

# Capítulo 1: Introdução

## Objetivos do capítulo: Visão geral:

- mostrar a “atmosfera” e a terminologia
- mais detalhes *mais adiante* no curso
- método:
  - usar Internet como exemplo
- o que é a Internet?
- o que é um protocolo?
- borda da rede; hospedeiros, rede de acesso, meio físico
- núcleo da rede: pacote/comutação de circuitos, estrutura da Internet
- desempenho: perda, atraso, vazão
- segurança
- camadas de protocolo, modelos de serviço

# Capítulo 1: Roteiro

## 1.1 O que é a Internet?

## 1.2 Borda da rede

- sistemas finais, redes de acesso, enlaces

## 1.3 Núcleo da rede

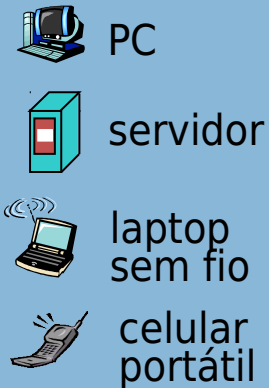
- comutação de circuitos, comutação de pacotes, estrutura da rede

## 1.4 Atraso, perda e vazão nas redes comutadas por pacotes

## 1.5 Camadas de protocolo, modelos de serviço

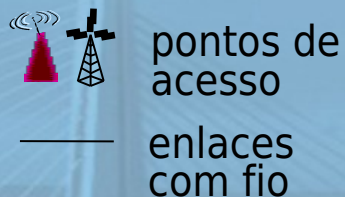
## 1.6 Redes sob ataque: segurança

# O que é a Internet: uma visão de hardware



- milhões de dispositivos de computação conectados:  
*hospedeiros = sistemas finais*
  - rodando *aplicações de rede*

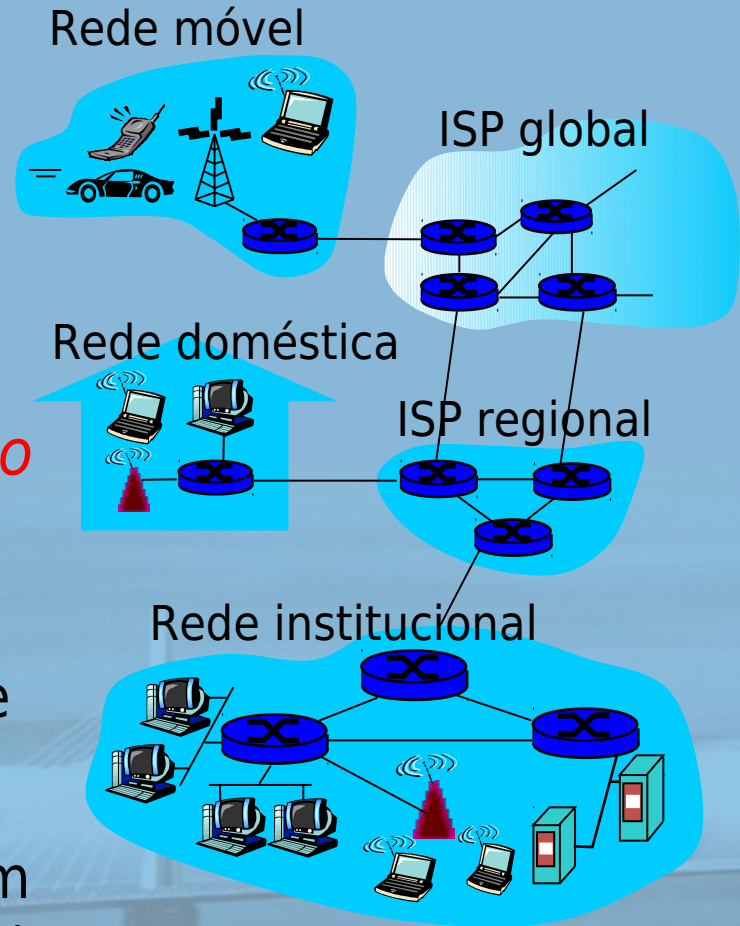
## □ *enlaces de comunicação*



- ❖ fibra, cobre, rádio, satélite
- ❖ ISP = Internet Service Provider

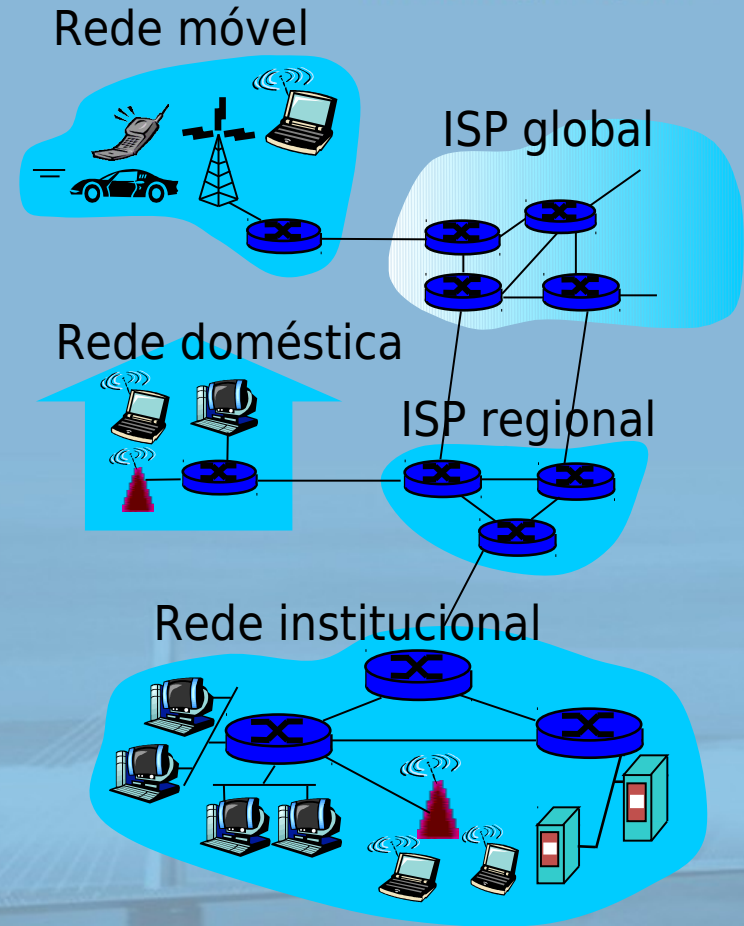


□ *roteadores*: encaminham pacotes (pedaços de dados)



# O que é a Internet: uma visão de arquitetura

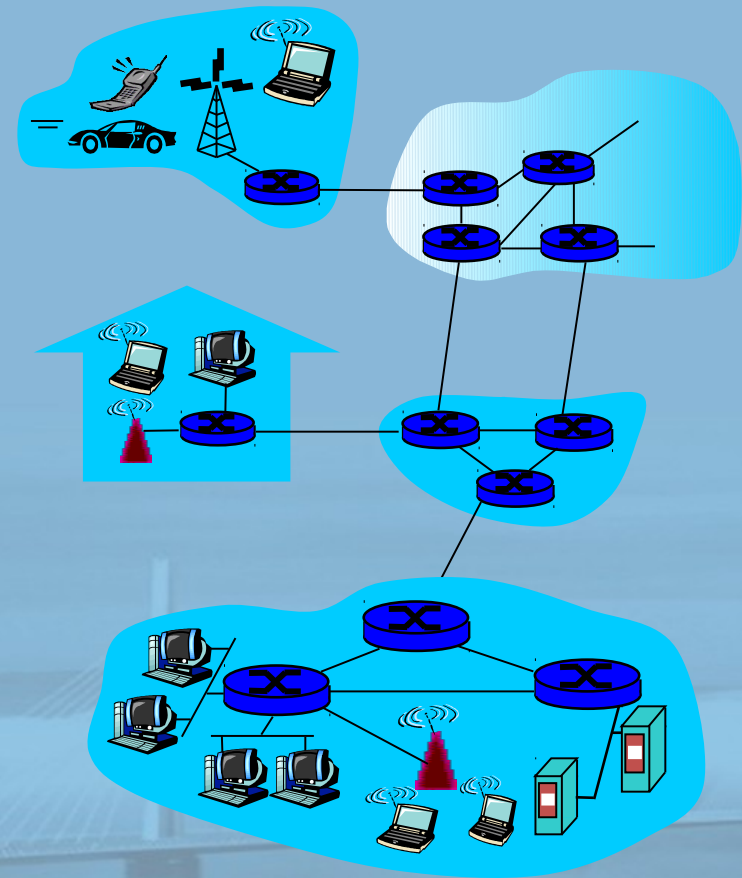
- **protocolos** controle de envio e recepção de msgs
  - p. e., TCP, IP, HTTP, Skype, Ethernet
- **Internet: “rede de redes”**
  - vagamente hierárquica
  - Internet pública *versus* intranet privada
- **padrões da Internet**
  - RFC: Request For Comments
  - IETF: Internet Engineering Task Force





# O que é a Internet: uma visão de serviço

- **infraestrutura de comunicação** possibilita aplicações distribuídas:
  - Web, VoIP, e-mail, jogos, e-commerce, compartilhamento de arquivos
- **serviços de comunicação** fornecidos às aplicações:
  - entrega de dados confiável da origem ao destino
  - entrega de dados pelo “melhor esforço” (não confiável)



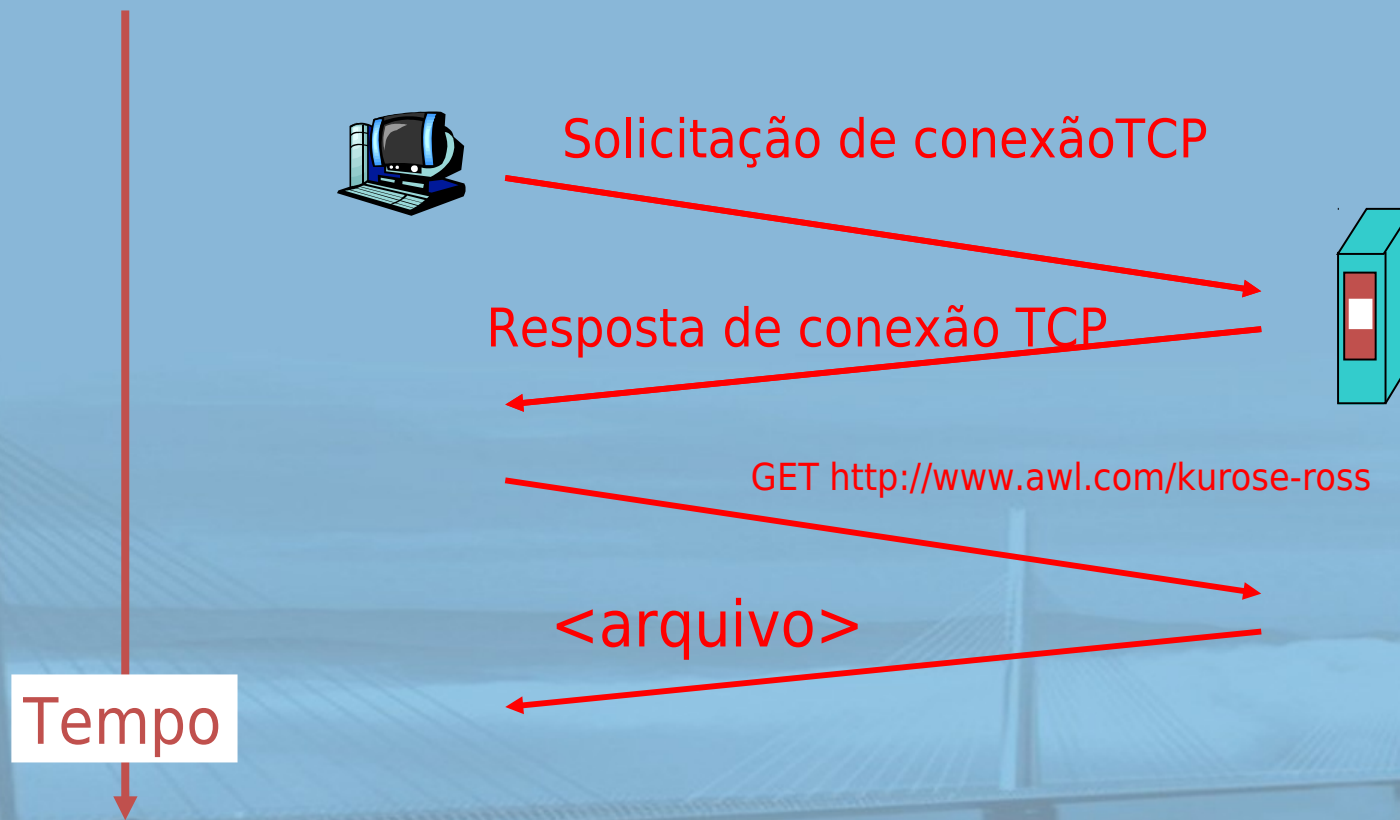
# O que é um protocolo?

## protocolos de rede:

- toda atividade de comunicação na Internet é controlada por protocolos
- Mensagem específicas são enviadas
- Ações específicas são tomadas quando mensagem são recebidas, ou outros eventos

*Protocolos definem formato, ordem de mensagens enviadas e recebidas entre entidades de rede e ações tomadas sobre transmissão e recepção de mensagens.*

um protocolo de rede de computadores:



# Capítulo 1: Roteiro

1.1 O que é a Internet?

1.2 Borda da rede

- sistemas finais, redes de acesso, enlaces

1.3 Núcleo da rede

- comutação de circuitos, comutação de pacotes, estrutura da rede

1.4 Atraso, perda e vazão nas redes comutadas por pacotes

1.5 Camadas de protocolo, modelos de serviço

1.6 Redes sob ataque: segurança



# Visão mais de perto da estrutura de rede:

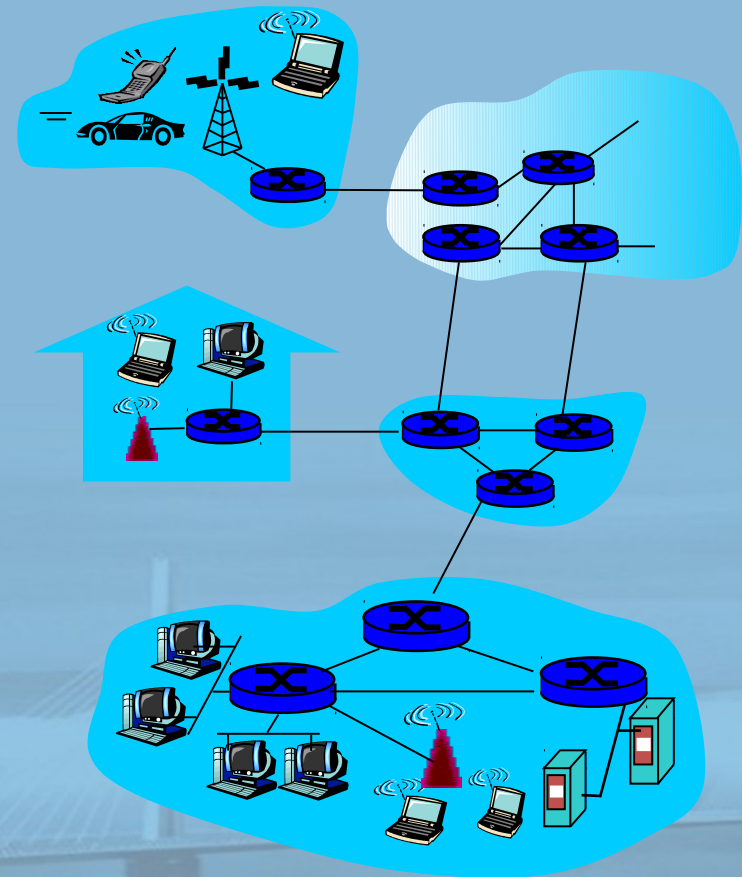
- **borda da rede:**

aplicações e  
hospedeiros

- **redes de acesso, meios físicos:** enlaces de comunicação com e sem fio

- **núcleo da rede:**

- ❖ roteadores interconectados
- ❖ rede de redes



## A borda da rede:

- **sistemas finais (hospedeiros):**

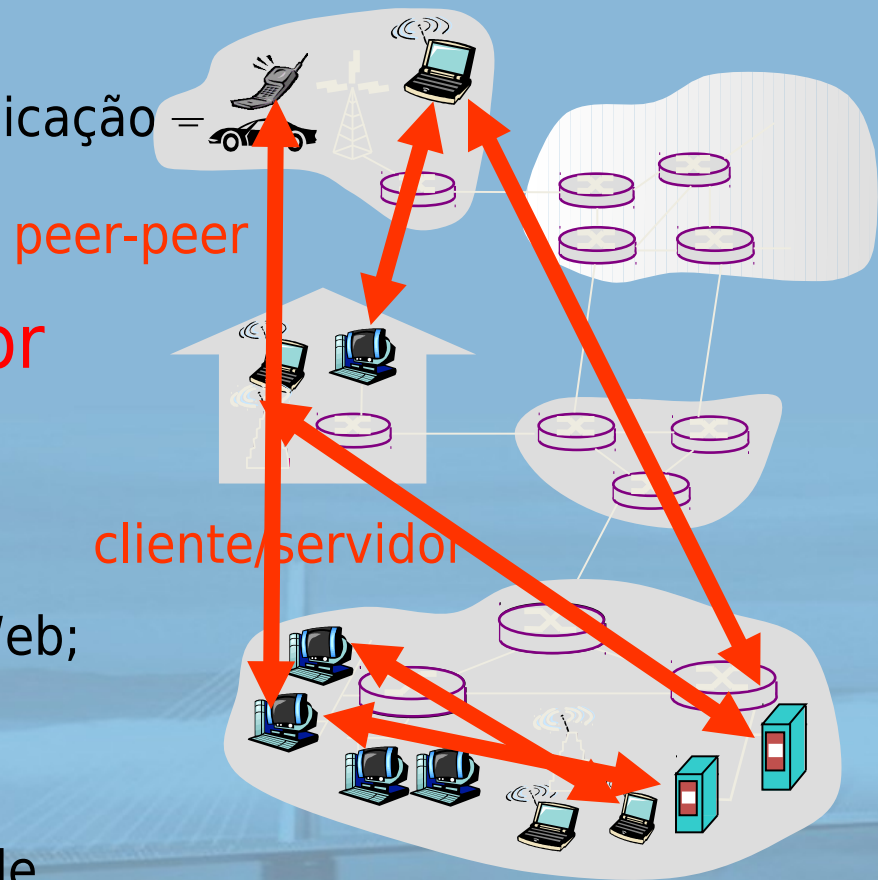
- executar programas de aplicação =
- p. e. Web, e-mail
- na “borda da rede”

- **modelo cliente/servidor**

- ❖ hospedeiro cliente solicita, recebe serviço de servidor sempre ativo
- ❖ p. e. navegador/servidor Web; cliente/servidor de e-mail

- **modelo peer-to-peer:**

- ❖ uso mínimo (ou nenhum) de servidores dedicados
- ❖ p. e. Skype, BitTorrent



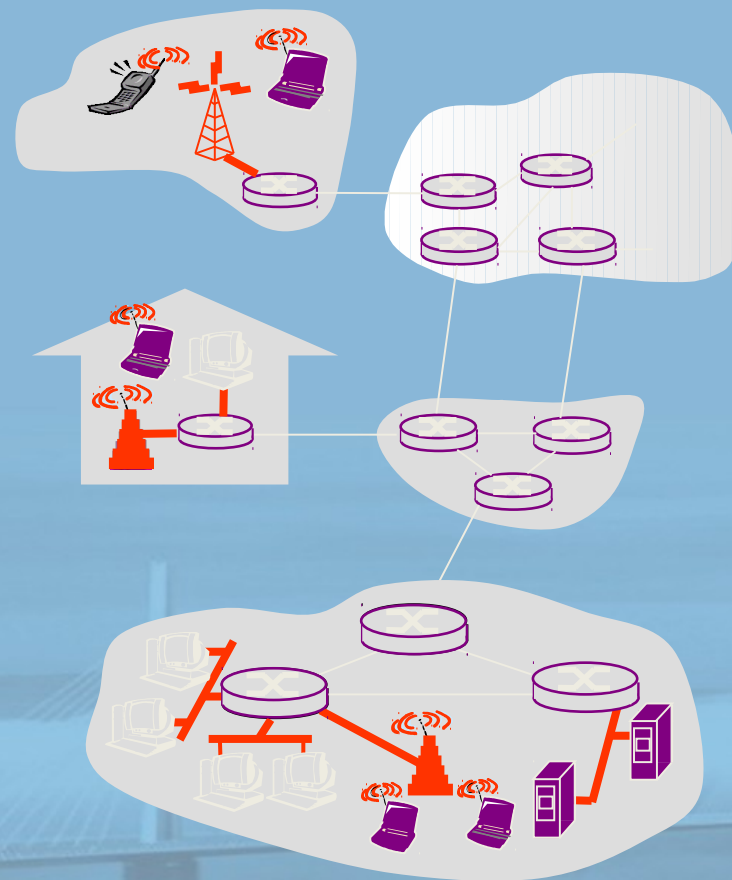
# Redes de acesso e meios físicos

*P: Como conectar sistemas finais ao roteador da borda?*

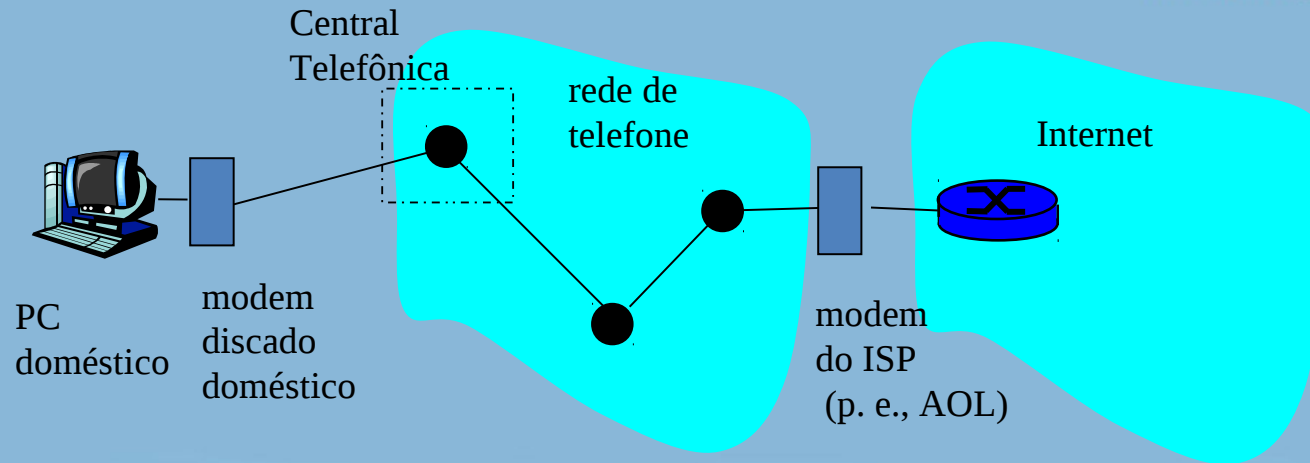
- redes de acesso residencial
- redes de acesso institucional (escola, empresa)
- redes de acesso móvel

*Propriedades:*

- largura de banda (bits por segundo) da rede de acesso?
- compartilhado ou dedicado?

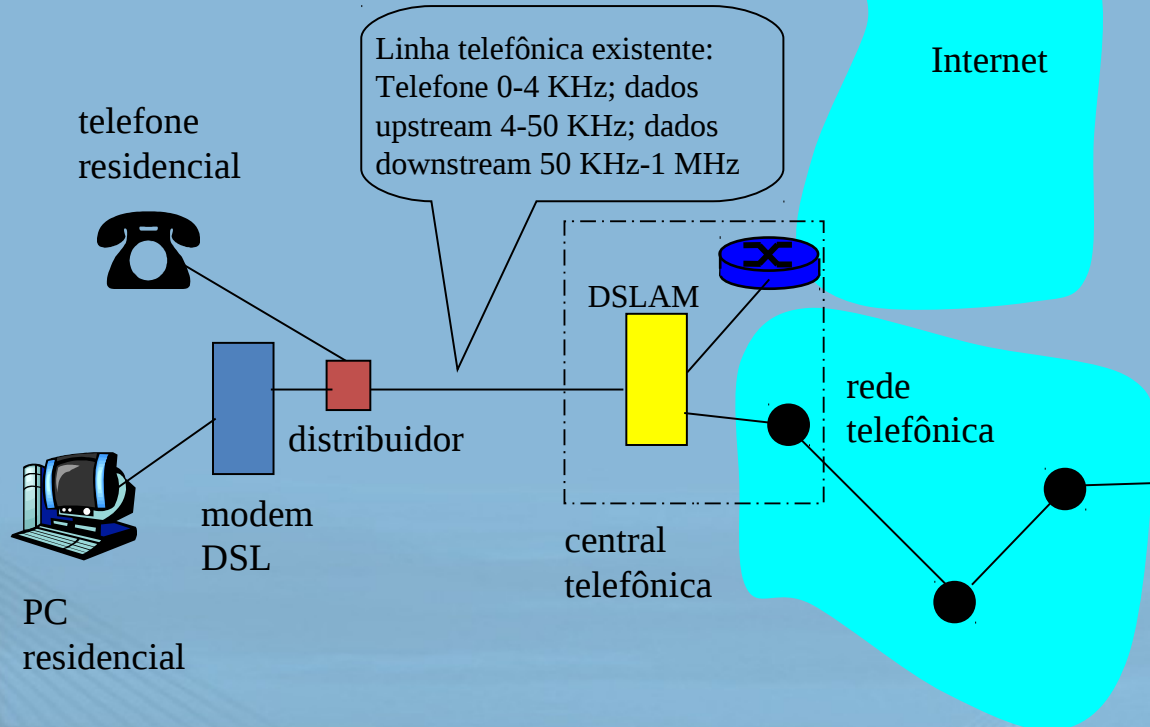


# Modem discado



- ❖ usa infraestrutura de telefonia existente
- ❖ casa conectada à **central de telefonia**
- ❖ até 56 kbps de acesso direto ao roteador (geralmente menos)
- ❖ não pode navegar e telefonar ao mesmo tempo
- ❖ não está **“sempre ligado”**

# Digital Subscriber Line (DSL)



- ❖ também usa infraestrutura de telefone existente
- ❖ até 1 Mbps upstream, até 8 Mbps downstream
- ❖ pode-se navegar e telefonar ao mesmo tempo
- ❖ está sempre ligado

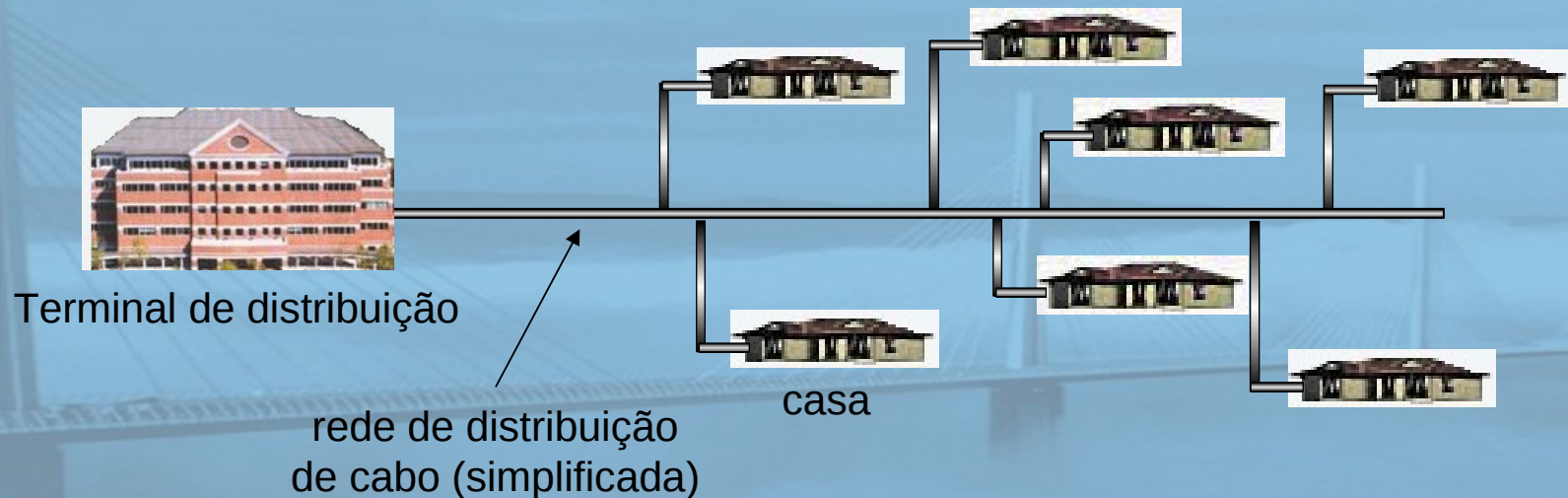


# Acesso residencial: modems a cabo

- não usa infraestrutura de telefone
  - usa infraestrutura de TV a cabo
- **HFC: Hybrid Fiber Coax**
  - assimétrico: até 30 Mbps downstream, 2 Mbps upstream
- **rede** de cabo e fibra conecta casas ao roteador ISP
  - casas **compartilham acesso** ao roteador
  - diferente de DSL, que tem **acesso dedicado**

