NEOROUTER

Version 2.4

User Manual

Last Updated: Dec 21, 2017

Web-site: http://www.neorouter.com

Technical Support: http://www.neorouter.com/support/

Table of Contents

Table of Contents....2
1. Scope of service....5
1.1 About NeoRouter....5
1.2 Key Features....5
1.3 What's New....6
1.4 Glossary and Concepts....6
1.5 How it works....8
1.6 System Requirements....9
1.7 Acknowledgements....9
2. Installation....10
2.1 Check list....10
2.2 Server Setup....10
2.2.1 Server Network Requirements....10
2.2.2 Install NeoRouter server on Windows....10
2.2.3 Install NeoRouter server on Mac....12
2.2.4 Install NeoRouter server on Linux....12
2.2.5 Install NeoRouter Server on FreeBSD....13
2.2.6 Install NeoRouter Server on OpenWRT Backfire....13
2.2.7 Install NeoRouter Server on Tomato....13
2.2.8 Setup NeoRouter server....14
2.2.9 Create first administrator account....14
2.2.10 Setup NeoRouter domain....15
2.2.11 Port forwarding....15
2.2.12 IPv6....15
2.3 Client Setup....16
2.3.1 Install NeoRouter Client on Windows....16
2.3.2 Install NeoRouter Client on Mac....17
2.3.3 Install NeoRouter Client on Android....17
2.3.4 Install NeoRouter Client on Linux....17
2.3.5 Install NeoRouter Client on FreeBSD....17
2.3.6 Install NeoRouter Client on OpenWRT Backfire....18
3. Network Explorer....18
3.1 Launch and Sign In....18
3.2 Computer List....19
3.3 Add-on....21
3.3.1 Add-on launch pad....21
3.3.2 Manage Add-ons (Windows)....23
3.3.3 Manage Add-ons (Mac)....26
3.4 Connection Options....28
3.4.1 P2P Connection....28
3.4.2 Proxy Setting....28
3.4.3 Server Local Address....29
3.5 Multi-Language....30
3.5.1 Install a language resource file....30
3.5.2 Language resource file format....30
3.5.3 Multi-Language support for Add-ons....31
3.6 Skin....31
3.7 Network Explorer CLI....31
3.7.1 Launch CLI....32
3.7.2 Computer List in CLI....32
3.8 Network Explorer Portable....32
3.8.1 Network Explorer Portable....33

3.8.2 Manage Add-On 33
3.8.3 Auto Run Configuration for USB 33
3.9 Change Password 35
4. NeoRouter for Android 35
4.1 Overview 35
4.2 VPN mode for Android 4.x and above 35
4.3 Tunnel Mode for Android 3.x and below 39
4.3.1 Quick start using dynamic port forward 39
4.3.2 Configure Dynamic Port Forward 41
4.3.3 Configure Static Port Forward 41
5. NeoRouter Remote Access Client 42
5.1 Prerequisites 42
5.2 System Requirements 42
5.3 Built-in add-ons 43
5.3.1 VNC 43
5.3.2 RDP 43
5.3.3 Telnet and SSH 44
5.3.4 FTP and SFTP 45
5.4 Tips 46
6. Configuration Explorer 46
6.1 Launch and Sign In 46
6.2 Managing Users 47
6.3 Managing Computers 48
6.4 Access Control List 49
6.4.1 Overview 49
6.4.2 Define Computer ACL 50
6.4.3 Define ACL entry 51
6.4.4 How Firewall Works 51
6.4.5 Example: hub-and-spoke 52
6.4.6 Example: one-way access 52
6.5 Managing Server and Domain 53
6.6 Branding 53
6.7 Server Configuration CLI 55
6.8 Web Console 55
7. Advanced Configuration 56
7.1 Change Server Port 56
7.2 Change Packet Filtering 56
7.3 Change DHCP 57
7.4 User Access Auditing 57
7.5 Account Lockout 58
7.6 Network Bridge 58
7.6.1 Overview 58
7.6.2 Routing vs. Bridging 59
7.6.3 Setup Network Bridge 59
7.6.4 Bridging Setup – point to site VPN 60
7.6.5 Routing Setup – site to site VPN 62
7.6.6 Bridging Setup – site to site VPN 64
7.6.7 Run Scripts 64
7.7 Build Custom Add-on (Windows) 65
7.7.1 Create Custom Add-on 65
7.7.2 Add-on File Formats 67
7.8 Configuration Files 68
7.8.1 Feature.ini template 68
7.8.2 Log.ini template 74
8. Licensing NeoRouter 77
8.1 Licensing Overview 77

8.2 Activation....77
8.3 Product Key Recovery....78
9. Troubleshooting and Support....78
9.1 Troubleshooting....78
9.1.1 Troubleshooting steps....78
9.1.2 Generate Log....79
9.2 Contact Us....80

1. Scope of service

1.1 About NeoRouter

NeoRouter is a cross-platform zero-configuration VPN solution that securely connects Windows, Mac and Linux computers at any locations into a virtual LAN and provides a networking platform for various applications like remote desktop, shared folders and printers, offsite backup, voice & video chat, games, etc. It is the ideal Remote Access and VPN solution for small businesses and homes.

Many small businesses or homes have high-speed internet and multiple computers, and users are facing challenges like remote access, directory management and network security. To solve similar problems at large enterprises, skilled administrators can deploy very expensive and complex tools like VPN, domain controller and corporate firewall. But small business or home users do not have the right tools that fit their needs.

Our mission is to provide low-cost zero-configuration networking solutions for small businesses and homes. This is why we have built NeoRouter.

1.2 Key Features

Feature	**Description**
Cross platform	Support Windows (Windows XP and above), Mac OSX (10.5 and above), Linux (all major distros), BSD, Android, iOS and router firmwares (tomato and openwrt).
Roaming Profile	You can sign in from any computer using the same account and your profile (including the computer list and your preference) will roam with you.
P2P	NeoRouter can setup direct peer-to-peer (P2P) connection between computers. When direct P2P connection is impossible (e.g. your computer is behind a corporate firewall), NeoRouter relays the network traffic through your own router, while other VPN products relay through a central server geologically located far away and shared by thousands of other users.
High portability	You can run NeoRouter portable client from a USB drive without installation. This feature is especially useful if you are using a computer that you do not have the privileges to setup new software, e.g. in a library or hotel.
Unattended servers	NeoRouter runs as a system service (daemon) and will automatically reconnect after reboot.
Add-ons	Add-ons extend NeoRouter and let you perform additional tasks over the virtual network.
Proxy	Proxy support allows you access your virtual network behind proxy servers that support HTTP Proxy, SOCKS4 and SOCKS5 protocols.
Remote Wakeup	You can put your computer to standby mode to conserve electricity and NeoRouter can wake up the computer when you actually use it.
Reliability	NeoRouter does not rely on a central server for connectivity, so you do not need to worry about the unexpected server maintenance and downtime.
Network Bridge (1.x only)	You can either bridge the NeoRouter virtual network with physical networks or create multiple site-to-site VPN.
Access control	You can grant or deny user's accesses to a computer or a service/port individually. For example, you can prevent your client Bob from accessing your internal file server even though they are on the same virtual LAN.
Customization	You can personalize the user interface with your native language and favorite skin.
Branding	Business users can integrate the company's logo and customize the banner.

1.3 What's New

Version 1.1.1

- Implemented GUI Network Explorer for Mac OSX 10.5 and above. See Network Explorer
- Enabled P2P support in NeoRouter Portable client.
- Merged NeoRouter USB and Portable into one package.
- Fixed OpenSSL incompatibility issue on Linux and supported more Linux distributions.
- Solved router hairpin issue. See Server Local Address.

Version 1.1.2

- Implemented NeoRouter Network Explorer for Android. See http://www.neorouter.com/android/.
- Ported NeoRouter client and server to BSD. See Install NeoRouter Server on FreeBSD and Install NeoRouter Client on FreeBSD.
- Added TightVNC client and Putty SSH client to NeoRouter Portable package.

Version 1.1.3

- Added Packet Filter support. See Change Packet Filtering.
- Optimized P2P connection and automatically close it when idle.

Version 1.2.0

- Improved server scalability on Windows and Linux to support thousands of client connections.
- Added user access auditing. See User Access Auditing.

Version 1.3.0

- Added support for OpenWRT Backfire mipsel 2.4 kernel.

Version 1.4.0

- Added support for OpenWRT Backfire x86, tested on Soekris and ALIX boards.

Version 1.5.0

- Added full computer list view support. See Computer List.
- Added IPv6 support for underlying client-server or peer-to-peer connections. See IPv6.
- Allowed NeoRouter Pro clients to connect to NeoRouter Free server.

Version 2.0.0

- Added support for Android (native VPN mode and dynamic port forward mode).
- Added NeoRouter Remote Access Client for Android
- Added NeoRouter Remote Access Client for iOS
- Added NeoRouter Remote Access Client for HTML5 Browsers
- Added NeoRouter Remote Access Client for Chrome Extension
- Added support for Raspberry Pi
- Added NeoRouter Web Console
- Added setup tool ***nrsetup***
- Added "Account lock out control" feature

Version 1.4.0

- Added support for OpenWRT Barrier Breaker (mipsel, x86, ar71xx).
- Added support for TLS 1.1/1.2

1.4 Glossary and Concepts

NeoRouter Virtual Network (VLAN): NeoRouter software connects a group of hosts from any locations into a virtual LAN-like network that has similar attributes as a physical LAN. Hosts can communicate as if they were attached to the same broadcast domain, even if they are not located on the same network switch.

NeoRouter Client: A host on the VLAN is called NeoRouter Client. It has a virtual network adapter and is assigned a virtual IP address.

NeoRouter Server: NeoRouter Server assists clients in discovering and communicating to each other. It also manages users' profiles and privileges, software licenses and branding. NeoRouter Clients must connect to server in order to join the VLAN.

NeoRouter Domain: One NeoRouter Server and multiple NeoRouter Clients that connect to this server are collectively called NeoRouter Domain. Each domain has a globally unique name as its identification. Domain names are managed by NeoRouter Inc.

NeoRouter User: A NeoRouter User is a person who uses NeoRouter software and accesses hosts on a virtual network. Please note that many other VPN solutions like OpenVPN or Hamachi do not distinguish a user from a client host. NeoRouter introduces the user concept so that a user will have the experience regardless on which computer he connects to the VLAN and admin can manage each user's access privilege.

NeoRouter Administrator: A NeoRouter Admin is a user who can also manage the VLAN.

NeoRouter Network Explorer: The main application installed on a client that allows users to log into the VLAN, view the connection status of other clients, and launch add-on programs to connect to remote clients. It may have graphic or command-line user interface (executable is nrclientcmd).

NeoRouter Network Explorer Portable/USB (aka Viewer): A version of the NeoRouter Network Explorer that requires no installation. It is ideal for users who need to connect from a kiosk but do not have the privilege to install software. It allows users to log in and launch add-on programs just like the regular Network Explorer. But the local computer will not join the VLAN and other clients will not be able to connect to it. It also ensures no personal information is left behind after use.

NeoRouter Configuration Explorer (aka Console): An application installed on a client or a server that allows administrators to manage a VLAN. Configuration Explorer for Windows has a graphic user interface and can be used to configure local or remote server. Configuration Explorer for Mac and Linux are built into server's command-line interface (executable is nrserver) and can configure local server only.

NeoRouter Web Console: A web-based version of NeoRouter Configuration Explorer. It supports HTML5 based web browsers, such as Chrome, Safari, IE10, BB10 and Firefox.

NeoRouter Client Service: A daemon program installed on a client that establishes connections to server and peer clients. It always runs in the background and ensures the connections, even when the Network Explorer is not running. Most users do not need to interactive with this program directly.

NeoRouter Remote Access: A client side tool, that allows users to remotely access computers in the NeoRouter network using built-in add-ons, such as VNC client, RDP client, Telnet/SSH client, FTP/SFTP client and Wake-On-Lan client. It supports HTML5 based web browsers, Android, iOS, BB10 and Chrome Extension.

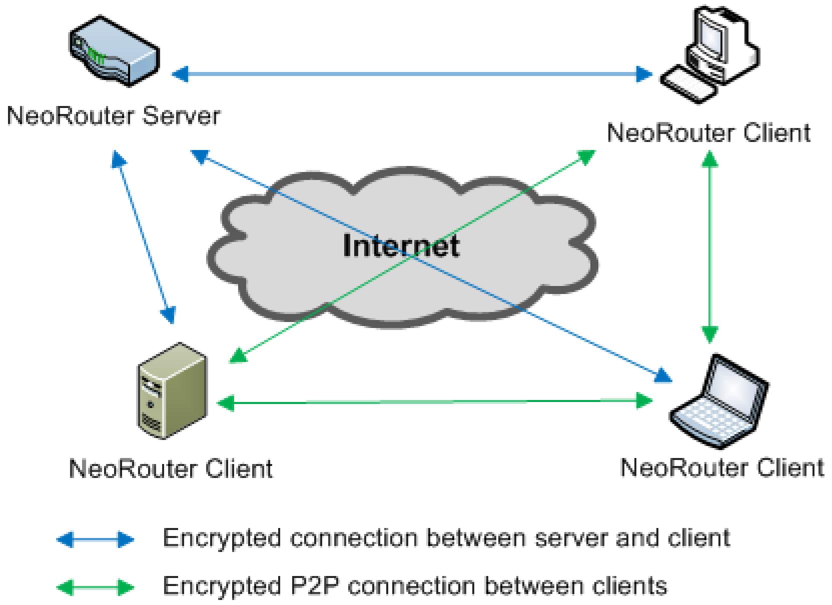
Access Control List (ACL): An ACL of a host specifies which users are granted or denied access to the host and which ports are allowed. Each host also has a default ACL which is used if a user's privilege is not explicitly defined in the host's ACL or if user does not sign in Network Explorer on the remote host.

NeoRouter Dashboard: A web-based application that allows users to manage domain information and view domain status. (https://www.neorouter.com/Dashboard)

NeoRouter Dynamic Domain Name System (DDNS): To simplify user log on, NeoRouter maintains domain name, public IP address and port of every NeoRouter server in a central DDNS server. When user launches Network Explorer and signs into a domain, Network Explorer contacts the DDNS server, translates the domain name into the actual IP address and port, and connects to the NeoRouter server.

NeoRouter Server setup: A NeoRouter server setup tool, that make it easy for users to setup the NeoRouter server when or after installation. On Window, it's included in the Installation Wizard; on non-Windows platforms, it's a separate command ***nrsetup***.

1.5 How it works


NeoRouter Server
NeoRouter Client
Internet
NeoRouter Client
NeoRouter Client
Encrypted connection between server and client
Encrypted P2P connection between clients

In the NeoRouter domain shown in the above diagram, three clients at different locations can establish direct P2P connections with the help from server and can communicate to each other as if they were in the same physical LAN.

A NeoRouter server is usually setup on an always-on host that has stable Internet connection and a static or dynamic public IP address. If server is behind a router (or firewall), user needs to configure the router and expose the NeoRouter server port (default to 32976) to Internet by port-forwarding.

NeoRouter client can connect from anywhere as long as it has Internet connection. User can simply launch NeoRouter Network Explorer, signs in with user credential and domain name, and he/she will be able to view the list of hosts in the VLAN and launch add-on programs to access them. Network Explorer uses a DDNS-like protocol to discover and connects to the NeoRouter server (blue lines). When user executes add-on programs, NeoRouter client will establish a direct P2P connection to the requested peer client (green lines) and a secure tunnel that transfers the network data from all the add-on programs.

NeoRouter server remembers the signature of a client after its first successful connection and NeoRouter Client Service daemon can then connect to the VLAN without requiring user to log into NeoRouter Network Explorer. This allows an untended server to always stay connected.

NeoRouter clients use the STUN and STUNT methods to establish the direct P2P connections and achieve highest connection speed. These methods are widely used in P2P programs and have very high success rate. If a client is behind a symmetric NAT which is often found in large corporations, these methods may fail and the connection to this client will fall back to relay mode. If the traffic between two clients is relayed through server, the server’s physical location, network speed and CPU load may affect the connection speed.

NeoRouter uses SSL/TLS1.2 (AES-256) protocol to secure the communication channel between client and server and uses a suite of protocols (RSA 2048bit, DH and AES-256) to protect P2P connections among clients. This solution meets the industry’s highest security standards.

User can setup NeoRouter server and client on the same host. NeoRouter server by itself cannot add a host into VLAN or communicate with peer clients using their virtual IP addresses. User often sets up NeoRouter client software on the same host as server so that this host can become part of the VLAN.

1.6 System Requirements

NeoRouter client and server can be installed on:

Windows (XP and above)
Mac OS X (10.5 and above)
Linux i386 and x64 (Redhat/Fedora/CentOS, Ubuntu/Debian, SuSE)
Linux Arm (Raspbian "wheezy")
BSD i386 and x64 (FreeBSD, PCBSD, Desktop BSD)
Linux-based router firmware (Tomato, OpenWRT Barrier Breaker)
Android (1.6 and above)
iOS (5 and above)

1.7 Acknowledgements

NeoRouter is made possible because of the following open-source projects:

OpenSSL: the Open Source toolkit for SSL/TLS. http://www.openssl.org

OpenWrt: a Linux based firmware program for embedded devices such as residential gateways and routers. http://www.openwrt.org

Tomato Firmware: a small, lean and simple replacement firmware for Broadcom-based routers. http://www.polarcloud.com/tomato

Tun-Tap OSX: the virtual network interface for Mac OS X. http://tuntaposx.sourceforge.net

Raspberry Pi: a credit-card-sized single-board computer. http://www.raspberrypi.org/

Nullsoft Scriptable Install System (NSIS): a professional open source system to create Windows installers. http://nsis.sourceforge.net

NRClientX: a GUI frontend for NeoRouter Network Explorer on Mac, Linux and Windows. http://sourceforge.net/projects/nrclientx/

2. Installation

2.1 Check list

Here are the steps to setup a NeoRouter Virtual LAN. Please refer to next few sections for detailed instructions on your target operating systems.

- Server Setup
    a. Choose a host that meets the network requirements as NeoRouter server
    b. Install NeoRouter server software
    c. Create the first administrator, if necessary
    d. Setup NeoRouter domain
    e. Configure router or firewall for port-forwarding, if necessary

  Note: NeoRouter Server for Windows has an install wizard that guides user through steps b, c & d.

- Client Setup
    a. Install NeoRouter client software
    b. Sign In Network Explorer and join this host to VLAN
    c. Install add-ons, if necessary

- License activation: See Chapter 8 Licensing NeoRouter.

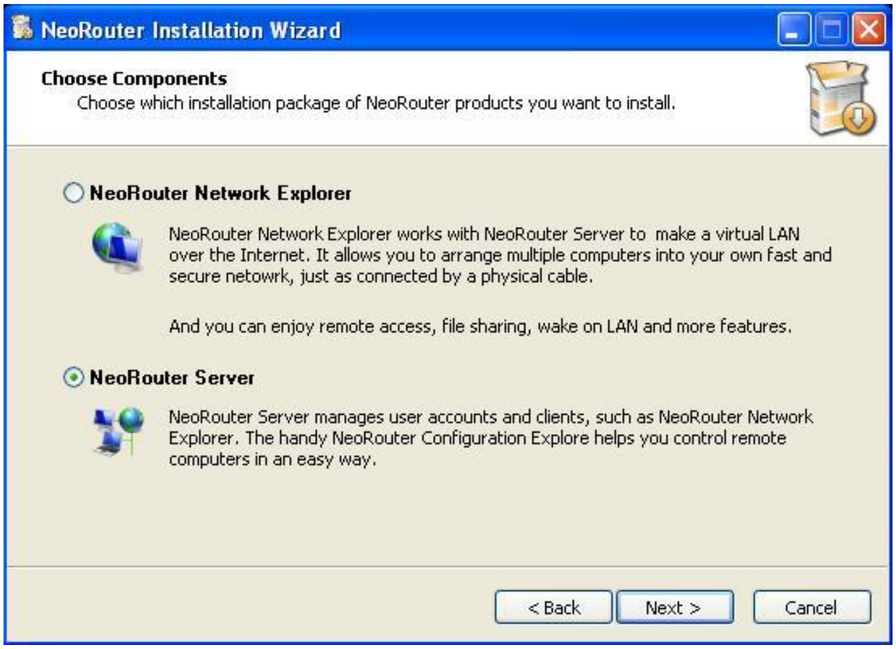
2.2 Server Setup

2.2.1 Server Network Requirements

A NeoRouter server is usually setup on an always-on host that has stable Internet connection and a static or dynamic public IP address. If server is behind a router (or firewall), user needs to configure the router and expose the NeoRouter server port (default to 32976) to Internet by port-forwarding.

2.2.2 Install NeoRouter server on Windows

1. Download NeoRouter installation package for Windows. NeoRouter server and client for Windows share the same installation package.
   If you are installing on Windows 2000, please download the package for this OS.
2. If you have installed an earlier version of NeoRouter, please uninstall it using Windows Add or Remove Program tool.
   You may be prompted with a dialog box asking whether to remove user data files generated by NeoRouter. These files include database, configuration and cached information. If you are simply upgrading, please click “No” to keep the files.
3. Launch the installation wizard, choose NeoRouter Server and click the Next button.



Choose Components

Choose which installation package of NeoRouter products you want to install.

○ **NeoRouter Network Explorer**

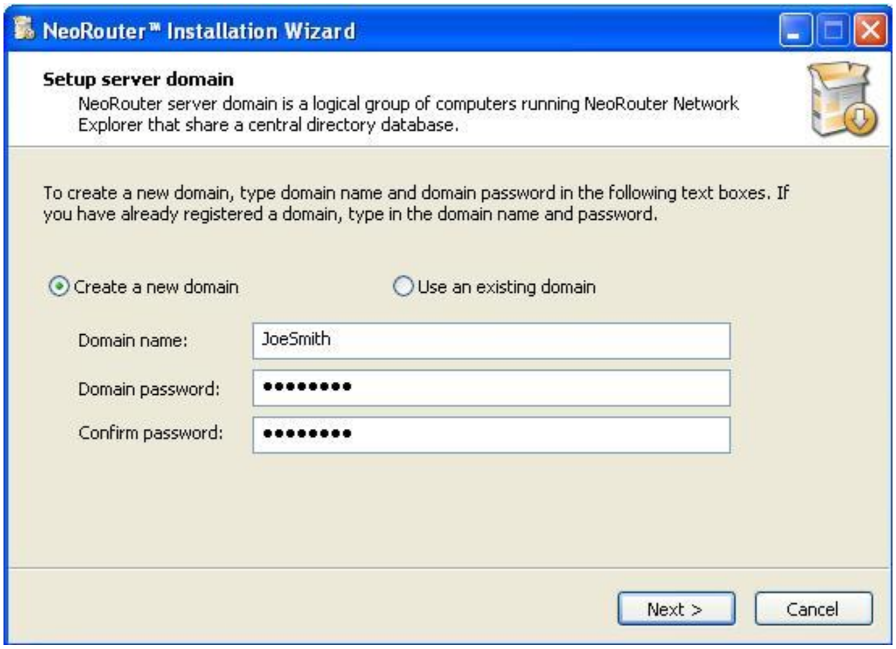
NeoRouter Network Explorer works with NeoRouter Server to make a virtual LAN over the Internet. It allows you to arrange multiple computers into your own fast and secure netowrk, just as connected by a physical cable.

And you can enjoy remote access, file sharing, wake on LAN and more features.

● **NeoRouter Server**

NeoRouter Server manages user accounts and clients, such as NeoRouter Network Explorer. The handy NeoRouter Configuration Explore helps you control remote computers in an easy way.

4. Setup a domain name that can uniquely identify your virtual LAN. You will need to enter the domain name in the "log on to" box during sign in.



Setup server domain

NeoRouter server domain is a logical group of computers running NeoRouter Network Explorer that share a central directory database.

To create a new domain, type domain name and domain password in the following text boxes. If you have already registered a domain, type in the domain name and password.

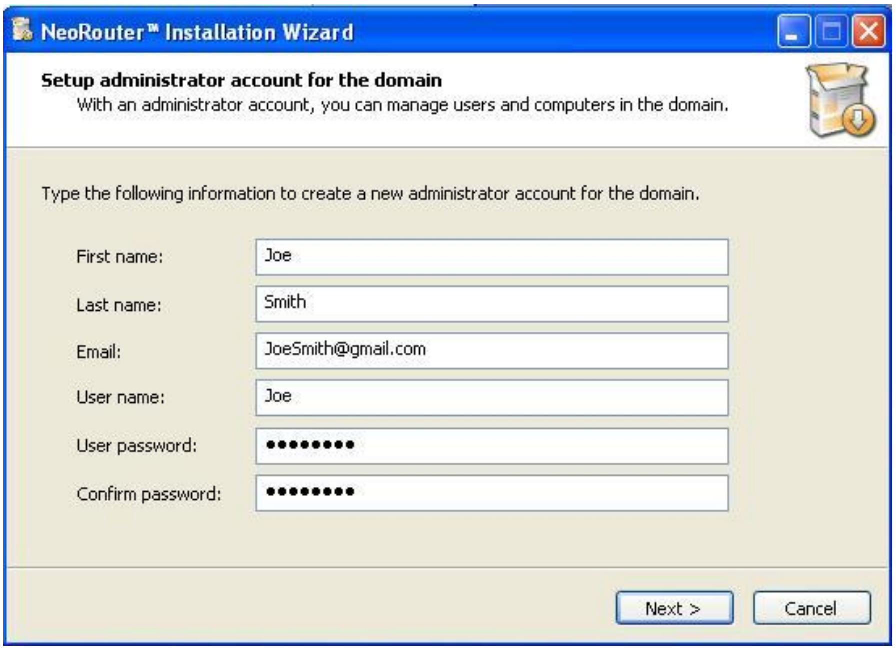
● Create a new domain ○ Use an existing domain

Domain name: JoeSmith

Domain password: ••••••••

Confirm password: ••••••••

5. Setup the administrator account for your domain. You will need to enter the username and password during sign in.



NeoRouter™ Installation Wizard

Setup administrator account for the domain

With an administrator account, you can manage users and computers in the domain.

Type the following information to create a new administrator account for the domain.

First name: Joe

Last name: Smith

Email: JoeSmith@gmail.com

User name: Joe

User password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

6. Click the Finish button to complete installation.
7. NeoRouter is installed under “%Program Files%\ZebraNetworkSystems\NeoRouter” and user data is stored under “%AllUsersAppdata%\ZebraNetworkSystems\NeoRouter”.
8. NeoRouter server daemon can be controlled in Services Console (services.msc).

2.2.3 Install NeoRouter server on Mac

1. Download NeoRouter server for Mac.
2. If you have installed an earlier version of NeoRouter, please uninstall it: In a terminal, execute command "sudo /Library/NeoRouter/rmnrserver.sh".
3. Double-click nrserver-<version>-<release>.dmg to open the disk image in Finder.
4. Double-click NeoRouterServer.mpkg to launch installer.
5. NeoRouter is installed under /Library/NeoRouter folder and user data is stored under /usr/local/ZebraNetworkSystems/NeoRouter.

2.2.4 Install NeoRouter server on Linux

1. Download NeoRouter Server for your Linux distribution.
2. If you have installed an earlier version of NeoRouter, please uninstall it:
   Redhat and Fedora: sudo rpm -e nrserver
   SuSE: sudo rpm -e nrserver
   Ubuntu, Debian and Raspbian: sudo dpkg -r nrserver
3. Install:
   Ubuntu and Debian: sudo dpkg -i nrserver-<version>-<release>.i386.deb
   Raspbian: sudo dpkg -i nrserver-<version>-<release>.armhf.deb
   SuSE: sudo rpm -i nrserver-<version>-<release>.i386.rpm
   Redhat and Fedora: sudo rpm -i nrserver-<version>-<release>.i386.rpm

   Configure OpenSSL: NeoRouter is compiled using openssl 0.9.8g. If you have an older version of Fedora, please upgrade the openssl package. You may also need to add the following symbol links:

   ```
   cd /lib
   ln -s libcrypto.so.0.9.8g libcrypto.so.0.9.8
   ln -s libssl.so.0.9.8g libssl.so.0.9.8
   ```
4. Configure firewall for NeoRouter server listening port:

Redhat and Fedora: In a terminal, run command "sudo nano /etc/sysconfig/iptables", add "-A INPUT -m state --state NEW -m tcp -p tcp --dport 32976 -j ACCEPT" before "COMMIT".
SuSE: Launch firewall configuration tool, choose "Allowed Services" in the left panel, choose "External Zone" in the first drop-down box, choose "NeoRouter server" in the second drop-down box, click "Add" button, click "Next", click "Finish" to save the changes
Ubuntu does not support firewall by default. If you setup any firewall, please open NeoRouter server port (32976 by default).

5. NeoRouter is installed under /usr/bin and user data is stored under /usr/local/ZebraNetworkSystems/NeoRouter.
6. (Optional) consider adding a cron job that automatically restarts nrserver in case it crashes.
   Using Ubuntu as an example, you can edit /etc/crontab and add "*/5 * * * * root /etc/init.d/nrserver.sh start".

2.2.5 Install NeoRouter Server on FreeBSD

1. Download NeoRouter Server for FreeBSD.
2. If you have installed an earlier version of NeoRouter, please uninstall it:
   ```
   su as root and run rmnrserver.sh
   ```
3. Install:
   ```
   Copy the downloaded package to /tmp
   cd /tmp; tar zxvf nrserver*.tgz
   cd /tmp/nrserver
   su as root and make install
   ```
4. (Optional) consider adding a cron job that automatically restarts nrserver in case it crashes.

2.2.6 Install NeoRouter Server on OpenWRT Backfire

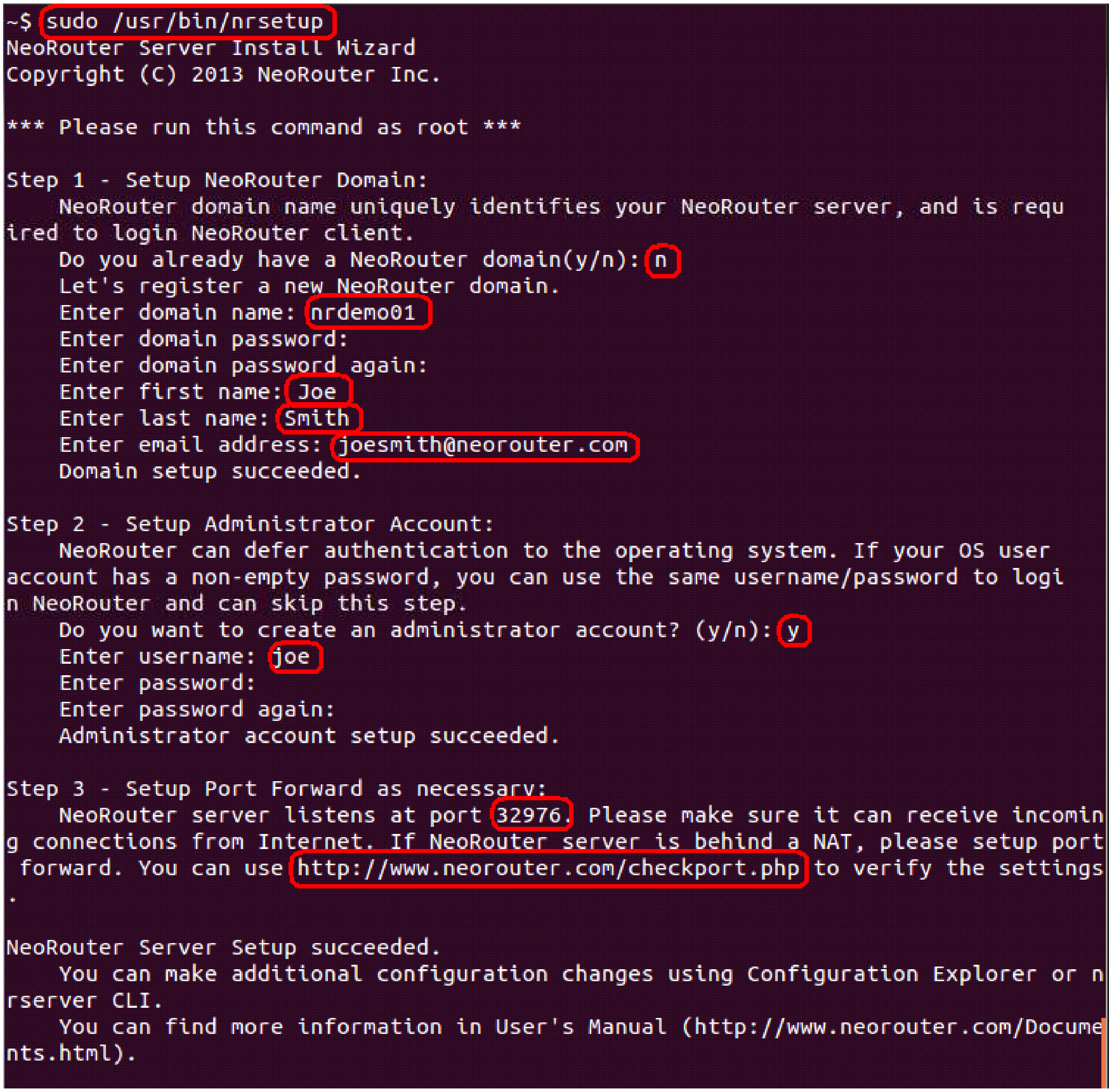
1. Connect to the router using ssh
2. Update available install packages using command: opkg update
3. If you have installed an earlier version of NeoRouter, please uninstall it: opkg uninstall nrserver
4. Install: opkg install http://www.neorouter.com/Downloads/...Backfire/nrserver_<version>-<release>_mipsel.ipk
5. Configure firewall for the NeoRouter server listening port.
   edit /etc/firewall.user and add the following
   ```
   iptables -t nat -A prerouting_wan -p tcp --dport 32976 -j ACCEPT
   iptables        -A input_wan      -p tcp --dport 32976 -j ACCEPT
   ```
6. NeoRouter is installed under /usr/bin and user data is stored under /usr/local/ZebraNetworkSystems/NeoRouter.

