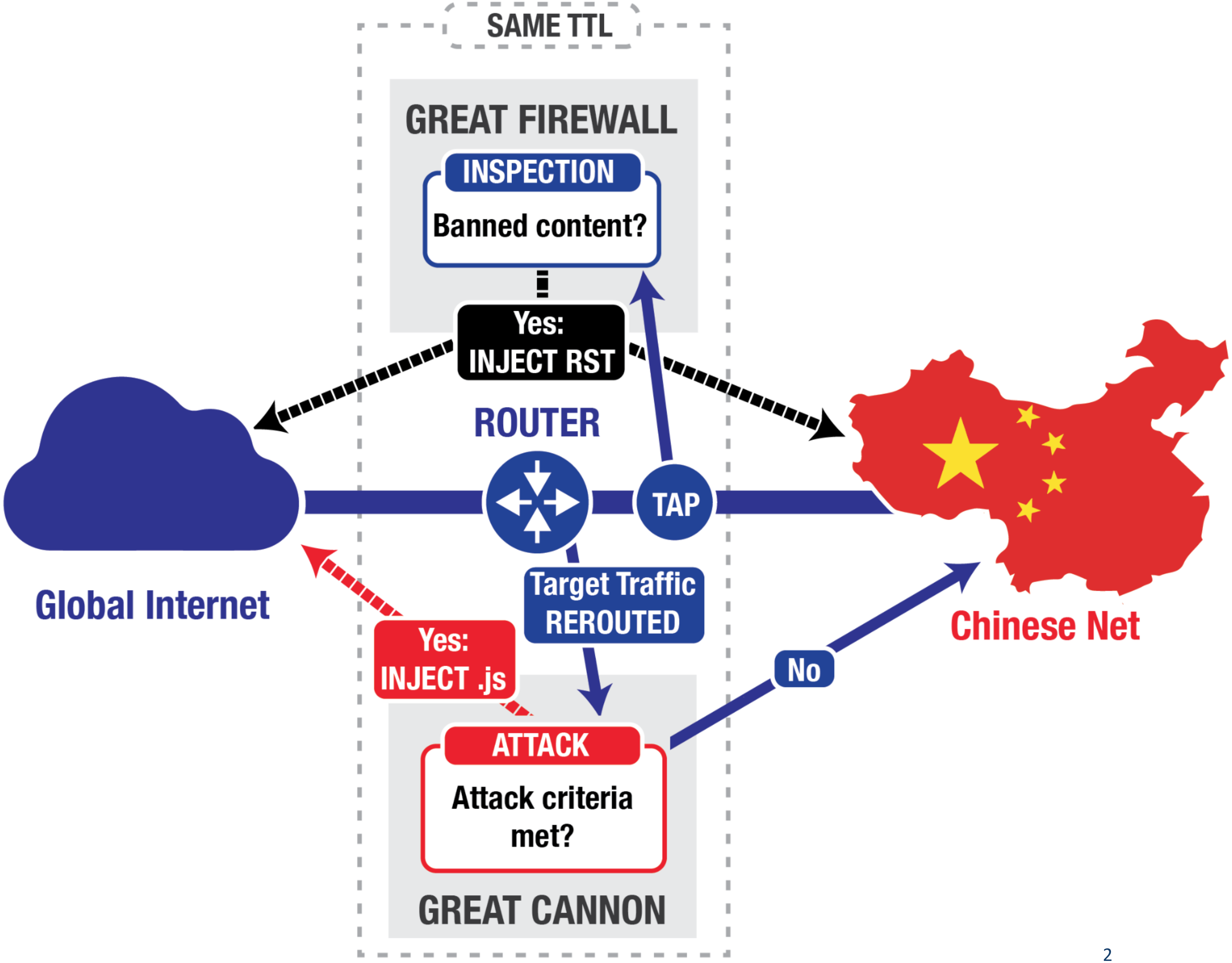
Network Defenses

KAMI VANIEA

26 SEPTEMBER 2017

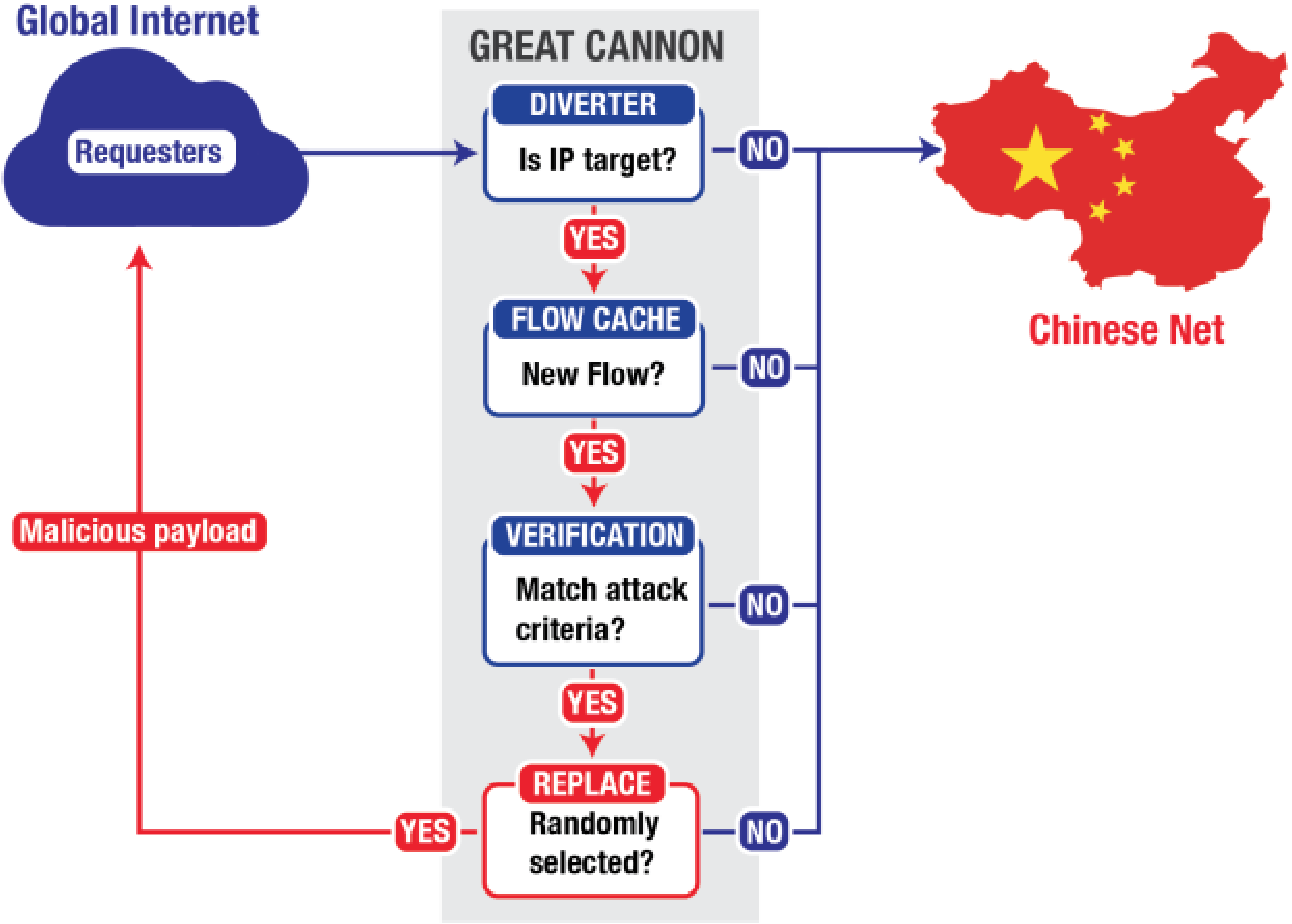
First the news…

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



First the news…

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



Tutorials

- Tutorials start in week 3
- We originally had tutorials and labs, now we just have tutorials
- “Tutorials” are very lab like

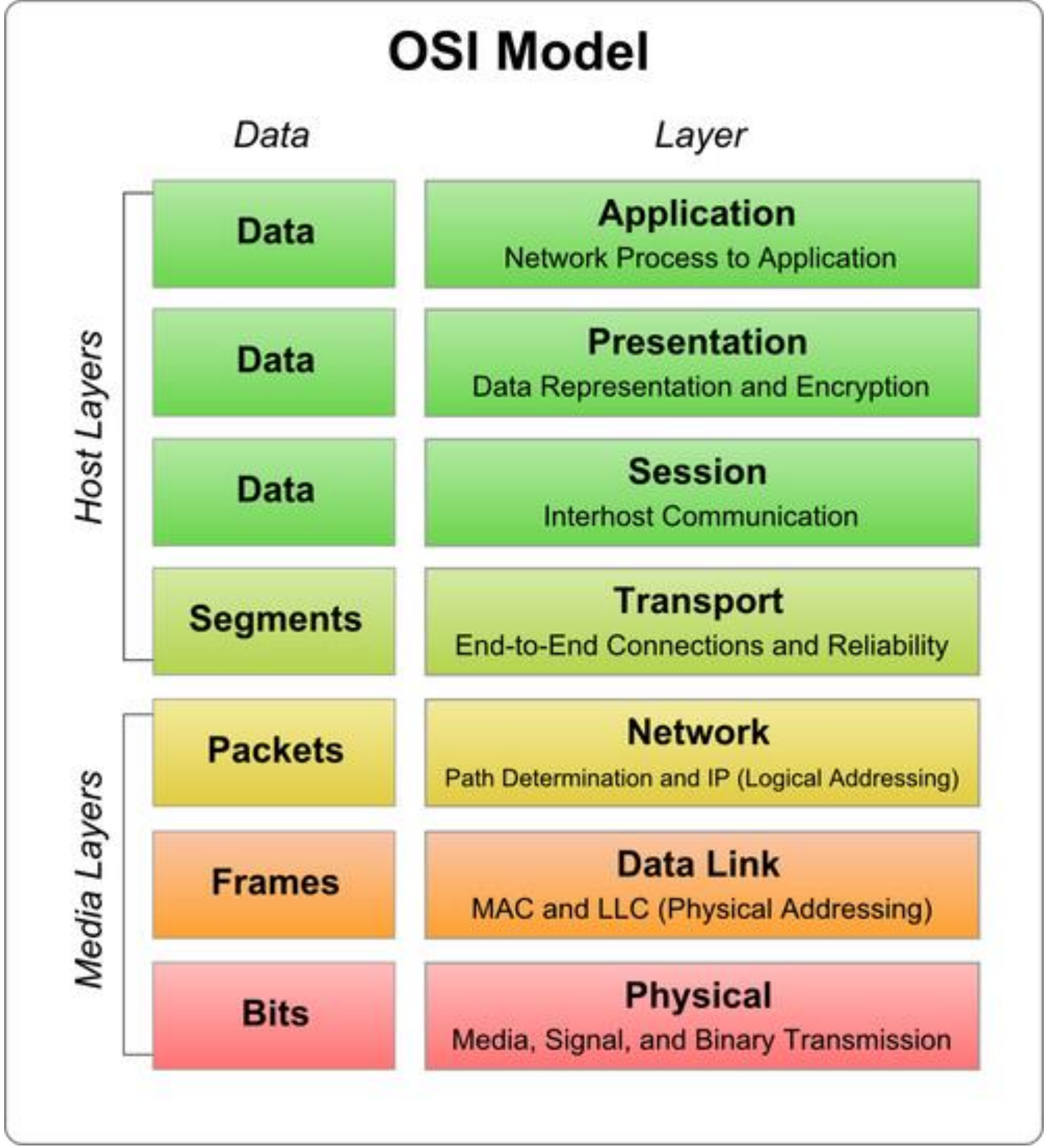
Today

- Open System Interconnect (OSI) model
- Firewalls
- Network Address Translation (NAT)
- Intrusion detection systems (IDS)

OSI Network Model

Open Systems Interconnect model

- A good way to think about networking steps logically
- Not how software is actually built

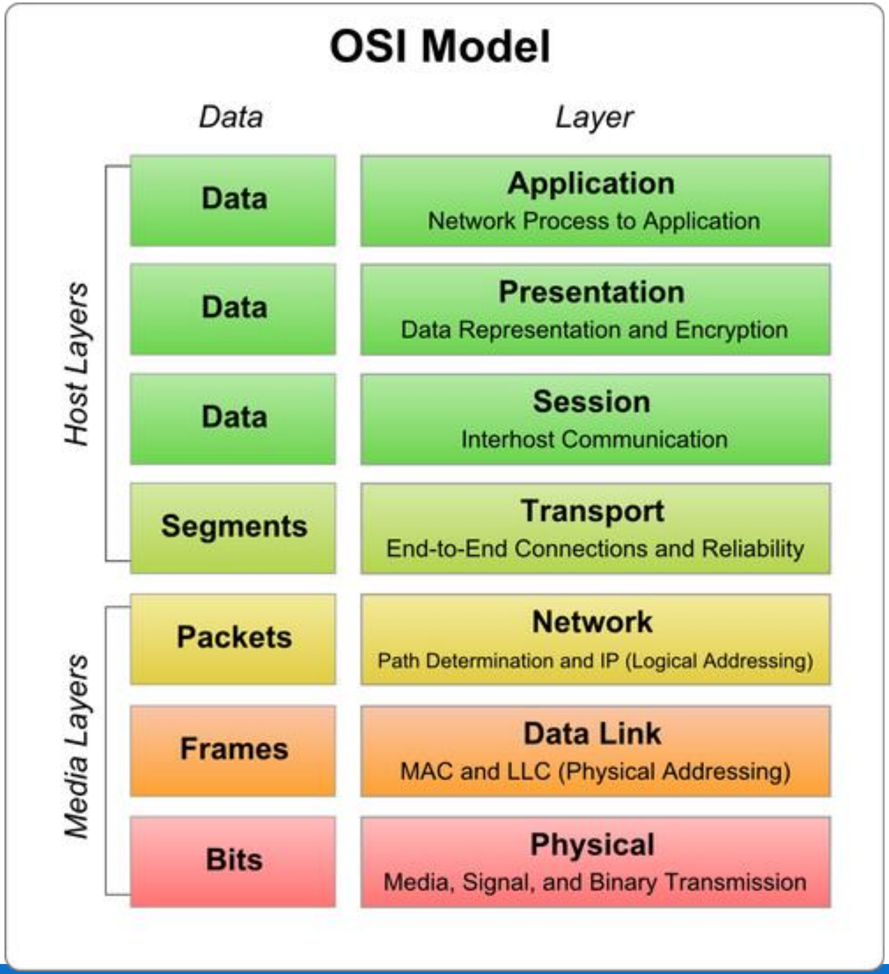


OSI Model

	Data	Layer
Host Layers	Data	**Application** Network Process to Application
	Data	**Presentation** Data Representation and Encryption
	Data	**Session** Interhost Communication
	Segments	**Transport** End-to-End Connections and Reliability
Media Layers	Packets	**Network** Path Determination and IP (Logical Addressing)
	Frames	**Data Link** MAC and LLC (Physical Addressing)
	Bits	**Physical** Media, Signal, and Binary Transmission

Image from: http://www.tech-faq.com/osi-model.html

OSI in terms of debugging errors



OSI Model

	Data	*Layer*
Host Layers	Data	**Application** Network Process to Application
	Data	**Presentation** Data Representation and Encryption
	Data	**Session** Interhost Communication
	Segments	**Transport** End-to-End Connections and Reliability
Media Layers	Packets	**Network** Path Determination and IP (Logical Addressing)
	Frames	**Data Link** MAC and LLC (Physical Addressing)
	Bits	**Physical** Media, Signal, and Binary Transmission

Can your browser open another website?

