HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

Individuelle **P**raktische **A**rbeit

802.1x

6. März – 22. März 2013

IPA-Kandidat:	Marco Koch
Fachverantwortlicher:	Roger Baumer
Hauptexperte:	Giuseppe Auriemma
Zweitexperte:	Roger Aepli

1 DOKUMENTINFORMATIONEN 7

1.1 VERSIONSÜBERSICHT 7

1.2 DARSTELLUNGEN UND ABKÜRZUNGEN 7

2 VORWORT 7

3 UMFELD UND ABLAUF 8

3.1 AUSGANGSLAGE 8

3.2 AUFGABENSTELLUNG 8

3.2.1 Konzept 8

3.2.2 Installation in der Testumgebung 9

3.2.3 Dokumentation 10

3.2.4 Tests 10

3.2.5 Systemgrenzen 10

4 PROJEKTORGANISATION 11

4.1 METHODE 11

4.1.1 IPERKA 11

4.2 VORSTELLUNG PERSONEN 12

4.3 DEKLARATION VORKENNTNISSE 12

4.4 DEKLARATION DER VORARBEITEN 12

5 ZEITPLAN 13

6 ARBEITSPROTOKOLL / JOURNAL 15

6.1 IPA-TAG 1 06.03.13 15

6.2 IPA-TAG 2 07.03.13 15

6.3 IPA-TAG 3 08.03.13 16

6.4 IPA-TAG 4 11.03.13 16

6.5 IPA-TAG 5 13.03.13 17

6.6 IPA-TAG 6 14.03.13 17

6.7 IPA-TAG 7 15.03.13 18

6.8 IPA-TAG 8 15.03.13 18

6.9 IPA-TAG 9 20.03.13 19

6.10 IPA-TAG 10 21.03.13 19

6.11 IPA-TAG 11 22.03.13 20

7 INFORMIEREN 21

7.1 IST-ZUSTAND 22

7.2 SOLL-ZUSTAND 22

7.3 CISCO-KOMPONENTEN 22

7.3.1 Access Switches 22

7.3.2 IP-Phones 23

7.4 RADIUS 23

7.5 CLIENT-BETRIEBSSYSTEME 23

7.5.1 Windows 7 23

7.5.2 Windows 8 23

7.5.3 Mac OS X 24

7.5.4 Linux Fedora 13 24

8 PLANEN 25

8.1 ALLGEMEINER AUFBAU 25

8.2 AUTHENTIFIKATIONS-METHODE 25

8.3 CLIENT- UND/ODER USER-AUTHENTIFIKATION 26

8.3.1 User-Authentifikation und VLAN-Zuweisung 26

8.3.2 Client-Authentifikation und VLAN-Zuweisung 26

8.3.3 User- und Client-Authentifikation und VLAN-Zuweisung 27

8.3.4 Auswirkungen auf den Betrieb 27

8.4 MÖGLICHE EINSATZGEBIETE 27

8.4.1 Sitzungszimmer 27

8.4.2 Übungsräume für Studierende 28

8.4.3 Dozenten- und Assistenzbüros 29

8.4.4 Büro IT-Client-Management 29

8.4.5 Problematik PXE Boot Installation 30

8.4.6 Fazit 30

8.5 TESTS 30

8.5.1 Windows-7-authentifizierte Clients 30

8.5.2 Windows-7-nicht-authentifizierte Clients 30

8.5.3 Switches 31

8.5.4 Radius 31

8.5.5 Benutzeranleitung ... 31

9 ENTSCHEIDEN ... 32

9.1 AUTHENTIFIKATIONS-METHODE ... 32

9.2 CLIENT- UND/ODER USER-AUTHENTIFIKATION ... 32

9.3 MÖGLICHE EINSATZGEBIETE ... 32

10 REALISIEREN ... 33

10.1 SYSTEMBESCHREIBUNG ... 33

10.2 KONFIGURATION FIREWALL ... 33

10.3 VORBEREITUNG CLIENTS ... 34

10.4 INSTALLATION RADIUS-SERVER ... 34

10.4.1 Installation svtest050 ... 34

10.4.2 Installation svtest051 ... 35

10.5 KONFIGURATION RADIUS-SERVER ... 36

10.5.1 Zertifikate ... 36

10.5.2 Radius-Clients ... 37

10.5.3 Network Policy ... 38

10.5.4 Switch Management Policy ... 40

10.6 KONFIGURATION SWITCHES ... 41

10.6.1 2908g-ipamkoch ... 42

10.6.2 2948s-ipamkoch ... 43

10.6.3 3524p-ipamkoch ... 44

10.7 ERSTELLEN DER GROUP POLICY ... 45

10.8 BENUTZERANLEITUNG ... 46

11 KONTROLLIEREN ... 58

11.1 TESTPROTOKOLL ... 58

11.1.1 Windows-7-authentifizierte Clients ... 58

11.1.2 Windows-7-nicht-authentifizierte Clients ... 62

11.1.3 Switches ... 63

11.1.4 Radius ... 64

11.1.5 Benutzeranleitung ... 66

12 AUSWERTUNG ... 66

12.1 TECHNISCHES FAZIT 66
12.2 ÜBERGANG ZUM BETRIEB 66
12.3 PERSÖNLICHES FAZIT 67
13 GLOSSAR 67
14 ABBILDUNGSVERZEICHNIS 68
15 TABELLENVERZEICHNIS 68
16 QUELLENVERZEICHNIS 69
17 ANHANG 70
17.1 KOMPLETTE KONFIG 2908G-IPAMKOCH 70
17.2 KOMPLETTE KONFIG 2948S-IPAMKOCH 72
17.3 KOMPLETTE KONFIG 3524S-IPAMKOCH 75

1 Dokumentinformationen

1.1 Versionsübersicht

Tabelle 1: Versionsübersicht

Datum	Änderung	Version	Wer
21.02.2013	Dokumentvorlage erstellt	0.1	Marco Koch
06.03.2013	Dokumentation begonnen	0.2	Marco Koch
20.03.2013	Korrekturlesen	1.0	Marco Koch

1.2 Darstellungen und Abkürzungen

Im zweiten Teil werden Servernamen, Dateipfade und Befehle fett oder kursiv dargestellt.
Für grössere Stellen Code oder Befehle wird `dieses Schriftbild` verwendet. Begriffe, die im Glossar erklärt werden, werden mit diesem Schriftbild dargestellt.

2 Vorwort

Dieses Dokument wurde während meiner IPA (zwischen dem 6.3. und dem 22.3.2013) erstellt. Es umfasst die Aufgabenstellung, die Planung und die Realisierung des Projektes.

Dank gebührt den Leuten, die die Umsetzung dieses Projektes möglich gemacht haben.

Roger Baumer	Aufgabenstellung/moralische Unterstützung
Parick Oberli	Firewall-Konfiguration
Anton Koolen	Typo3-Account
Veronika Koch	Korrekturlesen

Erster Teil

3 Umfeld und Ablauf

3.1 Ausgangslage

An der HSR werden alle Clients manuell in das entsprechende VLAN erfasst.
Aktuelle Clientbetriebssysteme sind Windows XP und Windows7 (Personal), Windows XP, Windows7 und Windows8, Mac OSX und Linux (Studenten).
Betriebssystem der Radius Server ist Windows Server 2008. Accessswitch Typen Cisco 2960G, 2960S und 3560P.

3.2 Aufgabenstellung

3.2.1 Konzept

Bei der Einführung von 802.1x müssen verschiedene Bereiche daraufhin analysiert werden, ob der Einsatz von 802.1x sinnvoll ist oder nicht. Entscheidend dabei sind die Bedürfnisse der jeweiligen Benutzergruppen und die Frage, ob 802.1x mit den vor Ort vorhandenen Einrichtungen realisiert werden kann. Pro Bereich müssen pro/contra 802.1x-Argumente gesammelt und eine Empfehlung abgegeben werden.

Bereiche, die analysiert werden sollen:

- Sitzungszimmer (Beispiel1.223)
- Übungsräume für Studierende (Beispiel 1.202)
- Dozenten- und Assistentenbüros (Beispiel 6.108)
- Büro IT-ClientMgmt (Beispiel 1.015)

Welche an der HSR verbreiteten Client-Betriebssysteme (Microsoft Windows7/Windows8, Mac OS X 10.x, Linux Fedora 13) unterstützen 802.1x in der Art, wie es laut Konzept/Testinstallation an der HSR eingeführt werden soll? Gibt es bestimmte Einschränkungen? Ist 802.1x bereits im Betriebssystem integriert oder muss ein Client installiert werden? Hier sind theoretische Abklärungen anhand der Herstellerangaben nötig, keine Testinstallationen.

Wie soll bei einem HSR weiten Wechsel auf 802.lx vorgegangen werden? Welche Gruppe aus IT-OS soll welche Aufgaben übernehmen? Wie werden unsere Benutzer informiert, welche Benutzerkreise werden informiert? Ziel ist, dass sich sämtliche Benutzergruppen ohne spezielle Schulung über 802.1x authentifizieren können.

3.2.2 Installation in der Testumgebung

Clients

Am Testarbeitsplatz müssen mindestens drei Netzwerkanschlüsse (1 x verbunden mit einem Cisco 2960G-Switchport, 1 x Cisco 2960S-Switchport und 1 x hinter einem VoIP-Phone, welches mit einem Cisco 3560P Switch verbunden ist) für 802.1x konfiguriert werden. Diese Anschlüsse müssen so vorbereitet werden, dass sie sich genauso in einem Sitzungszimmer befinden könnten.

Die Authentifizierung der Benutzer läuft redundant über die beiden Radius-Server in der Testumgebung. Es dürfen keine Passworte unverschlüsselt über das Netzwerk transportiert werden. Der 802.1x-Client muss transparent arbeiten, d.h. der Benutzer muss sein Login/Passwort während dem Bootprozess des Clients nur einmal eingeben.

Kann sich ein Benutzer erfolgreich über 802.1x authentifizieren, soll dem Client das angestammte VLAN zugeordnet werden. Kann sich ein Benutzer über 802.1x nicht anmelden oder nimmt der Client nicht am 802.1x Authentifizierungsprozess teil, muss der Switch dem Port automatisch das VLAN 229 zuordnen.

Lösung mit den bestehenden Accounts ITR\amuster (Zuweisung VLAN 1-40) und ITR\bmuster (Zuweisung VLAN 200).

Alle 802.1x Anmeldungen (egal ob erfolgreich oder nicht) müssen auf dem Radius-Server gelogt werden.

Switches, Radius Server & AD

Die Access-Switches haben eine Default-Konfiguration nach HSR Richtlinien. Der Radius Server wird auf Windows Server 2012 migriert und übernimmt ebenfalls die AAA Rolle.

Das 802.1x Attribut der Clients wird im Active Directory gesetzt.

3.2.3 Dokumentation

Sämtliche Konfigurationsanpassungen auf Netzwerkgeräten und Servern müssen für eine Fachperson verständlich dokumentiert werden.
Eine schematische Darstellung zeigt die gesamte 802.1x-Umgebung. Folgende Parameter sind angegeben: Hostnamen, IP-Adressen, VLAN- und Subnet-Informationen, für 802.1x spezifisch verwendete Protokolle und Verschlüsselungstechniken.
Für die HSR Benutzer muss eine kurze Anleitung (ausschliesslich für das Betriebssystem Windows7, HSR Standardinstallation) verfasst werden, welche die folgenden Fragen abdeckt:

- Was ist 802.1x, welche Vorteile (allenfalls auch welche Nachteile) bringt es mir an der HSR?
- Was ändert sich für mich?
- Wie muss ich meinen Client für die 802.lx-Authentifizierung vorbereiten?
- Wie muss ich mich über 802.1x anmelden und wie kann ich kontrollieren ob die Anmeldung erfolgreich war?
- Wer hilft mir bei Fragen/Problemen?

Auf den Webseiten der Informatikdienste muss den Benutzern die Benutzeranleitung als PDF, versehen mit einem kurzen Begleittext, zur Verfügung gestellt werden. (Im Typo-3 noch ausblenden)

3.2.4 Tests

Sämtliche Konfigurationen rund um die Authentifizierung mittels 802.1x müssen vollständig und nachvollziehbar getestet werden. Die Testresultate (positive und negative) gehören in die Dokumentation der IPA.

3.2.5 Systemgrenzen

- Keine Drucker Authentifizierung
- Nur Tests mit drahtgebundenem LAN, keine WLAN-Implementation
- Praktische Arbeiten und Tests der Clients nur unter Microsoft Windows 7 Enterprise
- Allenfalls nötige Anpassungen an einer Firewall werden auf Verlangen von Marco Koch vom Netzwerkteam durchgeführt.

4 Projektorganisation

Lernender	**Lehrbetrieb**
Marco Koch	Hochschule für Technik
Niederwies 18	Oberseestrasse 10
8857 Vorderthal	8640 Rapperswil
Fachverantwortlicher:	Roger Baumer
Hauptexperte:	Giuseppe Auriemma
Zweitexperte:	Roger Aepli

4.1 Methode

Für die Strukturierung des Projektes wurde IPERKA verwendet, einerseits weil ich dieses im RAU (Regionales Ausbildungszentrum Au) verwendet habe und andererseits weil ich nichts anderes kenne.

4.1.1 IPERKA

Die sechs Phasen von IPERKA erlauben einen sauberen Übergang von der Konzeptphase zur Realisierungsphase bis hin zur Auswertung.

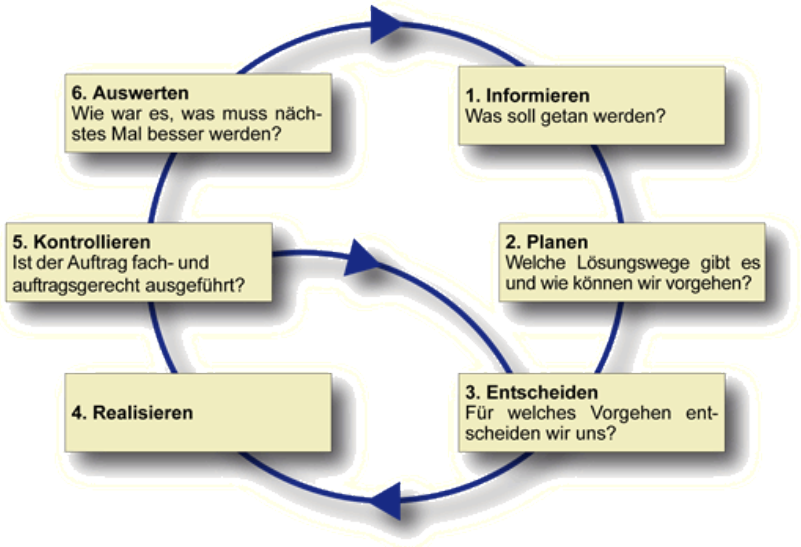


Abbildung 1: Phasen IPERKA

4.2 Vorstellung Personen

Tabelle 2 involvierte Personen

Name	Funktion
Anton Koolen	• Fachverantwortlicher ITIL • Chef Service Desk
Patrick Oberli	• Angestellter IT-Netzwerk
Roger Baumer	• Angestellter IT-Netzwerk • Fachverantwortlicher

4.3 Deklaration Vorkenntnisse

- IT Client Management (9 Monate)
  Clientsysteme (Windows/Linux)
- IT Server (4 Monate)
  Virtuelle Server erstellen (mit und ohne Template)
  Server-Installation (Windows Server 2008 R2, Windows Server 2012)
- IT Netzwerk (bisher 9 Monate)
  Netzwerkinfrastruktur (VLANs/DMZ)

4.4 Deklaration der Vorarbeiten

- Selbststudium zu Windows Server 2012
- Testinstallation mit einem Radius und Cisco 2960G Access Switch

5 Zeitplan

Nr.	Arbeitspaket	Soll Dauer	Ist Dauer		Tag 1 06.03.13	Tag 2 07.03.13	Tag 3 08.03.13	Tag 4 11.03.13	Tag 5 13.03.13	Tag 6 14.03.13	Tag 7 15.03.13	Tag 8 18.03.13	Tag 9 20.03.13	Tag 10 21.03.13	Tag 11 22.03.13
I	Arbeitspakete definieren und Zeitplan erstellen	2h	2h	Soll											
				Ist											
	Spezifikationen Client-Betriebssysteme	1.3h	1.3h	Soll											
				Ist											
	Spezifikationen Access Switches iOS & IP-Phone POE	1.3h	1.3h	Soll											
				Ist											
	Spezifikationen Windows Radius	1.3h	1.3h	Soll											
				Ist											
P	Netzplan	2h	2h	Soll											
				Ist											
	Konzept Client- / User-Authentifikation	4h	2h	Soll											
				Ist											
	Konzept Räumlichkeiten	4h	2h	Soll											
				Ist											
	Testprotokoll	4h	6h	Soll											
				Ist											
E	Welche Lösung?	1h	2h	Soll											
				Ist											
R	Dokumentieren	-	-	Soll											
				Ist											
	Installation Windows Server Konfiguration Radius und Switches	8h	14h	Soll											
				Ist											
	Group Policy ITR-Clients	2h	2h	Soll											
				Ist											
	Benutzeranleitung	2h	2h	Soll											
				Ist											
	Reserve	4h	-	Soll											
				Ist											
K	Testen gemäss Testprotokoll	12h	12h	Soll											
				Ist											
A	Fazit	4h	4h	Soll											
				Ist											
	Korrekturlesen / Drucken / Binden	16h	20h	Soll											
				Ist											
	Reserve	-	-	Soll											
				Ist											

Nr.	Arbeitspaket	Soll Dauer	Ist Dauer		Tag 1	Tag 2	Tag 3	Tag 4	Tag 5	Tag 6	Tag 7	Tag 8	Tag 9	Tag 10	Tag 11
					06.03.13	07.03.13	08.03.13	11.03.13	13.03.13	14.03.13	15.03.13	18.03.13	20.03.13	21.03.13	22.03.13
	Expertenbesuch	-	-	Soll											
				Ist											

Die folgenden Meilensteine sind als rote Linie im Zeitplan versehen

- Konzept fertig
- Konzept umgesetzt
- Umgebung getestet
- Dokumentation gedruckt und gebunden

6 Arbeitsprotokoll / Journal

6.1 IPA-Tag 1 06.03.13

Zeit	Erledigte Aufgabe	Dauer
08:00 – 08:10	Aufgabenstellung studiert	-
08:10 – 10:10	Arbeitspakete definiert und Zeitplan erstellt	2h
10:10 – 14:15	Spezifikationen und Handbücher recherchiert	4h
14:20 – 15:20	Netzplan erstellt	1h
15:20 – 16:20	Arbeitsplatz eingerichtet	1h
Tagestotal		8h

Vergleich mit Zeitplan

Ich habe für den Netzplan nicht volle 2 Stunden gebraucht. Dies ermöglichte mir allerdings meinen Arbeitsplatz fertig einzurichten, die drei Switches, die zwei Laptops und das IP-Phone zu organisieren und zu installieren.

6.2 IPA-Tag 2 07.03.13

Zeit	Erledigte Aufgabe	Dauer
08:00 – 10:00	Konzept Client- und User-Authentifikation	2h
10:00 – 12:00	Konzept Räumlichkeiten	2h
13:30 – 15:30	Testprotokoll	2h
15:30 – 17:30	Entscheidung	2h
Tagestotal		8h
Total		**16h**

Vergleich mit Zeitplan

Für den konzeptionellen Teil habe ich gut die Hälfte an Zeit gebraucht als ursprünglich eingeplant. Dies ermöglichte mir, ein wenig vorzugreifen und gleich mit der Entscheidung und dem Testprotokoll weiterzumachen.

