

für Lehrerfortbildung und Personalführung

Grundlagen der Schulvernetzung



Qualifizierung von Systembetreuerinnen und Systembetreuern



INHALT

Laborübung 01 -	Analyse eines neuen Computers	. 4
Laborübung 02 -	Anbindung an das Hausnetz per DHCP	. 6
Laborübung 03 -	Zugriff auf einen zentralen Datenspeicher im lokalen Netz	10
Laborübung 04 -	Logik der IP-Adressierung	16
Laborübung 05 -	Internetanbindung über einen Router	22
Laborübung 06 -	WLAN-Anbindung von mobilen Endgeräten	30
Laborübung 07 -	Planung einer Netzwerkstruktur an der Schule	34
Weiterführende La	aborübungen	39
Laborübung 08 -	Zugriff auf das Internet über einen Web-Proxy	40
Laborübung 09 -	Firewall-Einstellungen am Router	42
Laborübung 10 -	Installation der Amtlichen Schulverwaltung (ASV)	48
Anhang:		
Firewalleinstellun	gen und Freigaben unter Windows 7	62
SCHULNETZ-Ausst	attung für Laborübungen	71

IMPRESSUM

Herausgeber:	Akademie für Lehrerfortbildung und Personalführung Kardinal-von-Waldburg-Str. 6 - 7 89407 Dillingen
Autoren:	Georg Schlagbauer, Akademie Dillingen Barbara Maier, Akademie Dillingen
URL: Mail: Stand:	http://alp.dillingen.de/schulnetz schlagbauer@alp.dillingen.de Januar 2012

LABORÜBUNG 01 - ANALYSE EINES NEUEN COMPUTERS

Szenario

Ein Computer soll hinsichtlich seiner Ausstattung und Funktionsfähigkeit analysiert werden.



Vorbereitung

- Ein PC mit installiertem Betriebssystem
- ggf. BIOS-Passwort

Aufgaben

- 1. Identifizieren Sie die von außen sichtbaren Schnittstellen (Netzwerkanschluss, Peripheriegeräte).
- 2. Schalten Sie den Computer ein und rufen Sie das BIOS-Setup auf.
- 3. Notieren Sie die verschiedenen Bootmöglichkeiten des Computers (Festplatte, CD, Diskette, USB, Netzwerk) und ändern Sie ggf. die Bootreihenfolge ab.

Ihre Notizen



HINWEISE

Aufrufen des BIOS-Setup

Beim Hochfahren eines PCs wird in der Regel im unteren Bildschirmbereich angezeigt, mit welcher Taste oder Tastenkombination das BIOS-Setup aufgerufen werden kann. Je nach BIOS-Hersteller unterscheiden sich die Angaben z. B. F1, F2, ESC, Entf, Strg+Alt+Esc, Im BIOS kann die Bootreihenfolge dauerhaft eingerichtet werden.

Aufrufen des Bootmenüs

Beim Hochfahren eines PCs wird in der Regel im unteren Bildschirmbereich angezeigt, mit welcher Taste das Bootmenü aufgerufen werden kann. Im Bootmenü kann temporär das Startverhalten des PC beeinflusst werden z. B. Starten von CD/DVD, Festplatte, USB-Device, PXE-Boot,

LABORÜBUNG 02 -ANBINDUNG AN DAS HAUSNETZ PER DHCP

Szenario

Ein Computer wird an ein lokales Netz angeschlossen. Die per DHCP erhaltenen Netzwerkeinstellungen sollen ermittelt werden.



Vorbereitung

DHCP-Server im Hausnetz

Aufgaben

- 1. Konfigurieren Sie ggf. Ihren Computer so, dass dieser per DHCP die IP-Konfiguration erhält.
- 2. Notieren Sie sich die Netzwerkeinstellungen Ihres Computers:
 - IP-Adresse
 - Subnetzmaske
 - Standardgateway
 - DNS-Server
 - DHCP-Server
 - MAC-Adresse
- 3. Überprüfen Sie die Erreichbarkeit des Standardgateways und eines Web-Servers im Internet auf IP-Ebene (z. B. ping alp.dillingen.de).
- 4. Überprüfen Sie die Erreichbarkeit Ihres Nachbarcomputers auf IP-Ebene. (Beachten Sie ggf. die Firewall-Einstellungen des Nachbarcomputers).
- Interpretieren Sie die Ausgaben von ipconfig in folgenden Fällen:
 a) Am Computer ist kein Netzwerkkabel angeschlossen.
 - b) Der Computer ist an ein Netzwerk ohne DHCP-Server angeschlossen.



Grundlagen d	er Schulv	ernetzung
--------------	-----------	-----------

Ihre Notizen



HINWEISE

Netzwerkkonfiguration unter Windows

Systemsteuerung – Netzwerk und	Internet – Netzwerk- und Freigabecenter
ipconfig	Anzeige der lokalen IP-Einstellungen
ipconfig /all	Ausführliche Konfigurationsinformationen
ipconfig /release	Freigabe der aktuellen DHCP-Zuweisung
ipconfig /renew	Erneuerung der DHCP-Zuweisung

Netzwerkkonfiguration unter Linux

ifconfig	Anzeige der lokalen IP-Einstellungen
dhclient	Erneuerung der DHCP-Zuweisung

Verbindungstest mit ping (IPv4)

ping	<ip-adresse></ip-adresse>	Verbindungstest auf IP-Ebene
ping	127.0.0.1	Testet die korrekte Implementierung des TCP/IP- Stack auf dem eigenen Rechner.
ping	localhost	Testet die korrekte Implementierung des TCP/IP- Stack und die korrekte Namensauflösung auf dem eigenen Rechner.
ping	192.168.1.10	Überprüft eine Verbindung auf IP-Ebene zu einem Rechner mit der angegebenen IP-Adresse.
ping	alp.dillingen.de	Überprüft die Namensauflösung und die Verbin- dung auf IP-Ebene zu einem Rechner mit der ange- gebenen IP-Adresse.

IP-Adresse – MAC-Adresse – ARP-Protokoll

Jede Netzwerkkarte besitzt eine weltweit eindeutige MAC-Adresse. Diese MAC-Adresse wird zur Kommunikation im lokalen Netz benötigt. Die Abfrage nach der MAC-Adresse erfolgt mit dem Address Resolution Protocol (ARP). Auf eine ARP-Anfrage muss ein Computer selbst bei eingeschalteter Firewall antworten.

arp -a	Liest die Tabelle mit den Zuordnungen von IP-
	Adressen zu MAC-Adressen im lokalen Netz auf.
arp -d	Die Einträge in der arp-Tabelle werden gelöscht.

Verbindung zum Nachbarcomputer bei eingeschalteter Firewall

In einem lokalen Netz kann grundsätzlich jeder Computer mit jedem anderen Computer kommunizieren. Auch wenn ein Computer die lokale Windows-Firewall (z. B. ohne Ausnahmen) aktiviert hat und dadurch auf einen ping scheinbar nicht mehr reagiert, findet trotzdem eine Kommunikation über das arp-Protokoll statt.

ping <nachbarcomputer></nachbarcomputer>	keine Reaktion (100 % Verlust, wenn Firewall aktiv)		
arp -a	Anzeige der IP-Adresse und der MAC-Adresse des		
	Nachbarcomputers.		

APIPA-Adressen

Um auch ohne DHCP-Server mit dynamisch zugewiesenen IP-Adressen kommunizieren zu können, werden zufällig ausgewählte Adressen aus dem APIPA-Adressbereich 169.254.0.0/16 (Automatic Private IP Addressing) verwendet. APIPA-Adressen deuten darauf hin, dass der DHCP-Server nicht erreichbar ist.

LABORÜBUNG 03 - ZUGRIFF AUF EINEN ZENTRALEN DATENSPEICHER IM LOKALEN NETZ

Szenario

Die SCHULNETZ-Trainer erstellen auf einer NAS-Box zwei Freigaben, auf welche die Teilnehmer lesend bzw. schreibend zugreifen können (Vorführung der Trainer). Die Teilnehmer greifen auf verschiedenen Wegen auf diese Freigaben zu und nutzen diese zum Datenaustausch.



Vorbereitung

NAS (Network Attached Storage)

Aufgaben

- 1. Überprüfen Sie die Verbindung zum zentralen Datenspeicher (NAS) auf IP-Ebene.
- 2. Greifen Sie auf bereitgestellte Freigaben des zentralen Datenspeichers zu und überprüfen Sie Ihre Zugriffsrechte (keine Rechte, Leserechte, Schreibrechte).
- 3. Testen Sie unterschiedliche Zugriffsmethoden auf die Freigaben (z. B. Windows-Explorer, Kommandozeile).
- 4. Installieren Sie gegebenenfalls einen Netzwerkdrucker an Ihrem Computer.

