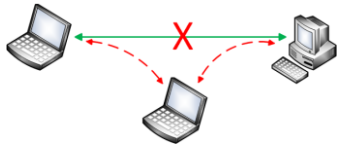
SBSeg 2017



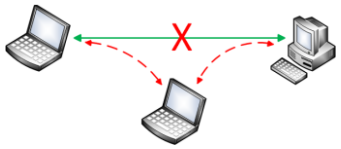
Estudo do mecanismo de descoberta de vizinhança do IPv6 para realização do ataque *man in the middle*

Matheus Dias Queiroz – madaqz@gmail.com

André Leon S. Gradvohl – gradvohl@ft.unicamp.br

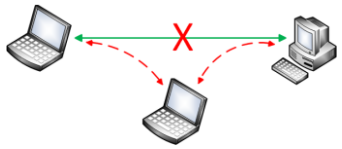
Faculdade de Tecnologia - Universidade Estadual de Campinas (UNICAMP)

Apresentação

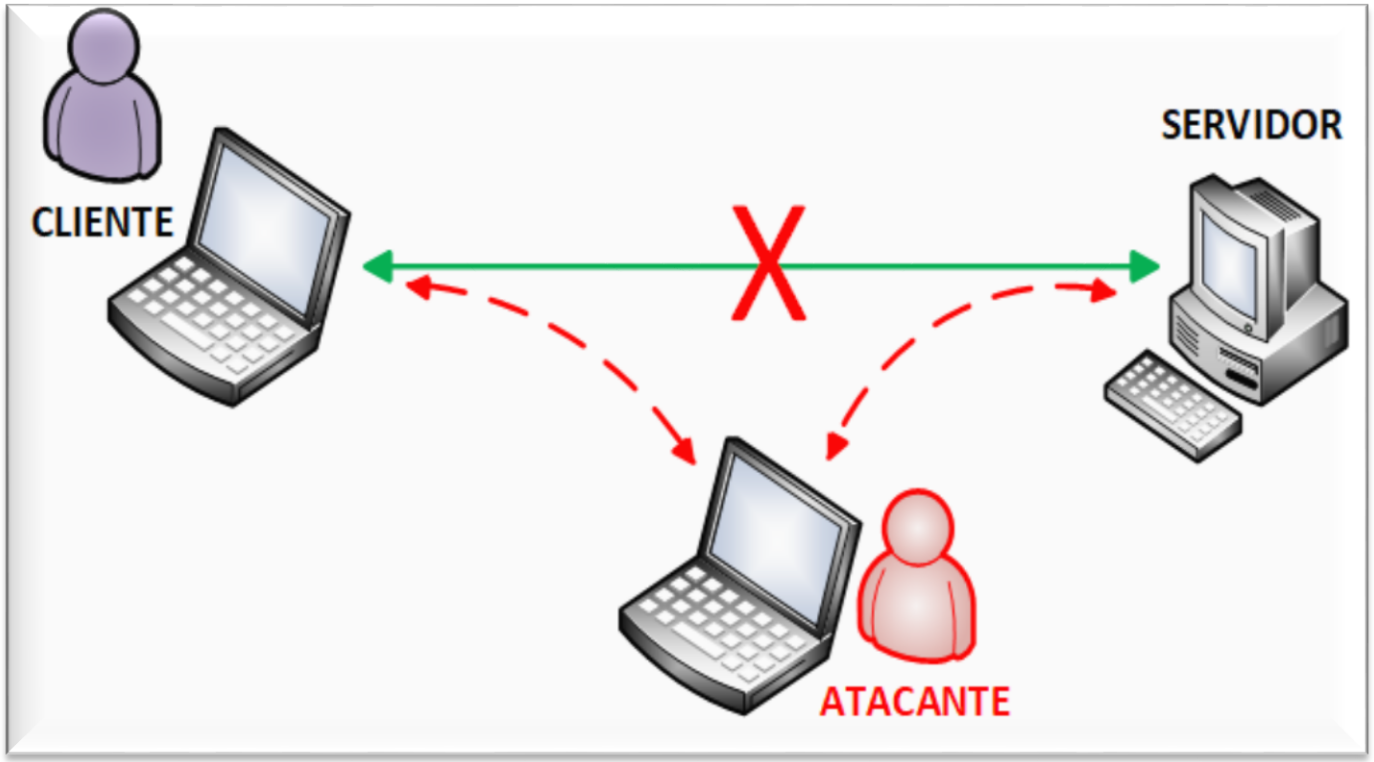


- Introdução
- ARP IPv4
- NDP IPv6
- Experimento
- Resultados
- Conclusão

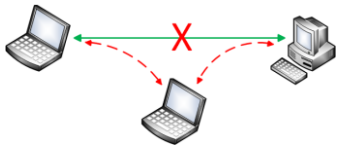
Introdução



- O que é um ataque do tipo *man in the middle?*

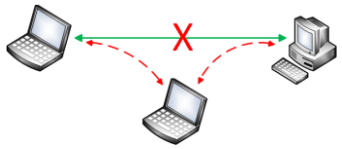


Introdução



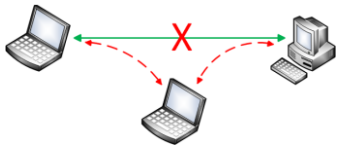
