REDES DE COMPUTADORES

Roteador

Em roteadores com capacidade limitada de processamento na porta de entrada, a porta pode simplesmente repassar o pacote para o processador de roteamento centralizado.

É esperado que o processamento da porta de entrada tenha capacidade de operar à velocidade da linha.

Geralmente os roteadores armazenam os registros das tabelas de repasse em uma estrutura de árvore de dados.

Roteador

Memórias de conteúdo endereçável (*Content Addressable Memories – CAMs*) permitem que um endereço IP de 32bits seja apresentado à CAM, que devolve o conteúdo do registro da tabela de repasse para o endereço em tempo essencialmente constante.

Após a determinação da porta de saída a ser utilizada, o pacote é repassado para o elemento de comutação. Mas, um pacote pode ser temporariamente impedido de entrar no elemento de comutação.

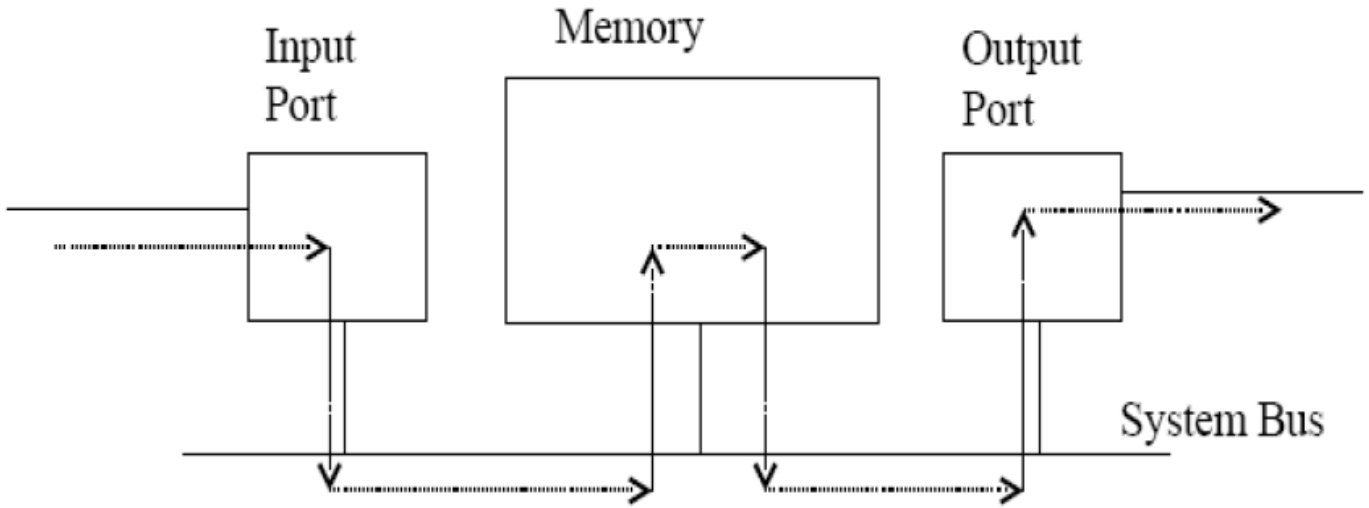
Um pacote impedido (bloqueado) deve entrar na fila da porta de entrada e então ser programado para atravessar o elemento de comutação.

Elemento de Comutação

- Comutação por memória
- Comutação por Barramento
- Comutação por uma rede de interconexão

Comutação por Memória

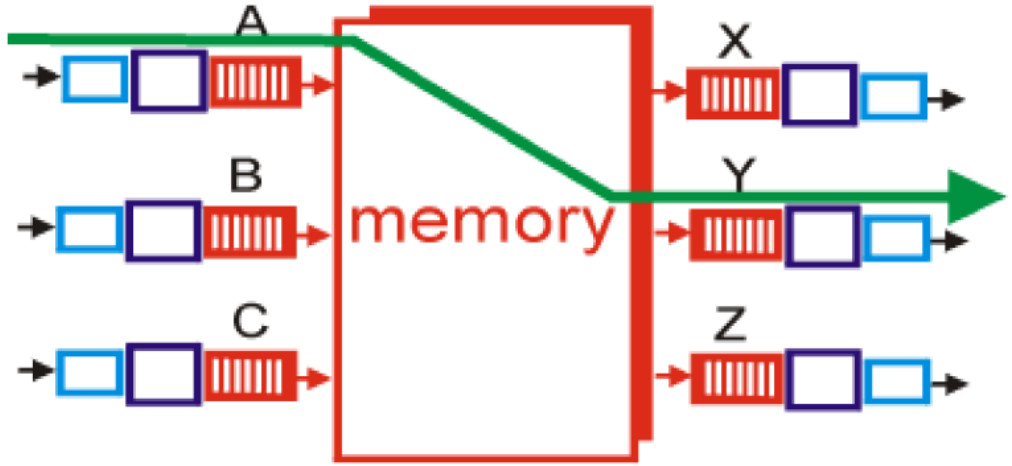
- Modelo mais simples de comutação.
- Os primeiros e mais simples roteadores quase sempre eram computadores tradicionais nos quais a comutação entre as portas de entrada e de saída era realizada sob o controle direto da CPU.



Comutação por Memória

As portas de entrada e saída funcionam como dispositivos tradicionais de entrada/saída de um sistema operacional tradicional.

Muitos roteadores modernos ainda comutam por memória, mas a consulta do endereço de destino e o armazenamento do pacote na localização adequada da memória são realizados por processadores nas placas de linha de entrada.



Comutação por um Barramento

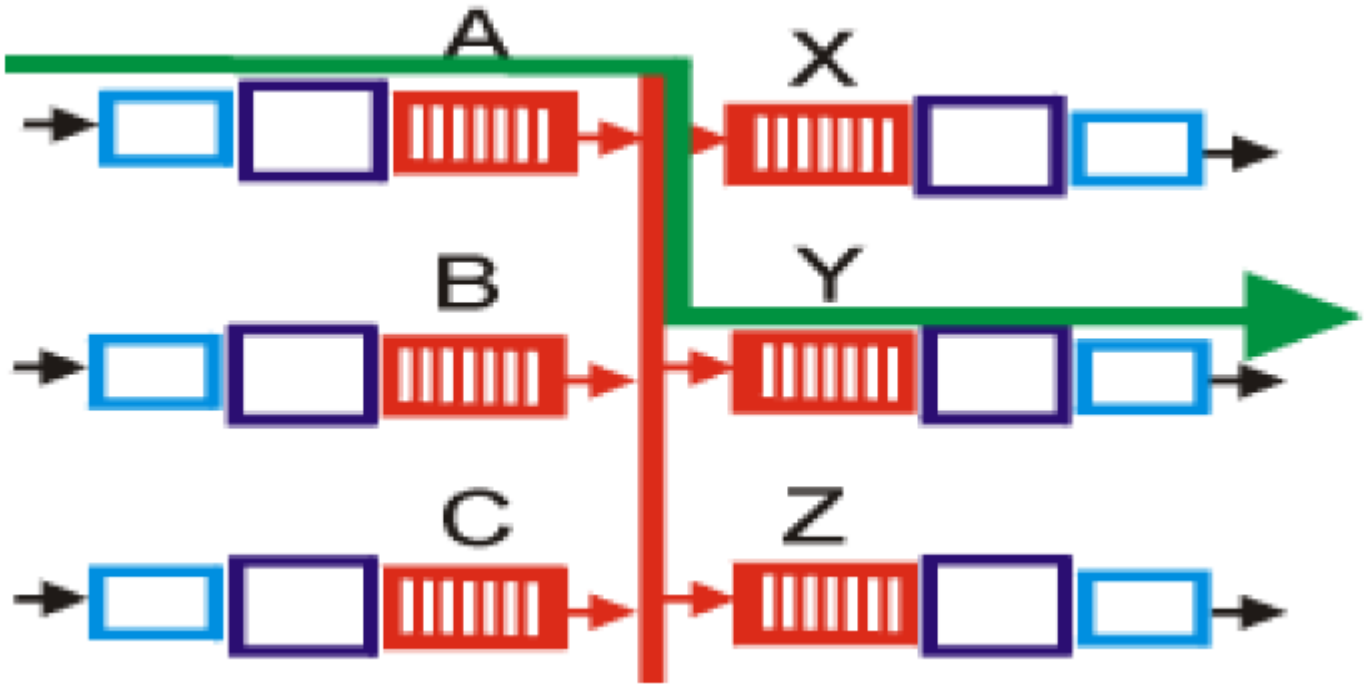
As portas de entrada transferem um pacote diretamente para a porta de saída por um barramento compartilhado sem a intervenção do processador de roteamento.

Como o barramento é compartilhado, somente um pacote por vez pode ser transferido por meio do barramento

Largura de banda de comutação do roteador fica limitada à velocidade do barramento.

A comutação por barramento muitas vezes é suficiente para roteadores que operam em redes de acesso e redes de empresas.

Comutação por um Barramento



Comutação por uma rede de Interconexão (*Crossbar*)

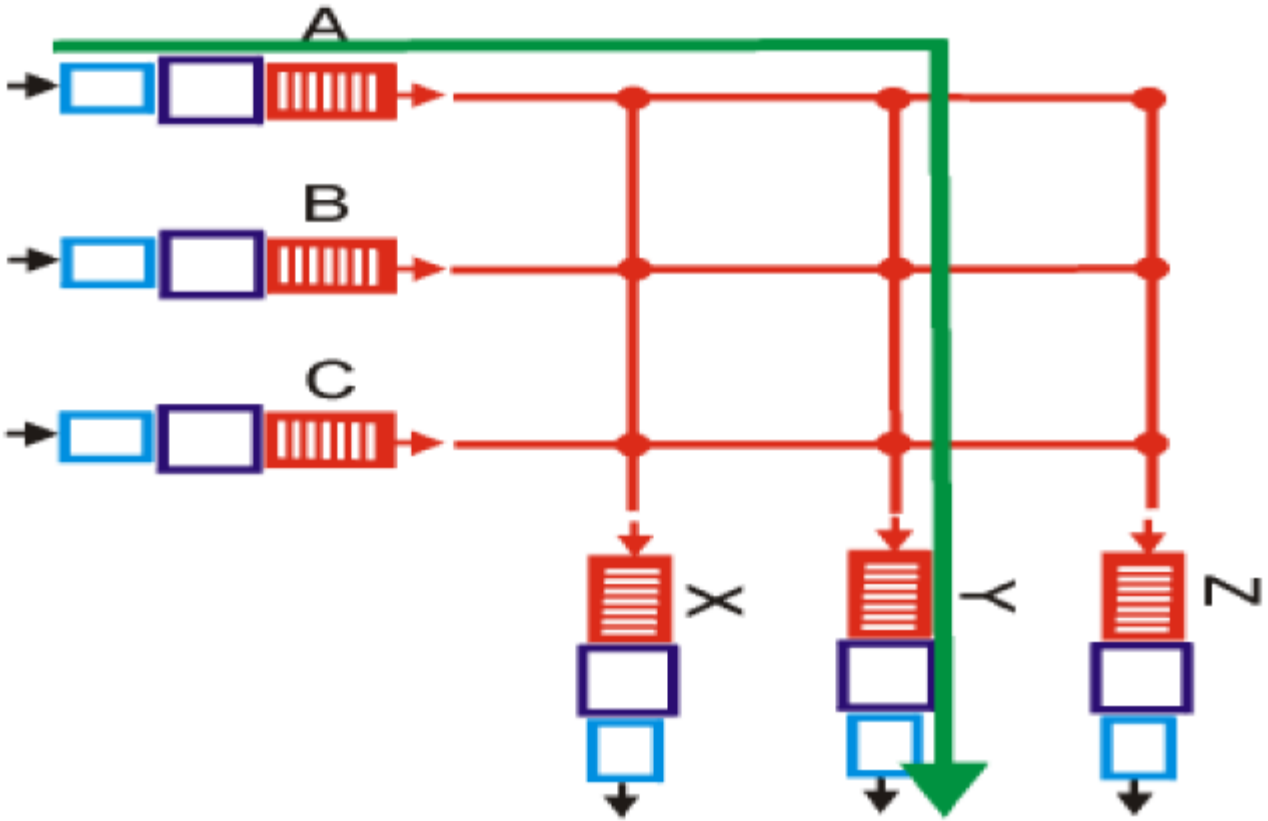
Basicamente uma rede dentro do roteador.

Desenvolvida para vencer a limitação da largura de banda da comutação por barramento.

É uma rede de interconexão que consistem em **2n** barramentos, conectando **n** portas de entrada a **n** portas de saída.

