Hasso Plattner Institut

IT Systems Engineering | Universität Potsdam

Challenges of IPv6: Security and New Applications

Seminar for Master of IT System Engineering (WS2010/2011)

Ahmad AlSadeh

Feng Cheng, Sebastian Roschke, and Prof. Dr. Meinel

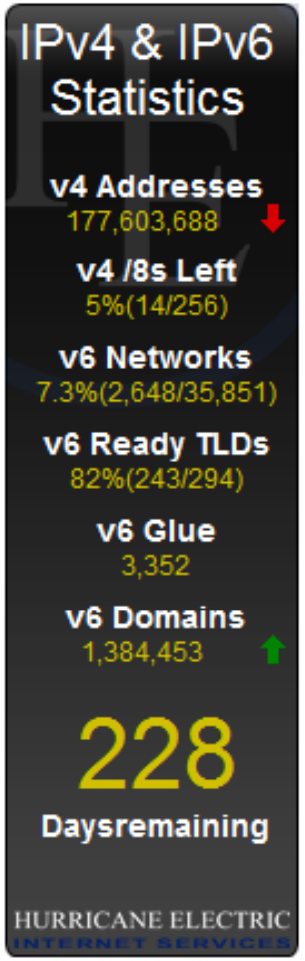
Outline

- Motivation
- Quick overview of IPv6
- Seminar topics
- Organization
- Evaluation

Motivation

Motivation (1)

- 2^{32} total addresses **-> 4 billion**
- IPv4 addresses are not enough for all new devices
  - Laptops, mobiles, GPS, other online devices
- IPv4 is full, only **5%** of IPv4 are left
- IPv4 probably will run out before **2012**
  - IANA pool depletion date: 170 days (08.04.2011)
- NAT is a temporary solution
  - NAT breaks end-to-end network
- IPv6 is the next generation Internet protocol



Motivation(2)

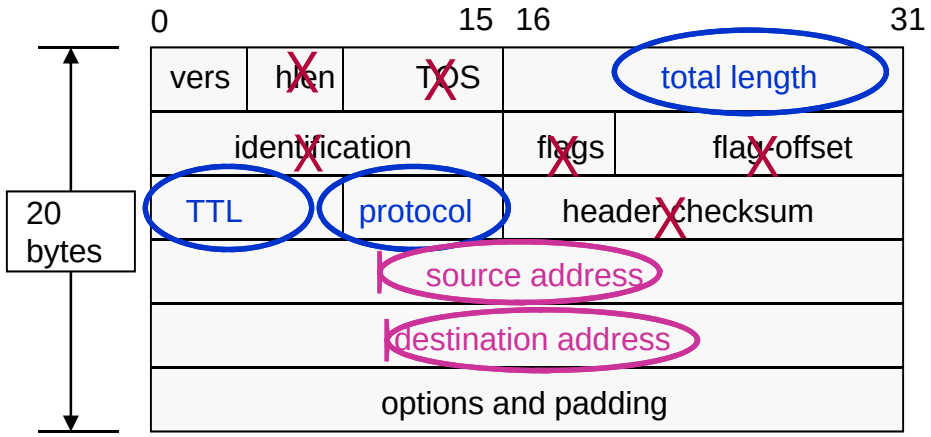
- IPv6 means Internet and **business continuity**
  - Everything on the Internet over IP
- **You have to be ready**
  - IPv6 is widely available and it is enabled by default in many systems
  - IPv6 is expected increasingly deployed in the coming few years
- IPv6 comes with new features
  - Security
  - Autoconfiguration
  - Extensibility
  - …
- IPv6 will coexist with IPv4 for long time
- **This seminar** will discuss both challenges of:
  - IPv6 security issues
  - IPv6 new applications

