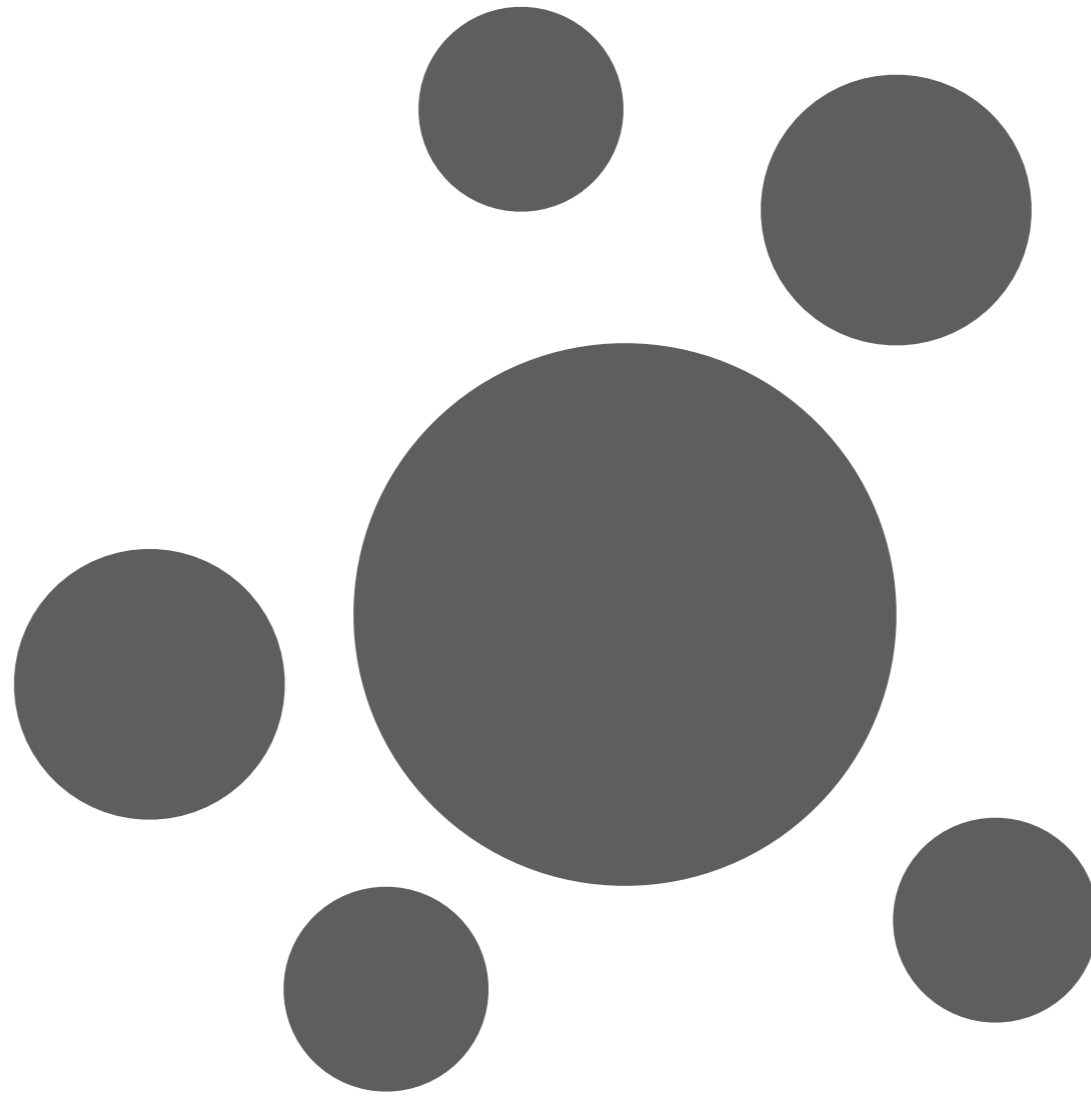


Faster better tech support with TLS Host Matching



MUM Costa Rica 2018



Chronic tech support calls bog down the help desk

my
network is
slow!

