Exploring the ICMPv6 Toolset

Nick Russo
NETWORK ENGINEER

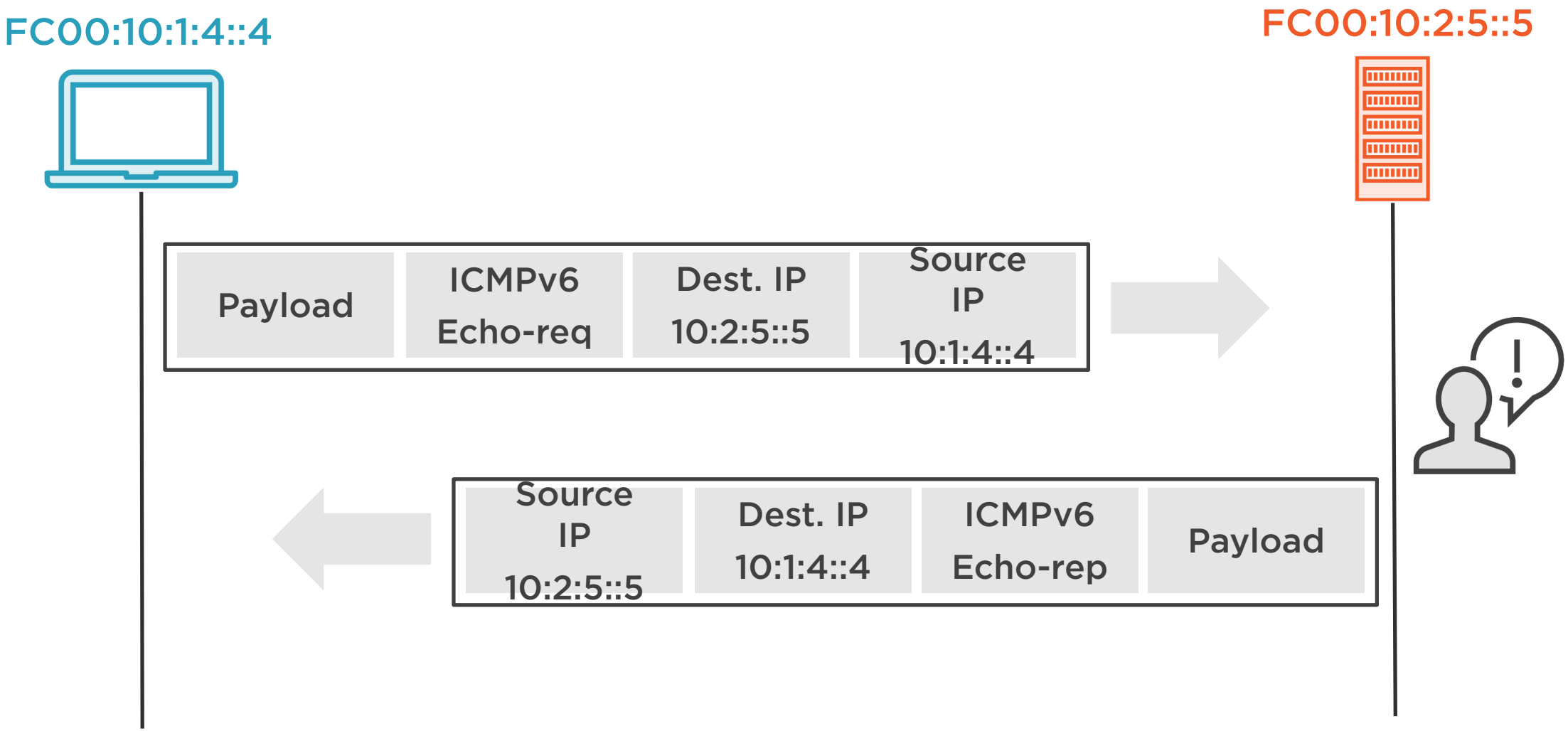
@nickrusso42518 www.njrusmc.net

Agenda

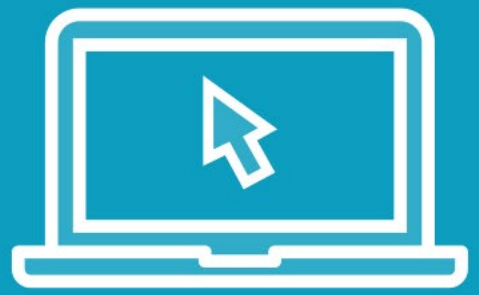
All our favorite features are back!