Do you have a viewer that supports jpg (image format)?

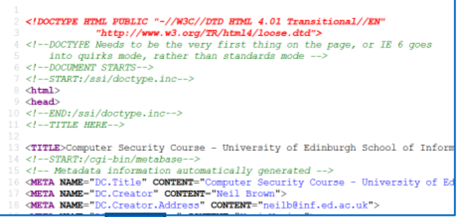
Can you ping the webserver you are trying to reach?

Can you ping the gateway or DNS server?

Do you have an IP address?

Is the light on the modem on?

Is the network cable plugged in?



```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
            "http://www.w3.org/TR/html4/loose.dtd">
<!--DOCTYPE Needs to be the very first thing on the page, or IE 6 goes
    into quirks mode, rather than standards mode -->
<!--DOCUMENT STARTS-->
<!--START:/ssi/doctype.inc-->
<html>
<head>
<!--END:/ssi/doctype.inc-->
<!--TITLE HERE-->

<TITLE>Computer Security Course - University of Edinburgh School of Inform
<!--START:/cgi-bin/metabase-->
<!-- Metadata information automatically generated -->
<META NAME="DC.Title" CONTENT="Computer Security Course - University of Ed
<META NAME="DC.Creator" CONTENT="Neil Brown">
<META NAME="DC.Creator.Address" CONTENT="neilb@inf.ed.ac.uk">
```

Sender: Apache server

7	**Application** Network process to application
6	**Presentation** Data representation and encryption
5	**Session** Interhost communication
4	**Transport** End-to-end connection and reliability
3	**Network** Path determination and IP (Logical Addressing)
2	**Data Link** MAC and LLC (Physical Addressing)
1	**Physical** Media, signal, and binary transmission

Data starts at the top of the OSI stack at level 7.

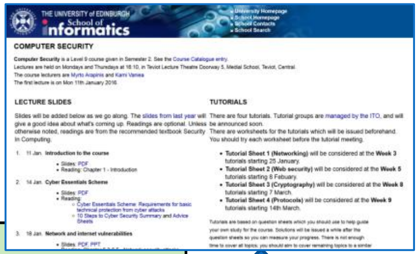
It progresses down the stack with each successive level adding or changing information.

At level 1 it travels across the physical layer to the recipient computer.

The recipient then processes the data up the stack. At level 7 an application processes the data.

Recipient: Firefox user

7	**Application** Network process to application
6	**Presentation** Data representation and encryption
5	**Session** Interhost communication
4	**Transport** End-to-end connection and reliability
3	**Network** Path determination and IP (Logical Addressing)
2	**Data Link** MAC and LLC (Physical Addressing)
1	**Physical** Media, signal, and binary transmission



COMPUTER SECURITY

Computer Security is a Level 9 course given in Semester 2. See the Course Catalogue entry.
Lectures are held on Mondays and Thursdays at 16:10, in Teviot Lecture Theatre Doorway 5, Medial School, Teviot, Central.
The course lecturers are Myrto Arapinis and Kami Vaniea
The first lecture is on Mon 11th January 2016.

LECTURE SLIDES

Slides will be added below as we go along. The slides from last year will give a good idea about what's coming up. Readings are optional. Unless otherwise noted, readings are from the recommended textbook Security in Computing.

1. 11 Jan. **Introduction to the course**
   - Slides: PDF
   - Reading: Chapter 1 - Introduction
2. 14 Jan. **Cyber Essentials Scheme**
   - Slides: PDF
   - Reading:
     - Cyber Essentials Scheme: Requirements for basic technical protection from cyber attacks
     - 10 Steps to Cyber Security Summary and Advice Sheets
3. 18 Jan. **Network and internet vulnerabilities**
   - Slides: PDF, PPT

TUTORIALS

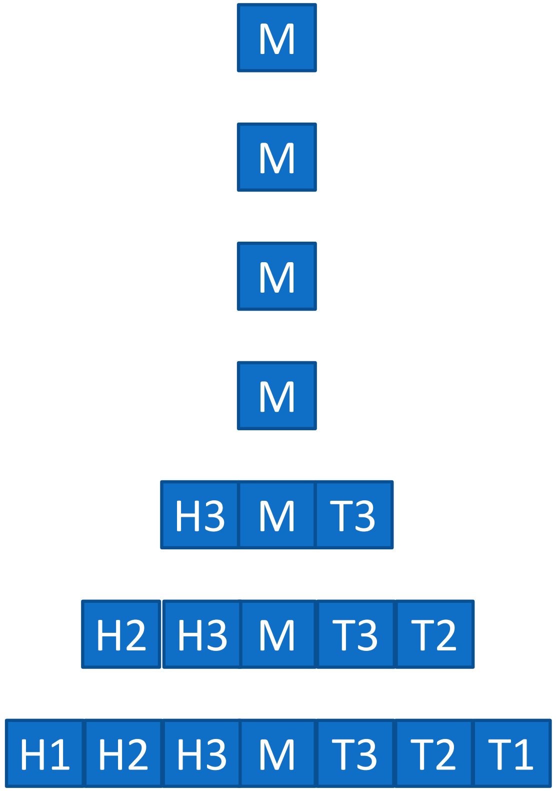
There are four tutorials. Tutorial groups are managed by the ITO, and will be announced soon.
There are worksheets for the tutorials which will be issued beforehand. You should try each worksheet before the tutorial meeting.

- **Tutorial Sheet 1 (Networking)** will be considered at the **Week 3** tutorials starting 25 January.
- **Tutorial Sheet 2 (Web security)** will be considered at the **Week 5** tutorials starting 8 Febuary.
- **Tutorial Sheet 3 (Cryptography)** will be considered at the **Week 8** tutorials starting 7 March.
- **Tutorial Sheet 4 (Protocols)** will be considered at the **Week 9** tutorials starting 14th March.

Tutorials are based on question sheets which you should use to help guide your own study for the course. Solutions will be issued a while after the question sheets so you can measure your progress. There is not enough time to cover all topics; you should aim to cover remaining topics to a similar

- Levels 7 and 6 involve the internal representation of the message
- Levels 5 and 4 involve setting up the connection
- Levels 3, 2, and 1 add header (H) and tail (T) information to each packet

Information is added to the message as it travels down the OSI levels



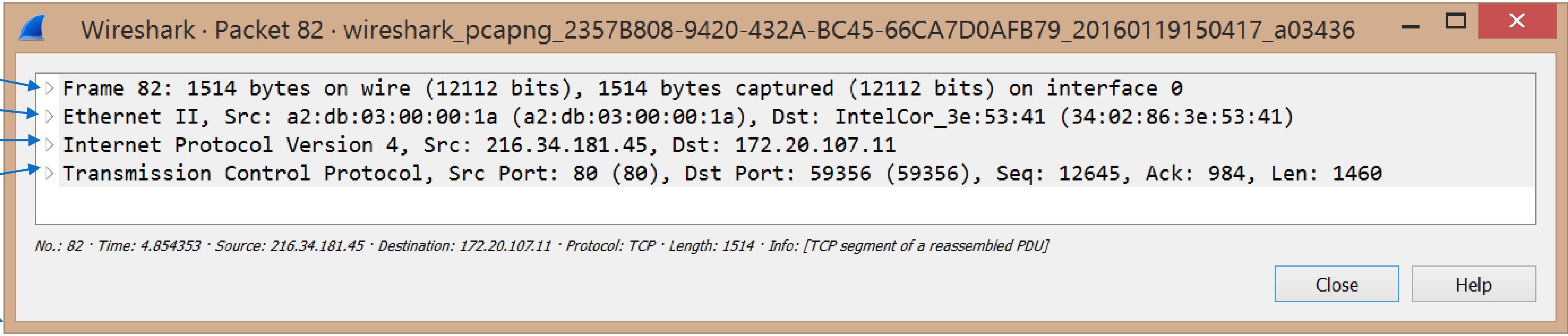
7	**Application** Network process to application
6	**Presentation** Data representation and encryption
5	**Session** Interhost communication
4	**Transport** End-to-end connection and reliability
3	**Network** Path determination and IP (Logical Addressing)
2	**Data Link** MAC and LLC (Physical Addressing)
1	**Physical** Media, signal, and binary transmission

Header data on a packet

1. Physical
2. Data link
3. Network
4. Transport

…

7. Application



Wireshark · Packet 82 · wireshark_pcapng_2357B808-9420-432A-BC45-66CA7D0AFB79_20160119150417_a03436

```
▷ Frame 82: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▷ Ethernet II, Src: a2:db:03:00:00:1a (a2:db:03:00:00:1a), Dst: IntelCor_3e:53:41 (34:02:86:3e:53:41)
▷ Internet Protocol Version 4, Src: 216.34.181.45, Dst: 172.20.107.11
▷ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 59356 (59356), Seq: 12645, Ack: 984, Len: 1460
```

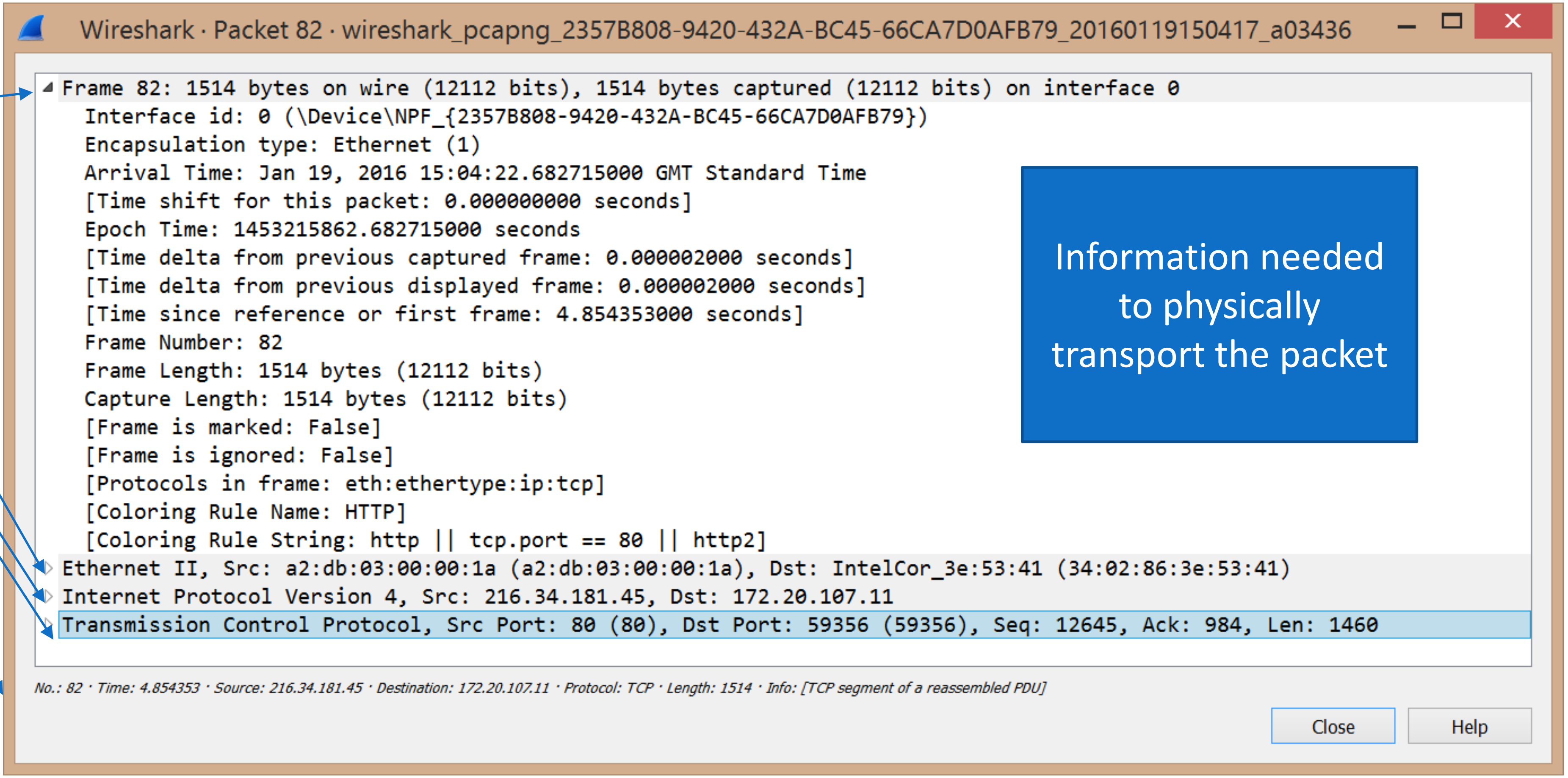
No.: 82 · Time: 4.854353 · Source: 216.34.181.45 · Destination: 172.20.107.11 · Protocol: TCP · Length: 1514 · Info: [TCP segment of a reassembled PDU]

