

# Neues vom Wächter im Netz



Digitalisierung  
erfolgreich gestalten.

Achim Burger

21.06.2023

# Referent und Housekeeping

- Achim Burger – bei telent seit 2007
  - 2004 – 2007 | Duales Studium – Informationstechnik – Schwerpunkt Netz- & Softwaretechnik
  - Seit Oktober 2007 | System Engineer Wireless, Routing & Switching
  - Hobbies: Radeln, Segeln, Posaunenchor, Kinder
  - Fragen bitte während der Session und gerne beim (alkoholfreien) Feierabendbier oder –kaffee (GET TOGETHER ab ca. 15:45 Uhr)

# Agenda

- **IBNS 2.0 – Was ist das, wie läuft es?**
  - Dynamische Portkonfiguration per Radius-Attribut
  - Ablauf der Authentifizierung wird in einer Policy definiert
- **Was bringen die neuen ISE-Versionen?**
  - Alarmierung auf Authorization Policies
  - Cloud Readiness
  - Neues Lizenzmodell
- **ISE Lifecycle**
  - ISE 3.2 ist salonfähig
  - ISE 2.7 sollte abgelöst werden
  - Es gibt neue Hardware Appliances

# IBNS 2.0 – Was ist das, wie läuft es?

- Ausgangssituation Portkonfiguration:
  - Nur wenige Attribute eines Switchports können dynamisch bei der Authentifizierung geändert werden (VLAN-ID / -Name, ACL, Redirect-URL)
  - Ports müssen manuell passend zum Endgerät konfiguriert werden (z. B. Flexconnect-AP)
  - Port-Descriptions müssen händisch gepflegt werden

# IBNS 2.0 – Was ist das, wie läuft es?

- Ausgangssituation Portkonfiguration:

- Nur wenige Attribute eines Switchports können dynamisch bei der Authentifizierung geändert werden (VLAN-ID / -Name, ACL, Redirect-URL)
- Ports müssen manuell passend zum Endgerät konfiguriert werden (z. B. Flexconnect-AP)
- Port-Descriptions müssen händisch gepflegt werden

```
interface GigabitEthernet1/0/1
description Workstation
switchport access vlan 11
switchport mode access
switchport voice vlan 9
authentication control-direction in
authentication event fail action next-method
authentication event server dead action authorize vlan 10
authentication event server alive action reinitialize
authentication host-mode multi-auth
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication periodic
authentication timer reauthenticate server
authentication timer inactivity server dynamic
authentication violation replace
mab
dot1x pae authenticator
dot1x timeout tx-period 5
```

<- VS. ->

```
interface GigabitEthernet1/0/2
description WLAN-AP
switchport trunk native vlan 8
switchport mode trunk
switchport trunk allowed vlan 8-11
authentication control-direction in
authentication event fail action next-method
authentication event server dead action authorize vlan 10
authentication event server alive action reinitialize
authentication host-mode multi-host
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication periodic
authentication timer reauthenticate server
authentication timer inactivity server dynamic
authentication violation replace
mab
dot1x pae authenticator
dot1x timeout tx-period 5
```

# IBNS 2.0 – Was ist das, wie läuft es?

- Dynamische Portkonfiguration per Radius-Attribut

```
interface GigabitEthernet1/0/1  
source template default-dot1x
```

Tatsächliche Portkonfig  
kommt aus dem Template

```
template default-dot1x  
dot1x pae authenticator  
dot1x timeout tx-period 2  
switchport mode access  
switchport voice vlan 9  
mab  
access-session control-direction in  
access-session closed  
access-session port-control auto  
access-session interface-template sticky timer 20  
authentication periodic  
authentication timer reauthenticate server  
service-policy type control subscriber Dot1x-Default  
!
```

Portkonfig wird bei der  
Authentifizierung geändert

```
template ap-flex  
switchport trunk native vlan 8  
switchport trunk allowed vlan 8-11  
switchport mode trunk  
access-session host-mode multi-host  
description Access Point - Flexconnect  
!
```

