# Corporate WLAN

## Implementierungsdokumentation

Verfasser: Reto Vogel
Email: reto.vogel@fhz.ch
Version: 1.4
Status: in Arbeit
Datum: 18.03.2005

## Änderungskontrolle

| Version | Datum | Ausführende Stelle | Bemerkung / Art der Änderung |
|---|---|---|---|
| 1.0 | 16.03.2005 | gat / vor | Erstellung des Dokumentes |
| 1.1 | 16.03.2005 | lan / stt | Überprüfung & Kontrolle |
| 1.2 | 17.03.2005 | gat | Weiterarbeit |
| 1.3 | 18.03.2005 | lan | Bearbeitung |
| 1.4 | 18.03.2005 | stt / vor | Ergänzungen |

## Prüfung

| Version | Datum | Ausführende Stelle | Bemerkung / Art der Änderung |
|---|---|---|---|
| 1.0 | | | |
| | | | |

# Inhaltsverzeichnis

1. Einführung ..... 4
2. Installation Server ..... 5
2.1. Domänencontroller ..... 5
2.1.1. Installation und Konfiguration ..... 5
2.1.2. Active Directory ..... 5
2.1.3. DNS ..... 5
2.1.4. DHCP ..... 6
2.1.5. Zertifizierungsstelle ..... 7
2.1.6. Computer zur Domain hinzufügen ..... 9
2.1.7. Benutzer zur Domain hinzufügen ..... 9
2.1.8. Gruppe zur Domain hinzufügen ..... 9
2.1.9. Sicherheitsrichtlinie für Domänen ..... 10
2.2. Internetauthentifizierungsdienst (IAS) ..... 11
2.2.1. Installation und Konfiguration ..... 11
2.2.2. IAS installieren ..... 11
2.2.3. Zertifikat erstellen ..... 12
2.2.4. RADIUS-Clients hinzufügen ..... 12
2.2.5. Erstellung einer RAS-Richtlinie ..... 13
3. Netzwerkkonfiguration ..... 14
3.1. Multi-Layer Switch ..... 14
3.1.1. Netzwerkkonfiguration ..... 14
3.1.2. VLAN erstellen ..... 14
3.1.3. VLAN konfigurieren ..... 14
3.1.4. Schnittstellen zuweisen ..... 15
3.1.5. Trunks erstellen ..... 15
3.1.6. Layer-3 Port Uplink ..... 16
3.1.7. VLANs ..... 16
3.1.8. Trunk ..... 16
3.1.9. Schnittstellen ..... 16
3.1.10. Running-Config ..... 16
3.2. Screening-Router ..... 19
3.3. Access Points ..... 19
3.3.1. SSID erstellen ..... 20
3.3.2. Einstellungen überprüfen ..... 20
3.3.3. Running-Config ..... 21
3.3.4. Power-over-Ethernet ..... 23
4. Quellen ..... 24

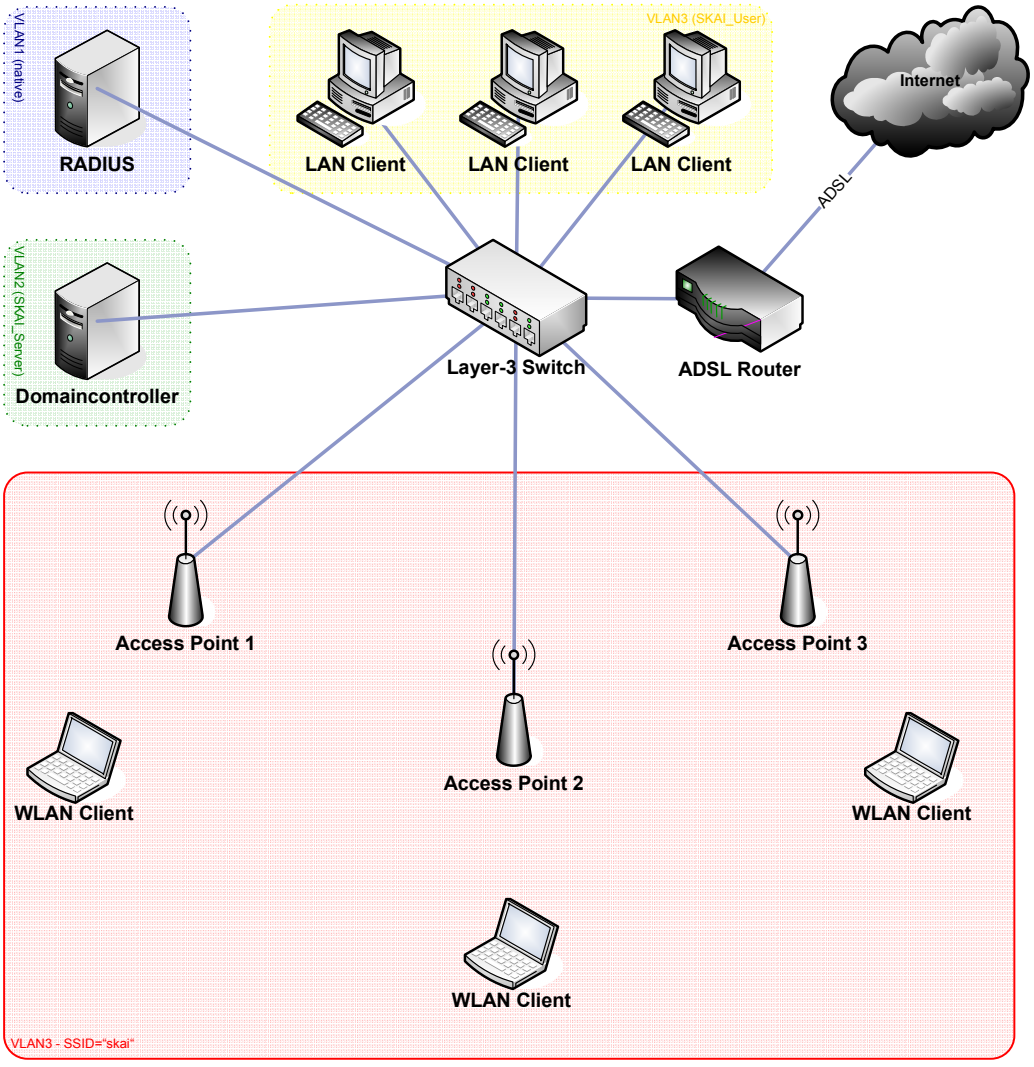
# 1. Einführung

Mit dieser Implementierungsdokumentation kann das gesamte WLAN-Projekt für die Firma Skai Logistik AG nachgebaut werden.

Alle dokumentierten Installationsabläufe sind auf einander abgestimmt und wurden so getestet. Die Abläufe sollten in der vorgegebenen Reihenfolge abgehandelt werden.
Die in dieser Dokumentation verwendeten technischen Angaben (DNS Namen, IP Bereiche, Domäne) gelten als 'best practices' und können je nach Situation oder bestehender Systeminfrastruktur angepasst werden.

Es wurden folgende Komponenten verwendet:

- **Domänencontroller (SKAISRV1)**
  Microsoft Windows Server 2003 Enterprise Edition mit DHCP, DNS und Zertifizierungsstelle (CA).
- **Internetauthentifizierungsdienst (SKAISRV2)**
  Microsoft Windows Server 2003 Enterprise Edition mit Remote Authentication Dial-in User Service (RADIUS).
- **Wireless Access Points**
  Cisco Aironet 1230b mit IOS 12.3(2)JA2.
- **Multi-Layer Switch**
  Cisco Catalyst 3550 mit IOS 12.1(22)EA1.
- **Wireless LAN Client**
  Microsoft Windows XP Professional mindestens mit Service Pack 1.

