

Netzwerkservice



Modul NS

Modulunterlagen

Dieses Dokument darf ohne schriftliche Zustimmung des RAU weder kopiert noch anderweitig vervielfältigt werden.
© RAU, 2021

Inhaltsverzeichnis

1	Netzwerktechnik – Basis	4
1.1	Lernjournal	4
1.2	Peer to Peer Netzwerk	5
1.3	Peer to Peer Netzwerk mit DHCP.....	6
1.4	Lernkontrolle	7
1.5	Freigabe von Ressourcen	8
1.6	Kabelltypen	9
2	Netzwerktechnik – Erweitert	10
2.1	Systemdokumentation.....	10
2.2	Netzwerkgrundlagen	11
2.3	Netzwerk mit Clients betreiben.....	14
2.4	WLAN	15
2.5	Netzwerk mit Server-Infrastruktur.....	18
2.6	Hacker-Attack	20
2.7	Virtualisierte Server-Infrastruktur.....	25
2.8	Internet.....	26
2.9	VLAN	29
3	Services	30
3.1	Lernjournal	30
3.2	Systemdokumentation.....	31
3.3	Soll Zustand	32
3.4	Vorbereitung der Infrastruktur.....	33
3.5	Active Directory	34
3.6	DHCP.....	36
3.7	DNS	36
3.8	Samba	37
3.9	Webserver.....	38
3.10	Datenbanken.....	39
3.11	WSUS	41
3.12	Mailserver	43
3.13	Scripting	45
3.14	Client Security	47

Modulunterlagen

Identifikation und Änderungsgeschichte

Dokumenttitel: Modulunterlagen
Thema: Modul NS Netzwerkservice
Autor: Dominik Uehlinger
Firma: RAU, Regionales Ausbildungszentrum Au
Dateiname: HandOut-NS_Netzwerkservice_v10.docx
Ablageort: K:\Module_ab_2021\NS_Netzwerkservice\Lernende\HandOut-NS_Netzwerkservice_v10.docx
Druckdatum: 19.11.2021

Version	Datum	Bemerkungen
1.0	November 2021	Initialversion basierend auf FA NWT und OS / DU

1 Netzwerktechnik – Basis

1.1 Lernjournal

1.1.1 Auftrag

Sie sind in diesem Modul verpflichtet, die wesentlichen Elemente von Theorien und die Erkenntnisse aus den Übungen in Lernjournal-Form elektronisch festzuhalten. Die vorliegenden Informationen regeln die Vorgaben und Rahmenbedingungen an Ihr Erzeugnis.

1.1.2 Formale Anforderungen

Die formalen Anforderungen sind hinsichtlich Darstellung und Rechtschreibung einzuhalten. Das Lernjournal soll für Drittpersonen nachvollziehbar sein.

Es wird ein Titelbild, ein Glossar und Quellenangaben verlangt.

1.1.3 Quellenangabe

Es ist zulässig (aber nicht immer sinnvoll), Texte aus Quellen wie dem Internet oder aus Büchern zu übernehmen. In diesen Fällen muss aber die Quelle angegeben und im Quellenverzeichnis beschrieben werden.

1.2 Peer to Peer Netzwerk

1.2.1 Theorie

- TCP/IP, IP-Adressklassen, reservierte IP-Adressen
- Subnetze
- statische Vergabe von IP-Adressen
- OSI-Schichten Referenzmodell

1.2.2 Aufgaben

A1	Verbinden Sie zwei Clients mit einem Netzwerk-Kabel.
A2	IP-Adressen aus dem Bereich 192.168.26.0 /24 werden vergeben. An der erweiterten Konfiguration von TCP/IP wird nichts verändert.
[F1]	Wie kann die Verbindung überprüft resp. getestet werden?
[F2]	Welche Fehler können hier entstehen und wie werden sie gefunden?
[F3]	Wer oder was übernimmt die Auflösung (Erkennung) der Computernamen, die ja offensichtlich in der Netzwerkumgebung von Windows angezeigt werden?
A3	Verbinden Sie sich jetzt zu zweit über einen Switch.
[F4]	Für was ist ein Switch da?
[F5]	Was kannst du über einen Router aussagen? Was macht dieser?

1.2.2.1 Netzwerkadministration

Folgende Befehle zur Analyse und zur Administration eines Netzwerkes mit TCP/IP werden untersucht und dokumentiert:

A1	<ul style="list-style-type: none"> • <i>ping</i> • <i>ipconfig</i> • <i>netstat</i> • <i>arp</i> • <i>nslookup</i> • <i>tracert</i>
----	---

1.3 Peer to Peer Netzwerk mit DHCP

1.3.1 Theorie

- Server als Service resp. Dienst verstehen und nicht als physikalische Maschine oder spezielles Betriebssystem (z.B. Windows Server)
- DHCP

1.3.2 Aufgaben

1.3.2.1 Konfiguration eines Clients auf DHCP

A1	Auf einem Notebook-Client wird die Konfiguration von TCP/IP so angepasst, dass dieser dynamisch eine IP-Adresse bezieht (obwohl noch kein DHCP-Dienst im Netzwerk vorhanden ist).
[F1]	Was geschieht bei einem Neustart?

1.3.2.2 Installation und Konfiguration eines DHCP-Dienstes

A2	Auf dem zweiten Client wird ein DHCP-Dienst installiert und mit einem gültigen Bereich (bspw. 192.168.5.x /24) konfiguriert. Der erste Client bezieht nun seine IP von diesem Dienst.
[F2]	Wie wirkt sich ipconfig /renew aus?
[F3]	Wie wirkt sich ipconfig /release aus?
[F4]	Warum findet ein Client einen DHCP-Dienst im Netzwerk?
[F5]	Wie kann die Lease-Dauer auf einem Client ermittelt werden, welcher seine IP dynamisch bezogen hat?

1.4 Lernkontrolle

[F1]	Welchen Schichten im OSI-Referenzmodell werden die Übertragungsprotokolle und welchen die Transportprotokolle zugeordnet?
[F2]	Durch welchen Umstand wird in der Praxis das Übertragungsprotokoll festgelegt?
[F3]	Welche Fehlermeldung erscheint, wenn TCP/IP auf einem Computer so konfiguriert ist, dass er seine IP dynamisch von einem DHCP beziehen soll, im Netzwerk aber nirgends ein solcher Dienst zur Verfügung steht?
[F4]	In welchen Fällen macht es in der Praxis beim Einsatz eines DHCP-Servers Sinn, IP Adressen weiterhin statisch zu vergeben und aus dem DHCP-Bereich (Pool) auszuschliessen?
[F5]	DHCP ist ein typischer Netzwerk-Dienst. Wie funktioniert das Protokoll, wie kommen die Clients zu ihrer IP-Adresse?
[F6]	In welchem Fall benötigen Sie eine öffentliche IP-Adresse? Woher bekommen Sie sie?
[F7]	Wie setzt sich eine IP-Adresse zusammen? Wie lang ist sie?
[F8]	Was zeichnet die privaten Bereiche der IP-Adressierung technisch aus?

1.5 Freigabe von Ressourcen

1.5.1 Theorie

- Freigabe von Druckern
- Freigabe von Verzeichnissen
- Lokale Benutzer und Gruppen
- Grundsatz bei der Vergabe von Rechten (Rechte an Gruppen)

1.5.2 Berechtigungen bei der Freigabe

1.5.2.1 Aufgaben Freigabe von Verzeichnissen

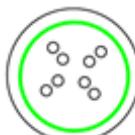
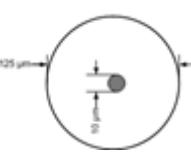
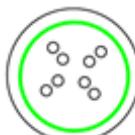
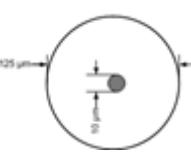
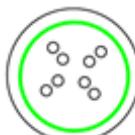
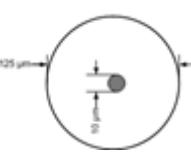
A1	Erstellen Sie auf dem Computer A einen neuen Benutzer Testuser und eine neue Gruppe Testgruppe und fügen Sie den Benutzer in diese Gruppe hinzu. Erstellen Sie ebenfalls auf dem Computer A ein Verzeichnis C:\Test und geben Sie dieses Verzeichnis ohne Änderung der Konfiguration frei.
[F1]	Kann auf das Verzeichnis C:\Test vom Computer B aus zugegriffen werden?
[F2]	Wie sind die Standardeinstellungen in Bezug auf die Berechtigung bei einer Freigabe?
A2	Ändern Sie die Berechtigungen auf den freigegebenen Ordner so, dass der Ordner nur noch für die Gruppe Testgruppe freigegeben ist.
[F3]	Kann auf das Verzeichnis C:\Test vom Computer B aus zugegriffen werden?
[F4]	Was ist die Problematik?

1.5.2.2 Aufgaben Freigaben von Drucker

A1	Geben Sie auf dem Client A einen nahegelegenen Drucker frei. Verbinden Sie anschließend diesen Drucker von einem Client B.
[F1]	Was muss angegeben werden, damit man einen Netzwerk-Drucker verbinden kann?
[F2]	Was ist der grosse Nachteil von dieser Art Drucker freizugeben?

1.6 Kabeltypen

1.6.1 Aufgabe

A1	<p>Recherchieren Sie im Internet und beantworten Sie die folgenden Fragen:</p> <table border="1"> <thead> <tr> <th>Kabeltyp</th><th>Fragen</th></tr> </thead> <tbody> <tr> <td>U/UTP Kat. 5/5e/6/6a</td><td> Was bedeutet die Bezeichnung U/UTP?</td></tr> <tr> <td>F/UTP Kat. 5/5e/6/6a Grüne Folie</td><td> Was bedeutet die Bezeichnung F/UTP?</td></tr> <tr> <td>S/FTP Kat. 5/5e/6/6a Grüner Gesamtschirm Rote Aderschirmung</td><td>Was bedeutet die Bezeichnung S/FTP?</td></tr> <tr> <td>LWL 50/125 µm Multimode</td><td> Welche Kategorien gibt es für Multimodefasern?</td></tr> <tr> <td>LWL 9/125 µm Singlemode</td><td> Welche Kategorien gibt es für Singlemodefasern?</td></tr> </tbody> </table>		Kabeltyp	Fragen	U/UTP Kat. 5/5e/6/6a	 Was bedeutet die Bezeichnung U/UTP?	F/UTP Kat. 5/5e/6/6a Grüne Folie	 Was bedeutet die Bezeichnung F/UTP?	S/FTP Kat. 5/5e/6/6a Grüner Gesamtschirm Rote Aderschirmung	Was bedeutet die Bezeichnung S/FTP?	LWL 50/125 µm Multimode	 Welche Kategorien gibt es für Multimodefasern?	LWL 9/125 µm Singlemode	 Welche Kategorien gibt es für Singlemodefasern?
Kabeltyp	Fragen													
U/UTP Kat. 5/5e/6/6a	 Was bedeutet die Bezeichnung U/UTP?													
F/UTP Kat. 5/5e/6/6a Grüne Folie	 Was bedeutet die Bezeichnung F/UTP?													
S/FTP Kat. 5/5e/6/6a Grüner Gesamtschirm Rote Aderschirmung	Was bedeutet die Bezeichnung S/FTP?													
LWL 50/125 µm Multimode	 Welche Kategorien gibt es für Multimodefasern?													
LWL 9/125 µm Singlemode	 Welche Kategorien gibt es für Singlemodefasern?													
	 Wikipe-dia	de.wikipedia.org/wiki/Twisted-Pair-Kabel												
	 Wikipe-dia	de.wikipedia.org/wiki/Lichtwellenleiter												

2 Netzwerktechnik – Erweitert

2.1 Systemdokumentation

2.1.1 Auftrag

Im Rahmen dieses Moduls installieren und konfigurieren Sie einige Komponenten und Systeme. Es gilt nun eine Dokumentation zu erstellen, die festhält, welche Einstellungen und Entscheidungen getroffen wurden. Die Dokumentation muss alle Informationen beinhalten, die es einem ausgebildeten Informatiker erlauben das System exakt nachzubilden.



