(Distributed) Denial of Service

CS-576 Systems Security

Instructor: Georgios Portokalidis

Spring 2018

Denial-of-Service (DoS) Attack

“An action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space.”

Denial-of-Service (DoS)

A form of attack on the availability of some service

Categories of resources that could be attacked are:

Network bandwidth

Relates to the capacity of the network links connecting a server to the Internet

For most organizations this is their connection to their Internet Service Provider (ISP)

System resources

Aims to overload or crash the network handling software

Application resources

Typically involves a number of valid requests, each of which consumes significant resources, thus limiting the ability of the server to respond to requests from other users

Network Flooding Attacks

Attacker generates large volumes of packets that have the target system as the destination address

Intent is to overload the network capacity on some link to a server

Congestion would result in the router connected to the final, lower capacity link

Virtually any type of network packet can be used

Network Flooding Attacks

Classified based on network protocol used

Virtually any type of network packet can be used

ICMP flood

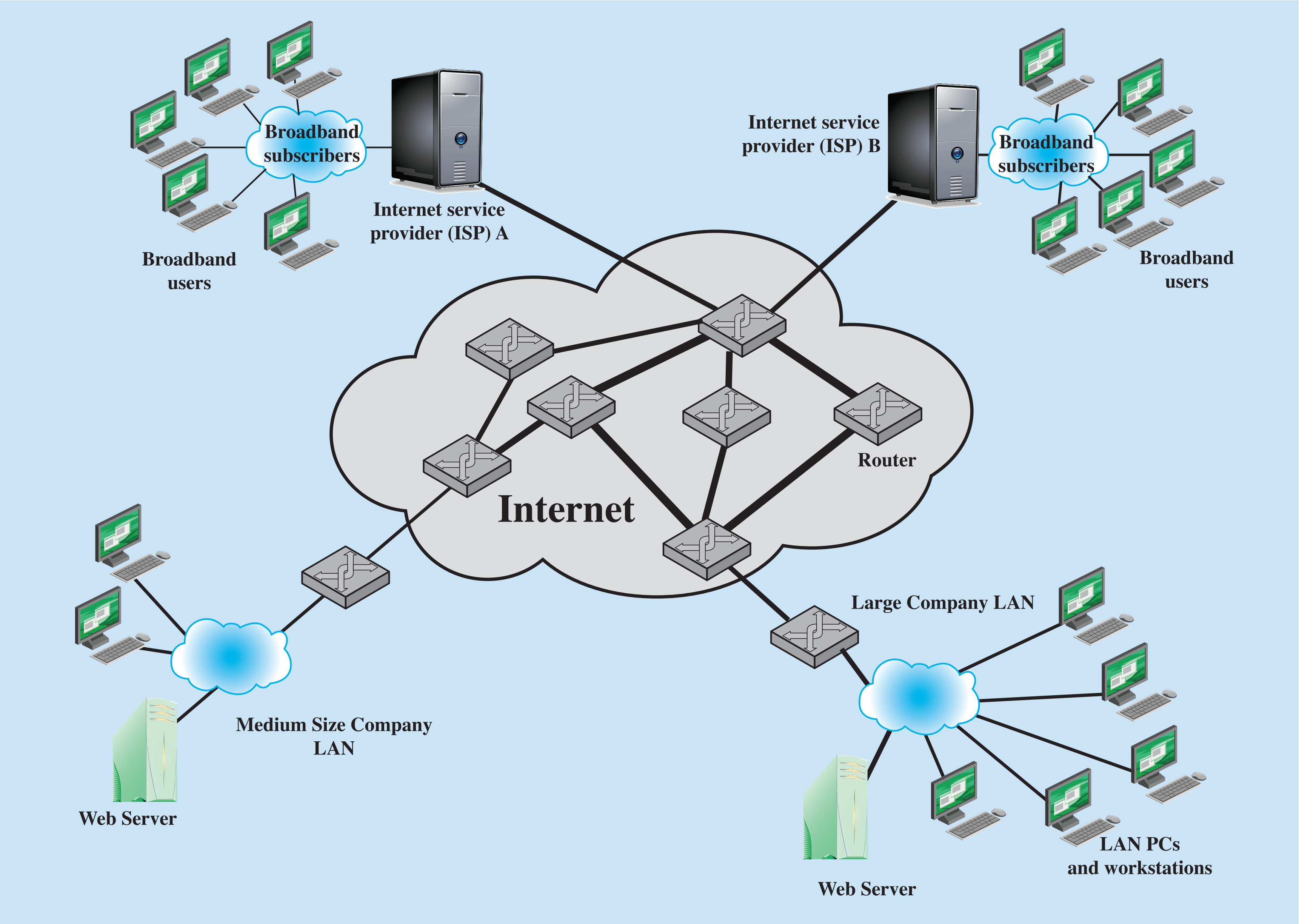
- Ping flood using ICMP echo request packets
- Traditionally network administrators allow such packets into their networks because ping is a useful network diagnostic tool

