

Redes de Computadores

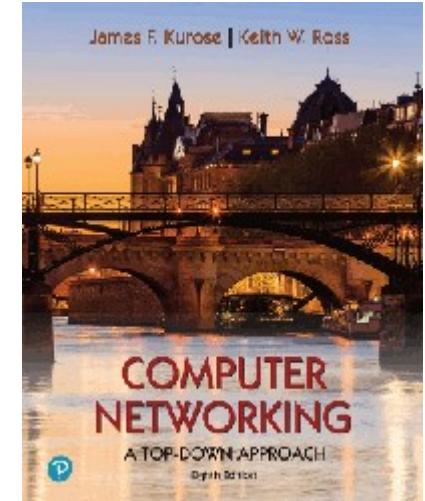
Introdução

Material baseado nas apresentações (*slides*) disponibilizados junto com o livro referência a seguir.

A note on the use of these Powerpoint slides:
We're making these slides freely available to all (faculty, students, readers). They're in PowerPoint form so you see the animations; and can add, modify, and delete slides (including this one) and slide content to suit your needs. They obviously represent a *lot* of work on our part. In return for use, we only ask the following:

Bibliografia:
Computer Networking: A Top Down Approach

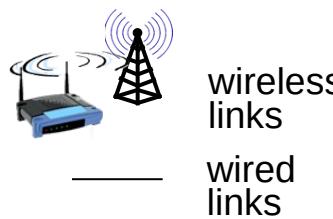
8th Edition, Global Edition
Jim Kurose, Keith Ross
Pearson 2020



Sumário

- O que é a Internet? O que é um protocolo?
- Borda da rede: hosts, acesso, meios físicos
- Núcleo da rede: comutação de circuitos e de pacotes; estrutura da Internet
- Questões de performance: perda, atraso, desempenho
- Segurança
- Camadas de protocolos, modelos de serviço
- História

O que é a Internet



Bilhões de **dispositivos conectados**:

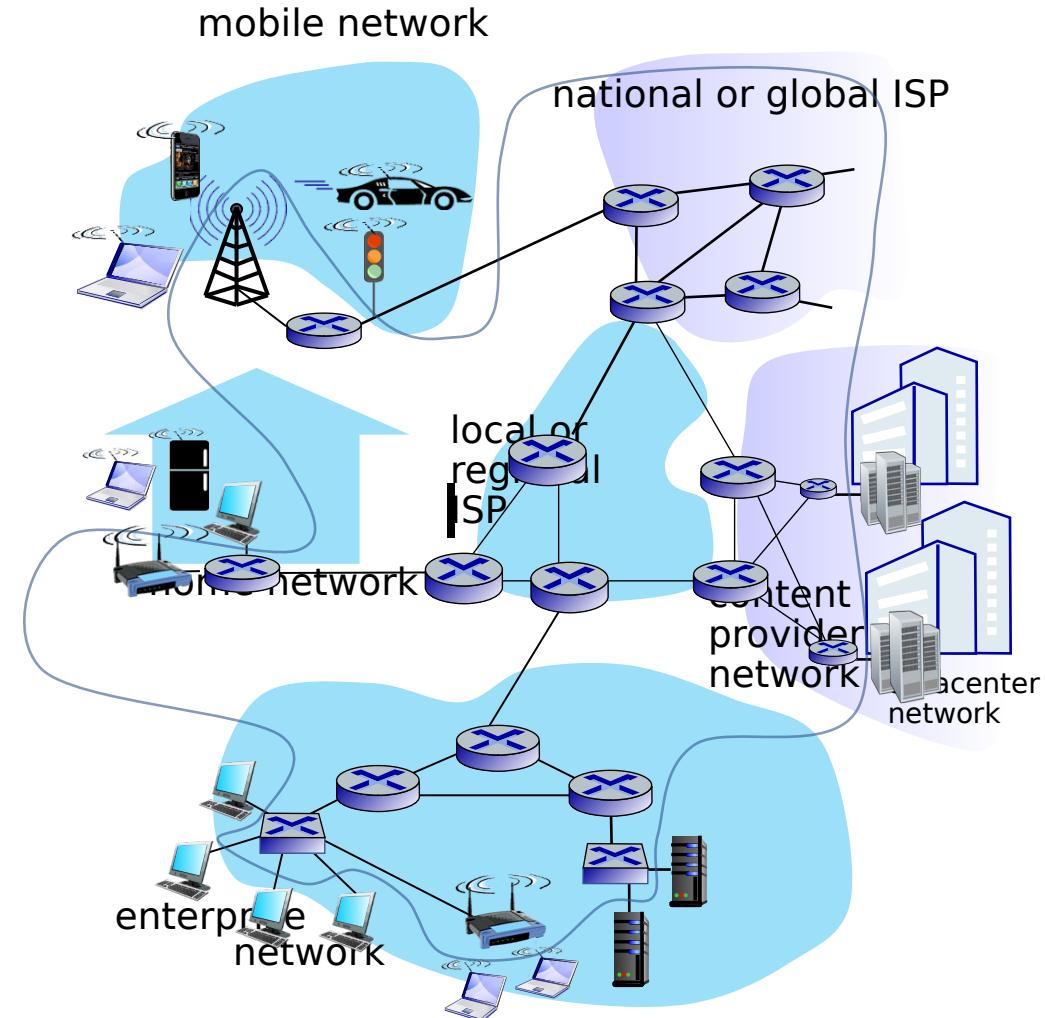
- hosts = sistemas finais
- Executam *aplicações de rede*

Enlaces de comunicação

- Fibra, fios de cobre (par trançado), rádio, satélite
- Razão de transmissão: **largura de banda**

Comutação de pacotes: encaminha pacotes (pedaços de dados)

- roteadores e switches



O que é a Internet



Amazon Echo



Internet refrigerator



Security Camera



Internet phones



IP picture frame



Slingbox: remote control cable TV



Pacemaker & Monitor



Web-enabled toaster + weather forecaster



sensorized, bed mattress

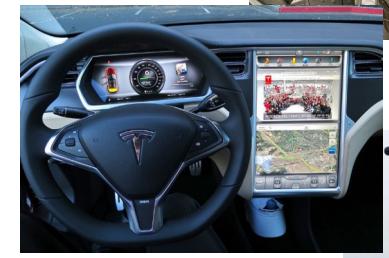


Fitbit



Tweet-a-watt:
monitor energy use

bikes



cars



scooters

O que é a Internet



Tweet-a-watt:
monitor energy use

IS



oters

Internet of Things (IoT)

Internet of Medical Things (IoMT)

Industrial Internet of Things (IioT)

Internet of Battlefield Things (IoBT)

.....



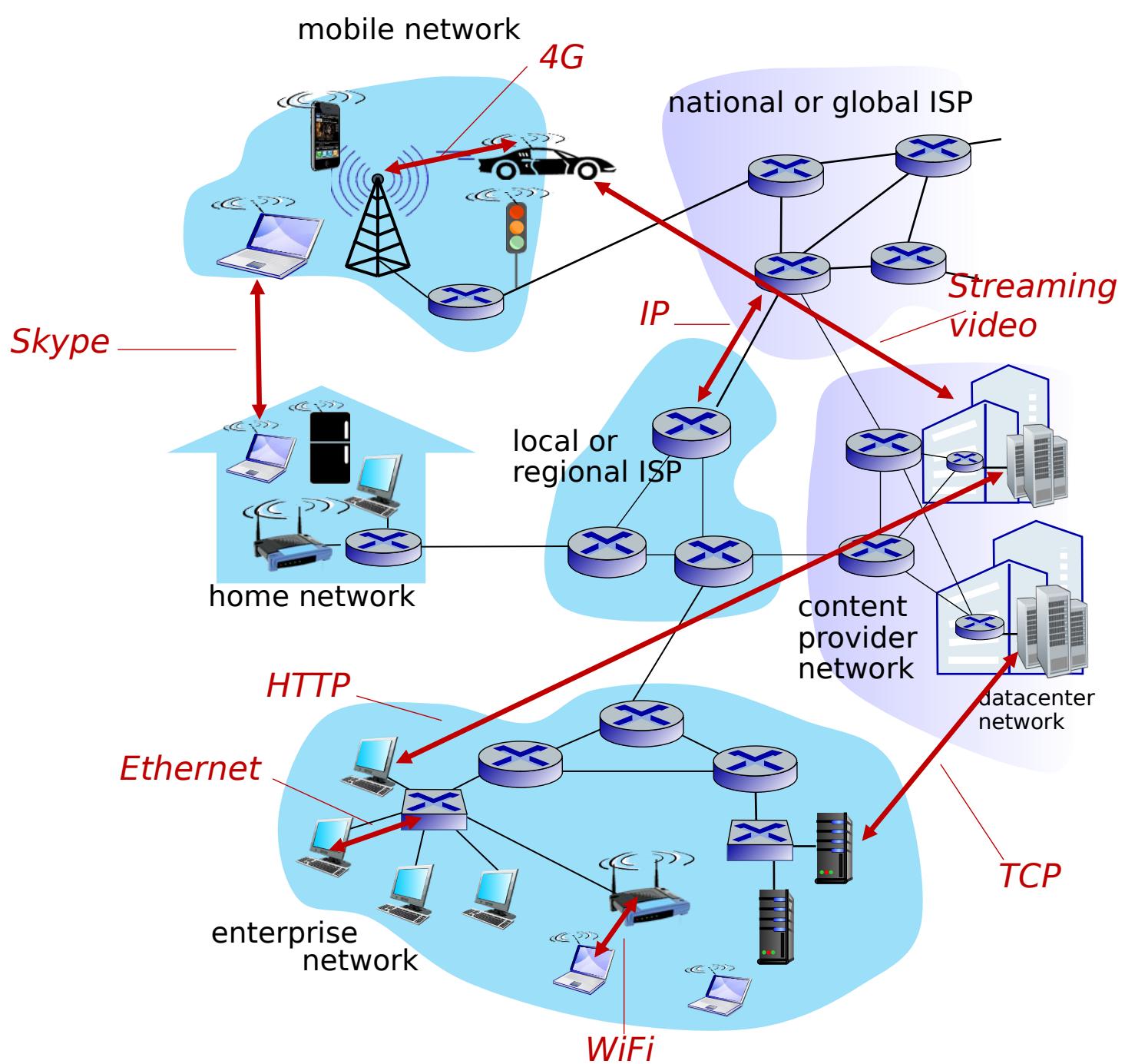
Internet phones



Gaming devices



Fitbit



Visão geral da Internet

Internet: “redes das redes”

ISPs interconectados

Protocolos controlando o envio e recebimento de mensagens

Ex.: TCP, IP, HTTP, DNS, DHCP, 802.11 (WiFi), 4/5G, Ethernet, streaming de vídeo e de áudio (Skype)

Padrões em Internet

RFC (*Request for Comments*)

IETF (*Internet Engineering Task Force*): www.ietf.org

Visão geral da Internet

Infraestrutura que provê serviço às aplicações:
Web, VoIP, email, games, e-commerce, redes sociais,
etc

Provê interface para a programação de aplicações distribuídas

- Meios para enviar e receber informações (dados, códigos, etc) usando o serviço de transporte da Internet
- As interfaces proveem opções de tipos de serviços
- Interface Sockets

O que é um protocolo?

Protocolos humanos:

- “que horas são?”
- Apresentações pessoais

... mensagens específicas são enviadas

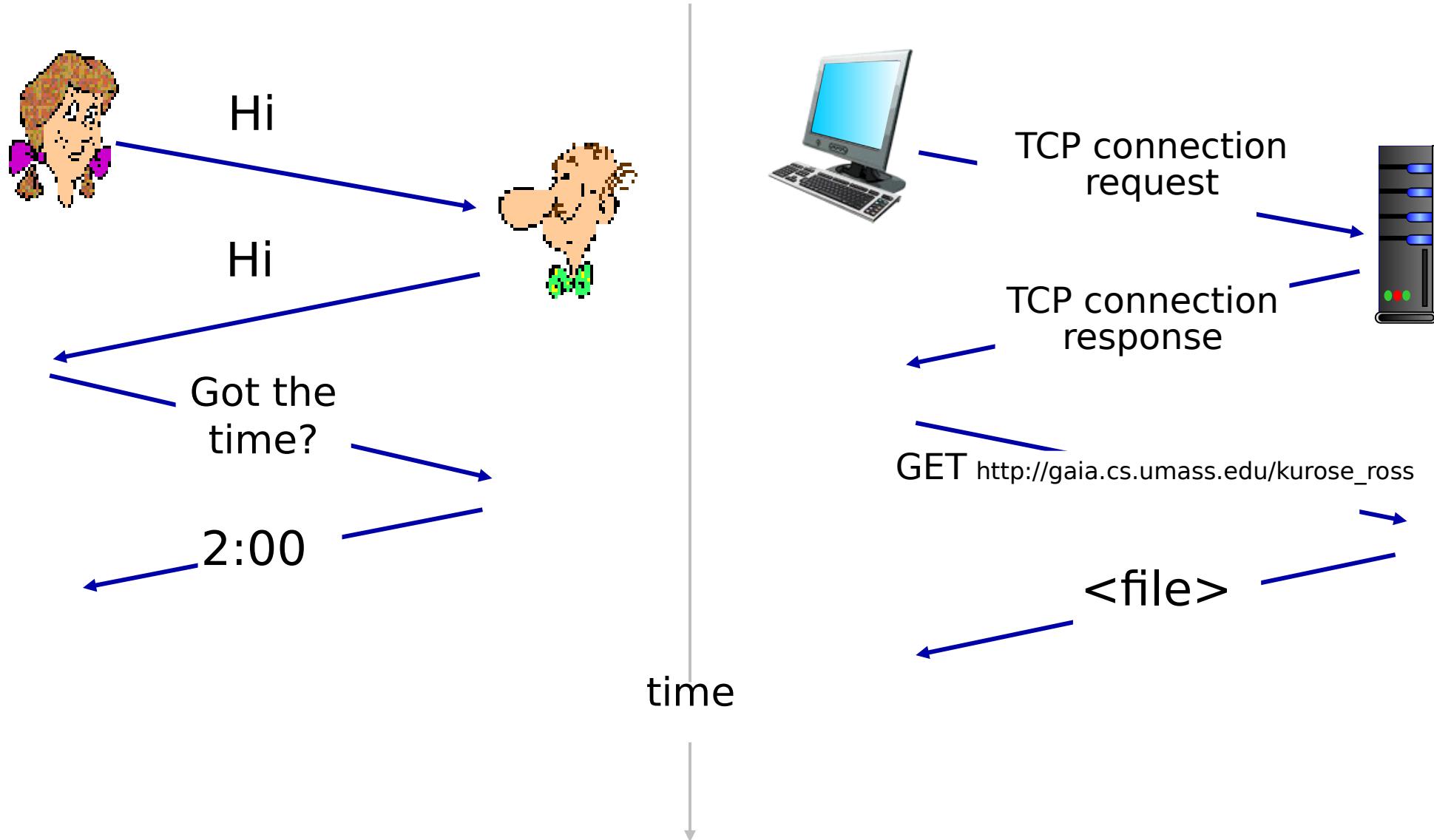
... ações específicas são tomadas quando mensagens chegam

Protocolos de rede:

- Máquinas e dispositivos (hw/sw)
- Toda atividade de comunicação na Internet é governada por protocolos

Protocolos definem **formato** e **ordem** das **mensagens enviadas e recebidas** entre entidades na rede, e as respectivas **ações tomadas** quando do recebimento e transmissão

O que é um protocolo?



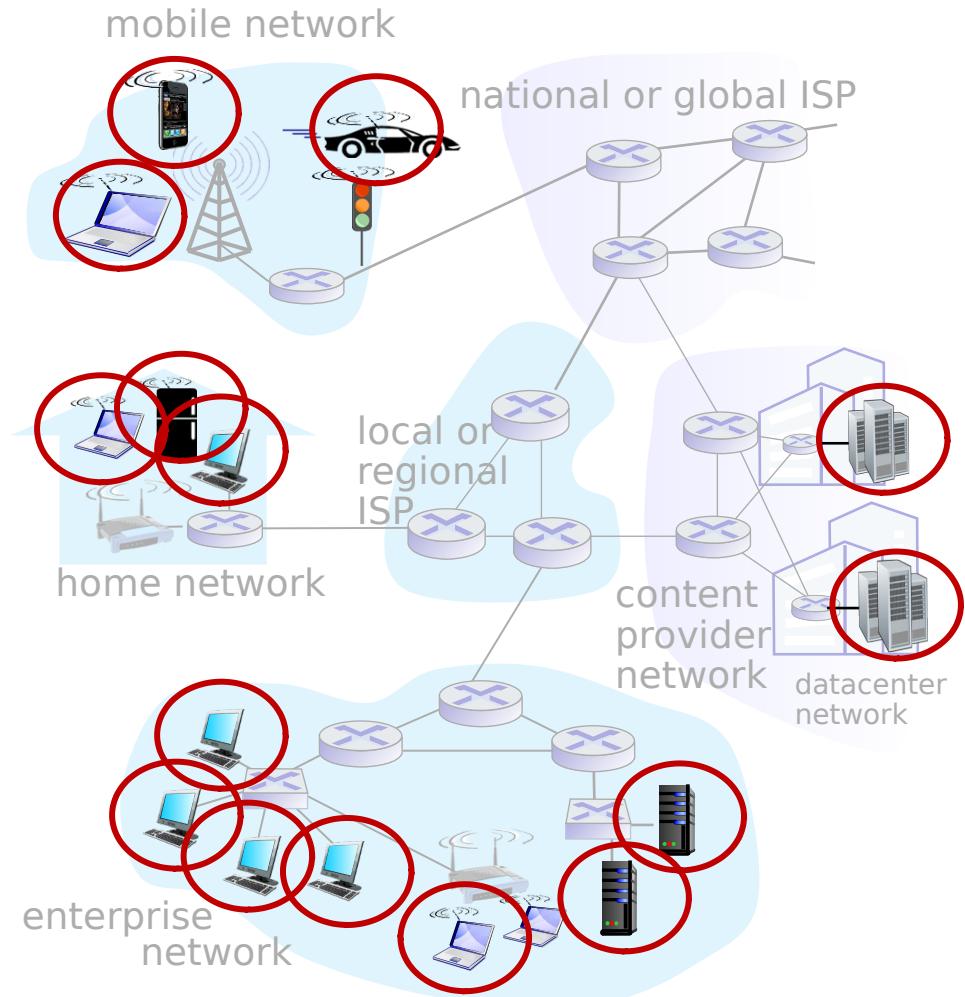
Sumário

- O que é a Internet? O que é um protocolo?
- **Borda da rede: hosts, acesso, meios físicos**
- Core da rede: comutação de circuitos e de pacotes; estrutura da Internet
- Questões de performance: perda, atraso, desempenho
- Segurança
- Camadas de protocolos, modelos de serviço
- História

Estrutura da Internet

Borda da rede

- **Hosts**: clientes e servidores : **sistemas finais**
- Servidores geralmente em centro de dados (cloud computing)



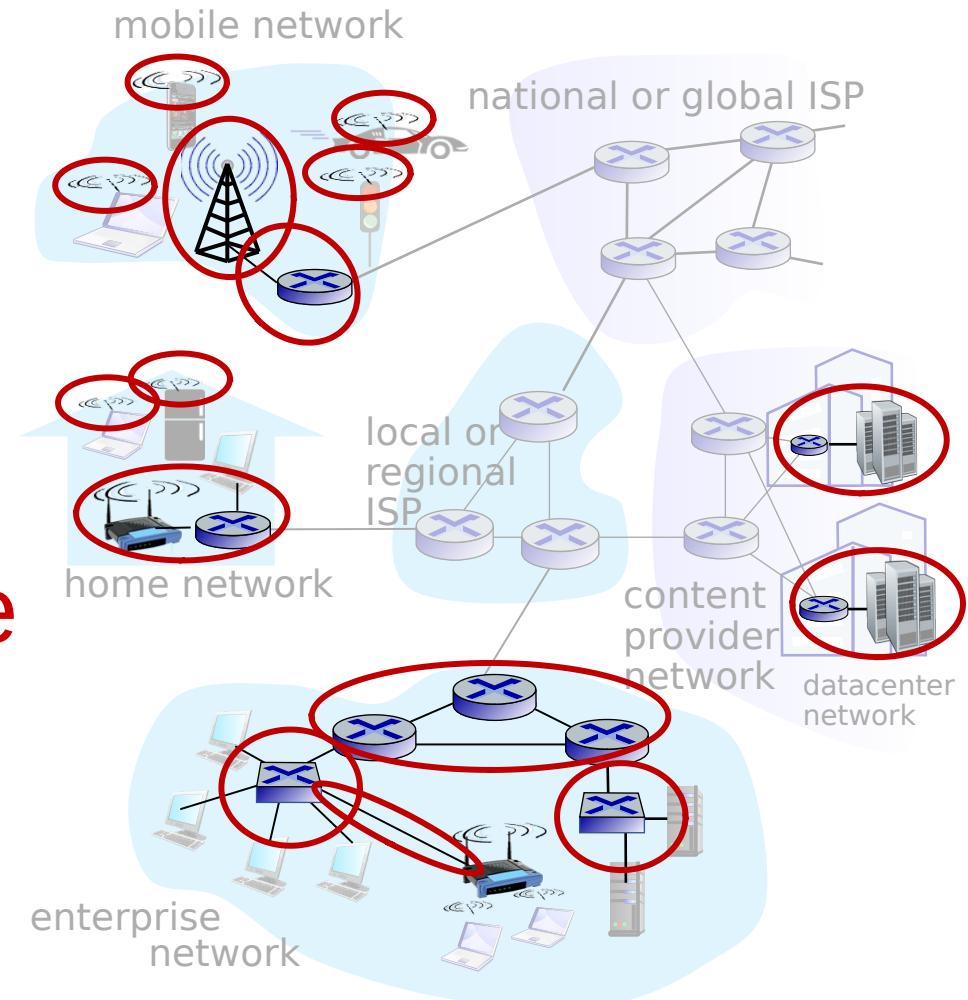
Estrutura da Internet

Borda da rede

- Hosts: clientes e servidores : sistemas finais
- Servidores geralmente em centro de dados (cloud computing)

Meios físicos para acesso à rede

Enlaces com fio e sem fio (wireless)



Estrutura da Internet

Borda da rede

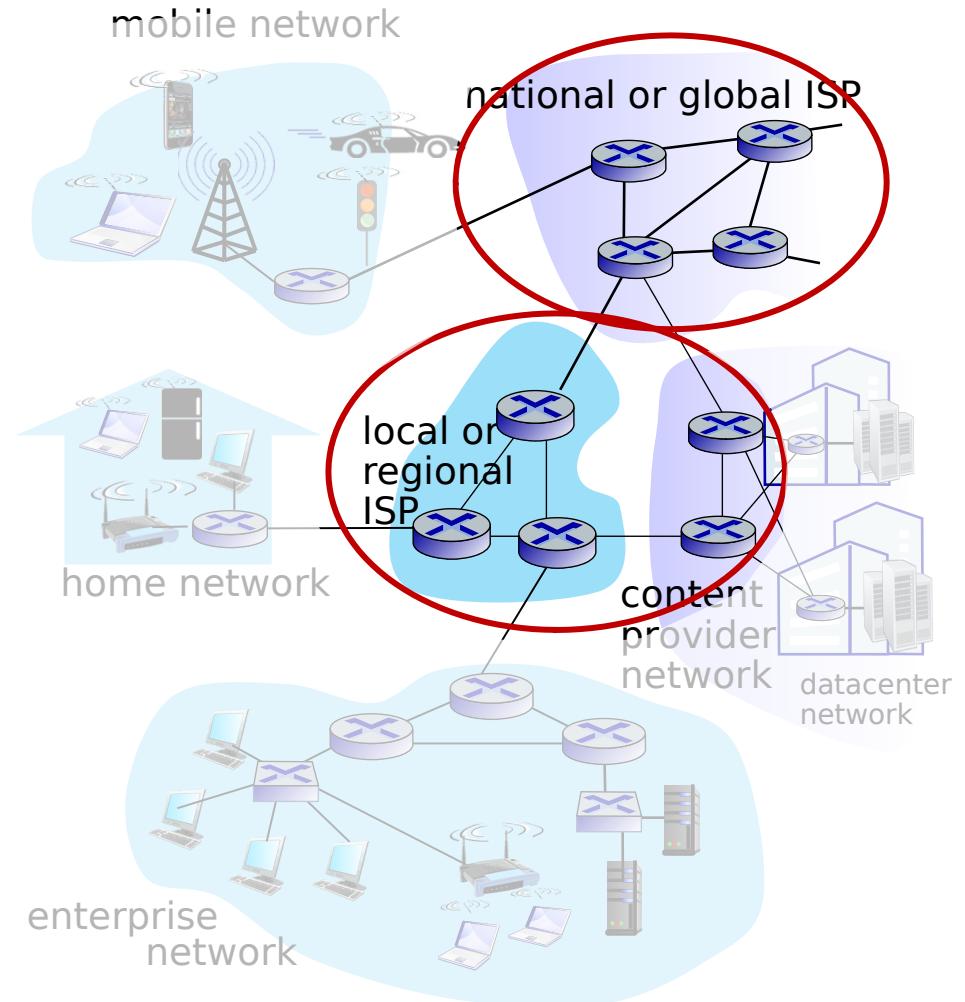
- Hosts: clientes e servidores : sistemas finais
- Servidores geralmente em centro de dados (cloud computing)

Meios físicos para acesso à rede

Enlaces com fio e sem fio (wireless)

Núcleo (core) da rede

- Interconexão de roteadores
- Rede de redes



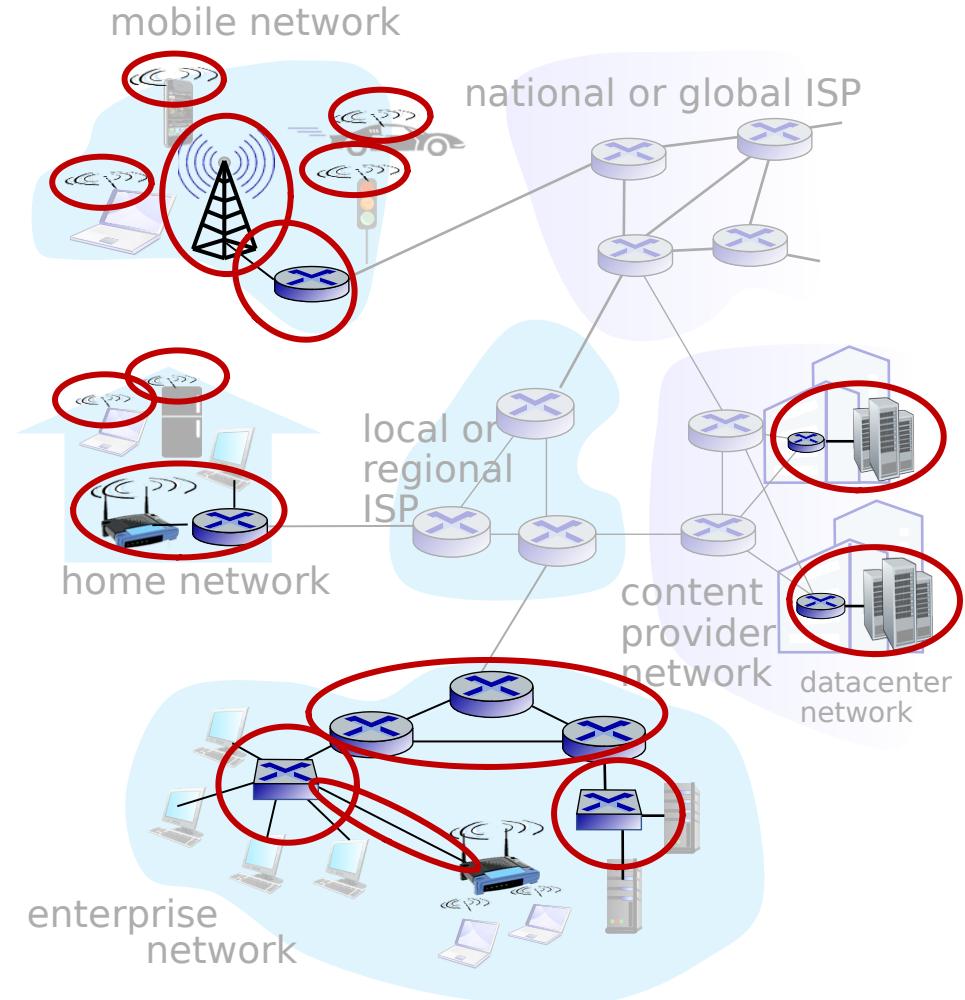
Redes de acesso e meios de conexão

Q: Como conectar sistemas finais aos roteadores do core?

