CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA FACULDADE DE TECNOLOGIA DE INDAIATUBA

CURSO DE TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

RAFAEL TOSHIO HONMA HONDA

**Redes**

INDAIATUBA

2018

1. **Cabos de Rede**

O cabeamento de uma rede faz parte do meio físico para interligar computadores, é um fator de extrema importância para o bom desempenho de uma rede. Ele envolve aspectos sobre a taxa de transmissão, largura de banda, facilidade de instalação, imunidade a ruídos, confiabilidade, custos de interface, exigências geográficas, conformidade com padrões internacionais e disponibilidades de componentes.

Existem basicamente três tipos diferentes de cabos de rede: cabos de par trançado, cabos de fibra óptica e cabos coaxiais.

* 1. **Cabo coaxial**

Cabos coaxiais são compostos por um condutor central de cobre, responsável por carregar o sinal, uma malha metálica de blindagem o que oferece melhor imunidade ao ruído que o par trançado.

O cabo coaxial pode transmitir altas taxas de dados por distâncias relativamente longas sem a necessidade de regeneração do sinal, por outro lado, o seu custo é maior e sua instalação não é simples.

Os cabos coaxiais são utilizados nas redes telefônicas, TV a cabo e em redes de computadores.

* 1. **Cabo par trançado**

Cabos de par trançado são compostos por pares de fio de cobre encapados, traçados entre si, criando assim uma barreira eletromagnética, protegendo as transmissões de interferências externas sem a necessidade de uma camada de blindagem, eles são classificados em categorias que indicam a qualidade do cabo e a frequência máxima suportada.

Os tipos de cabo par trançado são:

* Par trançado sem blindagem (*UTP -Unshielded Twistead-Pair*): é o cabo mais popular no uso das redes de computadores.
* Par trançado blindado (*STP – Shielded Twistead-Pair*): este cabo tem uma blindagem eletromagnética metálica ou revestimento em malha de cobre em cada par de fios isolados do cabo. Embora a blindagem melhore a qualidade do cabo, o cabo se torna mais caro e mais volumoso.

Classificação de cabos UTP

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Categoria | Largura de banda | Taxa de transmissão | Tipo de sinal | Aplicação |
| 1 | Muito baixa | < 100Kbps | A | Telefone |
| 2 | < 2Mhz | 2Mbps | A/D | Telefone/Dados |
| 3 | 16Mhz | 10Mbps | D | LAN |
| 4 | 20Mhz | 20Mbps | D | LAN |
| 5 | 100Mhz | 100Mbps | D | LAN |
| 6 | 200Mhz | 200Mbps | D | LAN |
| 7 | 600Mhz | 600Mbps | D | LAN |

\*A= Analógico D = Digital

* 1. **Cabo fibra óptica**

Uma fibra óptica é feita de vidro ou plástico e utiliza luz para a transmissão de dados, ao contrário de par trançado e do cabo coaxial, que transmitem sinais elétricos

Um sistema de transmissão óptica tem três componentes: a fonte de luz, meio de transmissão e o detector. O transmissor recebe um sinal elétrico, converte o sinal e o transmite por pulsos de luz. O detector gera um sinal elétrico quando entra em contato com a luz, recuperando a informação.

A fibra óptica oferece uma enorme capacidade de transmissão, além disso, a fibra é imune a ruídos eletromagnéticos. O problema da atenuação tem um efeito bem menor que em outros meios, permitindo maiores distâncias. Porém, a seus componentes e instalação ainda são caras e mais difíceis de reparar caso haja rompimento no cabo.

A fibra óptica é formada por:

* Um núcleo de vidro (ou plástico): onde a luz é guiada, aplicando a angulação correta.
* O núcleo e envolvido por um revestimento (por exemplo, plástico) com índice de refração menor que o núcleo. A diferença de densidade deve ser tal que um feixe de luz movendo-se através do núcleo seja refletido de volta pela casca em vez de sofrer refração.
* Jaqueta: cobertura externa de plástico.
* Fios de Kevlar: para dar resistência ao cabo.
* Cobertura plástica externa: serve para proteção.