Achtung

Die Systemdokumentation wird am letzten Modultag dem zuständigen Berufsbildner abgegeben. Die formale Abgabe ist ein PDF mit folgendem Dateinamen:
FA-NWT-GrNr.pdf

2.1.2 Formale Anforderungen

Die zu erstellende elektronische Dokumentation hat alle Anforderungen an den Aufbau und die Gestaltung eines professionellen Dokumentes zu erfüllen, wie dies im Rahmen des Moduls OK behandelt wurde. Neben den Vorgaben an die Gliederung und den Inhalt (vgl. unten), weist die Dokumentation zusätzlich folgende Elemente auf:

- Titelblatt
- Inhaltsverzeichnis
- Glossar (Erklärung der Abkürzungen und Fremdwörter) im Anhang
- Index (Auflistung der wichtigsten Begriffe mit Angabe der Seitenzahl) im Anhang
- Nummerierung der Tabellen und Abbildungen und entsprechende Verzeichnisse im Anhang

2.1.3 Quellenangabe

Es ist zulässig (aber nicht immer sinnvoll), Texte aus Quellen wie dem Internet oder aus Büchern zu übernehmen. In diesen Fällen muss aber die Quelle angegeben werden. Die wird am einfachsten mittels einer nummerierten Aufzählung der Quellen vorne im Dokument erzielt, wobei anschliessend im Text am Ende eines zitierten Absatzes (z.B. in eckigen Klammern [x]) auf die entsprechende Quelle referenziert wird.

Beispiel Internet und Buch:

Wikipedia: OSI-Modell. Abgerufen am 18.10.2021 unter <http://de.wikipedia.org/wiki/OSI-Modell>

„Das OSI-Modell¹ (englisch Open Systems Interconnection Model) ist ein Referenzmodell ...“

Andrew S. Tanenbaum, David J. Wetherall: Computernetzwerk.

¹ Zitat <http://de.wikipedia.org/wiki/OSI-Modell> abgerufen am 18.10.2021

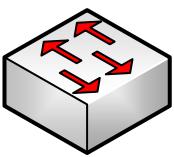
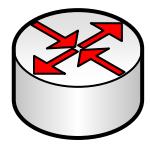
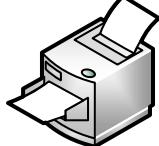
2.2 Netzwerkgrundlagen

2.2.1 OSI-Modell und Protokolle

A1	Lesen Sie im Buch „IT-Handbuch für Fachinformatiker“ folgende Kapitel:				
	 IT-Handbuch für Fachinformatiker	Kapitel: 4.2 Funktionsebenen von Netzwerken Kapitel: 4.3.1 Die Reichweite des Netzwerks Kapitel: 4.3.3 Der Zentralisierungsgrad des Netzwerks Kapitel: 4.6 Die TCP/IP-Protokollfamilie			
A2	Ordnen Sie die einzelnen Schichten in der richtigen Reihenfolge zu (1-7).				
	 Tipp	Lernen Sie die Begriffe auswendig.			
	Vermittlungsschicht, Physical Layer, Session Layer, Kommunikationssteuerungsschicht, Application Layer, Darstellungsschicht, Sicherungsschicht, Anwendungsschicht, Transport Layer, Bitübertragungsschicht, Data Link Layer, Network Layer, Transportschicht, Presentation Layer				
[F1]	Was bedeuten die folgenden Begriffe? WAN: LAN:				
A3	Beschreiben Sie mit eigenen Worten die „Definition eines Servers“ und die „Definition eines Clients“.				
A4	Ordnen Sie die Protokolle den einzelnen Schichten zu: TCP, FTP, SMTP (E-Mail), ARP, UDP, Ethernet, ICMP, IP, HTTP (www)				
Z1	Recherchieren Sie unter Wikipedia die Funktionsweise der Protokolle aus A4. Wozu dienen diese Protokolle? Wofür werden sie eingesetzt? Wie sind die Protokolle aufgebaut?				

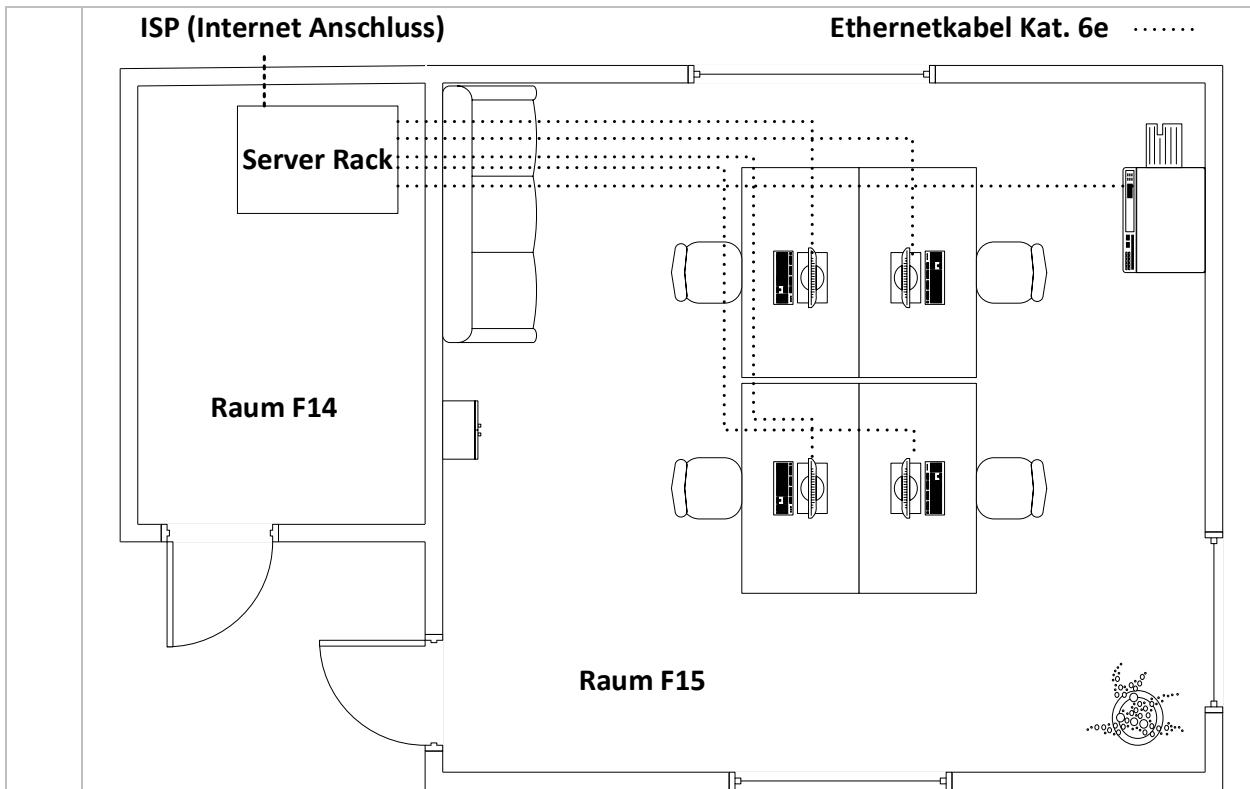
2.2.2 Logisches Netzwerkschema

A1	Erstellen Sie im Visio einen Netzplan der IN-Umgebung mit den unten dargestellten Symbolen und verbinden Sie die einzelnen Netzwerkkomponenten richtig. Benennen Sie die Komponenten mit Namen, Geräte-Typ, OS, IP-Adresse, MAC-Adresse und eventuellen Diensten. Geben Sie dem Router die LAN-IP 192.168.75.254 und die WAN-IP 178.196.82.233.
----	---

	         	
[F1]	Wozu und wann wird das Ethernet-Symbol im Visio eingesetzt? Was sind die Vor- und Nachteile?	<input type="text" value="192.168.75.0/24"/>
[F2]	Mit welchen Hilfsmitteln können Sie die IP des Routers (Standardgateway) feststellen?	
A2	Ermitteln Sie die WAN-IP mit Hilfe von z.B. https://www.iplocation.net/find-ip-address :	

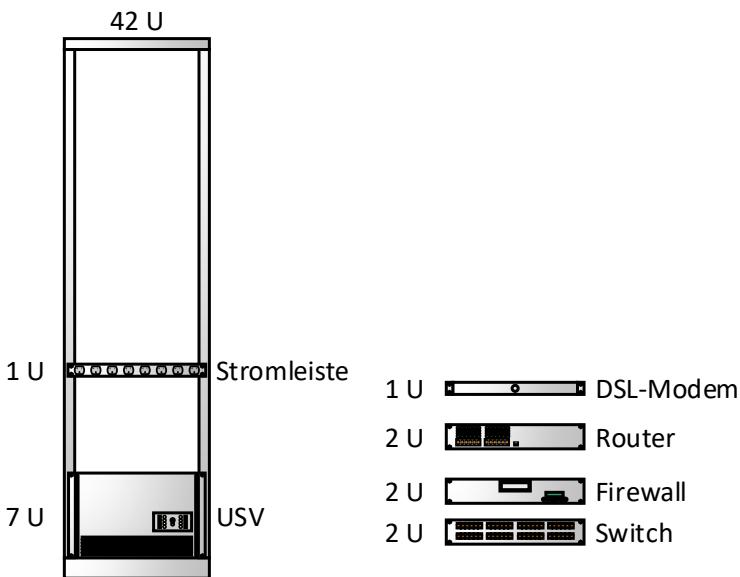
2.2.3 Physikalisches Netzwerkschema

A1	<p>Visio Schablonen einrichten</p> <p>Die Schablonen für das Visio werden vorbereitet. Dazu wird unter „Pläne und Grundriss“ ein Büroplan erstellt. Als Nächstes wird unter „Weitere Shapes“ > „Netzwerk“ > „Gestellmontierte Geräte“ hinzugefügt.</p> <p>Physikalisches Netzwerkschema</p> <p>Zeichnen Sie den Gebäudeplan des untenstehenden Bildes mit Büro- und Serverraum ab. Setzen Sie die Mauern, Türen und Fenster. Anschliessend wird der Raum möbliert und mit IT-Geräten ausgerüstet. Zum Schluss müssen die Computer und die Peripheriegeräte verkabelt und angeschlossen werden. Bezeichnen Sie die Kabeltypen mit der entsprechenden Kategorie.</p>
----	---



Serverack

Nun fehlt das Serverack. Dann ist unsere IT-Infrastruktur komplett dokumentiert. Dazu wird die Schablone „Gestellmontierte Geräte“ verwendet. Setzten Sie die einzelnen Netzwerkkomponenten (DSL-Modem, Router, Firewall, Switch, USV) in das Gestell ein.



Z1 Beschriftung der Verkabelung

Auf dem Switch haben die Ports Anschlussnummern. Die Ethernetkabel werden vom Switch zu den einzelnen Arbeitsplätzen verlegt und beschriftet. Es wird ein Verkabelungsplan mit den Portnummern und den Kabelnummern erstellt.

2.3 Netzwerk mit Clients betreiben

In den nächsten Übungen wird ein Netzwerk schrittweise aufgebaut und erweitert. Es werden verschiedene Netzwerkkomponenten ins Netzwerk integriert und diverse Dienste bereitgestellt.


Achtung

Es dürfen **nie** mehr als ein DHCP im gleichen Netzwerk betrieben werden!