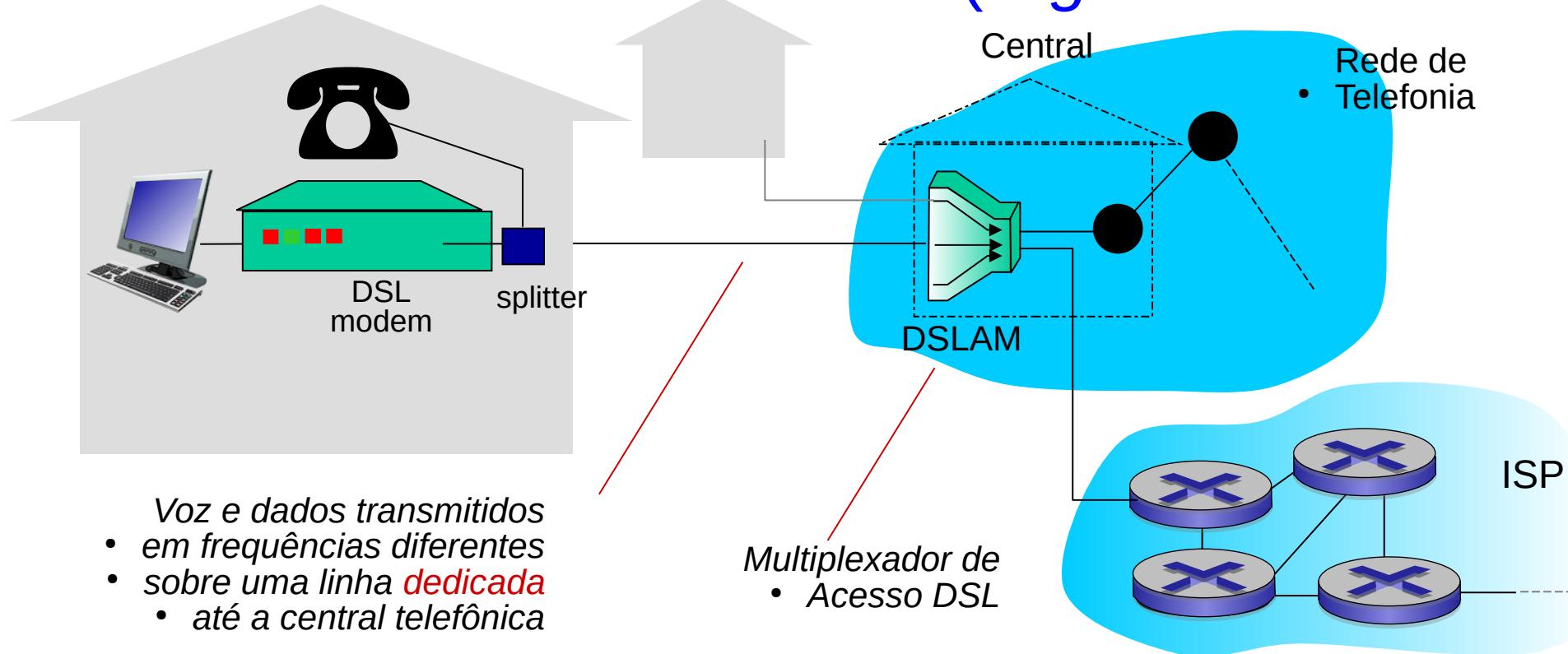
- Redes de acesso residenciais
- Redes de acesso institucionais (escolas, empresas)
- Redes de acesso móveis (WiFi, 4G/5G)

Observações:

- Qual a **banda de rede** (bits por segundo) do acesso
- O meio é **compartilhado ou dedicado**



Redes de acesso: linhas DSL (*Digital Subscriber Line*)



Usa as linhas de telefonia convencional pré-existentes entre as dependências do usuário e a central DSLAM

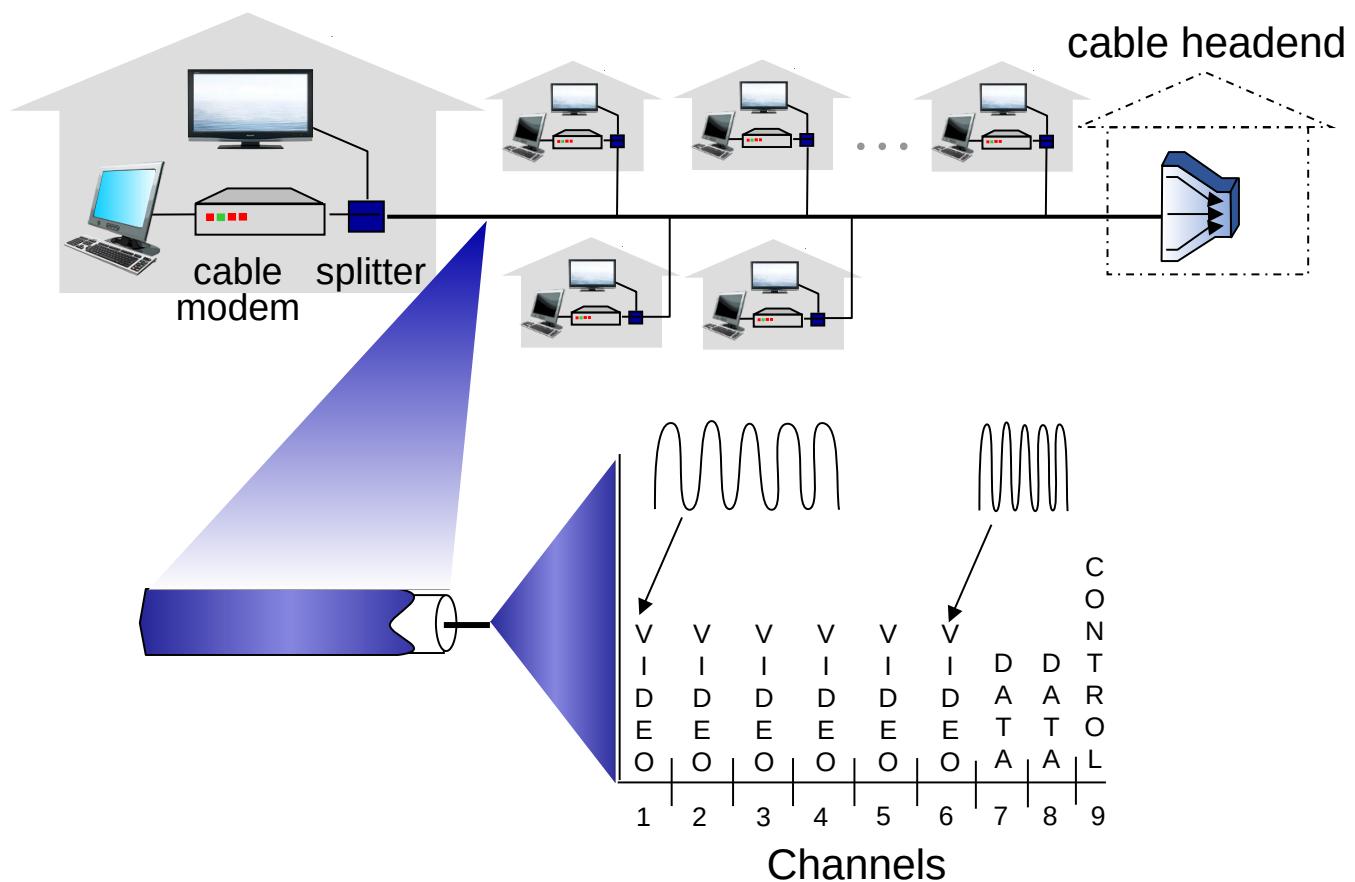
- **Dados** sobre a linha DSL vai para Internet

- **Voz convencional** sobre a linha DSL vai para a rede de telefonia

Razões de transmissão:

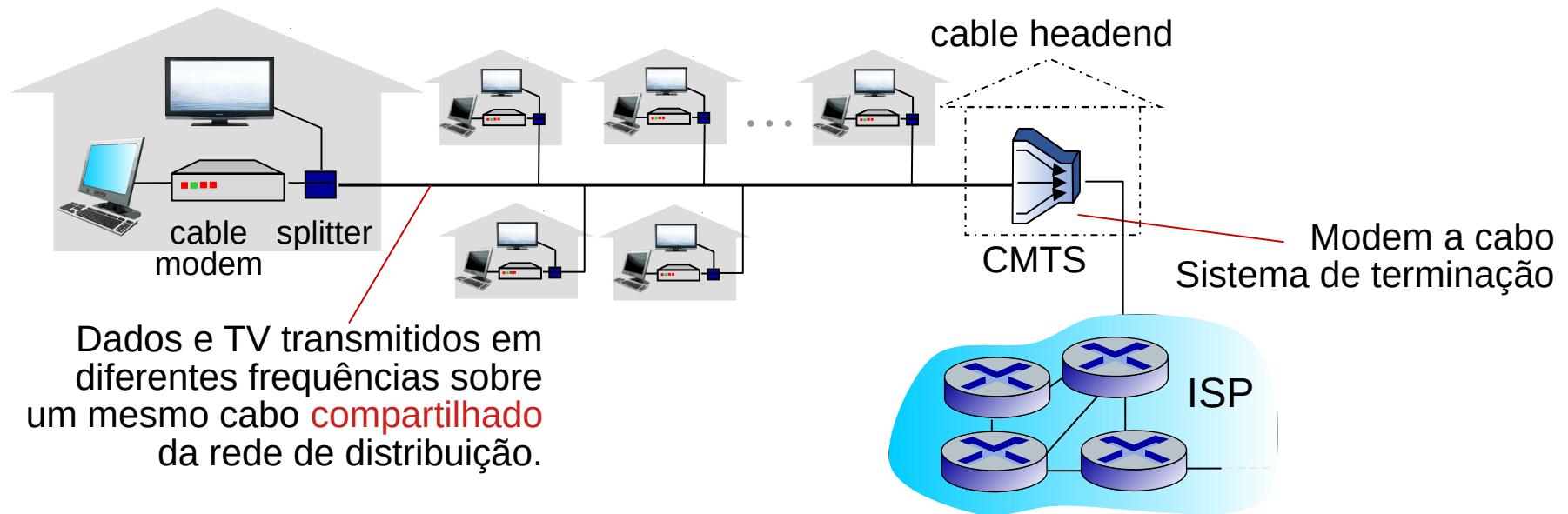
- Upstream < 2.5 Mbps (geralmente < 1 Mbps)
- Downstream < 24 Mbps downstream (tipicamente < 10 Mbps)

Redes de acesso e meios de conexão



Multiplexação por divisão de frequência (FDM – *Frequency Division Multiplexing*)
Diferentes canais transmitidos em diferentes bandas de frequência

Redes de acesso: acesso baseado em cabos



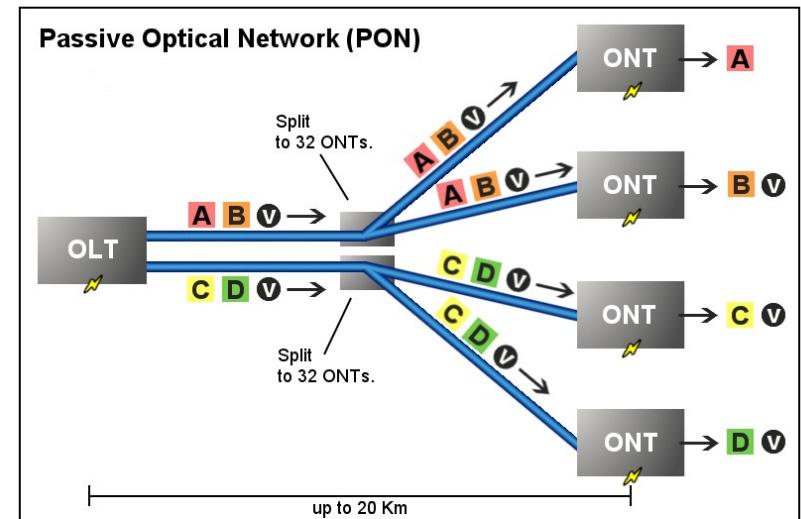
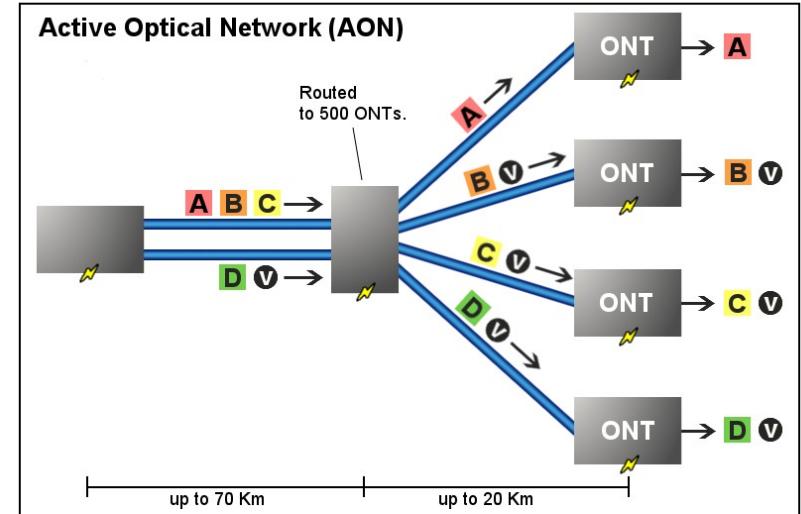
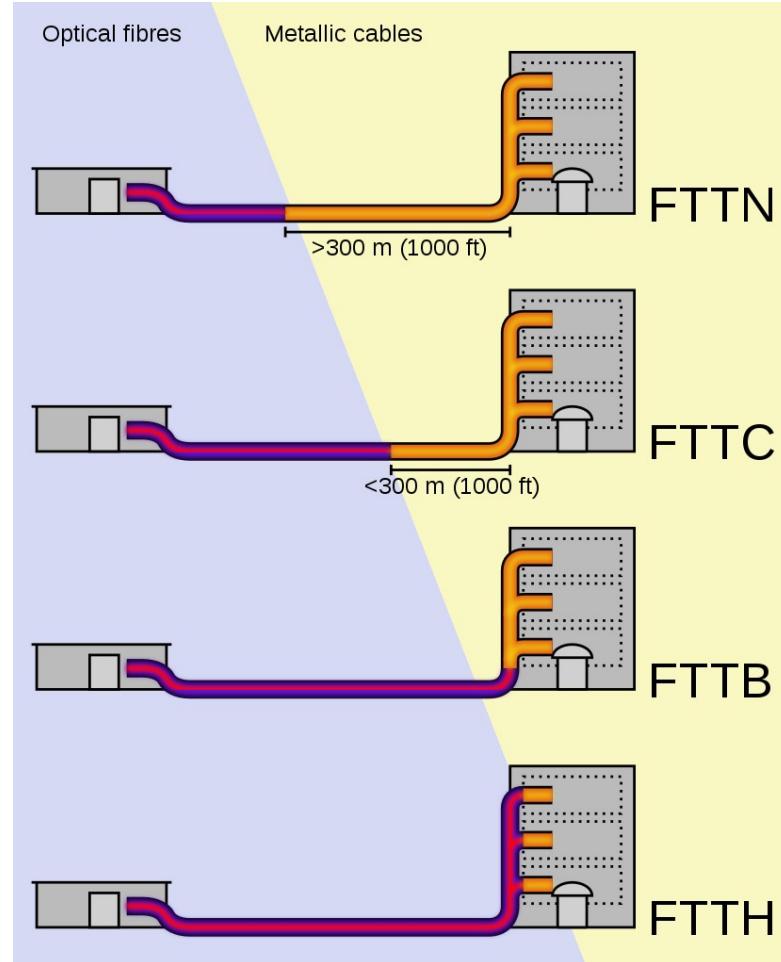
- **HFC (*Hybrid Fiber Coax*)**
 - Assimétrico: 40 Mbps – 1,2 Gbps (razão de transmissão *downstream*) 30-100 Mbps (razão de transmissão *upstream*)
- Rede de cabos, fibra conecta casas/escritórios ao roteador ISP
- **Compartilhamento da rede de acesso (*cable headend*)**

Redes de acesso: acesso baseado em cabos (fibra)

FFTX (*Fiber to the x*)

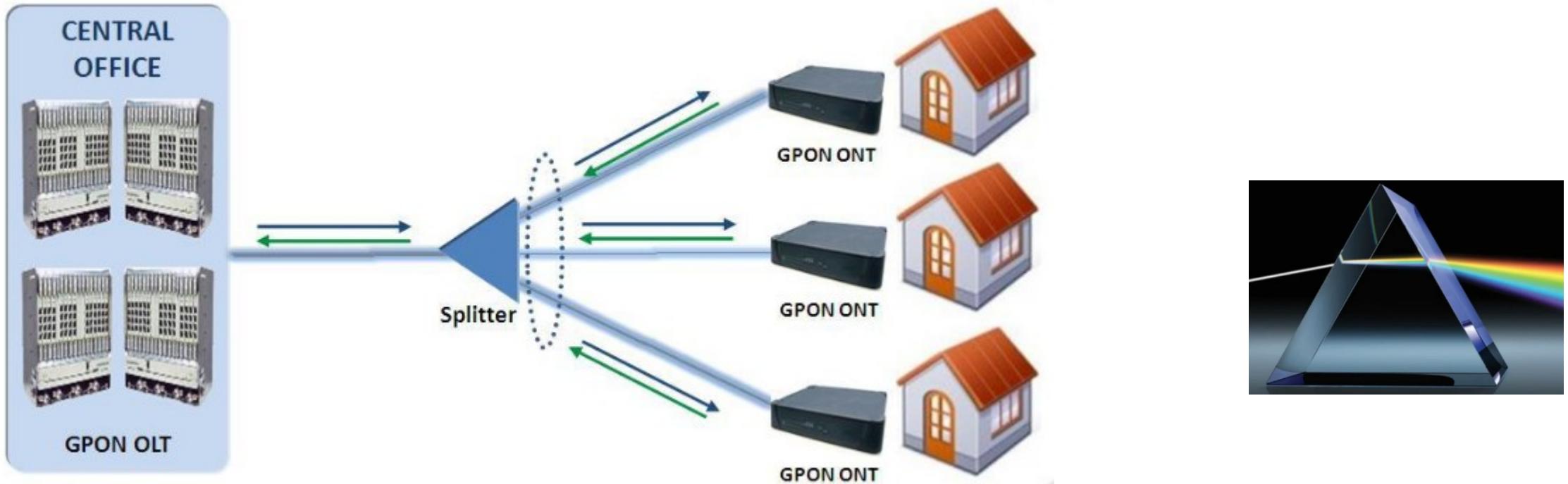
GPON (*Gigabit Passive Optical Network*)

EPON (*Ethernet PON*)



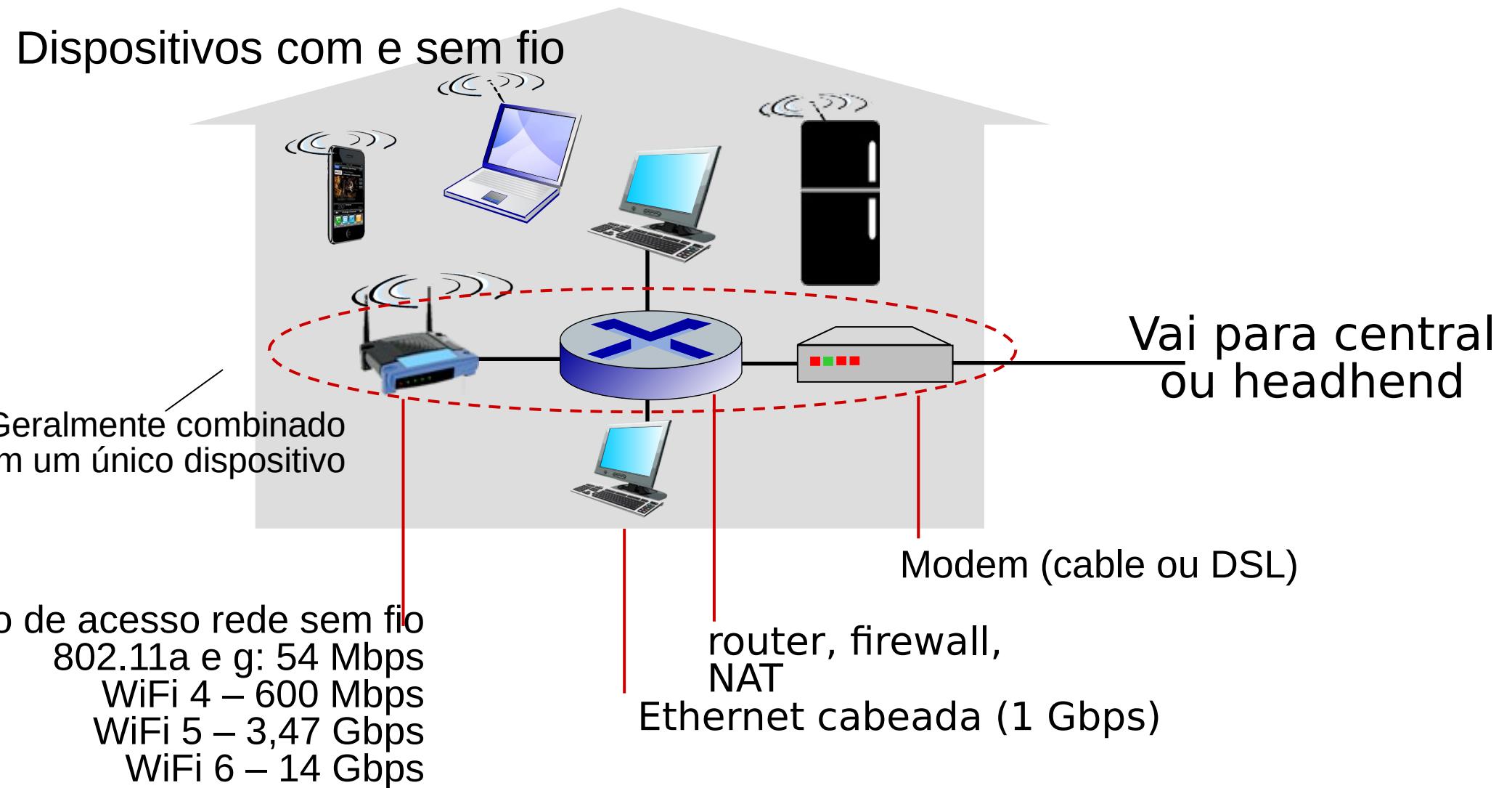
Key: **A** - Data or voice for a single customer. **V** - Video for multiple customers.

