IP addressing

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-ip-addressing.html

Private IPv4 addresses

When you launch an instance into a VPC, a primary private IP address from the IPv4 address range of the subnet is assigned to the instance's primary network interface (for example, eth0).

If you don't specify a primary private IP address, AWS selects an available IP address in the subnet range.

You can assign additional private IP addresses, known as secondary private IP addresses, to instances that are running in a VPC.

Unlike a primary private IP address, you can reassign a secondary private IP address from one network interface to another.

A private IP address remains associated with the network interface when the instance is stopped and restarted, and is released when the instance is terminated. For more information about primary and secondary IP addresses, see Multiple IP Addresses in the *Amazon EC2 User Guide*.

Regardless of the IP address range of your VPC, AWS does not support direct access to the internet from your VPC's CIDR block, including a publicly routable CIDR block. You must set up internet access through a gateway; for example, an internet gateway, a virtual private gateway, an AWS Site-to-Site VPN connection, or AWS Direct Connect.

Public IPv4 addresses

You can control whether your instance receives a public IP address by doing the following:

- Modifying the public IP addressing attribute of your subnet. For more information, see Modify the IP addressing attributes of your subnet.
- Enabling or disabling the public IP addressing feature during instance launch, which overrides the subnet's public IP addressing attribute.
- You can unassign a public IP address from your instance after launch by managing the IP addresses associated with a network interface. For more information, see Manage IP addresses in the *Amazon EC2 User Guide*.

A public IP address is mapped to the primary private IP address through network address translation (NAT).

If you are using Amazon VPC IP Address Manager (IPAM), you can get a contiguous block of public IPv4 addresses from AWS and use them to allocate sequential Elastic IP addresses to AWS resources.

Using contiguous IPv4 address blocks can significantly reduce management overhead for security access control lists and simplify IP address allocation and tracking for enterprises scaling on AWS. For more information, see Allocate sequential Elastic IP addresses from an IPAM pool in the *Amazon VPC IPAM User Guide*.

Note that some IPv6 addresses are reserved by the Internet Engineering Task Force. For more information about reserved IPv6 address ranges, see IANA IPv6 Special-Purpose Address Registry and RFC4291.

Private IPv6 addresses

If you want to connect to the internet from a resource that has a private IPv6 address, you can, but you must route traffic through a resource in another subnet with a public IPv6 address to do so.

There are two types of private IPv6 addresses:

- **IPv6 ULA ranges:** IPv6 addresses as defined in RFC4193. These address ranges always start with “fc” or “fd”, which makes them easily identifiable. **Valid IPv6 ULA space is anything under fd00::/8 that does not overlap with the Amazon reserved range fd00::/16**.
- **IPv6 GUA ranges:** IPv6 addresses as defined in RFC3587. **The option to use IPv6 GUA ranges as private IPv6 addresses is disabled by default and must be enabled before you can use it**. For more information, see Enable provisioning private IPv6 GUA CIDRs in the *Amazon VPC IPAM User Guide*.

Note the following:

- **Private IPv6 addresses are only available through Amazon VPC IP Address Manager (IPAM)**. IPAM discovers resources with IPv6 ULA and GUA addresses and monitors pools for overlapping IPv6 ULA and GUA address space.
- When you use private IPv6 GUA ranges, we require that you use IPv6 GUA ranges owned by you.
- Private IPv6 addresses are not and cannot be advertised on the internet by AWS. AWS does not allow direct egress to the public internet from a private IPv6 range, **even if there is an internet gateway or egress-only internet gateway in the VPC**. **Private IPv6 addresses are automatically dropped at the internet gateway edge, ensuring that they are not routed publicly**.
- AWS reserves the first 4 subnet private IPv6 addresses and the last one.
- Valid ranges for private IPv6 ULA are /9 to /60 starting with fd80::/9.
- **If you have a private IPv6 GUA range allocated to a VPC, you cannot use public IPv6 GUA space that overlaps the private IPv6 GUA space in the same VPC**.
- **Communication between resources with private IPv6 ULA and GUA address ranges is supported (such as across Direct Connect, VPC peering, transit gateway, or VPN connections)**.
- You can use private IPv6 addresses with IPv6-only and dual-stack VPC subnets, elastic load balancers and AWS Global Accelerator endpoints.
- There is no charge for private IPv6 addresses.

