Efficient Port-based Network Access Control for IP DSLAMs in Ethernet-based Fixed Access Networks

D. Duchow, S. Kubisch, H. Widiger, D. Timmermann
University of Rostock
Faculty of Computer Science and Electrical Engineering

T. Bahls
Siemens AG Greifswald

World Telecommunications Congress
WTC 2006
1st – 3rd May 2006, Budapest, Hungary
Outline

1. Background and Motivation
2. Network and System Architecture
3. Design Approaches
4. Problems and Implications
5. Conclusions
1. Background and Motivation

Why 802.1X in Access Network?

- PPP (Point-to-Point Protocol) encapsulation makes efficient IP multicast transport difficult to handle
- DSLAM’s (DSL Access Multiplexer) Ethernet/IP features can supersede PPP
- Migration to Ethernet enables new services and requires other features
  - IP DSLAMs mandatory provide DHCP for autoconfiguration
- 802.1X is designed for authentication/authorization for 802 media (Eth)
- IP DSLAMs are going to provide 802.1X for authentication

Implementation Issues on DSLAMs

- Several alternative solutions for implementation
- 802.1X-compliant implementation requires some adjustments
2. Network and System Architecture

Access Basic Components
- Centralized/remote DSLAMs
- CPN, CPE on customer side
- BNG/BRAS on provider side

Access Basic Topology
- Cascaded network structure
- Different level of aggregation
- Based on Ethernet technology
Efficient Port-based Network Access Control for IP DSLAMs in Ethernet-based Fixed Access Networks

**Basic DSLAM System Structure**

- Line cards aggregate customer lines to Ethernet
- Ethernet switching card aggregates line cards
- Additional IP feature processing
- Central DSLAM aggregates remote DSLAMs
Main Conditions for IEEE 802.1X Compliance

- Supplicant and Authenticator port have direct physical or logical one-to-one port relationship
- Authenticator performs access control for all Supplicant ports (i.e. filter for EAPOL frames)
- Authenticator system has IP stack and AAA client (e.g. RADIUS)
- Access is granted or denied dependent on RADIUS result (accept/reject)
- Authenticator authorizes / unauthorizes the port (i.e. set the filter)
3. Design Approaches - Overview

802.1X Authenticator Implementation Options

1. On every line card
2. On every central switching card
3. On central switching card of DSLAM at highest level of aggregation
3.1. Implementation on every Line Card

Pros

- P2P (point-to-point) connection characteristics of ports
- Complying with 802.1X standard

Cons

- Peripheral position
- Resource-intensive
- Expensive on line cards
3.2. Implementation on every Ethernet Central Switching Card

Pros

- Only one Authenticator system per DSLAM
- Central concentration of resource-intensive functions
- Cost reduction on line cards

Cons

- Loss of P2P connection characteristic
- Not standards-compliant

Extensions

- Access Controller on line card
- Message flow at control path
- Logical P2P connection characteristic of ports
- Authenticator controls line card ports
- standards-compliant again
- cost-effective on line cards
3.3. Implementation on centralized DSLAM’s Ethernet Card

**Pros**

- Only one Authenticator
- Central concentration of resource-intensive functions
- Cost reduction of line cards and remote DSLAMs

**Cons**

- Loss of P2P connection characteristic

**Extensions**

- Access Controller on line card
- Message exchange by layer 2 protocol
- Standards-compliant again
- Relieve line cards and remote DSLAMs: cost-effective
3.4. Distributed Authenticator and Access Controller

Access Controller module
- Controlled & uncontrolled ports by EAPOL filter
- Creation of logical port correlation
- Control mechanism for controlled port by extensions

Authenticator System module
- EAPOL Authenticator processing
- RADIUS client processing
- EAPOL to RADIUS handling
- Service offered by Authenticator’s system
- Port authorization by extension
4. Problems and Implications

<table>
<thead>
<tr>
<th>Logical Port Correlation</th>
<th>Control Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Using unique 1:1 VLAN assignment</td>
<td></td>
</tr>
<tr>
<td>- Scaling problem</td>
<td></td>
</tr>
<tr>
<td>- Not in 1:n VLAN scenarios</td>
<td></td>
</tr>
<tr>
<td>• Using unique Subscriber Port ID</td>
<td></td>
</tr>
<tr>
<td>- Well scalable</td>
<td></td>
</tr>
<tr>
<td>- VLAN independent</td>
<td></td>
</tr>
<tr>
<td>• Authenticator to Access Controller</td>
<td></td>
</tr>
<tr>
<td>• Intra-system on management plane</td>
<td></td>
</tr>
<tr>
<td>• Inter-system communication for centralized solution</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Generic Communication Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Connectionless layer 2 protocol</td>
</tr>
<tr>
<td>• Transport both Port and Control Information over Ethernet</td>
</tr>
<tr>
<td>• Minimized complexity eases optimized protocol implementation in hardware or software</td>
</tr>
<tr>
<td>• Open for additional features</td>
</tr>
</tbody>
</table>
5. Conclusions

### 802.1X Design Approaches

- On every line card: resource-intensive, not sufficient
- On every DSLAM: resource-efficient on line cards, suitable
- On centralized DSLAM: resource-efficient on line card and remote DSLAM, well suitable

### Implementation Extensions

- Access Controller with filter and port control mechanism
- Communication between Access Controller and Authenticator
- Extension on line cards yield marginal additional expenses

### Generic Communication Protocol

- Information exchange between different functional modules
- Transport port information and control information
- Provides a communication platform for further relevant features
Thank You!