

CAPPORT BoF

CAPtive PORtals

or some other words that make the CAPPORT acronym

Welcome to CAPPORT BoF

Chairs:

- Warren Kumari <warren@kumari.net>
- Mark Nottingham <mnot@mnot.net>

Jabber Scribe:

- capport@ietf.jabber.org

Minutes:

<http://tools.ietf.org/wg/capport/minutes>

- Note Well.
- Blue Sheets.
- ~~Agenda Bashing.~~

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- **The IETF plenary session**
- **The IESG, or any member thereof on behalf of the IESG**
- **Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices**
- **Any IETF working group or portion thereof**
- **Any Birds of a Feather (BOF) session**
- **The IAB or any member thereof on behalf of the IAB**
- **The RFC Editor or the Internet-Drafts function**

All IETF Contributions are subject to the rules of [RFC 5378](#) and [RFC 3979](#) (updated by [RFC 4879](#)).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult [RFC 5378](#) and [RFC 3979](#) for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.



A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

What are they?!


Sometimes it works!

The image shows a screenshot of the United website's Wi-Fi service page. The page features the United logo, navigation tabs for Home, Internet, and Flight information, and a Wi-Fi icon indicating internet availability. The main content area promotes "United Wi-Fi keeps you connected" with a price of \$19.99 and a "Purchase access" button. A link at the bottom says "Switch Internet access to a new device".

On the right side, a flight information panel for UA 989 | IAD to FRA is visible, showing destination information for Frankfurt, DE (FRA) with a temperature of 53°F / 12°C and a departure time of 5:46 p.m. on Saturday, July 11. Below this, a browser developer console window is open, displaying network request details for a GET request to http://www.ietf.org/. The status code is 302 Moved Temporarily, and the response headers include "X-Squid-Error: 403 Access Denied".

United  Internet is available 

Home Internet Flight information

 **United Wi-Fi keeps you connected.**

Full Web browsing access
Browse the Internet in addition to using email and mobile apps. Live video and Internet streaming services are not supported.


\$19.99

[Purchase access](#)

[Switch Internet access to a new device](#)

UA 989 | IAD to FRA

Destination information

 Frankfurt, DE (FRA)
53°F / 12°C | Clear
2:36 a.m. | Sat, Jul 11

Departed: IAD | 5:46 p.m.
Arrived: FRA | 7:44 a.m.

26 requests | 663 KB transferred | Finish: 6.36 s

× Headers Preview Response Timing

▼ General

Remote Address: 104.20.0.85:80
Request URL: http://www.ietf.org/
Request Method: GET
Status Code: ● 302 Moved Temporarily

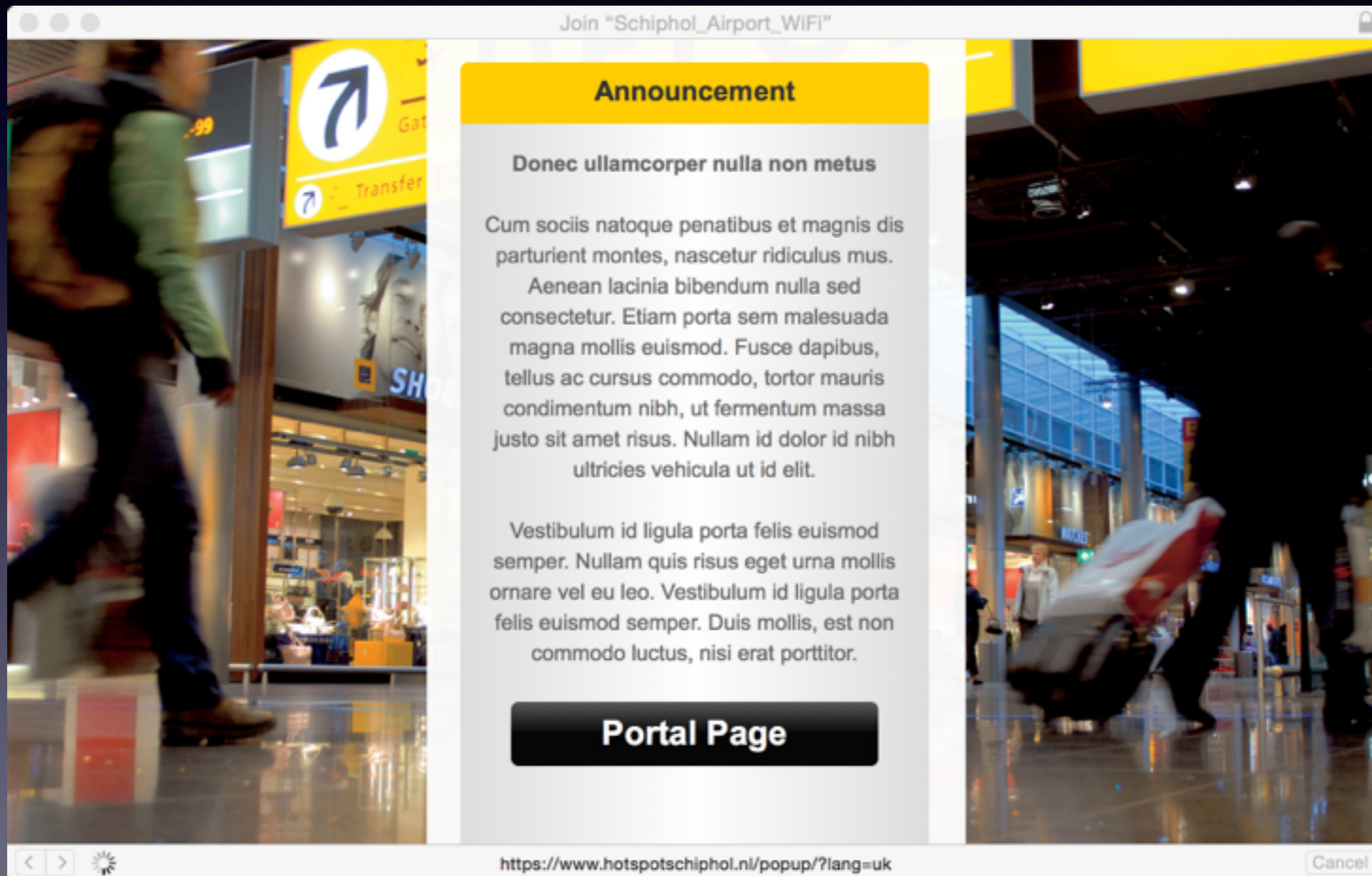
▼ Response Headers [view source](#)