Tipos de fibra óptica:

* Multimodo: são fibras que possuem vários modos de propagação, o que faz com que os raios de luz percorram por diversos caminhos o interior da fibra;
* Monomodo: as fibras monomodo possuem um único modo de propagação. Estas fibras possuem um diâmetro e densidade menor do que as multimodo. Por possuírem suas dimensões mais reduzidas, as fibras monomodais têm a fabricação mais complexa e consequentemente são mais caras. Contudo, estas fibras apresentam atenuação mais baixa, permitindo transmissão de longas distâncias e uma maior capacidade de transmissão

1. **Hubs**

Os Hubs são dispositivos concentradores, responsáveis por centralizar a distribuição dos quadros de dados em redes fisicamente ligadas em estrelas. Funcionando assim como uma peça central, que recebe os sinais transmitidos pelas estações e os retransmite para todas as demais.

Existem vários tipos de hubs:

* Passivos: Concentradores de cabos que não possuem qualquer tipo de alimentação elétrica, funcionando como um espelho, refletindo os sinais recebidos para todas as estações a ele conectadas. Como ele apenas distribui o sinal, sem fazer qualquer tipo de amplificação, o comprimento total dos dois trechos de cabo entre um micro e outro, passando pelo hub, não pode exceder os 100 metros permitidos pelos cabos de par trançado.
* Ativos: São hubs que regeneram os sinais que recebem de suas portas antes de enviá-los para todas as portas. Funcionando como repetidores. Enquanto usando um Hub passivo o sinal pode trafegar apenas 100 metros somados os dois trechos de cabos entre as estações, usando um hub ativo o sinal pode trafegar por 100 metros até o hub, e após ser retransmitido por ele trafegar mais 100 metros completos.
* Inteligentes: São hubs que permitem qualquer tipo de monitoramento. Este tipo de monitoramento, que é feito via software capaz de detectar e se preciso desconectar da rede estações com problemas que prejudiquem o tráfego ou mesmo derrube a rede inteira; detectar pontos de congestionamento na rede, fazendo o possível para normalizar o tráfego; detectar e impedir tentativas de invasão ou acesso não autorizado à rede entre outras funções, que variam de acordo com a fabricante e o modelo do Hub.
* Empilháveis: Também chamado *stackable*, esse tipo de hub permite a ampliação do seu número de portas.

1. **Bridges**

Os repetidores transmitem todos os dados que recebem para todas as suas saídas, assim, quando uma máquina transmite dados para outra máquina presente no mesmo segmento, todas as maquinas da rede recebem esses dados, mesmo aquelas que estão em outro segmento. A ponte é um repetidor Inteligente. Ela tem a capacidade de ler e analisar os quadros de dados que estão circulando na rede. Com isso ela consegue ler os campos de endereçamentos MAC do quadro de dados. Fazendo com que a ponte não replique para outros segmentos dados que tenham como destino o mesmo segmento de origem. Outro papel que a ponte em principio poderia ter é o de interligar redes que possuem arquiteturas diferentes.

1. **Switches**

O switch é um hub que, em vez de ser um repetidor é uma ponte. Com isso, em vez dele replicar os dados recebidos para todas as suas portas, ele envia os dados somente para o micro que requisitou os dados através da análise da Camada de link de dados onde possui o endereço MAC da placa de rede do micro, dando a ideia assim de que o switch é um hub Inteligente, além do fato dos switches trazerem micros processadores internos, que garantem ao aparelho um poder de processamento capaz de traçar os melhores caminhos para o trafego dos dados, evitando a colisão dos pacotes e ainda conseguindo tornar a rede mais confiável e estável. De maneira geral a função do switch é muito parecida com a de um bridge, com a exceção que um switch tem mais portas e um melhor desempenho, já que manterá o cabeamento da rede livre. Outra vantagem é que mais de uma comunicação pode ser estabelecida simultaneamente, desde que as comunicações não envolvam portas de origem ou destino que já estejam sendo usadas em outras comunicações.

Existem duas arquiteturas básicas de Switches de rede: *cut-through* e *store-and-forward*: *Cut-through*: apenas examina o endereço de destino antes de reencaminhar o pacote. *Store-and-forward*: aceita e analisa o pacote inteiro antes de o reencaminhar. Este método permite detectar alguns erros, evitando a sua propagação pela rede.

