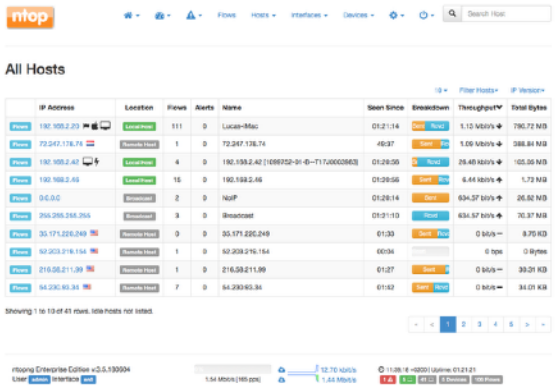
SharkFest '18 US

Packet Monitoring in the IoT and Cloud Days

Luca Deri <deri@ntop.org>
@lucaderi

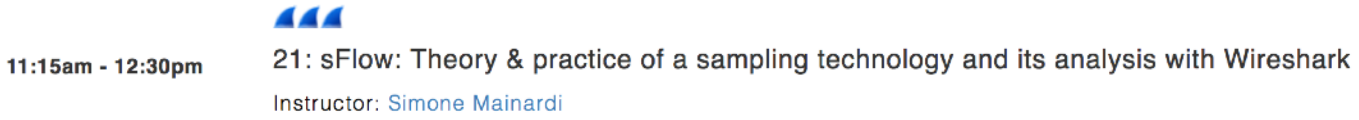
About Me

- (1997) Founder of the ntop.org project with purpose of creating a simple, and open source web-based traffic monitoring application.
- Lecturer at the University of Pisa, Italy.



ntop and Wireshark

- ntop contributed to wireshark in various components such as the NetFlow dissector, and high-speed packet filtering extcap modules (see Sharkfest Restrospective).
- Recently we have contributed with a Lua-based sFlow collector presented yesterday at sf18us.



Packet Traces

- This talk is a tutorial about networking focusing mostly on cloud and IoT.

- You can find packet traces of the various topics at: http://luca.ntop.org/Sharkfest2018/

Part 1:
(Tutorial on) Network and Traffic Trends

Motivation

- Networks have changed significantly in the past decade due to many advances in computing:
  - Protocols (peer to peer).
  - CDN (Content Delivery Networks) and Cloud Computing.
  - User (from PC to smartphones).

- These have been major changes that had an impact on traffic and thus on our daily activities.

Network Protocols [1/11]

- When the Internet was created each service had its own custom protocol designed to serve at best the needs of a specific application.
  - Email: SMTP, POP3, IMAP…
  - Name Resolution: DNS
  - Host Connectivity: telnet, SSH
  - Time: time, ntp…
  - VoIP: SIP, H.323…

Network Protocols [2/11]

```
+OK Hello there.
USER [redacted]
+OK Password required.
PASS [redacted]
+OK logged in.
STAT
+OK 7 32932
LIST
+OK POP3 clients that break here, they violate STD53.
1 5826
2 4602
3 7521
4 2587
5 4616
6 3335
7 4445
.
UIDL 1
+OK 1 UID146-1145365523
UIDL
+OK
1 UID146-1145365523
2 UID147-1145365523
3 UID148-1145365523
4 UID149-1145365523
5 UID150-1145365523
6 UID151-1145365523
7 UID152-1145365523
.
RETR 6
+OK 3335 octets follow.
Return-Path: <emailbusiness@email.it>
Delivered-To: emailbusiness@email.it
Received: from localhost (smtp-in06.email.it [127.0.0.1])
          by smtp-in06.email.it (Postfix) with ESMTP id 2DB4944008;
          Thu, 26 Oct 2006 01:07:00 +0200 (CEST)
X-Virus-Scanned: amavisd-new at email.it
Received: from smtp-in06.email.it ([127.0.0.1])
          by localhost (smtp-in06.email.it [127.0.0.1]) (amavisd-new, port 10024)
          with LMTP id J82mP03yfNBW; Thu, 26 Oct 2006 01:06:59 +0200 (CEST)
Received: from localhost.localdomain (unknown [80.247.77.99])
          by smtp-in06.email.it (Postfix) with ESMTP id 229DE4400C;
          Thu, 26 Oct 2006 01:06:59 +0200 (CEST)
Date: Thu, 26 Oct 2006 01:07:15 +0200
From: emailbusiness@email.it
Subject: Ponti in Beauty Farm da 156 euro!
Mime-Version: 1.0
Content-Type: multipart/alternative; boundary=ABCD
Message-Id: <20061025230659.229DE4400C@smtp-in06.email.it>
To: undisclosed-recipients:;
```

POP3

```
....INVITE sip:0239777289@sip.messagenet.it SIP/2.0
Via: SIP/2.0/udp 81.116.18.30:5060;branch=z9hG4bK816A42BEFF629368D009F9814DD16
Route: <sip:sip.messagenet.it:5061;lr>
From: <sip:5319921@sip.messagenet.it>;tag=C881DF084C6CE08915B3DC41EFFC3
To: <sip:0239777289@sip.messagenet.it>
Call-ID: 2C2C591F0B4E77E8FD433C24A7D37@81.116.18.30
CSeq: 7 INVITE
Contact: <sip:5319921@81.116.18.30;uniq=6C8E2C86C13E942742D9C4DB95BDF>
Max-Forwards: 70
Expires: 120
User-Agent: AVM FRITZ!Box Fon ata 1020 11.04.01 (Jan 25 2006)
Supported: 100rel, replaces
Allow-Events: telephone-event, refer
Allow: INVITE, ACK, OPTIONS, CANCEL, BYE, UPDATE, PRACK, INFO, SUBSCRIBE, NOTIFY, REFER, MESSAGE
Content-Type: application/sdp
Accept: application/sdp, multipart/mixed
Accept-Encoding: identity
Content-Length:   380

v=0
o=user 10296005 10296005 IN IP4 81.116.18.30
s=call
c=IN IP4 81.116.18.30
t=1157359145 1157362745
m=audio 7078 RTP/AVP 8 0 2 102 100 99 97 18 101
a=sendrecv
a=rtpmap:2 G726-32/8000
a=rtpmap:102 G726-32/8000
a=rtpmap:100 G726-40/8000
a=rtpmap:99 G726-24/8000
a=rtpmap:97 iLBC/8000
a=fmtp:97 mode=30
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-11
a=rtcp:7079
INVITE sip:0239777289@sip.messagenet.it SIP/2.0
Via: SIP/2.0/udp 81.116.18.30:5060;branch=z9hG4bK816A42BEFF629368D009F9814DD16
```

SIP

Network Protocols [3/11]

- All protocols were in clear text, and only later they have been replaced with an encrypted/ secure version. Two options:
  - Extend existing protocols: pop->pops
  - Encapsulation on a secure channel: telnet->SSH.

Network Protocols [4/11]

- Binary protocols such as Radius/DHCP were not that popular.
- Instead it was privileged portability across systems and CPU types, instead of ad-hoc compression/ encoding.
- The ASN.1 (Abstract Syntax Notation 1) is still serving the needs of data serialisation and portability: SNMP and 3G/UMTS, 4G/LTE use it.

Network Protocols [5/11]

- This model worked for a while until HTTP was created.
- HTTP stands for HyperText Transfer Protocol and it was initially designed for transferring hypertext (HTML, images….) but it has been transformed into a protocol used for mostly everything.
- One of reasons behind this success is that firewall/ proxy/etc allow it to flow through them: why look for trouble with a custom protocol if there is HTTP?

Network Protocols [6/11]

- The jeopardisation is not over, in particular with the upcoming HTTP/2.0….

DNS over HTTPS

From Wikipedia, the free encyclopedia

DNS over HTTPS (**DoH**) is an experimental protocol for performing remote Domain Name System (DNS) resolution via the HTTPS protocol. The goal of the method is to increase user privacy and security by preventing eavesdropping and manipulation of DNS data by man-in-the-middle attacks.[1] As of March 2018, Google and the Mozilla Foundation are testing versions of DNS over HTTPS.[2][3]

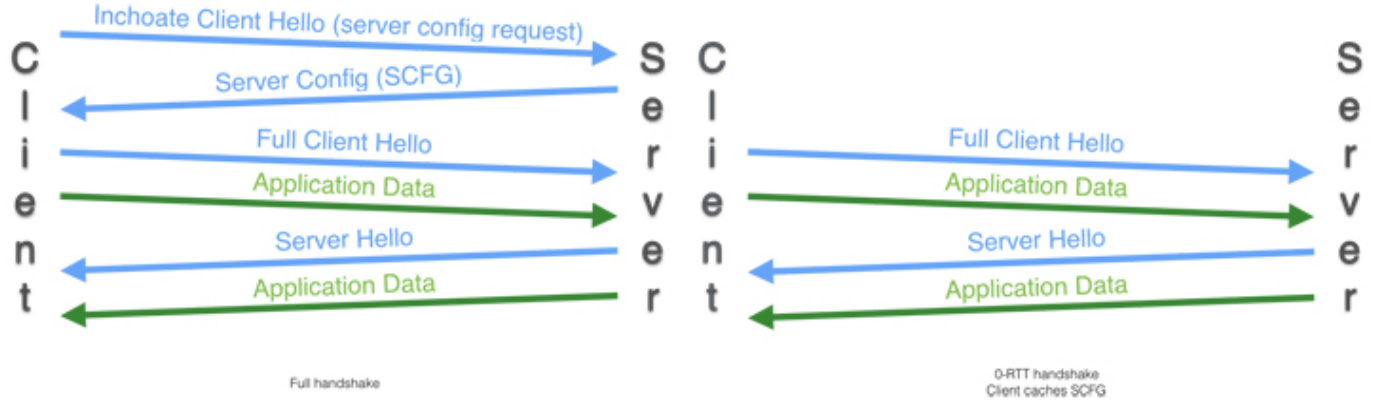
Network Protocols [7/11]

- The widespread “misuse” of HTTP has implications in traffic analysis as it makes it challenging to figure out what is the “real” protocol transported via HTTP(S), and what are the interactions between two peers.
- Today Netflix, Amazon Video, or your accounting software use HTTP(S) to transport video or data. It is the new TCP/IP in essence.

Network Protocols [8/11]

With some exceptions… (FaceBook Zero)

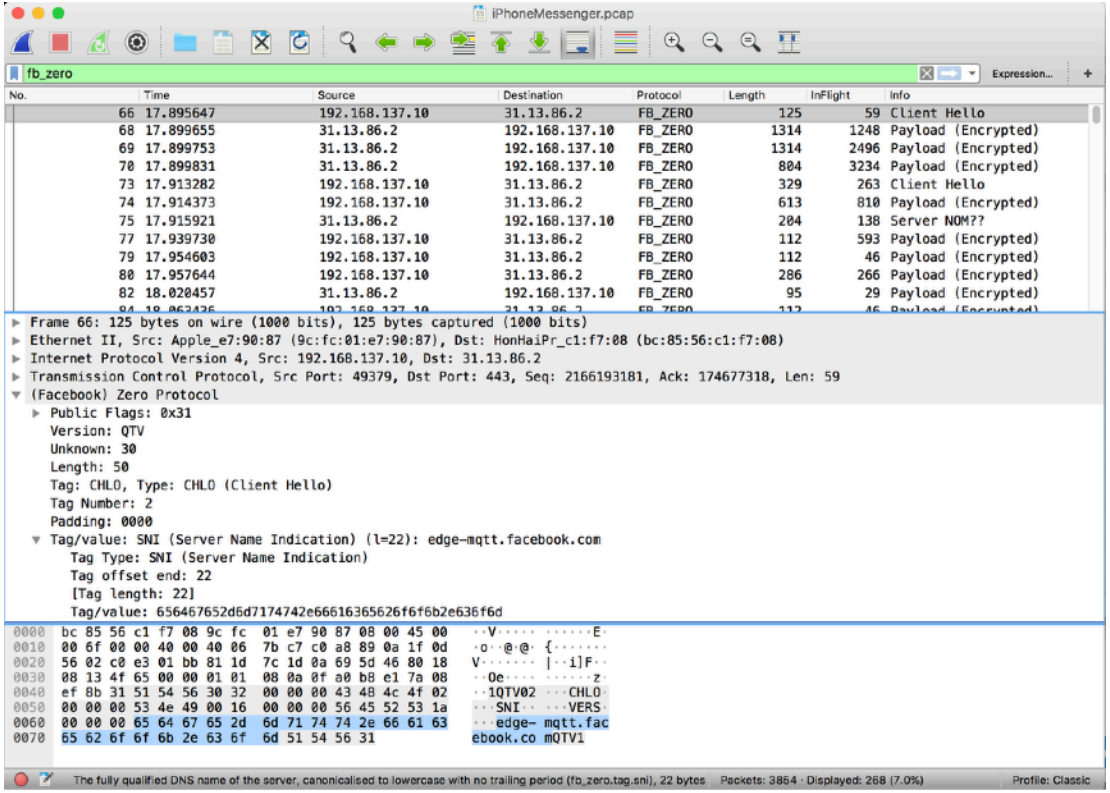
- TCP over port 443 (SSL)
- QUIC Derivative
- Performance improvement over TLS1.2
- Used in iOS and Android Facebook Messenger apps (but not on the browser version)



https://code.facebook.com/posts/608854979307125/building-zero-protocol-for-fast-secure-mobile-connections/
https://code.facebook.com/posts/557147474482256/this-browser-tweak-saved-60-of-requests-to-facebook/

Network Protocols [9/11]

With some exceptions…

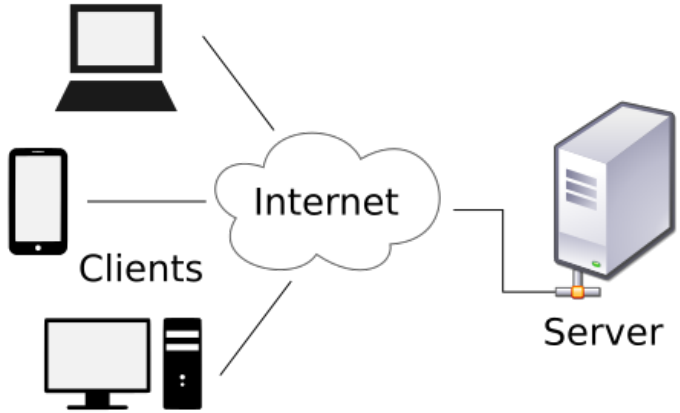


Note: Wireshark 2.6+

Network Protocols [10/11]

- Internet protocols have been originally designed on two main paradigms:
  - Store and forward (e.g. email): information is not delivered directly but through an intermediate station.
  - Client-Server: the server usually operates as a centralised system that serves multiple clients. Communications can be direct or decentralised based on the peer-to-peer paradigm.

