- Virtual Private Cloud
  - Logical network
    - Endpoints
      - Direct to AWS service
        - Gateway
        - Interface
      - External
    - subnets
      - Routed
      - Private
      - Public
      - one AZ at a time
      - 172.16/12
      - 192.168/16
      - 10/8
      - smallest /28
      - Reserved AWS Ips
        - first 4 and last 4 not used
          - Network Address .0
          - AWS VPC router .1
          - DNS .2
          - Future use .3
          - Network broadcast address .255
            - broadcast not supported
    - Peer VPCs
      - 1 center to 4
      - Star topology
      - no transative peering
  - Mutliple level of security
    - ACLS
      - stateless
      - Default VPC allow all by default
      - Custom VPC - Deny all by default
      - start at 400 for IPv6
      - A subnet can only have 1 ACL
      - Multiples subnets to An ACL
      - Start at 100 for IPv4
      - Rules in numercial order
      - Bi-directonal
        - Close where needed
        - Open as required
    - Flow logs
      - Log traffic flows
        - filter
          - Deny
          - Accept
        - Exceptions
          - AWS DNS
          - 169.254.169.254
          - Reserved VPC traffic
          - DHCP
          - AWS M$ KMS
      - Seperate Role
      - Destination
        - Log group
          - cloud Watch
        - S3 bucket
        - lambda
      - cannot change confugure - recreate
      - Cannot be taged
      - Levels
        - VPC
        - Subnet
        - NIC
    - Secuirty groups
      - Multiple AZ
      - don't span VPC
      - stateful
  - Virtual datacenter in AWS
    - Custom network configuration for workloads
    - one internet gateway per VPC
    - one default in region
      - soft limit of 5
        - can increase by request
    - Hardware VPN
      - Lan Extension
  - Types
    - Custom
      - Custom Subnets
        - CIDR
        - IP 6
        - IP V4
      - Tenancy
        - Dedicated
        - Shared
      - Route tables
        - logical networks
        - IG
    - Default VPC
      - All subnets have a route to internet
      - Auto assign public
  - NAT
    - Instances
      - Disable Source / Dest Check
      - AMI
      - Create Route out
      - Scripted Failover
      - Single OS
      - Bottle Neck
        - increase size
    - NAT Gateway
      - IPv4
      - Elastic IP needed
      - Nat based build
      - 10 GB
      - HA
        - place in multiple AZ
      - Managed by AWS
        - Patching
        - AV
      - Cannot be a hop box
  - LLBs
    - Application
    - Network
    - Classic
      - Legacy