Processadores localizados no mesmo(a)	Exemplos
1 m	Metro quadrado	Rede Pessoal (Bluetooth)
10 m	Sala	Rede Local (LAN)
100 m	Prédio	Rede Local (LAN)
1 km	Campus	Rede Local (LAN)
10 km	Cidade	Rede metropolitana (MAN)
100 km	País	Redes geograficamente distribuída (WAN)
1000 km	Continente	Redes geograficamente distribuída (WAN)
10.000 km	Planeta	Internet

Redes Locais (LAN):

- Permitem a interconexão de equipamentos dentro de uma área geográfica de alcance limitado. Ex: sala, andar de um prédio, prédio, conjunto Redes Locais. Ex: sala, andar de um prédio, prédio, conjunto concentrado de prédios.

- Interligam computadores presentes dentro de um mesmo espaço físico. Isso pode acontecer dentro de uma empresa, de uma escola ou dentro da sua própria casa, sendo possível a troca de informações e recursos entre os dispositivos participantes.

- O tipo de informação que trafega na rede é, normalmente, dados (tendência de mudança Redes Locais (cont.) normalmente, dados (tendência de mudança para tráfego multimídia).

- Operam a altas taxas de transmissão. Tipicamente: 10 Mbps, 100 Mbps e 1Gbps.

- Apresentam baixas taxas de erro. 1 em 107~ 108bits.

- Em geral, é de propriedade privada e é usada e operada por uma única organização.

- A topologia é usualmente limitada aos arranjos em barra, anel, estrela e árvore.

- LANs variam em tamanho e no número de computadores conectados.

- Exemplos de tecnologias de LANs: IEEE 802.3(“Ethernet”) IEEE 802.3µ (Fast Ethernet) IEEE 802.5 (Token Ring).

- Para quem quer acabar com os cabos, a WLAN, ou Rede Local Sem Fio, pode ser uma opção. Esse tipo de rede conecta-se à internet e é bastante usado tanto em ambientes residenciais quanto em empresas e em lugares públicos.

Redes Metropolitanas (MAN): Ocupa um estado intermediário entre as LAN e as WAN. Este termo, "Metropolitana", surgiu com o padrão IEEE 802.6. Elas apresentam características similares as redes locais, sendo que cobrem maiores distâncias. Sua abarangência vai de 1 Km à 12 Km.

- Desenvolvidas originalmente por operadoras de dados em resposta a uma grande demanda para interconexão de LANs sobre uma área metropolitana.

- As MANs cobrem uma área geográfica da ordem de dezenas a poucas centenas de quilômetros (ex: grupos de prédios, um conjunto industrial, uma cidade).

- Redes FDDI, por exemplo, suportam distâncias de até 2km entre estações, cobrindo uma área de até 200 km. Metro Ethernet, ATM e Frame-Relay são outros exemplos de tecnologias de MAN.

- A MAN pode ser proprietária e operada por uma única organização privada, mas normalmente é usada por várias organizações e operada por empresas públicas. Por exemplo, uma empresa pode interconectar os seus vários escritórios dentro de uma cidade ou estado usando uma MAN operada por uma companhia telefônica local. Ex: Agências bancárias municipais/estaduais interligadas por uma rede MPLS ou Frame Relay.

- Imaginemos, por exemplo, que uma empresa possui dois escritórios em uma mesma cidade e deseja que os computadores permaneçam interligados. Para isso existe a Metropolitan Area Network, ou Rede Metropolitana, que conecta diversas Redes Locais dentro de algumas dezenas de quilômetros.

- A WMAN é a versão sem fio da MAN, com um alcance de dezenas de quilômetros, sendo possível conectar redes de escritórios de uma mesma empresa ou de campus de universidades.

Redes Geograficamente Distribuidas (WAN): Estas redes surgiram com a necessidade de se compartilhar recursos especializados por uma maior comunidade de usuários geograficamente dispersos [SOARES, 1997]. Elas possuem custo elevado devido aos meios utilizados para comunicação em longa distância, tais como satélites e enlaces de microonda. Tais redes têm seus enlaces mantidos por grandes operadoras de telecomunicações (Telemar, Embratel, etc.) e seu acesso é público. Rede de Longa Distância, vai um pouco além da MAN e consegue abranger uma área maior, como um país ou até mesmo um continente.

- WANs são redes usadas para a interconexão de redes menores (LANs ou MANs) e sistemas computacionais dentro de áreas geográficas grandes (cidades, países ou até continentes).

- As WANs possuem um custo de comunicação bastante elevado devido aos circuitos para satélites e enlaces de microondas.

- São, em geral, mantidas, gerenciadas e de propriedade de grandes operadoras (públicas ou privadas), e o seu acesso é público.

- Por questões de confiabilidade, caminhos alternativos são oferecidos entre alguns nós. Com isso, a topologia da rede é, virtualmente, ilimitada.

- Voz, dados e vídeo são comumente integrados.

- A capacidade de chaveamento da rede permite a alteração dinâmica do fluxo de dados, ao contrário das LANs, que normalmente empregam o roteamento fixo.

- MPLS, ATM e X.25 são exemplos de tecnologias WAN.

- A WWAN, ou Rede de Longa Distância Sem Fio, alcança diversas partes do mundo. Justamente por isso, a WWAN está mais sujeita a ruídos

Rede Pessoal (PAN): O conceito de rede pessoal "Personal Area Network" está não só relacionado com a sua reduzida dimensão, mas com também com o fato de utilizar comunicação sem fios. O alcance limita-se a algumas dezenas de metros. Os débitos são relativamente baixos, na casa de 1 Mbps. São usadas para que dispositivos se comuniquem dentro de uma distância bastante limitada. Um exemplo disso são as redes Bluetooth e UWB.

Rede de Área de Armazenamento (SAN): As SANs, ou Redes de Área de Armazenamento, são utilizadas para fazer a comunicação de um servidor e outros computadores, ficando restritas a isso.