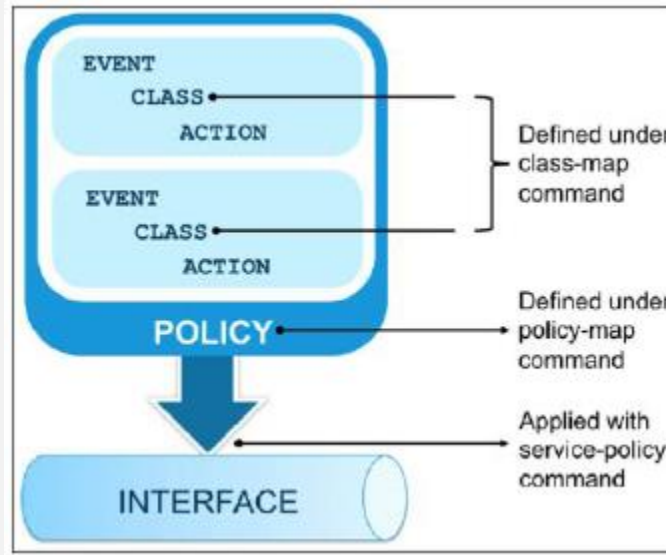
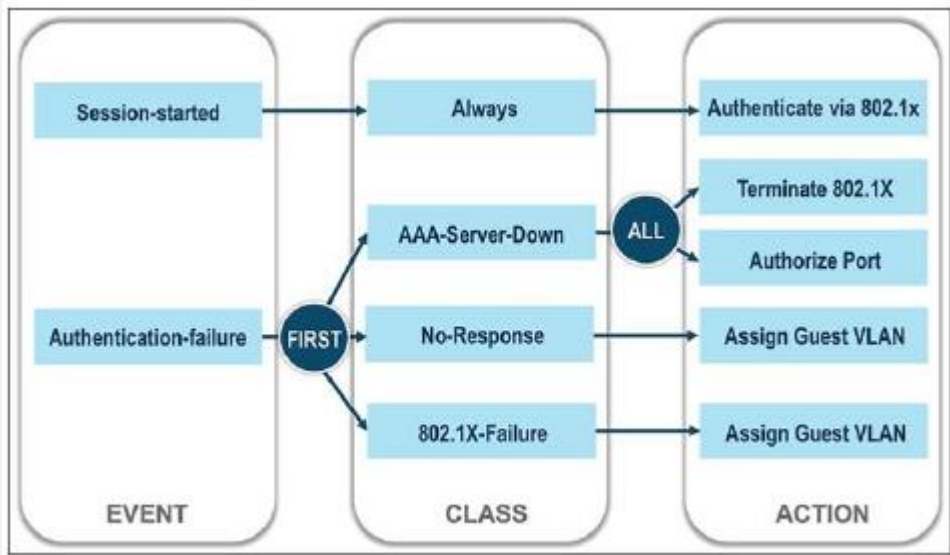
# IBNS 2.0 – Was ist das, wie läuft es?

- Ausgangssituation Authentifizierungsablauf:
  - Viele Befehle auf Interface-Level
  - Ablauf nicht klar erkennbar

```
interface GigabitEthernet1/0/1
description Workstation
switchport access vlan 11
switchport mode access
switchport voice vlan 9
authentication control-direction in
authentication event fail action next-method
authentication event server dead action authorize vlan 10
authentication event server alive action reinitialize
authentication host-mode multi-auth
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication periodic
authentication timer reauthenticate server
authentication timer inactivity server dynamic
authentication violation replace
mab
dot1x pae authenticator
dot1x timeout tx-period 5
!
```