6.3 IPA-Tag 3 08.03.13

Zeit	Erledigte Aufgabe	Dauer
08:00 – 12:00	Testprotokoll	4h
13:00 – 15:00	Installation 2x Radius und Konfiguration	2h
15:00 – 16:30	Expertenbesuch	1.5h
16:30 – 17:30	Installation 2x Radius und Konfiguration	1.5h
Tagestotal		8.5h
Total		**24.5h**

Vergleich mit Zeitplan

Heute habe ich letzten konzeptionellen Part abgeschlossen und bin zu der Phase der Realisierung übergegangen. Angefangen mit dem Aufsetzten der Server und dem Resetten der Switches kam ich gut vorwärts und hatte keine unvorhergesehenen Probleme.

Erfolge / Misserfolge:

Ich habe erfolgreich den ersten Meilenstein, welchen die Fertigstellung des Konzepts darstellte, erreicht. Mit dem Überschreiten dieses Meilensteins habe ich die konzeptionelle Phase abgeschlossen und mich für eine Lösung entschieden, dass heisst ab jetzt werden keine grundlegenden konzeptionellen Entscheide gefällt.

6.4 IPA-Tag 4 11.03.13

Zeit	Erledigte Aufgabe	Dauer
08:00 – 10:00	Testprotokoll	2h
10:00 – 11:30	Installation 2x Radius und Konfiguration	1.5h
Tagestotal		3.5h
Total		**28h**

Vergleich mit Zeitplan

Heute habe ich weitergemacht mit der Konfiguration der Server. Leider habe ich nach kurzer Zeit gemerkt, dass der Radius-Server unter Windows Server 2008 R2 Standard eine Lizenzbeschränkung eingebaut hat. Ich musste also den Server noch ein zweites Mal installieren. Dies verursachte aber trotzdem kein Zeitproblem.

Beanspruchte Hilfeleistung

Patrick Oberli hat mir per Anfrage die benötigten Ports auf der Firewall auf gemacht, damit die Switches mit den Radius-Server kommunizieren können.

6.5 IPA-Tag 5 13.03.13

Zeit	Erledigte Aufgabe	Dauer
08:00 – 12:00	Radius Server Policy umgesetzt	4h
13:30 – 14:30	Group Policy umgesetzt und dokumentiert	2h
14:30 – 15:30	Useranleitung erstellt	2h
Tagestotal		8h
Total		**36h**

Vergleich mit Zeitplan

Anfänglich dauerte die 802.1x-Authentifikation der Clients, welche keine 802.1x-Authentifikation unterstützen, über zwei Minuten. Nachdem ich ein wenig recherchiert hatte fand ich eine Lösung für dieses Zeitproblem. Ich habe die Timeouts etwas reduziert und somit die Authentifikations-Dauer auf 15 Sekunden reduziert.

Beanspruchte Hilfeleistung

Anton Koolen hat mir seinen Typo3-Account für den Upload der Benutzeranleitung, auf die HSR Webseite, zur Verfügung gestellt.

Erfolge / Misserfolge:

An diesem Tag habe ich die Umsetzung vollständig abgeschlossen und somit den zweiten Meilenstein erreicht. Die Konfiguration der Testumgebung ist abgeschlossen und das bereits erstellte Testprotokoll ist auch bereit um ausgefüllt zu werden.

6.6 IPA-Tag 6 14.03.13

Zeit	Erledigte Aufgabe	Dauer
8:00 – 12:00	Überarbeitung Radius- und Switch-Dokumentation	4h
13:00 – 17:00	Testprotokoll ausgeführt	4h
Tagestotal		8h
Total		**44h**

Vergleich mit Zeitplan

Heute kam ich gut vorwärts. Ich habe die eingeplante Reserve dafür verwendet, die Dokumentation des Radius-Server und die der Switches ein wenig zu überarbeiten und zu ergänzen, wo es nötig war. In der zweiten Hälfte des Tages konnte ich mit dem Testen der Umgebung beginnen.

6.7 IPA-Tag 7 15.03.13

Zeit	Erledigte Aufgabe	Dauer
8:00 – 9:30	Benutzeranleitung getestet	1.5h
9:30 – 12:00	Unbefugte Clients getestet	2.5h
13:00 – 15:00	Befugte Clients noch einmal getestet	2h
15:00 – 17:00	Radius-Logs getestet	2h
Tagestotal		8h
Total		**52h**

Vergleich mit Zeitplan

Das Testen der ganzen Umgebung hat sehr gut funktioniert und lief im geplanten zeitlichen Rahmen ab.

Erfolge / Misserfolge:

Mit dem letzten Test habe ich erfolgreich das Testen der Lösung abgeschlossen und somit den dritten Meilenstein erreicht. Sobald alles auf seine Funktion hin überprüft ist und die Kriterien erreicht sind, kann mit der Auswertung der Tests begonnen werden.

6.8 IPA-Tag 8 15.03.13

Zeit	Erledigte Aufgabe	Dauer
8:00 – 11:30	Auswertung dokumentiert	3.5h
Tagestotal		3.5h
Total		**55.5h**

Vergleich mit Zeitplan

Am heutigen Tag habe ich die Dokumentation um den entscheidenden Auswertungsteil erweitert und somit das Projekt und die Lösung abgeschlossen.

6.9 IPA-Tag 9 20.03.13

Zeit	Erledigte Aufgabe	Dauer
8:00 – 11:50	Korrekturlesen	4.0h
11:50 – 12:10	Expertenbesuch	0.3h
13:00 – 17:00	Korrekturlesen	4h
Tagestotal		8.3h
Total		**64h**

Vergleich mit Zeitplan

Heute habe ich meiner Dokumentation den letzten Schliff gegeben. An gewissen Stellen habe ich Unklarheiten ausgemerzt und unschöne Formatierungen entfernt. Ich liege sehr gut im Zeitplan und werde meine IPA wahrscheinlich bald drucken.

6.10 IPA-Tag 10 21.03.13

Zeit	Erledigte Aufgabe	Dauer
8:00 – 12:00	Korrekturlesen und Feinschliff	4.0h
13:00 – 17:00	Korrekturlesen und Feinschliff	4.0h
Tagestotal		8h
Total		**72h**

Vergleich mit Zeitplan

Am heutigen Tag habe ich mich hauptsächlich damit beschäftigt dem Dokument den letzten Schliff zu geben. Ich habe definiert wo einen neue Seite anfangen soll und wie der Inhalt umbricht. Einige verschiedene Formatierungen sind noch angeglichen worden, damit die Dokumentation auch einheitlich daher kommt. In der zweiten Hälfte des Tages wäre laut Plan das Korrekturlesen und das Drucken abgeschlossen gewesen. Aber ich habe Zeit trotzdem noch genutzt, da ich nicht einen Tag vorher abgeben wollte, sondern lieber noch mal alles kontrollieren.

6.11 IPA-Tag 11 22.03.13

Zeit	Erledigte Aufgabe	Dauer
8:00 – 12:00 13:00 – 16:00	Drucken und Binden Drucken und Binden	4.0h 3h
Tagestotal		7h
Total		**79h**

Vergleich mit Zeitplan

Am letzten Tag meiner IPA habe ich die Materialien zum Binden der Dokumentation beschafft. Die finale Version der IPA-Dokumentation wurde in dreifacher Ausführung gedruckt, gebunden und anschliessend Roger Baumer übergeben. Mit dem Drucken der IPA habe ich den vierten und letzten Meilenstein erreicht und somit das Projekt abgeschlossen.

Zweiter Teil Projekt

7 Informieren

Grundsätzlich ist 802.1x nur ein standardisiertes Framework, welches erlaubt, egal mit welcher Methode einen Client oder einen User am Netzwerk anzumelden. Wobei mich in diesem Projekt nur die Authentifikation über drahtgebundene Netzwerke interessiert. Welche Authentifizierungsmethode (MSCHAPv2, MSCHAP, CHAP, PAP oder SPAP) innerhalb von 802.1x-Paketen bzw. EAP/PEAP-Paketen eingesetzt wird, hängt vom eingesetzten Authentication Server und dem Client-Betriebssystem ab. Der Supplicant, in drahtgebundenen Netzwerken der Access Switch, muss nur EAP/PEAP bzw. 802.1x unterstützen, da er nur als eine Art Proxy dient.

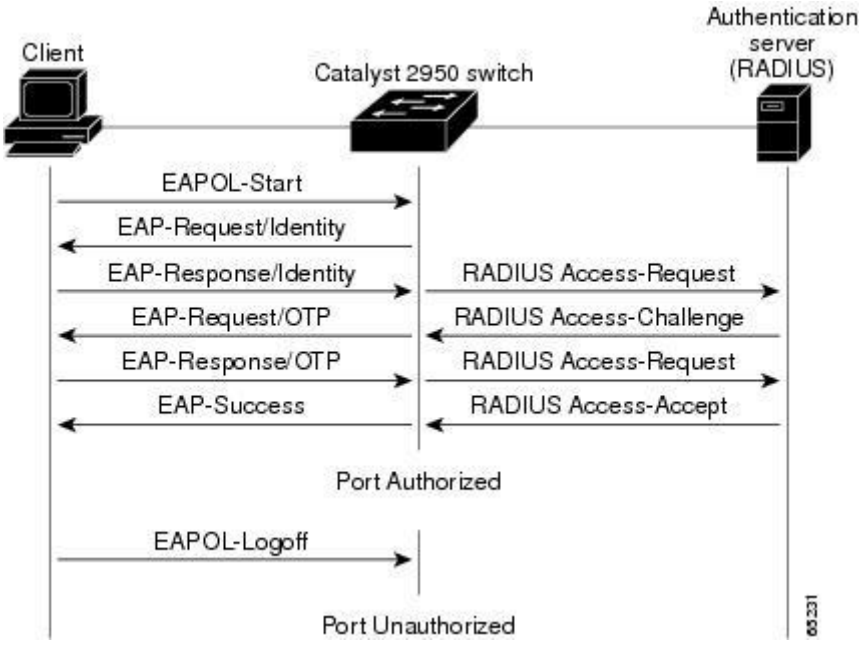


Abbildung 2: EAP-Ablauf

1. Der Supplicant meldet sich beim Authenticator (Link impuls), eine EAPOL (EAP over LAN)-Session wird gestartet.
2. Der Authenticator fragt den Supplicant nach dessen Host-Identifikationen.
3. Der Supplicant sendet dem Authenticator die Host-Identifikation.
4. Dem Radius wird ein Access Request mit den Host-Identifikation gesendet.
5. Der Radius teilt dem Authenticator mit, dass der User sich authentifizieren darf.
6. Der Authenticator fragt den Supplicant nach den Identifiaktionsdaten (User oder Client Credentials).
7. Der Supplicant sendet seine Authentifizierungsdaten dem Supplicant.
8. Der Supplicant sendet die Daten weiter.

9. Wenn der Radius den Supplicant authentifizieren konnte, sendet dieser einen Access-Accept zurück.

7.1 IST-Zustand

Am Netzwerk der Hochschule für Technik (HSR) werden rund 900 PC-Systeme in rund 20 verschiedenen Subnetzen verwendet. Etwa 50 bis 100 Systeme sind mobile Geräte von Angestellten und Dozenten, welche auf dem ganzen Campus verteilt im Einsatz sind. Diese Benutzer haben in der Regel einen festen Büroarbeitsplatz und das Bedürfnis in den Unterrichtsräumen und in den Sitzungszimmern uneingeschränkt, aber abgesichert, mit ihren persönlichen Notebooks auf ihre Daten zugreifen zu können. Aktuell werden diesen persönlichen Notebooks ihr „Heimsubnetz“ zugeteilt, in welchem ein zentraler DHCP aufgrund der MAC-Adresse die IP-Adresse zuteilt. Die Netzwerkports der Büroarbeitsplätze sind fix auf das „Heimsubnetz“ konfiguriert. In den Übungsräumen und Sitzungszimmern besteht über das WLAN die Möglichkeit, auf globale Ressourcen zuzugreifen. Dies hat aber im Vergleich zum „Heimsubnetz“, wegen der dazwischen geschalteten Firewall Einschränkungen zur Folge.

7.2 SOLL-Zustand

Das statische Konfigurieren der Ports und auch die statische Vergabe von IP-Adressen ist nicht mehr dynamisch genug. Es bedeutet immer Aufwand des Netzwerkteams, wenn irgendwo temporär ein Port umkonfiguriert werden muss. Heute wird diese Arbeit in Tickets abgebildet. Doch in Zukunft sollen die Ports universaler werden und gleichzeitig sicherer und schwieriger zu missbrauchen. Der Port soll das Heimsubnetz des Clients oder des Users aufschalten, wenn sich dieser an dem Port befindet. Damit fällt der Konfigurationsaufwand des Netzwerkteams weg. Die Ports werden einmalig als 802.1x-Port konfiguriert und verändern sich so wie man sie braucht. Über längere Zeit will man an der HSR den statischen IP-Adressbezug abschaffen und übergehen zu freien DHCP-Pools. Bevor dies aber geschieht, soll die 802.1x-Umgebung umgesetzt werden. Damit in dieser Übergangsphase nicht mehr Probleme auftreten als jetzt, muss unter anderem noch entschieden werden, wer sich am Netzwerk anmeldet. Ob sich die Clients oder die User der Domäne anmelden.

7.3 Cisco-Komponenten

7.3.1 Access Switches

Alle drei Switches bzw. IOS-Versionen unterstützen die *Vendor Specific Attributes*, welche zwingend notwendig sind für die dynamische Zuweisung der VLAN. Des Weiteren wird ein, pro Switch konfiguriertes, Guest VLAN unterstützt. Für die Kommunikation zwischen Switch und Radius-Server werden die normalen Radius-Ports (tcp/1645, tcp/1646, tcp/1812, tcp/1813) verwendet.

- 2960G 8 Ports
  Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(53)SE2,
  Quelle: 2960G 12.2(53)SE2 Command Reference
- 2960S 52 Ports
  Cisco IOS Software, C2960S Software (C2960S-UNIVERSALK9-M), Version 12.2(58)SE2,
  Quelle: 2960S 12.2(58)SE2 Command Reference
- 3560G 28 Ports
  Cisco IOS Software, C3560 Software (C3560-IPBASEK9-M), Version 12.2(58)SE1,
  Quelle: 3560G 12.2(58)SE1 Command Reference

7.3.2 IP-Phones

Quelle: Cisco UC Phone CP-8945 Reference

7.4 Radius

Diese Komponente des Projekts ist weniger kritisch als die Client-Betriebssysteme, da die nötigen Authentifikationsmechanismen alle schon unterstützt werden oder notfalls nachinstalliert werden könnten. Da die Dokumentation für den Radius unter Windows Server 2008 dieselbe ist wie unter Windows Server 2012, gehe ich davon aus, dass es dieselbe Version ist.

Quelle: Windows Server Radius

7.5 Client-Betriebssysteme

7.5.1 Windows 7

Einschränkungen:
Unter Windows 7 ist die Authentifizierung der Clients an kabelgebundenen Netzwerken per default deaktiviert. Der Service *Wired Auto Config* muss entweder jedes Mal gestartet werden oder einmalig auf *Automatic* gestellt werden, damit der Service immer läuft. Dies ist auch via Group Policy möglich.

Integration:
802.1x-Authentifikation wurde seit Windows Vista im Betriebssystem integriert. EAP/PEAP/PEAP-TLS mit der inneren Authentifizierung Methode MSCHAPv2 sind unterstützt.

Quelle: Windows 8 Integration

7.5.2 Windows 8

Einschränkungen:
Windows 8 verhält sich gleich wie Windows 7. Die Authentifizierung der Clients an kabelgebundenen Netzwerken ist per default deaktiviert. Der Service *Wired Auto Config* muss entweder jedes Mal

gestartet werden oder einmalig auf *Automatic* gestellt werden, damit der Service immer läuft. Dies ist auch via Group Policy möglich.

Integration:

802.1x-Authentifikation wurde seit Windows Vista im Betriebssystem integriert. EAP/PEAP/PEAP-TLS mit der inneren Authentifizierung Methode MSCHAPv2 sind unterstützt.

Quelle: Windows 7 Integration

7.5.3 Mac OS X

Einschränkungen:

Ich habe für Mac OS X keine bekannten Einschränkungen gefunden.

Integration:

802.1x-Authentifikation wurde bereits seit der Version 10.4.6 (Tiger) unterstützt. Die Funktionalität wurde stabilisiert in der Version 10.6.3 (Snow Leopard). Aktuell ist die Version 10.8 (Mountain Lion). EAP/PEAP/PEAP-TLS mit der inneren Authentifizierung Methode MSCHAPv2 sind unterstützt.

Quelle: Mac OS X 10.5 Integration

7.5.4 Linux Fedora 13

Einschränkungen:

Ich habe für Fedora 13 keine bekannten Einschränkungen gefunden.

Integration:

In Fedora 13 wurde 802.1x bereits integriert. EAP/PEAP/PEAP-TLS mit der inneren Authentifizierung Methode MSCHAPv2 sind unterstützt. Aktuell ist die Version Fedora 18.

Quelle: Linux Fedora 13 Integration

8 Planen

8.1 Allgemeiner Aufbau

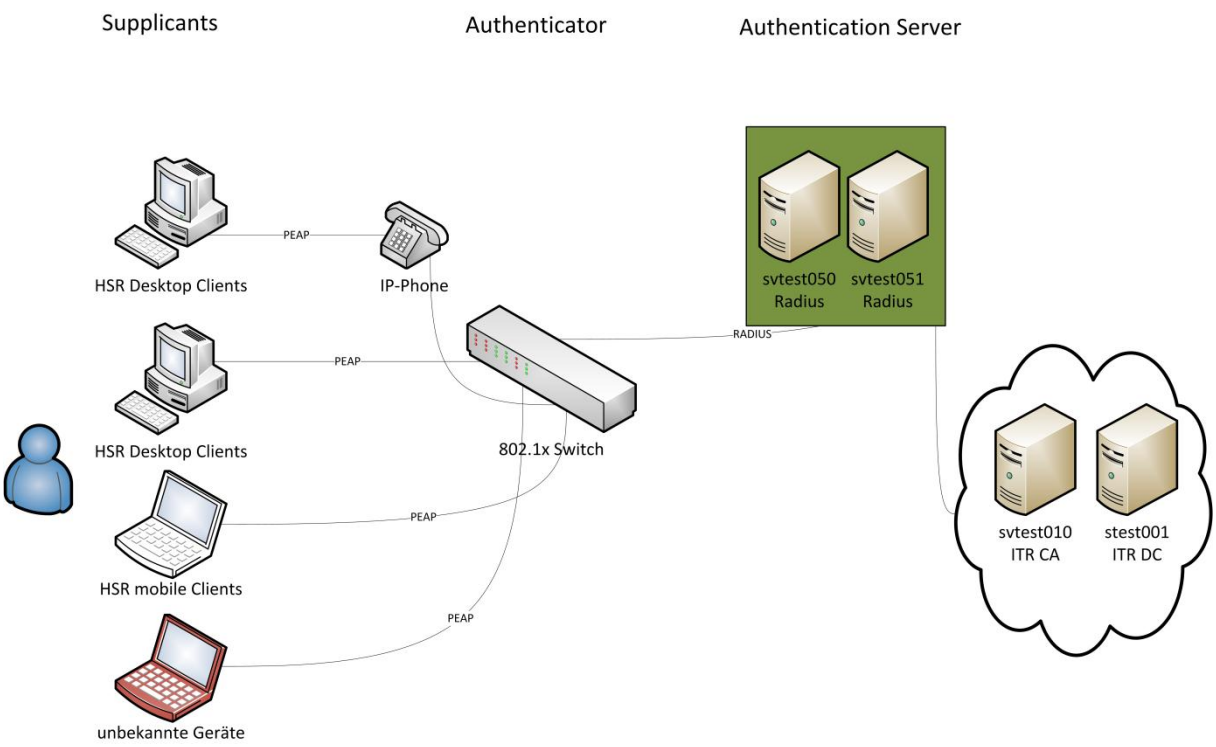


Abbildung 3: Allgemeiner Aufbau

Für die Planung müssen die in der Abbildung gezeigten Geräte oder Geräten-Gruppen berücksichtigt werden. Auf der linken Seite die Supplicants, die aus den stationären HSR-Desktop-Clients und den mobilen HSR-Geräten bestehen und die in rot markierten, unbekannten Geräte. Auf der rechten Seite sind die zwei Radius-Server, die als AAA-Server dienen. Weiter sind noch das AD der Testumgebung und die Certificate Authority als Infrastruktur-Server eingezeichnet. Diese betrachte ich allerdings als gegeben, da diese auch in der HSR-Liveumgebung bereits vorhanden sind und sie keine Änderung betrifft.