2.2.7 Install NeoRouter Server on Tomato

1. Download NeoRouter Server for Tomato. It is a custom build of the full tomato firmware in TRX format.
2. Flash your router with the downloaded firmware. See http://en.wikibooks.org/wiki/Tomato_(firmware) for instructions.
3. In tomato UI – Administration – Jffs2, enable jffs and format if needed
4. In tomato UI – Administration – scripts – WAN up, add "/usr/bin/nrserver.sh start"
5. Reboot router
6. NeoRouter is installed under /usr/bin and user data is stored under /usr/local/ZebraNetworkSystems/NeoRouter.
7. Troubleshoot: If you have trouble signing into NeoRouter Network Explorer from a remote client, please try DISABLE the Inbound Connection Logging. In tomato UI - Status - Logs - Logging Configuration, disable Inbound Connection

2.2.8 Setup NeoRouter server

On non-Windows platforms, user can use the setup tool ***nrsetup*** to configure the NeoRouter Server after installation.



```
~$ sudo /usr/bin/nrsetup
NeoRouter Server Install Wizard
Copyright (C) 2013 NeoRouter Inc.

*** Please run this command as root ***

Step 1 - Setup NeoRouter Domain:
    NeoRouter domain name uniquely identifies your NeoRouter server, and is requ
ired to login NeoRouter client.
    Do you already have a NeoRouter domain(y/n): n
    Let's register a new NeoRouter domain.
    Enter domain name: nrdemo01
    Enter domain password:
    Enter domain password again:
    Enter first name: Joe
    Enter last name: Smith
    Enter email address: joesmith@neorouter.com
    Domain setup succeeded.

Step 2 - Setup Administrator Account:
    NeoRouter can defer authentication to the operating system. If your OS user
account has a non-empty password, you can use the same username/password to logi
n NeoRouter and can skip this step.
    Do you want to create an administrator account? (y/n): y
    Enter username: joe
    Enter password:
    Enter password again:
    Administrator account setup succeeded.

Step 3 - Setup Port Forward as necessary:
    NeoRouter server listens at port 32976. Please make sure it can receive incomin
g connections from Internet. If NeoRouter server is behind a NAT, please setup port
 forward. You can use http://www.neorouter.com/checkport.php to verify the settings
.

NeoRouter Server Setup succeeded.
    You can make additional configuration changes using Configuration Explorer or n
rserver CLI.
    You can find more information in User's Manual (http://www.neorouter.com/Docume
nts.html).
```

2.2.9 Create first administrator account

On Windows, the install wizard will guide user to create the administrator.

On non-Windows platforms, NeoRouter can defer the authentication to the OS. So user can sign in NeoRouter using the same username and password as he/she logs into OS. An exception is that if user’s OS account does not have a password, NeoRouter will not allow he/she to log in. In this case user must create the first administrator account using nrserver CLI: “nrserver -adduser <username> <password> [admin|user]”. On Mac nrserver is located under “/Library/NeoRouter/”.

2.2.10 Setup NeoRouter domain

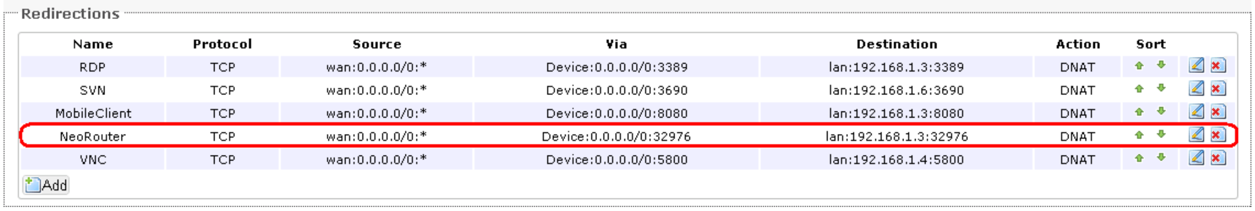
This step is only necessary on non-Windows platforms, because Windows install wizard does this automatically.

1. Launch web browser, navigate to Dashboard CreateDomain page https://www.neorouter.com/Dashboard/CreateDomain.aspx, fill the form and click Save.
2. Open a terminal on the server host and execute “nrserver -setdomain <domain name> <domain password>”. On Mac nrserver is located under “/Library/NeoRouter/”.

2.2.11 Port forwarding

This step is only necessary if your server host is behind a router or firewall. We need to expose the NeoRouter server port to Internet so server can accept incoming connections from the NeoRouter clients. If you are using NeoRouter in-a-box version and your router is directly connected to the cable/DSL modem, this step is unnecessary.

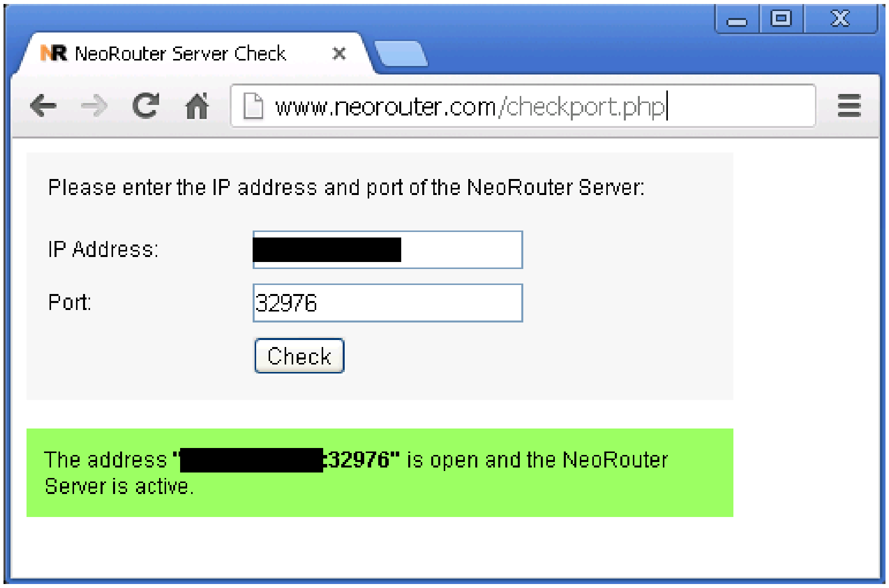
1. Assign the server host a static LAN IP address
2. Add <server host IP, port 32976> to Port Forwarding list. NeoRouter server listens at port 32976 by default and admin can change the port number using Configuration Explorer or nrserver CLI.



Redirections

Name	Protocol	Source	Via	Destination	Action	Sort	
RDP	TCP	wan:0.0.0.0/0:*	Device:0.0.0.0/0:3389	lan:192.168.1.3:3389	DNAT	↑ ↓	✎ ✖
SVN	TCP	wan:0.0.0.0/0:*	Device:0.0.0.0/0:3690	lan:192.168.1.6:3690	DNAT	↑ ↓	✎ ✖
MobileClient	TCP	wan:0.0.0.0/0:*	Device:0.0.0.0/0:8080	lan:192.168.1.3:8080	DNAT	↑ ↓	✎ ✖
NeoRouter	TCP	wan:0.0.0.0/0:*	Device:0.0.0.0/0:32976	lan:192.168.1.3:32976	DNAT	↑ ↓	✎ ✖
VNC	TCP	wan:0.0.0.0/0:*	Device:0.0.0.0/0:5800	lan:192.168.1.4:5800	DNAT	↑ ↓	✎ ✖

3. Check the server availability



Please enter the IP address and port of the NeoRouter Server:

IP Address: [redacted]

Port: 32976

The address "[redacted]:32976" is open and the NeoRouter Server is active.

2.2.12 IPv6

NeoRouter (v1.5 or above) supports IPv6 for the underlying client-server and peer-to-peer connections. So you can install NeoRouter client on computers or devices with public or NAT'd IPv4, public IPv6, or dual stacks, and connect all of them into a virtual LAN. You no longer need to worry about how and when your ISPs will switch their services to IPv6. The virtual LAN uses IPv4 virtual addresses, so your existing software will continue to function and you do not need to make expensive upgrades just for IPv6 support.

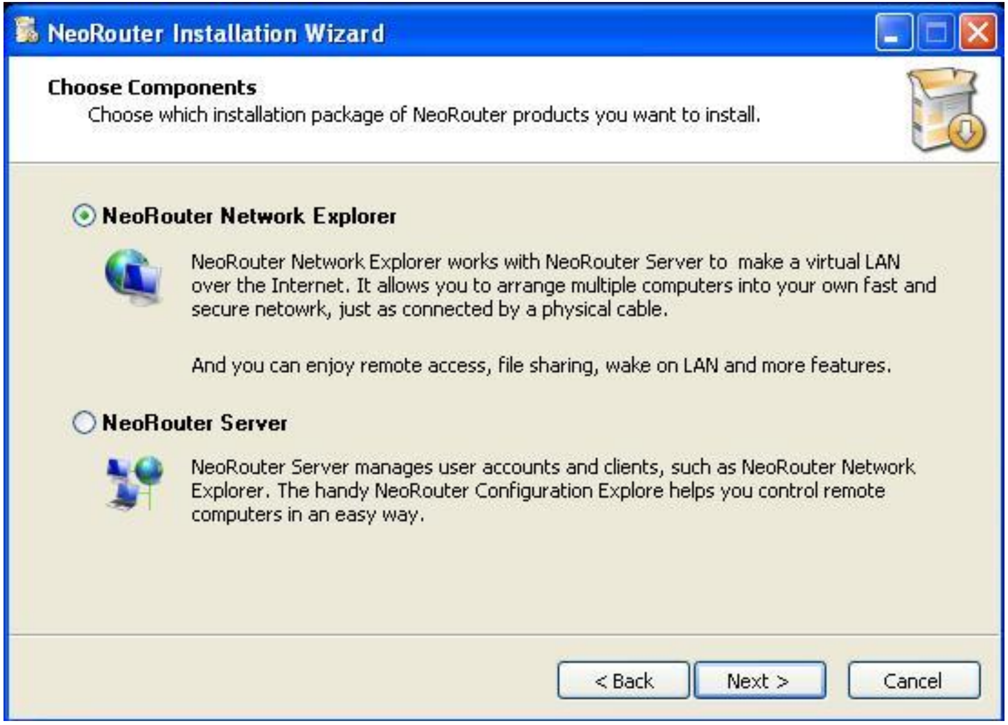
NeoRouter IPv6 support is available on all platforms except for Android and Tomato, and it is on by default. You only need to make sure the server host has both IPv4 and IPv6 public addresses. If your ISP does not provide IPv6 service yet, you can use a Tunnel Broker like SixXS, gogo6, or Hurrican Electric. No changes are needed on NeoRouter client computers.

Direct P2P connection can be established between two IPv4 computers or two IPv6 computers. Connection between an IPv4 only computer and an IPv6 only computer is relayed through NeoRouter server.

2.3 Client Setup

2.3.1 Install NeoRouter Client on Windows

1. Download NeoRouter installation package for Windows. NeoRouter server and client for Windows share the same installation package.
   If you are installing on Windows 2000, please download the special package for this OS.
2. If you have installed an earlier version of NeoRouter, please uninstall it using Windows Add or Remove Program tool.
3. Run the installation wizard, choose NeoRouter Client, and click the Next button.



NeoRouter Installation Wizard

Choose Components

Choose which installation package of NeoRouter products you want to install.

● **NeoRouter Network Explorer**

NeoRouter Network Explorer works with NeoRouter Server to make a virtual LAN over the Internet. It allows you to arrange multiple computers into your own fast and secure netowrk, just as connected by a physical cable.

And you can enjoy remote access, file sharing, wake on LAN and more features.

○ **NeoRouter Server**

NeoRouter Server manages user accounts and clients, such as NeoRouter Network Explorer. The handy NeoRouter Configuration Explore helps you control remote computers in an easy way.

4. On Vista and above, you may be prompted with a security warning because NeoRouter installs a virtual network adapter. Please allow the installer to proceed.
5. Follow the wizard to complete installation.
6. NeoRouter Network Explorer and Configuration Explorer are added to Windows Start menu.

7. NeoRouter is installed under “%Program Files%\ZebraNetworkSystems\NeoRouter” and user data is stored under “%AllUsersAppdata%\ZebraNetworkSystems\NeoRouter”.
8. NeoRouter client service daemon can be controlled in Services Console (services.msc).

2.3.2 Install NeoRouter Client on Mac

1. Download NeoRouter client for Mac.
2. If you have installed an earlier version of NeoRouter, please uninstall it: In a terminal, execute command "sudo /Library/NeoRouter/rmnrclient.sh".
3. Double-click nrclient-<version>-<release>.dmg to open the disk image in Finder.
4. Double-click tuntap-<version>.pkg to install virtual network interface kernel extension.
5. Double-click NeoRouterClient.mpkg to install NeoRouter client.
6. On Leopard or above, NeoRouter Network Explorer is installed to the Applications folder.
7. On PPC Tiger, a shortcut (nrclientcmd) is created on the Desktop and double-click it will launch Network Explorer CLI.
8. NeoRouter is installed under /Applications/NeoRouter.app and /Library/NeoRouter/ folder and user data is stored under /usr/local/ZebraNetworkSystems/NeoRouter.

2.3.3 Install NeoRouter Client on Android

Please visit http://www.neorouter.com/android/.

2.3.4 Install NeoRouter Client on Linux

1. Download NeoRouter Client for your Linux distribution.
2. If you have installed an earlier version of NeoRouter, please uninstall it:
   Redhat and Fedora: sudo rpm -e nrclient
   SuSE: sudo rpm -e nrclient
   Ubuntu, Debian and Raspbian: sudo dpkg -r nrclient
3. Install:
   RedHat and Fedora: sudo rpm -i nrclient-<version>-<release>.i386.rpm
   SuSE: sudo rpm -i nrclient-<version>-<release>.i386.rpm
   Ubuntu and Debian: sudo dpkg -i nrclient-<version>-<release>.i386.deb
   Raspbian: sudo dpkg -i nrclient-<version>-<release>.armhf.deb
4. Configure firewall for P2P connection (Optional)
   Establishing direct P2P connection on Linux requires user to disable firewall. Otherwise all connections to this client will be relayed via server. User must evaluate the trade-offs between performance and security. If this client is always physically located inside a trusted network, like office or home LAN, we recommend disabling firewall and allow P2P connection. If this client is physically located in an un-trusted network, like airport or coffee shop, we recommend enabling firewall and relay all traffic via server.
5. Run /usr/bin/nrclientcmd to launch Network Explorer CLI.
6. NeoRouter is installed under /usr/bin and user data is stored under /usr/local/ZebraNetworkSystems/NeoRouter.
7. (Rare) Run ifconfig and check whether the computer has an Ethernet interface named eth*. For example, Fedora HyperV may name its Ethernet interface seth*. If your computer does not have eth*, please edit /usr/local/ZebraNetworkSystems/NeoRouter/Feature.ini and enter:
   ```
   [default]
   NicInterfaceName="seth"
   ```
8. (Optional) consider adding a cron job that automatically restarts nrservice in case it crashes.
   Using Ubuntu as an example, you can edit /etc/crontab and add “*/5 * * * * root /etc/init.d/nrservice.sh start”.

2.3.5 Install NeoRouter Client on FreeBSD

1. Download NeoRouter Client for FreeBSD.

2. If you have installed an earlier version of NeoRouter, please uninstall it:

   ```
   su as root and run rmnrclient.sh
   ```
3. Install:

   ```
   Copy the downloaded package to /tmp
   cd /tmp; tar zxvf nrclient*.tgz
   cd /tmp/nrclient
   su as root and make install
   ```
4. (Optional) consider adding a cron job that automatically restarts nrservice in case it crashes.

2.3.6 Install NeoRouter Client on OpenWRT Backfire

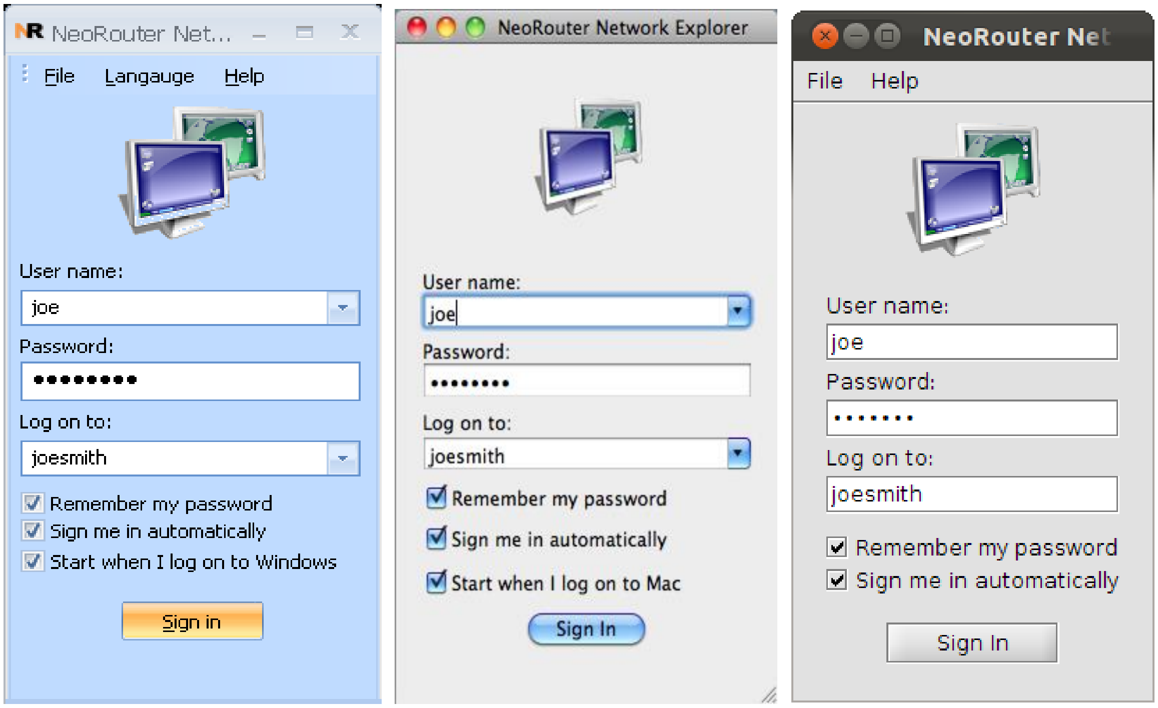
1. Connect to the router using ssh or telnet
2. Update available install packages using command: opkg update
3. If you have installed an earlier version of NeoRouter, please uninstall it: opkg uninstall nrclient
4. Install: opkg install http://www.neorouter.com/Downloads/...Backfire/nrclient_<version>-<release>_mipsel.ipk
5. Configure firewall for P2P connection (Optional)
   Please read NeoRouter client installation instructions for Linux and evaluate the trade-off between performance and security. If you decide to turn off firewall, here is the instruction:
   edit /etc/firewall.user and add the following:

   ```
   iptables -t nat -A prerouting_wan -p tcp -j ACCEPT
   iptables        -A input_wan      -p tcp -j ACCEPT
   iptables -t nat -A prerouting_wan -p udp -j ACCEPT
   iptables        -A input_wan      -p udp -j ACCEPT
   ```
6. Run /usr/bin/nrclientcmd to launch Network Explorer CLI.
7. NeoRouter is installed under /usr/bin and user data is stored under /usr/local/ZebraNetworkSystems/NeoRouter.
8. Turn your router into a file or backup server (Optional)
   If your router has 8MB or more flash, there should be enough space left for other packages. You can enable USB storage and Samba server, and turn your router into a file server. Or you can install rsync and turn it into a backup server. NeoRouter's remote access and VPN service will allow you to securely access the files from anywhere. This solution is a lot cheaper than Small Business server or Windows Home server.
   Enable USB Storage: http://nuwiki.openwrt.org/oldwiki/usbstoragehowto
   Install Samba: http://wiki.openwrt.org/oldwiki/sambahowto
   Install rsync: http://oldwiki.openwrt.org/rsync(2d)usb(2d)sambaHowTo.html

3. Network Explorer

3.1 Launch and Sign In

1. On Windows, launch NeoRouter Network Explorer from "Windows Start Menu | All Programs | NeoRouter | NeoRouter Network Explorer".
   On Mac Leopard or above, launch NeoRouter Network Explorer from Applications folder. You can also pin NeoRouter to the dock.
   On Linux or FreeBSD, launch NeoRouter Network Explorer by command “nrclient.sh”. (Note: Java 1.6+ is required on Linux or FreeBSD to launch the GUI client)



User name: joe
Password: ••••••••
Log on to: joesmith
☑ Remember my password
☑ Sign me in automatically
☑ Start when I log on to Windows

User name: joe
Password: ••••••••
Log on to: joesmith
☑ Remember my password
☑ Sign me in automatically
☑ Start when I log on to Mac

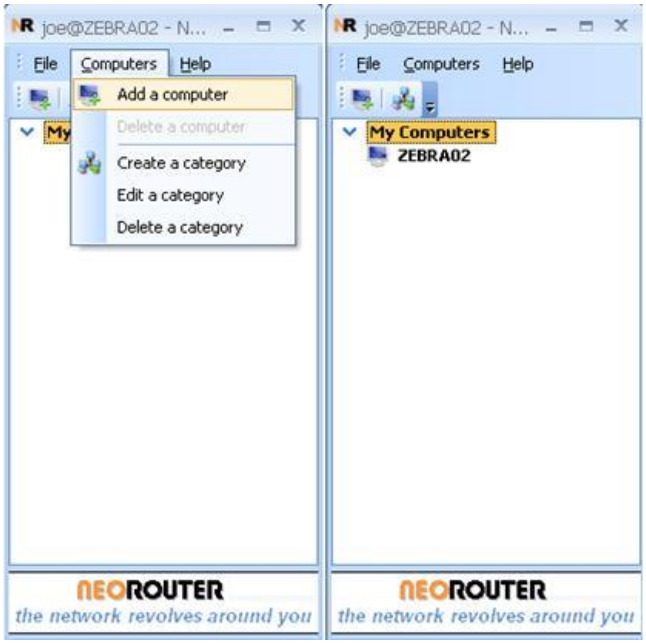
User name: joe
Password: •••••••
Log on to: joesmith
☑ Remember my password
☑ Sign me in automatically

2. Enter user credential.
   - If NeoRouter server is installed on Windows, please use the administrator account created during server setup.
   - If NeoRouter server is installed on other platforms, NeoRouter can defer the authentication to the operating system, so user can sign in using the same username and password as he/she logs into OS.
   - User can also use the additional accounts created in Configuration Explorer or server CLI.
   - If you are invited to a NeoRouter domain, please contact the administrator for your account information.
3. In the "Log on to" field, enter the domain name you have chosen during server setup. Alternatively you can enter the server’s IP address or computer name. You can also enter "localhost" if the Network Explorer is on the same host as the server.
4. If the client host is behind proxy, please choose Menu “File | Connections” to bring up the Connection Options dialog, click Proxy Setting tab, and then set proxy information.
5. Click the "Sign In" button.

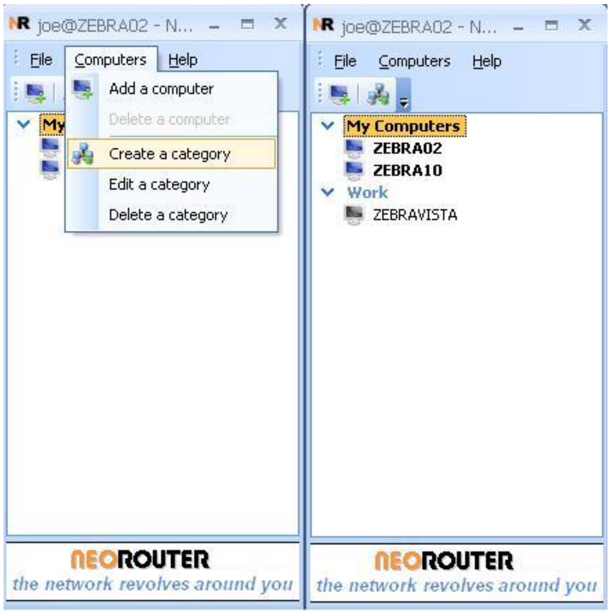
3.2 Computer List

The computer list is your view of the VLAN. By default, NeoRouter will manage the computer list for you and display all computers in your domain. If you have a large number of computers, you can switch to the personalized view mode (choose menu “Computers | Show Personalized View”) and organize according to your preference.

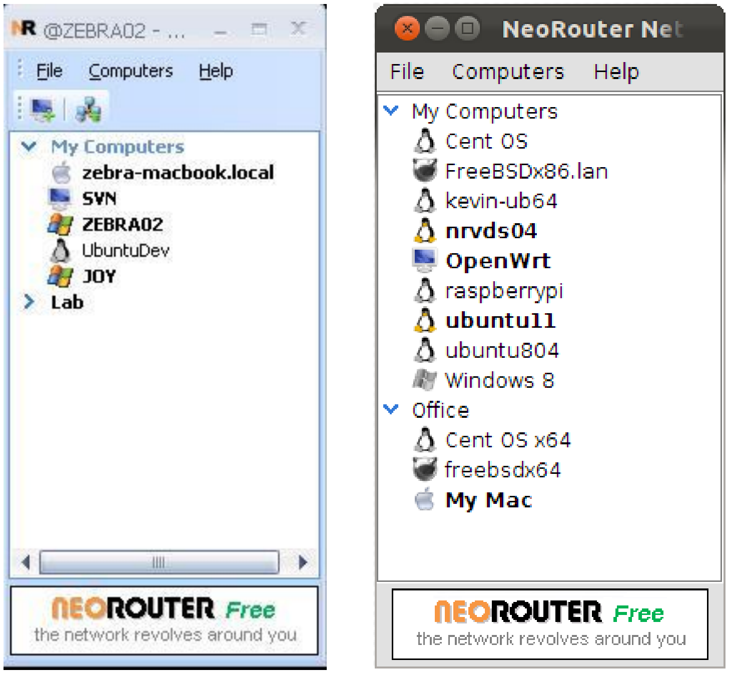
With Personalized view, you will always have the same list regardless where you sign in from. Each user will have his/her personalized view.
Initially, you will see an empty computer list (see the left picture below). To add a computer, you can choose the menu "Computers | Add a computer", and then select the computer and category in the dialog. Once complete, your computer list will be updated (see the right picture below).



You can use categories to help manage a long list of computers. To create a category, you can choose menu "Computers | Create a category". To move a computer to a different category, you can simply drag and drop.



Starting in release v0.9.8, the computer list shows the OS type icons next to a computer name. If a computer is online, its icon is colourful and its name is bold. If a computer is offline, its icon is grey and its name is not bold.

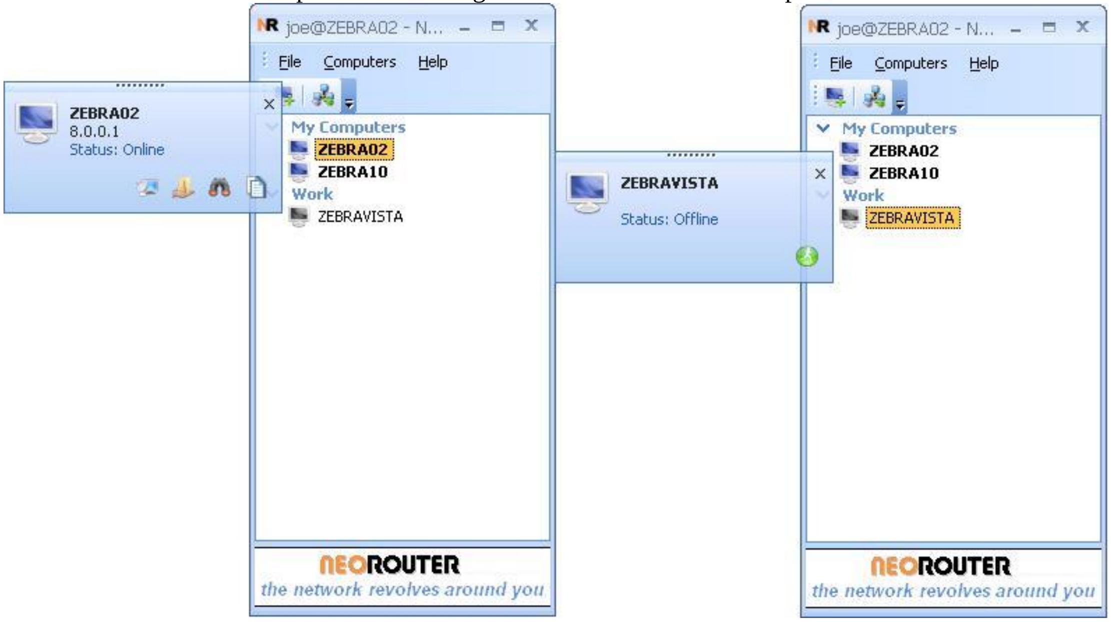


3.3 *Add-on*

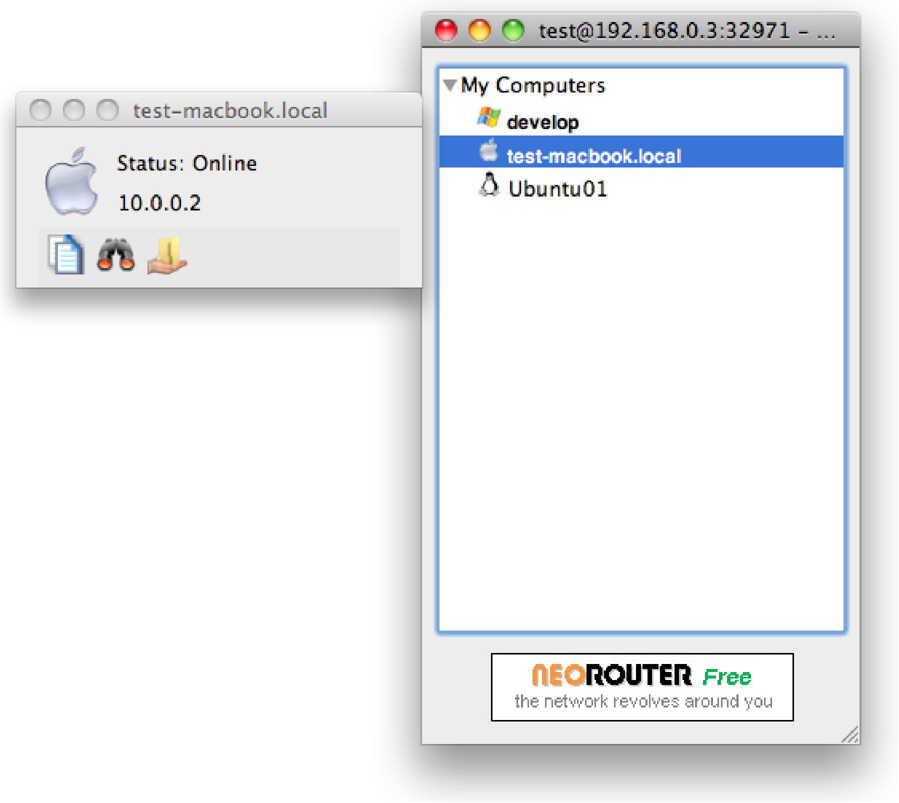
Add-ons extend NeoRouter Network Explorer and let you perform additional tasks over the virtual network.