Ihre Notizen



HINWEISE

Zugriffe auf SMB-Freigaben unter Windows

Adresszeile im Windows-Explorer:

😂 Arbei	itsplatz					_	
<u>D</u> atei	<u>B</u> earbeiten	<u>A</u> nsicht	<u>F</u> avoriten	E <u>x</u> tras	2		2
Adre <u>s</u> se	\\192.16	58.130.10					•

Netzlaufwerk verbinden im Windows-Explorer

🔄 Arbeitsplatz						
Datei	Bearbeiten	Ansicht	Favoriten	Extras	?	1
Adresse 🔽 Arbeitsplatz			Netzla	aufwerk	verbinden	
			Netzla	aufwerk	trennen	
			Synch	nronisier	en	
				Ordne	eroption	en

Netzlaufwerk verbinden auf der Kommandozeile

```
net use Laufwerk: \\servername\freigabename
net use x: \\192.168.130.10\Daten
Die Freigabe wird mit dem Laufwerksbuchstaben x: verbunden.
net use x: \\192.168.130.10\Daten /user:11
Die Freigabe wird mit dem Laufwerksbuchstaben x: verbunden.
Zur Authentifizierung wird der Benutzername (I1) übergeben.
net use x: \\192.168.130.10\Daten /user:11 12345
Die Freigabe wird mit dem Laufwerksbuchstaben x: verbunden.
Zur Authentifizierung werden der Benutzername (I1) und das
Passwort (12345) übergeben.
net use x: \\192.168.130.10\Daten /persistent:yes
Die Laufwerksverbindung x: wird erstellt und bei der nächsten
Anmeldung am lokalen System automatisch wieder hergestellt.
```

Trennen von SMB-Verbindungen

SMB-Verbindungen sind oft sehr dauerhaft. Windows "merkt" sich den Zugriff auf eine Freigabe und versucht, sich beim nächsten Zugriff mit den gespeicherten Anmeldeinformationen zu verbinden. Deshalb kann es bei den einzelnen Tests notwendig sein, sich am lokalen Computer abzumelden und neu anzumelden.

Windows-Explorer:

Extras – Netzlaufwerk trennen

Kommandozeile:

net	use	Laufwerk: /delete	
net	use	x: /delete	Das Netzlaufwerk x: wird getrennt
net	use	* /delete	Alle Netzlaufwerke werden getrennt

Zugriff auf einen Netzwerkdrucker

Netzwerkdrucker werden über die IP-Adresse (oder gegebenenfalls über den Namen bei funktionierender Namensauflösung) angesprochen.

Unter Windows werden die Drucker wie lokale Drucker (mit dem Anschlusstyp TCP/IP-Port) angelegt.

Netzwerkdrucker können auch über das Simple Service Discovery Protocol (SSDP) automatisch gefunden werden, wenn die Netzwerkdrucker dieses Protokoll unterstützen und wenn sich Computer und Drucker im gleichen Netz befinden.

Zugriffe auf SMB-Freigaben unter Linux (Gnome)

Menü: Orte – Verbindung zu Server

🛅 Mit Server verbinden 🛛 🕅
Dienste- <u>T</u> yp: Windows-Freigabe
Server: 10.36.104.10
Optionale Informationen:
<u>F</u> reigabe: Daten
Ordner:
Benutzername:
Domain-Name:
🗌 Lesezeichen <u>h</u> inzufügen
Lesezeichenname:
<u>H</u> ilfe <u>A</u> bbrechen <u>V</u> erbinden

Nautilus-Adressleiste:

smb://ip-Adresse
smb://ip-Adresse/freigabe
smb://user@<ip-Adresse>



Die Adressleiste beim Dateibrowser Nautilus muss ggf. mit <Strg>+L eingeblendet werden.

Ihre Notizen



LABORÜBUNG 04 - LOGIK DER IP-ADRESSIERUNG

Szenario

Mehrere Computer sollen miteinander vernetzt werden. Die Erreichbarkeit der Computer bei unterschiedlichen IP-Einstellungen wird getestet.



Vorbereitung

- Switch
- geeignete Twisted-Pair-Kabel
- 3 oder 4 Computer zum Vernetzen

Aufgaben

- 1. Verbinden Sie jeweils 3 oder 4 Computer über einen Switch und überprüfen Sie am Signalzustand der LEDs, ob ein Link vorhanden ist.
- Vergeben Sie IP-Adressen aus dem Netzwerk 192.168.1.0/24 und testen Sie die Verbindung der Computer auf IP-Ebene. Sorgen Sie dafür, dass der ping nicht durch die Firewall blockiert wird.
- 3. Ordnen Sie einem Rechner eine IP-Adresse aus dem Netzbereich 192.168.2.0/24 zu und testen Sie die Verbindungen auf IP-Ebene.
- 4. Ändern Sie die Subnetzmaske an allen Rechnern auf 255.255.0.0 ab und testen Sie die Verbindungen.



Ihre Notizen



HINWEISE

Aufbau einer IP-Adressen

Eine IP-Adresse (IPv4) besteht aus 4 Byte = 32 Bit (in Zukunft aus 16 Byte; IPv6). Jedes Byte kann einen Wert zwischen 0 und 255 annehmen. Für die Darstellung in Dezimalform wird die IP-Adresse in vier Oktette unterteilt.

IP-Adresse	192	168	1	10
	1. Oktett	2. Oktett	3. Oktett	4. Oktett

IP-Adresse und Subnetzmaske

Eine IP-Adresse enthält einen Netzanteil und einen Hostanteil. Der Netzanteil dient der Wegfindung, der Hostanteil der Zustellung zu einem bestimmten Computer im Zielnetz. Die Trennung von Netz- und Hostanteil erfolgt mit Hilfe der Subnetzmaske.

Wird der IP-Adresse 192.168.1.10 die Subnetzmaske 255.255.255.0 zugeordnet, so bedeutet dies, dass sich der Computer im Netz 192.168.1.0 befindet und die "Hausnummer" 10 besitzt. Die Subnetzmaske 255.255.255.0 kann auch mit /24 (Anzahl der binären 1-bits) abgekürzt werden.

IP-Adresse	192	168	1	10
Subnetzmaske	255	255	255	0

Daraus ergibt sich:

Netzanteil	192	168	1	0
Hostanteil	0	0	0	10

Kommunikation zwischen Computern

Computer, die sich im gleichen Netz befinden, können direkt miteinander kommunizieren. Computer in unterschiedlichen Netzen benötigen einen Router, der die Signale von einem Netz in das andere Netz weiterleitet.

Klasseneinteilung von IP-Adressen

In der Vergangenheit wurden IP-Adressen in Klassen (A, B, C) aufgeteilt. Diese Unterscheidung ist durch die Verwendung von Subnetzmasken überflüssig geworden.

Private IP-Adressen

Bestimmte IP-Adressen sind für die Nutzung innerhalb von LANs vorgesehen. Diese privaten IP-Adressen stehen weltweit allen Nutzern zur Verfügung. Da eine IP-Adresse immer eindeutig sein muss, werden diese Adressen nicht im Internet verwendet.

Klasse (veraltet)	Privater Adressbereich	Standard-Subnetzmaske
А	10.0.0.0 - 10.255.255.255	255.0.0.0
В	172.16.0.0 - 172.31.255.255	255.255.0.0
С	192.168.0.0 - 192.168.255.255	255.255.255.0

Multicast-Adressen

Um mehrere Computer gleichzeitig ansprechen zu können (z. B. bei Videoübertragungen oder beim Klonen mehrerer Computer), weisen diese Programme den beteiligten Computern zusätzlich eine Multicast-Adresse zu.

Adressbereich: 224.0.0.0 - 239.255.255.255

Loopback-Adressen

Mit einer Loopback-Adresse wird der eigene Computer angesprochen. Üblicherweise wird dazu die Adresse 127.0.0.1 verwendet.

Loopback-Adressen: 127.0.0.1 - 127.255.255.254

Broadcast Adressen

Die Kommunikation innerhalb eines Netzes erfordert auch Rundspruch-Nachrichten an alle Geräte. Broadcasts werden von Routern nicht an andere Netze weitergeleitet. Innerhalb eines Netzes spricht man deshalb von einer Broadcast-Domäne. Als Broadcast-Adresse ist immer die letzte IP-Adresse des Netzwerkadressbereiches definiert.

 Broadcast-Adresse des Netzes 192.168.1.0/24:
 192.168.1.255

 Allgemeine Broadcast-Adresse:
 255.255.255.255

APIPA-Adressen

Um auch ohne DHCP-Server mit dynamisch zugewiesenen IP-Adressen kommunizieren zu können, werden zufällig ausgewählte Adressen aus dem APIPA-Adressbereich 169.254.0.0/16 (Automatic Private IP Addressing) verwendet. APIPA-Adressen deuten darauf hin, dass der DHCP-Server nicht erreichbar ist.

FREIGABEN UNTER WINDOWS

Das Erstellen von einfachen Dateifreigaben unter Windows ist im Anhang erläutert.

Das Erstellen von Dateifreigaben mit Zugangsberechtigungen unter Windows ist Thema des Kurses "Windows 7-Netzwerke"

Das Erstellen von Dateifreigaben unter Linux ist Thema des Kurses "Linux-Netzwerke"

Ihre Notizen



LABORÜBUNG 05 -INTERNETANBINDUNG ÜBER EINEN ROUTER

Szenario

Mehrere Computer sollen über einen Router an das Hausnetz (bzw. über DSL an das Internet) angebunden werden.



Aufgaben

- 1. Stellen Sie einen Konfigurationszugang zum Router über das Webinterface her.
- 2. Konfigurieren Sie den Router so, dass die Verbindung der Computer des internen Netzes mit dem Internet bzw. Hausnetz funktioniert.
 - Wählen Sie dazu IP-Adressen aus einem privaten IP-Adressbereich, der nicht mit dem IP-Adressbereich des Hausnetzes kollidiert.
 - Ermöglichen Sie den Clients den Zugang zum Internet, indem Sie am externen Interface NAT/PAT aktivieren.
 - Konfigurieren Sie den Router als DHCP-Server und DNS-Relay für das interne Netz.

