

Familienname, Vorname (bitte durch eine Leerspalte trennen)

[illegible]

			Berufsnummer
--	--	--	--------------

IHK-Nummer

[illegible]

5	5		1	1	9	7								
---	---	--	---	---	---	---	--	--	--	--	--	--	--	--

Sp. 1-2

Sp. 3-6

Sp. 7-9

Sp. 10-14

Termin: Mittwoch, 25. April 2018

IHK

1197

1 Ganzheitliche Aufgabe I Fachqualifikationen

Fachinformatiker
Fachinformatikerin
Systemintegration

5 Handlungsschritte
90 Minuten Prüfungszeit
100 Punkte

Bearbeitungshinweise

1. Der vorliegende Aufgabensatz besteht aus insgesamt 5 Handlungsschritten zu je 25 Punkten.

In der Prüfung zu bearbeiten sind 4 Handlungsschritte, die vom Prüfungsteilnehmer frei gewählt werden können.

Der nicht bearbeitete Handlungsschritt ist durch Streichung des Aufgabentextes im Aufgabensatz und unten mit dem Vermerk „Nicht bearbeiteter Handlungsschritt: Nr. ... „ an Stelle einer Lösungsniederschrift deutlich zu kennzeichnen. Erfolgt eine solche Kennzeichnung nicht oder nicht eindeutig, gilt der 5. Handlungsschritt als nicht bearbeitet.

2. Füllen Sie zuerst die **Kopfzeile** aus. Tragen Sie Ihren Familiennamen, Ihren Vornamen und Ihre Prüflings-Nr. in die oben stehenden Felder ein.
3. Lesen Sie bitte den **Text** der Aufgaben ganz durch, bevor Sie mit der Bearbeitung beginnen.
4. Halten Sie sich bei der Bearbeitung der Aufgaben genau an die **Vorgaben der Aufgabenstellung** zum Umfang der Lösung. Wenn z. B. vier Angaben gefordert werden und Sie sechs Angaben anführen, werden nur die ersten vier Angaben bewertet.
5. Tragen Sie die frei zu formulierenden **Antworten dieser offenen Aufgabenstellungen** in die dafür lt. Aufgabenstellung vorgesehenen Bereiche (Lösungszeilen, Formulare, Tabellen u. a.) des Arbeitsbogens ein.
6. Sofern nicht ausdrücklich ein Brief oder eine Formulierung in ganzen Sätzen gefordert werden, ist eine **stichwortartige Beantwortung** zulässig.
7. Verwenden Sie nur einen Kugelschreiber und schreiben Sie deutlich und gut lesbar. Ein nicht eindeutig zuzuordnendes oder **unleserliches Ergebnis** wird als **falsch** gewertet.
8. Zur Lösung der Rechenaufgaben darf ein nicht programmierter, netzunabhängiger **Taschenrechner** ohne Kommunikationsmöglichkeit mit Dritten verwendet werden.
9. Wenn Sie ein **gerundetes Ergebnis** eintragen und damit weiterrechnen müssen, rechnen Sie (auch im Taschenrechner) nur mit diesem gerundeten Ergebnis weiter.
10. Für **Nebenrechnungen/Hilfsaufzeichnungen** können Sie das im Aufgabensatz enthaltene Konzeptpapier verwenden. Dieses muss vor Bearbeitung der Aufgaben herausgetrennt werden. Bewertet werden jedoch nur Ihre Eintragungen im Aufgabensatz.

Nicht bearbeiteter Handlungsschritt ist Nr.

Wird vom Korrektor ausgefüllt!

Bewertung

Für die Bewertung gilt die Vorgabe der Punkte in den Lösungshinweisen. Für den abgewählten Handlungsschritt ist anstatt der Punktzahl die Buchstabenkombination „AA“ in die Kästchen einzutragen.

Spalte 1 – 14 s. o.	Punkte 1. Handlungsschritt		Punkte 2. Handlungsschritt		Punkte 3. Handlungsschritt		Punkte 4. Handlungsschritt		Punkte 5. Handlungsschritt		
	15	16	17	18	19	20	21	22	23	24	
Gesamtpunktzahl											
	26	27	28								

Prüfungszeit

25

Die entsprechende Ziffer (1, 2 oder 3) finden Sie in der Abfrage nach der Prüfungszeit im Anschluss an die letzte Aufgabe.

Unterschrift _____

Gemeinsame Prüfungsaufgaben der Industrie- und Handelskammern. Dieser Aufgabensatz wurde von einem überregionalen Ausschuss, der entsprechend § 40 Berufsbildungsgesetz zusammengesetzt ist, beschlossen.

