# Master Thesis

# Supporting IPv6 host-based multihoming (shim6) in Linux Firewalls

Christoph Paasch

December 20, 2010

1 Theoretic overview

2 Shim6 and Firewalls: Problem statement

3 Implementation

4 Performance evaluation

5 Configuring a shim6-firewall

6 Conclusion

1 Theoretic overview
- Multihoming
- Shim6
- Statefull firewall

2 Shim6 and Firewalls: Problem statement
- Design of the shim6 firewall

3 Implementation
- Shim6-firewall architecture

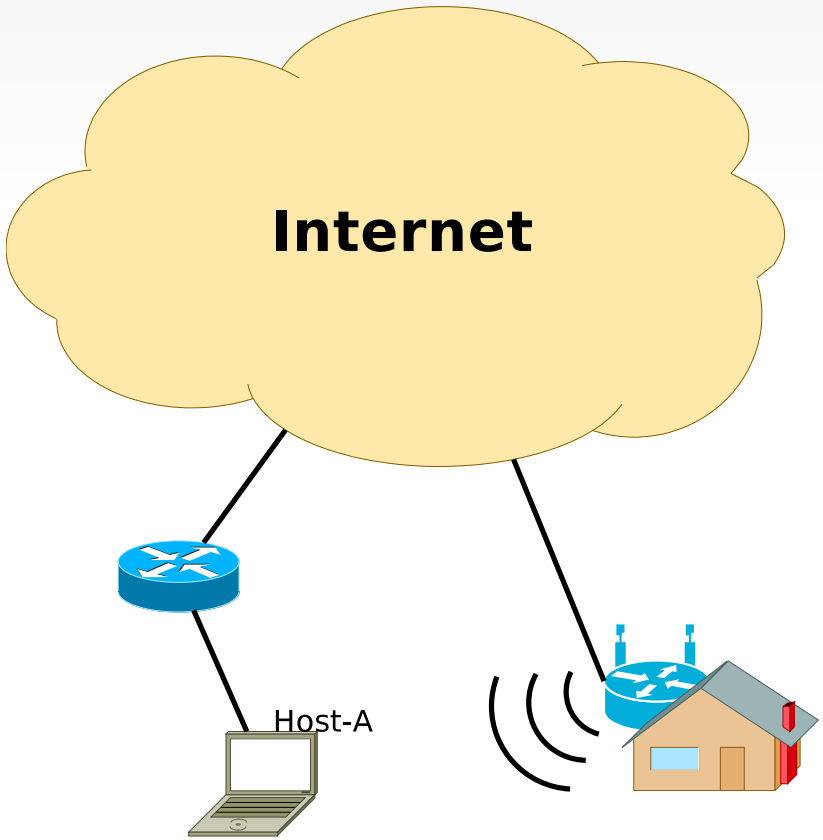