3.3.1 Add-on launch pad

If you click on a computer in the computer list, a popup dialog will display a list of actions you can take to remotely control and access this computer. This dialog is called the add-on launch pad.



Screenshots on Windows



Screenshot on Mac

NeoRouter Network Explorer has a few system default add-ons. If a computer is online, the following add-ons are available:

Icon	Action
🖥	remote desktop connection
📂	file sharing
🔭	ICMP ping
📋	copy the IP address
🔑	Ssh client
VNC	Vnc clinet
➡	Sftp client

If a computer is offline, the following add-ons are supported:

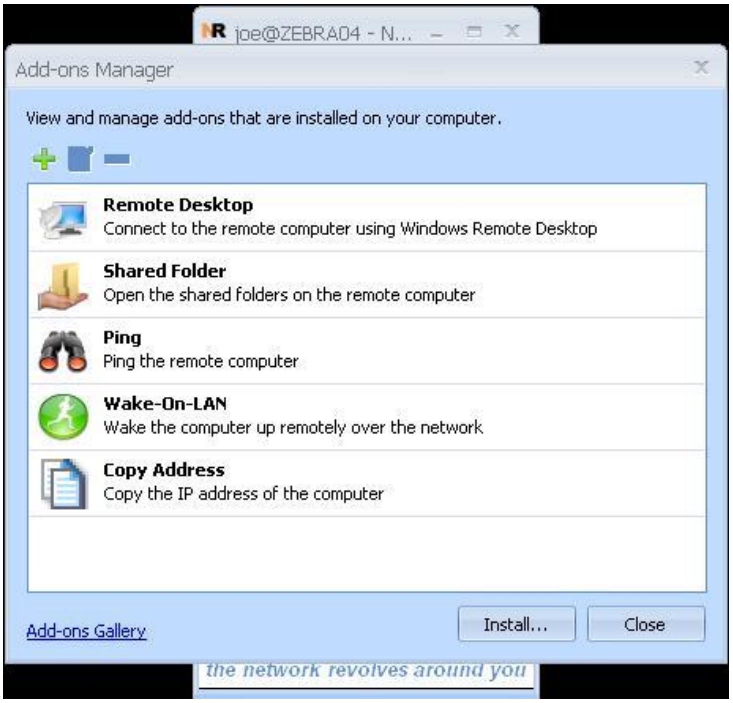
Icon	Action
⏻	remote wakeup (WOL)

Note on remote wakeup: NeoRouter server can send the Magic packet and wake up hosts that are WOL enabled. If the NeoRouter server is installed on a router, remote wakeup works for hosts directly attached to this router. If server is installed on Windows, Linux or Mac, remote wakeup works for hosts in the same physical LAN. Since v2.0, an active NeoRouter client can also wake up offline hosts in the same physical LAN. To enable WOL, you may need to change BIOS and OS settings.

3.3.2 Manage Add-ons (Windows)

You can download additional add-ons from the NeoRouter download website (http://www.neorouter.com/addons/index.html) and install them using the Add-on Manager. Here we use UltraVNC as an example to explain the setup process.

1. Launch NeoRouter Network Explorer; choose menu "File - Add-ons".
2. The Add-ons Manager dialog lists all the existing add-ons, including system default ones and those installed by user.



View and manage add-ons that are installed on your computer.

Remote Desktop
Connect to the remote computer using Windows Remote Desktop

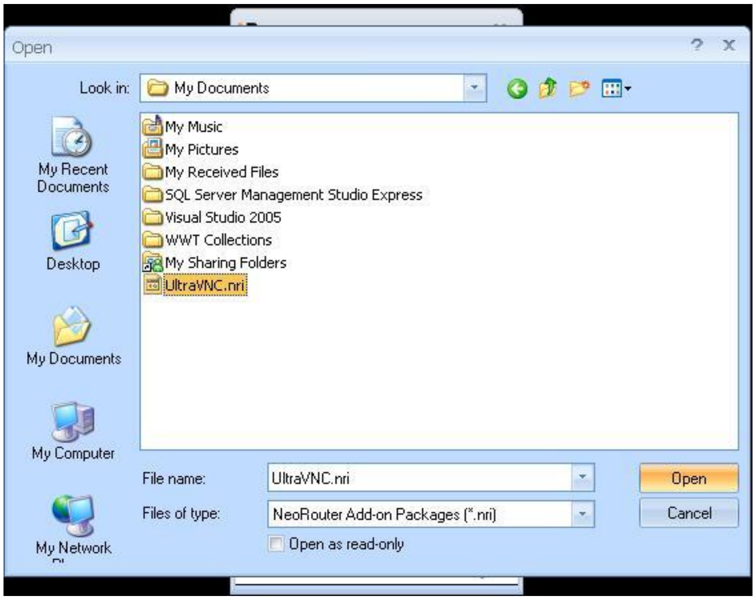
Shared Folder
Open the shared folders on the remote computer

Ping
Ping the remote computer

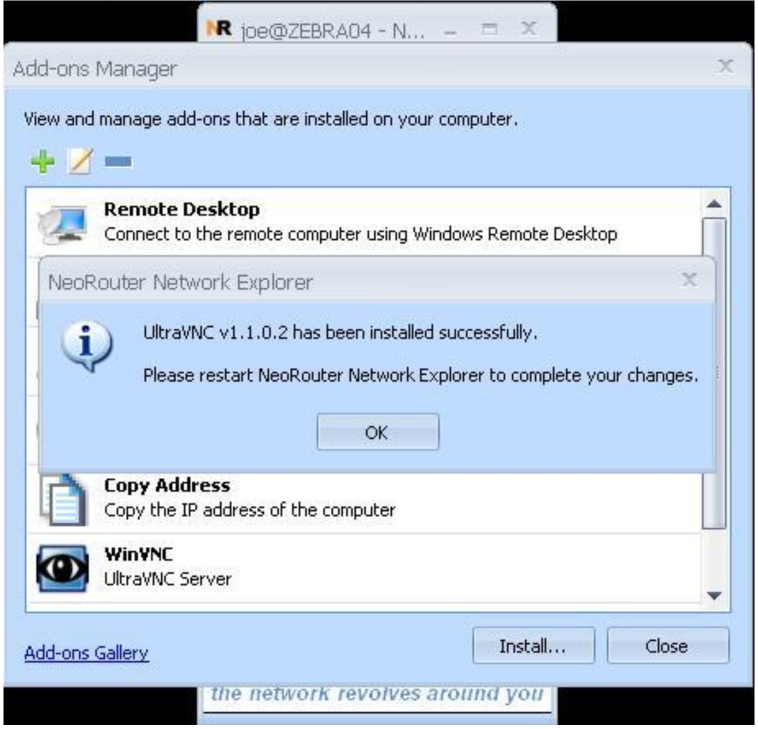
Wake-On-LAN
Wake the computer up remotely over the network

Copy Address
Copy the IP address of the computer

3. To find more add-ons, click on the "Add-ons Gallery" link at the bottom of the dialog, or visit http://www.neorouter.com/addons/index.html in your web browser. Download the add-on (*.nri) file to your computer.
4. In the Add-ons Manager dialog, click on "Install..." button, locate the *.nri file you just downloaded, and click "Open" to install the add-on.



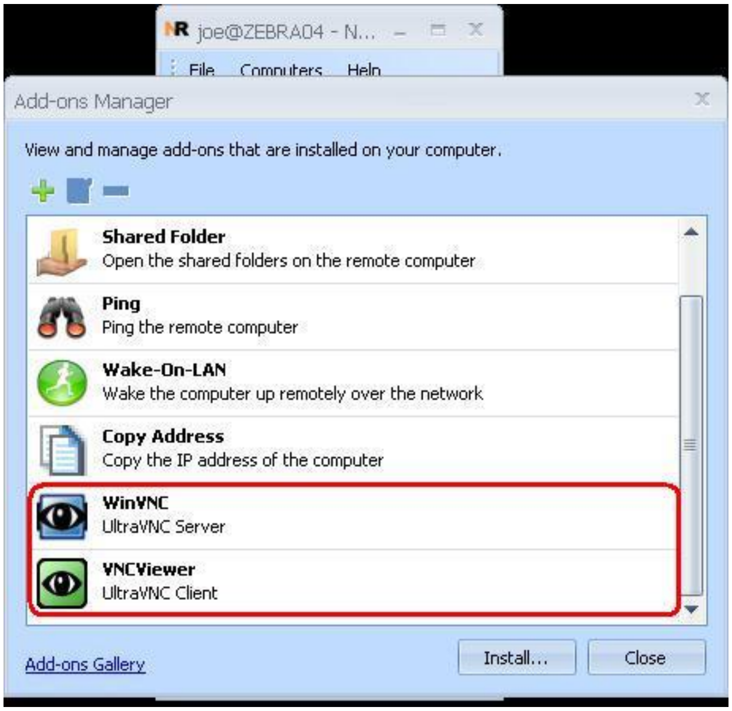
5. Some add-ons, including UltraVNC, may require user to restart the NeoRouter Network Explorer to complete the installation. In such case you will see the following message box. You can exit NeoRouter Network Explorer by right click its icon in system tray and choose exit.


joe@ZEBRA04 - N...
Add-ons Manager
View and manage add-ons that are installed on your computer.
Remote Desktop
Connect to the remote computer using Windows Remote Desktop
NeoRouter Network Explorer
OK
Copy Address
Copy the IP address of the computer
WinVNC
UltraVNC Server
Add-ons Gallery
Install...
Close
the network revolves around you

UltraVNC v1.1.0.2 has been installed successfully.

Please restart NeoRouter Network Explorer to complete your changes.

6. After installation, you will see the new add-ons show up in the list.



View and manage add-ons that are installed on your computer.

Shared Folder
Open the shared folders on the remote computer

Ping
Ping the remote computer

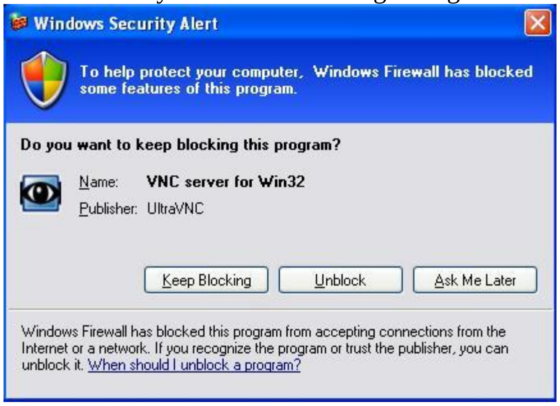
Wake-On-LAN
Wake the computer up remotely over the network

Copy Address
Copy the IP address of the computer

WinVNC
UltraVNC Server

VNCViewer
UltraVNC Client

7. When you re-launch NeoRouter Network Explorer, UltraVNC server will be started automatically. If you have not run UltraVNC server before, you will see the following firewall warning and VNC configuration dialog.
8. Please click the unblock button when you see the following dialog.



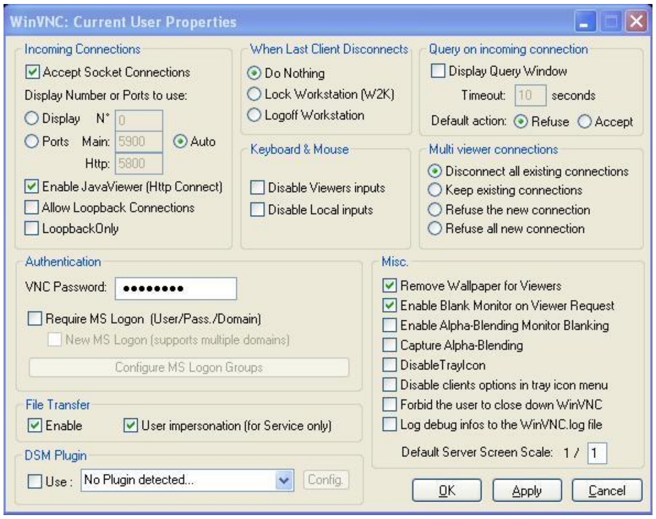
To help protect your computer, Windows Firewall has blocked some features of this program.

Do you want to keep blocking this program?

Name: VNC server for Win32
Publisher: UltraVNC

Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

Please enter VNC password then click the Ok button.



WinVNC: Current User Properties

Incoming Connections
☑ Accept Socket Connections
Display Number or Ports to use:
○ Display N° 0
○ Ports Main: 5900 ● Auto
Http: 5800
☑ Enable JavaViewer (Http Connect)
☐ Allow Loopback Connections
☐ LoopbackOnly

When Last Client Disconnects
● Do Nothing
○ Lock Workstation (W2K)
○ Logoff Workstation

Query on incoming connection
☐ Display Query Window
Timeout: 10 seconds
Default action: ● Refuse ○ Accept

Keyboard & Mouse
☐ Disable Viewers inputs
☐ Disable Local inputs

Multi viewer connections
● Disconnect all existing connections
○ Keep existing connections
○ Refuse the new connection
○ Refuse all new connection

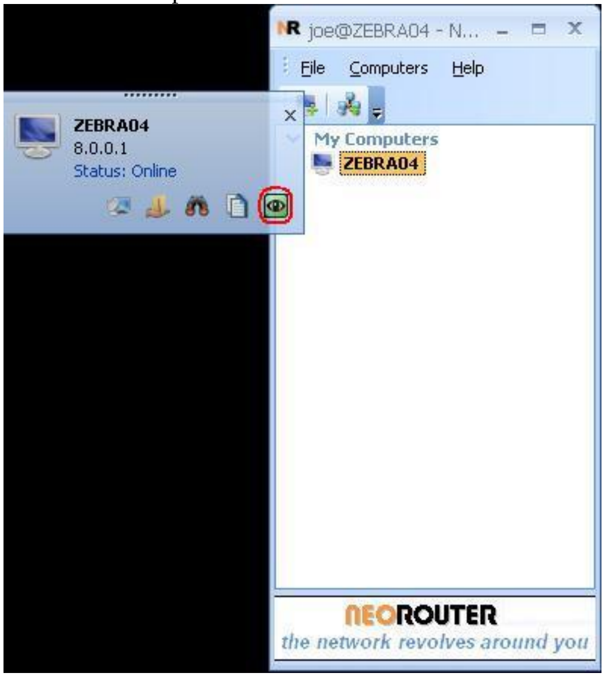
Authentication
VNC Password: ••••••••
☐ Require MS Logon (User/Pass./Domain)
☐ New MS Logon (supports multiple domains)
Configure MS Logon Groups

Misc.
☑ Remove Wallpaper for Viewers
☑ Enable Blank Monitor on Viewer Request
☐ Enable Alpha-Blending Monitor Blanking
☐ Capture Alpha-Blending
☐ DisableTrayIcon
☐ Disable clients options in tray icon menu
☐ Forbid the user to close down WinVNC
☐ Log debug infos to the WinVNC.log file
Default Server Screen Scale: 1 / 1

File Transfer
☑ Enable ☑ User impersonation (for Service only)

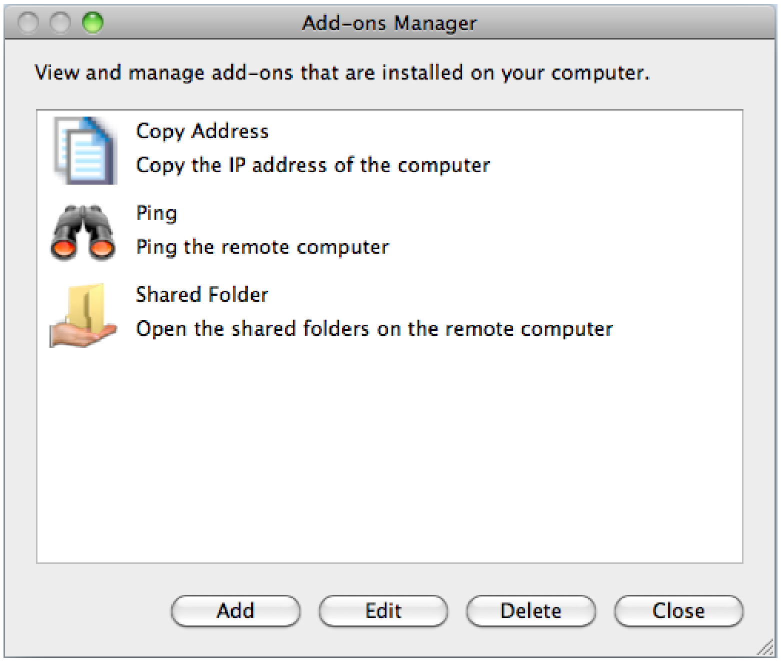
DSM Plugin
☐ Use : No Plugin detected... Config.

9. Repeat the above steps on the remote computer that you plan to access.
10. To launch VNC viewer and access the remote computer, choose the computer in the computer list, and click VNC viewer icon in the launch pad.



3.3.3 Manage Add-ons (Mac)

1. Launch NeoRouter Network Explorer; choose menu "File - Add-ons".
2. The Add-ons Manager dialog lists all the existing add-ons, including system default ones and those added by user.



Add-ons Manager

View and manage add-ons that are installed on your computer.

Copy Address
Copy the IP address of the computer

Ping
Ping the remote computer

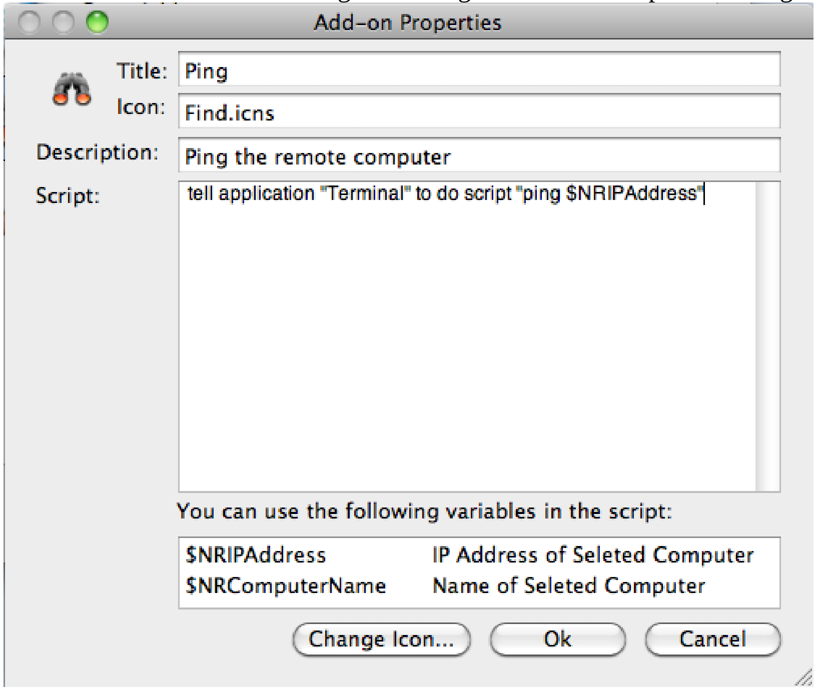
Shared Folder
Open the shared folders on the remote computer

3. An add-on is essentially an apple script with NeoRouter parameters. Here are some examples:

Name	Script
Copy IP	set the clipboard to "$NRIPAddress"
Ping	tell application "Terminal" to do script "ping $NRIPAddress"
Shared Folder	tell application "Finder" to open location "smb://$NRIPAddress"

Variables $NRIPAddress and $NRComputerName will be replaced with the IP and name of the selected computer before the add-on is executed.

4. You can also create new add-ons or edit existing ones using the Add-On Properties dialog.



Add-on Properties

Title: Ping

Icon: Find.icns

Description: Ping the remote computer

Script:

```
tell application "Terminal" to do script "ping $NRIPAddress"
```

You can use the following variables in the script:

$NRIPAddress	IP Address of Seleted Computer
$NRComputerName	Name of Seleted Computer

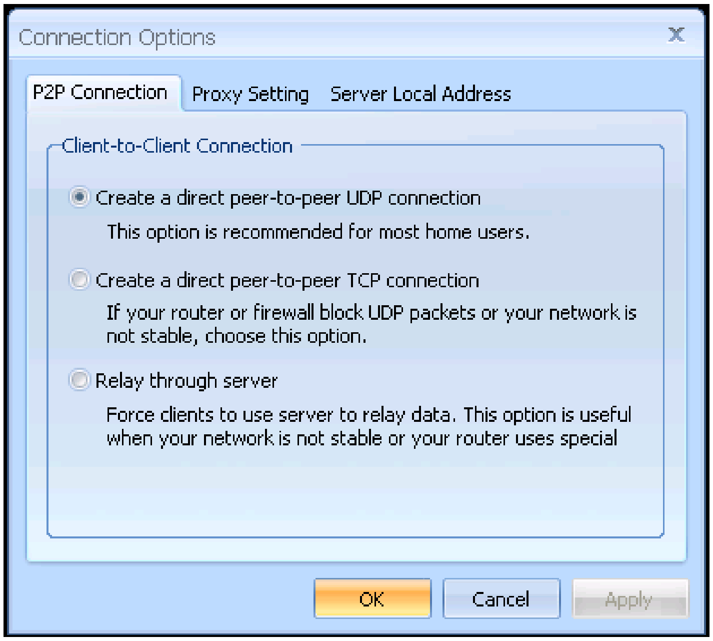
5. To learn more about Apple Script, please visit the following websites:
    - http://en.wikipedia.org/wiki/AppleScript
    - http://developer.apple.com/mac/library/documentation/AppleScript/Conceptual/AppleScriptX/AppleScriptX.html

3.4 Connection Options

Connection Options dialog can be opened from Network Explorer menu “File | Connection”.

3.4.1 P2P Connection

This option allows user to specify the connection type between this computer and its peers. The default option is UDP. User can also use direct TCP connection or relay traffic through NeoRouter server.



Client-to-Client Connection

● Create a direct peer-to-peer UDP connection

This option is recommended for most home users.

○ Create a direct peer-to-peer TCP connection

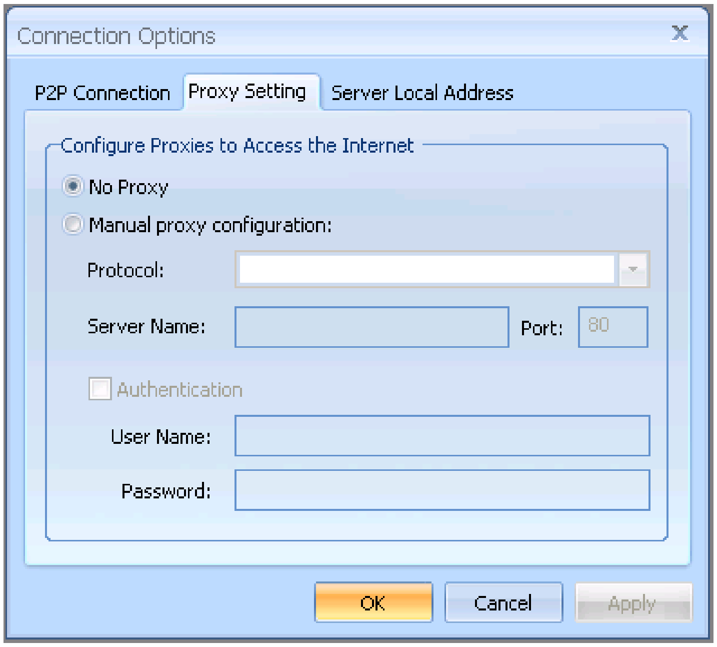
If your router or firewall block UDP packets or your network is not stable, choose this option.

○ Relay through server

Force clients to use server to relay data. This option is useful when your network is not stable or your router uses special

3.4.2 Proxy Setting

If the client host is behind proxy, user can enter the proxy information here.



Connection Options

P2P Connection | Proxy Setting | Server Local Address

Configure Proxies to Access the Internet

● No Proxy

○ Manual proxy configuration:

Protocol:

Server Name:

Port: 80

□ Authentication

User Name:

Password:

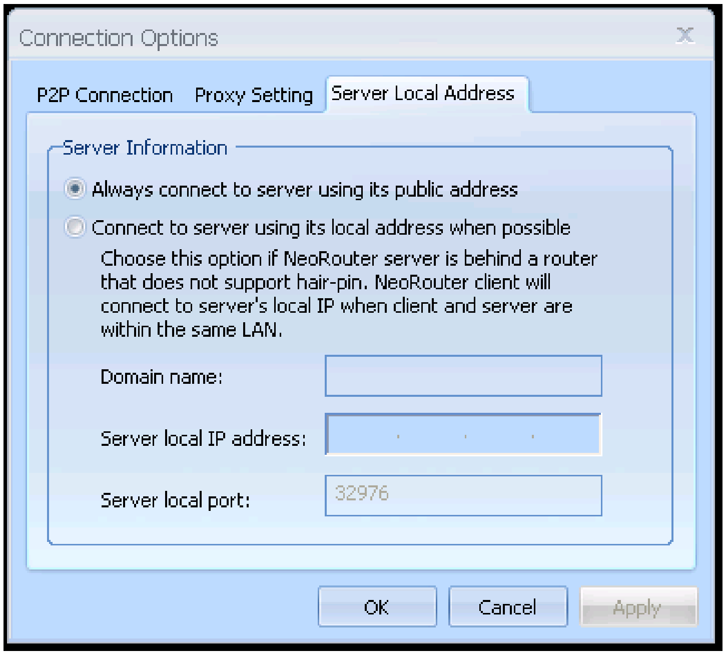
3.4.3 Server Local Address

This option can be used to work around the connectivity issue when NeoRouter server is behind a router that does not support hairpin.

A router supports hairpin if it allows a host behind it to send network messages to its public-facing interface. Unfortunately some popular routers do not support this feature or turn off this feature by default.

When user logs into NeoRouter, Network Explorer first translates domain name into router's public address using the NeoRouter DDNS service, and then tries to connect to server using this address. If both NeoRouter server and client are behind the same router and the router does not support hairpin, the router will block the messages that client sends to the router's public address, thus client fails to establish connection to server. User could work around this issue by entering server's LAN IP address instead of domain name in the "log on to" box, but this can be a hassle for laptop users who frequently move between networks.

These users can choose the second option "Connect to server using its local address when possible" in the following dialog and enter server's local address. NeoRouter Network Explorer can detect when client and server are behind the same router and automatically choose the specified local address to establish the connection to server.



Connection Options

P2P Connection | Proxy Setting | Server Local Address

Server Information

● Always connect to server using its public address

○ Connect to server using its local address when possible

Choose this option if NeoRouter server is behind a router that does not support hair-pin. NeoRouter client will connect to server's local IP when client and server are within the same LAN.

Domain name:

Server local IP address: . . .

Server local port: 32976

3.5 Multi-Language

Multi-Language support allows you to change the default language displayed in Network Explorer, NeoRouter Portable and Configuration Explorer.

3.5.1 Install a language resource file

NeoRouter applications support 34 languages and English is the default. To install a new language, you can download the language resource files from http://www.neorouter.com/wiki/index.php/NeoRouterWiki:Multilanguage and place them under the translation folder. Then the application will load them and list all available languages in the "Language" menu. You can switch language in the menu and the application will refresh its UI with the new language.

For NeoRouter Network Explorer and Configuration Explorer, the language resource files should be placed under one of the following folders:

- “%Program Files%\ZebraNetworkSystems\NeoRouter\Translation\”
- “%AllUsersAppdata%\ZebraNetworkSystems\NeoRouter\Translation\”

For NeoRouter Portable/USB, the language resource file should be placed under .\Translations\ folder next to application.

3.5.2 Language resource file format

The file name should have the following format. [Appliation Name] can be: NRClient, NRViewer and NRConsole; [LangCd] is the short language code.

[Application name].Resource[LangCd].[xml|dll]

For example, Simplified Chinese version has the following files: NRClient.ResourceZhCn.xml for Network Explorer, NRConsole.ResourceZhCn.xml for Configuration Explorer and NRViewer.ResourceZhCn.xml for NeoRouter Portable.

Each resource file is an xml that contains all the strings defined in the NeoRouter applications. The file is encoded in ANSI. The content should be in the format:

```
<?xml version="1.0" encoding="windows-1252"?>

<resource CompactMode="1" Language="English (United States)" LANGID="1033"
version="0.9.10.1650">

        <string id="100" value="OLE initialization failed.  Make sure that the OLE libraries are
the correct version."/>

...

</resource>
```

Encoding (="windows-1252"), Language(="English (United States)") and LANGID(="1033") are used to control the translation. version="0.9.10.1650" is resource file version number introduced in v0.9.10. The resource file can be recognized properly only when these parameters are set properly.

3.5.3 Multi-Language support for Add-ons

The names and descriptions of the add-ons can be translated to other languages as well. You can download the add-on configuration file from NeoRouter website and overwrite the following file:

%AllUserAppData%\ZebraNetworkSystems\NeoRouter\AddOns\AddOn.xml.

3.6 Skin

Skin allows you to further customize the user interfaces of Network Explorer, NeoRouter Portable and Configuration Explorer.

To install a new skin, you can download the skin resource file from http://www.neorouter.com/wiki/index.php/NeoRouterWiki:Skin, and place them under the skin folder.

For NeoRouter Network Explorer and Configuration Explorer, the language resource files should be placed under one of the following folders:

- “%Program Files%\ZebraNetworkSystems\NeoRouter\Skin\”
- “%AllUsersAppdata%\ZebraNetworkSystems\NeoRouter\Skin\”

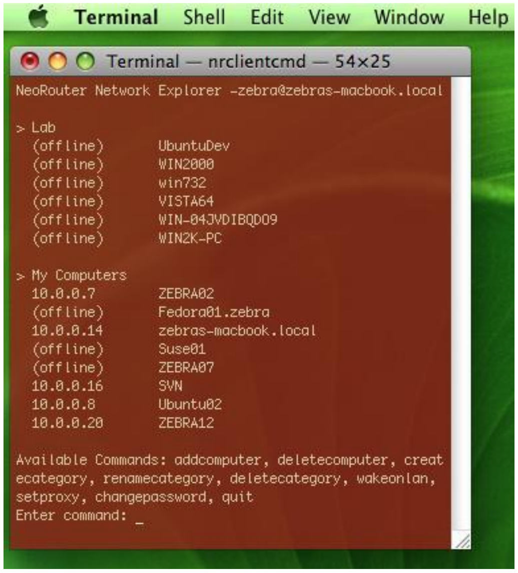
For NeoRouter Portable/USB, the language resource file should be placed under .\Skin\ folder next to executable.

