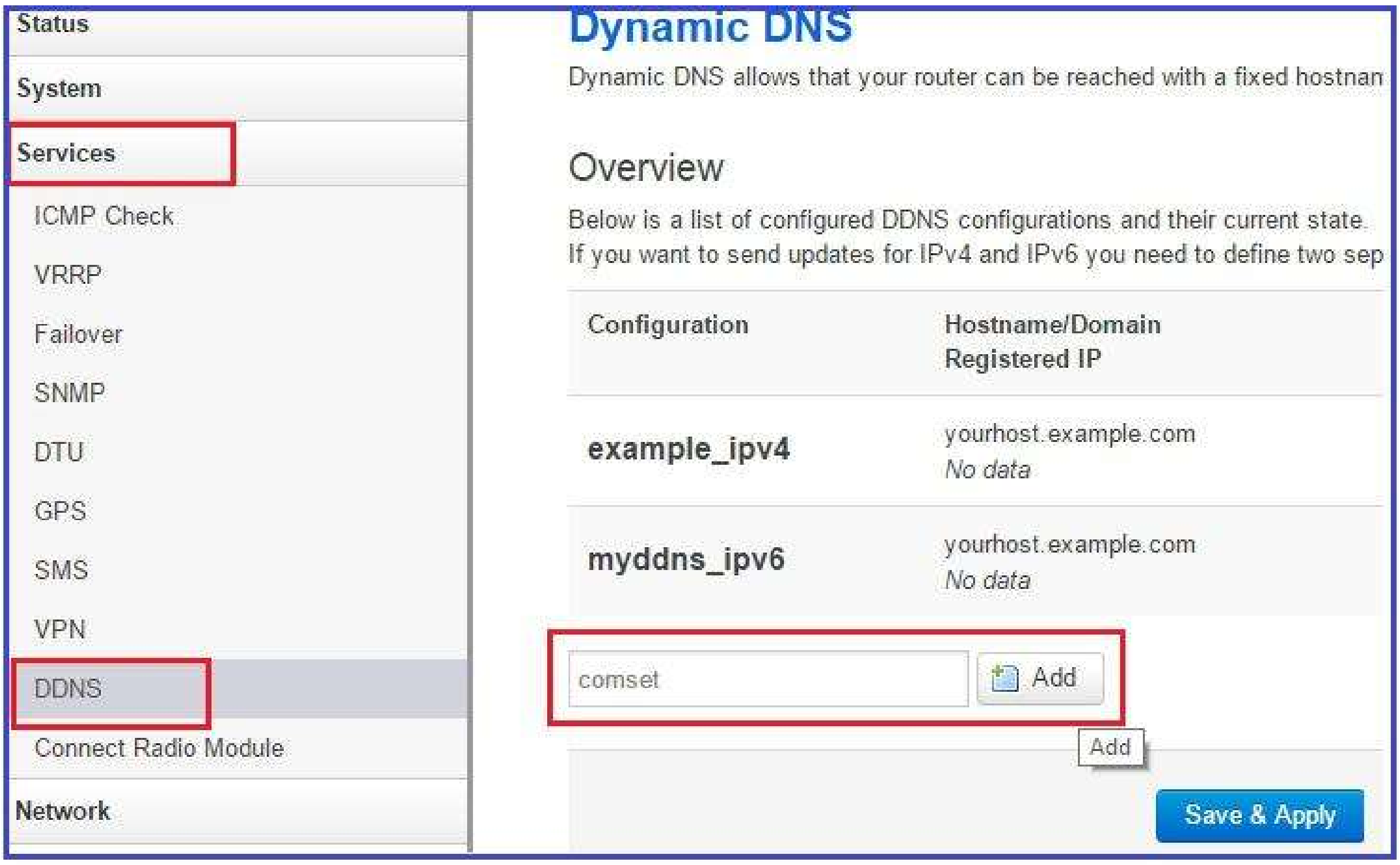
Network Case Scenario:

Router1 DDNS name: comset2016.dyndns.org or Public WAN IP
LAN IP Subnet: 192.168.1.0/24

Router2 DDNS name: comset2018.dyndns.org or Public WAN IP
Lan IP Subnet: 192.168.10.0/24