[F1]

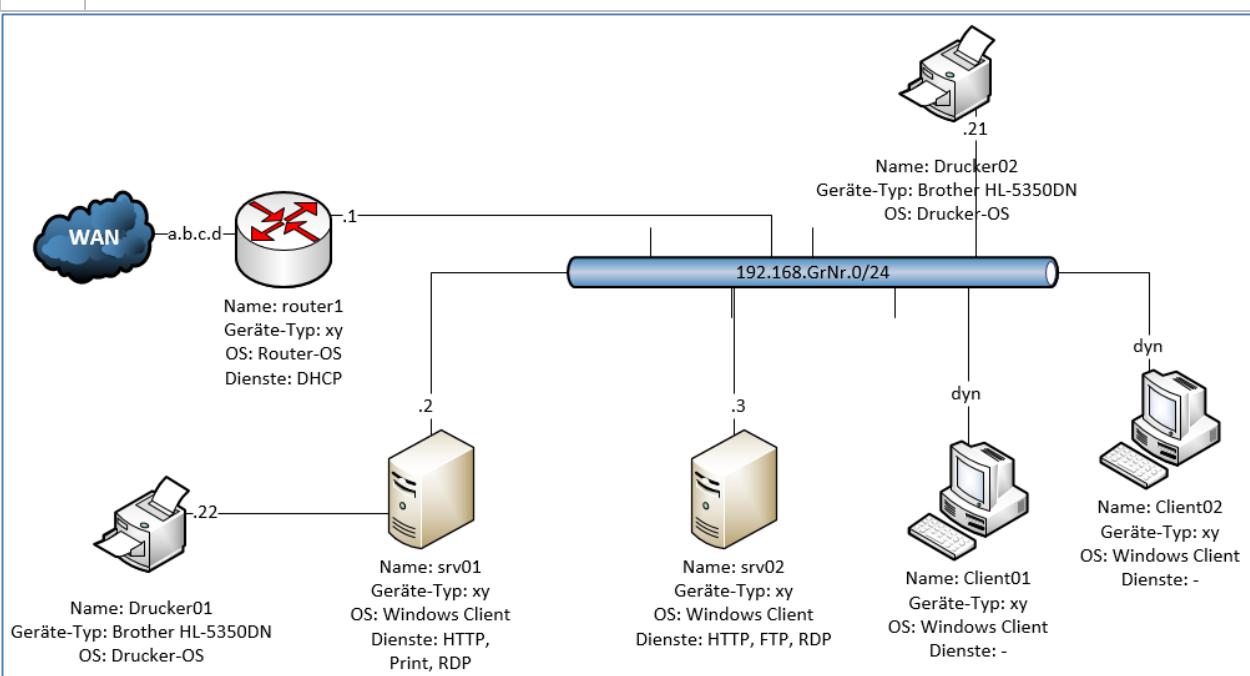
Was sind die Folgen, wenn die Regel nicht eingehalten wird?

A1 Planung Netzadresse

Jeder Gruppe erhält eine Gruppennummer; also 10, 20, 30, 40, 50, usw. Die Netzadresse ist 192.168.“Gruppennummer“.0/24. Teilen Sie nun die IP-Bereiche wie folgt auf:

- 192.168.10.1 Default Gateway
- 192.168.10.2 – 20 Server
- 192.168.10.21 – 50 Drucker
- 192.168.10.51 – 199 Clients
- 192.168.10.200 – 254 Netzwerkkomponenten z.B. Switch, Access Point, ...

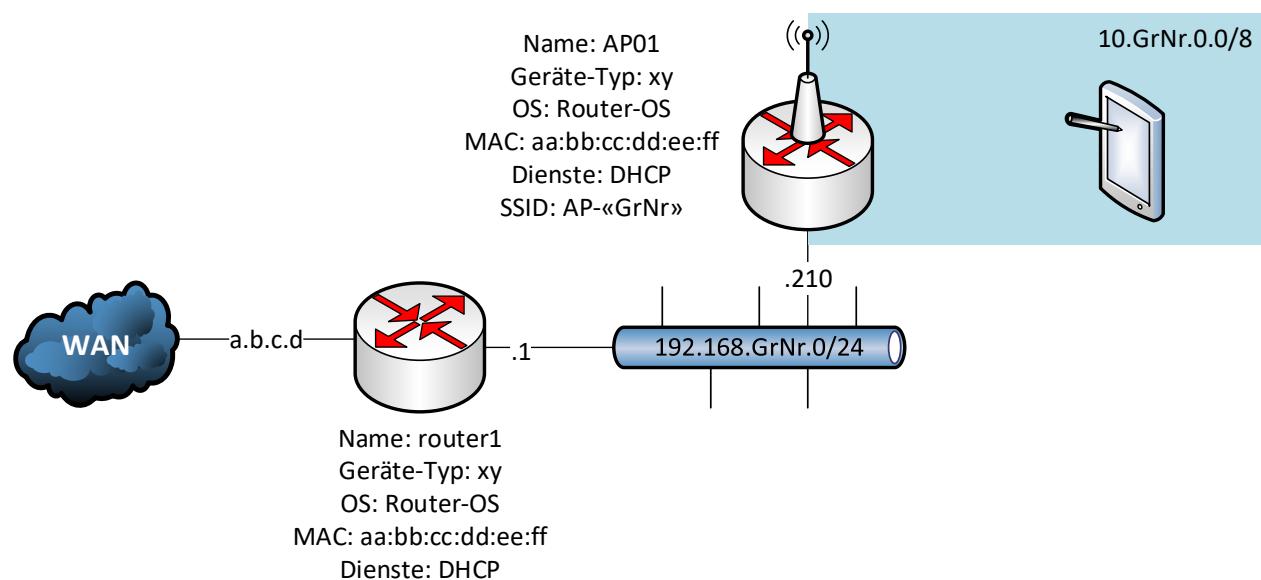
[F1] Wozu werden die Adressen 192.168.10.0 und 192.168.10.255 verwendet?



A2	<p>Netzaufbau</p> <p>Es wird folgendes Netzwerk aufgebaut und in der Systemdokumentation werden Installation und Konfiguration sauber beschrieben. Die Arbeiten werden sinnvoll auf die Gruppenmitglieder aufgeteilt, so dass am Schluss jedes Gruppenmitglied das Netzwerk selber aufbauen, konfigurieren und testen kann.</p> <ul style="list-style-type: none"> Router wird am RAU-Netzwerk (WAN) und am lokalen Netzwerk (LAN) angegeschlossen. Routern an Switch anschliessen. Server, Clients und Drucker verkabeln. Router wird mittels Webinterface konfiguriert (siehe Usermanual des Herstellers) DHCP mit Adresspool auf dem Router konfigurieren und testen. Bei beiden Servern (srv01, srv02) die IP statisch setzen. Auf den Servern werden die geforderten Dienste installiert und konfiguriert: <ul style="list-style-type: none"> HTTP wird mittels XAMPP realisiert. FTP wird mittels FileZilla realisiert. Die Homepage wird mittels FTP hochgeladen und gewartet. Die Homepage beinhaltet mindestens Servername, IP-Adresse, Gruppenmitglieder und Gruppennummer. Drucker01 über srv01 freigeben. Drucker02 als Netzwerkdrucker konfigurieren. Client01 und Client02 können auf die Serverdienste zugreifen, haben eine dynamische IP und haben Zugriff auf das Internet.
A3	<p>Testing</p> <p>Mit einem Testprotokoll werden die Netzwerkkomponenten und Dienste getestet.</p>

2.4 WLAN

Das Netzwerk wird mit Wireless-LAN erweitert.



2.4.1 Konfiguration

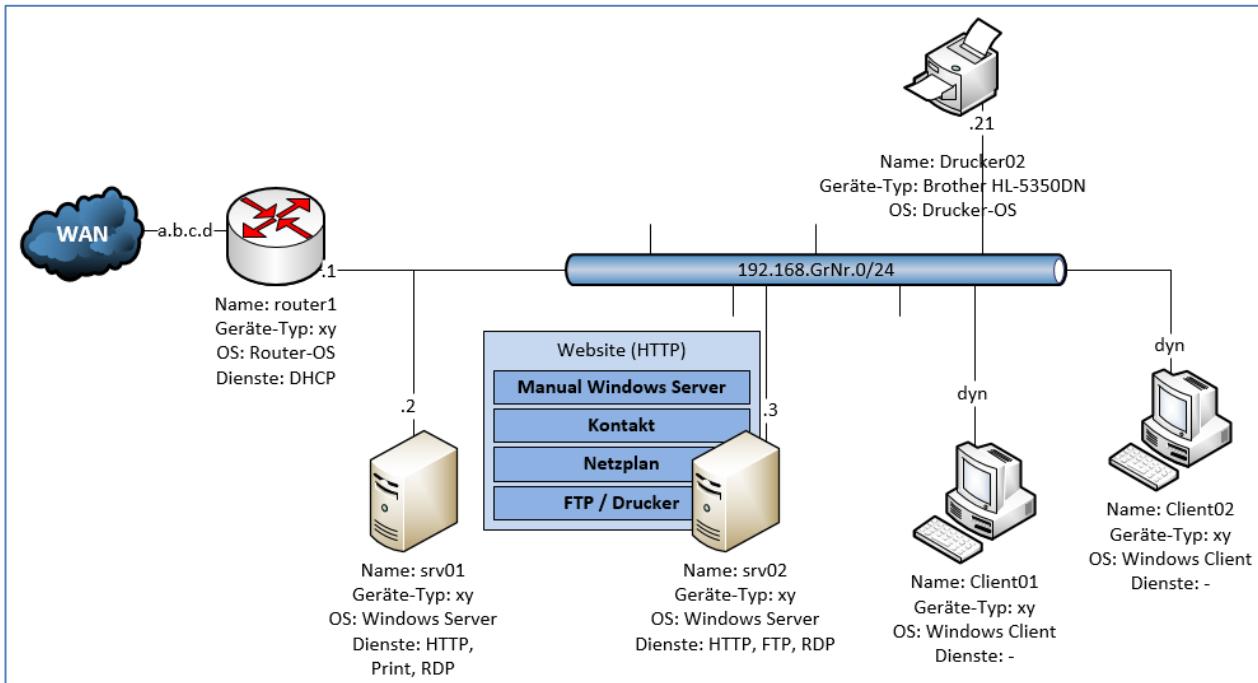
A1	Konfiguration Access Point <ul style="list-style-type: none">• Starkes Passwort setzen• Statische IP LAN/WAN setzen• DHCP für 100 Clients setzen, Startadresse ist 10.GrNr.0.10• WLAN 2.4G und 5G konfigurieren<ul style="list-style-type: none">◦ SSID auf AP-„GrNr“ setzen◦ Kanal manuell setzen◦ Verschlüsselung WPA2-PSK◦ Schlüssel setzen
A2	Testing Überprüfen Sie mit einem Testprotokoll, ob ... <ul style="list-style-type: none">• ... die Website www.r-au.ch angezeigt wird.• ... die Netzadresse 10.GrNr.0.0/8 stimmt (ipconfig /all).• ... der Defaultgateway richtig gesetzt ist.• ... die Website http://192.168.GrNr.2 angezeigt wird.

2.4.2 Netzstabilität und Netzsicherheit

A1	Zugriffskontrolle über MAC-Adresse Um den Zugriff im WLAN zu sichern, dürfen nur noch bestimmte MAC-Adressen zugelassen werden. Fügen Sie Ihre Geräte mit Hilfe der Zugriffskontrolle in das WLAN ein. Versuchen Sie mit einem nicht freigegebenen Computer (MAC nicht registriert) auf das WLAN zuzugreifen. Was passiert?
A2	WLAN Ausmessung Auf einem mobilen Gerät wird bspw. inSSIDer installiert und ausgeführt. Es werden die Signalstärken und die Kanalaufteilungen analysiert. Welche AP's haben ein hohes Signal? Wie ist die Kanalaufteilung an Ihrem Standort? Gibt es Störungen? Wie können diese behoben werden?
Z1	HeatMapper Installieren Sie HeatMapper und laden Sie den Gebäudeplan des RAUs. Nun definieren Sie mehrere Messpunkte. Danach laufen Sie die Messpunkte ab und zeichnen die Messungen auf. Werten Sie anschliessend die Ergebnisse aus. Wie sehen die Standorte der AP's aus? Ist die Abdeckung gut? Was gibt es für unbekannte und bekannte AP's? Wie sieht die RAU-WLAN-Infrastruktur aus?

2.5 Netzwerk mit Server-Infrastruktur

Die Windows-Clients (srv01, srv02) werden durch das professionelle Windows Server Betriebssystem ersetzt.