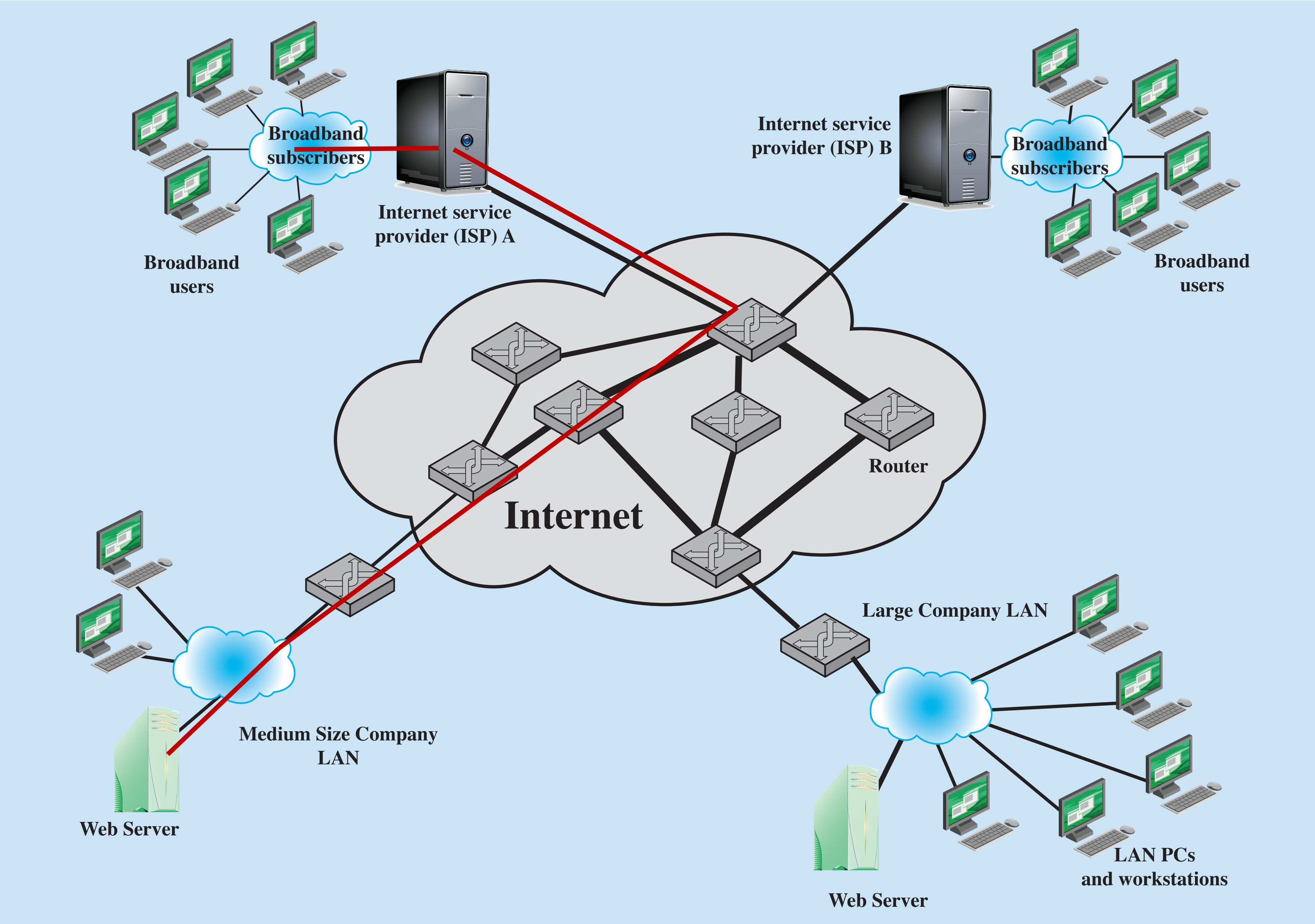
UDP flood

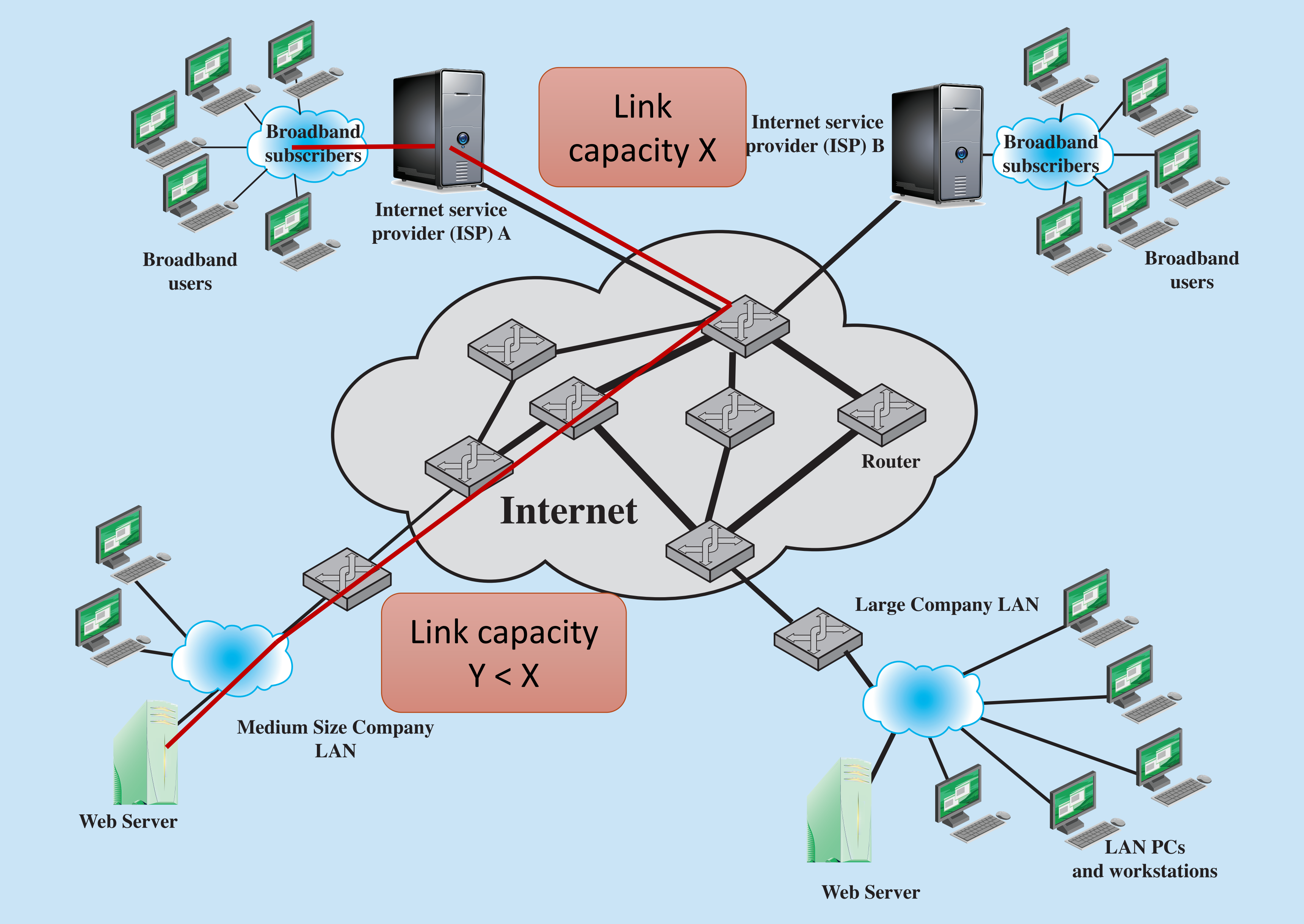
- Uses UDP packets directed to some port number on the target system

TCP SYN flood

- Sends TCP packets to the target system
- Total volume of packets is the aim of the attack rather than the system code

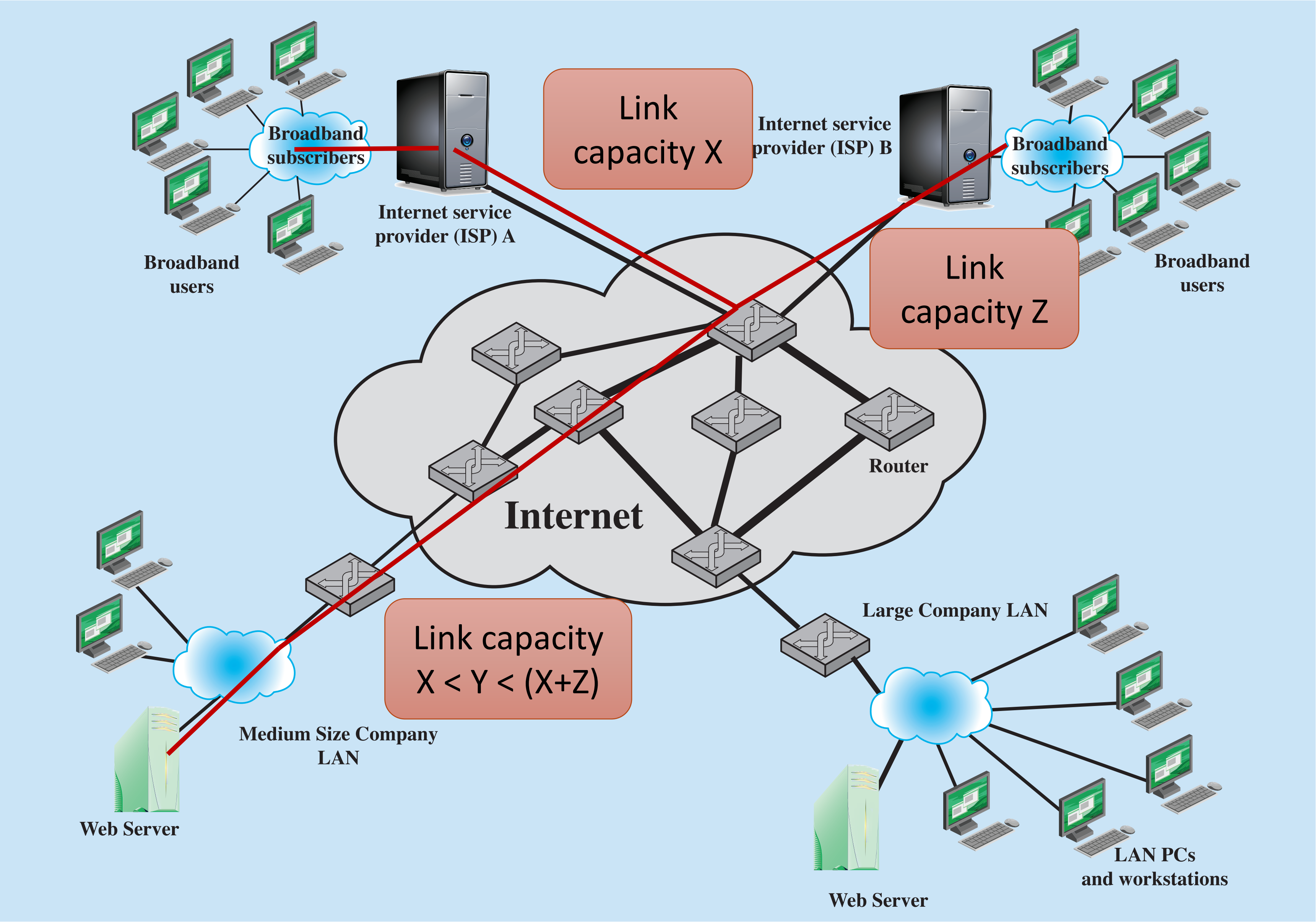

Broadband subscribers
Internet service provider (ISP) A
Broadband users
Internet service provider (ISP) B
Broadband subscribers
Broadband users
Router
Internet
Medium Size Company LAN
Web Server
Large Company LAN
LAN PCs and workstations
Web Server


Broadband subscribers
Internet service provider (ISP) A
Broadband users
Internet service provider (ISP) B
Broadband subscribers
Broadband users
Router
Internet
Large Company LAN
Medium Size Company LAN
Web Server
LAN PCs and workstations
Web Server

