

Usando o **Wireshark** para troubleshooting de redes

por **Jean Figueiredo**
Consultor de Tecnologia



O que a Sage Networks faz?



Consultoria e assessoria para Sistemas Autônomos em redes e especializada em **mitigação de DDoS**.

- Implantação de sistemas de **detecção** e automação de resposta a ataques.
- **Nuvem** de mitigação por VPN, VLAN bilateral ou cross connect.
- Implantação do produto de mitigação DDoS no **portfólio** de seu ISP ou data center.
- Consultoria em **redes** para Sistemas Autônomos.



Agenda

- O que é o Wireshark?
- Como instalar o Wireshark?
- Navegando pela interface do Wireshark
- Obtendo uma captura de pacote
- Filtragem de Pacotes
- Exemplo de troubleshooting
- Alternativas ao Wireshark



O que é o Wireshark?



O que é o Wireshark?



- Captura e Inspeção detalhada de pacotes
- Suporte a uma ampla variedade protocolos
- Ferramenta de Código Aberto
- Interface intuitiva
- Multiplataforma



Como instalar o Wireshark?

- Para Ubuntu e sistemas baseados no **Debian**:

```
sudo apt install wireshark
```

- Para Fedora e sistemas baseados no **Red Hat**:

```
sudo dnf install wireshark
```

- Para sistemas baseados no **Arch Linux**:

```
sudo pacman -S wireshark
```

- Para **macOS** (usando o **Homebrew**):

```
brew install wireshark
```

- Para sistema **Windows**:

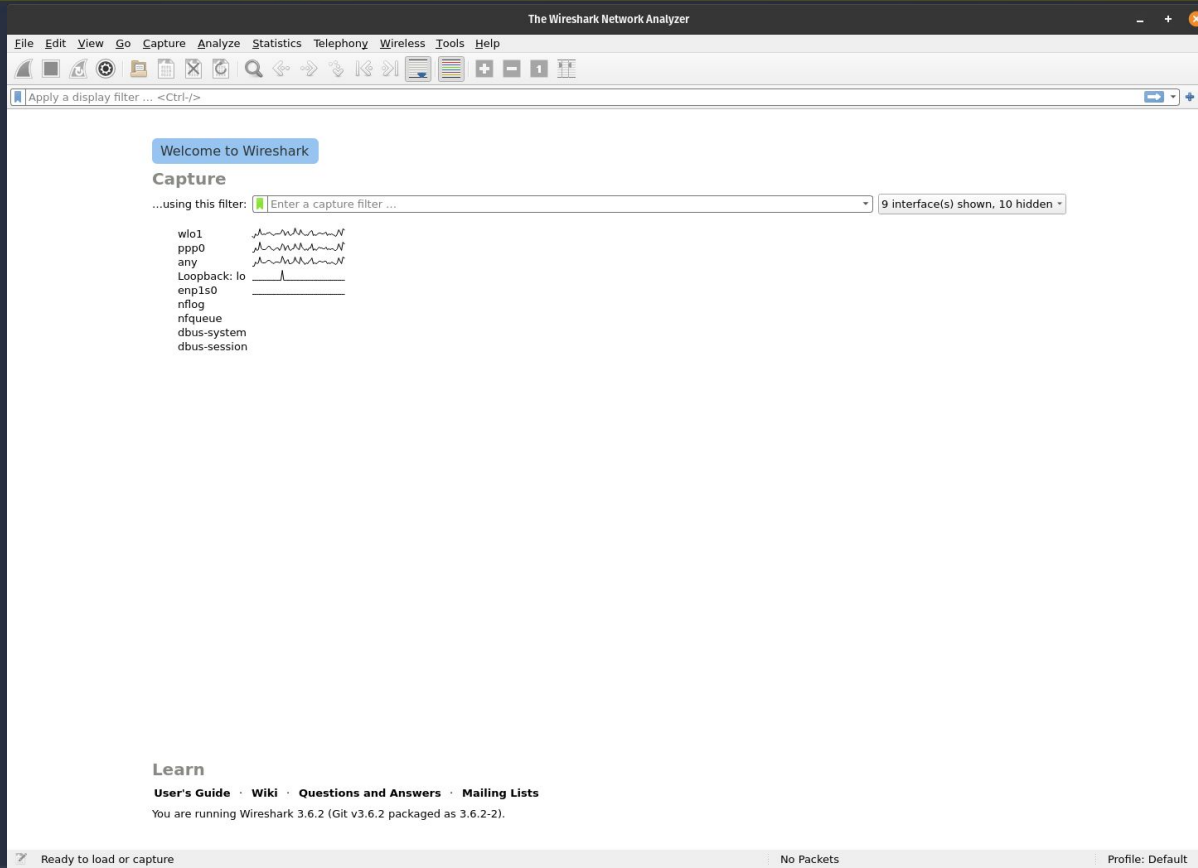
Download em <https://www.wireshark.org/download>



Navegando pela interface do Wireshark



Navegando pela interface do Wireshark



The screenshot shows the Wireshark Network Analyzer interface. At the top, the title bar reads "The Wireshark Network Analyzer". Below it is a menu bar with options: File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help. A toolbar with various icons is positioned below the menu bar. A status bar at the top indicates "Apply a display filter ... <Ctrl-/>".

The main content area is divided into sections:

- Welcome to Wireshark**: A blue button.
- Capture**: A section with a text input field "Enter a capture filter ..." and a dropdown menu showing "9 interface(s) shown, 10 hidden". Below this, a list of network interfaces is displayed with corresponding signal waveforms:
 - wlo1
 - ppp0
 - any
 - Loopback: lo
 - enp1s0
 - nflog
 - nfqueue
 - dbus-system
 - dbus-session
- Learn**: A section with links for "User's Guide", "Wiki", "Questions and Answers", and "Mailing Lists". Below the links, it states "You are running Wireshark 3.6.2 (Git v3.6.2 packaged as 3.6.2-2)".

At the bottom of the window, a status bar shows "Ready to load or capture", "No Packets", and "Profile: Default".



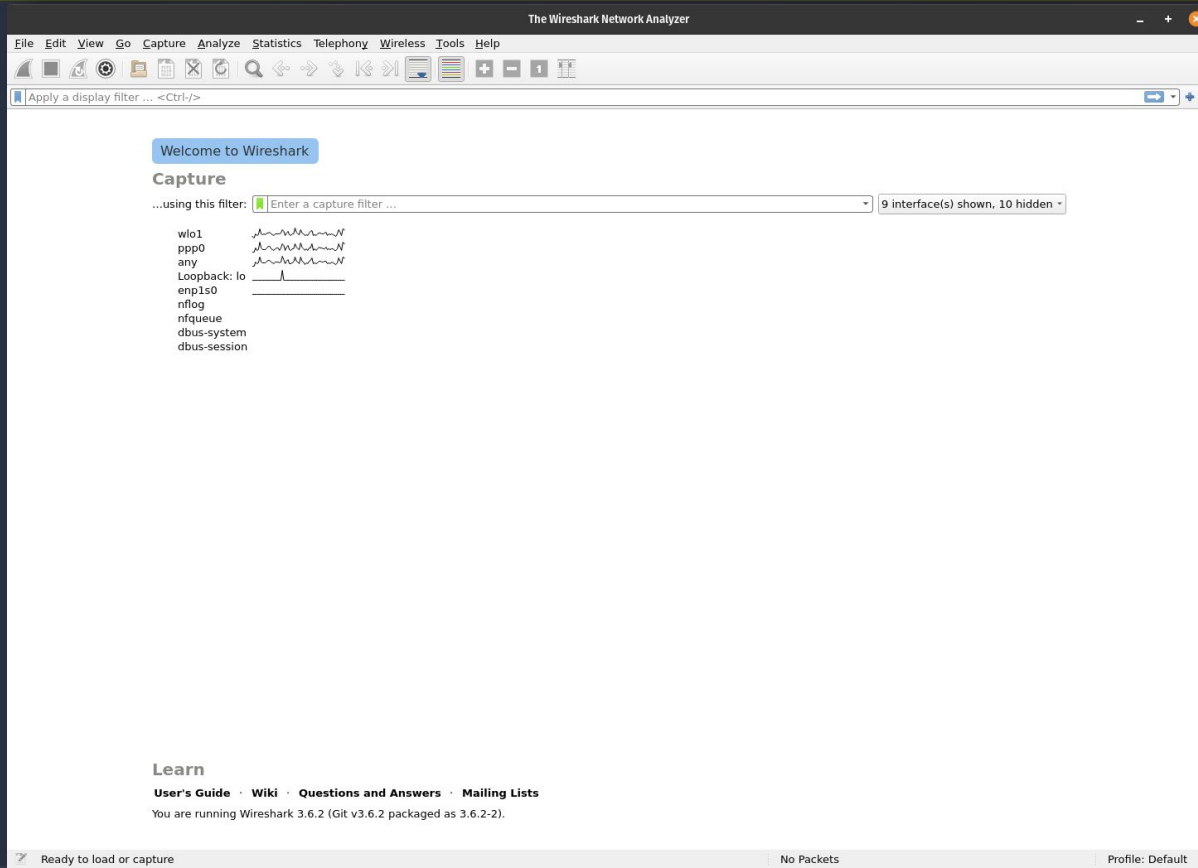
Navegando pela interface do Wireshark

A screenshot of the Wireshark Network Analyzer interface. The window title is "The Wireshark Network Analyzer". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture, and analysis. Below the toolbar is a display filter field with the text "Apply a display filter ... <Ctrl-/>". The main area is titled "Welcome to Wireshark" and "Capture". Under "Capture", there is a text field "Enter a capture filter ..." and a dropdown menu showing "9 interface(s) shown, 10 hidden". A list of network interfaces is displayed with their activity levels represented by waveforms:

wlc1	
ppp0	
any	
Loopback: lo	
enp1s0	
nflog	
nfqueue	
dbus-system	
dbus-session	

At the bottom of the interface, there is a "Learn" section with links for "User's Guide", "Wiki", "Questions and Answers", and "Mailing Lists". Below these links, it states "You are running Wireshark 3.6.2 (Git v3.6.2 packaged as 3.6.2-2)". The status bar at the bottom shows "Ready to load or capture", "No Packets", and "Profile: Default".

Navegando pela interface do Wireshark



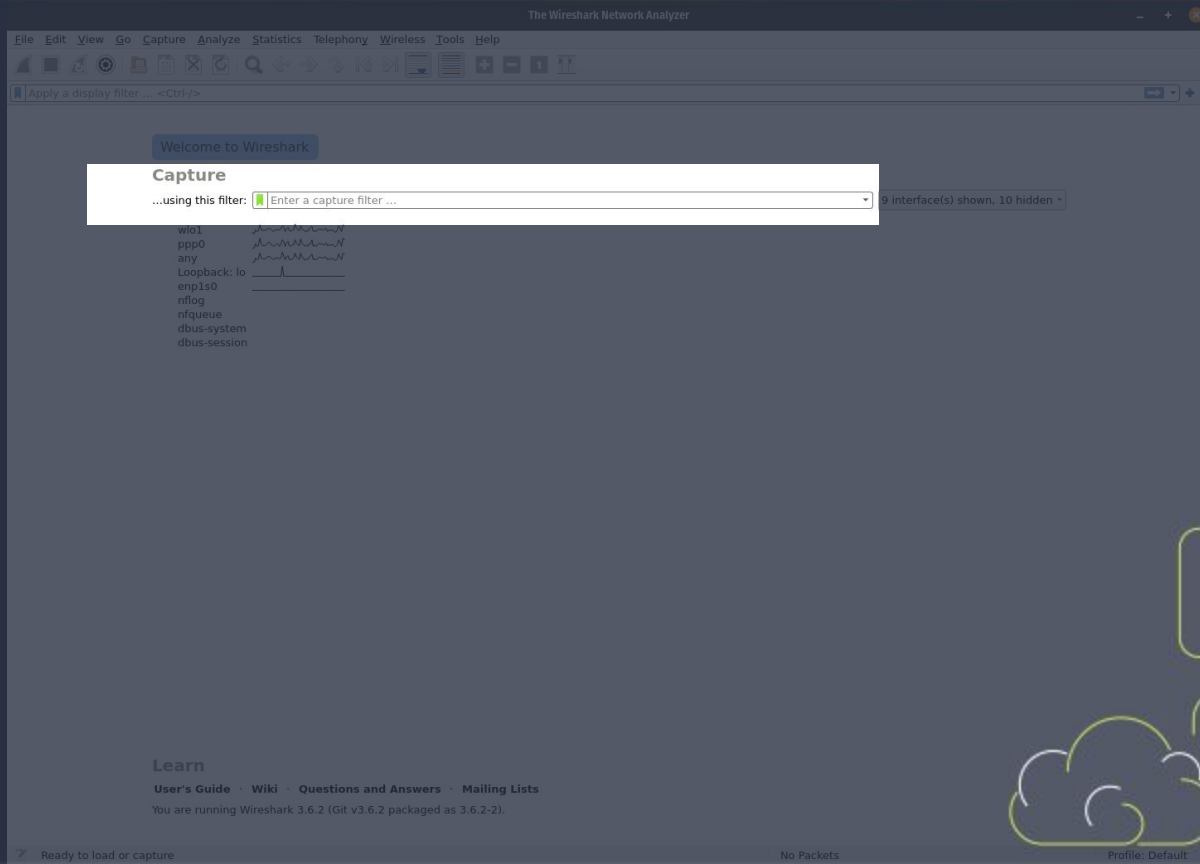
The screenshot shows the Wireshark Network Analyzer interface. At the top, the title bar reads "The Wireshark Network Analyzer". Below it is a menu bar with options: File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help. A toolbar contains various icons for file operations, capture control, and analysis. Below the toolbar is a display filter field containing "Apply a display filter ... <Ctrl-/>".

The main content area is divided into sections:

- Welcome to Wireshark**: A blue header.
- Capture**: A section with a text input field "Enter a capture filter ..." and a dropdown menu showing "9 interface(s) shown, 10 hidden". Below this is a list of network interfaces with their corresponding capture status indicators:
 - wlo1: [Active]
 - ppp0: [Active]
 - any: [Active]
 - Loopback: lo: [Active]
 - enp1s0: [Inactive]
 - nflog: [Inactive]
 - nfqueue: [Inactive]
 - dbus-system: [Inactive]
 - dbus-session: [Inactive]
- Learn**: A section with links for "User's Guide", "Wiki", "Questions and Answers", and "Mailing Lists". Below the links, it states: "You are running Wireshark 3.6.2 (Git v3.6.2 packaged as 3.6.2-2)." At the bottom of the interface, a status bar shows "Ready to load or capture", "No Packets", and "Profile: Default".



Navegando pela interface do Wireshark



The Wireshark Network Analyzer

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ...

9 interface(s) shown, 10 hidden

wlan1
ppp0
any
Loopback: lo
enp1s0
nflog
nfqueue
dbus-system
dbus-session

Learn

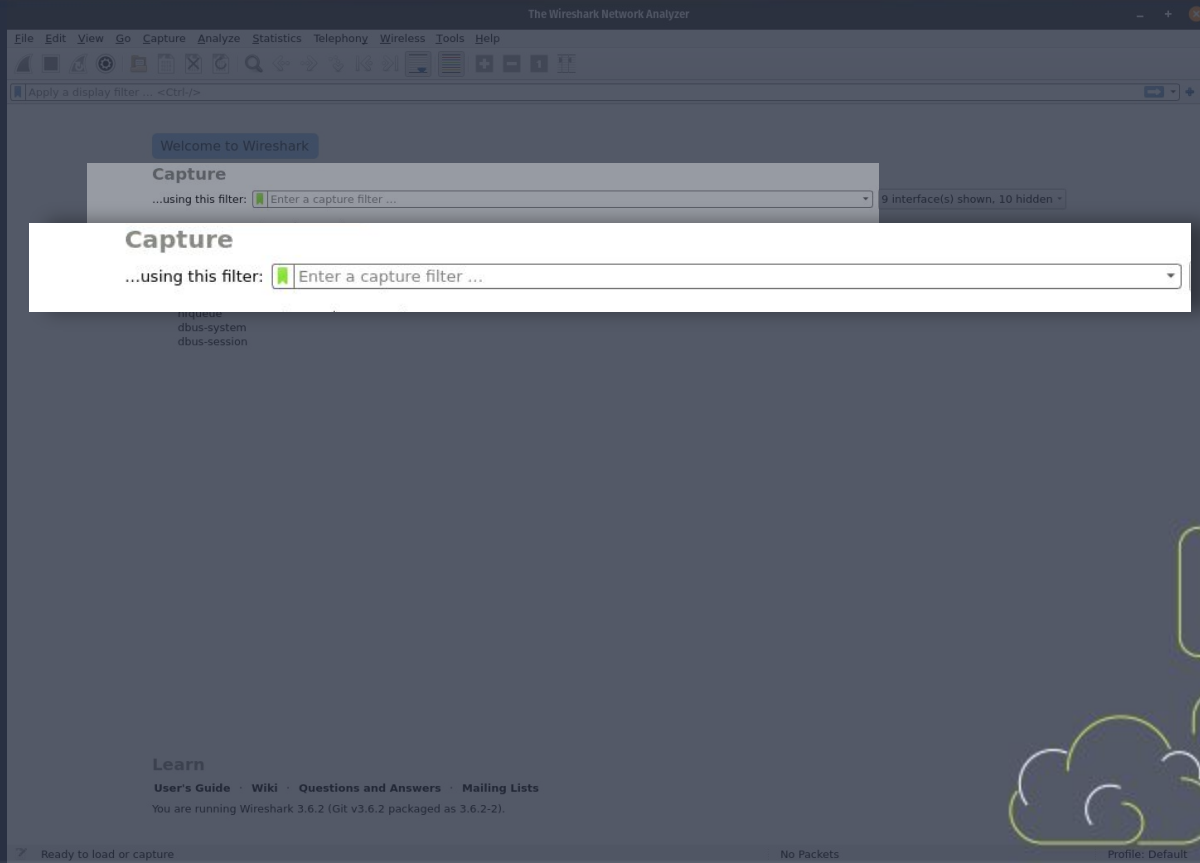
[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 3.6.2 (Git v3.6.2 packaged as 3.6.2-2).

Ready to load or capture No Packets Profile: Default




Navegando pela interface do Wireshark



Navegando pela interface do Wireshark

The Wireshark Network Analyzer

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



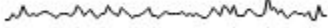



Apply a display filter ... <Ctrl-/>

Welcome to Wireshark

Capture

...using this filter:

wlo1	
ppp0	
any	
Loopback: lo	



Navegando pela interface do Wireshark

The Wireshark Network Analyzer




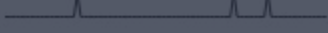
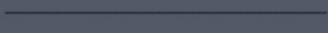
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Welcome to Wireshark

Capture

...using this filter:

wlo1	
ppp0	
any	
Loopback: lo	
enp1s0	
nflog	
nfqueue	



Navegando pela interface do Wireshark

The Wireshark Network Analyzer




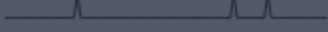
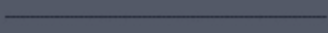


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help


Apply a display filter ... <Ctrl-/>

Welcome to Wireshark

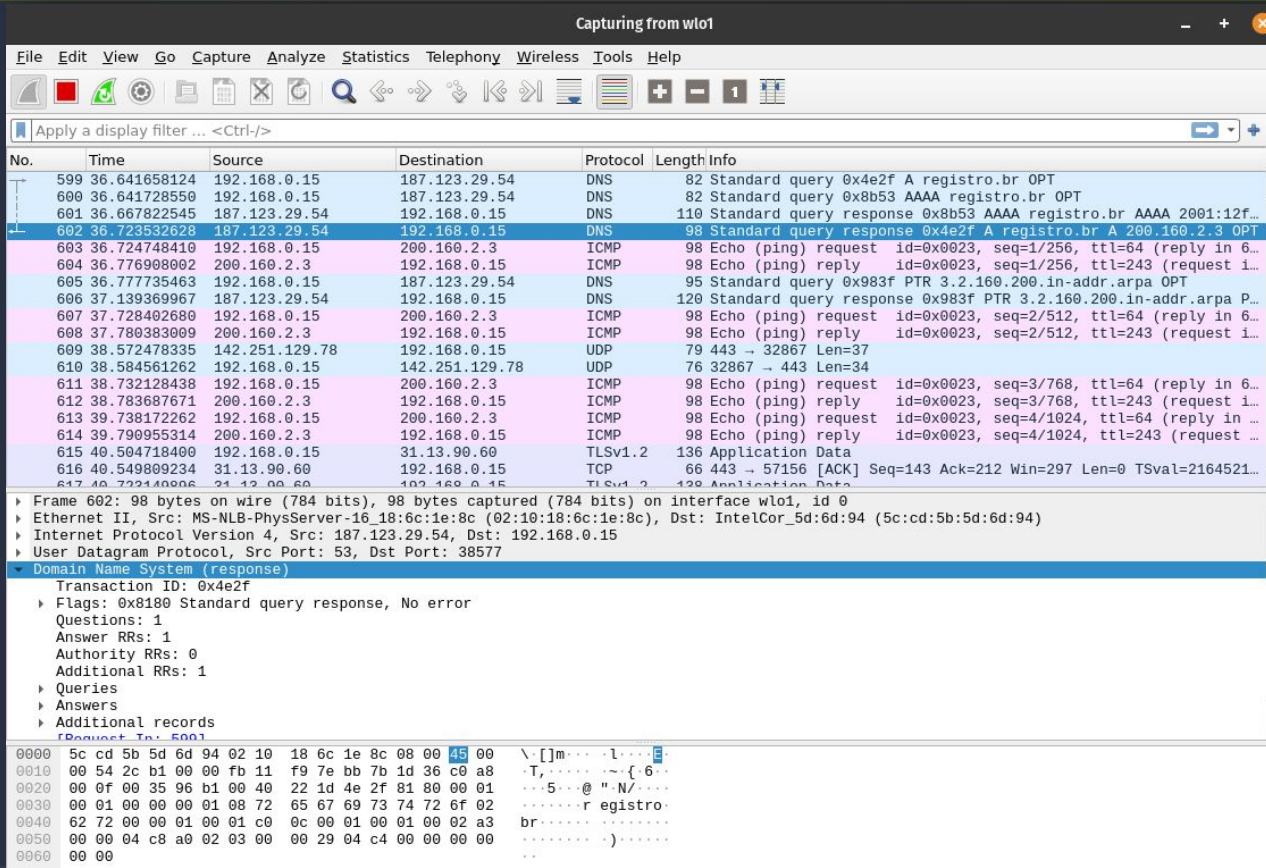
Capture

...using this filter:

wlo1	
ppp0	
any	
Loopback: lo	
enp1s0	
nflog	
nfqueue	



Navegando pela interface do Wireshark



Capturing from wlo1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
599	36.641658124	192.168.0.15	187.123.29.54	DNS	82	Standard query 0x4e2f A registro.br OPT
600	36.641728550	192.168.0.15	187.123.29.54	DNS	82	Standard query 0x8b53 AAAA registro.br OPT
601	36.667822545	187.123.29.54	192.168.0.15	DNS	110	Standard query response 0x8b53 AAAA registro.br AAAA 2001:12f...
602	36.723532628	187.123.29.54	192.168.0.15	DNS	98	Standard query response 0x4e2f A registro.br A 200.160.2.3 OPT
603	36.724748410	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=1/256, ttl=64 (reply in 6...
604	36.776908002	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=1/256, ttl=243 (request i...
605	36.777735463	192.168.0.15	187.123.29.54	DNS	95	Standard query 0x983f PTR 3.2.160.200.in-addr.arpa OPT
606	37.139369967	187.123.29.54	192.168.0.15	DNS	120	Standard query response 0x983f PTR 3.2.160.200.in-addr.arpa P...
607	37.728402680	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=2/512, ttl=64 (reply in 6...
608	37.780383009	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=2/512, ttl=243 (request i...
609	38.572478335	142.251.129.78	192.168.0.15	UDP	79	443 → 32867 Len=37
610	38.584561262	192.168.0.15	142.251.129.78	UDP	76	32867 → 443 Len=34
611	38.732128438	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=3/768, ttl=64 (reply in 6...
612	38.783687671	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=3/768, ttl=243 (request i...
613	39.738172262	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=4/1024, ttl=64 (reply in ...
614	39.790955314	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=4/1024, ttl=243 (request ...
615	40.504748400	192.168.0.15	31.13.90.60	TLSv1.2	136	Application Data
616	40.549809234	31.13.90.60	192.168.0.15	TCP	66	443 → 57156 [ACK] Seq=143 Ack=212 Win=297 Len=0 TSval=2164521...
617	40.723140906	192.168.0.15	192.168.0.15	TLSv1.2	129	Application Data

▶ Frame 602: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0
▶ Ethernet II, Src: MS-NLB-PhysServer-16 18:6c:1e:8c (02:10:18:6c:1e:8c), Dst: IntelCor_5d:6d:94 (5c:cd:5b:5d:6d:94)
▶ Internet Protocol Version 4, Src: 187.123.29.54, Dst: 192.168.0.15
▶ User Datagram Protocol, Src Port: 53, Dst Port: 38577

▼ Domain Name System (response)

- Transaction ID: 0x4e2f
- Flags: 0x8180 Standard query response, No error
- Questions: 1
- Answer RRs: 1
- Authority RRs: 0
- Additional RRs: 1
- Queries
- Answers
- Additional records

Request ID: 5001

```
0000 5c cd 5b 5d 6d 94 02 10 18 6c 1e 8c 08 00 45 00  \:[]m...l...
0010 00 54 2c b1 00 00 fb 11 f9 7e bb 7b 1d 36 c0 a8  T...{ 6
0020 00 0f 00 35 96 b1 00 40 22 1d 4e 2f 81 80 00 01  :5...@ "N/...
0030 00 01 00 00 01 08 72 65 67 69 73 74 72 6f 02  :...r registro
0040 62 72 00 00 01 00 01 c0 0c 00 01 00 01 00 02 a3 br:...
0050 00 00 04 c8 a0 02 03 00 00 29 04 c4 00 00 00 00 :...
0060 00 00
```



Navegando pela interface do Wireshark

Capturing from wlo1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
599	36.641658124	192.168.0.15	187.123.29.54	DNS	82	Standard query 0x4e2f A registro.br OPT
600	36.641728550	192.168.0.15	187.123.29.54	DNS	82	Standard query 0x8b53 AAAA registro.br OPT
601	36.667822545	187.123.29.54	192.168.0.15	DNS	110	Standard query response 0x8b53 AAAA registro.br AAAA 2001:12f...
602	36.723532628	187.123.29.54	192.168.0.15	DNS	98	Standard query response 0x4e2f A registro.br A 200.160.2.3 OPT
603	36.724748410	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=1/256, ttl=64 (reply in 6...
604	36.776908002	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=1/256, ttl=243 (request i...
605	36.777735463	192.168.0.15	187.123.29.54	DNS	95	Standard query 0x983f PTR 3.2.160.200.in-addr.arpa OPT
606	37.139369967	187.123.29.54	192.168.0.15	DNS	120	Standard query response 0x983f PTR 3.2.160.200.in-addr.arpa P...
607	37.728402680	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=2/512, ttl=64 (reply in 6...
608	37.780383009	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=2/512, ttl=243 (request i...
609	38.572478335	142.251.129.78	192.168.0.15	UDP	79	443 → 32867 Len=37
610	38.584561262	192.168.0.15	142.251.129.78	UDP	76	32867 → 443 Len=34
611	38.732128438	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=3/768, ttl=64 (reply in 6...
612	38.783687671	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=3/768, ttl=243 (request i...
613	39.738172262	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=4/1024, ttl=64 (reply in ...
614	39.790955314	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=4/1024, ttl=243 (request ...
615	40.504718400	192.168.0.15	31.13.90.60	TLSv1.2	136	Application Data
616	40.549809234	31.13.90.60	192.168.0.15	TCP	66	443 → 57156 [ACK] Seq=143 Ack=212 Win=297 Len=0 TSval=2164521...
617	40.723440006	31.13.90.60	192.168.0.15	TLSv1.2	132	Application Data

▶ Frame 602: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0

▶ Ethernet II, Src: MS-NLB-PhysServer-16:18:6c:1e:8c, Dst: IntelCor_5d:6d:94 (5c:cd:5b:5d:6d:94)

▶ Internet Protocol Version 4, Src: 187.123.29.54, Dst: 192.168.0.15

▶ User Datagram Protocol, Src Port: 53, Dst Port: 38577

Domain Name System (response)

- Transaction ID: 0x4e2f
- Flags: 0x8180 Standard query response, No error
- Questions: 1
- Answer RRs: 1
- Authority RRs: 0
- Additional RRs: 1
- Queries
- Answers
- Additional records

Request: Type: 5001

```
0000 5c cd 5b 5d 6d 94 02 10 18 6c 1e 8c 08 00 45 00  N: [m]...
0010 00 54 2c b1 00 00 fb 11 f9 7e bb 7b 1d 36 c9 a8  T: ...
0020 00 0f 00 35 96 b1 00 40 22 1d 4e 2f 81 80 00 01  ..5...@ "N/...
0030 00 01 00 00 01 08 72 65 67 69 73 74 72 6f 02  ..r registro...
0040 62 72 00 00 01 00 01 c0 0c 09 01 00 01 00 02 a3  ..
0050 00 00 04 c8 a0 02 03 00 00 29 04 c4 00 00 00 00  ..
0060 00 00
```



Navegando pela interface do Wireshark

Capturing from wlo1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
599	36.641658124	192.168.0.15	187.123.29.54	DNS	82	Standard query 0x4e2f A registro.br OPT
600	36.777735463	192.168.0.15	187.123.29.54	DNS	95	Standard query 0x983f PTR 3.2.160.200.in-addr.arpa OPT
606	37.139369967	187.123.29.54	192.168.0.15	DNS	120	Standard query response 0x983f PTR 3.2.160.200.in-addr.arpa P...
607	37.728492680	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=2/512, ttl=64 (reply in 6...
608	37.780383009	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=2/512, ttl=243 (request i...
609	38.572478335	142.251.129.78	192.168.0.15	UDP	79	443 → 32867 Len=37
610	38.584561262	192.168.0.15	142.251.129.78	UDP	76	32867 → 443 Len=34
611	38.732128438	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=3/768, ttl=64 (reply in 6...
612	38.783687671	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=3/768, ttl=243 (request i...
613	39.738172262	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=4/1024, ttl=64 (reply in ...
614	39.790955314	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=4/1024, ttl=243 (request ...
615	40.504718400	192.168.0.15	31.13.90.60	TLSv1.2	136	Application Data
616	40.549809234	31.13.90.60	192.168.0.15	TCP	66	443 → 57156 [ACK] Seq=143 Ack=212 Win=297 Len=0 TSval=2164521...
617	40.723440006	31.13.90.60	192.168.0.15	TLSv1.2	132	Application Data

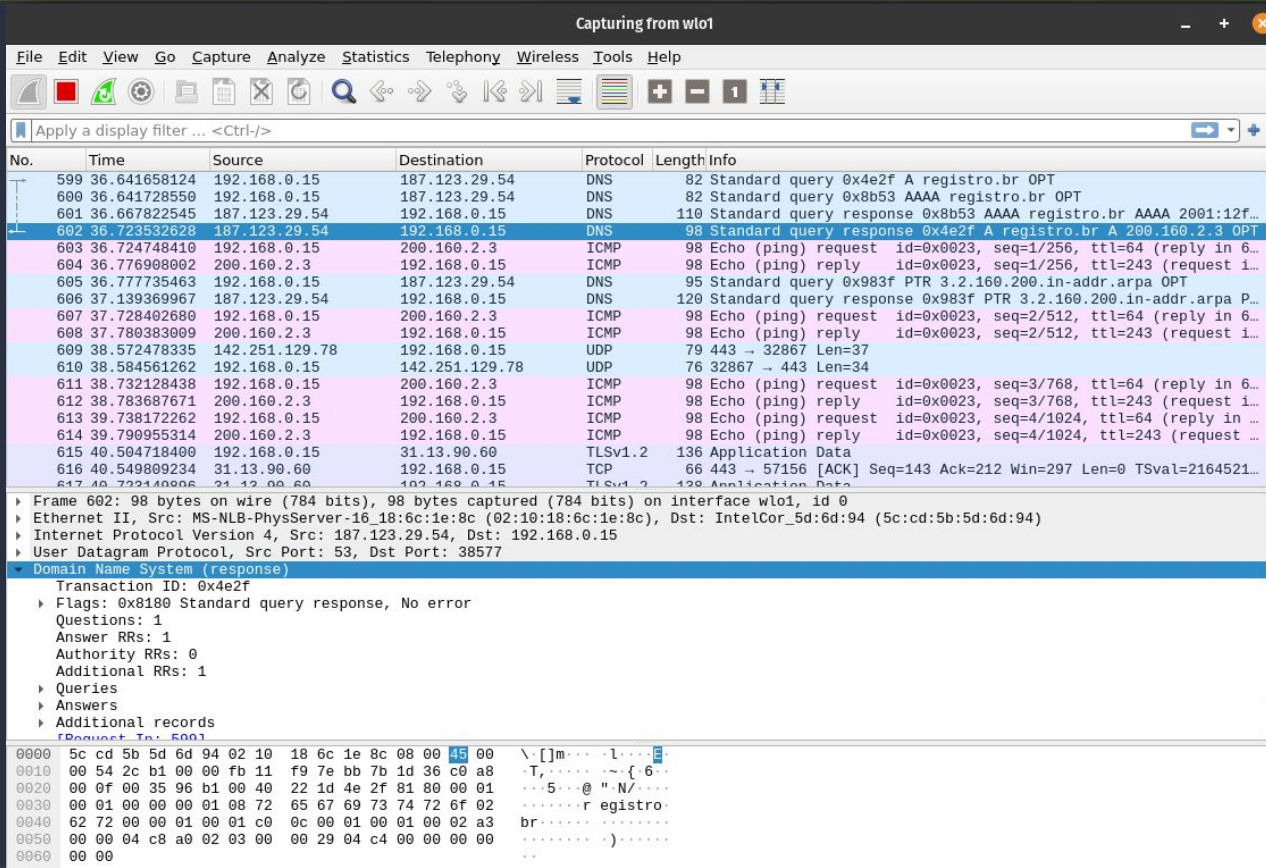
Frame 602: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0

- Ethernet II, Src: MS-NLB-PhysServer-16 18:6c:1e:8c (02:10:18:6c:1e:8c), Dst: IntelCor_5d:6d:94 (5c:cd:5b:5d:6d:94)
- Internet Protocol Version 4, Src: 187.123.29.54, Dst: 192.168.0.15
- User Datagram Protocol, Src Port: 53, Dst Port: 38577
- Domain Name System (response)
 - Transaction ID: 0x4e2f
 - Flags: 0x8180 Standard query response, No error
 - Questions: 1
 - Answer RRs: 1
 - Authority RRs: 0
 - Additional RRs: 1
 - Queries
 - Answers
 - Additional records (Domain: Tel: 5001)

0000 5c cd 5b 5d 6d 94 02 10 18 6c 1e 8c 08 00 45 00
0010 00 54 2c b1 00 00 fb 11 f9 7e bb 7b 1d 36 c9 a8
0020 00 0f 00 35 96 b1 00 40 22 1d 4e 2f 81 80 00 01
0030 00 01 00 00 01 08 72 65 67 69 73 74 72 6f 02
0040 62 72 00 00 01 00 01 c0 0c 09 01 00 01 00 02 a3
0050 00 00 04 c8 a0 02 03 00 00 29 04 c4 00 00 00 00
0060 00 00



Navegando pela interface do Wireshark



Capturing from wlo1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
599	36.641658124	192.168.0.15	187.123.29.54	DNS	82	Standard query 0x4e2f A registro.br OPT
600	36.641728550	192.168.0.15	187.123.29.54	DNS	82	Standard query 0x8b53 AAAA registro.br OPT
601	36.667822545	187.123.29.54	192.168.0.15	DNS	110	Standard query response 0x8b53 AAAA registro.br AAAA 2001:12f...
602	36.723532628	187.123.29.54	192.168.0.15	DNS	98	Standard query response 0x4e2f A registro.br A 200.160.2.3 OPT
603	36.724748410	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=1/256, ttl=64 (reply in 6...
604	36.776908002	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=1/256, ttl=243 (request i...
605	36.777735463	192.168.0.15	187.123.29.54	DNS	95	Standard query 0x983f PTR 3.2.160.200.in-addr.arpa OPT
606	37.139369967	187.123.29.54	192.168.0.15	DNS	120	Standard query response 0x983f PTR 3.2.160.200.in-addr.arpa P...
607	37.728402680	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=2/512, ttl=64 (reply in 6...
608	37.780383009	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=2/512, ttl=243 (request i...
609	38.572478335	142.251.129.78	192.168.0.15	UDP	79	443 → 32867 Len=37
610	38.584561262	192.168.0.15	142.251.129.78	UDP	76	32867 → 443 Len=34
611	38.732128438	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=3/768, ttl=64 (reply in 6...
612	38.783687671	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=3/768, ttl=243 (request i...
613	39.738172262	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=4/1024, ttl=64 (reply in ...
614	39.790955314	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=4/1024, ttl=243 (request ...
615	40.504748400	192.168.0.15	31.13.90.60	TLSv1.2	136	Application Data
616	40.549809234	31.13.90.60	192.168.0.15	TCP	66	443 → 57156 [ACK] Seq=143 Ack=212 Win=297 Len=0 TSval=2164521...
617	40.723140906	192.168.0.15	192.168.0.15	TLSv1.2	129	Application Data

▶ Frame 602: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0

▶ Ethernet II, Src: MS-NLB-PhysServer-16:18:6c:1e:8c (02:10:18:6c:1e:8c), Dst: IntelCor_5d:6d:94 (5c:cd:5b:5d:6d:94)

▶ Internet Protocol Version 4, Src: 187.123.29.54, Dst: 192.168.0.15

▶ User Datagram Protocol, Src Port: 53, Dst Port: 38577

Domain Name System (response)

- Transaction ID: 0x4e2f
- Flags: 0x8180 Standard query response, No error
- Questions: 1
- Answer RRs: 1
- Authority RRs: 0
- Additional RRs: 1
- Queries
- Answers
- Additional records

0000 5c cd 5b 5d 6d 94 02 10 18 6c 1e 8c 08 00 45 00 \[:]m...l...
0010 00 54 2c b1 00 00 fb 11 f9 7e bb 7b 1d 36 c0 a8 T...{ 6...
0020 00 0f 00 35 96 b1 00 40 22 1d 4e 2f 81 80 00 01 ...5...@ "N/...
0030 00 01 00 00 01 08 72 65 67 69 73 74 72 6f 02 ...r registro...
0040 62 72 00 00 01 00 01 c0 0c 00 01 00 01 00 02 a3 br...
0050 00 00 04 c8 a0 02 03 00 00 29 04 c4 00 00 00 00).....
0060 00 00



Navegando pela interface do Wireshark

Capturing from wlo1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

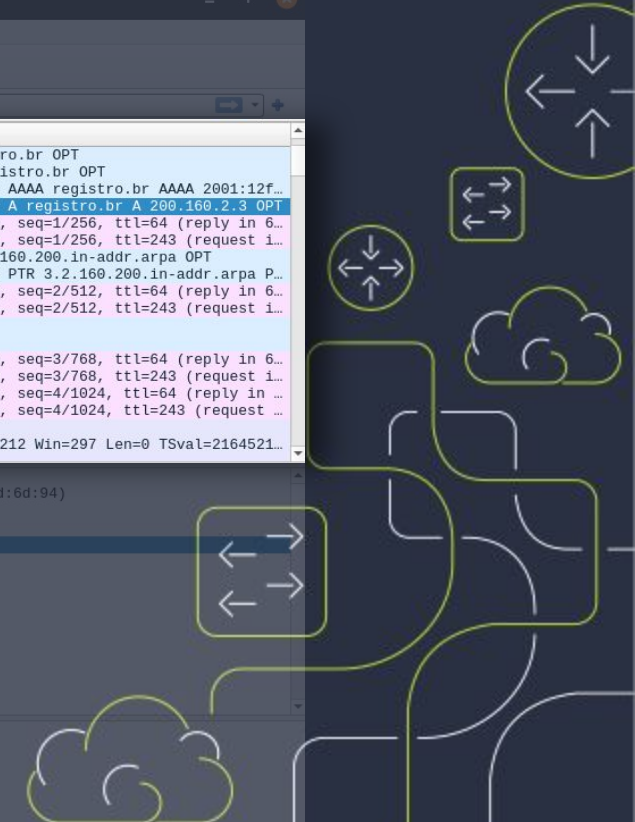
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
599	36.641658124	192.168.0.15	187.123.29.54	DNS	82	Standard query 0x4e2f A registro.br OPT
600	36.641728550	192.168.0.15	187.123.29.54	DNS	82	Standard query 0x8b53 AAAA registro.br OPT
601	36.667822545	187.123.29.54	192.168.0.15	DNS	110	Standard query response 0x8b53 AAAA registro.br AAAA 2001:12f...
602	36.723532628	187.123.29.54	192.168.0.15	DNS	98	Standard query response 0x4e2f A registro.br A 200.160.2.3 OPT
603	36.724748410	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=1/256, ttl=64 (reply in 6...
604	36.776908002	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=1/256, ttl=243 (request i...
605	36.777735463	192.168.0.15	187.123.29.54	DNS	95	Standard query 0x983f PTR 3.2.160.200.in-addr.arpa OPT
606	37.139369967	187.123.29.54	192.168.0.15	DNS	120	Standard query response 0x983f PTR 3.2.160.200.in-addr.arpa P...
607	37.728402680	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=2/512, ttl=64 (reply in 6...
608	37.780383009	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=2/512, ttl=243 (request i...
609	38.572478335	142.251.129.78	192.168.0.15	UDP	79	443 → 32867 Len=37
610	38.584561262	192.168.0.15	142.251.129.78	UDP	76	32867 → 443 Len=34
611	38.732128438	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=3/768, ttl=64 (reply in 6...
612	38.783687671	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=3/768, ttl=243 (request i...
613	39.738172262	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=4/1024, ttl=64 (reply in ...
614	39.790955314	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=4/1024, ttl=243 (request ...
615	40.504718400	192.168.0.15	31.13.90.60	TLSv1.2	136	Application Data
616	40.549809234	31.13.90.60	192.168.0.15	TCP	66	443 → 57156 [ACK] Seq=143 Ack=212 Win=297 Len=0 TSval=2164521...
617	40.7232140906	31.13.90.60	192.168.0.15	TLSv1.2	129	Application Data

Frame 602: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0

- Ethernet II, Src: MS-NLB-PhysServer-16:18:6c:1e:8c (02:10:18:6c:1e:8c), Dst: IntelCor_5d:6d:94 (5c:cd:5b:5d:6d:94)
- Internet Protocol Version 4, Src: 187.123.29.54, Dst: 192.168.0.15
- User Datagram Protocol, Src Port: 53, Dst Port: 38577
- Domain Name System (response)
 - Transaction ID: 0x4e2f
 - Flags: 0x8180 Standard query response, No error
 - Questions: 1
 - Answer RRs: 1
 - Authority RRs: 0
 - Additional RRs: 1
 - Queries
 - Answers
 - Additional records (Request: Tx: 500)

```
0000 5c cd 5b 5d 6d 94 02 10 18 6c 1e 8c 08 00 45 00
0010 00 54 2c b1 00 00 fb 11 f9 7e bb 7b 1d 36 c9 a8
0020 00 0f 00 35 96 b1 00 40 22 1d 4e 2f 81 80 00 01
0030 00 01 00 00 01 08 72 65 67 69 73 74 72 6f 02
0040 62 72 00 00 01 00 01 c0 0c 00 01 00 01 00 02 a3
0050 00 00 04 c8 a0 02 03 00 00 29 04 c4 00 00 00 00
0060 00 00
```



Navegando pela interface do Wireshark

Capturing from wlo1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Time	Source	Destination	Protocol	Length	Info
599	36.641658124	192.168.0.15	187.123.29.54	DNS	82	Standard query 0x4e2f A registro.br OPT
600	36.641728550	192.168.0.15	187.123.29.54	DNS	82	Standard query 0x8b53 AAAA registro.br OPT
601	36.667822545	187.123.29.54	192.168.0.15	DNS	110	Standard query response 0x8b53 AAAA registro.br AAAA 2001:12f...
602	36.723532628	187.123.29.54	192.168.0.15	DNS	98	Standard query response 0x4e2f A registro.br A 200.160.2.3 OPT
603	36.724748410	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=1/256, ttl=64 (reply in 6...
604	36.776908002	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=1/256, ttl=243 (request i...
605	36.777735463	192.168.0.15	187.123.29.54	DNS	95	Standard query 0x983f PTR 3.2.160.200.in-addr.arpa OPT
606	37.139369967	187.123.29.54	192.168.0.15	DNS	120	Standard query response 0x983f PTR 3.2.160.200.in-addr.arpa P...
607	37.728402680	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=2/512, ttl=64 (reply in 6...
608	37.780383009	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=2/512, ttl=243 (request i...
609	38.572478335	142.251.129.78	192.168.0.15	UDP	79	443 - 32867 Len=37
610	38.584561262	192.168.0.15	142.251.129.78	UDP	76	32867 - 443 Len=34
611	38.732128438	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=3/768, ttl=64 (reply in 6...
612	38.783687671	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=3/768, ttl=243 (request i...
613	39.738172262	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=4/1024, ttl=64 (reply in ...
614	39.790955314	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=4/1024, ttl=243 (request ...
615	40.504718400	192.168.0.15	31.13.90.60	TLSv1.2	136	Application Data
616	40.549809234	31.13.90.60	192.168.0.15	TCP	66	443 - 57156 [ACK] Seq=143 Ack=212 Win=297 Len=0 TSval=2164521...
617	40.722140906	31.13.90.60	192.168.0.15	TLSv1.2	128	Application Data

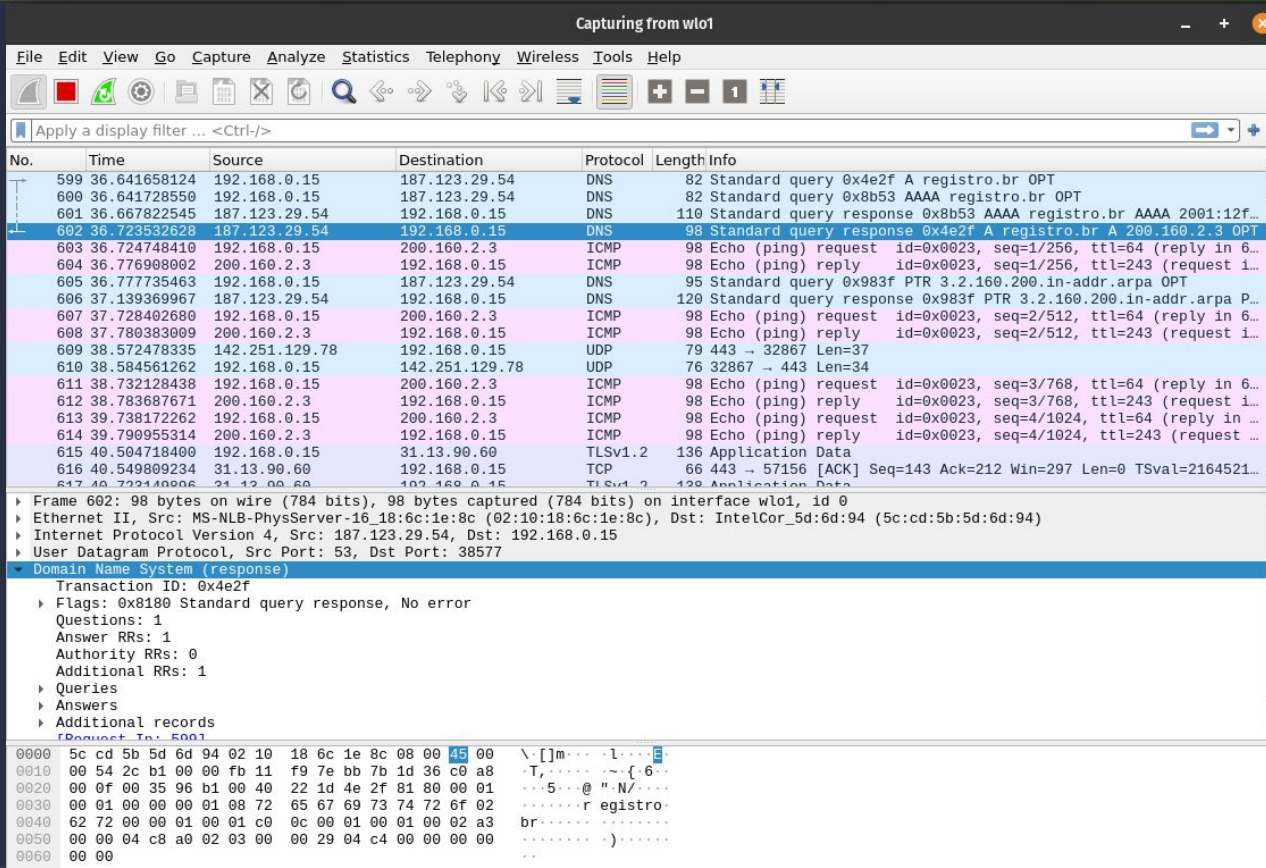
Transaction ID: 0x4e2f
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 1
Queries
Answers
Additional records
[Domain: Tel: 500]

```
0000 5c cd 5b 5d 6d 94 02 10 18 6c 1e 8c 08 00 00 00 00
0010 00 54 2c b1 00 00 fb 11 f9 7e bb 7b 1d 36 c9 a8
0020 00 0f 00 35 96 b1 00 40 22 1d 4e 2f 81 80 00 01
0030 00 01 00 00 01 08 72 65 67 69 73 74 72 6f 02
0040 62 72 00 00 01 00 01 c0 0c 09 01 00 01 00 02 a3
0050 00 00 04 c8 a0 02 03 00 00 29 04 c4 00 00 00 00
0060 00 00
```

```

T, seq=1/256, ttl=64
... 5... @ "N/...
... registro...
... (reply in 6...
```

Navegando pela interface do Wireshark



Capturing from wlo1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
599	36.641658124	192.168.0.15	187.123.29.54	DNS	82	Standard query 0x4e2f A registro.br OPT
600	36.641728550	192.168.0.15	187.123.29.54	DNS	82	Standard query 0x8b53 AAAA registro.br OPT
601	36.667822545	187.123.29.54	192.168.0.15	DNS	110	Standard query response 0x8b53 AAAA registro.br AAAA 2001:12f...
602	36.723532628	187.123.29.54	192.168.0.15	DNS	98	Standard query response 0x4e2f A registro.br A 200.160.2.3 OPT
603	36.724748410	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=1/256, ttl=64 (reply in 6...
604	36.776908002	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=1/256, ttl=243 (request i...
605	36.777735463	192.168.0.15	187.123.29.54	DNS	95	Standard query 0x983f PTR 3.2.160.200.in-addr.arpa OPT
606	37.139369967	187.123.29.54	192.168.0.15	DNS	120	Standard query response 0x983f PTR 3.2.160.200.in-addr.arpa P...
607	37.728402680	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=2/512, ttl=64 (reply in 6...
608	37.780383009	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=2/512, ttl=243 (request i...
609	38.572478335	142.251.129.78	192.168.0.15	UDP	79	443 → 32867 Len=37
610	38.584561262	192.168.0.15	142.251.129.78	UDP	76	32867 → 443 Len=34
611	38.732128438	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=3/768, ttl=64 (reply in 6...
612	38.783687671	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=3/768, ttl=243 (request i...
613	39.738172262	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=4/1024, ttl=64 (reply in ...
614	39.790955314	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=4/1024, ttl=243 (request ...
615	40.504748400	192.168.0.15	31.13.90.60	TLSv1.2	136	Application Data
616	40.549809234	31.13.90.60	192.168.0.15	TCP	66	443 → 57156 [ACK] Seq=143 Ack=212 Win=297 Len=0 TSval=2164521...
617	40.723140906	31.13.90.60	192.168.0.15	TLSv1.2	129	Application Data

▶ Frame 602: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0

▶ Ethernet II, Src: MS-NLB-PhysServer-16 18:6c:1e:8c (02:10:18:6c:1e:8c), Dst: IntelCor_5d:6d:94 (5c:cd:5b:5d:6d:94)

▶ Internet Protocol Version 4, Src: 187.123.29.54, Dst: 192.168.0.15

▶ User Datagram Protocol, Src Port: 53, Dst Port: 38577

▼ Domain Name System (response)

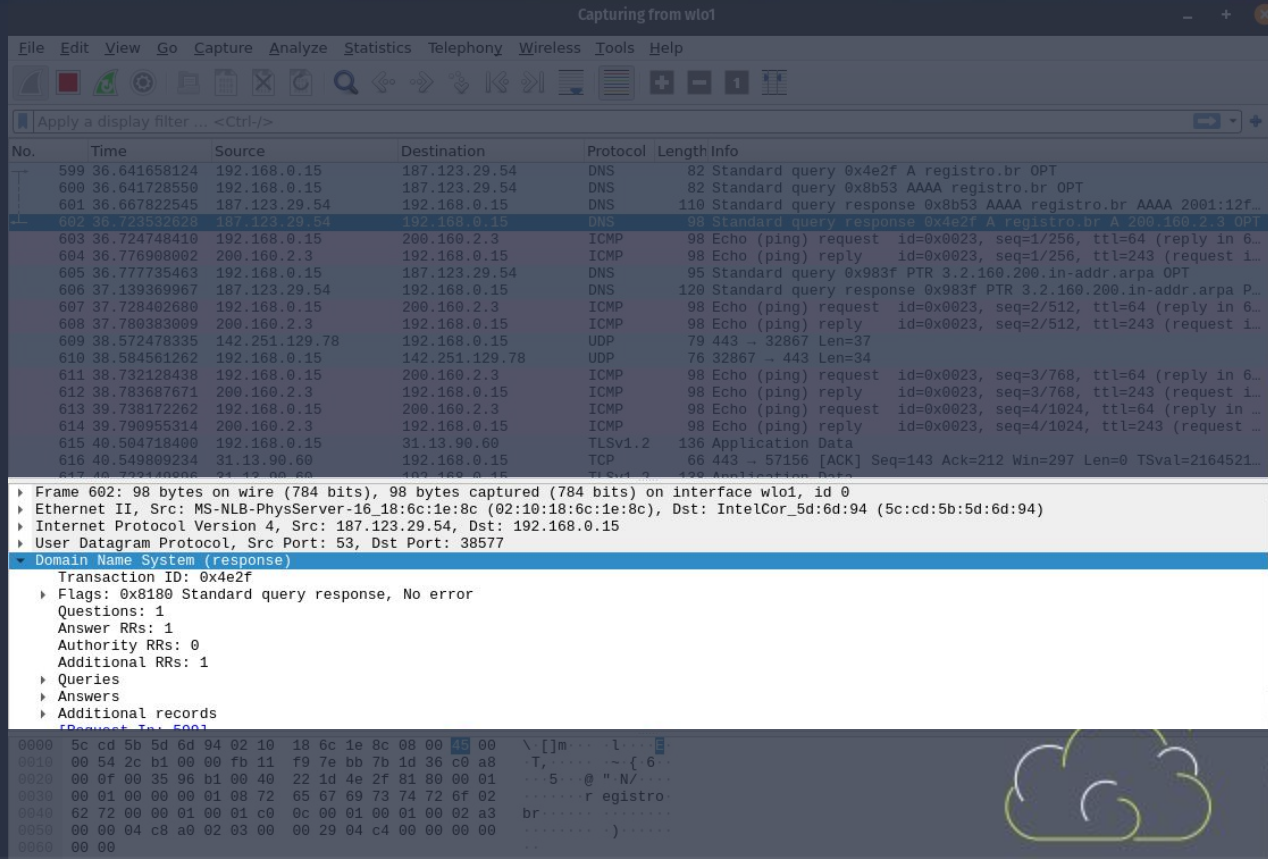
- Transaction ID: 0x4e2f
- Flags: 0x8180 Standard query response, No error
- Questions: 1
- Answer RRs: 1
- Authority RRs: 0
- Additional RRs: 1
- Queries
- Answers
- Additional records

Request ID: 5001

```
0000 5c cd 5b 5d 6d 94 02 10 18 6c 1e 8c 08 00 45 00  \:[]m...l...
0010 00 54 2c b1 00 00 fb 11 f9 7e bb 7b 1d 36 c0 a8  T...{ 6
0020 00 0f 00 35 96 b1 00 40 22 1d 4e 2f 81 80 00 01  :5...@ "N/...
0030 00 01 00 00 01 08 72 65 67 69 73 74 72 6f 02  :...r registro
0040 62 72 00 00 01 00 01 c0 0c 00 01 00 01 00 02 a3  br:...
0050 00 00 04 c8 a0 02 03 00 00 29 04 c4 00 00 00 00  :... )...
0060 00 00
```



Navegando pela interface do Wireshark



Capturing from wlo1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
599	36.641658124	192.168.0.15	187.123.29.54	DNS	82	Standard query 0x4e2f A registro.br OPT
600	36.641728550	192.168.0.15	187.123.29.54	DNS	82	Standard query 0x8b53 AAAA registro.br OPT
601	36.667822545	187.123.29.54	192.168.0.15	DNS	110	Standard query response 0x8b53 AAAA registro.br AAAA 2001:12f...
602	36.723552628	187.123.29.54	192.168.0.15	DNS	98	Standard query response 0x4e2f A registro.br A 200.160.2.3 OPT
603	36.724748410	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=1/256, ttl=64 (reply in 6...
604	36.776908002	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=1/256, ttl=243 (request i...
605	36.777735463	192.168.0.15	187.123.29.54	DNS	95	Standard query 0x983f PTR 3.2.160.200.in-addr.arpa OPT
606	37.139369967	187.123.29.54	192.168.0.15	DNS	120	Standard query response 0x983f PTR 3.2.160.200.in-addr.arpa P...
607	37.728402680	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=2/512, ttl=64 (reply in 6...
608	37.780383009	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=2/512, ttl=243 (request i...
609	38.572478335	142.251.129.78	192.168.0.15	UDP	79	443 → 32867 Len=37
610	38.584561262	192.168.0.15	142.251.129.78	UDP	76	32867 → 443 Len=34
611	38.732128438	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=3/768, ttl=64 (reply in 6...
612	38.783687671	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=3/768, ttl=243 (request i...
613	39.738172262	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=4/1024, ttl=64 (reply in ...
614	39.790955314	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=4/1024, ttl=243 (request ...
615	40.504718400	192.168.0.15	31.13.90.60	TLSv1.2	136	Application Data
616	40.549809234	31.13.90.60	192.168.0.15	TCP	66	443 → 57156 [ACK] Seq=143 Ack=212 Win=297 Len=0 TSval=2164521...
617	40.733448086	31.13.90.60	192.168.0.15	TLSv1.2	429	Application Data

▶ Frame 602: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0

▶ Ethernet II, Src: MS-NLB-PhysServer-16 18:6c:1e:8c (02:10:18:6c:1e:8c), Dst: IntelCor_5d:6d:94 (5c:cd:5b:5d:6d:94)

▶ Internet Protocol Version 4, Src: 187.123.29.54, Dst: 192.168.0.15

▶ User Datagram Protocol, Src Port: 53, Dst Port: 38577

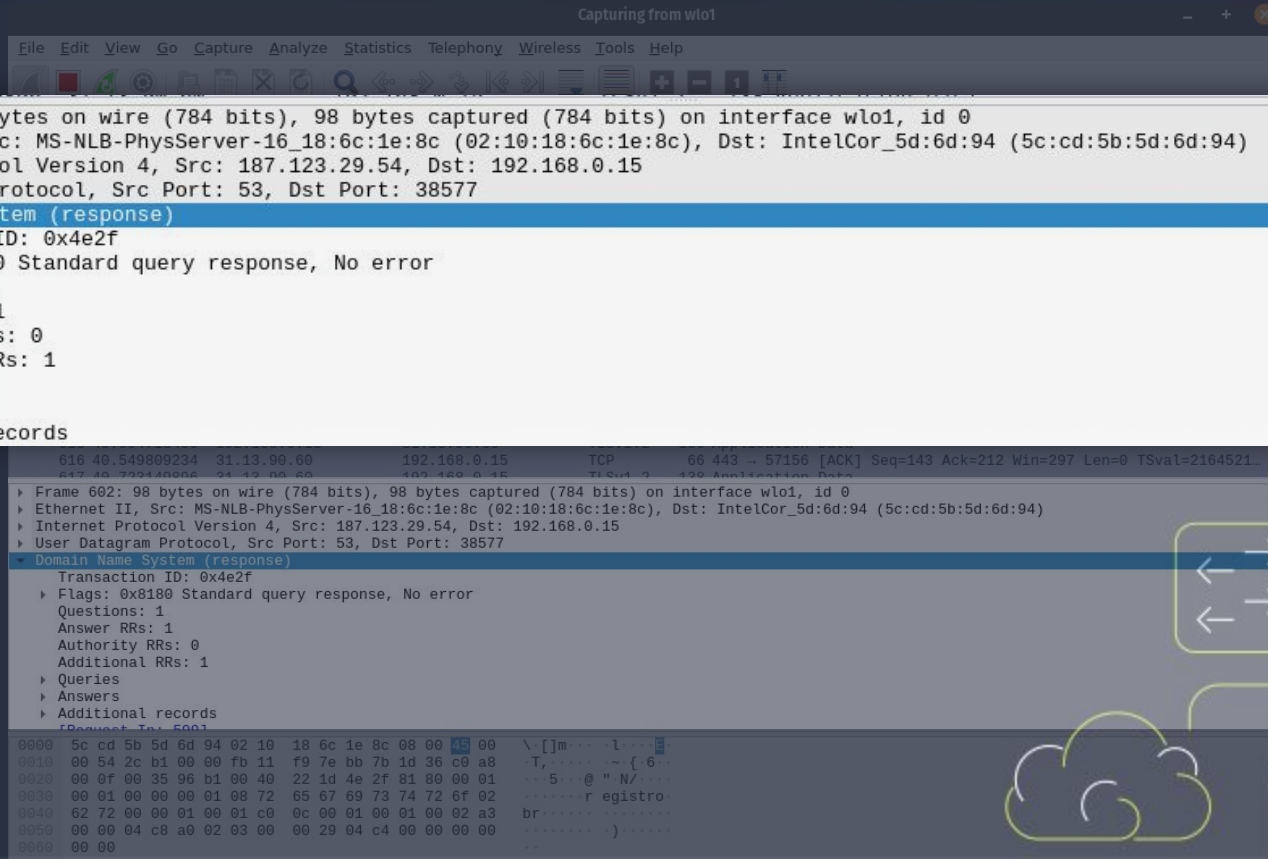
▼ Domain Name System (response)

- Transaction ID: 0x4e2f
- Flags: 0x8100 Standard query response, No error
- Questions: 1
- Answer RRs: 1
- Authority RRs: 0
- Additional RRs: 1
- Queries
- Answers
- Additional records

0000 5c cd 5b 5d 6d 94 02 10 18 6c 1e 8c 08 00 45 00
0010 00 54 2c b1 00 00 fb 11 f9 7e bb 7b 1d 36 c9 a8
0020 00 0f 00 35 96 b1 00 40 22 1d 4e 2f 81 80 00 01
0030 00 01 00 00 01 08 72 65 67 69 73 74 72 6f 02
0040 62 72 00 00 01 00 01 c0 0c 09 01 00 01 00 02 a3
0050 00 00 04 c8 a0 02 03 00 00 29 04 c4 00 00 00 00
0060 00 00



Navegando pela interface do Wireshark



Capturing from wlo1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

- ▶ Frame 602: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0
- ▶ Ethernet II, Src: MS-NLB-PhysServer-16_18:6c:1e:8c (02:10:18:6c:1e:8c), Dst: IntelCor_5d:6d:94 (5c:cd:5b:5d:6d:94)
- ▶ Internet Protocol Version 4, Src: 187.123.29.54, Dst: 192.168.0.15
- ▶ User Datagram Protocol, Src Port: 53, Dst Port: 38577
- ▼ Domain Name System (response)
 - Transaction ID: 0x4e2f
 - ▶ Flags: 0x8180 Standard query response, No error
 - Questions: 1
 - Answer RRs: 1
 - Authority RRs: 0
 - Additional RRs: 1
 - ▶ Queries
 - ▶ Answers
 - ▶ Additional records

816 40 549809234 31.13.99.60 192.168.0.15 TCP 66 443 - 57156 [ACK] Seq=143 Ack=212 Win=297 Len=0 TSval=2164521...

▶ Frame 602: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0

▶ Ethernet II, Src: MS-NLB-PhysServer-16_18:6c:1e:8c (02:10:18:6c:1e:8c), Dst: IntelCor_5d:6d:94 (5c:cd:5b:5d:6d:94)

▶ Internet Protocol Version 4, Src: 187.123.29.54, Dst: 192.168.0.15

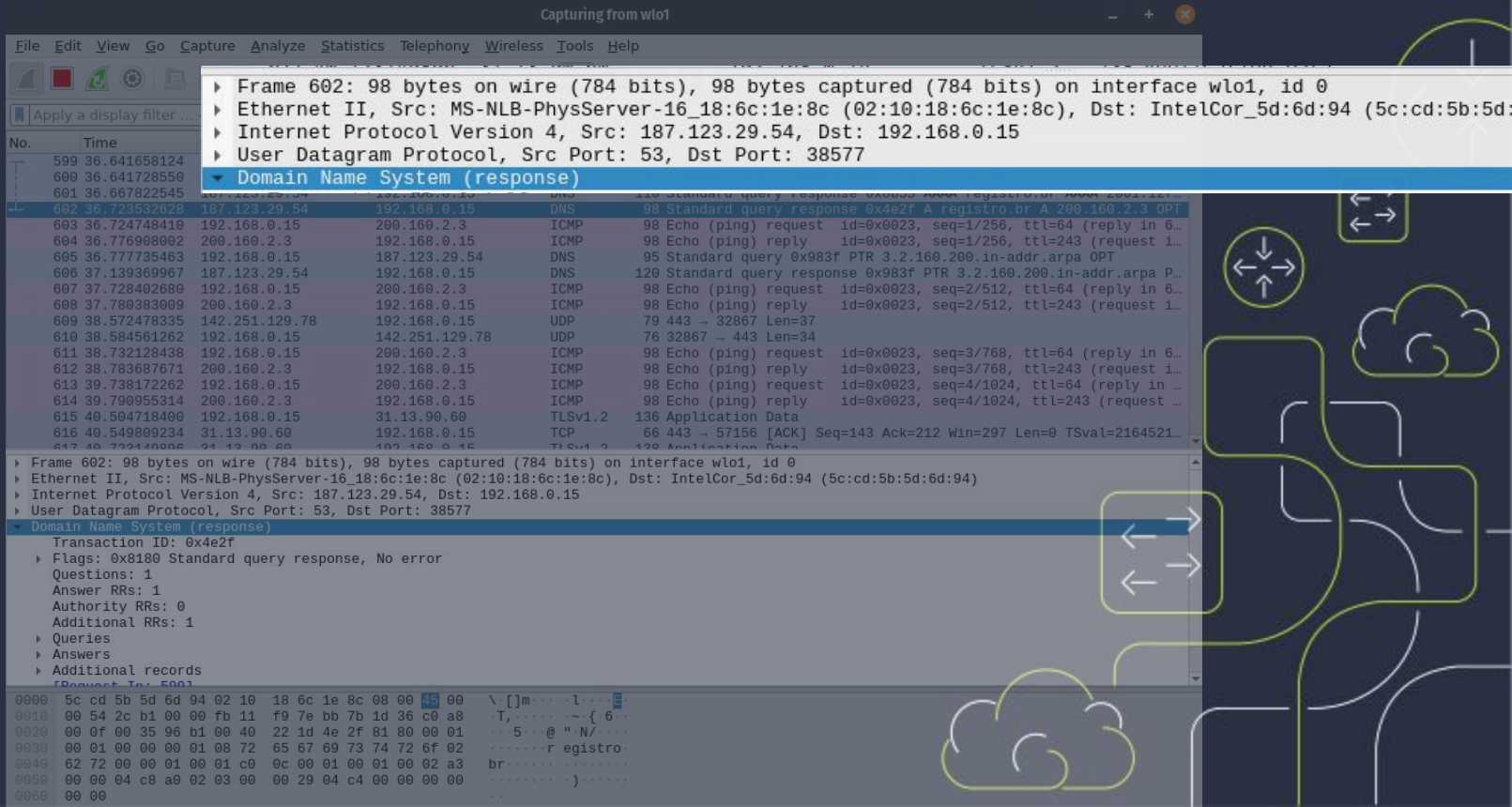
▶ User Datagram Protocol, Src Port: 53, Dst Port: 38577

▼ Domain Name System (response)

- Transaction ID: 0x4e2f
- ▶ Flags: 0x8180 Standard query response, No error
- Questions: 1
- Answer RRs: 1
- Authority RRs: 0
- Additional RRs: 1
- ▶ Queries
- ▶ Answers
- ▶ Additional records

0000 5c cd 5b 5d 6d 94 02 10 18 6c 1e 8c 08 00 45 00 X:\m... User...
0010 00 54 2c b1 00 00 fb 11 f9 7e bb 7b 1d 36 c9 a8 T, ... { 6...
0020 00 0f 00 35 96 b1 00 40 22 1d 4e 2f 81 80 00 01 ...5... @ "N/...
0030 00 01 00 00 00 01 08 72 65 67 69 73 74 72 6f 02 ...near registro...
0040 62 72 00 00 01 00 01 c0 0c 09 01 00 01 00 02 a3 b...
0050 00 00 04 c8 a0 02 03 00 00 29 04 c4 00 00 00 00 ...
0060 00 00

Navegando pela interface do Wireshark



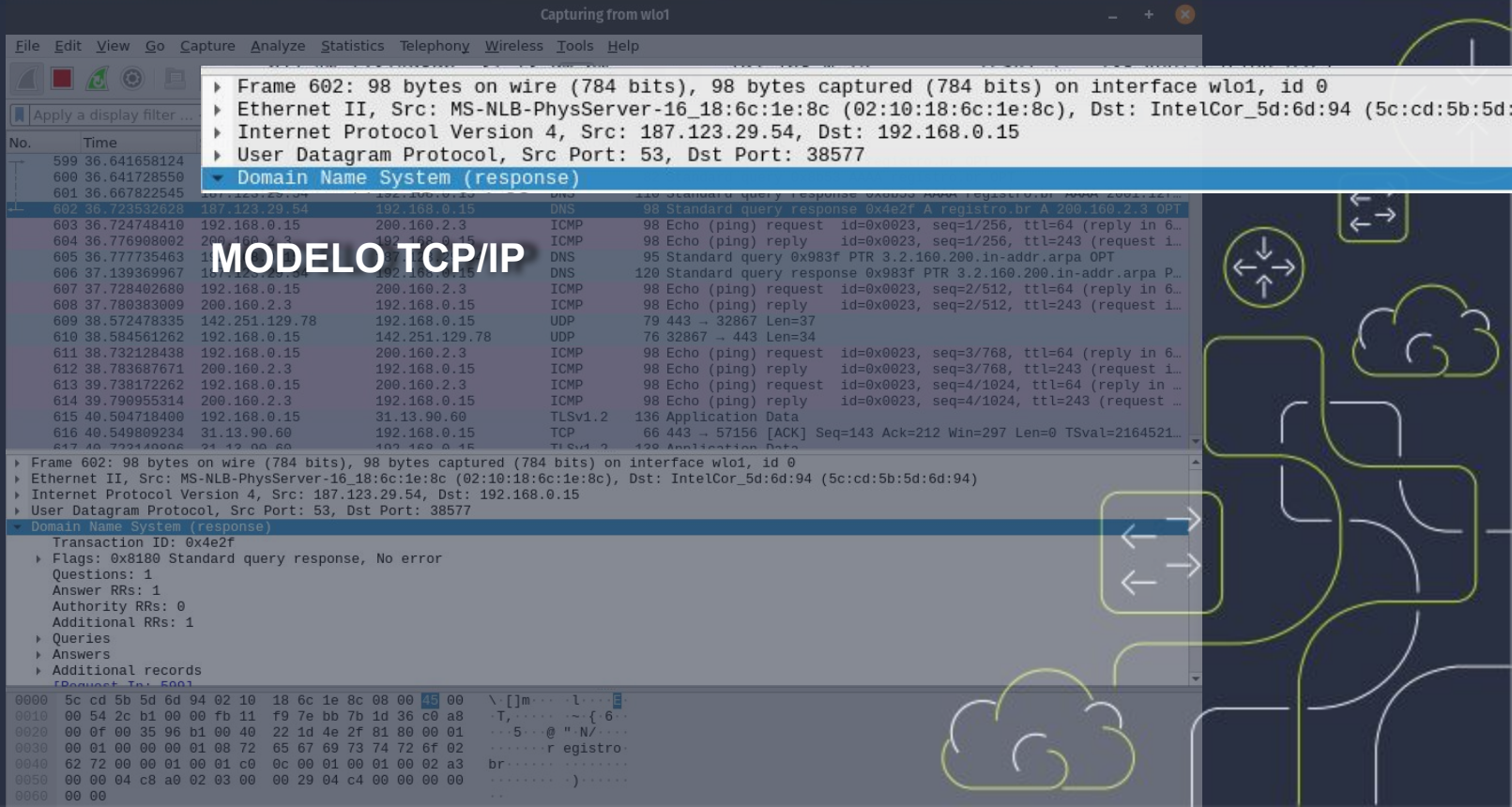
The screenshot displays the Wireshark interface with a packet capture from interface wlo1. The selected packet is a Domain Name System (response) packet, which is expanded to show its internal structure. The packet details pane shows the following information:

- Transaction ID: 0x4e2f
- Flags: 0x8180 Standard query response, No error
- Questions: 1
- Answer RRs: 1
- Authority RRs: 0
- Additional RRs: 1
- Queries
- Answers
- Additional records (Request ID: 500)

The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII. The ASCII portion includes the text "Standard query response" and "PTR 3.2.160.200.in-addr.arpa OPT".

No.	Time	Source	Destination	Protocol	Length	Info
599	36.641658124					
600	36.641728550					
601	36.667822545					
602	36.723532628	187.123.29.54	192.168.0.15	DNS	98	Standard query response 0x4e2f A registro.br A 200.160.2.3 OPT
603	36.724748410	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=1/256, ttl=64 (reply in 6...
604	36.776908002	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=1/256, ttl=243 (request i...
605	36.777735463	192.168.0.15	187.123.29.54	DNS	95	Standard query 0x983f PTR 3.2.160.200.in-addr.arpa OPT
606	37.139369967	187.123.29.54	192.168.0.15	DNS	120	Standard query response 0x983f PTR 3.2.160.200.in-addr.arpa P...
607	37.728402680	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=2/512, ttl=64 (reply in 6...
608	37.780383009	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=2/512, ttl=243 (request i...
609	38.572478335	142.251.129.78	192.168.0.15	UDP	79	443 → 32867 Len=37
610	38.584561262	192.168.0.15	142.251.129.78	UDP	76	32867 → 443 Len=34
611	38.732128438	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=3/768, ttl=64 (reply in 6...
612	38.783687671	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=3/768, ttl=243 (request i...
613	39.738172262	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=4/1024, ttl=64 (reply in ...
614	39.790955314	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=4/1024, ttl=243 (request ...
615	40.504781400	192.168.0.15	31.13.90.60	TLSv1.2	136	Application Data
616	40.549809234	31.13.90.60	192.168.0.15	TCP	66	443 → 57156 [ACK] Seq=143 Ack=212 Win=297 Len=0 TSval=2164521...
617	40.723440006	192.168.0.15	200.160.2.3	TLSv1.2	136	Application Data

Navegando pela interface do Wireshark



Capturing from wlo1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ...

No. Time


No.	Time	Source	Destination	Protocol	Length	Info
599	36.641658124					
600	36.641728550					
601	36.667822545					
602	36.723532628	187.123.29.54	192.168.0.15	DNS	98	Standard query response 0x4e2f A registro.br A 200.160.2.3 OPT
603	36.724748410	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=1/256, ttl=64 (reply in 6...
604	36.776908002	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=1/256, ttl=243 (request i...
605	36.777735463	192.168.0.15	192.168.0.15	DNS	95	Standard query 0x983f PTR 3.2.160.200.in-addr.arpa OPT
606	37.139369967	187.123.29.54	192.168.0.15	DNS	120	Standard query response 0x983f PTR 3.2.160.200.in-addr.arpa P...
607	37.728402680	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=2/512, ttl=64 (reply in 6...
608	37.780383009	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=2/512, ttl=243 (request i...
609	38.572478335	192.168.0.15	142.251.129.78	UDP	79	443 → 32867 Len=37
610	38.584561262	192.168.0.15	142.251.129.78	UDP	76	32867 → 443 Len=34
611	38.732128438	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=3/768, ttl=64 (reply in 6...
612	38.783687671	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=3/768, ttl=243 (request i...
613	39.738172262	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=4/1024, ttl=64 (reply in ...
614	39.790955314	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=4/1024, ttl=243 (request ...
615	40.504781800	192.168.0.15	31.13.90.60	TLSv1.2	136	Application Data
616	40.549809234	31.13.90.60	192.168.0.15	TCP	66	443 → 57156 [ACK] Seq=143 Ack=212 Win=297 Len=0 TSval=2164521...
617	40.723440006	192.168.0.15	192.168.0.15	TLSv1.2	120	Application Data

Frame 602: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0

- Ethernet II, Src: MS-NLB-PhysServer-16_18:6c:1e:8c (02:10:18:6c:1e:8c), Dst: IntelCor_5d:6d:94 (5c:cd:5b:5d:6d:94)
- Internet Protocol Version 4, Src: 187.123.29.54, Dst: 192.168.0.15
- User Datagram Protocol, Src Port: 53, Dst Port: 38577
- Domain Name System (response)
 - Transaction ID: 0x4e2f
 - Flags: 0x8180 Standard query response, No error
 - Questions: 1
 - Answer RRs: 1
 - Authority RRs: 0
 - Additional RRs: 1
 - Queries
 - Answers
 - Additional records

0000 5c cd 5b 5d 6d 94 02 10 18 6c 1e 8c 08 00 45 00
0010 00 54 2c b1 00 00 fb 11 f9 7e bb 7b 1d 36 c9 a8
0020 00 0f 00 35 96 b1 00 40 22 1d 4e 2f 81 80 00 01
0030 00 01 00 00 01 08 72 65 67 69 73 74 72 6f 02
0040 62 72 00 00 01 00 01 c0 0c 09 01 00 01 00 02 a3
0050 00 00 04 c8 a0 02 03 00 00 29 04 c4 00 00 00 00
0060 00 00

MODELO TCP/IP



Navegando pela interface do Wireshark

MODELO TCP/IP

- Frame 602: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0
- Ethernet II, Src: MS-NLB-PhysServer-16_18:6c:1e:8c (02:10:18:6c:1e:8c), Dst: IntelCor_5d:6d:94 (5c:cd:5b:5d:6d:94)
- Internet Protocol Version 4, Src: 187.123.29.54, Dst: 192.168.0.15
- User Datagram Protocol, Src Port: 53, Dst Port: 38577
- Domain Name System (response)

Acesso à Rede Ethernet

Transaction ID: 0x4e2f
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 1
Queries
Answers
Additional records (Request ID: 509)

```
0000 5c cd 5b 5d 6d 94 02 10 18 6c 1e 8c 08 00 45 00
0010 00 54 2c b1 00 00 fb 11 f9 7e bb 7b 1d 36 c9 a8
0020 00 0f 00 35 96 b1 00 40 22 1d 4e 2f 81 80 00 01
0030 00 01 00 00 00 01 08 72 65 67 69 73 74 72 6f 02
0040 62 72 00 00 01 00 01 c0 0c 09 01 00 01 00 02 a3
0050 00 00 04 c8 a0 02 03 00 00 29 04 c4 00 00 00 00
0060 00 00
```


Navegando pela interface do Wireshark

Frame 602: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0

- Ethernet II, Src: MS-NLB-PhysServer-16_18:6c:1e:8c (02:10:18:6c:1e:8c), Dst: IntelCor_5d:6d:94 (5c:cd:5b:5d:6d:94)
- Internet Protocol Version 4, Src: 187.123.29.54, Dst: 192.168.0.15
- User Datagram Protocol, Src Port: 53, Dst Port: 38577
- Domain Name System (response)

MODELO TCP/IP

Internet

Acesso à Rede

IPv4

Ethernet

0000 5c cd 5b 5d 6d 94 02 10 18 6c 1e 8c 08 00 45 00
0010 00 54 2c b1 00 00 fb 11 f9 7e bb 7b 1d 36 c9 a8
0020 00 0f 00 35 96 b1 00 40 22 1d 4e 2f 81 80 00 01
0030 00 01 00 00 01 08 72 65 67 69 73 74 72 6f 02
0040 62 72 00 00 01 00 01 c0 0c 09 01 00 01 00 02 a3
0050 00 00 04 c8 a0 02 03 00 20 04 c4 00 00 00 00
0060 00 00

Navegando pela interface do Wireshark

Capturing from wlo1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

- Frame 602: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0
- Ethernet II, Src: MS-NLB-PhysServer-16_18:6c:1e:8c (02:10:18:6c:1e:8c), Dst: IntelCor_5d:6d:94 (5c:cd:5b:5d:6d:94)
- Internet Protocol Version 4, Src Port: 187.123.29.54, Dst: 192.168.0.15
- User Datagram Protocol, Src Port: 53, Dst Port: 38577

Domain Name System (response)

No.	Time	Source	Destination	Protocol	Length	Info
599	6.641638124	192.168.0.15	200.160.2.3	DNS	98	Standard query response 0x4e2f A registro.br A 200.160.2.3 OPT
600	6.641728550	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) request id=0x0023, seq=1/256, ttl=64 (reply in 6...
601	6.667812545	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) reply id=0x0023, seq=1/256, ttl=243 (request i...
602	6.723512628	187.123.29.54	192.168.0.15	DNS	95	Standard query 0x983f PTR 3.2.160.200.in-addr.arpa OPT
603	6.724718410	192.168.0.15	200.160.2.3	DNS	120	Standard query response 0x983f PTR 3.2.160.200.in-addr.arpa P...
604	6.776938002	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) request id=0x0023, seq=2/512, ttl=64 (reply in 6...
605	6.777735463	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) reply id=0x0023, seq=2/512, ttl=243 (request i...
606	7.139319967	187.123.29.54	192.168.0.15	DNS	79	443 → 32867 Len=37
607	7.728432680	192.168.0.15	200.160.2.3	UDP	76	32867 → 443 Len=34
608	7.780333009	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) request id=0x0023, seq=3/768, ttl=64 (reply in 6...
609	8.572478335	142.251.129.78	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=3/768, ttl=243 (request i...
610	8.584511262	192.168.0.15	142.251.129.78	ICMP	98	Echo (ping) request id=0x0023, seq=4/1024, ttl=64 (reply in ...
611	8.732128438	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) reply id=0x0023, seq=4/1024, ttl=243 (request ...
612	8.783637671	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) request id=0x0023, seq=4/1024, ttl=64 (reply in ...
613	9.738172262	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) reply id=0x0023, seq=4/1024, ttl=243 (request ...
614	9.790955314	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) request id=0x0023, seq=3/768, ttl=64 (reply in 6...
615	9.504718400	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) reply id=0x0023, seq=3/768, ttl=243 (request i...
616	9.549839234	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) request id=0x0023, seq=4/1024, ttl=64 (reply in ...
617	9.723412628	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) reply id=0x0023, seq=4/1024, ttl=243 (request ...

MODELO TCP/IP

Transporte

Internet

Acesso à Rede

UDP

IPv4

Ethernet

Navegando pela interface do Wireshark

Capturing from wlo1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

- Frame 602: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0
- Ethernet II, Src: MS-NLB-PhysServer-16_18:6c:1e:8c (02:10:18:6c:1e:8c), Dst: IntelCor_5d:6d:94 (5c:cd:5b:5d:6d:94)
- Internet Protocol Version 4, Src Port: 187.123.29.54, Dst: 192.168.0.15
- User Datagram Protocol, Src Port: 53, Dst Port: 38577
- Domain Name System (response)

No.	Time	Source	Destination	Protocol	Length	Info
599	6.641638124	192.168.0.15	200.160.2.3	DNS	98	Standard query response 0x4e2f A registro.br A 200.160.2.3 OPT
600	6.641728550	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) request id=0x0023, seq=1/256, ttl=64 (reply in 6...
601	6.667822145	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) reply id=0x0023, seq=1/256, ttl=243 (request i...
602	6.723532128	187.123.29.54	192.168.0.15	DNS	95	Standard query 0x983f PTR 3.2.160.200.in-addr.arpa OPT
603	6.724718110	192.168.0.15	200.160.2.3	DNS	120	Standard query response 0x983f PTR 3.2.160.200.in-addr.arpa P...
604	6.776938602	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) request id=0x0023, seq=2/512, ttl=64 (reply in 6...
605	6.777735631	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) reply id=0x0023, seq=2/512, ttl=243 (request i...
606	7.139339167	187.123.29.54	192.168.0.15	DNS	98	Echo (ping) request id=0x0023, seq=3/768, ttl=64 (reply in 6...
607	7.728432180	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) reply id=0x0023, seq=3/768, ttl=243 (request i...
608	7.780333609	200.160.2.3	192.168.0.15	ICMP	79	443 → 32867 Len=37
609	8.572478135	192.168.0.15	200.160.2.3	UDP	76	32867 → 443 Len=34
610	8.584531762	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) request id=0x0023, seq=4/1024, ttl=64 (reply in 6...
611	8.732128438	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) reply id=0x0023, seq=4/1024, ttl=243 (request i...
612	8.783637671	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) request id=0x0023, seq=4/1024, ttl=64 (reply in ...
613	9.738122262	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) reply id=0x0023, seq=4/1024, ttl=243 (request ...
614	9.790955314	200.160.2.3	192.168.0.15	TLSv1.2	136	Application Data
615	9.504718400	192.168.0.15	200.160.2.3	TCP	66	443 → 57156 [ACK] Seq=143 Ack=212 Win=297 Len=0 TSval=2164521...
616	9.549839234	200.160.2.3	192.168.0.15	TLS	66	Application Data

MODELO TCP/IP

- Aplicação
- Transporte
- Internet
- Acesso à Rede

DNS

UDP

IPv4

Ethernet

Obtendo uma captura de pacote



captura.pcap



Obtendo uma captura de pacote

- Onde devo fazer a captura de pacote?



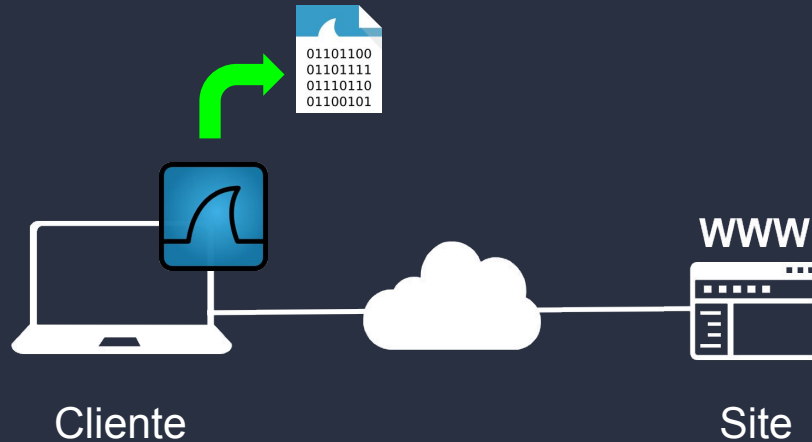
Obtendo uma captura de pacote

- Onde devo fazer a captura de pacote?



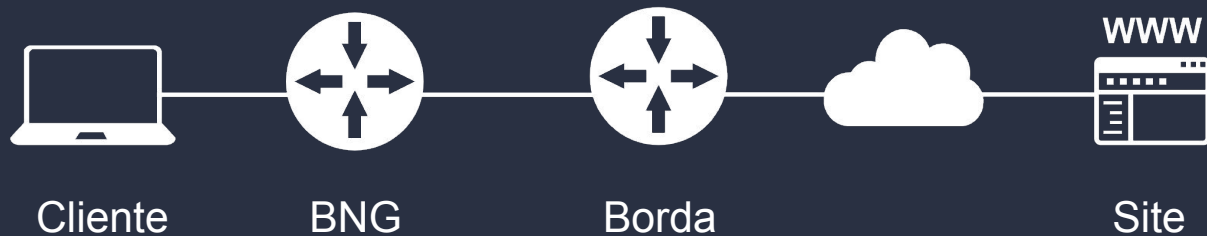
Obtendo uma captura de pacote

- Onde devo fazer a captura de pacote?



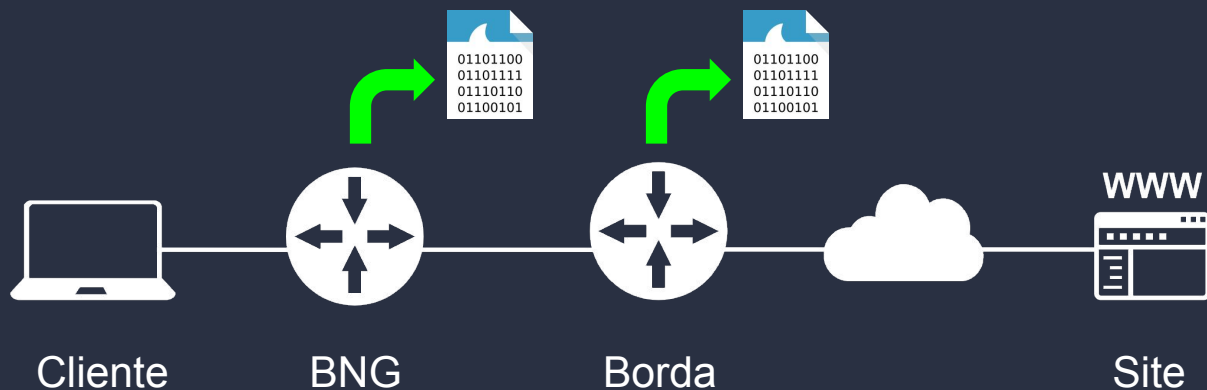
Obtendo uma captura de pacote

- Onde devo fazer a captura de pacote?



Obtendo uma captura de pacote

- Onde devo fazer a captura de pacote?



Obtendo uma captura de pacote

- Como fazer a captura de pacotes?



Obtendo uma captura de pacote

- Como fazer a captura de pacotes?

Roteadores Huawei:

```
# capture-packet forwarding interface 100GE0/1/0.23 packet-num 1000 file captura.pcap
```

Roteadores Cisco:

```
# monitor capture cap01 interface g0/0/1 both match any  
# monitor capture cap01 export location flash:/captura.pcap
```

Roteadores Juniper:

```
# monitor traffic interface ae0 no-resolve filter <filtro> write-file captura.pcap
```

Roteadores Mikrotik:

```
https://wiki.brasilpeeringforum.org/w/Como\_capturar\_pacotes\_no\_Mikrotik
```

Filtragem de Pacotes



Filtragem de Pacotes

Capturing from wlo1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
599	36.641658124	192.168.0.15	187.123.29.54	DNS	82	Standard query 0x4e2f A registro.br OPT
600	36.641728550	192.168.0.15	187.123.29.54	DNS	82	Standard query 0x8b53 AAAA registro.br OPT
601	36.667822545	187.123.29.54	192.168.0.15	DNS	110	Standard query response 0x8b53 AAAA registro.br AAAA 2001:12f...
602	36.723532628	187.123.29.54	192.168.0.15	DNS	98	Standard query response 0x4e2f A registro.br A 200.160.2.3 OPT
603	36.724748418	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=1/256, ttl=64 (reply in 6...
604	36.776988002	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=1/256, ttl=243 (request i...
605	36.777735463	192.168.0.15	187.123.29.54	DNS	95	Standard query 0x983f PTR 3.2.160.200.in-addr.arpa OPT
606	37.139369967	187.123.29.54	192.168.0.15	DNS	120	Standard query response 0x983f PTR 3.2.160.200.in-addr.arpa P...
607	37.728402680	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=2/512, ttl=64 (reply in 6...
608	37.780383009	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=2/512, ttl=243 (request i...
609	38.572478335	142.251.129.78	192.168.0.15	UDP	79	443 → 32867 Len=37
610	38.584561262	192.168.0.15	142.251.129.78	UDP	76	32867 → 443 Len=34
611	38.732128438	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=3/768, ttl=64 (reply in 6...
612	38.783687671	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=3/768, ttl=243 (request i...
613	39.738172262	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=4/1024, ttl=64 (reply in ...
614	39.790955314	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=4/1024, ttl=243 (request ...
615	40.504718400	192.168.0.15	31.13.90.60	TLSv1.2	136	Application Data
616	40.549809234	31.13.90.60	192.168.0.15	TCP	66	443 → 57156 [ACK] Seq=143 Ack=212 Win=297 Len=0 TSval=2164521...

▶ Frame 602: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0

▶ Ethernet II, Src: MS-NLB-PhysServer-16:18:6c:1e:8c (02:10:18:6c:1e:8c), Dst: IntelCor_5d:6d:94 (5c:cd:5b:5d:6d:94)

▶ Internet Protocol Version 4, Src: 187.123.29.54, Dst: 192.168.0.15

▶ User Datagram Protocol, Src Port: 53, Dst Port: 38577

▼ Domain Name System (response)

- Transaction ID: 0x4e2f
- Flags: 0x8180 Standard query response, No error
- Questions: 1
- Answer RRs: 1
- Authority RRs: 0
- Additional RRs: 1
- Queries
- Answers
- Additional records

```
0000  5c cd 5b 5d 6d 94 02 10 18 6c 1e 8c 08 00 45 00  \.[]m...l...E
0010  00 54 2c b1 00 00 fb 11 f9 7e bb 7b 1d 36 c0 a8  ,T...{6...
0020  00 0f 00 35 96 b1 00 40 22 1d 4e 2f 81 80 00 01  ...5...@ "N/...
0030  00 01 00 00 00 01 08 72 65 67 69 73 74 72 6f 02  ...r registro
0040  62 72 00 00 01 00 01 c0 0c 00 01 00 01 00 02 a3  br
0050  00 00 04 c8 a0 02 03 00 00 29 04 c4 00 00 00 00  (.....)....
0060  00 00
```



Filtragem de Pacotes

Capturing from wlo1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
599	36.641658124	192.168.0.15	187.123.29.54	DNS	82	Standard query 0x4e2f A registro.br OPT
600	36.641728550	192.168.0.15	187.123.29.54	DNS	82	Standard query 0x8b53 AAAA registro.br OPT
601	36.667822545	187.123.29.54	192.168.0.15	DNS	110	Standard query response 0x8b53 AAAA registro.br AAAA 2001:12f...
602	36.723532628	187.123.29.54	192.168.0.15	DNS	98	Standard query response 0x4e2f A registro.br A 200.160.2.3 OPT
603	36.724748418	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=1/256, ttl=64 (reply in 6...
604	36.776988002	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=1/256, ttl=243 (request i...
605	36.777735463	192.168.0.15	187.123.29.54	DNS	95	Standard query 0x983f PTR 3.2.160.200.in-addr.arpa OPT
606	37.139369967	187.123.29.54	192.168.0.15	DNS	120	Standard query response 0x983f PTR 3.2.160.200.in-addr.arpa P...
607	37.728402680	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=2/512, ttl=64 (reply in 6...
608	37.780383009	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=2/512, ttl=243 (request i...
609	38.572478335	142.251.129.78	192.168.0.15	UDP	79	443 - 32867 Len=37
610	38.584561262	192.168.0.15	142.251.129.78	UDP	76	32867 - 443 Len=34
611	38.732128438	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=3/768, ttl=64 (reply in 6...
612	38.783687671	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=3/768, ttl=243 (request i...
613	39.738172262	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=4/1024, ttl=64 (reply in ...
614	39.790955314	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=4/1024, ttl=243 (request ...
615	40.504718408	192.168.0.15	31.13.90.60	TLSv1.2	136	Application Data
616	40.549809234	31.13.90.60	192.168.0.15	TCP	66	443 - 57156 [ACK] Seq=143 Ack=212 Win=297 Len=0 TSval=2164521...
617	40.709400000	24.32.0.0.0.0	192.168.0.15	TLSv1.2	120	Application Data
▶ Frame 602: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0						
▶ Ethernet II, Src: MS-NLB-PhysServer-16_18:6c:1e:8c (02:10:18:6c:1e:8c), Dst: IntelCor_5d:6d:94 (5c:cd:5b:5d:6d:94)						
▶ Internet Protocol Version 4, Src: 187.123.29.54, Dst: 192.168.0.15						
▶ User Datagram Protocol, Src Port: 53, Dst Port: 38577						
▶ Domain Name System (response)						
Transaction ID: 0x4e2f						
▶ Flags: 0x8180 Standard query response, No error						
Questions: 1						
Answer RRs: 1						
Authority RRs: 0						
Additional RRs: 1						
▶ Queries						
▶ Answers						
▶ Additional records						
(Request ID: 501)						
0000	5c cd 5b 5d 6d 94 02 10	18 6c 1e 8c 08 00 45 00	N[...]m...			
0010	00 54 2c b1 00 00 fb 11	f9 7e bb 7b 1d 36 c0 a8	T... (6...			
0020	00 0f 00 35 96 b1 00 40	22 1d 4e 2f 81 80 00 01	5... N/...			
0030	00 01 00 00 00 01 08 72	65 67 69 73 74 72 6f 02	... registro...			
0040	62 72 00 00 01 00 01 c0	0c 00 01 00 01 00 02 a3	br...			
0050	00 00 04 c8 a0 02 03 00	00 29 04 c4 00 00 00 00	...			
0060	00 00					



Filtragem de Pacotes

Capturing from wlo1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
599	36.641658124	192.168.0.15	187.123.29.54	DNS	82	Standard query 0x4e2f A registro.br OPT
600	36.641728550	192.168.0.15	187.123.29.54	DNS	82	Standard query 0x8b53 AAAA registro.br OPT
601	36.667822545	187.123.29.54	192.168.0.15	DNS	110	Standard query response 0x8b53 AAAA registro.br AAAA 2001:12f...
602	36.723532628	187.123.29.54	192.168.0.15	DNS	98	Standard query response 0x4e2f A registro.br A 200.160.2.3 OPT

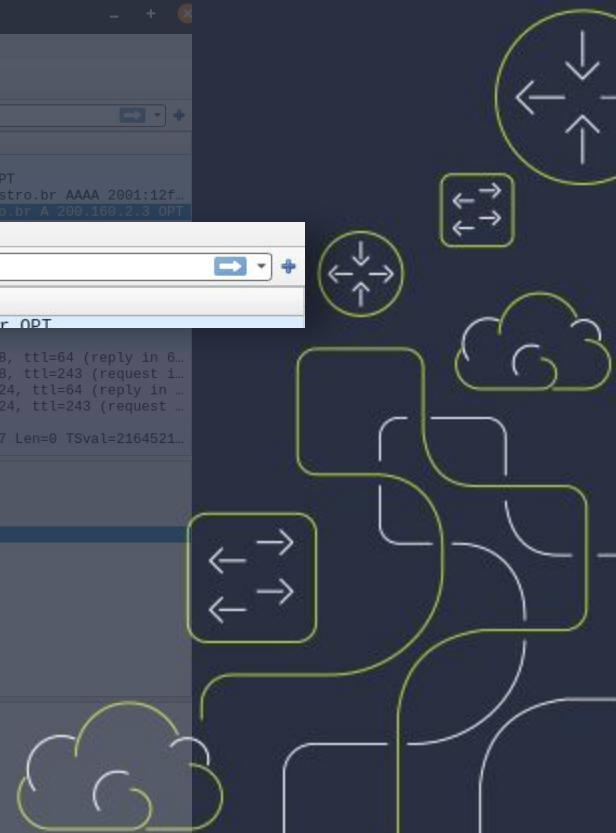
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
599	36.641658124	192.168.0.15	187.123.29.54	DNS	82	Standard query 0x4e2f A registro.br OPT
610	38.584561262	192.168.0.15	142.251.129.78	UDP	76	32867 → 443 Len=34
611	38.732128438	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=3/768, ttl=64 (reply in 6...
612	38.783687671	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=3/768, ttl=243 (request in ...
613	39.738172262	192.168.0.15	200.160.2.3	ICMP	98	Echo (ping) request id=0x0023, seq=4/1024, ttl=64 (reply in ...
614	39.790955314	200.160.2.3	192.168.0.15	ICMP	98	Echo (ping) reply id=0x0023, seq=4/1024, ttl=243 (request ...
615	40.504718409	192.168.0.15	31.13.90.69	TLSv1.2	136	Application Data
616	40.549809234	31.13.90.69	192.168.0.15	TCP	66	443 → 57156 [ACK] Seq=143 Ack=212 Win=297 Len=0 TSval=2164521...

Frame 602: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0

- Ethernet II, Src: MS-NLB-PhysServer-16 18:6c:1e:8c (02:10:18:6c:1e:8c), Dst: IntelCor_5d:6d:94 (5c:cd:5b:5d:6d:94)
- Internet Protocol Version 4, Src: 187.123.29.54, Dst: 192.168.0.15
- User Datagram Protocol, Src Port: 53, Dst Port: 38577
- Domain Name System (response)
 - Transaction ID: 0x4e2f
 - Flags: 0x8180 Standard query response, No error
 - Questions: 1
 - Answer RRs: 1
 - Authority RRs: 0
 - Additional RRs: 1
 - Queries
 - Answers
 - Additional records

0000 5c cd 5b 5d 6d 94 02 10 18 6c 1e 8c 08 00 48 00 N[...]m...U...
0010 00 54 2c b1 00 00 fb 11 f9 7e bb 7b 1d 36 c0 a8 -T... (6...
0020 00 0f 00 35 96 b1 00 40 22 1d 4e 2f 81 80 00 01 -5...@ "N/...
0030 00 01 00 00 00 01 08 72 65 67 69 73 74 72 6f 02 -...r registro...
0040 62 72 00 00 01 00 01 c0 0c 00 01 00 01 00 02 a3 br...
0050 00 00 04 c8 a0 02 03 00 00 29 04 c4 00 00 00 00 ...
0060 00 00



Filtragem de Pacotes

- **Operadores Lógicos**

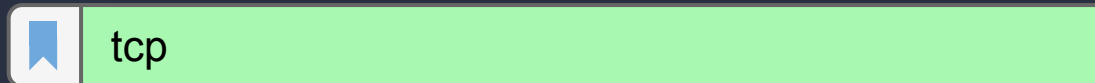
- **and** ou **&&** : Operador "E"
- **or** ou **||** : Operador "OU"
- **not** ou **!** : Negação
- **eq** ou **==** : Igualdade
- **ne** ou **!=** : Desigualdade
- **gt** ou **>** : Maior que
- **lt** ou **<** : Menor que
- **ge** ou **>=** : Maior ou igual
- **le** ou **<=** : Menor ou igual



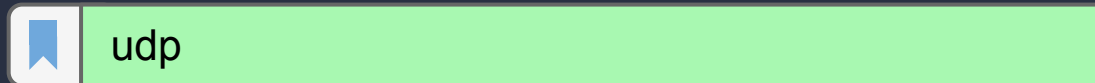
Filtragem de Pacotes

- **Filtrando protocolos**

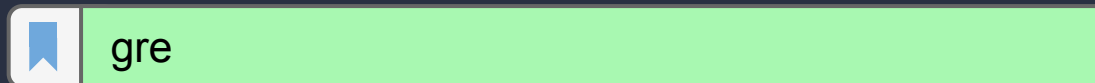
- **TCP**



- **UDP**




- **GRE**




Filtragem de Pacotes

- **Filtrando por IP de Origem e Destino**


- **Origem**

 ip.src == 192.168.1.1

- **Destino**

 ip.dst != 10.214.0.3

- **Origem ou Destino**


 ip.addr == 10.214.0.3




Filtragem de Pacotes

- **Filtrando por Portas TCP/UDP**

- **Porta TCP de origem ou destino**

 tcp.port == 25

- **Porta TCP de destino**

 tcp.dstport != 443

- **Porta TCP de origem**

 tcp.srcport >= 1024



Filtragem de Pacotes

- **Filtrando por Portas TCP/UDP**

- **Porta UDP de origem ou destino**



```
udp.port == 53
```

- **Porta UDP de destino**



```
udp.dstport <= 2000
```

- **Porta UDP de origem**



```
udp.srcport != 389
```



Filtragem de Pacotes

- Filtrando por string no payload
 - Contém a string "upnp" no payload



frame contains "upnp"



Filtragem de Pacotes

- Filtrando por tamanho do pacote
 - Tamanho total do pacote (bytes)
 - Tamanho do cabeçalho IP (bytes)



```
frame.len == 75
```



```
ip.len > 1024
```



Filtragem de Pacotes

- Combinações de filtros



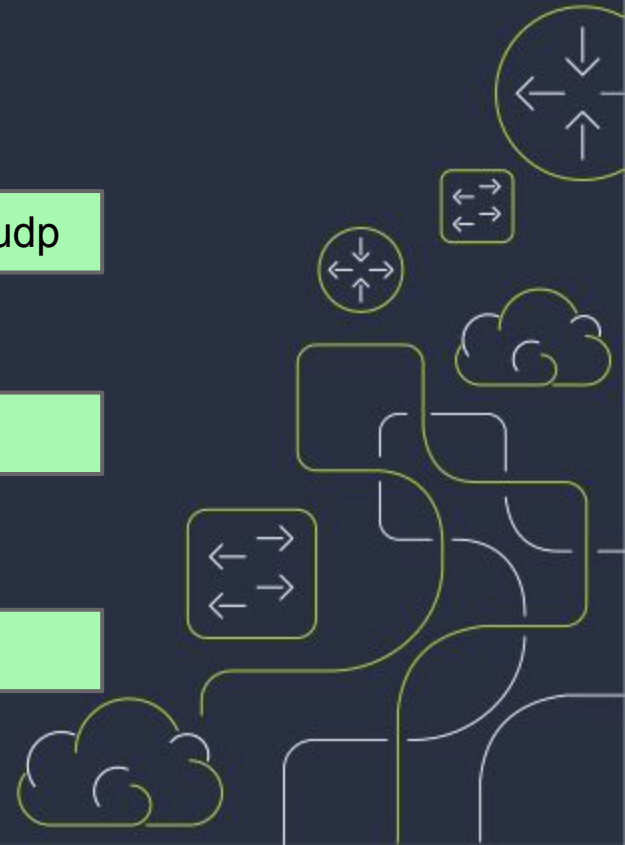
```
(ip.src == 192.168.1.1 && ip.dst == 10.214.0.3) && udp
```



```
(udp.srcport == 53) && ip.len == 61
```



```
(udp.srcport == 53) && ip.len >= 78
```



Filtragem de Pacotes

- Combinações de filtros



```
!(ip.src == 192.168.1.1 && ip.dst == 10.214.0.3)
```



```
udp.port >= 1024 && udp.port <= 2048
```



Filtragem de Pacotes

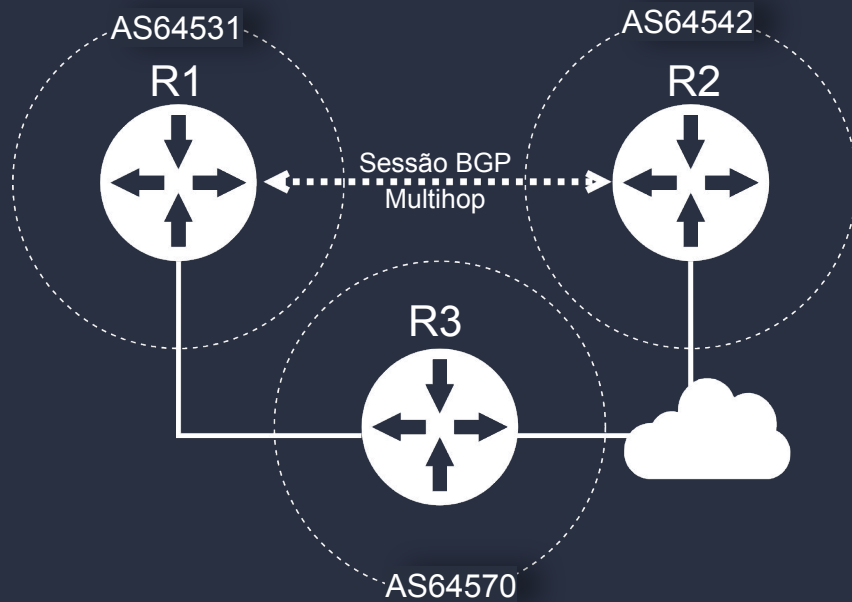
- Documentação sobre filtros



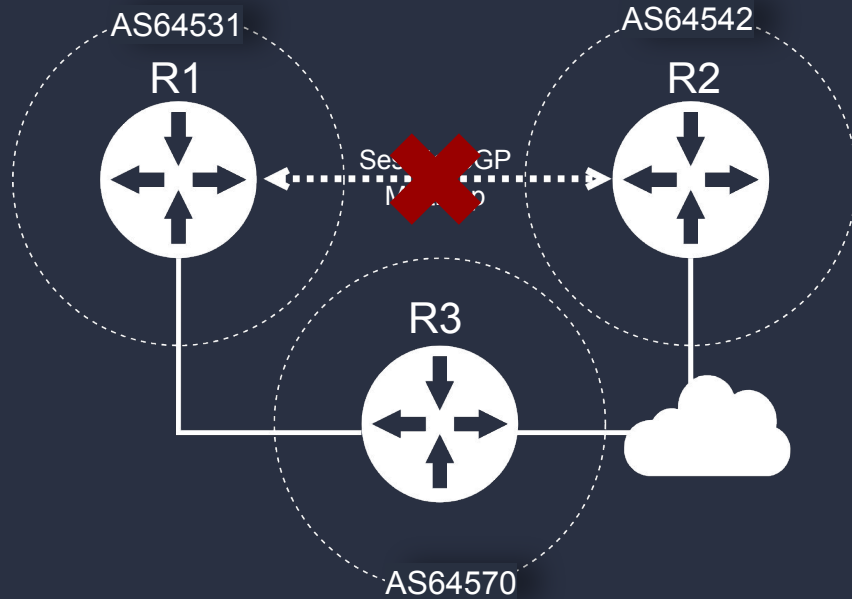
Troubleshooting com Wireshark



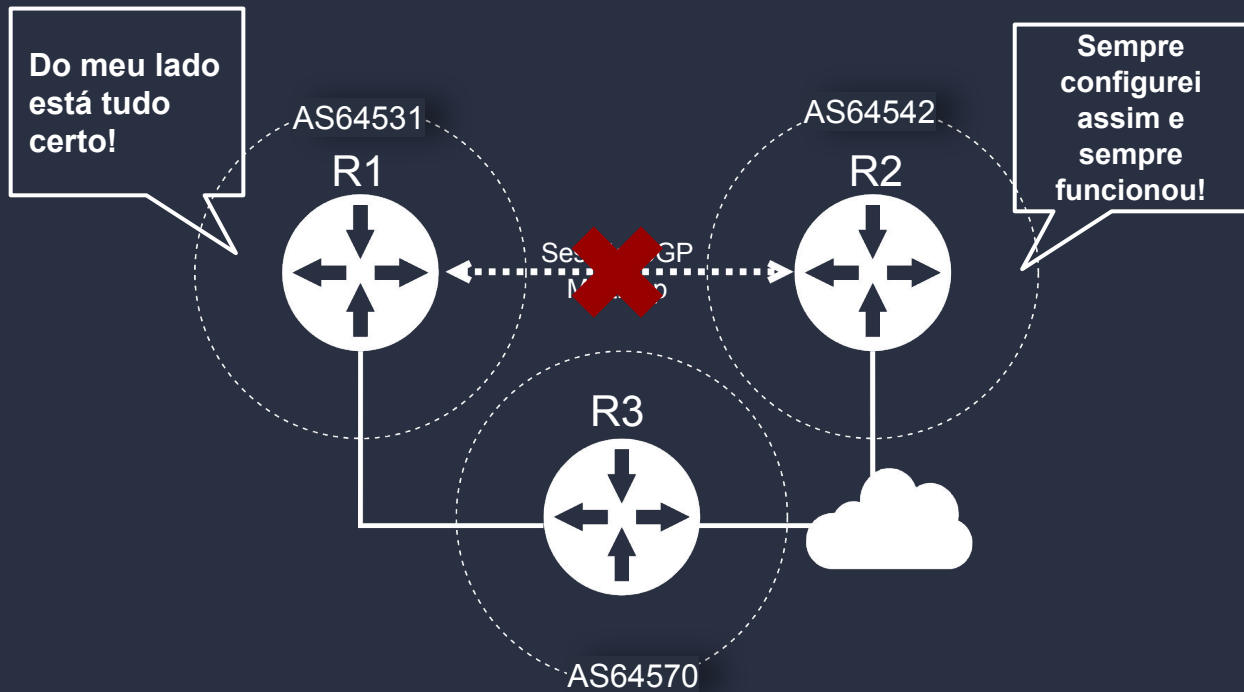
Troubleshooting com Wireshark



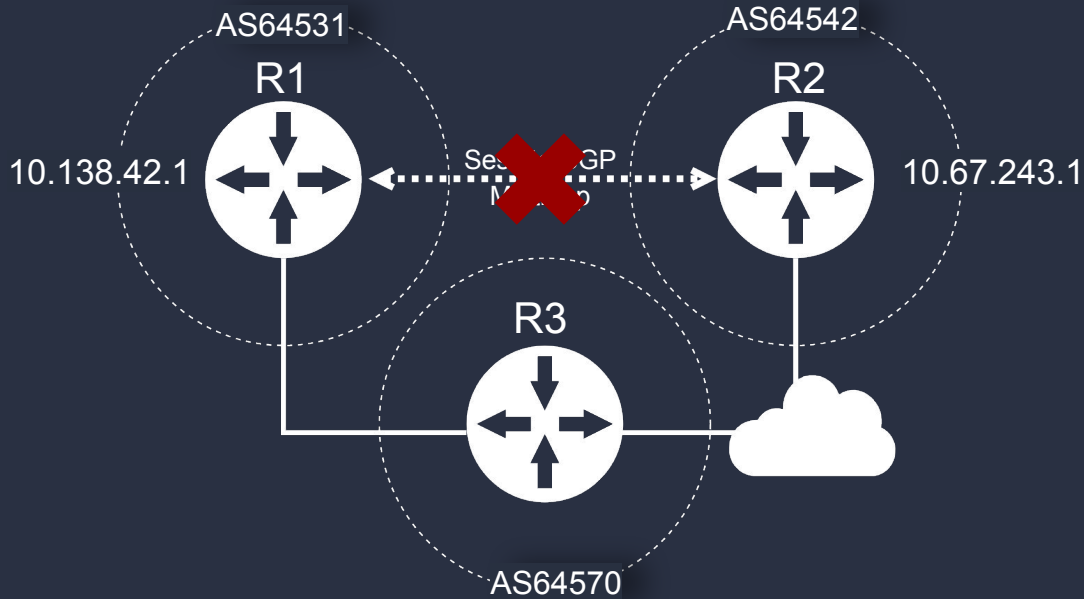
Troubleshooting com Wireshark



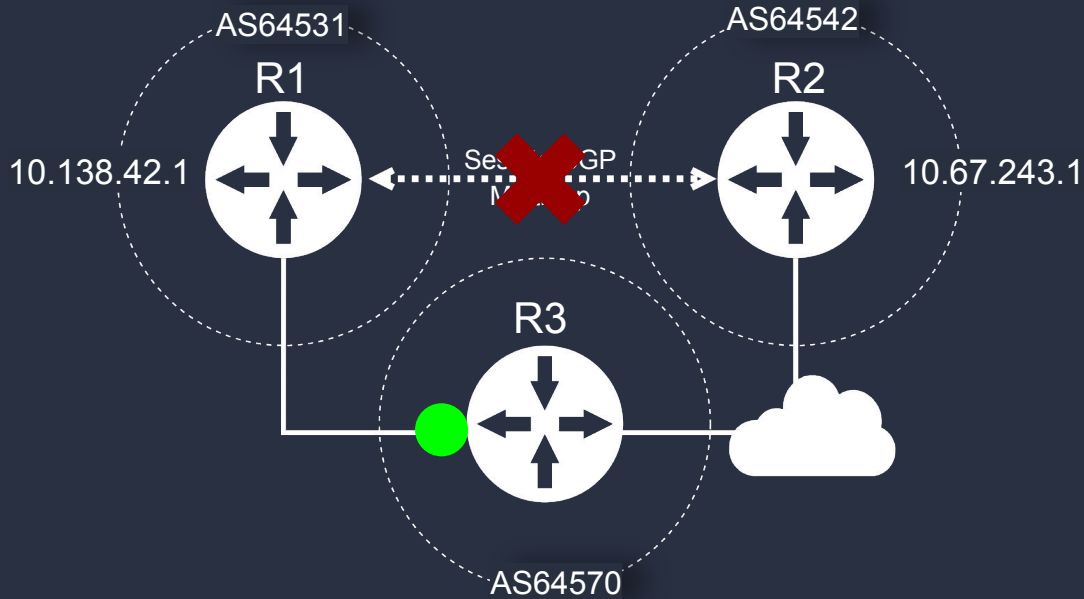
Troubleshooting com Wireshark



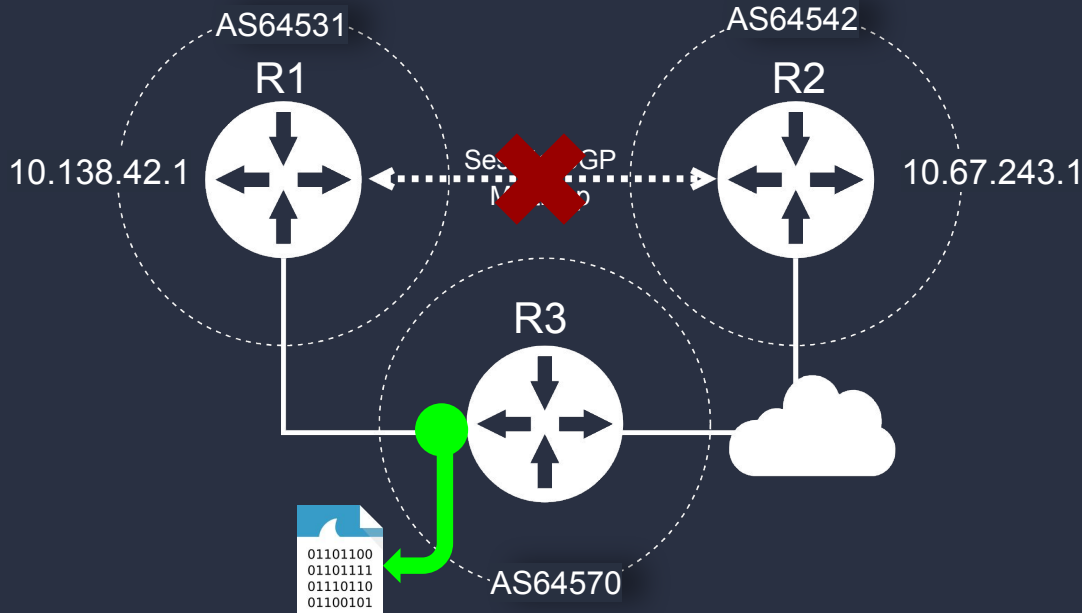
Troubleshooting com Wireshark



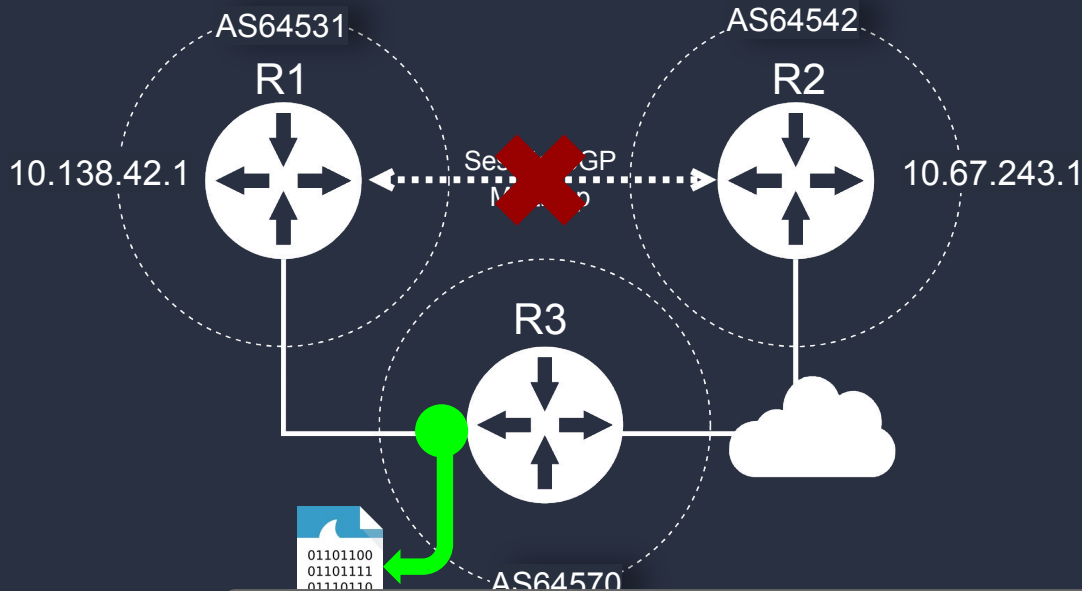
Troubleshooting com Wireshark



Troubleshooting com Wireshark



Troubleshooting com Wireshark



```
(ip.addr == 10.138.42.1 || ip.addr == 10.67.243.1) && tcp.port == 179
```



Troubleshooting com Wireshark



(ip.addr == 10.138.42.1 || ip.addr == 10.67.243.1) && tcp.port == 179

No.	Time	Source	Destination	Protocol	Length	Info
159	26.015815	198.18.10.1	10.67.243.1	TCP	66	54393 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5014534 TSecr=51...
160	26.016859	10.67.243.1	198.18.10.1	TCP	54	179 → 54393 [RST] Seq=2 Win=0 Len=0
269	46.017921	198.18.10.1	10.67.243.1	TCP	74	54394 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535...
270	46.019257	10.67.243.1	198.18.10.1	TCP	74	179 → 54394 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TS...
271	46.020519	198.18.10.1	10.67.243.1	TCP	66	54394 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5016535 TSecr=5153062
272	46.021191	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
273	46.021727	10.67.243.1	198.18.10.1	TCP	66	179 → 54394 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5153062 TSecr=501...
274	46.022362	10.67.243.1	198.18.10.1	TCP	54	179 → 54394 [RST] Seq=1 Win=0 Len=0
275	46.023079	198.18.10.1	10.67.243.1	TCP	66	54394 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5016535 TSecr=51...
276	46.024205	10.67.243.1	198.18.10.1	TCP	54	179 → 54394 [RST] Seq=2 Win=0 Len=0
375	66.025032	198.18.10.1	10.67.243.1	TCP	74	54395 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5018535...
376	66.026507	10.67.243.1	198.18.10.1	TCP	74	179 → 54395 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TS...
377	66.027841	198.18.10.1	10.67.243.1	TCP	66	54395 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5018536 TSecr=5155062
378	66.028696	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
379	66.029167	10.67.243.1	198.18.10.1	TCP	66	179 → 54395 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5155063 TSecr=501...
380	66.030029	10.67.243.1	198.18.10.1	TCP	54	179 → 54395 [RST] Seq=1 Win=0 Len=0
381	66.030437	198.18.10.1	10.67.243.1	TCP	66	54395 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5018536 TSecr=51...
382	66.031703	10.67.243.1	198.18.10.1	TCP	54	179 → 54395 [RST] Seq=2 Win=0 Len=0
495	86.036892	198.18.10.1	10.67.243.1	TCP	74	54396 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5020536...
496	86.038169	10.67.243.1	198.18.10.1	TCP	74	179 → 54396 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TS...
497	86.039485	198.18.10.1	10.67.243.1	TCP	66	54396 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5020537 TSecr=5157063
498	86.040168	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
499	86.040674	10.67.243.1	198.18.10.1	TCP	66	179 → 54396 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5157064 TSecr=502...

▶ Frame 498: 111 bytes on wire (888 bits), 111 bytes captured (888 bits)
▶ Ethernet II, Src: VMware_bc:e3:89 (00:0c:29:bc:e3:89), Dst: VMware_70:cc:53 (00:0c:29:70:cc:53)
▶ Internet Protocol Version 4, Src: 198.18.10.1, Dst: 10.67.243.1
▶ Transmission Control Protocol, Src Port: 54396, Dst Port: 179, Seq: 1, Ack: 1, Len: 45
▶ Border Gateway Protocol - OPEN Message

Troubleshooting com Wireshark



(ip.addr == 10.138.42.1 || ip.addr == 10.67.243.1) && tcp.port == 179

No.	Time	Source	Destination	Protocol	Length	Info
159	26.015815	198.18.10.1	10.67.243.1	TCP	66	54393 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5014534 TSecr=5014534
160	26.016859	10.67.243.1	198.18.10.1	TCP	54	179 → 54393 [RST] Seq=2 Win=0 Len=0
269	46.017921	198.18.10.1	10.67.243.1	TCP	74	54394 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=5016535
270	46.019257	10.67.243.1	198.18.10.1	TCP	74	179 → 54394 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=5016535
271	46.020519	198.18.10.1	10.67.243.1	TCP	66	54394 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5016535 TSecr=5153062
272	46.021191	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
273	46.021727	10.67.243.1	198.18.10.1	TCP	66	179 → 54394 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5153062 TSecr=5016535
274	46.022362	10.67.243.1	198.18.10.1	TCP	54	179 → 54394 [RST] Seq=1 Win=0 Len=0
275	46.023079	198.18.10.1	10.67.243.1	TCP	66	54394 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5016535 TSecr=5153062
276	46.024205	10.67.243.1	198.18.10.1	TCP	54	179 → 54394 [RST] Seq=2 Win=0 Len=0
375	66.025032	198.18.10.1	10.67.243.1	TCP	74	54395 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5018535 TSecr=5018535
376	66.026507	10.67.243.1	198.18.10.1	TCP	74	179 → 54395 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5018535 TSecr=5018535
377	66.027841	198.18.10.1	10.67.243.1	TCP	66	54395 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5018536 TSecr=5155062
378	66.028696	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
379	66.029167	10.67.243.1	198.18.10.1	TCP	66	179 → 54395 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5155063 TSecr=5018536
380	66.030029	10.67.243.1	198.18.10.1	TCP	54	179 → 54395 [RST] Seq=1 Win=0 Len=0
381	66.030437	198.18.10.1	10.67.243.1	TCP	66	54395 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5018536 TSecr=5155062
382	66.031703	10.67.243.1	198.18.10.1	TCP	54	179 → 54395 [RST] Seq=2 Win=0 Len=0
495	86.036892	198.18.10.1	10.67.243.1	TCP	74	54396 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5020536 TSecr=5020536
496	86.038169	10.67.243.1	198.18.10.1	TCP	74	179 → 54396 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5020536 TSecr=5020536
497	86.039485	198.18.10.1	10.67.243.1	TCP	66	54396 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5020537 TSecr=5157063
498	86.040168	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
499	86.040674	10.67.243.1	198.18.10.1	TCP	66	179 → 54396 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5157064 TSecr=5020537

▶ Frame 498: 111 bytes on wire (888 bits), 111 bytes captured (888 bits)
▶ Ethernet II, Src: VMware_bc:e3:89 (00:0c:29:bc:e3:89), Dst: VMware_70:cc:53 (00:0c:29:70:cc:53)
▶ Internet Protocol Version 4, Src: 198.18.10.1, Dst: 10.67.243.1
▶ Transmission Control Protocol, Src Port: 54396, Dst Port: 179, Seq: 1, Ack: 1, Len: 45
▶ Border Gateway Protocol - OPEN Message

Troubleshooting com Wireshark



(ip.addr == 10.138.42.1 || ip.addr == 10.67.243.1) && tcp.port == 179

No.	Time	Source	Destination	Protocol	Length	Info
159	26.015815	198.18.10.1	10.67.243.1	TCP	66	54393 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5014534 TSecr=51...
160	26.016859	10.67.243.1	198.18.10.1	TCP	54	179 → 54393 [RST] Seq=2 Win=0 Len=0
269	46.017921	198.18.10.1	10.67.243.1	TCP	74	54394 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535...
270	46.019257	10.67.243.1	198.18.10.1	TCP	74	179 → 54394 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TS...
271	46.020519	198.18.10.1	10.67.243.1	TCP	66	54394 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5016535 TSecr=5153062
272	46.021191	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
273	46.021727	10.67.243.1	198.18.10.1	TCP	66	179 → 54394 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5153062 TSecr=501...
274	46.022362	10.67.243.1	198.18.10.1	TCP	54	179 → 54394 [RST] Seq=1 Win=0 Len=0
275	46.023079	198.18.10.1	10.67.243.1	TCP	66	54394 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5016535 TSecr=51...
276	46.024205	10.67.243.1	198.18.10.1	TCP	54	179 → 54394 [RST] Seq=2 Win=0 Len=0
375	66.025032	198.18.10.1	10.67.243.1	TCP	74	54395 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5018535...
376	66.026507	10.67.243.1	198.18.10.1	TCP	74	179 → 54395 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TS...
377	66.027841	198.18.10.1	10.67.243.1	TCP	66	54395 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5018536 TSecr=5155062
378	66.028696	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
379	66.029167	10.67.243.1	198.18.10.1	TCP	66	179 → 54395 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5155063 TSecr=501...
380	66.030029	10.67.243.1	198.18.10.1	TCP	54	179 → 54395 [RST] Seq=1 Win=0 Len=0
381	66.030437	198.18.10.1	10.67.243.1	TCP	66	54395 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5018536 TSecr=51...
382	66.031703	10.67.243.1	198.18.10.1	TCP	54	179 → 54395 [RST] Seq=2 Win=0 Len=0
495	86.036892	198.18.10.1	10.67.243.1	TCP	74	54396 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5020536...
496	86.038169	10.67.243.1	198.18.10.1	TCP	74	179 → 54396 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TS...
497	86.039485	198.18.10.1	10.67.243.1	TCP	66	54396 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5020537 TSecr=5157063
498	86.040168	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
499	86.040674	10.67.243.1	198.18.10.1	TCP	66	179 → 54396 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5157064 TSecr=502...

▶ Frame 498: 111 bytes on wire (888 bits), 111 bytes captured (888 bits)
▶ Ethernet II, Src: VMware_bc:e3:89 (00:0c:29:bc:e3:89), Dst: VMware_70:cc:53 (00:0c:29:70:cc:53)
▶ Internet Protocol Version 4, Src: 198.18.10.1, Dst: 10.67.243.1
▶ Transmission Control Protocol, Src Port: 54396, Dst Port: 179, Seq: 1, Ack: 1, Len: 45
▶ Border Gateway Protocol - OPEN Message

Troubleshooting com Wireshark



(ip.addr == 10.138.42.1 || ip.addr == 10.67.243.1) && tcp.port == 179

No.	Time	Source	Destination	Protocol	Length	Info
159	26.015815	198.18.10.1	10.67.243.1	TCP	66	54393 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5014534 TSecr=5153062
160	26.016859	10.67.243.1	198.18.10.1	TCP	54	179 → 54393 [RST] Seq=2 Win=0 Len=0
269	46.017921	198.18.10.1	10.67.243.1	TCP	74	54394 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=5153062
270	46.019257	10.67.243.1	198.18.10.1	TCP	74	179 → 54394 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=5153062
271	46.020519	198.18.10.1	10.67.243.1	TCP	66	54394 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5016535 TSecr=5153062
272	46.021191	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
273	46.021727	10.67.243.1	198.18.10.1	TCP	66	179 → 54394 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5153062 TSecr=5014534
274	46.022362	10.67.243.1	198.18.10.1	TCP	54	179 → 54394 [RST] Seq=1 Win=0 Len=0
275	46.023079	198.18.10.1	10.67.243.1	TCP	66	54394 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5016535 TSecr=5153062
276	46.024205	10.67.243.1	198.18.10.1	TCP	54	179 → 54394 [RST] Seq=2 Win=0 Len=0
375	66.025032	198.18.10.1	10.67.243.1	TCP	74	54395 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5018535 TSecr=5155062
376	66.026507	10.67.243.1	198.18.10.1	TCP	74	179 → 54395 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5018535 TSecr=5155062
377	66.027841	198.18.10.1	10.67.243.1	TCP	66	54395 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5018536 TSecr=5155062
378	66.028696	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
379	66.029167	10.67.243.1	198.18.10.1	TCP	66	179 → 54395 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5155063 TSecr=5014534
380	66.030029	10.67.243.1	198.18.10.1	TCP	54	179 → 54395 [RST] Seq=1 Win=0 Len=0
381	66.030437	198.18.10.1	10.67.243.1	TCP	66	54395 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5018536 TSecr=5155062
382	66.031703	10.67.243.1	198.18.10.1	TCP	54	179 → 54395 [RST] Seq=2 Win=0 Len=0
495	86.036892	198.18.10.1	10.67.243.1	TCP	74	54396 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5020536 TSecr=5157064
496	86.038169	10.67.243.1	198.18.10.1	TCP	74	179 → 54396 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5020536 TSecr=5157064
497	86.039485	198.18.10.1	10.67.243.1	TCP	66	54396 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5020537 TSecr=5157064
498	86.040168	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
499	86.040674	10.67.243.1	198.18.10.1	TCP	66	179 → 54396 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5157064 TSecr=5020536

Frame 498: 111 bytes on wire (888 bits), 111 bytes captured (888 bits)
Ethernet II, Src: VMware_bc:e3:89 (00:0c:29:bc:e3:89), Dst: VMware_70:cc:53 (00:0c:29:70:cc:53)
Internet Protocol Version 4, Src: 198.18.10.1, Dst: 10.67.243.1
Transmission Control Protocol, Src Port: 54396, Dst Port: 179, Seq: 1, Ack: 1, Len: 45
Border Gateway Protocol - OPEN Message

Troubleshooting com Wireshark

(ip.addr == 10.138.42.1 || ip.addr == 10.67.243.1) && tcp.port == 179

No.	Time	Source	Destination	Protocol	Length	Info
159	26.015815	198.18.10.1	10.67.243.1	TCP	66	54393 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5014534 TSecr=50153062 Len=0
160	26.015815	10.67.243.1	198.18.10.1	TCP	54	179 → 54393 [ACK] Seq=1 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=50153062 Len=0
269	46.015815	198.18.10.1	10.67.243.1	TCP	74	179 → 54393 [ACK] Seq=1 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=50153062 Len=0
270	46.015815	10.67.243.1	198.18.10.1	TCP	66	54394 → 179 [ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5155063 TSecr=50153062 Len=0
271	46.021727	10.67.243.1	198.18.10.1	TCP	66	179 → 54393 [ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5155063 TSecr=50153062 Len=0
272	46.021727	198.18.10.1	10.67.243.1	TCP	66	54394 → 179 [ACK] Seq=1 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=50153062 Len=0
273	46.021727	10.67.243.1	198.18.10.1	TCP	66	179 → 54393 [ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5155063 TSecr=50153062 Len=0
274	46.022362	10.67.243.1	198.18.10.1	TCP	54	179 → 54393 [ACK] Seq=1 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=50153062 Len=0
275	46.023079	198.18.10.1	10.67.243.1	TCP	66	54394 → 179 [ACK] Seq=1 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=50153062 Len=0
276	46.024205	10.67.243.1	198.18.10.1	TCP	54	179 → 54393 [ACK] Seq=1 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=50153062 Len=0
375	66.025032	198.18.10.1	10.67.243.1	TCP	74	54395 → 179 [ACK] Seq=1 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=50153062 Len=0
376	66.026507	10.67.243.1	198.18.10.1	TCP	74	179 → 54393 [ACK] Seq=1 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=50153062 Len=0
377	66.027841	198.18.10.1	10.67.243.1	TCP	66	54395 → 179 [ACK] Seq=1 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=50153062 Len=0
378	66.028696	198.18.10.1	10.67.243.1	TCP	66	54395 → 179 [ACK] Seq=1 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=50153062 Len=0
379	66.029167	10.67.243.1	198.18.10.1	TCP	66	179 → 54393 [ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5155063 TSecr=50153062 Len=0
380	66.030029	10.67.243.1	198.18.10.1	TCP	54	179 → 54393 [ACK] Seq=1 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=50153062 Len=0
381	66.030437	198.18.10.1	10.67.243.1	TCP	66	54395 → 179 [ACK] Seq=1 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=50153062 Len=0
382	66.031703	10.67.243.1	198.18.10.1	TCP	54	179 → 54393 [ACK] Seq=1 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=50153062 Len=0
495	86.036892	198.18.10.1	10.67.243.1	TCP	74	54396 → 179 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=5020536 TSecr=50153062 Len=0
496	86.038169	10.67.243.1	198.18.10.1	TCP	74	179 → 54396 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=50153062 Len=0
497	86.039485	198.18.10.1	10.67.243.1	TCP	66	54396 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5020537 TSecr=50153062 Len=0
498	86.040168	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
499	86.040674	10.67.243.1	198.18.10.1	TCP	66	179 → 54396 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5157014 TSecr=50153062 Len=0

Source	Destination
198.18.10.1	10.67.243.1
10.67.243.1	198.18.10.1

R1
10.138.42.1
AS64531

R2
10.67.243.1
AS64542

- Frame 498: 111 bytes on wire (888 bits), 111 bytes captured (888 bits)
- Ethernet II, Src: VMware_bc:e3:89 (00:0c:29:bc:e3:89), Dst: VMware_70:cc:53 (00:0c:29:70:cc:53)
- Internet Protocol Version 4, Src: 198.18.10.1, Dst: 10.67.243.1
- Transmission Control Protocol, Src Port: 54396, Dst Port: 179, Seq: 1, Ack: 1, Len: 45
- Border Gateway Protocol - OPEN Message

Troubleshooting com Wireshark



(ip.addr == 10.138.42.1 || ip.addr == 10.67.243.1) && tcp.port == 179

No.	Time	Source	Destination	Protocol	Length	Info
159	26.015815	198.18.10.1	10.67.243.1	TCP	66	54393 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5014534 TSecr=51...
160	26.016859	10.67.243.1	198.18.10.1	TCP	54	179 → 54393 [RST] Seq=2 Win=0 Len=0
269	46.017921	198.18.10.1	10.67.243.1	TCP	74	54394 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535...
270	46.019257	10.67.243.1	198.18.10.1	TCP	74	179 → 54394 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TS...
271	46.020519	198.18.10.1	10.67.243.1	TCP	66	54394 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5016535 TSecr=5153062
272	46.021191	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
273	46.021727	10.67.243.1	198.18.10.1	TCP	66	179 → 54394 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5153062 TSecr=501...
274	46.022362	10.67.243.1	198.18.10.1	TCP	54	179 → 54394 [RST] Seq=1 Win=0 Len=0
275	46.023079	198.18.10.1	10.67.243.1	TCP	66	54394 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5016535 TSecr=51...
276	46.024205	10.67.243.1	198.18.10.1	TCP	54	179 → 54394 [RST] Seq=2 Win=0 Len=0
375	66.025032	198.18.10.1	10.67.243.1	TCP	74	54395 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5018535...
376	66.026507	10.67.243.1	198.18.10.1	TCP	74	179 → 54395 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TS...
377	66.027841	198.18.10.1	10.67.243.1	TCP	66	54395 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5018536 TSecr=5155062
378	66.028696	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
379	66.029167	10.67.243.1	198.18.10.1	TCP	66	179 → 54395 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5155063 TSecr=501...
380	66.030029	10.67.243.1	198.18.10.1	TCP	54	179 → 54395 [RST] Seq=1 Win=0 Len=0
381	66.030437	198.18.10.1	10.67.243.1	TCP	66	54395 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5018536 TSecr=51...
382	66.031703	10.67.243.1	198.18.10.1	TCP	54	179 → 54395 [RST] Seq=2 Win=0 Len=0
495	86.036892	198.18.10.1	10.67.243.1	TCP	74	54396 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5020536...
496	86.038169	10.67.243.1	198.18.10.1	TCP	74	179 → 54396 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TS...
497	86.039485	198.18.10.1	10.67.243.1	TCP	66	54396 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5020537 TSecr=5157063
498	86.040168	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
499	86.040674	10.67.243.1	198.18.10.1	TCP	66	179 → 54396 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5157064 TSecr=502...

▶ Frame 498: 111 bytes on wire (888 bits), 111 bytes captured (888 bits)
▶ Ethernet II, Src: VMware_bc:e3:89 (00:0c:29:bc:e3:89), Dst: VMware_70:cc:53 (00:0c:29:70:cc:53)
▶ Internet Protocol Version 4, Src: 198.18.10.1, Dst: 10.67.243.1
▶ Transmission Control Protocol, Src Port: 54396, Dst Port: 179, Seq: 1, Ack: 1, Len: 45
▶ Border Gateway Protocol - OPEN Message

Troubleshooting com Wireshark



(ip.addr == 10.138.42.1 || ip.addr == 10.67.243.1) && tcp.port == 179

No.	Time	Source	Destination	Protocol	Length	Info
159	26.015815	198.18.10.1	10.67.243.1	TCP	66	54393 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5014534 TSecr=5155062
160	26.016859	10.67.243.1	198.18.10.1	TCP	54	179 → 54393 [RST] Seq=2 Win=0 Len=0
269	46.017921	198.18.10.1	10.67.243.1	TCP	74	54394 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=5155062
270	46.019257	10.67.243.1	198.18.10.1	TCP	74	179 → 54394 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=5155062
271	46.020519	198.18.10.1	10.67.243.1	TCP	66	54394 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5016535 TSecr=5153062
272	46.021191	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
273	46.021727	10.67.243.1	198.18.10.1	TCP	66	179 → 54394 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5153062 TSecr=5016535
274	46.022362	10.67.243.1	198.18.10.1	TCP	54	179 → 54394 [RST] Seq=1 Win=0 Len=0
275	46.023079	198.18.10.1	10.67.243.1	TCP	66	54394 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5016535 TSecr=5155062
276	46.024205	10.67.243.1	198.18.10.1	TCP	54	179 → 54394 [RST] Seq=2 Win=0 Len=0
375	66.025032	198.18.10.1	10.67.243.1	TCP	74	54395 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5018535 TSecr=5155062
376	66.026507	10.67.243.1	198.18.10.1	TCP	74	179 → 54395 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5018535 TSecr=5155062
377	66.027841	198.18.10.1	10.67.243.1	TCP	66	54395 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5018535 TSecr=5155062
378	66.028696	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
379	66.029167	10.67.243.1	198.18.10.1	TCP	66	179 → 54395 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5155063 TSecr=5018535
380	66.030029	10.67.243.1	198.18.10.1	TCP	54	179 → 54395 [RST] Seq=1 Win=0 Len=0
381	66.030437	198.18.10.1	10.67.243.1	TCP	66	54395 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5018536 TSecr=5155062
382	66.031703	10.67.243.1	198.18.10.1	TCP	54	179 → 54395 [RST] Seq=2 Win=0 Len=0
495	86.036892	198.18.10.1	10.67.243.1	TCP	74	54396 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5020536 TSecr=5155062
496	86.038169	10.67.243.1	198.18.10.1	TCP	74	179 → 54396 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5020536 TSecr=5155062
497	86.039485	198.18.10.1	10.67.243.1	TCP	66	54396 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5020537 TSecr=5157063
498	86.040168	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
499	86.040674	10.67.243.1	198.18.10.1	TCP	66	179 → 54396 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5157064 TSecr=5020536

▶ Frame 498: 111 bytes on wire (888 bits), 111 bytes captured (888 bits)
▶ Ethernet II, Src: VMware_bc:e3:89 (00:0c:29:bc:e3:89), Dst: VMware_70:cc:53 (00:0c:29:70:cc:53)
▶ Internet Protocol Version 4, Src: 198.18.10.1, Dst: 10.67.243.1
▶ Transmission Control Protocol, Src Port: 54396, Dst Port: 179, Seq: 1, Ack: 1, Len: 45
▶ Border Gateway Protocol - OPEN Message

Troubleshooting com Wireshark



(ip.addr == 10.138.42.1 || ip.addr == 10.67.243.1) && tcp.port == 179

No.	Time	Source	Destination	Protocol	Length	Info
159	26.015815	198.18.10.1	10.67.243.1	TCP	66	54393 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5014534 TSecr=5153062
160	26.016859	10.67.243.1	198.18.10.1	TCP	54	179 → 54393 [RST] Seq=2 Win=0 Len=0
269	46.017921	198.18.10.1	10.67.243.1	TCP	74	54394 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=5153062
270	46.019257	10.67.243.1	198.18.10.1	TCP	74	179 → 54394 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=5153062
271	46.020510	198.18.10.1	10.67.243.1	TCP	66	54394 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5016535 TSecr=5153062
378	66.028696	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
274	46.022362	10.67.243.1	198.18.10.1	TCP	54	179 → 54394 [RST] Seq=1 Win=0 Len=0
275	46.023079	198.18.10.1	10.67.243.1	TCP	66	54394 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5016535 TSecr=5153062
276	46.024205	10.67.243.1	198.18.10.1	TCP	54	179 → 54394 [RST] Seq=2 Win=0 Len=0
375	66.025032	198.18.10.1	10.67.243.1	TCP	74	54395 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5018535 TSecr=5153062
376	66.026507	10.67.243.1	198.18.10.1	TCP	74	179 → 54395 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5018535 TSecr=5153062
377	66.027841	198.18.10.1	10.67.243.1	TCP	66	54395 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5018536 TSecr=5155062
378	66.028696	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
379	66.029167	10.67.243.1	198.18.10.1	TCP	66	179 → 54395 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5155063 TSecr=5020536
380	66.030029	10.67.243.1	198.18.10.1	TCP	54	179 → 54395 [RST] Seq=1 Win=0 Len=0
381	66.030437	198.18.10.1	10.67.243.1	TCP	66	54395 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5018536 TSecr=5155062
382	66.031703	10.67.243.1	198.18.10.1	TCP	54	179 → 54395 [RST] Seq=2 Win=0 Len=0
495	86.036892	198.18.10.1	10.67.243.1	TCP	74	54396 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5020536 TSecr=5157063
496	86.038169	10.67.243.1	198.18.10.1	TCP	74	179 → 54396 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5020536 TSecr=5157063
497	86.039485	198.18.10.1	10.67.243.1	TCP	66	54396 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5020537 TSecr=5157063
498	86.040168	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
499	86.040674	10.67.243.1	198.18.10.1	TCP	66	179 → 54396 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5157064 TSecr=5020536

Frame 498: 111 bytes on wire (888 bits), 111 bytes captured (888 bits)
Ethernet II, Src: VMware_bc:e3:89 (00:0c:29:bc:e3:89), Dst: VMware_70:cc:53 (00:0c:29:70:cc:53)
Internet Protocol Version 4, Src: 198.18.10.1, Dst: 10.67.243.1
Transmission Control Protocol, Src Port: 54396, Dst Port: 179, Seq: 1, Ack: 1, Len: 45
Border Gateway Protocol - OPEN Message

Troubleshooting com Wireshark



(ip.addr == 10.138.42.1 || ip.addr == 10.67.243.1) && tcp.port == 179

No.	Time	Source	Destination	Protocol	Length	Info
159	26.015815	198.18.10.1	10.67.243.1	TCP	66	54393 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5014534 TSecr=5153062
160	26.016859	10.67.243.1	198.18.10.1	TCP	54	179 → 54393 [RST] Seq=2 Win=0 Len=0
269	46.017921	198.18.10.1	10.67.243.1	TCP	74	54394 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=5153062
270	46.019257	10.67.243.1	198.18.10.1	TCP	74	179 → 54394 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=5153062
271	46.020510	198.18.10.1	10.67.243.1	TCP	66	54394 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5016535 TSecr=5153062
378	66.028696	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
274	46.022362	10.67.243.1	198.18.10.1	TCP	54	179 → 54394 [RST] Seq=1 Win=0 Len=0
275	46.023079	198.18.10.1	10.67.243.1	TCP	66	54394 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5016535 TSecr=5153062
276	46.024205	10.67.243.1	198.18.10.1	TCP	54	179 → 54394 [RST] Seq=2 Win=0 Len=0
375	66.025032	198.18.10.1	10.67.243.1	TCP	74	54395 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5018535 TSecr=5153062
376	66.026507	10.67.243.1	198.18.10.1	TCP	74	179 → 54395 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5018535 TSecr=5153062
377	66.027841	198.18.10.1	10.67.243.1	TCP	66	54395 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5018536 TSecr=5155062
378	66.028696	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
379	66.029167	10.67.243.1	198.18.10.1	TCP	66	179 → 54395 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5155063 TSecr=5018536
380	66.030029	10.67.243.1	198.18.10.1	TCP	54	179 → 54395 [RST] Seq=1 Win=0 Len=0
381	66.030437	198.18.10.1	10.67.243.1	TCP	66	54395 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5018536 TSecr=5155062
382	66.031703	10.67.243.1	198.18.10.1	TCP	54	179 → 54395 [RST] Seq=2 Win=0 Len=0
495	86.036892	198.18.10.1	10.67.243.1	TCP	74	54396 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5020536 TSecr=5157063
496	86.038169	10.67.243.1	198.18.10.1	TCP	74	179 → 54396 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5020536 TSecr=5157063
497	86.039485	198.18.10.1	10.67.243.1	TCP	66	54396 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5020537 TSecr=5157063
498	86.040168	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
499	86.040674	10.67.243.1	198.18.10.1	TCP	66	179 → 54396 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5157064 TSecr=5020537

▶ Frame 498: 111 bytes on wire (888 bits), 111 bytes captured (888 bits)
▶ Ethernet II, Src: VMware_bc:e3:89 (00:0c:29:bc:e3:89), Dst: VMware_70:cc:53 (00:0c:29:70:cc:53)
▶ Internet Protocol Version 4, Src: 198.18.10.1, Dst: 10.67.243.1
▶ Transmission Control Protocol, Src Port: 54396, Dst Port: 179, Seq: 1, Ack: 1, Len: 45
▶ Border Gateway Protocol - OPEN Message

Troubleshooting com Wireshark



(ip.addr == 10.138.42.1 || ip.addr == 10.67.243.1) && tcp.port == 179

No.	Time	Source	Destination	Protocol	Length	Info
159	26.015815	198.18.10.1	10.67.243.1	TCP	66	54393 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5014534 TSecr=5153062
160	26.016859	10.67.243.1	198.18.10.1	TCP	54	179 → 54393 [RST] Seq=2 Win=0 Len=0
269	46.017921	198.18.10.1	10.67.243.1	TCP	74	54394 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=5153062
270	46.019257	10.67.243.1	198.18.10.1	TCP	74	179 → 54394 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=5153062
271	46.020510	198.18.10.1	10.67.243.1	TCP	66	54394 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5016535 TSecr=5153062
378	66.028696	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
274	46.022362	10.67.243.1	198.18.10.1	TCP	54	179 → 54394 [RST] Seq=1 Win=0 Len=0
275	46.023079	198.18.10.1	10.67.243.1	TCP	66	54394 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5016535 TSecr=5153062
276	46.024205	10.67.243.1	198.18.10.1	TCP	54	179 → 54394 [RST] Seq=2 Win=0 Len=0
375	66.025032	198.18.10.1	10.67.243.1	TCP	74	54395 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5018535 TSecr=5153062
376	66.026507	10.67.243.1	198.18.10.1	TCP	74	179 → 54395 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5018535 TSecr=5153062
377	66.027841	198.18.10.1	10.67.243.1	TCP	66	54395 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5018536 TSecr=5155062
378	66.028696	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
379	66.029167	10.67.243.1	198.18.10.1	TCP	66	179 → 54395 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5155063 TSecr=5020536
380	66.030029	10.67.243.1	198.18.10.1	TCP	54	179 → 54395 [RST] Seq=1 Win=0 Len=0
381	66.030437	198.18.10.1	10.67.243.1	TCP	66	54395 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5018536 TSecr=5155062
382	66.031703	10.67.243.1	198.18.10.1	TCP	54	179 → 54395 [RST] Seq=2 Win=0 Len=0
495	86.036892	198.18.10.1	10.67.243.1	TCP	74	54396 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5020536 TSecr=5157063
496	86.038169	10.67.243.1	198.18.10.1	TCP	74	179 → 54396 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5020536 TSecr=5157063
497	86.039485	198.18.10.1	10.67.243.1	TCP	66	54396 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5020537 TSecr=5157063
498	86.040168	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
499	86.040674	10.67.243.1	198.18.10.1	TCP	66	179 → 54396 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5157064 TSecr=5020536

▶ Frame 498: 111 bytes on wire (888 bits), 111 bytes captured (888 bits)
▶ Ethernet II, Src: VMware_bc:e3:89 (00:0c:29:bc:e3:89), Dst: VMware_70:cc:53 (00:0c:29:70:cc:53)
▶ Internet Protocol Version 4, Src: 198.18.10.1, Dst: 10.67.243.1
▶ Transmission Control Protocol, Src Port: 54396, Dst Port: 179, Seq: 1, Ack: 1, Len: 45
▶ Border Gateway Protocol - OPEN Message

Troubleshooting com Wireshark

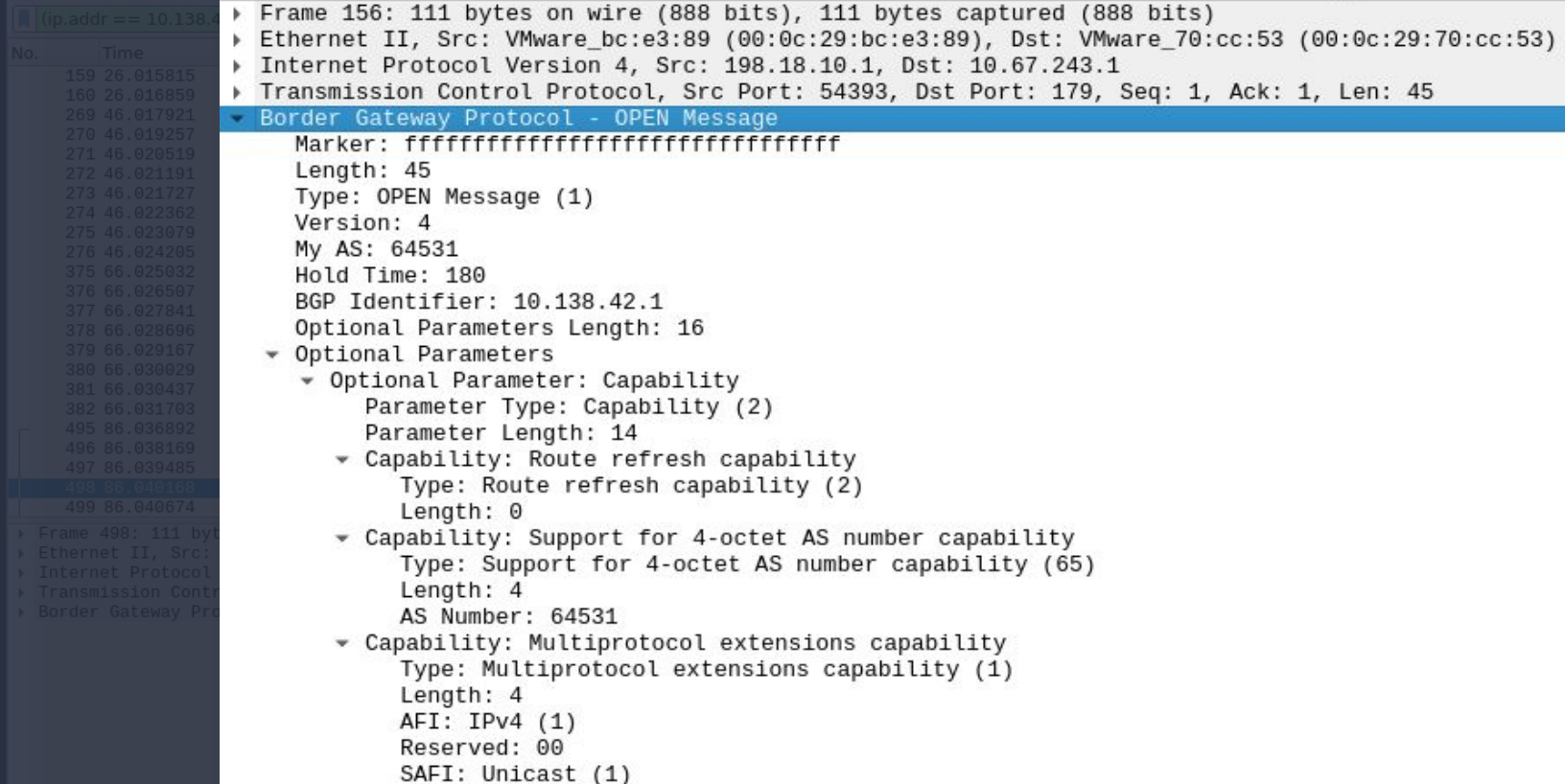
(ip.addr == 10.138.42.1 || ip.addr == 10.67.243.1) && tcp.port == 179

No.	Time	Source	Destination	Protocol	Length	Info
159	26.015815	198.18.10.1	10.67.243.1	TCP	66	54393 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5014534 TSecr=5153062
160	26.016859	10.67.243.1	198.18.10.1	TCP	54	179 → 54393 [RST] Seq=2 Win=0 Len=0
269	46.017921	198.18.10.1	10.67.243.1	TCP	74	54394 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=5153062
270	46.019257	10.67.243.1	198.18.10.1	TCP	74	179 → 54394 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5016535 TSecr=5153062
271	46.020510	198.18.10.1	10.67.243.1	TCP	66	54394 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5016535 TSecr=5153062
378	66.028696	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
274	46.022362	10.67.243.1	198.18.10.1	TCP	54	179 → 54394 [RST] Seq=1 Win=0 Len=0
275	46.023079	198.18.10.1	10.67.243.1	TCP	66	54394 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5016535 TSecr=5153062
276	46.024205	10.67.243.1	198.18.10.1	TCP	54	179 → 54394 [RST] Seq=2 Win=0 Len=0
375	66.025032	198.18.10.1	10.67.243.1	TCP	74	54395 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5018535 TSecr=5153062
376	66.026507	10.67.243.1	198.18.10.1	TCP	74	179 → 54395 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5018535 TSecr=5153062
377	66.027841	198.18.10.1	10.67.243.1	TCP	66	54395 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5018536 TSecr=5155062
378	66.028696	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
379	66.029167	10.67.243.1	198.18.10.1	TCP	66	179 → 54395 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5155063 TSecr=5018536
380	66.030029	10.67.243.1	198.18.10.1	TCP	54	179 → 54395 [RST] Seq=1 Win=0 Len=0
381	66.030437	198.18.10.1	10.67.243.1	TCP	66	54395 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5018536 TSecr=5155062
382	66.031703	10.67.243.1	198.18.10.1	TCP	54	179 → 54395 [RST] Seq=2 Win=0 Len=0
495	86.036892	198.18.10.1	10.67.243.1	TCP	74	54396 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5020536 TSecr=5157063
496	86.038169	10.67.243.1	198.18.10.1	TCP	74	179 → 54396 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=5020536 TSecr=5157063
497	86.039485	198.18.10.1	10.67.243.1	TCP	66	54396 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5020537 TSecr=5157063
498	86.040168	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
499	86.040674	10.67.243.1	198.18.10.1	TCP	66	179 → 54396 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5157064 TSecr=5020537

▶ Frame 498: 111 bytes on wire (888 bits), 111 bytes captured (888 bits)
▶ Ethernet II, Src: VMware_bc:e3:89 (00:0c:29:bc:e3:89), Dst: VMware_70:cc:53 (00:0c:29:70:cc:53)
▶ Internet Protocol Version 4, Src: 198.18.10.1, Dst: 10.67.243.1
▶ Transmission Control Protocol, Src Port: 54396, Dst Port: 179, Seq: 1, Ack: 1, Len: 45
▶ Border Gateway Protocol - OPEN Message

▶ Border Gateway Protocol - OPEN Message

Troubleshooting com Wireshark



Wireshark packet capture analysis showing a BGP OPEN message. The packet list on the left shows frame 156 selected. The packet details pane on the right shows the structure of the BGP message.

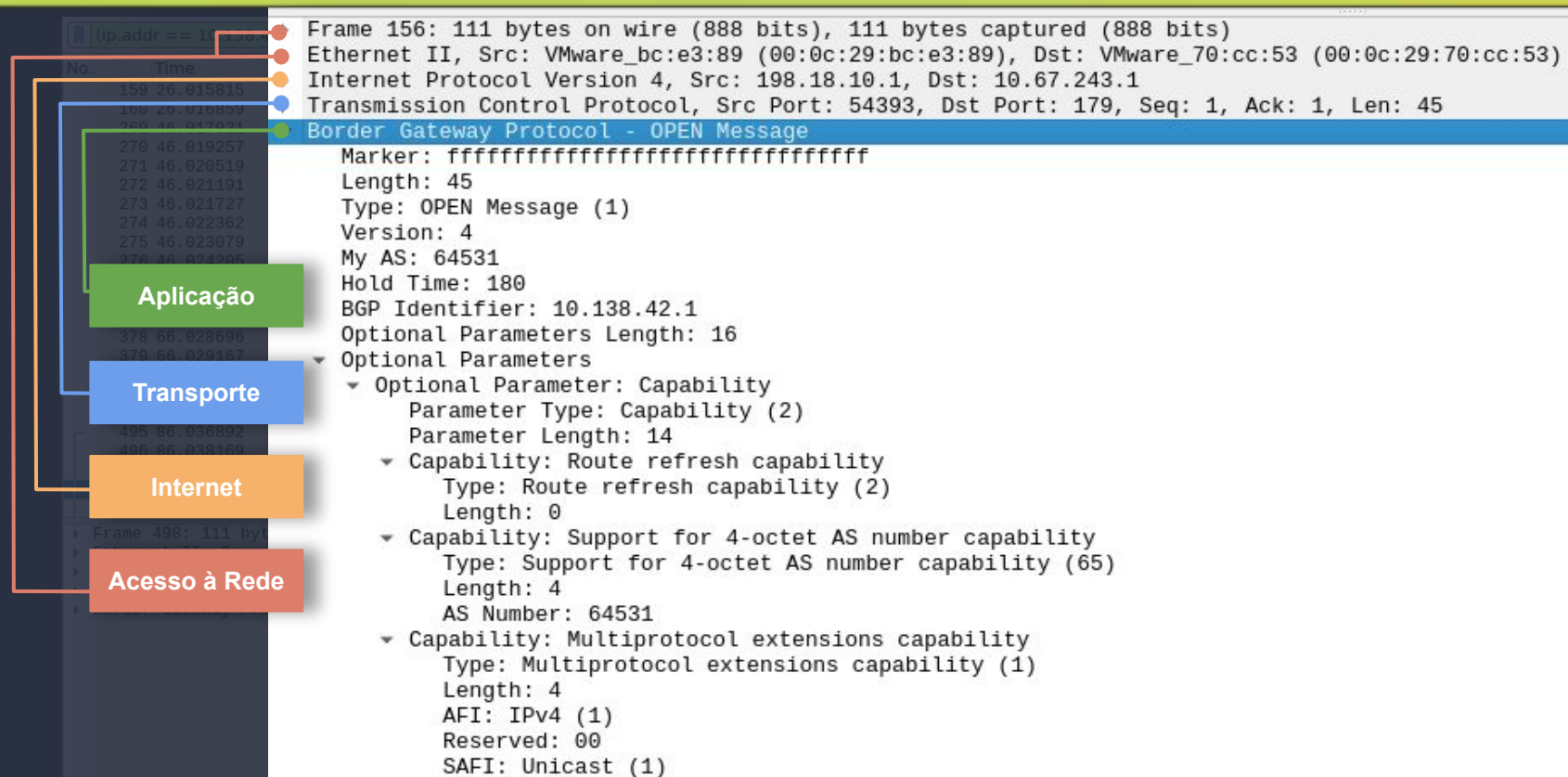
Filter: (ip.addr == 10.138.42.1)

No.	Time	Source	Destination	Protocol	Length	Info
159	26.015815	10.138.42.1	10.67.243.1	Ethernet II	1500	...
160	26.016859	10.67.243.1	10.138.42.1	Ethernet II	1500	...
269	46.017921	10.138.42.1	10.67.243.1	Ethernet II	1500	...
270	46.019257	10.67.243.1	10.138.42.1	Ethernet II	1500	...
271	46.020519	10.138.42.1	10.67.243.1	Ethernet II	1500	...
272	46.021191	10.67.243.1	10.138.42.1	Ethernet II	1500	...
273	46.021727	10.138.42.1	10.67.243.1	Ethernet II	1500	...
274	46.022362	10.67.243.1	10.138.42.1	Ethernet II	1500	...
275	46.023079	10.138.42.1	10.67.243.1	Ethernet II	1500	...
276	46.024205	10.67.243.1	10.138.42.1	Ethernet II	1500	...
375	66.025032	10.138.42.1	10.67.243.1	Ethernet II	1500	...
376	66.026507	10.67.243.1	10.138.42.1	Ethernet II	1500	...
377	66.027841	10.138.42.1	10.67.243.1	Ethernet II	1500	...
378	66.028696	10.67.243.1	10.138.42.1	Ethernet II	1500	...
379	66.029167	10.138.42.1	10.67.243.1	Ethernet II	1500	...
380	66.030029	10.67.243.1	10.138.42.1	Ethernet II	1500	...
381	66.030437	10.138.42.1	10.67.243.1	Ethernet II	1500	...
382	66.031703	10.67.243.1	10.138.42.1	Ethernet II	1500	...
495	86.036892	10.138.42.1	10.67.243.1	Ethernet II	1500	...
496	86.038169	10.67.243.1	10.138.42.1	Ethernet II	1500	...
497	86.039485	10.138.42.1	10.67.243.1	Ethernet II	1500	...
498	86.040163	10.67.243.1	10.138.42.1	Ethernet II	1500	...
499	86.040674	10.138.42.1	10.67.243.1	Ethernet II	1500	...

Frame 156: 111 bytes on wire (888 bits), 111 bytes captured (888 bits) on interface 0

- Ethernet II, Src: VMware_bc:e3:89 (00:0c:29:bc:e3:89), Dst: VMware_70:cc:53 (00:0c:29:70:cc:53)
- Internet Protocol Version 4, Src: 198.18.10.1, Dst: 10.67.243.1
- Transmission Control Protocol, Src Port: 54393, Dst Port: 179, Seq: 1, Ack: 1, Len: 45
- Border Gateway Protocol - OPEN Message**
 - Marker: ff
 - Length: 45
 - Type: OPEN Message (1)
 - Version: 4
 - My AS: 64531
 - Hold Time: 180
 - BGP Identifier: 10.138.42.1
 - Optional Parameters Length: 16
 - Optional Parameters
 - Optional Parameter: Capability
 - Parameter Type: Capability (2)
 - Parameter Length: 14
 - Capability: Route refresh capability
 - Type: Route refresh capability (2)
 - Length: 0
 - Capability: Support for 4-octet AS number capability
 - Type: Support for 4-octet AS number capability (65)
 - Length: 4
 - AS Number: 64531
 - Capability: Multiprotocol extensions capability
 - Type: Multiprotocol extensions capability (1)
 - Length: 4
 - AFI: IPv4 (1)
 - Reserved: 00
 - SAFI: Unicast (1)

Troubleshooting com Wireshark



Frame 156: 111 bytes on wire (888 bits), 111 bytes captured (888 bits)

- Ethernet II, Src: VMware_bc:e3:89 (00:0c:29:bc:e3:89), Dst: VMware_70:cc:53 (00:0c:29:70:cc:53)
- Internet Protocol Version 4, Src: 198.18.10.1, Dst: 10.67.243.1
- Transmission Control Protocol, Src Port: 54393, Dst Port: 179, Seq: 1, Ack: 1, Len: 45
- Border Gateway Protocol - OPEN Message**

Marker: ffffffffffffffffffffffffffffffffff
Length: 45
Type: OPEN Message (1)
Version: 4
My AS: 64531
Hold Time: 180
BGP Identifier: 10.138.42.1
Optional Parameters Length: 16

- Optional Parameters
 - Optional Parameter: Capability
 - Parameter Type: Capability (2)
 - Parameter Length: 14
 - Capability: Route refresh capability
 - Type: Route refresh capability (2)
 - Length: 0
 - Capability: Support for 4-octet AS number capability
 - Type: Support for 4-octet AS number capability (65)
 - Length: 4
 - AS Number: 64531
 - Capability: Multiprotocol extensions capability
 - Type: Multiprotocol extensions capability (1)
 - Length: 4
 - AFI: IPv4 (1)
 - Reserved: 00
 - SAFI: Unicast (1)

Aplicação

Transporte

Internet

Acesso à Rede

Troubleshooting com Wireshark

(ip.addr == 10.138.42.1)

No.	Time
159	26.015815
160	26.016859
270	46.019257
271	46.020519
272	46.021191
273	46.021727
274	46.022362
275	46.023079
378	66.028698
379	66.029167
380	66.030029
381	66.030437
382	66.031703
495	86.036892
496	86.038169
497	86.039485
498	86.040163
499	86.040674

Aplicação

- ▶ Frame 156: 111 bytes on wire (888 bits), 111 bytes captured (888 bits)
- ▶ Ethernet II, Src: VMware_bc:e3:89 (00:0c:29:bc:e3:89), Dst: VMware_70:cc:53 (00:0c:29:70:cc:53)
- ▶ Internet Protocol Version 4, Src: 198.18.10.1, Dst: 10.67.243.1
- ▶ Transmission Control Protocol, Src Port: 54393, Dst Port: 179, Seq: 1, Ack: 1, Len: 45

Border Gateway Protocol - OPEN Message

Marker: ffffffffffffffffffffffffffffffffff
Length: 45
Type: OPEN Message (1)
Version: 4
My AS: 64531
Hold Time: 180
BGP Identifier: 10.138.42.1
Optional Parameters Length: 16

