Abschlussprüfung Winter 2004/05

Fachinformatiker/Fachinformatikerin
Systemintegration
1197

Ganzheitliche Aufgabe I
Fachqualifikationen

Anlagen

Zum 1. und zum 3. Handlungsschritt

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

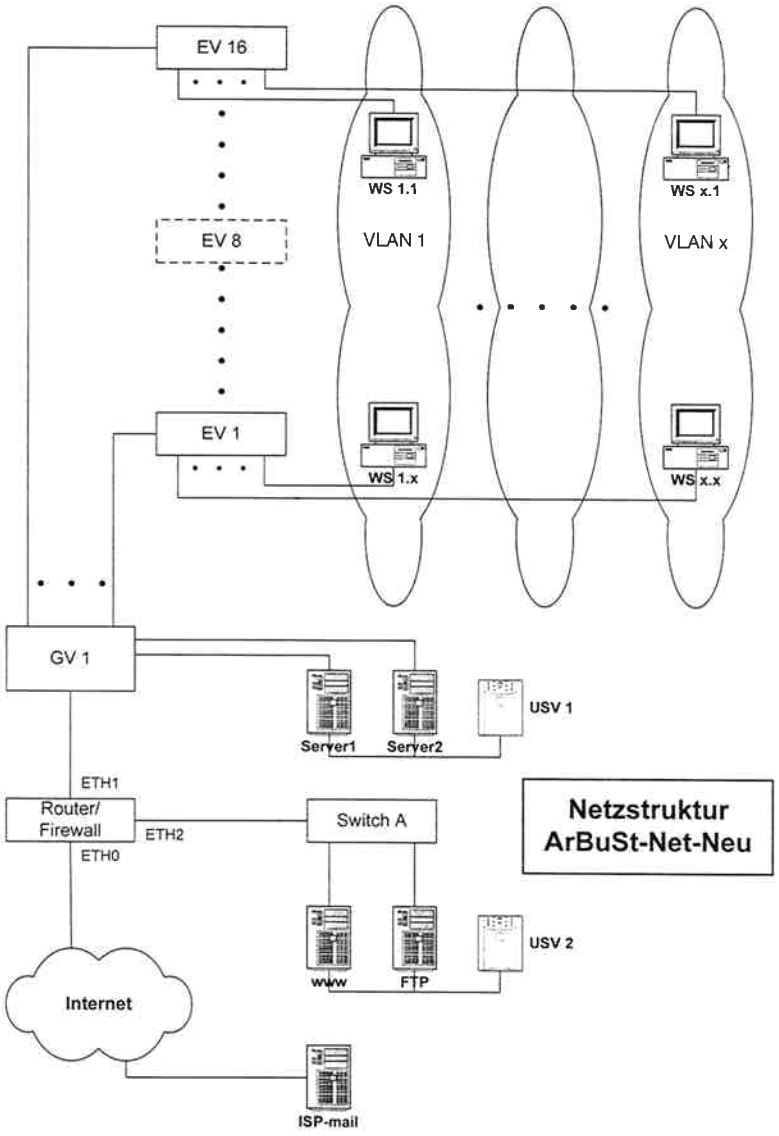
```
No. Time       Source          Destination     Protocol Info
  1 0.000000   172.18.2.115    Broadcast       ARP      Who has 172.18.2.50?  Tell 172.18.2.115
  2 0.001261   172.18.2.50     172.18.2.115    ARP      172.18.2.50 is at 00:30:1e:bd:c1:58
  3 0.001291   172.18.2.115    172.18.2.50     TCP      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 0.358872   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:

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

Die Handlungsschritte 1 bis 6 beziehen sich auf folgende Ausgangssituation:

Sie sind Mitarbeiter/-in der ArBuSt AG und arbeiten dort in der IT-Abteilung.

Die ArBuSt AG ist ein internationaler Finanzdienstleister.
In dem 16-stöckigen Gebäude der Zentralverwaltung ist ein DV-Netzwerk mit 1.850 PCs installiert. Das Netzwerk hat eine fünf Jahre alte strukturierte Verkabelung nach EN 50173-1. Bei der Erstinstallation wurden zur Sicherheit vom Gebäudeverteiler (GV) zu jedem Etagenverteiler (EV) jeweils drei Kat. 5 Kabel verlegt.

Zur Zeit wird die Infrastruktur des Netzes modernisiert.

Sie arbeiten im Modernisierungsprojekt mit.

Sie sollen...
- für das Netzwerk geeignete Koppelelemente auswählen (1. Handlungsschritt).
- das Netzwerk durch eine Firewall absichern (2. Handlungsschritt).
- ein Protokoll einer Netzwerkanalyse interpretieren (3. Handlungsschritt).
- einen Webserver konfigurieren (4. Handlungsschritt).
- ein Logfile auswerten (5. Handlungsschritt).
- das Netzwerk vor Viren und unerwünschten Mails schützen (6. Handlungsschritt).

1. Handlungsschritt (20 Punkte)

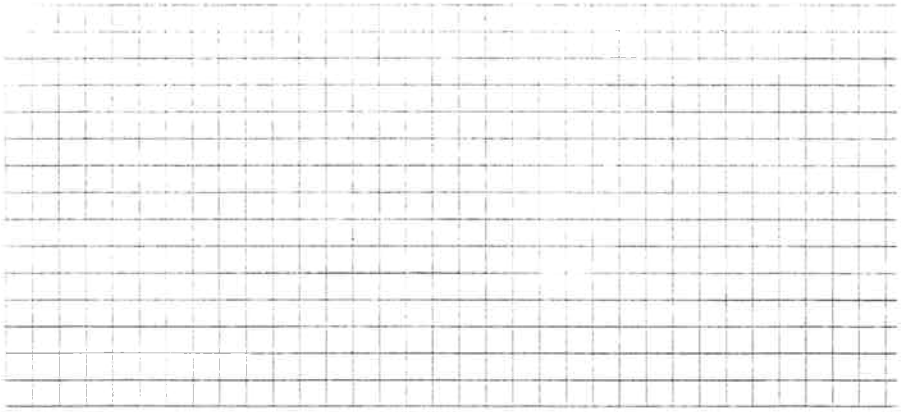
Unter Verwendung der bestehenden strukturierten Verkabelung soll die in der Anlage abgebildete Netzstruktur „ArBuSt-Net-Neu" aufgebaut werden. Um die Leistung und Flexibilität des Netzes zu verbessern, sollen die alten Koppelelemente für den Gebäudeverteiler und die Etagenverteiler ersetzt werden. Die neuen Geräte sollen die folgenden Anforderungen erfüllen:

1. Einrichtung von VLANs, die sich über alle Etagen des Verwaltungsgebäudes ausdehnen können
2. Bei Bedarf Erhöhung der Übertragungsrate zu einzelnen Etagenverteilern auf bis zu 300 Mbps
3. Bis zu 140 Arbeitsplatzanschlussdosen pro Stockwerk
4. Datenaustausch zwischen den VLANs

a) Ordnen Sie auf der Nebenseite die in der Anlage aufgeführten Koppelelemente A und B in der benötigten Anzahl dem Einsatz im GV bzw. in den EVs zu. Begründen Sie Ihre Auswahl durch Hinweise auf die Anforderungen 1 bis 4. (12 Punkte)

b) In jedem VLAN (Subnet) sollen bis zu 350 IP-Adressen (IP Version 4) vergeben werden können. Der Netzwerkkarte ETH 1 wird die private IP-Adresse 172.18.0.1/16 zugeordnet.

Ermitteln Sie die Anzahl VLANs, die maximal eingerichtet werden können; begründen Sie Ihre Lösung. (8 Punkte)



Korrekturrand

Korrekturrand

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)

Korrekturrand

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

- 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 →

Fortsetzung 4. Handlungsschritt

Korrekturrand

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

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)

5. Handlungsschritt (20 Punkte)

Korrekturrand

Korrekturrand

Zum Schutz Ihres Netzes setzt die ArBuSt AG eine Firewall ein, die die folgende Protokolldatei „t.log" erstellt:

```
================================================================================
System Event Log (Current system time: Mon, 23 Feb 2004 10:19:03)
================================================================================
Date        Time      Module  level Type   Description
2004-02-23  08:30:15  system  info  00533  VIP server 172.18.128.10 now alive
2004-02-23  08:30:15  system  crit  00023  VIP server 172.18.128.10 cannot be contacted
2004-02-23  03:43:02  system  info  00533  VIP server 172.18.128.10 now alive
2004-02-23  03:43:02  system  crit  00023  VIP server 172.18.128.10 cannot be contacted
2004-02-23  00:00:47  system  notif 00029  DNS has been refreshed.
2004-02-23  00:00:47  system  info  00529  DNS entries have been automatically refreshed
2004-02-22  22:17:43  system  info  00533  VIP server 172.18.128.10 now alive
2004-02-22  22:17:43  system  crit  00023  VIP server 172.18.128.10 cannot be contacted
2004-02-22  13:25:38  system  info  00533  VIP server 172.18.128.10 now alive
2004-02-22  13:25:38  system  crit  00023  VIP server 172.18.128.10 cannot be contacted
2004-02-22  11:04:44  system  info  00531  The system clock has been updated through NTP
```

a) Aus der Tabelle „t.log" sollen die Einträge mit dem Level „crit" in die Tabelle „TabCrit" einer bereits geöffneten Datenbank geschrieben werden.

TabCrit

lfdNumber(key)	datetime	modul	type
1	2004-02-23 08:30:1	System	00023

Entwerfen Sie auf der Nebenseite ein entsprechendes Programm unter Verwendung folgender Funktionen:

FindString(x, y)
- x ist die Zeichenfolge, nach der gesucht wird.
- y ist die Zeichenfolge, in der gesucht wird.
- Wenn x in y enthalten ist, gibt die Funktion eine 1 zurück.

WriteSQL(y)
fügt einen Datensatz an die Tabelle y an

Verwenden Sie als Darstellungsformen entweder ein
Struktogramm (DIN 66221), oder einen Programmablaufplan (DIN 66001) (16 Punkte)

b) Die Tabelle „TabCode" der Datenbank enthält die Beschreibungen der Fehlertypen.

TabCode

type(key)	description
00023	Server cannot be contacted
00029	DNS Refresh

Stellen Sie auf der Nebenseite die Tabellen TabCrit und TabCode und deren Beziehung in einem ER-Modell dar. (4 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)

Korrekturrand

c) Nennen Sie vier Kriterien, die für die Auswahl einer Antivirensoftware aus betrieblicher Sicht entscheidend sind. (4 Punkte)

d) Nennen Sie vier Mechanismen, mit denen man sich vor Spam Mails schützen kann. (6 Punkte)