

Laborauftrag_Raspberry-Ntopng-Traffic Server - 10.02.2025

Dieses Dokument zeigt eine Mitschrift zur Ausarbeitung eines Arbeitsauftrage/Laborauftrages im Unterrichtsfach **Betriebssysteme & Labor**.

Inhalt

1. Geräteübersicht	1
1.1 Benutzereinstellungen (Software)	1
2. Arbeitsziel.....	2
3. Installation.....	2
4. Erstinbetriebnahme	3
4.1 Zugriff über PuTTY.....	4
5. Installation Ntopng.....	4
5.1 Zugriff per Browser	5
5.2 RPI Monitor installieren	6
5.2.1 Bedeutung	6
5.2.2 Anwendung	6
5.3 IP-Adresse von DHCP auf „statisch“ ändern	7

1. Geräteübersicht

	Geräte	VM	Hypervisor	Betriebssystem	IP-Adresse (LAN)
1	LENOVO E16	nein	physisch	WIN11	192.168.1.134
2	Raspberry 400	Nein	Physisch		192.168.1.15
3					

1.1 Benutzereinstellungen (Software)

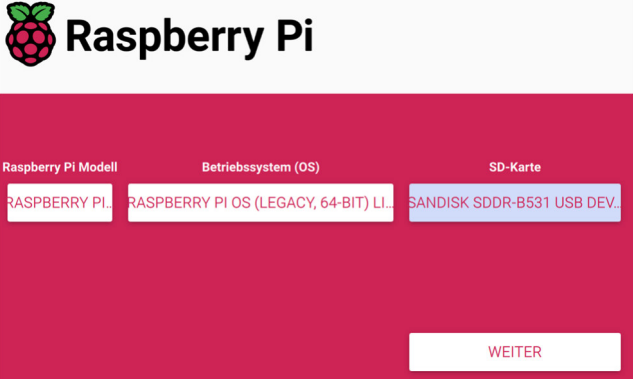
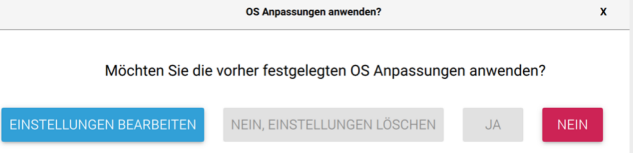
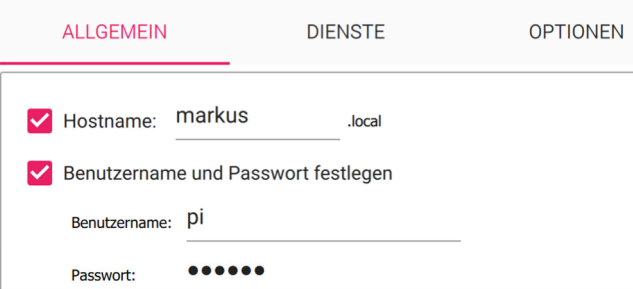
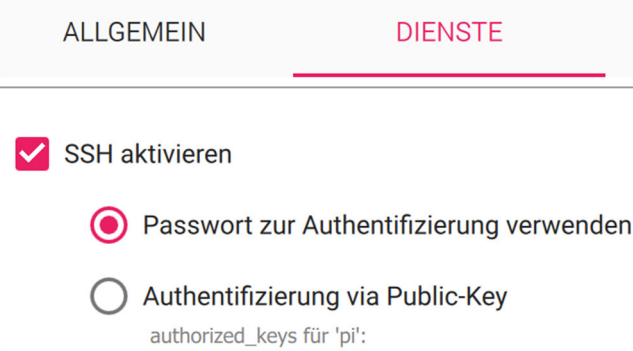
User-PC	Anwendung	Benutzername	Passwort	Gerätename	domain (AD)
	OS „Linux“	pi	123456	markus	---

2. Arbeitsziel

Installation und Konfiguration einer Software zur Visualisierung von Network-Traffic.

3. Installation

Zur Installation der folgenden Schritte wurde „Raspberry PI Imager“ verwendet.