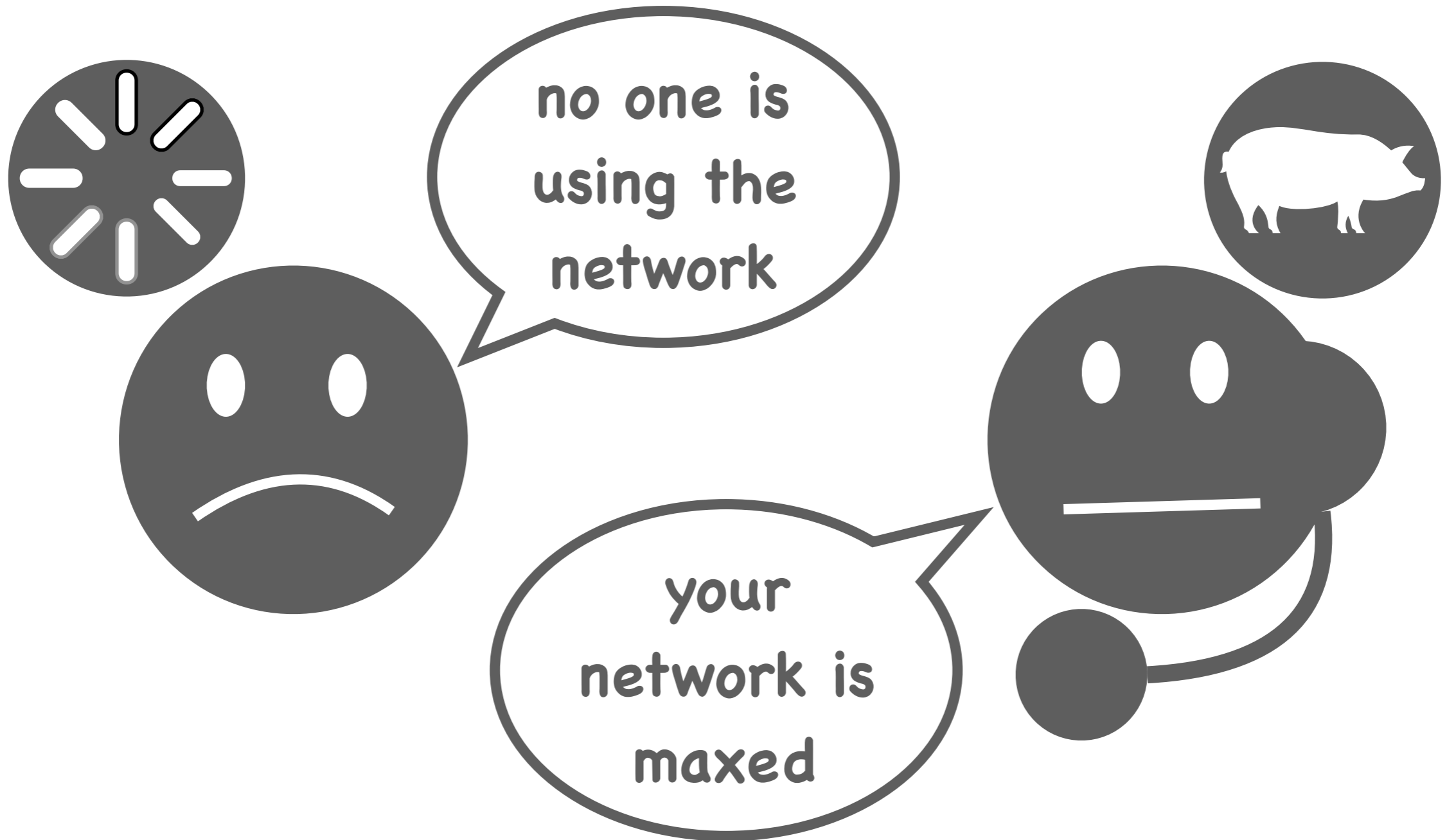
can I see
what my kids are
doing online?

what's
taking up the
bandwidth

are the
neighbors on my
wifi?