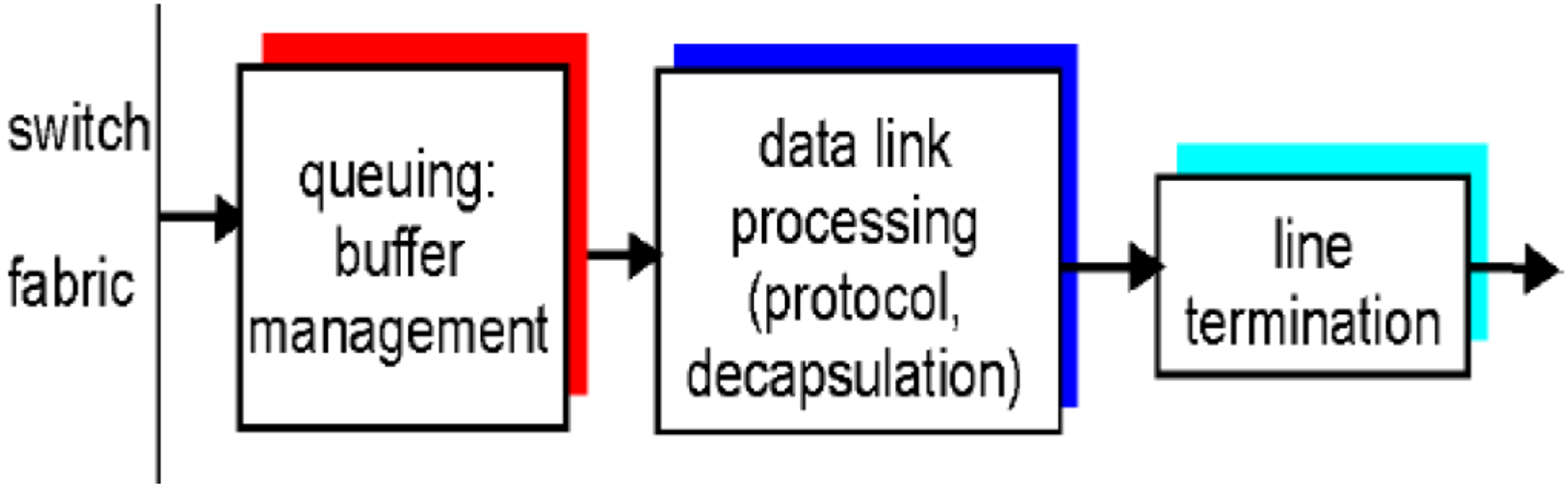
Uma tendência atual é fragmentar um datagrama IP de comprimento variável em células de comprimento fixo, marcar e comutar as células por meio da rede de interconexão.

Comutação por uma rede de Interconexão (*Crossbar*)



Portas de Saída

O processamento de portas de saída pega os pacotes que foram armazenados na memória da porta de saída, encapsula e transmite pelo enlace de saída.



Formação de Filas

Quando o tamanho da fila supera a capacidade de armazenamento do buffer ocorre a perda de pacotes.

O local real da perda do pacote dependerá da carga do tráfego, da velocidade relativa do elemento de comutação e da taxa da linha.

Roteamento

- Determinar o melhor caminho a ser tomado da origem até o destino.
- Se utiliza do endereço de destino para determinar a melhor rota.
- Roteador *default*, é o roteador ligado diretamente ao *host* (roteador do primeiro salto);
- Caminho de menor custo, é o caminho cuja soma do custo dos enlaces que ele percorre apresentam o menor valor;
- Caminho mais curto, o caminho com o menor número de saltos (roteadores);

Tipos de Algoritmos de Roteamento

Global

Calcula o caminho de menor custo entre uma fonte e um destino usando conhecimento completo e global sobre a rede;

Também denominado **algoritmo de estado de enlace** *(Link State* – LS*);*

Tem de possuir informações completas sobre a conectividade e o custo dos enlaces;

Descentralizado

O cálculo é realizado de forma distribuída e iterativa;

Não se tem conhecimento dos custos de todos enlaces da rede;

Baseia-se na troca de informações com o nó vizinho para cálculo da rota;

Também denominado **algoritmo de vetor de distâncias** (*Distance- Vector algorithm* – DV)

Tipos de Algoritmos de Roteamento

Algoritmos de Roteamento Estáticos

Tabelas fixas;

Alteradas de forma manual com pouca frequência;

Algoritmos de Roteamento Dinâmicos

As rotas são alteradas à medida que mudam as cargas de tráfego ou a topologia da rede;

Grafos

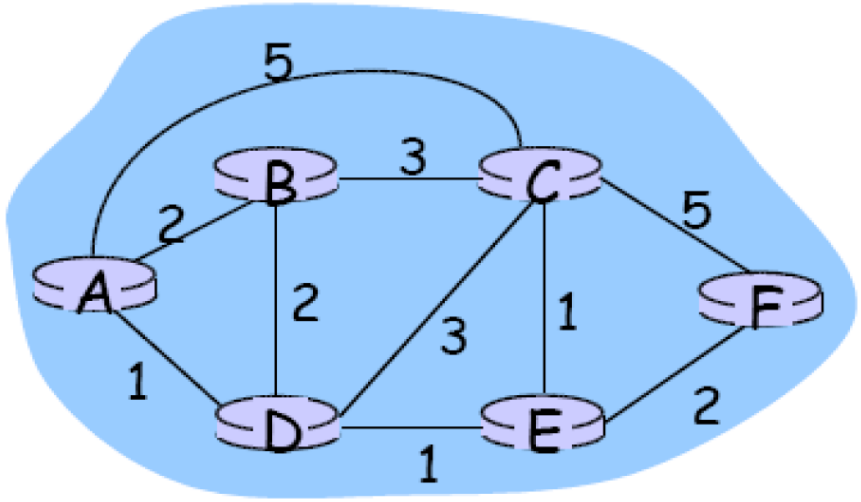
Um grafo é utilizado para formular problemas de roteamento.

No contexto do roteamento da camada de rede, os nós do grafo representam roteadores e as arestas que conectam esses nós representam os enlaces físicos entre esses roteadores.

Cada aresta tem um valor que representa seu custo.

O custo de um caminho é composto pelo somatório dos custos das arestas que compõem este caminho.

No caso de todos os caminhos terem o mesmo custo, é escolhido aquele que tiver menos saltos (caminho mais curto).



Algoritmo de Estado de Enlace

Cada nó transmite pacotes de estado de enlace a todos os outros nós da rede, sendo que cada um desses pacotes contém as identidades e os custos dos enlaces ligados a ele.

Um algoritmo comumente utilizado para determinar o melhor caminho é o algoritmo de Dijkstra.

O algoritmo de Dijkstra calcula o caminho de menor custo entre um nó e todos os outros nós da rede.

É um algoritmo iterativo e tem a propriedade de, após a n-ésima iteração, conhecer os caminhos de menor custo para 'n' nós de destino

Algoritmo de Dijkstra

1º passo: iniciam-se os valores

```
para todo v ∈ V[G]
d[v]← ∞
π[v] ← nulo

d[s] ← 0
```

2º passo: temos que usar o conjunto *Q*, cujos vértices ainda não contém o custo do menor caminho d[v] determinado.

```
Q ← V[G]
```

V[G] é o conjunto de vértices(v) que formam o Grafo G. d[v] é o vetor de distâncias de s até cada v. Admitindo-se a pior estimativa possível, o caminho infinito. π[v] identifica o vértice de onde se origina uma conexão até v de maneira a formar um caminho mínimo.

Algoritmo de Dijkstra

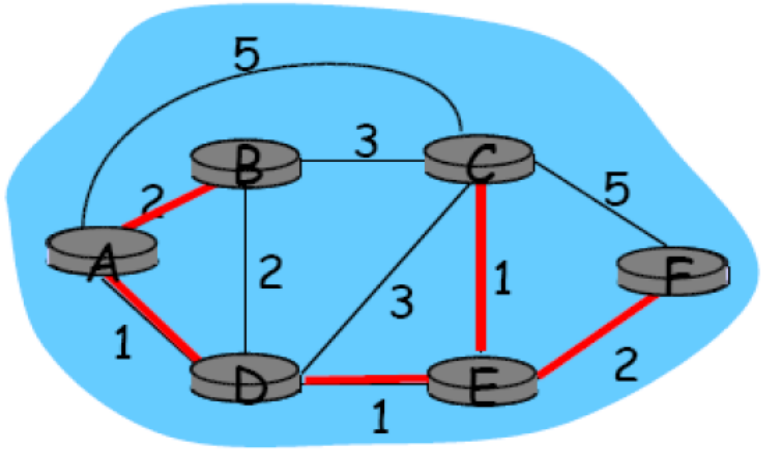
3º passo: realizamos uma série de **relaxamentos** das arestas, de acordo com o código:

```
enquanto Q ≠ ø
     u ← extrair-mín(Q) //Q ← Q - {u}
     para cada v adjacente a u
           se d[v] > d[u] + w(u, v) //relaxe (u, v)
               então d[v] ← d[u] + w(u, v)
               π[v] ← u

               Q ← Q ∪ {v}
```

Algoritmo de Dijkstra(ver animação)

Step	N	D(B),p(B)	D(C),p(C)	D(D),p(D)	D(E),p(E)	D(F),p(F)
0	A	2,A	5,A	1,A	infinity,-	infinity,-
1	AD	2,A	4,D	1,A	2,D	infinity,-
2	ADE	2,A	3,E	1,A	2,D	4,E
3	ADEB	2,A	3,E	1,A	2,D	4,E
4	ADEBC	2,A	3,E	1,A	2,D	4,E
5	ADEBCF	2,A	3,E	1,A	2,D	4,E



Algoritmo de Vetor de Distâncias

Iterativo: O processo continua até que mais nenhuma informação seja trocada entre os vizinhos.

Assíncrono: Não requer que todos os nós rodem simultaneamente

Distribuído: Cada nó recebe alguma informação de um ou mais vizinhos diretamente ligados a ele, realiza cálculos e, em seguida, distribui os resultados de seus cálculos para seus vizinhos.

Algoritmo de Bellman-Ford

- É utilizado para determinar qual o caminho de menor custo.
- Cada nó começa com os custos dos vizinhos ligados diretamente a ele.
- Cada nó envia, a intervalos regulares, uma cópia do seu vetor de distâncias a cada um de seus vizinhos.
- Quando um nó recebe um novo vetor de distâncias ele usa o algoritmo de Bellman-Ford para atualizar a sua tabela e a distribui.

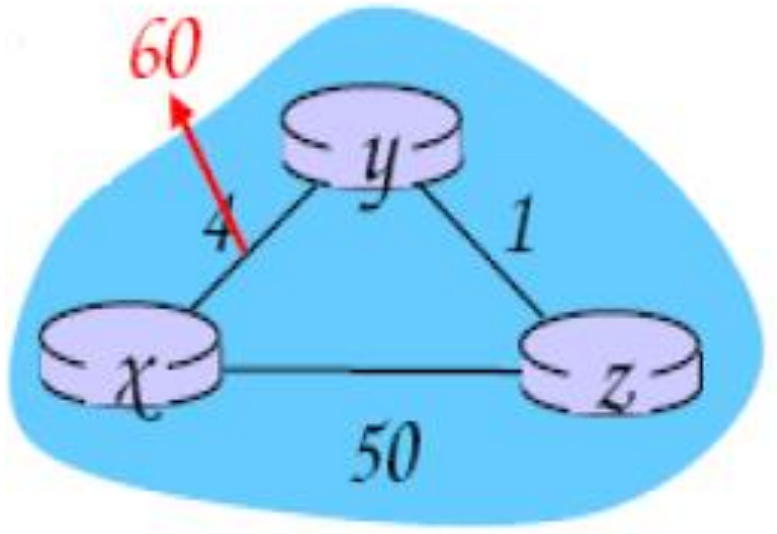
Mudanças de Custo do Enlace

Boas notícias se propagam rápido.

Más notícias se propagam devagar.

44 iterações até a estabilização.

Reversão envenenada:



- Evita o loop desnecessário.
- Se a rota de Z a X é por Y, então Z diz que seu custo para X é infinito.
- Não resolve totalmente o problema.

Comparação

	LS	DV
Complexidade da mensagem	Com n nós e E enlaces, O(nE) mensagens.	Troca de mensagens somente entre vizinhos.
Velocidade de convergência	Usa um algoritmo O(n2) e requer O(nE) mensagens, podendo haver oscilações	Tempo de convergência varia e pode ter loops de roteamento e a contagem até o infinito.
Robustez	O roteador pode informar um custo de enlace incorreto, mas cada nó calcula somente suas próprias tabelas	O roteador pode informar caminhos de custo incorreto. Um cálculo incorreto é difundido para a rede inteira.

