Protocol Deep Dive: ICMP

USING PING

Nick Russo
NETWORK ENGINEER

@nickrusso42518 www.njrusmc.net

Agenda

- Take a step back ... Why ICMP?
- Ping in action
- Packet analysis
- Troubleshooting with ping

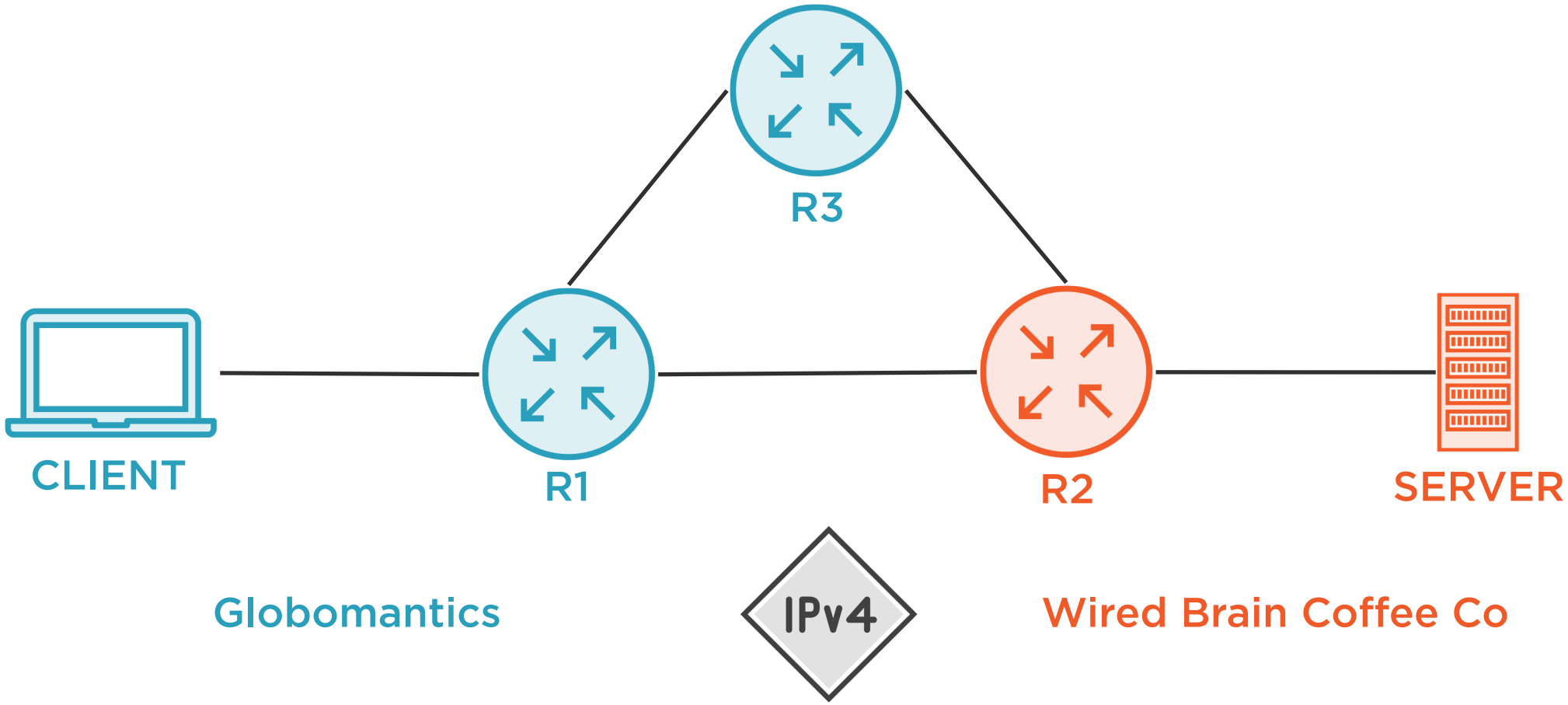
What Is ICMP?