Frame header data on a packet

1. Physical
2. Data link
3. Network
4. Transport

…

7. Application

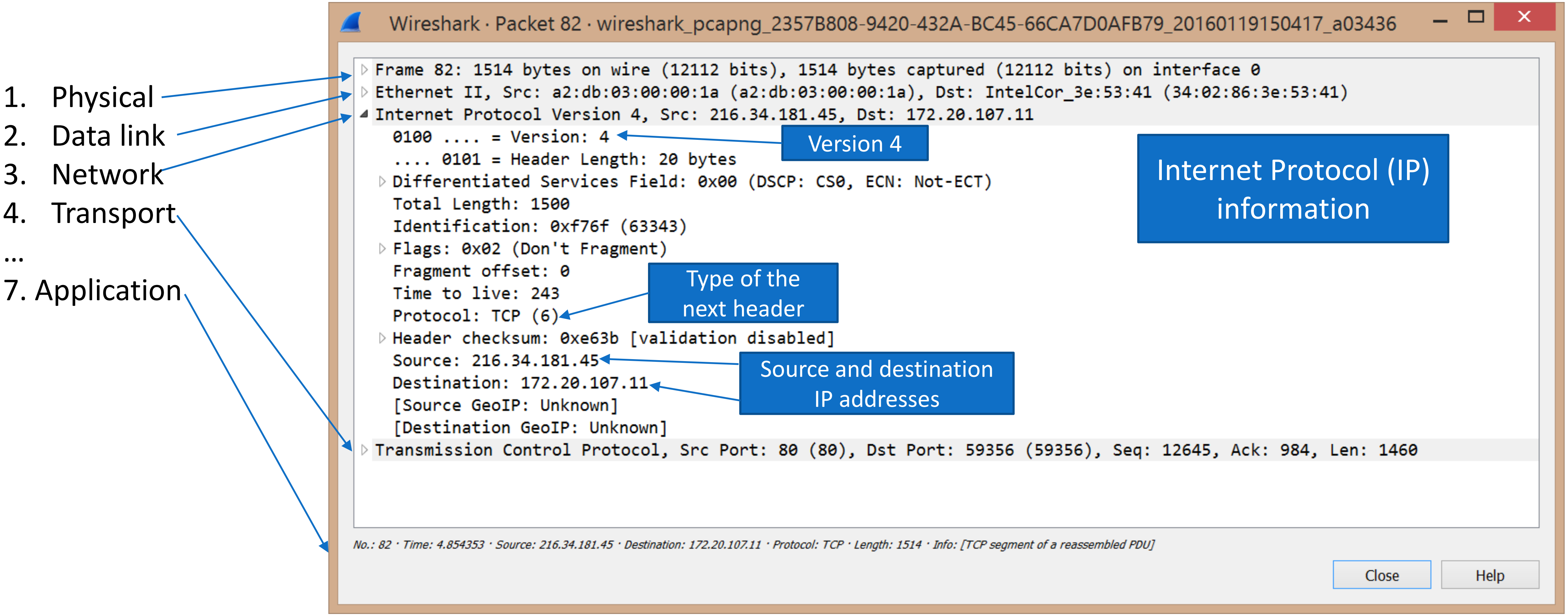

Wireshark · Packet 82 · wireshark_pcapng_2357B808-9420-432A-BC45-66CA7D0AFB79_20160119150417_a03436

```
◢ Frame 82: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
    Interface id: 0 (\Device\NPF_{2357B808-9420-432A-BC45-66CA7D0AFB79})
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 19, 2016 15:04:22.682715000 GMT Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1453215862.682715000 seconds
    [Time delta from previous captured frame: 0.000002000 seconds]
    [Time delta from previous displayed frame: 0.000002000 seconds]
    [Time since reference or first frame: 4.854353000 seconds]
    Frame Number: 82
    Frame Length: 1514 bytes (12112 bits)
    Capture Length: 1514 bytes (12112 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
▷ Ethernet II, Src: a2:db:03:00:00:1a (a2:db:03:00:00:1a), Dst: IntelCor_3e:53:41 (34:02:86:3e:53:41)
▷ Internet Protocol Version 4, Src: 216.34.181.45, Dst: 172.20.107.11
▷ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 59356 (59356), Seq: 12645, Ack: 984, Len: 1460
```

No.: 82 · Time: 4.854353 · Source: 216.34.181.45 · Destination: 172.20.107.11 · Protocol: TCP · Length: 1514 · Info: [TCP segment of a reassembled PDU]

Information needed to physically transport the packet

IP header data on a packet



1. Physical
2. Data link
3. Network
4. Transport

…

7. Application

Wireshark · Packet 82 · wireshark_pcapng_2357B808-9420-432A-BC45-66CA7D0AFB79_20160119150417_a03436

```
▷ Frame 82: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▷ Ethernet II, Src: a2:db:03:00:00:1a (a2:db:03:00:00:1a), Dst: IntelCor_3e:53:41 (34:02:86:3e:53:41)
◢ Internet Protocol Version 4, Src: 216.34.181.45, Dst: 172.20.107.11
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
  ▷ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0xf76f (63343)
  ▷ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 243
    Protocol: TCP (6)
  ▷ Header checksum: 0xe63b [validation disabled]
    Source: 216.34.181.45
    Destination: 172.20.107.11
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▷ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 59356 (59356), Seq: 12645, Ack: 984, Len: 1460
```

No.: 82 · Time: 4.854353 · Source: 216.34.181.45 · Destination: 172.20.107.11 · Protocol: TCP · Length: 1514 · Info: [TCP segment of a reassembled PDU]

Version 4

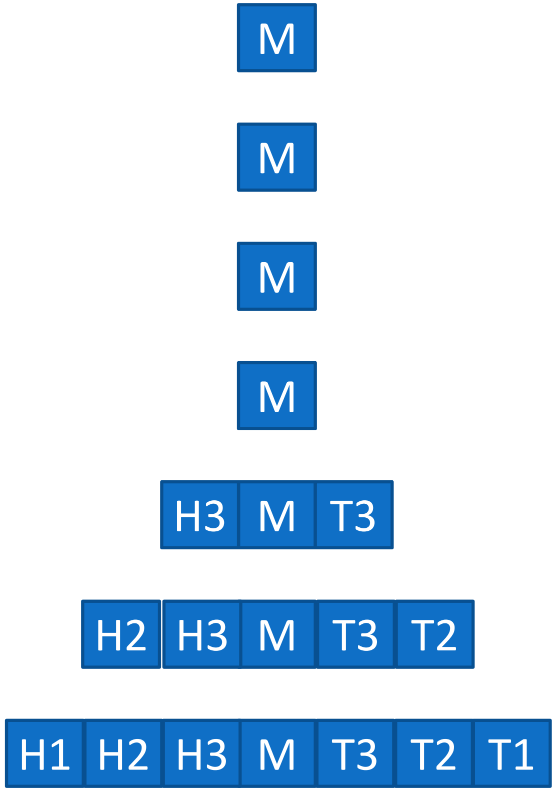
Internet Protocol (IP) information

Type of the next header

Source and destination IP addresses

Information is added to the message as it travels down the OSI levels

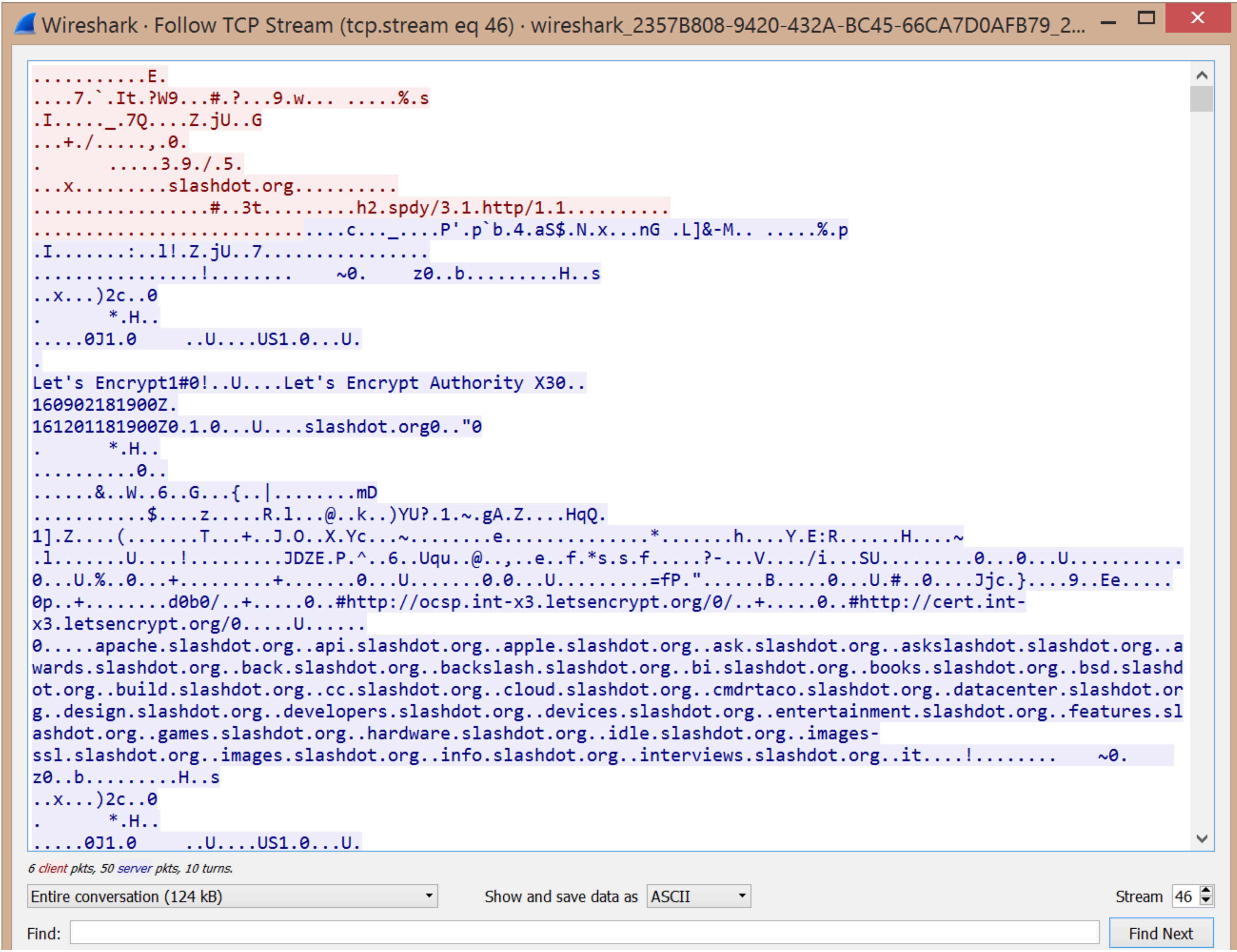
- Levels 7 and 6 involve the internal representation of the message
- Levels 5 and 4 involve setting up the connection
- Levels 3, 2, and 1 add header (H) and tail (T) information to each packet



7	**Application** Network process to application
6	**Presentation** Data representation and encryption
5	**Session** Interhost communication
4	**Transport** End-to-end connection and reliability
3	**Network** Path determination and IP (Logical Addressing)
2	**Data Link** MAC and LLC (Physical Addressing)
1	**Physical** Media, signal, and binary transmission

This is me visiting https://slashdot.org

- 6 packets were sent from my computer to the server
- 50 packets were sent from the server to my computer



Wireshark · Follow TCP Stream (tcp.stream eq 46) · wireshark_2357B808-9420-432A-BC45-66CA7D0AFB79_2...

```
...........E.
....7.`.It.?W9...#.?...9.w... .....%.s
.I....._.7Q....Z.jU..G
...+./.....,.0.
.       .....3.9./.5.
...x.........slashdot.org.........
.................#..3t.........h2.spdy/3.1.http/1.1..........
..........................c..._....P'.p`b.4.aS$.N.x...nG .L]&-M.. .....%.p
.I.......:..l!.Z.jU..7................
................!........    ~0.    z0..b.........H..s
..x...)2c..0
.       *.H..
.....0J1.0     ..U....US1.0...U.
.
Let's Encrypt1#0!..U....Let's Encrypt Authority X30..
160902181900Z.
161201181900Z0.1.0...U....slashdot.org0.."0
.       *.H..
..........0..
......&..W..6..G...{..|........mD
...........$....z.....R.l...@..k..)YU?.1.~.gA.Z....HqQ.
1].Z....(.......T...+..J.O..X.Yc...~........e..............*.......h....Y.E:R......H....~
.l.......U....!.........JDZE.P.^..6..Uqu..@..,..e..f.*s.s.f.....?-...V..../i...SU.........0...0...U..........
0...U.%..0...+.........+.......0...U.......0.0...U.........=fP."......B.....0...U.#..0....Jjc.}....9..Ee.....
0p..+........d0b0/..+.....0..#http://ocsp.int-x3.letsencrypt.org/0/..+.....0..#http://cert.int-
x3.letsencrypt.org/0.....U......
0.....apache.slashdot.org..api.slashdot.org..apple.slashdot.org..ask.slashdot.org..askslashdot.slashdot.org..a
wards.slashdot.org..back.slashdot.org..backslash.slashdot.org..bi.slashdot.org..books.slashdot.org..bsd.slashd
ot.org..build.slashdot.org..cc.slashdot.org..cloud.slashdot.org..cmdrtaco.slashdot.org..datacenter.slashdot.or
g..design.slashdot.org..developers.slashdot.org..devices.slashdot.org..entertainment.slashdot.org..features.sl
ashdot.org..games.slashdot.org..hardware.slashdot.org..idle.slashdot.org..images-
ssl.slashdot.org..images.slashdot.org..info.slashdot.org..interviews.slashdot.org..it....!........    ~0.
z0..b.........H..s
..x...)2c..0
.       *.H..
.....0J1.0     ..U....US1.0...U.
```

6 client pkts, 50 server pkts, 10 turns.

