Introduction to the CCN Lab:

In the following document you will find various links to topics that enable you to work with GNS3 and it will guide you step-by-step to GNS3 in more detail.

The lab is carried out in groups of 3 students each. To do this, use the "Lab > Groups" section in ILIAS as soon as it is activated. Your personal group folder contains the login details for your group's GNS3 instance.

Before your group acceptance sessions one member of your group needs to upload your solution of the according lab as a pdf and the working gns3.project file (both together in a zip file) in ILIAS under "Lab > Lab X > Lab X submission ".

GNS3 Installation:

The configurations, as described below, must be completely set up by you (installation, setup, VPN)!

The GNS3 **installation file** can be found in **ILIAS** in the "Lab > Introduction" folder. Make sure that ***version 2.2.34 of GNS3*** is required to work on the lab!

After you downloaded the installation file from ILIAS, you must rename it. (Remove the ending ".sec")

For all Mac users: Be sure to follow the instructions below, otherwise you will have problems working with GNS3!

The following links show the installation process, please make sure to use our installation file, NOT the one from gns3 website.

GNS3 Installation for Windows:
https://docs.gns3.com/docs/getting-started/installation/windows

GNS3 Installation for MacOS:
https://docs.gns3.com/docs/getting-started/installation/mac

GNS3 installation for Linux:

Visit the following link and add the repository according to the manual:

https://gatekeeper.informatik.fh-dortmund.de/personen/mitarbeiter/mernst/gns3/

```
After adding the repository run the following commands in your terminal to
install gns3

sudo apt-get update

sudo apt-cache madison gns3
```

> this will output the available version, please select here 2.2.34 (for example gns3-gui=2.2.34~focal1)

```
sudo apt-get install gns3-gui=2.2.34_XXXXX

sudo apt-mark hold gns3-gui
```

Access to the GNS3 server:

Important: VPN access is required*! (Unless you are at the campus and connected to FB4STUD.)*

GNS3 server data:

IP address: 172.22. XXX. XX

-> GNS3 server IP is available via the respective ILIAS group.

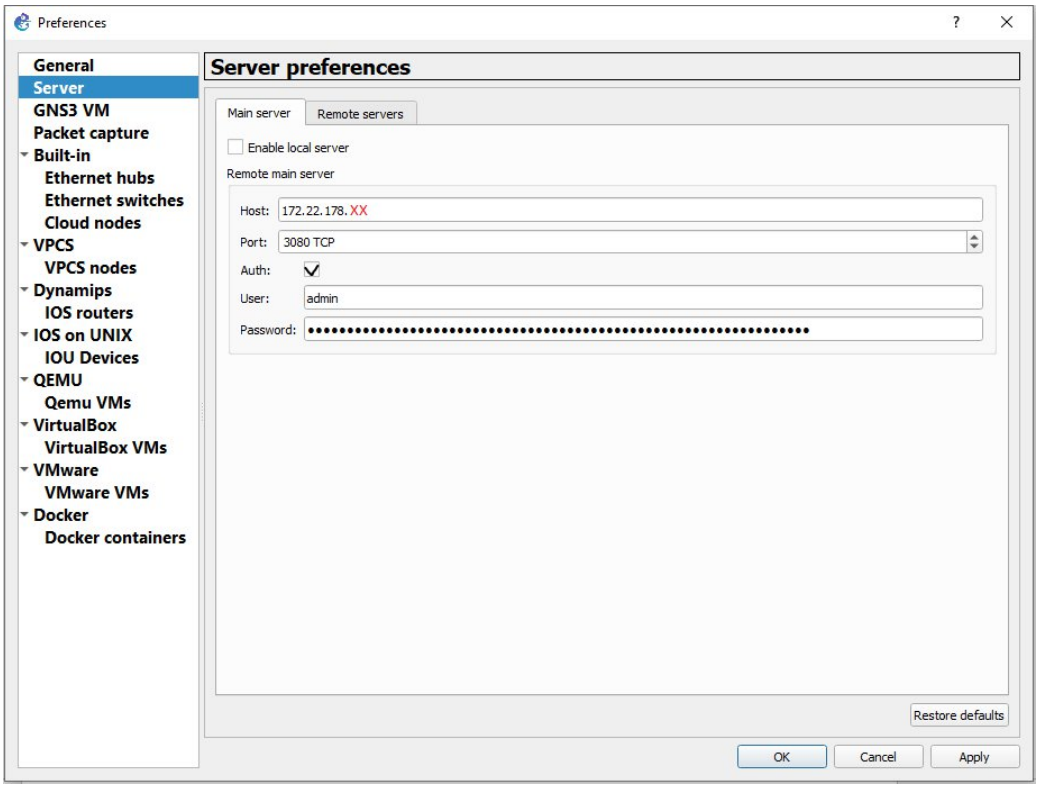
User: admin

Password: XXXX

-> Provided via the respective ILIAS group.

