

AWS LAB

Create my Virtual Private Cloud (VPC) to produce customized network.

VPC will contain a Public Subnet and a Private Subnet, each subnet with 1 EC2 instance

Purpose: ping to google.com from the EC2 located in the Private Subnet

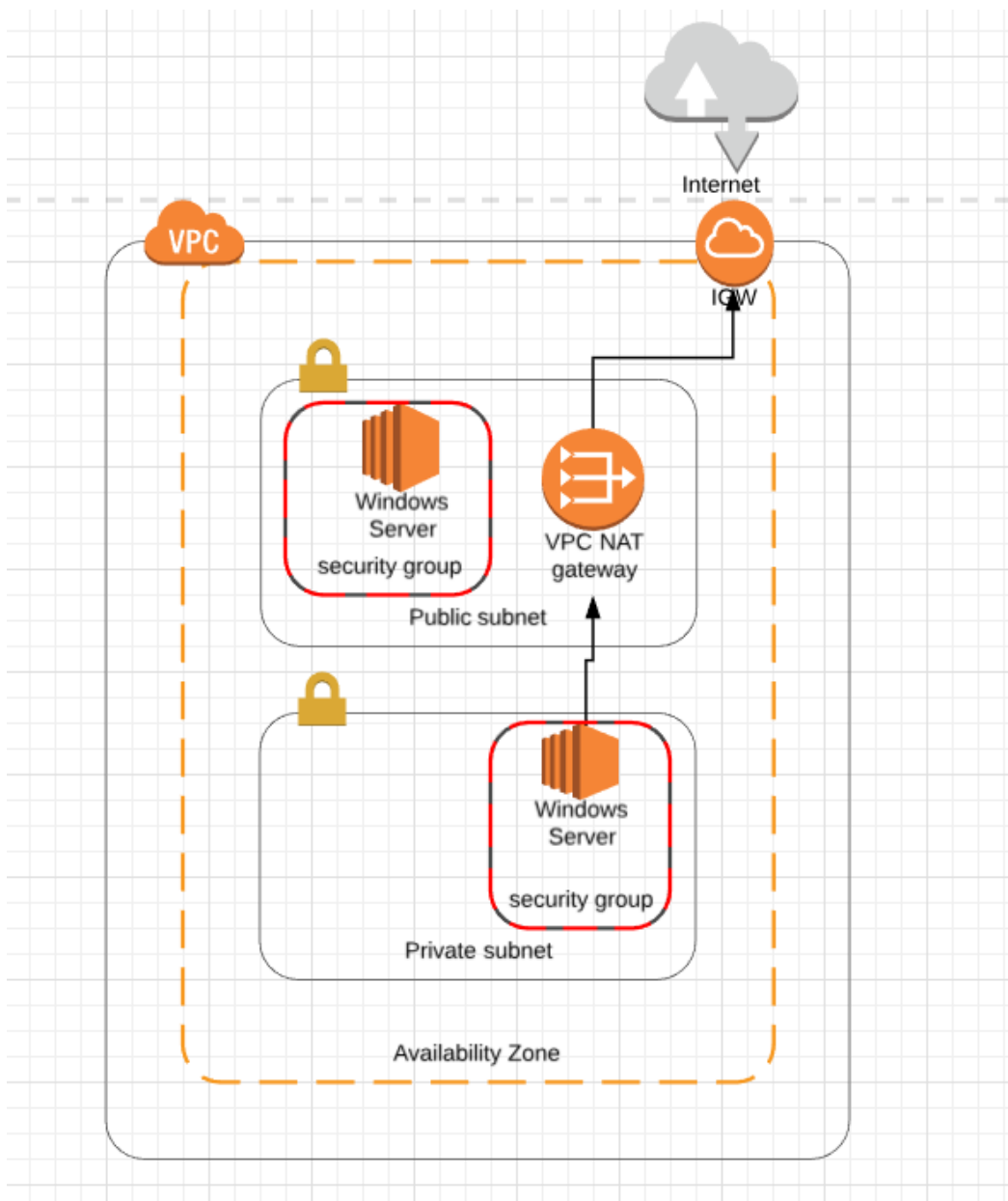
For this, a NAT Gateway will be configured in the public subnet.

Private subnet traffic should be routed through the NAT instance or Gateway for Internet access.

