

Spjaldtölvur og tölvuský á vinnustaðnum - öryggismál -

Ingimar Örn Jónsson

Rekjanleiki & ábyrgðarskylda

Reiknistofnun Háskóla
Íslands

Hínet

Rútað public ip tölu net

1Gb/10Gb Backbone

> 50 byggingar

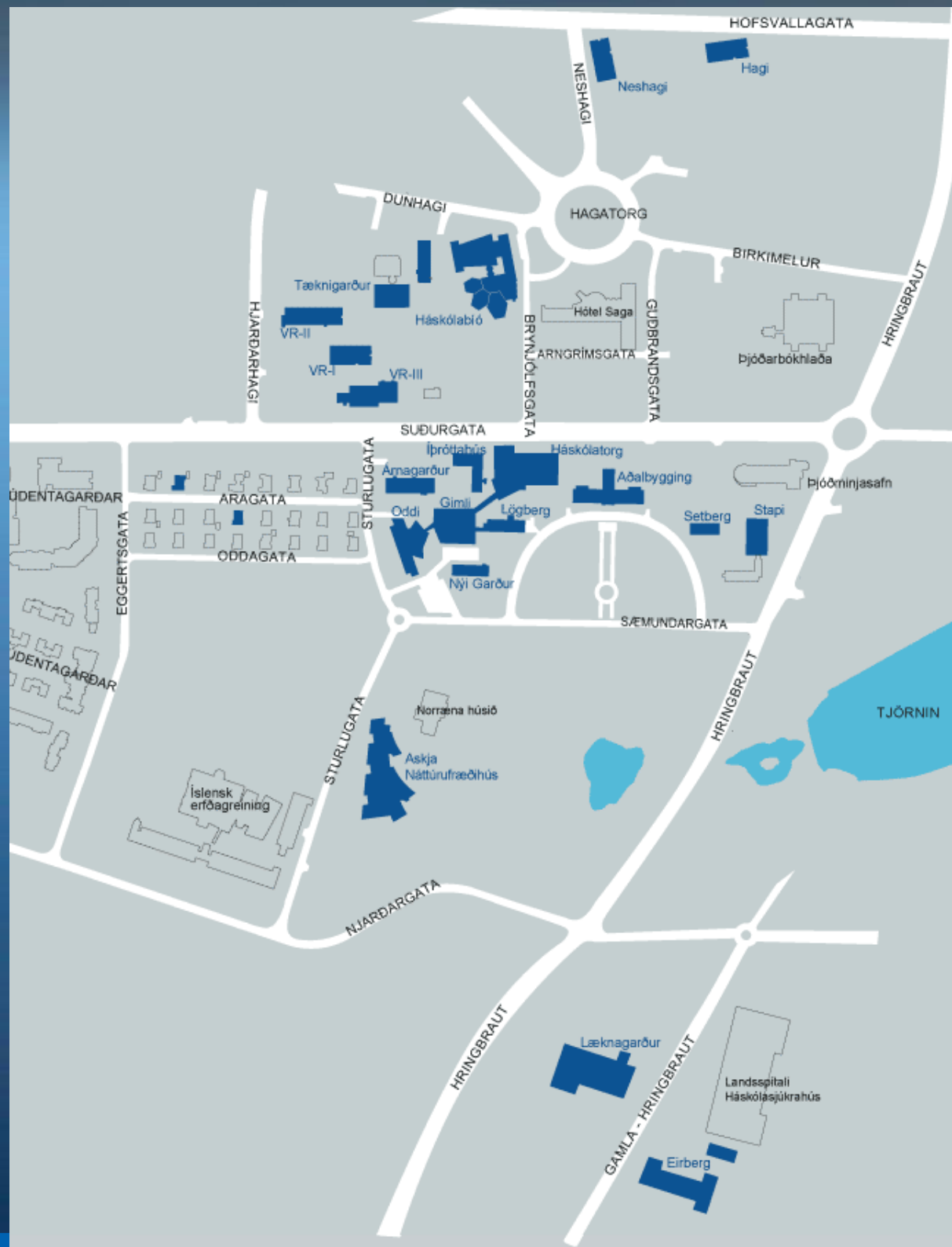
Reykjavík

Selfoss

Laugarvatn

Húsavík

Sandgerði





Hínet

149 undirnet

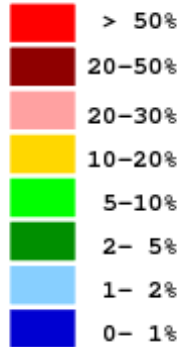
21 rúter/beinir

265 svissar

318 þráðlausir sendar

HÍnet

Mesta álag [% af burðargetu]