- Ping
- Traceroute
- MTU Discovery
- Firewalling

IPv6 Ping Packet Flow



Demo



IPv6 Ping in Action

ICMPv6 Echo-request

No.	Time	Source	Destination	Protocol	Info
1	0.000000	fc00:10:1:4::4	fc00:10:2:5::5	ICMPv6	Echo (ping) request id=0x0f18, seq=0, hop limit=64 (reply in 2)
2	0.000786	fc00:10:2:5::5	fc00:10:1:4::4	ICMPv6	Echo (ping) reply id=0x0f18, seq=0, hop limit=62 (request in 1)
3	0.000944	fc00:10:1:4::4	fc00:10:2:5::5	ICMPv6	Echo (ping) request id=0x0f18, seq=1, hop limit=64 (reply in 4)
4	0.006282	fc00:10:2:5::5	fc00:10:1:4::4	ICMPv6	Echo (ping) reply id=0x0f18, seq=1, hop limit=62 (request in 3)
5	0.006399	fc00:10:1:4::4	fc00:10:2:5::5	ICMPv6	Echo (ping) request id=0x0f18, seq=2, hop limit=64 (reply in 6)
6	0.011449	fc00:10:2:5::5	fc00:10:1:4::4	ICMPv6	Echo (ping) reply id=0x0f18, seq=2, hop limit=62 (request in 5)
7	0.011604	fc00:10:1:4::4	fc00:10:2:5::5	ICMPv6	Echo (ping) request id=0x0f18, seq=3, hop limit=64 (reply in 8)
8	0.016891	fc00:10:2:5::5	fc00:10:1:4::4	ICMPv6	Echo (ping) reply id=0x0f18, seq=3, hop limit=62 (request in 7)
9	0.017112	fc00:10:1:4::4	fc00:10:2:5::5	ICMPv6	Echo (ping) request id=0x0f18, seq=4, hop limit=64 (reply in 10)
	0.022022	fc00:10:2:5::5	fc00:10:1:4::4	ICMPv6	Echo (ping) reply id=0x0f18, seq=4, hop limit=62 (request in 9)

```
▶ Frame 1: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
▶ Ethernet II, Src: 00:00:a6:16:00:04, Dst: 00:00:a6:16:00:01
▶ Internet Protocol Version 6, Src: fc00:10:1:4::4, Dst: fc00:10:2:5::5
▼ Internet Control Message Protocol v6
    Type: Echo (ping) request (128)
    Code: 0
    Checksum: 0xeb93 [correct]
    [Checksum Status: Good]
    Identifier: 0x0f18
    Sequence: 0
    [Response In: 2]
  ▶ Data (52 bytes)
```

Type 128 is echo-request (no codes)

Used to identify process/daemon

Used to match request to reply

ICMPv6 Echo-reply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	fc00:10:1:4::4	fc00:10:2:5::5	ICMPv6	Echo (ping) request id=0x0f18, seq=0, hop limit=64 (reply in 2)
2	0.000786	fc00:10:2:5::5	fc00:10:1:4::4	ICMPv6	Echo (ping) reply id=0x0f18, seq=0, hop limit=62 (request in 1)
3	0.000944	fc00:10:1:4::4	fc00:10:2:5::5	ICMPv6	Echo (ping) request id=0x0f18, seq=1, hop limit=64 (reply in 4)
4	0.006282	fc00:10:2:5::5	fc00:10:1:4::4	ICMPv6	Echo (ping) reply id=0x0f18, seq=1, hop limit=62 (request in 3)
5	0.006399	fc00:10:1:4::4	fc00:10:2:5::5	ICMPv6	Echo (ping) request id=0x0f18, seq=2, hop limit=64 (reply in 6)
6	0.011449	fc00:10:2:5::5	fc00:10:1:4::4	ICMPv6	Echo (ping) reply id=0x0f18, seq=2, hop limit=62 (request in 5)
7	0.011604	fc00:10:1:4::4	fc00:10:2:5::5	ICMPv6	Echo (ping) request id=0x0f18, seq=3, hop limit=64 (reply in 8)
8	0.016891	fc00:10:2:5::5	fc00:10:1:4::4	ICMPv6	Echo (ping) reply id=0x0f18, seq=3, hop limit=62 (request in 7)
9	0.017112	fc00:10:1:4::4	fc00:10:2:5::5	ICMPv6	Echo (ping) request id=0x0f18, seq=4, hop limit=64 (reply in 10)
	0.022022	fc00:10:2:5::5	fc00:10:1:4::4	ICMPv6	Echo (ping) reply id=0x0f18, seq=4, hop limit=62 (request in 9)

