

Serie 2017
QV nach BiVo 2006

Qualifikationsverfahren
Telematikerin EFZ
Telematiker EFZ

Berufskennnisse schriftlich
Pos. 4.2 Telematik und Netzwerktechnik

Vorlage Expertinnen und Experten

Zeit: 75 Minuten für 23 Aufgaben auf 17 Seiten

Hilfsmittel: Massstab, Geodreieck und Zeichnungsschablone.

Bewertung:

- Die maximale Punktezahl ist bei jeder Aufgabe angegeben.
- Für die volle Punktezahl werden die Formeln oder Einheitengleichungen, die eingesetzten Zahlen mit Einheiten und die zweifach unterstrichenen Ergebnisse mit den Einheiten verlangt.
- Der Lösungsweg muss ersichtlich und nachvollziehbar sein.
- Wird in einer Aufgabe eine bestimmte Anzahl Antworten verlangt, ist die vorgegebene Anzahl verbindlich. Die Antworten werden in der aufgeführten Reihenfolge bewertet, überzählige Antworten werden nicht bewertet.
- Verwenden Sie bei Platzmangel für die Lösungen die Rückseite und vermerken Sie dies bei der Aufgabe.
- **Folgefehler sind bei der Korrektur zu berücksichtigen.**

Notenskala:	Maximale Punktezahl:	71,0
	67,5 - 71,0 Punkte = Note	6,0
	60,5 - 67,0 Punkte = Note	5,5
	53,5 - 60,0 Punkte = Note	5,0
	46,5 - 53,0 Punkte = Note	4,5
	39,5 - 46,0 Punkte = Note	4,0
	32,0 - 39,0 Punkte = Note	3,5
	25,0 - 31,5 Punkte = Note	3,0
	18,0 - 24,5 Punkte = Note	2,5
	11,0 - 17,5 Punkte = Note	2,0
	4,0 - 10,5 Punkte = Note	1,5
	0,0 - 3,5 Punkte = Note	1,0

Aus didaktischen Gründen werden
die Lösungen nicht abgegeben

(Beschluss der
Aufgabenkommission
vom 09.09.2008)

Sperrfrist: Diese Prüfungsaufgaben dürfen nicht vor dem 1. September 2018 zu Übungszwecken verwendet werden.

Erarbeitet durch: Arbeitsgruppe LAP des VSEI im Beruf
Telematikerin EFZ / Telematiker EFZ.

Herausgeber: SDBB, Abteilung Qualifikationsverfahren, Bern

Aufgaben		Anzahl Punkte	
		maximal	erreicht
1.	5.3.3. B1 Erklären Sie die Funktion der englischen Abkürzung auf Deutsch.	3	
	CLIR: (Calling Line Identification Restriction) Ist ein Leistungsmerkmal bei abgehenden Anrufen, bei welchen die Übermittlung der Rufnummer zum gerufenen Teilnehmer eingeschränkt bzw. unterdrückt wird.	0,5	
	CLIRO: (Calling Line Identification Restriction Override) Ist ein Leistungsmerkmal für Blaulicht-Organisationen, wobei ein aktivierter CLIR-Dienst des Anrufenden ignoriert und seine Rufnummer immer zum Angerufenen übermittelt wird.	0,5	
	ECT: (Explicit Call Transfer) Eine aktive Verbindung wird mit einer Verbindung, welche im HOLD-Zustand ist, verbunden. Somit sind die externen Teilnehmer miteinander verbunden, jedoch via Vermittlungsstelle und somit kostenpflichtig.	0,5	
	CNIP: (Calling Name Identification Presentation) Ist ein Leistungsmerkmal bei abgehenden Anrufen, dabei wird der Name und der Ort des rufenden Teilnehmers dem gerufenen Teilnehmer übertragen.	0,5	
	CCBS: (Completion of Calls to Busy Subscriber) Rückruf bei Besetzt. Sobald der zuvor besetzte Zielteilnehmer wieder frei ist, signalisiert das Endgerät dem Anrufer, dass der Zielteilnehmer nicht mehr besetzt ist.	0,5	
	3PTY: (Three-Party Conference) Ist eine Dreierkonferenz bei welcher drei Teilnehmer gleichzeitig miteinander verbunden sind.	0,5	

