

Die Handlungsschritte 1 bis 6 beziehen sich auf die folgende Ausgangssituation:

Sie sind Mitarbeiter/-in der Easy IT GmbH, einem IT-Systemhaus, das in den Bereichen Entwicklung, Consulting und Webhosting tätig ist.

Die Easy IT GmbH wurde von der Glabal KG mit der Erneuerung und Pflege ihrer IT beauftragt.

Sie arbeiten bei folgenden Aufgaben mit:

1. Netzwerk analysieren
2. CRM-System einführen
3. Netzwerkbetreuung durchführen
4. Datensicherheit erhöhen
5. Systemsupport durchführen
6. Benutzer anlegen und verwalten

1. Handlungsschritt (20 Punkte)

Seit einiger Zeit arbeitet das Netzwerk der Glabal KG (siehe perforierte Anlage) nicht einwandfrei.

- a) Der Mitarbeiter am PC Zentrale beschwert sich, dass er keinen Zugriff auf das Netz der Filiale hat. Sie lassen sich die Konfiguration mit dem Befehl ipconfig anzeigen:

Ethernet-Adapter LAN-Verbindung:

```
Verbindungslokale IPv6-Adresse . : fe80::2e0:81ff:fe55:32a7%10
Physikalische Adresse. . . . . : 00:E0:81:55:32:A7
IPv4-Adresse . . . . . : 192.168.0.1
Subnetzmaske . . . . . : 255.255.255.0
Standardgateway. . . . . : 192.168.0.254
```

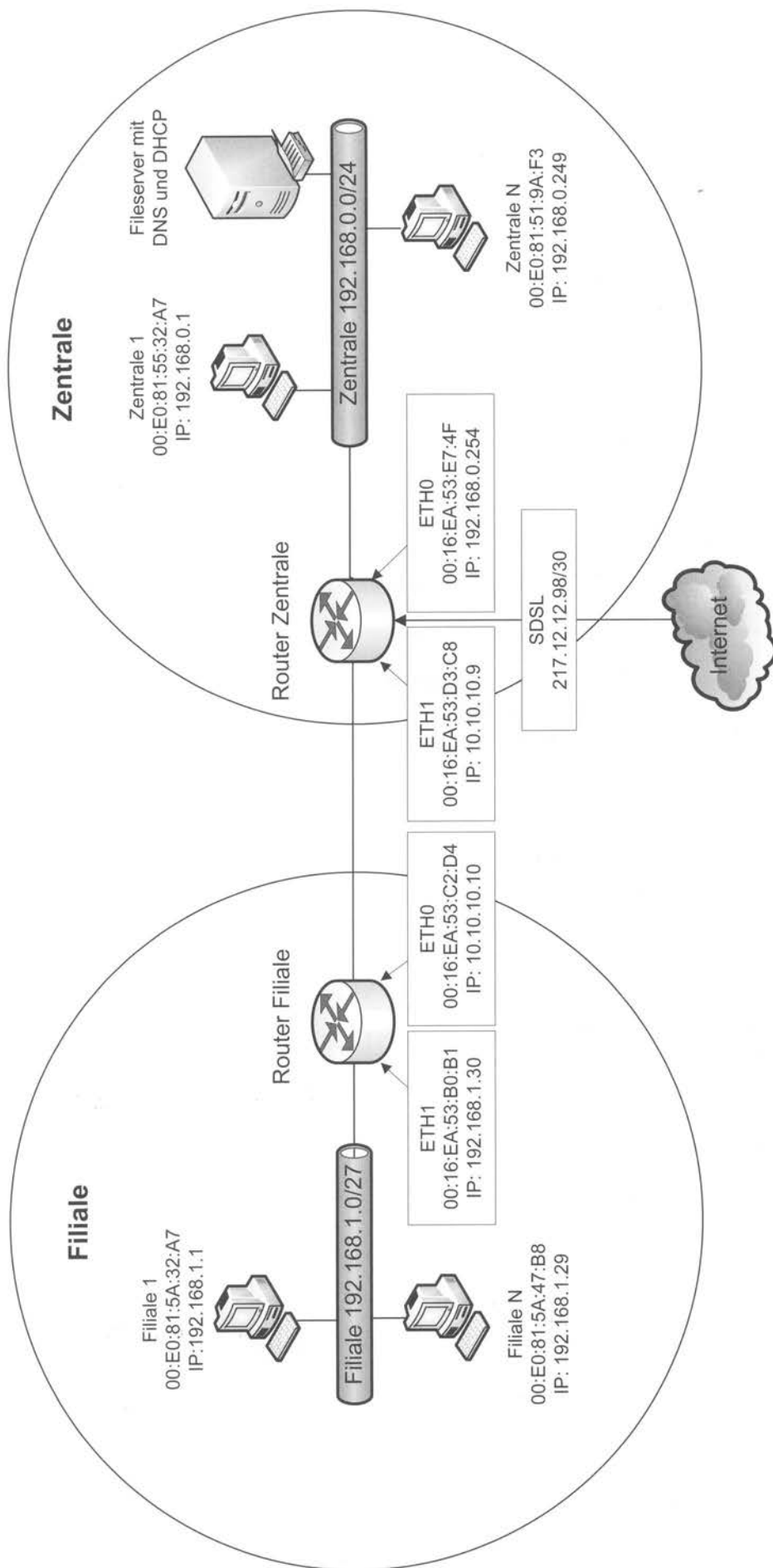
- aa) Nennen Sie jeweils den Namen der Schicht des OSI-Modells, auf der sich die physikalische Adresse und die IP-Adresse befinden. (2 Punkte)