Die Vervielfältigung, Verbreitung und öffentliche Wiedergabe der Prüfungsaufgaben und Lösungen ist nicht gestattet. Zuwiderhandlungen werden zivil- und strafrechtlich (§§ 97 ff., 106 ff. UrhG) verfolgt. – © ZPA Nord-West 2018 – Alle Rechte vorbehalten!

Die Handlungsschritte 1 bis 5 beziehen sich auf die folgende Ausgangssituation:

Sie sind Mitarbeiterin/Mitarbeiter der REXIT GmbH.
Die REXIT GmbH restrukturiert ihre IT-Ausstattung.
Sie arbeiten in diesem Projekt mit.

Sie sollen vier der folgenden fünf Aufgaben erledigen:

1. Das Netzwerk reorganisieren
2. Das Netzwerk gegenüber dem Internet absichern
3. Die Benutzerverwaltung und IT-Sicherheit optimieren
4. Das IPv6-Protokoll einführen
5. Einen Server beschaffen und ein Storage-System optimieren

Hinweis:

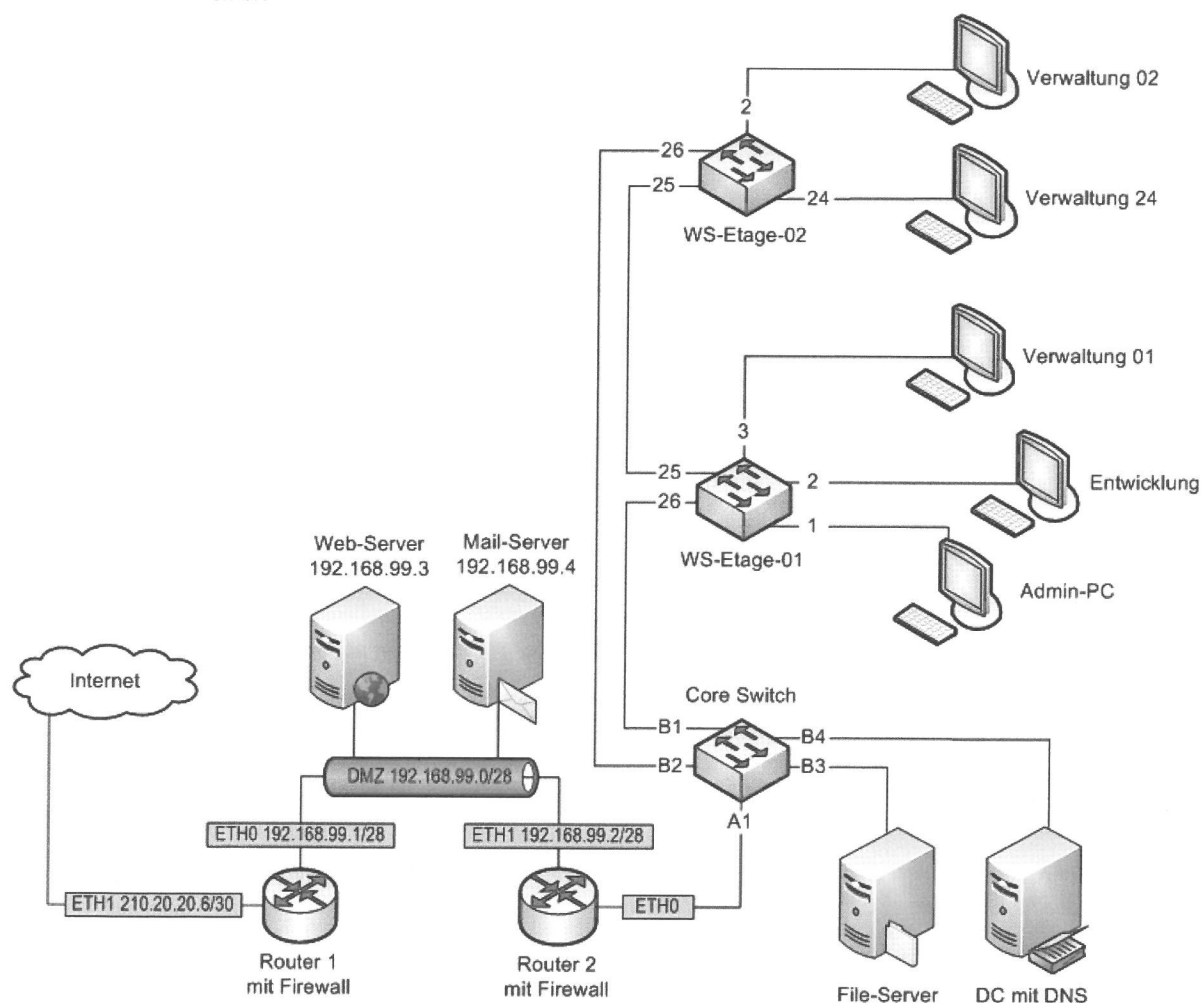
Es werden die folgenden Einheiten verwendet:

Speicherkapazität (z. B. Festplatten) in	MiB	1.024 * 1.024 Byte
Transferrate (z. B. PCI-Bus) in	MB/s	1.000 * 1.000 Byte/s
Transferrate (z. B. Ethernet, DSL) in	Mbit/s	1.000 * 1.000 bit/s

1. Handlungsschritt (25 Punkte)

Die REXIT GmbH organisiert ihr Netzwerk neu, siehe Netzwerkplan.

Netzwerk der REXIT GmbH



a) In der DMZ und im LAN sollen IP-Adressen und Subnetzmasken ergänzt werden.

- aa) Ermitteln Sie die maximale Anzahl der IP-Adressen für weitere Devices in der DMZ.
Die Herleitung ist anzugeben.

3 Punkte

- ab) Im LAN wird nach Konzernvorgaben die Netz-ID 10.0.0.0/22 verwendet.
Die ETH0-Schnittstelle von Router/Firewall 2 soll die letzte IP-Adresse erhalten.

Ermitteln Sie die entsprechende IP-Adresse.
Die Herleitung ist anzugeben.

3 Punkte

b) An mehreren PCs im LAN wird mit dem Befehl *ping* geprüft, ob Web-Server im Internet erreicht werden können. Der Test führt an allen PCs zu folgender Meldung:

Zielhost nicht erreichbar

Ein Ping auf den internen Web-Server in der DMZ funktioniert dagegen einwandfrei.
Sie lassen sich die Routing-Tabellen der beiden Router anzeigen.

Beschreiben Sie die Ursache für den Fehler und tragen Sie die erforderliche Ergänzung in die entsprechende Routing-Tabelle ein.

4 Punkte

Routing-Tabelle Router/Firewall 1

Netzwerk	Subnetzmaske	Schnittstelle	Next-Hop
192.168.99.0	255.255.255.240	ETH0	
210.20.20.4	255.255.255.252	ETH1	
0.0.0.0	0.0.0.0		210.20.20.5

Routing-Tabelle Router/Firewall 2

Netzwerk	Subnetzmaske	Schnittstelle	Next-Hop
10.0.0.0	255.255.252.0	ETH0	
192.168.99.0	255.255.255.240	ETH1	
0.0.0.0	0.0.0.0		192.168.99.1

c) In der REXIT GmbH sollen die Endgeräte ständig im Netz verfügbar sein. Das LAN wurde daher redundant ausgelegt und arbeitet mit dem Spanning Tree Protocol (STP).

- ca) Erläutern Sie, warum das Spanning Tree Protocol in einem geschwichten Netz mit redundanten Verbindungen eingesetzt wird.

4 Punkte

Fortsetzung 1. Handlungsschritt

cb) Das Spanning Tree wurde so konfiguriert, dass der Core Switch die Rolle der Root-Bridge übernimmt. Die Switches verfügen über folgende Ports:

	10/100/1.000 Mbit/s TX	1 Gbit/s FX	10 Gbit/s FX
Core Switch	-	A1 – A8	B1 – B8
WS-Etage-01	1 – 24	25	26
WS-Etage-02	1 – 24	25	26

Da es von WS-Etage-02 zwei Verbindungen zum Core Switch gibt, wird eine der Verbindungen von STP blockiert. Nennen Sie die blockierte Verbindung und ermitteln Sie die Pfadkosten der beiden offenen Verbindungen. 3 Punkte

$$\text{path cost} = 10.000.000.000 / \text{Übertragungsrate}$$

Hinweis: Übertragungsrate in bit/s

Beschreibung der blockierten Verbindung:

	Beschreibung der offenen Verbindungen	Pfadkosten	Berechnung
1.			
2.			

Rechenwege:

[illegible]

d) Auf den Switchen sollen für die einzelnen Abteilungen VLANs eingerichtet werden.

da) Erläutern Sie zwei Vorteile, die eine Aufteilung des LANs in VLANs bietet. 4 Punkte

db) Die Administratoren konfigurieren für jede Abteilung ein VLAN auf den Switchen.

