3.3 Disaster Recovery

Response Policy Primary Function	To prevent an incident from happening again
Incident Response Plan	Different from Disaster Recovery
Stopping IRP	Halting the attack
Containing IRP	Limiting the impact caused by the attack
Remediating IRP	Fixing the root cause of the incident
Rebuilding DR	Rebuilding the system
Parity	Error checking, splitting notes in three friends, main>little main>extra little main
Electrical Generator	Power Redundancy
Load Balancing Mechanisms	Round Robin, Content Switching and Multilayer Switching
Multilayer Switching	Combining layer 2 and layer 3 switching at the same time
Failover	Devices which act as backup if main system fails to work
Cold Site	Place only
Warm Site	Hardware only
Hot site	Hardware and Software configured
Least expensive implementation	A Cloud Site
RTO(Recovery Time Objective)	The time it takes to completely restore a system from the most recent backup
RPO(Recovery Point Objective)	How much data will be lost upon backup
BCP(Business Contingency Planning)	Umbrella term
MTTF	The time when the device will eventually fail, it is not recoverable. Light Bulb for

	example
MTBF	Mean time until the main component of system fails, it is recoverable, hard drive
MTTR	Mean time it takes to recover a system once it has been failed
MDT(Mean Downtime)	The mean time until a system is down during a failure or unavailability

Computers in Network Load Balancing Cluster	Host
Computers in a Failover Cluster	Node
Virtual IP	Clustering and Load Balancing
Clustering	Provides redundancy and fault tolerance
Active-Active	Both working
Active-Passive	One working, one over failure
For hard disk drives	MTBF is looked upon while setting up
Disk Mirroring	Mirroring disk only
Disk Duplexing	Mirroring disk along with its controller

	Parity	Stripping	Fault
RAID 0		✅	
RAID 1			✅
RAID 5	✅	✅	✅
RAID 10		✅	✅

Incremental Backup vs Full Backup	Incremental that we do everyday and Full backup happens once in a while. If we are restoring from a full backup point then we have to include a full backup point as

	wells as the all the incremental backups after it
Differential Backup	Only the difference between the full backup point and added items. If we are restoring from a backup point then we have to perform two backups, one for the incremental backup and one for the latest differential backup
In server backups, hard drives over tape drives are preferred for incremental backups	Because sometimes the individual pieces of data needs to be accessed from the drive, which are not possible with the tape drive as it stores data in a linear fashion
Configuration data	Firewalls, Rules, IP Addresses, VLAN settings etc
State Data	CPU, RAM, Logs, Caches etc