Attention: All participants of the group can see the steps of the other group members in real time!

To connect to the GNS3 server, you must enter the IP address and port 3080 as well as the password via Edit -> Preferences under the menu item “Server” in the tab “Main Server”. The box “Local Server” must **not** be checked.



To import the template project, you need for Lab1, download the template from "ILIAS > Lab > Introduction > ccnLab1template.gns3project". *(Again, you need to rename the file by removing the .sec)*

In GNS3 go to "File > Import portable project" and select the ccnLab1template.gns3project file.

VPN access:

To connect to the GNS3 server, VPN access is required.

Changes that need to be made from the official instructions:

VPN address: **vpn.inf.fh-dortmund.de** -> do not use vpngate.fh.dortmund.de!

Only for MacOS and Linux: Shared Secret: **fb4vpn** -> do not use FHDO!

VPN Instructions for Windows, MacOS, Linux:

Important: *Pay attention to changes from above!*

https://intranet.fh-dortmund.de/de/hs/hit/service/vpn/vpn-start.php

Introduction to GNS3:

Getting started with GNS3:

It is recommended that you take the first steps to familiarize yourself with the environment.

GNS3 User Interface:

https://docs.gns3.com/docs/using-gns3/beginners/the-gns3-gui

First GNS3 project:

https://docs.gns3.com/docs/getting-started/your-first-gns3-topology

Troubleshooting:

GNS3 installation issues:

https://docs.gns3.com/docs/troubleshooting-faq/troubleshoot-gns3

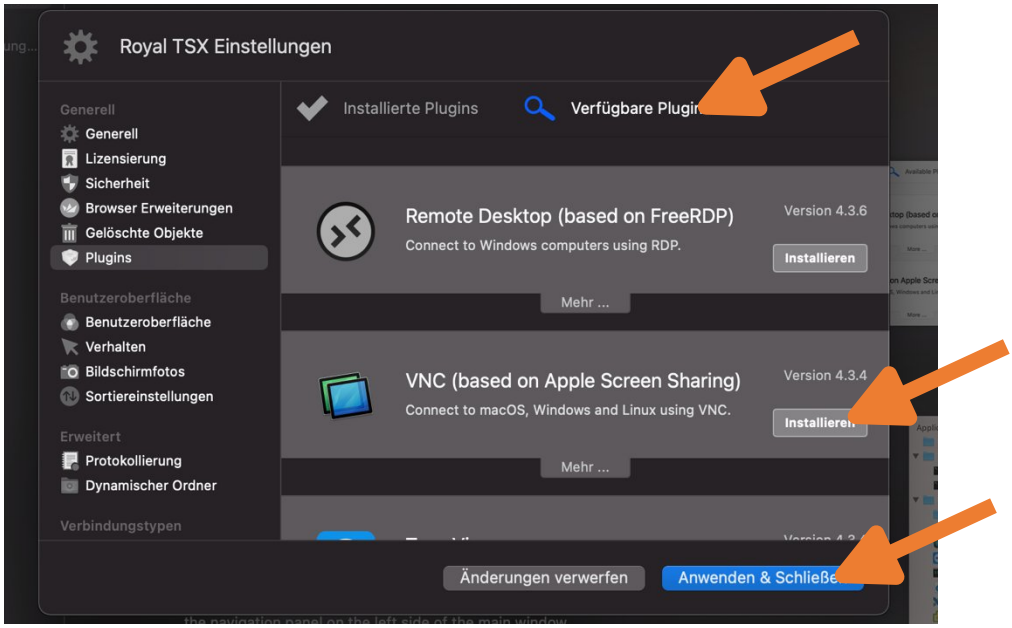
Troubleshooting Mac - Unable to connect to VNC on network devices

For certain versions of OSX or Mac with GNS3, there may be a problem establishing a remote desktop connection to the virtual devices on your GNS3 server.