Ihre Notizen



HINWEISE

Empfohlene Vorgehensweise bei der Konfiguration eines Routers:

- Zurücksetzen des Router
- Grundkonfiguration des Routers
- Konfiguration zusätzlicher Dienste (DNS, DHCP)
- Konfiguration der Firewall

Zurücksetzen eines Routers in den Auslieferungszustand

Bei einem "verkonfigurierten" Gerät oder wenn man nicht weiß, wie das Gerät vorher eingesetzt wurde, ist es sinnvoll das Gerät in den Auslieferungszustand zurückzusetzen.

Bei einfachen Routern erfolgt das Zurücksetzen meist über eine Reset-Taste. Verfügt ein Router über einen Konsolenzugang ist dies die bessere Alternative.

Eine Konsolenverbindung hat den Vorteil, dass sie unabhängig von Netzwerkeinstellungen funktioniert. Diese Möglichkeit bieten in der Regel nur professionelle Router.

Zur Kommunikation dienen Terminal-Emulatoren z. B.:

- Hyper Terminal
- Putty
- Tera Term

Konfiguration eines Routers

Die Konfiguration eines Routers kann über verschiedene Zugriffsmöglichkeiten erfolgen:

- Webinterface (http oder https)
- Telnet oder SSH
- SNMP (Simple Network Management Protocol)
- Konsole (serielle Schnittstelle; Terminal-Emulator)

Zurücksetzen des Routers bintec RS120 in den Auslieferungszustand

Bei einer bestehenden Konsolenverbindung wird der Bootvorgang des Routers durch betätigen der Leertaste (Space-Taste) unterbrochen:

Press <sp> for boot monitor or any other key to boot system

Danach erscheint ein Auswahlmenü:

- (1) Boot System
- (4) Delete Configuration

Konfiguration des Routers bintec RS120 über das Web-Interface

In der Standardkonfiguration ist der Router auf der internen Schnittstelle (en1-0, Port 1-4) unter der IP-Adresse 192.168.0.254 erreichbar.

Login:	admin
Password:	funkwerk

IP-Konfiguration der Schnittstellen

An der externen Schnittstelle (ETH5, en1-4) kann der Router die IP-Adresse gegebenenfalls auch per DHCP aus dem Hausnetz erhalten.

🖉 bintec R5120: IP Configuration - Interfaces - Windows Internet Explorer											
	/esi/795106/esi.cgi?j	page=status-inde	ex.xml&sessionID=30	09492010				• +	🗙 🔁 Bing	₽ -	
🔗 🖉 bintec RS120: IP Configuration - Interfaces											
bintec RS120	Language	English 💌	View Standard	i 🔽	Online Help	Logout	funkwerk))				
Save configuration Interfaces											
System Management 🛛 👻											
Physical Interfaces 🔹 👻	Interface	IP Address		Netmask		Address Mode	status	Action			
LAN	en1-0	192.168.0	.254	255.255.255.0 Static		0	1	P			
IP Configuration	en1-4	10.36.13.1	133	255.255.255	255.255.255.0 Static			1			
VLAN					17	~					
Routing 🗸					New						
WAN -											
VPN -											
Firewall 👻											
VoIP 🗸											
Local Services 🗸											
Maintenance 🔹										•	

Routing

Gegebenenfalls muss die Default-Route eingetragen werden, falls diese nicht per DHCP aus dem übergeordneten Netz vergeben wurde.

bintec RS120: Routen - IP-Routen	- Windows Internet E	xplorer								
	si/795106/esi.cgi?userId	ent=858031435					• +	× 🔁	Bing	P
☆ Øbintec RS120: Routen - IP-Route	n									
and A very be		12 14 44 14	Canan ta a 🖓 🖓 🖓	3	1		172 A 194	(191) (191)		
bintec RS120	Sprache Deutsc	h 🚽 🛛 Ansicht St	andard 💌	Online-Hilfe Ausloggen	funl	kwerk))				
		No. of Concession, Name		AND INCOME IN CASE OF	1 arps	Communications •				
Konfiguration speichern				IP-Routen Optionen						
Assistenten 👻										
Systemverwaltung 🗸 🗸										
Physikalische Schnittstellen 👻	Ansicht 20 p	oro Seite < 🚿 Filtern in	Keiner	gleich 🔽	Los					
LAN 👻	Ziel-IP-Adresse	Netzmaske	Gateway	Schnittstelle	Metrik	Erweiterte	Routentyp			
Routing	10.36.13.0	255.255.255.0	10.36.13.133	LAN_EN1-4	0		Netzwerkroute	窗		
Routen	192.168.0.0	255.255.255.0	192.168.0.254	LAN EN1-0	0	Г	Netzwerkroute	斎		
RIP	0.0.0.0	0.0.0.0	10.36.13.1	LAN EN1-4	1	-	Standardroute	圇		
Lastverteilung	Seite: 1, Objekte: 1 -	- 3				-				
Multicast										
QoS				Neu						
WAN -										
VPN 👻										
Firewall 🗸										

NAT

Am externen Interface muss NAT aktiviert werden.

🖉 bintec RS120: NAT - NAT-Schnittst	ellen - Windows In	ternet Explorer						
	esi/795106/esi.cgi?use	rIdent=858031435					💌 😽 🗙 🔁 Bing	₽ -
🔶 Dintec RS 120: NAT - NAT-Schnitt	stellen							
bintec RS120	Sprache Deut	sch 🔹 Ansich	nt Standard 💌	Online-Hilfe	Ausloggen	funkwerk))		
Konfiguration speichern Assistenten			NAT-S	chnittstellen <u>N</u>	AT-Konfigur	ation		
Systemverwaltung 🗸 🗸								1
Physikalische Schnittstellen 👻	Ansicht 20	pro Seite 🔍 🚿 F	ittern in Keiner	– g	gleich 💌		.05	
LAN 👻	Schnittstelle	NAT aktiv	Verwerfen ohne Rückm	eldung	PPTP-Pass	through	Portweiterleitungen	
Routing	LAN_EN1-0						0	
Routen	LAN_EN1-4	V					0	
NAT	Seite: 1, Objekte:	1 - 2						
RIP					brooken			
					brechen			
QoS								
WAN -								
von ·								
VPN ¥								
Firewall •								•
,								_

Network Address Translation (NAT)

Damit ein Computer im lokalen Netz mit Computern im Internet kommunizieren kann, ersetzt der Router die privaten Quelladressen aller IP-Pakete, die das lokale Netz verlassen, mit einer öffentlichen IP-Adresse (Netzadressübersetzung).

In der Regel wird mehreren Computern mit privaten IP-Adressen eine öffentliche IP-Adresse zugewiesen. Durch die gemeinsame Nutzung einer öffentlichen IP-Adresse durch mehrere Computer werden zur Differenzierung der Kommunikationsstränge noch Portnummern herangezogen.

Ansicht der NAT-Tabelle bei einem bintec-Router

Bei einem bintec-Router kann man die NAT-Tabelle über die Konsolenansicht oder über die SNMP-Ausgabe (Webinterface oder Dime-Tools) anzeigen lassen.

Konsole

ipnattable Anzeige der NAT-Tabelle

SNMP-Ansicht: ip - ipnattable

🕙 bintec R232b: ipNatTabl	le - ipNat	iTable - I	Mozilla	Firefox												
ii) bintec R232b: ipNatTable - ipNatTable 🔅																
bintec R232b		Sprac	Sprache Deutsch Ansicht SNMP-Browser Online-Hilfe Ausloggen funkwerk:))													
Konfiguration speicher	n		ipNatTable													
administration	-															
adsl	-															
alive	-	Index	Ifindex	Protocol	IntAddr	IntPort	ExtAddr	ExtPort	RemoteAddr	RemotePort	Direction	Age	Context	Timeout	State	Catego
apdisc	-	0	10001	tcp	192.168.0.112	1436	79.219.213.187	62312	208.88.186.6	34057	outgoing	735	0	3600	active	symm
atm	-	1	10001	tcp	192.168.0.112	1444	79.219.213.187	45794	212.161.8.6	12350	outgoing	7235	0	3600	active	symm
authentication	-	2	10001	tcp	192.168.0.111	49161	79.219.213.187	33316	205.188.11.47	443	outgoing	735	0	3600	active	symm
bridge		3	10001	tcp	192.168.0.111	49162	79.219.213.187	34171	64.12.73.134	443	outgoing	736	0	3600	active	symm
bridge	-	4	10001	tcp	192.168.0.111	49164	79.219.213.187	48124	64.12.73.195	443	outgoing	737	0	3600	active	symm
brrp	•	5	10001	tcp	192.168.0.110	1396	79.219.213.187	34056	209.85.148.106	80	outgoing	4137	0	3600	active	symm
capi	-	6	10001	tcp	192.168.0.110	1397	79.219.213.187	46329	209.85.148.106	80	outgoing	4138	0	3600	active	symm
hdsl2shdsl	-	7	10001	icmp	192.168.0.4	51014	79.219.213.187	32994	194.95.207.10	0	outgoing	2239	0	30	active	symm
interfaces	-	8	10001	udp	192.168.0.112	31432	79.219.213.187	40944	66.74.222.138	61404	outgoing	739	0	30	active	symm
ip		•														Þ
biboPingTable		New														
icmp																
ip																