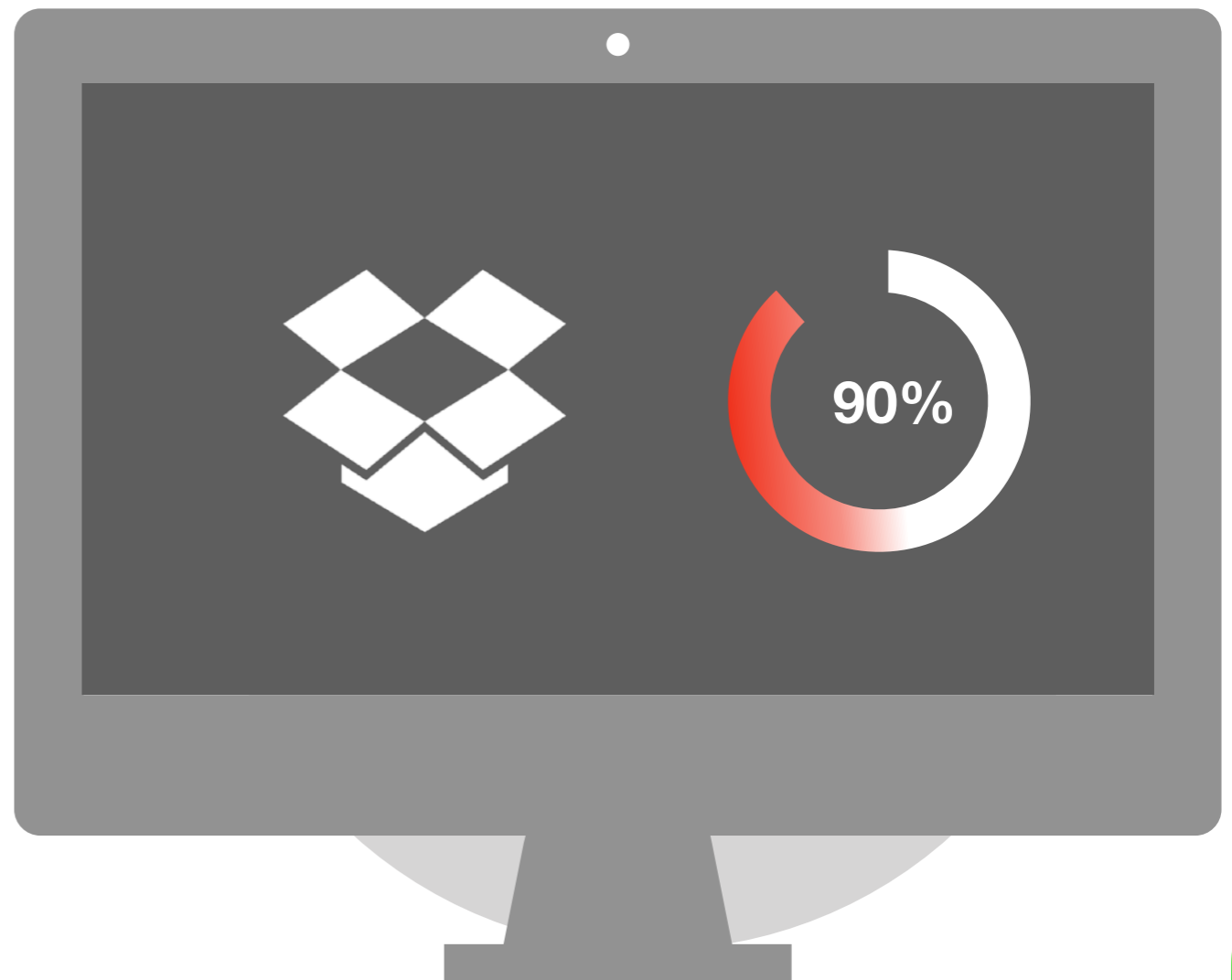
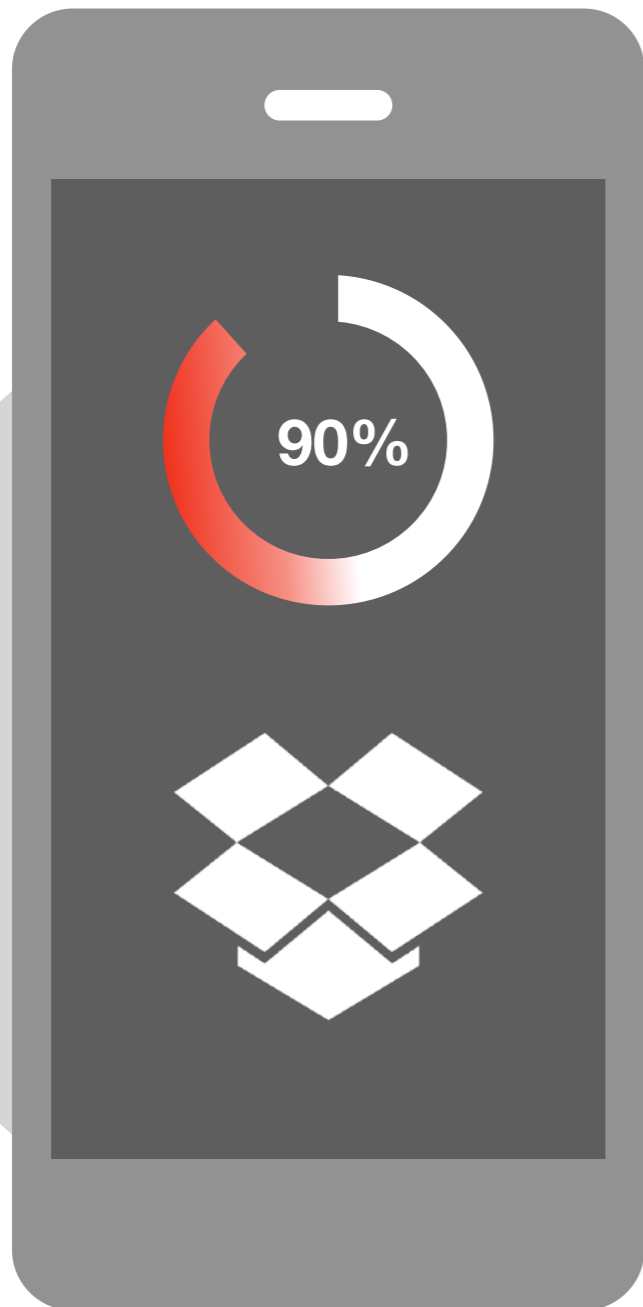
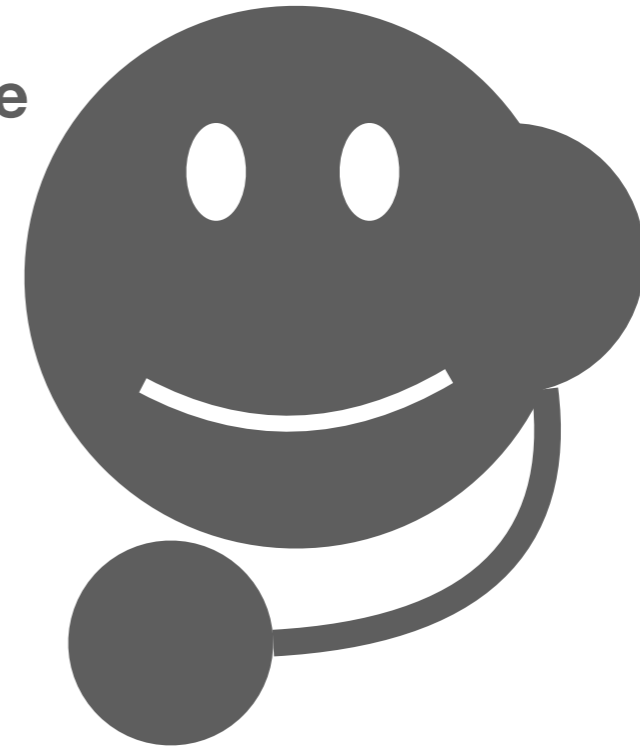


