Infraestrutura Computaciona III

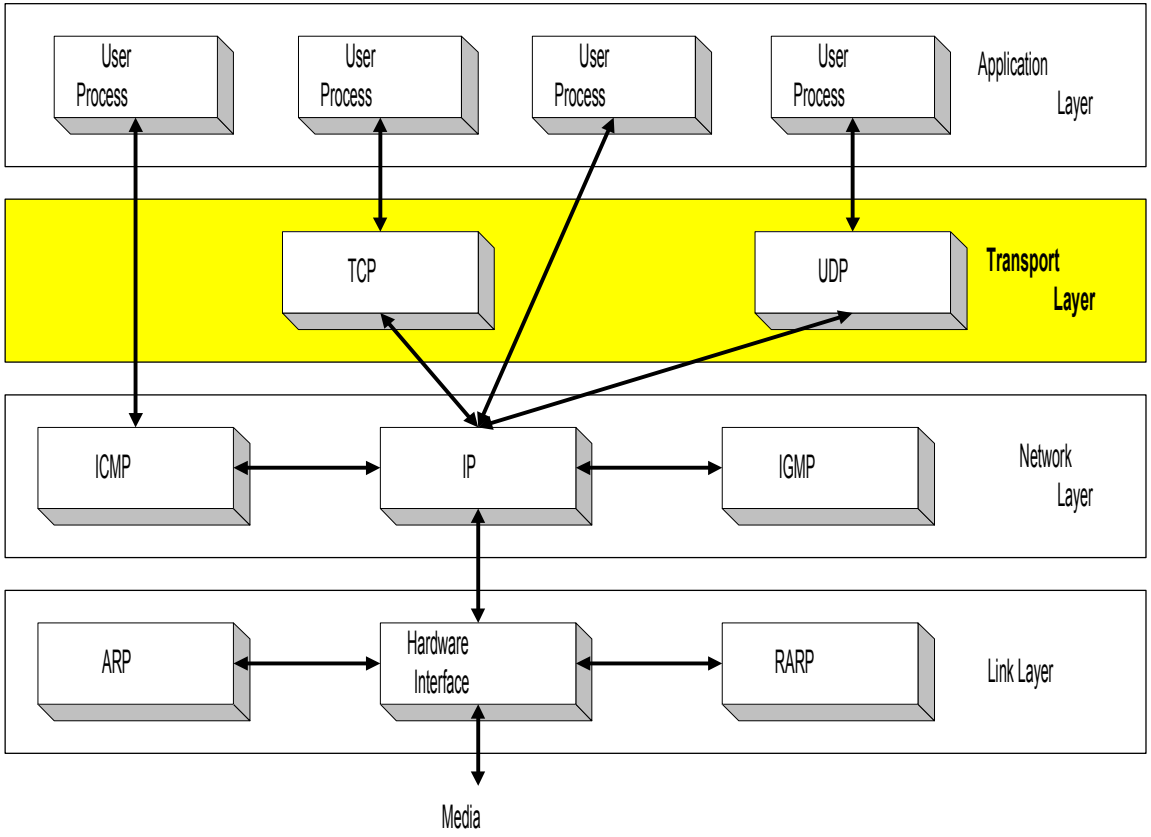
Internet Camadas de Rede e Transporte
Cloud Computing

Luis C.E. Bona (bona@inf.ufpr.br)

Slides parcialmente baseados no livro:

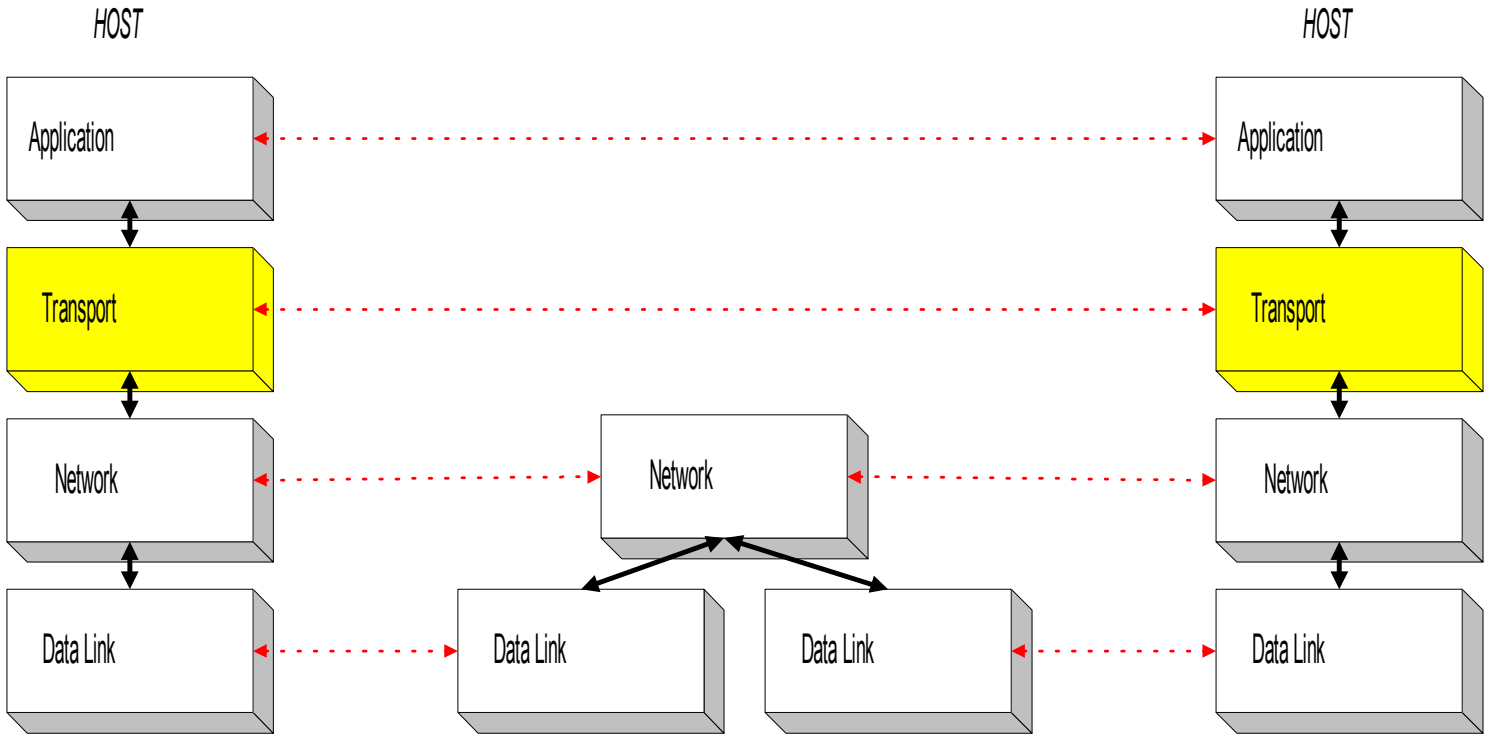
Computer Networking: A Top Down Approach. Jim Kurose, Keith Ross

Visão Geral


User Process
User Process
User Process
User Process
Application Layer
TCP
UDP
Transport Layer
ICMP
IP
IGMP
Network Layer
ARP
Hardware Interface
RARP
Link Layer
Media

Visão Geral

- É implementando fim-a-fim (somente nos “hosts”)