DHCP-Server

Durch einen DHCP-Server (**D**ynamic **H**ost **C**onfiguration **P**rotocol) können Clients ohne manuelle Konfiguration in ein bestehendes Netzwerk eingebunden werden. Ein DHCP-Server kann eine Vielzahl von Einstellungen an den Client übermitteln. Üblicherweise werden einem Client folgende Einstellungen zugewiesen:

- IP-Adresse und Netzwerkmaske
- Default-Gateway
- DNS-Server
- evtl. WINS-Server (für Microsoft Windows Clients)

Konfiguration des DHCP-Dienstes bei einem bintec-Router

C bintec R5120: DHCP Server - DHCP Pool - Windows Internet Explorer												
🔆 🔄 🗢 🙋 http://192.	168.0.254/	esi/795106/esi.cgi?	page=status-index.xml&&s	essionID=2146903669				• •	🗙 🔁 Bing	P -		
2 Contract RS 120: DHCP Server - DHCP Pool												
bintec RS120		Language [English View	Standard	Online Help	Logout	funkwerk))					
Save configuration				DHCP Pool	P/MAC Binding	DHCP R	elav Settings					
Assistants	-			-								
System Management	-											
Physical Interfaces	-	Interface	IP Address Range		Gateway		Lease Time	Status				
LAN	-	en1-0	192.168.0.10 - 192.16	58.0.49	Own IP Addres	s	120Min.	Enabled	<u>i</u>			
Routing	-			Maw	01/							
WAN	-			New	Un							
VPN	-											
Firewall	-											
VolP	-											
Local Services												
DNS												
HTTPS												
DynDNS Client												
DHCP Server												
Web Filter										•		



DNS-Relay

Ist in einem Netz kein DNS-Server vorhanden, kann der Router als DNS-Relay eingerichtet werden. Beim Client wird der Router als DNS-Server eingetragen. Der Router nimmt die DNS-Anfragen der Clients entgegen und reicht diese an einen ihm bekannten DNS-Server weiter.

Der Router selbst kann die DNS-Konfiguration auch dynamisch per DHCP erhalten (Dies ist bei DSL-Anschlüssen üblich.)

🕹 bintec R232b: DNS - Globale	Einstellungen - Mozilla Firefox															
🔌 bintec R232b: DNS - Globa	le Einstellu 🔶															
bintec R232b	Sprache Deutsch 💌 Ansicht	Standard	Online-Hilfe	Ausloggen												
Konfiguration speichern	Globale Einste	ellungen <u>Statis</u>	sche Hosts Dom	nänenweiterlei	tung <u>Cache</u>	<u>Statistik</u>										
Systemverwaltung -																
Physikalische -	Basisparameter															
Schnittstellen	Domänenname															
LAN - Routing -	DNS-Serverkonfiguration	O Dynamisch	C Statisch													
WAN -	DNS-Server	Primär	217.0.43.145													
VPN -		Sekundär	217.0.43.129													
Firewall v	WINS-Server	Primär	0.0.0.0													
Lokale Dienste		Sekundär	är 0.0.0.0													
DNS																
HTTPS	4	Erweiterte Einstellungen														
DynDNS-Client																
bior-server	· · · · · · · · · · · · · · · · · · ·					OK Abbrechen										

Konfiguration des DNS-Dienstes bei einem bintec-Router

Konfiguration der Firewall

An einem Router können beim Übergang von einem Netz in ein anderes Netz Firewallregeln definiert werden. Dazu ist eine weiterführende Übung (Laborübung 09 - Firewall-Einstellungen am Router) vorgesehen.

LABORÜBUNG 06 -WLAN-ANBINDUNG VON MOBILEN E<u>NDGERÄTEN</u>

Szenario

Notebooks sollen über WLAN in das bestehende Netzwerk eingebunden werden und Zugriff auf das Internet erhalten.



Aufgaben

- 1. Stellen Sie einen Konfigurationszugang zum Access Point über das Webinterface her.
- 2. Konfigurieren Sie den Access Point so, dass die Notebooks Zugriff auf das Internet erhalten.
- 3. Sichern Sie die Verbindung mit WPA2 (PSK) ab.

Ihre Notizen



HINWEISE

Zurücksetzen des Access-Points bintec W1002n in den Auslieferungszustand

Bei einer bestehenden Konsolenverbindung wird der Bootvorgang des Access-Points durch betätigen der Leertaste (Space-Taste) unterbrochen:

Press <sp> for boot monitor or any other key to boot system

Danach erscheint ein Auswahlmenü:

- (1) Boot System
- (4) Delete Configuration

Konfiguration des bintec W1002n

Die Konfiguration eines Access-Points kann über verschiedene Wege erfolgen:

- Webinterface (http oder https)
- Telnet oder SSH
- SNMP (Simple Network Management Protocol)
- Konsole (serielle Schnittstelle; Terminal-Emulator)

Konfiguration des bintec W1002n über das Web-Interface

Für den Webzugriff auf den Access-Point muss die IP-Adresse des Access-Points bekannt sein oder ermittelt werden. Der Access-Point verhält sich dabei folgendermaßen:

- Wenn es einen DHCP-Server im Netz gibt, bezieht der Access-Point von diesem eine IP-Adresse.
- Wenn es keinen DHCP-Server im Netz gibt, hat der Access-Point die IP-Adresse 192.168.0.252.

Eine per DHCP bezogene IP-Adresse kann auf folgenden Wegen ermittelt werden:

- Auf dem DHCP-Server können die vergebenen IP-Adressen ermittelt werden.
- Mit den Funkwerk-Dime-Tools können alle Access-Points im Netz ermittelt werden.

Bei einer Konsolenverbindung kann mit ifconfig die IP-Adresse ermittelt werden.

Zugriffsdaten:

Login:	admin
Password:	funkwerk

Konfiguration der WLAN-Einstellungen

Für die WLAN-Konfiguration genügen die Einstellungen unter Wireless LAN – WLAN.

🖉 bintec W1002n: WLAN - Einstellun	gen Funkmodul - Windows	Internet Explorer								
	/esi/796105/esi.cgi?page=statu	s-index.xml&sessionI	D=859134096				•	47 🗙 🔁	Bing	^
🙀 🍘 bintec W1002n: WLAN - Einstellungen Funkmodul										
bintec W1002n w1002n	Sprache Deutsch	Ansicht St	andard 🔽	Online-Hilfe	Auslogger	funkwerk	(i))			
Konfiguration speichern Assistenten			Einstellunger	Funkmodul	Drahtlosne	zwerke (VSS)]			
Systemverwaltung Physikalische Schnittstellen			E	instellungen Fun	kmodul					
LAN -	MAC-Adresse 00:0d:f0:24:2c:ba	Betriebsmodus Access-Point	Frequenzband 2.4 GHz	Verwendeter K	anal Ma Au	ximale Bitrate	Sendeleistung Max.	Status		
Wireless LAN							1	1-		
WLAN Verwaltung										
Wireless LAN Controller 🛛 👻										
Routing -										
WAN -										

Einstellungen unter Wireless LAN – WLAN – Einstellungen Funkmodul

Betriebsmodus:	Access-Point
Frequenzband:	2,4 GHz
Drahtloser Modus:	802.11b/g/n

Einstellungen unter Wireless LAN – WLAN – Drahtlosnetzwerke (VSS)

(Diese Einstellmöglichkeiten sind nur im Betriebsmodus Access-Point sichtbar.)

Netzwerkname (SSID):	(Name des Funknetzes)
Sicherheitsmodus:	WPA-PSK
WPA-Modus:	WPA 2
Preshared Key:	(Passwort)

LABORÜBUNG 07 -PLANUNG EINER NETZWERKSTRUKTUR AN DER SCHULE

Szenario

Die Lehrgangsteilnehmer sollen für ihre eigene Schule einen logischen Netzwerkplan erstellen und Firewall-Regeln für den Router bzw. Layer-3-Switch definieren.



Aufgaben

1. Planen Sie für Ihre Schule eine logische Netzstruktur mit unterschiedlichen Teilnetzen, die über einen Router oder Layer-3-Switch verbunden sind.

Beispiel 1 (100 Computer): Verwaltungsnetz, Lehrerzimmer, Unterrichtsnetz

Beispiel 2 (500 Computer): Verwaltungsnetz, Lehrerzimmer, Computerraum 1, Computerraum 2, Klassenzimmer 1. Stock, Klassenzimmer 2. Stock, mobile Geräte

2. Definieren Sie Firewall-Regeln für den Zugriff der einzelnen Netze untereinander und für den Zugriff ins Internet.

Ihre Notizen



HINWEISE

Trennung von Netzen

Lokale Netze können in mehrere voneinander geschützte Teilnetze unterteilt werden. Jedes dieser Teilnetze ist ein eigenes Netz (Broadcastdomäne). Die jeweilige Schnittstelle des Routers ist das Standardgateway für die Computer im jeweiligen Netz. Neben der Größe spielen für die Trennung vor allem Sicherheitsaspekte eine Rolle (z. B. Unterrichtsnetz, Lehrerzimmer, Verwaltungsnetz).

Kommunikation zwischen den Teilnetzen

Zur Verbindung von Teilnetzen ist ein Router oder ein Layer-3-Switch nötig. Damit lassen sich kontrollierbare Übergänge einrichten. An dieser Stelle kann sehr detailliert geregelt werden, wer mit wem über welches Protokoll kommunizieren kann. In der Schule ließe sich zum Beispiel regeln, dass sowohl vom Unterrichtsnetz und dem Lehrerzimmer auf den Schulserver zugegriffen werden kann, ohne dass ein Zugriff vom Unterrichtsnetz in das Lehrerzimmer möglich ist. Ebenso könnte geregelt werden, dass von einem Computer aus dem Verwaltungsnetz der Zugriff auf das Unterrichtsnetz erlaubt, jedoch jeglicher Zugriff vom Unterrichtsnetz in das Verwaltungsnetz verboten ist.