Aufgaben		Anzahl Punkte									
		maximal	erreicht								
2.	5.4.1.B2 Notieren Sie je zwei Vorteile von SSD und HDD.	2									
	<table border="1"> <tr> <td colspan="2">SSD</td> </tr> <tr> <td>Vorteil 1:</td> <td>- geringe Zugriffszeiten - stossfest - lautloser Betrieb</td> </tr> <tr> <td>Vorteil 2:</td> <td>- geringes Gewicht - kompakte Masse</td> </tr> </table>	SSD		Vorteil 1:	- geringe Zugriffszeiten - stossfest - lautloser Betrieb	Vorteil 2:	- geringes Gewicht - kompakte Masse	0,5			
	SSD										
	Vorteil 1:	- geringe Zugriffszeiten - stossfest - lautloser Betrieb									
Vorteil 2:	- geringes Gewicht - kompakte Masse										
		0,5									
	<table border="1"> <tr> <td colspan="2">HDD</td> </tr> <tr> <td>Vorteil 1:</td> <td>- sehr hohe Speicherkapazität - sehr preiswert</td> </tr> <tr> <td>Vorteil 2:</td> <td>- langlebiger als SSD</td> </tr> </table>	HDD		Vorteil 1:	- sehr hohe Speicherkapazität - sehr preiswert	Vorteil 2:	- langlebiger als SSD	0,5			
HDD											
Vorteil 1:	- sehr hohe Speicherkapazität - sehr preiswert										
Vorteil 2:	- langlebiger als SSD										
		0,5									
3.	5.2.2 B2 Die derzeit beste VoIP Sprachqualität ist HD Telefonie.	2									
	a) Füllen Sie die gesuchten Werte betreffend DECT HD Telefonie ein.	1									
	<table border="1"> <thead> <tr> <th>Typ des Telefonie</th> <th>HDVoIP CODEC</th> <th>Frequenzbereich</th> </tr> </thead> <tbody> <tr> <td>Mobile VoLTE</td> <td>AMR/AMR-WB</td> <td>50-7000 Hz</td> </tr> <tr> <td>DECT HD</td> <td>G.722</td> <td>50-7000Hz</td> </tr> </tbody> </table>	Typ des Telefonie	HDVoIP CODEC	Frequenzbereich	Mobile VoLTE	AMR/AMR-WB	50-7000 Hz	DECT HD	G.722	50-7000Hz	
Typ des Telefonie	HDVoIP CODEC	Frequenzbereich									
Mobile VoLTE	AMR/AMR-WB	50-7000 Hz									
DECT HD	G.722	50-7000Hz									
b) Welche Brutto-Bitrate wird benötigt, um einen Primäranschluss (30-Kanäle) mit einer VoIP DECT HD Technologie zu ersetzen, so dass alle Kanäle gleichzeitig benutzt werden können? Brutto-Bitrate = 30 x 80-100 kbit/s = Min. 2400 kbit/s. Max: 3 Mbit/s	1										

Aufgaben			Anzahl Punkte			
			maximal	erreicht		
4.	5.2.1 B2 Lesen Sie die folgenden Aussagen in Bezug auf drahtlose Technologie. Kreuzen Sie richtig oder falsch an.			2		
	richtig	falsch				
	X		RFID ist eine Technik zur Identifikation von Gegenständen über Funk und kann über mehrere Meter hinweg kommunizieren.			0,5
	X		NFC ist eine drahtlose Übertragungstechnik, die zum kontaktlosen Datenaustausch zwischen Geräten mit einer Distanz von bis zu 4 Zentimeter dient.			0,5
	X		Ab Bluetooth Version 4.0 und höher handelt es sich um eine besonders stromsparende Version von Bluetooth.			0,5
	X	In einem Hotel muss man einen WLAN Controller einsetzen, da nur dieser das Ticketing System verwalten kann.	0,5			
5.	5.3.3 B2 Die meisten Telefonanlagen haben auf der ISDN Karte ein integriertes Modem für die Fernwartung. Wird im Rahmen der All-IP Migration auf einen SIP Trunk migriert, geht die Funktion des Fernwartungsmodems verloren.			2		
	a) Notieren Sie zwei Möglichkeiten, einen Fernwartungszugang über ein IP Netzwerk zu realisieren.					
	Möglichkeit 1:	Remote Zugang mit Site-to-Site VPN				0,5
	Möglichkeit 2:	Reverse Proxy mit Raspberry Pi, Call to Service Portal				0,5
	b) Welche Konfigurationen werden an die Firewall und den Internetanschluss gestellt, um per Fernwartung von extern zugreifen zu können. Notieren Sie zwei Konfigurationen.					
Konfiguration 1:	Fixe IP Adresse auf dem Internet Anschluss		0,5			
Konfiguration 2:	VPN Lizenzen auf der Firewall		0,5			
Hinweis für Experten: Andere Lösungen sind möglich						