Sistemas Autônomos

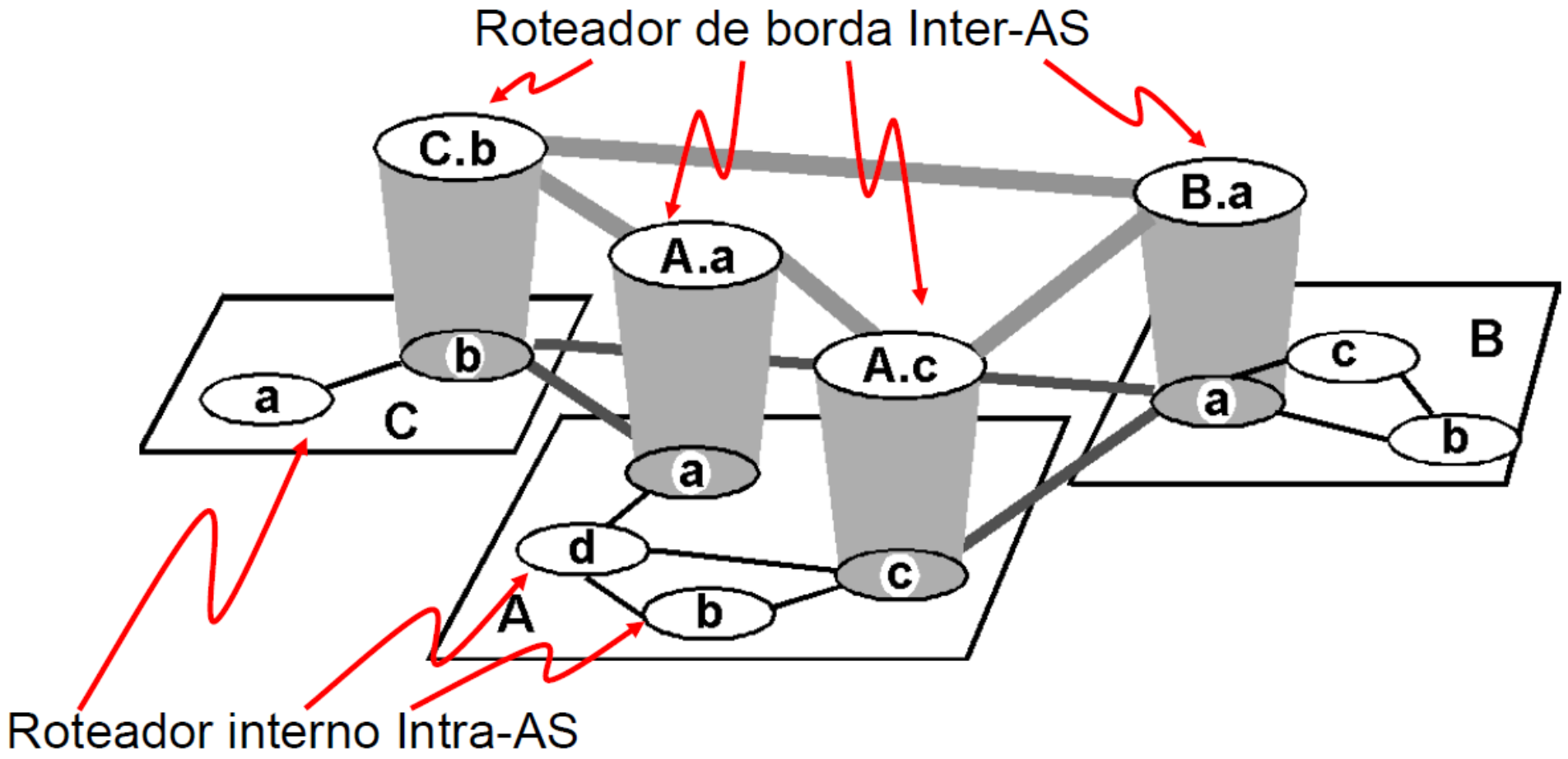
Os Sistemas Autônomos (*Autonomous Systems* – **AS**'s) foram criados por várias razões, principais:

- Escalabilidade, suportar o aumento constante na quantidade de roteadores;
- Autonomia administrativa, um certo ISP pode querer usar um algoritmo de roteamento de sua escolha, assim como não deixar visível informações da estrutura de sua rede;

O algoritmo que roda dentro de um AS é denominado protocolo de roteamento intra-sistema autônomo;

Roteadores de borda (***Gateway Routers***), são os roteadores que interconectam os AS's;

Sistemas Autônomos



Roteamento Intra-Sistema Autônomo

Interior Gateway Protocol – **IGP**;

Protocolos mais comuns:

- **RIP**;
- **OSPF**;
- **IGRP** (proprietário da CISCO);
- **EIGRP** (proprietário da CISCO);

RIP - *Routing Information Protocol*

Algoritmo do tipo vetor de distância;

O RIP 1.0 baseia-se na contagem de saltos ou *hops* (sub-rede percorrida) como métrica de custo;

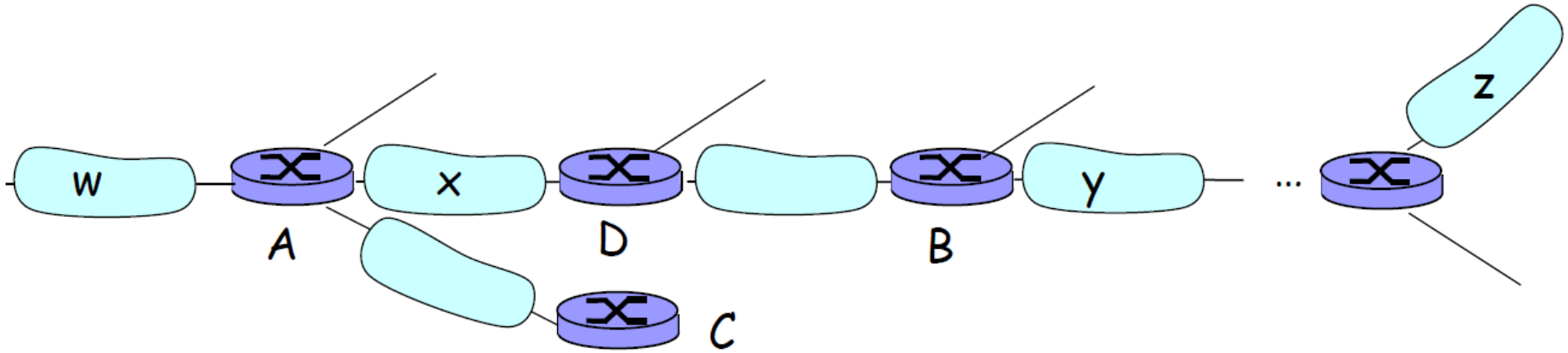
Os custos são definidos desde um roteador de origem até uma sub-rede de destino;

Custo máximo de um caminho é de 15 saltos;

Troca de informações (tabela de roteamento) a cada 30 segundos, usando uma mensagem de resposta RIP (anúncios RIP);

Cada anúncio RIP informa rotas para até 25 redes destino

RIP



Rede de Destino	Next Router	Num. de saltos para dest.
w	A	2
y	B	2
z	B	7
x	--	1
....	....	....

Tabela de roteamento em D

Após 180 segundos sem atualizações de um vizinho:

- O vizinho e o enlace são declarados mortos;
- Rotas através deste vizinho são anuladas;
- Novos anúncios são enviados quando as rotas são alteradas;
- A falha de um enlace se propaga rapidamente pela rede;
- ***Poison Reverse***, é um algoritmo utilizado para prevenir *loops*, isto é, evitar que a rota para um destino passe pelo próprio roteador que está enviando a informação de distância (distância infinita == 16 saltos);

Exemplo de tabela RIP

- 3 endereços classe C diretamente conectadas;
- Rota default (padrão) rota para endereços que não se enquadrem nas demais rotas;
- Endereço de rota *multicast* 224.0.0.0;
- *Loopback interface* 127.0.0.1, para depuração
- O protocolo RIP usa a porta 520 e o UDP dentro de um pacote IP padrão para transportar os anúncios;
- É um protocolo da camada de aplicação;

Destination	Gateway	Flags	Ref	Use	Interface
127.0.0.1	127.0.0.1	UH	0	26492	lo0
192.168.2.	192.168.2.5	U	2	13	fa0
193.55.114.	193.55.114.6	U	3	58503	le0
192.168.3.	192.168.3.5	U	2	25	qaa0
224.0.0.0	193.55.114.6	U	3	0	le0
default	193.55.114.129	UG	0	143454	

OSPF - *Open Shortest Path First*

Mais utilizado em ISP's de alto nível;

Protocolo disponível ao público (aberto – *Open*);

Usa um algoritmo do tipo *Link State* (LS):

Disseminação (*broadcast*) de pacotes LS;

Mapa topológico em cada nó;

Usa o algoritmo de Dijkstra para o cálculo da rota;

Custos dos enlaces determinados pelo administrador da rede;

As informações de roteamento (anúncios OSPF) são distribuídos para todos os roteadores e não somente para os vizinhos;

OSPF - *Open Shortest Path First*

É considerado robusto por monitorar de forma constante o estado dos enlaces;

Não impõe uma política para o modo como são determinados os pesos;

Transmite informações de estado do enlace sempre que houver mudanças, caso contrário, a cada 30 minutos envia informações de estado.

Os anúncios OSPF são transmitidos diretamente em pacotes IP, com um código de protocolo de camada superior igual a 89.

O próprio protocolo tem que implementar funcionalidades como transferência confiável de dados e transmissão *broadcast* de estado de enlace.

Avanços do OSPF

Segurança, trocas de dados autenticadas, podendo ser usada a autenticação simples ou a MD5 (através de chaves secretas compartilhadas), usa TCP para transporte de mensagens (porta 89);

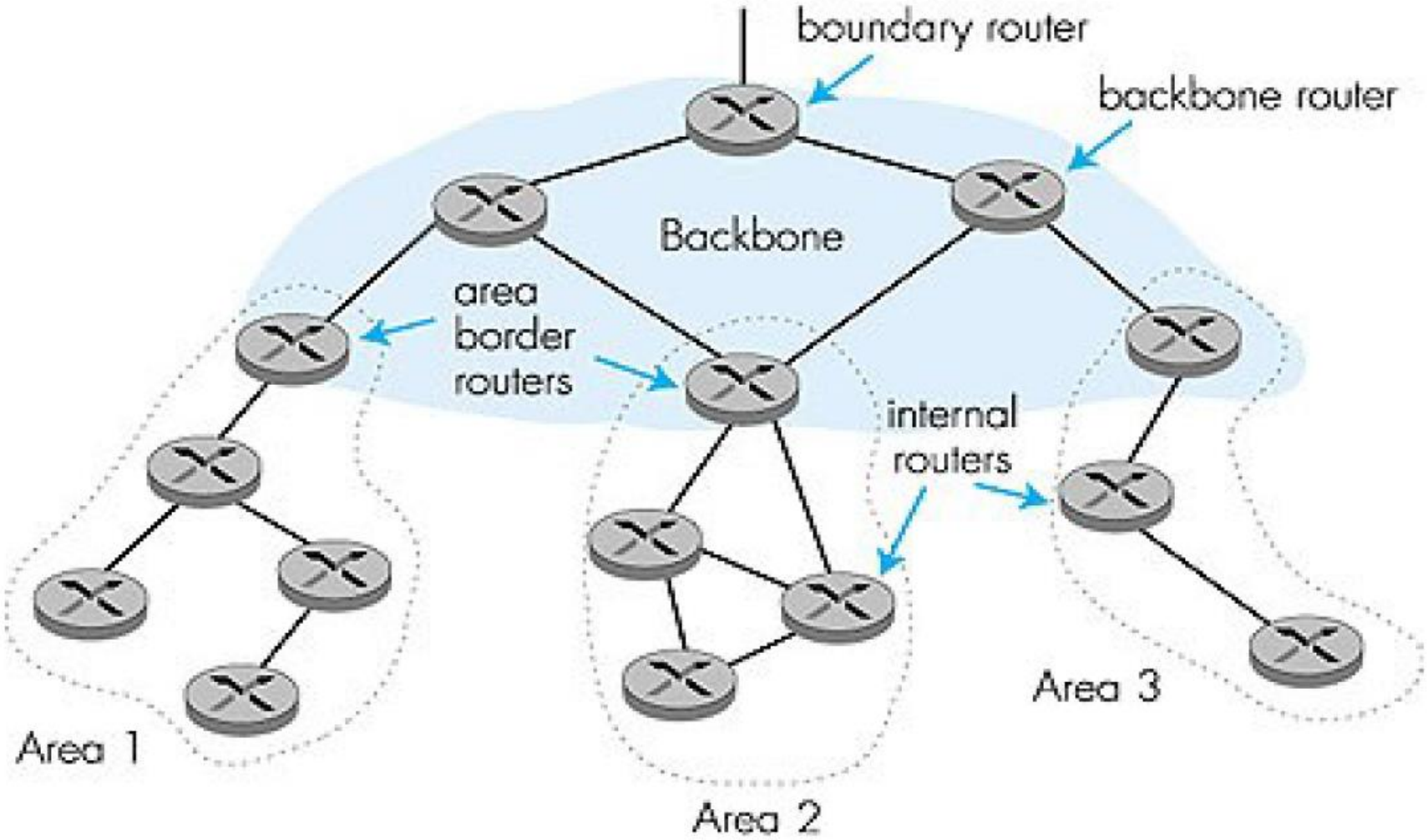
Caminhos múltiplos de igual custo, quando vários caminhos possuem o mesmo custo a carga é distribuída entre eles;

Múltiplas métricas para o mesmo enlace, a serem usadas de acordo com o tipo do serviço (***Type Of Service* – TOS**);

Suporte a roteamento *unicast* e *multicast*, através do OSPF *Multicast* (**MOSPF**) utilizando a mesma base de dados topológica do OSPF (RFC 1584);

Suporte a hierarquia dentro de um único domínio de roteamento, capacidade de estruturar hierarquicamente um AS.

