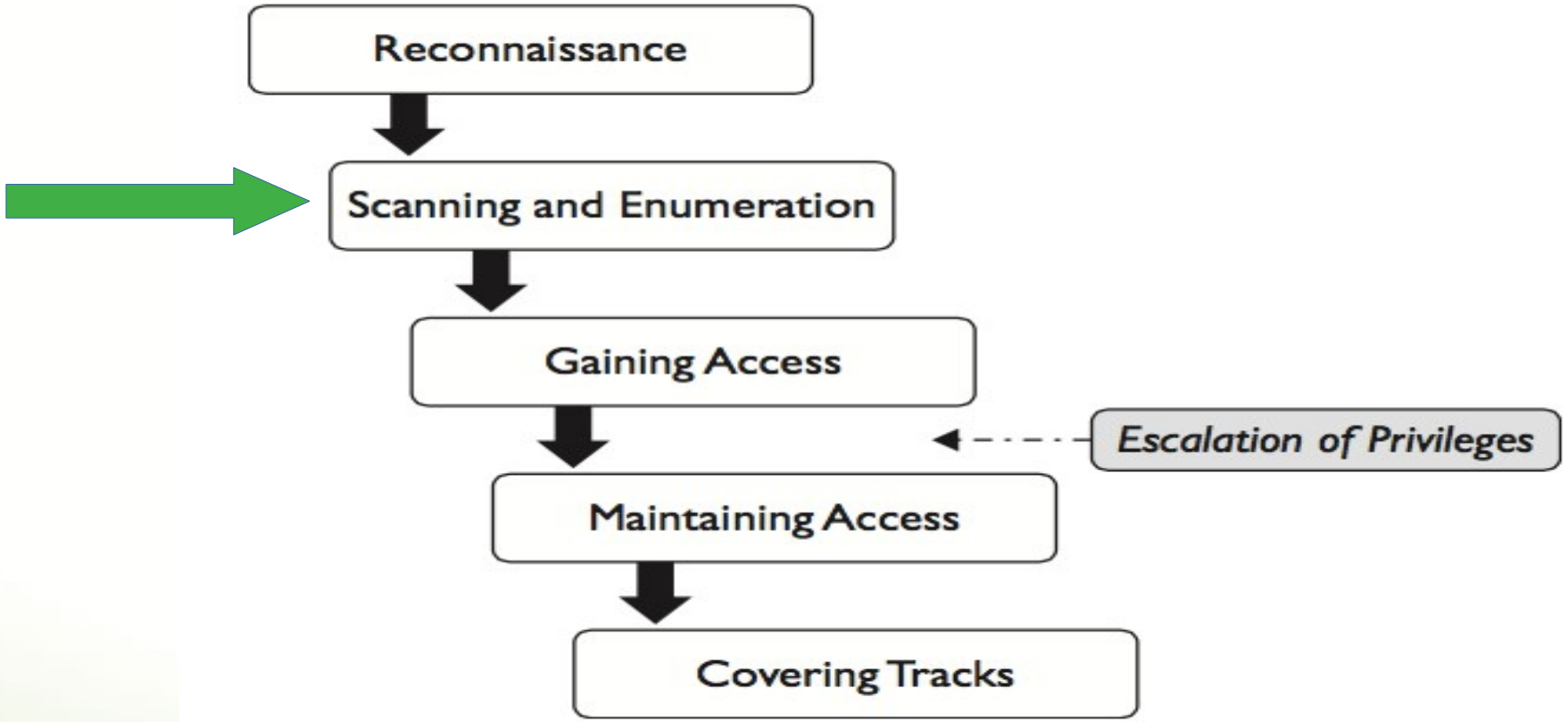
INSTITUTO FEDERAL
São Paulo
Câmpus Barretos

Segurança da Informação

Aula 4

Prof. Lucas

Fases


Reconnaissance
Scanning and Enumeration
Gaining Access
Escalation of Privileges
Maintaining Access
Covering Tracks

Introdução

- Primeiro passo após a fase de *footprint* é o scan
- Por exemplo:
  - *Footprint* mostrou o range de endereços IPs da rede e a fase de scan mostrará quais IPs estão em uso e qual serviço está sendo executado!
- Definição:
  - É o processo de descoberta de sistemas em uma rede e informações de quais portas estão abertas e quais aplicações estão rodando.
  - Começa a “tocar” cada dispositivo.