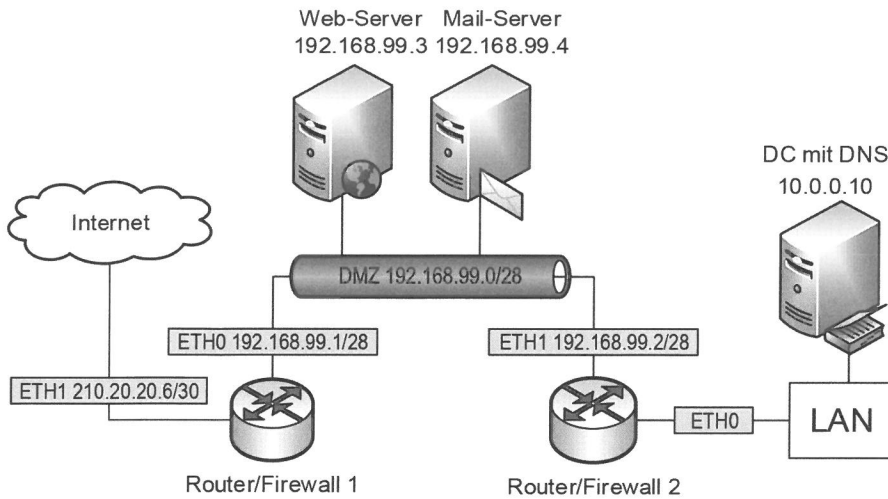
Erläutern Sie, warum Frames auf den Verbindungen zwischen den Switchen getagged werden müssen. 4 Punkte

2. Handlungsschritt (25 Punkte)

Korrekturrand

In der REXIT GmbH soll die Datensicherheit gewährleistet sein.

a) Im Netzwerk werden die Firewalls der Router 1 und 2 eingerichtet.



aa) Eine SPI-Firewall filtert den Datenverkehr auf zwei Schichten des OSI-Referenzmodells.

Nennen Sie die Bezeichnungen dieser zwei Schichten.

2 Punkte

ab) Die SPI-Firewall 2 soll nur folgende Dienste aus dem internen Netz erlauben:

- Zugriff auf Web-Server (siehe Regelsatz) und Web-Shops
- Zugriff auf den Mail-Server in der DMZ (unverschlüsseltes Senden und Empfangen von E-Mails)
- Namensauflösung für den DC

Anderer Datenverkehr ist verboten.

Ergänzen Sie den folgenden Regelsatz entsprechend dieser Vorgaben.

8 Punkte

Regelsatz für die Router/Firewall 2

Aktion	Protokoll	Quell-IP	Ziel-IP	Quell-Port	Ziel-Port	Von Interface	Nach Interface
Permit	TCP	10.0.0.0/22	Any	Any	80	ETH0	ETH1
Deny	IP	Any	Any	-	-		

Fortsetzung 2. Handlungsschritt →

Fortsetzung 2. Handlungsschritt

Korrekturrand

b) Sie überprüfen das Logfile von Router/Firewall 1.

Auszug aus dem Logfile von Router/Firewall 1:

From;To;Protocol;Port;Action

31.220.44.83;210.20.20.6;TCP;1433;Drop

34.239.248.82;210.20.20.6;TCP;22;Drop

40.191.72.114;210.20.20.6;TCP;445;Drop

37.220.1.85;210.20.20.6;TCP;23;Drop

194.17.12.212;210.20.20.6;TCP;445;Drop

...; ...; ...; ...; ...

<EOF>

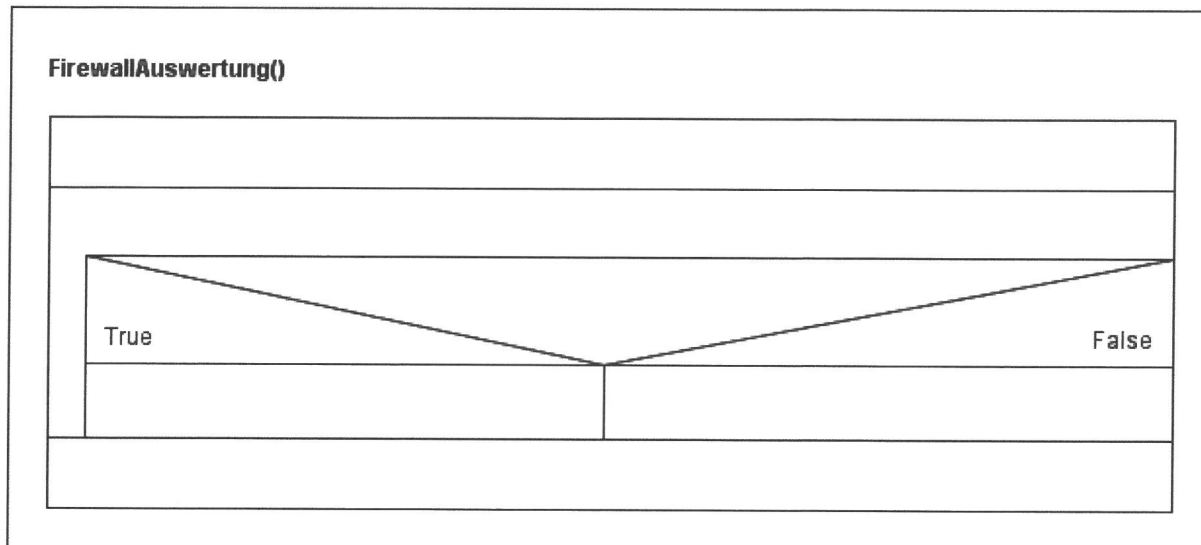
Das Logfile der Firewall soll mithilfe einer Funktion ausgewertet werden.

