# IP Network Planning

### Index

[Home](../README.md)

[Network Docs](README.md)

[Peering Definitions](Peering.md)

[Subnetting Calcuations and IPAM](IP_Planning.md) ## Overview

## IP Allocation Details

The IP allocations are calculated through by a script that reads in a framework file written in YAML. The script Allocates addresses at the VPC, AZ and Subnet Level based on the instructions in the framework file. Allocations are calculated from a base CIDR allocation (10.58.0.0/15) by defining the additional bits for the allocation and selecting the network number. For example if the VPC requires a /20 and the base bask is a /15 the VPC bits are 5 (15 + 5 = 20). The order of allocations to a VPC are controlled by indicating the appropriate netnumber. For the AZ Allocation the process is repeated with out the network number. The Script requires AZs have A minimum of 2 additional bits. This allows for the support of up to 4 AZs per VPC. The addressing is calculated for all 4 AZs. AZ Allocations allow for a starting offset and a AZ count. AZs are allocated sequentialy from the offset, even if the offset is 2 or 3 with a single az allocated the addressing is preserved for the 1st and 2nd AZs. This allows the network to be consistent and summarizable at the VPC and AZ level. The framework file also contains a list of subnet definitions. allocation details for the subnet.

TODO: Consolidate paragraphs

### CIDR Maths

The Network\_structure.py file generates the base model for the environment from the settings specified in the framework.yml file. From the top level allocation we add number of host bits and select the number of the network that we want to assign to a network asset VPC/TGW etc. The VPC method of the basemodel will calculate the VPC Summary, Add appropriate details to the vpc definition in the env\_details json file. It will also calculate the AZ Specifics, Subnet Specifics, create names etc for the environment and write those details to the env\_details json file. Address space is reserved in the calculations for AZs that are not used. The model uses contiguous AZs for a given VPC and limits the AZs to 4 to avoid significant waste. |Rule| Notes| |—|—| |AZ Limit| 4| |AZs are calculated consecutivly| |

### Example1

You want to create a new VPC with 4 subnets in 2 AZs Subnets are mirrored for all selected vpcs,

### Example Framework File

supernet: 10.58.0.0/15 region: us-east-1 vpns: - name: Clemson account: 646306087987 environment: all remote\_gateway: border-pan asn: 65104 tunnels: 2 description: Clemson VPN for SCDHHS target\_address: - 130.127.3.2 - 130.127.3.2 remote\_cidrs: - 10.60.0.0/16 local\_cidrs: - 10.58.0.0/15

lambdas: - name: tgw\_attachment file: assets/tgw\_attachment.py account: 646306087987

domains: - zone: aws-ibm.scdhhs.gov account: 646306087987 type: private comment: “private hosted zone for aws-ibm.scdhhs.gov” vpc\_name: “use1-prod-shared-services” - zone: 10.in-addr.arpa account: 646306087987 type: private comment: “private hosted zone 10.in-addr.arpa for reverse lookup” vpc\_name: “use1-prod-shared-services”

resolver\_endpoints: - name : use1-inbound-ns1 account: 646306087987 direction: “INBOUND” resolver\_rules: {} sg\_rules: [] subnet\_names: - use1-prod-shared-services-az1-core-snet - use1-prod-shared-services-az2-core-snet tags: - resolver\_rule\_direction: “inbound” vpc\_name: “use1-prod-shared-services” - name : use1-outbound-ns1 account: 646306087987 direction: OUTBOUND resolver\_rules: clemson.edu: name: internal\_routing\_outbound shared\_with: devops: 241740101340 rule\_type: FORWARD ips: - 130.127.255.250 - 130.127.255.251 - 130.127.255.252 - 10.60.105.17 scdhhs.gov: name: external\_routing\_outbound shared\_with: devops: 241740101340 rule\_type: FORWARD ips: - 208.80.124.159 - 208.80.125.159 - 208.80.126.159 - 208.80.127.159 - 208.94.148.159 - 208.94.149.159 sg\_rules: ingress: - description: “ingress rule” ip\_protocol: “tcp” cidr\_ipv4: “130.127.255.250/32” from\_port: 53 to\_port: 53 egress: - description: “egress rule” ip\_protocol: “tcp” cidr\_ipv4: “130.127.255.250/32” from\_port: 53 to\_port: 53 subnet\_names: - use1-prod-shared-services-az1-core-snet - use1-prod-shared-services-az2-core-snet tags: - resolver\_rule\_direction: “outbound” vpc\_name: “use1-prod-shared-services” tgws: - environment: all account: 646306087987 name: scdhhs asn: 64851 net\_number: 0 new\_bits: 6 route\_tables: - name: transit create: true tags: {} - name: ingress create: true

vpcs: - name: monitoring environment: prod account: 310718666933 tags: - phi : false - route\_table\_attachment: ingress - route\_table\_propagation: - transit

new\_bits: 7  
net\_number: 14  
start\_az: 0  
az\_count: 2  
az\_new\_bits: 2  
subnets:  
 - name: eks  
 new\_bits: 2  
 net\_number: 0  
 - name: tgw-attachment  
 new\_bits: 4  
 net\_number: 15  
 - name: tools  
 new\_bits: 2  
 net\_number: 1  
 - name: services-endpoints  
 new\_bits: 2  
 net\_number: 2