The IGW allows communication between instances in my VPC and Internet

Even if it is recommended to start with at least 2 Availability Zones, for this Lab I will use only 1, to simplify

Here is what looks like my Infrastructure:



AWS Console

- VPC -> Start VPC Wizard

Select VPC Configuration: VPC with Public and Private Subnets, in the same ZA

Step 2: VPC with Public and Private Subnets

IPv4 CIDR block:* (65531 IP addresses available)

IPv6 CIDR block: ☒ No IPv6 CIDR Block
☐ Amazon provided IPv6 CIDR block

VPC name:

Public subnet's IPv4 CIDR:* (251 IP addresses available)

Availability Zone:*

Public subnet name:

Private subnet's IPv4 CIDR:* (251 IP addresses available)

Availability Zone:*

Private subnet name:

You can add more subnets after AWS creates the VPC.

Specify the details of your NAT Instance ([Instance rates apply](#)).

Instance type:*

Key pair name:

Service endpoints

Enable DNS hostnames:* ☒ Yes ☐ No

Hardware tenancy:*

At this step, we have “VPC Manu Lab” created with the 2 Subnets: one Public, one Private

Search Subnets and their projects

<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR	Available IP	IF
<input checked="" type="checkbox"/>	Public subnet	subnet-c2f545a4	available	vpc-461d6e20 VPC Manu Lab	10.0.0.0/24	250	
<input type="checkbox"/>	Private subnet	subnet-d7ff4fb1	available	vpc-461d6e20 VPC Manu Lab	10.0.1.0/24	251	
<input type="checkbox"/>		subnet-8590a2de	available	vpc-1d1dc17b	172.31.32.0/20	4091	
<input type="checkbox"/>		subnet-de65a196	available	vpc-d81cc0be RosettaHUB VPC	172.30.1.0/24	250	
<input type="checkbox"/>		subnet-bc6da9f4	available	vpc-1d1dc17b	172.31.16.0/20	4091	
<input type="checkbox"/>		subnet-f49aa8af	available	vpc-d81cc0be RosettaHUB VPC	172.30.2.0/24	250	
<input type="checkbox"/>		subnet-600cfd06	available	vpc-1d1dc17b	172.31.0.0/20	4091	
<input type="checkbox"/>		subnet-c304f5a5	available	vpc-d81cc0be RosettaHUB VPC	172.30.0.0/24	250	

subnet-c2f545a4 | Public subnet

Route Table: [rtb-663eae1f](#)

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	lgw-9995eefe

- **Route Table configuration**

Search Route Tables and their associated VPCs

Name	Route Table ID	Explicitly Associated	Main	VPC
Public Route Table	rtb-663eae1f	1 Subnet	No	vpc-461d6e20 VPC Manu Lab
Private Route Table	rtb-7b27b702	0 Subnets	Yes	vpc-461d6e20 VPC Manu Lab
	rtb-3cca2845	0 Subnets	Yes	vpc-1d1dc17b
	rtb-20c92b59	0 Subnets	Yes	vpc-d81cc0be RosettaHUB VPC

rtb-663eae1f | Public Route Table

Summary | **Routes** | Subnet Associations | Route Propagation | Tags

Edit

View: All rules

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-9995ee0e	Active	No

- **Create my VPC security group**, with Inbound Rule set to RDP, in order to be able to connect to instances (Windows Servers) of my VPC from my laptop (set IP address where I am connecting from):

Create Security Group | Security Group Actions

Filter: All security groups

Name tag	Group ID	Group Name	VPC	Description
WebSecurityGroup	sg-7a284307	WebSecurityGroup	vpc-461d6e20 VPC Manu ...	Enable Internet access
	sg-08c86472	default	vpc-1d1dc17b	default VPC security group
	sg-1bca6661	vpc-d81cc0be-securit...	vpc-d81cc0be RosettaHUB...	RosettaHUB Master security group
	sg-1bf05c61	vpc-d81cc0be-securit...	vpc-d81cc0be RosettaHUB...	RosettaHUB Slave security group
	sg-6bf45811	vpc-d81cc0be-securit...	vpc-d81cc0be RosettaHUB...	RosettaHUB security group
	sg-6ec86414	vpc-d81cc0be-securit...	vpc-d81cc0be RosettaHUB...	RosettaHUB Efs security group
	sg-d5cf63af	default	vpc-d81cc0be RosettaHUB...	default VPC security group
	sg-d92b40a4	default	vpc-461d6e20 VPC Manu ...	default VPC security group

sg-7a284307 | WebSecurityGroup

Summary | **Inbound Rules** | Outbound Rules | Tags

Cancel **Save**

Type	Protocol	Port Range	Source	Description
RDP (3389)	TCP (6)	3389	109.210.64.103/32	