4 Performance evaluation

5 Configuring a shim6-firewall

6 Conclusion

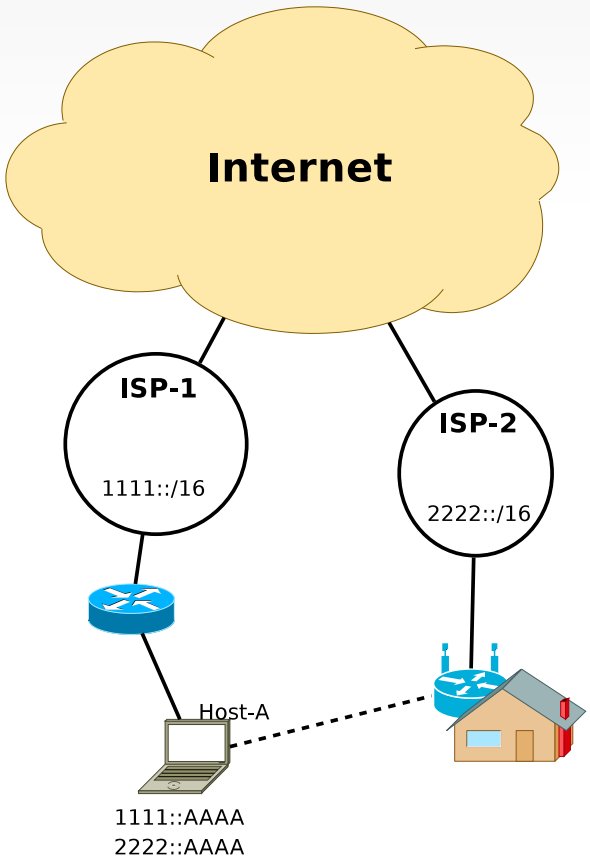
# Multihoming

Supporting **IPv6 host-based multihoming** (shim6) in Linux Firewalls



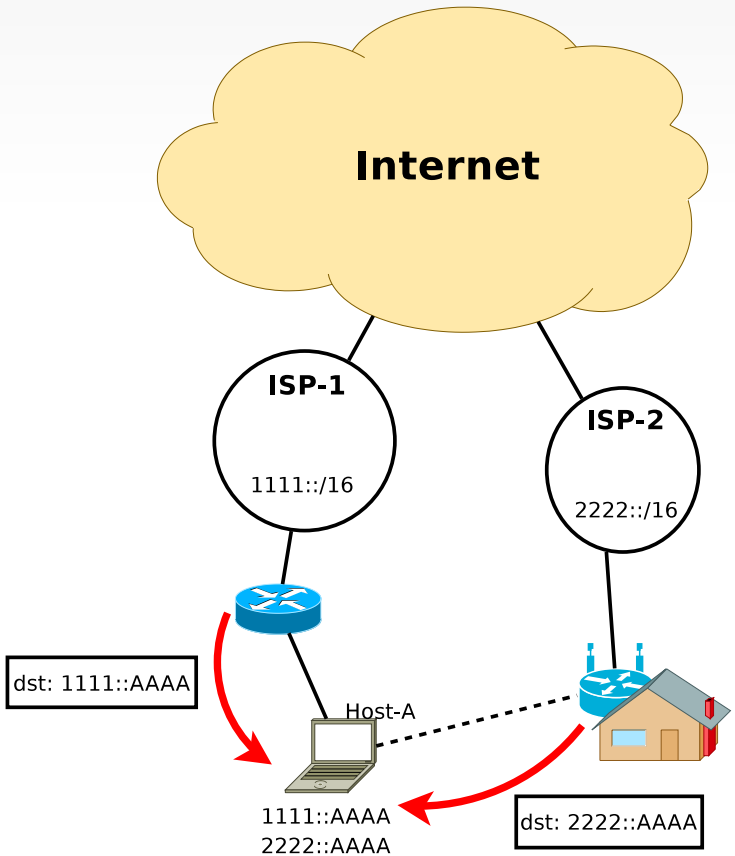
# Multihoming

Supporting **IPv6 host-based multihoming** (shim6) in Linux Firewalls



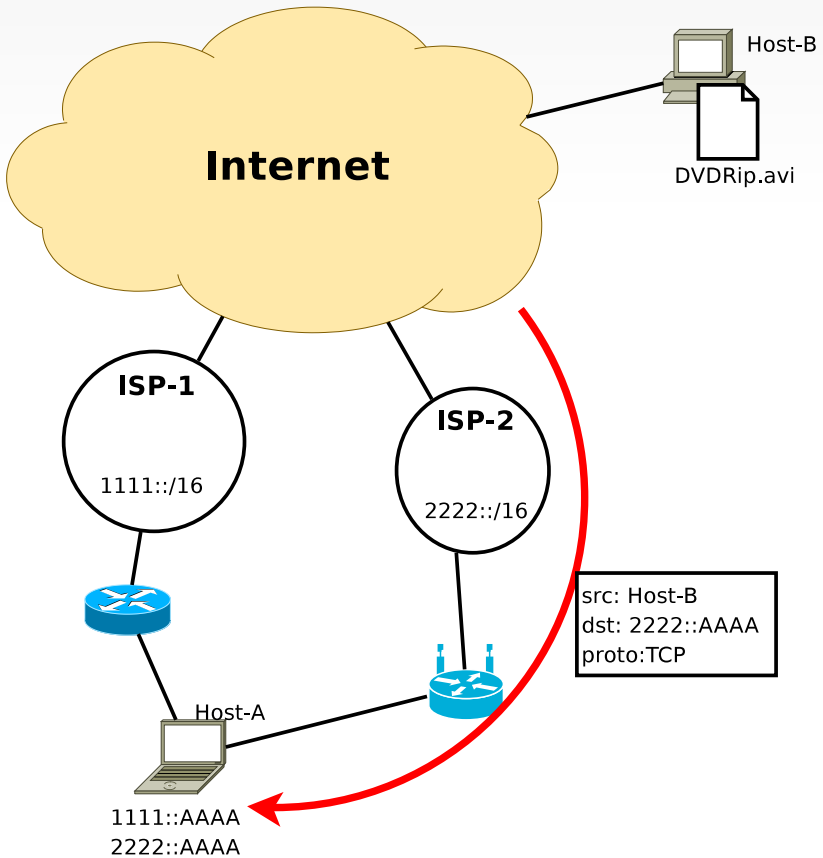
# Multihoming

Supporting **IPv6 host-based multihoming** (shim6) in Linux Firewalls



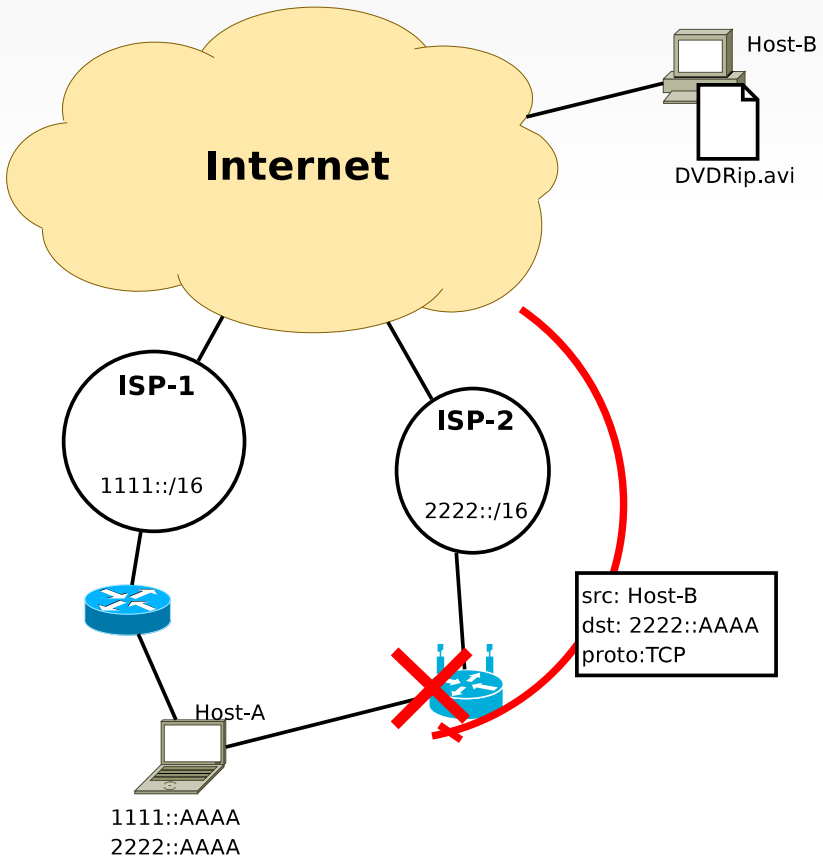
