



INSTITUTO FEDERAL

Norte de Minas Gerais

Campus Januária

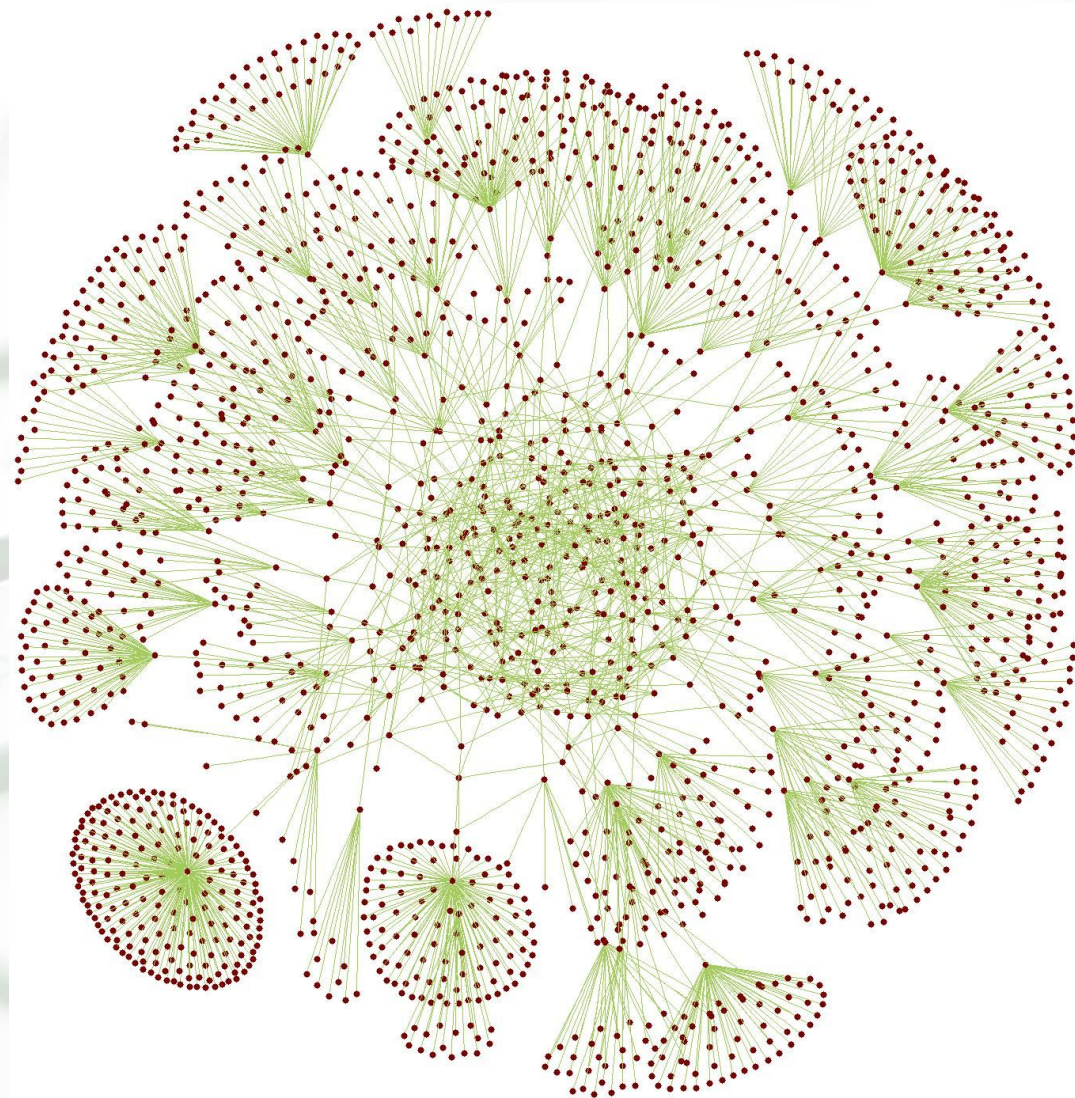
Admin. Serviços de Redes

- *Sockets & Utilitários* -



REVISÃO CONCEITUAL

A partir desta aula, deixaremos de abordar uma visão restrita à configuração básica de redes, para uma visão mais ampla, da configuração dos **SERVIÇOS** oferecidos pelas redes.