TOPOLOGIA DE REDE

A **topologia de rede** é o canal no qual o meio de rede está conectado aos computadores e outros componentes de uma rede de computadores. Essencialmente, é a estrutura topológica da rede, e pode ser descrito física ou logicamente. Há várias formas nas quais se podem organizar a interligação entre cada um dos nós (computadores) da rede. Existem duas categorias básicas de topologias de rede:

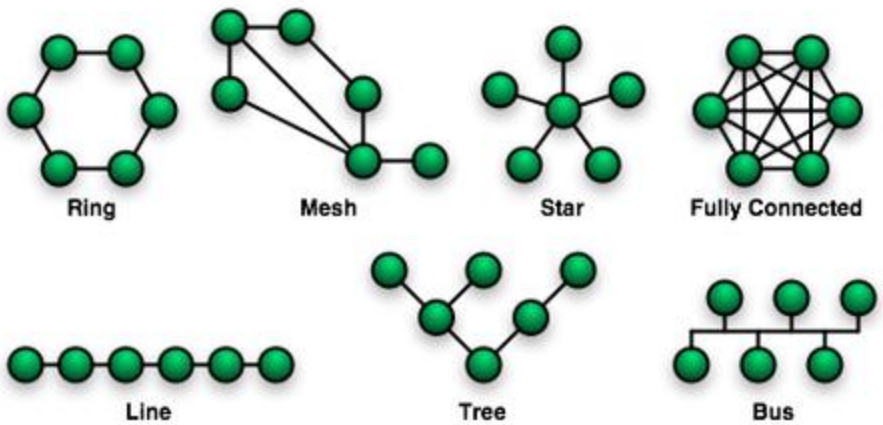
- Topologia física
- Topologia lógica

A topologia física é a verdadeira aparência ou layout da rede, enquanto que a lógica descreve o fluxo dos dados através da rede. A topologia física representa como as redes estão conectadas (layout físico) e o meio de conexão dos dispositivos de redes (nós ou nodos). A forma com que os cabos são conectados, e que genericamente chamamos de topologia da rede (física), influencia em diversos pontos considerados críticos, como a flexibilidade, velocidade e segurança.

A topologia lógica refere-se à maneira como os sinais agem sobre os meios de rede, ou a maneira como os dados são transmitidos através da rede a partir de um dispositivo para o outro sem ter em conta a interligação física dos dispositivos. Topologias lógicas são frequentemente associadas à Media Access Control, métodos e protocolos. Topologias lógicas são capazes de serem reconfiguradas dinamicamente por tipos especiais de equipamentos como roteadores e switches.

Ao mapear graficamente esses links, temos como resultado algumas formas geométricas que podem ser usadas para descrever diferentes topologias. Existem prós e contras para cada uma delas, uma vez que diferem na maneira como os dispositivos podem (ou não) se interconectar.

A topologia da rede pode ser estudada por meio de oito topologias básicas:



1.PONTO A PONTO: Peer-to-peer (do inglês par-a-par ou simplesmente ponto-a-ponto, com sigla P2P) é uma arquitetura de redes de computadores onde cada um dos pontos ou nós da rede funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central. As redes P2P podem ser configuradas em casa, em empresas e ainda na Internet. Todos os pontos da rede devem usar programas compatíveis para ligar-se um ao outro. Uma rede peer-to-peer pode ser usada para compartilhar músicas, vídeos, imagens, dados, enfim qualquer coisa com formato digital.

Um sistema P2P sem uma infraestrutura central.

Disposição de uma rede usual centralizada, baseada em servidores.

Vantagens

Por conta da simplicidade, as redes ponto a ponto são as alternativas mais populares quando se pensa em instalações residenciais, ou em qualquer outra situação em que você precisa estabelecer uma comunicação rápida entre dois dispositivos.

Desvantagens

Apesar da simplicidade, esses modelos não são recomendados para operações maiores e mais robustas. Nesse cenário, a infraestrutura deve escolher entre as topologias anteriores ou a uma variação da ponto a ponto, a topologia em Malha.

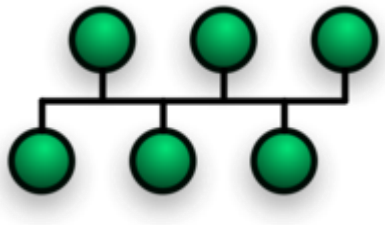
2.BARRAMENTO: Todos os computadores são ligados em um mesmo barramento físico de dados. Apesar de os dados não passarem por dentro de cada um dos nós, apenas uma máquina pode "escrever" no barramento num dado momento. Todas as outras "escutam" e recolhem para si os dados destinados a elas. Quando um computador estiver a transmitir um sinal, toda a rede fica ocupada e se outro computador tentar enviar outro sinal ao mesmo tempo, ocorre uma colisão e é preciso reiniciar a transmissão.

Essa topologia, normalmente, utiliza cabos coaxiais. Para cada barramento, existe um único cabo que vai de uma ponta a outra. O cabo é seccionado em cada local onde um computador será inserido. Com o seccionamento do cabo formam-se duas pontas e cada uma delas recebe um conector BNC. No computador é colocado um "T" conectado à

placa que junta apenas uma ponta. Embora ainda existam algumas instalações de rede que utilizam esse modelo, é uma tecnologia antiga.

Na topologia de barramento, apenas um dos computadores está ligado a um cabo contínuo que é terminado em ambas as extremidades por uma pequena ficha com uma resistência ligada entre a malha e o fio central do cabo (terminadores). A função dos "terminadores" é de adaptarem a linha, isto é, fazerem com que a impedância vista para interior e para o exterior do cabo seja a mesma, senão constata-se que há reflexão do sinal e, consequentemente, perda da comunicação.

Neste tipo de topologia a comunicação é feita por broadcast, isto é, os dados são enviados para o barramento e todos os computadores veem esses dados, no entanto, eles só serão recebidos pelo destinatário.



Vantagens

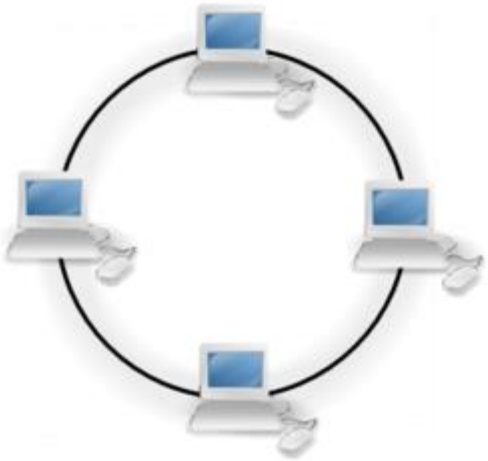
Sem sombra de dúvidas, é uma das estratégias mais económicas e versáteis de todas. O custo de implementação é baixo, assim como a complexidade de organização. Além disso, é uma topologia com manutenção simplificada, permitindo acrescentar novos dispositivos sem grandes planejamentos.