Network Protocols [11/11]



- Direct communications.
- Easy to monitor (ip.src==xxx).

Source: Wikipedia

- Mix: direct and peer-communications depending on the IP address (NAT prevents some communications patterns).
- Difficult to track communications end-to-end (Wireshark filters help partially).
- More peers other than the client and server (many IPs make packet traces difficult to understand).
- Custom data encryption (no SSL)

Cloud and CDN [1/19]

- The advent of cloud computing and CDN (Content Delivery Network), contributed to create dynamic decentralised architectures whose topology, number of peers and their IP address can change overtime based on current usage needs.
- From a business perspective this has shifted the focus from hardware/software to services that are often rented based on the current needs.

Cloud and CDN [2/19]

- From a traffic analysis perspective:
  - Cloud services often use application/network balancers: not simple to predict where your traffic will flow.
  - Nodes can serve multiple customers: filters on IP addresses won't necessarily restrict the traffic to the right target.
  - If you want to monitor cloud components traffic you are often forced to move monitoring tools to the cloud.
  - If you want to monitor customer access to cloud-based services, you need to sit at the customer premises in order to impersonate that real user experience.

Cloud and CDN [3/19]

- Using cloud services also means that IP addresses are no longer relevant, in particular when leveraging on large providers such as Amazon or Google. The (cloud) server:
  - Based on your network/location/service load you access a different server pool.
  - Symbolic name might be the same but associated to different IP addresses, or names.
    - Corollary: IP address is not persistent.
    - Sub-Corollary: Wireshark filtering is more complex than "ip.addr==www.facebook.com"

Cloud and CDN [4/19]

```
deri@ntop-digitaocean 204> host www.facebook.com
www.facebook.com is an alias for star-mini.c10r.facebook.com.
star-mini.c10r.facebook.com has address 31.13.64.35
star-mini.c10r.facebook.com has IPv6 address 2a03:2880:f106:83:face:b00c:0:25de
deri@ntop-digitaocean 205> traceroute www.facebook.com
traceroute to www.facebook.com (31.13.64.35), 30 hops max, 60 byte packets
 1  128.199.32.254 (128.199.32.254)  1.216 ms  1.186 ms  1.183 ms
 2  138.197.250.102 (138.197.250.102)  0.964 ms 138.197.250.98 (138.197.250.98)  0.971 ms 138.197.250.80 (138.197.250.80)  0.990 ms
 3  ae37.pr02.ams2.tfbnw.net (157.240.67.244)  2.140 ms  0.903 ms ae37.pr01.ams2.tfbnw.net (157.240.67.242)  0.865 ms
 4  po111.asw01.ams3.tfbnw.net (157.240.35.54)  1.050 ms po121.asw02.ams3.tfbnw.net (157.240.35.58)  1.039 ms po111.asw01.ams2.tfbnw.net
(31.13.31.36)  1.275 ms
 5  po241.psw02.ams2.tfbnw.net (157.240.35.181)  1.257 ms po212.psw01.ams2.tfbnw.net (157.240.32.13)  0.926 ms po231.psw01.ams2.tfbnw.net
(157.240.35.163)  1.084 ms
 6  173.252.67.1 (173.252.67.1)  1.180 ms 173.252.67.173 (173.252.67.173)  0.668 ms 173.252.67.3 (173.252.67.3)  1.085 ms
 7  edge-star-mini-shv-01-amt2.facebook.com (31.13.64.35)  0.879 ms  0.865 ms  0.847 ms
deri@ntop-digitaocean 206> ping6 www.facebook.com
PING www.facebook.com(edge-star-mini6-shv-01-ams3.facebook.com (2a03:2880:f11b:83:face:b00c:0:25de)) 56 data bytes
64 bytes from edge-star-mini6-shv-01-ams3.facebook.com (2a03:2880:f11b:83:face:b00c:0:25de): icmp_seq=1 ttl=58 time=1.23 ms
64 bytes from edge-star-mini6-shv-01-ams3.facebook.com (2a03:2880:f11b:83:face:b00c:0:25de): icmp_seq=2 ttl=58 time=0.939 ms
64 bytes from edge-star-mini6-shv-01-ams3.facebook.com (2a03:2880:f11b:83:face:b00c:0:25de): icmp_seq=3 ttl=58 time=0.635 ms
^C
--- www.facebook.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.635/0.935/1.232/0.245 ms
deri@ntop-digitaocean 207> ping -4 www.facebook.com
PING star-mini.c10r.facebook.com (31.13.91.36) 56(84) bytes of data.
64 bytes from edge-star-mini-shv-01-ams3.facebook.com (31.13.91.36): icmp_seq=1 ttl=58 time=1.03 ms
64 bytes from edge-star-mini-shv-01-ams3.facebook.com (31.13.91.36): icmp_seq=2 ttl=58 time=0.668 ms
^C
--- star-mini.c10r.facebook.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.668/0.853/1.039/0.187 ms
```

1/3

Cloud and CDN [5/19]

```
deri@Lucas-MacBookPro.local 201> host www.facebook.com
www.facebook.com is an alias for star-mini.c10r.facebook.com.
star-mini.c10r.facebook.com has address 31.13.86.36
star-mini.c10r.facebook.com has IPv6 address 2a03:2880:f108:83:face:b00c::25de
deri@Lucas-MacBookPro.local 202> ping 31.13.86.36
PING 31.13.86.36 (31.13.86.36): 56 data bytes
64 bytes from 31.13.86.36: icmp_seq=0 ttl=51 time=78.956 ms
64 bytes from 31.13.86.36: icmp_seq=1 ttl=51 time=66.536 ms
^C
--- 31.13.86.36 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 66.536/72.746/78.956/6.210 ms
deri@Lucas-MacBookPro.local 203> traceroute  www.facebook.com
traceroute to star-mini.c10r.facebook.com (31.13.86.36), 64 hops max, 52 byte packets
 1  172.20.10.1 (172.20.10.1)  1.209 ms  0.598 ms  0.455 ms
 2  * * *
 3  10.133.16.37 (10.133.16.37)  68.925 ms  26.025 ms  33.354 ms
 4  10.133.16.14 (10.133.16.14)  24.278 ms  23.648 ms  25.263 ms
 5  10.133.16.236 (10.133.16.236)  24.370 ms  26.927 ms  24.421 ms
^C
```

2/3

Cloud and CDN [6/19]

```
deri@builder 201> host www.facebook.com
www.facebook.com is an alias for star-mini.c10r.facebook.com.
star-mini.c10r.facebook.com has address 31.13.86.36
star-mini.c10r.facebook.com has IPv6 address 2a03:2880:f108:83:face:b00c:0:25de
deri@builder 202> ping  31.13.86.36
PING 31.13.86.36 (31.13.86.36) 56(84) bytes of data.
64 bytes from 31.13.86.36: icmp_seq=1 ttl=55 time=5.98 ms
64 bytes from 31.13.86.36: icmp_seq=2 ttl=55 time=6.02 ms
^C
--- 31.13.86.36 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 5.986/6.006/6.027/0.080 ms
deri@builder 203> traceroute  www.facebook.com
traceroute to www.facebook.com (31.13.86.36), 30 hops max, 60 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
```

3/3

Cloud and CDN [7/19]

- In essence
  - Same symbolic and numeric IP (in this case Wireshark filtering will still work)
  - Different server(s) locations (traceroute)
  - Different latencies
    - < 1 msec ← How is this possible?
    - ~ 60 msec

Cloud and CDN [8/19]

Gerald Combs
@geraldcombs

Follow

My #Wireshark #Lua skills were getting rusty so I wrote a postdissector that adds distance fields based on frame.time_delta_displayed.

gist.github.com/geraldcombs/d3...

No.	Time	Prev Δ	Cat 6 km	Length	Source
1	0.000000	0.000000000	0	1454	200.121.1.13
2	0.000011	0.000011000	2.14351	54	172.16.0.122
3	0.025738	0.025727000	5013.29	1454	200.121.1.13
4	0.025749	0.000011000	2.14351	54	172.16.0.122
5	0.076967	0.051218000	9980.58	1454	200.121.1.13
6	0.076978	0.000011000	2.14351	54	172.16.0.122
7	0.102939	0.025961000	5058.89	1454	200.121.1.13
8	0.102946	0.000007000	1.36405	54	172.16.0.122
9	0.128285	0.025339000	4937.68	1454	200.121.1.13
10	0.128319	0.000034000	6.6254	54	172.16.0.122
11	0.154162	0.025843000	5035.89	1454	200.121.1.13
12	0.154169	0.000007000	1.36405	54	172.16.0.122

6:44 PM - 11 Apr 2018

geraldcombs / **delta_distance.lua**

Created a month ago • Report gist

<> Code | Revisions 1 | ★ Stars 2 | Embed ▾ | <script

Wireshark Lua postdissector that converts frame.time_delta_displayed to distance values.

delta_distance.lua

```
1  -- delta_distance.lua
2  -- Add delta_distance.{copper,fiber}.{km,mi} fields
3  -- By Gerald Combs <gerald@wireshark.org>
4  -- Modified from https://wiki.wireshark.org/Lua/Examples/PostDissector
5  -- My Wireshark Lua skills were getting rusty so I wrote this. There are
6  -- probably mistakes.
7
8  -- Add a delta_distance protocol
9  local delta_distance_p = Proto("delta_distance", "Frame displayed delta distance")
10
11 -- Add our fields
12 local dd_cat6_km_field = ProtoField.float("delta_distance.cat6.km", "Cat 6 km")
13 local dd_cat6_mi_field = ProtoField.float("delta_distance.cat6.mi", "Cat 6 mi")
14 local dd_fiber_km_field = ProtoField.float("delta_distance.fiber.km", "Fiber km")
15 local dd_fiber_mi_field = ProtoField.float("delta_distance.fiber.mi", "Fiber mi")
```

Cloud and CDN [9/19]

Velocity factor

From Wikipedia, the free encyclopedia

The **velocity factor** (**VF**),[1] also called **wave propagation speed** or **velocity of propagation** (**VoP** or v_P),[2] of a transmission medium is the ratio of the speed at which a wavefront (of an electromagnetic signal, a radio signal, a light pulse in an optical fibre or a change of the electrical voltage on a copper wire) passes through the medium, to the speed of light in a vacuum. For optical signals, the velocity factor is the reciprocal of the refractive index.

The speed of radio signals in a vacuum, for example, is the speed of light, and so the velocity factor of a radio wave in a vacuum is unity, or 100%. In electrical cables, the velocity factor mainly depends on the insulating material (see table below).

The use of the terms *velocity of propagation* and *wave propagation speed* to mean a ratio of speeds is confined to the computer networking and cable industries. In a general science and engineering context, these terms would be understood to mean a true speed or velocity in units of distance per time,[3] while *velocity factor* is used for the ratio.

