



# Redes de Computadores II NAT, IPv6 & História

**Prof. Elias P. Duarte Jr.**

Universidade Federal do Paraná (UFPR)

Departamento de Informática

[www.inf.ufpr.br/elias/redes](http://www.inf.ufpr.br/elias/redes)

# Sumário da Aula de Hoje

- Uma aula e 3 tópicos
  - 1) NAT - *Network Address Translation*
  - 2) IPv6
  - 3) História da Internet

# NAT: Network Address Translation

- Nestas alturas do campeonato vamos voltar a falar sobre endereços IPv4
- Muitos de vocês já perceberam que as máquinas que usam às vezes têm endereços estranhos
  - por exemplo: 10.0.0.1
- Que endereços são estes?
- São endereços NAT, como vamos ver a seguir

# NAT: Contexto de Surgimento

- Como já falamos, no início dos anos 1990 houve uma ameaça real à Internet
- Esgotamento de endereços IP (classe B)
- Naquele momento, a comunidade se movimentou e foram propostas 3 soluções:
  - IPv6: uma versão inteiramente nova do IP
  - CIDR: reorganização completa dos endereços disponíveis
  - NAT: estratégia para economizar endereços IP
- NAT e CIDR foram adotados em larga escala

# NAT: Solução de Segurança!

- Apesar de que a economia de endereços proporcionada pelo NAT foi essencial
- Ele vai permanecer quando a Internet for totalmente IPv6
- O motivo: NAT é uma solução de segurança
- Concretamente protege os hosts internos da rede
- Segurança é um dos maiores problemas da Internet (o maior?)

# Espaços de Endereçamento

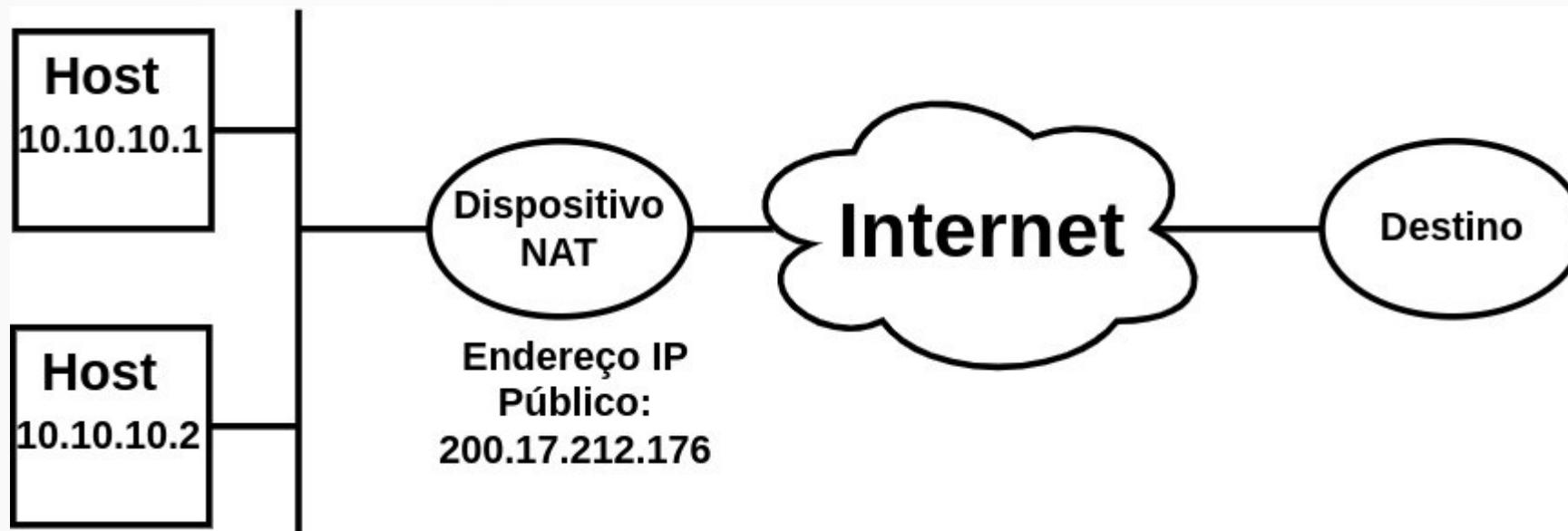
- Endereços públicos e privados
- A grande contribuição do NAT: permitir que hosts internos de uma organização tenham endereços inválidos
- Endereços privados, inválidos ou locais
- São não roteáveis, não são únicos na Internet
- Endereços públicos são válidos, roteáveis

