

Authentication and Authorization in Wired OpenFlow-Based Networks Using 802.1X

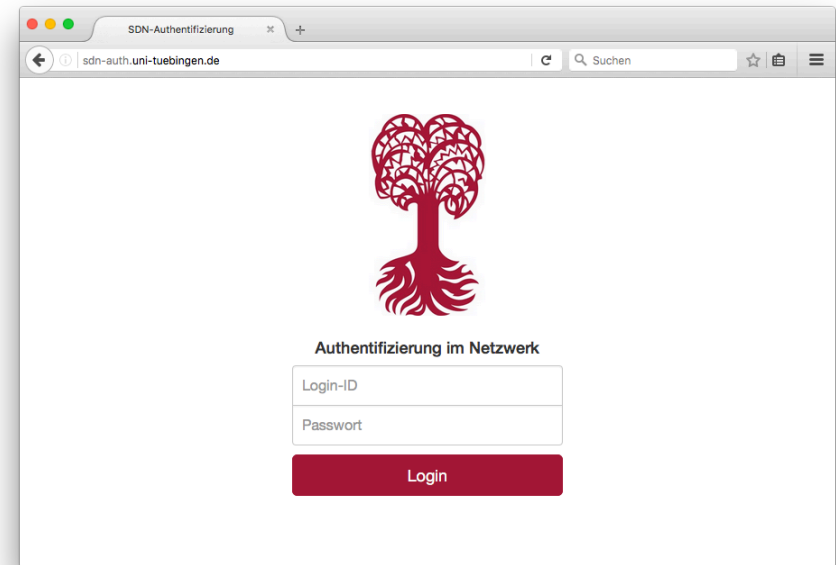
Frederik Hauser, Mark Schmidt, Michael Menth
frederik.hauser@uni-tuebingen.de

<http://kn.inf.uni-tuebingen.de>



- ▶ Extensive work on identity-based network control
 - Kinetics, Resonance, Ethane, ...

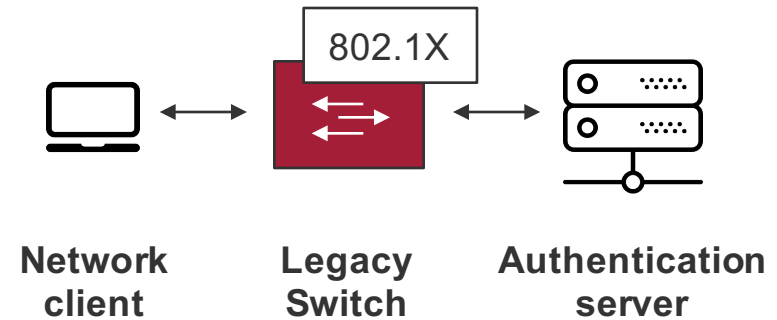
- ▶ Status quo
 - Web frontend authentication
 - User interaction required (reauthentication, ...)
 - Compatibility issues
 - Static MAC address to identity mapping
 - Highly insecure





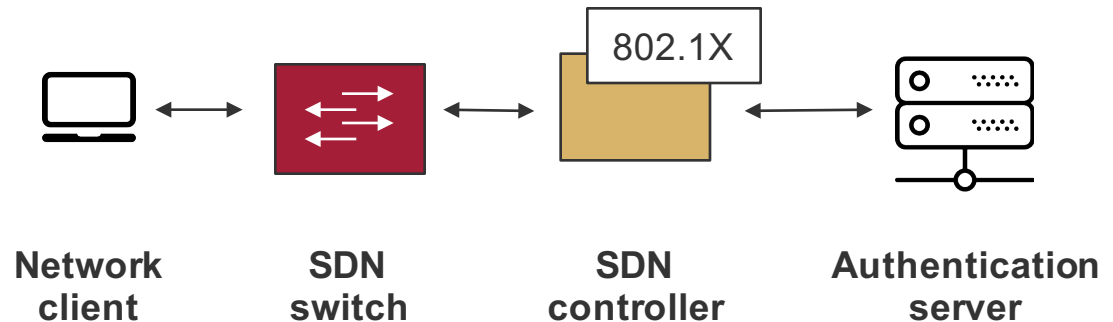
► 802.1X

- Most widely used standard for port-based authentication and authorization in access networks (e.g. eduroam)
- Leverages EAP (RFC 3748) and RADIUS (RFC 2865)



► Applicability of 802.1X to SDN

- Transformation of 802.1X Authenticator module on legacy switches into a network application