- IPv4: 1979, RFC 760 em 1980
- IPv4 = 2^32 (4 294 967 296 endereços)
- IETF: em 1991 declara que os endereços acabariam em 1994
- Esgotamento de endereços IPv4
- Desenvolvimento do IPv6. Primeiras RFCs em 1995
- IANA: 2011, distribuição dos últimos IPv4

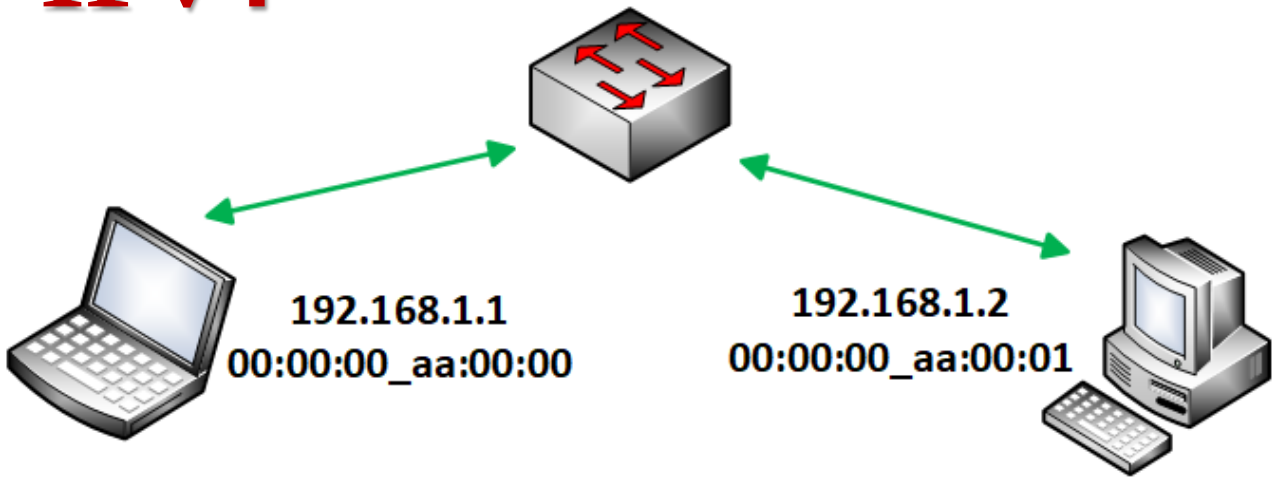
Introdução



- IPv6 = 2^128 = 340.282.366.920.938.463.463.374.607.431.768.211.456 endereços
- Equivale a 79 trilhões de vezes o IPv4
- É difícil imaginar!
- Tendência de aumento do IPv6 e diminuição do IPv4
- Mudou o mecanismo de descoberta de vizinhança. O que é isso?
- IPv4 = Address Resolution Protocol (ARP)
- IPv6 = Neighbor Discovery Protocol (NDP)

Address Resolution Protocol (ARP) IPv4





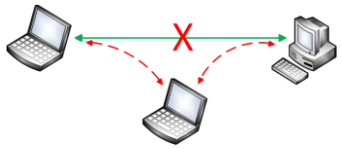
Mensagens ARP legítimas:

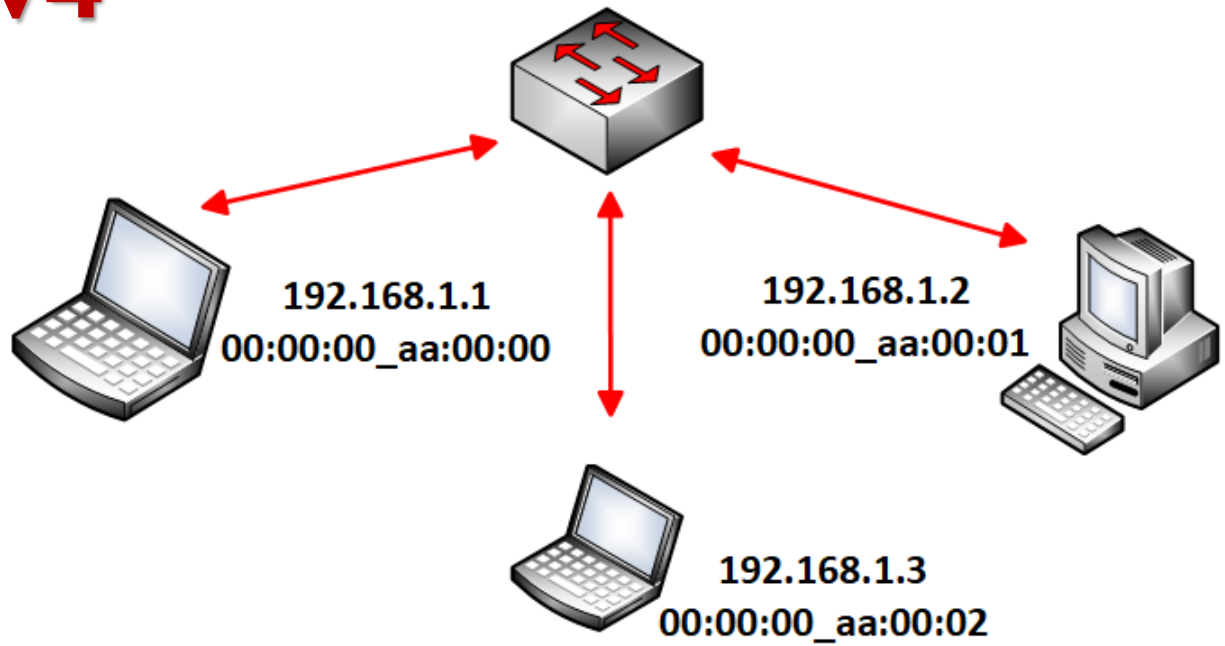
Source	Destination	Protocol	Info
00:00:00_aa:00:00	Broadcast	ARP	Who has 192.168.1.2? Tell 192.168.1.1
00:00:00_aa:00:01	00:00:00_aa:00:00	ARP	192.168.1.2 is at 00:00:00:aa:00:01
00:00:00_aa:00:01	00:00:00_aa:00:00	ARP	Who has 192.168.1.1? Tell 192.168.1.2
00:00:00_aa:00:00	00:00:00_aa:00:01	ARP	192.168.1.1 is at 00:00:00:aa:00:00

Tabela cache ARP:

```
root@n2:/tmp/pycore.33961/n2.conf# ip neigh
192.168.1.1 dev eth0 lladdr 00:00:00:aa:00:00 STALE
```

Address Resolution Protocol (ARP) IPv4

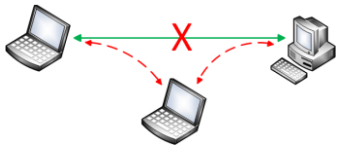




Mensagens ARP forjadas:

```
00:00:00_aa:00:02   Broadcast          ARP      192.168.1.1 is at 00:00:00:aa:00:02
00:00:00_aa:00:02   Broadcast          ARP      192.168.1.1 is at 00:00:00:aa:00:02
00:00:00_aa:00:02   Broadcast          ARP      192.168.1.1 is at 00:00:00:aa:00:02
```