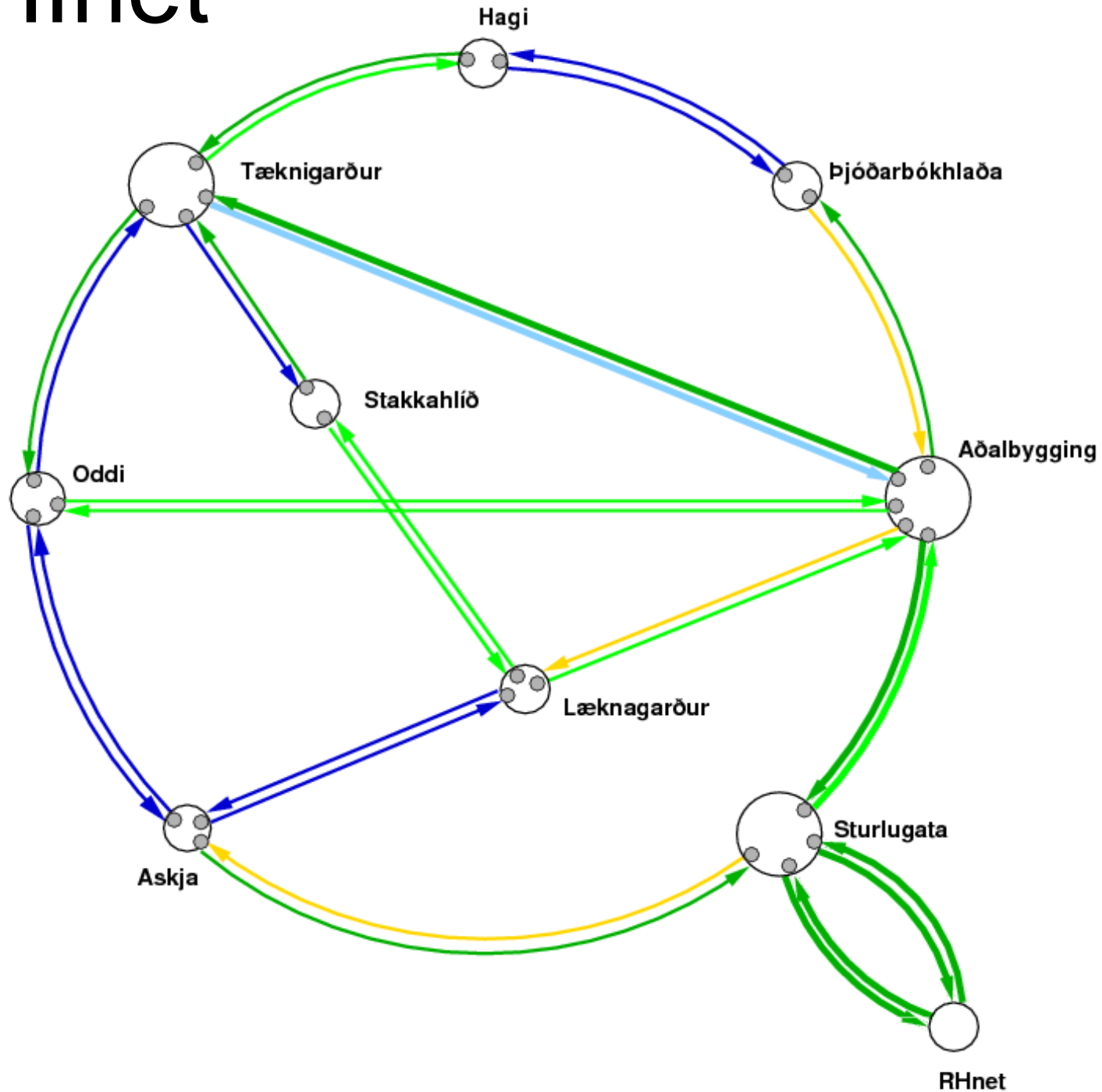


● Núverandi ástand

▢ Port

◆ SmokePing

◇ NetDisco



Hínet

	2005	2007	2008	2011
Skráðir notendur	13.759	14.461	18.231	20.638
Þar af nemendur	10.730	11.446	14.864	17.549
Skilgreind tæki	8.837	10.917	12.870	17.021
Þar af í léni RHÍ	4.289	5.912	8.017	12.361
ADSL notendur	1.716	1.186	1.082	870
Þráðlaus netkort	6.588	9.021	13.648	19.902
Notendur á Görðum	596	708	709	770

Rekjanleiki & ábyrgðarskylda

Notendur skrá macaddressu tölvunnar / símans til þess að fá aðgang að þráðlausu neti HÍ

Macaddressa er skráð á notendanafn viðkomandi

Nemendur geta skráð 2 macaddressur

DHCP úthlutun á WiFi

– IP tala -> Macaddressa -> Notandanafn

Rekjanleiki & ábyrgðarskylda

Sást síðast	Mac	IP	Nafn
30.03.2012 17:30:16	00:26:5e:2b:8c:45	130.208.107.4	s8-dw004.rhi.hi.is
30.03.2012 14:30:20	00:26:5e:2b:8c:45	130.208.79.28	tg-eduroam-28.rhi.hi.is
30.03.2012 12:30:05	00:26:5e:2b:8c:45	130.208.105.77	od-eduroam-13.rhi.hi.is
27.03.2012 14:30:24	00:26:5e:2b:8c:45	130.208.107.125	s8-dw125.rhi.hi.is
27.03.2012 09:30:12	00:26:5e:2b:8c:45	130.208.79.163	s8-eduroam-03.rhi.hi.is
