

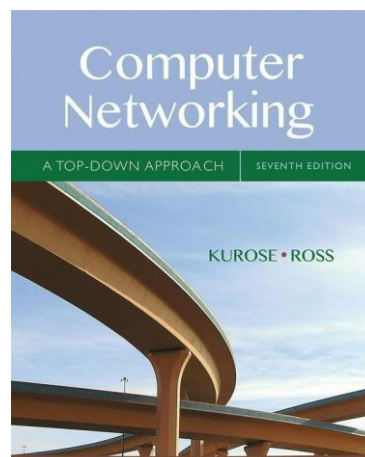


## Wireshark Lab: DHCP v7.0

Supplement to *Computer Networking: A Top-Down Approach*, 7<sup>th</sup> ed., J.F. Kurose and K.W. Ross

*"Tell me and I forget. Show me and I remember. Involve me and I understand."* Chinese proverb

© 2005-2016, J.F Kurose and K.W. Ross, All Rights Reserved



Nesta aula prática, daremos uma rápida olhada no DHCP. Lembre-se de que o DHCP é usado extensivamente em LANs corporativas, universitárias e de rede doméstica e sem fio para atribuir dinamicamente endereços IP a hosts (assim como para configurar outras informações de configuração de rede).

Esta aula prática é breve, pois só examinaremos os pacotes DHCP capturados por um *host*. Se você também tiver acesso administrativo (root) ao seu servidor DHCP, talvez queira repetir esta prática após fazer algumas alterações de configuração (como o tempo de concessão). Se você tiver um roteador em casa, você provavelmente poderá configurar seu servidor DHCP. Porque muitas máquinas linux / Unix (especialmente aquelas que servem muitos usuários) têm um endereço IP estático e porque manipular o DHCP em tais máquinas geralmente requer privilégios de superusuário, aqui apresentamos uma versão windows desta aula prática.

### EXPERIMENTO DHCP

Para observar DHCP em ação, executaremos vários comandos relacionados ao DHCP e capturaremos as mensagens DHCP trocadas como resultado da execução desses comandos. Faça o que se pede:

1. Comece abrindo o aplicativo de prompt de comando do Windows (que pode ser encontrado na sua pasta Acessórios). Conforme mostrado na Figura 1, insira "ipconfig /release". O executável para ipconfig está em C:\windows\system32. Este comando libera seu endereço IP atual, de modo que o endereço IP do seu host se torne 0.0.0.0.

```
C:\Users\davi->ipconfig /release

Configuração de IP do Windows

Adaptador Ethernet Ethernet:

    Sufixo DNS específico de conexão. . . . . : 
    Endereço IPv6 de link local . . . . . : fe80::d004:5927:f6c2:cbfa%3
    Gateway Padrão. . . . . :
```

2. Inicie o sniffer de pacotes Wireshark e comece a captura de pacotes do Wireshark.



## Lista 12 DHCP

9	1.218861	127.0.0.1	127.0.0.1	HTTP	584 HTTP/1.0 200 OK
10	1.218875	127.0.0.1	127.0.0.1	TCP	44 49301 → 1120 [ACK] Seq=157 Ack=541 Win=2160640 Len=0
11	1.218890	127.0.0.1	127.0.0.1	TCP	44 1120 → 49301 [FIN, ACK] Seq=541 Ack=157 Win=16228 Len=0
12	1.218896	127.0.0.1	127.0.0.1	TCP	44 49301 → 1120 [ACK] Seq=157 Ack=542 Win=2160640 Len=0
13	1.218903	127.0.0.1	127.0.0.1	TCP	44 49301 → 1120 [FIN, ACK] Seq=157 Ack=542 Win=2160640 Len=0
14	1.218955	127.0.0.1	127.0.0.1	TCP	44 1120 → 49301 [ACK] Seq=542 Ack=158 Win=16228 Len=0
15	1.994546	192.168.0.107	224.0.0.251	MDNS	77 Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
16	1.994694	fe80::d004:5927:f6c2::fb	ff02::fb	MDNS	97 Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
17	2.058060	192.168.0.107	239.255.255.250	SSDP	157 M-SEARCH * HTTP/1.1
18	3.993573	192.168.0.107	224.0.0.251	MDNS	77 Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question

