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

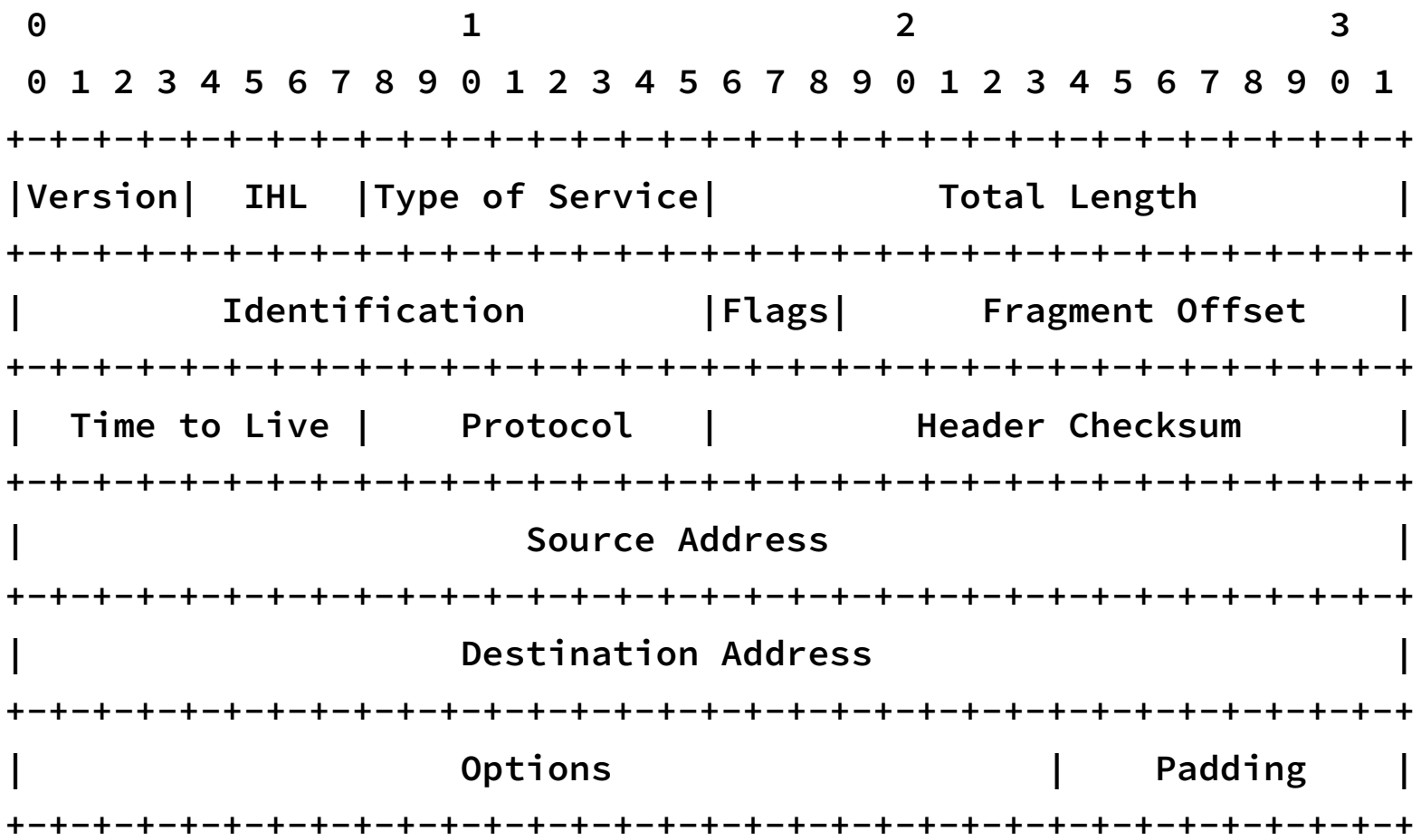
14 A 18 DE SETEMBRO DE 2020

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

