Resilient Network Design: Topologies, Risks, & Remediation

By Lucio Rodrigues

Introduction

In networking, the topology refers to how devices (nodes) are physically or logically arranged and connected. Each topology has unique characteristics affecting network **performance, reliability, scalability, and fault tolerance**.

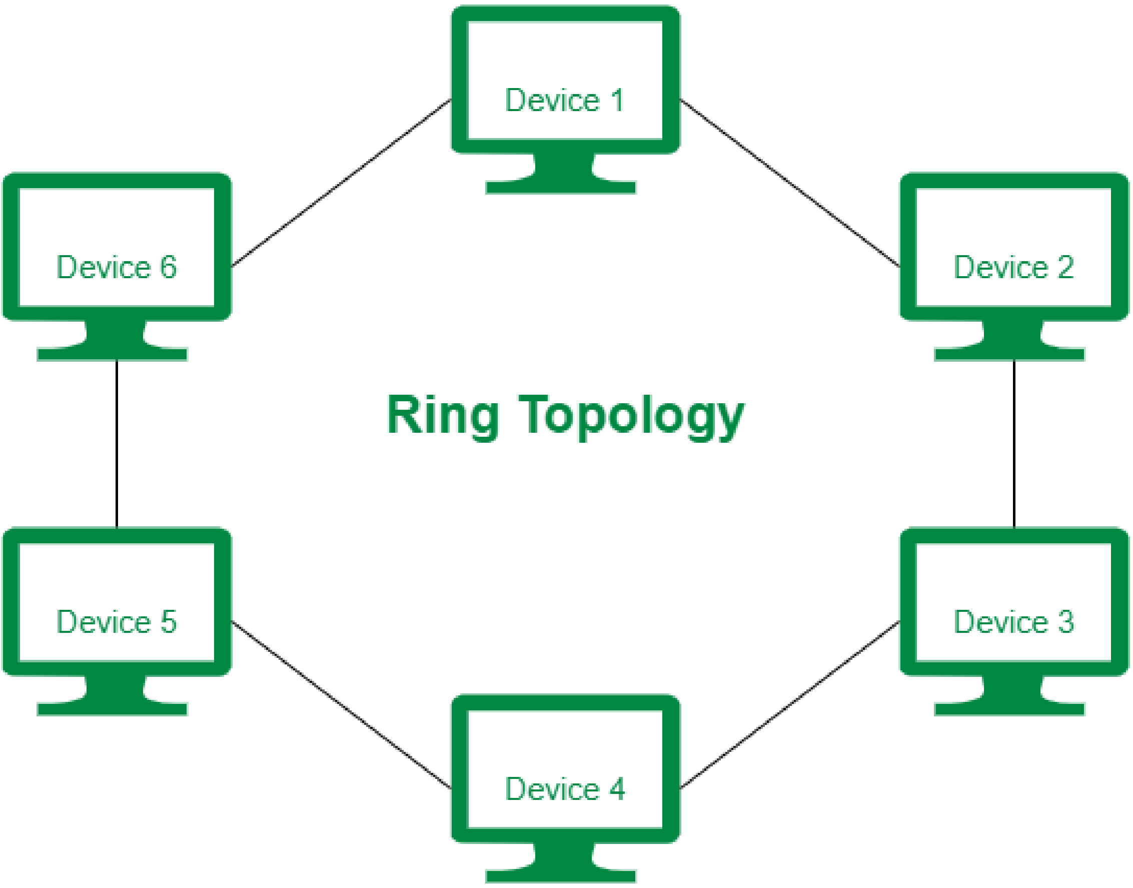
Understanding these helps design better networks and troubleshoot issues efficiently. The topologies I go over in this project are: **Ring**, **Bus**, **Tree** & **Star** Topology.

After reading this project, you will have a clear understanding of the 4 fundamental network topologies - their structures, use cases, and typical failure scenarios.

You'll also gain insight into how these topologies impact cybersecurity, including potential vulnerabilities and practical remediation strategies.

This foundational knowledge will equip you with a stronger grasp of how networks are designed, maintained, and secured. This is an essential skill set for anyone pursuing a career in IT or cybersecurity.