Entire conversation (124 kB)

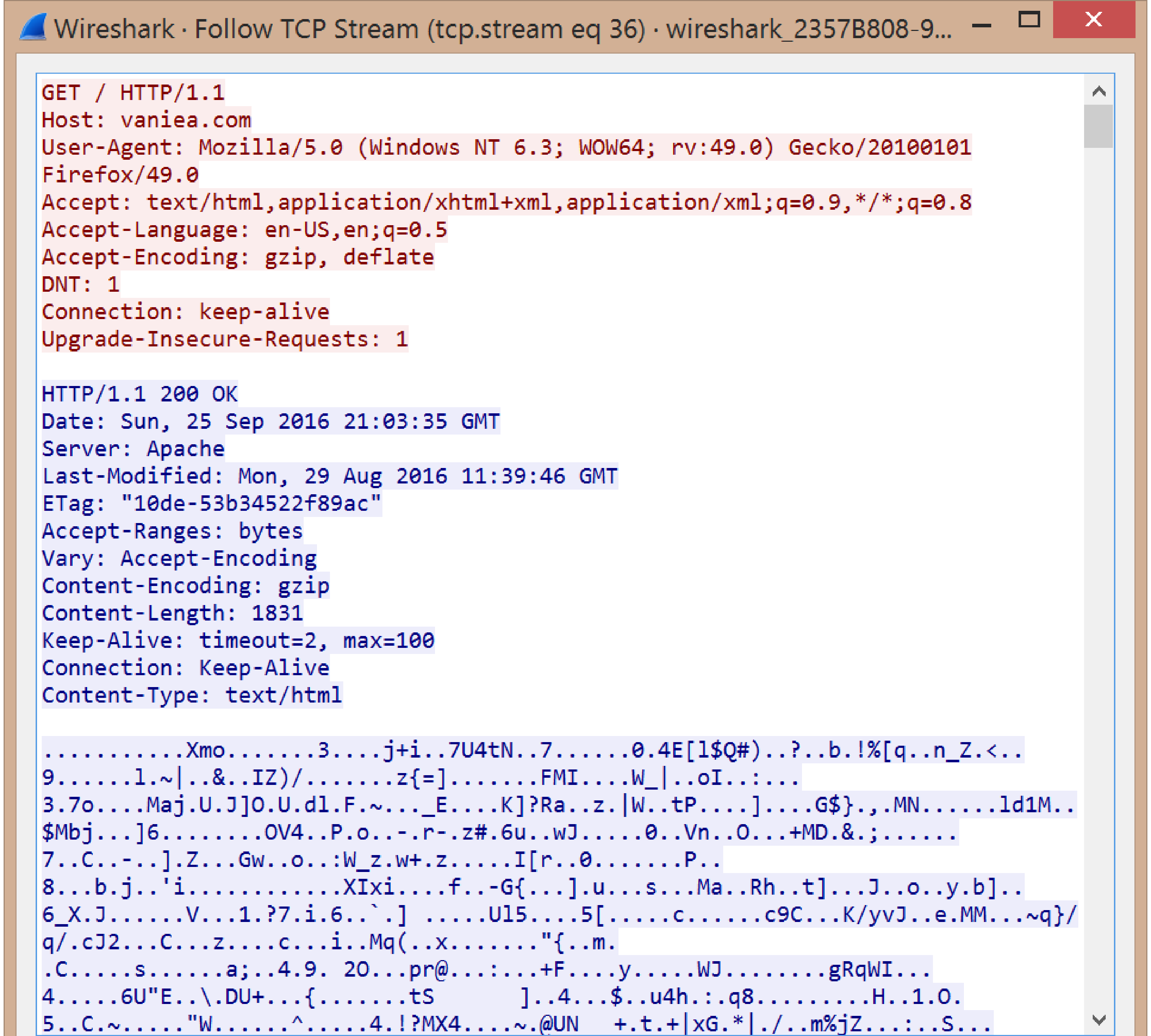
Show and save data as ASCII

Stream 46

Find:

This is me visiting http://vaniea.com

- Note the lack of https
- Why does the text look garbled anyway?



Wireshark · Follow TCP Stream (tcp.stream eq 36) · wireshark_2357B808-9...

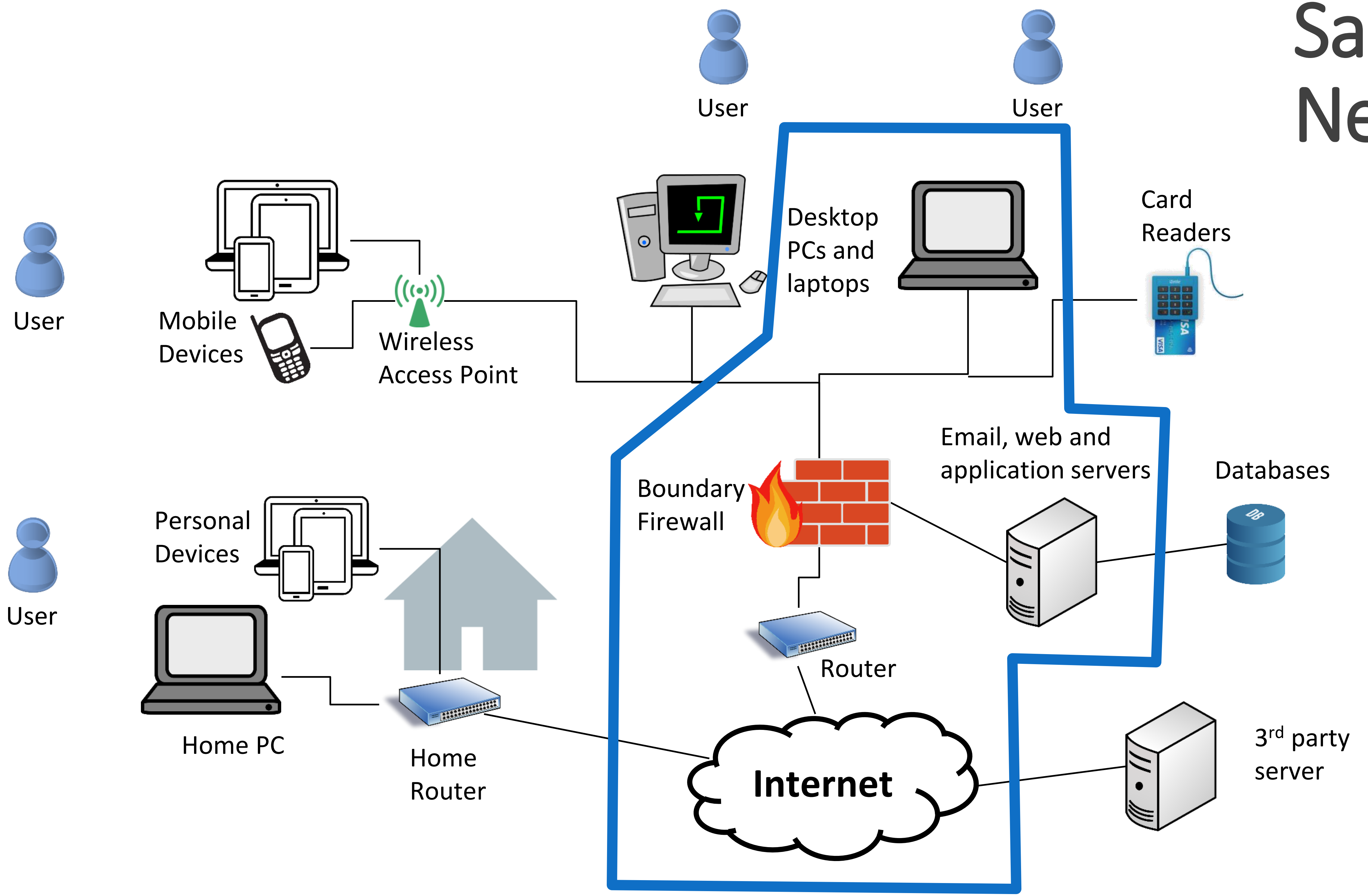
```
GET / HTTP/1.1
Host: vaniea.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:49.0) Gecko/20100101
Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Sun, 25 Sep 2016 21:03:35 GMT
Server: Apache
Last-Modified: Mon, 29 Aug 2016 11:39:46 GMT
ETag: "10de-53b34522f89ac"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 1831
Keep-Alive: timeout=2, max=100
Connection: Keep-Alive
Content-Type: text/html

...........Xmo.......3....j+i..7U4tN..7......0.4E[1$Q#)..?..b.!%[q..n_Z.<..
9......l.~|..&..IZ)/.......z{=].......FMI....W_|..oI..:...
3.7o....Maj.U.J]O.U.dl.F.~..._E....K]?Ra..z.|W..tP....]....G$}.,.MN......ld1M..
$Mbj...]6........OV4..P.o..-.r-.z#.6u..wJ.....0..Vn..O...+MD.&.;......
7..C..-..].Z...Gw..o..:W_z.w+.z.....I[r..0.......P..
8...b.j..'i...........XIxi....f..-G{...].u...s...Ma..Rh..t]...J..o..y.b]..
6_X.J......V...1.?7.i.6..`.] .....Ul5....5[.....c......c9C...K/yvJ..e.MM...~q}/
q/.cJ2...C...z....c...i..Mq(..x.......“{..m.
.C.....s......a;..4.9. 2O...pr@...:...+F....y.....WJ.........gRqWI...
4.....6U"E..\.DU+...{.......tS       ]..4...$..u4h.:.q8.........H..1.O.
5..C.~.....“W......^.....4.!?MX4....~.@UN   +.t.+|xG.*|./..m%jZ...:..S...
```

Firewalls

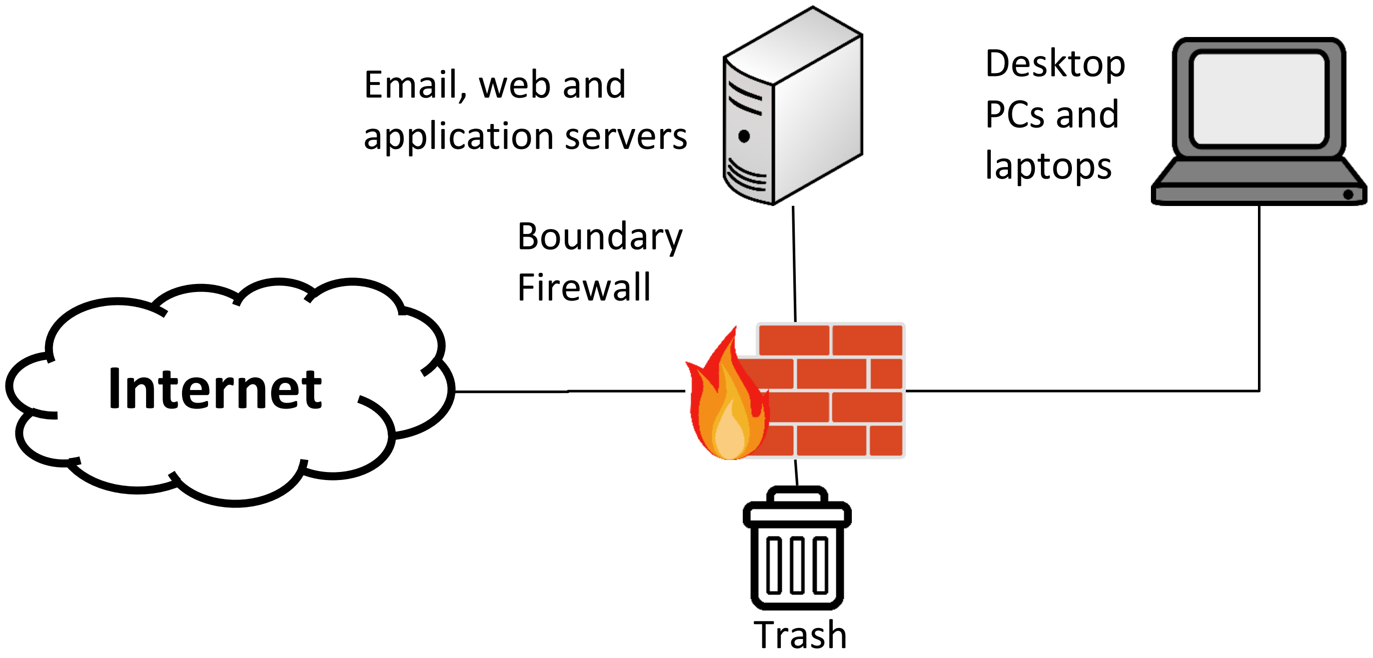
Firewalls

- Firewalls divide the untrusted outside of a network from the more trusted interior of a network
- Often they run on dedicated devices
  - Less possibilities for compromise – no compilers, linkers, loaders, debuggers, programming libraries, or other tools an attacker might use to escalate their attack
  - Easier to maintain few accounts
  - Physically divide the inside from outside of a network

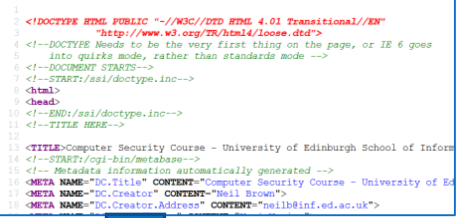
Sample Network



- Questionable things come from the internet AND from the local network
- Firewall applies a set of rules
- Based on rules, it allows or denies the traffic
- Firewalls can also act a routers deciding where to send traffic



