

EA080: Laboratório 07

Vinícius Esperança Mantovani,
247395.

Introdução)

Neste laboratório, foi feita uma análise forense, dada uma possível forma de topologia, como forma de se descobrir informações a respeito de tal topologia e de se entender a respeito de cada um dos nós que ela contém. Para tanto, foram utilizadas capturas de pacotes disponibilizadas como arquivos a serem analisados por meio do “*wireshark*”. Com isso, todos os objetivos de compreensão da rede foram satisfeitos, conforme se nota no desenvolvimento do presente relatório.

Vale ressaltar a imagem inicial da topologia cujos dispositivos devem ser descobertos:

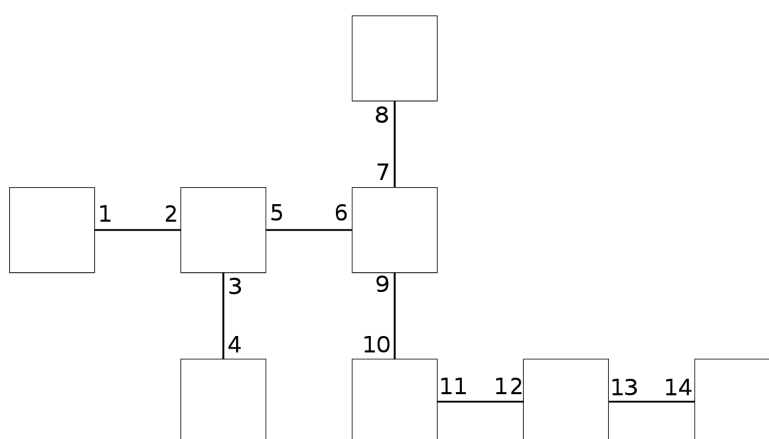


Figura 1: Topologia a ser desvendada neste experimento

Destaca-se ainda, que ao observar todas as capturas em um procedimento inicial sucinto, é possível notar que foram iniciadas em momentos muito próximos, de forma que é possível assumir que os pacotes que transitam entre pares diferentes de dispositivos ou aqueles que são ocasionados por outros pacotes, foram capturados de maneira que se mostrem, de fato, ligados. Logo, não foram destacados, durante a análise feita neste relatório, os momentos de emissão e recepção de pacote nenhum.

Finalmente, é importante notar que o presente documento é dividido em pseudo-seções, cada uma se iniciando na abertura de um novo “.pcap” quando convém e todas separadas por uma reta horizontal que ocupa uma linha completa.

Desenvolvimento)

Inicialmente, utilizou-se a captura “1-2.pcap”, de forma a se notar, já de início, a presença de no mínimo três dispositivos na rede, dois que ganham IPs, por meio do protocolo *DHCP*, do terceiro, que é um servidor *DHCP* e aparenta ser um roteador. Aqui, supõe-se por simplicidade que é usado um mesmo servidor *DHCP* pelos dois primeiros dispositivos citados, o que deve ser verdade pela topologia da *Figura 1*, mas será inexoravelmente provado mais adiante:

- Dispositivo 1:

Baseado nas figuras e explicações abaixo, pode-se notar que o dispositivo, chamado aqui de 1, tem:

MAC → 00:00:00:00:00:02

IPv4 → 10.0.0.12

1	2018-11-08 10:11:20,490601 0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover	- Transaction ID 0x9e3a9a1e
2	2018-11-08 10:11:20,492749 10.0.0.1	255.255.255.255	DHCP	323 DHCP Offer	- Transaction ID 0x9e3a9a1e
3	2018-11-08 10:11:20,493304 0.0.0.0	255.255.255.255	DHCP	342 DHCP Request	- Transaction ID 0x9e3a9a1e
4	2018-11-08 10:11:20,494694 10.0.0.1	255.255.255.255	DHCP	323 DHCP ACK	- Transaction ID 0x9e3a9a1e

Figura 2: Conjunto de pacotes DHCP envolvidos na aquisição de IPv4 pelo dispositivo 1

Conforme a Figura 2 apresenta, tem-se a aquisição de IPv4 pelo dispositivo 1 em contato seguindo o protocolo *DHCP* com o dispositivo 3 (assim será chamado tal dispositivo). Assim, conforme se nota na Figura 3, que apresenta informações do pacote *Discover* enviado por 1 em *broadcast*, o dispositivo 1 tem como MAC o valor apresentado anteriormente. Além disso, conforme a Figura 3, o dispositivo 1 recebe o IPv4 citado anteriormente por meio do pacote *Offer* enviado pelo dispositivo 3 para em *broadcast* e, o dispositivo 1 aceita tal endereço, conforme se nota pelo pacote *Request* que envia logo em seguida

