A Generalized Label-Forwarding Architecture for the Future Internet

2nd GI/ITG KuVS Workshop
Future Internet

Karlsruhe 11/2008

Achim Friedland
SONES GmbH / TU Ilmenau
achim.friedland@sones.de
Today's Internet model – in theory

- **APPLICATION**
- **TRANSPORT**
- **NETWORK**
- **LINK**
Today's Internet model – in reality

- **APPLICATION**
- **TRANSPORT**
- **NETWORK**

**Link Layer Security:**
- MACSec, 802.11i

**Transport Layer Security:**
- TLS, DTLS
- IPSec

**Network Layer Security:**
- IP-in-IP, GRE
- (G)MPLS

**Application Layer Security:**
- S/MIME
- DNSSec

**Transport Layer Protocols:**
- SOCKS, SSH
The Software Engineers’ way:
1. Refactoring
2. Enhancement
Lessons learned so far (1)…

• End-to-End semantics are good for overall robustness but bad for privacy

• Minimize the state within the network but allow some state at the (domain) edges (Firewalls, NAT, VPN, Proxies, MobileIP, QoS Classification)

• Protocol layering minimizes complexity and boosts abstraction but everyone tries to bypass the layer model using tunnels
Lessons learned so far (2)…

• Security is needed everywhere but has to be easily deployable (*IPSec* vs. *TLS*)

• Some of todays (Cross-Layer)-Designs can be seen as „lawfull“ layer violations (*e.g.* TCP, *IPSec*)

• Stackable Flow-Labels for traffic differentiation, aggregation and advanced traffic engineering (*e.g.* *MPLS*)
Basic Idea

• Label-switched network design between applications using „extended labels“

• Extended labels include a packet counter to support e.g. security, loss detection, …

• Label may be „globally unique“ for supporting e.g. IP Addresses, DIFF-Serv tags

• Network state is used to implement security, privacy, mobility and QoS
Proposed Architecture: ELSSA protocol

Extended Label Stream Switching Architecture

User Space
OS Kernel / Virt. Kernel
Network

Application MAIC
Extended Labels (Label Stack)
Transport MAIC

Front Padding
Application Data
Back Padding

Application MAIC

Label #1
Packet Counter #1
...
...
...

Label #n
Packet Counter #n

Transport MAIC

Underlay Transport Header
Properties and Comparisons

• Separation of forwarding and routing, location and addressing
• Built-in security and privacy
• Built-in (micro-)mobility and QoS
• Support of heterogeneous subnetworks, modularity and soft migration
Future Project Development

![Diagram showing layers of network architecture with Application, Path Maintenance, ELSSA, and Transport Underlay.]
Thank you for listening…
- Questions?
- Feedback?