Add another rule **No results**

- **Launch Instances**

Service menu -> EC2 -> Launch Instance

Microsoft Windows Server 2016 Base

Free tier eligible

Root device type: ebs | Virtualization type: hvm | ENA Enabled: Yes

Ubuntu Server 16.04 LTS (HVM), SSD Volume Type - ami-58d7e821

Ubuntu Server 16.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Free tier eligible

Root device type: ebs | Virtualization type: hvm | ENA Enabled: Yes

Are you launching a database instance? Try Amazon RDS.

Amazon Relational Database Service (RDS) makes it easy to set up, operate, and scale your database on AWS by automating time-consuming database management tasks. With RDS, you can easily deploy **Amazon Aurora**, **MariaDB**, **MySQL**, **Oracle**, **PostgreSQL**, and **SQL Server** databases on AWS. **Aurora** is a MySQL- and PostgreSQL-compatible, enterprise-class database at 1/10th the cost of commercial databases. [Learn more about RDS](#)

Launch a database using RDS

Microsoft Windows Server 2016 Base - ami-894c7b00

Microsoft Windows 2016 Datacenter edition [English]

Free tier eligible

Root device type: ebs | Virtualization type: hvm | ENA Enabled: Yes

Deep Learning AMI (Ubuntu) Version 9.0 - ami-da586ea3

Comes with latest binaries of deep learning frameworks pre-installed in separate virtual environments: MXNet, TensorFlow, Caffe, Caffe2, PyTorch, Keras, Chainer, Theano and CNTK. Fully-configured with NVIDIA CUDA, cuDNN and NCCL as well as Intel MKL-DNN

Choose T2.micro type

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance types Current generation Show/Hide Columns

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only
<input checked="" type="checkbox"/>	General purpose	t2.micro Free tier eligible	1	1	EBS only
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only

1st Instance in the Public Subnet

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower price.

Number of instances	1	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-461d6e20 VPC Manu Lab Create new VPC	
Subnet	subnet-c2f545a4 Public subnet eu-west-1a Create new subnet 250 IP Addresses available	
Auto-assign Public IP	Enable	
Placement group	<input type="checkbox"/> Add instance to placement group.	
Domain join directory	None Create new directory	
IAM role	None Create new IAM role	
Shutdown behavior	Stop	
Enable termination protection	<input type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring Additional charges apply.	
Tenancy	Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.	
Elastic GPU	<input type="checkbox"/> Add GPU Additional charges apply.	
T2 Unlimited	<input type="checkbox"/> Enable	

Create a new security group

- RDP Port 3389 to connect to this instance as the AMI requires port 3389 to be open in order to have access
- HTTP and HTTPS ports to allow Internet traffic (unrestricted access)

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group
☐ Select an existing security group

Security group name: launch-wizard-1

Description: launch-wizard-1 created 2018-05-28T21:24:19.229+02:00

Type	Protocol	Port Range	Source
HTTP	TCP	80	Anywhere 0.0.0.0/0 ::0
HTTPS	TCP	443	Anywhere 0.0.0.0/0 ::0
RDP	TCP	3389	My IP 109.210.64.103/32
Add Rule			

Create the 2nd instance in the private subnet

Number of instances [Launch into Auto Scaling Group](#)

Purchasing option ☐ Request Spot Instances

Network [Create new VPC](#)

Subnet [Create new subnet](#)
251 IP Addresses available

Auto-assign Public IP

Placement group ☐ Add instance to placement group.

Domain join directory [Create new directory](#)

IAM role [Create new IAM role](#)

Shutdown behavior

Protection protection ☐ Protect against accidental termination

Monitoring ☐ Enable CloudWatch detailed monitoring

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server a HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☐ Create a new security group

☐ Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source
Custom TCP	TCP	3309	Anywhere

Add Rule

I have now 3 instances:

- 2 inside my public Subnet:
 - Windows Server Public, created by myself
 - Nat Instance, created automatically by Wizard VPC

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs
Windows Server Public	i-02802ca4a431f457c	t2.micro	eu-west-1a	running	2/2 checks...	OK	ec2-34-247-29-26.eu-west-1.compute.amazonaws.com	34.247.29.26	-
Windows Server Private	i-069486ef5a41ae4a5	t2.micro	eu-west-1a	initializing	2/2 checks...	OK	-	-	-
	i-089e805fafc0fab32	t2.nano	eu-west-1a	running	2/2 checks...	OK	ec2-34-246-17-238.eu-west-1.compute.amazonaws.com	34.246.17.238	-