To change default skin, you need to modify (or create if not exists) %AllUserAppData%\ZebraNetworkSystems\NeoRouter\Feature.ini file and add the following:

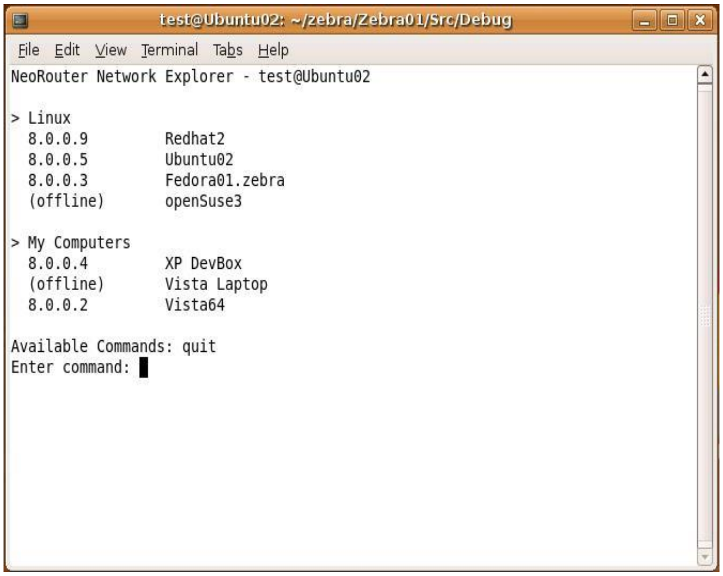
```
[Default]

SkinName=xxxx.styles

SkinStyle=xxxx.ini
```

3.7 Network Explorer CLI

NeoRouter Network Explorer Command Line Interface (CLI) allows user to sign in, manage the computer list and view computer status. Below are the screenshots on Mac and Ubuntu Linux.



```
NeoRouter Network Explorer -zebra@zebras-macbook.local

> Lab
  (offline)       UbuntuDev
  (offline)       WIN2000
  (offline)       win732
  (offline)       VISTA64
  (offline)       WIN-04JVDIBQDO9
  (offline)       WIN2K-PC

> My Computers
  10.0.0.7        ZEBRA02
  (offline)       Fedora01.zebra
  10.0.0.14       zebras-macbook.local
  (offline)       Suse01
  (offline)       ZEBRA07
  10.0.0.16       SVN
  10.0.0.8        Ubuntu02
  10.0.0.20       ZEBRA12

Available Commands: addcomputer, deletecomputer, creat
ecategory, renamecategory, deletecategory, wakeonlan,
setproxy, changepassword, quit
Enter command: _
```



```
NeoRouter Network Explorer - test@Ubuntu02

> Linux
  8.0.0.9        Redhat2
  8.0.0.5        Ubuntu02
  8.0.0.3        Fedora01.zebra
  (offline)      openSuse3

> My Computers
  8.0.0.4        XP DevBox
  (offline)      Vista Laptop
  8.0.0.2        Vista64

Available Commands: quit
Enter command: █
```

3.7.1 Launch CLI

Usage: nrclientcmd [-d DOMAIN] [-u USERNAME] [-p PASSWORD] [-setproxy] [-setconn] [-dbroot DBROOT] [-internal] [--help]

To launch Network Explorer CLI, you can simply run nrclientcmd in a terminal without parameters. Mac users can simply double-click on the nrclientcmd shortcut on the Desktop. You will be prompted for domain name and user credential.

If you need to launch nrclientcmd in a startup script, you can also provide domain name or credential in the command line arguments.

If the client host is behind a proxy, you can use –setproxy option. The proxy information will be stored in the configuration file and nrclientcmd will respect this setting subsequently.

There are also a few advance options:

- setconn: allow user to specify client-to-client connection type.
- dbroot: allow user to specify the location to store user data
- internal: nrclientcmd will generate tags between information sections. This option can be used by third party developers to create a UI wrapper for CLI.

3.7.2 Computer List in CLI

After signing in, you will see your computer list just like on Windows. The computer list will automatically update if there are any changes in your virtual LAN, e.g. a host comes online or offline.

At the bottom of the screen lists the available commands you can use to manage the computer list, change password, remotely wake up a computer, or to quit.

3.8 Network Explorer Portable

NeoRouter Network Explorer Portable can run from any computer without installation. It does not require administrator permission or use the virtual network adapter. This application can be extremely useful for users who need to connect to the VLAN from a public kiosk or from friend’s house.

Note: Prior to v1.1.1 Portable and USB are two separate packages. They are merged into one package in v1.1.1 and later releases. The new package is a zip file containing both the portable client and the USB Auto Run Configuration Tool. The functionalities are same as before.

3.8.1 Network Explorer Portable

To use Network Explorer Portable client, user can simply download it from NeoRouter download website and run. Then user will see the same user interface as the regular Network Explorer. The user experience is almost the same except for the following:

- The host running Portable/USB client cannot be added to the computer list or be accessed by remote computer. You can think of it as a “viewer of the VLAN”.
- NeoRouter administrator users can see and manage hosts running Portable/USB clients in the Configuration Explorer.

3.8.2 Manage Add-On

Network Explorer Portable supports all the add-ons as the full Network Explorer. The setup steps are slightly different.

1. To install a NeoRouter Add-on Package (*.nri) downloaded from NeoRouter website:
   - choose menu File | Add-ons and launch "Add-ons Manager" dialog
   - click the "Install..." button to install a NeoRouter Add-on Package (*.nri)
2. To add your own program as an Add-On:
   - choose menu File | Add-ons and launch "Add-ons Manager" dialog
   - Click on the "+" button on the toolbar to complete the wizard form to create new add-on properties for an application, then click on "Ok" button to save.
   - Alternatively you can drag and drop the executable on to the “Add-ons Manager” dialog
3. Network Explorer Portable was designed to run on a public computer and upon exit it will remove all user data, including add-ons. If you would like to keep the settings, you can follow the steps below:
   - On XP, create/edit X:\Documents and Settings\All Users\Application Data\ZebraNetworkSystems\NeoRouter\Feature.ini
   - On Vista or Win7, create/edit X:\Users\All Users\ZebraNetworkSystems\NeoRouter\Feature.ini
   - Enter the following content:

     ```
     [Default]
     ForceKeepSetting=1
     ```
   - Restart Network Explorer Portable

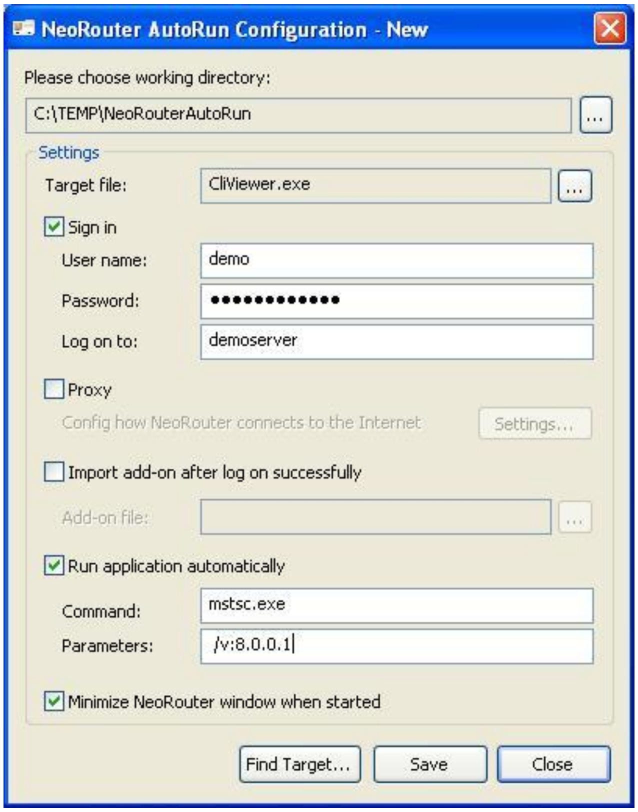
3.8.3 Auto Run Configuration for USB

(**Note**: The tool has been dropped since v2.0)

Auto Run Configuration Tool allows user to store the portable client, add-ons and configuration on a USB drive. You can even configure it to launch and sign in automatically when the USB drive is plugged into a computer and to sign out and exit when the USB drive is unplugged.

Here are the steps for setting up the USB package:

1. Download NeoRouter for USB.
2. Unzip the package to any folder. For example, C:\TEMP.
3. Launch the “Auto Run Configuration Tool” (AutoRunCfg.exe).



NeoRouter AutoRun Configuration - New

Please choose working directory: C:\TEMP\NeoRouterAutoRun

Settings

Target file: CliViewer.exe

☑ Sign in

User name: demo

Password: ●●●●●●●●●●●●

Log on to: demoserver

□ Proxy

Config how NeoRouter connects to the Internet

□ Import add-on after log on successfully

Add-on file:

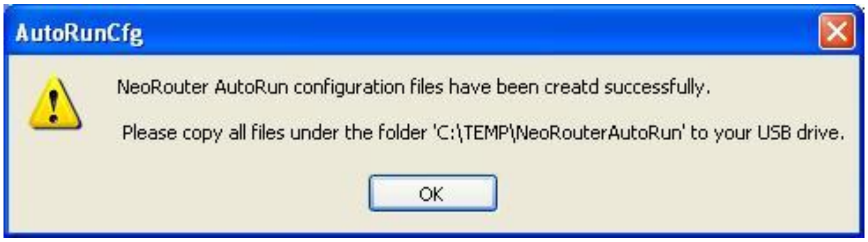
☑ Run application automatically

Command: mstsc.exe

Parameters: /v:8.0.0.1

☑ Minimize NeoRouter window when started

4. Click on the "…" button next to the working directory text box and specify a working path. If the target USB drive is plugged in, you can specify the USB drive root path as the working directory. Or you can specify a temporary path (e.g. C:\TEMP\USB) and copy the files to your USB driver later.
5. Once you specify a working directory, the "Settings" section will be enabled.
6. Choose CliViewer.exe from the same install zip package as the "Target file".
7. Check the "Sign in" checkbox and enter the domain name and user information to log into your NeoRouter VLAN.
8. Setup the proxy information if necessary.
9. If you want to import a NeoRouter add-on, click on the button on the right side of the "Add-on file" text box and specify an add-on *.nri file.
10. If you want to run an application automatically after signing in, click on the "Run application automatically" check box and input an executable file path and parameters.
11. If you want to hide the NeoRouter Viewer window, click on the "Minimize NeoRouter window when started".
12. Click on "Save" button to save the configuration files. It will generate the following files under the working directory.
    - Autorun.inf
    - CliViewer.exe, copied from the target file
    - NRAutoRun.xml
    - [add-on file].nri, if you specify an add-on
    - Proxy.xml, if you specify a proxy
13. You will also see the following dialog if the configuration was successful. Then please copy all files and sub-folder under the working directory to the root of your USB drive. And the USB drive is ready to use.

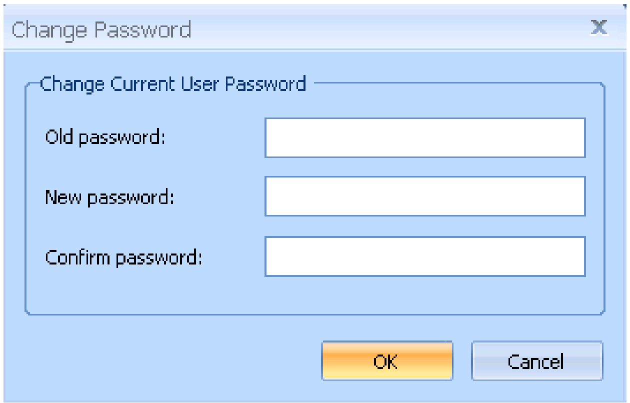

AutoRunCfg

NeoRouter AutoRun configuration files have been creatd successfully.

Please copy all files under the folder 'C:\TEMP\NeoRouterAutoRun' to your USB drive.

3.9 Change Password

A user can change his/her password in NeoRouter Network Explorer. User must sign in the Network Explorer using old password, then choose menu "File | Change Password", then enter the new password in the dialog.


Change Password

Change Current User Password

Old password:

New password:

Confirm password:

Network Explorer CLI has similar functionality. After signing in, user can use –changepassword command to enter new password.

If a user loses the old password, an administrator can create a new password for him/her using the Configuration Explorer User Management tool.

4. NeoRouter for Android

4.1 Overview

NeoRouter for Android enables users to remotely access and manage Windows, Mac and Linux computers right from your Android devices.

NeoRouter is a cross-platform zero-configuration VPN solution that securely connects your computers and devices at any locations into a virtual LAN and provides a networking platform for various applications like remote desktop, VNC, SSH, etc.

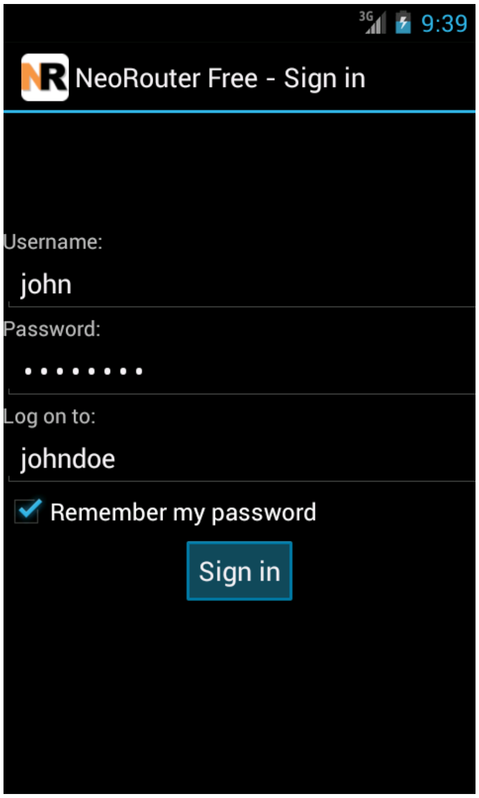
On devices with Android 4.x and above, NeoRouter for Android operates in VPN mode. User can seamlessly access remote computers by their virtual IP addresses using any app.

On devices with Android 3.x and below, NeoRouter for Android operates in Tunnel mode. User needs to configure dynamic or static port forward tunnels. It only works with apps that use outgoing TCP connections.

4.2 VPN mode for Android 4.x and above

This guide assumes that user had previously setup a NeoRouter Domain and added remote computers.

Launch NeoRouter for Android and Sign In. The sign-in experience on Android is similar to that on Windows and Mac. When you see the VPN connection warning dialog, please check “I trust this application” and then click Ok.



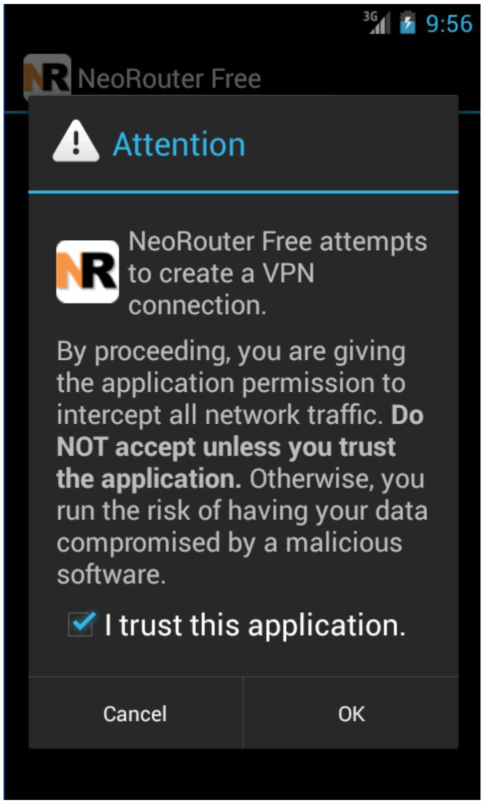
NeoRouter Free - Sign in

Username:
john

Password:
••••••••

Log on to:
johndoe

☑ Remember my password



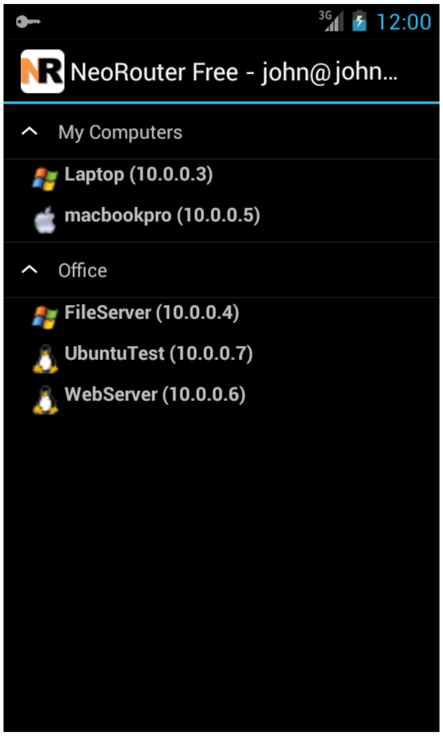
Attention

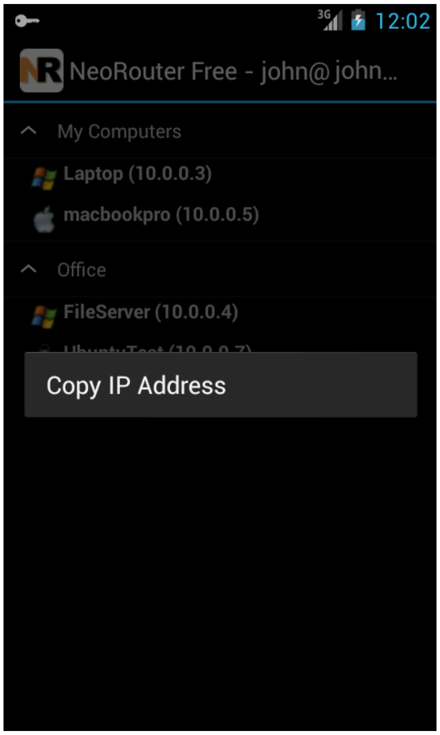
NeoRouter Free attempts to create a VPN connection.

By proceeding, you are giving the application permission to intercept all network traffic. **Do NOT accept unless you trust the application.** Otherwise, you run the risk of having your data compromised by a malicious software.

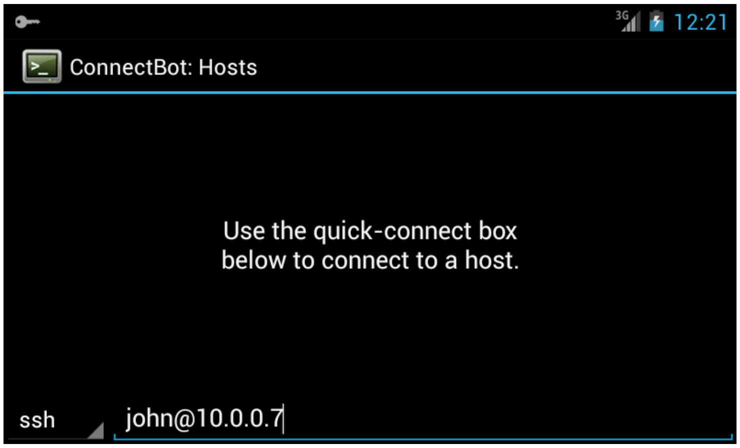
☑ I trust this application.

Once you have signed in, you will see the list of remote computers in your network. If online, a computer is shown in bold with a color icon. It is also assigned a virtual IP address as shown inside the parenthesis. You can long-click on an online computer to copy its virtual IP Address. You can also long-click an offline computer to wake-on-LAN.



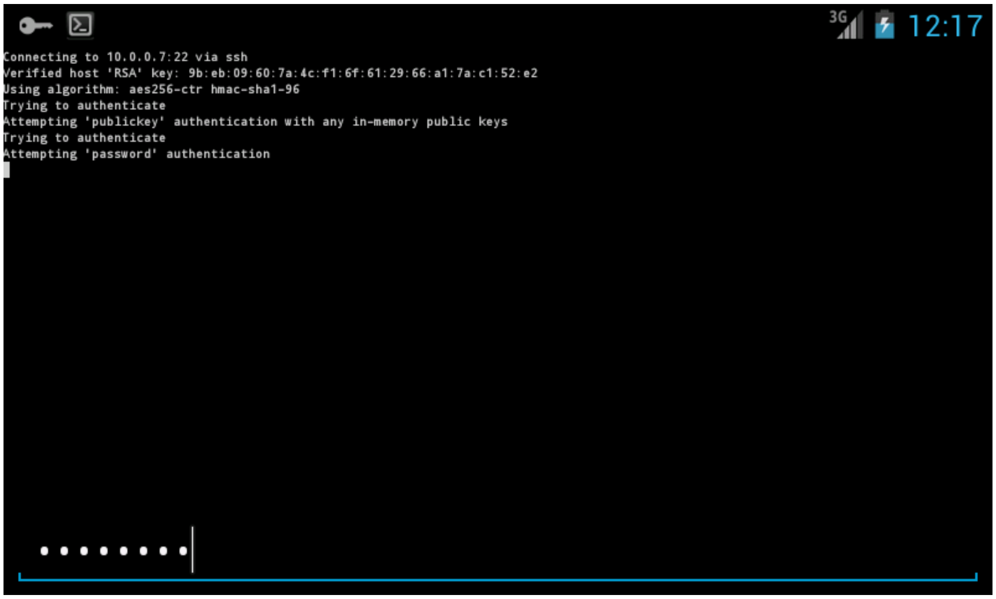


Launch ConnectBot, enter “user@{virtual ip address}”, and you will connect to the remote computer via SSH.



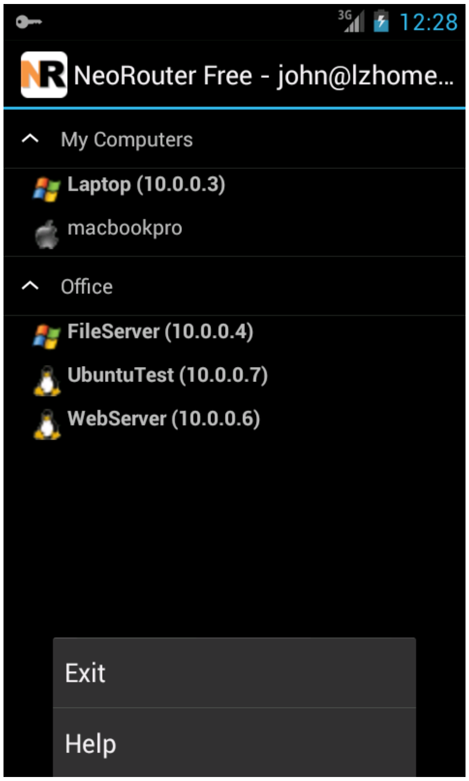
Use the quick-connect box below to connect to a host.

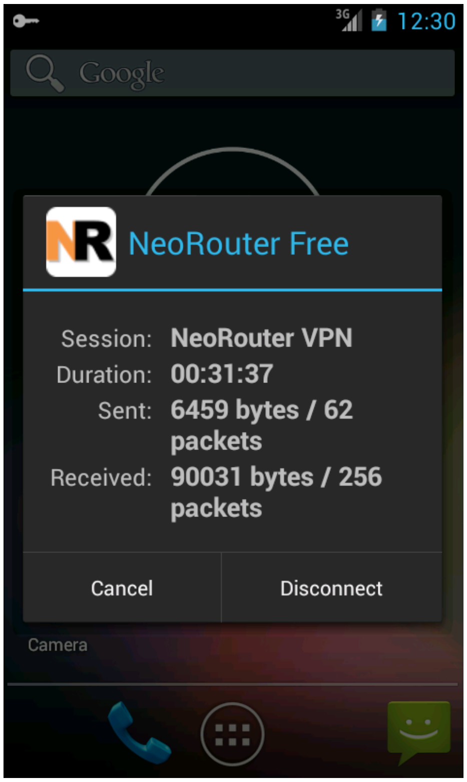
ssh john@10.0.0.7



```
Connecting to 10.0.0.7:22 via ssh
Verified host 'RSA' key: 9b:eb:09:60:7a:4c:f1:6f:61:29:66:a1:7a:c1:52:e2
Using algorithm: aes256-ctr hmac-sha1-96
Trying to authenticate
Attempting 'publickey' authentication with any in-memory public keys
Trying to authenticate
Attempting 'password' authentication
```

To exit NeoRouter VPN, you can click Menu – Exit. Alternatively you can open the key icon in the notification area and then click the disconnect button in the VPN status dialog.





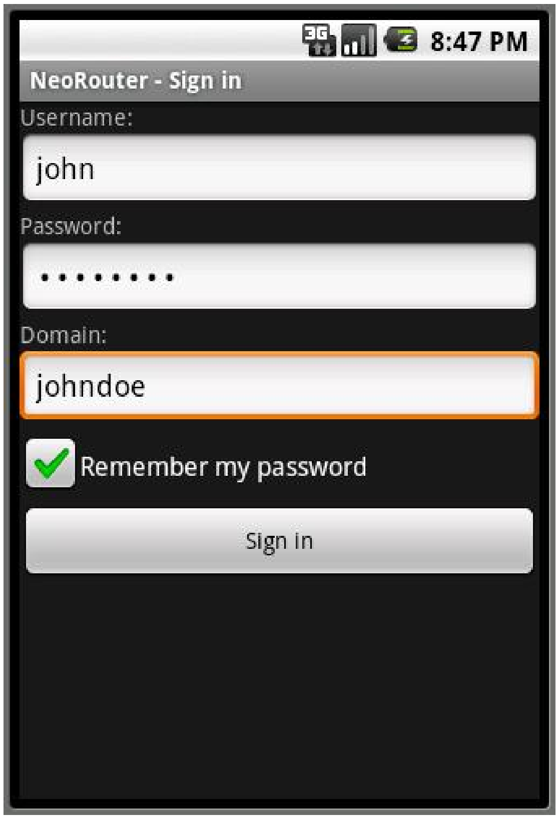
Session: NeoRouter VPN
Duration: 00:31:37
Sent: 6459 bytes / 62 packets
Received: 90031 bytes / 256 packets

4.3 *Tunnel Mode for Android 3.x and below*

4.3.1 Quick start using dynamic port forward

Using ConnectBot as example, I will show you how to setup NeoRouter for Android.

Download and install NeoRouter from Android market. Launch NeoRouter for Android and Sign In. The sign-in experience on Android is similar to that on Windows and Mac. Once you have signed in, you will see the list of remote computers in your network. If online, a computer is shown in bold with a color icon. It is also assigned a virtual IP address as shown inside the parenthesis.



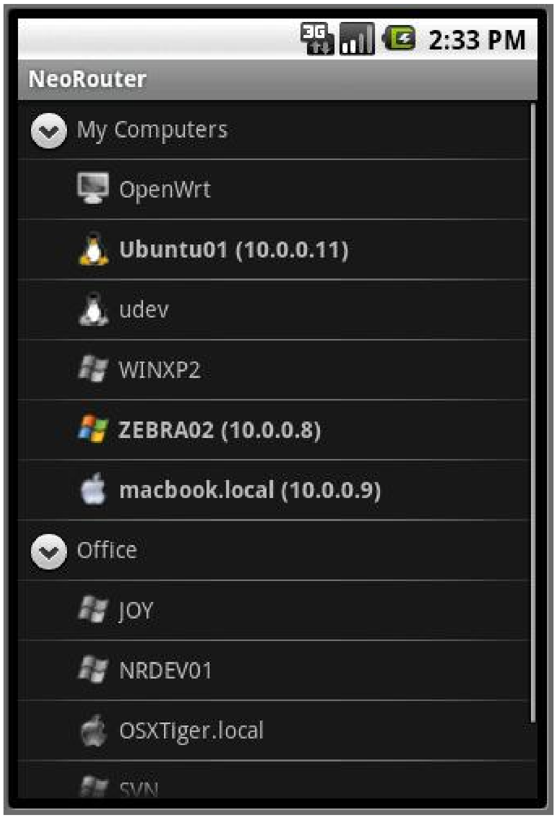
NeoRouter - Sign in

Username: john

Password: •••••••••

Domain: johndoe

☑ Remember my password



NeoRouter

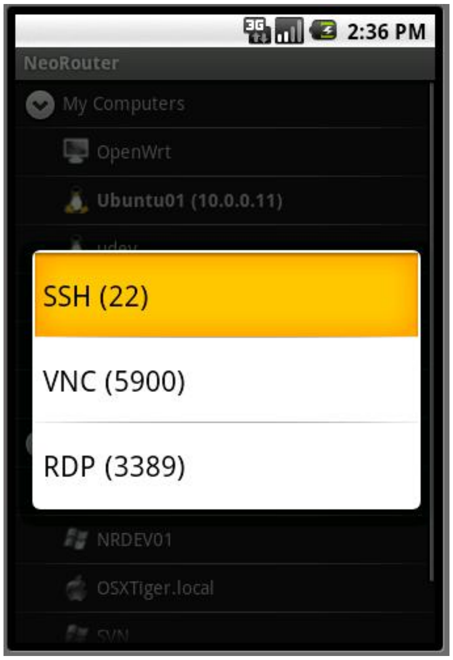
My Computers

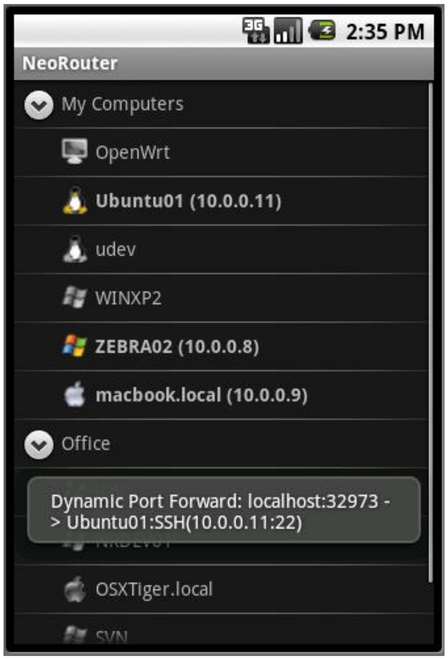
- OpenWrt
- **Ubuntu01 (10.0.0.11)**
- udev
- WINXP2
- **ZEBRA02 (10.0.0.8)**
- **macbook.local (10.0.0.9)**

Office

- JOY
- NRDEV01
- OSXTiger.local
- SVN

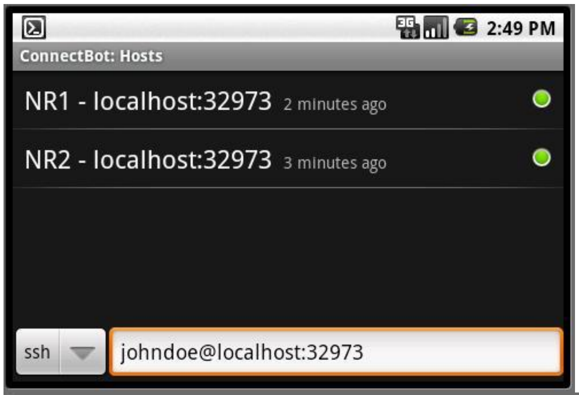
Long-click on an online computer and you will see the launch pad dialog with a list of applications/ports. Choose SSH (22) from the list and NeoRouter will setup port forward from localhost:32973 to the SSH port of the remote computer.



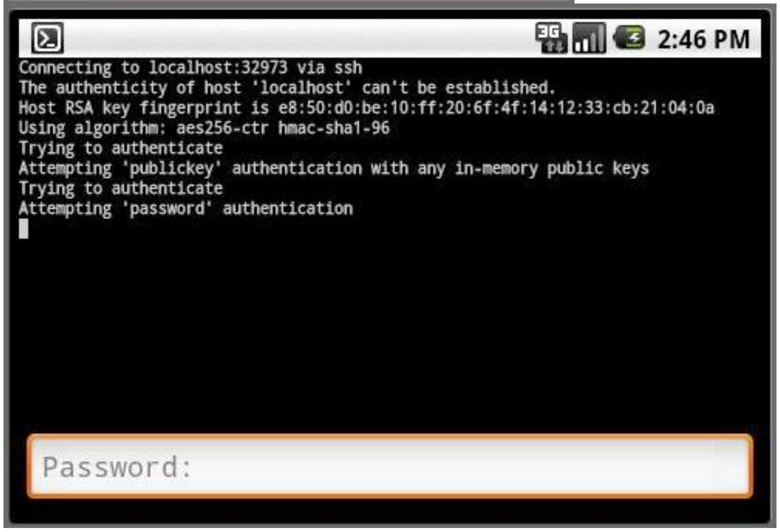


Dynamic Port Forward: localhost:32973 -> Ubuntu01:SSH(10.0.0.11:22)

Launch ConnectBot, enter “user@localhost:32973”, and you will connect to the remote computer via SSH. Tip: if you need multiple SSH connections concurrently, you can add multiple entries to localhost:32973 in ConnectBot by changing the Nick Name property. See ConnectBot’s FAQ for more information.


