

1

Ganzheitliche Aufgabe I Fachqualifikationen

Allgemeine Korrekturhinweise

Die Lösungs- und Bewertungshinweise zu den einzelnen Handlungsschritten sind als Korrekturhilfen zu verstehen und erheben nicht in jedem Fall Anspruch auf Vollständigkeit und Ausschließlichkeit. Neben hier beispielhaft angeführten Lösungsmöglichkeiten sind auch andere sach- und fachgerechte Lösungsalternativen bzw. Darstellungsformen mit der vorgesehenen Punktzahl zu bewerten. Der Bewertungsspielraum des Korrektors (z. B. hinsichtlich der Berücksichtigung regionaler oder branchenspezifischer Gegebenheiten) bleibt unberührt.

Zu beachten ist die unterschiedliche Dimension der Aufgabenstellung (nennen – erklären – beschreiben – erläutern usw.). Wird eine bestimmte Anzahl verlangt (z. B. „Nennen Sie fünf Merkmale ...“), so ist bei Aufzählung von fünf richtigen Merkmalen die volle vorgesehene Punktzahl zu geben, auch wenn im Lösungshinweis mehr als fünf Merkmale genannt sind. Bei Angabe von Teilpunkten in den Lösungshinweisen sind diese auch für richtig erbrachte Teilleistungen zu geben.

In den Fällen, in denen vom Prüfungsteilnehmer

- keiner der sechs Handlungsschritte ausdrücklich als „nicht bearbeitet“ gekennzeichnet wurde,
- der 6. Handlungsschritt bearbeitet wurde,
- einer der Handlungsschritte 1 bis 5 deutlich erkennbar nicht bearbeitet wurde,

ist der tatsächlich nicht bearbeitete Handlungsschritt von der Bewertung auszuschließen.

Ein weiterer Punktabzug für den bearbeiteten 6. Handlungsschritt soll in diesen Fällen allein wegen des Verstoßes gegen die Formvorschrift nicht erfolgen!

Für die Bewertung gilt folgender Punkte-Noten-Schlüssel:

Note 1 =	100 – 92 Punkte	Note 2 =	unter	92 – 81 Punkte	
Note 3 =	unter	81 – 67 Punkte	Note 4 =	unter	67 – 50 Punkte
Note 5 =	unter	50 – 30 Punkte	Note 6 =	unter	30 – 0 Punkte

1. Handlungsschritt (20 Punkte)

a) 2 Punkte

Entlastung des Hauptnetzes

b) 3 Punkte

Ein Multiprozessorboard mit 4 CPUs

Schnelle Ausführung von Anwendungsprogrammen

c) 4 Punkte

Server1

Dienste:

- Subdomaincontroller
- DNS
- DHCP

d) 2 Punkte

Erhöhung der Ausfallsicherheit

e) 2 Punkte

RAID 1 (Spiegelung)

RAID 5 (Stripe Set mit Parität)

f) 5 Punkte

49 IP-Adressen

	Adressen
DHCP	30
Server	3
Arbeitsstationen	14
Drucker	2

g) 2 Punkte

255.255.255.192 auch möglich /26

2. Handlungsschritt (20 Punkte)

a) 4 Punkte, 2 x 2 Punkte

- Einfache Anpassung des Netzes an die Unternehmensstruktur möglich: Veränderung nur der logischen und nicht der physikalischen Netzstruktur
- VLAN Wechsel eines Clients nur am Kopplungselement möglich
- Priorisierung von Daten (QoS)
- Bessere Nutzung der Bandbreite
- Entlastung des Netzes von Broadcast-/Multicast-Aufrufen
- Einfache Administration
- u. a.

b) 6 Punkte

Statisches (port-basierendes) VLAN:

Eindeutige und feste Zuordnung von Switchports zu einem VLAN

Dynamisches VLAN:

Zuordnung eines Clients zu einem VLAN erfolgt durch Protokollidentifikation, MAC-Adresse oder Authentifizierung (z. B. Radius-Server, Zertifikate).

c) 6 Punkte

- VLAN Tags werden von Frames entfernt, die an Ports gesendet werden, an denen sich Endgeräte befinden.
- VLAN Tags werden vom Switch hinzugefügt, wenn ein Frame von einem Switch zu einem anderen Switch (trunk) versendet wird.

d) 4 Punkte

- Der Rechner mit der MAC-Adresse XYZ darf sich im VLAN anmelden.
- Der Rechner mit der IP-Adresse a.b.c.d darf sich im VLAN anmelden.
- Der Rechner mit dem Zertifikat ABC darf sich im VLAN anmelden.
- u. a.