A1	Deaktivieren Sie zuerst den DHCP auf dem Router.	
A2	Machen Sie sich mit dem Manual „Windows Server 2012 R2“ vertraut und lesen Sie die vorgeschlagenen Kapitel. Studieren Sie den Netzplan.	
	 Windows Server 2012 R2	Kapitel: 4.3 Einige grundlegende Netzwerk-protokolle
A3	Windows Server (Englisch) wird auf dem Client srv01 und srv02 installiert. Arbeiten Sie nach einer erfolgreichen Installation immer mit dem Remotedesktop. Nehmen Sie an, dass der Server im Serverraum mit Tastatur / Maus / Bildschirm installiert wird. Danach gehen Sie wieder ins Büro nehmen auf Ihrem Client die restlichen Konfigurationsschritte vor.	
	 Windows Server 2012 R2	Kapitel: 6 Installation Kapitel: 19 Remotedesktopdienste
A4	Active Directory Domain Services auf srv01 aktivieren und konfigurieren. AD Domain-Name: gruppeGrNr.tech	
	 Windows Server 2012 R2	Kapitel: 8 Active Directory-Domänenendienste

Modulunterlagen

A5	DHCP einrichten. Adressbereich festlegen, Lease-Dauer auf 4 Tage setzen, Standard-gateway richtig definieren. Es gelten die gleichen Vorgaben wie beim letzten Netzwerk. Achtung! Es darf nur ein DHCP pro Netzwerk betrieben werden!		
	 Windows Server 2012 R2 Kapitel: 9.2 DHCP		
Z1	DNS einrichten und Hostnamen mit „nslookup“ testen.		
	 Windows Server 2012 R2 Kapitel: 9.1 DNS		
A6	IIS installieren. Es wird eine eigene Website erstellt. Die Startseite hat vier Links. Der erste Link führt zum "Manual Windows Server". Hierbei kann die Website des Openbooks aufgeschaltet werden. Der zweite Link führt zu "Kontakt". Diese Seite beinhaltet die Kontaktdata der Gruppe, um einen Support für die User anzubieten. Der dritte Link führt zu "Netzplan". Dabei wird der vollständige Netzplan als PDF publiziert. Über den Vierten gelangt man zu "FTP / Drucker". Hierbei erscheint ein Manual für den Zugang zum FTP, also eine Beschreibung um Dateien hochzuladen. Achtung, die Passwörter für den FTP-Zugang dürfen nicht öffentlich sein. Zudem gehört ein Drucker-Manual dazu, welches dem User aufzeigt, wie er den Drucker bedienen kann.		
	 Windows Server 2012 R2 Kapitel: 17.3 Installation		
Z2	Mehrere Websites auf dem Server verwalten und betreiben.		
	 Windows Server 2012 R2 Kapitel: 17.5 Webserver, Websites, Anwendungen, virtuelle Verzeichnisse und Anwendungspools		
A7	Website kann von einem Client gewartet werden. Entweder über FTP oder einem File-dienst (Ordnerfreigabe).		
A8	Richten Sie auf srv01 die Rolle "Print and Document Services" ein. Darüber soll ein Drucker auf dem Server installiert und freigegeben werden. Über diese Freigabe sollen die Clients im Anschluss ausdrucken können.		

2.6 Hacker-Attack

In Hacker-Attack werden verschiedene Angriffspunkte im Netzwerk betrachtet. Es geht vorwiegend darum, die Schwächen eines Netzwerkes kennen zu lernen.

2.6.1 Wireshark

[F1]	<p>Grundrecht auf Datenschutz</p> <p><i>„Jede Person hat das Recht, über die Weitergabe und Verwendung ihrer persönlichen Daten zu bestimmen (informationelles Selbstbestimmungsrecht).“</i></p> <p>Ich sniffe am Netzwerk und schaue die privaten E-Mails meiner Mitlernenden an. Zudem klaue ich das Passwort für den Mailzugriff von Tobias. Mache ich mich strafbar (mit Begründung)? Wenn ja, warum?</p> <p>Darf ich mit dem Passwort die Mails von Tobias anschauen? Ich lasse alles so wie es ist und verändere nichts.</p>								
A1	<p>Installation Wireshark</p> <p>Machen Sie sich mit der Dokumentation von Wireshark (www.wireshark.org) vertraut und installieren Sie das Tool. Wählen Sie das Interface für den LAN-Adapter aus und starten Sie die Aufzeichnung.</p>								
A2	<p>TCP Stream Filter</p> <p>Starten Sie eine neue Aufzeichnung.</p> <p>Im Webbrowser öffnen Sie die Website www.r-au.ch. Wenn die Website vollständig angezeigt wird, wird die Aufzeichnung im Wireshark gestoppt. Jetzt filtern Sie die Pakete auf „HTTP“</p>  <p>Als Nächstes wird auf die Anfrage der Website gefiltert. Dazu wird das Paket mit der Info „GET / HTTP/1.1“ ausgewählt und mit der rechten Maustaste wählen Sie den Befehl „Follow TCP Stream“. Nun werden alle Requests und Response der Seite übersichtlich angezeigt. Der Filter wird wieder mit „Clear“ zurückgesetzt.</p>								
A3	<p>IP Filter</p> <p>Es werden drei Filter getestet. Was stellen Sie fest und wie verhält sich der Filter?</p> <table border="1"> <thead> <tr> <th>Filter</th> <th>Verhalten</th> </tr> </thead> <tbody> <tr> <td>ip.addr==192.168.200.124</td> <td></td> </tr> <tr> <td>ip.src==192.168.200.124</td> <td></td> </tr> <tr> <td>ip.dst==192.168.200.124</td> <td></td> </tr> </tbody> </table>	Filter	Verhalten	ip.addr==192.168.200.124		ip.src==192.168.200.124		ip.dst==192.168.200.124	
Filter	Verhalten								
ip.addr==192.168.200.124									
ip.src==192.168.200.124									
ip.dst==192.168.200.124									

A4	<p>Pakete suchen</p> <p>Öffnen Sie eine Website und zeichnen Sie die Pakete in Wireshark auf. Anschliessend suchen Sie das Startpaket mit „GET“. Wie gehen Sie vor?</p> <p>Wie wird diese Such-Funktion verwendet, um ein Passwort zu finden?</p>
----	---

2.6.2 Starke Passwörter

Das sicherste und beste System nützt nichts, wenn der Anwender ein schwaches Passwort nimmt. Die Stärke bei einem Passwort ist durch die Anzahl Symbole und durch die Anzahl Zeichen definiert. Die Formel lautet:

$$\text{Anzahl Symbole}^{\text{Anzahl Zeichen}}$$

Daraus ergibt sich:

Symbole	Anzahl Symbole	Mögliche Kombinationen bei 8 Zeichen	
A...Z	26	26 ⁸ =	208'827'064'576
A...Z, 0...9	36	36 ⁸ =	2'821'109'907'456
A...Z, a...z, 0...9	62	62 ⁸ =	218'340'105'584'896

Wichtig ist, dass jedes Zeichen zufällig ist. Kombinationen wie „1234“, „abcd“ oder „Wörter“ dürfen nicht verwendet. Sie sind einfach zu hacken.

A1	Berechnen Sie die Kombinationen bei 12 Zeichen:			
	Symbole	Anzahl Symbole	Mögliche Kombinationen bei 12 Zeichen	
	A...Z	26		
	A...Z, 0...9	36		
	A...Z, a...z, 0...9	62		
A2	Schätzen Sie die Stärke der Passwörter ein:			
Passwort	schwach	stark	Begründung	
aaaaaa	<input type="checkbox"/>	<input type="checkbox"/>		
aaaaaaaaaaaaaaaa	<input type="checkbox"/>	<input type="checkbox"/>		
Raurau1234	<input type="checkbox"/>	<input type="checkbox"/>		
Los_angeles	<input type="checkbox"/>	<input type="checkbox"/>		
Lo\$ @_ngele\$	<input type="checkbox"/>	<input type="checkbox"/>		
AznHu4Uv	<input type="checkbox"/>	<input type="checkbox"/>		
Ak15_p5cMp7!	<input type="checkbox"/>	<input type="checkbox"/>		

Modulunterlagen

A3 Entwerfen Sie ein starkes Passwort anhand des Beispiels. Merken Sie sich die Eselsbrücke.

Satz	Passwort
An meinem 18 Geburtstag war ich in New York – bäm	Am18GwiiNY-b

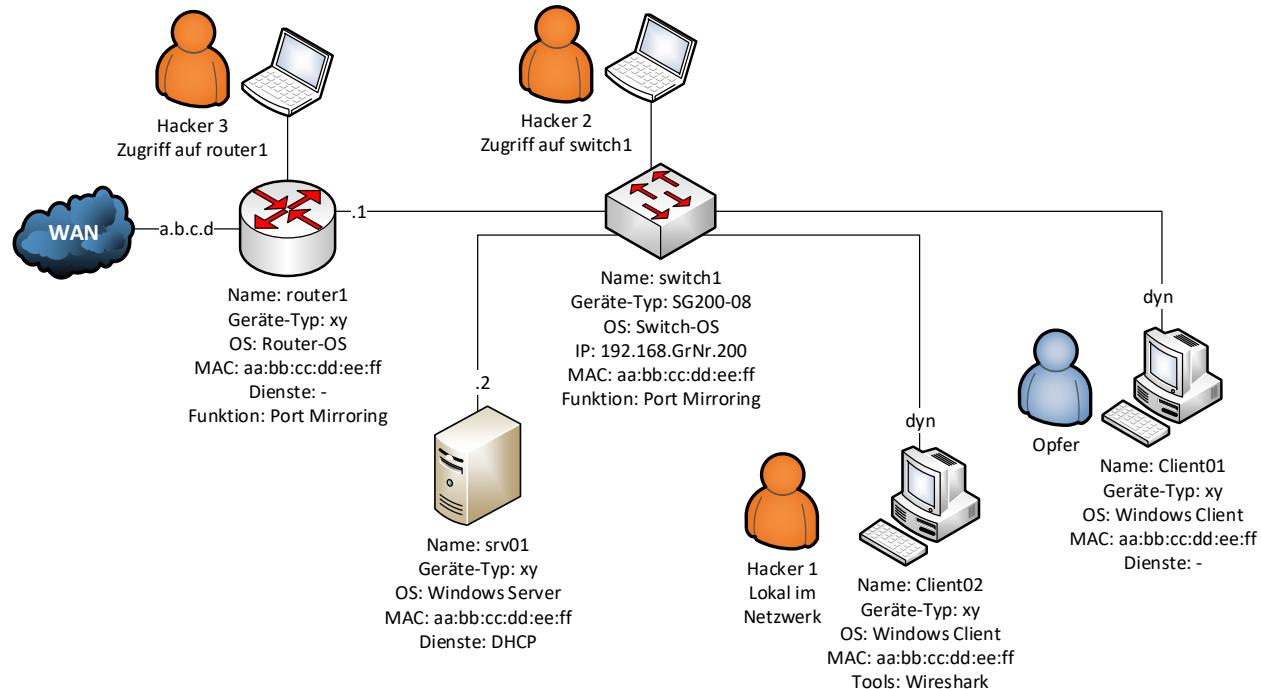


Achtung

Ab heute werden im geschäftlichen Bereich nur noch **starke Passwörter** verwendet!

2.6.3 Netzaufbau

Erweitern Sie das Netzwerk.



A1 Konfiguration Switch SG200-08

Machen Sie sich mit dem Manual des Herstellers bekannt. Dann konfigurieren Sie den Switch SG200-08. Es wird ein starkes Passwort zum Anmelden verwendet. Die IP des Switchs wird statisch auf 192.168.GrNr.200 gesetzt. Jetzt schliessen Sie den Hacker PC an und mittels „Port Mirroring“ werden die Pakete zum Hacker gespiegelt.

A2 Konfiguration Router

Auf dem Router wird das „Port Mirroring“ für den Hacker-PC frei geschaltet.

2.6.4 Attack

A1	Opfer
	Das Opfer öffnet verschiedene Webseiten im Internet.
A2	Hacker 1
	Versuchen Sie herauszufinden, auf welchen Seiten das Opfer surft. Was stellen Sie fest?
A3	Hacker 2
	Versuchen Sie herauszufinden, auf welchen Seiten das Opfer surft. Was stellen Sie fest?
A4	Hacker 3
	Versuchen Sie herauszufinden, auf welchen Seiten das Opfer surft. Was stellen Sie fest?