# Shim6

Supporting IPv6 host-based multihoming (**shim6**) in Linux Firewalls



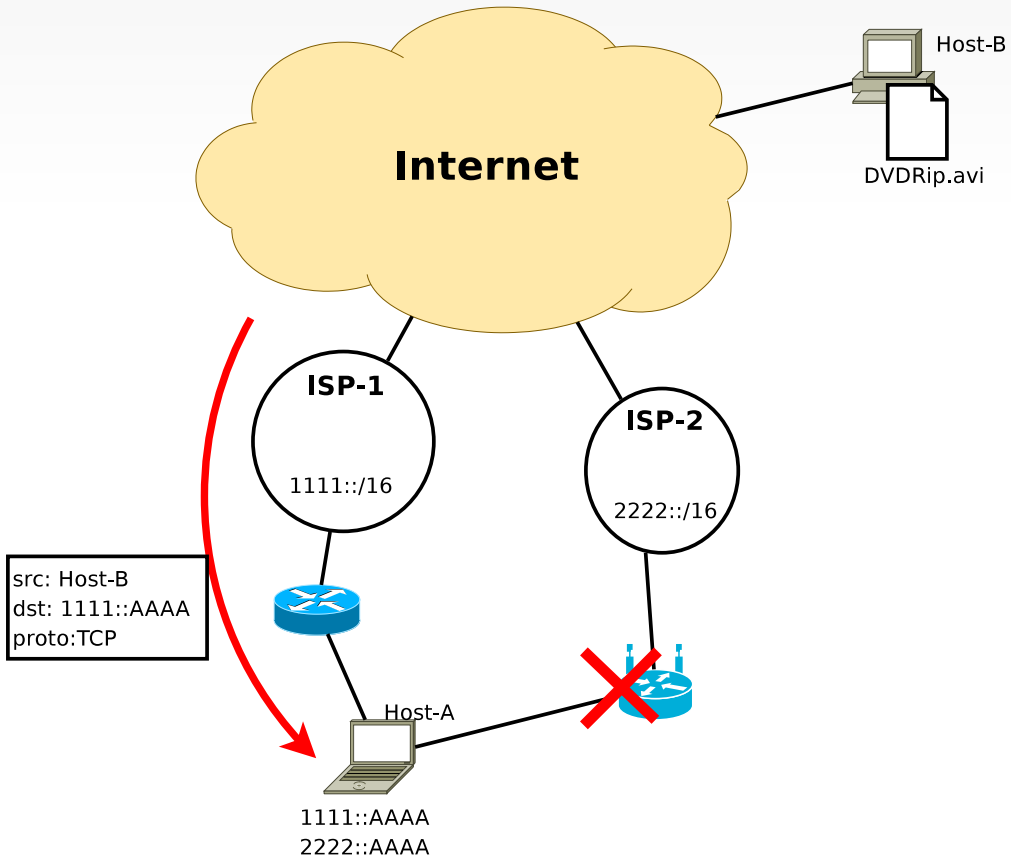
# Shim6

Supporting IPv6 host-based multihoming (**shim6**) in Linux Firewalls



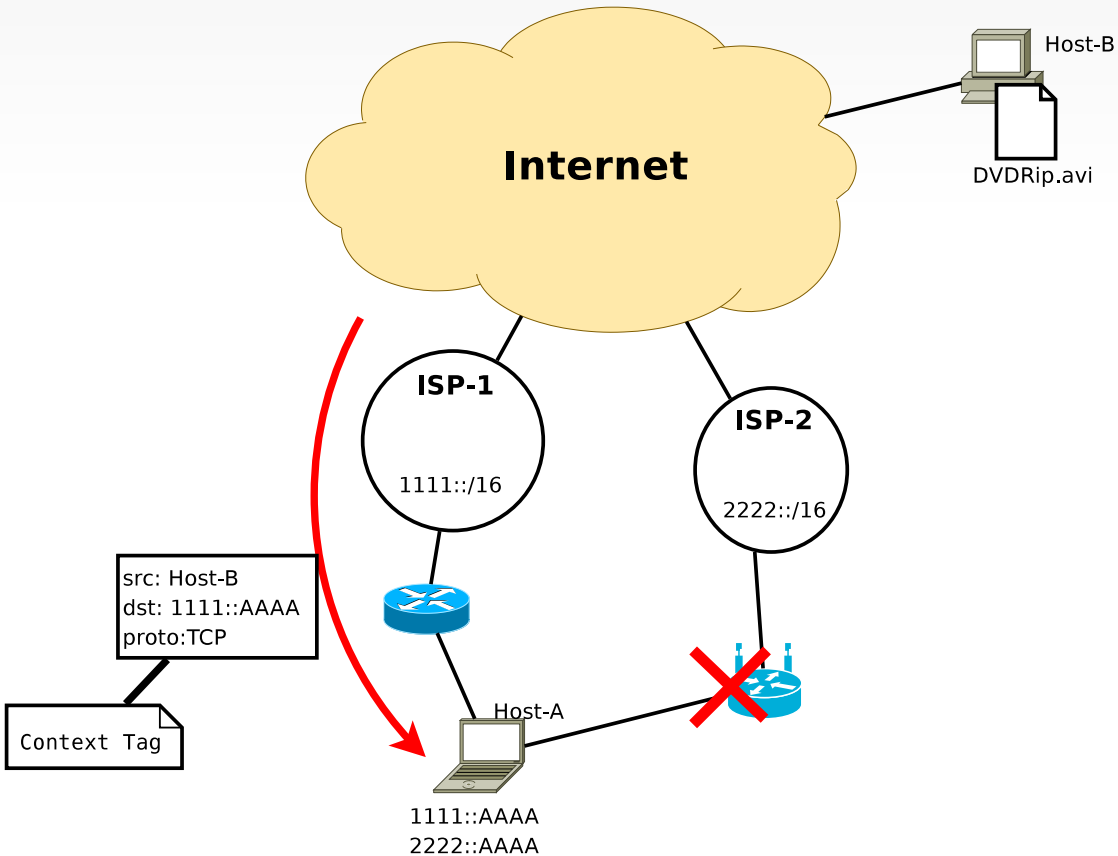
# Shim6

Supporting IPv6 host-based multihoming (**shim6**) in Linux Firewalls



# Shim6

Supporting IPv6 host-based multihoming (**shim6**) in Linux Firewalls

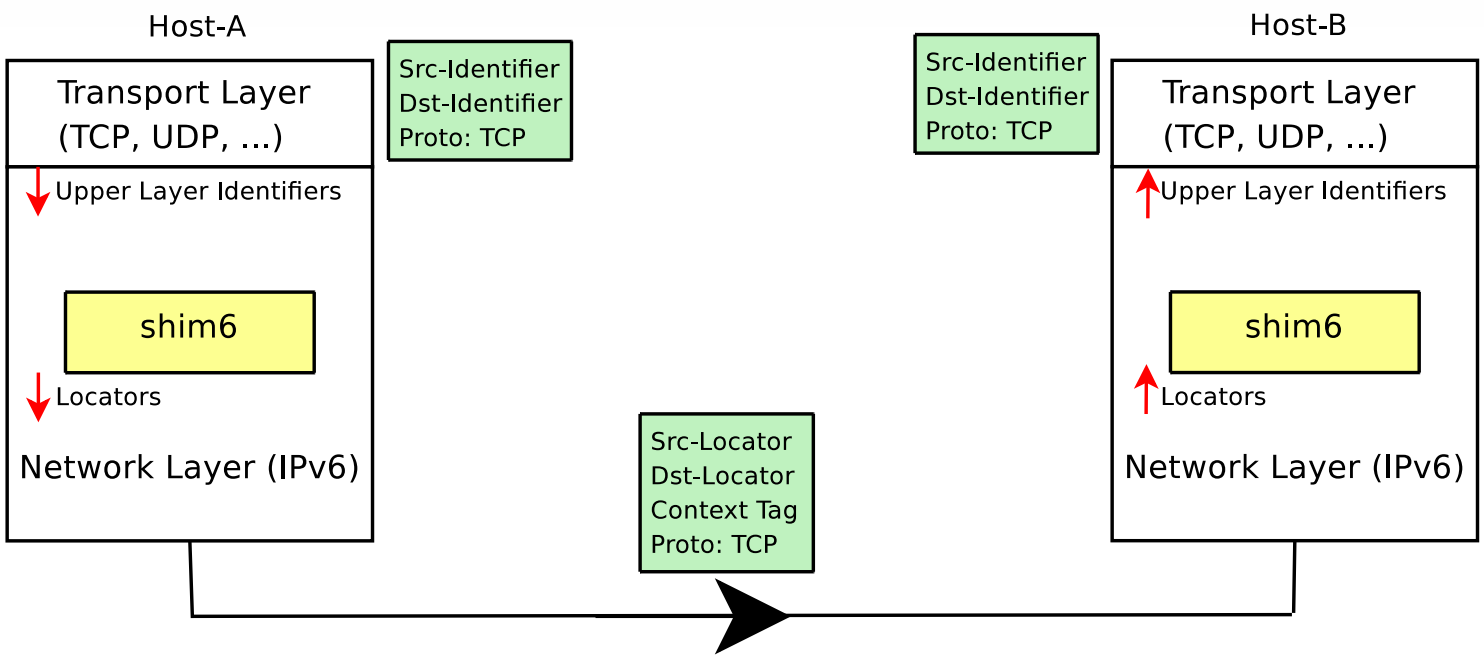


# Shim6

Separate Locators from Identifiers.