Firewall

Die Regelung, welche Teilnetze mit welchen Protokollen aufeinander zugreifen dürfen, ist Aufgabe der Firewall. Die Firewall beschränkt dazu mögliche Verbindungen zwischen den Netzen, indem einzelne Pakete nicht weitergeleitet sondern verworfen werden. Mit Firewall-Regeln lässt sich der Datenverkehr sehr detailliert regeln.

Beschreibung der Firewallregeln

Die Definition der Firewallregeln für unterschiedliche Teilnetze lässt sich am einfachsten in einer Matrix erfassen, in der die Zugriffe beschrieben sind.

Logischer Netzwerkplan



Firewallregeln

nach von	Unterrichtsnetz	Lehrerzimmer	Verwaltung	Internet
Unterrichtsnetz		Kein Zugriff	Kein Zugriff	Zugriff nur für den Proxy auf Port 80, 443
Lehrerzimmer	Zugriff auf die NAS-Box		Zugriff auf den Notenmanager	Zugriff auf Port 80, 443
Verwaltung	Kein Zugriff	Kein Zugriff		Zugriff auf Port 80, 443, 25



WEITERFÜHRENDE LABORÜBUNGEN

LABORÜBUNG 08 -ZUGRIFF AUF DAS INTERNET ÜBER EINEN WEB-PROXY

Szenario

Der Zugang zum Internet soll über einen Web-Proxy (mit Webfilter) eingerichtet werden.



Aufgaben

- 1. Installieren Sie den OpenSchoolProxy an einem Computer und konfigurieren Sie den Webfilter.
- 2. Tragen Sie am Browser des Computers den Proxy ein und testen Sie die Funktionalität.

HINWEISE

Proxy

Ein Proxy (Stellvertreter) ist ein Serverdienst, der auf der Anwendungsebene arbeitet. Proxys gibt es für verschiedene Internet-Anwendungen, z. B. für http, ftp, smtp. Am bekanntesten sind die Web-Proxy (z. B. Squid). Ein Client baut dabei keine direkte Verbindung zum Internet auf, sondern sendet seine Anfrage an den Proxy. Dieser sendet daraufhin eine eigenständige Anfrage an den Webserver und leitet die Antwort an den Client weiter. Der Webserver im Internet sieht als Absender nur den Proxy und nicht den anfragenden Client.

Da ein Proxy den kompletten Inhalt der angefragten Informationen zwischenspeichert, kann zusätzlich noch ein Webfilter eingesetzt werden, um unerwünschten Datenverkehr zu verhindern.

Webfilter

Die meisten angebotenen Webfilter arbeiten mit URL-Filterlisten. Die Anbieter versuchen dabei möglichst alle Webseiten zu erfassen und jede Webseite einer oder mehrerer Kategorien zuzuordnen (z. B. Spiele, Gewalt, Bildung, …). Dem Filter wird dann mitgeteilt, welche Kategorien geblockt werden sollen. Die angebotenen Filterlösungen lassen es zum Teil auch zu, dass benutzer-, klassenraum- oder zeitspezifisch unterschiedliche Kategorien gesperrt werden.

Die Filterlisten werden dabei lokal auf dem Proxy vorrätig gehalten und regelmäßig aktualisiert oder es wird bei jeder Webanfrage zunächst ein Filterserver im Internet nach der zu kategorisierenden Seite befragt.

LABORÜBUNG 09 -FIREWALL-EINSTELLUNGEN AM ROUTER

Szenario

Am Router soll eine Firewall eingerichtet werden, die nur dem Web-Proxy den Zugang ins Internet erlaubt.



Aufgaben

- 1. Richten Sie das von Ihnen verwaltete Netz so ein, dass der Internetzugang funktioniert. In Ihrem Netz befindet sich ein Web-Proxy mit einer Filterlösung. Der Router soll dabei als DHCP-Server und DNS-Relay fungieren.
- 2. Richten Sie am Router eine Firewall ein, so dass der Zugriff zum Internet nur noch über den Web-Proxy möglich ist.
- 3. Schränken Sie gegebenenfalls die Firewall so ein, dass der Proxy nur über Port 80 ins Internet kommt.

Ihre Notizen



HINWEISE

Firewall

Eine Firewall beschränkt mögliche Verbindungen, indem einzelne Pakete nicht weitergeleitet sondern verworfen werden. Mit Firewallregeln lässt sich der Datenverkehr sehr detailliert regeln.

Firewallregeln

Eine Firewallregel besteht aus Filterkriterien und einer zugehörigen Aktion. Die Filterkriterien sind Quelle, Ziel und Dienstekennung (z. B. DNS oder http). Die möglichen Aktionen sind Zugriff, Verweigern und Zurückweisen.

Quelle und Ziel können Schnittstellen, IP-Netze oder einzelne IP-Adressen sein. Mögliche Dienste sind alle Layer-3 und Layer-4-Protokolle (z. B. IP, ICMP, TCP, UDP) und über die TCP- und UDP-Ports definierten Standardanwendungen (z. B. http, DNS, smtp).

Mögliche Aktionen sind:

•	Zugriff (Access)	Pakete werden weitergeleitet.
•	Verweigern (Deny)	Pakete werden verworfen.
•	Zurückweisen (Reject)	Pakete werden verworfen, der Absender erhält eine Information

Beispiele

	Aktion		
Quelle	Ziel	Dienst	
Schnittstelle 1	Schnittstelle 2	any	Deny
Schnittstelle 1	Schnittstelle 4	http	Access
192.168.0.0/24	Schnittstelle 2	icmp	Access

Die Firewallregeln werden von oben nach unten abgearbeitet. Wenn das Filterkriterium greift (d. h. wenn Quelle, Ziel und Dienstekennung mit einem ankommenden IP-Paket übereinstimmen) wird die festgelegte Aktion angewendet. Alle nachfolgenden Regeln werden für dieses IP-Paket nicht mehr beachtet.

Üblicherweise trägt man in eine Firewall nur die Wege oder Verbindungen ein, die erlaubt sein sollen. Alles andere ist automatisch verboten (implicit deny).

Stateful Inspection Firewall

Bei einer Stateful Inspection Firewall muss für Antwortpakete keine eigene Regel definiert werden. Antwortpakete sind automatisch erlaubt, wenn diese zu einer bestehenden Verbindung passen. Detail zu Firewalltypen sind in der Broschüre "Sichere Internetanbindung von Schulen" (<u>http://alp.dillingen.de/schulnetz/materialien</u>) erläutert.

Besonderheiten bei bintec Routern:

- Solange noch keine Firewallregel gesetzt ist, ist die Firewall nicht aktiv, obwohl diese als aktiv markiert ist.
- Der Router selbst wird (bei Quelle oder Ziel) mit LOCAL angesprochen. Je nach Firmware-Version ist es gegebenenfalls notwendig, zunächst eine Regel zu erstellen, die verhindert, dass man sich selbst aussperrt und den Router nicht mehr über das Webinterface konfigurieren kann.

Der administrative Zugriff in der Systemverwaltung korrespondiert mit entsprechenden Firewallregeln.

bintec RS120: Policies - F	ilter Rule	es - Windo	ows Internet Explorer									
🔾 🗢 🕖 http://192.:	168.0.254/	esi/795106	i/esi.cgi?page=status-ind	ex.xml&&sessionID=21469	903669			-	- •	×	🔁 Bin	g
bintec RS120: Policies	- Filter Ru	les										
bintec RS120		Langu	uage English 💌	View Standard	Online	Help Logou	t funkwerk))				10	
Save configuration	•				Filter R	iles <u>QoS</u> Oj	ptions					
System Management	-											
Physical Interfaces	-	View	20 per page 🥢	Filter in None	▼ equal	-	Go					
LAN	-	Order	Source	Destination	Service	Action	Priority	Policy active	-			
Routina	-	1	LAN_EN1-0	LOCAL	any	Access	None	Enabled		E+	â (6
- NAN	-	2	Web-Proxy	LAN_EN1-4	http	Access	None	Enabled			Î	6
/PN	-	3	Web-Proxy	LAN_EN1-4	http (SSL)	Access	None	Fnabled		E*	ê (3
Firewall		Page:	1, Items: 1 - 3							_		
Policies				Ne		OK	Cancel					
Interfaces							Galicer					
Addresses												
Services												
VoIP	-											
Local Services	-											
Maintenance	-											

Troubleshooting von Firewallregeln

Beim Setzen von Firewallregeln können Fehler vermieden werden, wenn strukturiert vorgegangen wird. Dazu einige Grundsätze:

- Eine Firewall schränkt Verbindungen ein. Bevor eine Firewall eingerichtet wird, muss getestet werden, ob alle Verbindungen funktionieren. Erst wenn dies gewährleistet ist, macht das Einschalten der Firewall Sinn. Für das Troubleshooting bei nicht funktionierenden Verbindungen kann man die Firewall vorübergehend wieder abschalten.
- Zunächst sollte man eine Regel für den weiteren administrativen Zugriff auf den Router setzen oder sich vergewissern, dass diese Regel automatisch gesetzt wird. Ansonsten sperrt man sich selbst aus und kann die Konfiguration des Routers wieder von vorn beginnen.
- Häufig werden Regeln für "Hilfsdienste" (z. B. DHCP, DNS) vergessen. Diese können nur funktionieren, wenn die entsprechenden Server erreichbar sind.
- Wenn man beim Setzen einer Firewallregel nicht weiterkommt, hilft es, wenn man eine Regel zunächst sehr allgemein definiert und diese anschließend zunehmend verfeinert:

Die nachfolgende Regel würde beispielsweise alles erlauben:

Quelle	Ziel	Dienst	Aktion
Any	any	any	Access

Anschließend kann man Quelle, Ziel und Dienst weiter spezifizieren.

