

1 - Camada de Enlace

A camada de Enlace descreve características e conceitos relativos à organização dos bits em conjuntos significativos de dados, como endereçá-los ao dispositivo de destino e como controlar esta comunicação. Associados a esta camada estão os conceitos de:

- Topologias lógicas
- Controle de acesso ao meio
- Endereçamento MAC
- Serviços de conexão
- Endereçamento de Protocolos da camada de rede
- Detecção de erros e descarte de pacotes.

Esta camada está subdividida em duas subcamadas.

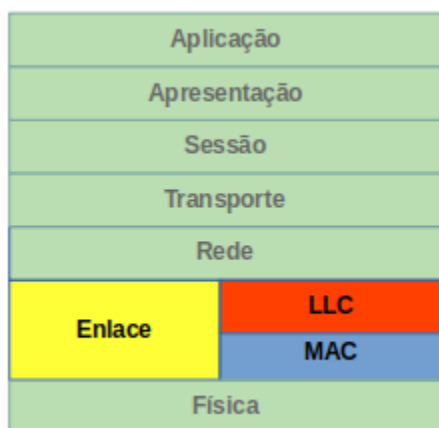


Fig. 1 Subcamadas da camada de Enlace fonte: o autor

subcamada MAC - Mídia Access Control (Controle de Acesso ao Meio) - Descreve as topologias lógicas, os procedimentos de acesso ao meio e endereçamento. Já a

subcamada LLC - Logical Link Control (Controle Lógico do Link - Enlace) - Descreve os serviços de conexão (controle da comunicação) no enlace de dados.

Tecnologias da camada de Enlace

Os protocolos da camada de enlace para redes de locais - LANs e WLANs, e redes metropolitanas - MAN são determinados pelo IEEE em seu comitê 802. A figura 2 apresenta um quadro esquemático dos principais protocolos dessa família.

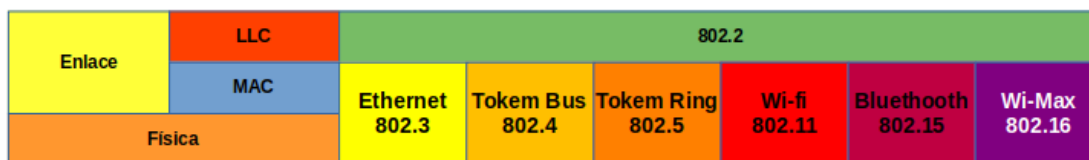
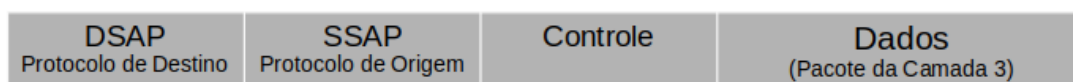


Fig. 2 - Principais protocolos da família de protocolos IEEE802

OBS: Os protocolos do IEEE além de descreverem as funções relacionadas ao controle de acesso ao meio também descrevem as características físicas das interfaces. Por isso estão mostrados na figura associados também a camada física do modelo OSI.

1.1. Subcamada LLC

Esta subcamada é definida pelo protocolo IEEE 802.2, apresentado na figura 3.



LLC with SNAP Header

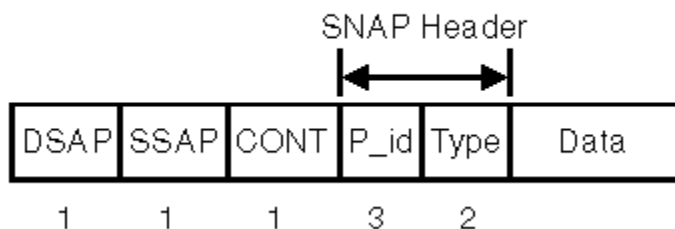


Fig. 3 Quadro IEEE 802.2 e 802.2 SNAP

Ela faz a interface entre o software de rede nas camadas superiores e o hardware do dispositivo nas camadas inferiores, abstraindo das camadas superiores a complexidade da rede física. Permite a multiplexação de protocolos da camada de rede (ex. IPv4 e IPv6) na camada de enlace, o quadro (DSAP/SSAP) identifica qual protocolo de camada de rede está sendo usado para o quadro da subcamada MAC (Endereçamento de serviço). Além disso, ela é responsável pela implementação de serviços de conexão (controle da conexão, controle de erro e controle de fluxo) na camada de enlace.

Destaque: As implementações das redes locais e metropolitanas geralmente não utilizam os serviços de conexão da camada de enlace. Os aspectos relacionados a serviços de conexão serão melhor estudados na unidade 5 - Camada de Transporte.

1.2. Subcamada MAC

Esta subcamada é implementada por vários protocolos (IEEE 802.3, 802.11 ou 802.15) no hardware das interfaces de rede dos dispositivos, ela é responsável pelo encapsulamento de dados e controle de acesso à mídia, além de fornecer endereçamento físico - MAC integrando várias tecnologias de camada física. Nas redes locais suas principais responsabilidades são:

- **Topologias Lógicas** - Definem como os dispositivos enxergam a rede, isto é, como eles se conectam logicamente, em outras palavras, como os dados trafegam entre estes dispositivos.
- **Controle de acesso ao meio** - Permitindo que vários dispositivos se comuniquem através de uma mídia compartilhada e controle de fluxo (half/full-duplex).
- **Enquadramento** - Fornece delimitadores importantes para identificar campos dentro de um quadro, esses bits também possibilitam a sincronização entre os nós de transmissão e de recepção.
- **Endereçamento** - Fornece endereçamento de origem e destino para transportar o quadro da Camada 2 entre dispositivos na mesma mídia compartilhada.
- **Deteção de erro** - Inclui um trailer (rodapé) usado para detectar erros de transmissão.