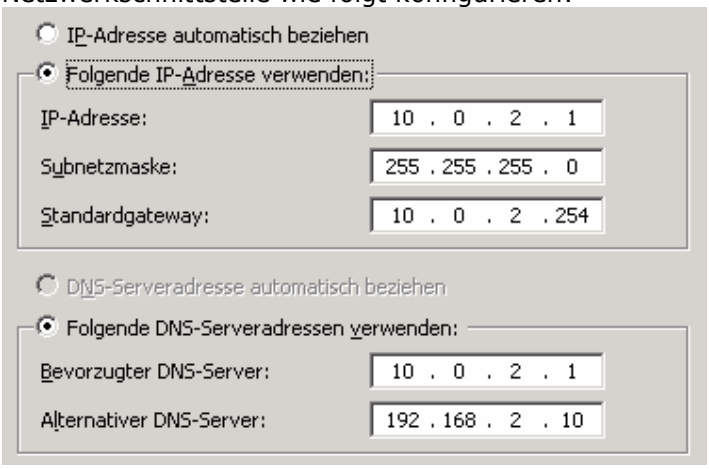


# 2. Installation Server

## 2.1. Domänencontroller

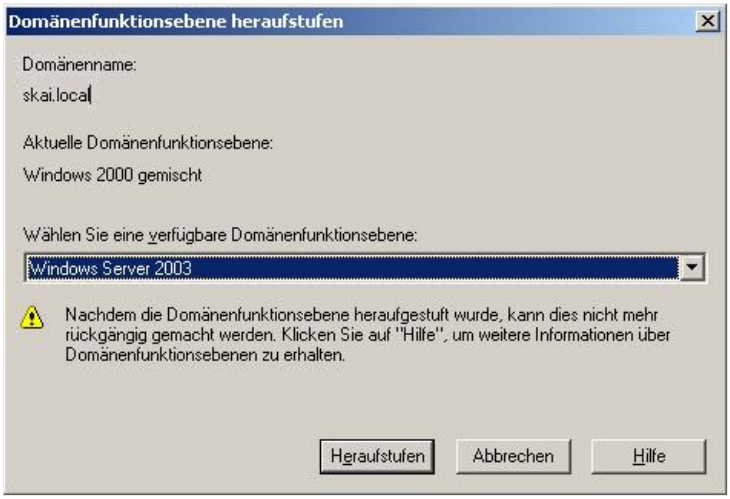
### 2.1.1. Installation und Konfiguration

- Microsoft Windows Server 2003 Enterprise Edition installieren.
- Netzwerkschnittstelle wie folgt konfigurieren:



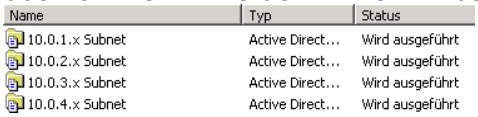

### 2.1.2. Active Directory

- Durch den Befehl 'dcpromo.exe' den Active Directory Wizard starten um ein Domänencontroller für eine neue Domäne namens 'skai.local' zu erstellen.
- Während der Installation des AD wird ein weiterer Assistent zur Installation des DNS gestartet.
- Nach erfolgter Installation des Domaincontroller und DNS über 'domain.msc' die 'Active Directory-Domänen und –Vertrauensstellungen' öffnen und die Domänenfunktionsebene auf 'Windows Server 2003' heraufstufen:

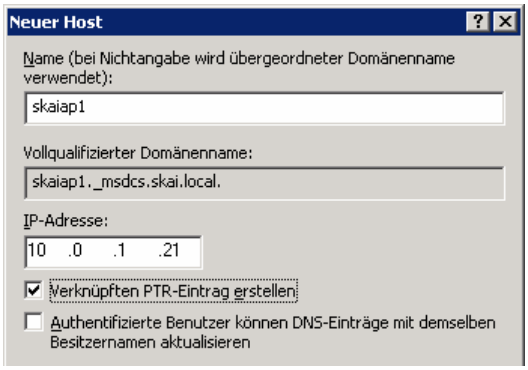


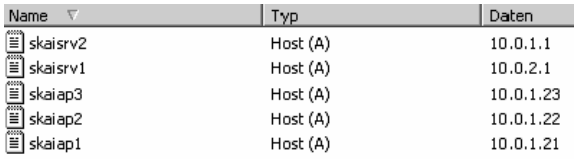

### 2.1.3. DNS

- Während der Installation des Active Directory wird der DNS-Dienst automatisch mitinstalliert. Nun muss dieser noch konfiguriert werden. Die Forward-Lookupzone wird ebenfalls automatisch erstellt.
- Es müssen dann für jedes VLAN eine Reverse-Lookupzone erstellt werden. Die Zonen werden als primäre Zonen hinzugefügt und die vorgegebene Option zur Replikation (Auf allen DNS-Servern in der Active Directory-Domäne „skai.local") kann übernommen werden. Es müssen folgende Subnetze erfasst werden:



- In der Forward-Lookupzone müssen dann die Access Points und die Server (AD & RADIUS) als neuer Host (A) erfasst werden. Die Checkbox 'Verknüpften PRT-Eintrag erstellen' aktivieren:



| Name | Typ | Daten |
|---|---|---|
| skaisrv2 | Host (A) | 10.0.1.1 |
| skaisrv1 | Host (A) | 10.0.2.1 |
| skaiap3 | Host (A) | 10.0.1.23 |
| skaiap2 | Host (A) | 10.0.1.22 |
| skaiap1 | Host (A) | 10.0.1.21 |

### 2.1.4. DHCP

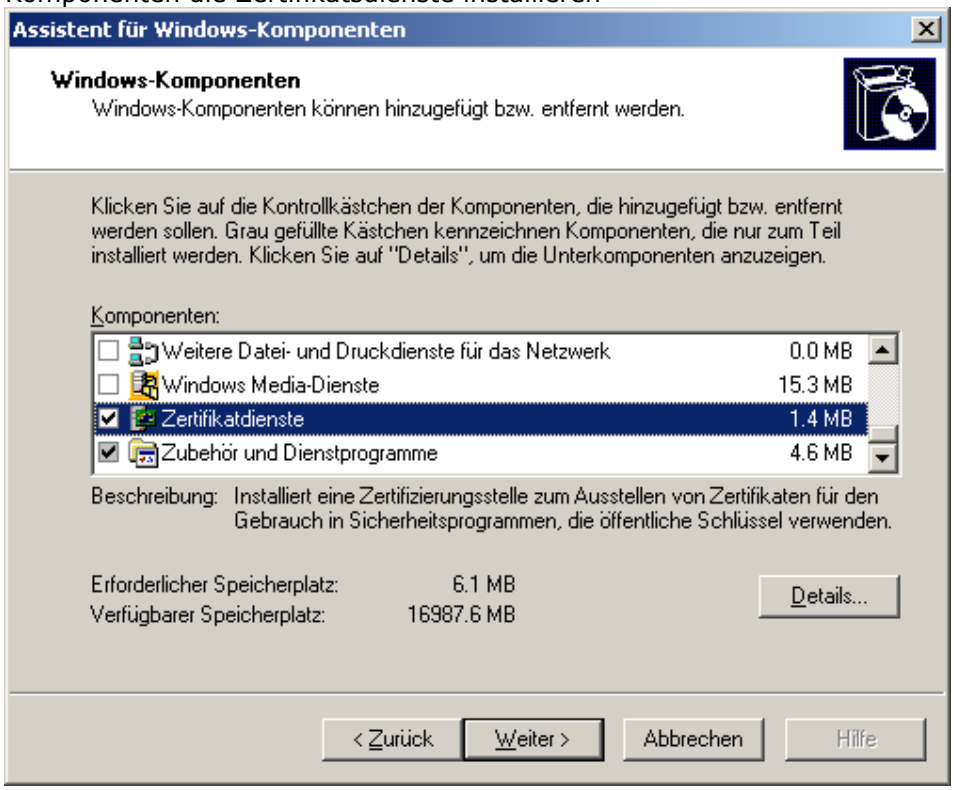
- Über den Server-Konfigurationsassistenten den DHCP Dienst installieren
- Nach der Installation muss der DHCP Dienst 'skaisrv1.skai.local' über das Snap-In autorisiert werden.
- Als nächstes werden folgende Bereiche konfiguriert:

| | | |
|---|---|---|
| **Bereich VLAN1** | | |
| Netzwerk: | 10.0.1.0 /24 | |
| Adresspool: | 10.0.1.1 – 10.0.1.253 | |
| Ausgeschlossene IPs: | 10.0.1.1 – 10.0.2.30 | |
| Bereichsoptionen: | 003 Router | 10.0.1.254 |
| | 006 DNS-Server | 10.0.2.1 |
| | 015 DNS-Domänenname | skai.local |
| Reservierungen: | Reservierungsname: | skaiap1.skai.local |
| | IP-Adresse: | 10.0.1.21 |
| | MAC-Adresse: | 00119228044d |
| | Beschreibung: | Wireless AP 1 |
| | Reservierungsname: | skaiap2.skai.local |
| | IP-Adresse: | 10.0.1.22 |
| | MAC-Adresse: | 000d65b75dd0 |
| | Beschreibung: | Wireless AP 2 |
| | Reservierungsname: | skaiap3.skai.local |
| | IP-Adresse: | 10.0.1.23 |
| | MAC-Adresse: | 000d65bfa955 |
| | Beschreibung: | Wireless AP 3 |
| **Bereich VLAN2** | | |
| Netzwerk: | 10.0.2.0 /24 | |
| Adresspool: | 10.0.2.1 – 10.0.2.253 | |
| Ausgeschlossene IPs: | 10.0.2.1 – 10.0.2.10 | |
| Bereichsoptionen: | 003 Router | 10.0.2.254 |
| | 006 DNS-Server | 10.0.2.1 |
| | 015 DNS-Domänenname | skai.local |