Grundlagen	der	Schulvernetzung

Ihre Notizen



LABORÜBUNG 10 - INSTALLATION DER AMTLICHEN SCHULVERWALTUNG (ASV)

Szenario

Das Programm zur amtlichen Schulverwaltung soll in einer Client-/Server-Installation (Mehrplatzinstallation) für mehrere Client-Computer installiert und eingerichtet werden (eine Serverinstallation, mehrere Clientinstallationen).



Aufgaben

- 1. Prüfen Sie, ob am Server und an den Clients die richtige Java-Version installiert ist. Installieren Sie gegebenenfalls die korrekte Java-Runtime-Version (JRE). Deaktivieren Sie die automatischen Java-Updates, damit die Version erhalten bleibt.
- 2. Installieren Sie am Server die korrekte Version von PostgreSQL.
- 3. Installieren Sie das Servermodul (DSS) von ASV auf einen Windows- oder Linux-Computer.
- 4. Installieren Sie das Clientmodul von ASV (ASV-Client) auf mehreren Windows-Computern und testen Sie den Zugriff auf den ASV-Server.
- 5. Überprüfen Sie, ob die Anmeldung an ASV funktioniert. (Anmeldung als Systemadministrator sys (Kennwort: !!ASV!!).
- 6. Erstellen Sie eine Sicherung der ASV-Datenbank. Legen Sie eine neue Datenbank an und spielen Sie die Sicherung dorthin zurück. Sorgen Sie dafür, dass ASV die neue Datenbank verwendet.

Ihre Notizen



HINWEISE

Begrifflichkeiten zu ASV

- ASD Amtliche Schuldaten (Auswertungswerkzeug für die Schulaufsicht)
- ASV Amtliche Schulverwaltung (Datenverwaltung und Auswertungen an den Schulen)
- ISB Ideen Software Branchenwissen (Unternehmen, das die Erstellung von ASV übernommen hat) – nicht zu verwechseln mit dem Staatsinstitut für Schulqualität und Bildungsforschung
- JRE Java Runtime Environment Laufzeitumgebung für ASV
- RZ Rechenzentrum
- ZSS Zentraler ASV-Server am RZ Süd
- DSS Dezentraler ASV-Server bei Client-/Serverinstallation an einer Schule oder auch regional-zentrale Installation

Installationsvarianten von ASV

• Einzelplatz

Alle ASV-Komponenten (Datenbank, DSS, Client) werden auf einem Computer installiert. Da bei dieser Installation nur eine einfache Datenbank (Derby-Datenbank) verwendet wird, ist diese Installation nicht erweiterbar. Es ist nicht möglich, dass ein weiterer Client auf ASV zugreift.

Mehrplatzinstallation

ASV-Server (DSS) und ASV-Client sollen auf verschiedenen Computern installiert werden. Es können mehrere ASV-Clients auf den Server zugreifen. Als Datenbank wird Postgres verwendet.

• "Geteilter Arbeitsplatz"

Dies entspricht der Mehrplatzinstallation. ASV-Server (DSS) und ASV-Client werden jedoch am gleichen Computer installiert. Bei Bedarf können weitere Clients auf ASV zugreifen.

Voraussetzungen für die ASV-Installation

Server:

- Java Runtime Environment (Version 1.6 Update 24)
- PostgreSQL (Version 8)

Client bzw. Einzelplatz:

• Java Runtime Environment (Version 1.6, Update 24)

- 🗆 ×

*

JAVA RUNTIME ENVIRONMENT

Überprüfung der installierten Version

Mit dem Befehl java -version kann die Installation von Java überprüft werden. Veraltete oder nicht kompatible Java-Installationen sollten ggf. entfernt werden (Systemsteuerung – Software).

C:\Windows\system32\cmd.exe

```
C:\Users\gs>java -version
java version "1.6.0_24"
Java(TM) SE Runtime Environment (build 1.6.0_24-b07)
Java HotSpot(TM) 64-Bit Server VM (build 19.1-b02, mixed mode)
C:\Users\gs}_
```

Installation der JRE

Die beiden neuesten Updates 25 und 26 der Version 1.6 bereiten Probleme in Verbindung mit ASV. Aktuell (Stand Juli 2011) sollte unbedingt Update 24 verwendet werden.

Download älterer JRE-Versionen: http://www.oracle.com/technetwork/java/archive-139210.html

Deaktivieren automatischer Updates

Automatische Aktualisierungen von Java sollten ggf. deaktiviert werden (Systemsteuerung – Programme). Je nach Java-Version kann sich das Menü unterscheiden.

🍝 Java Co	ntrol Panel					
Allgemein	Aktualisierung Java Sicherheit Erweitert					
Benachrie	htigung über Aktualisierungen					
S.	Java-Update gewährleistet, dass Sie stets über die neueste Version der Java-Plattform verfügen. Mit den nachfolgenden Optionen können Sie festlegen, wie Aktualisierungen abgerufen und angewendet werden.					
	Benachrichtigung ausgeben: Vor dem Herunterladen 💌					
	Automatisch nach Aktualisierungen suchen Erweitert					
	Klicken Sie unten auf "Jetzt aktualisieren", um die Suche nach Aktualisierungen zu starten. Wenn eine Aktualisierung verfügbar ist, wird in der Taskleiste ein Symbol eingeblendet. Den Status der Aktualisierung sehen Sie, wenn Sie den Mauszeiger über das Symbol setzen.					
	Java-Update wurde zuletzt am 23.07.11 Jetzt aktualisieren um 02:42 ausgeführt.					
	OK Abbrechen An <u>w</u> enden					

🛓 Java Control Panel	_ 🗆 X
Allgemein Java Sicherheit Erweitert	
Einstellungen Debugging Java-Konsole Standard-Java für Browser Java-Plug-In Frstellung von Verkrüpfungen JNLP-Datei/MIME-Zuordnung Automatischer JRE-Download C Immer automatisch herunterladen C Benutzer fragen Nie automatisch herunterladen Sicherheit Diverses	
OK Abbrechen An	venden

POSTGRESQL

Der DSS-Server benötigt Zugriff auf eine Postgres-Datenbank. Diese kann auf dem DSS-Server selbst oder auf einem anderen Server installiert sein.

Derzeit wird die PostgreSQL-Version 8 empfohlen.

Download unter:

http://www.enterprisedb.com/products-services-training/pgdownload#windows

Installation von PostgreSQL unter Windows

Bei der Installation wird folgendes abgefragt:

- Passwort für den Superuser postgres
- Port für die Datenkommunikation (Standard: 5432)

Test ob PostgreSQL läuft

Mit dem Befehl netstat kann man überprüfen, ob ein bestimmter Port geöffnet ist, d. h. ob es eine Anwendung gibt, die auf diesem Port lauscht.

• netstat -a | find "5432"

Das interaktive PostgreSQL-Terminalprogramm psql

PostgreSQL bietet zur Administration verschiedene Kommandozeilenbefehle oder das grafische Frontend pgAdmin. Zum Aufruf der Kommandozeilenbefehle muss man in das Verzeichnis bin der Postgres-Installation wechseln.

Aufruf von psql

```
psql
psql --help
psql -U postgres Datenbank Angabe des Benutzernamens und der Daten-
bank
```

Beispiele für interaktive Kommandos von psql

Die interaktiven Kommandos werden innerhalb des Programms psql aufgerufen

\h	Hilfe f
\?	Hilfe f
\1	Auflist
\c Datenbank	Wech
<pre>select version();</pre>	Anzei
create database Datenbank;	Anleg
drop database Datenbank;	Lösche
/d	Beend

Hilfe für SQL-Kommandos Hilfe für interne psql-Befehle Auflisten aller Datenbanken Wechsel zur angegebenen Datenbank Anzeige der Postgres-Version Anlegen einer neuen Datenbank Löschen einer Datenbank Beenden von psql

Dienstprogramme für PostgreSQL

Dienstprogramme sind ausführbare Dateien (exe-Dateien), mit denen grundlegende Funktionen aufgerufen werden können. Gegebenenfalls muss vorher in das Postgres-Verzeichnis gewechselt werden oder es muss ein Pfad gesetzt werden.

createdb.exe Datenbank	Anlegen einer neuen Datenbank
dropdb.exe Datenbank	Löschen einer Datenbank
pg_dump.exe Datenbank > Datei	Ein Datenbankauszug (dump) wird erzeugt
pg_dumpall.exe > <i>Datei</i>	Alle Datenbanken sichern
psql.exe Datenbank < Datei	Ein Datenbankauszug (dump) wird in eine
	(neue) Datenbank eingelesen. Die Datenbank
	muss vorher angelegt werden.