- ab) PC Zentrale 1 schickt ein Datenpaket an den PC Filiale 1. Ergänzen Sie den folgenden Frameaufbau. (2 Punkte)

Quell-MAC	Ziel-MAC	Quell-IP	Ziel-IP	Daten	CRC

- ac) Erläutern Sie, wie der PC Zentrale 1 ermittelt, dass die Daten an den Router geschickt werden müssen. (2 Punkte)

Anlage zum 1. Handlungsschritt



b) Sie vermuten den Kommunikationsfehler in der Konfiguration der Router.

ba) Sie lassen sich die Routingtabelle des Routers in der Zentrale anzeigen:

192.168.0.0	255.255.255.0	eth0
10.10.10.8	255.255.255.252	eth1
0.0.0.0	0.0.0.0	217.12.12.97

Nennen Sie den Fehler, den Sie feststellen können.

(2 Punkte)

bb) Bei der Überprüfung der Routingtabelle des Routers in der Filiale stellen Sie fest, dass keine Default-Route eingetragen ist.

Nennen Sie den Eintrag, den Sie vornehmen müssen.

(2 Punkte)

c) Sie vermuten einen Fehler in der Konfiguration am Clientrechner in der Filiale. Der Befehl ipconfig bzw. ifconfig ergibt folgende Ausgabe:

Ausgabe Linux

```
eth0 Link encap:Ethernet HWaddr 00:E0:81:55:32:A7
      inet6 addr: fe80::2e0:81ff:fe55:32a7/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
```

Ausgabe Windows

Ethernet-Adapter LAN-Verbindung:

```
Verbindungslokale IPv6-Adresse . : fe80::2e0:81ff:fe55:32a7%10
DHCP aktiviert . . . . . : Ja
IPv4-Adresse . . . . . : 169.254.1.117
Subnetzmaske . . . . . : 255.255.0.0
Standardgateway. . . . . :
```

Erläutern Sie, warum der Client die Adresse 169.254.1.117 (Windows) bzw. keine IP-Adresse (Linux) erhalten hat und wie der Fehler behoben werden kann.

(4 Punkte)

Fortsetzung 1. Handlungsschritt

d) Erläutern Sie mithilfe des folgenden englischen Textes, nach welchem Verfahren die IPv6-Adresse **fe80::2e0:81ff:fe55:32a7** generiert wurde.

(4 Punkte)

IPv6 hosts automatically assign each of their interfaces a unique address based on the IEEE 802 MAC address. This auto configuration is specified in RFC 4862. A link-local unicast address has the prefix fe80::/10 in standard IPV6 CIDR notation.