Protocolos de Transporte TCP/IP

UDP - User Datagram Protocol

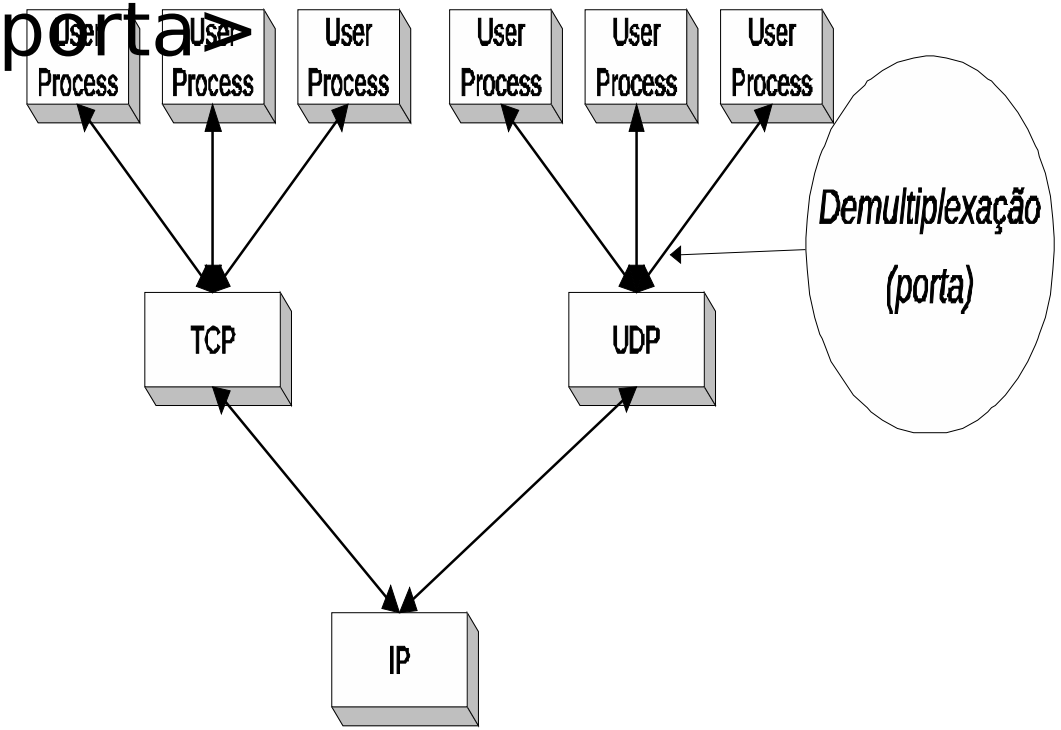
- Datagramas
- Não confiável, sem conexão
- Simples
- Usado em situações especiais
  - DNS, Voz, Tempo-Real,

TCP - Transmission Control Protocol

- Stream de bytes (dividido em segmentos)
- Confiável, orientado a conexão
- Complexo
- Usado na maioria das aplicações (mais simples para o programador)
  - Http, smtp, ftp, ssh, ….

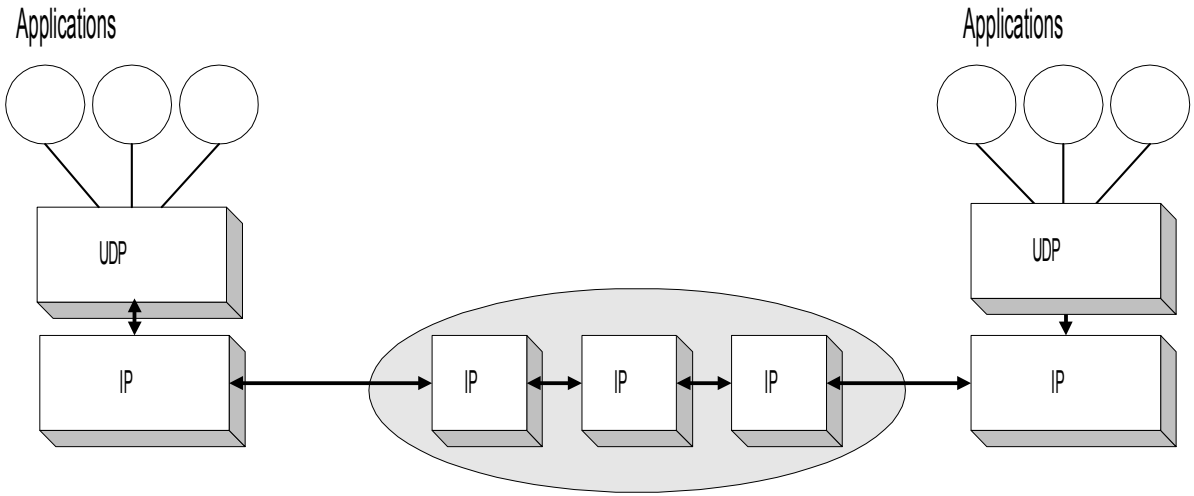
Número de portas

- Portas identificam aplicações (processo no host)
- Um endereço na camada de transporte é uma tupla <IP,porta>

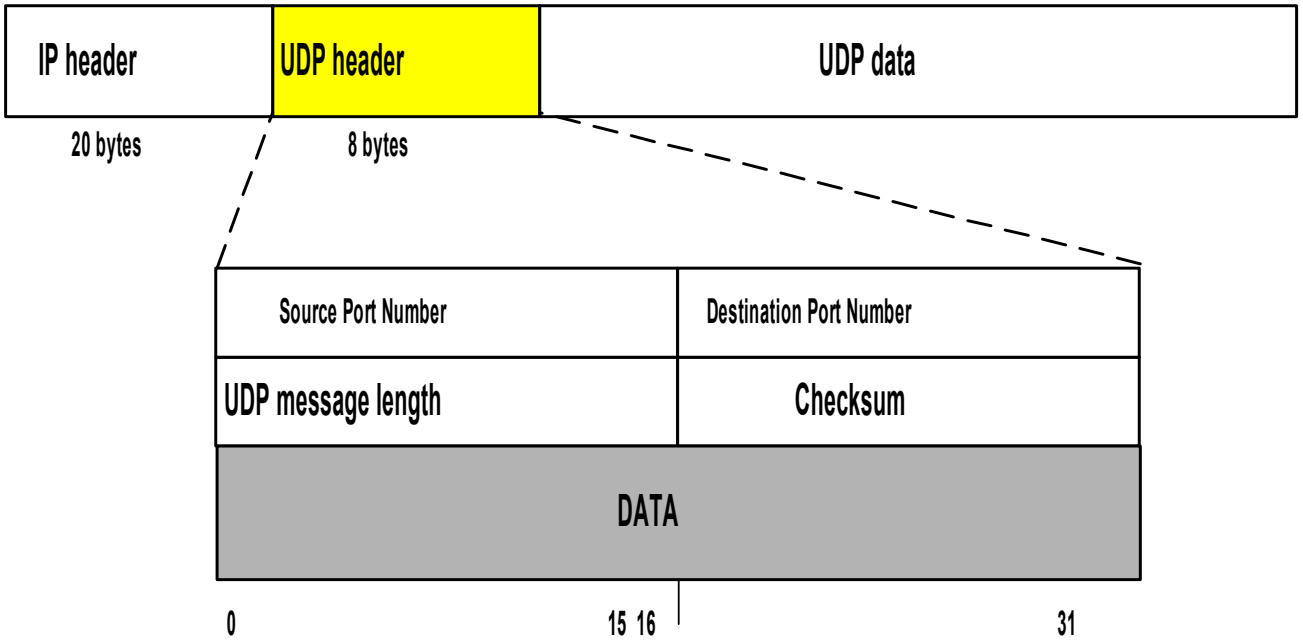


UDP - User Datagram Protocol

- UDP oferece como serviço apenas comunicação não segura de *datagramas*
- UDP estende o serviço host-to-to-host da camada IP para um serviço aplicação-aplicação (ponta-a-ponta)
- Apenas inclui portas (multiplexação e demultiplexação)



Formato UDP



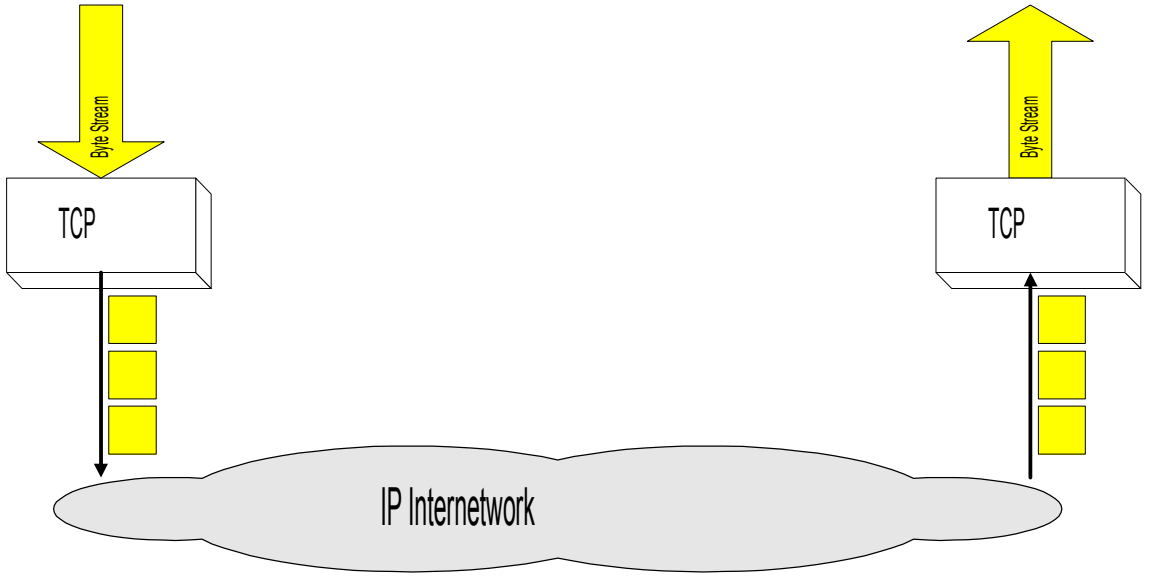
- **Número de Porta** (2^{16}-1= 65,535)
- **Tamanho da Mensagem** máximo 65,535 (~64K)
- **Checksum**