These are some of the ways you can prepare to use private IPv6 addresses for your workloads:

- Create an IPAM with Amazon VPC IP Address Manager and provision a private IPv6 *ULA* range to an IPAM address pool. For more information, see Create IPv6 pools in the *Amazon VPC IPAM User Guide*.
- Create an IPAM with Amazon VPC IP Address Manager and provision a private IPv6 *GUA* range to an IPAM address pool. **The option to use IPv6 GUA ranges as private IPv6 addresses is disabled by default and must be enabled on your IPAM before you can use it.** For more information, see Enable provisioning private IPv6 GUA CIDRs in the *Amazon VPC IPAM User Guide*.

Once you are prepared to use private IPv6 addresses, you can allocate a private IPv6 CIDR block from an IPAM pool to your VPC (see Add or remove a CIDR block from your VPC) and associate the IPv6 CIDR block with your subnets (see Modify the IP addressing attributes of your subnet).

VPC CIDR blocks

A VPC must have an associated IPv4 CIDR block. You can optionally associate additional IPv4 CIDR blocks and one or more IPv6 CIDR blocks. For more information, see IP addressing for your VPCs and subnets.

IPv4 VPC CIDR blocks

When you create a VPC, you must specify an IPv4 CIDR block for the VPC. **The allowed block size is between a /16 netmask (65,536 IP addresses) and /28 netmask (16 IP addresses)**. After you've created your VPC, you can associate additional IPv4 CIDR blocks with the VPC.

```
Some AWS services use the 172.17.0.0/16 and 172.16.0.0/12 CIDR
ranges. Services can experience IP address conflicts if the IP
```

```
address ranges are already in use anywhere in your network. For
example, AWS Cloud9 and Amazon SageMaker AI use 172.17.0.0/16 and
Amazon RDS uses 172.16.0.0/12. To avoid conflicts, don't use these
ranges when creating your VPC. For more information, see Can't
connect to EC2 environment because VPC's IP addresses are used by
Docker in the AWS Cloud9 User Guide.
```

To add a CIDR block to your VPC, the following rules apply:

- The allowed block size is between a /28 netmask and /16 netmask.
- The CIDR block must not overlap with any existing CIDR block that's associated with the VPC.
- There are restrictions on the ranges of IPv4 addresses you can use. For more information, see **IPv4 CIDR block association restrictions**.
- **You cannot increase or decrease the size of an existing CIDR block**.
- You have a quota on the number of CIDR blocks you can associate with a VPC and the number of routes you can add to a route table. You cannot associate a CIDR block if this results in you exceeding your quotas. For more information, see Amazon VPC quotas.
- The CIDR block must not be the same or larger than a destination CIDR range in a route in any of the VPC route tables. For example, in a VPC where the primary CIDR block is 10.2.0.0/16, you have an existing route in a route table with a destination of 10.0.0.0/24 to a virtual private gateway. You want to associate a secondary CIDR block in the 10.0.0.0/16 range. Because of the existing route, you cannot associate a CIDR block of 10.0.0.0/24 or larger. However, you can associate a secondary CIDR block of 10.0.0.0/25 or smaller.
- The following rules apply when you add IPv4 CIDR blocks to a VPC that's part of a VPC peering connection:
    - If the VPC peering connection is active, you can add CIDR blocks to a VPC provided they do not overlap with a CIDR block of the peer VPC.
    - If the VPC peering connection is pending-acceptance, the owner of the requester VPC cannot add any CIDR block to the VPC, regardless of whether it overlaps with the CIDR block of the accepter VPC. Either the owner of the accepter VPC must accept the peering connection, or the owner of the requester VPC must delete the VPC peering connection request, add the CIDR block, and then request a new VPC peering connection.

