

Neighbor Discovery e Roteamento Estático no IPv6

Nome: Luiza Kuze Gomes

Disciplina: RCO786202

6. Vamos testar o *Neighbor Discovery*, anote a saída do comando. A partir do pc2 execute: `ndisc6 -m fc00:2::1 eth0`. Esse comando descobre e retorna o *MAC address* da interface de rede que possui o endereço IPv6 informado. É equivalente ao protocolo ARP do IPv4.



```
IMUNES: pc2 (console) bash
root@pc2:/# ndisc6 -m fc00:2::1 eth0
Soliciting fc00:2::1 (fc00:2::1) on eth0...
Target link-layer address: 42:00:AA:00:00:06
from fc00:2::1
root@pc2:/#
```

7. Observe que todas as interfaces de rede já estão pré-configuradas, exceto do pc3.

8. Vamos adicionar o endereço IPv6 à interface de rede no pc3: `ip addr add fc00:2::21/64 dev eth0`

9. Faça um ping6 entre o pc3 ao pc2: `ping6 fc00:2::20`. Se tudo estiver devidamente configurado, deve-se obter sucesso no ping entre o pc3 e pc2. Entrega direta ou indireta?

A entrega entre pc3 e pc2 é direta, pois ambos estão na mesma sub-rede (fc00:2::/64), e a comunicação não requer o uso de um roteador. O ping6 funcionou diretamente através da interface eth0 dos dois dispositivos.

```

root@pc2:/# ip addr add fc00:2::21/64 dev eth0
root@pc2:/# ping6 fc00:2::20
PING fc00:2::20(fc00:2::20) 56 data bytes
64 bytes from fc00:2::20: icmp_seq=1 ttl=64 time=0.024 ms
64 bytes from fc00:2::20: icmp_seq=2 ttl=64 time=0.060 ms
64 bytes from fc00:2::20: icmp_seq=3 ttl=64 time=0.055 ms
64 bytes from fc00:2::20: icmp_seq=4 ttl=64 time=0.056 ms
64 bytes from fc00:2::20: icmp_seq=5 ttl=64 time=0.025 ms
64 bytes from fc00:2::20: icmp_seq=6 ttl=64 time=0.039 ms
^C
--- fc00:2::20 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5122ms
rtt min/avg/max/mdev = 0.024/0.043/0.060/0.014 ms
root@pc2:/#

```

10. Faça um ping6 entre o pc3 ao pc0. Obteve sucesso? Sim ou não e por quê?

Não. pc2 funciona porque está na mesma sub-rede que pc3 (fc00:2::/64), e a tabela de roteamento de pc3 inclui automaticamente uma rota para essa sub-rede, permitindo comunicação direta sem a necessidade de roteadores. Já pc0 não funciona porque está em uma sub-rede diferente (fc00:20::/64), e a tabela de roteamento de pc3 não contém uma rota para essa sub-rede, fazendo com que pc3 não saiba para onde encaminhar os pacotes, resultando em "Network is unreachable".

12. No pc3, liste a tabela de roteamento com o comando: ip -6 route show

```

root@pc3:/# ping6 fc00::20
ping6: connect: Network is unreachable
root@pc3:/# ip -6 route show
::1 dev lo0 proto kernel metric 256 pref medium
fc00:2::/64 dev eth0 proto kernel metric 256 pref medium
fe80::/64 dev eth0 proto kernel metric 256 pref medium

```

13. No pc3, acrescente o *default gateway* com o seguinte comando: ip -6 route add default via fc00:2::1 dev eth0. Confira novamente a tabela de roteamento do pc3.

```

root@pc3:/# ip -6 route add default via fc00:2::1 dev eth0
root@pc3:/# ip -6 route show
::1 dev lo0 proto kernel metric 256 pref medium
fc00:2::/64 dev eth0 proto kernel metric 256 pref medium
fe80::/64 dev eth0 proto kernel metric 256 pref medium
default via fc00:2::1 dev eth0 metric 1024 pref medium
root@pc3:/#

```

14. Faça novamente um ping6 entre o pc3 ao pc0. Obteve sucesso? Sim ou não e por quê?

Sim, porque agora há uma rota configurada.

```
root@pc3:/# ping6 fc00:2::20
PING fc00:2::20(fc00:2::20) 56 data bytes
64 bytes from fc00:2::20: icmp_seq=1 ttl=64 time=0.102 ms
64 bytes from fc00:2::20: icmp_seq=2 ttl=64 time=0.099 ms
^C
--- fc00:2::20 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1052ms
rtt min/avg/max/mdev = 0.099/0.100/0.102/0.001 ms
```

16. A partir do computador pc0 use o comando traceroute6 e anote a rota para todos os demais PCs.

```
root@pc0:/# traceroute6 fc00::20
traceroute to fc00::20 (fc00::20) from fc00::20, port 33434, from port 65432, 30
 hops max, 60 bytes packets
 1 fc00::20 (fc00::20) 0.003 ms 0.001 ms 0.002 ms
root@pc0:/# traceroute6 fc00:1::20
traceroute to fc00:1::20 (fc00:1::20) from fc00::20, port 33434, from port 65431
, 30 hops max, 60 bytes packets
 1 fc00::1 (fc00::1) 0.004 ms 0.173 ms 0.057 ms
 2 fc00:1::20 (fc00:1::20) 0.024 ms 0.020 ms 0.003 ms
root@pc0:/# traceroute6 fc00:2::20
traceroute to fc00:2::20 (fc00:2::20) from fc00::20, port 33434, from port 65430
, 30 hops max, 60 bytes packets
 1 fc00::1 (fc00::1) 0.004 ms 0.087 ms 0.559 ms
 2 fc00:3::1 (fc00:3::1) 0.018 ms 0.295 ms 0.086 ms
 3 fc00:2::20 (fc00:2::20) 0.036 ms 0.030 ms 0.002 ms
root@pc0:/#
```

18. Baseado na captura de pacotes do Wireshark explique o processo de descoberta de vizinhança (*Neighbor Solicitation* - NS e *Neighbor Advertisement* - NA), citando os endereços de multicast e link local utilizados. Obs.: ao final do roteiro há alguns exemplos de mensagens.

O dispositivo solicitante (ex.: pc2) envia um NS para resolver o endereço MAC de fc00:2::1. O roteador ou dispositivo com esse endereço (fc00:2::1) responde com um NA contendo seu endereço MAC (42:00:aa:00:00:06).

Esse processo permite que a comunicação seja estabelecida no nível da camada de enlace.

- Endereço Multicast: Destino no NS: ff02::1:ff00:1.
- Endereço Link-Local: Origem no NS: fe80::4000:aa:ff:fe00:4

*- [eth0@R1 (115c1)]					
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help					
Apply a display filter ... <Ctrl>->					
No.	Time	Source	Destination	Protocol	Length Info
1	0.000000	fe80::4000:aaff:fe00:6	ff02::9	RIPng	86 Command Request, Version 1
2	0.204999	fe80::1433:5aff:fe58:fc9e	ff02::2	ICMPv6	70 Router Solicitation from 16:33:5a:58:fc:9e
3	0.716018	fe80::4000:aaff:fe00:5	ff02::2	ICMPv6	70 Router Solicitation from 42:00:aa:00:00:05
4	0.717032	fe80::84ac:76ff:fe33:be0e	ff02::2	ICMPv6	70 Router Solicitation from 16:33:5a:58:fc:9e
5	2.764181	fe80::4000:aaff:fe00:4	ff02::2	ICMPv6	70 Router Solicitation from 42:00:aa:00:00:04
6	9.335871	fe80::4000:aaff:fe00:4	ff02::1:ff00:1	ICMPv6	86 Neighbor Solicitation for fc00:2::1 from 42:00:aa:00:00:04
7	9.335884	fc00:2::1	fe80::4000:aaff:fe00:4	ICMPv6	86 Neighbor Advertisement fc00:2::1 (rtr, sol, ovr) is at 42:00:aa:00:00:06
8	14.540969	fe80::4000:aaff:fe00:6	fe80::4000:aaff:fe00:4	ICMPv6	86 Neighbor Solicitation for fe80::4000:aaff:fe00:4 from 42:00:aa:00:00:06
9	14.541024	fe80::4000:aaff:fe00:4	fe80::4000:aaff:fe00:6	ICMPv6	78 Neighbor Advertisement fe80::4000:aaff:fe00:4 (sol)
10	15.564023	fe80::1433:5aff:fe58:fc9e	ff02::2	ICMPv6	70 Router Solicitation from 16:33:5a:58:fc:9e
11	16.883063	fe80::4000:aaff:fe00:5	ff02::16	ICMPv6	110 Multicast Listener Report Message v2
12	16.969049	fe80::4000:aaff:fe00:6	ff02::9	RIPng	146 Command Response, Version 1
13	16.987994	::	ff02::1:ff00:21	ICMPv6	86 Neighbor Solicitation for fc00:2::21
14	17.012032	fe80::4000:aaff:fe00:5	ff02::16	ICMPv6	110 Multicast Listener Report Message v2
15	17.100998	fe80::4000:aaff:fe00:5	ff02::2	ICMPv6	70 Router Solicitation from 42:00:aa:00:00:05
16	17.612103	fe80::84ac:76ff:fe33:be0e	ff02::2	ICMPv6	70 Router Solicitation from 16:33:5a:58:fc:9e
17	19.660233	fe80::4000:aaff:fe00:4	fe80::4000:aaff:fe00:6	ICMPv6	86 Neighbor Solicitation for fe80::4000:aaff:fe00:6 from 42:00:aa:00:00:04
18	19.660256	fe80::4000:aaff:fe00:6	fe80::4000:aaff:fe00:4	ICMPv6	78 Neighbor Advertisement fe80::4000:aaff:fe00:6 (rtr, sol)
19	20.171999	fe80::4000:aaff:fe00:4	ff02::2	ICMPv6	70 Router Solicitation from 42:00:aa:00:00:04
20	20.727176	fc00:2::21	ff02::1:ff00:20	ICMPv6	86 Neighbor Solicitation for fc00:2::20 from 42:00:aa:00:00:05
21	32.969203	fe80::4000:aaff:fe00:6	ff02::9	RIPng	146 Command Response, Version 1
22	45.773033	fe80::1433:5aff:fe58:fc9e	ff02::2	ICMPv6	70 Router Solicitation from 16:33:5a:58:fc:9e
23	53.452016	fe80::84ac:76ff:fe33:be0e	ff02::2	ICMPv6	70 Router Solicitation from 16:33:5a:58:fc:9e
24	53.452041	fe80::4000:aaff:fe00:5	ff02::2	ICMPv6	70 Router Solicitation from 42:00:aa:00:00:05

19. Numa mensagem do tipo *Neighbor Solicitation* qual é o endereço IPv6 de origem e destino? Explique/defina ambos.

Em uma mensagem NS, o endereço IPv6 de origem é o endereço link-local da interface que envia a solicitação. Esse endereço pertence ao intervalo fe80::/64 e é atribuído automaticamente a todas as interfaces IPv6. Ele identifica unicamente o dispositivo solicitante dentro do mesmo enlace, permitindo que o dispositivo alvo saiba quem está solicitando a resolução de seu endereço MAC.

O endereço IPv6 de destino, por sua vez, é um Solicited-Node Multicast Address, calculado a partir dos últimos 24 bits do endereço IPv6 que está sendo consultado. Esse endereço tem o formato ff02::1:ffXX:XXXX, onde XX:XXXX representa os 24 bits finais do endereço IPv6 alvo.

