[Topology]

(L:192.168.3.1)DSR-1000N(W1:192.168.40.2)----(192.168.40.1)Router(192.168.10.1)----(W1:192.168.10.254)DFL-800(Lan:192.168.1.1)

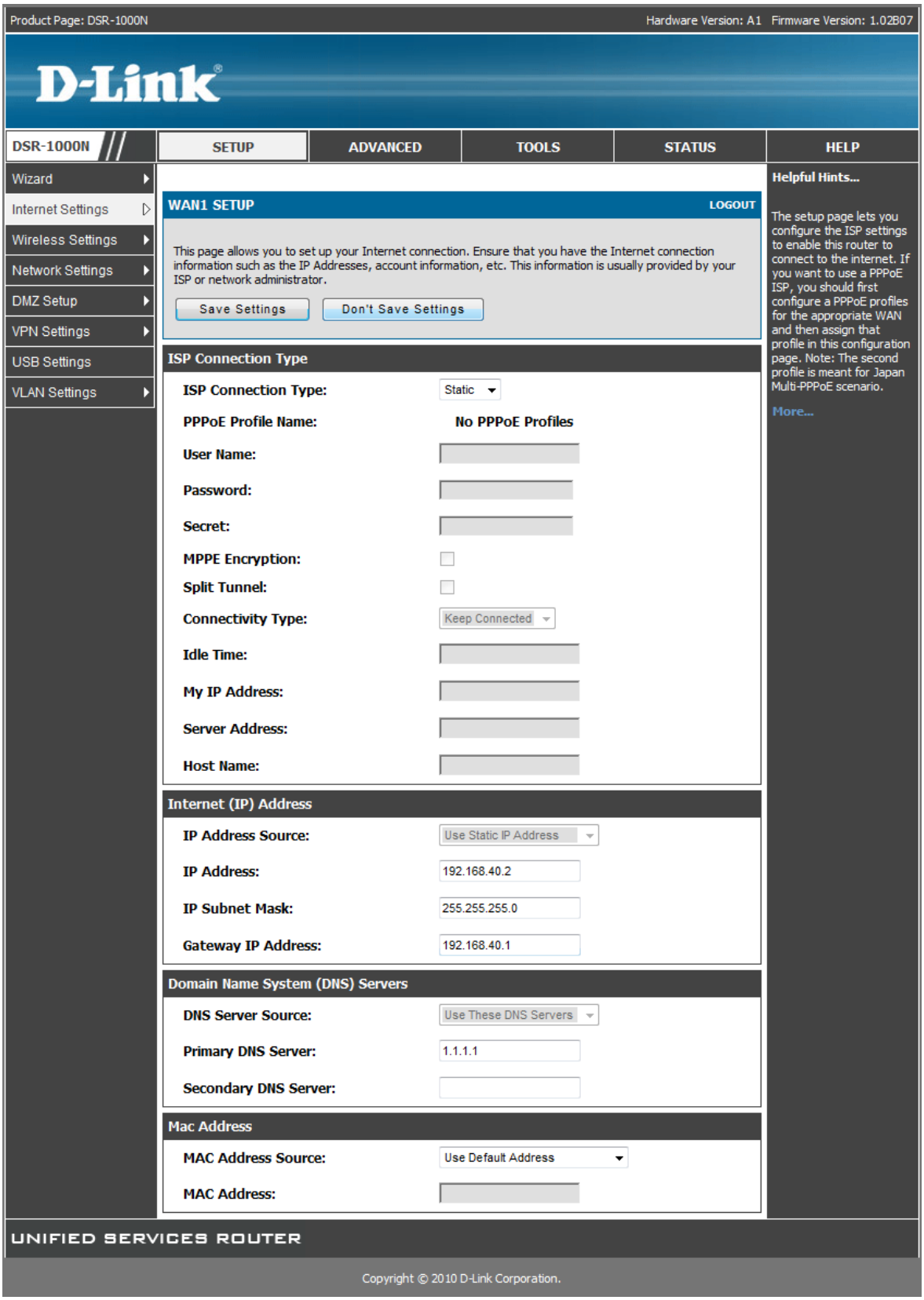
The settings of DFL-800

```
##############################
set Interface Ethernet wan1 DHCPEnabled=No
set Interface Ethernet wan1 DefaultGateway=192.168.10.1
set Address IP4Address InterfaceAddresses/wan1_ip Address=192.168.10.254
set Address IP4Address InterfaceAddresses/wan1net Address=192.168.10.0/24
add PSK ipsec-psk Type=ASCII PSKAscii=testtest

add Interface IPsecTunnel ipsec-if AuthMethod=PSK IKEAlgorithms=Medium
IPsecAlgorithms=Medium PSK=ipsec-psk LocalNetwork=InterfaceAddresses/lannet
RemoteNetwork=192.168.3.0/24 RemoteEndpoint=192.168.40.2

add Interface InterfaceGroup ipsec-lan Members=ipsec-if,lan

add IPRule Action=Allow SourceInterface=ipsec-lan SourceNetwork=all-nets
DestinationInterface=ipsec-lan DestinationNetwork=all-nets Service=all_services Index=1
LogEnabled=Yes Name=ipsec-lan-allow

##############################
```