TCP

Visão Geral

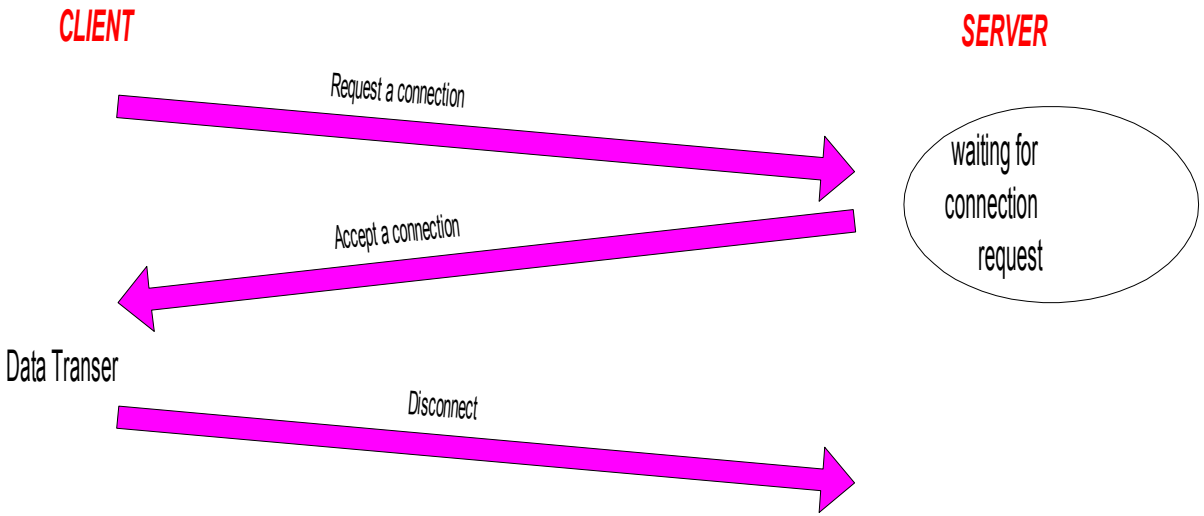
TCP (Transmission Control Protocol)

- Orientado a conexção
- Serviço confiável de comunicação de stream de bytes fim-a-fim sobre uma rede não confiável



Orientado a Conexão

- Antes de qualquer transmissão de dados é necessário realizar a conexão
- Uma vez conectado a comunicação é full-duplex



Confiável

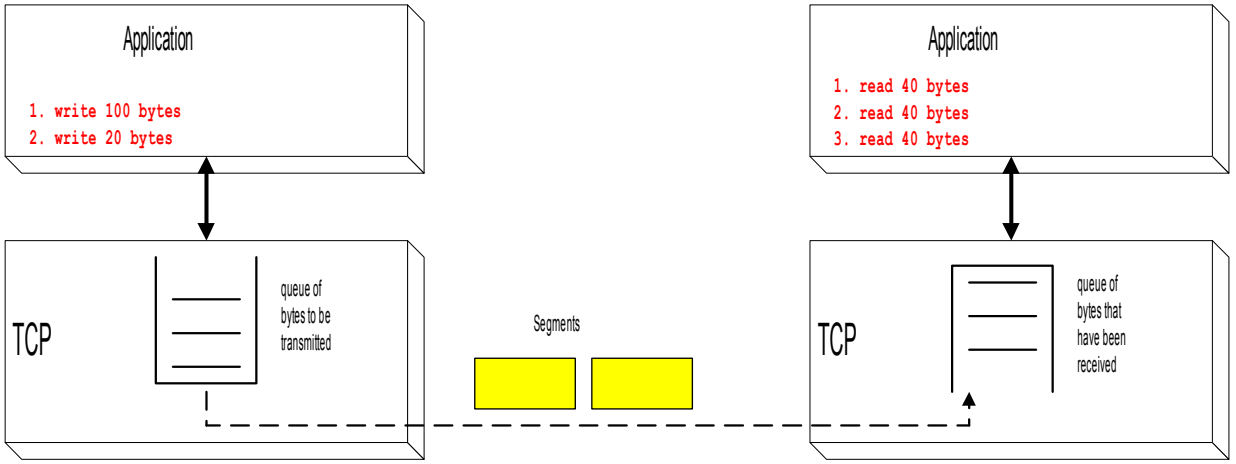
- O stream de bytes é quebrado em pedaços chamados segmentos

- Utiliza o conceito de Janelas Deslizantes para Controle de Fluxo e Erro

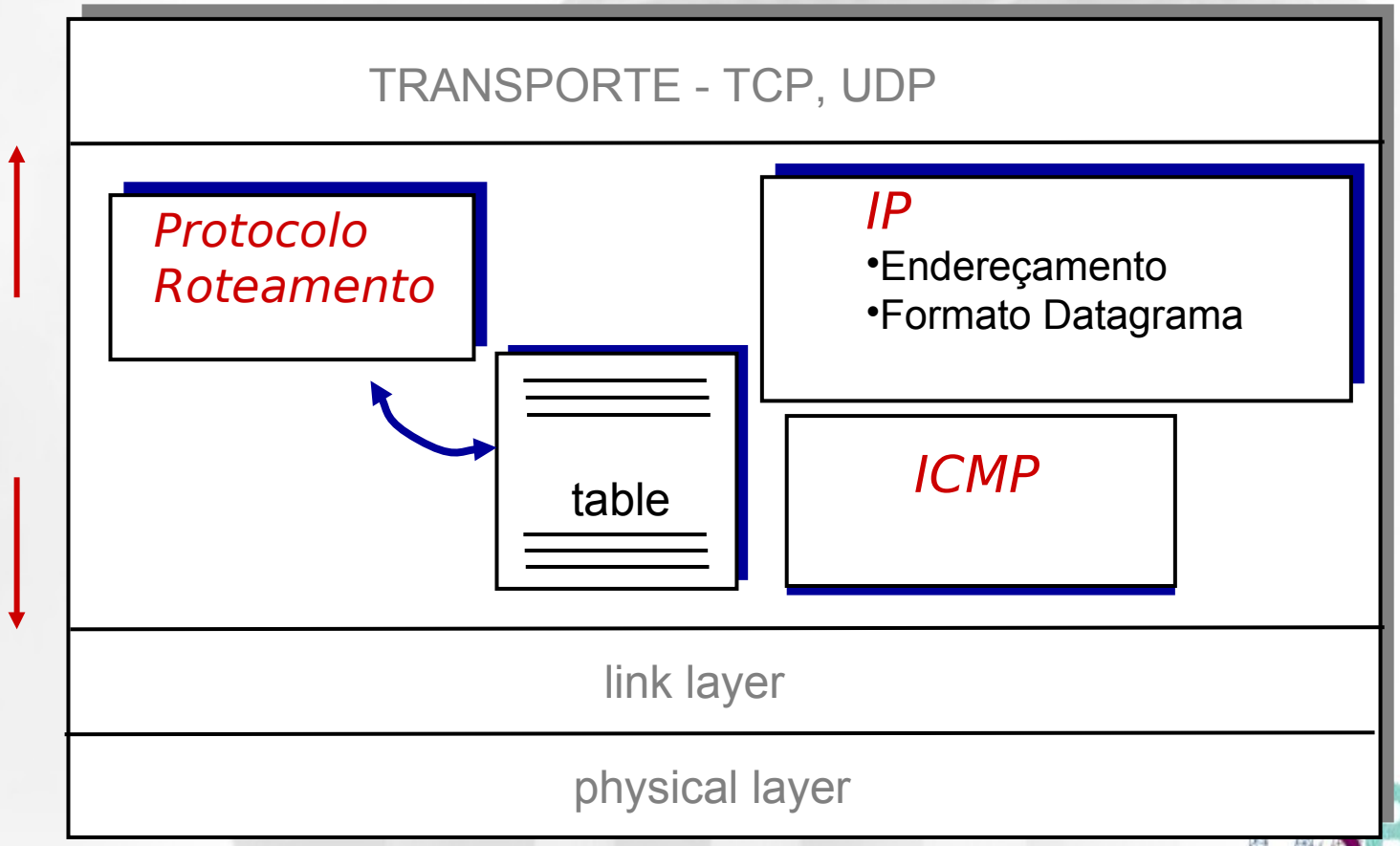
- Para quem utiliza o serviço é como a rede fosse livre de erros