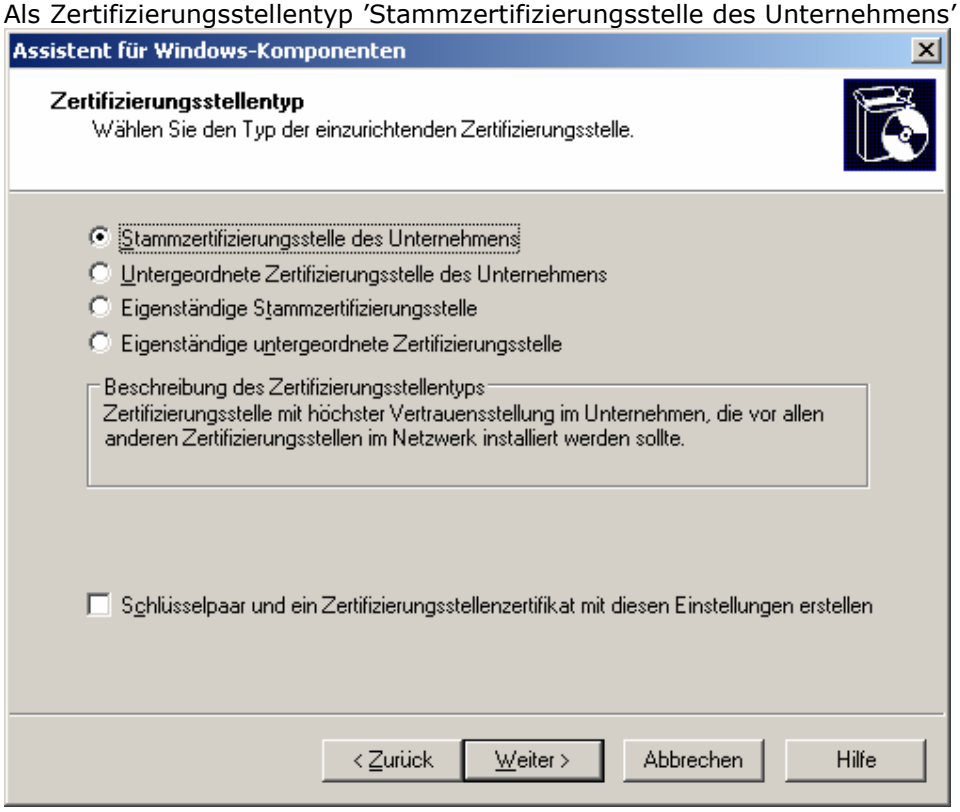
| | | |
|---|---|---|
| **Bereich VLAN3** | | |
| Netzwerk: | 10.0.3.0 /24 | |
| Adresspool: | 10.0.3.1 – 10.0.3.253 | |
| Ausgeschlossene IPs: | 10.0.3.1 – 10.0.3.10 | |
| Bereichsoptionen: | 003 Router | 10.0.3.254 |
| | 006 DNS-Server | 10.0.2.1 |
| | 015 DNS-Domänenname | skai.local |

### 2.1.5. Zertifizierungsstelle

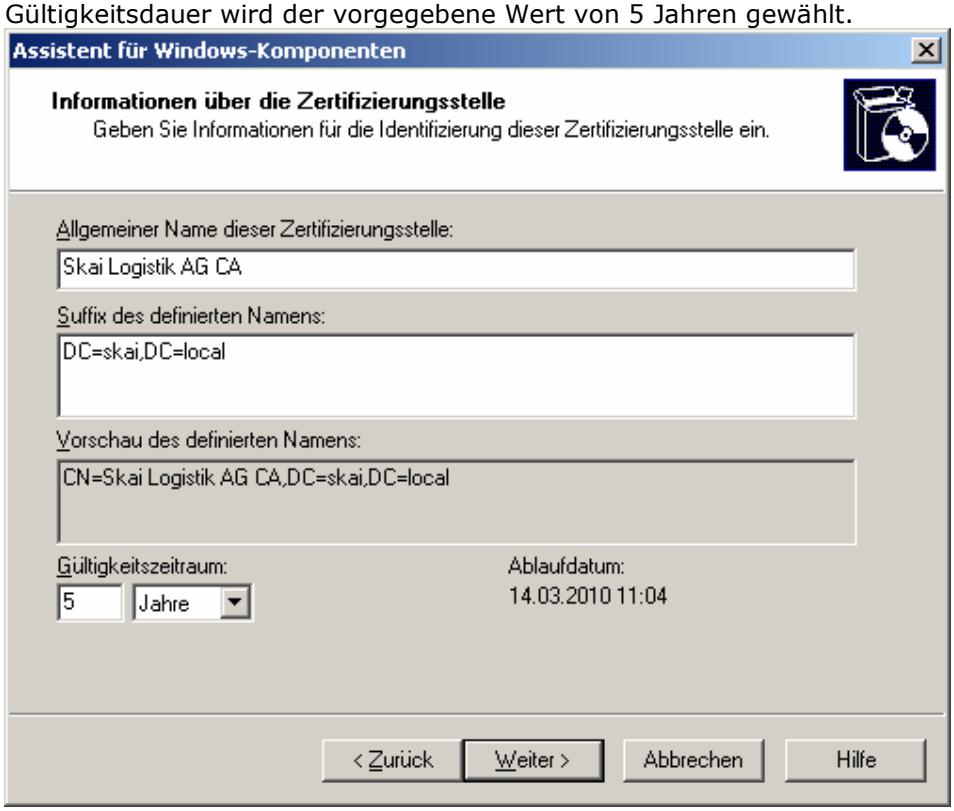
- In der Systemsteuerung unter Software über den Assistenten für Windows-Komponenten die Zertifikatsdienste installieren



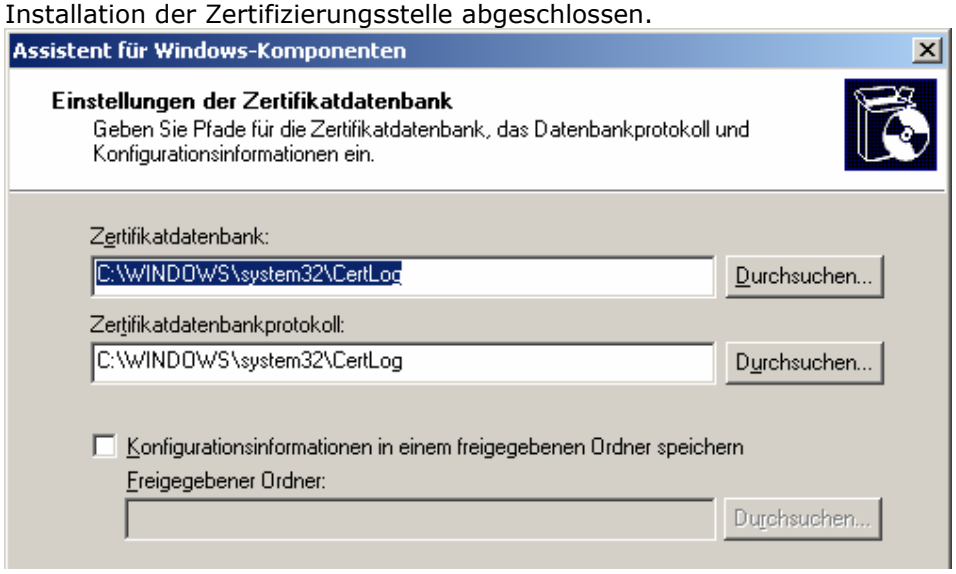
- Als Zertifizierungsstellentyp 'Stammzertifizierungsstelle des Unternehmens' wählen




- Als 'Allgemeiner Name dieser Zertifizierungsstelle' wird 'Skai Logistik AG CA' gewählt. Die anderen zwei Felder sind bereits vorgegeben oder passen sich dem Namen an. Als Gültigkeitsdauer wird der vorgegebene Wert von 5 Jahren gewählt.

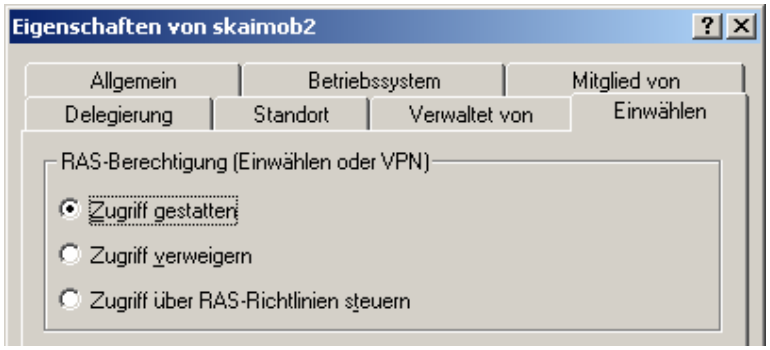


- Der Pfad der Zertifikatdatenbank wird wie gegeben übernommen. Danach ist die Installation der Zertifizierungsstelle abgeschlossen.