Address Resolution Protocol (ARP) IPv4



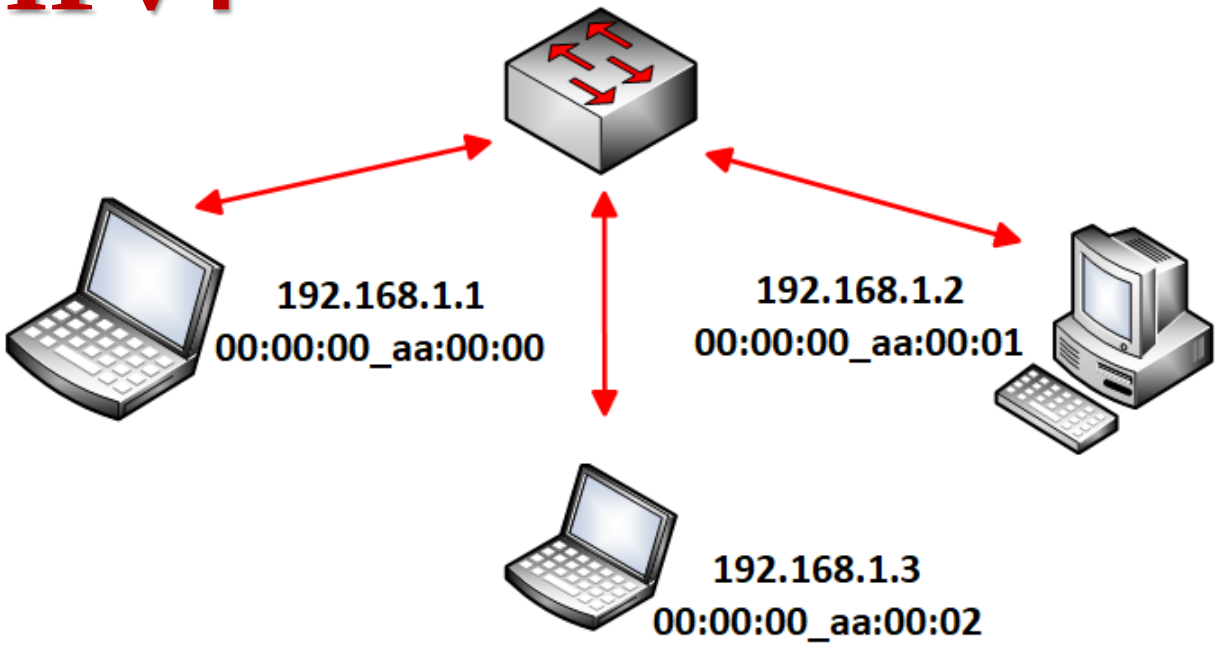
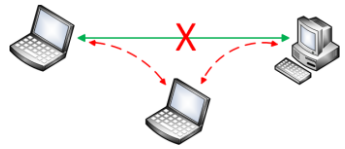


Tabela cache ARP:

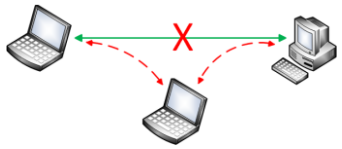
```
root@n2:/tmp/pycore.33961/n2.conf# ip neigh
192.168.1.1 dev eth0 lladdr 00:00:00:aa:00:00 STALE
root@n2:/tmp/pycore.33961/n2.conf# ip neigh
192.168.1.1 dev eth0 lladdr 00:00:00:aa:00:02 STALE
root@n2:/tmp/pycore.33961/n2.conf#
```