# Endereços Inválidos

- A IANA reservou 3 faixas para endereços inválidos
- Usando notação com prefixo CIDR são:
- 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
- Todos os hosts da organização podem ter endereços inválidos!
- Mas observe que queremos que estes hosts possam se comunicar na Internet
- Devem ser capazes de transmitir/receber dados

# Dispositivos NAT

- Para permitir que os hosts com endereços inválidos se comuniquem, precisamos de um dispositivo NAT
- Fica na fronteira da rede privada e a Internet
- O dispositivo NAT deve ter um endereço público



# Dispositivo NAT

- Pulo do gato: para comunicar na Internet, todos os hosts usam o endereço público, válido do dispositivo NAT

# Dispositivo NAT

- Pulo do gato: para comunicar na Internet, todos os hosts usam o endereço público, válido do dispositivo NAT
- Quando um host interno com endereço inválido vai comunicar na Internet...
- ... os pacotes devem passar pelo dispositivo NAT, que substitui o endereço inválido pelo público
- Como se o próprio dispositivo NAT estivesse comunicando



# Sessão NAT

- Cada comunicação de host interno com a Internet é tratada pelo NAT como uma sessão
- O dispositivo NAT mantém todas as informações necessárias para possibilitar a comunicação
- O primeiro passo é substituir o endereço privado do host pelo endereço público do NAT
- Mas e se múltiplos hosts estiverem comunicando? Como identificar para quem é um pacote que chega?

# Para ser mais preciso: NAT

- Apesar de que ao longo da história diversos tipos de NAT surgiram, o mais comum é o NAT
- Network Address Port Translation
- Vamos continuar chamando de NAT simplesmente
- O NAT usa portas para identificar as sessões NAT
- Assim que um novo host comunica, assinala uma porta disponível para todos os pacotes que serão transmitidos na Internet

# Porta Identifica Sessão NAT

- Quando retorna um pacote da Internet...
- ... basta olhar a porta para saber quem é o destinatário “de verdade” na rede interna
- Observe que há uma restrição importante:
- A sessão NAT é criada quando o host interno transmite o 1º pacote
- Assim: toda comunicação deve ser iniciada internamente
- Servidores devem ter endereços válidos

# Um Conceito Importante: DMZ

- DMZ: *DeMilitarized Zone*
- Nem todo recurso pode ficar “escondido” atrás do NAT, por exemplo o servidor Web de uma organização
- Mais: servidor de nomes, de e-mail, entre outros
- A rede interna fica protegida: todo acesso só pode partir dela e a comunicação vai passar por firewall, dispositivo NAT, etc.

# Tabela de Sessões NAT

- 1) Tipo da Sessão (UDP ou TCP)
- 2) Estado da Conexão TCP (importante para, por exemplo, detectar encerramento)
- 3) ip\_local do host que iniciou a comunicação
- 4) porta\_local do processo interno
- 5) ip\_destino
- 6) porta\_NAT que identifica a sessão, usada para comunicação externa
- 7) ip\_externo sendo usado (quando tem +D1)
- 8) temporizador: permite identificar sessões silenciosas

# Completando o NAT

- Além de fazer as trocas de endereço IP e porta, o dispositivo NAT deve recalcular o checksum

# O Protocolo IPv6

- Uma nova versão do protocolo IP

# O Protocolo IPv6

- Uma nova versão do protocolo IP
- Nova??? Já tem quase 30 anos 
- RFC 2460, hoje RFC 8200
- Motivação também esgotamento do IPv4
- Aumento de 32 para 128 bits → definitivo!
- O número de endereços por metro quadrado do planeta
- $2^{128}$  endereços ( $3,4 * 10^{38}$ ); Terra tem  $5,1 * 10^{14}$  metros quadrados →  $6.67 * 10^{23}$  endereços por metro quadrado do planeta

# Um Projeto Especial

- Além do endereço ser definitivo
- O protocolo também foi projetado para ser definitivo
- Como assim?