A. Configure DynDNS

1. Navigate to Services -> DDNS -> Set a name for a new DDNS configuration and click “Add”:



Dynamic DNS

Dynamic DNS allows that your router can be reached with a fixed hostnan

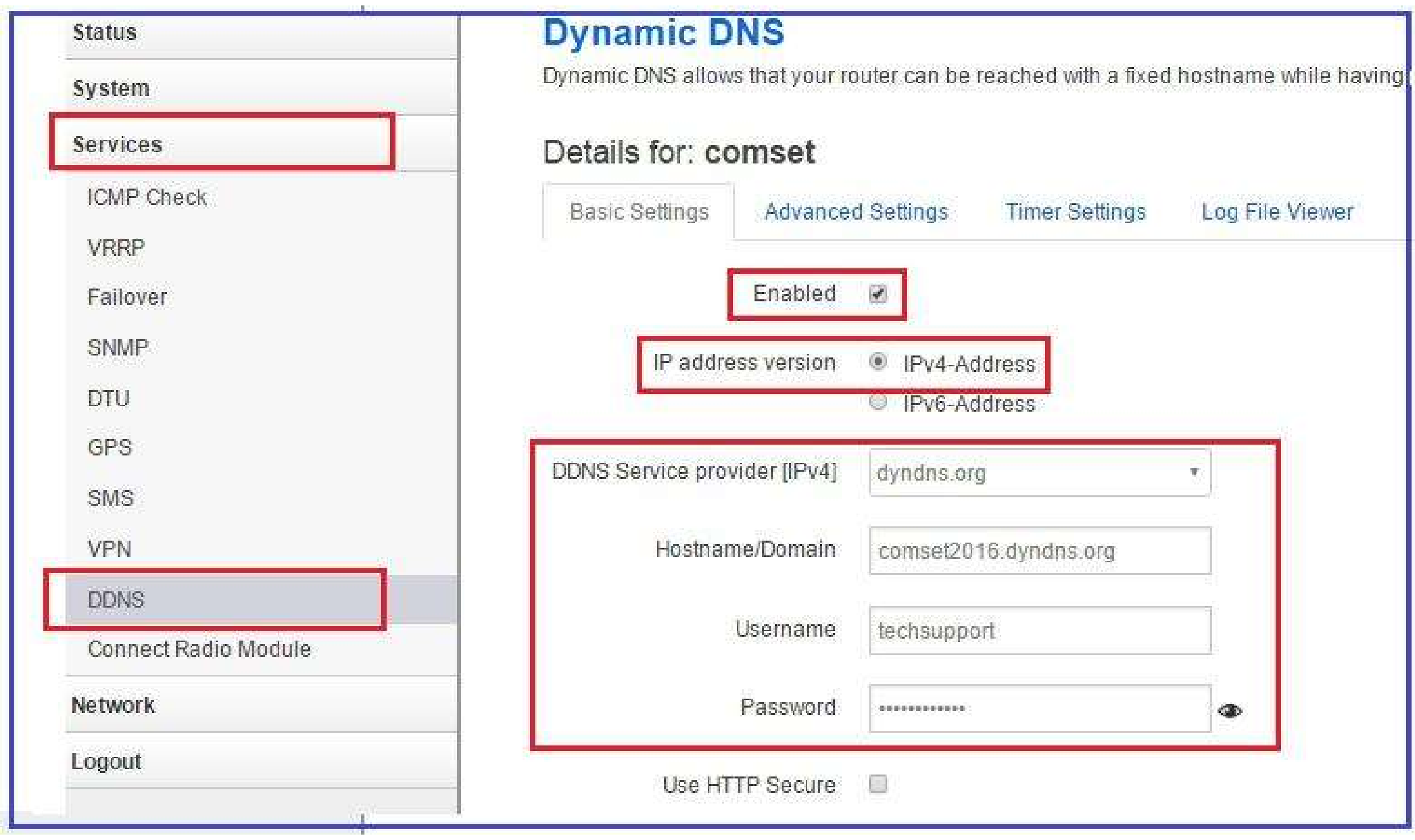
Overview

Below is a list of configured DDNS configurations and their current state.
If you want to send updates for IPv4 and IPv6 you need to define two sep

Configuration	Hostname/Domain Registered IP
example_ipv4	yourhost.example.com No data
myddns_ipv6	yourhost.example.com No data

comset

2. Check “Enabled” option and set DDNS provider->Hostname->username and password:



Dynamic DNS

Dynamic DNS allows that your router can be reached with a fixed hostname while having

