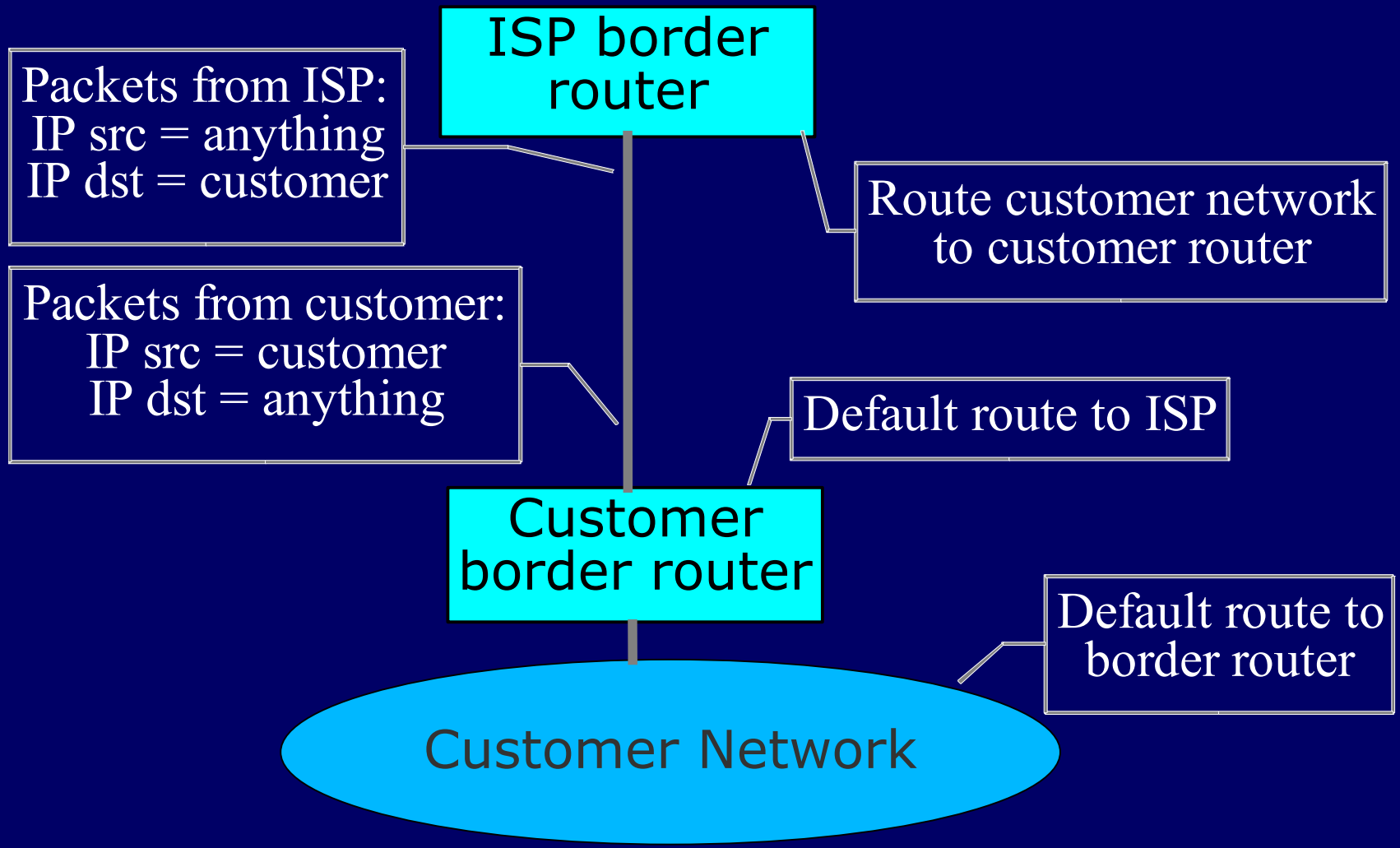
Filtering Spoofed Packets

Network Ingress Filtering (BCP 38)