# Um Projeto Especial

- Além do endereço ser definitivo
- O protocolo também foi projetado para ser definitivo
- Ao invés de 1 header como nos demais protocolos, o pacote tem uma sequência variável de headers



# Campos do Header Básico

- Um header é o básico, sempre presente
- Os demais headers são chamados de “extension headers” (headers de extensão)
- Qual o primeiro campo do header básico do IPv6?

# Campos do Header Básico

- Um header é o básico, sempre presente
- Os demais headers são chamados de “extension headers” (headers de extensão)
- Qual o primeiro campo do header básico do IPv6?

Version	Traffic class	Flow label	
Payload length		Next header	Hop limit
Source address			
Destination address			

# Campos do Header Básico

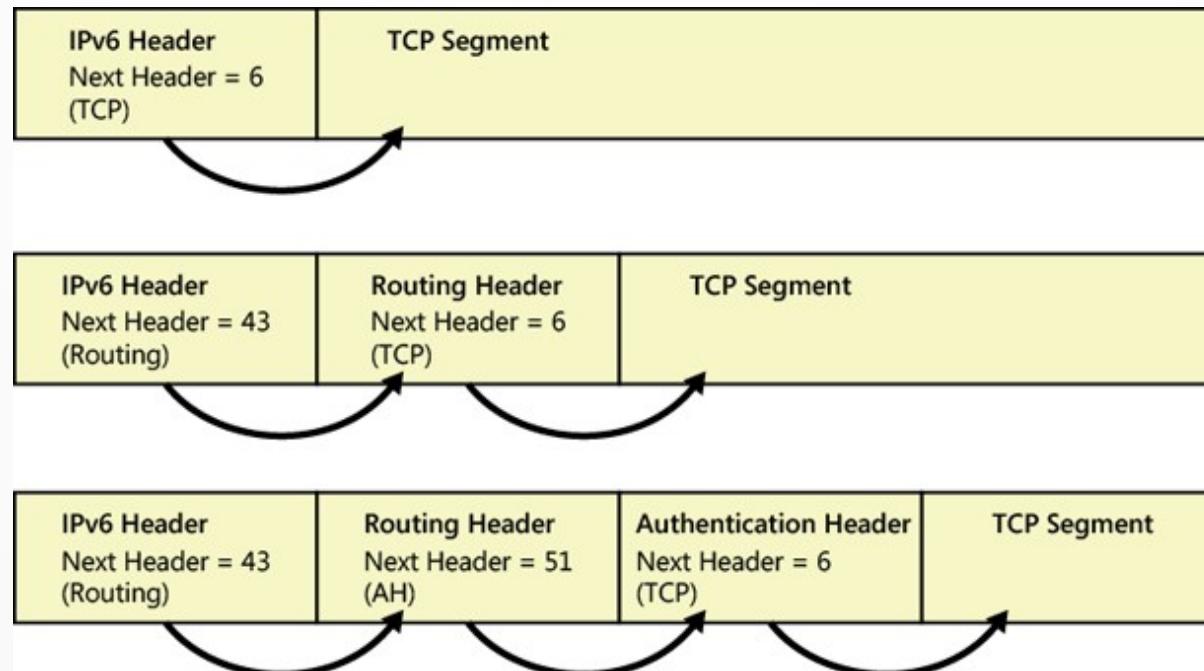
- Qual o primeiro campo do header básico do IPv6?
- Versão, 4 bits, exatamente igual ao IPv4
- Lembre-se: permite a co-existência de versões distintas do protocolo
- Classe de Tráfego: tratamento de QoS requerido
- *Flow Label*: identificador do fluxo