Redes de acesso: acesso baseado em cabos (fibra)



Backbone: Terminal de Linha Óptica (*Optical Line Terminal* – OLT)
Cliente: Terminais de Rede Óptica (*Optical Network Terminal* – ONT)
ou ONU (*Optical Network Unit*)
Cliente - CPE (*Customer-Premises Equipment*)

Redes de acesso: rede doméstica



Redes de acesso de acesso sem fio

Redes de acesso sem fio **compartilhado** entre os sistemas finais até o roteador (através de uma estação conhecida como “access point”)

LANs sem fio

- Dentro edificações (70m 802.11n)
- 802.11b/g/n/ac/ad (WiFi): 11, 54, 450 Mbps

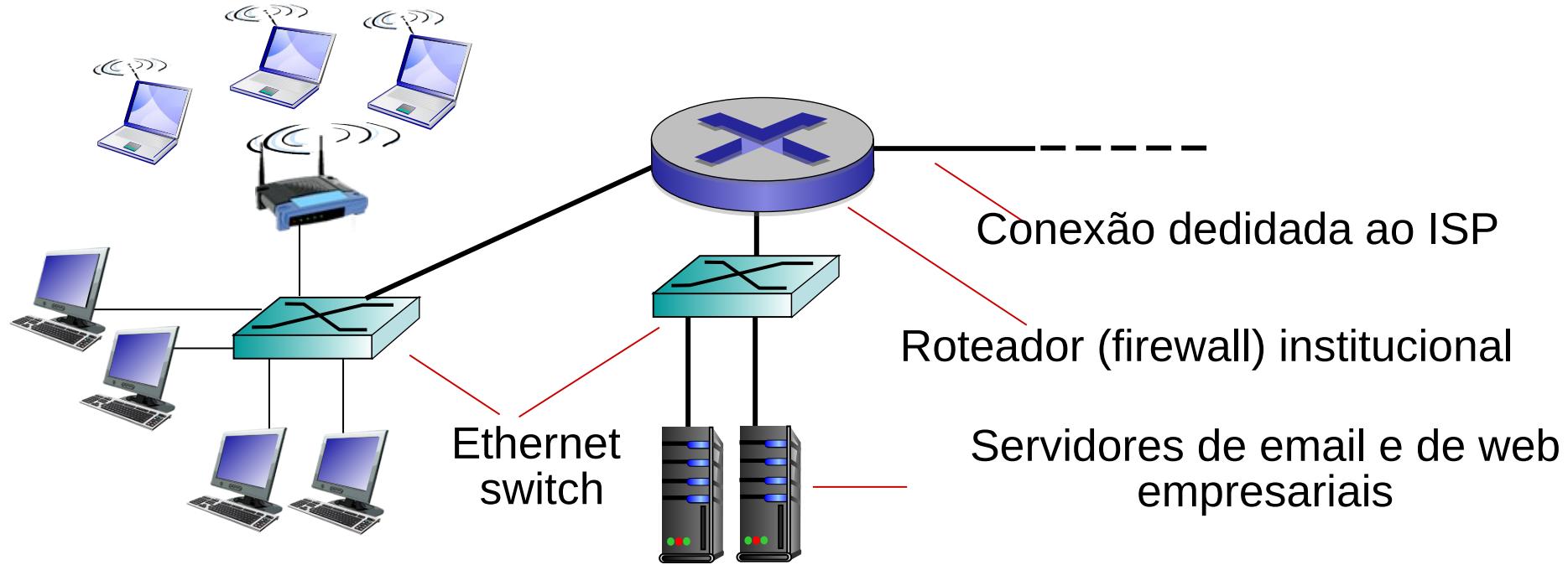


Redes celulares de acesso (wide-area)

- Provido pelas operadoras telco (celular), 10 km
- 10 Mbps
- 3G, 4G: LTE, 5G



Redes empresariais (Ethernet)



Tipicamente usado em companhias, universidades, órgãos, etc.
Meios físicos cabeados e sem fio, usando roteadores e switches:
Ethernet: 100Mbps, 1Gbps, 10Gbps
WiFi: pontos de acesso para mobilidade: 11, 54, 450 Mbps

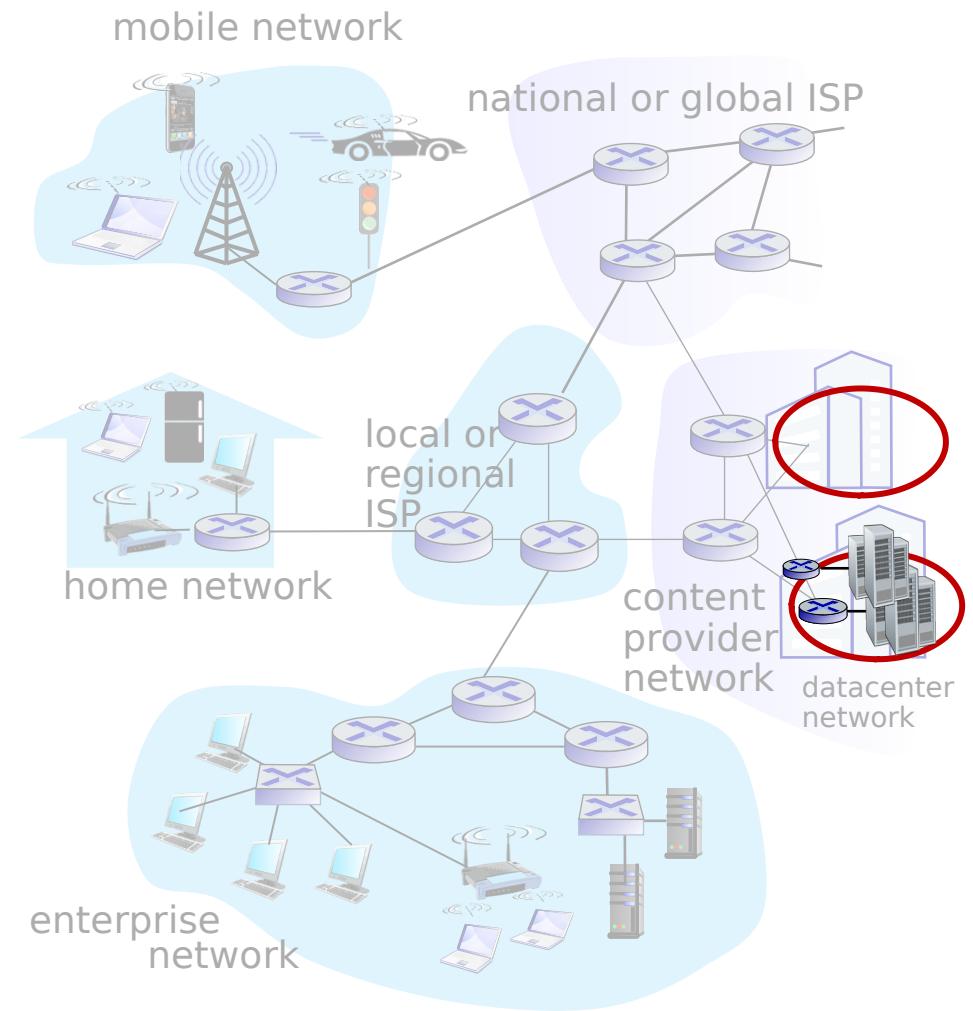
Redes de acesso: redes de centros de dados

Usa enlaces de alta largura de banda
(10 a 100 Gbps)



Courtesy: Massachusetts Green High Performance Computing Center (mghpcc.org)

<https://www.google.com/about/datacenters/>



Engenharia de Confiabilidade do Google: Como o Google administra seus sistemas de produção – SRE (Site Reliability Engineering) (BEYER et al, 2016)

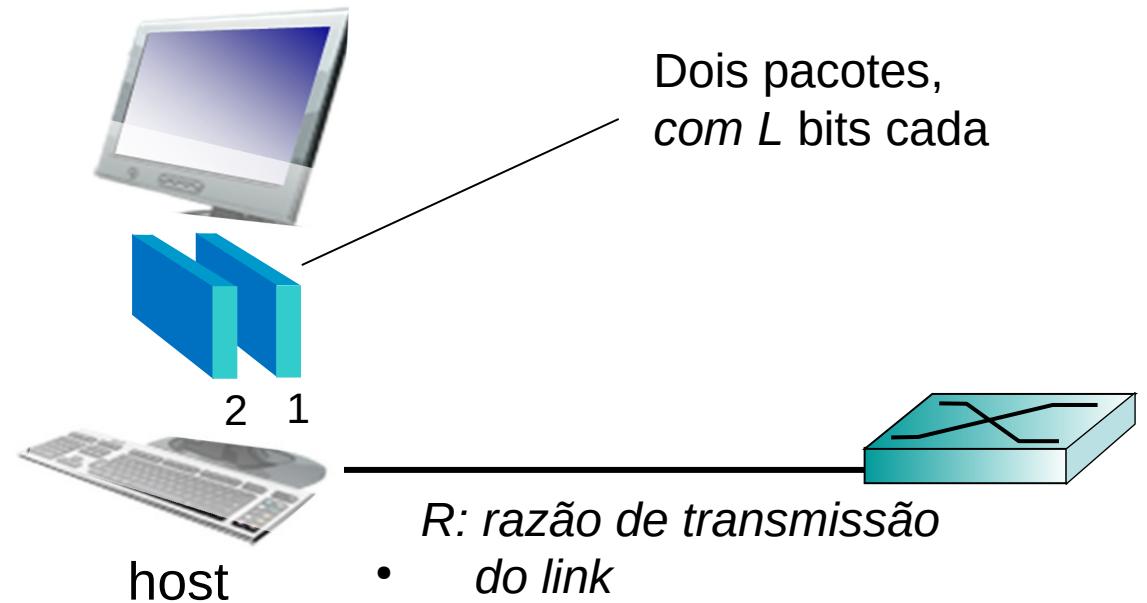
Host: envio de pacotes de dados para a rede

Função de envio de dados pelo host

- Recebe a mensagem da aplicação
- Quebra em “pedaços” menores (*chunks*) conhecidos como *pacotes*, de tamanho L bits
- Transmite pacotes para dentro da rede com uma *taxa de transmissão*

R

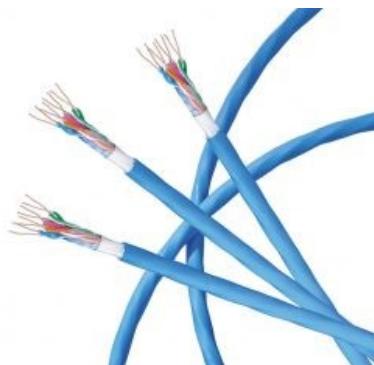
- O enlace transmite à razão conhecida como *capacidade do link, ou largura de banda (bandwidth)*



$$\text{Delay transmissão pacote} = \frac{\text{Tempo necessário para transmitir pacotes de tamanho } L\text{-bit para dentro do enlace}}{R \text{ (bits/s)}}$$

Enlaces físicos (mídia de conexão)

- **bit**: propaga-se entre pares de transmissores e receptores
 - **Enlace físico**: é o meio interliga o transmissor e receptor
 - **Meio guiado**:
 - Sinais são propagados em meios sólidos: cobre, fibra, coaxial
 - **Meios não guiados**:
 - Sinais propagam livremente: ondas de rádio
- Par trançado (TP): UTP, S/FTP*
- Dois fios de cobre isolados (trançados): quatro pares
 - Cat 5e: 10/100/1000BASE-T, 1 Gbps Ethernet
 - Cat 6 e 6a: 10GBASE-T: Ethernet 10Gbps
 - Cat 7: 10Gbps (8P8C) 7a (TERA ou GG45)
 - Cat 8: em estudos



Meios físicos: **cabo coaxial**

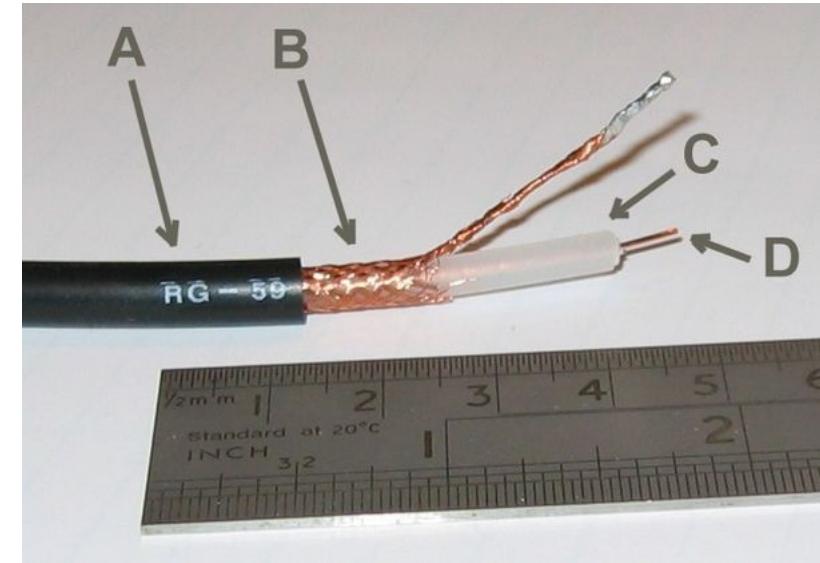
Dois condutores
concêntricos
Bidirecional

Broadband (banda larga):

Vários canais (múltiplas
frequências) no cabo

HFC (*Hybrid fiber-coaxial*)

Televisão a cabo



Meios físicos: fibra óptica

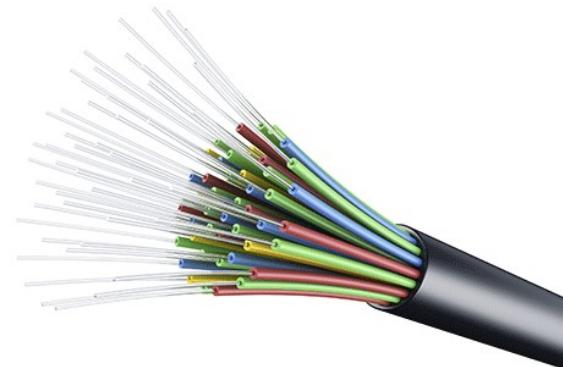
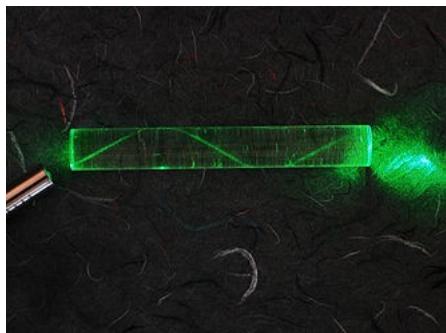
Fibra de vidro ou plástico transportando pulsos de luz (cada pulso um bit)

Reflexão interna devido refração (diferentes materiais)

Alta velocidade de operação: transmissão ponto-a-ponto de alta velocidade (10-100 Gbps)

Baixa taxa de erro devido à imunidade às interferências eletromagnéticas.

Consequências: uso de cabeamento óptico para grandes distâncias e uso de repetidores largamente espaçados.



Conectores.
Dois cabos que
Permitem comunicação
Full-duplex.

Enlaces físicos

Sem fio via rádio

- Sinal transportado pelo espectro eletromagnético
- Não há fios
- Bidirecional
- Broadcast, “half-duplex”
- Efeitos da propagação no ambiente:
 - Reflexão
 - Obstrução
 - Interferência

Tipos de enlaces de rádio

- Microondas terrestres
 - Enlaces ponto-a-ponto; suportam canais até 45 Mbps
- LAN (WiFi)
 - 54 Mbps, 150 Mbps (802.11n), 866,7 Mbps (802.ac) – banda **ISM**
- Redes *wide-area* (celular)
 - 4G cellular: ~ 10 Mbps, 100 Mbps a 1 Gbps
- Satélite
 - Canais: Kbps até 45Mbps
 - Delay fim a fim: 270 ms
 - Órbitas geossíncronas versus baixa altitude
- Bluetooth
 - Substituição de cabos para curtas distâncias

Sumário

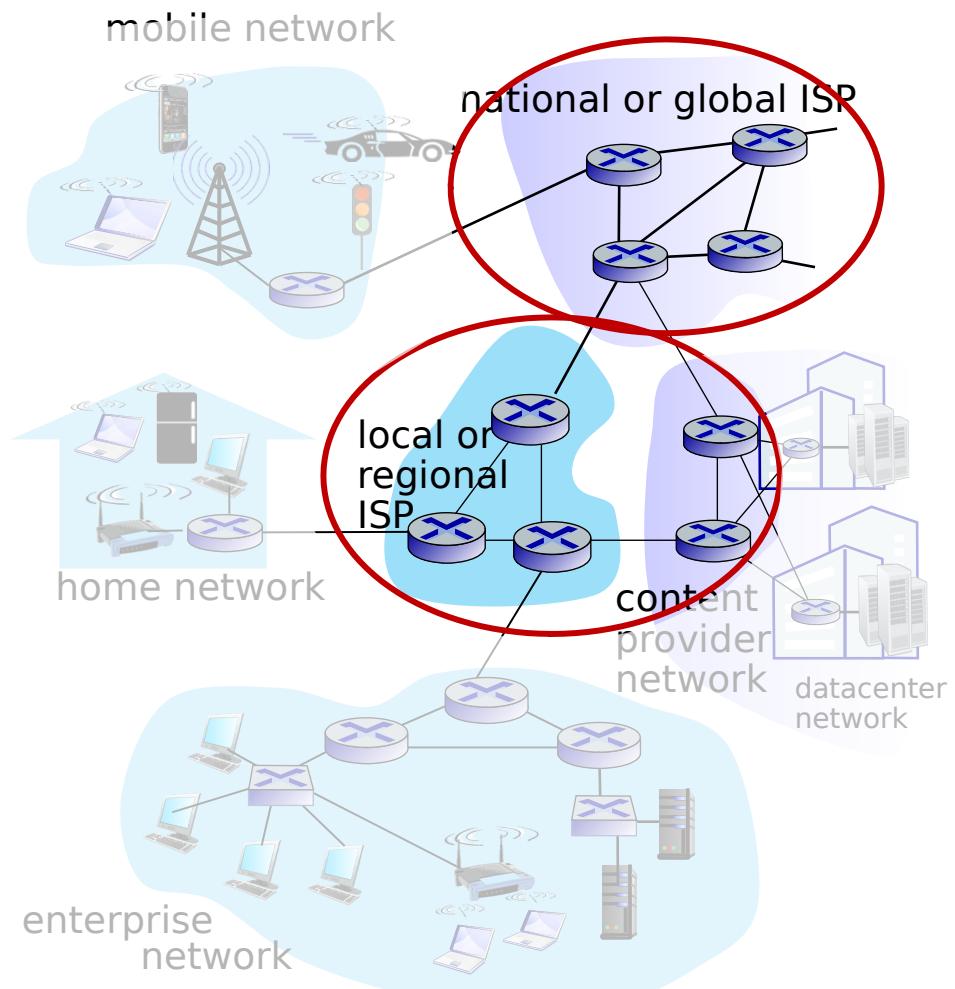
- O que é a Internet? O que é um protocolo?
- Borda da rede: hosts, acesso, meios físicos
- Núcleo da rede: comutação de circuitos e de pacotes; estrutura da Internet
- Questões de performance: perda, atraso, desempenho
- Segurança
- Camadas de protocolos, modelos de serviço
- História

O núcleo (core) da Internet

Malhas (*mesh*) de roteadores interconectados

Chaveamento de pacotes (*packet-switching*): hosts quebram as mensagens da camada de aplicação em pacotes (*packets*)

Rede encaminha (*forwards*) pacotes de um roteador para o próximo através dos enlaces no caminho da origem para o destino (usando a capacidade máxima de transferência do link)

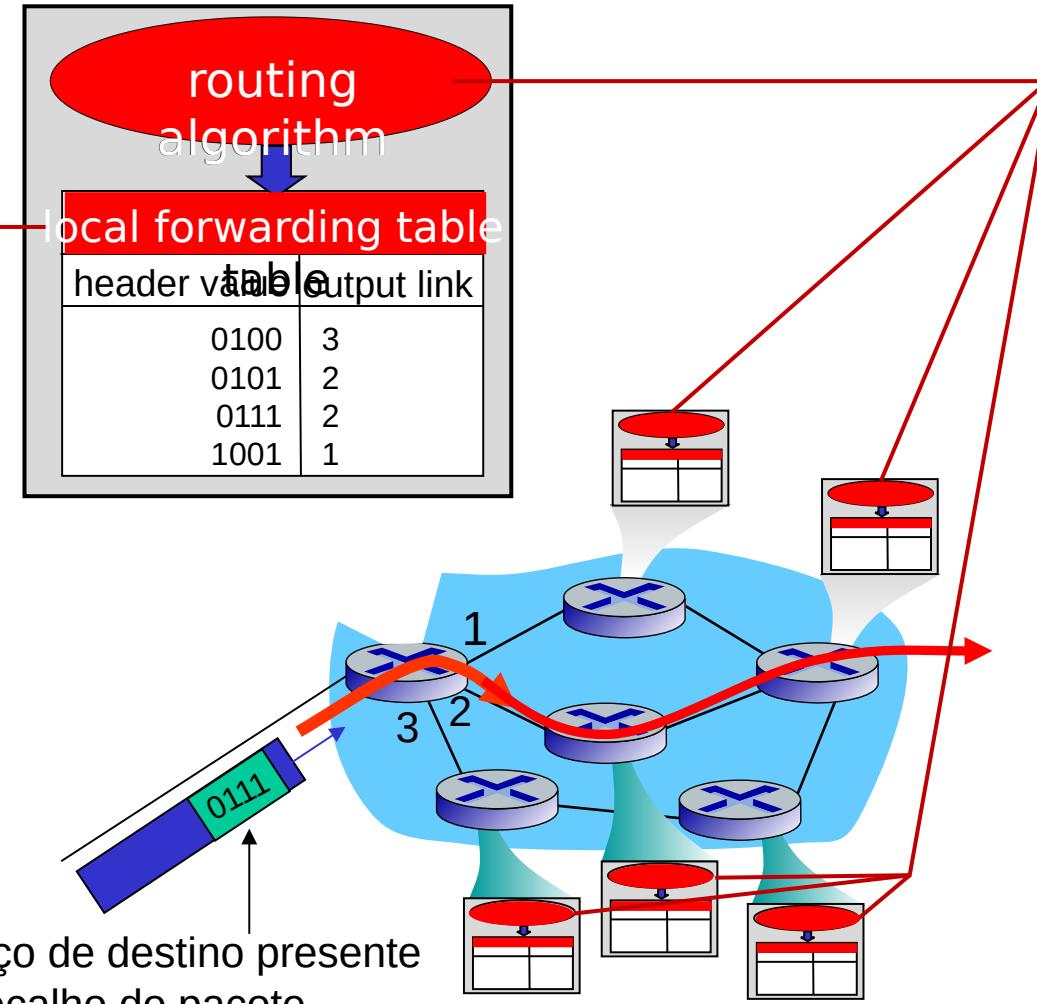


Duas funções principais do núcleo

Encaminhamento

(*forwarding*):

- Também conhecido como “switching”
- **Ação local:** mover pacotes que chegam do enlace de entrada para a apropriada porta de saída do roteador (enlace de saída)



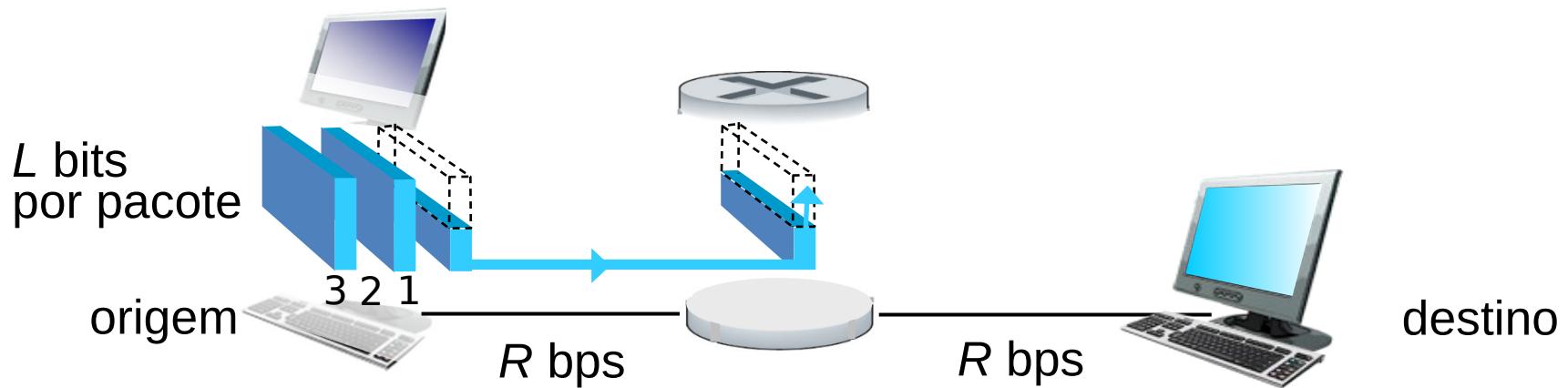
Roteamento

- **Ação global:** determina caminhos origem-destino que os pacotes devem seguir
- Algoritmos de roteamento (RIP, BGP, OSPF, ...)