Optionen beim Aufruf von Dienstprogrammen

Ähnlich wie beim Aufruf von psql stehen auch für die anderen Dienstprogramme die üblichen Optionen zur Verfügung.

```
--help
-U Benutzername
-h host
-p port
```

Das graphische Datenbank-Frontend pgAdmin

🕼 pgAdmin III		_ 🗆 X
Datei Bearbeiten Plugins Anzeigen Werk	zeuge <u>H</u> ilfe	
🔌 🤁 🗰 🎭 🐨 🛛	Y 📰 🛃 🌽 🔯 • 🗣 💡	
Objektbrowser X	Eigenschaften Statistiken Abhängigkeiten Abhängige	
Server (1)	Datenbank Eigentümer Kommentar	
□ □	asv asv asv10 asv postgres postgres	Þ
	SQL-Feld	×
	▲	

Über das graphische Datenbankfrontend pgAdmin lassen sich alle administrativen Aufgaben zur Pflege der Postgres-Datenbank erledigen. Nachteilig im Vergleich zur Kommandozeile ist, dass die einzelnen administrativen Schritte nicht skripiert werden können.

Dokumentationen zu PostgreSQL

http://www.postgresql.org/docs/ http://www.postgresql.org/docs/books/pghandbuch.html.de

INSTALLATION DES ASV-SERVERS (DSS)

👫 IzPack - Instal	llation von ASV	<u>- </u>
ASV	Installationsart Einzelplatz Mehrplatz-Server Mehrplatz-Client Geteilter Arbeitsplatz Heimarbeitsplatz Zertifikat-Installation	
(Erstellt mit IzPaci	k - http://izpaok.org/) 🔶 Zurück 🕼 Weiter 🔇 Be	enden

PostgreSQL-Verbindungsdaten

Kennung:	postgres	Postgres-Benutzer mit administrativen Rechten
Passwort:	* * * *	
Host:	localhost	localhost bzw. IP-Adresse des Postgres-Servers
Port:	5432	Port, auf den der Postgres-Server hört
Initiale Datenbank:	postgres	Verwaltungsdatenbank von Postgres
ASV-Datenbank:	asv	Name der neu anzulegenden ASV-Datenbank

Zielverzeichnis

Zielverzeichnis: C:\ASV\Server

Beim vorgeschlagenen Installationsverzeichnis (C:\ASV) sollte man ein eindeutiges Verzeichnis für den ASV-Server wählen. Dies verhindert mögliche Konflikte bei einer eventuellen späteren Clientinstallation.

Installationsinformationen

Am Ende der Installation wird die Datei install-info.txt angezeigt, die zusammengefasst die Zugriffsinformationen enthält.

```
INSTALL_TYPE=SERVER
postgreHost=localhost
postgrePort=5432
postgrePassword=12345
postgreUsername=postgres
INSTALL_PATH=c:\ASV\Server
DSSpath=10.36.13.246:8765
```

Serverkonfigurationsdatei Config.ini

Die Serverkonfiguration ist in der Datei configuration\config.ini unterhalb des ASV-Verzeichnisses gespeichert. In dieser Datei findet man auch den Verbindungseintrag zur Postgres-Datenbank.

app.db.pass=asv
app.db.user=asv
app.db.path=10.36.13.246:5432/asv

INSTALLATION DES ASV-CLIENT

💦 IzPack - Insta	Ilation von ASV	_ 🗆 🗙
ASV	 Installationsart Einzelplatz Mehrplatz-Server Mehrplatz-Client Geteilter Arbeitsplatz Heimarbeitsplatz Zertifikat-Installation 	
(Erstellt mit IzPac	sk - http://izpack.org/)	Beenden

DSS-Verbindungsdaten

DSS Adresse: 10.36.13.246:8765 IP-Adresse und Port des DSS-Servers

Zielverzeichnis

Zielverzeichnis: C:\ASV\Client

Als Installationsverzeichnis wird C:\ASV vorgeschlagen. Um mögliche Konflikte mit einer Serverinstallation zu vermeiden, sollte ein eindeutiges Verzeichnis für den ASV-Client gewählt werden.

Installationsinformationen

Am Ende der Installation wird die Datei install-info.txt angezeigt, die zusammengefasst die Zugriffsinformationen enthält.

```
INSTALL_TYPE=CLIENT
INSTALL_PATH=c:\ASV\Client
DSSpath=10.36.13.246:8765
```



Clientkonfigurationsdatei config.ini

Die Clientkonfiguration ist in der Datei configuration\config.ini unterhalb des ASV-Verzeichnisses gespeichert. In dieser Datei findet man auch den Verbindungseintrag zum DSS-Server.

```
#DSS
server.url=http://10.36.13.246:8765/svp
```

ERSTE SCHRITTE IN ASV

Benutzertypen in ASV

Systemadministrator	Der Systemadministrator "sys" verwaltet die Schulen und legt Administratoren für die Schulen an.
Administrator	Der Administrator wird bei der Neuanlage einer Schule erzeugt und legt Benutzer für die Schule an.
Benutzer	Einem Benutzer können Rollen hinzugefügt werden, aus denen sich die Benutzerrechte ergeben.

Erste Anmeldung bei ASV

Die erste Anmeldung erfolgt als Systemadministrator "sys" mit dem Standardpasswort !!ASV!!.

🔊 ASV Anmeldung	
Willko	mmen bei ASV
	(Client) Aktuallar Datum, 05.08.2011
Benutzerkennung	sys
Passwort	******
	Anmelden Abbrechen

Dokumentation zum Amtlichen Schulverwaltungsprogramm ASV: <u>http://www.asv.bayern.de</u>

ANHANG: FIREWALLEINSTELLUNGEN UND FREIGABEN UNTER WINDOWS 7

NETZWERKSTANDORTE UNTER WINDOWS 7

Windows 7 bietet als Grundeinstellung vier verschiedene Netzwerkstandorte (Netzwerkadressen) an:

- Heimnetzwerk
- Arbeitsplatznetzwerk
- Öffentliches Netzwerk
- Domäne

Die Netzwerkstandorte unterscheiden sich im Wesentlichen durch vordefinierte Firewall-Einstellungen. Bei einem öffentlichen Netzwerk sind die Firewall-Einstellungen sehr restriktiv eingestellt, so dass der Computer auf das Internet zugreifen kann, jedoch selbst nichts freigibt.

Computer, die Mitglied in einer Domäne sind, werden automatisch dem Netzwerkstandort "Domäne" zugeordnet. Für andere Computer kann man den Netzwerkstandort (Netzwerkadresse) selbst festlegen.

Festlegen des Netzwerkstandortes

Systemsteuerung – Netzwerk und Internet – Netzwerk- und Freigabecenter



Windows 7 speichert den einmal gewählten Netzwerkstandort für das jeweilige Netzwerk ab. Als Kriterium verwendet Windows 7 die MAC-Adresse des zugewiesenen Standardgateways. In Netzwerken ohne Standardgateway führt dies dazu, dass diese Netze immer als öffentliche Netze betrachtet werden und der Netzwerkstandort auf dem üblichen Weg nicht geändert werden kann. Als einfacher Ausweg bietet sich an, auch in einem Netzwerk ohne Verbindung zum Internet, einen beliebigen anderen Computer als Standardgateway einzutragen.

In der Registry sind die Netzwerkstandorte unter HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows\CurrentVersion\HomeGroup\NetworkLocations gespeichert.

FIREWALL-EINSTELLUNGEN UNTER WINDOWS 7

Die Firewall-Einstellungen können bei Windows 7 sehr differenziert vorgenommen werden. Bei einem Verbindungstest schaltet man üblicherweise die gesamte Firewall für den jeweiligen Bereich (privates oder öffentliches Netz) vorübergehend aus. Nach der Testphase definiert man in den erweiterten Firewall-Einstellungen eine neue Regel oder aktiviert eine vorhandene Regel.



Windows-Firewall mit e	erweiterter Sicherheit					<u> </u>
Datei Aktion Ansicht	2					
🗢 🔿 🖄 📅 🗟 🛛	2 🖬					
Windows-Firewall mit erw	Eingehende Regeln					Aktionen
Eingehende Regeln	Name	Gruppe 🔺	Profil	Aktiviert	Aktion 🔺	Eingehend 🔻
Verbindungssicherhei	Anmeldedienst (NP eingehend)	Anmeldedienst	Alle	Nein	Zulassen	
T I I Uberwachung	BranchCache - Gehosteter Cacheserver (HT	BranchCache	Alle	Nein	Zulassen	Datei- und 🔺
	BranchCache - Inhaltsabruf (HTTP eingehend)	BranchCache	Alle	Nein	Zulassen	🕢 Regel
	BranchCache - Peerermittlung (WSD eingehe	BranchCache	Alle	Nein	Zulassen	Ausse.
	Computernamen-Registrierungsdienst von	Computernam	Alle	Nein	Zulassen	Ausse
	Computernamen-Registrierungsdienst von	Computernam	Alle	Nein	Zulassen	E Kopieren
	Datei- und Druckerfreigabe (Echoanforderun	Datei- und Dr	Privat, Öffentlich	Ja	Zulassen	🔀 Löschen
	Datei- und Druckerfreigabe (Echoanforderun	Datei- und Dr	Domäne	Nein	Zulassen	
	Datei- und Druckerfreigabe (Echoanforderun	Datei- und Dr	Privat, Öffentlich	Nein	Zulassen	Eigens
	Datei- und Druckerfreigabe (Echoanforderun	Datei- und Dr	Domäne	Nein	Zulassen	🛛 🛛 Hilfe
	Datei- und Druckerfreigabe (LLMNR-UDP ein	Datei- und Dr	Alle	Nein	Zulassen	-
	Datei- und Druckerfreigabe (NB-Datagramm	Datei- und Dr	Privat, Öffentlich	Nein	Zulassen	
	Datei- und Druckerfreigabe (NB-Datagramm	Datei- und Dr	Domäne	Nein	Zulassen	
	Datei- und Druckerfreigabe (NB-Name einge	Datei- und Dr	Domäne	Nein	Zulassen	
	Datei- und Druckerfreigabe (NB-Name einge	Datei- und Dr	Privat, Offentlich	Nein	Zulassen 💌	
						J

EINFACHE DATEIFREIGABE UNTER WINDOWS 7

Vorbereitungen zur "Einfachen Dateifreigabe"

Für eine "Einfache Dateifreigabe" kann der Freigabeassistent genutzt werden. Im Windows-Explorer unter Extras – Ordneroptionen – Ansicht kann der Freigabeassistent ein- oder ausgeschaltet werden. Standardmäßig ist der Freigabeassistent eingeschaltet.