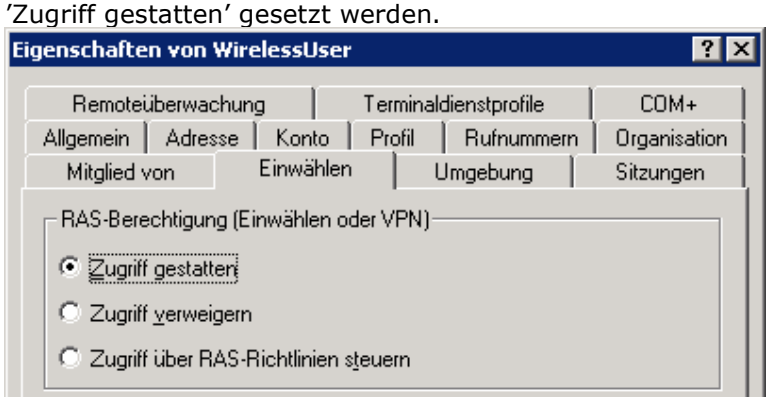

### 2.1.6. Computer zur Domain hinzufügen

- Bei jedem Computer der sich über das Wireless LAN autorisieren soll, muss in den Computereigenschaften die Einwahl für den RADIUS auf 'Zugriff gestatten' eingestellt werden.



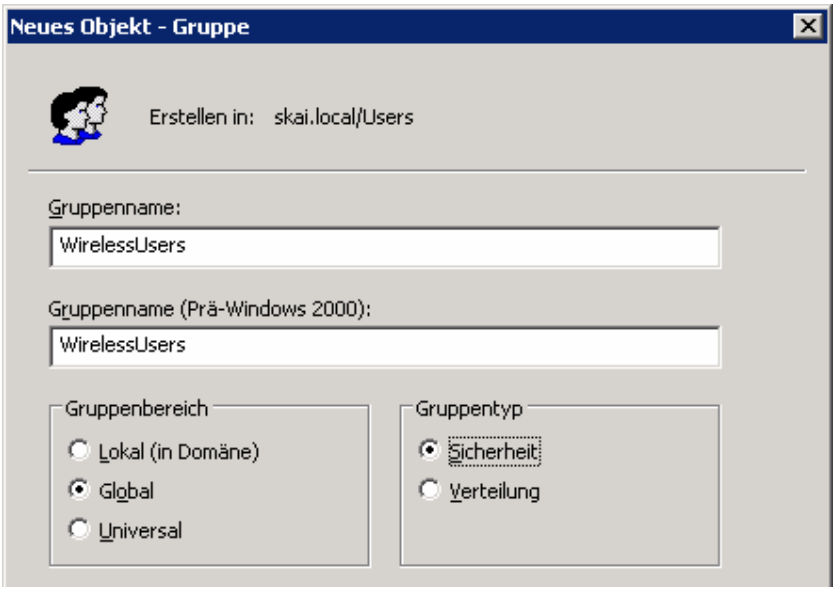

### 2.1.7. Benutzer zur Domain hinzufügen

- Wie bei den Computern muss auch den Domain-Benutzern die RAS-Berechtigung auf 'Zugriff gestatten' gesetzt werden.




### 2.1.8. Gruppe zur Domain hinzufügen

- Um den Verwaltungsaufwand auf dem RADIUS mit der Vergabe von Benutzerrechten gering zu halten, erstellt man eine Gruppe in der AD, der dann auf dem RADIUS die entsprechenden Berechtigungen erteilt werden. Diese Gruppe wird als globaler Gruppebereich und als Typ 'Sicherheit' erstellt:

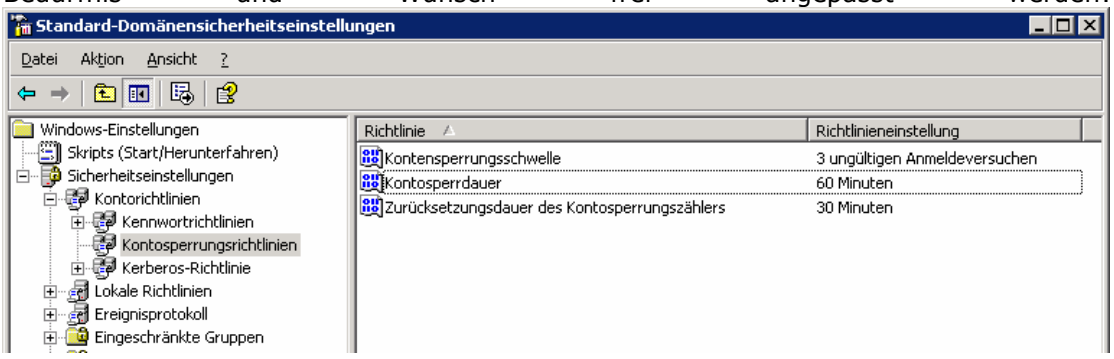



In diese Gruppe müssen alle Computer und User hinzugefügt werden die auf das WLAN Zugriff haben sollen. Sie werden dadurch authentifiziert.


### 2.1.9. Sicherheitsrichtlinie für Domänen

Wenn der Benutzer sein Password dreimal falsch eingibt wird sein Konto im Active Directory gesperrt. Dies muss dann vom Administrator wieder entsperrt werden.

- Im Snap-In 'Sicherheitsrichtlinie für Domänen', das in der Verwaltung zu finden ist, stellen wir die Kontosperrrichtlinien ein
- Als Kontosperrdauer haben wir 60 Minuten eingestellt, dies kann natürlich je nach Bedürfnis und Wunsch frei angepasst werden:



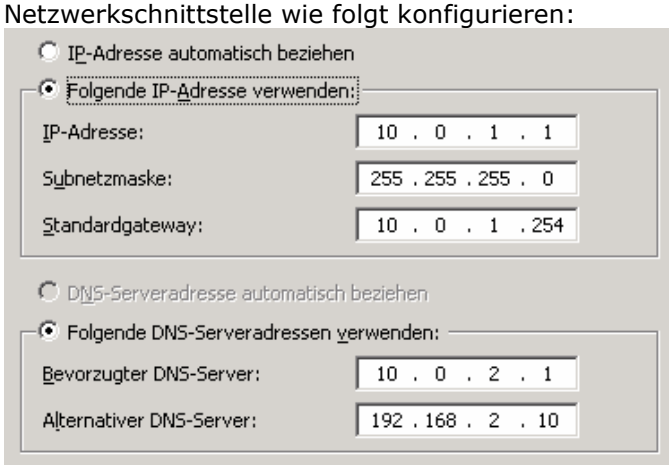

- Damit die Richtlinien übernommen werden, muss der Server neu gestartet werden oder es müssen die Policies mit dem Befehl `gpupdate /force /target:computer` aktualisiert werden.

## 2.2. Internetauthentifizierungsdienst (IAS)

Für den Internetauthentifizierungsdienst muss mindestens als Betriebssystem Microsoft Windows Server 2003 Standard Edition installiert sein. Auf dem IAS wird er RADIUS installiert der die Authentifizierung und Autorisierung für den Zugang ins Wireless LAN übernimmt.

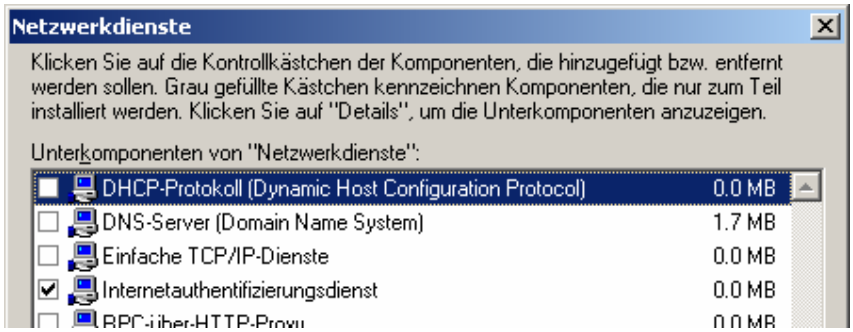
### 2.2.1. Installation und Konfiguration

- Microsoft Windows Server 2003 Enterprise Edition installieren.
- Netzwerkschnittstelle wie folgt konfigurieren:

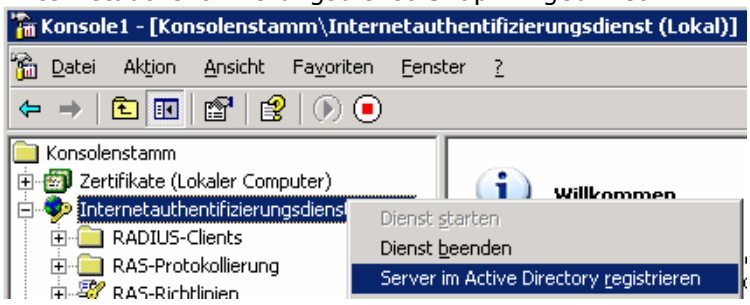


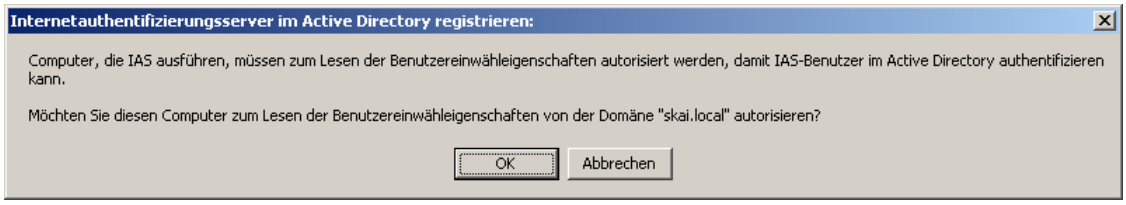

### 2.2.2. IAS installieren

- In der Systemsteuerung unter Software über den Assistenten für Windows-Komponenten unter 'Netzwerkdienste' den 'Internetauthentifizierungsdienst' installieren.