Rule	Type	Source Address	Destination Address	Destination Port	Action
1	TCP	*	192.168.1.*	22	Permit
2	UDP	*	192.1681.*	69	Permit
3	TCP	192.168.1.*	*	80	Permit
4	TCP	*	192.168.1.18	80	Permit
5	UDP	*	192.168.1.*	*	Deny

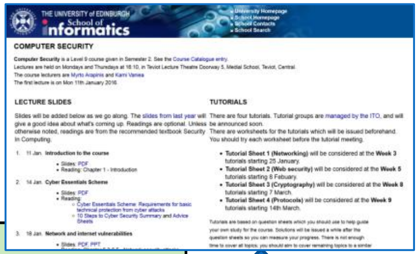


```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
            "http://www.w3.org/TR/html4/loose.dtd">
<!--DOCTYPE Needs to be the very first thing on the page, or IE 6 goes
    into quirks mode, rather than standards mode -->
<!--DOCUMENT STARTS-->
<!--START:/ssi/doctype.inc-->
<html>
<head>
<!--END:/ssi/doctype.inc-->
<!--TITLE HERE-->

<TITLE>Computer Security Course - University of Edinburgh School of Inform
<!--START:/cgi-bin/metabase-->
<!-- Metadata information automatically generated -->
<META NAME="DC.Title" CONTENT="Computer Security Course - University of Ed
<META NAME="DC.Creator" CONTENT="Neil Brown">
<META NAME="DC.Creator.Address" CONTENT="neilb@inf.ed.ac.uk">
```

Sender:
Apache server

7	Apache **Application** Network process to application
6	**Presentation** Data representation and encryption
5	**Session** Interhost communication
4	**Transport** End-to-end connection and reliability
3	**Network** Path determination and IP (Logical Addressing)
2	**Data Link** MAC and LLC (Physical Addressing)
1	**Physical** Media, signal, and binary transmission

Recipient:
Firefox user



THE UNIVERSITY of EDINBURGH
School of informatics

- University Homepage
- School Homepage
- School Contacts
- School Search

COMPUTER SECURITY

Computer Security is a Level 9 course given in Semester 2. See the Course Catalogue entry.
Lectures are held on Mondays and Thursdays at 16:10, in Teviot Lecture Theatre Doorway 5, Medial School, Teviot, Central.
The course lecturers are Myrto Arapinis and Kami Vaniea
The first lecture is on Mon 11th January 2016.

LECTURE SLIDES

Slides will be added below as we go along. The slides from last year will give a good idea about what's coming up. Readings are optional. Unless otherwise noted, readings are from the recommended textbook Security in Computing.

1. 11 Jan. **Introduction to the course**
   - Slides: PDF
   - Reading: Chapter 1 - Introduction
2. 14 Jan. **Cyber Essentials Scheme**
   - Slides: PDF
   - Reading:
     - Cyber Essentials Scheme: Requirements for basic technical protection from cyber attacks
     - 10 Steps to Cyber Security Summary and Advice Sheets
3. 18 Jan. **Network and internet vulnerabilities**
   - Slides: PDF, PPT

TUTORIALS

There are four tutorials. Tutorial groups are managed by the ITO, and will be announced soon.
There are worksheets for the tutorials which will be issued beforehand. You should try each worksheet before the tutorial meeting.

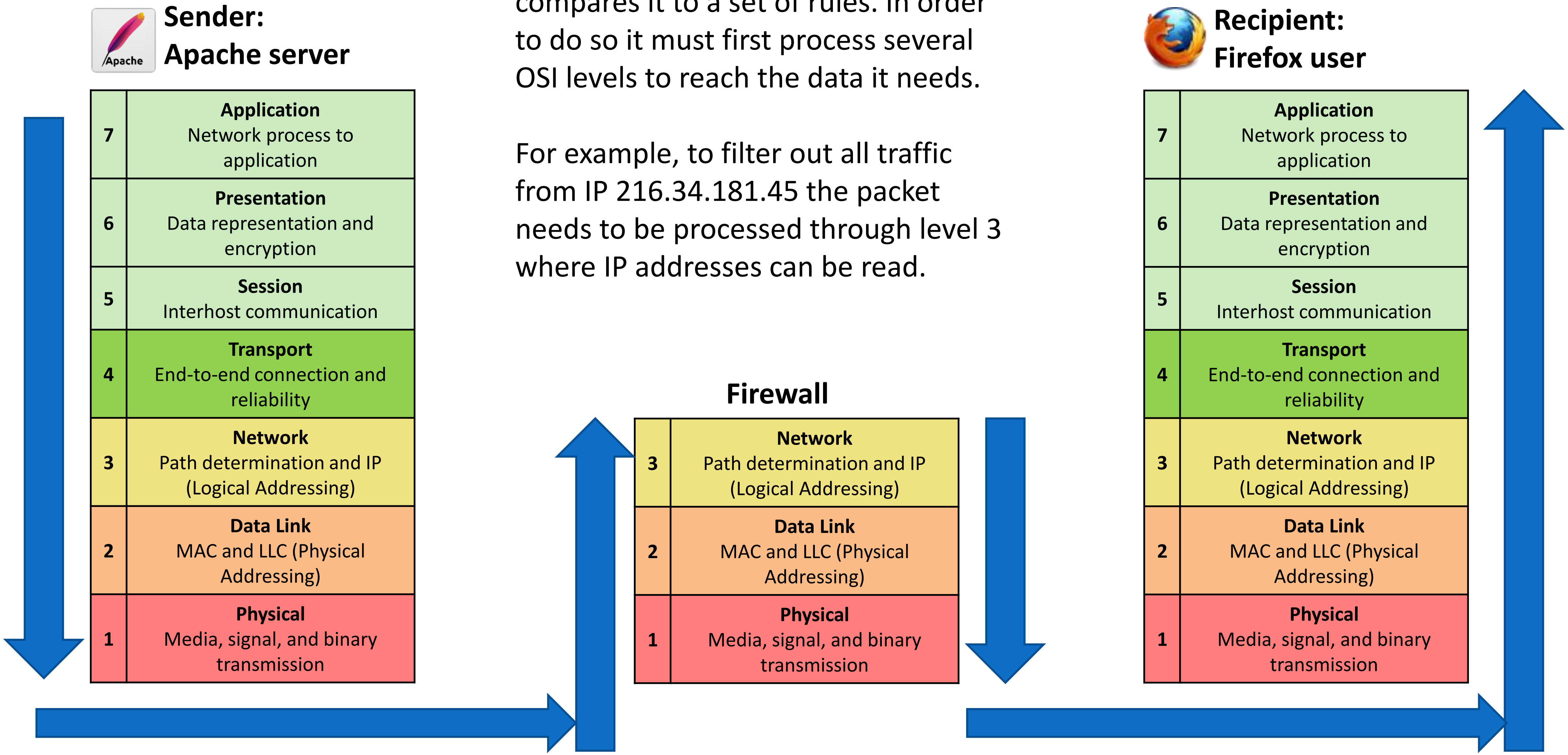
- **Tutorial Sheet 1 (Networking)** will be considered at the **Week 3** tutorials starting 25 January.
- **Tutorial Sheet 2 (Web security)** will be considered at the **Week 5** tutorials starting 8 Febuary.
- **Tutorial Sheet 3 (Cryptography)** will be considered at the **Week 8** tutorials starting 7 March.
- **Tutorial Sheet 4 (Protocols)** will be considered at the **Week 9** tutorials starting 14th March.

Tutorials are based on question sheets which you should use to help guide your own study for the course. Solutions will be issued a while after the question sheets so you can measure your progress. There is not enough time to cover all topics; you should aim to cover remaining topics to a similar

7	**Application** Network process to application
6	**Presentation** Data representation and encryption
5	**Session** Interhost communication
4	**Transport** End-to-end connection and reliability
3	**Network** Path determination and IP (Logical Addressing)
2	**Data Link** MAC and LLC (Physical Addressing)
1	**Physical** Media, signal, and binary transmission

A firewall takes in network traffic and compares it to a set of rules. In order to do so it must first process several OSI levels to reach the data it needs.

For example, to filter out all traffic from IP 216.34.181.45 the packet needs to be processed through level 3 where IP addresses can be read.



Sender: Apache server

7	**Application** Network process to application
6	**Presentation** Data representation and encryption
5	**Session** Interhost communication
4	**Transport** End-to-end connection and reliability
3	**Network** Path determination and IP (Logical Addressing)
2	**Data Link** MAC and LLC (Physical Addressing)
1	**Physical** Media, signal, and binary transmission

Firewall

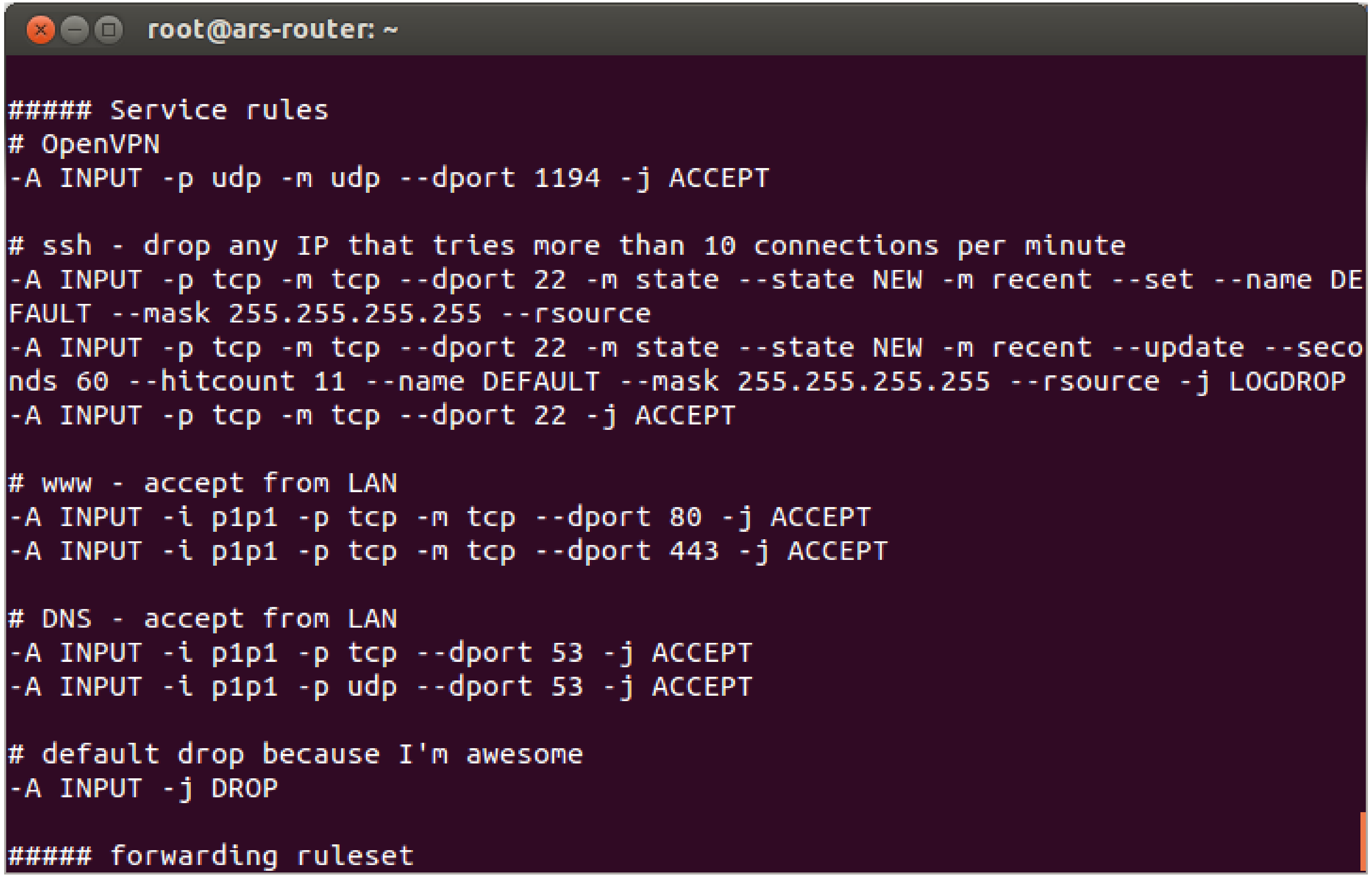
3	**Network** Path determination and IP (Logical Addressing)
2	**Data Link** MAC and LLC (Physical Addressing)
1	**Physical** Media, signal, and binary transmission

Recipient: Firefox user

7	**Application** Network process to application
6	**Presentation** Data representation and encryption
5	**Session** Interhost communication
4	**Transport** End-to-end connection and reliability
3	**Network** Path determination and IP (Logical Addressing)
2	**Data Link** MAC and LLC (Physical Addressing)
1	**Physical** Media, signal, and binary transmission

Firewall ruleset from a custom home router

- Taken from an ARSTechnica article



```
##### Service rules
# OpenVPN
-A INPUT -p udp -m udp --dport 1194 -j ACCEPT

# ssh - drop any IP that tries more than 10 connections per minute
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --set --name DE
FAULT --mask 255.255.255.255 --rsource
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --update --seco
nds 60 --hitcount 11 --name DEFAULT --mask 255.255.255.255 --rsource -j LOGDROP
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT

# www - accept from LAN
-A INPUT -i p1p1 -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -i p1p1 -p tcp -m tcp --dport 443 -j ACCEPT

# DNS - accept from LAN
-A INPUT -i p1p1 -p tcp --dport 53 -j ACCEPT
-A INPUT -i p1p1 -p udp --dport 53 -j ACCEPT

# default drop because I'm awesome
-A INPUT -j DROP

##### forwarding ruleset
```