What are spoofed or forged packets?
Why are they bad?
How to keep them out

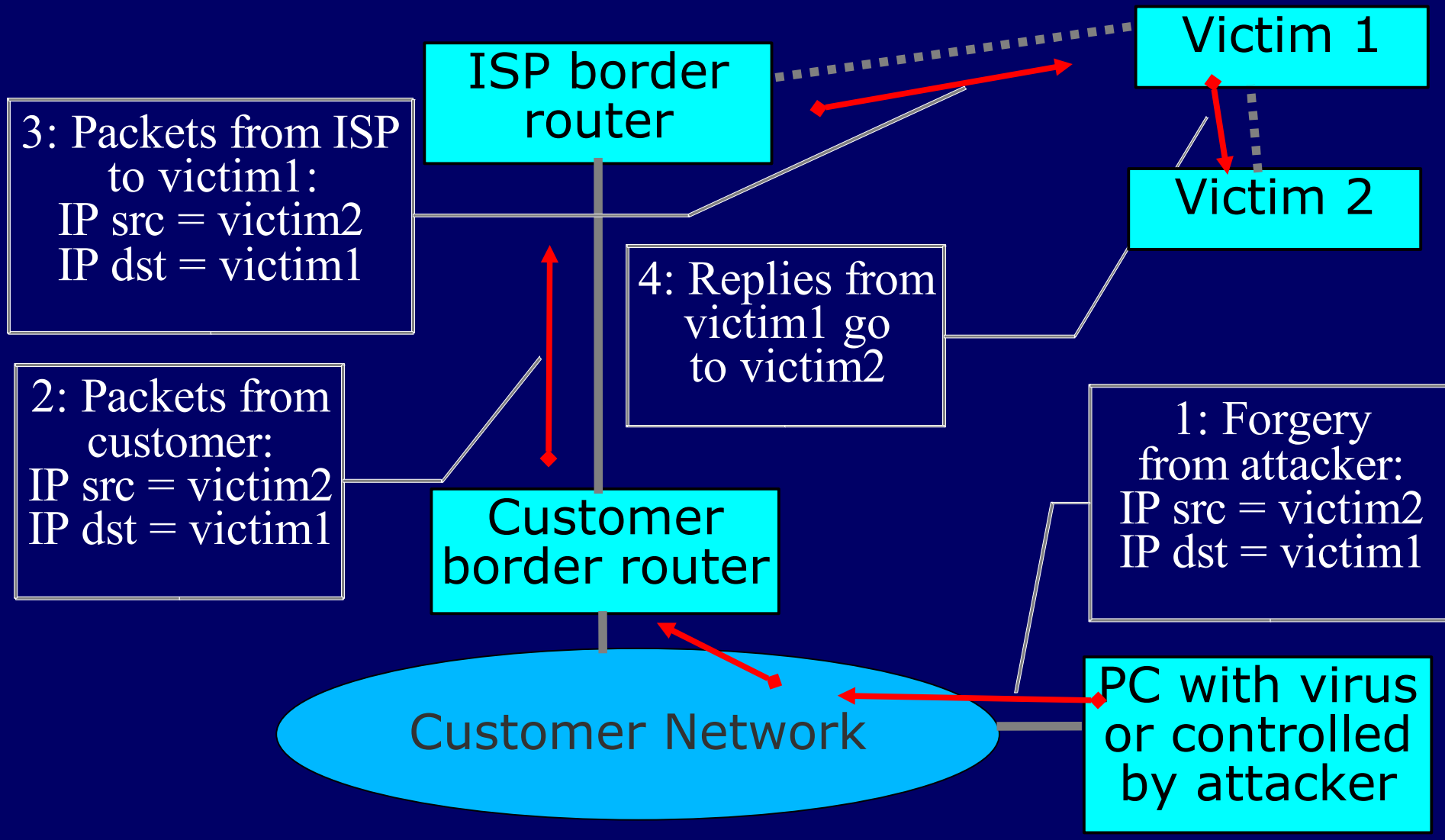
A typical connection from an ISP to a customer