Contents [hide]

~300k KM/s - ~190k Miles/s

https://en.wikipedia.org/wiki/Velocity_factor

Cloud and CDN [10/19]

Minimum velocity factors for network cables

VF (%)	Cable	Ethernet physical layer
74–79	Cat-7 twisted pair	
77	RG-8/U	Minimum for 10BASE5[4]
67	Optical fiber	Minimum for 10BASE-FL,[5] 100BASE-FX, ...
65	RG-58A/U	Minimum for 10BASE2[6]
65	Cat-6A twisted pair	10GBASE-T
64	Cat-5e twisted pair	100BASE-TX, 1000BASE-T
58.5	Cat-3 twisted pair	Minimum for 10BASE-T[7]

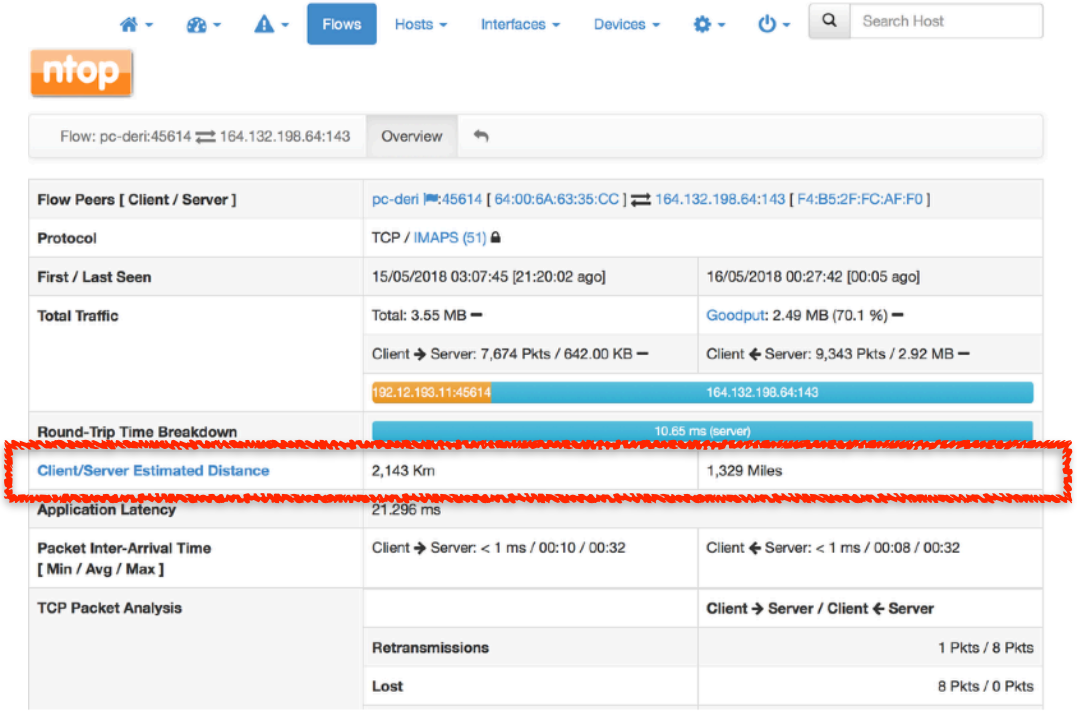
- Note: this is the pure network speed based on propagation. Add latency due to packet processing, queueing… to compute realistic distances. Typical RTT:
  - LAN: < 5 msec
  - Continent: < 25 msec
  - Across Atlantic: 100+ msec

Cloud and CDN [11/19]

```
function formatValue(amount)
   local formatted = amount

   if(formatted == nil) then return(0) end
   while true do
      formatted, k = string.gsub(formatted, "^(-?%d+)(%d%d%d)", '%1,%2')
      if(k==0) then
        break
      end
   end
   return formatted
end

function distance(label, delta_t)
   local c_vacuum_km_s = 299792
   local c_vacuum_mi_s = 186000
   local fiber_vf      = .67
   local dd_fiber_km
   local dd_fiber_mi

   delta_t = delta_t / 1000 -- msec -> sec

   dd_fiber_km   = delta_t * c_vacuum_km_s * fiber_vf
   dd_fiber_mi   = delta_t * c_vacuum_mi_s * fiber_vf

   print("\t"..label..": "..formatValue(dd_fiber_km).." Km / "..formatValue(dd_fiber_mi).." Miles ["..delta_t.." sec]")
end

print("Distance to www.facebook.com")
distance("Wind IT", 0.935)
distance("DigitalOcean", 1.232)
distance("Vodafone 3G", 78.956)
```

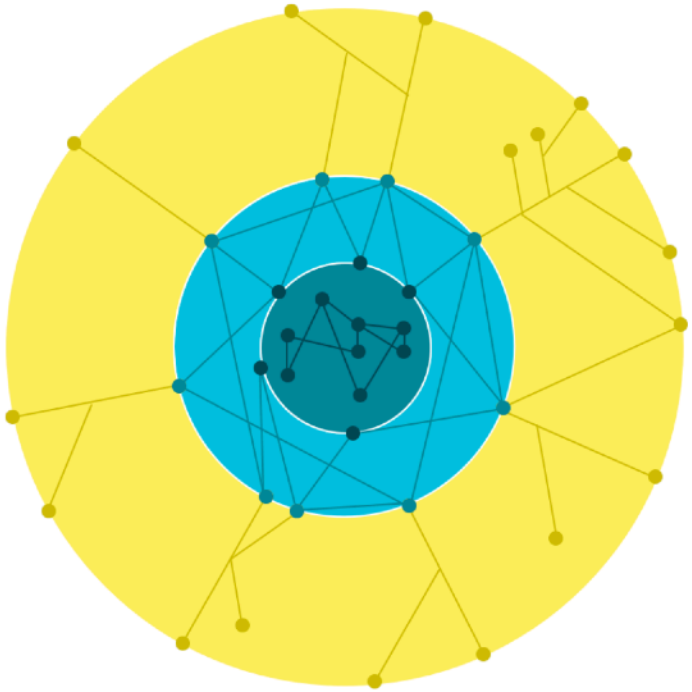
```
deri@Lucas-MacBookPro.local 235> lua distance.lua
Distance to www.facebook.com
    Wind IT: 187.8046984 Km / 116.5197 Miles [0.000935 sec]
    DigitalOcean: 247.46030848 Km / 153.53184 Miles [0.001232 sec]
    Vodafone 3G: 15,859.15269184 Km / 9,839.49672 Miles [0.078956 sec]
```

Cloud and CDN [12/19]



https://github.com/ntop/ntopng

Cloud and CDN [13/19]



Google aims to deliver its services with high performance, high reliability, and low latency for users, in a manner that respects open internet principles.

We have invested in network infrastructure that is aligned with this goal and that also allows us to work with network operators to exchange traffic efficiently and cost-effectively.

Google's network infrastructure has three distinct elements:

- Core data centers
- Edge Points of Presence (PoPs)
- Edge caching and services nodes (Google Global Cache, or GGC)

Source: https://peering.google.com/

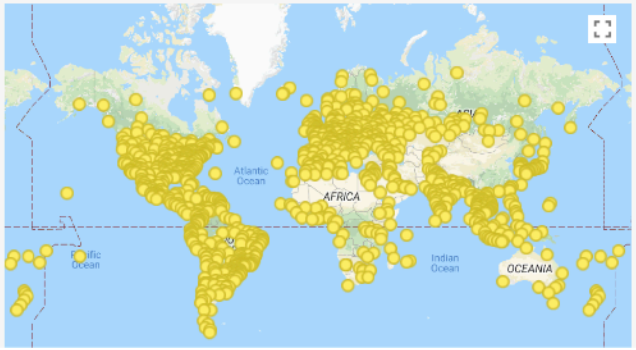
Cloud and CDN [14/19]

Edge nodes (Google Global Cache, or GGC)

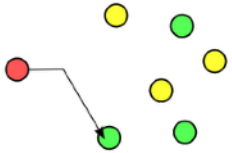
Our edge nodes (called Google Global Cache, or GGC) represent the tier of Google's infrastructure closest to our users. With our edge nodes, network operators and internet service providers deploy Google-supplied servers inside their network.

Static content that is very popular with the local host's user base, including YouTube and Google Play, is temporarily cached on edge nodes. Google's traffic management systems direct user requests to an edge node that will provide the best experience.

In some locations, we also use our edge nodes to support the delivery of other Google services, such as Google Search, by proxying traffic where it will deliver improved end-to-end performance for the end user.



Cloud and CDN [15/19]



- Anycast is a popular addressing and routing technology pioneered in DNS, that provides multiple route paths to two or more destinations.
- In essence the principle that (public) IP addresses are unique (i.e. each server must have a unique IP) is gone, as it is now possible to have IP address 1.2.3.4 multiple times on the Internet.

Cloud and CDN [16/19]

- Through anycast it is now possible to
  - Announce the same IP network multiple times (reliability through replication).
  - Let routing protocols select the desired path on the basis of number of hops, distance, lowest cost, latency measurements or least congested route.

Cloud and CDN [17/19]

- CDNs heavily use anycast routing to bring (static) content close to their users.
- This on a reliable fashion as:
  - If the best node is unreachable (e.g. due to maintenance) another node can be used.
  - DDoS attacks will affect only regional servers as routing will protect “sub-optimal” routes

Cloud and CDN [18/19]

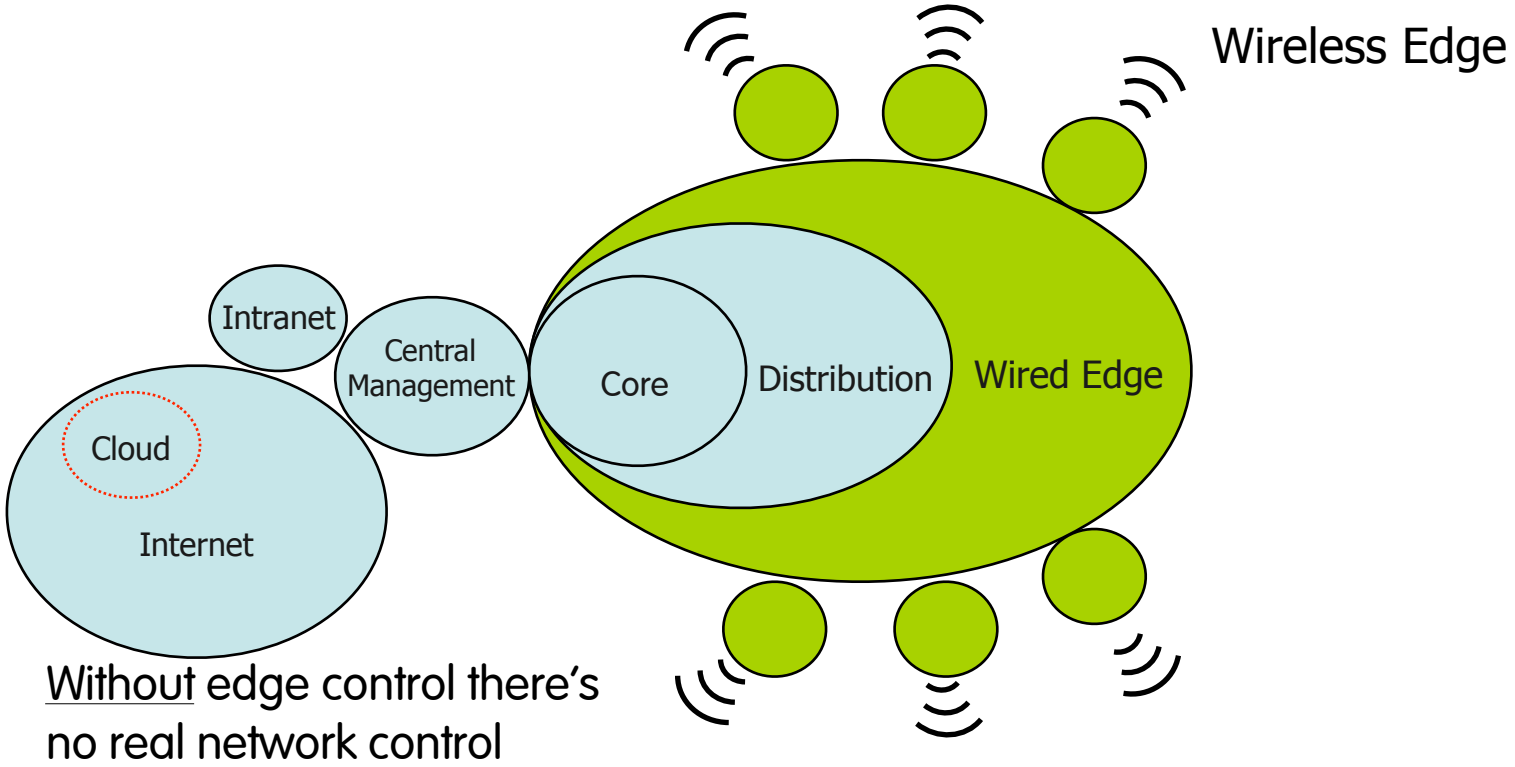
- In summary cloud and CDNs make traffic analysis a bit more challenging.
  - The same numeric IP might be on different locations (one IP one host no longer holds).
  - Latency is crucial: providers place nodes as close as possible to users but this deceives consolidated technologies such as geo-location.
  - Packet-based analysis must be aware of all this, as service transparency and data caching might make troubleshooting more tricky.

