ITU-T Kaleidoscope Conference
Innovations in NGN

Architecture for Broadband and Mobile VPN over NGN

Masahisa Kawashima
NTT Information Sharing Platform Laboratories
kawashima.masahisa@lab.ntt.co.jp

Geneva, 12-13 May 2008

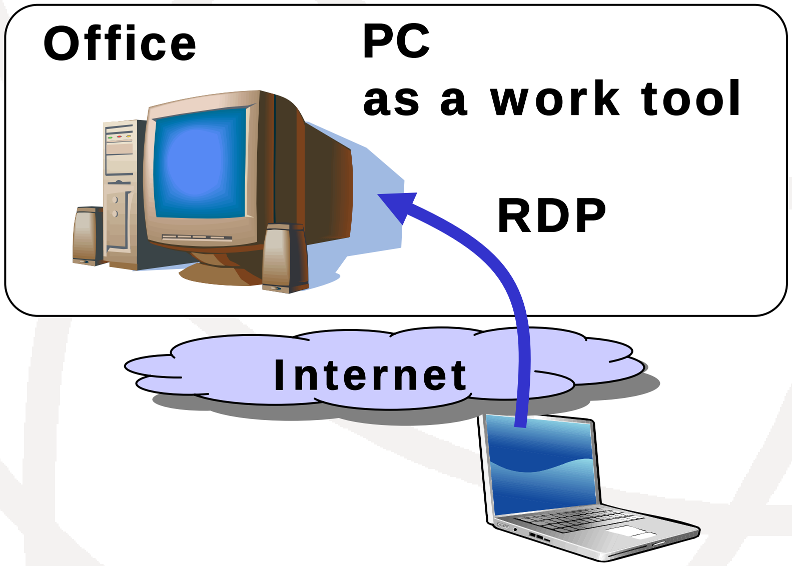
Architecture for Broadband and Mobile VPN over NGN

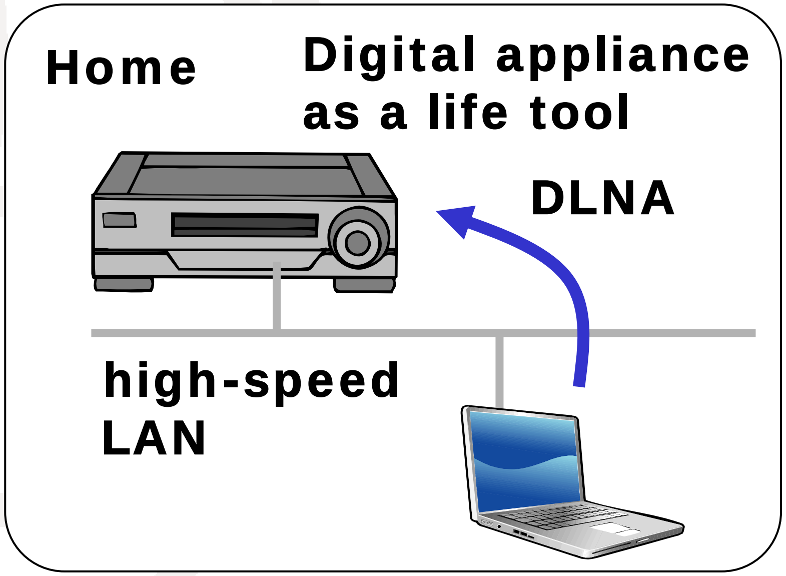
Outline

1. Background and objective
2. Usage model and requirements
3. Existing technologies: IKE/IPsec + Mobile IP
4. Proposed method: SIP Dial-up
5. Evaluation
6. Business opportunities and standardization issues
7. Summary