2:49 PM
ConnectBot: Hosts
NR1 - localhost:32973 2 minutes ago
NR2 - localhost:32973 3 minutes ago
ssh

johndoe@localhost:32973



```
Connecting to localhost:32973 via ssh
The authenticity of host 'localhost' can't be established.
Host RSA key fingerprint is e8:50:d0:be:10:ff:20:6f:4f:14:12:33:cb:21:04:0a
Using algorithm: aes256-ctr hmac-sha1-96
Trying to authenticate
Attempting 'publickey' authentication with any in-memory public keys
Trying to authenticate
Attempting 'password' authentication
```

Password:

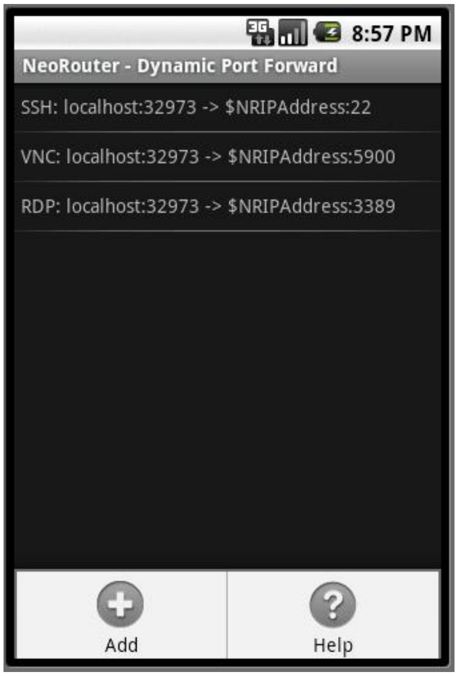
If you need to connect to a different computer or to use a different application, you can simply repeat the above steps to setup a different Dynamic Port Forward in NeoRouter. Then new connections to localhost:32973 will be forwarded to this new remote address. The change does not interrupt existing connections.

To exit NeoRouter, you can click Menu – Exit.

4.3.2 Configure Dynamic Port Forward

With Dynamic Port Forward, NeoRouter always listens at port 32973 of localhost, and user can specify remote computer and port dynamically by long-click a computer then choose a port (See Quick Start Guide for example). After setting remote computer and port, new connections to localhost:32973 will be forwarded to this remote address. User can change the remote address at any time without interrupting existing connections.

By default, NeoRouter supports three remote ports: SSH (22), VNC (5900) and RDP (3389). To change the default settings, user can sign in, click “menu” – “Settings” – “Configure Dynamic Port Forward”. Note that “$NRIPAddress” will be replaced with the IP address of the remote computer.

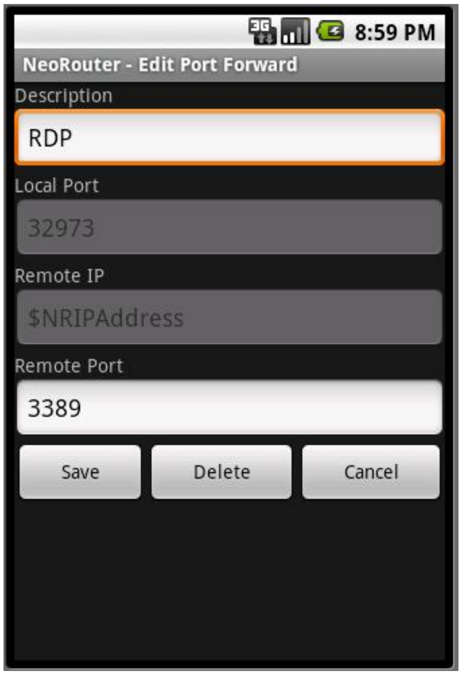


NeoRouter - Dynamic Port Forward

SSH: localhost:32973 -> $NRIPAddress:22

VNC: localhost:32973 -> $NRIPAddress:5900

RDP: localhost:32973 -> $NRIPAddress:3389



NeoRouter - Edit Port Forward

Description: RDP

Local Port: 32973

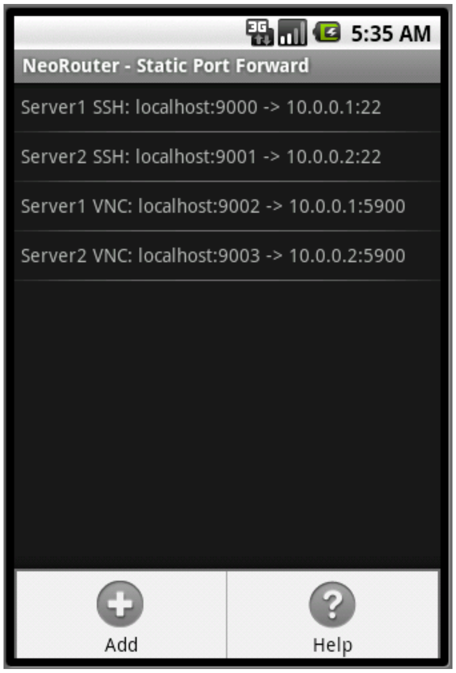
Remote IP: $NRIPAddress

Remote Port: 3389

4.3.3 Configure Static Port Forward

With Static Port Forward, user assigns a local port for every remote [server:port]. For example, if a user needs access to two remote computers for SSH and VNC, he/she will need to create four static port forward mappings as shown in the screenshot below.

NeoRouter will listen at all these local ports and forward the incoming connections according to the mappings.
To edit static port forward, user needs to sign in, then click “menu” – “Settings” – “Configure Static Port Forward”.



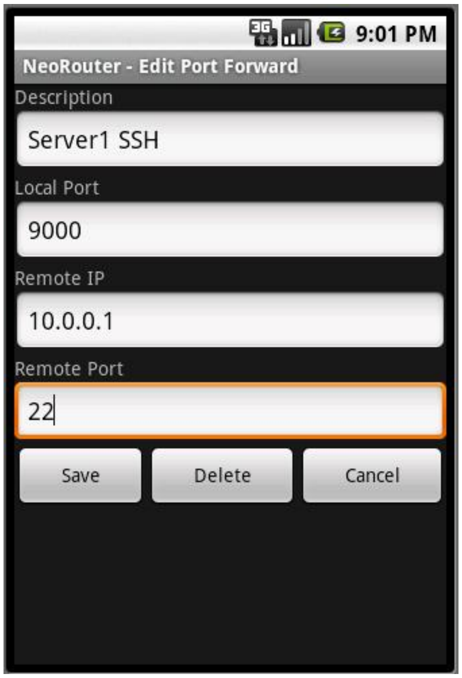
NeoRouter - Static Port Forward

Server1 SSH: localhost:9000 -> 10.0.0.1:22

Server2 SSH: localhost:9001 -> 10.0.0.2:22

Server1 VNC: localhost:9002 -> 10.0.0.1:5900

Server2 VNC: localhost:9003 -> 10.0.0.2:5900



NeoRouter - Edit Port Forward

Description: Server1 SSH

Local Port: 9000

Remote IP: 10.0.0.1

Remote Port: 22

5. NeoRouter Remote Access Client

NeoRouter Remote Access Client allows you to remotely access Windows/Mac/Linux/BSD computers using RDP, VNC, SSH/Telnet, SFTP/FTP. It supports iOS/Android devices (as installable apps) and HTML5 enabled web browsers, running PC or mobile devices such as Microsoft Surface, iPad, iPhone, iTouch and BlackBerry10. All connections are encrypted using TLSv1/SSLv3(AES-256). The mobile apps can establish direct P2P connections to your remote computers to achieve fastest connection speed.

5.1 Prerequisites

Before using this client, you must
1) setup your NeoRouter server(v1.9 and above) and domain
2) install NeoRouter client on remote computers and join them to this domain.

The NeoRouter software has three editions: Free, Pro and Mesh. The Free edition allows up to 2 mobile clients and 2 web clients; each client can have up to 2 active add-on sessions. Upgrade to Professional or Mesh edition to enjoy unlimited access.

5.2 System Requirements

For iOS and Android users: although this app supports devices of various form factors, we highly recommend using a full-size tablet. We also recommend using a hardware keyboard for higher productivity.

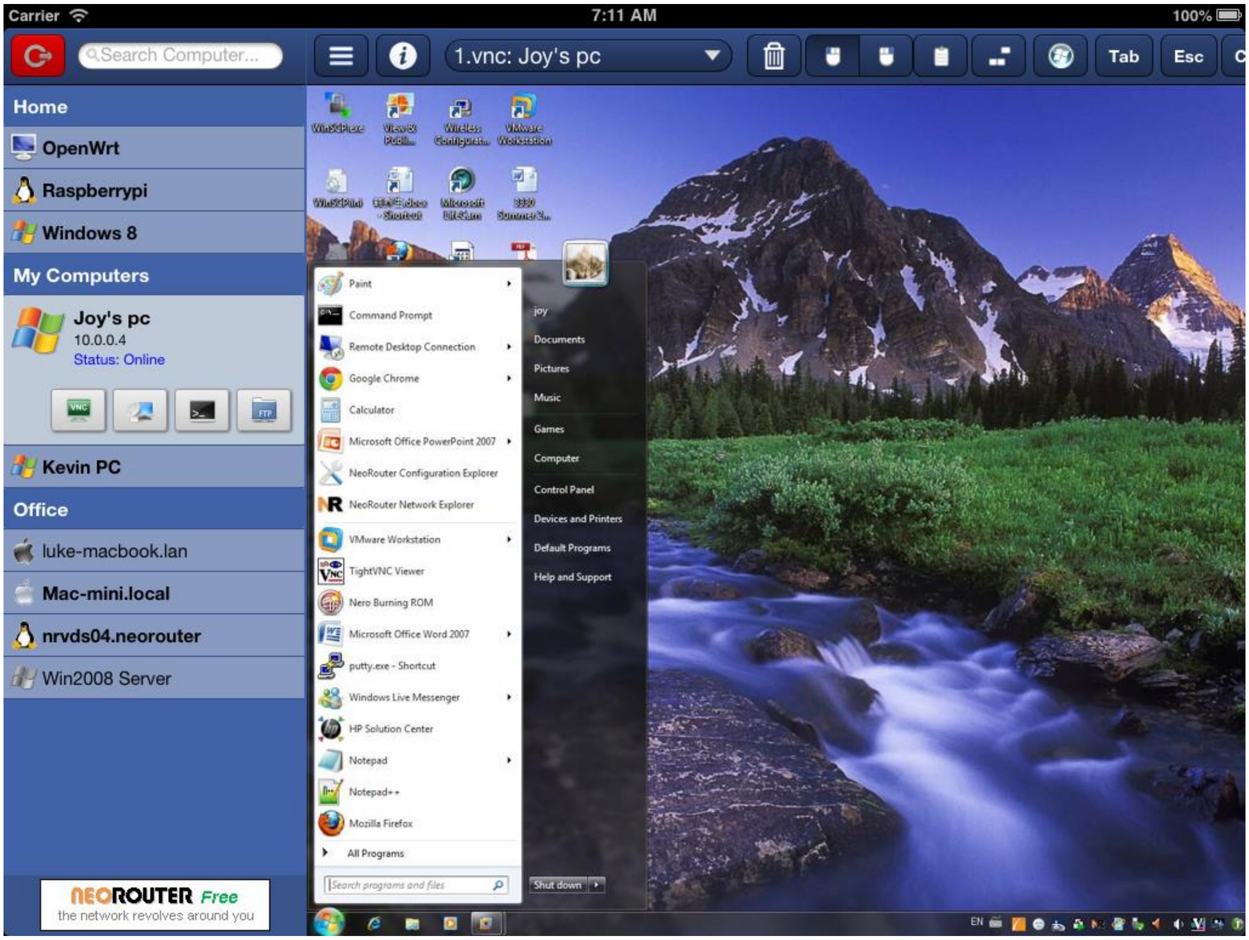
For browser based users: this app uses HTML5 features like Canvas, Web Socket and Web Storage. We recommend the latest Chrome or Safari browsers.

5.3 Built-in add-ons

NeoRouter Remote Access Client comes with several built-in add-ons, such as VNC client, RDP client, Telnet/SSH client, FTP/SFTP client and Wake-On-Lan.

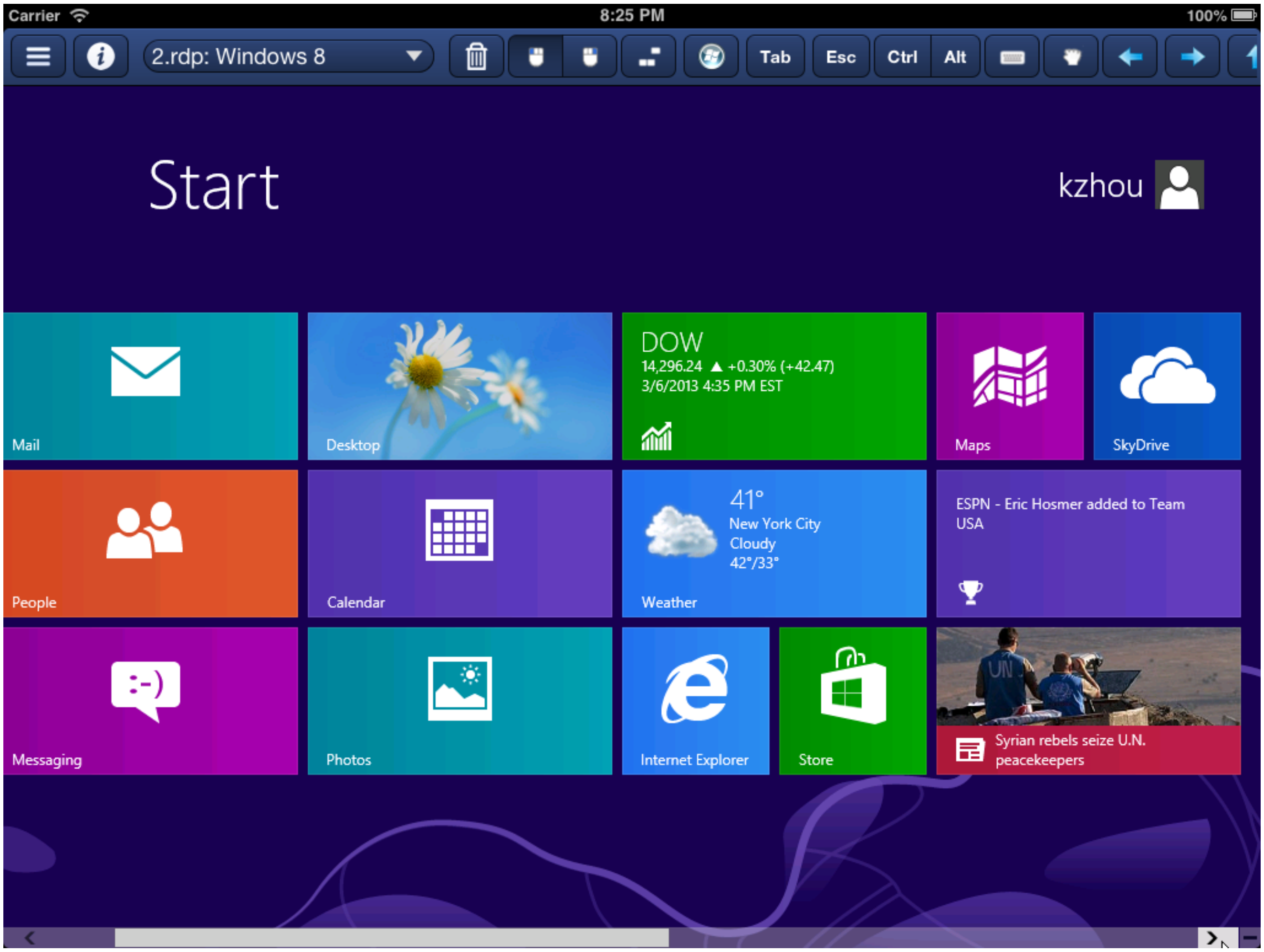
5.3.1 VNC

The VNC add-on supports all standard VNC servers, running on any platforms. For TightVNC server, it provides better performance by implementing the Tight Protocol. It supports mouse/touch events, clipboard, win-key, ctrl-alt-del key, tab, esc, ctrl, alt, arrow keys. It also supports zoom-in and zoom-out for higher resolution. On tablets and smart-phones, it supports both soft keyboard and hard keyboard.



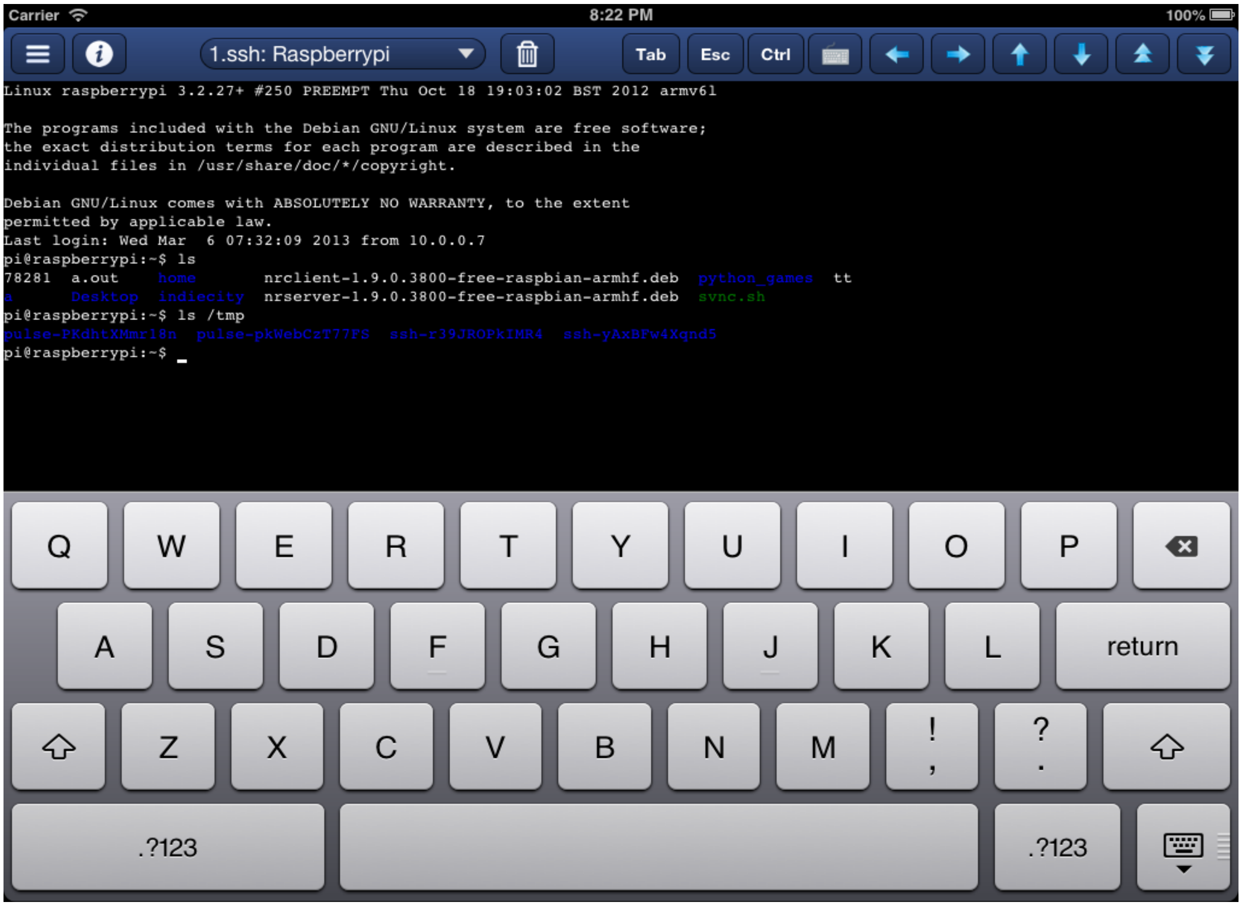
5.3.2 RDP

The RDP add-on can to connect to Microsoft Windows computers running Remote Desktop Services, including Windows 2000 and above. It supports mouse/touch events, win-key, ctrl-alt-del key, tab, esc, ctrl, alt, arrow keys. On tablets and smart-phones, it supports both soft keyboard and hard keyboard.



5.3.3 Telnet and SSH

The Telnet/SSH add-on can to connect to the standard telnet and ssh service, running Windows, Linux and Unix. It supports tab, esc, ctrl, arrow keys. On tablets and smart-phones, it supports both soft keyboard and hard keyboard.



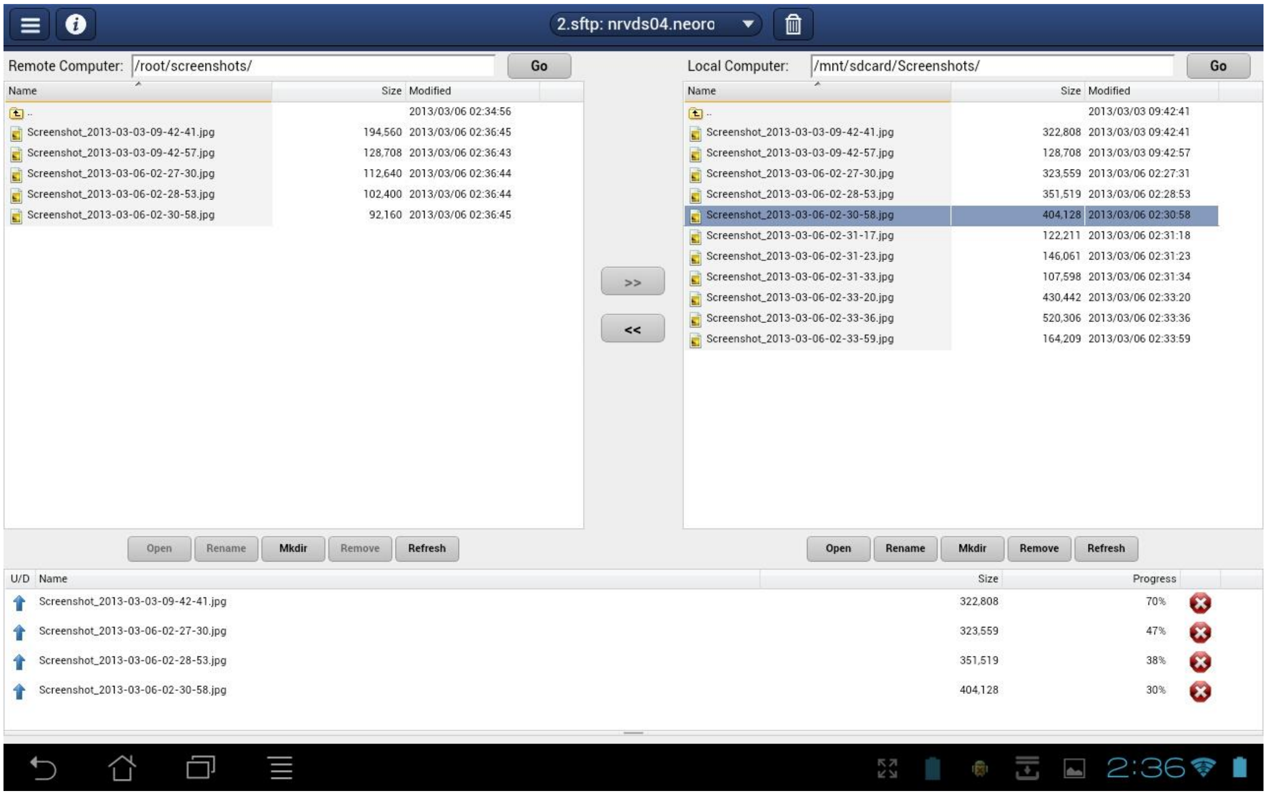
```
Linux raspberrypi 3.2.27+ #250 PREEMPT Thu Oct 18 19:03:02 BST 2012 armv6l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Mar  6 07:32:09 2013 from 10.0.0.7
pi@raspberrypi:~$ ls
78281  a.out    home       nrclient-1.9.0.3800-free-raspbian-armhf.deb  python_games  tt
a      Desktop  indiecity  nrserver-1.9.0.3800-free-raspbian-armhf.deb  svnc.sh
pi@raspberrypi:~$ ls /tmp
pulse-PKdhtXMmrl8n  pulse-pkWebCzT77FS  ssh-r39JROPkIMR4  ssh-yAxBFw4Xqnd5
pi@raspberrypi:~$ _
```

5.3.4 FTP and SFTP

The Ftp/Sftp add-on can to connect to the standard ftp and ssh service. It allows user to download/upload files, rename remote files and folders, move remote files and folder and create new folder on the remote computers. On a desktop browsers, the downloaded files will be saved in the download file folder. On mobile devices, it will save to the target folder specified by users. On Android devices, it can also open the selected files.

Note:

- It allows user to upload and download multiple times concurrently.
- In some browsers/devices, such as iPad and BlackBerry 10, that does not support full HTML5 API, the add-on may not be able to download files. But other functionalities should work.



Remote Computer: /root/screenshots/

Name	Size	Modified
..		2013/03/06 02:34:56
Screenshot_2013-03-03-09-42-41.jpg	194,560	2013/03/06 02:36:45
Screenshot_2013-03-03-09-42-57.jpg	128,708	2013/03/06 02:36:43
Screenshot_2013-03-06-02-27-30.jpg	112,640	2013/03/06 02:36:44
Screenshot_2013-03-06-02-28-53.jpg	102,400	2013/03/06 02:36:44
Screenshot_2013-03-06-02-30-58.jpg	92,160	2013/03/06 02:36:45

Local Computer: /mnt/sdcard/Screenshots/

Name	Size	Modified
..		2013/03/03 09:42:41
Screenshot_2013-03-03-09-42-41.jpg	322,808	2013/03/03 09:42:41
Screenshot_2013-03-03-09-42-57.jpg	128,708	2013/03/03 09:42:57
Screenshot_2013-03-06-02-27-30.jpg	323,559	2013/03/06 02:27:31
Screenshot_2013-03-06-02-28-53.jpg	351,519	2013/03/06 02:28:53
Screenshot_2013-03-06-02-30-58.jpg	404,128	2013/03/06 02:30:58
Screenshot_2013-03-06-02-31-17.jpg	122,211	2013/03/06 02:31:18
Screenshot_2013-03-06-02-31-23.jpg	146,061	2013/03/06 02:31:23
Screenshot_2013-03-06-02-31-33.jpg	107,598	2013/03/06 02:31:34
Screenshot_2013-03-06-02-33-20.jpg	430,442	2013/03/06 02:33:20
Screenshot_2013-03-06-02-33-36.jpg	520,306	2013/03/06 02:33:36
Screenshot_2013-03-06-02-33-59.jpg	164,209	2013/03/06 02:33:59

U/D	Name	Size	Progress	
↑	Screenshot_2013-03-03-09-42-41.jpg	322,808	70%	☒
↑	Screenshot_2013-03-06-02-27-30.jpg	323,559	47%	☒
↑	Screenshot_2013-03-06-02-28-53.jpg	351,519	38%	☒
↑	Screenshot_2013-03-06-02-30-58.jpg	404,128	30%	☒

5.4 Tips

1. Add-on toolbar is scrollable. On devices with small screens, all the toolbar buttons are not shown. Swipe on the toolbar to show more buttons.

2. If hardware keyboard is attached or detached from the tablet, NeoRouter Remote Access Client will detect the change when you sign out and then sign back in.

3. To find computer(s) in a large computer list, try entering computer name, category name, virtual ip address or status("online" or "offline") in the search box above the computer list.

4. When using SFTP/FTP on tablet, long touch click opens a folder or file. On desktop, mouse double-click opens it.

5. When using RDP on a tablet with a single-core CPU (e.g. iPad first generation), please reduce Desktop Size.

6. Configuration Explorer

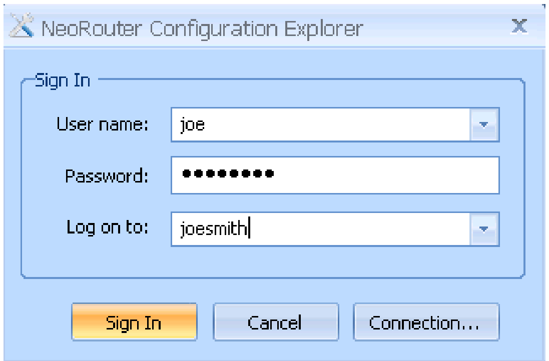
NeoRouter Configuration Explorer is a management tool that allows an administrator to manage local or remote NeoRouter server. This is the recommended method to change server settings.

On Windows, user can use the NeoRouter Configuration Explorer for Windows included in the installation package. On non-Windows platforms, nrserver CLI can be used to perform most configurations. Since NeoRouter v2.0, user can also use the web based NeoRouter Web Console to manage the server.

6.1 Launch and Sign In

Note: Only administrators can sign in Configuration Explorer.

1. User can launch it from "Windows Start Menu | All Programs | NeoRouter | NeoRouter Network Explorer" or from NeoRouter Network Explorer menu “File | Options”.
2. After launch, user will see a sign-in dialog that is similar to the Network Explorer counterpart. Please enter domain name and user credential to sign in. If the local host is behind a proxy, please click on Connection button to set proxy information.

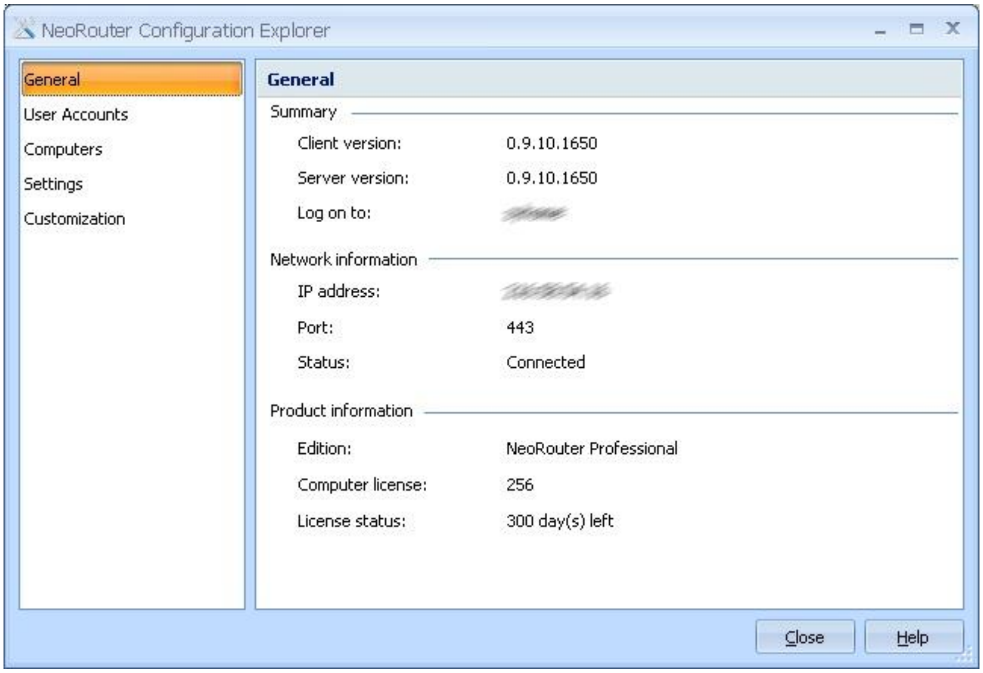


User name: joe

Password: ●●●●●●●●●

Log on to: joesmith

3. After sign in, the following general information page will be displayed.



General

Summary

Client version: 0.9.10.1650

Server version: 0.9.10.1650

Log on to: [redacted]

Network information

IP address: [redacted]

Port: 443

Status: Connected

Product information

Edition: NeoRouter Professional

Computer license: 256

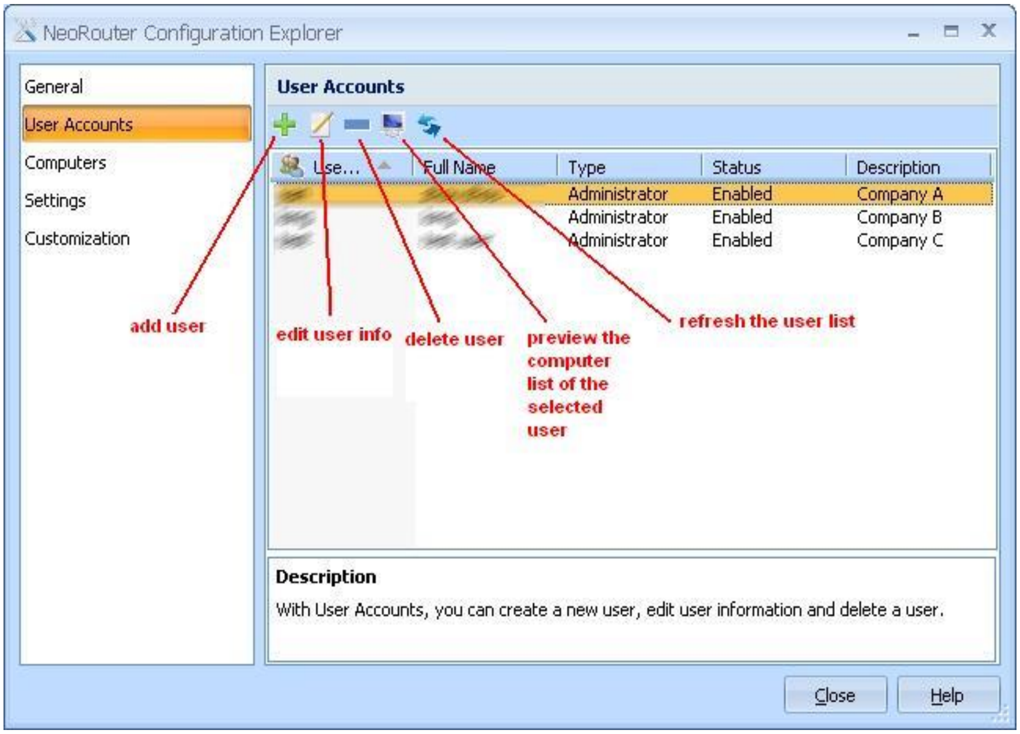
License status: 300 day(s) left

6.2 *Managing Users*

In the User Accounts page, you can perform the following tasks:

- View existing users: The users list can be sorted by any column.
- Add a new user: admin will create a temporary password for the new user and user can change the password in Network Explorer.
- Edit user information: you can enter anything like employer, contact info, etc.
- Set user’s password. If a user loses password, admin can set a temporary password for him/her. Then user can change the password again in Network Explorer.