8.2 Authentifikations-Methode

Da aus der Aufgabenstellung hervorgeht, dass keine Passwörter in Klartext übers Netzwerk übertragen werden dürfen, kommen nur die verschlüsselten EAP-Varianten infrage. Diese wären EAP-TLS, welche für jeden Client und den Server ein Zertifikat voraussetzt, und PEAP, welches nur ein Server-Zertifikat voraussetzt, und keines für den Clients. Mit beiden Methoden wird die Aushandlung der inneren Methode und die eigentliche Authentifizierung durch einen verschlüsselten Tunnel transportiert. Als innere Methode steht MSCHAPv2 als de-facto-Standard zur Verfügung, sowie

frühere Versionen dieser Methode. Die Kombination PEAP und MSCHAPv2 wird von allen Client-Betriebssystemen und den Radius-Servern unterstützt.

Welche Methode verwendet werden soll, kann für HSR-Geräte via Group Policy festgelegt werden.

8.3 Client- und/oder User-Authentifikation

An der HSR werden die IP-Adressen in den meisten Client-Netzten statisch vergeben. Das heisst, dass der DHCP-Server einer MAC-Adresse immer dieselbe IP-Adresse zugewiesen wird. Mit der Methode PEAP und MSCHAPv2 können sich Domänen-User und Domänen-Clients am Radius anmelden. In der nachfolgenden Tabelle sind die zwei Varianten und die Kombination der beiden Varianten gegenübergestellt. Unterschieden wird zwischen Desktop Office, die persönlichen Clients der Angestellten, und Desktop Public, die Clients, an denen die Studenten in den Übungsräumen arbeiten.

Tabelle 3: Client- und User-Authentifikation

Netzwerkteilnehmer	HSR-Clients			Unbekannte authentifizierte Clients	Unbekannte Clients
	Desktop Public	Desktop Office	Mobile Clients		
User Auth.	Client zwingend selbes VLAN (User Auth. via Group Policy)			Geräte von Studenten und Angestellten	Gäste VLAN
Client Auth.	OK (Client Auth. via Group Policy)			-	Gäste VLAN
User & Client Auth.	OK (Client Auth. via Group Policy)			Geräte von Studenten und Angestellten	Gäste VLAN

8.3.1 User-Authentifikation und VLAN-Zuweisung

Weil an der HSR die IP-Adressen statisch mit MAC-Adressen verknüpft werden, dürfte der Angestellte nur sein eigenes Gerät verwenden und Studenten nur die Geräte ihres Studiengangs, da sonst der Client im falschen VLAN landet und vom DHCP Server keine IP-Adresse bekommt. Zusätzlich hatte man keine Kontrolle darüber mit welchen Geräten sich die User am Netzwerk anmeldet.

8.3.2 Client-Authentifikation und VLAN-Zuweisung

Die Problematik, dass der Client im falschen VLAN landet, besteht mit dieser Methode nicht. Der Client wird einmalig im Active Directory einer VLAN-Access-Gruppe hinzugefügt. Problematisch ist an dieser Methode, dass man nicht genau weiss, welcher User sich gerade an dem Client angemeldet hat, da sich der Client selbst anmeldet. Diese Problematik ist aber gleichzeitig ein Vorteil, wenn es um

die erste Anmeldung eines Users an einem Client geht. Der Client ist authentifiziert, bevor der User sich anmelden will, und kann somit das Profil auf den Client kopieren. Dies wäre mit einer reinen User-Authentifizierung nicht möglich.

8.3.3 User- und Client-Authentifikation und VLAN-Zuweisung

Der Parallelbetrieb von beiden Methoden ist durchaus möglich. Somit könnte man Client-Authentifikation für die VLAN einsetzen, in denen die IP-Adressen statisch vergeben werden. Und User-Authentifikation in den Netzen, in denen freie DHCP-Pools verwendet werden. Mit der Kombination wäre schrittweise der Übergang zu freien DHCP-Pools möglich.

8.3.4 Auswirkungen auf den Betrieb

Der Einfluss auf den Betrieb ist bei der Authentifizierung der Clients eher gering. Die Authentifizierung passiert versteckt im Hintergrund ohne Interaktion des Users. Das genaue Gegenteil besteht bei der User-Authentifizierung. Die User müssen Bescheid wissen, dass der Client sich zuerst mit den Login-Daten des Users am Netzwerk anmelden muss, bevor er sich am Client anmelden kann. Dies passiert zwar gleichzeitig, wenn sich der User schon einmal an dem Client angemeldet hat, birgt aber neue Probleme, wenn sich der User noch nie angemeldet hat.

8.4 Mögliche Einsatzgebiete

In diesem Kapitel soll untersucht werden, welche Räumlichkeiten sich für den Einsatz einer 802.1x-Authentifikation eigen.

Die HSR-User lassen sich in drei Nutzergruppen unterteilen. Die Angestellten benutzen ihr persönliches Notebook oder ihren persönlichen Desktop Client. Die Studenten benutzen die Desktop Clients in den Übungsräumen und ihr eigenes privates Notebook. Und zum Schluss die externen Mitarbeiter, welche nur ihr eigenes Gerät verwenden.

8.4.1 Sitzungszimmer

Die Sitzungszimmer werden von verschieden HSR-Angestellten und externen Mitarbeiter benutzt. Sie verwenden ihr persönliches HSR-Notebook oder ein Ausleihgerät, welches vom Service Desk zur Verfügung gestellt wird. Als Beispiel dient das Zimmer 1.223.

+ pro

- Es können sich nur HSR-Clients bzw. HSR-User anmelden welche sich auch in einer VLAN-Access-Gruppe befinden. So wird eine höhere Sicherheit garantiert.
- Der Netzwerkanschluss kann verwendet werden, ohne dass das Netzwerkteam die Dose umpatchen muss.

- Schlägt die Authentifizierung fehl, kann der unbekannte User sich trotzdem noch via Gäste-VLAN mit dem Internet verbinden.

- contra

- -

Empfehlung:

Der Einsatz von 802.1x in den Sitzungsräumen bietet sich an, da die User und Geräte immer wechseln und das bisher immer ein Umpatchen der Dose bedeutete.

8.4.2 Übungsräume für Studierende

Die Übungsräume werden von verschieden HSR-Angestellten und Studenten benutzt.
Verwendet werden die fest installierten Übungsraumrechner und das persönliche Notebook des Dozenten. Als Beispiel dient das Zimmer 1.202.

+ pro

- Es können sich nur HSR-Clients bzw. HSR-User anmelden, welche sich auch in einer VLAN-Access-Gruppe befinden. So wird eine höhere Sicherheit garantiert.
    - Bei der Client-Authentifizierung könnte zusätzlich sichergestellt werden, dass die Studenten die Netzwerkanschlüsse der Übungsraumrechner nicht für ihr persönliches Notebook verwenden können.
- Der Netzwerkanschluss kann verwendet werden, ohne dass das Netzwerkteam die Dose umpatchen muss.
- Schlägt die Authentifizierung fehl, kann der unbekannte User sich trotzdem noch via Gäste-VLAN mit dem Internet verbinden.

- contra

- Bei der User-Authentifizierung könnten Studenten die Netzwekanschlüsse auch mit ihren persönlichen Notebooks nutzen.
- PXE Boot für die Installation der Übungsräume wird erschwert.

Empfehlung:

In den Übungsräumen würde sich eine Client-Authentifizierung nicht nur am Dozentenplatz anbieten, sondern auch bei den stationären Übungsraumrechnern, da diese Netzwerkanschlüsse häufiger ausgesteckt und missbraucht werden. Allerdings erschwert dies das Aufsetzen des Übungsraumes, weil dafür der PXE Boot verwendet wird.

8.4.3 Dozenten- und Assistenzbüros

Die Büros werden von Dozenten und deren Assistenten benutzt. Die Clients in diesen Büros wechseln eher selten, somit werden auch selten verschiedene VLAN gebraucht. Es werden hauptsächlich HSR-Clients verwendet. Als Beispiel dient das Zimmer 6.108.

+ pro

- Es können sich nur HSR-Clients bzw. HSR-User anmelden welche sich auch in einer VLAN-Access-Gruppe befinden. So wird eine höhere Sicherheit garantiert.
- Der Netzwerkanschluss kann verwendet werden, ohne dass das Netzwerkteam die Dose umpatchen muss.
- Schlägt die Authentifizierung fehl, kann der unbekannte User sich trotzdem noch via Gäste-VLAN mit dem Internet verbinden.

- contra

- PXE Boot für die Installation der Clients wird erschwert.

Empfehlung:
In diesen Büros würde der Einsatz von 802.1x nur erhöhte Sicherheit als Vorteil bringen.

8.4.4 Büro IT-Client-Management

In diesem Büro besteht ein ständiger Wechsel von Geräten. Hier werden Geräte aufgesetzt und gewiped. Ausserdem befinden sich hier die Desktop-Geräte von IT-Angestellten mit je einem IP-Phone. Als Beispiel dient das Zimmer 1.015.

+ pro

- Es können sich nur HSR-Clients bzw. HSR-User anmelden welche sich auch in einer VLAN Access-Gruppe befinden. So wird eine höhere Sicherheit garantiert.
- Der Netzwerkanschluss kann verwendet werden, ohne dass das Netzwerkteam die Dose umpatchen muss.
- Schlägt die Authentifizierung fehl kann der unbekannte User sich trotzdem noch via Gäst-VLAN mit dem Internet verbinden.

- contra

- Bei der User-Authentifizierung könnten Studenten die Netzwerkanschlüsse auch mit ihren persönlichen Notebooks nutzen.
- Geräte, die aus wichtigen Gründen nicht in der Domäne sind, benötigen 802.1x-Ausnahmen.
- PXE Boot wird erschwert.

Empfehlung:

In diesen Büros wäre der Einsatz von 802.1x nur auf der Installationsbank sinnvoll, da nicht so wie jetzt für jedes VLAN, dass gebraucht wird, dedizierte Ports bereitgestellt werden müssen. Für die Clients der Angestellten wären die Vorteile gering.

8.4.5 Problematik PXE Boot Installation

Um den Prozess des Imaging der Clients zu automatisieren, wird an der HSR Altiris eingesetzt. Dies ist eine Sammlung von Tools, welche es ermöglichen, einen ganzen Workflow aufzubauen. Teil dieses komplexen Systems ist der PXE Boot. Der Client startet von einem Image, welches er sich über das Netzwerk von einem TFTP-Server holt. Da der PXE Client auf den Geräten bis jetzt keine 802.1x-Authentifikation unterstützt, wäre, ein PXE Boot nur mit eine MAC Address bypass möglich. Eine zweite Möglichkeit wäre, den PXE Boot für den Zeitraum der Installation zu deaktivieren. Die dritte Variante wäre den PXE Boot im Gäste-VLAN anzubieten, und somit die Clients, die neu zu installieren sind, nicht zu authentifizieren. Allerdings müsste der ganze Aufsetz-Prozess daraufhin untersucht werden, da ganz viele dieser Schritte auch ausserhalb des PXE Boot passieren und somit das halb installierte Betriebssystem auch im Gäste-VLAN fertiggestellt werden können muss.

8.4.6 Fazit

Der Einsatz von 802.1x in den öffentlichen Bereichen ist zu empfehlen. Hier kann die Sicherheit markant erhöht werden. Mit öffentlichen Bereichen sind die Übungsräume und die Gänge gemeint. Was die Büros angeht, bringt die Netzwerk-Authentifikation nur gering mehr Sicherheit, da der Zugriff in die Räume bereits per Schlüssel gesichert ist.

8.5 Tests

Das ausführliche Testszenario und dessen Ergebnisse befinden sich im Kapitel „Kontrollieren“. Hier wird aber grob erklärt, was getestet wird.

8.5.1 Windows-7-authentifizierte Clients

Erhält der Client das angestammte VLAN wenn,

- er sich hinter einem IP-Phone befindet.
- er sich direkt am Switch befindet.
- er entsperrt wird.
- er neu gestartet wird.

8.5.2 Windows-7-nicht-authentifizierte Clients

Erhalten die unbekannten Clients das Gäste VLAN wenn,

- sie keine 802.1x-Authentifikation unterstützen (Timeout).
- sie nicht erfolgreich authentifiziert werden konnten.

8.5.3 Switches

Die Switches weisen allen Rechnern das Gäste-VLAN zu, wenn

- beide Radius-Server down sind.

Die Switches senden Access-Request an den anderen Radius-Server, wenn einer offline ist.

8.5.4 Radius

Der Radius-Server loggt, wenn

- eine erfolglose Authentifikation erfolgt.
- eine erfolgreiche Authentifikation erfolgt.

8.5.5 Benutzeranleitung

- Download möglich

9 Entscheiden

In diesem Kapitel werde ich festlegen, welche der Varianten, beschrieben im Kapitel „Planen“, in der Testumgebung zum Einsatz kommen werden.

9.1 Authentifikations-Methode

Hier habe ich mich für PEAP mit der inneren Methode MSCHAPv2 entschieden. Dieses Setup wird von allen Client-Betriebssystemen unterstützt. Für die Clients aus der HSR-Domäne können diese Einstellungen via Group Policy verteilt werden.

9.2 Client- und/oder User-Authentifikation

Da die Auswirkungen auf den Betrieb bei der Client-Authentifikation geringer sind als bei der User-Authentifikation, habe ich mich primär dafür entschieden. Um ein erfolgreiches Login von fremden Clients aber trotzdem testen zu können, werde ich in der Testumgebung die Kombination von beiden Authentifikationen umsetzen.

9.3 Mögliche Einsatzgebiete

Hier sind die Empfehlungen aus dem Kapitel „Planen“ zu beachten.

10 Realisieren

10.1 Systembeschreibung

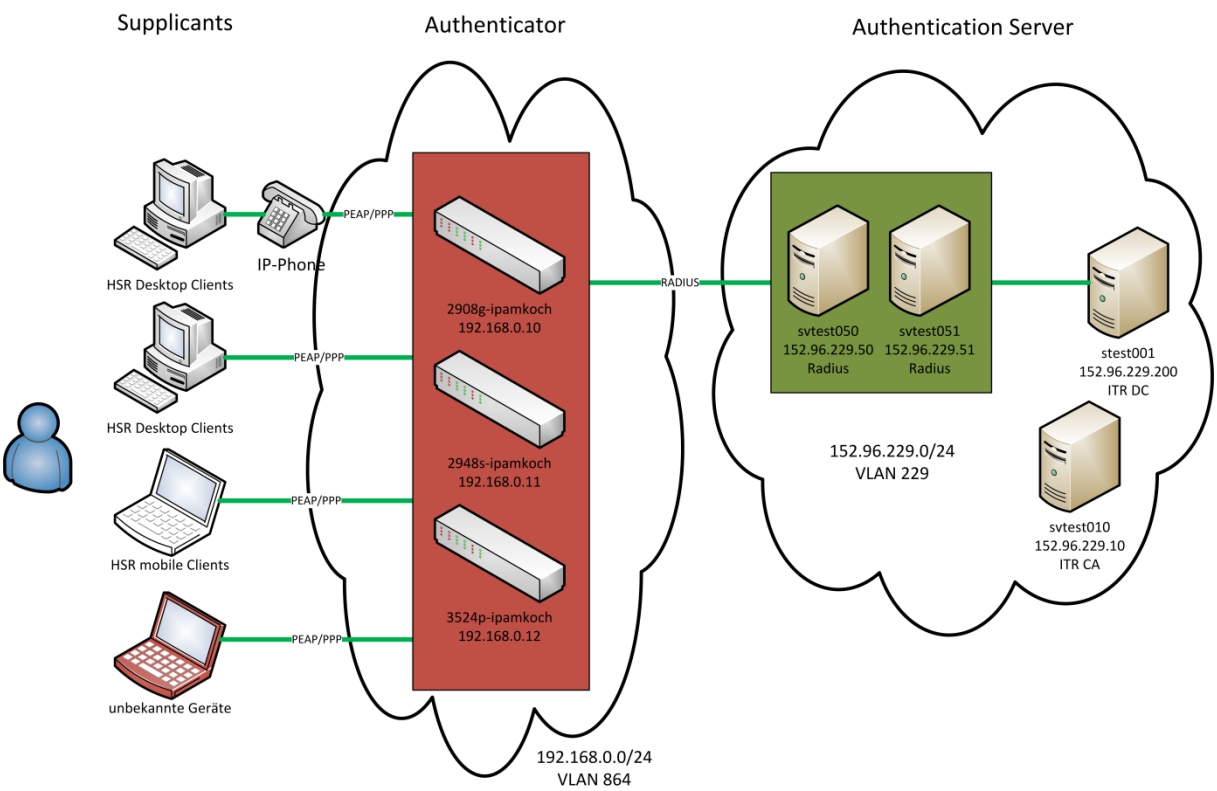


Abbildung 4: Netzplan

Um die ganze Konfiguration realitätsnah testen zu können, kommt die ITR-Testumgebung zum Einsatz. Diese Testumgebung ist gleich aufgebaut wie die HSR-Liveumgebung. Sie besteht aus einem Active Directory und einer VMware-Umgebung mit drei ESX Hosts. Die Radius-Testserver werden auf dieser VMware-Umgebung installiert und betrieben. Im Active Directory der Testumgebung existieren alle Gruppen, die auch im Active Directory existieren würden. Zusätzlich wurden einige Test-User angelegt (amuster, bmuster, cmuster, hmuster, pmuster).

10.2 Konfiguration Firewall

Als erstes musste der Zugriff aus dem Switch Management VLAN 864 zu den Radius-Servern im VLAN 229 erlaubt werden. Das Netzwerkteam hat mir dafür vier Firewall-Regeln hinzugefügt und aktiv geschaltet.