Quick overview of IPv6

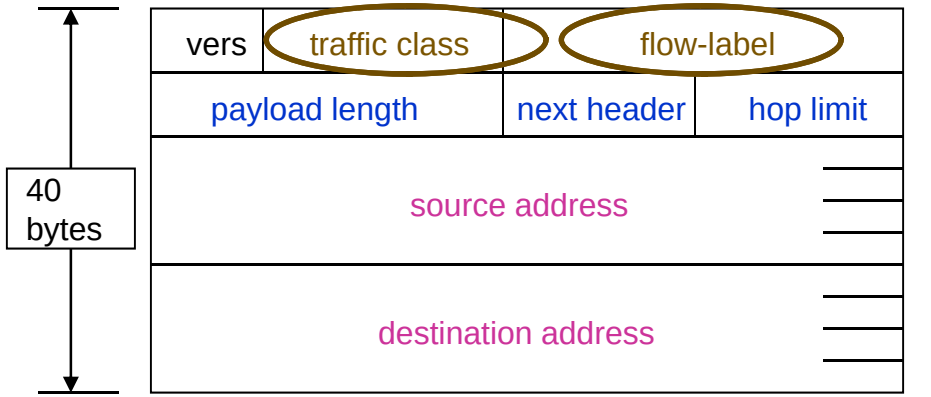
IPv4 & IPv6 Comparison (addresses)

	IPv4	IPv6
Address Size	32-bit number	128-bit number
Number of Addresses	2^{32} = 4,294,967,296 = **4 billion** addresses	2^{128} = 340,282,366,920, 938,463,463,374,607,431, 768,211,456 =**340 trillion trillion trillion** addresses
Address Format	Decimal notation: 192.146.200.67	Hexadecimal notation: 2001:5Feb:Beef::Cafe
Prefix Notation	192.146.0.0/**24**	2001:5Feb:Beef::/**48**

IPv4 & IPv6 comparison (headers)



IPv4



IPv6

Removed (6)

- hlen, TOS
- ID, flags, flag offset
- header checksum

Changed (3)

- total length => payload
- protocol => next header
- TTL => hop limit

Added (2)

- traffic class
- flow label

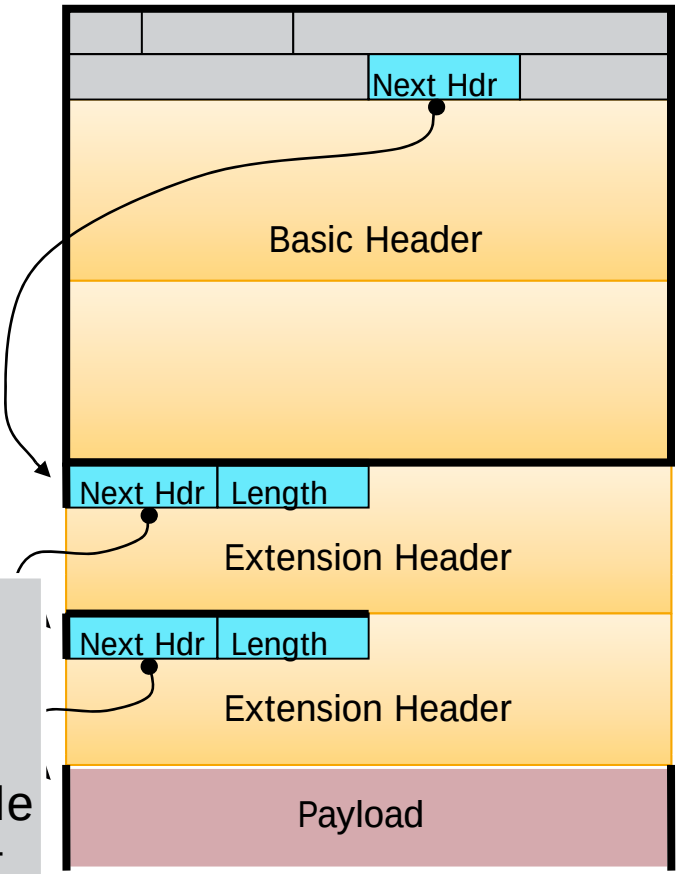
Expanded

- address 32 to 128 bits

Extension headers

- Extension Header Types
  - Routing Header
  - Fragmentation Header
  - Hop-by-Hop Options Header
  - Destinations Options Header
  - Authentication Header
  - Encrypted Security Payload Header

