

# Identity Based Networking Services 2.0 an der Hochschule Luzern

Finanzen & Services

IT Services

**Pascal Gertsch**

ICT System Ingenieur

T direkt +41 41 228 21 29

pascal.gertsch@hslu.ch

Luzern 15.06.2016

## Agenda

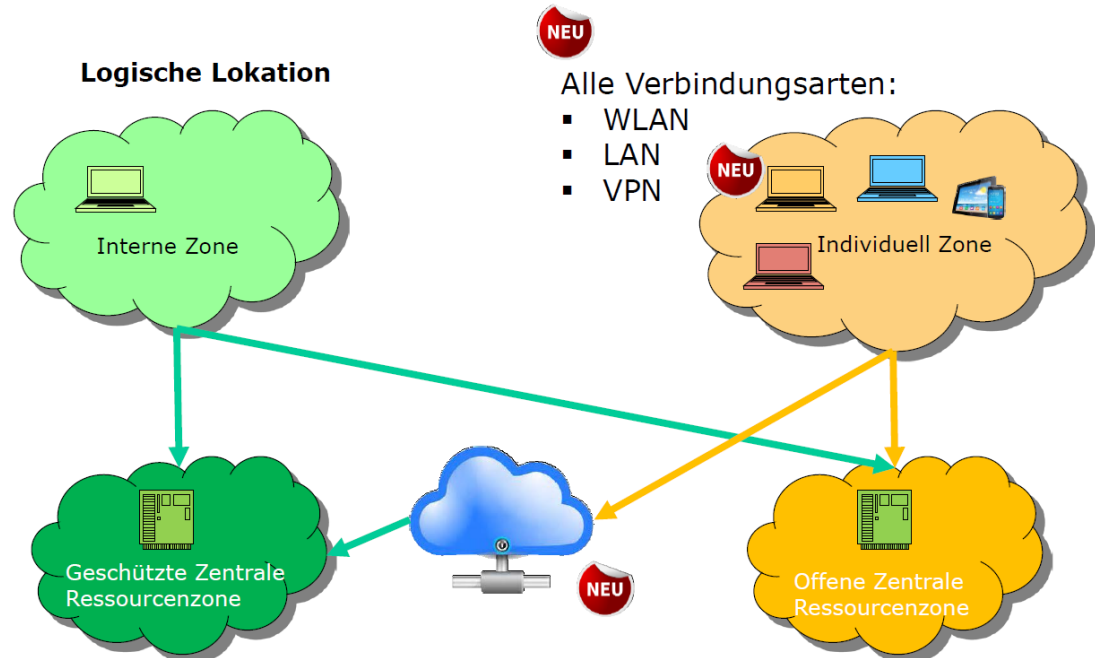
- Vorstellung Hochschule Luzern & IT-Services
- IT Strategie
- 802.1X vor IBNS 2.0
- Nachteile der «legacy» 802.1X Implementation
- IBNS 2.0 und die Identity Control Policy
- Vorteile und technische Aspekte der neuen Lösung
- Zusammenfassung
- Fragen

## Ein paar Fakten

- 24 Standorte (Luzern, Horw, Littau, Emmenbrücke, Zug, Rotkreuz, etc)
- Netzwerk für ca. 15'000 Nutzer
- Aktuelle Situation:
  - 5'000 Studenten Notebooks
  - 2'200 PCs & NBs
  - 430 Macs
  - 470 Drucker

