

# NR500 Series Industrial Cellular VPN Router

## Application Note 008

### OpenVPN Client with Username&Password

**Version:** V1.0.0  
**Date:** Aug 2018  
**Status:** Confidential



## Directory

1. Introduction.....	3
1.1 Overview.....	3
1.2 Compatibility.....	3
1.3 Version.....	3
1.4 Corrections.....	3
2. Topology.....	4
3. Configuration.....	5
3.1 Server Configuration.....	5
3.2 Client01 Configuration.....	7
3.3 Client02 Configuration.....	8
4. Route Table.....	10
4. Testing.....	11

# 1. Introduction

## 1.1 Overview

This document contains information regarding the configuration and use of OpenVPN client with username and password.

This guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product, and of the requirements for their specific application.

## 1.2 Compatibility

This application note applies to:

**Models Shown:** NR500 series.

**Firmware Version:** V1.0.0(903.0) or newer

**Other Compatible Models:** None

## 1.3 Version

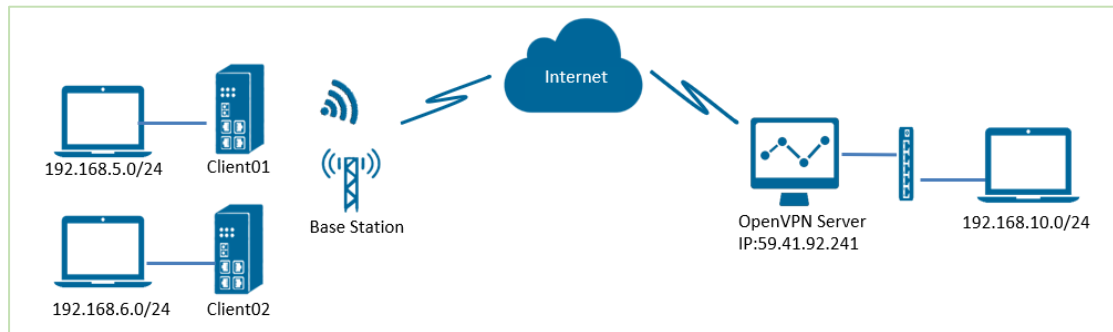
Updates between document versions are cumulative. Therefore, the latest document will include all the content of previous versions.

Release Date	Doc. Version	Firmware Version	Change Description
2018/08/03	V1.0.0	V1.0.0(903.0)	First released

## 1.4 Corrections

Appreciate for corrections or rectifications to this application note, and if any request for new application notes please email to: [support@navigateworx.com](mailto:support@navigateworx.com)

## 2. Topology

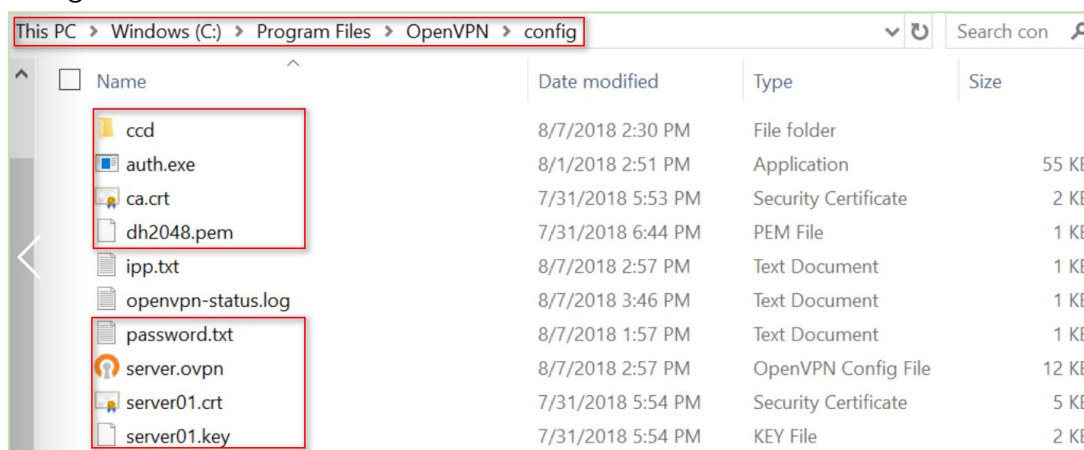


1. Two NR500 Pro run as OpenVPN Client01 and Client02 with any kind of IP, which can ping OpenVPN server IP successfully.
2. A PC runs as OpenVPN Server with a static public IP and open a specified a listening port for OpenVPN.
3. OpenVPN tunnel is established between Server and Client. Client01 can ping Client02 successfully and vice versa.