Background

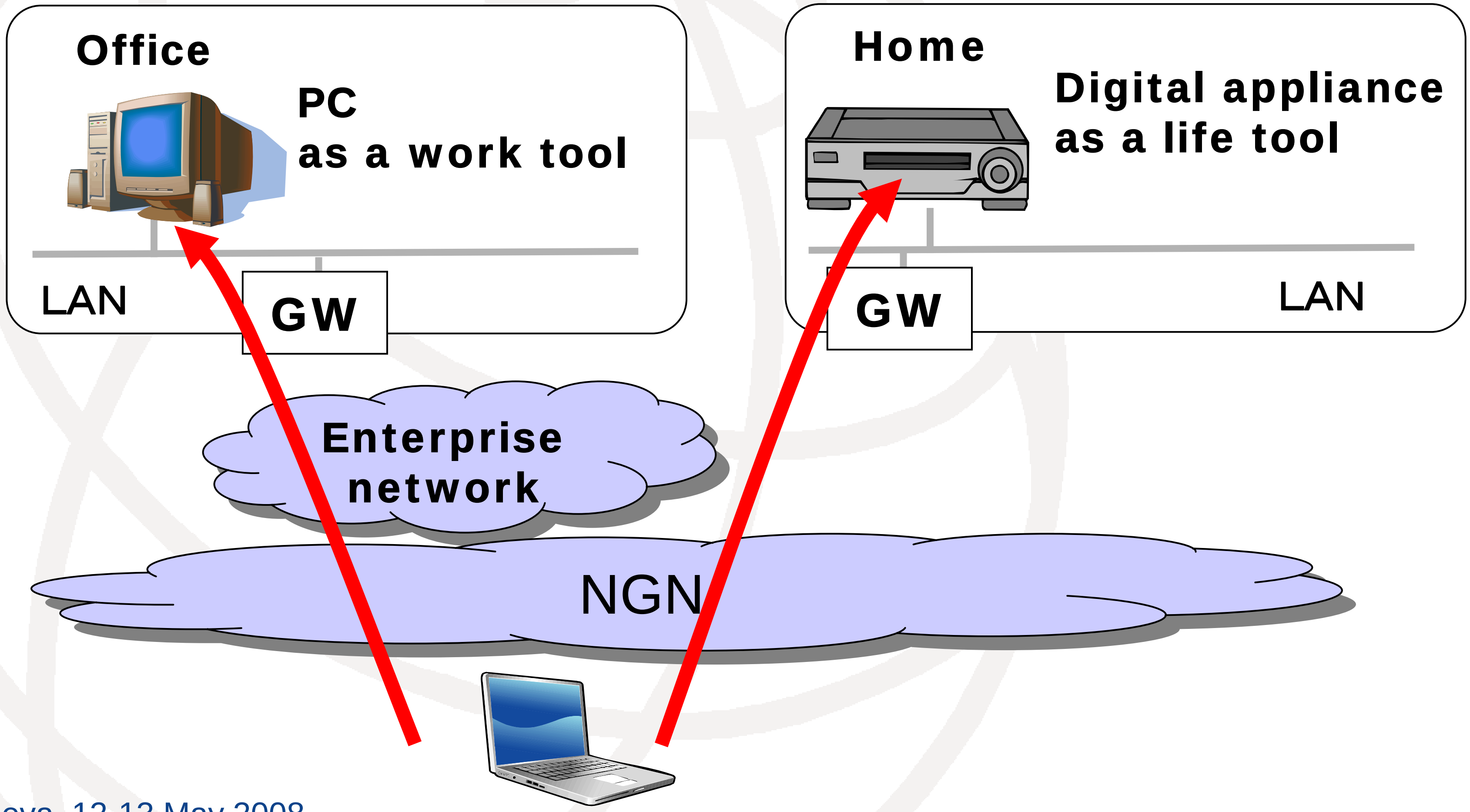
- Many tools have become digital
  - at office: PC for documenting and organizing data
  - at home: digital appliances, e.g. video recorder
- Tools have remote service capabilities
  - RDP for PC: Experience depends on network QoS
  - DLNA for digital appliances: Only within LAN





Objective

- To achieve remote access to digital tools with global mobility and stable QoS



Important assumptions on usage

- Ordinary users
  - Consumers and small businesses
  - may not be skillful enough
- Multiple LANs inside enterprise network
  - for office-LAN access
  - e.g. per business unit, per location
  - possibility of attacks inside enterprise
- LAN applications
  - Bandwidth-consuming
  - No application-level encryption
  - Communicates with users' private IP
- Multiple access networks
  - Users hop between access networks