- Nach der Installation wird der IAS in der AD registriert. Dazu wird das 'Internetauthentifizierungsdienst-Snap-In' geöffnet:



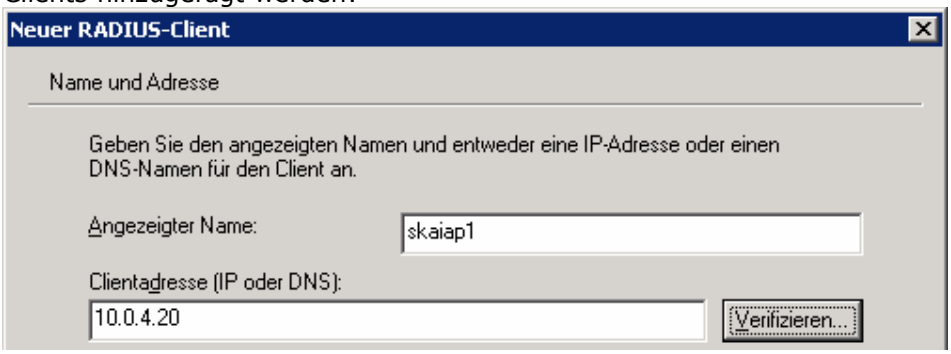
### 2.2.3. Zertifikat erstellen

- Im 'Zertifikate Snap-In' des lokalen Computers muss ein neues Zertifikat vom Domaincontroller angefordert werden:


Bei der Anforderung des Zertifikates muss ein Namen vergeben werden. Danach ist die Erstellung abgeschlossen

### 2.2.4. RADIUS-Clients hinzufügen

- Im 'Internetauthentifizierungsdienst Snap-In' müssen die Access Points als RADIUS-Clients hinzugefügt werden:

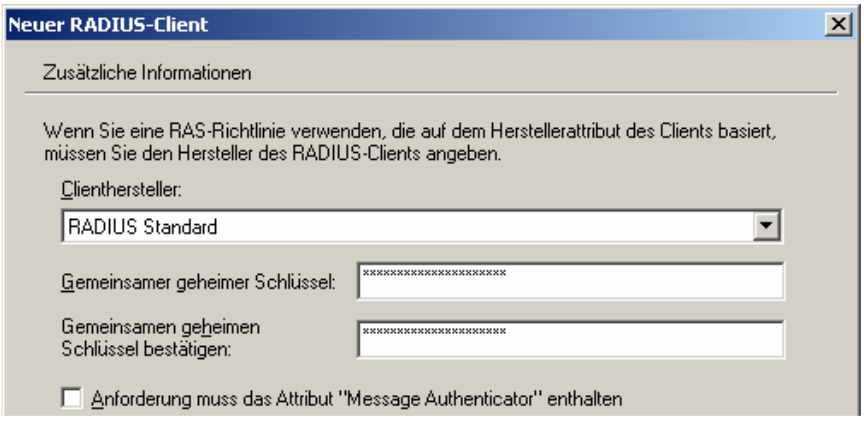



Dieser Vorgang muss für folgende 3 Access Points erledigt werden:

| Angezeigter Name | Clientadresse (IP) |
|---|---|
| skaiap1 | 10.0.4.20 |
| skaiap2 | 10.0.4.21 |
| skaiap3 | 10.0.4.22 |

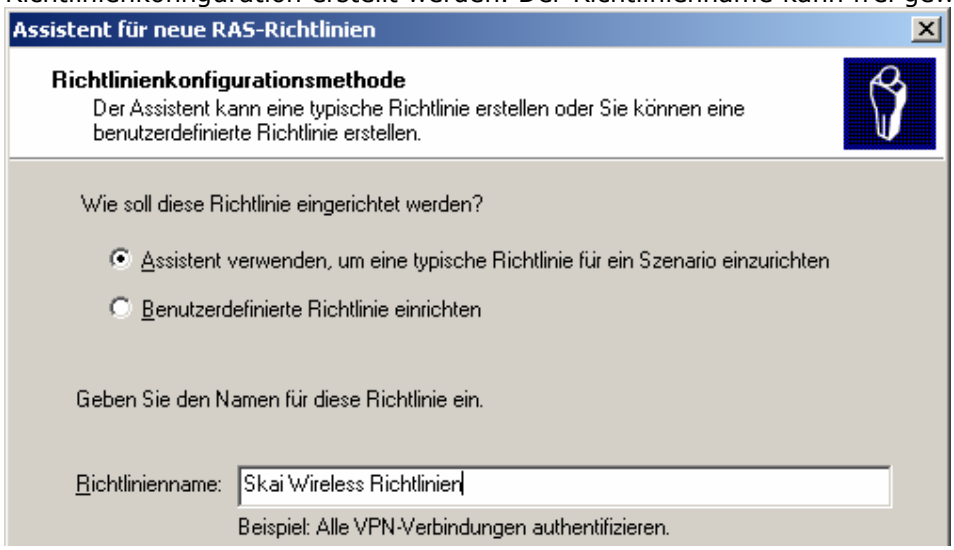
Als gemeinsamer geheimer Schlüssel (sog. 'Shared Secret') wird eine beliebig gewählte Zeichenkombination gewählt. Umso länger diese ist und umso mehr Sonderzeichen darin vorkommen, umso sicherer wird der Schlüssel. Wichtig ist, dass dieser Schlüssel im RADIUS-Eintrag des Access Points und auf dem Access Point genau gleich ist. Hier wurde folgende Zeichenkombination gewählt:

| Skai_%13Logistik-7#AG |
|---|

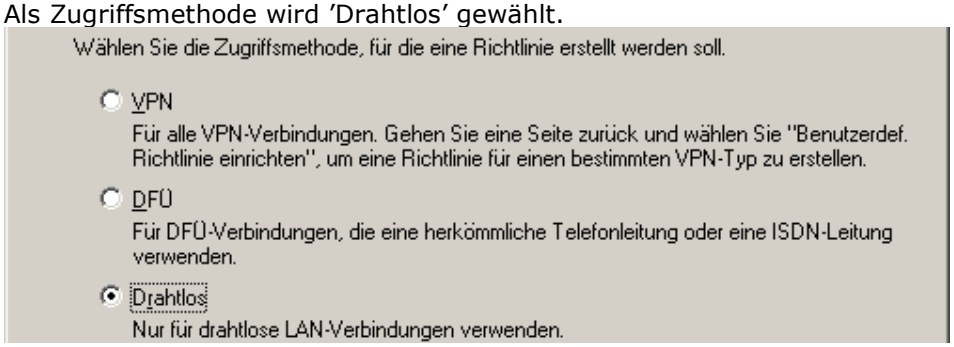


### 2.2.5. Erstellung einer RAS-Richtlinie

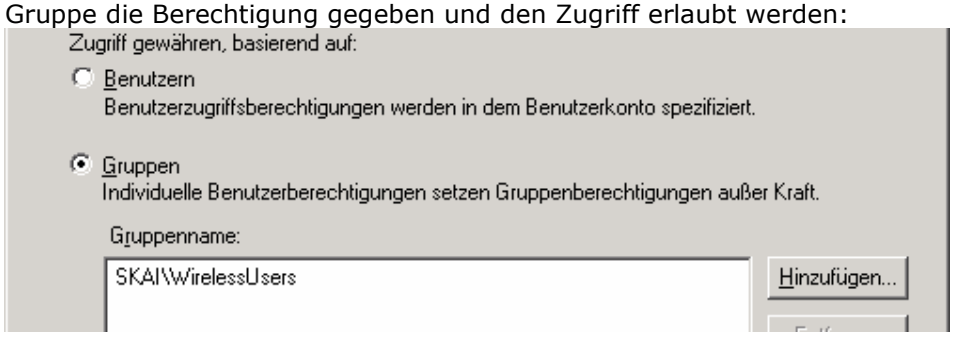
- Über den 'Assistent für neue RAS-Richtlinien' muss als nächstes eine neue Richtlinienkonfiguration erstellt werden. Der Richtlinienname kann frei gewählt werden.