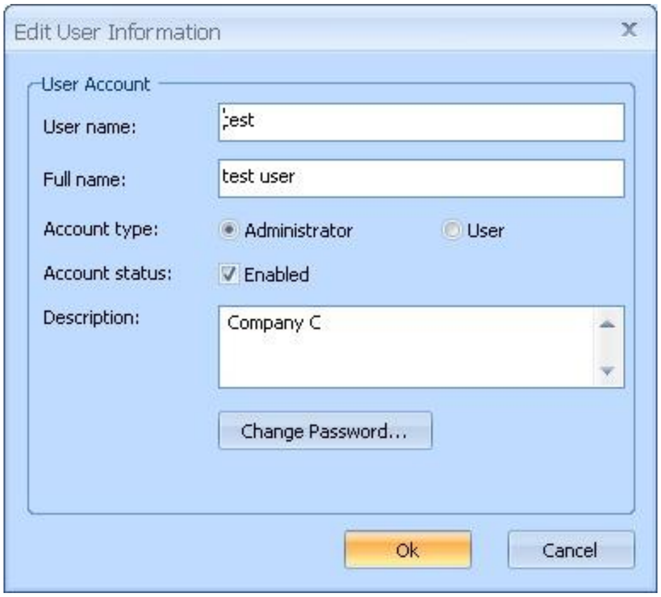
- Disable (block) a user: A disabled user will not be able to sign in Network Explorer or Configuration Explorer. The user’s profile and ACL settings are retained.
- Delete a user: all information of this user is deleted.
- View the computers that are visible to this user. (see ACL section for details)



Use...	Full Name	Type	Status	Description
[redacted]	[redacted]	Administrator	Enabled	Company A
[redacted]	[redacted]	Administrator	Enabled	Company B
[redacted]	[redacted]	Administrator	Enabled	Company C

Description

With User Accounts, you can create a new user, edit user information and delete a user.

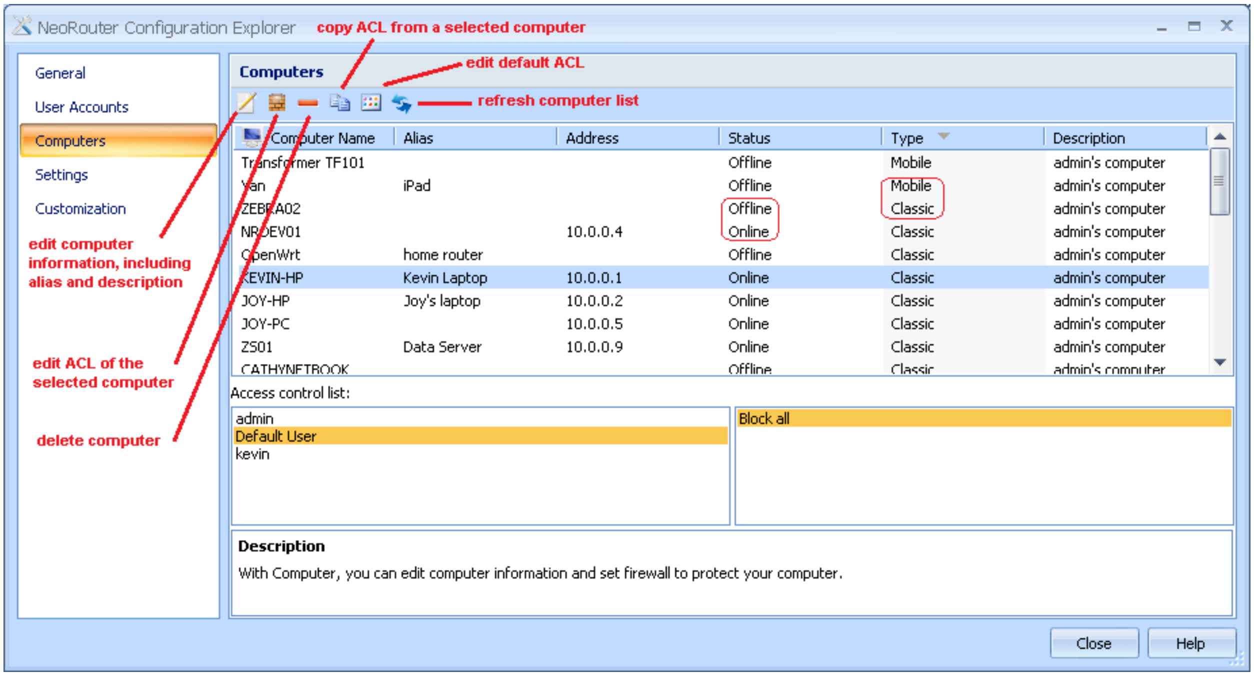


User name:	test
Full name:	test user
Account type:	● Administrator ○ User
Account status:	☑ Enabled
Description:	Company C

6.3 Managing Computers

In the Computers page, you can perform the following tasks:

- View existing computers: please note that the Type column will show “Temporary” for Network Explore Portable/USB clients, “Classic” for regular clients and "Mobile" for mobile/tablets clients. NeoRouter Remote Access web clients won't be shown in this list. The computer list can be sorted by any column.
- Edit a computer’s alias. When a computer is added to the virtual network, NeoRouter reads the computer name from the OS and displays it in the computer list. If you prefer a different name, you can create an alias which will then be used in the computer list.
- Edit a computer’s description: you can enter anything like computer owner, location, asset id, etc.
- Edit ACL: this will be discussed in next section.



copy ACL from a selected computer

edit default ACL

refresh computer list

edit computer information, including alias and description

edit ACL of the selected computer

delete computer

Computer Name	Alias	Address	Status	Type	Description
Transformer TF101			Offline	Mobile	admin's computer
Yan	iPad		Offline	Mobile	admin's computer
ZEBRA02			Offline	Classic	admin's computer
NRDEV01		10.0.0.4	Online	Classic	admin's computer
OpenWrt	home router		Offline	Classic	admin's computer
KEVIN-HP	Kevin Laptop	10.0.0.1	Online	Classic	admin's computer
JOY-HP	Joy's laptop	10.0.0.2	Online	Classic	admin's computer
JOY-PC		10.0.0.5	Online	Classic	admin's computer
ZS01	Data Server	10.0.0.9	Online	Classic	admin's computer
CATHYNETBOOK			Offline	Classic	admin's computer

Access control list:

admin
Default User
kevin

Block all

Description

With Computer, you can edit computer information and set firewall to protect your computer.

6.4 Access Control List

This feature is available in NeoRouter Profession Edition only.

6.4.1 Overview

The ACL of a host specifies which users are granted or denied access to the host and which specific services or ports are allowed. Administrators can use ACL to manage a NeoRouter domain that has users with different trust levels.

For example, Joe uses NeoRouter to manage the office network at his small business. He wants to share some documents on a file server with a customer, but block this customer from accessing other services on this file server and other computers at office. At the same time, Joe and his coworkers should continue to have full access to all computers.

This can be a daunting task with traditional VPN solutions. Once Joe’s customer is connected into the office network, he/she can access all network resources just like Joe and his coworkers. If the office uses a domain controller, it can help mitigate the threat, but Joe would have to check all the computers to ensure they are secure. Some coworkers can make innocent mistakes and share important files or internal websites with “everyone”. With NeoRouter, Joe can manage all the access control at one place and easily solve this challenge.

ACL defines the relationships between users and computers that can be conceptually represented using a table. In Joe's case, he needs to define the ACL as follows.

	Default User	Joe (Admin)	Customer	Joe' Co-workers
Default Computer ACL	Block all			
File Server	Allow all		Allow file sharing, block other services	
Office Computer A	Allow all		Block all	
Office Computer B	Allow all		Block all	
Joe's laptop	Allow all		Block all	
Customer's Computer				

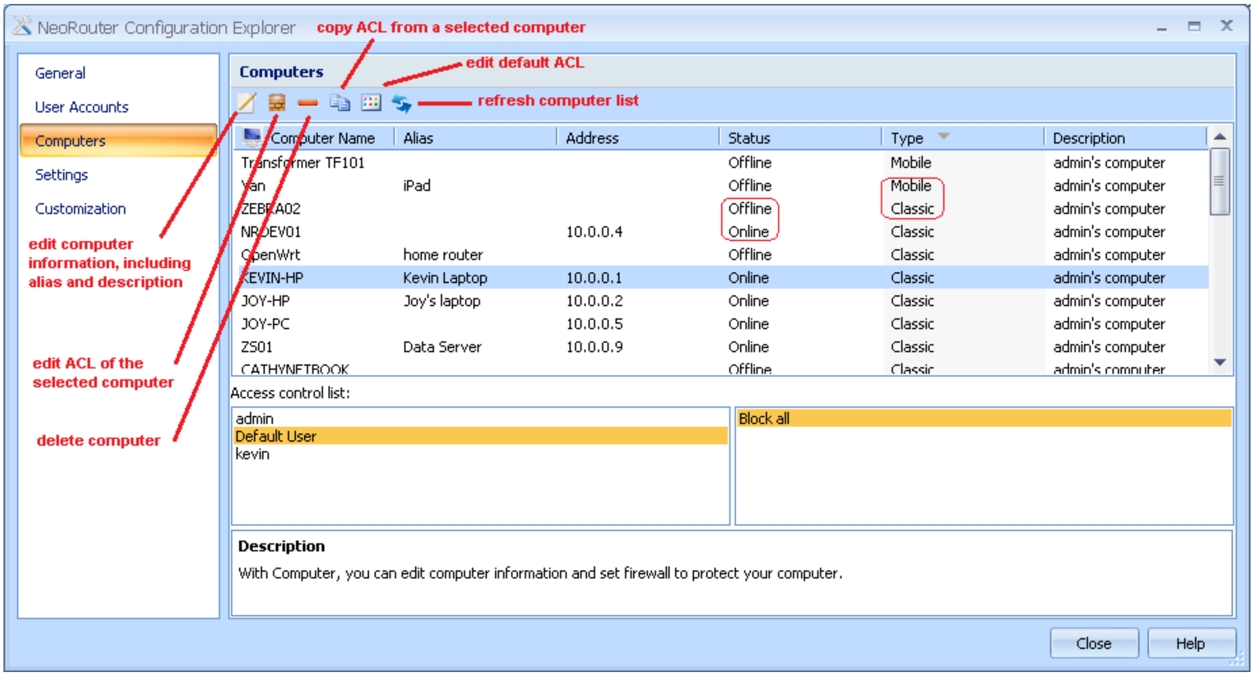
Let's first look at the row for File Server. Joe's customer will only have access to the files sharing service. There is no ACL defined for Joe and his co-workers, so the ACL for Default User is effective and they have full access. Similarly the customer will be blocked from accessing office computer A and B as well as Joe's laptop, while Joe and his coworkers have full access to these computers.

When the customer connects to Joe's NeoRouter domain, his computer will be added to the domain. Because the ACL for this computer is undefined, it will have the same ACL as "Default Computer". Thus the customer's computer will block all users, including Joe, from accessing it. The customer has physical access to his own computer.

6.4.2 Define Computer ACL

You can think of a computer's ACL as a row in the above ACL table. An admin can select any computer in the computer list and edit its ACL. If a group of computers share the same ACL, admin can copy ACL from one computer to another.

To edit the Default Computer ACL, you can click on the "Edit Default ACL" button in the tool bar.


NeoRouter Configuration Explorer
copy ACL from a selected computer
edit default ACL
refresh computer list
General
User Accounts
Computers
Settings
Customization
edit computer information, including alias and description
edit ACL of the selected computer
delete computer
Computers
Close
Help

Computer Name	Alias	Address	Status	Type	Description
Transformer TF101			Offline	Mobile	admin's computer
Yan	iPad		Offline	Mobile	admin's computer
ZEBRA02			Offline	Classic	admin's computer
NRDEV01		10.0.0.4	Online	Classic	admin's computer
OpenWrt	home router		Offline	Classic	admin's computer
KEVIN-HP	Kevin Laptop	10.0.0.1	Online	Classic	admin's computer
JOY-HP	Joy's laptop	10.0.0.2	Online	Classic	admin's computer
JOY-PC		10.0.0.5	Online	Classic	admin's computer
ZS01	Data Server	10.0.0.9	Online	Classic	admin's computer
CATHYNETBOOK			Offline	Classic	admin's computer

Access control list:

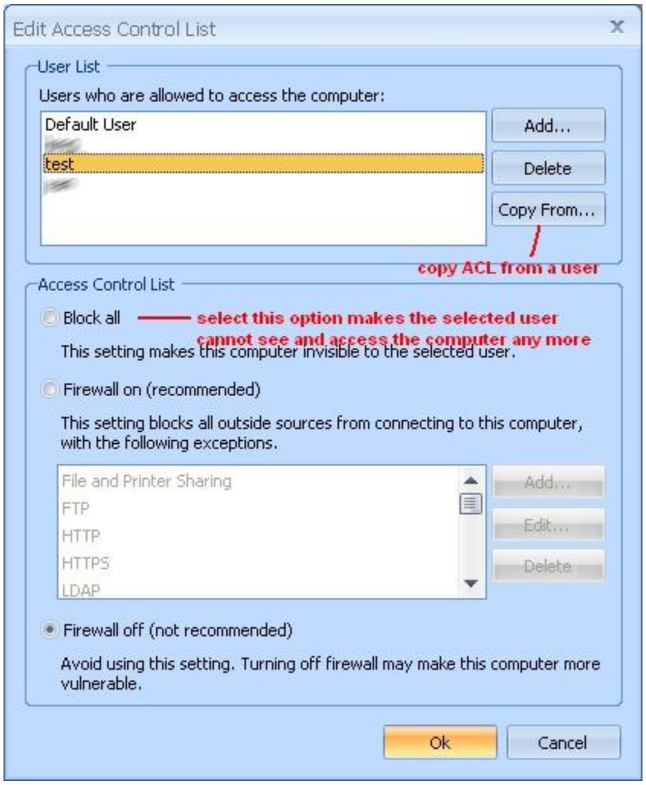
admin	Block all
Default User	
kevin	

Description

With Computer, you can edit computer information and set firewall to protect your computer.

6.4.3 Define ACL entry

An ACL entry defines the relationship between one user and one computer. You can think of it as a cell in the above table. To edit an ACL entry, you can select the computer in the computer list, click Edit ACL in the tool bar, and then select the user in the User List in the following dialog. If the user does not exist in the list, you can click Add button and add him/her.



Edit Access Control List

User List

Users who are allowed to access the computer:

Default User
[redacted]
test
[redacted]

copy ACL from a user

Access Control List

○ Block all — select this option makes the selected user cannot see and access the computer any more

This setting makes this computer invisible to the selected user.

○ Firewall on (recommended)

This setting blocks all outside sources from connecting to this computer, with the following exceptions.

File and Printer Sharing
FTP
HTTP
HTTPS
LDAP

● Firewall off (not recommended)

Avoid using this setting. Turning off firewall may make this computer more vulnerable.

There are 4 types of ACL entries:

- **Undefined**: the relationship between the user and the computer is not explicitly defined. The user does not show up in the User List of the ACL. In this case the Default User ACL entry for this computer will be effective.
- **Block All**: the computer is invisible to the user. User cannot add the computer to his/her computer list in Network Explorer or connect to it.
  Note: admin can view the list of computers that is visible to a specific user. Click on the User Accounts tab, choose the user, and then click on the “User Computer List” button from tool bar.
- **Firewall On**: User can only access the services in the exceptions list provided by the computer.
- **Firewall Off**: User can access all services provided by the computer.

To define the Default User ACL entry for a computer, choose Default User from User List. If several users have the same trust level, admin can copy the ACL entry from one user to another using the “Copy From” button.

6.4.4 How Firewall Works

NeoRouter Client Service daemon has a built-in firewall that monitors traffic in the virtual network. The firewall downloads the ACL from server and uses it to allow or deny incoming connections in the virtual network.

When a remote computer establishes a direct P2P or relayed connection to local host, it also informs which user has signed into the Network Explorer on the remote computer. Then the local host's firewall will use the user id to choose the appropriate ACL entry and control the virtual network traffic between these two computers. If user does not sign in Network Explorer on the remote computer, the Default User ACL entry is used.

As a result, NeoRouter firewall can control a user's access to a network resource (a computer, or a service on a computer) based on the ACL.

6.4.5 Example: hub-and-spoke

Jeff's company has three business partners A, B and C. Jeff needs to setup bidirectional network connections with each partner, but these partners should be invisible to each other. Jeff setup a NeoRouter domain and invited the partners to. Then Jeff creates the following ACL to achieve his access control goals.

	Default User	Jeff (Admin)	Partner A	Partner B	Partner C
Default Computer ACL	Block all	Allow all			
Jeff's Computer 1 (Hub 1)	Allow all				
Jeff's Computer 2 (Hub 2)	Allow all				
Partner A's Computer					
Partner B's computer					
Partner C's computer					

Every user will have access to Jeff's two computers (hub) because they have Default User ACL entry as "Allow all". Partner A's computer does not have a specific ACL defined, so the Default Computer ACL is effective. The Default Computer ACL grants Jeff access to Partner A's computer, but make the computer invisible to Partner B and C. Partner A have physical access to his own computer.

6.4.6 Example: one-way access

Jason's company provide technical support for customer A. Jason needs to have one-way access to Customer A's computer but block Customer A from accessing Jason's computer. Jason sets up the following ACL for his domain and invites Customer A to join his domain. Jason can access all the computers in the domain while Customer A can access none except for his own.

One day Jason visits another Customer B's office. He installs NeoRouter client on Customer B's computer so that he can provide technical support remotely in the future. When he signs into Network Explorer, he makes sure to uncheck "remember my password" checkbox. When he leaves customer B's office, he exits the Network Explorer. Because Network Explorer is not running on Customer B's computer, the Default User ACL governs the connections from Customer B's computer to other computers in the VLAN. Thus Customer B does not have access to any computers except for his own. When Jason goes back to his office, he can connect to Customer B's computer remotely and provide customer support.

The difference between Customer A and B is that Customer A has a NeoRouter user account while Customer B does not. The result is that Jason has access to all three computers while Customer A or B can only access his/her own computer.

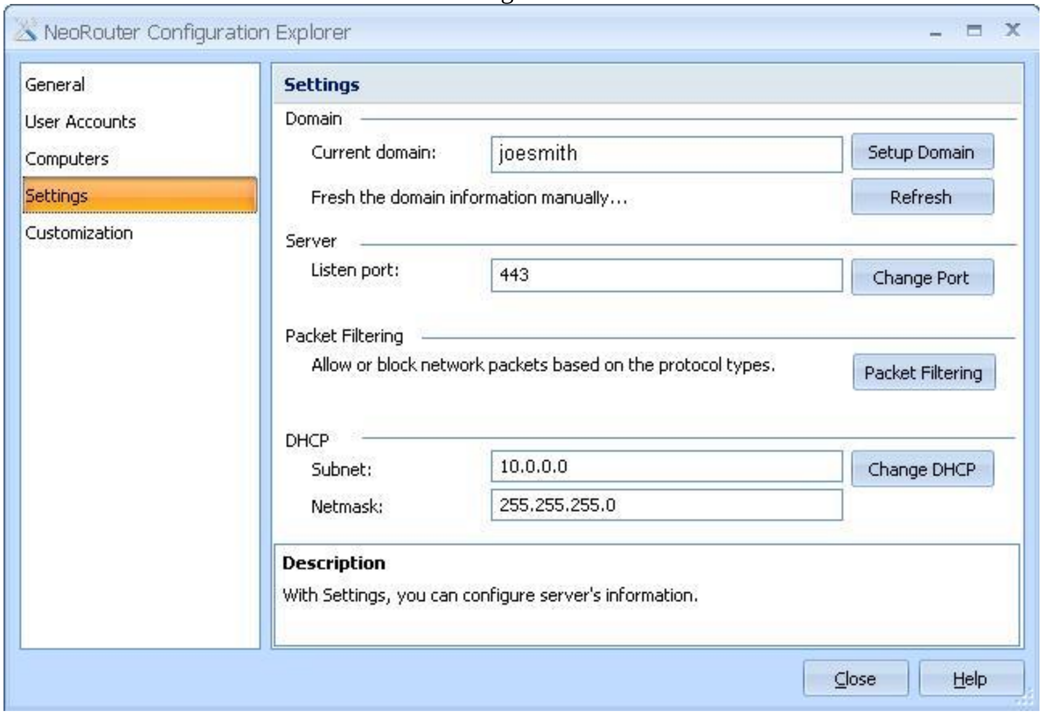
	Default User	Jason (Admin)	Customer A
Default Computer ACL	Block all	Allow all	
Jason's Computer			
Customer A's Computer			
Customer B's Computer			

6.5 Managing Server and Domain

In the Settings page, you can perform the following tasks:

- Change domain name: User should have setup a domain during the server installation. If you decide to change the domain name, you can create a new domain at NeoRouter Dashboard website and then use Configuration Explorer to switch the server to new domain.
- Change Listen Port: this is discussed in the Advanced Configuration chapter.
- Change Packet Filtering: this is discussed in the Advanced Configuration chapter.
- Change DHCP: this is discussed in the Advanced Configuration chapter.

Please restart the NeoRouter server daemon after changes.



Settings

Domain

Current domain: joesmith

Fresh the domain information manually…

Server

Listen port: 443

Packet Filtering

Allow or block network packets based on the protocol types.

DHCP

Subnet: 10.0.0.0

Netmask: 255.255.255.0

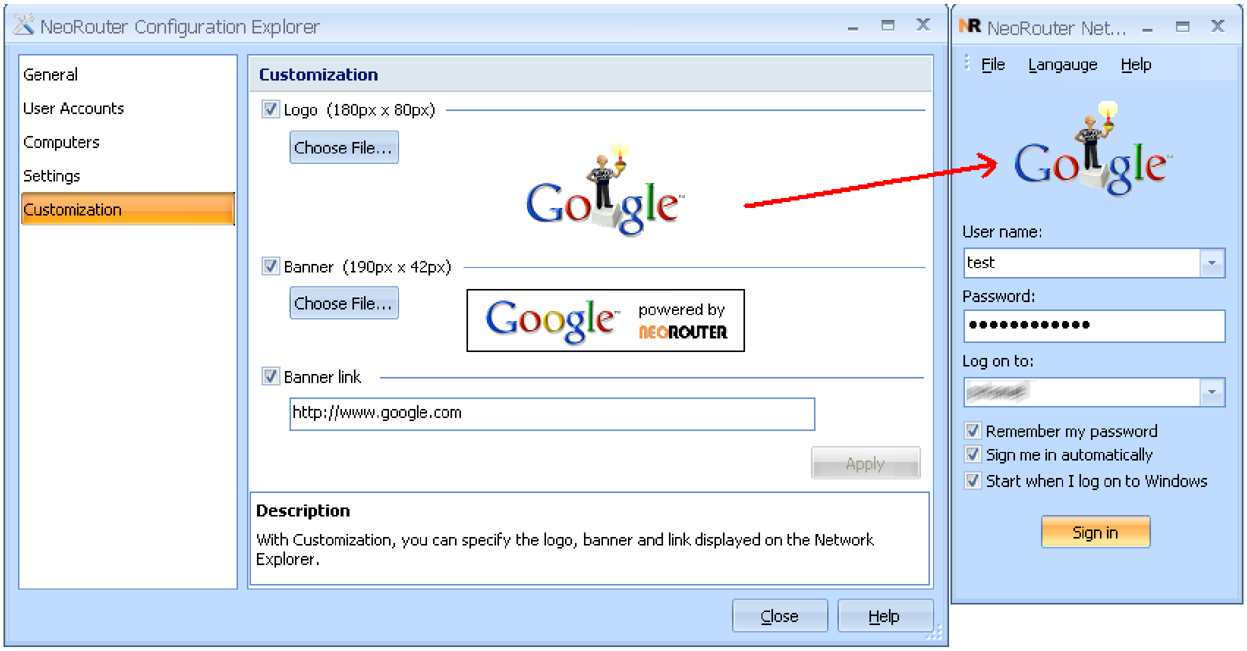
Description

With Settings, you can configure server's information.

6.6 Branding

This feature is available in NeoRouter Profession Edition only.

Admin can customize the logo on the sign-in page NeoRouter Network Explorer and the banner below the computer list. The customization page of the Configuration Explorer allows user to make these changes. The changes will be effective next time user signs into the Network Explorer.



NeoRouter Configuration Explorer

General
User Accounts
Computers
Settings
Customization

Customization

☑ Logo (180px x 80px)

Choose File...

☑ Banner (190px x 42px)

Choose File...

☑ Banner link

http://www.google.com

Apply

Description

With Customization, you can specify the logo, banner and link displayed on the Network Explorer.

Close Help

NeoRouter Net...

File Langauge Help

User name: test

Password: ●●●●●●●●●●●●

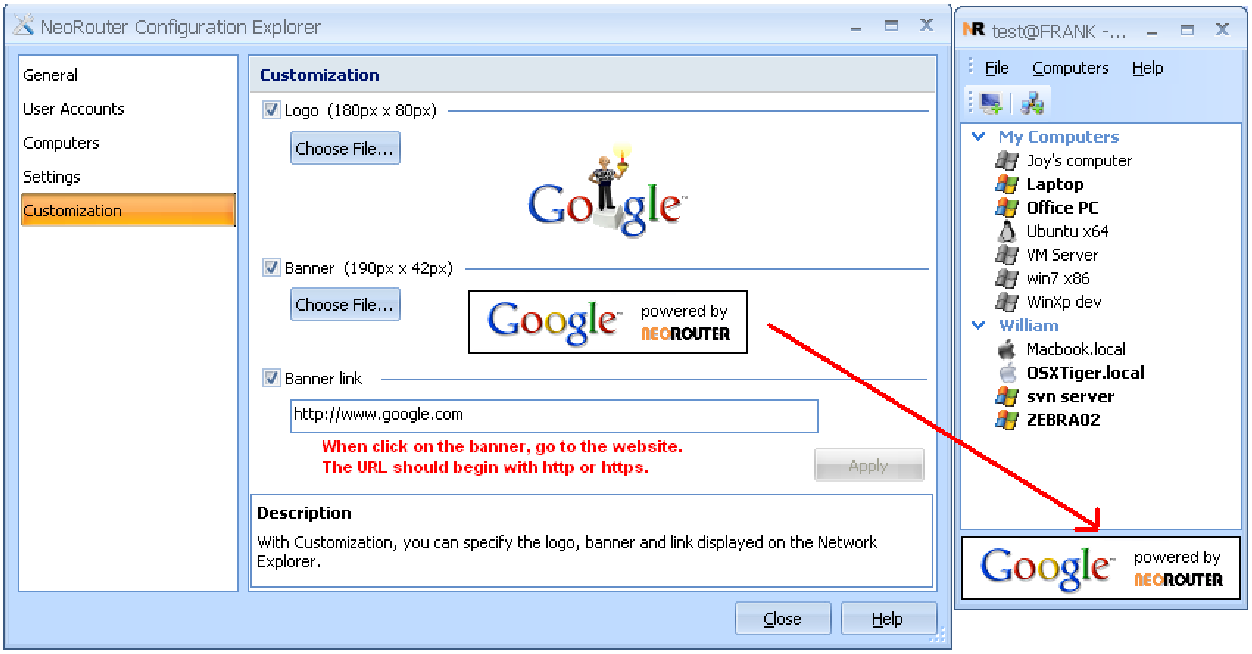
Log on to:

☑ Remember my password

☑ Sign me in automatically

☑ Start when I log on to Windows

Sign in



NeoRouter Configuration Explorer

General
User Accounts
Computers
Settings
Customization

Customization

☑ Logo (180px x 80px)

Choose File...

☑ Banner (190px x 42px)

Choose File...

☑ Banner link

http://www.google.com

When click on the banner, go to the website.
The URL should begin with http or https.

Apply

Description

With Customization, you can specify the logo, banner and link displayed on the Network Explorer.

Close Help

test@FRANK -...

File Computers Help

My Computers
- Joy's computer
- Laptop
- Office PC
- Ubuntu x64
- VM Server
- win7 x86
- WinXp dev

William
- Macbook.local
- OSXTiger.local
- svn server
- ZEBRA02

1. Logo format: custom logo can be .JPG, .JPEG, .BMP or .GIF files. The Logo will be displayed in 180 * 80 pixels and the file will be automatically resized to fit. The color of the pixel at (0, 0) will be used as the transparent color.
2. Banner format: custom banner can be .JPG, .JPEG, .BMP or .GIF files. The banner will be displayed in 190* 42 pixels and the file will be automatically resized to fit.
3. When user clicks on the banner, Network Explorer will launch a web browser and navigate to the link specified in the “Banner Link” box. The banner link should be a valid URL that begins with http://, e.g. http://www.google.com.

