Disaster Recovery for Networks: The PureIoT Business Continuity Plan

Introduction

A network disaster recovery (DR) plan is a documented, structured approach that describes how an organization can quickly resume mission-critical network operations following a catastrophic event (e.g., fire, flood, major cyberattack). This guide provides a checklist for building a robust DR plan focused on network infrastructure.

1. Define Recovery Objectives

Before writing the plan, you must define what success looks like.

- **Recovery Time Objective (RTO):** The maximum acceptable length of time that your network can be down after a disaster. (e.g., 4 hours).
- **Recovery Point Objective (RPO):** The maximum acceptable amount of data loss measured in time (e.g., 15 minutes).
- **Business Impact Analysis (BIA):** Identify which network services are most critical to business operations (e.g., VoIP, ERP access, Internet access) and prioritize their recovery.

2. Network Configuration Backup

The most critical element of network recovery is having a current, offsite backup of all device configurations.

- **Automated Backups:** Implement a system to automatically back up the configuration files for all routers, switches, firewalls, and wireless controllers.
- **Offsite Storage:** Store configuration backups in a secure, geographically separate location (e.g., a secure cloud storage provider).
- **Version Control:** Maintain multiple versions of configuration files to allow rollback to a known good state.

3. Redundancy and Failover Mechanisms

The best recovery is one that happens automatically.

- **High Availability (HA):** Deploy critical devices (firewalls, core routers) in an HA pair, where a secondary device automatically takes over if the primary fails.
- **Redundant Links:** Use multiple ISP connections (e.g., Fibre and LTE) with automatic failover configured on the router.
- **Virtualization:** Ensure all servers are virtualized. This allows for rapid migration of server images to new hardware or a cloud environment.

4. The Disaster Recovery Checklist

This checklist is executed immediately following a disaster declaration.

Step	Action	RTO Goal
1. Assess Damage	Verify the extent of the damage and confirm which network components are affected.	15 Minutes
2. Declare Disaster	Activate the DR team and notify all relevant stakeholders.	30 Minutes
3. Restore Core Connectivity	Deploy pre-configured backup routers/firewalls and restore core network links.	1 Hour
4. Restore Network Services	Restore critical services (DNS, DHCP, Active Directory) and verify network segmentation (VLANs).	2 Hours
5. Restore Server Configurations	Deploy server images from backup to recovery hardware or cloud environment.	4 Hours
6. Test and Verify	Perform end-to-end testing of all mission-critical applications.	6 Hours
7. Stand Down	Notify all stakeholders that network operations have resumed.	8 Hours

5. Testing and Maintenance

A DR plan is useless if it is not tested.

- **Annual Simulation:** Conduct a full, unannounced simulation of the DR plan at least once a year.
- **Documentation Review:** Review and update the DR plan documentation every six months or after any major infrastructure change.

Conclusion

A comprehensive network disaster recovery plan is the ultimate insurance policy for your business. PureIoT specializes in developing, implementing, and testing DR plans to ensure your business continuity.