HANDS-ON: ANÁLISE DE TRÁFEGO EM REDES TCP/IP

ADRIANA VIRIATO

Analista de Redes
PoP-BA

GILDÁSIO JÚNIOR

Analista de Segurança
PoP-BA

Realização:

PoP-BA Ponto de Presença da RNP na Bahia

RNP

Apoio:

STI Superintendência de Tecnologia da Informação | UFBA

nic.br

Importância da Análise de Tráfego de Rede

- *Troubleshooting* de redes
- Investigação de incidentes de segurança
- Estudo de protocolos de redes
- ...

RFCs Relevantes

RFCs são cruciais para o conhecimento de redes de computadores. Algumas delas são essenciais para entendimento dos protocolos e análise do tráfego:

- 768: UDP
- 791: IP
- 792: ICMP
- 793: TCP
- 1122: Requirements for Internet Hosts
- 6890: Special-Purpose IP Address Registries
- 8200: IPv6

E suas respectivas atualizações.

Ferramentas Utilizadas

Existem diversas ferramentas que podem ser usadas no processo de conhecimento e verificação da rede e de seus protocolos através de verificação de serviços, geração e análise de tráfego. Algumas ferramentas utilizadas no curso:

- *tcpdump / windump / wireshark*
- *nc*
- *traceroute / mtr*
- *hping3*
- *nmap*

Existem muitas outras ferramentas que podem ser usadas no processo de análise de tráfego mas que não serão demonstradas aqui nesse curso. Por exemplo: *tcptraceroute*, *iptables*, *iperf*, *packit* ...

Referências para estudo

A captura de tráfego é uma das atividades essenciais no processo de análise. Recomendamos a continuação dos estudos para além do momento do curso.

Livro Análise de Tráfego em Redes TCP/IP

- MOTA FILHO, João Eriberto. Análise de Tráfego em Redes TCP/IP: Utilize tcpdump na análise de tráfegos em qualquer sistema operacional. Novatec Editora, 2013.
- Minicurso Análise de Tráfego em Redes TCP/IP Parte 1: https://www.youtube.com/watch?v=gK3gl3Vh8L0
- Minicurso Análise de Tráfego em Redes TCP/IP Parte 2: https://www.youtube.com/watch?v=YFOBLyf2SG0

Existem capturas de tráfegos divulgadas publicamente que podem ser utilizadas para esse fim.

Lista de captura de tráfegos feita pela equipe de desenvolvimento do Wireshark

- https://wiki.wireshark.org/SampleCaptures

O Curso: Funcionamento

Dois encontros:

- Segunda, 14/09, 14h ~ 16h
- Quarta, 16/09, 14h ~ 16h

Uso da sala de vídeo conferência:

- https://conferenciaweb.rnp.br/webconf/wtr

Praticar:

- Máquina virtual disponibilizada; ou
- Computador com as ferramentas instaladas:
  - *tcpdump / windump / wireshark*
  - *nc*
  - *traceroute / mtr*
  - *hping3*
  - *nmap*

O Curso: Conteudo

Explicaremos os principais protocolos da rede TCP/IP verificando os campos de seus cabeçalhos.

- Dia 1
  - IPv4 / IPv6
  - ICMP
- Dia 2
  - TCP
  - UDP
  - Exemplos de uso de análise de tráfego para *troubleshooting*

O *tcpdump* será a ferramenta utilizada para verificação dos campos dos cabeçalhos em algumas situações do dia a dia.

O Curso: Objetivo

Fornecer o conhecimento de base necessário para que os alunos sejam capazes de realizar análises de tráfego em redes TCP/IP utilizando como ferramenta para:

- Identificar e resolver problemas no que tange área de redes computacionais;
- Estudar e aprender a fundo sobre os protocolos de rede;
- Analisar comportamentos anômalos em redes de computadores;
- Dentre outras atividades.

WTR
WORKSHOP
DE TECNOLOGIAS DE REDES DO POP-BA

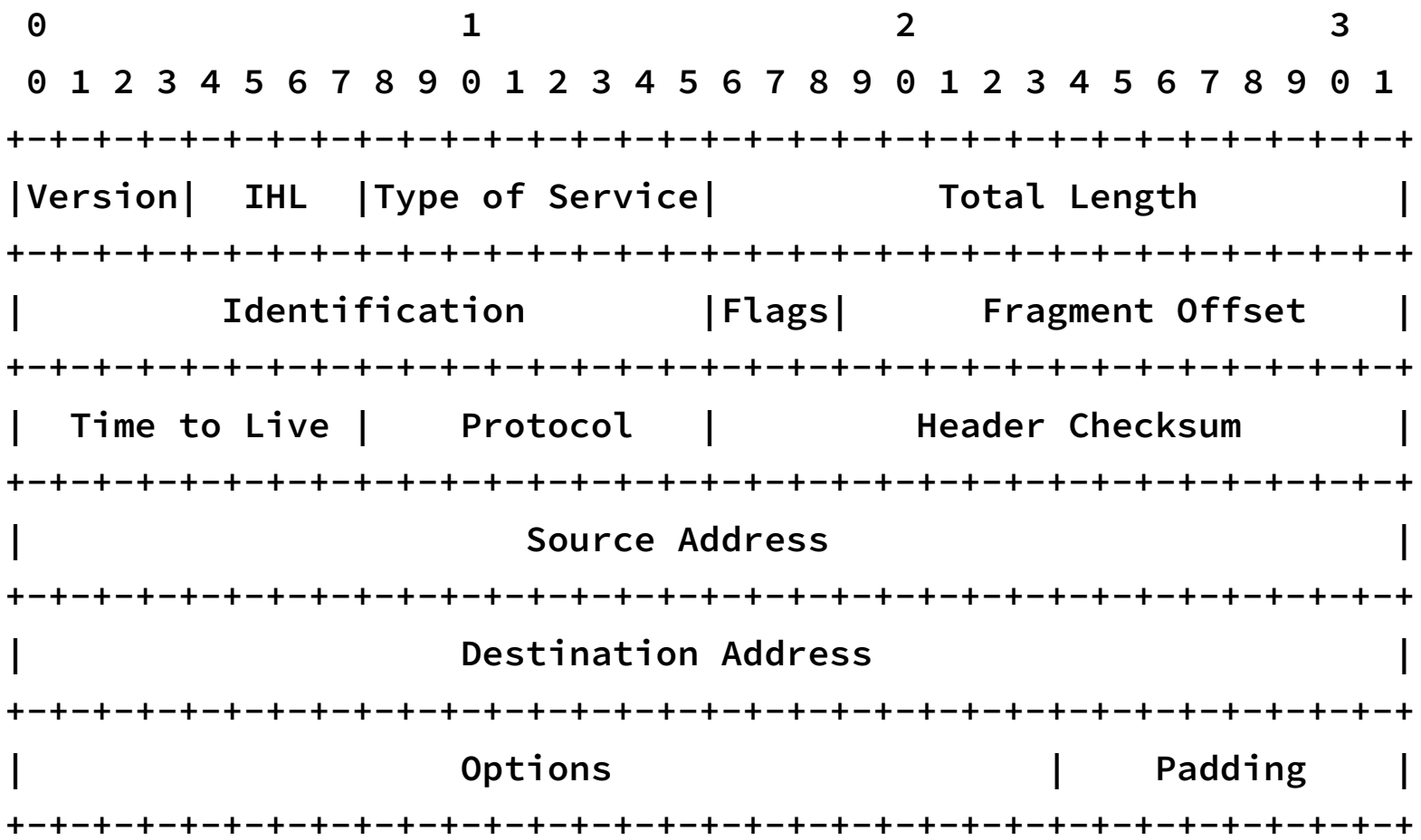
14 A 18 DE SETEMBRO DE 2020

IPv4

PoP-BA
Ponto de Presença da RNP na Bahia

RNP 30 anos
ORGANIZAÇÃO SOCIAL DO MCTI

IPv4


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Version
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Options
Padding