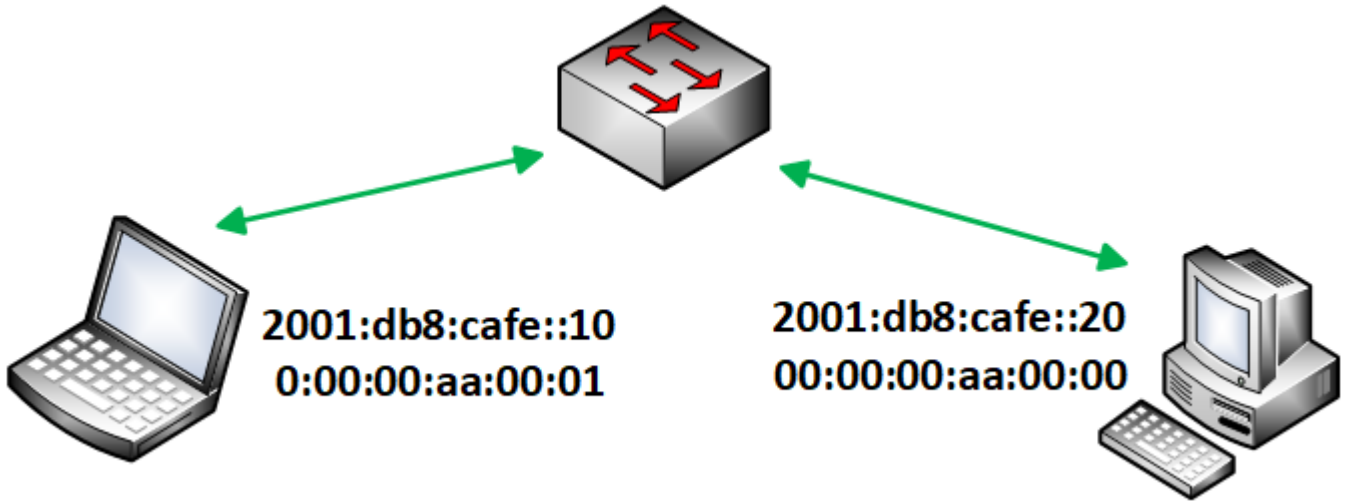
Neighbor Discovery Protocol IPv6



MENSAGEM	DESCRIÇÃO
ROUTER SOLICITATION (RS)	Enviada pelos hosts para encontrar roteadores.
ROUTER ADVERTISEMENT (RA)	Enviada por um roteador em resposta a um RS. Também pode ser enviada sem ter sido solicitada.
NEIGHBOR SOLICITATION (NS)	Enviado por um host para descobrir o endereço físico de outro host.
NEIGHBOR ADVERTISEMENT (NA)	Mensagem em resposta a um NS mas também podendo ser enviada sem solicitação.
REDIRECT	Enviada por um roteador para redirecionar rotas.

Neighbor Discovery Protocol IPv6

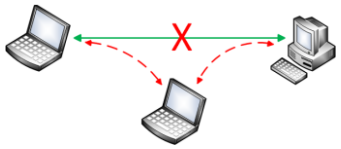


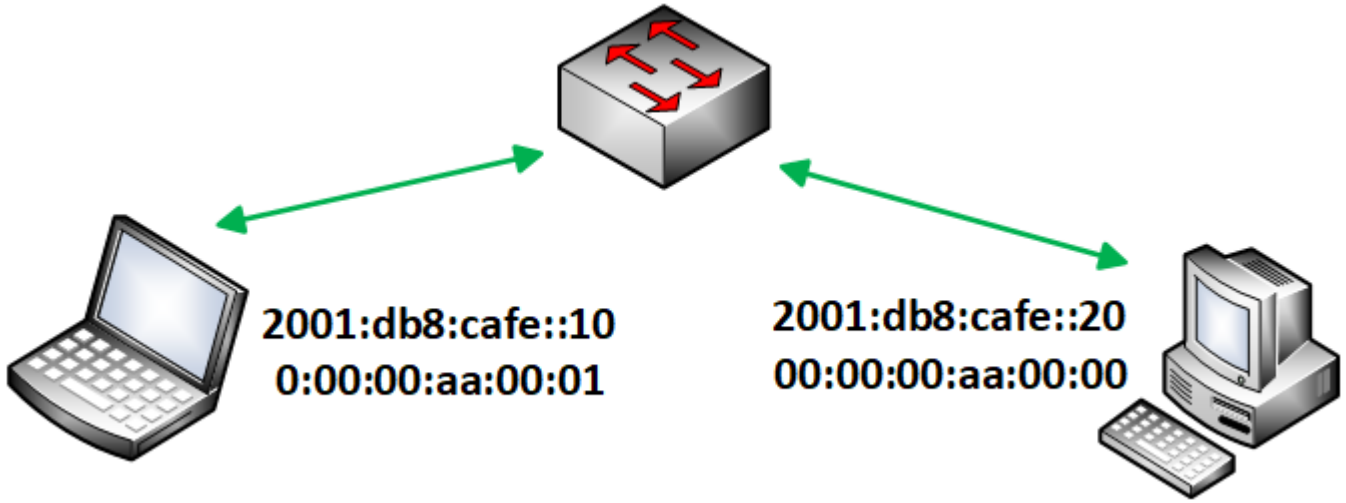


Source	Destination	Protocol	Info
2001:db8:cafe::10	ff02::1:ff00:20	ICMPv6	Neighbor Solicitation for 2001:db8:cafe::20 from 00:00:00:aa:00:01
2001:db8:cafe::20	2001:db8:cafe::10	ICMPv6	Neighbor Advertisement 2001:db8:cafe::20 (sol, ovr) is at 00:00:00:aa:00:00
2001:db8:cafe::10	2001:db8:cafe::20	ICMPv6	Echo (ping) request id=0x0011, seq=1, hop limit=64 (reply in 24)
2001:db8:cafe::20	2001:db8:cafe::10	ICMPv6	Echo (ping) reply id=0x0011, seq=1, hop limit=64 (request in 23)

