Unidade 6
A camada de enlace

Nesta unidade, será analisada a camada de enlace. Os protocolos e os métodos de acesso serão comparados. Você verá que a camada de enlace está relacionada aos protocolos de redes locais. Ao final da unidade, voce poderá:

- Perceber as diferenças entre os métodos de acesso ao meio
- Entender o endereçamento MAC
- Entender os campos dos quadros Ethernet e discernir as funções de cada campo dentro do envelope digital
- Entender o funcionamento do protocolo ARP

Na Net-pizza, a camada de enlace funciona como os veículos de transporte de pizza. Os diferentes tipos de veículos podem ser comparados com as diferentes tecnologias da camada 2: ATM, SONET, ADSL, Ethernet, Token Ring, Frame Relay. Essas tecnologias possuem formatos próprios para transportar os dados e, como voce já viu, podem ser comparadas a envelopes digitais. A documentação das pizzas (notas fiscais, pedidos) transportadas nos veículos podem ser vistas como os cabeçalhos dos quadros ou *frames*.

Contêm informações sobre o conteúdo, quantidades, endereços de origem e destino.

Seção 1 – Estrutura e Serviços

Como é a segunda camada do modelo OSI, a camada de enlace (*Data Link Layer*) fornece serviços para a cada de rede logo acima. Os protocolos da camada de enlace são utilizados para transportar um datagrama sobre um segmento de rede, que pode ser visto como **um enlace individual**.

Na net-pizza, os furgões são requisitados pelo pessoal da expedição/recebimento de materiais (que fazem o papel dos roteadores, escolhendo os melhores caminhos até o destino)

A camada de enlace utiliza os serviços da camada física (os dados serão transformados em sinais eletricos, ópticos ou outros – rádio, laser, infra-vermelho). Alguns dos serviços oferecidos para a camada de rede são: enquadramento, sequenciação, controle de fluxo, detecção de erros.

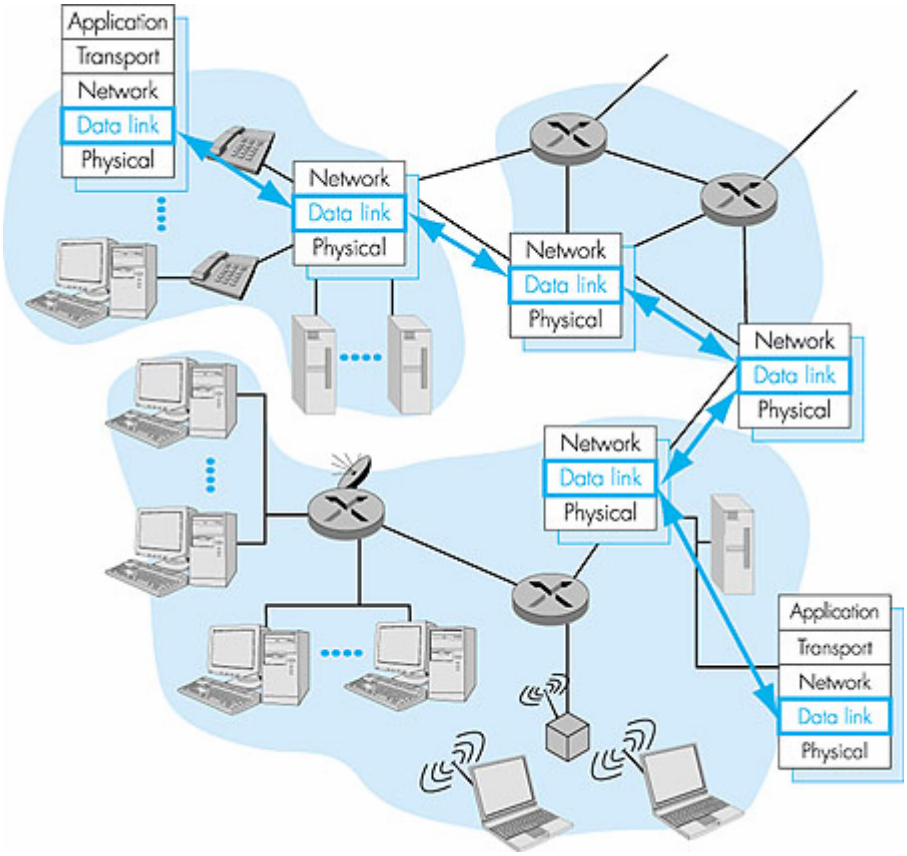


Figura 1 - A camada de enlace e a comunicação entre redes

Na Figura 2, você pode notar que existe uma comunicação direta entre as interfaces de rede unidas pelo enlace físico. Nessa figura, um host é representado na pilha da esquerda, com 5 camadas – modelo híbrido, comunicando-se com o seu gateway (três camadas). Sempre que o destino não se encontra na mesma rede física da origem, o gateway é quem fornecerá a passagem para outra rede.

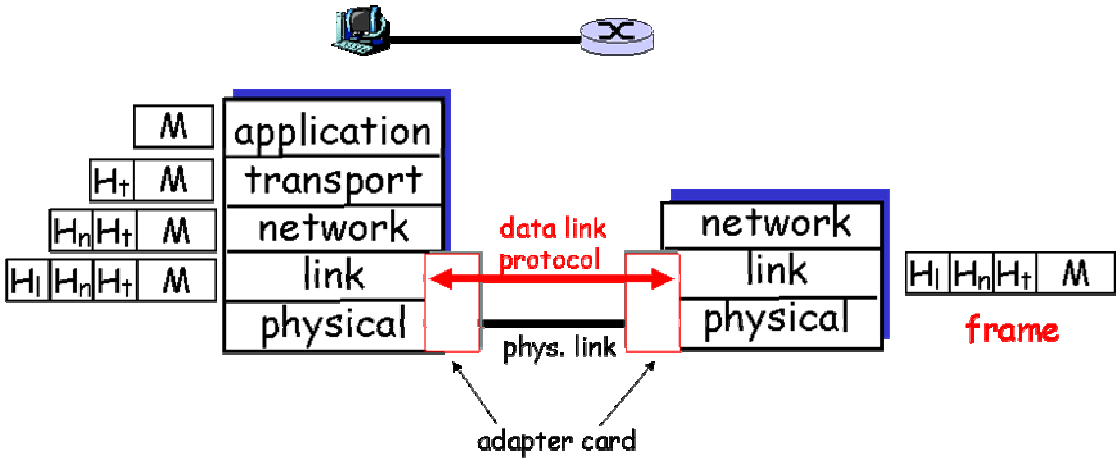


Figura 2 - A camada de enlace, uma comunicação direta entre as interfaces através de um link físico

Voce deve perceber essa situação como um veículo (frame da camada de enlace) transportando uma caixa de pizza (datagrama da camada de rede). Perceba também que essa situação deve ser analizada

desde a saída da porta da pizzaria até a próxima porta ou entrada em uma via de transporte diferente. Se ocorrer uma passagem dessas, por mais uma porta (condomínio do destinatário por exemplo), toda a documentação (cabeçalhos) deve ser analisada. É possível que o proto-boy tenha que trocar de veículo (frame da camada 2) devido as leis de trânsito diferenciadas nas ruas do condomínio. Por exemplo, o porteiro – que funciona como um roteador- vai analisar a documentação e informar: voce deve se dirigir ao terceiro bloco, saindo por essa porta. Abandone a moto e vá de bicicleta. Isso acontece com os datagramas que saem de uma tecnologia – Ethernet por exemplo, para ser transportado por uma rede ATM no próximo enlace.

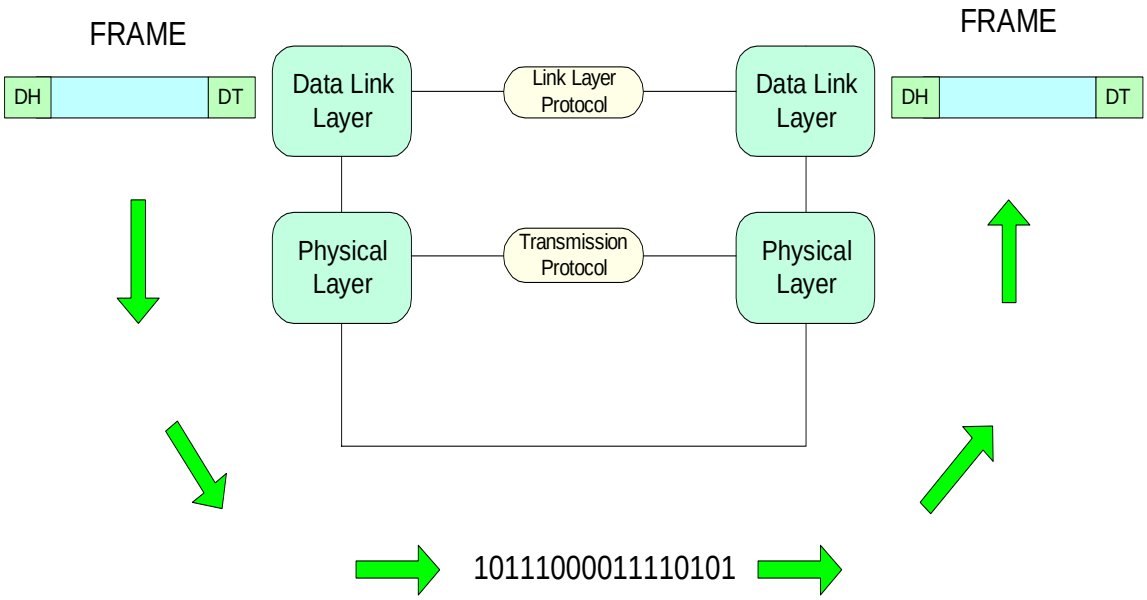
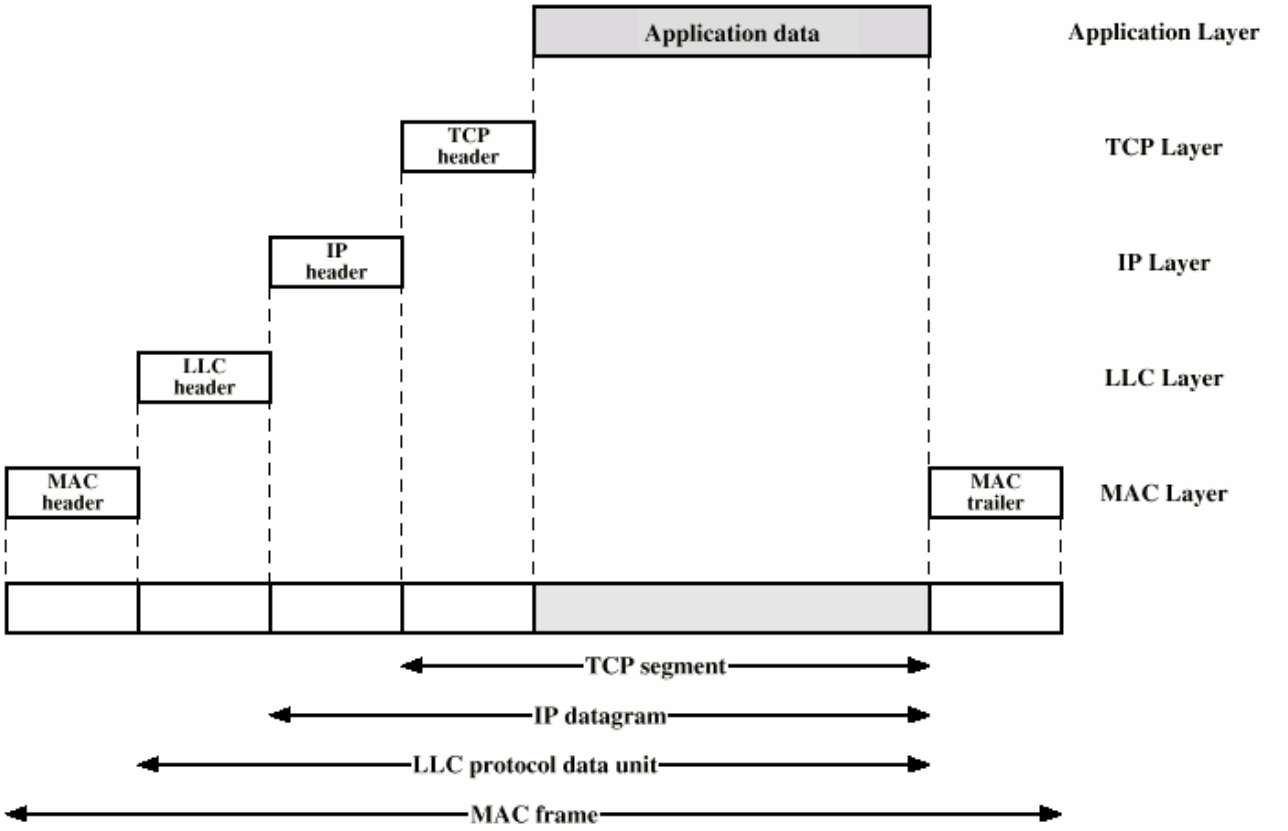


Figura 3 - A camada de enlace e os frames

Voce deve lembrar que as unidades de dados trocadas pela camada de enlace (PDUs) são denominadas frames e que cada frame encapsula uma PDU de camada 3, denominada datagrama[1].

[1] Analisado com com mais detalhes, existe outra denominação para as PDUs de camada 3. Elas podem se denominadas “pacotes”, sempre que uma dessas unidades ultrapassar o tamanho máximo possível de ser encapsulado no frame. Essas diferenças serão observadas na próxima unidade.



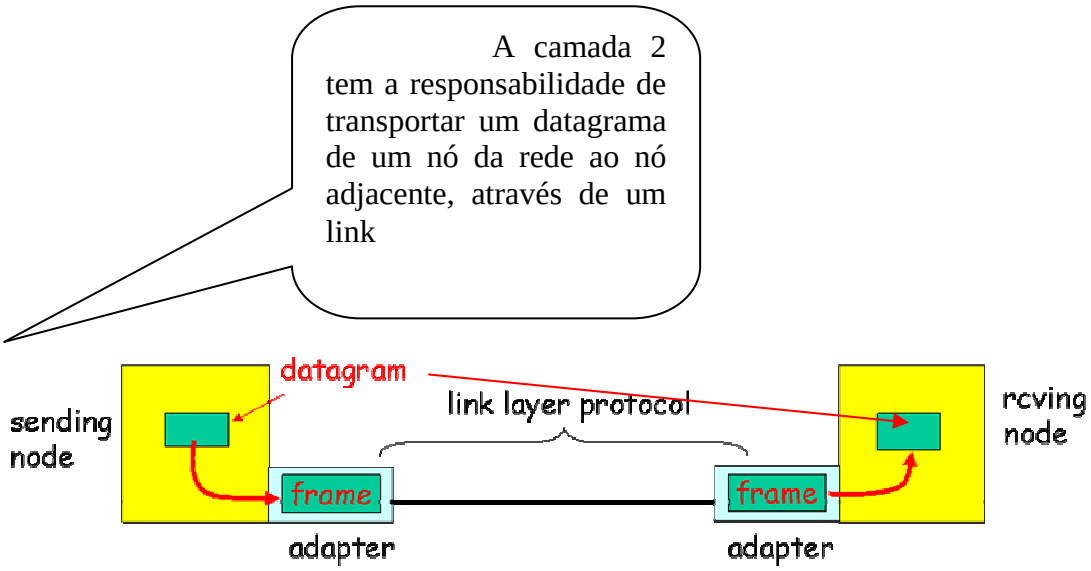


Figura 4 - Datagrama encapsulado atravessa o link "dentro" do frame

datagrama = caixa de pizza,
frame = furgao do protoboy.
Link=rua
nó de origem=net-pizza
Destino=cliente

A camada de enlace trata de resolver as principais carências da camada física:

- Endereçamento
- Formatação do fluxo de bits (enquadramento)
- Controle de acesso ao meio

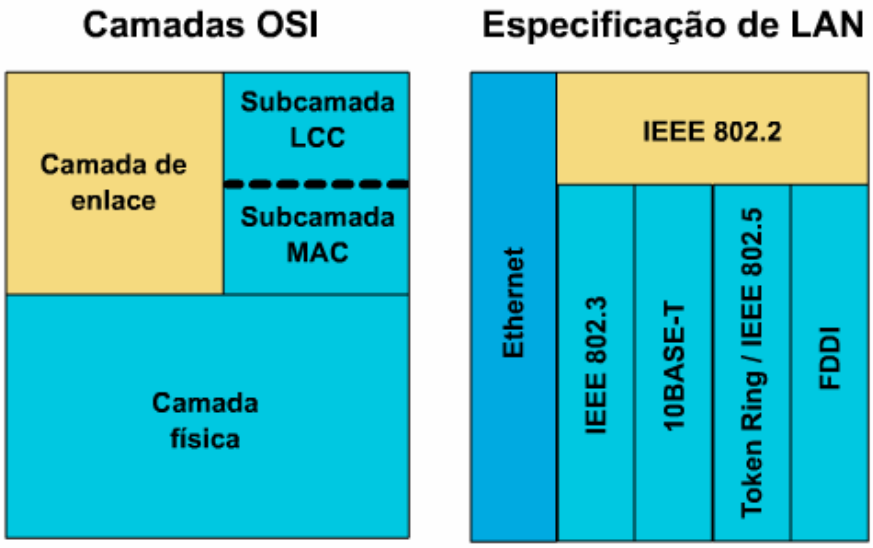


Figura 5 - as divisões da camada de enlace e as tecnologias

Tipicamente, a camada de enlace é implementada nos drivers de dispositivos e nas ROMs[2] das placas de rede. Os drivers fazem a ligação entre uma placa específica de um fabricante e o sistema operacional, também específico de um fabricante. Você já deve ter ouvido falar de algo parecido com "... o driver da placa 3COM para o windows 2000...".

O IEEE divide a camada de enlace do modelo OSI em 2 sub-camadas: LLC e MAC (Figura 5).

1.1 LLC – *Logical Link Control*, ou Controle Lógico de Ligações

Três funções principais nessa subcamada: Enquadramento, controle de fluxo e detecção de erros (sendo possivel algum tipo de correção).

Enquadramento

Essa subcamada é a responsável pela montagem do frame, processo denominado "enquadramento", pois insere todas as informações nos campos correspondentes. A Figura 6 mostra um frame genérico a ser preenchido com bits pela LLC.

[2] ROM – Read Only Memory, ou memória de leitura somente, é um componente que armazena código de software e não pode ser alterado ou apagado.

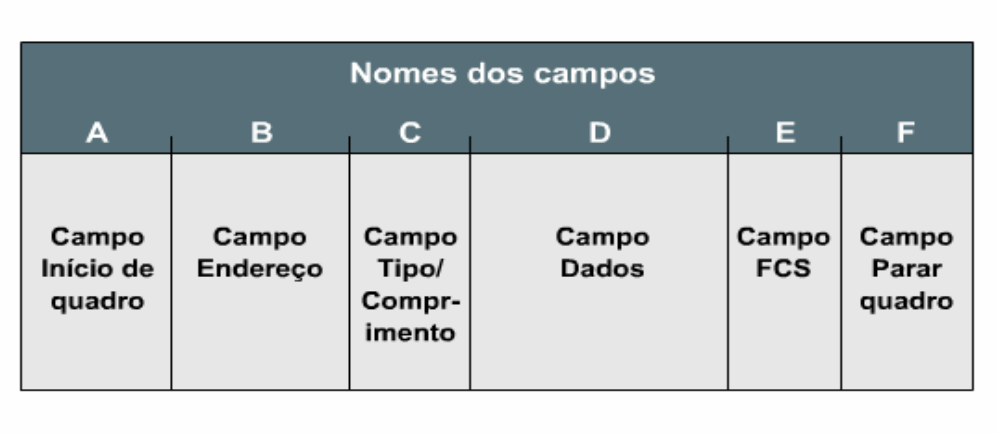


Figura 6 - Quadro genérico com os campos principais

Enquadramento é o processo de particionar uma sequência de bits em unidades discretas ou blocos de dados, denominadas quadros.

Existem formatos e sequências de tempos específicos para cada tecnologia de rede. Com a subdivisão da sequência de bits em quadros, é possivel para as estações de origem e destino entender o início e o final de cada unidade, sincronizando a transmissão e a recepção. Também através do uso dessa técnica é possível mandar informações sobre o quadro e seu conteúdo, o que habilita a capacidade de detectar erros.

Controle de fluxo

O controle de fluxo é a segunda função da subcamada LLC. Controlar o fluxo significa interferir na taxa da troca de dados entre os nós que estão se comunicando.

Para controlar o fluxo, é necessário um mecanismo de retroalimentação que informe a máquina de origem sobre a capacidade de receber informações pela máquina destinatária.

O controle de fluxo é necessário para evitar que um nó transmita quadros em uma taxa superior a que o destinatário consiga processar.

Buffers / reservatórios de memória

Um buffer é um espaço na memória reservado para armazenar informações. As maquinas que participam da comunicação armazenam os quadros que estão entrando ou saindo das interfaces em filas de espera para o processamento ou transmissão. Se a taxa de envio supera a capacidade de processamento do receptor, os quadros excedentes são armazenados nos buffers a espera de processamento. Se o controle de fluxo não funcionar, os quadros que excederem a capacidade do buffer serão descartados.

Imagine que os quadros são as caixas de pizza (as caixas possuem informações de endereço, quantidades e conteúdos como o quadro genérico da Figura 6). O cliente da net-pizza é um voraz consumidor, um tipo de troglodita fanático por pizzas. Ele fez uma encomenda de 20 caixas semanais, e nosso proto-boy faz as entregas regularmente. Se, por algum motivo o troglodita contemporâneo deixar de consumir as pizzas (pode, por exemplo, ter recebido alguns javalis de presente), ele precisa armazenar as caixas no freezer. Se não controlar o fluxo das pizzas, avisando a net-pizza para interromper momentaneamente a remessa, o freezer esgota a capacidade, e as pizzas excedentes serão de alguma forma descartadas.

Existem basicamente dois algoritmos usados para controlar os fluxos: Stop-wait (parar-esperar) e slidding windows (janelas deslizantes). Esse segundo tipo será analisado na unidade 8, quando voce estudar o protocolo de transporte Transmission Control Protocol – TCP.

Controle de erros

O controle de erros envolve a detecção de bits errados e um segundo processo, a correção. A correção nem sempre é possível, e nem sempre é vantajosa. Na maioria das vezes, as tecnologias da camada de enlace preferem descartar os quadros onde algum erros foi detectado. Isso evita prejuizos computacionais maiores, porque corrigir envolve recursos suplementares, mais custosos que simplesmente retransmitir os quadros errados.

Controlar erros significa garantir que a informação que chegou ao destino é confiável. Isso pode implicar em descarte das informações erradas.

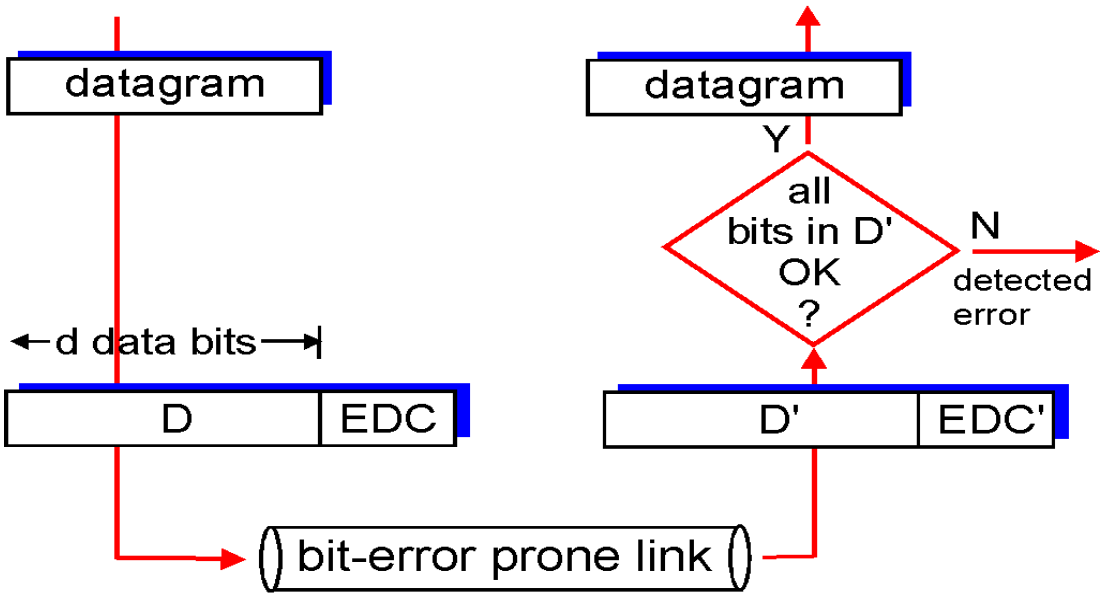


Figura 7 - Detecção de erros

A Figura 7 mostra um algoritmo simples para detectar erros. Os dados a serem protegidos contra os erros sofrem o acréscimo dos bits EDC no nó de origem (error-detection and correction bits). Ambos os campos D e *EDC* são transmitidos através do enlace. No nó de destino, uma sequência de bits *D*' e *EDC*' são recebidos. Você deve perceber que a interface de destino não tem com saber com certeza sobre as informações originais. A informação que chegou pode (D' e ECD') podem ser diferentes dos originais. O grande desafio do destinatário é acreditar que, se os bits de proteção ECD' afirmam que D' está isento de erros, D' é igual a D.

Quando o dado chega ao destino com os bits de proteção acusando erro, o destinatário pode somente acreditar que um erro foi detectado, mas não existe certeza que tenha de fato ocorrido. De qualquer forma, o tratamento de erros deve ser ativado. Isso significa tentar corrigir ou descartar.

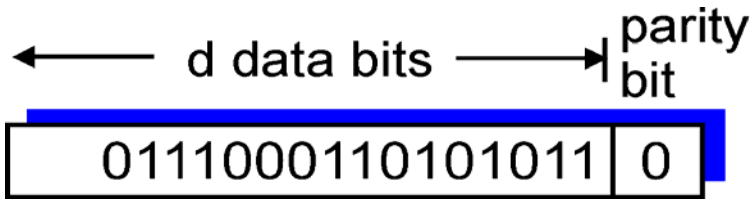


Figura 8 Sistema de paridade impar

A

Figura 8 mostra um método simples de detecção de erros, denominado bit de paridade.

Deve-se optar inicialmente pelo tipo de paridade a ser confirmada: Se par, uma quantidade par de bits 1 deve ser enviada. Quando ímpar, o bit de paridade vai complementar uma quantidade impar de bits 1.

Pelo método, um bit é acrescentado ao final da cadeia. No exemplo da figura, a paridade escolhida foi impar. Um bit 0 foi acrescentado na cadeia, pois o número de bits 1 já era ímpar (9 bits eram iguais a 1).

O receber a cadeia, o destinatário confere os bits e paridade. Obviamente, o método só funciona para detectar erro em um único bit. Também não é possível com o método localizar o bit errado.

1.2 – MAC - Subcamada de controle de acesso ao meio (Media Access Control)

As redes locais são ditas redes de difusão, onde todas as estações utilizam recursos de forma compartilhada. Nessas redes, o acesso aos recursos deve ser controlado de alguma forma, para evitar-se confusão.

O acesso ao meio compartilhado pode ser análogo a uma fila de furgões da net-pizza, todos com problema nos motores. Eles estão com a carga pronta (pizzas pra todos os gostos) mas não conseguem deixar o prédio antes que o único furgão com o motor bom retorne. O motor bom é o recurso compartilhado, e cada um deve ter o acesso ao recurso de uma forma ordenada. A espera pode ser longa, mas o proto-boy deve aguentar firme. E o cliente devorador de pizzas também. Uma forma de evitar as filas de espera para acessar o recurso seria todos os furgões terem seus próprios motores. O recurso deixa de ser compartilhado para ser privado. Obviamente, isso implica em custos.

Basicamente existem duas formas de controle de acesso: Centralizados e Distribuídos (Figura 9).

Os controles distribuídos podem ser classificados em dois grupos:

Controles estatísticos ou estocásticos

Controles determinísticos (por passagem de mensagens ou fichas)

Você verá mais sobre os controles de acesso na próxima seção.

Seção 2 Controles de acesso

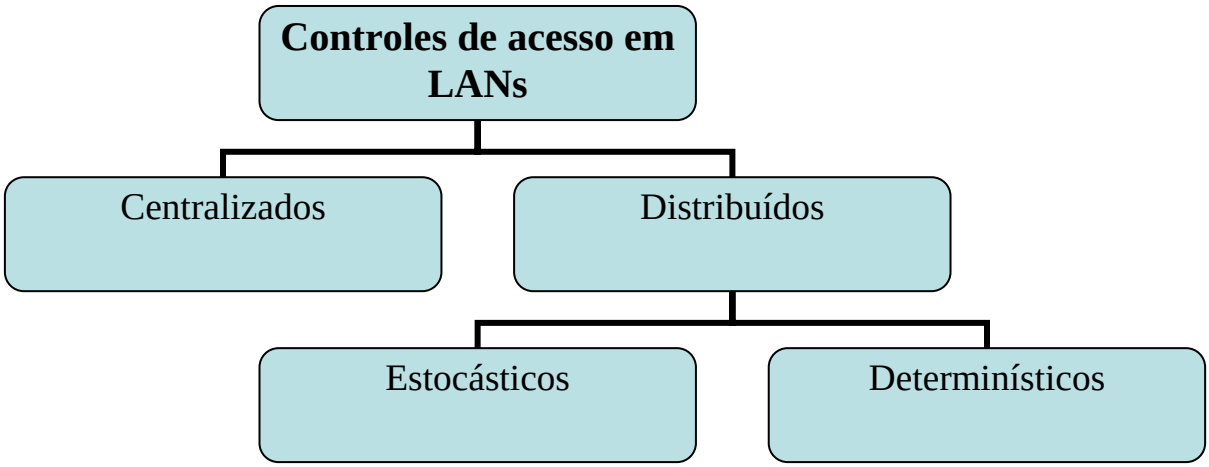


Figura 9 -Controles de acesso

Controles centralizados

Nesse tipo de controle de acesso, um dispositivo central (normalmente um switch) determina qual a estação que poderá realizar uma conexão ou iniciar uma transmissão de dados. Esse é o caso de algumas tecnologias mais sofisticadas, como o ATM e o 100VG Any LAN (IEEE 802.12), que possui controles de prioridades. Nos switches ATM, as estações que possuem informações para transmitir precisam obter a licença de acesso passando pelo crivo do CAC, ou conrole de admissão de conexao (Conection Admission Control). Com esse tipo de mecanismo, se pode garantir que o desempenho será satisfatório, uma vez que, quando não existem os recursos requeridos pela estação, o dispositivo central não libera o acesso.

Você pode relacionar esse tipo de controle com uma via de transporte onde um policial (dispositivo central) determina quais os veículos (frames) que podem trafegar em um determinado momento. Ele pode inclusive determinar que alguns veículos possuem prioridade, como algum furgão da net-pizza que esteja transportando para algum evento presidencial ou parlamentar. Como você sabe, muitos desses eventos acabam em pizza.

Controles Distribuidos

Os controles distribuídos são independentes de um dispositivo central, uma vez que cada interface que precise transmitir deve se auto-controlar. Nesse caso, é mais difícil de se impor alguma prioridade que seja aceita por todos os participantes, mas devido a sua maior simplicidade, esses controles possuem menores custos. As tecnlogias mais comuns nas redes locais (Ethernet e Token Ring) utilizam controles distribuídos.

Você pode pensar no controle de acesso distribído como sendo a responsabilidade do policial transferida para todos os motoristas dos veículos que querem acessar uma rodovia. Cada qual precisa seguir com rigor o mesmo protocolo, para evitar que um veículo colida ou que se apodere de um recurso e não libere mais (uma vaga de tempo limitado sendo usada indefinidamente, por exemplo).

Como visto anteriormente, os controles de acesso distribuídos dividem-se em estocásticos ou não sequenciais e determinísticos. Vamos analisar os dois tipos.

1)Estocásticos ou não sequenciais.

Esses controles baseiam-se na idéia que uma estação pode transmitir sempre que tiver informações prontas para transmissão. Nesse caso, ela precisa disputar o acesso. Alguns autores denominam esses protocolos de protocolos de disputa. Os mais comuns são os CSMA (*Carrier Sense Multiple Access*). Você vai estudar os dois mais famosos. O protocolo que detecta colisão caso ela ocorra (CSMA/CD) e o que a evita (CSMA/CA).

a. CSMA/CD

Esse nomezinho sinistro significa: Acesso Múltiplo com Percepção da Portadora e Detecção de Colisão (*Carrier Sense Multiple Access/Colision Detection)*. Esse protocolo é usado pela tecnologia mais comum do planeta, a Ethernet de meio compartilhado. Também conhecida por *Ethernet de hub*, ou Ethernet half-duplex foi a grande sensação das LANs antes do surgimento dos switches.

Robert Metcalfe, com a ajuda de David Boggs, inventou a tecnologia Ethernet, baseado em um protocolo denominado ALOHA, que também usava acessos aleatórios. Nessa época, trabalhava na ARPANet, no MIT, onde fazia sua tese de doutorado. Saindo do MIT, ele foi para a Xerox. O Ethernet original de Metcalfe e Boggs rodava nos precursores dos PCs da IBM, os computadores da Xerox denominados Alto. A velocidade inicial era de 2,94 Mbps. Eles forjaram uma aliança entre, a Digital, a Intel, e a Xerox, estabelecendo o padrão de 10Mbps para o Ethernet (Foi o DIX Ethernet, com as iniciais das companhias). O IEEE ratificou o padrão (802.3). Metcalfe fundou a 3COM, uma vez que a Xerox não teve interesse em comercializar as interfaces Ethernet. No ano de 2000, a 3Com, já sem

Metcalfe, capitalizava 15 bilhões de dólares e 13 mil funcionários. Com certeza, uma das grandes empresas mundiais de dispositivos de rede.

Vamos verificar como funciona o CSMA/CD

a) Uma estação que tem um frame para transmitir "escuta" o meio físico.
b) Se estiver ocupado (ou seja, percebe sinal trafegando), continua escutando.
c) Se estiver livre, inicia a transmissão do quadro. Perceba que livre significa que a interface não percebeu sinal no meio. Isso não significa necessariamente a inexistência do sinal. O meio já poderia estar ocupado em uma regiao próxima, pela transmissão de um vizinho.
d) A estação deve transmitir até encerrar o frame, pois é assim que ela poderá perceber alguma ruptura do padrão elétrico, o que significaria que seu frame colidiu com o frame de algum vizinho

Caso perceba colisão, a interface deve:

b. Interromper a transmissão
c. Inundar o canal com sinal de bloqueio (JAM)
d. Processar um algoritmo de penalização, denominado "recuo exponencial" ou "*exponential back-off*", descrito a seguir.

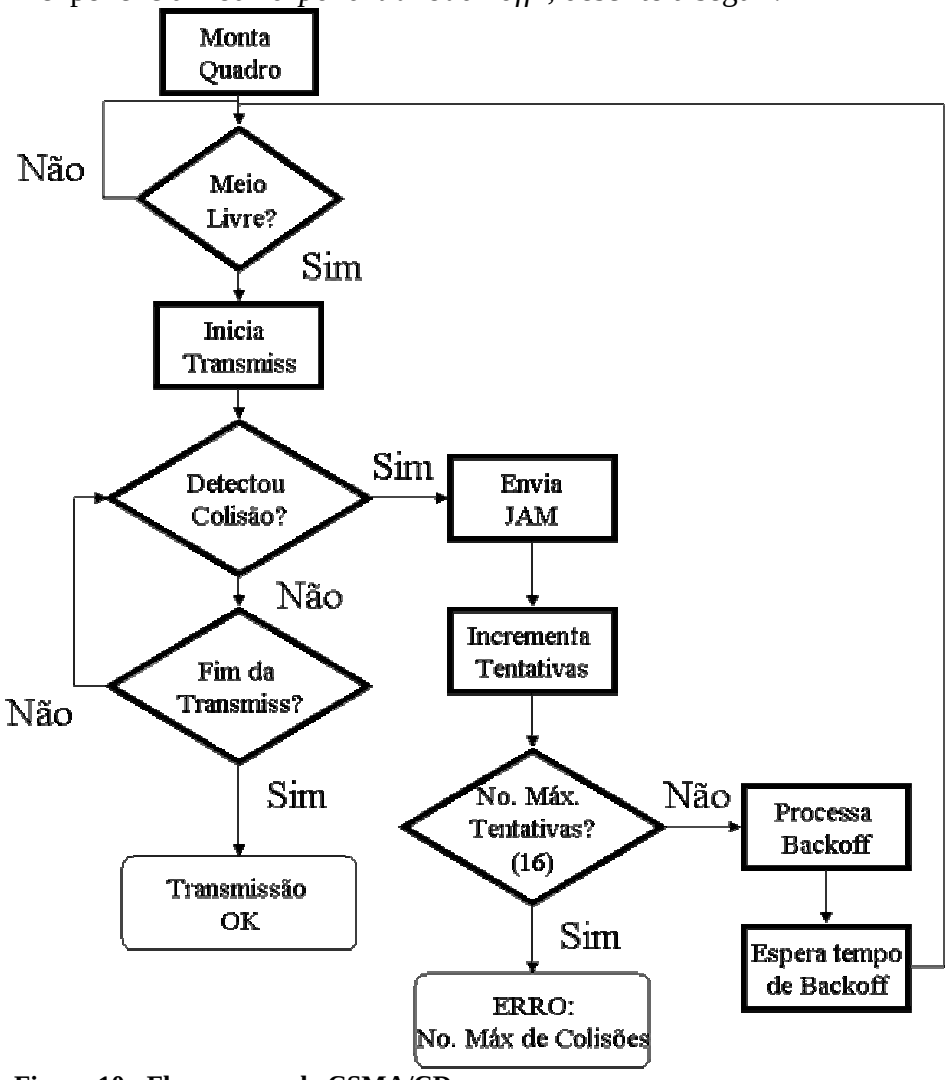


Figura 10 - Fluxograma do CSMA/CD

e) Se a transmissão prosseguiu até o final sem colisão, a estação não tem mais dados daquele frame, e libera o canal para outra estação transmitir. Perceba que só um frame pode ser transmitido.
f) A estação volta a perceber o meio para tentar transmitir o proximo frame ou, se não tem mais dados, fica inativa.

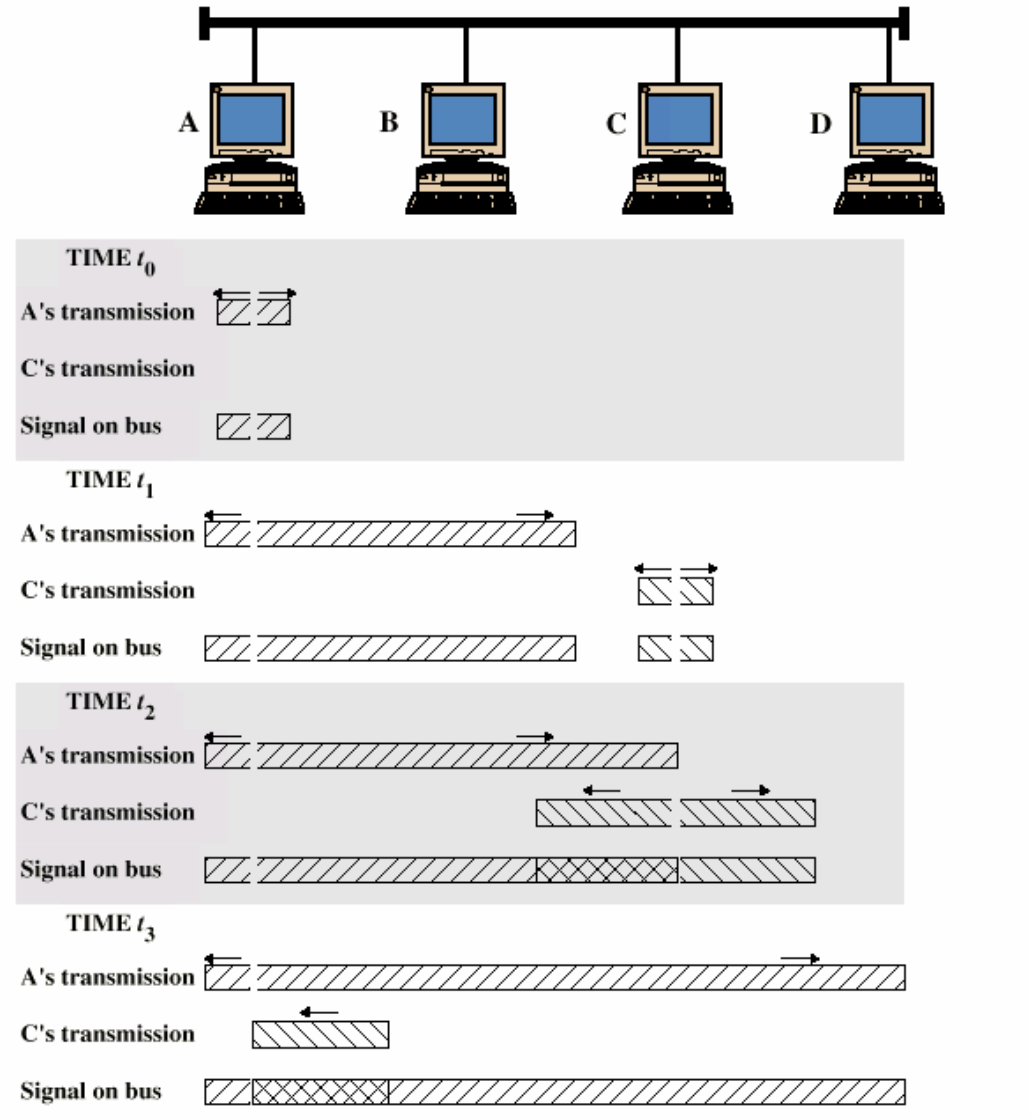


Figura 11 CSMA/CD e os sinais no meio físico

Algoritmo de recuo exponencial:
As interfaces cujos frames colidiram devem processar o seguinte algoritmo:

a) Um intervalo de tempo, (por exemplo 0 a t ms) é escolhido como faixa inicial
b) um número aleatório, por exemplo 5,3 milisegundos, dentro do intervalo, é amostrado.
c) Esse número significa o tempo no qual a interface deve recuar na tentativa de transmissão do frame que colidiu.
d) Passado o tempo escolhido, a interface tem o direito de tentar novamente
e) Caso haja nova colisão, o intervalo de tempo da amostragem do número aleatório é dobrado (por exemplo t=t*2). Isso permite uma chance menor de duas interfaces esperarem o mesmo tempo.
f) O número de tentativas de transmissão do frame é incrementado (**tent=tent**+1).
g) Se **tent** for menor que 16, volta ao passo b.

h) Se **tent** for igual a 16, a rede está congestionada e deve ser bloqueada.

Name	Cable	Max. segment	Advantages
100Base-T4	Twisted pair	100 m	Uses category 3 UTP
100Base-TX	Twisted pair	100 m	Full duplex at 100 Mbps (Cat 5 UTP)
100Base-FX	Fiber optics	2000 m	Full duplex at 100 Mbps; long runs

Tabela com o cabeamento do fast-Ethernet 802.3u

e. CSMA/CA

Outro nomezinho estranho, significa (*Carrier Sense Multiple Access/Colision Avoidance)* ou

Acesso Múltiplo com Percepção da Portadora / Prevenção de Colisão. Usado pelas tecnologias de redes locais e metropolitanas sem fio, (IEEE 802.11, 802.16), e pela tecnologia LocalTalk da Apple, um sistema ponto-a-ponto para pequenas redes.

Embora o algoritmo básico seja o mesmo (CSMA) que o anterior, a filosofia aqui não é detectar as colisões, mas sim evitá-las.

- ☐ O nó receptor, ao receber uma transmissão, envia uma confirmação.
- ☐ Dessa forma, o transmissor sabe que não houve colisão
- ☐ Se o transmissor não recebe a confirmação, retransmite.

O protocolo tem outros recursos importantes. Dois tipos de frames especiais participam da comunicação:

RTS – *Request to send* ou solicitação para transmitir
CTS – *Clear to send* ou liberação para transmitir

Esses frames especiais ajudam a minimizar as colisões. A estação que quer transmitir envia um RTS à estação de destino. Se estiver disponível para receber, a estação de destino envia um CTS.

2)Método de acesso Determinístico ou por passagem de ficha

Ao contrário dos estatísticos, os métodos determinísticos pretendem uma justiça plena no uso do canal, e uma previsibilidade que não existe

Esses protocolos baseiam-se em concessões de permissões para transmitir. Tal concessão é determinada pela posse de um frame especial, denominado *token* ou ficha. A estação que tem a ficha pode acessar o meio. Não existe disputa, e tampouco possibilidade de colisão. Esse método é usado pelas tecnologias Token Ring (IEEE 802.5), Token Bus (IEEE 802.4) e Fiber Distributed Data Interface - FDDI (ANSI).

A filosofia básica é a seguinte: A estação que possui a ficha pode transmitir. Quando teminar de transmitir um frame, deve liberar a ficha. As demais precisam aguardar a ficha. Isso evita a disputa e a colisão de frames.

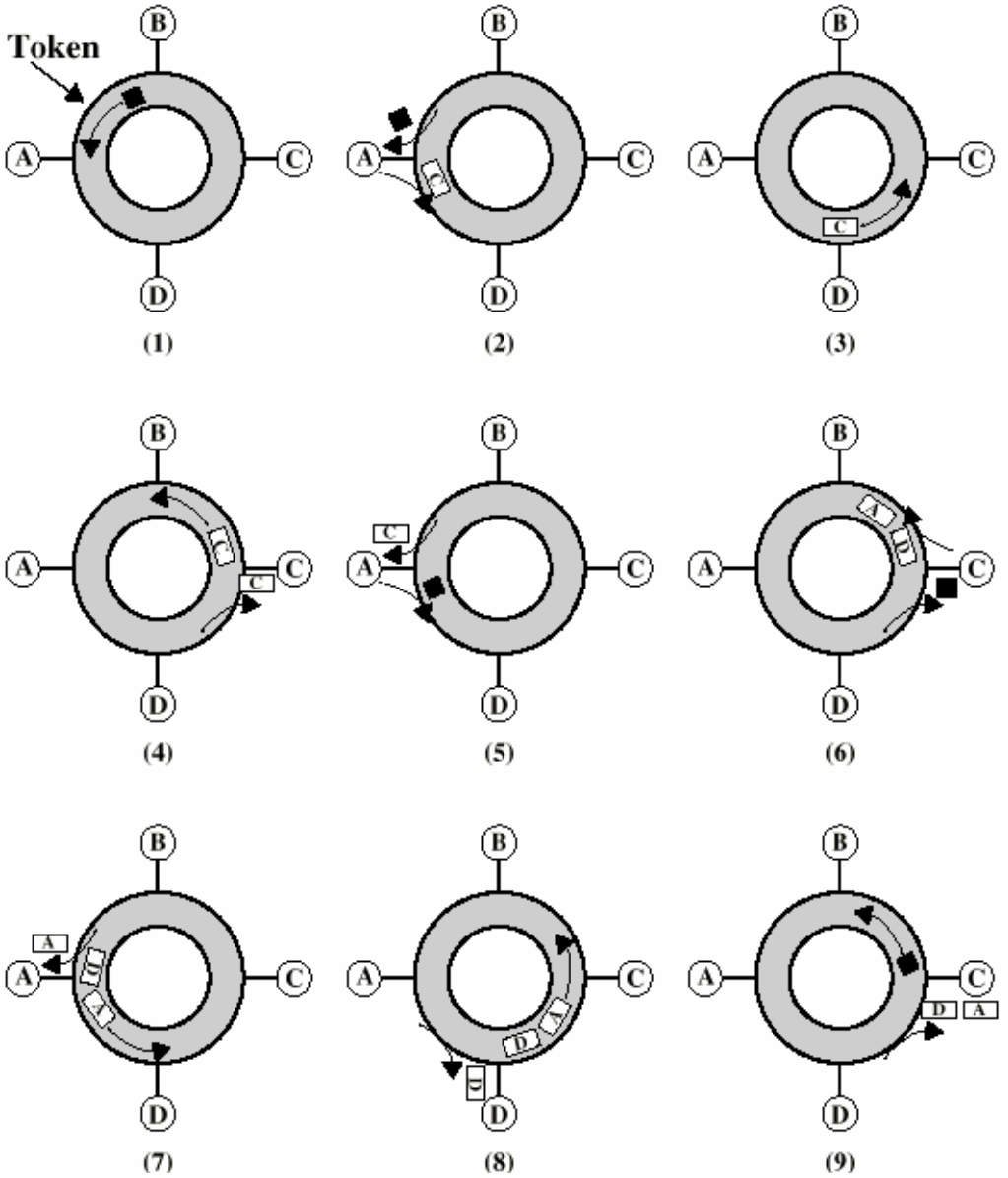


Figura 12 – Acesso por passagem de ficha -Topologia em anel

Na Figura 12, temos a seguinte sequencia na transmissão dos frames:

1) A ficha (token) está circulando livre pelo anel.
2) A estação A tem um frame destinado para C. Ela captura a ficha, e transmite o frame.
3) O frame com destino a C passa pela estação D, que não tem nada a ver com isso, e fica na dela.
4) A estação C recebe o frame, faz uma cópia, e devolve o cara para o anel.
5) A estação A recebe de volta o frame, retira do anel e libera a ficha.

(Note que como foi o nó de origem que retirou o frame do meio, é possível que a estação de destino marque um bit para dizer que recebeu, tudo ok, beleza). Isso é uma confirmação de entrega, como se o cliente da net-pizza assinasse um recibo e mandasse de volta pelo proto boy.

6) Agora é a estação C que possui frames para A e D. Ela se apodera da ficha e transmite um frame para os dois destinatários.
7) A estação A faz a sua cópia e repõe o frame no meio.
8) A estação D também copia e devolve
9) A estação C retira o frame e libera a ficha.

Agora que você já viu os dois principais métodos de acesso, estatístico e estocástico, vamos analizar as vantagens e desvantagens de cada um (Tabela 1):

Método de acesso	Vantagem	Desvantagem
Estatístico	Rápido com baixa carga	Queda de desempenho com cargas elevadas
Determinístico	Previsível com carga alta, garante o acesso.	Possui atraso fixo mesmo que a carga seja baixa

Tabela 1 - Comparação dos Métodos de acesso

Imagine que o proto-boy está entregando nossas pizzas em um tempo elogiável, cheirosas e quentinhas, porque existe pouco trânsito nas ruas do bairro. O trânsito é tão baixo que foi combinado entre os motoristas o seguinte protocolo: Ao chegar próximo de um cruzamento, buzine. Se você não ouvir uma buzina em resposta, pode passar livre (CSMA-escute o meio, se estiver livre, acesse). Se alguem responder, pare e espere.

Se o tráfego começa a aumentar, o risco de colisão aumenta, os atrasos também. As pizzas esfriam, e chega-se a conclusão de que é necessário um semáforo.

Agora, todos vão ter um tempo determinado de espera, sabe-se exatamente qual o pior tempo para passar por um número X de semáforos. Não existe colisão – todos os motoristas SEGUEM o protocolo. Em compensação, se o tráfego volta a diminuir, nosso proto-boy vai precisar esperar inutilmente diante de um sinal vermelho, enquanto o cruzamento está totalmente livre.

Seção 3 - Sistemas de endereçamento

Existem 4 níveis de endereçamento dentro da pilha de protocolos (Figura 14):

- Camada 5 – Os nomes dos dispositivos (por exemplo virtual.unisul.br)
- Camada 4 – as portas onde os processos estão rodando (por exemplo porta 80 para o http)
- Camada 3 – O endereço do protocolo de internet (IP), por exemplo 200.18.12.33
- Camada 2 – O endereço físico das interfaces, por exemplo 00:0e:83:ca:bb:fa

Modos de endereçamento

- Unicast :Uma máquina envia para outra
- Broadcast: Uma máquina envia para todas as máquinas de um domínio
- Multicast: Uma máquina envia para um grupo de máquinas cadastradas

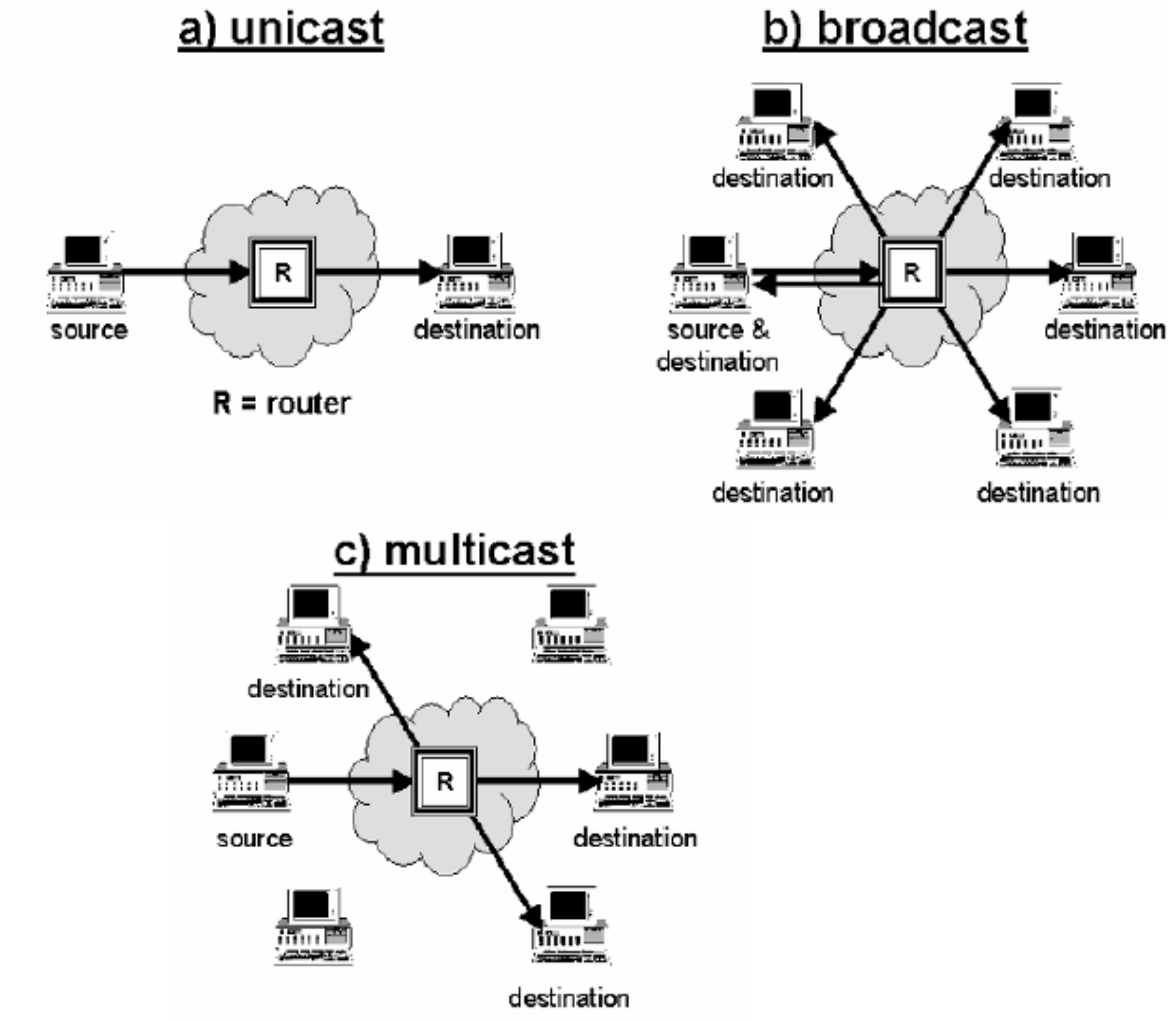


Figura 13 - Modos de endereçamento

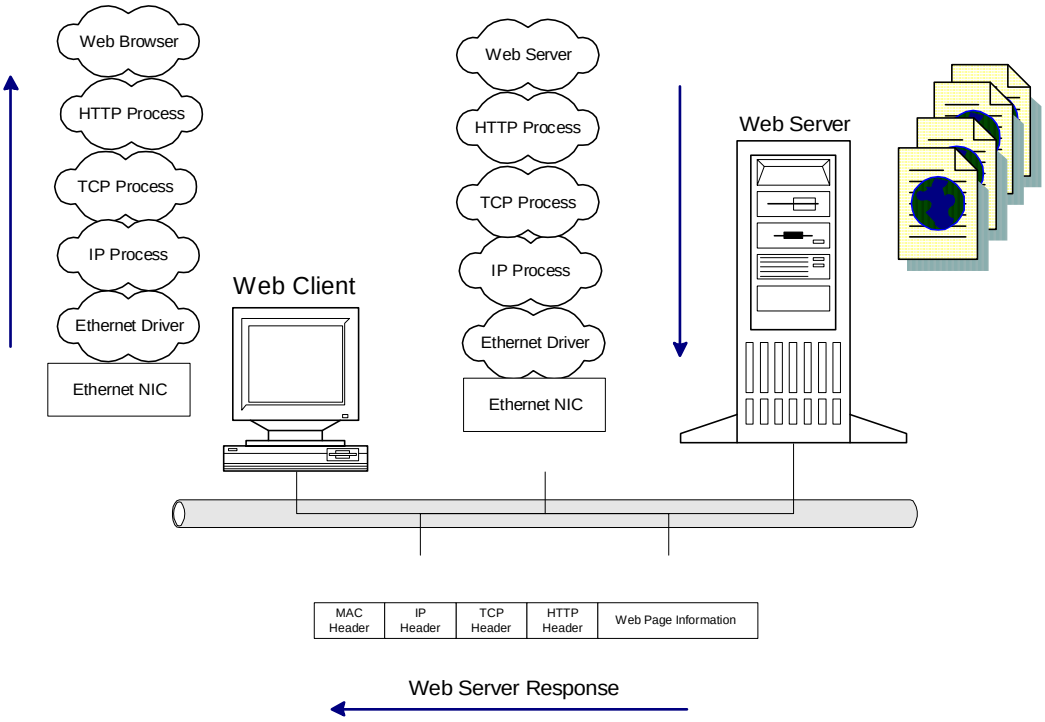


Figura 14 - Os endereços e as camadas

a. Nomes de máquinas

As máquinas de uma rede recebem nomes que são significativos para os humanos, embora não o sejam para elas próprias (como você sabe, elas precisam traduzir tudo para zeros e uns). Esses nomes são meramente simbólicos, e quando o usuário digita www.virtual.unisul.br, esse nome simbólico deve ser traduzido para o endereço IP da camada 3, que é exigido pelos protocolos inferiores. Um servidor específico para fazer essa tradução deve estar disponível na rede (servidor de nomes). Normalmente, essa tradução é feita sem que o usuário perceba.

Abra o prompt do MSDOS (Clique em iniciar, executar, command). Digite **ping www.virtual.unisul.br**.
Esse endereço de camada 5, é um nome simbólico, será traduzido pelo seu servidor de nomes para um endereço IP – de camada 3.

Da mesma forma, quando um usuário digita o endereço de um destinatário de e-mail, por exemplo angelina_jolie@unisul.br esse nome de máquina precisa ser traduzido para um endereço ip, que corresponde ao servidor de e-mail da Unisul.

Essa base de dados com os nomes das máquinas não é mantida em um único servidor. Ela está distribuída em inúmeros servidores ao redor do planeta. Os principais, que mantém os registros dos dominios superiores (.com, .net, .org...) estão localizados em 13 máquinas denominadas root-servers. Os espelhos, ou replicações do servidor root-F estão ilustrados na Figura 15. Esse sistema de resolução de nomes é denominado DNS, ou Domain Name System. Para saber mais sobre os serviços de resolução de nomes, acesso o site do ISC:
http://www.isc.org

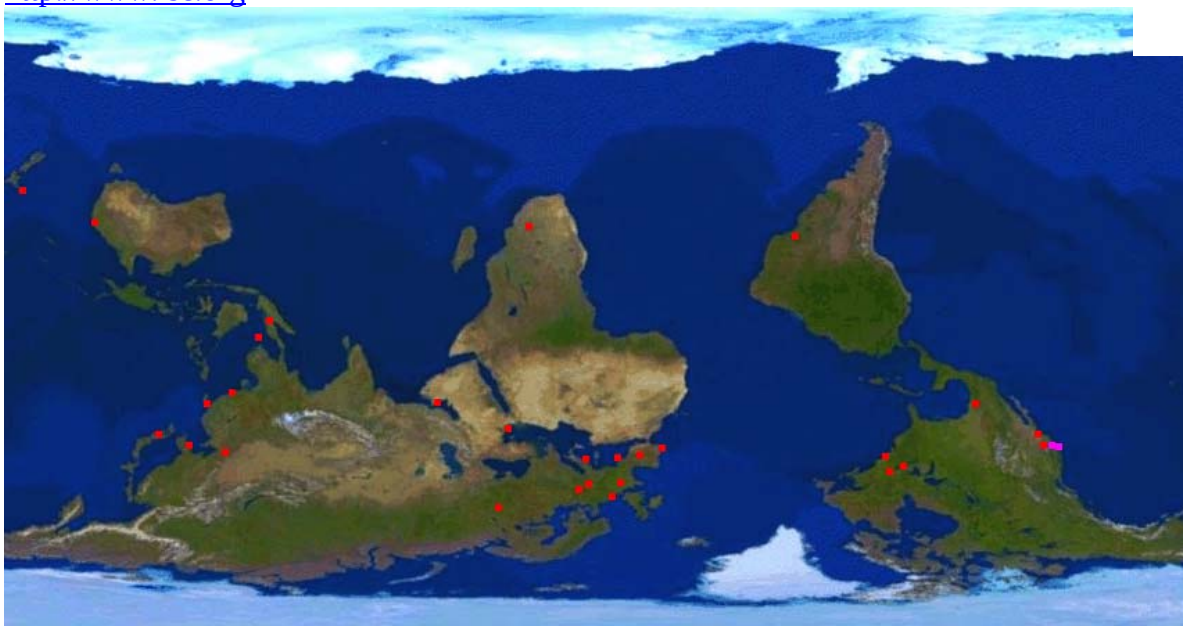
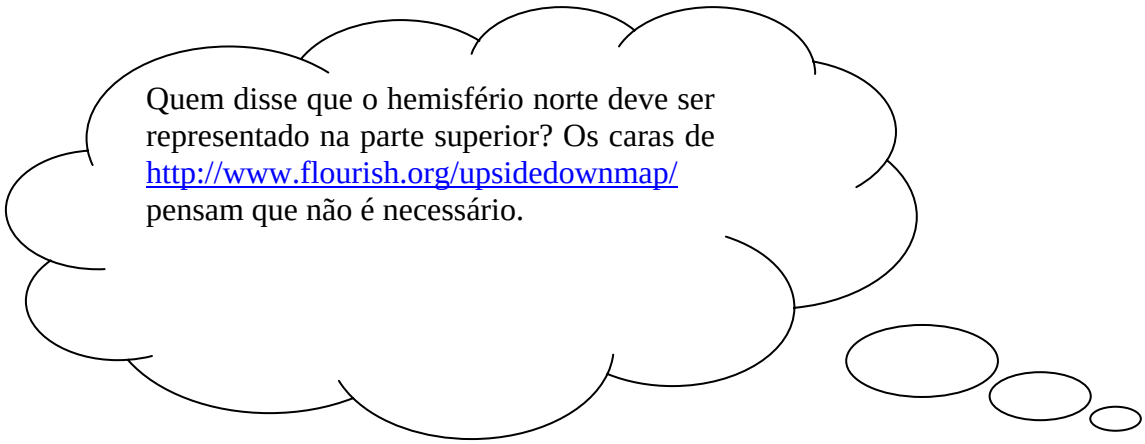


Figura 15 - Os 18 servidores de nome espelho do raíz F(Root-server F) mantidos pelo IANA.



b. Portas de transporte

O segundo nível onde ocorre endereçamento é na camada de transporte. Você verá mais sobre essa camada na unidade 8. Por enquanto vamos analisar somente um nível de abstração dessa camada, as portas de endereçamento. Com o uso das portas, o espaço de endereços pode ser extendido, e um processo que esteja transmitindo pode referenciar uma porta específica no host de destino. Os endereços das camadas mais baixas servem

para localizar uma máquina na rede, mas não os processos entro daquela máquina.

Na net-pizza, as portas da camada de transporte podem ser consideradas como salas onde diferentes serviços são executados. O pessoal do 2º. Andar é que controla as encomendas, tanto dos suprimentos quanto das entregas de pizzas. Esse povo possui uma tabela de encaminhamentos, que funciona como as portas da camda de transporte:

Serviço	*Sala*
Forno	*50*
Montagem	*32*
Seleção de componentes	*28*
Fatiadores das pizzas	*67*
Embalagem	*78*
Refreigeração	*19*
Cortadores dos componentes	*15*
Almoxarifado	*21*
Escritorios	*70*

Quando chega algum suprimento para a pizzaria, (por exemplo, madeira para o forno a lenha) esse suprimento precisa ser encaminhado para o pessoal encarregado do forno. Então, dentro do mesmo prédio (host), existem divisões de tarefas (serviços). Digamos que os assadores trabalhem na sala 50. A lenha para o forno deve ser encaminhada para essa sala.

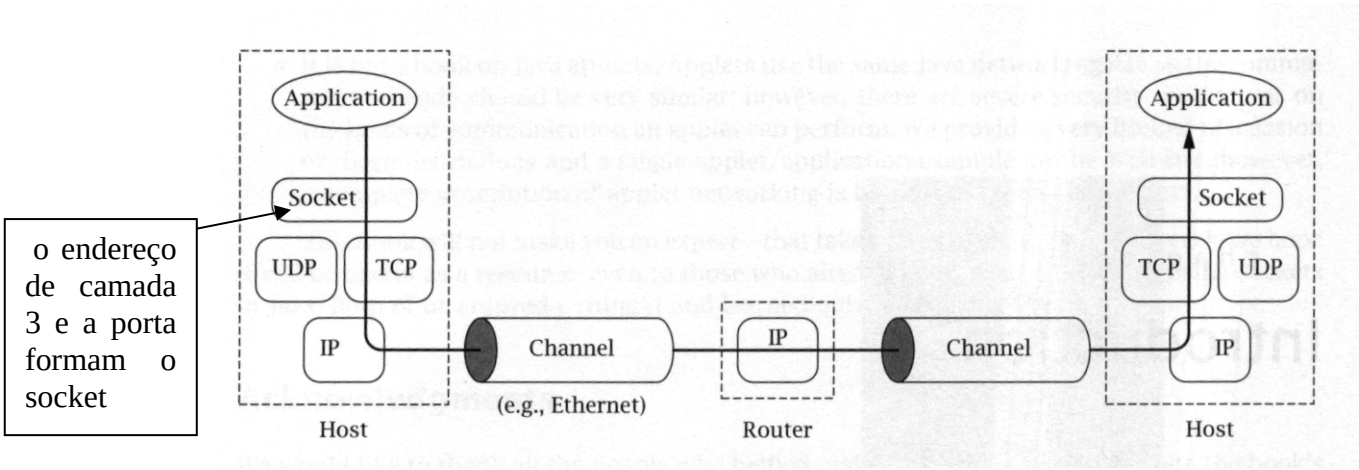


Figura 16 As aplicações e os endereços

A RFC 1700 (veja no site do IETF) contém os números usados pelos protocolos, e as portas para os serviços bem conhecidos. Existem 65538 portas possíveis para cada um dos protocolos de camada 4. elas são classificadas em altas e baixas.

- Portas baixas (well-know ports) São usadas pelos principais serviços no lado servidor da comunicação Tabela 2. São endereços estáticos, e variam de 0 a 1023.

Protocolo	porta
FTP	21
SSH	22
TELNET	23
SNMP	25
DNS	65
HTTP	80
POP3	110
SNMP	161

Tabela 2 Portas baixas

- Portas altas

São abertas no lado cliente, dinamicamente. Os clientes podem inicializar várias requisições simultaneamente, para o mesmo host de destino, e a mesma porta desse destinatário. Mesmo assim, o destinatáro conseguira responder as requisições, usando o numero da porta alta do cliente para entregá-las. Usam os números acima de 1023.

c. Endereços IP

Os endereços do protocolo IP servem para a localização dos hosts de destino, mesmo que não se conheçam as implementações físicas da rede de destino. Por exemplo, você não precisa saber qual a tecnologia da placa de rede do computador da Debora Secco para enviar um e-mail para ela. Basta saber o endereço de nível mais alto.

Os endereços IP são números de 32 bits e dividem-se em dois segmentos: Rede e Host. A parte de rede é usada pelos roteadores para encontrar a rede local onde o destinatário se encontra. Uma vez que tenha chegado na rede

local de destino, o endereço do hardware (MAC address, a seguir) deve ser localizado. Para isso, os roteadores usam a porção de host do endereço IP, em conjunto com o protocolo ARP (na seção 5).

Os endereços IP não estão relacionados aos hosts, mas sim às interfaces dos hosts que estão conectadas em uma rede. Um mesmo host pode ter mais de uma interface para redes diferentes, necessitando mais de um endereço IP.

Na net-pizza, o endereço ip corresponde ao número do prédio da pizzaria. Como nosso prédio tem mais de uma saída, ou seja, tem porta para mais de uma rua, o prédio deve ter um número que o identifique em cada rua.

Os endereços podem ser representados na forma binária ou decimal pontuada. Nesse caso, temos 4 octetos separados por um ponto decimal, que resulta em um número variando de 0 a 255 em cada octeto, ou byte.

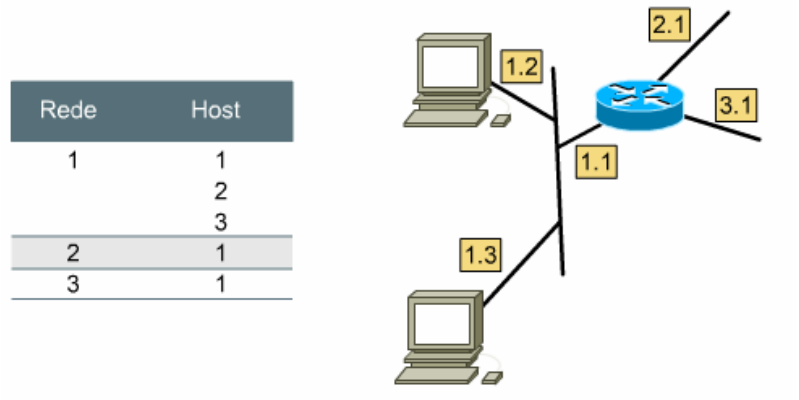


Figura 17- Porção de rede e host no endereço IP

Perceba, pela Figura 17, que os endereços divididos dessa forma apresentam uma hierarquia, que possibilita um crescimento das redes e facilita a localização.

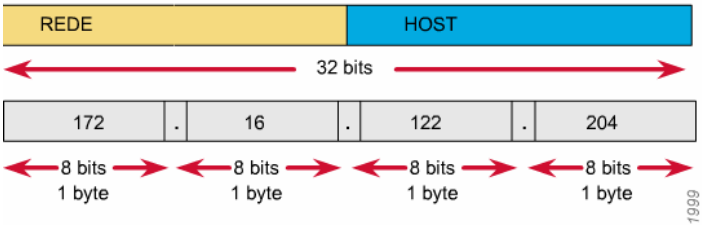


Figura 18 - Os octetos e a divisão rede/host no endereço IP

Um exemplo de endereçamento IP é 172.16.122.204. Veja na Figura 18 como ficam as divisões Rede/Host, bem como os octetos separados por pontos.

Os endereços foram divididos em 5 classes, A,B,C,D e E. As classes usadas em roteamento normal são A, B, e C conforme a Figura 19. A classe D é usada para roteamento Multicas, e não será estudada nessa disciplina. A classe E foi reservada para experimentos.

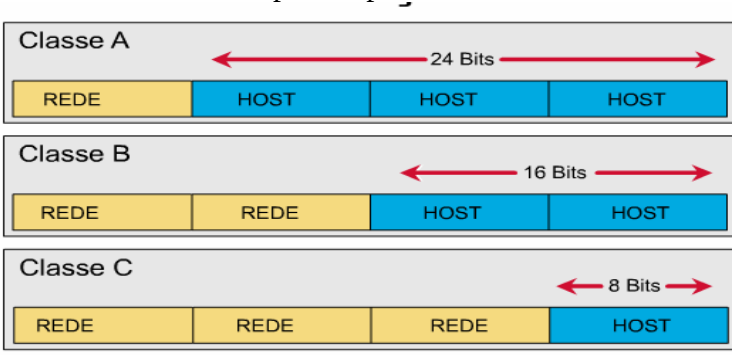


Figura 19 - Classes de endereços A, B e C

Verifique seu enderço IP com o comando ipconfig.

Perceba que quanto mais bits para hosts, maiores ficam as redes. Sob essa óptica, as redes de classe A seriam as maiores e as de classe C, as menores.
As faixas de endereços de cada classe podem ser resumidas como na Tabela 3.

Address Class	Dotted-Decimal Notation Ranges
A (/8 prefixes)	1.xxx.xxx.xxx through 126.xxx.xxx.xxx
B (/16 prefixes)	128.0.xxx.xxx through 191.255.xxx.xxx
C (/24 prefixes)	192.0.0.xxx through 223.255.255.xxx

Tabela 3 - faixas de endereços de cada classe na forma decimal

Descubra qual a classe de endereços da sua rede, com base decimal que representa o no 1º. Octeto.

d. MAC address

Os endereços MAC (endereço de hardware, endereço físico ou de placa de rede) são endereços de camada 2. Os endereços de camada 2 são a referência final para a entrega dos frames. A informação só chega ao destino depois que esse nível de endereços é conhecido.

Os endereços MAC têm 48 bits de comprimento e são expressos com doze dígitos hexadecimais (Figura 20). Os primeiros seis dígitos hexadecimais, que são administrados pelo IEEE, identificam o fabricante ou fornecedor e, portanto, formam o Identificador único de Organização (*Organizational Unique Identifier - OUI*). Os seis dígitos hexadecimais restantes formam o *número serial de interface*, ou outro valor administrado pelo fornecedor específico.

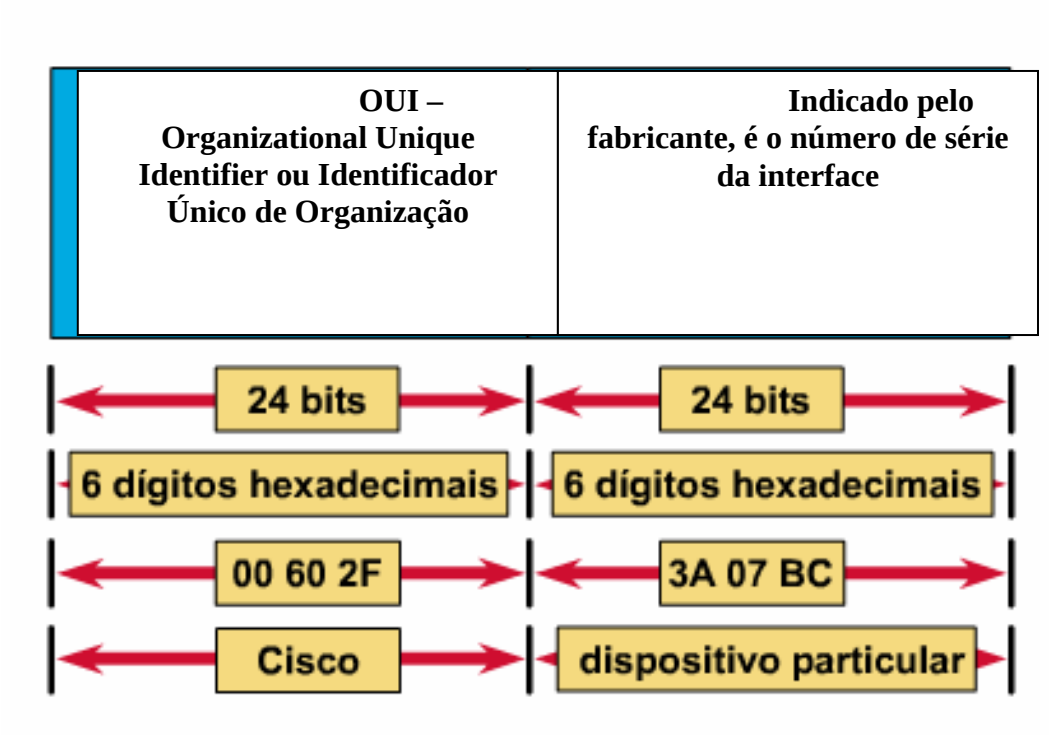
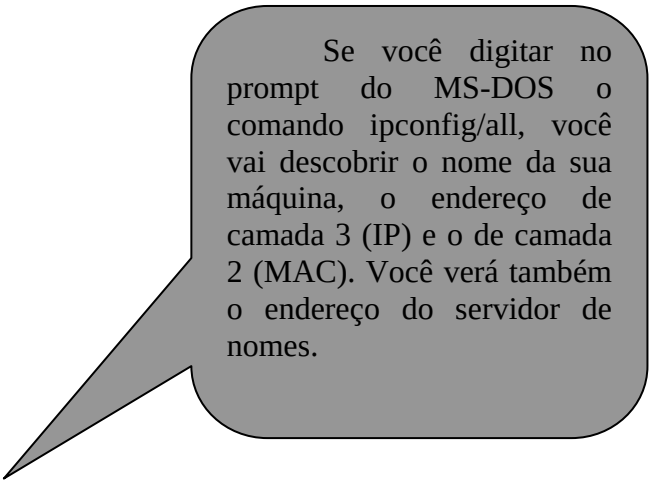


Figura 20 - Formato do endereço MAC

Os endereços MAC são algumas vezes chamados de *burned-in addresses* (*BIAs*) porque eles são gravados na memória apenas de leitura (ROM), e são copiados na memória de acesso aleatório (RAM) quando a placa de rede é inicializada.

Mais sobre os MAC address em:

http://standards.ieee.org/faqs/OUI.html



Os endereços MAC são vitais para o funcionamento de uma rede de computadores. Eles fornecem uma forma dos computadores se identificarem. Eles dão aos hosts um nome exclusivo e permanente. O número de endereços possíveis não vão se esgotar tão cedo já que há 16^12 (ou seja, mais de 2 trilhões!) de endereços MAC possíveis.

e. Fluxos

Um fluxo de dados é uma identificação completa de uma transferência entre os processos clientes e servidores nas redes TCP/IP. Para que possamos caracterizar um fluxo, as seguintes identificações precisam se estabelecer:

- ☐ Endereços IP da origem e do destino
- ☐ Protocolo da camada de transporte
- ☐ Porta do servidor
- ☐ Porta do cliente
- ☐ Direção do fluxo

IP Origem	IP destino	Protocolo	Porta Origem	Porta destino	Direção
10.10.1.1	20.20.1.2	TCP	36021	80	IN
10.10.1.1	20.20.116.4	UDP	23321	161	OUT
10.10.1.1	20.20.116.4	TCP	12872	25	Out

Tabela 4 - Exemplo de identificação de um fluxo

Perceba que um mesmo cliente pode abrir várias conexões para um mesmo servidor, em portas diferentes. Na verdade para que a identificação de um fluxo seja única, é necessária a combinação de todas as variaveis. Dessa forma um mesmo cliente pode requisitar várias conexões na porta 80 de um mesmo servidor, porque em cada uma delas, vai existir a variação na porta de origem.

Seção 4 - Os formatos dos principais quadros

Nesta seção, veremos o Ethernet como exemplo de frame. As demais tecnologias de camada 2 serão apenas ilustradas. Os detalhes do Ethernet são

importantes porque a tecnologia é a dominante nas redes locais. Existem livros inteiros sobre a tecnologia Ethernet.

Veja na pagina de Charles Spurgeon: http://www.xxxxxxxx.com

Para saber mais sobre os formatos de frames:
http://www.cisco.com/univercd/cc/td/doc/product/lan/trsrb/frames.htm

a) Ethernet

Ethernet						
?	1	6	6	2	46-1500	4
Preâmbulo	Início do delimitador de quadro	Endereço de destino	Endereço de origem	Tipo	Dados	Seqüência de verificação de quadro

IEEE 802.3						
?	1	6	6	2	64-1500	4
Preâmbulo	Início do delimitador de quadro	Endereço de destino	Endereço de origem	Compri-mento	Cabeçalho e dados 802.2	Seqüência de verificação de quadro

Figura 21 - Os frames Ethernet original e o 802.3 do IEEE

1-Preâmbulo:

Esse campo com 7 bytes de sequência 10101010, serve para sinaliza a existência de uma transmissão, e sincronizar as interfaces de rede.

2 –Inicio do delimitador de quadro:

Esse campo é composto por um byte, com o formato 10101011. O último bit igual a 1 marca o inicio do frame propriamente dito. Esses dois campos iniciais não são computados no tamanho total do cabeçalho.

3-Endereço de destino

Endereço físico do adaptador de destino. Esse endereço deve ser preenchido após o protocolo ARP (descrito na seção 5 a seguir) ter desempenhado sua função de traduzir o endereço de camada 3 em endereço de camada 2. Quando a interface de destino recebe um frame que não contenha o seu próprio endereço, nem o endereço de broadcast, descarta o frame.

Como os endereços MAC só tem validade na rede local, se o destinatário estiver em uma rede remota, esse campo será preenchido com o endereço do gateway da rede de origem.

4-endereço de origem

Obviamente, a interface não precisa de auxílio para preencher esse campo com o seu próprio endereço de hardware. Ele será usado pelo destinatário, para que possa encaminhar a resposta.

5- tipo/tamanho

O campo tipo/tamanho é que diferencia a tecnologia Ethernet do padrão IEEE 802.3. No Ethernet original, o tipo representa u protocolo de camada 3 que está

sendo transportado. No padrão do IEEE, esse campo representa o tamanho da unidade de dados que está sendo transportada nesse frame.

Como se na net-pizza o furgão trafegasse até o destino com a nota fiscal designando “pizzas de queijo”, pizzas calabresa, refrigerante, cerveja. Cada tipo poderia ter destinatários diferentes no destino. Os tipos são importantes. Imgine que o pessoal da net-pizza fez uma encomenda de suprimentos. Agora, eles estão atuando como clientes de um servidor remoto. Os suprimentos trafegam nas vias (camada física) dentro de furgões. São datagramas, portanto. Na chegada ao prédio da net-pizza, o furgão entra por uma porta da expedição. Os suprimentos serão encaminhados para cada departamento com base nas informações contidas nos campos de descrição das caixas. Se uma caixa contiver a descrição correspondente a “lenha”, será encaminhada ao pessoal do forno. Se for “azeitona” , será encaminhada ao pessoal da montagem das pizzas- Desde que o pessoal da expedição não esteja com muita vontade de comer.

O tipo no envelope digital representa o conteúdo do envelope: IP, IPX, ARP, AppleTalk são exemplos de protcolos que podem ser transportados pela Ethernet ou outra tecnologia de camada 2.

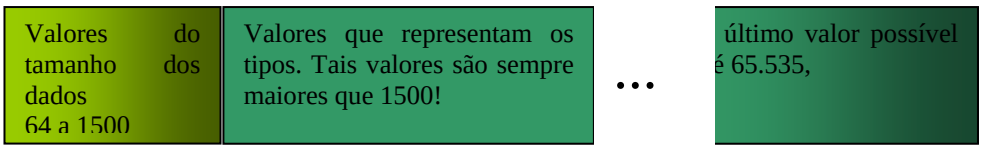
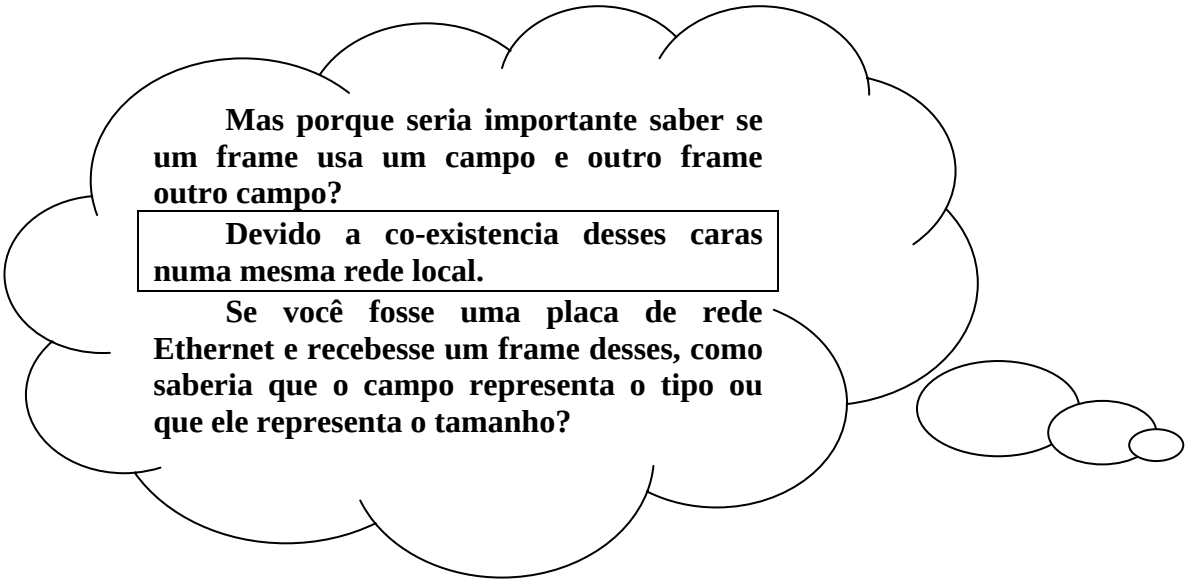


Figura 22 - Valores do campo tipo, de 16 bits (pode variar de 0 a 65.535)



O valor numérico do campo tipo/tamanho tem a resposta. O consórcio DIX designou poucos tipos de protocolos a serem transportados pelo envelope Ethernet, antes do estabelecimento do padrão 802.3. Como resultado, os valores numéricos sempre

foram maiores que o hexadecimal 0x0600. Em decimal, isso sempre será maior que 1536. Uma vez que o tamanho máximo de um frame Ethernet é de 1518 bytes (1500 de dados + 18 da soma dos tamnhos dos campos de cabeçalho), os valores nunca irão conflitar. Quando a interface de destino recebe o frame, verifica o campo tipo/tamanho, ela terá certeza que:

a) o campo está indicando tamanho se o valor for menor que 1536 (na verdade sempre menor que 1501).

b)significa o tipo de protocolo se o valor for maior que 1535, que marca o início dos valores dos tipos.

Os valores do campo tipo estão na RFC 1700. Acesse a página do IETF e encontre o valor do tipo para os protocolos IP e ARP. Transforme na calculadora os valores hexadecimais para decimais. Verifique se realmente correspondem com a solução descrita acima e com a Figura 1Figura 22.

6-Dados:

Esse é o "compartimento" onde são guardados os dados, ou o pacote oriundo da camada de rede acima. Normalmente é um datagrama IP. No padrão 802.3, podemos considerar ainda a inserção da subcamada LLC. Lembre-se que foi o IEEE quem dividiu a camada de enlace em LLC e MAC.

Na net-pizza, considere o espaço destinado para armazenar pizza no furgão.

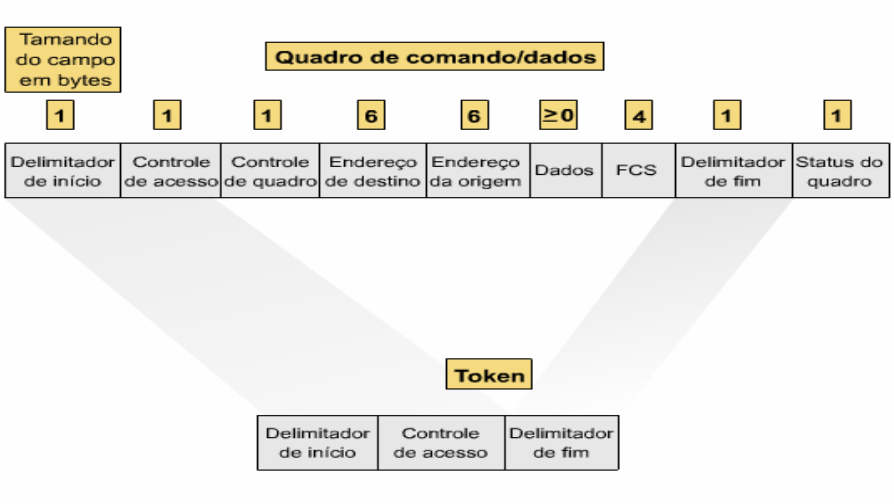
O campo de dados tem um tamanho que varia de 46 a 1500 bytes. A unidade máxima de transferência (MTU-Maximum Transfer Unit) do Ethernet é de 1500 bytes. Isso significa que se o datagrama IP tiver mais de 1500 bytes, deverá ser fragmentado. Se tiver menos que 46, o campo de dados deve ser "recheado" com stuff-bits 9 (bits de enchimento)

Na net-pizza, os stuff-bits seriam como um plastico bolha ou uma revestimento qualquer que ajustasse as pizzas no compartimento de menor tamanho do furgão.

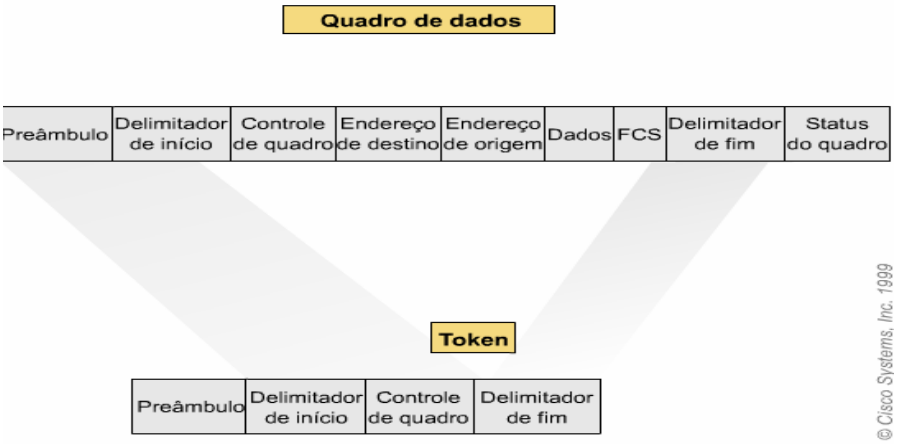
7-CRC (Verificação de redundância Cíclica)

Permite que a interface de destino verifique a existência de erros no quadro. Caso detecte erro, a interface de destino descarta o quadro. O destino não avisa sobre o descarte, nem sobre os erros. As camadas superiores (transporte e aplicação) é que irão tratar desse problema.

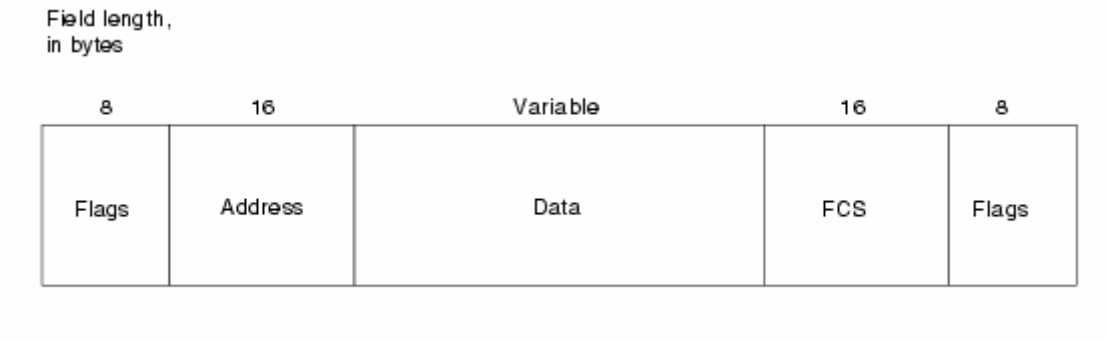
b) Token Ring



c) FDDI

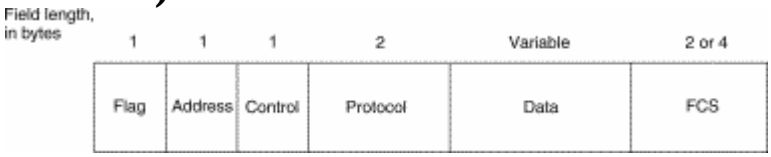


d) Frame Relay



Para saber mais sobre o frame relay:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/frame.htm

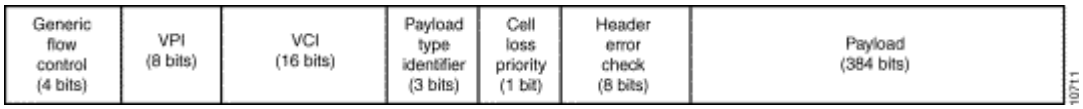
e) PPP



Para saber mais sobre o PPP

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ppp.htm

f) ATM



Veja mais sobre o ATM no site do ATM-forum: http://www.atmforum.com

Seção 5 - ARP, o protocolo de resolução de endereços

O Protocolo de resolução de Endereços, ARP, fornece um mecanismo para os dispositivos de rede TCP/IP localizarem o endereço de hardware de outros dispositivos na mesma rede. Esse mecanismo é necessário para que os dispositivos baseados no Ip se comuniquem.

O ARP está descrito na RFC 826, e está baseado em dois tipos de mensagem: Uma requisição (ARP request) e uma resposta (ARP reply). Esse método é rotineiro nas redes locais para que a origem da mensagem encontre o MAC address do destinatário.

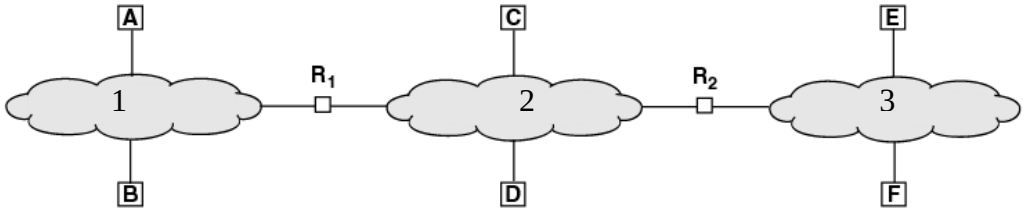


Figura 23 - 3 redes locais (1,2,3) conectadas por 2 roteadores (R1 e R2)

Na Figura 23, você pode notar 3 redes locais, conectadas por 2 roteadores. Como as requisições de ARP só tem validade nas redes locais, pois funcionam em broadcast, uma requisição na rede 1 seria processada pelas interfaces de A, de B e do roteador R1. Na rede 2, processariam os pacotes ARP as interfaces C, D e as dos roteadores R1 e R2.

ARP request

É a requisição, e contém o endereço IP que deve ser traduzido para o MAC address. Funciona sempre em broadcast (o endereço de broadcast é FF: FF: FF: FF: FF: FF). A interface (w) que precisa descobrir o MAC envia um quadro para todos as demais da mesma rede local situação (a) na
Figura 24.

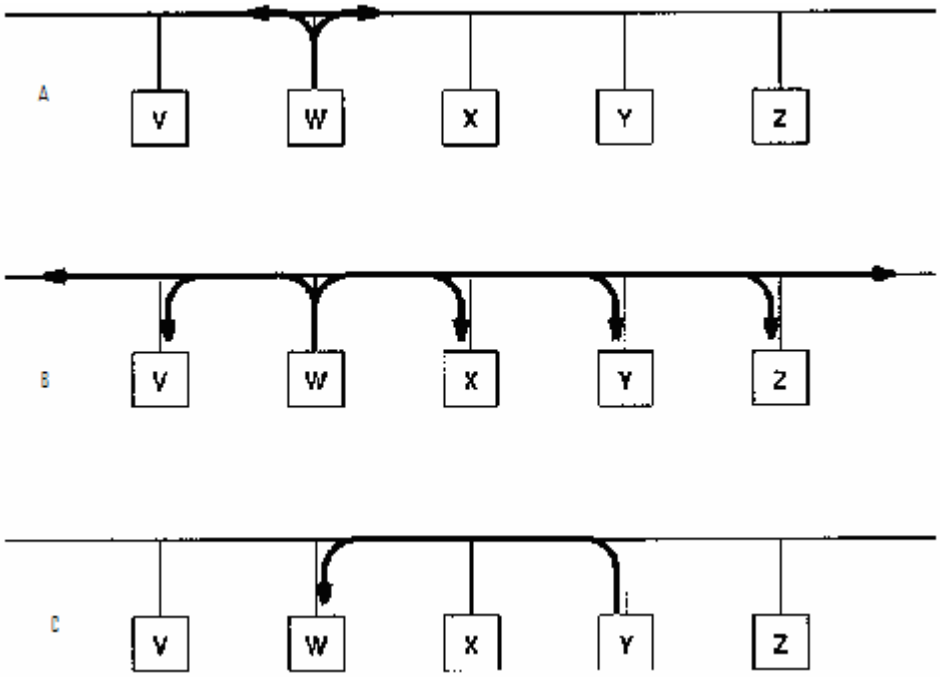


Figura 24 - ARP em funcionamento

Todas as interfaces processam o cabeçalho do ARP, entendem a requisção (b). A interface que possui o IP requisitado (Y) responde com seu MAC (c). Obviamente, essa resposta não é feita em broadcast, e sim em unicast, uma vez que a interface (Y) já sabe quem originou a requisição (W).

Na Figura 26, está representada a inserção das mensagens de ARP dentro do frame da rede local. Se o IP do destinatário não estiver na rede local, quem recebe o datagrama é o roteador (gateway) que se encarrega de repassá-lo para as redes remotasFigura 25.

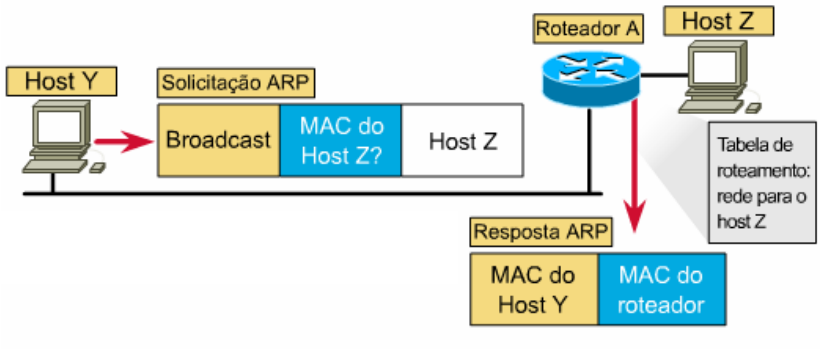


Figura 25 - Requisição ARP, hosts remotos

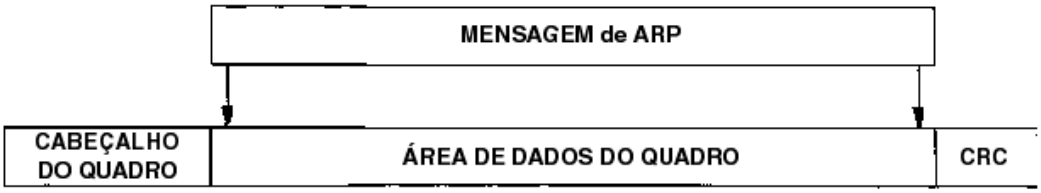


Figura 26 - Inserção dos dados ARP dentro do frame de camada 2

Para evitar que a cada envio de pacotes na rede deva existir uma resolução de endereços, o ARP mantém uma tabela com os endereços mais recentes (Figura 27). As entradas da tabela são retiradas assim que os hosts passarem um tempo sem comunicarem-se. A sequencia lógica do envio dos dados está na Figura 28.

Endereço IP	Endereço de Hardware
197.15.3.2	0A : 07 : 4B : 12 : 82 : 36
197.15.3.3	0A : 9C : 28 : 71 : 32 : 8D
197.15.3.4	0A : 11 : C3 : 68 : 01 : 99
197.15.3.5	0A : 74 : 59 : 32 : CC : 1F
197.15.3.6	0A : 04 : BC : 00 : 03 : 28
197.15.3.7	0A : 77 : 81 : 0E : 52 : FA

Figura 27 - Tabela de endereços armazenada no cache ARP

Para fazer on line:
1. Verifique a tabela arp do seu desktop com o comando ***arp –a*** no prompt do MS-DOS. 2. execute um ping para um host de sua rede, e teste o conteúdo da tabela novamente 3. Execute o ping para um host externo a rede (por exemplo, www.cisco.com) e verifique a tabela arp outra vez. 4. Espere algum tempo, por exemplo 5 minutos. 5. Teste a tabela novamente. 6. Explique o que aconteceu com a tabela.

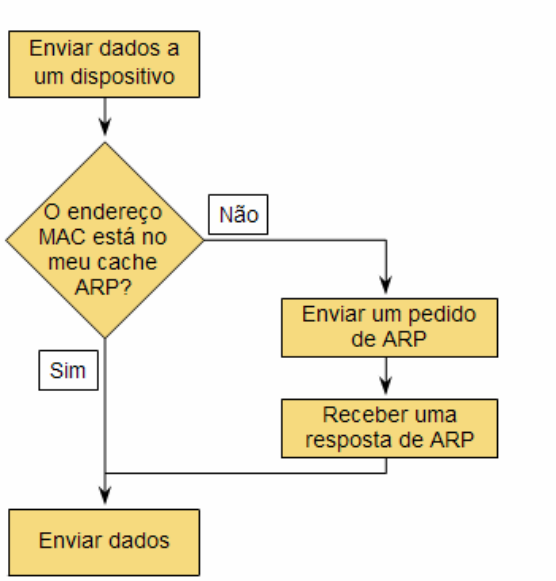


Figura 28 - Fluxograma do ARP

Para saber mais sobre a camada de enlace:

Charles Spurgeon's Ethernet Web Site
http://www.ethermanage.com/Ethernet
Informação extensa sobre Ethernet (IEEE 802.3), inclusive 100 Mbps Fast Ethernet (802.3u), 1000 Mbps Gigabit Ethernet (802.3z/802.3ab), e 10 Gigabit Ethernet (802.3ae).

Páginas de LANs de Godred Fairhurst's
http://www.erg.abdn.ac.uk/users/gorry/eg3561/lan-pages/enet.html
Godred Fairhurst da University of Aberdeen, mantém um conjunto de páginas Web sobre Ethernet, CSMA/CD, bridges, ARP e outros tópicos.

802.11 Planet.com
http://www.80211-planet.com/

Working Group for Wireless LAN Standards
http://grouper.ieee.org/groups/802/11

Bluetooth Sites
http://www.bluetooth.com/,
http://www.bluetooth.org/