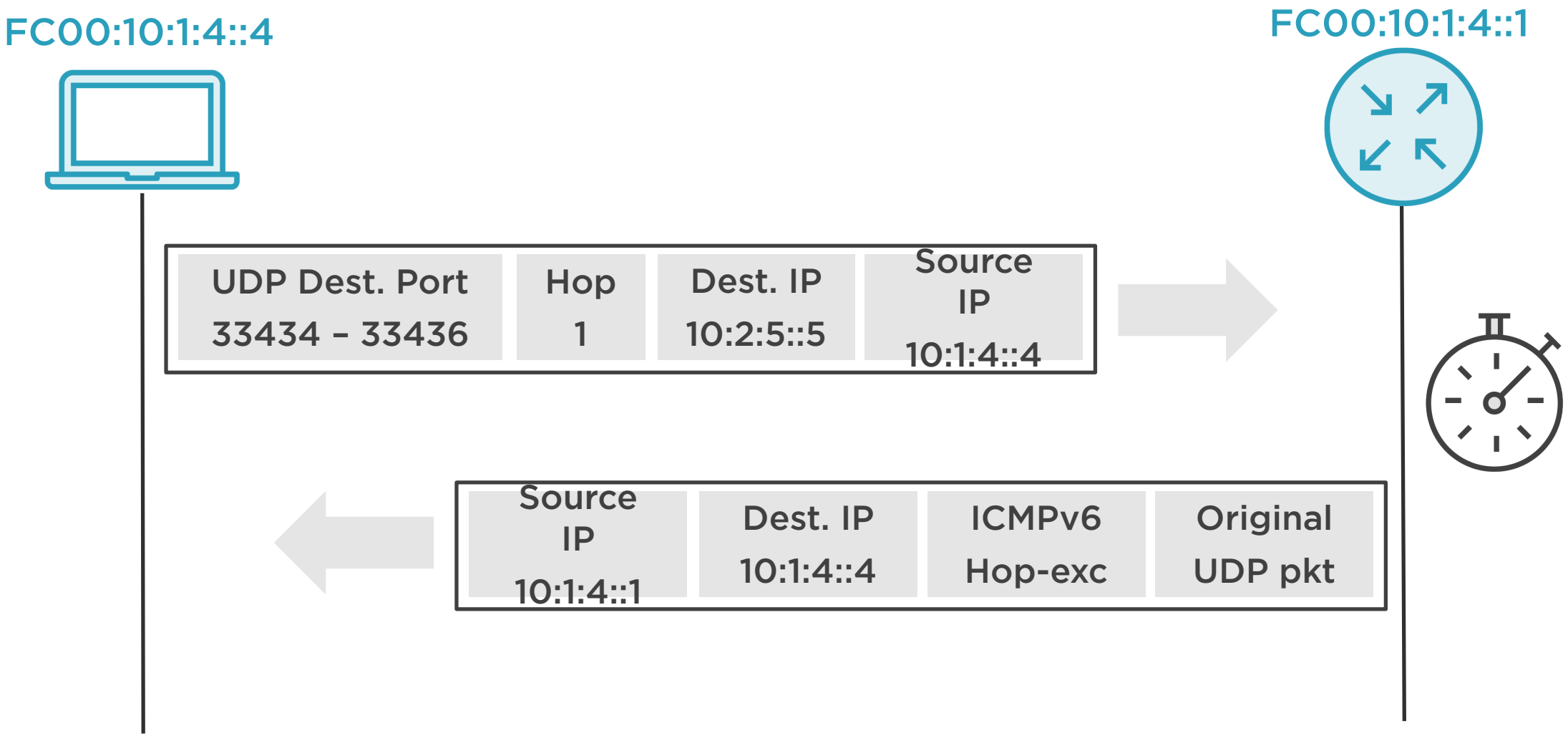
```
▶ Frame 2: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
▶ Ethernet II, Src: 00:00:a6:16:00:01, Dst: 00:00:a6:16:00:04
▶ Internet Protocol Version 6, Src: fc00:10:2:5::5, Dst: fc00:10:1:4::4
▼ Internet Control Message Protocol v6
    Type: Echo (ping) reply (129)
    Code: 0
    Checksum: 0xea93 [correct]
    [Checksum Status: Good]
    Identifier: 0x0f18
    Sequence: 0
    [Response To: 1]
    [Response Time: 0.786 ms]
  ▶ Data (52 bytes)
```

Type 129 is echo-reply (no codes)

