

Bring Your Own IP Address to the Cloud

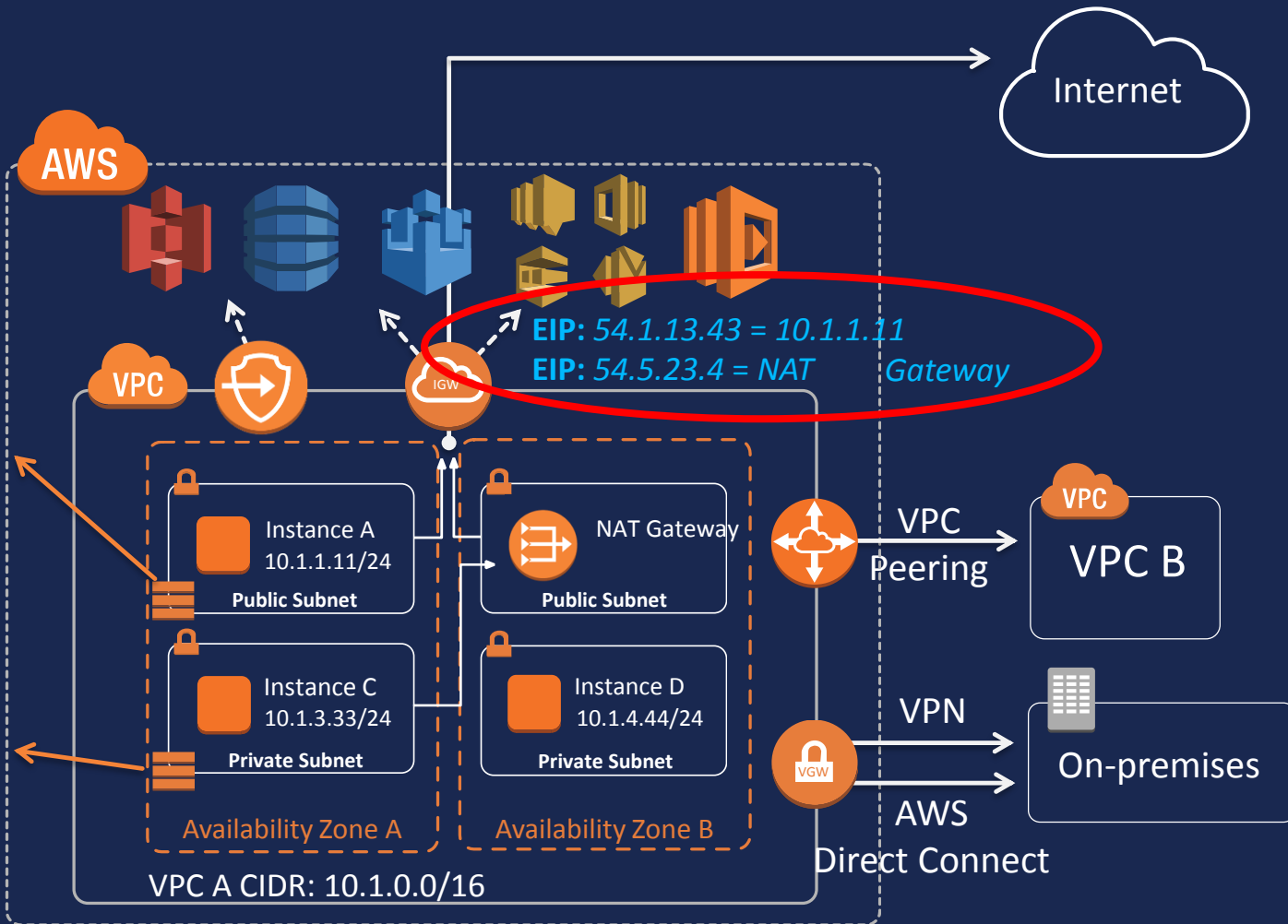
Anupam Pandey - *Sr Product Manager, Amazon Web Services*