Chaveamento de pacotes (packet-switching): **store-and-forward**



Atraso transmissão pacotes: leva L/R s para transmitir um pacote de tamanho L -bits em um enlace de R bps (taxa)

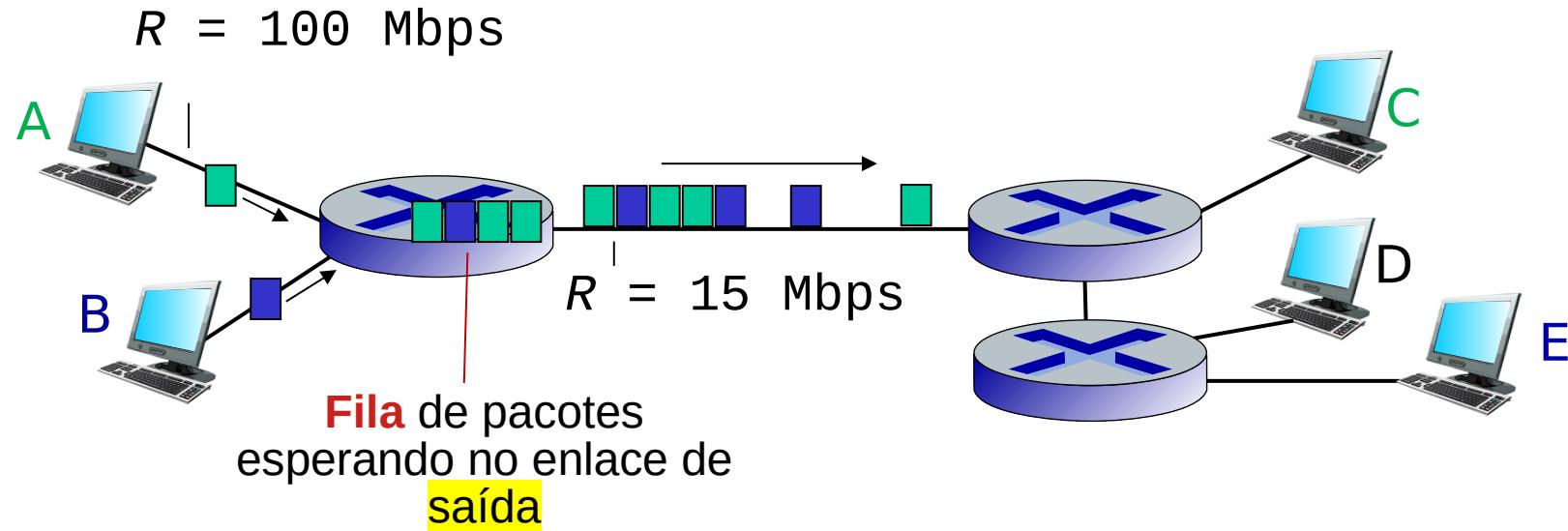
Armazena e encaminha (store and forward): o pacote inteiro precisa chegar no roteador antes de ser encaminhado para o próximo

Exemplo para um hop:

- $L = 10$ Kbits
- $R = 100$ Mbps
- Atraso de transmissão para um hop = 0,1 ms

Delay (atraso) fim a fim = $2L/R$ (sem atrasos na propagação)

Chaveamento de pacotes (packet-switching): filas (*queueing*)



Enfileiramento e perda:

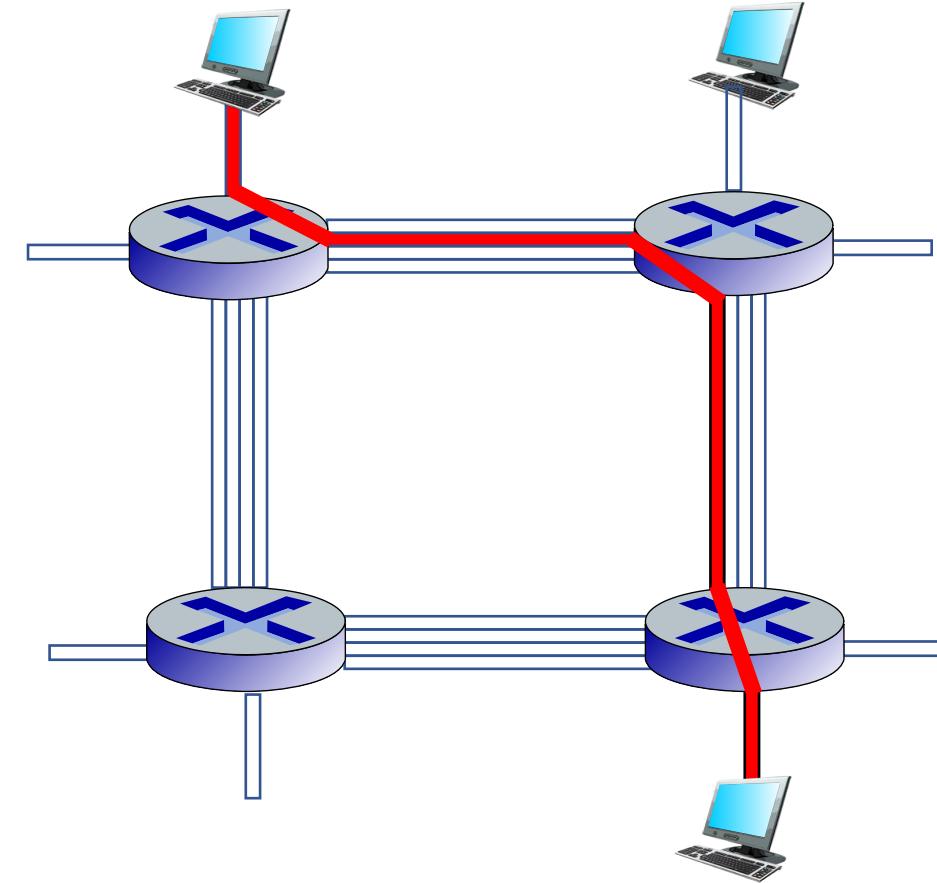
Se a razão (em bits/s = bps) de chegada no enlace excede a capacidade (razão em bps) de transmissão por um período de tempo:

- Pacotes serão **enfileirados**, esperando para transmissão; e
- Pacotes podem ser **descartados** (perda) se a memória (buffer) estiver cheia

Comutação de circuitos: uma alternativa à comutação de pacotes

Recursos fim a fim alocados e reservados durante o estabelecimento do enlace de comunicação entre origem-destino:

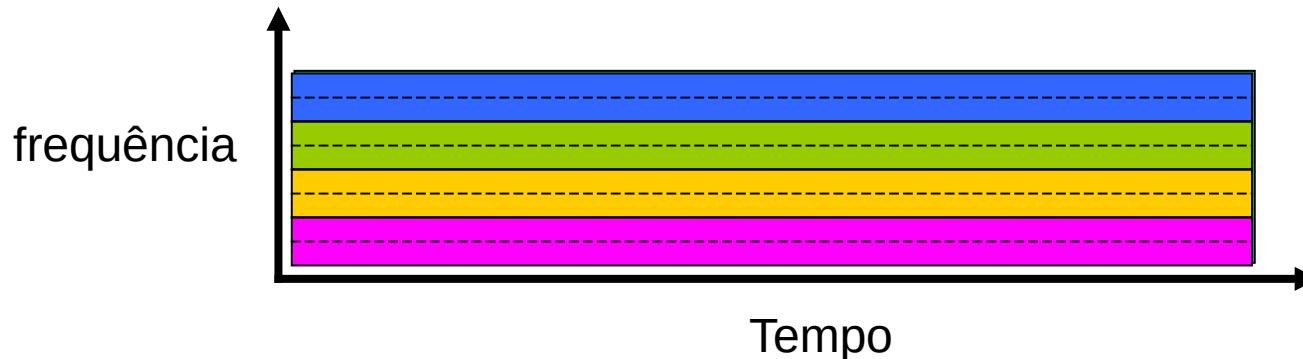
- Recursos dedicados: sem compartilhamento
- Circuito: garantia de performance
- Segmento de um circuito permanece ocioso se não usado (não é compartilhado)
- Comumente usado nas redes de telefonia tradicionais



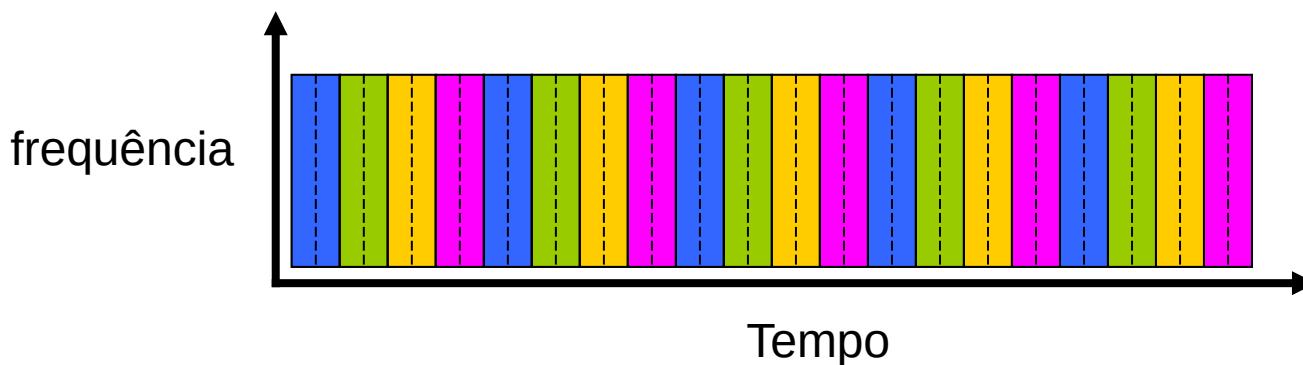
Comutação de circuitos: FDM versus TDM

FDM

Exemplo:
Quatro usuários



TDM



Comutação de circuitos: FDM versus TDM

Frequency Division Multiplexing (FDM)

Frequências ópticas e eletromagnéticas podem ser divididas em bandas de frequência estreitas. Por exemplo: nos serviços GPON/EPON uma fibra trafega sinais em downstream (1480 a 1500 nm) e sinais em upstream (1290 a 1330 nm) (tecnologia de WDM)

Time Division Multiplexing (TDM)

Tempo dividido em slots.

Uma transmissão consegue ocupar toda a banda disponível de frequência durante o seu intervalo de tempo (slot). Exemplo: nos serviços GPON as transmissões dos clientes ONU até à OLT usam TDM.

Comutação de circuitos versus comutação de pacotes

Exemplo:

Enlace: 1 Gbps (Gb/s)

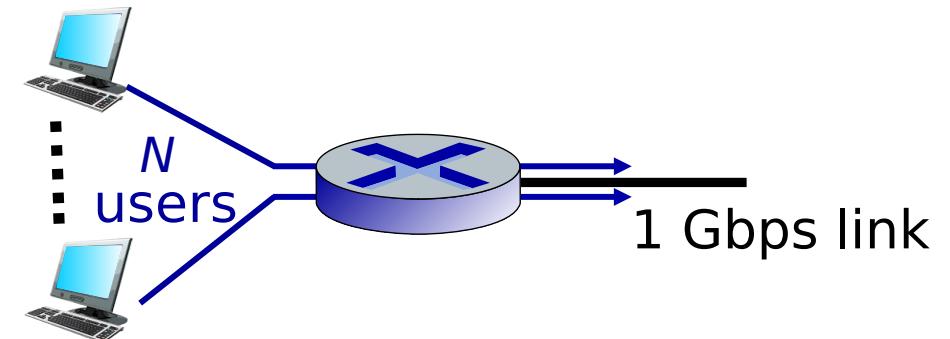
Cada usuário:

- 100 Mb/s quando “ativo”, e
- Ativo em 10% do tempo

Questão: quantos usuários podem ser suportados em cada tecnologia?

Comutação de circuitos: 10 usuários

Comutação de pacotes: com 35 usuários, probabilidade de que mais de 10 ativos ao mesmo tempo: menor que 0,0004



Logo, a rede na comutação de pacotes suporta maior quantidade de usuários

Comutação de circuitos versus comutação de pacotes

Será a comutação de pacotes a melhor?

- Boa para **dados em “rajadas”**
- **Compartilhamento de recursos**
- **Simples**, não precisa da fase de estabelecimento do canal (call setup)

Possibilidade de congestionamento excessivo: **atraso e perda**: protocolos necessitam de transferência de dados com confiança e controle de congestionamento

Q: Como prover comportamento de comutação de circuitos em uma rede por **comutação de pacotes**?

Garantia de largura de banda necessária para aplicações de áudio/vídeo (ainda não totalmente solicitedado).

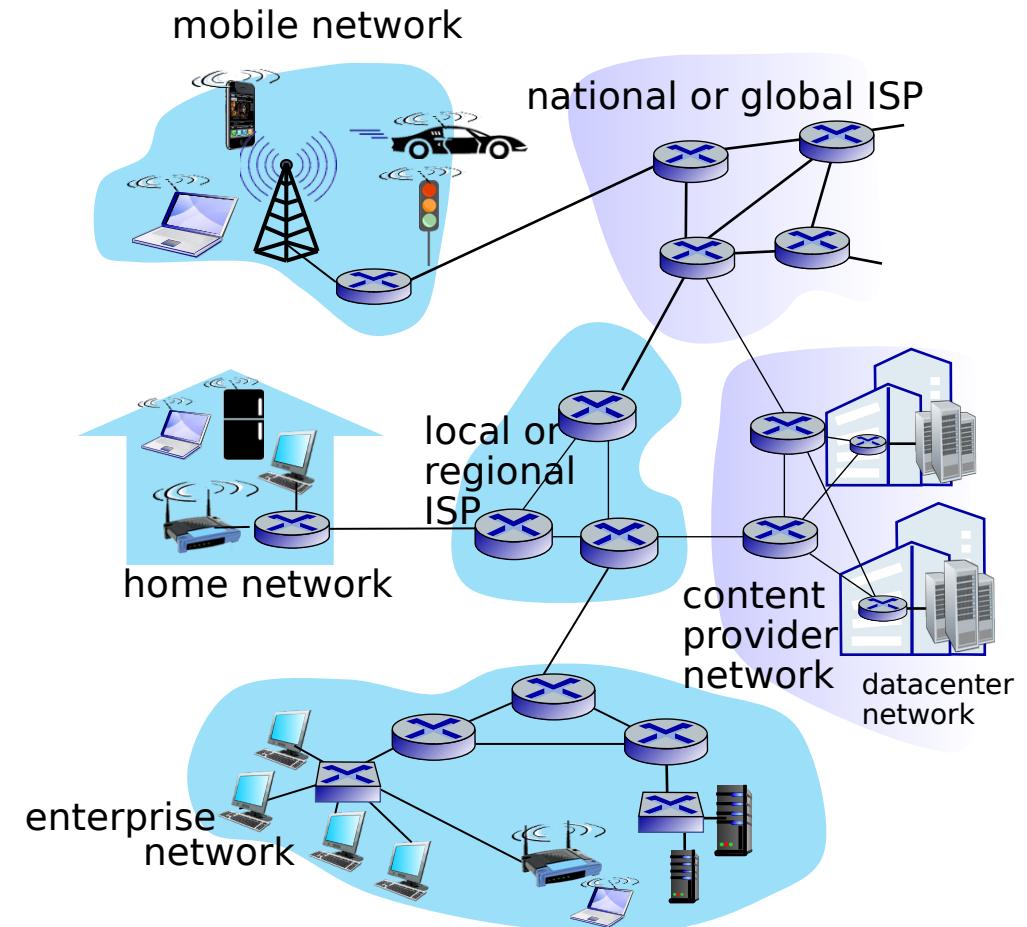
Um exemplo de protocolo que implementa circuito virtual sobre uma rede IP é o MPLS, baseado em rótulos.

Internet: “rede das redes”

Sistemas finais conectados à Internet via **acesso provido por ISPs** (Internet Service Providers): residencial, empresas e companhias

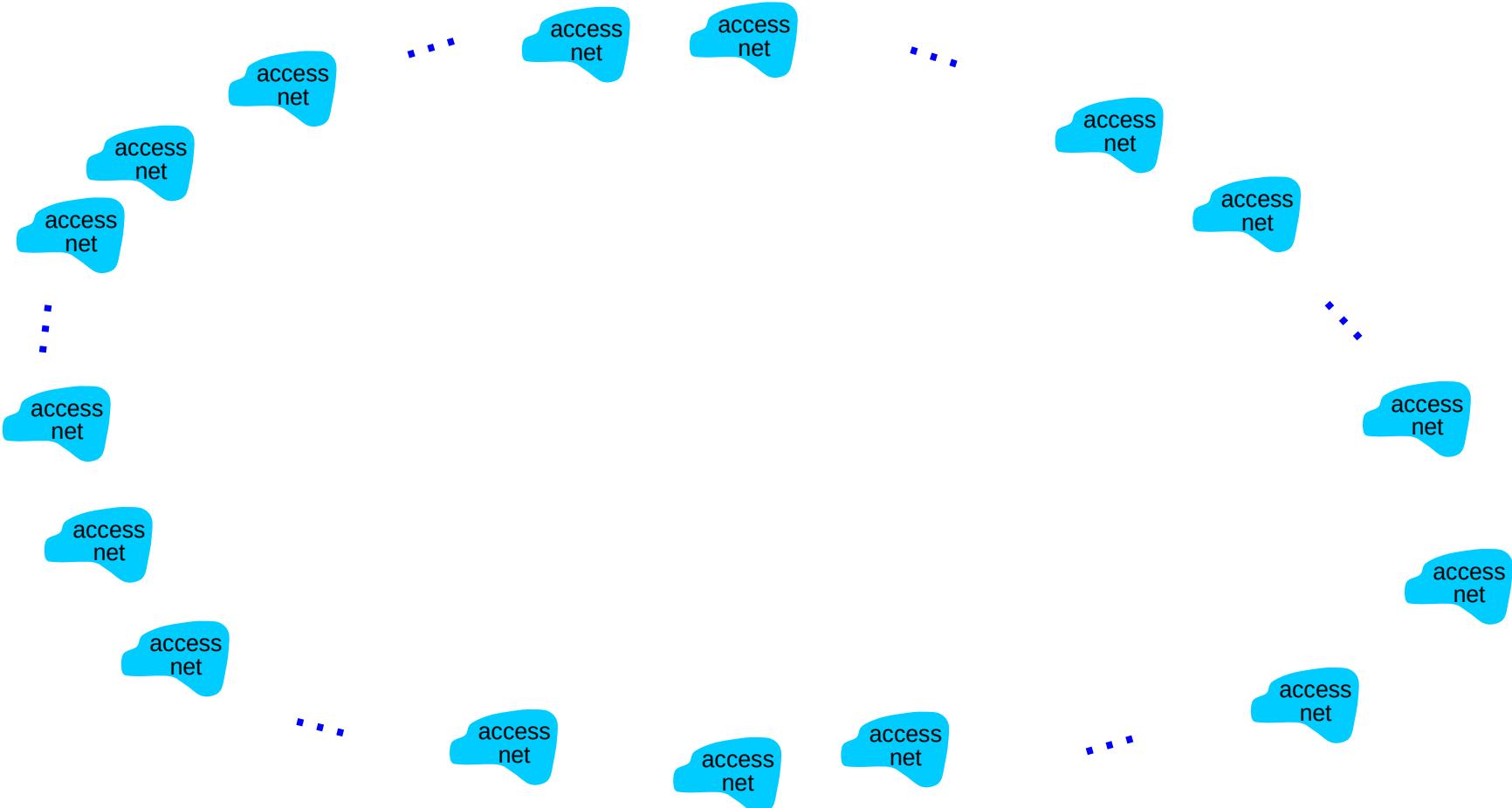
Os ISPs precisam estar interconectados

A rede das redes resultante é bastante complexa: evolução foi ditada pela **economia** e por **políticas nacionais**



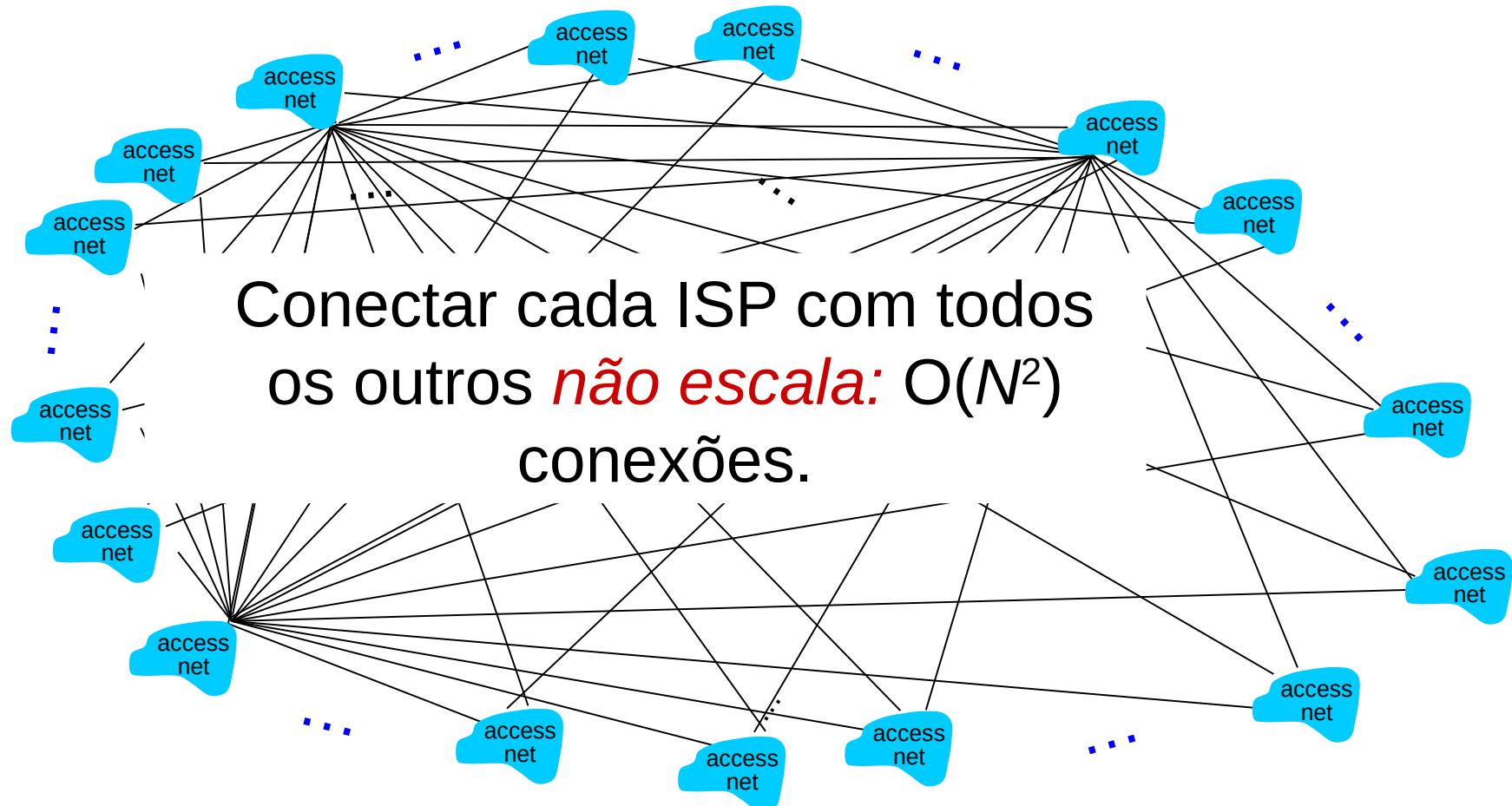
Estrutura da Internet: “rede das redes”

Questão: dado que existem muitos provedores ISP de acesso à rede, como conectar todos?



Estrutura da Internet: “rede das redes”

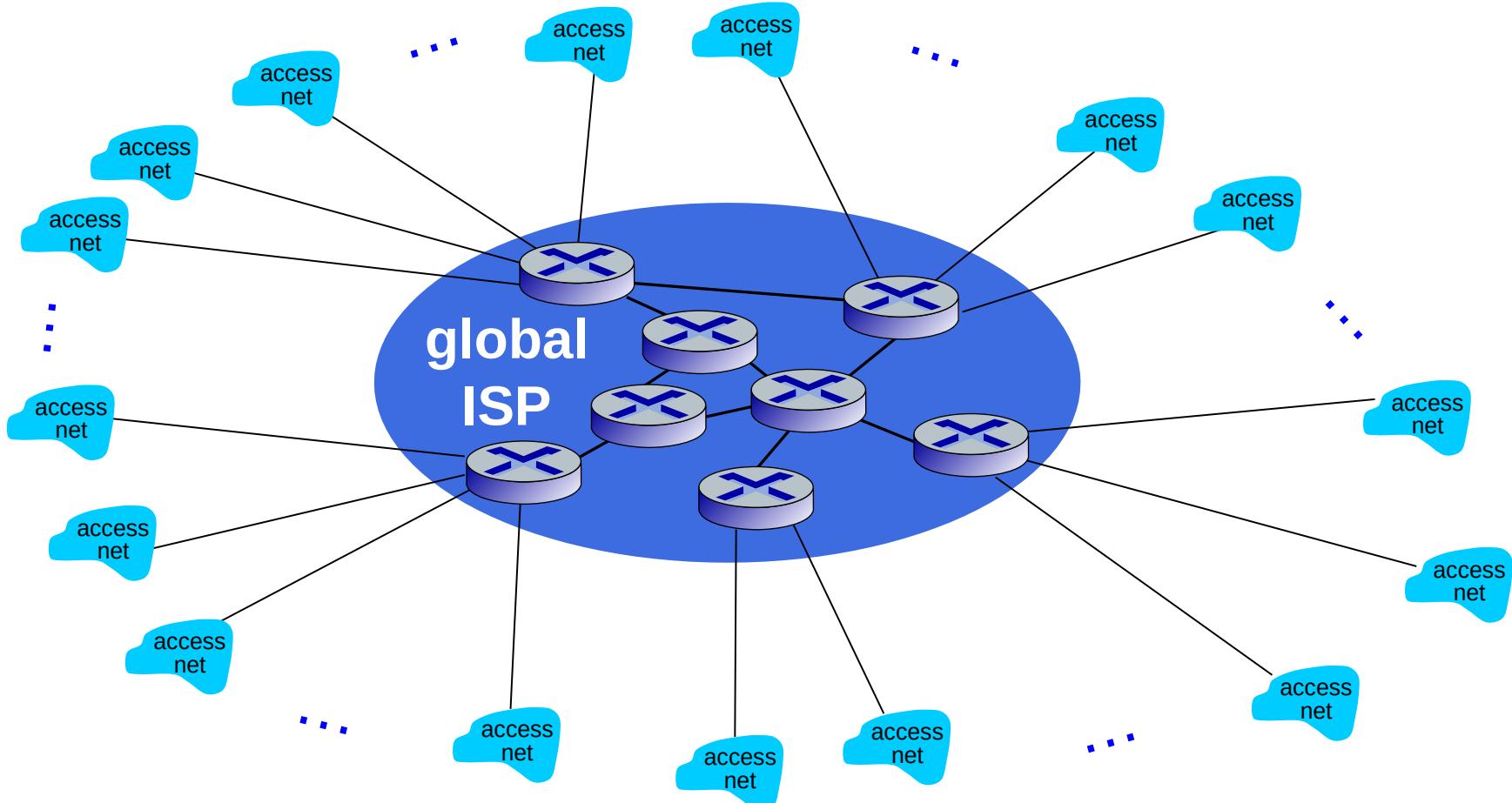
Questão: dado que existem muitos provedores ISP de acesso à rede, como conectar todos?