3. Agora volte para o prompt de comando do Windows e digite "ipconfig/renew". Isso instrui seu host a obter uma configuração de rede, incluindo um novo endereço IP. Na Figura 1, o host obtém o endereço IP 192.168.1.108

```
C:\Users\davi->ipconfig /renew

Configuração de IP do Windows

Adaptador Ethernet Ethernet:

    Sufixo DNS específico de conexão. . . . . : 
    Endereço IPv6 de link local . . . . . : fe80::d004:5927:f6c2:cbfa%3
    Endereço IPv4. . . . . : 192.168.0.107
    Máscara de Sub-rede . . . . . : 255.255.255.0
    Gateway Padrão. . . . . : 192.168.0.1
```

4. Aguarde até que o "ipconfig/renew" tenha terminado. Em seguida, digite o mesmo comando "ipconfig/renew" novamente.

```
C:\Users\davi->ipconfig /renew

Configuração de IP do Windows

Adaptador Ethernet Ethernet:

    Sufixo DNS específico de conexão. . . . . : 
    Endereço IPv6 de link local . . . . . : fe80::d004:5927:f6c2:cbfa%3
    Endereço IPv4. . . . . : 192.168.0.107
    Máscara de Sub-rede . . . . . : 255.255.255.0
    Gateway Padrão. . . . . : 192.168.0.1
```

5. Quando o segundo "ipconfig/renew" terminar, digite o comando "ipconfig /release" para liberar o endereço IP previamente atribuído ao seu computador.

```
C:\Users\davi->ipconfig /release

Configuração de IP do Windows

Adaptador Ethernet Ethernet:

    Sufixo DNS específico de conexão. . . . . : 
    Endereço IPv6 de link local . . . . . : fe80::d004:5927:f6c2:cbfa%3
    Gateway Padrão. . . . . :
```

6. Finalmente, digite "ipconfig /renew" para ser novamente atribuído um endereço IP para o seu computador.



## Lista 12 DHCP

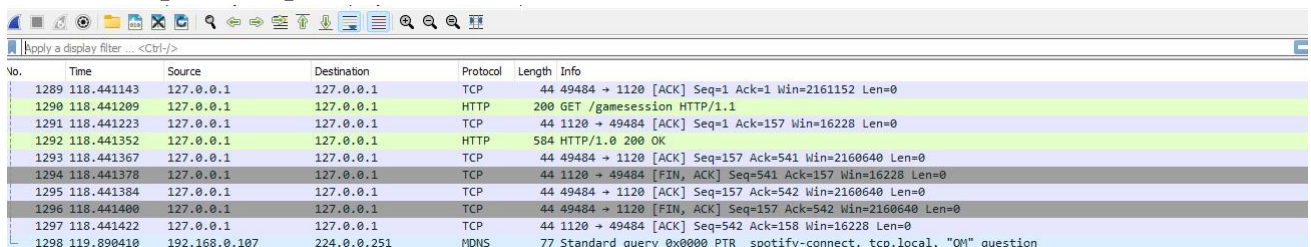
```
C:\Users\davi->ipconfig /renew
```

Configuração de IP do Windows

Adaptador Ethernet Ethernet:

```
Sufixo DNS específico de conexão. . . . . :  
Endereço IPv6 de link local . . . . . : fe80::d004:5927:f6c2:cbfa%3  
Endereço IPv4. . . . . : 192.168.0.107  
Máscara de Sub-rede . . . . . : 255.255.255.0  
Gateway Padrão. . . . . : 192.168.0.1
```

### 7. Pare a captura de pacotes do Wireshark.



No.	Time	Source	Destination	Protocol	Length	Info
1289	118.441143	127.0.0.1	127.0.0.1	TCP	44	49484 → 1120 [ACK] Seq=1 Ack=1 Win=2161152 Len=0
1290	118.441209	127.0.0.1	127.0.0.1	HTTP	200	GET /gamesession HTTP/1.1
1291	118.441223	127.0.0.1	127.0.0.1	TCP	44	1120 → 49484 [ACK] Seq=1 Ack=157 Win=16228 Len=0
1292	118.441352	127.0.0.1	127.0.0.1	HTTP	584	HTTP/1.0 200 OK
1293	118.441367	127.0.0.1	127.0.0.1	TCP	44	49484 → 1120 [ACK] Seq=157 Ack=541 Win=2160640 Len=0
1294	118.441378	127.0.0.1	127.0.0.1	TCP	44	1120 → 49484 [FIN, ACK] Seq=541 Ack=157 Win=16228 Len=0
1295	118.441384	127.0.0.1	127.0.0.1	TCP	44	49484 → 1120 [ACK] Seq=157 Ack=542 Win=2160640 Len=0
1296	118.441400	127.0.0.1	127.0.0.1	TCP	44	49484 → 1120 [FIN, ACK] Seq=157 Ack=542 Win=2160640 Len=0
1297	118.441422	127.0.0.1	127.0.0.1	TCP	44	1120 → 49484 [ACK] Seq=542 Ack=158 Win=16228 Len=0
1298	119.890410	192.168.0.107	224.0.0.251	MDNS	77	Standard query 0x0000 PTR _spotify-connect_tcp.local, "QM" question