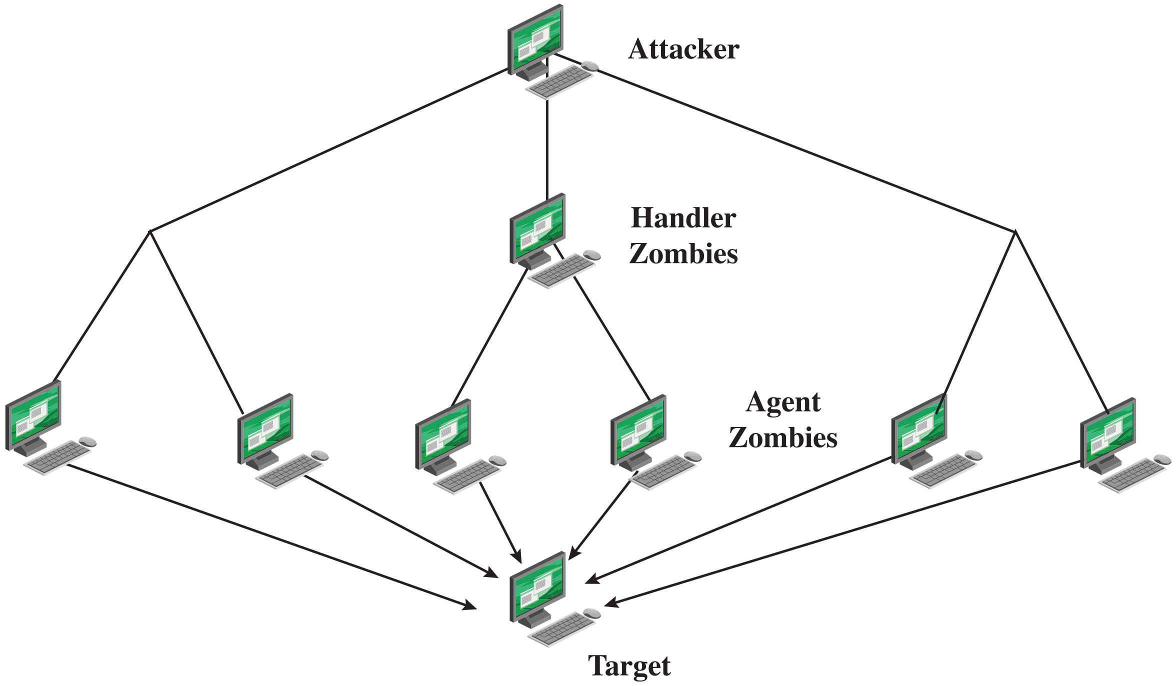


Link capacity X

Link capacity Y < X

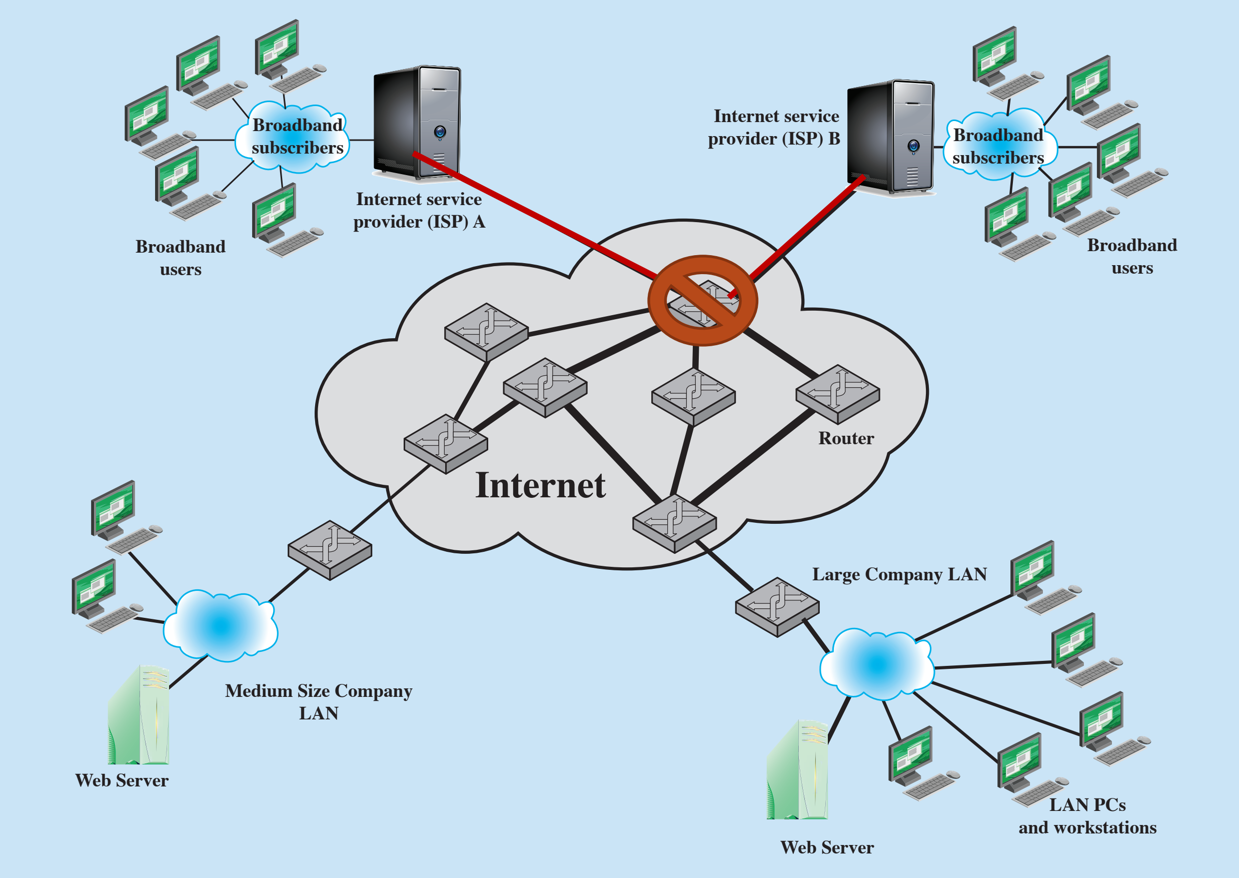

Broadband subscribers
Internet service provider (ISP) A
Link capacity X
Internet service provider (ISP) B
Broadband subscribers
Broadband users
Link capacity Z
Broadband users
Internet
Router
Large Company LAN
Link capacity X < Y < (X+Z)
Medium Size Company LAN
Web Server
Web Server
LAN PCs and workstations