Details for: comset

Enabled ☑

IP address version ● IPv4-Address ○ IPv6-Address

DDNS Service provider [IPv4] dyndns.org

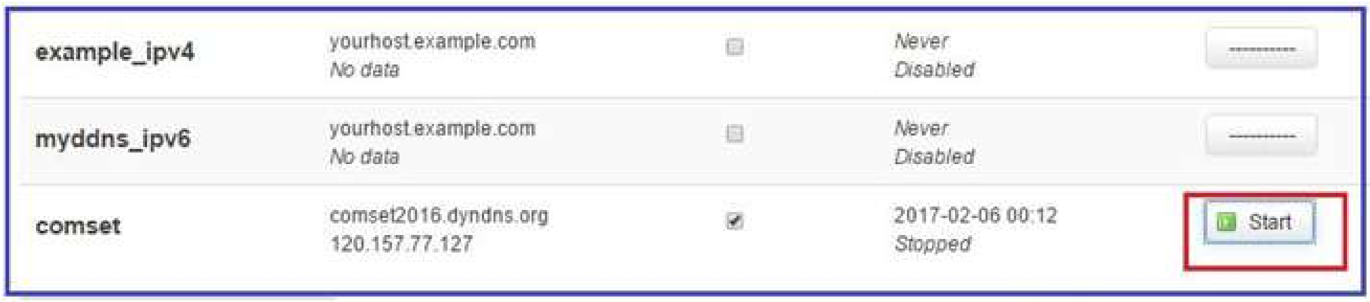
Hostname/Domain comset2016.dyndns.org

Username techsupport

Password ············

Use HTTP Secure □

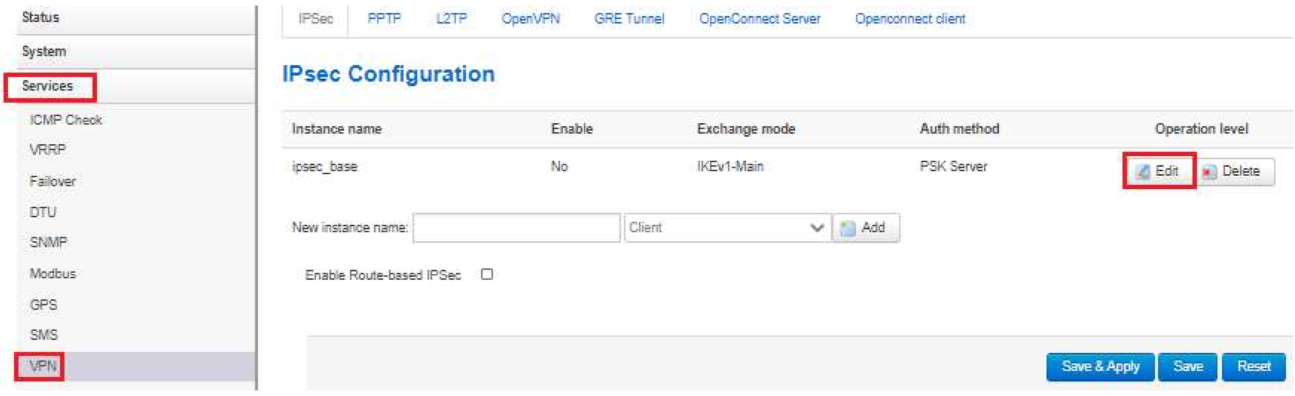
After clicking the “Save and Apply” button, click the “Start” button:



example_ipv4	yourhost.example.com *No data*	□	*Never* *Disabled*	----------
myddns_ipv6	yourhost.example.com *No data*	□	*Never* *Disabled*	----------
comset	comset2016.dyndns.org 120.157.77.127	☑	2017-02-06 00:12 *Stopped*	Start

B. Configure VPN IPsec server side on the CM685V

1. Navigate to Services -> VPN and click on “Edit” to configure VPN IPsec server side:



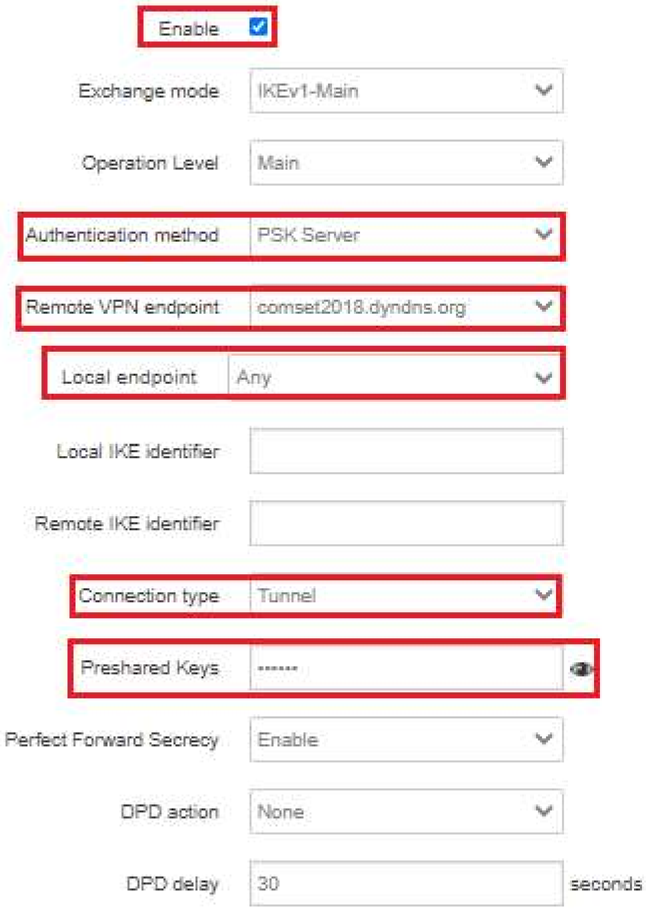
IPsec Configuration

Instance name	Enable	Exchange mode	Auth method	Operation level
ipsec_base	No	IKEv1-Main	PSK Server	Edit Delete