Matt Lehwess - *Principal Solutions Architect, Amazon Web Services*

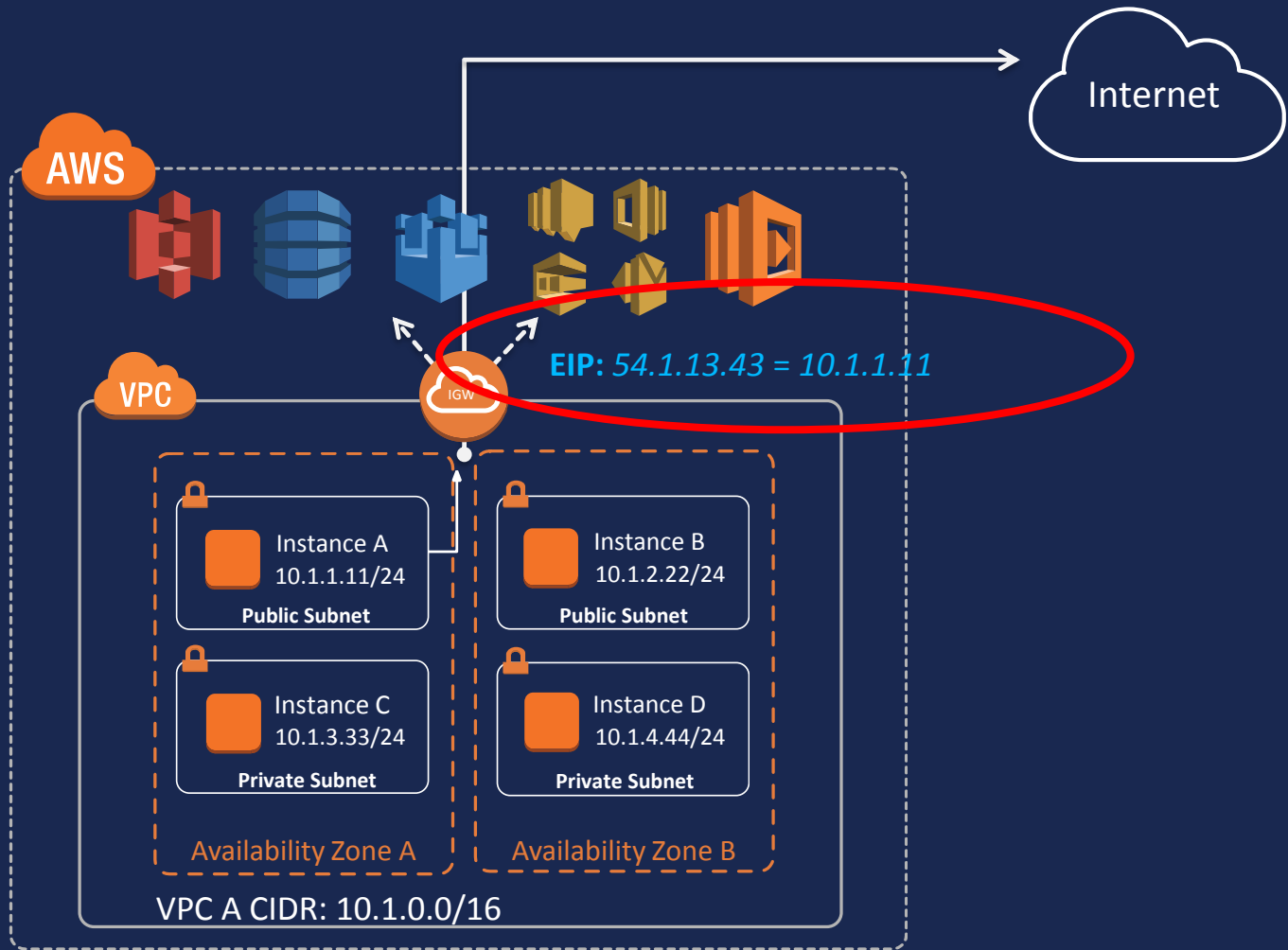
VPC foundations

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	IGW
S3.prefix.list	VPCE-123
On-prem	VGW
VPC-B	PCX-123

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	NAT-GW
S3.prefix.list	VPCE-123
On-prem	VGW
VPC-B	PCX-123



What is an Elastic IP?