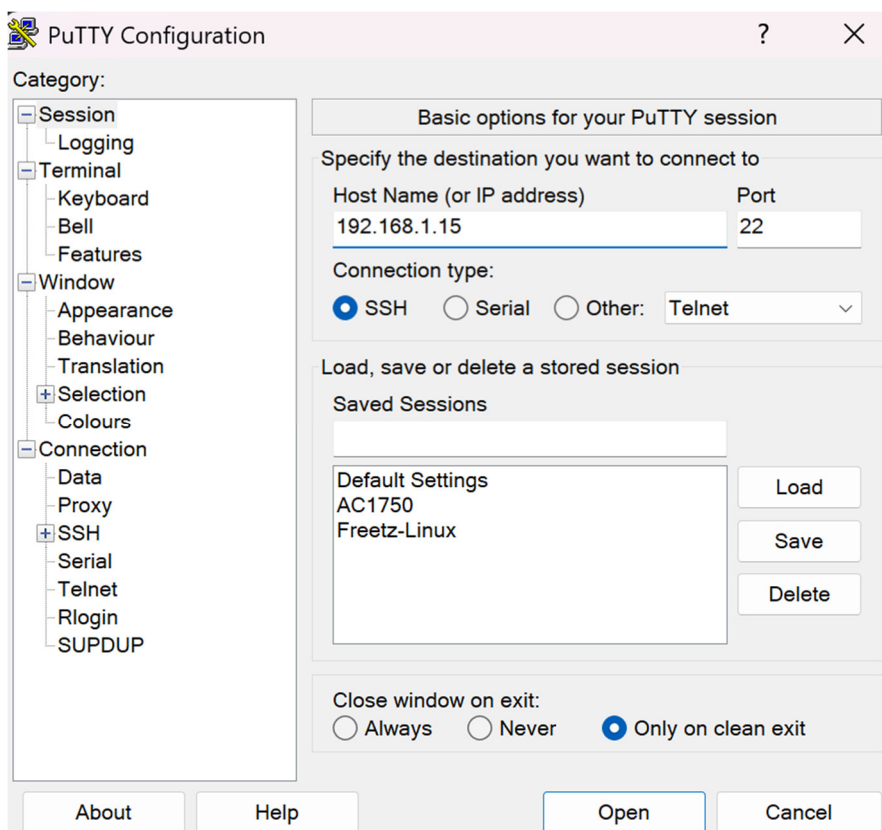
Erklärung	Beispiel
Auswahl eines geeigneten Betriebssystems	 Raspberry Pi OS (Legacy, 64-bit) Lite A port of Debian Bullseye with security updates and no desktop environment Veröffentlicht: 2024-10-22 Online - 0.3 GB Download
Auswahl - PI-Modell - Betriebssystem - Datenträger	 Raspberry Pi Imager interface showing the selection of the Raspberry Pi model, the operating system (Raspberry Pi OS (Legacy, 64-bit) Lite), and the SD card (SANDISK SDDR-B531 USB DEV.). The 'WEITER' button is visible.
Einstellungen bearbeiten	 OS Anpassungen anwenden? x Möchten Sie die vorher festgelegten OS Anpassungen anwenden? EINSTELLUNGEN BEARBEITEN NEIN, EINSTELLUNGEN LÖSCHEN JA NEIN
Unter „Allgemein“ Eingabe des Hostnames Festlegen von Benutzernamen & Passwort	 ALLGEMEIN DIENSTE OPTIONEN ☒ Hostname: markus.local ☒ Benutzernamen und Passwort festlegen Benutzername: pi Passwort: ●●●●●●
Unter „Dienste“ Aktivierung von SSH	 ALLGEMEIN DIENSTE ☒ SSH aktivieren ☒ Passwort zur Authentifizierung verwenden ☐ Authentifizierung via Public-Key authorized_keys für 'pi':

Bestätigung des Schreibvorganges mit JA	Alle vorhandenen Daten auf 'SanDisk SDDR-B531 USB Device' werden gelöscht. Möchten Sie wirklich fortfahren? NEIN JA
Wurde der Schreibvorgang beendet, kann die SD-Karte in den Raspi gesteckt und das System gestartet werden.	Raspberry Pi OS (Legacy, 64-bit) Lite wurde auf SanDisk SDDR-B531 USB Device geschrieben Sie können die SD-Karte nun aus dem Lesegerät entfernen WEITER

4. Erstinbetriebnahme

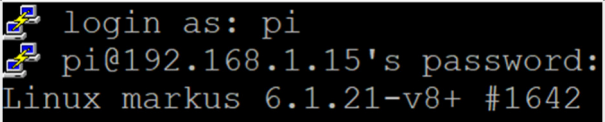
Über einen angeschlossenen Monitor wurde nach dem Login die IP-Adresse mittels Eingabe im Terminal „ifconfig“ festgestellt.