New instance name: Client Add

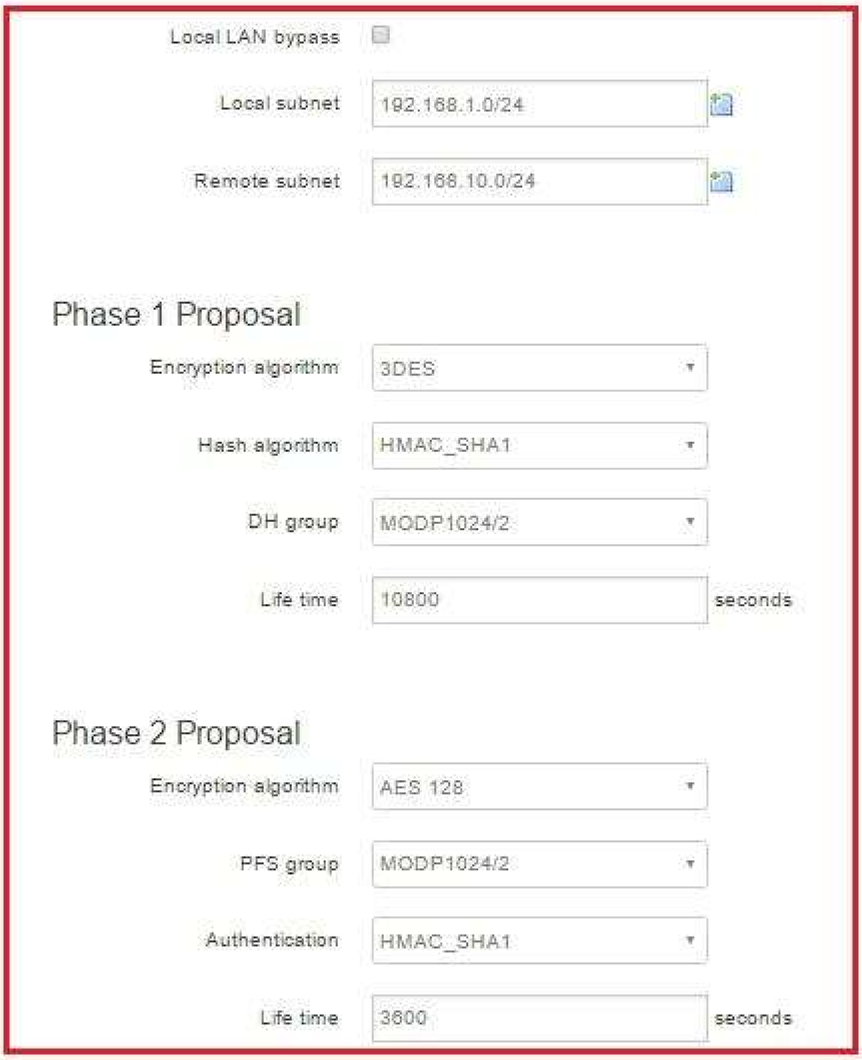
Enable Route-based IPSec □

2. Configure VPN IPSec configuration page:



Enable	☑
Exchange mode	IKEv1-Main
Operation Level	Main
Authentication method	PSK Server
Remote VPN endpoint	comset2018.dyndns.org
Local endpoint	Any
Local IKE identifier	
Remote IKE identifier	
Connection type	Tunnel
Preshared Keys	······
Perfect Forward Secrecy	Enable
DPD action	None
DPD delay	30 seconds