Desvantagens

Mas como sempre, a simplicidade cobra seu preço. Por ser uma rede em que o fluxo de dados é unidirecional e, assim como a Anel, é um pouco mais complicado diagnosticar e isolar os problemas na rede. Isso porque todos os dispositivos estão centralizados a um único fluxo.

Além disso, a topologia Barramento sofre com a mesma vulnerabilidade da dependência exclusiva. Enquanto o layout Árvore pode cair com a falha no Hub Central, a Barramento pode ser paralisada caso aconteça uma falha ou dano ao Cabo Central. Para finalizar, o aumento do tráfego interfere diretamente na velocidade da rede.

3.ANEL: Na topologia em anel, os dispositivos são conectados em série, formando um circuito fechado (anel). Os dados são transmitidos unidirecionalmente de nó em nó até atingir o seu destino. Uma mensagem enviada por uma estação passa por outras estações, através das retransmissões, até ser retirada pela estação destino ou pela estação fonte. Os sinais sofrem menos distorção e atenuação no enlace entre as estações, pois há um repetidor em cada estação. Há um atraso de um ou mais bits em cada estação para processamento de dados. Há uma queda na confiabilidade para um grande número de estações. A cada estação inserida, há um aumento de retardo na rede. É possível usar anéis múltiplos para aumentar a confiabilidade e o desempenho.



Vantagens

Um dos grandes benefícios da topologia Anel é que ela é bem eficiente na transmissão de dados sem erros. Isso acontece porque apenas uma estação da rede consegue enviar dados por vez, o que diminui a chance de ocorrer uma colisão entre pacotes.

Em grandes redes, a topologia Anel pode utilizar repetidores de sinal, aumentando a confiabilidade da transmissão e evitando a perda de dados. Além disso, o desempenho da rede não é prejudicado pelo aumento do volume de pessoas usuárias.

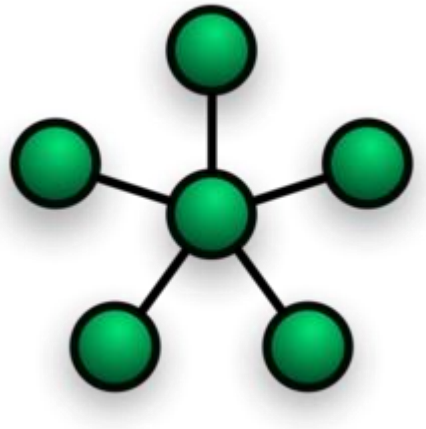
Desvantagens

Apesar de suas vantagens, a disposição em círculo apresenta uma grande vulnerabilidade: a falha de um dispositivo pode prejudicar a estabilidade de toda a rede. Nesse sentido, mesmo que você monitore a condição dos nodes, uma falha ainda pode acontecer em um deles, derrubando a conexão.

Além disso, a topologia Anel não é tão recomendada para operações em crescimento. Afinal de contas, todos os dispositivos estão conectados e consumindo uma mesma banda. Sendo assim, a cada dispositivo adicionado, a rede aumenta o seu delay, justamente pelo maior número de estações pelo quais os dados precisarão passar.

4.ESTRELA: A topologia em estrela é caracterizada por um elemento central que "gerencia" o fluxo de dados da rede, estando diretamente conectado (ponto-a-ponto) a cada nó, daí surgiu a designação "Estrela". As informações trafegam na rede de um host para o outro. Toda informação enviada de um nó para outro é enviada primeiro ao dispositivo que fica no centro da estrela, portanto os dados não passam por todos os hosts. O concentrador encarrega-se de encaminhar o sinal especificamente para as estações solicitadas, economizando tempo. Existem também redes estrela com conexão passiva (similar ao barramento), na qual o elemento central nada mais é do que uma peça mecânica que atrela os "braços" entre si, não interferindo no sinal que flui por todos os nós, da mesma forma que o faria em redes com topologia barramento. Mas este tipo de conexão passiva é mais comum em redes ponto-a-ponto lineares, sendo muito pouco utilizado já que os dispositivos concentradores (HUBs, Multiportas, Pontes e outros) não apresentam um custo tão elevado se levarmos em consideração as vantagens que são oferecidas.

As redes em estrela, que são as mais comuns hoje em dia, utilizam cabos de par trançado e uma switch como ponto central da rede. O hub se encarrega de retransmitir todos os dados para todas as estações, mas com a vantagem de tornar mais fácil a localização dos problemas, já que se um dos cabos, uma das portas do hub ou uma das placas de rede estiver com problemas, apenas o PC ligado ao componente defeituoso ficará fora da rede, ao contrário do que ocorre nas redes 10Base2, onde um mau contato em qualquer um dos conectores derruba a rede inteira.



Vantagens

Essa é uma das estratégias mais convenientes do ponto de vista do gerenciamento da rede. A conexão independente de cada node ao Hub Central facilita a identificação de problemas. Além disso, a falha isolada de uma máquina não causa perturbação à rede, já que o fluxo de dados é sempre exclusivo entre o Hub Central e seus respectivos nodes.

Desvantagens

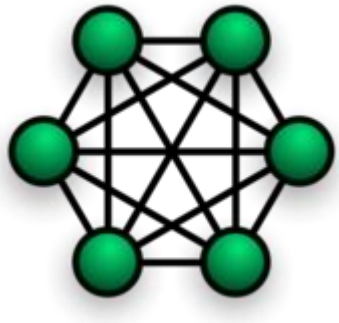
Assim como a topologia Barramento, o padrão Estrela também sofre com a vulnerabilidade da dependência exclusiva. Nesse caso, basta o Hub Central cair para que toda a rede perca a conexão. A topologia Árvore também sofre com o mesmo problema, mas conta com um diferencial.

5.MALHA (MESH): Na rede mesh ou rede de malha, os dispositivos se conectam diretamente, podendo se comunicar entre si. Devido às suas características, essa topologia faz contraste com outros tipos, como a Estrela, em que nesta toda o fluxo de informação gerado deve passar por um dispositivo central, também chamado de nó. Na rede de malha, os dispositivos possuem vários caminhos dentro da rede para que acessem os demais, conferindo maior resistência a falhas, Por esse motivo também é dito que consiste em uma rede do tipo ad-hoc.