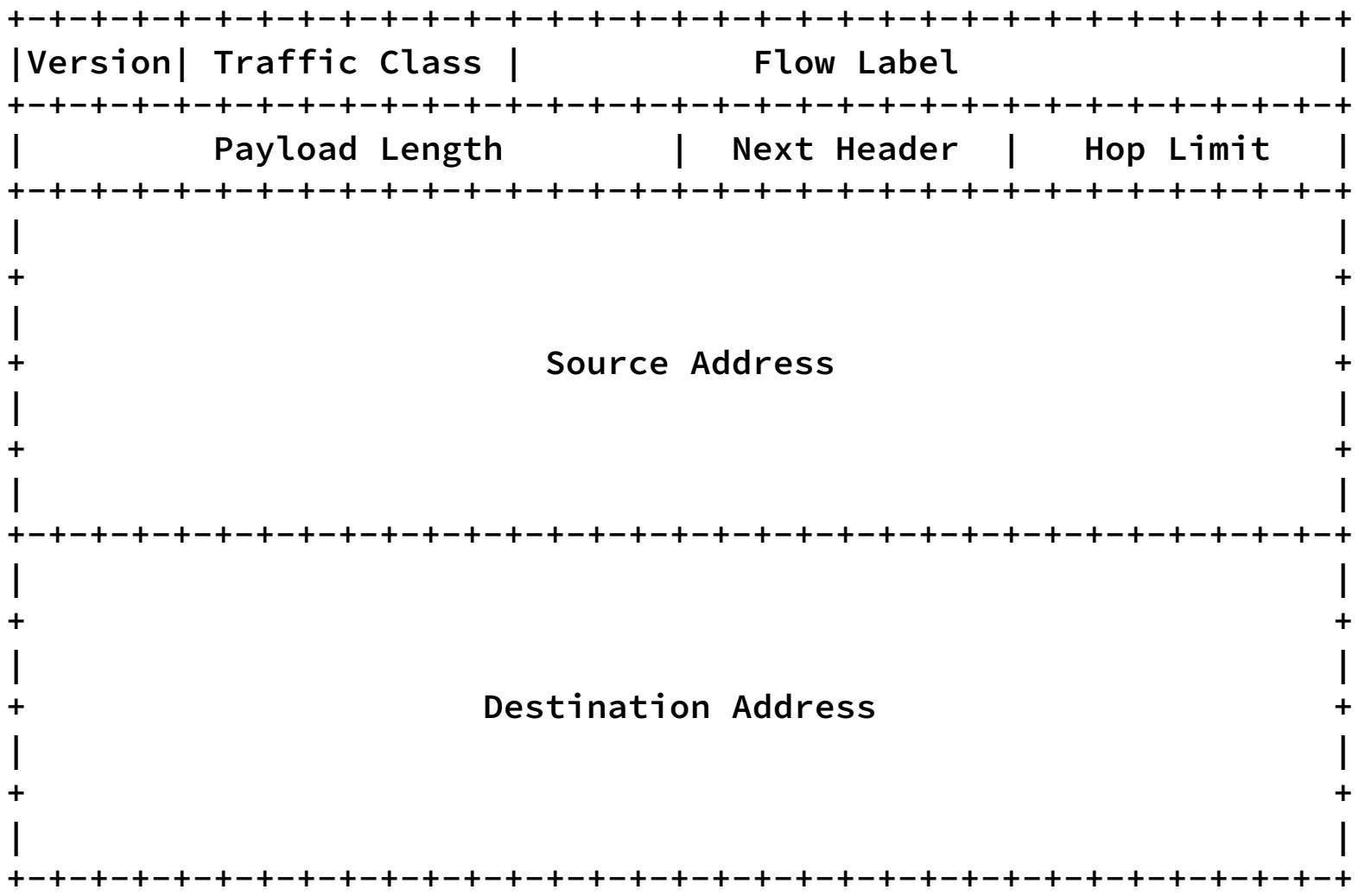
14 A 18 DE SETEMBRO DE 2020

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

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