



MENU

How to access localhost from another computer connected to the same network?

👤 Amarjit Singh 📅 May 4, 2018 💬 No Comments

Sometimes there occurs a situation. where you have to show your website which is hosted on your computer to your boss or to any of your colleague who is not sitting beside you. But he is connected to the same network that your computer is connected to.

In this case, you can show your website to your boss or colleague. All you have to do is just allow traffic for the port that your web server is listening on.

Note: If you want to access your localhost on a computer that is not connected to the same LAN. Then you should read [this article](#).

Here are the steps to make localhost accessible from any computer on the same local network.

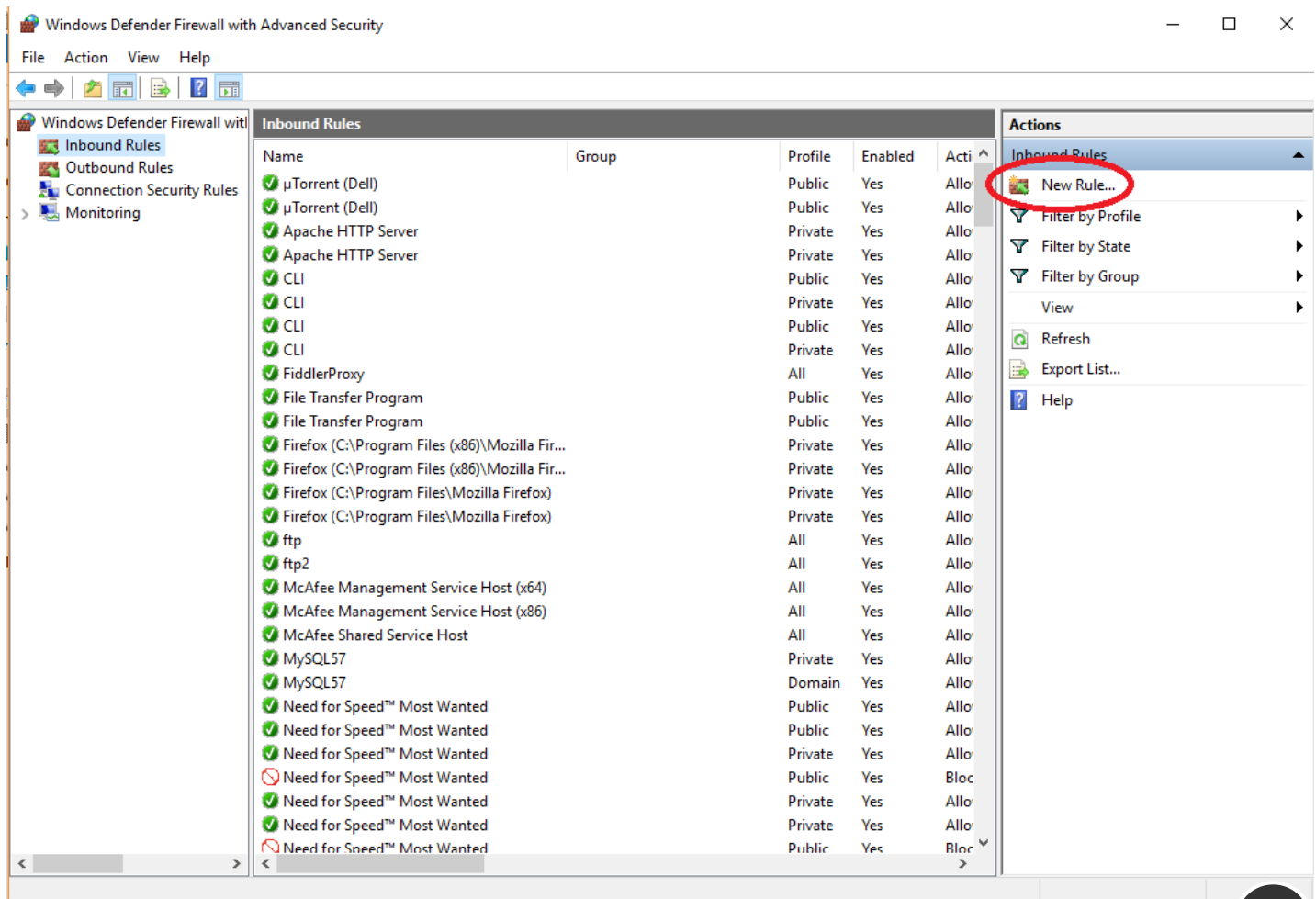
Make localhost accessible from another computer on Windows.