Introdução

- Base para compreender esta fase:
  - Metodologia
  - TCP/IP

INSTITUTO FEDERAL
São Paulo

Metodologias de scan

- Visa assegurar que não foi esquecido nada e todas as bases foram cobertas

- São apenas diretrizes para seguir e não obrigatoriamente passar por cada passo
  - Dependendo da situação você terá que pular um passo ou o scan de um passo poderá sobrepor um outro passo

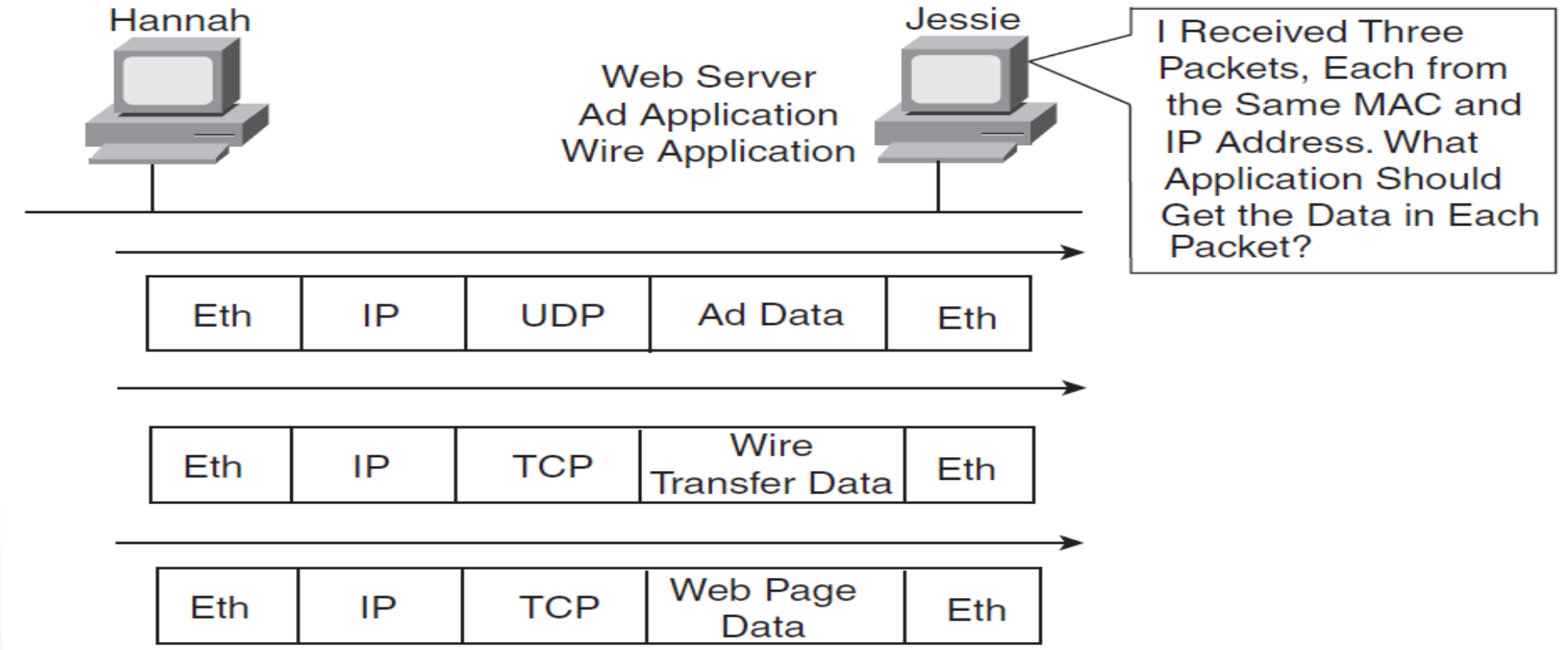
- Fases:
  - **Checar por sistemas "live"**: `ping`
  - **Checar por portas abertas**
  - **Scan além do IDS**
  - ***Banner grabbing****:* Conhecer o SO e os serviços
  - **Scan por vulnerabilidades**
  - **Desenhar o diagrama de rede**
  - **Preparar os proxies**