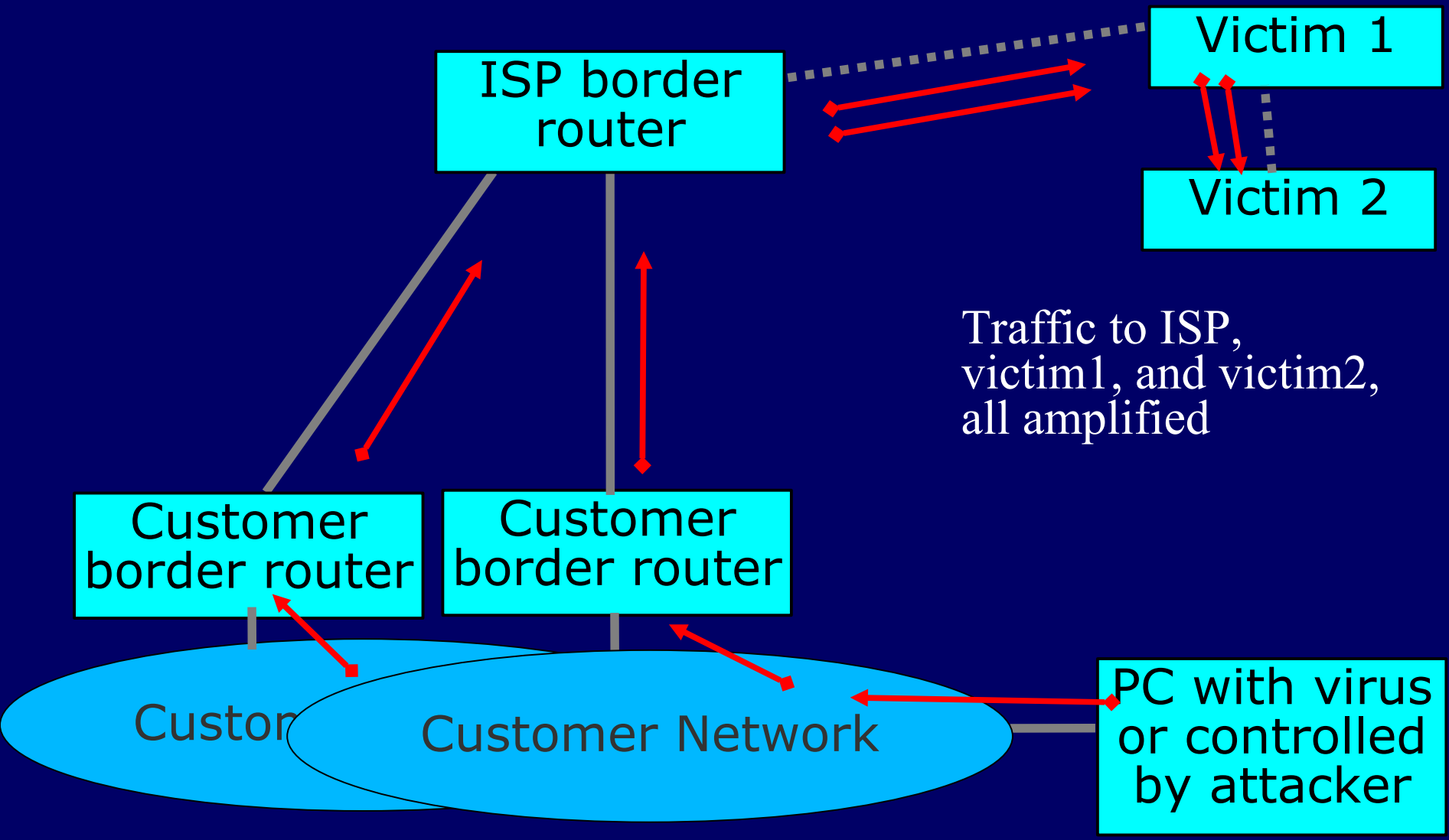
The Problem

- Attackers gain control of thousands or millions of hosts
  - Worm or virus infection
  - Bot nets
- Hosts send forged packets
  - IP source = forgery (random or victim)
  - IP destination = victim
- Forged packets go to victims
  - DNS request, TCP SYN, etc.
- Responses go to random places or other victims
  - DNS response, TCP ACK/RST, ICMP, etc.

