



The Future Internet

**Lessons from the Past and
Indications for the Future**

Peter T. Kirstein, UCL

Plan of Talk

- **Short history of previous migration to IPv4**
 - **Impact on migration to IPv6**
 - **Impact on revolutionary change in Internet**
- **Factors impacting take-up of IPv6 features**
 - **Struggle between desirable features and legacy positions**
- **Other critical challenges in future**
 - **Deliberate sabotage of critical infrastructure**
 - **Responsibilities in multi-party systems**
 - **Individual optimisation vs common good**

Not to be addressed

- **Most of the important issues raised in the excellent MANA paper presented to this forum**
- **Detailed questions of management and control of the future Internet**
- **The Activities of any particular project under the FIA Action Plan**

Some Lessons from Past

- **Change of protocols was already hard in '80s**
 - **Very much more difficult now**
- **Even fairly small change IPv4→IPv6 long**
 - **More radical change will not happen**
- **IPv6 has many desirable features**
 - **Commercial and other pressures have watered some fo these down**
 - **Look at Mobility, security and NATs**

Changing Internet Protocols

- Compare IPv6→IPv4 with NCP→TCP
 - **Though this change comparatively small**
- Scale of NCP → TCP many orders of magnitude less on any measure
 - **Next two slides show magnitude of changeover and times of first one**
 - **Do not believe that radically different Internet will happen by design**
- **Remember failure of Internet → GOSSIP**

The Scale of Changeover

- | | | |
|--|--|---|
| <ul style="list-style-type: none">• Item<ul style="list-style-type: none">– Nodes– Countries– Computers– Users– Services– Protocols– Real-time, Security, QoS, mobility, NAT support• Changeover | <ul style="list-style-type: none">• NCP→IP<ul style="list-style-type: none">– 50+– 1+– 200+– Thousands– ~ 10– tens– None• Months | <ul style="list-style-type: none">• IPv4→IPv6<ul style="list-style-type: none">– 10s of millions– Hundreds– 100s of millions– Billion– Hundreds– Hundreds– Lots• Decade?? |
|--|--|---|

The Timeline of Changeover

- **Item**
 - **Defined**
 - **Implemented**
 - **Piloted**
 - **Dual stack**
 - **Service**
 - **Changeover**
 - **Really worked**
 - **New Protocols**
 - **Protocol Development**
- **NCP→IP IPv4→IPv6v6**
 - '74 '93-'00
 - '75-'79 '98-'05
 - '78-'80 '04-'09
 - '81/'82 '05-??
 - '06 ???
 - '83 ???
 - '84 '05
 - '83-'04 '03-???
 - **Ongoing Ongoing**

Discarded Aspects of IPv6

- **Very difficult to force through changes unless user, entrenched supplier and regulatory agencies agree**
- **Examples where Mandatory Requirement have had to be weakened to optional**
 - **Mobile IP**
 - **IPSec**
 - **Only end-end communications**

Mandatory Mobile IP

- **Mobile Telephone Operators unwilling to weaken customer control through SIM card**
- **Multi-homing support also both technical and political problem**
- **New support for mobile networks (NEMO)**
 - **Little interest from conventional suppliers**
 - **New Applications Suppliers interested**
- **Ad-hoc networks important option (MANEMO)**
 - **Again little supplier support**
 - **New Applications Suppliers interested**

Mandatory IPSec

- **Key exchange protocols not really accepted**
- **Extra complexity not always acceptable performance**
 - **May require hardware assist**
- **Alternate forms of security like VPN often preferred**
 - **Easier to achieve corporate control**
- **Some countries do not permit encryption**
 - **Others require key deposition**

The End of NATs

- **Clearly NATs hide corporate network**
 - **Corporations often prefer them even if not needed for address shortage**
 - **Even some home users may prefer it for security**
- **Constraints on legal interception capability**
 - **Important for some regulatory climates**