Serviço de Stream de Bytes

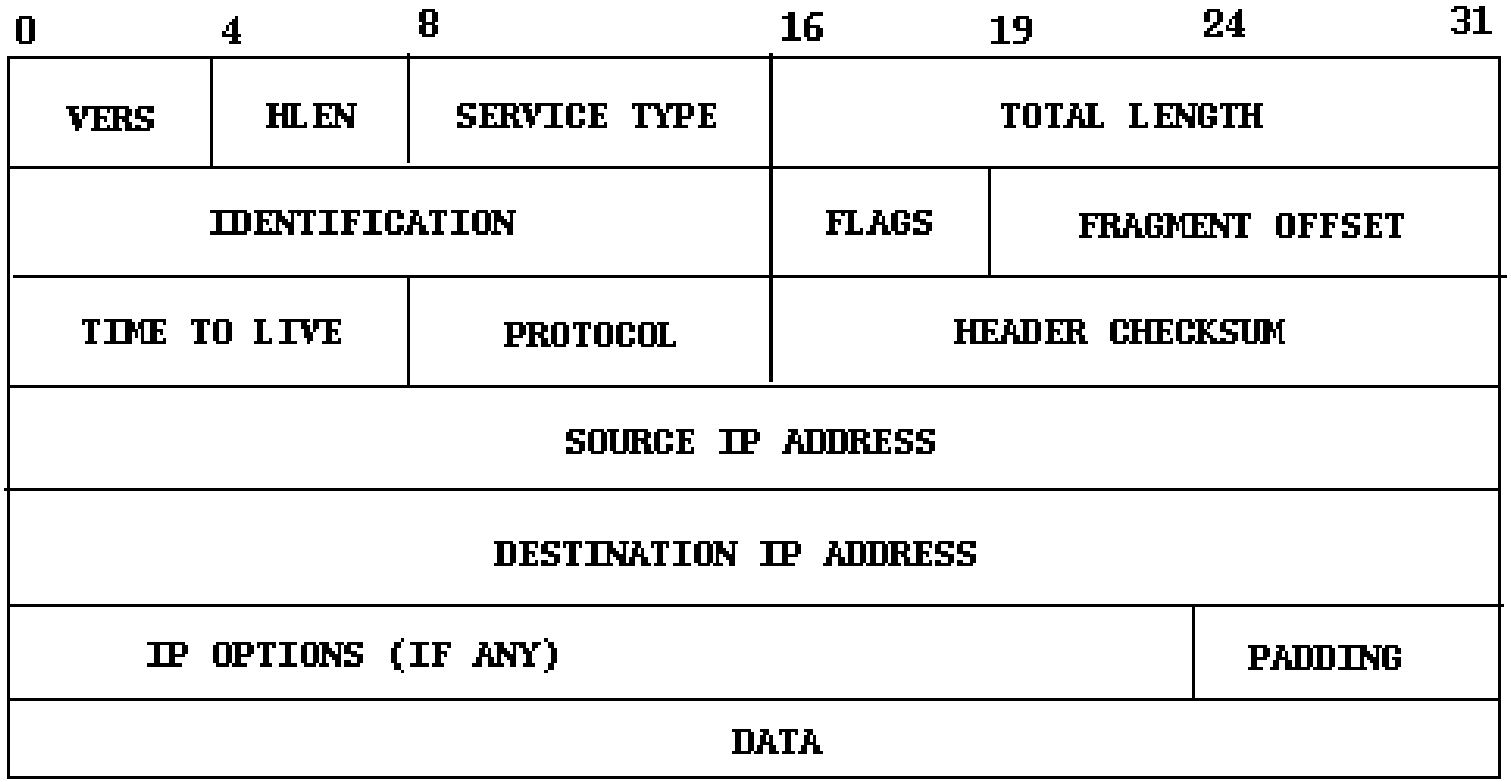
- TCP trata os dados como uma sequência de bytes sem identificar limites. As aplicações não sabem nada sobre início ou fim de segmentos.



Camada de Internet



Como é um datagrama?



Endereçamento IPv4

- ENDEREÇO
  - 32 bits, representado por 4 octetos
  - Classes
    - A 0.0.0.0 até 127.0.0.0
    - B 128.0.0.0 até 191.255.0.0
    - C 192.0.0.0 até 223.255.255.0
  - Endereços Privados
    - 10.0.0.0 - 10.255.255.255
    - 172.16.0.0 - 172.31.255.255
    - 192.168.0.0 - 192.168.255.255

Endereçamento IPv4

- INTERFACE
  - Conexão física entre host/roteador e a ligação física
- Um endereço especial é 127.0.0.1
- Configurar a rede, minimanente envolver:
  - Configurar o endereço IP
  - Configurar a rede e máscara
  - Roteadores
- Manual (arquivos) ou automático (DHCP)

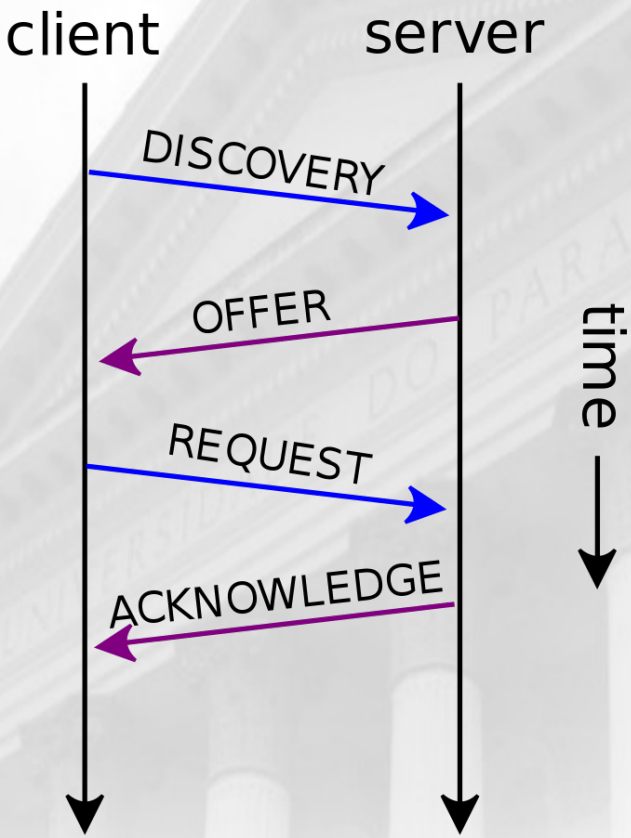
Configuração IP

- Comandos tradicionais:
  - ifconfig e route
- Agora
  - ip addr, ip link; ip route
- Configurações
  - *Old School*
    - */etc/network/interfaces*
  - *Desktop modernos*
    - *Utiliza Network Manager*

DHCP

- Dynamic Host Control Protocol (DHCP)
  - Conectar um host na Internet requer a configuração de vários parâmetros: gateway, endereço e máscaras de rede, servidor de dns, etc...
  - Boa parte dos hosts obtém esses endereços automaticamente da rede através do DHCP

DHCP



DHCP

- Você pode observar os logs de interação do seu host com o DHCP
- Procure por `dhclient` no arquivo *`/var/log/daemon.log`*
- Normalmente os servidores de DHCP oferecem configurações de duas maneiras:
  - Estática, considerando o endereço físico da interface de rede (no exemplo acima `00:16:c8:ec:2f:fc`)
  - Dinâmica, oferecendo endereços de forma independente do endereço físico (ISP, são um exemplo)

ICMP

- Usando pelo host e roteadores para se comunicarem na camada de rede
- Utiliza o protocolo IP

Type	Code	description
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

DSBD

Ping e Traceroute

```
bona@swamp:~$ route -n
Tabela de Roteamento IP do Kernel
Destino         Roteador        MáscaraGen.     Opções Métrica Ref    Uso
Iface
0.0.0.0         10.254.222.3    0.0.0.0          UG    100    0        0
enp7s0f0
10.254.222.0    0.0.0.0         255.255.255.0    U     100    0        0
enp7s0f0
169.254.0.0     0.0.0.0         255.255.0.0      U     1000   0        0
enp7s0f0
bona@swamp:~$ ping 10.254.222.3
PING 10.254.222.3 (10.254.222.3) 56(84) bytes of data.
64 bytes from 10.254.222.3: icmp_seq=1 ttl=64 time=0.177 ms
64 bytes from 10.254.222.3: icmp_seq=2 ttl=64 time=0.160 ms
^C
--- 10.254.222.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1006ms
rtt min/avg/max/mdev = 0.160/0.168/0.177/0.015 ms
bona@swamp:~$
```

