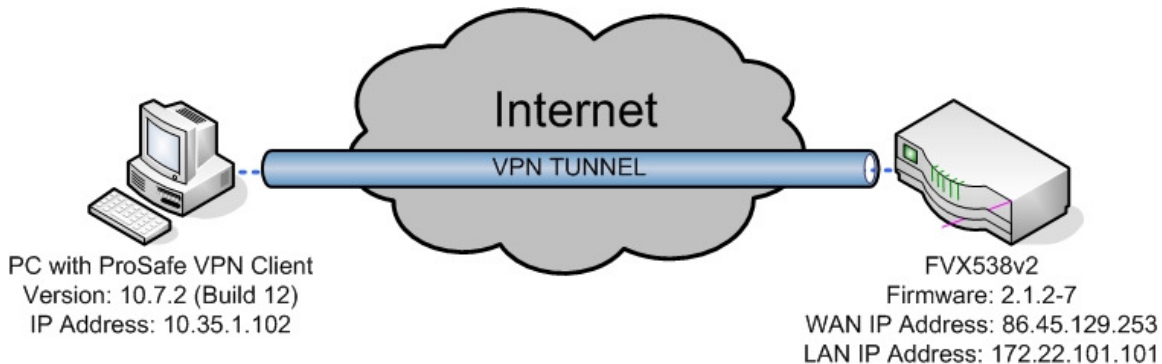


# NETGEAR®

Connect with Innovation™

## Mode Config of a VPN tunnel from ProSafe Client to FVX538v2 Router:

Mode Config is a feature included in some of the Netgear Routers which allows the IP addressing of the remote client devices be handled and controlled by the VPN Router by using a Virtual Adapter. This document will guide you on how to create IKE and Mode Config policies for your FVX538v2, as well as how to configure the VPN Pro-Safe VPN client in order to allow a Virtual Private Network to be established over the internet.



**NOTE:** This document assumes that your FVX538v2 is either receiving a public IP address on the WAN interface or that the gateway device(s) have the correct port forwarding or DMZ configured so that port 500 UDP is open for the FVX538v2, these gateway devices must also allow VPN pass-through.

## FVX538v2 – Mode Config:

To configure it, go to the VPN section and then select Mode Config. For our example we'll use the following settings:

The screenshot displays the NETGEAR ProSafe VPN Firewall FVX538 web interface. The top navigation bar includes links for Network Configuration, Security, VPN, Administration, Monitoring, Web Support, and Logout. The current page is titled 'Edit Mode Config Record' and shows a successful operation message: 'Operation succeeded.'

The configuration is divided into two main sections:

- Client Pool:** This section is for configuring the VPN client pool. The record name is 'vpn'. It includes fields for three IP pools and two DNS/WINS servers.
  - First Pool:** Starting IP: 192.168.24.1, Ending IP: 192.168.24.250
  - Second Pool:** Starting IP: 0.0.0.0, Ending IP: 0.0.0.0
  - Third Pool:** Starting IP: 0.0.0.0, Ending IP: 0.0.0.0
  - WINS Server:** Primary: 0.0.0.0, Secondary: 0.0.0.0
  - DNS Server:** Primary: 0.0.0.0, Secondary: 0.0.0.0
- Traffic Tunnel Security Level:** This section is for configuring the security level of the traffic tunnel.
  - PFS Key Group: DH Group 2 (1024 bit)
  - SA Lifetime: 3600 Seconds
  - Encryption Algorithm: 3DES
  - Integrity Algorithm: SHA-1
  - Local IP Address: 172.22.101.0
  - Local Subnet Mask: 255.255.255.0

At the bottom of the configuration area, there are 'Apply' and 'Reset' buttons. The footer of the page indicates '2006 © Copyright NETGEAR®'.

The first pool of IP addresses, 192.168.24.1 to 192.168.24.250, lists the addresses that the clients will acquire when they connect. Notice that you can add up to three pools, addresses from the second pool will be used when the addresses of the first pool are all in use. Likewise for the third pool, it'll be used when the first and second pools are exhausted. Notice that you can also set particular DNS servers or WINS for the client virtual adapters.

**(Note: DO NOT** add IP addresses that are currently in use in any of the networks at either side of the VPN tunnel – Use completely different subnets.)