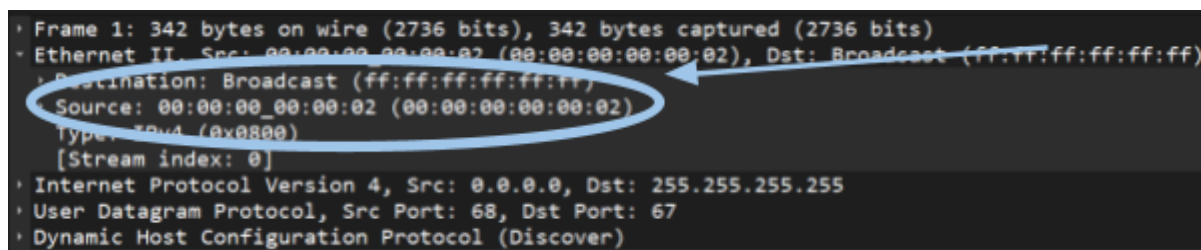


Figura 3: Informação de MAC do dispositivo 1 como fonte do pacote DHCP “discover”

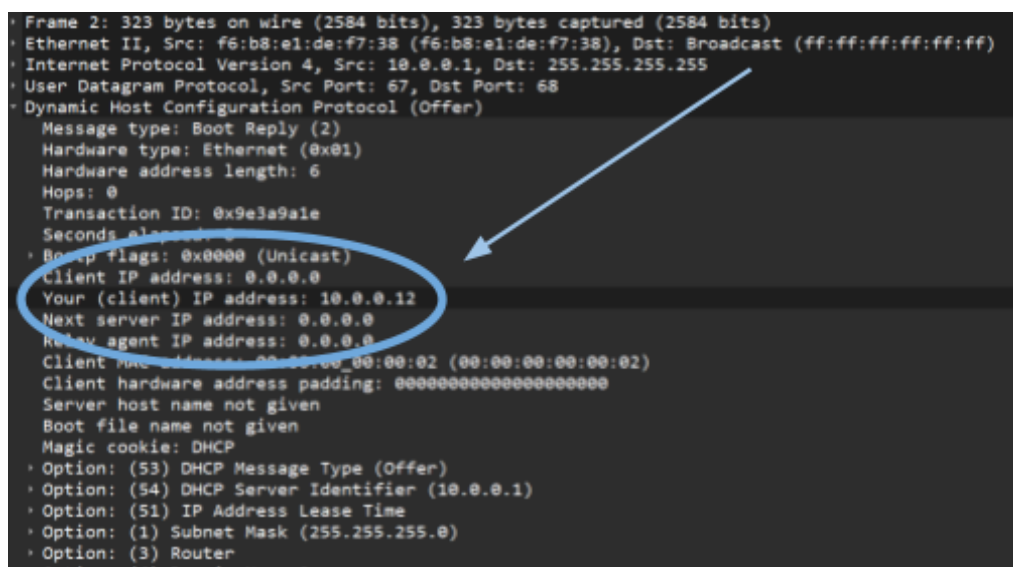


Figura 4: Informação de IPv4 adquirido pelo dispositivo 1 no pacote DHCP “offer”

- Dispositivo 2:

Pelo mesmo processo apresentado para o dispositivo 1, sabe-se que:

MAC → 00:00:00:00:00:03

IPv4 → 10.0.0.13

5	2018-11-08 10:11:21,616248	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover	- Transaction ID 0xfa0b0f5b
6	2018-11-08 10:11:21,617513	10.0.0.1	255.255.255.255	DHCP	323 DHCP Offer	- Transaction ID 0xfa0b0f5b
7	2018-11-08 10:11:21,618686	0.0.0.0	255.255.255.255	DHCP	342 DHCP Request	- Transaction ID 0xfa0b0f5b
8	2018-11-08 10:11:21,619742	10.0.0.1	255.255.255.255	DHCP	323 DHCP ACK	- Transaction ID 0xfa0b0f5b

Figura 5: Conjunto de pacotes DHCP envolvidos na aquisição de IPv4 pelo dispositivo 2

```

Frame 5: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: 00:00:00_00:00:03 (00:00:00:00:00:03), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Source: 00:00:00_00:00:03 (00:00:00:00:00:03)
Type: IPv4 (0x0800)
[Stream index: 2]
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Discover)

```

Figura 6: Informação de MAC do dispositivo 2 como fonte do pacote DHCP “discover”

```

Frame 6: 323 bytes on wire (2584 bits), 323 bytes captured (2584 bits)
Ethernet II, Src: f6:b8:e1:de:f7:38 (f6:b8:e1:de:f7:38), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 10.0.0.1, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 67, Dst Port: 68
Dynamic Host Configuration Protocol (Offer)
  Message type: Boot Reply (2)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xfa0b0f5b
  Seconds elapsed: 0
  Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 10.0.0.11
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: 00:00:00_00:00:03 (00:00:00:00:00:03)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  Option: (53) DHCP Message Type (Offer)
  Option: (54) DHCP Server Identifier (10.0.0.1)
  Option: (51) IP Address Lease Time
  Option: (1) Subnet Mask (255.255.255.0)
  Option: (3) Router