Cloud and CDN [19/19]

Packet analysis with CDNs and cloud-based services is not special but:

- You need to be able to interpret the results Wireshark will report you (including geo-location).
- During a troubleshooting session be ready to see the same service provided by different servers so adapt your filtering rules as necessary.

Networks Have Changed [1/2]



Without edge control there's no real network control

Networks Have Changed [2/2]

Traffic analysis implications:

- Packet capture location might be challenging with mobile users. If you analyse:
  - Internet traffic: being close to the gateway will be enough.
  - LAN traffic: the gateway will be too far away, in particular if you want to inspect traffic for security purposes. Being closed to the edge might help.

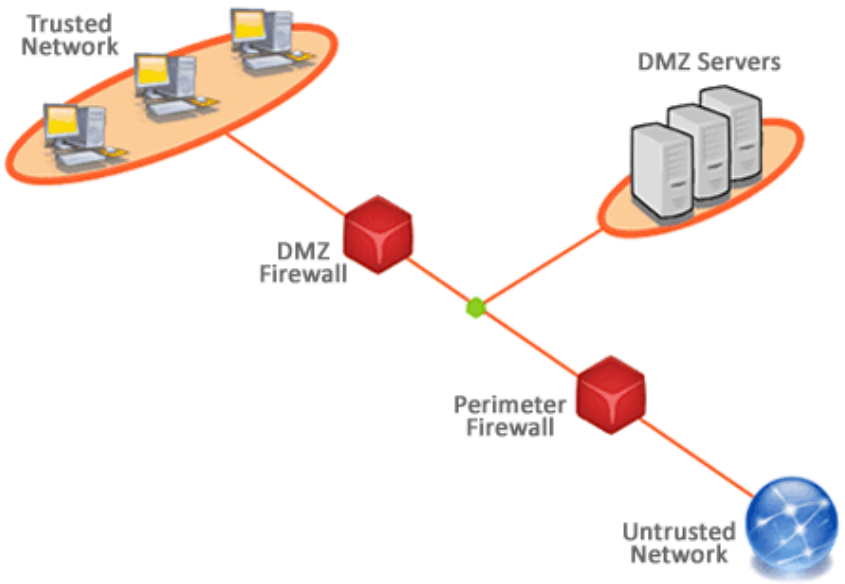
A Middle Age Approach

- For years security was tackled with as a middle age problem:
  - Bad guys are outside of my network
  - Good guys are in
  - If I have an internal service to expose to the Internet I need to place it on a DMZ where the firewall can enforce selected traffic policies
- This approach was good until devices/users where easy to partition in groups but with the advent of BYOD (Bring Your Own Device), IoT and cloud computing things became more difficult.

A Broken Security Model [1/3]

"Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job." - Jerome Saltzer

- Procedural Security
- Logical Security
- Physical Security



Denning's Least Privilege Principle

A Broken Security Model [2/3]

- The Low-voltage Environment:
  - Wide-spread use of IoT devices.
  - Increasing interconnection between edge devices and corporate networks: an edge device has important topological privileges.
  - Edge devices lack built-in security features: too simple, yes easy to attack or replace with "trojan" devices.
  - Physical location makes networks vulnerable to external attack – even without Internet connection

A Broken Security Model [3/3]

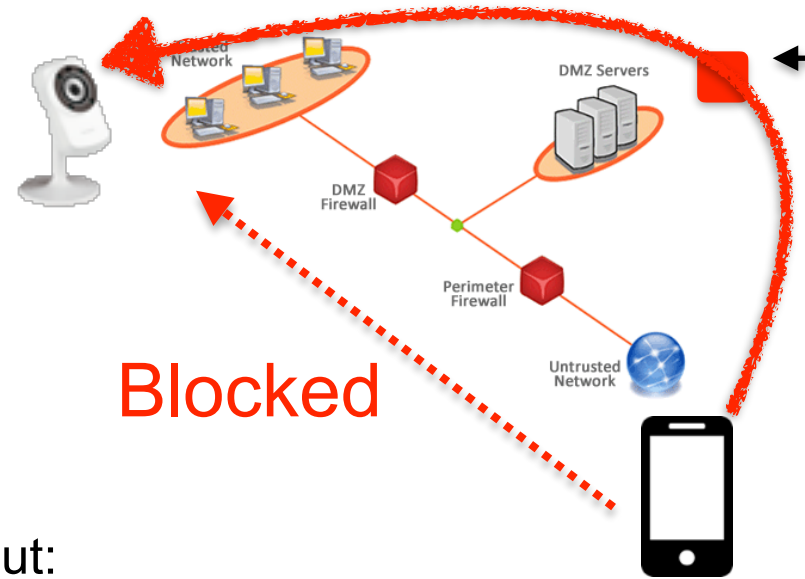
- Unsecured low-voltage devices:
  - Access control
    - Unauthorised opening of gates/doors, false attendance information.
  - Video surveillance cameras
    - Manipulation of video camera streams, unauthorised viewing or disabling video edge-device elements.
  - Building-management/Fire-alarm systems
    - False readings, disabling or blinding.
  - Perimeter IP-based sensors
    - False readings, disabling or blinding.
  - DDoS (Distributed Denial of Service) attacks, can disrupt network operations and thus break a complex system/factory.

Part 2:
Practical Traffic Analysis

Cloud-Managed Devices [1/6]

- The current trend in consumer device is the following:
  - Install the device in the designated network, usually behind a firewall or at least a NAT.
  - Configure the device from the designated network usually connecting to the device through a web browser and/or (optional) a mobile application connected to the WiFi network.
  - Access your device on-the-go using the mobile app.

Cloud-Managed Devices [2/6]



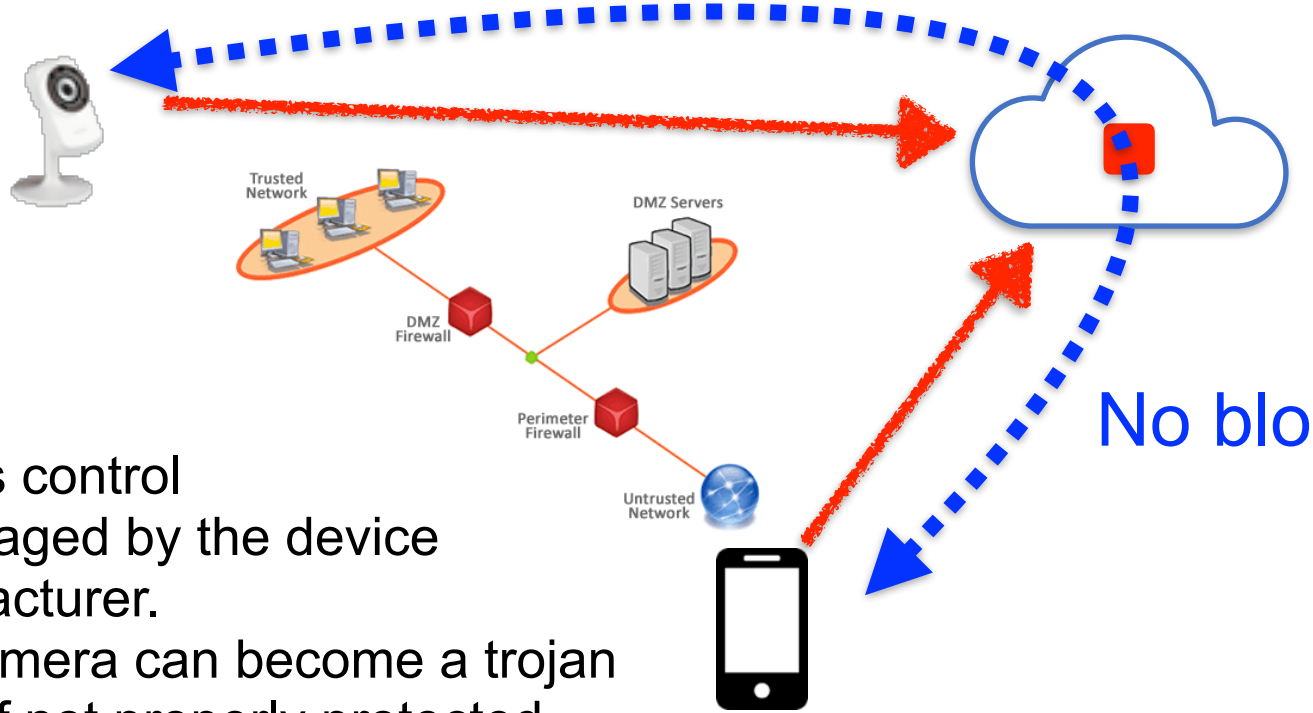
This is where the camera was supposed to be ideally located:

- Open a fixed TCP port
- Use it as a pivot to reach the Internal network

But:

- Most home networks have no DMZ nor static IP
- People do not like to configure anything, just unbox the camera and plug it to electricity

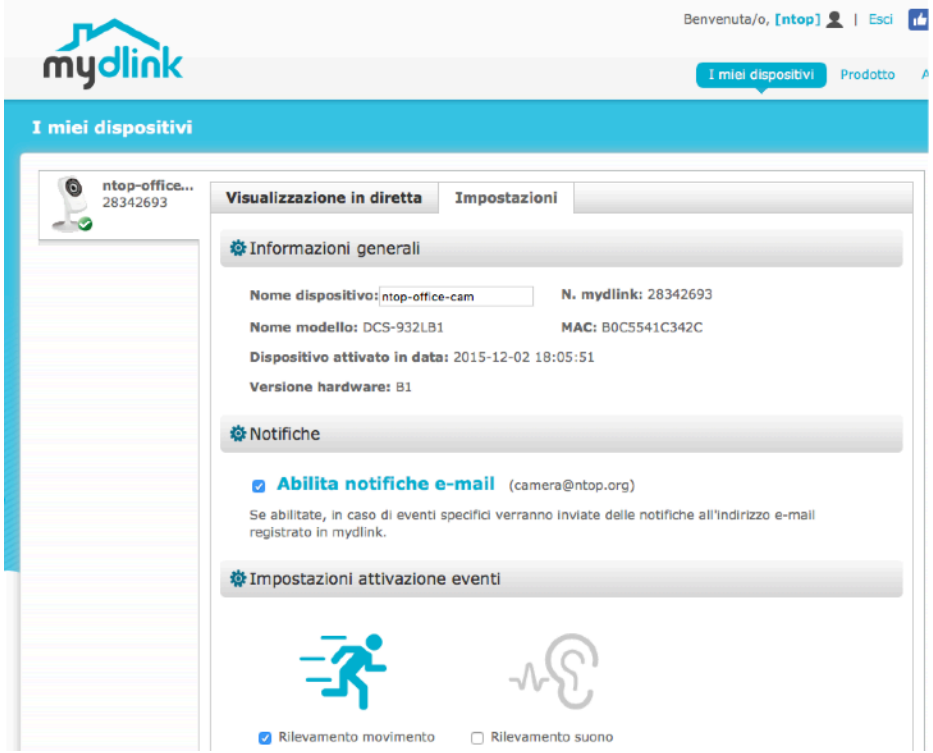
Cloud-Managed Devices [3/6]

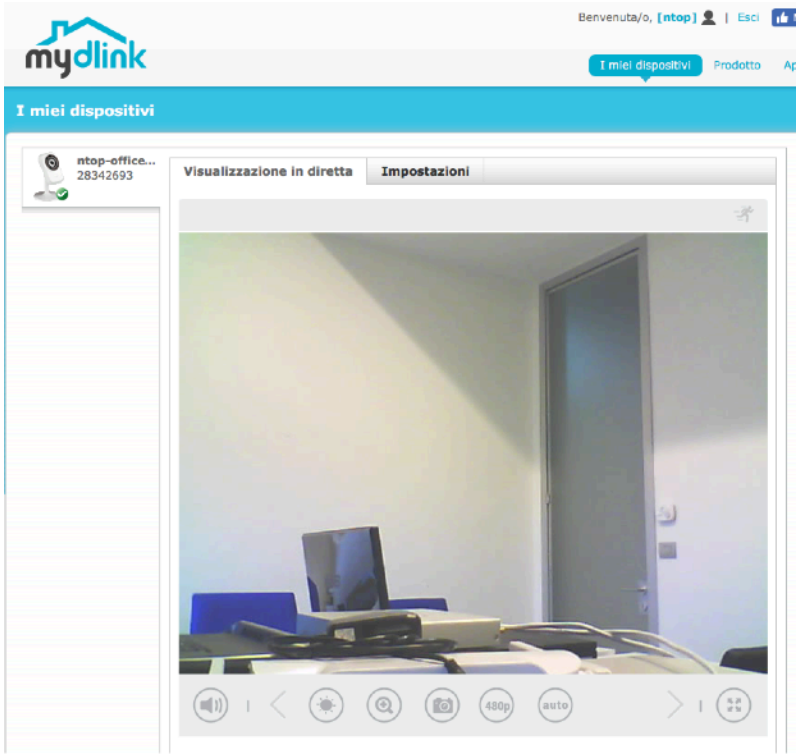


Caveats

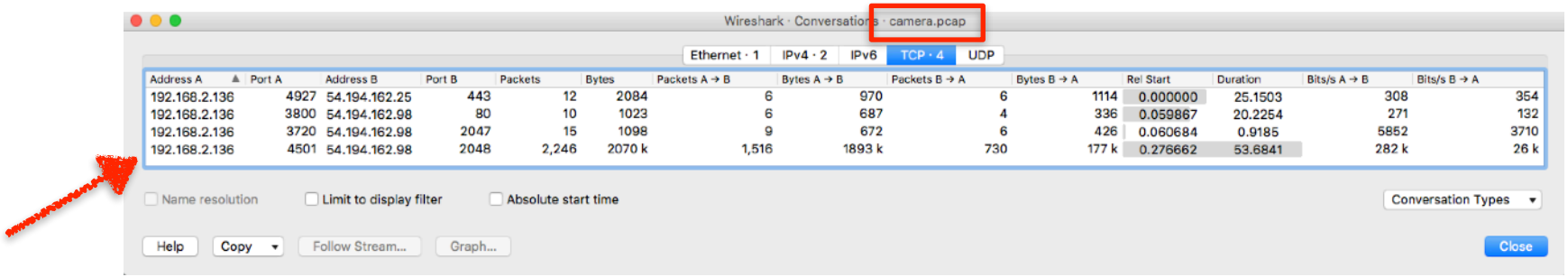
- Access control is managed by the device manufacturer.
- The camera can become a trojan horse if not properly protected.

