9.12.3 Redundancy Facts

The best way to handle an unavoidable disaster is by anticipating potential problems and putting measures into place that speed recovery. *Fault tolerance* is the ability to respond to an unexpected hardware or software failure without loss of data or loss of operation. *Redundancy* is a method of providing fault tolerance by providing duplicate or multiple components that perform the same function. If one component is lost, the redundant component is still available and can provide the necessary service. Methods for providing redundancy for network services and components include:

- Having multiple network paths between any two devices on the network
- Duplicating system components, such as network adapters (adapter teaming) or power supplies
- Keeping identical spare parts on hand for quick replacement
- Providing alternate means of power, including Uninterruptible Power Supplies (UPSs) or backup generators
- Implementing RAID 1 or RAID 5
- Maintaining data backups
- Configuring duplicate servers as passive servers that are immediately available if the active server fails (clustering or load balancing)
- Obtaining a separate internet connection from a different Internet Service Provider (ISP).

In addition to planning for redundant system components and network connections, you can plan for redundancy in your physical sites. The following table lists the types of redundancy solutions:

Type	Description
Hot	The *hot site* (also known as an active backup model) is a redundant facility that is immediately available, requiring just a few minutes or hours to activate. This facility is necessary when an organization can only tolerate a short period of downtime. A hot site is: ▪ Fully configured with cabling infrastructure (power, A/C, and so on) and ready to be powered up. ▪ Fully configured with mirrored/duplicated servers and devices. Mechanisms must be put in place to constantly duplicate data from the main site to the servers at the backup site. ▪ The most effective backup site for disaster recovery. ▪ Expensive to maintain. A hot site requires constant maintenance to keep the hardware, software, data, and applications ready to run; it also presents a security risk. A *mirror site* is a hot site that has instant fail over, provides for parallel processing, and is immediately available in the event of a disaster. This facility is necessary when an organization cannot tolerate any downtime. A mirror site is: ▪ Fully configured, with infrastructure (power, A/C, etc.), network systems, telephone connectivity, and internet connectivity in place. ▪ Fully configured with functional servers and clients that are an up-to-date mirror of the production system. ▪ Expensive to maintain. A mirror site requires constant maintenance to keep the hardware, software, data, and applications ready to run; it also presents a security risk. A *rolling hot site* is a mobile facility, typically in the back of an 18-wheel truck. It has all of the capabilities of a hot site and is very versatile, but expensive.
Warm	The *warm site* is a partially configured redundant facility that takes a few days to a few weeks to activate. This facility may be adequate when an organization's *maximum tolerable downtime* (MTD) is a short time period (such as a couple of days). A warm site is: ▪ Fully configured with infrastructure (power, A/C, and so on) and ready to be powered. ▪ Equipped with communication links and other data elements that commonly take a long time to order and install. ▪ Equipped with servers and clients, but the applications may not be installed or configured. Recovery from backups may be required. ▪ Considerably cheaper than a hot site. A warm site consumes less administrative and maintenance resources than a mirror or hot site. A *reciprocal agreement*, or mutual aid agreement, is an arrangement with another company that may have similar computing needs. In a mutual aid agreement: ▪ Both parties agree to support each other in the case of a disruptive event. ▪ Both parties operate under the assumption that each organization will have the capacity to support the other's operations system in the time of need. Unfortunately, this is a big assumption that is usually wrong. ▪ Mutual aid agreements typically have no initial cost related to them. Optionally, you can set up a reciprocal agreement with another organization to use a warm site as a *reciprocal site*. This allows two organizations to share the costs of one site and keep the costs down. Because only one organization can take possession of the warm site at a time, the two organizations should not be located close enough to each other that a single disaster could affect both at the same time.
Cold	The *cold site* takes a few weeks to a few months to activate. A cold site is: ▪ An empty facility ready for equipment to be brought in (there is no hardware on site). ▪ Equipped with hookups for electrical power, HVAC, telephone, and internet; however, these services might not be activated. ▪ The least ready of the three site types, but may be better than nothing. ▪ The least expensive of the redundant sites.

	▪ Probably the most common redundant site type. A cold site can be a prefabricated building, such as those used by school districts. This type of building is transportable and relatively inexpensive.

A *service bureau* is a contracted site that provides all alternate backup processing services. A service bureau can provide any of the three types of sites. Additionally:

- It provides quick response and availability.
- Testing may be possible.
- The major disadvantages are the expense and resource contention during a large emergency.
- It is common for the service provider to oversell its processing capabilities.

Following are important redundant site considerations:

- Effective redundant site use requires complete documentation of what you have and what you will need in case of disaster. You must also fully document procedures for moving operations to the failover location.
- Locate redundant sites at least 25 miles from the primary site. This will help prevent both facilities from being destroyed by the same disaster.
- Acquire the location *before* the disaster. During a disaster, locations may be difficult to find and much more expensive.
- Keep systems and information at the redundant site up-to-date. Change control processes should include compatibility between sites.
- Ensure that contracts for redundant sites specify your requirements for the site and a detailed process for your use of the site.
- Move the most critical functions first when moving operations to a backup facility.
- Return the least critical functions first when returning services from the backup facility back to the primary facility.

Redundancy measurement parameters include the following:

Parameter	Description
Recovery Time Objective	Recovery Time Objective (RTO) is the actual time required to successfully recover all operations.
Recovery Point Objective	Recovery Point Objective (RPO) is a measurement of how old data is at the point that it is successfully recovered. Any data that has been lost between the RPO and the present must either be accepted as lost or reconstructed. Another aspect of RPO is the number of backups to choose from. Some systems offer multiple recovery points; others offer only one recovery point.
Mean Time Between Failures	The Mean Time Between Failures (MTBF) identifies the average lifetime of a system or component. Components should be replaced about the time that the MTBF is reached.
Mean Time to Failure	The Mean Time to Failure (MTTF) measures the average time to failure of a system or component. This metric assumes that the system or component is not repaired at any point in its lifetime, which would extend its useful life.
Mean Time to Repair	The Mean Time to Repair (MTTR) identifies the average amount of time to repair a failed component or to restore operations. This time frame is also referred to as Mean Time to Restore.
Maximum Tolerable Downtime	Maximum Tolerable Downtime (MTD) combines the RPO, RTO, MTBF, and MTTR to identify the length of time an organization can survive with a specified service, asset, or process down.

Some other redundancy considerations:

- *Single point of failure* - The idea that any one failure in your system or site could cause systematic failure to your organization.
- *Mission Essential Functions* - The label given to functions that help an organization accomplish their goals or missions.
- *Order of Restoration* - The idea that there is a defined order in which systems or services must be restored to working order.
- *Offsite Backups* - The practice of storing backups in another location apart from your main campus.
- *Location Selection* - While choosing a location for your organization, you may need to take geographic considerations into account. Distance from other locations is also a factor.
- *Legal Implications* - There could be legal issues when systems fail that could cost companies or organizations large amounts of money.
- *Data Sovereignty* - Data that is stored by organizations is subject to the laws of the country in which they reside. This means administrators should understand the laws of the country they are in concerning data they have stored.