Diese Kopfleiste bitte unbedingt ausfüllen!

Familienname, Vorname (bitte durch eine Leerspalte trennen, ä = ae etc.)

Fach	Berufsnummer				Prüflingsnummer								
5	5	1	1	9	7								
Sp. 1-2		Sp. 3-6				Sp. 7-14							

IHK

Termin: Dienstag, 23. November 2004

Abschlussprüfung Winter 2004/05

Fachinformatiker/Fachinformatikerin Systemintegration 1197

1 Ganzheitliche Aufgabe I
Fachqualifikationen

6 Handlungsschritte
Mit Anlage
90 Minuten Prüfungszeit
100 Punkte

Zugelassene Hilfsmittel:
- Netzunabhängiger, geräuscharmer Taschenrechner
- Ein IT-Handbuch/Tabellenbuch/Formelsammlung

Bearbeitungshinweise

1. Der vorliegende Aufgabensatz besteht aus insgesamt 6 Handlungsschritten zu je 20 Punkten.

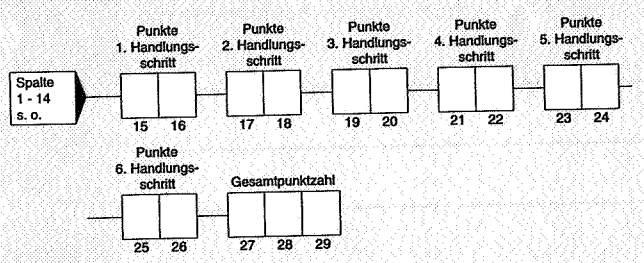
   In der Prüfung zu bearbeiten sind 5 Handlungsschritte, die vom Prüfungsteilnehmer frei gewählt werden können.

   Der nicht bearbeitete Handlungsschritt ist durch Streichung des Aufgabentextes im Aufgabensatz und unten mit dem Vermerk „Nicht bearbeiteter Handlungsschritt: Nr. ... „ an Stelle einer Lösungsniederschrift deutlich zu kennzeichnen. Erfolgt eine solche Kennzeichnung nicht oder nicht eindeutig, gilt der 6. Handlungsschritt als nicht bearbeitet.
2. Füllen Sie zuerst die **Kopfzeile** aus. Tragen Sie Ihren Familiennamen, Ihren Vornamen und Ihre Prüflings-Nr. in die oben stehenden Felder ein.
3. Lesen Sie bitte den **Text** der Aufgaben ganz durch, bevor Sie mit der Bearbeitung beginnen.
4. Halten Sie sich bei der Bearbeitung der Aufgaben genau an die **Vorgaben der Aufgabenstellung** zum Umfang der Lösung. Wenn z. B. vier Angaben gefordert werden und Sie sechs Angaben anführen, werden nur die ersten vier Angaben bewertet.
5. Tragen Sie die frei zu formulierenden **Antworten dieser offenen Aufgabenstellungen** in die dafür lt. Aufgabenstellung vorgesehenen Bereiche (Lösungszeilen, Formulare, Tabellen u. a.) des Arbeitsbogens ein.
6. Sofern nicht ausdrücklich ein Brief oder eine Formulierung in ganzen Sätzen gefordert werden, ist eine **stichwortartige Beantwortung** zulässig.
7. Schreiben Sie deutlich und gut lesbar. Ein nicht eindeutig zuzuordnendes oder **unleserliches Ergebnis** wird als **falsch** gewertet.
8. Ein netzunabhängiger geräuscharmer Taschenrechner ist als Hilfsmittel zugelassen.
9. Wenn Sie ein **gerundetes Ergebnis** eintragen und damit weiterrechnen müssen, rechnen Sie (auch im Taschenrechner) nur mit diesem gerundeten Ergebnis weiter.
10. Für **Nebenrechnungen/Hilfsaufzeichnungen** können Sie das im Aufgabensatz enthaltene Konzeptpapier verwenden. Dieses muss vor Bearbeitung der Aufgaben herausgetrennt werden. Bewertet werden jedoch nur Ihre Eintragungen im Aufgabensatz.

Nicht bearbeiteter Handlungsschritt ist Nr.

Wird vom Korrektor ausgefüllt!

Bewertung
Für die Bewertung gilt die Vorgabe der Punkte in den Lösungshinweisen. Für den abgewählten Handlungsschritt ist anstatt der Punktzahl die Buchstabenkombination „AA" in die Kästchen einzutragen.



