Abschlussprüfung Winter 2013/14
Lösungshinweise

IHK

Fachinformatiker/Fachinformatikerin
Systemintegration
1197

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 fünf Handlungsschritte ausdrücklich als „nicht bearbeitet" gekennzeichnet wurde,
- der 5. Handlungsschritt bearbeitet wurde,
- einer der Handlungsschritte 1 bis 4 deutlich erkennbar nicht bearbeitet wurde,

ist der tatsächlich nicht bearbeitete Handlungsschritt von der Bewertung auszuschließen.

Ein weiterer Punktabzug für den bearbeiteten 5. 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 (25 Punkte)

a) 9 Punkte, 9 x 1 Punkt

Fehler Nr. 2

Beschreibung:	Client N2 mit falschem Gateway (192.168.1.**240**)
Auswirkung:	Keine Kommunikation mit anderen Netzen möglich
Fehlerbeseitigung:	Richtiges Gateway 192.168.1.254 eintragen

Fehler Nr. 3

Beschreibung:	Client N199 mit falscher Subnetzmaske (255.255.**0**.0)
Auswirkung:	Keine Kommunikation mit Clients an den anderen Standorten möglich
Fehlerbeseitigung:	Ändern der Subnetzmaske auf 255.255.255.0

Fehler Nr. 4

Beschreibung:	Clients A1 und A2 mit gleicher IP-Adresse (192.168.2.11)
Auswirkung:	Adresskonflikt, nur einer der Clients kann kommunizieren.
Fehlerbeseitigung:	Ändern der IP-Adresse von Client A2 auf 192.168.2.12

ba) 4 Punkte, 2 x 2 Punkte

- *Ping* überprüft die Erreichbarkeit eines Ziel-Hosts mit einem echo request.
- *Tracert* überprüft den Weg zu einem Ziel-Host.

bb) 3 Punkte

Die Kommunikation funktioniert nicht, weil auf dem Router in der Außenstelle B keine Route in das Netz der Zentrale (192.168.1.0/24) eingetragen ist.

bc) 3 Punkte

In die Routingtabelle des Routers der Außenstelle B-Heim muss eingetragen werden,
entweder der Route:

Netz	**Subnetzmaske**	**Schnittstelle/Next Hop**
192.168.1.0	255.255.255.0	10.10.10.13

oder der Defaultroute:

0.0.0.0	0.0.0.0	10.10.10.13

ca) 3 Punkte, 3 x 1 Punkt

- RIP ist ein Distanz-Vektor-Routing-Protokoll
- Metrik ist der Hop Count
- Austausch der Routingtabellen alle 30 Sekunden
- Maximaler Hop Count 15

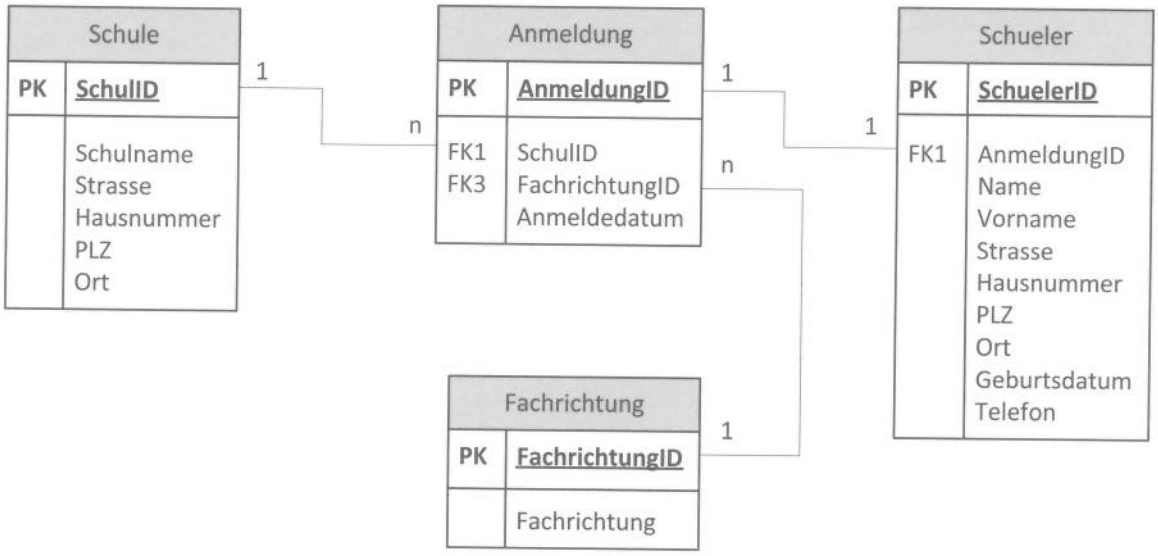
cb) 3 Punkte

Die Daten gehen direkt von der Außenstelle A-Hausen zur Außenstelle B-Heim über die SDSL-Leitung, da dieser Weg der mit den wenigsten Hops ist. Die Bandbreite der Verbindung spielt bei RIP keine Rolle.