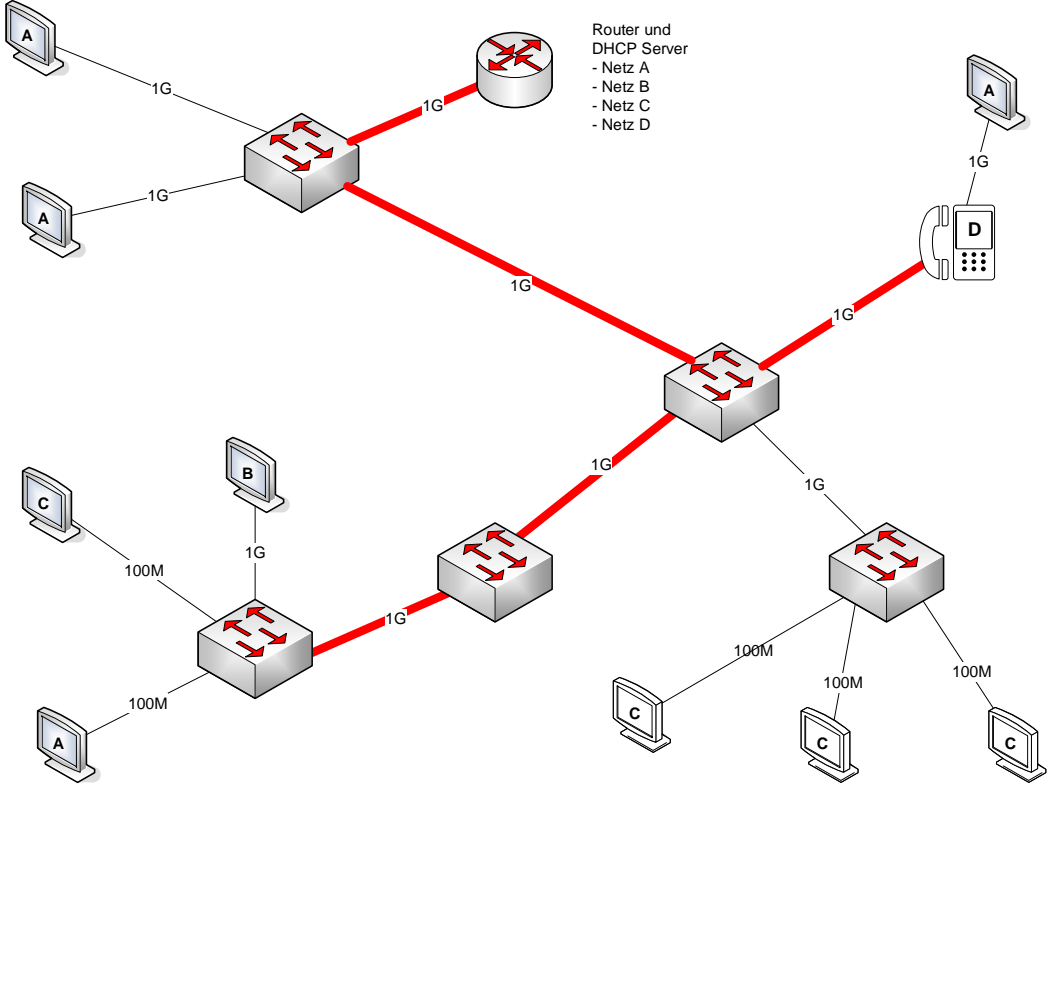
Aufgaben			Anzahl Punkte			
			maximal	erreicht		
8.	5.4.2 B1 Welche Bedienungen muss eine Software erfüllen, damit diese als Open-Source-Lizenz von der Open-Source-Initiative anerkannt wird? Kreuzen Sie erfüllt oder nicht erfüllt an.		3			
	erfüllt	nicht erfüllt			Aussagen	
		X			Die Software ist auf eine bestimmte Hardware ID lizenziert und darf nur auf dieser betrieben werden.	0,5
	X				Die Software liegt in einer für den Menschen lesbaren und verständlichen Form vor.	0,5
		X			Die Software unterliegt einer jährlichen Lizenzgebühr.	0,5
		X			Die Software unterliegt Eigentumsrechten, Patentrechten, Urheberrechten des Herstellers.	0,5
	X				Die Software darf verändert und in der veränderten Form weitergegeben werden.	0,5
		X			Es handelt sich dabei um eine zeitlich limitierte Lizenz.	0,5
9.	5.5.3 B2 Erklären Sie den Zweck folgender Elemente einer Telefonanlage:		3			
	a) Bündel: Fasst die Kanäle eines Amtsanschlusses oder einer Querverbindung zusammen und definiert die Einstellungen für alle Kanäle in der Gruppierung.				1	
	b) Leitweg: Definiert über welchen Weg ein Anruf gelenkt werden soll, um ein Ziel zu erreichen, welches nicht lokal auf der Telefonanlage erreichbar ist.				1	
	c) SIP Trunk: Voice over IP Telefonanschluss zum Anschluss einer Telefonanlage an einen Amtsanschluss oder an ein Fremdsystem.				1	