Prüfungsort, Datum

Unterschrift

2. Handlungsschritt (20 Punkte)

Korrekturrand

In der ArBuSt AG soll der Internetzugang für das lokale Firmennetzwerk (LAN) in Zukunft durch eine Firewall abgesichert werden.

Zusätzlich soll das Firmennetzwerk um eine DMZ erweitert werden. Darin sollen auf einer Server-Plattform sowohl www- als auch ftp-Dienste für das öffentliche Netz zur Verfügung gestellt werden.

Im Internet steht der ArBuSt AG bereits ein externer E-Mail-Server bei einem Internet-Service-Provider (ISP) zur Verfügung. Darauf sind E-Mail-Konten für alle im Firmen-LAN zugangsberechtigten Mitarbeiter eingerichtet.

Das geplante Netzwerkkonzept ist aus Abbildung „ArBuSt-Net-Neu" ersichtlich.

Als Firewall-Lösung soll eine Paketfilter-Firewall zum Einsatz kommen.

Als Filter-Strategie gilt der Grundsatz: Nur explizit ausgewählte Pakete dürfen passieren, alles andere wird abgewiesen.

Ihre Aufgabe ist es, für die Paketfilter-Firewall ein Filterkonzept zu entwickeln. Hierzu sind im Vorfeld einige Überlegungen anzustellen.

a) Erläutern Sie kurz, warum sich TCP-Pakete präziser filtern lassen als UDP-Pakete. (5 Punkte)

b) Für die Mitarbeiter der ArBuSt AG sollen folgende Zugriffe in das Internet ermöglicht werden:

Korrekturrand

- Aufrufen von Webseiten (http)
- Downloads von Daten
- Senden von E-Mails
- Abrufen von E-Mails
- Domain-Name-Service

Wählen Sie aus der folgenden Zuordnungstabelle die hierfür erforderlichen Dienste und Ports aus und tragen Sie diese in die unten stehende Tabelle ein.

(5 Punkte)

Zuordnungstabelle zwischen Dienst-Namen und -Ports

Dienst	**Portnummer**
FTP Data Channel	20
FTP Control Channel	21
TELNET	23
SMTP	25
WHOIS	43
DNS	53
TFTP	69
Gopher	70
WWW	80
POP3	110
NNTP	119
NTP	123
SNMP	161

Zugriff	**Dienst**	**Portnummer**
Aufrufen von Webseiten		
Downloads von Daten		
Senden von E-Mails		
Abrufen von E-Mails		
Domain-Name-Service		

Fortsetzung 2. Handlungsschritt →

Fortsetzung 2. Handlungsschritt

Korrekturrand

c) Bei einer Internetrecherche haben Sie für eine Paketfilter-Firewall folgendes Regelset für eine Filtertabelle entdeckt:

Interface: bad								
Regel	**Richtung**	**Quell-IP**	**Ziel-IP**	**Protokoll**	**Quell-Port**	**Ziel-Port**	**Ack-Flag**	**Aktion**
1	rein	egal	DMZ-www	TCP	> 1023	80	egal	weiterleiten
2	raus	DMZ-www	egal	TCP	80	> 1023	ja	weiterleiten
3	egal	jede	jede	jedes	jeder	jeder	egal	blockieren

Hier ist beispielhaft ein Regelset für eine äußere Netzwerkkarte dargestellt.
Damit wird der Zugriff aus dem Internet auf einen www-Server in einer DMZ erlaubt.

Entwickeln Sie analog dazu ein Regelset, das die Kommunikation der LAN-Clients mit dem externen Mail-Server über eine TCP-Verbindung ermöglicht.

Das Regelset soll folgende Funktionen enthalten:
- Senden von E-Mails
- Abrufen von E-Mails
- alles Andere blockieren

Hinweis: In den Feldern Quell- und Ziel-IP tragen Sie die vereinfachte Form „Mail-Server" und „LAN" anstelle der exakten IP-Adressen ein.