Modelo OSI

- Bit -> frame -> pacote -> segmento
- 1 -> 2 -> 3 -> 4

- Camada 4: TCP flags e numeração de porta (multiplexação)

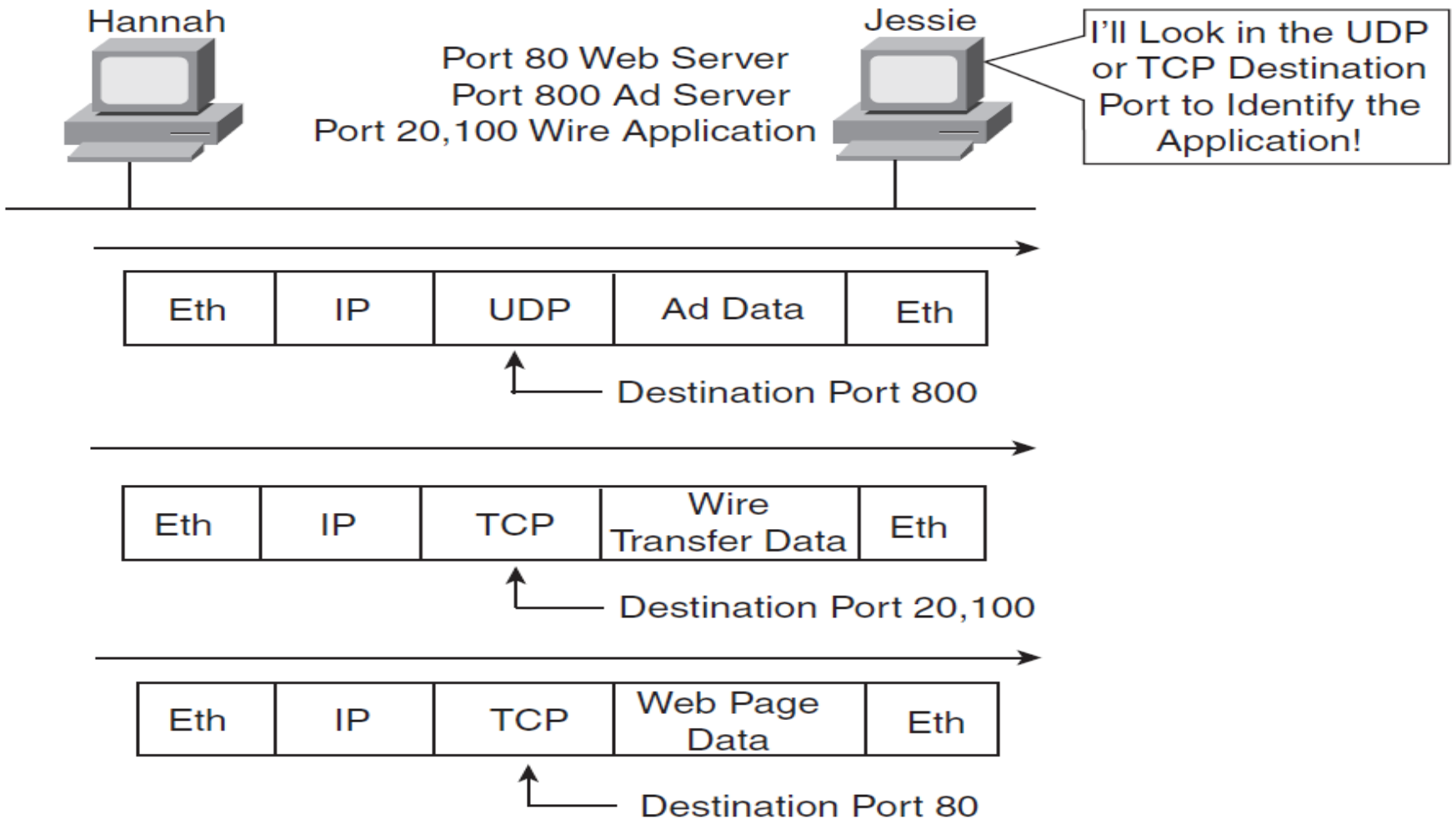
Revisão - multiplexação



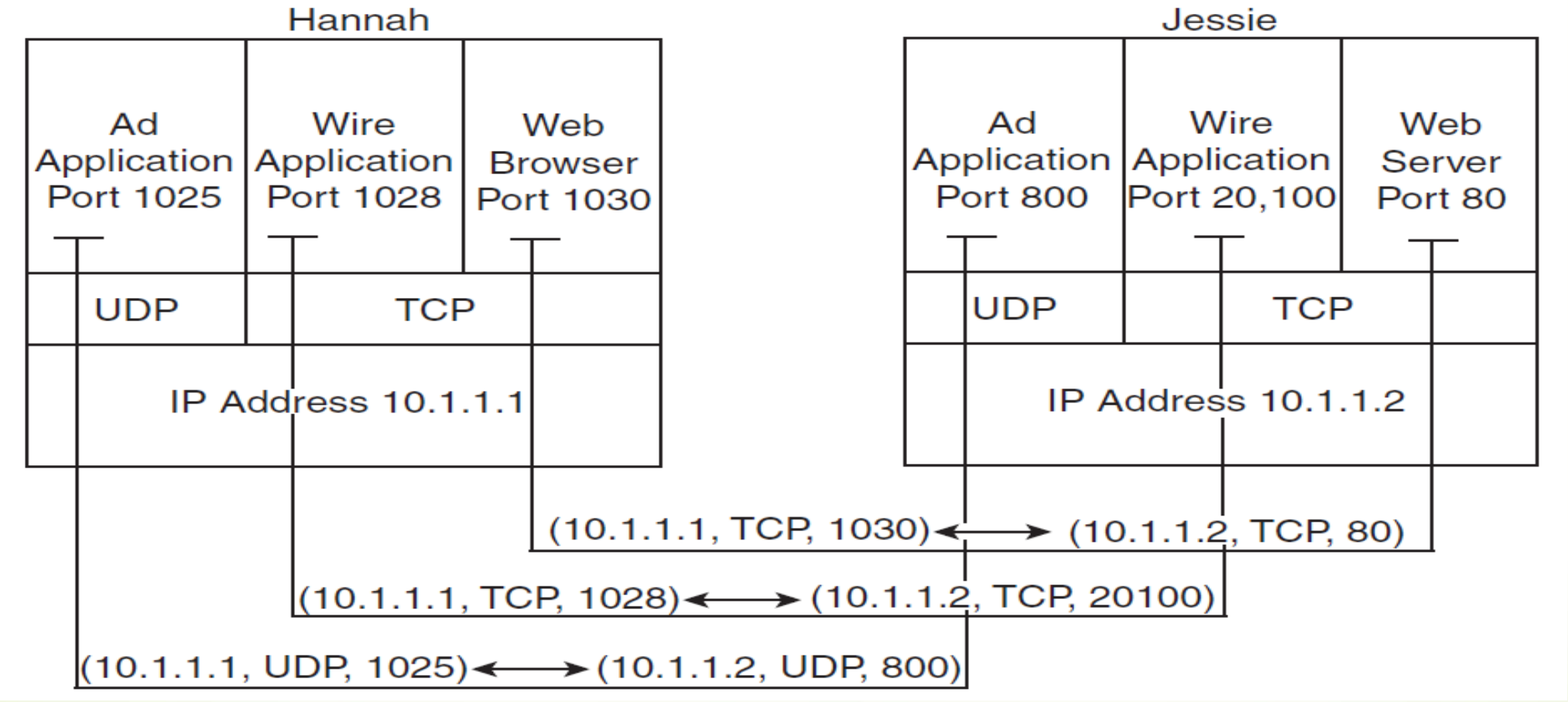
Revisão - multiplexação

- O multiplexing depende de um conceito chamado socket. Um socket consiste de três características:
  - Um endereço IP
  - Um protocolo de transporte
  - Um número de porta