**Image from [UC San Diego Jacobs School of Engineering](https://www.jacobs-engineering.com/).*



REVISÃO CONCEITUAL

Modelo OSI

Camada de Aplicação

Camada de Apresentação

Camada de Sessão

Camada de Transporte

Camada de Rede

Camada de Enlace

Camada de Física

Arquitetura TCP / IP

Camada de Aplicação

Camada de Transporte

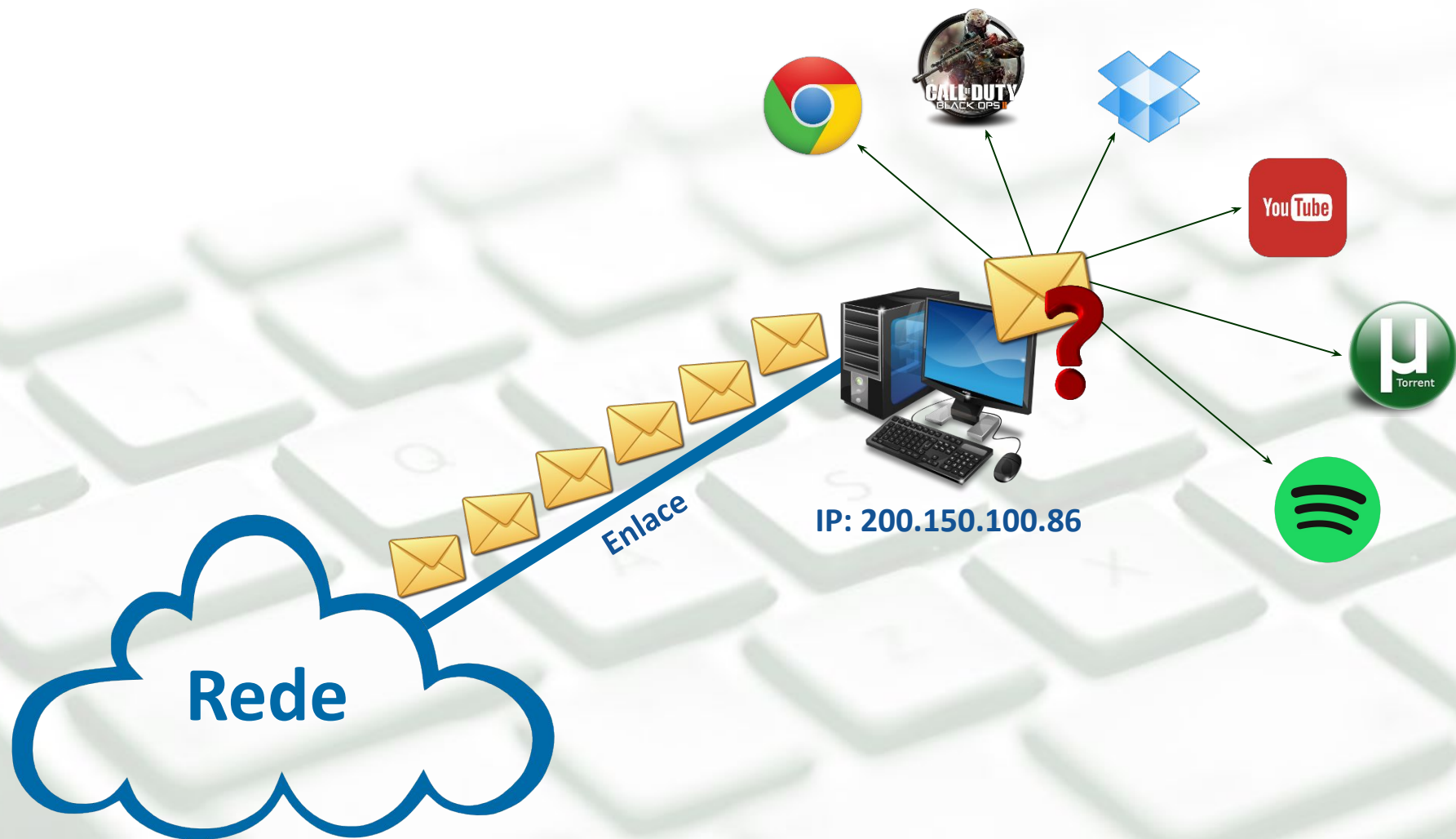
Camada Internet / Inter-Redes

Camada Host / Rede ou
Interface de Rede



INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

REVISÃO CONCEITUAL





REVISÃO CONCEITUAL

Modelo OSI

Camada de Aplicação

Camada de Apresentação

Camada de Sessão

Camada de Transporte

Camada de Rede

Camada de Enlace

Camada de Física

Arquitetura TCP / IP

Camada de Aplicação

Camada de Transporte

Camada Internet / Inter-Redes

Camada Host / Rede ou
Interface de Rede



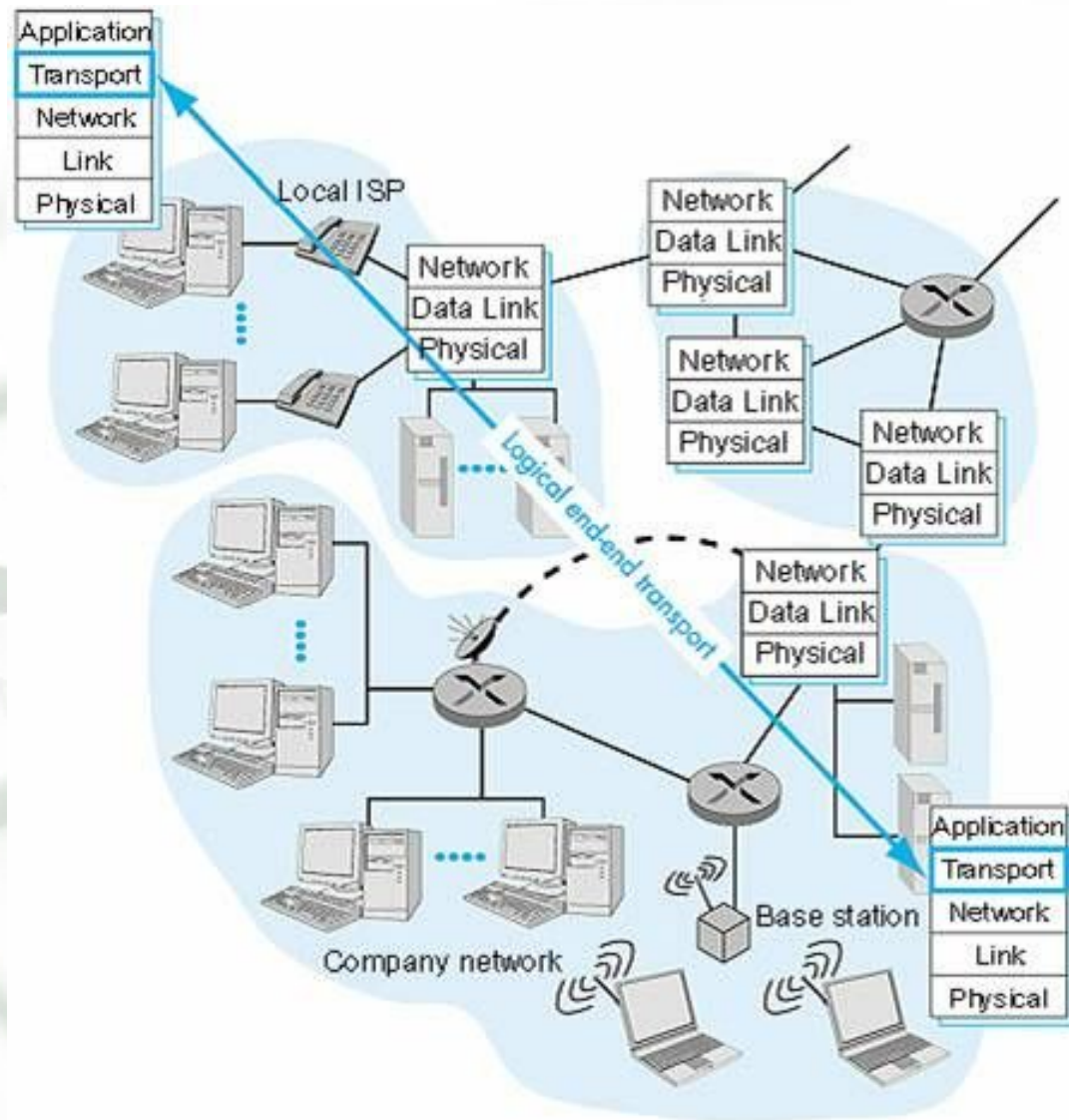
Camada de Transporte

- A finalidade real de uma rede de computadores é fazer com que **aplicações (processos) troquem informações entre si**.
- Porém, um único *host* pode executar **inúmeros processos que utilizam a rede** de comunicação simultaneamente.
- A **Camada de Transporte** é responsável pelo transporte de dados **na comunicação inter-processos, dos sistemas finais de uma rede**.



Comunicação Inter-Processos

A camada de transporte realiza **“Comunicação Lógica Fim-a-Fim”**, conectando processos remotos (aplicações de rede) e fazendo o transporte de suas mensagens.