Distributed Denial-of-Service



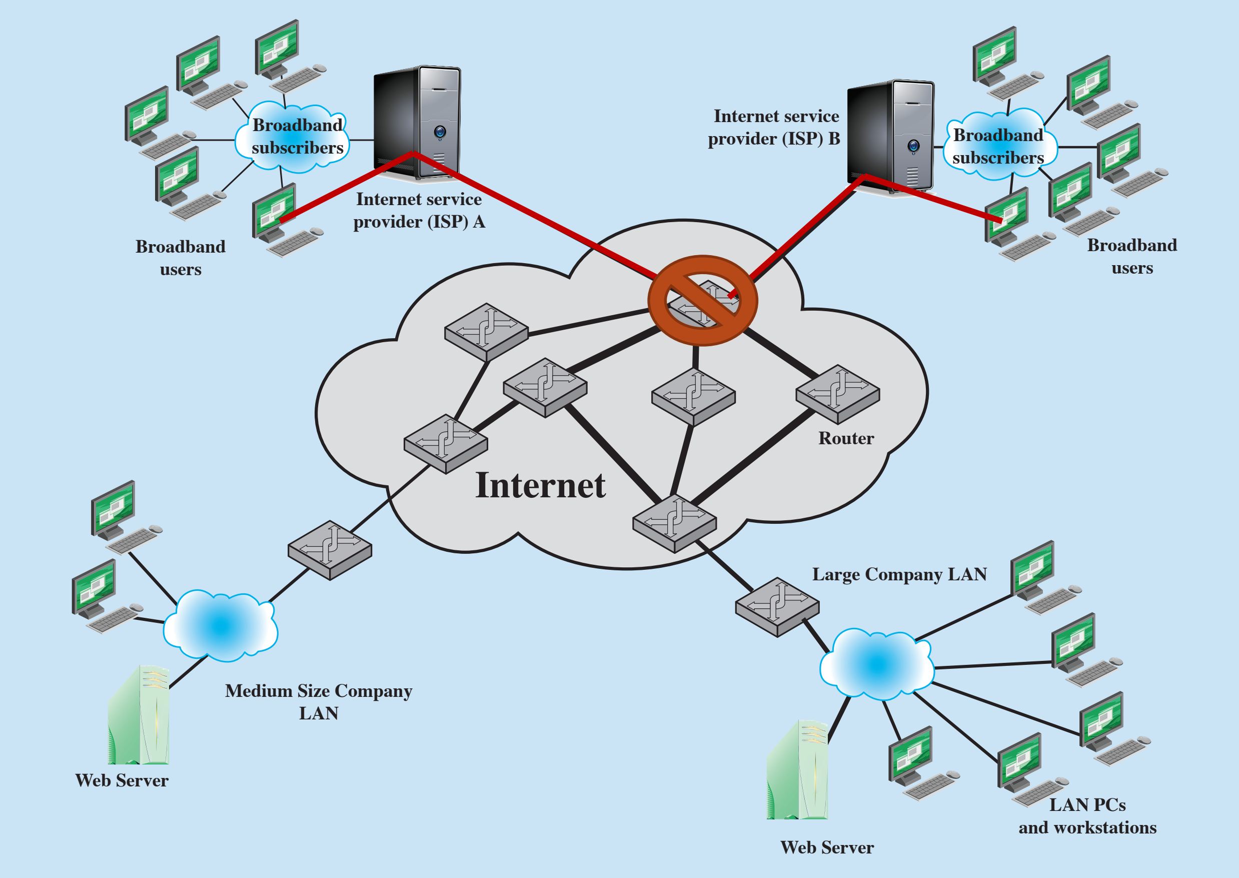
Simple Solution

Block subnets that flood server



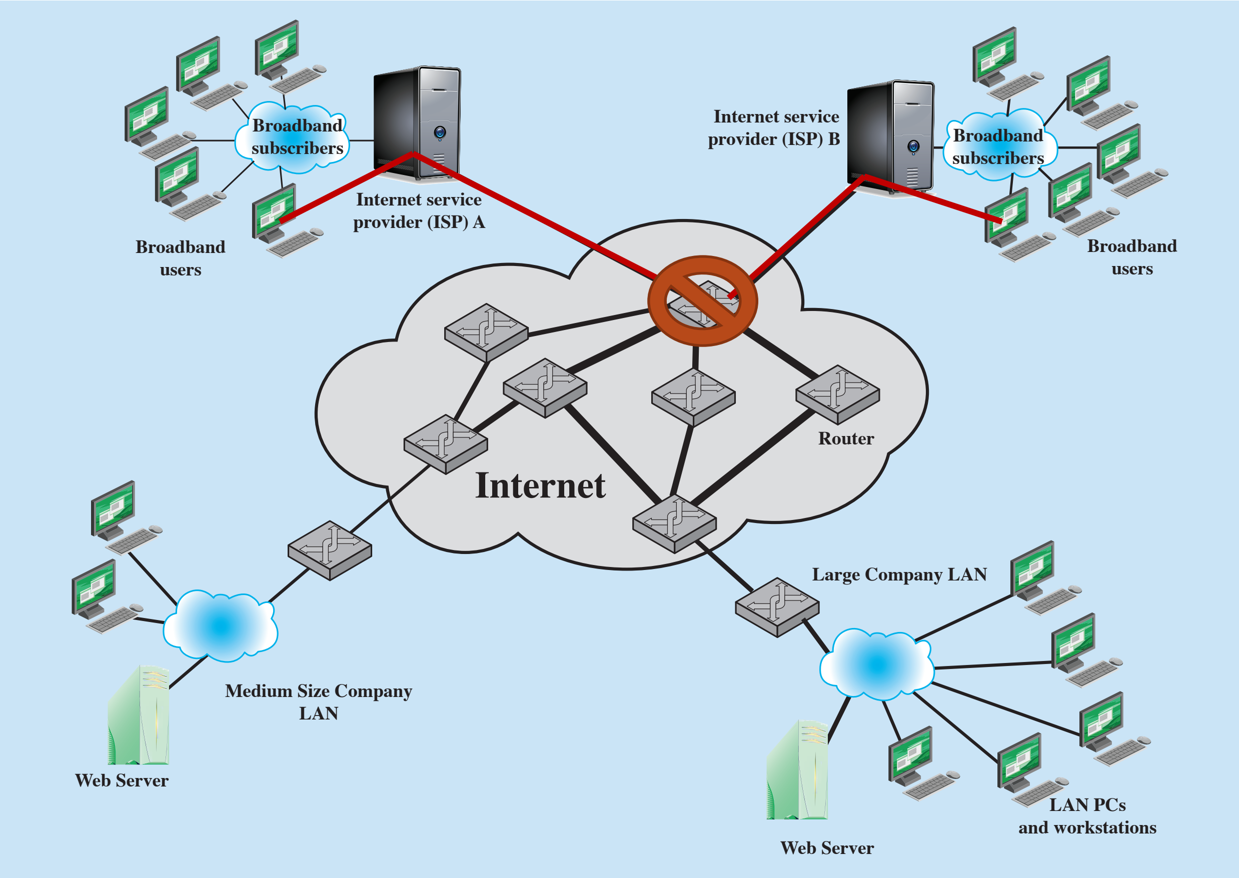
Slightly Less Simple Solution

Block **IPs** that flood server



Where to Block?

