



Cisco UC –

Identity Management und
Identity Networking



Yves Fauser

Technical Solutions Architect - Voice/UC

Public Sector Deutschland

fauser@cisco.com

26.02.09



CCIE Voice, CCIE R&S #8055

AGENDA

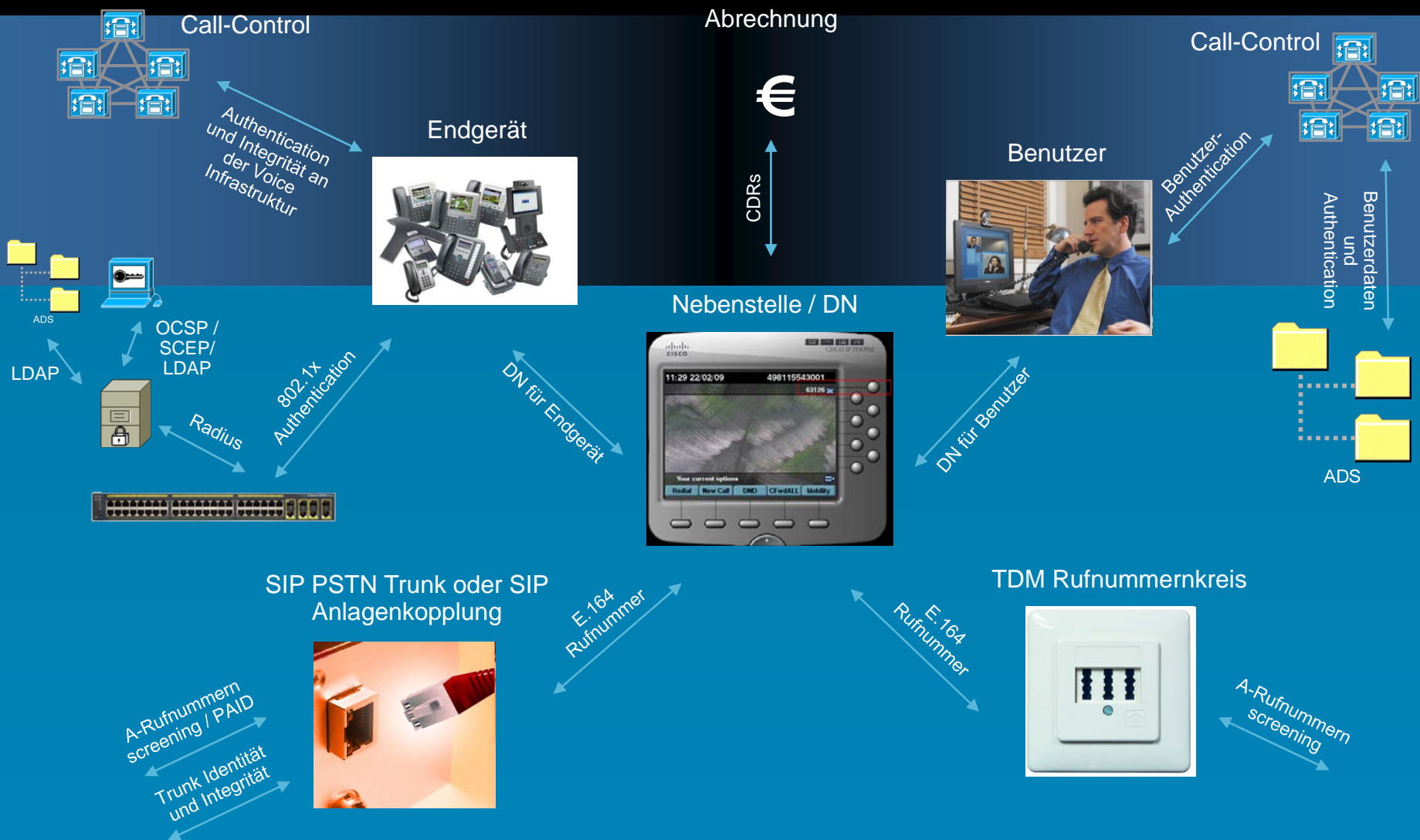
- Arten von Identität in VoIP Netzen
- Endgeräte und Benutzerverwaltung bei Cisco's UC Lösung
- Authentisierung und Integritätsprüfung für Endgeräte (SIP, H.323 und SCCP) und IP Trunks (H.323 und SIP)
- Identity Based Networking für VoIP Switchports auf Cisco Switches



Arten von Identität in VoIP Netzen



Was sind eigentlich die Identitäten in einem VoIP Netz ?



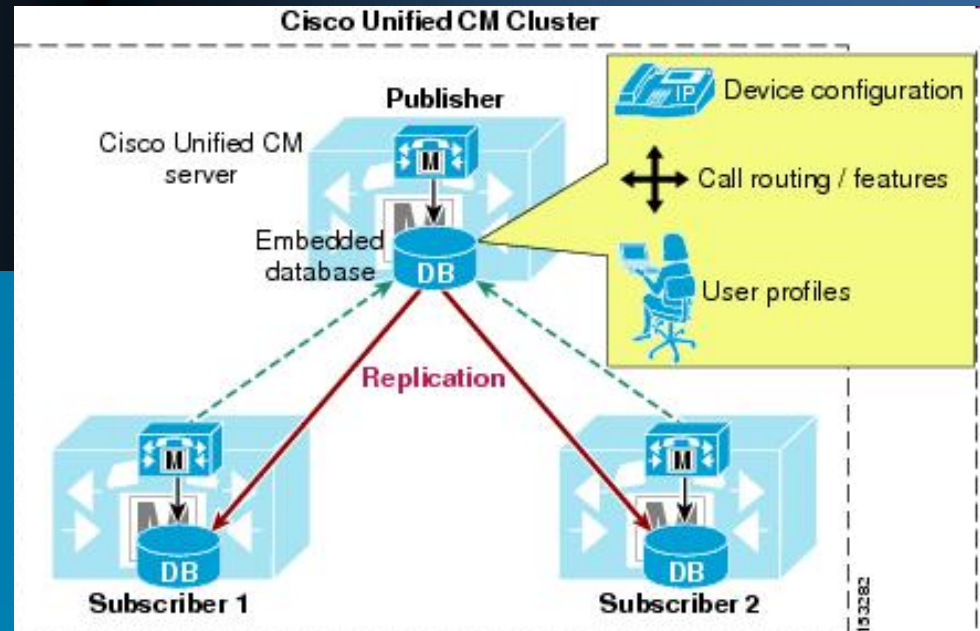


Endgeräte und Benutzerverwaltung bei Cisco's UC Lösung



Cisco Unified Communication Manager Datenbank

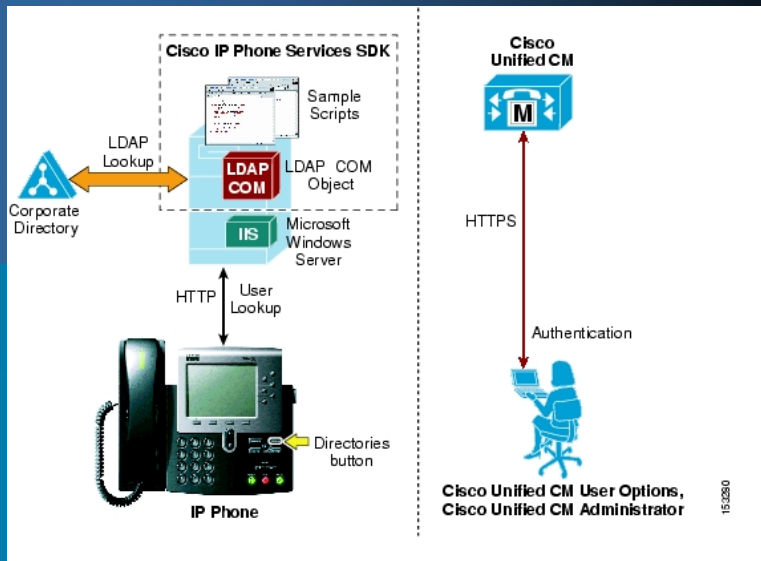
- Alle Endgeräte, Eigenschaften des Systems, Routing Regeln, Trunks in die “Außenwelt” liegen in einer SQL Datenbank (auf Sybase Basis)
- Benutzer liegen ebenfalls in der Datenbank, können aber mit einem LDAP connector Importiert werden.
- Benutzerprofile, mit deren Rufnummern liegen ebenfalls in der Datenbank (für Rufnummernmobilität mit Cisco Endgeräten)



