Abschlussprüfung Winter 2021/22
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 (30 Punkte)

a) 8 Punkte

Bereich	Anzahl Hosts	Netzadresse	Subnetzmaske (dezimal)
Abteilung 1	80	**172.16.102.0**	**255.255.255.128**
Abteilung 2	50	**172.16.102.128**	**255.255.255.192**
Abteilung 3	20	**172.16.102.192**	**255.255.255.224**
IT	10	**172.16.102.224**	**255.255.255.240**

b) 6 Punkte

Netzwerk	Subnetzmaske (dezimal)	Schnittstelle	Next-Hop
172.16.64.0	**255.255.224.0**	**eth0**	**10.10.10.42**
172.16.96.0	**255.255.252.0**	**eth0**	**10.10.10.42**
203.0.113.8	**255.255.255.248**	**eth0**	**10.10.10.42**
172.16.100.0	**255.255.254.0**	**eth1**	**10.10.10.54**
0.0.0.0	**0.0.0.0**	**eth0**	**10.10.10.42**

Die ersten drei Zeilen sind optional, sie können entfallen, wenn die Default-Route (letzte Zeile) richtig gesetzt ist.

c) 6 Punkte

Richtung	Quell-IP	Ziel-IP	Quell-Port	Ziel-Port	Protokoll	Regel
eingehend	any	203.0.113.10	any	**443**	**TCP**	**accept**
eingehend	any	203.0.113.11	**any**	**25**	**TCP**	accept
eingehend	**any**	**203.0.113.11**	any	993 (IMAP TLS)	**TCP**	**accept**
eingehend	**any**	203.0.113.11	**any**	465 (SMTP TLS)	**TCP**	**accept**
eingehend	any	**203.0.113.11**	any	587 (SMTP STARTTLS)	TCP	accept
eingehend	**any**	**any**	**any**	**any**	**any**	drop

Die Bewertung erfolgt mit 1 Punkt pro Zeile.

d) 4 Punkte

- Intrusion Detection System/Intrusion Prevention System – automatische Erkennung und Abwehr von externen Angriffen (z. B. Abwehr von SYN Flood)
- Schadsoftwareerkennung – Filterung des Datenverkehrs (z. B. eingehende SMTP, Web, SQL, SMB-Verbindungen)
- Anti-Virus-/Anti-SPAM-Filter Mail-Relay – Filterung von eingehenden E-Mails auf bekannte Schadsoftware/SPAM-Merkmale
- QoS-Management – Priorisierung von Netzwerkdiensten (z. B. VoIP) und Bereitstellung abgestufter Bandbreiten für die Datenübertragung
- Payload des Datenstroms – Anwendungen werden identifiziert und können blockiert oder in der Nutzung der Bandbreite eingeschränkt werden.
- u. a.

e) 6 Punkte

Pro „dynamisches Routing"/contra „statisches Routing":

- Routing-Entscheidungen basieren auf dem aktuellen Status des Netzwerkes/Leitungen
- Es wird automatisch nach alternativen Routen gesucht
- Ausfall von einzelnen Leitungen führen nicht zu einem Totalausfall
- Netzwerk dynamisch erweiterbar (neuer Standort)
- Wartungsaufwand geringer, da neue Netzwerke automatisch bei den anderen Standorten konfiguriert werden

Contra „dynamisches Routing"/pro „statisches Routing":

- Höhere Prozessorlast als beim statischen Routing
- Höhere Netzwerkbelastung, da Routinginformationen regelmäßig übertragen werden
- Höherer Aufwand für die Konfiguration und Wartung
- Wissen über Konfiguration von Routing-Protokollen erforderlich

Weitere Argumente auch möglich!

