Abschlussprüfung Sommer 2023
Lösungshinweise

Fachinformatiker/Fachinformatikerin
Systemintegration (AO 2020)
1202

2 Analyse und Entwicklung von Netzwerken

Teil 2 der Abschlussprüfung

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.).

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. Aufgabe (26 Punkte)

aa) 4 Punkte

- Mehr Sicherheit, da logische Trennung der Netzwerksegmente
- Mehr Flexibilität, da neue Netzwerksegmente leicht erzeugt werden können
- Weniger Hardware, da mehrere Netzwerksegmente auf einem Switch/Kabel laufen
- Weniger Kosten, da weniger Hardware angeschafft werden muss
- Weniger Verkabelung, da mehrere Netzwerksegmente auf einem Switch/Kabel laufen

Andere Lösungen sind möglich.

ab) 3 Punkte

Zwischen den Switches muss die Information, zu welchem VLAN ein Frame gehört, mitgeschickt werden. Ein Standard-Frame hat dafür keine Felder in seinem Header vorgesehen. Eine Information, die in diesen Tag geschrieben wird, ist die VLAN-ID.

Andere Lösungen sind möglich.

ac) 4 Punkte

Statisch: Der Administrator ordnet die Ports manuell fest einem bestimmten VLAN zu. Beispiel: Ports in der Werkstatt werden dem VLAN „Werkstatt" zugeordnet.
IEEE 802.1X: ein Gerät wird anhand der Anmeldedaten einem bestimmten VLAN zugeordnet. Beispiel: Der Useraccount „Chef" wird immer dem VLAN-Verwaltung zugeordnet, egal an welchem PC des Unternehmens er sich anmeldet.

ba) 4 Punkte

DHCP Discover
DHCP Offer
DHCP Request
DHCP Ack

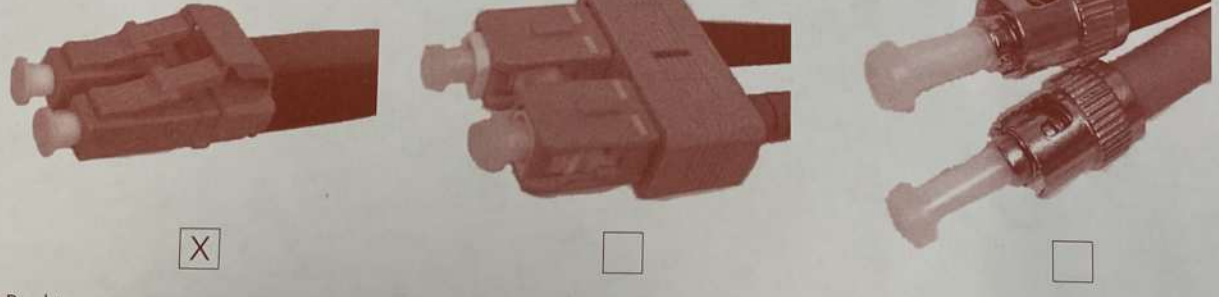
bb) 3 Punkte

DHCP arbeitet als Broadcast, dieser endet am Layer-3-Switch. DHCP-Relay für jedes VLAN-Interface konfigurieren, sodass der DHCP-Broadcast an den DHCP-Server weitergeleitet wird.
(ip helper-address auch gültige Lösung)

ca) 3 Punkte

SFP-Module erweitern einen Switch um einen bestimmten Anschluss, bspw. um dort eine Glasfaser anschließen zu können. SFP+ bietet höhere Übertragungsrate als SFP (SFP+ 10 GBit/s, SFP nur bis 1 GBit/s).

cb) 1 Punkt



[X] [ ] [ ]

cc) 4 Punkte

Protokoll	Funktionsweise, solange beide Leitungen störungsfrei sind	Reaktion der Verbindung, wenn eine Leitung ausfällt
Spanning-Tree-Protocol	STP lässt eine der beiden Leitungen ungenutzt liegen, weiß aber, dass diese Verbindung vorhanden ist.	Fällt die verwendete Leitung aus, so aktiviert der STP-Algorithmus die ungenutzte Leitung und überträgt die Daten über diese Leitung.
Link-Aggregation	Die beiden Leitungen werden „gebündelt", sodass sich die Übertragungsrate zwischen den Switches verdoppelt.	Fällt eine der beiden Leitungen aus, so werden die Daten nur noch mit reduzierter Übertragungsrate über die verbleibende Leitung gesendet.

2. Aufgabe (25 Punkte)

aa) 9 Punkte

IPv4-Routentabelle			
Aktive Routen für:	**Router Essen**		
Netzwerkziel	**Netzmaske**	**Gateway/Next-Hop**	**Interface**
10.1.0.0	255.255.0.0	direct	IF1
10.2.0.0	255.255.0.0	192.168.0.2	-
10.3.0.0	255.255.0.0	192.168.0.6	-
10.4.0.0	255.255.0.0	192.168.0.10	-
192.168.0.0	255.255.255.252	direct	IF2
192.168.0.4	255.255.255.252	direct	IF3
192.168.0.8	255.255.255.252	direct	IF4
0.0.0.0	0.0.0.0	210.10.10.1	-
210.10.10.1	255.255.255.255	direct	dsl

ab) 4 Punkte

Nur mit dynamischem Routing kann das Netz selbstständig auf Störungen reagieren und somit redundant sein.

ac) 4 Punkte

Link-State, da bei DV die direkte Verbindung zwischen Duisburg und Essen weiterhin bevorzugt werden würde.

ba) 5 Punkte

IP 10.1.0.10 wird bereits von einem anderen Gerät genutzt. Daher hat sich der File-Server die APIPA-Adresse 169.254.102.223 zugewiesen.

bb) 3 Punkte

Gerät mit der IP `10.1.0.10` identifizieren und diesem Gerät eine andere IP zuweisen. Anschließend IP-Konfiguration auf dem Fileserver aktualisieren.