Die Funktion soll alle Quell-IP-Adressen auf dem Bildschirm ausgeben, die auf den Port 445 zielten und deren Datenpakete verworfen wurden.

Der Algorithmus dieser Funktion FirewallAuswertung() soll in einem Struktogramm dargestellt werden.

Ergänzen Sie dazu folgendes Struktogramm.

10 Punkte



c) Der Internetverkehr soll über einen Proxyserver erfolgen.

Nennen Sie zwei Aufgaben, die der Proxyserver übernimmt.

2 Punkte

d) Der aus dem Internet eingehende Datenverkehr an Router/Firewall 1 wird überwacht. Das dazu eingesetzte Programm ist nur in der Lage, ausführbare Dateien und Office-Dateien zu scannen.

Erläutern Sie, warum dieser Schutz nicht ausreichend ist.

3 Punkte

3. Handlungsschritt (25 Punkte)

Sie administrieren und optimieren im Bereich der Benutzerverwaltung und der IT-Sicherheit.

- a) Jeder Beschäftigte der REXIT GmbH besitzt ein Systemkonto.
Die User-IDs der Systemkonten sind 5-stellige Zahlen, die eindeutig vergeben werden.
Für das Projekt „KWJ“ wird der Netzwerkordner „KWJ\$“ eingerichtet.
Die Projektmitglieder erhalten, wie in der folgenden Tabelle angegeben, Zugriff auf den Netzwerkordner.

Projektmitglieder

Gruppe	User-ID der Mitglieder	Berechtigung
KWJ_Lesen	12224, 13601	Lesen
KWJ_Schreiben	10459, 15777	Schreiben
KWJ_Ausfuehren	11446, 20009	Programme ausführen
KWJ_Aendern	13602, 50317	Ändern
KWJ_Verwalten	23188, 45532	Verwalten

Folgende Datei- und Ordnerberechtigungen können vergeben werden:

Permission	Action
Read	Read the file and view its attributes, ownership, and permission set.
Write	Overwrite the file, change its attributes, view its ownership, and view the permission set.
Read & Execute	Run and execute the application. In addition, the user can perform all duties allowed by the Read permission.
Modify	Modify and delete a file including perform all of the actions permitted by the Read, Write, and Read and Execute file permissions.
Full Control	Change the permission set on a file, take ownership of the file, and perform actions permitted by all of the other file permissions.

Die folgenden Aufgaben beziehen sich auf den Netzwerkordner „KWJ\$“, in dem Dokumente und Programme gespeichert werden.

- aa) Ermitteln Sie die User-IDs der Projektmitglieder, die berechtigt sind, Dateien im Netzwerkordner „KWJ\$“ zu löschen.
3 Punkte

- ab) Ermitteln Sie die User-IDs der Projektmitglieder, die berechtigt sind, Dateien im Netzwerkordner „KWJ\$“ auf Read-Only zu setzen.
3 Punkte

Fortsetzung 3. Handlungsschritt

Korrekturrand

ac) Mit dem Kommandozeilenbefehl `adacl` können sowohl Berechtigungen gewährt als auch entzogen werden.

Syntax:

`adacl [/Pfad] [/Aktion] [/Benutzer] [/Berechtigung]`

adacl	Befehlsname
Pfad	Dateiname oder Ordnername
Aktion	grant = Gewähren von Berechtigungen revoke = Entziehen von Berechtigungen
Benutzer	User-ID
Berechtigung	N = kein Zugriff R = Lesen W = Schreiben RX = Lesen und Ausführen M = Ändern F = Vollzugriff

Ein weiteres Projektmitglied mit der User-ID 55671 soll die Berechtigung zum Ausführen der Programme erhalten, die sich im Netzwerkordner `KWJ$` befinden.

Erstellen Sie die entsprechende Anweisung.