Aufgaben		Anzahl Punkte	
		maximal	erreicht
10.	5.1.2 B1 In einer Firewall kommen mehrere Filterarten zum Einsatz. Beschreiben Sie die Arbeitsweise und die Eigenschaften der nachfolgenden Filterarten:	2	
	a) Paketfilter: Die einfache Filterung von Datenpaketen anhand der Netzwerkadressen. Das Paketfilter ist für Aufgaben, wie das Vergleichen von Quell- oder Zieladresse der Pakete, die die Firewall passieren, verantwortlich.	0,5	
	b) Stateful Inspection: Diese zustandsgesteuerte Filterung ist eine erweiterte Form der Paketfilterung. Damit gelingt es, den Zugriff auf eine etablierte Verbindung genauer zu beschränken.	0,5	
	c) Deep Packet Inspection: Dabei werden gleichzeitig der Datenteil und der Headerteil des Datenpaketes auf bestimmte Merkmale wie Protokollverletzungen, Computerviren, Spam und weitere unerwünschte Inhalte untersucht.	0,5	
	d) Proxyfilter: Ein Proxyfilter stellt stellvertretend für den anfragenden Client die Verbindung mit dem Zielsystem her und leitet die Antwort des Zielsystems an den tatsächlichen Client weiter.	0,5	
11.	5.4.3 B2 In modernen Netzwerken werden immer häufiger IP-Kameras eingesetzt.	3	
	a) Erklären Sie mit welchem Protokoll der Video Stream einer Kamera auf mehreren Bildschirmen angezeigt werden kann? IP-Multicast ermöglicht in einem IP-Netzwerk Pakete von einer einzigen Quelle an eine Gruppe von Empfängern zu senden.	1	
	b) Welches Protokoll wird für das Management dieser Übertragungsart benutzt? Internet Group Management Protocol (IGMP) dient zur Organisation von Multicast Gruppen.	1	
	c) Welcher spezielle Adressbereich ist in IPv4 für diese Übertragungsart reserviert? In IPv4 ist hierfür der Adress-Bereich 224.0.0.0 bis 239.255.255.255 reserviert.	1	

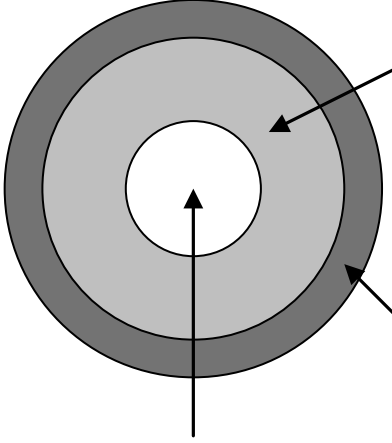
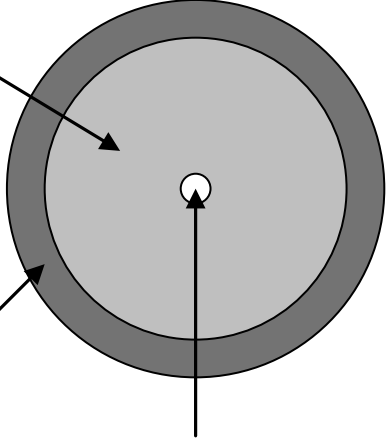
Aufgaben		Anzahl Punkte	
		maximal	erreicht
12.	5.4.1 B2 Handelsübliche Computer haben zum Teil zwei Festplatten eingebaut. Diese können die Daten mit „RAID 0“ oder „RAID 1“ sichern.	4	
	a) Erklären Sie die Funktionsweise von „RAID 0“ und „RAID 1“ und notieren Sie den jeweiligen Hauptvorteil. RAID 0: Speichert die eine Hälfte der Daten auf Festplatte 1 die andere Hälfte auf Festplatte 2. Damit wird die <u>Zugriffszeit</u> halbiert, die volle Festplattenkapazität ausgenutzt, jedoch keine zusätzliche Datensicherheit geschaffen. RAID 1: Speichert sämtliche Daten auf Festplatte 1 und kopiert diese anschliessend auf Festplatte 2. Damit wird die Zugriffszeit nicht verkleinert, dafür aber die <u>Datensicherheit</u>. Bei zwei gleich grossen Festplatten wird die nutzbare Kapazität halbiert, bei unterschiedlich grossen Festplatten kann nur die Kapazität der kleineren Festplatte genutzt werden.	1	
	b) In Servern wird zur Speicherung der Daten oft RAID 5 verwendet. Wie ist dessen Funktionsweise und was ist die minimale Anzahl Festplatten für RAID 5? RAID 5 benötigt mindestens drei Festplatten. Diese werden als ein Laufwerk zusammengefasst. Die Daten werden ähnlich wie bei einem RAID 0 auf die angeschlossenen Festplatten verteilt. Neben den geschriebenen Daten werden auch Parity-Daten erstellt, die zur Wiederherstellung genutzt werden können, falls eine Festplatte ausfällt. Dazu braucht es einen Controller welcher relativ teuer ist. RAID 5 kann auch mit mehr als <u>drei Festplatten</u> aufgebaut werden, je mehr Festplatten eingebaut werden, desto höher ist die Performance.	2	






