Análise de tráfego em redes TCP/IP com tcpdump

João Eriberto Mota Filho

Brasília, DF, 18 abr. 2020

Sumário

- A análise de tráfego
- A estrutura de um protocolo
- O protocolo IP
- O protocolo TCP
- O protocolo UDP
- O protocolo ICMP
- O modelo OSI
- Técnica de uso do tcpdump na análise de tráfego
- Payloads que falam...
- Bridges na análise de tráfego
- Conclusão

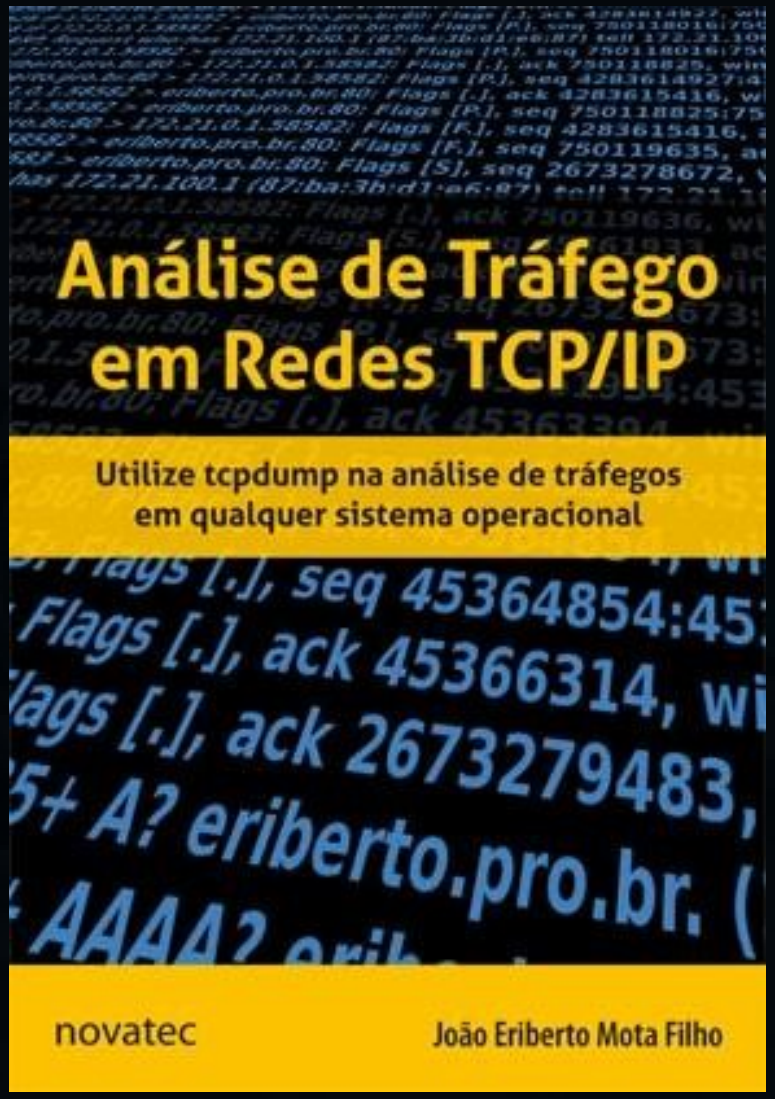
Sumário

A análise de tráfego

- Auxiliar de rede diz:
  - Chefe, deu pane! Parou tudo!
- Gerente de rede diz:
  - Troca o switch!
  - Agora troca o roteador!
  - Não deu. Troca os cabos.
  - Deve ser o link da tele. Liga pra lá.
- Auxiliar de rede diz:
  - Ai meu Deus... Tenho trabalho na faculdade hoje...
- Gerente de rede diz:
  - Nada disso! E já pede a pizza...

A análise de tráfego

Este minucurso está baseado em partes do livro Análise de Tráfego em Redes TCP/IP, da Novatec Editora.



A análise de tráfego

- A análise de tráfego permite, entre outras possibilidades:
  - Encontrar pontos de bloqueio na rede.
  - Detectar anomalias na rede.
  - Descobrir equipamentos e cabeamento defeituosos.
  - Observar importantes mensagens de sistema não mostradas pelas aplicações.
- A análise dependerá, principalmente, do conhecimento a respeito de protocolos de rede e de modelo OSI.
- Para entender os protocolos é necessário estudar RFCs.
- RFCs regulam o funcionamento da Internet!!!

A análise de tráfego

- Algumas RFCs importantes para a análise de tráfego: 768, 791, 792, 793, 1122, 6890, 8200 e todas as respectivas atualizações.
- Disponíveis em http://ietf.org/standards/ e outros sites.
- A ferramenta: tcpdump.
- Outras formas de auxílio: tshark, wireshark, mtr, ping, netcat, iptraf, packit etc.
- Auxílio para testes e estudo: simulador de redes CORE.
- Há diversas capturas de tráfego, disponíveis para estudo, em https://wiki.wireshark.org/SampleCaptures

A análise de tráfego

- Alguns pockets que podem ser usados como referência:

  > TCP/IP and tcpdump Pocket Reference Guide da SANS:

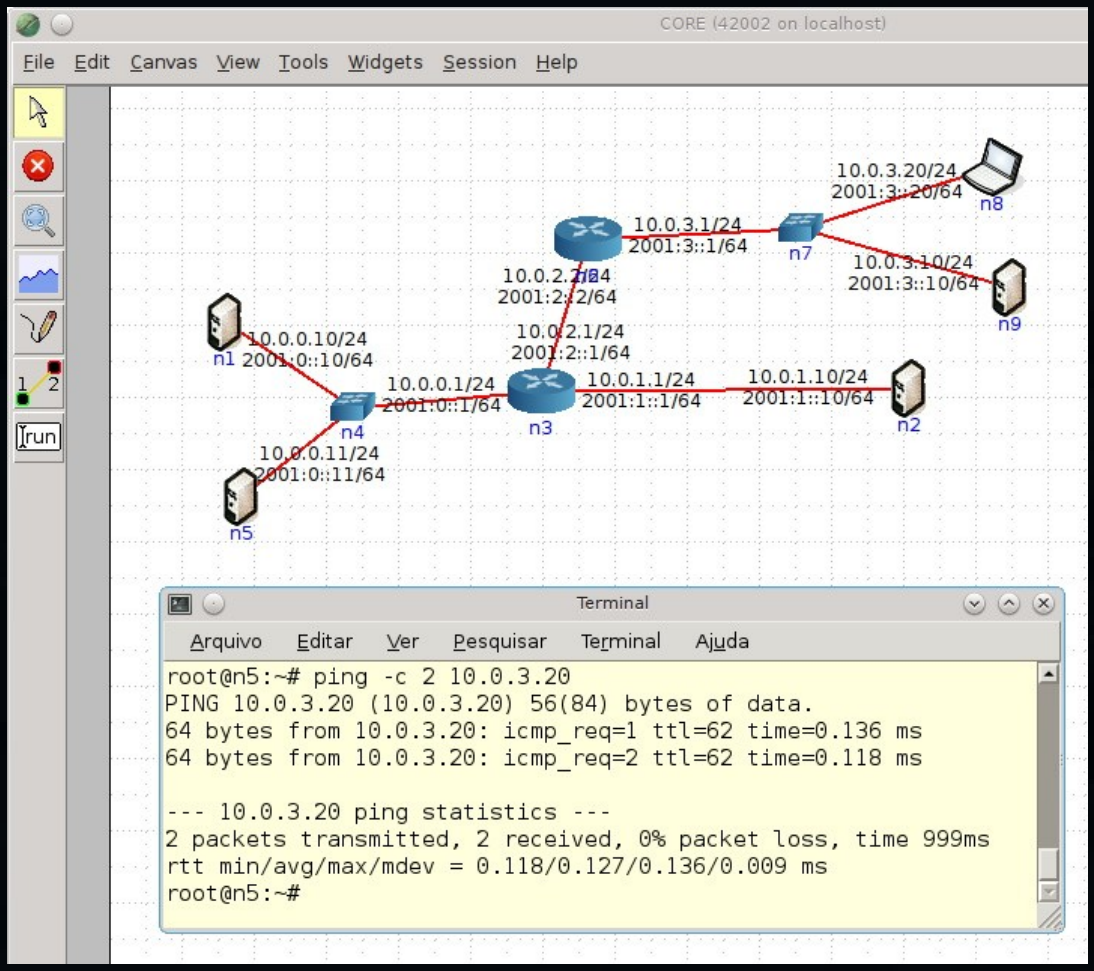
  https://www.sans.org/security-resources/tcpip.pdf (IPv4)

  https://www.sans.org/security-resources/ipv6_tcpip_pocketguide.pdf (IPv6)