(10 Punkte)

Interface: ETH0								
Regel	**Richtung**	**Quell-IP**	**Ziel-IP**	**Protokoll**	**Quell-Port**	**Ziel-Port**	**Ack-Flag**	**Aktion**

3. Handlungsschritt (20 Punkte)

Korrekturrand

Zur Fehleranalyse und zum Monitoring führen Sie in regelmäßigen Abständen eine Protokollanalyse in verschiedenen Segmenten des Netzwerkes der ArBuSt AG durch. Dabei haben Sie den Protokollauszug „Management-Access" aufgezeichnet.

a) Strukturieren Sie die Zusammenfassung in funktional aufeinander folgende Phasen; berücksichtigen Sie, dass der aufgelöste Frame 18 der erste Frame mit Anwendungsdaten ist. (8 Punkte)

b) Erklären Sie die Bedeutung der Angabe Win=1024 in einem TCP-Segment. (4 Punkte)

Fortsetzung 3. Handlungsschritt →

Fortsetzung 3. Handlungsschritt

Korrekturrand

c) Geben Sie die MAC-Adresse an, die zur IP 172.18.2.115 gehört. (2 Punkte)

d) Interpretieren Sie die Angaben Dst Port: 1033, Len: 9 und Flags: 0x0018 (PSH, ACK) im Zusammenhang mit den Angaben des Frame 18. (6 Punkte)

4. Handlungsschritt (20 Punkte)

Korrekturrand

In der DMZ der ArBuSt AG soll ein www- und ftp-Server für Kundenanfragen aus dem Internet eingerichtet werden.

Sie sollen für den Server ein Konzept erstellen. Hierzu sind im Vorfeld einige Fragen zu klären.

a) Der Server soll hochverfügbar sein. Deswegen soll ein SCSI-Hardware-RAID-System zum Einsatz kommen. Im BIOS des RAID-Controllers können die Level 0, 1 und 5 konfiguriert werden.

aa) Wählen Sie die beiden geeigneten Level für den o. g. Server aus. (2 Punkte)

ab) Erläutern Sie die jeweilige Funktion der beiden geeigneten Level und beschreiben Sie deren Vor- und Nachteile. (6 Punkte)

Fortsetzung 4. Handlungsschritt →

b) Das Konzept soll die verschiedenen Konfigurationen für den www-Dienst (Server) bereits weitgehend vorgeben. Folgende Konfigurationsmöglichkeiten sind hier im Vorfeld noch zu klären.

Korrekturrand

ba) Neben dem Standard-TCP-Port 80 steht auch noch der TCP-Port 443 (SSL) zur Verfügung. Erklären Sie, wofür der Port 443 vorgesehen ist. (3 Punkte)

bb) Erklären Sie, wozu die Zeitangabe bei der Funktion „Verbindungstimeout" dient. (3 Punkte)

bc) Beschreiben Sie, was man erreicht, wenn die Funktion „HTTP-Keep-Alive" aktiviert wird. (3 Punkte)

bd) Laut Handbuch kann bei stark frequentierten Webseiten die Anzahl der Verbindungen begrenzt werden. Nennen Sie jeweils einen Vor- und Nachteil dieser Option. (3 Punkte)

6. Handlungsschritt (20 Punkte)

Korrekturrand

Das Netzwerk der ArBuSt AG soll vor Malware und Spam Mails geschützt werden.
Sie sollen das Schutzkonzept entwerfen.

a) Nennen Sie zwei typische Angriffsprogramme und beschreiben Sie deren jeweilige Vorgehensweise. (4 Punkte)

b) Erläutern Sie drei Maßnahmen, mit denen die Gefahr einer Infektion reduziert werden kann. (6 Punkte)