Cloud-Managed Devices [4/6]





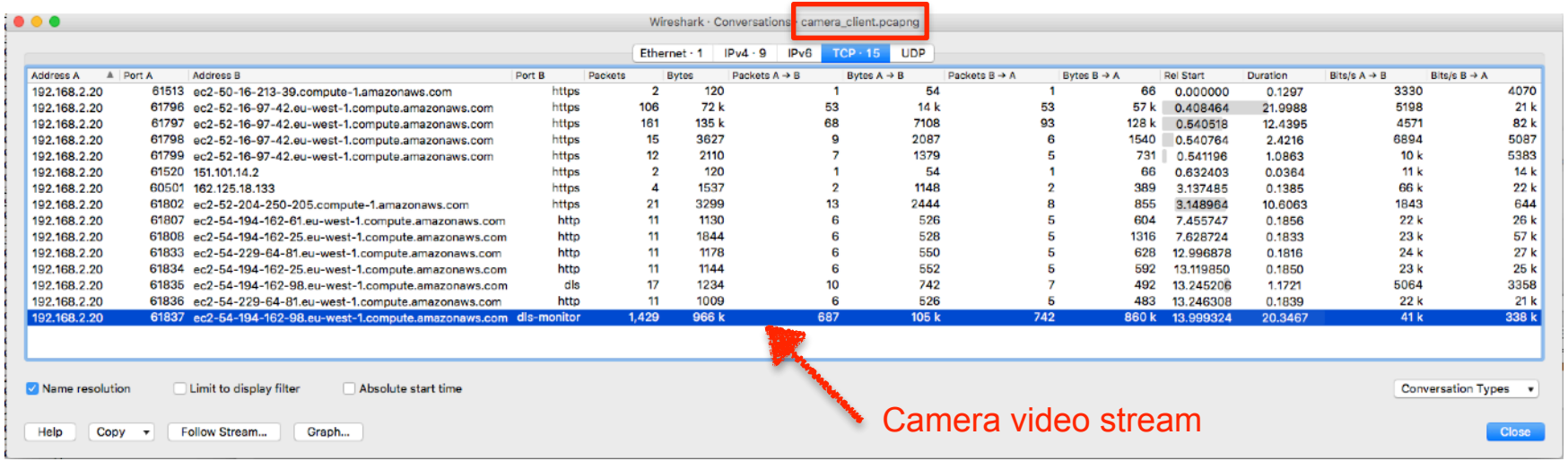
Cloud-Managed Devices [5/6]



Camera view

1. Open a permanent connection camera <-> cloud and wait for commands sent from the cloud
2. Communications are encrypted, local sysadmins cannot pass/deny commands based on stream content

Cloud-Managed Devices [6/6]



Client view

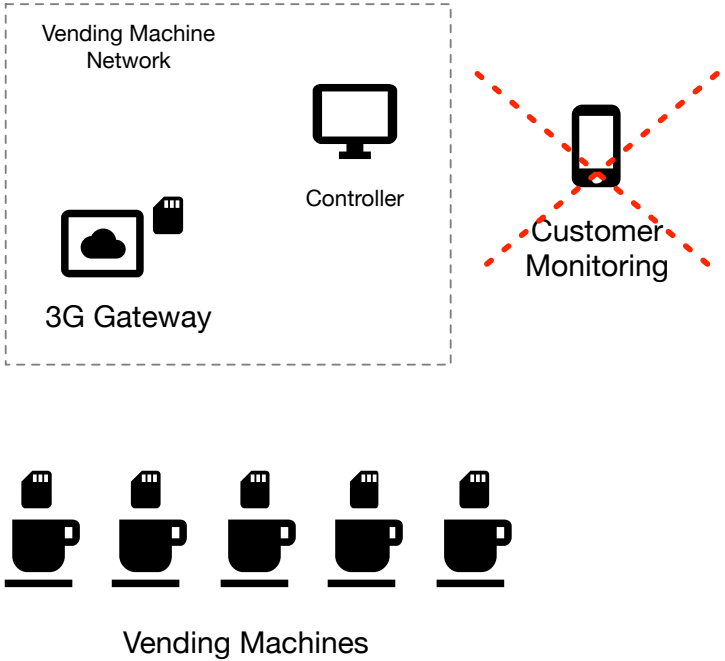
1. The communications camera <-> client do not use the same cloud host for displaying camera info or configuration
2. Camera <-> client talk with the same cloud host only for camera video stream

IoT Devices in Cloud [1/10]

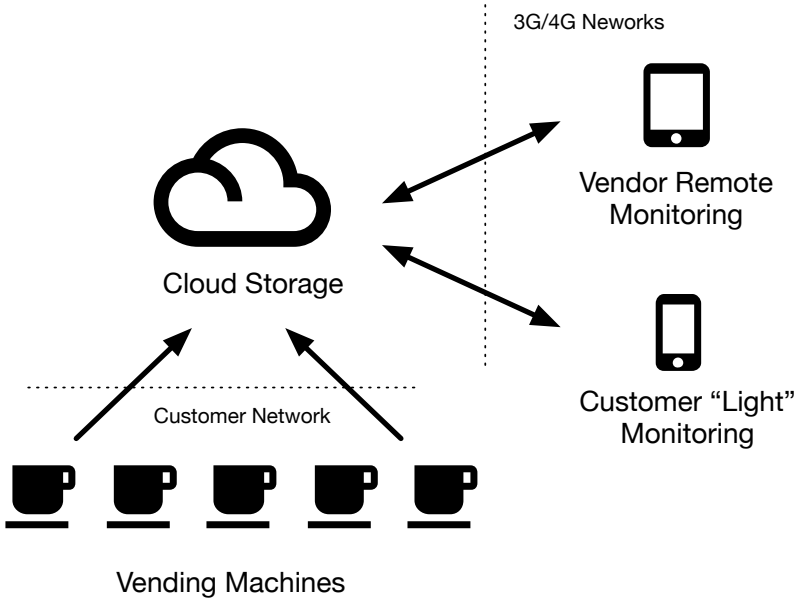
- "Modern" programmers use technologies such as the cloud, Web services, containers pretty extensively as they simplify application development.
- Platforms like Thingspeak for IoT analytics. Assumptions:
  - Devices are all Internet connected (if not a backup 3G connection will be installed).
  - Metrics storage is on the cloud, with no local persistency.
  - All devices interaction is not direct but through cloud-based services.

IoT Devices in Cloud [2/10]

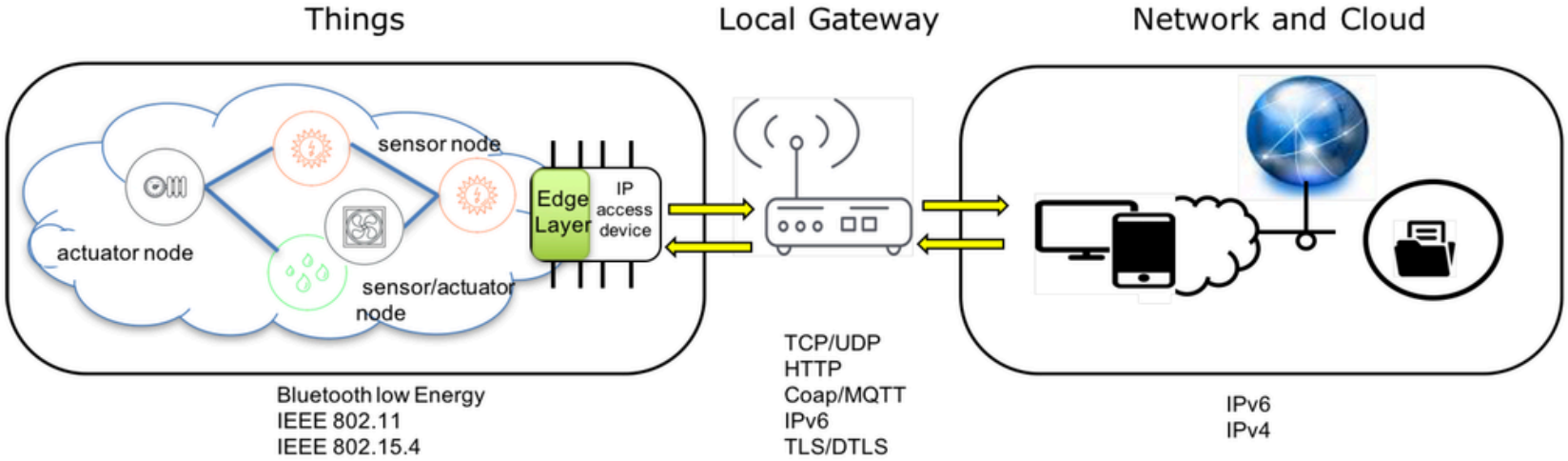
Before the Cloud



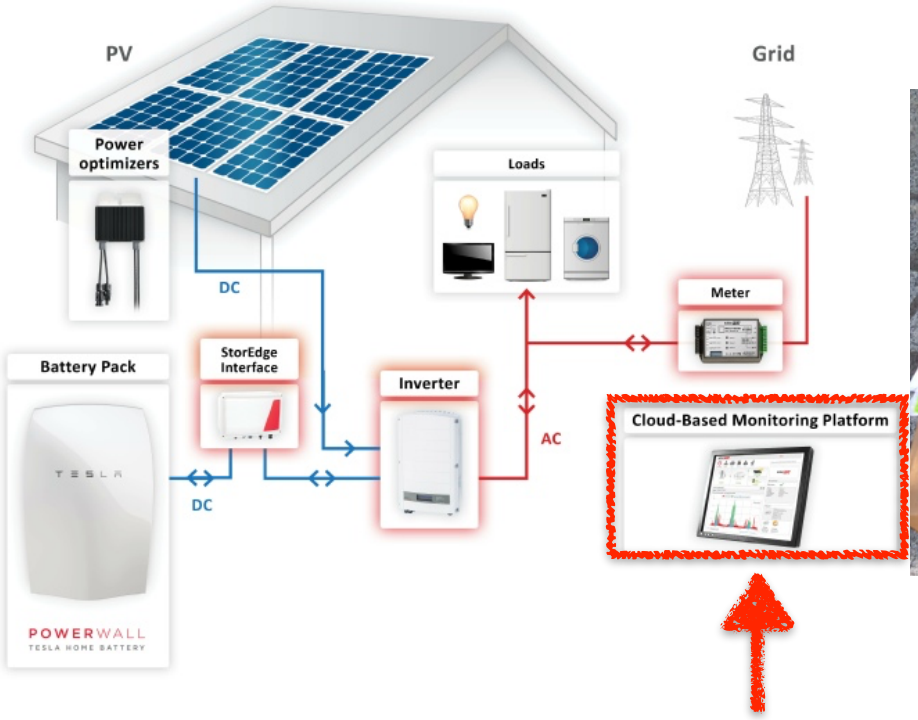
Today



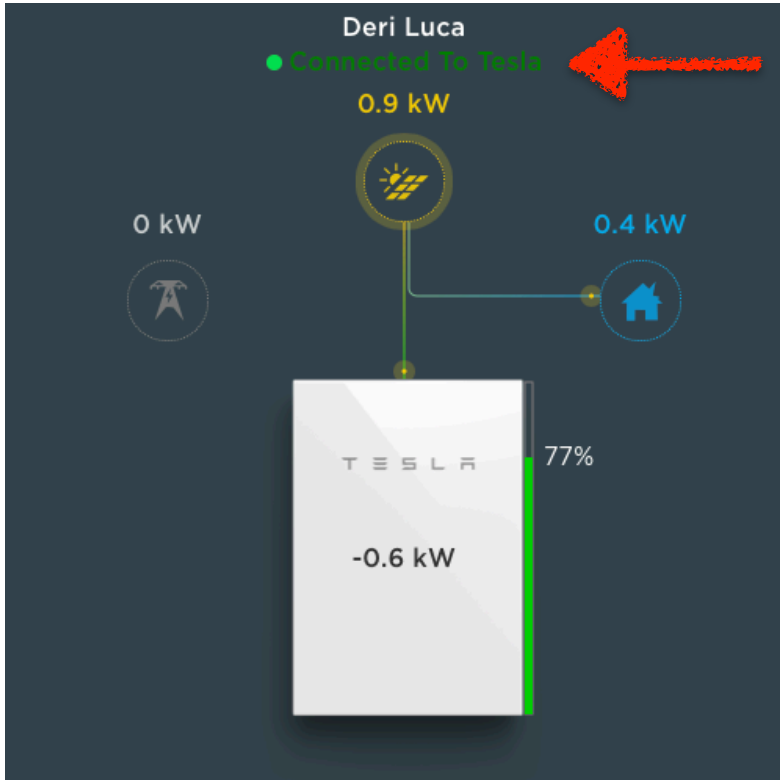
IoT Devices in Cloud [3/10]

