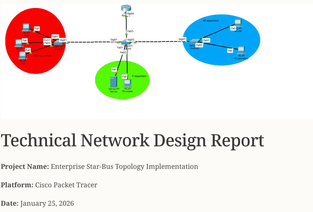

Technical Network Design Report

Project Name: Enterprise Star-Bus Topology Implementation

Platform: Cisco Packet Tracer

Date: January 25, 2026

1. Executive Summary

This project demonstrates the design and implementation of a scalable local area network (LAN) utilizing a Star-Bus topology. The primary design objectives included ensuring network reliability, optimizing performance for critical services, facilitating ease of management, and providing a clear path for future expansion. The chosen Star-Bus topology offers significant benefits in fault isolation, as a failure in one spoke (e.g., a workstation) does not affect the entire network, and it allows for centralized network management and troubleshooting from the core.

The network integrates centralized server resources (DNS, DHCP, Web) with multiple departmental endpoints, secured by administrative access controls and a centralized router gateway. This structured approach enhances network security, simplifies IP address management, and ensures that all devices can efficiently access shared resources while maintaining separation between departmental segments for improved performance and security. The design's inherent scalability allows for the seamless addition of new devices and entire network segments without requiring a complete redesign of the underlying infrastructure.

2. Network Topology Overview

The network architecture employs a robust Star-Bus topology, logically segmenting the enterprise network into three primary operational segments. Each segment is connected to a central routing device via high-speed Gigabit Ethernet trunk links, ensuring efficient inter-segment communication and high bandwidth for critical applications.

- **Core Segment (Switch0):** This is the central hub of the network. It houses the primary Gateway Router (responsible for all internal routing and external connectivity), the Enterprise Server (hosting vital services like DNS, DHCP, and Web), and the Administrator terminal. This segment is engineered for high availability and performance, serving as the backbone for all other connected segments. Connections within this segment are typically high-speed, facilitating rapid data exchange between the core infrastructure components.
- **Expansion Segment A (Switch1):** Designed to provide connectivity for the general workstation pool (e.g., PC0, PC1, PC2). This segment represents a typical departmental or common user area. It is connected to the core via a dedicated trunk link, allowing for efficient traffic aggregation and isolation from other segments. The switch in this segment acts as an access layer device, providing connectivity to end-user devices.
- **Expansion Segment B (Switch2):** This segment is dedicated to supporting sensitive departments, specifically the Administrative and HR departments (e.g., PC-HR, PC-Secretary). Its isolation ensures that traffic from these critical business units is handled separately, potentially with different Quality of Service (QoS) or security policies applied at the router level. This segment also connects back to the core using a high-speed trunk link for robust data flow and resource access.

This segmented design, anchored by a central router, facilitates easier traffic management, enhances security by allowing granular control over inter-segment communication, and streamlines troubleshooting by localizing potential issues within specific segments.

3. Logical Addressing Plan

The network leverages a private Class C IPv4 address space, specifically the 192.168.1.0/24 subnet. This subnet provides 254 usable IP addresses, which is ample for the current enterprise size and allows for significant future growth. The uniform subnet mask of 255.255.255.0 (equivalent to /24 CIDR notation) simplifies routing within the LAN and ensures all devices are on the same broadcast domain.

A structured IP allocation strategy has been implemented to clearly distinguish between network infrastructure, servers, administrative devices, and dynamic workstations. Critical infrastructure devices and servers are assigned static IP addresses to ensure consistent availability and simplify management and troubleshooting. End-user workstations are configured to obtain IP addresses dynamically via DHCP for administrative efficiency.

Device	Interface	IP Address	Subnet Mask	Default Gateway
Gateway Router	Gig0/0	192.168.1.1	255.255.255.0	N/A
Enterprise Server	Fa0	192.168.1.10	255.255.255.0	192.168.1.1
PC-Admin	Fa0	192.168.1.11	255.255.255.0	192.168.1.1
Workstations	DHCP	192.168.1.100+	255.255.255.0	192.168.1.1

This clear distinction between static and dynamic addressing not only aids in network organization but also provides a foundational security layer by making it easier to identify and manage critical network components.

4. Implemented Services

To enhance network functionality and ease of use, several key services have been implemented and configured on the Enterprise Server. These services are fundamental for daily operations, streamlining network administration, and providing access to essential resources.

4.1 DHCP (Dynamic Host Configuration Protocol)

To significantly reduce administrative overhead and mitigate IP address conflicts, the Enterprise Server has been configured to function as a DHCP server.

- **Address Pool:** A defined pool of IP addresses, ranging from 192.168.1.100 to 192.168.1.150, has been established. This range provides 51 dynamic IP addresses for workstations, ensuring sufficient capacity for all current and future client devices.
- **Automated Distribution:** The DHCP server is configured to automatically assign essential network parameters to all workstations upon connection. This includes the IP address, Subnet Mask, Default Gateway (192.168.1.1), and DNS Server (192.168.1.10, the Enterprise Server itself). This automation ensures consistent network configurations across all client devices and minimizes manual configuration errors.