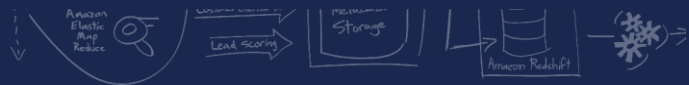




Your IP address is
not just a number



Amazon
Elastic
Map
Reduce
Running On



Your IP address is
not just a number



Amazon
Elastic
Map
Reduce
Running On



Bring your own IP

EASILY MIGRATE TO AWS WITH YOUR PUBLIC ipv4 ADDRESSES

Keep your IP address reputation

Avoid changes to IP address whitelists

Move legacy applications with no need to change IP addresses

**Why would you want to
bring your own IP? (BYOIP)**

IP reputation

Your IP reputation is how you are perceived on the public internet

Whitelisting

Tell your friends who you are at an IP level, and know this doesn't need to change

Migration

Avoid IP address changes to applications when you migrate to the AWS Cloud

Redundancy

Hot standby for your on-premises

This is great!

Let's talk about the process

What do I need to start?

The address range must be registered with your regional internet registry (RIR).

Supported RIRs include the **American Registry for Internet Numbers (ARIN)** and **RIPE**.

Preparing you IP range:

Authorization

1. Create an **ROA** to authorize Amazon ASNs 16509 and 14618 to advertise your address range.

What is a **Route Origin Authorization**?

“A ROA is a cryptographically signed object that states which Autonomous System (AS) is authorized to originate a particular IP address prefix or set of prefixes. ROAs may only be generated for Internet number resources covered by your resource certificate.” - ARIN

Where can I get a ROA?

ARIN:

<https://www.arin.net/resources/rpki/roarequest.html>

RIPE:

<https://www.ripe.net/manage-ips-and-asns/resource-management/certification/resource-certification-roa-management>

Preparing you IP range:

Authorization

1. Create an **ROA** to authorize Amazon ASNs 16509 and 14618 to advertise your address range.

Preparing your IP range:

Authentication

2. Generate an RSA 2048-bit key pair

```
openssl genrsa -out private.key 2048
```

Preparing you IP range:

Authentication

3. Create a public X509 certificate from the key pair using the following command

```
openssl req -new -x509 -key private.key -days 365 | tr -d "\n" > publickey.cer
```

Preparing you IP range:

Authentication

4. Create a signed message. The format of the message is as follows:

```
1|aws|account|cidr|YYYYMMDD|SHA256|RSAPSS
```

1

2

3

4

5

6

7

1 | aws | account | cidr | YYYYMMDD | SHA256 | RSAPSS

1

Version – Should always be 1

2

AWS Partition. *Valid values* – aws, aws-cn, aws-iso, aws-iso-b, aws-us-gov

3

12-digit AWS Account Number

4

CIDR being brought – should follow standard CIDR notation

5

Expiration date in ISO 8601 format (YYYYMMDD). The signature will no longer be valid after this date 00:00:00 UTC.

6

Hashing algorithm, Must be SHA256. (Might support more in the future)

7

RSAPSS (Might support more in the future)

Preparing you IP range:

Authentication

4. (Continued). The following command signs the message using the key pair you created and saves it as `base64_urlsafesignature`:

```
echo "1|aws|123456789012|198.51.100.0/24|20191201|SHA256|RSAPSS" | tr -d "\n" | openssl dgst -sha256 -sigopt rsa_padding_mode:pss -sigopt rsa_pss_saltlen:-1 -sign private.key -keyform PEM | openssl base64 | tr --'+=/' '-_~' | tr -d "\n" > base64_urlsafesignature
```


Preparing you IP range:

Authentication

5. Update the RDAP record for your RIR with the X509 certificate.

Be sure to copy the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----
from the certificate.

Preparing you IP range:

Authentication

To view your certificate, run the following command:

```
cat publickey.cer
```

For ARIN, add the certificate in the "Public Comments" section for your address range.

For RIPE, add the certificate as a new "desc" field for your address range.

Provisioning your IP Range

Where the rubber hits the road...