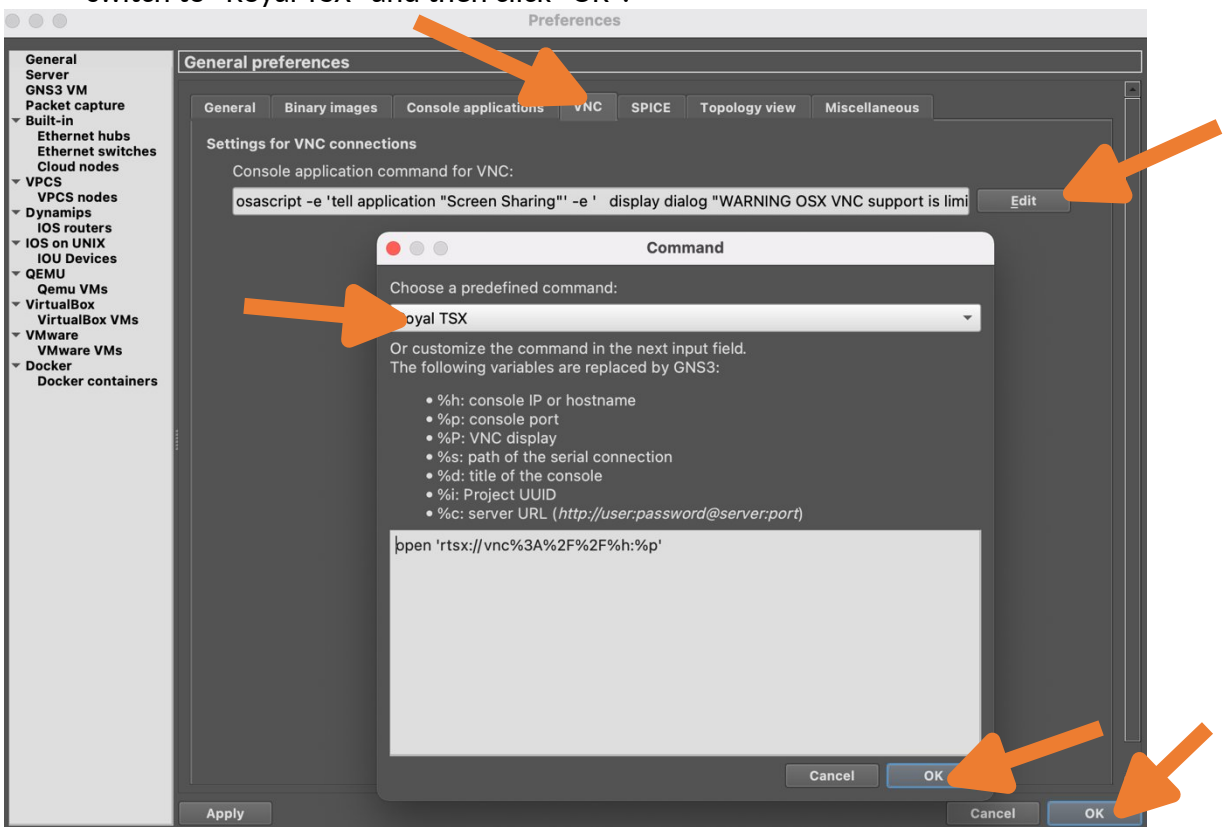
With GNS3, when you open a device's console, OSX's built-in VNC screen sharing is used by default and the following error appears:

If this is the case for you, you must install and configure an alternative VNC connection program:

1. Please install the program "Royal TSX" via https://royalapps.com/ts/mac/download
2. Start "Royal TSX" (you can skip personal information etc. by clicking on "Continue", these are not required) and select "Plugins" in the settings. Install the plugin "VNC (based on Apple Screen Sharing)" under "Available Plugins" and then restart Royal TSX or click on "Apply & Close":



3. In the GNS3 settings, in the "General" section under the "VNC" tab, click on "Edit" to switch to "Royal TSX" and then click "OK":



4. Now try to open the console on a host with a right click. A tab with the desktop of the corresponding host should now appear in Royal TSX.

Wireshark Installation

Windows:

Step 1: Download the Windows Installer (64-bit) from https://www.wireshark.org/download.html

Step 2: Click on Next -> Noted -> Next -> Next

Step 3: Choose your desired options. (You can use the default values). Then click „Next“

Step 4: Choos your desired installation path. (You can use the default path), then click „Next“

Step 5: CHECK „Install Npcap 1.xx“, then click Next

Step 6: UNCHECK „Install USBPcap 1.x.x.x“, then click Install

Step 7: After a short time, the Npcap installer opens. Click on „I Agree“.

Step 8: Choose your desired options. (You can use the default values). Then click „Install“

Step 9: After the installation is complete, click Next and then Finish

Step 10: the wireshark installer will continue after the Npcap installer finished. Click on Next, then Finish

Mac

Step 1: Download the Mac Installer from https://www.wireshark.org/download.html

Step 2: Open the dmg file and follow the installation process.

Step 3: MacOS Notifications may ask you for specific permission, confirm these.

Linux:

Step 1: Open a terminal. On most linux distributions, you can do this by typing „terminal“ in the search bar.

Step 2: Run the following command in the terminal: sudo apt update && sudo apt install -y wireshark

You’ll most likely be asked to enter your password. If you get an error message like „sudo: command not found“, please run this command as the root user before running the above command: apt install -y sudo

Step 3: The wireshark installation process is going to ask you if non-root users should be able to monitor network traffic. Choose „Yes“ when you are prompted.

Step 4: After the installation, run the following command in the terminal: sudo usermod -aG wireshark $(whoami)

Step 5: Reboot your system