Tabelle 4: Firewall-Regeln

von Swiches	Port	zu Radius
192.168.0.0/24	udp/1645	152.96.229.50
192.168.0.0/24	udp/1645	152.96.229.51
192.168.0.0/24	udp/1646	152.96.229.50
192.168.0.0/24	udp/1646	152.96.229.51

10.3 Vorbereitung Clients

In der Testumgebung kommen zwei physikalische Clients zum Einsatz. Es handelt sich hierbei um zwei Ausleihgeräte des Service Desk. Der eine Client wurde aus der Domäne HSR entfernt und in die ITR-Domäne gesteckt. Der zwei Client wurde nur aus der HSR-Domäne entfernt und dient als fremdes bzw. unbekanntes Gerät.

Tabelle 5: Client Übersicht

Art	**physikalisch**	**physikalisch**
FQDN	**nb-lease-114366.itr.ch**	**nb-lease-115535.**
Domäne	**itr.ch**	**-**
IP-Adresse	**152.96.200.45**	**152.96.140.164**
OS	**Windows 7 Enterprise**	**Windows 7 Enterprise**

10.4 Installation Radius-Server

Im Kapitel „Planen“ habe ich herausgefunden, dass der Radius-Server unter Windows Server 2008 und unter Windows Server 2012 derselbe ist. Aus diesem Grund habe ich mich dafür entschieden, den svtest050 mit Windows Server 2008 R2 und den svtest051 mit Windows Server 2012 aufzusetzen.

10.4.1 Installation svtest050

Tabelle 6: Übersicht svtest050

Art	**virtuell**
FQDN	**svtest050.itr.ch**
IP-Adresse	**152.96.229.50**
OS	**Windows Server 2008 R2 Enterprise**
Rollen	**Network Policy Server**

Der Server wurde gemäss Installationsanleitung der HSR installiert.

Als Installationsmedium wurde folgendes iso-File verwendet:

SW_DVD5_Windows_Svr_DC_EE_SE_Web_2008_R2_64Bit_English_w_SP1_MLF_X17-22580.ISO

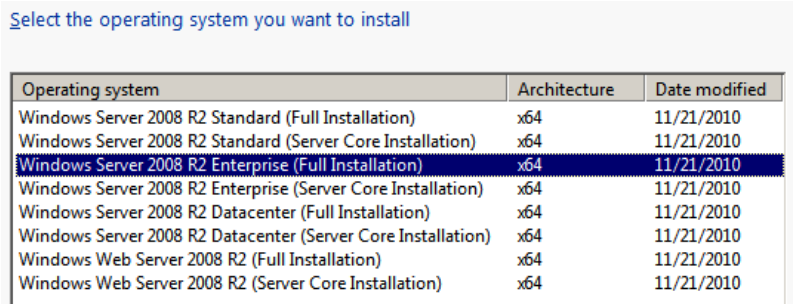


Abbildung 5: Auswahl des Betriebssystems

Bei der Auswahl des Betriebssystems muss zwingend Windows Server 2008 R2 Enterprise ausgewählt werden, da ansonsten später aus lizenztechnischen Gründen der Radius gewisse Funktionen verweigert.

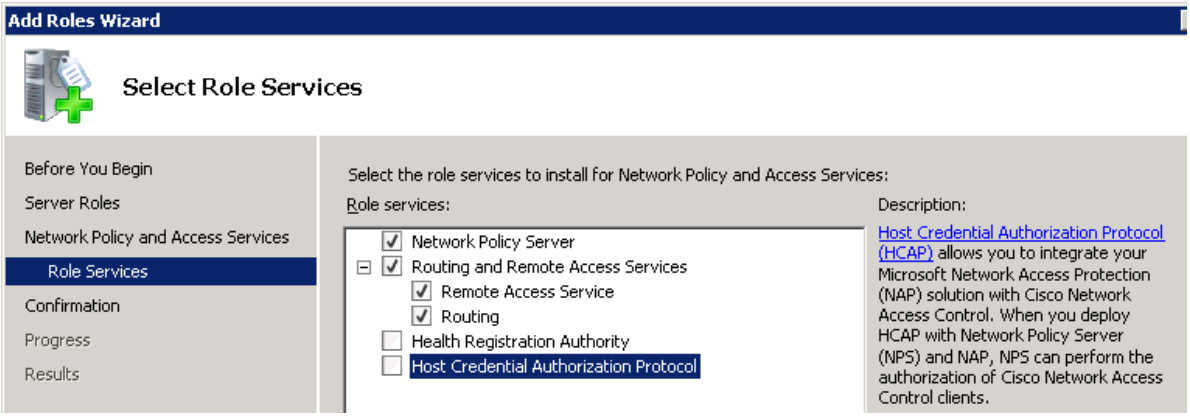


Abbildung 6: Auswahl der Rollen Server 2008

10.4.2 Installation svtest051

Tabelle 7: Übersicht svtest051

Art	**virtuell**
FQDN	**svtest051.itr.ch**
IP-Adresse	**152.96.229.51**
OS	**Windows Server 2012 Standard**
Rollen	**Network Policy Server**

Auch dieser Server wurde gemäss Installationsanleitung der HSR installiert. Als Installationsmedium wurde folgendes iso verwendet: *SW_DVD5_Win_Svr_Std_and_DataCtr_2012_64Bit_English_Core_MLF_X18-27588.ISO*

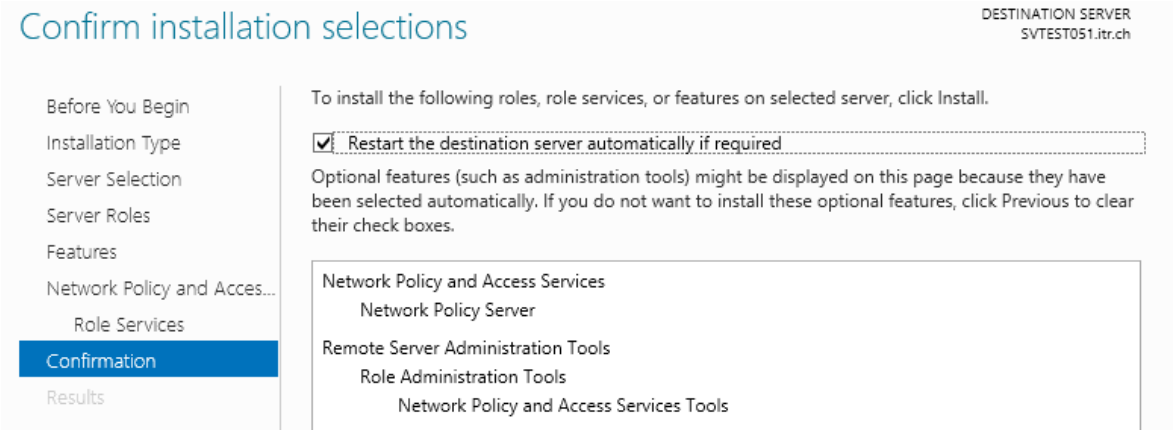


Abbildung 7: Auswahl der Rollen Server 2012

10.5 Konfiguration Radius-Server

Die nötigen Policies werden auf einem Radius-Server erstellt und anschliessend per Import- und Export-Konfiguration auf den zweiten Server übertragen.

10.5.1 Zertifikate

Damit eine verschlüsselte Kommunikation zwischen Supplicant und Radius-Server möglich ist, müssen die beiden Radius-Server noch ein Zertifikat ausgestellt bekommen. In der ITR-Testumgebung ist dafür die CA da, welche auch in der Liveumgebung der HSR vorhanden ist. Dieser Schritt muss für beide Server gemacht werden.

- MMC öffnen
- Snap-in hinzufügen
  Certificates für den Computer Account: Local Computer
- Unter Personal > Rechtsklick auf Certificates > All Tasks > Request New Certificate

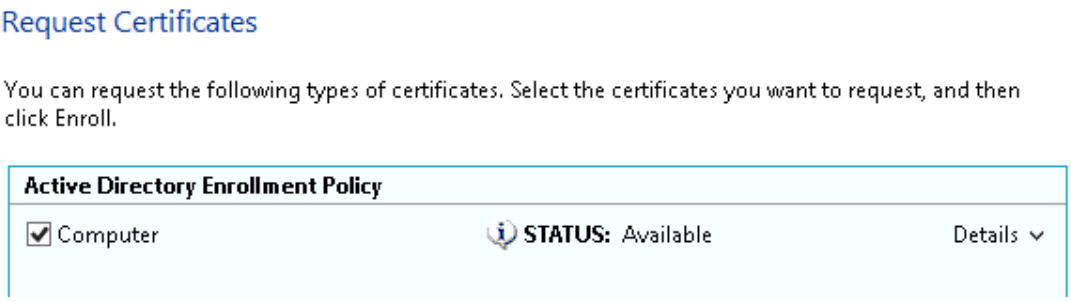


Abbildung 8: Request Certificates

- Als Verwendungszweck sollten Folgendes angegeben werden:

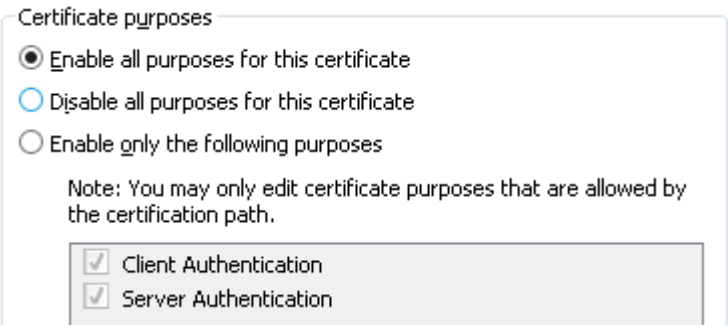


Abbildung 9: Certificate Purposes

10.5.2 Radius-Clients

- Network Policy Server MMC öffnen
- Rechtsklick Radius Clients > New
- Friendly Name: **access-switches**
  Dieser wird in der Netzwerkpolicy verwendet, um die Radius-Client-Gruppe zu identifizieren.
- Adresse: **192.168.0.0/24**
  Hier wird das Management-Netz der Switches angegeben. Nur Switches mit einer Adresse aus diesem Netz können später am Radius User und Clients authentifizieren.
- Shared secret: **MyRadiusKey**
  Derselbe Key muss auch in der Konfiguration der Switches hinterlegt sein, sonst verweigert der Radius-Server die Verbindung zum Switch.

- Unter dem Reiter Advanced > Vendor name: **Cisco**

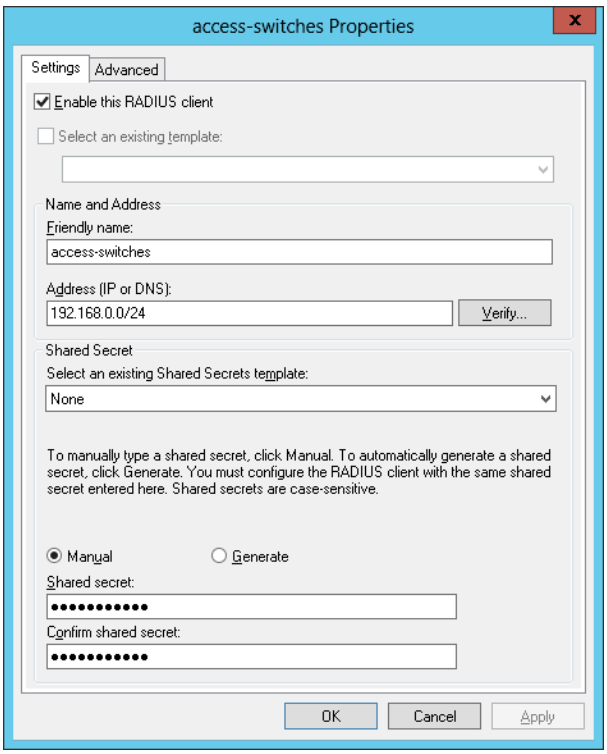


Abbildung 10: Radius Client

10.5.3 Network Policy

Nachfolgend wird die Erstellung der Network Policy für das 200 VLAN beschrieben. Weitere Policys für andere VLAN unterscheiden sich nur in dem Attribut für das VLAN und in der Auswahl der korrespondierenden Access-Gruppe. In der Testumgebung wird je eine Policy für das VLAN 200 und das VLAN 140 erstellt.

- Gruppe ITR\access.vl200 im Active Directory erstellt
- Network Policy Server MMC öffnen
- Rechtsklick Network Policies > New
- Tab: Overview
  - Name: **access.vl200 allgemeine auth**
  - Grant access. Grant access if the connection request matches this policy auswählen
  - Ignore user dial-in properties aktivieren
  - Type of network access server: **Unspecified**
- Tab: Conditions
  - Friendly name: **access-switch**
  - Windows Groups: **ITR\access.vl200**
    wählt man hier User Groups oder Client Groups trifft die Policy auch nur auf Users oder Clients zu. Wählt man Windows Groups, trifft sie auf beides zu.
- Tab: Constraints

- Unter Authentication Methods > Add

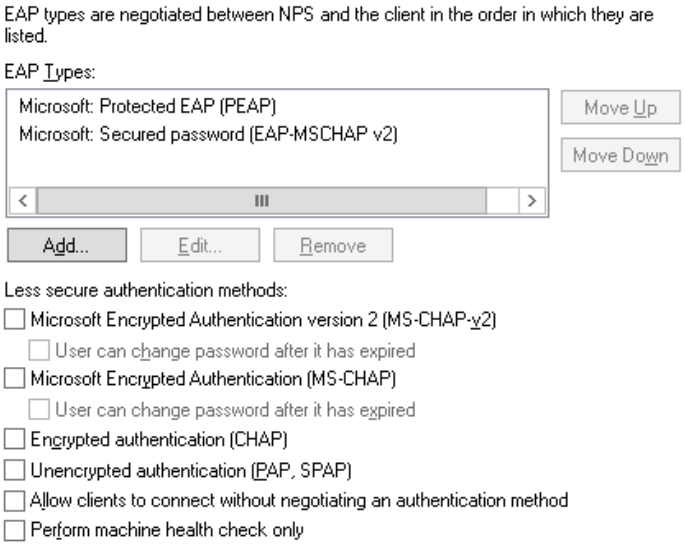


Abbildung 11: Authentication Methods 1

- Less secure authentication Methods > alle abwählen
- Protected EAP (PEAP) auswählen > Edit

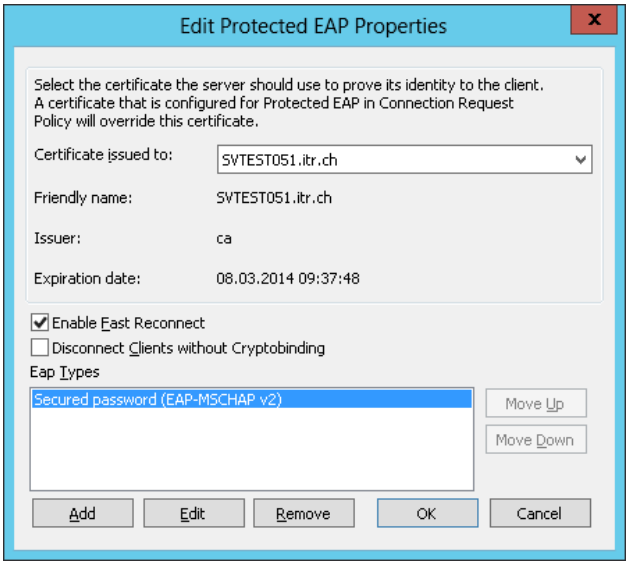


Abbildung 12: PEAP Settings

- Hier wird das Zertifikat ausgewählt, welches im Punkt „Zertifikate“ erstellt bzw. requested wurde.

- Unter Nas Port Type nur Ethernet anwählen

- Tab: Settings

- Unter Radius Attrubutes > Standard folgende Attribute eintragen

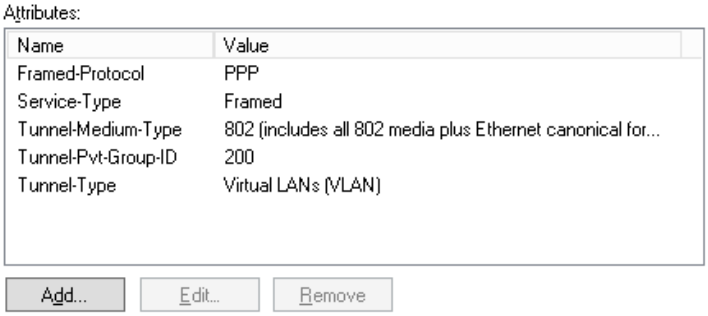


Abbildung 13: Radius Attributes

- Das Attribut Tunnel Pvt-Group-ID steht für das VLAN, in welches der Client oder der User Zugriff erhalten soll.
- Unter Routing and Remote Access > Encryption

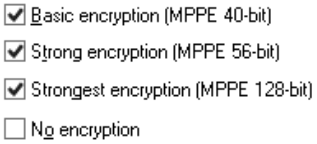


Abbildung 14: Encryption

- Es werden nur verschlüsselte Verbindungen unterstützt.

10.5.4 Switch Management Policy

Die nachfolgende Policy ist nur für das Login des Netzwerkteams da. Mit ihr können sie die Switches via ssh oder auch direkt via serielle Schnittstelle mit ihren HSR- bzw. ITR-Accounts konfigurieren.

- Gruppe APP.Radius.Network im Active Directory erstellt
- Network Policy Server MMC öffnen
- Rechtsklick Network Policies > New
- Tab: Overview
  - Name: **Switch Management**
  - Grant access. Grant access if the connection request matches this policy auswählen
  - Ignore user dial-in properties aktivieren
  - Type of network access server: **Unspecified**
- Tab: Conditions
  - Friendly name: **access-switch**
  - User Groups: **ITR\APP.Radius.Network**

    Bei dieser Policy sollen sich nur User anmelden können.
- Tab: Constraints

- Unter Authentication Methods

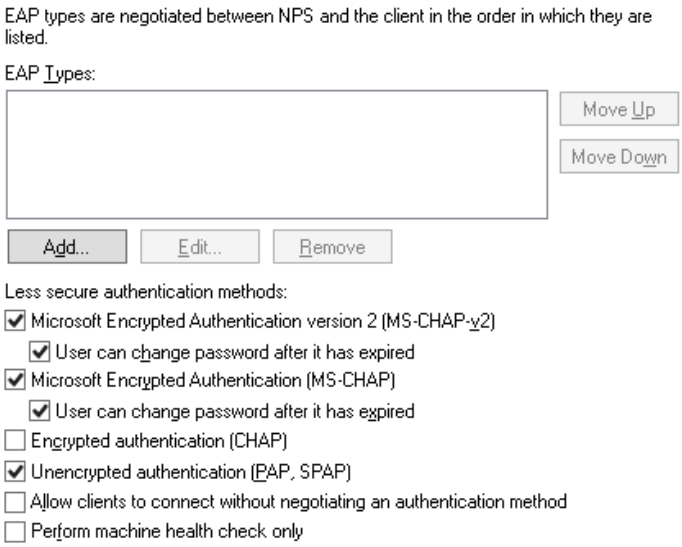


Abbildung 15: Authentication Methods 2

- Unter Nas Port Type folgendes anwählen
  - Async (Modem)
  - Virtual (VPN)
  - Common > Async (Modem)

- Tab: Settings
  - Unter Standard wird das Attribut Service-Type auf NAS Prompt gesetzt.
  - Unter den Vendor specific Attributes wird das Attribut CiscoAV-Pair gesetzt. Dieses Attribut regelt die Rechte des einzuloggenden Users auf dem Switch.

