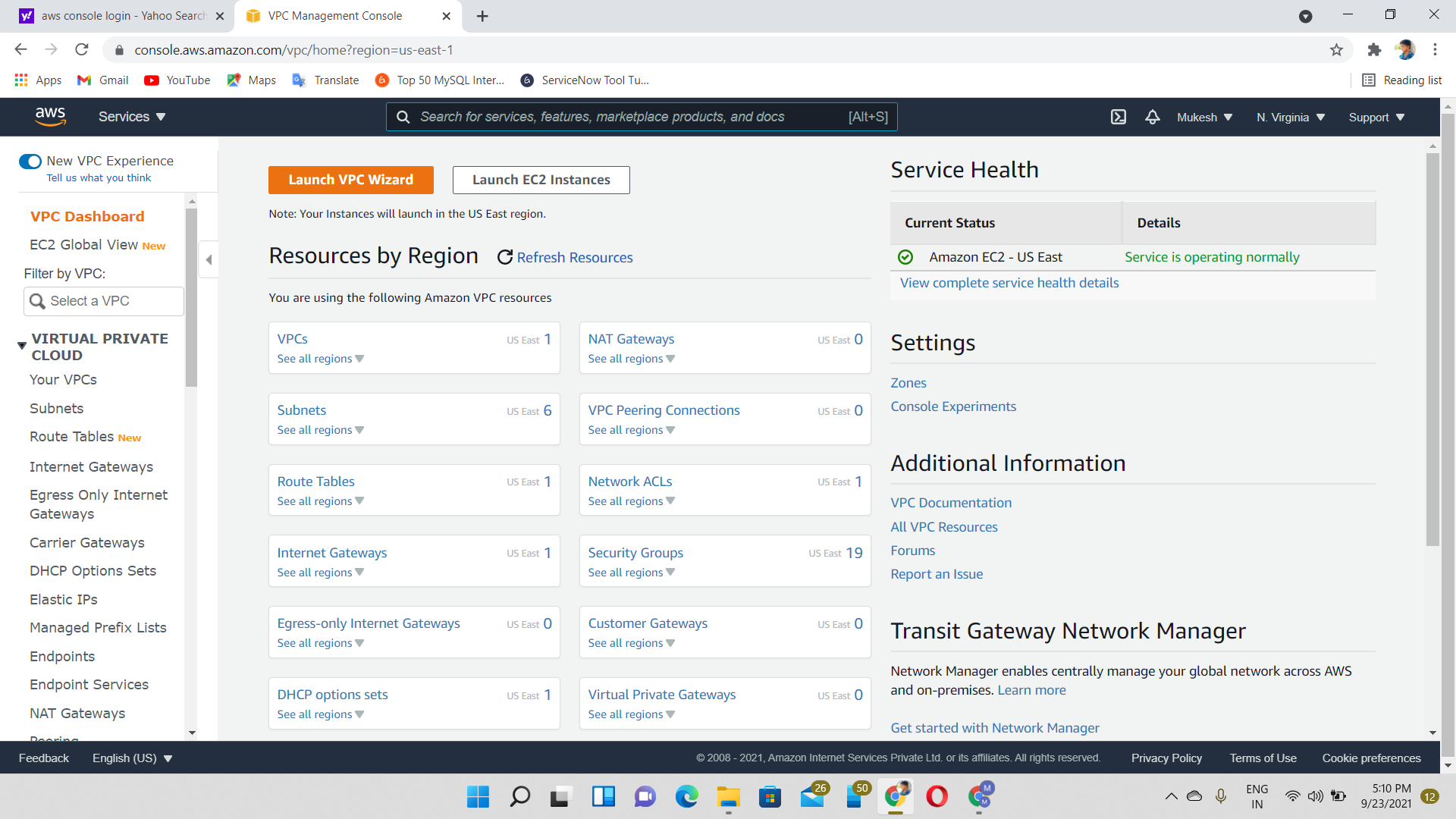
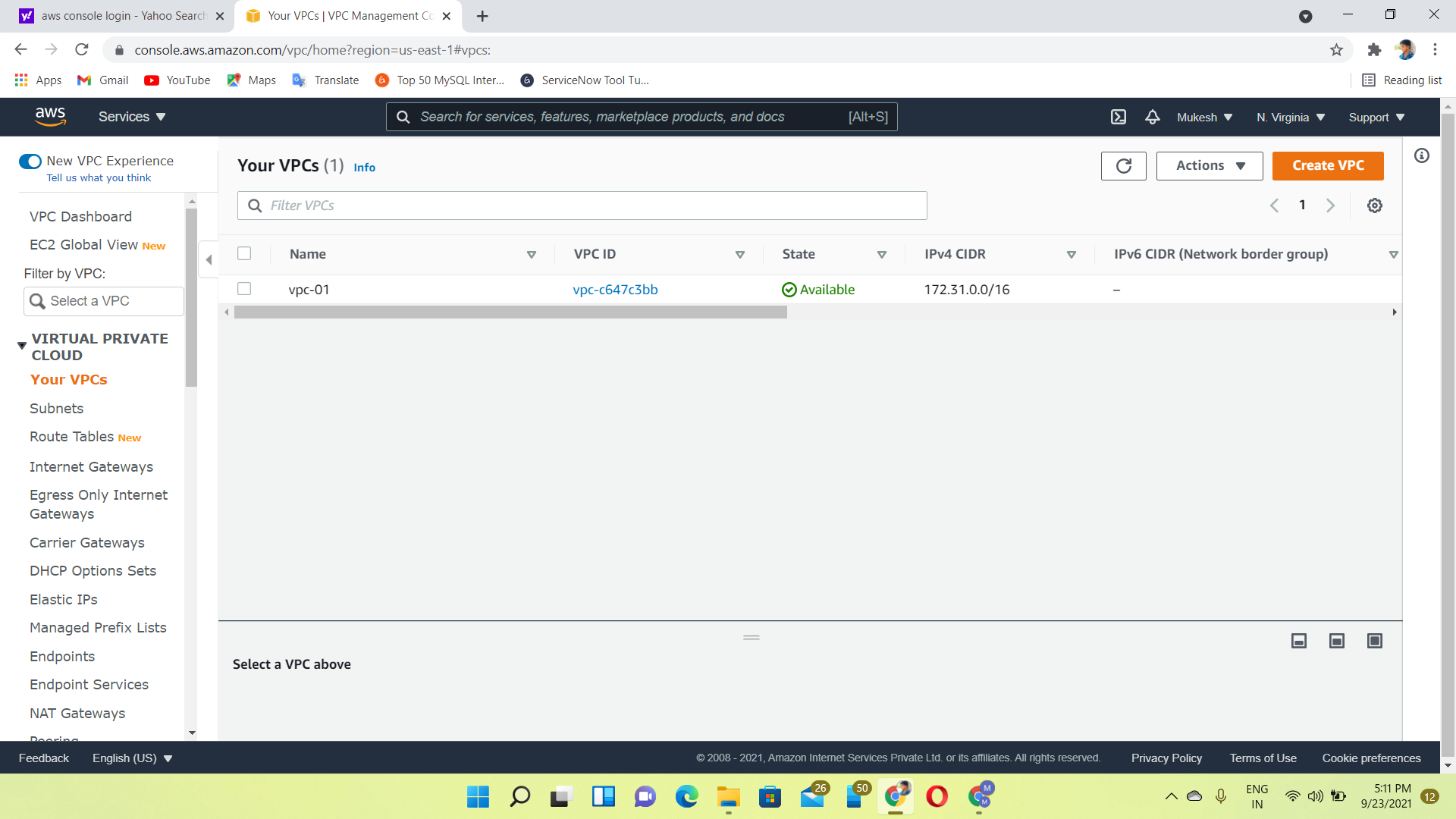
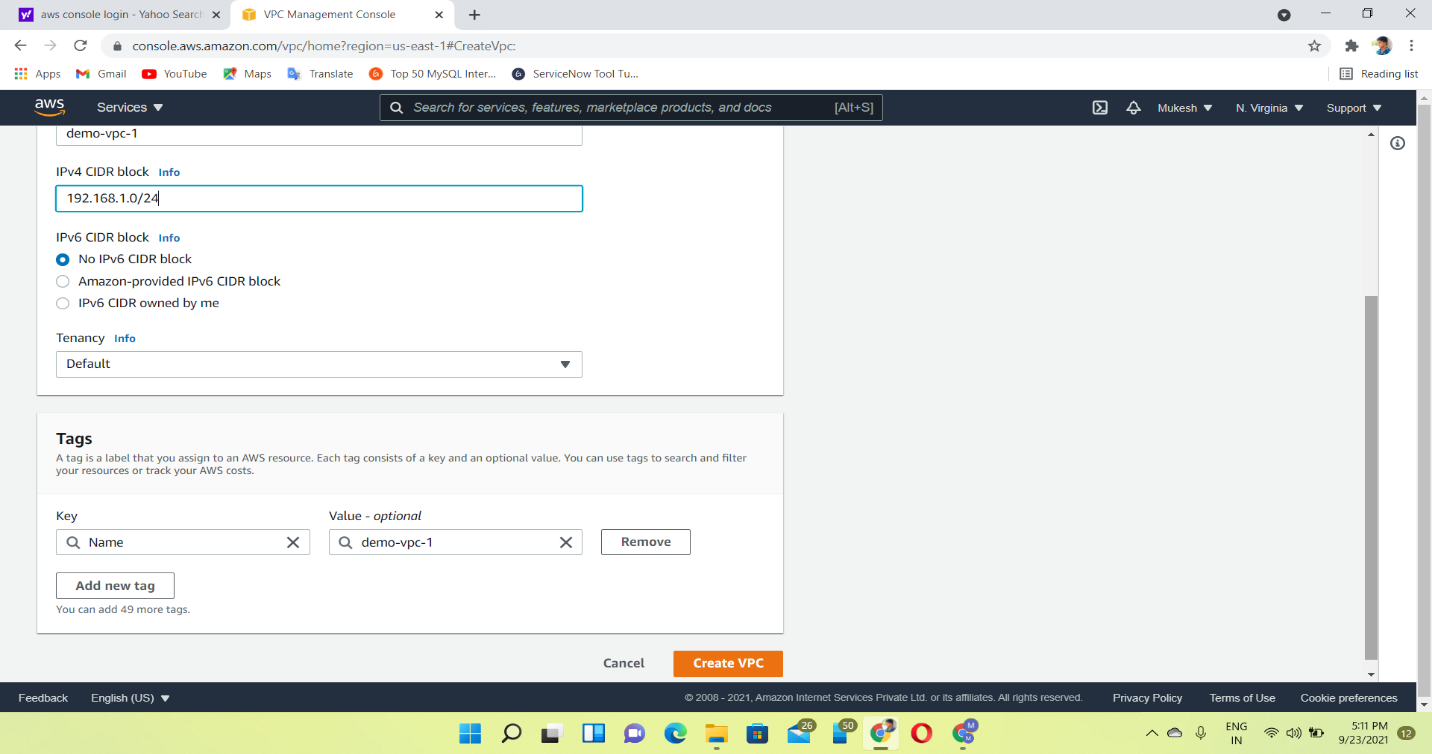
**VPC:**

**Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.**

Step 1🡪click VPC



Step2🡪create demo-VPC-1 in 192.168.1.0/24



**SUBNET🡪dividing an n/w into two (or) more n/w is called sub netting. AWS provides two types of subnetting.one is public, which allows the internet to access the machine & another one is private, which hidden from the internet.**

**Magic Number:**

The magic number is the number of IP addresses in each subnet if and only if the number of bits for the network id and the magic number tells us how to find our networks.

Types:

Case 1

Case 2

Case 3

**Case 1** Condition:

If X < 8 leave the first Bit number as it is,

Formula Second Bit number as it is,

Magic number = (2^X) Third Bit number as it is,

Fourth Bit number = Add magic number

**Case 2**

If X = 8, X > 8, X < 16

Formula

Magic number = (2^X) / (2^8)

**Condition**:

Leave the first Bit number as it is,

Second Bit number as it is,

Third Bit number = Add magic Number,

Fourth Bit number = 0

**Case 3**

If X = 16, X > 16, X < 24

Formula

Magic number = (2^X) / (2^16)

**Condition:**

Leave the first Bit number as it is,

Second Bit number = Add magic Number,

Third Bit number = 0,

Fourth Bit number = 0

**Calculation (Example)**

Network ID = 192.168.1.0/24

Required Number of hosts/subnets=50

**Formula**:

Number of subnets = 2^n

Number of hosts/subnets=2^x-2

n=1 n=2 n-3 n=4 n=5 n=6

2^1=2=2<50 2^2=4<50 2^3=8<50 2^4=16<50 2^5=32<50 2^6=64>50

So, borrow 6 bits from host part to provide 64 subnets.

We calculate subnet masks

Default subnet mask of class C = 255.255.255.0

Then, convert to binary form of host bits only.

=255.255.255.(0.0.0.0.0.0.0.0)

=255.255.255.(1.1.1.1.1.1.0.0)

=255.255.255.252 where, n is a number of bits borrowed

n=6 x is a number of 0's left after borrowing

x=2 and also it means CIDR=32-2=30

So, we can use case 1 because, X<8

MN=2^x=2^2=4

Subnet is,

1->192.168.1.0/30 First IP -192.168.1.1, Last IP-192.168.1.2, Broadcast IP - 192.168.1.3

2->192.168.1.4/30

3->192.168.1.8/30

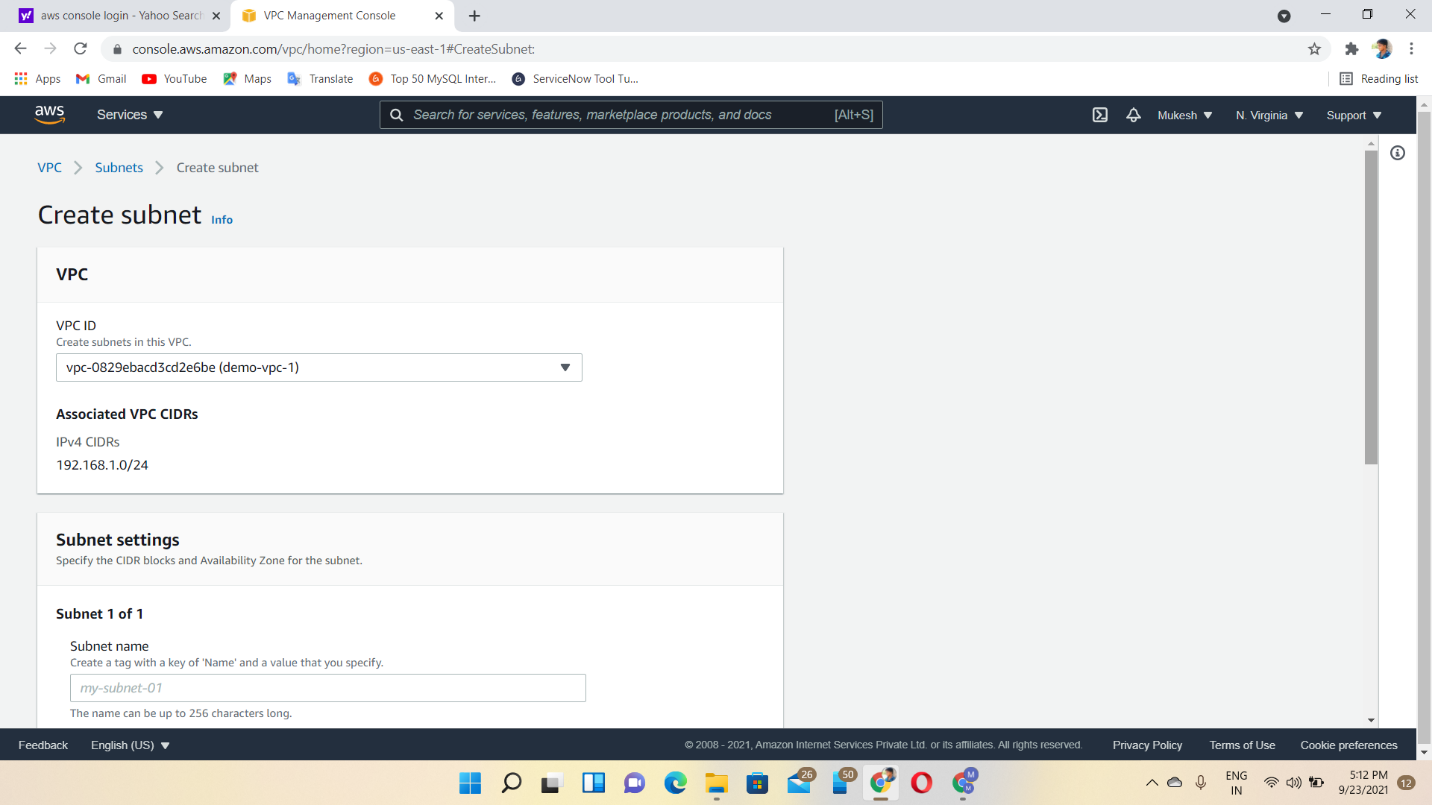
4->192.168.1.12/30

.

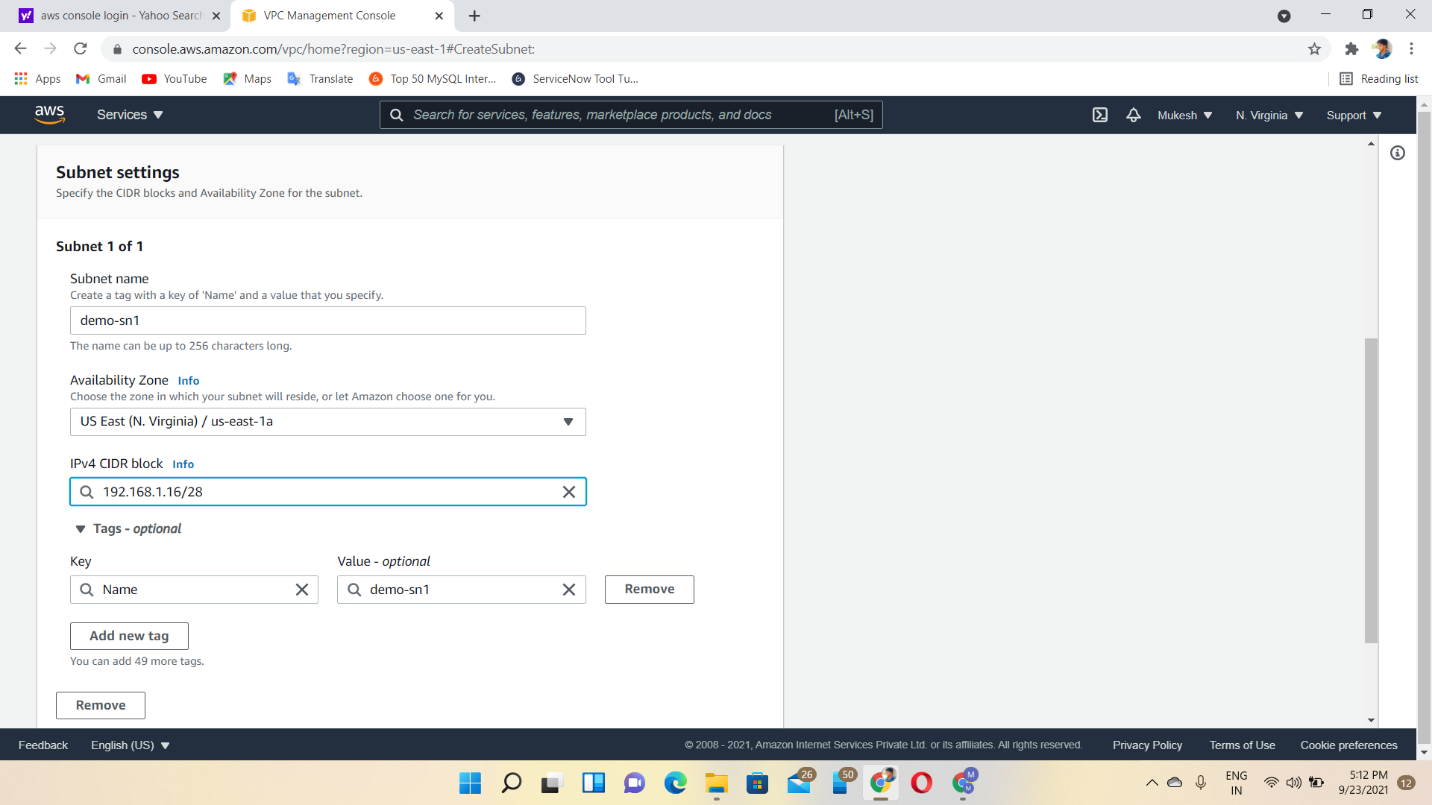
.

192.168.1.252/30

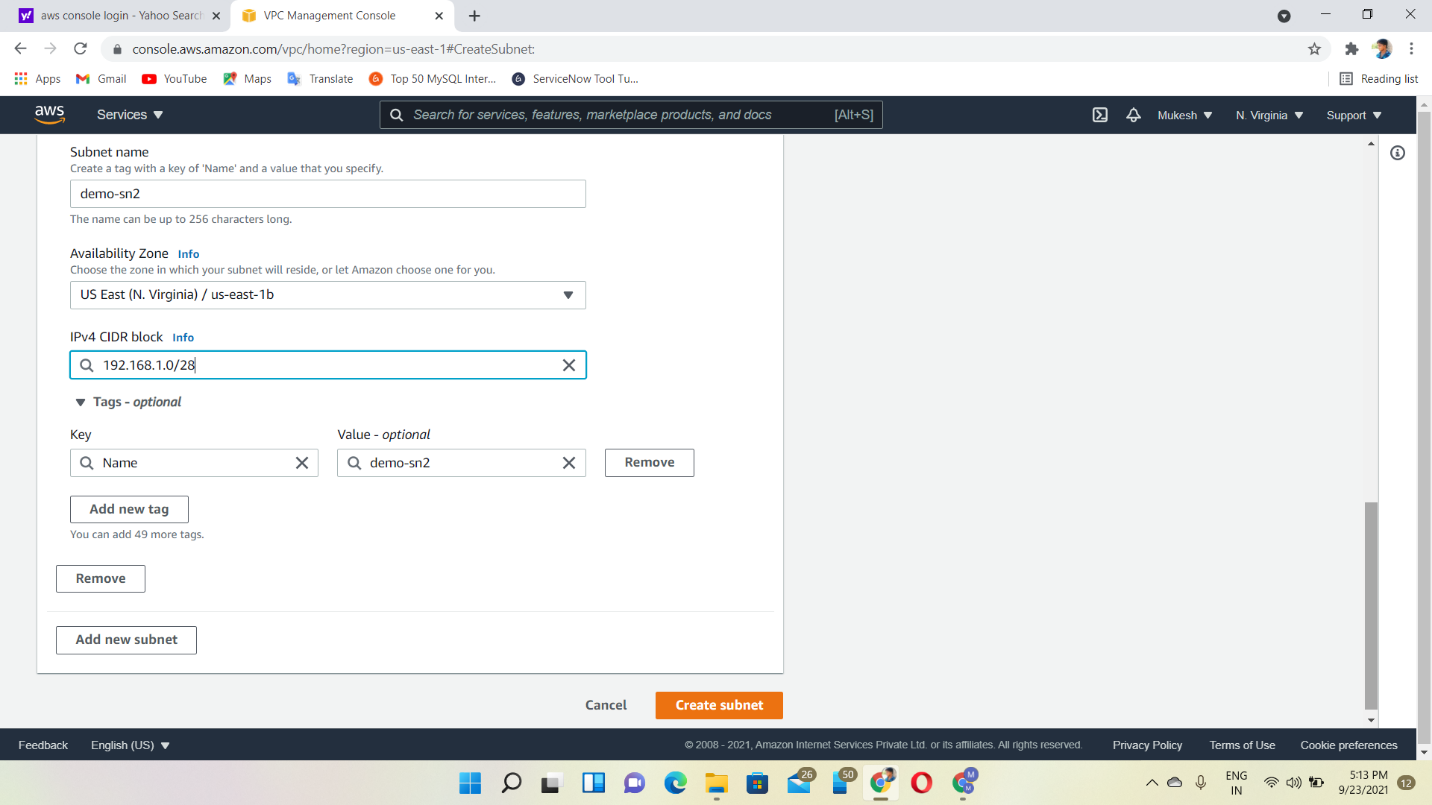
Step3🡪Choose the VPC



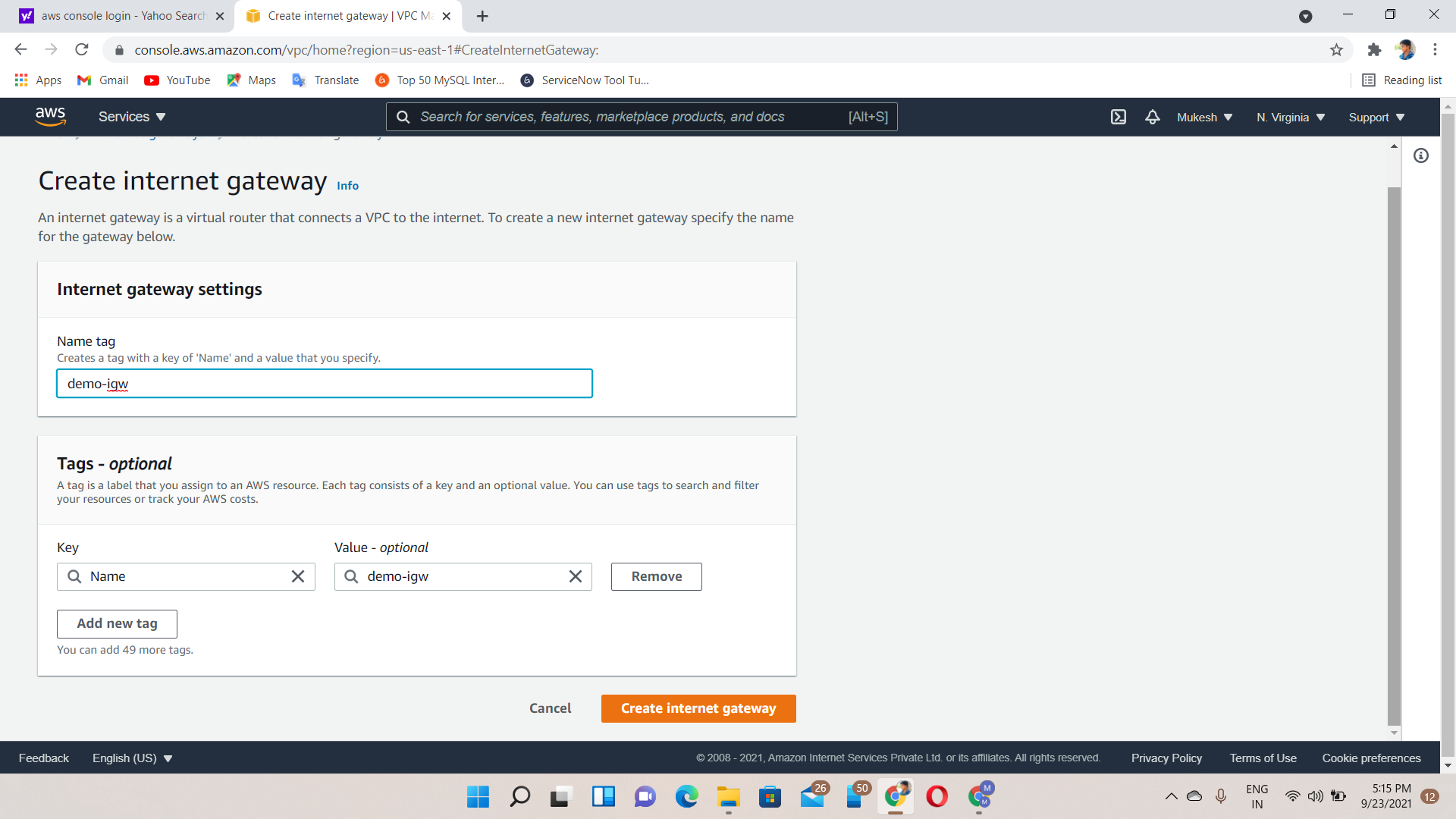
Step4🡪 Create subnet 1



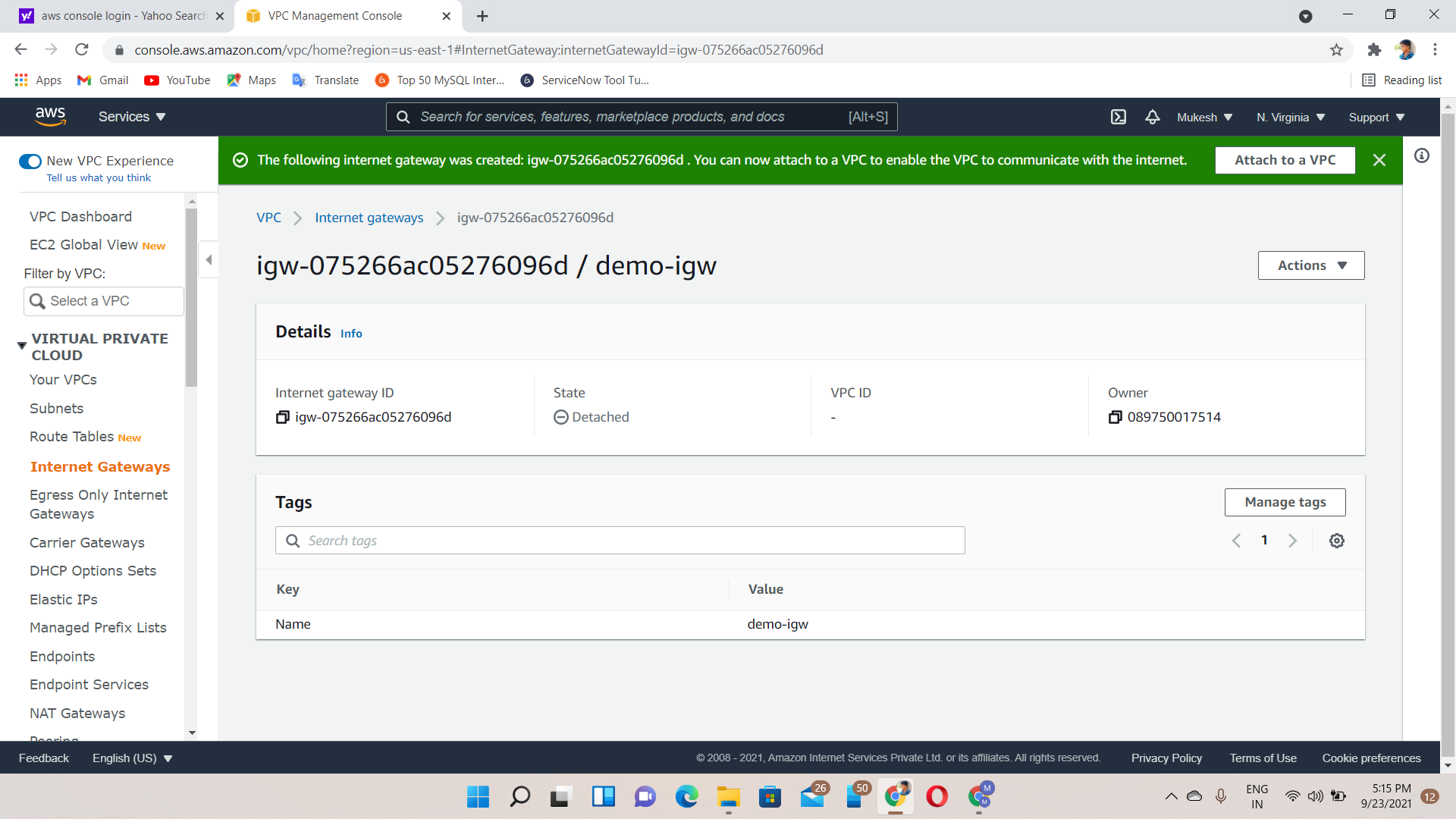
Step5🡪Create subnet 2



Internet Gateway🡪it is used to allow resources in our VPC to access internet.

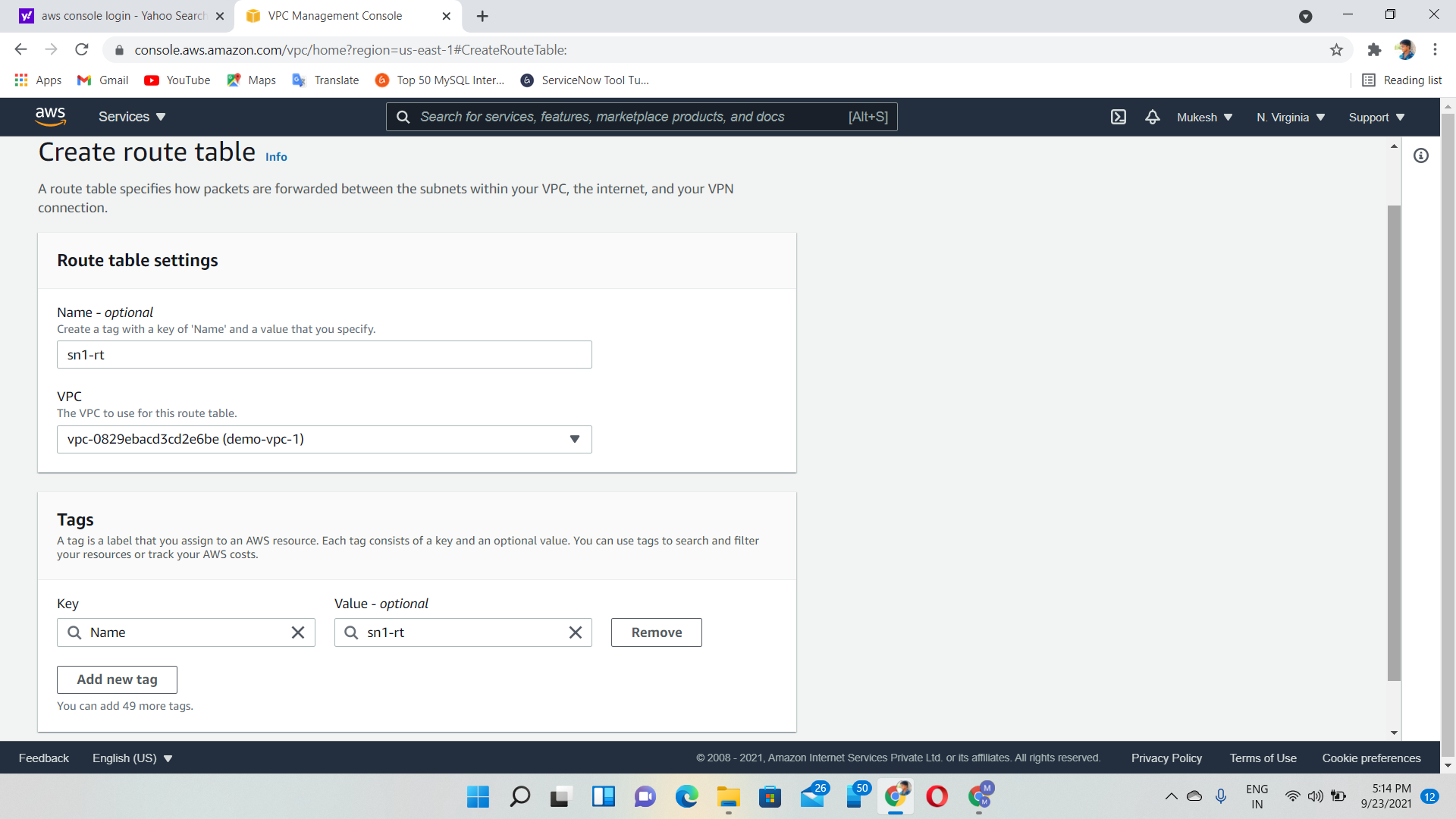
Step6🡪create internet gateway

Step7🡪attach to VPC

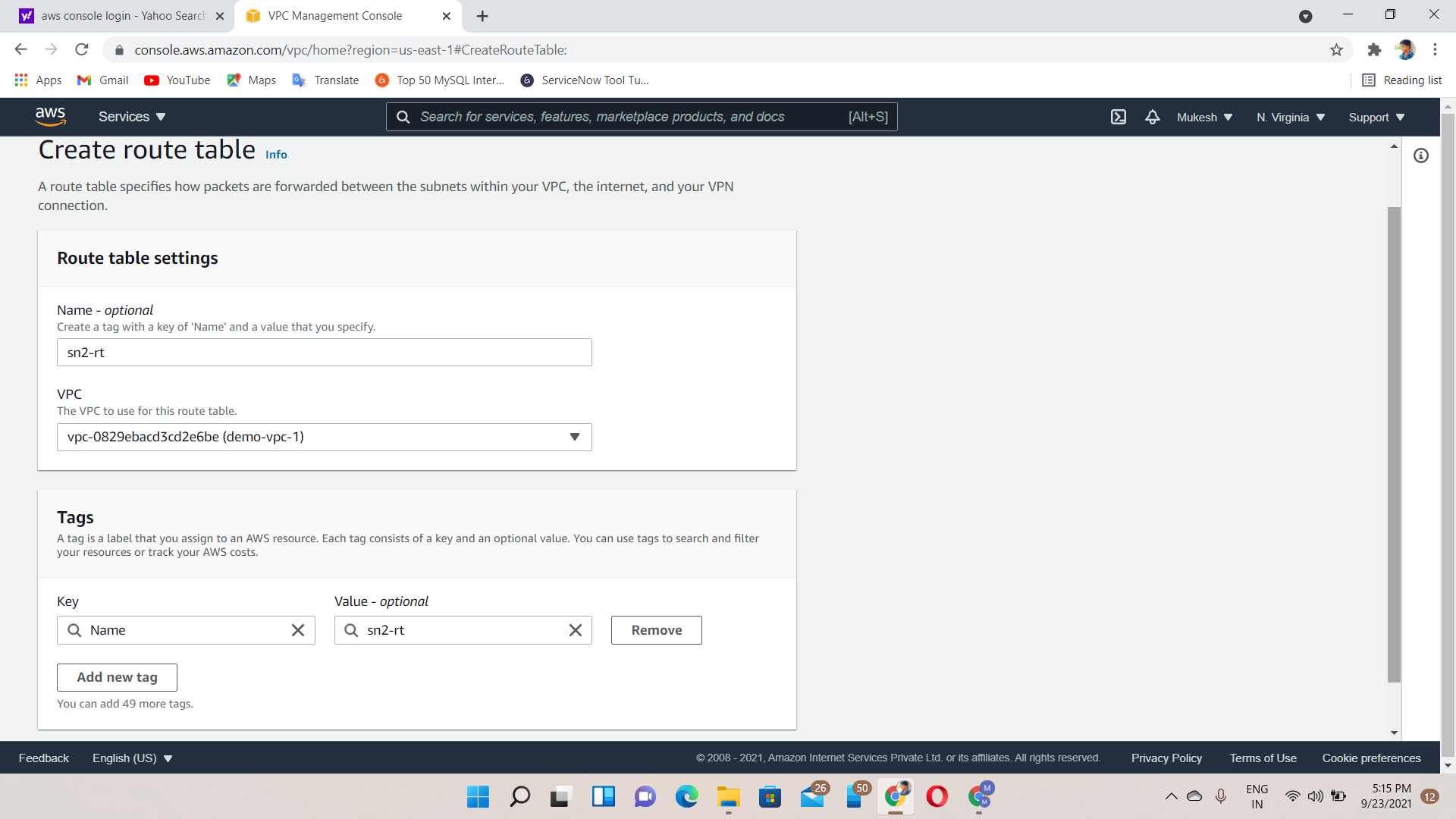


Route Table🡪it used to N/W packets which way they need to go to their destination.

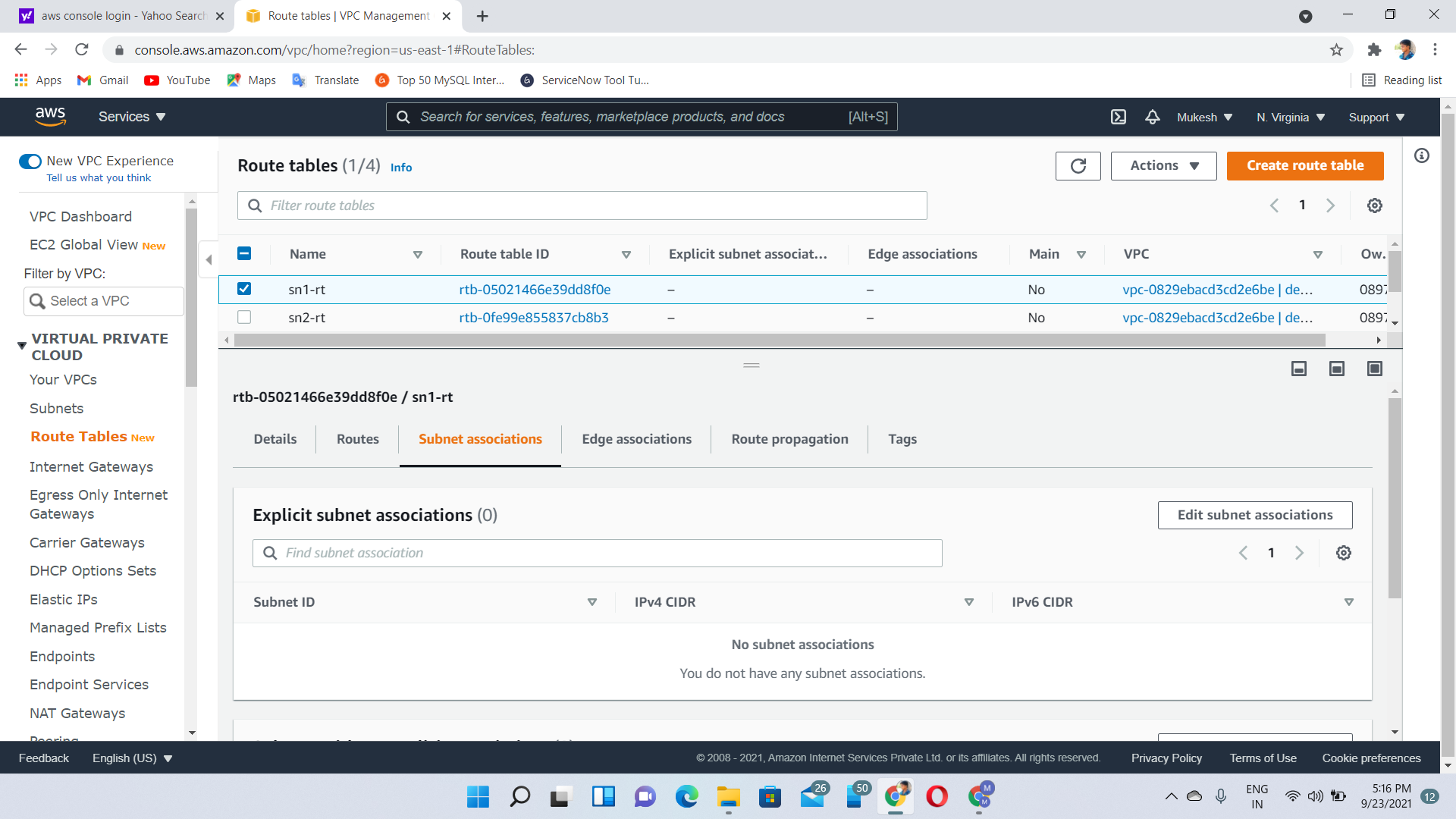
Step8🡪create Route table 1 for SN1

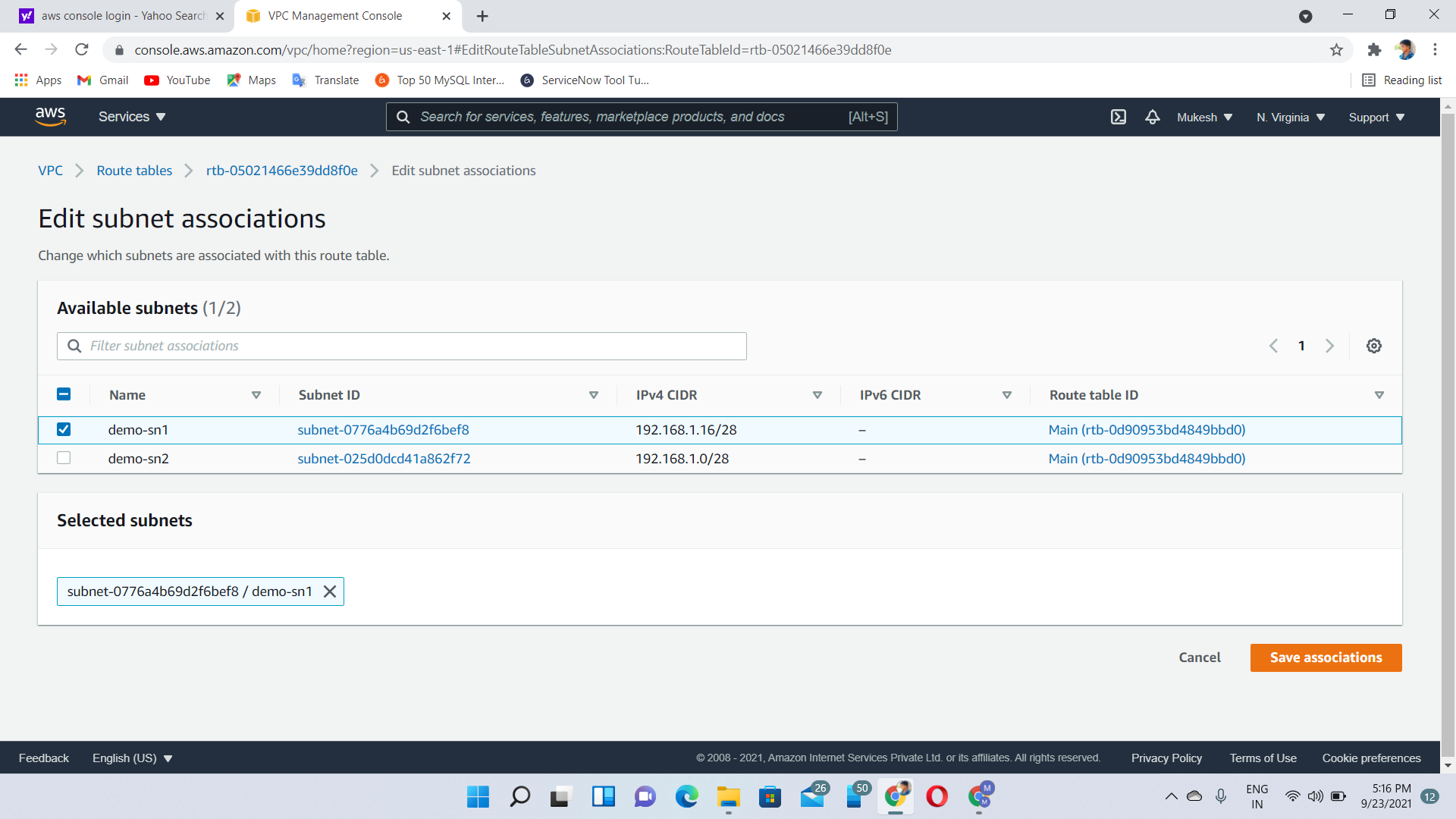


Step9🡪create Route Table for SN2

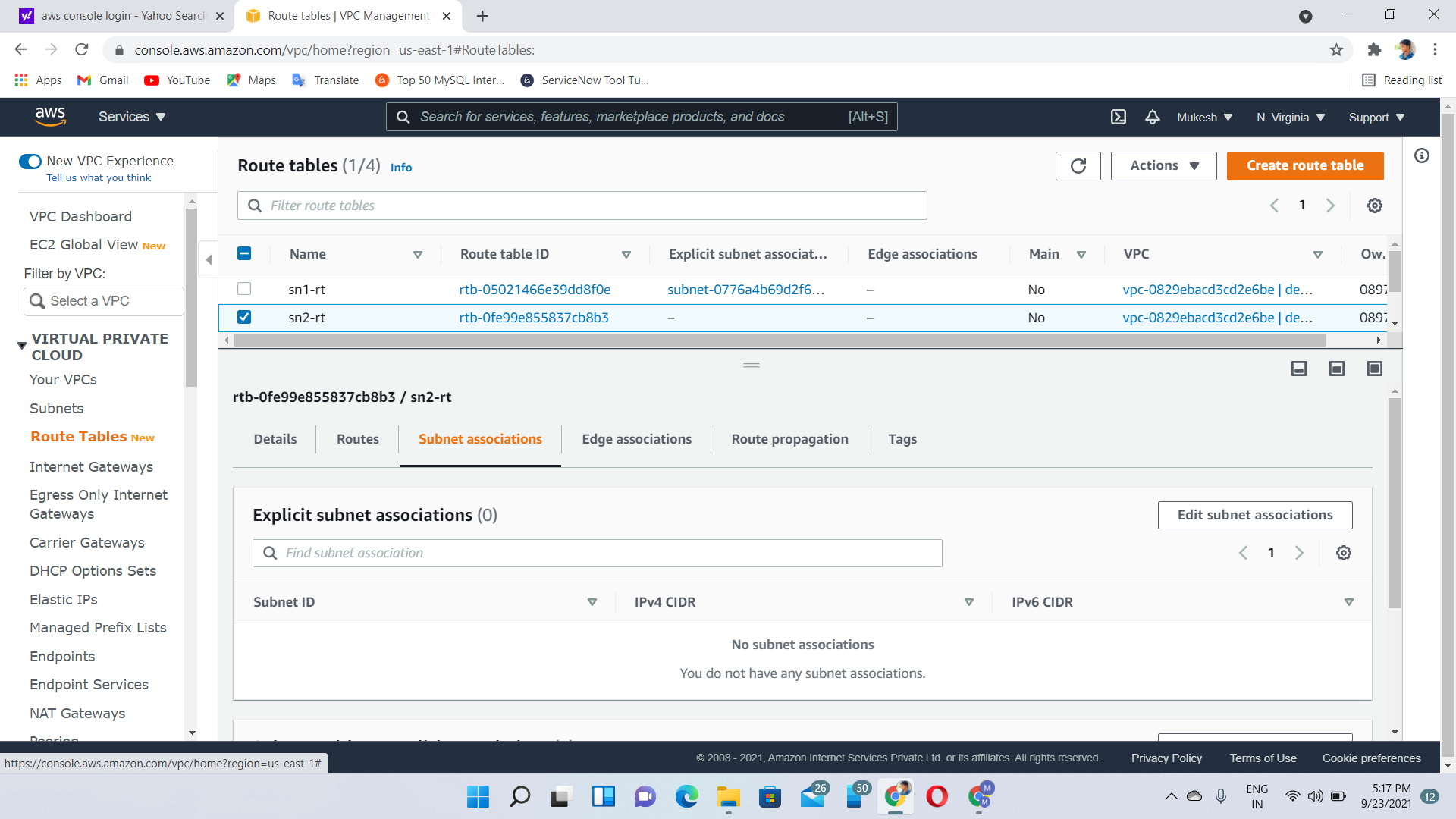


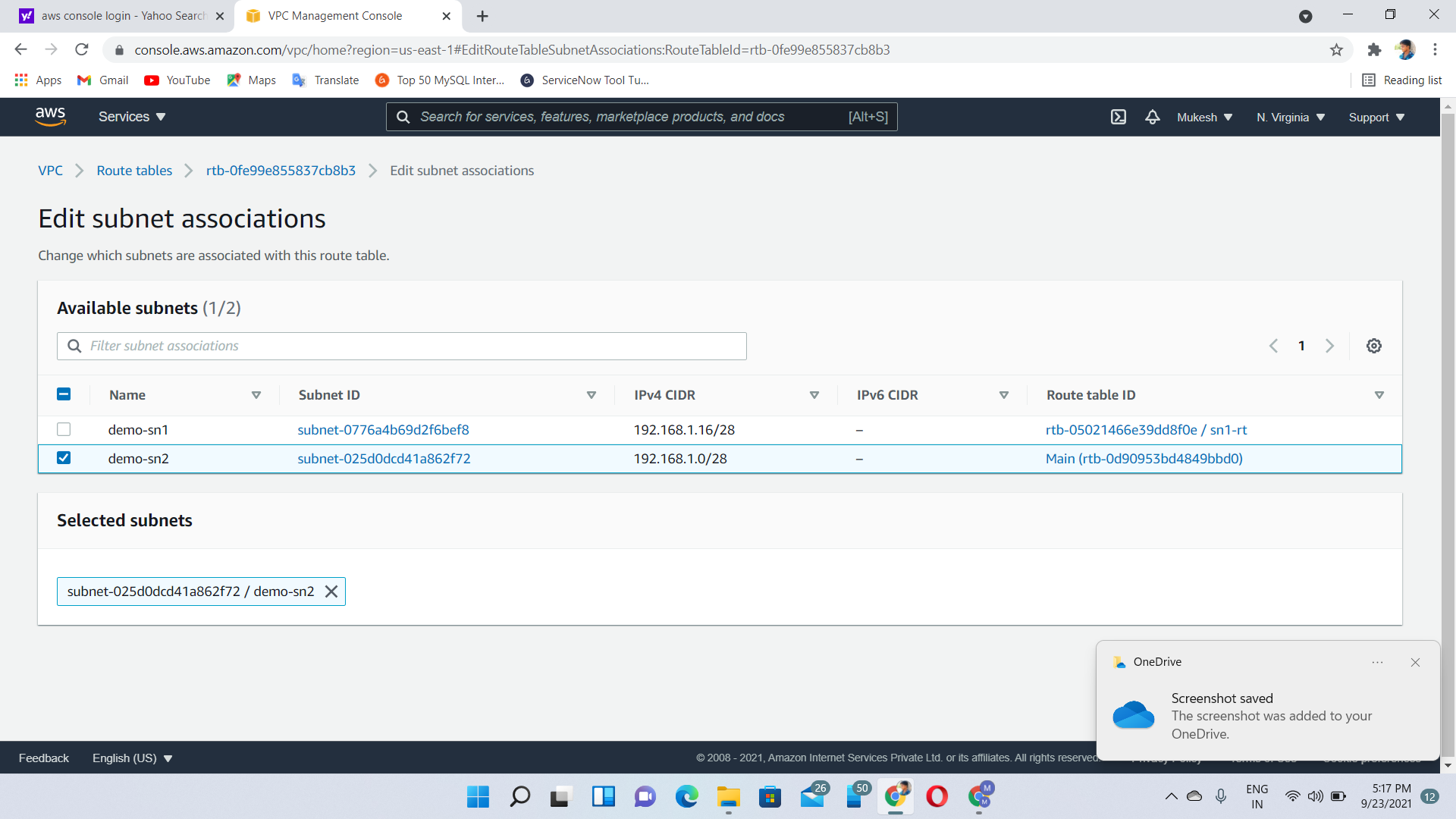
Step10🡪SN1-subnet Association



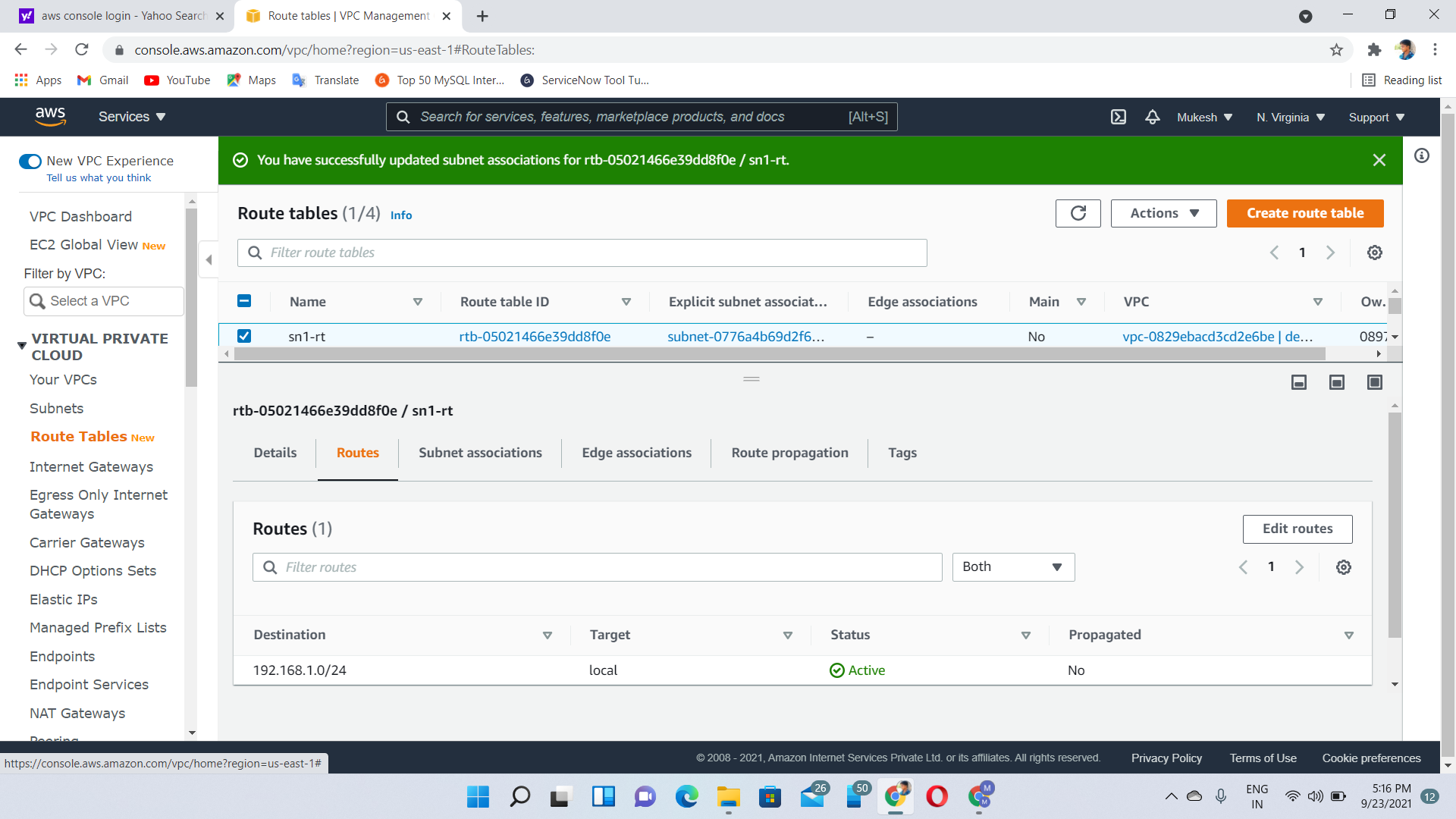


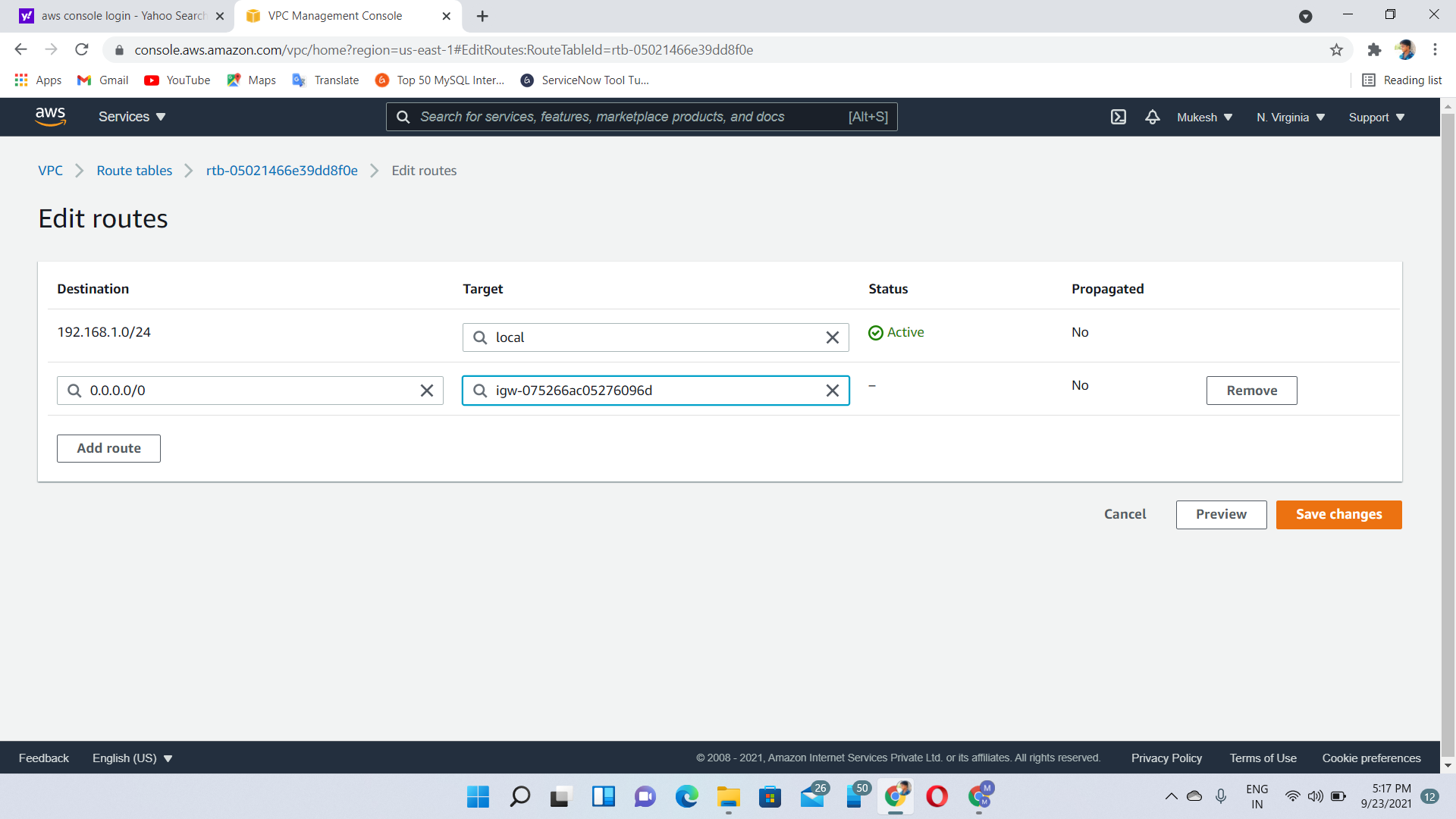
Step11🡪SN2-Subnet Association





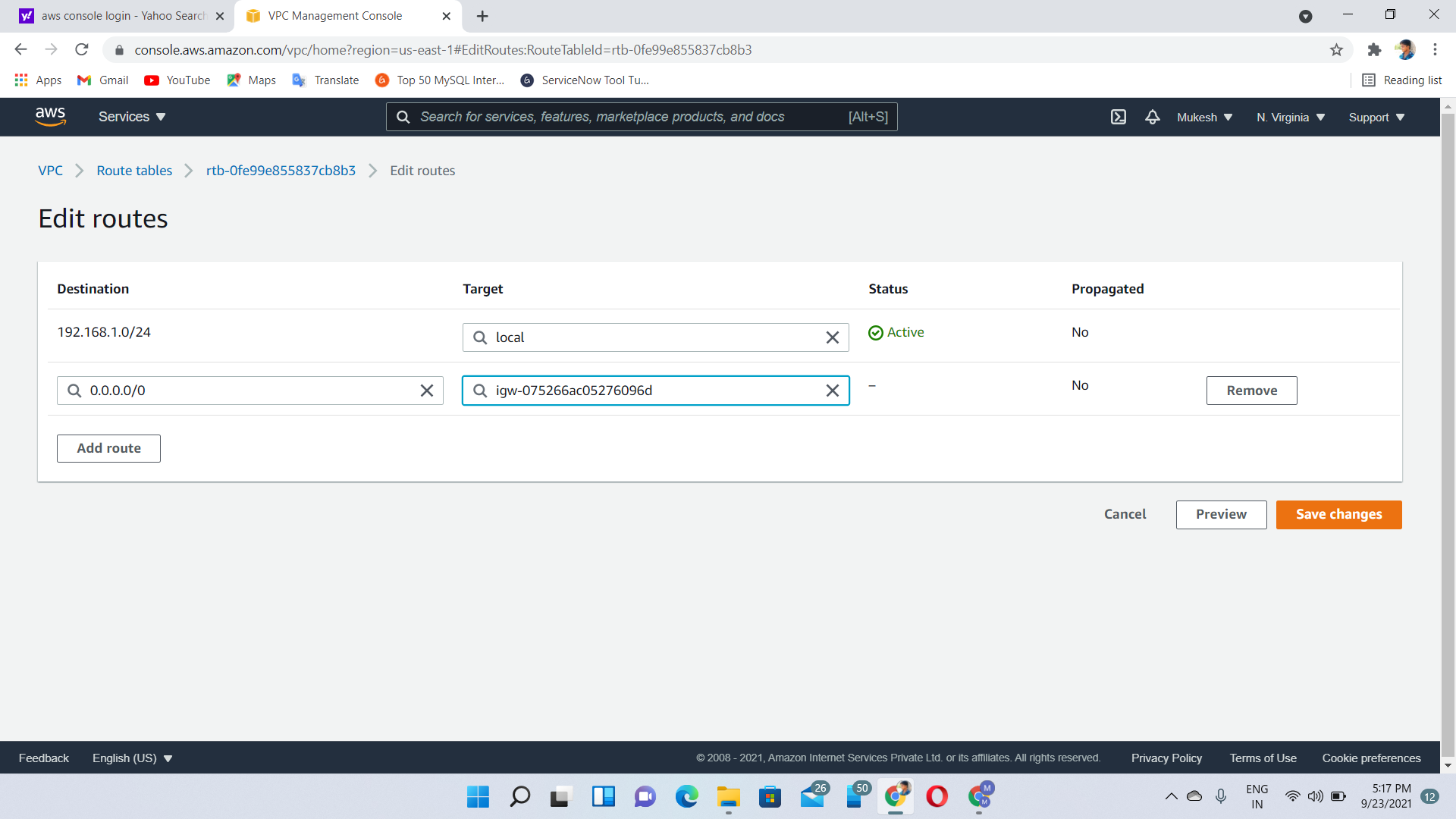
Step12🡪SN1-Edit Routes





Step13🡪SN2-Edit Routes





**Nacl**:

* NACL stands for Network Access Control Lists.
* It is a security layer for your VPC that controls the traffic in and out of one or more subnets.
* It is an optional layer for your VPC.
* You can set up a Network ACL similar to the security group that adds an additional layer of security to your VPC.
* A Network ACL contains numbered lists of rules that are evaluated in order, starting from the lowest numbered rule, to determine whether the traffic goes in or out of the subnet associated with the Network ACL. The highest numbered rule can be 32766. It is recommended to create new rules with increments (For example, increments of 10 or 100) so that you can easily add new rules where you need later on.

**Network ACL Components**

The following are the components of a Network ACL:

**Rule number**: Rule number is a number associated with every rule. Rules are evaluated starting with the lowest-numbered rule. As soon as the rule matches traffic, the rule is applied regardless of whether the highest-numbered rule contradicts to it.

**Protocol**: You can specify any protocol that has a standard protocol number. For example, Http, Https, ICMP, SSH, etc.

**Inbound rules**: It specifies the source of the traffic and the destination port.

**Outbound rules**: It specifies the destination traffic and destination port.