The closer to the source of the traffic the better



Source Address Spoofing

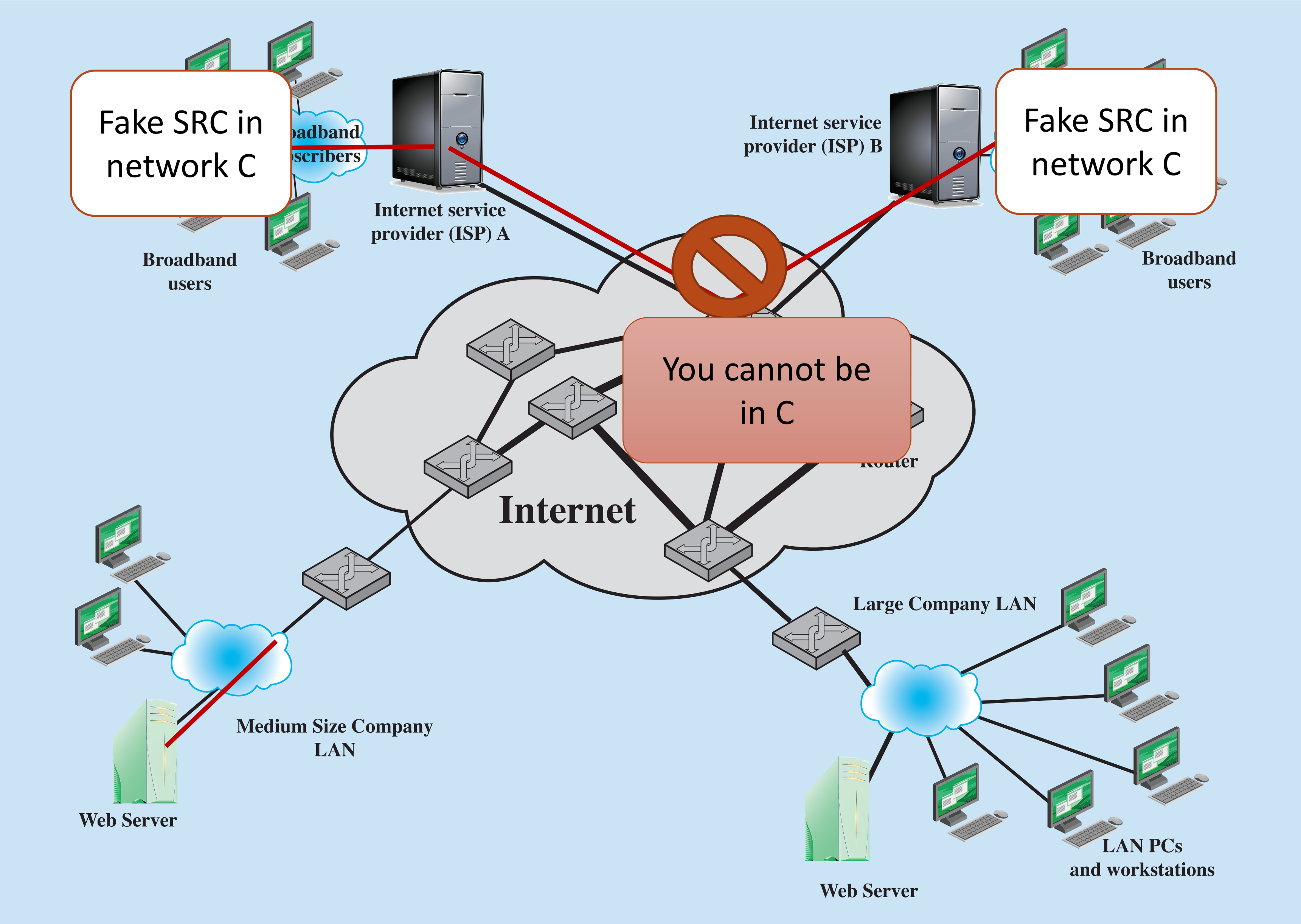
Use forged source addresses

- E.g., via the raw socket interface

Identifying culprits and blocking IPs is harder

Local routers can potentially filter such packets

- Not really done today



Fake SRC in network C

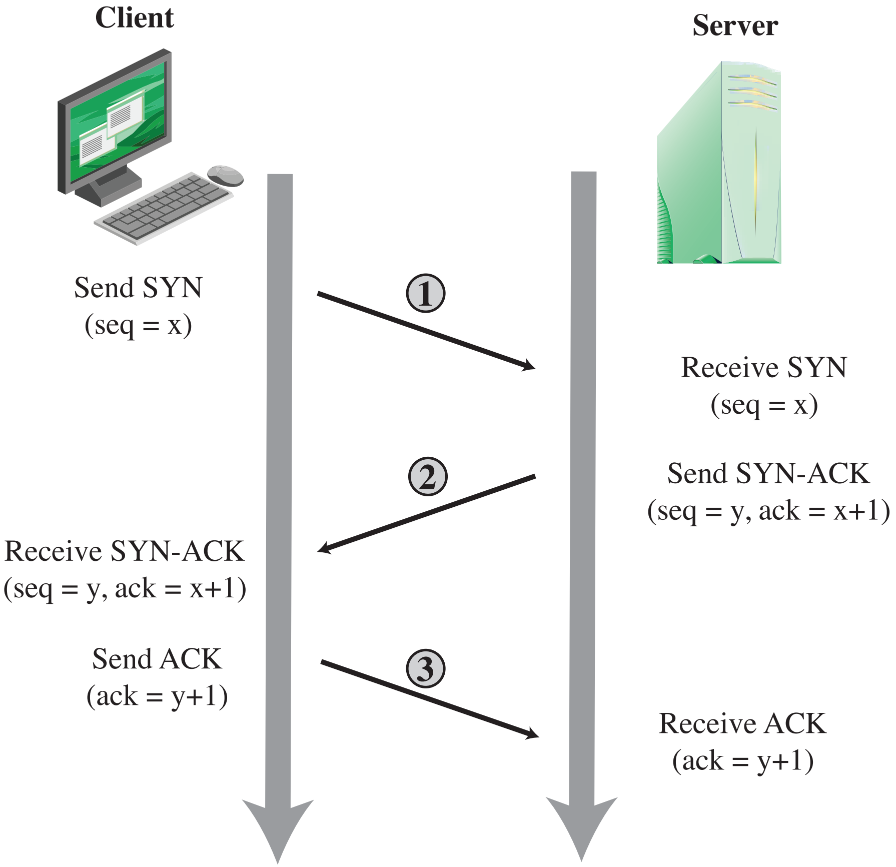
Fake SRC in network C

You cannot be in C

Figure 7.1 Example Network to Illustrate DoS Attacks

SYN Packet Tricks

SYN is one of the first packets sent to establish a TCP connection

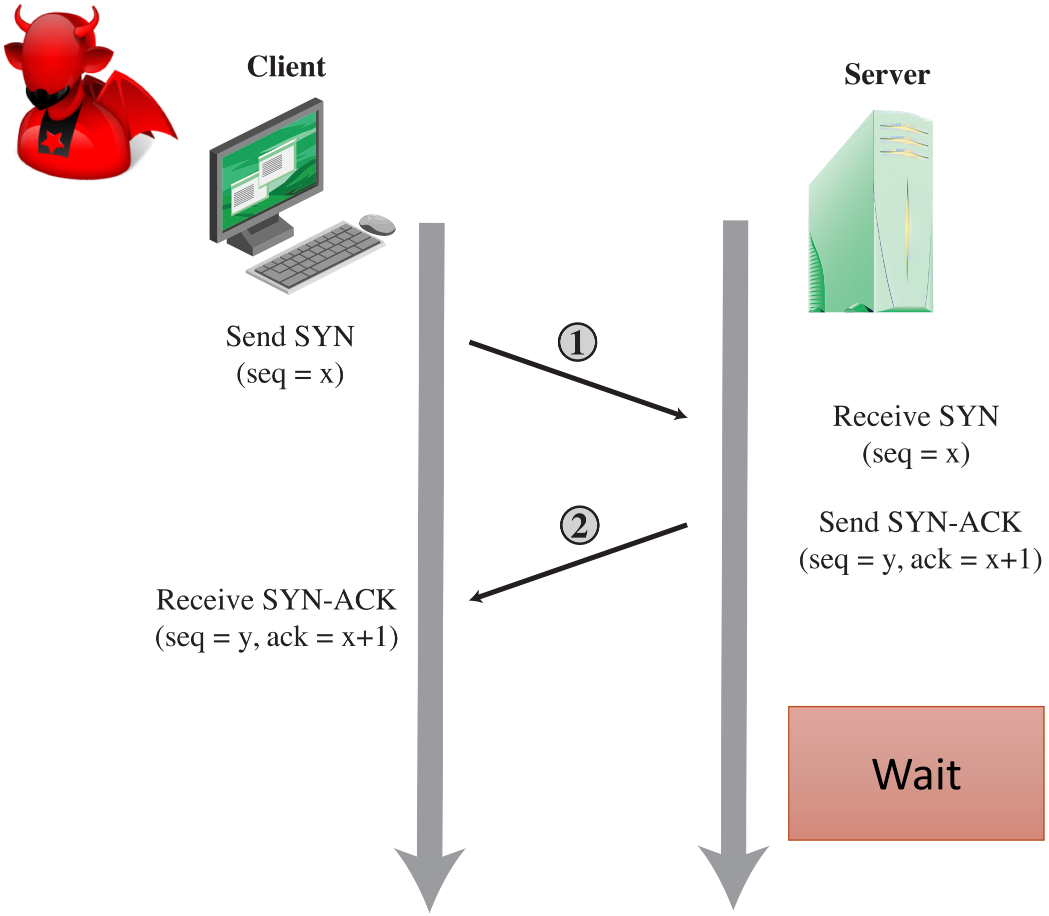


SYN Floods Targeting the System

Attacks the ability of a server to respond to future connection requests by overflowing the tables used to manage them

Thus legitimate users are denied access to the server

Hence an attack on system resources, specifically the network handling code in the operating system



Client

Server

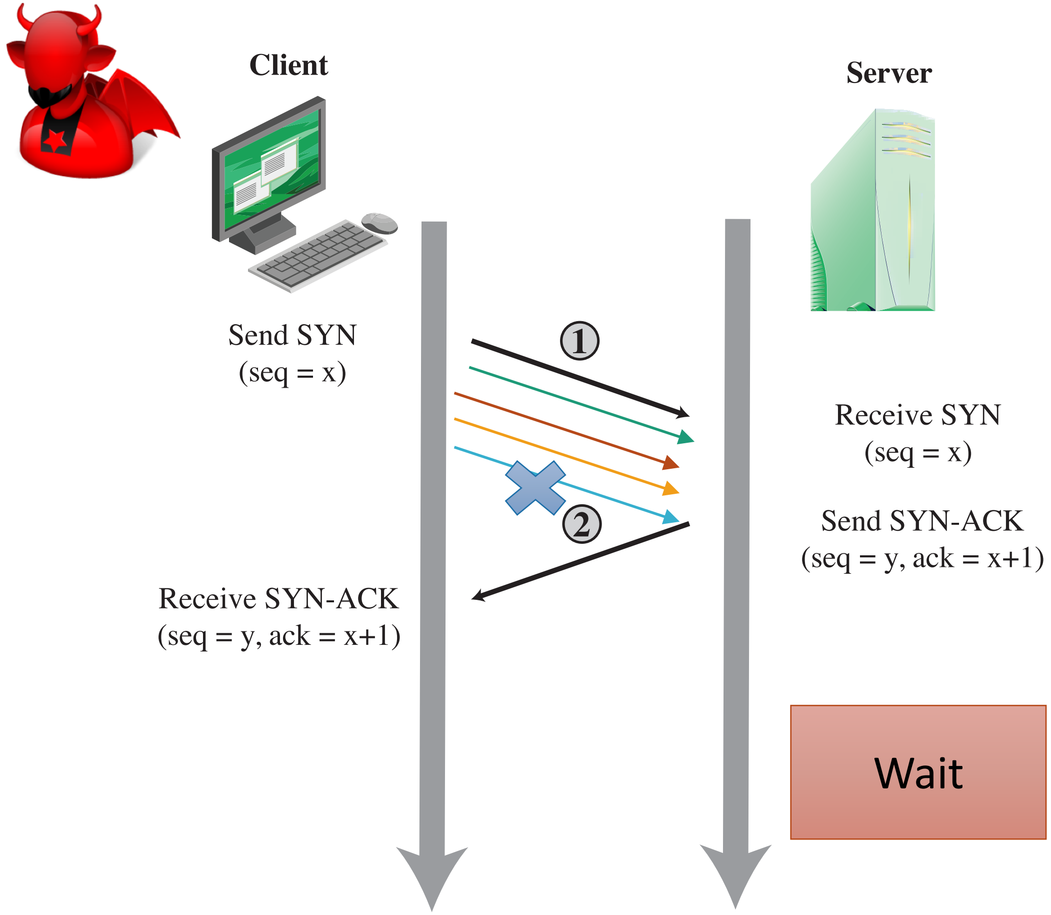
Send SYN
(seq = x)