2. Aufgabe (21 Punkte)

a) 4 Punkte

Accesspoint	– Übergang zwischen kabelgebundenem und kabellosem Netzwerk – Strahlt „das WLAN" aus, strahlt die Funksignale/-wellen aus – u. a.
WLAN-Controller	– Zentrale Konfiguration der Accesspoints – Überwachung der Accesspoints – u. a.

b) 4 Punkte
WPA2-PSK verwendet einen gemeinsamen (geheimen) Netzwerkschlüssel für die Verbindung mit dem WLAN, in der Enterprise-Variante kommen benutzerbezogene Zugangsdaten zum Einsatz. Dies ist von Vorteil, wenn bspw. ein Mitarbeiter das Unternehmen verlässt, da dann gezielt dessen Zugangsdaten deaktiviert werden können und das Passwort nicht an allen Geräten im WLAN geändert werden muss.

c) 3 Punkte
Authentifizierung: feststellen, wer der anfragende Benutzer ist (Username/Passwort)
Autorisierung: Zuteilen von Rechten an den Benutzer (Zugriff auf das Netzwerk)
Accounting: Erfassen der Nutzung durch den Benutzer (Zeit, Datenvolumen)

d) 4 Punkte
Die Gäste erhalten jeweils einen Zettel (Ticket) mit Zugangsdaten, die für einen bestimmten Zeitraum gültig sind. Diese müssen sie auf einer Website eingeben, die nach Verbindung mit der angegebenen SSID erscheint.

Vorteile z. B.:
- Durch das Zugangsportal kann vom Gast die Zustimmung zu den Nutzungsbedingungen eingeholten werden.
- Zeitliche Begrenzung
- Volumenabhängige Begrenzung
- Freigabe von Diensten abhängig vom jeweiligen Ticket
- Auf der Portalseite können dem Gast direkt Informationen angeboten werden, z. B. zu eigenen Produkten (Promotion, Umfrage etc.)
- u. a.

e) 6 Punkte
Switch A sollte nicht ausgewählt werden, da die Anzahl Ports nicht ausreichend ist. Es ist mindestens ein Port für den Uplink zu einem anderen Switch erforderlich, denn die Ausleuchtung hat ergeben, dass acht Accesspoints benötigt werden.

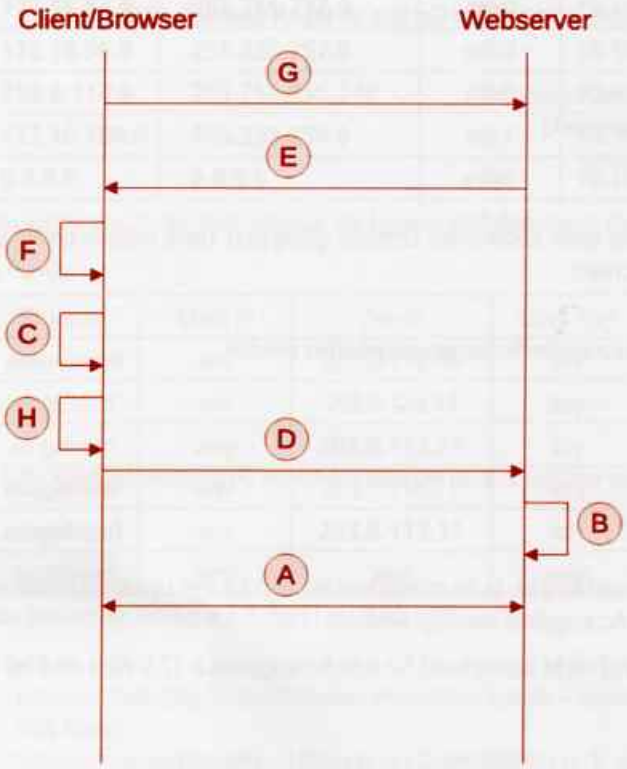
Switch B sollte nicht ausgewählt werden, da die Gesamtleistung über PoE nicht ausreichend für acht Accesspoints à 17,9 Watt ist. Eine Lösung über externe PoE-Injektoren wäre denkbar.

Switch C kann gewählt werden.