- Ferramenta mais básica de diagnóstico de rede

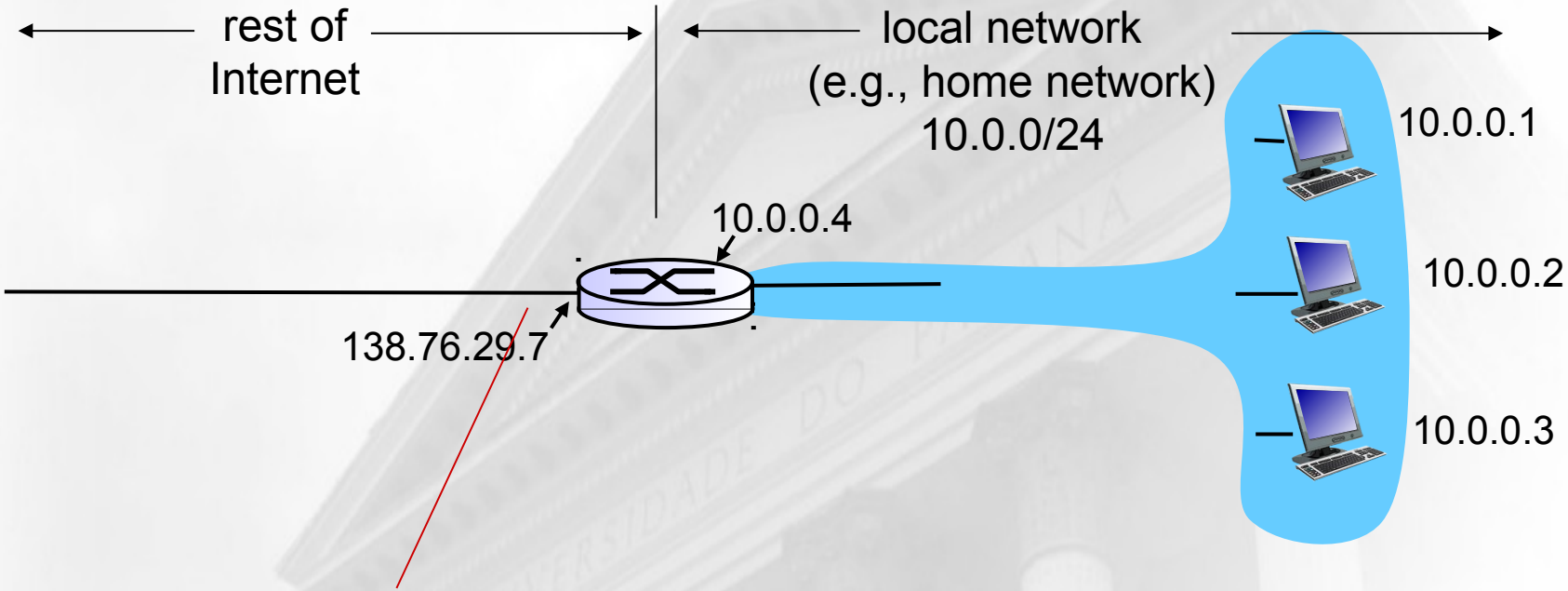
Ping e Traceroute

- PING
  - Além da conectividade oferece estatísticas de pacotes perdidos e latência
- TRACEROUTE/TRACEPATH
  - Mostra os caminhos feitos na camada de Internet pelo pacotes
  - Utiliza o TTL

NAT: Network Address Translation

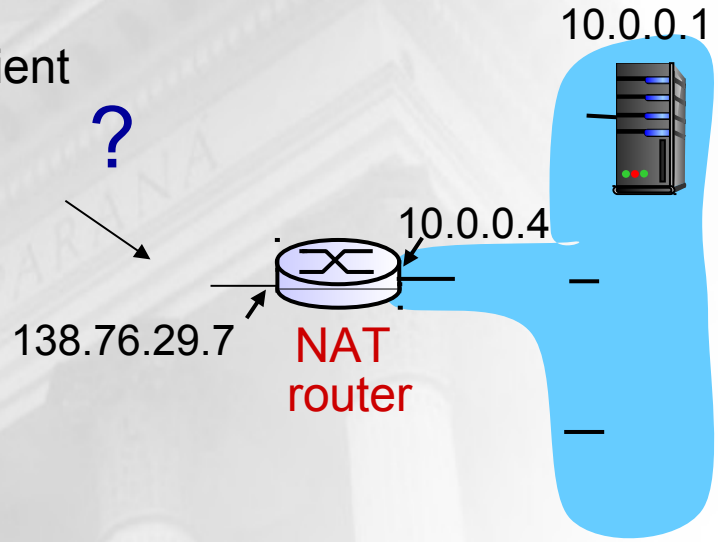
- Solução para o esgotamento do IPv4
- Mas mesmo com o IPv6 sendo instado continua resistindo
- Permite que uma rede local utilize apenas um endereço IP para se identificar externamente
- Esquemas de virtualização de rede simples são baseados em NAT
  - As alternativas envolvem *bridges*, que são interfaces virtuais.

NAT


rest of
Internet
local network
(e.g., home network)
10.0.0/24
10.0.0.1
10.0.0.4
10.0.0.2
138.76.29.7
10.0.0.3

NAT

- Um problema é “atravessar” o NAT



NAT

- Soluções para as máquinas internas
  - Configurar um encaminhamento estático de uma porta do IP válido para um IP/porta interno
  - Encaminhamento dinâmico usando UPnP (se suportado pelo roteador). Comum nos roteadores atuais
  - Utilização de intermediários

Firewall

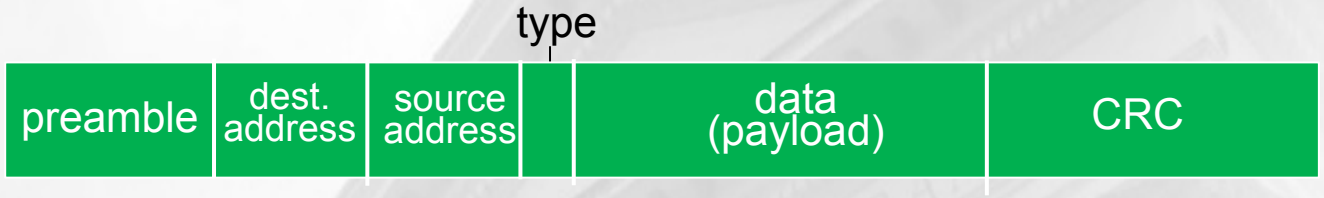
- Um firewall é basicamente um filtro de pacotes operanda na camada de Internet e Tranposrte
- Executado nos roteadores oferecendo proteção entre diferentes redes
  - Não protege máquinas da mesma rede
  - Mas um host pode executar um FW apenas para se proteger de outras máquinas na rede
- Uma política simples é não permite a entrada de nenhum tráfego a não ser os das requisições estabelecidas

Redes locais

- Padrões dominantes para redes com fio (802.3) e sem fio (802.11)
- O padrão 802.3 também é conhecido como Ethernet
  - Engloba diferentes meios físicos e velocidades de transmissão (no início 10Mbps agora passando de 40Gbps)
- O protocolo pouco mudou nos últimos anos, até podemos dizer que foi simplificado