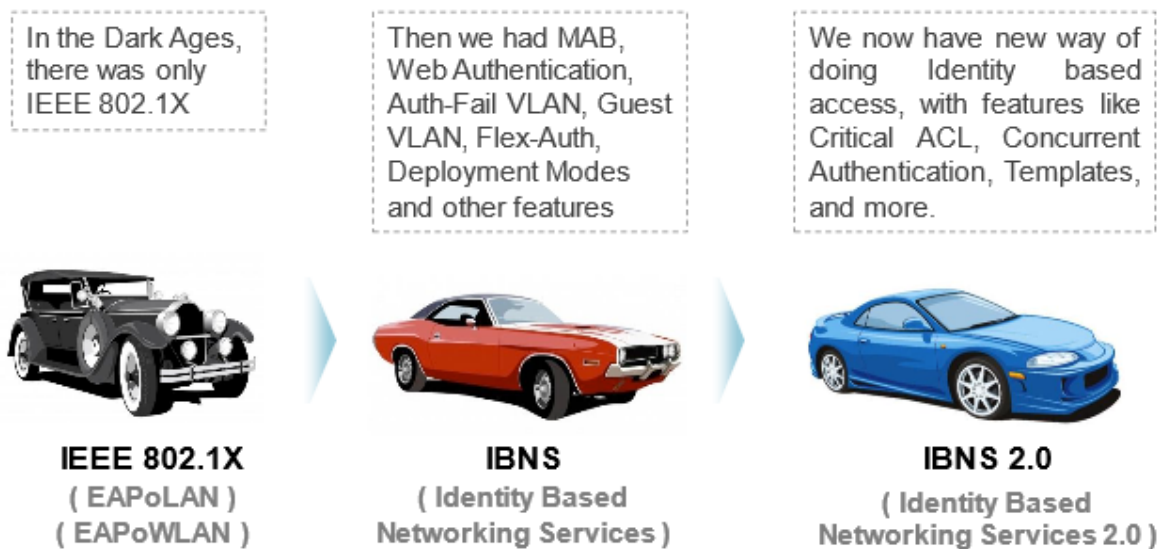
## IT Strategie und Umsetzung

- Strategie
  - Sicherheit dezentraler IT-Infrastruktur
- Umsetzung
  - 802.1X auf dem WLAN → Bereits bestehend
  - 802.1X auf dem LAN
  - Neues Zonenkonzept



## 802.1X vor IBNS 2.0

- 802.1X ist bereits seit August 2015 bei ca. 60 IT Mitarbeitern in Betrieb.
- Proof of Concept wurde im 2014/2015 mit 802.1X Basisfunktionalitäten entwickelt. Dazumal waren nur wenige IBNS Funktionen verfügbar.



# ISE als Authentication Server

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

**Policy Sets**

Search policy names & descriptions.

Summary of Policies  
A list of all your policies

**Global Exceptions**  
Rules across entire deployment

- WLAN\_UNI-WLC**  
UNI-WLC-AUTH
- EDUROAM**  
EDUROAM-AUTH
- MPP**  
MPP-AUTH

Policy Set	Policy Name	Description
<input checked="" type="checkbox"/> EDUROAM	EDUROAM-AUTH	DEVICE:Device Type EQUALS Device Type#All Device Types#RADSEC-PROXIES
<input checked="" type="checkbox"/> MPP	MPP-AUTH	DEVICE:Device Type EQUALS Device Type#All Device Types#MPP
<input checked="" type="checkbox"/> WLAN_HSLU_PHLU	Wlan 8021x	Radius:Called-Station-ID ENDS WITH :hslu OR Radius:Called-Station-ID ENDS WITH :phlu OR Airespace:Airespace-Wlan-Id EQUALS 1 OR Airespace:Airespace-Wlan-Id EQUALS 4
<input checked="" type="checkbox"/> WIRED_8021X	Wired 8021x	DEVICE:Device Type EQUALS Device Type#All Device Types#IOS AND Wired_802.1X
<input checked="" type="checkbox"/> WIRED_MAB	MAB-Authentication	Wired_MAB AND DEVICE:Device Type EQUALS Device Type#All Device Types#IOS
<input checked="" type="checkbox"/> Default	Default Policy Set	

Timestamp	Status	Device	IP	MAC	Device Type	Policy Set
2016-06-13 07:51:33.799	<input checked="" type="checkbox"/>	...	...	...	Unknown	EDUROAM >> Default ...
2016-06-13 07:51:30.874	<input checked="" type="checkbox"/>	...	...	...	Apple-IPhone	WLAN_HSLU_PHLU >...
2016-06-13 07:51:30.259	<input checked="" type="checkbox"/>	...	...	...	Apple-Device	WLAN_HSLU_PHLU >...
2016-06-13 07:51:30.247	<input checked="" type="checkbox"/>	...	...	...	Apple-Device	WLAN_HSLU_PHLU >...
2016-06-13 07:51:30.076	<input checked="" type="checkbox"/>	...	...	...	Apple-Device	WIRED_8021X >> Def...
2016-06-13 07:51:29.985	<input checked="" type="checkbox"/>	...	...	...	Apple-Device	WIRED_MAB >> Defau...
2016-06-13 07:51:29.976	<input checked="" type="checkbox"/>	...	...	...	Apple-Device	WIRED_MAB >> Defau...
2016-06-13 07:51:28.091	<input checked="" type="checkbox"/>	...	...	...	Apple-Device	WLAN_HSLU_PHLU >...
2016-06-13 07:51:27.551	<input checked="" type="checkbox"/>	...	...	...	Apple-Device	WLAN_HSLU_PHLU >...
2016-06-13 07:51:26.880	<input checked="" type="checkbox"/>	...	...	...	Apple-Device	WLAN_UNI-WLC >> D...
2016-06-13 07:51:26.266	<input checked="" type="checkbox"/>	...	...	...	Apple-Device	WLAN_UNI-WLC >> D...