Análise de Tráfego

```
$ sudo tcpdump -i eno1 -n host 10.1.0.38
$ nc 10.1.0.38 80
```

```
11:13:48.627195 IP 10.1.0.114.36520 > 10.1.0.38.80: Flags [S], seq
3424060001, win 64240, options [mss 1460,sackOK,TS val 500434377 ecr
0,nop,wscale 7], length 0
```

Análise de Tráfego


```
$ sudo tcpdump -i eno1 -n host 10.1.0.38 or host fe80::c4aa:2dff:fe74:4dc3
$ ping -c 1 10.1.0.38
$ ping -c 1 fe80::c4aa:2dff:fe74:4dc3

11:27:09.227398 IP 10.1.0.114 > 10.1.0.38: ICMP echo request, id 31795,
seq 1, length 64
11:27:09.253030 IP 10.1.0.38 > 10.1.0.114: ICMP echo reply, id 31795, seq
1, length 64

11:27:11.680654 IP6 fe80::87a3:4fca:e840:9748 > fe80::c4aa:2dff:fe74:4dc3:
ICMP6, echo request, seq 1, length 64
11:27:11.713113 IP6 fe80::c4aa:2dff:fe74:4dc3 > fe80::87a3:4fca:e840:9748:
ICMP6, echo reply, seq 1, length 64
```

Análise de Tráfego

```
$ sudo tcpdump -i eno1 -n host 10.1.0.38 -vv
$ nc 10.1.0.38 80
```

```
11:14:13.406988 IP (tos 0x0, ttl 64, id 16480, offset 0, flags [DF],
proto TCP (6), length 60) 10.1.0.114.36594 > 10.1.0.38.80: Flags [S],
cksum 0x14c8 (incorrect -> 0x2cd9), seq 3136765178, win 64240, options
[mss 1460,sackOK,TS val 500459156 ecr 0,nop,wscale 7], length 0
```

Análise de Tráfego

```
$ sudo tcpdump -i eno1 -n -vvv icmp
$ ping -c 1 -s 4000 10.1.0.38
```

```
11:32:15.798311 IP (tos 0x0, ttl 64, id 5432, offset 0, flags [+], proto
ICMP (1), length 1500) 10.1.0.114 > 10.1.0.38: ICMP echo request, id
32010, seq 1, length 1480
```

```
11:32:15.798321 IP (tos 0x0, ttl 64, id 5432, offset 1480, flags [+],
proto ICMP (1), length 1500) 10.1.0.114 > 10.1.0.38: ip-proto-1
```

```
11:32:15.798325 IP (tos 0x0, ttl 64, id 5432, offset 2960, flags [none],
proto ICMP (1), length 1068) 10.1.0.114 > 10.1.0.38: ip-proto-1
```

Análise de Tráfego

```
$ sudo tcpdump -i eno1 -n -v host 10.1.0.38
$ ping -c 1 -M do 10.1.0.38 -s 1472


11:43:05.266393 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto
ICMP (1), length 1500)
    10.1.0.114 > 10.1.0.38: ICMP echo request, id 32371, seq 1, length
1480
11:43:05.287230 IP (tos 0x0, ttl 64, id 42271, offset 0, flags [none],
proto ICMP (1), length 1500)
    10.1.0.38 > 10.1.0.114: ICMP echo reply, id 32371, seq 1, length
1480
```

Análise de Tráfego

```
$ ping -c 1 -M do 10.1.0.38 -s 4000

PING 10.1.0.38 (10.1.0.38) 4000(4028) bytes of data.
ping: local error: Message too long, mtu=1500

--- 10.1.0.38 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms
```

Análise de Tráfego

http://www.iana.org/assignments/protocol-numbers

```
$ less /etc/protocols

$ getent protocols tcp
tcp                   6 TCP

$ getent protocols udp
udp                   17 UDP

$ getent protocols icmp
icmp                  1 ICMP
```

Análise de Tráfego


```
$ sudo tcpdump -i eno1 -n -v ip dst 10.1.0.38 and not arp
$ nc 10.1.0.38 80
$ nc -u 10.1.0.38 23
$ ping  -c 1 10.1.0.38
```

```
15:27:51.020143 IP (tos 0x0, ttl 64, id 33997, offset 0, flags [DF], proto
UDP (17), length 34) 10.1.0.114.36278 > 10.1.0.38.23: UDP, length 6
15:28:09.906333 IP (tos 0x0, ttl 64, id 43653, offset 0, flags [DF], proto
ICMP (1), length 84) 10.1.0.114 > 10.1.0.38: ICMP echo request, id 1788, seq
1, length 64
15:28:18.224347 IP (tos 0x0, ttl 64, id 27312, offset 0, flags [DF], proto
TCP (6), length 60) 10.1.0.114.41278 > 10.1.0.38.80: Flags [S], cksum 0x14c8
(incorrect -> 0x225a), seq 4121385857, win 64240, options [mss
1460,sackOK,TS val 515703975 ecr 0,nop,wscale 7], length 0
```

Análise de Tráfego


```
$ sudo tcpdump -i eno1 -n -vvv -X icmp
$ ping -c 1 10.1.0.38

11:30:10.889735 IP (tos 0x0, ttl 64, id 52808, offset 0, flags [DF], proto
ICMP (1), length 84)
    10.1.0.114 > 10.1.0.38: ICMP echo request, id 31927, seq 1, length 64
        0x0000:  4500 0054 ce48 4000 4001 57c7 0a01 0072  E..T.H@.@.W....r
        0x0010:  0a01 0026 0800 bbec 7cb7 0001 7295 575f  ...&....|...r.W_
        0x0020:  0000 0000 2993 0d00 0000 0000 1011 1213  ....).........
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
```

Análise de Tráfego

Versão: 0x4

```
11:30:10.889735 IP (tos 0x0, ttl 64, id 52808, offset 0, flags [DF], proto
ICMP (1), length 84)
    10.1.0.114 > 10.1.0.38: ICMP echo request, id 31927, seq 1, length 64
        0x0000:  4500 0054 ce48 4000 4001 57c7 0a01 0072  E..T.H@.@.W....r
        0x0010:  0a01 0026 0800 bbec 7cb7 0001 7295 575f  ...&....|...r.W_
        0x0020:  0000 0000 2993 0d00 0000 0000 1011 1213  ....).........
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
```

Análise de Tráfego

IHL: 0x5

```
11:30:10.889735 IP (tos 0x0, ttl 64, id 52808, offset 0, flags [DF], proto
ICMP (1), length 84)
    10.1.0.114 > 10.1.0.38: ICMP echo request, id 31927, seq 1, length 64
        0x0000:  4500 0054 ce48 4000 4001 57c7 0a01 0072  E..T.H@.@.W....r
        0x0010:  0a01 0026 0800 bbec 7cb7 0001 7295 575f  ...&....|...r.W_
        0x0020:  0000 0000 2993 0d00 0000 0000 1011 1213  ....).........
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
```

Análise de Tráfego

ToS: 0x00

```
11:30:10.889735 IP (tos 0x0, ttl 64, id 52808, offset 0, flags [DF], proto
ICMP (1), length 84)
    10.1.0.114 > 10.1.0.38: ICMP echo request, id 31927, seq 1, length 64
        0x0000:  4500 0054 ce48 4000 4001 57c7 0a01 0072  E..T.H@.@.W....r
        0x0010:  0a01 0026 0800 bbec 7cb7 0001 7295 575f  ...&....|...r.W_
        0x0020:  0000 0000 2993 0d00 0000 0000 1011 1213  ....).........
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
```

Análise de Tráfego

```
Total Length: 0x0054


11:30:10.889735 IP (tos 0x0, ttl 64, id 52808, offset 0, flags [DF], proto
ICMP (1), length 84)
    10.1.0.114 > 10.1.0.38: ICMP echo request, id 31927, seq 1, length 64
        0x0000:  4500 0054 ce48 4000 4001 57c7 0a01 0072  E..T.H@.@.W....r
        0x0010:  0a01 0026 0800 bbec 7cb7 0001 7295 575f  ...&....|...r.W_
        0x0020:  0000 0000 2993 0d00 0000 0000 1011 1213  ....).........
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
```