The customer and the helpdesk agent don't see the same thing



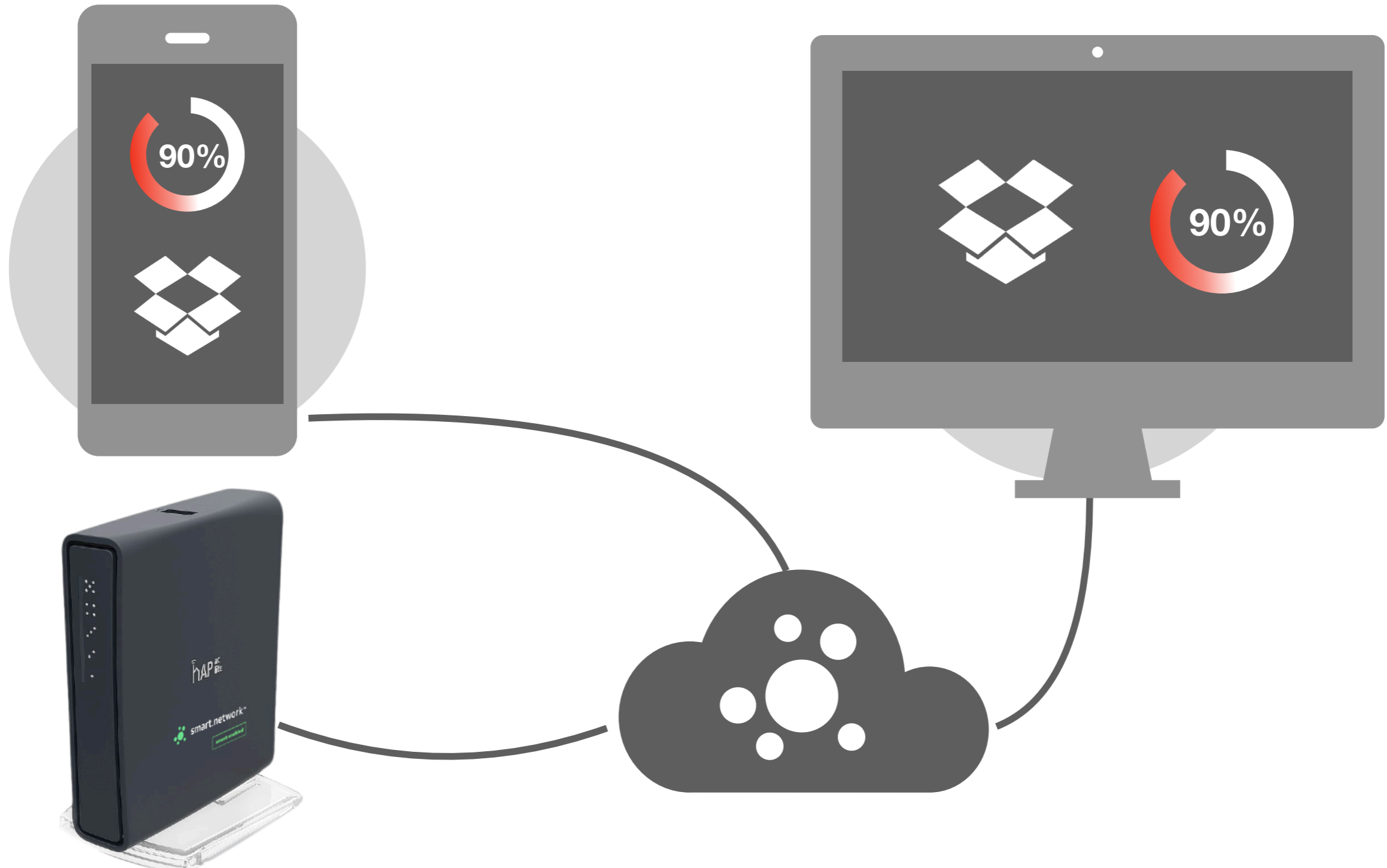
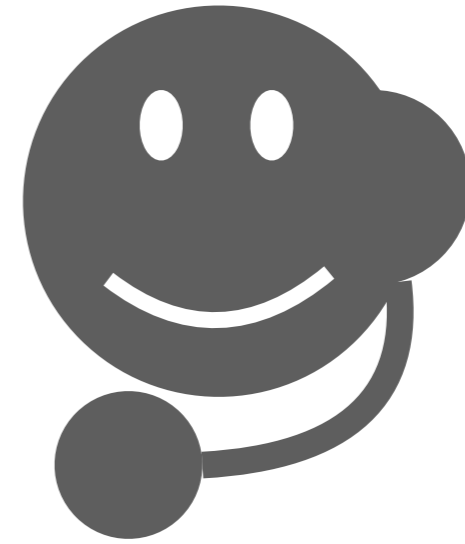