# IBNS 2.0 – Was ist das, wie läuft es?

- Ablauf der Authentifizierung wird als Policy definiert



```
policy-map type control subscriber Dot1x-Default
event session-started match-all
  10 class always do-until-failure
  10 authenticate using dot1x retries 2 retry-time 1 priority 10
  20 authenticate using mab priority 20
event authentication-failure match-first
  5 class DOT1X_FAILED do-until-failure
  10 terminate dot1x
  20 authenticate using mab priority 20
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
  10 activate service-template CRITICAL
  20 authorize
  30 pause reauthentication
  20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
  10 pause reauthentication
  20 authorize
  30 class DOT1X_NO_RESP do-until-failure
  10 terminate dot1x
  20 authenticate using mab priority 20
  40 class MAB_FAILED do-until-failure
  10 terminate mab
  20 authentication-restart 60
  60 class DOT1X_TIMEOUT do-until-failure
  10 terminate dot1x
  20 authenticate using mab priority 20
  70 class always do-until-failure
  10 terminate dot1x
  20 terminate mab
  30 authentication-restart 60
event agent-found match-all
  10 class always do-until-failure
  10 terminate mab
  20 authenticate using dot1x retries 2 retry-time 0 priority 10
event aaa-available match-all
  10 class IN_CRITICAL_VLAN do-until-failure
  10 clear-session
  20 class NOT_IN_CRITICAL_VLAN do-until-failure
  10 resume reauthentication
event inactivity-timeout match-all
  10 class always do-until-failure
  10 clear-session
event violation match-all
  10 class always do-until-failure
  10 replace
```



# Was bringen die neuen ISE-Versionen?

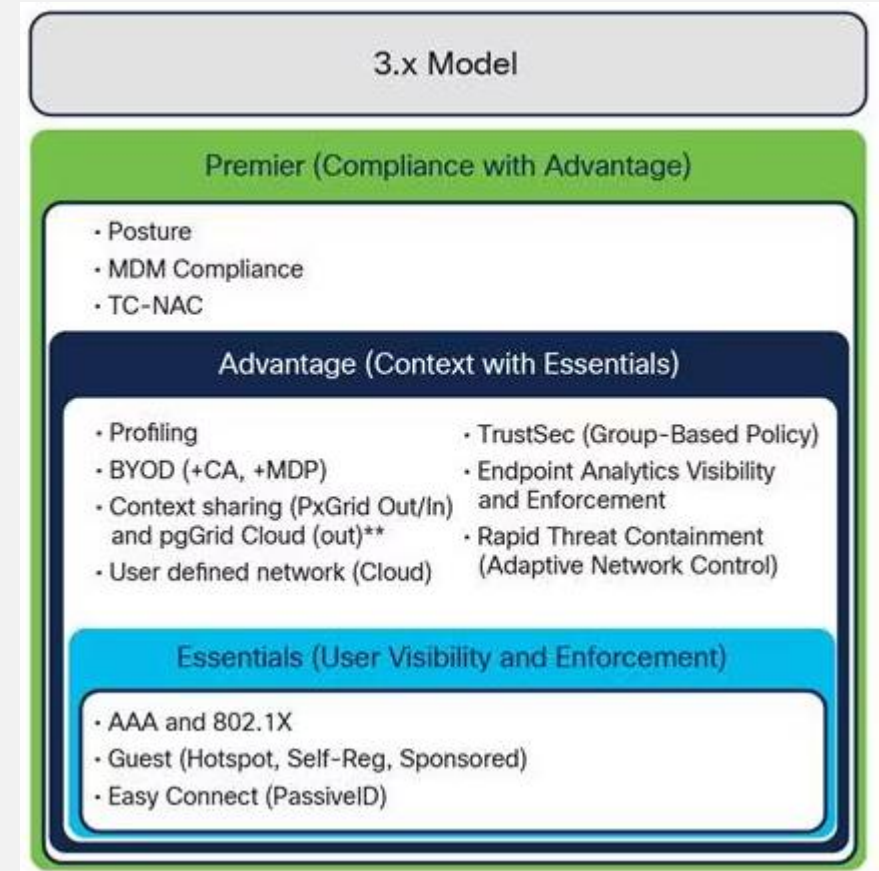
- Alarmierung auf Authorization Policies (ab ISE 3.1)
  - Benachrichtigung bei unbekanntem MAC-Adressen
  - Benachrichtigung bei Versetzen eines Clients in Quarantäne
  - Benachrichtigung bei Ablauf eines Client-Zertifikates
  - Kundenwünsche und –ideen?

# Was bringen die neuen ISE-Versionen?

- Cloud Readiness
  - Ab ISE 3.0 AWS und Azure nicht nativ
  - Ab ISE 3.1 nativ in AWS
  - Ab ISE 3.2 nativ in Azure

# Was bringen die neuen ISE-Versionen?

- Neues Lizenzmodell
  - Ab ISE 3.0 neues Lizenzmodell
  - Aus Base wird Essentials
  - Aus Plus wird Advantage
  - Aus Apex wird Premier
  - Aus Perpetual wird Term-Based
  - Ab ISE 3.1 gibt es Specific License Reservation (SLR)



- VM (R-ISE-VMC-K9=)
- Device Admin license (L-ISE-TACACS-ND=)

# ISE Lifecycle

- ISE 3.2 ist salonfähig
  - Released im Oktober 2022, Patch 2 im Mai 2023
  - Upgrade ist ab Version 2.7 möglich
- ISE 2.7 sollte abgelöst werden
  - Ab 22. September 2023 keine Patches mehr!
  - Migrierte Base-Lizenzen laufen am 31. Oktober 2023 ab!
  - ISE 2.7 ist die letzte Version, die traditionelle Lizenzierung unterstützt!
- Es gibt neue Hardware Appliances
  - SNS-3715, 3755, 3795
  - SNS-3600 wurden abgekündigt, EOL: 2028
  - Fun Fact: SNS-3515 wurde zuletzt von ISE 3.0 unterstützt, SNS-3595 auch noch von ISE 3.2 (EOL: 2024)

# Bonus-Thema

- Wie fühlt sich der Helpdesk beim NAC-Troubleshooting?
  - Zugriff auf ISE und Switch erforderlich
  - ISE Live Log ist leicht unübersichtlich
  - Switch Output ist sehr unübersichtlich
  - Insider-Wissen bzw. KI notwendig
  - telent-Produkt liefert die Lösung!

Cisco ISE

Overview	
Event	5200 Authentication succeeded
Username	1C:6A:7A:E2:B7:7C
Endpoint Id	1C:6A:7A:E2:B7:7C ⓘ
Endpoint Profile	Cisco-Switch
Authentication Policy	Default >> MAB
Authorization Policy	Default >> Basic_Authenticated_Access
Authorization Result	PermitAccess

Authentication Details	
Source Timestamp	2023-05-12 12:50:25.829
Received Timestamp	2023-05-12 12:50:25.829
Policy Server	ab-ise60
Event	5200 Authentication succeeded
Username	1C:6A:7A:E2:B7:7C
User Type	Host
Endpoint Id	1C:6A:7A:E2:B7:7C
Calling Station Id	1C-6A-7A-E2-B7-7C
Endpoint Profile	Cisco-Switch
Authentication Identity Store	Internal Endpoints
Identity Group	RegisteredDevices
Audit Session Id	0608090A000000500F9555E0
Authentication Method	mab
Authentication Protocol	Lookup
Service Type	Call Check
Network Device	C9300-2-ANB
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	10.9.8.6
NAS Port Id	GigabitEthernet1/0/5

Steps	
11001	Received RADIUS Access-Request
11017	RADIUS created a new session
11027	Detected Host Lookup UseCase (Service-Type = Call Check (10))
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15041	Evaluating Identity Policy
15048	Queried PIP - Normalised Radius.RadiusFlowType
15013	Selected Identity Source - Internal Endpoints
24209	Looking up Endpoint in Internal Endpoints IDStore - 1C:6A:7A:E2:B7:7C
24211	Found Endpoint in Internal Endpoints IDStore
22037	Authentication Passed
15036	Evaluating Authorization Policy
15048	Queried PIP - Radius.NAS-Port-Type
15048	Queried PIP - EndPoints.LogicalProfile
15048	Queried PIP - Network Access.AuthenticationStatus
15016	Selected Authorization Profile - PermitAccess
24209	Looking up Endpoint in Internal Endpoints IDStore - 1C:6A:7A:E2:B7:7C
24211	Found Endpoint in Internal Endpoints IDStore
11002	Returned RADIUS Access-Accept

NAS Port Type	Ethernet
Authorization Profile	PermitAccess
Response Time	135 milliseconds

Other Attributes	
ConfigVersionId	82
DestinationPort	1812
Protocol	Radius
NAS-Port	50105
Framed-MTU	1472
Original.UserName	1c6a7ae2b77c
NetworkDeviceProfile	b0699505-3150-4215-a800-6753d45d5f6c
IsThirdPartyDeviceFlow	false
AcqSessionId	ab-ise60/472656968/49
SelectedAuthenticationDomain	Internal Endpoints
AuthenticationStatus	AuthenticationPassed
IdentityPolicyMatchedRule	MAB
AuthorizationPolicyMatchedRule	Basic_Authenticated_Access
EndPointMACAddress	1C-6A-7A-E2-B7-7C
ISEPolicySetName	Default
IdentitySelectionMatchedRule	MAB
TotalAuthenticacy	135
ClientLatency	0
DTLSsupport	Unknown
HostIdentityGroup	Endpoint Identity Groups:RegisteredDevices
Network Device Profile	Cisco
Location	LocationAll Locations
Device Type	Device TypeAll Device Types
IPSEC	IPSEC/CAs IPSEC DeviceNo
LogicalProfile	Infrastructure Network Devices
Name	Endpoint Identity Groups:RegisteredDevices
RADIUS Username	1C:6A:7A:E2:B7:7C
Device IP Address	10.9.8.6
CPMSessionId	0608090A000000500F9555E0
Called-Station-Id	68:2C:7B:8D:8A:05
CiscoAVPair	service-type=Call Check,audit-session-id=0608090A000000500F9555E0,method=mab,client-iff-id=371836169,vlan-id=8,AuthenticationIdentityStore=Internal Endpoints
UseCase	Host Lookup

Result	
UserName	1C:6A:7A:E2:B7:7C
User-Name	1C-6A-7A-E2-B7-7C
Class	CACS:0608090A000000500F9555E0:ab-ise60/472656968/49
cisco-av-pair	profile-name=Cisco-Switch
License Types	Essential license consumed.

Session Events	
2023-05-12 12:50:25.841	RADIUS Accounting start request
2023-05-12 12:50:25.829	Authentication succeeded

```
C9300-2-ANB#show access-s int g1/0/5 det
Interface: GigabitEthernet1/0/5
IIF-ID: 0x1629C509
MAC Address: 1c6a.7ae2.b77c
IPv6 Address: fe80::1e6a:7aff:fee2:b77c
IPv4 Address: 10.9.8.199
User-Name: 1C-6A-7A-E2-B7-7C
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Common Session ID: 0608090A000000500F9555E0
Acct Session ID: 0x00000048
Handle: 0xf2000046
Current Policy: Dot1x-Default
```

```
Server Policies:

Method status list:
Method      State
dot1x      Stopped
mab        Authc Success
```

```
C9300-2-ANB#show mac add int g1/0/5
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
8       1c6a.7ae2.b77c  STATIC   Gi1/0/5
Total Mac Addresses for this criterion: 1
C9300-2-ANB#show der int g1/0/5
Building configuration...
```

```
Derived configuration : 427 bytes
!
interface GigabitEthernet1/0/5
switchport access vlan 8
switchport mode access
switchport voice vlan 10
authentication periodic
authentication timer reauthenticate server
access-session closed
access-session port-control auto
access-session interface-template sticky timer 20
mab
dot1x pae authenticator
dot1x timeout tx-period 10
spanning-tree portfast
service-policy type control subscriber Dot1x-Default
end
C9300-2-ANB#
```

---

# Vielen Dank für Ihre Aufmerksamkeit!

© 2023 telent GmbH  
Alle Rechte vorbehalten

## Kontaktdaten:

Achim Burger  
Technology Center

Mail: [achim.burger@telent.de](mailto:achim.burger@telent.de)

Digitalisierung  
erfolgreich gestalten.