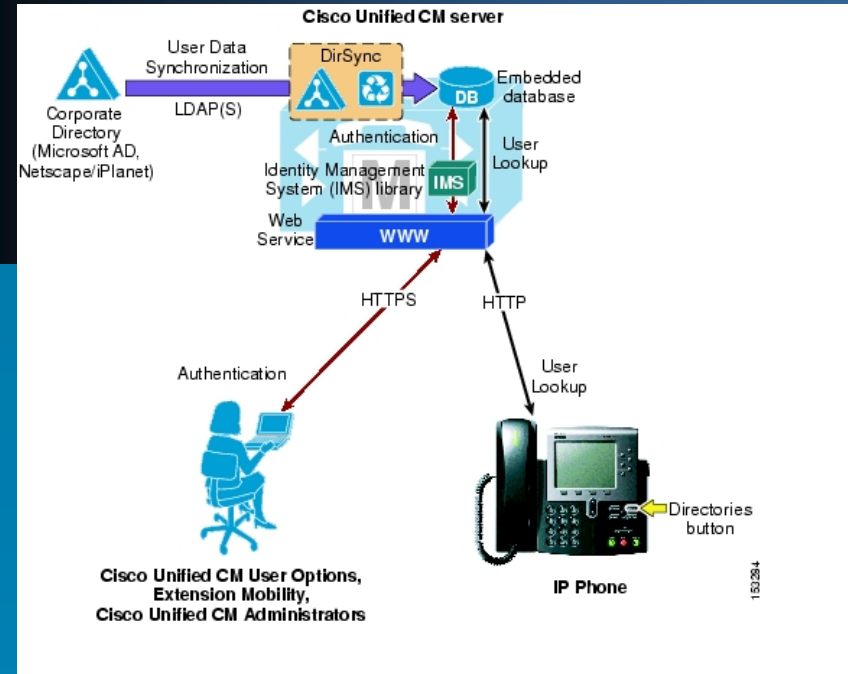
- Die Datenbank wird von einem Publisher Server auf bis zu 16 Subscriber repliziert. Die Subscriber haben eine Read-Only Datenbank, mit Schreibzugriff auf einige Felder wie z.B. Rufumleitungen, Rufnummern-Mobilität, etc.
- Für alle Konfigurationsdaten steht eine XML / SOAP Schnittstelle zur Verfügung um eigene Provisionierungssysteme zu programmieren

Directory Integration

Entweder

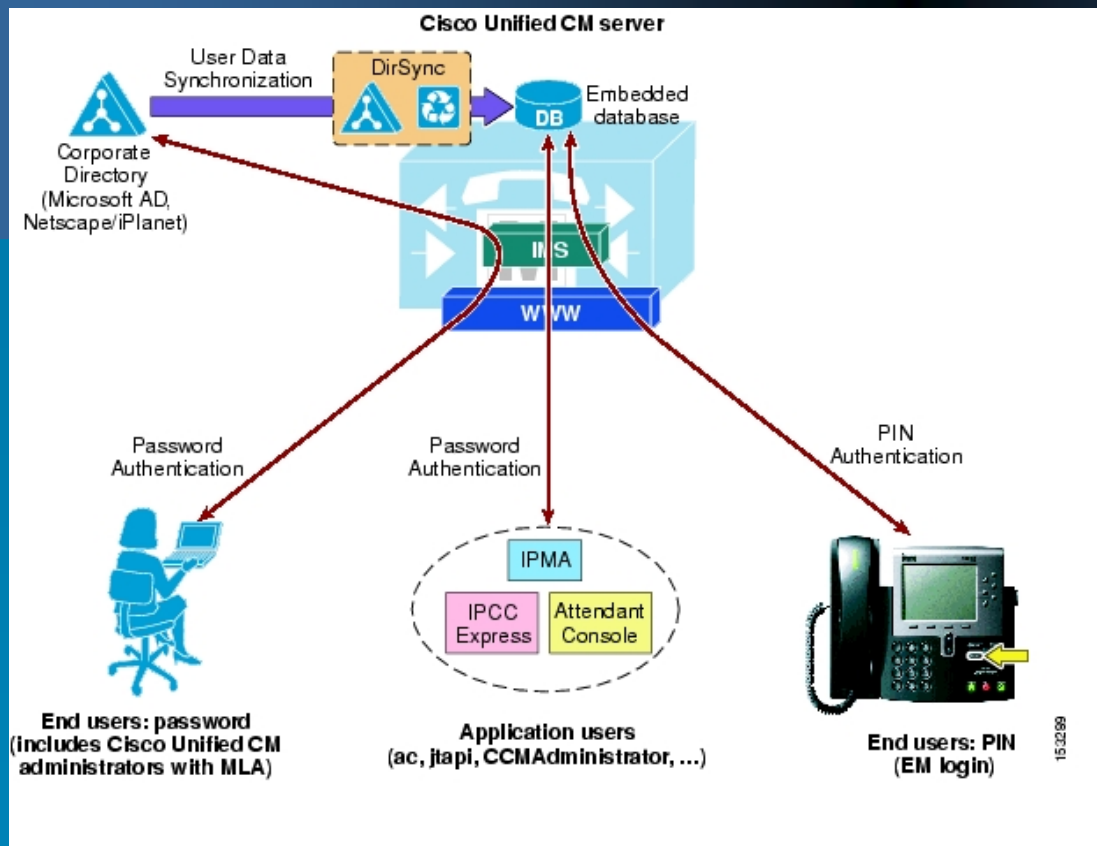


Oder



- Lookup - elektronisches Telefonbuch
- Benutzer-Authentication
- Authentication für IP Phone End-User (Rufnummernmobilität "extension mobility" und Self-Service Portal)
- Authentication für Rufnummernmobilität, User Self Service und Administratoren

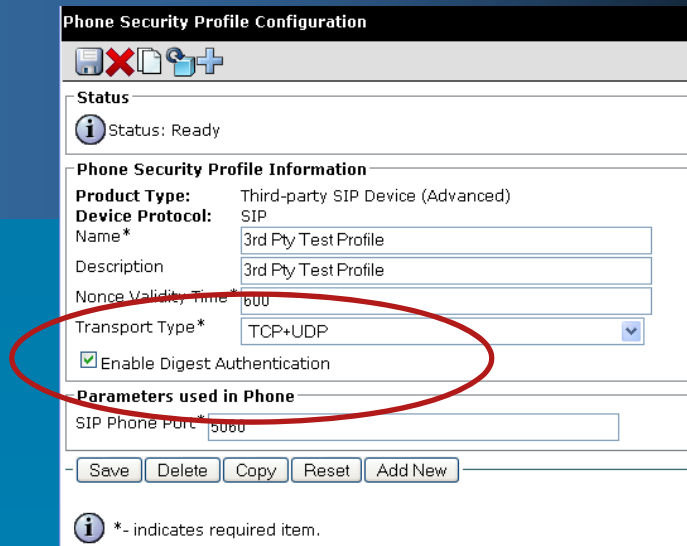
LDAP Authentication



1. First, a user connects to the Unified CM User Options page via HTTPS and attempts to authenticate with a user name and password.
2. Unified CM then issues an LDAP query for the user name jsmith, using the value specified in the LDAP Search Base on the LDAP Authentication configuration page as the scope for this query.
3. The corporate directory server replies via LDAP with the full Distinguished Name (DN) of user jsmith (for example, "cn=jsmith, ou=Users, dc=vse, dc=lab").
4. Unified CM then attempts an LDAP bind using this full DN and the password provided by the user.
5. If the LDAP bind is successful, Unified CM allows the user to proceed to the configuration page requested.

Endgeräteverwaltung – SIP 3rd Party Endpunkte

1. Konfiguration des Security Profile



Phone Security Profile Configuration

Status
Status: Ready

Phone Security Profile Information

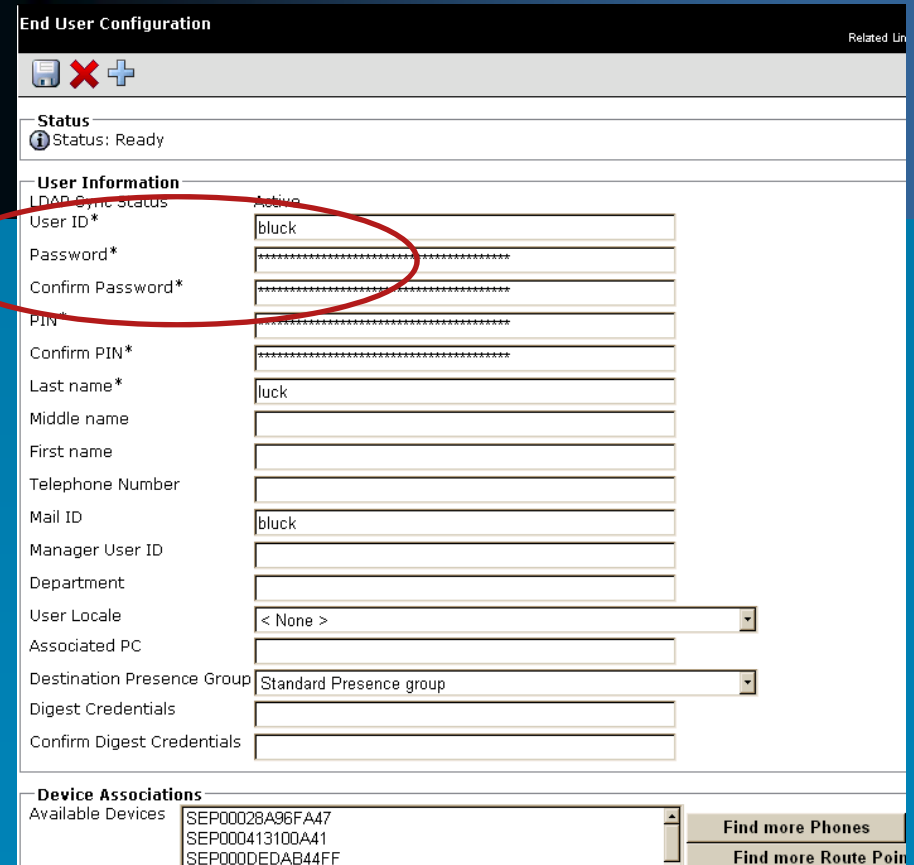
Product Type: Third-party SIP Device (Advanced)
Device Protocol: SIP
Name*: 3rd Pty Test Profile
Description: 3rd Pty Test Profile
Nonce Validity Time: 600
Transport Type*: TCP+UDP
☒ Enable Digest Authentication

Parameters used in Phone
SIP Phone Port*: 5060

Save Delete Copy Reset Add New

*- indicates required item.