Image: http://arstechnica.co.uk/gadgets/2016/01/numbers-dont-lie-its-time-to-build-your-own-router/

There are many types of Firewalls

Key differences include:

- How implemented
  - Software – slower, easier to deploy on personal computers
  - Hardware – faster, somewhat safer, harder to add in
- Number of OSI levels of processing required
  - Packet size (level 1)
  - MAC (level 2) and IP (level 3) filtering
  - Port filtering (level 3)
  - Deep packet (level 4+)

Today we will talk about:

- Packet filtering gateway
- Stateful inspection firewall
- Application proxy
- Personal firewalls

Packet filtering gateway or screening router

- Simplest – compares information found in the headers to the policy rules
- Operate at OSI level 3
- Source addresses and ports can be forged, which a packet filter cannot detect
- Design is simple, but tons of rules are needed, so it is challenging to maintain

Stateful inspection firewall

- Maintains state from one packet to another
- Similar to a packet filtering gateway, but can remember recent events
- For example, if a outside host starts sending packets to many internal destination ports (aka a port scan) a stateful firewall would record the number of ports probed and once it is over the threshold specified in the policy it would block all further traffic

Port scan

- An attacker is looking for applications listening on ports
- A single IP address (right) is contacting many ports (left) to see if any respond

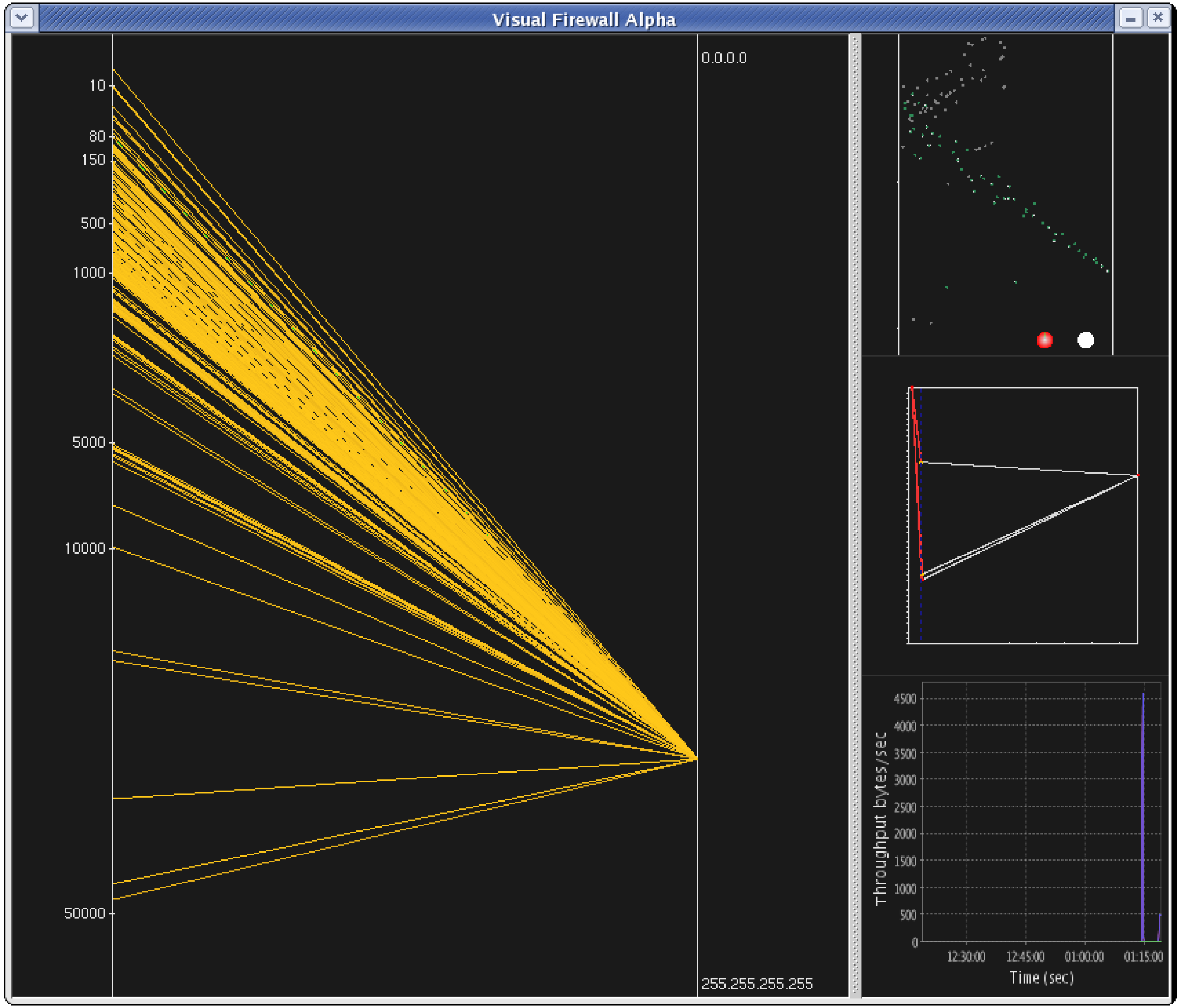
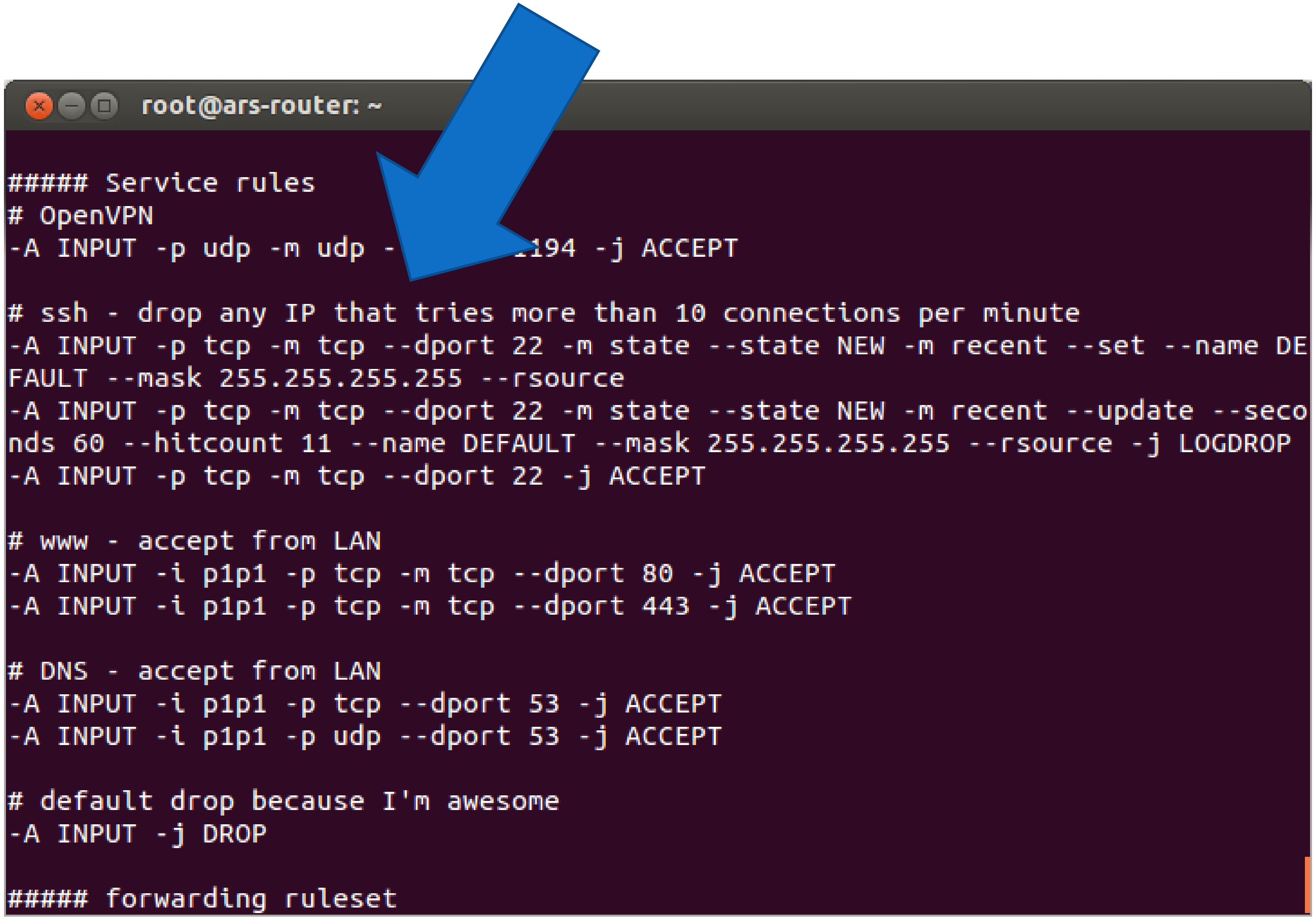


Image: http://chrislee.dhs.org/projects/visualfirewall.html

Firewall ruleset from a custom home router

- Taken from an ARSTechnica article



```
##### Service rules
# OpenVPN
-A INPUT -p udp -m udp -      194 -j ACCEPT

# ssh - drop any IP that tries more than 10 connections per minute
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --set --name DE
FAULT --mask 255.255.255.255 --rsource
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --update --seco
nds 60 --hitcount 11 --name DEFAULT --mask 255.255.255.255 --rsource -j LOGDROP
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT

# www - accept from LAN
-A INPUT -i p1p1 -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -i p1p1 -p tcp -m tcp --dport 443 -j ACCEPT

# DNS - accept from LAN
-A INPUT -i p1p1 -p tcp --dport 53 -j ACCEPT
-A INPUT -i p1p1 -p udp --dport 53 -j ACCEPT

# default drop because I'm awesome
-A INPUT -j DROP

##### forwarding ruleset
```

Image: http://arstechnica.co.uk/gadgets/2016/01/numbers-dont-lie-its-time-to-build-your-own-router/

Application proxy

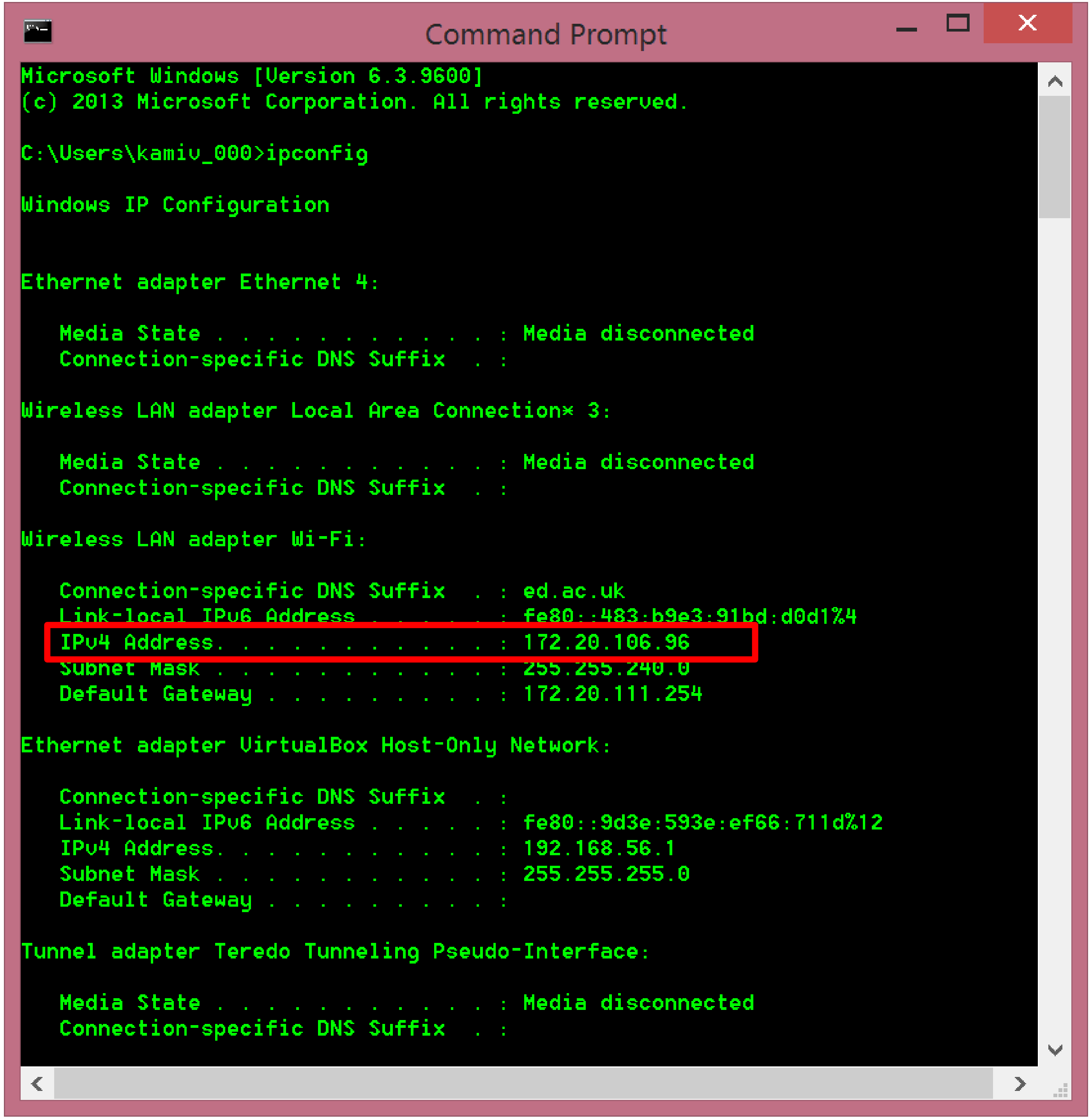
- Simulates the (proper) effects of an application at OSI level 7
- Effectively a protective Man In The Middle that screens information at an application layer (OSI 7)
- Allows an administrator to block certain application requests.
- For example:
    - Block all web traffic containing certain words
    - Remove all macros from Microsoft Word files in email
    - Prevent anything that looks like a credit card number from leaving a database

Personal firewalls

- Runs on the workstation that it protects (software)
- Provides basic protection, especially for home or mobile devices
- Malicious software can disable part or all of the firewall
- Any rootkit type software can disable the firewall

Network Address Translation (NAT)

Looking at the IP address of my laptop which is connected to the University WIFI.