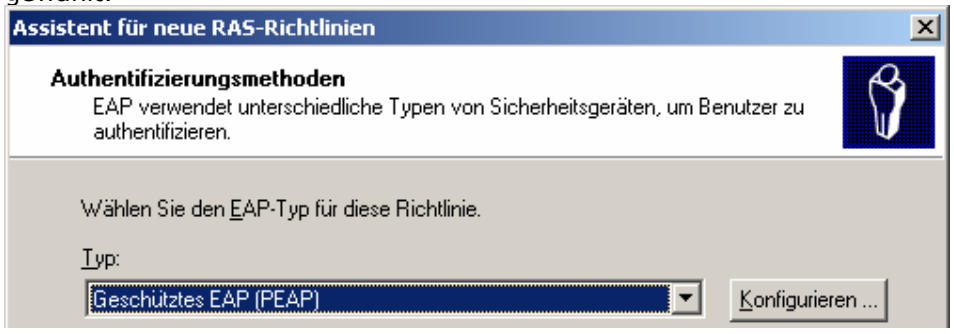

- Als Zugriffsmethode wird 'Drahtlos' gewählt.




- Nun muss der unter '2.1.7 Gruppe zur Domain hinzufügen' erstellten Active Directory Gruppe die Berechtigung gegeben und den Zugriff erlaubt werden:



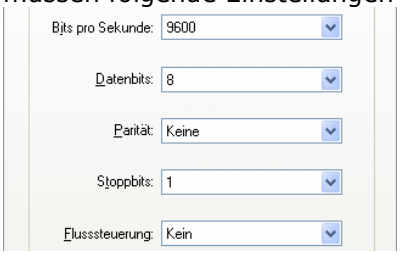

- Zum Schluss wird noch die Authentifizierungsmethode 'Geschütztes EAP (PEAP)' gewählt.



# 3. Netzwerkkonfiguration

## 3.1. Multi-Layer Switch

Zur Konfiguration des Multi-Layer Switches muss durch eine Terminalverbindung über den COM-Port zum Konsoleport des Switches hergestellt werden. Als Verbindungseinstellungen müssen folgende Einstellungen gewählt werden:



(Windows XP HyperTerminal)

### 3.1.1. Netzwerkkonfiguration

| Befehl | Beschreibung |
|---|---|
| `Swi001>enable` | |
| `Swi001#config terminal` | |
| `Swi001(config)#ip subnet-zero` | Unterstes Subnetz zulassen. |
| `Swi001(config)#ip classless` | Klassenloses Subnetting erlauben. |

### 3.1.2. VLAN erstellen

| Befehl | Beschreibung |
|---|---|
| `Swi001#config terminal` | |
| `Swi001#vlan database` | |
| `Swi001(vlan)#vlan 1` | VLAN 1 erstellen, falls nicht bereits vorhanden. |
| `Swi001(vlan)#vlan 2 name SKAI_Server` | VLAN 2 erstellen. |
| `Swi001(vlan)#vlan 3 name SKAI_User` | VLAN 3 erstellen. |
| `Swi001(vlan)#exit`<br>`APPLY completed.`<br>`Exiting....` | VLAN Konfiguration verlassen. |

### 3.1.3. VLAN konfigurieren

| Befehl | Beschreibung |
|---|---|
| `Swi001#configure terminal` | |
| `Swi001(config)#interface vlan 1` | VLAN 1 als Interface auswählen. |
| `Swi001(config-if)#ip address 10.0.1.254 255.255.255.0` | IP-Adressvergabe für das virtuelle Interface VLAN. Diese Adresse fungiert als Default-Gateway für das VLAN. |
| `Swi001(config-if)#no shutdown` | Interface aktivieren, falls deaktiviert. |
| `Swi001(config)#interface vlan 2` | VLAN 2 als Interface auswählen. |
| `Swi001(config-if)#ip address 10.0.2.254 255.255.255.0` | IP-Adressvergabe für das virtuelle Interface VLAN. Diese Adresse fungiert als Default-Gateway für das VLAN. |
| `Swi001(config-if)#no shutdown` | Interface aktivieren, falls deaktiviert. |
| `Swi001(config)#interface vlan 3` | VLAN 3 als Interface auswählen. |
| `Swi001(config-if)#ip address 10.0.3.254 255.255.255.0` | IP-Adressvergabe für das virtuelle Interface VLAN. Diese Adresse fungiert als Default Gateway für das VLAN. |
| `Swi001(config-if)#no shutdown` | Interface aktivieren, falls deaktiviert. |

Hinweis:
Alle Endgeräte, welche am Switch angeschlossen werden, müssen den Default-Gateway des entsprechenden VLAN-Interface eintragen.
Beispiel: Alle Geräte in VLAN 3 müssen die Gateway-Adresse von VLAN3 (10.0.3.254) als Default Gateway eintragen.

### 3.1.4. Schnittstellen zuweisen

| Befehl | Beschreibung |
|---|---|
| `Swi001#config terminal` | |
| `Swi001(config)#interface Gi0/2` | GigabitEthernet 0/2 auswählen. |
| `Swi001(config-if)#switchport access vlan 1` | Fügt das Gi0/2 dem VLAN1 hinzu. |
| `Swi001(config-if)# interface Gi0/3` | GigabitEthernet 0/3 auswählen. |
| `Swi001(config-if)#switchport access vlan 2` | Fügt das Gi0/3 dem VLAN2 hinzu. |
| `Swi001(config-if)# interface Gi0/4` | GigabitEthernet 0/4 auswählen. |
| `Swi001(config-if)#switchport access vlan 3` | Fügt das Gi0/4 dem VLAN3 hinzu. |
| `Swi001(config-if)# interface Gi0/5` | GigabitEthernet 0/5 auswählen. |
| `Swi001(config-if)#switchport access vlan 3` | Fügt das Gi0/5 dem VLAN3 hinzu. |
| `Swi001(config-if)# interface Gi0/6` | GigabitEthernet 0/6 auswählen. |
| `Swi001(config-if)#switchport access vlan 3` | Fügt das Gi0/6 dem VLAN3 hinzu. |
| `Swi001(config-if)# interface Gi0/7` | GigabitEthernet 0/7 auswählen. |
| `Swi001(config-if)#switchport access vlan 3` | Fügt das Gi0/7 dem VLAN3 hinzu. |

### 3.1.5. Trunks erstellen

| Befehl | Beschreibung |
|---|---|
| `Swi001#config terminal` | |
| `Swi001(config-if)# interface Gi0/8` | GigabitEthernet 0/8 auswählen. |
| `Swi001(config-if)#switchport trunk encapsulation dot1q` | Port Gi0/8 wird ein 802.1q Trunk. |
| `Swi001(config-if)#switchport trunk native vlan 1` | Native VLAN ist VLAN1. |
| `Swi001(config-if)#switchport mode trunk` | Trunking-Modus wird aktiviert. |
| `Swi001(config-if)#switchport nonegotiate` | |
| `Swi001(config-if)# interface Gi0/9` | GigabitEthernet 0/9 auswählen. |
| `Swi001(config-if)#switchport trunk encapsulation dot1q` | Port Gi0/9 wird ein 802.1q Trunk. |
| `Swi001(config-if)#switchport trunk native vlan 1` | Native VLAN ist VLAN1. |
| `Swi001(config-if)#switchport mode trunk` | Trunking-Modus wird aktiviert. |
| `Swi001(config-if)#switchport nonegotiate` | |
| `Swi001(config-if)# interface Gi0/10` | GigabitEthernet 0/10 auswählen. |
| `Swi001(config-if)#switchport trunk encapsulation dot1q` | Port Gi0/10 wird ein 802.1q Trunk. |
| `Swi001(config-if)#switchport trunk native vlan 1` | Native VLAN ist VLAN1. |
| `Swi001(config-if)#switchport mode trunk` | Trunking-Modus wird aktiviert. |
| `Swi001(config-if)#switchport nonegotiate` | |
| `Swi001(config-if)#end` | Verlässt den Config-Modus. |
| `Swi001#write memory` | Startup-Config mit Running-Config überschreiben. |

### 3.1.6. Layer-3 Port Uplink

Der Port Gi0/1 dient als Uplink zum ADSL-Router. Alle Pakete, welche nicht in interne Subnetze geroutet werden können, werden über das Interface GigabitEthernet 0/1 (192.168.2.201) zum ADSL-Router (192.168.2.1) gesendet.

| Befehl | Beschreibung |
|---|---|
| `Swi001(config)#interface Gi0/1` | Gi0/1 als Interface auswählen. |
| `Swi001(config-if)#no switchport` | Gi0/1 wird Layer-3 Port. |
| `Swi001(config-if)#ip address 192.168.2.201 255.255.255.0` | Die IP-Adresse muss im selben Subnetz sein wie der Default-Router (ADSL-Router). |
| `Swi001(config-if)#no shutdown` | Interface aktivieren, falls deaktiviert. |
| `Swi001(config-if)#exit` | Interface-Config verlassen. |
| `Swi001(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.1` | Konfiguriert die Default-Route für den Switch. |
| `Swi001#write memory` | Startup-Config mit Running-Config überschreiben. |

### 3.1.7. VLANs

Nach der obigen Konfiguration sollten die VLAN mit dem `show vlan` Befehl angezeigt werden.