## 3. Configuration

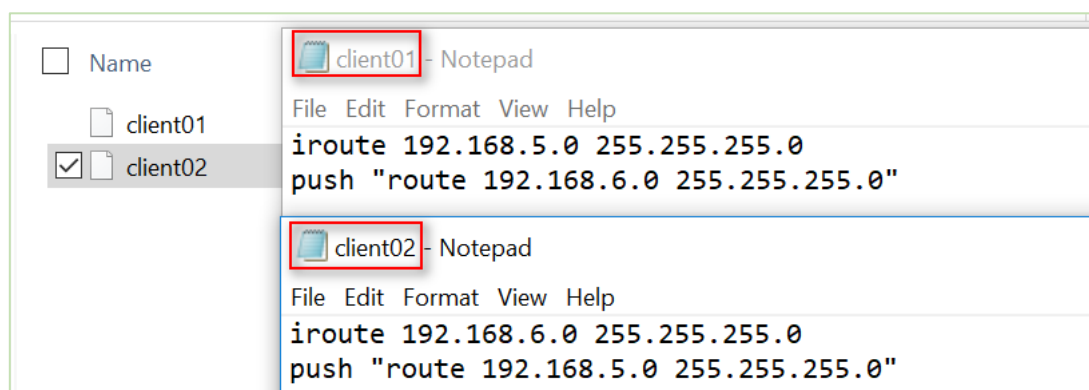
### 3.1 Server Configuration

1. Install OpenVPN software on PC and copy the related certifications and configuration to the PC like below:



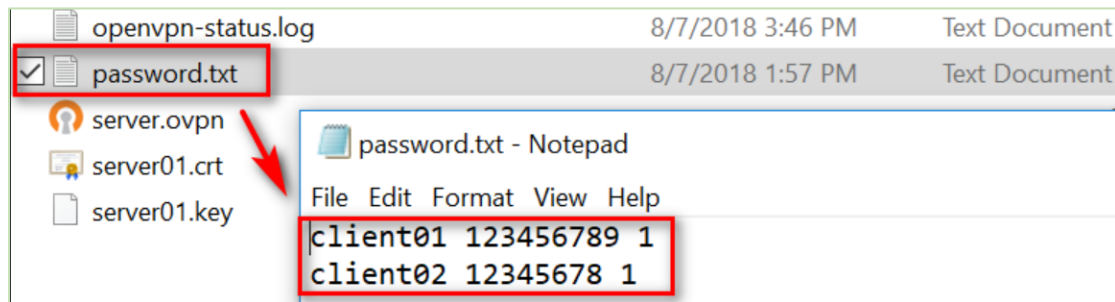
**Note:** a) Kindly download OpenVPN software with: <https://openvpn.net/>  
 b) Kindly install and run OpenVPN software with **administrator authority**.