    - If the VPC peering connection is pending-acceptance, the owner of the acceptor VPC can add CIDR blocks to the VPC. **If a secondary CIDR block overlaps with a CIDR block of the requester VPC, the VPC peering connection request fails and cannot be accepted**.
- If you're using AWS Direct Connect to connect to multiple VPCs through a Direct Connect gateway, **the VPCs that are associated with the Direct Connect gateway must not have overlapping CIDR blocks**. If you add a CIDR block to one of the VPCs that's associated with the Direct Connect gateway, ensure that the new CIDR block does not overlap with an existing CIDR block of any other associated VPC. For more information, see Direct Connect gateways in the *AWS Direct Connect User Guide*.
- When you add or remove a CIDR block, it can go through various states: **associating | associated | disassociating | disassociated | failing | failed**. The CIDR block is ready for you to use when it's in the associated state.

IPv6 VPC CIDR blocks

You can associate a single IPv6 CIDR block when you create a new VPC, or **you can associate up to five IPv6 CIDR blocks from /44 to /60 in increments of /4**.

For example, you create a VPC and specify that you want to associate an Amazon-provided IPv6 CIDR block with the VPC.

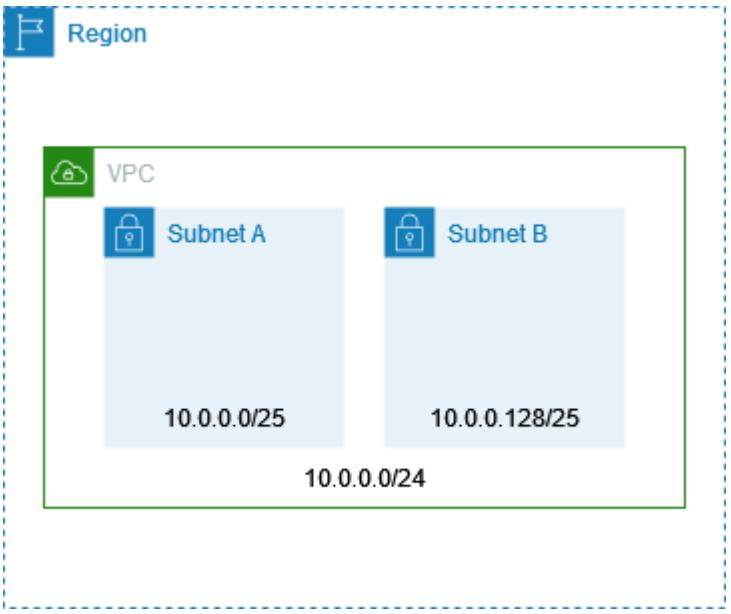
Amazon assigns the following IPv6 CIDR block to your VPC:

2001:db8:1234:1a00::/56. **You cannot choose the range of IP addresses yourself**. You can create a subnet and associate an IPv6 CIDR block from this range; for example, 2001:db8:1234:1a00::/64.

You can disassociate an IPv6 CIDR block from a VPC. **After you've disassociated an IPv6 CIDR block from a VPC, you cannot expect to receive the same CIDR if you associate an IPv6 CIDR block with your VPC again later**.

Subnet CIDR blocks

The CIDR block of a subnet can be the same as the CIDR block for the VPC (to create a single subnet in the VPC), or a subset of the CIDR block for the VPC (to create multiple subnets in the VPC).



Subnet sizing for IPv4

The allowed IPv4 CIDR block size for a subnet is between a `/28` netmask and `/16` netmask.

The first four IP addresses and the last IP address in each subnet CIDR block are reserved by AWS.