IPSec



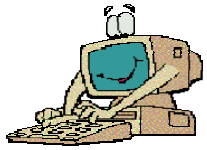
Security concerns:

- Manipulate a malicious packet is possible
- Header chain can make filtering difficult

Address configuration

Three ways of configuration:

1. Manual (Least preferred, but possible)
2. DHCPv6 → required a Server
3. **Stateless Autoconfiguration**



Prefix	Interface Identifier

IPv6 Address

Prefix can be

- Link-Local address (FE80::/64)
- Global Unicast address
  - Routers send periodic Router Advertisement (**RA**) which contains link prefix, lifetime, MTU, etc.
  - Host may also send router solicitation (**RS**) to get trigger RA

The interface ID generated by

- EUI-64→ Formed from MAC address of interface
- Randomly generated → Provides some level of privacy
- Cryptographically Generated Addresses (CGA)
- Possible other methods in the future

Neighbor Discovery Protocol (NDP)

- **Neighbor discovery Protocol functions:**
  - Discover the presence and MAC addresses on the same link
  - Duplicate address detection
  - Discover routers
  - Detect when a local node become unreachable

- **Some of NDP messages**
  - ICMPv6 router solicitation (RS)
  - ICMPv6 router advertisement(RA)
  - ICMPv6 neighbor solicitation(NS)
  - ICMPv6 neighbor advertisement(NA)
  - ICMPv6 redirect

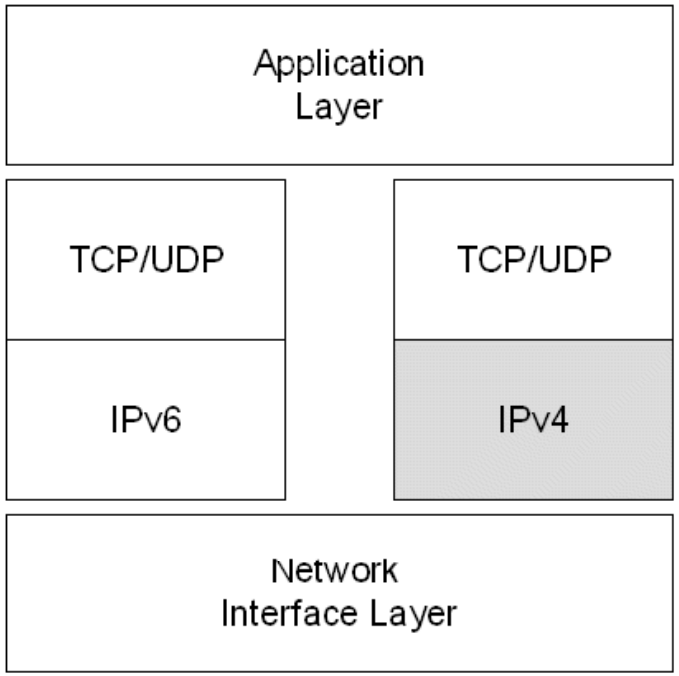
Security concerns:

- NDP has no built-in security → similar to the ARP in IPv4
- Possible attacks against NDP
  - Stealing address
  - DoS attacks
  - Forged router
  - ...