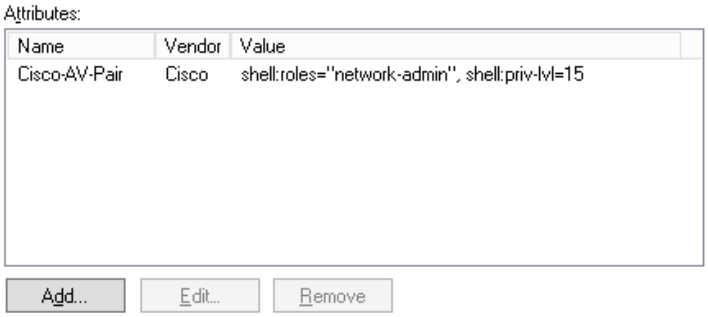


Abbildung 16: VSA Switch Management

10.6 Konfiguration Switches

Nachfolgend werden die einzelnen 802.1x-spezifischen Befehle aufgeführt und erklärt. Die Konfiguration baut auf der Standard HSR-Konfiguration auf. Die komplette Konfiguration der drei Switches befindet sich im Anhang.

10.6.1 2908g-ipamkoch

Tabelle 8: Übersicht 2908g-ipamkoch

Art	**physikalisch 2960G**
FQDN	**2908g-ipamkoch.hsr.ch**
IP-Adresse	**192.168.0.10**

In der Zeile **4–6** werden die in Zeile **21 und 22** definierten Radius-Server in die Radius-Gruppe „DOT“ gesteckt.

Zeile **8–10** sind die 802.1x-relevanten Befehle, welche alle auf die Radius-Gruppe „DOT“ zeigen. Die `Authentication` ist für die Überprüfung der Credientials. Das `Accounting` ist für Start- und Stop-Meldungen, welche an den Radius-Server gesendet werden. Und zum Schluss die `Authorization`, welche vom Radius-Server die Vendor Specific Attributes empfängt.

In der Zeile **11–16** ist das Login der Netzwerk-User noch abgebildet.

Zeile **17** sorgt dafür dass die 802.1x-Authentifikation auf dem Switch eingeschaltet wird.

In der **19** wird dem Switch mitgeteilt, über welches Interface er die Requests an den Radius-Server senden soll. Das VLAN864 ist das das Switch Management VLAN.

In der Zeile **21–23** werden dem Switch die zwei Radius-Server bekannt gemacht. Der Befehl enthält Informationen über die verwendeten Ports für das Accounting und die Authentifikation sowie den Shared Secret, welcher beim Radius Client hinterlegt wurde. In der Liveumgebung würde es sich empfehlen, einen sichereren Key zu verwenden. In der Zeile **23** werden die Vendor Specific Attributes noch eingeschaltet, mit welchen der Radius-Server z.B. die VLAN-Information überträgt.

In der Zeile **20 und 24** wird der Timeout Value gesetzt. Ist der Radius-Server für 5 Sekunden nicht erreichbar, wird er als offline betrachtet. Zusätzlich wird der retransmit-Wert auf 0 gesetzt, was bedeutet, dass der Switch die Requests nur einmal an den Radius sendet.

```
1  aaa new-model
2  !
3  !
4  aaa group server radius DOT
5   server 152.96.229.50 auth-port 1645 acct-port 1646
6   server 152.96.229.51 auth-port 1645 acct-port 1646
7  !
8  aaa authorization network default group DOT
9  aaa accounting dot1x default start-stop group DOT
10 aaa authentication dot1x default group DOT
11 aaa authentication fail-message ^CCCC Bitte nochmals versuchen... ^C
12 aaa authentication login DOT group radius local
13 aaa authentication enable default group DOT enable
14 aaa authorization console
15 aaa authorization exec DOT group radius local
```

```
16 aaa accounting exec default start-stop group DOT
17 dot1x system-auth-control
18 logging source-interface Vlan864
19 ip radius source-interface Vlan864
20 radius-server timeout 5
21 radius-server host 152.96.229.51 auth-port 1645 acct-port 1646 key MyRadiusKey
22 radius-server host 152.96.229.50 auth-port 1645 acct-port 1646 key MyRadiusKey
23 radius-server vsa send authentication
24 radius-server retransmit 0
25 interface range GigabitEthernet 0/1 - 7
26  switchport mode access
27  spanning-tree portfast
28  spanning-tree bpduguard enable
29  authentication port-control auto
30  dot1x pae authenticator
31  dot1x guest-vlan 229
32  dot1x auth-fail vlan 229
33  dot1x auth-fail max-attempts 2
34  authentication event server dead action authorize vlan 229
35  dot1x timeout tx-period 5
36 exit
```

Die Interface Konfiguration findet man in den Zeilen **25–36**, wobei die 802.1x-relevanten Befehle sich auf den Zeilen **29–35** befinden. Es wird zuerst konfiguriert, dass für den Port eine Authentifizierung notwendig ist. Danach wird noch das guest VLAN und das VLAN für zwei fehlgeschlagene Versuche definiert. Zusätzlich wird dem Interface noch angegeben, welches VLAN es autorisieren soll, wenn die Radius-Server offline sind. Der Befehl auf der Zeile **35** ist für die Dauer zwischen den Requests des Switches. Jede tx-periode dauert 5 Sekunden. Insgesammt macht der Switch 3 davon, demnach dauert es also 15 Sekunden bis der unbekannte Client im Gäste-VLAN ist.

10.6.2 2948s-ipamkoch

Tabelle 9: Übersicht 2948s-ipamkoch

Art	**physikalisch 2960S**
FQDN	**2948s-ipamkoch.hsr.ch**
IP-Adresse	**192.168.0.11**

Die Konfiguration dieses Switches unterscheidet sich eigentlich nur minimal von der des Switches 2908g-ipamkoch. Einzig die Konfiguration des Interface bezieht sich auf einen grösseren range (**Zeile 1**), da der Switch mehr Ports hat.

```
1 interface range gigabitEthernet 1/0/1 - 45
2  switchport mode access
3  spanning-tree portfast
4  spanning-tree bpduguard enable
```

```
5   authentication port-control auto
6   dot1x pae authenticator
7   dot1x guest-vlan 229
8   dot1x auth-fail vlan 229
9   dot1x auth-fail max-attempts 2
10  authentication event server dead action authorize vlan 229
11  dot1x timeout tx-period 5
    !
```

10.6.3 3524p-ipamkoch

Tabelle 10: Übersicht 3524p-ipamkoch

Art	**physikalisch 3560G**
FQDN	**3524p-ipamkoch.hsr.ch**
IP-Adresse	**192.168.0.12**

Die Konfiguration dieses Switch unterscheidet sich nur in einem Befehl von den anderen beiden Switches. In den Zeilen **11 und 12** werden noch die Power-over-Ethernet-Einstellungen vorgenommen und das Voice-VLAN konfiguriert, welches das IP-Phone benötigen wird.

```
1   interface range GigabitEthernet 0/1 - 23
2    switchport mode access
3    spanning-tree portfast
4    authentication port-control auto
5    dot1x pae authenticator
6    dot1x guest-vlan 229
7    dot1x auth-fail vlan 229
8    dot1x auth-fail max-attempts 2
9    authentication event server dead action authorize vlan 229
10   dot1x timeout tx-period 5
11   switchport voice vlan 101
12   power inline auto
13  !
```

10.7 Erstellen der Group Policy

Damit alle Clients, die sich in der Domäne befinden, nicht alle einzeln konfiguriert werden müssen, erstelle ich eine Group Policy, welche die Einstellungen am Client automatisiert vornimmt.

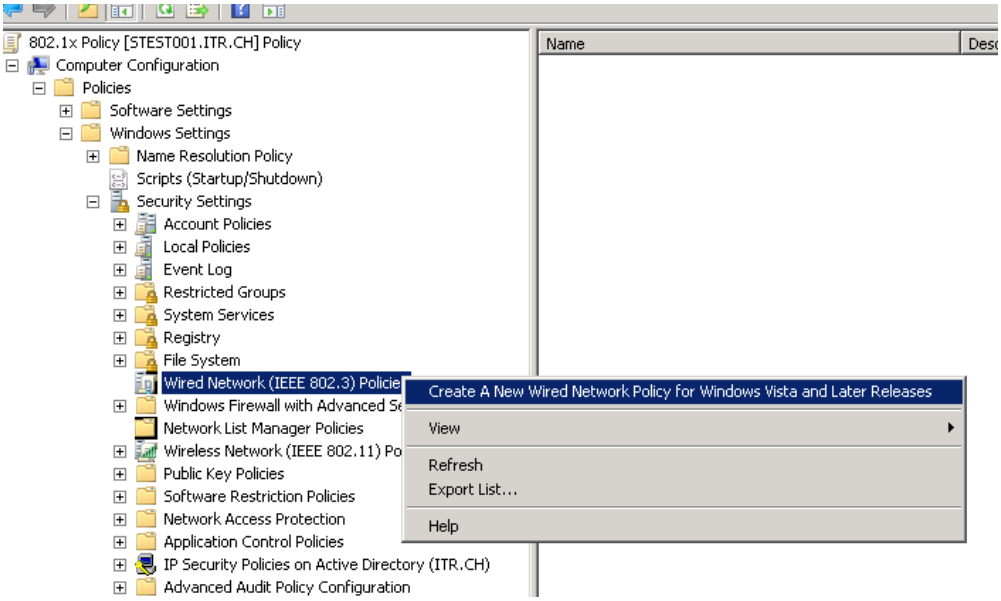


Abbildung 17: Create GPO

- Neues Group Policy Objekt erstellt
- Neue Policy > Rechtsklick > Edit
- Wie in der Abbildung 17 gezeigt, wird eine neue Wired Network Policy erstellt
- Einstellungen vornehmen wie in Abbildung 18
    - Tab: General
        - Policy Name: **Client Auth**
        - Description: **IPA mkoch**
        - Use Windows Wired Auto Config service for clients auswählen
    - Tab: Security
        - Authentication Method: **Microsoft Protected EAP (PEAP)**
        - Authentication Mode: **Computers only**
        - Max Authentication Failures: **2**
- GPO verlinken in die oberste Ebene der ITR-AD

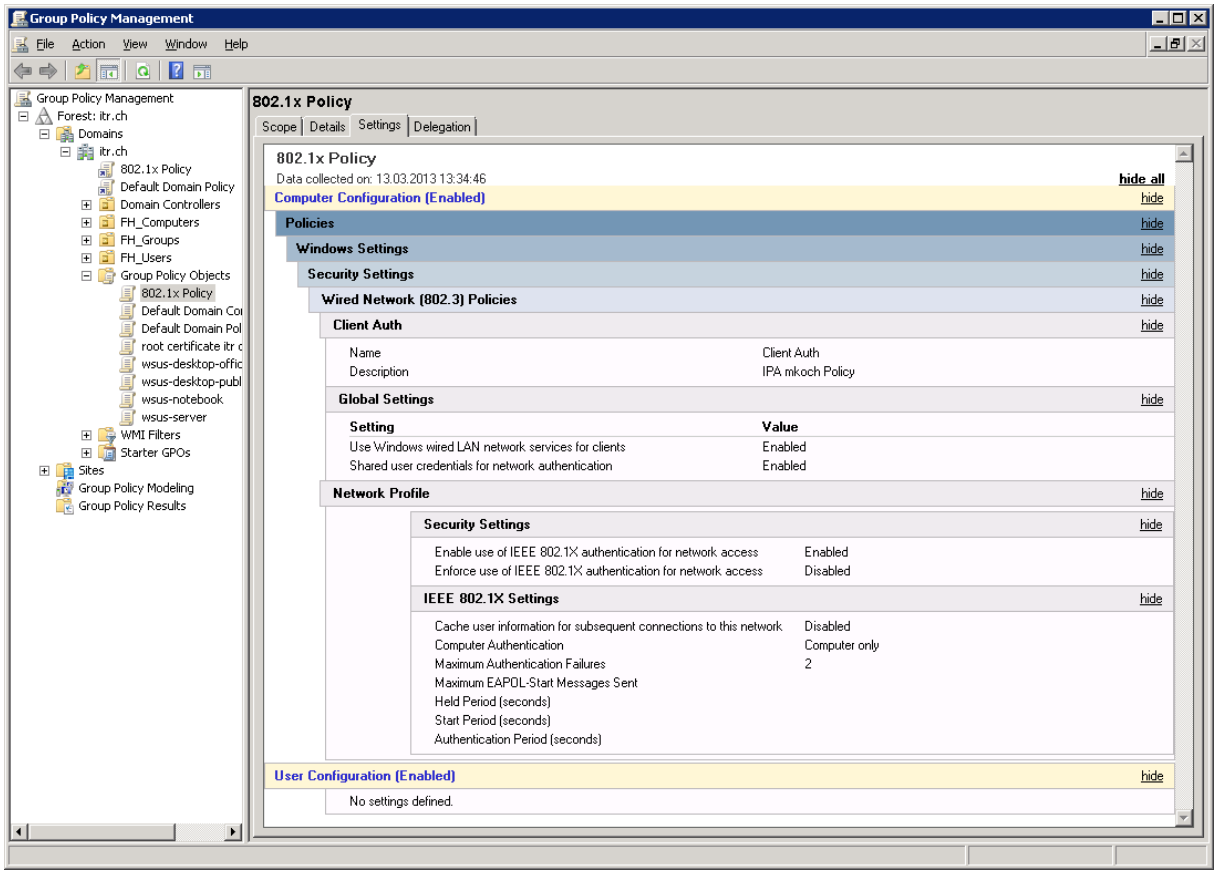


Abbildung 18: Übersicht 802.1x Policy

10.8 Benutzeranleitung

Der Zweck dieser Benutzeranleitung ist noch etwas fraglich. Denn die ITR-Clients melden sich via Client-Authentifikation an und dafür ist keine Benutzeranleitung notwendig. Die Anleitung betrifft also HSR-Angestellte, welche ihr privates Gerät an der HSR ins Netzwerk aufnehmen wollen. Laut HSR-Nutzungsvereinbarung für die Informatikmittel ist dies weder erwünscht noch erlaubt.

Die Benutzeranleitung und das Root-Zertifikat wurde mithilfe von Anton Koolens Account auf die HSR-Webseite hochgeladen. Anschliessend wurde eine Seite angelegt, welche auf die zwei Dateien verlinkt.

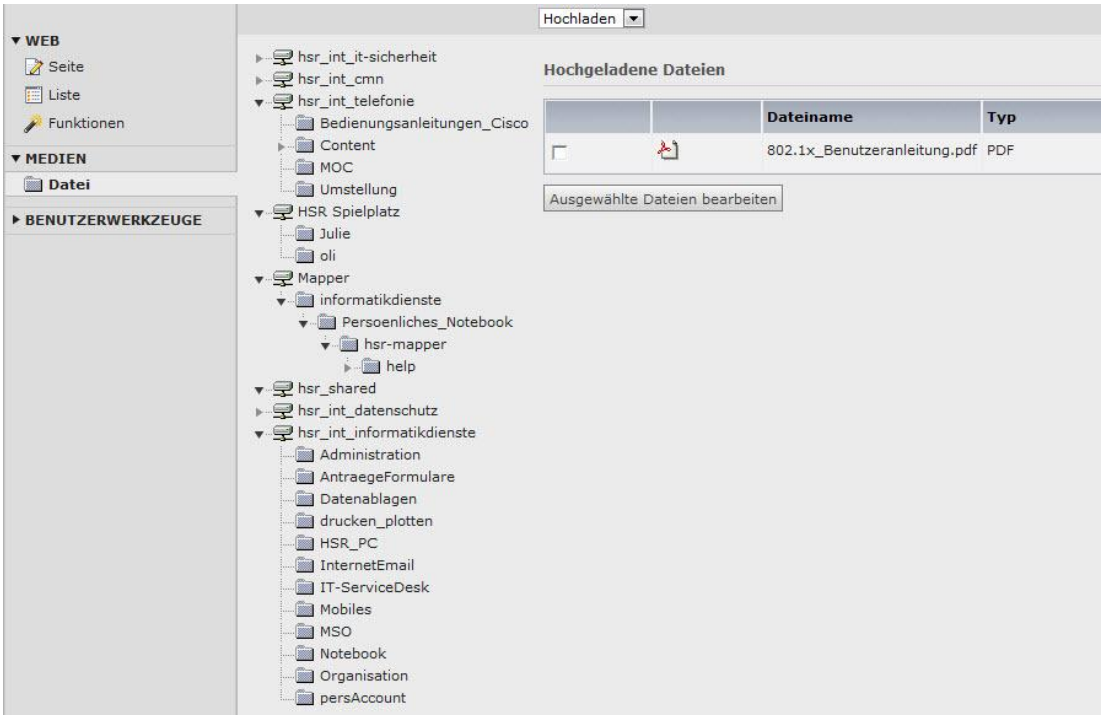


Abbildung 19: Hochladen der Benutzeranleitung

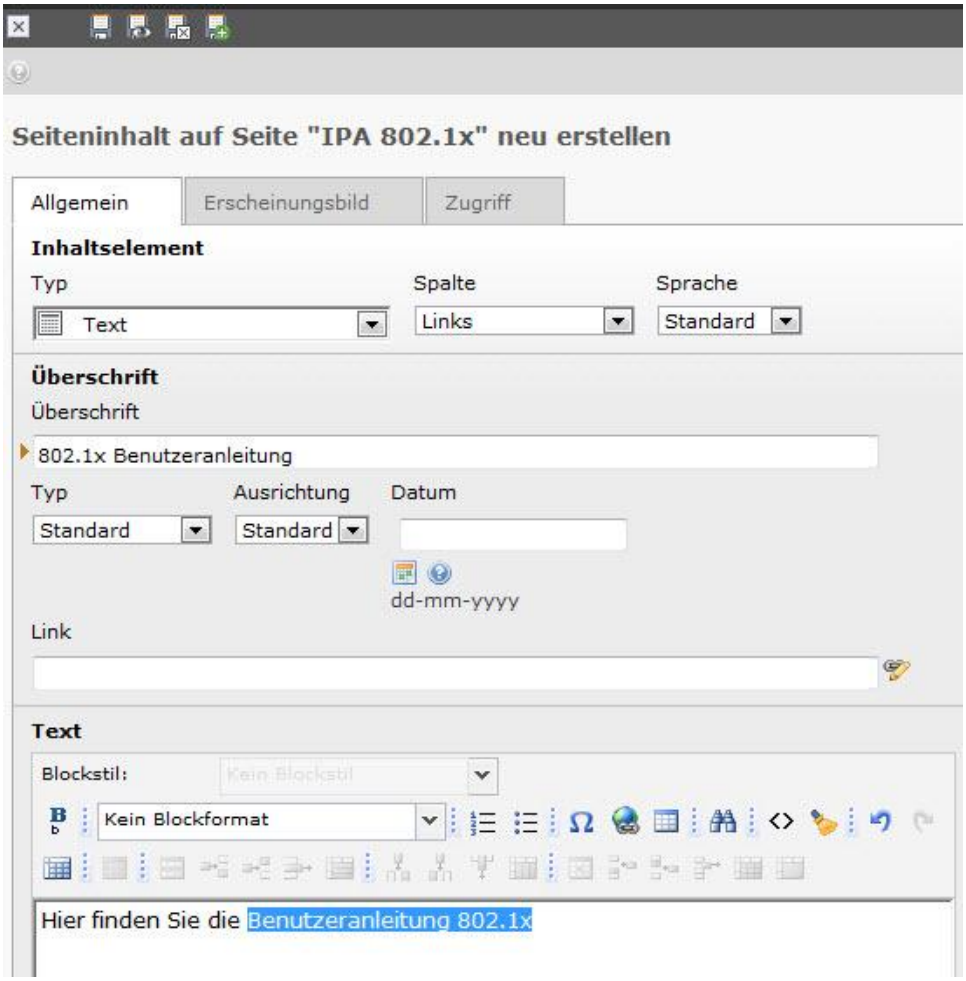


Abbildung 20: Erstellen der Seite

Verbinden via 802.1x (kabelgebunden)