03.03.2012 16:30:04	00:26:5e:2b:8c:45	130.208.105.116	ag-eduroam-20.rhi.hi.is

Rekjanleiki & ábyrgðarskylda

IP	Mac	Not/Vél	Sást fyrst	Sást síðast
130.208.115.38	70:1a:04:fb:f6:12	spj3	2012-04-02 09:22:00	2012-04-02 16:21:14
130.208.115.38	70:1a:04:fb:f6:12	spj3	2012-03-29 12:30:25	2012-03-29 19:46:01
130.208.115.38	70:f1:a1:27:11:86	krb31	2012-03-28 09:15:57	2012-03-28 14:44:58
130.208.115.38	70:f1:a1:27:11:86	krb31	2012-03-27 11:07:31	2012-03-27 15:51:43
130.208.115.38	70:f1:a1:27:11:86	krb31	2012-03-26 12:46:09	2012-03-26 15:48:59
130.208.115.38	78:ca:39:b4:06:9c	smk5	2012-03-23 08:14:16	2012-03-23 15:10:30
130.208.115.38	00:27:10:ab:5d:0c	ktm	2012-03-21 08:57:41	2012-03-21 15:53:09
130.208.115.38	c4:46:19:0e:ed:83	ruk1	2012-03-16 08:24:22	2012-03-16 10:53:45

Rekjanleiki & ábyrgðarskylda

Þráðlaus:

00:0c:e7:45:4f:af ingimar-2 Tenging?
00:17:f2:49:89:55 ingimar-0 Tenging?
00:1c:9a:1b:45:01 ingimar-3 Tenging?
00:24:07:4e:e6:4c ingimar-4 Tenging?
00:24:d7:4e:e6:4c ingimar-5 Tenging?
00:26:5e:2b:8c:45 ingimar-1 Tenging?