Modulunterlagen

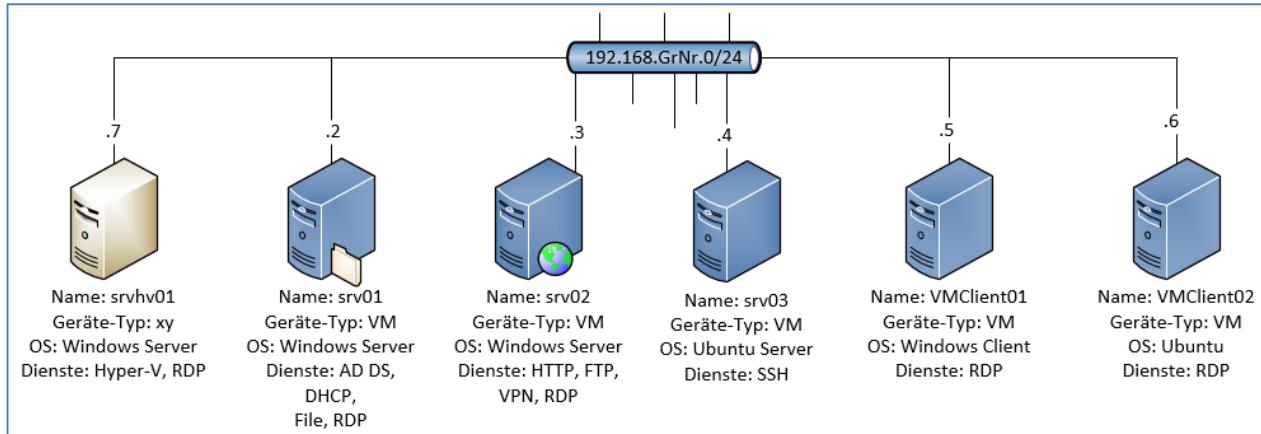
Z1	Portscanner
----	-------------

Installieren Sie den Portscanner www.nmap.org. Starten Sie das Tool im lokalen Netzwerk und schauen Sie, welche Computer vorhanden sind. Vergleichen Sie die gemessenen Resultate mit Ihrem Netzplan.

2.7 Virtualisierte Server-Infrastruktur

Um die Computer in Zukunft besser zu warten und zu verwalten, werden die einzelnen Server virtualisiert. Dazu kann unter Windows Server der Dienst Hyper-V verwendet werden.

Die Netzerweiterungen sind im folgenden Netzplan dargestellt. Die IPs und Dienste sind pro Server beschrieben.



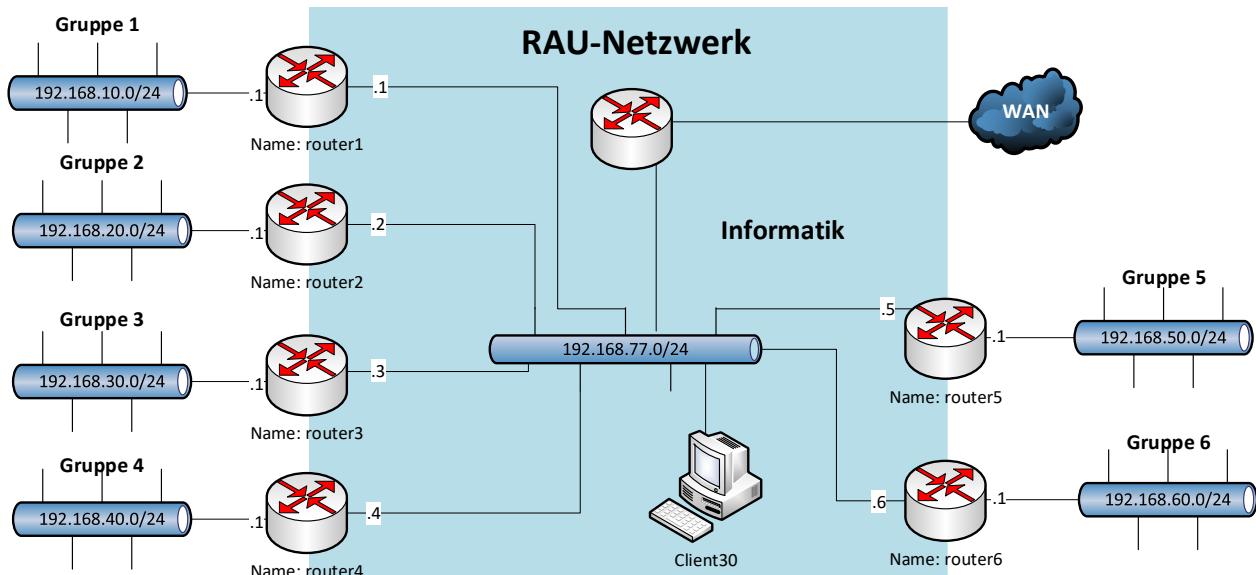
A1	Es wird eine neue Installation des Windows Server vorgenommen. Auf diesem Server läuft der Dienst Hyper-V und Remotedesktop wird aktiviert.	
	 Windows Server 2012 R2	Kapitel: 22 Servervirtualisierung mit Hyper-V
A2	Installieren und konfigurieren Sie srv01 (Englisch). Benutzen Sie dazu Ihre Installationsanleitung aus der Systemdokumentation. Zusätzlich wird der Fileserver-Dienst hinzugefügt. Dieser besteht aus einem „Öffentlich“ Ordner, der im Netzwerk freigegeben wird. Für den Zugriff wird ein Benutzer „Besucher“ mit Passwort „DRbsadS317.“ im Active Directory definiert. Auf dem Ordner hat der Benutzer Lese- und Schreibrecht.	
A3	Installieren und konfigurieren Sie srv02 (Englisch). Benutzen Sie dazu wieder Ihre Installationsanleitung aus der Systemdokumentation.	
A4	Installieren Sie Ubuntu Server (Englisch) auf srv03.	
Z1	Um auf den Server srv03 von extern zugreifen zu können, braucht es den Dienst SSH. Installieren / Konfigurieren Sie SSH und versuchen von einem Windows Client mit dem Tool PuTTY auf den Server zu verbinden.	
A5	Installieren Sie Windows auf dem Testclient „testClient01“. Diese Maschine dient nur zu Testzwecken und hat sonst keine Verwendung. Testen Sie mit diesem Client Ihren File-Dienst.	
A6	Installieren Sie Ubuntu auf dem testClient02 und aktivieren Sie Remotedesktop.	
Z2	Verbinden Sie vom Ubuntu testClient02 mittels SSH auf den Ubuntu Server.	

2.8 Internet

Wir bauen nun ein „Internet“ Schritt für Schritt auf.

2.8.1 Öffentliche Website

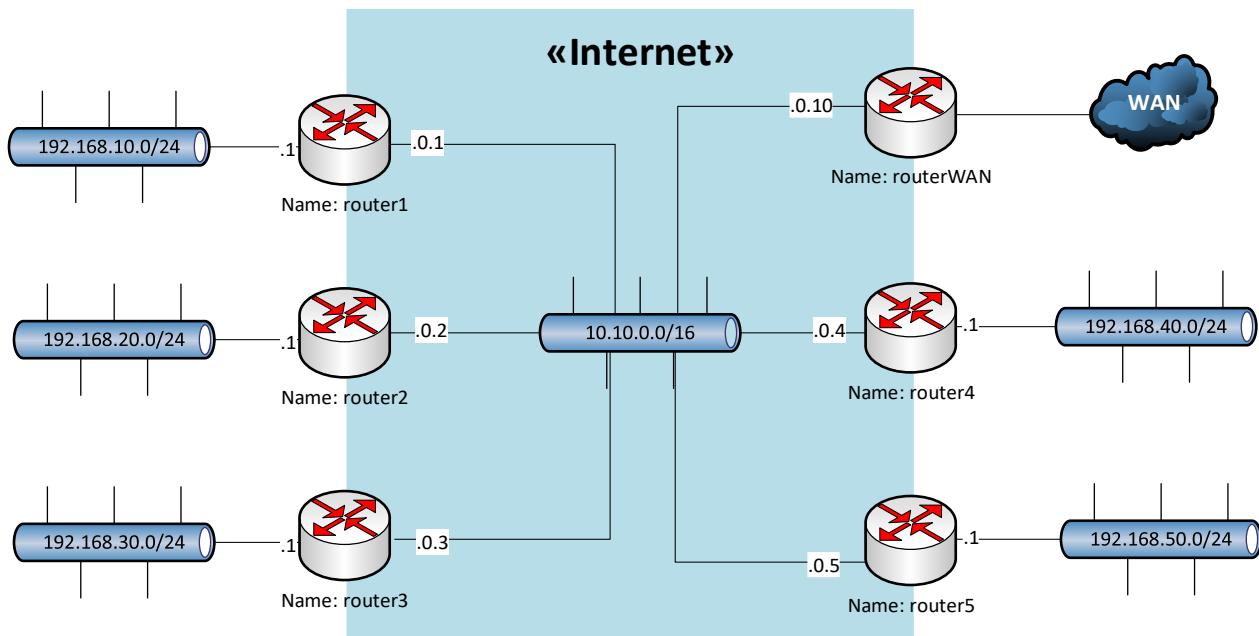
Zuerst werden die lokalen Dienste ausserhalb des Netzes bereitgestellt. Das bedeutet, dass unsere Website auch vom RAU-Netzwerk aufgerufen werden kann.



A1	<p>Port Forwarding</p> <p>Lesen Sie den Artikel de.wikipedia.org/wiki/Portweiterleitung. Die Aufgabe ist es nun, dass „Port Forwarding“ auf dem Router zu konfigurieren. Wie immer, machen Sie sich mit dem Usermanual des Routers vertraut.</p> <p>Anschliessend müssen Sie den Port 80 (http) des Routers router1 (Gruppe 1) auf den Server srv02 (Gruppe 1) umleiten. Wenn der Client client30 im RAU-Netzwerk im Webbrowser die IP 192.168.77.1 eingibt, erscheint die Webseite des srv02 (Gruppe 1). Die gleiche Konfiguration gilt auch für die Gruppe 2. Hier wird jedoch Client client30 die IP 192.168.77.2 verwenden um die Webseite des Servers srv02 (Gruppe 2) zu öffnen.</p>
A2	<p>Testing</p> <p>Erstellen Sie ein Testprotokoll und testen Sie die Portweiterleitung für alle Gruppen:</p> <ul style="list-style-type: none"> • Client30 öffnet Website der Gruppe 1 (IP 192.168.77.1) • Client30 öffnet Website der Gruppe 2 (IP 192.168.77.2) • Client30 öffnet Website der Gruppe 3 (IP 192.168.77.3) • ...

2.8.2 Routing-Table

Unser Internet wird über statische Routing-Tables aufgebaut. Jede Gruppe erstellt Ihre eigene Routingtabelle. Wenn alle Gruppen die Tabelle korrekt konfiguriert haben, können vom lokalen Netzwerk die Website der anderen Gruppen geöffnet werden.

**A1 Chief of Internet**

Bestimmen Sie den Chef des Internets und seine zwei Assistenten. Der Chef ist verantwortlich dafür, ...

- ... dass jedes Gruppennetz über einen Switch miteinander verbunden ist.
- ... dass die Netzadressen der Gruppen korrekt sind.
- ... das unser Internet über den Router (routerWAN) mit dem richtigen „Internet“ verbunden ist.

A2 Routing Table

Jede Gruppe erstellt Ihre Routing Table.

Netzadresse	Subnetzmaske	Gateway
192.168.80.0		
...		
0.0.0.0		

Modulunterlagen

[F1]	Was bedeutet der Eintrag 0.0.0.0 in der Routing Table und wozu dient diese Adresse?
A3	Konfiguration Konfigurieren Sie die Routing Table auf Ihrem Router.
A4	Testing Überprüfen Sie mit einem Testprotokoll, ob die ... <ul style="list-style-type: none">• ... Website www.r-au.ch angezeigt wird.• ... Website http://192.168.10.2 angezeigt wird.• ... Website http://192.168.20.2 angezeigt wird.• ... Website http://192.168.30.2 angezeigt wird.• ... Website http://192.168.40.2 angezeigt wird.• ... Website http://192.168.50.2 angezeigt wird.