The implementation of DHCP is crucial for efficient network management, especially in environments with a fluctuating number of client devices, enabling plug-and-play connectivity for end-users.

4.2 DNS (Domain Name System)

Centralized name resolution is a critical component implemented on the Enterprise Server, allowing users to access local network resources using human-readable Fully Qualified Domain Names (FQDNs) instead of raw IP addresses.

- **DNS Record Configuration:** A specific A record has been created: **www.central.com** resolves to the Enterprise Server's IP address (192.168.1.10). This allows all devices on the network to access the internal web server by its domain name.

This setup not only enhances user convenience but also provides flexibility, as the underlying IP address of the server can be changed without requiring updates to client configurations, only an update to the DNS record. It is essential for facilitating internal communication and resource discovery.

4.3 HTTP (Web Server)

A localized intranet homepage is hosted on the Enterprise Server, providing a central landing page for all internal employees. This service is configured to serve web content via the HTTP protocol.

- **Purpose:** The intranet page can be used for disseminating company announcements, providing quick access to internal tools and documents, or serving as a dashboard for departmental information.
- **Accessibility:** Accessible by navigating to **www.central.com** from any workstation within the network, leveraging the configured DNS service. The server is configured to listen for HTTP requests on port 80.

This internal web server enhances collaboration and information sharing across the enterprise, offering a dedicated and controlled platform for internal communications.

5. Security Configuration

To safeguard the network infrastructure from unauthorized access and configuration tampering, the Gateway Router, as the central control point, has undergone extensive hardening. These measures are critical to maintaining the integrity, confidentiality, and availability of network services.

1. **Privileged Exec Security (Enable Secret):** An encrypted secret password has been implemented for the enable mode. This measure is crucial because the privileged exec mode grants full control over the router's configuration. By requiring a strong, encrypted password, it prevents unauthorized users from gaining administrative privileges and making malicious or accidental changes to the network's core routing policies.
2. **Console Security (Console Line Password):** Physical access to the router's console port is protected via a console line password. This is a fundamental security practice, as direct physical access can bypass many network-based security controls. Protecting the console port ensures that only authorized personnel can connect directly to the router for initial configuration, recovery, or maintenance, preventing unauthorized local configuration access.
3. **VTY Security (Telnet/SSH Line Passwords):** Remote management access to the router via Virtual TeleType (VTY) lines (e.g., Telnet or SSH) is secured with strong passwords. This protects against unauthorized remote administrative access, which is a common vector for network attacks. While Telnet is used in this simulation, in a production environment, SSH (Secure Shell) would be preferred for its encryption capabilities to prevent credential interception.
4. **Global Encryption (service password-encryption):** The global command "service password-encryption" has been enabled. This command obfuscates all plain-text passwords within the router's running and startup configuration files. Its importance lies in preventing the easy discovery of sensitive credentials by shoulder-surfers or if the configuration file is accidentally exposed. While not true encryption, it makes passwords unreadable to casual inspection, adding a significant layer of protection.

These layered security measures collectively contribute to a more resilient network infrastructure, reducing the risk of unauthorized access and ensuring that only authenticated administrators can manage the critical Gateway Router.

6. Connectivity Verification

A comprehensive testing methodology was employed to confirm the successful implementation and operational integrity of the network design. These tests validated both basic connectivity and the proper functioning of implemented services across different network segments.

- **ICMP Echo (Ping):** Extensive ping tests were conducted to verify end-to-end connectivity. For instance, successful pings between PC0 (located in Expansion Segment A) and PC-HR (located in Expansion Segment B) confirmed not only that both segments are reachable but also that the Gateway Router is correctly routing traffic between these distinct broadcast domains. Furthermore, all workstations successfully pinged the Enterprise Server and the Gateway Router, ensuring that fundamental network access is functional for all devices.
- **Web Traffic (DNS and HTTP):** To confirm the correct operation of both DNS and HTTP services, a workstation (specifically the PC-Secretary terminal) was used to attempt to access the internal web server. Successful name resolution of **www.central.com** to 192.168.1.10, followed by the successful loading of the intranet homepage, validated the DNS server's ability to resolve FQDNs and the HTTP server's capability to serve web content. This test was replicated from multiple workstations to ensure consistent service availability.
- **Gateway Access and Routing:** Verification of the Router's Gigabit Ethernet 0/0 interface confirmed its active status and correct IP configuration (192.168.1.1). Furthermore, internal traffic flow from various segments through the router was monitored to ensure it was successfully routing packets as per the defined logical addressing plan. This includes verifying that workstations could reach devices in other segments and that all devices could reach the Enterprise Server, confirming the router's role as the central inter-segment traffic distributor.

The successful completion of these verification steps confirms the network's robust design, proper configuration, and readiness for enterprise operations, ensuring reliable communication and service delivery.

End of Documentation