2. Handlungsschritt (25 Punkte)

a) 10 Punkte

2 Punkte, 4 x 0,5 Punkte je Primärschlüssel
3 Punkte, 3 x 1 Punkt je Fremdschlüssel
3 Punkte, Kardinalitäten
2 Punkte, Entität Fachrichtungen



ba) 4 Punkte, 3 Punkte für Erläuterung und 1 Punkt für Vorteil

Erläuterung:
Sender und Empfänger kennen und benutzen für die Ver- und Entschlüsselung einer Nachricht den gleichen geheimen Schlüssel.

Vorteil: Schnellere Ver- und Entschlüsselung

Andere Lösungen sind möglich.

bb) 4 Punkte, 3 Punkte für Erläuterung und 1 Punkt für Vorteil

Erläuterung:

Der Empfänger besitzt einen öffentlichen und einen privaten Schlüssel (Public und Private Key). Der Empfänger schickt den öffentlichen Schlüssel an den Sender, der damit die zu übertragenden Daten verschlüsselt. – Nur der Empfänger kann diese Daten mit seinem privaten Schlüssel wieder entschlüsseln.

Vorteil: Der Schlüsselaustausch über einen unsicheren Kanal ist möglich.

Andere Lösungen sind möglich

ca) 3 Punkte

HTTPs verschlüsselt den http-Datenverkehr über den Port 443.

cb) 4 Punkte

Bei HTTPs authentifiziert sich der Server gegenüber dem Client mit seinem Zertifikat. Dieses enthält die digitale Signatur der CA. Diese Signatur prüft der Client mit dem Public Key der CA. Da der Client diesen Public Key nicht hat, kann er auch die Korrektheit des Zertifikats nicht bestätigen. → Sicherheitswarnung im Browser

3. Handlungsschritt (25 Punkte)

a) 6 Punkte

3600 GiB ((6 – 2 + 4 - 2) * 600 GiB)

Es stehen acht Festplatten zur Verfügung (vier Festplatten zu je 600 GiB und vier Festplatten zu 750 GiB). Bei RAID-6 werden zwei Festplattenkapazitäten für die Redundanz reserviert. Es bleiben sechs Festplatten. Zur Berechnung der Nettokapazität wird diese Anzahl (6) mit der Kapazität der kleinsten Festplatte (600 GiB) multipliziert.

ba) 3 Punkte, 1 Punkt Abzug für jedes zu viel genannte Band

V4 (1 Punkt)

2D2 (2 Punkte)

bb) 4 Punkte

Hinweis an die Korrektorin/den Korrektor:
Der Prüfling soll erkannt haben, dass wegen der gesetzten Archive-Bits bei den nächsten Tagessicherungen alle Dateien gesichert werden. Das entspricht im Prinzip jeweils einem Vollbackup.

Beispiel für eine Lösung:

Nach dem Restore sind die Archiv-Bits aller Dateien gesetzt. Die Differenzielle Datensicherung sichert alle Dateien, deren Archiv-Bit gesetzt ist und setzt die Archiv-Bits anschließend **nicht** zurück. Damit sind die Datensicherungen vom Donnerstag, Freitag und Samstag im Prinzip Vollbackups. Dies erklärt den erhöhten Zeitbedarf für die Datensicherung.

c) 3 Punkte

Nicht sinnvoll, da sich die Auslagerungsdatei im Backup auf den Systemzustand vor dem Systemabsturz bezieht und daher nicht mehr relevant ist.

Die Auslagerungsdatei wurde vom Betriebssystem bereits neu erstellt.

d) 3 Punkte

Die Gigabit-Ethernet Schnittstelle ist mit ca. 1.000 MBit/s die Schnittstelle mit der niedrigsten Datenübertragungsrate.