2. Add a "ccd" folder, and create a new notepad, rename it without suffix, configure it like below:



**Note:** client01 and client02 are the common name.

3. Create a "password.txt" file, which including below content:



The format would be: **common name password 1 or 0(1=enable,0=disable)**

4. The configuration of **server.ovpn** like below:

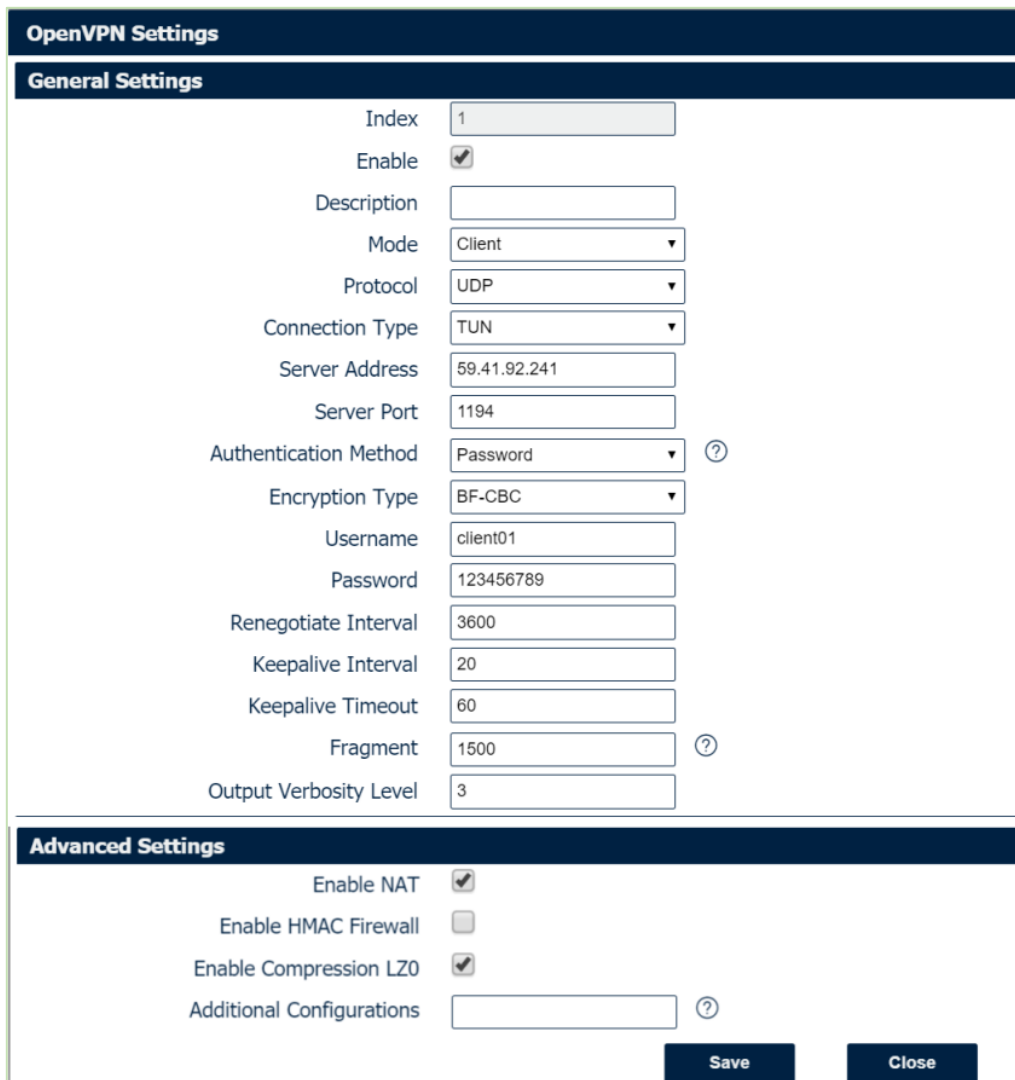
```

=====
local 59.41.92.241
mode server
port 1194
proto udp
client-cert-not-required
username-as-common-name
auth-user-pass-verify auth.exe via-env
script-security 3 system
dev tun
tun-mtu 1500
fragment 1500
ca ca.crt
cert server01.crt
key server01.key # This file should be kept secret
dh dh2048.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "route 192.168.10.0 255.255.255.0"
client-config-dir ccd
route 192.168.5.0 255.255.255.0
route 192.168.6.0 255.255.255.0
client-to-client
keepalive 10 120
cipher BF-CBC
comp-lzo
max-clients 100
persist-key
persist-tun
status openvpn-status.log
verb 3
=====

```

## 3.2 Client01 Configuration

1. Go to **VPN>OpenVPN>OpenVPN>General Settings**, click the Edit Button and configure OpenVPN as below picture. Click Save.



OpenVPN Settings	
General Settings	
Index	1
Enable	<input checked="" type="checkbox"/>
Description	
Mode	Client
Protocol	UDP
Connection Type	TUN
Server Address	59.41.92.241
Server Port	1194
Authentication Method	Password
Encryption Type	BF-CBC
Username	client01
Password	123456789
Renegotiate Interval	3600
Keepalive Interval	20
Keepalive Timeout	60
Fragment	1500
Output Verbosity Level	3