Análise de Tráfego

```
Identification: 0xce48


11:30:10.889735 IP (tos 0x0, ttl 64, id 52808, offset 0, flags [DF], proto
ICMP (1), length 84)
    10.1.0.114 > 10.1.0.38: ICMP echo request, id 31927, seq 1, length 64
        0x0000:  4500 0054 ce48 4000 4001 57c7 0a01 0072  E..T.H@.@.W....r
        0x0010:  0a01 0026 0800 bbec 7cb7 0001 7295 575f  ...&....|...r.W_
        0x0020:  0000 0000 2993 0d00 0000 0000 1011 1213  ....).........
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
```

Análise de Tráfego

```
Flags: 0x4 → 0100
               0DM
                FF
11:30:10.889735 IP (tos 0x0, ttl 64, id 52808, offset 0, flags [DF], proto
ICMP (1), length 84)
    10.1.0.114 > 10.1.0.38: ICMP echo request, id 31927, seq 1, length 64
        0x0000:  4500 0054 ce48 4000 4001 57c7 0a01 0072  E..T.H@.@.W....r
        0x0010:  0a01 0026 0800 bbec 7cb7 0001 7295 575f  ...&....|...r.W_
        0x0020:  0000 0000 2993 0d00 0000 0000 1011 1213  ....).........
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
```

Análise de Tráfego

Fragment Offset: 0x4000 → 01000000 00000000

```
11:30:10.889735 IP (tos 0x0, ttl 64, id 52808, offset 0, flags [DF], proto
ICMP (1), length 84)
    10.1.0.114 > 10.1.0.38: ICMP echo request, id 31927, seq 1, length 64
        0x0000:  4500 0054 ce48 4000 4001 57c7 0a01 0072  E..T.H@.@.W....r
        0x0010:  0a01 0026 0800 bbec 7cb7 0001 7295 575f  ...&....|...r.W_
        0x0020:  0000 0000 2993 0d00 0000 0000 1011 1213  ....).........
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
```

Análise de Tráfego

```
Time To Live: 0x40


11:30:10.889735 IP (tos 0x0, ttl 64, id 52808, offset 0, flags [DF], proto
ICMP (1), length 84)
    10.1.0.114 > 10.1.0.38: ICMP echo request, id 31927, seq 1, length 64
        0x0000:  4500 0054 ce48 4000 4001 57c7 0a01 0072  E..T.H@.@.W....r
        0x0010:  0a01 0026 0800 bbec 7cb7 0001 7295 575f  ...&....|...r.W_
        0x0020:  0000 0000 2993 0d00 0000 0000 1011 1213  ....).........
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
```

Análise de Tráfego

```
Protocol: 0x01


11:30:10.889735 IP (tos 0x0, ttl 64, id 52808, offset 0, flags [DF], proto
ICMP (1), length 84)
    10.1.0.114 > 10.1.0.38: ICMP echo request, id 31927, seq 1, length 64
        0x0000:  4500 0054 ce48 4000 4001 57c7 0a01 0072  E..T.H@.@.W....r
        0x0010:  0a01 0026 0800 bbec 7cb7 0001 7295 575f  ...&....|...r.W_
        0x0020:  0000 0000 2993 0d00 0000 0000 1011 1213  ....).........
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
```

Análise de Tráfego

```
Header Checksum: 0x57c7


11:30:10.889735 IP (tos 0x0, ttl 64, id 52808, offset 0, flags [DF], proto
ICMP (1), length 84)
    10.1.0.114 > 10.1.0.38: ICMP echo request, id 31927, seq 1, length 64
        0x0000:  4500 0054 ce48 4000 4001 57c7 0a01 0072  E..T.H@.@.W....r
        0x0010:  0a01 0026 0800 bbec 7cb7 0001 7295 575f  ...&....|...r.W_
        0x0020:  0000 0000 2993 0d00 0000 0000 1011 1213  ....).........
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
```

Análise de Tráfego


```
Source Address: 0x0a 0x01 0x00 0x72


11:30:10.889735 IP (tos 0x0, ttl 64, id 52808, offset 0, flags [DF], proto
ICMP (1), length 84)
    10.1.0.114 > 10.1.0.38: ICMP echo request, id 31927, seq 1, length 64
        0x0000:  4500 0054 ce48 4000 4001 57c7 0a01 0072  E..T.H@.@.W....r
        0x0010:  0a01 0026 0800 bbec 7cb7 0001 7295 575f  ...&....|...r.W_
        0x0020:  0000 0000 2993 0d00 0000 0000 1011 1213  ....).........
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
```

Análise de Tráfego

```
Destination Address: 0x0a 0x01 0x00 0x26


11:30:10.889735 IP (tos 0x0, ttl 64, id 52808, offset 0, flags [DF], proto
ICMP (1), length 84)
    10.1.0.114 > 10.1.0.38: ICMP echo request, id 31927, seq 1, length 64
        0x0000:  4500 0054 ce48 4000 4001 57c7 0a01 0072  E..T.H@.@.W....r
        0x0010:  0a01 0026 0800 bbec 7cb7 0001 7295 575f  ...&....|...r.W_
        0x0020:  0000 0000 2993 0d00 0000 0000 1011 1213  ....).........
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
```