## FVX538v2 – IKE Policy:

With the Mode Config policy created, go to VPN, Policies, IKE policies and create a new one. For our example, we'll use the following settings.

**NETGEAR PROSAFE** NETGEAR ProSafe VPN Firewall FVX538

Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout

Polices :: VPN Wizard :: Certificates :: Mode Config :: VPN Client :: Connection Status

Edit IKE Policy Add New VPN Policy

Operation succeeded.

**Mode Config Record** help

Do you want to use Mode Config Record?  
 Yes  No  
Select Mode Config Record: vpn view selected

**General** help

Policy Name: vpn  
Direction / Type: Responder  
Exchange Mode: Aggressive

**Local** help

Select Local Gateway:  WAN1  WAN2  
Identifier Type: FQDN  
Identifier: fvx\_local.com

**Remote** help

Identifier Type: FQDN  
Identifier: fvx\_remote.com

**IKE SA Parameters** help

Encryption Algorithm: 3DES  
Authentication Algorithm: SHA-1  
Authentication Method:  Pre-shared key  RSA-Signature  
Pre-shared key: 123456789 (Key Length 8 - 49 Char)  
Diffie-Hellman (DH) Group: Group 2 (1024 bit)  
SA-Lifetime (sec): 28800  
Enable Dead Peer Detection:  Yes  No  
Detection Period: 10 (Seconds)  
Reconnect after failure count: 3

**Extended Authentication** help

**XAUTH Configuration**

None  
 Edge Device  
 IPSec Host

Authentication Type: User Database  
Username:  
Password:

Apply Reset

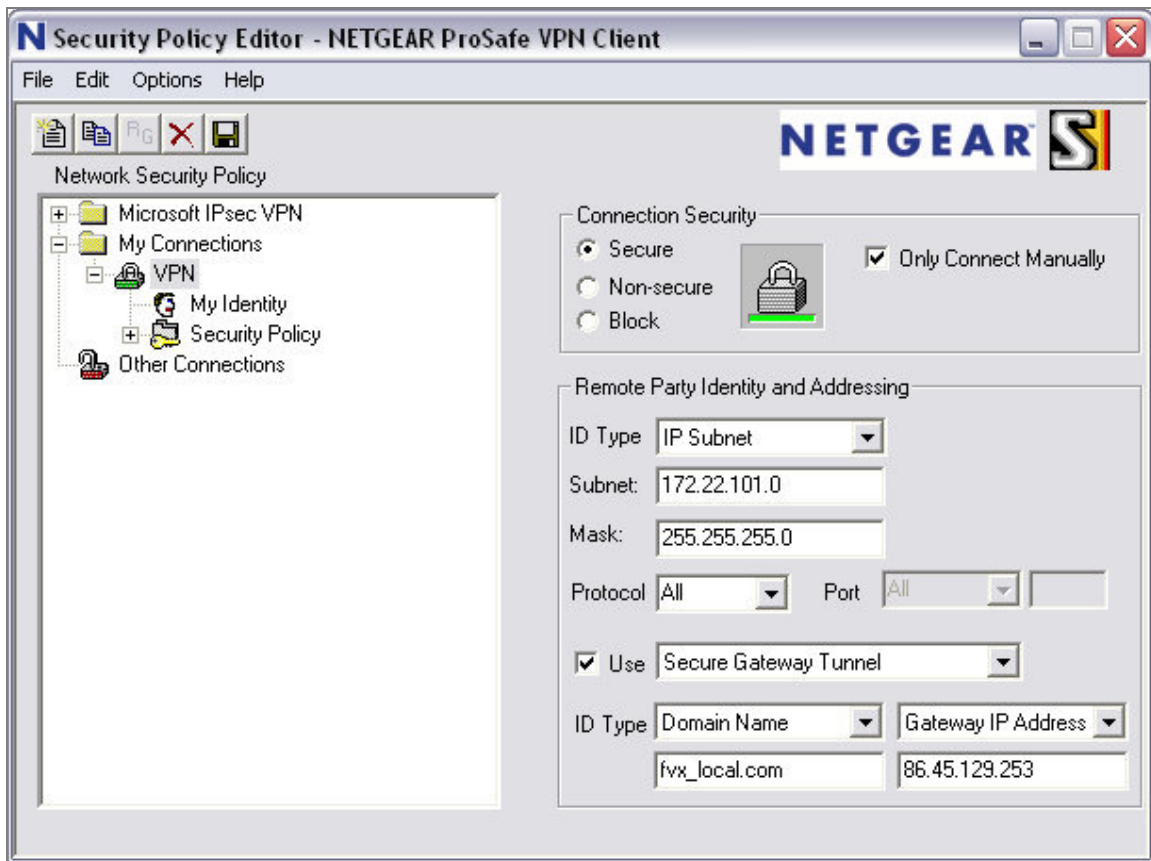
2006 © Copyright NETGEAR

(Note: The pre-shared key could be any alphanumeric string)