Rede OSPF Hierarquicamente Estruturada



Rede OSPF Hierarquicamente Estruturada

Hierarquia de dois níveis, área local e *backbone*; ▪ Os anúncios de LS são enviados somente para roteadores dentro da mesma área local;

Cada nó tem uma visão detalhada da sua área e apenas caminhos mais curtos para outras redes;

Area borders routers (roteadores de borda de área), conectam a área ao *backbone*, são responsáveis por rotear os pacotes para fora da área local;

Backbone routers, responsáveis pelo roteamento de pacotes entre as áreas;

Bondary routers (roteadores de borda), responsáveis por fornecer a conexão entre AS's;

Internal routers (roteadores internos), contêm informações de sua área somente;

IGRP - *Interior Gateway Routing Protocol*

É um protocolo que foi desenvolvido na década de 80 pela Cisco Systems.;

Um protocolo de vetor de distância, mas possui uma métrica composta (atraso, banda, confiabilidade, carga...);

Usa o TCP para trocar informações;

O limite máximo de hops suportados pelo RIP (16) restringiu o crescimento das redes; a sua única métrica (contagem de hops) somente de balançar da carga de igual custo não permitiu muita flexibilidade de roteamento em ambientes complexos;

IGRP é um Protocolo de Gateway Interior do vetor da distância (IGP)

BGP – *Border Gateway Protocol*

A versão 4 do BGP (BGP4) é o padrão para roteamento entre AS's na internet;

Agoritmo *Path Vector* (vetor de caminho):

Similar ao protocolo *Distance Vector*;

Cada roteador de borda envia nos seus *broadcasts* aos seus vizinhos o caminho inteiro (a sequência de AS's) até o destino;

Utiliza conexões semipermanentes TCP (porta 179) para transferência de informações entre roteadores (podem ocorrer inter-AS ou intra- AS);

Todo AS é identificado por um número de sistema autônomo (***Autonomous System Number* – ASN**)

BGP

Sessão BGP, conexão TCP semipermanente entre dois roteadores.

Sessão BGP externa (eBGP), sessão entre roteadores de diferentes AS´s.

Sessão BGP interna (iBGP), sessão entre roteadores dentro de um mesmo AS.

Permite que cada AS conheça quais **destinos** podem ser alcançados via seus **AS´s vizinhos**

Quando um roteador anuncia um prefixo de rede através de uma sessão BGP, são enviados vários atributos, entre eles os mais importantes são:

AS-PATH, contém os AS's pelos quais passou o anúncio para o prefixo, usado para evitar loops de anúncios;

NEXT-HOP, informa por qual endereço o anúncio foi enviado (para indicar a interface pela qual foi enviado o anúncio);

BGP – Seleção de Rota

Para determinar qual rota utilizar, o BGP se vale algumas regras, entre elas:

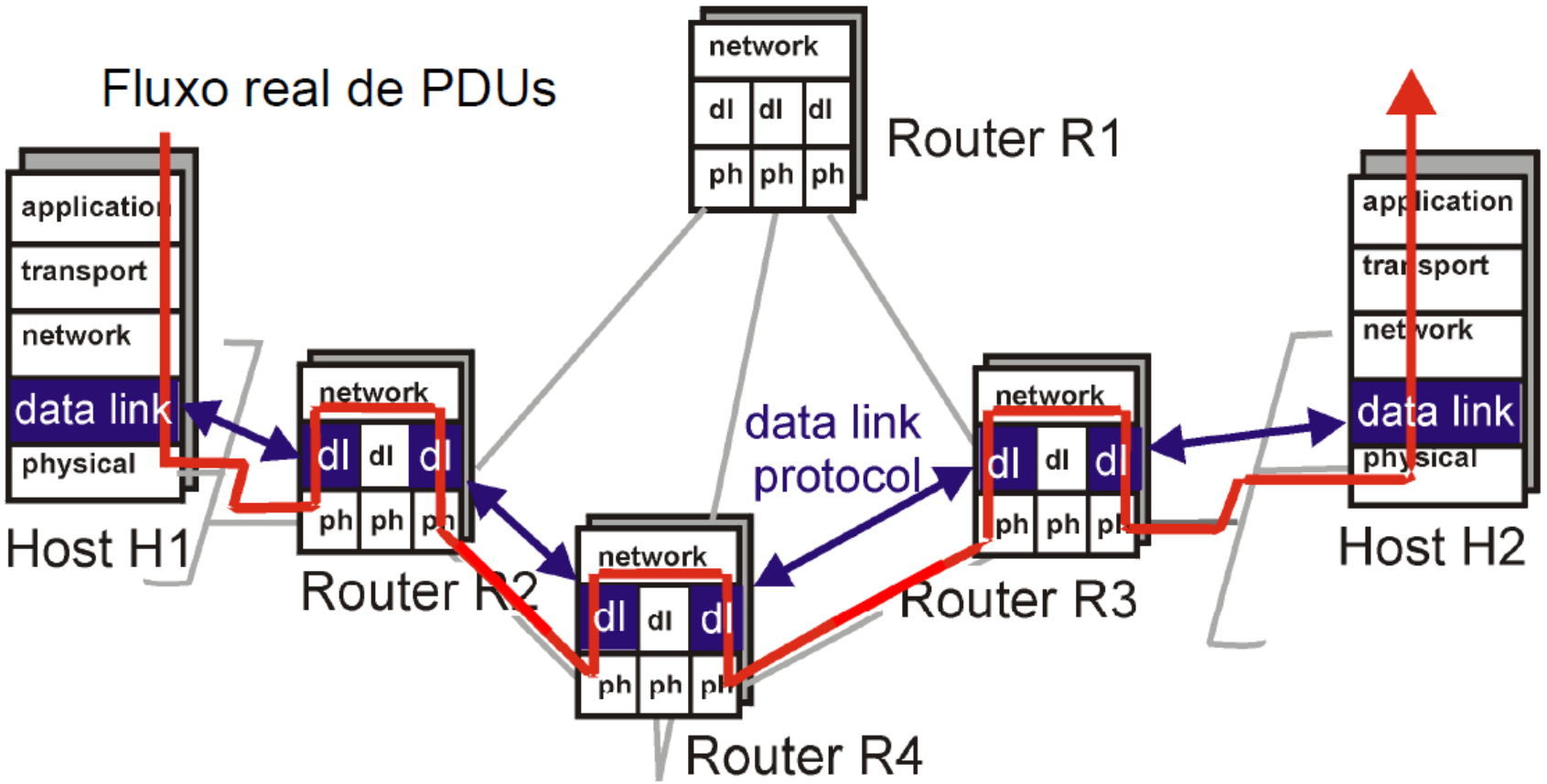
1)Valor de preferência indicada pelo administrador da rede;

2)Rota com o AS-PATH mais curto;

3)Rota com o NEXT-HOP mais próximo (caminho de menor custo determinado pelo algoritmo Intra-AS);

4)Se houver mais de uma rota, são utilizados identificadores BGP para selecionar a rota.

Camada de Enlace


Fluxo real de PDUs
application
transport
network
data link
physical
Host H1
network
dl dl dl
ph ph ph
Router R1
network
dl dl dl
ph ph ph
Router R2
network
dl dl dl
ph ph ph
Router R4
data link
protocol
network
dl dl dl
ph ph ph
Router R3
application
transport
network
data link
physical
Host H2

Tarefas Básicas da camada de enlace

- Conexão dos enlaces, ativação e desativação. Estas funções incluem o uso de facilidades multiponto físico para suportar conexões em funções da camada de rede.
- Mapeamento de unidades de dados para a camada de rede dentro das unidades do protocolo de enlace para transmissão.
- Multiplexação de um enlace de comunicação para várias conexões físicas.
- Delimitação de unidades de transmissão para protocolos de comunicação.
- Detecção, notificação e recuperação de erros.
- Identificação e troca de parâmetros entre duas partes no enlace.

Protocolos da camada de enlace

Protocolos da camada de enlace

- 802.11 (Wi-Fi);
- Ethernet;
- Token ring;
- PPP;

O protocolo da camada de enlace é responsável por transportar datagramas da camada de rede de um nó até outro nó em um único enlace. Um datagrama pode ser manipulado por diferentes protocolos de enlace nos diferentes enlaces do caminho até o host destino.

Serviços da Camada de Enlace

Enquadramento de dados, quase todos os protocolos da camada de enlace encapsulam cada datagrama dentro de um único quadro antes de transmiti-lo pelo enlace;

Acesso ao enlace, um protocolo de controle de acesso ao meio (***Medium Access Control protocol*** **– MAC**) especifica as regras que ditam a forma como o quadro será transmitido pelo enlace;

Entrega confiável, quando oferecido, é garantida a entrega de um datagrama pela camada de enlace sem erros;

Controle de Fluxo, para evitar perda de dados;

Detecção de erros, é um serviço comum entre protocolos da camada de enlace;

Correção de erros, similar a anterior, com a diferença que o protocolo pode determinar o local do erro e possivelmente corrigí-lo;

Endereços de LAN

Endereços IP de 32-bit:

Endereços da *camada de rede;*

Usados para levar o datagrama até a rede de destino;

Estrutura hierárquica.

Endereço de LAN (ou MAC ou físico):

Usado para levar o datagrama de uma interface física a outra fisicamente conectada com a primeira (isto é, na mesma rede);

Endereços MAC com 48 bits (na maioria das LANs) gravados na memória fixa (ROM) do adaptador de rede

Endereço não-hierárquico e único.

Address Resolution Protocol - ARP

Cada nó IP (hospedeiro, roteador) numa LAN tem um módulo e uma tabela ARP;

Tabela ARP: mapeamento de endereços IP/MAC para alguns nós da LAN

< endereço IP; endereço MAC; TTL>

TTL (*Time To Live*): tempo depois do qual o mapeamento de endereços será esquecido (tipicamente 20 min)

Funcionamento do ARP

A quer enviar um datagrama para B, e o endereço MAC de B não está na tabela ARP de A;

A faz *broadcast* de pacote de consulta ARP, contendo o endereço IP de B:

end. MAC de destino = FF-FF-FF-FF-FF-FF;

todas as máquinas na LAN recebem a consulta ARP.

B recebe o pacote ARP, responde para A com seu endereço MAC (de B)

Quadro enviado para o endereço MAC de A (*unicast*)

A faz um cache (salva) o par de endereços IP para MAC em sua tabela ARP até que a informação se torne antiga (expirada) *soft state*: informação que expira (é descartada) sem atualização.

ARP é “plug-and-play”:

 Nós criam suas tabelas ARP sem intervenção do administrador da rede.

Roteamento para outra LAN

A cria o pacote IP com origem A, destino B;

A usa ARP para obter o endereço de camada física de R correspondente ao endereço IP 111.111.111.110;

A cria um quadro *Ethernet* com o endereço físico de R como destino, o quadro *Ethernet* contém o datagrama IP de A para B;

A camada de enlace de A envia o quadro *Ethernet*;

A camada de enlace de R recebe o quadro *Ethernet*;

R remove o datagrama IP do quadro *Ethernet*, verifica que ele se destina a B;

R usa ARP para obter o endereço físico de B;

R cria quadro contendo um datagrama de A para B e envia para B.

DHCP

Protocolo cliente-servidor. Imagine um cliente é um *host* que acabou de chegar e quer obter informações sobre a configuração de rede, incluindo um endereço IP para si mesmo;

Algumas redes utilizam um *agent relay* DHCP (geralmente um roteador) que encaminha as mensagens de e para o servidor DHCP que se encontra em outra rede, vejamos as etapas da Descoberta de um Endereço:

- Descoberta de servidor DHCP: Através de uma **mensagem de descoberta DHCP** que um cliente envia dentro de um pacote UDP à porta 67, é enviado pela rede com endereço de *broadcast* de destino e origem com 0.0.0.0;
- Oferta(s) de servidor DHCP: Um servidor DHCP que receba a mensagem de descoberta DHCP responde com uma **mensagem de oferta DHCP**, contendo um endereço IP, mascara de rede, tempo do aluguel do endereço IP e outras informações de rede (se necessário);
- Requisição DHCP: O cliente escolhe entre as ofertas e responde ao servidor da oferta selecionada com a **mensagem de requisição DHCP**;
- DCHP ACK: O servidor responde à mensagem de requisição DHCP com uma mensagem **DCHP ACK**, confirmando os parâmetros requisitados.

Ethernet

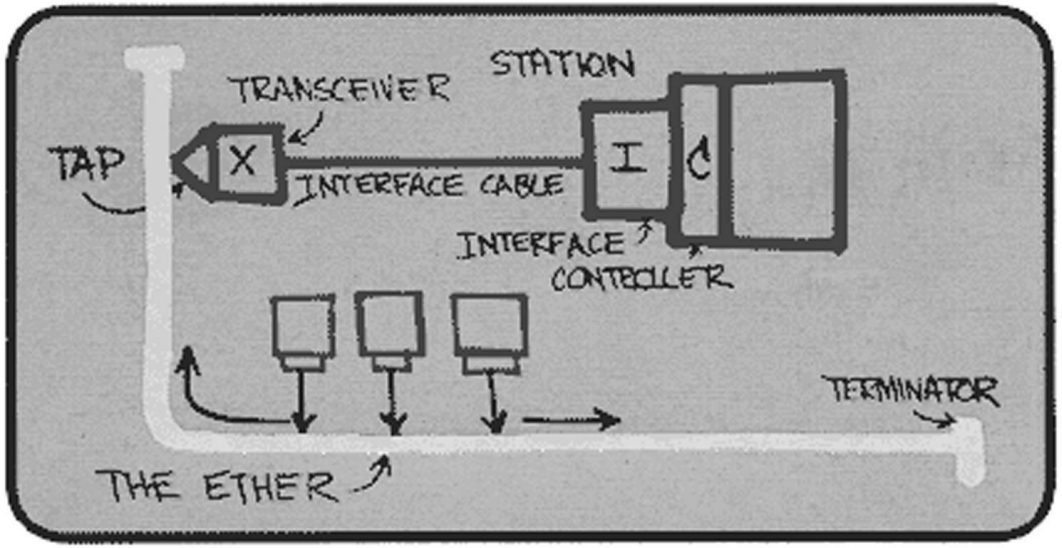
Tecnologia de rede local “dominante”

Primeira tecnologia de LAN largamente usada;

Mais simples e mais barata que LANs com token e ATM;

Velocidade crescente: 10 Mbps – 10 Gbps.