Inhaltsverzeichnis

Informationen zu 802.1x **49**
Betriebssysteme **50**
Windows 7 50

Revisionen

Datum	Version	Changelog
13.03.2013	1.0	Initialrevision

Informationen zu 802.1x

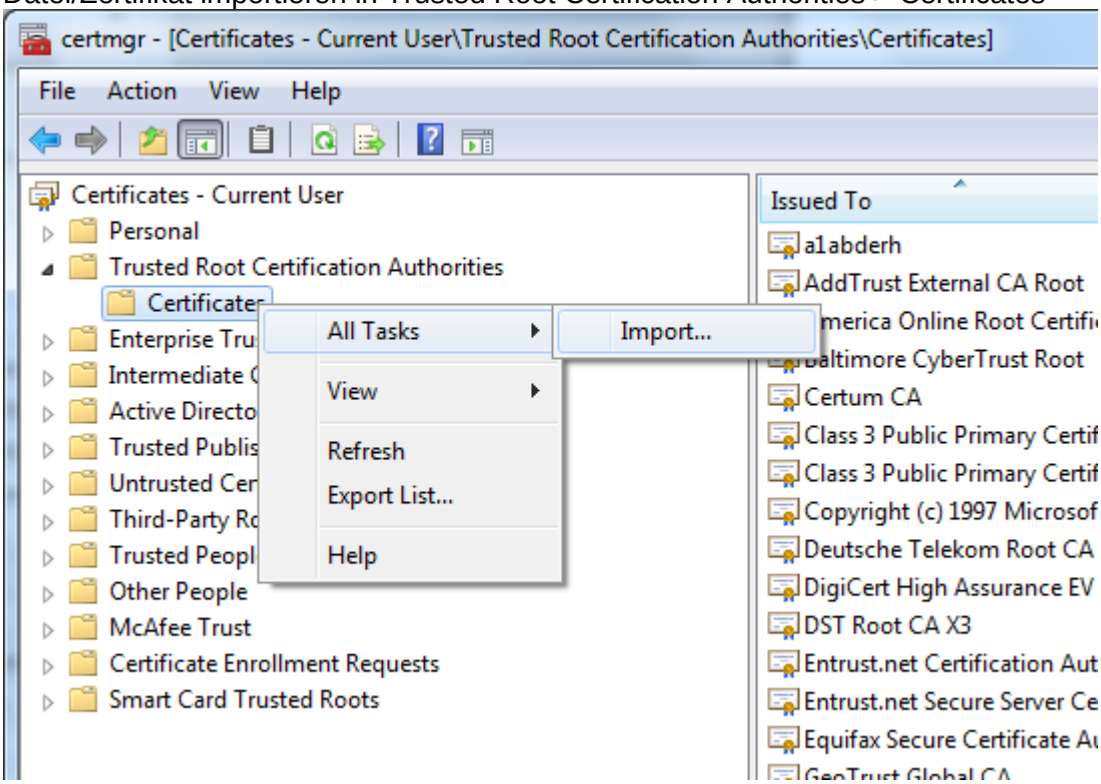
802.1x ist eine Technologie, die es erlaubt, eine kabelgebundene Authentifikation am HSR-Netzwerk vorzunehmen. Somit können unberechtigte Zugriffe auf das HSR-Netzwerk verhindert werden.
Wenn Sie diese Anleitung schrittweise befolgen, ermöglicht das Ihrem Computer, an dem Authentifizierungs-Prozess teilzunehmen. Das bringt für Sie den Vorteil, dass Sie nicht mehr wissen müssen, an welchem Port Sie Ihr Laptop einstecken dürfen. Der Port verwandelt sich nach erfolgreicher Authentifikation in einen Anschluss in Ihr „Heimnetz“.
Sollte die Authentifizierung nicht erfolgreich ablaufen, werden Sie in ein Gäste-Netz eingeteilt, in dem nur der Internetanschluss gewährleistet ist und keine lokalen HSR-Dienste wie z.B. das Drucksystem oder die Dateiablagen zur Verfügung stehen. Dieses Dokument richtet sich nicht an Benutzer, welche ihr privates Gerät verwenden. Bei den persönlichen Geräten erfolgt die Authentifikation automatisch.

Betriebssysteme

Windows 7

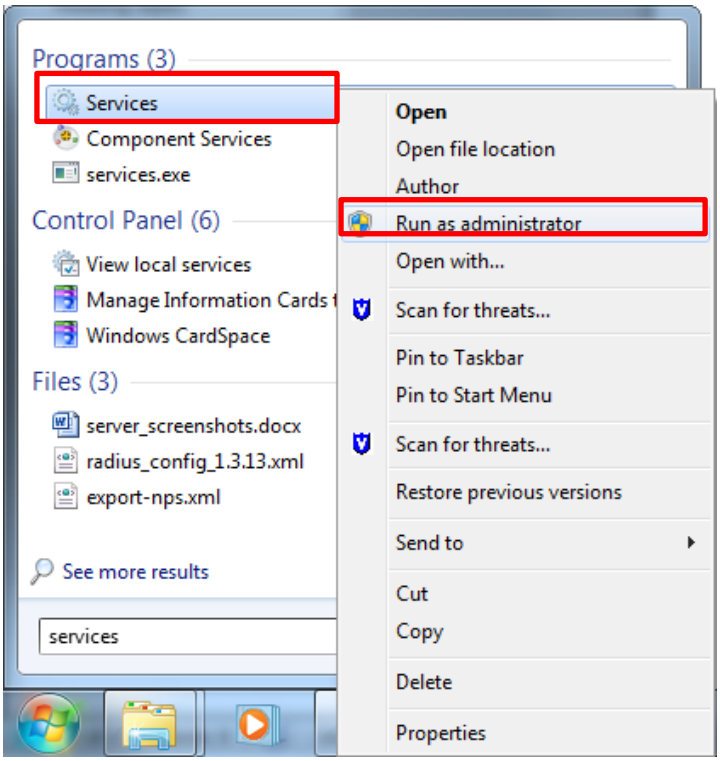
Schritt 1

- Datei/Zertifikat herunterladen von hier
- Windows-Taste
- certmgr.msc eingeben und öffnen
  Datei/Zertifikat importieren in Trusted Root Certification Authorities > Certificates



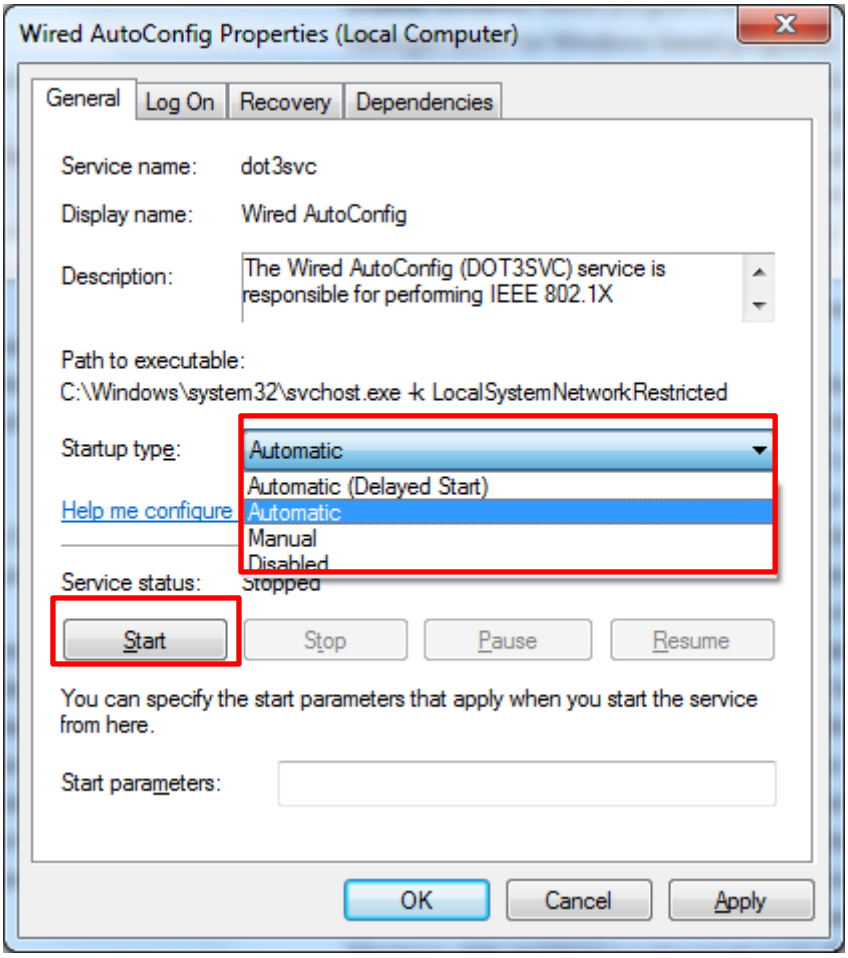
Schritt 2

- Services öffnen



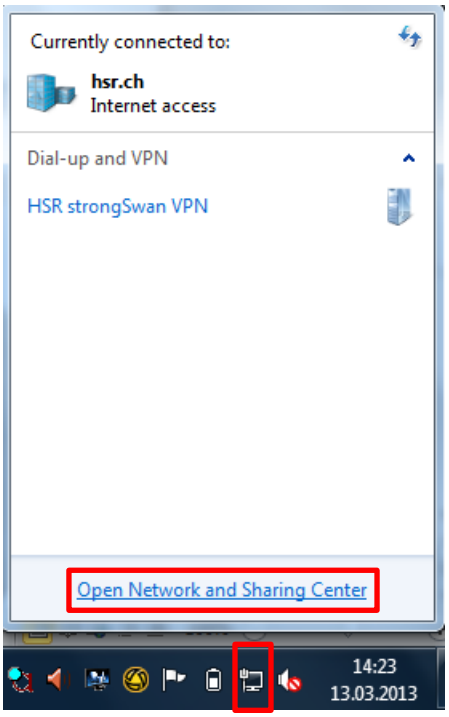
Schritt 3

- Service Wired AutoConfig anwählen > Rechtsklick > Properties
- Startup type auf Automatic stellen und dann den Service mit dem Button „Start“ starten



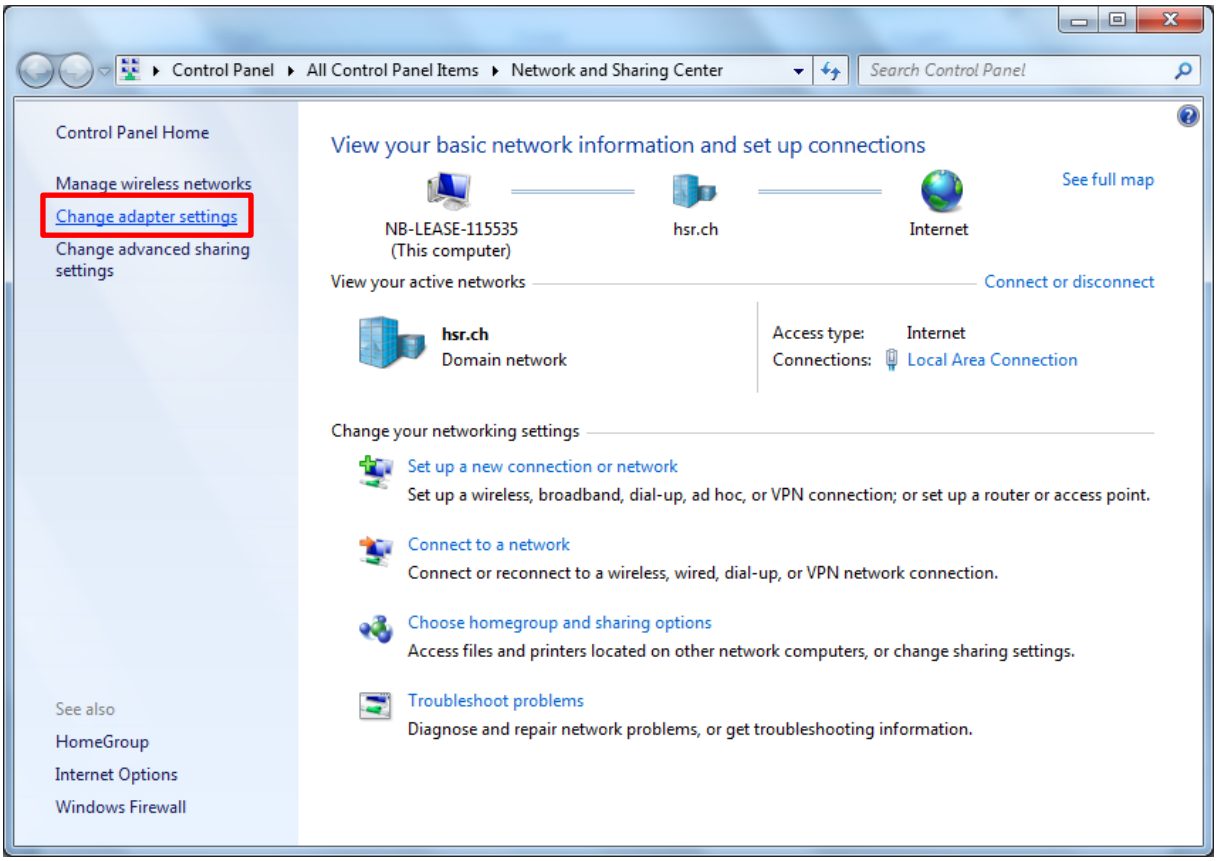
Schritt 4

- Open Network and Sharing Center



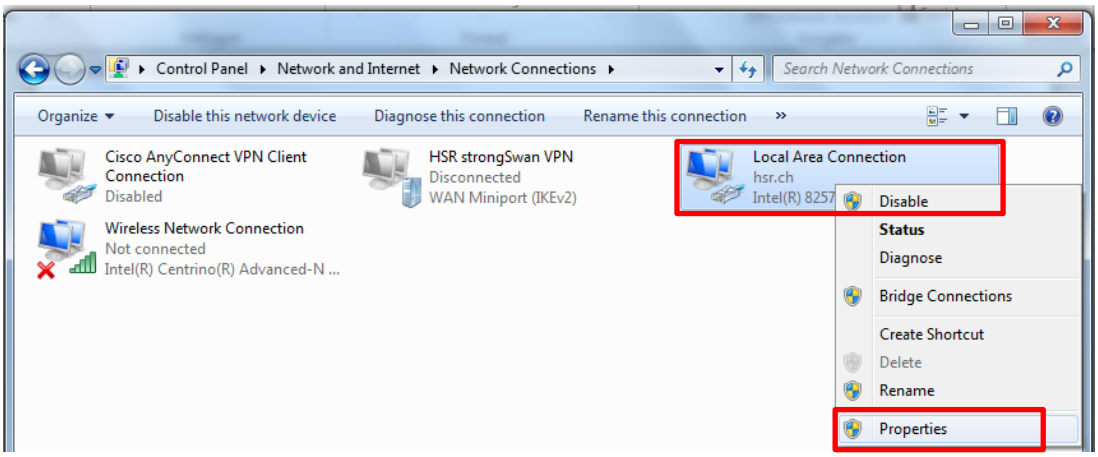
Schritt 4

- Change adapter settings öffnen



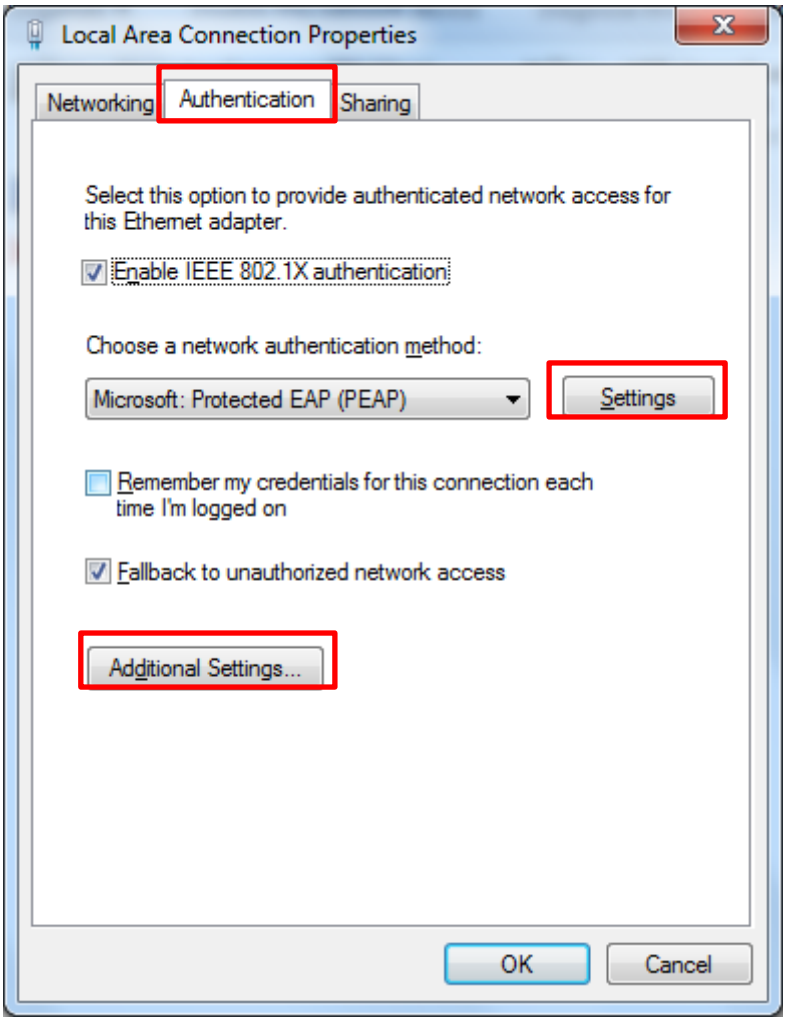
Schritt 5

- Rechtsklick auf den Adapter Local Area Connection > Properties



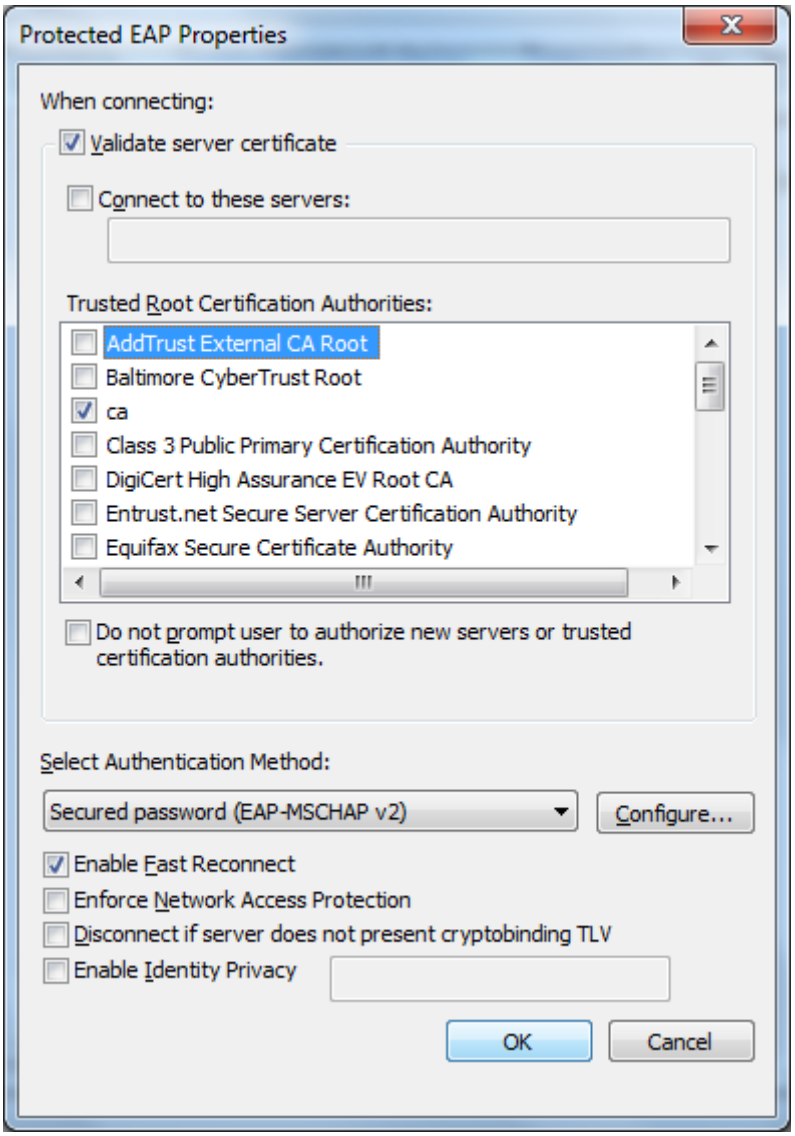
Schritt 6

- In den Tab Authentication wechseln
  - Enable IEEE 802.1X authentication aktivieren
  - Microsoft: Protected EAP (PEAP) auswählen
- auf den Button „Settings" klicken