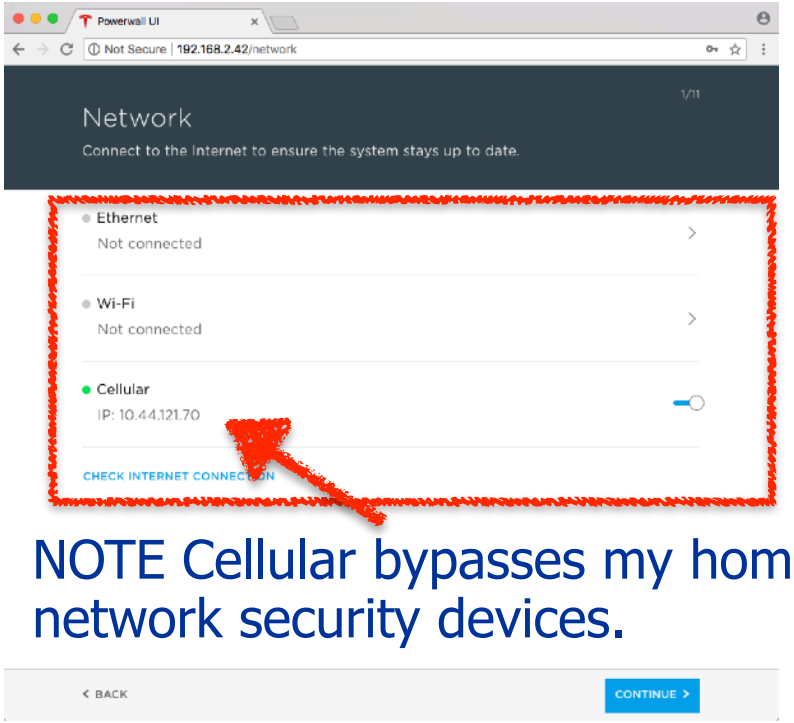


IoT Devices in Cloud [4/10]



IoT Devices in Cloud [5/10]





NOTE Cellular bypasses my home network security devices.

IoT Devices in Cloud [6/10]

```
#!/bin/bash
watch 'curl -s http://192.168.2.36/api/meters/aggregates | jq
"{battery:.battery.instant_power,solar:.solar.instant_power,grid:.site.instant_p
ower,house:.load.instant_power}"'
```

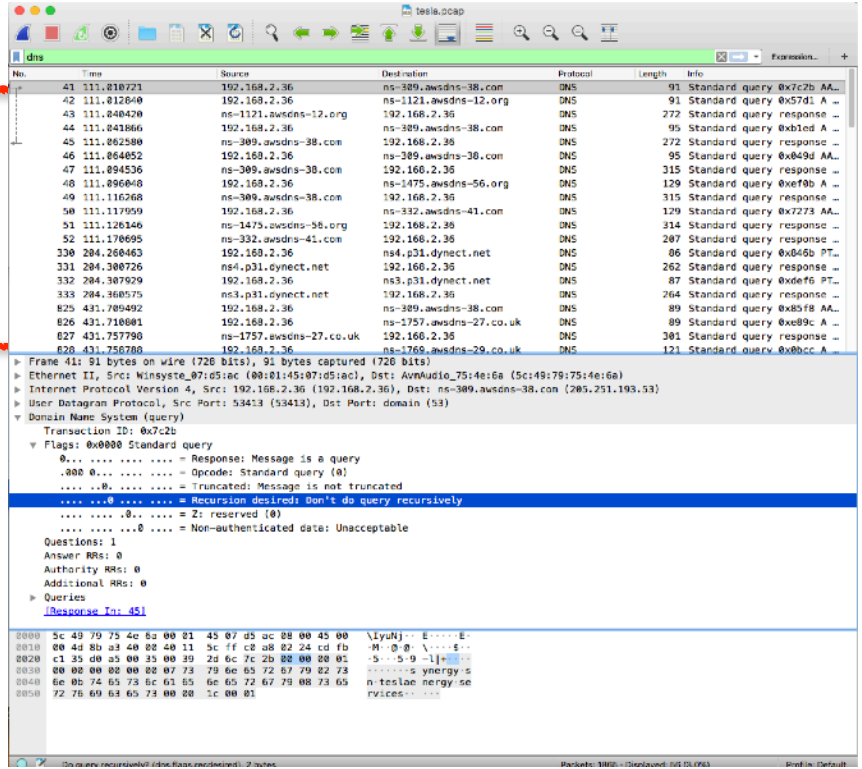
```
Every 2.0s: curl -s http://192.168.2.36/api/meters/aggregates |...  Sat Jun  9 11:22:56 2018

{
  "battery": -530,
  "solar": 845.3064575195312,
  "grid": -11.2249755859375,
  "house": 304.08148193359375
}
```

IoT Devices in Cloud [7/10]

- Cellular connectivity does not allow a customer to analyse what is the device reporting to the cloud (local security devices are bypassed).
- Disabling cellular allows Wireshark to analyse the network traffic produced by the Powerwall.
- See tesla.pcap: capture of Powerwall traffic to the Internet

IoT Devices in Cloud [8/10]

DNS

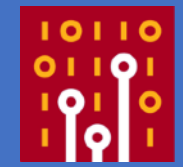


See tesla.pcap

IoT Devices in Cloud [9/10]

```
deri@ntop-digitalocean 201> dig +norecurse synergy.sn.teslaenergy.services

; <<>> DiG 9.11.3-1ubuntu1-Ubuntu <<>> +norecurse synergy.sn.teslaenergy.services
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 58690
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;synergy.sn.teslaenergy.services. IN  A

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sat Jun 09 11:49:35 CEST 2018
;; MSG SIZE  rcvd: 60
```

IoT Devices in Cloud [10/10]



```
deri@ntop-digitalocean 202> dig +norecurse @205.251.193.53 synergy.sn.teslaenergy.services

; <<>> DiG 9.11.3-1ubuntu1-Ubuntu <<>> +norecurse @205.251.193.53 synergy.sn.teslaenergy.services
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39134
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;synergy.sn.teslaenergy.services. IN A

;; ANSWER SECTION:
synergy.sn.teslaenergy.services. 60 IN    CNAME    hermes-stream-prd.sn.tesla.services.

;; AUTHORITY SECTION:
sn.teslaenergy.services. 172800  IN   NS   ns-1121.awsdns-12.org.
sn.teslaenergy.services. 172800  IN   NS   ns-1757.awsdns-27.co.uk.
sn.teslaenergy.services. 172800  IN   NS   ns-309.awsdns-38.com.
sn.teslaenergy.services. 172800  IN   NS   ns-914.awsdns-50.net.

;; Query time: 1 msec
;; SERVER: 205.251.193.53#53(205.251.193.53)
;; WHEN: Sat Jun 09 11:52:39 CEST 2018
;; MSG SIZE  rcvd: 241
```

Home IoT Devices [1/11]

See smart_home.pcap

Sonos

(192.168.177.122)

Alexa Echo Dot

(192.168.179.172)

Weather Station

(192.168.179.169)

(non-smart) TV

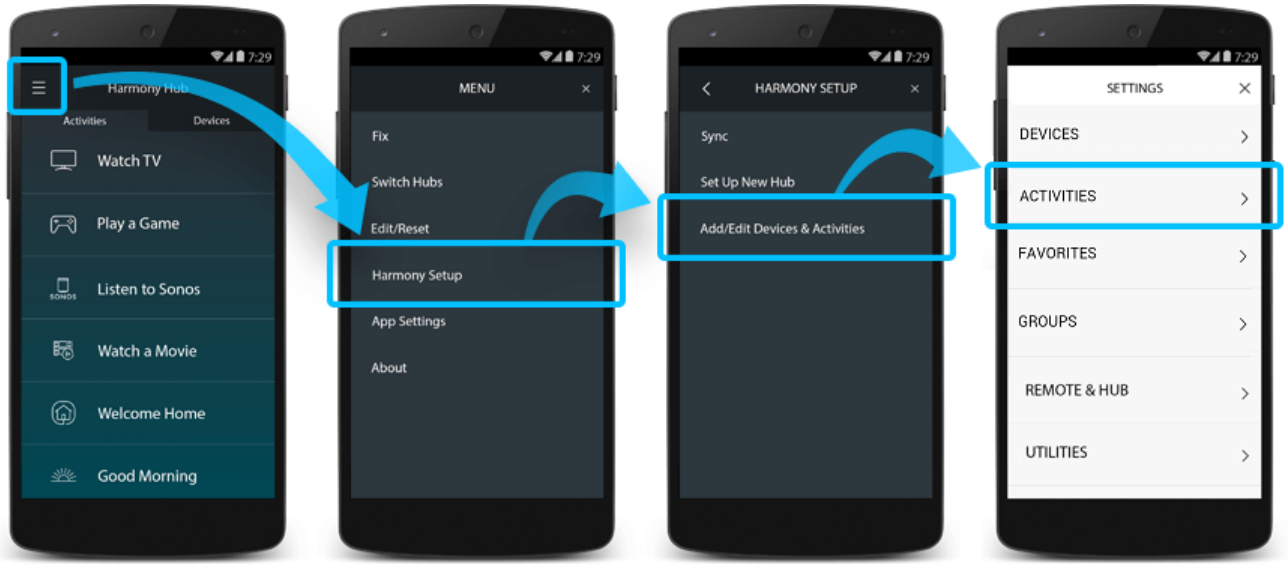
Logitech Harmony

(192.168.182.11)

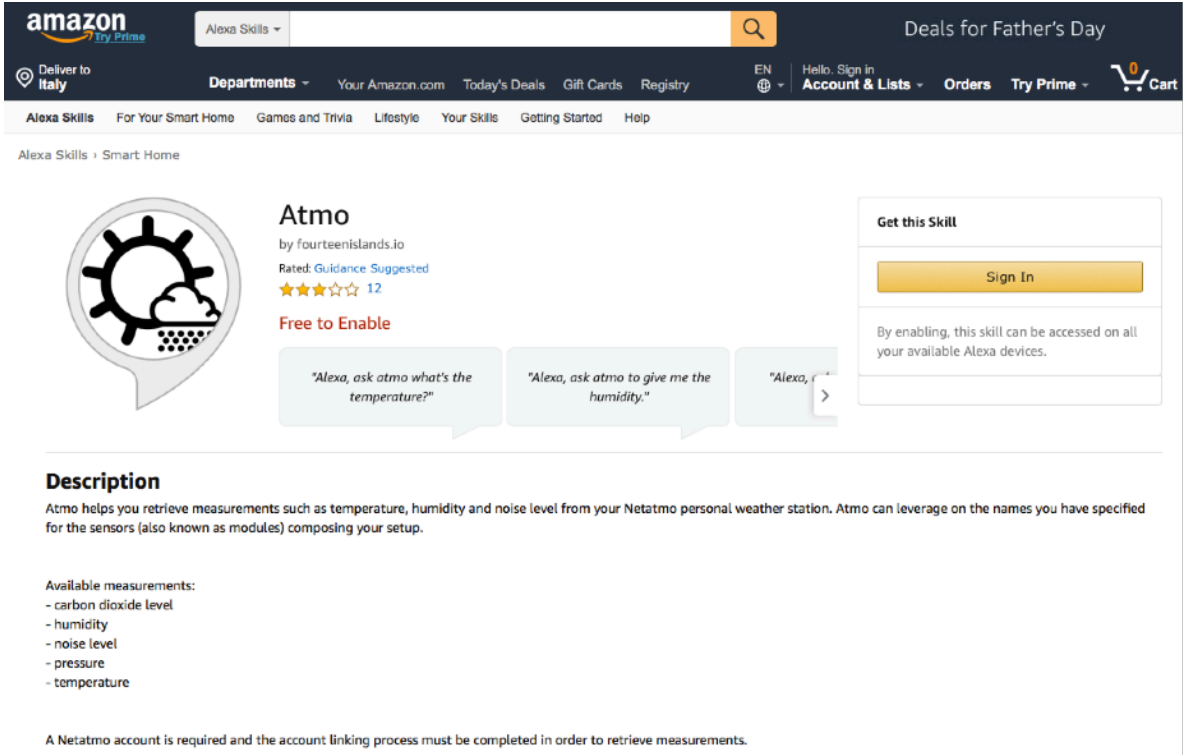
Roomba

(192.168.183.129)