3. Handlungsschritt (20 Punkte)

aa) 3 Punkte, 3 x 1 Punkt

- Sicherheitsrichtlinien für Passwörter erstellen
- Rechte der Nutzer einschränken
- Nicht benötigte Systemdienste abschalten
- E-Mail-Anhänge auf Schädlinge prüfen
- Persönliche Firewalls einsetzen
- Hardware durch Sperren (BIOS, Wechselmedien) schützen
- Internetzugang sperren oder über Proxy leiten
- Internetbrowser maximal absichern
- Sicherheitstest durchführen
- Schulung und Sensibilisierung der Anwender
- u. a.

ab) 3 Punkte, 3 x 1 Punkt

- Abgestufte Sicherheitszonen mit Firewalls einrichten
- Subnetze einrichten
- IPsec bzw. IPv6 einführen
- Zugang zu Verteilerräumen sperren oder kontrollieren
- Nicht benötigte Netzdosen sperren
- Externe Personen beaufsichtigen
- Sicherheitsseminare für IT-Personal durchführen
- Sicherheitstest durchführen
- Netzwerk-Monitoring durchführen
- u. a.

b) 6 Punkte

1. Bezug des öffentlichen Schlüssels des Empfängers
2. Prüfung dieses öffentlichen Schlüssels auf Gültigkeit und Echtheit (CA)
3. Bildung eines Hash-Wertes anhand des E-Mail-Textes
4. Erstellung einer Signatur durch Verschlüsselung des Hash-Wertes mit privatem Schlüssel des Senders
5. Verschlüsselung des E-Mail-Textes und der Signatur mit dem öffentlichen Schlüssel des Empfängers
6. Versenden der verschlüsselten E-Mail

c) 4 Punkte

MD5: Hash-Funktion zur Signatur
RSA: Asymmetrisches Verschlüsselungsverfahren

d) 4 Punkte

Die Zeit zur Entschlüsselung verdoppelt sich bei jedem weiteren Bit. Bei 14 zusätzlichen Bits beträgt die Zeit zur Entschlüsselung demnach:

$$2^{14} / 24 / 7 = 97,5 \text{ Wochen}$$

4. Handlungsschritt (20 Punkte)

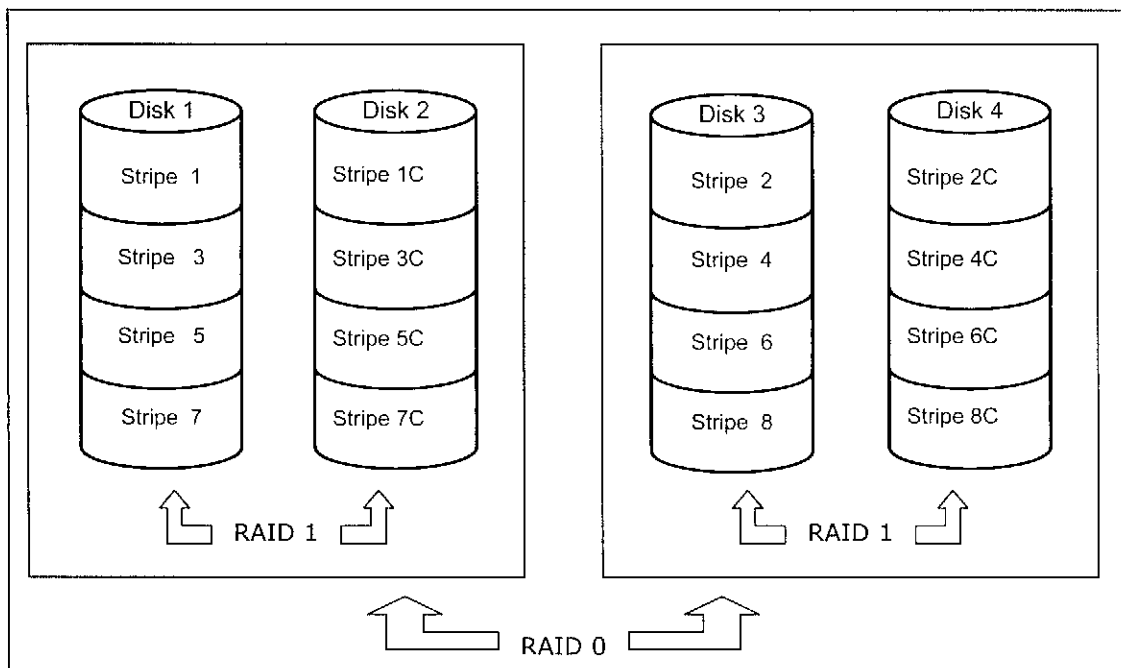
a) 3 Punkte, 3 x 1 Punkt

- Vereint die Vorteile von SATA (Geschwindigkeit) und SCSI (robustes Protokoll)
- Automatische Konfiguration, somit keine Adresskonflikte möglich
- Protokollkompatibilität mit SCSI
- Dual Port möglich
- Hohe Bandbreite durch serielle Punkt-zu-Punkt-Verbindung im Vollduplex-Modus
- Anschluss vieler Festplatten ist möglich, erweiterbar mit Expandern
- Vereinfachte Anschlusstechnik, kleinere aber längere Kabel, geringe Störanfälligkeit
- Hotplug-fähig
- Anschluss von SATA-Platten möglich, daher mehrstufige Speicherlösungen möglich
- u. a.

ba) 3 Punkte

250 GByte ($500 \times 2 / 4$)

bb) 6 Punkte



ca) 3 Punkte, 2 x 1,5 Punkt

2 Festplatten:

- Disk 1 und Disk 2
- Disk 3 und Disk 4

Andere Lösungen möglich, wenn Disk 1 bis 4 anders zu RAID 10 kombiniert wurden.

cb) 3 Punkte, 3 x 1 Punkt

3 Festplatten:

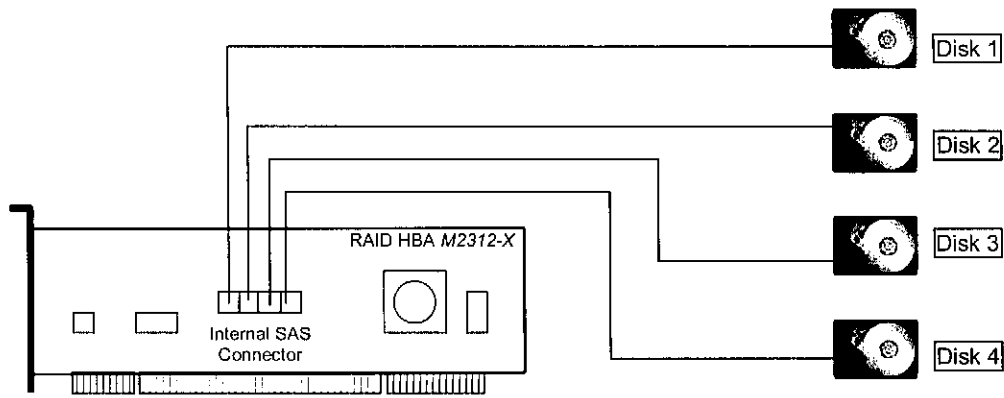
- Disk 1, Disk 3, Disk 4
- Disk 2, Disk 3, Disk 4
- Disk 1, Disk 2, Disk 3
- Disk 1, Disk 2, Disk 4

Andere Lösungen möglich, wenn Disk 1 bis 4 anders zu RAID 10 kombiniert wurden.

Fortsetzung 4. Handlungsschritt →

Fortsetzung 4. Handlungsschritt

d) 2 Punkte



Andere Lösungen möglich

5. Handlungsschritt (20 Punkte)

a) 10 Punkte, 5 x 2 Punkte

Beispiel: Leitungsmessung um Konnektivität auf Schicht 1 sicherzustellen
Physikalische Zuordnung der Clients und Server zu drei Segmenten mittels Switches oder Switch-Verbund (z. B. kaskadierende Switches)
Anschluss der Segmente an die zentrale Firewall
Konfiguration der IP-Adressen auf der Firewall. Die IP-Adressen müssen aus dem jeweiligen Subnetz des Segments sein
Konfiguration der Subnetz-Clients und -Server mit IP-Adressen aus dem Segment, der Subnetzwerkmaske und dem Gateway (IP-Adresse der Firewall in diesem Segment)
Erstellen der Regeln für den Zugriff aus den beiden Client-Netzen in das Server-Netz und vom Server-Netz in die Client-Netze