1. Go to Windows Firewall settings and click on advanced settings.

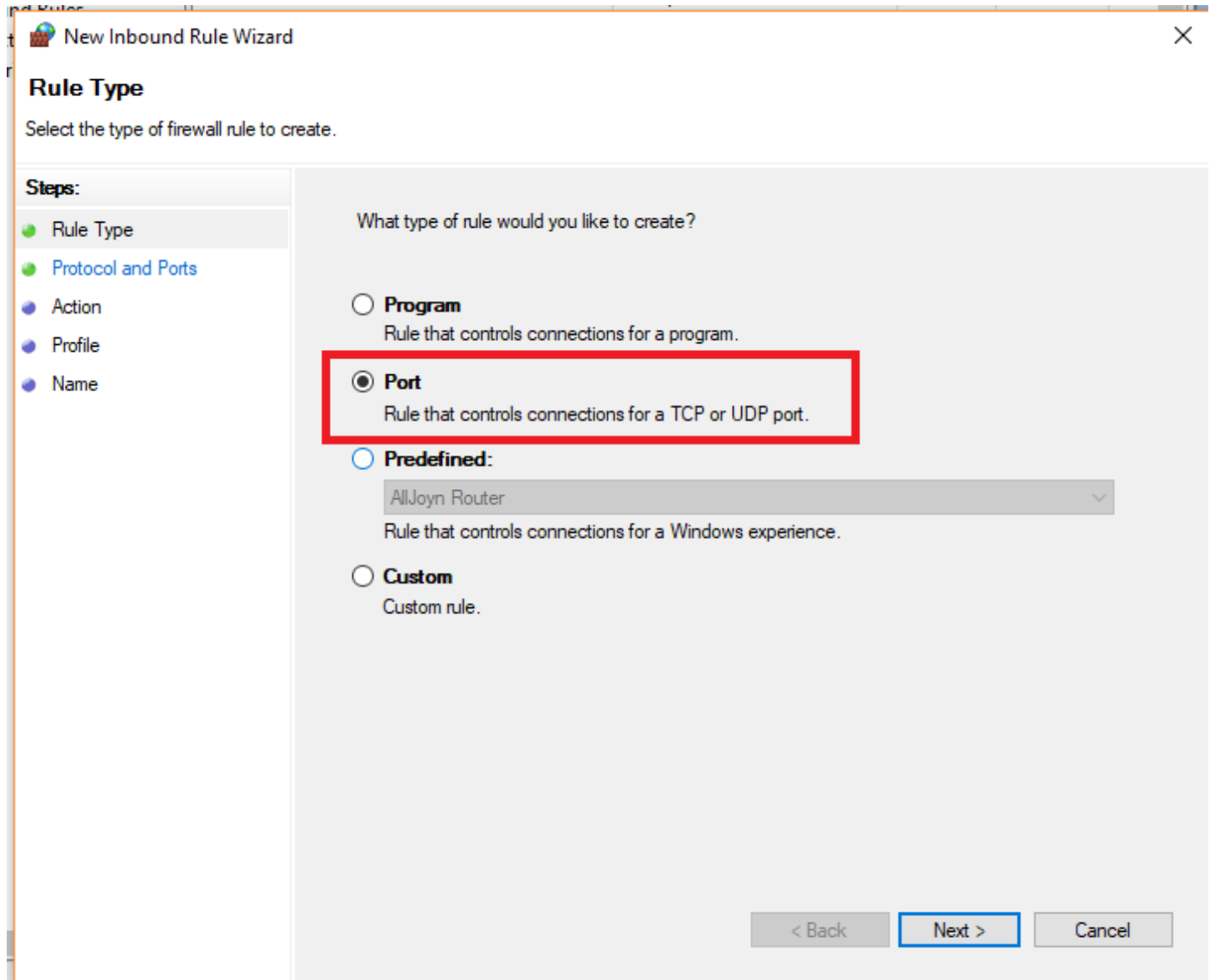




2. In the Inbound rules, click on "New Rule" option and a wizard window will pop up.



3. In the wizard there are five steps. In the first step you have to select type of rule. Since we are to allow traffic for a specific port. Therefore select the port option.



4. Now choose "Specific local ports" option **and** enter port number that your web server is listening on.

If you don't know on which port your web server is listening on then it is the number that you specify after ":" symbol in URL bar of your web browser while opening localhost on your computer. Eg: If you type "localhost:8000" or "127.0.0.1:8000" to access localhost on your computer then your web server is listening on port number "8000". **But** If you don't specify any number, that is you only type "localhost" or "127.0.0.1" then your browser implicitly enters default port. which is port number "80". That means your web server is listening on port number "80".



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

☒ **TCP**

☐ **UDP**

Does this rule apply to all local ports or specific local ports?