2.9 VLAN

2.9.1 Aufbau und Konfiguration

[F1]	<p>Theorie VLAN</p> <p>Lesen Sie den Artikel de.wikipedia.org/wiki/Virtual_Local_Area_Network und beantworten Sie die folgenden Fragen:</p> <p>Wozu wird VLAN eingesetzt? Nennen Sie drei Beispiele.</p> <p>Wie funktionieren die portbasierten VLANs?</p> <p>Wie sind die Tagged VLANs aufgebaut?</p>
A1	<p>Konfiguration VLAN</p> <p>Es wird ein VLAN auf dem Layer-3 Switch konfiguriert. Alle VLANs sind untagged. Die Ports 1-2 gehören zum VLAN 1, also zum Default VLAN. Die Ports 3-5 werden dem VLAN 2 und die Ports 6-8 werden dem VLAN 3 zugeordnet.</p> <p>Als erstens werden die VLANs erstellt. Dann können Sie unter „Port To VLAN“ die Zuordnungsmatrix erstellen und den einzelnen VLANs die Ports zuordnen.</p>

2.9.2 Testing und Ausmessung

A1	<p>Ping-Testing</p> <p>Überprüfen Sie Ihre Konfiguration. Dazu schliessen Sie die Computer an die einzelnen VLAN-Netze an. Mithilfe des „Ping“ überprüfen Sie die Erreichbarkeit der Clients. Sind die Computer im gleichen VLAN-Netz, so ist der Ping erfolgreich. Sind die Computer in verschiedenen VLANs, so verlieren Sie die Pakete des Pings.</p> <p>Es wird ein Testprotokoll erstellt und die verschiedenen Möglichkeiten werden getestet.</p>
Z1	<p>DHCP-Testing</p> <p>Am VLAN 2 wird ein DHCP-Service mit der Netzadresse 192.168.35.0/24 betrieben. Das VLAN 3 wird durch einen weiteren DHCP-Service mit Netzadresse 192.168.68.0/24 bedient. Zum Testen werden die Computer an die entsprechenden Ports angeschlossen und die dynamische IP mithilfe von „ipconfig“ überprüft. An den Ports 3-5 erhält der Client die IP 192.168.35.x und an den Ports 6-8 wird die IP auf 192.168.68.y gesetzt. Halten Sie die Ergebnisse in einem Testprotokoll fest.</p>

3 Services

3.1 Lernjournal

3.1.1 Auftrag

Im Rahmen des Moduls Server-Dienste kommen Sie in den Genuss einiger Theorieblöcke, welche anschliessend mit praktischen Übungen vertieft werden. Parallel zur Theorie wird Ihnen aus methodischen Gründen bewusst kein Skript abgegeben. Sie sind in diesem Modul verpflichtet, die wesentlichen Elemente aus der Theorie und die Erkenntnisse aus den Übungen in einer entsprechenden Dokumentation elektronisch festzuhalten. Ziel dieser Dokumentation ist es, das gelernte für sich selbst nochmals festzuhalten und später nachvollziehen zu können. Das vorliegende Dokument regelt die Vorgaben und Rahmenbedingungen an die zu erstellende Dokumentation.

3.1.2 Formale Anforderungen

Die zu erstellende elektronische Dokumentation hat alle Anforderungen an den Aufbau und die Gestaltung eines professionellen Dokumentes zu erfüllen, wie dies im Rahmen des Moduls IN1 behandelt wurde. Neben den Vorgaben an die Gliederung und den Inhalt (vgl. unten), weist die Dokumentation zusätzlich folgende Elemente auf:

- Titelblatt
- Inhaltsverzeichnis
- Glossar (Erklärung der Abkürzungen und Fremdwörter) im Anhang
- Index (Auflistung der wichtigsten Begriffe mit Angabe der Seitenzahl) im Anhang
- Nummerierung der Tabellen und Abbildungen und entsprechende Verzeichnisse im Anhang

3.1.3 Quellenangabe

Es ist zulässig (aber nicht immer sinnvoll), Texte aus Quellen wie dem Internet oder aus Büchern zu übernehmen. In diesen Fällen muss aber die Quelle angegeben werden. Die wird am einfachsten mittels einer nummerierten Aufzählung der Quellen vorne im Dokument erzielt, wobei anschliessend im Text am Ende eines zitierten Absatzes (z.B. in eckigen Klammern [x]) auf die entsprechende Quelle referenziert wird.

Beispiel Internet und Buch:

Wikipedia: OSI-Modell. Abgerufen am 18.10.2021 unter <http://de.wikipedia.org/wiki/OSI-Modell>

„Das OSI-Modell² (englisch Open Systems Interconnection Model) ist ein Referenzmodell ...“

Andrew S. Tanenbaum, David J. Wetherall: Computernetzwerk.

² Zitat <http://de.wikipedia.org/wiki/OSI-Modell> abgerufen am 18.10.2021

3.2 Systemdokumentation

3.2.1 Auftrag

Im Rahmen des Moduls Server-Dienste installieren und konfigurieren Sie einige Systeme. Es gilt nun eine Dokumentation zu erstellen, die festhält, welche Einstellungen und Entscheidungen getroffen wurden. Die Dokumentation muss alle Informationen beinhalten, die es einem ausgebildeten Informatiker erlauben das System exakt nachzubilden. Zudem werden der Systemdokumentation Testprotokolle der einzelnen Services hinzugefügt.

3.2.2 Formale Anforderungen

Die zu erstellende elektronische Dokumentation hat alle Anforderungen an den Aufbau und die Gestaltung eines professionellen Dokumentes zu erfüllen, wie dies im Rahmen des Moduls OK behandelt wurde. Neben den Vorgaben an die Gliederung und den Inhalt (vgl. unten), weist die Dokumentation zusätzlich folgende Elemente auf:

- Titelblatt
- Inhaltsverzeichnis
- Glossar (Erklärung der Abkürzungen und Fremdwörter) im Anhang
- Index (Auflistung der wichtigsten Begriffe mit Angabe der Seitenzahl) im Anhang
- Nummerierung der Tabellen und Abbildungen und entsprechende Verzeichnisse im Anhang

3.2.3 Quellenangabe

Es ist zulässig (aber nicht immer sinnvoll), Texte aus Quellen wie dem Internet oder aus Büchern zu übernehmen. In diesen Fällen muss aber die Quelle angegeben werden. Die wird am einfachsten mittels einer nummerierten Aufzählung der Quellen vorne im Dokument erzielt, wobei anschliessend im Text am Ende eines zitierten Absatzes (z.B. in eckigen Klammern [x]) auf die entsprechende Quelle referenziert wird.

Beispiel Internet und Buch:

Wikipedia: OSI-Modell. Abgerufen am 18.10.2021 unter <http://de.wikipedia.org/wiki/OSI-Modell>

„Das OSI-Modell³ (englisch Open Systems Interconnection Model) ist ein Referenzmodell ...“

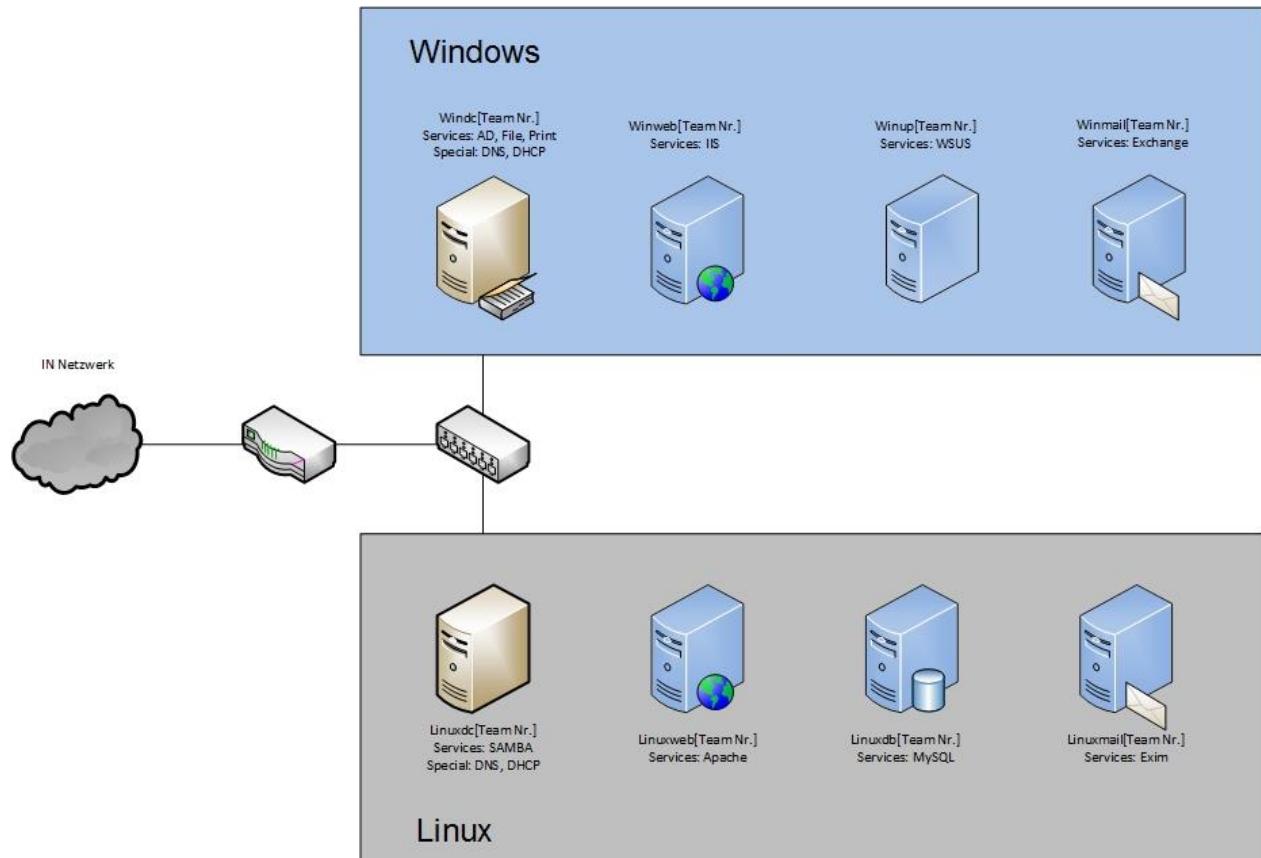
Andrew S. Tanenbaum, David J. Wetherall: Computernetzwerk.

³ Zitat <http://de.wikipedia.org/wiki/OSI-Modell> abgerufen am 18.10.2021

3.3 Soll Zustand

Im Verlauf des Moduls werden Sie eine Infrastruktur installieren, welche die wichtigsten Serverdienste beinhaltet. Im Folgenden soll die Infrastruktur kurz gezeigt werden.

Es handelt sich dabei um zwei Clients, auf denen die jeweiligen Server installiert werden.



Zusätzlich zu den oben gezeigten Servern wird ein virtueller Client installiert, um verschiedene Dienste zu testen. Wichtig ist, dass Sie die virtuellen Systeme nicht direkt mit dem RAU Netzwerk verbinden. Dienste wie DHCP und AD können sonst zu ungewünschten Auswirkungen führen. Stellen Sie daher sicher, dass Ihre Test-Infrastruktur hinter dem Router läuft.

3.4 Vorbereitung der Infrastruktur

Bevor wir unsere Dienste installieren und konfigurieren müssen wir die virtuelle Umgebung aufbauen.

3.4.1 Hyper-V

A1	Aktivieren Sie Hyper-V auf Ihrem PC, um später virtuelle Maschinen erstellen zu können.		
A2	Erstellen Sie einen virtuellen Switch, der mit dem Netzwerk verbunden ist.  Open-book Windows Server 2012 R2: Kapitel 22		
A3	Erstellen Sie für jeden der oben gezeigten Server eine virtuelle Maschine und benennen Sie sie richtig. Ein Teammitglied kann die Windows-Server übernehmen und das andere Teammitglied die Linux-Server.		