ff02::1:ff00:0020

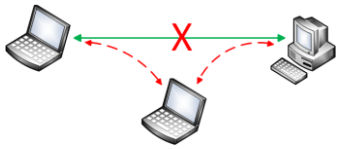
Neighbor Discovery Protocol IPv6

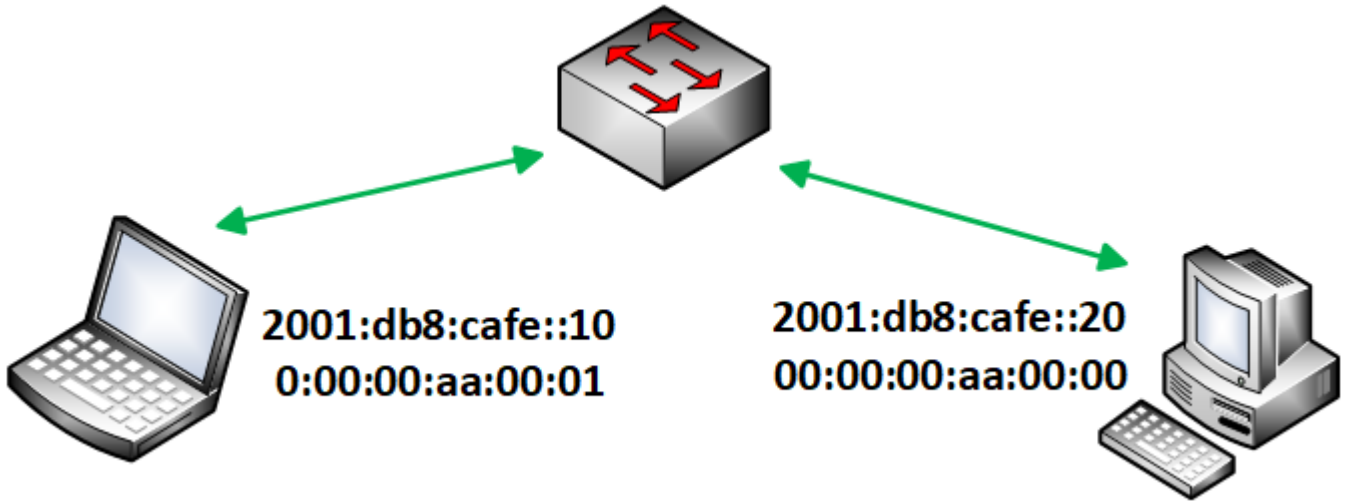





```
root@n2:/tmp/pycore.35829/n2.conf# ip -6 neigh
fe80::200:ff:feaa:0 dev eth0 lladdr 00:00:00:aa:00:00 STALE
2001:db8:cafe::20 dev eth0 lladdr 00:00:00:aa:00:00 STALE
root@n2:/tmp/pycore.35829/n2.conf#
```