Estrutura da Internet: “rede das redes”

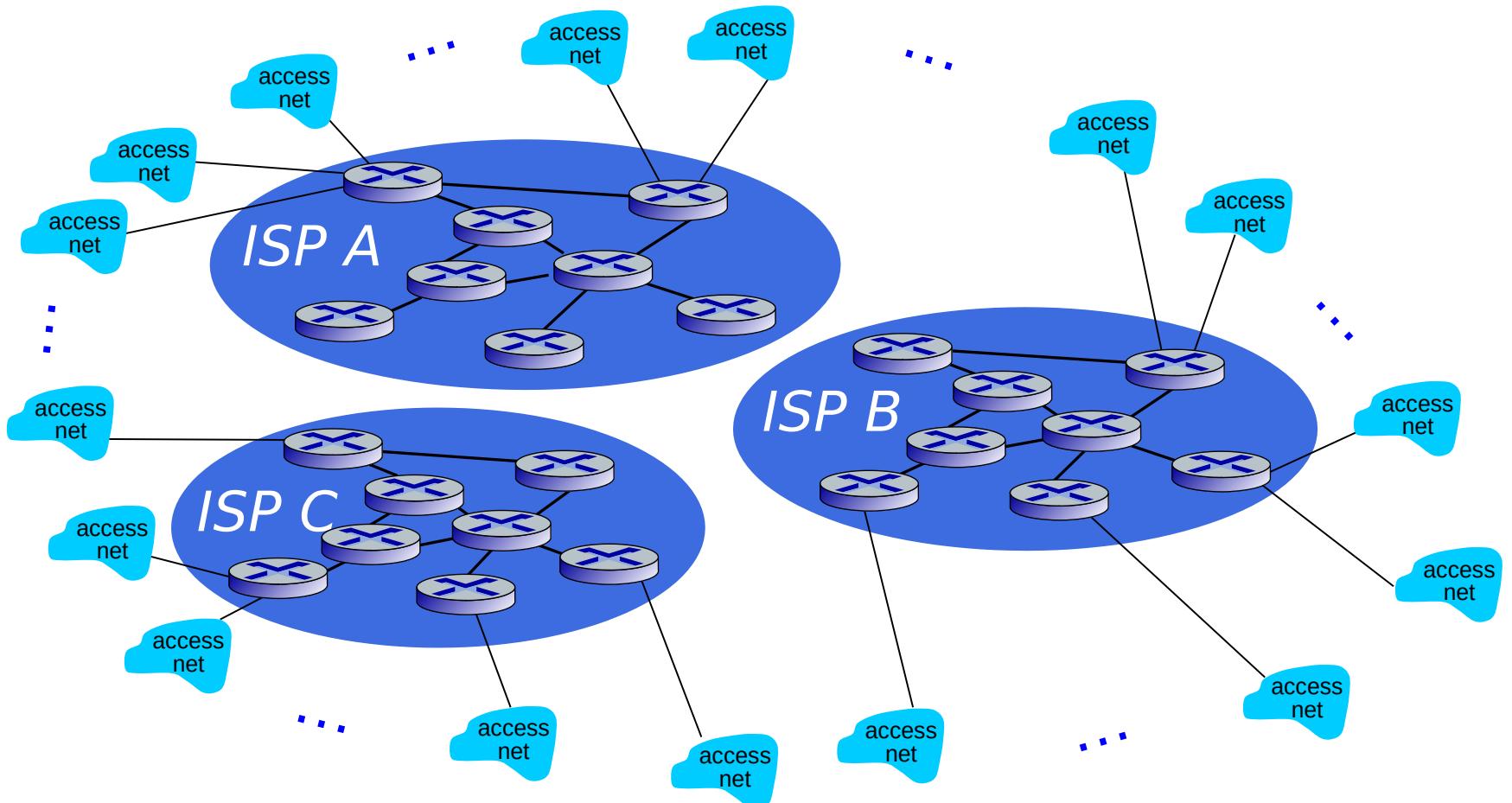
Opção: conectar cada ISP em um único ISP global?

ISP global e provedores de acesso devem possuir acordo econômico.



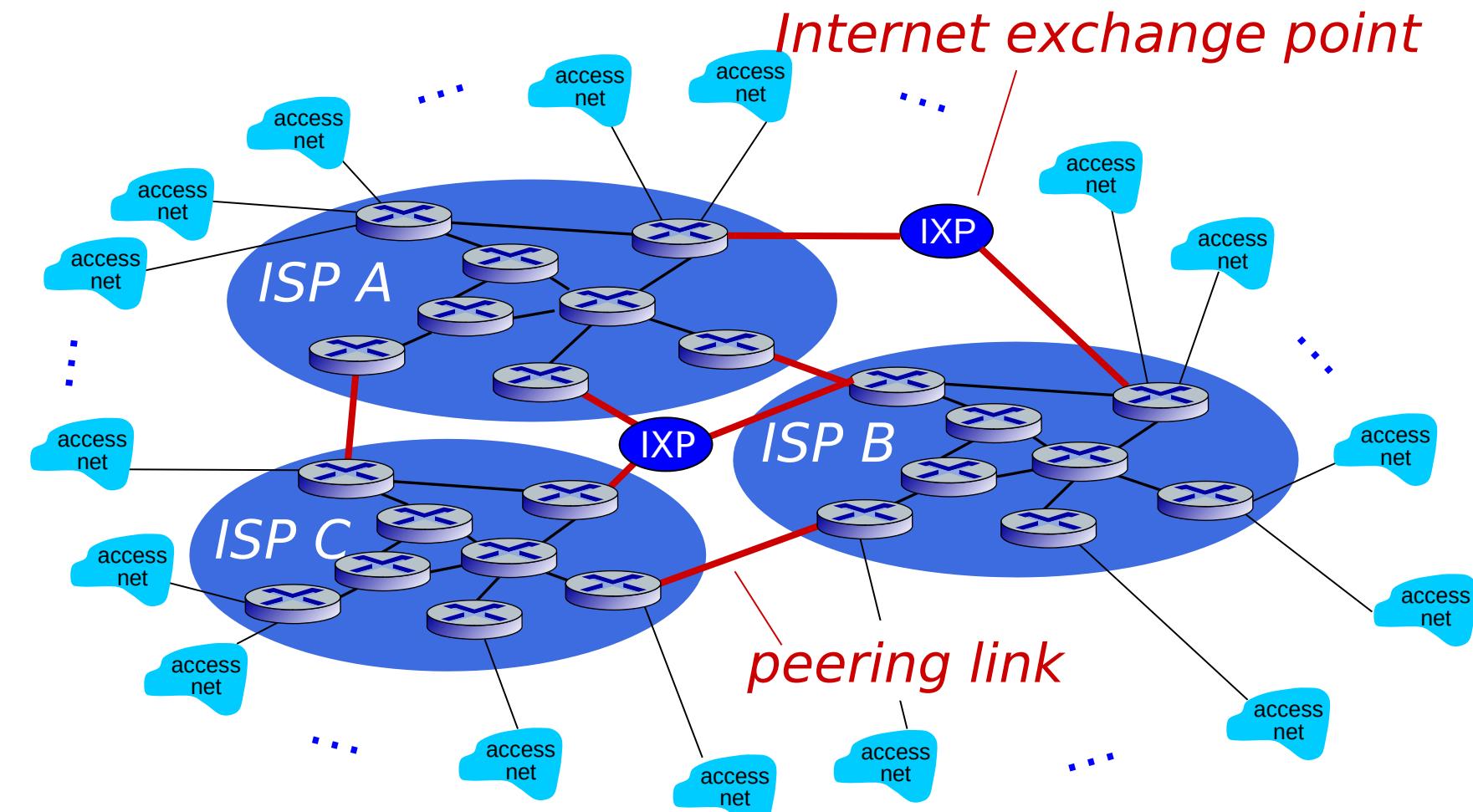
Estrutura da Internet: “rede das redes”

Mas se um único ISP global é viável enconomicamente, então pode haver competidores ...



Estrutura da Internet: “rede das redes”

Mas se um único ISP global é viável enconomicamente, então pode haver competidores, que precisam se interconectar.

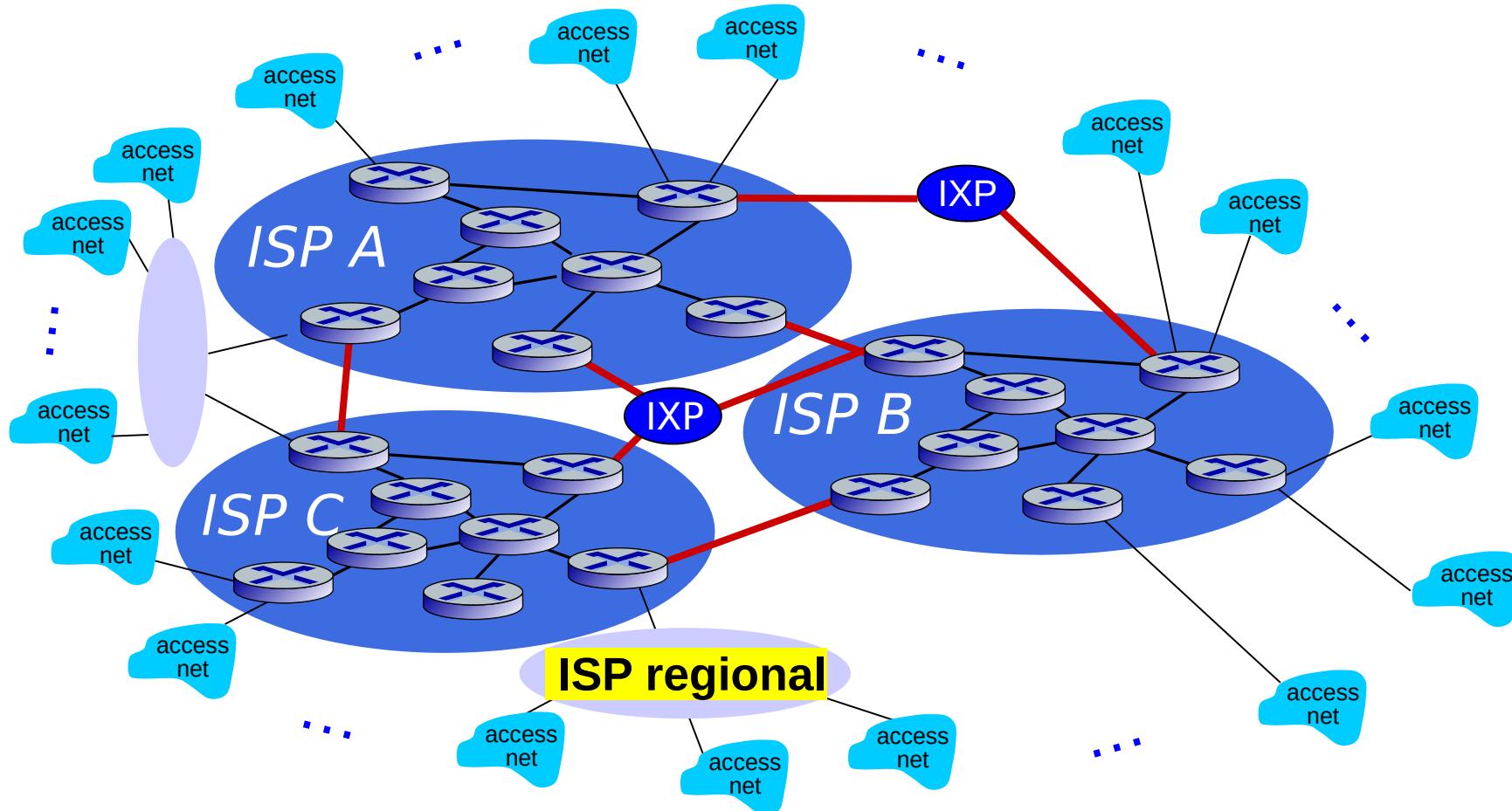


Nic.br - IX.br
<https://ix.br>

No Brasil,
também
conhecido como
PTT (Ponto de
Troca de Tráfego)

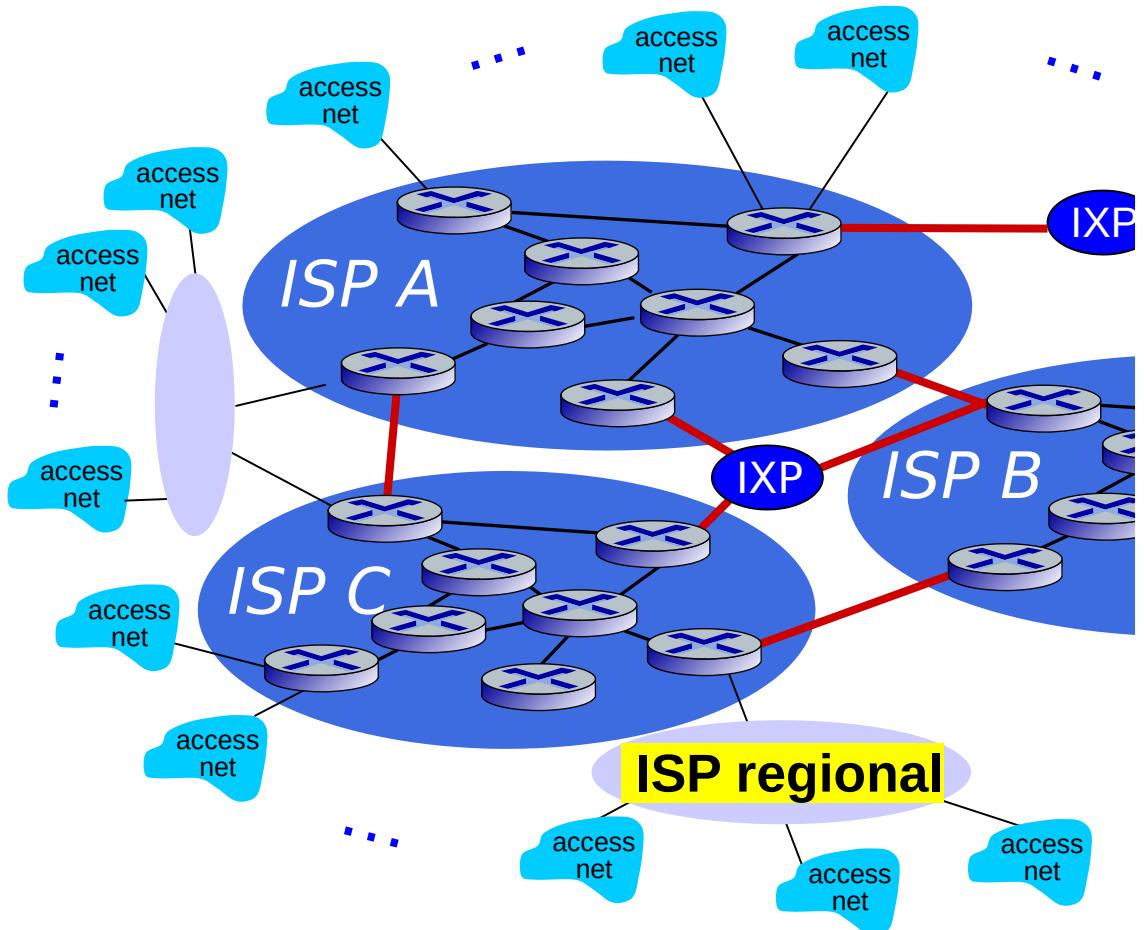
Estrutura da Internet: “rede das redes”

As redes regionais (ISP regionais) se estabelecem para conectar usuários finais às redes dos ISP globais e nacionais.



Estrutura da Internet: “rede das redes”

As redes regionais (ISP regionais) se estabelecem para conectar usuários finais às redes dos ISP globais e nacionais.



AS (Sistemas Autônomos)

Redes que compõem uma unidade administrativa (e, consequentemente, que adota uma política unificada de roteamento).

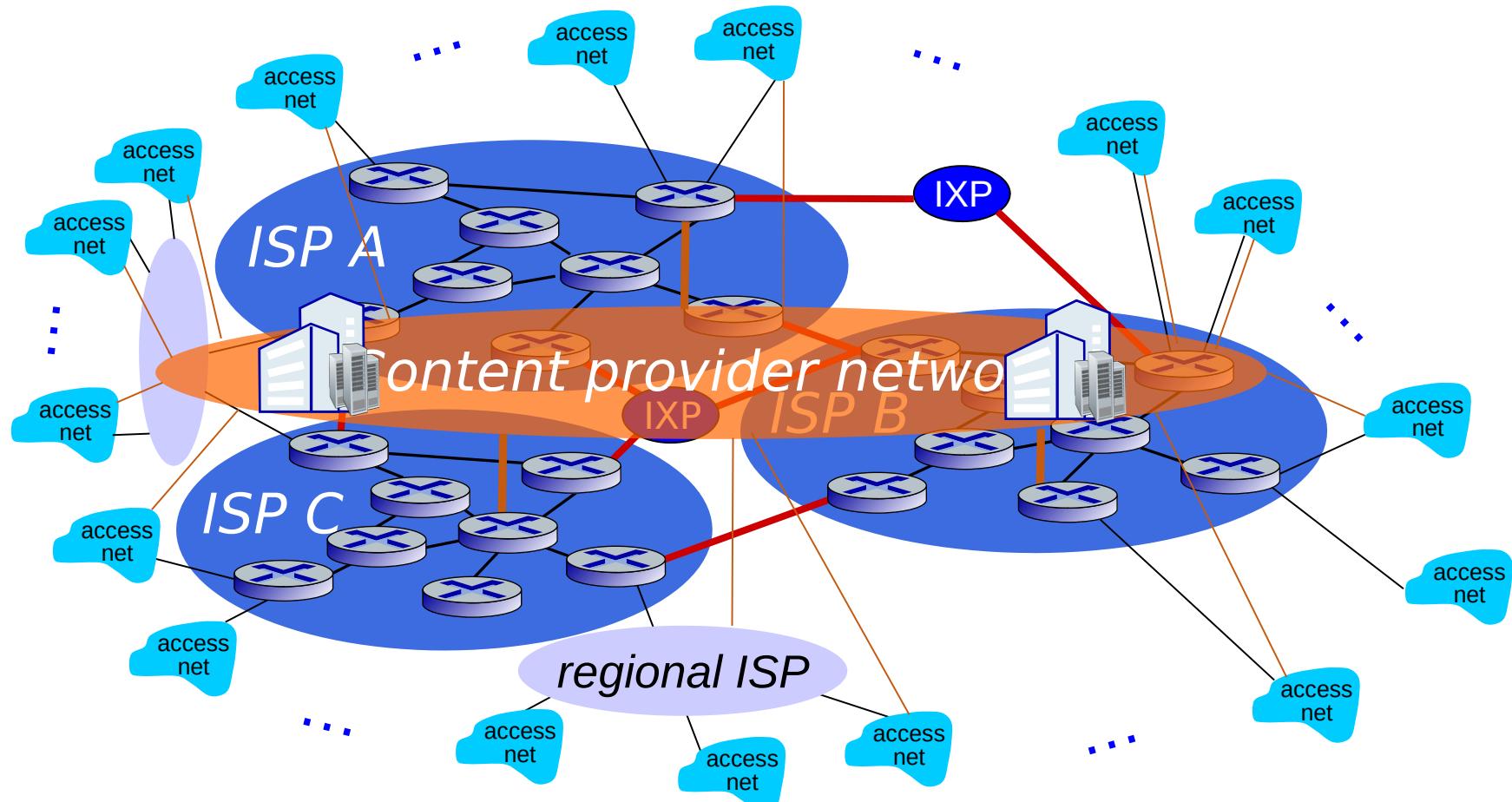
São identificados por números de 32 bits (ASNs).

Mapa de AS brasileiros:

<https://mapadeas.ceptro.br/>

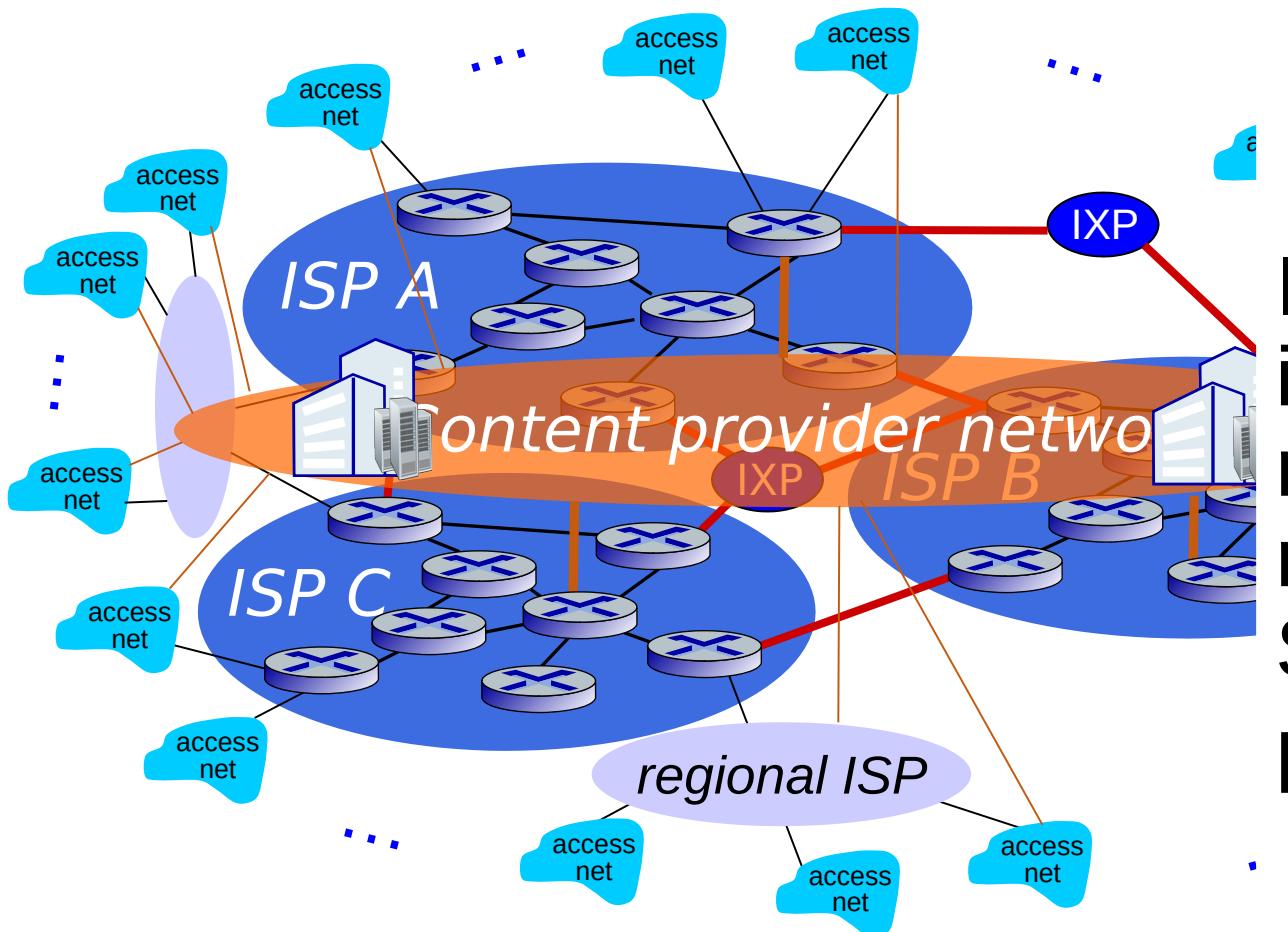
Estrutura da Internet: “rede das redes”

Surgem as redes provedoras de conteúdo – CDN (Google, Microsoft, Akamai, Netflix) que podem estabelecer suas próprias redes para fornecer serviços e **levar conteúdos para perto dos usuários**.