Aufgaben		Anzahl Punkte	
		maximal	erreicht
13.	5.4.5 B3 Einer Ihrer Kunden will die Speicherung der Daten neu organisieren. Dabei möchte er seine Daten in einem modernen Serverraum speichern und das Backup in einem externen Rechencenter auslagern.	3	
	a) Erklären Sie dem Kunden, auf welche physikalischen Sicherheitseinrichtungen er beim Bau des Serverraumes achten muss. Notieren Sie vier Punkte. <ul style="list-style-type: none"> - Zutrittskontrolle, um Zutritt von Unbefugten zu verhindern - Schutz gegen Feuer (Brandmeldeanlage oder Brandlöschanlage) - Schutz gegen Wasser oder mind. Erkennung von Wasser - Notstromversorgung - Kühlanlage zum Schutz vor Überhitzung - Videoüberwachung, Schutz gegen Einbruch <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Experten Hinweis: Pro korrekte Antwort 0,5 Punkte. Andere Lösungen sind möglich.</p> </div>	2	
	b) Was muss der Kunde betreffend Datenübertragung zwischen Serverraum und externem Rechencenter beachten? Notieren Sie zwei wesentliche Punkte. <ul style="list-style-type: none"> - Genügend Bandbreite - Verschlüsselung 	1	
14.	5.4.5 B3 Sie beraten einen Kunden bezüglich Datensicherheit in dessen Unternehmen. Der Kunde verfügt im gesicherten Bereich über ein Netzwerk in dem Computer, Drucker, Telefone eingebunden sind. Im zugänglichen Bereich, sind IP-Kameras eingebunden.	4	
	a) Welche Anforderungen an die Sicherheit bezüglich Konfiguration und Leistungsmerkmale der Switches sind zu beachten? Notieren Sie zwei Anforderungen. <ul style="list-style-type: none"> - Switches zur Erstellung unterschiedlicher VLAN's - Keine Standard Passworte verwenden - Alle Geräte in zugänglichen Netzen sollen keine Antwort auf Ping - Anfragen geben - Konfiguration bei den IP Kameras darf nur von einer vergebenen IP-Adresse aus möglich sein. 	2	
	b) Die Switches befinden sich alle in einem separaten, jedoch nicht abschliessbaren Raum. Was stellen Sie an den Switches ein, damit eine Manipulation an einem Port keine Wirkung auf den Betrieb hat. Begründen Sie! <p>802.1x-User-Zuordnung: Der Benutzer muss sich am Netzwerk anmelden. Abhängig von seinem Benutzerprofil wird der Switch konfiguriert und der Switchport, an dem er soeben angeschlossen ist, wird für das jeweilige VLAN konfiguriert.</p>	2	