Esboço da *Ethernet* por Bob Metcalf



Topologia *Ethernet*

Topologia de bus popular em meados dos anos 90;

Agora a topologia em estrela prevalece;

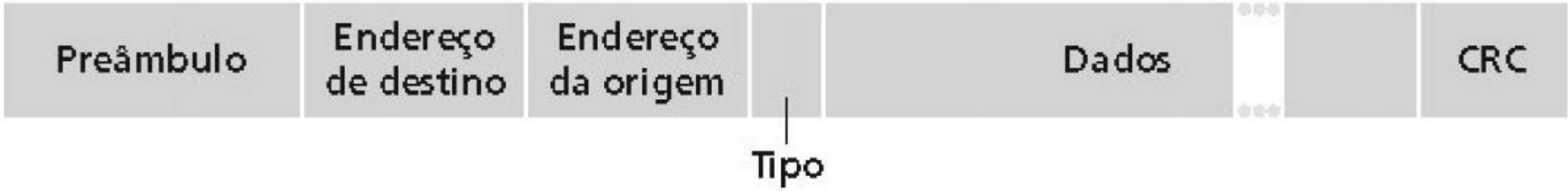
Opções de conexão: hub ou switch.

Quadro Ethernet

Adaptador do transmissor encapsula o datagrama IP (ou outro pacote de protocolo da camada de rede) num quadro Ethernet;

Preâmbulo: 8 bytes

- 7 bytes com padrão 10101010 seguido por um byte com padrão 10101011;
- Usado para sincronizar as taxas de relógio do transmissor e do receptor.



Quadro Ethernet

Endereços: 6 bytes. Se o adaptador recebe um quadro com endereço de destino coincidente ou com endereço de broadcast (ex., pacote ARP), ele passa o dado no quadro para o protocolo da camada de rede;

Tipo: indica o protocolo da camada superior geralmente é o protocolo IP, mas outros podem ser suportados, tais como Novell IPX e AppleTalk;

CRC: verificado no receptor; se um erro é detectado, o quadro é simplesmente descartado.

Serviço Ethernet

Sem conexão: não ocorre conexão entre o adaptador transmissor e o receptor;

Não confiável: adaptador receptor não envia ACKs ou NACKs para o adaptador transmissor;

O fluxo de datagramas que passa para a camada de rede pode deixar lacunas;

Lacunas serão preenchidas se a aplicação estiver usando TCP;

Caso contrário, a aplicação verá as lacunas.

CSMA/CD

CSMA/CD (*Carrier Sense Multiple Access/Colision Detection* – Acesso múltiplo com detecção de portadora com detecção de colisão);

Adaptador não transmite se ele detectar algum outro adaptador transmitindo, isto é, *carrier sense*;

O adaptador transmissor aborta quando detecta outro adaptador transmitindo, isto é, *collision detection*;

Antes de tentar uma retransmissão, o adaptador espera um período aleatório, isto é, *random access*;

10Base T e 100Base T

Taxa de 10/100 Mbps; chamado mais tarde de "*fast ethernet*";

T significa "*Twisted Pair*" (par de fios trançados de cobre);

Nós se conectam a um *hub*: "topologia em estrela"; 100 m é a distância máxima entre os nós e o *hub*;

Gigabit Ethernet

Usa o formato do quadro do *Ethernet* padrão;

Permite enlaces ponto-a-ponto e canais de múltiplo acesso compartilhados;

No modo compartilhado, o CSMA/CD é usado;

Exige pequenas distâncias entre os nós para ser eficiente;

Usa *hubs*, chamados aqui de Distribuidores com Armazenagem "*Buffered Distributors*";

Full-duplex a 1 Gbps para enlaces ponto-a-ponto;

10 Gbps agora!

HUBS

Hubs são essencialmente repetidores de camada física:

- Bits que chegam de um enlace se propagam para todos os outros enlaces;
- Com a mesma taxa;
- Não possuem **armazenagem de quadros;**
- Não há CSMA/CD no hub: adaptadores detectam colisões;
- Provê funcionalidade de gerenciamento de rede.

Interconexão com Hubs

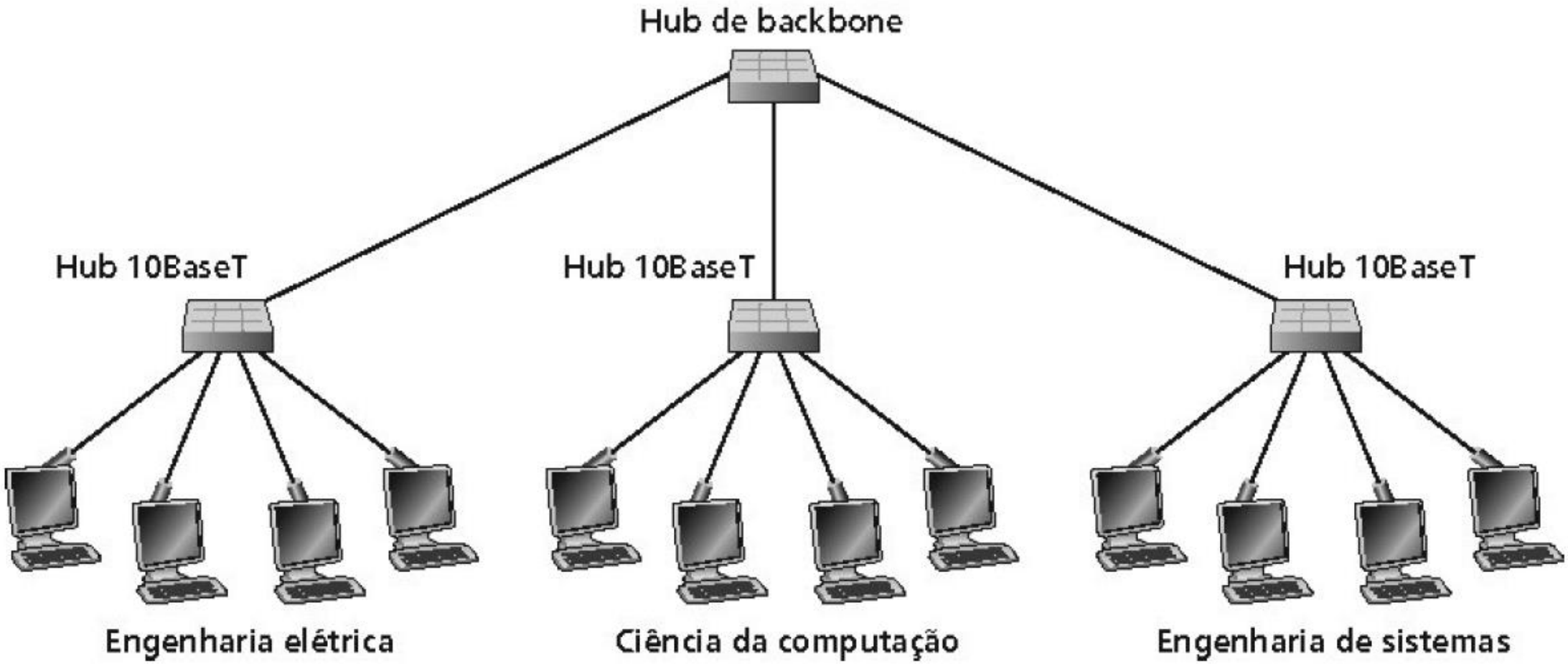
Hub de *backbone* interconecta segmentos de LAN;

Estende a distância máxima entre os nós;

No entanto, domínios de colisão individuais tornam-se um único e grande domínio de colisão;

Não pode interconectar 10BaseT e 100BaseT;

Interconexão com Hubs



SWITCH

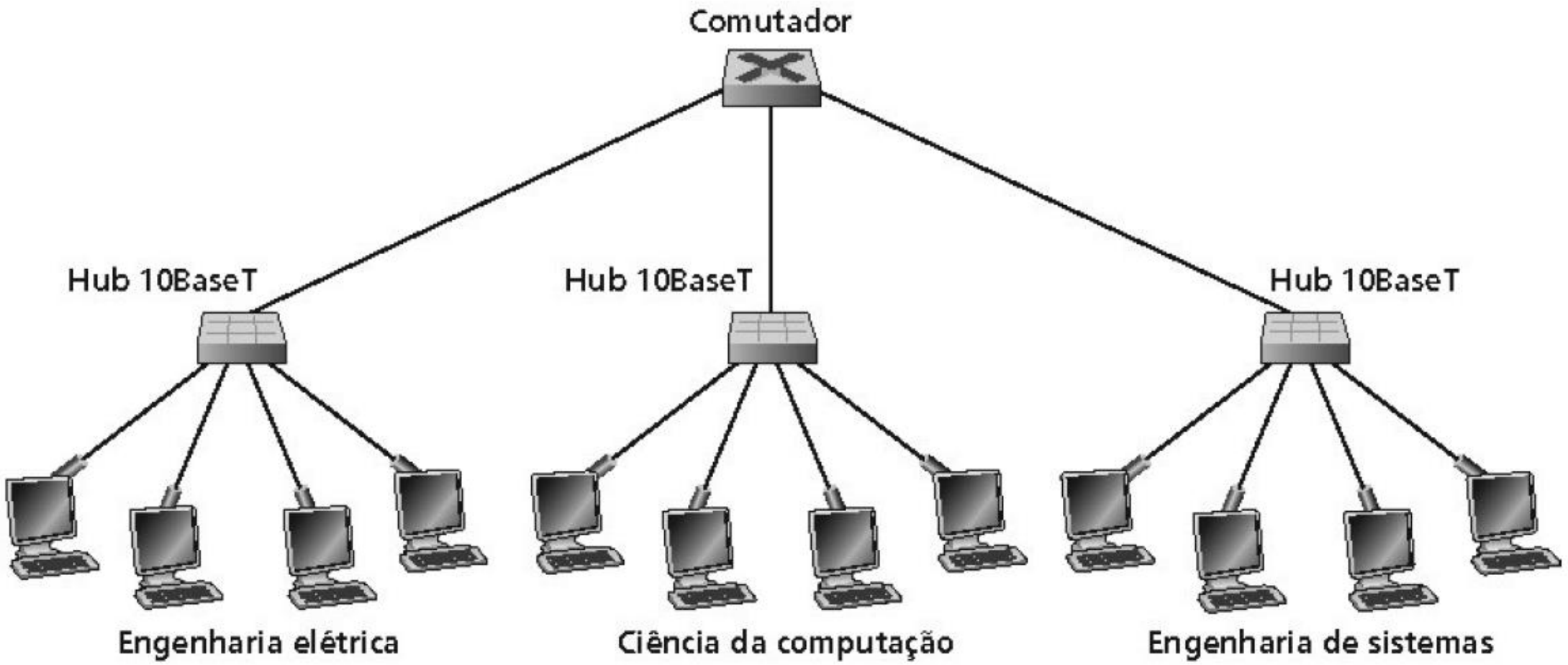
Dispositivo de camada de enlace:

- Armazena e encaminha quadros *Ethernet*;
- Examina o cabeçalho do quadro e seletivamente encaminha o quadro baseado no endereço MAC de destino;
- Quando um quadro está para ser encaminhado no segmento, usa CSMA/CD para acessar o segmento;

Transparente:

- Hospedeiros são inconscientes da presença dos *switches Plug-and-play*, *self-learning* (auto-aprendizado)
- *Switches* não precisam ser configurados

Encaminhamento



Auto-Aprendizado

Um *switch* possui uma tabela de *switch*;

Entrada na tabela do *switch*:

- Endereço MAC, interface, marca de tempo;
- Entradas expiradas na tabela são descartadas (TTL pode ser 60 min).

Switch **aprende** quais hospedeiros podem ser alcançados através de suas interfaces:

- Quando recebe um quadro, o *switch* "aprende" a localização do transmissor: segmento da LAN que chega;
- Registra o par transmissor/localização na tabela.

Full-Duplex e sem colisões.