Rekjanleiki & ábyrgðarskylda

DMCA kvartanir – áframsent sjálfvirkt

Vírus – macaddressa fær ekki auðkenningu
í RADIUS

SPAM – viðkomandi notandi fær tilkynningu

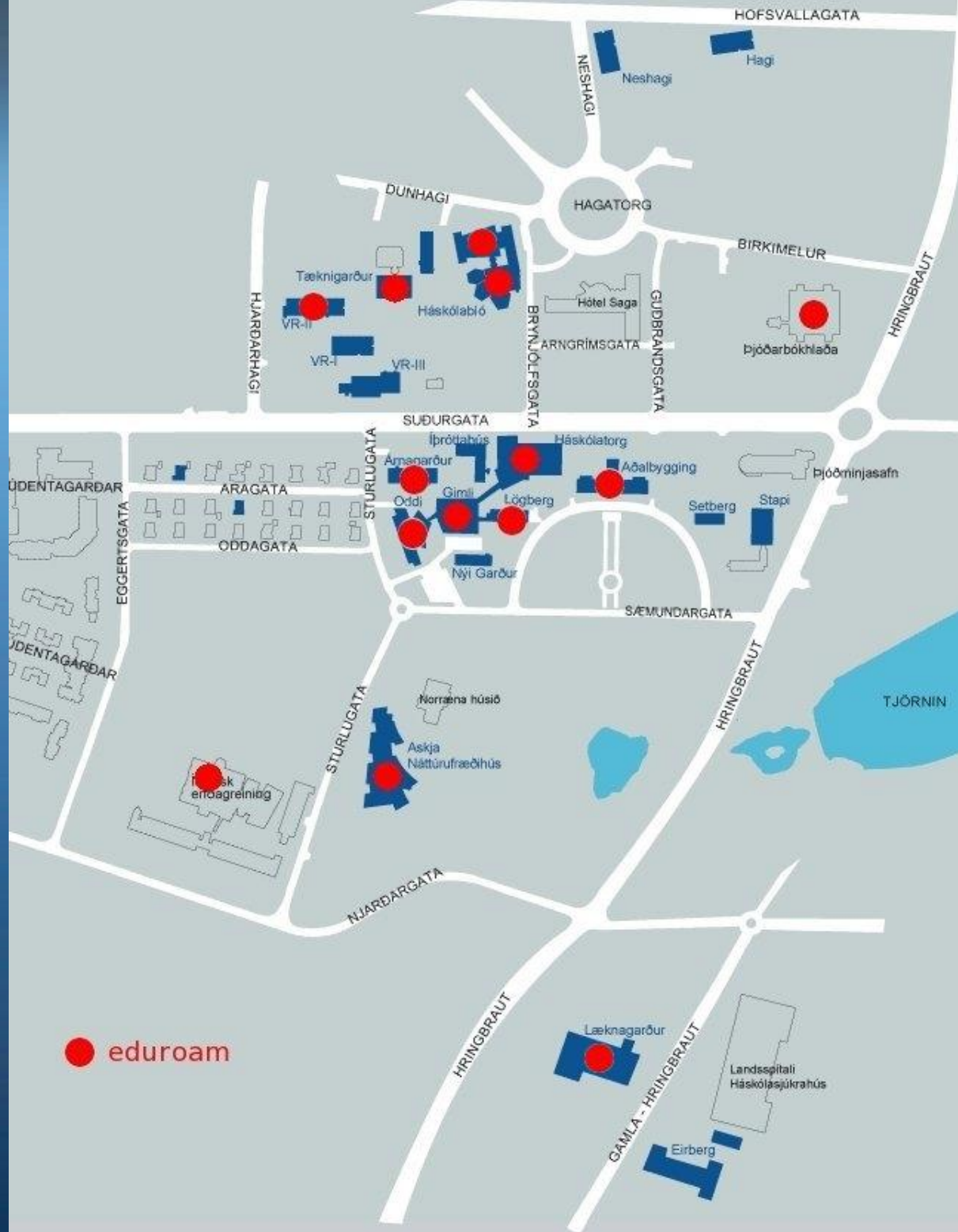
Rekjanleiki & ábyrgðarskylda

Macaddressu auðkenning + WEP :-)

Næsta útfærsla verður eduroam – 802.1X

Helstu stillingar fyrir eduroam eru;