Aufgaben		Anzahl Punkte																																									
		maximal	erreicht																																								
15.	<p>5.5.4 B2</p> <p>Beantworten Sie die Fragen auf der Grundlage der folgenden Informationen:</p> <p>NAT/PAT:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th colspan="3">NAT/PAT</th> </tr> <tr> <th colspan="2">LAN</th> <th>WAN</th> </tr> <tr> <th>IP</th> <th>Port</th> <th>Port</th> </tr> </thead> <tbody> <tr> <td>192.168.55.28</td> <td>5555</td> <td>5060</td> </tr> <tr> <td>10.10.10.10</td> <td>80</td> <td>12345</td> </tr> <tr> <td>192.168.2.6</td> <td>80</td> <td>80</td> </tr> <tr> <td>172.31.23.12</td> <td>12345</td> <td>55555</td> </tr> <tr> <td>192.168.55.23</td> <td>12345</td> <td>43892</td> </tr> </tbody> </table> <p>Port Analyse eines ankommenden Paketes WAN-Seite.</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th colspan="4">WAN Sockets</th> </tr> <tr> <th colspan="2">Source Socket</th> <th colspan="2">Destination Socket</th> </tr> <tr> <th>IP Source</th> <th>Port Source</th> <th>IP Destination</th> <th>Port Destination</th> </tr> </thead> <tbody> <tr> <td>73.35.67.89</td> <td>5555</td> <td>123.45.66.77</td> <td>12345</td> </tr> </tbody> </table> <p>a) Wie lautet die Destination Socket: 10.10.10.10 :80</p> <p>b) Welches ist die Adresse des Routers auf der WAN Seite? Öffentliche IP: 123.45.66.77</p>	NAT/PAT			LAN		WAN	IP	Port	Port	192.168.55.28	5555	5060	10.10.10.10	80	12345	192.168.2.6	80	80	172.31.23.12	12345	55555	192.168.55.23	12345	43892	WAN Sockets				Source Socket		Destination Socket		IP Source	Port Source	IP Destination	Port Destination	73.35.67.89	5555	123.45.66.77	12345	<p>2</p>	
	NAT/PAT																																										
LAN		WAN																																									
IP	Port	Port																																									
192.168.55.28	5555	5060																																									
10.10.10.10	80	12345																																									
192.168.2.6	80	80																																									
172.31.23.12	12345	55555																																									
192.168.55.23	12345	43892																																									
WAN Sockets																																											
Source Socket		Destination Socket																																									
IP Source	Port Source	IP Destination	Port Destination																																								
73.35.67.89	5555	123.45.66.77	12345																																								
16.	<p>5.5.4 B2</p> <p>Es stehen verschiedene Arten von Cloud Lösungen zur Verfügung. Erklären Sie die Eigenschaften der folgenden Cloud Bereitstellungsmodelle.</p> <p>a) Public Cloud:</p> <p>Eine Public Cloud ist generell jedem zugänglich, d.h. jede Firma oder Privatperson kann (virtualisierte) IT-Ressourcen in der Public Cloud reservieren und nutzen. Da die Nutzergruppe nicht beschränkt ist, können Skaleneffekte besonders gut ausgenutzt werden, wodurch Public-Cloud-Dienste im Vergleich zu den anderen Cloud-Typen oft besonders günstig sind.</p> <p>b) Private Cloud:</p> <p>Eine Private Cloud wird dediziert für eine bestimmte Firma betrieben, ist also fest einer Firma zugeordnet. Diese kann im unternehmenseigenen Rechenzentrum oder durch einen Cloud Dienstleister bereitgestellt werden.</p>	<p>2</p> <p>1</p> <p>1</p>																																									

Aufgaben		Anzahl Punkte	
		maximal	erreicht
17.	<p>5.5.6 B2</p> <p>Sie stellen fest, dass bei Ihrem Kunden eine feste IP-Konfiguration auf vier verschiedenen Netzwerken (A, B, C und D), die sich dieselbe Netzwerk-Infrastruktur teilen, installiert wurde.</p> <p>Um die Sicherheit zu verbessern und um die IP Adressen per DHCP zu verteilen, setzen Sie die VLAN Technologie ein.</p> <p>Markieren Sie die Stränge, die zwingend mit 802.1PQ Standard "getaggt" sein müssen, so dass der Router alle Geräte in verschiedenen VLANs erreichen kann. Es sind möglichst wenige administrierbare Switches einzusetzen.</p>	2	
 <p style="text-align: center;">Router und DHCP Server - Netz A - Netz B - Netz C - Netz D</p> <div style="border: 1px solid black; padding: 10px; margin-top: 20px; text-align: center;"> <p>Experten Hinweis: Strecke Telefon zu PC -1 Punkt; Switch zu PC's C -1Punkt; Switch zu Switch -1 Punkt.</p> </div>			

Aufgaben		Anzahl Punkte	
		maximal	erreicht
18.	5.4.4 B2 Beschreiben Sie den Verwendungszweck folgender Protokollvarianten zum Übertragen von E-Mail Nachrichten.	4	
	a) Post Office Protocol (POP): Dieses Protokoll dient zum Abrufen der Emails durch einen E-Mail Client von einem E-Mail Server. Die E-Mails werden vom SMTP Server abgeholt und auf dem Client System gespeichert.	1	
	b) Internet Message Access Protocol (IMAP): Dieses Protokoll ist eine Weiterentwicklung des POP Protokolls. Bei diesem Protokoll werden die E-Mails auf dem Server belassen und der Client greift online darauf zu.	1	
	c) Simple Mail Transfer Protocol (SMTP): Dieses Protokoll dient zum Versenden von E-Mails zwischen Client und Server, sowie zwischen den E-Mail Servern. <div style="border: 1px solid black; padding: 5px;">Experten Hinweis: Client und Server gibt die volle Punktzahl oder nur E-Mail Server ergibt die volle Punktzahl.</div>	1	
d) Welche der oben genannten Protokolle übertragen E-Mails in unverschlüsselter Form: POP, SMTP, IMAP	1		