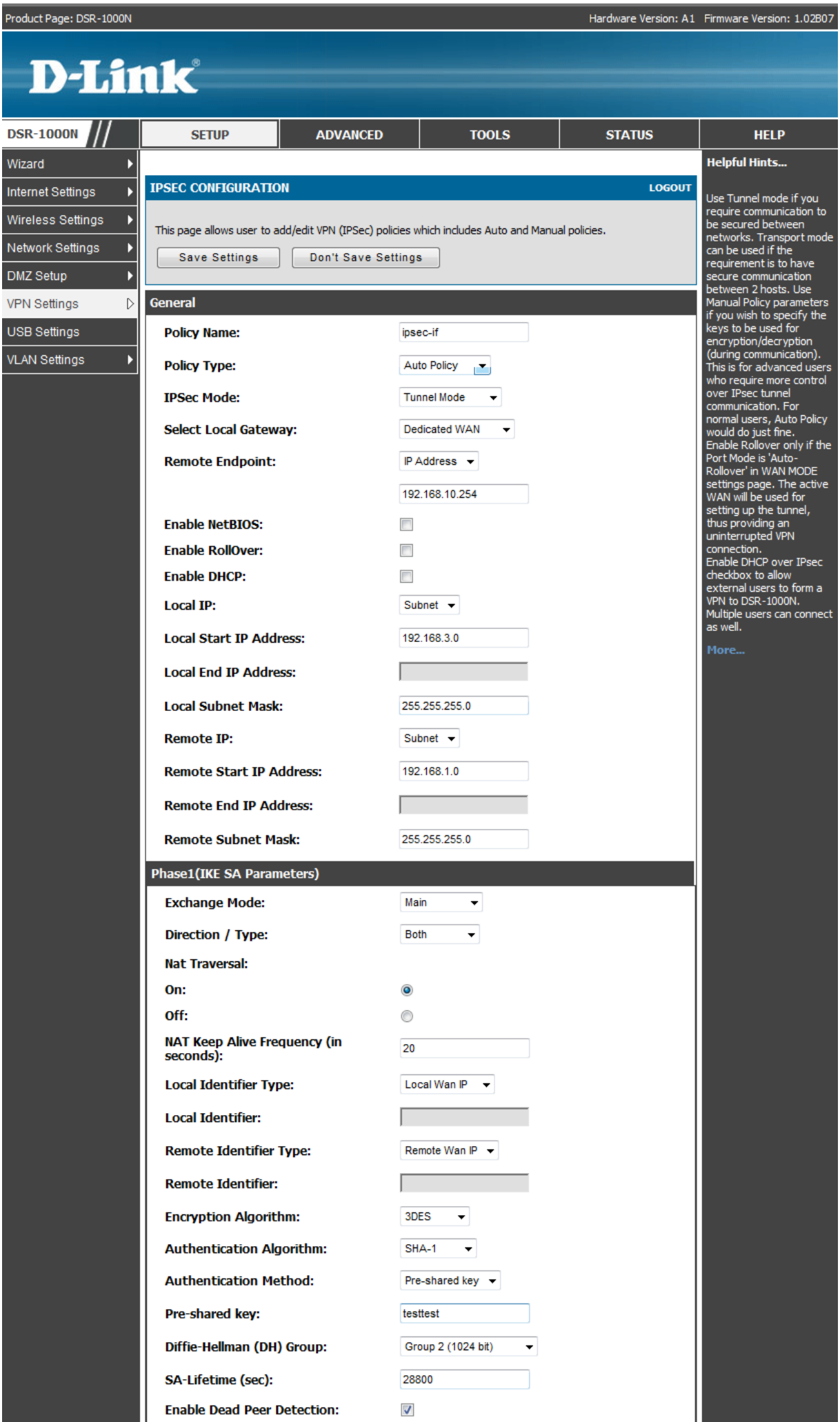
The settings of DSR-1000N

```
##############################
```