Uma rede de infraestrutura é composta de APs (Access point = Ponto de acesso) e clientes, os quais necessariamente devem utilizar aquele AP para trafegarem em uma rede. Uma rede *mesh* é composta de vários nós/roteadores, que passam a se comportar como uma única e grande rede, possibilitando que o cliente se conecte em qualquer um destes nós. Os nós têm a função de repetidores e cada nó está conectado a um ou mais dos outros nós.

Esta topologia é muito utilizada em várias configurações, em especial redes sem fio, pois diferentemente das redes sem fio tradicionais, que normalmente possuem um AP central e consequentemente estão suscetíveis a falhas relacionadas ao ponto central, nesta os dispositivos possuem diversos caminhos para se comunicarem.

Um problema encontrado é em relação às interfaces de rede, já que para cada segmento de rede seria necessário instalar, em uma mesma estação, um número equivalente de placas de rede. Uma vez que cada estação envia sinais para todas as outras com frequência, a largura da banda de rede não é bem aproveitada. O maior problema nesta topologia é devido à existência de processamento adicional causado pela atribuição da função de roteamento aos nós da rede.



Vantagens

Confiabilidade e estabilidade. Como todos os dispositivos estão cabeados entre si, a falha individual ou até mesmo coletiva de algumas máquinas não será o suficiente para derrubar a conexão. Além disso, a topologia em Malha permite que os nodes sempre tenham a opção de enviar os pacotes de dados pela rota mais eficiente.

Desvantagens

Cabear e conectar todos os dispositivos de uma rede entre si é uma tarefa que exige um nível de planejamento considerável. Ainda que o diagnóstico de erros seja facilitado nesse padrão, a implementação inicial é bastante custosa e complicada.

6.ÁRVORE: A topologia em árvore é essencialmente uma série de barras interconectadas. Geralmente existe uma barra central onde outros ramos menores se conectam. Esta ligação é realizada através de repartidores e as conexões das estações realizadas do mesmo modo que no sistema de barra padrão. Esse tipo de topologia se diferencia do tipo estrela pois permite que estações conectadas à central também se conectem com outras estações. E, diferentemente da topologia em malha, não permite a existência de conexões fechando circuitos, dessa forma, a possibilidade de um pacote percorrer pelo menos três estações, de modo que o computador inicial e o final sejam os mesmos, é inexistente.

Na imagem, percebemos que o elemento central, que é conhecido como raiz, encontra-se na parte inferior e, logo após, encontram-se dois computadores, que representam os ramos. Posteriormente, os computadores chamados de folhas, ficam nas extremidades. Essa sequência também pode ser conhecida como primeiro da árvore, segundo nível da árvore e terceiro nível da árvore.

Cuidados adicionais devem ser tomados nas redes em árvores, pois cada ramificação significa que o sinal deverá se propagar por dois caminhos diferentes. A menos que estes caminhos estejam perfeitamente casados, os sinais terão velocidades de propagação diferentes e refletirão os sinais de diferentes maneiras. Por estes motivos, geralmente as redes em árvore vão trabalhar com taxas de transmissão menores do que as redes em barra comum.

Atualmente não se usa a topologia em árvore, por que caso haja falha, a rede pode ser comprometida.

Usa-se normalmente uma topologia física baseada numa estrutura hierárquica de várias redes e sub-redes. Existem um ou mais concentradores que ligam cada rede local e existe um outro concentrador que interliga todos os outros concentradores. Esta topologia facilita a manutenção do sistema e permite, em caso de avaria, detectar com melhor facilidade o problema.

Vantagens

O grande trunfo da topologia Árvore é eliminar a vulnerabilidade da topologia Anel, em que uma falha em qualquer um dos dispositivos da rede poderia colocar tudo abaixo. Além disso, esse padrão facilita a identificação de erros, uma vez que cada branch da rede pode ser diagnosticado individualmente.

Por esse tipo de topologia não permitir a existência de ciclos, não ocorre uma ocupação desnecessária dos recursos de banda, já que a possibilidade de um pacote permanecer em loop na rede é eliminada.

Por fim, a topologia Árvore também oferece um layout muito mais simples e prático para operações em crescimento. O acréscimo de novos dispositivos não causa retardo na conexão, uma vez que os pacotes de dados viajam segmentados a partir do hub central para os secundários e os seus destinos.

Desvantagens

A esse ponto, é bem possível que você já tenha identificado o calcanhar de Aquiles na topologia Árvore. Exatamente, o Hub Central! Nesse padrão, toda a rede depende de um único ponto de origem, o nó raiz. Isso significa que, se esse Hub sofrer com uma falha, todos os dispositivos conectados a ele (Hubs Secundários) cairão também, passando a existir dois grupos de computadores isolados que não poderão se comunicar.

7.HÍBRIDA: É a topologia mais utilizada em grandes redes. Assim, adequa-se a topologia de rede em função do ambiente, compensando os custos, expansibilidade, flexibilidade e funcionalidade de cada segmento de rede. São as que utilizam mais de uma topologia ao mesmo tempo, podendo existir várias configurações que podemos criar utilizando uma variação de outras topologias. Elas foram desenvolvidas para resolver necessidades específicas.

Muitas vezes acontecem demandas imediatas de conexões e a empresa não dispõe de recursos, naquele momento, para a aquisição de produtos adequados para a montagem da rede. Nestes casos, a administração de redes pode utilizar os equipamentos já disponíveis considerando as vantagens e desvantagens das topologias utilizadas.

Consideremos o caso de um laboratório de testes computacionais onde o número de equipamentos é flutuante e que não admite um layout definido. A aquisição de concentradores ou comutadores pode não ser conveniente, pelo contrário até custosa. Talvez uma topologia em barramento seja uma solução mais adequada para aquele segmento físico de rede.

Numa topologia híbrida, o desenho final da rede resulta da combinação de duas ou mais topologias de rede. A combinação de duas ou mais topologias de rede permite-nos beneficiar das vantagens de cada uma das topologias que integram esta topologia. Embora muito pouco usada em redes locais, uma variante da topologia em malha, a malha híbrida, é usada na Internet e em algumas WANs. A topologia de malha híbrida pode ter múltiplas ligações entre várias localizações, mas isto é feito por uma questão de redundância, além de que não é uma verdadeira malha porque não há ligação entre cada um e todos os nós, somente em alguns por uma questão de backup.