```

Figura 7: Informação de IPv4 adquirido pelo dispositivo 2 no pacote DHCP “offer”

9	2018-11-08 10:11:27,630412	00:00:00_00:00:02	Broadcast	ARP	42 Who has 10.0.0.1? Tell 10.0.0.12
10	2018-11-08 10:11:27,633089	f6:b8:e1:de:f7:38	00:00:00_00:00:02	ARP	42 10.0.0.1 is at f6:b8:e1:de:f7:38

Figura 8: Solicitação e resposta de busca ARP feita pelo dispositivo 1

Ainda sob análise desse primeiro “pcap”, pode-se observar que o dispositivo 1 faz uma busca *ARP*, naturalmente em *broadcast*, pelo dispositivo com IPv4 10.0.0.1, que responde no MAC f6:b8:e1:de:f7:38 (Figura 8 acima). Disso, observando ainda o campo “*DHCP Server Identifier*” nos pacotes *DHCP* “*offer*” apresentados nas Figuras 4 e 7, é possível notar que o IPv4 em questão é do dispositivo 3 e, por consequência, a suposição de que um mesmo dispositivo teria dado IPv4 aos dispositivos 1 e 2 é real e esse dispositivo, 3, tem os endereços citados neste parágrafo. Logo, sabe-se que:

- Dispositivo 3:

Com base no que se explica anteriormente, este dispositivo tem:

MAC → f6:b8:e1:de:f7:38

IPv4 → 10.0.0.1

Seguindo na captura já citada, vê-se uma comunicação *TCP* entre dois hosts da topologia, sendo eles o dispositivo 1 (descoberto, agora, como host) e um dispositivo 4, que entrou agora em discussão na topologia (host de IPv4 172.16.143.2). Este novo dispositivo está, obviamente, em outra rede, pelo IPv4 que apresenta, o que significa que há ao menos um roteador entre o dispositivo 1 e o 4. Nesse sentido, temos de novidade:

- Dispositivo 4:

Baseado no que se afirma acima, tem-se:

MAC → ?

IPv4 → 172.16.143.2

Além do citado acima, anteriormente à conexão *TCP*, houve uma comunicação *DNS* entre o dispositivo 1 e um servidor *DNS* que, por simplicidade, será chamado de “dispositivo *DNS*”, ao contrário dos demais dispositivos que foram numerados. De tal dispositivo, sabe-se que:

- Dispositivo *DNS*:

Com base na figura abaixo, nota-se que:

MAC → ?

IPv4 → 172.31.255.2

11 2018-11-08 10:11:27,634488 10.0.0.12	172.31.255.2	DNS	74 Standard query 0x0176 A webserver.test
12 2018-11-08 10:11:27,635756 10.0.0.12	172.31.255.2	DNS	74 Standard query 0x44ff AAAA webserver.test
13 2018-11-08 10:11:27,639018 172.31.255.2	10.0.0.12	DNS	90 Standard query response 0x0176 A webserver.test A 172.16.143.2
14 2018-11-08 10:11:27,642764 172.31.255.2	10.0.0.12	DNS	90 Standard query response 0x44ff AAAA webserver.test A 172.16.143.2

Figura 9: Comunicação *DNS* para tradução de nome *webserver.test* para *IPv4* (172.16.143.2)

Continuando, foi aberto o segundo conjunto de pacotes capturados, “3-4.pcap”, para se descobrir mais a respeito do dispositivo 3 e das posições dos dispositivos até agora descobertos (incluindo o 3). Desse modo, tem-se a parte apresentada abaixo sendo explorada e, descobriu-se o que se demonstra mais adiante:

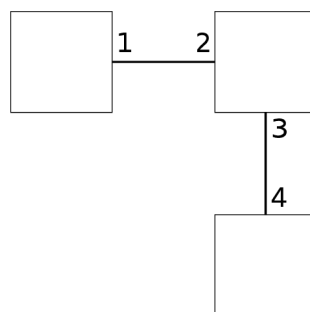


Figura 10: Parte explorada da topologia até o momento

Tendo a micro-topologia apresentada acima, é possível afirmar, trivialmente, que o dispositivo 2 (de interface 4) é um host, assim como o dispositivo 1.