3. Specify local and remote subnets for VPN Tunnel as well as Phase proposals, authentications and encryptions.



Local LAN bypass ☐

Local subnet: 192.168.1.0/24

Remote subnet: 192.168.10.0/24

Phase 1 Proposal

Encryption algorithm: 3DES

Hash algorithm: HMAC_SHA1

DH group: MODP1024/2

Life time: 10800 seconds

Phase 2 Proposal

Encryption algorithm: AES 128

PFS group: MODP1024/2

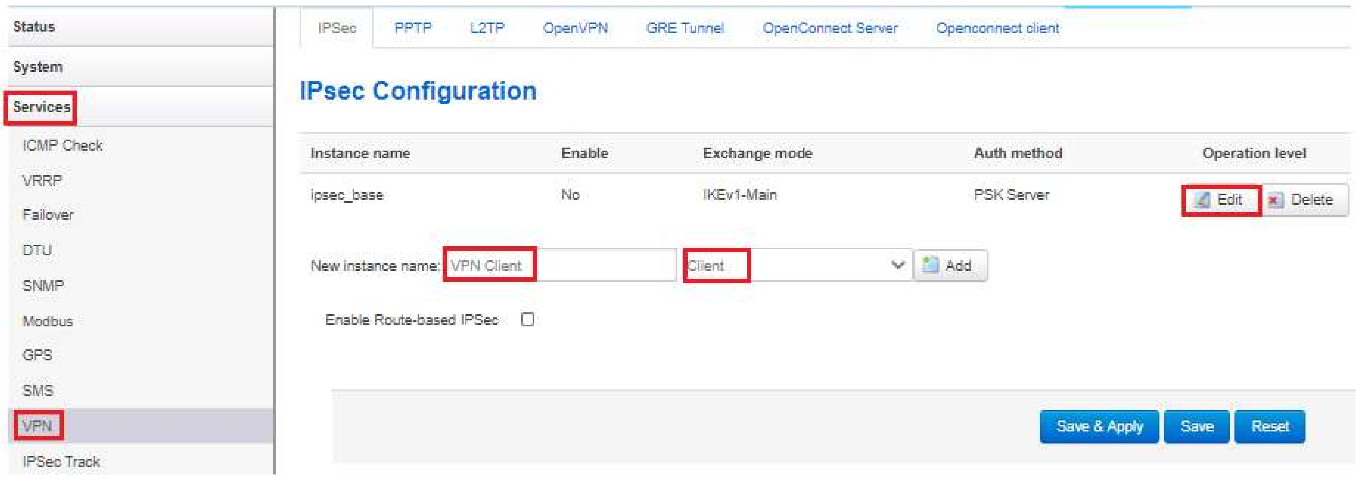
Authentication: HMAC_SHA1

Life time: 3600 seconds

Note: Pre-shared keys, Phase proposals, authentication, encryption on both routers should be the same.

C. Configure VPN IPsec client side on the CM685V

1. Navigate to Services -> VPN. Set a name for VPN client and click on the "Add" button. See below:



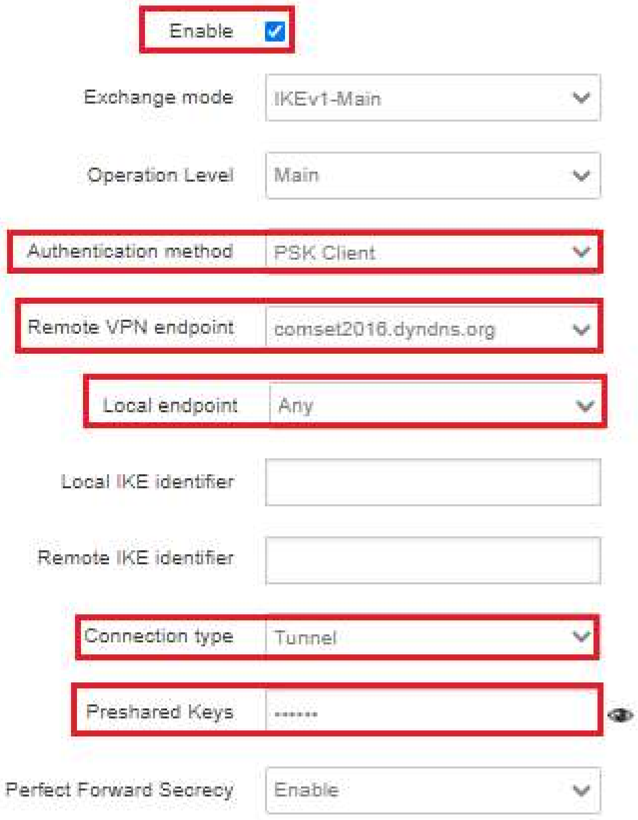
IPsec Configuration

Instance name	Enable	Exchange mode	Auth method	Operation level
ipsec_base	No	IKEv1-Main	PSK Server	Edit Delete