What if they could see
the same thing like
LogMeIn or
PCAnywhere but for
networks?



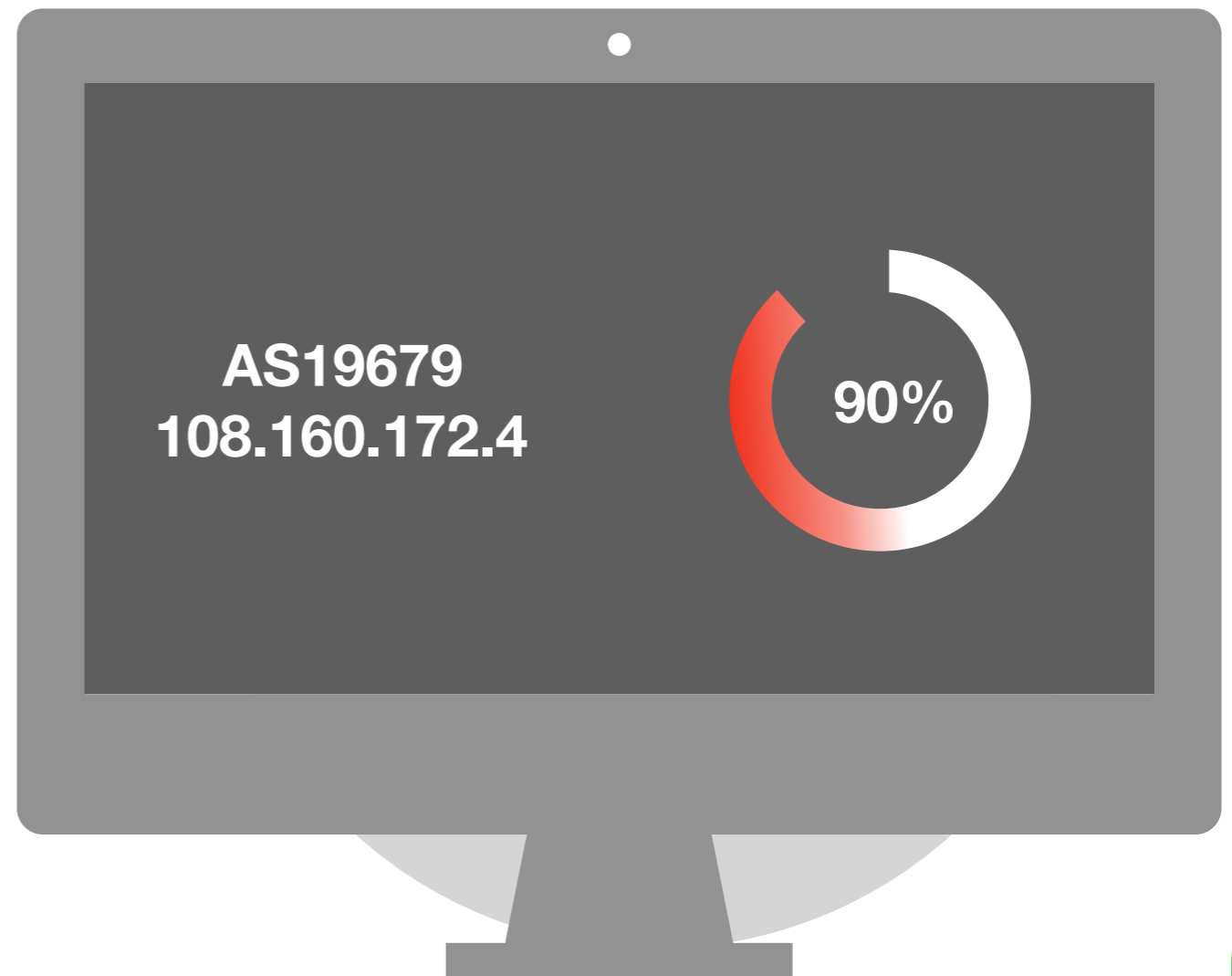
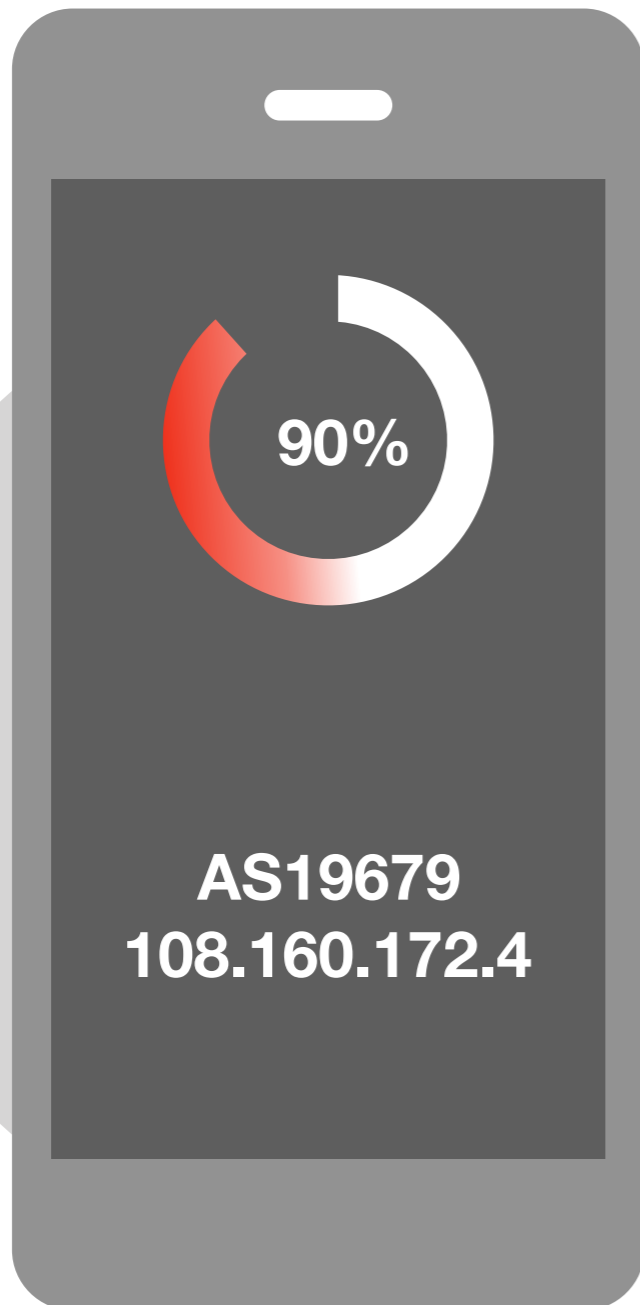
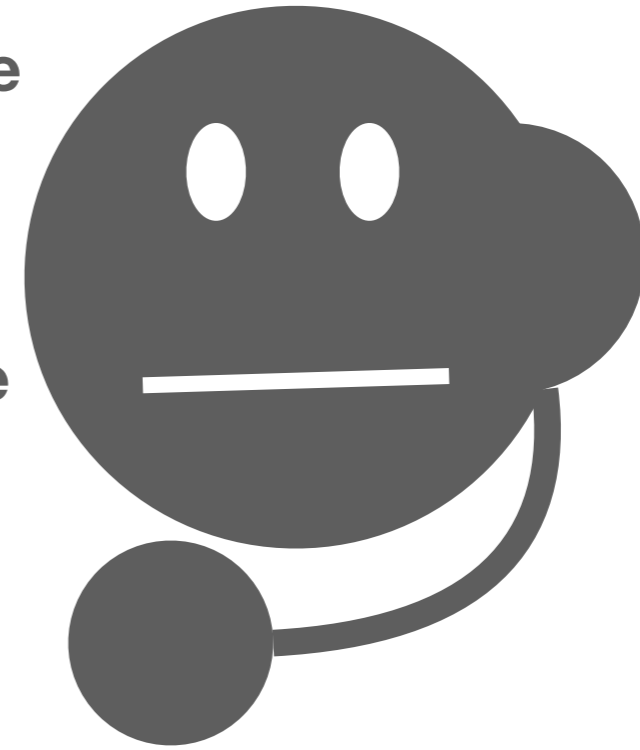


That is exactly what smart.network offers, a way for the customer and agent to view the network together, in real time, and in non technical terms





Without TLS host matching, many of the services would not show on the screen with friendly names that are useful for the agent and the customer