Revisão - multiplexação

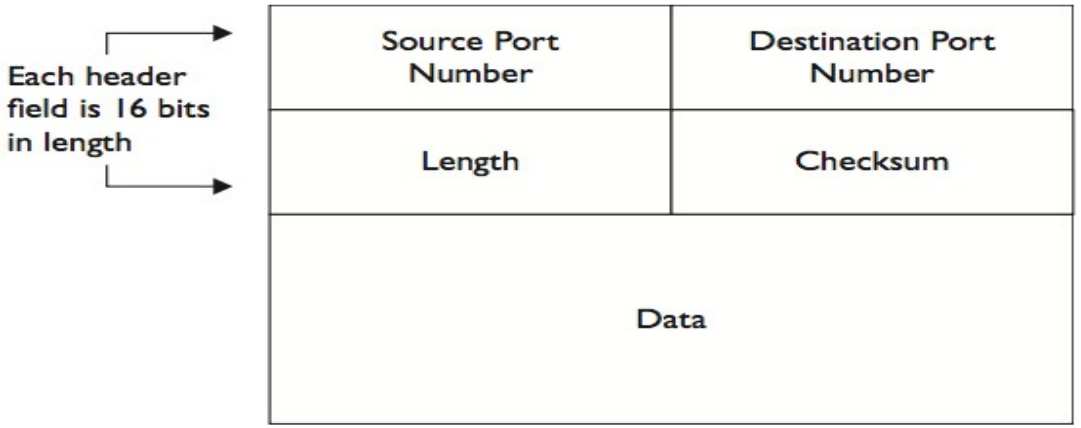


Revisão - multiplexação



Tcp x udp

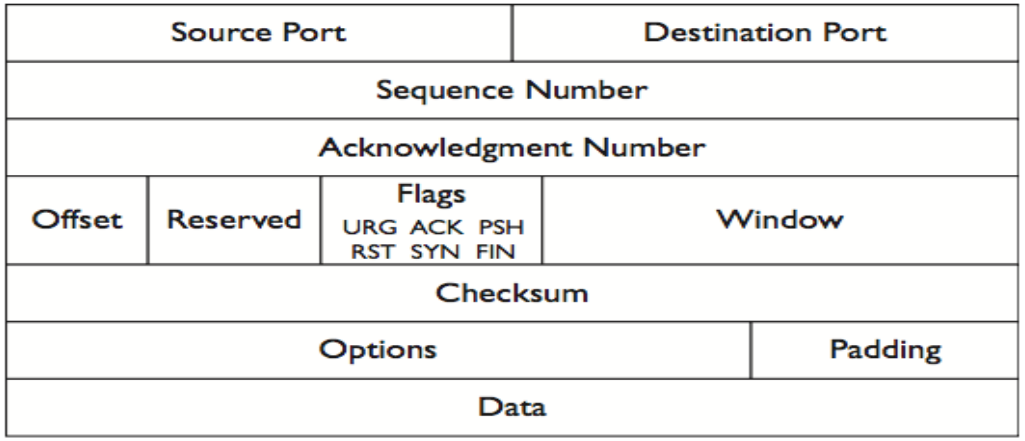
UDP




```
▷ Frame 469: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface 0
▷ Ethernet II, Src: Apple_a4:cb:aa (9c:f3:87:a4:cb:aa), Dst: Tp-LinkT_cc:f1:f4 (00:23:cd:cc:f1:f4)
▷ Internet Protocol Version 4, Src: 192.168.1.112 (192.168.1.112), Dst: 200.204.0.10 (200.204.0.10)
▽ User Datagram Protocol, Src Port: 62283 (62283), Dst Port: 53 (53)
    Source Port: 62283 (62283)
    Destination Port: 53 (53)
    Length: 57
  ▷ Checksum: 0xd090 [validation disabled]
    [Stream index: 13]
▷ Domain Name System (query)
```