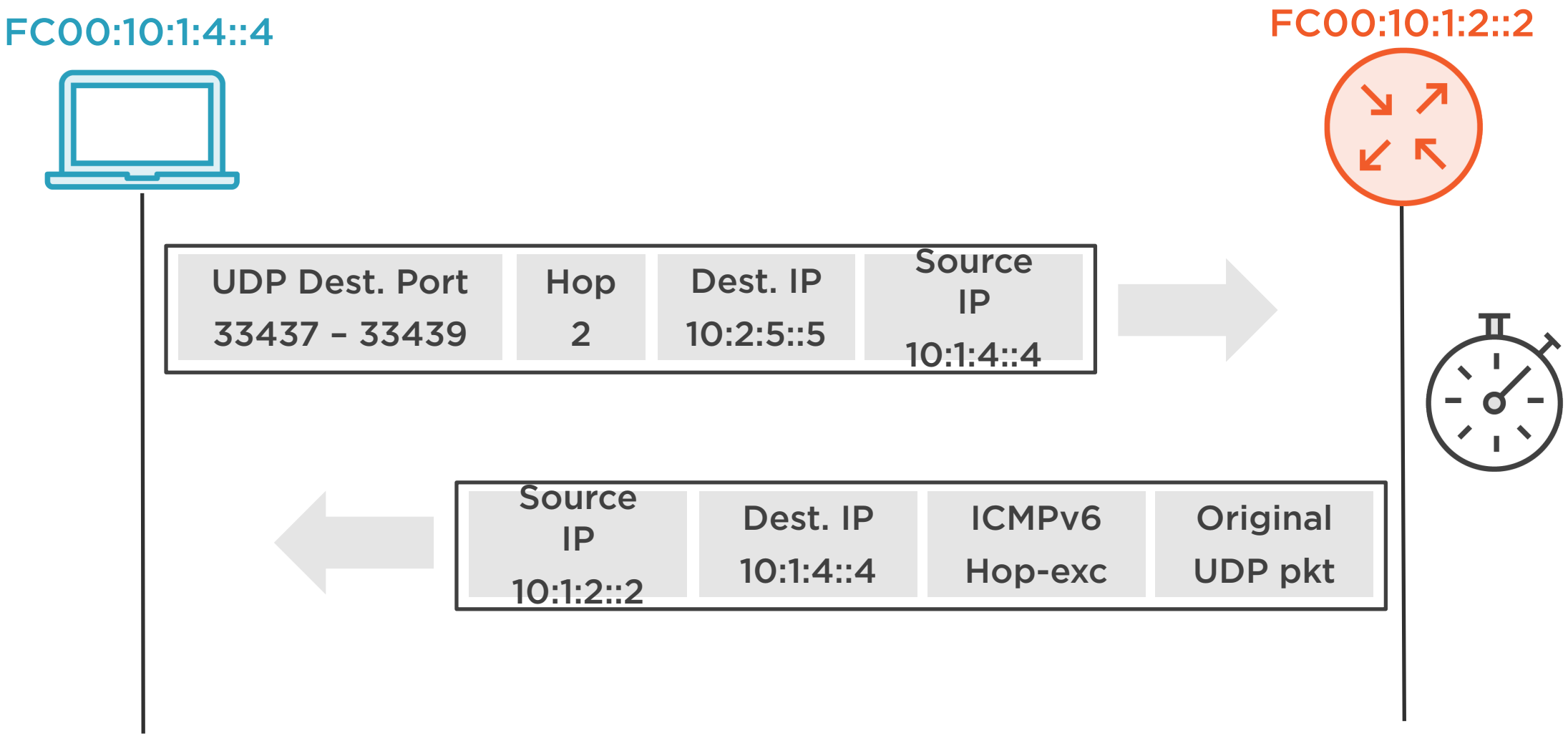
Replying node retains value

Replying node retains value

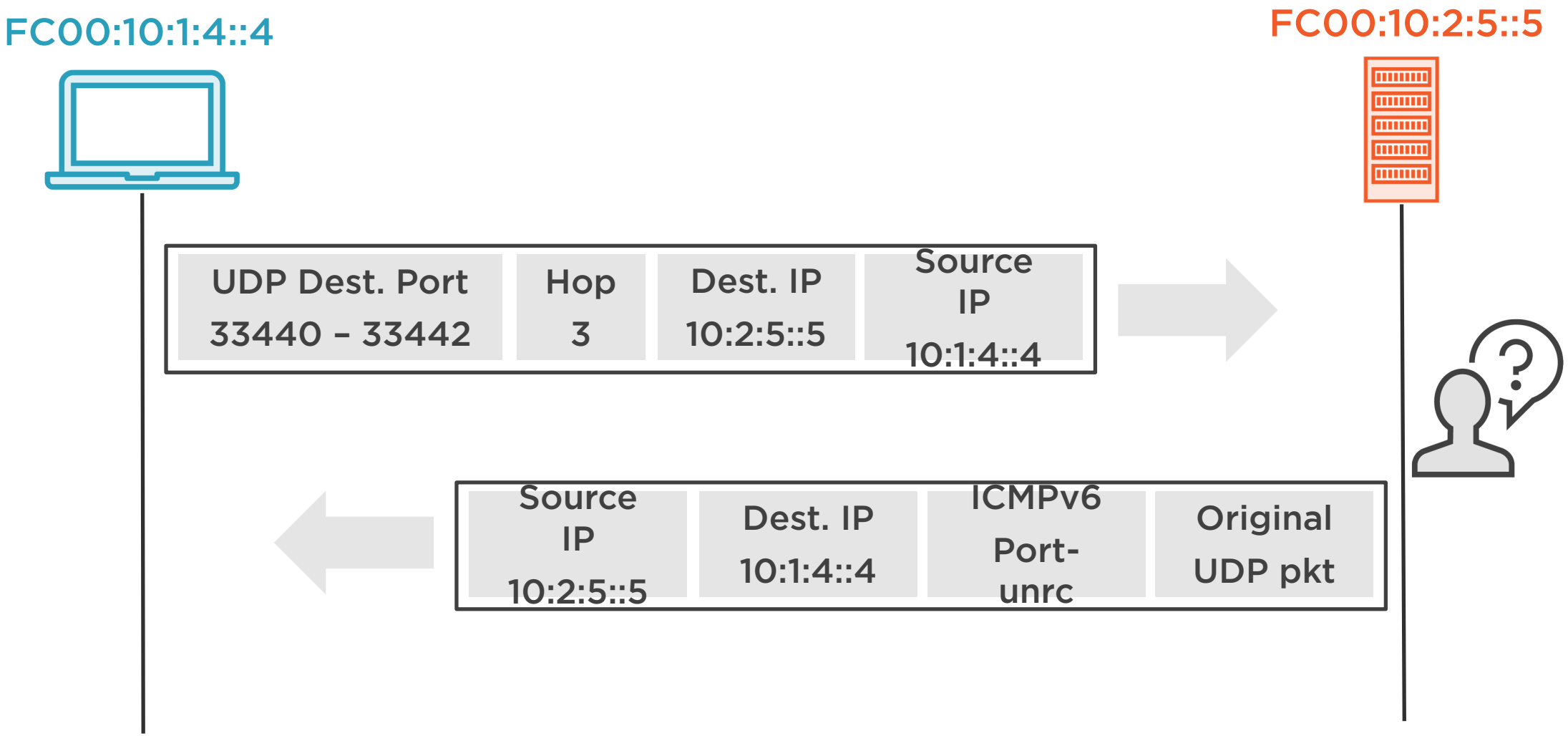
IPv6 Traceroute Packet Flow – First Hop



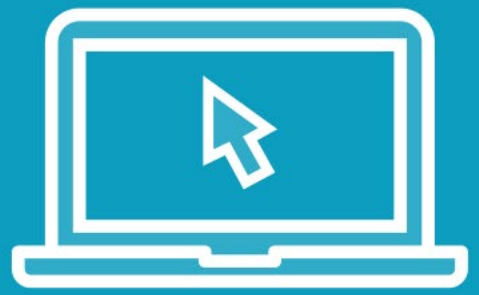
IPv6 Traceroute Packet Flow – Second Hop



IPv6 Traceroute Packet Flow – Termination



Demo



IPv6 Traceroute in Action

IPv6 UDP Traceroute Probe

No.	Time	Source	Destination	Protocol	Hop limit	Info
1	0.000000	fc00:10:1:4::4	fc00:10:2:5::5	UDP	1	59674→33434 Len=0
2	0.000470	fc00:10:1:4::1	fc00:10:1:4::4	ICMPv6	64,1	Time Exceeded (hop limit exceeded in transit)
3	0.000586	fc00:10:1:4::4	fc00:10:2:5::5	UDP	1	56362→33435 Len=0
4	0.000840	fc00:10:1:4::1	fc00:10:1:4::4	ICMPv6	64,1	Time Exceeded (hop limit exceeded in transit)
5	0.005832	fc00:10:1:4::4	fc00:10:2:5::5	UDP	1	59665→33436 Len=0
6	0.006411	fc00:10:1:4::1	fc00:10:1:4::4	ICMPv6	64,1	Time Exceeded (hop limit exceeded in transit)
7	0.010828	fc00:10:1:4::4	fc00:10:2:5::5	UDP	2	64584→33437 Len=0
8	0.011692	fc00:10:1:2::2	fc00:10:1:4::4	ICMPv6	63,1	Time Exceeded (hop limit exceeded in transit)
9	0.016235	fc00:10:1:4::4	fc00:10:2:5::5	UDP	2	51662→33438 Len=0
	0.017019	fc00:10:1:2::2	fc00:10:1:4::4	ICMPv6	63,1	Time Exceeded (hop limit exceeded in transit)
	0.021403	fc00:10:1:4::4	fc00:10:2:5::5	UDP	2	65394→33439 Len=0
	0.021681	fc00:10:1:2::2	fc00:10:1:4::4	ICMPv6	63,1	Time Exceeded (hop limit exceeded in transit)

```
▶ Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
▶ Ethernet II, Src: 00:00:a6:16:00:04, Dst: 00:00:a6:16:00:01
▶ Internet Protocol Version 6, Src: fc00:10:1:4::4, Dst: fc00:10:2:5::5
▼ User Datagram Protocol, Src Port: 59674, Dst Port: 33434
    Source Port: 59674
    Destination Port: 33434
    Length: 8
    Checksum: 0x9bf2 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
```