OBS.: No linux empregue: dhclient -v -r **enp3s0** e dhclient **enp3s0** (release e renew na interface enp3s0).

```
C:\WINDOWS\SYSTEM32>ipconfig/release
Windows IP Configuration

IP Address for adapter Local Area Connection has already been released.

C:\WINDOWS\SYSTEM32>ipconfig/renew
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : ne2.client2.attbi.com
    IP Address. . . . . : 192.168.1.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\WINDOWS\SYSTEM32>ipconfig/renew
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : ne2.client2.attbi.com
    IP Address. . . . . : 192.168.1.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\WINDOWS\SYSTEM32>ipconfig/release
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    IP Address. . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . :

C:\WINDOWS\SYSTEM32>ipconfig/renew
Windows IP Configuration

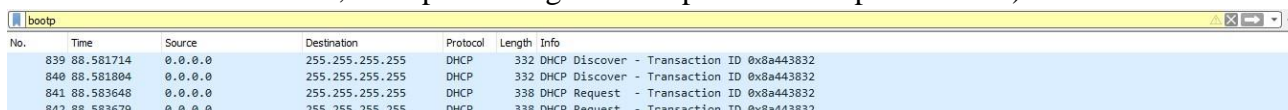
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : ne2.client2.attbi.com
    IP Address. . . . . : 192.168.1.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\WINDOWS\SYSTEM32>_
```

**Figure 1** Janela de prompt de comando mostrando a sequência de comandos ipconfig que você deve inserir.

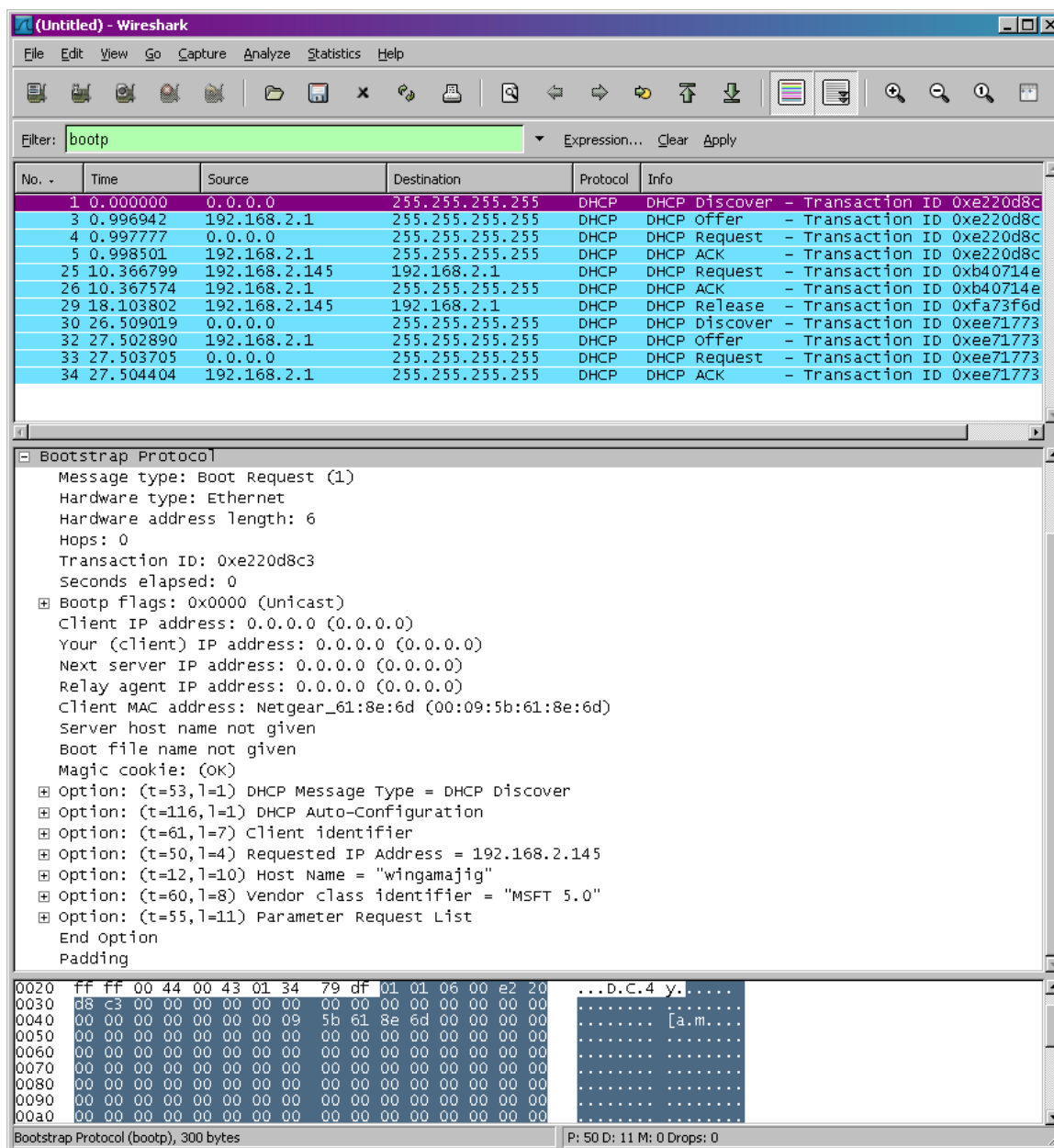
Agora vamos dar uma olhada na janela Wireshark resultante. Para ver apenas os pacotes DHCP, entre no campo de filtro "bootp". (DHCP deriva de um protocolo mais antigo chamado BOOTP. Ambos BOOTP e DHCP usam os mesmos números de porta, 67 e 68. Para ver pacotes DHCP na versão atual do Wireshark, você precisa digitar "bootp" e não "dhcp" no filtro .)



