

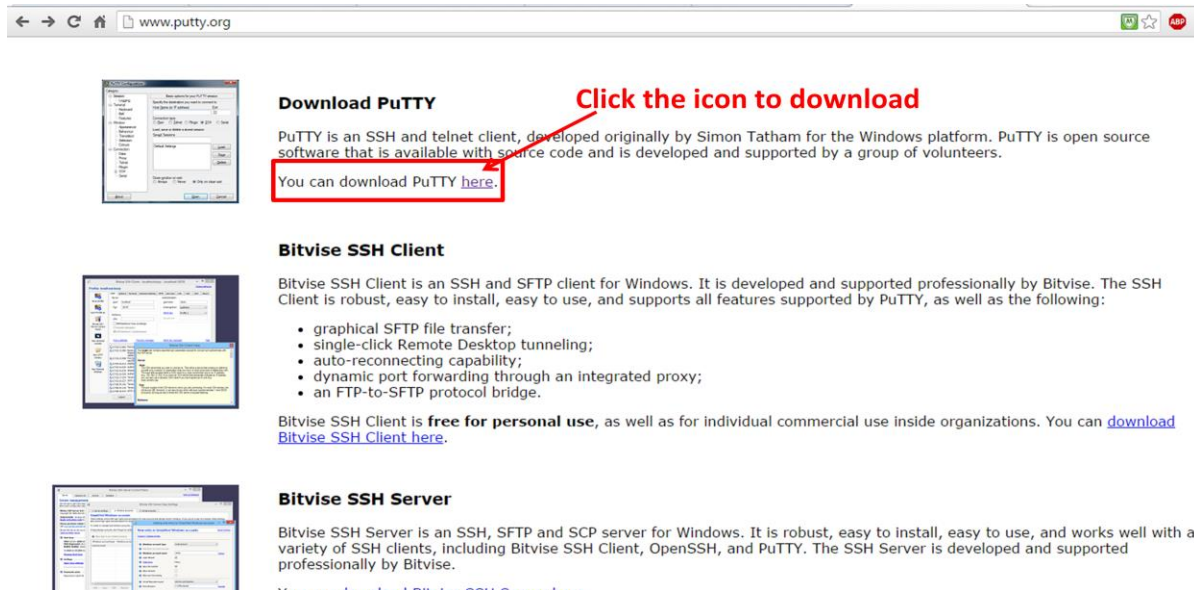
## Installing and Using PuTTY

PuTTY is a telnet/rsh/ssh client authored and maintained by Simon Tatham. PuTTY can be used on a Windows system to log in remotely to ARSC systems and to run commands on them. This software is free to download and is easy to configure through a graphical interface.

### Downloading and Installing PuTTY

The following steps cover downloading and installing PuTTY.

- a. Download puTTY from the official site <http://www.putty.org/>



**Download PuTTY**

PuTTY is an SSH and telnet client, developed originally by Simon Tatham for the Windows platform. PuTTY is open source software that is available with source code and is developed and supported by a group of volunteers.

You can download PuTTY [here](#).

**Click the icon to download**

**Bitvise SSH Client**

Bitvise SSH Client is an SSH and SFTP client for Windows. It is developed and supported professionally by Bitvise. The SSH Client is robust, easy to install, easy to use, and supports all features supported by PuTTY, as well as the following:

- graphical SFTP file transfer;
- single-click Remote Desktop tunneling;
- auto-reconnecting capability;
- dynamic port forwarding through an integrated proxy;
- an FTP-to-SFTP protocol bridge.

Bitvise SSH Client is **free for personal use**, as well as for individual commercial use inside organizations. You can [download Bitvise SSH Client here](#).

**Bitvise SSH Server**

Bitvise SSH Server is an SSH, SFTP and SCP server for Windows. It is robust, easy to install, easy to use, and works well with a variety of SSH clients, including Bitvise SSH Client, OpenSSH, and PuTTY. The SSH Server is developed and supported professionally by Bitvise.

You can download Bitvise SSH Server [here](#).

- b. Click putty.exe icon to download puTTY



**PuTTY Download Page**

[Home](#) | [Licence](#) | [FAQ](#) | [Docs](#) | [Download](#) | [Keys](#) | [Links](#)  
[Mirrors](#) | [Updates](#) | [Feedback](#) | [Changes](#) | [Wishlist](#) | [Team](#)

Here are the PuTTY files themselves:

- PuTTY (the SSH and Telnet client itself)
- PSCP (an SCP client, i.e. command-line secure file copy)
- PSFTP (an SFTP client, i.e. general file transfer sessions much like FTP)
- PuTTYtel (a Telnet-only client)
- Plink (a command-line interface to the PuTTY back ends)
- Pageant (an SSH authentication agent for PuTTY, PSCP, PSFTP, and Plink)
- PuTTYgen (an RSA and DSA key generation utility).

**LEGAL WARNING:** Use of PuTTY, PSCP, PSFTP and Plink is illegal in countries where encryption is outlawed. We believe it is legal to use PuTTY, PSCP, PSFTP and Plink in England and Wales and in many other countries, but we are not lawyers, and so if in doubt you should seek legal advice before downloading it. You may find useful information at [cryptolaw.org](http://cryptolaw.org), which collects information on cryptography laws in many countries, but we can't vouch for its correctness.