Requirements on VPN method

- Req 1: Protection of VPN gateways from malicious traffic
  - VPN gateways are maintained by ordinary users
  - Packet filtering by network or firewalls
- Req 2: Separation of VPN gateways from firewalls
  - There may be attacks inside an enterprise network.
  - NAT traversal for VPN gateways is required.
- Req 3: Reservation of QoS
  - Some applications require stable QoS.
- Req 4: Hand-over of VPN session (Application continuity)
  - Re-starting applications would be inconvenient.
  - Location management and session maintenance

Existing technologies

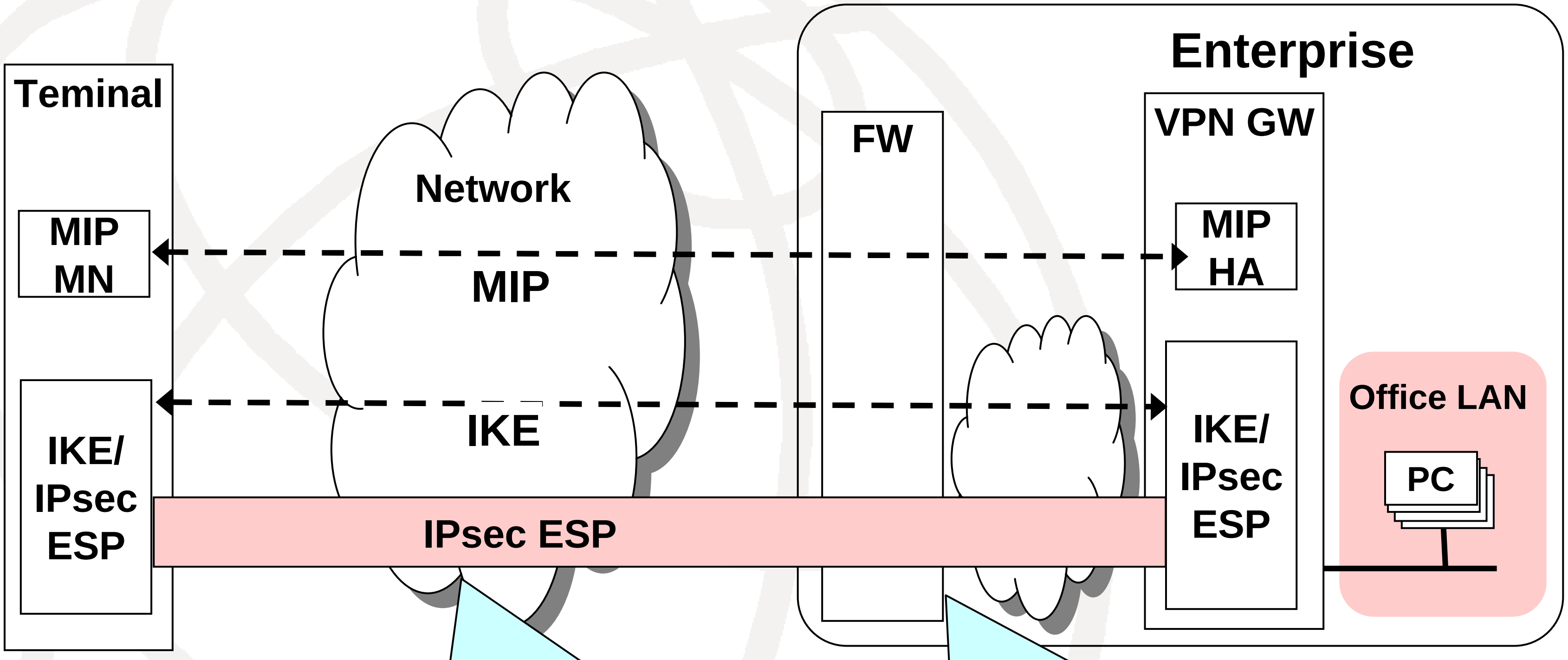
- Internet Key Exchange (IKE)
  - VPN session establishment
  - Authentication between VPN entities
  - Key management for VPN

- IPsec
  - tunneling communication with private IP
  - packet encryption

- Mobile IP (MIP)
  - IP-level location management for application continuity
  - Packet forwarding by Home Agent (HA)

Implementation with Existing Technologies

MIP HA (Home Agent) and IKE/IPsec functions are co-located in VPN GW.



cannot recognize set-up and tear-down of VPN sessions. (difficult to achieve QoS reservation and packet filtering)

cannot authenticate incoming VPN requests nor identify the target GW. (difficult to achieve NAT traversal)

Evaluation of existing technologies

- IKE/IPsec and MIP alone cannot fully satisfy the requirements.