Uma mistura de topologia em anel (ligação central) com em estrela (nas extremidades). Como há uma ligação dupla entre os dois concentradores, a tendência é utilizar apenas uma via para transmissão entre as redes, deixando a outra como reserva. Isso é possível graças à evolução dos equipamentos, que permitem que as redes funcionem mesmo em condições de falhas, tornando mais eficiente a organização, que não precisa parar para que seja feita a manutenção.

Interconexão entre duas Topologias (Árvore e Anel), formando a topologia Híbrida.

Vantagens

Sem sombra de dúvidas, esse é o padrão mais flexível e adaptável de todos. A estrutura pode se integrar a redes com topologia Estrela, Árvore e Barramento, evitando o custo necessário para uma reestruturação completa.

Por essa razão, a topologia Híbrida é frequentemente utilizada em grandes empresas, interligando departamentos, setores e escritórios, conforme eles são integrados na operação da empresa.

Desvantagens

A complexidade é a principal desvantagem. Apesar de ser uma solução prática para integrar topologias já existentes, a cada nova integração, mais densa se torna a rede, exigindo muita atenção e experiência do especialista responsável pela organização da rede.

8.DAISY CHAIN: Exceto para redes conectadas em estrela, a maneira mais fácil de adicionar mais computadores em uma rede é por encadeamento (Daisy-Chaining), ou seja, ligar cada computador em série com o próximo. Se a mensagem se destina a um computador distante no caminho da linha, cada sistema a retransmite em sequência, até que ela chegue ao seu destino. Uma rede encadeada (Daisy-Chained) pode assumir duas formas básicas: linear e anel.

A topologia linear coloca um link de duas vias entre um computador e outro. No entanto, isso era caro nos primeiros dias da computação, uma vez que cada computador (exceto os que estão em cada extremidade), necessitava de dois receptores e dois transmissores.

A topologia em anel pode ser formada conectando-se os computadores em cada extremidade. Uma das vantagens do anel é que a metade do número de transmissores e receptores pode sair de serviço, já que uma mensagem fará uma volta eventualmente por todo o outro lado. Quando um nó transmite uma mensagem, a mensagem é processada por todos os computadores do anel. Se um computador não é o nó destino, ele vai passar a mensagem para o nó seguinte, até que a mensagem chegue ao seu destino. Se a mensagem não for aceita por nenhum nó da rede, ela vai percorrer todo o anel e retornar ao remetente. Isto potencialmente resulta em uma duplicação do tempo de transmissão para os dados.

CLASSIFICAÇÃO DE REDES QUANTO A HIERARQUIA

A classificação das redes de computadores quanto a hierarquia refere-se ao modo como os computadores dentro de uma rede se comunicam. Entre os principais tipos de classificação quanto a hierarquia, estão as **redes ponto-a-ponto (Peer to Peer)** e as **redes cliente-servidor (Server-Client).**

REDES PONTO-A-PONTO: É utilizada em pequenas redes. Os computadores trocam informações entre si, compartilhando arquivos e recursos. Suas características pontuais são:
• É utilizada em pequenas redes.
• São de implementação fácil e de baixo custo.
• Possuem pouca segurança.
• Apresentam um sistema de cabeamento simples.

REDES CLIENTE-SERVIDOR: O tipo de rede cliente-servidor possui um ou mais servidores, responsáveis por prover serviços de rede aos demais computadores conectados a ele que são chamados clientes. Cada cliente (computador que compõe este tipo de rede), denominados nós, que deseja acessar um determinado serviço ou recurso faz essa solicitação ao servidor da rede, por isso o nome cliente-servidor. Esse tipo de rede surgiu da necessidade de criar uma estrutura que pudesse centralizar o processamento em um computador central da rede (no caso o servidor, com recursos de hardware preparados para tal processamento).

Como características deste tipo de rede podemos citar:
• Maior custo e implementação mais complexa que uma rede do tipo ponto-aponto.
• Existência de pelo menos um servidor da rede.
• Redes do tipo cliente-servidor, apresentam uma estrutura de segurança melhorada, pois as informações encontram-se centralizadas no servidor, o que facilita o controle e o gerenciamento dos mesmos.
• Neste tipo de rede não há tolerância a falhas (como existe em um sistema descentralizado) haja vista um único sistema centralizado de informações (servidor).
• Um servidor de rede é um computador projetado (hardware) para suportar a execução de várias tarefas que exigem bastante do hardware (como disco rígido e processador), diferentemente de uma estação de trabalho (cliente), que não possui características para realizar o trabalho de um servidor (quando falamos puramente do hardware necessário a um computador servidor).
• No contexto do software para servidores, deve prover serviços usuais para atender os clientes da rede: autenticação, compartilhamento de recursos, entre outros.

CLASSES DE IPS

No **IPv4,** o campo do cabeçalho reservado para o endereçamento possui 32 bits, com um máximo de 4.294.967.296 (232) endereços distintos.Na época de seu desenvolvimento, esta quantidade era considerada suficiente para identificar todos os computadores na rede e suportar o surgimento de novas sub-redes. No entanto, com o rápido crescimento da Internet, surgiu o problema da escassez dos endereços IPv4, motivando a criação de uma nova geração do protocolo IP.

Assim, o **IPv6** surgiu, com um espaço para endereçamento de 128 bits, podendo obter 340.282.366.920.938.463.463.374.607.431.768.211.456 endereços (2^{128}). Este valor representa aproximadamente 79 octilhões ($7{,}9x10^{28}$) de vezes a quantidade de endereços IPv4 e representa, também, mais de 56 octilhões ($5{,}6x10^{28}$) de endereços por ser humano na Terra, considerando-se a população estimada em 6 bilhões de habitantes.

- IPV4: O protocolo IP atualmente mais utilizado é o IPv4 (IP versão 4). Utiliza 32 bits para endereçamento representados em 4 segmentos de números decimais variando de 0 a 255.

- IPV6: O IPv6 é a versão 6 do protocolo IP projetado para substituir o IPv4. O IPv6 quadruplica o número de bits do endereço de rede de 32 bits para 128 bits, permitindo uma flexibilidade maior em atribuir endereços. O endereço é apresentado em 8 segmentos de 4 números hexadecimais.

