ITU-D Regional Development Forum for the Asia Pacific Region

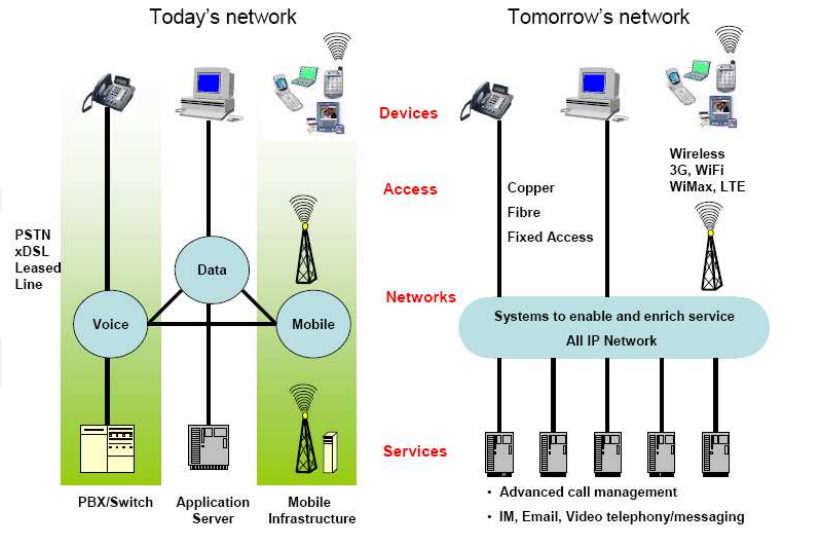
"NGN and Broadband, Opportunities and Challenges"
Yogyakarta, Indonesia, 27 – 29 July 2009

Regulatory and security issues arising from the migration to the NGN

Mr. Eric Lam,
Assistant Director
Office of the Telecommunications Authority (OFTA), Hong Kong China

Agenda

- NGN
- Evolution of the IP-based NGN Platform
- NGN Standardization
- Interconnection and Interoperability
- Cybersecurity Aspects
- Anti-Spamming in Hong Kong, China



- Separate networks for difference services
- Equipment duplication
- Service duplication

- One network for converged services
- Multi-service network
- Service creation and use simplified

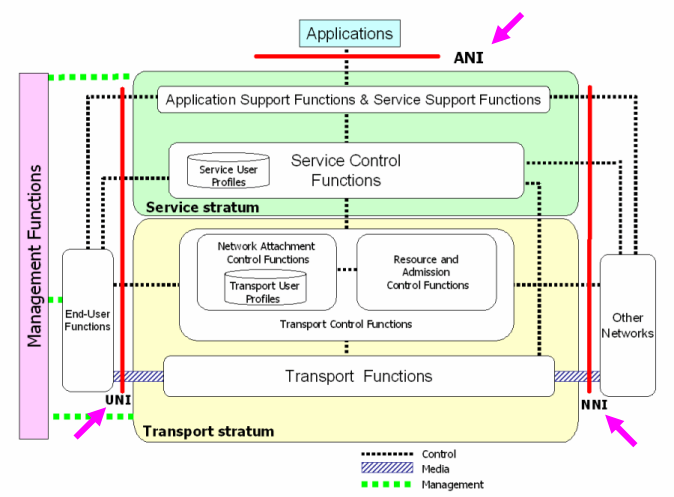
Evolution of the IP-based NGN Platform

- Existing networks are designed to serve only a particular service.
- Existing multi-network approach suffers from high operation and maintenance cost.
- It lacks the flexibility for service innovation and time to market.
- Market competition and technologies advances driving more and innovative services as well as integration of voice, video, and data services
- Service providers are finding it becoming more challenging to address market need based on existing solutions.
- Require a network to support all services to meet today's market need.
- A new IP based platform that can provide multiple services to fulfil the nowadays and future requirements is needed.

Important NGN features

- Single IP-based core network handling an operator's full range of telecoms services, whether fixed or mobile.
- Support for multiple access network technologies.
- Seamless interworking with legacy networks.
- Distributed rather than centralised switching, routing and network intelligence.
- Offers unrestricted access by users to different service providers.
- Supports generalized mobility to allow consistent and ubiquitous provision of services to users.