# Arquitetura de rede a cabo: visão geral

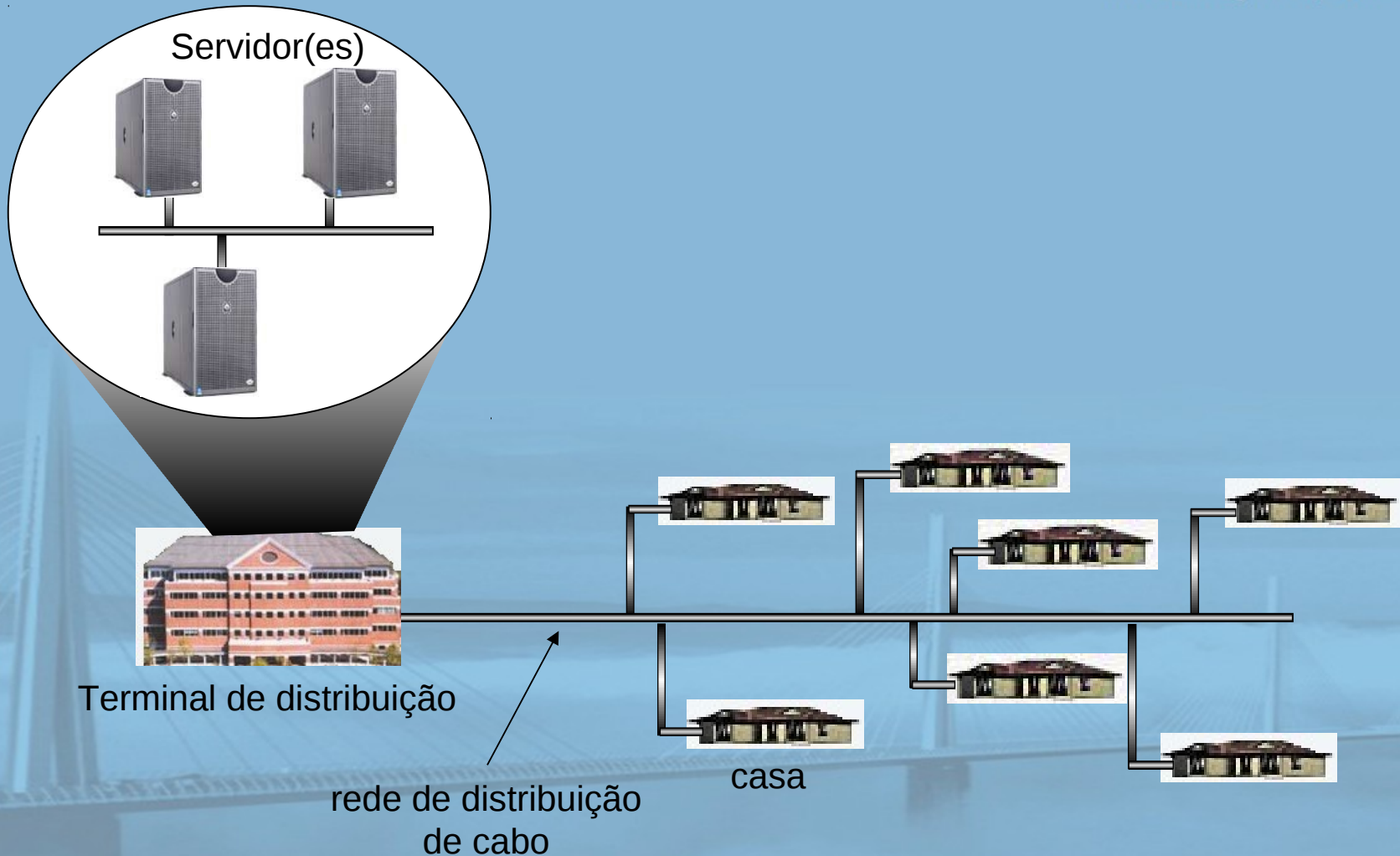
geralmente, 500 a 5.000 casas



# REDES DE COMPUTADORES E A INTERNET

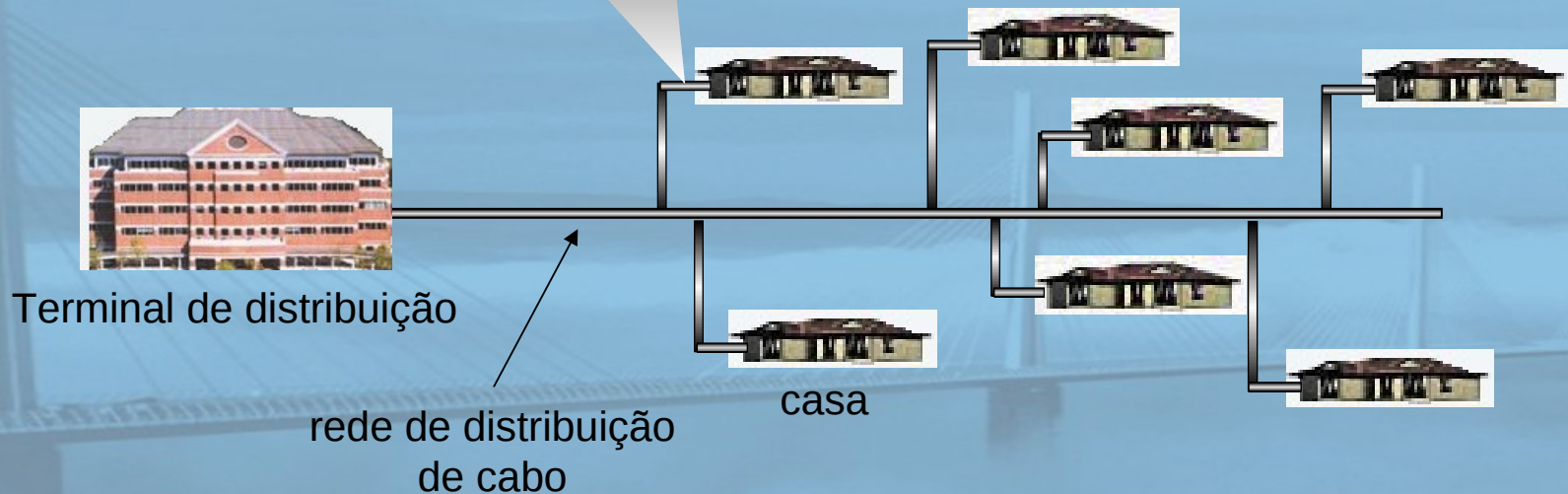
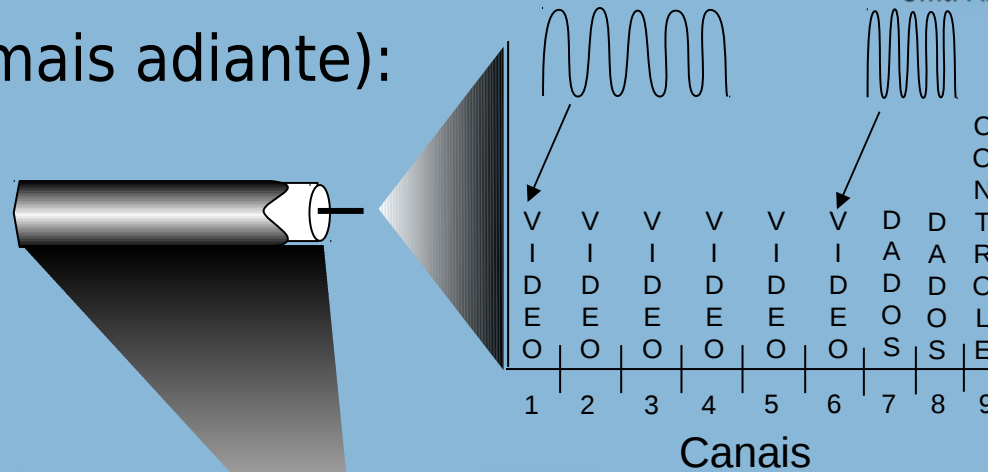
5ª edição

*Uma Abordagem Top-Down*

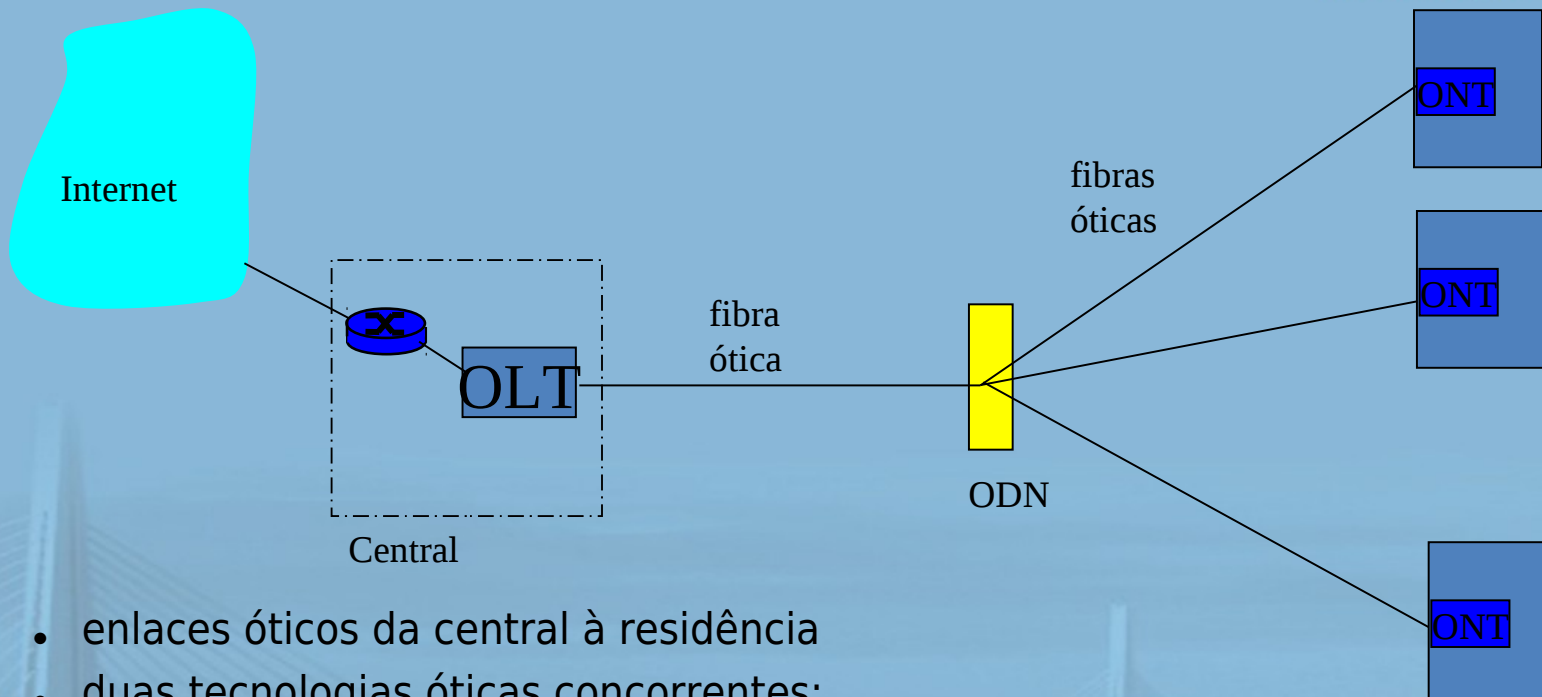


FDM (mais adiante):

*Uma Abordagem Top-Down*



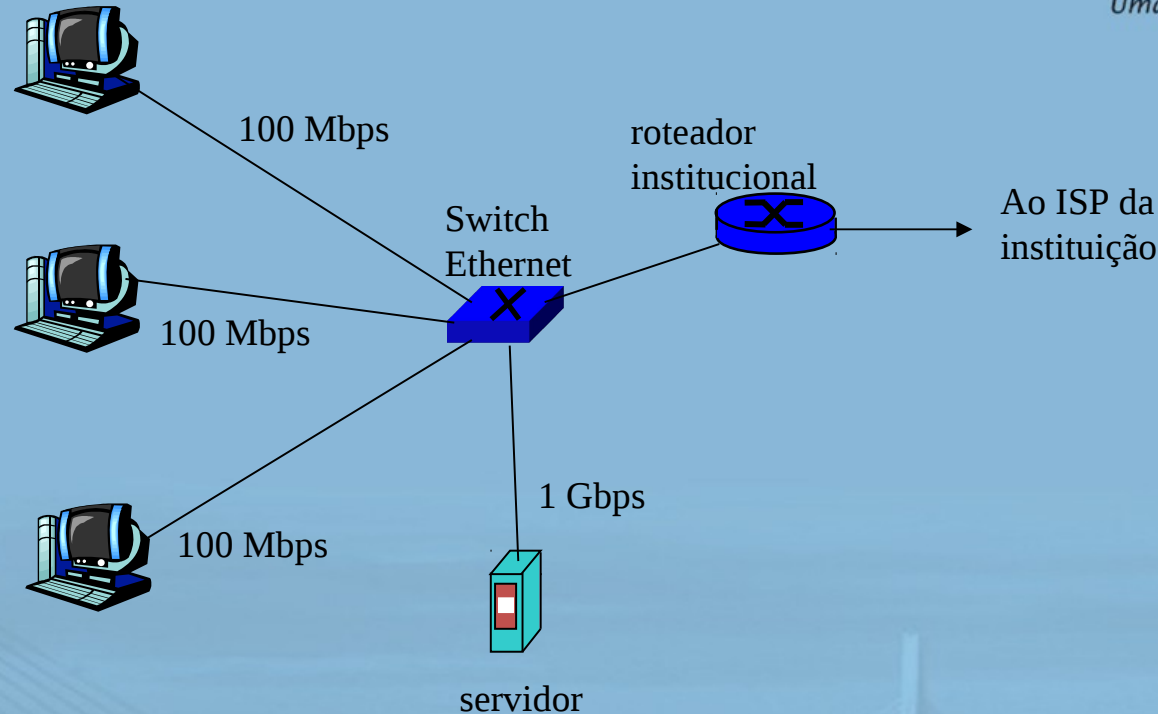
# Fibra nas residências



- enlaces óticos da central à residência
- duas tecnologias óticas concorrentes:
  - Passive Optical Network (PON)
  - Active Optical Network (PAN)
- Nós: ONT (Optical Network Terminal), ODN (Optical Distribution Network) e OLT (Optical Line Terminal)
- velocidades de Internet muito mais altas; fibra também transporta serviços de TV e telefone



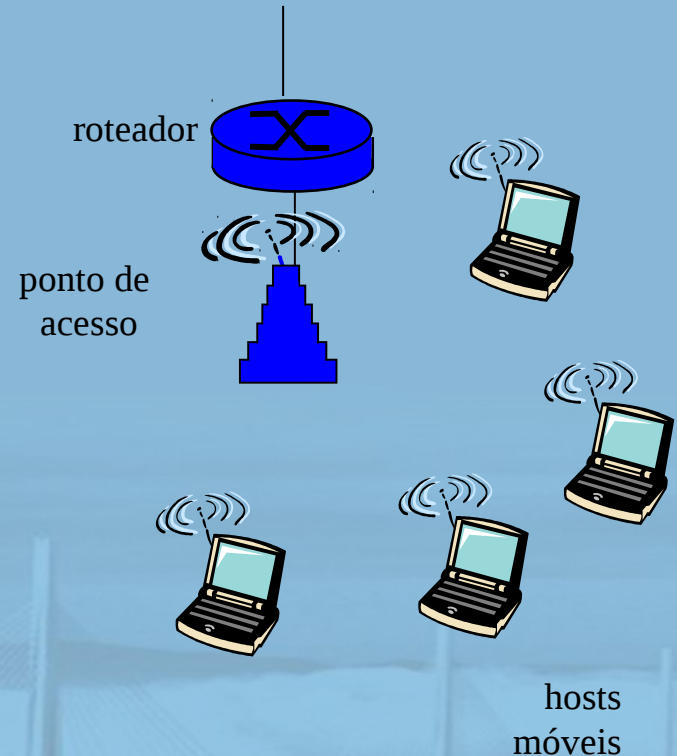
# Acesso à Internet por Ethernet



- normalmente usado em empresas, universidade etc.
- ❑ Ethernet a 10 Mbs, 100 Mbps, 1 Gbps, 10 Gbps
- ❑ os sistemas finais normalmente se conectam ao comutador Ethernet