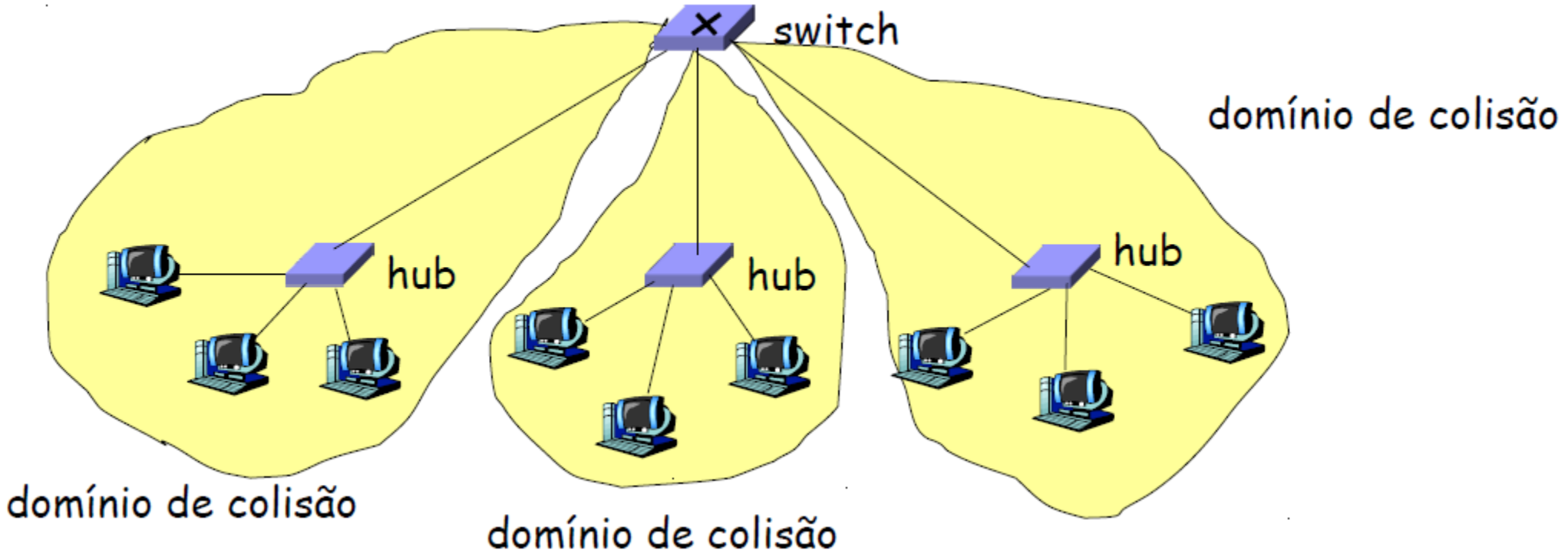
Isolação de Tráfego

A instalação do *switch* quebra as sub-redes em segmentos de LAN;

Switch filtra pacotes:

- Alguns quadros do mesmo segmento de LAN não são usualmente encaminhados para outros segmento de LAN;
- Segmentos se tornam separados em domínios de colisão.

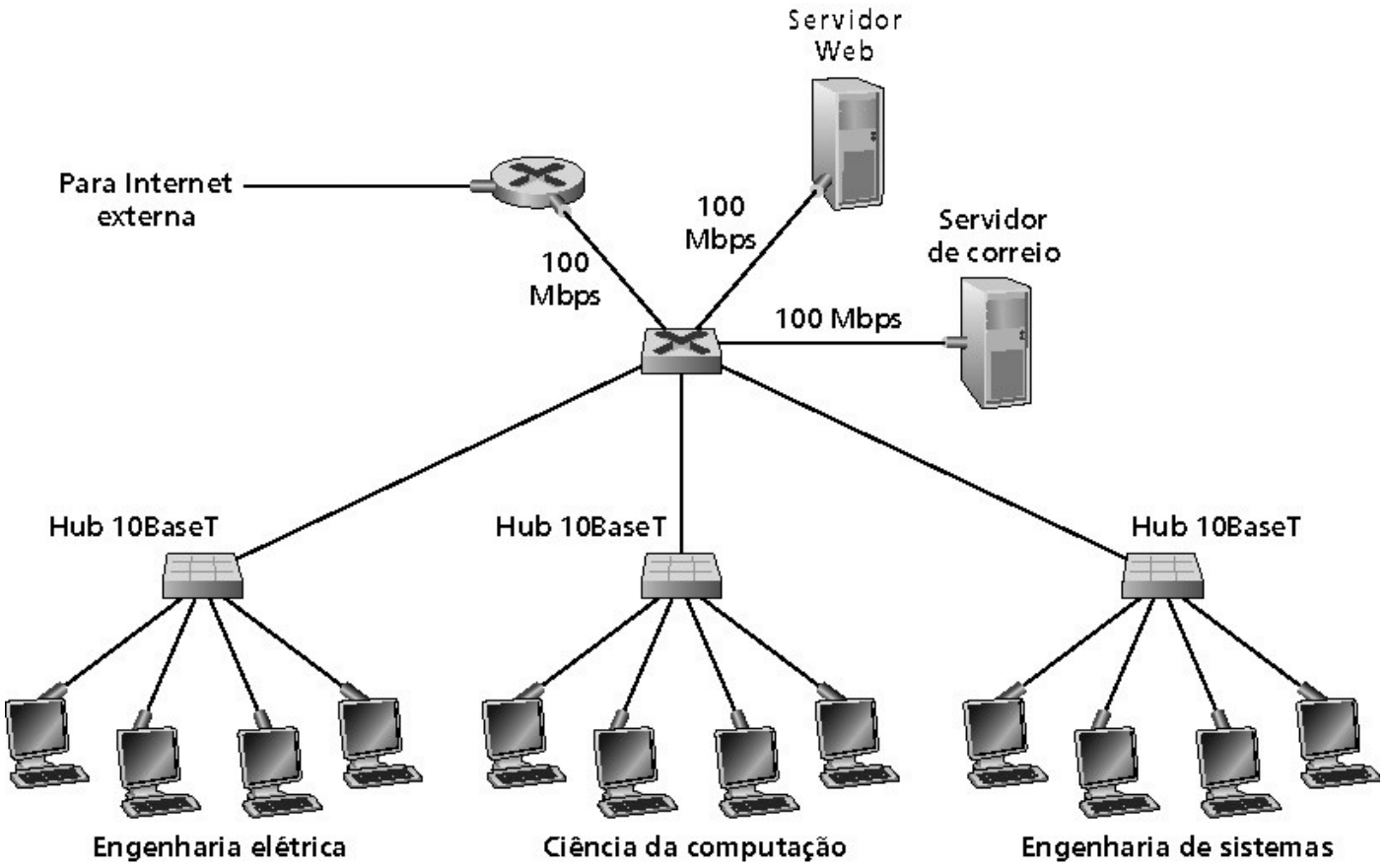
Segmentação



Características de *Switches*

Cut-Through: O *switch* lê somente a parte do cabeçalho que contêm os endereços e o encaminha ao destino (mais rápido que o *storeand- forward*);

Store-and-Forward: Tipo mais comum de funcionamento, o *switch* lê todo o quadro antes de enviá-lo.



Switches versus Roteadores

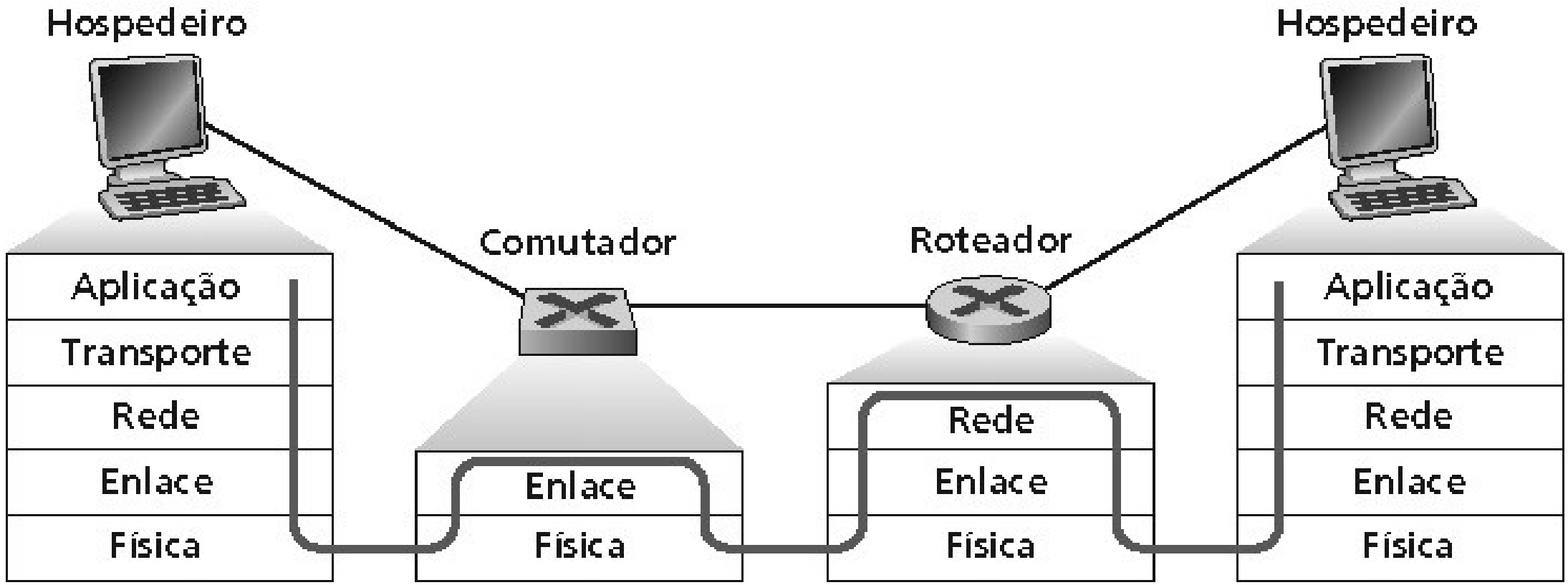
Ambos são dispositivos *store-and-forward*:

- Roteadores: dispositivos de camada de rede (examinam cabeçalhos da camada de rede);
- *Switches* são dispositivos da camada de enlace.

Roteadores mantêm tabelas de roteamento, implementam algoritmos de roteamento;

Switches mantêm tabelas de *switch*, implementam filtragem, algoritmos de aprendizagem

Switches versus Roteadores



Switches versus Roteadores versus Hubs

	hubs	roteadores	*switches*
isolação de tráfego	não	sim	sim
plug & play	sim	não	sim
roteamento ótimo	não	sim	não
cut through	sim	não	sim

Detecção e Correção de Erros

Detecção e Correção de Erros no nível de bits

- Detecção da corrupção de bits em um quadro da camada de enlace enviado de um nó para outro nó vizinho fisicamente ligado a ele.

Para que os dados enviados fiquem protegidos contra erros de bits, eles são aumentados com bits de detecção e de correção (*Error Detectionand- Corretion bits* – EDC).

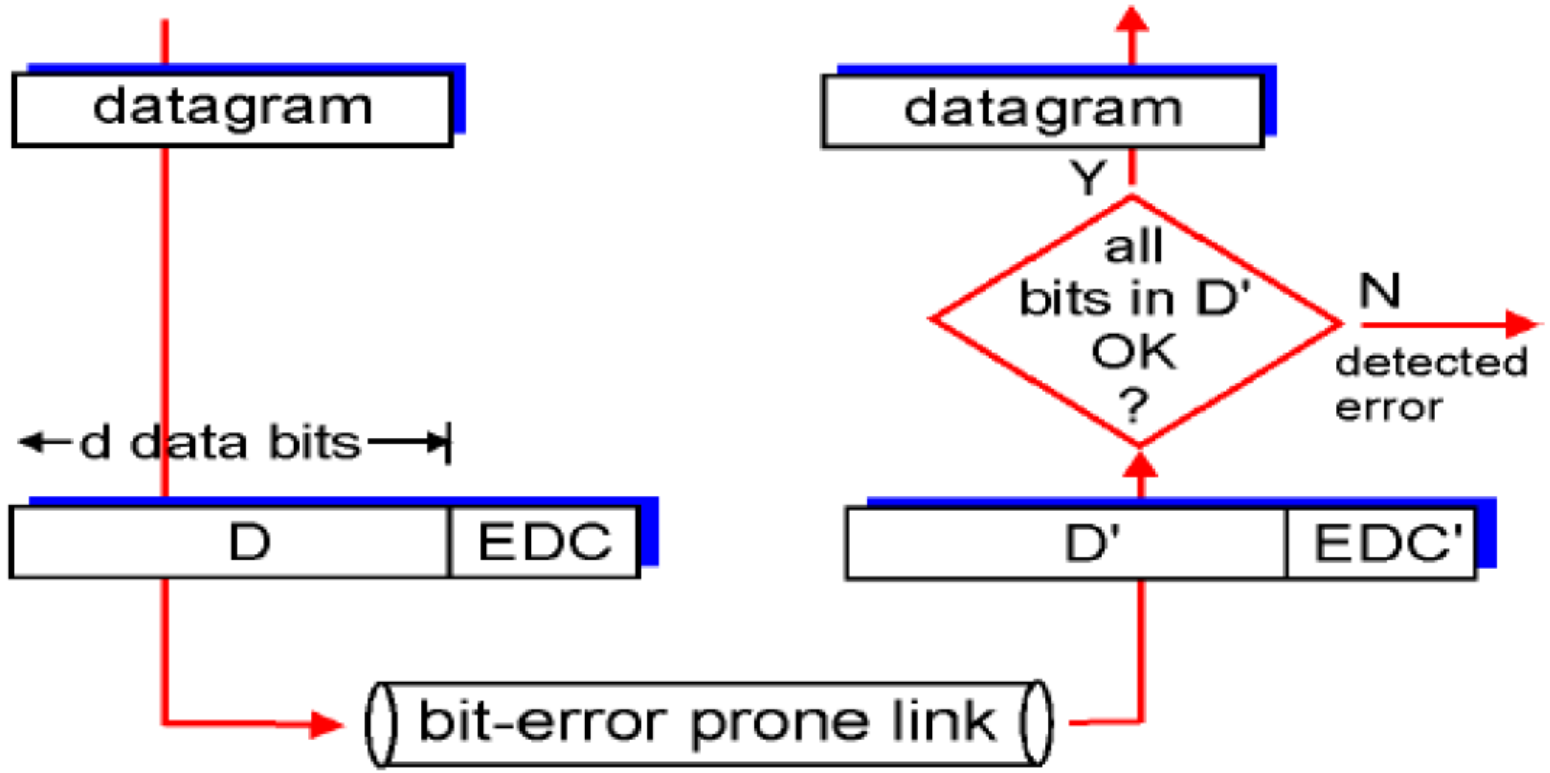
Além dos dados enviados, vários campos do cabeçalho são protegidos.