Abschlussprüfung Winter 2004/05

IHK

Fachinformatiker/Fachinformatikerin
Systemintegration
1197

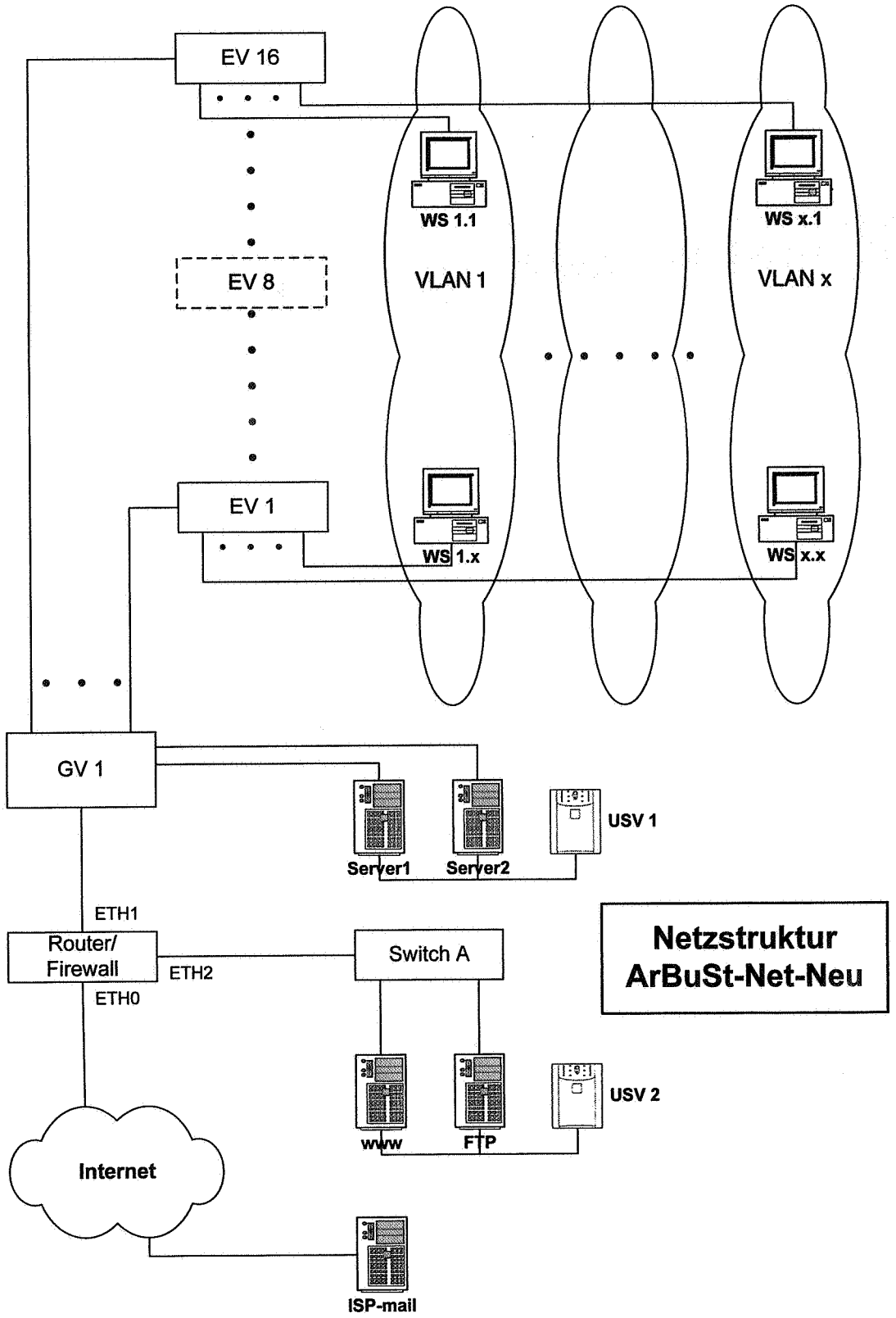
1 Ganzheitliche Aufgabe I
Fachqualifikationen

Anlagen

Zum 1. und zum 3. Handlungsschritt

Anlage zum 1. Handlungsschritt

Anlage: ArBuSt-Net-Neu



Anlage zum 1. Handlungsschritt

Anlage: Koppelelemente

Koppelelement A

High-Density, Stackable 10/100 Switching

Deploy high-performance, feature-rich Ethernet LAN switching with high port density. This affordable, intelligent 10/100 switch is fully manageable, making it a good choice for networks of any size.

Rapid Spanning Tree, stack-wide trunking, resilient stacking, link aggregation and built-in redundant power supply support deliver robust performance and fault tolerance.

A1. 802.1X Network Login and RADIUS support allows users to be assigned to designated VLANs with user-specific QoS settings; advanced application filtering, Secure Shell (SSH) encryption, and trusted IP settings provide additional network security.

A2. Expansion ports provide a cost-effective means to implement Gigabit Ethernet backbone links, ensuring rapid access to important network resources at the network core

A3. Forwarding up to 10.1 million pps, with a massive switching fabric of 17.6 Gbps, provides industry-leading performance

A4. Mix and match 24-port and 48-port Switchs to create a resilient stack of up to a total of 384 10/100 connections

Koppelelement B

Affordable, Flexible Layer 3 10/100 Switching
For workgroup 10/100 deployments needing the added benefits of Layer 3 switching. This wirespeed switch has twenty-four 10/100 ports and two 10/100/1000 or SFP-based fiber Gigabit dual-purpose ports.

The Switch's Layer 3 capabilities improve workgroup performance by routing segmented traffic locally at the wiring closet, without the need to send the traffic to the network core for routing. Through its support of dynamic (RIP) routing, deployment and management is greatly simplified over working with static routes, with automatic reconfiguration when there are topology changes.