  > Análise de tráfego em redes TCP/IP com tcpdump e windump:

  http://eriberto.pro.br/files/guia_tcpdump.pdf

A análise de tráfego



Simulador de redes CORE

(https://github.com/coreemu/core)

Docker: https://hub.docker.com/r/d3f0/coreemu_vnc/

Sumário

A estrutura de um protocolo

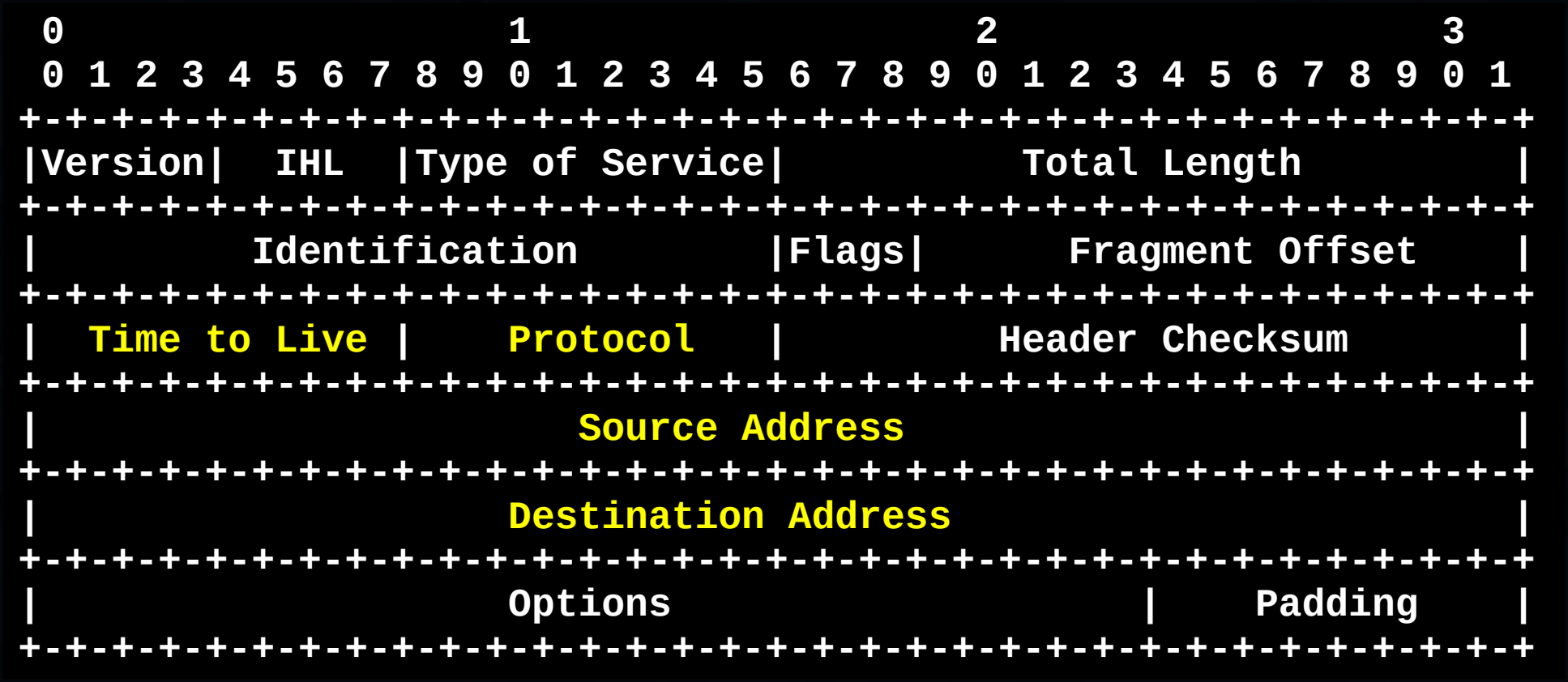
- Protocolos de rede são um conjunto de regras literais que estabelecem um padrão de comunicação e comportamento.

- Protocolos de rede, quando implementados, possuem uma estrutura básica, formada por um cabeçalho (ou header) e um payload (ou área de dados).

Sumário

O protocolo IP

- IP, RFC 791. O protocolo mais importante da família TCP/IP.

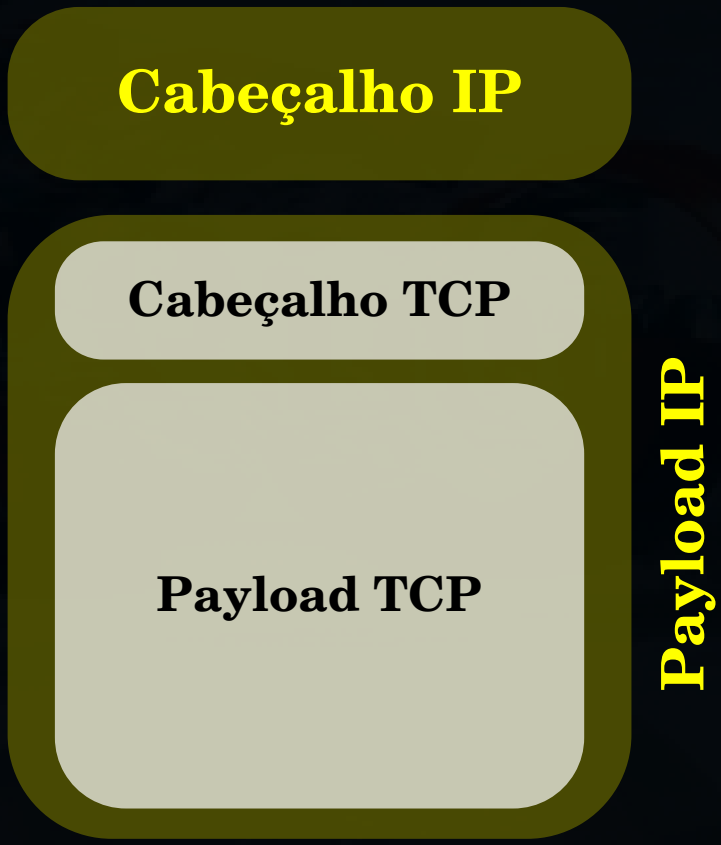


O protocolo IP

- O campo TTL é importante porque permite estimar o sistema operacional oposto e a quantidade de roteadores entre o host oposto e o local.
- Por default, sistemas operacionais utilizam valores iniciais de TTL que podem ser alterados. Unix e derivados diretos = 255, MS Windows = 128 e GNU/Linux = 64.
- Protocolos IP: são os protocolos que são encapsulados pelo IP. São listados pela IANA e um resumo poderá ser encontrado em /etc/protocols. Exemplos: ICMP, TCP e UDP.

O protocolo IP

- O IP é utilizado para transportar outros protocolos. Então, sempre haverá um protocolo IP no seu payload.