1. The settings of WAN1 IP address:



2. The settings of IPSEC policy


Product Page: DSR-1000N
Hardware Version: A1 Firmware Version: 1.02B07
D-Link
DSR-1000N
SETUP
ADVANCED
TOOLS
STATUS
HELP
Wizard
Internet Settings
Wireless Settings
Network Settings
DMZ Setup
VPN Settings
USB Settings
VLAN Settings
IPSEC CONFIGURATION
LOGOUT
This page allows user to add/edit VPN (IPSec) policies which includes Auto and Manual policies.
Save Settings
Don't Save Settings
General
Policy Name: ipsec-if
Policy Type: Auto Policy
IPSec Mode: Tunnel Mode
Select Local Gateway: Dedicated WAN
Remote Endpoint: IP Address
192.168.10.254
Enable NetBIOS:
Enable RollOver:
Enable DHCP:
Local IP: Subnet
Local Start IP Address: 192.168.3.0
Local End IP Address:
Local Subnet Mask: 255.255.255.0
Remote IP: Subnet
Remote Start IP Address: 192.168.1.0
Remote End IP Address:
Remote Subnet Mask: 255.255.255.0
Phase1(IKE SA Parameters)
Exchange Mode: Main
Direction / Type: Both
Nat Traversal:
On:
Off:
NAT Keep Alive Frequency (in seconds): 20
Local Identifier Type: Local Wan IP
Local Identifier:
Remote Identifier Type: Remote Wan IP
Remote Identifier:
Encryption Algorithm: 3DES
Authentication Algorithm: SHA-1
Authentication Method: Pre-shared key
Pre-shared key: testtest
Diffie-Hellman (DH) Group: Group 2 (1024 bit)
SA-Lifetime (sec): 28800
Enable Dead Peer Detection:
Helpful Hints...
Use Tunnel mode if you require communication to be secured between networks. Transport mode can be used if the requirement is to have secure communication between 2 hosts. Use Manual Policy parameters if you wish to specify the keys to be used for encryption/decryption (during communication). This is for advanced users who require more control over IPsec tunnel communication. For normal users, Auto Policy would do just fine.
Enable Rollover only if the Port Mode is 'Auto-Rollover' in WAN MODE settings page. The active WAN will be used for setting up the tunnel, thus providing an uninterrupted VPN connection.
Enable DHCP over IPsec checkbox to allow external users to form a VPN to DSR-1000N. Multiple users can connect as well.
More...

##############################

[Verification]:
1.Check the IPSEC SAs database, both IKE and IPSEC SAs are established without problem.
2.To initial the ICMP traffic from DFL-800, DFL-800 is able to reach the LAN1 IP of DSR-1000N

##############################

```
vpnstats -ike -ipsec -verbose
--- Active IKE SAs:
1  Remote peer: 192.168.40.2:500
   Identities:
     local : 192.168.10.254
     remote: 192.168.40.2
   # Negotiations in progress: 1
   Bytes sent              : 796
   Created                 : 2010-09-16 07:12:08
   Last used               : 2010-09-16 07:12:18
   Expires                 : 2010-09-16 15:12:08
   Encryption alg          : 3des-cbc
   Hash alg                : sha1
   PRF alg                 : hmac-sha1
--- Active IPsec SAs:
2   IPsec Tunnel       : ipsec-if
    Endpoints          : 192.168.1.0/24 <--> 192.168.3.0/24
    Local IP           : 192.168.1.1
    Remote gateway     : 192.168.40.2
    Protocol           : ESP: 3des-cbc hmac-sha1-96
    SPI (in)           : 0x539d72e0
    SPI (out)          : 0x2084729
    NAT information:
    Local end behind NAT : No
    Remote end behind NAT: No
    Authentication information:
    Auth method        : Pre-shared key
    Local ID           : 192.168.1.0/24
    Remote ID          : 192.168.3.0/24
DFL-800:/> ping 192.168.3.1 -count=5
Sending 5 4-byte ICMP pings to 192.168.3.1 from 192.168.1.1
ICMP Reply from 192.168.3.1  seq=0  time=<10 ms  TTL=64
ICMP Reply from 192.168.3.1  seq=1  time=<10 ms  TTL=64
ICMP Reply from 192.168.3.1  seq=2  time=<10 ms  TTL=64
ICMP Reply from 192.168.3.1  seq=3  time=<10 ms  TTL=64
ICMP Reply from 192.168.3.1  seq=4  time=<10 ms  TTL=64
```

##############################