3 Punkte

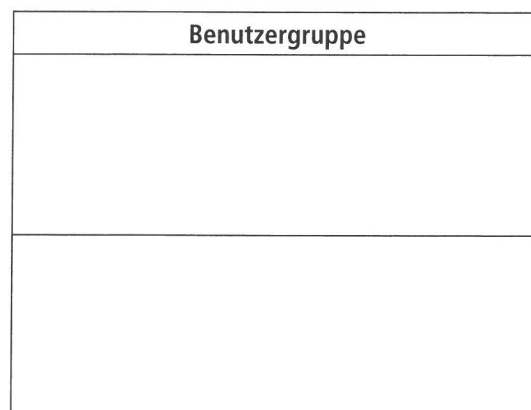
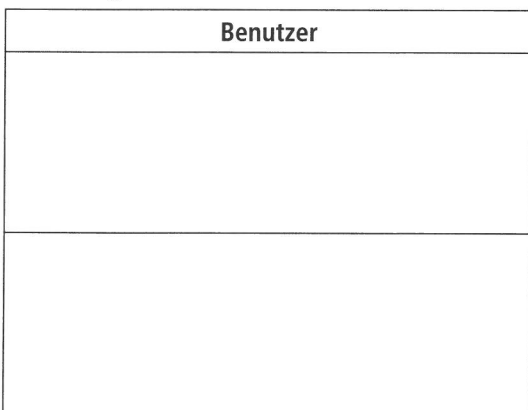
b) Zur Optimierung der Benutzerverwaltung soll ein entsprechendes objektorientiertes Programm entwickelt werden. Im zugehörigen Klassendiagramm sind die Klassen `Benutzer` und `Benutzergruppe` zu implementieren.

Ergänzen Sie dazu das Klassendiagramm mit ...

- zwei privaten Attributen je Klasse (keine Doppelnennungen, ohne Datentypen).
- zwei öffentlichen Methoden je Klasse (keine Doppelnennungen, ohne Parameter).
- der Darstellung der Beziehung mit Multiplizität zwischen den beiden Klassen.

10 Punkte

Klassendiagramm



c) Bestimmte Vorgaben zur Datenspeicherung dienen gleichzeitig dem Datenschutz und der Datensicherheit.

Erläutern Sie eine konkrete Maßnahme im Zusammenhang mit der Speicherung von Daten, die geeignet ist, den Datenschutz und die Datensicherheit gleichzeitig zu verbessern.

3 Punkte

Maßnahme:

Erläuterung:

- d) Bislang wird der Zugang zum System nach Eingabe von Benutzername und Passwort gewährt. Zukünftig soll eine Zwei-Faktoren-Authentifizierung erfolgen.

Erläutern Sie das Prinzip der Zwei-Faktoren-Authentifizierung an einem Beispiel.

3 Punkte

4. Handlungsschritt (25 Punkte)

Die Administratoren haben beschlossen, das IPv6-Protokoll einzuführen. Dazu wurde eine Testumgebung eingerichtet.

- a) Auf dem Router wird Dual-Stack aktiviert.

Erklären Sie den Begriff „Dual-Stack“.

2 Punkte

- b) Bei einer Kontrolle im Netzwerk wurde folgendes IPv6-Paket aufgezeichnet.

Trace

```
60 00 00 00 00 40 11 40 fc 00 0d b8 00 10 00 00
00 00 af c1 00 f7 00 51 fd 00 00 ff 00 00 00 03
00 00 00 be fe 30 01 f0 ...
```

- ba) Ermitteln Sie aus dem Trace das Protokoll des Feldes „Next Header“.

3 Punkte

ID	Next Header
1	ICMP
6	TCP
17	UDP
27	RDP
58	ICMPv6
59	no next header
92	MTP

IPv6 Header

Version (4 bit)	Traffic Class (8 bit)	Flow Label (20 bit)	
Payload Length (16 bit)		Next Header (8 bit)	Hop Limit (8 bit)
Source Address (128 bit)			
Destination Address (128 bit)			

- bb) Ermitteln Sie die Quelladresse und die Zieladresse des IPv6-Pakets. Geben Sie diese auch in verkürzter Schreibweise wieder.

4 Punkte

Quelladresse	
verkürzte Quelladresse	

Zieladresse	
verkürzte Zieladresse	

Fortsetzung 4. Handlungsschritt →

Fortsetzung 4. Handlungsschritt

Korrekturrand

c) Bei IPv6 werden bestimmte Funktionalitäten per Multicast bereitgestellt.

Multicast Addresses (Übersicht)

1111 1111	Flag	Scope	Group ID
8 bit	4 bit	4 bit	112 bit

Multicast Address: ff::/8

Flag: 0x0000 well-known multicast addresses
0x0001 for transient addresses

Scope: 0x0001 node-local
0x0010 link-local
0x0011 subnet-local
0x0100 admin-local
0x0101 site-local
0x1000 organization-local
0x1110 global (internet)

other reserved!