## Pro-Safe VPN Client - Configuration:

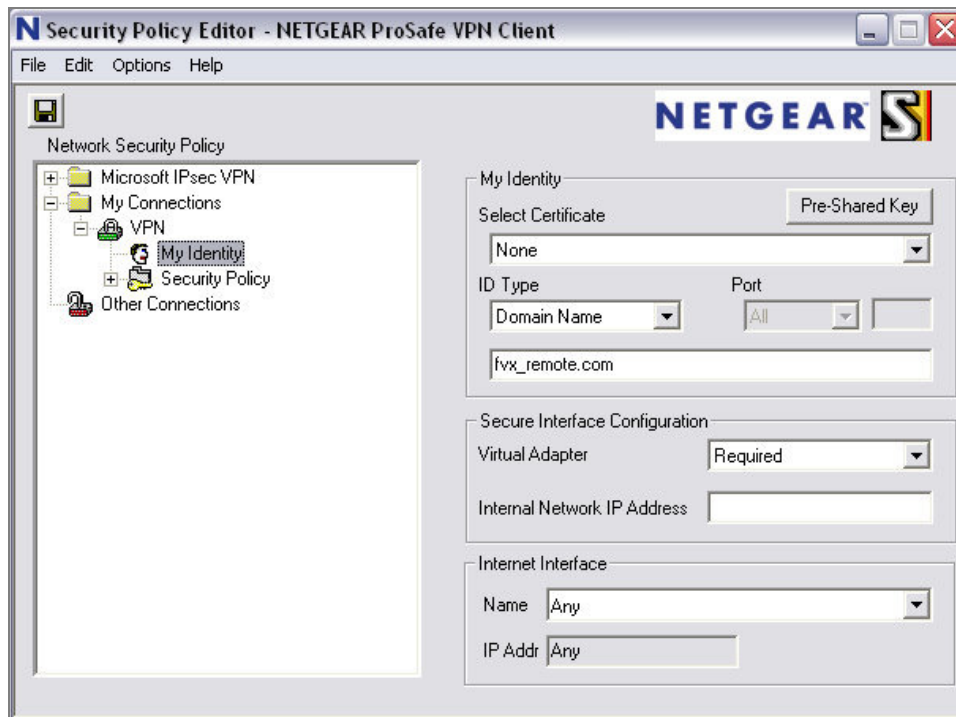
Right click on “**My Connections**” and add a new connection. Use the same name you used to name the VPN policy in your VPN gateway. In this example the name will be “VPN”.

Click on the name of the new created connection and fill the parameters accordingly, for this example we'll use these:

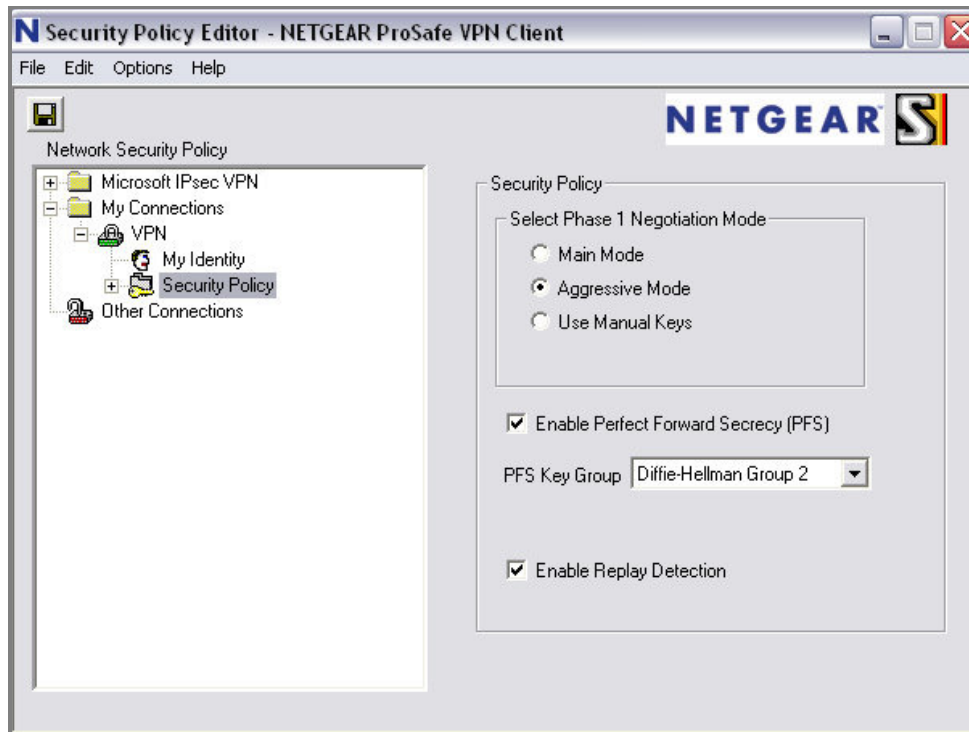


**(NOTE:** The Subnet and Mask must be those of the LAN side of your FVX538. The Gateway IP address field must be the WAN IP address of the FVX538. )

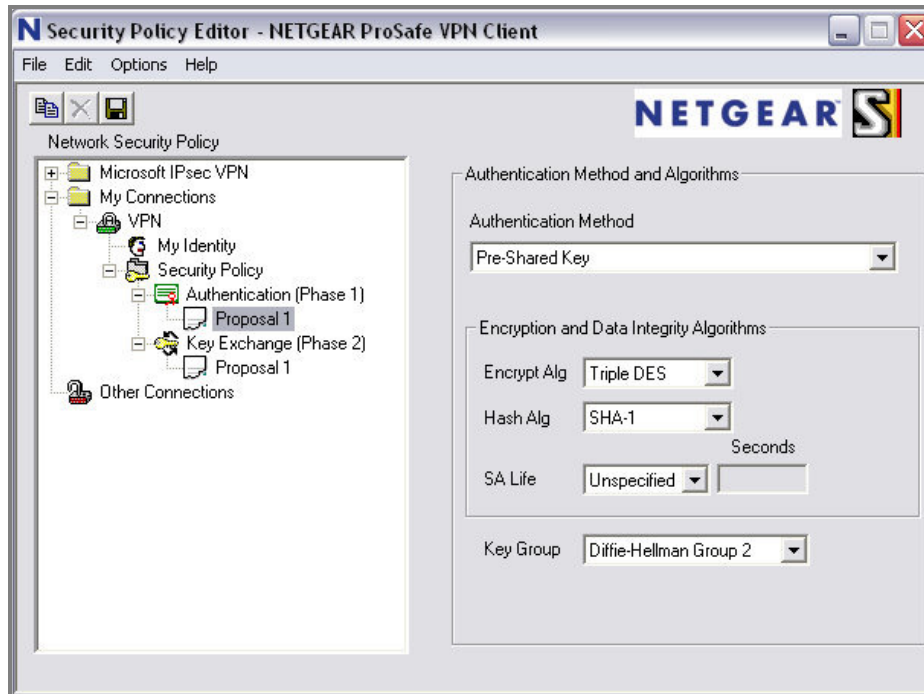
Click on **“My Identity”** and fill the fields accordingly, **be sure to click on the Pre-Shared Key button and input your own pre shared key.** Here are the settings used in our example:



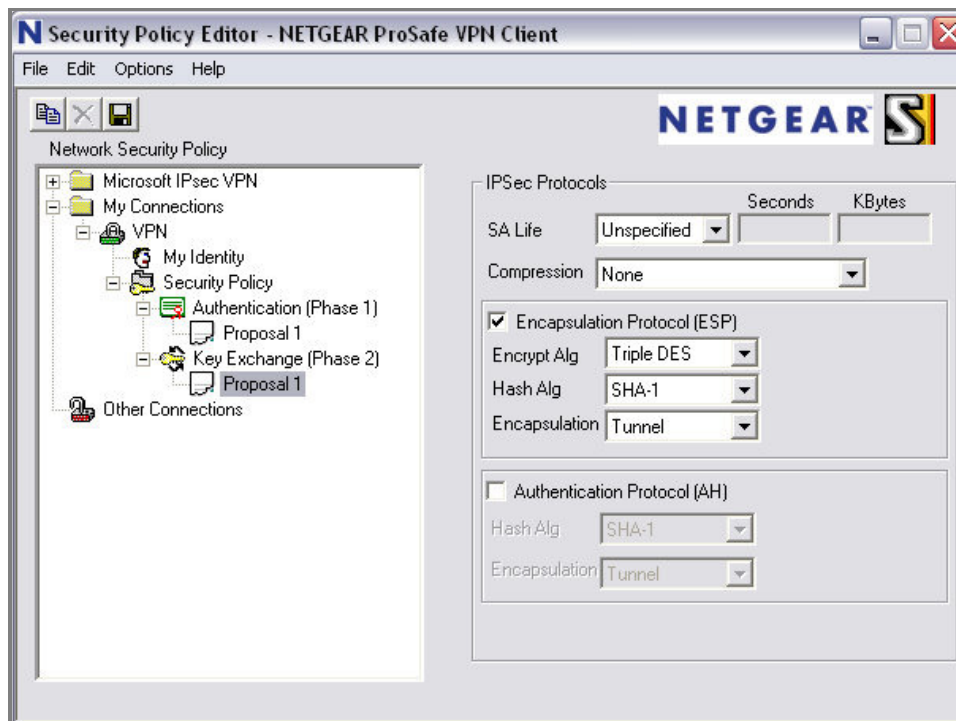
Click on **“Security Policy”** and verify the following settings:



Next, expand “**Security Policy**” and “**Authentication (Phase 1)**” – Click on “**Proposal 1**” and verify the settings contained to match the ones of your policy. Functional settings in our example:

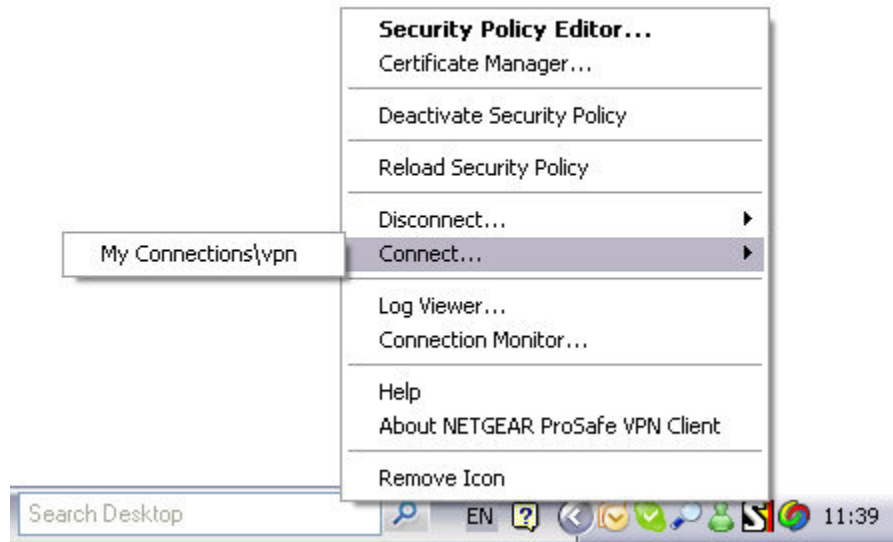


Open the “**Key Exchange (Phase 2)**” category – Click on “**Proposal 1**” and verify the settings contained to match the ones of your policy. Functional settings in our example:





For last, right click on the tray icon of the Netgear VPN client with your mouse, select connect and select the connection you just created.

