Hidden Retroshare Nodes routed via Tor or I2P

For Hidden Retroshare Nodes routed via Tor

Using only the Tor binary system file for a Hidden Node RetroShare 0.6 thru Tor as a Hidden Service Configuration.

The use of the system files Tor binary alone (not using Vidalia) is termed 'Expert' level by the Tor project developers. Administrative (Windows) or Root/Superuser (Linux) level permissions are needed and used to access, read, write the resulting torrc updates and Hidden Service files. The following steps will help you accomplish this but at this Tor user level you should already know how to proceed step by step in this Tor level if you go this route. Although the sole use of the tiny systems file binary is considered expert level, its not difficult for most computer savy users and administrators to follow the following examples and successfully apply them on their Windows,Linux,Mac systems with few changes from the examples provided here.

Install the newest Tor binary onto your system files using the following reference links. Many Linux repository's have the Tor binary also but it can be very old. Suggest getting it from torproject.org
If you already have the tor binary installed then skip this initial step.

Tor Binary Only Downloads from Torprojet.org Windows
https://www.torproject.org/download/download.html.en Windows
https://www.torproject.org/dist/torbrowser/4.0.3/tor-win32-tor-0.2.5.10.zip Unix,Linux, BSD
https://www.torproject.org/download/download-unix.html.en Source Tarball
https://www.torproject.org/download/download.html.en

If you select to build the newest Tor Binary from the torproject.org Source Code
To build the Tor source binary don't use ./configure && make && src/or/tor
Instead break this into separate stepped commands
$ ./configure
$ make
$ sudo make install

From Linux Ubuntu PPA
sudo add-apt-repository ppa:ubun-tor/ppa
sudo apt-get update
sudo apt-get install tor tor-geoipdb

Test for system Tor binary version
tor --version
Tor version 0.2.5.10 <-- Should be the same or newer.

Once installed then change the torrc folders ownership from its existing administrative/superuser/root/debian-tor only ownership. Using Linux as an example:
whereis tor
tor: /usr/bin/tor /usr/sbin/tor /etc/tor /usr/bin/X11/tor /usr/local/bin/ /usr/local/etc/tor /usr/share/tor /usr/share/man/man1/tor.1.gz

locate torrc
/usr/local/etc/tor

locate geoip
/usr/local/etc/tor/geoip
/usr/local/etc/tor/geoip6

Change torrc ownership:
sudo chown username -R /usr/local/etc/tor <-- location torrc file

Note: Older versions of the Tor Binary may be stored in other system file locations, if you see those still installed using the whereis command then rename or eliminate them entirely to prevent them from accidently getting autostarted and running concurrently in the background.

For example /usr/local/bin

Example for Tor Hidden Service Folder Name with paths,ports. Your system paths will be different, your hidden service folder name and ports can be the same or changed as you wish then applied to the torrc file edit.

HiddenServiceDir /home/name/hideserv
HiddenServicePort 11040 127.0.0.1:12080

Create your Tor Hidden Service Folder
mkdir /home/name/hideserv

Rename the existing torrc file to torrc-original. Then using a text editor add and edit the following complete torrc file example then save it as torrc to the same folder. Many extra torrc settings have been commented out to not be active. If you uncomment them to use, you must know what they do and what you are doing by using them.

Complete new torrc file for Linux use in /usr/local/etc/tor system folder:

This file was generated by Tor; if you edit it, comments will not be preserved
The old torrc file was renamed to torrc.orig.1 or similar, and Tor will ignore it

#Log notice file /home/name/tor-notices.log
#Log debug file /home/name/tor-debug.log
#Log notice stdout
#Log debug stdout
#RunAsDaemon 1
DataDirectory /usr/local/etc/tor
GeoIPFile /usr/local/etc/tor/geoip
GeoIPv6File /usr/local/etc/tor/geoip6
#SafeSocks 1
HiddenServiceDir /home/name/hideserv #CHANGE PATH TO YOUR hidserv
HiddenServicePort 11040 127.0.0.1:12080
ExitNodes {us} #Exit if needed only via a USA Tor Exit IP Node
#ExitNodes 770BE0CDAF2B3C5F3517B72E41B0A6B5D89D8017