Aufgaben		Anzahl Punkte	
		maximal	erreicht
5.5.1 B1			
19.	<p>Beschriften Sie die Schichten der unten dargestellten Glasfaserkabel mit den dazugehörigen Durchmessern und ergänzen Sie die fehlenden Angaben.</p> <div style="display: flex; justify-content: space-around; align-items: flex-start;"> <div style="text-align: center;"> <p>Fasertyp: Multimodefaser</p>  <p>Kernglas 50 μm oder 62.5 μm</p> <p>Lichtquelle: Diode</p> <p>Typische Wellenlängen: 850 nm und 1300 nm</p> </div> <div style="text-align: center;"> <p>Fasertyp: Singlemodefaser</p>  <p>Kernglas 9 μm</p> <p>Lichtquelle: Laser</p> <p>Typische Wellenlängen: 1310 nm und 1550 nm</p> </div> </div>	5	

Aufgaben		Anzahl Punkte			
		maximal	erreicht		
20.	5.4.3 B1			5	
	a) Notieren Sie die Bezeichnung der Schnittstellen und kreuzen Sie jeweils die zutreffende Eigenschaft an.				
		3,5 mm Klinke	<input checked="" type="checkbox"/> Mono <input type="checkbox"/> Mono / Stereo <input type="checkbox"/> Stereo	1	
		USB 3.0	Bruttodatenrate: <input type="checkbox"/> 12 Mbit/s <input type="checkbox"/> 480 Mbit/s <input checked="" type="checkbox"/> 4000 Mbit/s <input type="checkbox"/> 6000 Mbit/s	1	
	b) Notieren Sie die Bezeichnung der Schnittstellen und geben Sie je eine Anwendung an.				
		LC-Duplex	Patchkabel	1	
		RJ11	Hörer / Mikrotelkabel	1	
		Firewire 400	Externe Festplatte Kamera	1	

Aufgaben		Anzahl Punkte	
		maximal	erreicht
21.	5.5.4 B2 Notieren und erklären Sie drei verschiedene Technologien, um den unbeaufsichtigten Fernwartungszugriff via Internet auf ein Kundensystem im Netzwerk zu gewährleisten.	3	
	<p>a) Fernwartungs-Software</p> <p>(Broker Service wie Teamviewer, Netviewer, LogMeln) Auf einem Rechner im Netzwerk des Kunden, welcher immer online ist und Zugriff auf die Maschine hat, wird eine Fernwartungssoftware installiert. Die Fernwartungssoftware öffnet von innen durch die Firewall eine Verbindung zu einem Broker-Service. Der Hersteller baut die Verbindung via Brokerservice auf. An der Firewall sind keine Einstellungen notwendig da abgehende Verbindungen standardmässig erlaubt sind.</p>	1	
	<p>b) VPN</p> <p>Auf der Firewall des Kunden wird für die Herstellerfirma ein Benutzerkonto eingerichtet. Dieses wird für den Zugriff aus dem Internet auf die interne Netzwerkadresse der Maschine berechtigt.</p>	1	
	<p>c) NAT Firewall-Regel</p> <p>Auf der Firewall des Kunden wird ein TCP-Port der externen IP-Adresse auf einen TCP-Port der internen Adresse der Maschine weitergeleitet. Der Hersteller kann so direkt auf die Maschine des Kunden zugreifen. Der Zugriff muss durch den Hersteller abgesichert werden.</p>	1	
<div style="border: 1px solid black; padding: 5px; margin-top: 20px;"> Experten Hinweis: pro Nennung 0,5 Punkte und pro Erklärung 0,5 Punkte </div>			