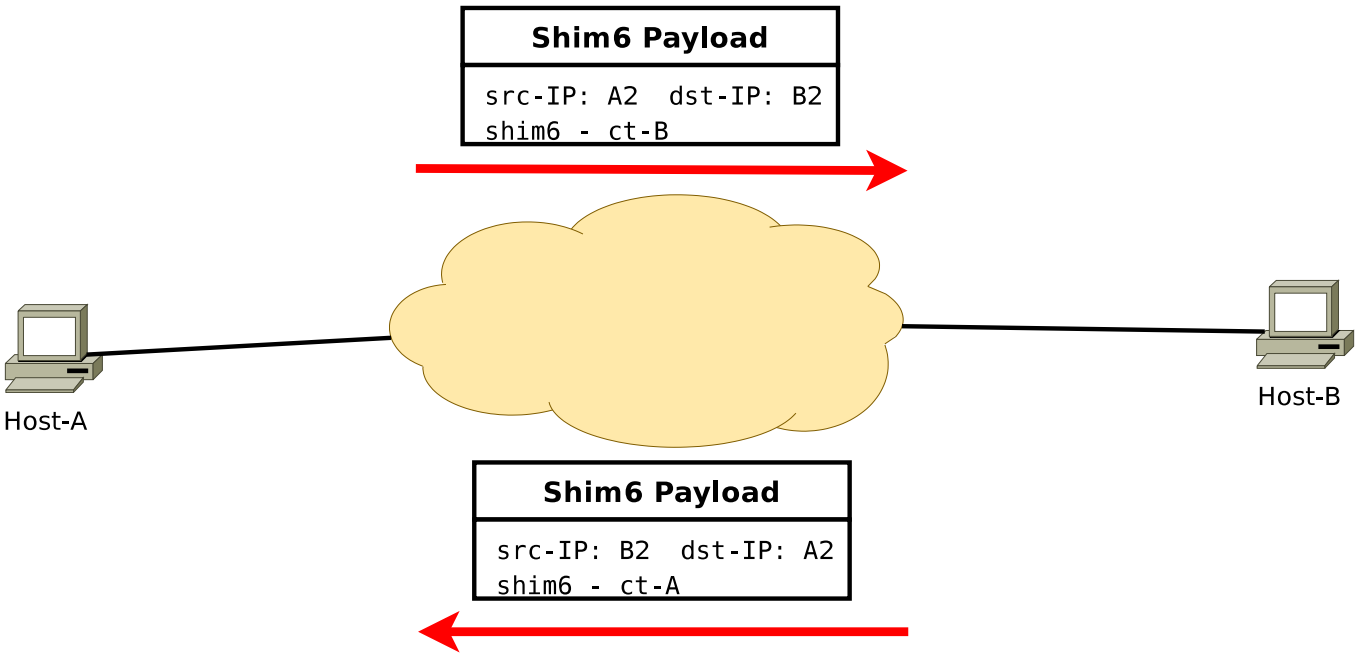
**Identifier** Identifies a connection and is passed to the upper layer protocols.

**Locators** Used inside the packet.



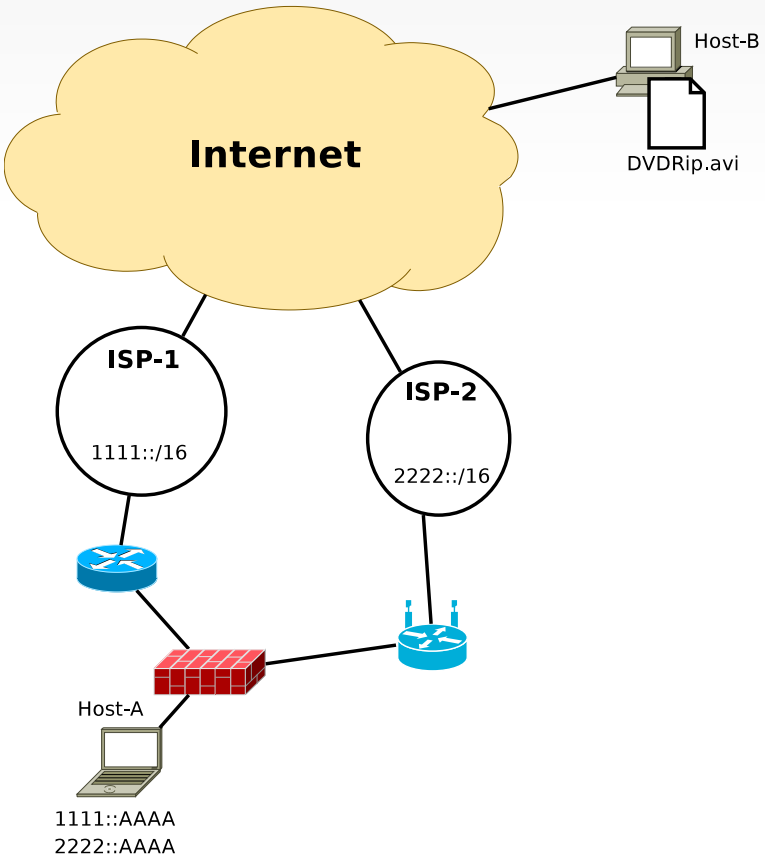
# Shim6

- Shim6 control messages
  - Establish the shim6 session
  - Assure connectivity
  - Switch locators
- Shim6 payload messages
  - Transport payload-data, tagged with the context tag