No.	Time	Source	Destination	Protocol	Length	Info
839	88.581714	0.0.0.0	255.255.255.255	DHCP	332	DHCP Discover - Transaction ID 0x8a443832
840	88.581804	0.0.0.0	255.255.255.255	DHCP	332	DHCP Discover - Transaction ID 0x8a443832
841	88.583648	0.0.0.0	255.255.255.255	DHCP	338	DHCP Request - Transaction ID 0x8a443832
842	88.583679	0.0.0.0	255.255.255.255	DHCP	338	DHCP Request - Transaction ID 0x8a443832



Na Figura 2, vemos que o primeiro comando ipconfig/renew gerou quatro pacotes DHCP: um pacote DHCP Discover, um pacote DHCP Offer, um pacote DHCP Request e um pacote DHCP ACK.



**Figure 2** Janela do Wireshark com o primeiro pacote DHCP - o pacote DHCP Discover - expandido.

**1. As mensagens DHCP são enviadas através de UDP ou TCP?**

UDP



## Lista 12 DHCP

839	88.581714	0.0.0.0	255.255.255.255	DHC
840	88.581804	0.0.0.0	255.255.255.255	DHC
841	88.583648	0.0.0.0	255.255.255.255	DHC
842	88.583679	0.0.0.0	255.255.255.255	DHC

```
> Frame 839: 332 bytes on wire (2656 bits), 332 bytes captured (2656) on interface 0
> Null/Loopback
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
  Source Port: 68
  Destination Port: 67
  Length: 308
  Checksum: 0xcae9 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 23]
  > [Timestamps]
  UDP payload (300 bytes)
> Dynamic Host Configuration Protocol (Discover)
```

2. Desenhe um datagrama de temporização ilustrando a sequência da primeira troca de DHCP de quatro pacotes de DISCOVER/OFFER /REQUEST /ACK entre o cliente e o servidor. Para cada pacote, indique os números de porta de origem e de destino.

Pacote DISCOVER:

Porta de origem: Não definida (0)  
Porta de destino: 67 (Servidor DHCP)  
Pacote OFFER:

Porta de origem: 67 (Servidor DHCP)  
Porta de destino: 68 (Cliente DHCP)  
Pacote REQUEST:

Porta de origem: 68 (Cliente DHCP)  
Porta de destino: 67 (Servidor DHCP)  
Pacote ACK:

Porta de origem: 67 (Servidor DHCP)  
Porta de destino: 68 (Cliente DHCP)

3. Qual é o endereço da camada de enlace (por exemplo, Ethernet) do seu host?

```
Client MAC address: ASUSTek_7b:c4:b7 (3c:7c:3f:7b:c4:b7)
```



**4. Quais valores na mensagem de DISCOVER de DHCP diferenciam da mensagem de REQUEST DHCP?**

Na troca de mensagens DHCP, existem diferenças nos valores dos campos entre uma mensagem DISCOVER e uma mensagem REQUEST.