Aberto o “pcap” a ser analisado, nota-se a presença somente dos pacotes apresentados na Figura 11:

No.	Time	Source	Destination	Protoc	Len	Info
1	2018-11-08 10:11:20,491690	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x9e3a9a1e
2	2018-11-08 10:11:20,492751	10.0.0.1	255.255.255.255	DHCP	323	DHCP Offer - Transaction ID 0x9e3a9a1e
3	2018-11-08 10:11:20,494005	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x9e3a9a1e
4	2018-11-08 10:11:20,494696	10.0.0.1	255.255.255.255	DHCP	323	DHCP ACK - Transaction ID 0x9e3a9a1e
5	2018-11-08 10:11:21,615130	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xfa0b0f5b
6	2018-11-08 10:11:21,617516	10.0.0.1	255.255.255.255	DHCP	323	DHCP Offer - Transaction ID 0xfa0b0f5b
7	2018-11-08 10:11:21,617955	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xfa0b0f5b
8	2018-11-08 10:11:21,619745	10.0.0.1	255.255.255.255	DHCP	323	DHCP ACK - Transaction ID 0xfa0b0f5b
9	2018-11-08 10:11:27,631790	00:00:00_00:00:02	Broadcast	ARP	42	Who has 10.0.0.1? Tell 10.0.0.12

Figura 11: Pacotes em “3-4.pcap”

Nessa figura, percebe-se imediatamente que o processo *DHCP*, explicado no desenvolvimento a respeito dos dispositivos 1 e 2, é aqui também apresentado, o que demonstra que os dispositivos 2 e 3 estão na mesma rede. Além disso, nota-se que os pacotes que não são enviados em *broadcast* (pacotes *TCP* e resposta *ARP*) trocados internamente à rede ou entre redes não são reconhecidos no enlace 3-4. Isso indica que o dispositivo que contém as interfaces 2 e 3 é um *switch*, o qual se responsabiliza por repassar corretamente os pacotes para os devidos nós da rede. Logo, descobriu-se, portanto, um dispositivo 5 na mesma rede que 1 e 2, que está ligado entre estes conforme a figura abaixo:

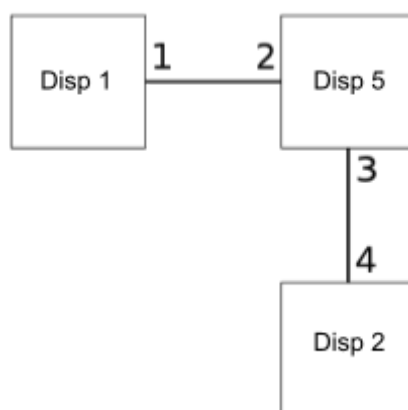


Figura 12: Parte inteiramente reconhecida da topologia até o momento

Tudo o que foi explicado anteriormente significa que o dispositivo 3 está em algum dos próximos nós a serem analisados, possivelmente no próximo (participante já de “5-6.pcap”).

Dando sequência ao procedimento, analisando-se a captura “5-6.pcap”, pode-se notar que os pacotes apresentados nessa captura são exatamente os mesmos apresentados em “1-2.pcap”, o que significa que o dispositivo 3 é provavelmente o que está ligado ao 5 pela interface 6, conforme a figura abaixo. No entanto, é possível que esse dispositivo seja um *switch* e, nesse caso, o dispositivo 3 seria outro, ainda.

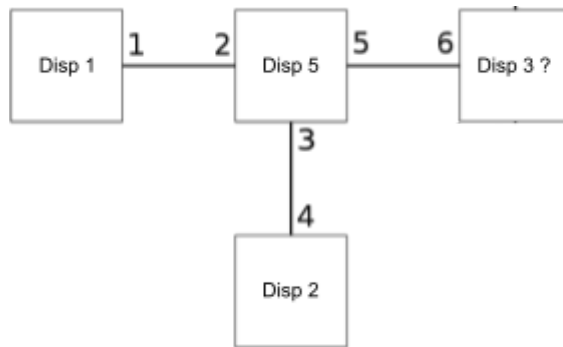


Figura 13: Parte inteiramente estudada da topologia com o conhecimento de “5-6.pcap”

Continuando, embora conheçamos a possibilidade de o dispositivo ligado à interface 6 ser o dispositivo 3 e ser um roteador, segue-se com um estudo de outra interface ligada a esse dispositivo. Seja essa, a interface 7 (“7-8.pcap”), o que expande nossa zona de conhecimento a:

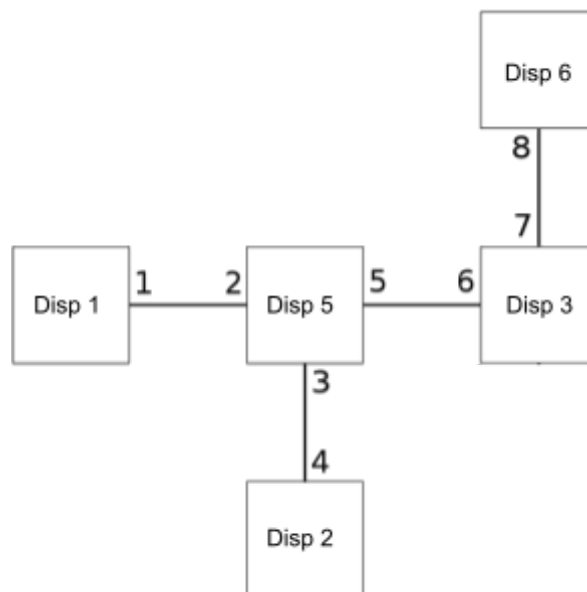


Figura 14: Parte inteiramente estudada da topologia com o conhecimento de “7-8.pcap”