2. Características da subcamada MAC

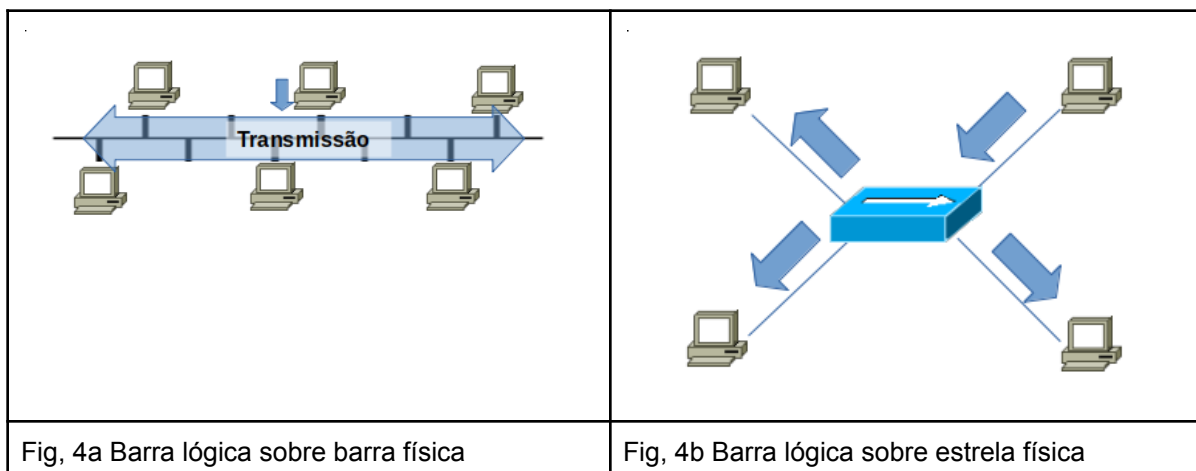
2.1. Topologias Lógicas

Enquanto topologias físicas definem o layout físico da rede, isto é, como o meio de comunicação entre os dispositivos é disponibilizado, as topologias lógicas determinam o caminho dos dados entre estes dispositivos. Elas podem diferir da topologia física de forma que uma topologia física em estrela pode, por exemplo, apresentar uma topologia lógica em barra ou anel.

2.1.1. Topologia em Barra

Nesta topologia a informação é transmitida a todos os dispositivos da rede ao mesmo tempo, sendo recebido por todos cabendo ao dispositivo receptor identificar seu endereço no pacote transmitido recebendo ou descartando a informação. Podem ser implementadas tanto por uma barra física com cabos coaxiais, nesse caso os

dispositivos são encadeados e terminados de alguma forma em cada extremidade, como através de uma física em estrela por meio de repetidores (Hubs), conforme mostrado nas figuras 4a e 4b.



Na topologia em barra lógica os dispositivos disputam o meio de transmissão, nesse caso se dois ou mais dispositivos transmitirem ao mesmo tempo, haverá uma mistura dos sinais transmitidos. A esse fenômeno dá-se o nome de colisão.

2.1.2. Topologia em Anel

Nesta topologia 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. Podem ser implementadas em uma topologia física de anel ou estrela (Token Ring - IEEE 802.5 ou FDDI - ANSI - ASC X3T9), e em barra (Token Bus - IEEE 802.4), conforme apresentado nas figuras 5a e 5b.

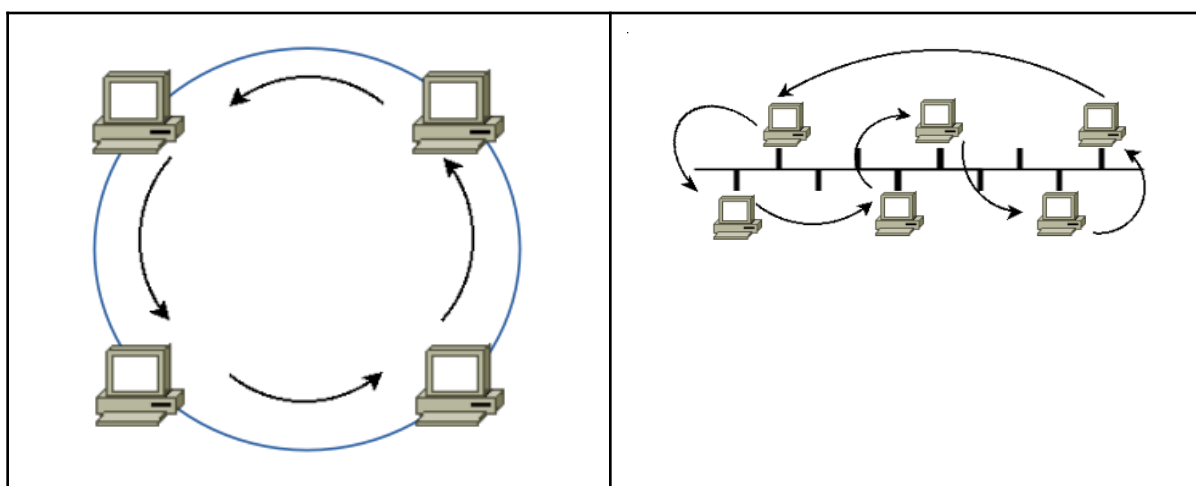


Fig. 5a Anel lógico sobre anel físico

Fig. 5a Anel lógico sobre barra física

Na topologia em anel não, mesmo quando implementada em um barra não há colisão, pois apenas um dispositivo transmite por vez.