3.4.2 Server VM

A1	Installieren Sie auf den VMs die aktuellste Windows Server-Version mit GUI. Installieren Sie parallel dazu auf den Linux VMs die aktuelle Server-Version von Ubuntu. Erstellen Sie neben den Standardbenutzern einen Benutzer mit dem Namen „admin-grp[Gruppennummer]“		
A2	Stellen Sie sicher, dass Sie sich mit allen Servern mittels RDP bzw. SSH verbinden können.  Open-book Linux: Kapitel 21		
A3	Benutzen Sie PuTTY auf Ihrem Client und erzeugen Sie einen SSH Key für Ihren Benutzer. Stellen Sie sicher, dass Sie kein Passwort mehr eingeben müssen bei der Verbindung mit SSH.		
A4	Legen Sie alle nötigen IPs fest. Vergessen Sie nicht den Standardgateway.  Tipp Halten Sie diese Entscheidungen direkt in der Systemdokumentation fest.		
A5	Konfigurieren Sie bei allen Servern eine feste IP, welche nicht über DHCP bezogen wird. Achten Sie darauf, dass Sie über den Standard-Gateway eine Internetverbindung herstellen können. Die DNS-Einträge werden später ergänzt.  Open-book Linux: Kapitel 15		

3.4.3 Client VM

Um die bereitgestellten Dienste später Testen zu können, erfüllen Sie folgende Aufgaben.

A1	Erstellen Sie auf jedem Client eine zusätzliche virtuelle Maschine.
A2	Installieren Sie auf beiden Systemen eine aktuelle Windows Client Version.
Z1	Erstellen Sie drei weitere virtuelle Maschinen mit einem Windows Client OS.
Z2	Testen Sie, ob Sie in der Lage sind eine VM von einem Client auf den anderen zu kopieren.

3.5 Active Directory

Das Active Directory bietet die Möglichkeit, eine Windows Domäne zu erstellen und zentral zu verwalten. Es werden Benutzer- und Computerkonten verwaltet, um sie authentifizieren zu können. Ein wichtiges Tool darin sind die Gruppenrichtlinien. Mit dessen ist man in der Lage, unterschiedlichste Einstellungen über sogenannte administrative Vorlagen (Richtlinien) oder bevorzugte Einstellungen (Preferences) vorzunehmen. Dabei wird zwischen Computer- und Benutzerkonfiguration unterschieden.

3.5.1 Installation

A1	Verbinden Sie sich mit dem windc Server.	
	 Tipp	Dies ist auch direkt über die Hyper-V Konsole oder RDP möglich.
A2	Kontrollieren Sie den Servernamen und die IP. Ist der Server erst einmal als Domain Controller eingerichtet, dürfen diese Einstellungen nicht mehr geändert werden.	
A3	Bei der Anmeldung öffnet sich immer der Server Manager. Dieser kann für die Verwaltung vieler Server verwendet werden. Benutzen Sie nun den Server Manager um den Server folgende Features und Rollen hinzuzufügen. <ul style="list-style-type: none"> • AD DS • DNS • DHCP • Druckerverwaltung 	
	 Open-book	Windows Server 2012 R2: Kapitel 8
A4	Für gewisse Rollen-Installationen muss der Server neu gestartet werden. Öffnen Sie den Server Manager nach dem Neustart, wird Ihnen eine Meldung im Benachrichtigungsfeld gezeigt. Benutzen Sie diese, um den Server zum Domaincontroller herauf zu stufen.	
A5	Erstellen Sie eine neue Gesamtstruktur und geben Sie ihr den passenden Namen: internal.gruppe[Nr.].tech	

3.5.2 Konfiguration

A1	<p>Erstellen Sie folgende Struktur als Organisationseinheiten (OU).</p> <ul style="list-style-type: none"> • internal.gruppe01.tech <ul style="list-style-type: none"> ◦ RAU <ul style="list-style-type: none"> ▪ Mechanik ▪ Informatik ▪ Konstruktion ▪ Elektronik ▪ Verwaltung 				
	<table border="1"> <tr> <td></td><td>Tipp</td></tr> <tr> <td colspan="2">Verwenden Sie immer den Server Manager.</td></tr> </table>		Tipp	Verwenden Sie immer den Server Manager.	
	Tipp				
Verwenden Sie immer den Server Manager.					
A2	Definieren Sie separate OU's für Clients sowie die Benutzer. Überlegen Sie sich für Ihre Lösung eine Begründung.				
A3	Erstellen Sie für alle Lernenden im BLJ einen Benutzer unter der OU Informatik.				
A4	Erstellen Sie in der OU Informatik eine Gruppe mit dem Namen GRP-Informatik.				
A5	Fügen Sie die Informatik-Lernenden in die erstellte Gruppe hinzu.				
A6	Stellen Sie mittels einer GPO sicher, dass die GRP-Informatik lokale Administratoren-Rechte auf jedem Client hat.				
A7	Definieren Sie die Startseite von Microsoft Edge sowie Internet Explorer für alle Benutzer auf www.r-au.ch .				
A8	Erstellen Sie eine Freigabe, in der sämtliche Benutzer Zugriff haben. Verbinden Sie über GPO diese Freigabe als Netzlaufwerk.				
Z1	Fügen Sie mittels GPO allen Informatik-Lernenden auf dem Desktop eine Verknüpfung für die Benutzerdateien (User folder) hinzu.				
Z2	<p>Erstellen Sie eine neue Freigabe „Home“, welche in der Netzwerk-Übersicht nicht ersichtlich ist.</p> <p>Definieren Sie die Freigaben- und NTFS-Berechtigungen gemäss Anweisung im Kursnotizbuch:</p> <table border="1"> <tr> <td></td><td>Notizbuch</td><td>Seite «Berechtigung»</td></tr> </table> <p>Richten Sie jetzt eine GPO ein, welches für jeden Benutzer einen persönlichen Ordner in der «Home»-Freigabe erstellt, welcher nach dem Benutzernamen benannt ist. Dieser Ordner soll ebenfalls als Netzlaufwerk verbunden werden.</p>		Notizbuch	Seite «Berechtigung»	
	Notizbuch	Seite «Berechtigung»			

3.6 DHCP

Für unsere Clients wird ein DHCP Server genutzt.

A1	Schalten Sie, wenn nötig, den DHCP-Server des Windows AD-Server aus.		
A2	Erstellen Sie auf dem linuxdc Server einen DHCP Pool für Ihr Subnetz.		
	 Tipp Vergessen Sie nicht, später den DNS Server anzupassen.		
	 Open-book		Linux: Kapitel 17.3

3.7 DNS

[F1]	Um das DNS System zu verstehen, lesen Sie den Wikipedia-Artikel dazu. Wichtig ist, dass Sie folgende Fragen beantworten können: <ul style="list-style-type: none">• Wie und wo werden die Informationen gespeichert?• Wenn ich eine Internetseite öffnen will, wie findet mein Client die IP Adresse des Webservers heraus?• Welche verschiedenen Arten von Einträgen können von einem DNS Server verwaltet werden?		
A1	Erstellen Sie für alle Server in Ihrem Netzwerk einen DNS Eintrag.		
	 Open-book		Windows Server 2012 R2: Kapitel 9.1
A2	Stellen Sie sicher, dass der IIS Webserver auch über web.ihredomain.tech erreichbar sein wird.		
A3	Stellen Sie sicher, dass andere Mailserver die IP Ihres zukünftigen Windows Mailservers finden.		
A4	Erstellen Sie für Ihr Netzwerk eine Reverse Lookup Zone.		
A5	Für was wird eine Reverse Lookup Zone benötigt?		
A6	Erstellen Sie dieselbe Konfiguration auf Ihrem linuxdc. Verwenden Sie für die Einträge von A2+3 aber die Linux Server.		
	 Open-book		Linux: Kapitel 20
Z1	Erstellen Sie auf einer eigenen VM einen DNS Server für die Top Level Domain (TLD) .tech. Diese enthält die Nameservereinträge für alle Domains der verschiedenen Gruppen.		
	 Tipp Sie haben schon einige VMs vielleicht müssen Sie nicht noch einmal das OS installieren.		

3.8 Samba

Im Folgenden repetieren wir einen Teil aus M305. Wir nutzen jedoch noch weitere Funktionen von Samba.

A1	Erstellen Sie für alle BLJ Lernenden einen Benutzer für SAMBA.		
		Openbook	Linux: Kapitel 17.7
A2	Erstellen Sie je eine Freigabe für Applikationsentwickler und Systemtechniker.		
A3	Binden Sie eine beliebige Freigabe Ihres Windows Servers ein.		
A4	Erstellen Sie mit Hilfe dieser Anleitung einen zusätzlichen AD Domain Controller für Ihre bereits erstelle Domäne auf Linux-Basis.		
		Web	Samba-Wiki
A5	Testen Sie nun, ob Sie sich mit einem Client über Samba als Domänencontroller anmelden können.		
Z1	Teilen Sie einen Drucker, damit Sie den Server als Printserver verwenden können.		

3.9 Webserver

Auch hier werden gewisse Teile wiederholt. Es sollte jedoch jeder Informatiker in der Lage sein, einen Webserver bereit zu stellen.

3.9.1 IIS

IIS kennen Sie schon von der Fachausbildung Netzwerktechnik.

A1	Stellen Sie eine neue Seite über den IIS Server bereit.	
	 Open-book	Windows Server 2012 R2: Kapitel 17

3.9.2 Apache

A1	Installieren Sie Apache, falls dies nicht bereits der Fall ist.	
A2	Konfigurieren Sie den Server so, dass Sie wieder Ihre Seite hosten können.	
	 Open-book	Linux: Kapitel 19.1
A3	Um das Konzept der virtuellen Hosts anzuwenden, stellen Sie ein zweites Graffiti-Projekt mit einer neuen Subdomain online.	
Z1	Stellen Sie sicher, dass PHP korrekt installiert ist und testen Sie dies mit der Funktion <code>phpinfo()</code> .	
Z2	Sichern Sie Ihre Installation mit Hilfe einiger Tipps.	
	 Web	Apache-Security-Tips

3.10 Datenbanken

3.10.1 MySQL

A1	Installieren Sie den MySQL Server mit Hilfe des Paketmanagers.		
A2	Installieren Sie nun phpMyAdmin. Unter Ubuntu ist dies mit dem Paketmanager möglich.		
A3	Erstellen Sie mit Hilfe von phpMyAdmin eine neue Datenbank.		
A4	Erstellen Sie nun eine andere Datenbank nur über die Konsole. Die Datenbank soll mindestens zwei Tabellen besitzen.		
		Open-book	Linux: Kapitel 19.2
A5	Stellen Sie sicher, dass sie auch von einem anderen Server oder Client auf die MySQL Installation zugreifen können über die Konsole.		
Z1	Erstellen Sie eine Datenbank, welche die Informationen zu Ihrer Gruppe speichert. Mindestens werden Namen und Adresse gespeichert. Benutzen Sie mindestens zwei Tabellen.		
Z2	Erstellen Sie einen zusätzlichen Adminbenutzer, der sämtliche Rechte hat.		
Z3	Erstellen Sie einen Applikationsbenutzer, der nur SELECT, INSERT und UPDATE ausführen darf.		
Z4	Lesen Sie Ihre Informationen aus und verändern bestimmte Werte.		

3.10.2 Microsoft SQL

A1	Installieren Sie die aktuelle SQL Express Version.		
A2	Installieren Sie das SQL Management Studio für die Verwaltung der Datenbanken.		
A3	Melden Sie sich am Management Studio an und erstellen Sie eine neue Datenbank.		
A4	Machen Sie sich mit den Möglichkeiten von PowerShell innerhalb von Microsoft SQL vertraut.		
		Web	<u>SQL PowerShell</u>
A5	Erstellen Sie jetzt eine neue Datenbank nur mit PowerShell. Die Datenbank soll mindestens zwei Tabellen besitzen.		
A6	Stellen Sie sicher, dass sie auch von einem anderen Server oder Client auf die SQL Installation zugreifen können.		
A7	Erstellen Sie einen zusätzlichen Datenbank Admin-Benutzer, der sämtliche Rechte hat.		
Z1	Erstellen Sie einen Applikationsbenutzer, der nur SELECT, INSERT und UPDATE ausführen darf.		