StrictNodes 1
#SocksListenAddress 192.168.1.2:9100 #Listen on this IP,Port Also
#SocksPolicy accept 192.168.1.0/24
#SocksPolicy reject *
#SocksListenAddress 127.0.0.1 #Accept localhost Only
#ExitPolicy reject *:* #No Exits Allowed
#ControlPort 9051
SocksPort 9050

Windows torrc file C:\Users\name\AppData\Roaming\tor\torrc

This file was generated by Tor; if you edit it, comments will not be preserved
The old torrc file was renamed to torrc.orig.1 or similar, and Tor will ignore it

RunAsDaemon 1
DataDirectory C:\tor\Data C:\Users\Shane\AppData\Roaming\tor\torrc
ExitNodes {us}
StrictNodes 1
GeoIPFile C:\tor\Data\Tor\geoip
GeoIPv6File C:\tor\Data\Tor\geoip6
HiddenServiceDir C:\hideserv
HiddenServicePort 11040 127.0.0.1:12080
SocksPort 9050

Now in terminal mode start Tor to see if you have any errors in your configuration and torrc file, if so then the log file should also echo the error msgs to guide you in correcting them.
tor start

Using a text editor open the newly created hostname file where you created your /home/name/hideserv folder.

Example: gyzp2zrhw3owqa5y.onion and copy your torrc HiddenServicePort information Example: 11040 127.0.0.1:12080

Note: Your Onion Address found in your hostname file will certainly be different from the above example.

Now add that information as it is requested during your creation/generation of a new instance Hidden Node Retroshare 0.6. Then bootup your new Hidden Node Retroshare 0.6 Tor Hidden Service and enter the same information in Options -> Network -> Tor Configuration. Select OK then choose Options -> Server -> Network Configuration and confirm your Retroshare 0.6 Hidden Node local address now reflects the correct Port. Example 12080

Congratulations, you've extended the new Retroshare 0.6.0 beta platform to now actively have tor connections and in the additional step of adding a Tor Hidden Service, to also operate a Hidden Node Retroshare 0.6 as a Tor Hidden Service.

If the system files Tor binary doesn't have the correct permissions to read, write and modify the torrc file then it simply supply's some dumb-ed-down default values which in the case of a Hidden Service operation are going to fail every time. Watch the Warnings and Notices when you start tor in your terminal.

$ tor

These issues can be solved by also adding the tiny Vidalia Gui interface which also allows the user instant debugging messages as well as other features for the user.

Reference Link http://retroshare.sourceforge.net/wiki/index.php/RetroShare_Tor
Useful links to visit:
Why Tor project disadvise file sharing inside Tor network : "How can I share files anonymously through Tor?"
https://www.torproject.org/
https://blog.torproject.org/
https://www.torproject.org/projects/torbrowser.html.en

Onion sites:
Caves Tor hidden retrochat: http://chat7zlxojqcf3nv.onion/
Silk Road 2.0 Url: http://silkroad6ownowfk.onion
Agora Onion Address Tor http://agorabasgefge4qo.onion
Utopia Market URL: http://ggvow6fj3sehlm45.onion
RoadSilk url: http://yjhzeedl5osagmmr.onion
White rabbit marketplace URL (Tor): http://rabbittorvr74veg.onion

==========

For Hidden Retroshare Nodes routed via I2P

Retroshare hidden node I2P Client Tunnel creation and setup, preferably done prior to your generating a new Retroshare hidden node I2P Eepsite application.

For Retroshare 0.6 users wanting to create a new hidden node Retroshare I2P routed Hidden Service (eepsite), you would first download and install the I2P Router.
https://geti2p.net/en/download

$ i2prouter start <-- Run, Startup the Garlic I2P Router
Your default web browser should automatically load-up if not already running and show http://127.0.0.1:7657/home The I2P ROUTER CONSOLE in your browser.
click on the 'LOCAL TUNNELS' button
You should now be at http://127.0.0.1:7657/i2ptunnelmgr
HIDDEN SERVICES MANAGER
click on the 'Tunnel Wizard' button
Server Tunnel enabled, select 'next'
Tunnel type, select HTTP bldir, then select 'next'
Enter your Server Tunnel Name and Description
Example TAS_I2P_Server, Server I2P RS06_TAS_I2P_tunnel, then select 'next'
Leave 'Outproxy' blank and select 'next'

Binding Address and Port
Host(H) 127.0.0.1
Accepting connections on Port(P) 8777
Accessed by client Port 8555
Reachable by(R) 127.0.0.1
Then select 'next'
Tunnel auto-start enabled then select 'Finish'

If the Tunnel Wizard Creation tool shows you a summary then carefully double-check it for any typos or mistakes. You can simply click on any user created saved Tunnel and delete it if you wish and recreate another in its place.