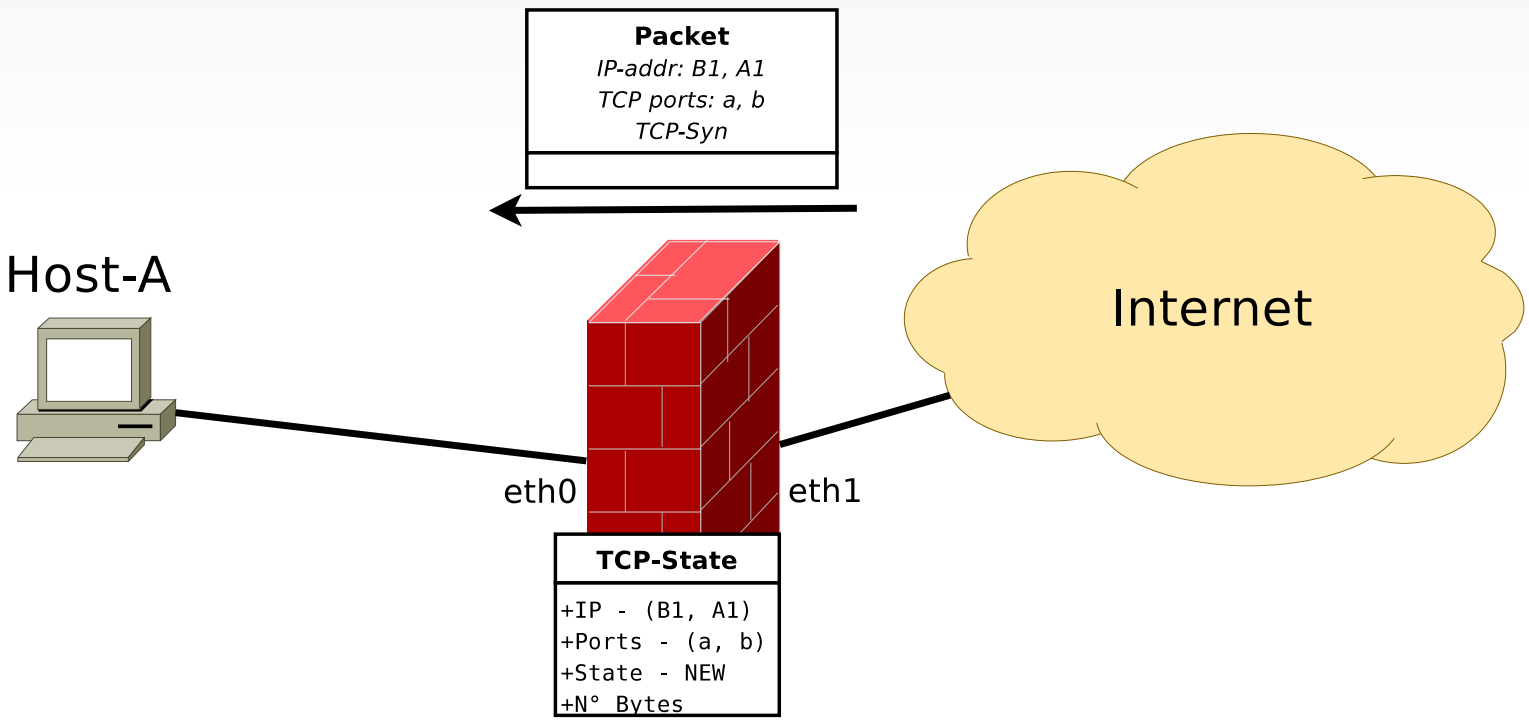
# Statefull firewall

Supporting IPv6 host-based multihoming(shim6) in **Linux Firewalls**



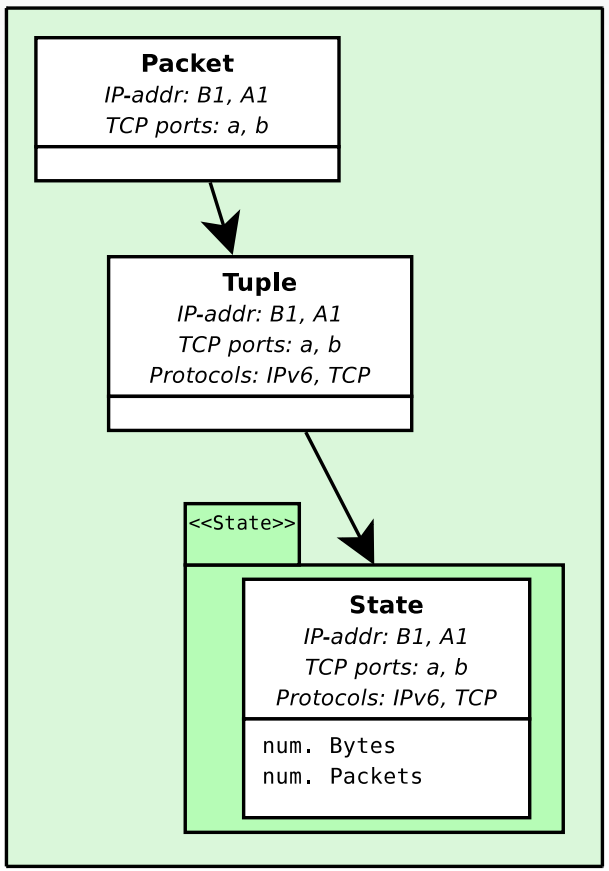
# Statefull firewall

Supporting IPv6 host-based multihoming(shim6) in **Linux Firewalls**



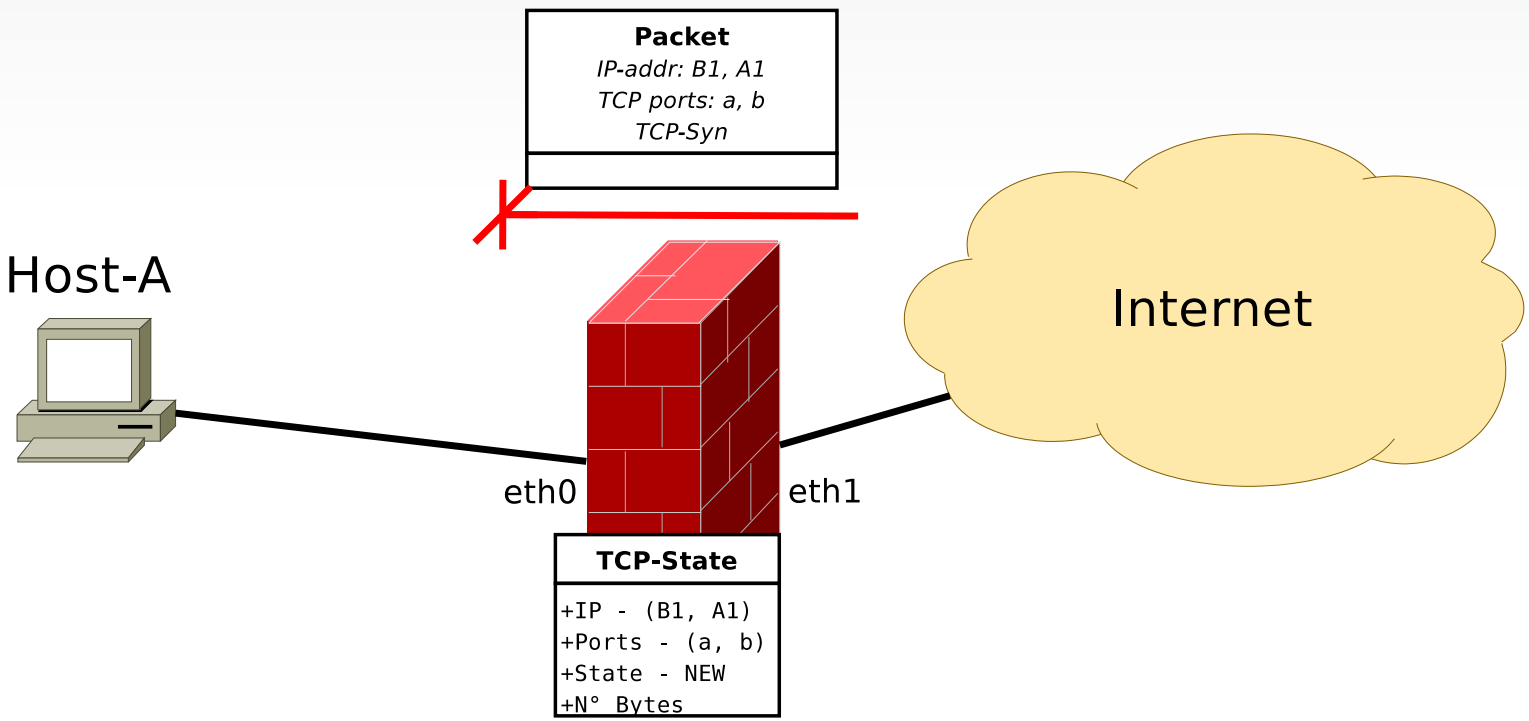
# Statefull firewall

Supporting IPv6 host-based multihoming(shim6) in **Linux Firewalls**



# Statefull firewall

Supporting IPv6 host-based multihoming(shim6) in **Linux Firewalls**




iptables -i eth1 --state NEW -j DROP

1 Theoretic overview
- Multihoming
- Shim6
- Statefull firewall