2. Konfiguration des End User (oder LDAP)



End User Configuration

Status
Status: Ready

User Information

LDAP Sync Status: Active
User ID*: bluck
Password*:
Confirm Password*:
PIN*:
Confirm PIN*:
Last name*: luck
Middle name:
First name:
Telephone Number:
Mail ID: bluck
Manager User ID:
Department:
User Locale: < None >
Associated PC:
Destination Presence Group: Standard Presence group
Digest Credentials:
Confirm Digest Credentials:

Device Associations

Available Devices
SEP00028A96FA47
SEP000413100A41
SEP000DEDA844FF

Find more Phones
Find more Route Points

Endgeräteverwaltung – SIP 3rd Party Endpunkte

3. 3rd party SIP Device anlegen

Select the type of phone you would like to create

Phone Type* -- Not Selected --

Next

* - indicates
- Device re

- Cisco 7970
- Cisco 7971
- Cisco 7985
- Cisco ATA 186
- Cisco IP Communicator
- Cisco Unified Personal Communicator
- H.323 Client
- IP-STE
- Motorola CN622
- Third-party SIP Device (Advanced)
- Third-party SIP Device (Basic)

4. User zuordnen

Ein Benutzer muß pro
Device angelegt werden

Protocol Specific Information

Presence Group* Standard Presence group

MTP Preferred Originating Codec* 711ulaw

SIP Phone Security Profile* 3rd Pty Test Profile

Rerouting Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile* < None >

Digest User < None >

☐ Media Termination Point Require

☐ Unattended Port

Endgeräteverwaltung – SIP 3rd Party Endpunkte

Konfiguration der Authorization ID auf dem Phone.

Nebenstelle: Diese muss vom Telefon bei der Register message verwendet werden

CUCM IP

Proxy and Registration	
Proxy:	172.18.197.224
Outbound Proxy:	
Register:	<input type="checkbox"/>
Register Expires:	3600
Use DNS SRV:	<input type="checkbox"/>
Proxy Fallback Intvl:	3600
Use Outbound Proxy:	<input type="checkbox"/>
Use OB Proxy In Dialog:	<input type="checkbox"/>
Make Call Without Reg:	<input type="checkbox"/>
Ans Call Without Reg:	<input type="checkbox"/>
DNS SRV Auto Prefix:	<input type="checkbox"/>
Proxy Redundancy Method:	Normal

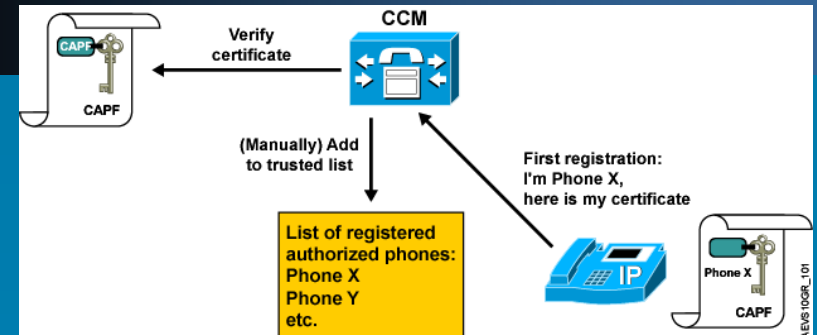
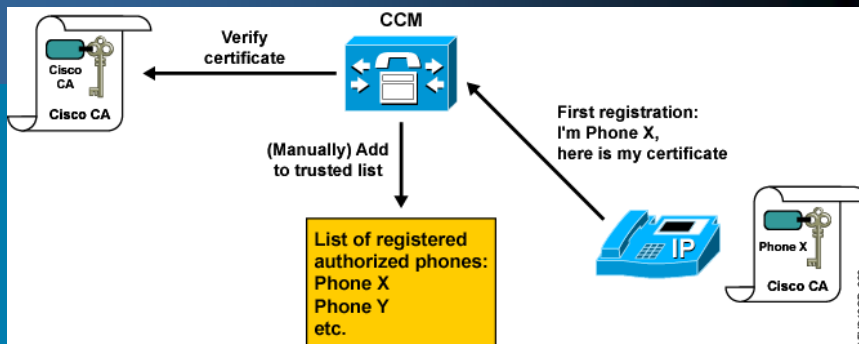
Subscriber Information	
Display Name:	1010
Password:	*****
Auth ID:	bluck
Mini Certificate:	
S RTP Private Key:	
User ID:	1010
Use Auth ID:	<input type="checkbox"/>

- Bei einigen Implementationen wie z.B. XLITE muss die Rufnummer = der Auth ID sein, damit das Telefon sich mit der richtigen Nummer registriert

Linksys Beispiel

Endgeräteverwaltung – Cisco Endpunkte

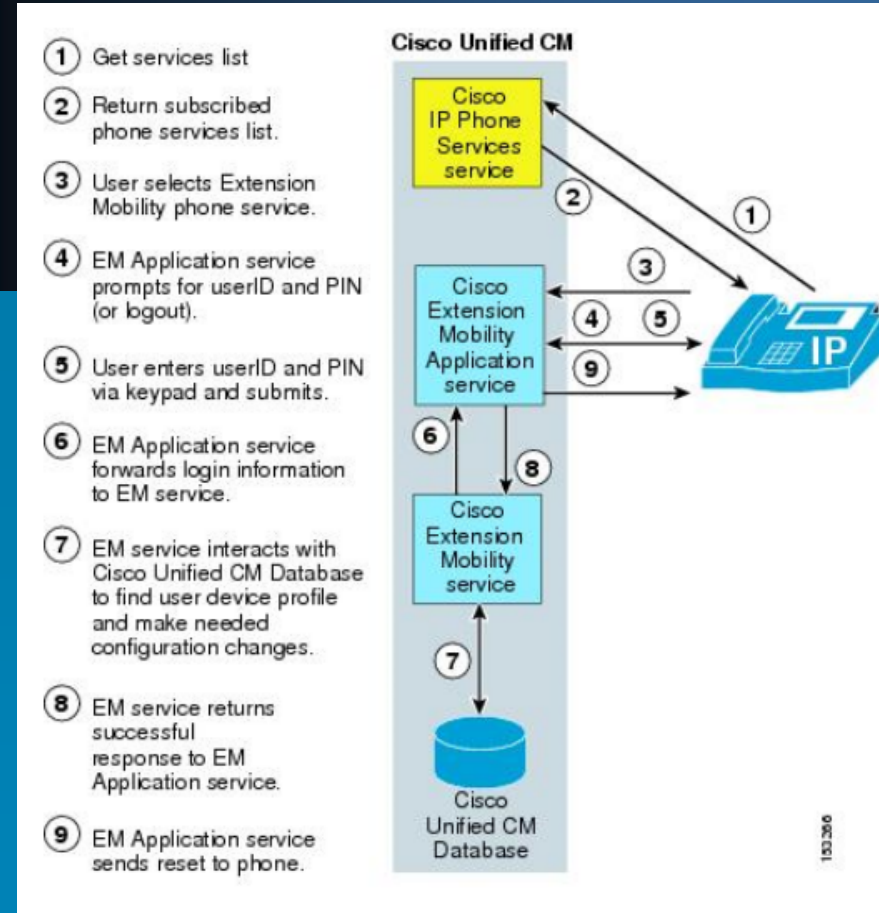
- Nach der Initialen Installation werden Cisco Endpunkte nur über Ihre MAC Adresse und dem Gerätetyp identifiziert
- Anders als bei 3rd Party SIP Endpunkten hängt die Identität des Endpunktes nicht an einer Benutzer-Identität.
- Konfigurationen der Telefone werden vom Phone per TFTP heruntergeladen. Diese Konfigurationsdatei ist signiert und verschlüsselt. Über den TFTP Service wird auch die Verwaltung der Firmware Versionen



- Cisco Telefone werden ab Werk mit einem von einer Cisco Root CA signiertem X.509v3 Zertifikat ausgeliefert (MIC)
- Der CUCM vertraut nach der Installation allen Endgeräte-Zertifikaten die von einer Cisco Manufacturing CA signiert wurden
- Nach der Installation von Zertifikaten auf den Telefonen, die von der Kunden-CA signiert wurden (LSCs), können die Cisco Root CA Zertifikate vom CUCM gelöscht werden
- Der Kunde kann den CAPF Dienst (Certificate Authority Proxy Function) verwenden um eigene Zertifikate auf die Telefone zu bringen (LSC)
- Der CAPF ist dabei eine intermediate CA
- Der Zertifikat vom CAPF kann durch die Kunden-Eigene CA signiert werden