IPv6 and IPv4 Coexistence

- More than 16 methods
- Theses methods can be categorized into 3 types
  - Dual Stack
  - Tunneling
  - Translation: to allow IPv6-only devices to communicate with IPv4-only devices (deprecated by IETF)
- Expect to be used in combination

Dual Stack

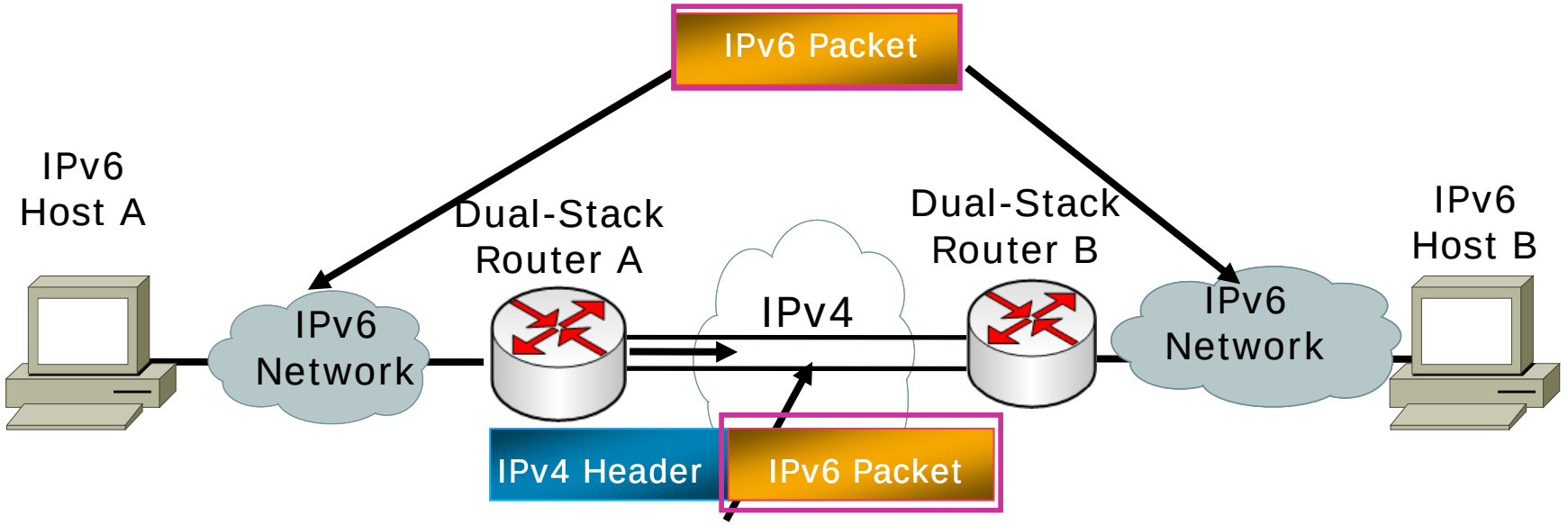


Security concerns:

- Consider the security for both protocols

Allow IPv4 and IPv6 to coexist in the same node

Tunneling

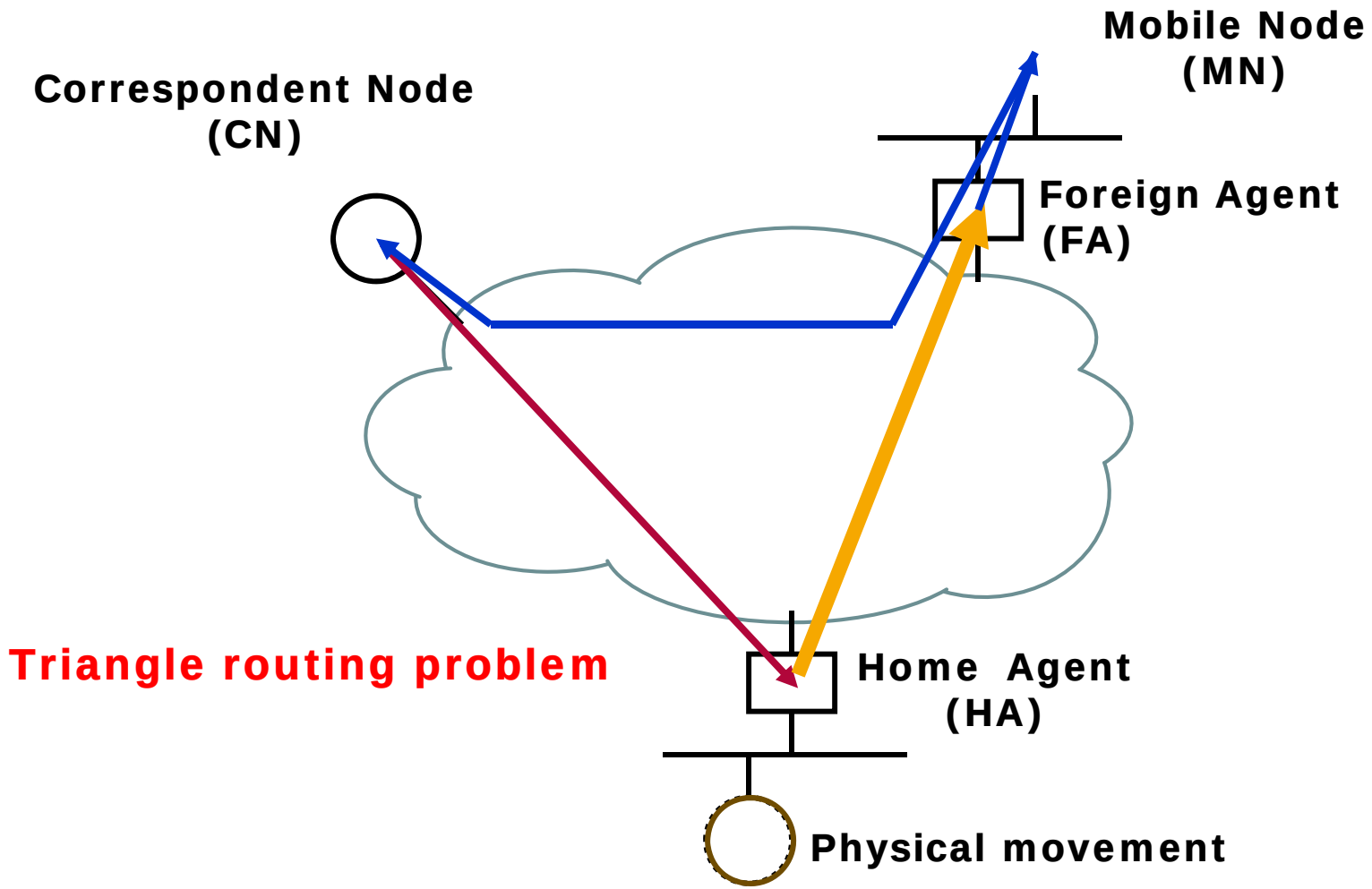


Tunnel: Encapsulating IPv6 in IPv4 Packet

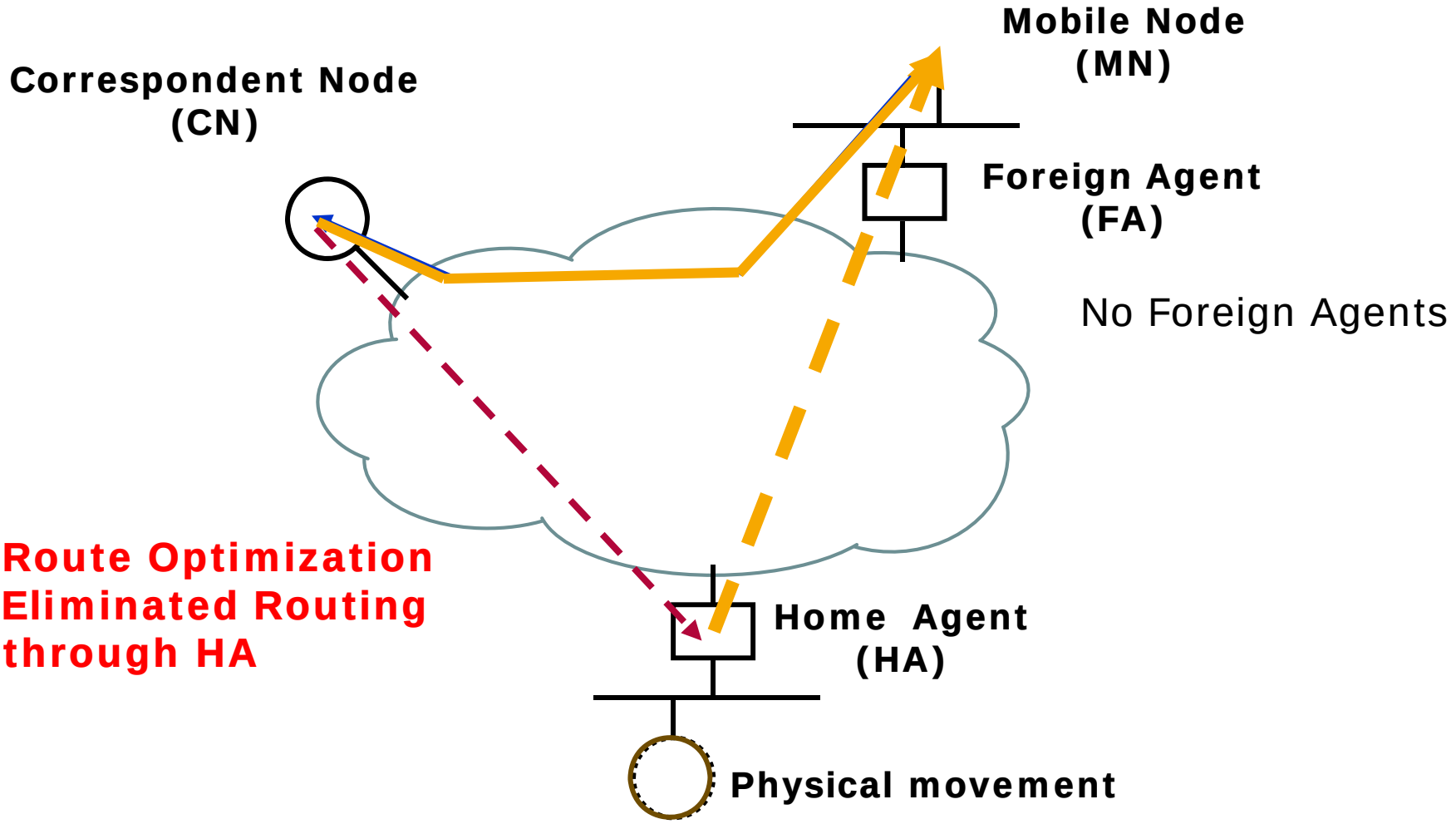
Security concerns:

- Bypass IPv6-unaware firewalls
- Provide a hiding place for DoS attacks

Mobile IP (v4 version)



Mobile IP (v6 version)



IPv6 Security

- Security was considered from the beginning in IPv6
  - IPSec useable with the core IPv6 protocol (**IPSec save the World!**)
  - Cryptographically Generated Addresses (CGA)
  - SEcure Neighbour Discovery (SEND)

Some questions:

- Why IPSec is not widely used in IPv6 network?
- Why SEND is not implemented by some vendors?
- What is the cost of deploying the CGA in limited recourses devices?

Summary of main of IPv6 features

- **Large address space**
  - Facilitating end-to-end services and applications
  - Improving address allocation and managing routing table growth
- **Simplifed header**
  - Faster header processing
- **Autoconfiguration**
  - Reduced network administration costs
- **Built-in security**
  - IPSec → mandate the implement
  - SEND→ SEcure Neighbor Discovery
- **Efficient Mobility**
  - MIPv6: More efficient and robust mechanisms
- **Others**
  - Enhanced QoS, Improved support for options / extensions

Seminar topics

Topics for IPv6 Security (1)

- **IPSec with IPv6**
  - IPSec configurations and implementation considered in IPv6
  - IPSec computationally intensive
  - Denial of Service (DoS) attacks on IPSec