Important group ID's last 32 bit

0000 0000 0000 0000 0000 0000 0000 0001	nodes
0000 0000 0000 0000 0000 0000 0000 0010	routers
0000 0000 0000 0000 0000 0000 0000 1001	RIP Routers
0000 0000 0000 0000 0000 0000 1111 1011	DNS
0000 0000 0000 0000 0000 0001 0000 0001	NTP-Server
0000 0000 0000 0000 0000 0001 0001 0001	Multicast Transport
0000 0000 0000 0000 0000 0001 0000 1000	NIS
0000 0000 0000 0001 0000 0000 0000 0010	DHCP server or relay agent

ca) Ermitteln Sie mithilfe der Übersicht, welche Funktionalität die folgende Multicast-Adresse bereitstellt.

4 Punkte

ff05::1:2

cb) Ermitteln Sie die Multicast-Adresse, die alle Schnittstellen eines Netzwerksegments anspricht.

4 Punkte

d) In der IPv6-Netzwerkconfiguration eines Servers sind die Privacy Extensions aktiviert.

Erläutern Sie, warum dieses Verfahren bei Servern sinnvollerweise nicht genutzt werden sollte.

4 Punkte

e) Nach dem erfolgreichen Test beantragt die REXIT GmbH beim Provider ein IPv6-Netz.

Sie erhält folgenden Adressbereich zugewiesen:

2001:db8:10ab::/48

Dieses IPv6-Netz soll in vier gleich große Teilnetze unterteilt werden.

Ermitteln Sie die Netz-IDs der vier Netze.

4 Punkte

Netz	Netz-ID
1	
2	
3	
4	

5. Handlungsschritt (25 Punkte)

Die REXIT GmbH schafft einen weiteren Server an.

a) Der neue Server verfügt u. a. über folgende Ausstattungsmerkmale:

- Intel Xeon
- E5-2600 v4 Series 30 MB L3 Cache
- 4x Nodes
- Dual 2 x CPU
- Hyperthreading 112 CPU Kerne/224 Threads
- RAM 2400 MHz DDR4 Quad Channel

aa) Beschreiben Sie das Ausstattungsmerkmal „Hyperthreading“.

2 Punkte

ab) Beschreiben Sie das Ausstattungsmerkmal „Quad Channel“.

2 Punkte

ac) Die CPU des neuen Servers besitzt einen besonders leistungsfähigen Cache.

Erläutern Sie die Aufgabe eines CPU Cache.

4 Punkte

Korrekturrand

Fortsetzung 5. Handlungsschritt

Korrekturrand

ad) Zur Auswahl des Storage-Systems sollen Sie eine Präsentation zu den in folgendem Text beschriebenen Systemen vorbereiten.

Direct-attached storage (DAS)

The simplest storage is one or more Hard Disks connected to your server. It could be deployed directly in the server chassis or as an external storage enclosure plugging directly into a SCSI/SAS card on the server's internal bus. DAS is not shareable.

Network-attached storage (NAS)

Network-attached storage provides connectivity to the virtual server through a TCP/IP connection and storage access is provided at the file level.