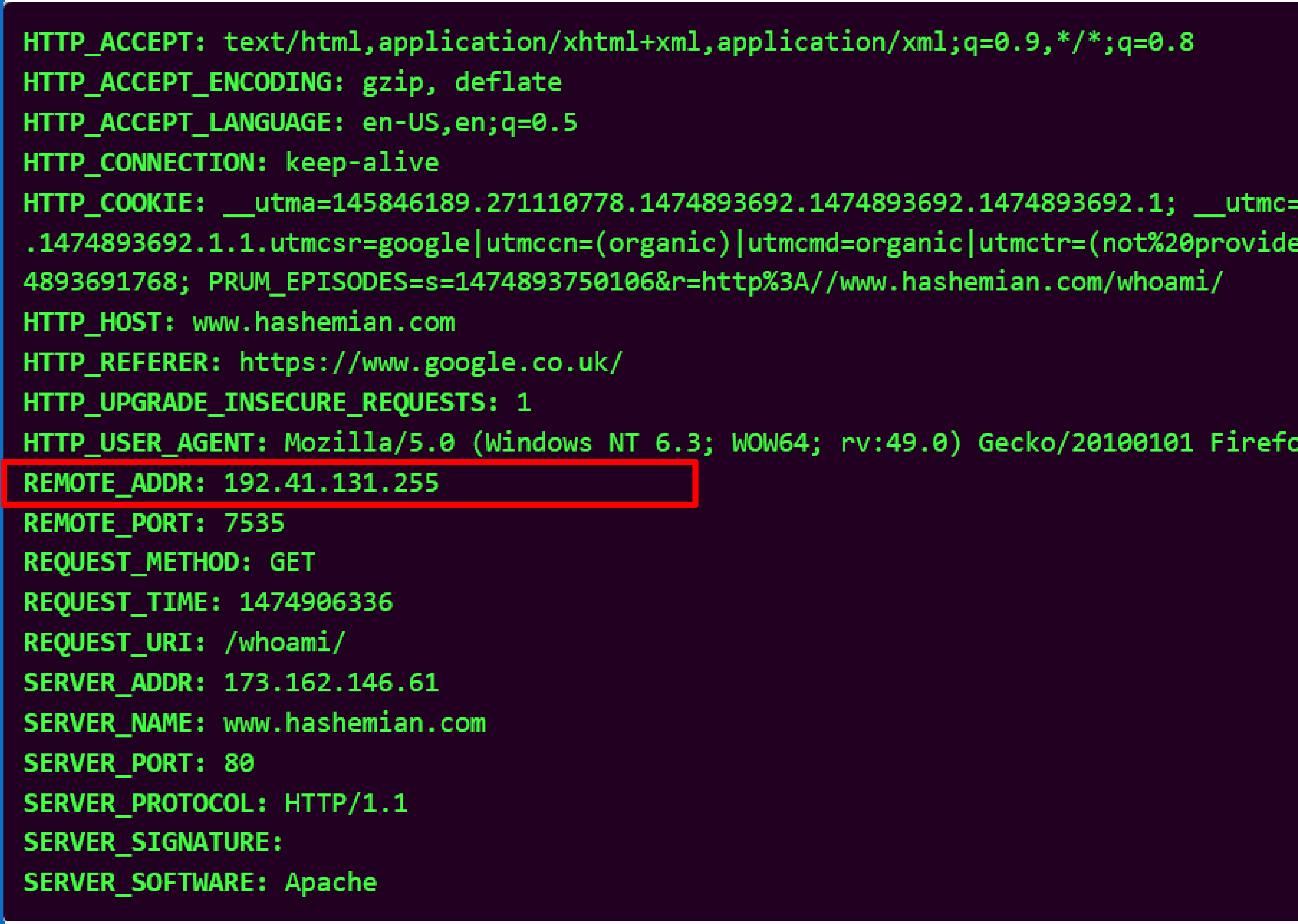
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kamiv_000>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 4:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : ed.ac.uk
   Link-local IPv6 Address . . . . . : fe80::483:b9e3:91bd:d0d1%4
   IPv4 Address. . . . . . . . . . . : 172.20.106.96
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 172.20.111.254

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9d3e:593e:ef66:711d%12
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

My computer as seen from a remote server

(http://www.hashemian.com/whoami/)

My IP previously showed as: 172.20.106.96

What happened?

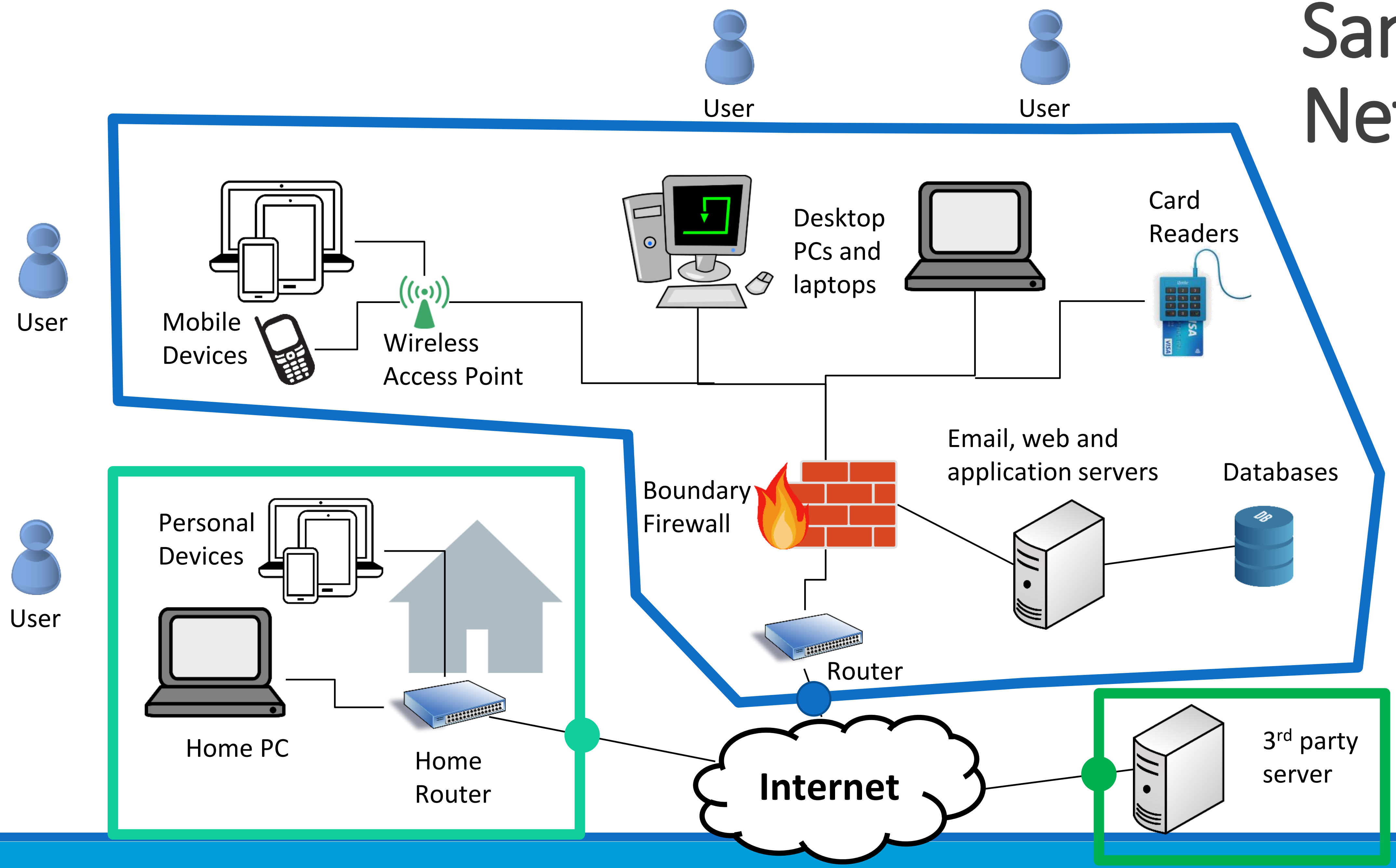


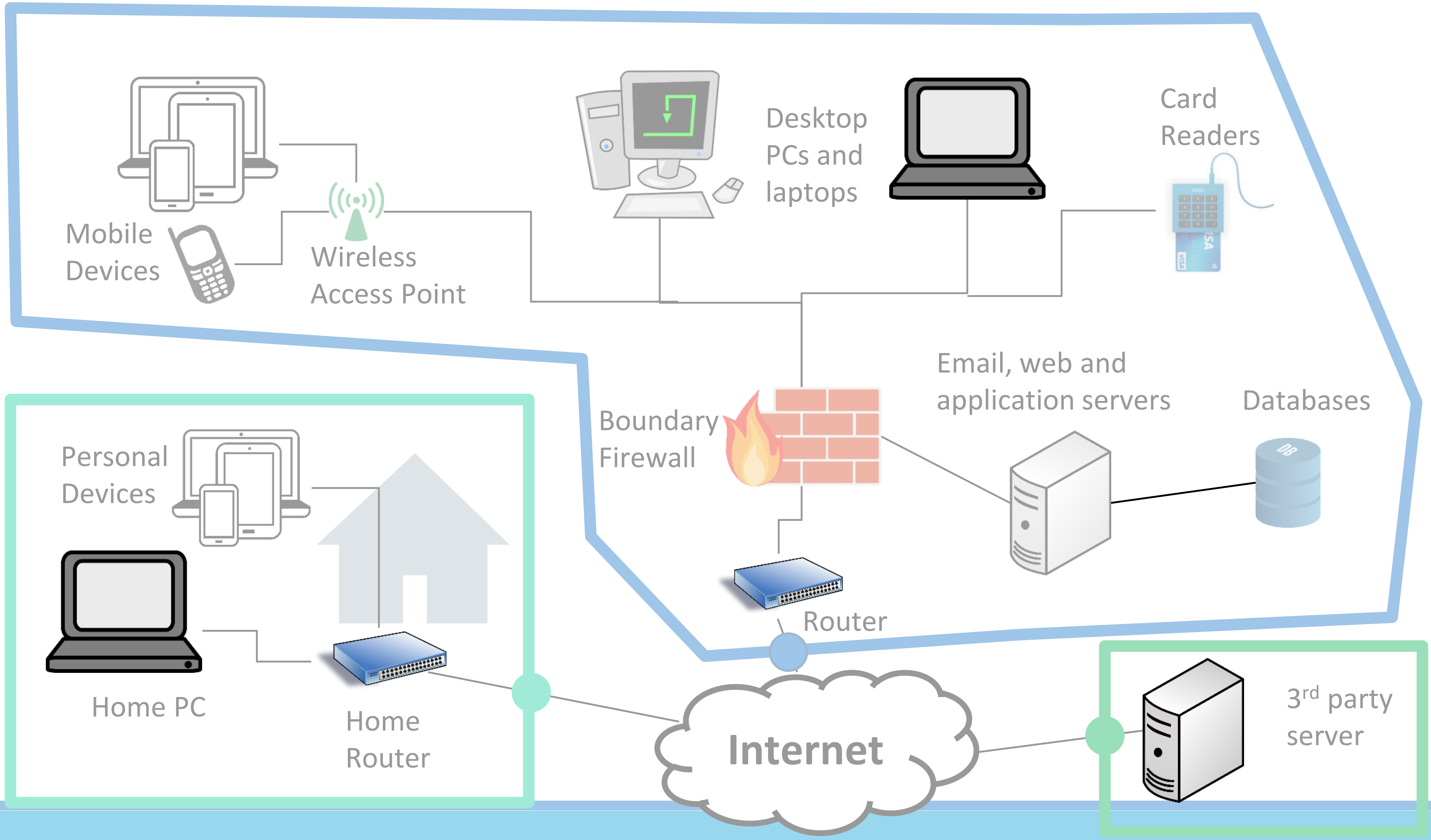
```
HTTP_ACCEPT: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_ENCODING: gzip, deflate
HTTP_ACCEPT_LANGUAGE: en-US,en;q=0.5
HTTP_CONNECTION: keep-alive
HTTP_COOKIE: __utma=145846189.271110778.1474893692.1474893692.1474893692.1; __utmc=
.1474893692.1.1.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provide
4893691768; PRUM_EPISODES=s=1474893750106&r=http%3A//www.hashemian.com/whoami/
HTTP_HOST: www.hashemian.com
HTTP_REFERER: https://www.google.co.uk/
HTTP_UPGRADE_INSECURE_REQUESTS: 1
HTTP_USER_AGENT: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:49.0) Gecko/20100101 Firefo
REMOTE_ADDR: 192.41.131.255
REMOTE_PORT: 7535
REQUEST_METHOD: GET
REQUEST_TIME: 1474906336
REQUEST_URI: /whoami/
SERVER_ADDR: 173.162.146.61
SERVER_NAME: www.hashemian.com
SERVER_PORT: 80
SERVER_PROTOCOL: HTTP/1.1
SERVER_SIGNATURE:
SERVER_SOFTWARE: Apache
```