  Proposed task
  - **Implement a DoS attack against IPSec in IPv6 and IPv4 environments and evaluate the effectiveness of such attack.**

  Other possible direction
  - Build a performance test for evaluating IPSec performance in IPv6 environment
  - Design automatic rekeying for Internet Key Exchange (IKE) sessions

Topics for IPv6 Security (2)

- **Cryptographically Generated Addresses (CGA)**
  - Secure IPv6 applications using CGA
  - CGAs generation and verification take a long time to be computed

  Proposed task
  - **Implemented interaction module between the central server (e.g. DHCPv6) to do the computation of CGAs and distributed it to other nodes inside the LAN**

  Other possible direction
  - Implement and interactive module between IPSec and CGAs

Topics for IPv6 Security (3)

- **Neighbor Discovery and Secure Neighbor Discovery (SEND)**
  - If NDP is not secured, it is vulnerabilities to several attacks
  - SEND is proposed to avoid NDP threats
  - SEND is **not** implement in many systems

  Proposed task
  - **Implement misuse detection and prevention to mitigate NDP threats based on IPv6 protocol analysis**

  Other possible direction
  - Security analysis and performance evaluation of SEND

Topics for IPv6 Security (4)

- **IPv6 Firewalls**
  - IPv6 firewalls is not exactly mapped to IPv4 firewalls

  Proposed task

  - **Design and implement successful penetration on IPv6 firewalls by manipulating possible attacks by using the IPv6 extension header or other new property comes with IPv6**

  Other possible direction

  - Build a distributed IPv6 firewalls

Topics for IPv6 Security (5)

- **Threats of IPv6 transition mechanisms: Dual stack, tunneling**
  - Analysis the transition techniques from security point of view
  - Find how these techniques may affect the existing defense mechanisms such as Firewalls, IDS

  Proposed task
  - **Design and implement succesful new attaks based on the IPv6 transition mechanisims**

Other topics for IPv6 Security (6)

- **IPv6 based IDS and IPv6 Anomaly traffic monitoring**
  - IDS design and implementation for IPv6 environment

  Proposed task

  - Building intrusion detection models based on IPv6 protocol analysis and how the IDS works if IPSec is used.
- **Mobile IPv6 Security**
  - Security and privacy issues in mobile IPv6
  - Security evaluation of mobile operating system such as Windows
- ....

Topics for IPv6 Applications

Implement a new application that benifits from the new features comes with IPv6 and it is expected to work better in IPv6 enviroments

- Voice over IPv6
  - compare the QoS on IPv6 networks to IPv4 networks
- IPv6 Peer2Peer
  - P2P communication in IPv4 and IPv6 coexistance
- Multimedia stream in IPv6 networks
- IPv6 in wireless mobile devices (Mobiles, PDAs,..)
- ...

Testing environment

- Based on your topic, you can test your implementation on:
  - Virtual Machines (preferable)
  - Network simulators (Mobile scenarios)
    - OMNeT++
    - NS-3

Organization

Organization

- **3** ECTS Points
- Meeting
  - Location: HPI, Room A-2.2
  - Time: 09:15 – 10:45, Wednesday
- Web page of this seminar
  - http://www.hpi.uni-potsdam.de/meinel/lehre/lectures_classes/challenges_of_ipv6_ws201011.html
- Prerequisites
  - A good knowledge of networking concepts is assumed
  - Experience with IPv4 management is expected
- Registration
  - Send an email with your favorite **topic (Ahmad AlSa'deh)** before **27.10.2010**
  - The number is limited to **10**. First send, first get in the seminar.
  - You will receive a notification by replying to your email on **28.10.2010**

Organization

What you have to do?