2.2. Métodos de controle de acesso ao meio

A maioria das implementações de LANs e WLANa são topologias tipo multiponto, onde vários dispositivos compartilham o mesmo meio de transmissão, logo é necessário mecanismos que garantam o acesso ordenado ao meio de transmissão - controle de acesso ao meio. Há basicamente dois tipos de protocolos: os de acesso determinístico ou controlado onde cada dispositivo sabe exatamente quando pode transmitir e de acesso aleatório ou de contenção, onde dispositivos disputam entre si o controle do meio para transmitir.

2.2.1. Acesso baseado em Contenção

Em redes multiponto baseadas em contenção, todos os nós operam em half-duplex, competindo pelo uso do meio e apenas um dispositivo pode enviar seus dados por vez. Se mais de um dispositivo transmitir simultaneamente os sinais serão misturados ocorrendo o que chamamos de colisão. Como exemplos de métodos de acesso baseados em contenção podemos listar:

- **CSMA/CD** - Acesso múltiplo por detecção de portadora com detecção de colisão usado em LANs Ethernet de topologia lógica de barramento legada, isto inclui as redes Ethernet IEEE802.3 - 10base2 e 10base5 que utilizam cabos coaxiais e as redes Ethernet IEEE802.3 - 10/100baseT que utilizam concentradores (Hubs).
- **CSMA/CA** - Acesso múltiplo por detecção de portadora com prevenção de colisão usado em LANs sem fio.

2.2.2. Acesso Controlado

Em uma rede multiponto determinística, cada nó tem seu próprio tempo para usar o meio. Esse tipo são ineficientes porque um dispositivo deve aguardar sua vez para acessar o meio e atualmente só são encontradas em tecnologias legadas. Como exemplo de protocolo de acesso ao meio determinístico temos o Token Passing utilizados nas redes Token Ring - IEEE 802.5, FDDI - ANSI - ASC X3T9 Token Bus - IEEE 802.4.

2.2.3. CSMA/CD - Carrier Sense Multiple Access/Collision Detection

Esse protocolo opera no modo half-duplex, isto é, apenas um dispositivo pode

transmitir por vez. Quando um dispositivo deseja transmitir, ele verifica, "escuta", se o meio está livre, detectando a existência da portadora no meio (carrier sense). Caso o meio esteja livre, a estação transmite, se o meio estiver ocupado, ela persistirá na "escuta" até que este seja desocupado para efetuar a transmissão. Após transmitir o dado o dispositivo deverá continuar "escutando" o meio para detectar a ocorrência de colisão (collision detection). Ao detectar uma colisão os dispositivos envolvidos na colisão calculam um tempo aleatório (contenção ou backoff) para tentar a retransmissão, sendo que uma nova colisão pode ocorrer gerando uma nova contagem e uma nova tentativa de transmissão.

OBS: O tempo durante o qual o dispositivo deve permanecer "escutando" o barramento é função do tempo de propagação do sinal no meio, de forma que a observância das distâncias máximas estabelecidas pelos padrões, devem ser seguidas à risca, de forma a não prejudicar a eficiência da rede.

2.2.4. CSMA/CA - Carrier Sense Multiple Access/Collision Avoidance

Este protocolo é utilizado principalmente em redes sem fio e também opera no modo half-duplex, logo, apenas um dispositivo pode transmitir por vez, além disso precisa lidar com aspectos como o fato de que nem sempre os dispositivos da rede estão no alcance de transmissão um do outro.

2.3. Enquadramento

Enquadramento é o mecanismo que organiza os dados para que possam ser representados através de uma sinalização no meio físico. Nas redes Ethernet isso é feito através da definição do quadro Ethernet.

O Quadro Ethernet é uma organização lógica, um padrão, cujo tamanho mínimo é de 64 bytes e o máximo de 1518 bytes, incluindo o campo de dados (o pacote da camada 3), e os campos de endereços de origem e destino e o campo FCS (Frame Check Sequence), que permite a detecção de erro. Os campos de preâmbulo e delimitação do quadro não são incluídos ao descrever o tamanho do quadro.

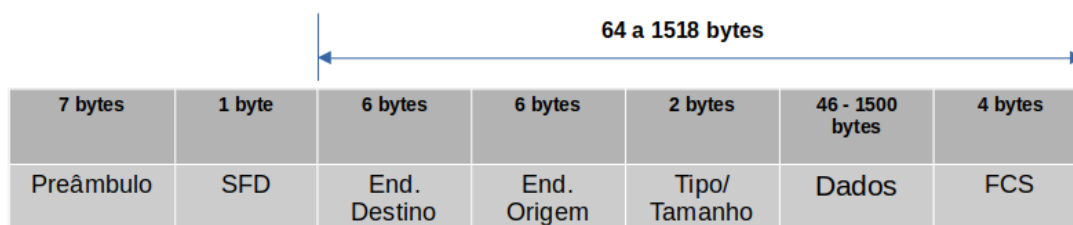


Fig. 6 - Quadro Ethernet

Tabela 1 - Campos do quadro Ethernet

Campo	Descrição
Preâmbulo (7 bytes)	Utilizado para sincronização entre o transmissor e receptor.
SFD - Delimitador Início de Quadro (1 byte)	Identifica para o receptor o início efetivo do quadro.
Endereço MAC de Destino (6 bytes)	Identifica o destinatário desejado. Permite ao receptor determinar se um quadro é endereçado a ele. O endereço MAC do quadro é comparado com o endereço MAC do dispositivo receptor, caso haja correspondência, o receptor aceita o quadro. Este endereço pode ser de unicast, multicast ou broadcast.
Endereço MAC de Origem (6 bytes)	Identifica a placa de rede (NIC) do transmissor.
Tipo/Comprimento (2 bytes)	Identifica o protocolo da camada superior encapsulado no quadro Ethernet. Os valores comuns são, em hexadecimal, 0x800 para IPv4, 0x86DD para IPv6 e 0x806 para ARP. Nota: Você também pode ver este campo referido como EtherType, Tipo ou Comprimento.
Dados (46 - 1500 bytes)	Este campo contém os dados encapsulados da camada superior, uma PDU de Camada 3, normalmente, um pacote IPv4 ou IPv6. Como um quadro deve ter um tamanho mínimo de 64 bytes, se um pacote da camada 3 muito pequeno for encapsulado, bits adicionais (de enchimento) chamados PAD são usados para aumentar o tamanho do quadro para este tamanho mínimo.
FCS – Sequência de verificação do Quadro (4 bytes)	Usado para detectar erros em um quadro. Ele utiliza uma verificação de redundância cíclica (CRC). O dispositivo de envio calcula e inclui o resultado de um CRC no campo FCS do quadro. O dispositivo receptor recebe o quadro e calcula o CRC do quadro recebido. Se o cálculo corresponder ao valor do FCS recebido, significa que não houve erro, caso contrário é uma indicação de que os dados foram alterados e o quadro recebido é descartado.