WTR
WORKSHOP
DE TECNOLOGIAS DE REDES DO POP-BA

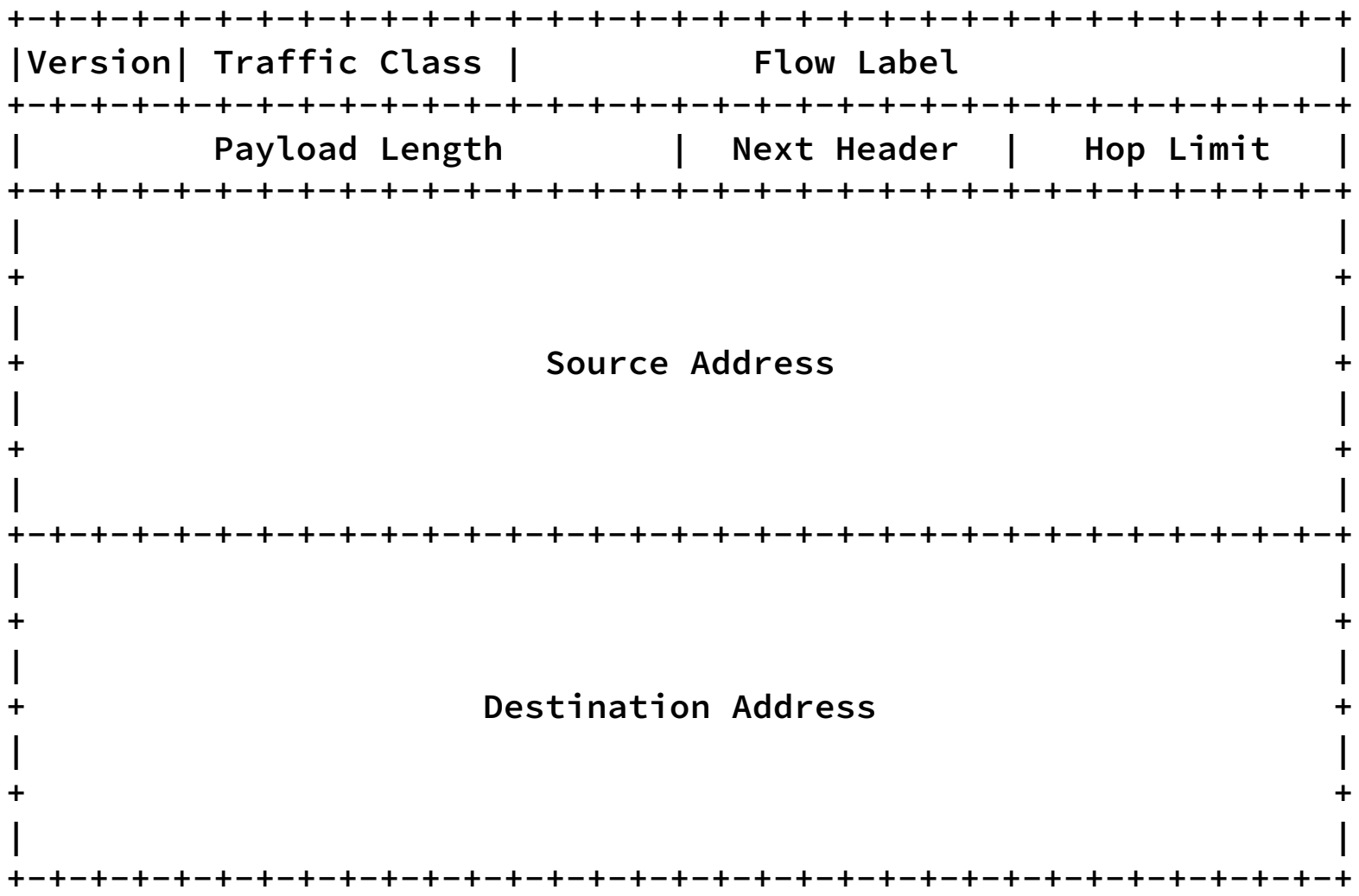
14 A 18 DE SETEMBRO DE 2020

IPv6

PoP-BA
Ponto de Presença da RNP na Bahia

RNP 30 anos
ORGANIZAÇÃO SOCIAL DO MCTI

IPv6


Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
Source Address
Destination Address

IPv6

IPv4	IPv6
Version	Version
Source Address	Source Address
Destination Address	Destination Address
Type of Service	Traffic Class
Total Length	Payload Length
Protocol	Next Header
Time To Live	Hop Limit
-	Flow Label

WTR
WORKSHOP
DE TECNOLOGIAS DE REDES DO POP-BA

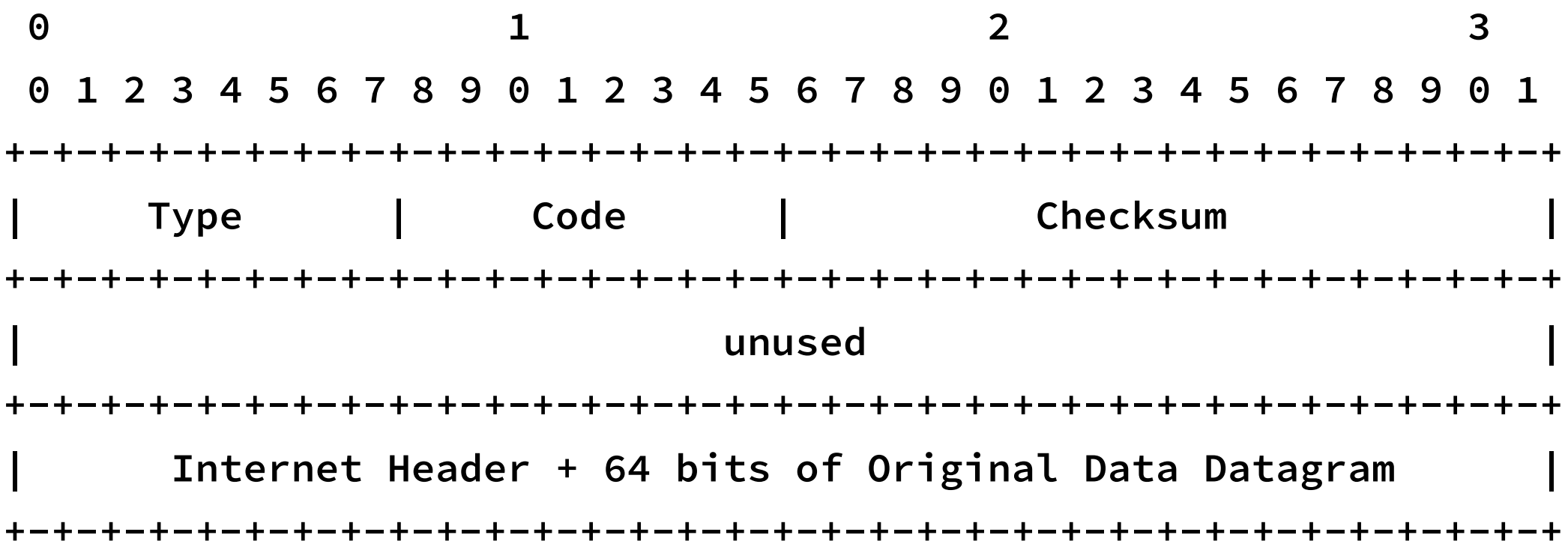
14 A 18 DE SETEMBRO DE 2020

ICMP

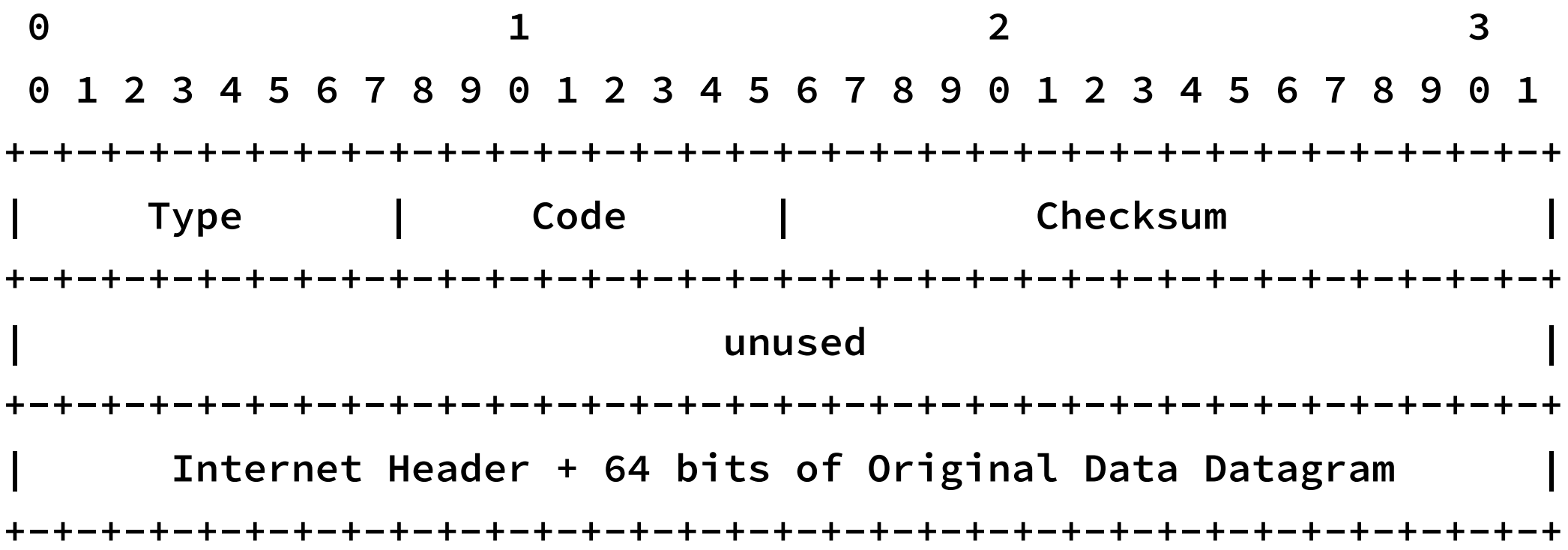
PoP-BA
Ponto de Presença da RNP na Bahia