Tipo de mensagem (opção DHCP Message Type):

DISCOVER: Valor 1 (DHCP Discover)

REQUEST: Valor 3 (DHCP Request)

Endereço IP solicitado (opção Requested IP Address):

DISCOVER: Normalmente definido como 0.0.0.0, indicando que o cliente não tem um endereço IP específico em mente.

REQUEST: O cliente especifica o endereço IP que foi oferecido pelo servidor DHCP no pacote OFFER anteriormente.

Endereço do servidor DHCP (opção DHCP Server Identifier):

DISCOVER: Normalmente definido como 0.0.0.0, indicando que o cliente está aberto para receber uma oferta de qualquer servidor DHCP disponível.

REQUEST: O cliente define o endereço IP do servidor DHCP específico para o qual está enviando a solicitação.

**5. Qual é o valor do Transaction-ID em cada uma das quatro primeiras mensagens de DHCP (Discover / Offer / Request / ACK)? Qual é a finalidade do campo Transaction-ID?**

O campo Transaction-ID (Identificador de Transação) é um campo importante nas mensagens DHCP. Ele é usado para associar as respostas do servidor DHCP às solicitações correspondentes do cliente DHCP. Cada mensagem DHCP tem um valor único no campo Transaction-ID para identificar uma transação específica. Aqui estão os valores do Transaction-ID nas quatro primeiras mensagens de DHCP (DISCOVER, OFFER, REQUEST, ACK):

DISCOVER:

Valor do Transaction-ID: É um valor aleatório gerado pelo cliente DHCP.

OFFER:

Valor do Transaction-ID: É o mesmo valor do Transaction-ID presente na mensagem DISCOVER enviada pelo cliente. O servidor DHCP copia esse valor para a resposta OFFER.

REQUEST:

Valor do Transaction-ID: É o mesmo valor do Transaction-ID presente na mensagem DISCOVER ou OFFER, dependendo de qual mensagem o cliente está respondendo. O



cliente DHCP copia esse valor da mensagem DISCOVER ou OFFER para a solicitação REQUEST.

ACK (Acknowledgment):

Valor do Transaction-ID: É o mesmo valor do Transaction-ID presente na mensagem REQUEST. O servidor DHCP copia esse valor para a resposta ACK para indicar que o endereço IP foi alocado com sucesso ao cliente.

O campo Transaction-ID é essencial para garantir que as mensagens DHCP sejam associadas corretamente entre o cliente e o servidor durante todo o processo de atribuição de endereços IP. Ele permite que as respostas do servidor sejam mapeadas para as solicitações correspondentes do cliente, mantendo a integridade da transação DHCP.

- 6. Um host usa DHCP para obter um endereço IP. O endereço IP de um host não é confirmado até o final da troca de quatro mensagens! Para cada uma das quatro mensagens DHCP (Discover / Offer / Request / ACK DHCP), indique os endereços IP de origem e destino que são transportados no datagrama IP encapsulante.**

Ao longo do processo de troca de mensagens DHCP (DISCOVER, OFFER, REQUEST e ACK), o endereço IP de origem e destino no datagrama IP encapsulante varia em cada mensagem.

DISCOVER:

Endereço IP de origem: 0.0.0.0 (indicando que o cliente ainda não tem um endereço IP atribuído)

Endereço IP de destino: 255.255.255.255 (endereço de broadcast) ou o endereço de broadcast de sub-rede específico, dependendo da configuração da rede.

OFFER:

Endereço IP de origem: Endereço IP do servidor DHCP que oferece o endereço ao cliente.

Endereço IP de destino: 255.255.255.255 (endereço de broadcast) ou o endereço de broadcast de sub-rede específico, dependendo da configuração da rede.

REQUEST:

Endereço IP de origem: 0.0.0.0 (indicando que o cliente ainda não tem um endereço IP atribuído) ou o endereço IP atual do cliente.

Endereço IP de destino: 255.255.255.255 (endereço de broadcast) ou o endereço de broadcast de sub-rede específico, dependendo da configuração da rede.

ACK (Acknowledgment):

Endereço IP de origem: Endereço IP do servidor DHCP que confirma a alocação do endereço ao cliente.

Endereço IP de destino: Endereço IP do cliente que solicitou o endereço.

