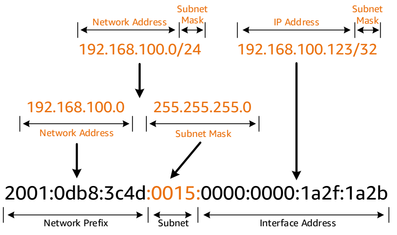
Amazon Web Services IPv6 Cheat Sheet

Reading IPv6 Addresses



IPv4 uses a decimal (base 10) number system: digits can be any of the following range: 0, 1, 2, 3, 4, 5, 6, 7, 8 & 9.

IPv6 uses a hex (base 16) number system: digits can be any of the following range: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e & f.

The following examples show sequential IPv6 network address ranges:
::0000, ::0001 … ::0009, ::000a, ::000b, ::000c, ::000d, ::000e, ::000f, ::0010

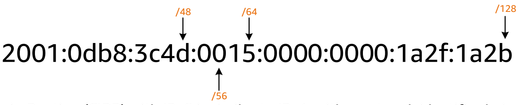
Shortening IPv6 Addresses

Leftmost 0's can be eliminated…
2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b
2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b
2001:db8:3c4d:15:0:0:1a2f:1a2b

An entire string of zeros can be replaced with "::" once per address…
2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b
2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b
2001:0db8:3c4d:0015::1a2f:1a2b

Combining both rules…
2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b
2001:db8:3c4d:15::1a2f:1a2b

CIDR with IPv6



Classless Inter-Domain Routing (CIDR) with IPv6 is similar to IPv4, with a network identifier being followed by a suffix (e.g. /64) indicating the number of bits for the network prefix.

With IPv6 the network identifier is 64 bits (/64) by convention, smaller subnets are not allocated to end users.

Common Network Sizes:
64 bits = /64 = 2^64 hosts = 18,446,744,073,709,551,616 hosts
56 bits = /56 = 2^72 hosts = 256 * /64 networks
48 bits = /48 = 2^80 hosts = 65536 * /64 networks

IPv6 and AWS Services

VPC: Has an IPv4 address pool of up to /16 in size (65536 addresses). Can optionally have an IPv6 address pool of size /56 assigned – this can be provided by Amazon or from an imported customers range.
Subnet: Has an IPv4 address pool of up to /16 in size. Can optionally have an IPv6 address pool of size /64 assigned, as long as the VPC is running in dual-stack mode.

Internet Gateway: Supports both IPv4 and IPv6 traffic.

Elastic Network Interface (ENI): Support both IPv4 and IPv6 addresses. An ENI must always have an IPv4 address, this effectively limits the number of hosts to the size of the IPv4 address space of the subnet.

Security Group: Rules must be defined separately for IPv4 and IPv6 traffic.
Network Access Control List (NACL): Rules must be defined separately for IPv4 and IPv6 traffic.

VPC Flow Log: Supports both IPv4 and IPv6 traffic.

Route Table: Routes must be defined separately for IPv4 and IPv6 traffic.

VPC Endpoints: Support only IPv4 traffic currently.

Traffic Mirroring: Supports both IPv4 and IPv6 traffic.

NAT Gateway: NAT is not required or supported with IPv6, all addresses are "public" and routable.

Egress Only Internet Gateway (EIGW): Supports only IPv6 traffic, creates an equivalent "private" IPv6 subnet by only allowing egress traffic. IPv6 addresses behind an EIGW are "routable" but not "reachable" on the public Internet

VPC Peering: IPv6 traffic is supported over a VPC peering arrangement between two dual-stack VPCs.

Elastic Load Balancing (ELB): Partial support both IPv4 and IPv6 traffic to end users.
Target Group: Communications with members of a Target Group will only use IPv4.

Application Load Balancer (ALB): Supports both IPv4 and IPv6 traffic to end users when internet-facing, internal ALBs support IPv4 only.

Network Load Balancer (NLB): Supports both IPv4 and IPv6 traffic to end users when internet-facing, internal NLBs support IPv4 only.

Classic Load Balancer (CLB): Supports only IPv4 traffic in EC2-VPC mode. Supports both IPv4 and IPv6 in EC2-Classic mode.

Gateway Load Balancer (GWLB): Supports only IPv4 traffic.

Transit Gateway: Supports both IPv4 and IPv6 traffic. Route Tables must include separate entries for IPv4 and IPv6 routes.

Amazon Route 53: Supports both IPv4 and IPv6 traffic. Use the record type of AAAA to map names to IPv6 addresses. The VPC DNS Resolver endpoint in each subnet supports IPv6.

Amazon CloudFront: Supports both IPv4 and IPv6 traffic to end users. Origin fetches only support IPv4.

AWS WAF: Supports both IPv4 and IPv6 traffic. Address matching must include separate entries for IPv4 and IPv6 matches.

Amazon Network Firewall: Supports only IPv4 traffic.

Amazon Elastic Compute Cloud (EC2): Uses ENIs & therefore supports both IPv4 & IPv6 traffic. Local services such as instance Metadata support IPv6 via Unique Local Addresses (ULA).

AWS Lambda: Supports only IPv4 traffic.

Amazon Relational Database Service (RDS): Supports only IPv4 traffic.

Amazon Elastic Container Service (ECS): Supports both IPv4 & IPv6 traffic when deployed in a dual-stack VPC.

Amazon Elastic Kubernetes Service (EKS): Supports only IPv4 traffic.

Amazon Simple Storage Service (S3): Supports both IPv4 & IPv6 traffic via dual-stack endpoints.

aws professional services