Receive SYN
(seq = x)

Send SYN-ACK
(seq = y, ack = x+1)

Receive SYN-ACK
(seq = y, ack = x+1)

Wait


Client
Server
Send SYN
(seq = x)
1
Receive SYN
(seq = x)
Send SYN-ACK
(seq = y, ack = x+1)
2
Receive SYN-ACK
(seq = y, ack = x+1)
Wait

SYN Spoofing

Spoof the source address of the SYN packet

The destination will try to establish a connection with the spoofed address

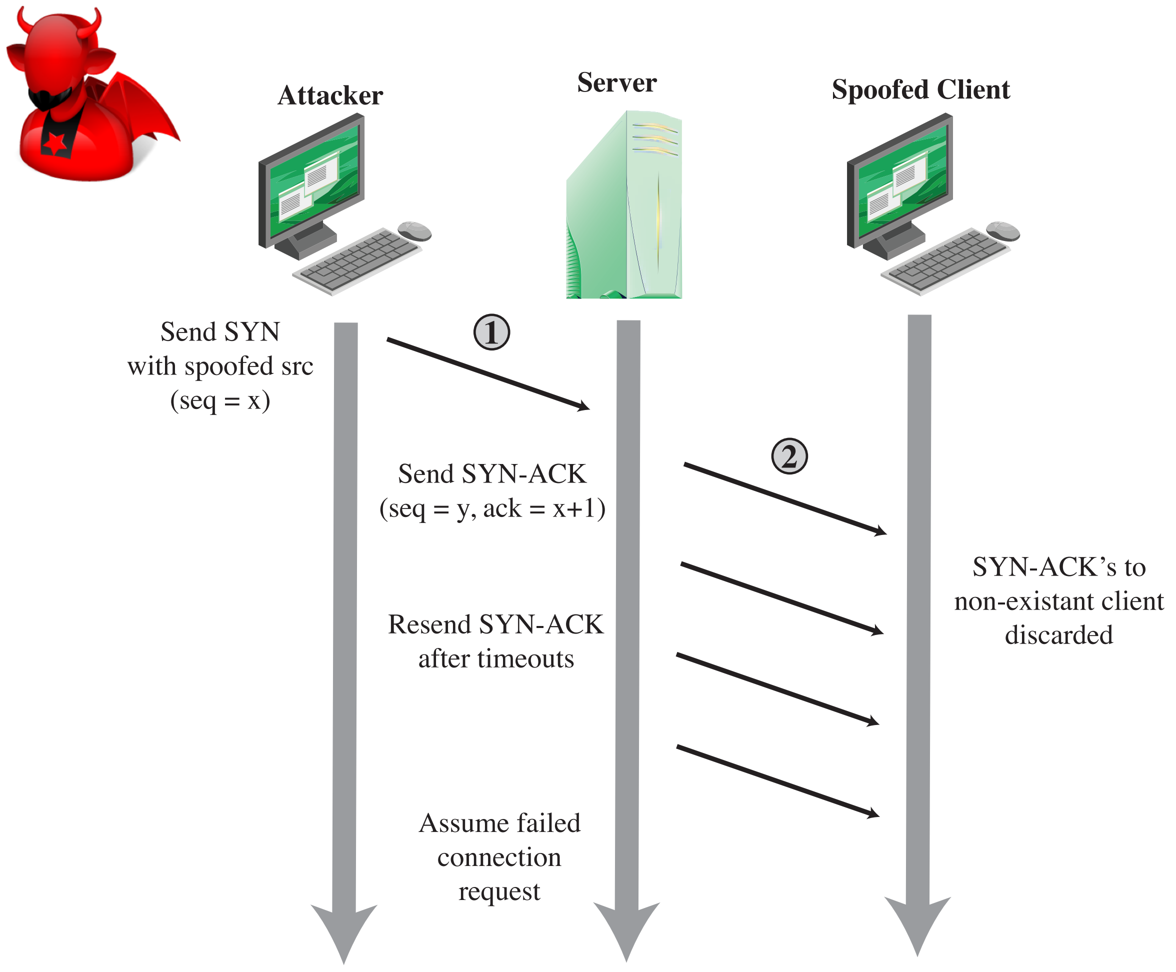

Attacker
Server
Spoofed Client
Send SYN with spoofed src (seq = x)
1
Send SYN-ACK (seq = y, ack = x+1)
2
SYN-ACK's to non-existant client discarded
Resend SYN-ACK after timeouts
Assume failed connection request

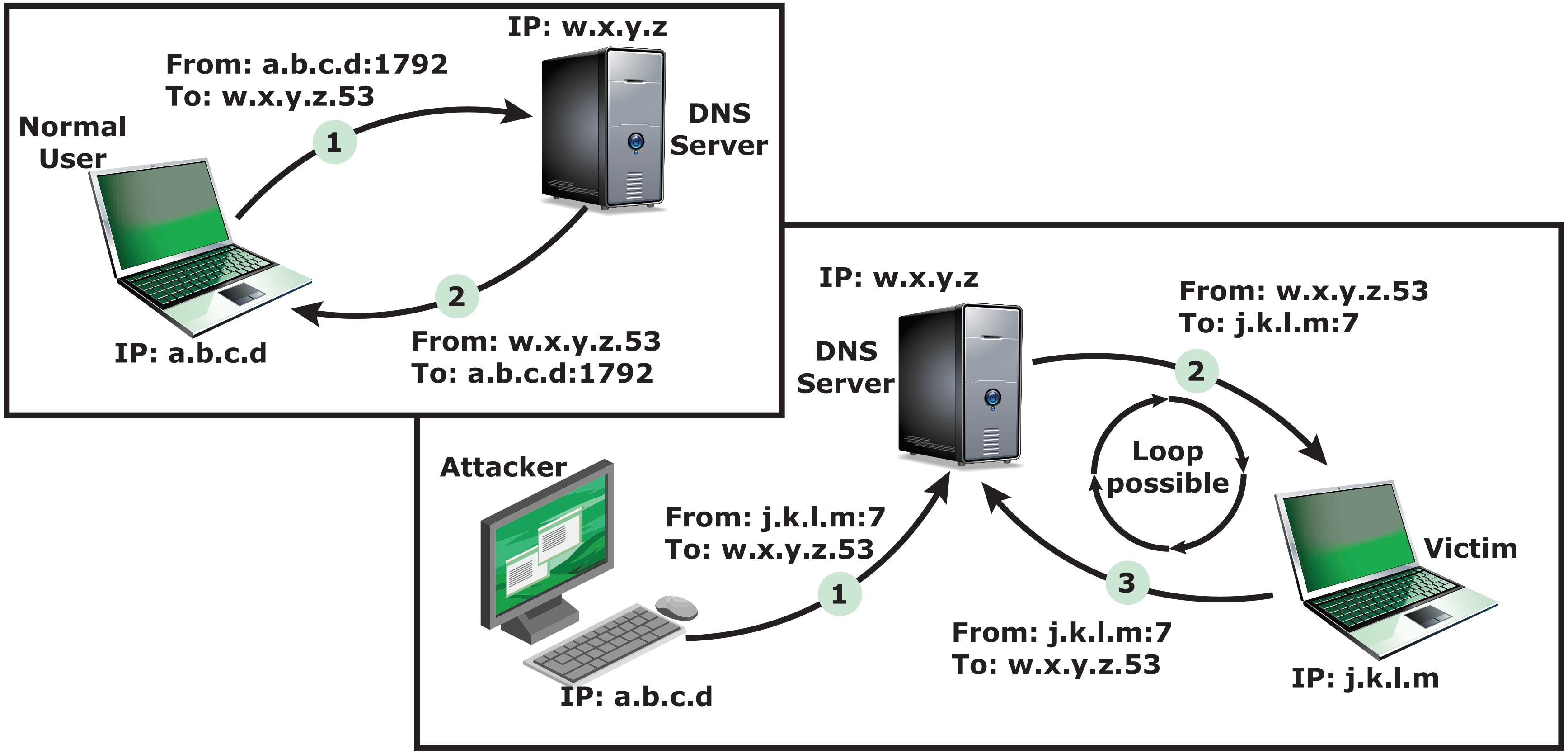
Figure7.3 TCP SYN Spoofing Attack

Reflection Attacks

Attacker sends packets to a known service on the intermediary with a spoofed source address of the actual target system