2.3. Endereçamento

O endereço MAC identifica os dispositivos físicos, isto é, as placas de rede (NIC) de origem e destino dentro de um enlace de rede local, é um endereço de 48 bits (6 bytes) representado através de 12 dígitos hexadecimais (cada 02 dígitos representa 01 byte)

1111	1111	1111	1111	1111	1111	1111	1111	1111	1111	1111	1111
F	F	F	F	F	F	F	F	F	F	F	F
FF		FF		FF		FF		FF		FF	

48 bits
12 Hexadecimais
6 bytes

End. MAC = 02:42:21:45:09:AE (Hex)
= 00000100100001000101100010001010000100110101110 (Bin)

02		42		2C		45		09		AE		6 bytes
0	2	4	2	2	C	4	5	0	9	A	E	12 Hexadecimais
0000	0010	0100	0010	0010	1100	0100	0101	0000	1001	1010	1110	48 bits

Fig. 7 Endereço MAC e sua representação.

Cada dispositivo deve ter seu endereço MAC exclusivo, todos os fornecedores de placas de rede (NIC) Ethernet devem ser registrados no IEEE e, a partir daí, receber um identificador único para sua organização de 24 bits ou 3 bytes, chamado (OUI - Organizationally Unique Identifier). Assim um endereço MAC é formado pelo OUI do fabricante (3 bytes e um número sequencial que identifica o dispositivo para aquele fabricante).

02	42	2C	02	42	2C
OUI			ID da Interface		

Fig. 8 - Formação do Endereço MAC para cada fabricante

Importante: É responsabilidade do fabricante garantir que nenhum de seus dispositivos tenha um endereço MAC duplicado, entretanto, é possível que endereços MAC duplicados sejam encontrados devido a erros de fabricação, ou em implementação de máquinas virtuais ou mesmo por alterações feitas diretamente no dispositivo usando uma das várias ferramentas de software existentes no mercado ou embutidas no próprio sistema operacional.

2.3.1. Tipos de endereços MAC Ethernet

- **Endereçamento MAC Unicast** - É o endereçamento exclusivo usado quando

um quadro é enviado de um único dispositivo de transmissão para um único dispositivo de destino. Nesse caso o endereço de origem recebe o MAC da estação transmissora e o de destino o MAC da estação receptora.

- **Endereçamento MAC Broadcast** - Uma transmissão Broadcast é uma transmissão de um para todos os dispositivos conectados no mesmo segmento de rede, assim um endereço de broadcast tem como endereço de origem o MAC da estação transmissora e o de destino o MAC FF:FF:FF:FF:FF:FF. Este endereço corresponde a todos os bits do endereço de destino iguais ao binário 1 (um). Por padrão este quadro será admitido por todos os dispositivos no barramento e difundido para todas as portas do switch exceto para a porta de origem do quadro.
- **Endereçamento MAC Multicast** - Uma transmissão em multicast é uma transmissão de um para vários, quando um quadro de multicast Ethernet é recebido é processado apenas pelas estações na LAN Ethernet que pertencem ao mesmo grupo de multicast. Um endereço de multicast Ethernet tem como endereço de origem o MAC da estação transmissora e o de destino depende de certas condições listadas a seguir.
 - Um endereço MAC de destino 01-00-5E quando os dados encapsulados são um pacote multicast IPv4 e um endereço MAC de destino de 33-33 quando os dados encapsulados são um pacote multicast IPv6.
 - Há outros endereços MAC de destino multicast reservados para quando os dados encapsulados não são IP, como STP (Spanning Tree Protocol) e LLDP (Link Layer Discovery Protocol), etc

3. Ethernet Comutada

As duas tecnologias de redes locais mais utilizadas são Ethernet (IEEE 802.3) e WLAN (IEEE 802.11). A tecnologia Ethernet (IEEE802.3) suporta larguras de banda de até 100 Gbps, que somado ao seu baixo custo explica sua popularidade. Desde sua criação esta tecnologia vem evoluindo, desde redes de e meio físico compartilhado com topologia em barra com cabo coaxial (10base2 e 10base5), depois redes com topologia física em estrela e barra lógica, baseadas em Hubs (10baseT), até o advento dos switches (comutadores) que eliminaram de vez os domínios de colisão, permitindo as transmissões full duplex e velocidades cada vez maiores com novos esquemas de sinalização. É sobre essa tecnologia que vamos aprender agora.

3.1. Switches Ethernet de camada 2

3.1.1. Ethernet compartilhada

Uma rede Ethernet na sua origem é uma rede baseada em contenção, que usa o protocolo CSMA/CD como método de acesso, nela as estações disputam o acesso ao meio para transmitir seus dados, se duas ou mais estações transmitem ao mesmo tempo há a ocorrência de colisões, que cresce com o número de estações conectadas ao barramento e com o tráfego total da rede.