Ring Topology



source: geeksforgeeks.org

What is Ring Topology?

A ring topology connects each device to exactly two others, forming a circular data path. Data travels in one direction (or sometimes both) around the ring until it reaches its destination.

Why Use Ring Topology?

- Efficient for small to medium-sized networks.
- Predictable data flow; easy to manage data collisions.
- Good for networks needing orderly, sequential access.

Realistic Failure Scenario

Scenario: A single device or connection in the ring fails (e.g., a cable breaks or a device powers off).

Impact: The entire network communication is interrupted because data cannot complete the circular path.

Cybersecurity Implications

1. A failure in a ring topology can cause network downtime, which attackers might exploit by launching denial-of-service (DoS) attacks during these vulnerable periods.

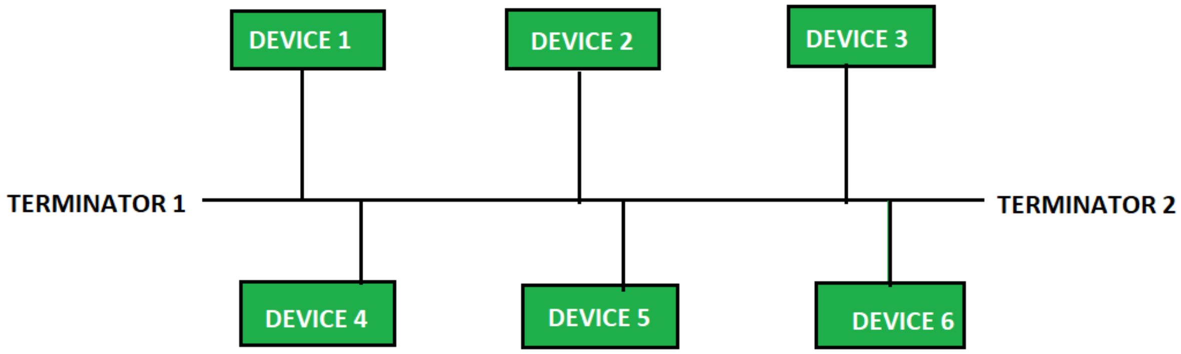
2. Additionally, because data travels sequentially through each node, a compromised device in the ring can intercept or modify data packets, enabling man-in-the-middle (MITM) attacks.

3. Protecting the ring with encryption and implementing network monitoring can help detect suspicious activities and prevent exploitation.

Remediation Solutions

- Implement a dual ring topology (counter-rotating rings) to provide redundancy.
- Use token ring protocol with failure detection to isolate the failed segment.
- Monitor network health actively with network management tools.
- Physically inspect and replace faulty cables or devices immediately.

Bus Topology



source: geeksforgeeks.org

What is Bus Topology?

In bus topology, all devices share a single communication line. Data sent by one device travels in both directions along the bus and is received by all devices.

Why Use Bus Topology?

- Simple and cost-effective for small networks.
- Easy to extend by adding more devices to the bus.
- Minimal cabling required compared to star or tree.

Realistic Failure Scenario

Scenario: A break or fault in the main bus cable or one of the terminators failing.

Impact: Communication is disrupted for all devices connected past the fault point, meaning the network segment could be isolated.