Possible Routes for Introduction

- Just substitution of IPv4 current services by IPv6 ones slow route to migration
 - Protocol coexistence, e.g. dual-stack, vital for acceptance
- Fact that some new protocols defined only for IPv6 a more cogent reason
 - 6LoWPAN, MANEMO, Stateless Address Autoconfiguration, Renumbering aids
- Where new large-scale systems have to be introduced with new hardware
- E.g. Internet of Things
 - Crisis management, smart metering, smart energy/green ICT
 - Need *ad hoc* collaboration, autoconfiguration, sensor nets, security, mobility, large-scale addressing

Some other Challenges

- **Proven safety of critical infrastructure**
- **Proven applicability, attainability and responsibility of SLAs**
- **Optimising performance for the individual without endangering all**
- **Meeting user requirements in single network economically**
- **Any form of migration from here to there**
- **Enforcing decisions internationally**

Proven safety of critical infrastructure

- **Always hard but has depended on some trust**
 - **Have not faced the consequences of concerted efforts by outside nations**
- **Of course has been tackled in military systems**
 - **But has included restriction of suppliers**
- **But Civil systems are also critical**
 - **telephone, power generation, all utility transmission, government information, industrial processes**
- **Restraints on suppliers for all above serious**
 - **Large impact on costs and hence economic prospects**
 - **Potentially very serious impact on trade agreements**
- **Major technical challenge to prove correctness**

Proven applicability, attainability and responsibility of SLAs

- **SLAs often reflect pattern of usage envisaged by suppliers**
 - **May be quite different from that expected by user**
 - **real-time over ADSL**
 - **Actual duration of occupancy through queuing**
 - **Down-time of service**
- **Supplier may define for his service; customer may expect on end-end basis**
- **May be difficult to determine reason for shortfall**
 - **May be very hard to assign responsibility in systems with multiple organisations involved**

Optimising Individual vs Mass

- **Old Internet envisaged benign participants**
 - **E.g. TCP had exponential back-off if congestion**
- **Cannot rely on this now**
 - **If behaviour gives economic or performance advantage, it will be used.**
 - **Standards bear this in mind, but users or suppliers can avoid constraints in standards**
- **Clear that applications are becoming network-aware and networks application-aware**
 - **How can impact on fairness be judged, optimised and controlled?**

Meeting user requirements in single networks economically

- Often user organisations need conflicting characteristics for different applications
 - High availability, high bandwidth, low jitter, low cost, widespread availability
- Often not all the above are needed together
 - High availability needed for some traffic
 - High bandwidth occasionally
 - Low jitter only for voice
 - Widespread availability only for limited services
- Yet organisations want limits on the number of networks, gateways and commercial contracts

Disinclination to Migrate

- **Even if alternate suppliers offer almost the same services, users may find migration hard**
- **If there is a real difference in the systems interfaces, suppliers may have to hide almost all the differences by migration aids**
 - **Often these preclude use of advanced features – thus reducing the incentive to migrate**
 - **Significant and widespread training and changes may be needed to take real advantages of features**

Enforcing Decisions Internationally

- The various bodies like the IGF are grappling with who should judge what to legislate – and how to enforce any such rulings
- The early IETF was a model of how to legislate for, and make work, a complex system
 - It took many decisions on Protocols
 - They were defined fairly easily, and adopted willingly
- Recent activities there show how difficult this becomes when vital interests are involved
 - It has proved very difficult to enforce them
 - It is becoming increasingly difficult to make any such decisions really mandatory internationally

Conclusions

- **A radical change to the Internet will not happen**
 - **Only progressive changes to meet urgent problems**
 - **Even with mechanisms to reduce impact on users**
- **Great care must be taken in introducing even important features, if they might disrupt established markets and practices**
 - **Though there is an opportunity if the feature is important enough – like Skype or SPAM filters**
- **Must resolve problem of proving safety of critical infrastructure**
 - **Or require major expense to protect the infrastructure**
 - **And threaten widespread undermining of WTO**