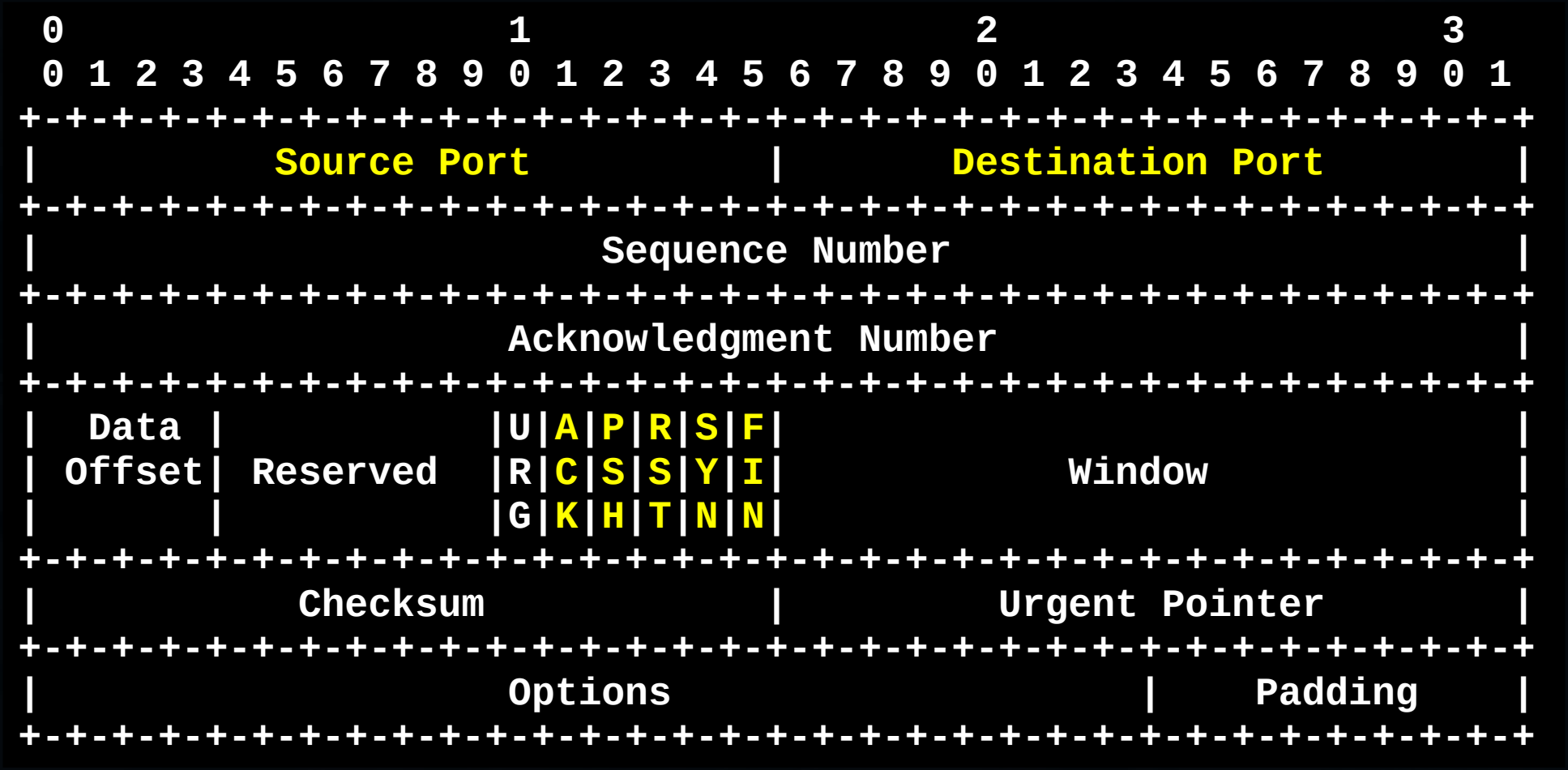
O protocolo IP

- Os protocolos IP mais importantes para a análise de tráfego são o TCP, o UDP e o ICMP.
- Entre todos os protocolos IP, somente o TCP e o UDP utilizam portas.

Sumário

O protocolo TCP

- TCP, RFC 793. O protocolo de transporte mais controlado, confiável e complexo da família TCP/IP.



O protocolo TCP - flags

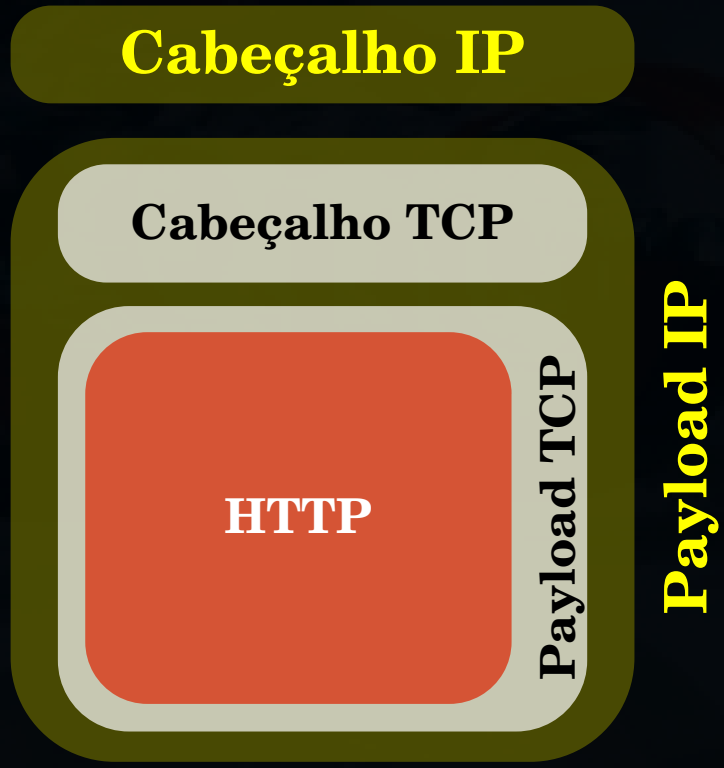
- Flags TCP:

  - Syn (synchronize): inicia conexões.
  - Fin (finish): finaliza conexões.
  - Psh (push): envia dados.
  - Ack (acknowledgment): confirmação de que é conhecido o número de sequência do próximo segmento a ser enviado pelo lado oposto.
  - Rst (reset): “não entendi”.

IMPORTANTE: as flags TCP são disparadas contra portas e somente a flag push possui payload.

O protocolo TCP

- O TCP (e também o UDP) é utilizado para transportar protocolos de uso específico dos usuários e das suas aplicações. Ex.: http, smtp, pop-3, ftp, msn, ssh, telnet, irc etc.



O protocolo TCP

- O protocolo TCP é orientado à conexão e a garante por intermédio do three-way handshake.
- É um protocolo full duplex.
- Em uma rede, independente do protocolo, é sempre o cliente quem inicia a conexão.
- Não há rede sem servidor ou serviço.

O protocolo TCP

```
cygnus:~# tcpdump -nSt host www.eriberto.pro.br

IP 10.1.1.15.49012 > 203.0.113.4.80: Flags [S], seq 747415379, win 5840, options
  [mss 1460,sackOK,TS val 11081666 ecr 0,nop,wscale 6], length 0
IP 203.0.113.4.80 > 10.1.1.15.49012: Flags [S.], seq 2372044971, ack 747415380, win
  5840, options [mss 1460], length 0
IP 10.1.1.15.49012 > 203.0.113.4.80: Flags [.], ack 2372044972, win 5840, length 0
IP 10.1.1.15.49012 > 203.0.113.4.80: Flags [P.], seq 747415380:747415928, ack
  2372044972, win 5840, length 548
IP 203.0.113.4.80 > 10.1.1.15.49012: Flags [.], ack 747415928, win 6576, length 0
IP 203.0.113.4.80 > 10.1.1.15.49012: Flags [P.], seq 2372044972:2372045807, ack
  747415928, win 6576, length 835
IP 10.1.1.15.49012 > 203.0.113.4.80: Flags [.], ack 2372045807, win 6680, length 0
IP 203.0.113.4.80 > 10.1.1.15.49012: Flags [F.], seq 2372045807, ack 747415928, win
  6576, length 0
IP 10.1.1.15.49012 > 203.0.113.4.80: Flags [.], ack 2372045808, win 6680, length 0
IP 10.1.1.15.49012 > 203.0.113.4.80: Flags [F.], seq 747415928, ack 2372045808, win
  6680, length 0
IP 203.0.113.4.80 > 10.1.1.15.49012: Flags [.], ack 747415929, win 6576, length 0
```

O protocolo TCP

```
cygnus:~# tcpdump -nStA host www.eriberto.pro.br

[...]
IP 10.1.1.15.49012 > 203.0.113.65.80: Flags [P.], seq 747415380:747415928, ack
  2372044972, win 5840, length 548
E..L..@.@.
...J7)..t.P,..T.b..P....Z..GET /teste.html HTTP/1.1
Host: www.eriberto.pro.br
User-Agent: Mozilla/5.0 (X11; U; Linux i686; pt-BR; rv:1.9.1.10) Gecko/20100623
  Iceweasel/3.5.10 (like Firefox/3.5.10)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: pt-br,pt;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
[...]
```