← Target won't be listening

No payload data

ICMPv6 Hop Limit Exceeded

No.	Time	Source	Destination	Protocol	Hop limit	Info
1	0.000000	fc00:10:1:4::4	fc00:10:2:5::5	UDP	1	59674→33434 Len=0
2	0.000470	fc00:10:1:4::1	fc00:10:1:4::4	ICMPv6	64,1	Time Exceeded (hop limit exceeded in transit)
3	0.000586	fc00:10:1:4::4	fc00:10:2:5::5	UDP	1	56362→33435 Len=0
4	0.000840	fc00:10:1:4::1	fc00:10:1:4::4	ICMPv6	64,1	Time Exceeded (hop limit exceeded in transit)
5	0.005832	fc00:10:1:4::4	fc00:10:2:5::5	UDP	1	59665→33436 Len=0
6	0.006411	fc00:10:1:4::1	fc00:10:1:4::4	ICMPv6	64,1	Time Exceeded (hop limit exceeded in transit)
7	0.010828	fc00:10:1:4::4	fc00:10:2:5::5	UDP	2	64584→33437 Len=0
8	0.011692	fc00:10:1:2::2	fc00:10:1:4::4	ICMPv6	63,1	Time Exceeded (hop limit exceeded in transit)
9	0.016235	fc00:10:1:4::4	fc00:10:2:5::5	UDP	2	51662→33438 Len=0
	0.017019	fc00:10:1:2::2	fc00:10:1:4::4	ICMPv6	63,1	Time Exceeded (hop limit exceeded in transit)
	0.021403	fc00:10:1:4::4	fc00:10:2:5::5	UDP	2	65394→33439 Len=0
	0.021681	fc00:10:1:2::2	fc00:10:1:4::4	ICMPv6	63,1	Time Exceeded (hop limit exceeded in transit)

```
▶ Frame 2: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
▶ Ethernet II, Src: 00:00:a6:16:00:01, Dst: 00:00:a6:16:00:04
▶ Internet Protocol Version 6, Src: fc00:10:1:4::1, Dst: fc00:10:1:4::4
▼ Internet Control Message Protocol v6
    Type: Time Exceeded (3)
    Code: 0 (hop limit exceeded in transit)
    Checksum: 0x936c [correct]
    [Checksum Status: Good]
    Reserved: 00000000
  ▶ Internet Protocol Version 6, Src: fc00:10:1:4::4, Dst: fc00:10:2:5::5
  ▶ User Datagram Protocol, Src Port: 59674, Dst Port: 33434
```

Type 3 is "time exceeded"
Code 0 means "hop limit"

Encapsulates original UDP probe

ICMPv6 Port-unreachable

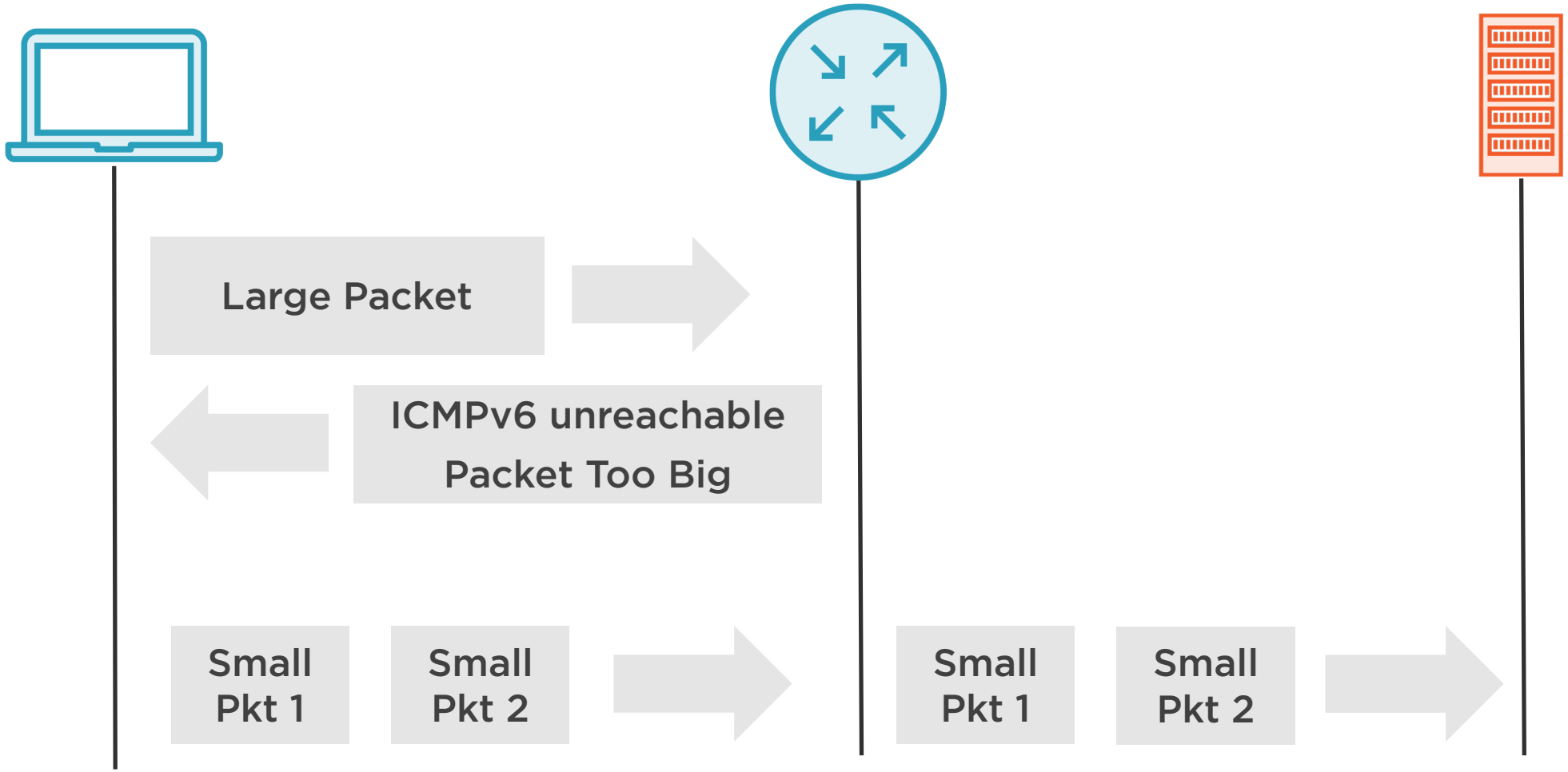
No.	Time ▲	Source	Destination	Protocol	Hop limit	Info
	0.027377	fc00:10:1:4::4	fc00:10:2:5::5	UDP	3	53021→33440 Len=0
	0.028218	fc00:10:2:5::5	fc00:10:1:4::4	ICMPv6	62,1	Destination Unreachable (Port unreachable)
	0.032884	fc00:10:1:4::4	fc00:10:2:5::5	UDP	3	60249→33441 Len=0
	0.033419	fc00:10:2:5::5	fc00:10:1:4::4	ICMPv6	62,1	Destination Unreachable (Port unreachable)
	0.035217	fc00:10:1:4::4	fc00:10:2:5::5	UDP	3	57782→33442 Len=0
	0.035738	fc00:10:2:5::5	fc00:10:1:4::4	ICMPv6	62,1	Destination Unreachable (Port unreachable)

```
▶ Frame 14: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
▶ Ethernet II, Src: 00:00:a6:16:00:01, Dst: 00:00:a6:16:00:04
▶ Internet Protocol Version 6, Src: fc00:10:2:5::5, Dst: fc00:10:1:4::4
▼ Internet Control Message Protocol v6
    Type: Destination Unreachable (1)
    Code: 4 (Port unreachable)
    Checksum: 0x9562 [correct]
    [Checksum Status: Good]
    Reserved: 00000000
  ▶ Internet Protocol Version 6, Src: fc00:10:1:4::4, Dst: fc00:10:2:5::5
  ▶ User Datagram Protocol, Src Port: 53021, Dst Port: 33440
```

