Using Traceroute

Nick Russo
NETWORK ENGINEER

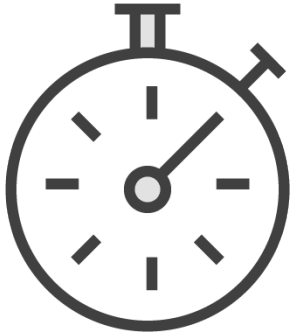
@nickrusso42518 www.njrusmc.net

Agenda

- New ICMP messages
- Traceroute behind the scenes
- Traceroute in action
- Packet analysis
- Troubleshooting with traceroute

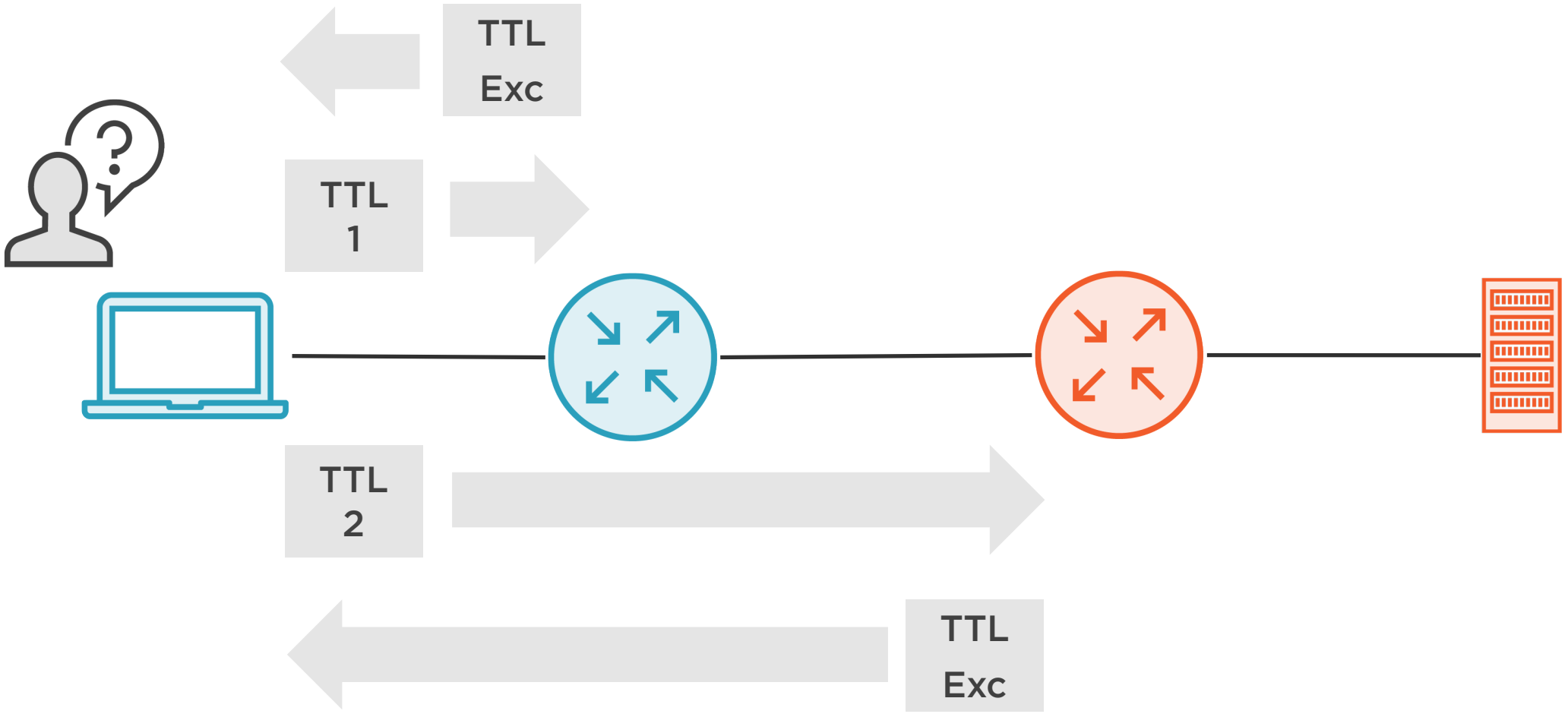
New ICMP Messages with Traceroute

TTL Exceeded

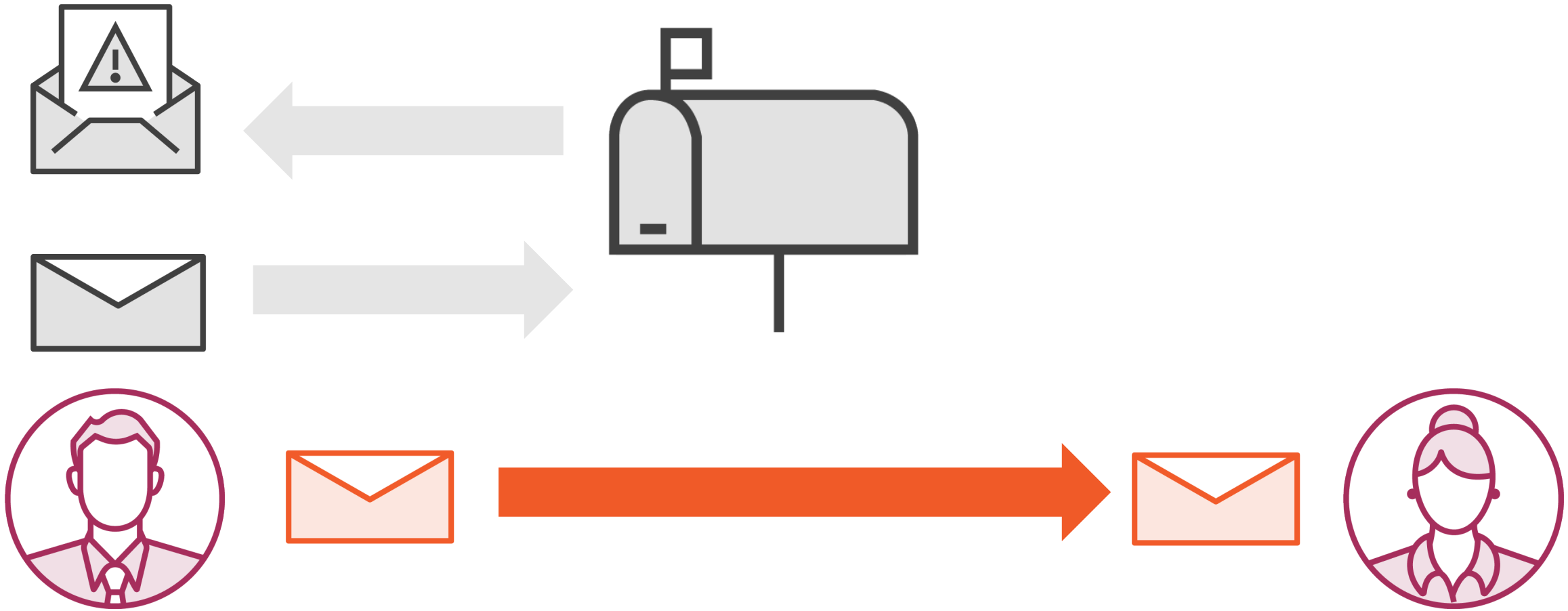


Port Unreachable

ICMP TTL-exceeded (11/0)

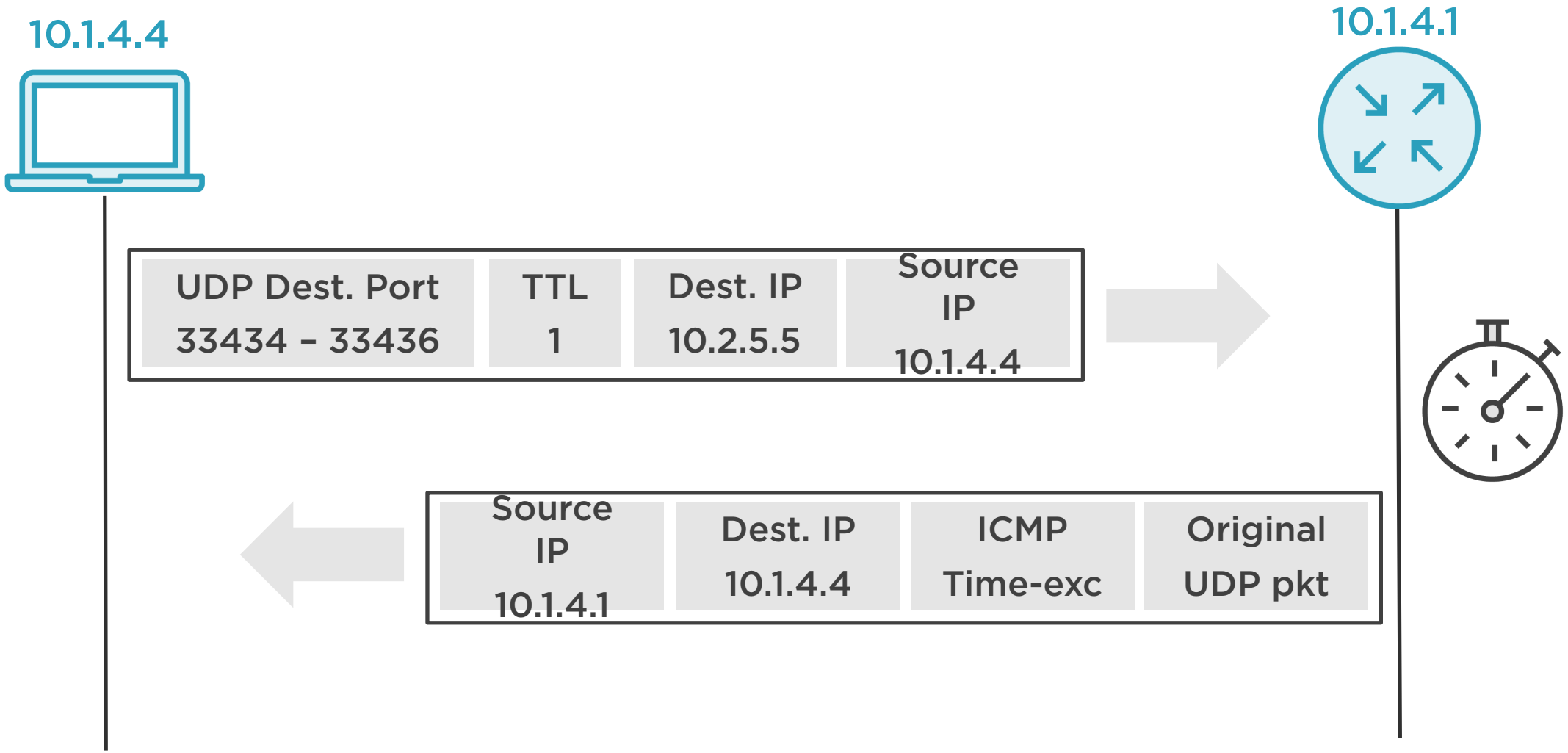


ICMP TTL-exceeded with Postage

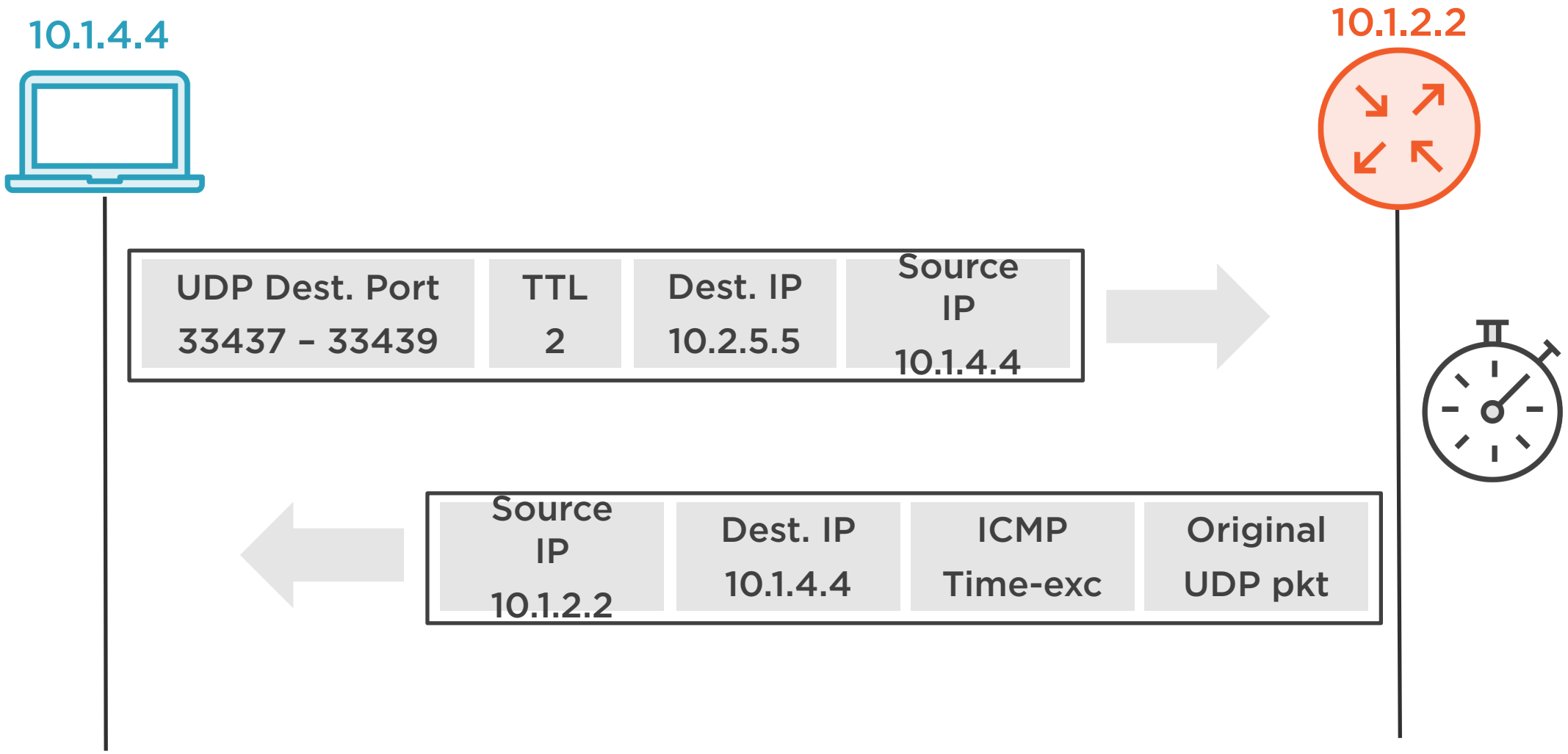


ICMP Port-unreachable (3/3)

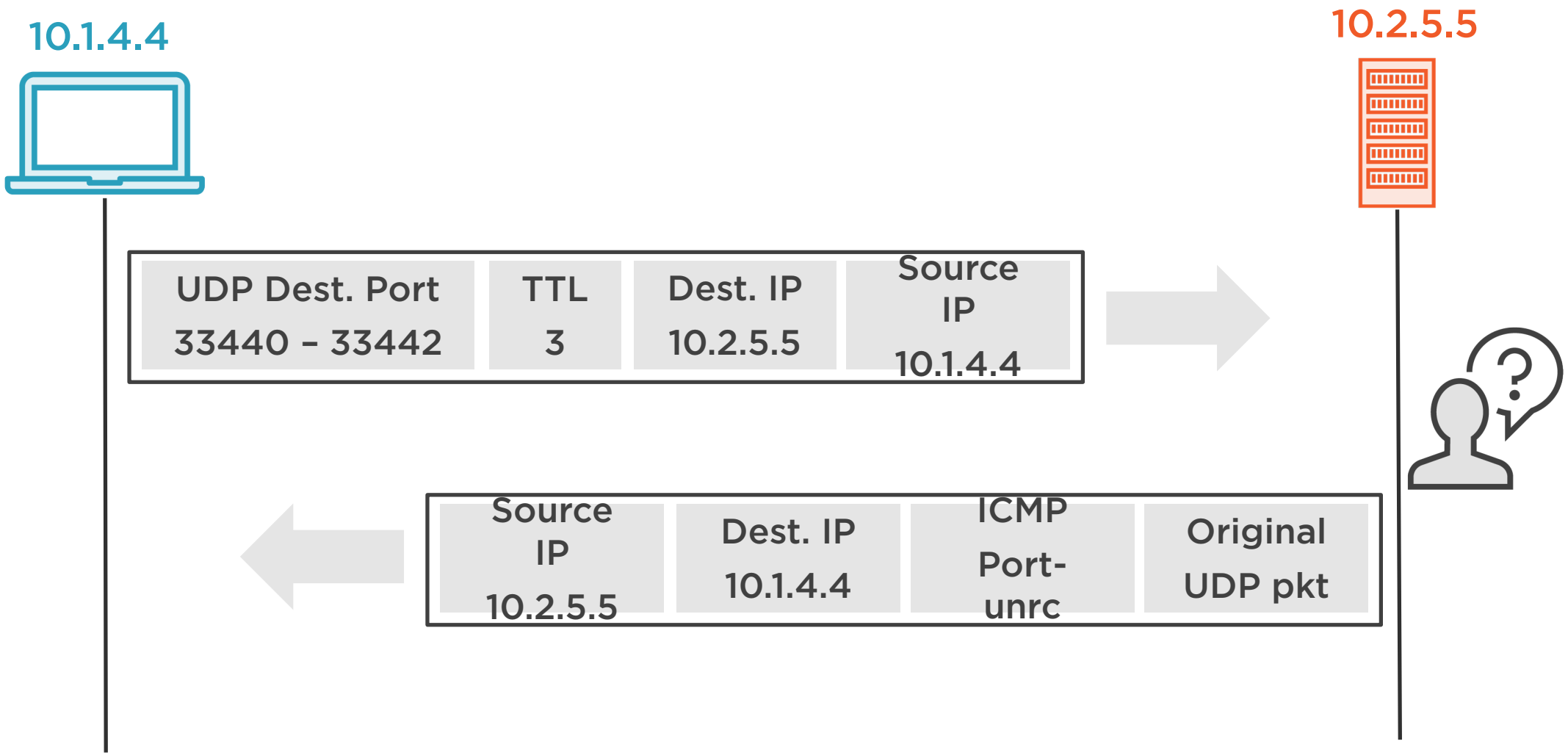
Traceroute Packet Flow – First Hop



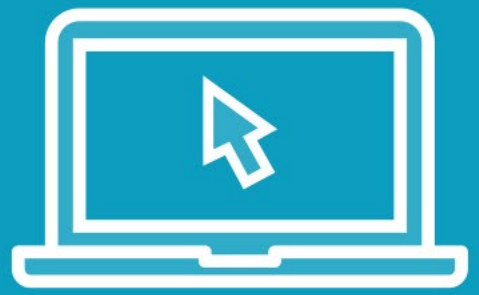
Traceroute Packet Flow – Second Hop



Traceroute Packet Flow – Termination



Demo



Traceroute in action

UDP Traceroute Probe

No.	Time	Source	Destination	Protocol	Time to live	Info
1	0.000000	10.1.4.4	10.2.5.5	UDP	1	49154→33434 Len=0
2	0.000460	10.1.4.1	10.1.4.4	ICMP	255,1	Time-to-live exceeded (Time to live exceeded in transit)
3	0.000627	10.1.4.4	10.2.5.5	UDP	1	49155→33435 Len=0
4	0.001082	10.1.4.1	10.1.4.4	ICMP	255,1	Time-to-live exceeded (Time to live exceeded in transit)
5	0.001212	10.1.4.4	10.2.5.5	UDP	1	49156→33436 Len=0
6	0.001624	10.1.4.1	10.1.4.4	ICMP	255,1	Time-to-live exceeded (Time to live exceeded in transit)

```
▶ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▶ Ethernet II, Src: 00:00:a6:16:00:04, Dst: 00:00:a6:16:00:01
▶ Internet Protocol Version 4, Src: 10.1.4.4, Dst: 10.2.5.5
▼ User Datagram Protocol, Src Port: 49154, Dst Port: 33434
    Source Port: 49154
    Destination Port: 33434
    Length: 8
    Checksum: 0xa035 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
```

← Target won't be listening

← Remember this checksum

← No payload data

ICMP TTL-exceeded

No.	Time	Source	Destination	Protocol	Time to live	Info
1	0.000000	10.1.4.4	10.2.5.5	UDP	1	49154→33434 Len=0
2	0.000460	10.1.4.1	10.1.4.4	ICMP	255,1	Time-to-live exceeded (Time to live exceeded in transit)
3	0.000627	10.1.4.4	10.2.5.5	UDP	1	49155→33435 Len=0
4	0.001082	10.1.4.1	10.1.4.4	ICMP	255,1	Time-to-live exceeded (Time to live exceeded in transit)
5	0.001212	10.1.4.4	10.2.5.5	UDP	1	49156→33436 Len=0
6	0.001624	10.1.4.1	10.1.4.4	ICMP	255,1	Time-to-live exceeded (Time to live exceeded in transit)

```
▶ Frame 2: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
▶ Ethernet II, Src: 00:00:a6:16:00:01, Dst: 00:00:a6:16:00:04
▶ Internet Protocol Version 4, Src: 10.1.4.1, Dst: 10.1.4.4
▼ Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0x1225 [correct]
    [Checksum Status: Good]
  ▶ Internet Protocol Version 4, Src: 10.1.4.4, Dst: 10.2.5.5
  ▼ User Datagram Protocol, Src Port: 49154, Dst Port: 33434
      Source Port: 49154
      Destination Port: 33434
      Length: 8
      Checksum: 0xa035 [unverified]
      [Checksum Status: Unverified]
      [Stream index: 0]
```

Type 11 is "time exceeded"
Code 0 means "in transit"

Encapsulates original UDP probe

Look familiar?

ICMP Port-unreachable

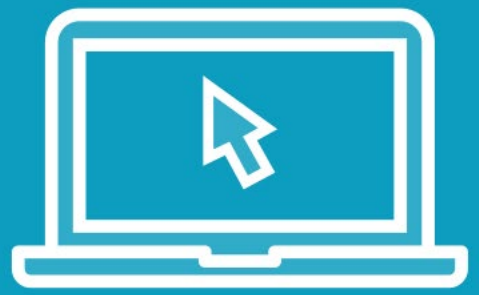
No.	Time	Source	Destination	Protocol	Time to live	Info
	0.012680	10.1.4.4	10.2.5.5	UDP	3	49160→33440 Len=0
	0.013327	10.2.5.5	10.1.4.4	ICMP	253,1	Destination unreachable (Port unreachable)
	0.013513	10.1.4.4	10.2.5.5	UDP	3	49161→33441 Len=0
	0.013760	10.2.5.5	10.1.4.4	ICMP	253,1	Destination unreachable (Port unreachable)
	0.018151	10.1.4.4	10.2.5.5	UDP	3	49162→33442 Len=0
	0.018852	10.2.5.5	10.1.4.4	ICMP	253,1	Destination unreachable (Port unreachable)

```
▶ Frame 14: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
▶ Ethernet II, Src: 00:00:a6:16:00:01, Dst: 00:00:a6:16:00:04
▶ Internet Protocol Version 4, Src: 10.2.5.5, Dst: 10.1.4.4
▼ Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
    Checksum: 0x1a22 [correct]
    [Checksum Status: Good]
    Unused: 00000000
  ▶ Internet Protocol Version 4, Src: 10.1.4.4, Dst: 10.2.5.5
  ▼ User Datagram Protocol, Src Port: 49160, Dst Port: 33440
      Source Port: 49160
    ▶ Destination Port: 33440
      Length: 8
      Checksum: 0xa029 [unverified]
      [Checksum Status: Unverified]
      [Stream index: 6]
```

Type 3 is "unreachable"
Code 3 means "layer-4 port"

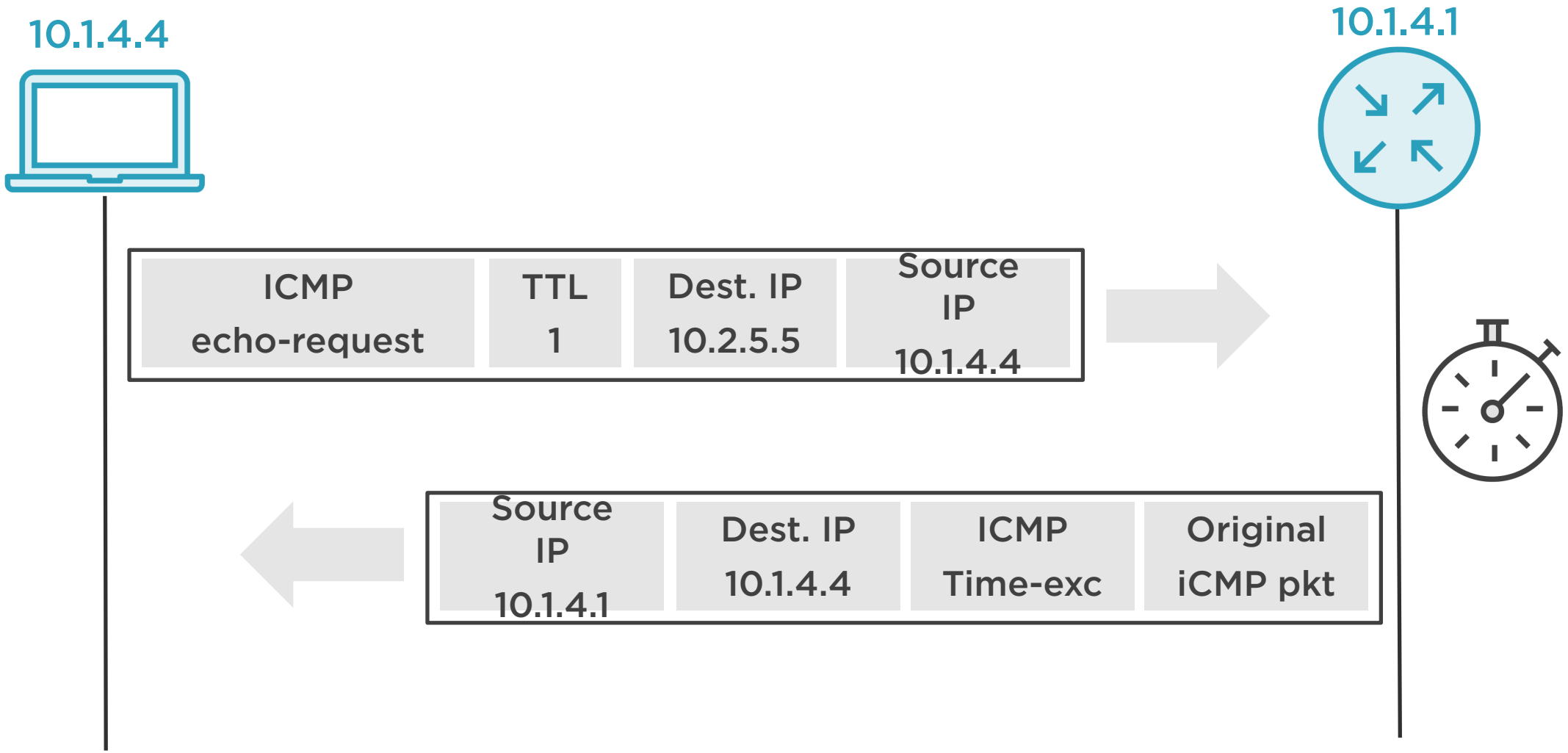
Encapsulates original UDP probe

Demo

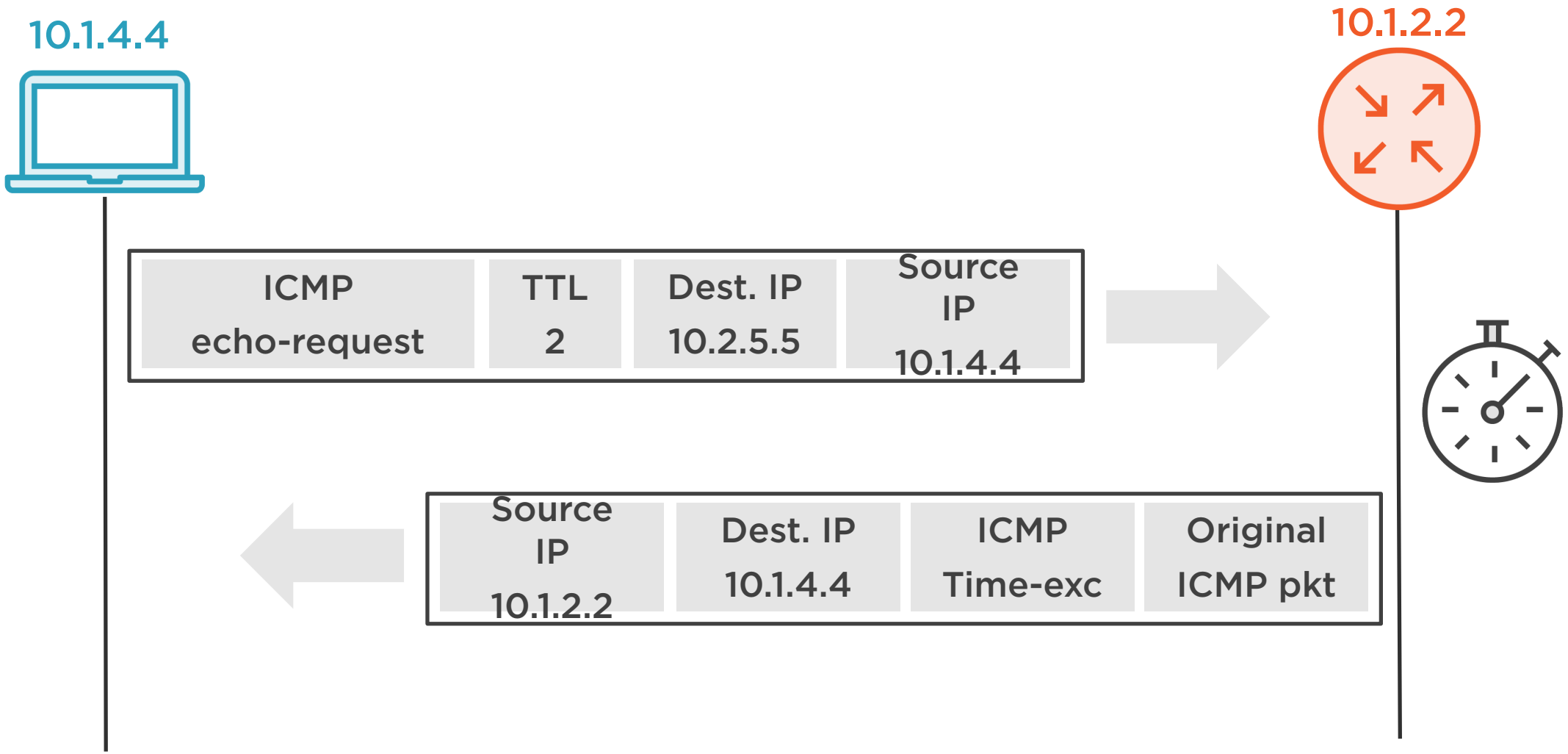


Troubleshooting with traceroute

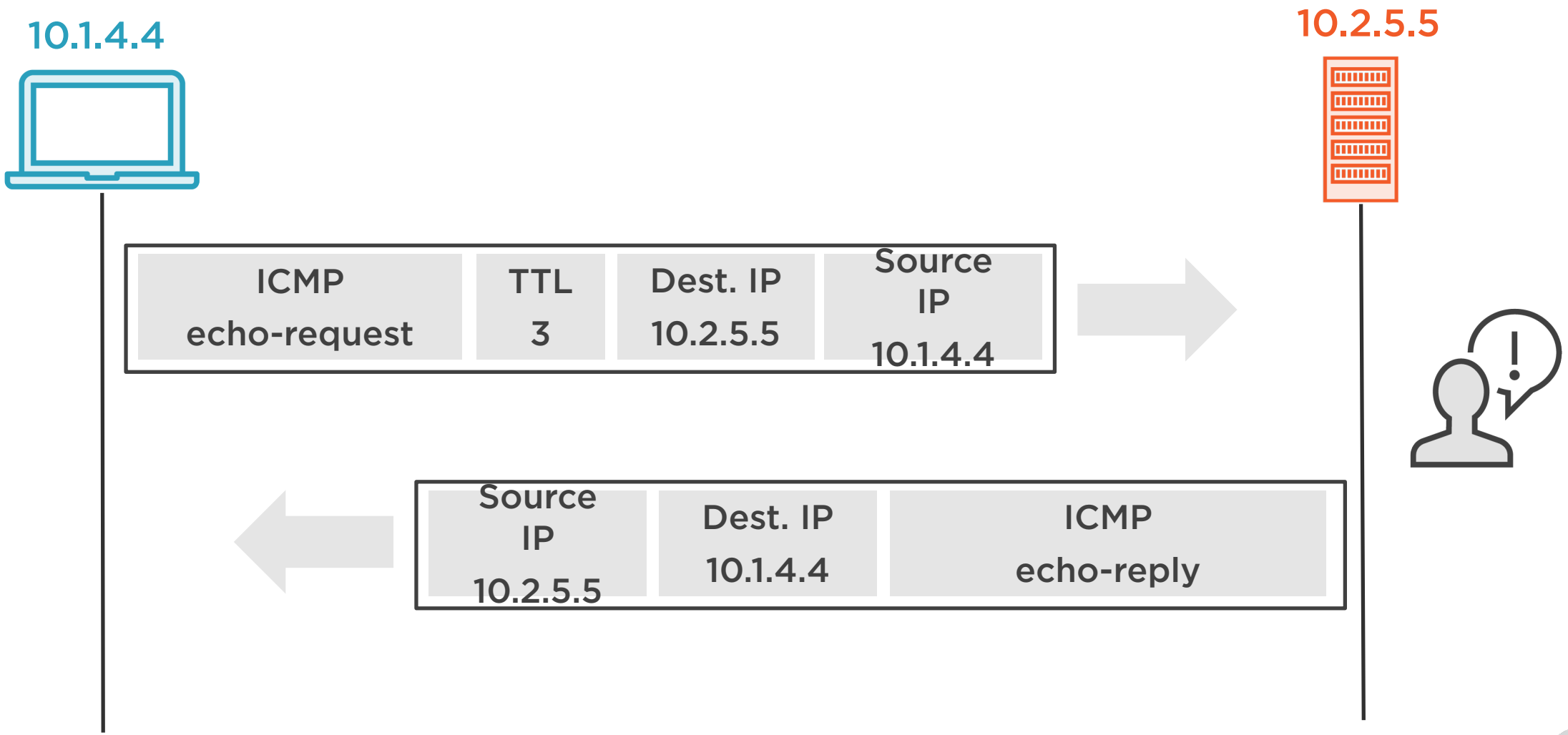
Using ICMP Echo Instead of UDP – First Hop



Using ICMP Echo Instead of UDP – Second Hop



Using ICMP Echo Instead of UDP – Termination



Traceroute In Review

UDP probes +

ICMP replies

TTL exceeded +

Port unrecahable

Used to find path through network