A adoção em maior escala desta tecnologia, fez com que os segmentos de rede crescessem aumentando o que chamamos de domínio de colisão com muitas máquinas e muito tráfego, fazendo com que o número de colisões no segmento aumentasse até o ponto de colapsar a rede.

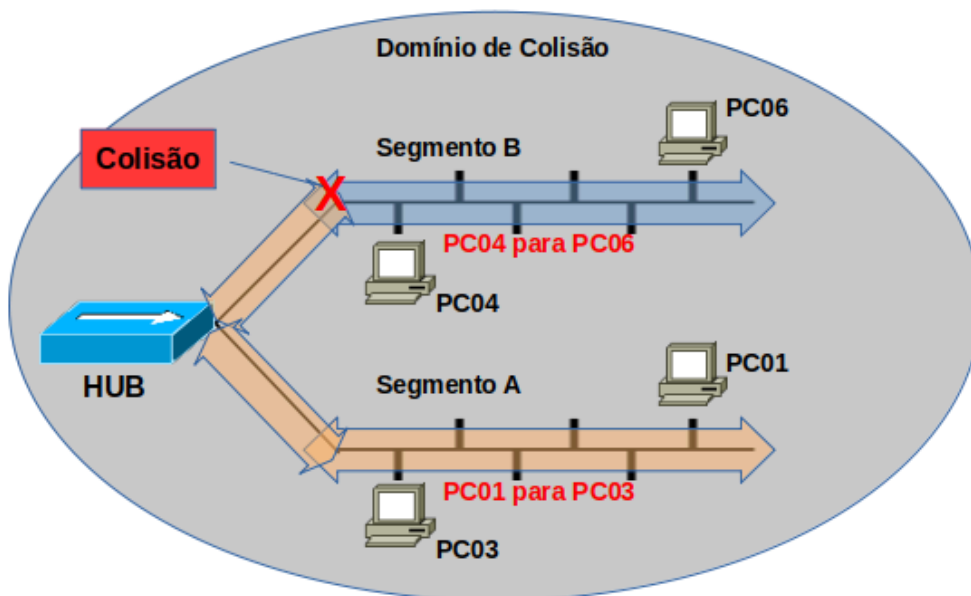


Fig. 9 Ethernet compartilhada

Na figura podemos ver que a transmissão com origem no PC01 e destino no PC03 no segmento A da rede colide com a transmissão com origem no PC04 e destino no PC06 no segmento B, pois mesmo em segmentos diferentes pertencem ao mesmo domínio de colisão, pois a rede se comporta como uma barra única.

3.1.2. A segmentação da rede com Bridges (Pontes)

Fez-se necessário então um mecanismo que reduzisse estes domínios de colisão restringindo o tráfego ao seu segmento local e permitindo o tráfego para outros segmentos apenas quando necessário. O primeiro mecanismo projetado foram as

Bridges (Pontes). Uma Bridge é um dispositivo de camada 2 que toma decisões de encaminhamento de quadros com base no endereço MAC de destino.

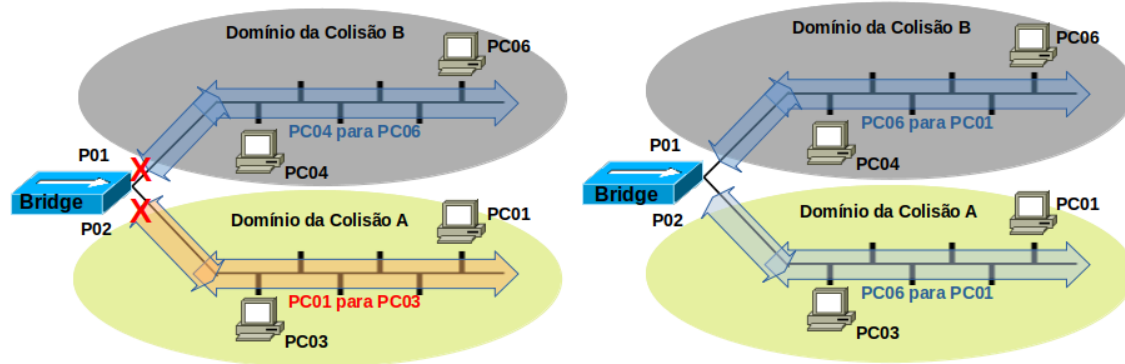


Fig. 10 Segmentação de redes com bridges

Na figura podemos ver que a bridge divide a rede em dois domínios de colisão e que os quadros com origem no PC01 e destino no PC03 no segmento A da rede e os quadros com origem no PC04 e destino no PC06 no segmento B não são replicados para outros segmentos, pois as portas da Bridge descartam os quadros restringindo este tráfego aos seus respectivos domínios de colisão. Por outro lado o tráfego com origem no PC06 e destino no PC01 é recebido pela porta P01 da Bridge e encaminhado para a porta P02.

3.2. Switches Ethernet - Noções básicas

Uma Ethernet comutada é a implementação desta tecnologia com base em switches. Um switch Ethernet de camada 2, assim como as Bridges, usa os endereços MAC para tomar decisões de encaminhamento dos quadros. A principal diferença entre esses dois dispositivos é que nas bridges isso era feito por software e nos switches é feito no hardware dos mesmos, graças aos processadores ASICs (Application Specific Integrated Circuits), que são a tecnologia base no projeto dos switches.

Um switch Ethernet, ao contrário do Hub, examina sua tabela de endereços MAC, também chamada memória de conteúdo endereçável (CAM - Content Address Memory), para tomar uma decisão de encaminhamento para cada quadro recebido.

Ao ser ligado a tabela de endereços MAC do switch inicia vazia.

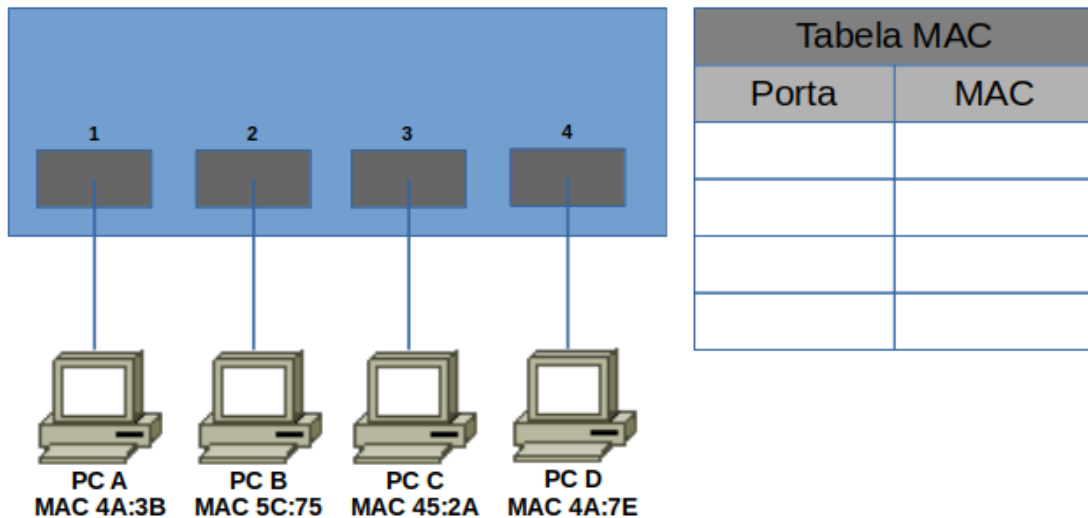


Fig. 11 - Tabela de endereços MAC vazia.

3.2.1. Aprendizado

O switch preenche a tabela de endereços MAC dinamicamente examinando o endereço MAC de origem dos quadros recebidos em cada uma das portas. Isso é feito examinando o endereço MAC de origem do quadro e o número da porta em que o quadro entrou no switch. Se o endereço MAC de origem não consta na tabela, é adicionado juntamente com o número da porta de entrada.

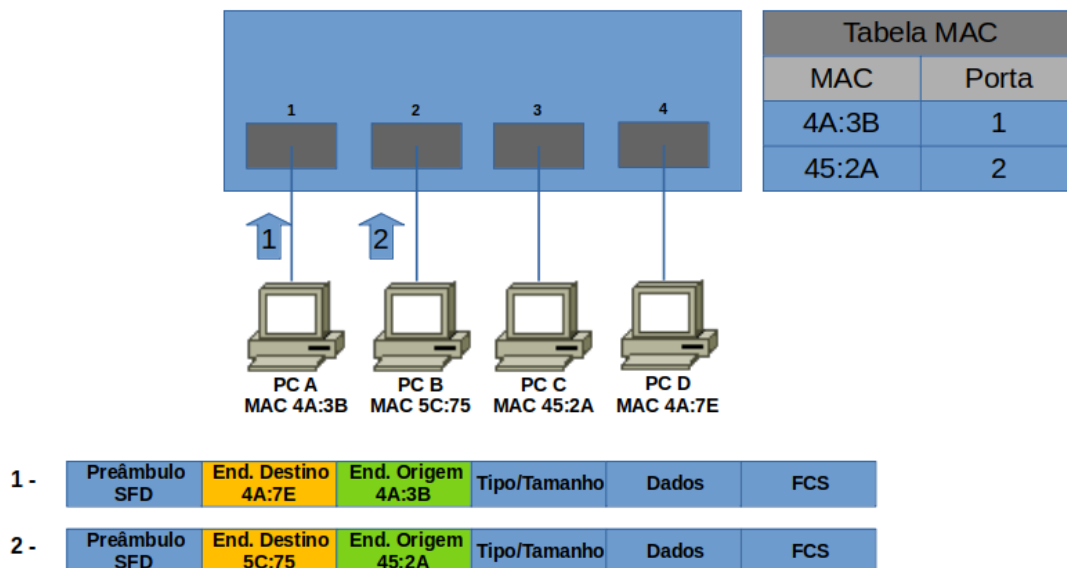


Fig.12 - Aprendizado e preenchimento da tabela de endereços MAC

Vemos que os endereços MAC de origem dos quadros são aprendidos à medida que os quadros entram pelas portas do switch e a tabela de endereços MAC é preenchida associando o endereço MAC de origem do quadro à porta de entrada do mesmo. Se o endereço MAC de origem existir, o switch atualizará o temporizador de atualização para essa entrada na tabela. Por padrão, a maioria dos switches Ethernet mantém uma entrada na tabela por 5 minutos.

3.2.2. Encaminhamento

O switch encaminha os quadros procurando uma correspondência entre o endereço MAC de destino do quadro e uma entrada na tabela de endereços MAC. Se o endereço MAC de destino não estiver na tabela, o switch “inunda”, isto é, o switch encaminhará o quadro para todas as portas, exceto a porta de entrada do quadro.

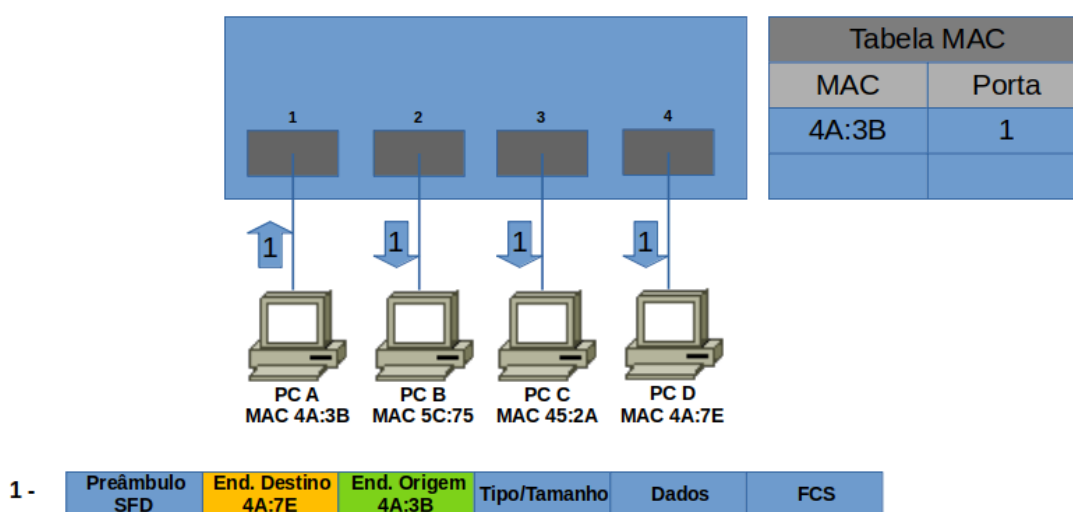


Fig. 13 - Encaminhamento de pacotes - MAC não consta da tabela.

Aqui como o endereço de destino do quadro que chega ao switch pela porta 1 não consta na tabela de endereços MAC o switch “inunda”.

Porém, se o endereço MAC de destino estiver na tabela, ele encaminhará o quadro pela porta correspondente.

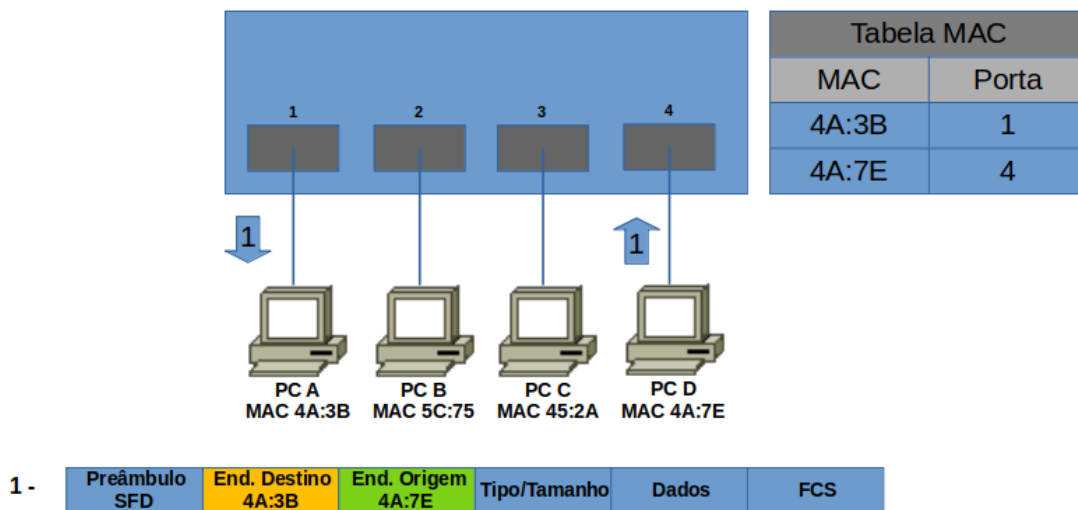


Fig. 14 - Encaminhamento de pacotes - MAC consta da tabela.

Aqui o quadro com origem no PC D, e com destino no PC A recebido na porta 4, é encaminhado diretamente para a porta 1 associado ao MAC 4A:3B enquanto o MAC 4A:7E de origem é aprendido e adicionado à tabela de endereços MAC do switch.

3.2.3. Métodos de Encaminhamento de Quadros

- **Switching store-and-forward** - Neste método o switch recebe o quadro inteiro, armazena em memória e faz a verificação de erro. Se o quadro está íntegro, o switch procura na tabela de endereços MAC o endereço de destino, que determina a interface de saída. Em seguida, o quadro é encaminhado para fora da porta correspondente.
- **Switching cut-through** - Neste método o switch encaminha o quadro antes de ser totalmente recebido, encaminhando imediatamente o quadro depois de ler o endereço de destino (Fast-forward),
- **Fragment-free** - O switch armazena os primeiros 64 bytes do quadro antes de encaminhá-lo, isto porque a maioria dos erros e das colisões de rede ocorre durante os primeiros 64 bytes.

Switches store-and-forward garantem maior integridade, pois determinam se um quadro tem erros antes propagá-lo e promovendo o descarte, o que reduz o consumo de largura de banda por dados corrompidos. Estes switches são necessários em redes onde a qualidade de serviço (QoS) é exigida como em redes convergentes onde a classificação de quadros para priorização de tráfego é necessária. Já os switches

cut-through são mais rápidos, pois retêm os quadros por menos tempo mas dependem da confiabilidade do meio físico. O switching fragment-free procura um meio termo entre a alta latência e a alta integridade do switching store-and-forward e a baixa latência e a integridade reduzida do switching fast-forward.

Importante: Alguns switches podem adaptar o método de encaminhamento em função das taxas de erro medidas na rede.

3.2.4. Buffers de Memória

Tabela 2 - Tipos de buffers de memória utilizados no switches	
Método	Descrição
Memória por porta	<ul style="list-style-type: none">• Os quadros são armazenados em filas vinculadas às portas de entrada e saída.• Um quadro só é transmitido para a porta de saída quando todos os quadros à frente na fila foram transmitidos com sucesso.• É um único quadro atrasar a transmissão de todos os os quadros na memória devido a uma porta de destino ocupada, isso ocorre mesmo que os outros quadros possam ser transmitidos para portas de destino abertas.
Memória compartilhada	<ul style="list-style-type: none">• Armazena todos os quadros em um buffer de memória compartilhado por todas as portas do switch e a quantidade de memória necessária para cada porta é alocada dinamicamente.• Os quadros no buffer são vinculados dinamicamente à porta de destino, permitindo que um que seja recebido em uma porta e, em seguida, transmitido em outra porta, sem movê-lo para uma fila diferente.

