Abschlussprüfung Winter 2024/25
Lösungshinweise

Fachinformatiker/Fachinformatikerin
Systemintegration
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 (25 Punkte)

aa) 6 Punkte

- Die Aufteilung eines Netzwerks in VLANs verkleinert die Broadcast-Domänen und reduziert damit unnötigen Datenverkehr.
- Benutzer oder Geräte können unabhängig von ihrer physischen Position flexibel im Netzwerk einem bestimmten VLAN zugeordnet werden.
- Die Sicherheit erhöht sich, da sich die Benutzer in verschiedenen Netzsegmenten befinden.
- Die Skalierung des Netzwerkes wird erleichtert.
- Dienste können priorisiert werden (QoS).
- Die vorhandenen Switche können Ports, Bandbreiten und Uplinks effizient nutzen und damit Kosten reduzieren.
- Die Verwaltung des Netzwerkes wird vereinfacht.

Weitere Lösungen sind möglich.

ab) 6 Punkte

Portbasierte VLANs werden auf einem Switch konfiguriert und basieren auf den physischen Ports des Switches. Jeder Port ist einem bestimmten VLAN zugeordnet, unabhängig davon, welches Gerät an diesen Port angeschlossen ist.

Dynamische VLANs sind flexibel und erlauben die Zuordnung von VLANs basierend auf den Merkmalen des Benutzers oder des Geräts, wie Anmeldeinformationen oder anderen Identifikationsmerkmalen, das an den Switch angeschlossen ist.

Ähnliche Lösungen sind möglich.

ba) 3 Punkte

Ausgehende Frames auf diesem Port werden um einen Tag erweitert, in dem unter anderem die VLAN-ID mitgesendet wird. Bei eingehenden Frames wird diese VLAN-ID ausgewertet und der Frame dem entsprechenden VLAN zugeordnet.

bb) 2 Punkte

1 Punkt für Port 1, 2 und 3
1 Punkt für Port 7
1 Punkt Abzug, falls Port 8 angekreuzt ist

Core-Switch	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8
Option: Tagged	X	X	X				X	

ca) 2 Punkte

Auf dem Trunk werden Frames, die dem native VLAN zugeordnet sind, übertragen, ohne dass sie mit einem Tag versehen werden.

cb) 2 Punkte

Sind default VLAN und native VLAN identisch, so besteht die Gefahr, dass das Netzwerk durch VLAN-Hopping angegriffen wird.

d) 4 Punkte

- Einrichtung eines Management VLANs für die Verwaltung und Überwachung der Netzwerkinfrastruktur
- Zuweisen einer IP-Adresse auf dem Management VLAN des Switches
- Einrichten eines geeigneten Netzwerkprotokolls wie ssh oder https auf dem Switch
- Verwendung komplexer Kennwörter und sicherer Zugriffskontrolle
- 2FA
- Aktivitäten auf dem Switch loggen und protokollieren
- Regelmäßige Firmware-Updates durchführen

Andere Lösungen sind möglich.

2. Aufgabe (30 Punkte)

aa) 4 Punkte

VLAN	Netzwerk-ID	Subnetzmaske
10	172.16.0.0	255.252.0.0
20	172.20.0.0	255.252.0.0
30	172.24.0.0	255.252.0.0
40	172.28.0.0	255.252.0.0

ab) 5 Punkte

VLAN	IP des Standardgateways
10	172.19.255.254
20	172.23.255.254
30	172.27.255.254
40	172.31.255.254

Ggf. Folgefehler aus Aufgabe aa) berücksichtigen!

VLAN	IP des Standardgateways
99	10.255.255.254

ac) 2 Punkte
192.168.0.0 /16

ba) 2 Punkte
Der Client kann den DHCP-Server nicht erreichen und erzeugt sich dann selbstständig eine Adresse aus diesem Bereich (APIPA).
Alternativ: Bei IPv4-Adresskonflikten kann ebenfalls diese Adresse zugeordnet werden.

Ähnliche Lösungen sind möglich.

bb) 4 Punkte
Vermutlich ist keine DHCP-Weiterleitung eingerichtet. DHCP arbeitet mit Broadcast-Nachrichten, die nicht in ein anderes Netz weitergeleitet werden. Dies muss auf dem Core-Switch manuell aktiviert werden. (Andere Lösungen sind möglich.)

ca) 2 Punkte
Alle internen Netze sind direkt mit dem Core-Switch verbunden. Nur Traffic, der in ein entferntes Netz (das Internet) geschickt werden muss, muss an den Router gesendet werden.

cb) 2 Punkte

Netzwerk-ID	Subnetzmaske (dezimal)	Next-Hop
0.0.0.0	0.0.0.0	192.168.250.2

da) 3 Punkte
Durch NAT und PAT wird beim Verlassen des Firmennetzes durch den Router die interne private Adresse und die Portnummer durch die öffentliche IPv4-Adresse und eine neue Portnummer ersetzt. Auf dem Rückweg des Traffics wird dieser Tausch rückgängig gemacht.

Andere Formulierungen sind möglich.

db) 2 Punkte
Vorteile:
- Die interne Struktur des Netzes ist nach außen nicht sichtbar (masquerading).
- Viele Geräte können über eine einzige öffentliche IPv4-Adresse mit dem Internet kommunizieren.
- u. a.