Hinweis: Andere Reihenfolge und andere logische Arbeitsschritte möglich

ba) 2 Punkte

Zielnetz	Subnetzmaske	Schnittstelle/Gateway
172.16.1.0	/24	172.16.1.254
172.16.2.0	/24	172.16.2.254
172.16.3.0	/24	172.16.3.254
192.168.10.0	/24	eth0 oder z.B. 192.168.254.2
0.0.0.0	0.0.0.0	SDSL

bb) 2 Punkte

Zielnetz	Subnetzmaske	Schnittstelle/Gateway
192.168.1.0	/24	192.168.1.254
192.168.10.0	/24	192.168.10.254
172.16.3.0	/24	eth1 oder z.B. 192.168.254.1
0.0.0.0	0.0.0.0	SDSL

c) 4 Punkte

Aktion	Protokoll	Quell-IP	Quell-Port	Ziel-IP	Ziel-Port	Interface	Richtung
allow	tcp	172.16.1.0/24	any	192.168.10.200/32	80	Eth0	Ausgehend
allow	tcp	192.168.10.200/32	80	172.16.1.0/24	any	Eth0	Eingehend
allow	tcp	172.16.2.0/24	any	192.168.10.200/32	80	Eth0	Ausgehend
allow	tcp	192.168.10.200/32	80	172.16.2.0/24	any	Eth0	Eingehend
allow	tcp	192.168.1.0/24	any	172.16.3.250/32	3200	Eth1	Eingehend
allow	tcp	172.16.3.250/32	3200	192.168.1.0/24	any	Eth0	Ausgehend

d) 2 Punkte

Portforwarding bzw. statisches NAT

6. Handlungsschritt (20 Punkte)

aa) 2 Punkte

- Bezeichnet ein Netzwerk oder einen Rechner
- Kann genutzt werden um ein privates Netzwerk aufzubauen, ähnlich dem privaten Adressraum 10.x.x.x bei IPv4.

ab) 2 Punkte

- Bezeichnet eine einzelne Netzwerkschnittstelle
- Pakete werden zu der festgelegten, eindeutigen Adresse der Netzwerkschnittstelle gesendet.

ac) 2 Punkte

- Bezeichnet eine Gruppe von Netzwerkgeräten
- Pakete werden zu einer bestimmten Gruppe von Netzwerkschnittstellen gesendet
- Bei IPv6 gibt es keine Broadcasts, diese Funktion wird durch Multicast-Adressen ersetzt

ad) 2 Punkte

- Adresse zwischen einer Unicast und einer Multicast-Adresse
- Bezeichnet eine oder wenige Schnittstellen einer Gruppe von Netzwerkgeräten (z. B. der nächste DNS- oder DHCP-Server)

b) Trace 1:

```
60 00 00 00 00 40 3A 40 FE C0 00 01 00 00 00 00
00 00 AF C1 00 B4 00 01 FE C0 00 01 00 00 00 00
00 00 00 BE FE 30 01 F0 81 00 A4 6B 0C 1C 00 41
52 0F 36 47 9F 89 0C 00 08 09 0A 0B 0E 0F 10 11
...
```

ba) 2 Punkte

6 = IPv6

bb) 2 Punkte, 2 x 1 Punkt

FEC0:0001:0000:0000:0000:AFC1:00B4:0001 = FEC0:1::AFC1:B4:1

bc) 2 Punkte, 2 x 1 Punkt

FEC0:0001:0000:0000:0000:00BE:FE30:01F0 = FEC0:1::BE:FE30:1F0

Trace 2:

```
45 00 00 54 A1 1B 00 00 41 01 55 52 C0 A8 01 02
C0 A8 01 E9 00 00 9B E3 3F 1C 00 09 24 13 36 47
D5 98 0D 00 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13
14 15 16 17 18 19 1A 1B 1C 1F 20 21 22 23 24 25
...
```

bd) 2 Punkte

4 = IPv4

be) 2 Punkte, 2 x 1 Punkt

C0 A8 01 02 = 192.168.1.2

bf) 2 Punkte, 2 x 1 Punkt

C0 A8 01 E9 = 192.168.1.233