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/2
2    SKAI_SERVER                      active    Gi0/3
3    SKAI_USER                        active    Gi0/4, Gi0/5, Gi0/6, Gi0/7
```

### 3.1.8. Trunk

Nach dem Einrichten der Trunks sollten auch diese über den Befehl `show interface g0/x trunk` angezeigt werden können. Als x gilt der Port der anzuzeigenden Konfiguration.

```
Port        Mode         Encapsulation  Status        Native vlan
Gi0/10      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gi0/10      1-4094

Port        Vlans allowed and active in management domain
Gi0/10      1-3

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/10      1-3
```

### 3.1.9. Schnittstellen

Am Router sind die Schnittstellen folgendermassen angeschlossen und konfiguriert:

| Port | VLAN | Ziel | IP | Maske | Gateway |
|---|---|---|---|---|---|
| Gi0/1 | Switchport | (ADSL Router) | 192.168.2.201 | 255.255.255.0 | 192.168.2.1 |
| Gi0/2 | 1 | SKAISRV2 | 10.0.1.1 | 255.255.255.0 | 10.0.1.254 |
| Gi0/3 | 2 | SKAISRV1 | 10.0.2.1 | 255.255.255.0 | 10.0.2.254 |
| Gi0/4 | 3 | (LAN-Client) | 10.0.3.x | 255.255.255.0 | 10.0.3.254 |
| Gi0/5 | 3 | (LAN-Client) | 10.0.3.x | 255.255.255.0 | 10.0.3.254 |
| Gi0/6 | 3 | (LAN-Client) | 10.0.3.x | 255.255.255.0 | 10.0.3.254 |
| Gi0/7 | 3 | (LAN-Client) | 10.0.3.x | 255.255.255.0 | 10.0.3.254 |
| Gi0/8 | Trunk | SKAIAP1 | 10.0.1.21 | 255.255.255.0 | 10.0.1.254 |
| Gi0/9 | Trunk | SKAIAP2 | 10.0.1.22 | 255.255.255.0 | 10.0.1.254 |
| Gi0/10 | Trunk | SKAIAP3 | 10.0.1.23 | 255.255.255.0 | 10.0.1.254 |

### 3.1.10. Running-Config

Die folgende Konfiguration stammt vom Router Cisco Catalyst 3550. Wenn die oben genannte Konfiguration beibehalten wurde, muss an der Running-Config nichts mehr geändert werden. Genauere Infos sind als Kommentar direkt in der Running-Config zu finden.

**Running-Config Router (Cisco Catalyst 3550)**

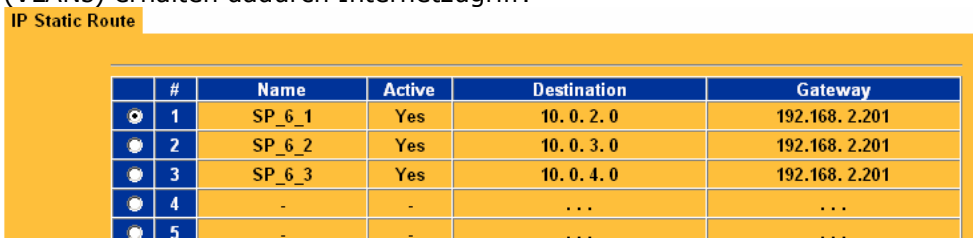
```
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname swi001
!
enable password Cisco
!
ip subnet-zero
ip routing
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
!
interface GigabitEthernet0/1
 no switchport
 ip address 192.168.2.201 255.255.255.0
!
interface GigabitEthernet0/2
 switchport mode dynamic desirable
!
interface GigabitEthernet0/3
 switchport access vlan 2
 switchport mode dynamic desirable
!
interface GigabitEthernet0/4
 switchport access vlan 3
 switchport mode dynamic desirable
!
interface GigabitEthernet0/5
 switchport access vlan 3
 switchport mode dynamic desirable
!
interface GigabitEthernet0/6
 switchport access vlan 3
 switchport mode dynamic desirable
!
interface GigabitEthernet0/7
 switchport access vlan 3
 switchport mode dynamic desirable
!
interface GigabitEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet0/9
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet0/10
 switchport trunk encapsulation dot1q
```

```
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet0/11
 switchport access vlan 5
 switchport mode dynamic desirable
!
interface GigabitEthernet0/12
 switchport access vlan 5
 switchport mode dynamic desirable
!
interface Vlan1
 ip address 10.0.1.254 255.255.255.0
 ip helper-address 10.0.2.1
 no ip route-cache
 no ip mroute-cache
!
interface Vlan2
 ip address 10.0.2.254 255.255.255.0
 ip helper-address 10.0.2.1
 no ip route-cache
 no ip mroute-cache
!
interface Vlan3
 ip address 10.0.3.254 255.255.255.0
 ip helper-address 10.0.2.1
 no ip route-cache
 no ip mroute-cache
!
interface Vlan4
 ip address 10.0.4.254 255.255.255.0
 ip helper-address 10.0.2.1
 no ip redirects
 no ip unreachables
 ip directed-broadcast
 no ip route-cache cef
 no ip mroute-cache
!
interface Vlan10
 ip address 10.0.10.254 255.255.255.0
 ip helper-address 10.0.2.1
 no ip route-cache
 no ip mroute-cache
 shutdown
!
router eigrp 88
 redistribute static
 passive-interface Vlan1
 passive-interface Vlan2
 passive-interface Vlan3
 passive-interface Vlan4
 network 10.0.0.0
 network 192.168.2.0
 no auto-summary
 no eigrp log-neighbor-changes
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.2.1
no ip http server
!
access-list 100 deny   ip 10.0.4.0 0.0.0.255 any
access-list 100 permit ip 10.0.4.0 0.0.0.255 192.168.2.0 0.0.0.255
```