Cisco Endpunkte - Rufnummernmobilität

- Mit Cisco Endpunkten wird die Benutzer ID nicht für die SIP Registrierung verwendet
- Die Benutzererkennung wird im Normalfall verwendet um Rufnummern-Mobilität zu ermöglichen
- Dem Benutzer ist ein Benutzerprofil mit einer Rufnummer zugeordnet, diese Rufnummer kann identisch mit der Rufnummer eines Telefones sein das dem Benutzer zugeordnet ist
- Der Benutzer meldet sich über die XML Schnittstelle der Telefones beim CUCM an, dann wird dem Telefon das Benutzerprofil übertragen

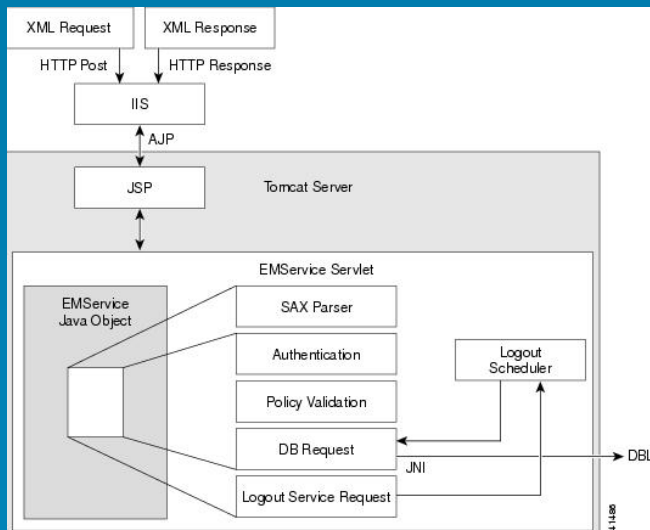


Cisco Endpunkte – Rufnummernmobilität – Externer Login Dienst

- Über eine externe XML API (Extension Mobility API) kann der Login/Logout Vorgang auf Cisco Endpunkten automatisiert werden
- Beispiele sind z.B. Smart-Card Logins an Thin-Clients die mit Rufnummernmobilität gekoppelt sind.

Beispiel :

Testaufbau mit SUN Ray Ultra Thin Clients im SUN Solution Center in München





Authentisierung und Integritätsprüfung IP Trunks (H.323 und SIP)



Authentisierung und Integritätsprüfung IP Trunks (H.323 und SIP)

- Bei H.323 Trunks und MGCP ist nur IPSec möglich. IPSec kann native beim CUCM auf der Plattform betrieben werden. Wird ein IPSec Profile verwendet, muß jeglicher Traffic von spezifischen IP Adressen IPSec Encrypted sein. Authentication Options : pre-shared-key oder Zertifikate
- SIP Trunks können entweder nur Authenticated sein (MD5-Digest Authentication) oder über TLS gesichert. Wird TLS verwendet müssen natürlich Zertifikate verwendet werden

SIP Trunk Security

SIP Trunk Security Profile Information	
Name *	Non Secure SIP Trunk Profile
Description	Non Secure SIP Trunk Profile authenticated by null Str
Device Security Mode	Non Secure
Incoming Transport Type *	TCP+UDP
Outgoing Transport Type	TCP
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins) *	600
X.509 Subject Name	
Incoming Port *	5060
<input type="checkbox"/> Enable Application Level Authorization	
<input checked="" type="checkbox"/> Accept Presence Subscription	
<input checked="" type="checkbox"/> Accept Out-of-Dialog REFER	
<input checked="" type="checkbox"/> Accept Unsolicited Notification	
<input type="checkbox"/> Accept Replaces Header	
<input type="checkbox"/> Transmit Security Status	

IPSec

IPSEC Policy Details	
Policy Group Name *	
Policy Name *	
Authentication Method *	Certificate
Preshared Key	Pre-shared Key
Peer Type *	Same
Certificate Name	
Destination Address *	
Destination Port *	ANY
Source Address *	
Source Port *	ANY
Mode *	Transport
Remote Port *	500
Protocol *	TCP
Encryption Algorithm *	DES
Hash Algorithm *	SHA1
ESP Algorithm *	Null Encryption
Phase 1 DH Group	

H.323 / TDM A-Number Screening und SIP Provider Asserted Identity (PAID / PPID)

- A-Rufnummer = Identity der Rufnummer des Teilnehmers
- Wird vom Provider abgeprüft, nur Rufnummern die zu dem Rufnummernkreis des Anschlusses passen sind erlaubt
- CLIP-NO-Screening erlaubt das Verwenden von User Provided Numbers als A-Rufnummer, dabei wird aber eine ACgPN mit der Trunk Nummer hinzugefügt
- SIP Abbildung davon ist P-Asserted-Identity und P-Preferred-Identity, damit wird in SIP auch das Problem mit verborgenen Rufnummern gelöst
- RFC 4474 definiert auch die Verwendung von Zertifikaten zu Sicherung von Identitäten. Ist aber noch nicht verbreitet

```
Calling Party Number i = 0x2181, '8974500127'  
Plan:ISDN, Type:National  
Called Party Number i = 0xC1, '406891002'  
Plan:ISDN, Type:Subscriber(local)
```

```
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=0530d61a-70ea-4796-b0d6-6d9d6e4f3b14-19198220  
SIP Display info: "Anonymous"  
SIP from address: sip:anonymous@anonymous.invalid  
SIP tag: 0530d61a-70ea-4796-b0d6-6d9d6e4f3b14-19198220  
Allow-Events: presence  
P-Asserted-Identity: "Ren\303\251 Fran\303\247ais" <sip:+4981199881309@25.1.1.83>  
Supported: 100rel,timer,resource-priority,replaces  
Min-SE: 1800  
Remote-Party-ID: "Ren\303\251 Fran\303\247ais" <sip:+4981199881309@25.1.1.83>;party=calling;screen=yes;privacy=full  
Content-Length: 206  
User-Agent: Cisco-CUCM7.0  
Privacy: id  
To: <sip:30011003@25.1.1.82>  
SIP to address: sip:30011003@25.1.1.82  
Contact: <sip:+4981199881309@25.1.1.83:5060;transport=tcp>  
Contact Binding: <sip:+4981199881309@25.1.1.83:5060;transport=tcp>  
URI: <sip:+4981199881309@25.1.1.83:5060;transport=tcp>  
SIP contact address: sip:+4981199881309@25.1.1.83:5060
```



Identity Based Networking für VoIP Switchports auf Cisco Switches



802.1X Voice Overview

- Ein Voice-Port gehört zu zwei VLANs
 - **Native** oder Port VLAN Identifier (**PVID**)
 - **Auxiliary** oder Voice VLAN Identifier (**VVID**)
- Erlaubt die Konfiguration von 802.1x auf dem Daten VLAN (und Authentisierung des Voice VLAN im untagged vlan)
- Voice traffic ist ausschließlich im Voice VLAN (VVID)
- Untagged data traffic (Ohne VLAN Tag) geht vom PC direkt in das Native VLAN (PVID)



Cisco Discovery Protocol (CDP)

- Cisco Discovery Protocol erscheint erstmals 1994, als erstes Discovery Protokoll in der Industrie
- CDP ermöglicht es Managementsystemen automatisch über die an dem System angeschlossenen (Nachbar) Systeme eine Übersicht zu bekommen
- CDP läuft auf Cisco Geräten, wurde aber auch lizenziert um auf Drittherstellergeräten zu laufen (Z.B. HP Procurve, etc)
- CDP läuft auf Ethernet, ATM und Frame Relay Verbindungen, und es ist unabhängig vom eingesetzten Protokoll (z.B. TCP/IP, IPX, AppleTalk, etc).

Cisco Discovery Protocol version 2

- Eine zweite Version des Protokolls, CDPv2, verwendet zusätzliche TLVs (Type Length Value Elemente) um erweiterte Informationen zu transportieren, und auszutauschen :
- CDPv2 unterstützt :
 - Power Negotiation
 - Vlan Aushandlung
 - Switch QOS Trust Boundary extension zum Phone
 - Phone detection für 802.1x authentication bypass
 - OER (Optimized Edge Routing)
 - Cisco Emergency Responder (basiert auf CDP MIB)
- CDP installed base
 - +11M IP Phones
 - switches, routers und access points

LLDP (IEEE 802.1AB)

- LLDP = Link Layer Discovery Protocol
- Cisco entwickelte mit dem IEEE und anderen Industrieteilnehmern daran 802.1AB (Station and Media Access Control Connectivity Discovery zu Standardisieren– dies wurde später zum Link Layer Discovery Protocol LLDP). LLDP erschien im Mai 2005
- LLDP ermöglicht eine Standardbasierte Discovery Methode zwischen verschiedenen Herstellern
 - Device Discovery in Multi-Vendor Netzwerken
 - Network inventory
 - Network device capabilities
 - Erkennen von inkorrekten Konfigurationen (Duplex, etc.)

LLDP-MED

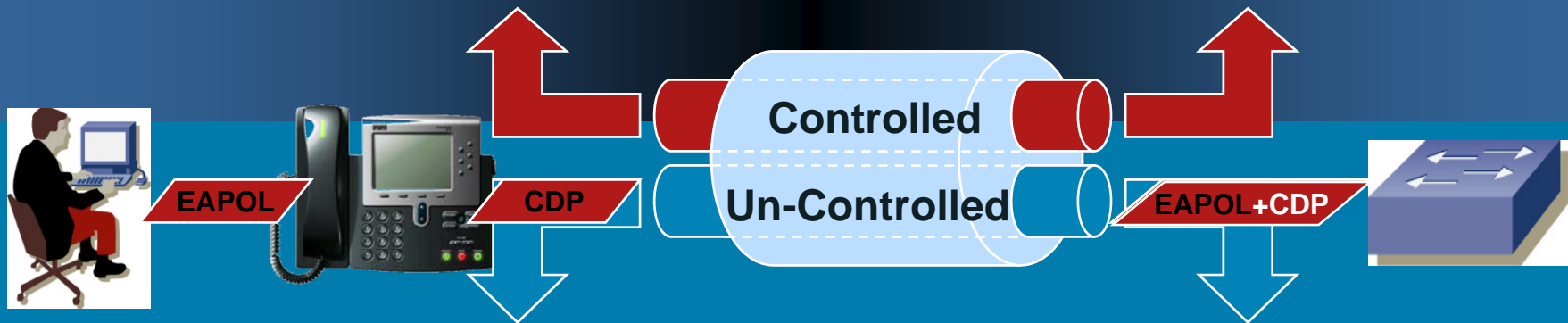
- MED - Media Endpoint Discovery
- TIA (Telecommunications Industry Association) TR-41.4 subcommittee Erweiterungen von LLDP, um spezielle Anforderungen der IP Telefonie zu erfüllen
- LLDP-MED Ermöglicht :
 - Interoperabilität zwischen Herstellern
 - Inventory management: Location, version, etc
 - E-911, emergency service mit location management
 - Troubleshooting: duplex, speed, network policy
 - Fast start, automatic network policy convergence: L2, L3, VLAN
 - MIB support
 - Plug and Play

LLDP-MED Concept

- LLDP-MED ist ähnlich einer Standardbasierte Implementation von CDPv2
 - Capabilities Discovery – Was für ein Device ist angeschlossen
 - LAN Speed und Duplex Discovery
 - Network Policy Discovery – VLAN Vergabe
 - Location Identification Discovery
 - Etc.

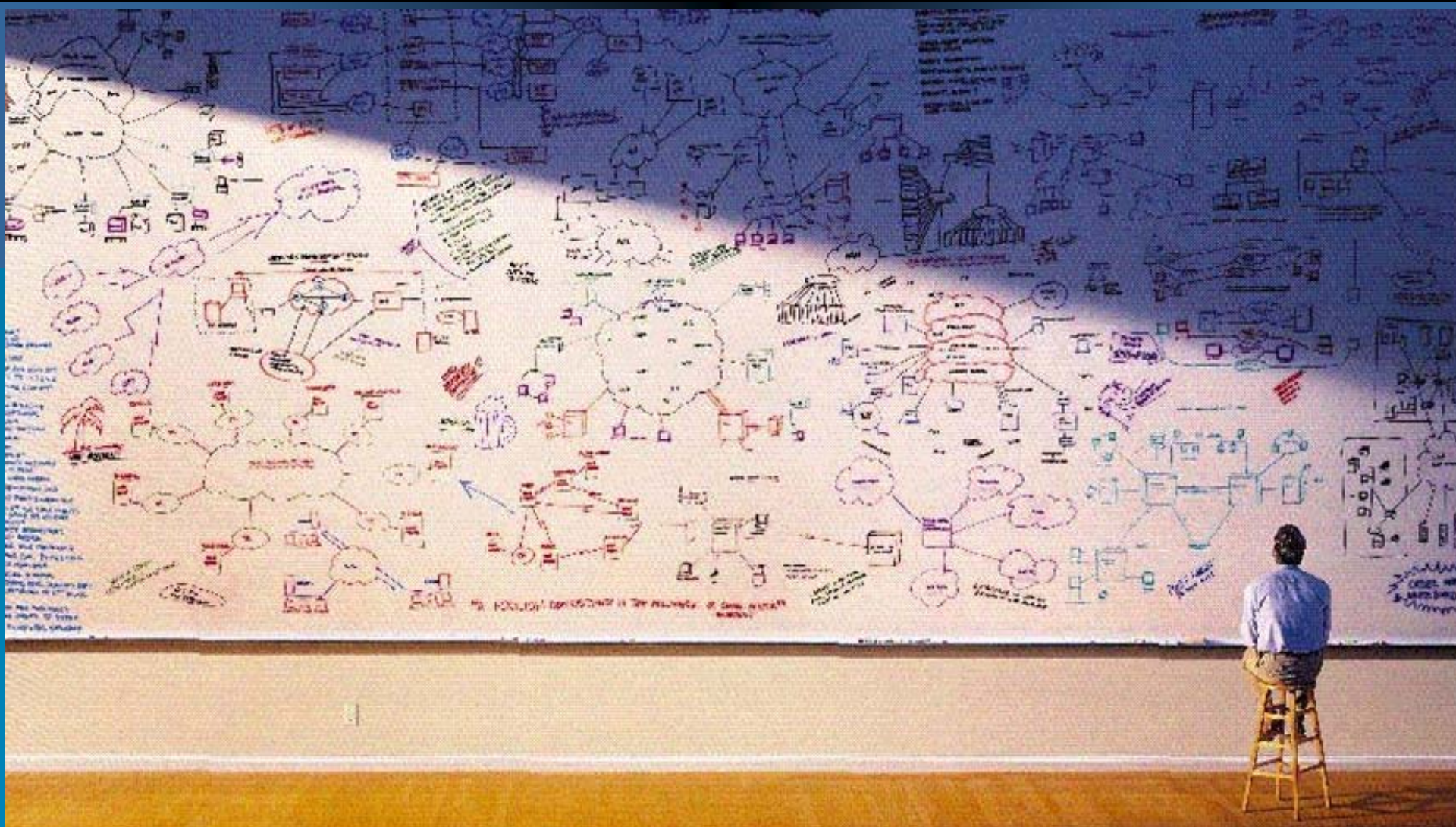
802.1X und Voice Overview

Der “Controlled” Port ist nur offen wenn eine Authentisierung über 802.1X erfolgt ist (oder die Backup-Methode zuschlägt (Auth Fail VLAN, Guest VLAN, MAB,etc.)



Der “uncontrolled” Port ist im Default-Zustand **NUR** offen für Extensible Authentication Protocol over LAN (EAPOL) **UND** CDP traffic LLDP und LLDP-MED sind erst möglich nachdem der Port Authentisiert ist

So, jetzt mal zu den Details



Lösung 1:

Statischer 802.1Q Trunk, kein CDPv2, kein LLDP-MED und kein 802.1x



Vorteil :

- Einfachste Konfiguration

Nachteil :

- Voice-VLAN ist völlig ungeschützt !!
- Kein 802.1x möglich, da es sich um einen Trunk Port handelt
- Voice-VLAN muss auf dem Telefon entweder über DHCP oder per manueller Konfiguration bekanntgegeben werden

IOS

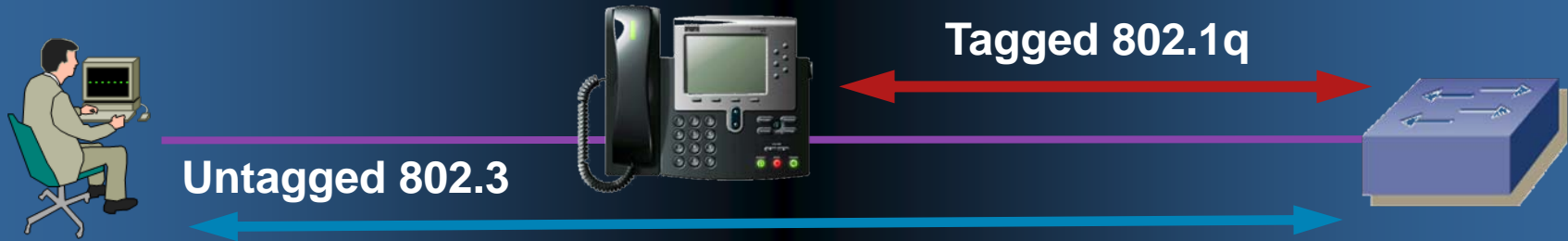
```
interface FastEthernet0/48
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 10
  switchport mode trunk
  switchport nonegotiate
  spanning-tree portfast
```

Weitere Nachteile :

- Bei der Nutzung von DHCP zur voice Vlan Vergabe muss der DHCP Admin die VLAN Struktur kennen, und aktuell halten

Lösung 2 :

Dynamisches Voice VLAN vergeben über CDPv2 od. LLDP-MED, aber kein 802.1x, und kein 802.1x zum PC



Vorteil :

- Einfache Konfiguration
- Durch CDPv2 oder LLDP-MED wird das Voice-VLAN vergeben. Voice-VLAN wird aber auch ohne CDPv2 oder LLDP-MED aktiv
- Leichter in der Administration (z.B. Keine DHCP zu VLAN Korrelation oder manuelle Konfiguration am Telefon nötig)
- 802.1x für den PC bleibt möglich (anders als beim Trunk-Port)

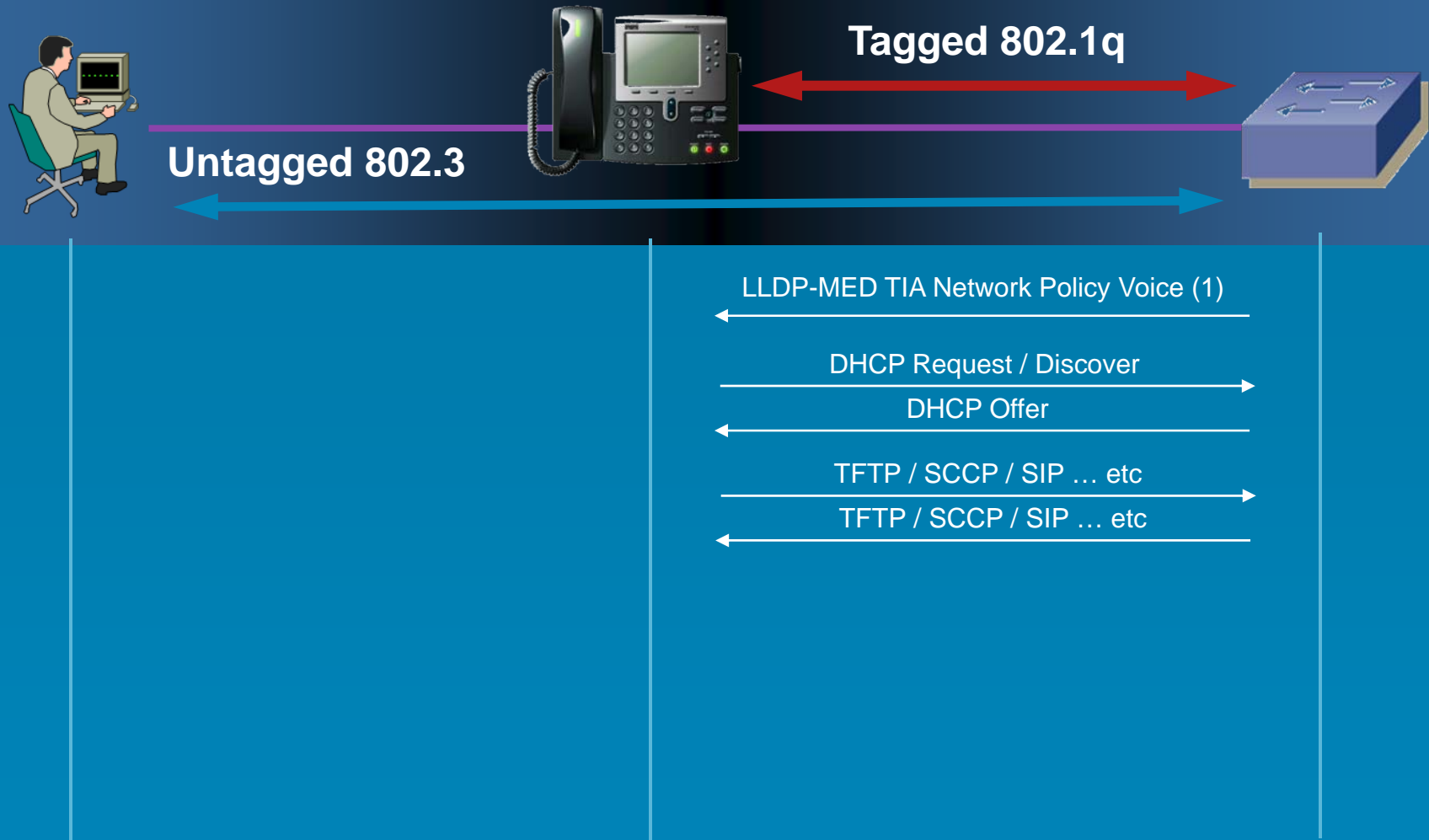
IOS

```
interface FastEthernet0/2
switchport mode access
switchport access vlan 10
switchport voice vlan 20
spanning-tree portfast
```

Nachteil :

- Keinerlei Schutz für das Voice-VLAN ! (Wie statischer Trunk Port)
- Die Kombination mit 802.1x Authentisierung für den PC, ohne 802.1x Phone Authentisierung ist nur möglich, wenn CDPv2 verwendet wird ! Mit LLDP-MED ist dies nicht möglich

Lösung 2 (Flow-Chart zu LLDP-MED) : Dynamisches Voice VLAN vergeben über CDPv2 od. LLDP-MED, aber kein 802.1x, und kein 802.1x zum PC



Lösung 3 :

Dynamisches Voice VLAN vergeben über CDPv2, aber ohne 802.1x, kein 802.1x zum PC, Authentisierung über CDPv2



Vorteil :

- Einfache Konfiguration
- Durch CDPv2 wird das Voice-VLAN vergeben. Voice-VLAN wird ohne CDPv2 nicht aktiv. Schwerer für Angreifer
- Leichter in der Administration (z.B. Keine DHCP zu VLAN Korrelation oder manuelle Konfiguration am Telefon nötig)

Nachteil :

- CDPv2 kann recht einfach vom Angreifer simuliert werden
- Ist nur mit Cisco Phones möglich (CDPv2)

IOS

```
interface FastEthernet0/2
switchport mode access
switchport access vlan 10
switchport voice vlan 20
switchport voice detect cisco-phone
spanning-tree portfast
```

Weitere Nachteile :

- Auf dem Port kann nur noch ein Cisco Phone angeschlossen werden ! (mit daran angeschlossenem PC)
- Macht Probleme wenn Telefonnetzteile verwendet werden, und die Ethernetverbindung temporär getrennt wird

Lösung 3 (Flow-Chart) : Dynamisches Voice VLAN vergeben über CDPv2, aber ohne 802.1x, kein 802.1x zum PC, Authentisierung über CDPv2



Lösung 3.1 :

Dynamisches Voice VLAN vergeben über CDPv2 od. LLDP-MED, aber ohne 802.1x zum Telefon, 802.1x zum PC



Vorteil :

- Einfache Konfiguration
- Durch CDPv2 oder LLDP-MED wird das Voice-VLAN vergeben. Voice-VLAN wird aber auch ohne CDPv2 oder LLDP-MED aktiv
- Leichter in der Administration
- 802.1x für den PC
- Daten VLAN id kann vom Radius Server vergeben werden (802.1x Dyn VLAN)

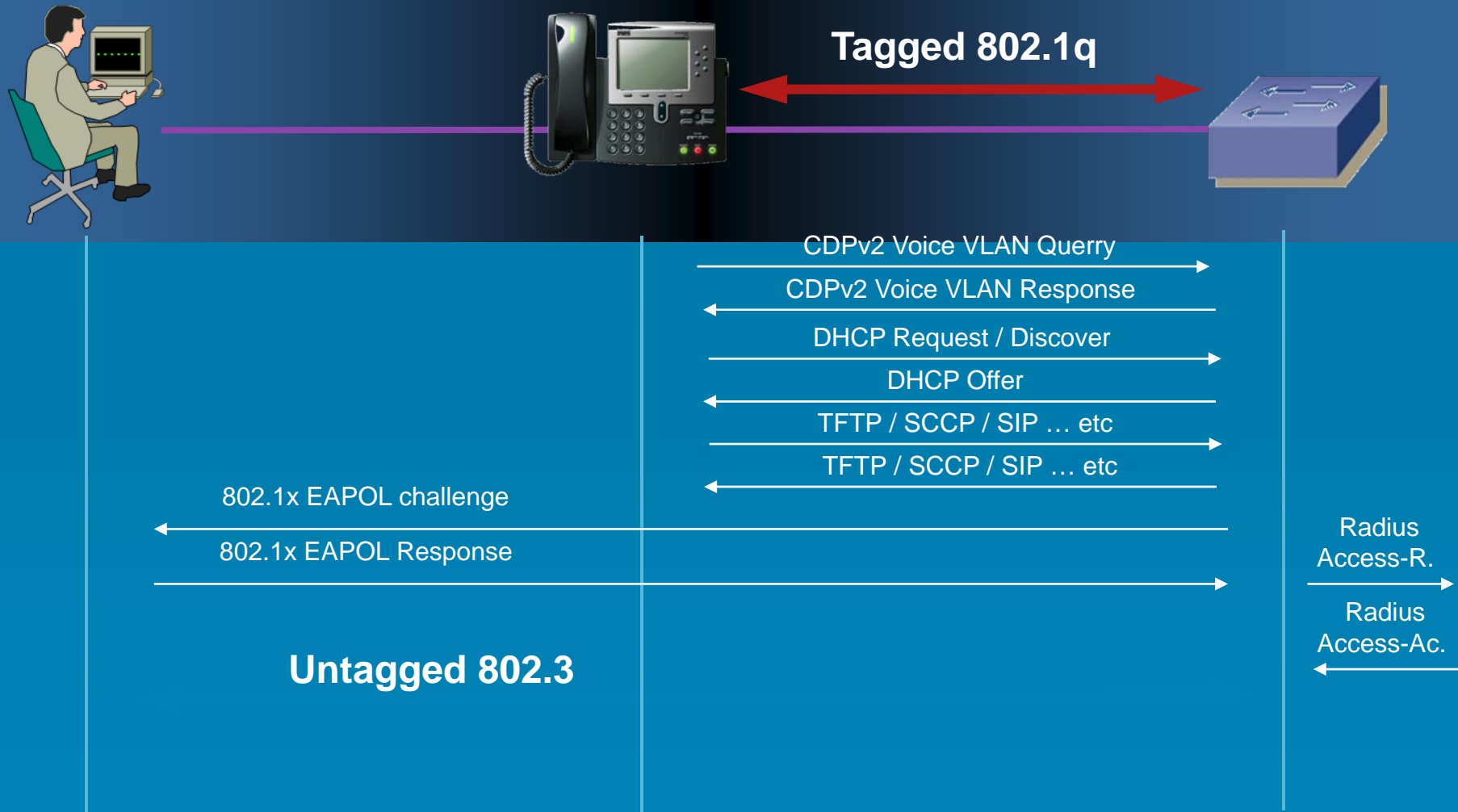
IOS

```
interface FastEthernet0/2
switchport mode access
switchport access vlan 10
switchport voice vlan 20
spanning-tree portfast
dot1x port-control auto
```

Nachteil :

- Keinerlei Schutz für das Voice-VLAN !
(Wie statischer Trunk Port)
- Die Kombination mit 802.1x Authentisierung für den PC, ohne 802.1x Phone Authentisierung ist nur möglich wenn CDPv2 verwendet wird ! Mit LLDP-MED ist dies nicht möglich

Lösung 3.1 (Flow-Chart) : Dynamisches Voice VLAN vergeben über CDPv2 od. LLDP-MED, aber ohne 802.1x zum Telefon, 802.1x zum PC



Lösung 3.1 (Flow-Chart) :

EAPOL Logoff : Sicheres Trennen des Daten-VLANs



Untagged 802.3

**Wenn PC Verbindung
zum Telefon getrennt wird :**

802.1x EAPOL Logoff (für das Daten-VLAN)

Untagged 802.3

Cisco Telefone senden einen EAPOL Logoff zum Switch, wenn der PC vom Port am Telefon getrennt wird. Dies ist ZWINGEND für eine sichere Implementation !!

Lösung 3.2 :

Dynamisches Voice VLAN vergeben über CDPv2 od. LLDP-MED, aber ohne 802.1x zum Telefon, 802.1x zum PC mit MAC Auth Bypass, usw.



Vorteil :

- Durch CDPv2 oder LLDP-MED wird das Voice-VLAN vergeben. Voice-VLAN wird aber auch ohne CDPv2 oder LLDP-MED aktiv
- 802.1x für den PC und MAB z.B. für Drucker oder Gäste
- Daten VLAN id kann vom Radius Server vergeben werden (802.1x Dyn VLAN)
- Weiterhin möglich Guest VLAN, Auth Fail VLAN

IOS

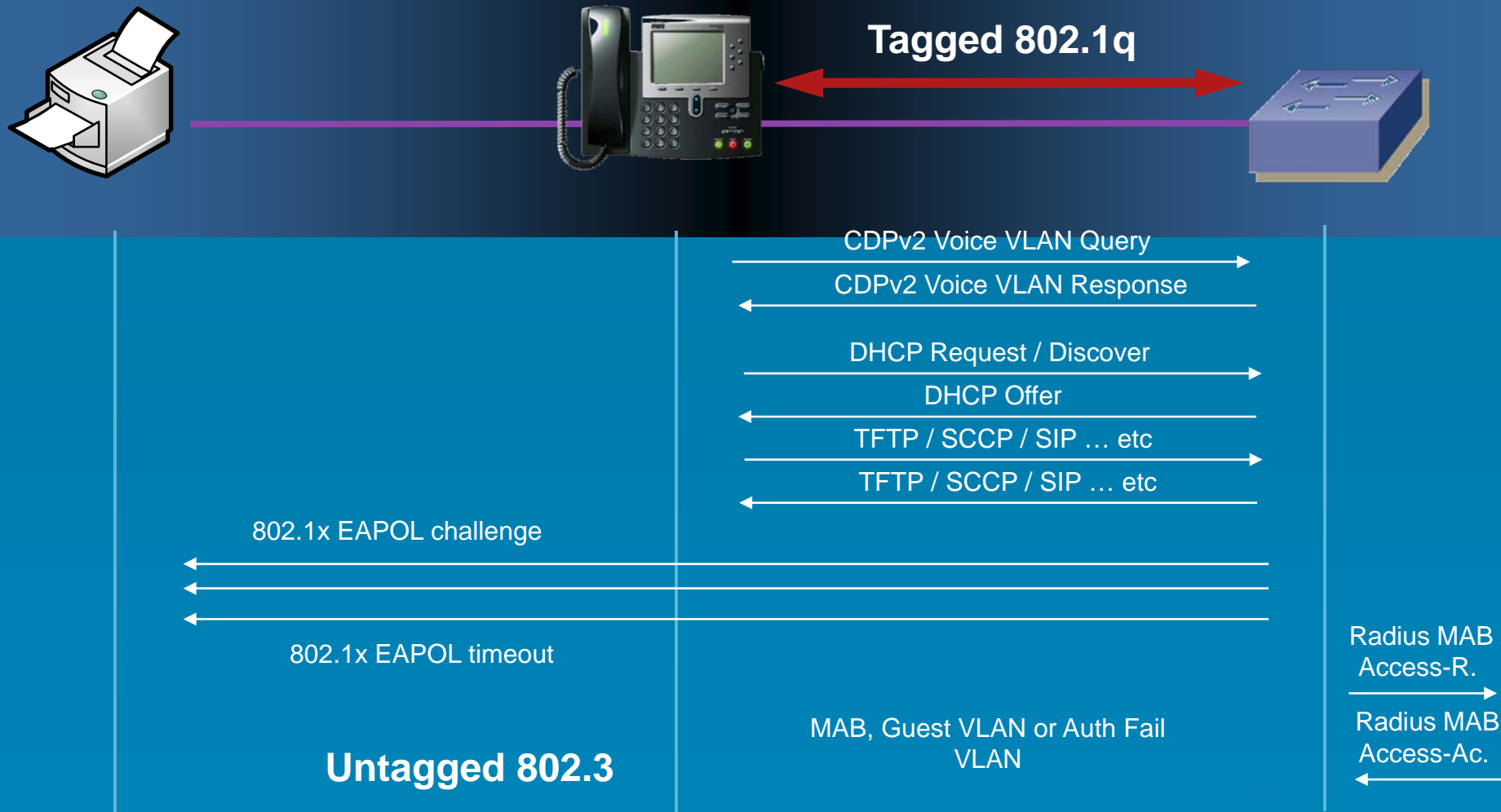
```
interface FastEthernet0/2
switchport access vlan 10
switchport mode access
switchport voice vlan 20
dot1x mac-auth-bypass
dot1x mac-auth-bypass timeout inactivity 300
dot1x pae authenticator
dot1x port-control auto
dot1x violation-mode protect
dot1x guest-vlan 25
dot1x auth-fail vlan 25
spanning-tree portfast
```

Nachteil :

- Keinerlei Schutz für das Voice-VLAN
- Wird MAB verwendet, bleibt der PC Port hinter dem Telefon Authentisiert bis der Timeout zuschlägt, auch wenn der PC abgesteckt wird !

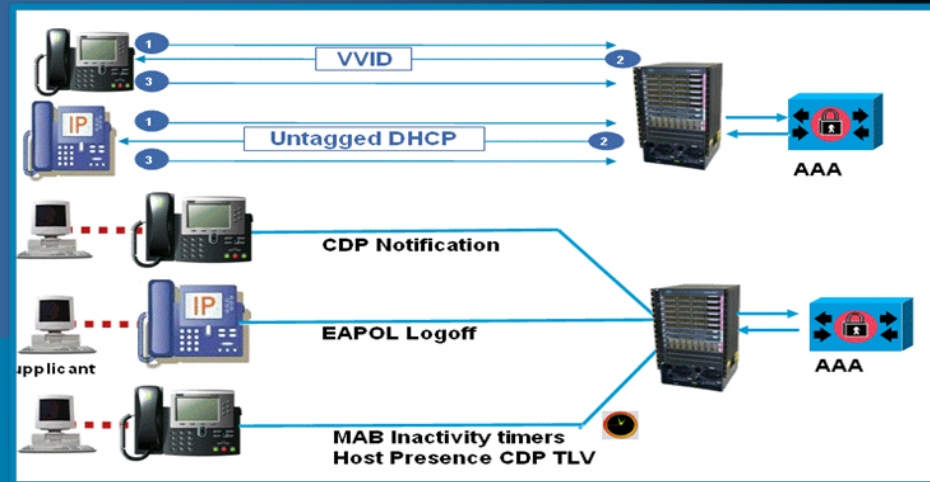
Lösung 3.2 (Flow-Chart) :

Dynamisches Voice VLAN vergeben über CDPv2 od. LLDP-MED, aber ohne 802.1x zum Telefon, 802.1x zum PC mit MAC Auth Bypass



Lösung 3.2 :

Dynamisches Voice VLAN vergeben über CDPv2 od. LLDP-MED, aber ohne 802.1x zum Telefon, 802.1x zum PC mit MAC Auth Bypass



Enhanced IPT Support

Solves “PC move” issue with MAB aging and new CDP “host presence” TLV

Problemlösung :