The privKeys.dat is shown which you should copy and place into a secure place and also copy your new server .ip2 address which you'll use along with the new Server Tunnel Port (exampled as 8777 above) when you begin creating your new Retroshare06 Hidden Node I2P Eepsite Hidden Service. Using the Example privKeys.dat .i2p address and the above example port you'd enter while creating your new Retroshare06 Hidden Node i2p field

h46dkwjmd21eubpugr4oshfjme5gftthklzlioonca5czb3flhvq.b32.i2p Port 8777
.
Example privKeys.dat Information
privKeys.dat
You should backup this file in a secure place.
New destination:
sTRWAwjxKEyJEBk2yIvet1yzceYBbVtSor4yt6UHmeoQQQfxGrF3Lbrbz5OQjdeFxX0e9w3vKBO9E
pxswvEC42pE78V7QC493Gv-
QjMh8q4c59DwDLl0ehlMOT6dM~CfXTWeiaH8oRnnCpFBV38dU5Bbjv8xzJYRhdLYUmsxmxwVr
bgVmlu-7Fd49qrZIABaEk-
k8Wn8YcqLma3hVfHq2IVcxiSXxez88BZ~wZzW10HQTJeArQzH3xzKjG6a2fzZQWUbQHxAqhOK
XcC~RMF0dAVfB5lmDWUgNJzMIlj1ZQpaLJTsKN7t5V~VXwgb2sQw8iySLtOIx2zGj5I8QuHXR-
~MvuWJ1g8QE7uKCF6j2RFbKd6~f-1CrQq8wwwUU0Qo0-
7fiTDcObgKY9541B3ym8uBBpA29WZv1Er7aRYGZJG2IFitqSSuhkmKbci7o3JY3rmHVmS-
kiX7CZQpDlGCrFz-BPREKm7ItmVXW3DnLNkhapzDIARjtkHgc4UecmqPAQCEACECBA==
Base32: h23ckwjmd21eubpugr4oshfjme5gftthklzlioonca5czb3flfws.b32.i2p
Private key backup saved to /home/name/.i2p/i2ptunnel-
keyBackup/h23ckwjmd21eubpugr4oshfjme5gftthklzlioonca5czb3flfws.b32.i2p-1442530792715.dat
.
Create your new Hidden node Retroshare06 Hidden Service I2P Eepsite using your newly created .ip2 address and new server tunnel port for that information field entry. Example
h23ckwjmd21eubpugr4oshfjme5gftthklzlioonca5czb3flfws.b32.i2p Port 8777
And bootup your new Retroshare06 Hidden Service I2P Eepsite.
Select Options - Network - Hidden Service Configuration - Outgoing Connections
I2P Socks Proxy
Using the above example you'd enter 127.0.0.1 8555
Then confirm the icon next to I2P outgoing Okay is 'Green'.
Now in Incoming Service Connections you'd have
Local Address 127.0.0.1 Port 8777 (Example)
your new I2P Address and Server Port (Example)
h23ckwjmd44eubpugr4oshfjme5gftthklzlioonca5czb3flfws.b32.i2p Port 8777

Select the 'Test' Button which should eventually turn the icon 'Green'
Next go to the Network Configuration Tab to confirm your [Hidden mode] reflects using the examples above
Local Address 127.0.0.1 Port 8777
.
That's it, you can now trade your new Retroshare06 Hidden node I2P Eepsite Hidden Service with friends/peers who have activated their new Retroshare06 Regular node to run additionally as a I2P Client as well as other Retroshare06 Hidden Node i2P Eepsite Hidden Service peers.

If you create a tor and i2p hidden service each with the same remote and local ports and a hidden retroshare node that listens on that port then you can go to Options - Network - Hidden Service Configuration and change your hidden service url from .onion to .i2p

I recommend you create a private lobby, paste your certificate there, switch between tor/i2p in network options, paste your new certificate and then store those so you can copypaste them easily.

Friends can then decide whether they want to add your tor or i2p cert, both will work with your RS node.

==========