Exemplo: 1F44.25AB.112E.0000.0988.87EC.9900.0076

Características IPv6:

- Os endereços IPv6 têm um tamanho de 128 bits.
- Suporte para atribuição automática de endereços numa rede IPv6, podendo ser omitido o servidor de DHCP a que estamos habituados no IPv4.
- Simplifica as tabelas de encaminhamento dos roteadores da rede, diminuindo assim a carga de processamento dos mesmos.
- O formato do cabeçalho foi totalmente remodelado em relação ao IPv4.
- Cabeçalhos de extensão como opção para guardar informação adicional.
- Aplicações de áudio e vídeo passam a estabelecer conexões apropriadas tendo em conta as suas exigências em termos de qualidade de serviço (QoS).
- Permite adicionar novas especificações de forma simples.
- Diversas extensões no IPv6 permitem, à partida, o suporte para opções de segurança como autenticação, integridade e confidencialidade dos dados.

Existem no IPv6 três tipos de endereços definidos:

- Unicast: este tipo de endereço identifica uma única interface, de modo que um pacote enviado a um endereço unicast é entregue a uma única interface. Os endereços unicast são utilizados para comunicação entre dois nós, por exemplo, telefones VoIPv6, computadores em uma rede privada, etc., e sua estrutura foi definida para permitir agregações com prefixos de tamanho flexível, similar ao CIDR do IPv4. Comunicação na qual um quadro é enviado de um host e endereçado a um destino específico.

QUADRO*: É um pacote de dados (é a informação transmitida entre as máquinas). Ex.: Um ping que é realizado no terminal de comando, enviará uma quantidade "X" de pacotes de dados (quadros) para o endereço especificado.*
Na transmissão *Unicast*, há apenas um remetente e um receptor. Esta é a forma predominante de transmissão em redes locais e na Internet, onde ocorrer a transmissão ponto-a-ponto. Entre os exemplos de protocolos que usam transmissões *Unicast* estão HTTP, SMTP, FTP e Telnet.
O Unicast é o sistema de roteamento mais comum usado na internet, com cada nó atribuído à um endereço IP exclusivo. Os roteadores identificam a origem e destino dos dados e determinam o caminho mais curto (ou o mais viável) para o envio dos pacotes de dados. Os dados são entregues entre roteadores até que ele chegue ao seu destino final.

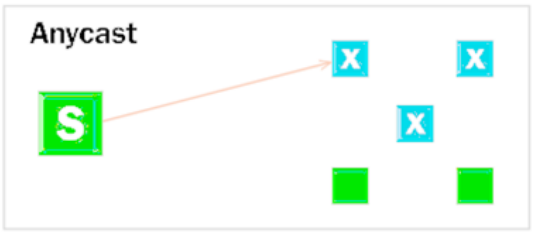
- **Anycast**: identifica um conjunto de interfaces. Um pacote encaminhado a um endereço anycast é entregue a interface pertencente a este conjunto mais próxima da origem (de acordo com distância medida pelos protocolos de roteamento). Um endereço anycast é utilizado em comunicações de um-para-um-de-muitos. Esta é uma forma de encaminhamento onde os dados são distribuídos "ao destino mais próximo" ou "melhores" definidos pelo *routing* da rede. **Anycast** é um sistema que utiliza endereços de rede e métodos de roteamento, a fim de enviar os dados para o nó mais próximo disponível dentro de um grupo de receptores que estão usando o mesmo endereço IP. Em termos práticos, o uso de *Anycast* reduz a latência (aumentando assim a velocidade de entrega) e ajuda um provedor para equilibrar as cargas de servidor, ao fornecer "apoio" em caso de falha do servidor dentro do grupo que compartilha o endereço IP. Por esta razão, o *Anycast* é usado geralmente como uma maneira de fornecer disponibilidade elevada e balanceamento de carga para serviços sem estado, como o acesso a dados replicados. Os três principais benefícios do uso de roteamento *Anycast* são a velocidade, balanceamento de carga e redundância. Dois outros benefícios que são quase tão importante são: melhor escalabilidade e melhor resposta a ataques DoS e DDoS. *Anycast* é capaz de ajudar a responder a ataques de rede. Os ataques DoS ou DDoS pode facilmente sobrecarregar um Servidor *Unicast.* Porém, quando o tráfego é espalhar-se através de uma rede *Anycast,* cada servidor absorve uma parte do ataque diminuindo a possibilidade de toda a rede "caia". Isto é particularmente essencial para a maioria dos ataques DoS, que geralmente se concentram no nó mais próximo para as *"máquinas zumbis"*.

- **Multicast**: também identifica um conjunto de interfaces, entretanto, um pacote enviado a um endereço multicast é entregue a todas as interfaces associadas a esse endereço. Um endereço multicast é utilizado em comunicações de um-para-muitos. Comunicação na qual um quadro é enviado para um grupo específico de dispositivos ou clientes. Os clientes da transmissão *multicast* devem ser membros de um grupo *multicast* lógico para receber as informações. Um exemplo de transmissão *multicast* é a transmissão de vídeo e de voz associada a uma reunião de negócios colaborativa, com base em rede. Ao invés de ser enviado para um único destino (endereço IP específico), o tráfego de *multicast*, permite o envio de informações para um determinado grupo de clientes, cada um com um endereço IP diferente, ao mesmo tempo. O *Multicast* não é normalmente usado pelos roteadores de Internet, é comum sua utilização em ambientes de redes corporativas, afim de entregar o tráfego sem o uso de uma enorme quantidade de largura de banda.

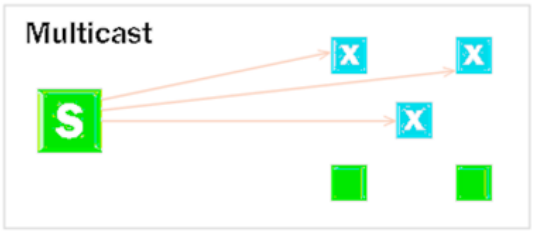
Atenção: No IPv4, o suporte a multicast é opcional, já que foi introduzido apenas como uma extensão ao protocolo. Entretanto, no IPv6 é requerido que todos os nós suportem multicast, visto que muitas funcionalidades da nova versão do protocolo IP utilizam esse tipo de endereço.
Seu funcionamento é similar ao do broadcast, dado que um único pacote é enviado a vários hosts, diferenciando-se apenas pelo fato de que no broadcast o pacote é enviado a todos os hosts da rede, sem exceção, enquanto que no multicast apenas um grupo de hosts receberá esse pacote. Deste modo, a possibilidade de transportar apenas uma cópia dos dados a todos os elementos do grupo, a partir de uma árvore de distribuição, pode reduzir a utilização de recurso de uma rede, bem como otimizar a entrega de dados aos hosts receptores. Aplicações como videoconferência, distribuição de vídeo sob demanda, atualizações de softwares e jogos on-line, são exemplos de serviços que vêm ganhando notoriedade e podem utilizar as vantagens apresentadas pelo multicast.