- Attendance
  - You should show up in all sessions
  - Discussion and challenging questions are highly encouraged
- Select a Topic
  - Investigation, survey
- Give a Talk about your topic and your plan for implementation
  - In English
  - 25 minutes: Presentation
  - 10 minutes: discussion and comments
- Write a Report
  - In English
  - Around 8-10 pages, Springer LNCS

Organization

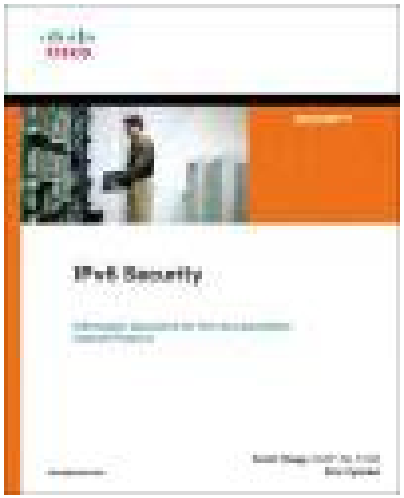
- Evaluation. Your final grade will be based on
  - Talk 20%
  - Participation in the seminar 10%
  - Implementation and testing 30%
  - Final report 40%

Important dates

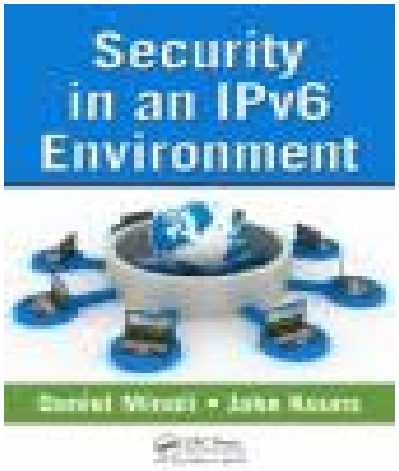
20.10.2010	**Introduction**
27.10.2010	********
03.11.2010	**Phase 0**: Assign the topics, making the groups
10.11.2010	********
17.11.2011	********
24.11.2010	********
01.12.2010	********
08.12.2010	**Phase 1**: Presentation of the assigned topic
15.12.2010	********
22.12.2010	********
29.12.2010	off
05.01.2011	********
12.01. 2011	********
19.01.2011	********
26.01.2011	********
02.02.2011	**Phase 2:** Showing the practical testing and implementation
09.02.2011	********
16.03.2011	**Phase 3**: submision the final report

Literature

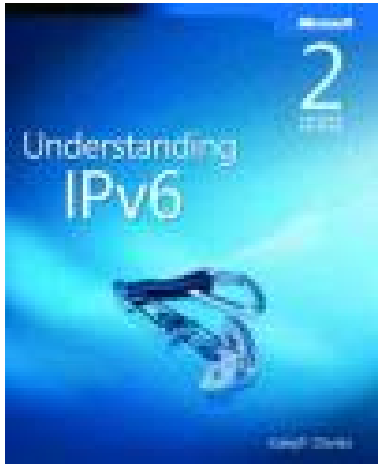
S. Hogg, E. Vyncke, IPv6 Security, Cisco Press, 2009



D. Minoli, J. Kouns, Security in an IPv6 Environment, 2009



J. Davies, Understanding IPv6, Second Edition, 2008



List of other IPv6 Books

http://www.goipv6.se/ipv6books.html

Contact Information

If you have any questions, feel freely to contact us:

- Ahmad AlSadeh
  - Email: ahmad.al-sadeh@hpi.uni-potsdam.de
  - Office: Room H.1.13
  - Tel.: -0331 5509 573
- Feng Cheng
  - Email: feng.cheng@hpi.uni-potsdam.de
  - Office: Room H.1.13
  - Tel.: 0331 5509 521
- Sebastian Roschke
  - Email: sebastian.roschke@hpi.uni-potsdam.de
  - Office: Room H.1.13
  - Tel.: 0331 5509 530

Questions

Seminar topics summary

- IPSec with IPv6
- Cryptographically Generated Addresses (CGA)
- Neighbor Discovery and Secure Neighbor Discovery (SEND)
- IPv6 Firewalls
- Threats of IPv6 transition mechanisms: Dual stack, tunneling
- Implement new applications for IPv6