Conquering the Fear of Fragmentation

Nick Russo
NETWORK ENGINEER

@nickrusso42518 www.njrusmc.net

Agenda

Fragmentation ... Who cares?

Discovering MTU

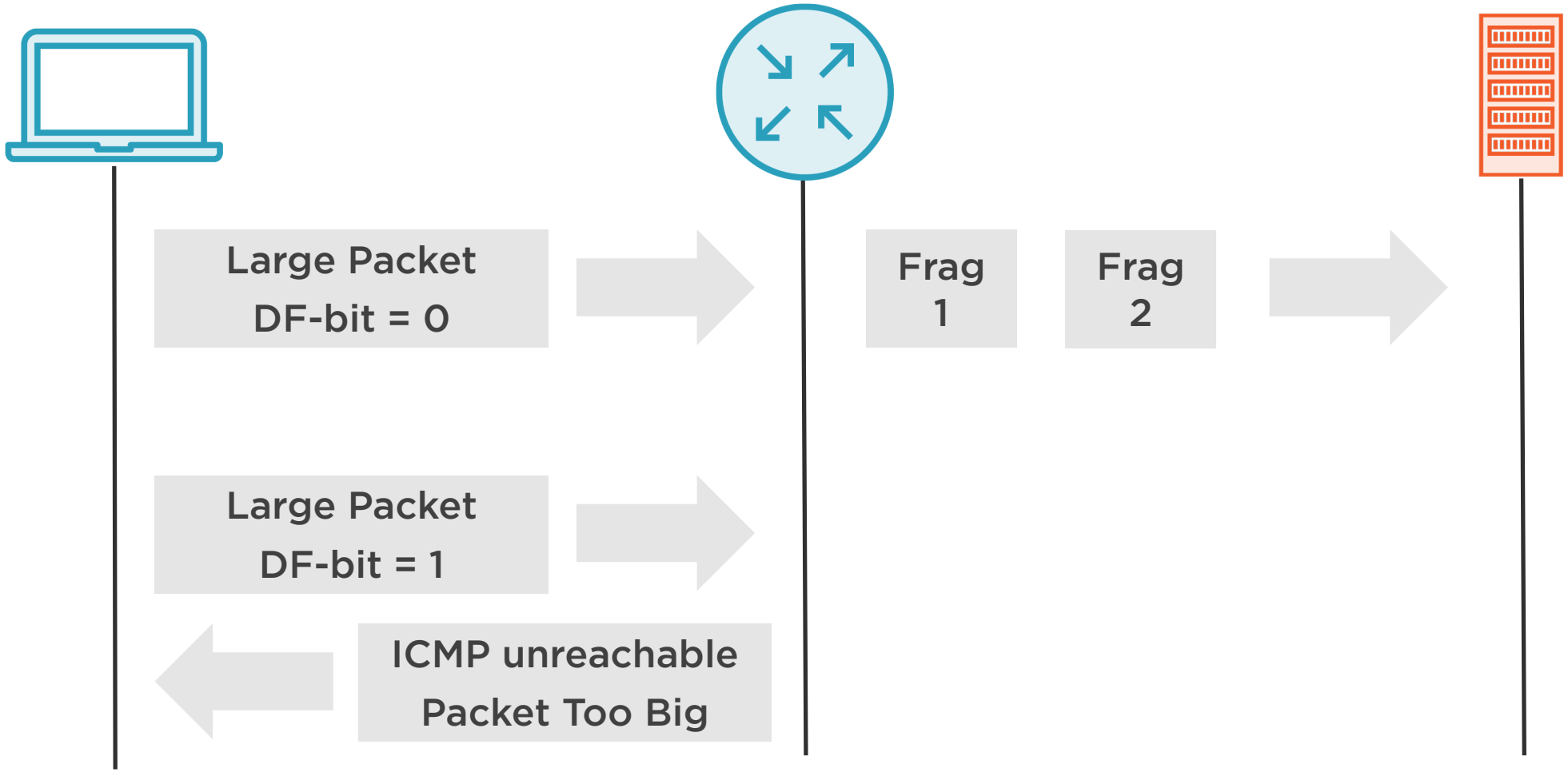
- Using ping bracketing
- Using ping sweeping

Packet analysis

Fragmentation

Break large packets into smaller packets (fragments), so that the resulting pieces can pass through a link with a smaller MTU than the original packet size.