1. **Diferença entre Hubs e Switche**s

Um hub simplesmente retransmite todos os dados que chegam para todas as estações conectadas a ele, como um espelho. Causando o famoso broadcast que causa muito conflitos de pacotes e faz com que a rede fica muito lenta. O switch ao invés de simplesmente encaminhar os pacotes para todas as estações, encaminha apenas para o destinatário correto pois ele identifica as maquinas pelo o MAC address que é estático. Isto traz uma vantagem considerável em termos desempenho para redes congestionadas, além de permitir que, em casos de redes, onde são misturadas placas 10/10 e 10/100, as comunicações possam ser feitas na velocidade das placas envolvidas. Ou seja, quando duas placas 10/100 trocarem dados, a comunicação será feita a 100M bits. Quando uma das placas de 10M bits estiver envolvida, será feita a 10M bits.

1. **Roteadores**

Roteadores são pontes que operam na camada de Rede do modelo OSI (camada três), essa camada é produzida não pelos componentes físicos da rede (Endereço MAC das placas de rede, que são valores físicos e fixos), mais sim pelo protocolo mais usado hoje em dia, o TCP/IP, o protocolo IP é o responsável por criar o conteúdo dessa camada. Isso significa que os roteadores não analisam os quadros físicos que estão sendo transmitidos, mas sim os datagramas produzidos pelo protocolo que no caso é o TCP/IP, os roteadores são capazes de ler e analisar os datagramas IP contidos nos quadros transmitidos pela rede. O papel fundamental do roteador é poder escolher um caminho para o datagrama chegar até seu destino. Em redes grandes pode haver mais de um caminho, e o roteador é o elemento responsável por tomar a decisão de qual caminho percorrer. Em outras palavras, o roteador é um dispositivo responsável por interligar redes diferentes, inclusive podendo interligar redes que possuam arquiteturas diferentes.

A grande diferença entre uma ponte e um roteador é que o endereçamento que a ponte utiliza é o endereçamento usado na camada de Link de Dados do modelo OSI, ou seja, o endereçamento MAC das placas de rede, que é um endereçamento físico. O roteador, por operar na camada de Rede, usa o sistema de endereçamento dessa camada, que é um endereçamento lógico. No caso do TCP/IP esse endereçamento é o endereço IP. Em redes grandes, a Internet é o melhor exemplo, é praticamente impossível para uma ponte saber os endereços MAC de todas as placas de rede existentes na rede. Quando uma ponte não sabe um endereço MAC, ela envia o pacote de dados para todas as suas portas. Agora imagine se na Internet cada roteador enviasse para todas as suas portas dados toda vez que ele não soubesse um endereço MAC, a Internet simplesmente não funcionaria, pelo excesso de dados. Devido a isso, os roteadores operam com os endereços lógicos, que trabalham em uma estrutura onde o endereço físico não é importante e a conversão do endereço lógico (Endereço IP) para o endereço físico (endereço MAC) é feita somente quando o datagrama chega à rede de destino. A vantagem do uso de endereços lógicos em redes grandes é que eles são mais fáceis de serem organizados hierarquicamente, isto é, de uma forma padronizada. Mesmo que um roteador não saiba onde esta fisicamente localizada uma máquina que possua um determinado endereço, ele envia o pacote de dados para um outro roteador que tenha probabilidade de saber onde esse pacote deve ser entregue (roteador hierarquicamente superior). Esse processo continua até o pacote atingir a rede de destino, onde o pacote atingira a máquina de destino. Outra vantagem é que no caso da troca do endereço físico de uma máquina em uma rede, a troca da placa de rede defeituosa não fará com que o endereço lógico dessa máquina seja alterado. É importante notar, que o papel do roteador é interligar redes diferentes (redes independentes), enquanto que papel dos repetidores, hub, pontes e switches são de interligar segmentos pertencentes a uma mesma rede.