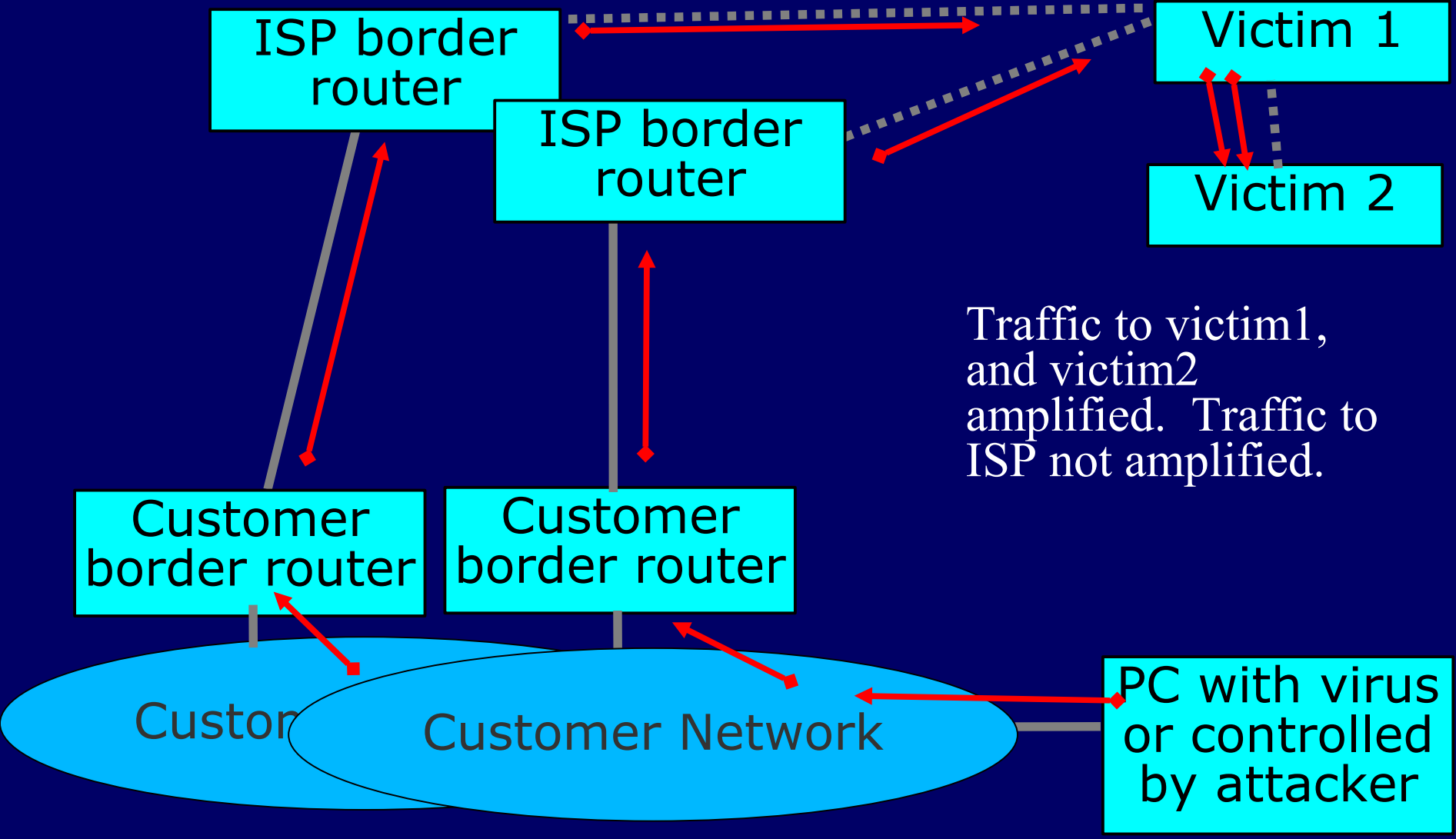
Forged packets cause traffic to victims