Requirements	Evaluation
R1: protection of VPN gateways from malicious traffic	NO
R2: separation of VPN gateways from firewalls	NO
R3: QoS reservation	NO
R4: Hand-over of VPN session	YES

Dilemma between end-to-end and network involvement

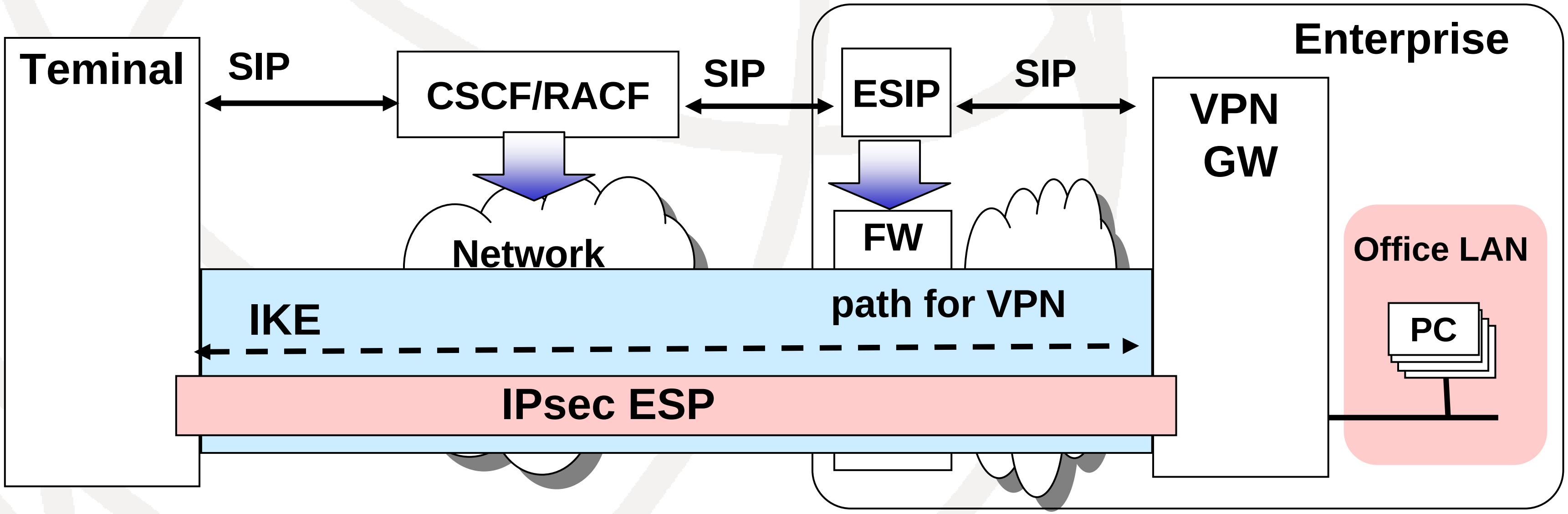
- Design philosophy of IKE
  - Chooses End-to-end approach
  - Reasonable for assuring end-to-end security
  - Prevents connectivity management and security enhancement by intermediate nodes

This dilemma can be solved by complementing IKE with SIP.