Der anschließende Zugriff erfolgte über eine SSH-Verbindung per Putty



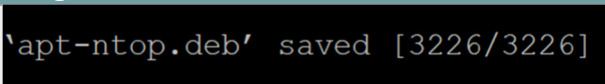
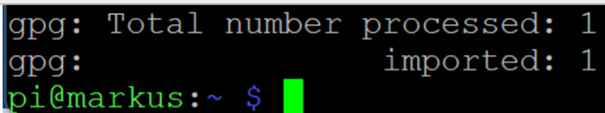
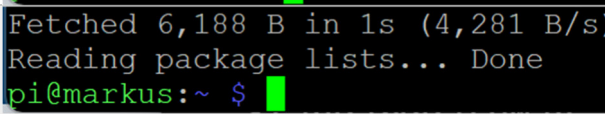
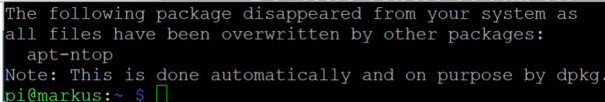
4.1 Zugriff über PuTTY

PuTTY ist ein weit verbreitetes, kostenloses und Open-Source-Terminalprogramm, das es ermöglicht, sich mit anderen Computern über Netzwerkverbindungen zu verbinden. Es wird hauptsächlich auf Windows-Systemen verwendet, kann aber auch auf Linux und macOS durch Zusatzsoftware installiert werden. PuTTY ist besonders nützlich für die Verbindung mit Linux-Servern oder -Geräten über SSH (Secure Shell) oder Telnet.

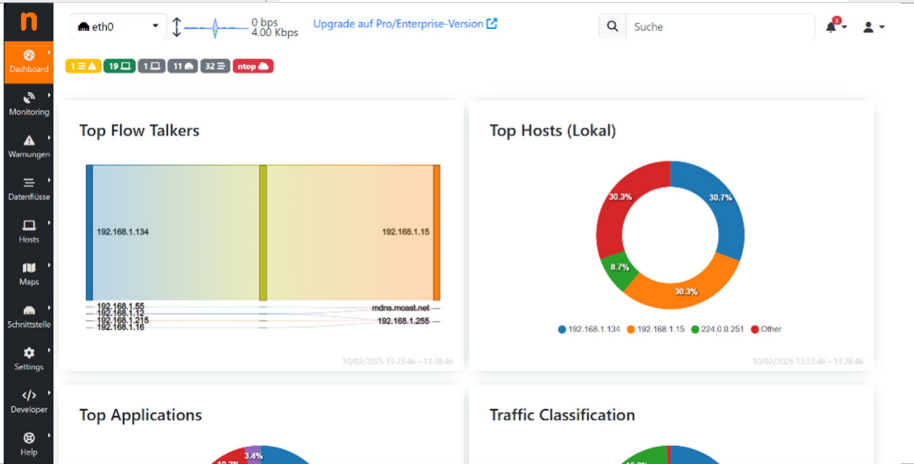
Login as: pi Password: 123456	
sudo apt-get update	Dieser Befehl aktualisiert die Paketlisten aus den konfigurierten Paketquellen.
sudo apt-get full-upgrade	Führt ein vollständiges Upgrade des Systems durch.
sudo reboot	Startet das System neu.
sudo ist notwendig, da nur der Administrator das System neu starten darf.	

5. Installation Ntopng

ntopng ist ein mächtiges Tool zur Netzwerküberwachung, das sowohl für kleine als auch große Netzwerke nützlich ist. Mit seiner einfachen Web-Oberfläche und tiefgehenden Analysefunktionen eignet es sich besonders für Administratoren und Sicherheitsexperten.

Syntax	Ausgabe
wget https://packages.ntop.org/RaspberryPI/apt-ntop.deb	
sudo dpkg -i apt-ntop.deb	
sudo apt-get update	
sudo apt-get install ntopng nprobe	

5.1 Zugriff per Browser

Aktion	Ergebnis
Zugriff per „OPERA-Browser“	⚠ Nicht sicher 192.168.1.15:3000/lua/login.lua Welcome to ntopng Username (default admin) Password (default admin) Login 🔒 Unable to login? User's Guides Community Support FAQ Code Contact Us © 1998-24 - ntop ntopng is released under GPLv3.
Benutzer: admin Passwort: admin	
neues Passwort: 123456 Änderung der Sprache auf Deutsch	Change Password Default admin password must be changed. Please enter a new password below. Password Confirm Password Language 🇩🇪 German ▼ Change Password
GUI von ntopng	

5.2 RPI Monitor installieren

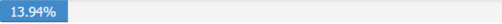
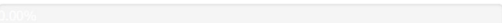
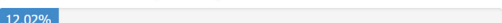
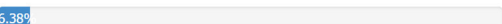
5.2.1 Bedeutung

- Bei RPI handelt es sich um eine Metrik, die die relative Bedeutung eines bestimmten Protokolls im Netzwerkverkehr bewertet.
- RPI wird als Prozentsatz angegeben und zeigt, welchen Anteil ein bestimmtes Protokoll am gesamten Netzwerkverkehr hat.
- Eine höhere RPI-Zahl bedeutet, dass das Protokoll im Vergleich zu anderen einen größeren Anteil am Datenverkehr hat.