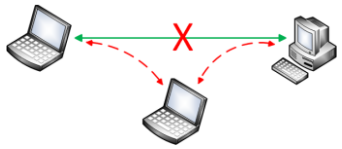
Neighbor Discovery Protocol IPv6

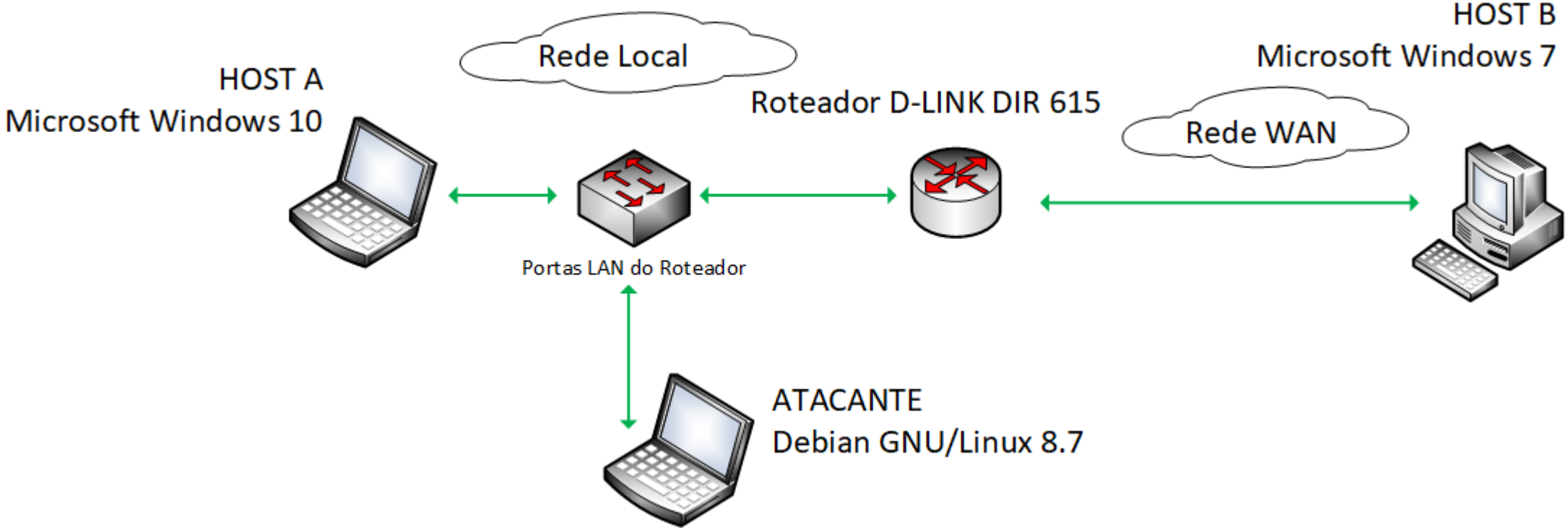




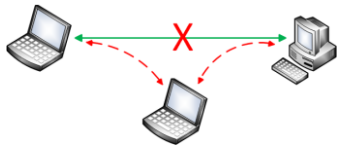

```
root@n1:/tmp/pycore.35829/n1.conf# ip -6 neigh
2001:db8:cafe::10 dev eth0 lladdr 00:00:00:aa:00:01 STALE
fe80::200:ff:feaa:1 dev eth0 lladdr 00:00:00:aa:00:01 STALE
root@n1:/tmp/pycore.35829/n1.conf#
```

Experimento



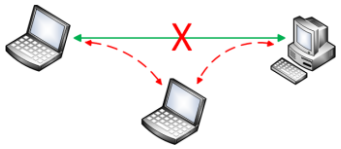


Experimento



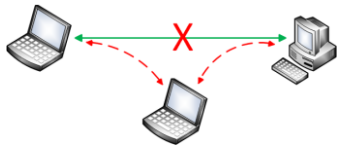
CAMADA ETHERNET	
Origem: 78:2b:cb:be:2d:9d (MAC do atacante)	Destino: 33:33:00:00:00:01
CAMADA IPv6	
Origem: fe80::a2ab:1bff:fe31:92e4 (IPv6 link-local roteador)	Destino: ff02::1
CAMADA ICMPv6	
Tipo: Neighbor Advertisement	Flags: R = 1 S = 0 O = 1
Target Address: fe80::a2ab:1bff:fe31:92e4	Target link-layer address: 78:2b:cb:be:2d:9d

Experimento



Source	Destinatior	Protocol	Length	Info
fe80::a2ab:1bff:fe31:92e4	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::a2ab:1bff:fe31:92e4 (rtr, ovr) is at 78:2b:cb:be:2d:9d

Resultados



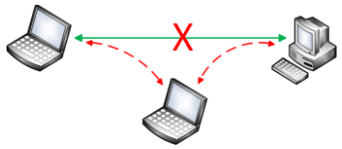
- Tabela Neighbor Cache do Host A antes do ataque:

C:\Windows\system32\cmd.exe

```
Interface 11: Ethernet

Endereço na Internet                            Endereço Físico   Tipo
----------------------------------------------  ----------------  -----------
fe80::a2ab:1bff:fe31:92e4                       a0-ab-1b-31-92-e4  Acessível (Roteador)
ff02::1                                         33-33-00-00-00-01  Permanente
ff02::2                                         33-33-00-00-00-02  Permanente
ff02::16                                        33-33-00-00-00-16  Permanente
ff02::1:2                                       33-33-00-01-00-02  Permanente
ff02::1:3                                       33-33-00-01-00-03  Permanente
ff02::1:ff00:3                                  33-33-ff-00-00-03  Permanente
ff02::1:ff31:92e4                               33-33-ff-31-92-e4  Permanente
ff02::1:ff40:9ccc                               33-33-ff-40-9c-cc  Permanente
ff02::1:ff81:1df8                               33-33-ff-81-1d-f8  Permanente
```