Proposed method: SIP Dial-up (SIP-DU)

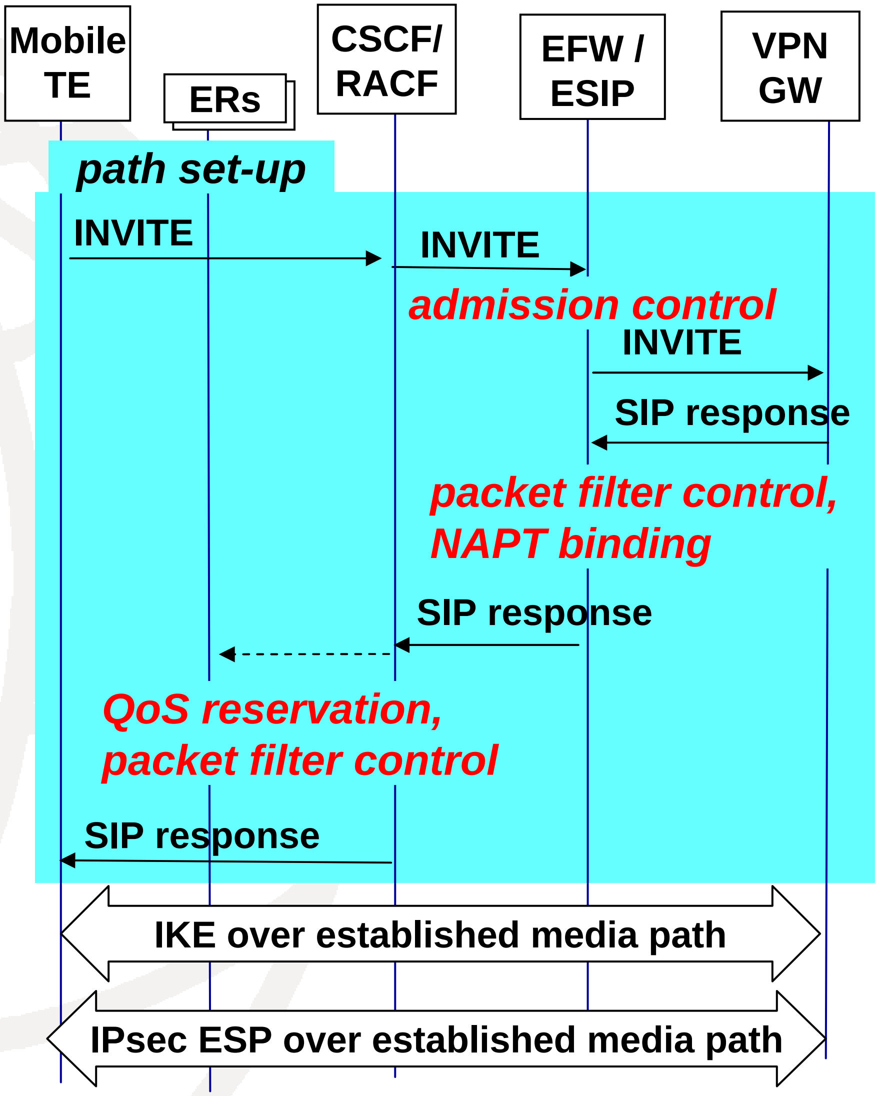
By complementing IKE with SIP, the proposed method achieves

- **Security enhancement**
  - **SIP-based authentication and admission control**
  - **Dynamic packet filtering**
- **Connectivity management**
  - **QoS reservation**
  - **Addressing target VPN gateways for dynamic NAPT binding (NAT traversal)**