5.2.2 Anwendung

- RPI hilft dabei, die wichtigsten Protokolle im Netzwerk zu identifizieren.
- Es kann verwendet werden, um ungewöhnlichen oder unerwarteten Datenverkehr zu erkennen.
- Netzwerkadministratoren nutzen RPI, um Bandbreitenverteilung und mögliche Anomalien zu analysieren.

Syntax	Erklärung
<code>sudo wget http://goo.gl/vewCLL -O /etc/apt/sources.list.d/rpimonitor.list</code>	versucht, eine Datei namens rpimonitor.list in das Verzeichnis /etc/apt/sources.list.d/ herunterzuladen.
<code>sudo apt-key adv --recv-keys --keyserver keyserver.ubuntu.com 2C0D3C0F</code>	versucht, einen GPG-Schlüssel mit der ID 2C0D3C0F vom Keyserver keyserver.ubuntu.com zu importieren.
<code>sudo apt-get update</code>	Dieser Befehl aktualisiert die Paketlisten auf deinem Raspberry Pi, damit er die neuesten Versionen der Software kennt.
<code>sudo apt-get install rpimonitor</code>	installiert den RPI Monitor
Nun kannst auf die Weboberfläche von RPI Monitor zugreifen, indem du im Browser die IP-Adresse deines Raspberry Pi mit Port 8888 aufrufst: 192.168.1.15:8888	

RPI-Monitor (markus) Status Statistics Addons Options About ▾	
 Version Processor: BCM2835 Distribution: Debian GNU/Linux 11 (bullseye) Kernel version: Linux 6.1.21-v8+ aarch64 Firmware: #1642 Package(s): Update needed... Execute <code>sudo /etc/init.d/rpimonitor update</code> to update this data. To add or remove automatic update of this data, execute <code>sudo /etc/init.d/rpimonitor install_auto_package_status_update</code> or <code>sudo /etc/init.d/rpimonitor remove_auto_package_status_update</code>.	 Memory Used: 529.01MB (13.94%) Available: 3.19GB Total: 3.71GB  13.94%
 Uptime Raspberry Pi time: 13:05:37 Uptime: 01 hour 23 minutes 55 seconds	 Swap Used: 0B (0.00%) Free: 100.00MB Total: 100.00MB  0.00%
 CPU Load Load Load	 SD card /boot Used: 30.64MB (12.02%) Free: 224.34MB Total: 254.99MB  12.02% / Used: 1.85GB (6.38%) Free: 27.12GB Total: 28.97GB  6.38%
<code>sudo /etc/init.d/rpimonitor update</code>	führt ein Update für RPI Monitor durch, wenn eine neue Version verfügbar ist. Er lädt die neuesten Updates herunter und installiert sie.
<code>sudo reboot</code>	führt einen Neustart deines Raspberry Pi durch.

5.3 IP-Adresse von DHCP auf „statisch“ ändern

Erneute Verbindung per PuTTY auf die IP-Adresse des Hosts.

1. Bearbeiten der Datei `/etc/dhcpd.conf`.
2. Konfigurieren der statische IP-Adresse, das Standard-Gateway und DNS-Server.
3. Speichern und starten des Netzwerkdienstes neu oder starten des Systems neu.

Eingabe	
<code>sudo nano /etc/dhcpd.conf</code>	Öffnen der Netzwerkkonfigurationsdatei in „Nano“
Scrolle durch die Datei und suche nach einem Abschnitt, der wie folgt aussieht:	<pre># Example static IP configuration: #interface eth0</pre>
Um eine statische IP-Adresse zu setzen, bearbeite den Abschnitt wie folgt:	
<pre># Example static IP configuration: #interface eth0 #static ip_address=192.168.1.15/24 #static ip6_address=fd51:42f8:caae:d92e::ff/64 #static routers=192.168.1.1 #static domain_name_servers=192.168.1.1 8.8.8.8 fd51:42f8:caae:d92e::1</pre>	

Nachdem du die Änderungen vorgenommen hast, speichere die Datei und beende den nano-Editor:	• Drücke Ctrl + X (zum Beenden). • Drücke Y (um die Änderungen zu speichern). • Drücke Enter, um die Datei zu speichern.
sudo service dhcpd restart oder sudo reboot	Nachdem du die Datei bearbeitet und gespeichert hast, musst du den Netzwerkdienst neu starten, damit die Änderungen wirksam werden.