A 64-bit interface identifier is most commonly derived from its 48-bit MAC address. A MAC address 00:1D:BA:06:37:64 is turned into a 64-bit EUI-64 by inserting FF:FE in the middle: 00:1D:BA:FF:FE:06:37:64. When this EUI-64 is used to form an IPv6 address it is modified: the meaning of the Universal/ Local bit (the 7th most significant bit of the EUI-64, starting from 1) is inverted, so that a 1 now means Global.

e) Das Netzwerk soll in der Zentrale um eine DMZ mit der Netz-ID 212.20.20.24/29 erweitert werden.

(2 Punkte)

Vervollständigen Sie die folgende Tabelle:

Netz-ID	Hostbereich	Broadcast	Subnetmaske
212.20.20.24			255.255.____.____

2. Handlungsschritt (20 Punkte)

Korrekturrand

Die Global KG erwägt, ein CRM-System einzuführen (CRM = Customer Relationship Management) und will von der Easy IT GmbH beraten werden.

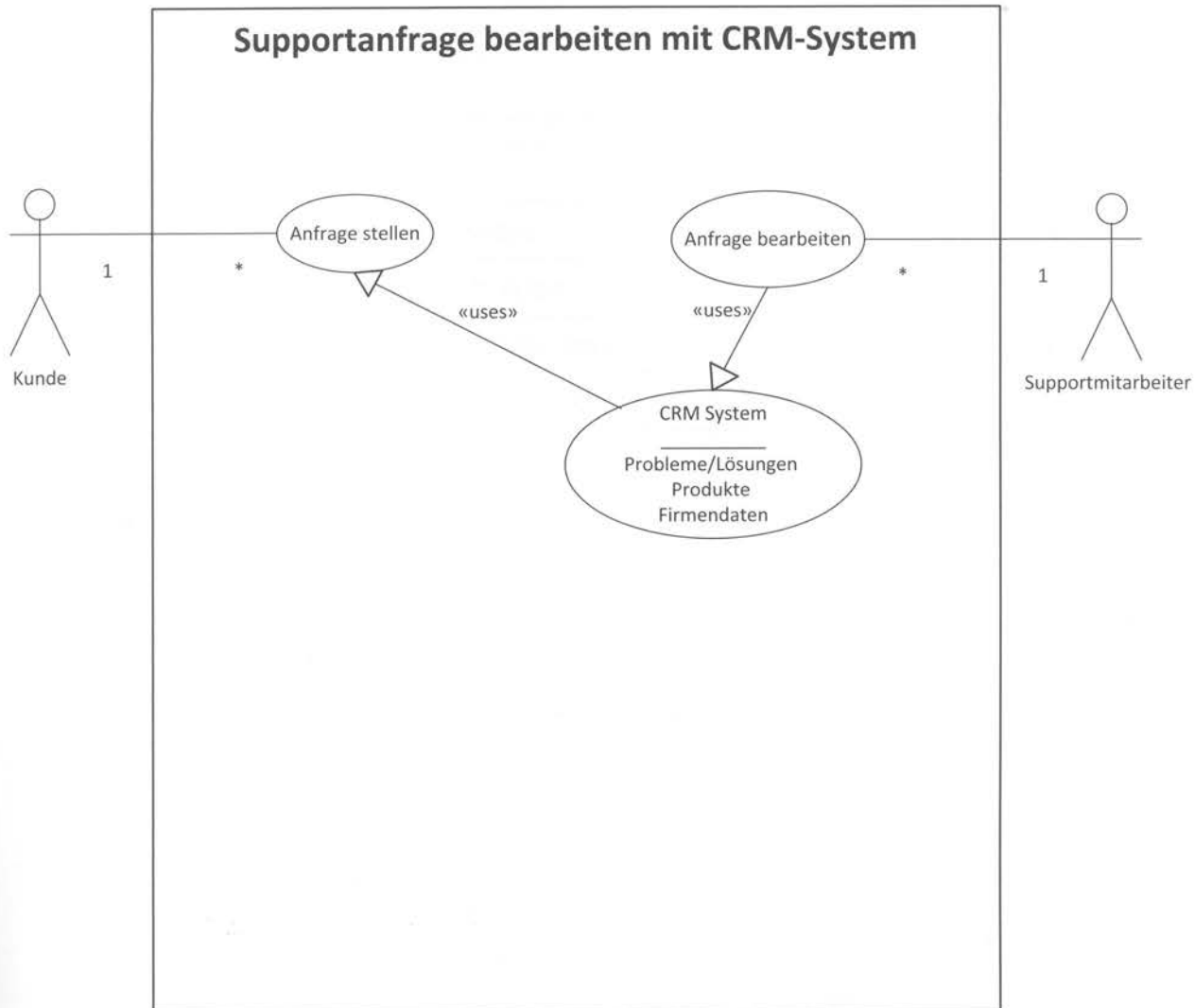
a) Mit dem CRM-System soll ein Supportmitarbeiter die Supportanfragen von Kunden wie folgt bearbeiten:

Der Supportmitarbeiter soll die Datenbank öffnen und daraus folgende Daten erfassen:

– 1. Firmendaten, 2. gekaufte Produkte und 3. bisher aufgetretene Probleme.

Er soll weiterhin das aktuelle Problem in der Datenbank des CRM-Systems protokollieren.

Wie der Supportmitarbeiter die oben dargestellte Supportanfrage eines Kunden mithilfe des CRM-Systems bearbeitet, soll in einem Use-Case-Diagramm abgebildet werden. Vervollständigen Sie dazu den folgenden Entwurf. (14 Punkte)



Fortsetzung 2. Handlungsschritt →

Fortsetzung 2. Handlungsschritt

- b) Sie sollen zur Vorbereitung eines Gesprächs mit der Geschäftsführung der Global KG Vor- und Nachteile eines CRM-Systems gegenüberstellen.

Korrekturra

Nennen Sie in folgender Tabelle jeweils drei Argumente, die für bzw. gegen ein CRM-System sprechen können. (6 Punkte)

Pro	Kontra

3. Handlungsschritt (20 Punkte)

Korrekturrand

Bei einem Kunden der Easy IT GmbH sollen Sie die Netzwerksicherheit analysieren und optimieren.

- a) Das Netzwerkteam erörtert Möglichkeiten der Absicherung des Netzwerks. Diese beziehen sich jeweils auf verschiedene Schichten des OSI-Modells.

Im Besprechungsprotokoll lesen Sie die in folgender Tabelle angegebenen Textpassagen.

Geben Sie zu jeder Textpassage die Nummer der Schicht des OSI-Modells an, auf die sich die Textpassage inhaltlich bezieht.

Hinweis: Die Sitzungs-, Darstellungs- und Anwendungsschicht sollen als eine Schicht betrachtet werden, die mit 7 gekennzeichnet werden soll.

(5 Punkte)

Textpassage aus Besprechungsprotokoll	Nr. der OSI-Schicht
LWL-Strecken tragen zur höheren Abhörsicherheit bei.	
Die Migration von RIPv1 nach OSPF hat Priorität.	
SSL/TSL hat als Basis Schicht.	
Bestimmte Angriffe manipulieren das TTL-Feld.	
Telearbeitsplätze werden nur über PPTP angebunden.	
Eine Network Security Appliance soll angeschafft werden.	
Die Benutzer-Authentifikation erfolgt über einen Radius-Server.	
Bestimmte Dienste werden über ihre Port-Nummern gesperrt.	
Port-Mirroring hilft bei der Lösung von Netzwerkproblemen.	
Die Verwaltung bekommt ein eigenes VLAN.	

- b) Sie sollen Netzwerkangriffe aufspüren.

- ba) Sie überprüfen den Client mit der Internetadresse 193.166.12.39/24 auf Netzwerkangriffe und lassen sich seinen ARP-Cache anzeigen:

Internetadresse	Physische Adresse	Typ
193.166.12.29	00-01-6A-94-D7-E4	dynamisch
193.166.12.49	00-D0-03-95-D0-45	dynamisch
193.166.12.133	00-D0-03-95-D0-45	dynamisch
193.166.12.137	00-D0-03-95-D0-45	dynamisch
193.166.12.221	00-D0-03-95-D0-45	dynamisch
193.166.12.239	00-D0-03-95-D0-45	dynamisch
193.166.12.246	00-D0-03-95-D0-45	dynamisch
193.166.12.255	FF-FF-FF-FF-FF-FF	dynamisch
224.0.0.22	01-00-5E-00-00-16	statisch
224.0.1.60	01-00-5E-00-01-3C	statisch

Erläutern Sie, welche Art von Angriff hier vermutlich vorliegt und worauf sich Ihre Vermutung stützt.