2 Shim6 and Firewalls: Problem statement
- Design of the shim6 firewall

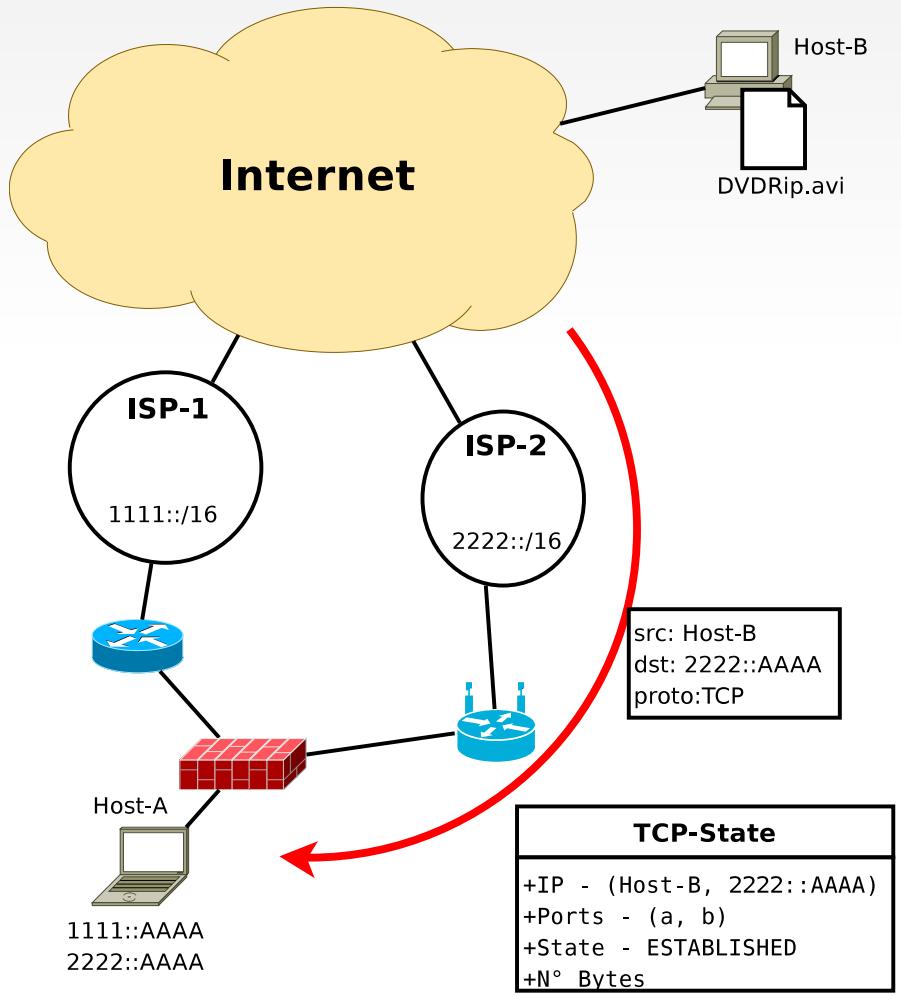
3 Implementation
- Shim6-firewall architecture

4 Performance evaluation

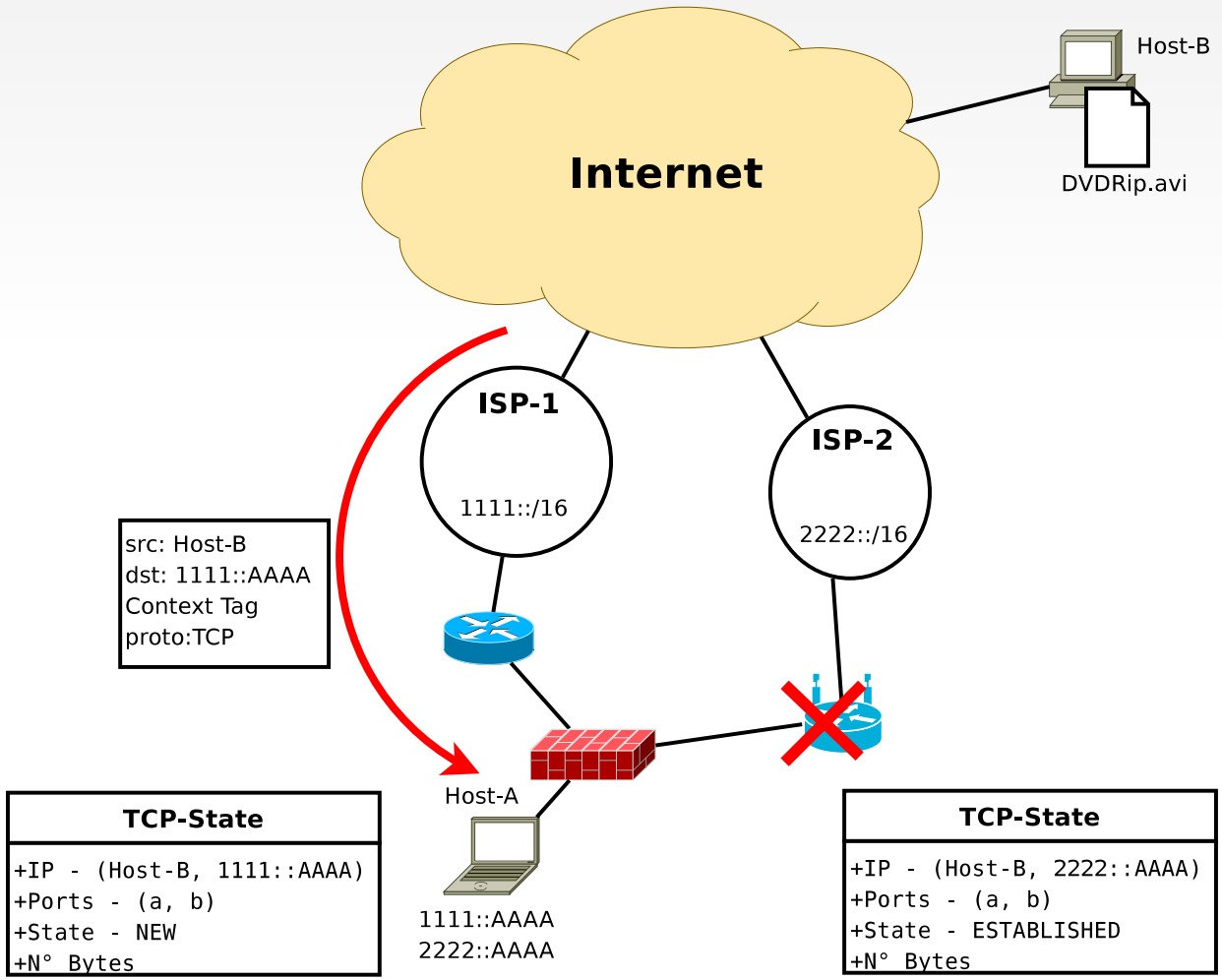
5 Configuring a shim6-firewall

6 Conclusion

# Shim6 vs. Stateful Firewalls



# Shim6 vs. Stateful Firewalls



# Solution

- Associate the new flow to the original state
- Track shim6 context establishment
- Map Context Tag to the pair of identifiers

## Problems

Shim6 does not allow support of each feature in stateful firewalls.
Shim6 needs to be changed.