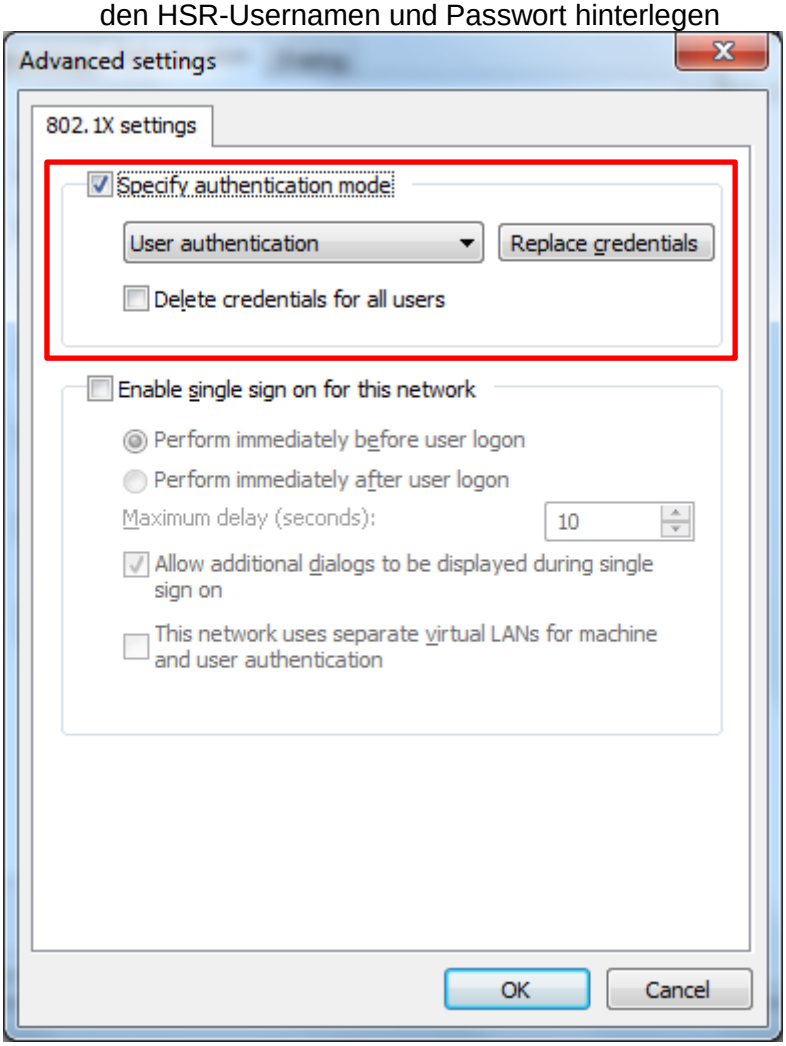
Schritt 7

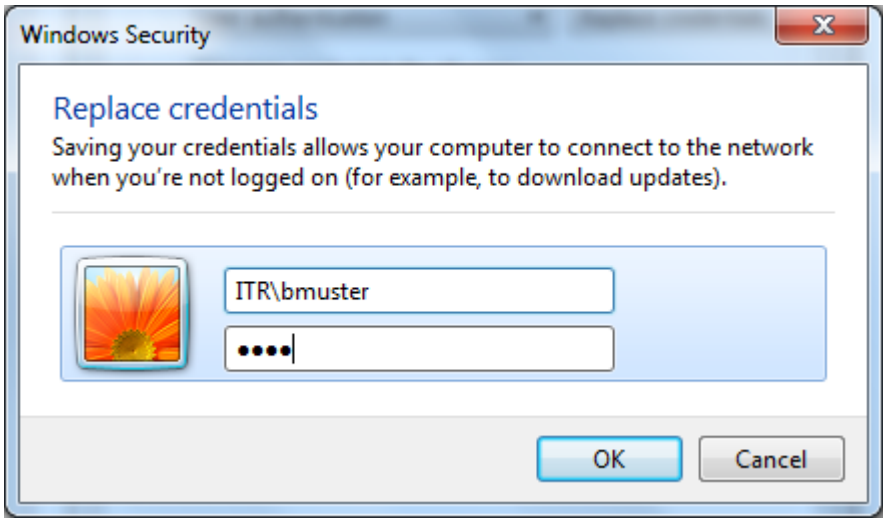
- Validate server certificate aktivieren
- Select Authentication Method auf MSCHAPv2 stellen
- Enable Fast Reconnect aktivieren
- Mit OK das Fenster wieder schliessen
- auf den Button „Aditional Settings“ klicken



Schritt 8

- User authentication auswählen
- Mit dem Button „Save credentials“ oder auch „Replace credentials“ den HSR-Usernamen und Passwort hinterlegen





11 Kontrollieren

11.1 Testprotokoll

11.1.1 Windows-7-authentifizierte Clients

Anschliessend folgen acht Tests, welche die Funktionalität der ITR-Clients, welche in der Liveumgebung die HSR-Clients darstellen würden, testen. Behandelt werden verschiedene Szenarien jeweils hinter einem bereits gestarteten IP-Phone und hinter einem IP-Phone, das gerade startet.

Nr.	1.1		
Datum	14.03.13	**Client**	nb-lease-114366
Verwendete Applikation	Wireshark	**Verwendetes Betriebssystem**	Windows 7
Ablauf des Tests			
• Der ITR-Client ist bereits gestartet. • Ein Test-User ist angemeldet. • Der Client wird direkt an einem 802.1x-Port eingesteckt.			
Erwartetes Ergebnis			
Der Client erhält das VLAN 200, weil er sich in jener Access-Gruppe befindet.			
Tatsächliches Ergebnis			
Der Client war wie erwartet sofort authentifiziert. Der CDP-Nachricht des Switches konnte ich entnehmen, dass der Port nun im VLAN 200 ist. DHCP hat auch funktioniert, der Client erhielt seine zugewiesene IP.			
Anmerkungen, Abweichungen, Verbesserungsvorschläge			

Nr.	1.2		
Datum	14.03.13	**Client**	nb-lease-114366
Verwendete Applikation	Wireshark	**Verwendetes Betriebssystem**	Windows 7
Ablauf des Tests			
• Der ITR-Client ist bereits gestartet. • Ein Test-User ist angemeldet. • Der Client wird an einem 802.1x-Port hinter einem bereits laufenden IP-Phone eingesteckt.			
Erwartetes Ergebnis			
Der Client erhält das VLAN 200, weil er sich in jener Access-Gruppe befindet.			
Tatsächliches Ergebnis			
Der Client war wie erwartet sofort authentifiziert. Der CDP-Nachricht des Switches konnte ich entnehmen, dass der Port nun im VLAN 200 ist. DHCP hat auch funktioniert, der Client erhielt seine zugewiesene IP.			
Anmerkungen, Abweichungen, Verbesserungsvorschläge			

Nr.	1.3		
Datum	14.03.13	**Client**	nb-lease-114366
Verwendete Applikation	Wireshark	**Verwendetes Betriebssystem**	Windows 7
Ablauf des Tests			
• Der ITR-Client ist bereits gestartet. • Ein Test-User ist angemeldet. • Der Client wird an einem 802.1x-Port hinter einem IP-Phone eingesteckt, welches dann startet.			
Erwartetes Ergebnis			
Der Client erhält das VLAN 200, weil er sich in jener Access-Gruppe befindet.			
Tatsächliches Ergebnis			
Der Client sendete in der Zeit, in der das IP-Phone startete, ein paar EAPOL-Nachrichten, um die Authentifikation zu starten. Als das IP-Phone dann bereit war und den Client mit dem Switch verbinden konnte, konnte die Authentifizierung erfolgreich fortgesetzt werden. DHCP hat auch funktioniert, der Client erhielt seine zugewiesene IP.			
Anmerkungen, Abweichungen, Verbesserungsvorschläge			

Nr.	1.4		
Datum	14.03.13	**Client**	nb-lease-114366
Verwendete Applikation	Wireshark	**Verwendetes Betriebssystem**	Windows 7
Ablauf des Tests			
• Der Client wird an direkt einem 802.1x-Port eingesteckt mit bereits laufendem IP-Phone. • Der ITR-Client wird gestartet. • Anschliessend meldet sich der Test-User, der sich noch nie am Gerät angemeldet hatte.			
Erwartetes Ergebnis			
Der Client erhält das VLAN 200, weil er sich in jener Access-Gruppe befindet. Das Login funktioniert.			
Tatsächliches Ergebnis			
Der Client war wie erwartet sofort authentifiziert, bevor der User sich anmelden konnte. Der CDP-Nachricht des Switches konnte ich entnehmen, dass der Port nun im VLAN 200 ist. DHCP hat auch funktioniert, der Client erhielt seine zugewiesene IP.			
Anmerkungen, Abweichungen, Verbesserungsvorschläge			

Nr.	1.5		
Datum	14.03.13	**Client**	nb-lease-114366
Verwendete Applikation	Wireshark	**Verwendetes Betriebssystem**	Windows 7
Ablauf des Tests			
• Der Client wird an einem 802.1x-Port eingesteckt hinter einem IP-Phone, welches dann startet. • Der ITR-Client wird gestartet. • Anschliessend meldet sich der Test-User, der sich noch nie am Gerät angemeldet hatte.			
Erwartetes Ergebnis			
Der Client erhält das VLAN 200, weil er sich in jener Access-Gruppe befindet. Das Login funktioniert.			
Tatsächliches Ergebnis			
Als das IP-Phone gestartet war und den Client mit dem Switch verbinden konnte, konnte die Authentifizierung erfolgreich fortgesetzt werden. Der Client war authentifiziert, bevor der User sich anmelden konnte. DHCP hat auch funktioniert, der Client erhielt seine zugewiesene IP.			
Anmerkungen, Abweichungen, Verbesserungsvorschläge			

Nr.	1.6		
Datum	14.03.13	**Client**	nb-lease-114366
Verwendete Applikation	Wireshark	**Verwendetes Betriebssystem**	Windows 7
Ablauf des Tests			
• Der ITR-Client ist bereits gestartet, und ein Test-User ist angemeldet, aber gesperrt. • Der Client wird direkt an einem 802.1x-Port eingesteckt. • Anschliessend entsperrt der Test-User das Gerät			
Erwartetes Ergebnis			
Der Client erhält das VLAN 200, weil er sich in jener Access-Gruppe befindet. Das Entsperren funktioniert.			
Tatsächliches Ergebnis			
Der Client war sofort authentifiziert. Der User konnte das Gerät entsperren. DHCP hat auch funktioniert, der Client erhielt seine zugewiesene IP.			
Anmerkungen, Abweichungen, Verbesserungsvorschläge			

Nr.	1.7		
Datum	14.03.13	**Client**	nb-lease-114366
Verwendete Applikation	Wireshark	**Verwendetes Betriebssystem**	Windows 7
Ablauf des Tests			
• Der ITR-Client ist bereits gestartet, und ein Test-User ist angemeldet, aber gesperrt. • Der Client wird an einem 802.1x-Port eingesteckt hinter einem IP-Phone, welches bereits gestartet ist. • Anschliessend entsperrt der Test-User das Gerät.			
Erwartetes Ergebnis			
Der Client erhält das VLAN 200, weil er sich in jener Access-Gruppe befindet. Das Entsperren funktioniert.			
Tatsächliches Ergebnis			
Der Client war sofort authentifiziert. Der User konnte das Gerät entsperren. DHCP hat auch funktioniert, der Client erhielt seine zugewiesene IP.			
Anmerkungen, Abweichungen, Verbesserungsvorschläge			

Nr.	1.8		
Datum	14.03.13	**Client**	nb-lease-114366
Verwendete Applikation	Wireshark	**Verwendetes Betriebssystem**	Windows 7
Ablauf des Tests			
• Der ITR-Client ist bereits gestartet, und ein Test-User ist angemeldet, aber gesperrt. • Der Client wird an einem 802.1x-Port eingesteckt hinter einem IP-Phone, welches daraufhin startet. • Anschliessend entsperrt der Test-User das Gerät.			
Erwartetes Ergebnis			
Der Client erhält das VLAN 200, weil er sich in jener Access-Gruppe befindet. Das Entsperren funktioniert.			
Tatsächliches Ergebnis			
Der Client war nach dem Start des IP-Phones authentifiziert. Der User konnte das Gerät entsperren. DHCP hat auch funktioniert, der Client erhielt seine zugewiesene IP.			
Anmerkungen, Abweichungen, Verbesserungsvorschläge			

11.1.2 Windows-7-nicht-authentifizierte Clients

Nr.	2.1		
Datum	15.03.13	**Client**	nb-lease-115535
Verwendete Applikation	Wireshark	**Verwendetes Betriebssystem**	Windows 7
Ablauf des Tests			
• Ein Client, welcher keine 802.1x-Authentifizierung unterstützt, wird angeschlossen.			
Erwartetes Ergebnis			
Der Client erhält das Gäste VLAN 229.			
Tatsächliches Ergebnis			
Der Switch forderte den Client dreimal auf, insgesamt 15 Sekunden, sich zu authentifizieren. Als der Client nicht darauf reagierte, verschob er ihn in das Gäste-VLAN.			
Anmerkungen, Abweichungen, Verbesserungsvorschläge			

Nr.	2.2		
Datum	15.03.13	**Client**	nb-lease-115535
Verwendete Applikation	Wireshark	**Verwendetes Betriebssystem**	Windows 7
Ablauf des Tests			
• Der Client authentifiziert sich mit falschem Username oder Passwort.			
Erwartetes Ergebnis			
Der Client erhält das Gäste VLAN 229.			
Tatsächliches Ergebnis			
Der Client versucht, sich zweimal mit den falschen Credentials anzumelden, wird aber anschliessend ins Gäste-VLAN verschoben.			
Anmerkungen, Abweichungen, Verbesserungsvorschläge			

11.1.3 Switches

Nr.	3.1		
Datum	15.03.13		
Verwendete Applikation	Putty / Wireshark	**Verwendetes Betriebssystem**	IOS
Ablauf des Tests			
• Beide Radius-Server werden vom Netz genommen.			
Erwartetes Ergebnis			
Alle Clients erhalten das Gäste-VLAN (ITR und unbekannte Clients).			
Tatsächliches Ergebnis			
Der Switch probiert zwar noch kurz, mit dem Radius zu kommunizieren, aber nach 10 Sekunden werden die Clients alle ins Gäste-VLAN verschoben.			
Anmerkungen, Abweichungen, Verbesserungsvorschläge			

Nr.	3.2		
Datum	15.03.13		
Verwendete Applikation	Wireshark / Putty	**Verwendetes Betriebssystem**	IOS
Ablauf des Tests			
• Einer der beiden Radius-Server wird vom Netz genommen.			
Erwartetes Ergebnis			
Der Switch sendet die Anfragen nun zum anderen Radius-Server.			
Tatsächliches Ergebnis			
Der Switch bemerkt, dass der eine Radius-Server offline ist, und verwendet von da an den anderen.			
Anmerkungen, Abweichungen, Verbesserungsvorschläge			

11.1.4 Radius

Nr.	4.1		
Datum	15.03.13		
Verwendete Applikation	Event Viewer	**Verwendetes Betriebssystem**	Windows Server

Ablauf des Tests

- Eine erfolgreiche Authentifizierung wird gemacht.

Erwartetes Ergebnis

Der Radius-Server loggt den erfolgreichen Versuch.

Tatsächliches Ergebnis

Network Policy Server granted full access to a user because the host met the defined health policy.

User:
Security ID: ITR\NB-LEASE-114366$
Account Name: host/NB-LEASE-114366.itr.ch
Account Domain: ITR
Fully Qualified Account Name: ITR\NB-LEASE-114366$

Client Machine:
Security ID: NULL SID
Account Name: -
Fully Qualified Account Name: -
OS-Version: -
Called Station Identifier: B4-A4-E3-46-D8-27
Calling Station Identifier: B0-99-28-CC-62-4E

NAS:
NAS IPv4 Address: 192.168.0.11
NAS IPv6 Address: -
NAS Identifier: -
NAS Port-Type: Ethernet
NAS Port: 50139

RADIUS Client:
Client Friendly Name: access-switches
Client IP Address: 192.168.0.11

Authentication Details:
Connection Request Policy Name: Use Windows authentication for all users
Network Policy Name: access.vl200 allgemeine auth
Authentication Provider: Windows
Authentication Server: SVTEST051.itr.ch
Authentication Type: PEAP
EAP Type: Microsoft: Secured password (EAP-MSCHAP v2)
Account Session Identifier: -

Quarantine Information:
Result: Full Access
Extended-Result: -
Session Identifier: -
Help URL: -
System Health Validator Result(s): -

Anmerkungen, Abweichungen, Verbesserungsvorschläge

Network Policy Server granted full access to a user because the host met the defined health policy.