Protocol operation: Session establishment

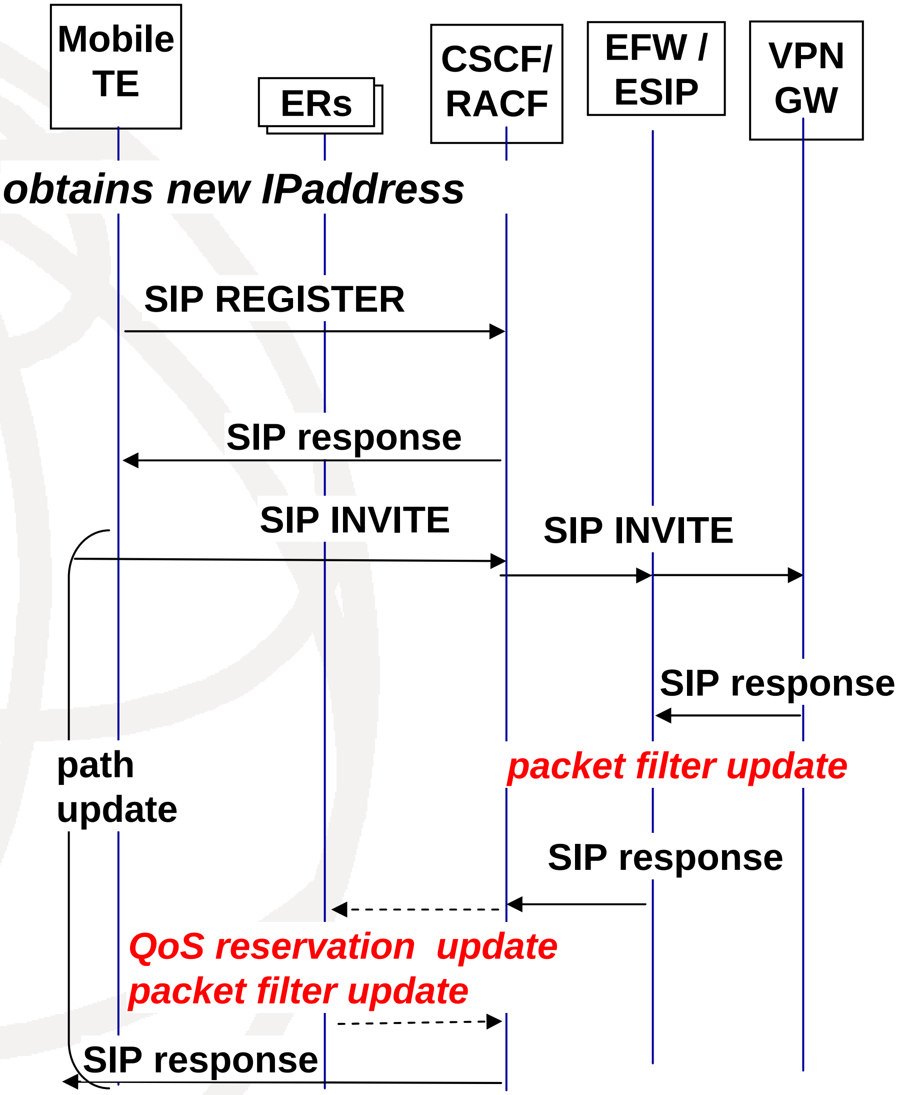
- Path set-up by SIP
  - before starting IKE/IPsec
  - a UDP-based media path
  - Security enhancement
    - admission control
    - dynamic packet filtering
  - Connectivity management
    - dynamic NAPT binding
    - QoS reservation
- IKE/IPsec on the path



Mobile TE
ERs
CSCF/ RACF
EFW / ESIP
VPN GW
path set-up
INVITE
INVITE
admission control
INVITE
SIP response
packet filter control, NAPT binding
SIP response
QoS reservation, packet filter control
SIP response
IKE over established media path
IPsec ESP over established media path

Protocol operation: Hand-over

- REGISTER and re-INVITE
  - when terminal switches to a new access point
  - initiated by terminal
  - VPN session maintenance
    - VPN gateway updates the terminal's address for the media path
  - Connectivity maintenance
    - update packet filtering parameters
    - update QoS reservation parameters