Provisioning your IP Range

Provisioning with `provision_byoip_cidr`

```
mlehwiss — -bash — 121x25

prompt$
prompt$ aws ec2 provision-byoip-cidr --region us-west-2
--cidr 130.137.24.0/23 --description "range for prod"
--cidr-authorization-context Message="1 | aws | <account>
| 130.137.24.0/23 | 20201231 | SHA256",Signature="<signature>"
{
  "ByoipCidr": {
    "Cidr": "130.137.24.0/23",
    "Description": "range for prod",
    "State": "pending-provision"
  }
}
prompt$ clear
```



Provisioning your IP Range

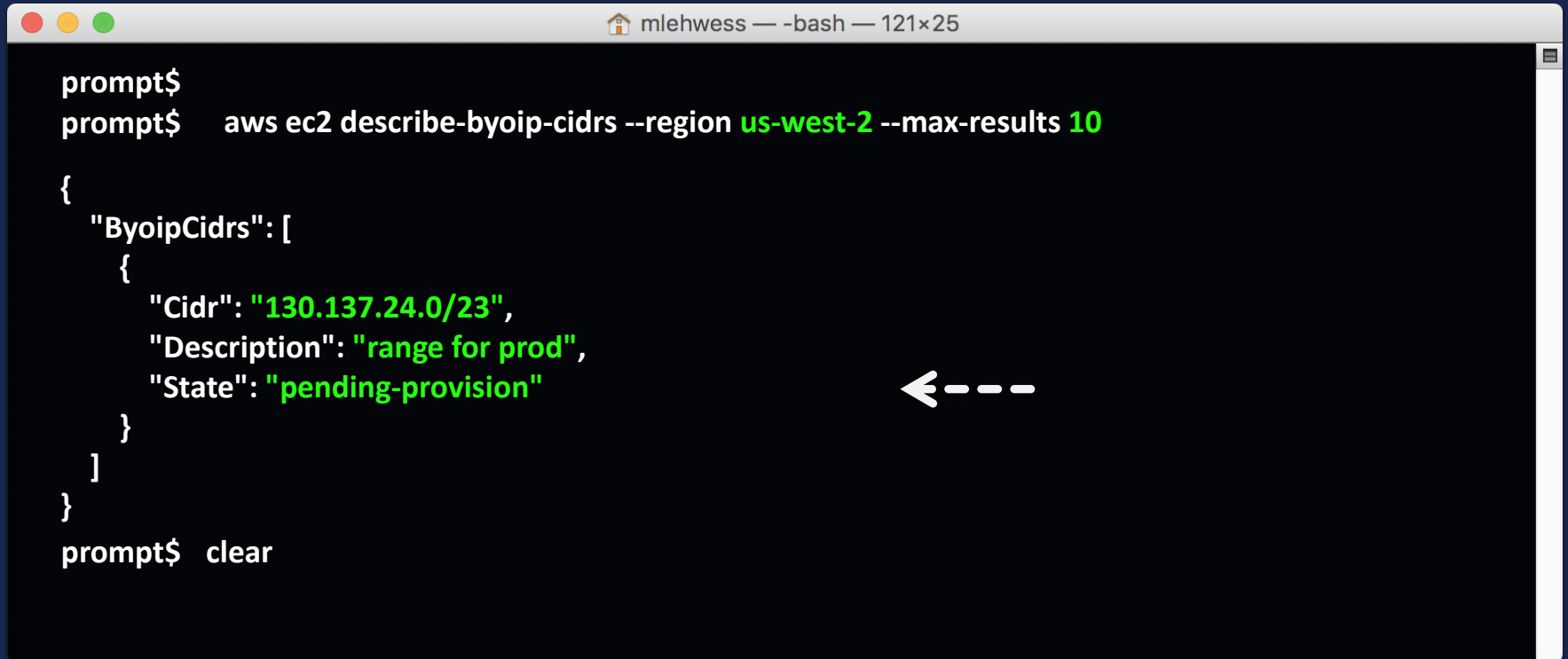
Monitoring status using `describe-byoip-cidrs`

```
mlehwiss — -bash — 121x25

prompt$
prompt$ aws ec2 describe-byoip-cidrs --region us-west-2 --max-results 10

{
  "ByoipCidrs": [
    {
      "Cidr": "130.137.24.0/23",
      "Description": "range for prod",
      "State": "pending-provision"
    }
  ]
}

prompt$ clear
```

A terminal window with a dark background and light text. The window title bar shows 'mlehwiss — -bash — 121x25'. The terminal content shows a shell prompt 'prompt\$' followed by the command 'aws ec2 describe-byoip-cidrs --region us-west-2 --max-results 10'. The output is a JSON object with a 'ByoipCidrs' array containing one object with fields 'Cidr', 'Description', and 'State'. The 'State' value is 'pending-provision'. A dashed arrow points from the right towards the 'pending-provision' text.

Provisioning your IP Range

Monitoring status using `describe-byoip-cidrs`

... sometime later

```
mlehwess — -bash — 121x25

prompt$
prompt$ aws ec2 describe-byoip-cidrs --region us-west-2 --max-results 10

{
  "ByoipCidrs": [
    {
      "Cidr": "130.137.24.0/23",
      "Description": "range for prod",
      "StatusMessage": "Cidr successfully provisioned into Ipv4Pool: ipv4pool-ec2-
0588c9b75a25d1a02", ← ---
      "State": "provisioned"
    }
  ]
}
prompt$ clear
```

Provisioning has completed

Advertising your IP Range

Advertisement of the address range by Amazon

```
mlehwess — -bash — 121x25

prompt$
prompt$  aws ec2 advertise-byoip-cidr --region us-west-2
--cidr 130.137.24.0/23
{
  "ByoipCidr": {
    "Cidr": "130.137.24.0/23",
    "Description": "range for prod",
    "State": "advertised"
  }
}
prompt$  clear
```

←---

The prefix/CIDR is now advertised by Amazon

Creating an Amazon Elastic IP

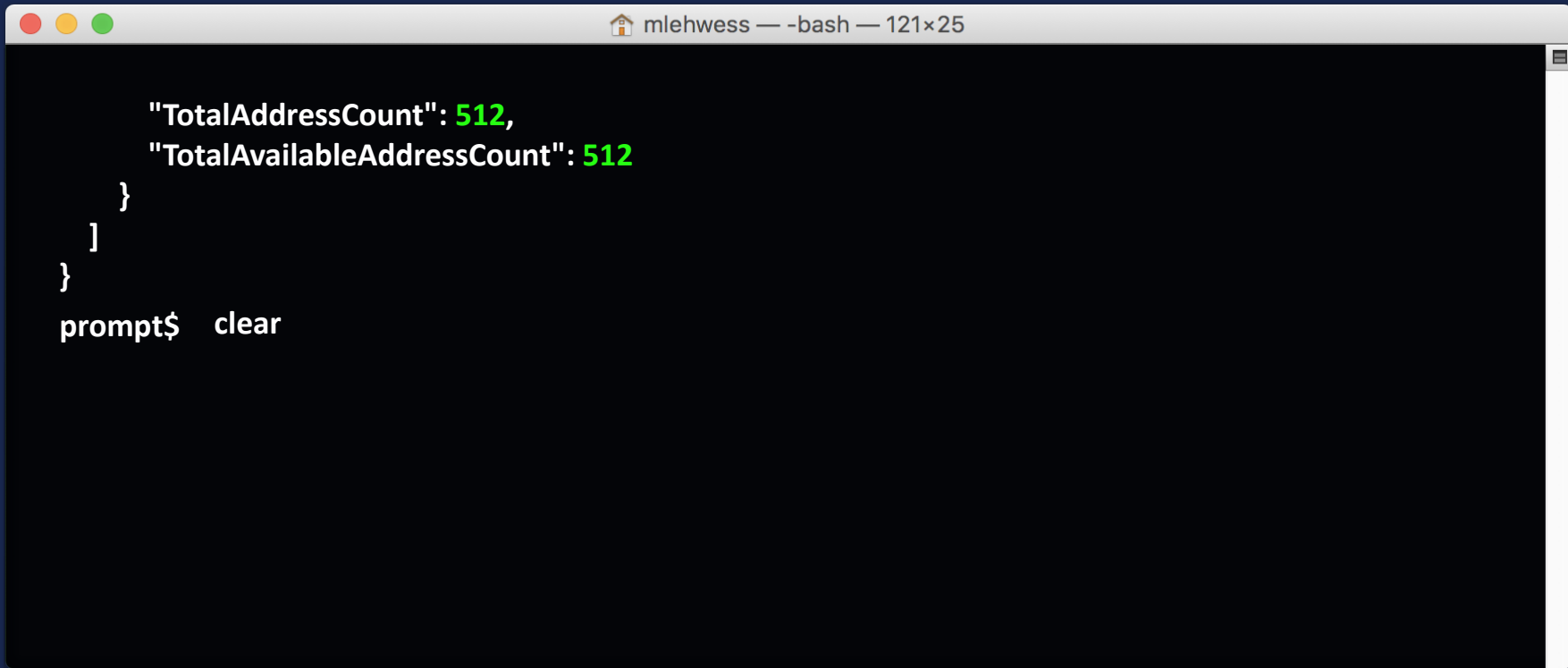
First, use `describe-public-ipv4-pools`

```
mlehwiss — -bash — 121x25

prompt$
prompt$ aws ec2 describe-public-ipv4-pools --region us-west-2
{
  "PublicIpv4Pools": [
    {
      "PoolId": "ipv4pool-ec2-0588c9b75a25d1a02",
      "Description": "range for prod",
      "PoolAddressRanges": [
        {
          "FirstAddress": "130.137.24.0",
          "LastAddress": "130.137.25.255",
          "AddressCount": 512,
          "AvailableAddressCount": 512
        }
      ],
    }
  ],
}
```


Creating an Amazon Elastic IP

First, use `describe-public-ipv4-pools`



```
mlehwiss — -bash — 121x25  
  
    "TotalAddressCount": 512,  
    "TotalAvailableAddressCount": 512  
  }  
]  
}  
prompt$ clear
```

Creating an Amazon Elastic IP

Next, use `allocate-address` (random)

```
mlehwiss — -bash — 121x25

prompt$
prompt$ aws ec2 allocate-address --region us-west-2 --domain vpc
--public-ipv4-pool ipv4pool-ec2-0588c9b75a25d1a02
{
  "PublicIpv4Pool": "ipv4pool-ec2-0588c9b75a25d1a02",
  "PublicIp": "130.137.24.135",
  "AllocationId": "eipalloc-e4a4 added ← ---
  "Domain": "vpc"
}

prompt$ clear
```

Allocates a random address

Creating an Amazon Elastic IP

Next, use `allocate-address` (specific)

```
mlehwiss — -bash — 121x25

prompt$
prompt$ aws ec2 allocate-address --region us-west-2 --domain vpc
--address 130.137.24.77 ←---
{
  "PublicIpv4Pool": "ipv4pool-ec2-0588c9b75a25d1a02",
  "PublicIp": "130.137.24.77", ←---
  "AllocationId": "eipalloc-4da3fa71",
  "Domain": "vpc"
}

prompt$ clear
```

Allocates a specific address

Creating an Amazon Elastic IP

Next, use `allocate-address` (Amazon)

```
mlehwess — -bash — 121x25

prompt$
prompt$ aws ec2 allocate-address --region us-west-2 --domain vpc
{
  "PublicIpv4Pool": "amazon",
  "PublicIp": "52.41.102.233",
  "AllocationId": "eipalloc-8fa5fcb3",
  "Domain": "vpc"
}
prompt$ clear
```

← ---

Allocates an Amazon address

Creating an Amazon Elastic IP

Describe now shows 2 addresses from the pool and 1 from Amazon

```
mlehwe$ --bash -- 121x25

prompt$
prompt$ aws ec2 --region us-west-2 describe-addresses
{
  "Addresses": [
    {
      "AllocationId": "eipalloc-e4a4fdd8",
      "PublicIpv4Pool": "ipv4pool-ec2-0588c9b75a25d1a02",
      "PublicIp": "130.137.24.135",
      "Domain": "vpc"
    },
    {
      "AllocationId": "eipalloc-4da3fa71",
      "PublicIpv4Pool": "ipv4pool-ec2-0588c9b75a25d1a02",
      "PublicIp": "130.137.24.77",
      "Domain": "vpc"
    }
  ]
}
```

← ---
First address from BYOIP Pool

← ---
Second address from BYOIP Pool

Creating an Amazon Elastic IP

Describe now shows two addresses from pool and one from Amazon

```
mlehwiss — -bash — 121x25
},
{
  "AllocationId": "eipalloc-8fa5fcb3",
  "PublicIpv4Pool": "amazon",
  "PublicIp": "52.41.102.233",
  "Domain": "vpc"
}
]
}
prompt$ clear
```

