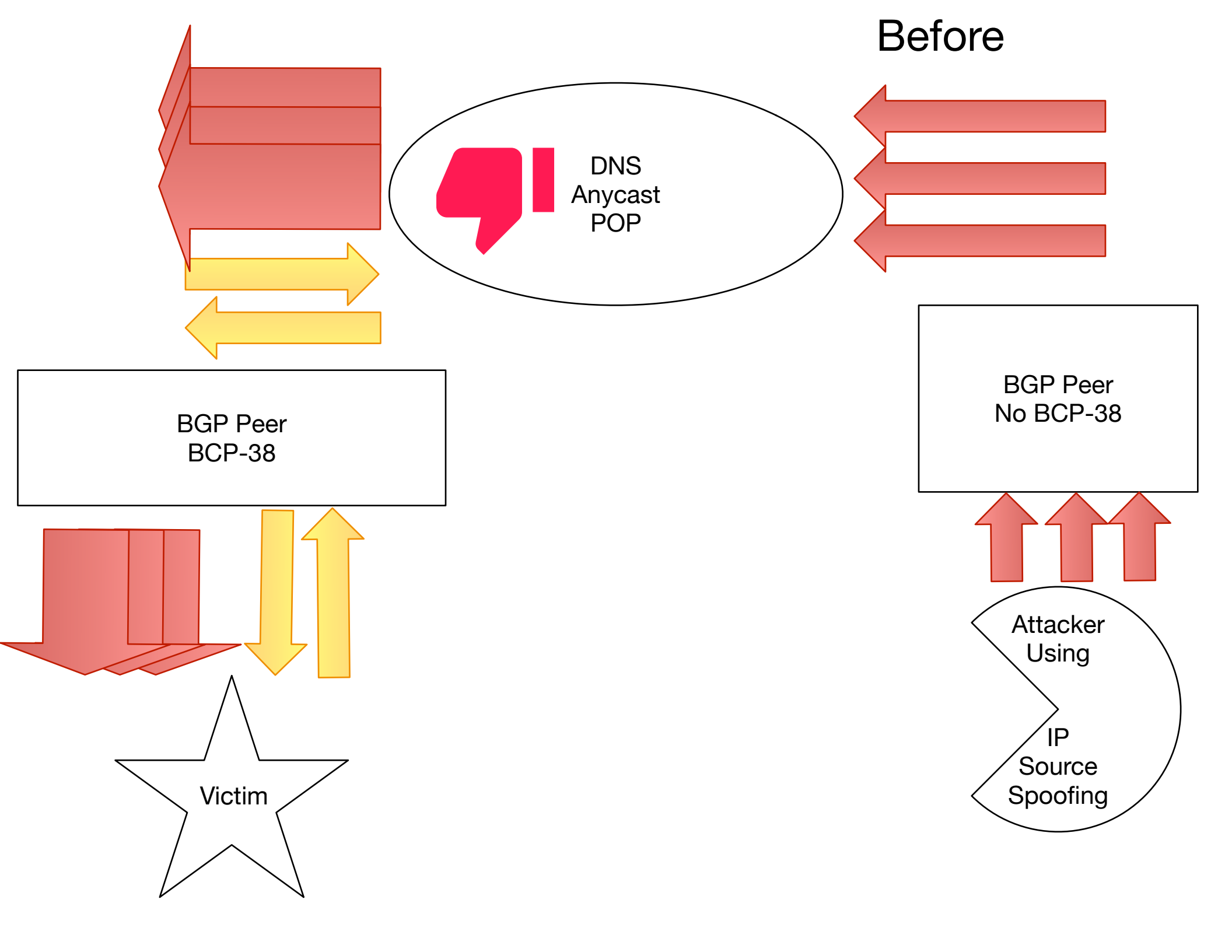
Sending UDP Responses by MAC Address

Before

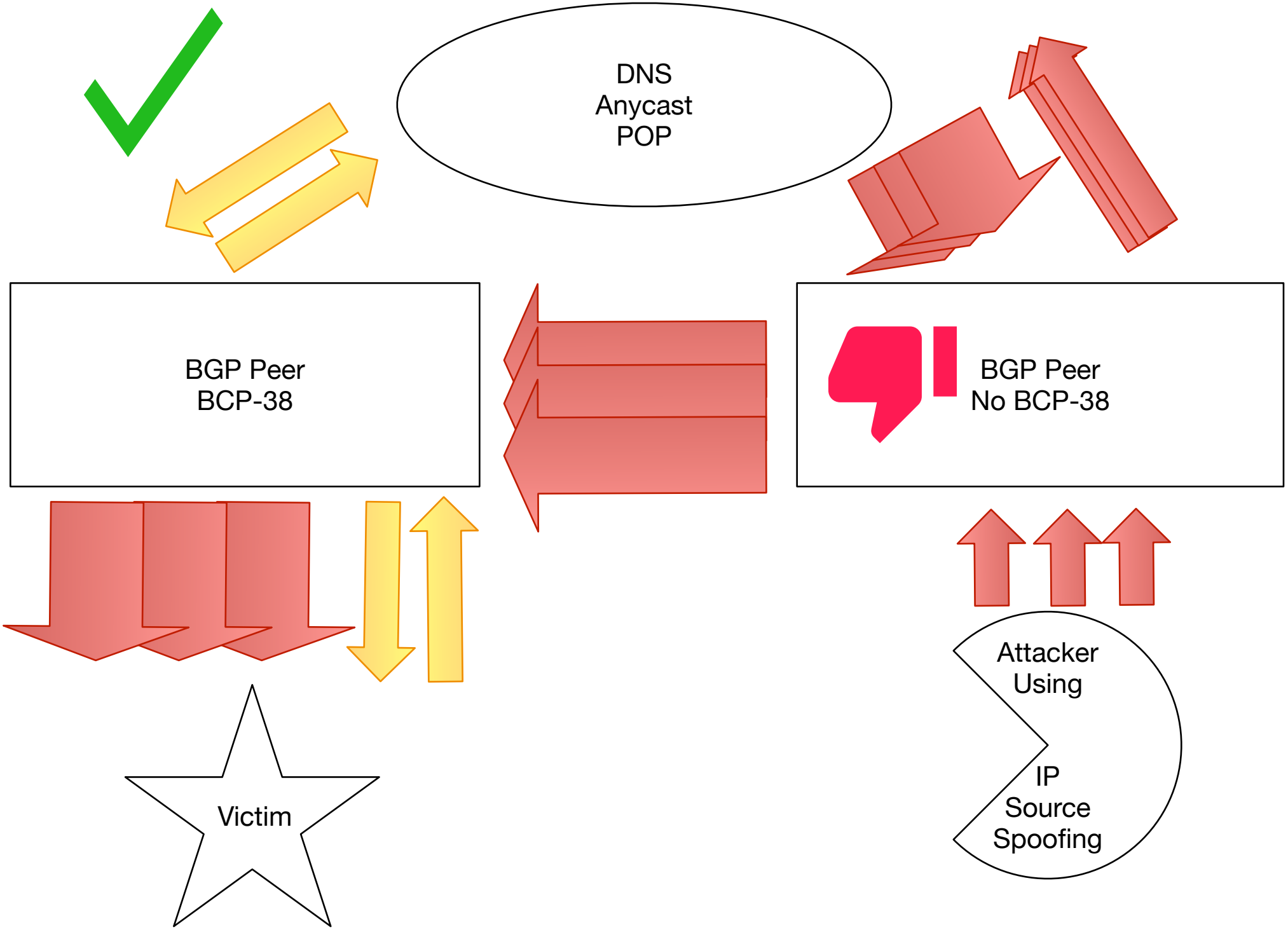
- Response packets get routed
- Spoofed and non-spoofed queries, have responses intermingled
- Shared-fate: non-victim responses on destination path, become collateral damage
- Authority DNS operators MUST be involved in resolving DDOS amplification attacks which use their DNS servers as the “attack vector”
- Not much leverage against ISPs that do not block spoofed source DNS packets

Sending UDP Response by MAC Address

- Responses get sent back to *original* incoming network
- Spoofed and non-spoofed queries, have responses separated if queries are separate
- ISPs who don't allow spoofed packets, get "clean" incoming traffic
- Non-victim responses on *sending* connection, become collateral damage
- Authority DNS operators NO LONGER need to be involved in resolving DDOS attacks
- Victim ISP sees attack traffic coming from the "bad" ISP that allows the spoofed packets
- Strong pressure against ISPs that do not block spoofed source DNS packets


Before
DNS
Anycast
POP
BGP Peer
BCP-38
BGP Peer
No BCP-38
Attacker
Using
IP
Source
Spoofing
Victim

After


DNS
Anycast
POP
BGP Peer
BCP-38
BGP Peer
No BCP-38
Victim
Attacker
Using
IP
Source
Spoofing