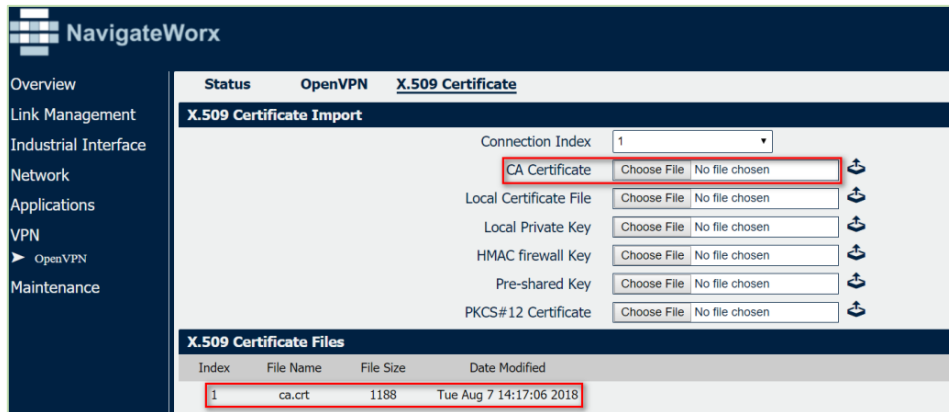
  

Advanced Settings	
Enable NAT	<input checked="" type="checkbox"/>
Enable HMAC Firewall	<input type="checkbox"/>
Enable Compression LZ0	<input checked="" type="checkbox"/>
Additional Configurations	

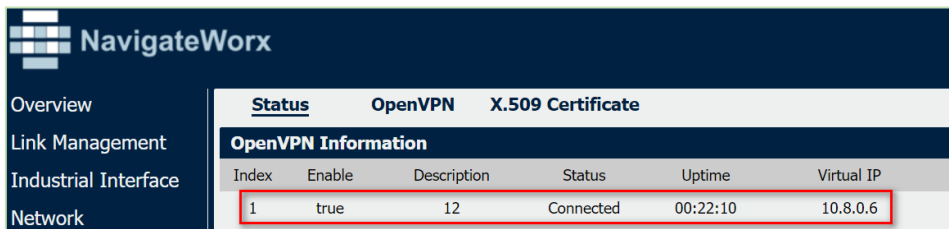
Save Close

2. Click Save>Apply.

3. Go to **VPN>OpenVPN>X.509 Certificate**, to import the related certification, Click Apply.



4.Route had connected to OpenVPN server. Go to **VPN>OpenVPN>Status** to check the connection status.



### 3.3 Client02 Configuration

1. Go to **VPN>OpenVPN>OpenVPN>General Settings**, click the Edit Button and configure OpenVPN as below picture. Click Save.



**OpenVPN Settings**

**General Settings**

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/>
Description	<input type="text"/>
Mode	<input type="text" value="Client"/>
Protocol	<input type="text" value="UDP"/>
Connection Type	<input type="text" value="TUN"/>
Server Address	<input type="text" value="59.41.92.241"/>
Server Port	<input type="text" value="1194"/>
Authentication Method	<input style="border: 1px solid #ccc;" type="text" value="Password"/>
Encryption Type	<input type="text" value="BF-CBC"/>
Username	<input type="text" value="client02"/>
Password	<input type="text" value="12345678"/>
Renegotiate Interval	<input type="text" value="3600"/>
Keepalive Interval	<input type="text" value="20"/>
Keepalive Timeout	<input type="text" value="60"/>
Fragment	<input type="text" value="1500"/>
Output Verbosity Level	<input type="text" value="3"/>

**Advanced Settings**

Enable NAT	<input checked="" type="checkbox"/>
Enable HMAC Firewall	<input type="checkbox"/>
Enable Compression LZ0	<input checked="" type="checkbox"/>
Additional Configurations	<input type="text"/>

2. Click Save>Apply.

3. Go to **VPN>OpenVPN>X.509 Certificate**, to import the related certification, Click Apply.

**NavigateWorx**

Overview  
 Link Management  
 Industrial Interface  
 Network  
 Applications  
 VPN  
   ▶ OpenVPN  
 Maintenance

<b>Status</b>	<b>OpenVPN</b>	<b>X.509 Certificate</b>
---------------	----------------	--------------------------