- Um das Problem mit den weiterhin authentisierten MAC Auth Bypass Teilnehmern zu lösen, wird ein neues TLV in CDPv2 eingebaut (Host-Present)
- Wird der PC abgesteckt, wird der Switch vom Telefon über CDP darüber informiert
- Erhältlich je nach Plattform zwischen Q3 2008 und Q1 2009

Nachteil :

- Derzeit nur mit CDP und Cisco Switch / Cisco Phone möglich
- Auf den kleinen Switches (29xx, 35xx, 37xx) erst ab Q1 2009 möglich

Lösung 4 (Multi Domain Authentication) : Dynamisches Voice VLAN vergeben über CDPv2 od. LLDP-MED, 802.1x zum Telefon, 802.1x zum PC



Vorteil :

- !! Voice-VLAN ist geschützt !!
- Durch CDPv2 oder LLDP-MED wird das Voice-VLAN vergeben. Voice-VLAN wird aber auch ohne CDPv2 oder LLDP-MED aktiv
- 802.1x für den PC und 802.1x für das Telefon
- Daten VLAN id kann vom Radius Server vergeben werden (802.1x Dyn VLAN)
- Weiterhin möglich Guest VLAN, Auth Fail VLAN, MAB, etc.
- Funktioniert auch mit nicht-Cisco Phones

IOS

```
interface FastEthernet0/2
switchport access vlan 10
switchport mode access
switchport voice vlan 20
dot1x pae authenticator
dot1x port-control auto
dot1x host-mode multi-domain
dot1x violation-mode protect
spanning-tree portfast
```

Nachteil :

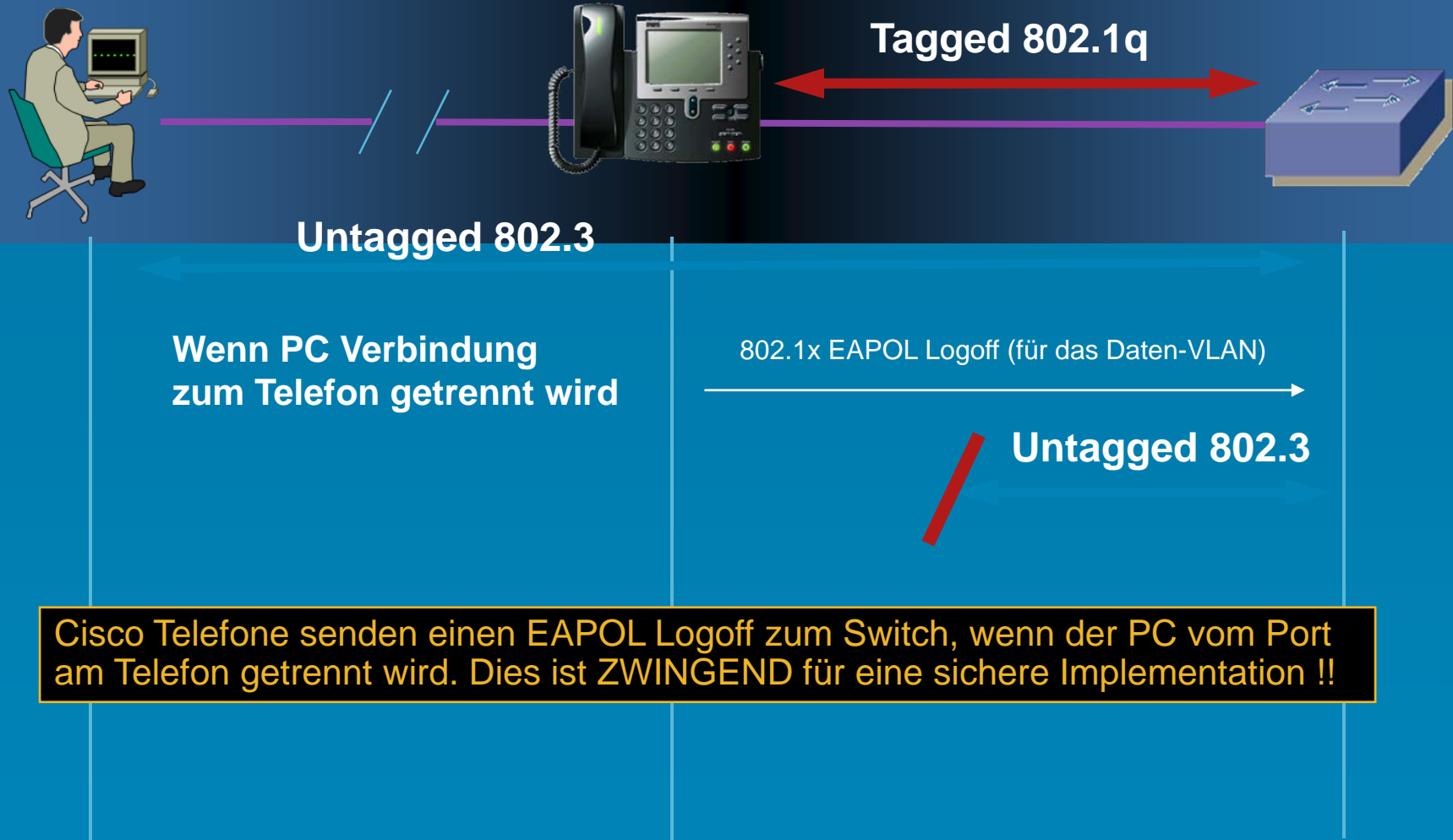
- Alle Telefone müssen als User im LDAP / Radius Datenbank eingepflegt werden (Bei EAP-MD5)
- Derzeit muss an jedem Phone ein Passwort (bei der Einrichtung) angegeben werden

Lösung 4 (Multi Domain Authentication) (Flow Chart): Dynamisches Voice VLAN vergeben über CDPv2 od. LLDP-MED, 802.1x zum Telefon, 802.1x zum PC



Lösung 4 (Flow-Chart) :

EAPOL Logoff : Sicheres Trennen des Daten-VLANs



Lösung 4 :

EAP-MD5 / EAP-TLS

EAP-MD5

- User-basierte Authentisierung
- Erfordert eine Eingabe von User / Passwort
- Derzeit auf allen Cisco Telefonen der aktuellen Generation unterstützt (next-gen, nicht auf 7905/12/40/60)

EAP-TLS

- Zertifikatsbasierte Authentisierung
- Erfordert keine Passwort Eingabe
- Eingebunden in der PKI
- EAP-TLS support wird im Mai 2009 auf Cisco Telefonen mit der neuen 8.5(2) Firmware zur Verfügung stehen (nicht auf 7905/12/40/60)

Lösung 5 (Multi Domain Authentication mit MAC Auth Bypass) : Dynamisches Voice VLAN vergeben über CDPv2 od. LLDP-MED, MAC Auth Bypass für das Telefon, 802.1x zum PC



Vorteil :

- Voice-VLAN ist zumindest durch die MAC Adresse geschützt
- Durch CDPv2 oder LLDP-MED wird das Voice-VLAN vergeben.
- 802.1x für den PC aber kein 802.1x für das Telefon
- Funktioniert auch mit nicht-Cisco Phones

Nachteil :

- MAC Adressen können leicht gefälscht werden

IOS

```
interface FastEthernet0/2
switchport access vlan 10
switchport mode access
switchport voice vlan 20
dot1x mac-auth-bypass
dot1x mac-auth-bypass timeout inactivity 300
dot1x pae authenticator
dot1x port-control auto
dot1x host-mode multi-domain
dot1x violation-mode protect
spanning-tree portfast
```

Weitere Nachteile :

- „Pseudo-Sicherheit“ für Installationen mit Telefonen ohne 802.1x Supplikanten
- Wird MAB verwendet, bleibt der PC Port hinter dem Telefon Authentisiert bis der Timeout zuschlägt, auch wenn der PC abgesteckt wird (bei LLDP-MED)!

Lösung 5 (Multi Domain Authentication mit MAC Auth Bypass) : Dynamisches Voice VLAN vergeben über CDPv2 od. LLDP-MED, MAC Auth Bypass für das Telefon, 802.1x zum PC



Wie muss sich ein IP Phone verhalten, wenn Cisco's Multi Domain Authentication (MDA) funktionieren soll ?

1. Das Telefon authentisiert sich im „untagged VLAN“, BEVOR es irgend etwas anderes schickt (d.h. kein DHCP, kein LLDP .. etc)
2. Nachdem die Authentisierung erfolgreich ist, handelt der Telefon mit dem Switch das Voice VLAN per LLDP-MED aus
3. Nachdem das Voice VLAN ausgehandelt ist, sendet das IP Phone einen DHCP Request im Voice VLAN um seine IP Adresse zu bekommen. Anschließend kommuniziert es ausschließlich im Voice VLAN (außer LLDP-MED) .
4. Wird ein PC am PC Port vom Telefon angeschlossen, sendet das Telefon die EAPOL Pakete von Switch und PC weiter
5. Wird der PC vom PC Port am Telefon abgesteckt, schickt das Telefon einen EAPOL Logoff zum Switch

(Siehe Folien 41/42)

Zeit für offene Fragen und zur weiteren Diskussion





Herzlichen Dank für Ihr Interesse und Ihre Zeit