Instance: i-02802ca4a431f457c (Windows Server Public) Public DNS: ec2-34-247-29-26.eu-west-1.compute.amazonaws.com

Description	Status Checks	Monitoring	Tags
Instance ID	i-02802ca4a431f457c	Instance state	running
Instance type	t2.micro	Elastic IPs	-
Availability zone	eu-west-1a	Private DNS	ip-10-0-0-169.eu-west-1.compute.internal
Security groups	launch-wizard-1	Private IPs	10.0.0.169
Scheduled events	No scheduled events	Secondary private IPs	-
AMI ID	Windows_Server-2016-English-Full-Base-2018.05.09 (ami-894c7bf0)	VPC ID	vpc-461d6e20
Platform	windows	Subnet ID	subnet-c2f545a4
		Network interfaces	eth0

- 1 inside my Private Sunet
 - Windows Server Private, created by myself

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs
Windows Server Public	i-02802ca4a431f457c	t2.micro	eu-west-1a	running	2/2 checks...	OK	ec2-34-247-29-26.eu-west-1.compute.amazonaws.com	34.247.29.26	-
Windows Server Private	i-069486ef5a41ae4a5	t2.micro	eu-west-1a	initializing	2/2 checks...	OK	-	-	-
	i-089e805fafc0fab32	t2.nano	eu-west-1a	running	2/2 checks...	OK	ec2-34-246-17-238.eu-west-1.compute.amazonaws.com	34.246.17.238	-

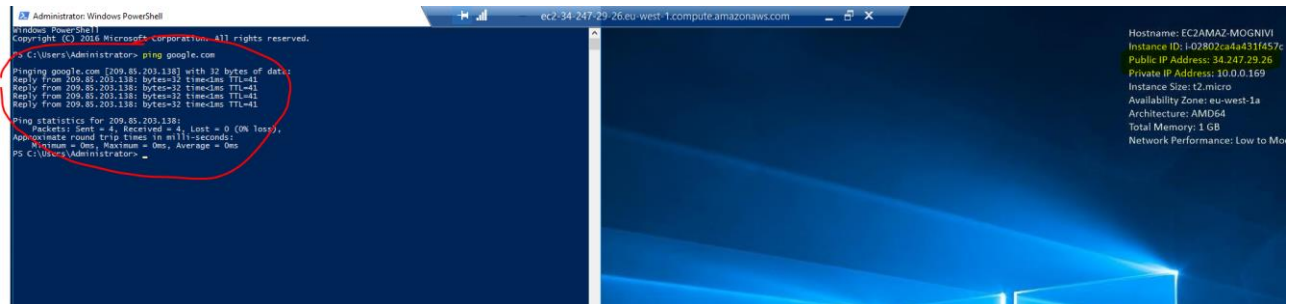
Instance: i-069486ef5a41ae4a5 (Windows Server Private) Private IP: 10.0.1.68

Description	Status Checks	Monitoring	Tags
Instance ID	i-069486ef5a41ae4a5	Instance state	running
Instance type	t2.micro	Elastic IPs	-
Availability zone	eu-west-1a	Private DNS	ip-10-0-1-68.eu-west-1.compute.internal
Security groups	launch-wizard-2	Private IPs	10.0.1.68
Scheduled events	No scheduled events	Secondary private IPs	-
AMI ID	Windows_Server-2016-English-Full-Base-2018.05.09 (ami-894c7bf0)	VPC ID	vpc-461d6e20
Platform	windows	Subnet ID	subnet-d7ff4fb1
IAM role	-	Network interfaces	eth0
Key pair name	manu_VPC_TP	Source/dest check	True
		T2 Unlimited	Disabled

Before to configure the NAT Gateway (Bastion), let's connect to the instance and check if ping is working

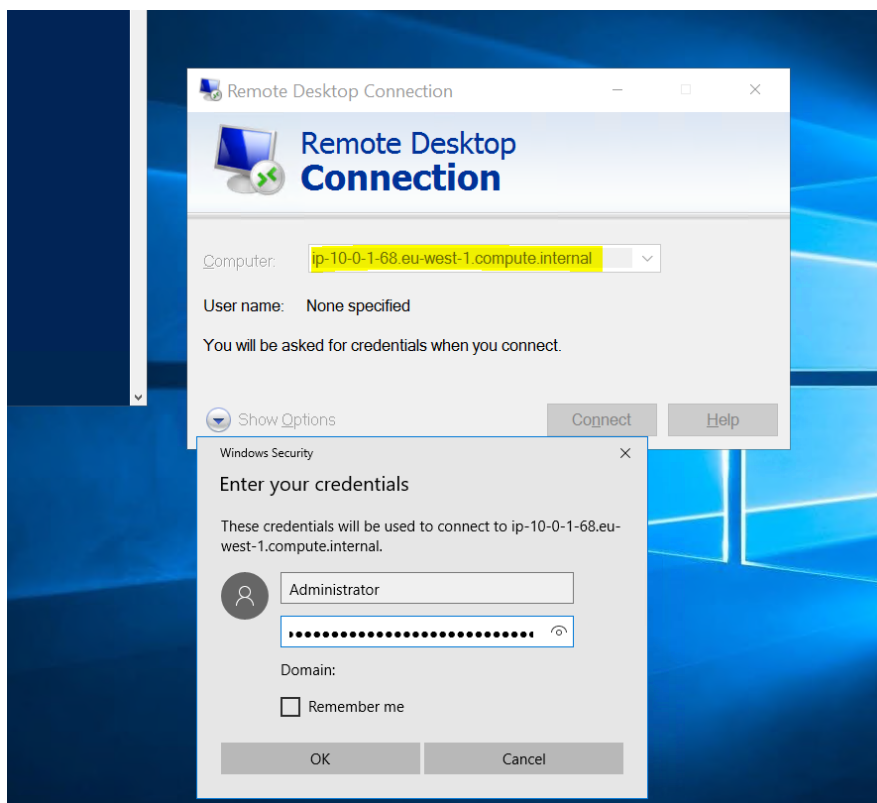
- **Connect to the Instance Windows Server Public**

Let's do the ping ...



... it is working

- **Launch instance in Private Subnet, from instance in public subnet**



Let's do the ping ...



It's not working.

This is expected.

Let's now create the NAT Gateway, in the Public Subnet, And edit the private Route Table to associate it to the NAT Gateway.

Create NAT Gateway

Create a NAT gateway and assign it an Elastic IP address. [Learn more](#)

Subnet subnet-c2f545a4

Elastic IP Allocation ID* eipalloc-7792e84a

Create New EIP

* Required

Create Route Table

Delete Route Table

Set As Main Table

Search Route Tables and their

<input type="checkbox"/>	Name	Route Table ID	Explicitly Associat	Main	VPC
<input type="checkbox"/>		rtb-3cca2845	0 Subnets	Yes	vpc-1d1dc17b
<input type="checkbox"/>		rtb-20c92b59	0 Subnets	Yes	vpc-d81cc0be RosettaHUB V
<input type="checkbox"/>	Public Route Table	rtb-663eae1f	1 Subnet	No	vpc-461d6e20 VPC Manu La
<input checked="" type="checkbox"/>	Private Route Table	rtb-7b27b702	1 Subnet	Yes	vpc-461d6e20 VPC Manu La

rtb-7b27b702 | Private Route Table

Summary

Routes

Subnet Associations

Route Propagation

Tags

Cancel

Save

View: All rules

Destination	Target	Status	Propagated	Remove
10.0.0.0/16	local	Active	No	
0.0.0.0/0		Active	No	

Add another route

igw-9995eeef

i-089e805fafc0fab32

nat-05ed0ee46d4f842b4

And now test again the ping ...

```

PS C:\Users\Administrator> ping google.com
Pinging google.com [216.58.211.174] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 216.58.211.174:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator> ping google.com
Pinging google.com [216.58.211.174] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 216.58.211.174:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\Administrator> ping google.com
Pinging google.com [209.85.202.102] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 209.85.202.102:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\Administrator> ping google.com
Pinging google.com [209.85.202.102] with 32 bytes of data:
Reply from 209.85.202.102: bytes=32 time=2ms TTL=40
Reply from 209.85.202.102: bytes=32 time=1ms TTL=40
Reply from 209.85.202.102: bytes=32 time=1ms TTL=40
Reply from 209.85.202.102: bytes=32 time=1ms TTL=40

Ping statistics for 209.85.202.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
PS C:\Users\Administrator>

```

... Magic, it is replying now 😊