3.11 WSUS

Windows Server Update Service

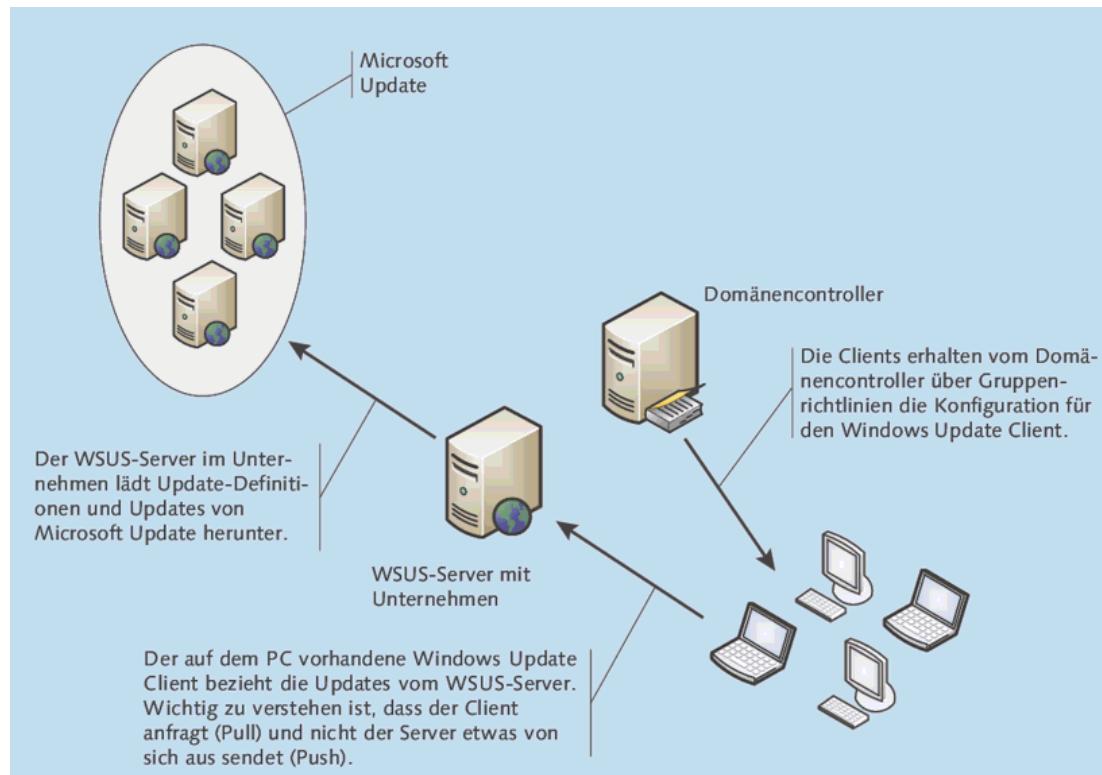


Abbildung 1: Quelle - Galileo Windows Server 2012 R2

A1	Fügen Sie Ihrem Server eine zweite Disk mit einer Grösse von 40 GB hinzu. Definieren Sie die Disk mit fixer Grösse.		
A2	Installieren Sie gemäss Demo die WSUS-Rolle auf Ihrem Windows Server.		
		Open-book	Windows Server 2012 R2: Kapitel 14.3
	Wählen Sie in der Sprache-, Produkte- und Klassifizierungs-Auswahl nur folgendes:		
	<ul style="list-style-type: none"> - Sprache: Englisch - Produkte: NUR aktuelles Windows - Klassifizierung: Critical Updates, Security Updates 		
A3	Erstellen Sie eine Computer-Gruppe und stellen Sie anschliessend sicher, dass neue Computer mittels Gruppenrichtlinie in WSUS zugewiesen werden.		
A4	Erstellen Sie die «Automatic Approvals» Regel und führen Sie diese danach aus.		

Modulunterlagen

A5	<p>Erstellen Sie eine neue GPO für die WSUS-Einstellungen für Clients. Den Einstellungs-Bereich dafür finden Sie unter <Computer Configuration – Administrative Templates – Windows Components – Windows Updates>. Zwingende Einstellungen darin sind:</p> <ul style="list-style-type: none">- Configure Automatic Updates- Specify intranet Microsoft update service location- Enable client-side targeting <p>Überlegen Sie sich, was für Einstellungen in einem Unternehmen Sinn machen würde. Diese Vorschläge werden wir im Plenum besprechen.</p>
A6	<p>Wenden Sie die Richtlinie nach unserer Besprechung auf die entsprechende OU an, wo die Clients liegen.</p>

3.12 Mailserver

3.12.1 Exchange

Im Folgenden werden Sie die aktuellste Version von Microsoft Exchange-Server installieren, konfigurieren und soweit bereitstellen, damit Sie erfolgreich Mails versenden können.

A1	Installation von aktuellstem Windows Server-Betriebssystem. Die Mindestanforderungen sind: <ul style="list-style-type: none"> - CPU: 2 Cores - RAM: mind. 8 GB (fixe Grösse) - Pagefile: mind. 9 GB - 2 Disks: 1x 60 GB (System), 1x 10 GB (Queue) 		
A2	Stellen Sie sicher, dass alle Voraussetzungen erfüllt werden (Updates installieren, UCMA usw.)		
A3	Führen Sie die Grund-Installation mit Hilfe der OneNote-Anleitung durch.		
		OneNote	Seite «Exchange»
		Tipp	Das Setup prüft alle Voraussetzungen vor der Installation.
A4	Erstellen Sie für alle Gruppenmitglieder ein Postfach und testen Sie dieses über Outlook Web Access.		
A5	Installieren Sie auf den Test-Clients die aktuellste Outlook-Version. Fügen Sie anschliessend das Mail-Konto pro Gruppenmitglieder hinzu. → Alle Einstellungen sollten Automatisch erkannt werden (sogenanntes <i>Autodiscover</i>)		

Modulunterlagen

Z1	<p>Stellen Sie sicher, dass Sie auch Mails zu anderen Gruppen senden können.</p> <table border="1"> <tr> <td></td><td>Tipp Sie benötigen nun einen zentralen DNS Server, der die einzelnen Gruppe-Domains verwaltet.</td></tr> </table> <p>Rahmenbedingungen:</p> <ul style="list-style-type: none"> - Separater Client mit aktuellstem Windows Server VM <ul style="list-style-type: none"> o Fixe IP im IN-Netzwerk - DNS Server konfigurieren - Alle Gruppen DNS-Domänen als DNS-Zonen erstellen <ul style="list-style-type: none"> o Ressourcen-Einträge pro DNS-Zone erstellen - Router konfigurieren, damit der Mail-Verkehr sichergestellt ist 		Tipp Sie benötigen nun einen zentralen DNS Server, der die einzelnen Gruppe-Domains verwaltet.
	Tipp Sie benötigen nun einen zentralen DNS Server, der die einzelnen Gruppe-Domains verwaltet.		

3.12.2 Exim

A1	Erstellen Sie für Ihren Linux Mailserver eine Subdomain.		
A2	Installieren Sie Exim mit Hilfe des Paketmanagers.		
A3	Konfigurieren Sie Exim gleich (wo möglich) dem Exchange Server. Die Domain ist jedoch eine andere.		
		Open-book	Linux: Kapitel 18

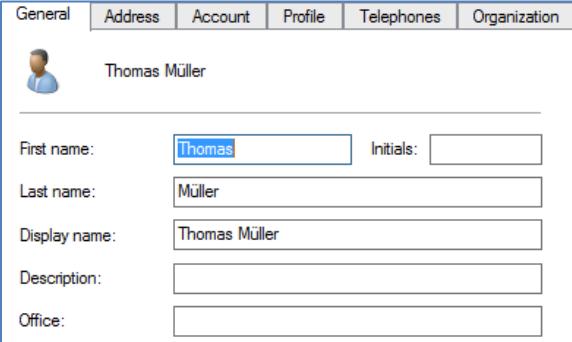
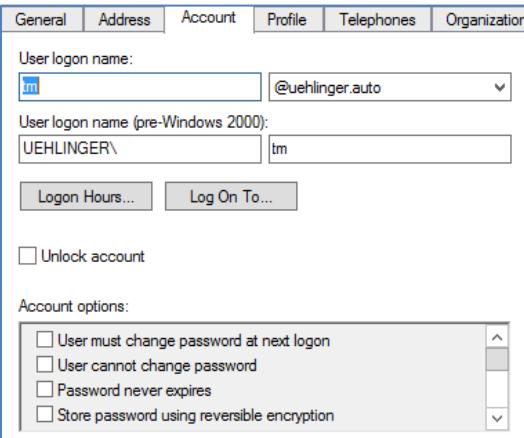
3.13 Scripting

Script-Sprachen wie Linux Shell Scripts und Windows PowerShell können sehr mächtige Werkzeuge sein. Im Alltag gibt es viele Abläufe, die täglich oder wöchentlich ausgeführt werden müssen. Werden die Abläufe per Hand ausgeführt, ist das sehr ineffizient. Gute Administratoren versuchen deshalb so viel wie möglich zu automatisieren. Es muss sichergestellt werden, dass Fehler bei der Ausführung erkannt und behoben werden können.

	Openbook	Linux: Kapitel 19.2
	Openbook	Windows Server 2012 R2: Kapitel 23

3.13.1 Aufgaben

Lösen Sie die folgenden Aufgaben auf beiden Betriebssystemen, sofern dies möglich ist.

A1	<p>Erstellen Sie mit PowerShell einen AD-Benutzer, welcher in der OU Informatik abgelegt ist.</p> <p>Die Anforderung ist, dass der Benutzer aktiv ist und bei der Erstellung ein Kennwort vergeben werden muss (Kennwort nicht vordefiniert). Außerdem sollen mindestens folgende Attribute abgefüllt sein:</p>  
A2	Fügen Sie den neuen Benutzer mittels PowerShell zu zwei AD-Gruppen hinzu.

Modulunterlagen

A3	Erstellen Sie mittels Exchange Management Shell für den erstellen Benutzer ein Postfach auf dem Exchange.
A4	Erstellen Sie ein Script, welches eine neue Webseite bereitstellt. Es muss also ein Verzeichnis angelegt werden, ein virtueller Host konfiguriert und ein DNS Eintrag erstellt werden.

3.14 Client Security

Es folgen verschiedene Fragen zum Thema Security. Sie sollen die Grundlagen für eine aktive Diskussion schaffen, bei der alle bezüglich der Security und möglichen Massnahmen sensibilisiert werden.

3.14.1 Allgemeine Diskussion und Fragen

[F1]	Was ist Malware?
[F2]	Welche Arten von Malware existieren oder welche Ziele werden damit verfolgt?
[F3]	Wie verbreitet sich Malware?
[F4]	Welche Malware oder welche Art von Malware ist gerade sehr aktuell?
[F5]	Was waren Ihrer Meinung nach die schwerwiegendsten Sicherheitslücken der letzten Jahre?
[F6]	Welche weiteren Begriffe bezüglich Malware und Security kennen Sie oder wollen Sie besser kennen lernen?
[F7]	Wie infiziert denn Malware einen PC?
[F8]	Wie kann man sich vor Malware schützen?
[F9]	Kennen Sie andere spezielle Geschichten oder Angriffe aus IT Security?
[F10]	Was konnten Sie bis jetzt noch nicht sagen?
[F11]	Wie funktioniert Anti Viren Software überhaupt?
	Web http://www.melani.admin.ch

3.14.2 Präsentation Virus

Um uns genauer mit Schadsoftware auseinander zu setzen hält jede Gruppe eine kurze Präsentation über eine Schwachstelle bzw. einen Virus.

A1	<p>Dauer: 5min. Vorbereitungszeit: 1h Minimaler Inhalt:</p> <ul style="list-style-type: none">• Genutzte Sicherheitslücke / Technische Beschreibung• Entdeckung• Auswirkungen• Gegenmassnahmen und Prävention
----	--