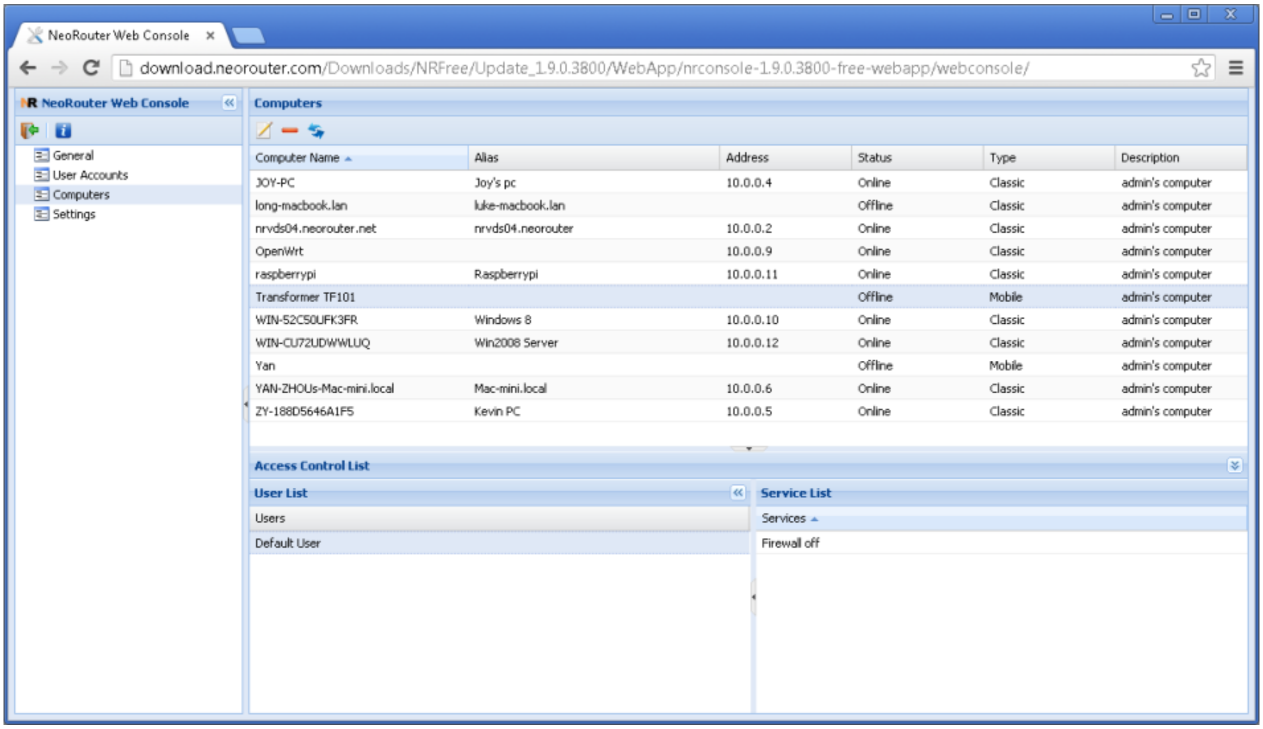
6.7 Server Configuration CLI

Another way to configure the NeoRouter server is to use nrserver's CLI. If user does not have a Windows computer with Configuration Explorer, this tool can be used to set most configurations.

```
Usage: nrserver [options]
-run [--dbroot <DBROOT>]]
-showsettings
-setdomain <DOMAINNAME> <DOMAINPASSWORD>
-setport <PORT>
-dhcp <SUBNET> <NETMASK>
-showusers
-adduser <USERNAME> <PASSWORD> [admin|user]
-setpassword <USERNAME> <NEW PASSWORD>
-setrole <USERNAME> [admin|user]
-enableuser <USERNAME>
-disableuser <USERNAME>
-deleteuser <USERNAME>
-showcomputers
-deletecomputer COMPUTERNAME
-setalias COMPUTERNAME ALIAS
-help
```

6.8 Web Console

Since v2.0, NeoRouter server starts supporting Web Console, that is web version of Configuration Explorer and provides full configuration features. It can be run from any HTML5 based browsers, including Chrome, Firefox, IE10 and BB10.



Computer Name ▲	Alias	Address	Status	Type	Description
JOY-PC	Joy's pc	10.0.0.4	Online	Classic	admin's computer
long-macbook.lan	luke-macbook.lan		Offline	Classic	admin's computer
nrvds04.neorouter.net	nrvds04.neorouter	10.0.0.2	Online	Classic	admin's computer
OpenWrt		10.0.0.9	Online	Classic	admin's computer
raspberrypi	Raspberrypi	10.0.0.11	Online	Classic	admin's computer
Transformer TF101			Offline	Mobile	admin's computer
WIN-52C50UFK3FR	Windows 8	10.0.0.10	Online	Classic	admin's computer
WIN-CU72UDWWLUQ	Win2008 Server	10.0.0.12	Online	Classic	admin's computer
Yan			Offline	Mobile	admin's computer
YAN-ZHOUs-Mac-mini.local	Mac-mini.local	10.0.0.6	Online	Classic	admin's computer
ZY-188D5646A1F5	Kevin PC	10.0.0.5	Online	Classic	admin's computer

Users
Default User

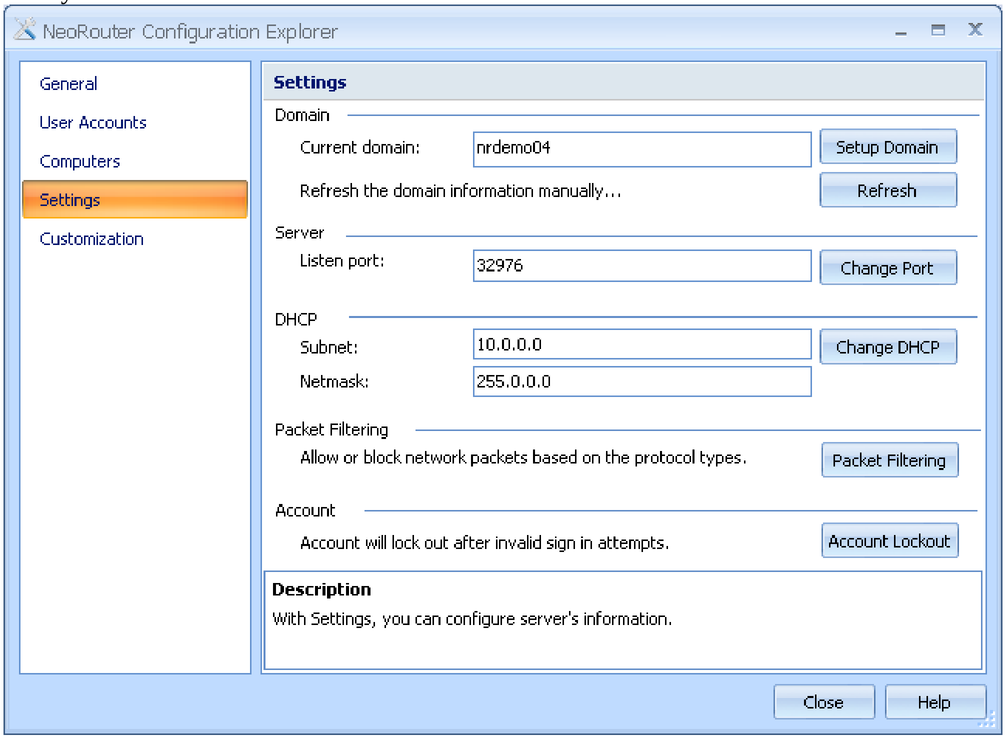
Services ▲
Firewall off

7. Advanced Configuration

7.1 *Change Server Port*

By default, NeoRouter server listens at TCP port 32976 for incoming client connections. User can change the listening port to any valid number between 1 and 65534.

1. Launch Configuration Explorer, sign in, and open the Settings tab.
2. Click on “Change Port” button, input the new listening port and click “Ok” to save the settings.
3. If the NeoRouter Server is running on the same computer, user will be prompted for restarting the NeoRouter Server.
4. If the NeoRouter Server is running on a different computer or device, user needs to restart the server manually.



Current domain: nrdemo04

Refresh the domain information manually…

Listen port: 32976

Subnet: 10.0.0.0

Netmask: 255.0.0.0

Allow or block network packets based on the protocol types.

Account will lock out after invalid sign in attempts.

Description

With Settings, you can configure server's information.

Note:

- The new settings will not take effect until the NeoRouter server stops and restarts
- Since the listening port has been changed, all NeoRouter clients connected to the server will be disconnected and have to reconnect to the server.

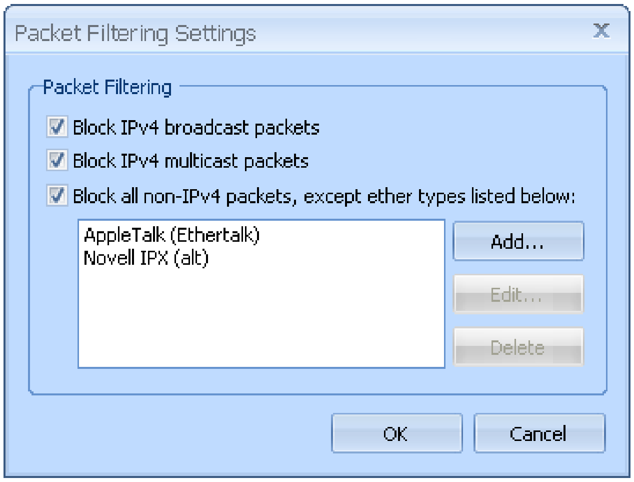
7.2 *Change Packet Filtering*

This feature is available in NeoRouter Profession Edition version 1.2 and above.

Admin can allow or block network packets based on the protocol types. Some LAN-based protocols can be very chatty. If user has a very large number of clients in the virtual LAN, broadcast and multicast packages can use much bandwidth and affect performance. With packet filtering, admin can selectively block nonessential protocols. Packet Filtering currently can block IPv4 broadcast/multicast packets as well as non-IPv4 packets based on their EtherType (http://en.wikipedia.org/wiki/EtherType). One special case is that ARP packets are never blocked regardless of settings.

1. Run Configuration Explorer, sign in and open the “Settings” tab.

2. Click on “Packet Filtering” button, specify the types of packets to block, and then click “Ok” to save the settings
3. If the NeoRouter Server is running on the same computer, user will be prompted for restarting the NeoRouter Server.
4. If the NeoRouter Server is running on a different computer or device, user needs to restart the server manually.



Packet Filtering Settings

Packet Filtering

☑ Block IPv4 broadcast packets

☑ Block IPv4 multicast packets

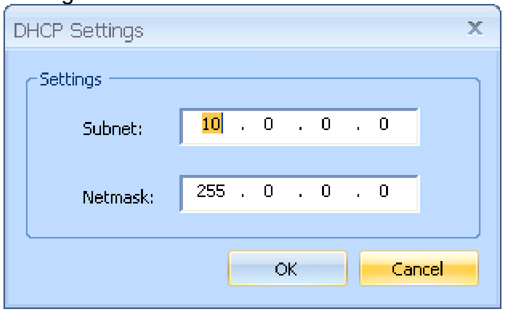
☑ Block all non-IPv4 packets, except ether types listed below:

AppleTalk (Ethertalk)
Novell IPX (alt)

7.3 Change DHCP

NeoRouter server acts as a DHCP server to allocate the virtual IP address when a NeoRouter client connects to it. By default the base IP address is 10.0.0.0/255.255.255.0. User can change the base IP address to any valid network IP address to meet the specific requirements.

1. Run Configuration Explorer, sign in and open the “Settings” tab.
2. Click on “Change DHCP” button, input the new IP address and netmask, and then click “Ok” to save the settings



DHCP Settings

Settings

Subnet: 10 . 0 . 0 . 0

Netmask: 255 . 0 . 0 . 0

3. If the NeoRouter Server is running on the same computer, user will be prompted for restarting the NeoRouter Server.
4. If the NeoRouter Server is running on a different computer or device, user needs to restart the server manually.

Note:

- The new settings will not take effect until the NeoRouter server stops and restarts
- The NeoRouter virtual network range must be valid IP range and not be used by the existing private network

7.4 User Access Auditing

This feature is available in NeoRouter Profession Edition version 1.2 and above. When User Access Auditing is enabled, NeoRouter server will log user access activities, such as sign in and sign out, to a text file. Administrators can then review the log using an editor or text analysis tools.

You can enable this feature using Feature.ini configuration file. The file should be placed under %AllUserAppData%\ZebraNetworkSystems\NeoRouter\ on Windows and /usr/local/ZebraNetworkSystems/NeoRouter/ on Linux or Mac. Here is an example of the Feature.ini.

```
[Default]
Auditing=1
AuditLogFileLocation=c:\audit
MaxNumOfLinesPerLog=20000
```

There are three settings related to the auditing feature.

1. Enable or disable auditing
   Auditing=[1|0]
   1 - enable auditing
   0 - disable auditing
   By default, auditing is disabled.

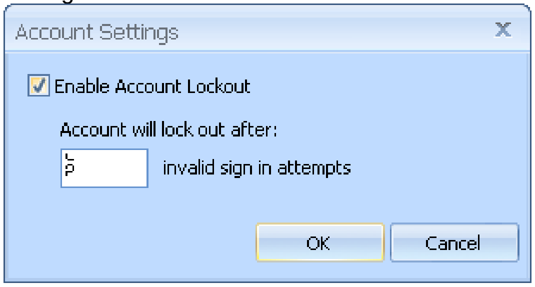
2. Specify the folder for audit log files
   AuditLogFileLocation=[folder for the log files]
   Please make sure the folder exists and nrserver have the write privilege.
   If not specified, the audit log files will be written to the main configuration folder.
   The auditing file name is in the format: NRADT_yyyyMMddHHmmss.log

3. Specify max number of lines in log file
   MaxNumOfLinesPerLog=[integer value]
   Nrserver will start a new log file whenever the current file reaches the maximum number of lines. If the value is not specified or is zero, all data will be logged into a single audit log file.

7.5 *Account Lockout*

This feature is available in NeoRouter Profession Edition version 1.6 and above. When Account Lockout is enabled, NeoRouter server will lock out the account after invalid sign in attempts.

1. Run Configuration Explorer, sign in and open the “Settings” tab.
2. Click on “Account Lockout” button, click on the "Enable Account Lockout" , and then click “Ok” to save the settings


Account Settings

☑ Enable Account Lockout

Account will lock out after: 5 invalid sign in attempts

3. One can also change the number of attempts allowed before locking out the account.

7.6 *Network Bridge*

7.6.1 Overview

(Note: This feature has been dropped since v1.9)

NeoRouter (v0.9.9 to v1.6.3) supports the Network Bridge feature, which uses two very different means for interconnecting networks: routing and bridging. Once the feature is enabled, the ACL feature will be disabled automatically, as we cannot control the packets from the external networks anymore and may cause security issues if it's not setup properly. So, this is an advanced feature for the users who know about it every well.

- **Routing** - refers to the interconnection of separate and independent "sub-networks" (subnets) which have non-overlapping ranges of IP addresses. Upon receiving a packet sent to it, a network "router" examines the destination IP address to determine which of several connected networks should receive it, after which that packet is forwarded to the proper network.

- **Bridging** - by comparison, is much simpler. A network "bridge" is simply an electrical interconnection between separate physical networks that are all carrying the same ranges of IP addresses. Standard dumb network "hubs" and "switches" are examples of network bridges. With a hub, packets arriving at any port are "bridged" and sent out to every other port. A switch is a bit smarter, since it is able to adaptively learn which network interface cards (NICs) are attached to which ports. But a switch is still interconnecting network segments carrying the same ranges of IP addresses.

7.6.2 Routing vs. Bridging

Although "routed" connections are the most common and straightforward to configure, they suffer from significant operational limitations. By comparison, "bridged" connections are generally much trickier to configure, and are not even natively available under all operating systems, so they are not the default connection type. But when bridging is properly setup it correctly does everything that we want.

Bridging and routing are functionally very similar, with the major difference being that a routed VPN will not pass IP broadcasts while a bridged VPN will.

- Routing advantages
  - Efficiency and scalability.
  - Allows better tuning of MTU for efficiency.
- Routing disadvantages
  - Clients must use a WINS server (such as samba) to allow cross-VPN network browsing to work.
  - Routes must be set up linking each subnet.
  - Software that depends on broadcasts will not "see" machines on the other side of the VPN.
  - Works only with IPv4 in general and IPv6 in cases where tun/tap drivers on both ends of the connection support it explicitly.
- Bridging advantages
  - Broadcasts traverse the VPN -- this allows software that depends on LAN broadcasts such as Windows NetBIOS file sharing and network neighborhood browsing to work.
  - No route statements to configure.
  - Works with any protocol that can function over ethernet
  - Relatively easy-to-configure solution for road warriors.
- Bridging disadvantages
  - Less efficient than routing, and does not scale well.

7.6.3 Setup Network Bridge

With either bridging mode or routing mode, one can create point-to-site VPN, site-to-site VPN or even multiple site-to-site networks. Once a network structure is well designed, one can use Feature.ini file to control NeoRouter client service to implement it.

The file Feature.ini is located in the main configuration folder, which can be various for different OS.

- On Windows Xp:

X:\Documents and Settings\All Users\Application Data\ZebraNetworkSystems\NeoRouter

- On Vista+:

X:\Users\All Users\ZebraNetworkSystems\NeoRouter
On Linux and Mac OSX:
/usr/local/ZebraNetworkSystems/NeoRouter

- On in-a-box:

/jffs
If it does not exist, please create one.

The only thing to do is define the parameters in the Feature.ini file.

- NetworkBridge=1
- LANSegment parameter

This is a set of parameters used for mapping the external IP address or IP range to a virtual IP address, so that NeoRouter can route the packets to the proper tunnel. It's defined in the following format:
LANSegment[index]=[IP|IP range|segment],VIP

[index] - number, start from 1, for example: 1,2,3...
[IP] - a valid external IP address, for example: 192.168.129.126
[IP range] - a set of external IP addresses, in the format as IP_BEGIN-IP_END. For example: 192.168.129.126-192.168.129.128
[segment] - a set of external IP addresses, in the format as SUBNETWORK/NETMASK. For example: 192.168.129.0/255.255.255.0

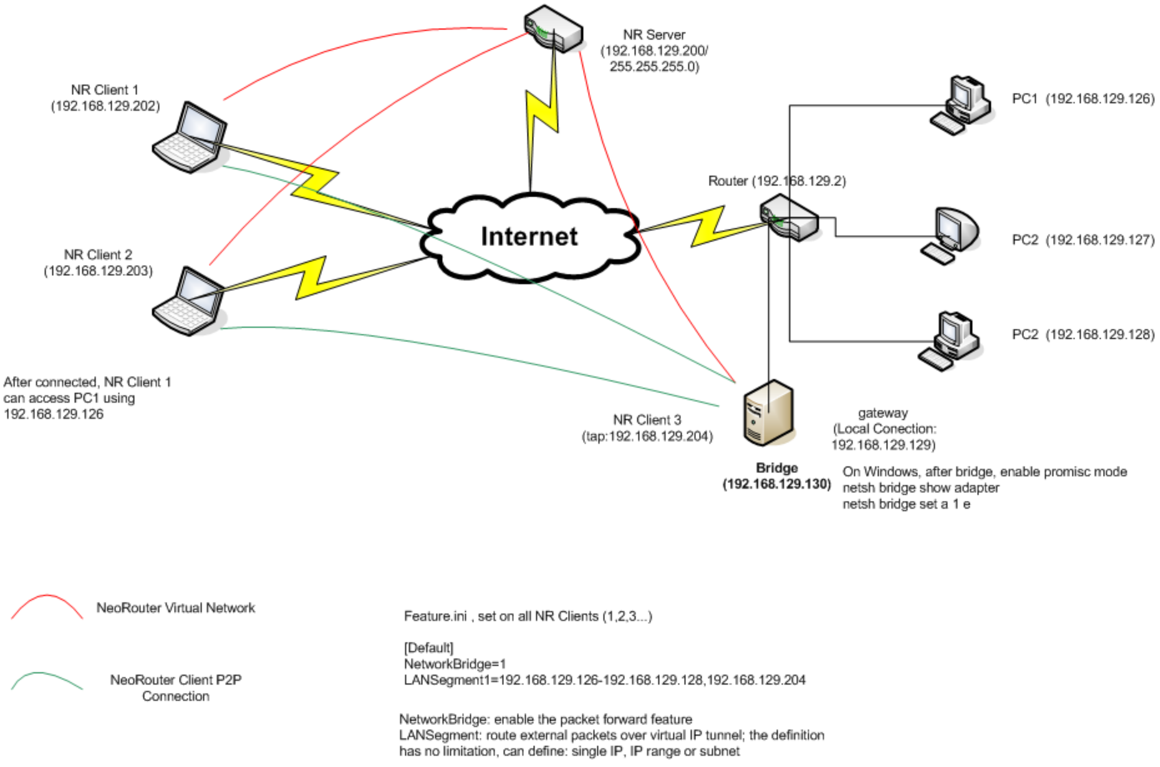
For example:

```
[Default]
NetworkBridge=1
LANSegment1=192.168.129.126-192.168.129.128,192.168.129.204
LANSegment2=192.168.129.120,192.168.129.205
LANSegment3=192.168.3.0/255.255.255.0,192.168.129.206
```

In the sample above, the setting tells NeoRouter how to route packets.

Here are several common scenarios.

7.6.4 Bridging Setup – point to site VPN



After connected, NR Client 1
can access PC1 using
192.168.129.126

On Windows, after bridge, enable promisc mode

```
netsh bridge show adapter
netsh bridge set a 1 e
```

Feature.ini , set on all NR Clients (1,2,3...)

```
[Default]
NetworkBridge=1
LANSegment1=192.168.129.126-192.168.129.128,192.168.129.204
```

NetworkBridge: enable the packet forward feature
LANSegment: route external packets over virtual IP tunnel; the definition has no limitation, can define: single IP, IP range or subnet

- Requirement:

A company wants create a point-to-site VPN, so that the employees can remotely access the printers or computers in the office from home or customer site. Since NeoRouter client cannot be installed on the printers and some computers, that are running Unix OS (HP-Unix, Solaris or SCO Unix), the NeoRouter Network Bridge feature would the best choice.

- Design:

Since we want to use the printer, it's better to use the bridging mode. Depending on the requirements, we split the network into 3 groups.
1. 192.168.129.126 - 192.168.128.128 used for computers or printers
2. 192.168.129.200 - 192.168.129.254 used for NeoRouter DHCP
3. Other IP address we don't want packets from these IP range go to our VPN

- Setup:

1. Setup NeoRouter server and config the DHCP address to 192.168.129.200/255.255.255.0
2. Setup the gateway computer by creating a bridge to combine the NeoRouter virtual adapter and a local adapter.

On Windows XP+ (except WinXp x64), one can use Windows tool to create a bridge.
(check out MSDN for details).
Since some adapters may not fully support prosmic mode, one has to enable it manually.
(check out http://support.microsoft.com/kb/302348)

```
> netsh bridge show adapter
> netsh bridge set a 1 e
> netsh bridge set a 2 e
```

On Linux, one can use brctl command to create a bridge

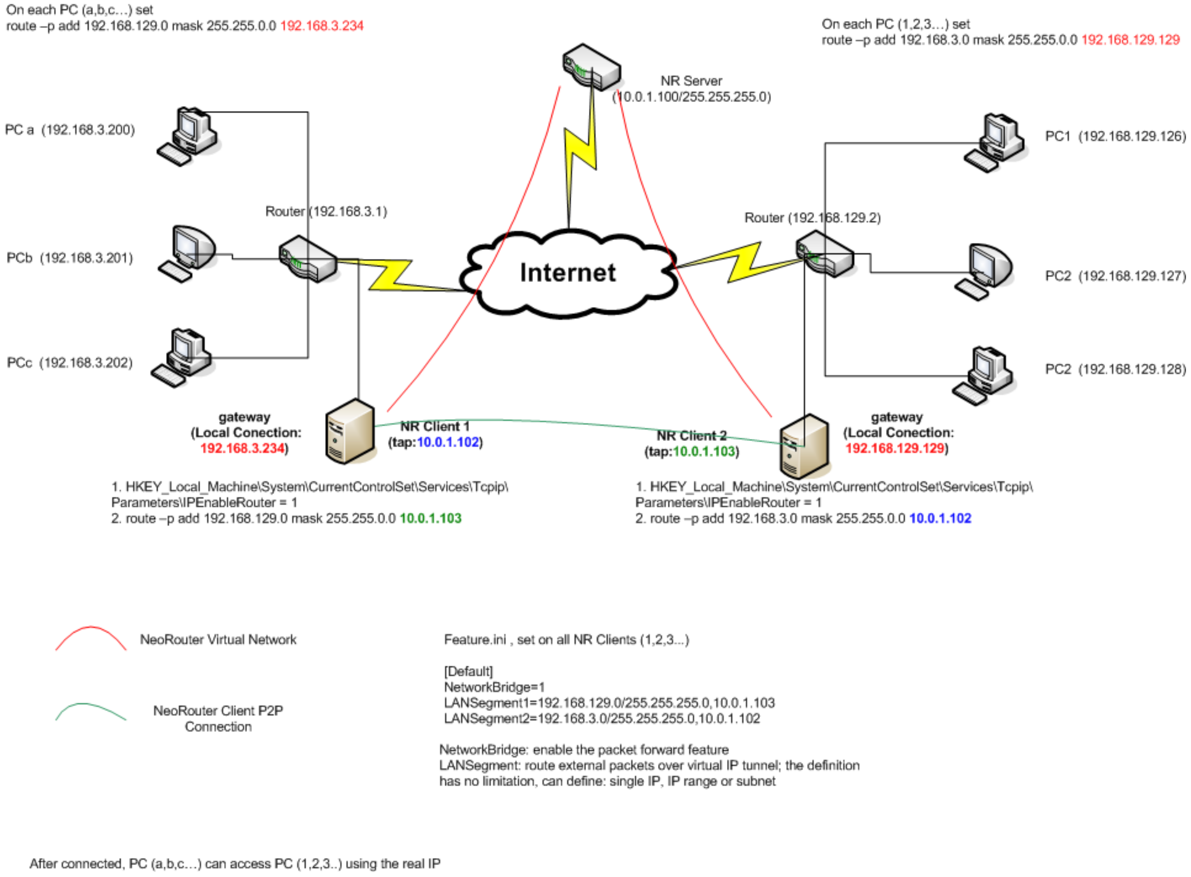
```
> brctl addbr $br
> brctl addif $br eth0
> brctl addif $br nrtap
> ifconfig nrtap 0.0.0.0 promisc up
> ifconfig eth0 0.0.0.0 promisc up
> ifconfig $br $eth_ip netmask $eth_netmask broadcast $eth_broadcast
>
> ifconfig $br down
> brctl delbr $br
```

3. Setup Feature.ini file on each member of the NeoRouter network. The content of the file is:

```
[Default]
NetworkBridge=1
LANSegment1=192.168.129.126-192.168.129.128,192.168.129.204
```

After setting the file, restart the nrservice or reboot computer.

7.6.5 Routing Setup – site to site VPN



On each PC (a,b,c…) set

```
route –p add 192.168.129.0 mask 255.255.0.0 192.168.3.234
```

On each PC (1,2,3…) set

```
route –p add 192.168.3.0 mask 255.255.0.0 192.168.129.129
```

```
1. HKEY_Local_Machine\System\CurrentControlSet\Services\Tcpip\
Parameters\IPEnableRouter = 1
2. route –p add 192.168.129.0 mask 255.255.0.0 10.0.1.103
```

```
1. HKEY_Local_Machine\System\CurrentControlSet\Services\Tcpip\
Parameters\IPEnableRouter = 1
2. route –p add 192.168.3.0 mask 255.255.0.0 10.0.1.102
```

Feature.ini , set on all NR Clients (1,2,3...)

```
[Default]
NetworkBridge=1
LANSegment1=192.168.129.0/255.255.255.0,10.0.1.103
LANSegment2=192.168.3.0/255.255.255.0,10.0.1.102
```

NetworkBridge: enable the packet forward feature
LANSegment: route external packets over virtual IP tunnel; the definition has no limitation, can define: single IP, IP range or subnet

After connected, PC (a,b,c…) can access PC (1,2,3..) using the real IP

- Requirement:

A company wants create a site-to-site VPN to link two offices located in different cities. They cannot install NeoRouter client software on their computers running Unix OS (HP-Unix, Solaris or SCO Unix). The NeoRouter Network Bridge feature would be the best choice.

- Design:

To make the VPN fast, it's better to use the routing mode. From the requirements, we can see 3 networks.
1. 192.168.129.0/255.255.255.0 Office 1
2. 192.168.3.0/255.255.255.0 Office 2
3. 10.0.1.0/255.255.255.0 NeoRouter virtual network

- Setup:

1. Setup NeoRouter client on each gateway computers
2. One each gateway computer, enable the feature allowing the OS to forward packets

On Windows 2000+,
create HKEY_Local_Machine\System\CurrentControlSet\Services\Tcpip\Parameters\IPEnableRouter as a string value equal to 1 in the registry. This will require a system reboot to take effect. To confirm it is enabled, do ipconfig /all from the command line. IP Routing Enabled should say yes. If not, confirm your registry setting and reboot again. This setting is flaky in non-server versions of Windows.

Also refer to http://support.microsoft.com/kb/230082/en-us

On Linux,

```
> echo 1 > /proc/sys/net/ipv4/ip_forward
```

On Mac OS X,
1) The easy way is to create or edit /etc/sysctl.conf and add net.inet.ip.forwarding=1
or
2) > *sysctl -w net.inet.ip.forwarding=1*

3. Setup route on each gateway

On the gateway of the 192.168.3.x network:
> route –p add 192.168.129.0 mask 255.255.0.0 10.0.1.103

On the gateway of the 192.168.129.x network:
> route –p add 192.168.3.0 mask 255.255.0.0 10.0.1.102

4. Setup route stable. When using routing method, you need to tell your other machines how to cross the VPN to access computers on the opposite network.

Option1:

This requires more work, but limits configuration changes to be at the computer level.

On each computer of the 192.168.3.x network:
> route –p add 192.168.129.0 mask 255.255.0.0 192.168.3.234

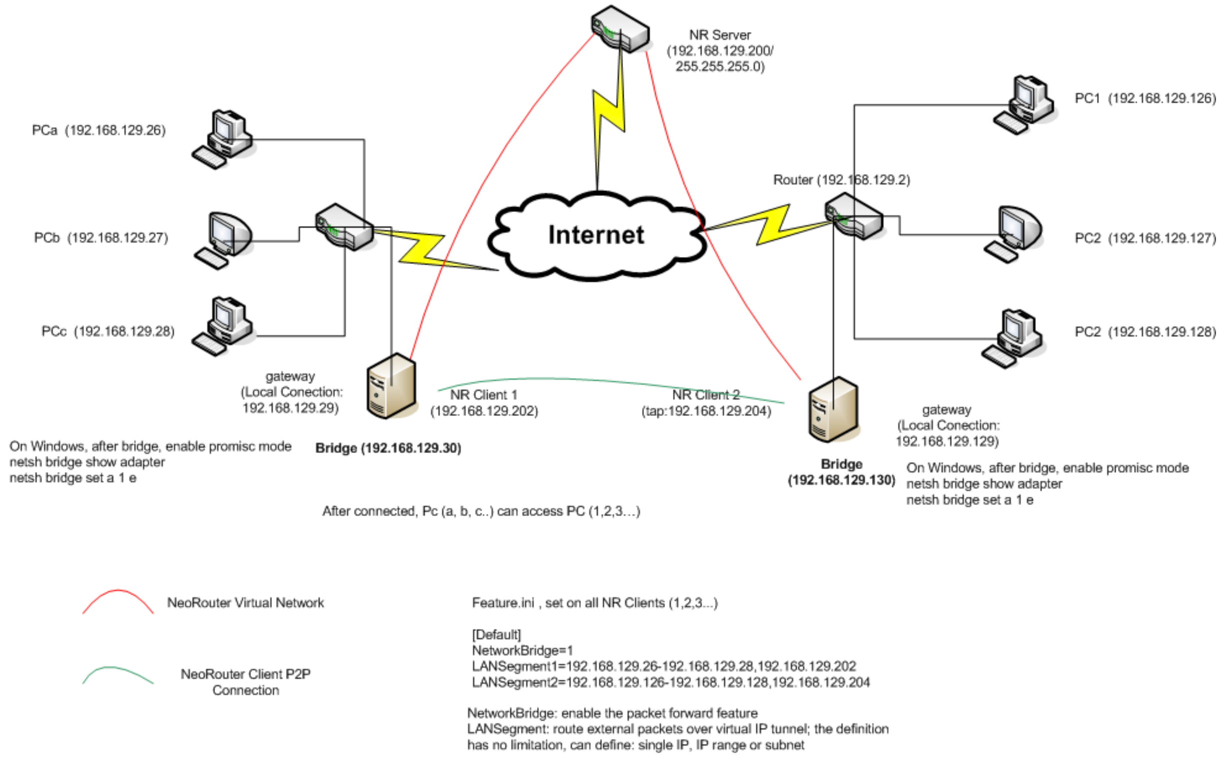
On each computer of the 192.168.129.x network:
> route –p add 192.168.3.0 mask 255.255.0.0 192.168.129.129

Option 2: (not all routers support this, but it is the minimal configuration method)

On the router acting as the default gateway for 192.168.3.x network, add a static route that says any traffic destined for 192.168.129.0 network go through 192.168.3.x (IP address of NeoRouter PC on 192.168.3.x network)

On the router acting as the default gateway for 192.168.129.x network, add a static route that says any traffic destined for 192.168.3.0 network go through 192.168.129.x (IP address of NeoRouter PC on 192.168.129.x network)

7.6.6 Bridging Setup – site to site VPN



On Windows, after bridge, enable promisc mode

```
netsh bridge show adapter
netsh bridge set a 1 e
```

On Windows, after bridge, enable promisc mode

```
netsh bridge show adapter
netsh bridge set a 1 e
```

After connected, Pc (a, b, c..) can access PC (1,2,3…)

Feature.ini , set on all NR Clients (1,2,3...)

```
[Default]
NetworkBridge=1
LANSegment1=192.168.129.26-192.168.129.28,192.168.129.202
LANSegment2=192.168.129.126-192.168.129.128,192.168.129.204
```

NetworkBridge: enable the packet forward feature
LANSegment: route external packets over virtual IP tunnel; the definition has no limitation, can define: single IP, IP range or subnet

7.6.7 Run Scripts

When Network Bridge feature is enabled, one can define commands getting called by NR Client on the following events.