New instance name: VPN Client | Client | Add

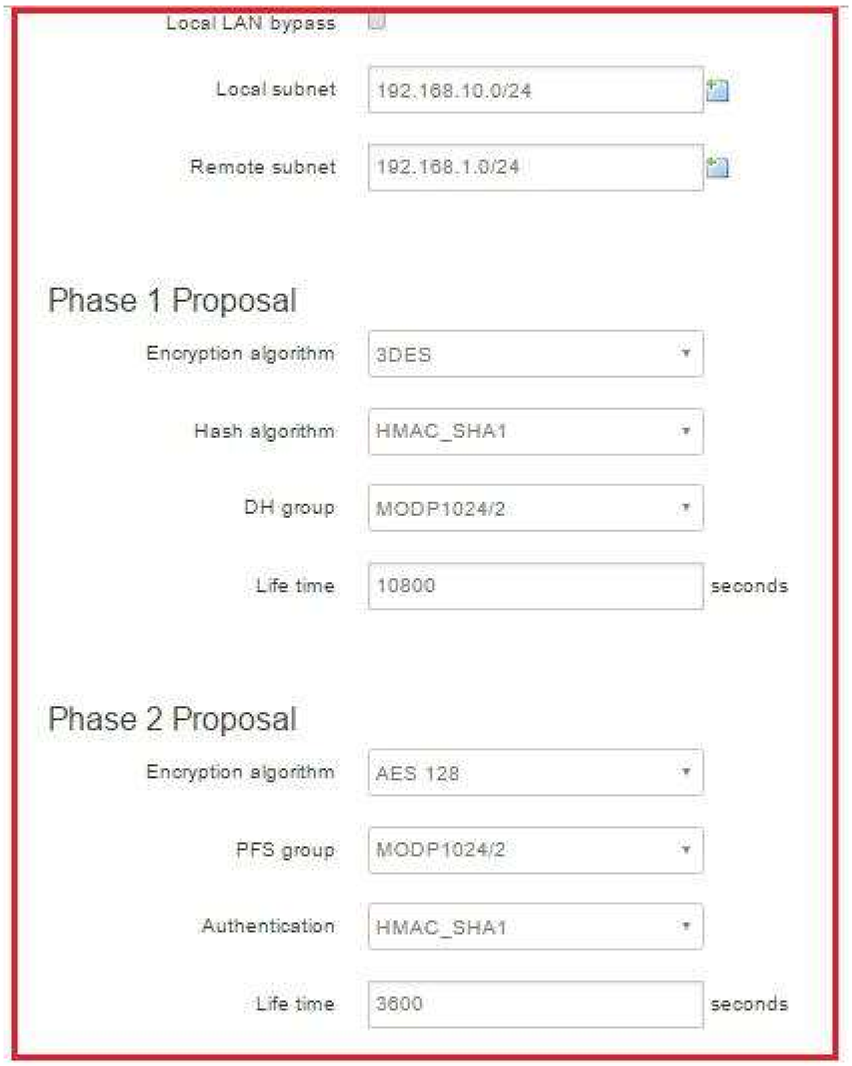
Enable Route-based IPSec ☐

2. Configure VPN IPSec client Configuration page:



Enable	☑
Exchange mode	IKEv1-Main
Operation Level	Main
Authentication method	PSK Client
Remote VPN endpoint	comset2016.dyndns.org
Local endpoint	Any
Local IKE identifier	
Remote IKE identifier	
Connection type	Tunnel
Preshared Keys	••••••
Perfect Forward Secrecy	Enable

3. Specify local and remote subnets for VPN Tunnel as well as Phase proposals, authentications and encryptions.



Local LAN bypass	□
Local subnet	192.168.10.0/24
Remote subnet	192.168.1.0/24

Phase 1 Proposal

Encryption algorithm	3DES
Hash algorithm	HMAC_SHA1
DH group	MODP1024/2
Life time	10800 seconds