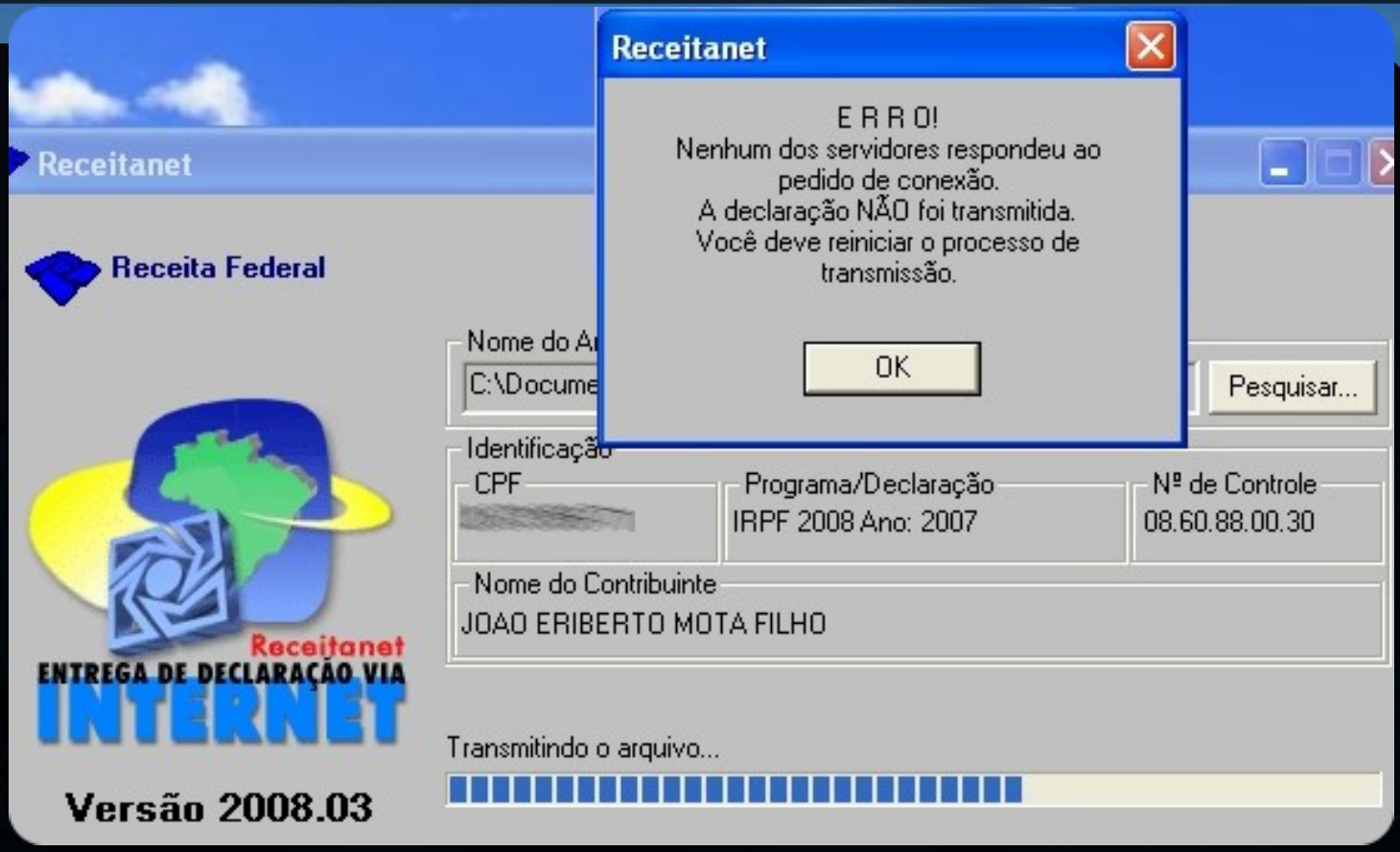
O protocolo TCP

```
cygnus:~# tcpdump -nSt port 81

IP 10.1.1.15.47887 > 203.0.113.8.81: Flags [S], seq 2535659221, win 5840, options
  [mss 1460,sackOK,TS val 295864 ecr 0,nop,wscale 6], length 0


IP 203.0.113.8.81 > 10.1.1.15.47887: Flags [R.], seq 0, ack 2535659222, win 0,
  length 0
```

O protocolo TCP




```
2008-04-30 02:52:37.137288 IP 192.168.1.100.52075 > 161.148.185.130.3456: Flags [S],
  seq 3214674887, win 5840, options [mss 1460,sackOK,TS val 810225 ecr 0,nop,wscale
  7], length 0

2008-04-30 02:52:37.152227 IP 161.148.185.130.3456 > 192.168.1.100.52075: Flags [R.],
  seq 2748955468, ack 3214674888, win 62780, length 0
```

O protocolo TCP

```
cygnus:~# tcpdump -nSt host hamurabi.acc.umu.se

IP 10.1.1.15.36306 > 130.239.18.165.80: Flags [S], seq 1134470901, win 5840,
  options [mss 1460,sackOK,TS val 547187 ecr 0,nop,wscale 6], length 0
IP 130.239.18.165.80 > 10.1.1.15.36306: Flags [S.], seq 1887642709, ack 1134470902,
  win 5792, options [mss 1460,sackOK,TS val 324228655 ecr 547187,nop,wscale 7],
  length 0
IP 10.1.1.15.36306 > 130.239.18.165.80: Flags [.], ack 1887642710, win 92, options
  [nop,nop,TS val 547265 ecr 324228655], length 0
IP 10.1.1.15.36306 > 130.239.18.165.80: Flags [P.], seq 1134470902:1134471443, ack
  1887642710, win 92, options [nop,nop,TS val 547265 ecr 324228655], length 541
IP 130.239.18.165.80 > 10.1.1.15.36306: Flags [.], ack 1134471443, win 54, options
  [nop,nop,TS val 324228688 ecr 547265], length 0
     [...] Ctrl c
IP 10.1.1.15.36306 > 130.239.18.165.80: Flags [F.], seq 1134471443, ack 1888127990,
  win 3563, options [nop,nop,TS val 549148 ecr 324229384,nop,nop,sack 2
  {1888135190:1888148150}{1888129430:1888130870}], length 0
IP 130.239.18.165.80 > 10.1.1.15.36306: Flags [P.], seq 1888148150:1888149590, ack
  1134471443, win 54, options [nop,nop,TS val 324229401 ecr 549051], length 1440
IP 10.1.1.15.36306 > 130.239.18.165.80: Flags [R], seq 1134471443, win 0, length 0
```