- **Broadcast**: Diferente do IPv4, no IPv6 não existe endereço **broadcast**, responsável por direcionar um pacote para todos os nós de um mesmo domínio. No IPv6, essa função foi atribuída à tipos específicos de endereços multicast.
Comunicação na qual um quadro é enviado de um endereço para todos os outros endereços. Nesse caso, há apenas um remetente, mas as informações são enviadas para todos os receptores conectados. A transmissão de *broadcast* é essencial durante o envio da mesma mensagem para todos os dispositivos na rede local. Um exemplo de transmissão de *broadcast* é a consulta de resolução de endereços que o Protocolo de Resolução de Endereços (ARP, *Address Resolution Protocol*) envia para todos os computadores em uma rede local.
Um equipamento muito comum em domínio de *broadcast* é o HUB, que está cada vez mais em desuso, pois ao trabalhar em *broadcast*, enviando uma mensagem para todos conectados, gera um grande tráfego na rede, reduzindo o desempenho e aumentando as colisões de pacotes.

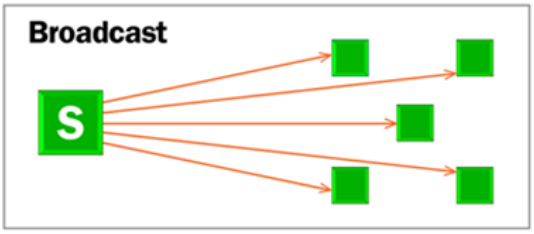
"Um para Um"



Um para o mais próximo de um determinado grupo



"Um para muitos"
Um grupo específico



"Um para Todos"

IMPORTANTE: O aumento no número de endereços não é a única mudança do IPv6. Ao contrário do IPv4, o IPv6 não implementa o **broadcast**. Ao invés disso, ele realiza o **multicast**. Por isso, alguns protocolos baseados em broadcast, como o **ARP**, não existem na nova versão.
Alguns protocolos, como o **ICMP** e o **DHCP**, receberam novas versões no IPv6, o ICMPv6 e o DHCPv6.
Além dessas, outras mudanças foram feitas. O cabeçalho do protocolo IPv6 tem menos campos que o do IPv4, bem como a segurança do IPv6 foi aumentada.
Outra coisa que muda em relação ao IPv4 é a máscara de rede. No IPv6 utilizamos a **notação CIDR** para dizer qual parte do endereço pertence a rede e qual parte pertence ao host. Essa notação diz qual parte do endereço pertence a rede e qual pertence ao host.
Dessa forma, deixa de existir **máscaras de sub-rede**. Já que a identificação da rede está no próprio endereço.

COMUTAÇÃO

Os switches operam semelhantemente a um sistema telefónico com linhas privadas. Neste sistema, quando uma pessoa liga para outra, a central telefónica conecta-as numa linha dedicada, possibilitando um maior número de conversações simultâneas.A função básica de um switch é juntar ou conectar dispositivos em uma rede. É importante deixar claro que um switch NÃO fornece conectividade com outras redes por si só e, obviamente, também NÃO fornece conectividade com a Internet.

Um comutador opera na camada 2 (enlace) do modelo OSI, encaminhando os pacotes de acordo com o endereço MAC de destino, e é destinado a redes locais para segmentação. Porém, atualmente (2005) existem comutadores que operam em conjunto na camada 3 (rede), herdando algumas propriedades dos roteadores (*routers*).

O switch aprende com a rede e depois apenas encaminha para os endereços conhecidos. Exemplo de funcionamento: considere uma rede com 4 computadores (A, B, C e D) conectados nas portas 1, 2, 3 e 4 respectivamente, onde o computador A envia um *frame* ao computador D, o comutador ainda não sabe aonde está o computador D por isso ele faz *broadcast* para todas as outras 3 portas (2, 3 e 4), mas ele já gravou que o computador A está na porta 1. Em outro momento, o computador C envia um *frame* ao computador A, então o comutador não precisa mais fazer *broadcast* porque ele já aprendeu que o computador A está na porta 1, então ele envia somente para esta porta, e também já aprendeu que o computador C está na porta 3, e assim sucessivamente até aprender em quais portas estão todos os computadores da rede, a partir de então ele envia somente à porta de destino específico (*unicast*).

MÉTODOS DE COMUTAÇÃO: Existem 4 métodos de comutação que um comutador pode usar, dos quais do segundo ao quarto apresentaram melhora de desempenho quando usados em produtos "comutados" com a mesma largura de banda de entrada e saída de porta:

1. **Store and forward:** o comutador verifica cada quadro antes de encaminhá-lo; um quadro é recebido na íntegra antes de ser encaminhado. Todo o quadro é recebido antes de ser encaminhado. Os endereços de destino e de origem são lidos e os filtros são aplicados antes que o quadro seja encaminhado. A latência ocorre enquanto o quadro está sendo recebido. A latência é maior com quadros maiores, pois todo o quadro precisa ser recebido antes que o processo de comutação comece. O switch tem tempo para verificar se há erros, o que proporciona maior detecção de erros.
2. **Cut Through:** O comutador, não propaga domínios, envia o *frame* após ler seu endereço MAC de destino. Não averigua o valor da soma de verificação. Um switch que realiza comutação cut-through somente lê o endereço de destino ao receber o quadro. O switch começa a encaminhar o quadro antes que este chegue por completo. Esse modo diminui a latência da transmissão, mas tem uma detecção de erros ruim. Há duas formas de comutação cut-through:

- **Fast-forward** – Este tipo de comutação oferece o nível mais baixo de latência encaminhando imediatamente um pacote após receber o endereço de destino. A latência é medida a partir do primeiro bit recebido até o primeiro bit transmitido, ou seja, o primeiro a entrar é o primeiro a sair (FIFO, first in first out). Este modo tem uma detecção de erros ruim na comutação de rede local.

- **Fragment-free** – Este tipo de comutação filtra e elimina os fragmentos de colisão, que constituem a maior parte dos erros de pacote, antes de iniciar o encaminhamento. Geralmente, os fragmentos de colisão são menores do que 64 bytes. A comutação fragment-free aguarda até que seja determinado que o pacote recebido não é um fragmento de colisão antes de encaminhá-lo. A latência também é medida como FIFO.