Use of the Telnet-only binary (PuTTYtel) is unrestricted by any cryptography laws.

There are cryptographic signatures available for all the files we offer below. We also supply cryptographically signed lists of checksums. To download our public keys and find out more about our signature policy, visit the [Keys page](#). If you need a Windows program to compute MD5 checksums, you could try this one at [pc-tools.net](http://pc-tools.net) (This MD5 program is also cryptographically signed by its author.)

**Binaries**

**The latest release version (beta 0.66)**

This will generally be a version we think is reasonably likely to work well. If you have a problem with the release version, it might be worth trying out the latest development snapshot (below) to see if we've already fixed the bug, before reporting it.

**For Windows on Intel x86**

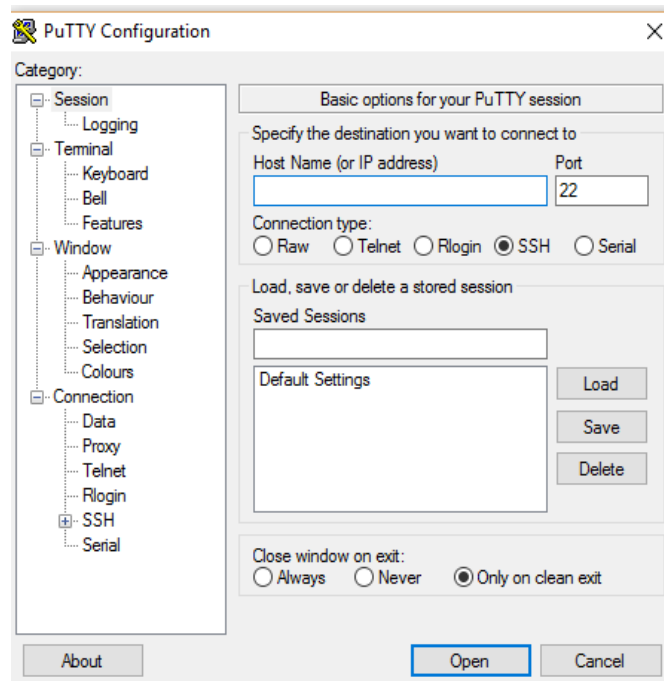
PuTTY:	<a href="#">putty.exe</a>	(or by FTP)	(signature)
PuTTYtel:	<a href="#">puttytel.exe</a>	(or by FTP)	(signature)
PSCP:	<a href="#">pscp.exe</a>	(or by FTP)	(signature)
PSFTP:	<a href="#">psftp.exe</a>	(or by FTP)	(signature)

**Click the icon to download**

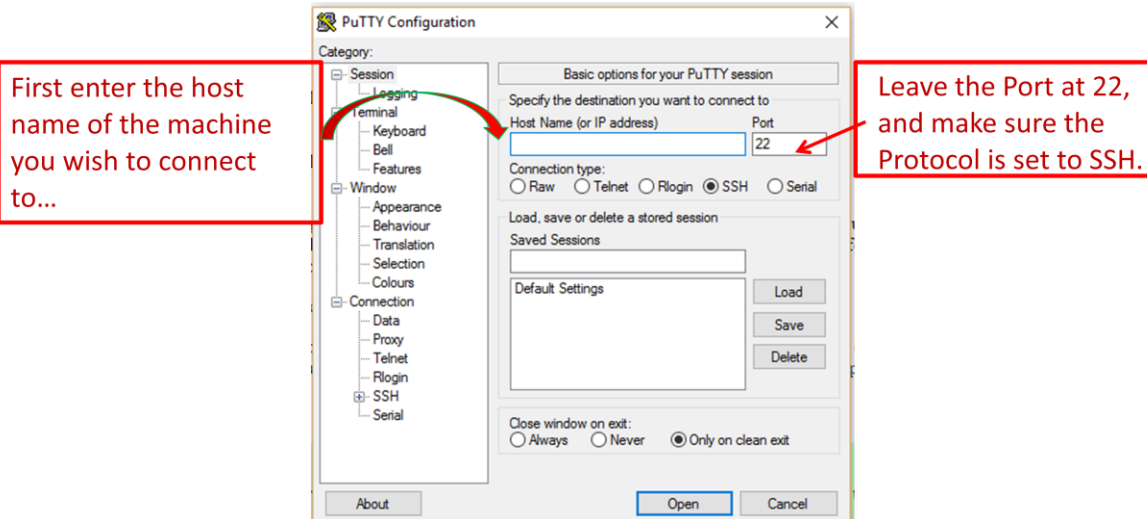
## c. Run putty.exe file.