(3 Punkte)

Fortsetzung 3. Handlungsschritt →

Fortsetzung 3. Handlungsschritt

bb) Außerdem baut der Client nach jedem Systemstart sofort eine TCP/IP-Verbindung zu der Netzwerkstations-Internetadresse 141.146.9.91 auf.

bba) Nennen Sie eine Möglichkeit, mit der Sie Informationen über die Verantwortlichkeit oder den Standort der Netzwerkstations-Internetadresse erlangen können. (2 Punkte)

bbb) Nennen Sie eine Möglichkeit, um zu erkennen, welcher Dienst bzw. welches Programm die Verbindung nutzt. (2 Punkte)

c) Der Kunde möchte den Datenverkehr in seinem lokalen Netzwerk auf Basis von IPsec im Transportmodus verschlüsselt durchführen.

ca) Erläutern Sie, welche zusätzliche Sicherheit bei IPsec der Tunnelmodus gegenüber dem Transportmodus bietet. (3 Punkte)

cb) Nach der Implementierung von IPsec wollen Sie durch Auswertung mitgeschnittener Datenpakete überprüfen, ob der Datenaustausch tatsächlich verschlüsselt erfolgt.

Nennen Sie Protokollfelder, die darauf schließen lassen, dass IPsec mit Verschlüsselung arbeitet. (2 Punkte)

cc) Folgender Ethernet-Frame wird vom (Hardware)-Sniffer mit „Frame-Error“ markiert.

0000	00	12	3f	8d	78	e1	00	d0	03	93	d0	00	08	00	45	00
0010	05	dc	6c	78	40	00	3b	06	55	ce	d4	c9	64	8e	c0	a1
0020	7a	9b	14	a4	2e	ba	a7	71	70	c6	85	00	9b	0b	2b	bb
0030	31	5c	fb	a5	a5	9f	bd	75	9c	b1						

Nennen Sie den Grund, warum dieser Frame fehlerhaft ist.

(3 Punkte)

4. Handlungsschritt (20 Punkte)

Die Global KG betreibt einen Datenserver.

- a) Die Daten werden sonntags durch ein Vollbackup und montags bis samstags inkrementell über das Netzwerk gesichert. Im Fehlerfall müssen die Daten innerhalb von fünf Stunden wiederhergestellt werden können.
- aa) Ermitteln Sie anhand folgender Werte, in welcher Zeit der Datenbestand nach der letzten inkrementellen Sicherung vom Samstag wiederhergestellt werden kann.

Der Rechenweg ist anzugeben,

$$1\text{ GiB} = 1.024 \cdot \text{MiB} = 1.024 \cdot 1.024 \text{ kiB} = 1.024 \cdot 1.024 \cdot 1.024 \text{ Byte} (= 2^{30} \text{ Byte}).$$

(8 Punkte)

Datenbestand beim letzten Vollbackup	750 GiB
Durchschnittliche Datenänderungen pro Werktag	40 GiB
Nutz-Datendurchsatz im Netzwerk	50 MiB/s

- ab) Erläutern Sie eine Backupstrategie, mit der eine Rückspielung in der geforderten Zeit von fünf Stunden möglich ist. Der Rechenweg ist anzugeben.

(4 Punkte)

- b) Der Grad der Datensicherheit und der Grad des Datenschutzes hängen von der elektrischen, logischen, physikalischen und organisatorischen Sicherheit ab.

Zur Gewährleistung hoher Sicherheitsgrade sind entsprechende Maßnahmen erforderlich.