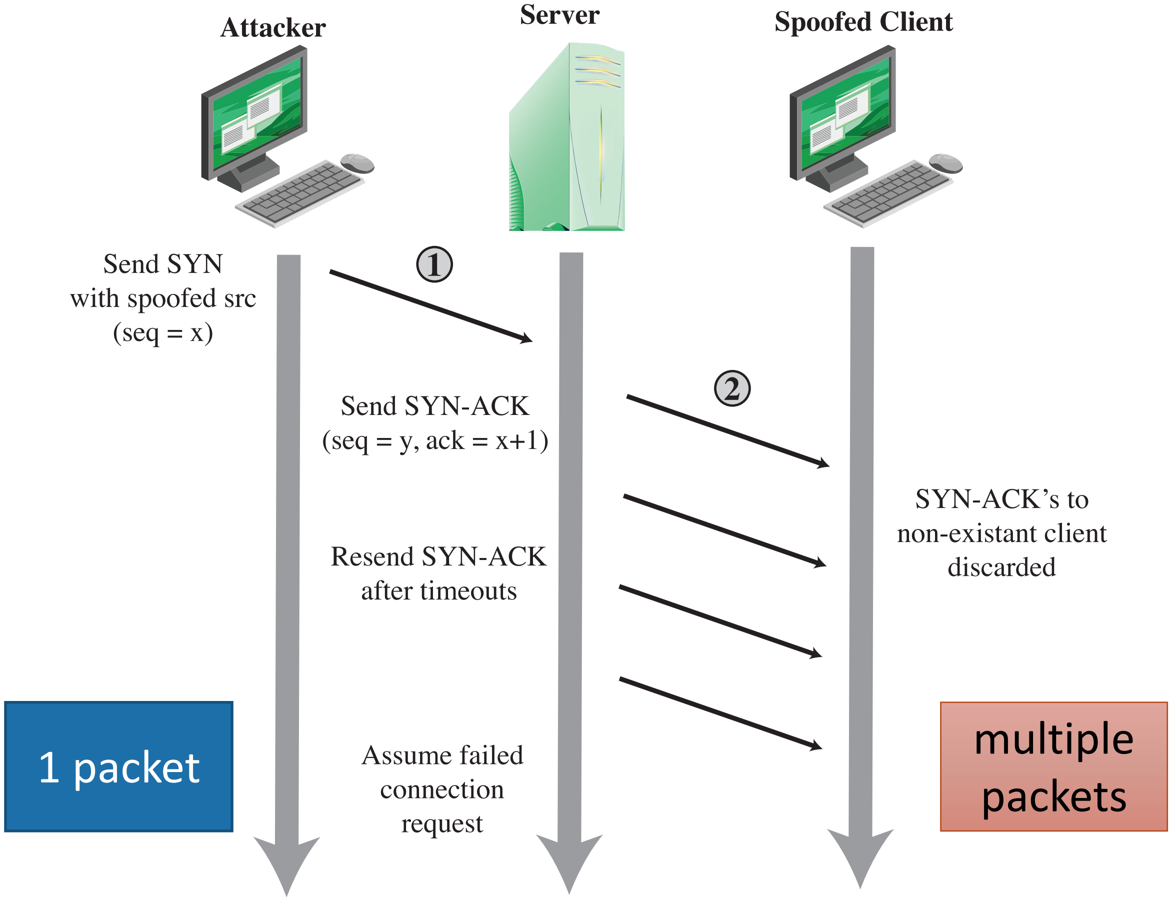
When intermediary responds, the response is sent to the target → It **“Reflects”** the attack off the intermediary (reflector)