Aufgaben		Anzahl Punkte	
		maximal	erreicht
22.	<p>5.5.4 B3</p> <p>Ihr Kunde erweitert seine Netzwerkinfrastruktur aufgrund einer Fusion von zwei Firmen. Heute besteht eine Gigabit-Netzwerkverkabelung und ein C-Klasse IP-Adressierungskonzept für 200 Arbeitsplätze. 50 weitere Adressen sind für Server, Drucker und Netzwerkgeräte reserviert. Die heutige Netzwerkadresse lautet: 10.20.0.0 mit Subnetzmaske 255.255.255.0. Neu werden 150 Arbeitsplätze sowie 50 Drucker und Netzwerkgeräte hinzukommen, jedoch keine weiteren Server. Beantworten Sie folgende Fragen zu dieser Erweiterung:</p> <p>a) Der Kunde möchte das IP-Adressierungskonzept für seine Server aufgrund der Erweiterung nicht ändern. Welche zwei Möglichkeiten haben Sie, um dieses Ziel zu erreichen. Beschreiben Sie zwei Varianten, damit trotzdem alle Arbeitsstationen und Netzwerkgeräte auf die Server zugreifen können?</p> <p>Variante 1:</p> <p>Vergrossern der Anzahl adressierbarer Hosts im Netzwerk durch Anpassung der Subnetzmaske: Ist: $/24 = 255.255.255.0 = 254$ adressierbare Hosts (10.20.0.1 – 10.20.0.254)</p> <p>Soll (Beispiel): $/22 = 255.255.252.0 = 1022$ adressierbare Hosts (10.20.0.1 – 10.20.3.254)</p> <p>Die IP Adressen der Server bleiben gleich, die Subnetzmaske muss aber angepasst werden. Es braucht keine zusätzlichen Router.</p> <p>Variante 2:</p> <p>Erstellen eines oder mehrerer zusätzlichen IP-Subnetze wie z.B. 10.20.1.0/24 mit zusätzlichen 254 adressierbaren Hosts und 10.20.2.0/24 mit zusätzlichen 254 adressierbaren Hosts</p> <p>Die IP Adressen der Server bleiben gleich, die Subnetzmaske muss nicht angepasst werden. Allerdings muss für den Zugriff zwischen den Subnetzen ein Router eingesetzt werden, damit Hosts in einem anderen Subnetz erreicht werden können.</p> <p>b) Kann der Kunde die UKV-Anschlüsse ohne Einschränkungen mit Splittern verdoppeln, damit er für die neuen Arbeitsplätze keine neuen Kabel installieren lassen muss? Begründen Sie Ihre Antwort.</p> <p>Nein.</p> <p>Will der Kunde weiterhin Gigabit-Verbindungen zu den Arbeitsplätzen haben, können die Anschlüsse nicht gesplittet werden. FastEthernet 100Mbit/s braucht 2 Paare GigabitEthernet 1000 Mbit/s braucht 4 Paare</p>	5	
		2	
		2	
		1	

Aufgaben		Anzahl Punkte			
		maximal	erreicht		
23.	5.5.2 B2		4		
	<p>a) Dieses Gebiet ist mit unterschiedlichen Verbindungsarten vernetzt. Die Leitungen sollen Daten sowie Telefonie übertragen. In der Kassenstation Nord befindet sich die TVA, welche das ganze Gebiet mittels VoIP-Telefonie versorgt. Auf dem benachbarten Berg befindet sich ein Restaurant. Im Zuge der Renovierung der Tourismusgenossenschaft soll auch die Kommunikation zur Kassenstation Süd verbessert werden, denn der Kunde beklagt sich über Instabilität bei der Amtsanbindung. Was wäre eine mögliche Ursache und mit welchen Massnahmen könnte man die Situation verbessern?</p>				
	<p>Ursache: Die Richtstrahlverbindung ist stark von der Witterung abhängig. Ebenfalls ist der Quality of Service mit einer Richtstrahlantenne nicht gewährleistet und somit ist die Amtsanbindung nicht konstant.</p>				1
	<p>Verbesserung: Mietleitung, als Ersatz respektive Redundanz zum bestehenden Richtstrahl. Experten Hinweis: Ein gerichtetes WLAN ist auch möglich, man wäre aber immer noch abhängig von der Witterung und wäre somit nicht richtig.</p>				1
	<p>b) Das renovierte Restaurant soll nun auch an die TVA in der Kassenstation Nord angebunden werden. Es ist eine bestehende Kupferleitung zwischen Kassenstation Nord und Restaurant vorhanden. Nun ist zu überprüfen, ob diese Verbindung durch eine LWL Verbindung ersetzt werden soll. Notieren Sie zwei Argumente, welche für den Austausch des Kupfers sprechen.</p>				
<p>Argument 1:</p> <ul style="list-style-type: none"> - Galvanische Trennung - LWL ist unempfindlicher gegenüber Atmosphärischen Störungen (Blitz) 	1				
<p>Argument 2:</p> <ul style="list-style-type: none"> - Grösse Distanz - Hohe Übertragungsrate - Saubere IP Verbindung - Skalierbar für die Zukunft 	1				
Total		71			