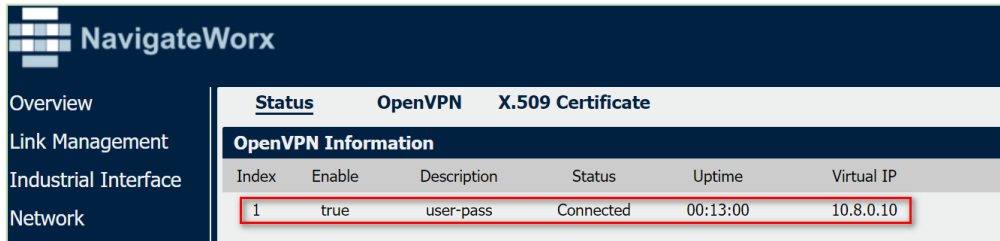
**X.509 Certificate Import**

Connection Index	<input type="text" value="1"/>
CA Certificate	<input style="border: 1px solid #ccc;" type="text" value="Choose File"/> <input style="border: none; background: none; color: #ccc;" type="button" value="No file chosen"/>
Local Certificate File	<input style="border: 1px solid #ccc;" type="text" value="Choose File"/> <input style="border: none; background: none; color: #ccc;" type="button" value="No file chosen"/>
Local Private Key	<input style="border: 1px solid #ccc;" type="text" value="Choose File"/> <input style="border: none; background: none; color: #ccc;" type="button" value="No file chosen"/>
HMAC firewall Key	<input style="border: 1px solid #ccc;" type="text" value="Choose File"/> <input style="border: none; background: none; color: #ccc;" type="button" value="No file chosen"/>
Pre-shared Key	<input style="border: 1px solid #ccc;" type="text" value="Choose File"/> <input style="border: none; background: none; color: #ccc;" type="button" value="No file chosen"/>
PKCS#12 Certificate	<input style="border: 1px solid #ccc;" type="text" value="Choose File"/> <input style="border: none; background: none; color: #ccc;" type="button" value="No file chosen"/>

**X.509 Certificate Files**

Index	File Name	File Size	Date Modified
1	ca.crt	1188	Tue Aug 7 14:17:06 2018

4.Route had connected to OpenVPN server. Go to **VPN>OpenVPN>Status** to check the connection status.



The screenshot shows the 'Status' page for OpenVPN. The 'OpenVPN Information' table is as follows:

Index	Enable	Description	Status	Uptime	Virtual IP
1	true	user-pass	Connected	00:13:00	10.8.0.10

## 4. Route Table

1. Route Table on OpenVPN Server for reference.

```
IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
-----
0.0.0.0                    0.0.0.0          192.168.111.1   192.168.111.19   291
0.0.0.0                    0.0.0.0          192.168.10.1    192.168.10.10    291
10.8.0.0                   255.255.255.0    10.8.0.2        10.8.0.1         35
10.8.0.0                   255.255.255.252  On-link         10.8.0.1         291
10.8.0.1                   255.255.255.255  On-link         10.8.0.1         291
10.8.0.3                   255.255.255.255  On-link         10.8.0.1         291
127.0.0.0                  255.0.0.0        On-link         127.0.0.1        331
127.0.0.1                  255.255.255.255  On-link         127.0.0.1        331
127.255.255.255           255.255.255.255  On-link         127.0.0.1        331
192.168.5.0                255.255.255.0    10.8.0.2        10.8.0.1         35
192.168.6.0                255.255.255.0    10.8.0.2        10.8.0.1         35
192.168.10.0               255.255.255.0    On-link         192.168.10.10    291
192.168.10.10             255.255.255.255  On-link         192.168.10.10    291
```