These commands should be defined in the Feature.ini file.

1.When initialize the tap device, but not activate it yet
CmdOnTapInit=xxxxxxxxx

2.When the tap device gets activated
CmdOnTapActive=xxxxxxxxx

3.When tap device gets destroyed
CmdOnTapUninit=xxxxxxxxx

These options are available on all platforms.
For example, one can define a script to setup static route table after the tap gets activated and has virtual IP address assigned.

Feature.ini

```
....
CmdOnTapActive=/usr/bin/setroutetable.sh
....
```

7.7 *Build Custom Add-on (Windows)*

7.7.1 Create Custom Add-on

You can customize an add-on or even create your own.

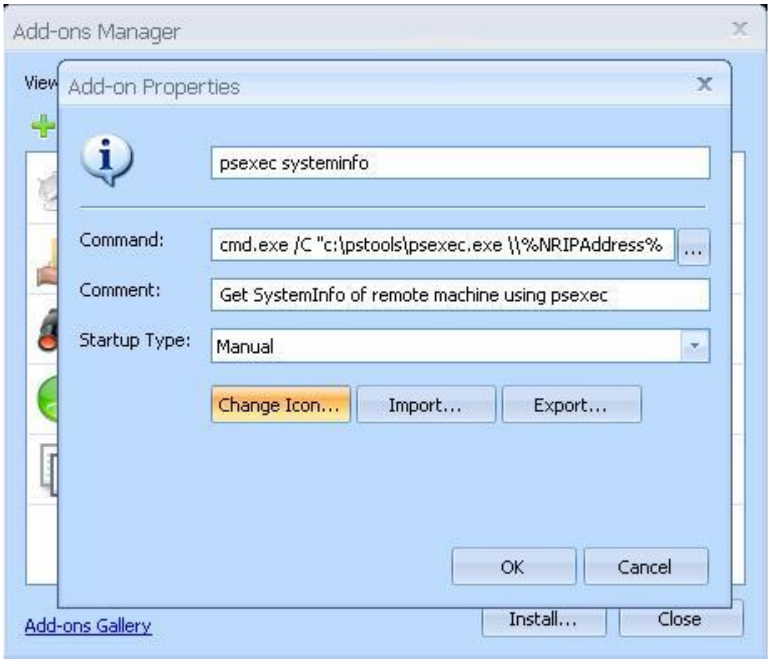
As an example, let's create an add-on to get the system info of a remote computer using PsTools by Mark Russinovich and systeminfo.exe command shipped with Windows.

- PsTools: http://technet.microsoft.com/en-us/sysinternals/bb896649.aspx
- systeminfo: http://technet.microsoft.com/en-us/library/bb491007.aspx

1. Launch NeoRouter Network Explorer, open Add-ons Manager dialog
2. Click "+" button to create a new add-on
3. In add-on properties dialog, enter the following:
   - Add-on name: psexec systeminfo
   - Command:

     cmd.exe /C "c:\pstools\psexec.exe \\%NRIPAddress% -u <username> systeminfo & pause"

     Please replace <username> with username on the remote computer
   - Comment: Get SystemInfo of remote machine using psexec
   - Startup Type: Manual
   - Icon: click "Change Icon" button to choose one that's easy to recognize.



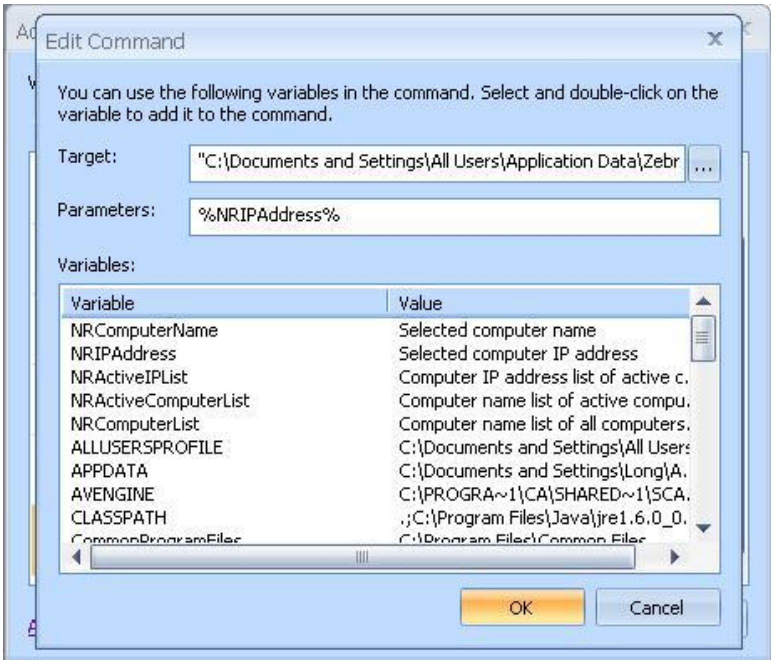
psexec systeminfo

Command: cmd.exe /C "c:\pstools\psexec.exe \\%NRIPAddress%

Comment: Get SystemInfo of remote machine using psexec

Startup Type: Manual

4. In the command, you can use Windows environment variables or NeoRouter variables like "%NRIPAddress%". If you click on the "..." button next to the Command edit box, you will see the "Edit Command" dialog with a list of variables you can use.



You can use the following variables in the command. Select and double-click on the variable to add it to the command.

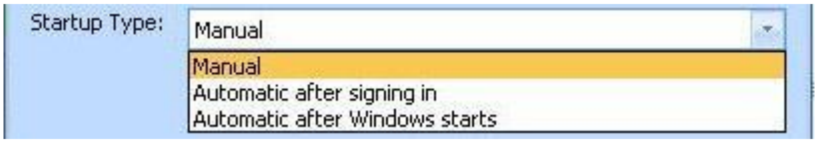
Target: "C:\Documents and Settings\All Users\Application Data\Zebr

Parameters: %NRIPAddress%

Variables:

Variable	Value
NRComputerName	Selected computer name
NRIPAddress	Selected computer IP address
NRActiveIPList	Computer IP address list of active c.
NRActiveComputerList	Computer name list of active compu.
NRComputerList	Computer name list of all computers.
ALLUSERSPROFILE	C:\Documents and Settings\All Users
APPDATA	C:\Documents and Settings\Long\A.
AVENGINE	C:\PROGRA~1\CA\SHARED~1\SCA.
CLASSPATH	.;C:\Program Files\Java\jre1.6.0_0.
CommonProgramFiles	C:\Program Files\Common Files

5. Three "Startup types" are supported:

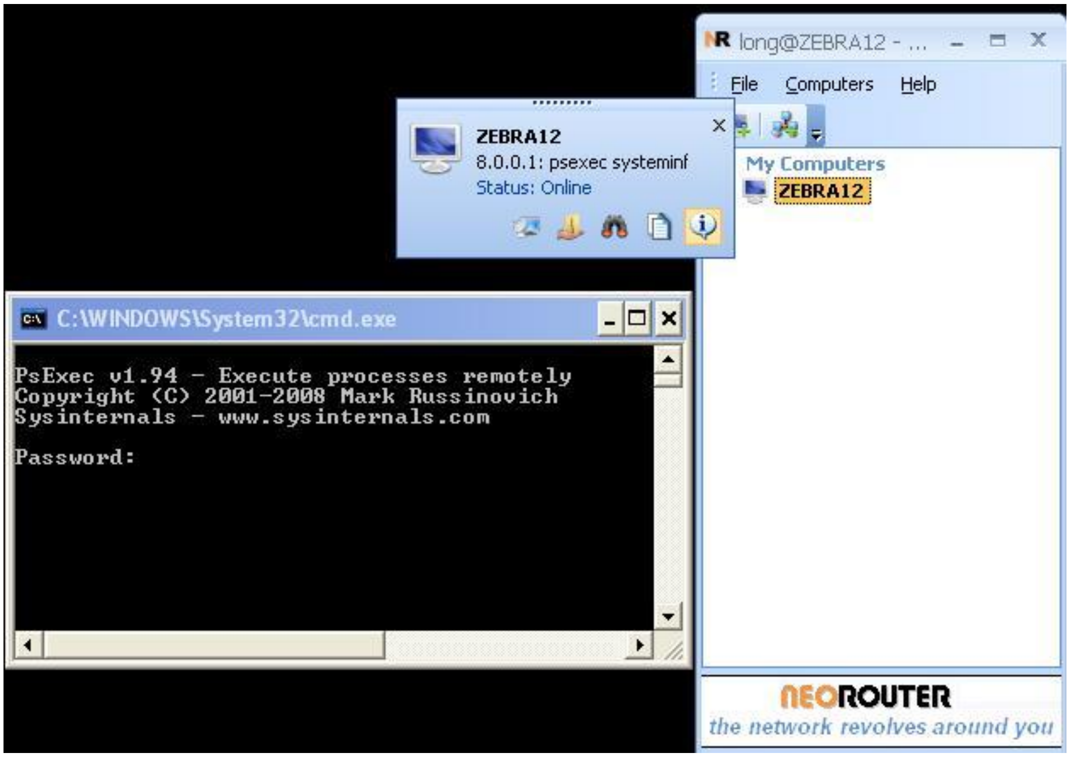


Startup Type: Manual

Manual
Automatic after signing in
Automatic after Windows starts

- **Manual**: the add-on will be displayed in the launch pad of Network Explorer and user can manually launch the program.
- **Automatic after signing in**: the add-on command is automatically executed when user signs into NeoRouter Network Explorer.
- **Automatic after Windows starts**: the add-on command is automatically executed when Windows starts.

6. Launch the new add-on, just click on the target computer in Network Explorer, and choose the add-on in the pop-up launch pad.



```
PsExec v1.94 - Execute processes remotely
Copyright (C) 2001-2008 Mark Russinovich
Sysinternals - www.sysinternals.com

Password:
```

7. In the above steps, I have assumed that PsTools are installed at "c:\PsTools" and the remote computer has telnet service enabled. If not, let's configure the system now.
   PsTools: download from http://technet.microsoft.com/en-us/sysinternals/bb896649.aspx, and extract to "c:\PsTools" folder

8. Configure telnet service on remote computer: This step is required on XP/Vista, but not necessary on Windows 2003/2008 servers.
   - Run services.msc from the "Start -> Run" command window and configured the Telnet service for Automatic. Start the service.
   - Follow the instructions here: http://support.microsoft.com/kb/298060/en-us
   - Launch Windows firewall, and add C:\WINDOWS\System32\tlntsvr.exe to exception list.

7.7.2 Add-on File Formats

NeoRouter supports two types of add-on files: *.nri and *.nra. Most users only need to deal with *.nri files; all files downloaded from http://www.neorouter.com/addons/index.html are in this format. *.nra files are used by advanced users to build custom add-ons.

- **.nri** is the full installation package that contains both the application and the the configure info. Users can simply download *.nri files from and use the "Install" button to setup the add-on.
- **.nra** contains only the configuration info. Advanced users can create custom add-ons and export the configuration info as *.nra files using the "Export" button in the add-on properties dialog. Then he/she can import the *.nra file on another client. But remember that you will need to manually setup the application as well.

7.8 Configuration Files

NeoRouter uses multiple configuration files to control some advanced features. The most useful files are Feature.ini and Log.ini. Feature.ini is used for customizing some internal feature set, performance tuning and debugging purpose. Log.ini is used for tracing application information for troubleshooting.

We provide the file templates as below:

7.8.1 Feature.ini template

```
#==================================================================
# Feature.ini
#
# This is the feature set configuration file for NeoRouter software.
# If contains the configuration directives that give both client
# and server programs instructions.
#
# This file should be located in the main configuration folder of
# NeoRouter. For NeoRouter Portable, this file can be loaded from
# the same folder as the executable file.
#
# Any changes to this file won't take into effect until the
# application restarts.
#
# If there is no value assigned to a setting key, default value will
# be choose.
#==================================================================

[Default]
#Description: Current Language LocaleID
#Options:     local ID on Windows
#Default:     1033
LangId=1033

#Description: Current Skin Name
#Options:     Skin file name
#Default:     Office2007.styles
SkinName=Office2007.styles

#Description: Current Skin Style
#Options:     Skin style name
#Default:     NormalBlue.ini or NormalAqua.ini
SkinStyle=NormalBlue.ini

#Description: Create P2P connection between peers
#Options:     0-Disabled; 1-Enabled
#Default:     1
P2P=1

#Description: Support UDP P2P only (do not try TCP P2P connection)
```

```
#Options:     0-Disabled; 1-Enabled
#Default:     1
UdpOnly=1

#Description: Encrypt packets before sending
#Options:     0-Disabled; 1-Enabled
#Default:     1
Encrypt=1

#Description: Compress packets between befor sending (without encrption)
#Options:     0-Disabled; 1-Enabled
#Default:     0
Compress=0

#Description: Compress and encrypt packets before sending
#Options:     0-Disabled; 1-Enabled
#Default:     0
CompressEncrypt=0

#Description: Number of threads in the thread pool (Windows and Linux ONLY)
#Options:     2*number of CPU cores
#Default:     5
MaxInstanceThreads=5

#Description: Maintain TCP connection using heart beat mechanism
#Options:     0-Disabled; 1-Enabled
#Default:     1
TcpHeartBeat=1

#Description: The type of heart beat for TCP
#Options:     0-keep ping; 1-ping when idle
#Default:     1
TcpHeartBeatMode=1

#Description: Maintain UDP connection using heart beat mechanism
#Options:     0-Disabled; 1-Enabled
#Default:     1
UdpHeartBeat=1

#Description: The type of heart beat for UDP
#Options:     0-keep ping; 1-ping when idle
#Default:     1
UdpHeartBeatMode=1

#Description: time interval between keep alive probes
#Options:     >0
#Default:     15 seconds
KeepAliveIntvl=15
```

```
#Description: time of connection inactivity after which the first keep alive
request is sent
#Options:     >0
#Default:     15 seconds
KeepAliveTime=15

#Description: number of keep alive requests retransmitted before the
connection is considered broken. For example, when a client lost network
connection for total time = KeepAliveTime + KeepAliveIntvl * KeepAliveProbes,
it will be traded as disconnected.
#Options:     >0
#Default:     3 times
KeepAliveProbes=3

#Description: Close the P2P tunnel when it's idle
#Options:     0-Disabled; 1-Enabled
#Default:     1
AutoDisconnectTunnel=1

#Description: Work with bSupportAutoDisconnectTunnel, time of a tunnel when
idle
#Options:     >0
#Default:     600 seconds (10min)
TunnelAliveTime=600

#Description: Keep TCP connection alive
#Options:     0-Disabled; 1-Enabled
#Default:     1
KeepAlive=1

#Description: Socket Send Buffer
#Options:     > 8KB
#Default:     2097152 Bytes (2MB)
SoSendBuf=2097152

#Description: Socket Recv Buffer
#Options:     > 8KB
#Default:     2097152 Bytes (2MB)
SoRecvBuf=2097152

#Description: Timer for creating p2p tunnel
#Options:     > 600000
#Default:     600000 ms (10 min)
TunnelP2PTimerInterval=600000

#Description: Reset tap device when switch domain (Windows ONLY)
#Options:     0-Disabled; 1-Enabled
```

```
#Default:     1
RestartTap=1

#Description: Virtual IP metric
#Options:     >0
#Default:     9000
VIPMetric=9000

#Description: Run script before tap gets initialized
#Options:     Any script or command
#Default:
CmdOnTapInit=

#Description: Run script after tap is initialized
#Options:     Any script or command
#Default:
CmdOnTapActive=

#Description: Run script when tap get uninitialized
#Options:     Any script or command
#Default:
CmdOnTapUninit=

#Description: Keep custom changes, such as add-ons, DNS cache, proxy and so
on
#Options:     0-Disabled; 1-Enabled
#Default:     1
ForceKeepSetting=1

#Description: Check DNS cache first when parsing NeoRouter Domain Name,
instead of calling NeoRouter Domain server
#Options:     0-Disabled; 1-Enabled
#Default:     1
DNSCache=0

#Description: Interval to refresh DNS cache
#Options:     > 0
#Default:     15 days
DNSCacheExpireTime=15

#Description: Server updates domain server automatically (once a hour)
#Options:     0-Disabled; 1-Enabled
#Default:     1
AutoUpdateDomain=1

#Description: Trade the log on name as NeoRouter Domain name instead of a
computer name
#Options:     0-Disabled; 1-Enabled
```

```
#Default:     1
NRDomain=1

#Description: Alternative server IP address
#Options:     local IP address of the server, in format [domain name],[local
ip address]:[port]
#Example:     testdomain,192.168.0.115:32976
#Default:
AltServer=

#Description: Network Interface name used for getting MAC address
#Options:     the primary network interface having MAC address
#Default:     eth (on Linux) or ed (on FreeBSD)
NicInterfaceName=eth

#Description: Hardware ID for client (it's used when cannot find a valid
network interface on Linux)
#Options:     Any unique string
#Default:
HardwareId=

#Description: Allow to create point-to-site or site-to-site VPN
#Options:     0-Disabled; 1-Enabled
#Default:     0
NetworkBridge=0

#Description: Hardware ID for client (it's used when cannot find a valid
network interface on Linux)
#Options:     Any unique string
#Default:     The parameters are in the format below:
#             LANSegment[nIndex]=[value]
#             [nIndex] is a number (>0);
#             [value] is a string in the format: Network/SubnetMask,VIP
#LANSegment1=192.168.0.100,10.0.0.1
#LANSegment2=192.168.2.0/255.255.255.0,10.0.0.2
#LANSegment3=192.168.3.100-192.168.3.149,10.0.0.3

#Description: Server audits users activities
#Options:     0-Disabled; 1-Enabled
#Default:     0
Auditing=0

#Description: Max Lines of a Log File, after that a new log file will be
created
#Options:     0-unlimited
#Default:     0
MaxNumOfLinesPerLog=0
```

```
#Description: Path of the audit file
#Options:     a folder with proper permission
#Default:     main configuration folder
AuditLogFileLocation=

#Description: Specify protocol nrserver uses
#Options:     1-compatible with v1 or v2 clients; 2-clients must be v2.
#Default:     1
ProtocolVersion=1

#Description: Specify host IP type for nrserver
#Options:     0-detect; 1-IPv4; 2-IPv6; 3-Dual
#Default:     0
HostIPType=0

#Description: Max number of client connections that are
connecting/authenticating to nrserver
#Options:     > 0
#Default:     10
ServerAuthBacklog=10

#Description: Support Web Gateway
#Options:     0-Disabled; 1-Enabled
#Default:     1
WebGateway=1

#Description: Support Web Console
#Options:     0-Disabled; 1-Enabled
#Default:     1
WebConsole=1

#Description: Support Web Client
#Options:     0-Disabled; 1-Enabled
#Default:     1
WebClient=1

#Description: Whether can sign in with Server host OS user account
#Options:     0-Disabled; 1-Enabled
#Default:     1
SupportOSUser=1

#Description: Whether disable SSLv3 protocol and use TLS only
#Options:     0-Disabled; 1-Enabled
#Default:     1
DisableSSLv3=1

#Description: The interval for re-create p2p tunnel.
#Options:     Seconds. 0 - disabled; suggested value: 10*60
```

```
#Default:     0
TunnelP2PRetryInterval=0

#Description: Timeout value of client connections that are
connecting/authenticating to nrserver
#Options:     milliseconds. > 17000
#Default:     17*1000
ServerAuthTimeout=17000

#Description: Min listen port when establishing P2P connection
#Options:     0 - use port allocated by OS; > 0 specify start port number of
the port range, that is used by Client to establish P2P connections.
#Default:     0
MinP2PListenPort=0

#Description: Max number of retry times to activate Tap
#Options:     >=0
#Default:     12
TapRetryTimes=12

#Description: Before next Tap activation, it waits for n seconds
#Options:     >=0
#Default:     10
TapRetryPeriod=10

#Description: Before verifying Tap status, it waits for n seconds
#Options:     >=0
#Default:     5
TapVerifyInterval=5
```

7.8.2 Log.ini template

```
#==================================================================
# Log.ini
#
# This is the logging configuration file for NeoRouter software.
# If contains the configuration directives that give both client
# and server programs instructions.
#
# This file will be searched in the following paths:
# 1. the same folder as the executable file
# 2. the main configuration folder
#
# Any changes to this file won't take into effect until the
# application restarts.
#
# If there is no value assigned to a setting key, default value will
# be choosen.
#
# If a specific application section gets defined, the values in the
# [Default] section would be replaced with the specific values if
# it is re-defined
#
#MASK
#  Format: FF FFFFFF = Level Modules
#  ALL   : FF FFFFFF = 4294967295
#  TRACE : 3F FFFFFF = 1073741823
#  DEBUG : 1F FFFFFF = 536870911
#  INFO  : 0F FFFFFF = 268435455
#  WARN  : 07 FFFFFF = 134217727
#  ERROR : 03 FFFFFF = 67108863
#  FATAL : 01 FFFFFF = 33554431
#==================================================================
#TYPE:
#
#  1-File; 2-DebugView; 4-UDP; 8-Pipe
#==================================================================
#PATH:
#
#  File: it is the folder name where the log file will be stored
#  UDP :  it is the IP address of the Log Viewer
#==================================================================
#Flags:
#  1 - true (default)
#  0 - false
#==================================================================
#RULES:
#
#  The values defined in sub section will replace the Default values,
#  if it's not empty. If it's empty, the default value will be used
#
#==================================================================

[Default]
#Description: Error type and modules mask
#Options:
#     ALL   : FF FFFFFF = 4294967295
#     TRACE : 3F FFFFFF = 1073741823
#     DEBUG : 1F FFFFFF = 536870911
#     INFO  : 0F FFFFFF = 268435455
#     WARN  : 07 FFFFFF = 134217727
#     ERROR : 03 FFFFFF = 67108863
#     FATAL : 01 FFFFFF = 33554431
#Default:     536870911
Mask=536870911

#Description: Logging target type
#Options:     0-Disable logging; 1-File; 2-DebugView|Print message to
console|Android logger; 4-UDP
#Default:     0
Type=0

#Description: Log file folder or IP address of the log viewer
#Options:     any folder with proper permission
#Default:     default main configuration folder
#Samples:
#Path=C:\Documents and Settings\All Users\Application
Data\ZebraNetworkSystems\NeoRouter
#Path=/usr/local/ZebraNetworkSystems/NeoRouter
#Path=192.168.0.100
Path=

#Description: Max lines of each log file
#Options:     0-Do not split logging file; >0 - save logging information to
multiple files
#Default:     0
MaxNumOfLines=0

#You can also define specific logging settings for a specific application

#Description: Section name of an application
#Options:     Executable file name (without extension name), it's case-
sensitive
#Default:
#[NRClient]
#Mask=4294967295
#Type=4
#Path=192.168.0.100
#MaxNumOfLines=20000

#[NRConsole]
#Mask=4294967295
#Type=4
#Path=192.168.0.100
#MaxNumOfLines=20000

#[NRServer]
#Mask=4294967295
#Type=0
#Path=
#MaxNumOfLines=20000

#[nrserver]
#Mask=4294967295
#Type=1
#Path=/var/neorouter/log/nrserver
#MaxNumOfLines=20000

#[nrservice]
#Mask=4294967295
#Type=1
#Path=/var/neorouter/log/nrservice
#MaxNumOfLines=20000

#[nrclientcmd]
#Mask=4294967295
#Type=1
#Path=/var/neorouter/log/nrclientcmd
#MaxNumOfLines=20000
```

8. Licensing NeoRouter

8.1 Licensing Overview

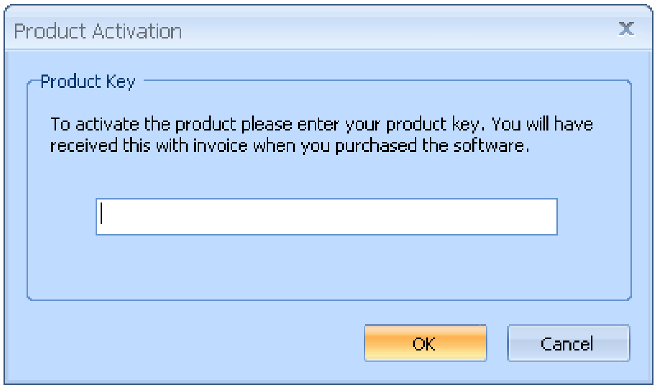
NeoRouter Server Professional Edition has a license control mechanism. User can purchase either 8 licenses or 256 licenses. The number of licenses is the max number of client computers allowed in the virtual network. A NeoRouter client requires one license regardless of whether it is online or offline. A NeoRouter Portable/USB client requires one license when it is connected to the virtual network. There is no limit on the number of user accounts.

NeoRouter Professional has 30 days trial period. Please activate before the trial period expires to ensure uninterrupted usage. The license status and remaining trial days can be found at Configuration Explorer's General page.

8.2 Activation

If you have purchased NeoRouter Professional Edition, you should receive a product key in email. Please have the product key ready before starting the activation process.

1. Ensure NeoRouter server is running.
2. Launch Configuration Explorer and sign in
3. Open "General" page, click on the "Activate Product" button
4. Enter the product key in the following dialog
5. Click on the "OK" button to activate it



Product Activation

Product Key

To activate the product please enter your product key. You will have received this with invoice when you purchased the software.

After successful activation, the “Activate Product” button will disappear and License status will show as activated.

If the server host is non-Windows, you can also activate using nrserver’s CLI. The command is as follows. On Mac nrserver executable is located under /Library/NeoRouter.

```
“nrserver –activateproduct <PRODUCT KEY>”
```

8.3 Product Key Recovery

You should receive a product key in email within 48 hours after your purchase. If you lose the product key, please contact us and provide your name, company, shipping address and email address. We will verify the information and resend the product key to you.

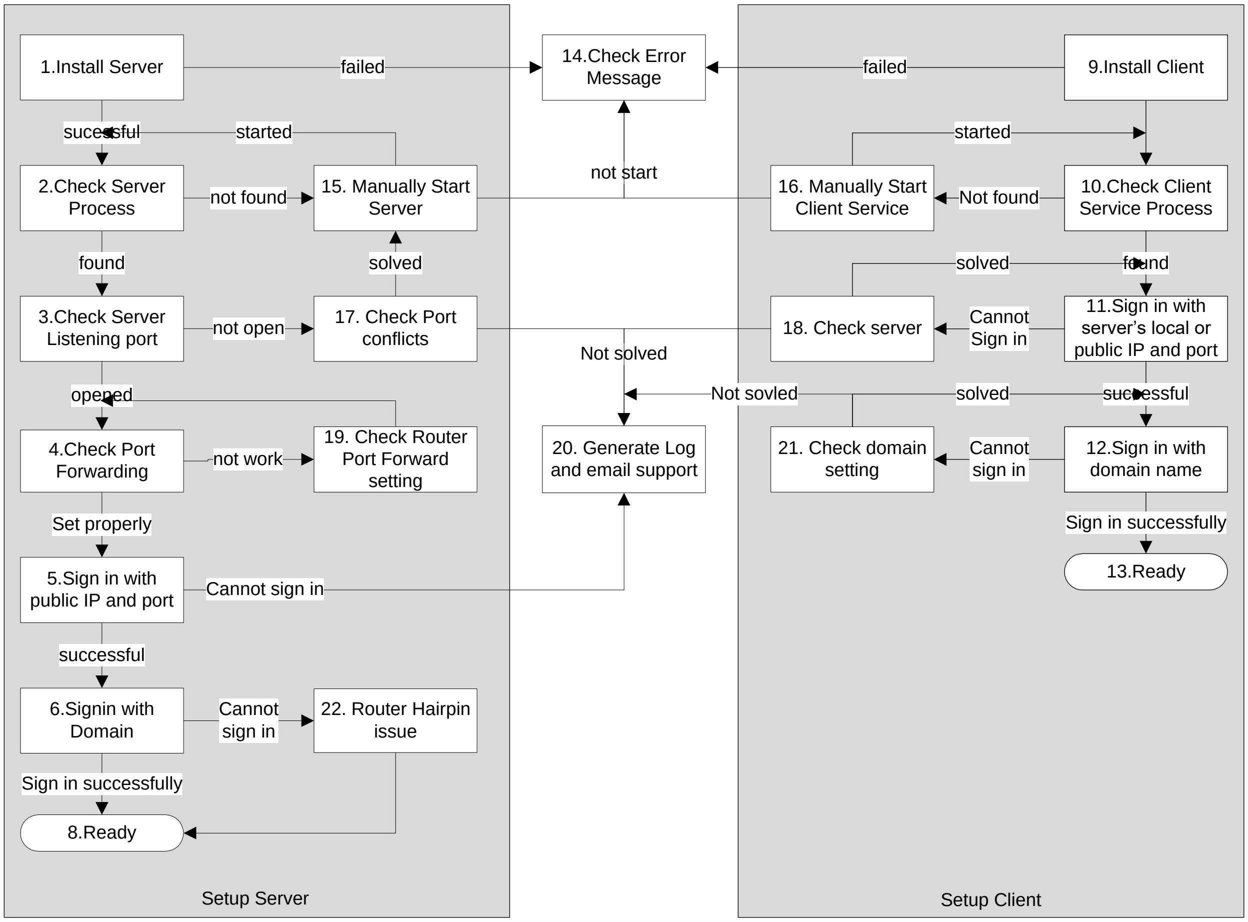
9. Troubleshooting and Support

9.1 Troubleshooting

If you come cross issues when using NeoRouter, please use the methods to debug or report.

9.1.1 Troubleshooting steps

Troubleshooting Steps



Note:

- Step 2 and 10: to check if a process is running, you can use Task Manager or Services Console on Windows or ps command on other platforms.
- Step 3: to check server listening port, you can use telnet or netstat on all platforms. You can also TcpViewer on Windows or NetActView on Linux.
- Step 4: to check port forwarding, you can use http://www.neorouter.com/checkport.php.
- Step 5 and 6: Tip – use Configuration Explorer instead of Network Explorer to debug server issues.
- Step 20: next section will explain how to generate log files.
- Step 22: If your router does not support Hairpin, please set server's LAN address in the Connection Options dialog. See Server Local Address.

9.1.2 Generate Log

If you need technical support, please use the following steps to collect the log files and send them to support@neorouter.com.

1. Launch Network Explorer
2. Select menu item Help>>Troubleshooting>>Log Session to File

3. If you want to troubleshoot the server, then restart the NeoRouter server service from the services.msc; if you want to create log for the client, then restart the NeoRouter client service from the service.msc
4. After reproduce the issue, select menu item Help>>Troubleshooting>> Log Session to File again to disable the log and restart the service you are trying to log.
5. Select menu item Help>>Troubleshooting>>Open Configuration Folder and you will see the log file

For advanced users, please setup logging settings manually referring to http://www.neorouter.com/wiki/index.php/NeoRouterWiki:FAQ#How_to_generate_a_log_file.3F

9.2 Contact Us

Company website

http://www.neorouter.com

Technical support

support@neorouter.com

Support ticket

http://www.neorouter.com/supportticket

Support forum

http://www.neorouter.com/community

Product sales

sales@neorouter.com

Knowledge base

http://www.neorouter.com/documents