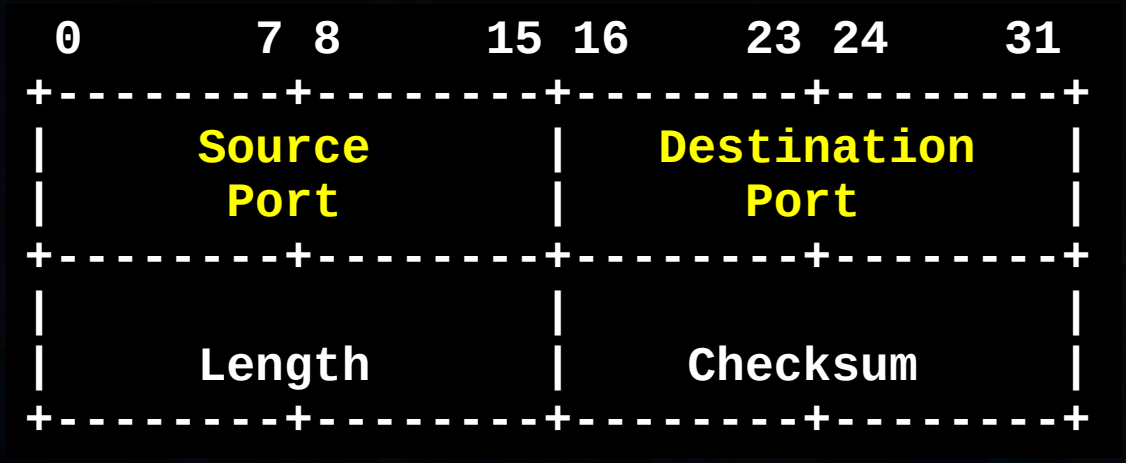
O protocolo TCP

```
IP6 2001::10.33467 > 2001:1::10.80: Flags [S], seq 4052414885, win 14400, options
  [mss 1440,sackOK,TS val 222843 ecr 0,nop,wscale 7], length 0
IP6 2001:1::10.80 > 2001::10.33467: Flags [S.], seq 3060786677, ack 4052414886, win
  14280, options [mss 1440,sackOK,TS val 222843 ecr 222843,nop,wscale 7], length 0
IP6 2001::10.33467 > 2001:1::10.80: Flags [.], ack 1, win 113, options [nop,nop,TS
  val 222843 ecr 222843], length 0
IP6 2001::10.33467 > 2001:1::10.80: Flags [P.], seq 1:237, ack 1, win 113, options
  [nop,nop,TS val 222844 ecr 222843], length 236
IP6 2001:1::10.80 > 2001::10.33467: Flags [.], ack 237, win 120, options
  [nop,nop,TS val 222844 ecr 222844], length 0
IP6 2001:1::10.80 > 2001::10.33467: Flags [P.], seq 1:725, ack 237, win 120,
  options [nop,nop,TS val 222845 ecr 222844], length 724
IP6 2001::10.33467 > 2001:1::10.80: Flags [.], ack 725, win 124, options
  [nop,nop,TS val 222845 ecr 222845], length 0
IP6 2001:1::10.80 > 2001::10.33467: Flags [F.], seq 725, ack 237, win 120, options
  [nop,nop,TS val 222845 ecr 222845], length 0
IP6 2001::10.33467 > 2001:1::10.80: Flags [F.], seq 237, ack 726, win 124, options
  [nop,nop,TS val 222845 ecr 222845], length 0
IP6 2001:1::10.80 > 2001::10.33467: Flags [.], ack 238, win 120, options
  [nop,nop,TS val 222845 ecr 222845], length 0
```

Sumário

O protocolo UDP

- UDP, RFC 768. O protocolo de transporte mais rápido da família TCP/IP.



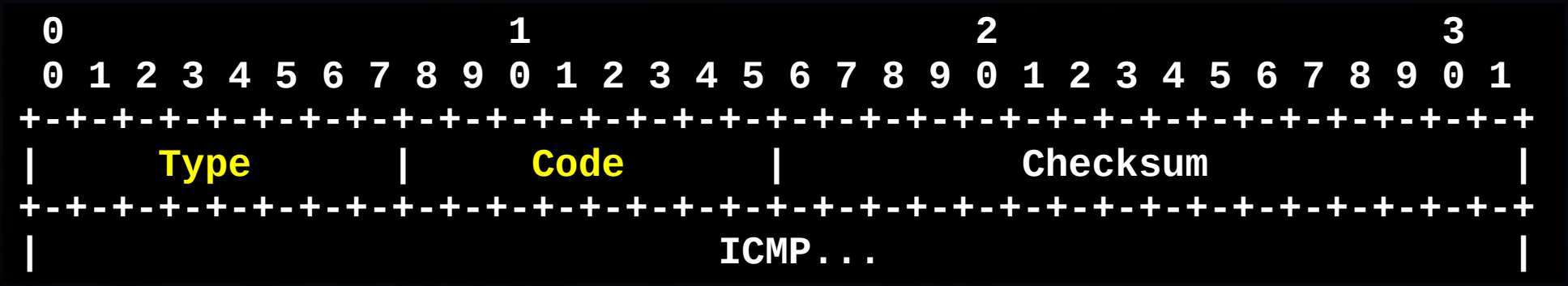
O protocolo UDP

- Somente os protocolos TCP e UDP possuem portas.
- Sempre que houver uma nova conexão TCP ou UDP, a porta do cliente mudará.
- O protocolo UDP é rápido mas exige que todo o controle de fluxo seja feito pela aplicação, ao contrário do TCP.

Sumário

O protocolo ICMP

- ICMP, RFC 792. O protocolo de controle do IP.



- Exemplos:

  - Tipo 8: echo request.
  - Tipo 0: echo reply.
  - Tipo 3, código 3: porta de destino inacessível.
  - Tipo 11, código 0: TTL expirado em trânsito.

O protocolo ICMP

- O ICMP é utilizado para controlar as atividades de rede.
- De um modo geral, entre os protocolos IP, somente o TCP não é assessorado pelo ICMP.
- Há vários tipos e códigos ICMP.
- Não se bloqueia ICMP em redes!!! Isso não cria segurança e sim descontrole. O correto é controlar o ICMP pelo sistema de firewall.
- Sistemas de firewall são compostos por diversos elementos como filtros de pacotes, proxies, IDS, IPS, verificadores de integridade etc. Firewalls não controlam somente TCP e UDP!

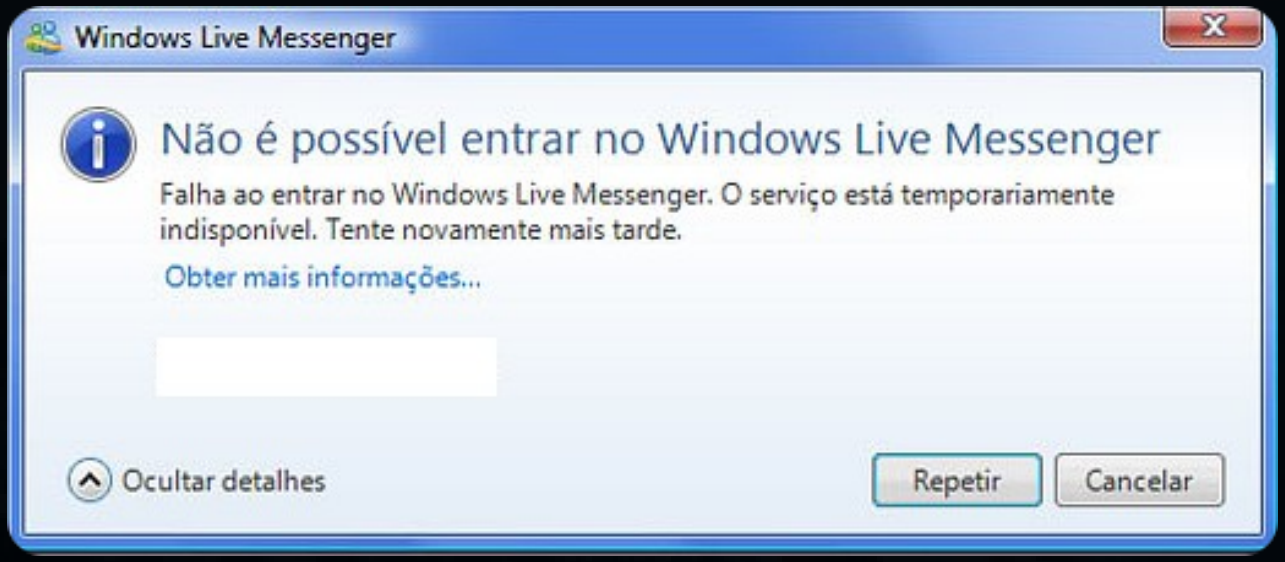
O protocolo ICMP

```
cygnus:~# tcpdump -nSt port 54 or icmp

IP 10.1.1.15.47014 > 10.1.1.1.54: UDP, length 6

IP 10.1.1.1 > 10.1.1.15: ICMP 10.1.1.1 udp port 54 unreachable, length 42
```

O protocolo ICMP




```
21:03:42.745064 IP 201.22.137.119 > 10.1.4.25: ICMP 65.54.179.248 unreachable -
  need to frag (mtu 1492), length 556
```

Sumário

O modelo OSI

- Modelo criado pela ISO para que fabricantes de hardware de rede possam desenvolver equipamentos compatíveis entre si.