Mesmo com a utilização de bits de detecção de erros, ainda há a possibilidade de ocorrência de erros de bits não detectados.

Técnicas mais sofisticadas de detecção e correção de erros ficam sujeitas a uma sobrecarga maior.

EDC – *Error Detection and Correction bits* (Redundância)

D - Dados



Verificação de Paridade

Maneira mais simples de detectar erros é utilizar um único bit de paridade.

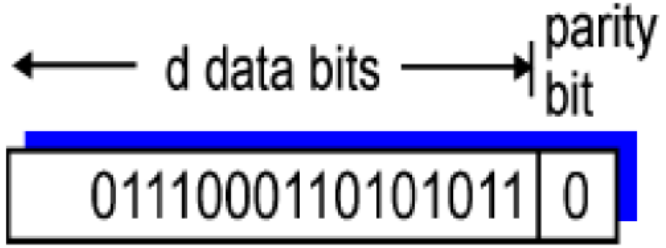
Paridade Par

- Acrescenta um bit para que o somatório dos 1's seja par.

Paridade Impar

- Acrescenta um bit para que o somatório dos 1's seja impar.

Não detecta um número par de erros na mesma sequência de bits.

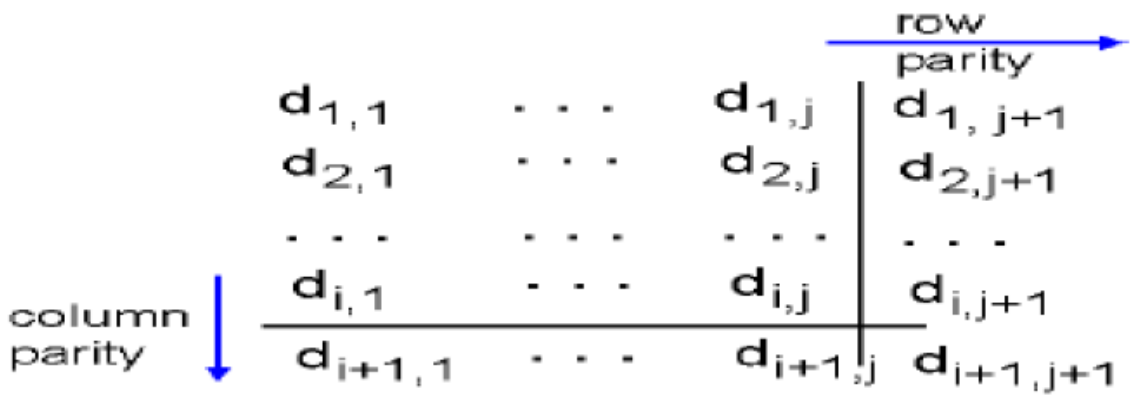


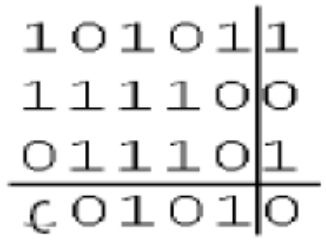
Como é comprovado que a maioria dos erros ocorrem em rajadas, é necessário um esquema de detecção de erros mais robusto.

Paridade Bidimensional, generalização bidimensional do esquema de paridade de bit único.

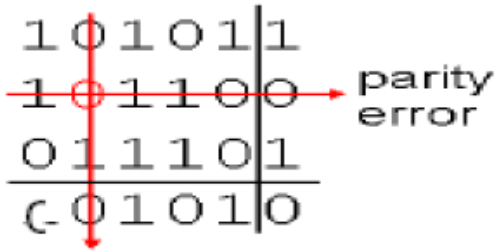
O receptor não somente pode detectar que ocorreu um erro de um bit único, como identificar o bit e corrigí-lo.

Paridade Bidimensional





no errors



correctable single bit error

A paridade bidimensional pode detectar qualquer combinação de dois erros em um pacote.

A capacidade do receptor para detectar e corrigir erros é conhecida como **correção de erros de repasse** (*Foward Error Correction* – FEC).

As técnicas FEC são importantes pois reduzemo número de retransmissões.

Soma de Verificação (*Check Sum*)

Nas técnicas de somas de verificação, os bits são tratados como uma sequência de números inteiros de k bits.

Um método simples é somar os inteiros de k bits e usar o total resultante como bits de correção de erros, a **soma de verificação da Internet** usa essa abordagem.

Bytes de dados são tratados como inteiros de 16 bits e somados.

O complemento de 1 dessa soma então forma a soma de verificação da internet, que é carregada no cabeçalho do segmento.

Soma de Verificação (*Check Sum*)

O receptor verifica a soma de verificação calculando os complementos de 1 da soma dos dados recebidos e verificando se o resultado contém somente bits 1.

Métodos de soma de verificação exigem relativamente pouca sobrecarga de pacote.

Oferecem proteção relativamente baixa contra erros.

É utilizada na camada de transporte devido a facilidade de implementação via software.

Verificação de Redundância Cíclica

Cyclic Redundancy Check – CRC.

Também conhecido como código polinomial

Considera a cadeia de bits como um polinômio cujos coeficientes são os valores 0 e 1.

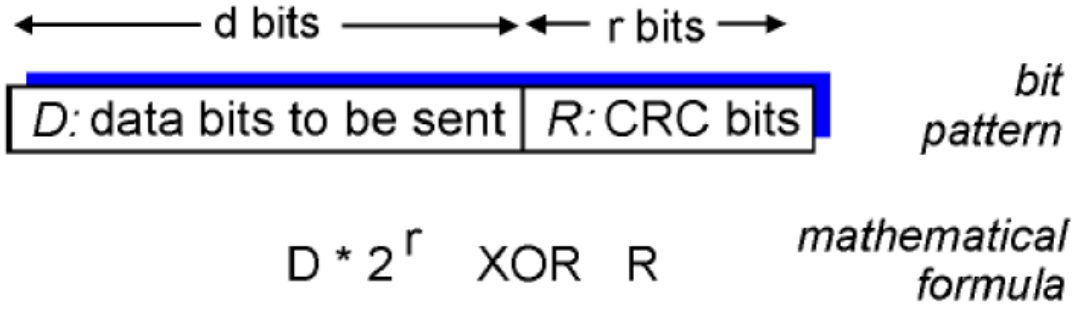
As operações na cadeia de bits interpretadas como aritmética polinomial.

Verificação de Redundância Cíclica

Enxerga os bits de dados , D, como um número binário.

Escolhe um gerador de r + 1 bits (G)

Encontrar os bits CRC, R, tal que:



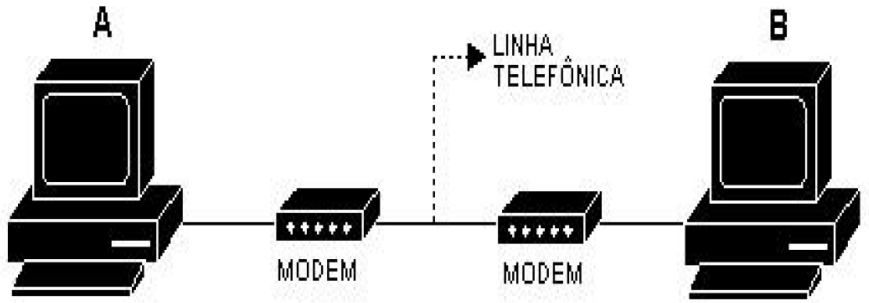
- <D,R> sejam divisíveis por G
- O receptor saiba que G divide <D,R>, resto diferente de 0 caracteriza um erro.
- Pode detectar erros de rajada menores que r + 1 bits

Enlace Ponto-a-Ponto

- Um emissor, um receptor, um enlace:
    - Sem controle de acesso ao meio;
    - Sem necessidade de uso de endereços MAC;
    - X.25, dialup link, ISDN.
- Protocolos PPP populares:
    - PPP (*Ponit-to-Point Protocol*)
    - HDLC (*High-level Data Link Control*)

Protocolo Ponto-a-Ponto (PPP)

Protocolo comumente escolhido para o enlace discado entre hospedeiros residenciais e ISP´s.



Exigências Originais da IETF

Enquadramento do Pacote

- O remetente deve ser capaz de encapsular um pacote em um quadro PPP
- Transparência
- O PPP não deve impor nenhuma restrição sobre os dados que aparecem no pacote da camada de rede
- Múltiplos protocolos da camada de rede
- Deve estar habilitado a suportar múltiplos protocolos da camada de rede e multiplexá-los
- Múltiplos tipos de enlaces

Exigências Originais da IETF

Detecção de erros

- Vida da Conexão
- Detectar uma falha no nível de enlace e informar o erro à camada de rede
- Negociação do endereço de camada de rede
- Fornecer um mecanismo para determinação dos endereços dos protocolos da camada de rede
- Simplicidade
- A grande característica, segundo o RFC 1547, é a simplicidade, regida por mais de 50 RFC´s.

Não é obrigação do PPP

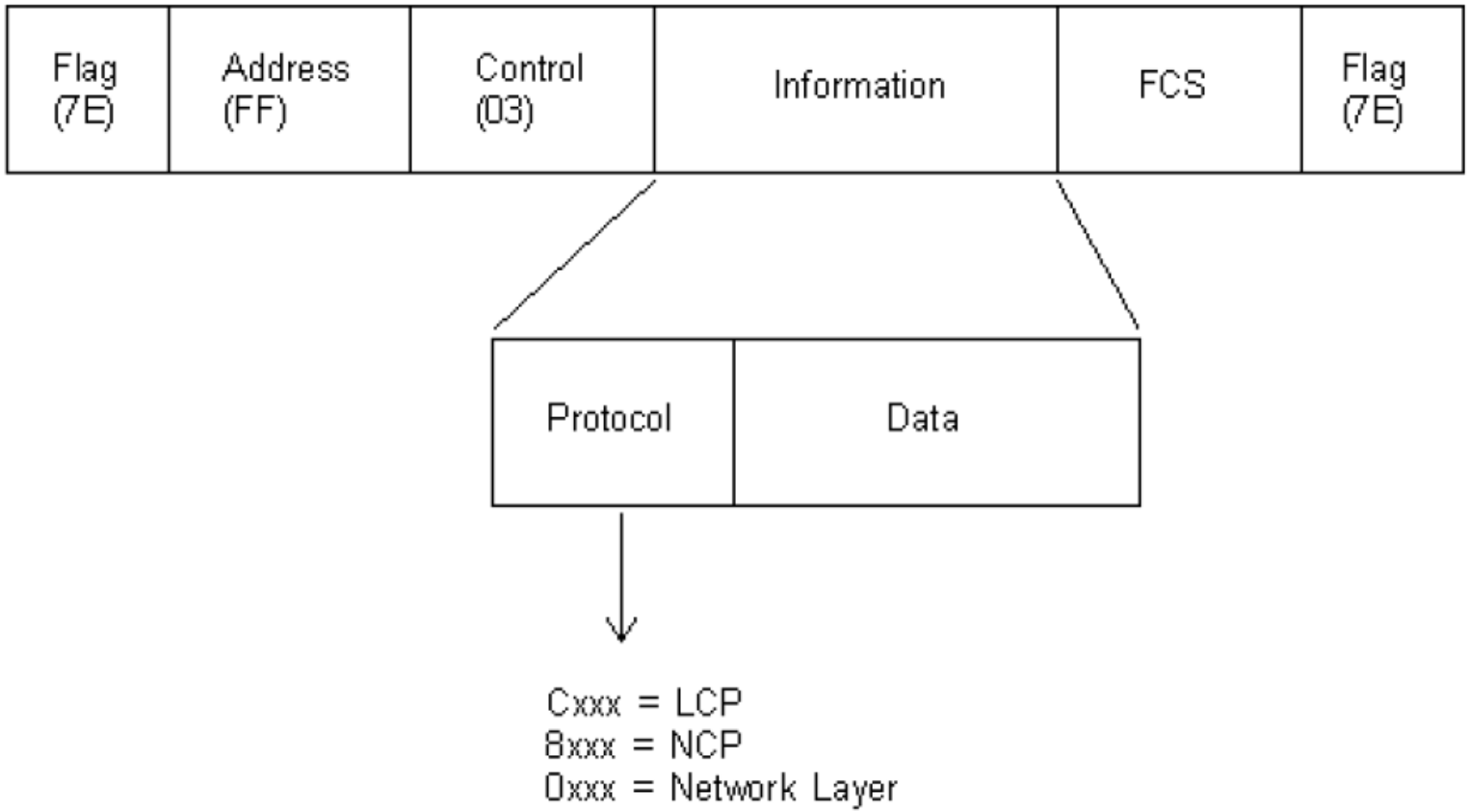
Correção de erros

- Controle de fluxo
- Espera-se que o PPP possa enviar e receber dados na velocidade máxima que o enlace pode oferecer.
- Sequenciamento
- Enlaces multiponto
- Opera apenas com um único remetente e um único receptor.