Nennen und erläutern Sie in folgender Tabelle jeweils eine weitere Maßnahme (siehe Beispiele).

ba) Maßnahmen zur Gewährleistung der elektrischen Sicherheit

(2 Punkte)

	Maßnahme	Erläuterung
1.	Redundante Datenserver	Beispiel: Durchgehende Verfügbarkeit der Daten, Schutz vor Datenverlust
2.		

bb) Maßnahmen zur Gewährleistung der logischen Sicherheit

(2 Punkte)

	Maßnahme	Erläuterung
1.	Zugriffsberechtigungen	Beispiel: Schutz vor Datenmissbrauch und Datenmanipulation
2.		

bc) Maßnahmen zur Gewährleistung der physikalischen Sicherheit

(2 Punkte)

	Maßnahme	Erläuterung
1.	Zugangssicherung für Serverraum mit Code-Karte	Beispiel: Schutz vor Sabotage, Schutz vor Diebstahl von Datenträgern
2.		

bd) Maßnahmen zur Gewährleistung der organisatorischen Sicherheit

(2 Punkte)

	Maßnahme	Erläuterung
1.	Dokumentation	Beispiel: Informationen zu Datenspeichersystemen sind schnell verfügbar.
2.		

5. Handlungsschritt (20 Punkte)

Korrekturrand

An einem Fileserver der Global KG kommt es unregelmäßig zu Systemabstürzen. Sie sollen die Fehlerursache lokalisieren und für einen stabilen Betrieb sorgen.

- a) Zur systematischen Fehlereingrenzung unterscheiden Sie nach Hardware-, Software- und sonstigen Fehlern.

Nennen Sie jeweils zwei weitere Fehlerursachen, die für Systemabstürze in Frage kommen.

(3 Punkte)

	Fehlerursache
Hardware	Beispiel: Fehlerhafter Arbeitsspeicher (Lesefehler)
Software	Beispiel: Treiberprobleme (veraltet, inkompatibel)
Sonstige	Beispiel: Netzspannungsversorgung (Wackelkontakte, Spikes)

- b) Der Server ist mit vier 512 MiB Speichermodulen (No-ECC) ausgestattet.

Drei Speichertests liefern folgende Ergebnisse (hexadezimale Darstellung):

Error at Address: 0x43A4B317

Data written: AAAA AAAA AAAA AAAA

Data read: AAAA AABA AAAA AAAA

Error at Address: 0x43A4B317

Data written: CCCC CCCC CCCC CCCC

Data read: CCCC CCDC CCCC CCCC

Error at Address: 0x43A4B317

Data written: EEEE EEEE EEEE EEEE

Data read: EEEE EEF EEEE EEEE

- ba) Geben Sie mit kurzer Begründung den Speicherfehlertyp aus folgender Auflistung an, den Sie dem Testergebnis zufolge vermuten.

(4 Punkte)

Different types of memory errors:

Address-Decoder Fault:

When reading from or writing to a specific memory address, a wrong memory cell is selected.

Stuck-at-0 Fault:

A memory cell fails to retain the assigned data. One or more bits retain permanent at 0.

Coupling Fault:

Data change in a certain memory cell causes unwanted data changes in another cell.

Read-Disturb:

A section of memory changes when being read.

Stuck-at-1 Fault:

A memory cell fails to retain the assigned data. One or more bits retain permanent at 1.

Retention Fault:

One or more bits lose their contents after a period of time.

Transition Fault:

A section of memory may not allow values to change.

- bb) Ermitteln Sie das fehlerhafte Speichermodul, indem Sie Tabelle mit den fehlenden Adressen in hexadezimaler Schreibweise ergänzen und das defekte Modul kennzeichnen. (4 Punkte)

Adressbereich	Startadresse	Endadresse	Defekt (ja/nein)
Modul 1	0x00000000		
Modul 2			
Modul 3			
Modul 4		0x7FFFFFFF	

- bc) Auf dem fraglichen Speichermodul lesen Sie die Bezeichnung „PC2-8500-CL5“.

Erläutern Sie, was hierbei die Angabe CL5 aussagt.

(2 Punkte)

- c) Die Daten des Fileservers (500 GiB) sollen in ein vorhandenes SAN (Storage-Area-Network) verlagert werden.

ca) Nennen Sie zwei Aspekte, warum in größeren Firmen SANs Kostenvorteile bieten.