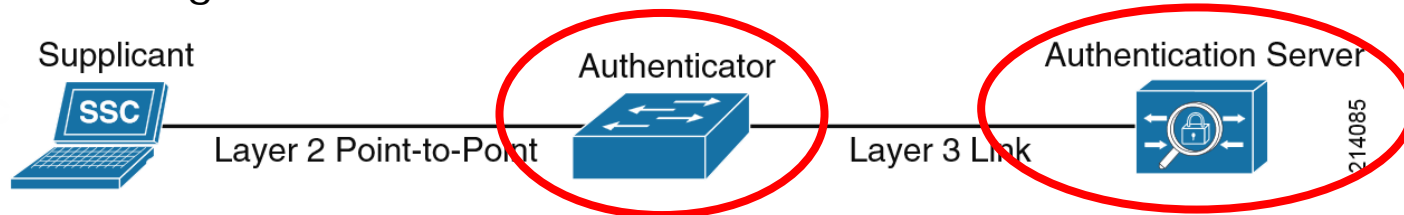
## Nachteile der «legacy» 802.1X Implementation

- 14 Sekunden Verzögerung, falls der Client nicht 802.1X fähig ist
- Nur ein Supplikant pro Port erlaubt
- Inkompatibilitäten mit Mac OSX
- Keine periodische Reauthentifizierung
- Viele repetitive Interface Kommandos

```
Interface GigabitEthernet 1/0/1
description 0421 / gep
switchport access vlan 777
switchport mode access
switchport nonegotiate
ip arp inspection limit rate 50
power inline never
authentication control-direction in
authentication event fail retry 1 action authorize vlan 333
authentication event server dead action authorize vlan 666
authentication event no-response action authorize vlan 333
authentication event server alive action reinitialize
authentication host-mode multi-domain
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication timer restart 3600
authentication violation restrict
mab
macro description DOT1X
dot1x pae authenticator
dot1x timeout tx-period 7
no cdp enable
no lldp transmit
spanning-tree portfast
spanning-tree guard root
ip verify source
ip dhcp snooping limit rate 15
```

## Was ist IBNS 2.0?

- Identity Based Networking Services 2.0 ist die neuste Entwicklungsstufe in der identitätsbezogenen Authentifizierung von Cisco
- IBNS 2.0 ist ein Set von verschiedenen 802.1X und Switch Funktionalitäten
- Veränderungen im Bereich des Authenticators und Authentication Server



- Mit IBNS 2.0 wird ein neuer 802.1X Switch-Konfigurationsmodus eingeführt  
→ den sogenannten New-Style



## IBNS 2.0 Funktionen und Vorteile

- Identity Control Policy
  - Ermöglicht eine an die Situation angepasste Authentifizierung
- Concurrent Auth
  - Schnellere Authentifizierung für Nicht-802.1X Clients möglich
- Service Templates
  - Critical und Gäste-VLAN können zentral verwaltet werden
- Multi Auth per MAC VLAN
  - Ermöglicht mehrere unabhängige Authentifizierungen pro Port
- Change of Authorization (CoA) \*
  - Erlaubt das Ändern von Session Attributen nach einer Authentifizierung
- Interface Templates \*
  - Reduziert die repetitiven Interface Kommandos

\*Kein neues IBNS 2.0 Feature.