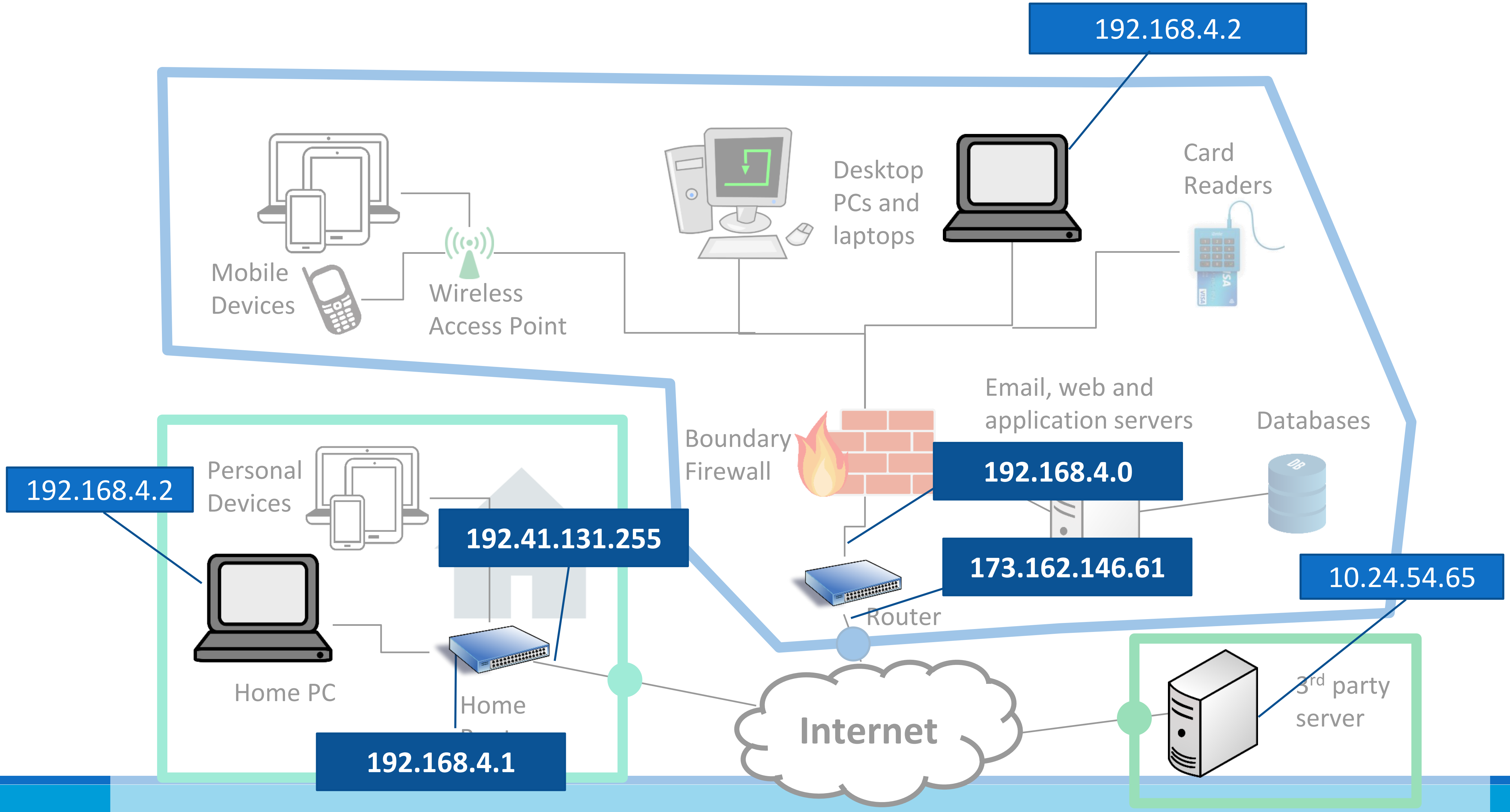
IPv4 and address space exhaustion

- Version 4 of the Internet Protocol
  - 192.168.2.6
- There are less than 4.3 billion IPv4 addresses available
- We do not have enough addresses for every device on the planet
- Answer: Network Address Translation
  - Internal IP different than external IP
  - Border router maps between its own IP and the internal ones

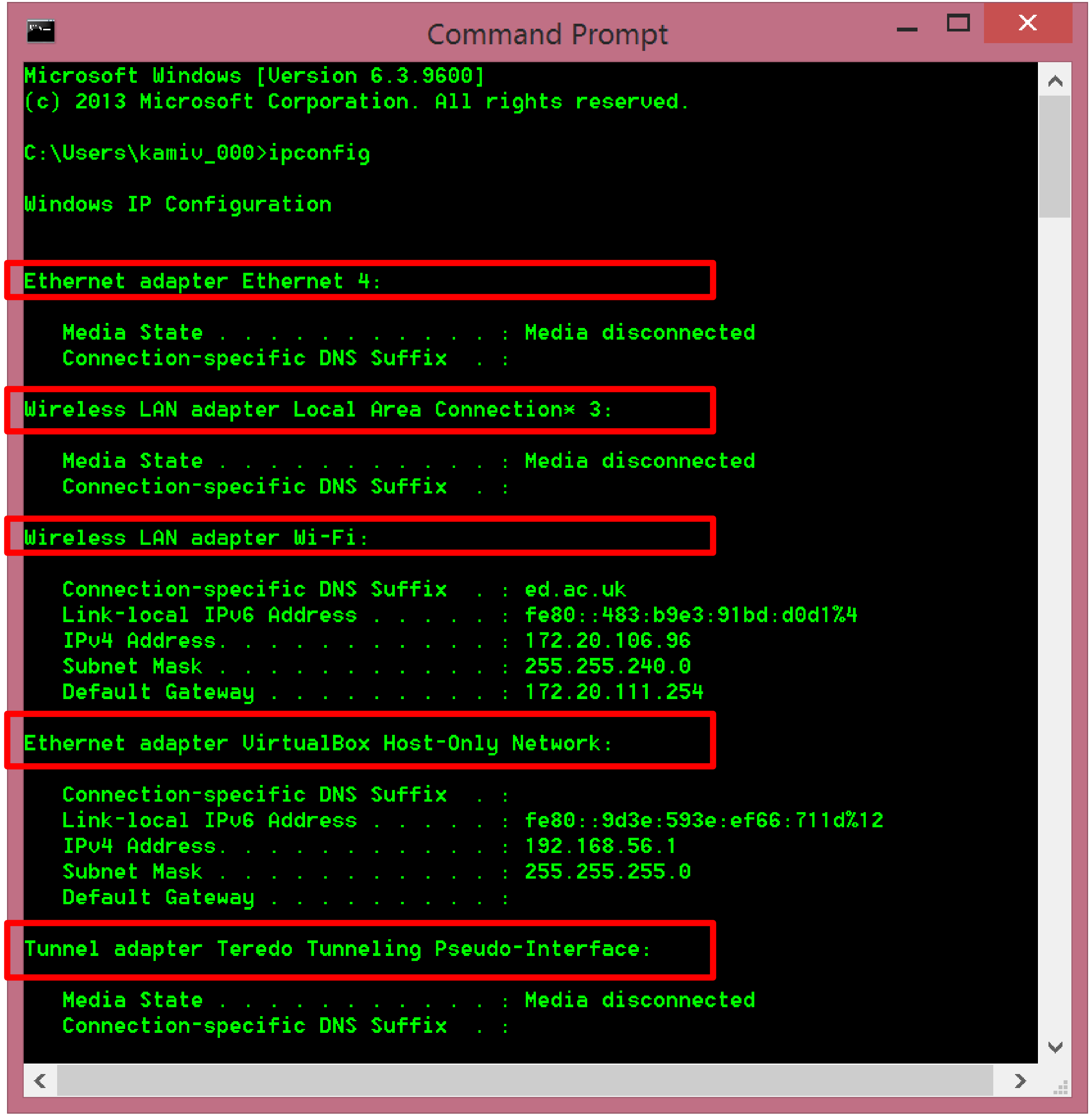
Sample Network



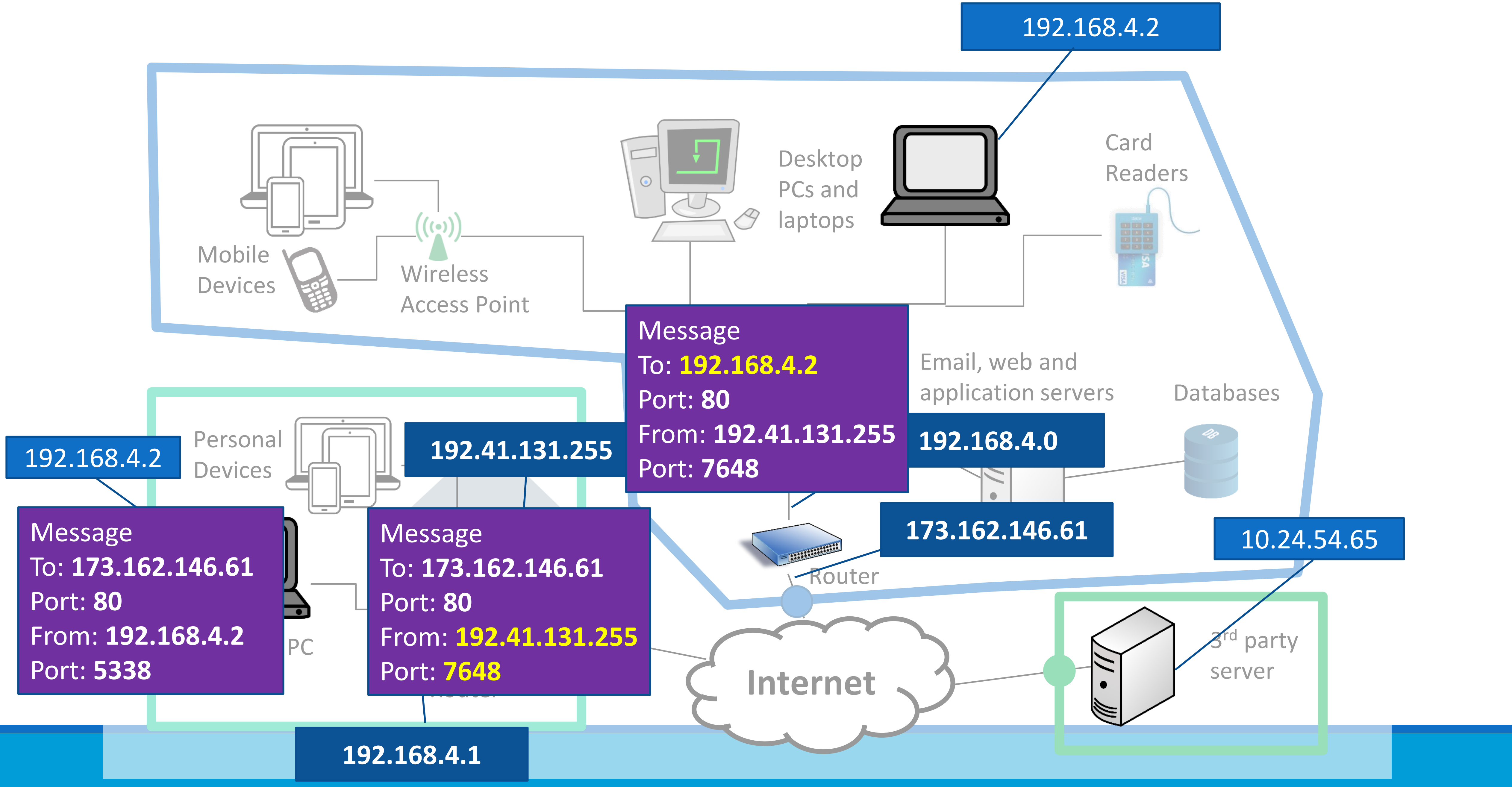

Mobile Devices
Wireless Access Point
Desktop PCs and laptops
Card Readers
Email, web and application servers
Databases
Boundary Firewall
Router
Personal Devices
Home PC
Home Router
Internet
3rd party server


192.168.4.2
Mobile Devices
Wireless Access Point
Desktop PCs and laptops
Card Readers
Email, web and application servers
Databases
Boundary Firewall
192.168.4.0
173.162.146.61
Router
10.24.54.65
Personal Devices
192.168.4.2
192.41.131.255
Home PC
Home
192.168.4.1
Internet
3rd party server

My laptop can have multiple IPs and bridge networks too. Here it shows IPs for both my VirtualBox and my WIF.



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kamiv_000>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 4:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : ed.ac.uk
   Link-local IPv6 Address . . . . . : fe80::483:b9e3:91bd:d0d1%4
   IPv4 Address. . . . . . . . . . . : 172.20.106.96
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 172.20.111.254

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9d3e:593e:ef66:711d%12
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```



Message
To: **192.168.4.2**
Port: **80**
From: **192.41.131.255**
Port: **7648**

Message
To: **173.162.146.61**
Port: **80**
From: **192.168.4.2**
Port: **5338**

Message
To: **173.162.146.61**
Port: **80**
From: **192.41.131.255**
Port: **7648**

Intrusion Detection Systems (IDS)

1:53 58
7:53 58
12:53 58
17:53 58
20:53 58
12:53:58
1
T22 COUNTDOWN

Firewalls are preventative,
IDS detects a potential incident in progress

- At some point you have to let some traffic into and out of your network (otherwise users get upset)
- Most security incidents are caused by a user letting something into the network that is malicious, or by being an insider threat themselves
- These cannot be prevented or anticipated in advance
- The next step is to identify that something bad is happening quickly so you can address it

Signature based

- Perform simple pattern matching and report situations that match the pattern
- Requires that admin anticipate attack patterns in advance
- Attacker may test attack on common signatures
- Impossible to detect a new type of attack
- High accuracy, low false positives

Heuristic based

- Dynamically build a model of acceptable or “normal” behavior and flag anything that does not match
- Admin does not need to anticipate potential attacks
- System needs time to warm up to new behavior
- Can detect new types of attacks
- Higher false positives, lower accuracy

Number of alarms is a big problem

- In the Target breach the IDS did correctly identify that there was an attack on the Target network
- There were too many alarms going off to investigate all of them in great depth
- Some cyberattack insurance policies state that if you know about an attack and do nothing they will not cover the attack.
- Having a noisy IDS can potentially be a liability

Questions