Estrutura da Internet: “rede das redes”

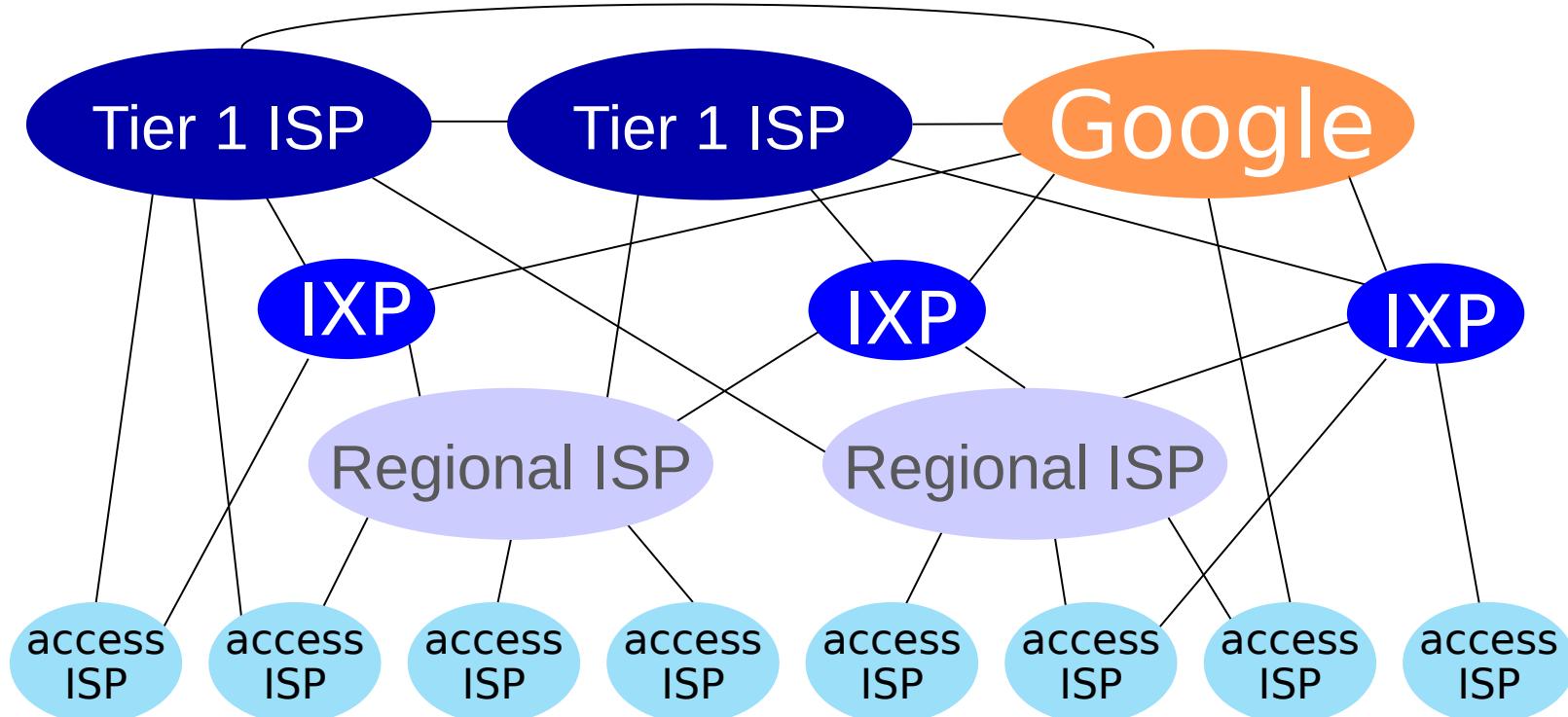
Surgem as redes provedoras de conteúdo – CDN (Google, Microsoft, Akamai, Netflix) que podem estabelecer suas próprias redes para fornecer serviços e **levar conteúdos para perto dos usuários**.



OpenCDN

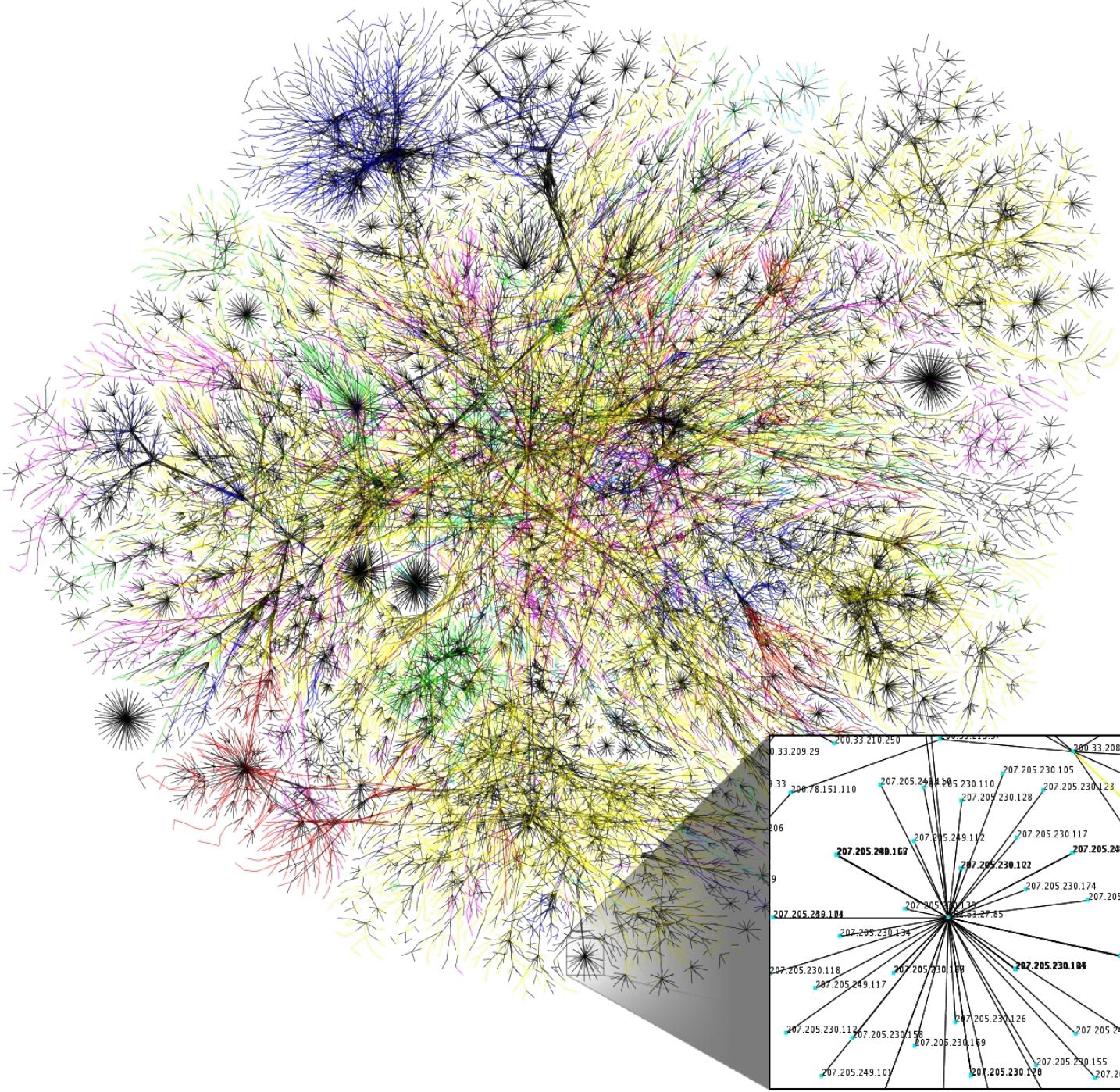
Iniciativa do NIC.br para instalar sistemas de CDN nos provedores de internet e nos PTTs (atualmente em Salvador, Manaus e Brasília).
<https://opencdn.nic.br/>

Estrutura da Internet: “rede das redes”

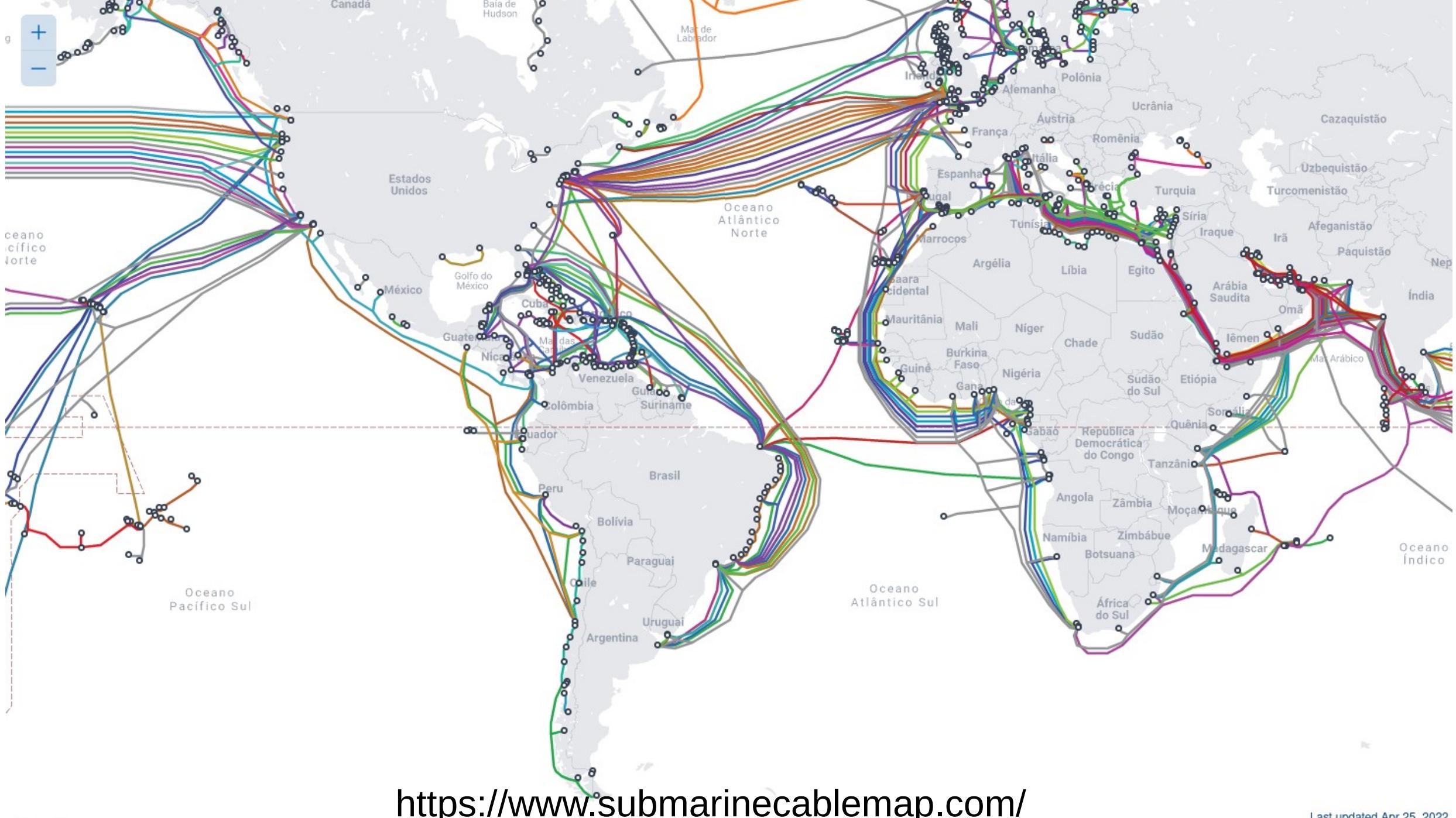


No “centro”: poucas mas bem conectadas grandes redes

- **ISPs comerciais de nível “tier-1”** (ex.: Arelion (antiga Telia), Level 3, Sprint, AT&T, NTT) cobertura nacional e internacional
- **Redes provedoras de conteúdo** (ex.: Google, Facebook, Netflix): redes privadas que conectam seus centros de dados à internet, por vezes “bypassando” ISPs regionais e ISPs tier-1
- <https://www2.arelion.com/product-sheet-InternetExposed>



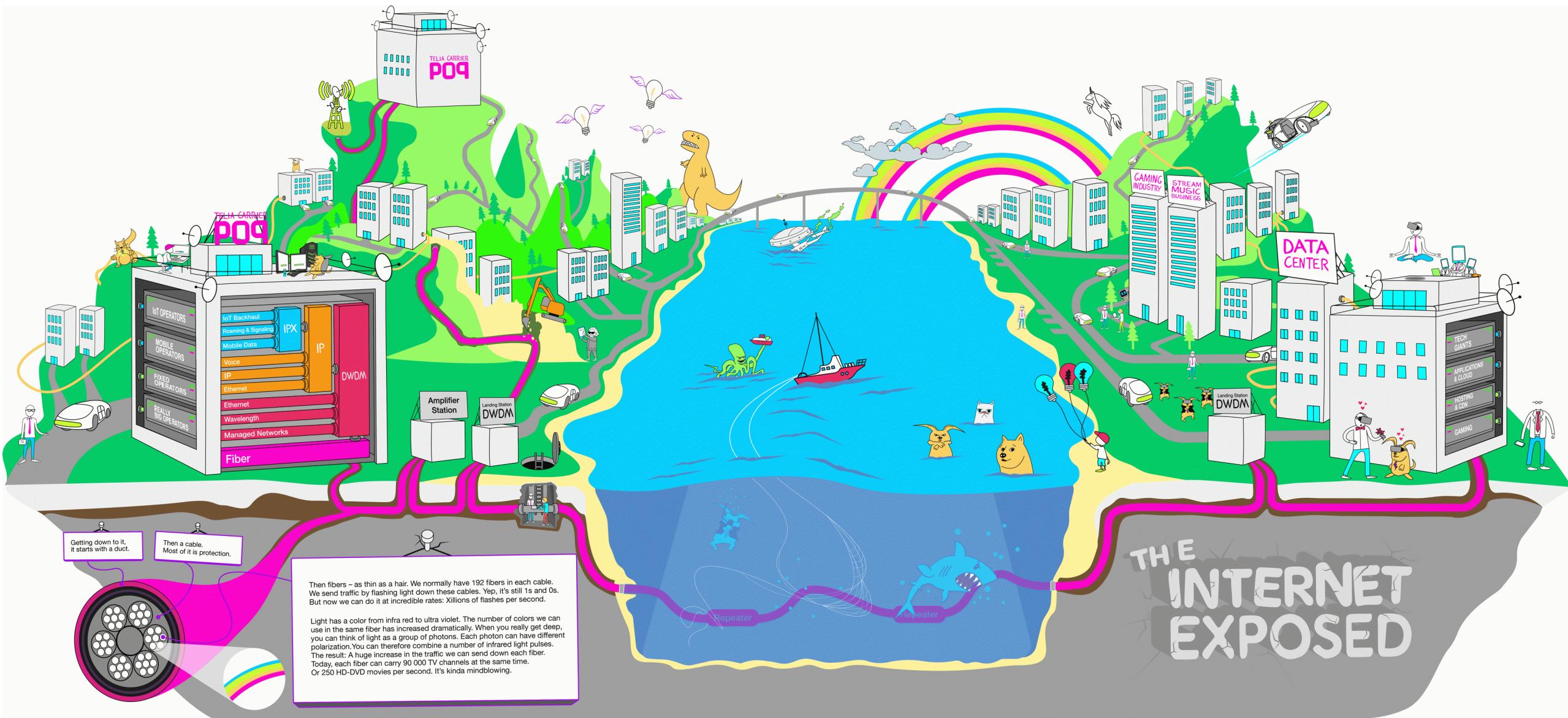
<https://www.opte.org/the-internet>



Map info and instructions



<http://www.routeviews.org/routeviews/index.php/map/>



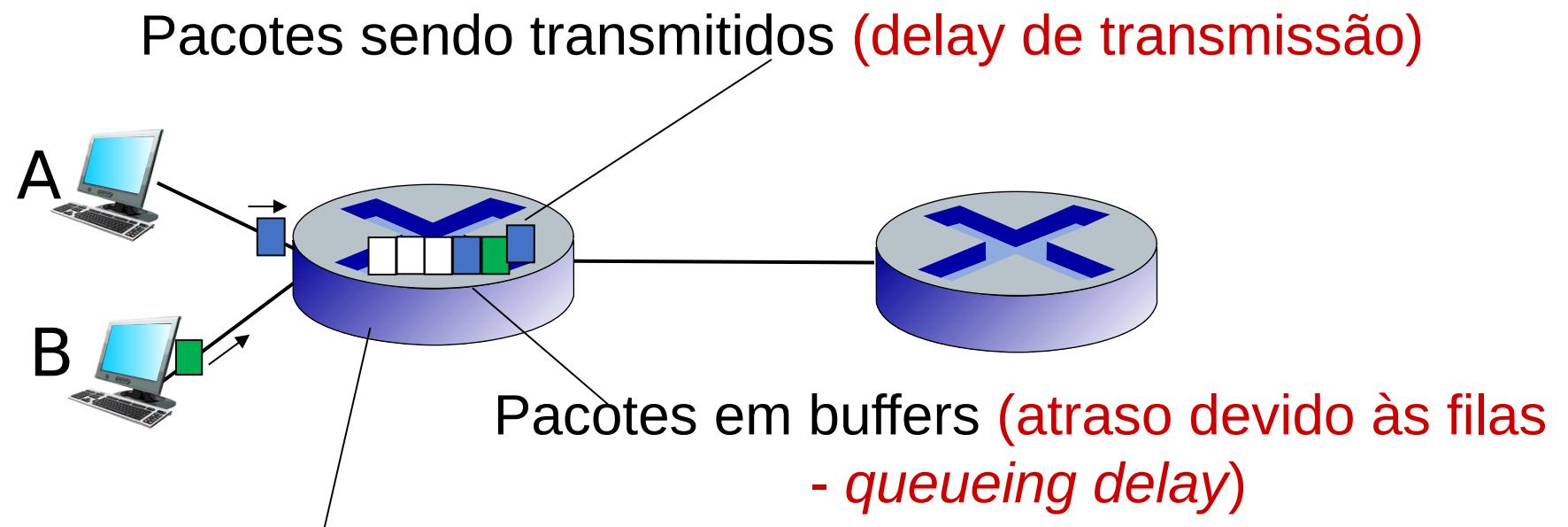
<https://www2.arelion.com/product-sheet-InternetExposed>

Sumário

- O que é a Internet? O que é um protocolo?
- Borda da rede: hosts, acesso, meios físicos
- Core da rede: comutação de circuitos e de pacotes; estrutura da Internet
- **Questões de performance: perda, atraso, desempenho**
- Segurança
- Camadas de protocolos, modelos de serviço
- História

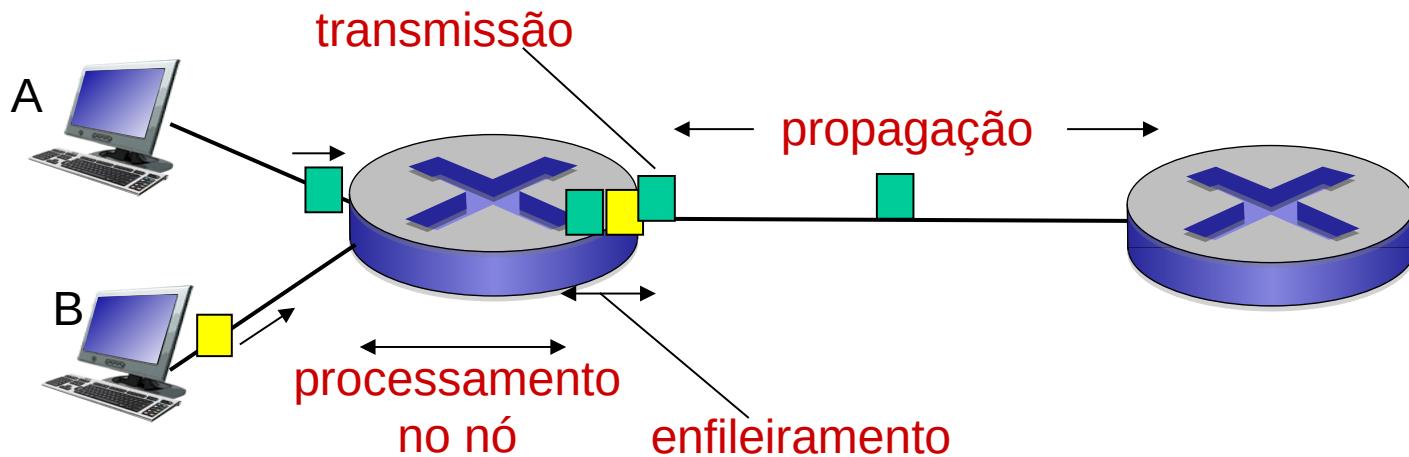
Como ocorre o atraso (*delay*) e perda de pacotes

Pacotes chegam, entram em filas (buffers), são processados, e são encaminhados para as filas de saída, esperando por transmissão: o tamanho da fila cresce se a taxa do link de entrada excede a capacidade (taxa) do link de saída. **Perdas** ocorrem quando a memória (buffer) “estoura”.



Buffers: pacotes que chegam são **descartados** se não há memória livre

Quatro fontes de atraso (delay)



$$d_{\text{nó}} = d_{\text{proc}} + d_{\text{queue}} + d_{\text{trans}} + d_{\text{prop}}$$

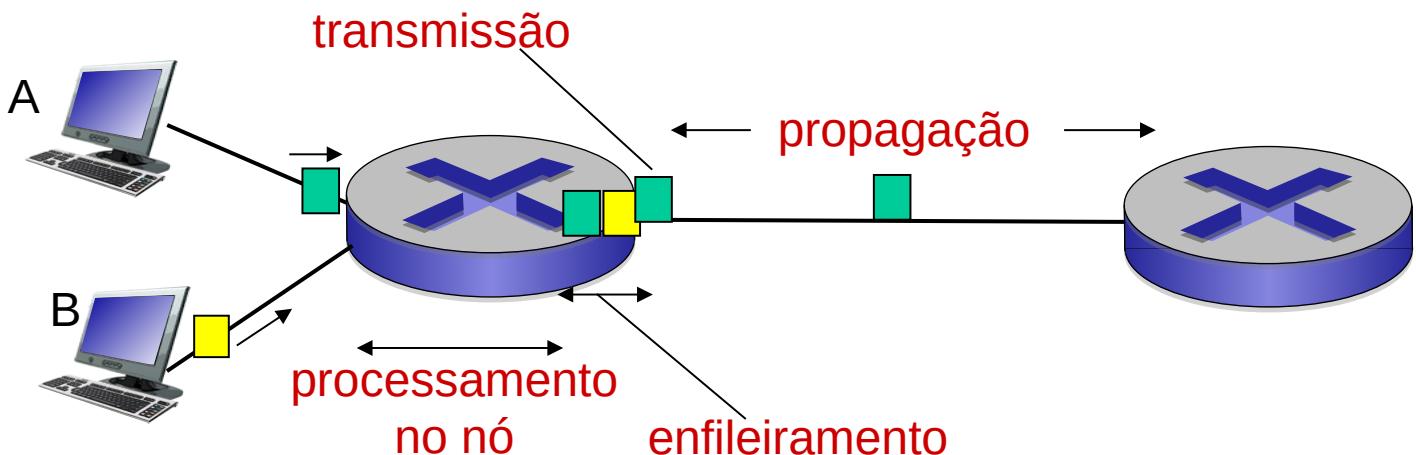
d_{proc} : processamento no nó

- Checar erros no bits
- Determinar o enlace de saída
- Tipicamente < ms

d_{queue} : atraso devido enfileiramento

- Tempo gasto esperando o enlace de saída estar disponível
- Depende do nível de congestionamento no roteador

Quatro fontes de atraso (delay)



$$d_{\text{nó}} = d_{\text{proc}} + d_{\text{queue}} + d_{\text{trans}} + d_{\text{prop}}$$

d_{trans} : atraso na transmissão

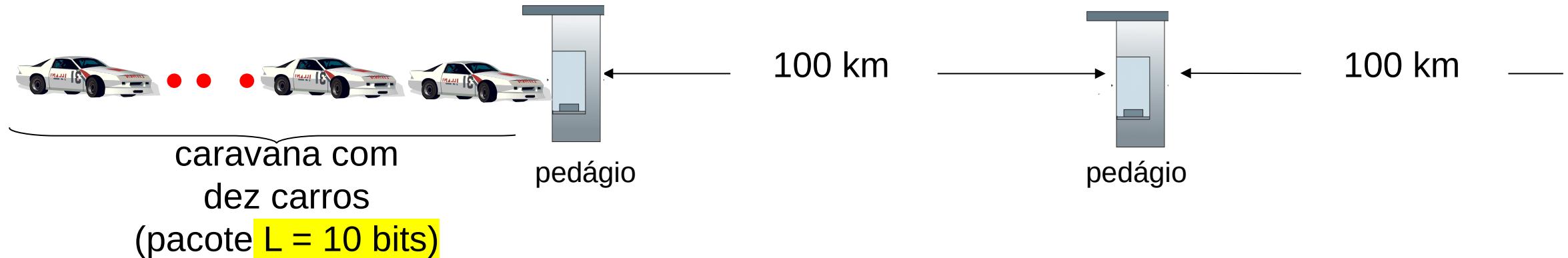
- L: tamanho do pacote (bits)
- R: largura de banda do enlace (bps)
- $d_{\text{trans}} = L/R$

d_{trans} e d_{prop}
bem diferentes
(μ s a ms – ms)

d_{prop} : atraso devido à propagação

- d: tamanho (comprimento) do enlace físico do enlace
- s: velocidade de propagação ($\sim 2 \times 10^8$ m/s – 3×10^8 m/s)
- $d_{\text{prop}} = d/s$

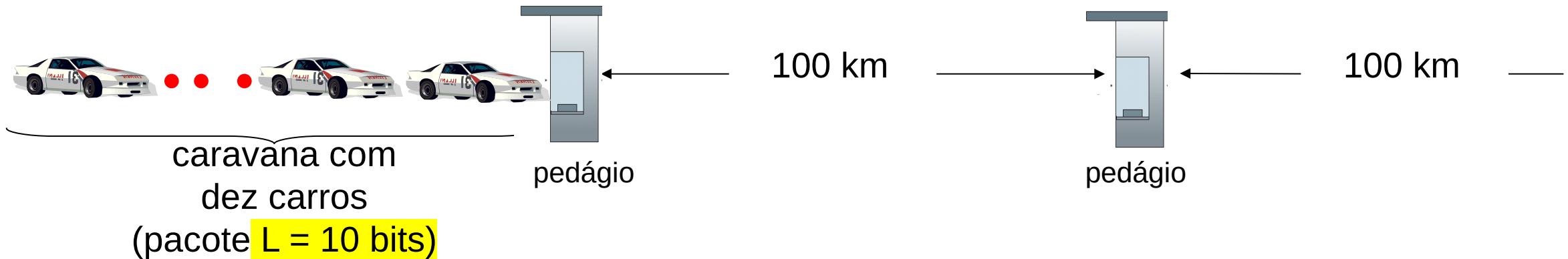
Fontes de atraso (delay): analogia da caravana



- car ~ bit; carava ~ packet; service pedágio ~ link transmissão
- Pedágio leva 12 s para atender um carro (tempo de transmissão do bit)
- Carros se propagam na velocidade de 100 km/h (delay propagação)
- Q: Quanto tempo até o último carro chegar ao segundo pedágio?