←---

Third address from Amazon

Creating an Amazon Elastic IP

Describing just the pool, shows only two addresses used

```
mlehwiss — -bash — 121x25

prompt$
prompt$ aws ec2 describe-public-ipv4-pools
{
  "PublicIpv4Pools": [
    {
      "PoolId": "ipv4pool-ec2-0588c9b75a25d1a02",
      "Description": "range for prod",
      "PoolAddressRanges": [
        {
          "FirstAddress": "130.137.24.0",
          "LastAddress": "130.137.25.255",
          "AddressCount": 512,
          "AvailableAddressCount": 510
        }
      ],
    },
  ],
}
```

Creating an Amazon Elastic IP

Describing just the pool, shows only two addresses used



```
mlehwess — -bash — 121x25  
    "TotalAddressCount": 512,  
    "TotalAvailableAddressCount": 510  
  }  
]  
}  
prompt$ clear
```


Withdraw Advertisement

Withdrawing the advertisement of the address range by Amazon

```
mlehwess — -bash — 121x25

prompt$
prompt$ aws ec2 withdraw-byoip-cidr --region us-west-2
--cidr 130.137.24.0/23
{
  "ByoipCidr": {
    "Cidr": "130.137.24.0/23",
    "Description": "range for prod",
    "State": "provisioned"
  }
}
prompt$ clear
```

←---

The prefix/CIDR is now withdrawn by Amazon and goes back to a state of “provisioned”

Deprovisioning Address Range

After deallocating all EIPs from the pool

```
mlehwiss — -bash — 121x25

prompt$
prompt$ aws ec2 deprovision-byoip-cidr --region us-west-2
--cidr 130.137.24.0/23

{
  "ByoipCidr": {
    "Cidr": "130.137.24.0/23",
    "Description": "range for prod",
    "State": "pending-deprovision"
  }
}

prompt$ clear
```

←---

The prefix/CIDR is now “pending-deprovisioning”

Let's checkout the console
cool.

Allocate new address

Allocate a new Elastic IP address by selecting the scope in which it will be used

- IPv4 Address**
- Use an address provided by AWS
 - Use an address from a custom pool



*

ipv4pool-ec2-0270a58b21a6af41c



Select address from pool

- Use any address
- Select a specific address from the selected pool

Cancel

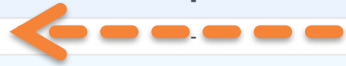
Allocate

- Dedicated Hosts
- Scheduled Instances
- IMAGES
 - AMIs
 - Bundle Tasks
- ELASTIC BLOCK STORE
 - Volumes
 - Snapshots
- NETWORK & SECURITY
 - Security Groups
 - Elastic IPs**
 - Placement Groups
 - Key Pairs
 - Network Interfaces
- LOAD BALANCING
 - Load Balancers
 - Target Groups
- AUTO SCALING
 - Launch Configurations
 - Auto Scaling Groups
- SYSTEMS MANAGER

Allocate new address Actions

Filter by tags and attributes or search by keyword

Name	Elastic IP	Allocation ID	Instance	Private IP address	Scope	Association ID	Network Interface
<input checked="" type="checkbox"/>	130.137.24.135	eipalloc-e4a4fdd8	-	-	vpc	-	-
<input type="checkbox"/>	130.137.24.77	eipalloc-4da3fa71	-	-	vpc	-	-
<input type="checkbox"/>	52.41.102.233	eipalloc-8fa5fcb3	-	-	vpc	-	-



Address: 130.137.24.135

Description Tags

Elastic IP	130.137.24.135	Allocation ID	eipalloc-e4a4fdd8
Instance	-	Private IP address	-
Scope	vpc	Association ID	-
Public DNS	-	Network interface ID	-
Network interface owner	-		

What more do I need to know?

What the most specific prefix I can bring via
BYOIP?

The most specific prefix you can bring via
BYOIP is a /24 IPv4 prefix.

Can I move a CIDR between regions?

Yes you can.

You will have to **de-provision** your CIDR from one region and provision it to the other.

Will the CIDRs on-boarded in preview work when you go public?

Yes, they will continue to work with no interruption.

The CIDRs you on-boarded during the preview will work exactly like CIDRs on-boarded after the feature is public.

Thank you!

prompt\$ clear