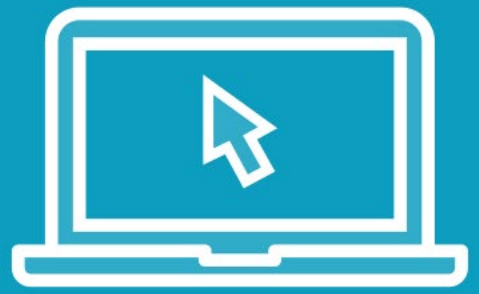
Type 1 is "unreachable"
Code 4 means "layer-4 port"

Encapsulates original UDP probe

IPv6 MTU Signaling and "Fragmentation"



Demo



Smarter Fragmentation with IPv6

ICMPv6 "Packet Too Big"

No.	Time	Source	Destination	Protocol	Payload length	Info
1	0.000000	fc00:10:1:4::4	fc00:10:2:5::5	ICMPv6	1360	Echo (ping) request id=0x0ace, seq=0, hop limit=64 (reply in 2)
2	0.000347	fc00:10:2:5::5	fc00:10:1:4::4	ICMPv6	1360	Echo (ping) reply id=0x0ace, seq=0, hop limit=62 (request in 1)
3	1.563591	fc00:10:1:4::4	fc00:10:2:5::5	ICMPv6	1361	Echo (ping) request id=0x1083, seq=0, hop limit=64 (no response found!)
4	1.563809	fc00:10:1:4::1	fc00:10:1:4::4	ICMPv6	1240,1361	Packet Too Big