Vale ressaltar que, durante a troca de mensagens DHCP, o endereço IP de origem do cliente pode mudar à medida que ele passa a ter um endereço IP atribuído pelo servidor. Além disso, o endereço IP de destino pode variar dependendo do tipo de broadcast utilizado (broadcast direto ou broadcast limitado à sub-rede). As informações acima são baseadas em um cenário típico de DHCP, mas podem variar dependendo da configuração da rede.

- 7. Qual é o endereço IP do seu servidor DHCP?**





### Configuração de IP do Windows

Adaptador Ethernet Ethernet:

```
Sufixo DNS específico de conexão. . . . . :  
Endereço IPv6 de link local . . . . . : fe80::d004:5927:f6c2:cbfa%3  
Endereço IPv4. . . . . : 192.168.0.107  
Máscara de Sub-rede . . . . . : 255.255.255.0  
Gateway Padrão. . . . . : 192.168.0.1
```

8. Qual o endereço IP que o servidor DHCP oferece ao seu host na mensagem DHCP Offer? Indique qual mensagem DHCP contém o endereço DHCP oferecido.

```
C:\Users\davi->ipconfig /renew
```

### Configuração de IP do Windows

Adaptador Ethernet Ethernet:

```
Sufixo DNS específico de conexão. . . . . :  
Endereço IPv6 de link local . . . . . : fe80::d004:5927:f6c2:cbfa%3  
Endereço IPv4. . . . . : 192.168.0.107  
Máscara de Sub-rede . . . . . : 255.255.255.0  
Gateway Padrão. . . . . : 192.168.0.1
```

9. Explique a finalidade das linhas de máscara de sub-rede e roteador na mensagem de OFFER DHCP.

Na mensagem de OFFER DHCP, as linhas de máscara de sub-rede (Subnet Mask) e roteador (Router) têm a seguinte finalidade:

Máscara de sub-rede (Subnet Mask):

A máscara de sub-rede é um valor de 32 bits que define qual parte de um endereço IP pertence à rede e qual parte pertence aos dispositivos específicos na rede (hosts). A máscara de sub-rede permite que os dispositivos identifiquem e segmentem corretamente os pacotes de rede. Na mensagem de OFFER DHCP, a linha de máscara de sub-rede especifica a máscara de sub-rede que o cliente DHCP deve usar para configurar sua interface de rede. Essa informação é essencial para que o cliente entenda como interpretar corretamente os endereços IP na rede.

Roteador (Router):

A linha de roteador na mensagem de OFFER DHCP fornece ao cliente DHCP o endereço IP do roteador padrão (gateway) que deve ser usado para encaminhar pacotes para redes externas. O roteador é responsável por encaminhar o tráfego entre redes diferentes. Ao fornecer o endereço do roteador na mensagem de OFFER DHCP, o servidor DHCP informa ao cliente qual é o roteador padrão que deve ser configurado em sua interface de rede. Isso permite que o cliente se conecte a redes externas e acesse recursos fora da rede local.

Em resumo, a máscara de sub-rede informa ao cliente DHCP como interpretar os endereços IP na rede local, enquanto o roteador fornece ao cliente o endereço IP do roteador padrão



para encaminhamento de tráfego para redes externas. Essas informações são essenciais para configurar corretamente a interface de rede do cliente DHCP e garantir sua conectividade adequada na rede.

**10.** Explique a finalidade do lease time. Quanto é o lease time de sua captura?

O lease time (tempo de concessão) é um parâmetro utilizado no DHCP para definir a duração em que um cliente DHCP tem permissão para usar um endereço IP atribuído pelo servidor DHCP. O servidor DHCP atribui um lease time ao endereço IP, especificando por quanto tempo o cliente pode utilizar esse endereço antes de precisar renovar a concessão.

A finalidade do lease time é permitir um controle eficiente do uso dos endereços IP em uma rede. Ao definir um tempo de concessão, o servidor DHCP pode garantir que os endereços IP sejam liberados e possam ser reutilizados quando não são mais necessários pelos clientes.

O valor do lease time é definido pelo administrador da rede e pode variar dependendo da política de gerenciamento de endereços IP da organização. Geralmente, os lease times podem ser configurados para minutos, horas, dias ou até mesmo semanas, dependendo das necessidades e da dinâmica da rede.

No caso desta interação por meio de mensagens de texto, como sou uma entidade virtual e não estou associada a uma rede, não tenho um lease time específico para fornecer. Cabe ao administrador da rede configurar o lease time adequado para seus clientes DHCP com base nas políticas e requisitos da rede.