Back in the days, traffic was not encrypted so traditional packet inspections was useful



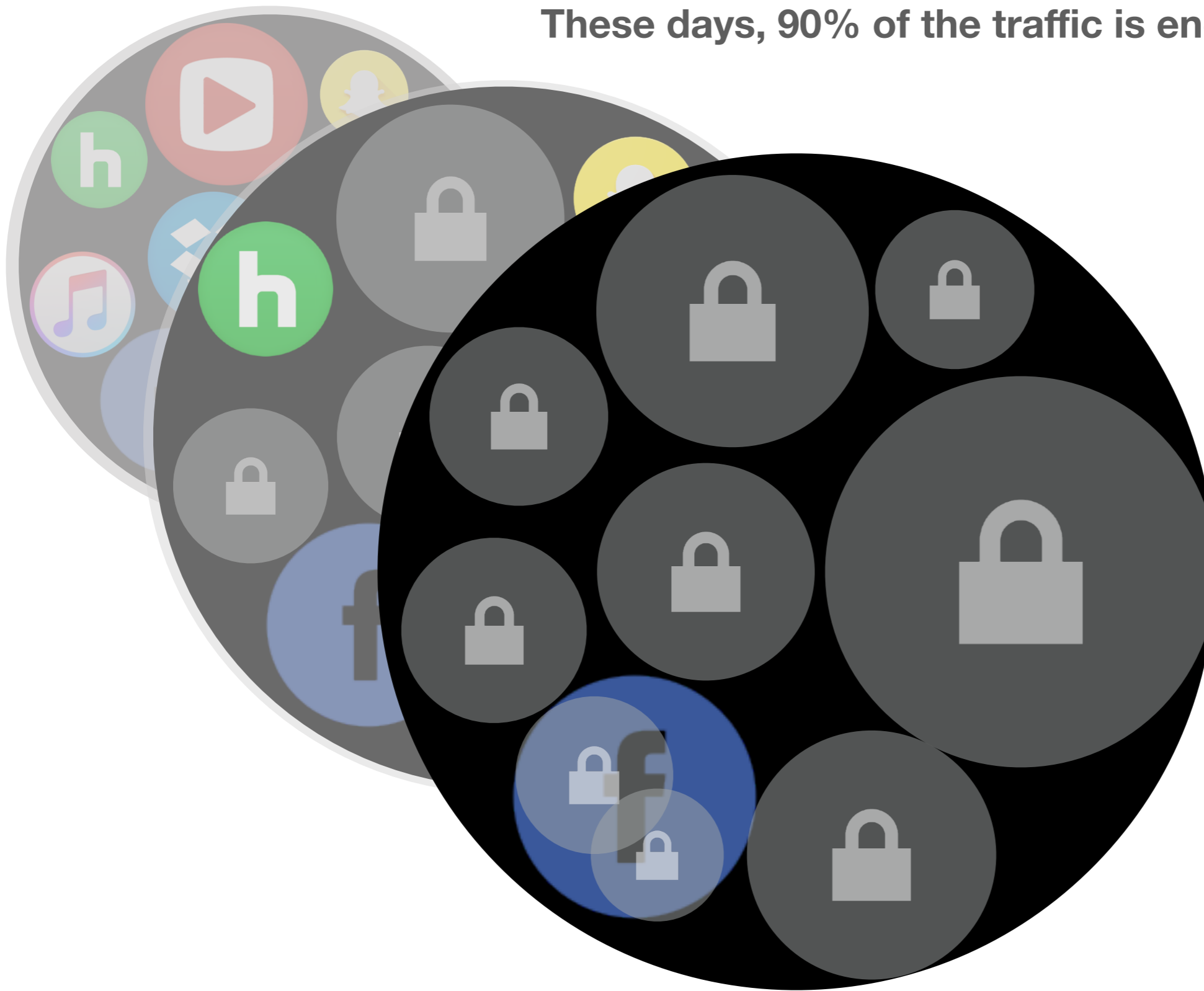
2008

By 2013, between 30% and 50% of the traffic was encrypted



2013

These days, 90% of the traffic is encrypted



2018

Other means are used to identify and classify encrypted traffic



ASN

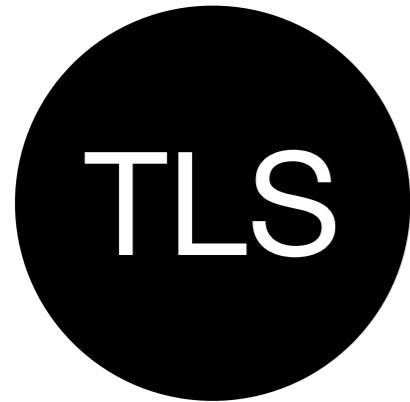
Port

Pattern

DNS

TLS

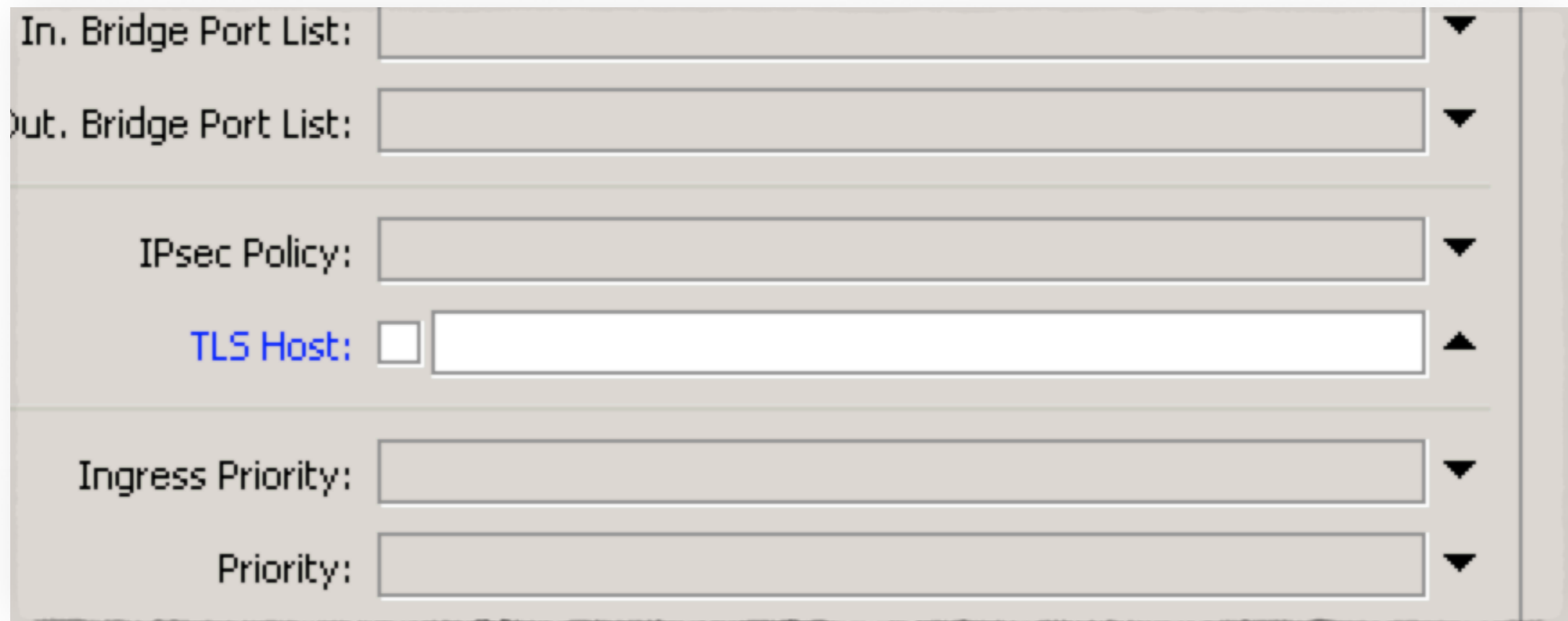
TLS host matching is a big help on classifying ssl traffic



“Allows to match https traffic based on TLS SNI hostname. Accepts GLOB syntax for wildcard matching. Note that matcher will not be able to match hostname if TLS handshake frame is fragmented into multiple TCP segments (packets).”

Where to find TLS Host matching settings:

IP > Firewall > New Firewall/NAT/Mangle Rule
> Advanced tab



The image shows a screenshot of the Mikrotik Firewall rule configuration interface, specifically the Advanced tab. The interface is a light gray form with several fields and a checkbox. The fields are: In. Bridge Port List, Out. Bridge Port List, IPsec Policy, Ingress Priority, and Priority. The TLS Host field is highlighted with a blue border and contains a white text input field. The checkbox next to the TLS Host label is unchecked. The form is set against a dark gray background.

In. Bridge Port List:	<input type="text"/>	▼
Out. Bridge Port List:	<input type="text"/>	▼
IPsec Policy:	<input type="text"/>	▼
TLS Host:	<input type="checkbox"/> <input type="text"/>	▲
Ingress Priority:	<input type="text"/>	▼
Priority:	<input type="text"/>	▼

`youtube.com` or `*.youtube.com` or `*youtube*`

Most services will use other domains to call content from, so additional
hosts need to be found

youtube.com or *.youtube.com or *youtube*



yting.com and googlevideo.com

Here are some examples of other TLS Hosts related to primary domains



cnn.com

bbc.com

vimeo.com

twitter.com

cnnios-
f.akamaihd.net

bbci.co.uk

vimeocdn.com

t.co

ugdturner.com

bbcfmt.hs.llnwd.net

vimeo.akamaized.net

twimg.com

turner.com

bbc.co.uk

To find more, one has to go deep with Wireshark
look for client hello, SSL handshake server name!