Dados	Aplicação	Usuário, http, ftp, smtp, pop3, chat etc
Dados	Apresentação	SSL, conversão de padrões, (des)compressão
Dados	Sessão	Sessão de aplicações
Segmentos	Transporte	TCP, UDP
Pacotes[1]	Rede	IP e protocolos IP (exceto TCP e UDP) / roteador
Quadros[2]	Enlace	Ethernet, ATM, PPP, frame relay / switch, bridge
Bits	Física	Hub, cabos, placa de rede, ondas wireless etc

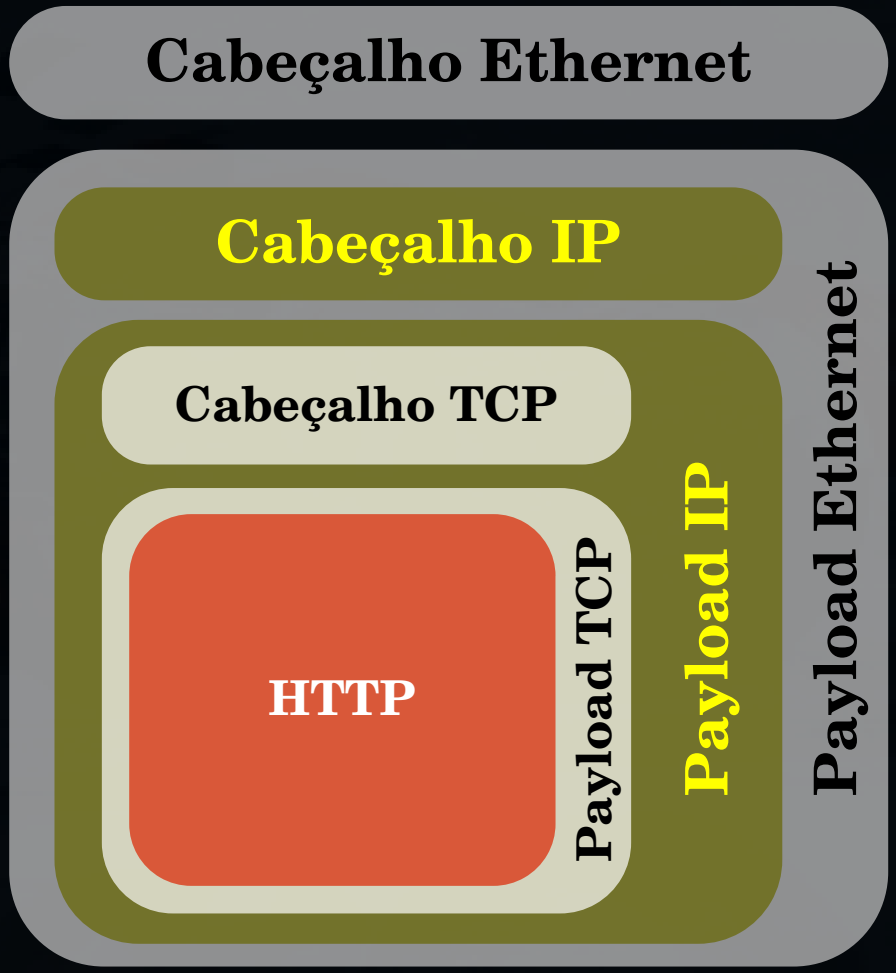
[1] pacotes ou datagramas
[2] quadros ou frames

O modelo OSI

Mas, de uma forma simples, o que é o modelo OSI???

O modelo OSI

- O modelo OSI é, em uma visão simplificada, isso:



O modelo OSI

- O modelo OSI, na prática, é uma referência ao encapsulamento de dados e protocolos, com níveis de preparação e controle.
- Um exemplo, utilizando o protocolo HTTP como aplicação:

O modelo OSI

- É importante ressaltar que os protocolos de transporte (TCP e UDP) servem para "transportar" dados referentes a usuários. Se não houver usuários, não haverá as camadas 4 a 7.

Sumário

Técnica de uso do tcpdump na análise de tráfego

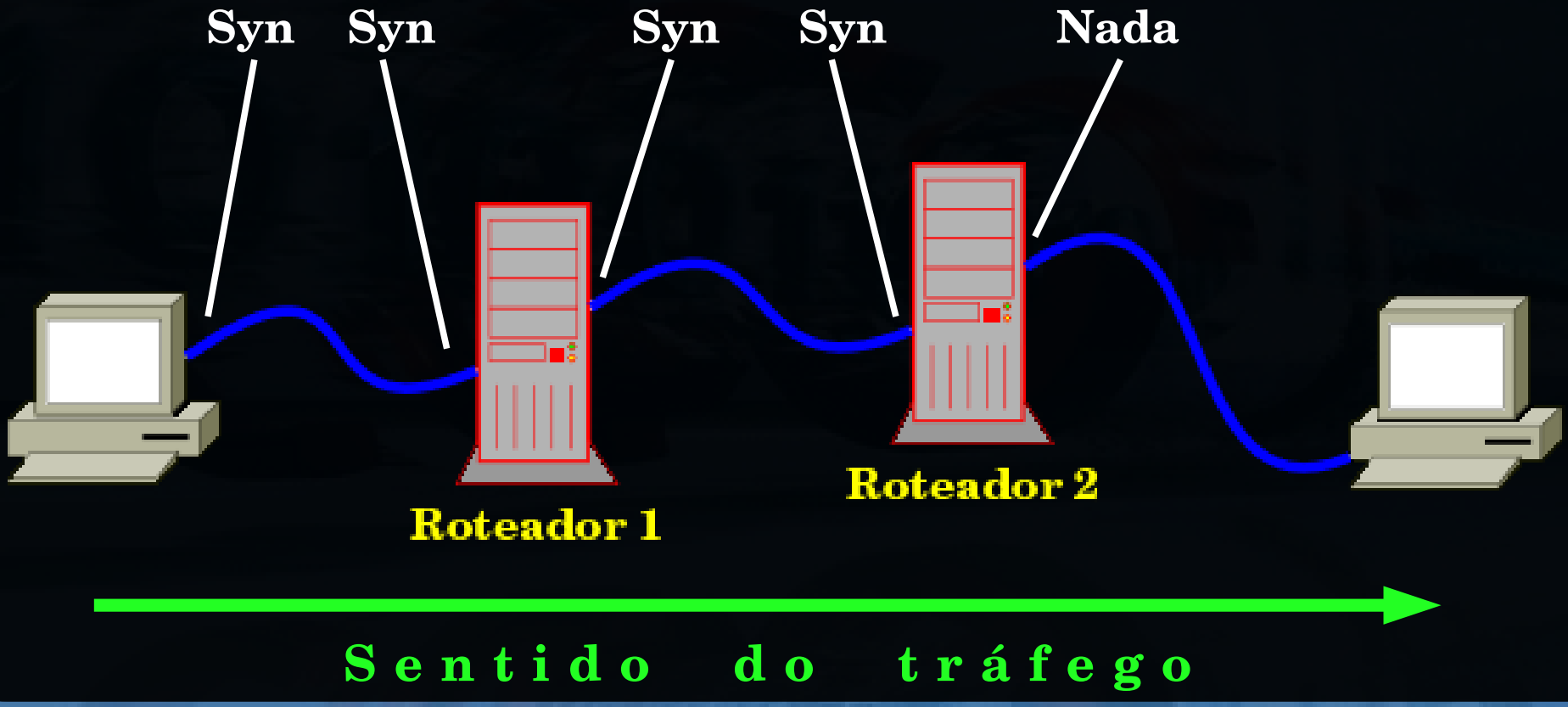
- Caso 1: bloqueio do tráfego em um elemento intermediário de rede (regras de filtragem mal feitas, erro no roteamento etc).

Técnica de uso do tcpdump na análise de tráfego

- Aplicar o tcpdump ao longo da topologia para descobrir o ponto de bloqueio.

Técnica de uso do tcpdump na análise de tráfego

- Aplicar o tcpdump ao longo da topologia para descobrir o ponto de bloqueio.

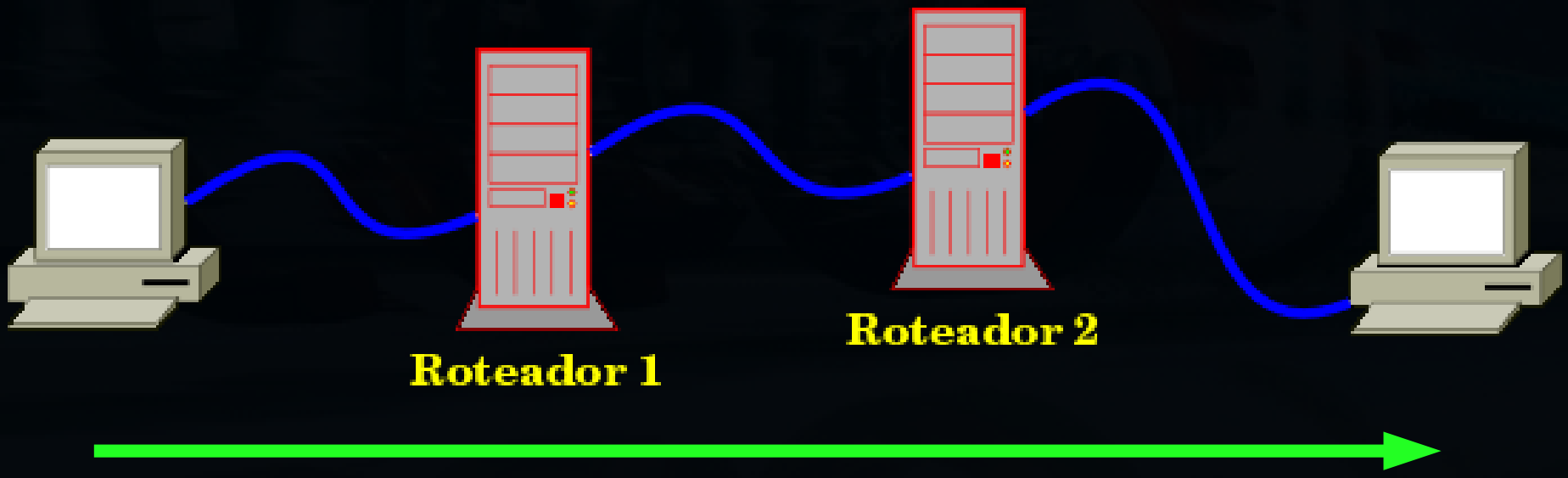


Técnica de uso do tcpdump na análise de tráfego

- Caso 2: bloqueio do tráfego por falha física na topologia.

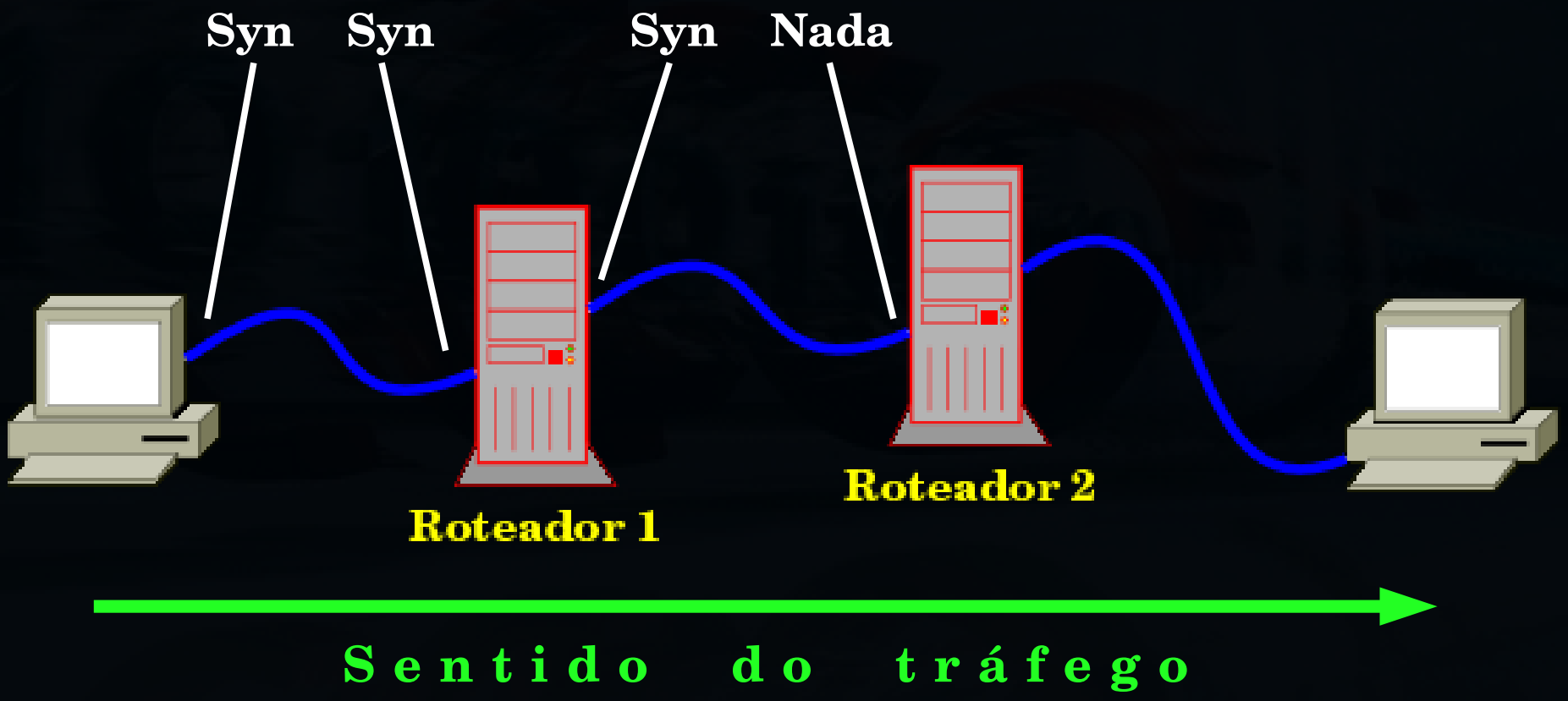
Técnica de uso do tcpdump na análise de tráfego

- Aplicar o tcpdump ao longo da topologia para descobrir o ponto de falha.



Técnica de uso do tcpdump na análise de tráfego

- Aplicar o tcpdump ao longo da topologia para descobrir o ponto de falha.



Sumário

Payloads que falam...

- Em casos de falhas de conexão em serviços, analise o payload do tráfego com o tcpdump.
- Muitos servidores dizem as causas dos problemas mas as aplicações não mostram o que foi dito. Exemplos: jabber, aplicações que usam bancos de dados etc.
- Utilize a opção -A para ver o payload.

Payloads que falam...

Payload:

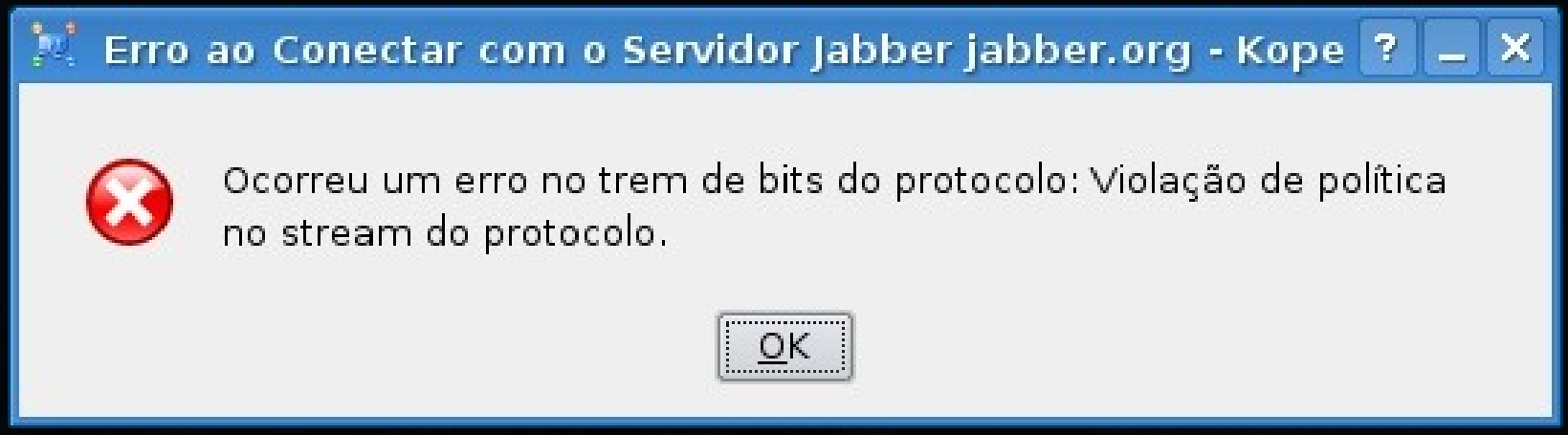
```
00:12:03.499715 IP 192.168.1.104.3306 > 192.168.1.101.34941: Flags [P.], seq 1:75,
  ack 1, win 33, options [nop,nop,TS val 23718975 ecr 5218436], length 74
E..~..@.@......h...e...}.(..@1&....!.......
.i.?.O..F....j.Host '192.168.1.101' is not allowed to connect to this MySQL server
```

Payloads que falam...

Payload:

```
16:48:26.120296 IP 172.16.10.49.3306 > 172.16.10.42.39903: Flags [P.], seq 79:162,
  ack 80, win 181, options [nop,nop,TS val 3773032 ecr 3202030], length 83
E....E@.@......1...*......bx........Z......
.9.h.0..O......#42000Access denied for user 'alpha31'@'172.16.10.42' to database
  'wikinet3'
```

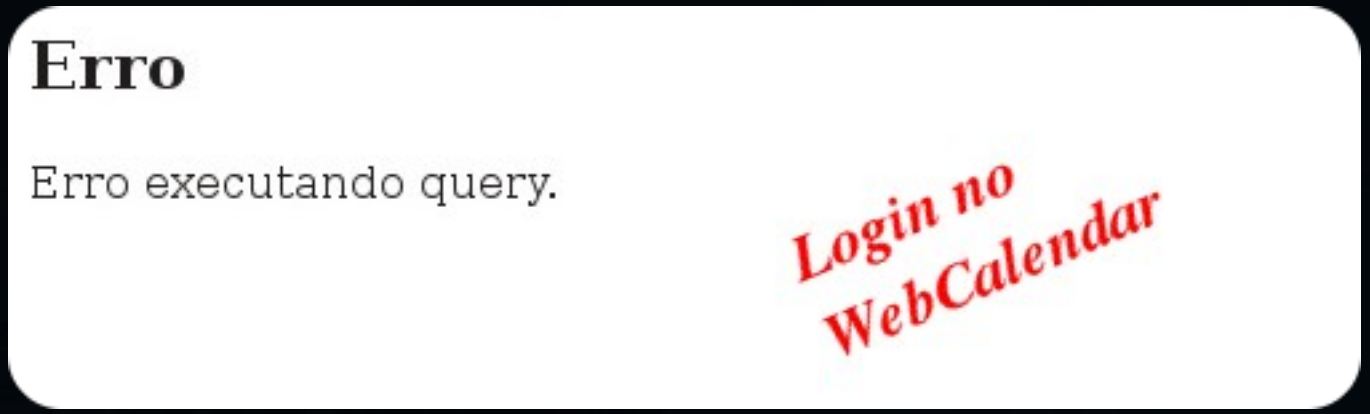
Payloads que falam...



Payload:

```
11:22:42.833577 IP 208.68.163.220.5222 > 172.16.0.1.57148: Flags [P.], seq 1:355, ack
  126, win 46, options [nop,nop,TS val 1913276961 ecr 20144826], length 354
E....$@.0....D.......f.<Y.E..1.......s.....
r
J!.3b.<?xml version='1.0'?><stream:stream xmlns='jabber:client' xmlns:stream='http://
  etherx.jabber.org/streams' id='521585298' from='jabber.org'
  xml:lang='en'><stream:error><policy-violation xmlns='urn:ietf:params:xml:ns:xmpp-
  streams'/><text xml:lang='' xmlns='urn:ietf:params:xml:ns:xmpp-streams'>Use of
  STARTTLS required</text></stream:error></stream:stream>
```

Payloads que falam...



Payload:

```
16:19:50.614450 IP 172.30.1.5.3306 > 172.30.1.4.58868: Flags [P.], seq 391:467, ack
  611, win 972, options [nop,nop,TS val 306116600 ecr 306114953], length 76
E...~.@.@.a=.............~e..........Z......
.>...>..H......#HY000File './agenda1/webcal_entry_log.MYD' not found (Errcode: 30)
```

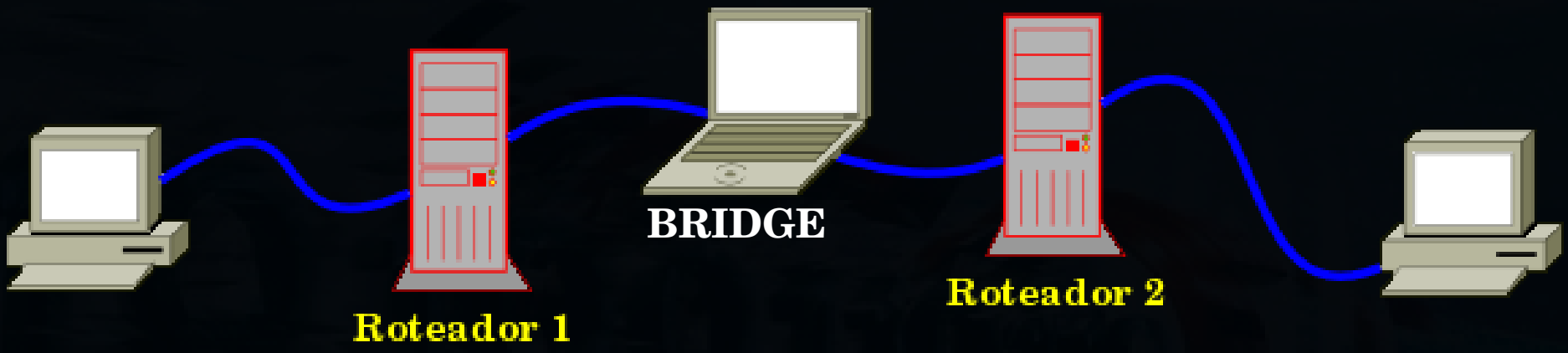
Sumário

Bridges na análise de tráfego

- Bridges são elementos que atuam na camada 2 do modelo OSI e são como switches (e são invisíveis!).
- Caso os ativos de rede não permitam o uso de tcpdump (roteadores proprietários etc.), utilize um notebook, com duas placas de rede configuradas como bridge, para fazer a análise.
- A opção -e no tcpdump mostra a camada de enlace no tráfego.
- A segunda placa de rede poderá ser um adaptador USB-Ethernet.
- Bridges no Debian: http://bit.ly/bridge_debian

Bridges na análise de tráfego

- O uso de bridge na análise de tráfego.



Adaptador USB-Ethernet (venda em lojas, Mercado Livre e eBay). Custa US$ 2 no eBay.

Sumário

Conclusão

- A análise de tráfego é um conhecimento fundamental para quem trabalha com redes de computadores. Sem ela, em momentos de panes e de problemas em redes, o administrador será um mero testador de possibilidades infundadas.
- A ferramenta tcpdump é a melhor aliada na análise de tráfego. No entanto, outras ferramentas como o wireshark e o mtr poderão ser úteis, principalmente para o estudo e aprendizado.
- Payloads falam coisas importantes... ouça-os!
- Não se bloqueia ICMP em redes! Sem ele, haverá um certo grau de perda de controle.

continua...

Conclusão

Referências (usando tcpdump) para estudo:

- MOTA FILHO, João Eriberto. Análise de tráfego em redes TCP/IP. Editora Novatec, 2013.
- STEVENS, W. Richard; FALL, Kevin R. TCP/IP Illustrated, Volume I, 2ª edição. Editora Addison-Wesley, 2011.
- WIRESHARK.ORG. Seção de capturas no site, em http://wiki.wireshark.org/SampleCaptures.

Esta palestra está disponível em:

http://eriberto.pro.br

Siga-me no Twitter @eribertomota