Tcp x udp

TCP




```
▷ Frame 467: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
▷ Ethernet II, Src: Apple_a4:cb:aa (9c:f3:87:a4:cb:aa), Dst: Tp-LinkT_cc:f1:f4 (00:23:cd:cc:f1:f4)
▷ Internet Protocol Version 4, Src: 192.168.1.112 (192.168.1.112), Dst: 178.236.7.228 (178.236.7.228)
▽ Transmission Control Protocol, Src Port: 50481 (50481), Dst Port: 80 (80), Seq: 405, Ack: 8099, Len: 0
    Source Port: 50481 (50481)
    Destination Port: 80 (80)
    [Stream index: 8]
    [TCP Segment Len: 0]
    Sequence number: 405    (relative sequence number)
    Acknowledgment number: 8099    (relative ack number)
    Header Length: 20 bytes
  ▽ .... 0000 0001 0000 = Flags: 0x010 (ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
    Window size value: 8169
    [Calculated window size: 261408]
    [Window size scaling factor: 32]
  ▷ Checksum: 0x85dc [validation disabled]
    Urgent pointer: 0
  ▷ [SEQ/ACK analysis]
```

Não confundir a flag ACK com o campo de Acknowledgment!

Flags tcp

- **SYN (Syncronize)**: Flag setada durante o estabelecimento de uma conexão
- **ACK (Acknowledgment)**: Flag setada como um reconhecimento para a flag SYN. Flag setada para todos os segmentos depois de uma flag SYN.
- **RST (Reset):** Esta flag força o término de uma comunicação (em ambas as direções)
- **FIN (Finish):** Significa um pedido para término de comunicação

Início de conexão

Término de conexão

INSTITUTO FEDERAL
São Paulo

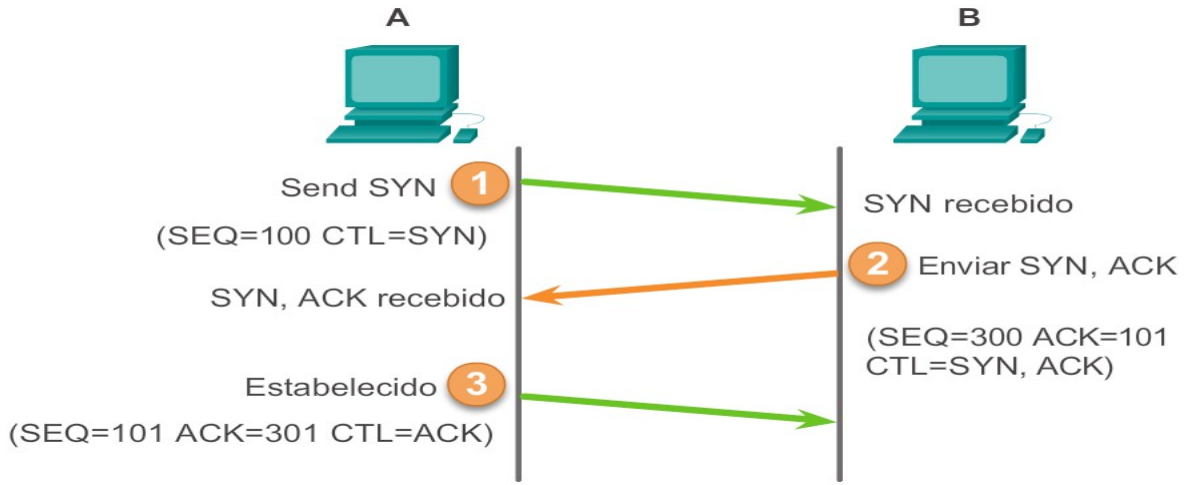
Flags tcp

- **URG (Urgent):** Dados preferenciais – não espera o buffer de memória do tcp. Exemplo: telnet
- **PSH (Push):** espera o buffer de memória do tcp. Exemplo: FTP

Transferência de dados

INSTITUTO FEDERAL
São Paulo

3 way handshake



1474	148.997704000	192.168.1.112	66.235.153.36	TCP	78 50930→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=735805143 TSecr=0 SACK_PERM=1
1485	149.217115000	66.235.153.36	192.168.1.112	TCP	74 80→50930 [SYN, ACK] Seq=0 Ack=1 Win=4320 Len=0 MSS=1440 TSval=3572585060 TSecr=735805143 SACK_PERM=1
1486	149.217227000	192.168.1.112	66.235.153.36	TCP	66 50930→80 [ACK] Seq=1 Ack=1 Win=65535 Len=0 TSval=735805360 TSecr=3572585060