# Fluxos (Flows)

- Cada vez mais importantes na Internet
- A base de tecnologias modernas, como SDN (*Software Defined Networks*), em particular o OpenFlow
- Um fluxo é uma sequência de pacotes que tem em comum: (IP\_origem, Porta\_Origem, Protocolo, IP\_destino, Porta\_destino)
- A ideia é permitir que a rede trate fluxos, não pacotes individuais

# Headers IPv6

- Tamanho do Pacote: 16 bits
- Campo ProxHeader indica o header seguinte, se não for um *extension header* indica p.ex. TCP

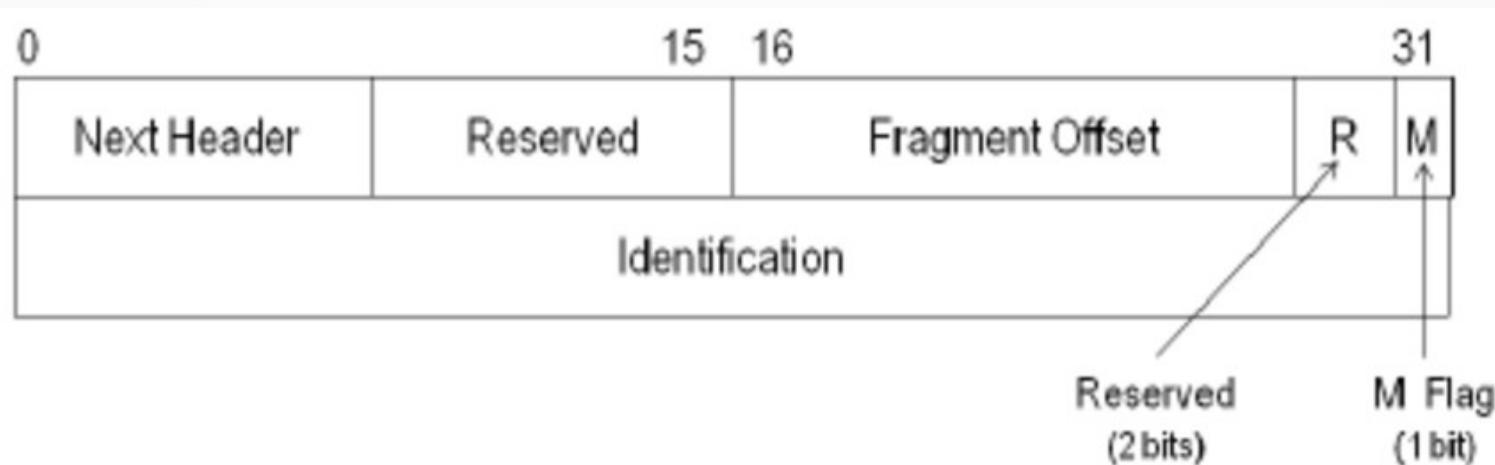


# Uma Discussão Relevante

- Fragmentação está em *extension header*
- É possível eliminar a fragmentação de uma versão futura do IP?

# Uma Discussão Relevante

- Fragmentação está em *extension header*
- É possível eliminar a fragmentação de uma versão futura do IP?
- Não! O IP deve poder ser usado sobre qualquer tecnologia, qualquer MTU, sempre é possível que haja necessidade de fragmentação



# Mais Campos do Header Básico

- ~~TTL~~ ops, mudou de nome: Hop Limit (8 bits)
- ~~Checksum~~: sumiu! Ficou para enlace e transporte
- Atenção: alguns extension headers são processados por todos os roteadores (hop-by-hop), outros só pelo destino (end-to-end)
- Os headers processados passo a passo devem vir antes

# Endereços IPv6

- Optou-se por hexadecimal (realmente fica mais compacto do que seria decimal)
- Cada par de bytes (16 bits) é representado por 4 hexas e separado por “:”
- Por exemplo:
  - 75A1:4A90:FFFF:FFFF:0:3280:87B:FFFF
- Não precisa representar zero a esquerda
- Além disso 1 sequência de zeros pode ser suprimida