In der Systemsteuerung unter Netzwerk und Internet – Netzwerk- und Freigabecenter – Erweiterte Freigabeeinstellungen wird das kennwortgeschützte Freigeben ausgeschaltet. Dadurch wird automatisch auch das Gastkonto aktiviert (siehe Computerverwaltung – Lokale Benutzer und Gruppen).

Grundlagen der Schulvernetzung

😵 Erweiterte Freigabeeinstellungen	
😋 🕞 🗸 Netzwerk- und Freigabecenter 🔹 Erweiterte Freigabeeinstellungen 🔹 😰 Systemsteuerung durchsuchen	<u> </u>
Kennwortgeschütztes Freigeben	1
Heimnetzgruppen-Verbindungen Normalerweise werden die Verbindungen mit anderen Computern der Heimnetzgruppe unter Windows verwaltet. Wenn Sie jedoch an allen Computern dieselben Benutzerkonten und Kennwörter verwenden, können Sie veranlassen, dass für die Heimnetzgruppe stattdessen Ihr Konto verwendet wird. <u>Entscheidungshilfe</u>	•
Abbrechen	

Erstellen einer "Einfachen Dateifreigabe"

🏝 Lokaler Datenträger (C:)				_	
Computer	r 🔻 Lokaler Datenträger (C:) 👻	▼ 100	Lokaler Datenträger (C:)) durchsuchen	2
Organisieren 👻 词 Öffner	n In Bibliothek aufnehmen 🔻 Freigeben für 🔻	Neuer Ordner		··· ·	(?)
🔆 Favoriten	Name ^	Änderungsdatum	Тур	Größe	
🧮 Desktop	🐌 Benutzer	21.10.2010 16:09	Dateiordner		
📜 Downloads	🔑 PerfLogs	14.07.2009 05:20	Dateiordner		
🔠 Zuletzt besucht	📙 Programme	21.10.2010 15:49	Dateiordner		
	🌗 Programme (x86)	14.07.2009 06:57	Dateiordner		
Bibliotheken	ili Windows	21.10.2010 16:07	Dateiordner		
Dokumente	Daten Öffnen In neuem Fenster öffnen	06.2011 13:02	Dateiordner		
J Musik	Freigeben für Vorgängerversionen wiederherst In Bibliothek aufnehmen	Niemand ellen Heimnetzgruppe	e (Lesen) e (Lesen/Schreiben)		
🖳 Computer	Senden an	Bestimmte Perc	open		
辑 Netzwerk	Ausschneiden Kopieren	Desumine Pers			
	Verknüpfung erstellen Löschen				
Daten Ände Dateiordner	erungsdatum: 1 Umbenennen Eigenschaften				

👩 Da	teifreigabe	
\bigcirc	🔉 Dateifreigabe	
	Personen für die Freigabe auswählen Geben Sie einen Namen ein, und klicken Sie dann auf "Hinzufü nach Personen zu suchen.	igen", oder klicken Sie auf den Pfeil, um
		▼ <u>H</u> inzufügen
	Name	Berechtigungsebene
	💈 Gast	Lesen/Schreiben 🔻
	🙎 gs	Besitzer
	Ich habe Probleme beim Freigeben	
		<u>F</u> reigabe Abbrechen

Im Freigabeassistenten wird der Benutzer "Gast" ausgewählt und diesem die entsprechenden Rechte gewährt.

Überprüfen der Freigaben und aktiven Verbindungen

In der Computerverwaltung lassen sich die Freigaben und aktiven Verbindungen kontrollieren.

🛃 Computerverwaltung								×
<u>D</u> atei Ak <u>t</u> ion <u>A</u> nsicht <u>?</u>								
🗢 🔿 🖄 🖬 🧕 🖬 🚺								
E Computerverwaltung (Lokal)	Benutzer 🔺	Computer	Тур	Anzahl der	Verbindungszeit	Leerlaufze	Aktionen	
 □ [™] [™]	Gast	SCHULNE	Windows	3	00:12:59	00:01:58	Sitzungen	•
							Weitere Aktionen	
👸 Freigaben 😥 Sitzungen								
i Geöffnete Dateien ⊕ 🌆 Lokale Benutzer und Gruppen								
 Datenspeicher Datenträgerverwaltung 								
🕀 📷 Dienste und Anwendungen								
	•					F		

EINFACHE DATEIFREIGABE UNTER WINDOWS XP

Vorbereitungen zur "Einfachen Dateifreigabe"

Die "Einfache Dateifreigabe" kann im Windows-Explorer unter Extras – Ordneroptionen – Ansicht ein- oder ausgeschaltet werden. Standardmäßig ist die "Einfache Dateifreigabe" eingeschaltet.

Für Computer, die in eine Domäne eingebunden sind, ist die Option "Einfache Dateifreigabe" nicht verfügbar.

Ordneroptionen
Allgemein Ansicht Dateitypen Offlinedateien
Ordneransicht Sie können die Ansicht (z. B. Details oder Kacheln), die Sie für diesen Ordner verwenden, für alle Ordner übernehmen. Für glie übernehmen Alle zurücksetzen
Erweiterte Einstellungen:
Dateien und Ordner Ansichtoptionen für jeden Ordner speichem Ansichtoptionen für jeden Ordner speichem Automatisch nach Netzwerkordnem und Druckem suchen Dateigrößeinformationen in Ordnertipps anzeigen Firfache Dateifreigabe verwenden (empfohlen) Einfache Dateifreigabe verwenden (empfohlen) Einfache Ordnerasicht in der Ordnerliste des Explorers anzeige Erweiterungen bei bekannten Dateitypen ausblenden Geschützte Systemdateien ausblenden (empfohlen) Inhalte von Systemordnem anzeigen Miniaturansichten nicht zwischenspeichem Ordneffenster in einem eigenen Prozess starten
<u>Wi</u> ederherstellen
OK Abbrechen Ü <u>b</u> emehmen

Erstellen einer "Einfachen Dateifreigabe"

Beim ersten Versuch, eine Freigabe zu erstellen, bietet Windows XP einen Assistenten an, der jedoch eine Freigabe nur für die "Gemeinsamen Dokumente" erstellt. Dieser Assistent sollte ignoriert werden.

Eigenschaften von Daten	<u>? × </u>
Allgemein Freigabe Anpassen	
Kicken Sie auf diesen Ordner, un den Ordner <u>Gemeinsame Dokum</u> Benutzer dieses Computers freizu Aktivieren Sie folgendes Kontrolli Ordner und untergeordnete Ordn ☐ Diesen Ordner nicht freigebe Netzwerkfreigabe und sicherheit Aus Sicherheitsgründen wurde d diesem Computer deaktiviert. Sie Netzwerkinstallations-Assistent v Remotezugriff und die Dateifreigz aktivieren.	Dateifreigabe aktivieren Falls die Dateifreigabe auf diesem Computer ohne Verwendung des Netzwerkinstallations-Assistenten aktiviert wird, kann der Computer möglicherweise nicht vor Angriffen aus dem Internet geschützt werden. Daher wird strengsteins empfohlen, dass der Netzwerkinstallations-Assistent ausgeführt wird. C Assistent zum Aktivieren der Dateifreigabe verwenden (empfohlen) OK Abbrechen
Klicken Sie hier, wenn Sie sich des Sicherheitsrisikos. bewusst sind, aber Dateien dennoch freideben möchten, ohne den Assistenten auszuführen. Weitere Informationen über Freidabe und Sicherheit. OK Abbrechen Übernehmen	

Wurde der Assistent ignoriert, erhält man zukünftig nur noch das nachfolgende Fenster, mit dem man Ordner im Netzwerk freigeben und auch auswählen kann, ob die Benutzer nur Lese- oder Lese/Schreibrechte erhalten sollen.



SCHULNETZ-AUSSTATTUNG FÜR LABORÜBUNGEN

Zur Durchführung der SCHULNETZ-Laborübungen steht neben den Computern und Notebooks der Schulen folgende Ausstattung zur Verfügung:

- Switch (HP ProCurve 1410, nicht managebar)
- Router (bintec RS120)
- Access-Point (bintec W1002N)
- NAS-Server QNAP TS-459

Weitere Konfigurationbeispiele für die bintec-Router und Access-Points werden von Funkwerk im Internet angeboten:

http://www.funkwerk-ec.com Download – Router – RS-Serie bzw. Download – Wireless LAN – W1002N