- ▼ Optional Parameters
 - ▼ Optional Parameter: Capability
 - Parameter Type: Capability (2)
 - Parameter Length: 14
 - ▼ Capability: Route refresh capability
 - Type: Route refresh capability (2)
 - Length: 0
 - ▼ Capability: Support for 4-octet AS number capability
 - Type: Support for 4-octet AS number capability (65)
 - Length: 4
 - AS Number: 64531
 - ▼ Capability: Multiprotocol extensions capability
 - Type: Multiprotocol extensions capability (1)
 - Length: 4
 - AFI: IPv4 (1)
 - Reserved: 00
 - SAFI: Unicast (1)

▶ Frame 498: 111 bytes on wire (888 bits), 111 bytes captured (888 bits) on interface 0
▶ Ethernet II, Src: VMware_70:cc:53 (00:0c:29:70:cc:53), Dst: VMware_bc:e3:89 (00:0c:29:bc:e3:89)
▶ Internet Protocol Version 4, Src: 10.67.243.1, Dst: 198.18.10.1
▶ Transmission Control Protocol, Src Port: 179, Dst Port: 54393, Seq: 1, Len: 45
▶ Border Gateway Protocol, Src AS: 64531, Dst AS: 64531, Type: OPEN Message



Troubleshooting com Wireshark

No.	Time
159	26.015815
160	26.016859
269	46.017921
270	46.019257
271	46.020519
272	46.021191
273	46.021727
274	46.022362
275	46.023079
276	46.024205
375	66.025032
376	66.026507
377	66.027841
378	66.028696
379	66.029167
380	66.030029
381	66.030437
382	66.031703
495	86.036892
496	86.038169
497	86.039485
498	86.040163
499	86.040674

- ▶ Frame 156: 111 bytes on wire (888 bits), 111 bytes captured (888 bits)
- ▶ Ethernet II, Src: VMware_bc:e3:89 (00:0c:29:bc:e3:89), Dst: VMware_70:cc:53 (00:0c:29:70:cc:53)
- ▶ Internet Protocol Version 4, Src: 198.18.10.1, Dst: 10.67.243.1
- ▶ Transmission Control Protocol, Src Port: 54393, Dst Port: 179, Seq: 1, Ack: 1, Len: 45

▼ Border Gateway Protocol - OPEN Message

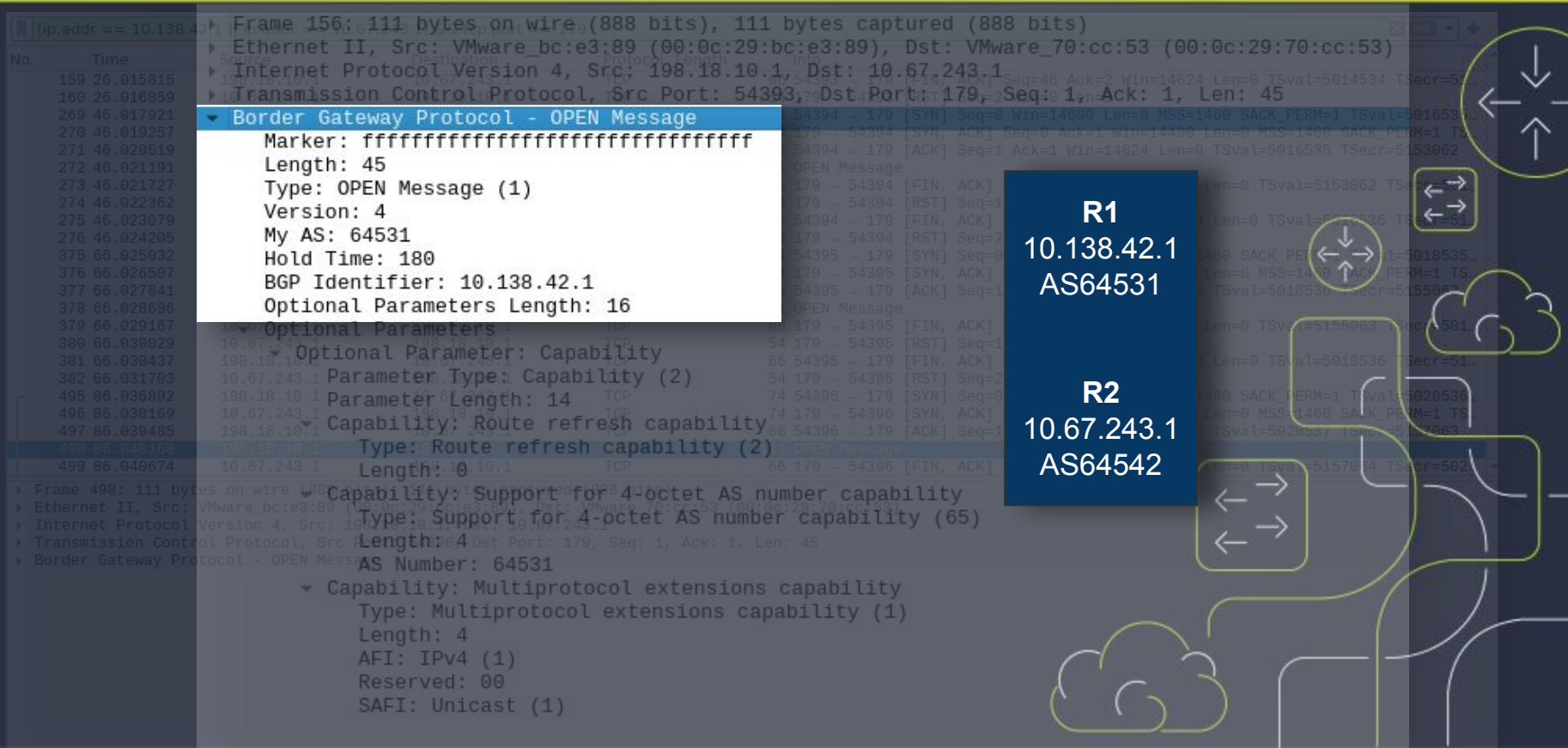
- Marker: ffffffffffffffffffffffffffffffffff
- Length: 45
- Type: OPEN Message (1)
- Version: 4
- My AS: 64531
- Hold Time: 180
- BGP Identifier: 10.138.42.1
- Optional Parameters Length: 16
- ▼ Optional Parameters
 - ▼ Optional Parameter: Capability
 - Parameter Type: Capability (2)
 - Parameter Length: 14
 - ▼ Capability: Route refresh capability
 - Type: Route refresh capability (2)
 - Length: 0
 - ▼ Capability: Support for 4-octet AS number capability
 - Type: Support for 4-octet AS number capability (65)
 - Length: 4
 - AS Number: 64531
 - ▼ Capability: Multiprotocol extensions capability
 - Type: Multiprotocol extensions capability (1)
 - Length: 4
 - AFI: IPv4 (1)
 - Reserved: 00
 - SAFI: Unicast (1)

R1
10.138.42.1
AS64531

R2
10.67.243.1
AS64542



Troubleshooting com Wireshark



The image shows a Wireshark packet capture analysis of a BGP OPEN message. The background displays a list of network packets, with the selected packet (Frame 156) expanded to show its details. A white box highlights the BGP OPEN message details, and a blue box on the right identifies the source and destination routers.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
159	26.015815					
160	26.016859					
269	46.017921					
270	46.019257					
271	46.020519					
272	46.021191					
273	46.021727					
274	46.022362					
275	46.023079					
276	46.024205					
375	66.025032					
376	66.026507					
377	66.027841					
378	66.028696					
379	66.029167					
380	66.030029					
381	66.030437					
382	66.031703					
495	86.036892					
496	86.038169					
497	86.039485					
498	86.040169					
499	86.040674					

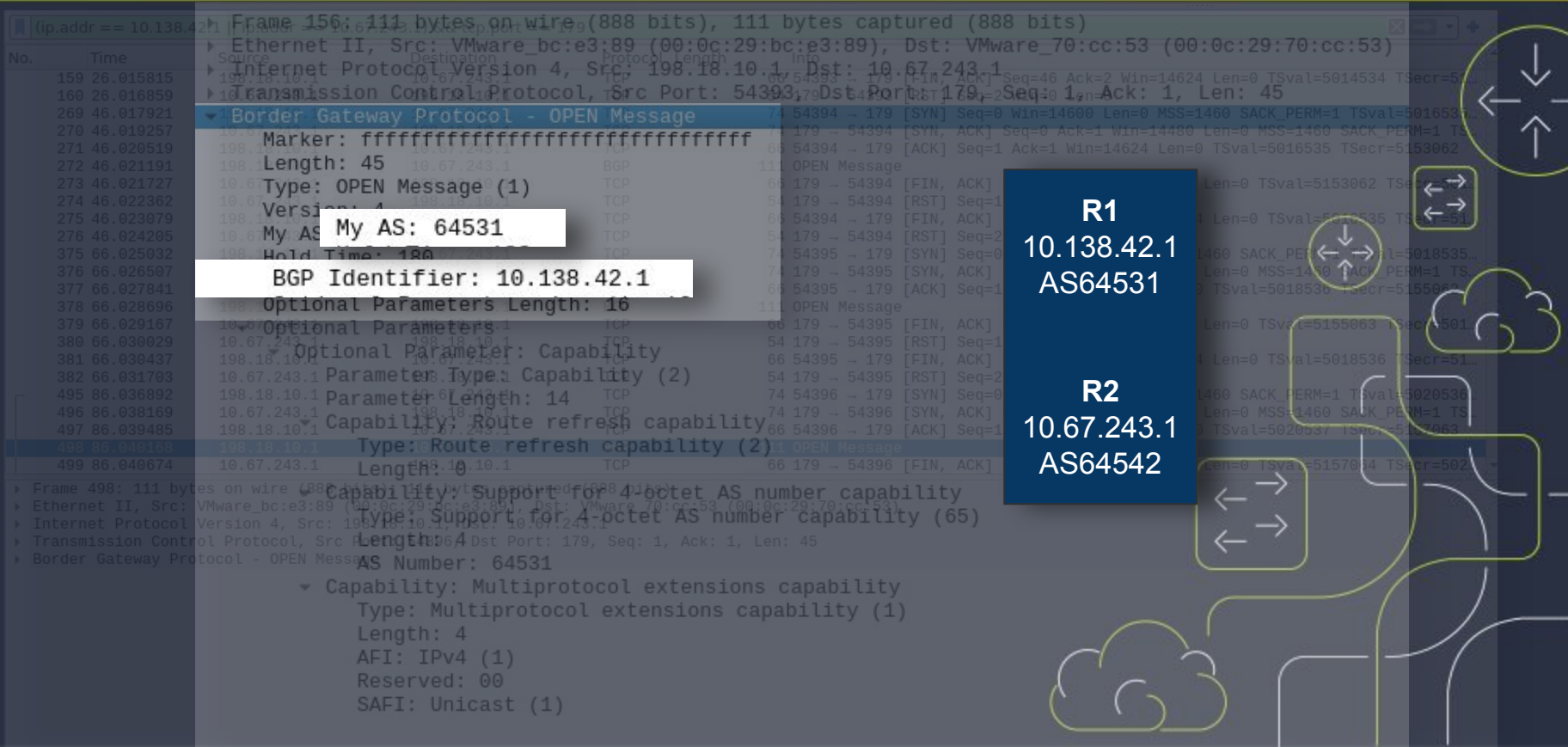
Frame 156 Details:

- Frame 156: 111 bytes on wire (888 bits), 111 bytes captured (888 bits)
- Ethernet II, Src: VMware_bc:e3:89 (00:0c:29:bc:e3:89), Dst: VMware_70:cc:53 (00:0c:29:70:cc:53)
- Internet Protocol Version 4, Src: 198.18.10.1, Dst: 10.67.243.1
- Transmission Control Protocol, Src Port: 54393, Dst Port: 179, Seq: 1, Ack: 1, Len: 45
- Border Gateway Protocol - OPEN Message**
 - Marker: ffffffffffffffffffffffffffffffffff
 - Length: 45
 - Type: OPEN Message (1)
 - Version: 4
 - My AS: 64531
 - Hold Time: 180
 - BGP Identifier: 10.138.42.1
 - Optional Parameters Length: 16
 - Optional Parameters
 - Optional Parameter: Capability
 - Parameter Type: Capability (2)
 - Parameter Length: 14
 - Capability: Route refresh capability
 - Type: Route refresh capability (2)
 - Length: 0
 - Capability: Support for 4-octet AS number capability
 - Type: Support for 4-octet AS number capability (65)
 - Length: 4
 - AS Number: 64531
 - Capability: Multiprotocol extensions capability
 - Type: Multiprotocol extensions capability (1)
 - Length: 4
 - AFI: IPv4 (1)
 - Reserved: 00
 - SAFI: Unicast (1)

R1
10.138.42.1
AS64531

R2
10.67.243.1
AS64542

Troubleshooting com Wireshark



Frame 156: 111 bytes on wire (888 bits), 111 bytes captured (888 bits) on interface 0

Ethernet II, Src: VMware_b3:e3:89 (00:0c:29:bc:e3:89), Dst: VMware_70:cc:53 (00:0c:29:70:cc:53)

Internet Protocol Version 4, Src: 198.18.10.1, Dst: 10.67.243.1

Transmission Control Protocol, Src Port: 54393, Dst Port: 179, Seq: 1, Ack: 1, Len: 45

Border Gateway Protocol - OPEN Message

Marker: ffffffffffffffffffffffffffffffffff

Length: 45

Type: OPEN Message (1)

Version: 4

My AS: **My AS: 64531**

Hold Time: 180

BGP Identifier: **BGP Identifier: 10.138.42.1**

Optional Parameters Length: 16

Optional Parameters

Optional Parameter: Capability

Parameter Type: Capability (2)

Parameter Length: 14

Capability, Route refresh capability

Type: Route refresh capability (2)

Length: 10

Capability: Support for 4-octet AS number capability

Type: Support for 4-octet AS number capability (65)

Length: 4

AS Number: 64531

Capability: Multiprotocol extensions capability

Type: Multiprotocol extensions capability (1)

Length: 4

AFI: IPv4 (1)

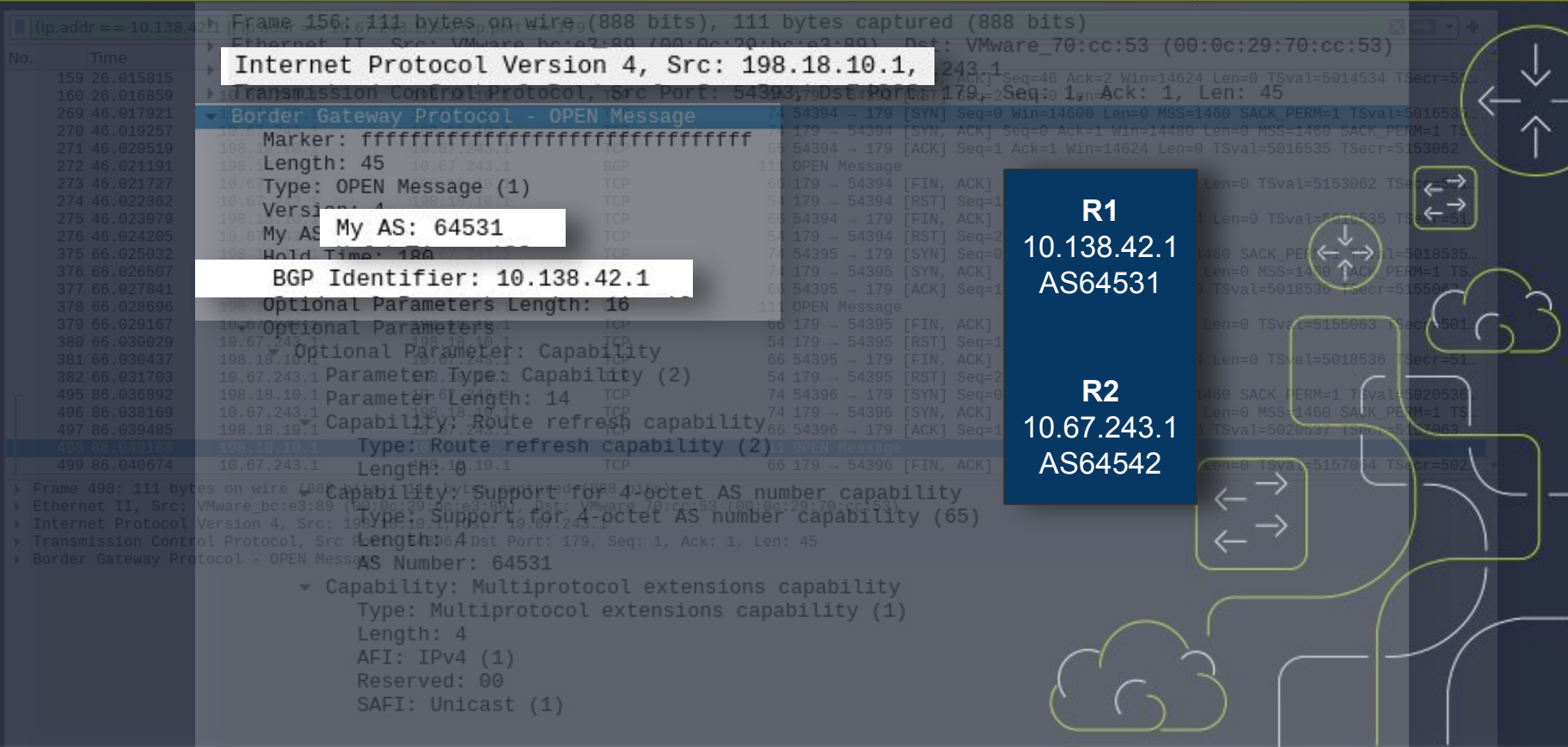
Reserved: 00

SAFI: Unicast (1)

R1
10.138.42.1
AS64531

R2
10.67.243.1
AS64542

Troubleshooting com Wireshark



Internet Protocol Version 4, Src: 198.18.10.1, Dst: 10.67.243.1

Border Gateway Protocol - OPEN Message

Marker: ffffffffffffffffffffffffffffffffff

Length: 45

Type: OPEN Message (1)

Version: 4

My AS: 64531

BGP Identifier: 10.138.42.1

Optional Parameters Length: 16

Optional Parameters

Optional Parameter: Capability

Parameter Type: Capability (2)

Parameter Length: 14

Capability: Route refresh capability

Type: Route refresh capability (2)

Capability: Support for 4-octet AS number capability

Type: Support for 4-octet AS number capability (65)

Length: 4

AS Number: 64531

Capability: Multiprotocol extensions capability

Type: Multiprotocol extensions capability (1)

Length: 4

AFI: IPv4 (1)

Reserved: 00

SAFI: Unicast (1)

R1
10.138.42.1
AS64531

R2
10.67.243.1
AS6452

Troubleshooting com Wireshark

Frame 156: 111 bytes on wire (888 bits), 111 bytes captured (888 bits) on interface 0

Ethernet II, Src: VMware_bce3:89:(00:0c:29:70:cc:53), Dst: VMware_70:cc:53:(00:0c:29:70:cc:53)

Internet Protocol Version 4, Src: 198.18.10.1, Dst: 10.67.243.1

Transmission Control Protocol, Src Port: 54393, Dst Port: 179, Seq: 1, Ack: 1, Len: 45

Border Gateway Protocol - OPEN Message

Marker: ffffffffffffffffffffffffffffffffff

Length: 45

Type: OPEN Message (1)

Version: 4

My AS: 64531

BGP Identifier: 10.138.42.1

Optional Parameters Length: 16

Optional Parameters

Optional Parameter: Capability

Parameter Type: Capability (2)

Parameter Length: 14

Capability: Route refresh capability

Type: Route refresh capability (2)

Capability: Support for 4-octet AS number capability

Type: Support for 4-octet AS number capability (65)

Length: 4

AS Number: 64531

Capability: Multiprotocol extensions capability

Type: Multiprotocol extensions capability (1)

Length: 4

AFI: IPv4 (1)

Reserved: 00

SAFI: Unicast (1)

R1
10.138.42.1
AS64531

R2
10.67.243.1
AS6452

Troubleshooting com Wireshark

The image shows a Wireshark packet capture of a BGP OPEN message. The packet list pane shows the following details:

- Internet Protocol Version 4, Src: 198.18.10.1 (marked with a red X)
- Border Gateway Protocol - OPEN Message
- Marker: ffffffffffffffffffffffffffffffffff
- Length: 45
- Type: OPEN Message (1)
- Version: 4
- My AS: 64531 (marked with a green checkmark)
- BGP Identifier: 10.138.42.1 (marked with a green checkmark)
- Optional Parameters Length: 16
- Optional Parameters

On the right side, there is a network diagram with two routers:

- R1**
10.138.42.1
AS64531
- R2**
10.67.243.1
AS64542

Arrows indicate connections between R1 and R2, and between R1 and a cloud representing the Internet.

Conclusão:

O Roteador R1 está enviando requisições BGP para o IP e AS correto de R2. No entanto, R1 não configurou o IP 10.138.42.1 como update-source, resultando em requisições com IP de origem incorreto (198.18.10.1). Roteador R2 recusa a conexão.

Alternativas ao Wireshark

- tshark (wireshark cli)

```
jean@unicron:~/pcaps$ tshark -r 5bgpcap-filtred.pcap
 1  0.000000 198.18.10.1 → 10.67.243.1  TCP 74 54393 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=5014
534 TSecr=0 WS=32
 2  0.001253 10.67.243.1 → 198.18.10.1  TCP 74 179 → 54393 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1
 TSval=5151061 TSecr=5014534 WS=32
 3  0.002470 198.18.10.1 → 10.67.243.1  TCP 66 54393 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=5014534 TSecr=51510
61
 4  0.003209 198.18.10.1 → 10.67.243.1  BGP 111 OPEN Message
 5  0.003622 10.67.243.1 → 198.18.10.1  TCP 66 179 → 54393 [FIN, ACK] Seq=1 Ack=1 Win=14496 Len=0 TSval=5151061 TSecr=
5014534
 6  0.004263 10.67.243.1 → 198.18.10.1  TCP 54 179 → 54393 [RST] Seq=1 Win=0 Len=0
 7  0.004977 198.18.10.1 → 10.67.243.1  TCP 66 54393 → 179 [FIN, ACK] Seq=46 Ack=2 Win=14624 Len=0 TSval=5014534 TSecr
=5151061
 8  0.006021 10.67.243.1 → 198.18.10.1  TCP 54 179 → 54393 [RST] Seq=2 Win=0 Len=0
```



Alternativas ao Wireshark

- termshark

termshark 2.2.0 | 5bgpcap-filtred.pcap Analysis Misc

Filter: <Apply> <Recent>

No. -	Time -	Source -	Destination -	Protocol -	Length -	Info -
1	0.000000	198.18.10.1	10.67.243.1	TCP	74	54393 → 179 [SYN] Seq=0 Win=14600 Len=0 MSS=1
2	0.001253	10.67.243.1	198.18.10.1	TCP	74	179 → 54393 [SYN, ACK] Seq=0 Ack=1 Win=14480
3	0.002470	198.18.10.1	10.67.243.1	TCP	66	54393 → 179 [ACK] Seq=1 Ack=1 Win=14624 Len=0
4	0.003209	198.18.10.1	10.67.243.1	BGP	111	OPEN Message
5	0.003622	10.67.243.1	198.18.10.1	TCP	66	179 → 54393 [FIN, ACK] Seq=1 Ack=1 Win=14496
6	0.004263	10.67.243.1	198.18.10.1	TCP	54	179 → 54393 [RST] Seq=1 Win=0 Len=0

[+] Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
[+] Ethernet II, Src: VMware_bc:e3:89 (00:0c:29:bc:e3:89), Dst: VMware_70:cc:53 (00:0c:29:70:cc:53)
[+] Internet Protocol Version 4, Src: 198.18.10.1, Dst: 10.67.243.1
[+] Transmission Control Protocol, Src Port: 54393, Dst Port: 179, Seq: 0, Len: 0

0000	00 0c 29 70 cc 53	00 0c 29 bc e3 89 08 00 45 c0	.)p.S..).....E.
0010	00 3c 4d d4 40 00 ff 06 5f cf c6 12 0a 01 0a 43		.<M.@... _.....C
0020	f3 01 d4 79 00 b3 c1 1a c9 d2 00 00 00 00 a0 02		...y....
0030	39 08 5d 35 00 00 02 04 05 b4 04 02 08 0a 00 4c		9.]5.....L
0040	84 06 00 00 00 00 01 03 03 05	



Obrigado!



E-mail:

jean.figueireido@sagenetworks.com.br

Site: sagenetworks.com.br

Telefone: (19) 3500-6269