Connection: close
Content-Length: 0
Content-Type: text/html
Date: Sat, 11 Jul 2015 00:42:10 GMT
Location: http://www.unitedwifi.com
Mime-Version: 1.0
Server: squid/3.1.10
Via: 1.0 bc01 (squid/3.1.10)
X-Cache: MISS from bc01
X-Squid-Error: 403 Access Denied

Often it doesn't

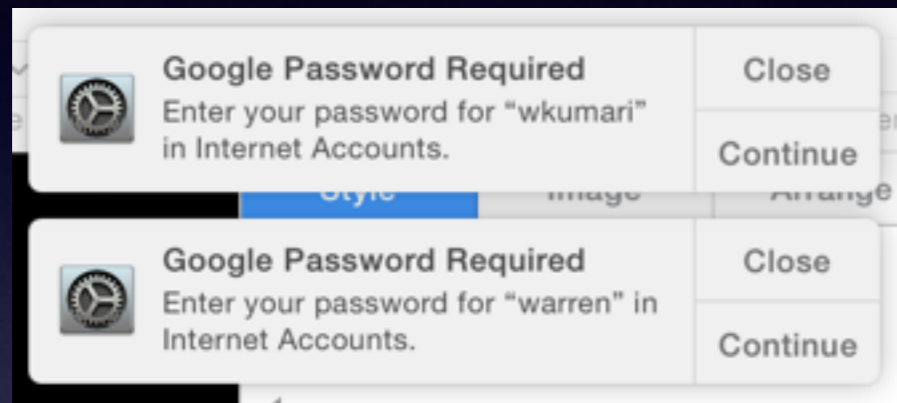


Often it doesn't



Often it doesn't...

...and makes things sad.



What's the problem?!

- Interception techniques suck
 - They look like MitM attacks
 - More secure endpoints become sad with MitM attacks
 - VPNs, HTTPS, DNSSEC, etc
- Interacting with captive portals sucks
 - Connecting to them sucks
 - Displays on phones, i8n, accessibility
 - Reconnecting to them sucks
 - Not knowing if you have connected to them sucks
- Notice a pattern here?

What do we want?

- A way to find the Captive Portal
 - Avoid interception / MitM attacks
 - Avoid 'iTunes cannot validate this cert'
 - Avoid applications breaking

What do we want to do?

- A way to talk to the Captive Portal
 - Protocol to interact with CP
 - Discover the status
 - Discover time remaining
 - Re-authenticate before expiry
- Automated logins

What do we want to **not** do?

- Kvetch
 - Not helpful...

Challenges...

- Not all CPs want to streamline this...
 - Eyeballs are important...
 - “... to get access, like us on Facebook.”
- Legacy clients
- Getting vendor involvement.

Strawman charter

Some networks require interaction from users prior to authorizing network access. Prior to granting that authorization, network access might be limited in some fashion. Frequently, this authorization process requires human interaction, frequently to either arrange for payment or accept some legal terms.

Currently, network providers use a number of interception techniques to reach a human user (such as intercepting cleartext HTTP to force a redirect to a web page of their choice), many of which look like a MitM attack. As endpoints become inherently more secure, existing interception techniques will become less effective and/or will fail. This results in a poor user experience as well as a lower rate of success for the Captive Portal operator.

Strawman charter (cont)

The CAPPOT WG will define mechanisms and protocols to:

- allow endpoints to discover that they are in such a limited environment
- allow endpoints to learn about the parameters of their confinement
- provide a URL to interact with the Captive Portal and satisfy the requirements
- interact with the Captive Portal to obtain information such as status, remaining access time, etc.
- (optionally) advertise a service whereby devices can enable or disable unrestricted access without human interaction

Milestones:

TDB: Initial problem statement / use case document

TBD: Initial terminology document

TBD: Initial portal interaction document (perhaps based upon <http://coova.org/CoovaChilli/JSON> ?)

TBD: Extended portal interaction document (for systems without browsers)

Open Questions

- Want to form a WG?
 - Can we get A: enough and B: the right participation?
- Who will actually do work?
- What are we missing?