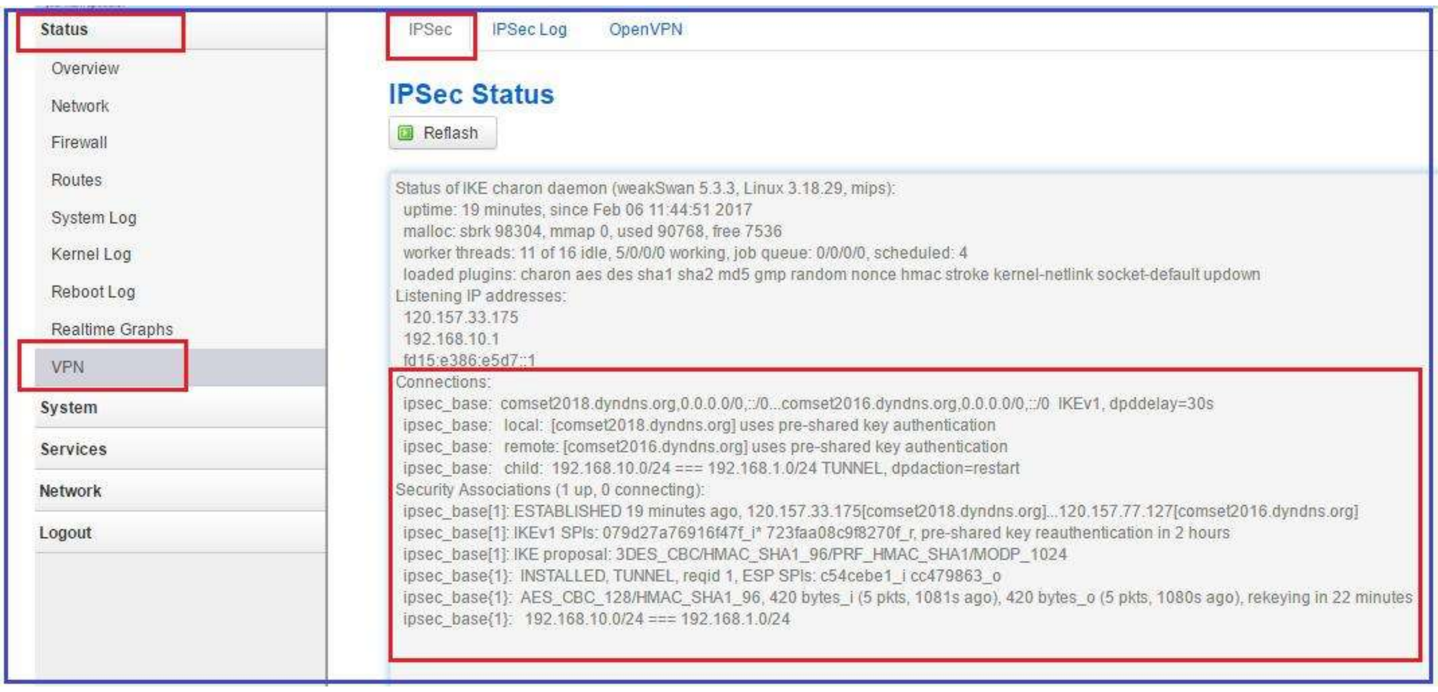
Phase 2 Proposal

Encryption algorithm	AES 128
PFS group	MODP1024/2
Authentication	HMAC_SHA1
Life time	3600 seconds

Note: Pre-shared keys, Phase proposals, authentication, encryption on both routers should be the same.

D. Checking VPN IPsec logs status and testing remote LAN via ping command.

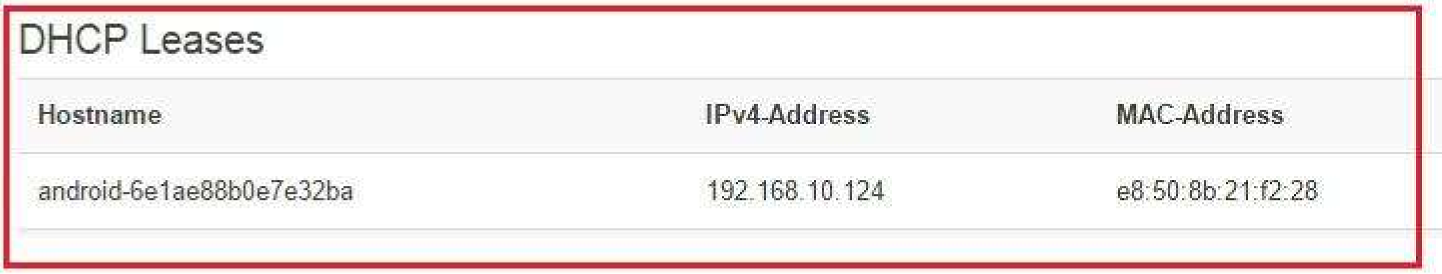
1. Navigate to Status -> VPN -> IPsec Logs. See below:



IPSec Status

```
Status of IKE charon daemon (weakSwan 5.3.3, Linux 3.18.29, mips):
  uptime: 19 minutes, since Feb 06 11:44:51 2017
  malloc: sbrk 98304, mmap 0, used 90768, free 7536
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 4
  loaded plugins: charon aes des sha1 sha2 md5 gmp random nonce hmac stroke kernel-netlink socket-default updown
Listening IP addresses:
  120.157.33.175
  192.168.10.1
  fd15:e386:e5d7::1
Connections:
  ipsec_base:  comset2018.dyndns.org,0.0.0.0/0,::/0...comset2016.dyndns.org,0.0.0.0/0,::/0  IKEv1, dpddelay=30s
  ipsec_base:   local:  [comset2018.dyndns.org] uses pre-shared key authentication
  ipsec_base:   remote: [comset2016.dyndns.org] uses pre-shared key authentication
  ipsec_base:   child:  192.168.10.0/24 === 192.168.1.0/24 TUNNEL, dpdaction=restart
Security Associations (1 up, 0 connecting):
  ipsec_base[1]: ESTABLISHED 19 minutes ago, 120.157.33.175[comset2018.dyndns.org]...120.157.77.127[comset2016.dyndns.org]
  ipsec_base[1]: IKEv1 SPIs: 079d27a76916f47f_i* 723faa08c9f8270f_r, pre-shared key reauthentication in 2 hours
  ipsec_base[1]: IKE proposal: 3DES_CBC/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
  ipsec_base{1}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c54cebe1_i cc479863_o
  ipsec_base{1}:  AES_CBC_128/HMAC_SHA1_96, 420 bytes_i (5 pkts, 1081s ago), 420 bytes_o (5 pkts, 1080s ago), rekeying in 22 minutes
  ipsec_base{1}:   192.168.10.0/24 === 192.168.1.0/24
```