For example, in a subnet with CIDR block `10.0.0.0/24`, the following five IP addresses are reserved:

- **10.0.0.0: Network address**.
- **10.0.0.1: Reserved by AWS for the VPC router**.
- **10.0.0.2**: Reserved by AWS. The **IP address of the DNS server is the base of the VPC network range plus two**. For VPCs with multiple CIDR blocks, the IP address of the DNS server is located in the primary CIDR.

  AWS also reserves the base of each subnet range plus two for all CIDR blocks in the VPC. For more information, see Amazon DNS server.

- **10.0.0.3: Reserved by AWS for future use**.
- **10.0.0.255: Network broadcast address**. **AWS does not support broadcast in a VPC**, therefore, AWS reserve this address.

If you create a subnet using a command line tool or the Amazon EC2 API, the CIDR block is automatically modified to its canonical form.

For example, if you specify 100.68.0.18/18 for the CIDR block, AWS creates a CIDR block of 100.68.0.0/18.

If you bring an IPv4 address range to AWS using BYOIP, you can use all of the IP addresses in the range, including the first address (the network address) and the last address (the broadcast address).

Subnet sizing for IPv6

If you've associated an IPv6 CIDR block with your VPC, you can associate an IPv6 CIDR block with an existing subnet in your VPC, or when you create a new subnet. Possible IPv6 netmask lengths are between `/44` and `/64` in increments of `/4`.

The first four IPv6 addresses and the last IPv6 address in each subnet CIDR block are not available for your use, and they cannot be assigned to an EC2 instance.

For example, in a subnet with CIDR block `2001:db8:1234:1a00/64`, the following five IP addresses are reserved:

- `2001:db8:1234:1a00::`
- `2001:db8:1234:1a00::1`: Reserved by AWS for the VPC router.
- `2001:db8:1234:1a00::2`
- `2001:db8:1234:1a00::3`
- `2001:db8:1234:1a00:ffff:ffff:ffff:ffff`

In addition to the IP address reserved by AWS for the VPC router in the example above, the following IPv6 addresses are reserved for the default VPC router:

- A link-local IPv6 address in the FE80::/10 range generated using EUI-64. For more information about link-local addresses, see Link-local address.
- The link-local IPv6 address `FE80:ec2::1`.

Characteristic	IPv4	IPv6
VPC size	Up to 5 CIDRs from /16 to /28. This quota is adjustable.	Up to 5 CIDRs from /44 to /60 in increments of /4. This quota is adjustable.
Subnet size	From /16 to /28.	From /44 to /64 in increments of /4.
Address selection	You can choose the IPv4 CIDR block for your VPC or you can allocate a CIDR block from Amazon VPC IP Address Manager (IPAM). For more information, see What is IPAM? in the Amazon VPC IPAM User Guide.	You can bring your own IPv6 CIDR block to AWS for your VPC, choose an Amazon-provided IPv6 CIDR block, or you can allocate a CIDR block from Amazon VPC IP Address Manager (IPAM). For more information, see What is IPAM? in the Amazon VPC IPAM User Guide.
Internet access	Requires an internet gateway.	Requires an internet gateway. Supports outbound-only communication using an egress-only internet gateway.
Elastic IP addresses	Supported. Gives an EC2 instance a permanent, static public IPv4 address.	Not supported. EIPs keep the public IPv4 address of an instance static on instance restart. IPv6 addresses are static by default.
NAT gateways	Supported. Instances in private subnets can connect to the internet using a public NAT gateway or to	Supported. You can use a NAT gateway with NAT64 to enable instances in IPv6-only subnets to communicate with IPv4-only

	resources in other VPCs using a private NAT gateway.	resources within VPCs, between VPCs, in your on-premises networks, or over the internet.
DNS names	Instances receive Amazon-provided IPBN or RBN-based DNS names. The DNS name resolves to the DNS records selected for the instance.	Instance receive Amazon-provided IPBN or RBN-based DNS names. The DNS name resolves to the DNS records selected for the instance.