2. Route Table on Client01 for reference.

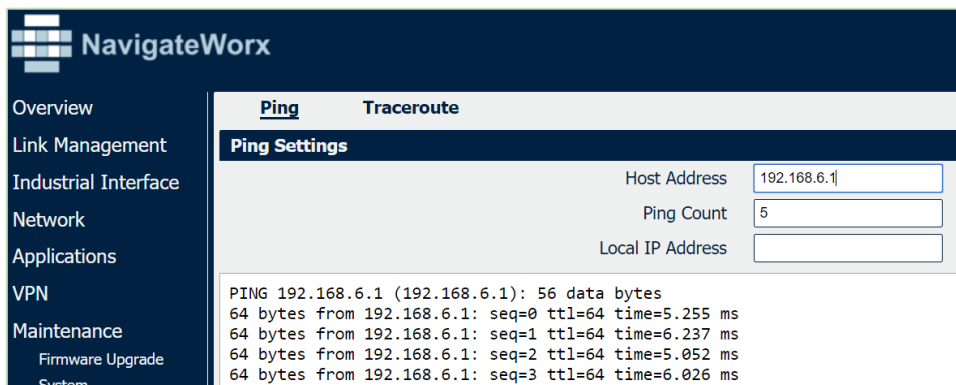
Route Table Information				
Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.8.0.0	255.255.255.0	10.8.0.5	tun1
3	10.8.0.5	255.255.255.255	0.0.0.0	tun1
4	192.168.5.0	255.255.255.0	0.0.0.0	lan0
5	192.168.6.0	255.255.255.0	10.8.0.5	tun1
6	192.168.10.0	255.255.255.0	10.8.0.5	tun1
7	192.168.111.0	255.255.255.0	0.0.0.0	wan

3. Route Table on Client02 for reference.

Route Table Information				
Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.8.0.0	255.255.255.0	10.8.0.9	tun1
3	10.8.0.9	255.255.255.255	0.0.0.0	tun1
4	192.168.5.0	255.255.255.0	10.8.0.9	tun1
5	192.168.6.0	255.255.255.0	0.0.0.0	lan0
6	192.168.10.0	255.255.255.0	10.8.0.9	tun1
7	192.168.111.0	255.255.255.0	0.0.0.0	wan

## 4. Testing

1. Ping from Client01 to Client02 as below:



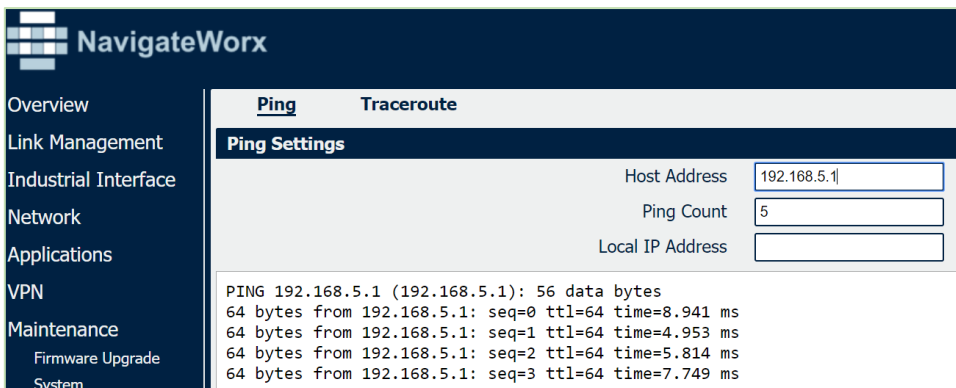
The screenshot shows the NavigateWorx interface with the 'Ping' tool selected. The 'Ping Settings' section shows the Host Address set to 192.168.6.1 and Ping Count set to 5. The results show four successful ping attempts from 192.168.6.1 to 192.168.5.1 with varying response times.

Host Address	Ping Count	Local IP Address
192.168.6.1	5	

```

PING 192.168.6.1 (192.168.6.1): 56 data bytes
64 bytes from 192.168.6.1: seq=0 ttl=64 time=5.255 ms
64 bytes from 192.168.6.1: seq=1 ttl=64 time=6.237 ms
64 bytes from 192.168.6.1: seq=2 ttl=64 time=5.052 ms
64 bytes from 192.168.6.1: seq=3 ttl=64 time=6.026 ms
  
```

2. Ping from Client02 to Client01 as below:



The screenshot shows the NavigateWorx interface with the 'Ping' tool selected. The 'Ping Settings' section shows the Host Address set to 192.168.5.1 and Ping Count set to 5. The results show four successful ping attempts from 192.168.5.1 to 192.168.6.1 with varying response times.

Host Address	Ping Count	Local IP Address
192.168.5.1	5	

```

PING 192.168.5.1 (192.168.5.1): 56 data bytes
64 bytes from 192.168.5.1: seq=0 ttl=64 time=8.941 ms
64 bytes from 192.168.5.1: seq=1 ttl=64 time=4.953 ms
64 bytes from 192.168.5.1: seq=2 ttl=64 time=5.814 ms
64 bytes from 192.168.5.1: seq=3 ttl=64 time=7.749 ms
  
```

3. Test successfully