Ethernet

- Formato do Frame

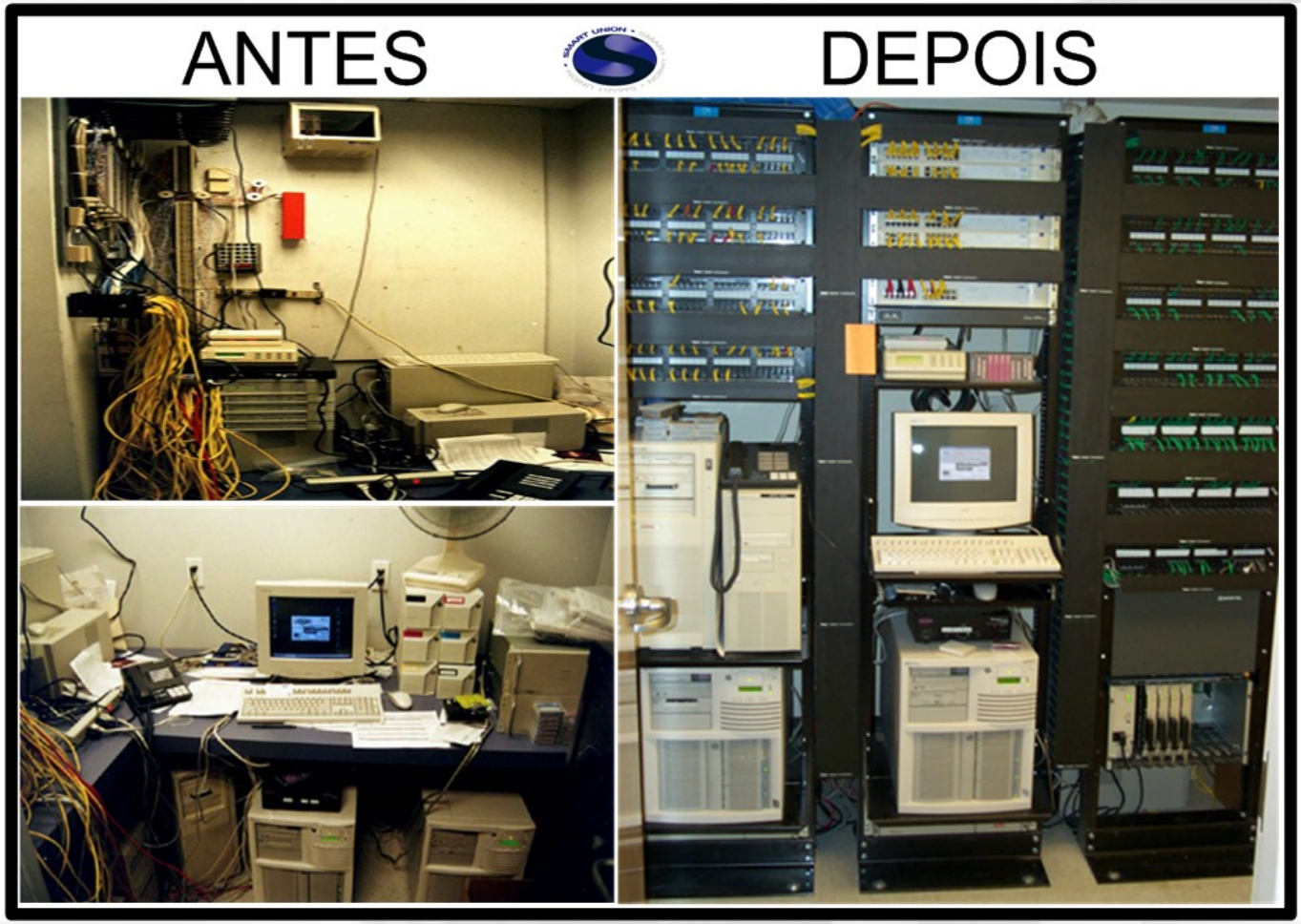


- O padrão ainda é o inicial de 1500 bytes
  - Existe a possibilidade de usar jumboframes
- Os endereços são de 6 bytes, representados em hexa:
    - 70:85:c2:08:88:ba
  - E são únicos no mundo

Ethernet Switch

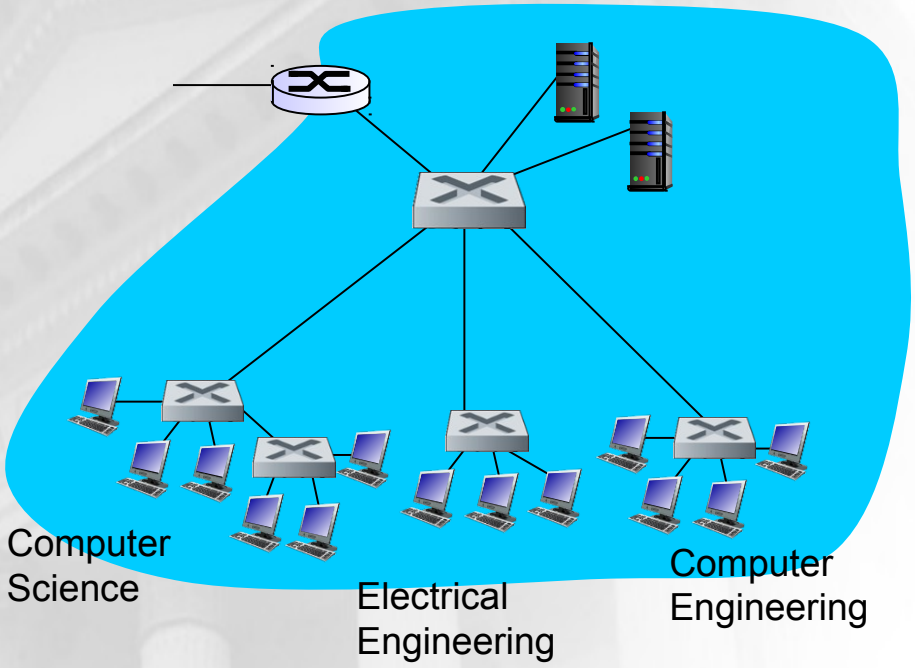
- Diferente de um roteador não fala IP, ou seja, encaminha somente baseado no MAC ADDRESS
- Não faz roteamento, apenas “aprende” os endereços físico acessíveis através de cada porta
- Podemos interligar vários switches, mas eles formaram uma única rede vendo todos frames

Cabeamento Estruturado



VLANs

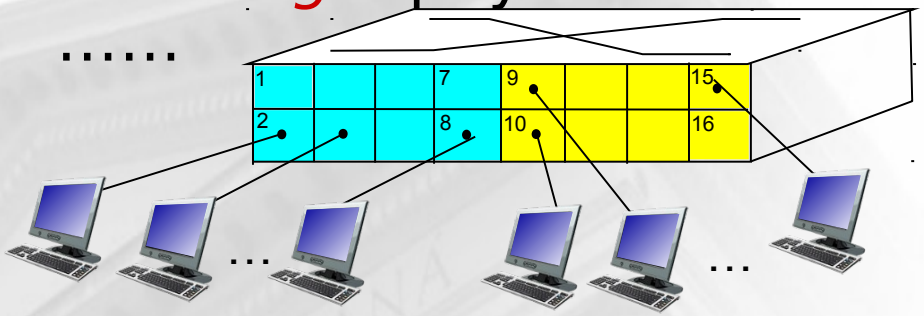
- Ter uma única rede ethernet gera dois problemas
  - Único domínio de broadcast
  - Isolamento de tráfego
  - Segurança e privacidade



VLANs

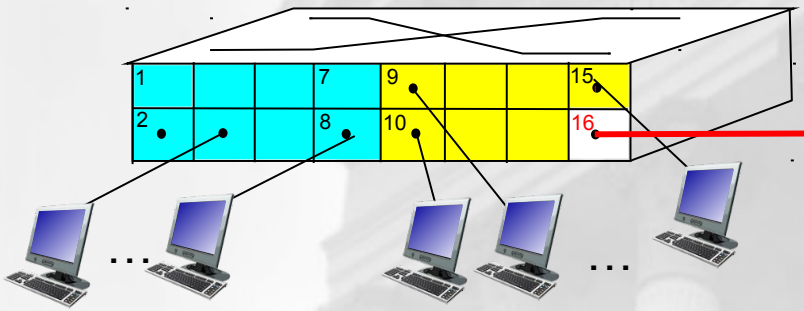
- Criação de VLANs
  - Redes Virtuais
  - Baseadas em portas
  - Baseadas em TAGs (coloridas)

port-based VLAN: switch ports grouped (by switch management software) so that *single* physical switch ……



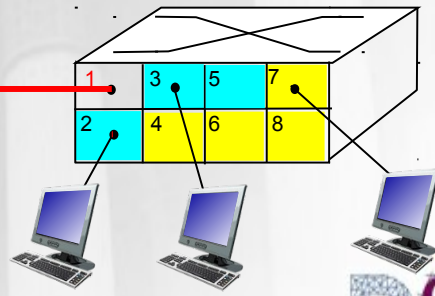
Electrical Engineering (VLAN ports 1-8)

Computer Science (VLAN ports 9-15)



Electrical Engineering (VLAN ports 1-8)

Computer Science (VLAN ports 9-15)



Ports 2,3,5 belong to EE VLAN
Ports 4,6,7,8 belong to CS VLAN

Nuvens Computacionais

- Evolução dos modelos computacionais
  - Do mainframe para o PC
  - Década de 90 dominada pelo paradigma Cliente-Servidor
  - Sucesso da Internet e primeiras aplicações distribuídas em larga escala
  - Surgimento do modelo de *Cloud Computing*

Nuvens Computacionais

- Outros fatores
  - Economia de Escala
  - Sistema e software mais complexo
  - Dificuldades de manutenção de infraestrutura
    - Tanto física como lógica
  - Dispositivos móveis com recursos *escassos*