20. Em todos os hosts rode o comando `ip -6 neighbor show`

```
IMUNES: R0 (console) bash
root@R0:/# ip -6 neighbor show
fe80::4000:aaff:fe00:7 dev eth2 lladdr 42:00:aa:00:00:07 router STALE
fe80::4000:aaff:fe00:3 dev eth1 lladdr 42:00:aa:00:00:03 STALE
fe80::4000:aaff:fe00:1 dev eth0 lladdr 42:00:aa:00:00:01 STALE

IMUNES: R1 (console) bash
root@R1:/# ip -6 neighbor show
fe80::4000:aaff:fe00:8 dev eth1 lladdr 42:00:aa:00:00:08 router STALE
fe80::4000:aaff:fe00:4 dev eth0 lladdr 42:00:aa:00:00:04 STALE
fe80::84ac:76ff:fe33:be0e dev eth0 lladdr 16:33:5a:58:fc:9e STALE
fe80::4000:aaff:fe00:5 dev eth0 lladdr 42:00:aa:00:00:05 STALE
fe80::1433:5aff:fe58:fc9e dev eth0 lladdr 16:33:5a:58:fc:9e STALE
root@R1:/#

IMUNES: pc2 (console) bash
root@pc2:/# ip -6 neighbor show
fe80::4000:aaff:fe00:6 dev eth0 lladdr 42:00:aa:00:00:06 router STALE
fe80::4000:aaff:fe00:5 dev eth0 lladdr 42:00:aa:00:00:05 STALE
fc00:2::21 dev eth0 lladdr 42:00:aa:00:00:05 STALE
root@pc2:/#

IMUNES: pc1 (console) bash
root@pc1:/# ip -6 neighbor show
root@pc1:/# ip -6 neighbor show
root@pc1:/#

IMUNES: pc0 (console) bash
root@pc0:/# ip -6 neighbor show
root@pc0:/#

IMUNES: pc3 (console) bash
root@pc3:/# ip -6 neighbor show
fc00:2::20 dev eth0 lladdr 42:00:aa:00:00:04 STALE
fe80::4000:aaff:fe00:4 dev eth0 lladdr 42:00:aa:00:00:04 STALE
root@pc3:/#
```

1. Qual é a funcionalidade desse comando?

Exibe a tabela de vizinhos IPv6 mantida pelo dispositivo. Essa tabela lista os dispositivos diretamente conectados ao enlace, associando os endereços IPv6 aos endereços MAC.

2. Qual é o significado do conteúdo dessa tabela?

Endereço IPv6: O endereço do vizinho que está sendo rastreado.

Interface: A interface de rede onde esse vizinho foi detectado.

lladdr (Link-Layer Address): O endereço MAC do vizinho correspondente ao endereço IPv6.

Estado:

STALE: O endereço foi resolvido, mas não houve comunicação recente com o vizinho.

REACHABLE: O endereço foi resolvido e o vizinho está acessível no momento.

DELAY ou PROBE: Estados intermediários quando o vizinho está sendo validado.

3. A tabela mostrada em cada um dos casos é compatível com o diagrama da rede montado?

Sim, as tabelas refletem a topologia da rede apresentada no diagrama

4. Por que, por exemplo, na tabela do pc2 não há uma referência explícita ao pc0?

No pc2, não há uma referência explícita ao pc0 porque eles estão em sub-redes diferentes. O NDP só exibe vizinhos diretamente conectados (na mesma sub-rede).

21. Explique sucintamente as diferenças na comunicação baseada em IPv4 e IPv6.

Endereços

IPv4: Endereços de 32 bits. Exemplo do formato: XXX.XXX.X.X.

IPv6: Endereços de 128 bits. Exemplo do formato:
XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX.

Descoberta de Vizinhança

IPv4: Utiliza o protocolo ARP (Address Resolution Protocol) para mapear endereços IP para endereços MAC.

IPv6: Utiliza o NDP (Neighbor Discovery Protocol), que substitui o ARP e oferece funcionalidades adicionais, como descoberta de roteadores e prefixos.

Encapsulamento

IPv4: Cabeçalhos incluem opções e fragmentação dentro do próprio pacote.

IPv6: Cabeçalhos simplificados, removendo opções e fragmentação, com funcionalidades adicionais em cabeçalhos de extensão.

Segurança

IPv4: Não inclui segurança nativa, mas pode ser estendido com IPsec.

IPv6: Suporta IPsec nativamente, aumentando a segurança.

Multicast

IPv4: Suporte limitado e opcional.

IPv6: Multicast é essencial para o funcionamento de protocolos como o NDP e outras funcionalidades.