1 Theoretic overview
- Multihoming
- Shim6
- Statefull firewall

2 Shim6 and Firewalls: Problem statement
- Design of the shim6 firewall

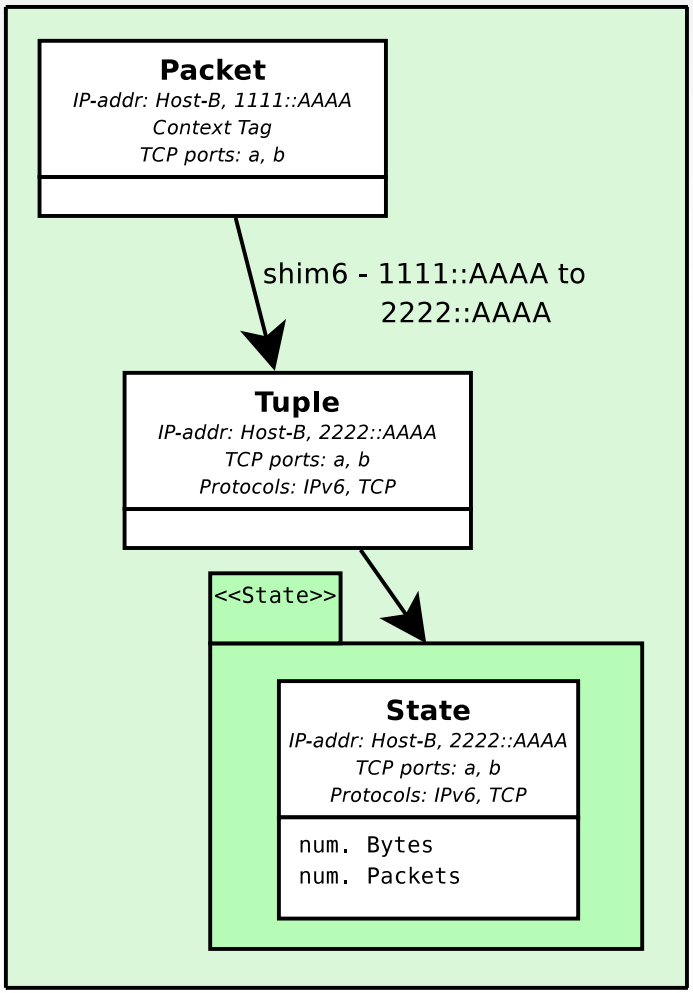
3 Implementation
- Shim6-firewall architecture

