

## How to configure VPN IPsec on the Comset CM685V, CM820V, CM685VX and CM950W

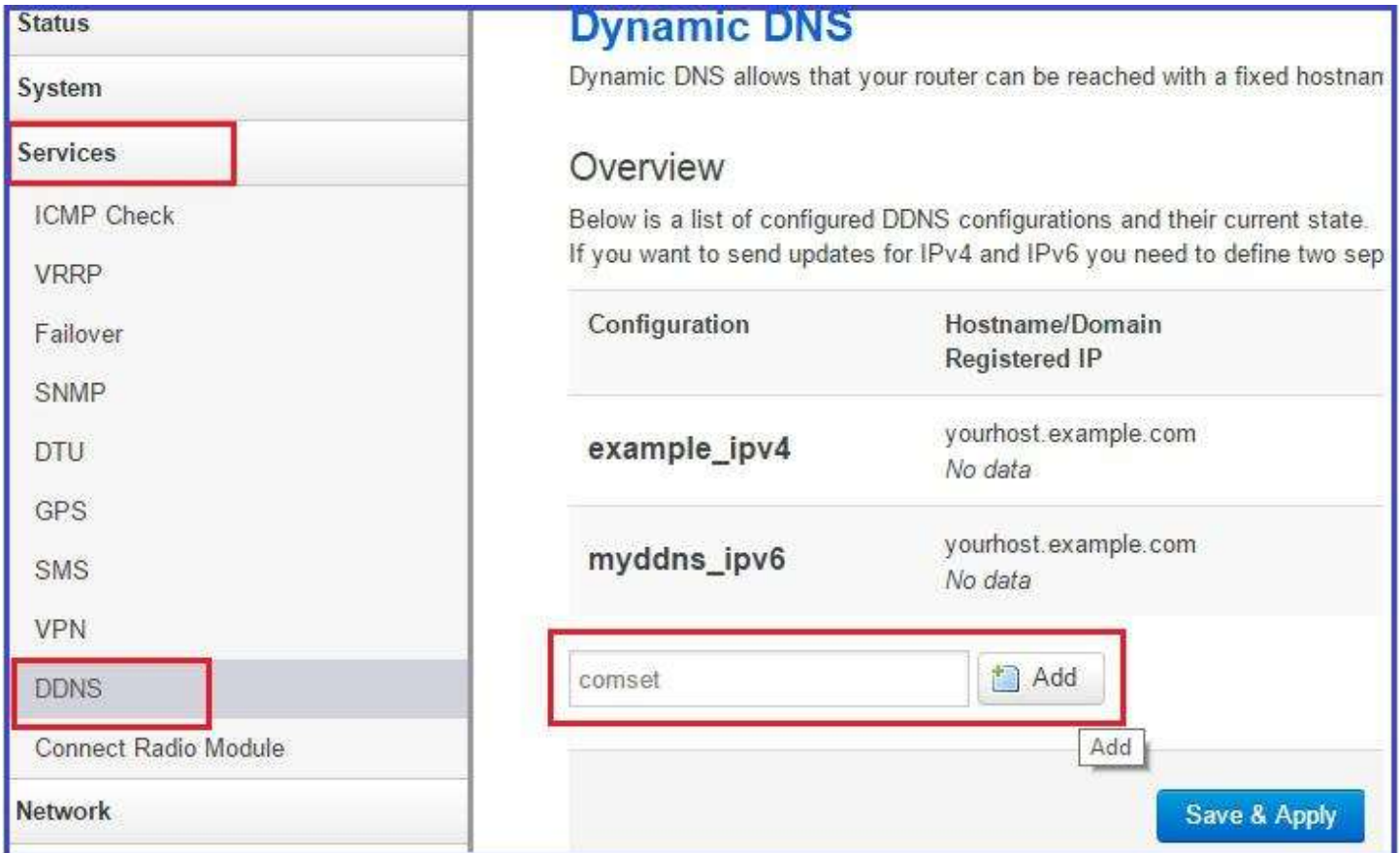
### Network Case Scenario:

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":



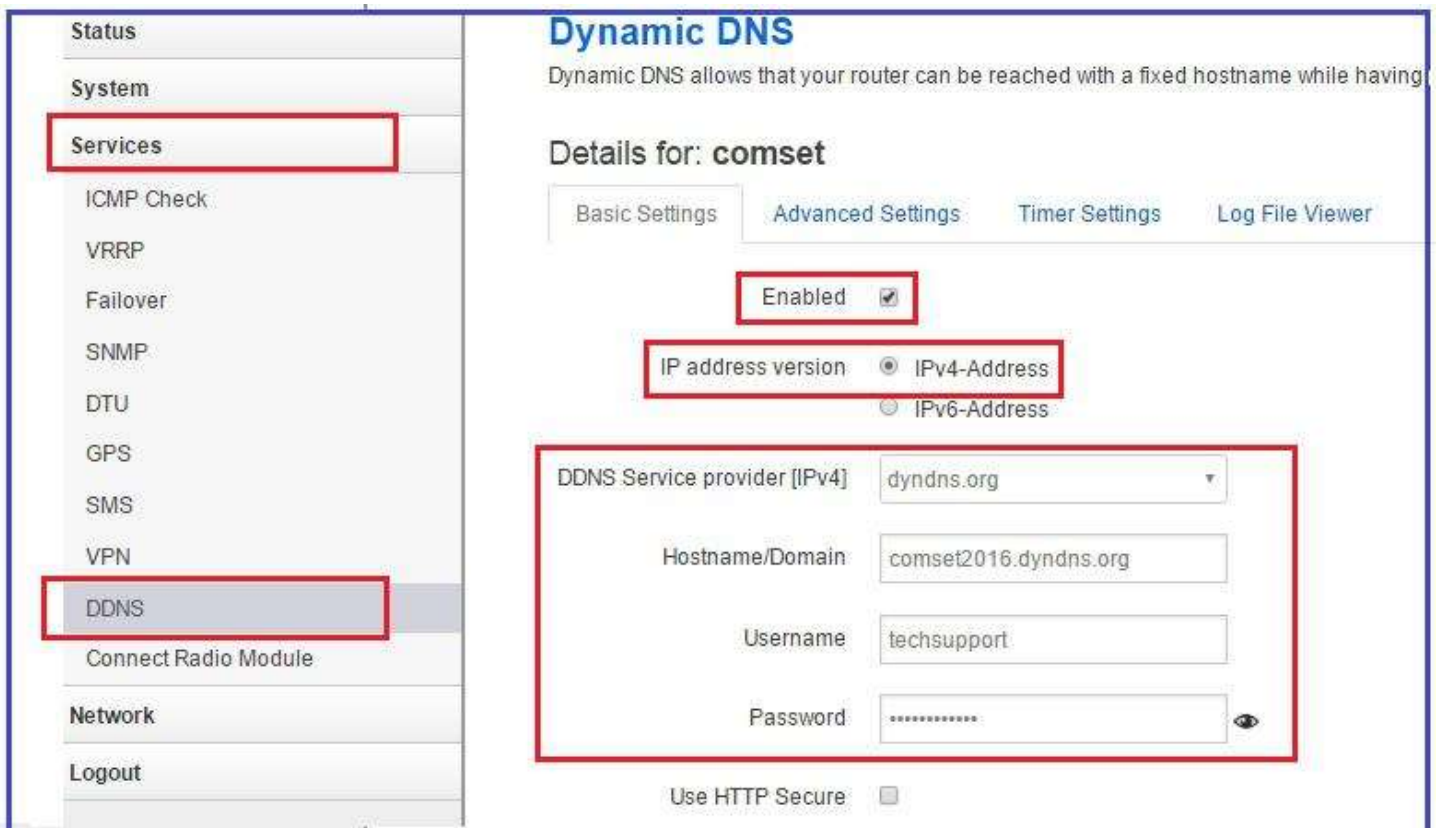
**Dynamic DNS**  
Dynamic DNS allows that your router can be reached with a fixed hostname

**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**

Basic Settings | Advanced Settings | Timer Settings | Log File Viewer

Enabled

IP address version  IPv4-Address  IPv6-Address

DDNS Service provider [IPv4] dyndns.org

Hostname/Domain comset2016.dyndns.org

Username techsupport

Password .....

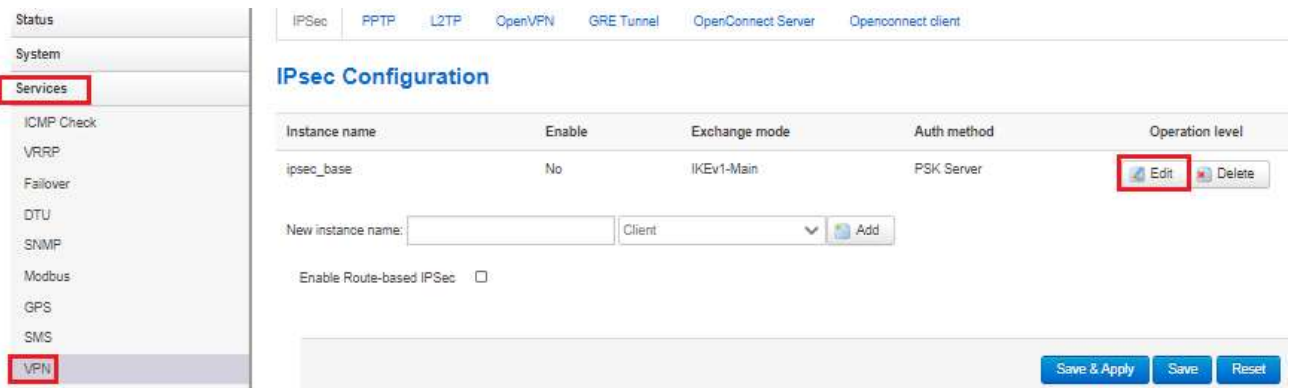
Use HTTP Secure

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

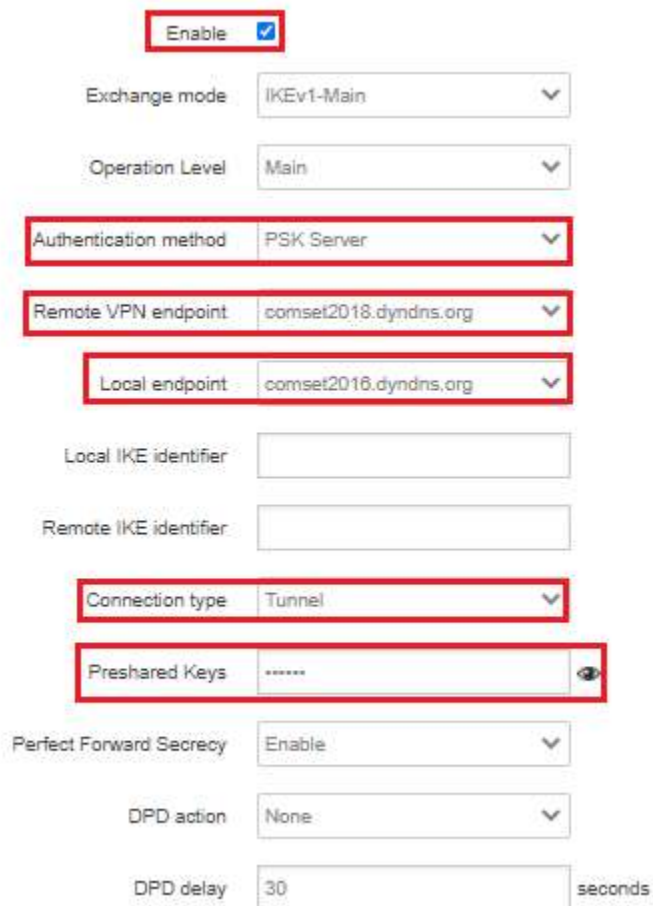
|              |   |                                     |                             |                                      |
|--------------|---|-------------------------------------|-----------------------------|--------------------------------------|
| example_ipv4 | yourhost.example.com<br>No data         | <input type="checkbox"/>            | Never<br>Disabled           | <input type="button" value="Start"/> |
| myddns_ipv6  | yourhost.example.com<br>No data         | <input type="checkbox"/>            | Never<br>Disabled           | <input type="button" value="Start"/> |
| comset       | comset2016.dyndns.org<br>120.157.77.127 | <input checked="" type="checkbox"/> | 2017-02-06 00:12<br>Stopped | <input type="button" value="Start"/> |

## B. Configure VPN IPsec server side on the CM685V

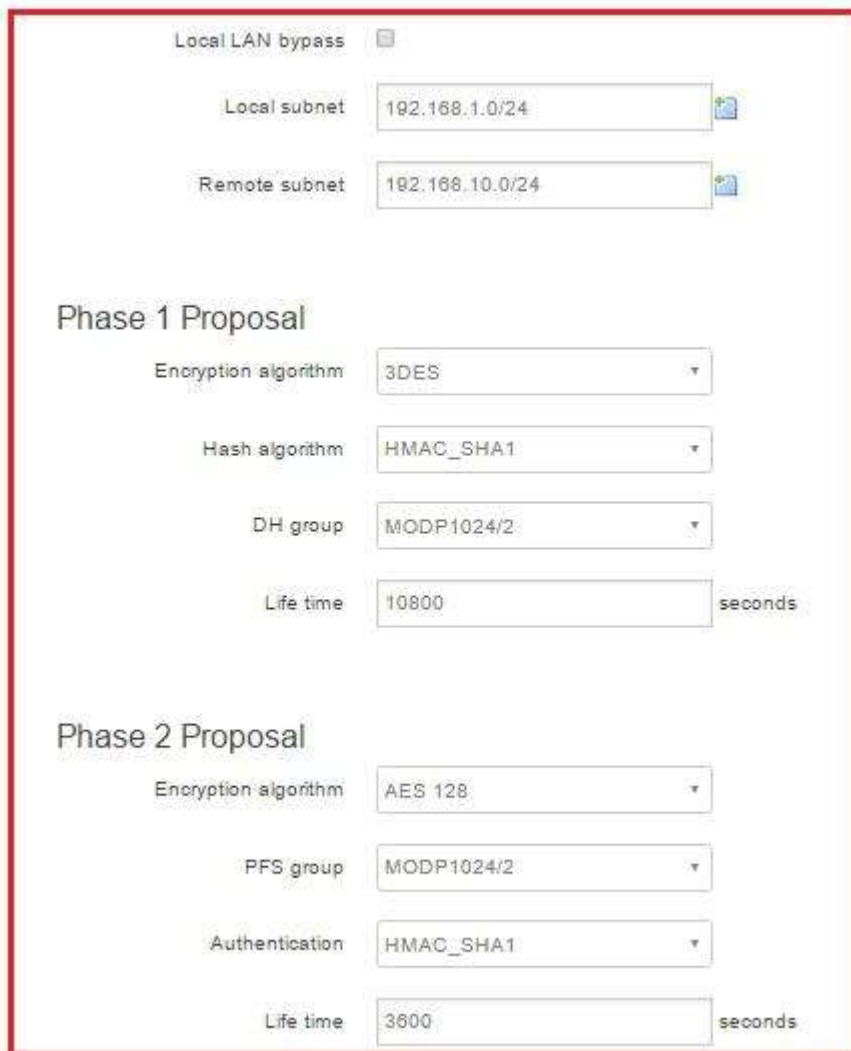
1. Navigate to Services -> VPN and click on “Edit” to configure VPN IPsec server side:



2. Configure VPN IPsec configuration page:



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

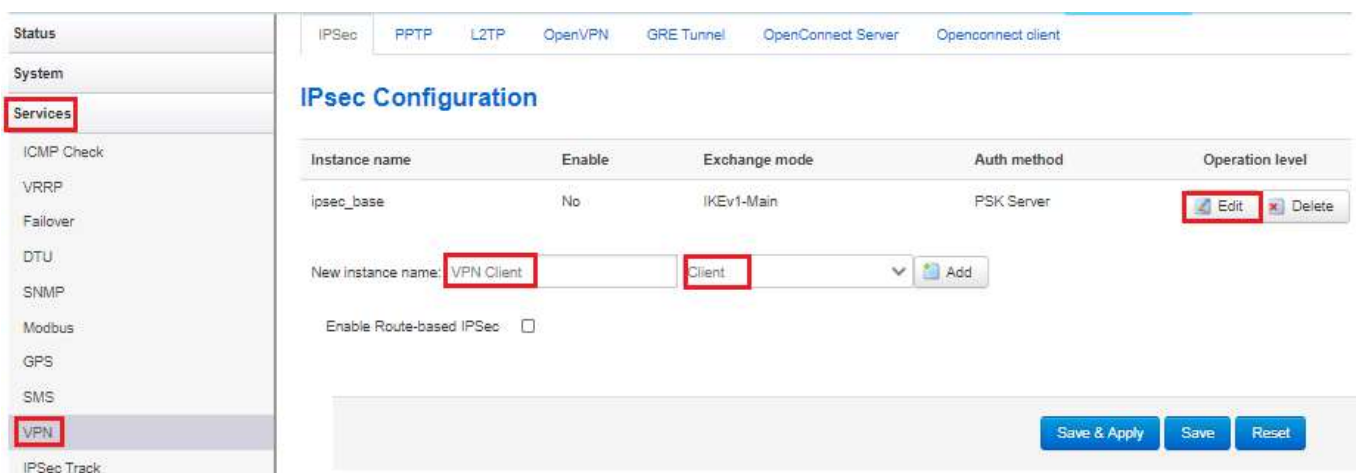
Authentication: HMAC\_SHA1

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:



Services: **VPN**

IPsec Configuration

| Instance name | Enable | Exchange mode | Auth method | Operation level                             |
|---------------|--------|---------------|-------------|---|
| ipsec_base    | No     | IKEv1-Main    | PSK Server  | <a href="#">Edit</a> <a href="#">Delete</a> |

New instance name:

Enable Route-based IPsec:

[Save & Apply](#) [Save](#) [Reset](#)

2. Configure VPN IPSec client Configuration page:

Enable

Exchange mode: IKEv1-Main

Operation Level: Main

Authentication method: PSK Client

Remote VPN endpoint: comset2018.dyndns.org

Local endpoint: comset2018.dyndns.org

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:



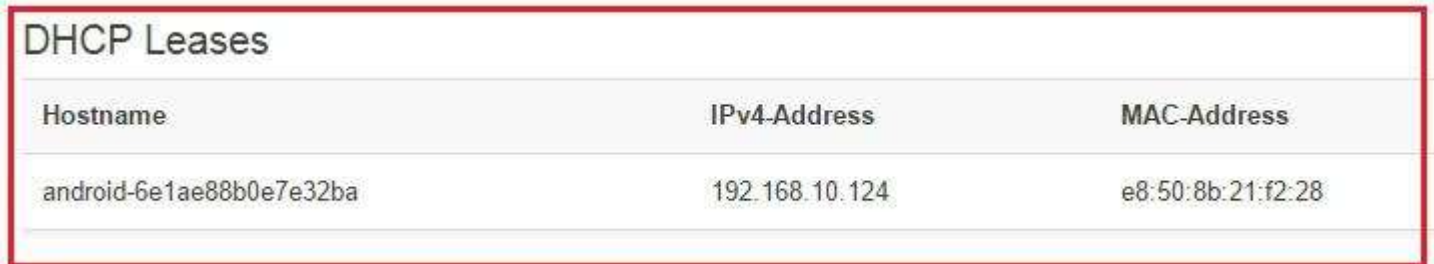
**IPSec Status**

Refresh

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

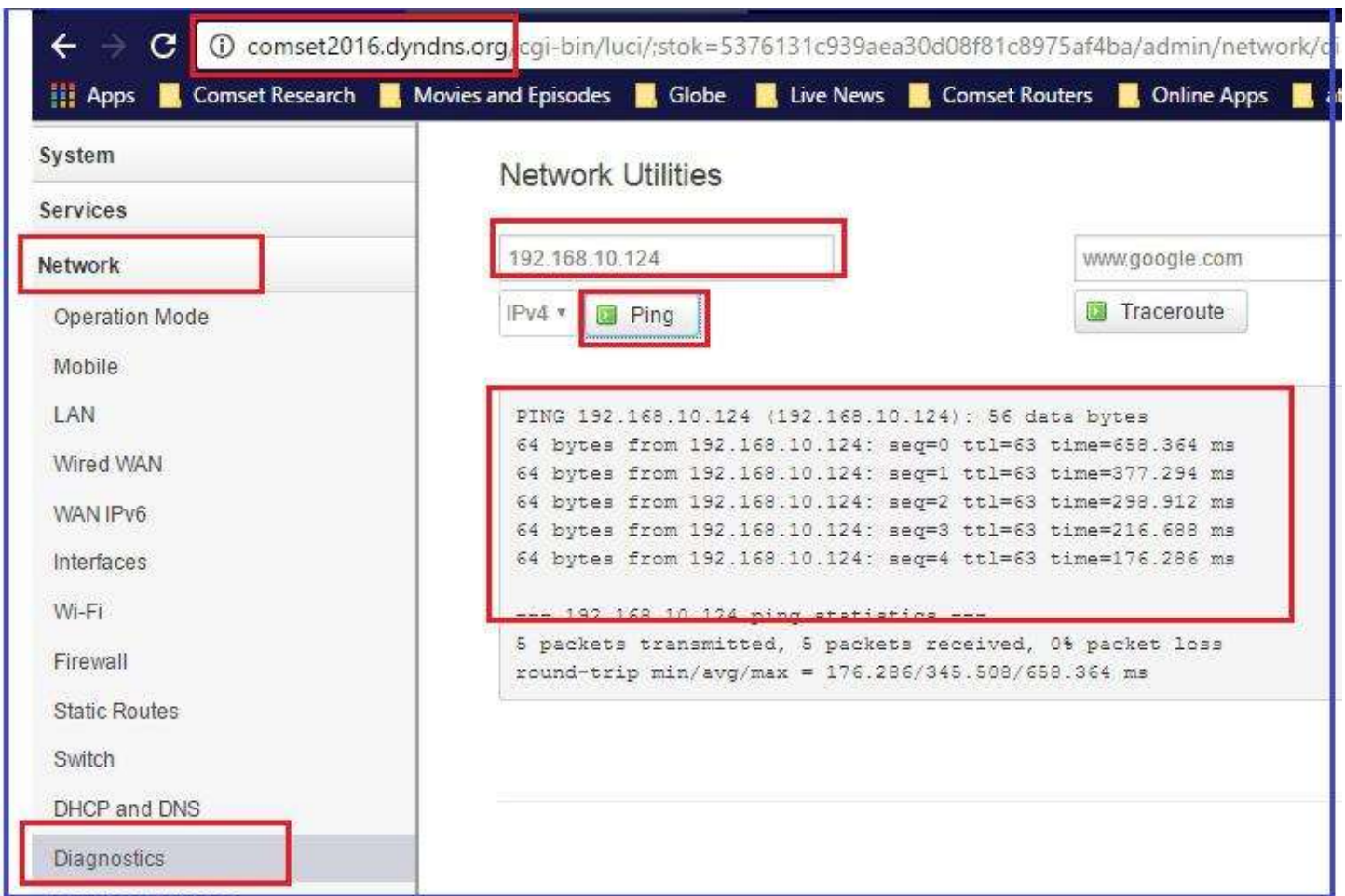
Connections:  
 ipsec\_base: comset2018.dyndns.org.0.0.0.0/0::0...comset2016.dyndns.org.0.0.0.0/0::0 IKEv1, dpddelay=30s  
 ipsec\_base: local: [comset2018.dyndns.org] uses pre-shared key authentication  
 ipsec\_base: remote: [comset2016.dyndns.org] uses pre-shared key authentication  
 ipsec\_base: 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: 079d27a7691647f\_j\* 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:



| 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.



comset2016.dyndns.org/cgi-bin/luci/stok=5376131c939aea30d08f81c8975af4ba/admin/network/...

Apps Comset Research Movies and Episodes Globe Live News Comset Routers Online Apps

**Network**

Operation Mode  
Mobile  
LAN  
Wired WAN  
WAN IPv6  
Interfaces  
Wi-Fi  
Firewall  
Static Routes  
Switch  
DHCP and DNS  
Diagnostics

**Network Utilities**

192.168.10.124 www.google.com

IPv4 Ping Traceroute

```
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
```