```
route-map policy permit 0
 match ip address 100
 set interface GigabitEthernet0/1
!
!
line con 0
line vty 0 4
 login
line vty 5 15
 login
!
!
end
```

## 3.2. Screening-Router

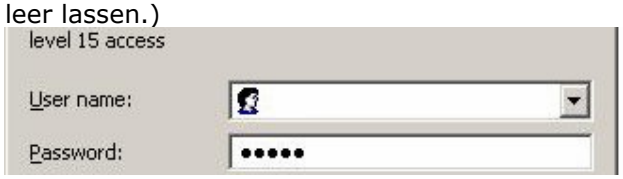
Die ADSL-Internetanbindung wird über einen Screening-Router (Zyxel ZyWALL 10W) realisiert. Da kein dynamisches Routing eingesetzt wird, werden die Routen für die Netzwerke der Skai-Domäne statisch auf dem ADSL Router eingetragen. Alle eingetragenen Netzwerke (VLANs) erhalten dadurch Internetzugriff:



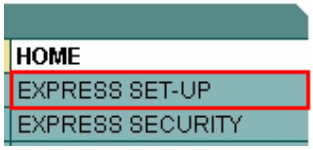

## 3.3. Access Points

Vorgehensweise bei der Konfiguration via Webinterface:

- Vor der Inbetriebnahme des Access Points muss abgeklärt werden, mit welchen Standardeinstellungen (z.B. IP-Adresse, Passwort,…) das Gerät vorkonfiguriert wurde. In unserem Fall (Cisco Aironet 1200 Serie) ist der Access Point als DHCP Client konfiguriert. Vorgängig muss also ein DHCP Dienst in Betrieb genommen werden (siehe 2.1.4 DHCP).
- Der Access Point wird an einen Trunk-Port des Multi-Layer Switches angeschlossen, da der er über mehrere VLAN kommunizieren muss.
- Kurze Zeit nach dem Start des Access Points kann via Webbrowser auf 'http://10.0.1.21' (oder DNS-Name 'http://skaiap1') zugegriffen werden. (In unserem Fall ist die IP-Adresse bekannt, da sie im DHCP Dienst auf die MAC-Adresse des Access Points reserviert wurde).
- Das Standard-Passwort auf diesem Cisco Access Point lautet 'Cisco'. (Username-Feld leer lassen.)




- Zum Menüpunkt 'EXPRESS SET-UP' navigieren.



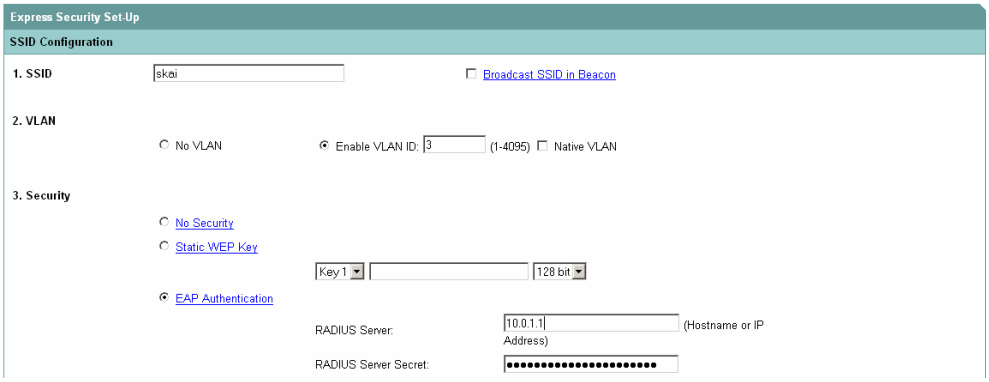

- Neuer System Name 'skaiap1' eingeben.
- Mit der Schaltfläche 'Apply' wird die Änderung übernommen.

Hinweis:
Es wird dringend empfohlen, das Standard-Passwort zu ändern!! Eine bereits vordefinierte SSID (hier: 'tsunami') wird sofort gelöscht, da für diese SSID keine Sicherheitsmechanismen aktiviert wurden.

### 3.3.1. SSID erstellen

- Zum Menüpunkt 'EXPRESS SECURITY' navigieren.
- Sicherheitseinstellungen vornehmen. Das 'Shared Secret' muss mit dem 'geheimen Schlüssel' auf dem IAS übereinstimmen:

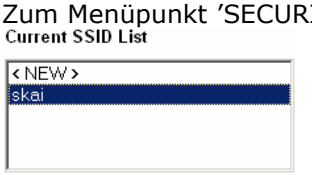
Skai_%13Logistik-7#AG



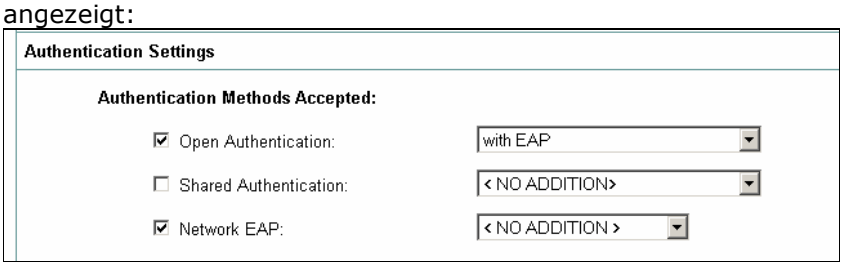

- 'Apply' klicken um die SSID zu speichern.

### 3.3.2. Einstellungen überprüfen

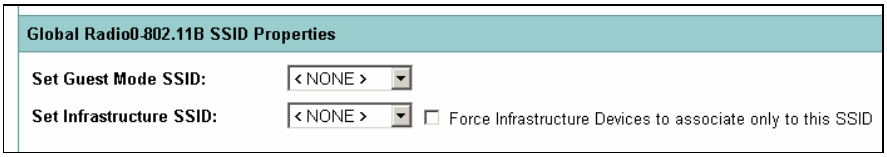
- Zum Menüpunkt 'SECURITY - SSID Manager' navigieren und SSID 'skai' wählen.




- In der Sektion 'Authentication Settings' werden die Einstellungen für die gewählte SSID angezeigt:



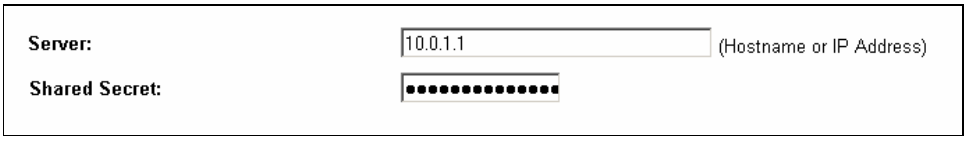

- In der untersten Sektion 'Global Radio Proporties' wird weder eine Gast-SSID noch eine Infrastruktur-SSID definiert.



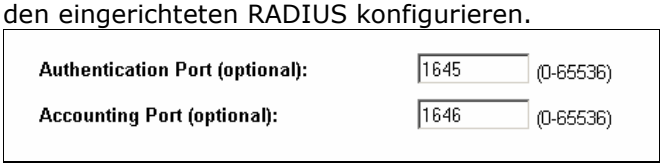

Hinweis:
Beim Einsatz eines Access Points im Repeater-Modus wird sämtlicher Netzwerkverkehr zwischen den Parent- und Repeater Access Points über die Infrastruktur-SSID geführt.

- Zum Menüpunkt 'SECURITY - Server Manager' navigieren.

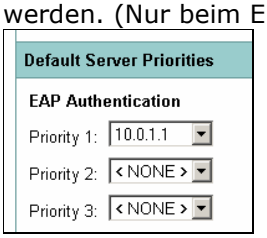
Aus der 'Current Server List' die IP-Adresse '10.0.1.1' wählen.



- Auf dem IAS sind standardmässig die Ports 1645 & 1812 für Authentifizierungs- und die Ports 1646 & 1813 für Accountingzwecke eingerichtet. Hier können die Ports für den eingerichteten RADIUS konfigurieren.




- Mit 'Apply' werden die Einstellungen gespeichert.
- In der Sektion 'Default Server Priorities' kann die RAIDUS-Server Priorität konfiguriert werden. (Nur beim Einsatz von mehreren RADIUS Servern nötig!)




### 3.3.3. Running-Config

Die folgende Konfiguration stammt vom 'skaiap1'. Da alle drei eingesetzten Access Points dieselbe Konfiguration nutzen, unterscheiden sich die Konfigurationen lediglich im Hostname des Gerätes.

- Damit nicht alle Access Points einzeln konfiguriert werden müssen, wird die Running-Config mit dem CLI-Befehl `copy running-config tftp://192.168.2.158/SKAIAP1.txt` auf einen TFTP Server kopiert.
- Der 'hostname' wird in der Konfigurationsdatei für die weiteren Access Points entsprechend angepasst.
- Die bearbeiteten (und umbenannten) Konfigurationsdateien werden nun mit dem CLI-Befehl `copy tftp startup-config` nun auf die anderen Access Points 'skaiap2' und 'skaiap3' kopiert.
- Nach einem Neustart der Access Points werden die Änderungen übernommen.

**Running-Config Skaiap1 (Cisco Aironet 1230b)**

```
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname skaiap1
!
enable secret 5 $1$WYUY$leqtpwMXZKMuCaFmTdAFi/
!
username Cisco password 7 0802455D0A16
ip subnet-zero
!
aaa new-model
!
!
aaa group server radius rad_eap
 server 10.0.1.1 auth-port 1645 acct-port 1646
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
```

```
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
aaa session-id common
!
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
  !
  encryption vlan 3 mode wep mandatory
  !
  ssid skai
     vlan 3
     authentication open eap eap_methods
     authentication network-eap eap_methods
  !
 speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
 station-role root
 no cdp enable
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio0.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
 bridge-group 3 subscriber-loop-control
 bridge-group 3 block-unknown-source
 no bridge-group 3 source-learning
 no bridge-group 3 unicast-flooding
 bridge-group 3 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface FastEthernet0.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
 no bridge-group 3 source-learning
 bridge-group 3 spanning-disabled
```

```
!
interface BVI1
 ip address dhcp client-id FastEthernet0
 no ip route-cache
!
ip http server
no ip http secure-server
ip                                  http                                help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
logging snmp-trap emergencies
logging snmp-trap alerts
logging snmp-trap critical
logging snmp-trap errors
logging snmp-trap warnings
radius-server attribute 32 include-in-access-req format %h
radius-server   host   10.0.1.1   auth-port   1645   acct-port   1646   key   7
02350F5A02394A701F62061E0C04060207497D68050F
radius-server vsa send accounting
bridge 1 route ip
!
!
!
line con 0
 transport preferred all
 transport output all
line vty 0 4
 transport preferred all
 transport input all
 transport output all
line vty 5 15
 transport preferred all
 transport input all
 transport output all
!
end
```

### 3.3.4. Power-over-Ethernet

Es ist möglich die Stromzufuhr für den Access Point über das Ethernetkabel zu führen. Power-over-Ethernet (PoE) ist die Technologie, mit der netzwerkfähige Geräte über das 8-adrige Ethernet-Kabel mit Strom versorgt werden können. Mit einem Adapter kann Strom und Netzwerkanschluss zusammengeführt werden.

Strom und Ethernet gebündelt gehen danach zusammen über ein Kabel zum. Dieses kann am Access Point angebracht werden. Dieser läuft dann ohne Problem mit dieser Option.

# 4. Quellen


- http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_configuration_example09186a00801d0815.shtml
- http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_technical_reference09186a00801444a1.html
- http://www.cisco.com/en/US/products/hw/switches/ps646/
- http://www.cisco.com/en/US/tech/tk389/tk815/technologies_configuration_example09186a008019e74e.shtml
- http://www.cisco.com/en/US/tech/tk389/tk815/technologies_configuration_example09186a008015f17a.shtml
- http://www.cisco.com/warp/public/793/lan_switching/3.html
- http://www.microsoft.com/downloads/details.aspx?FamilyID=0f7fa9a2-e113-415b-b2a9-b6a3d64c48f5&DisplayLang=en