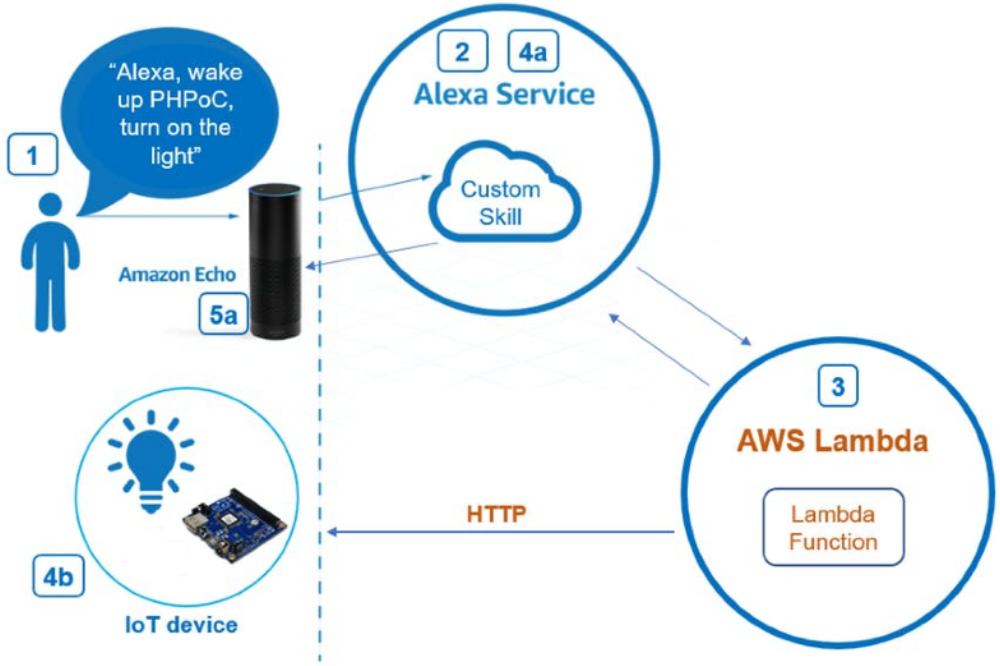
Home IoT Devices [2/11]



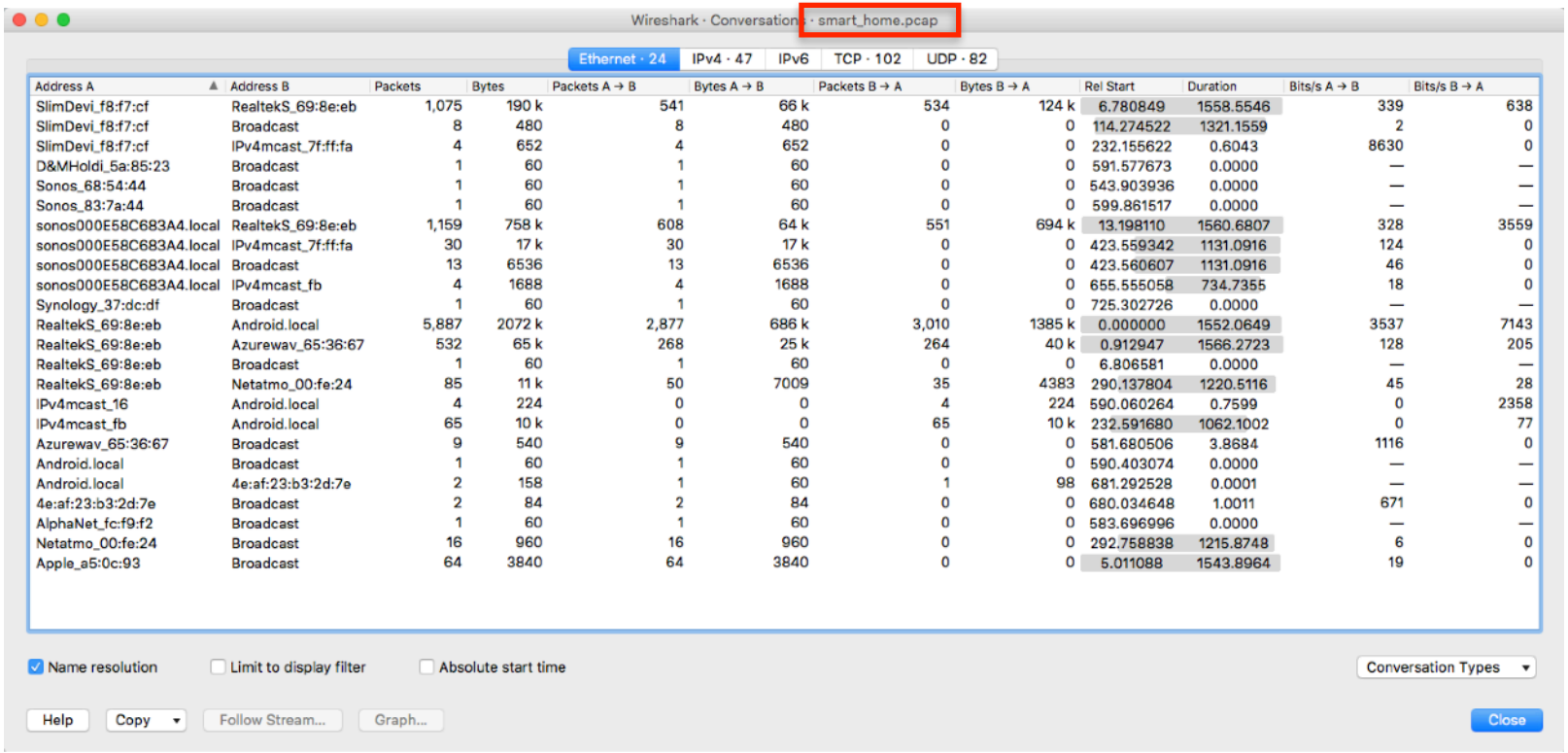
Home IoT Devices [3/11]



Home IoT Devices [3/11]



Home IoT Devices [4/11]



Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
SlimDevi_f8:f7:cf	RealtekS_69:8e:eb	1,075	190 k	541	66 k	534	124 k	6.780849	1558.5546	339	638
SlimDevi_f8:f7:cf	Broadcast	8	480	8	480	0	0	114.274522	1321.1559	2	0
SlimDevi_f8:f7:cf	IPv4mcast_7f:ff:fa	4	652	4	652	0	0	232.155622	0.6043	8630	0
D&MHoldi_5a:85:23	Broadcast	1	60	1	60	0	0	591.577673	0.0000	—	—
Sonos_68:54:44	Broadcast	1	60	1	60	0	0	543.903936	0.0000	—	—
Sonos_83:7a:44	Broadcast	1	60	1	60	0	0	599.861517	0.0000	—	—
sonos000E58C683A4.local	RealtekS_69:8e:eb	1,159	758 k	608	64 k	551	694 k	13.198110	1560.6807	328	3559
sonos000E58C683A4.local	IPv4mcast_7f:ff:fa	30	17 k	30	17 k	0	0	423.559342	1131.0916	124	0
sonos000E58C683A4.local	Broadcast	13	6536	13	6536	0	0	423.560607	1131.0916	46	0
sonos000E58C683A4.local	IPv4mcast_fb	4	1688	4	1688	0	0	655.555058	734.7355	18	0
Synology_37:dc:df	Broadcast	1	60	1	60	0	0	725.302726	0.0000	—	—
RealtekS_69:8e:eb	Android.local	5,887	2072 k	2,877	686 k	3,010	1385 k	0.000000	1552.0649	3537	7143
RealtekS_69:8e:eb	Azurewav_65:36:67	532	65 k	268	25 k	264	40 k	0.912947	1566.2723	128	205
RealtekS_69:8e:eb	Broadcast	1	60	1	60	0	0	6.806581	0.0000	—	—
RealtekS_69:8e:eb	Netatmo_00:fe:24	85	11 k	50	7009	35	4383	290.137804	1220.5116	45	28
IPv4mcast_16	Android.local	4	224	0	0	4	224	590.060264	0.7599	0	2358
IPv4mcast_fb	Android.local	65	10 k	0	0	65	10 k	232.591680	1062.1002	0	77
Azurewav_65:36:67	Broadcast	9	540	9	540	0	0	581.680506	3.8684	1116	0
Android.local	Broadcast	1	60	1	60	0	0	590.403074	0.0000	—	—
Android.local	4e:af:23:b3:2d:7e	2	158	1	60	1	98	681.292528	0.0001	—	—
4e:af:23:b3:2d:7e	Broadcast	2	84	2	84	0	0	680.034648	1.0011	671	0
AlphaNet_fc:f9:f2	Broadcast	1	60	1	60	0	0	583.696996	0.0000	—	—
Netatmo_00:fe:24	Broadcast	16	960	16	960	0	0	292.758838	1215.8748	6	0
Apple_a5:0c:93	Broadcast	64	3840	64	3840	0	0	5.011088	1543.8964	19	0

Home IoT Devices [5/11]

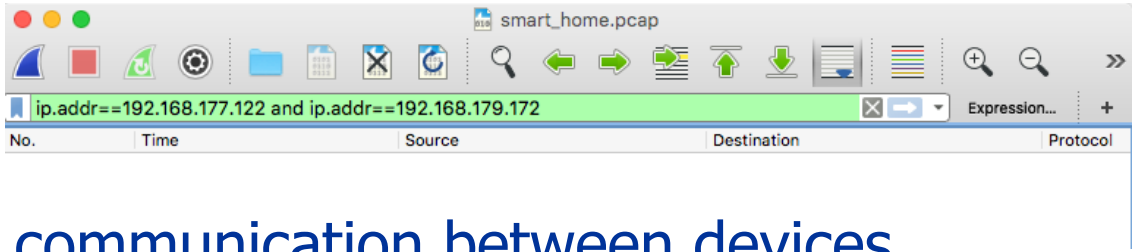
Source Mac Addresses

20 ▾ Filter Macs ▾ Device Type ▾ Manufacturer ▾

Mac Address	Manufacturer	Device Type	Name	Hosts	ARP	Seen Since	Breakdown	Throughput	Traffic
5C:33:8E:FC:F9:F2	Alpha Networks Inc.	Computer	5C:33:8E:FC:F9:F2	0	1	70 days, 01:17:08	Sent	0 bit/s	60 Bytes
40:B4:CD:2B:4C:9E	Amazon Technologies Inc.	Multimedia	amazon-bd974b201	1	81	70 days, 01:26:52	Sent Rcvd	0 bit/s	1.99 MB
98:01:A7:A5:0C:93	Apple, Inc.	Multimedia	98:01:A7:A5:0C:93	0	64	70 days, 01:26:47	Sent	0 bit/s	3.75 KB
40:9F:38:65:36:67	AzureWave Technology Inc.	IoT	Roomba	1	93	70 days, 01:26:51	Sent Rcvd	0 bit/s	64.49 KB
00:05:CD:5A:85:23	D&M Holdings Inc.	Unknown	00:05:CD:5A:85:23	0	1	70 days, 01:17:00	Sent	0 bit/s	60 Bytes
70:EE:50:00:FE:24	Netatmo	IoT	Netatmo-Personal-Weather-Station	1	23	70 days, 01:22:02	Sent Rcvd	0 bit/s	12.06 KB
00:E0:4C:69:8E:EB	Realtek Semiconductor Corp.	Router/Switch	00:E0:4C:69:8E:EB	36	312	70 days, 01:26:52	Sent Rcvd	0 bit/s	2.95 MB
00:04:20:F8:F7:CF	Slim Devices, Inc.	IoT	HarmonyHub	1	103	70 days, 01:26:45	Sent Rcvd	0 bit/s	187.25 KB
00:0E:58:68:54:44	Sonos, Inc.	Multimedia	SonosZB	0	1	70 days, 01:17:48	Sent	0 bit/s	60 Bytes
00:0E:58:83:7A:44	Sonos, Inc.	Multimedia	00:0E:58:83:7A:44	0	1	70 days, 01:16:52	Sent	0 bit/s	60 Bytes
00:0E:58:C6:83:A4	Sonos, Inc.	Multimedia	SonosZP	1	48	70 days, 01:26:39	Rcvd	0 bit/s	765.94 KB
00:11:32:37:DC:DF	Synology Incorporated	NAS	00:11:32:37:DC:DF	0	1	70 days, 01:14:46	Sent	0 bit/s	60 Bytes
4E:AF:23:B3:2D:7E	n/a	Computer	rock64	1	3	70 days, 01:15:32	Sent Rcv	0 bit/s	242 Bytes