Resultados



- Tabela Neighbor Cache do Host A depois do ataque:

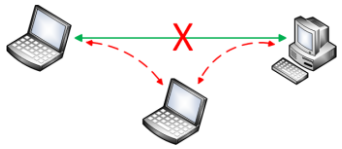
C:\Windows\system32\cmd.exe

```
ff02::1:ffbe:2d9d                                         Permanente

Interface 11: Ethernet


Endereço na Internet                                  Endereço Físico   Tipo
----------------------------------------------------  ----------------  ----------
fe80::7a2b:cbff:febe:2d9d                             78-2b-cb-be-2d-9d  Acessível (Roteador)
fe80::a2ab:1bff:fe31:92e4                             78-2b-cb-be-2d-9d  Inalcançável (Roteador)
ff02::1                                               33-33-00-00-00-01  Permanente
ff02::2                                               33-33-00-00-00-02  Permanente
ff02::16                                              33-33-00-00-00-16  Permanente
ff02::1:2                                             33-33-00-01-00-02  Permanente
ff02::1:3                                             33-33-00-01-00-03  Permanente
ff02::1:ff00:3                                        33-33-ff-00-00-03  Permanente
ff02::1:ff31:92e4                                     33-33-ff-31-92-e4  Permanente
ff02::1:ff40:9ccc                                     33-33-ff-40-9c-cc  Permanente
ff02::1:ff81:1df8                                     33-33-ff-81-1d-f8  Permanente
```

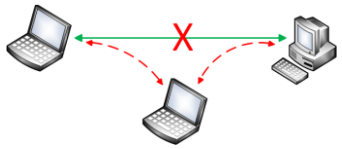
Resultados



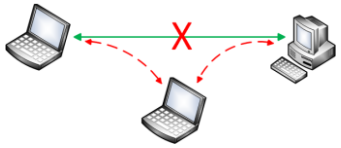
- Pacotes de rede interceptados:

Source	Destination	Protocol	Length	Info
2001:db8:cafe:0:31e1:ecfb:4f40:9ccc	2001:db8:faca::1	FTP	84	Request: AUTH TLS
fe80::7a2b:cbff:febe:2d9d	2001:db8:cafe:0:31e1:ecfb:4f40:9cc	ICMPv6	174	Redirect is at a0:ab:1b:31:92:e4
2001:db8:cafe:0:31e1:ecfb:4f40:9ccc	2001:db8:faca::1	FTP	84	[TCP Retransmission] Request: AUTH TLS
2001:db8:cafe:0:31e1:ecfb:4f40:9ccc	2001:db8:faca::1	FTP	84	Request: AUTH SSL
fe80::7a2b:cbff:febe:2d9d	2001:db8:cafe:0:31e1:ecfb:4f40:9cc	ICMPv6	174	Redirect is at a0:ab:1b:31:92:e4
2001:db8:cafe:0:31e1:ecfb:4f40:9ccc	2001:db8:faca::1	FTP	84	[TCP Retransmission] Request: AUTH SSL
2001:db8:cafe:0:31e1:ecfb:4f40:9ccc	2001:db8:faca::1	FTP	86	Request: USER HostA
fe80::7a2b:cbff:febe:2d9d	2001:db8:cafe:0:31e1:ecfb:4f40:9cc	ICMPv6	182	Redirect is at a0:ab:1b:31:92:e4
2001:db8:cafe:0:31e1:ecfb:4f40:9ccc	2001:db8:faca::1	FTP	86	[TCP Retransmission] Request: USER HostA
2001:db8:cafe:0:31e1:ecfb:4f40:9ccc	2001:db8:faca::1	FTP	89	Request: PASS FTPhosta
fe80::7a2b:cbff:febe:2d9d	2001:db8:cafe:0:31e1:ecfb:4f40:9cc	ICMPv6	182	Redirect is at a0:ab:1b:31:92:e4
2001:db8:cafe:0:31e1:ecfb:4f40:9ccc	2001:db8:faca::1	FTP	89	[TCP Retransmission] Request: PASS FTPhosta

Conclusões



- Ataque *man in the middle* – Mensagens NA / RA
- Roteador (rota padrão) e seu endereço link-local, endereço físico do atacante
- Alta quantidade de endereços IPv6 possíveis
- Endereços multicast
- Descoberta de hosts ativos



Obrigado!!

Apresentação disponível em:

DOI: 10.5281/zenodo.1041957