1. You'll want to save this file in an easily accessible location. I personally recommend the desktop, so that you're just a double-click away.
2. Now, let's begin! Double-click the PuTTY icon, and the PuTTY Configuration window will appear:

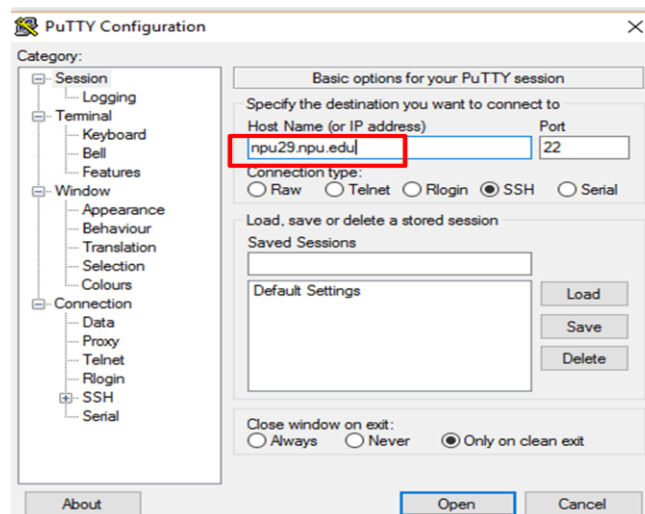


## 3. Enter the Host Name (IP address)



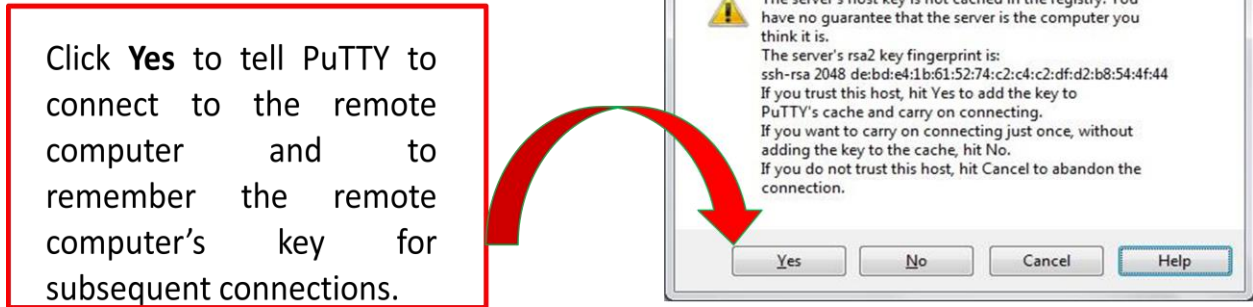
Enter any one of the below Host Names:

npu8.npu.edu (or) npu20.npu.edu (or) npu29.npu.edu



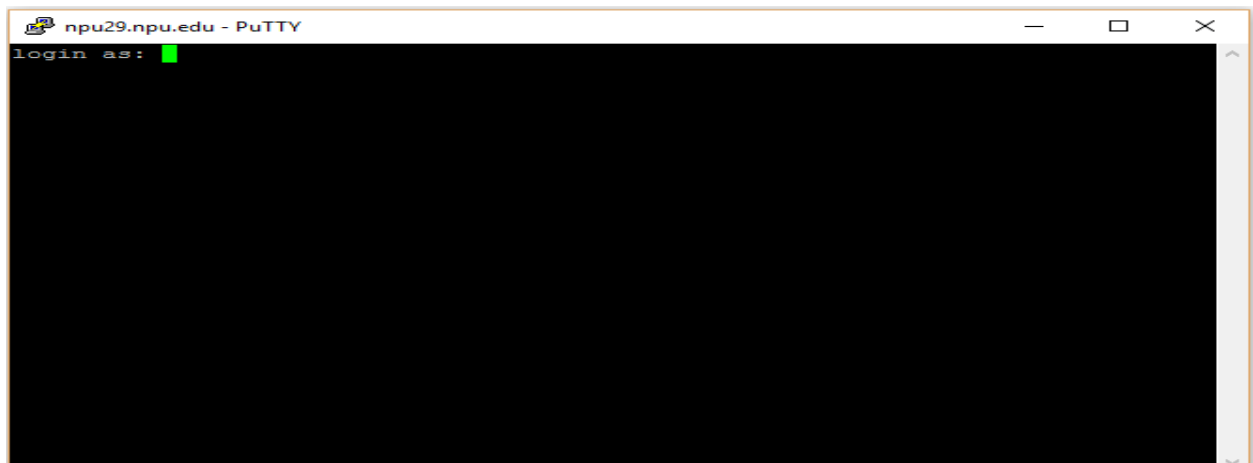
## 4. Select "Open".

5. You may receive a popup alert similar to the below one. This is a warning displayed the first time your SSH client connects to any computer to which it has never connected before, for security purposes. If you have never connected to this remote computer using this PuTTY installation, select "Yes". PuTTY will now remember the remote computer's fingerprint and suppress this message on recognition.



6. Since you do trust this machine, click Yes. You will not see this dialog box on subsequent connections.

7. Next, you will see the “login as” prompt:



8. Enter your NPU user name, and press Enter. The system will then ask you for your password: enter it, and press Enter once more. You will then be presented with the shell prompt, at which you can enter commands to be executed on the remote computer.