Internet Control Message Protocol

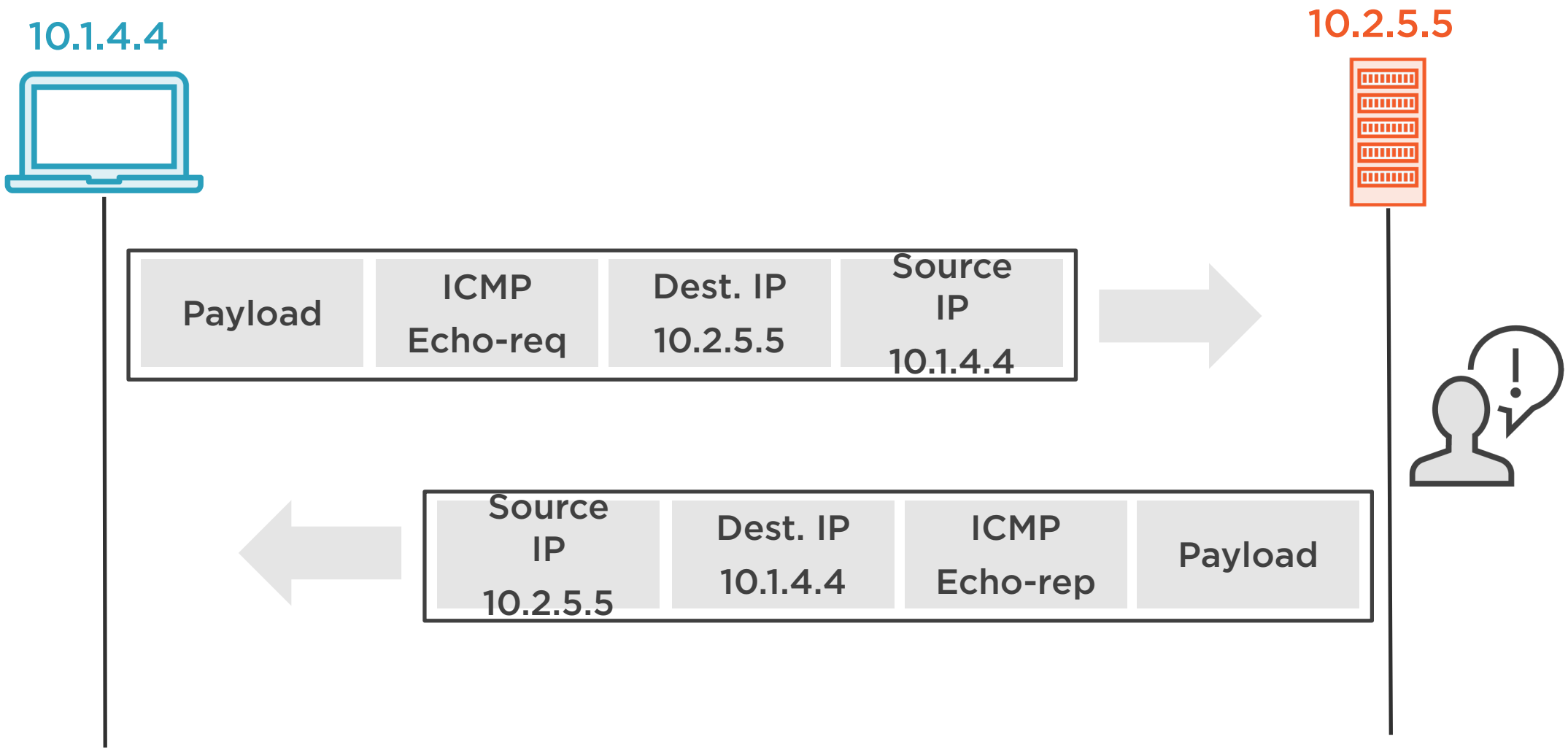
RFC 792

More than ping ... but ping best known

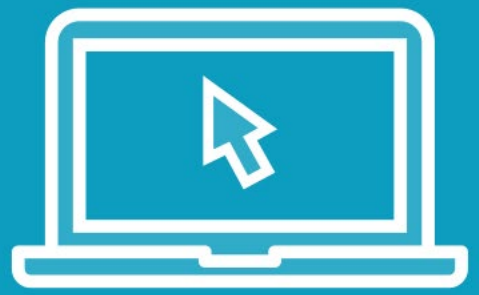
Our Network


R3
CLIENT
R1
R2
SERVER
Globomantics
IPv4
Wired Brain Coffee Co

Ping Packet Flow



Demo



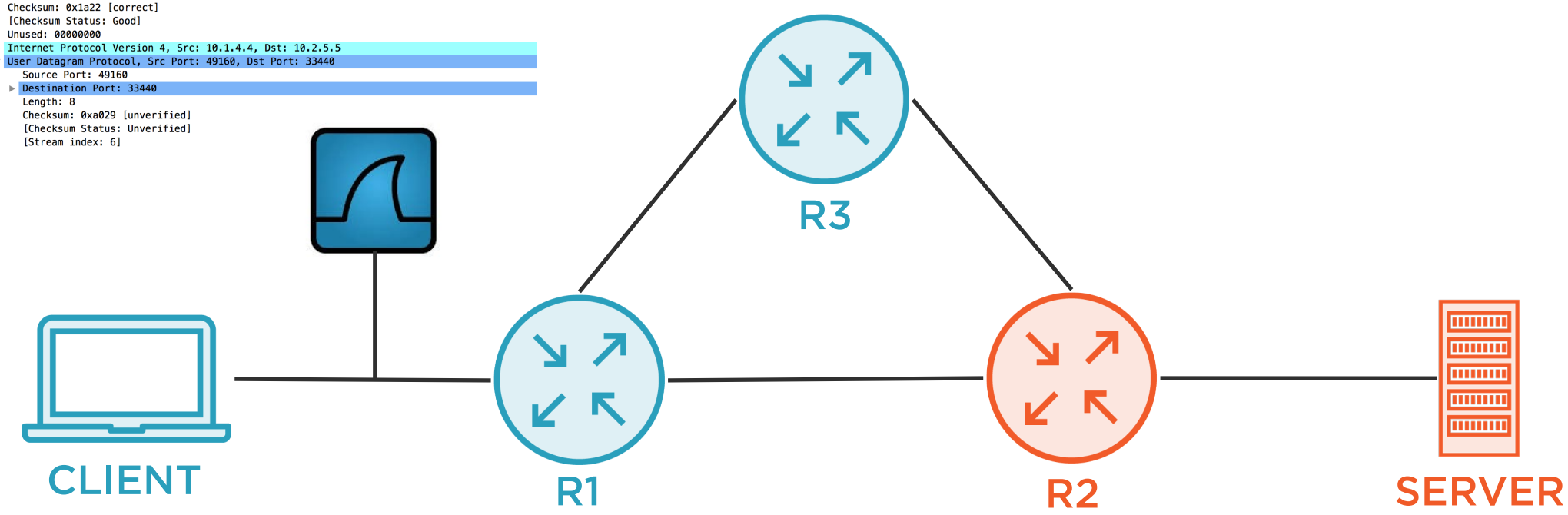
Ping in action

Detour: Wireshark

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]
```

Free download:
wireshark.org



ICMP Echo-request

No.	Time	Source	Destination	Protocol	Info
→ 1	0.000000	10.1.4.4	10.2.5.5	ICMP	Echo (ping) request id=0x0005, seq=0/0, ttl=255 (reply in 2)
← 2	0.000627	10.2.5.5	10.1.4.4	ICMP	Echo (ping) reply id=0x0005, seq=0/0, ttl=253 (request in 1)
3	0.000741	10.1.4.4	10.2.5.5	ICMP	Echo (ping) request id=0x0005, seq=1/256, ttl=255 (reply in 4)
4	0.000996	10.2.5.5	10.1.4.4	ICMP	Echo (ping) reply id=0x0005, seq=1/256, ttl=253 (request in 3)