The IPv4 "Don't Fragment" (DF) Bit



Fragmentation Discussed

Advantages

Increased application portability

Disadvantages

Compute-intensive on routers (IPv4)

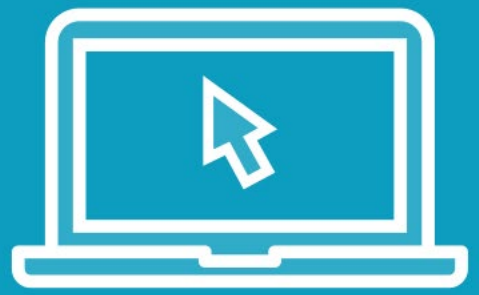
Compute-intensive on targets

Reduced application performance

Increased encapsulation

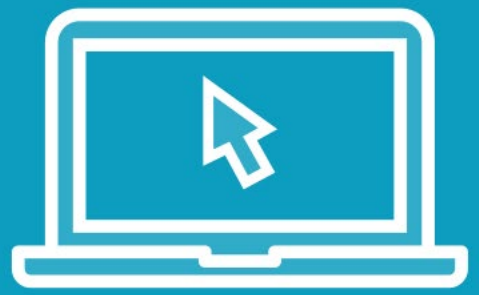
Attack vector

Demo



MTU Discovery via Ping Bracketing

Demo



MTU Discovery via Ping Sweeping

Packet with DF-bit Set

No.	Time	Source	Destination	Protocol	Total Length	Info
1	0.000000	10.1.4.4	10.2.5.5	ICMP	1400	Echo (ping) request id=0x0003, seq=0/0, ttl=255 (reply in 2)
2	0.000893	10.2.5.5	10.1.4.4	ICMP	1400	Echo (ping) reply id=0x0003, seq=0/0, ttl=253 (request in 1)
3	2.691457	10.1.4.4	10.2.5.5	ICMP	1401	Echo (ping) request id=0x0004, seq=0/0, ttl=255 (no response found!)
4	2.691716	10.1.4.1	10.1.4.4	ICMP	56,1401	Destination unreachable (Fragmentation needed)

```
▶ Frame 3: 1415 bytes on wire (11320 bits), 1415 bytes captured (11320 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
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1401                          ← Large packet
    Identification: 0x0010 (16)
  ▶ Flags: 0x02 (Don't Fragment)                ← DF-bit is set
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x5968 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.1.4.4
    Destination: 10.2.5.5
▶ Internet Control Message Protocol
```

ICMP "Packet Too Big"

No.	Time	Source	Destination	Protocol	Total Length	Info
1	0.000000	10.1.4.4	10.2.5.5	ICMP	1400	Echo (ping) request id=0x0003, seq=0/0, ttl=255 (reply in 2)
2	0.000893	10.2.5.5	10.1.4.4	ICMP	1400	Echo (ping) reply id=0x0003, seq=0/0, ttl=253 (request in 1)
3	2.691457	10.1.4.4	10.2.5.5	ICMP	1401	Echo (ping) request id=0x0004, seq=0/0, ttl=255 (no response found!)
4	2.691716	10.1.4.1	10.1.4.4	ICMP	56,1401	Destination unreachable (Fragmentation needed)

```
▶ Frame 4: 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: 3 (Destination unreachable)
    Code: 4 (Fragmentation needed)
    Checksum: 0x076d [correct]
    [Checksum Status: Good]
    Unused: 0000
    MTU of next hop: 1400
  ▶ Internet Protocol Version 4, Src: 10.1.4.4, Dst: 10.2.5.5
  ▶ Internet Control Message Protocol
```

Type 3 is "unreachable"
Code 4 is "packet too big"

Reveals the MTU

Encapsulates original packet

Fragmentation In Review

Minimum MTU along path

Packet-too-big

Security risks