DSBD

Definição de computação em nuvem

- Um modelo para provisionar através da rede recursos computacionais (rede, tempo de processamento, aplicações, armazenamento, etc) sob demanda de forma escalável e elástica com esforço de gerência reduzido
- Na definição do NIST são dados 5 caracteristícas essenciais, 3 modelos de serviço e 4 modelos de implantação

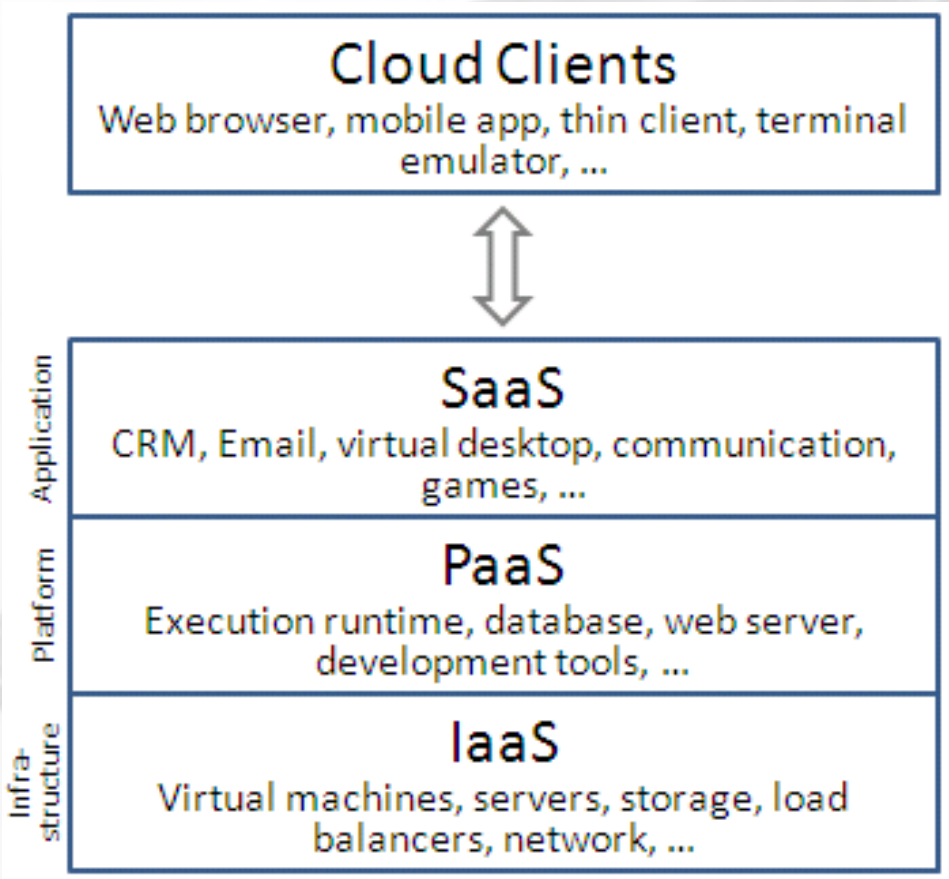
Características

- Auto-serviço sob demanda
- Amplo acesso a rede
- Reunião de recursos (*resource pooling*)
- Elasticidade rápida
- Serviços mesuráveis

Modelo de Serviço

- Principais modelos:
  - Software as a Service (SaaS)
  - Platform as a Service (Paas)
  - Infrastructure as a Service (Iaas)
- Mas pode ser um XaaS
  - Payments as a Service
  - Maps as a Service
  - Storage as a Service

Camadas


Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
Application
SaaS
CRM, Email, virtual desktop, communication, games, ...
Platform
PaaS
Execution runtime, database, web server, development tools, ...
Infra-structure
IaaS
Virtual machines, servers, storage, load balancers, network, ...

Termos de serviço

- SLA (Service Level-Agreement) que normalmente compreende:
  - Disponibilidade
  - Compensações por falhas de desempenho
  - Condições de preservação dos dados
  - Proteção legal das informações do assinantes
- Limitações do SLA
  - Interrupções programadas
  - Eventos de força maior
  - Mudanças no SLA
  - Segurança
  - Mudança na API

SaaS

- Software distribuído como serviço, hospedado e acessado via Internet
- Tipicamente se cobra pelo número de usuários, tempo de uso, por execução ou registros processados, banda de rede ou quantidade de dados armazenados
- A maior parte da lógica de negócio é executado no provedor de nuvem
- O acesso é feito por credenciais pelos usuários finais
- Questão chave é que a aplicação deve escalar conforme a necessidade do assinante

DSBD

SaaS - Vantagens

- Footprint das ferramentas de software é muito pequeno
- Uso eficiente de licensas de Software
- Dados e gerenciamento centralizado (do ponto de vista do usuário)
- Tarefa de gerência da plataforma é dos provedores

SaaS – Riscos e questionamentos

- Riscos relacionados ao navegador de Internet
- Dependência de rede
- Custo pode ser um problema
- Isolamento vs Eficiência
- Manter cópia dos dados

SaaS

- Em geral mais adequado para
  - Lógica de negócio
  - Colaboração
  - Ferramentas de produtividade
- Complicado para
  - Aplicações de tempo real e críticas
  - Volume massivo de dados

SaaS

- Exemplos
  - Google Apps
  - Salesforce
  - Wordpress
  - SurveyMonkey
- Visualização a analytics tem se tornado popular
  - Plot.ly
  - ...

Exemplos locais

- https://dadoseducacionais.c3sl.ufpr.br
- https://transparencia.c3sl.ufpr.br

PaaS

- Oferece ferramentas para o desenvolvimento, implantação e administração de software
- Projetado para suportar um grande número de assinantes e processar grandes quantidades de dados
- Em geral acessado de qualquer lugar da Internet
- Utilizado por: desenvolvedores, implantadores, administradores e usuários finais
- Cobrança depende do tipo de usuários ou do tipo de recurso consumido

PaaS - Vantagens

- Facilitar o desenvolvimento e a implementação de aplicações escaláveis
- Tanto para prover processamento e armazenamento como para
- aplicações completas via navegador
- Permite escrever aplicações que operam adequadamente mesmo sob grande variação na demanda
- Pode ajudar a melhorar a qualidade de desenvolvimento

PaaS – Riscos

- Falta de portabilidade entre os diferentes provedores PaaS
  - Por exemplo, openstreemaps vs googlemaps
- Engenharia de segurança
  - A aplicação é naturalmente exposta

Paas

- Muitos exemplos interessantes. Alguns bastante simples
  - CEP, Endereços, Mapas, análise de dados, gráficos, URBS, ...

Paas

```
bona@swamp:~$ wget http://api.postmon.com.br/v1/cep/81530980
--2018-05-11 13:08:25--
http://api.postmon.com.br/v1/cep/81530980
Resolvendo api.postmon.com.br (api.postmon.com.br)...
104.31.64.254, 104.31.65.254, 2400:cb00:2048:1::681f:41fe, ...
Conectando-se a api.postmon.com.br (api.postmon.com.br)|
104.31.64.254|:80... conectado.
A requisição HTTP foi enviada, aguardando resposta... 200 OK
Tamanho: não especificada [application/json]
Salvando em: “81530980”

2018-05-11 13:08:25 (6,05 MB/s) - “81530980” salvo [304]

bona@swamp:~$ cat 81530980
{"bairro": "Jardim das Am\u00e9ricas", "cidade": "Curitiba",
"logradouro": "Avenida Nossa Senhora de Lourdes, 779",
"estado_info": {"area_km2": "199.307,985", "codigo_ibge": "41",
"nome": "Paran\u00e1"}, "cep": "81530980", "cidade_info":
{"area_km2": "435,036", "codigo_ibge": "4106902"}, "estado":
"PR"}
```

Geocoding

- `http://maps.google.com/maps/api/geocode/json?address=centro+politecnico+ufpr`

OpenStreetMaps

- `http://openstreetmap.c3sl.ufpr.br/osm/0/0/0.png`

SIMMC

- Coleta dados dos projetos de inclusão digital
- Oferece uma API
- http://simmc.c3sl.ufpr.br/#/opendata
- http://simmc.c3sl.ufpr.br/api/opendata/data/json?metrics=Banda%20contratada%20m%C3%A9dia%20(upload)&dimensions=C%C3%B3digo%20IBGE%2CNome%20da%20cidade%2CRegi%C3%A3o&filters=Cidade%20digital%3D%3Dtrue

Dados abertos EU

- http://data.europa.eu/euodp/en/developerscorner
- http://data.europa.eu/euodp/en/linked-data