## Der New-Style

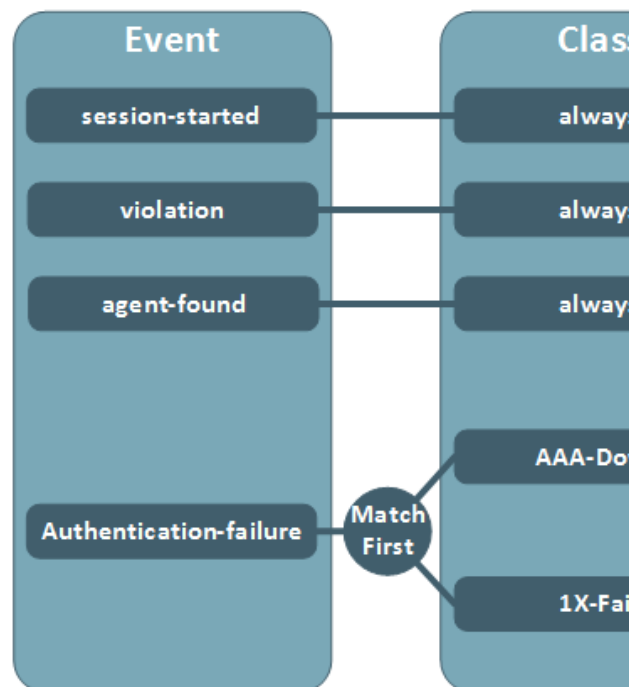
- Der New-Style basiert auf einer richtlinienbasierten Authentifizierung
- Aktiviert wird die Policy Based Configuration (New-Style) mit:

```
s1# authentication display new-style
```

- Die bestehenden 802.1X Interface Kommandos werden automatisch in New-Style kompatible Befehle umgewandelt
- Für jeden Port wird eine eigene Identity Control Policy und passende Service Templates erstellt.

## Identity Control Policy

- Die Policy definiert, welche Aktionen aufgrund von eingetroffenen Events und Bedingungen ausgelöst werden.
- Eine grosse Anzahl an Aktionen, Bedingungen und Events können kombiniert werden.



```

policy-map type control subscriber DOT1X
  event session-started match-all
    10 class always do-until-failure
    10 authenticate using dot1x
  event authentication-failure match-first
    10 class AAA-Down do-all
    10 activate service-template CRIT_AUTH_VLAN
    20 authorize
    30 terminate dot1x
    40 terminate mab
    20 class 1X-Fail do-until-failure
    10 authenticate using mab
  event agent-found match-all
    10 class always do-until-failure
    10 authenticate using dot1x
  event violation match-all
    10 class always do-until-failure
    10 restrict
  
```

## Ein Beispiel

- **Anforderung:** Ein Access Point soll bei einem Ausfall der ISE in ein spezielles VLAN (Critical AP VLAN) verschoben werden
- **Event:** Authentifizierung eines APs während einem Ausfall der ISE
- **Conditions:** Ist die ISE nicht erreichbar? Ist das angeschlossene Gerät ein AP? Ist das Gerät noch nicht authentifiziert?
- **Action:** Anwenden des Critical AP VLANs

## Implementation mit IBNS 2.0

lokales Profiling aktivieren, VLAN definieren

```
device classifier
service-template CRITICAL_AP_VLAN
  vlan 999
```

Condition

```
class-map type control subscriber match-all AAA_SVR_DOWN_UAUTH_AP
  match device-type "Cisco-AIR-LAP"
  match result-type aaa-timeout
  match authorization-status unauthorized
```

Event, Condition und Action in Identity Control Policy verknüpfen

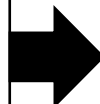
```
policy-map type control subscriber POLICY_DOT1X
  event authentication-failure match-first
  7 class AAA_SVR_DOWN_UAUTH_AP do-until-failure
  10 activate service-template CRITICAL_AP_VLAN
  20 authorize
```

## Interface und Service Templates

```
Interface GigabitEthernet 1/0/1
description 0421 / gep
authentication control-direction in
authentication event fail retry 1
action authorize vlan 333
authentication event server dead
action authorize vlan 666
authentication event no-response
action authorize vlan 333
authentication port-control auto
dot1x pae authenticator
...
```

```
Interface GigabitEthernet 1/0/2
description 0422 / rec
authentication control-direction in
authentication event fail retry 1
action authorize vlan 333
authentication event server dead
action authorize vlan 666
authentication event no-response
action authorize vlan 333
authentication port-control auto
dot1x pae authenticator
...
```

```
policy-map type control subscriber DOT1X
...
template DOT1X-ACCESS
dot1x pae authenticator
access-session control-direction in
access-session port-control auto
...
service-template CRIT_AUTH_VLAN
vlan 666
service-template GUEST_VLAN
vlan 333
```



```
Interface GigabitEthernet 1/0/1
description 0421 / gep
source template DOT1X-ACCESS
service-policy type control subscriber DOT1X
...

Interface GigabitEthernet 1/0/2
description 0422 / rec
source template DOT1X-ACCESS
service-policy type control subscriber DOT1X
```