Manipulando flags

- Colasoft's Packet Builder
  - http://www.colasoft.com/packet_builder/

INSTITUTO FEDERAL
São Paulo

Numeração de porta

- Os campos de porta de origem e destino na comunicação TCP e UDP definem os protocolos que serão usados no processamento dos dados

- Portas: 0 – 65.535

  - Bem conhecidas: 0 – 1.023
  - Registradas: 1.024 – 49.151
  - Dinâmicas: 49.152 – 65.535

Numeração de porta

Port Number	Protocol	Transport Protocol	Port Number	Protocol	Transport Protocol
20/21	FTP	TCP	110	POP3	TCP
22	SSH	TCP	135	RPC	TCP
23	Telnet	TCP	137–139	NetBIOS	TCP and UDP
25	SMTP	TCP	143	IMAP	TCP
53	DNS	TCP and UDP	161/162	SNMP	UDP
67	DHCP	UDP	389	LDAP	TCP and UDP
69	TFTP	UDP	443	HTTPS	TCP
80	HTTP	TCP	445	SMB	TCP

Numeração de porta

- *Listening*: Porta aberta
- Established: conexão estabelecida
- CLOSE_WAIT: lado remoto finalizou a conexão
- TIME_WAIT: seu lado finalizou a conexão
- Obs.: A conexão é mantida por um tempo para permitir a chegada de pacotes atrasados!

Exercício

- Olhar as portas abertas no seu SO
  - Baixe e instale o CurrPorts (http://www.nirsoft.net/utils/cports.html)
  - Selecione uma porta e vá para File->Properties
  - Baixe e instale Fport (http://www.mcafee.com/us/downloads/free-tools/fport.aspx)
  - `netstat -an`
  - `netstat -b` (administrator)

INSTITUTO FEDERAL
São Paulo

Checando máquinas “live”

- Protocolo IP é um protocolo sem conexão – por si só não garante a entrega do pacote
- ICMP (*Internet Control Message Protocol*) foi criado para contornar este problema
- Provê mensagens de erros na camada de rede e apresenta a informação para o emissor em diversos tipos ICMP

Checando máquinas “live”

ICMP Message Type	Description and Important Codes
0: Echo Reply	Answer to a Type 8 Echo Request.
3: Destination Unreachable	Error message indicating the host or network cannot be reached. Codes: 0—Destination network unreachable 1—Destination host unreachable 6—Network unknown 7—Host unknown 9—Network administratively prohibited 10—Host administratively prohibited 13—Communication administratively prohibited
4: Source Quench	A congestion control message.
5: Redirect	Sent when there are two or more gateways available for the sender to use and the best route available to the destination is not the configured default gateway. Codes: 0—Redirect datagram for the network 1—Redirect datagram for the host
8: ECHO Request	A ping message, requesting an Echo reply.
11: Time Exceeded	The packet took too long to be routed to the destination (Code 0 is TTL expired).

Ping sweep

- Processo de pingar uma rede inteira

- Ferramentas:
  - Angry IP Scanner
  - Nmap
  - Pinger
  - WS_Ping
  - SuperScan
  - Friendly Pinger
  - Pinkie

- Obs.: Podem ser descobertas por IDS

Scan de portas

- Maioria dos scans de portas funcionam com a manipulação das flags do TCP

- Nmap: ferramenta mais utilizada para scan
  - Identificação de máquinas ativas
  - Scan de portas
  - Enumeração
  - Controla a velocidade do scan (mais lento mais difícil a descoberta)
  - Linha de comando e GUI
  - Múltiplas plataformas
  - Scan sobre TCP e UDP
  - Gratuito

nmap

- Sintaxe
  - `nmap <scan options> <target>`

- O `<target>` pode ser um único IP, múltiplos Ips (separados por espaços) ou uma rede inteira (notação por prefixo)

Nmap - exemplos

- `nmap 192.168.1.100`
- `nmap 192.168.1.100 192.168.1.101`
- `nmap 192.168.1.0/24`

- Ao executar o nmap sem nenhum parâmetro, a opção *default* será um scan “regular”

Exercícios

- Responder o questionário disponível no moodle!

INSTITUTO FEDERAL
São Paulo