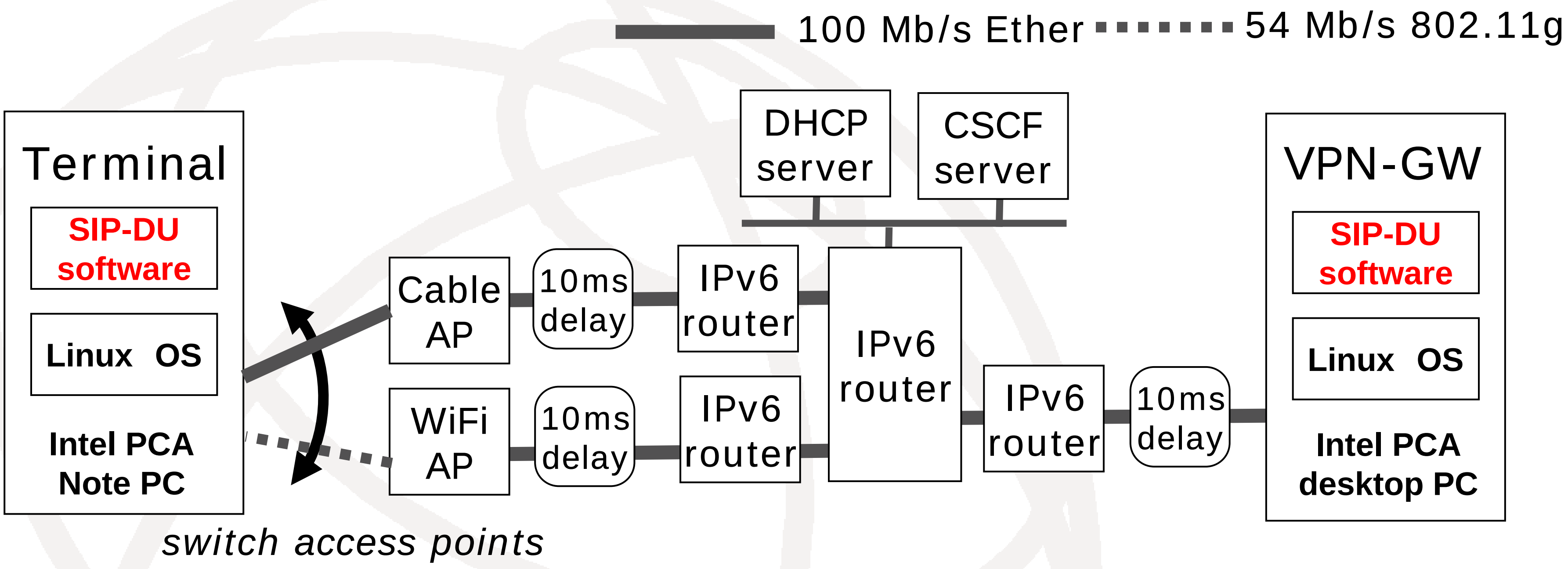
Evaluation

The adoption of SIP achieves

- Security enhancement for Req 1
- Connectivity management for Req 2 and 3
- Session and connectivity maintenance for Req 4

Requirements	Evaluation
Req1: protection of VPN gateways from malicious traffic	YES
Req2: separation of VPN gateways from firewalls	YES
Req3: QoS reservation	YES
Req4: Hand-over of VPN session	YES

Performance Test with Prototype



- **Throughput: 73.8 Mbps**
  - **rate of tunneled UDP data**
  - **when mobile terminal is attached to the cable AP.**
- **Hand-over delay: about 6.1 sec**
  - **Time for DHCP, SIP re-REGISTER and re-INVITE.**
  - **SIP re-REGISTER with IMS-AKA is the major component (4.5 sec).**

Expected opportunities

- For users
  - Work-style innovations with ubiquitous access to office
  - Innovations in appliance usage with ubiquitous access
- For device vendors
  - Office products with new functions for remote access
  - Home appliances with new function for remote access
  - Sales of VPN gateways to consumers and small businesses
- For NGN carriers
  - VPN services for consumers and small businesses

These opportunities can be maximized with standardization efforts.

Standardization benefits and issues

- Benefits of standardization
  - proliferation of SIP-DU products
    - mobile terminal
    - VPN gateway
  - assures global mobility
    - SIP-DU across NGN carriers with roaming agreement
- Standardization issues
  - System architecture and message flows
  - Tunneling protocols to be supported
    - Many alternatives: IPsec ESP/UDP, PPP/SRTP/UDP, Ether/SRTP/UDP, PPP/L2TP/IPsec/UDP, etc
  - SDP descriptors for tunneling protocols

Summary

- Objective: Broadband and mobile VPN over NGN
  - to achieve remote access to essential tools in office / home LAN with global mobility and stable QoS
- Proposed method: SIP Dial-Up
  - complements IKE with SIP
  - achieves security enhancement and connectivity management by intermediate nodes
- Opportunities
  - innovations in work-style and appliance usage
  - products with new remote access functions
- Standardization
  - maximize opportunities
  - standardization issues: system architecture and message flows, supported tunneling protocol, SDP descriptors