IoT Devices in Cloud [6/11]

- smart_home.pcap interactions include:
  - Alexa (.172) turns on music on Sonos (.122)
  - Alexa checks the temperature
  - Alexa starts turns on the robot cleaner

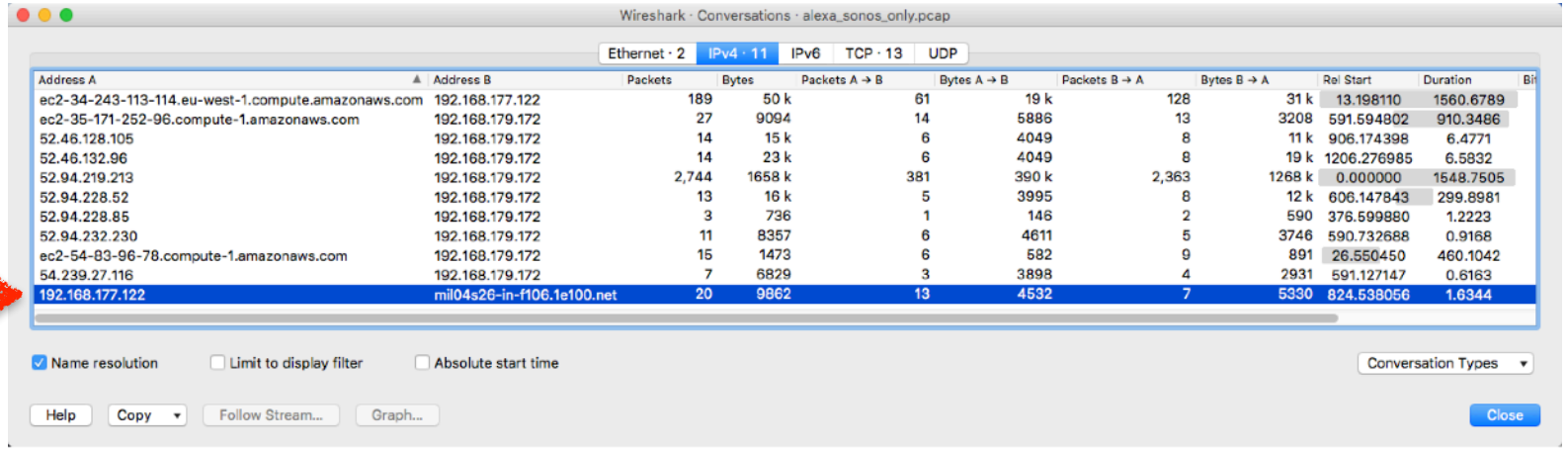


No direct communication between devices

IoT Devices in Cloud [7/11]

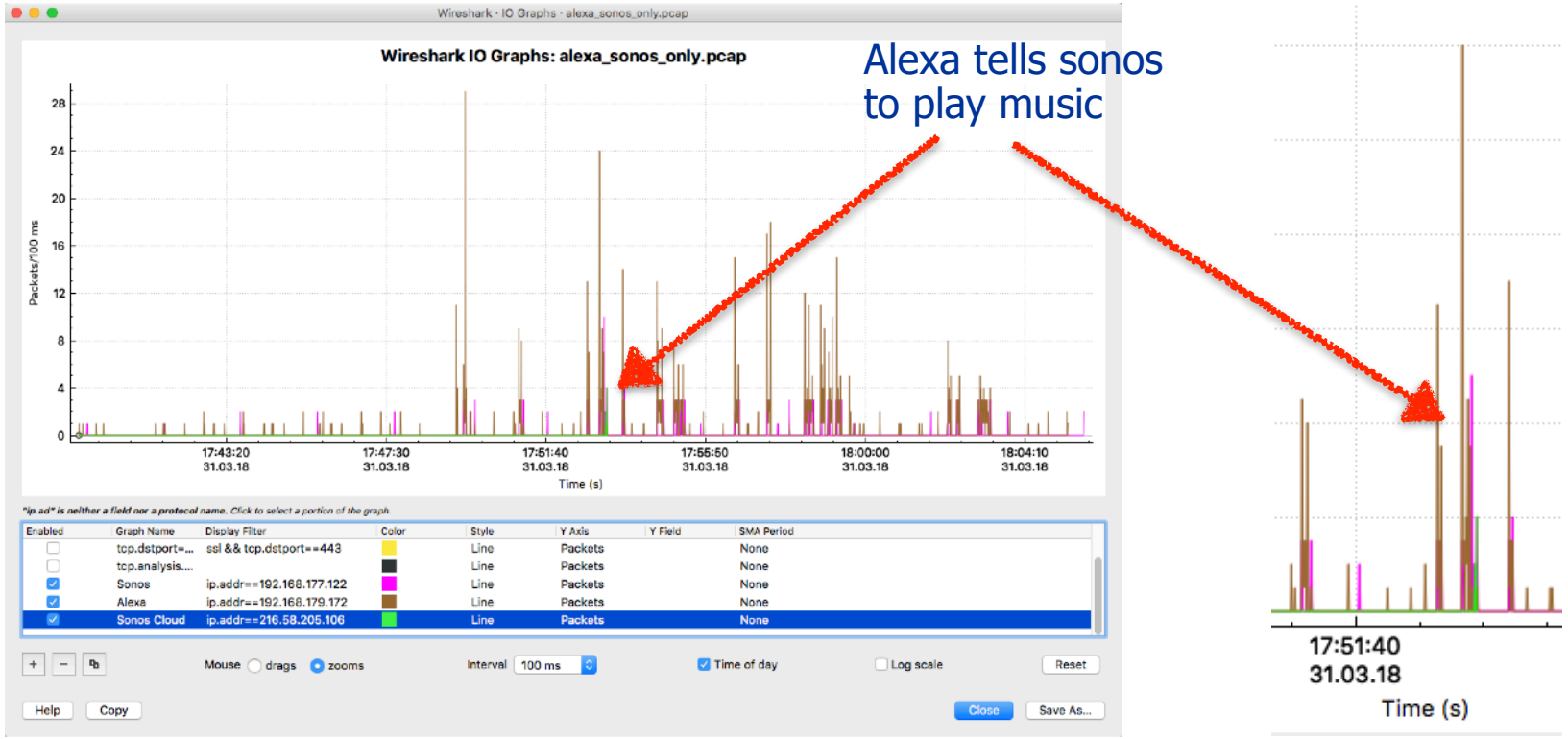
- Select traffic with "(ip.addr==192.168.177.122 or ip.addr==192.168.179.172) and ssl" or see alexa_sonos_only.pcap

sonos

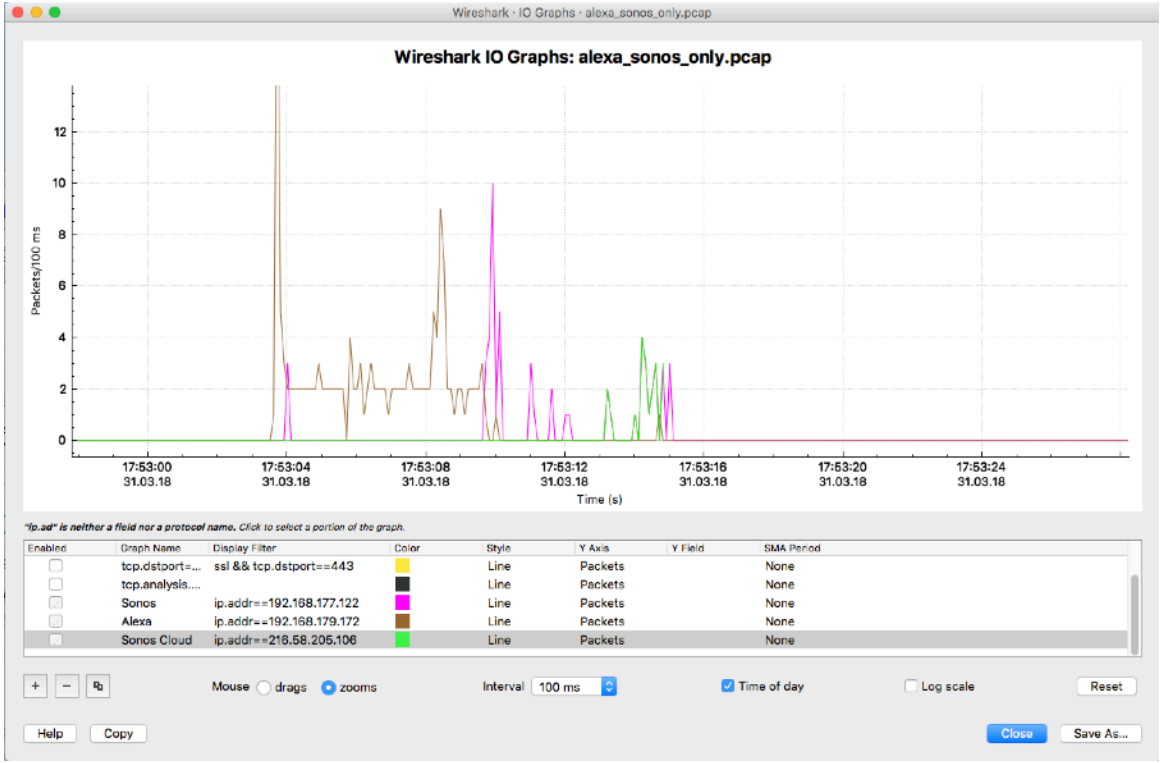


Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
ec2-34-243-113-114.eu-west-1.compute.amazonaws.com	192.168.177.122	189	50 k	61	19 k	128	31 k	13.198110	1560.6789
ec2-35-171-252-96.compute-1.amazonaws.com	192.168.179.172	27	9094	14	5886	13	3208	591.594802	910.3486
52.46.128.105	192.168.179.172	14	15 k	6	4049	8	11 k	906.174398	6.4771
52.46.132.96	192.168.179.172	14	23 k	6	4049	8	19 k	1206.276985	6.5832
52.94.219.213	192.168.179.172	2,744	1658 k	381	390 k	2,363	1268 k	0.000000	1548.7505
52.94.228.52	192.168.179.172	13	16 k	5	3995	8	12 k	606.147843	299.8981
52.94.228.85	192.168.179.172	3	736	1	146	2	590	376.599880	1.2223
52.94.232.230	192.168.179.172	11	8357	6	4611	5	3746	590.732688	0.9168
ec2-54-83-96-78.compute-1.amazonaws.com	192.168.179.172	15	1473	6	582	9	891	26.550450	460.1042
54.239.27.116	192.168.179.172	7	6829	3	3898	4	2931	591.127147	0.6163
192.168.177.122	mil04s26-in-f106.1e100.net	20	9862	13	4532	7	5330	824.538056	1.6344

IoT Devices in Cloud [8/11]



IoT Devices in Cloud [9/11]



Let's zoom...

IoT Devices in Cloud [10/11]

- Alexa/Sonos do not talk directly but only through the cloud even though they are sitting on the same network.
- Cloud-based interactions are encrypted. The only options are: pass or drop with no restrictions on actions performed by the devices.
- As cloud communications are started from the local network (inside NAT), the cloud can remotely instruct local devices to do everything.

IoT Devices in Cloud [11/11]

2.5 Privacy Requirements

The skill must not:

1. Contain references to or include malicious hacking, such as phishing or Trojans. This includes rooting a device or circumventing Amazon's or any developer's digital rights management (DRM) software.
2. Contain references to or include malicious user spying or tracking, including stalking, in the skill or skill metadata.
3. Misuse customer personally identifiable information or sensitive personal information.
4. Collect personal information from end users without doing *all* of the following: (i) provide notice of that data collection to end users in your skill's detail page,
   (ii) use the information in a way that end users have consented to, and
   (iii) ensure that your collection and use of that information complies with your privacy notice and all applicable laws.

   Prior to submitting a skill that collects personal information from end users, you are required to supply a privacy policy that will be displayed to end users on your skill's detail page in the Alexa App.

https://developer.amazon.com/docs/custom-skills/security-testing-for-an-alexa-skill.html

Final Remarks

- As shown with Tesla, there are some (limited) checks to make sure the device is running on a “free” network.
- HTTP public certificate pinning can definitively help to detect intruders but device owner still need to trust the device manufacturer (https://en.wikipedia.org/wiki/HTTP_Public_Key_Pinning).
- SSL implements privacy/security (good) but on the other hand limits inspection (bad).
- Alternative connectivity (e.g. cellular network with Tesla) can further complicate all this.