NGN Architecture



Source: ITU-T

NGN Architecture

- No standard architecture for NGN.
- In general, NGN would comprise (i) user network, (ii) access Network, and (iii) core network.
- Access networks are various like xDSL, cable modem, Ethernet, WiMax, WiFi, 3G and etc.
- Core networks must be optical fibre basis such as SONET/SDH, Metro Ethernet, ATM for high capacity and efficient transmission.
- Three Layers in NGN operation
  - Application Layer
  - Service Control Layer
  - Transport and Access Layer

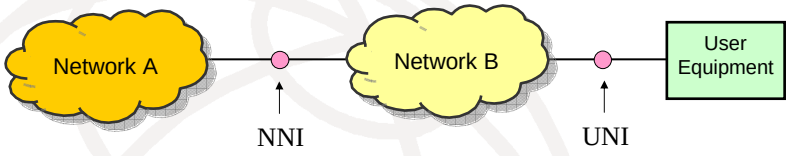
NGN Standardization

- IETF can be considered to be the founder of the NGN. It created SIGTAN, a set of important standards for the reliable transport of signalling over IP networks
- IMS specifications from 3GPP relatively mature, some IMS products from vendors
- Some standards from IETF referenced by ITU, ETSI, 3GPP specifications
- SIP-I for NGN-PSTN interworking relatively well standardized
- SIP identified as NGN signalling protocol

Interconnection and Interoperability

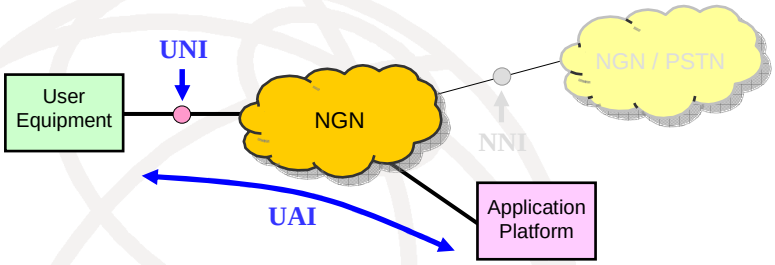
- ITU recommendations on NGN-PSTN interworking (between SIP and C7, i.e. SIP-I) is well standardized e.g. Rec. Q.1912.5.
- ITU has published the NGN Network-to Network Interface (NNI, for NGN-NGN interworking) and User-to-Network Interface (UNI for NGN-NGN interworking) signalling profiles based on SIP for multimedia services, e.g. ITU-T Rec. Q.3401 NNI SIP Profile
- ETSI and 3GPP have adopted ITU's recommendations on SIP with some modifications, e.g. TR29.865

Interconnection and Interoperability



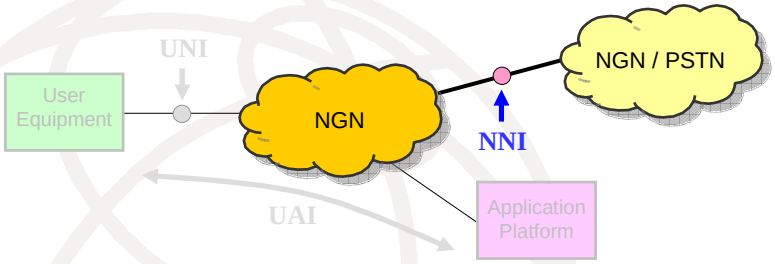
- **UNI standards**
  =>to ensure interoperability of user equipment with telecommunications system
- **NNI standards**
  =>to ensure compatibility of interfacing equipment between interconnecting networks

Interconnection and Interoperability



- In addition to UNI, Standards on User-to-Application Interface (UAI) may also be required
- May need requirements on codec, QoS, security to ensure service interoperability

Interconnection and Interoperability



- NGN supports multiple services => different interconnection requirements for different services
- May need to identify services to be controlled, and interconnection scenarios: NGN-NGN, NGN-PSTN
- May need requirements on physical layer, signalling protocol, IPv4/IPv6 interworking, QoS, security