# Redes de acesso sem fio

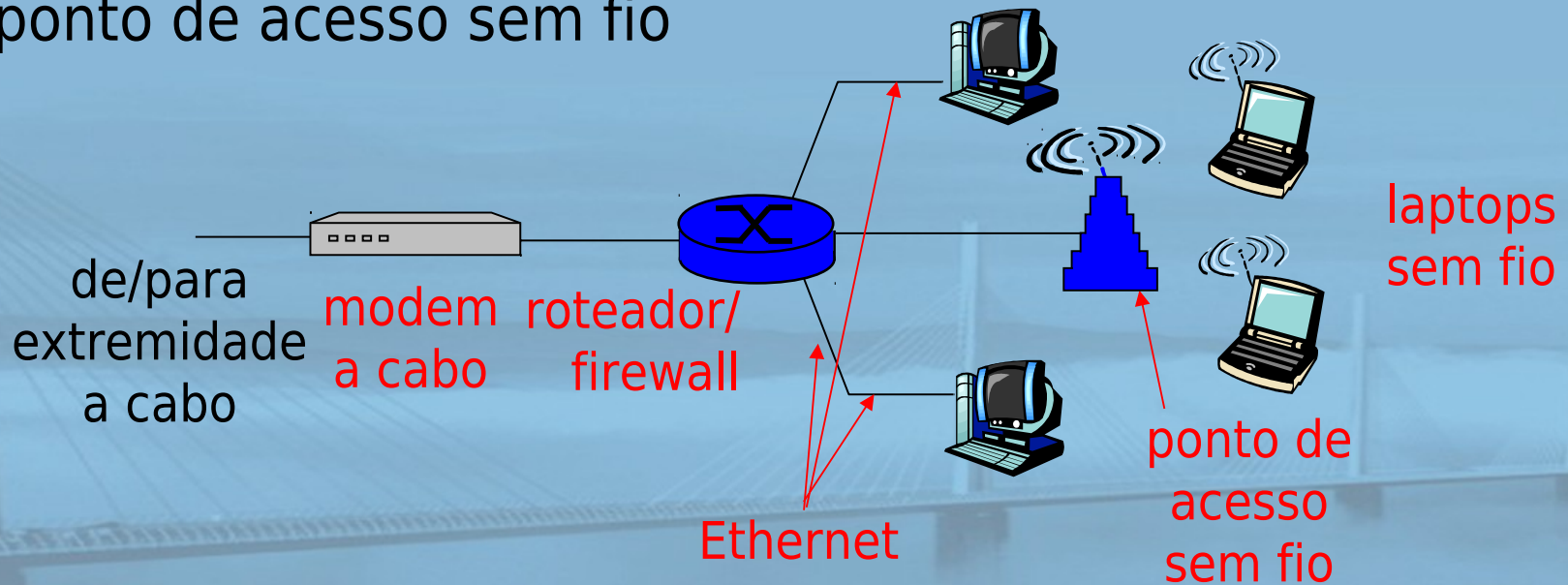
- rede de acesso *sem fio* compartilhado conecta sistema final ao roteador
  - via um ponto de acesso (access point)
- LANs sem fio:
  - 802.11b/g (WiFi): 11 ou 54 Mbps
- acesso sem fio de área mais remota
  - fornecido pelo operador de telecomunicação
  - por sistema celular
  - 3G



# Redes residenciais

## componentes típicos da rede residencial:

- modem DSL ou a cabo
- roteador/firewall/nat
- Ethernet
- ponto de acesso sem fio



# Meios físicos

- **bit:** propaga entre pares de transmissor/receptor
- **enlace físico:** o que fica entre transmissor e receptor
- **meio guiado:**
  - sinais se propagam em meio sólido: cobre, fibra, coaxial
- **meio não guiado:**
  - sinais se propagam livremente, p. e., rádio

## Par Trançado (TP)

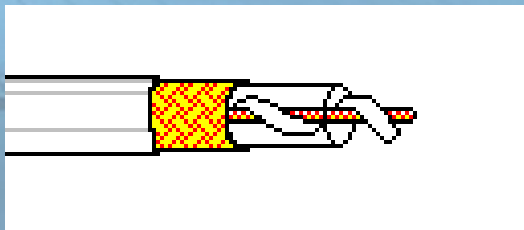
- dois fios de cobre isolados
  - categoria 3: fios de telefone tradicionais, Ethernet a 10 Mbps
  - categoria 5: Ethernet a 100 Mbps



# Meio físico: cabo coaxial, fibra

## cabo coaxial:

- dois condutores de cobre concêntricos
- bidirecional
- banda base:
  - único canal no cabo
  - Ethernet legado
- banda larga:
  - múltiplos canais no cabo
  - HFC



## cabo de fibra ótica:

- ❑ fibra de vidro conduzindo pulsos de luz; cada pulso um bit
- ❑ operação em alta velocidade:
  - ❖ transmissão em alta velocidade ponto a ponto (p. e., 10-100 Gps)
- ❑ baixa taxa de erro: repetidores bastante espaçados; imune a ruído eletromagnético





# Meio físico: rádio

- sinal transportado no espectro eletromagnético
- nenhum “fio” físico
- bidirecional
- efeitos no ambiente de propagação:
  - reflexão
  - obstrução por objetos
  - interferência

## Tipos de Conexão:

- ❑ **micro-ondas terrestre**
  - ❖ p. e. até canais de 45 Mbps
- ❑ **LAN** (p. e., Wifi)
  - ❖ 11 Mbps, 54 Mbps
- ❑ **área ampla** (p. e., celular)
  - ❖ celular 3G: ~ 1 Mbps
- ❑ **satélite**
  - ❖ canal de Kbps a 45Mbps (ou múltiplos canais menores)
  - ❖ atraso fim a fim de 270 msec
  - ❖ geoestacionário *versus* baixa altitude

# Capítulo 1: Roteiro

1.1 O que é a Internet?

1.2 Borda da rede

- ❑ sistemas finais, redes de acesso, enlaces

1.3 Núcleo da rede

- ❑ comutação de circuitos, comutação de pacotes, estrutura da rede

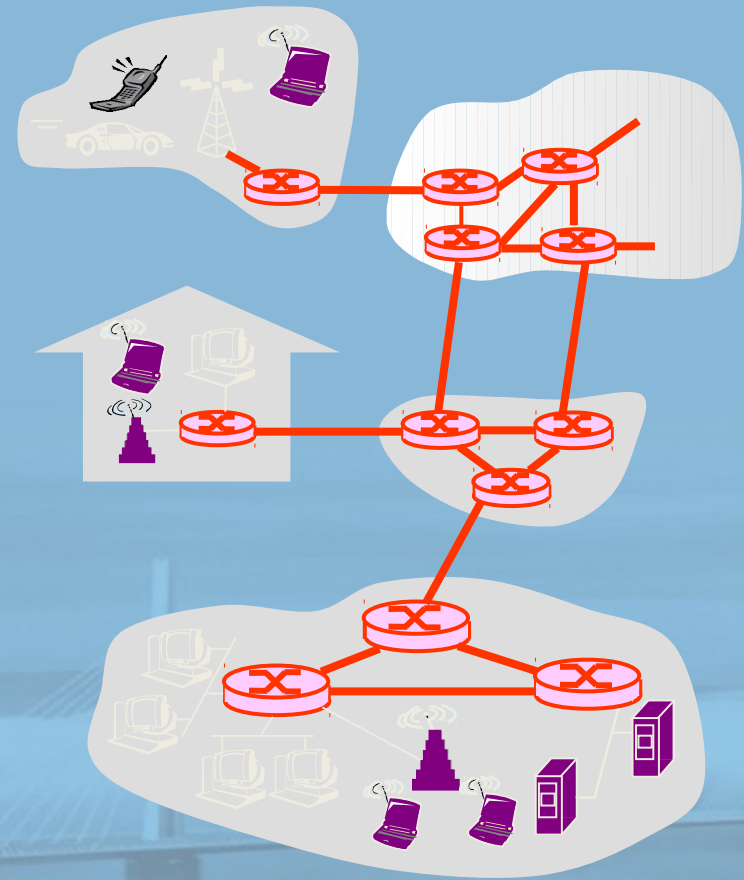
1.4 Atraso, perda e vazão nas redes comutadas por pacotes

1.5 Camadas de protocolo, modelos de serviço

1.6 Redes sob ataque: segurança

# O núcleo da rede

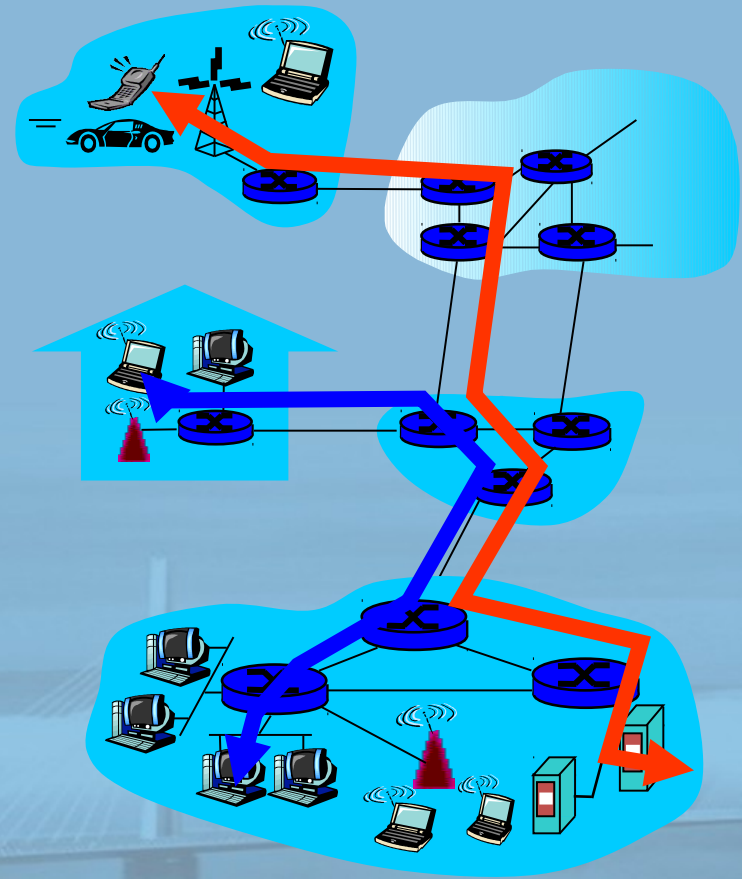
- malha de roteadores interconectados
- **a questão fundamental:** como os dados são transferidos pela rede?
  - **comutação de circuitos:** circuito dedicado por chamada: rede telefônica
  - **comutação de pacotes:** dados enviados pela rede em “pedaços” discretos



# Núcleo da rede: comutação de circuitos

recursos fim a fim  
reservados para  
“chamada”

- largura de banda do enlace, capacidade de comutação
- recursos dedicados: sem compartilhamento
- desempenho tipo circuito (garantido)
- exige preparação de chamada



recursos de rede (p. e.,  
largura de banda)  
**divididos em “pedaços”**

- pedaços alocados a chamadas
- pedaço de recurso **ocioso** se não usado por chamada particular (*sem compartilhamento*)

- ❑ dividindo largura de banda do enlace em “pedaços”
  - ❖ divisão de frequência
  - ❖ divisão de tempo

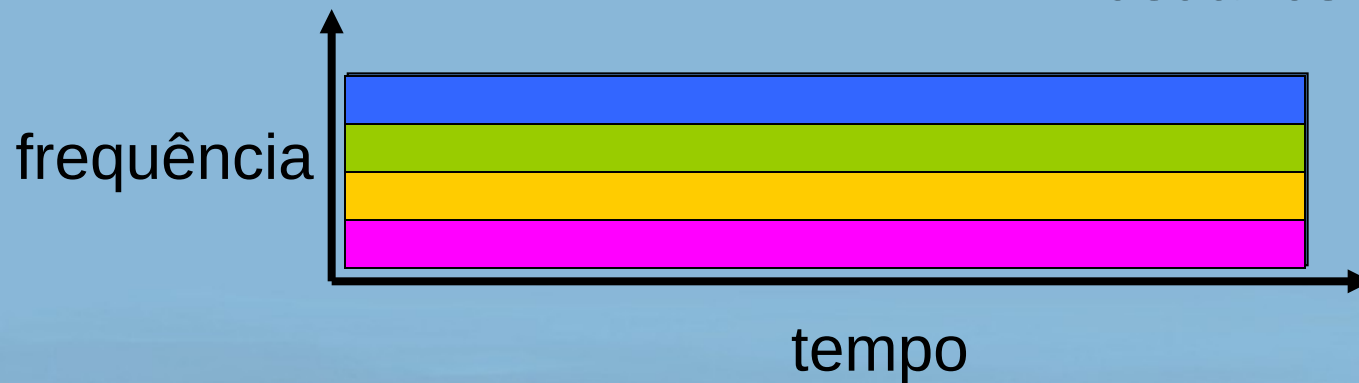


# Comutação de circuitos: FDM e TDM

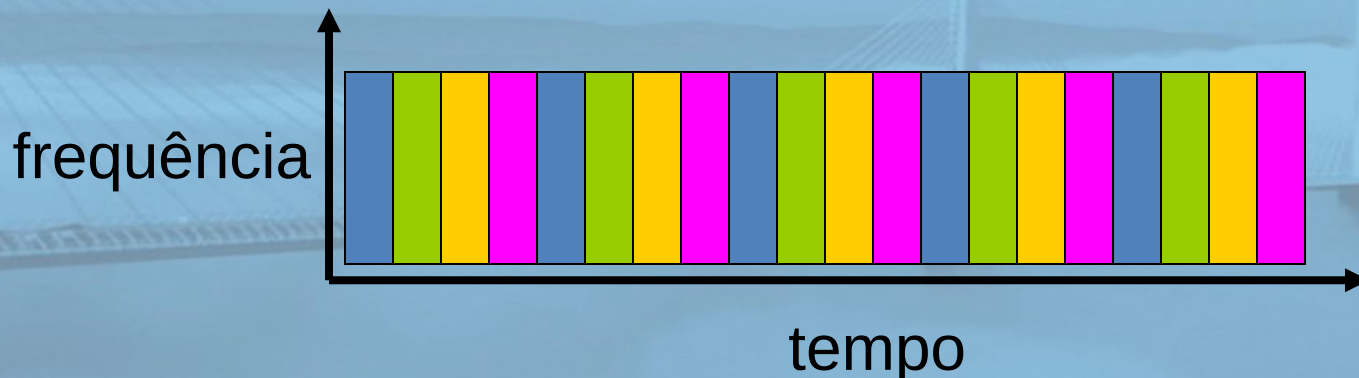
Exemplo:

4 usuários 

FDM: Frequency-Division Multiplexing



TDM: Time-Division Multiplexing



## Exemplo numérico

- Quanto tempo leva para enviar um arquivo de 640.000 bits do hospedeiro A para o hospedeiro B em uma rede de comutação de circuitos?
  - todos os enlaces são de 1,536 Mbps
  - cada enlace usa TDM com 24 slots/seg
  - 500 ms para estabelecer circuito fim a fim

# Núcleo da rede: comutação de pacotes

cada fluxo de dados fim a fim  
dividido em *pacotes*

- vários usuários *compartilham* recursos da rede para envio de pacotes
- cada pacote usa largura de banda total do enlace
- recursos usados *quando necessários*

disputa por recursos

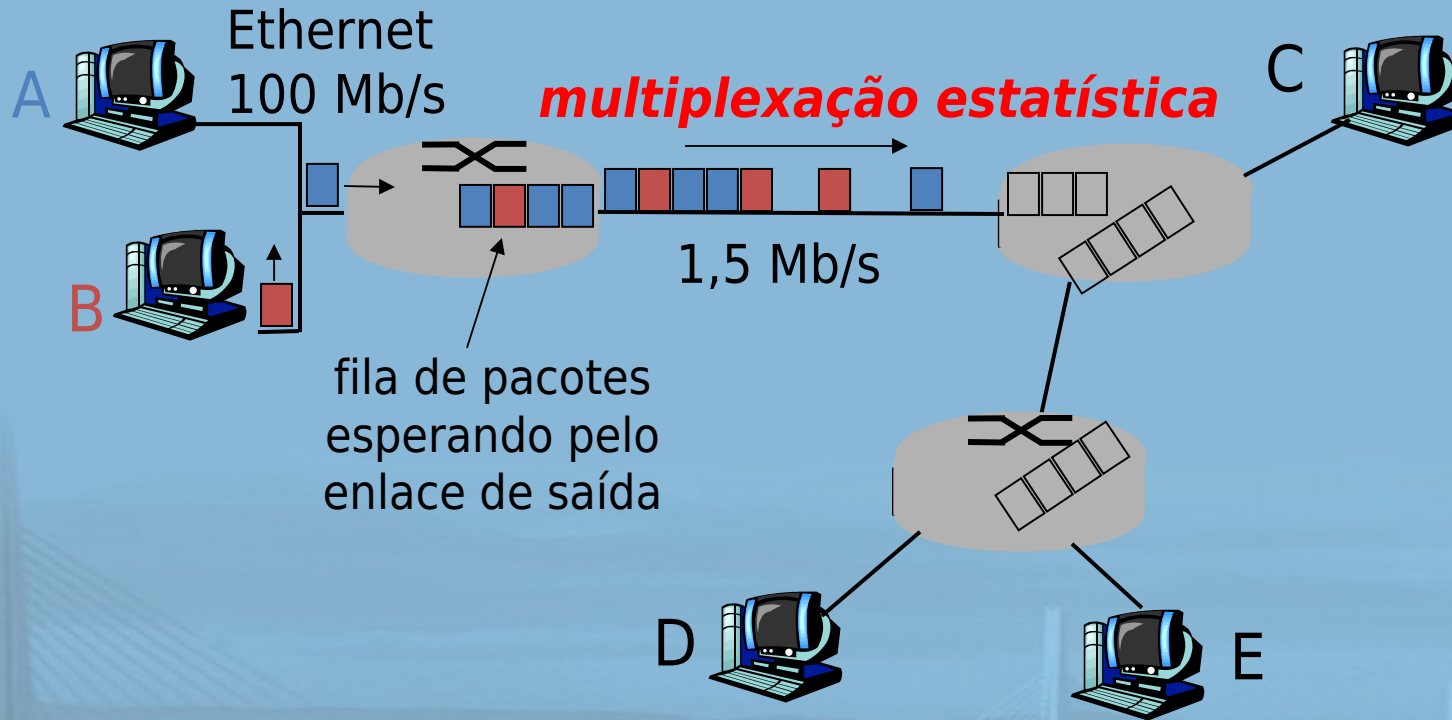
- demanda de recurso agregado pode exceder quantidade disponível
- *congestionamento: fila de pacotes, espera por uso do enlace*
- *store and forward: pacotes se movem um salto de cada vez*
- *nó recebe pacote completo antes de encaminhar*

Divisão da largura de banda em “pedaços”

Alocação dedicada

Reserva de recursos

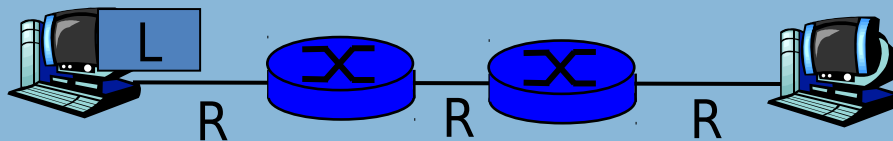
# Comutação de pacotes: multiplexação estatística



Sequência de pacotes A & B não tem padrão fixo, largura de banda compartilhada por demanda ➔ **multiplexação estatística**.

TDM: cada hospedeiro recebe mesmo slot girando quadro TDM.

# Comutação de pacotes: *store-and-forward*



- leva  $L/R$  segundos para transmitir (*push out*) pacote de  $L$  bits para enlace em  $R$  bps
- ***store-and-forward***: pacote inteiro deve chegar ao roteador antes que possa ser transmitido no próximo enlace
- atraso =  $3L/R$  (supondo zero atraso de propagação)

## Exemplo:

- $L = 7,5$  Mbits
- $R = 1,5$  Mbps
- atraso de transmissão = 15 s

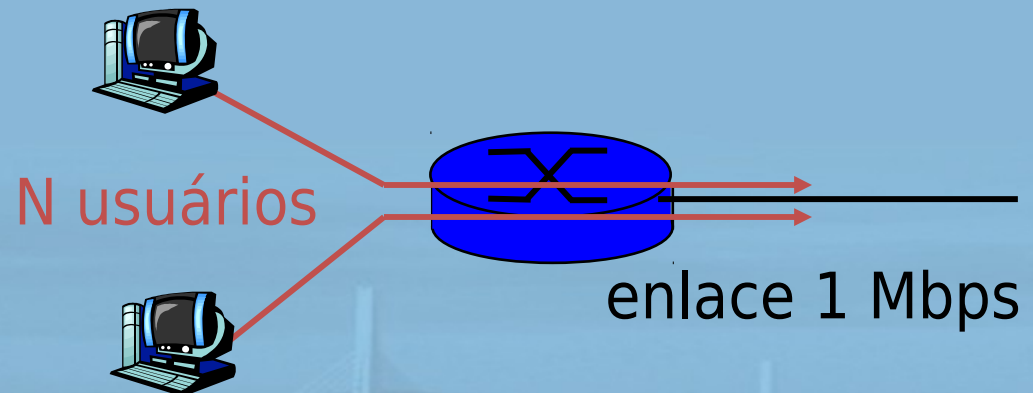
} mais sobre atraso adiante...



# Comutação de pacotes *versus* comutação de circuitos

*Comutação de pacotes permite que mais usuários usem a rede!*

- enlace de 1 Mb/s
- cada usuário:
  - 100 kb/s quando “ativo”
  - ativo 10% do tempo
- *comutação de circuitos*
  - 10 usuários
- *comutação de pacotes:*
  - com 35 usuários,  
probabilidade  $> 10$  ativos  
ao mesmo tempo é menor  
que 0,0004



P: Como obtivemos o valor 0,0004?

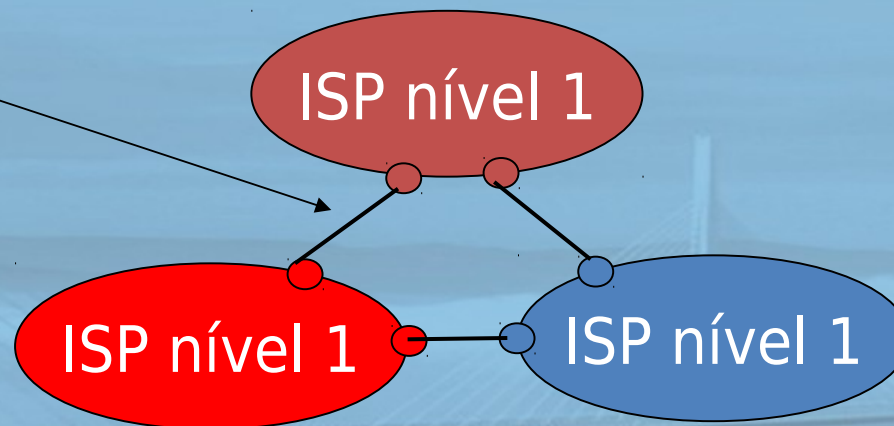
# A comutação de pacotes é a “grande vencedora”?

- ótima para dados em rajadas
  - compartilhamento de recursos
  - mais simples, sem configuração de chamada
- **congestionamento excessivo:** atraso e perda de pacotes
  - protocolos necessários para transferência de dados confiável, controle de congestionamento
- **P: Como fornecer comportamento tipo circuito?**
  - largura de banda garantida necessária para aplicações de áudio/vídeo
  - ainda um problema não resolvido (Capítulo 7)

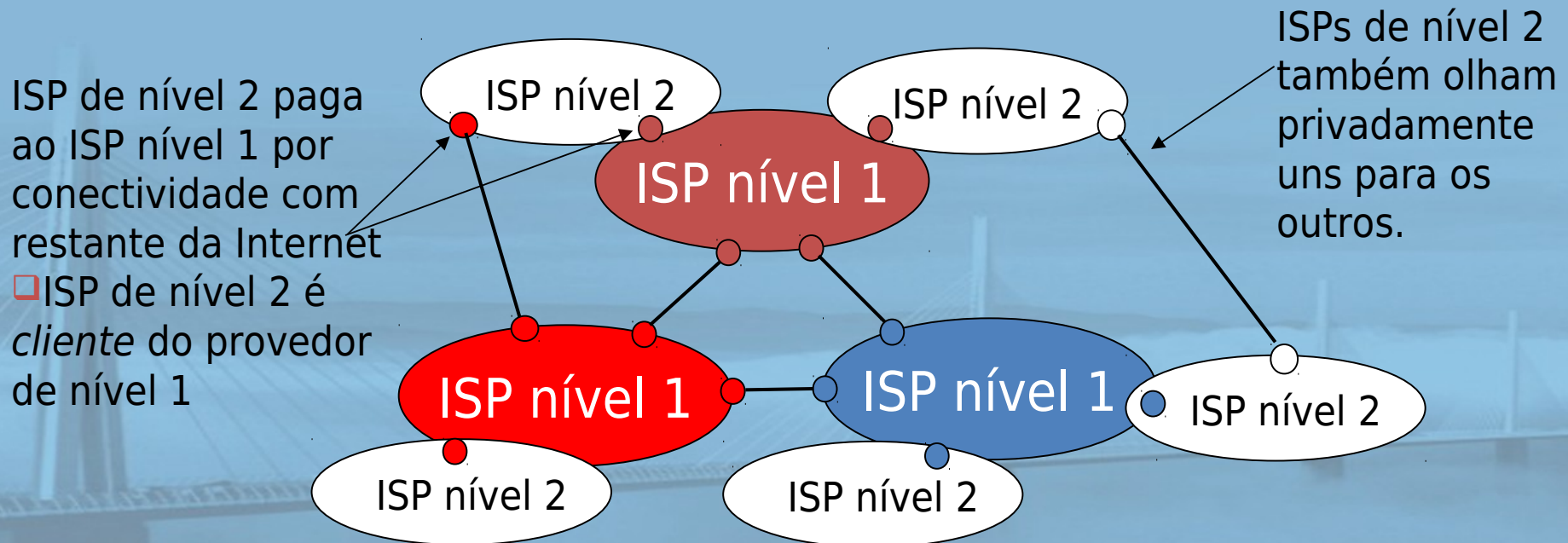
# Estrutura da Internet: rede de redes

- aproximadamente hierárquica
- ISPs (Internet Service Providers)
- **no centro: ISPs de “nível 1”**
  - cobertura nacional/internacional
  - tratam uns aos outros como iguais

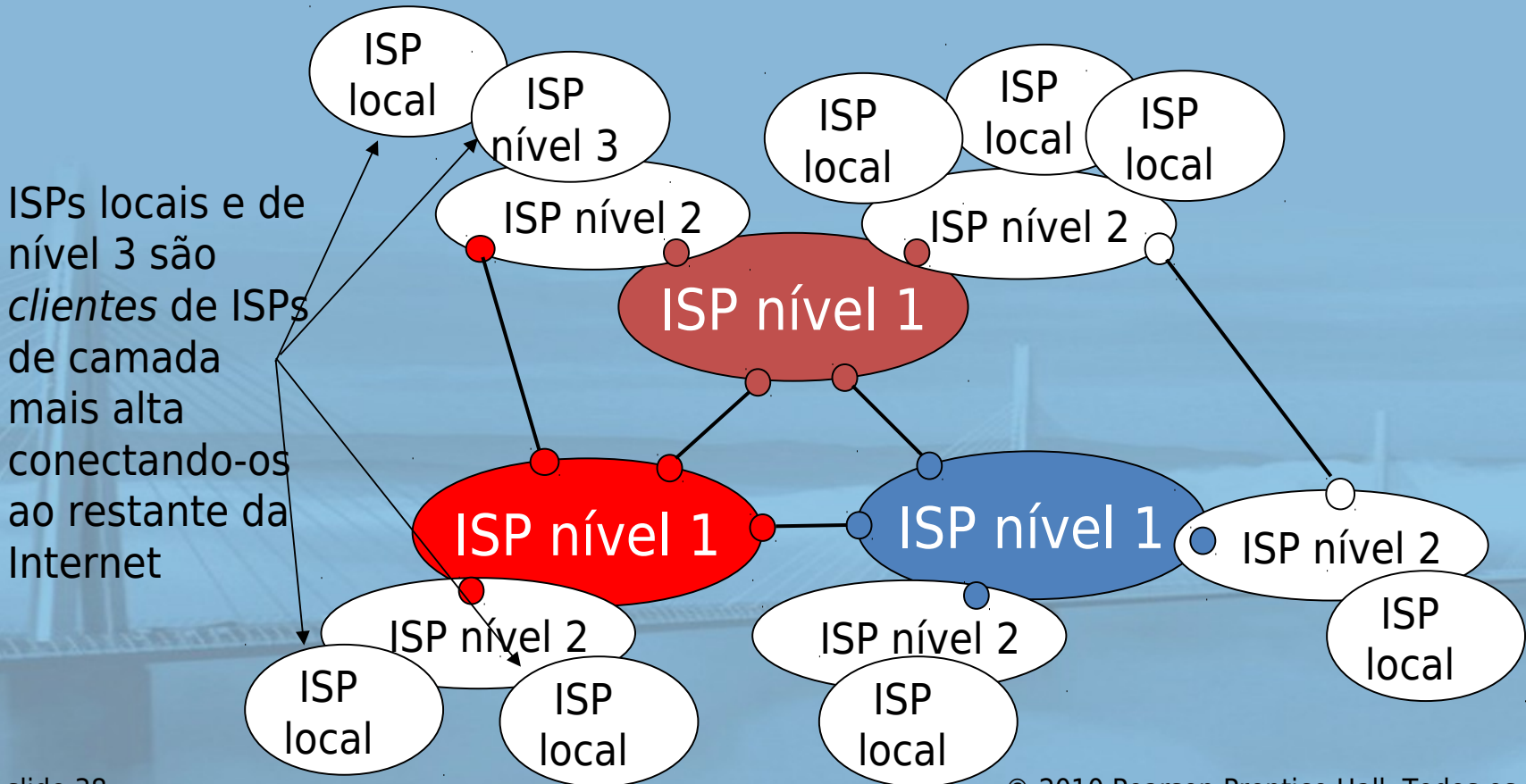
interconexão de  
provedores de  
nível 1 (peer)  
privadamente



- **ISPs de nível 2: ISPs menores (geralmente regionais)**
  - conectam a um ou a mais ISPs de nível 1, possivelmente outros ISPs de nível 2

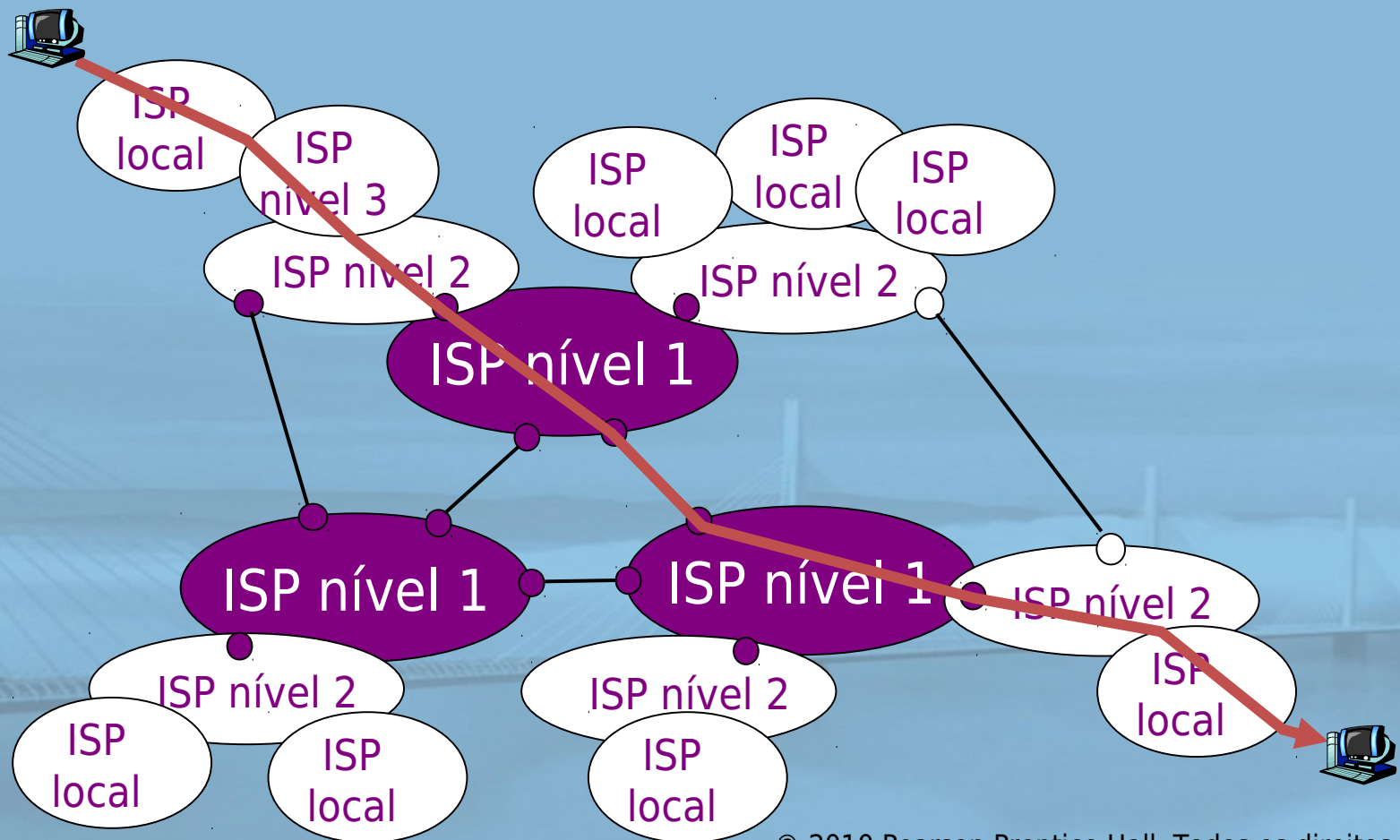


- ISPs de nível 3 e ISPs locais
  - rede do último salto (“acesso”), mais próxima dos sistemas finais





- um pacote passa por muitas redes!



# Capítulo 1: Roteiro

## 1.1 O que é a Internet?

## 1.2 Borda da rede

- sistemas finais, redes de acesso, enlaces

## 1.3 Núcleo da rede

- comutação de circuitos, comutação de pacotes, estrutura da rede

## 1.4 Atraso, perda e vazão nas redes comutadas por pacotes

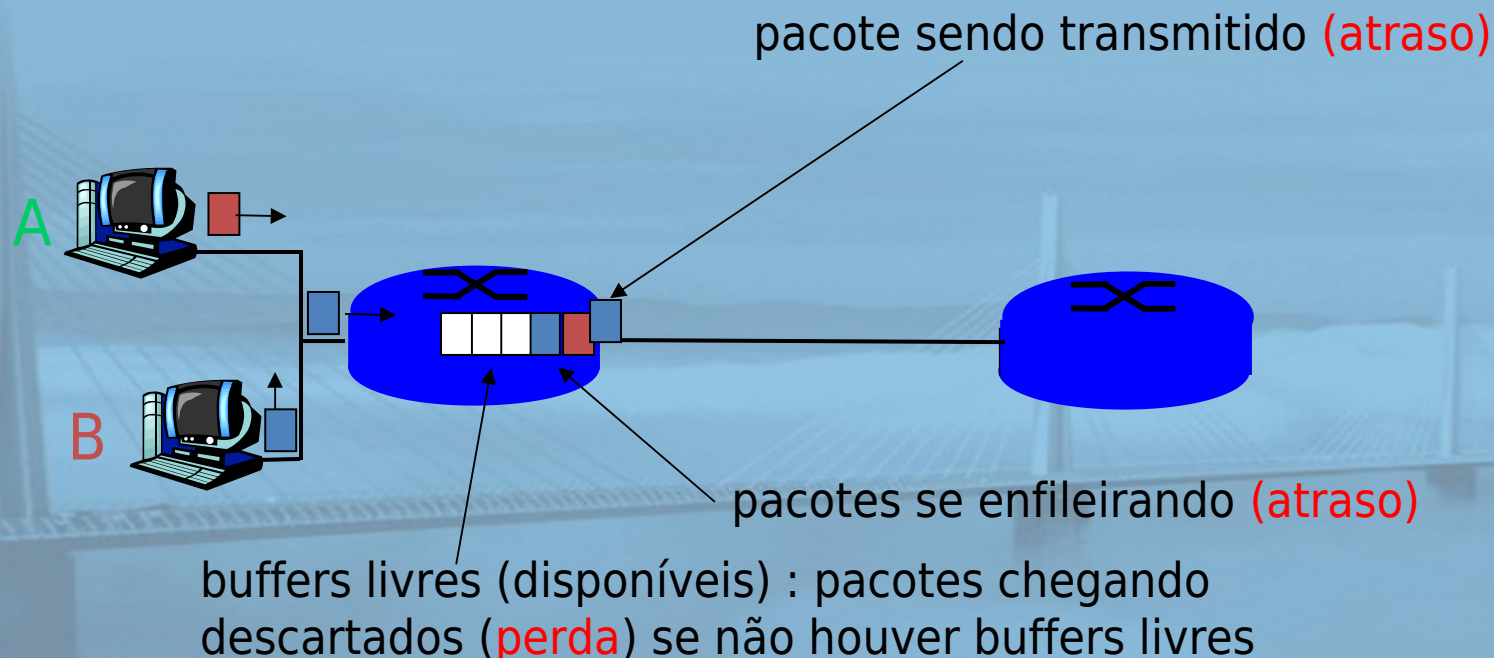
## 1.5 Camadas de protocolo, modelos de serviço

## 1.6 Redes sob ataque: segurança

# Como ocorrem a perda e o atraso?

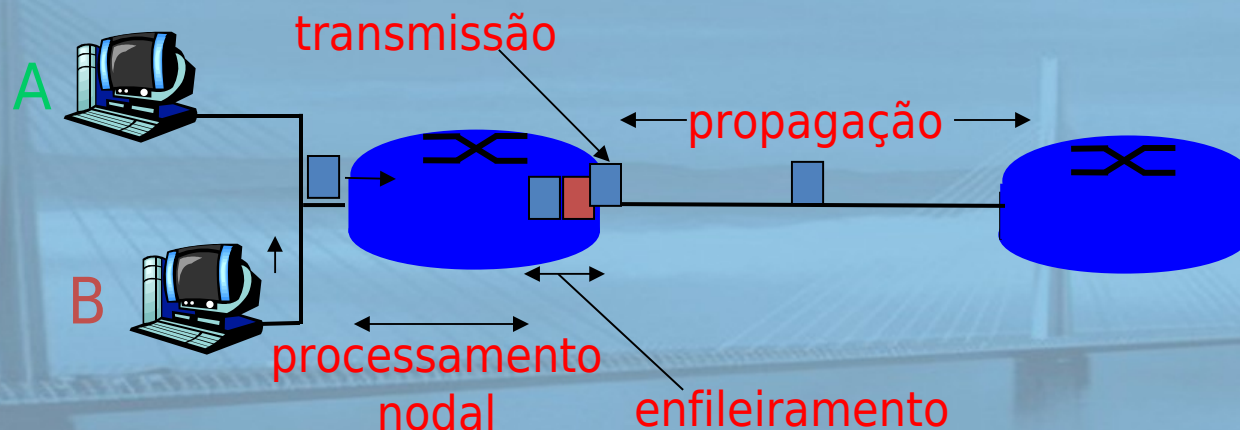
pacotes se *enfileiram* em buffers de roteador

- taxa de chegada de pacotes ao enlace ultrapassa capacidade de saída do enlace
- pacotes se enfileiram, esperam por sua vez



# Quatro fontes de atraso de pacote

- 1. processamento nodal:
  - verificar erros de bit
  - determinar enlace de saída
- 2. enfileiramento
  - ❖ tempo esperando por transmissão no enlace de saída
  - ❖ depende do nível de congestionamento do roteador



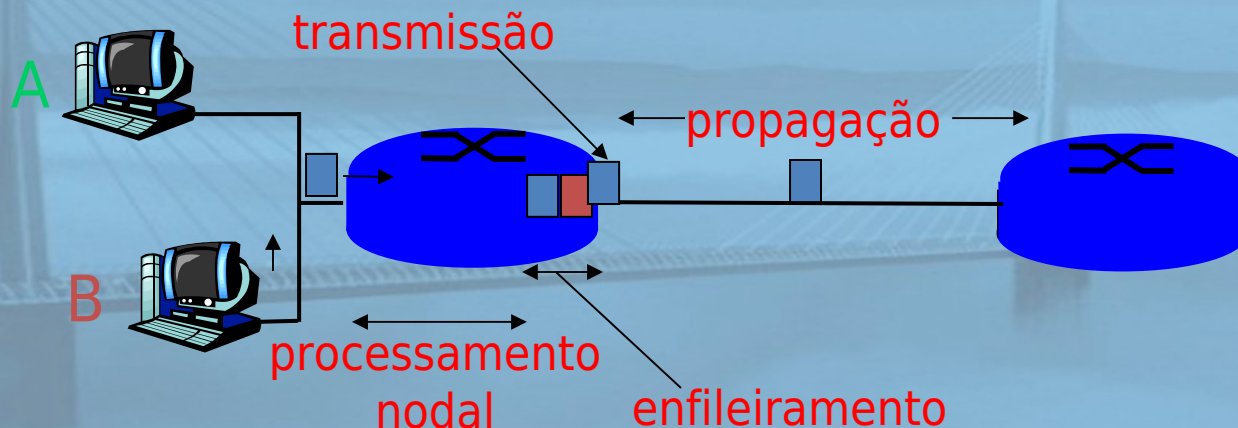
# Atraso nas redes comutadas por pacotes

## 3. atraso de transmissão:

- $R$  = largura de banda do enlace (bps)
- $L$  = tamanho do pacote (bits)
- tempo para enviar bits no enlace =  $L/R$

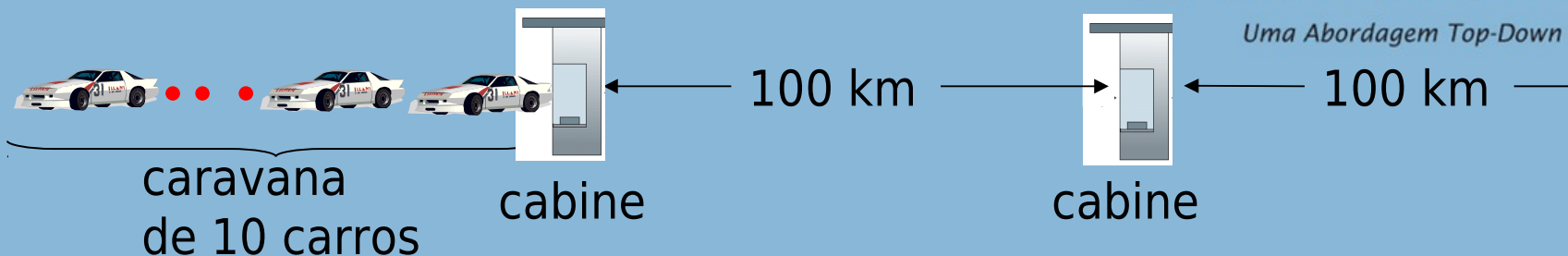
## 4. atraso de propagação:

- $d$  = tamanho do enlace físico
- $s$  = vel. de propagação no meio ( $\sim 2 \times 10^8$  m/s)
- atraso de propagação =  $d/s$



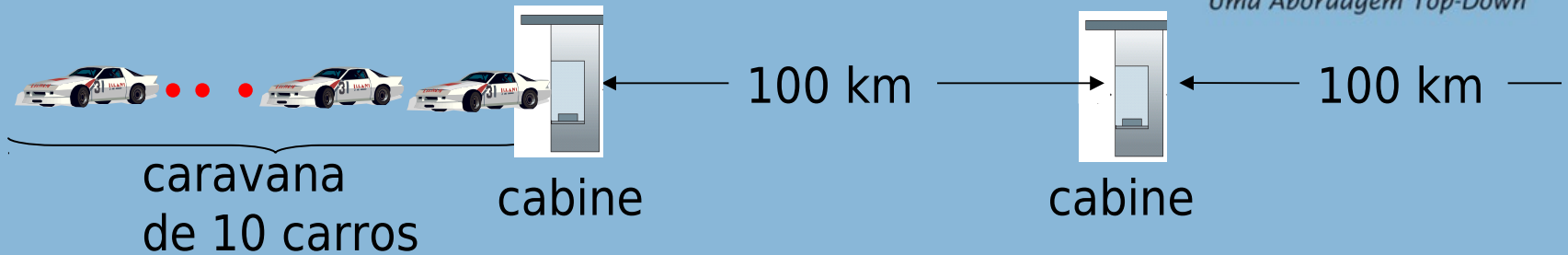


# Analogia da caravana



- carros se “propagam” a 100 km/h
- cabines de pedágio levam 12 s para atender carro (tempo de transmissão)
- carro ~ bit; caravana ~ pacote
- **P: Quanto tempo para a caravana formar fila antes da 2ª cabine?**

- tempo para “empurrar” caravana inteira pela cabine na estrada =  $12 \times 10 = 120$  s
- tempo para último carro se propagar da 1ª à 2ª cabine de pedágio:  $100 \text{ km} / (100 \text{ km/h}) = 1 \text{ h}$
- **Resposta: 62 minutos**



- carros agora se “propagam” a 1000 km/h
- cabine agora leva 1 min para atender um carro
- **P:** Os carros chegarão à 2ª cabine antes que todos os carros sejam atendidos na 1ª cabine?
- **Sim!** Após 7 min, 1º carro na 2ª cabine e 3 carros ainda na 1ª cabine.
- 1º bit do pacote pode chegar ao 2º roteador antes que o pacote seja totalmente transmitido no 1º roteador!