B1. Edge-optimized Layer 3 switching to speed performance for those environments with network segmentation among its workgroups

B2. Supports dynamic (RIP) routing, easing the setup and ongoing maintenance of the network

B3. 24 10/100 ports with two dual-purpose Gigabit ports supporting 10/100/1000 or SFP fiber modules for maximum flexibility and link aggregation

B4. Wirespeed, non-blocking performance

B5. Enhanced security includes IEEE 802.1X network log-in, Access Control Lists, and encrypted SSL (HTTPS) and SSH management sessions

Anlage: Protokollanalyse „Management-Access", ArBuSt AG Net, Zusammenfassung

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.18.2.115	Broadcast	ARP	Who has 172.18.2.50? Tell 172.18.2.115
2	0.001261	172.18.2.50	172.18.2.115	ARP	172.18.2.50 is at 00:30:1e:bd:c1:58
3	0.001291	172.18.2.115	172.18.2.50	TCP	1033 > telnet [SYN] Seq=0 Ack=0 Win=8192 Len=0 MSS=1460
4	0.003383	172.18.2.50	172.18.2.115	TCP	telnet > 1033 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0 MSS=1436
5	0.003421	172.18.2.115	172.18.2.50	TCP	1033 > telnet [ACK] Seq=1 Ack=1 Win=8616 Len=0
6	0.011282	172.18.2.50	172.18.2.115	TELNET	Telnet Data ...
7	0.011590	172.18.2.115	172.18.2.50	TELNET	Telnet Data ...
8	0.026069	172.18.2.50	172.18.2.115	TELNET	Telnet Data ...
9	0.195945	172.18.2.115	172.18.2.50	TCP	1033 > telnet [ACK] Seq=4 Ack=10 Win=8607 Len=0
10	0.198058	172.18.2.50	172.18.2.115	TELNET	Telnet Data ...
11	0.198153	172.18.2.115	172.18.2.50	TELNET	Telnet Data ...
12	0.355760	172.18.2.50	172.18.2.115	TCP	telnet > 1033 [ACK] Seq=15 Ack=10 Win=1024 Len=0
13	0.355872	172.18.2.115	172.18.2.50	TELNET	Telnet Data ...
14	0.555754	172.18.2.50	172.18.2.115	TCP	telnet > 1033 [ACK] Seq=15 Ack=13 Win=1024 Len=0
15	2.072489	172.18.2.115	172.18.2.50	TELNET	Telnet Data ...
16	2.074994	172.18.2.50	172.18.2.115	TELNET	Telnet Data ...
17	2.198806	172.18.2.115	172.18.2.50	TCP	1033 > telnet [ACK] Seq=15 Ack=17 Win=8600 Len=0
18	**2.200945**	**172.18.2.50**	**172.18.2.115**	**TELNET**	**Telnet Data ...**
19	2.399085	172.18.2.115	172.18.2.50	TCP	1033 > telnet [ACK] Seq=15 Ack=26 Win=8591 Len=0
20	3.475120	172.18.2.115	172.18.2.50	TELNET	Telnet Data ...
85	22.945758	172.18.2.50	172.18.2.115	TELNET	Telnet Data ...
86	23.021134	172.18.2.50	172.18.2.115	TELNET	Telnet Data ...
87	23.021263	172.18.2.115	172.18.2.50	TCP	1033 > telnet [ACK] Seq=36 Ack=1503 Win=8588 Len=0
88	25.720395	172.18.2.115	172.18.2.50	TCP	1033 > telnet [FIN, ACK] Seq=36 Ack=1503 Win=8588 Len=0
89	25.722376	172.18.2.50	172.18.2.115	TCP	telnet > 1033 [ACK] Seq=1503 Ack=37 Win=1024 Len=0

Frame 18 (63 bytes on wire, 63 bytes captured)
Ethernet II, Src: 00:30:1e:bd:c1:58, Dst: 00:04:76:1c:ca:af
Internet Protocol, Src Addr: 172.18.2.50 (172.18.2.50), Dst Addr: 172.18.2.115 (172.18.2.115)
Transmission Control Protocol, Src Port: telnet (23), Dst Port: 1033 (1033), Seq: 17, Ack: 15, Len: 9
    Source port: telnet (23)
    Destination port: 1033 (1033)
    Sequence number: 17
    Next sequence number: 26
    Acknowledgement number: 15
    Header length: 20 bytes
    Flags: 0x0018 (PSH, ACK)
    Window size: 1024
    Checksum: 0x317a (correct)
Telnet
    Data: \r\n
    Data: Login: