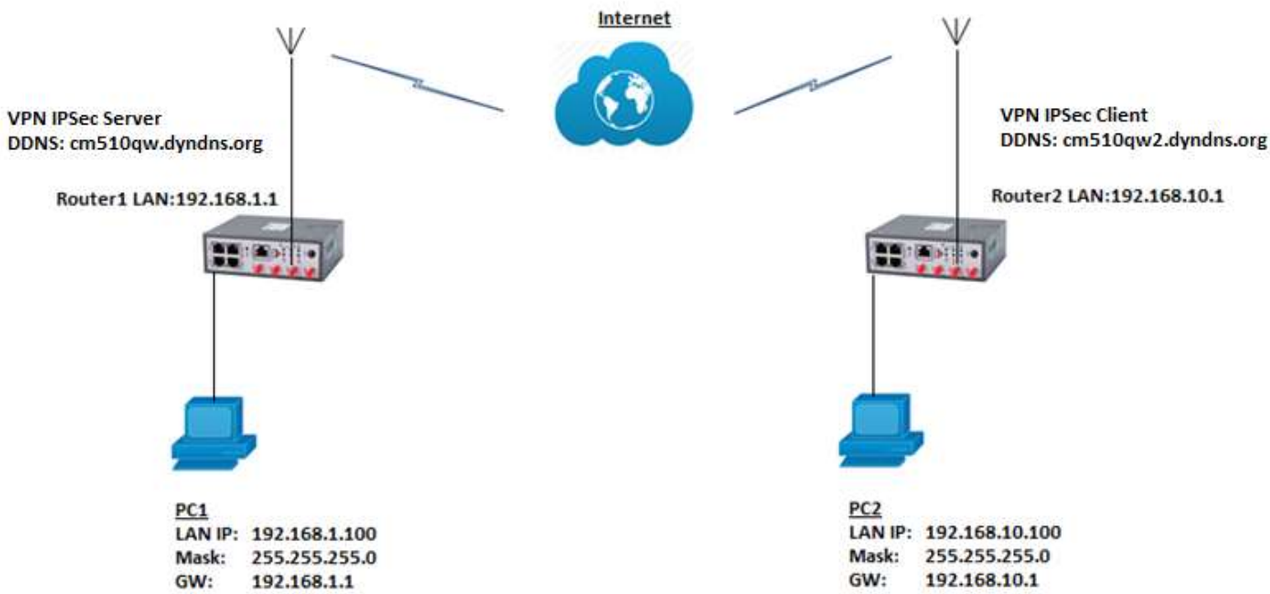
How to configure VPN IPSec on a Comset CM510Q-W

Network Topology:

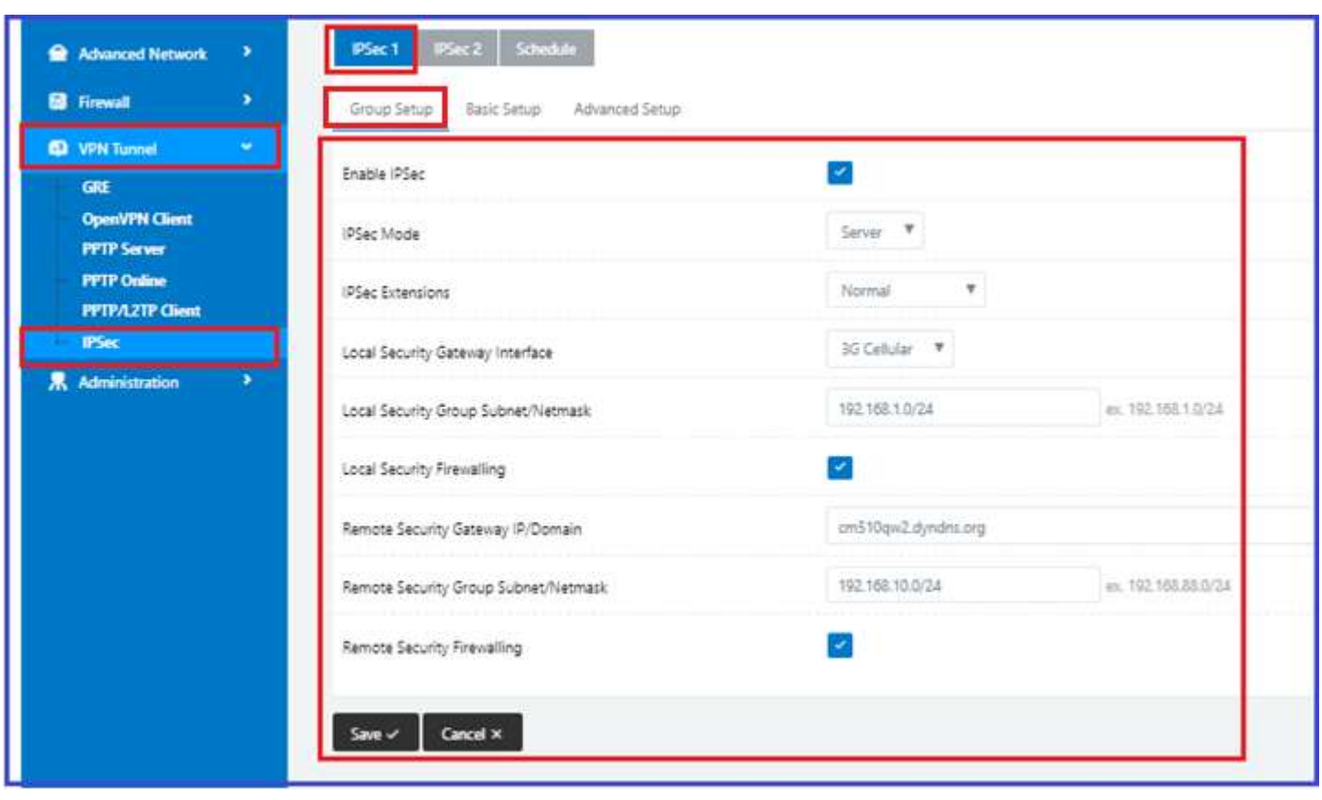


To configure VPN IPSec on the CM510Q-W router, please configure the router with the correct APN that will provide you with a Public WAN IP address, such as **telstra.extranet** for a Telstra Data SIM. You need to ask your carrier to activate your SIM card with a Public WAN IP.

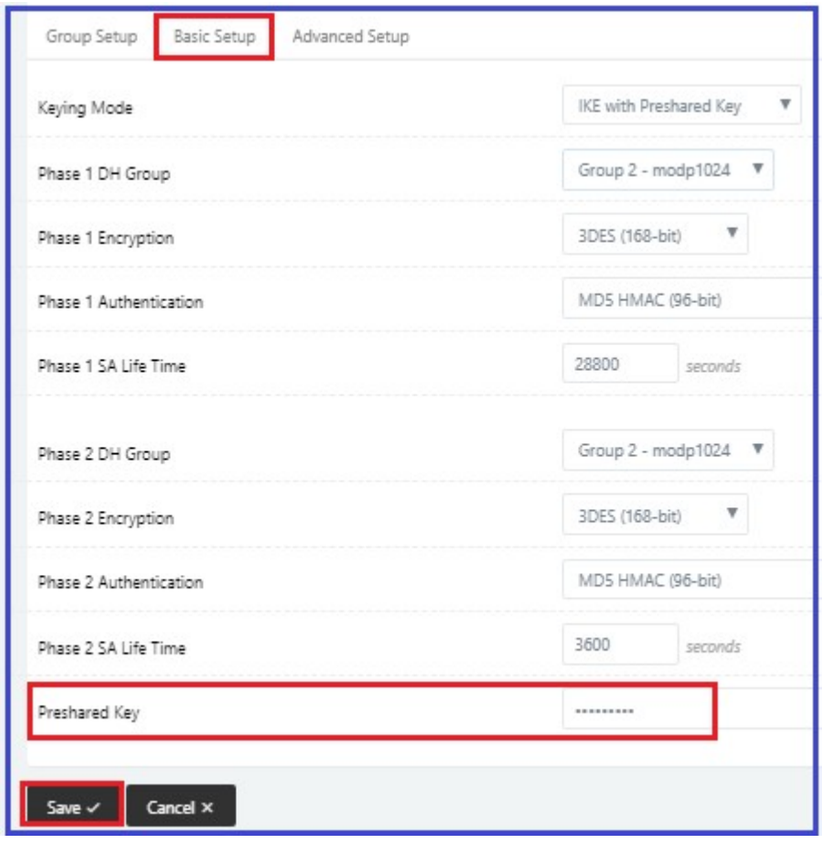
VPN Server Side

1. Go to VPN Tunnel -> IPSec1 -> Group Set-up. Set as below.

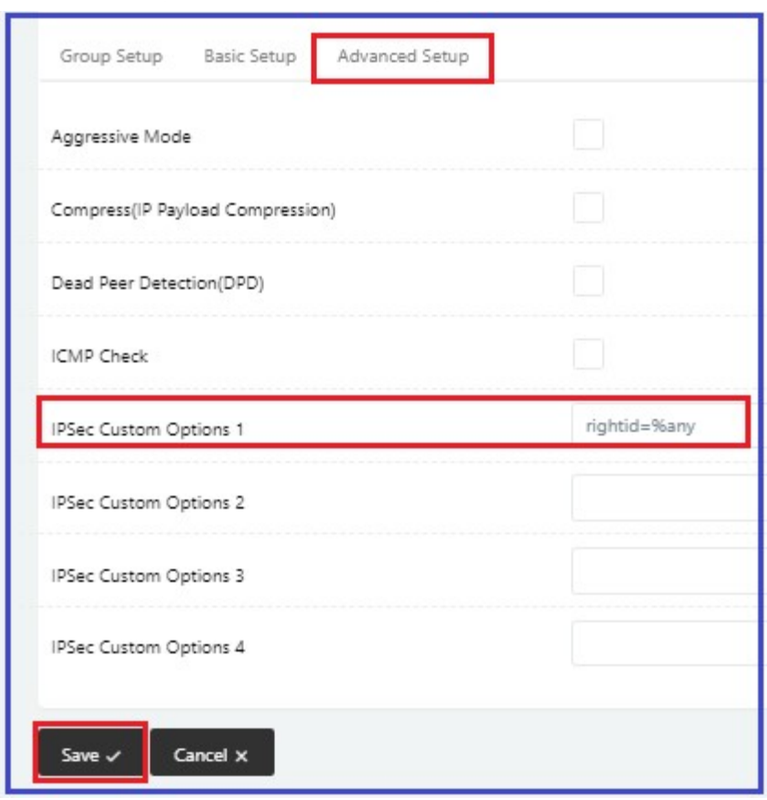
IPsec Mode:	**Server**
Local Security Group Subnet/Netmask:	**192.168.1.0/24**
Local Security Firewalling:	**Enabled**
Remote Security Gateway:	**cm510qw2.dyndns.org**
Remote Security Firewalling:	**192.168.10.0/24**
Remote Security Firewalling:	**Enabled**



2. Click on Basic Set-up.
   Set default Phase1 and Phase2 Groups such as Encryption, Authentication, Lifetime.
   Set Pre-shared key for VPN IPSec.
   Note: Pre-shared key should be the same on both routers to establish connection.



3. Click on Advanced Set-up and set IPSec Custom Options 1
   IPSec Custom Options 1: **rightid=%any**

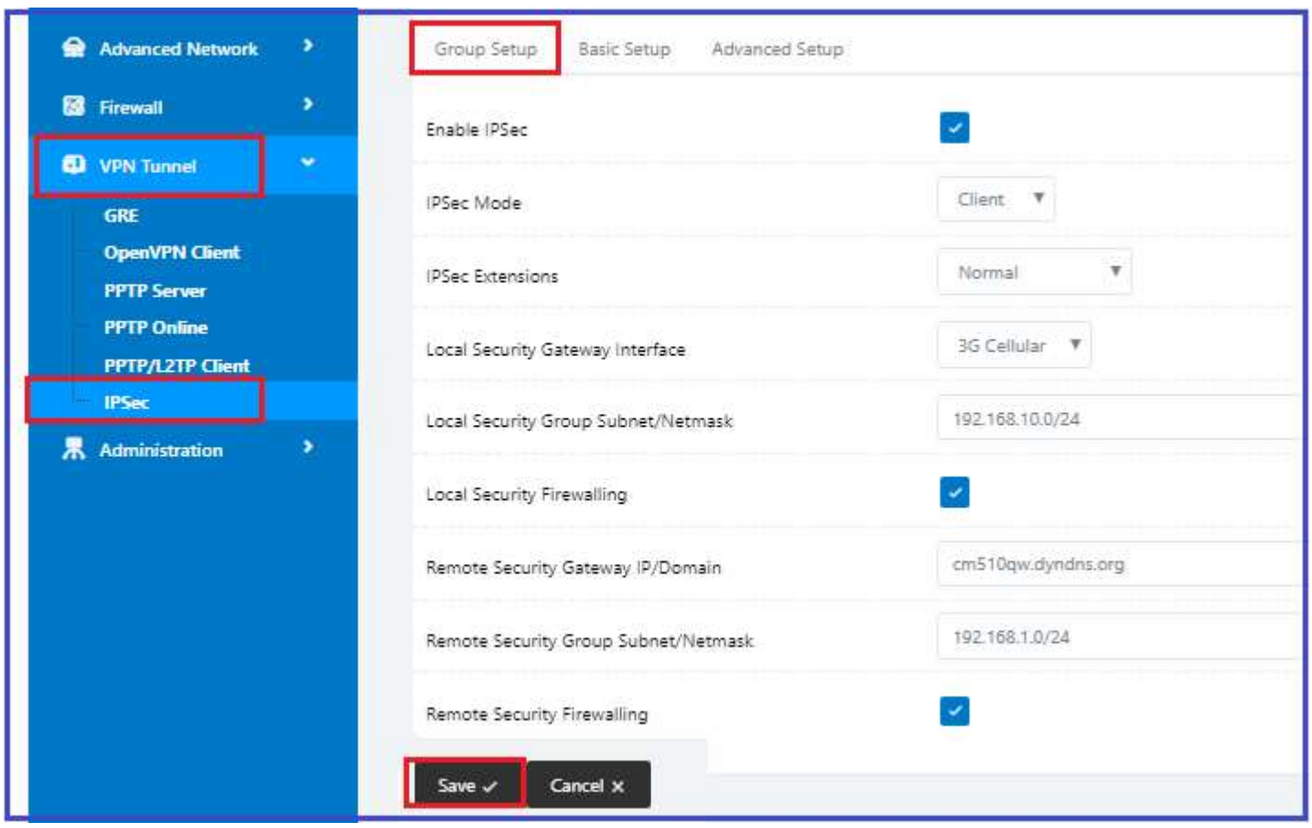


4. Go to Administration -> Admin Access -> **Uncheck"** Block WAN Ping" and Save apply. See below.

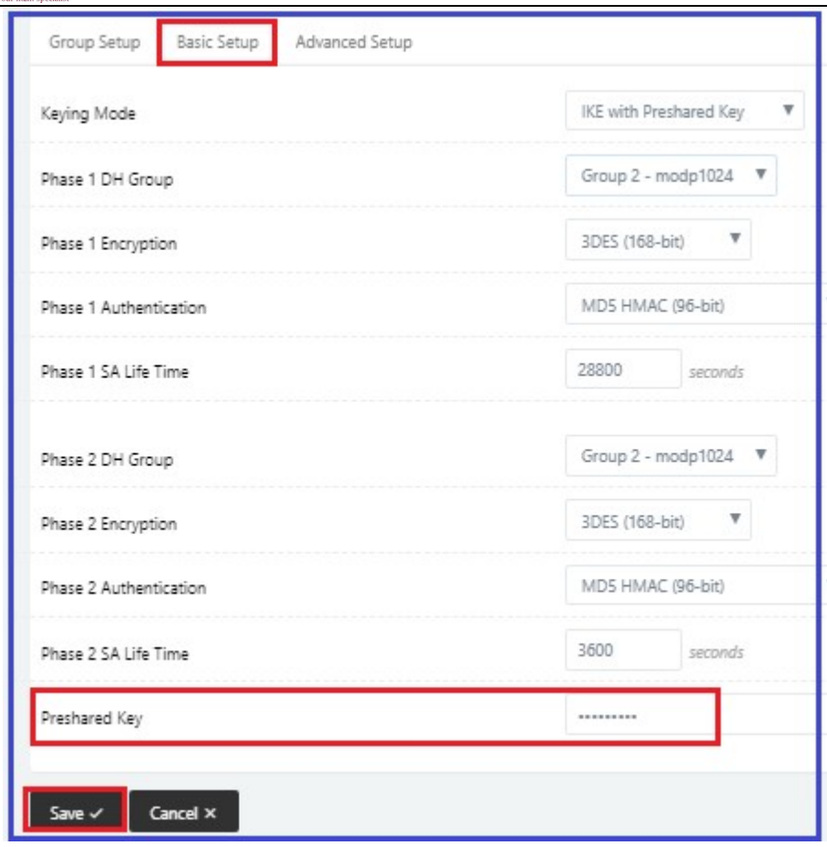
IPSec Client Side

1. Go to VPN Tunnel -> IPSec -> Group Setup

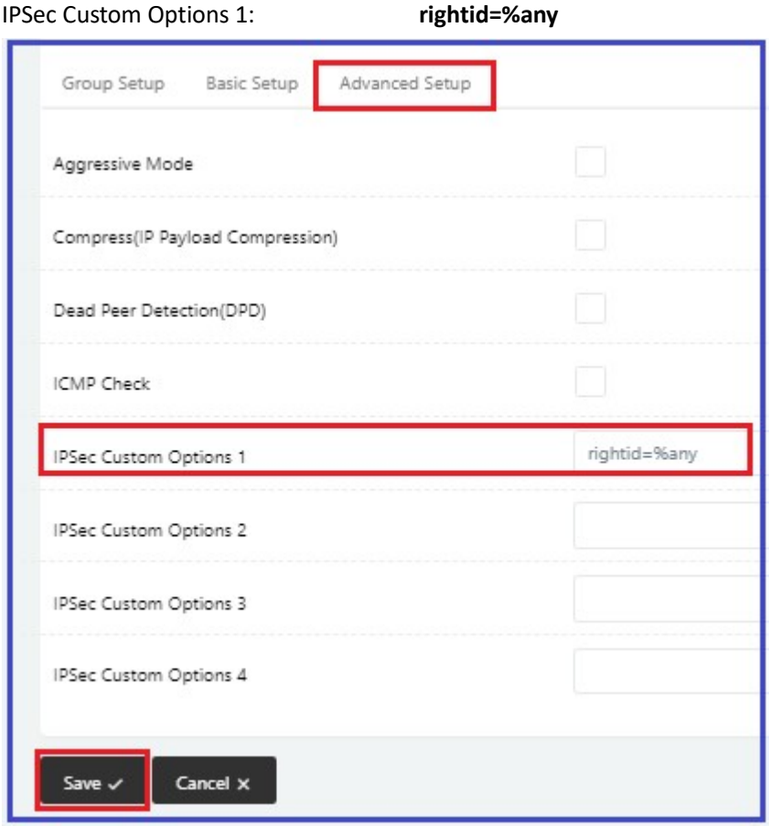
IPsec Mode:	**Client**
Local Security Group Subnet/Netmask:	**192.168.10.0/24**
Local Security Firewalling:	**Enabled**
Remote Security Gateway:	**cm510qw.dyndns.org**
Remote Security Firewalling:	**192.168.1.0/24**
Remote Security Firewalling:	**Enabled**



2. Click on Basic Set-up.
   Set default Phase1 and Phase2 Groups such as Encryption, Authentication, Lifetime.
   Set Pre-shared key for VPN IPSec.
   Note: Pre-shared key should be the same on both routers to establish connection.



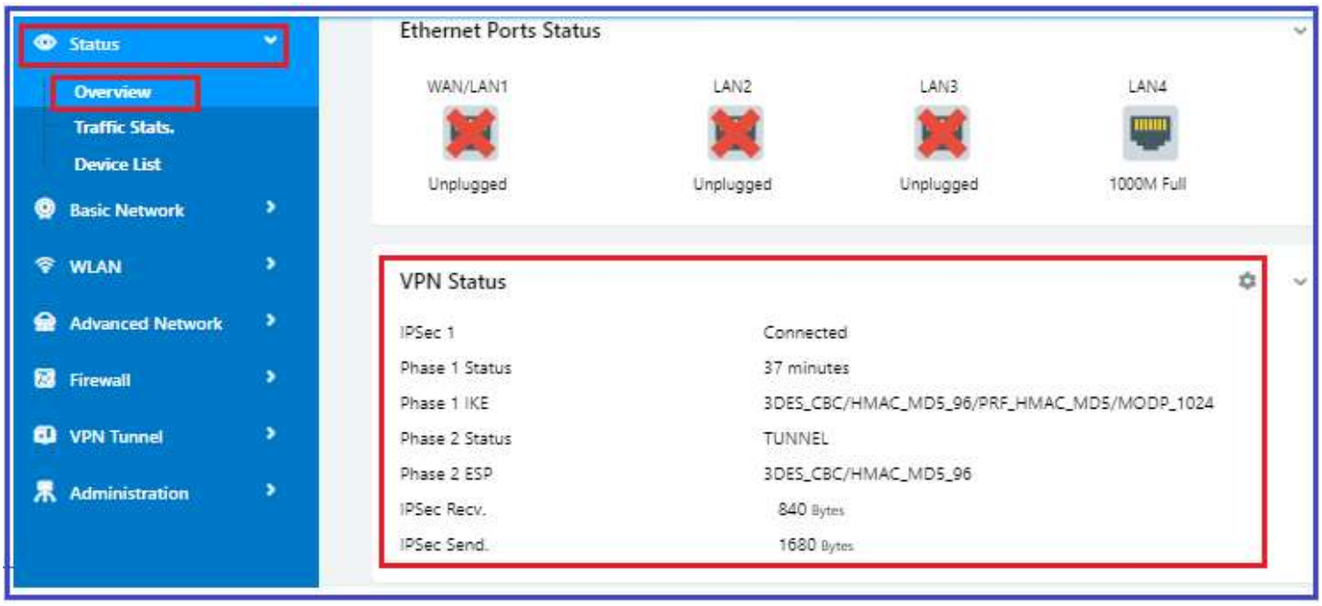
3. Click on Advanced Set-up and set IPSec Custom Options 1
   IPSec Custom Options 1: **rightid=%any**



4. Go to Administration -> Admin Access -> **Uncheck"** Block WAN Ping" and Save apply. See below.

Checking VPN IPSec Status and Testing VPN Tunnel.

1. Go to Status -> Overview -> VPN Status



2. Check Ping connection from PC1(192.168.1.100) behind the IPSec_server to PC2(192.168.10.100) behind the IPSec_client.

```
C:\Users\Tony>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9c70:98fe:2b67:b3c8%15
   IPv4 Address. . . . . . . . . . . : 192.168.1.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

```
C:\Users\Tony>ping 192.168.10.100

Pinging 192.168.10.100 with 32 bytes of data:
Reply from 192.168.10.100: bytes=32 time=70ms TTL=126
Reply from 192.168.10.100: bytes=32 time=63ms TTL=126
Reply from 192.168.10.100: bytes=32 time=73ms TTL=126
Reply from 192.168.10.100: bytes=32 time=92ms TTL=126

Ping statistics for 192.168.10.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 63ms, Maximum = 92ms, Average = 74ms
```

3. Check Ping connection from PC2(192.168.10.100) behind the IPSec_client to PC1(192.168.1.100) behind the IPSec_server

```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9571:4168:f214:45c9%15
   IPv4 Address. . . . . . . . . . . : 192.168.10.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1
```

```
C:\Users\a>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.1.100: bytes=32 time=185ms TTL=126
Reply from 192.168.1.100: bytes=32 time=158ms TTL=126
Reply from 192.168.1.100: bytes=32 time=99ms TTL=126
Reply from 192.168.1.100: bytes=32 time=371ms TTL=126

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 99ms, Maximum = 371ms, Average = 203ms
```