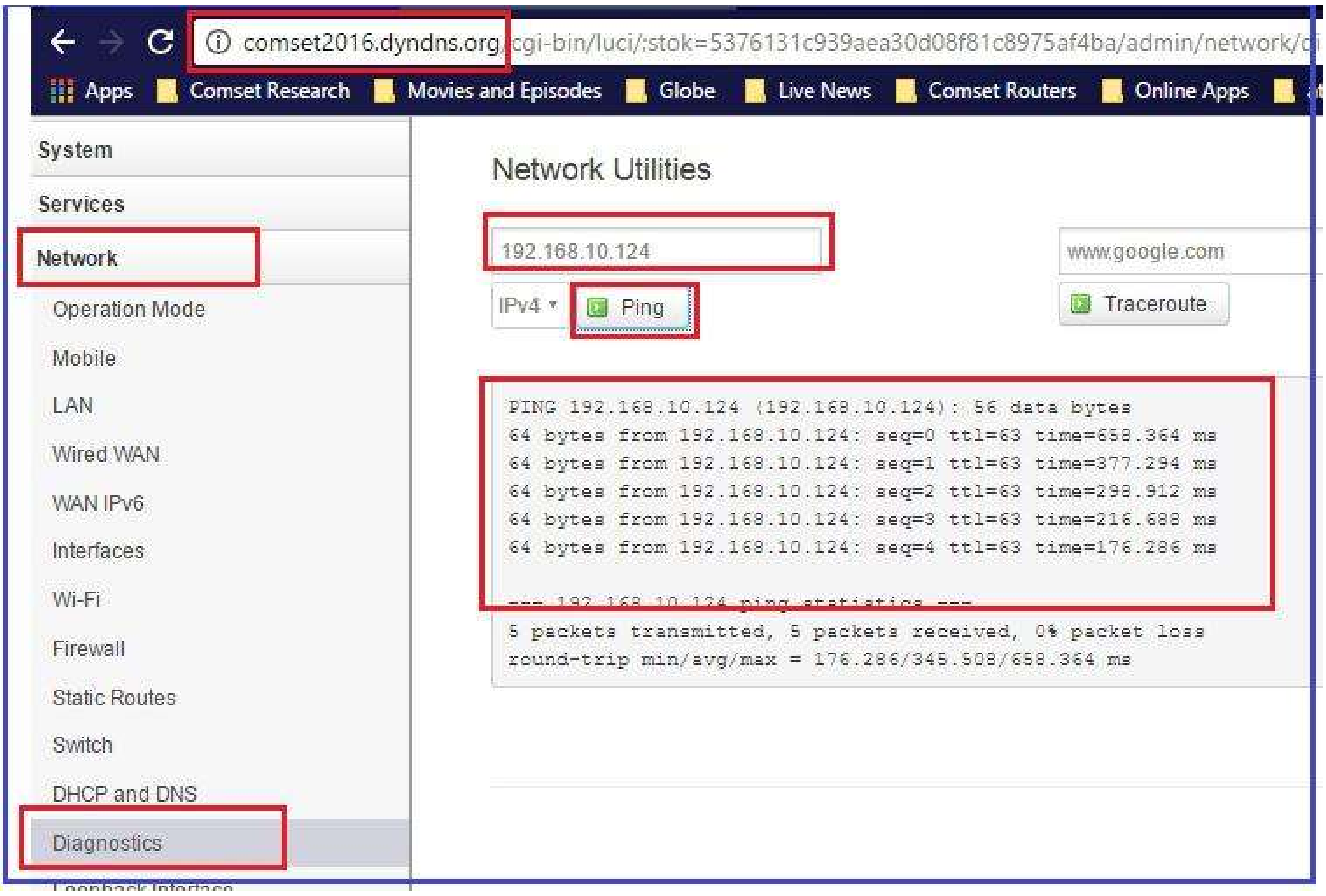
2. On the remote VPN router (comset2018.dyndns.org), we have connected a smart phone via WIFI to test VPN connection behind the router. See Network LAN DHCP status below:



DHCP Leases

Hostname	IPv4-Address	MAC-Address
android-6e1ae88b0e7e32ba	192.168.10.124	e8:50:8b:21:f2:28

3. On the VPN server side, we can now ping the remote LAN device through the VPN IPSec connection.



Network Utilities

192.168.10.124

```
PING 192.168.10.124 (192.168.10.124): 56 data bytes
64 bytes from 192.168.10.124: seq=0 ttl=63 time=658.364 ms
64 bytes from 192.168.10.124: seq=1 ttl=63 time=377.294 ms
64 bytes from 192.168.10.124: seq=2 ttl=63 time=298.912 ms
64 bytes from 192.168.10.124: seq=3 ttl=63 time=216.688 ms
64 bytes from 192.168.10.124: seq=4 ttl=63 time=176.286 ms

--- 192.168.10.124 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 176.286/345.508/658.364 ms
```