RNP 30 anos
ORGANIZAÇÃO SOCIAL DO MCTI

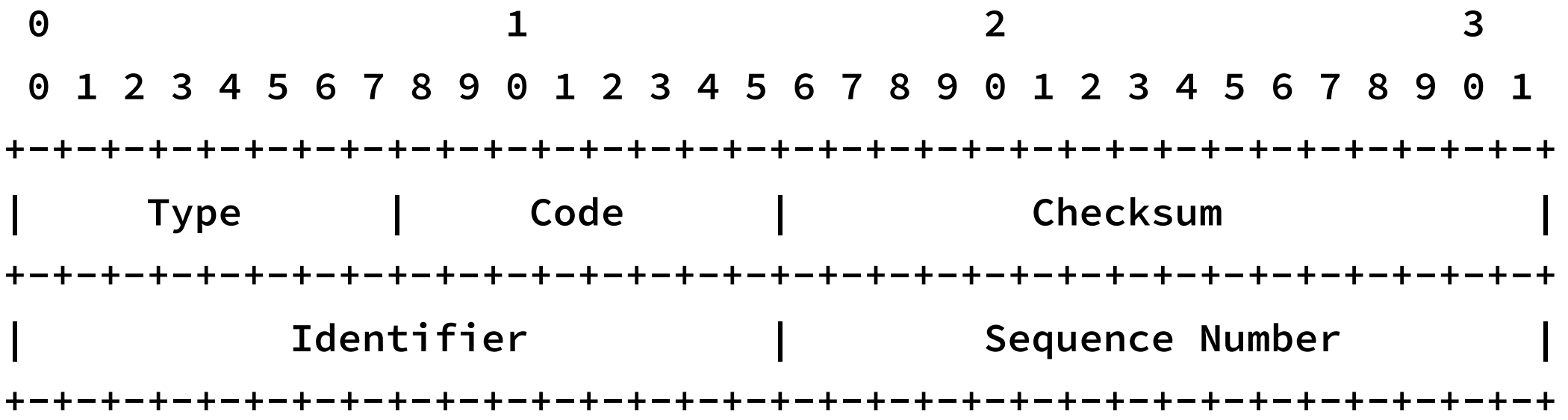
ICMP – Destination Unreachable Message



ICMP – Time Exceeded Message



ICMP – Echo Request/Reply



Análise de Tráfego

```
$ sudo tcpdump -i eno1 -n -v host 10.1.0.38 and icmp
$ ping -c 1 10.1.0.38


16:01:16.464365 IP (tos 0x0, ttl 64, id 40816, offset 0, flags [DF],
proto ICMP (1), length 84)
    10.1.0.114 > 10.1.0.38: ICMP echo request, id 2254, seq 1, length 64
16:01:16.492272 IP (tos 0x0, ttl 64, id 46883, offset 0, flags [none],
proto ICMP (1), length 84)
    10.1.0.38 > 10.1.0.114: ICMP echo reply, id 2254, seq 1, length 64
```

Análise de Tráfego

```
$ sudo tcpdump -i eno1 -n -v host 10.1.0.200
$ ping -c 1 10.1.0.200


15:56:46.212251 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has
10.1.0.200 tell 10.1.0.38, length 28
15:56:47.238372 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has
10.1.0.200 tell 10.1.0.38, length 28


PING 10.1.0.200 (10.1.0.200) 56(84) bytes of data.
From 10.1.0.38 icmp_seq=1 Destination Host Unreachable
--- 10.1.0.200 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms
```

Análise de Tráfego

```
$ sudo tcpdump -i eno1 -n -v host 10.1.0.38 and icmp
$ nc -u 10.1.0.38 80


15:52:54.456291 IP (tos 0xc0, ttl 64, id 63743, offset 0, flags [none],
proto ICMP (1), length 60)
    10.1.0.38 > 10.1.0.114: ICMP 10.1.0.38 udp port 80 unreachable,
length 40
        IP (tos 0x0, ttl 64, id 1818, offset 0, flags [DF], proto UDP
(17), length 32)
    10.1.0.114.56723 > 10.1.0.38.80: UDP, length 4
```

Análise de Tráfego

```
$ sudo tcpdump -i any -n -v icmp
$ ping -4 -c 1 -t 1 rnp.br

16:05:54.725935 IP (tos 0x0, ttl 1, id 1972, offset 0, flags [DF], proto
ICMP (1), length 84)
    10.1.0.114 > 104.22.9.95: ICMP echo request, id 2570, seq 1, length 64

16:05:54.726138 IP (tos 0xc0, ttl 64, id 29906, offset 0, flags [none],
proto ICMP (1), length 112)
    10.1.0.1 > 10.1.0.114: ICMP time exceeded in-transit, length 92
        IP (tos 0x0, ttl 1, id 1972, offset 0, flags [DF], proto ICMP (1),
length 84)
    10.1.0.114 > 104.22.9.95: ICMP echo request, id 2570, seq 1, length 64
```

Análise de Tráfego

```
$ sudo tcpdump -i any -n -v icmp
$ ping -4 -c 1 -t 2 rnp.br

16:07:28.922857 IP (tos 0x0, ttl 2, id 26013, offset 0, flags [DF], proto
ICMP (1), length 84)
    10.1.0.114 > 104.22.8.95: ICMP echo request, id 2578, seq 1, length 64

16:07:28.923270 IP (tos 0x0, ttl 254, id 0, offset 0, flags [none], proto
ICMP (1), length 56)
    200.128.6.148 > 10.1.0.114: ICMP time exceeded in-transit, length 36
        IP (tos 0x0, ttl 1, id 26013, offset 0, flags [DF], proto ICMP (1),
length 84)
    10.1.0.114 > 104.22.8.95: ICMP echo request, id 2578, seq 1, length 64
```

Exercício de Análise de Tráfego

- Como verificar conectividade em uma rede/equipamento que não responde a ICMP?

WTR
WORKSHOP
DE TECNOLOGIAS DE REDES DO POP-BA

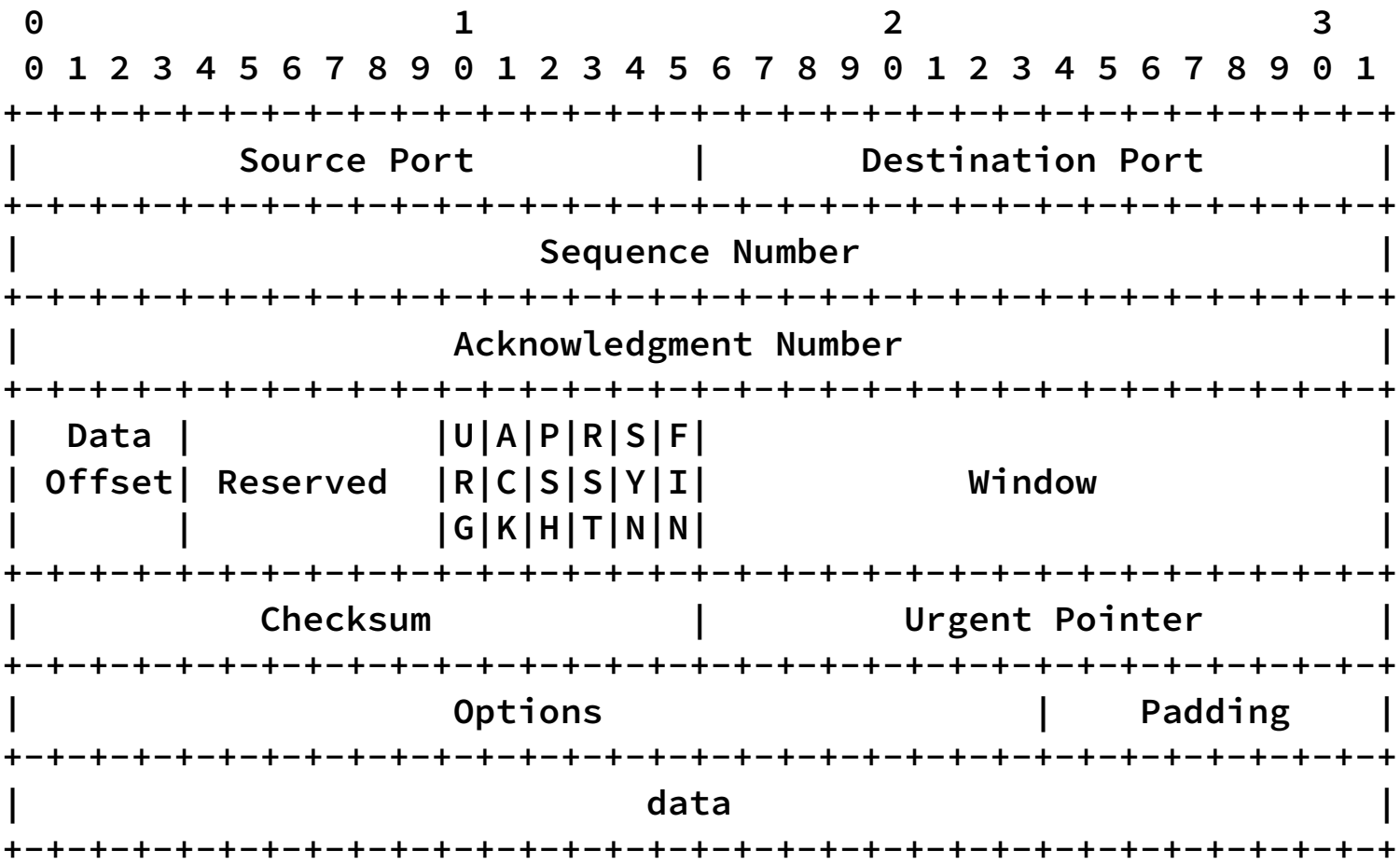
14 A 18 DE SETEMBRO DE 2020

TCP

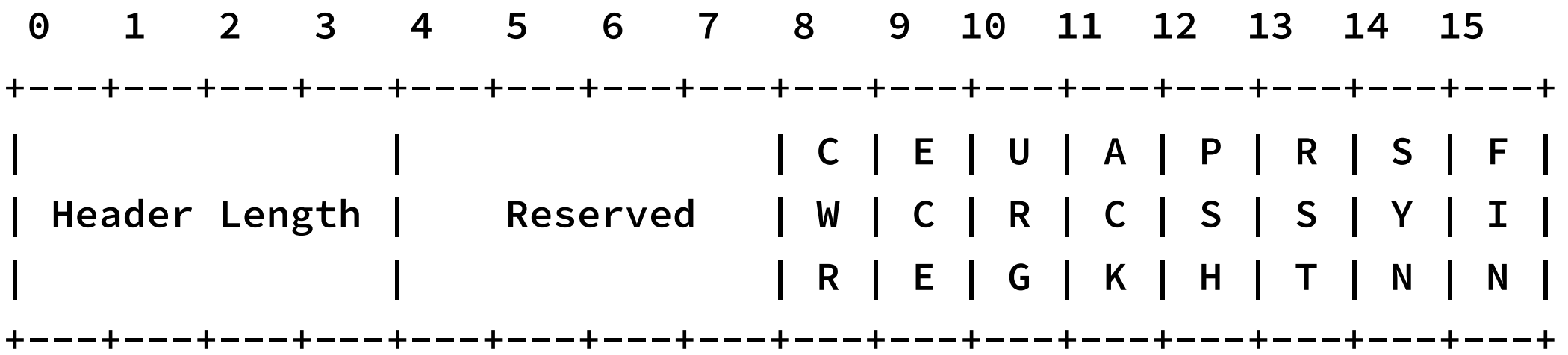
PoP-BA
Ponto de Presença da RNP na Bahia

RNP 30 anos
ORGANIZAÇÃO SOCIAL DO MCTI

TCP


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Source Port
Destination Port
Sequence Number
Acknowledgment Number
Data Offset
Reserved
U R G
A C K
P S H
R S T
S Y N
F I N
Window
Checksum
Urgent Pointer
Options
Padding
data

TCP – Novas Flags



Análise de Tráfego

```
$ sudo tcpdump -i eno1 -n -v host 10.1.0.38 and tcp
$ nc 10.1.0.38 80
```

```
14:12:07.770326 IP 10.1.0.114.38504 > 10.1.0.38.80: Flags [S], seq 2231480575, win
64240, options [mss 1460,sackOK,TS val 597533526 ecr 0,nop,wscale 7], length 0
14:12:07.793391 IP 10.1.0.38.80 > 10.1.0.114.38504: Flags [S.], seq 3213945376, ack
2231480576, win 65160, options [mss 1324,sackOK,TS val 728386932 ecr
597533526,nop,wscale 7], length 0
14:12:07.793456 IP 10.1.0.114.38504 > 10.1.0.38.80: Flags [.], ack 1, win 502, options
[nop,nop,TS val 597533549 ecr 728386932], length 0
14:12:08.632724 IP 10.1.0.114.38504 > 10.1.0.38.80: Flags [F.], seq 1, ack 1, win 502,
options [nop,nop,TS val 597534388 ecr 728386932], length 0
14:12:08.662462 IP 10.1.0.38.80 > 10.1.0.114.38504: Flags [F.], seq 1, ack 2, win 510,
options [nop,nop,TS val 728387801 ecr 597534388], length 0
14:12:08.662513 IP 10.1.0.114.38504 > 10.1.0.38.80: Flags [.], ack 2, win 502, options
[nop,nop,TS val 597534418 ecr 728387801], length 0
```

Análise de Tráfego

- Faça uma nova conexão como a anterior
- Observe as portas do cliente e do servidor. O que mudou?

Análise de Tráfego

https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

```
$ less /etc/services

$ getent services http
http                    80/tcp

$ getent services 53
domain                  53/tcp

$ getent services ftp
ftp                     21/tcp
```

Análise de Tráfego

Ver portas que estão em modo *listening*:

```
$ sudo lsof -i
$ sudo netstat -lnvpt
$ sudo ss -lnpt
```

Análise de Tráfego


```
$ sudo tcpdump -i eno1 -n host 10.1.0.38 and tcp -S
$ nc 10.1.0.38 80
```

```
14:17:46.392644 IP 10.1.0.114.39002 > 10.1.0.38.80: Flags [S], seq 3886319713, win 64240, options [mss 1460,sackOK,TS val 597872148 ecr 0,nop,wscale 7], length 0
14:17:46.443354 IP 10.1.0.38.80 > 10.1.0.114.39002: Flags [S.], seq 1108175147, ack 3886319714, win 65160, options [mss 1324,sackOK,TS val 728725561 ecr 597872148,nop,wscale 7], length 0
14:17:46.443402 IP 10.1.0.114.39002 > 10.1.0.38.80: Flags [.], ack 1108175148, win 502, options [nop,nop,TS val 597872199 ecr 728725561], length 0
14:17:47.691998 IP 10.1.0.114.39002 > 10.1.0.38.80: Flags [F.], seq 3886319714, ack 1108175148, win 502, options [nop,nop,TS val 597873447 ecr 728725561], length 0
14:17:47.717521 IP 10.1.0.38.80 > 10.1.0.114.39002: Flags [F.], seq 1108175148, ack 3886319715, win 510, options [nop,nop,TS val 728726855 ecr 597873447], length 0
14:17:47.717592 IP 10.1.0.114.39002 > 10.1.0.38.80: Flags [.], ack 1108175149, win 502, options [nop,nop,TS val 597873473 ecr 728726855], length 0
```

Análise de Tráfego


```
$ sudo tcpdump -i eno1 -n host 10.1.0.38 and tcp
$ nc 10.1.0.38 80

14:26:16.208894 IP 10.1.0.114.39010 > 10.1.0.38.80: Flags [S], seq 2777450481, win 64240, options [mss 1460,sackOK,TS val 598381964 ecr 0,nop,wscale 7], length 0
14:26:16.235235 IP 10.1.0.38.80 > 10.1.0.114.39010: Flags [S.], seq 1470946849, ack 2777450482, win 65160, options [mss 1324,sackOK,TS val 729235377 ecr 598381964,nop,wscale 7], length 0
14:26:16.235284 IP 10.1.0.114.39010 > 10.1.0.38.80: Flags [.], ack 1, win 502, options [nop,nop,TS val 598381991 ecr 729235377], length 0
14:26:20.975069 IP 10.1.0.114.39010 > 10.1.0.38.80: Flags [P.], seq 1:14, ack 1, win 502, options [nop,nop,TS val 598386730 ecr 729235377], length 13: HTTP
14:26:21.089951 IP 10.1.0.38.80 > 10.1.0.114.39010: Flags [.], ack 14, win 509, options [nop,nop,TS val 729240145 ecr 598386730], length 0
14:26:21.090004 IP 10.1.0.38.80 > 10.1.0.114.39010: Flags [P.], seq 1:484, ack 14, win 509, options [nop,nop,TS val 729240146 ecr 598386730], length 483: HTTP: HTTP/1.1 400 Bad Request
14:26:21.090033 IP 10.1.0.114.39010 > 10.1.0.38.80: Flags [.], ack 484, win 501, options [nop,nop,TS val 598386845 ecr 729240146], length 0
14:26:21.090050 IP 10.1.0.38.80 > 10.1.0.114.39010: Flags [F.], seq 484, ack 14, win 509, options [nop,nop,TS val 729240146 ecr 598386730], length 0
14:26:21.133130 IP 10.1.0.114.39010 > 10.1.0.38.80: Flags [.], ack 485, win 501, options [nop,nop,TS val 598386888 ecr 729240146], length 0
14:26:22.199244 IP 10.1.0.114.39010 > 10.1.0.38.80: Flags [F.], seq 14, ack 485, win 501, options [nop,nop,TS val 598387955 ecr 729240146], length 0
14:26:22.260712 IP 10.1.0.38.80 > 10.1.0.114.39010: Flags [.], ack 15, win 509, options [nop,nop,TS val 729241371 ecr 598387955], length 0
```

Análise de Tráfego

```
$ sudo tcpdump -i tap0 -n host 10.1.0.38 and tcp -X
$ netcat  10.1.0.38 80

14:42:28.415951 IP 10.1.0.114.39016 > 10.1.0.38.80: Flags [S], seq
2570042444, win 64240, options [mss 1460,sackOK,TS val 599354171 ecr
0,nop,wscale 7], length 0

0x0000:  4500 003c 4986 4000 4006 dc9c 0a01 0072  E..<I.@.@......r
0x0010:  0a01 0026 9868 0050 992f bc4c 0000 0000  ...&.h.P./.L....
0x0020:  a002 faf0 14c8 0000 0204 05b4 0402 080a  ................
0x0030:  23b9 6b3b 0000 0000 0103 0307            #.k;........
```

Análise de Tráfego


```
$ sudo tcpdump -i tap0 -n host 10.1.0.38 and tcp
$ netcat  10.1.0.38 80

14:45:49.524193 IP 10.1.0.114.39018 > 10.1.0.38.80: Flags [S], seq 584169342, win 64240, options [mss 1460,sackOK,TS val 599555280 ecr
0,nop,wscale 7], length 0
14:45:49.539439 IP 10.1.0.38.80 > 10.1.0.114.39018: Flags [S.], seq 356366604, ack 584169343, win 65160, options [mss 1324,sackOK,TS val
730408696 ecr 599555280,nop,wscale 7], length 0
14:45:49.539486 IP 10.1.0.114.39018 > 10.1.0.38.80: Flags [.], ack 1, win 502, options [nop,nop,TS val 599555295 ecr 730408696], length 0
14:45:52.905342 IP 10.1.0.114.39018 > 10.1.0.38.80: Flags [P.], seq 1:5, ack 1, win 502, options [nop,nop,TS val 599558661 ecr
730408696], length 4: HTTP
14:45:52.918869 IP 10.1.0.38.80 > 10.1.0.114.39018: Flags [.], ack 5, win 510, options [nop,nop,TS val 730412075 ecr 599558661], length 0
14:45:52.931831 IP 10.1.0.38.80 > 10.1.0.114.39018: Flags [P.], seq 1:484, ack 5, win 510, options [nop,nop,TS val 730412075 ecr
599558661], length 483: HTTP: HTTP/1.1 400 Bad Request
14:45:52.931895 IP 10.1.0.114.39018 > 10.1.0.38.80: Flags [.], ack 484, win 501, options [nop,nop,TS val 599558687 ecr 730412075], length
0
14:45:52.931916 IP 10.1.0.38.80 > 10.1.0.114.39018: Flags [F.], seq 484, ack 5, win 510, options [nop,nop,TS val 730412075 ecr
599558661], length 0
14:45:52.973122 IP 10.1.0.114.39018 > 10.1.0.38.80: Flags [.], ack 485, win 501, options [nop,nop,TS val 599558729 ecr 730412075], length
0
14:45:54.113664 IP 10.1.0.114.39018 > 10.1.0.38.80: Flags [F.], seq 5, ack 485, win 501, options [nop,nop,TS val 599559869 ecr
730412075], length 0
14:45:54.286325 IP 10.1.0.38.80 > 10.1.0.114.39018: Flags [.], ack 6, win 510, options [nop,nop,TS val 730413403 ecr 599559869], length 0
```

Exercício de Análise de Tráfego

Analise o tráfego abaixo e identifique as flags TCP presentes.

```
0x0000:  4500 0034 ea30 4000 4006 3bfa 0a01 0026  E..4.0@.@.;....&
0x0010:  0a01 0072 0050 9868 acd9 56a0 992f bc54  ...r.P.h..V../.T
0x0020:  8011 01fe 53f8 0000 0101 080a 2b86 3ab4  ....S.......+.:.
0x0030:  23b9 9082                                #...
```

Exercício de Análise de Tráfego

Analise o tráfego abaixo e identifique as flags TCP presentes.

```
0x0000:  4500 0034 ea30 4000 4006 3bfa 0a01 0026  E..4.0@.@.;....&
0x0010:  0a01 0072 0050 9868 acd9 56a0 992f bc54  ...r.P.h..V../.T
0x0020:  8011 01fe 53f8 0000 0101 080a 2b86 3ab4  ....S.......+.:.
0x0030:  23b9 9082                                #...
```

Exercício de Análise de Tráfego

Analise o tráfego abaixo e identifique as flags TCP presentes.

```
0x0000:  4500 0034 ea30 4000 4006 3bfa 0a01 0026  E..4.0@.@.;....&
0x0010:  0a01 0072 0050 9868 acd9 56a0 992f bc54  ...r.P.h..V../.T
0x0020:  8011 01fe 53f8 0000 0101 080a 2b86 3ab4  ....S.......+.:.
0x0030:  23b9 9082                                #...
```

0x11 → 0b00010001

A C K

F I N

Análise de Tráfego


```
$ sudo tcpdump -i eno1 -n host 10.1.0.38 and tcp
$ sudo hping3 -p 80 -S 10.1.0.38 -c 1
$ sudo nmap -p80 --scanflags SYN 10.1.0.38

14:50:56.793485 IP 10.1.0.114.35101 > 10.1.0.38.80: Flags [S], seq 842197359, win 1024, options [mss 1460], length 0
14:50:56.831311 IP 10.1.0.38.80 > 10.1.0.114.35101: Flags [S.], seq 2319280844, ack 842197360, win 64240, options [mss 1324], length 0
14:50:56.831363 IP 10.1.0.114.35101 > 10.1.0.38.80: Flags [R], seq 842197360, win 0, length 0

15:12:03.232303 IP 10.1.0.38.51948 > 10.1.0.114.80: Flags [S], seq 1657538111, win 64240, options [mss 1460,sackOK,TS val 731927289 ecr 0,nop,wscale 7], length 0
15:12:03.258416 IP 10.1.0.114.80 > 10.1.0.38.51948: Flags [S.], seq 3586172498, ack 1657538112, win 65160, options [mss 1324,sackOK,TS val 601073889 ecr 731927289,nop,wscale 7], length 0
15:12:03.258478 IP 10.1.0.38.51948 > 10.1.0.114.80: Flags [.], ack 1, win 502, options [nop,nop,TS val 731927316 ecr 601073889], length 0
15:12:04.909626 IP 10.1.0.38.51948 > 10.1.0.114.80: Flags [P.], seq 1:7, ack 1, win 502, options [nop,nop,TS val 731928967 ecr 601073889], length 6: HTTP: get /
```

WTR
WORKSHOP
DE TECNOLOGIAS DE REDES DO POP-BA

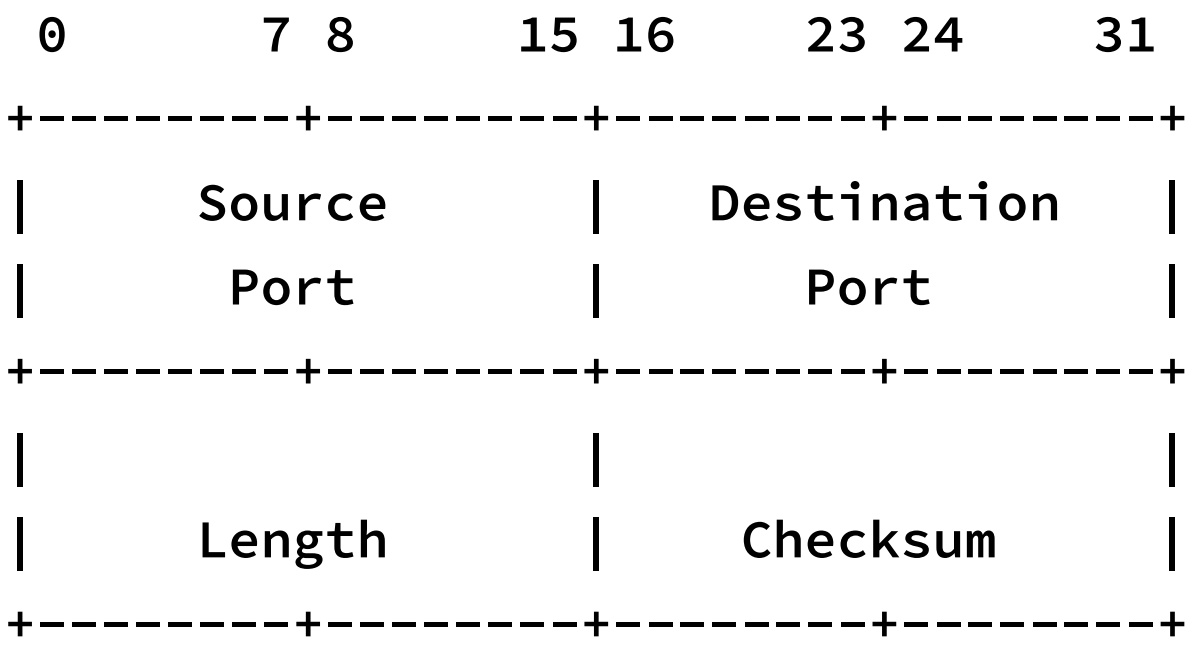
14 A 18 DE SETEMBRO DE 2020

UDP

PoP-BA
Ponto de Presença da RNP na Bahia

RNP 30 anos
ORGANIZAÇÃO SOCIAL DO MCTI

UDP


0 7 8 15 16 23 24 31
Source Port
Destination Port
Length
Checksum

Análise de Tráfego

```
$ sudo tcpdump -i eno1 -n host 10.1.0.38 and udp
$ nc -u 10.1.0.38 23

$ sudo tcpdump -i eno1 -n host 10.1.0.38 and tcp
$ nc 10.1.0.38 79
```

WTR
WORKSHOP
DE TECNOLOGIAS DE REDES DO POP-BA

14 A 18 DE SETEMBRO DE 2020

Troubleshooting

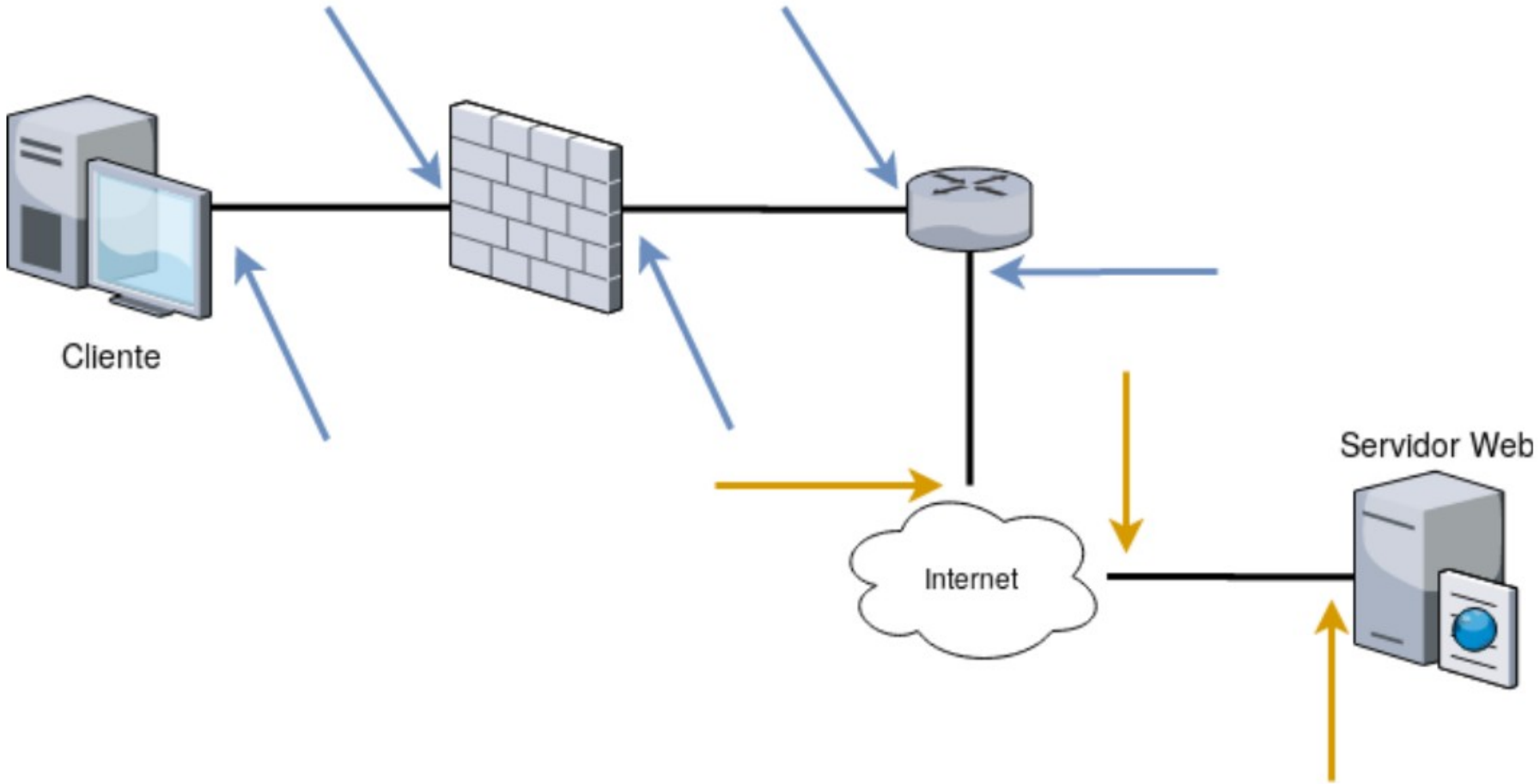
PoP-BA
Ponto de Presença da RNP na Bahia

RNP 30 anos
ORGANIZAÇÃO SOCIAL DO MCTI

Troubleshooting

- Há conectividade entre hosts intermediários?
- Onde o tráfego está se comportando diferente?
- Quais as possibilidades de problemas dado o comportamento diferente do trafego?

Troubleshooting



WTR

WORKSHOP

DE TECNOLOGIAS DE REDES DO POP-BA

14 A 18 DE SETEMBRO DE 2020

PoP-BA Ponto de Presença da RNP na Bahia

RNP 30 anos ORGANIZAÇÃO SOCIAL DO MCTI

MINISTÉRIO DO TURISMO

MINISTÉRIO DA DEFESA

MINISTÉRIO DA SAÚDE

MINISTÉRIO DA EDUCAÇÃO

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES

PÁTRIA AMADA BRASIL GOVERNO FEDERAL