Network Security

- NGN is an open network and rides on IP technologies that security threats happening in the Internet world may also occur in telecommunications networks
- Coordinated measures and safeguards may be required to cope with the growing complicated security issues in NGN
- NGN operators would implement appropriate security measures to safeguard their facilities
- User protection is an important element in NGN security

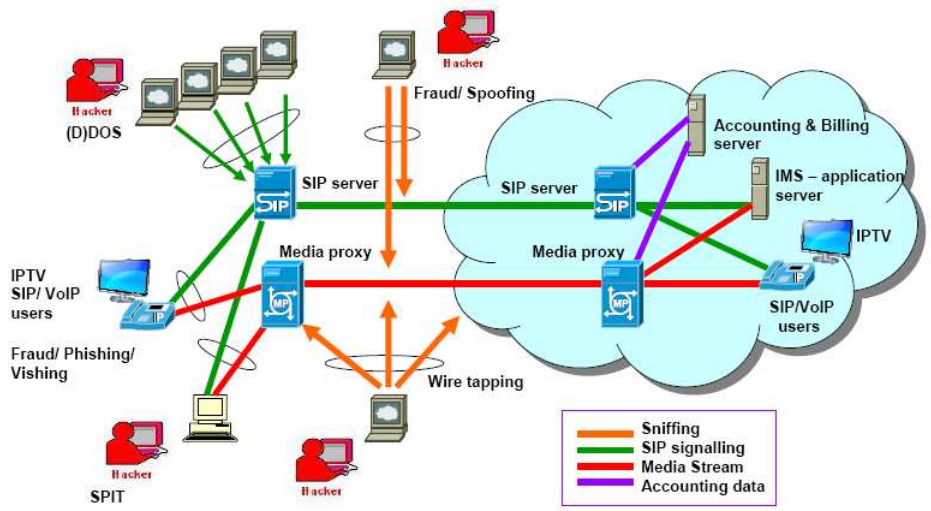
ITU's definition on Cybersecurity

- Cybersecurity refers to "the prevention of damage to, unauthorized use of, exploitation of, and if needed, the restoration of electronic information and communication systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems"

Cyber Threat or Cyber Attack

- Following the change of electronic communications systems from the conventional TDM based to IP based operation, public telecom networks which are generally classified as critical infrastructures could be subject to cyber threat/attack
- Examples of cyber threat hampering the safety and security of internet are
  - Malware
  - Spam
  - Phishing
  - Botnet etc

Variety of Security threats in NGNs



Source: ETSI

International awareness

- Many countries have established or appointed organisation(s) and group(s) to look after cybersecurity issues, including the development and implementation of
  - plans to protect "critical infrastructures"
  - public awareness and education programmes etc.,
  - international coordination etc.

Arrangements in Hong Kong (1)

- Lead Policy Bureau – the Security Bureau
- Lead Government Agency – OGCIO
  - The Government Information Security Incident Response Office (GIRO) to provide central advice and co-ordination to bureaus and government departments on overall information security management and operations
  - HKCert to provide a centralised contact on computer and network incident reporting and response for local enterprises and end users

Arrangement in Hong Kong (2)

- Ad Hoc Groups during special events/for special tasks
  - Internet Infrastructure Liaison Group comprising members from OGCIO, OFTA, the Police, HKCert, HKIX, HKISP and HKDNR to ensure better coordination to ensure stability, security, availability and resilience of the local internet infrastructure during special events
  - A special task force with close cooperation between OFTA, HKDNR, HKCert and the Police to identify and suspend spamvertised.hk domain

Arrangements in Hong Kong (3)

- Special arrangements for some business sectors, e.g. the banking sector
  - close collaboration between Hong Kong Monetary Authority (HKMA), the Police and HKCert to tackle cyber threats/ attacks to the banking Sector
  - relatively stringent guidelines on cybersecurity measures for banks

Hong Kong Experience

The problem of Spam

- Spam has been identified as one of the most important vehicles for carrying cyber attacks.
- Various industry reports indicate that spam emails accounted for a significant proportion of email traffic. For example, MessageLabs (*) estimated that spam emails on average accounted for 81% of email traffic in 2008.