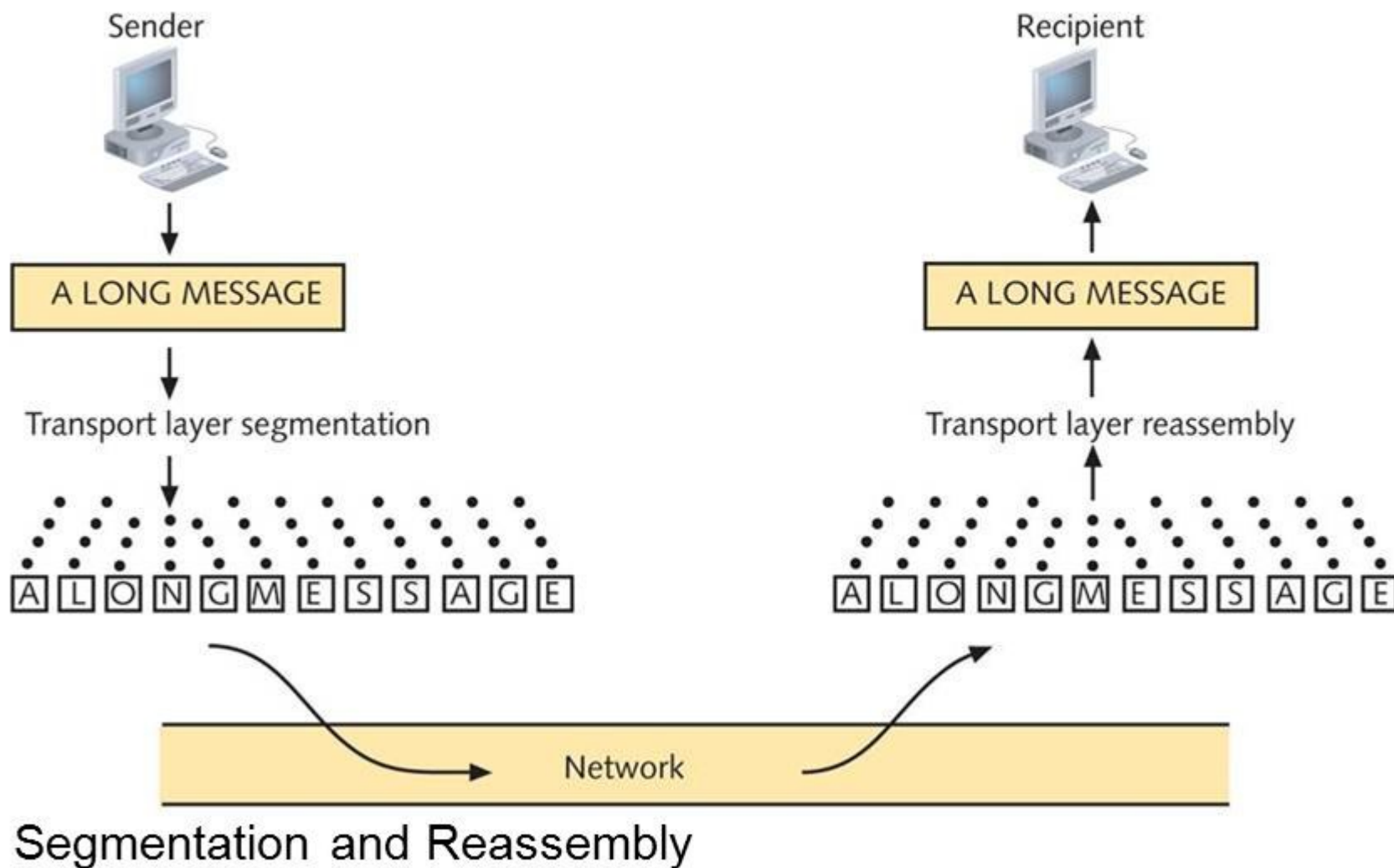


Camada de Transporte

- Os dados das aplicações são **segmentados** em **pacotes IP** e repassados para a camada de rede, que efetuará o roteamento até o *host* de destino.
- Em nível de Rede, cada segmento pode seguir rotas diversas, mesmo sendo parte de uma mensagem maior.
- Os pacotes recebidos pela rede são direcionados para a camada de transporte, que realizará o controle, remontagem e a entrega para a aplicação correspondente.



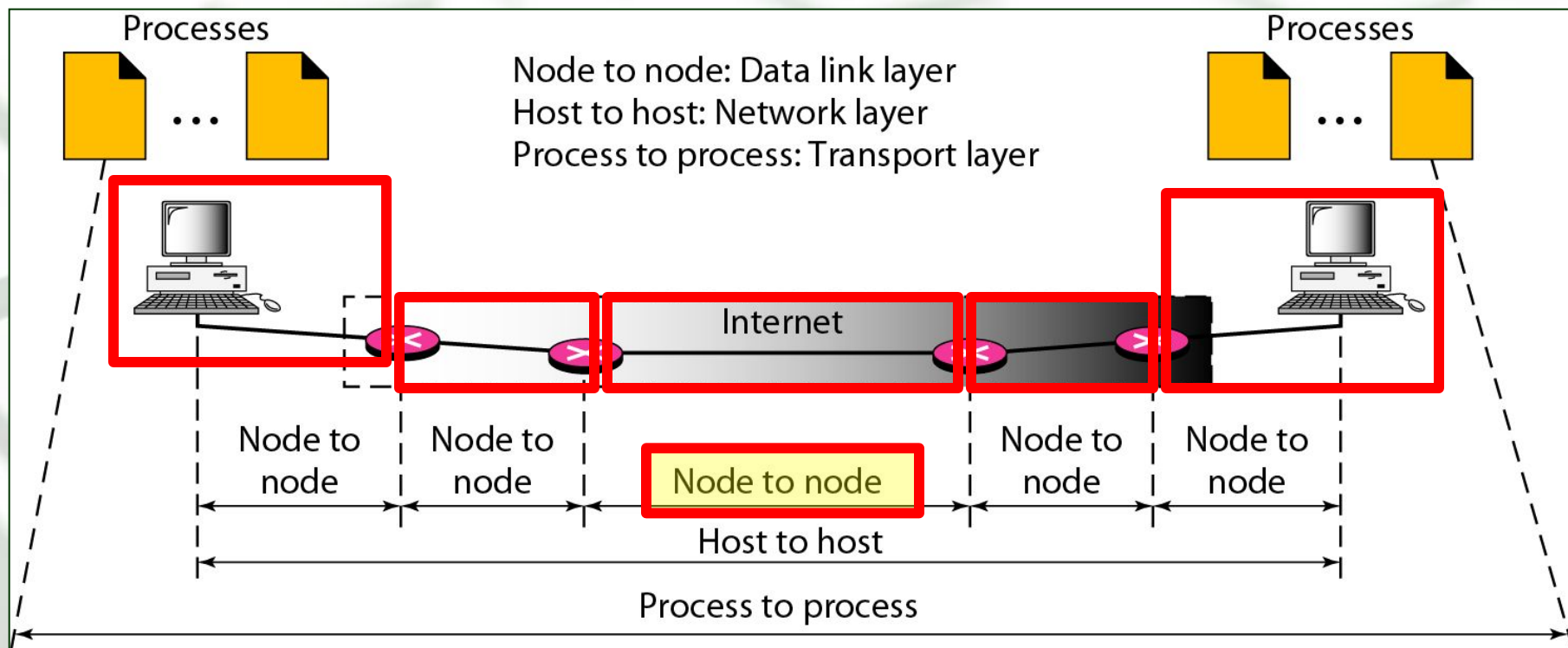
Segmentação de Dados





Comunicação Inter-Processos

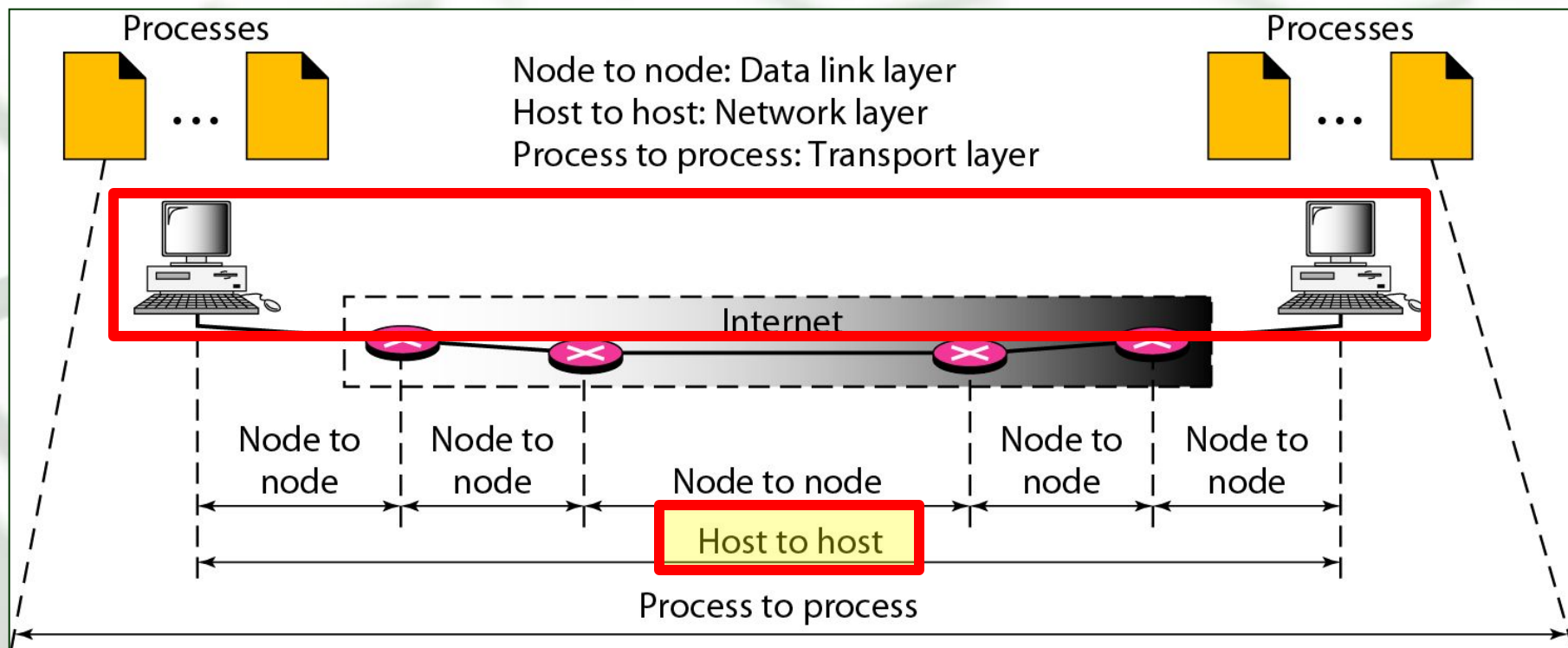
■ Comunicação em **Nível de Enlace (MAC Address)**.





Comunicação Inter-Processos

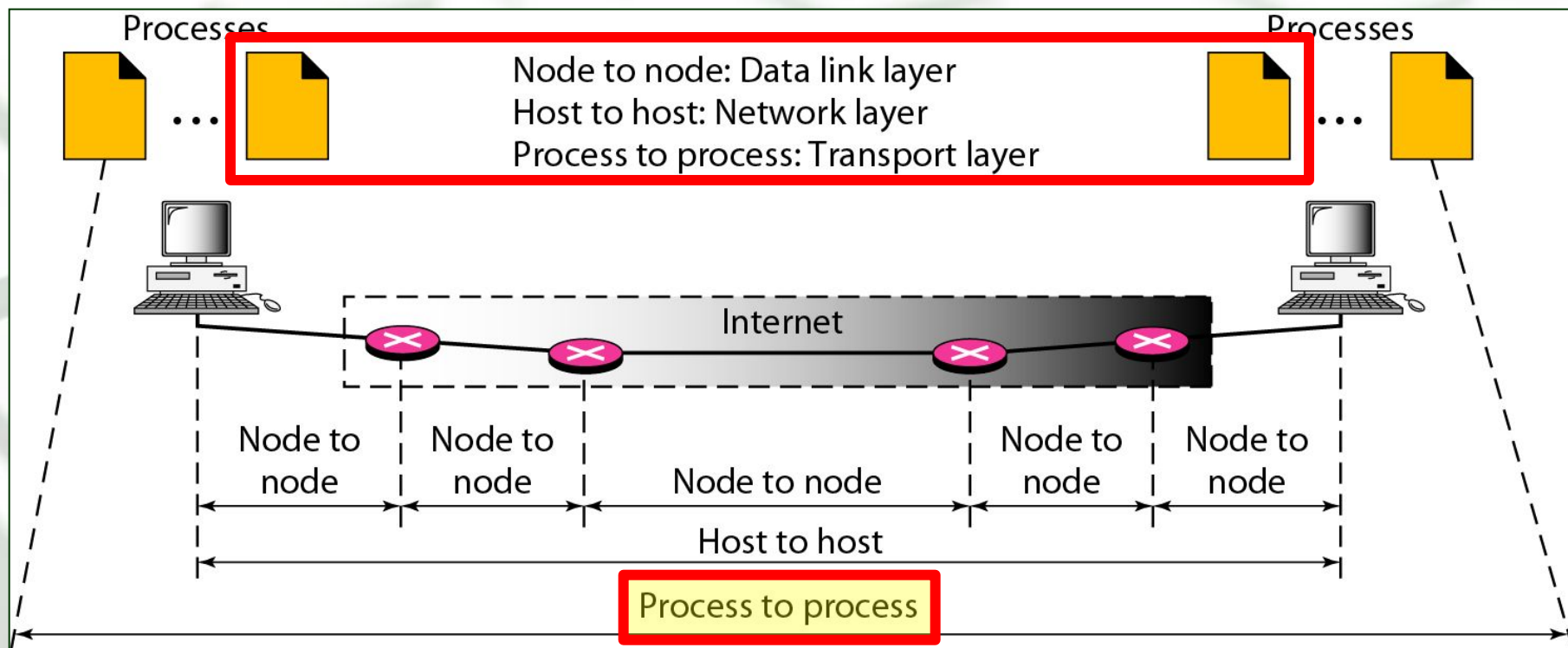
■ Comunicação em **Nível de Rede (IP Address)**.





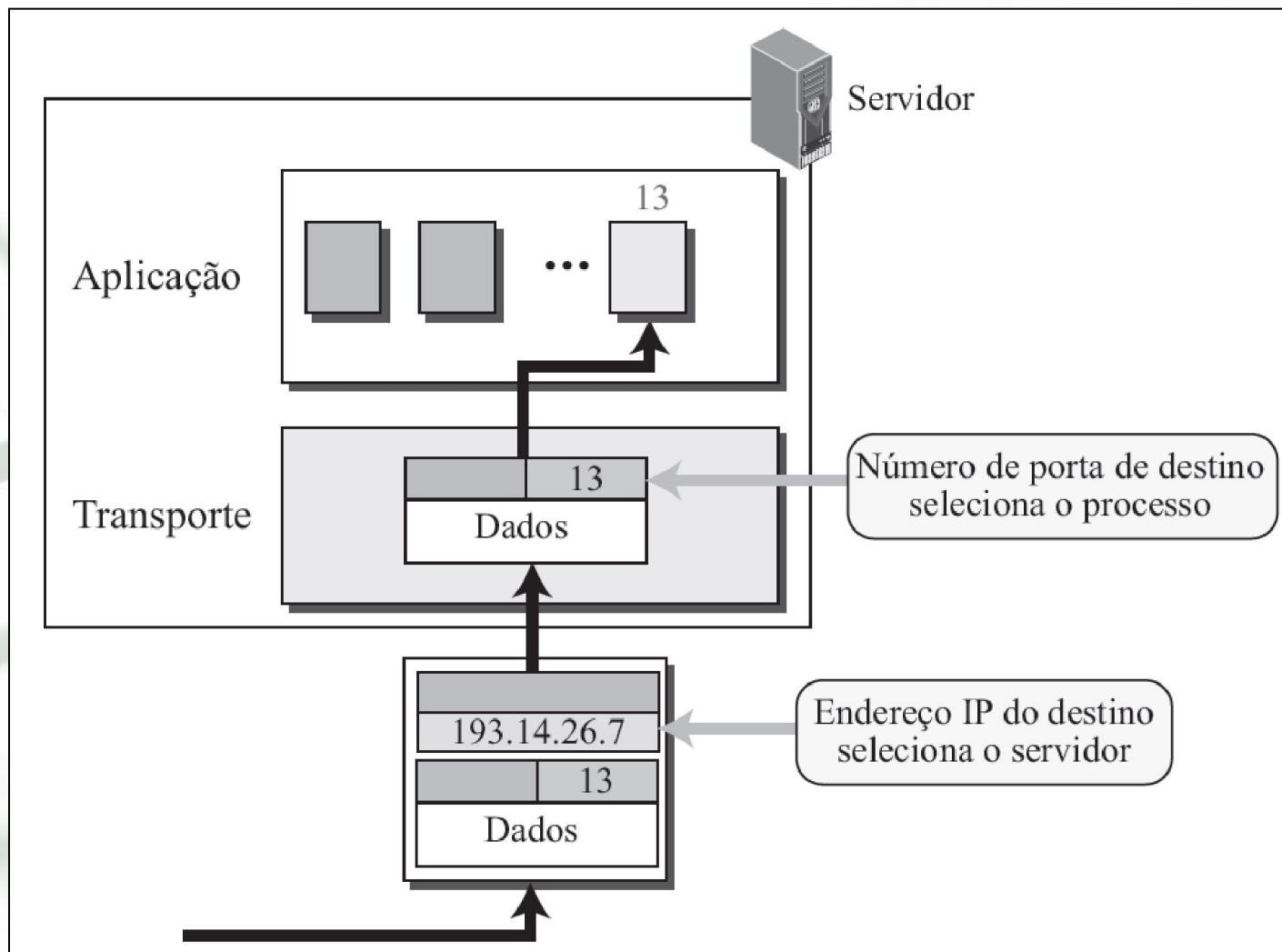
Comunicação Inter-Processos

■ Comunicação em **Nível de Transporte** (???)





Portas de Comunicação





Portas de Comunicação

- Na arquitetura TCP/IP, uma porta de comunicação é um número inteiro de 16 bits.
 - $0 \leftrightarrow 65.535$
- Uma porta mapeia um determinado processo (aplicação) que está utilizando a rede de comunicação.

Problema... Para que um cliente possa acessar um web-site, ele precisaria saber antecipadamente qual a porta que este site está “escutando”???



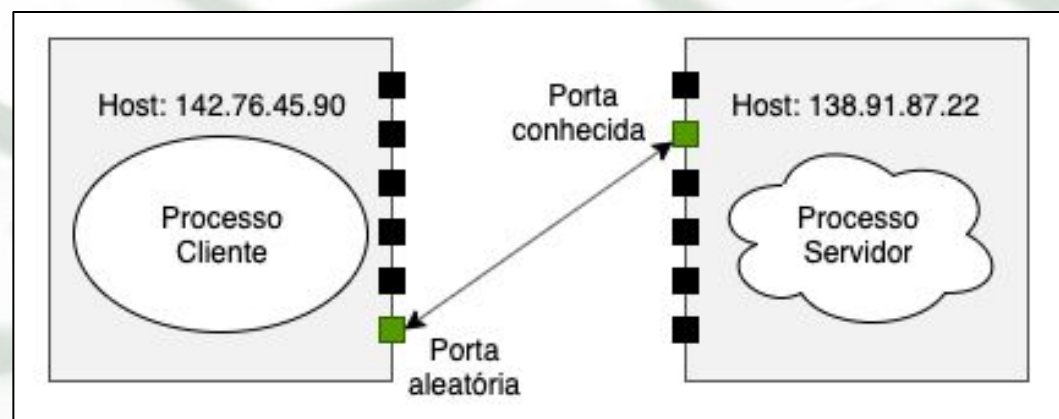
Faixas IANA

Nome	Faixa	Descrição
Portas Conhecidas	0 – 1023	Atribuídas e controladas pela IANA.
Portas Registradas	1024 – 49151	Necessita registro junto à IANA.
Portas Dinâmicas	49152 – 65535	Portas para uso geral.



Portas Conhecidas

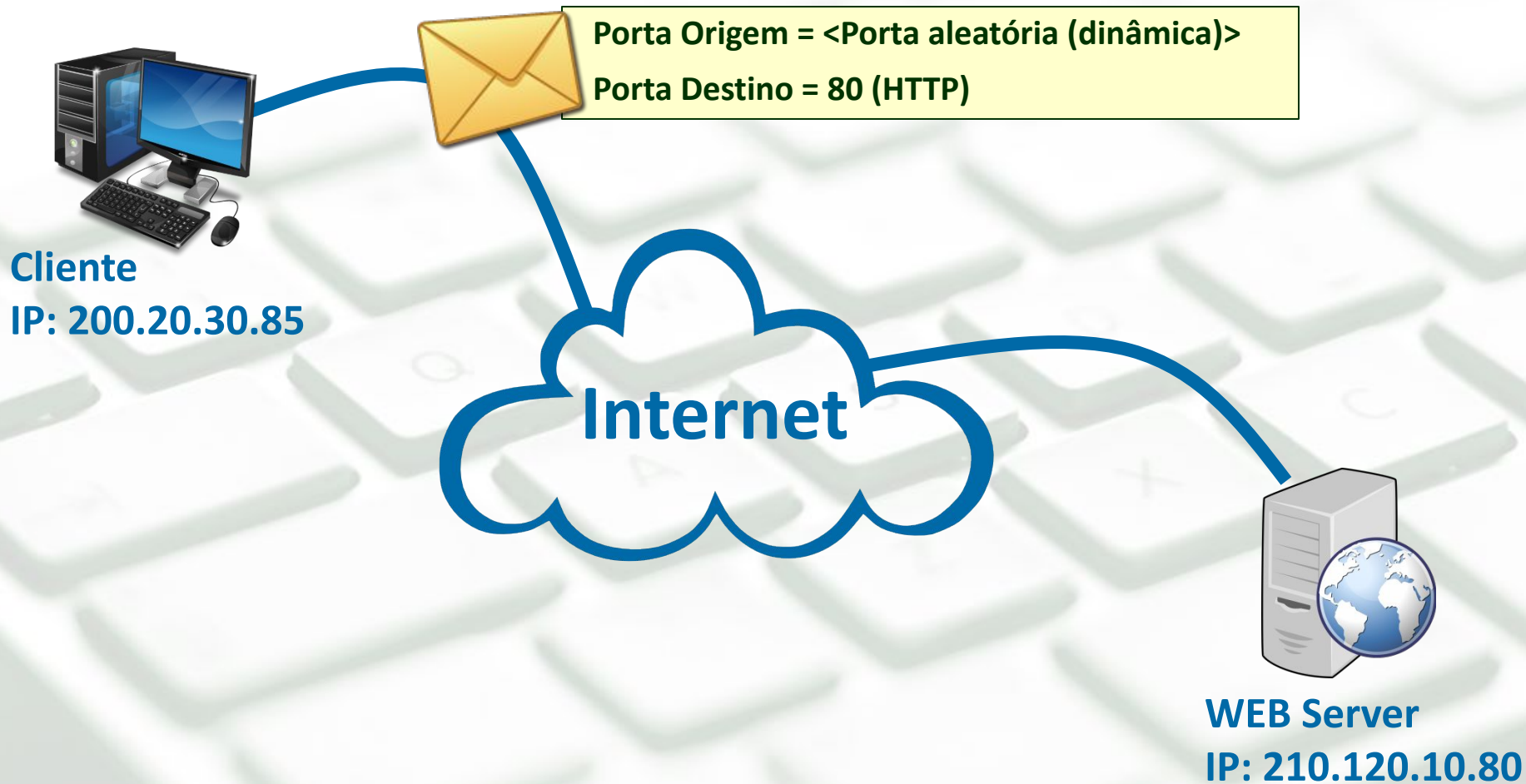
- Servidores de aplicações e seus protocolos padrões já possuem portas bem definidas, designadas por meio de RFCs (normativas).
 - 21 -> *FTP*
 - 22 -> *SSH*
 - 25 -> *SMTP*
 - 53 -> *DNS*
 - 67 -> *DHCP*
 - 80 -> *HTTP*
 - 443 -> *HTTPS*





INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Portas de Comunicação





Socket / Soquete

A combinação **IP:PORTA** identifica exclusivamente um processo em execução na rede.



Cliente

IP: 200.20.30.85

200.20.30.85:58569



210.120.10.80:80

WEB Server

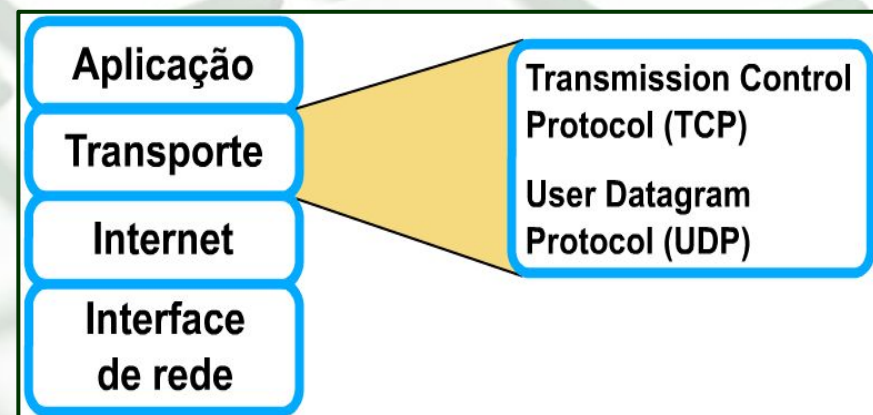
IP: 210.120.10.80

Chamamos essa combinação de **SOCKET** de rede.



Protocolos de Transporte

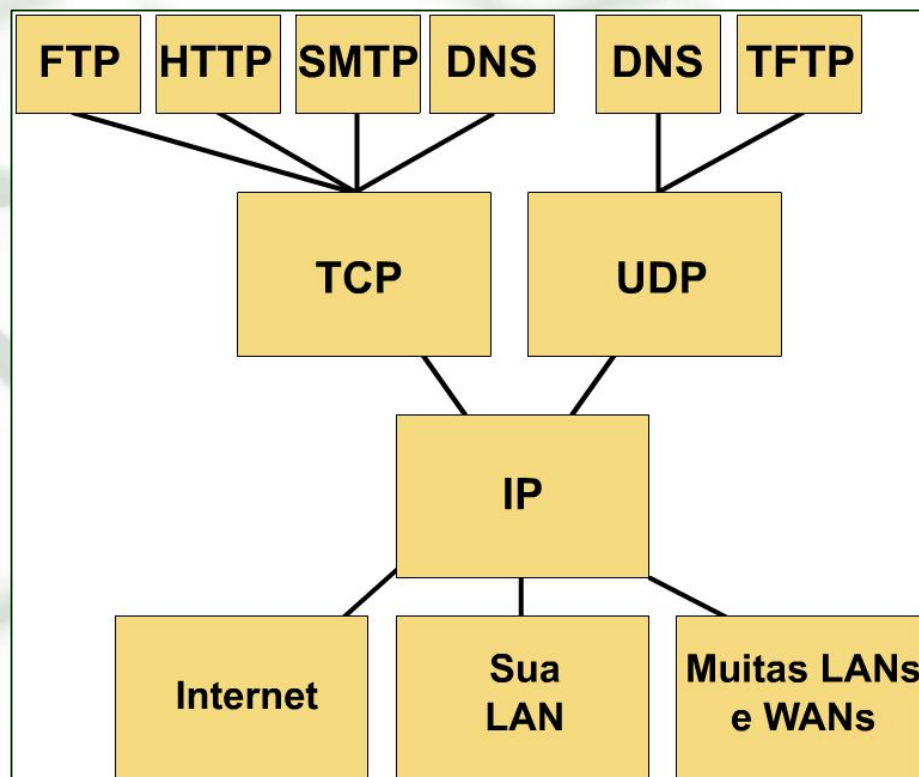
- TCP/IP prevê dois serviços de transporte...
 - ***TCP – Transmission Control Protocol***
 - *Connection-oriented*
 - *Serviço Confiável*
 - ***UDP – User Datagram Protocol***
 - *Connectionless*
 - *Serviço sem garantias*





Arquitetura TCP/IP

- Aplicações selecionam o **protocolo de transporte** de acordo com o tipo de tráfego e requisitos de qualidade.





Conexão TCP

Uma conexão TCP é identificada por um par de sockets.



Cliente

IP: 200.20.30.85

200.20.30.85:58569



210.120.10.80:80

WEB Server

IP: 210.120.10.80

Conexão TCP



3 Way Handshake

Uma conexão TCP é identificada por um par de sockets.



Cliente

IP: 200.20.30.85

200.20.30.85:58569



210.120.10.80:80

WEB Server

IP: 210.120.10.80

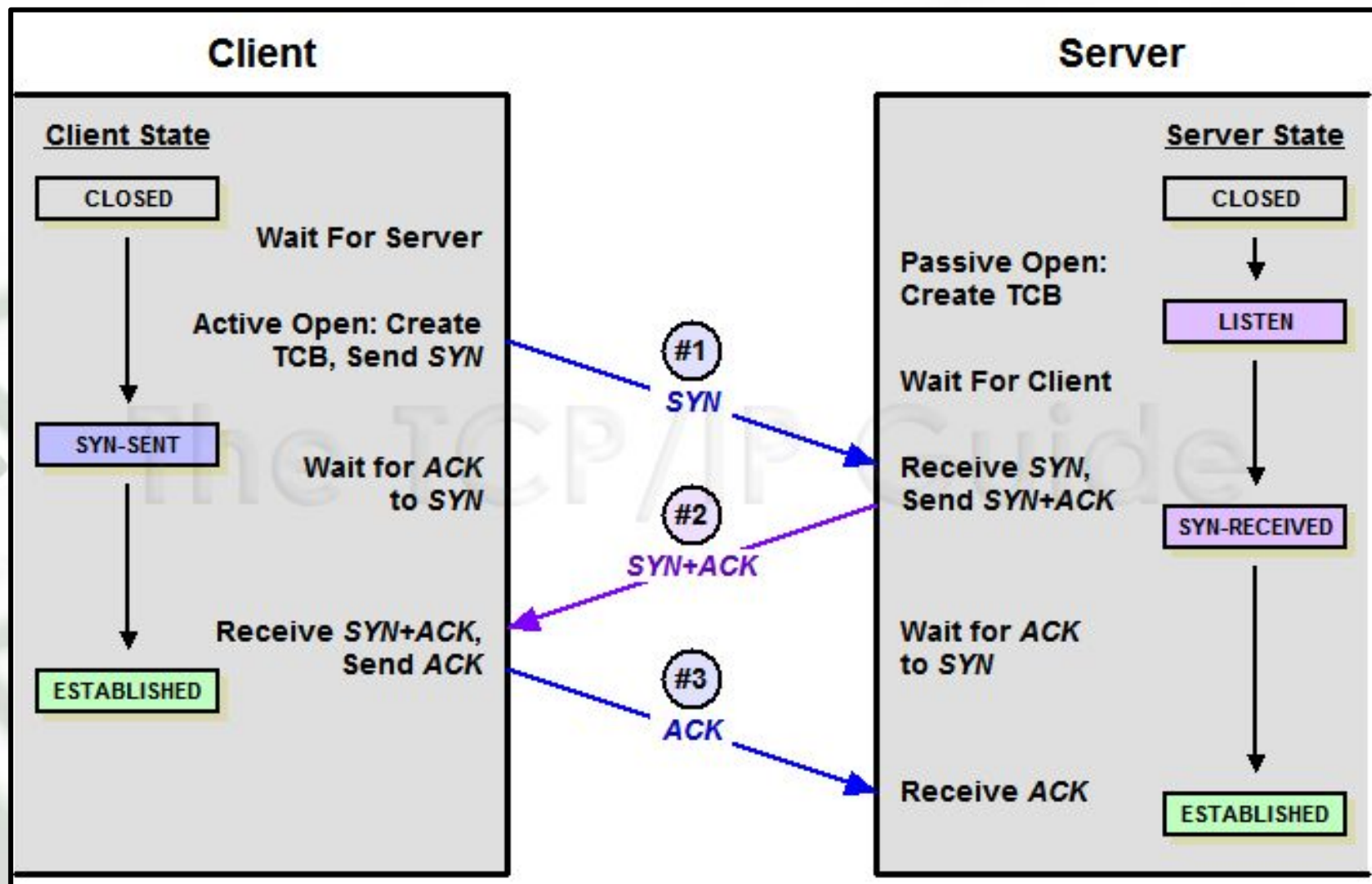
Conexão TCP

3-Way Handshake





3 Way Handshake





Netstat

- O utilitário **netstat** permite obter informações atualizadas sobre o status das portas e conexões de transporte (*sockets*) em um host.
- Além disso, provê informações estatísticas sobre os principais protocolos da arquitetura TCP/IP.
- O utilitário **ss** é uma alternativa ao **netstat**, e apresenta os mesmos parâmetros para utilização.



Netstat

<code>netstat -l</code>	Exibe sockets em estado “Listening” (Servidor)
<code>netstat -t</code>	Exibe sockets para o protocolo TCP.
<code>netstat -u</code>	Exibe sockets para o protocolo UDP.
<code>netstat -n</code>	Exibe informações numéricas ao invés de nomes.
<code>netstat -p</code>	Exibe os processos envolvidos.
<code>netstat -ltnp</code>	Exibe sockets TCP em estado “Listening” sem resolver nomes e com os processos envolvidos.
<code>netstat -A inet</code>	Exibe dados somente da pilha TCP/IP.
<code>netstat -a</code>	Exibe todos os sockets ativos.
<code>netstat -s</code>	Exibe estatísticas sobre protocolos.
<code>netstat -r</code>	Exibe a tabela de roteamento.



Netstat

netstat -l

Exibe sockets em estado “Listening” (Servidor)

```

adriano@adriano-notebook: ~
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda
adriano@adriano-notebook:~$ netstat -tn
Conexões Internet Ativas (sem os servidores)
Proto Recv-Q Send-Q Endereço Local          Endereço Remoto          Estado
tcp      0      0 192.168.1.5:50426      157.240.226.60:443      ESTABELECID
tcp      0      0 192.168.1.5:50046      35.241.29.71:443       ESTABELECID
tcp      0      0 192.168.1.5:42642      142.251.0.188:5228     ESTABELECID
tcp      0      0 192.168.1.5:45544      172.64.41.3:443        ESTABELECID
tcp      0      0 192.168.1.5:46474      34.96.128.111:443      ESTABELECID
tcp      0      0 192.168.1.5:45638      34.80.0.147:443        ESTABELECID
tcp      0      0 192.168.1.5:33620      142.251.128.133:443    ESTABELECID
tcp      0      0 192.168.1.5:51654      34.96.128.111:443      ESTABELECID
tcp      0      0 192.168.1.5:34376      172.64.41.3:443        TIME_WAIT
tcp      0      0 192.168.1.5:60272      162.125.21.3:443       ESTABELECID
tcp      0      0 192.168.1.5:50034      35.241.29.71:443       ESTABELECID
tcp      0      0 192.168.1.5:55662      172.67.71.73:443       TIME_WAIT
tcp      0      0 192.168.1.5:48176      35.190.80.1:443        ESTABELECID
tcp      0      0 192.168.1.5:47484      54.77.146.235:8282     ESTABELECID
adriano@adriano-notebook:~$

```

netstat -r

Exibe a tabela de roteamento.



ss (show sockets)

ss -l	Exibe sockets em estado “Listening” (Servidor)
ss -t	Exibe sockets para o protocolo TCP.
ss -u	Exibe sockets para o protocolo UDP.
ss -n	Exibe informações numéricas ao invés de nomes.
ss -p	Exibe os processos envolvidos.
ss -ltnp	Exibe sockets TCP em estado “Listening” sem resolver nomes e com os processos envolvidos.
ss -A inet	Exibe dados somente da pilha TCP/IP.
ss -a	Exibe todos os sockets ativos.
ss -s	Exibe estatísticas sobre protocolos.
ss -r	Exibe a tabela de roteamento.



Netcat

- O utilitário **netcat** permite de maneira simples e fácil, abrir sockets para envio e recepção de informações entre hosts.
- O **netcat** é uma aplicação Cliente x Servidor, e atua da seguinte forma.

```
# nc -lp 12345
```

*Abre a porta 12345 em estado
"Listening" (Servidor)*



Netcat

■ O ut
socl

■ O n
form

nc

```
adriano@adriano-notebook: ~
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda

Conexões Internet Ativas (somente servidores)
Proto Recv-Q Send-Q Endereço Local          Endereço Remoto          Estado
tcp      0      0 0.0.0.0:111             0.0.0.0:*                OUÇA
tcp      0      0 127.0.0.1:30800         0.0.0.0:*                OUÇA
tcp      0      0 127.0.0.1:44115         0.0.0.0:*                OUÇA
tcp      0      0 127.0.0.1:30900         0.0.0.0:*                OUÇA
tcp      0      0 192.168.122.1:53        0.0.0.0:*                OUÇA
tcp      0      0 127.0.0.53:53           0.0.0.0:*                OUÇA
tcp      0      0 0.0.0.0:22              0.0.0.0:*                OUÇA
tcp      0      0 127.0.0.1:631           0.0.0.0:*                OUÇA
tcp      0      0 0.0.0.0:12345           0.0.0.0:*                OUÇA
tcp      0      0 0.0.0.0:17500           0.0.0.0:*                OUÇA
tcp      0      0 127.0.0.1:17600         0.0.0.0:*                OUÇA
tcp      0      0 127.0.0.1:17603         0.0.0.0:*                OUÇA
tcp      0      0 0.0.0.0:902             0.0.0.0:*                OUÇA
tcp6     0      0 :::111                  :::*                      OUÇA
tcp6     0      0 :::1716                  :::*                      OUÇA
tcp6     0      0 :::22                    :::*                      OUÇA
tcp6     0      0 ::1:3350                 :::*                      OUÇA
tcp6     0      0 ::1:631                  :::*                      OUÇA
tcp6     0      0 :::17500                 :::*                      OUÇA
tcp6     0      0 :::3389                  :::*                      OUÇA
tcp6     0      0 :::902                   :::*                      OUÇA
adriano@adriano-notebook:~$
```

inte

do



Laboratório 07-1

- Através do netcat, abra um socket para ouvir a porta 80.

```
# nc -lp 80
```

***Abre a porta 12345 em estado
“Listening” (Servidor)***

- A partir do seu navegador WEB, tente acessar o site “localhost”



Laboratório 07-1

■ Atra

nc

■ A pa

```
adriano@adriano-notebook: ~  
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda  
adriano@adriano-notebook:~$ sudo nc -lp 80  
GET / HTTP/1.1  
Host: localhost  
Connection: keep-alive  
Cache-Control: max-age=0  
sec-ch-ua: "Not.A/Brand";v="8", "Chromium";v="114", "Google Chrome";v="114"  
sec-ch-ua-mobile: ?0  
sec-ch-ua-platform: "Linux"  
DNT: 1  
Upgrade-Insecure-Requests: 1  
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Sec-Fetch-Site: none  
Sec-Fetch-Mode: navigate  
Sec-Fetch-User: ?1  
Sec-Fetch-Dest: document  
Accept-Encoding: gzip, deflate, br  
Accept-Language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7  
  
[ ]
```

ado

st"



Laboratório 07-2

- Através do utilitário **netcat**, faça uma sessão de chat com o seu colega ao lado.
- Através do utilitário **netstat**, descubra...
 - O netcat abre sockets TCP ou UDP?
 - Verifique qual foi o socket (IP:Porta) aberto pelo processo cliente na conexão do chat.

```
# nc -lp 12345
```

*Abre a porta 12345 em estado
"Listening" (Servidor)*

```
# nc ip_servidor 12345
```

*Solicita conexão ao servidor através
da porta de destino 12345*



INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Netcat

- **Gostou do Netcat?**
- Assista ao vídeo abaixo (Vagner Fonseca) para conhecer diversas outras possibilidades de uso do Netcat.





Nmap

- O utilitário **nmap** permite o mapeamento de *hosts* e *serviços* (*sockets*) ativos em uma rede.
- Em algumas distribuições não é um pacote padrão, sendo necessário a instalação prévia.

```
# sudo apt-get install nmap
```



Nmap

■ Principais parâmetros:

<code>nmap -sS alvo</code>	Utiliza TCP-SYN para procurar portas TCP abertas no alvo.
<code>nmap -sS rede/x -p1-65535</code>	Escaneia todas as portas da faixa de rede estabelecida.
<code>nmap -p80 rede/x</code>	Rastreia a porta 80 nos hosts definida pela rede/x.
<code>nmap -sP rede/x</code>	Utiliza “Ping Scan” para listar os hosts ativos na rede.
<code>nmap -A alvo</code>	Faz uma varredura completa no alvo.
<code>nmap -O alvo</code>	Busca o Sistema Operacional do alvo.
<code>-n</code>	Desativa a resolução de nomes (torna mais rápido)
<code>-v</code>	Modo verboso



Laboratório 07-2

- Todos devem abrir uma sessão do Netcat em modo servidor (*listening*) escolhendo um número de porta aleatório.
- Através do utilitário **netstat**, descubra os sockets do laboratório que estão abertos para conexão.

```
# sudo nmap -sS -p1-65535 faixaRededoLaboratorio -nv
```

- Tente iniciar conversas com os colegas através do netcat, partir dos parâmetros descobertos pelo nmap.



Seminário Individual

Sistemas de Criptografia

- Criptografia de Chave Simétrica
- Criptografia de Chave Assimétrica
- Diferenças
- Vantagens e Desvantagens