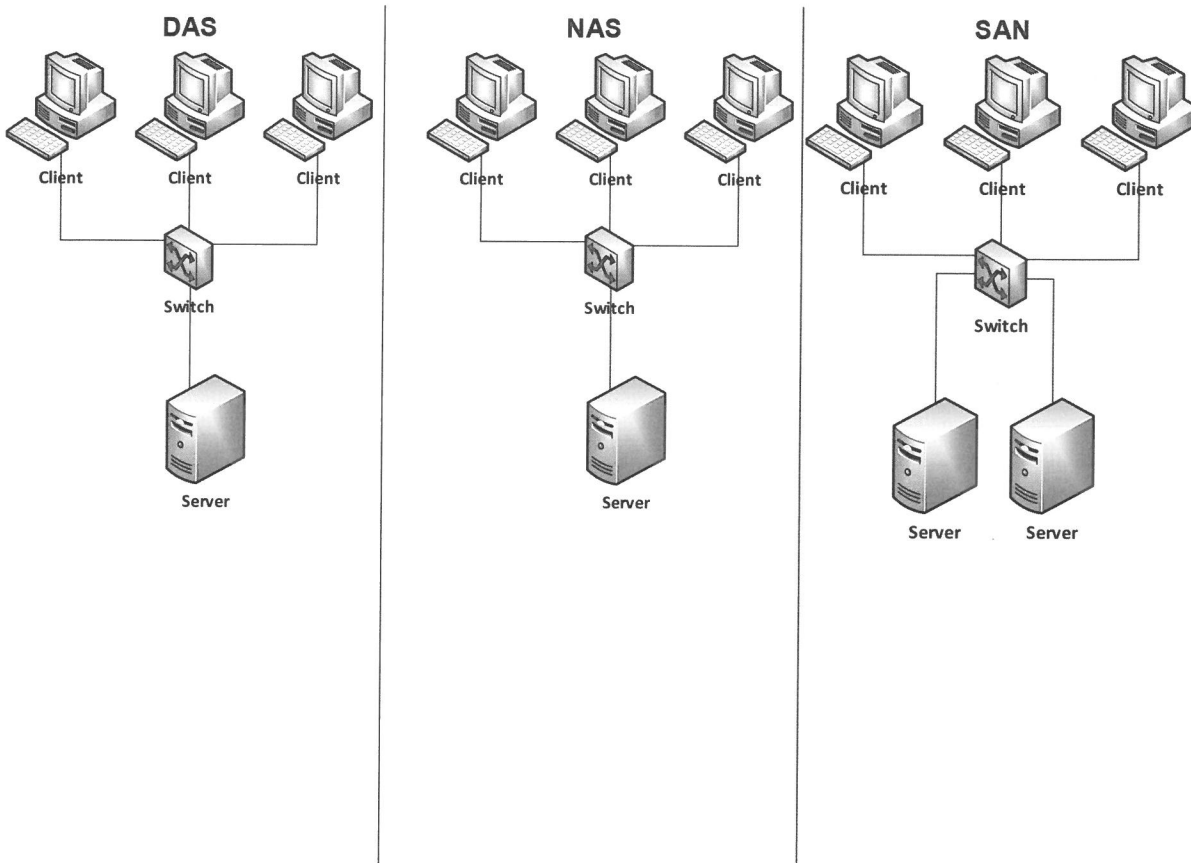
NAS is shareable. NAS abstracts storage management from the server.

Storage area networks in a virtual environment (SAN)

Storage area networks provide connectivity to the virtual server using either the Fibre Channel (FC) or iSCSI protocols. Resources may be easily shared between multiple virtual server hardware devices.

Ergänzen Sie die folgenden Abbildungen zu DAS, NAS und SAN, indem Sie die jeweiligen Speichermedien einzeichnen und entsprechend verbinden.

4 Punkte



- b) Die Administratoren beschließen ein SAN mit einem Storage-Array einzurichten. Dazu sind folgende Komponenten verfügbar:

- 2 Festplatten (je 2 TiB Speicherkapazität)
- 7 Festplatten (je 750 GiB Speicherkapazität)
- PCIe RAID-Hostadapter (620 MB/s Datenübertragungsrate beim Lesen)

- ba) Mit den gegebenen Festplatten soll eine fehlertolerante RAID-Konfiguration erstellt werden, welche die größtmögliche Nettospeicherkapazität bietet. Das System erlaubt, mehrere RAID-Systeme zu konfigurieren.

Nennen Sie die entsprechende RAID-Konfiguration und berechnen Sie deren Nettospeicherkapazität in GiB.

4 Punkte

Der Rechenweg ist anzugeben.

RAID-Level:

Netto-Speicherkapazität:

Rechenweg

[illegible]

- bb) Für einen Vergleich soll auch die Speicherkapazität ermittelt werden, die erzielt werden kann, wenn die gegebenen Festplatten als JBOD genutzt werden.

Ermitteln Sie die entsprechende Speicherkapazität in GiB.

2 Punkte

Der Rechenweg ist anzugeben.

Speicherkapazität in GiB:

Rechenweg

[illegible]

- bc) Nennen Sie zwei Vorteile, die ein Laufwerksverbund als JBOD gegenüber einem RAID 0 bietet.

2 Punkte

- c) Der Server mit einer veranschlagten Leistungsaufnahme von 650 VA soll über eine USV mit Strom versorgt werden, deren Bemessungsleistung 1.400 VA beträgt und die zwei 12 V-Akkumulatoren mit je 10 Ah enthält.

Berechnen Sie die Zeit in Minuten, die die USV bei einem Netzausfall theoretisch maximal überbrücken kann. Runden Sie das Ergebnis auf volle Minuten. 5 Punkte

5 Punkte

Der Rechenweg ist anzugeben.

Stützzeit: Minuten

[illegible]

PRÜFUNGSZEIT – NICHT BESTANDTEIL DER PRÜFUNG!

Wie beurteilen Sie nach der Bearbeitung der Aufgaben die zur Verfügung stehende Prüfungszeit?

7

- 1 Sie hätte kürzer sein können. 2 Sie war angemessen. 3 Sie hätte länger sein müssen.