5	0.001078	10.1.4.4	10.2.5.5	ICMP	Echo (ping) request id=0x0005, seq=2/512, ttl=255 (reply in 6)
6	0.001283	10.2.5.5	10.1.4.4	ICMP	Echo (ping) reply id=0x0005, seq=2/512, ttl=253 (request in 5)
7	0.006586	10.1.4.4	10.2.5.5	ICMP	Echo (ping) request id=0x0005, seq=3/768, ttl=255 (reply in 8)
8	0.007057	10.2.5.5	10.1.4.4	ICMP	Echo (ping) reply id=0x0005, seq=3/768, ttl=253 (request in 7)
9	0.012692	10.1.4.4	10.2.5.5	ICMP	Echo (ping) request id=0x0005, seq=4/1024, ttl=255 (reply in 10)
	0.013141	10.2.5.5	10.1.4.4	ICMP	Echo (ping) reply id=0x0005, seq=4/1024, ttl=253 (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 4, Src: 10.1.4.4, Dst: 10.2.5.5
▼ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xe180 [correct]
    [Checksum Status: Good]
    Identifier (BE): 5 (0x0005)
    Identifier (LE): 1280 (0x0500)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
    [Response frame: 2]
  ▶ Data (72 bytes)
```

← Type 8 is echo-request (no codes)

← Used to identify process/daemon

← Used to match request to reply

ICMP Echo-reply

No.	Time	Source	Destination	Protocol	Info
→ 1	0.000000	10.1.4.4	10.2.5.5	ICMP	Echo (ping) request id=0x0005, seq=0/0, ttl=255 (reply in 2)
← 2	0.000627	10.2.5.5	10.1.4.4	ICMP	Echo (ping) reply id=0x0005, seq=0/0, ttl=253 (request in 1)
3	0.000741	10.1.4.4	10.2.5.5	ICMP	Echo (ping) request id=0x0005, seq=1/256, ttl=255 (reply in 4)
4	0.000996	10.2.5.5	10.1.4.4	ICMP	Echo (ping) reply id=0x0005, seq=1/256, ttl=253 (request in 3)
5	0.001078	10.1.4.4	10.2.5.5	ICMP	Echo (ping) request id=0x0005, seq=2/512, ttl=255 (reply in 6)
6	0.001283	10.2.5.5	10.1.4.4	ICMP	Echo (ping) reply id=0x0005, seq=2/512, ttl=253 (request in 5)
7	0.006586	10.1.4.4	10.2.5.5	ICMP	Echo (ping) request id=0x0005, seq=3/768, ttl=255 (reply in 8)
8	0.007057	10.2.5.5	10.1.4.4	ICMP	Echo (ping) reply id=0x0005, seq=3/768, ttl=253 (request in 7)
9	0.012692	10.1.4.4	10.2.5.5	ICMP	Echo (ping) request id=0x0005, seq=4/1024, ttl=255 (reply in 10)
	0.013141	10.2.5.5	10.1.4.4	ICMP	Echo (ping) reply id=0x0005, seq=4/1024, ttl=253 (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 4, Src: 10.2.5.5, Dst: 10.1.4.4
▼ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xe980 [correct]
    [Checksum Status: Good]
    Identifier (BE): 5 (0x0005)
    Identifier (LE): 1280 (0x0500)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
    [Request frame: 1]
    [Response time: 0.627 ms]
  ▶ Data (72 bytes)
```

← Type 0 is echo-reply (no codes)

← Replying node retains value

← Replying node retains value

Interesting ICMP Type/Code Examples

Type 8: ICMP echo-request

Code 0: No code

Type 0: ICMP echo-reply

Code 0: No code

Type 3: Destination unreachable

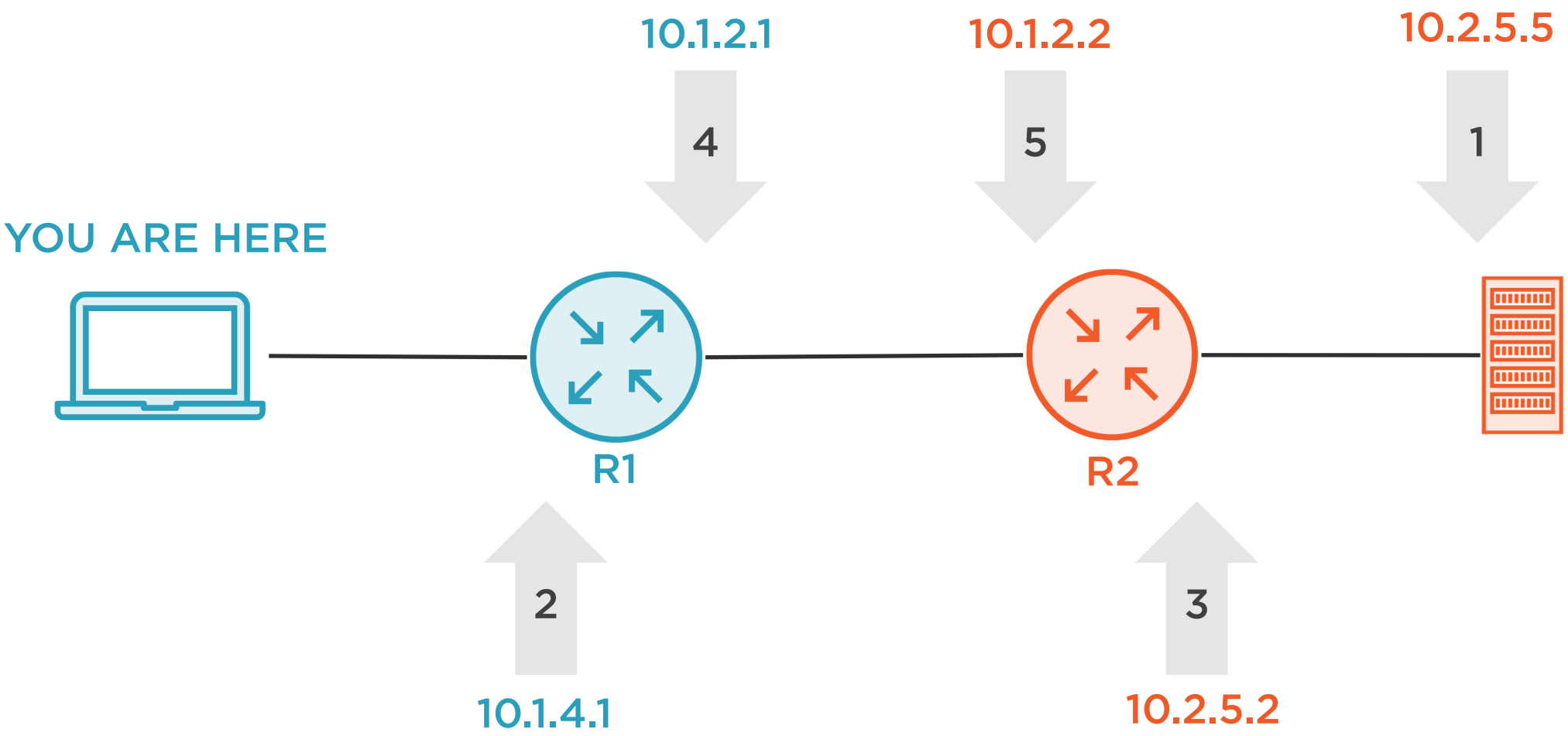
Code 3: Port unreachable

Code 4: Packet Too Big

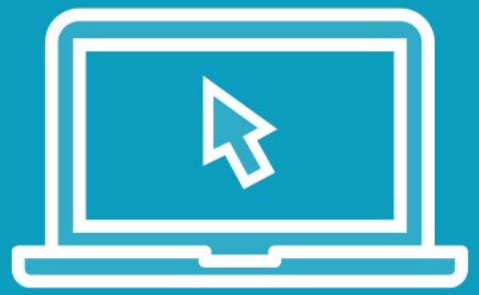
Code 13: Admin prohibited

... up to 15!

Finding the Fault



Demo



Troubleshooting with ping

ICMP Ping In Review

Test connectivity

Per-packet accounting

Outside in troubleshooting