3.2.4. Negociação automática

Permite que dois dispositivos negociem automaticamente as melhores capacidades de velocidade e duplex. Assim, cada interface individualmente pode negociar operar em full-duplex ou half-duplex e em 10 Mbps ou 100 Mbps ou 1 Gbps, porém portas Gigabit Ethernet só operam em modo full-duplex.

Importante: A incompatibilidade duplex, isto é, quando uma ou ambas as portas em um link são redefinidas e o processo de negociação automática não resulta nos dois parceiros de link com a mesma configuração, é uma das causas mais comuns de problemas de desempenho nos links Ethernet 10/100 Mbps. Ocorre quando uma porta no link opera em half-duplex, enquanto a outra porta opera em full-duplex.

3.2.4. Auto MDIX

Detectam automaticamente se o cabo usado é direto ou crossover.

3.3. Redes Hierárquicas

A adoção em larga escala dos switches, devido principalmente à redução do custo de fabricação, permitiu o crescimento exponencial das redes locais e do número de dispositivos conectados, em adição permitiu a convergência de novos serviços para rede de dados, como a convergência de voz e vídeo. Isso trouxe novos desafios ao projeto de rede, que além de largura de banda e baixa latência, precisou lidar aspectos como qualidade de serviço, alta disponibilidade, tolerância a falhas e segurança. A primeira resposta a esse desafio vem com o conceito de redes hierárquicas.

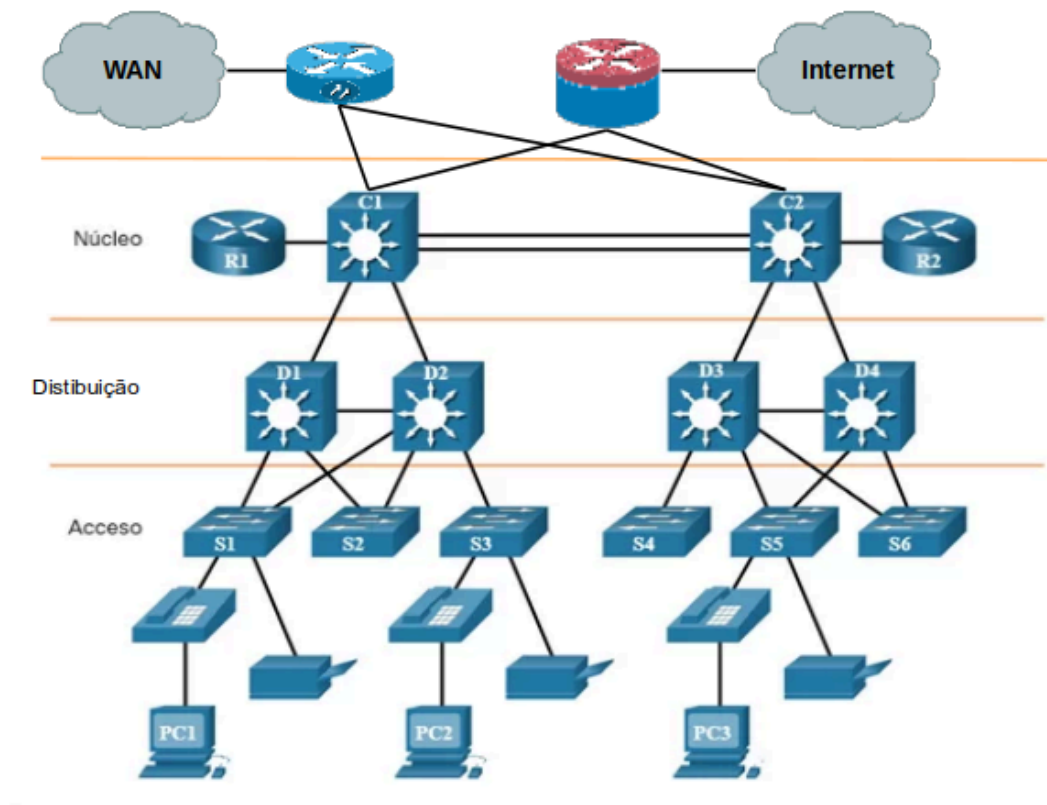


Fig. 15 - Rede Hierárquica fonte: o autor adaptado de <https://ccna.network/redes-hierarquicas/>

Estas redes propõem um projeto em três camadas introduzindo modularidade permitindo maior resiliência, flexibilidade e escalabilidade para fornecer serviços de rede críticos e convergentes.

- **Camada de Acesso** Essa camada provê conectividade para os dispositivos finais (ETDs), como PCs, impressoras e telefones IP. Nesta camada vamos encontrar switches e pontos de acesso wireless (AP), um dos principais objetivos é prover controle de acesso ao meio físico da rede.
- **Camada de Distribuição** - Essa camada é responsável por agregar os dados recebidos dos switches da camada de Acesso e transmiti-los para a camada de Núcleo. Essa camada controla o fluxo do tráfego agregando funções de roteamento entre VLANs.
- **Camada de Núcleo (Core)** - Esta camada é o backbone de alta velocidade das redes interconectadas. Provê conectividade entre os dispositivos da camada de distribuição, com alta disponibilidade e redundância. Também provê acesso à redes externas e Internet.

OBS: Em redes menores, é comum a junção da camada de distribuição e da camada de núcleo em uma única camada, que chamamos de núcleo ou Backbone colapsado.