* 1. **Protocolos**

Os roteadores possuem uma tabela interna que lista as redes que eles conhecem, chamada tabela de roteamento. Essa tabela possui ainda uma entrada informando o que fazer quando chegar um datagrama com endereço desconhecido. Essa entrada é conhecida como rota default ou default gateway. Assim, ao receber um datagrama destinado a uma rede que ele conhece, o roteador envia esse datagrama a essa rede, através do caminho conhecido. Caso ele receba um datagrama destinado a uma rede cujo caminho ele não conhece, esse datagrama é enviado para o roteador listado como sendo o default gateway. Esse roteador irá encaminhar o datagrama usando o mesmo processo. Caso ele conheça a rede de destino, ele enviará o datagrama diretamente a ela. Caso não conheça, enviará ao roteador listado como seu default gateway. Esse processo continua até o datagrama atingir a sua rede de destino ou o tempo de vida do datagrama ter se excedido o que indica que o datagrama se perdeu no meio do caminho. As informações de rotas para a propagação de pacotes podem ser configuradas de forma estática pelo administrador da rede ou serem coletadas através de processos dinâmicos executando na rede, chamados protocolos de roteamento. Protocolos de roteamento são protocolos que trocam informações utilizadas para construir tabelas de roteamento. É importante distinguir a diferença entre protocolos de roteamento (*routing protocols*) e protocolos roteados (*routed protocols*). Protocolo roteado é aquele que fornece informação adequada em seu endereçamento de rede para que seus pacotes sejam roteados, como o TCP/IP e o IPX.

Um protocolo de roteamento possui mecanismos para o compartilhamento de informações de rotas entre os dispositivos de roteamento de uma rede, permitindo o roteamento dos pacotes de um protocolo roteado. Um protocolo de roteamento usa um protocolo roteado para trocar informações entre dispositivos roteadores. Exemplos de protocolos de roteamento são o RIP (com implementações para TCP/IP e IPX) e o EGRP.

* 1. **Roteamento estático e roteamento dinâmico**

A configuração de roteamento de uma rede específica nem sempre necessita de protocolos de roteamento. Existem situações onde as informações de roteamento não sofrem alterações, por exemplo, quando só existe uma rota possível, o administrador do sistema normalmente monta uma tabela de roteamento estática manualmente. Algumas redes não têm acesso a qualquer outra rede e portanto não necessitam de tabela de roteamento. Dessa forma, as configurações de roteamento mais comuns são:

* Roteamento estático: uma rede com um número limitado de roteadores para outras redes pode ser configurada com roteamento estático. Uma tabela de roteamento estático é construída manualmente pelo administrador do sistema, e pode ou não ser divulgada para outros dispositivos de roteamento na rede. Tabelas estáticas não se ajustam automaticamente a alterações na rede, portanto devem ser utilizadas somente onde as rotas não sofrem alterações. Algumas vantagens do roteamento estático são a segurança obtida pela não divulgação de rotas que devem permanecer escondidas; e a redução do overhead introduzido pela troca de mensagens de roteamento na rede.
* Roteamento dinâmico: redes com mais de uma rota possível para o mesmo ponto devem utilizar roteamento dinâmico. Uma tabela de roteamento dinâmico é construída a partir de informações trocadas entre protocolos de roteamento. Os protocolos são desenvolvidos para distribuir informações que ajustam rotas dinamicamente para refletir alterações nas condições da rede. Protocolos de roteamento podem resolver situações complexas de roteamento mais rápida e eficientemente que o administrador do sistema. Protocolos de roteamento são desenvolvidos para trocar para uma rota alternativa quando a rota primária se torna inoperável e para decidir qual é a rota preferida para um destino. Em redes onde existem várias alternativas de rotas para um destino devem ser utilizados protocolos de roteamento.
  1. **Protocolos de roteamento**

Todos os protocolos de roteamento realizam as mesmas funções básicas, eles determinam a rota preferida para cada destino e distribuem informações de roteamento entre os sistemas da rede. Como eles realizam estas funções, em particular eles decidem qual é a melhor rota, é a principal diferença entre os protocolos de roteamento.

Tipos de Protocolos:

IGP (*interior gateway protocol*) - Estes são utilizados para realizar o roteamento dentro de um Sistema Autônomo. Existem vários protocolos IGP:

* RIP (*Routing Information Protocol*)
* IGRP (*Interior Gateway Routing Protocol*)
* Enhanced IGRP
* OSPF (*Open Shortest Path First*)
* IS-IS *(Intermediate System-to-Intermediate System*)

EGP (exterior gateway protocol) - Estes são utilizados para realizar o roteamento entre Sistemas Autônomos diferentes. É dividido em:

* EGP (*Exterior Gateway Protocol*)
* BGP (*Border Gateway Protocol*)