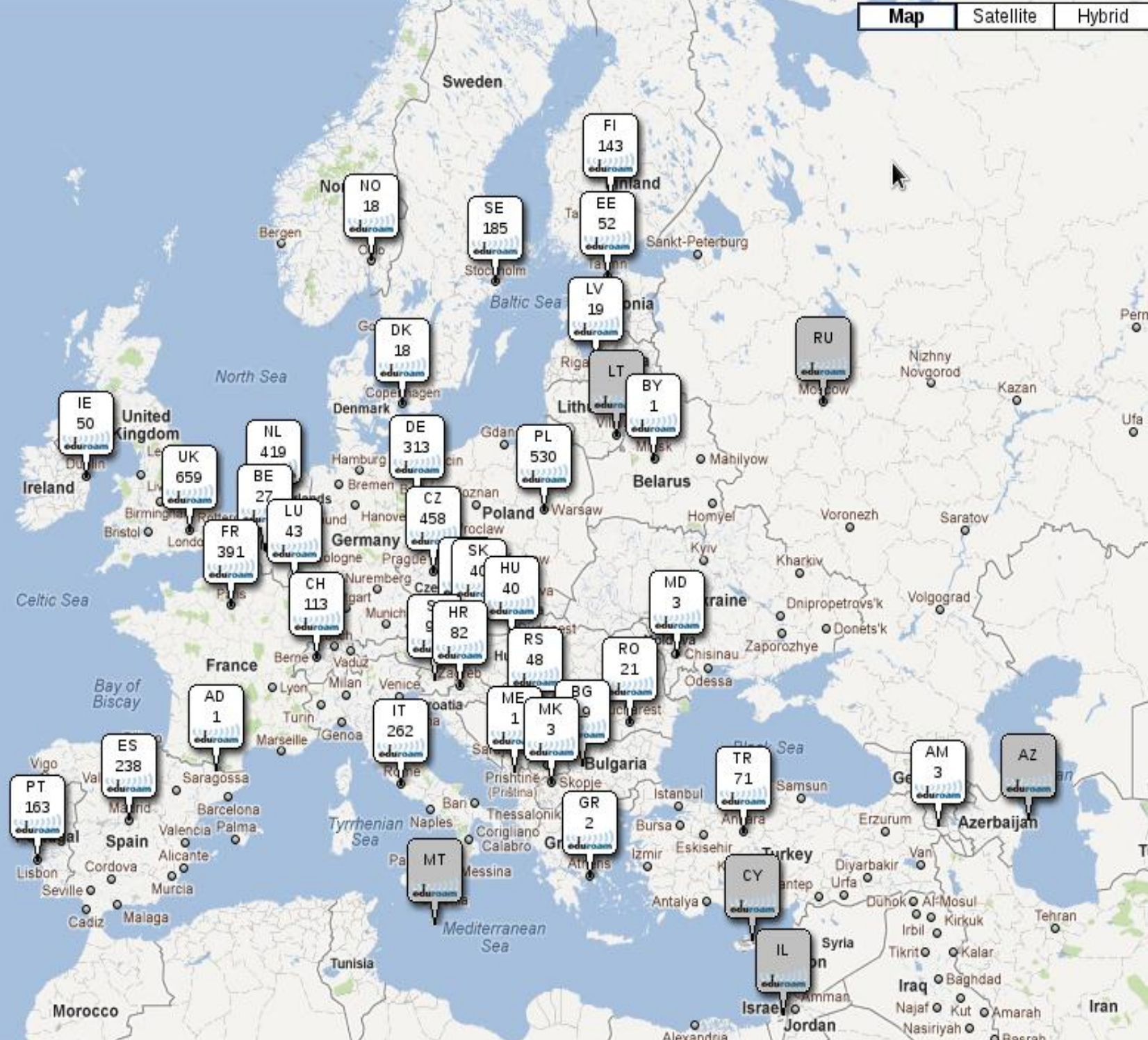
- Auðkenning/authentication: IEEE 802.1X
- EAP tegund/type: TTLS or PEAP
- Tunneled authentication protocol (TTLS or PEAP): MS-CHAPv2
- Notandanafn: notandanafn@hi.is + Uglu lykilorð
- WLAN SSID: eduroam
- Encryption (WLAN): TKIP (WPA) or AES (WPA2)
- IP address: DHCP



● eduroam



IS 18
eduroam



Til athugunar

Cisco 3560E-12D – Macaddressu tafla er bara 2k “directly-connected Ipv4 hosts”

WEP encryption á 802.11n sendum gerist í software – ekki hardware

- Það næst aldrei meira en 54Mb hraði á 11n sendum ef encryption er WEP

Hvernig lokum við á macaddressu þegar auðkenning er 802.1X?

- Post process í FreeRADIUS – macaddressu blacklist

Takk fyrir