# Suprimindo Sequência de Zeros

- Uma única sequência de zeros pode ser suprimida
- Por exemplo: 76B2:0:0:0:0:0:0:3280
- Fica assim: 76B2::3280

# Suprimindo Sequência de Zeros

- Uma única sequência de zeros pode ser suprimida
- Por exemplo: 76B2:0:0:0:0:0:0:0:3280
- Fica assim: 76B2::3280
- Se tiver duas sequências só uma pode
- Por exemplo: 76B2:0:0:AAAA:0:0:0:3280
- Fica assim: 76B2:0:0:AAAA::3280

# Suprimindo Sequência de Zeros

- Uma única sequência de zeros pode ser suprimida
- Por exemplo: 76B2:0:0:0:0:0:0:0:3280
- Fica assim: 76B2::3280
- Se tiver duas sequências só uma pode
- Por exemplo: 76B2:0:0:AAAA:0:0:0:3280
- Fica assim: 76B2:0:0:AAAA::3280
- Se fizer assim dá erro: 76B2::AAAA::3280
  - impossível saber quantos zeros tem cada uma

# Zeros no Início do Endereço

- Se os zeros estiverem no início do endereço basta começar com “::”
- Por exemplo → ::1284:FFFF
- Usando para especificar endereços IPv4 no mundo IPv6
- Por exemplo → ::200.17.212.176
- O IPv6 também permite o uso de prefixo CIDR
- Por exemplo: 35FF::A156:0:0:0:0/60

# Endereços Especiais

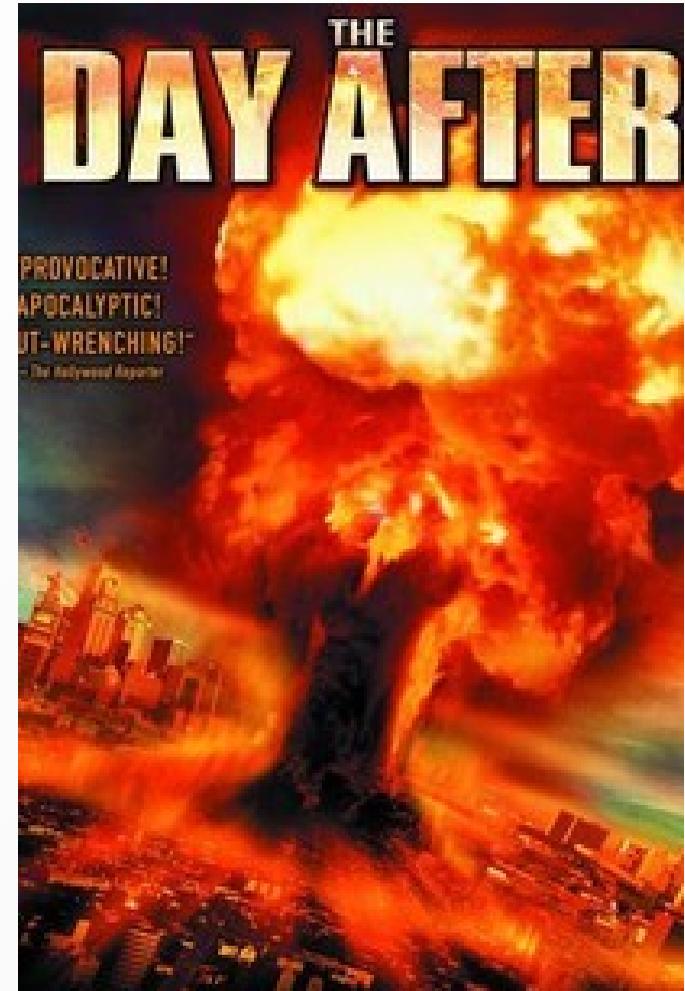
- Loopback IPv6 → 0::<1
- IPv6 oferece nativamente: broadcast, multicast, unicast (lógico né) e anycast
- Anycast: entrega para 1 membro do grupo
- Formato do endereço unicast:
  - NET-ID (“Prefixo de Roteamento Global”): N-bits
  - Subrede (64-N bits)
  - HOST-ID: 64 bits

# Como está a transição?

- Dados de 2020
- Aproximadamente 1 bilhão de endereços IPv6 alocados, o restante dos mais de 5 bilhões: IPv4
- Existe uma ameaça concreta de exaustão de IPv4, já aconteceu em partes (ICANN para Ásia há alguns anos esgotou)
- Uma hora vai haver a transição total!