Cybersecurity Implications

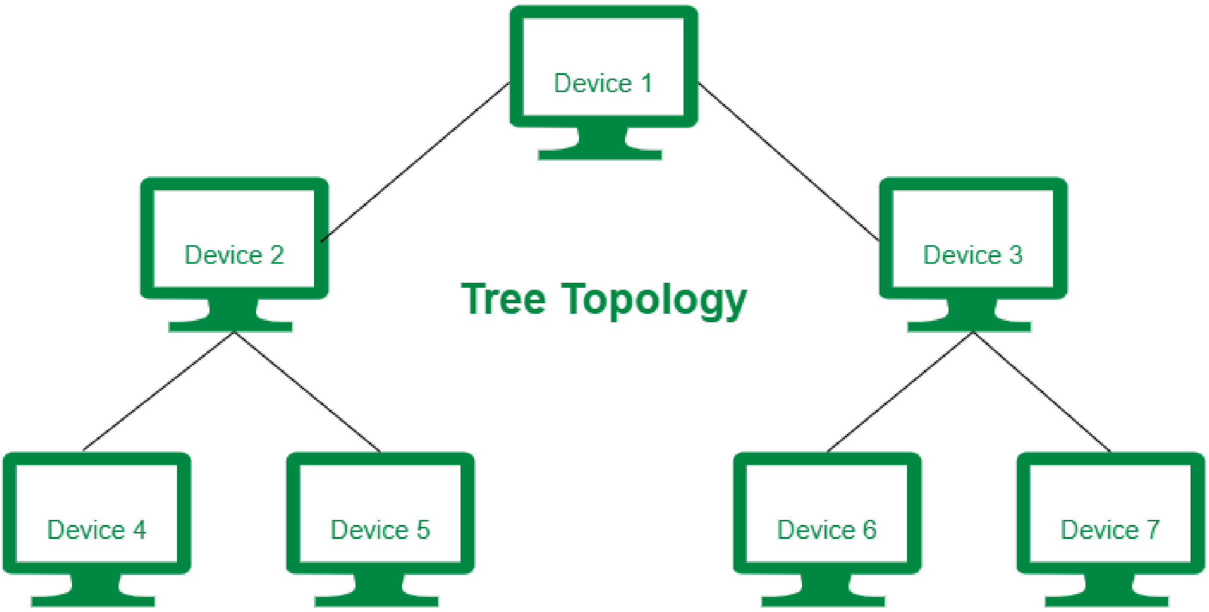
1. Since all devices share the same communication line in bus topology, it is particularly susceptible to eavesdropping and data interception. An attacker who taps into the main bus cable can capture all network traffic, compromising confidentiality.

2. Also, disruption or sabotage of the main bus cable can cause a complete network outage, which can be leveraged for disruption attacks. Using physical security measures, encryption, and network segmentation can reduce these risks.

Remediation Solutions

- Use proper termination at both ends of the bus to prevent signal reflection.
- Employ network monitoring tools to detect cable faults quickly.
- Replace or repair damaged cables or terminators promptly.
- Consider migrating to a more fault-tolerant topology if the network grows.

Tree Topology



source: geeksforgeeks.org

What is Tree Topology?

Tree topology is a hierarchical structure combining characteristics of star and bus topologies. Devices are arranged in groups connected to a central “root” node, forming a branching structure.

Why Use Tree Topology?

- Scalable and easy to manage large networks.
- Supports segmentation for efficient data flow.
- Easier to isolate and troubleshoot faults.

Realistic Failure Scenario

Scenario: Failure of a central node (branch point) or uplink cable connecting a branch to the root.

Impact: Entire subtree connected to the failed node becomes isolated, losing network connectivity.