- Tempo para “entregar” toda a caravana do pedágio para a rodovia = $12 * 10 = 120$ s
- Tempo para o último carro “propagar” do primeiro para o segundo pedágio:
 $100\text{km}/(100\text{km/h})= 1$ h
- R: 62 minutos

Fontes de atraso (*delay*): analogia da caravana



Supondo, agora, que os carros se “propaguem” na velocidade de 1000 km/h
E que o pedágio leve **um minuto** para atender um carro: 10 min/pacote completo (caravana)

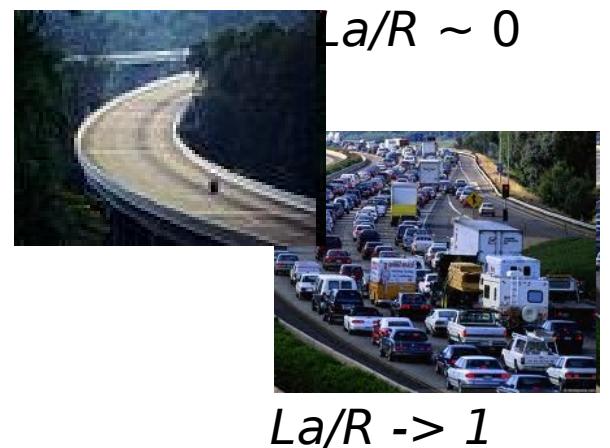
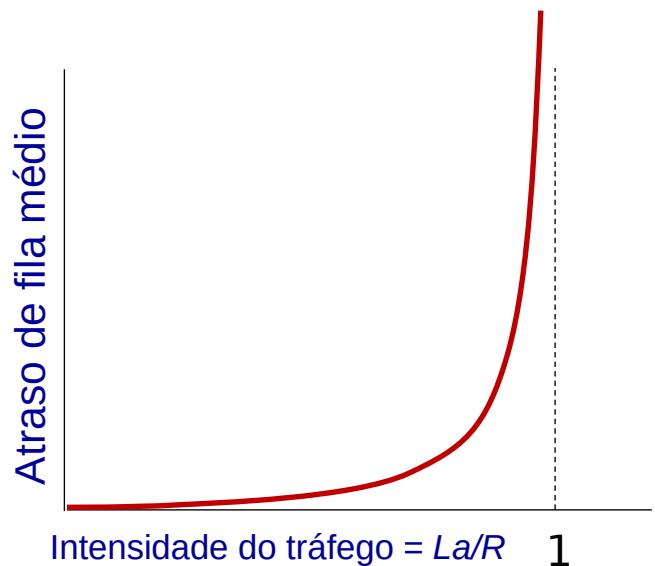
Q: Carros chegarão ao segundo pedágio antes que tenham passado completamente pelo primeiro pedágio?

$$d_{\text{prop}} = 100 \text{ km} / 1000 \text{ km/hora} = 0,1 * 60 \text{ min} = 6 \text{ min}$$

R: Sim, depois de 7 minutos, o primeiro carro chega ao segundo pedágio; três carros ainda estarão esperando no primeiro pedágio.

Atraso de enfileiramento de pacotes

- R: largura de banda do enlace (bps)
 - L: tamanho do pacote (bits)
 - a: razão média de chegada dos pacotes
 - La/R : (razão chegada de bits)/(taxa do enlace) = define a **intensidade do tráfego**
-
- $La/R < 1$ ou ~ 0 : média de atraso devido fila pequeno
 - $La/R \rightarrow 1$: média de atraso devido fila é muito grande
 - $La/R > 1$: mais chegadas do que podem ser tratadas; média de atraso tendendo ao infinito

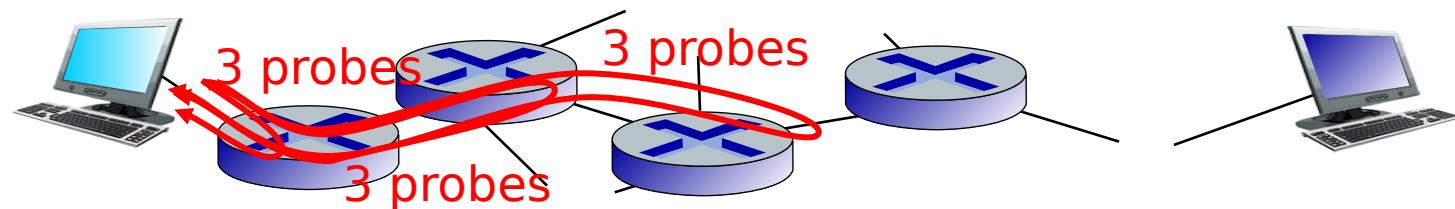


Internet: atrasos e rotas

Como se obtém medidas de atrasos e de perda de pacotes na Internet?

traceroute: provê medidas de atraso da origem até um roteador ao longo do caminho até o destino final dos pacotes. Para todos os roteadores i :

- Envia três pacotes que alcançarão o roteador i no caminho até o destino final.
- Roteador i retornará os pacotes até o emissor.
- O emissor computará o tempo entre a transmissão e a chegada dos respectivos pacotes.



Internet: atrasos e rotas

traceroute: gaia.cs.umass.edu até www.eurecom.fr

Comandos: Linux: **traceroute/tracepath** Windows: **tracert**

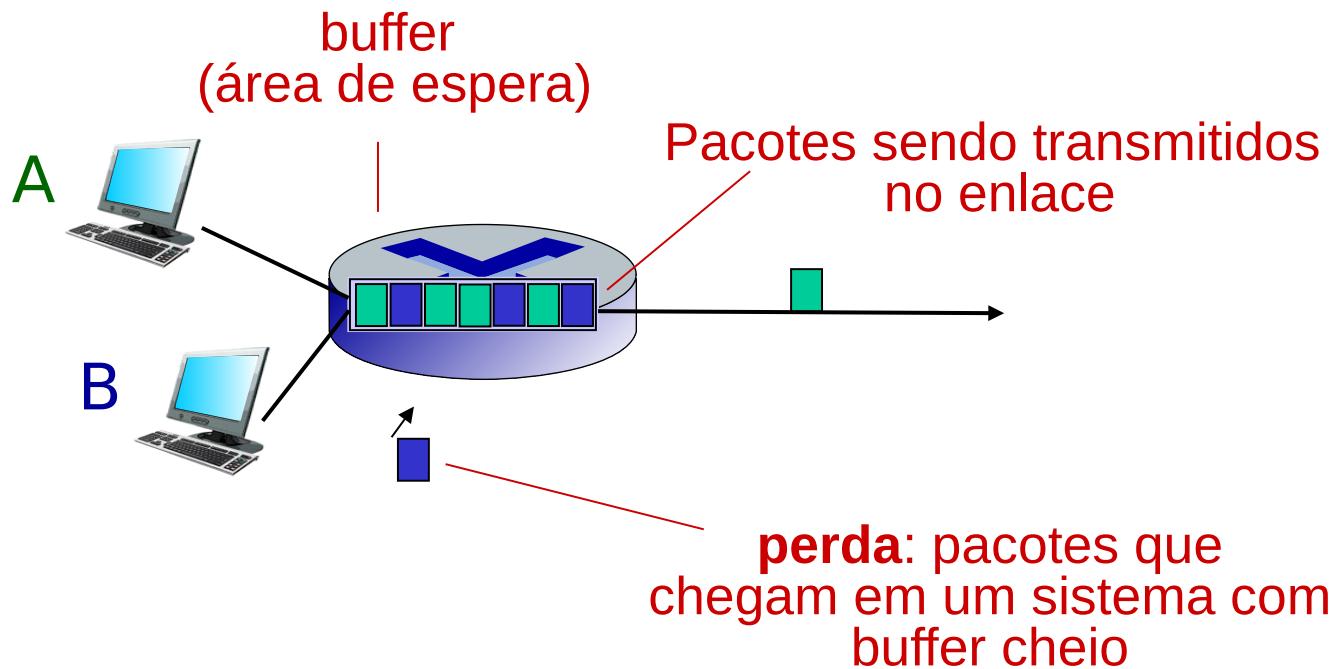
3 medidas de atraso (*delay*) da máquina
gaia.cs.umass.edu até cs-gw.cs.umass.edu

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-s07-0-0-0.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	* * *					* indica sem resposta (<i>probe lost, router not replying</i>)
19	fantasia.eurecom.fr (193.55.113.142)	132 ms	128 ms	136 ms		

Enlace
trans-oceânico

Internet: perda de pacotes

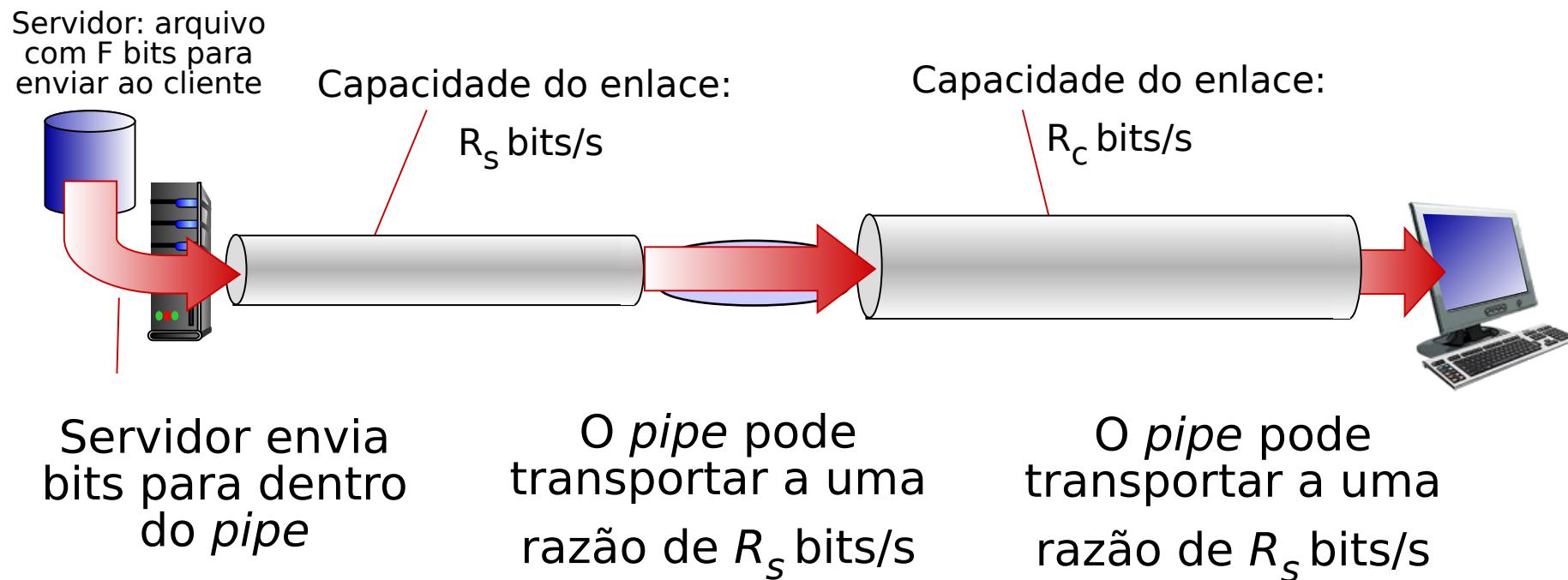
- Fila (buffer) do enlace de chegada tem capacidade limitada
- Pacote que chega a uma fila cheia é descartado (dropped; lost)
- Pacote perdido pode ser retransmitido pelo sistema de origem (confiabilidade provida por protocolos de nível superior) ou não.



Desempenho: vazão (*throughput*)

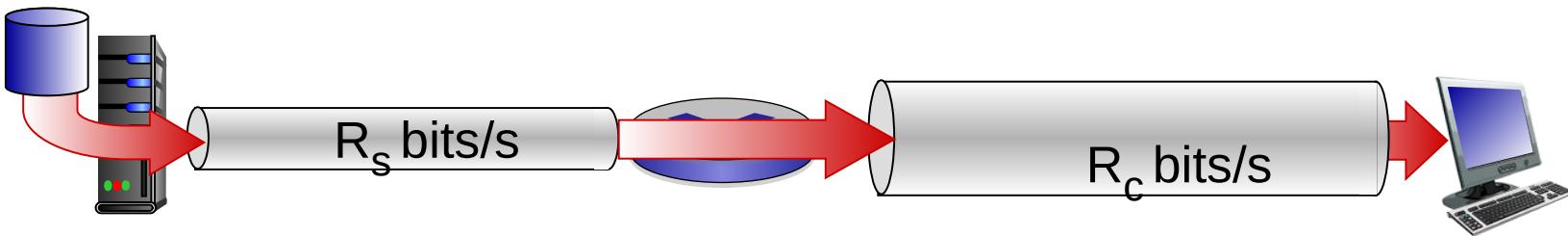
Vazão (*throughput*): razão (bits/unidade tempo) na qual são transferidos entre emissor/receptor

- **instantânea**: razão em um dado tempo
- **média**: razão sobre um período de tempo mais longo

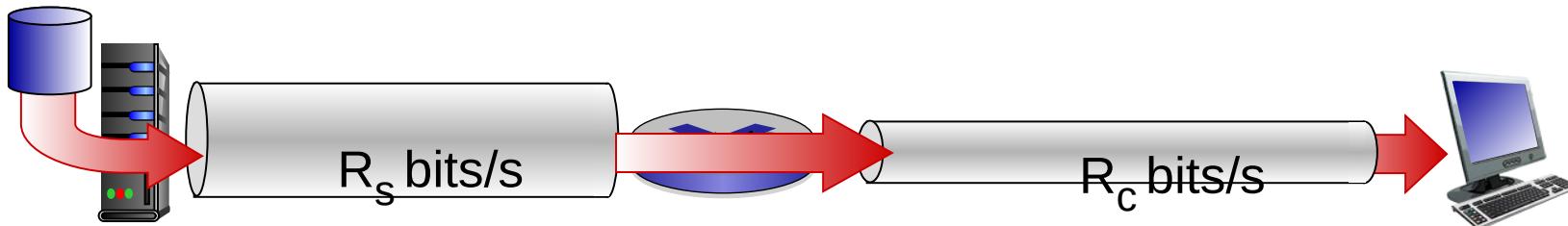


Desempenho: vazão (*throughput*)

- $R_s < R_c$ Qual a média da vazão fim-a-fim?



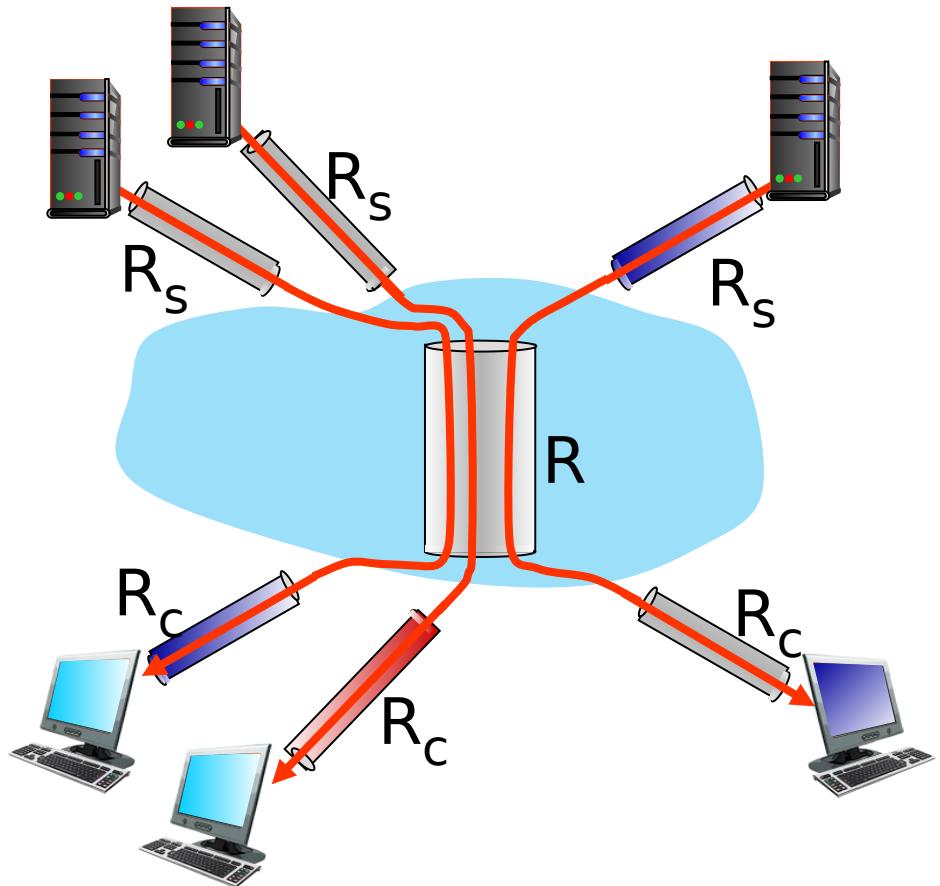
- $R_s > R_c$ Qual a média da vazão fim-a-fim?



Gargalo no enlace

Enlace que limita a vazão fim-a-fim

Desempenho: cenário da Internet



10 conexões compartilham (*fairly*)
o enlace de backbone (R bits/s)

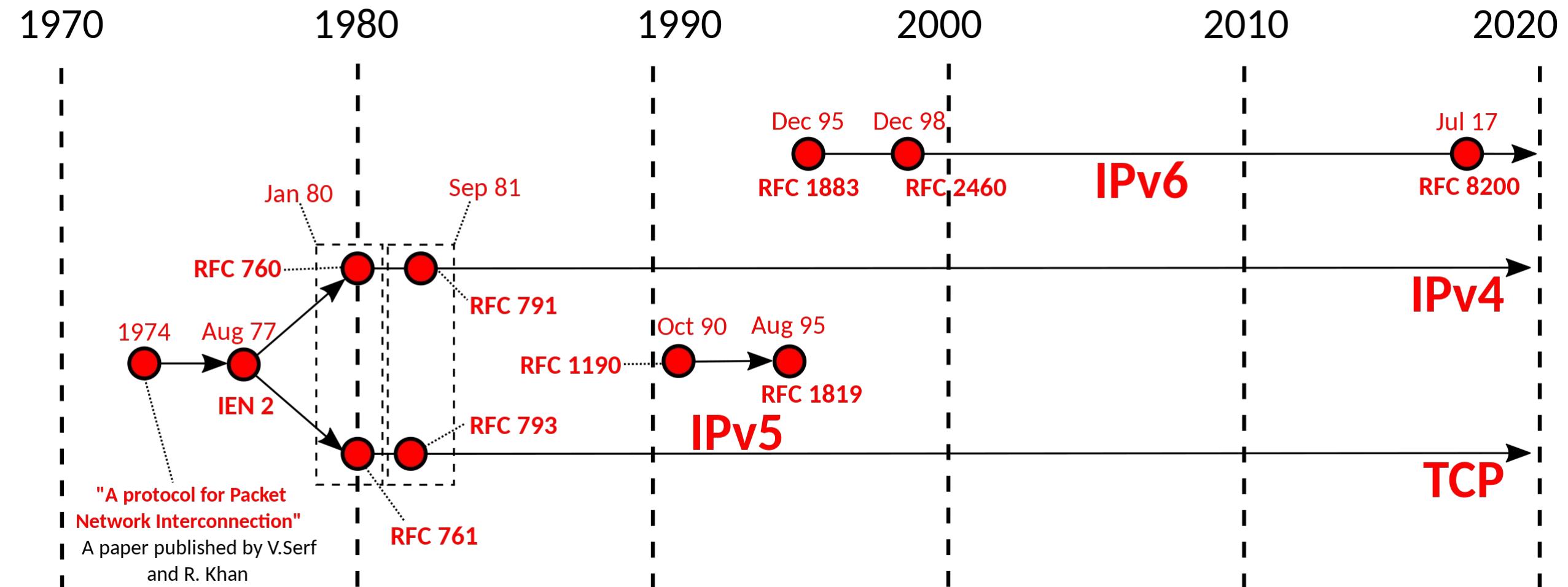
Vazão por conexão
fim-a-fim:

$$\min(R_c, R_s, R/10)$$

Na prática: R_c ou R_s
é geralmente o
gargalo

Sumário

- O que é a Internet? O que é um protocolo?
- Borda da rede: hosts, acesso, meios físicos
- Core da rede: comutação de circuitos e de pacotes; estrutura da Internet
- Questões de performance: perda, atraso, desempenho
- **Segurança**
- Camadas de protocolos, modelos de serviço
- História



Segurança de Rede (*network security*)

A Internet não foi projetada originalmente visando segurança

- Visão original: “*a group of mutually trusting users attached to a transparent network*”
- Protocolos projetados para funcionalidades
- A segurança deve ser considerada em todos os níveis

Questões

- Como ataques podem ser perpetrados
- Como se defender
- Como projetar arquiteturas “imunes” a ataques

“Infectando” hosts com malware

Malware podem chegar num host a partir de:

virus: programa que se autoreplica e infecta hosts através do recebimento e execução de objetos (por exemplo, arquivos anexados em e-mail).

worm: infecção que se replica através do recebimento de forma passiva de um objeto que é autoexecutado. O objeto é um arquivo executável e o ataque ocorre via rede.

Spyware malware pode registrar e armazenar digitação, sítios visitados, obter e enviar dados pessoais.

Ransomware: extorsão digital via criptografia de dados e pedido de resgates

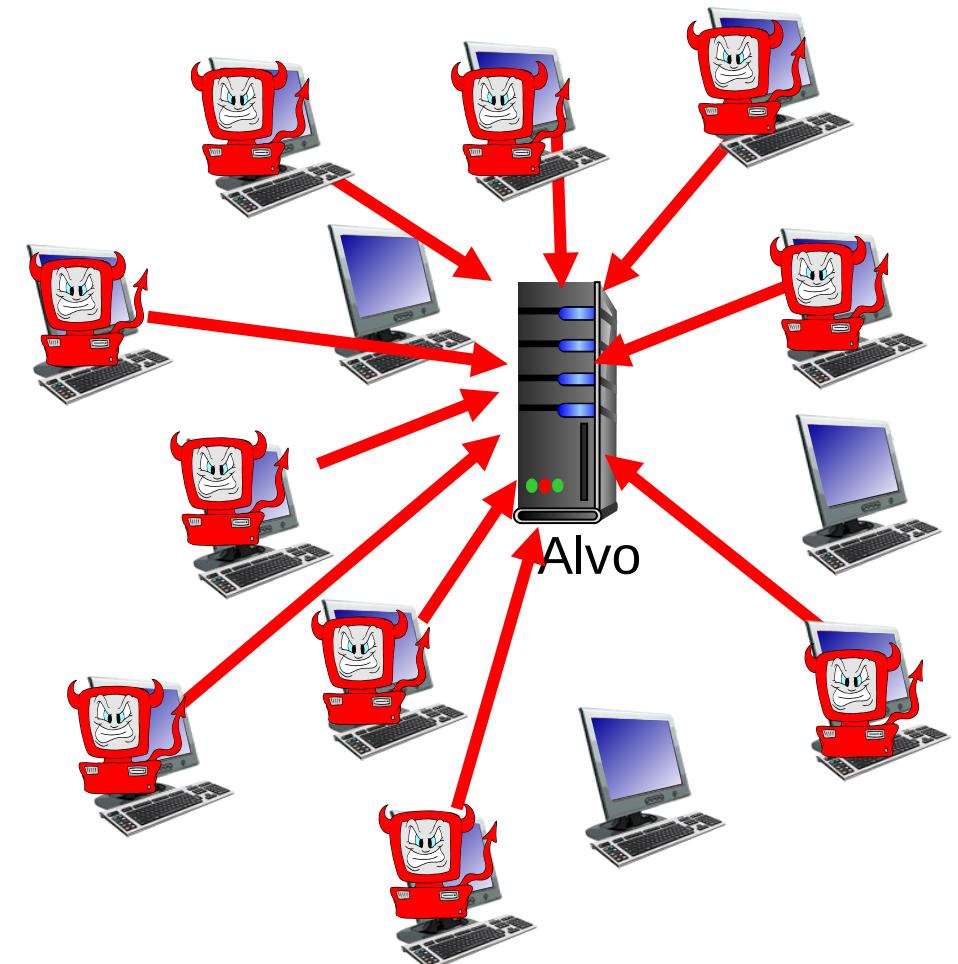
Um host infectado pode se tornar um membro de uma **botnet**, rede que é usada para diversas atividades, como gerar spam, realizar ataques **DDoS**.