Plot.ly

- https://plot.ly/python/line-charts/

IaaS

- Oferece acesso a recursos computacionais virtualizados:
- Computadores, armazenamento e componentes de rede
- O assinante típico deste tipo de serviço é administrador de sistemas
- A tarifação é tipicamente por hora (CPU, armazenamento erede)
- Pode incluir algum tipo de serviço agregado como:
  - monitoração e gerencia de desempenho
- É o serviço base para construir PaaS e SaaS

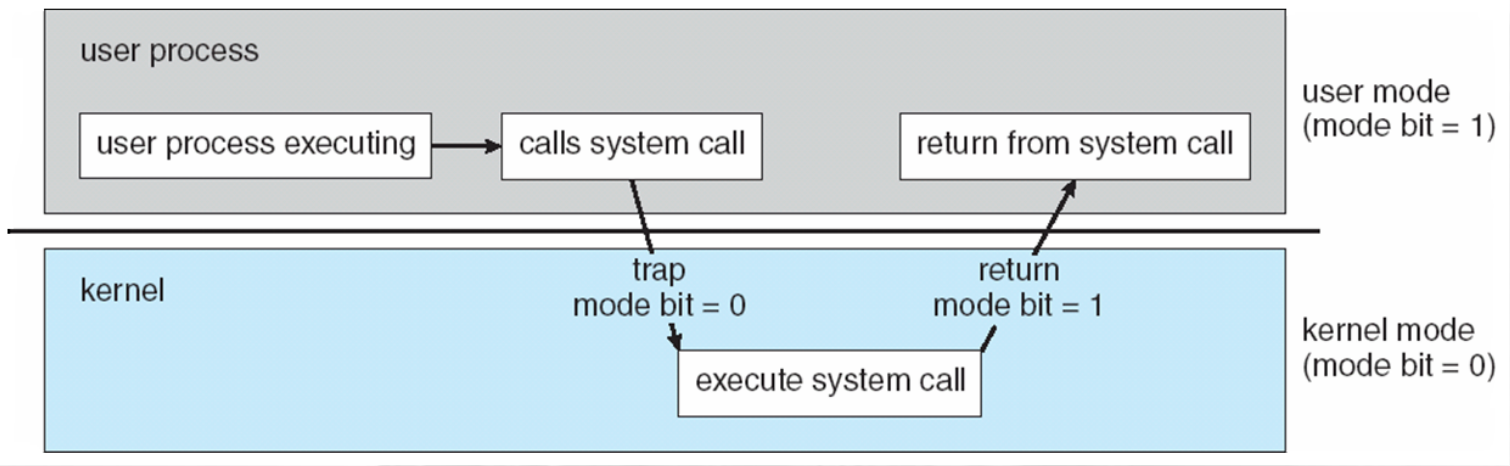
IaaS - Vantagens

- Como nos outros modelos ajuda a reduzir custos antecipados
- Oferece controle total dos recursos computacionais
- Pode ser visto como uma forma eficiente e flexivel de aluguel de recursos de hardware
- Uma maneira de levar aplicações legadas para a Nuvem

IaaS - Riscos

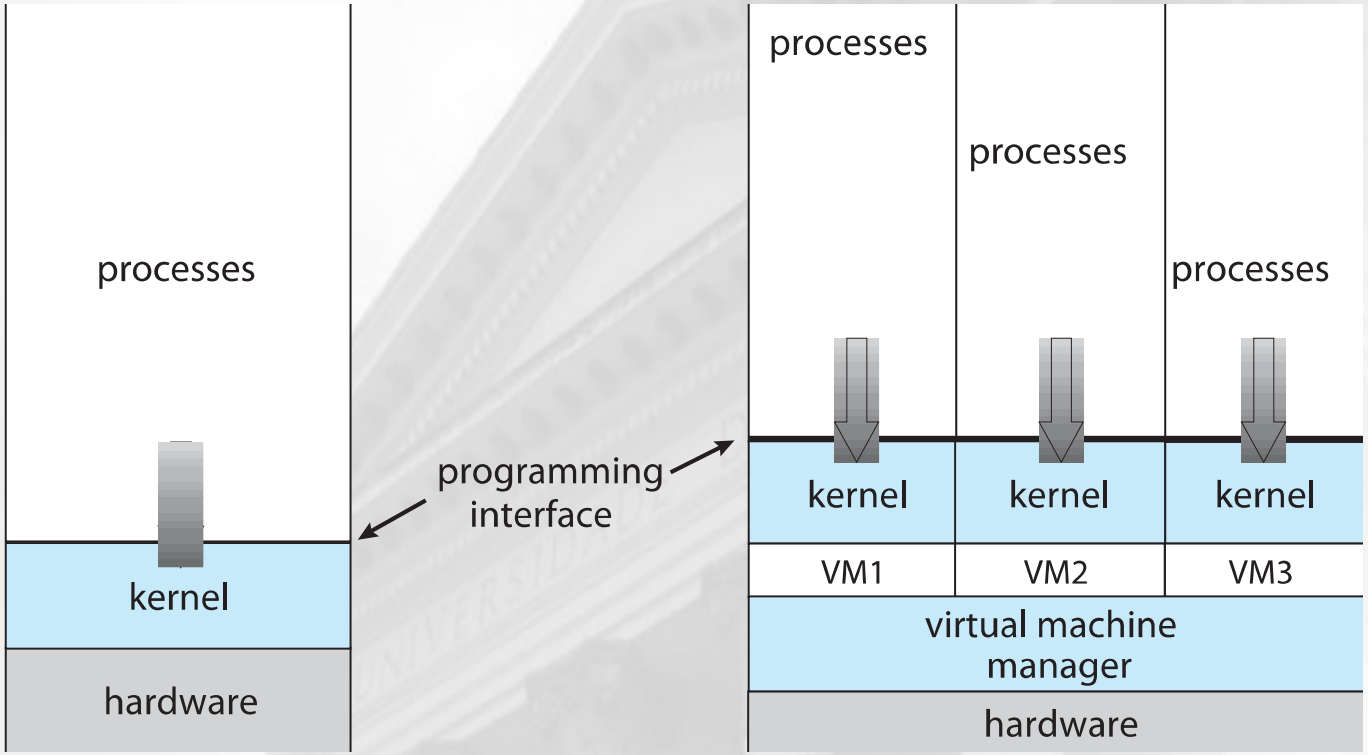
- Vulnerabilidade legadas
- Manutenção da instalação das máquina virtuais
- Confiabilidade da solução de isolamento de máquinas virtuais
- Recursos para isolamento de rede
- Políticas para apagar os dados

Virtualização



- O mecanismo de proteção do Sistema Operacional é um das principais dificuldades para prover Virtualização

Virtualização



Tipos

- Tipo 1 (bare-metal)
  - Software construído para executar no lugar do SO e prover virtualização
    - Vmware ESX, Citrix XenServer
  - Em alguns casos o SO é um Hypervisor
    - KVM
- Tipo 2 (hosted)
  - Executam sobre o Sistema Operacional
    - Vmware Workstation, Oracle VirtualBox

Técnicas

- Full Virtualization
  - VMware(1998) binary translation
- Paravirtualization
  - O *guest* tem ciência que está sendo virtualizado e utilizar *hypercalls (Xen)*
- Hardware Assisted Virtualization
  - Intel (Virtualization Technology) / AMD (Secure Virtual Machine)
  - Basicamente prover níveis de proteção intermediários

Outras virtualizações

- Outras variações
  - Ambiente de Execução de Código “Virtual”
    - Java bytecodes
  - Emuladores
    - O objetivo é emular um HW diferente para as aplicações
    - Mas também podemo emular um SO
      - Emulação Windows no Linux
  - Containers
    - Prover isolamento, mas manter um único núcleo (*kernel)* do Sistema Operacional
    -

Containers

- O avô dos containers é o chroot
- Linux Vserver (2001-2006)
- OpenVZ (2005)
- LXC (Linux Containers) usando cgroups e Linux Namespaces
- Docker (2013)
  - Um ecossistema completo. Incentiva o uso de conceitos de microserviços.

Plataformas mais populares

- VMware ESX
  - Tipo 1. Provavelmente a solução mais madura, mas a versão livre é bastante limitada
- Xen
  - Tipo 1. Inicialmente foi líder em paravirtualização; atualmente pode executar *guests* não modificados
- Virtualbox
  - Tipo 2. Uma das soluções mais simples para emulação de desktops
- KVM
  - Módulos na mainstream do kernel. Presente no mainstream do kernel, usa extensões de HW e algumas artifícios de paravirtualização. U