Managed Prefix List

A set of one or more CIDR blocks.

You can use prefix lists to make it easier to configure and maintain your security groups and route tables.

You can create a prefix list from the IP addresses you frequently use and reference them as a set in security group rules and routes instead of individually.

You can also use managed prefix lists with other AWS accounts using Resource Access Manager (RAM).

There are two types of prefix lists:

- **Customer-managed prefix lists —** Sets of IP address ranges that you define and manage. You can share your prefix list with other AWS accounts, enabling those accounts to reference the prefix list in their resources.
- **AWS-managed prefix lists —** Sets of IP address ranges for AWS services. You cannot create, modify, share, or delete an AWS-managed prefix list.

Prefix lists concepts and rules

A prefix list consists of *entries*. Each entry consists of a CIDR block and, optionally, a description for the CIDR block.

Customer-managed prefix lists

The following rules apply to customer-managed prefix lists:

- **A prefix list supports a single type of IP addressing only (IPv4 or IPv6). You cannot combine IPv4 and IPv6 CIDR blocks in a single prefix list.**

- A prefix list applies only to the Region where you created it.

- When you create a prefix list, you must specify the maximum number of entries that the prefix list can support.

- When you reference a prefix list in a resource, the maximum number of entries for the prefix lists counts against the quota for the number of entries for the resource. For example, if you create a prefix list with 20 maximum entries and you reference that prefix list in a security group rule, this counts as 20 security group rules.

- When you reference a prefix list in a route table, route priority rules apply. For more information, see Route priority for prefix lists.

- You can modify a prefix list. When you add or remove entries, we create a new version of the prefix list. Resources that reference the prefix always use the current (latest) version. You can restore the entries from a previous version of the prefix list, which also creates a new version.

- There are quotas related to prefix lists. For more information, see Customer-managed prefix lists.

- Customer-managed prefix lists are available in all commercial AWS Regions (including GovCloud (US) and China Regions).

AWS-managed prefix lists

The following rules apply to AWS-managed prefix lists:

- You cannot create, modify, share, or delete an AWS-managed prefix list.
- Different AWS-managed prefix lists have different weights when you use them. For more information, see AWS-managed prefix list weight.
- You cannot view the version number of an AWS-managed prefix list.

AWS service	Prefix list name	Weight
Amazon CloudFront	com.amazonaws.global.cloudfront.origin-facing	55
Amazon DynamoDB	com.amazonaws.region.dynamodb	1
Amazon EC2 Instance Connect	com.amazonaws.region.ec2-instance-connect	2
	com.amazonaws.region.ipv6.ec2-instance-connect	2
AWS Ground Station	com.amazonaws.global.groundstation	5
Amazon Route 53	com.amazonaws.region.ipv6.route53-healthchecks	25
	com.amazonaws.region.route53-healthchecks	25
Amazon S3	com.amazonaws.region.s3	1
Amazon S3 Express One Zone	com.amazonaws.region.s3express	6
Amazon VPC Lattice	com.amazonaws.region.vpc-lattice	10
	com.amazonaws.region.ipv6.vpc-lattice	10

The weight of an AWS-managed prefix list refers to the number of entries that it takes up in a resource.

For example, the weight of an Amazon CloudFront managed prefix list is 55. Here's how this affects your Amazon VPC quotas:

- **Security groups** – The default quota is 60 rules, leaving room for only 5 additional rules in a security group. You can request a quota increase for this quota.
- **Route tables** – The default quota is 50 routes, so you must request a quota increase before you can add the prefix list to a route table.

AWS IP address ranges

https://docs.aws.amazon.com/vpc/latest/userguide/aws-ip-ranges.html#aws-ip-download

AWS services use IP addresses to connect with other resources, either on AWS or your on-prem network. You can get AWS IP addresses ranges using below command.

```
curl -O https://ip-ranges.amazonaws.com/ip-ranges.json
```