Ataques de negação de serviço (*denial of service*)

Denial of Service (DoS): atacantes esgotam os recursos (servidores, largura de banda), tornando-os indisponíveis para usuários legítimos.

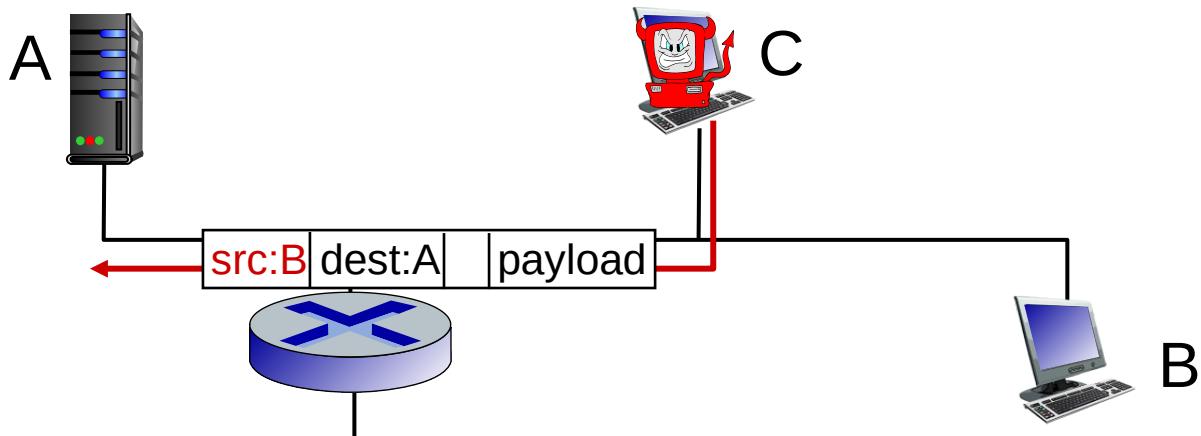
1. Seleção do alvo
2. Ataque a hosts tornando-os “escravos”(botnet)
3. O atacante envia comandos aos hosts comprometidos para que enviem pacotes ao alvo

DDoS (Distributed DoS): quando são usadas várias máquinas e dispositivos (normalmente na forma de uma botnet).



Uso de endereços de rede falsos

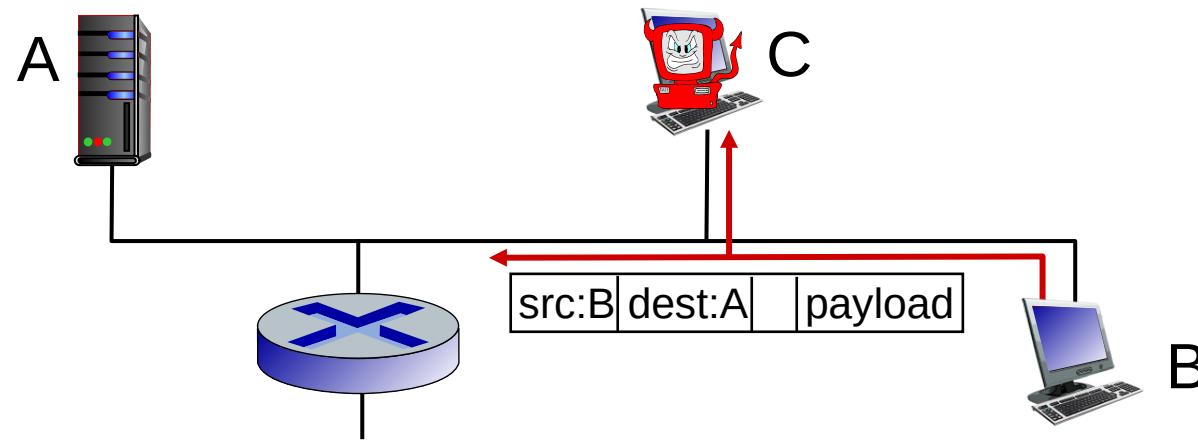
IP spoofing: enviar um pacote com endereço falso de origem



Na prática, podem ser falsificados: endereços de rede IP, endereços de enlace MAC e de números de porta (camada de transporte).

Interceptando tráfego (pacotes/frames de rede)

Packet “**sniffing**”: **captura** de dados de rede; no sentido geral, pacotes de rede, e em sentido restrito, frames de rede (unidade básica de dados da camada de enlace), a qual permite analisar todos os protocolos das diversas camadas que estejam sendo transportados. A palavra vem de “farejar” dados de rede.



Wireshark: programa de código aberto e livre para diversas plataformas que é usado para realizar captura e análise de tráfego de rede.

Linhas de defesa (considerando a infra de rede)

- **Autenticação:** provar que alguém (ou sistema) é quem diz ser: normalmente usuário:senha, mas outros fatores (como biometria) podem ser usados (MFA MultiFactor AuthN). Redes celulares usam cartões SIM como identificadores e para autenticação
- **Confidencialidade:** dados somente podem ser acessados por quem foi permitido/autorizado. A técnica mais comum é o uso de criptografia.
- **Integridade:** garantia de que não houve violação de dados. Pode ser conseguido por: funções hash; assinaturas digitais; códigos MAC (Message Authentication Code)
- **Restrições de acesso (autorização):** sistemas de controle de controle de acesso; redes privadas virtuais (VPN)
- **Firewalls:** equipamentos especializados (“middleboxes”) ou computadores executando funções de firewall:
 - Definem perímetros de rede (segura vs insegura)
 - Default: filtrar/bloquear requisições da Internet para a rede interna; enquanto, libera (filtra) as conexões originadas internamente à rede
 - Estão associados a sistemas de detecção de intrusão (IDS) para reagir a eventos de ataques



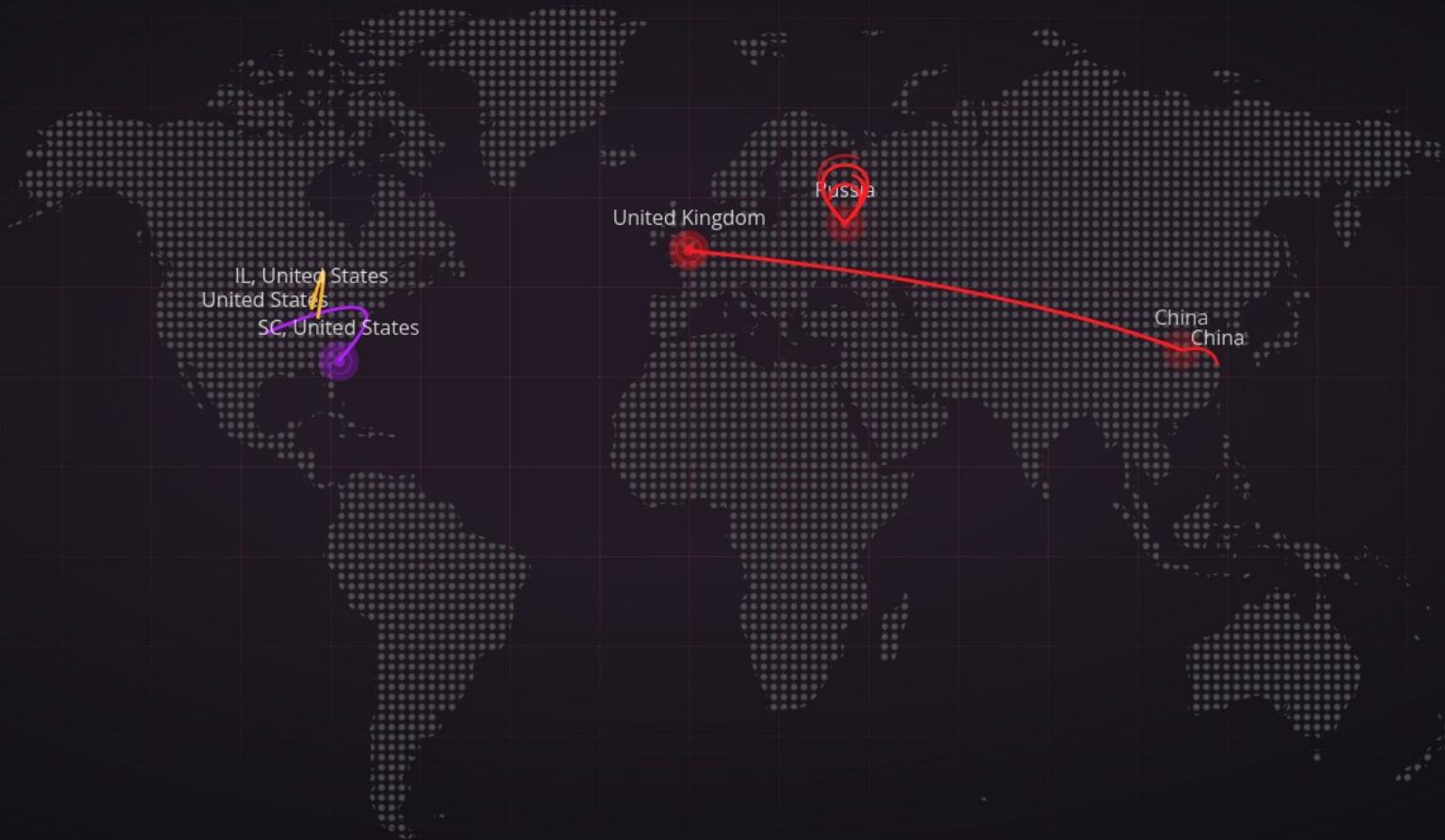
RECENT DAILY ATTACKS

ATTACKS Current rate 4 +

- Linux System Files Information Disclo...
14:51:22 IL, United States → IN, United Sta...
- Ref.TC.w
14:51:21 Russia → Russia
- Ref.TC.w
14:51:21 Russia → Russia
- Linux System Files Information Disclo...
14:51:21 IL, United States → IN, United Sta...
- Cryptbot.TC.uj
14:51:21 China → United Kingdom
- Phishing.TC.avntna
14:51:20 United States → SC, United States
- Ref.TC.w
14:51:20 Russia → Russia

LIVE CYBER THREAT MAP

21,308,714 ATTACKS ON THIS DAY



Malware



Phishing



Exploit

DON'T WAIT TO BE ATTACKED
PREVENTION STARTS NOW>

TOP TARGETED COUNTRIES

Highest rate of attacks per organization in the last day.

- Mongolia
- Nepal
- Georgia
- Bolivia
- Macao

TOP TARGETED INDUSTRIES

Highest rate of attacks per organization in the last day.

- Education
- Government
- Healthcare

TOP MALWARE TYPES

Malware types with the highest global impact in the last day.

- Adware
- Backdoor
- Phishing



<https://threatmap.checkpoint.com/>

Sumário

- O que é a Internet? O que é um protocolo?
- Borda da rede: hosts, acesso, meios físicos
- Core da rede: comutação de circuitos e de pacotes; estrutura da Internet
- Questões de performance: perda, atraso, desempenho
- Segurança
- **Camadas de protocolos, modelos de serviço**
- História

Camadas de protocolos

Redes **são complexas**, com muitas partes:

- hosts
- roteadores
- enlaces de diversos tipos
- aplicações
- protocolos
- hardware, software

Questão:

existe alguma “esperança” de organizar essa estrutura de rede?

.... ou ao menos na organização da discussão sobre redes?

Analogia: como é uma viagem aérea

ticket (compra)

bagagem (check)

portões (load)

decolagem

rota de voo

ticket (complain)

bagagem (claim)

portões (unload)

pouso

rota de voo

Rota de voo

Uma série de passos que envolvem diversos serviços para transferir fim-a-fim uma pessoa e sua bagagem.

Analogia: como é uma viagem aérea

ticket (purchase)	<i>ticketing service</i>	ticket (complain)
baggage (check)	<i>baggage service</i>	baggage (claim)
gates (load)	<i>gate service</i>	gates (unload)
runway takeoff	<i>runway service</i>	runway landing
airplane routing	<i>routing service</i>	airplane routing

Camadas: cada camada implementa um serviço:

- Através de ações internas na camada
- Usando os serviços providos pela camada mais abaixo

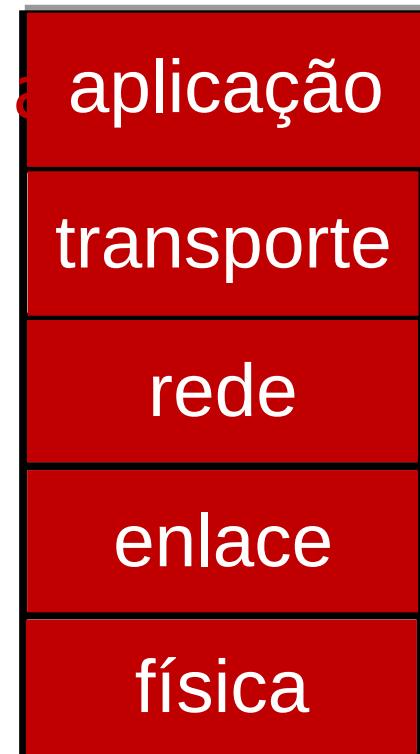
Porquê de camadas?

Tratar/projetar/discutir sistemas complexos:

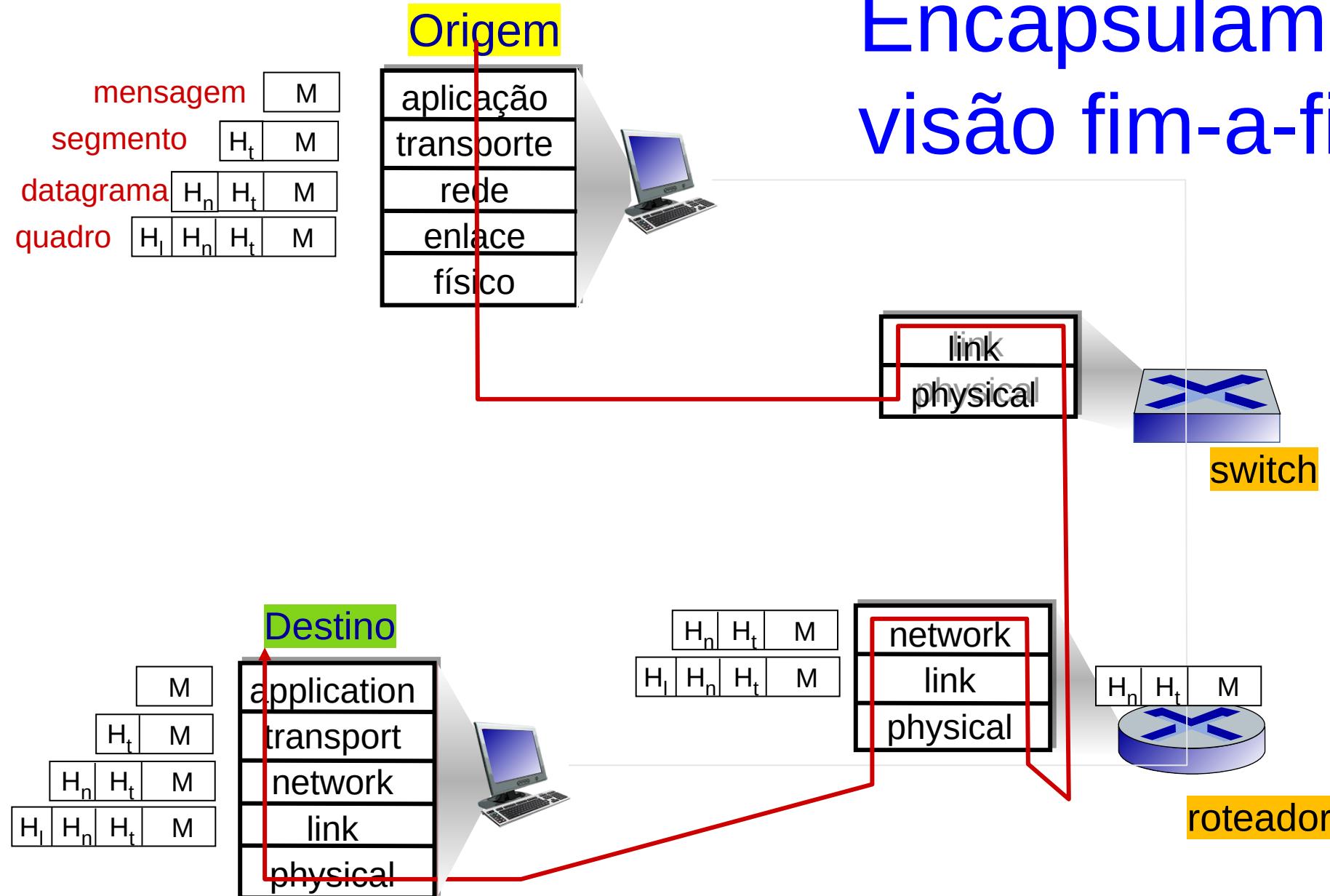
- Estrutura explícita permite identificação e o estabelecimento da relação entre os elementos: uso de **modelos de referência** de camadas para discussão
- Modularização facilita a manutenção e atualizações: mudança na implementação em um serviço de uma camada é transparente ao resto do sistema

Pilha de protocolos Internet

- **Aplicação:** suporta as aplicações de rede
 - HTTP, IMAP, SMTP, DNS
- **Transporte:** trata da transferência de dados entre processos em rede
 - TCP, UDP
- **Rede:** roteamento dos datagramas entre a origem e o destino
 - IP, protocolos de roteamento (BGP, OSPF, RIP, ...)
- **Enlace:** transferência de dados entre dispositivos próximos (uso de um único meio de conexão)
 - Ethernet, 802.11 (WiFi), PPP
- **Físico:** bits “*on the wire*”



Encapsulamento: visão fim-a-fim



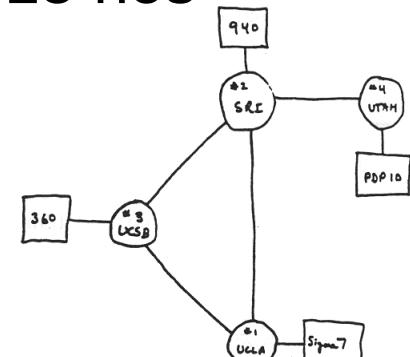
Sumário

- O que é a Internet? O que é um protocolo?
- Borda da rede: hosts, acesso, meios físicos
- Core da rede: comutação de circuitos e de pacotes; estrutura da Internet
- Questões de performance: perda, atraso, desempenho
- Segurança
- Camadas de protocolos, modelos de serviço
- **História**

História da Internet

1961-1972: princípios da comutação de pacotes

- 1961: Kleinrock – teoria de filas mostra a efetividade da **comutação de pacotes**
- 1964: Baran – comutação de pacotes em redes militares
- 1967: ARPAnet definida pela agência *Advanced Research Projects Agency*
- 1969: primeiro nó operacional da ARPAnet
- 1972:
 - ARPAnet public demo
 - **NCP (Network Control Protocol)** primeiro protocolo para comunicação host-host
 - Primeiro programa de e-mail
 - ARPAnet possui 15 nós



THE ARPA NETWORK

História da Internet

1972-1980: *Internetworking*: conexão entre redes; criação de redes; redes proprietárias

- 1970: ALOHAnet: rede por satélite no Hawaii
- 1974: Cerf e Kahn – arquitetura para interconexão de redes
- 1976: Ethernet no Xerox PARC
- Final década 70: arquiteturas rede proprietárias: DECnet, SNA, XNA
- Final década 70: comutação de pacotes com tamanho fixo (precursors do ATM)
- 1979: ARPAnet registra 200 nós

Princípios de internetworking (Cerf e Kahn):

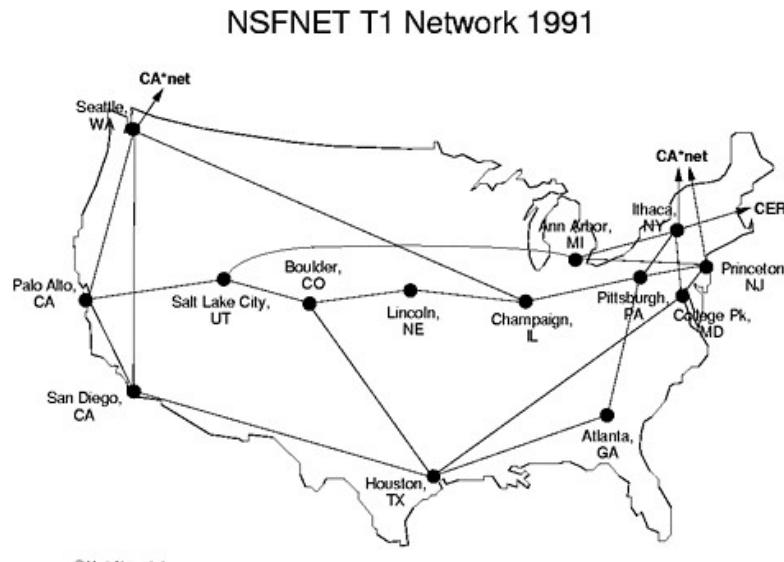
- Minimalismo, autonomia – sem mudanças internas requeridas para interconectar redes
- Modelo de serviço melhor esforço (*best effort*)
- Roteadores sem estado (*stateless*)
- Controle descentralizado

Que definem a arquitetura da Internet atual

História da Internet

1980-1990: novos protocolos e proliferação das redes

- 1983: desenvolvimento do TCP/IP
- 1982: protocolo de e-mail: SMTP
- 1983: protocolo para tradução nomes-para-endereços: DNS
- 1985: protocolo pra transferência arquivos: FTP
- 1988: controle de congestionamento TCP
- Novas redes nacionais: CSnet, BITnet, NSFnet, Minitel
- 100.000 hosts conectados às diversas redes



História da Internet

Décadas 1990 e 2000: comercialização na Web; novas aplicações

- Início 1990: ARPAnet foi decomissionada
- 1991: NSF retirou restrições ao uso comercial da rede NSFnet (1995)
- Década de 1990: Web
 - Hypertexto [Bush 1945, Nelson 1960's]
 - HTML, HTTP: Berners-Lee
 - 1994: Mosaic, depois Netscape
 - Final da década 1990: comercialização na Web

Entre 1990 e 2000:

- Mais “*killer apps*”: mensagens instantâneas, compartilhamento arquivos P2P
- Segurança de rede
- Estimativas de 50 milhões de hosts e mais de 100 milhões de usuários
- Enlaces de *backbone* chegando a taxas de Gbps

História da Internet

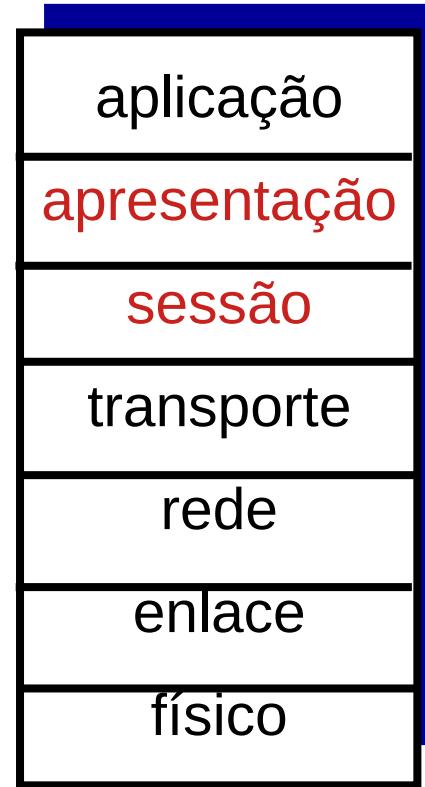
2005-até o presente: escala, SDN, mobilidade, *cloud computing*

- Desenvolvimento agressivo do acesso via banda larga (10 a centenas de Mbps)
- 2008: *software-defined networking* (SDN)
- Aumento e disseminação do acesso via redes sem fio de alta velocidade: 4G/5G, WiFi
- Provedores de serviço (Google, FB, Microsoft) criando suas próprias redes (implementação de CDNs): “bypassando” grandes provedoras para posicionarem seus sistemas mais perto dos usuários, e com isso fornecer acesso instantâneo a conteúdos
- Empresas executando seus serviços em nuvem (Amazon Web Services - AWS, Microsoft Azure, Google Cloud Platform)
- Aumento no número de smartphones: mais dispositivos móveis acessando à internet que dispositivos fixos (2017)
- ~18B dispositivos conectados à internet (2017): aumento de dispositivos IoT conectados às redes

Modelo de referência OSI da ISO

Duas camadas não presentes na arquitetura TCP/IP

- **apresentação:** permite aplicações interpretar o significado dos dados: compressão, criptografia, convenções específicas da máquina (*endianess*)
- **sessão:** sincronização, pontos de checagem, recuperação durante troca de dados
- Camadas “ausentes” da pilha Internet: esses serviços, se necessários, deverão ser implementados pelas aplicações



Modelo de referência OSI/ISO

Wireshark