3. Aufgabe (21 Punkte)

a) 4 Punkte
- Version
- Name des Zertifikatsinhabers
- Signaturverfahren
- Aussteller des Zertifikats (CA)
- Gültigkeitsdauer
- Verschlüsselungsverfahren
- Öffentlicher Key (encryption) des Zertifikatsinhabers
- u. a.

b) 8 Punkte
Lösungshinweise



c) 6 Punkte
Hybrid: Es wird sowohl ein asym. wie auch ein sym. Verfahren eingesetzt.
Bei TLS bedeutet dies: Beim Verbindungsaufbau/Schlüsselaustausch wird ein asym. Verfahren eingesetzt, nach dem Schlüsselaustausch wird auf ein sym. Verfahren gewechselt.
Asym. Verfahren ist rechenaufwendig, aber kann verwendet werden, ohne vorher ein gemeinsames Schlüsselwort/Geheimnis zu vereinbaren. Dies kann über die unsichere Verbindung erfolgen. Danach wird auf das performantere sym. Verfahren gewechselt.

Weitere Antworten sind möglich.

d) 3 Punkte
Die Gültigkeit des Zertifikates wurde geprüft. Server-Zertifikat lag in der übermittelten Form bei der CA vor und wurde signiert.
HINWEIS: Über die Qualität der Prüfung der Inhalte/Kontaktdaten durch die CA ist nichts ausgesagt.

4. Aufgabe (28 Punkte)

aa) 6 Punkte

Mögliche Lösungen:

Port x Link up	Bool	false/true
Port x Speed	Integer	10 Mbit/sec
Port x Full Duplex	Bool	false/true
Fan Speed	Integer	7.200 U/min
System Load	Float	10 % Last
System online	Bool	false/true
Papierfach leer (bei Drucker)	Bool	false/true
Toner leer (bei Drucker)	Bool	false/true
Standortbezeichnung	String	Netzwerkverteiler 3. OG

Weitere Lösungen sind möglich.

ab) 3 Punkte

Der abgefragte Wert stellt nur den Wert bei der Abfrage dar. Ein außergewöhnlicher Vorfall wie der Ausfall des Lüfters oder steigende Systemtemperatur wird nicht sofort bzw. erst bei der nächsten Abfrage erkannt.

ac) 3 Punkte

Auf dem zu überwachenden Gerät wird z. B. ein Monitoring-Agent (o. Ä.) installiert, der bei Überschreiten eines Schwellwertes eine Nachricht (Trap) an das Monitoringsystem sendet.

ba) 4 Punkte

Auf dem Zielsystem oder auf dem Netzwerkweg ist das Protokoll ICMP durch eine Firewall-Regel gesperrt.

Andere Lösungen sind möglich.

bb) 6 Punkte

(2) Name des antworteten DNS-Servers; hier router.local
(3) IP-Adresse des DNS-Servers; hier IPv6-Adresse fe80::1
(4) „nicht autorisierende Antwort" gibt an, dass es kein offizieller DNS-Server der abgefragten Zone bzw. ein lokaler DNS-Server ist.
(5) Name des abgefragten Servers; hier www.google.de
(6) IPv6 Adresse von www.google.de 2a00:1450:4001:815::2003
(7) IPv4 Adresse von www.google.de 216.58.208.35

ca) 3 Punkte

Da das Feld TTL beim Durchlauf bearbeitet wurde, wird eine Zeile im Trace angezeigt. Das Netzwerkgerät unterstützt keinen Trace/keine Antwort per ICMP oder gibt die Daten nicht zurück.

cb) 3 Punkte

- Der Name wurde auf eine andere IPv6-Adresse aufgelöst (Loadbalancing per DNS). Das Routing zum neuen Zielsystem führt über einen anderen Weg.
- Da das Routing im Internet dynamisch ist, kann sich die Route ändern und die Pakete einen anderen Weg zum Zielsystem nehmen.