Nachteil:
- Interne Geräte sind von außen nicht ohne Weiteres direkt adressierbar.
- Keine echte Ende-zu-Ende-Verbindung bei der Kommunikation
- u. a.

ea) 2 Punkte
Die letzten 64 Bit dürfen nicht verwendet werden. Für das Subnetting steht der Bereich ab dem 56. Bit zur Verfügung: 64 – 56 = 8
Mit diesen 8 Bit können 256 Subnetze gebildet werden (2 hoch 8).

eb) 2 Punkte
Erstes Netz: 2001:db8:1234::/64
Letztes Netz: 2001:db8:1234:ff::/64

3. Aufgabe (22 Punkte)

aa) 2 Punkte
Der Router ist mit IPv6 erreichbar.
Weitere Lösungen sind möglich (z. B. ICMPv6).

ab) 6 Punkte

Zeile 2:	Name des antwortenden DNS-Servers; hier ns.ihk-med.de
Zeile 3:	IP-Adresse des DNS-Servers; hier IPv6-Adresse 2001:db8:1234::53
Zeile 4:	„nicht autorisierende Antwort" gibt an, dass es kein offizieller DNS-Server bzw. ein lokaler DNS-Server ist.
Zeile 5:	Name des abgefragten Servers; hier www.google.de
Zeile 6:	IPv6 Adresse von www.google.de 2a00:1450:4001:815::2003
Zeile 7:	IPv4 Adresse von www.google.de 142.251.36.163

Ähnliche Lösungen sind möglich.

b) 2 Punkte
Fehlerquelle:
- Falsche Konfiguration der Netzwerkkarte, 100 Mbit/sec eingestellt
- Falsche Konfiguration des Ports am Switch; 100 Mbit/sec eingestellt
- Fehlerhafte Verbindung in der Netzwerkverkabelung
- u. a.

ca) 3 Punkte
- Am Webserver ist das Protokoll icmp abgeschaltet.
- Die Website www.ihk-med.de ist durch eine Firewall geschützt, die icmp bzw. ping blockiert.
- Die eigene Firewall blockiert ausgehende bzw. zurückkommende icmp-Pakete.
- u. a.

cb) 3 Punkte
- Im Webserver ist kein Default-Eintrag auf „index.html" o. Ä. konfiguriert.
- Die Datei „index.html" o. Ä. ist nicht vorhanden.
- Der Dateipfad zu „index.html" o. Ä. ist nicht verfügbar.
- u. a.

d) 6 Punkte
Grund: (3 Punkte)
Der alias DNS Eintrag CNAME für ftp.ihk-med.de zeigt auf den DNS-Namen ihk-med.de (IP 203.0.113.80). Somit wird Anfrage auf einen falschen Server weitergeleitet.

Fehlerbeseitigung: (3 Punkte)

Eintrag 5. Zeile ändern auf
ftp.ihk-med.de. CNAME ftp1.ihk-med.de.

Oder

Zeile 5 löschen und folgende zwei Zeilen einfügen:
ftp.ihk-med.de. A 203.0.113.21
ftp.ihk-med.de. AAAA 2001:db8:1234::21

4. Aufgabe (23 Punkte)

aa) 6 Punkte
Aufbau einer HTTPS-Verbindung zwischen NGFW und Website. Aufbau einer HTTPS-Verbindung zwischen Client und NGFW mittels eigenen NGFW-Zertifikats. Überprüfen der Daten der Website hinsichtlich der Vorgaben in der NGFW.

Oder

Es kommt keine Verbindung zwischen Client und Webseite zustande. Eine Verbindung wird zwischen Client und NGFW und weiterhin zwischen NGFW und Webseite aufgebaut, dadurch kann die NGFW als (gewünschter) Man-in-the-Middle fungieren.

Andere Lösungen sind möglich.

ab) 2 Punkte
Überprüfen der Inhalte der Website trotz TLS/HTTPS-Verbindung möglich

ac) 4 Punkte
- Man-in-the-Middle- (MitM) Angriffe innerhalb der NGFW möglich
- Datenschutz hinsichtlich des Mitarbeiters ist kompromittiert
- Höhere Performance der NGFW notwendig
- Bestimmte Dienste/Seiten im Internet sind ggf. nicht funktionsfähig
- Ende-zu-Ende-Verbindung wird aufgebrochen

ad) 2 Punkte
- Verbieten privater Nutzung des Internets
- Information des Mitarbeiters/Betriebsrates

ba) 3 Punkte
Fehler: Die (Intermediate) CA ist dem Browser nicht bekannt. (1 Punkt)
Behebung: Intermediate CA im Browser oder Betriebssystem hinterlegen. (2 Punkte)

bb) 3 Punkte
Fehler: Die Gültigkeitsdauer des (Intermediate) Zertifikats ist abgelaufen. (1 Punkt)
Behebung: Neues Intermediate Zertifikat erstellen mit validem Gültigkeitszeitraum. (2 Punkte)

Alternativ:
Fehler: Systemzeit des Clients ist falsch. (1 Punkt)
Behebung: Systemzeit aktualisieren. (2 Punkte)

bc) 3 Punkte
Fehler: Die von der NGFW angebotene SSL/TLS-Version oder die vorgeschlagene Verschlüsselung stimmen nicht mit den im Browser erwarteten Versionen überein. (Hierfür sind verschiedene Ursachen möglich.) (1 Punkt)

Eine der folgenden Alternativen ist möglich: (2 Punkte)
- Behebung: Browser aktualisieren
- Behebung: SSL/TLS-Cache löschen oder System neu starten
- Behebung: NGF updaten