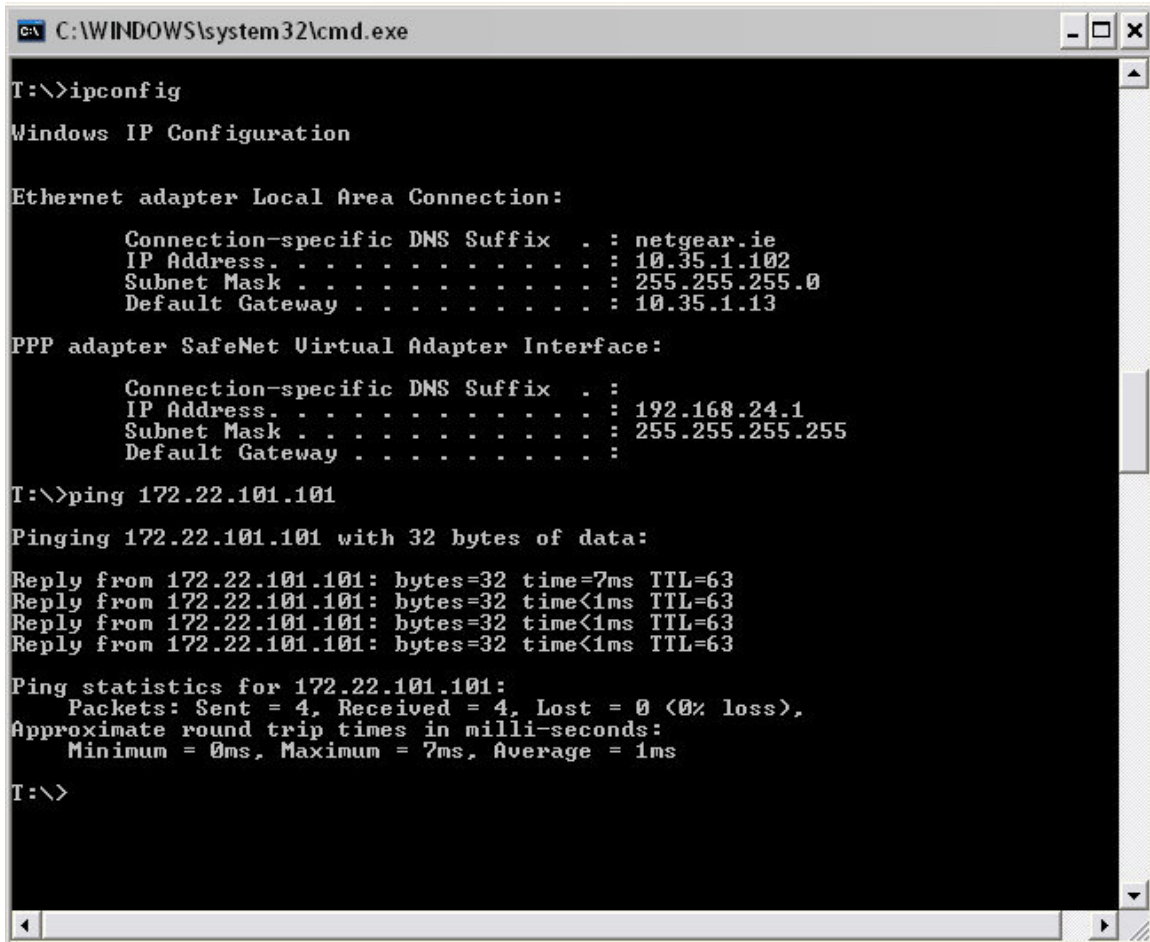


If your settings are correct you'll receive a message confirming the connection.



## FVX538v2 – Verifying connection:

If you wish to verify that the connection is established, which IP did you receive from the Mode Config pools and whether you can access the LAN side of the VPN router, open a command console and use the **IPCONFIG** command to see the IP address of the Virtual Adapter. You can also use the command **PING** towards the LAN address of your router to verify connectivity.



```
C:\WINDOWS\system32\cmd.exe

T:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : netgear.ie
    IP Address. . . . .                : 10.35.1.102
    Subnet Mask . . . . .              : 255.255.255.0
    Default Gateway . . . . .          : 10.35.1.13

PPP adapter SafeNet Virtual Adapter Interface:

    Connection-specific DNS Suffix  . :
    IP Address. . . . .                : 192.168.24.1
    Subnet Mask . . . . .              : 255.255.255.255
    Default Gateway . . . . .          :

T:\>ping 172.22.101.101

Pinging 172.22.101.101 with 32 bytes of data:

Reply from 172.22.101.101: bytes=32 time=7ms TTL=63
Reply from 172.22.101.101: bytes=32 time<1ms TTL=63
Reply from 172.22.101.101: bytes=32 time<1ms TTL=63
Reply from 172.22.101.101: bytes=32 time<1ms TTL=63

Ping statistics for 172.22.101.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 1ms

T:\>
```