Na figura acima, deve-se notar que o dispositivo que era anteriormente uma incógnita é, agora, dado como dispositivo 3. Isso pode ser feito, por causa dos motivos que se seguem após a Figura 15:

1	2018-11-08	10:11:27,634547	00:00:00_00:00:04	Broadcast	ARP	42	Who has 172.31.255.2? Tell 172.31.255.1
2	2018-11-08	10:11:27,634565	00:00:00_00:00:01	00:00:00_00:00:04	ARP	42	172.31.255.2 is at 00:00:00:00:00:01
3	2018-11-08	10:11:27,634569	10.0.0.12	172.31.255.2	DNS	74	Standard query 0x0176 A webserver.test
4	2018-11-08	10:11:27,635776	10.0.0.12	172.31.255.2	DNS	74	Standard query 0x44ff AAAA webserver.test
5	2018-11-08	10:11:27,638947	172.31.255.2	10.0.0.12	DNS	90	Standard query response 0x0176 A webserver.test A 172.16.143.2
6	2018-11-08	10:11:27,642736	172.31.255.2	10.0.0.12	DNS	90	Standard query response 0x44ff AAAA webserver.test A 172.16.143.2

Figura 15: Pacotes em “7-8.pcap”

Na figura acima, pode-se notar que os únicos pacotes que circulam entre as interfaces 7 e 8 são dois de *ARP* e alguns de *DNS*. Nesse sentido, analisando de início os pacotes ligados ao *DNS*, pode-se afirmar que o dispositivo 172.31.255.2 está ligado ao dispositivo de interfaces 6 e 7 por esta

segunda interface. Além disso, sabe-se que ele está ligado somente a esse dispositivo, logo, esse dispositivo é um *switch* ou um roteador. Por fim, notando-se que o *ARP* foi feito entre dois dispositivos de IPs que não condizem com a rede anteriormente analisada e que esse *ARP* busca pelo servidor *DNS* com o qual o dispositivo 1 (da outra rede) tenta se comunicar, pode-se afirmar que o dispositivo em questão é um roteador e, por consequência, é o dispositivo anteriormente chamado de 3.

No contexto apresentado, portanto, tem-se mais algumas informações a respeito do dispositivo 3. São elas:

- **Dispositivo 3:**

Por meio das análises anteriores e das figuras abaixo, pode-se afirmar que:

MAC interface 6 → f6:b8:e1:de:f7:38

MAC interface 7 → 00:00:00:00:00:04

IPv4 interface 6 → 10.0.0.1

IPv4 interface 7 → 172.31.255.1

Além disso, ainda até a captura no enlace 7-8, é possível afirmar, trivialmente, que o dispositivo 6 é um *host* servidor *DNS*, sendo ele, então, o que se chamou anteriormente de dispositivo *DNS*. A respeito dele, tem-se:

- **Dispositivo *DNS* (6):**

Com base na figura apresentada abaixo e na explicação dada acima, sabe-se que:

MAC → 00:00:00:00:00:01

IPv4 → 172.31.255.2

Passado o procedimento anterior, seguiu-se para o próximo arquivo de captura, o “9-10.pcap”. Nele, espera-se naturalmente uma outra rede definida pelo roteador (dispositivo 3), porém, é possível que existam mais roteadores na topologia.

Aberto o novo “pcap” a ser analisado, nota-se imediatamente a presença de mensagens *BGP*, Border Gate Protocol, responsável pela sincronização de rotas entre roteadores (para comunicação inter-redes). Logo, é possível afirmar que existe mais um roteador na topologia. Além disso, pela mensagem *BGP* “update” apresentada na figura a seguir, enviada de 192.168.1.1 para 192.168.1.2, faz-se explícito que o primeiro IPv4 citado é da interface 9 do dispositivo 3 já discutido. Isso porque, conforme se observa na figura, entre as informações do protocolo contidas no pacote, está o alcance do roteador que o emitiu e esse alcance inclui três redes, das quais, duas são as já estudadas.

```

* Frame 20: 129 bytes on wire (1032 bits), 129 bytes captured (1032 bits)
* Ethernet II, Src: 32:06:37:2d:43:a6 (32:06:37:2d:43:a6), Dst: 00:00:00_00:00:05 (00:00:00:00:00:05)
  * Destination: 00:00:00_00:00:05 (00:00:00:00:00:05)
  * Source: 32:06:37:2d:43:a6 (32:06:37:2d:43:a6)
  Type: IPv4 (0x0800)
  [Stream index: 1]
* Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2
* Transmission Control Protocol, Src Port: 179, Dst Port: 39958, Seq: 92, Ack: 151, Len: 63
* Border Gateway Protocol - UPDATE Message
  Marker: ffffffffffffffffffffffffffffffffff
  Length: 63
  Type: UPDATE Message (2)
  Withdrawn Routes Length: 0
  Total Path Attribute Length: 28
  - Path attributes
    * Path Attribute - ORIGIN: INCOMPLETE
    * Path Attribute - AS_PATH: 100
    * Path Attribute - NEXT_HOP: 192.168.1.1
    * Path Attribute - MULTIPLE NEXT_HOP: 1
  Network Layer Reachability Information (NLRI)
    * 10.0.0.0/24
    * 192.168.1.0/24
    * 172.31.255.0/24

```

Figura 16: Informações de pacote BGP update emitido pelo dispositivo 3

Além de se reconhecer a nova rede definida pelo roteador já conhecido (dispositivo 3) e por um novo, que será o dispositivo 7, é possível ver o endereço MAC da nova interface do dispositivo 3. Ademais, na Figura 17, ainda representante do pacote apresentado, vê-se o valor do IPv4 dessa última interface.

```
Source Address: 192.168.1.1
Destination Address: 192.168.1.2
```

Figura 17: Informações da camada de rede provindas do pacote já apresentado

Com o que se mostra acima, pode-se complementar as informações a respeito do dispositivo 3, que será chamado, finalmente, de roteador 1. Feito isso, apresenta-se também uma nova figura com a parte da topologia reconhecida até este passo:

- Roteador 1:

Conforme explicado durante todo o curso deste relatório, as informações a respeito deste roteador são, definitivamente:

```
MAC interface 6 → f6:b8:e1:de:f7:38
MAC interface 7 → 00:00:00:00:00:04
MAC interface 9 → 32:06:37:2d:43:a6
IPv4 interface 6 → 10.0.0.1
IPv4 interface 7 → 172.31.255.1
IPv4 interface 9 → 192.168.1.1
```

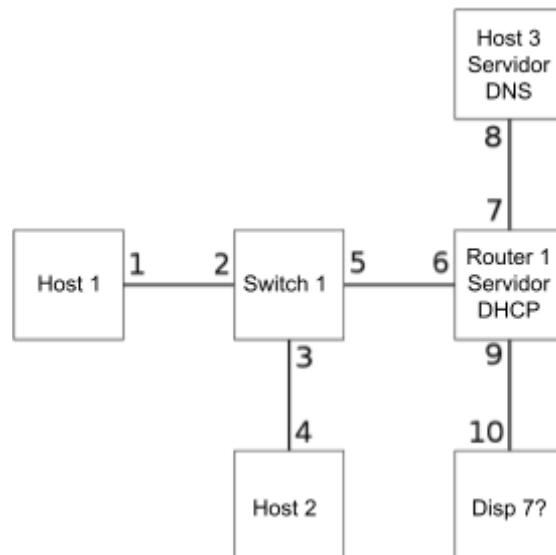



Figura 18: Topologia conhecida até “9-10.pcap”

Do mesmo modo quando se estudava a possibilidade do primeiro roteador descoberto ser o dispositivo 3, ou seja, ser um roteador e não um *switch*, estudar-se-á a possibilidade do dispositivo de interface 10 ser o dispositivo 7, no entanto, isso só é garantido a partir da análise das capturas da interface 11. Ainda assim, já é possível determinar algumas características do dispositivo 7. Para tanto, usou-se as Figuras 16 e 17 novamente, como forma de se obter IPv4 e MAC do dispositivo 7:

- Dispositivo 7:

Conforme explicado durante todo o curso deste relatório, as informações a respeito deste roteador são, definitivamente:

MAC→ 00:00:00:00:00:05

IPv4→ 192.168.1.2

Estudando em sequência o arquivo “11-12.pcap”, observam-se de início, novamente, dois pacotes *ARP*. Tais pacotes estão voltados ao reconhecimento do *MAC* do dispositivo de IPv4 172.16.143.2, que conforme já se sabe é um host com o qual o dispositivo 1 (também host) executa conexão *TCP*. Sendo assim, o dispositivo emissor tem de ser o roteador da rede, pois não há espaço para outro host na topologia da Figura 1. Nesse sentido, mesmo ignorando a topologia da primeira figura, é possível ver que o pacote *ARP* está relacionado, pelo momento em que foi enviado, aos pacotes *TCP* que vão do dispositivo 1 ao 4, sendo uma busca do roteador pelo dispositivo 4 para repassar os pacotes *TCP* para ele. Desse modo, como o IPv4 da interface 11 do dispositivo de interfaces 10 e 11 é diferente do IPv4 da interface 10, pode-se concluir que esse dispositivo é o segundo roteador da topologia, sendo, por conseguinte, o dispositivo 7. Logo, a respeito de tal dispositivo, pode-se mostrar que:

- **Roteador 2 (Dispositivo 7):**

Tendo em vista o que se explica acima e a figura abaixo, afirma-se que:

MAC interface 10 → 00:00:00:00:00:05

MAC interface 11 → be:61:96:2b:2d:5f

IPv4 interface 10 → 192.168.1.2

IPv4 interface 11 → 172.16.143.1

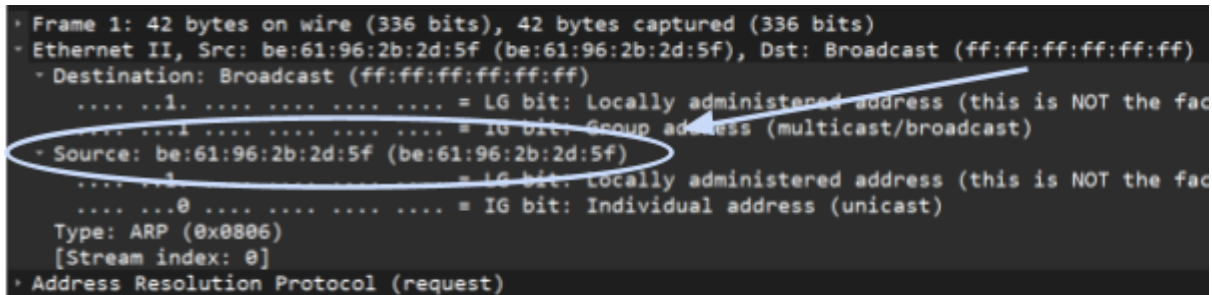


Figura 19: Informações do pacote broadcast ARP feito por 172.16.143.1 (dispositivo 7, roteador 2)

Além disso, é possível descobrir, também, o endereço MAC do dispositivo 4 (host 4), estudando o pacote de resposta *ARP* que esse host envia ao roteador 2. Para tanto, pode-se ver a figura a seguir, que apresenta tal endereço em destaque entre informações do pacote em questão.

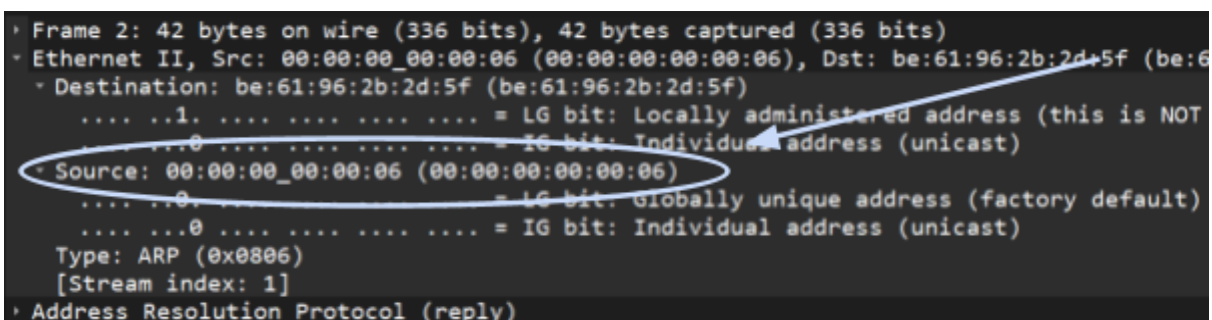


Figura 20: Informações do pacote ARP de resposta enviado pelo dispositivo 4 (host 4)

Com o que se explicou, pode-se desenvolver:

- **Host 4 (Dispositivo 4):**

Baseado no que se afirma acima, tem-se:

MAC → 00:00:00:00:00:06

IPv4 → 172.16.143.2

Quanto ao dispositivo restante, abrindo-se o próximo arquivo de captura (“13-14.pcap”), como no caso da abertura do “5-6.pcap” após a abertura de “1-2.pcap”, notou-se que os pacotes capturados neste novo enlace a ser analisado são exatamente os mesmos que aqueles capturados no enlace 11-12. Logo, de modo equivalente ao caso anterior citado, pode-se concluir que o dispositivo cujas interfaces são 12 e 13 é um *switch*.

Finalmente, conforme se observa nos pacotes *TCP* que transitam entre os hosts 1 e 4 (Figura 21 como ilustração), o roteador 1 realiza tradução *NAT* na interface com IPv4 192.168.1.1. Isso pode

ser afirmado, pois os IPv4s que deveriam ser 10.0.0.12 nos pacotes *TCP* são substituídos por 192.168.1.1 em todos os dispositivos de rede que partem desta última interface. Ou seja, os pacotes que são repassados ou recebidos pela interface 192.168.1.1 do roteador 1, têm esse endereço como IPv4 referente, respectivamente, ao emissor e ao receptor.