* MessageLabs Intelligence 2008 Annual Security Report

Anti-spam Legislation in HK

- After two rounds of public consultation and legislative debate, the Unsolicited Electronic Messages Ordinance (UEMO) was passed in June 2007.
- Came into full effect in December 2007, in line with the establishment of the Do-not-call Register (DNC).

Other Anti-spamming measures

- Legislation is only one of the measures.
- Government has launched the STEPS campaign to fight the spam epidemic with a basket of measures as follows:-
  - **S** – Strengthening existing regulatory measures
  - **T** – Technical solutions
  - **E** – Education
  - **P** – Partnerships
  - **S** – Statutory measures

Technical Measures - Anti-spam Code of Practice for ISP

- Code of Practice issued by Hong Kong ISP Association (HKISPA) in June 2005, which among other measures, suggest ISPs to:
  - Block outgoing port 25 (SMTP) for switched access clients
  - Restrict the amount of outgoing mail provided to web email and pre-paid accounts
  - Disallow email relay from third parties in mail servers
- Many ISPs are also:
  - Providing spam filtering for residential email users
  - Rate limit outgoing mail to minimize the impact of botnets

Technical Measures - Spamvertised Domains

- HK Domain Name Registration Company Limited (HKDNR) has put in place various measures since mid 2007 against suspicious websites like phishing or domains being advertised in spams.
- Daily reports of these cases dropped significantly.

Partnership - International Co-operation

- HK has joined with other 11 agencies in the Asia-Pacific region in the Seoul-Melbourne Multilateral Memorandum of Understanding (MoU) on Co-operation in Countering Spam.
- The MOU encourages:
  - closer cooperation among the signatories in minimising spam originating in or passing through each country/region;
  - the exchange of information on technical, educational and policy solutions to the spam problem in accordance with the relevant laws of each country/region.

Thank you !!!

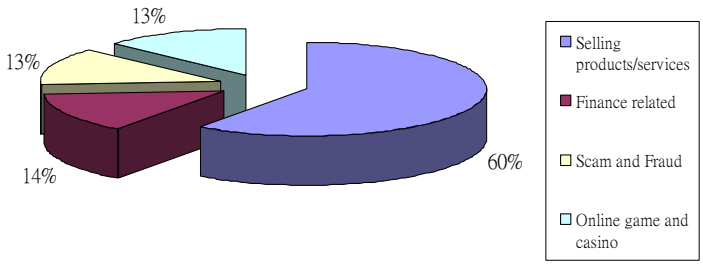
Eric Lam

elam@ofta.gov.hk

ITU-D Regional Development Forum for the Asia Pacific Region

- Back up Slides

Categories of Spam



Source from Symantec - The State of Spam Reports for November 2008 to January 2009

- Promotion of products or services continue to occupy the majority of spam.

Six Sending Rules

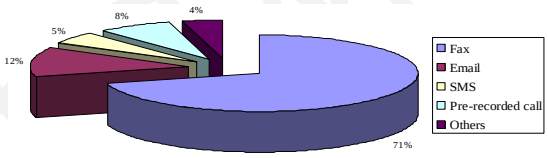
1. Provide accurate sender information
2. Provide free unsubscribe facility
3. Honour unsubscribe requests
4. Not to send messages to numbers listed on DNC
5. Not to use misleading subject heading in emails
6. Not to withhold calling number display when sending messages from a telephone or fax number

Penalty for Contravention of the Sending Rules

- Telecommunications Authority to issue Enforcement Notice (EN) to direct the sender to remedy the contravention
- Contravention of EN
  - First conviction: a fine up to HK$100,000 (about US$12,820)
  - Second and subsequent conviction: a fine up to HK$500,000 (about US$64,100)
  - An additional daily fine of HK$1,000 in case of continuing offence (about US$128)

Enforcement Statistics

- By end of Mar 2009, about 10500 reports received:



- Enforcement Actions taken:
  - Warning letters (71)
  - Enforcement notice (1)
  - Prosecution (0)