☐ **All local ports**

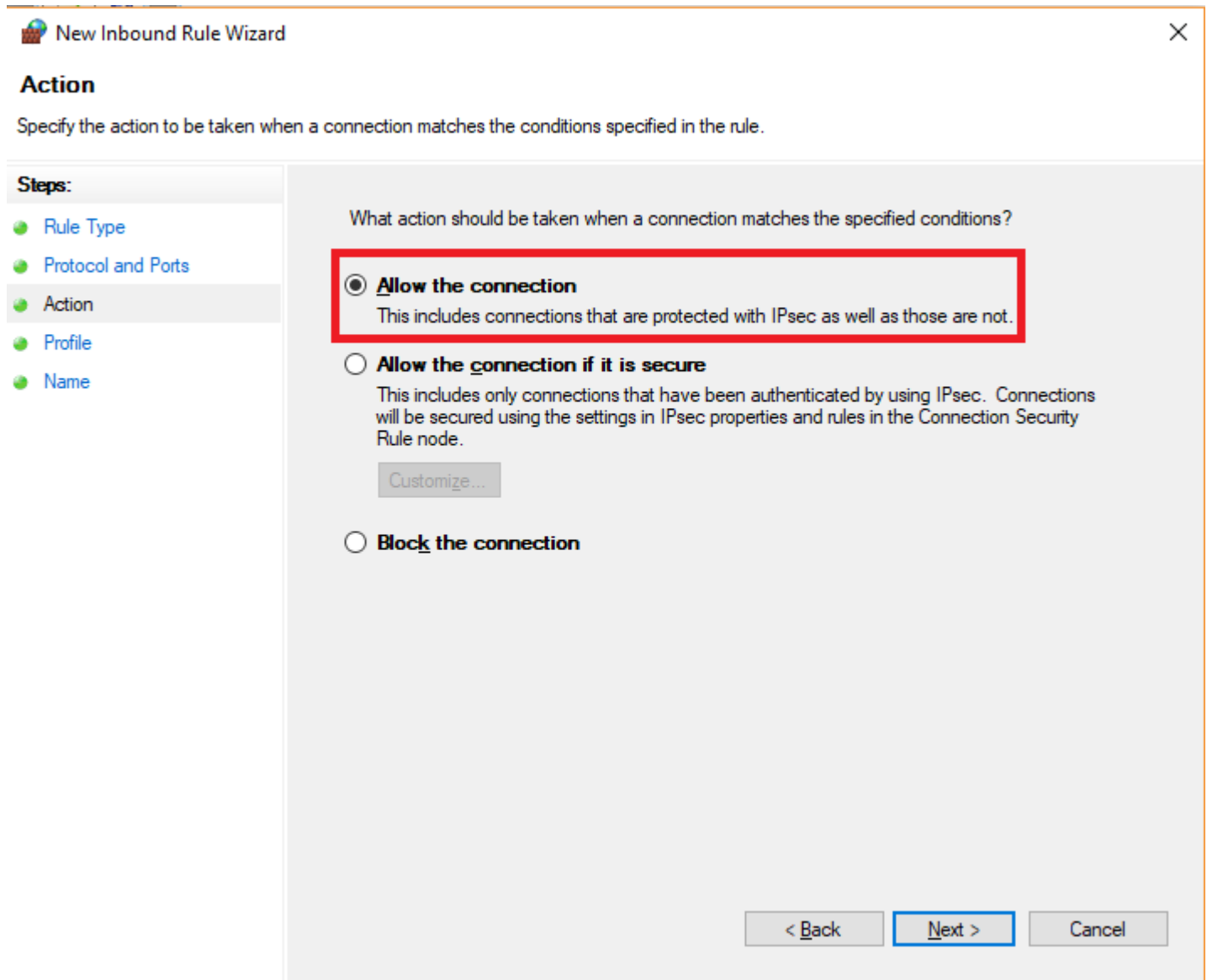
☒ **Specific local ports:**

Example: 80, 443, 5000-5010

< Back Next > Cancel

5. Now you have to choose an action. choose "Allow the connection".





New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

☒ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

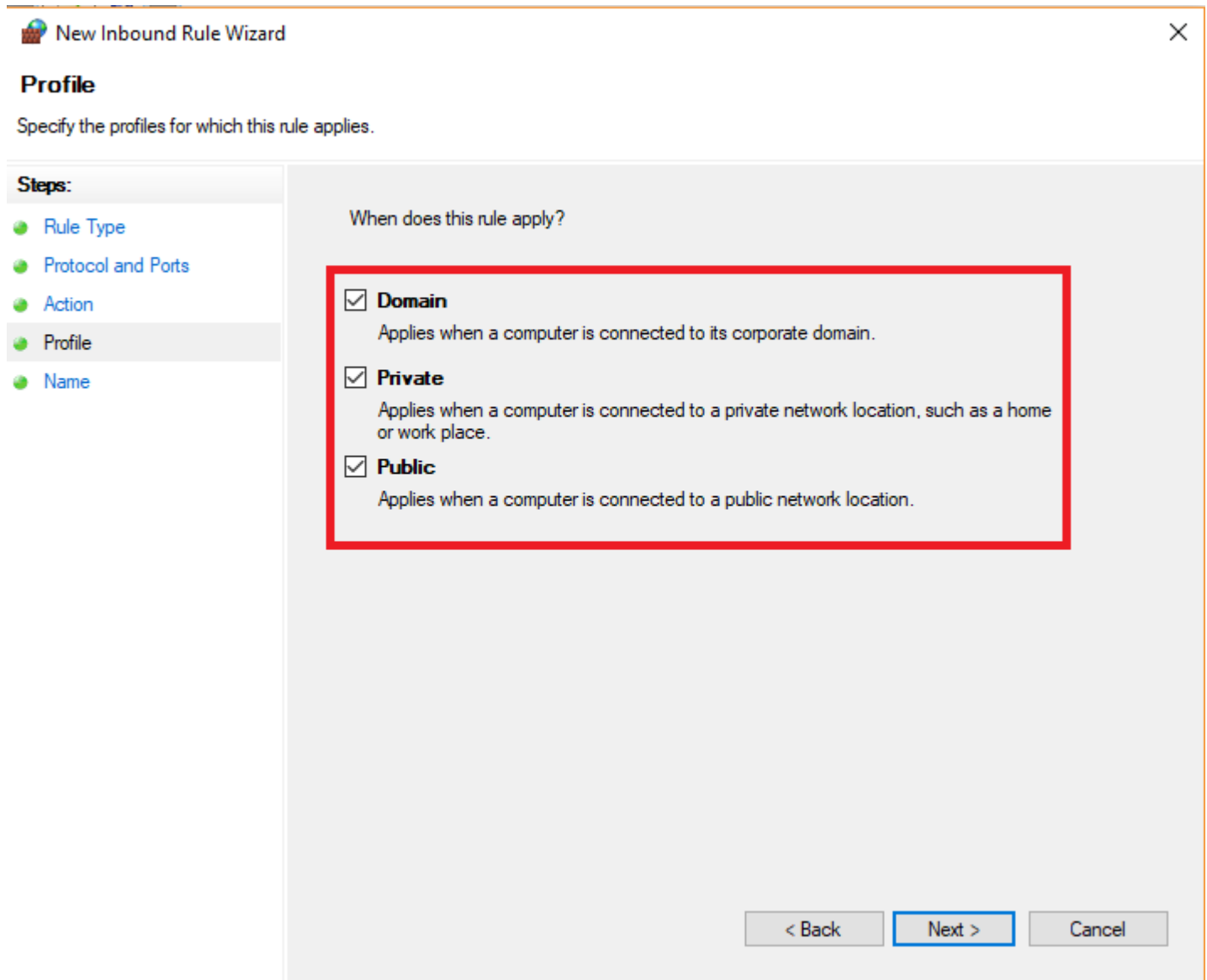
☐ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
[Customize...](#)

☐ **Block the connection**

< Back **Next >** Cancel

6. Now specify when does this rule should apply. choose all of the options.





The image shows a Windows Firewall 'New Inbound Rule Wizard' window, specifically the 'Profile' step. The window title is 'New Inbound Rule Wizard' with a close button in the top right. The 'Profile' section is active, with the instruction 'Specify the profiles for which this rule applies.' On the left, a 'Steps:' pane lists 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name', with 'Profile' being the current step. The main area, titled 'When does this rule apply?', contains three checked options: 'Domain' (Applies when a computer is connected to its corporate domain.), 'Private' (Applies when a computer is connected to a private network location, such as a home or work place.), and 'Public' (Applies when a computer is connected to a public network location.). A red rectangular box highlights these three options. At the bottom right, there are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile**
- Name

When does this rule apply?

- ☒ **Domain**
Applies when a computer is connected to its corporate domain.
- ☒ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.
- ☒ **Public**
Applies when a computer is connected to a public network location.

< Back Next > Cancel

7. Now give a name for this rule. You can also specify a description for this rule which is not mandatory.



New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name**

Name:

HTTP

Description (optional):

To make web server of this computer to be accessible from other computers.

< Back Finish Cancel

8. Finally click on the finish button to save the new rule.

now just go ahead and type local IP address of your computer in web browser of other computer which is connected to same local network. To find local IP address of your use `ipconfig` command.

If It doesn't work then you have to configure your web server to listen on local IP address or all available IP addresses for your computer.

Make localhost accessible from another computer on Ubuntu.



In Ubuntu, the requests for port 80 are already allowed. Therefore you don't have to mess up with firewall settings. Just type your Local IP address in a web browser on another computer.

To find local IP address of your computer type `ifconfig` in terminal.

 Networking