22	2018-11-08	10:11:27,645134	192.168.1.1	172.16.143.2	TCP	74	44824 → 80	[SYN]	Seq=0	Win=2
23	2018-11-08	10:11:27,648041	172.16.143.2	192.168.1.1	TCP	74	80 → 44824	[SYN, ACK]	Seq=0	
24	2018-11-08	10:11:27,648914	192.168.1.1	172.16.143.2	TCP	66	44824 → 80	[ACK]	Seq=1	Ack=1
25	2018-11-08	10:11:27,650113	192.168.1.1	172.16.143.2	HTTP	188	GET /index.html	HTTP/1.1		

Figura 21: Pacotes TCP que trafegam entre os hosts 1 e 4 capturados no enlace 9-10

Resultados)

Feito todo o processo em destaque, chegou-se à topologia final da rede que se apresenta abaixo:

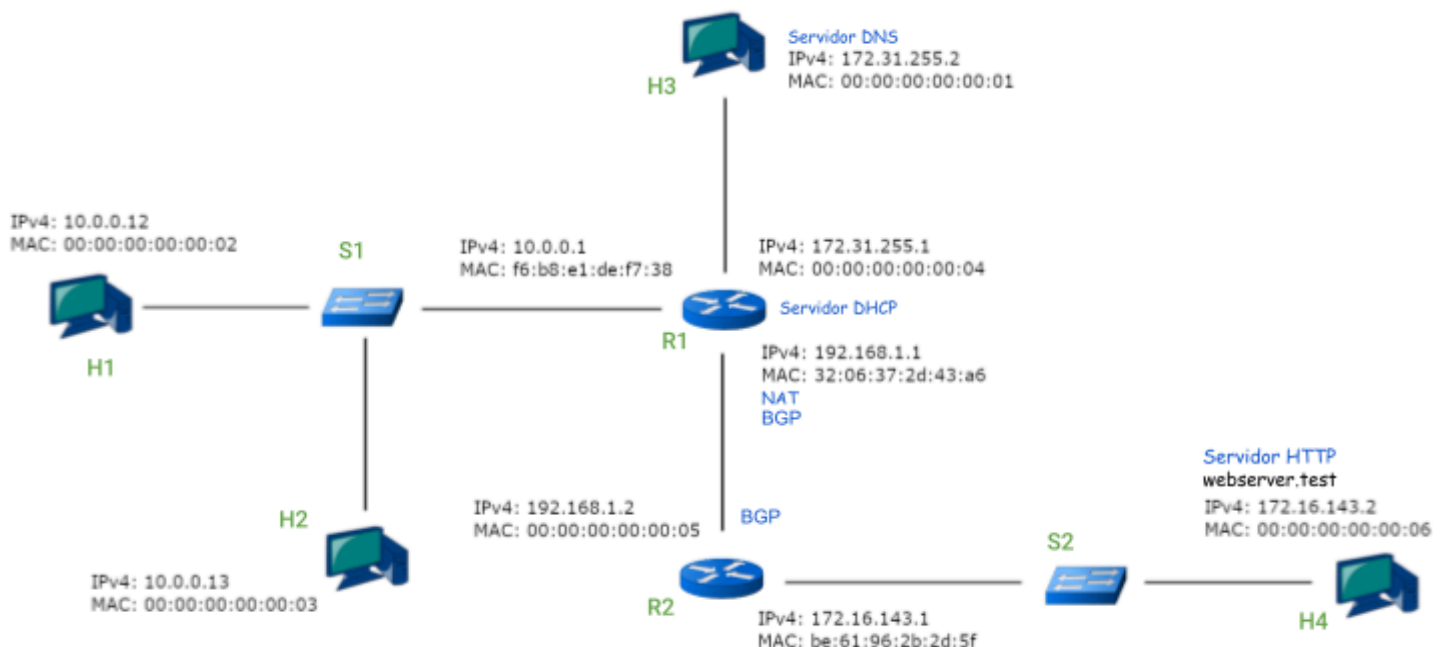


Figura 22: Versão final da rede, com todas suas sub-redes e os endereços de cada um de seus nós

Foi feito também, um diagrama completo com os pacotes passados entre os nós da topologia estudada. O resultado disso foi o que se apresenta na *Figura 23* após breves destaques abaixo.

Cabe destacar que o diagrama apresentado acima está contido em um documento *JPG* enviado juntamente com este relatório. Nesse documento, é possível observar melhor os pacotes, uma vez que, por ser um único diagrama, a fonte das letras ficou bastante reduzida. Além disso, é importante ressaltar que, as reticências no diagrama foram usadas para suprimir pacotes TCP do protocolo *BGP*, facilitando o entendimento da sequência de pacotes *BGP* e, no terceiro caso, para evitar a repetição de parte da sequência em que se tinha um TCP para um lado e um para o outro.