4 Performance evaluation

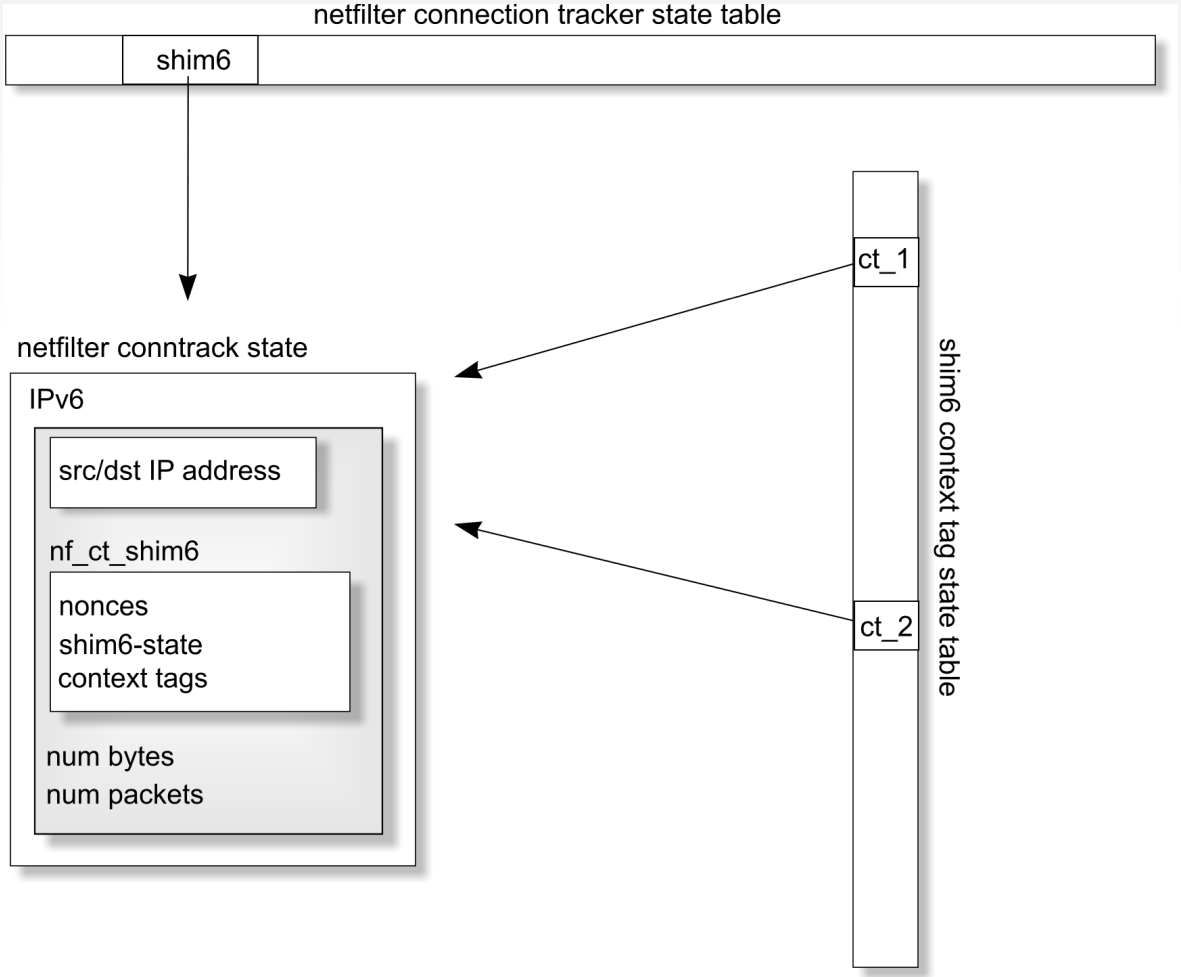
5 Configuring a shim6-firewall

6 Conclusion

# Shim6-Firewall architecture



# Shim6-Firewall architecture



1 Theoretic overview
- Multihoming
- Shim6
- Statefull firewall

2 Shim6 and Firewalls: Problem statement
- Design of the shim6 firewall

3 Implementation
- Shim6-firewall architecture

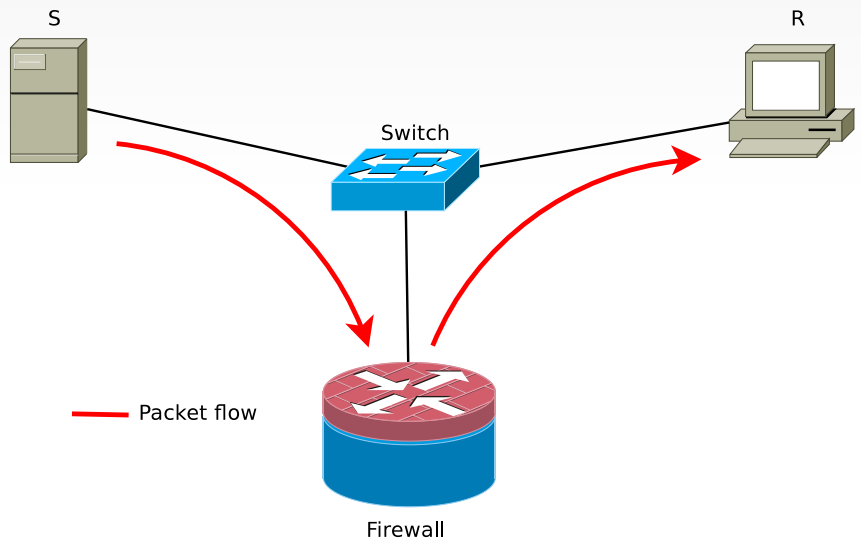
4 Performance evaluation

5 Configuring a shim6-firewall

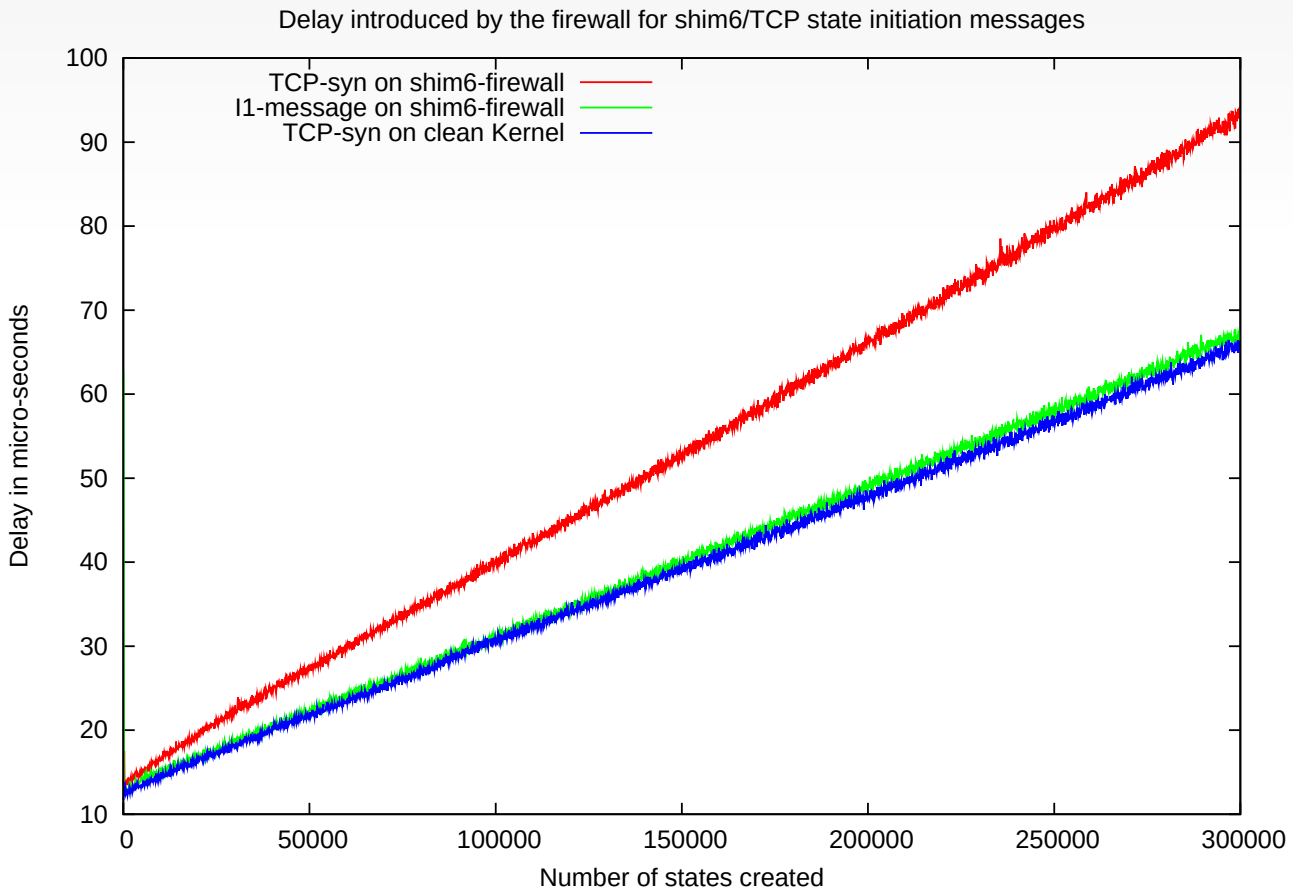
6 Conclusion

# Test Setup

- Creation of a huge number of firewall-states
- Delay measured that the firewall introduces



# Session Initiation messages



1 Theoretic overview
- Multihoming
- Shim6
- Statefull firewall

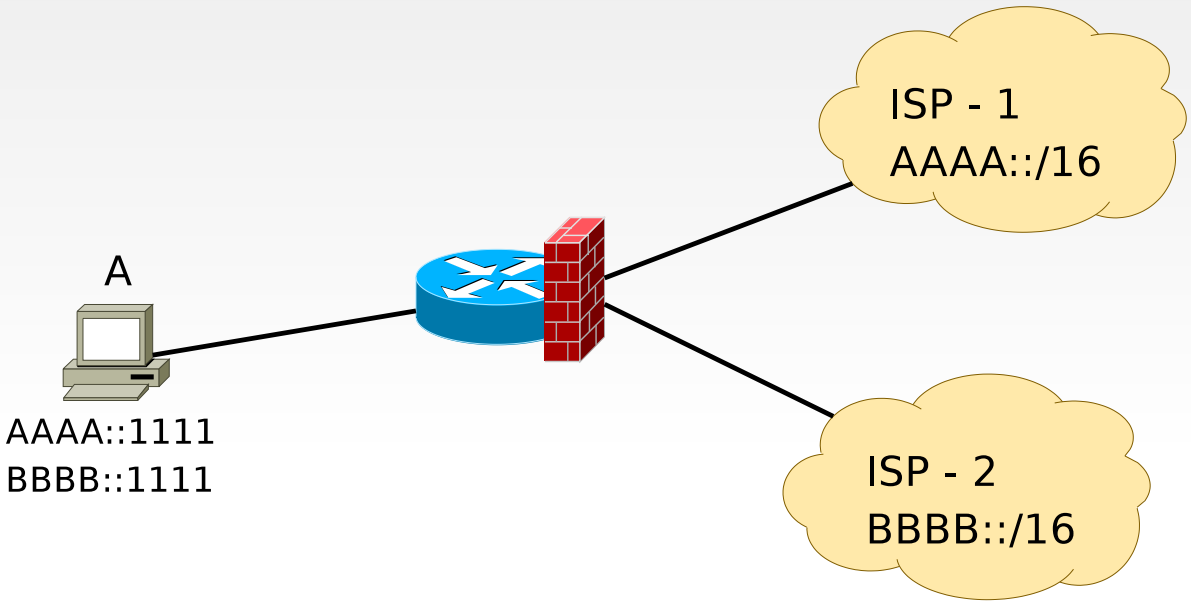
2 Shim6 and Firewalls: Problem statement
- Design of the shim6 firewall

3 Implementation
- Shim6-firewall architecture

4 Performance evaluation

5 Configuring a shim6-firewall

6 Conclusion




## Express consistent rules

- Filter on identifiers rather than on locators.
- Avoid locator-specific rules.
- Avoid per-locators rate-limiting rules.

1 Theoretic overview
- Multihoming
- Shim6
- Statefull firewall

2 Shim6 and Firewalls: Problem statement
- Design of the shim6 firewall

3 Implementation
- Shim6-firewall architecture

4 Performance evaluation

5 Configuring a shim6-firewall

6 Conclusion

# Conclusion

- Most parts of shim6 are supported in the Linux firewall.
- Performs very well even with a huge number of states.
- Configuring the firewall needs to be done carfully.

## Future Work

- Minor modifications to the shim6 protocol.
- Adapt firewall to these changes.
- Tweak the firewall to achieve best performance.

# Questions?