# Um Pouco de História da Internet

- Anos 1960: Guerra Fria
- Uma ameaça real!
- Filme bom para compreender
- DARPA: Departamento de Pesquisa Avançada das Forças Armadas dos EUA
- Projeto: uma rede que sobrevivesse a um ataque nuclear



# 1º Passo: Comutação de Pacotes

- O Prof. Leonard Kleinrock da UCLA “inventa” comutação de pacotes
- Antes: redes baseadas em comutação de circuitos
- Colocada em prática: ARPANET entra em funcionamento em dezembro de 1969
- Construída pela empresa BBN (hardware/software)
- 4 nodos: UCLA, UCSB, SRI, University of Utah

# ARPANET

- Os roteadores daquele rede original: chamados IMPs (*Interface Message Processors*)
- Minicomputadores Honeywell com 12KB de memória
- Conectados por enlaces de 56Kbps
- Uma topologia com redundância: lembre-se da motivação original
- Nos anos seguintes: crescimento exponencial

# ARPANET: 1974



# Ao Mesmo Tempo...

- O DARPA estava fazendo pesquisa também em outros tipos de rede
  - redes baseadas em satélites
  - redes baseadas em rádio
  - outras tecnologias
- Surge naturalmente a necessidade interconectar redes de tecnologias diferentes
- Conceito de *internetworking*

# Protocolos TCP/IP Inventados

- Um esforço principalmente de universidades
- O DARPA financia também a implementação dos protocolos TCP/IP no BSD/UNIX
- Sopa no mel!
- Justamente naquela época universidades começavam a ter mais de um computador
- Necessidade de software de redes
- 10 entre 10 universidades americanas usavam BSD/UNIX

# NSFNET

- Paralelamente, nos anos 1970 a National Science Foundation criou uma rede de supercomputadores: NSFNET
- Conectando instituições em todos os EUA
- O Brasil também tem uma rede de supercomputadores: CENAPAD
- Centro Nacional de Processamento de Alto Desempenho
- Em Petrópolis: super computador Santos Dumont (LNCC)

# 1983

- Um ano fundamental na história da Internet
- Separa a MILNET, junta a NSFNET
- Protocolos TCP/IP: obrigatórios (antes experimentação possível)
- O DARPA deixa de ser o responsável
- DCA assume: *Defense Communications Agency*
- *Nome muda: Internet*