# Atraso nodal

$$d_{\text{nodal}} = d_{\text{proc}} + d_{\text{fila}} + d_{\text{trans}} + d_{\text{prop}}$$

- $d_{\text{proc}}$  = atraso de processamento
  - normalmente, poucos microssegundos ou menos
- $d_{\text{fila}}$  = atraso de enfileiramento
  - depende do congestionamento
- $d_{\text{trans}}$  = atraso de transmissão
  - $L/R$ , significativo para enlaces de baixa velocidade
- $d_{\text{prop}}$  = atraso de propagação
  - alguns microssegundos a centenas de ms

# Atraso de enfileiramento (revisado)

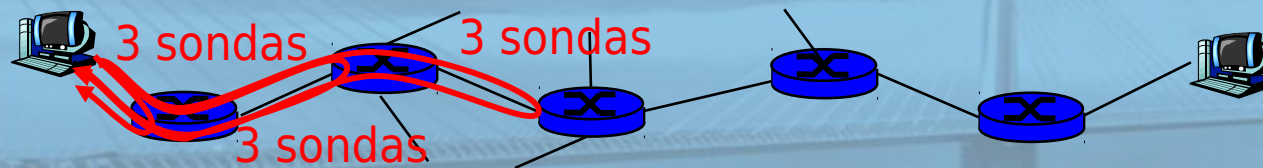
- $R$  = largura de banda do enlace (bps)
- $L$  = tamanho do pacote (bits)
- $a$  = taxa média de chegada de pacote

intensidade de tráfego =  $\lambda a$

- ❑  $\lambda a \sim 0$ : pequeno atraso de enfileiramento médio
- ❑  $\lambda a \rightarrow 1$ : atrasos tornam-se grandes
- ❑  $\lambda a > 1$ : mais “trabalho” chegando do que pode ser atendido, atraso médio infinito!

# Atrasos e rotas “reais” da Internet


- Como são os atrasos e perdas “reais” da Internet?
- Programa Traceroute: fornece medida do atraso da origem ao roteador ao longo do caminho de fim a fim da Internet para o destino. Para todo  $i$ :
  - envia três pacotes que alcançarão roteador  $i$  no caminho para o destino
  - roteador  $i$  retornará pacotes ao emissor
  - emissor temporiza intervalo entre transmissão e resposta.





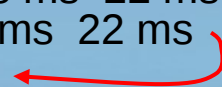
**traceroute:** gaia.cs.umass.edu para www.eurecom.fr

Tres medições de atraso de  
gaia.cs.umass.edu para cs-  
gw.cs.umass.edu




1 cs-gw (128.119.240.254) 1 ms 1 ms 2 ms  
2 border1-rt-fa5-1-0.gw.umass.edu (128.119.3.145) 1 ms 1 ms 2 ms  
3 cht-vbns.gw.umass.edu (128.119.3.130) 6 ms 5 ms 5 ms  
4 jn1-at1-0-0-19.wor.vbns.net (204.147.132.129) 16 ms 11 ms 13 ms  
5 jn1-so7-0-0-0.wae.vbns.net (204.147.136.136) 21 ms 18 ms 18 ms  
6 abilene-vbns.abilene.ucaid.edu (198.32.11.9) 22 ms 18 ms 22 ms  
7 nycm-wash.abilene.ucaid.edu (198.32.8.46) 22 ms 22 ms 22 ms  
8 62.40.103.253 (62.40.103.253) 104 ms 109 ms 106 ms  
9 de2-1.de1.de.geant.net (62.40.96.129) 109 ms 102 ms 104 ms  
10 de.fr1.fr.geant.net (62.40.96.50) 113 ms 121 ms 114 ms  
11 renater-gw.fr1.fr.geant.net (62.40.103.54) 112 ms 114 ms 112 ms  
12 nio-n2.cssi.renater.fr (193.51.206.13) 111 ms 114 ms 116 ms  
13 nice.cssi.renater.fr (195.220.98.102) 123 ms 125 ms 124 ms  
14 r3t2-nice.cssi.renater.fr (195.220.98.110) 126 ms 126 ms 124 ms  
15 eurecom-valbonne.r3t2.ft.net (193.48.50.54) 135 ms 128 ms 133 ms  
16 194.214.211.25 (194.214.211.25) 126 ms 128 ms 126 ms  
17 \* \* \*  
18 \* \* \*  
19 fantasia.eurecom.fr (193.55.113.142) 132 ms 128 ms 136 ms

enlace trans-oceânico

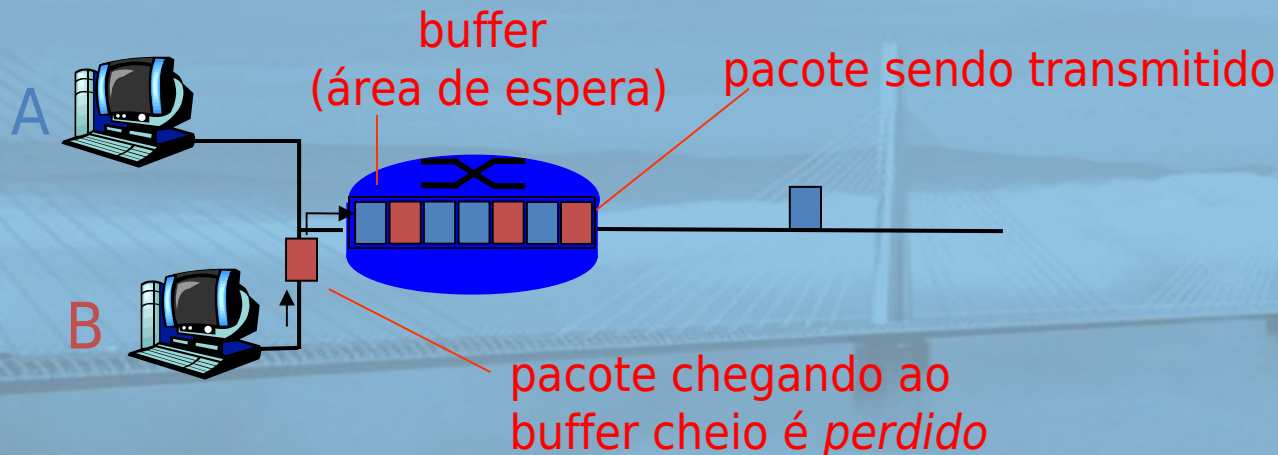


\* significa sem resposta (sonda perdida, roteador sem resposta)



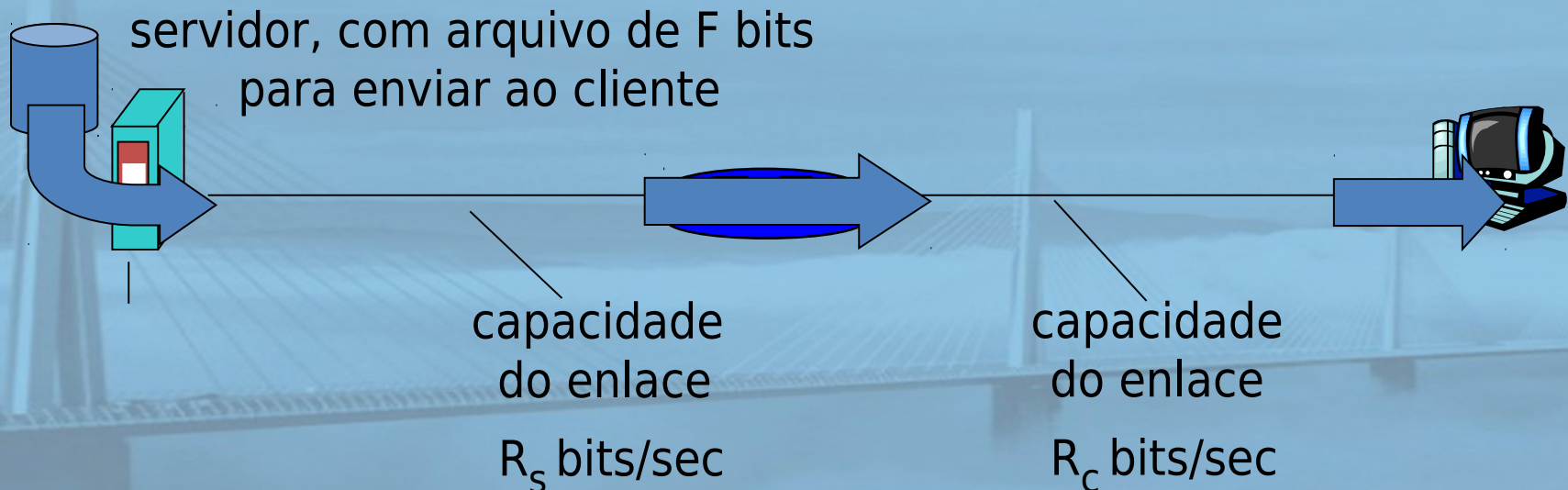
# Perda de pacote

- fila (ou buffer) antes do enlace no buffer tem capacidade finita
- pacote chegando à fila cheia descartado (ou perdido)
- último pacote pode ser retransmitido pelo nó anterior, pela origem ou de forma nenhuma

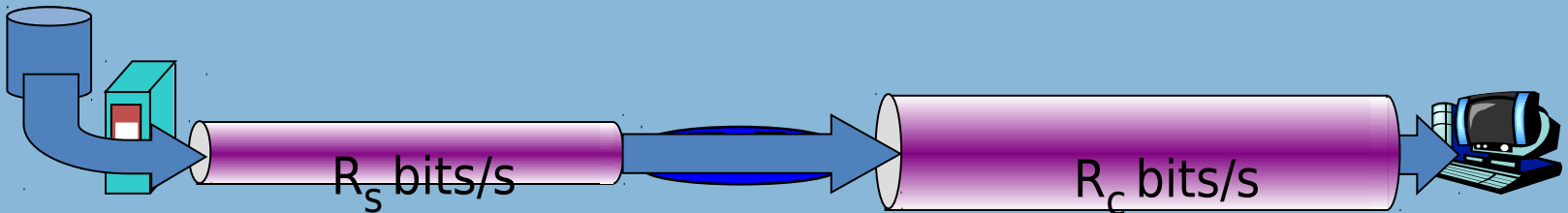


# Vazão

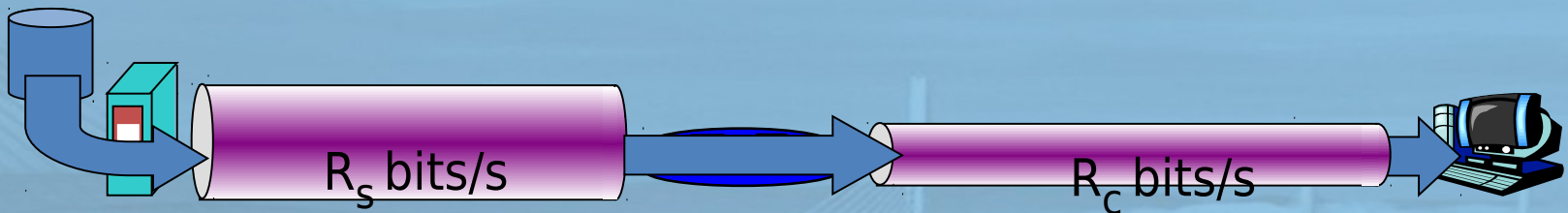
- *vazão*: taxa (bits/unidade de tempo) em que os bits são transferidos entre emissor/receptor
  - *instantânea*: taxa em determinado ponto no tempo
  - *média*: taxa por período de tempo maior



- $R_s < R_c$  Qual é a vazão média de fim a fim?



- $R_s > R_c$  Qual é a vazão média de fim a fim?

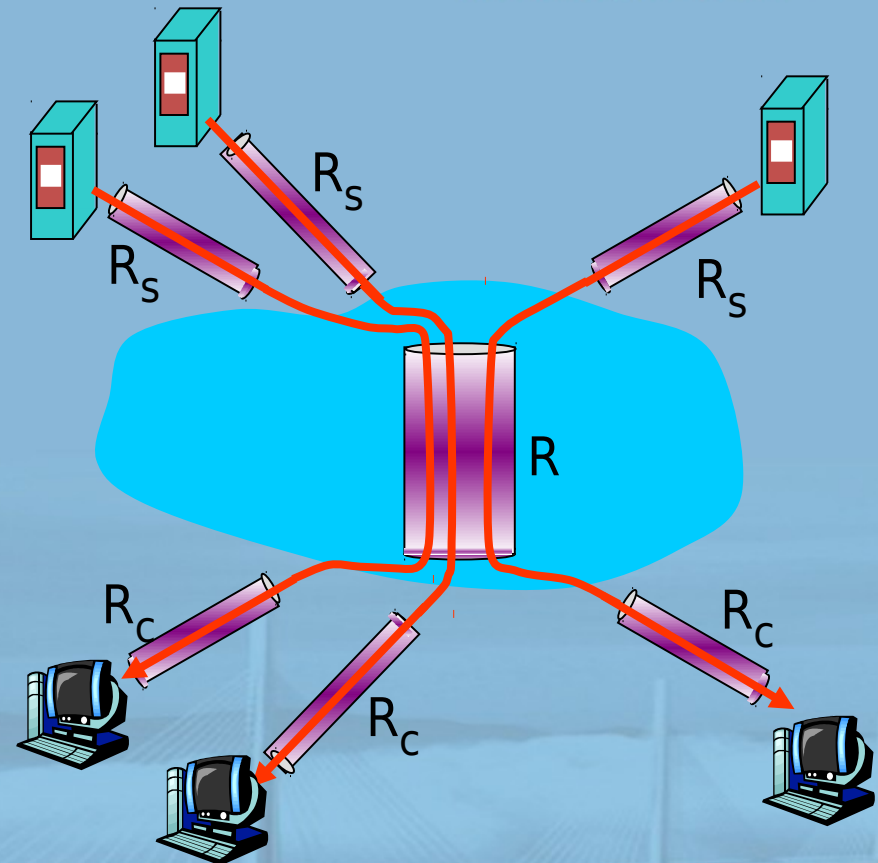


*enlace de gargalo*

enlace no caminho de fim a fim que restringe a vazão de fim a fim

# Vazão: cenário da Internet

- na prática:  $R_c$  ou  $R_s$  normalmente é gargalo
- vazão de fim a fim por conexão:  
 $\min(R_c, R_s, R/10)$



10 conexões (aproximadamente)  
compartilham enlace de gargalo do  
backbone a  $R$  bits/s



# Capítulo 1: Roteiro

1.1 O que é a Internet?

1.2 Borda da rede

- sistemas finais, redes de acesso, enlaces

1.3 Núcleo da rede

- comutação de circuitos, comutação de pacotes, estrutura da rede

1.4 Atraso, perda e vazão nas redes comutadas por pacotes

1.5 Camadas de protocolo, modelos de serviço

1.6 Redes sob ataque: segurança

# “Camadas” de protocolo

## Redes são complexas!

- muitas “partes”:
  - hospedeiros
  - roteadores
  - enlaces de vários meios físicos
  - aplicações
  - protocolos
  - hardware, software

## Pergunta:

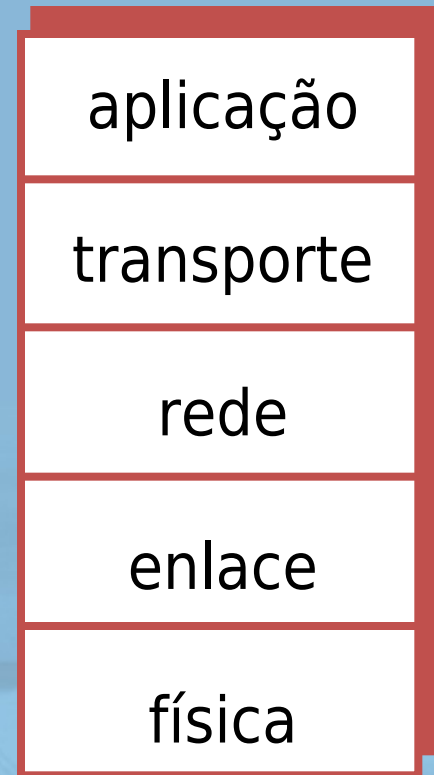
Existe esperança de *organizar* a estrutura da rede?

