# Mobility Task Force

## Summary of specific technical issues raised by the TF Mobility list

*Last updated 28.05.03*
*Updated by James Sankar*

This is a "living" document created from technical discussions on the mobility mailing list. All TF Mobility members are encouraged to add items to this list. If you have any specific information about wireless or authentication please share your knowledge with the mobility mailing list at **mobility@terena.nl**

**Q: What happens when multicast is streamed over wireless to a wireless client?**

A: Observations in Italy show that multicast can stream over the wireless link to a wireless client, however when the client moves to connect to another access point, the multicast sessions remains but continues to stream from the previous access point and the new access point and so on. If one is not careful multicast will take most of the shared bandwidth.

**Q: How can I set up Bluetooth, GPRS connection and IPv6 for an iPAQ 3870 with Linux?**

A: See the details at http://dnsv6.iihe.ac.be/iPAQGPRSv6/BtConfig.html

**Q: Do you know the current position/plans of the regulation for 802.11a (and other 5.8ghz products such as Tsunami bridges) in Spain?**

A: The exact regulations are not completely known to me, but this information might help. As I understand it, the European union dictates that, in order to be allowed to transmit in the 5GHz band, the transmitter must support Automatic Frequency Selection when a carrier frequency is already in use, and it also must adjust its transmitted power according to the other transmissions in the 5 GHz area. Work is in progress to include these two features, which will lead to 802.11h. However, Intel and Philips have 11a products that are certified, as they say: http://www.80211-planet.com/news/article/0,4000,1481_1008161,00.html. They probably have proprietary mechanisms built in that implement these two features. Since most EU countries try to unify their policies on spectrum and bandwidth allocation, I suspect that the situation in Spain will be(come) the same.

**Q: Have there been any tests of 802.11g equipment?**
A: See http://www.nwfusion.com/reviews/2003/0512rev11g.html

**Q: Are there any web based solutions commercially available today? Also did anybody try the authentication solution provided by the NoCat gateway (http://nocat.net)? It seems interesting, even though based on filtering by ipchains, but would like to know about some practical implementation results?**

A: See http://www.nomadix.com/applications/wifi-hotspots.asp. The Portuguese University of Coimbra is testing the nomadix solution, which seems to run quite well, with the advantages of a captive portal (service differentiation, pricing, and so on). However, it requires the use of a VPN server: the gateway allows VPN tunnels established, but does not incorporate a VPN server. Actually there are quite many this kind of commercial and free solutions to do web page based authentication. Most of these also support also VPN pass-through or termination or it's possible to add it later. Some of the solutions include

Vernier Networks (commercial):
http://www.verniernetworks.com/

Nokia Public Access Controller (commercial):
http://www.wbs.nokia.com/networks/product_catalog/pc_product_highlights/1,6929,,00.html?prod_id=RAS00090&path=tmcat&mcat=45796&scat=48256&tech_id=517

NoCatNet (free): http://nocat.net/When starting to work on TUT Public Access Architecture last year I tried NoCat, but at least then the development seemed to be based heavily on the community network they had. It wasn't very easy to separate and configure the software to be used in different kind of environment than the developers were using. It may be better now and it seems to have quite a lot of features. We (FCCN) on the other hand, are currently using another free software called Oasis as the access controller software. Oasis has a few annoying bugs which have lead me to think about writing own access controller
software,

Oasis (free):
http://software.stockholmopen.net/index.shtml

HUPNet (free):
http://www.helsinki.fi/~vviitane/hupnet/

All these devices or software are able to authenticate against Radius and are therefore compatible with the Radius-based roaming solution.