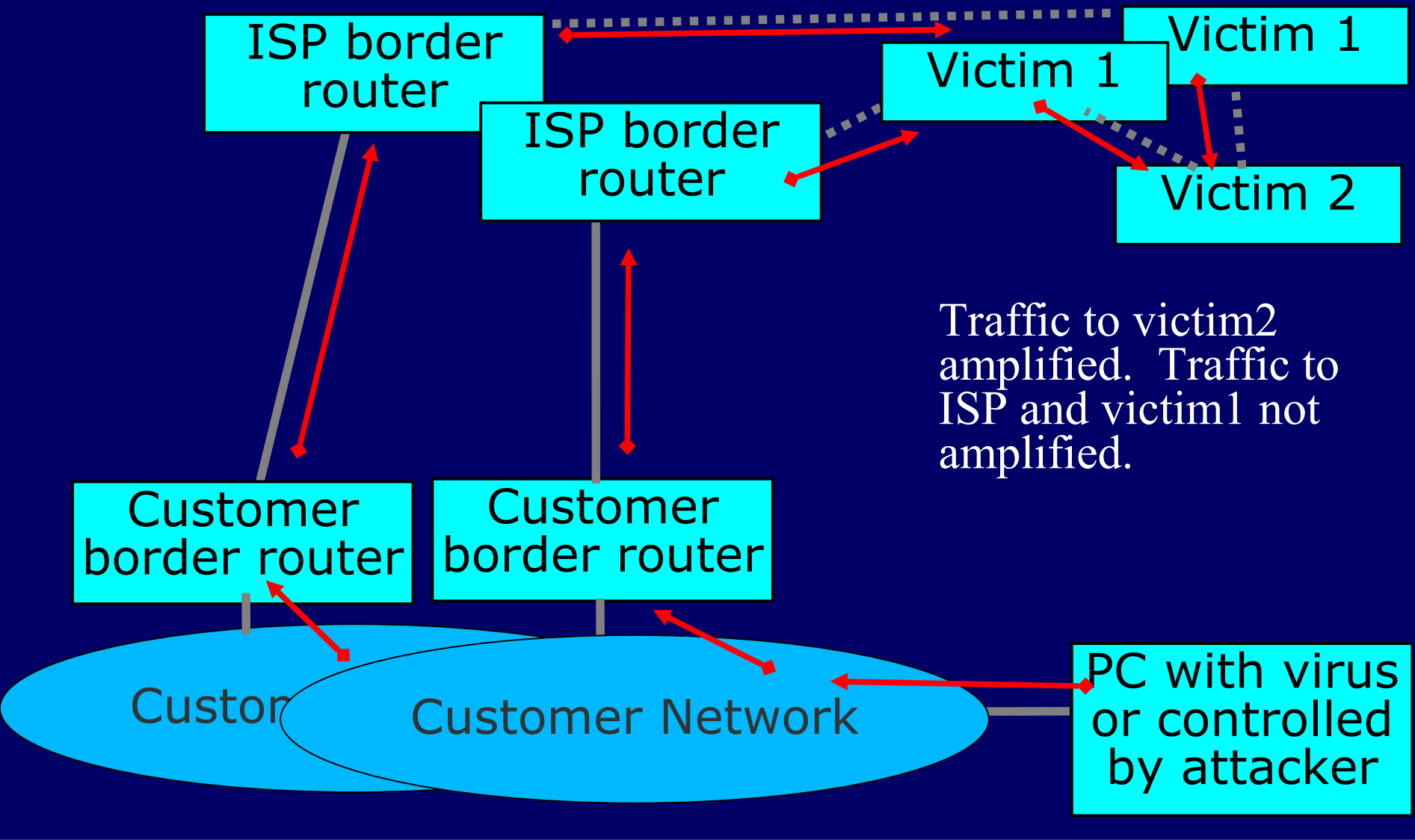
Amplification: multiple forgery sources in the same ISP