Ou, pelo menos, nossa discussão sobre redes?

# Pilha de protocolos da Internet

## CAMADAS

- **aplicação:** suporte a aplicações de rede
  - FTP, SMTP, HTTP
- **transporte:** transferência de dados processo-processo
  - TCP, UDP
- **rede:** roteamento de datagramas da origem ao destino
  - IP, protocolos de roteamento
- **enlace:** transferência de dados entre elementos vizinhos da rede
  - PPP, Ethernet
- **física:** bits “nos fios”



# Modelo de referência ISO/OSI

## CAMADAS

- **apresentação:** permite que as aplicações interpretem significado de dados, p. e., criptografia, compactação, convenções específicas da máquina
- **session:** sincronização, verificação, recuperação de troca de dados
- Pilha da Internet “faltando” essas camadas!
  - estes serviços, *se necessários*, devem ser implementados na aplicação
  - necessários?

aplicação

transporte

rede

enlace

física

# Por que usar camadas?

## lidando com sistemas complexos:

- estrutura explícita permite identificação e relação entre partes complexas do sistema
  - **modelo de referência** em camadas para discussão
- modularização facilita manutenção e atualização do sistema
  - mudança de implementação do serviço da camada transparente ao restante do sistema
  - p. e., mudanças no procedimento de porta não afeta o restante do sistema
- uso de camadas considerado prejudicial?



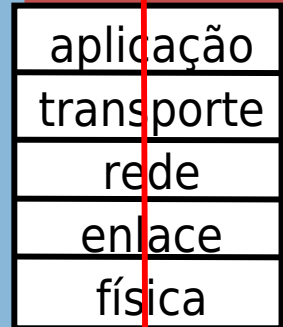
origem

mensagem M

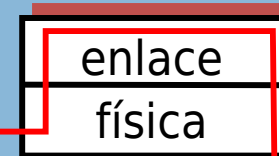
segmento H<sub>t</sub> M

datagrama H<sub>n</sub> H<sub>t</sub> M

quadro H<sub>l</sub> H<sub>n</sub> H<sub>t</sub> M



H<sub>l</sub> H<sub>n</sub> H<sub>t</sub> M



comutador

## Encapsulamento

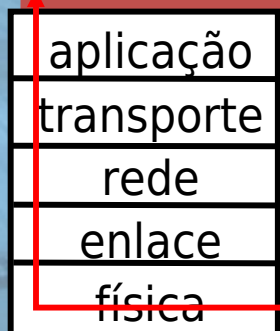
destino

M

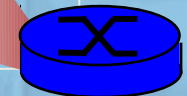
H<sub>t</sub> M

H<sub>n</sub> H<sub>t</sub> M

H<sub>l</sub> H<sub>n</sub> H<sub>t</sub> M



H<sub>n</sub> H<sub>t</sub> M



roteador

# Capítulo 1: Roteiro

1.1 O que é a Internet?

1.2 Borda da rede

- ❑ sistemas finais, redes de acesso, enlaces

1.3 Núcleo da rede

- ❑ comutação de circuitos, comutação de pacotes, estrutura da rede

1.4 Atraso, perda e vazão nas redes comutadas por pacotes

1.5 Camadas de protocolo, modelos de serviço

1.6 Redes sob ataque: segurança

# Segurança de rede

- o campo da segurança de rede trata de:
  - como defender as redes contra ataques
  - como maus sujeitos atacam redes de computadores
  - como projetar arquiteturas imunes a ataques
- Internet não criada originalmente com (muita) segurança em mente
  - *visão original*: “um grupo de usuários mutuamente confiáveis conectados a uma rede transparente”
  - protocolos da Internet são abertos
  - considerações de segurança em todas as camadas!

# Malicious Software (Malwares)

- Maus sujeitos podem colocar malware em hospedeiros via internet
- malware pode entrar em um hospedeiro por **vírus**, **worm** ou **cavalo de Troia**.
- **malware do tipo spyware** pode registrar toques de teclas, sites visitados na Web, enviar informações para sites de coleta.
- hospedeiro infectado pode ser alistado em um **botnet**, usado para spam e ataques de DDoS.
- malware normalmente é **autorreplicável**: de um hospedeiro infectado, busca entrada em outros hospedeiros

- **cavalo de Troia**

- parte oculta de algum software útil
- hoje, normalmente em uma página Web (Active-X, plug-in)

- **vírus**

- infecção ao receber objeto (p. e., anexo de e-mail), executando ativamente
- autorreplicável: propagando-se para outros hospedeiros, usuários

- **worm:**

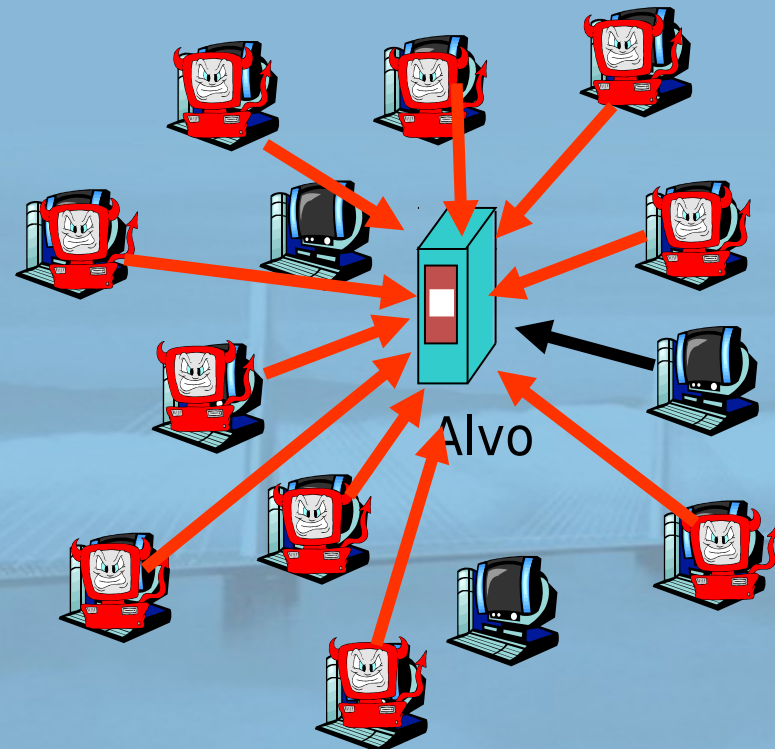
- ❖ infecção recebendo passivamente objeto a ser executado
- ❖ autorreplicável: propaga-se para outros hospedeiros, usuários



# Maus sujeitos podem atacar servidores e infraestrutura de rede

- Denial of Service (DoS): atacantes deixam recursos (servidor, largura de banda) indisponíveis ao tráfego legítimo, sobrecarregando recurso com tráfego

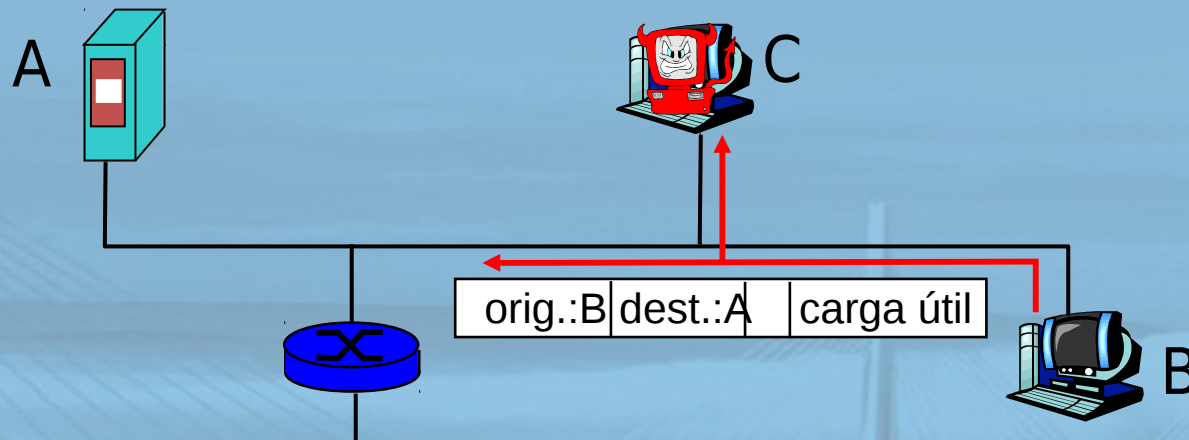
1. selecionar alvo
2. invadir hospedeiros na rede (ver botnet)
3. enviar pacotes para o alvo a partir dos hospedeiros comprometidos



# Maus sujeitos podem farejar pacotes

## *Farejamento de pacotes (sniffing):*

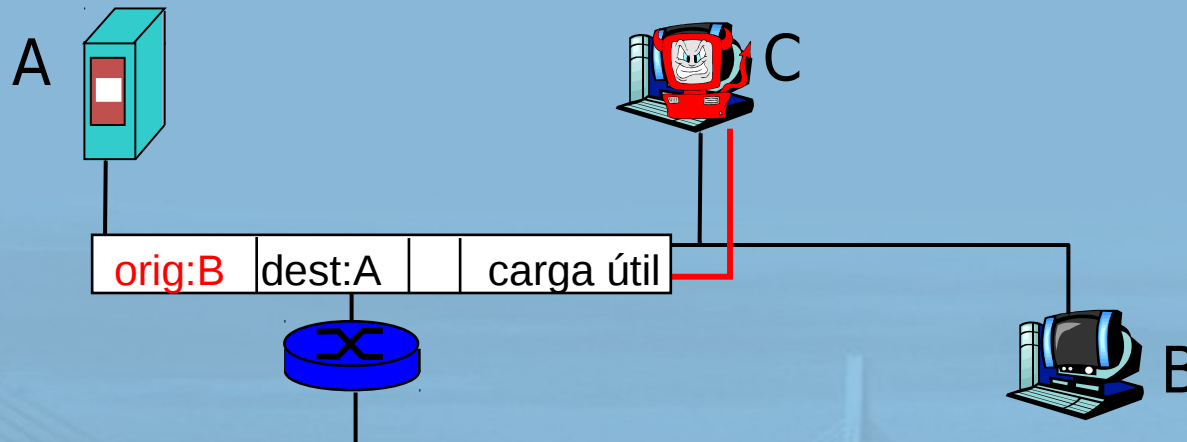
- meio de broadcast (Ethernet compartilhada, sem fio)
- interface de rede promíscua lê/registra todos os pacotes (p. e., incluindo senhas!)



- ❖ software Wireshark usado para laboratório do farejador de pacotes (gratuito)

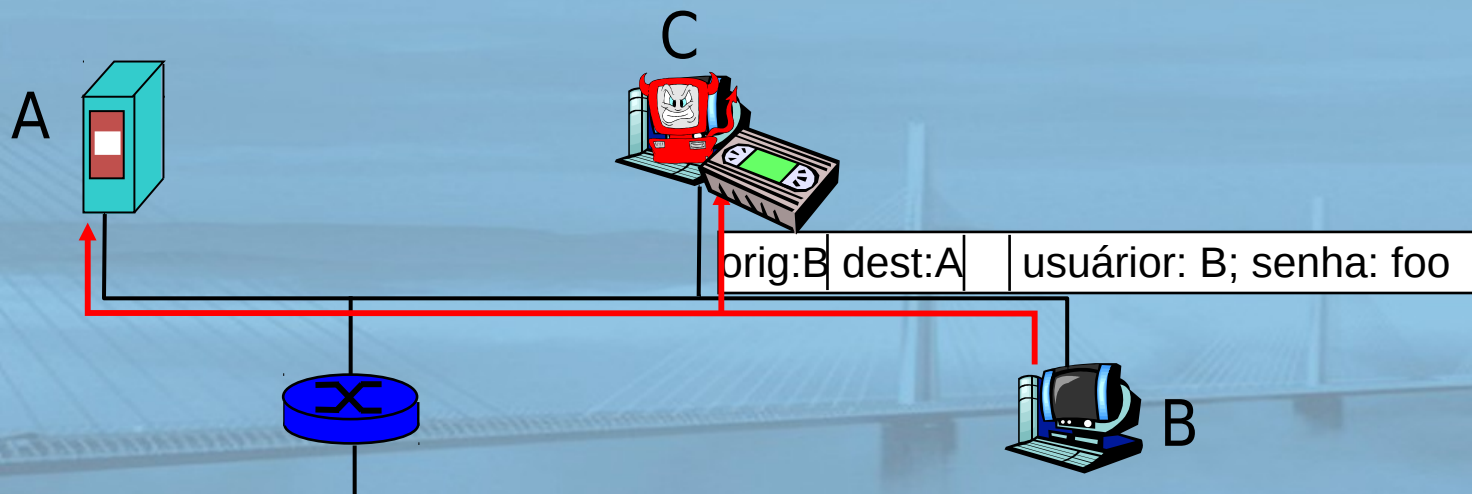
# Maus sujeitos podem usar endereços de origem falsos

- *IP spoofing*: enviar pacote com endereço de origem falso



# Maus sujeitos podem gravar e reproduzir

- **gravar-e-reproduzir**: informação confidencial (p. e., senha) é usada mais tarde
  - quem tem a senha é esse usuário, do ponto de vista do sistema



# Introdução: resumo

## Vimos muito material!

- visão geral da Internet
- O que é um protocolo?
- borda da rede, núcleo, rede de acesso
  - comutação de pacotes e circuitos
  - estrutura da Internet
- desempenho: perda, atraso e vazão
- camadas, modelos de serviço
- segurança

## Objetivo:

- contexto, visão geral, “sentido” de rede