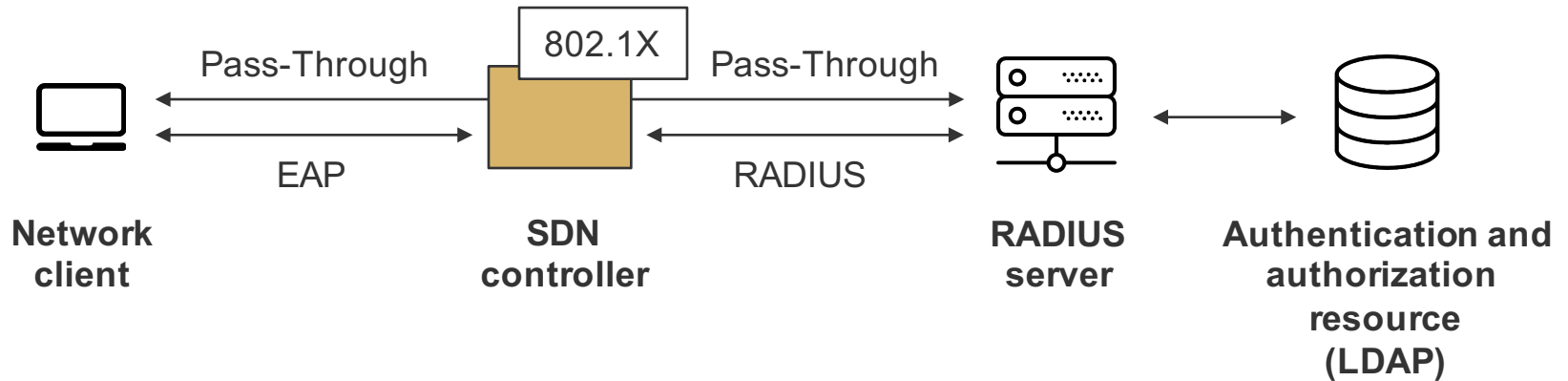


► Compliance to standards

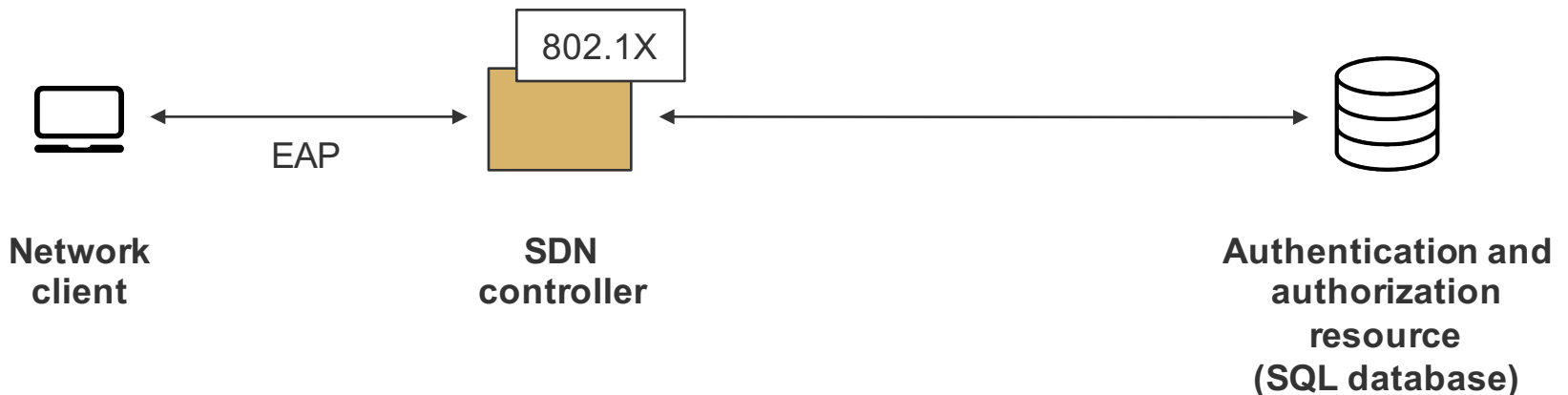
► Modification transparent to endpoints



► Authentication and authorization using RADIUS



► Additional authentication resources (other than RADIUS)





► Session management for authorization

- Network-wide session database for identity-based network control

```
{ test@uni-tuebingen.de : { max_sessions : 1, sessions : (
    { aaa_time : Mo 13 Jun 2016 14:16:26 CEST,
      aaa_method : Radius(ip=10.0.20.100, meth=EAP-TLS),
      phys_port : OF-Switch(ip=10.0.20.222, port=1),
      assigned_vlans : (10)},
  )}}
```

- Check for simultaneous usage boundaries
- Support for fine-grained and complex admission rules

```
student = ["bob"]; prof = ["alice"];
[(isrc="prof") ^ (protocol="https") ^ (idst="student") ]: allow;
```

- Immediate enforcement of authorization changes



- ▶ Proof-of-concept implementation
 - Application for Ryu SDN controller
 - Various test scenarios
 - Various authentication and authorization resources

- ▶ Further work
 - Performance study
 - Use of NFV to provide scalability
 - Open source
 - Documentation