Nr.	4.2		
Datum	15.03.13		
Verwendete Applikation	Event Viewer	**Verwendetes Betriebssystem**	Windows Server

Ablauf des Tests

- Eine erfolglose Authentifizierung wird durchgeführt.

Erwartetes Ergebnis

Der Radius-Server loggt den erfolglosen Versuch.

Tatsächliches Ergebnis

Network Policy Server denied access to a user.

Contact the Network Policy Server administrator for more information.

User:
Security ID: ITR\pmuster
Account Name: ITR\pmuster
Account Domain: ITR
Fully Qualified Account Name: ITR\pmuster

Client Machine:
Security ID: NULL SID
Account Name: -
Fully Qualified Account Name: -
OS-Version: -
Called Station Identifier: -
Calling Station Identifier: async

NAS:
NAS IPv4 Address: 192.168.0.10
NAS IPv6 Address: -
NAS Identifier: -
NAS Port-Type: Async
NAS Port: 0

RADIUS Client:
Client Friendly Name: access-switches
Client IP Address: 192.168.0.10

Authentication Details:
Connection Request Policy Name: Use Windows authentication for all users
Network Policy Name: -
Authentication Provider: Windows
Authentication Server: SVTEST051.itr.ch
Authentication Type: PAP
EAP Type: -
Account Session Identifier: -
Logging Results: Accounting information was written to the local log file.
Reason Code: 16
Reason: Authentication failed due to a user credentials mismatch. Either the user name provided does not map to an existing user account or the password was incorrect.

Anmerkungen, Abweichungen, Verbesserungsvorschläge

Authentication failed due to a user credentials mismatch. Either the user name provided does not map to an existing user account or the password was incorrect.

11.1.5 Benutzeranleitung

Nr.	5.1		
Datum	15.03.13		
Verwendete Applikation	-	**Verwendetes Betriebssystem**	Windows 7
Ablauf des Tests			
• Die Anleitung wird im Internet Explorer heruntergeladen.			
Erwartetes Ergebnis			
Das PDF ist anschliessend in lesbarer Form auf der lokalen Festplatte.			
Tatsächliches Ergebnis			
PDF liess sich herunterladen und öffnen.			
Anmerkungen, Abweichungen, Verbesserungsvorschläge			

12 Auswertung

12.1 technisches Fazit

Die gewählte Lösung funktioniert und ist auch anwendbar auf die Einsatzgebiete der HSR. Sobald der Aufsetzt-Prozess der Clients auch 802.1x-Ready ist, können noch mehr Gebiete, wie die Übungsräume der Studenten umgestellt werden. Was die Migration der Radius-Server in der Live-Umgebung auf Windows Server 2012 betrifft, wurde in dieser Dokumentation und mit dem Testaufbau bewiesen, dass sogar der Parallelbetrieb möglich ist, somit die Migration keine Probleme bereiten sollte.
In Zukunft wäre es noch empfehlenswert als Zertifikat für die beiden Radius-Server ein öffentlich vertrautes Zertifikat zu verwenden, wie es auch im WLAN der HSR zum Einsatz kommt. Damit würde der Schritt mit dem Importieren des Root-Zertifikats wegfallen.

12.2 Übergang zum Betrieb

In den Wireless Netzwerken der HSR ist 802.1x-Authentifiaktion bereits umgesetzt. Der grosse Unterschied zwischen kabelgebundenen Netzwerken zu drahtlosen Netzwerken im Bezug auf 802.1x ist, dass man beim kabelgebundenen Netzwerk nicht sieht was man erhält. In der Wireless Netzwerken kann man an der SSID ablesen, um welches Netzwerk es sich handelt. Hier stehen z.B. HSR-WLAN und HSR-Secure zur Verfügung. Einem 802.1x aktivierten Port sieht man dies nicht an und muss durch Einstecken erst probieren was passiert. Aus diesem Grund und weil 802.1x nicht überall an der HSR zum Einsatz kommen wird, müssen die Ports in irgendeiner Weise angeschrieben werden, so dass dies der User sofort erkennt.
Für den Übergang arbeiten Client-Management und IT-Netzwerk zusammen. Zuerst wird die Policy in

den gewünschten Bereichen (mobile Geräte) aktiviert und erst anschliessend werden die einzelnen Ports von der statischen VLAN-Zuweisung gewechselt zu einem 802.1x-Port. Damit kann sichergestellt werden, dass die Clients das Policy Update erhalten bevor der Port umgestellt ist.

12.3 persönliches Fazit

Es hat mir grossen Spass bereitet dieses Projekt von Anfang an umzusetzen. Es ist essentiell, dass sich die HSR allgemeinen Sicherheitsstandards annimmt und probiert sie zu implementieren. Nach der Realisierung dieses Projekts ist die HSR wieder ein bisschen sicherer worden. Zudem lässt sich in Zukunft die Nutzung des Netzwerks mit der neuen Authentifikation genauer auswerten.
Schön finde ich auch, dass die neue Technik auch einiges an Aufwand einsparen kann, da die Netzwerk-Ports universaler in der Nutzung werden. Und die Lösung mit der Client-Authentifikation läuft sehr transparent ab, dass heisst die Benutzer merken kaum etwas von der Änderung. Was sicherlich nicht der Fall gewesen wäre wenn sich die Benutzer am Netzwerk anmelden hätten müssen. Deshalb besteht der Übergang zu der 802.1x-Authentifiaktion nur aus einer Group Policy und nicht aus einer grossen Benutzeranleitung. Während der Dauer des Projektes sind wenige Probleme aufgetreten, was dafür spricht, dass die Technik doch ausgereifter ist als noch vor ein paar Jahren.
Ausserdem half mir die Organisationsmethode IPERKA sehr einen sauberen Ablauf in die Planung und die Realisierung zu bringen und im vorgegebenen Zeitrahmen fertig zu werden. Die definierten Meilensteine halfen dabei eine klare Trennung zwischen die einzelnen IPERKA-Schritte zu bringen und jede Phase des Projekts sauber abzuschliessen.

13 Glossar

Begriff	Beschreibung
RADIUS	Remote Authentication Dial In User Service
AAA-Server	Authentication, Authorization und Accounting Server Anbieter eines Authentifizierung- und Log-Dienstes
Authenticator	Switch der die Authentifikations-Anfragen an den AAA Sever weiterleitet.
Supplicant	Bezieher eines Authentifikation-Dienstes
EAPOL	Extensible Authentication Protocol Over Lan
PEAP	Protected Extensible Authentication Protocol
MSCHAPv2	Microsoft Challenge-Handshake Authentication Protocol Protokoll für den Austausch und Überprüfung der Credentials
VLAN	Virtual Local Area Network
Credentials	Username & Passwort

14 Abbildungsverzeichnis

Abbildung 1: Phasen IPERKA 11
Abbildung 2: EAP-Ablauf 21
Abbildung 3: Allgemeiner Aufbau 25
Abbildung 4: Netzplan 33
Abbildung 5: Auswahl des Betriebssystems 35
Abbildung 6: Auswahl der Rollen Server 2008 35
Abbildung 7: Auswahl der Rollen Server 2012 36
Abbildung 8: Request Certificates 36
Abbildung 9: Certificate Purposes 37
Abbildung 10: Radius Client 38
Abbildung 11: Authentication Methods 1 39
Abbildung 12: PEAP Settings 39
Abbildung 13: Radius Attributes 40
Abbildung 14: Encryption 40
Abbildung 15: Authentication Methods 2 41
Abbildung 16: VSA Switch Management 41
Abbildung 17: Create GPO 45
Abbildung 18: Übersicht 802.1x Policy 46
Abbildung 19: Hochladen der Benutzeranleitung 47
Abbildung 20: Erstellen der Seite 48

15 Tabellenverzeichnis

Tabelle 1: Versionsübersicht 7
Tabelle 2 involvierte Personen 12
Tabelle 3: Client- und User-Authentifikation 26
Tabelle 4: Firewall-Regeln 34
Tabelle 5: Client Übersicht 34
Tabelle 6: Übersicht svtest050 34
Tabelle 7: Übersicht svtest051 35

Tabelle 8: Übersicht 2908g-ipamkoch 42

Tabelle 9: Übersicht 2948s-ipamkoch 43

Tabelle 10: Übersicht 3524p-ipamkoch 44

16 Quellenverzeichnis

- Windows Server Radius
  Typ: PDF
  Abrufdatum: 06.03.13
  http://technet.microsoft.com/en-us/library/cc755248.aspx
- 2960G 12.2(53)SE2 Command Reference
  Typ: PDF
  Abrufdatum: 06.03.13
  http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_53_se/command/reference/2960cr.pdf
- 2960G 12.2(53)SE2 Command Reference
  Typ: PDF
  Abrufdatum: 06.03.13
  http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_58_se/command/reference/2960_cr.pdf
- 3560G 12.2(58)SE1 Command Reference
  Typ: PDF
  Abrufdatum: 06.03.13
  http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_58_se/command/reference/3560scr.html
- Cisco UC Phone CP-8945 Reference
  Typ: Webseite
  Abrufdatum: 06.03.13
  http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps10451/ps11158/data_sheet_c78-649595.html
- Windows 7 Integration
  Typ: Webseiten
  Abrufdatum: 06.03.13
  http://windows.microsoft.com/de-at/windows7/enable-802-1x-authentication
  http://technet.microsoft.com/de-de/library/hh831831.aspx
- Windows 8 Integration
  Typ: Webseiten

Abrufdatum: 06.03.13
http://technet.microsoft.com/de-de/library/hh831831.aspx

- Mac OS X 10.5 Integration
  Typ: Webseiten
  Abrufdatum: 06.03.13
  http://support.apple.com/kb/ht3326
  http://de.wikipedia.org/wiki/Mac_OS_X
- Linux Fedora 13 Integration
  Typ: Webseiten
  Abrufdatum: 06.03.13
  http://docs.fedoraproject.org/en-US/Fedora/13/html/Deployment_Guide/sec-Configuring_Connection_Settings.html
  http://fedoraproject.org/de/
- Abbildung 1: IPERKA Phasen
  Typ: Bild
  Abrufdatum: 08.03.13
  http://tgabathuler.ch/IPERKA/bilder/IPERKA_Modell.gif
- Abbildung 2: EAP Ablauf
  Typ: Bild
  Abrufdatum: 08.03.13
  http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/guide/Sw8021x.html

17 Anhang

17.1 Komplette Config 2908g-ipamkoch

```
vtp mode client
vtp domain hsr
vtp password <wurde entfernt>
!
!
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
!
hostname 2908g-ipamkoch
ip domain-name hsr.ch
!
enable secret 5 <wurde entfernt>
!
username netzwerkteam privilege 15 secret 5 <wurde entfernt>
!
aaa new-model
!
!
```

```
aaa group server radius DOT
 server 152.96.229.50 auth-port 1645 acct-port 1646
 server 152.96.229.51 auth-port 1645 acct-port 1646
!
aaa authentication fail-message ^CCCC Bitte nochmals versuchen... ^C
aaa authentication login DOT group radius local
aaa authentication enable default group DOT enable
aaa authentication dot1x default group DOT
aaa authorization console
aaa authorization exec DOT group radius local
aaa authorization network default group DOT
aaa accounting dot1x default start-stop group DOT
aaa accounting exec default start-stop group DOT
!
aaa session-id common
clock timezone GMT 1
clock summer-time GMT recurring
system mtu routing 1500
ip subnet-zero
!
dot1x system-auth-control
!
no ip domain-lookup
!
mvr
!
!
errdisable recovery cause udld
errdisable recovery cause bpduguard
errdisable recovery interval 180
no file verify auto
spanning-tree mode rapid-pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface range GigabitEthernet 0/1 - 7
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
 authentication port-control auto
 dot1x pae authenticator
 dot1x guest-vlan 229
 dot1x auth-fail vlan 229
 dot1x auth-fail max-attempts 2
 authentication event server dead action authorize vlan 229
 dot1x timeout tx-period 5
exit
!
interface GigabitEthernet0/8
 switchport mode trunk
 udld port aggressive
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan864
```

```
 ip address 192.168.0.10 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.0.1
no ip http server
no ip http secure-server
logging source-interface Vlan864
ip radius source-interface Vlan864
logging 152.96.20.56
snmp-server community mdcnkmnl RO
snmp-server location ipamkoch
snmp-server contact netzwerk@hsr.ch
snmp-server enable traps snmp authentication linkdown linkup coldstart
snmp-server enable traps tty
snmp-server enable traps config
radius-server retransmit 0
radius-server timeout 5
radius-server host 152.96.229.51 auth-port 1645 acct-port 1646 key MyRadiusKey
radius-server host 152.96.229.50 auth-port 1645 acct-port 1646 key MyRadiusKey
radius-server vsa send authentication
!
control-plane
!
!
line con 0
 session-timeout 15
 authorization exec DOT
 login authentication DOT
line vty 0 4
 session-timeout 15
 authorization exec DOT
 login authentication DOT
 transport preferred none
 transport input ssh
 transport output telnet
line vty 5 15
 session-timeout 15
 authorization exec DOT
 login authentication DOT
 transport preferred none
 transport input ssh
 transport output telnet
!
ntp clock-period 36028681
ntp server 192.168.0.1
crypto key generate rsa
2048
end
```

17.2 Komplette Konfig 2948s-ipamkoch

```
vtp mode client
vtp domain hsr
vtp password <wurde entfernt>
!
!
no service pad
service timestamps debug datetime localtime
```

```
service timestamps log datetime localtime
service password-encryption
!
hostname 2948s-ipamkoch
ip domain-name hsr.ch
!
enable secret 5 <wurde entfernt>
!
username netzwerkteam privilege 15 secret 5 <wurde entfernt>
aaa new-model
!
!
aaa group server radius DOT
 server 152.96.229.51
 server 152.96.229.50
!
aaa authentication fail-message ^CCCCC Bitte nochmals versuchen... ^C
aaa authentication login DOT group radius local
aaa authentication enable default group DOT enable
aaa authentication dot1x default group DOT
aaa authorization console
aaa authorization exec DOT group radius local
aaa authorization network default group DOT
aaa accounting dot1x default start-stop group DOT
aaa accounting exec default start-stop group DOT
!
!
!
aaa session-id common
!
clock timezone GMT 1
clock summer-time GMT recurring
ip subnet-zero
!
dot1x system-auth-control
!
mvr
!
errdisable recovery cause udld
errdisable recovery cause bpduguard
errdisable recovery interval 180
spanning-tree mode rapid-pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
!
!
interface range gigabitEthernet 1/0/1 - 45
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
 authentication port-control auto
 dot1x pae authenticator
 dot1x guest-vlan 229
 dot1x auth-fail vlan 229
 dot1x auth-fail max-attempts 2
 authentication event server dead action authorize vlan 229
 dot1x timeout tx-period 5
!
interface GigabitEthernet1/0/49
```

```
 udld port aggressive
 switchport mode trunk
 !
interface range GigabitEthernet1/0/46 - 48
 switchport mode trunk
 udld port aggressive
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan864
 ip address 192.168.0.11 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.0.1
no ip http server
no ip http secure-server
logging source-interface Vlan864
logging 152.96.20.56
snmp-server community mdcnkmnl RO
snmp-server location ipamkoch
snmp-server contact netzwerk@hsr.ch
snmp-server enable traps snmp authentication linkdown linkup coldstart
snmp-server enable traps tty
snmp-server enable traps config
ip radius source-interface Vlan864
radius-server retransmit 0
radius-server timeout 5
radius-server host 152.96.229.50 key MyRadiusKey
radius-server host 152.96.229.51 key MyRadiusKey
radius-server vsa send authentication
!
line con 0
 session-timeout 15
 authorization exec DOT
 login authentication DOT
line vty 0 4
 session-timeout 15
 authorization exec DOT
 login authentication DOT
 transport preferred none
 transport input ssh
 transport output telnet
line vty 5 15
 session-timeout 15
 authorization exec DOT
 login authentication DOT
 transport preferred none
 transport input ssh
 transport output telnet
!
!
ntp server 192.168.0.1
crypto key generate rsa
2048
end
```

17.3 Komplette Konfig 3524s-ipamkoch

```
vtp mode client
vtp domain hsr
vtp password <wurde entfernt>
!
no service pad
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
!
hostname 3524p-ipamkoch
ip domain-name hsr.ch
!
enable secret 5 <wurde entfernt>
!
username netzwerkteam privilege 15 secret 5 <wurde entfernt>
aaa new-model
!
!
aaa group server radius DOT
 server 152.96.229.50
 server 152.96.229.51
!
aaa authentication fail-message ^CCCCC Bitte nochmals versuchen... ^C
aaa authentication login DOT group radius local
aaa authentication enable default group DOT enable
aaa authentication dot1x default group DOT
aaa authorization console
aaa authorization exec DOT group radius local
aaa authorization network default group DOT
aaa accounting dot1x default start-stop group DOT
aaa accounting exec default start-stop group DOT
!
!
!
aaa session-id common
!
clock timezone gmt 1
clock summer-time gmt recurring
ip subnet-zero
!
dot1x system-auth-control
!
mvr
!
errdisable recovery cause udld
errdisable recovery cause bpduguard
errdisable recovery interval 180
no file verify auto
spanning-tree mode rapid-pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface range GigabitEthernet 0/1 - 23
 switchport mode access
 spanning-tree portfast
```

```
 authentication port-control auto
 dot1x pae authenticator
 dot1x guest-vlan 229
 dot1x auth-fail vlan 229
 dot1x auth-fail max-attempts 2
 authentication event server dead action authorize vlan 229
 dot1x timeout tx-period 5
 switchport voice vlan 101
 power inline auto
!
interface GigabitEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
 udld port aggressive
!
interface GigabitEthernet0/26
 shutdown
!
interface GigabitEthernet0/27
 shutdown
!
interface GigabitEthernet0/28
 shutdown
!

interface Vlan1
 no ip address
 shutdown
!
interface Vlan864
 ip address 192.168.0.12 255.255.255.0
!
ip classless
no ip http server
no ip http secure-server
ip default-gateway 192.168.0.1
!

logging source-interface Vlan864
logging 152.96.20.56
snmp-server community mdcnkmnl RO
snmp-server location xipamkoch
snmp-server contact netzwerk@hsr.ch
snmp-server enable traps snmp authentication linkdown linkup coldstart
snmp-server enable traps tty
snmp-server enable traps config
!
ip radius source-interface Vlan864
radius-server retransmit 0
radius-server timeout 5
radius-server host 152.96.229.50 key MyRadiusKey
radius-server host 152.96.229.51 key MyRadiusKey
radius-server vsa send authentication
!
line con 0
 session-timeout 15
 authorization exec DOT
 login authentication DOT
line vty 0 4
 session-timeout 15
```

```
 authorization exec DOT
 login authentication DOT
 transport preferred none
 transport input ssh
 transport output telnet
line vty 5 15
 session-timeout 15
 authorization exec DOT
 login authentication DOT
 transport preferred none
 transport input ssh
 transport output telnet
!
!
ntp server 192.168.0.1
crypto key generate rsa
2048
end
```