## Interface und Service Templates

```
Interface GigabitEthernet 1/0/1
description 0421 / gep
authentication control-direction in
authentication event fail retry 1
action authorize vlan 333
authentication event server dead
action authorize vlan 666
authentication event no-response
```

```
policy-map type control subscriber DOT1X
...
template DOT1X-ACCESS
dot1x pae authenticator
access-session control-direction in
access-session port-control auto
...
service-template CRIT_AUTH_VLAN
```

Stack (2 Members)	Global Config	Interface Config	Total Zeilen
802.1X	535	1296	1831
802.1X & IBNS 2.0	609	528	1137

```
description 0422 / rec
authentication control-direction in
authentication event fail retry 1
action authorize vlan 333
authentication event server dead
action authorize vlan 666
authentication event no-response
action authorize vlan 333
authentication port-control auto
dot1x pae authenticator
...
```

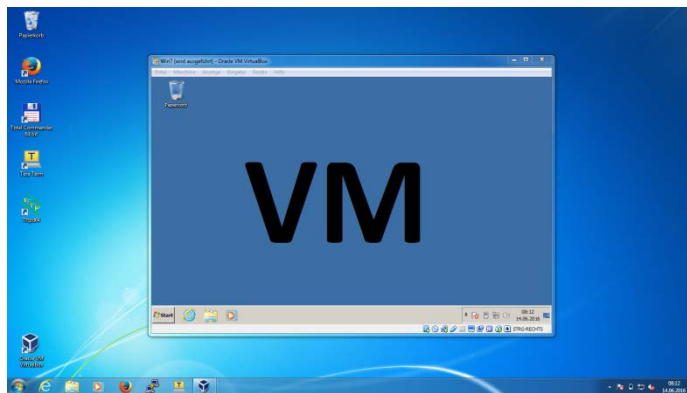
```
Interface GigabitEthernet 1/0/1
description 0421 / gep
source template DOT1X-ACCESS
service-policy type control subscriber DOT1X
...

Interface GigabitEthernet 1/0/2
description 0422 / rec
source template DOT1X-ACCESS
service-policy type control subscriber DOT1X
```

## Multi Auth per MAC VLAN

- Unabhängige Authentifizierungen (je MAC-Adresse) auf einem Port
- Aktivierung auf dem Interface mit

```
S1(int-config)# access-session host-mode multi-auth
```



*Nur mit Catalyst 2960X,  
3650 oder 3850 möglich*



VLAN	VLAN Name	Status	Port
456	Mitarbeiter VLAN	Active	GigabitEthernet 1/0/2
123	Labor VLAN	Active	GigabitEthernet 1/0/2



## Zusätzliche Einstellungen auf der ISE

- Idle Timeout
  - Sobald der Client eine Stunde keine Pakete mehr sendet, wird die Session terminiert
- Periodic Reauthentication
  - Alle 18 Stunden wird eine unterbruchsfreie Reauthentisierung durchgeführt

The screenshot displays the configuration interface for Reauthentication. It includes a checked checkbox for 'Reauthentication', a 'Timer' field set to '65000' with the instruction '(Enter value in seconds )', and a 'Maintain Connectivity During Reauthentication' dropdown menu set to 'RADIUS-Request'. Below this is a section titled 'Advanced Attributes Settings' which contains a configuration entry for 'Radius:Idle-Timeout' set to '3600'.

Reauthentication

Timer  (Enter value in seconds )

Maintain Connectivity During Reauthentication

▼ **Advanced Attributes Settings**

Radius:Idle-Timeout  - +

## Zusammenfassung

- ✓ Grössere Flexibilität bei der Authentifizierung mit Identity Control Policy
- ✓ Mehrere unabhängige Auth. mit Multi Auth per MAC VLAN pro Port
- ✓ Bessere User Experience mit Concurrent Auth
- ✓ Bessere Security durch die periodische Reauthentifizierung
- ✓ Flexiblere und übersichtlichere Konfiguration mit Interface Templates
  
- ✗ Wenig Erfahrung mit New-Style und Identity Control Policy

**Vielen Dank...**

für die Aufmerksamkeit.