Amplification: multiple forgery sources in different ISPs



Amplification: multiple "victim 1", single "victim 2"



“Denial of Service” (DoS) attacks

- The attacker wants to cause some service to stop working for some victim
- Attacker controls many hosts
  - Attacker instructs hosts to send forged packets to victim
- Victim gets lots of packets from many sources
  - Distributed Denial of Service (DDoS)
  - Difficult for victim to filter effectively when packets have forged source addresses

Ingress filtering

- ISPs can block the forged packets as they transit from the customer network to the ISP border router
- ISP knows what IP addresses the customer is allowed to use
- ISP can therefore block packets with source IP addresses outside the range that the customer is allowed to use
- This will prevent the attack

Why use Ingress Filtering

- Save bandwidth from ISP to victims by not forwarding forged packets
- If you don't send forged packets, you won't be contacted by investigators
- If you send forged packets, you may eventually be blacklisted by other ISPs
- When your customers are the victms, you will wish that other ISPs had blocked the attack

Simple case: Single-homed customer

- If the customer is single-homed, then the only addresses they are allowed to use are the addresses that the ISP routes to them
- ISP can easily configure the border router to block all other addresses
- Cisco feature - uRPF:

```
interface Serial1/2
  ip verify unicast reverse-path (strict mode)
    OR
  ip verify unicast source reachable-via any
  (loose mode)
```

Complex case: Multi-homed customer

- If the customer is multi-homed, then they may also use addresses from other ISPs
  - e.g. Satellite downlink from ISP A, uplink to ISP B
- ISPs can still block the forged packets
  - Need to have a list of valid addresses
- Use generic filtering features, such as cisco access lists
  - Not just one trivial command, but still worth doing

Remote Triggered Black Hole

- Allows you to quickly drop DoS/DDoS traffic at any point in the network

```
! Set the black hole path
ip route 192.0.2.1 255.255.255.255 null0

! Create a logical Null interface
interface null0
 no ip unreachables

! Create the BGP routing policy that will black hole
route-map BLACKHOLE permit 10
 match ip address prefix-list blackhole
 set community 100:666 no-export
 set ip next-hop 192.0.2.1
```

Remote Triggered Black Hole

```
! Let other routes, that don't match, through
route-map BLACKHOLE permit 20

! Add the "bad" routes to your IGP for pull-up
ip route 10.0.0.0 255.255.255.0 null0
ip route 172.16.0.0 255.255.255.0 null0

! Export this policy via BGP
router bgp 100
 neighbor 1.1.1.1 route-map BLACKHOLE out
 network 10.0.0.0 mask 255.255.255.0
 network 172.16.0.0 mask 255.255.255.0
```

```
! Define the interesting routes to black hole
! Add more routes to black hole as necessary
ip prefix-list blackhole seq 10 permit 10.0.0.0/24
ip prefix-list blackhole seq 20 permit 172.16.0.0/24
```

Further Reading

- BCP 38 (RFC 2827)
  http://www.ietf.org/rfc/rfc2827.txt
- Team Cymru
  http://www.cymru.com/
- A few presentations
  http://bgphints.ruud.org/articles/urpf.html
  http://www.nanog.org/mtg-0602/pdf/greene.ppt
  http://www.cisco.com/warp/public/732/Tech/security/docs/urpf.pdf