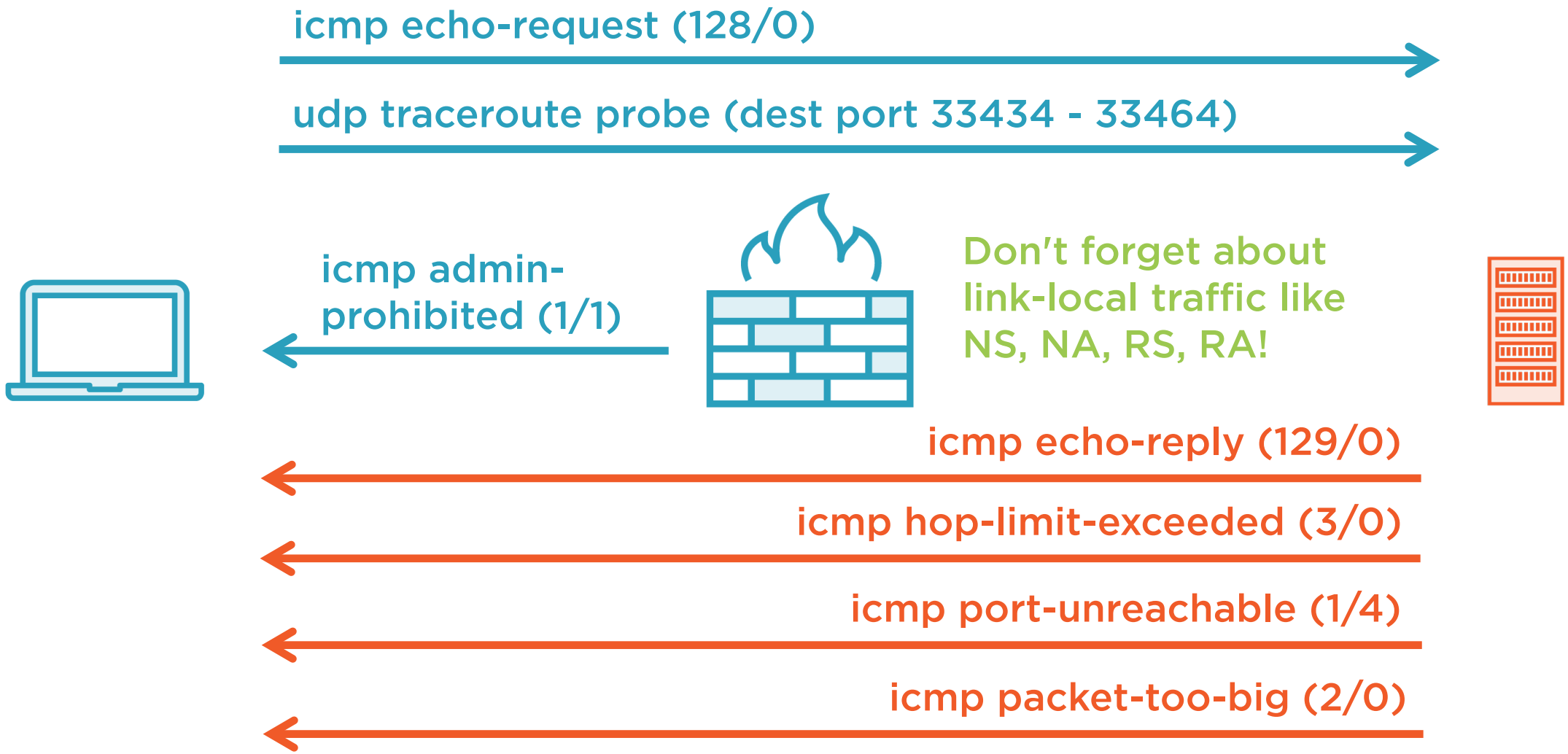
```
▶ Frame 4: 1294 bytes on wire (10352 bits), 1294 bytes captured (10352 bits) on interface 0
▶ Ethernet II, Src: 00:00:a6:16:00:01, Dst: 00:00:a6:16:00:04
▶ Internet Protocol Version 6, Src: fc00:10:1:4::1, Dst: fc00:10:1:4::4
▼ Internet Control Message Protocol v6
    Type: Packet Too Big (2)
    Code: 0
    Checksum: 0x917b [correct]
    [Checksum Status: Good]
    MTU: 1400
  ▶ Internet Protocol Version 6, Src: fc00:10:1:4::4, Dst: fc00:10:2:5::5
  ▶ Internet Control Message Protocol v6
```

Type 2 is "packet too big" (no codes)

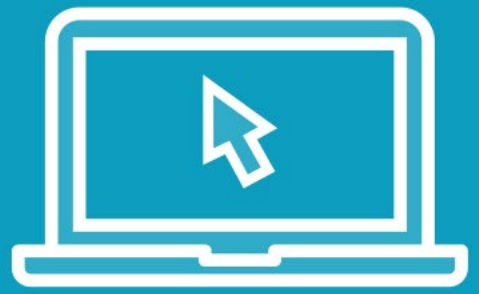
Reveals the MTU

Encapsulates original packet

Firewall Design for ICMPv6



Demo



Firewalling for ICMPv6

ICMPv6 Admin-prohibited

No.	Time	Source	Destination	Protocol	Info
1	0.000000	fc00:10:1:4::4	fc00:10:2:5::5	TCP	20722→80 [SYN] Seq=0 Win=4128 Len=0 MSS=516
2	0.000609	fc00:10:1:3::3	fc00:10:1:4::4	ICMPv6	Destination Unreachable (Administratively prohibited)

```
▶ Frame 2: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface 0
▶ Ethernet II, Src: 00:00:a6:16:00:01, Dst: 00:00:a6:16:00:04
▶ Internet Protocol Version 6, Src: fc00:10:1:3::3, Dst: fc00:10:1:4::4
▼ Internet Control Message Protocol v6
    Type: Destination Unreachable (1)
    Code: 1 (Administratively prohibited)
    Checksum: 0x9352 [correct]
    [Checksum Status: Good]
    Reserved: 00000000
  ▶ Internet Protocol Version 6, Src: fc00:10:1:4::4, Dst: fc00:10:2:5::5
  ▶ Transmission Control Protocol, Src Port: 20722, Dst Port: 80, Seq: 1161381482
```

Type 1 is "unreachable"
Code 1 is "firewall denied"

Encapsulates original packet

Final Thoughts

IPv4 and IPv6 are similar

Study IPv6 ND

Thank you!