Hinweis an die Korrektorin/den Korrektor:
Genaue Werte werden nicht verlangt, hier nur zur Übersicht:

SATA-III	600 MB/s
eSATA	300 MB/s
Gigabit-Ethernet	125 MB/s
SAS-2	600 MB/s
PCIe 2.1 - x2	1.000 MB/s

e) 6 Punkte

4 Akkupacks

Anzahl Akkupacks = (Belastungsleistung · Überbrückungszeit)/(Kapazität je Akkupack · Spannung)
4 Akkupacks ~ 3,75 = (1.500 VA · 1h) / (20 Ah · 24 V)

4. Handlungsschritt (25 Punkte)

a) 4 Punkte, 4 x 1 Punkt

- IP-Adresse
- Subnetzmaske
- Gateway
- DNS-Server
- WINS-Server
- Timeserver
- u. a.

ba) 3 Punkte

Auflösung der Namen in IP-Adressen
Der Client sendet eine Anfrage mit den Zielnamen an den DNS-Server. Der DNS-Server gibt die IP-Adresse an den Client zurück.

Andere Lösungen möglich

bb) 4 Punkte

Ausgabe	Beschreibung
`> nslookup www.ihk.de`	Befehlsaufruf
`Server: dns.local`	Name des lokalen DNS-Servers
`Address: 192.168.1.250`	IP-Adresse des DNS-Server
`Nicht autorisierte Antwort:`	Lokaler DNS konnte den Namen nicht selbst auflösen
`Name: www.ihk.de`	Aufgelöster Name
`Address: 141.88.222.155`	IP-Adresse des IHK-Servers

bc) 4 Punkte

Der lokale DNS-Server kann nur Namensanfragen für seine eigene Domäne beantworten. Namensanfragen für andere Domänen müssen von anderen DNS-Servern aufgelöst werden. Deswegen werden diese Anfragen an den Forwarder weitergeleitet.

bd) 3 Punkte

Root-Nameserver bilden die Wurzel eines DNS-Serververbunds, der hierarchisch aufgebaut ist. Wenn ein lokaler DNS oder der DNS beim ISP (Internet Service-Provider) einen Domain-Namen nicht im Speicher hat, wird dieser beim nächsthöherem Nameserver nachgefragt, dies kann bis zu den Root-Nameservern erfolgen, um die IP des Toplevel-Domainservers zu erhalten.

Andere Lösungen möglich

ca) 3 Punkte

Die E-Mails werden nicht mehr vom E-Mail-Server heruntergeladen (POP3), sondern verbleiben auf den E-Mail-Server (IMAP4). So können die E-Mails von verschiedenen Rechnern gelesen werden.

Andere Lösungen möglich

cb) 2 Punkte

Es muss das Protokoll für den Posteingangsserver von POP3 auf IMAP4 geändert werden.

cc) 2 Punkte

Änderung an der Firewall bzw. am Router

Alternativ:
Im Falle einer neuen IP-Adresse des Mail-Servers könnte der mx-Eintrag im DNS-Server geändert werden.

5. Handlungsschritt (25 Punkte)

a) 3 Punkte

- Wesentlich größerer Adressraum durch 128 Bit Adressen
- Schnelleres Routing (Wegfall der IP-Header-Checksum, Flowlabel)
- Mobile IP-Adresse
- Autokonfiguration der Clients
- u. a.

ba) 2 Punkte

```
2001:DB8:45:C00::/60
```

bb) 3 Punkte

16 Subnetze
64 Bit Netz-ID (128 Bit IPv6 Adresse – 64 Bit Host-Identifier)
60 Bit sind bereits vorgegeben, verbleiben 4 Bit zur eigenen Verfügung -> 2^4 = 16 Subnetze

c) 3 Punkte

Auf dem Host sind sowohl das IPv4- als auch das IPv6-Protokoll konfiguriert und aktiviert.

da) 2 Punkte

```
fe80::2e0:81ff:fe55:32a7
```

db) 2 Punkte

```
2001:db8:45:c00:2e0:81ff:fe55:32a7
```

dc) 5 Punkte

Die globale eindeutige Adresse (öffentliche Adresse) des Clients besteht aus einer 64-Bit-Netz-ID und einer 64-Bit-Interface-ID. Die Interface-ID wurde aus der MAC-Adresse generiert. Damit ist es möglich, IP-Pakete auf die MAC-Adresse des Hosts zurückverfolgen. Ein anonymes Surfen ist damit nicht mehr möglich.

Alternativ:
Der Client kann über seine globale eindeutige Adresse (öffentliche Adresse) auch von außen erreicht werden, da im Gegensatz zu IPv4 kein NAT mehr stattfindet. Möglichkeit für einen Angriff auf den Client.

dd) 5 Punkte

Auf dem Client ist kein IPv6-Gateway eingetragen.
Dieser muss in der IPv6-Konfiguration ergänzt werden, um die Kommunikation aus dem eigenen Netz heraus zu ermöglichen.