Enquadramento de Dados PPP

- Campo de flag
  - Todo quadro começa e termina com um campo de flag
- Campo de endereço
  - O único valor do campo é 11111111
- Campo de controle
  - Valor do campo 00000011. Pode ser utilizado para implementações futuras
- Protocolo
  - Utilizado para multiplexar os dados para a camada de rede
- Informação
  - Contém o pacote encapsulado. O tamanho máximo padrão é de 1.500 bytes.
- Soma de Verificação
  - Utilizado para detecção de erros em um pacote transmitido. Usa um código de redundância cíclica padrão HDLC de 2 ou 4 bytes

Quadro PPP


Flag
(7E)
Address
(FF)
Control
(03)
Information
FCS
Flag
(7E)
Protocol
Data
Cxxx = LCP
8xxx = NCP
0xxx = Network Layer

Protocolo de Controle de Enlace - LCP

- *Link Control Protocol* – LCP

- Responsável pela abertura, manutenção, indicação de erro e fechamento de um enlace PPP.

- Antes do início da troca de dados os dois pares devem primeiramente rodar uma quantidade considerável de trabalho para configurar o enlace.

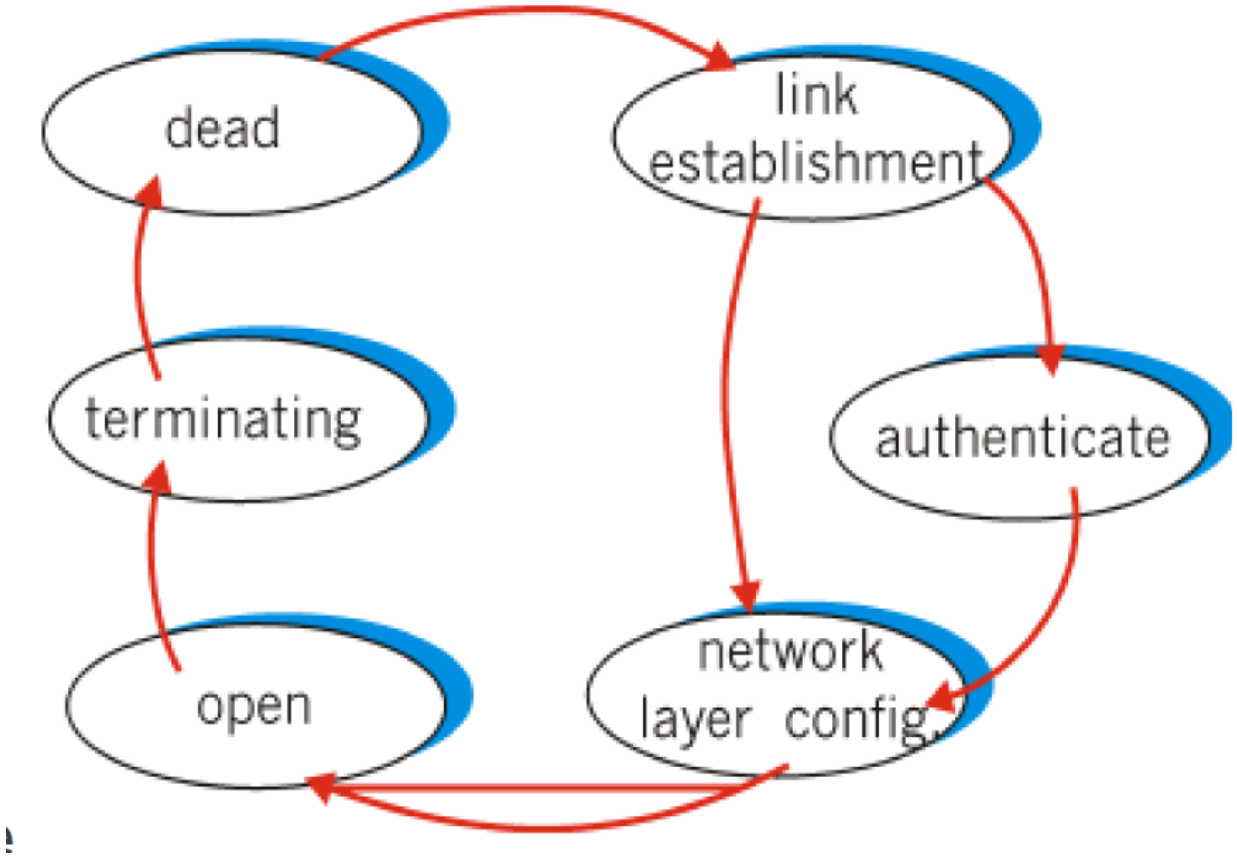
Todo enlace PPP começa e termina em estado inativo

- Detecta camada física entra em modo de estabelecimento de enlace

Protocolo de Controle de Enlace - LCP

- É enviado um quadro LCP ***configure-request***, solicitando uma Configuração. Pode receber ***configure-ack***, ***configure-nak*** ou ***configure-reject***

- No quadro LCP pode estar informando entre outras coisas o descarte dos campos de endereço e de controle, economizando assim 2 bytes em cada quadro PPP



Protocolos de Controle de Rede

Network Control Protocol – NCP

- Após o estabelecimento do enlace, negociadas as opções e realizada a autenticação, entra em ação o NCP.
- Troca de pacotes específicos de controle da camada de rede para cada protocolo de rede.
- Se o IP estiver rodando, será utilizado protocolo de controle IP (RFC 1332) para configurar os módulos do procolo IP em cada lado do enlace.

PPPoE e PPPoA

- PPPoA, PPP *over* ATM
    - Protocolo a ser utilizado sobre redes ATM
- PPPoE, PPP *over Ethernet*
    - Protocolo a ser utilizado sobre redes *Ethernet*

Camada Física

Camada física da ISO

Fornece as características mecânicas, elétricas, funcionais e de procedimento para ativar, manter e desativar conexões físicas para a transmissão de bits entre entidades de nível de ligação possivelmente através de sistemas intermediários.

Uma unidade de dados do nível físico consiste de uma sequencia de bits, em uma transmissão serial, ou “n” bits conjuntos em uma transmissão paralela. Um exemplo de uma comunicação serial pode ser o acesso, via Telnet, para um terminal remoto, um exemplo de comunicação paralela é a comunicação entre uma impressora e uma CPU (computador).

Tarefas Básicas da camada de física

As tarefas de planejamento desta camada devem garantir que quando um lado envia um bit 1, este seja recebido do outro lado como um bit 1, não como um bit 0. Algumas perguntas típicas são: quantos volts deveriam ser usados para se representar um 1 e quantos para um 0; quantos microssegundos um bit deve durar; se a transmissão deve proceder em ambas as direções; como a conexão inicial é estabelecida entre as partes e como ela é desfeita quando os dois lados tiverem terminado; quantos pinos o conector de rede deverá ter e qual a funcionalidade de cada um desses pinos.

Tarefas Básicas da camada física

Mecânicas: propriedades físicas da interface com o meio físico de transmissão, incluindo, por exemplo, o tipo de conector utilizado.

Elétricas: se relacionam com a representação de um bit em termos de, por exemplo, nível de tensão utilizado e taxa de transmissão de bits.

Funcionais: definem as funções a serem implementadas por esta interface;

Procedurais: especificam a sequência de eventos trocados durante a transmissão de uma série de bits através do meio de transmissão

REDES SEM FIO

QUADRO IEEE 802.11

Tem semelhanças com o quadro *ethernet*, com a adição de vários campos específicos para utilização nos enlaces sem fio.

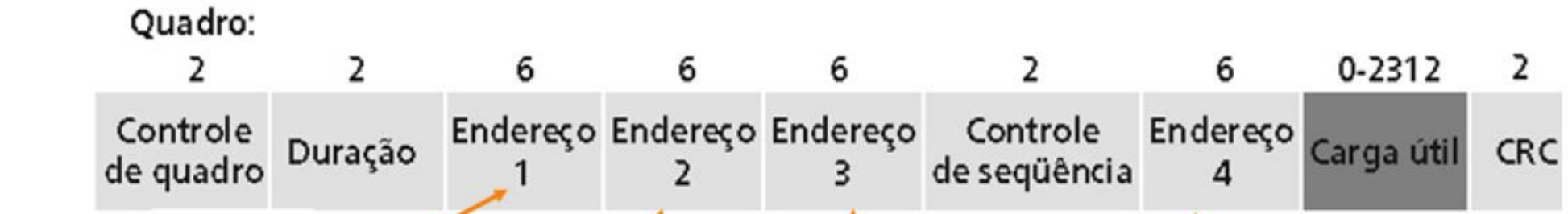
- No coração do quadro está a carga útil, que consiste, tipicamente, em um datagrama IP ou em um pacote ARP e apesar de poder transportar 2.312 bytes, normalmente o campo é menor que 1.500 bytes.

- Possui quatro campos de endereço de 6 bytes (MAC).

- 3 são utilizados para fim de interconexão em rede.

- O quarto endereço é utilizado em redes ad hoc.

QUADRO IEEE 802.11



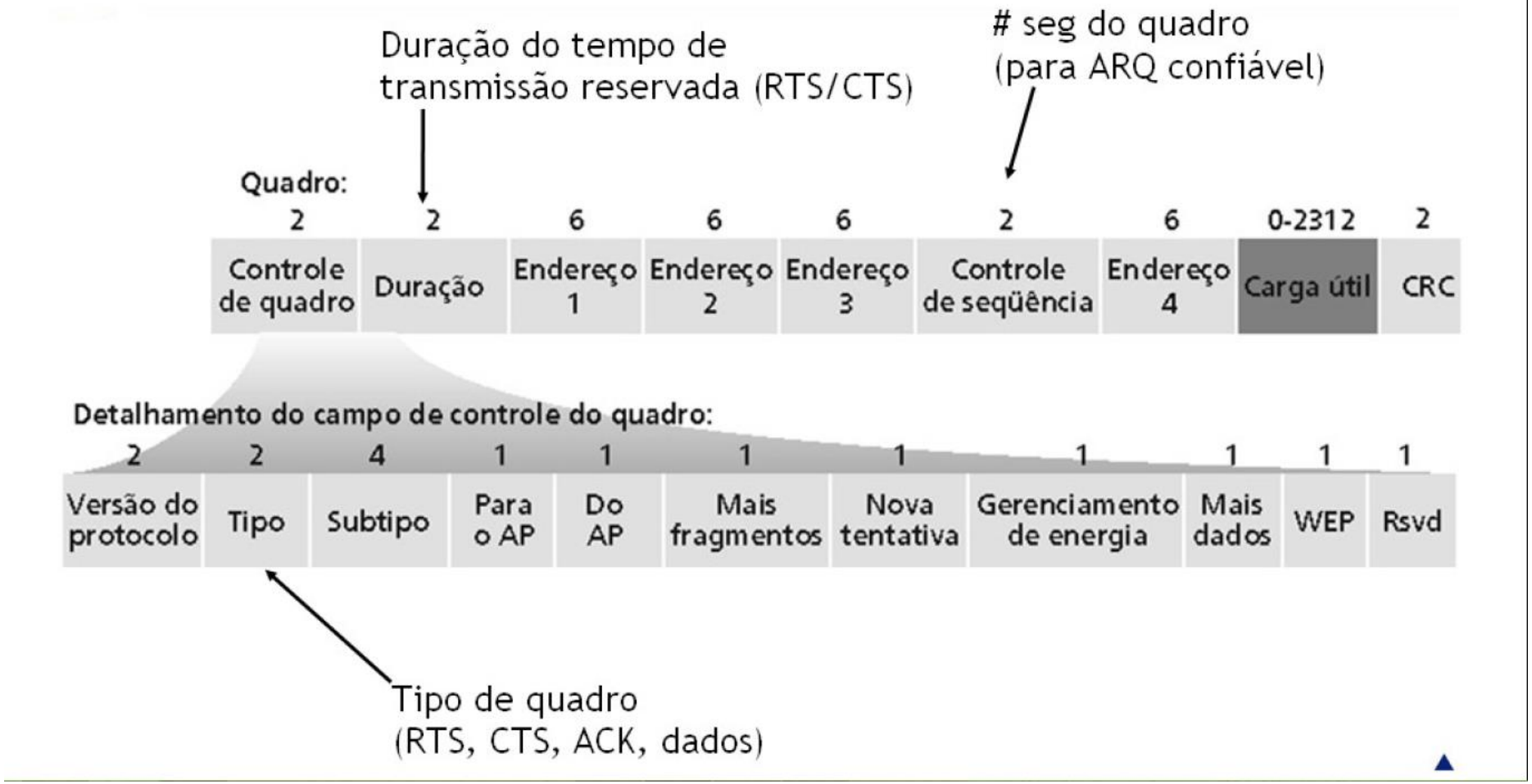
Endereço 1: endereço MAC do Hospedeiro sem fio ou AP que deve receber o quadro

Endereço 2: endereço MAC do hospedeiro sem fio ou AP transmitindo este quadro

Endereço 3: endereço MAC da interface do roteador à qual o AP é ligado

Endereço 4: usado apenas no modo ad hoc

QUADRO IEEE 802.11



EMAIL:

jesse.filho@bonfim.ifbaiano.edu.br

MATERIAL

http://softwarelivre.org/jessenery/jesse-nery-filho