3. **Fragment Free:** tenta utilizar os benefícios do *Store-and-Forward* e *Cut Through*. Verifica os primeiros 64 *bytes* do *frame*, onde as informações de endereçamento estão armazenadas.
4. **Comutação adaptativa (*adaptative cut-switching*):** faz o uso dos outros três métodos. Este modo de transmissão é um modo híbrido que combina cut-through e store-and-forward. Neste modo, o switch usa cut-through até detectar uma determinada quantidade de erros. Uma vez atingido o limiar de erros, o switch muda para o modo store-and-forward.

DIFERENÇAS ENTRE SWITCH L2 E L3:

Switch L2 utiliza o endereço MAC (nível 2) contido no pacote de dados para enviar a informação, enquanto que o **Switch L3** utiliza os endereços de nível 2 ou nível 3 (um exemplo é o endereço IP) para determinar o destino do pacote, permitindo que os pacotes sejam roteados.

Um **Switcing adaptável** é designado para atuar normalmente no modo Cut-Through. Contudo, se a taxa de erro em uma de suas portas for muito alta, o switch reconfigura automaticamente a porta para atuar no modo Store-and-Forward.

Essa característica otimiza o funcionamento do dispositivo, uma vez que permite que o mesmo provenha um switching (comutação) mais rápido com uma maior taxa de transmissão pelo modo cut-through, ou em caso de alta taxa de erro, alterar a porta para o modo store-and-forward. Switches adaptáveis garantem o melhor funcionamento possível para o sistema, pois conciliam o melhor de cada tipo de tecnologia comutadora.

DOMINIO DE COLISÃO

Numa rede de computadores, o **domínio de colisão** é uma área lógica onde os pacotes podem *colidir* uns contra os outros, em particular no protocolo Ethernet. Quanto mais colisões ocorrem menor é a eficiência da rede.

Um domínio de colisão pode existir num único segmento da rede (como numa rede em barramento) ou numa porção ou total de uma rede maior (note-se que a utilização de *hubs* faz propagar o domínio de colisão a todos os seus segmentos). Em redes Ethernet, ao utilizar um hub, temos uma topologia lógica de barramento e as estações comportam-se como se estivessem todas ligadas a um único meio físico. Isso simplifica a transmissão de dados e reduz o investimento em equipamentos intermediários, mas em compensação traz um grave problema: as colisões de pacotes que ocorrem sempre que duas (ou mais) estações tentam transmitir dados ao mesmo tempo.

O protocolo de comunicação CSMA/CD que controla o acesso ao meio em redes Ethernet minimiza este problema através de um conjunto de medidas relativamente simples: antes de transmitir um pacote, a estação "escuta" o meio físico para verificar se outra estação já está transmitindo. Na verdade cada host, por meio do CSMA/CD, verifica se há uma onda portadora indicando transmissão. Caso o meio físico esteja ocupado ela espera, caso esteja livre ela transmite. Em caso de colisão, ele imediatamente interrompe a transmissão, enviando um *Jam Signal* que repete a colisão, informando aos hosts envolvidos. Nesses hosts o jam signal ativará um algoritmo de *backoff* que fará com que cada host espere por um tempo aleatório e crescente, em caso de reincidência de colisão, para retransmitir.

Agora, restringindo-nos a Hubs, Switches e Roteadores, vamos discuti-los em referência aos domínios abaixo:

1. **Domínio de Colisão:** Um Domínio de Colisão é um cenário em que quando um dispositivo envia uma mensagem para a rede, todos os outros dispositivos que estão incluídos em seu domínio de colisão devem estar atentos a ele, independentemente de ser ou não destinado a eles. Isto causa um problema porque, numa situação em que dois dispositivos enviam as suas mensagens simultaneamente, ocorrerá uma colisão que os fará aguardar e retransmitir as respectivas mensagens, uma de cada vez. Lembre-se, isso acontece apenas no caso de um modo half-duplex.
2. **Domínio de broadcast:** Um domínio de broadcast é um cenário no qual quando um dispositivo envia uma mensagem de broadcast, todos os dispositivos presentes em seu domínio de broadcast devem prestar atenção a ele. Isso cria muito congestionamento na rede, comumente chamado de congestionamento de LAN, que afeta a largura de banda dos usuários presentes nessa rede.

   A partir disso, podemos perceber que quanto mais o número de domínios de colisão e mais o número de domínios de broadcast, mais eficiente é a rede fornecendo melhor largura de banda a todos os seus usuários.

Então, quais dos nossos dispositivos de rede quebram os domínios de colisão e quais deles quebram os domínios de broadcast?

- HUB: Começamos com um hub porque devemos nos livrar dele o mais rápido possível. A razão é que ele não quebra um domínio de colisão nem um domínio de broadcast, ou seja, um hub não é um separador de domínio de colisão nem um separador de domínio de broadcast. Todos os dispositivos conectados a um hub estão em uma única colisão e domínio de transmissão único. Lembre-se de que os hubs não segmentam uma rede, apenas conectam segmentos de rede.

- SWITCH: No que diz respeito aos switches, temos uma vantagem sobre o hub. Cada porta em um switch está em um domínio de colisão diferente, ou seja, um switch é um separador de domínio de colisão. Portanto, as mensagens que vêm de dispositivos conectados a portas diferentes nunca sofrem uma colisão. Isso nos ajuda durante o projeto de redes, mas ainda há um problema com os interruptores. Eles nunca quebram os domínios de broadcast, o que significa que não é um separador de domínio de broadcast. Todas as portas do switch ainda estão em um único domínio de broadcast. Se um dispositivo enviar uma mensagem de difusão, ainda causará congestionamento.

- ROUTER: Por último, mas não menos importante, temos nosso salvador. Um roteador não apenas interrompe os domínios de colisão, mas também interrompe os domínios de broadcast, o que significa que ele é tanto um separador de colisão quanto de broadcast. Um roteador cria uma conexão entre duas redes. Uma mensagem de transmissão de uma rede nunca alcançará a outra, pois o roteador nunca a deixará passar.

Além disso, como repetidores e pontes diferem de hubs e switches apenas em termos do número de portas, um repetidor não interrompe os domínios de colisão e broadcast, enquanto uma ponte interrompe apenas os domínios de colisão.