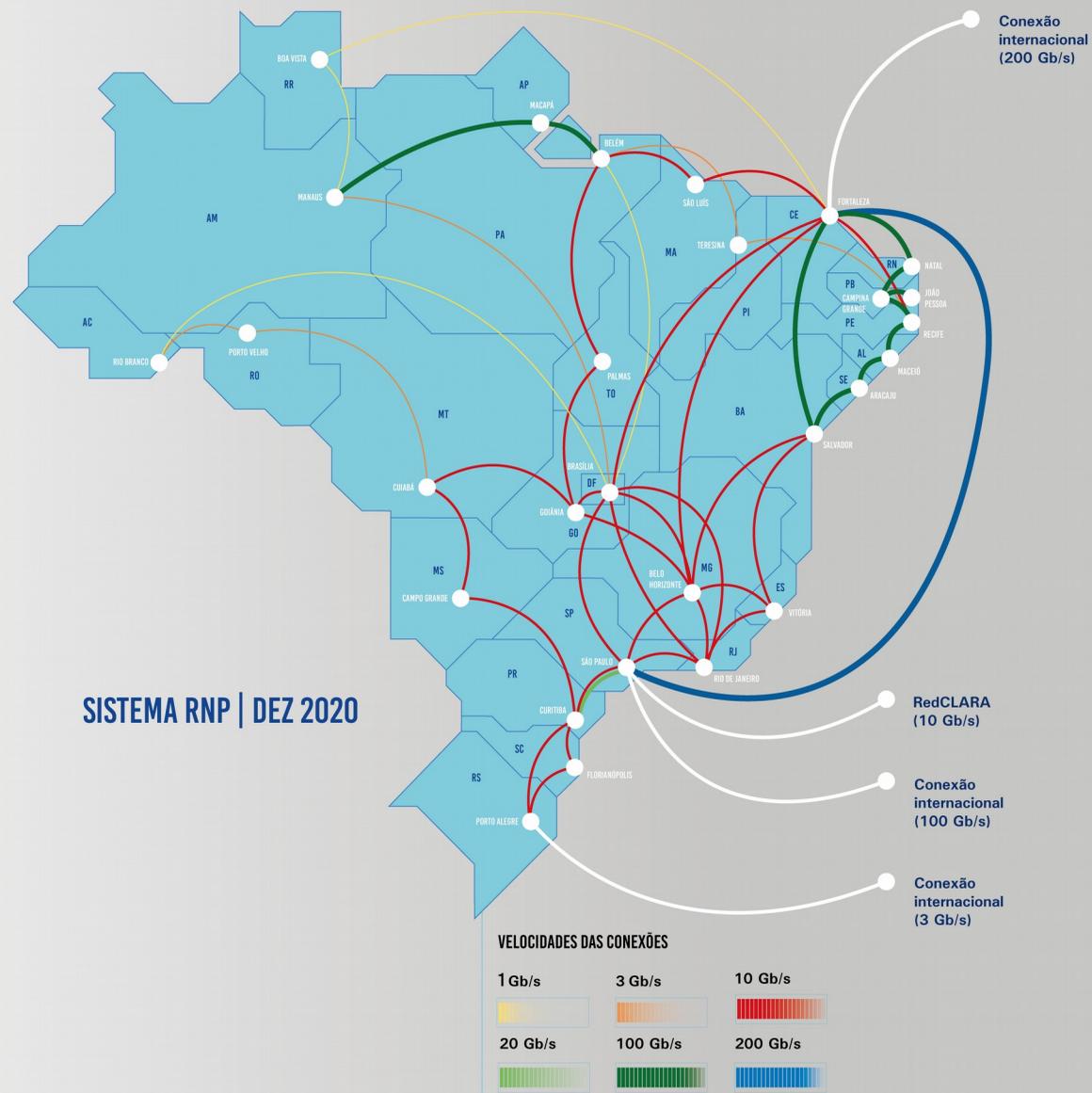
# Pressão de Entidades Comerciais

- Até este momento: basicamente universidades e empresas de alta tecnologia voltadas para a própria rede
- Entidades comerciais começam a pressionar para entrar na rede
- Uma organização se forma com um consórcio de empresas (IBM, MCI, ...): ANS (*Advanced Networks and Services*)
- A ANS obtém o controle do backbone da NSFNET: ANSNET
- Se transforma em AOL: America OnLine

# 1992

- Outro ano fundamental para a Internet
- As forças armadas americanas deixam o controle da rede
- Criada a Internet Society
- Diversas empresas passam a oferecer serviço IP comercial
- Internet chega no Brasil! Um dos Pontos de Presença originais da RNP – Rede Nacional de Ensino e Pesquisa
  - [www.rnp.br](http://www.rnp.br)

# Backbone da RNP: Rede Ipê



# A partir de então

- Crescimento continuou exponencial
- Hoje (julho de 2021) são mais de 5 bilhões de pessoas conectadas em todo o mundo
- Grandes avanços ainda estão por vir
- Internet das Coisas (IoT - *Internet of Things*), tecnologia 5G, redes virtualizadas, redes baseadas em software, etc. etc. etc.

# Conclusão

- Nossa aula de hoje teve 3 partes
  - NAT
  - IPv6
  - História da Internet
- Muitos, muitos recursos disponíveis na própria Internet sobre estes tópicos: agora é com vocês!

**Obrigado!**

Lembrando: a página da disciplina é:  
<https://www.inf.ufpr.br/elias/redes>