Cybersecurity Implications

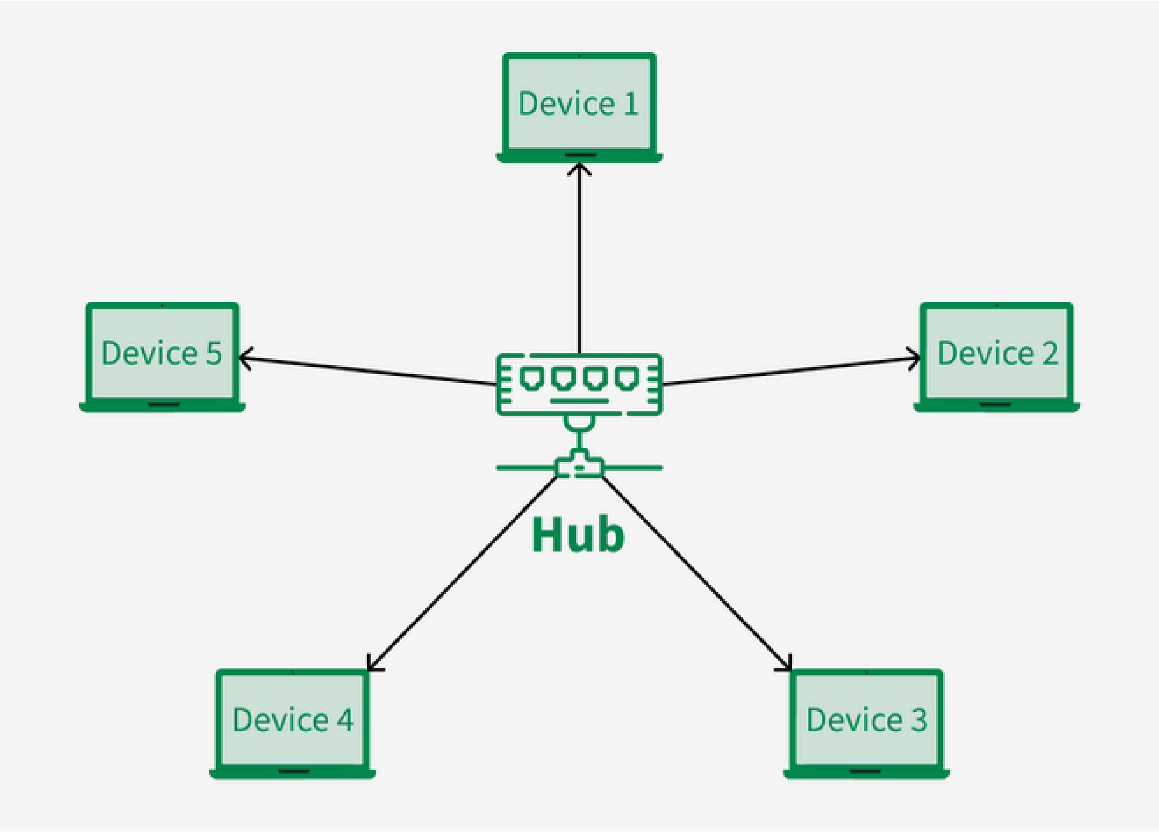
1. In tree topology, the failure or compromise of a central node (such as a root switch) can isolate entire branches of the network. Attackers might target these critical nodes to gain wide access or disrupt large segments of the network.

2. Proper segmentation, access control, and monitoring of these key nodes are essential to prevent lateral movement and contain breaches.

Remediation Solutions

- Implement redundant links between key nodes to provide alternate paths.
- Use network segmentation and monitoring to quickly detect and isolate faults.
- Design the topology with fault-tolerant hardware.
- Train administrators on hierarchical troubleshooting approaches.

Star Topology



source: geeksforgeeks.org

What is Star Topology?

In star topology, all devices connect to a central hub or switch. Communication passes through the central node.

Why Use Star Topology?

- High fault tolerance - failure of a single peripheral device does not affect others.
- Easy to add or remove devices without impacting the network.
- Centralised management and monitoring.

Realistic Failure Scenario

Scenario: The central hub/switch fails or loses power.

Impact: Entire network communication halts since all devices depend on the central node.

Cybersecurity Implications

1. The central hub or switch in star topology is a single point of failure and a prime target for attackers. If an attacker compromises the hub, they can intercept, alter, or disrupt all communications passing through it.

2. Ensuring strong authentication, implementing redundancy, and securing the central device with updated firmware and firewalls help protect the network's integrity and availability.

Remediation Solutions

- Use high-quality, redundant hubs or switches with failover capabilities.
- Implement UPS (uninterruptible power supply) for critical network devices.
- Regularly monitor central node health and performance.
- Design backup network paths if feasible.

Summary Table for Quick Reference

Topology	Pros	Cons	Common Failure	Remediation
Ring	Predictable data flow, orderly	Single failure disrupts all	Break in ring	Dual ring, monitoring
Bus	Simple, cost-effective	Cable fault disrupts all	Cable/terminator failure	Proper termination, repair
Tree	Scalable, easy to manage	Central node failure isolates subtree	Branch point failure	Redundancy, monitoring
Star	Fault tolerance, easy management	Central hub failure disrupts all	Hub/switch failure	Redundant hardware, UPS

Final Thoughts

By bridging traditional network design principles with modern security considerations, this project highlights the importance of building not only functional but also resilient and secure network infrastructures.