Reflection Through DNS



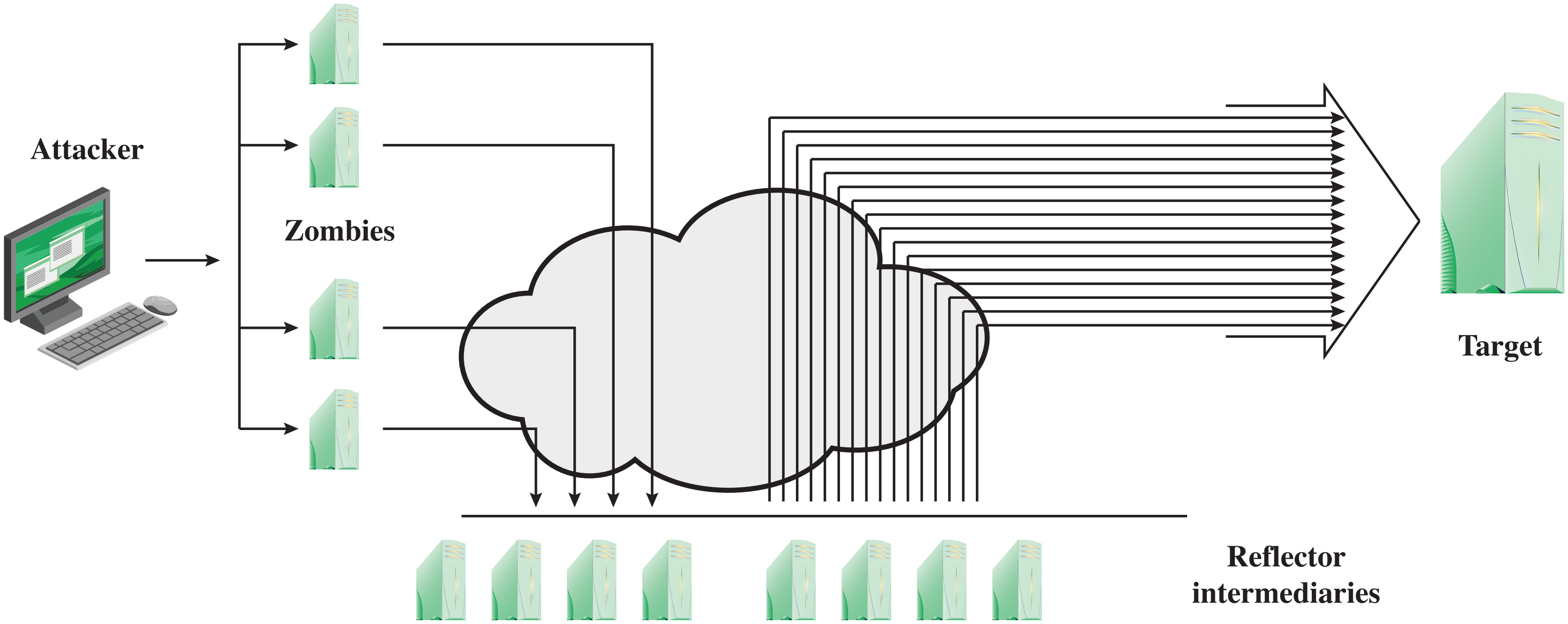
Amplification Attacks

Single spoofed packet results in multiple packets to target



Amplification Attacks

Higher-layer protocols, like DNS, can also be used



DNS Amplification Attacks

Spoofed DNS query packets are sent to legitimate DNS server

DNS generates one larger packet which it sends to the spoofed address

Amplification occurs because response is larger in size than the original query

HTTP-Based Attacks

HTTP flood

Attack that bombards Web servers with HTTP requests

Consumes considerable resources

Slowloris

Create many HTTP requests to server that never complete

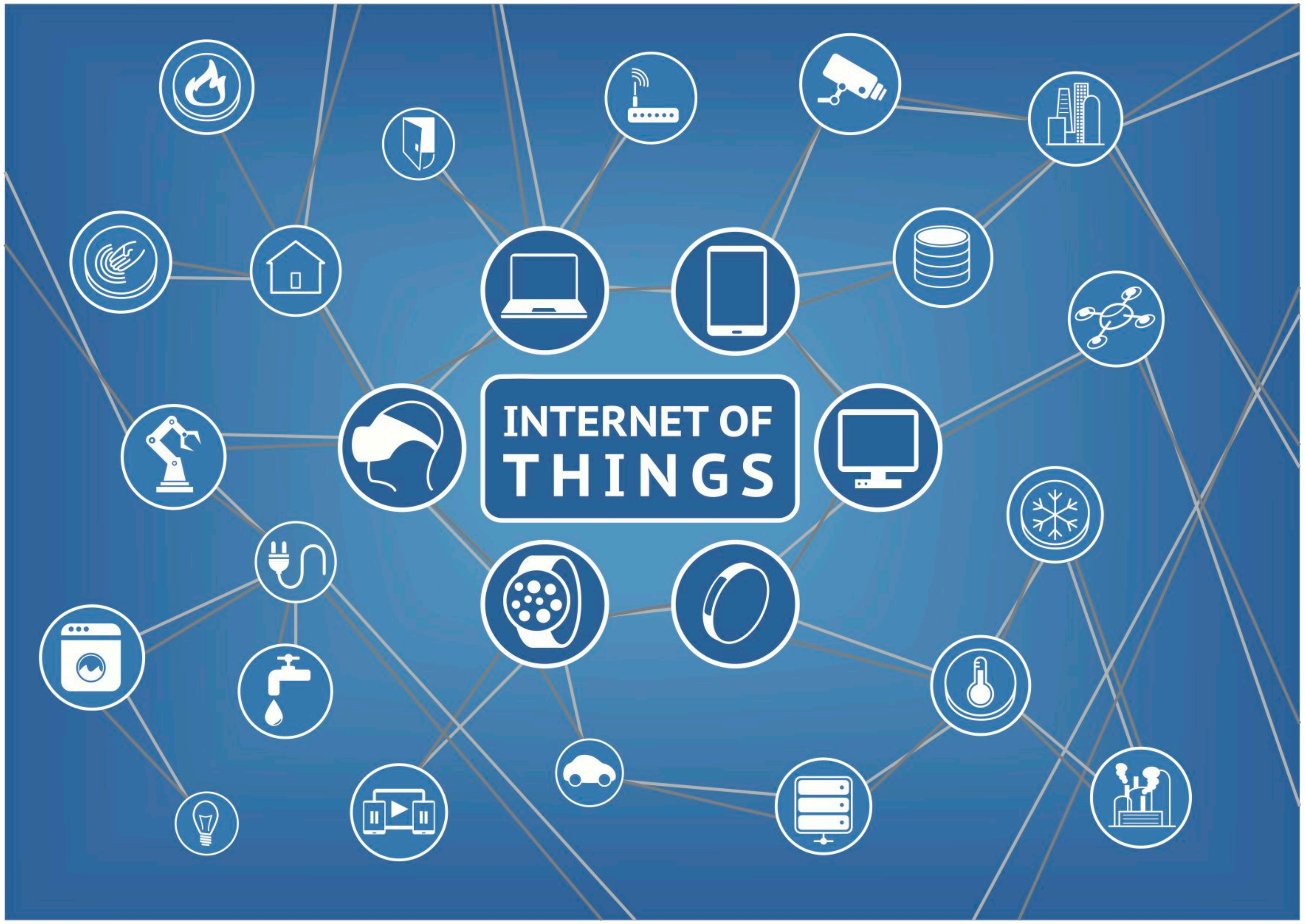
- Send partial requests as slowly as possible

Consumes Web server’s connection capacity

Hard to differentiate from client with limited connectivity

Internet of Things

Internet connected devices/objects



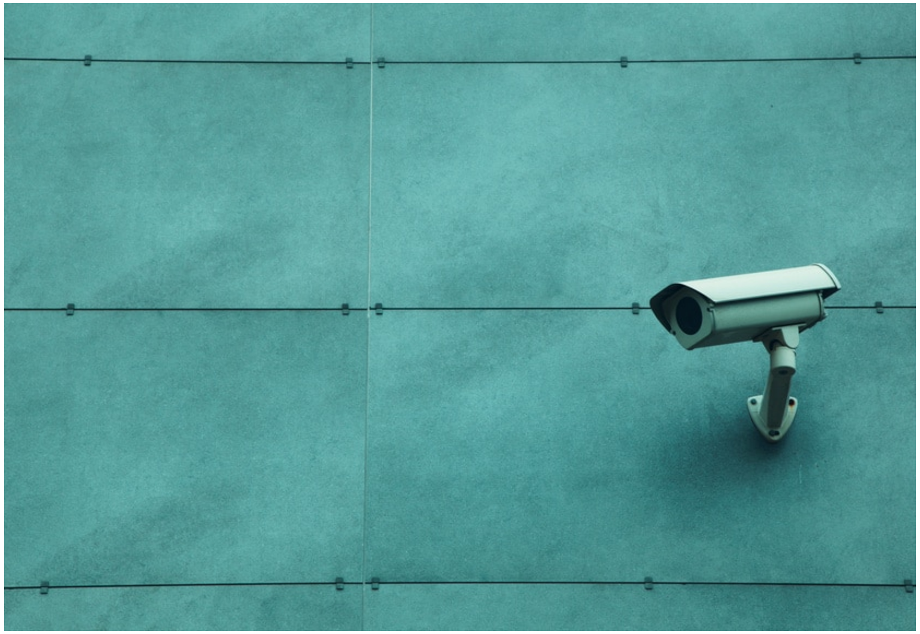
Mirai Botnet

Exploited vulnerable CCTV cameras

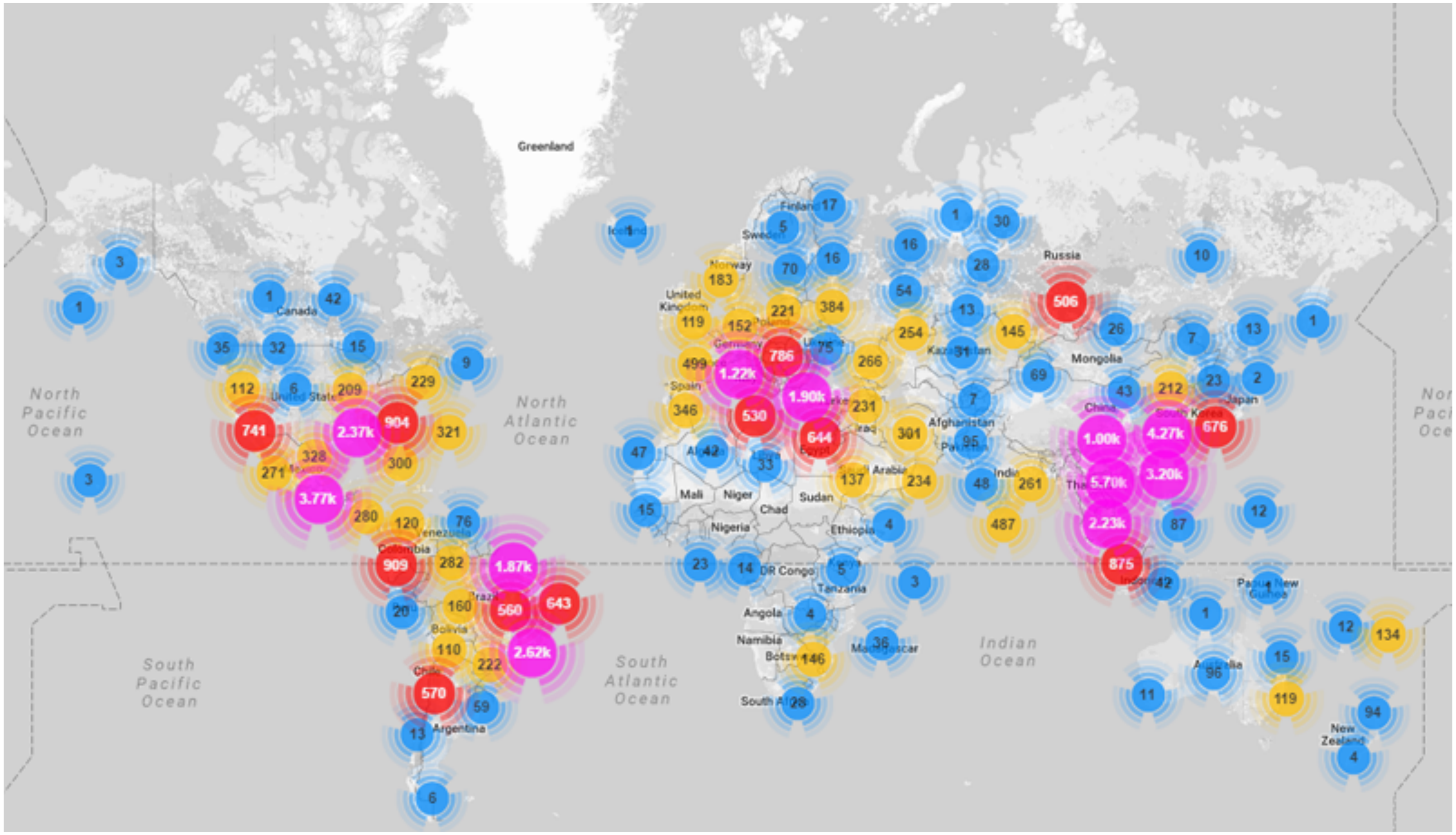
Multiple vulnerabilities found on CCTV cameras:

- Weak authentication, stack overflow, etc.

Estimated to control more than 100k devices



IoT Botnet-Driven DDoS



Reading: https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html