To:
Aileen Chia (Ms)
Deputy Chief Executive (Policy, Regulation & Competition Development)
Director-General (Telecoms & Post)
Infocomm Media Development Authority
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438

From:
Lee Shu Yuan (Max)
IT Executive (Previously in Education Sector)
Freelance IT Technician (For Homes, Ad-hoc basis)
93897846
dj_symx@hotmail.com

**Table Of Contents**



## Security Requirements for Residential Gateways(Opening)

Home IT infrastructure are setup unlike for business where enterprise level of hardware is used as well as establishing policies such as network security etc.
In an enterprise network, security protocols are established to ensure no authorized access from outsider and etc.

For Home IT Infrastructure to setup like business IT infrastructure is not ideal, not to mention "Consumer" grade of network equipment are usually straight forward to setup and configure. Without need of technical knowledge or certification to handle such equipment.

I have noticed there are no IT service provider who provide maintenance or repair for home IT equipment except installation or delivery of IT equipment. Mainly due to profit margin as charges could not be too high to cater to all income group.

Here are my comments about the following points in the public consultation.

## Requirement for Credentials such as login and WIFI

Different manufacturer routers have different preloaded settings like login credentials.
For example, Linksys routers during initial setup, there is a window where user could set up their desired credentials for the router and WIFI.

If users were to skip the Setup wizard, the user credentials for the router would be set to the defaults. Having random password prior before sale maybe a good ideal, ultimately educating users on setting such password on their own would be much ideal than factory randomizer password.

My suggestion would be during at the point of sale:
- Sales person could give a checklist of what to do after the router is purchased.
- Inside the checklist, password requirement such as combination of both numeric and alphabet numbers.

Verifying the checklist can be done either by requesting for the checklist to be attached to the warranty card and some manufacturers will need the warranty card to be mailed back.
Another issue with randomizing password is what if the router needed to be service?

Does it mean a new set of passwords would be required after the service?

**Device Setup & Administration**

Universal Plug and Play (UPnP) pose security risk thus in a commercial network, UPnP are required to be turned off to prevent authorized access from outsider etc. In a home network, there are network activities like multiplayer online gaming players from Singapore connect and play with those from overseas.

If UPnP are to be make turned off mandatory which will mean activities such as multiplayer gaming would be disabled. There are work around if UPnP is turned off which is enabling certain ports for such services to work but it will pose high security risk.

My view about UPnP is it not only depend on end user device as well as activities.
Game consoles are generally safe as they network are govern by respective companies such as Sony and Microsoft.

Any vulnerabilities they would announce and realize any firmware to ensure the game console are not affected. PC wise if educating users to purchase anti-virus with firewall solutions from Bitdefender etc.

It would help to ensure that network activity/traffic from PC are not intrude by anyone during multiplayer gameplay or any online activity when one is connected to another network/server.

Generally, most uses either free anti-virus software or Windows defender to protect their PC.
Other than network activity, if UPnP is turned off mandatory home network will be much difficult to setup since one must assign IP address for each device and connect them manually to the network.

Which is practice in business environment but not at home and technical knowledge will be required.
UPNP is turned on which is a default setting for most routers thus it makes easier for end users to connect their devices.

**Firmware Updates**

This is a subjective topic as different manufacturer have different implementation for firmware updates. Similarly, like setting up the router different manufacturers have different ways of setting up as well as user interface.

Manufactures like Linksys have automated firmware meaning if there are new firmware release, it will install on its own. However, router unlike PCs that runs Microsoft Windows operating system doesn't require Windows monthly updates to patch vulnerability.

Firmware may release at one point in time or so to address certain vulnerability or issues with the product itself. Another factor why firmware isn't release frequently is because unlike PC, firmware may cause issues or make router unstable.

Enforcing firmware update would not be ideal thus the ideal solution would be considering engaging companies who could provide home IT maintenance. Such service provider/vendor could assist to setup home network and provide maintenance when required especially if there is a firmware update.

When there is firmware update, they would ensure it is updated properly and if in one home there are more than one router or uses WIFI extender etc. They will ensure after the firmware update, other devices are working properly and not disconnect.

Which is one reason if routers are working fine, end-user would leave it as it is to minimize disruptions. Retailers like Challenger does provide installation for network equipment purchase but as the installation charges are rather high thus some choose to do on their own.

I quote based on my experience when using Asus routers which release new firmware once every few months. Despite it fixes vulnerability down the road but there have been several incidents the router failed after firmware update thus I am not in favour of frequent firmware update.

**Conclusion**

Much of the point in the public consultation, educating users on "IT Best practices." Would be ideal. Most routers do have certain feature mentioned in the public consultation but whether users are aware of them as well as understand what will be required of them after the router is purchased.

Most users are not IT savvy nor study in the field of IT thus most will not understand certain aspects raise in the consultation except password requirement is straight forward. Home network are straight forward thus just plug and play and, it would be feasible for an IT service provider who can assist with repair, maintenance and educating users on "IT Best practices" at home.

Due to profit margin as such business is not profitable, considering freelancers who can provide such service could be another viable option. My focus has been on End user side but not the equipment as I phase it this way.

If you own a fast car but driver doesn't know how to operate it than the car potential isn't reached. Network is one aspect of security but what about end user devices? Not all household owns latest PC that runs on Windows 10 etc. some are using older PCs running Windows 7 or Windows 8.1.

As well as purchase of anti-virus solution with firewall like Bitdefender as most uses either free anti-virus solution or Windows defender to protect their PC. More support such as subsidies like "Education pricing" for those who are still using old PCs or dated PCs could be considered as well as software.

Regards,
Lee Shu Yuan