(2 Punkte)

Fortsetzung 5. Handlungsschritt

Korrekturrand

cb) Das SAN mit RAID Level 6 besteht aus sieben Festplatten mit je 147 GiB und ist zu 72 % belegt.

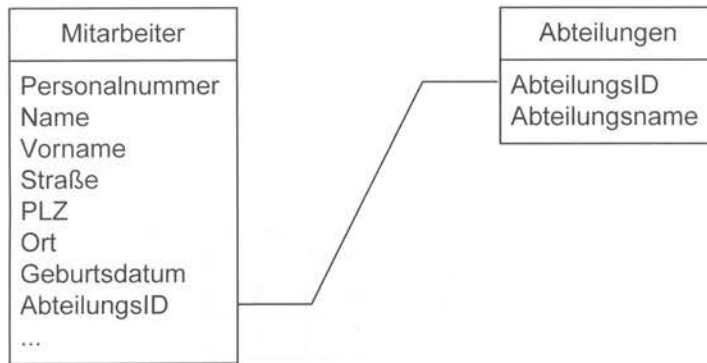
Berechnen Sie nachvollziehbar, um wie viele Festplatten (je 147 GiB) das SAN erweitert werden muss, um die Daten des Fileservers aufzunehmen und anschließend noch mindestens 200 GiB freien Speicherplatz zu haben. (5 Punkte)

Raid 6 provides fault tolerance from two drive failures; the array continues to operate with up to two failed drives. This makes larger RAID groups more reliable, especially for high-availability systems.

6. Handlungsschritt (20 Punkte)

Korrekturrand

Die Mitarbeiter/-innen der Global KG werden mithilfe der folgenden Datenbank verwaltet:



- a) Erstellen Sie eine SQL-Abfrage, die von allen Mitarbeitern und Mitarbeiterinnen jeweils Name, Vorname, Geburtsdatum und Abteilungsname liefert. (4 Punkte)

- b) Nennen Sie vier Eigenschaften eines Benutzers, die automatisch angelegt werden sollen. (2 Punkte)

- c) Benutzer werden im Netzwerk zu Gruppen zusammengefasst.
Erläutern Sie, warum diese Vorgehensweise sinnvoll ist. (2 Punkte)

Fortsetzung 6. Handlungsschritt →

Fortsetzung 6. Handlungsschritt

Korrekturrand

- d) In der Glabal KG sind u. a. die Sekretärin Sonja Wagner, die Personalsachbearbeiterin Jutta Brandt und der Systemadministrator Wilfried Freund beschäftigt. Weiterhin existieren die Benutzergruppen AlleMitarbeiter, Sekretariat, Personalverwaltung und Administratoren sowie die Verzeichnisse Vorlagen, Personal und Projekte.

Auf das Verzeichnis Vorlagen sollen AlleMitarbeiter Leserecht, Sekretariat das Ändernrecht und Administratoren Vollzugriff erhalten. Auf das Verzeichnis Personal soll die Gruppe Personalverwaltung Vollzugriff erhalten. Auf das Verzeichnis Projekte erhalten AlleMitarbeiter Leserecht, Sekretariat Ändernrecht und Administratoren Vollzugriff.

- da) Ergänzen Sie die folgende Tabelle über die Rechtestruktur:
(L = Lesen, Ä = Ändern, V = Vollzugriff)

(6 Punkte)

Benutzergruppen	Vorlagen			Personal			Projekte		
	L	Ä	V	L	Ä	V	L	Ä	V
AlleMitarbeiter	X	-	-	-	-	-			
Sekretariat									
Personalverwaltung									
Administratoren									

- db) Erläutern Sie, welches effektive Recht sich für Jutta Brandt im Verzeichnis Projekte ergibt.

(2 Punkte)

- dc) Erläutern Sie, ob Wilfried Freund ein Update an der Datenbank mitarbeiter.db im Verzeichnis Personal vornehmen kann.

(2 Punkte)

- e) In Netzwerken kommt bei der Benutzerverwaltung das Protokoll LDAP zum Einsatz.

Erläutern Sie die Aufgabe von LDAP bei der Benutzerverwaltung.

(2 Punkte)