3. Aufgabe (20 Punkte)

aa) 4 Punkte

End-to-Site:
Die Fahrguth GmbH nutzt diese Variante, um den Außendienstmitarbeitern/Home-Office-Arbeitern Zugriff auf das Firmennetz zu gewähren.

Site-to-Site:
Die Fahrguth GmbH nutzt diese Variante, um die verschiedenen Filialen gesichert an die Zentrale anzubinden.

Andere Beispielsituationen sind auch denkbar.

ab) 3 Punkte

- Version
- Seriennummer
- Inhaber (Common Name, Orga etc.)
- Public Key des Inhabers
- Algorithmen-ID
- Aussteller (Zertifizierungsstelle)
- Gültigkeit
- Signatur-Algorithmus
- Signatur (verschlüsselter Hash-Wert)

b) 5 Punkte (3 Punkte für Fehlerursache, 2 Punkte für Vorschlag Fehlerbeseitigung)
Fehlerursache:
- Der Hotspot verwendet NAT und evtl. PAT. Es werden IP und Ports verändert, dadurch kann die Integrität der Pakete verletzt werden und die Pakete werden verworfen.
- Bei IPsec mit ESP kann der Hotspot-Router die TCP bzw. UDP-Checksummen nicht überprüfen. Die Pakete werden als ungültig verworfen.

Fehlerbeseitigung:
Einsatz von NAT-Traversal bei IPsec

oder

Fehlerursache:
Paketgröße (MTU) zu groß eingestellt. Die Pakete werden fragmentiert, dadurch wird die Integrität verletzt und die Pakete werden verworfen

Fehlerbeseitigung:
Paketgröße (MTU) im VPN-Client verringern

Weitere Lösungen sind möglich.

ca) 5 Punkte
Der Laptop wird an einem Netz betrieben, das IPv4 und IPv6 unterstützt. Vom Router erhält der Laptop zusätzliche IPv6-Adressen. Diese IPv6-Adressen nutzt der Client, um Verbindung mit dem Internet herzustellen. Die VPN-Verbindung wird umgangen (IPv6 VPN Breakout).

cb) 3 Punkte
- Auf den Laptops das IPv6-Protokoll in der Netzwerkkonfiguration auf disable setzen.
- Dual-Stack deaktivieren
- IPv6-Netzwerk in die Konfiguration des VPN-Client aufnehmen.

Weitere Lösungen sind möglich.

4. Aufgabe (29 Punkte)

aa) 2 Punkte
DNS übernimmt die Auflösung von Hostnamen bzw. URLs in IP-Adressen bzw. umgekehrt.

ab) 3 Punkte
Durch die Einrichtung der Weiterleitung muss der lokale DNS-Server die Anfrage nicht selbst iterativ auflösen. Er sendet die komplette Anfrage an den DNS-Server des Providers weiter, dieser hat evtl. schon viele Einträge in seinem Cache liegen und kann die Anfrage schnell beantworten.

ac) 6 Punkte
Der Nameserver löst die Anfrage iterativ auf. Er befragt zunächst die Root-Server, wer für die DE-Zone zuständig ist. Dort fragt er nach, wer in der Zone DE für den Bereich `ihk.de` verantwortlich ist. Von dort holt er sich die IP-Adresse für `www.ihk.de`.

ba) 3 Punkte
Es fehlen die A-Records der beiden Mail-Server.

bb) 5 Punkte
Der Absender `newsletter@fahrguth.gmbh` kann nicht vom Newsletter-Anbieter verwendet werden, da der SPF-Eintrag dies nicht zulässt. Der korrekte SPF-Eintrag würde es dem Newsletter-Anbieter erlauben, Mails mit der Domäne `fahrguth.gmbh` als Absender zu versenden.

c) 4 Punkte
- DNS-Spoofing: Dem beim Kunden eingetragenen DNS-Server wurden massenweise gefälschte DNS-Antworten gesendet. Bei Erneuern des DNS-Caches wurde ein gefälschter Eintrag (IP-Adresse) für die Seite `www.fahrguth.gmbh` gespeichert und als neue Antwort weitergegeben.
- DNS Injection: Im DNS-Server wurden gefälschte/falsche Daten konfiguriert.
- u. a.

d) 6 Punkte
Authentizität: Der Absender der DNS-Auskunft ist der, für den er sich ausgibt. Hierzu wird eine digitale Signatur bzw. ein digitales Zertifikat benutzt.
Integrität: Die ausgelieferte DNS-Auskunft wurde auf ihrem Weg zum Empfänger nicht verändert. Dazu werden Hash-Werte des Inhalts gebildet, die vom Empfänger überprüft werden können.