Network Infrastructure Report

2025-07-30

Contents

1 Executive Summary

This report comprehensively details the design, configuration, and validation of JbSolutions' enterprise network infrastructure spanning Office A, Office B, and the Data Center. Emphasis is placed on crafting a secure, scalable, and highly available LAN and WAN environment tailored to business needs. Utilizing Cisco Packet Tracer simulations, we modeled network behavior to enforce stringent Access Control Lists (ACLs) and verify end-to-end connectivity and segmentation integrity. The approach ensures isolated departmental traffic, controlled external access, and robust internal service availability, setting a strong foundation for future expansion and operational efficiency.

2 Network Architecture Overview

The network infrastructure is segmented into three physical locations, each with dedicated subnets, VLAN configurations, devices, and services to optimize operational workflows and security.

2.1 Office A

- **Subnet:** 192.168.1.0/24
- **VLANs:** HR (VLAN 10), Customer Service (VLAN 20), R&D (VLAN 30), Marketing (VLAN 40)
- **Devices:** Email Server (192.168.1.100), Router, 4 Switches
- **Services:** Telnet, DNS Client, Email

2.2 Office B

- **Subnet:** 192.168.4.0/24
- **VLANs:** Finance (VLAN 50), Sales (VLAN 60), IT (VLAN 70), Operations (VLAN 80)
- **Devices:** Email Server (192.168.4.100), DNS Server, Router, 4 Switches
- **Services:** Telnet, DNS Server, Email

2.3 Data Center

- **Subnet:** 192.168.7.0/24
- **Devices:** Web Servers (192.168.7.150–152), Email Server (192.168.7.100), DNS Authoritative Server (192.168.7.10), Router, 4 Switches
- **Services:** Web, DNS Authoritative, Telnet

3 Subnet Calculations

Subnetting was applied to segment the networks efficiently, supporting scalability and minimizing broadcast domains.

3.1 Office A —192.168.1.0/25

Section	Gateway	IP Range	Broadcast
A	192.168.1.1	192.168.1.2 – 192.168.1.126	192.168.1.127
B	192.168.1.129	192.168.1.130 – 192.168.1.254	192.168.1.255

3.2 Office B —192.168.4.0/25

Section	Gateway	IP Range	Broadcast
A	192.168.4.1	192.168.4.2 – 192.168.4.126	192.168.4.127
B	192.168.4.129	192.168.4.130 – 192.168.4.254	192.168.4.255

The subnetting scheme divides the network into two equal halves per office, optimizing address allocation for departmental use and reducing unnecessary broadcast traffic.

4 ACL Configuration Summary

Access Control Lists were meticulously designed to enforce security policies, restricting unauthorized access while permitting legitimate traffic.

4.1 INBOUND-ICMP ACL

This ACL blocks all ICMP traffic towards critical servers from external sources to mitigate reconnaissance and DoS attempts, while allowing other traffic.

```
deny icmp any host 192.168.1.100
deny icmp any host 192.168.1.200
...
deny icmp any host 192.168.7.200
permit ip any any
```

4.2 Telnet Access ACL

Telnet access is restricted strictly to authorized administrative hosts to prevent unauthorized remote configuration changes.

5 DNS Load Balancing Simulation

The DNS infrastructure supports efficient internal and external name resolution with load balancing logic as follows:

- Intranet devices in both offices are configured to use Office B's DNS server for resolving `jbsolutions.com`, directing traffic internally.
- External clients access the Data Center DNS server, which balances load across multiple external web servers using priority ordering of A records, simulating round-robin DNS behavior.

This approach ensures optimized resource utilization and fault tolerance for DNS queries.

6 Email Server Configuration

The enterprise email system is centralized under the domain `jbsolutions.com` with alias mappings managed via DNS A records. Key attributes include:

- Thirty employee accounts are distributed evenly between Office A and Office B email servers to balance load and enhance reliability.
- Alias mapping simplifies user addressing, facilitating internal and external mail delivery.

This configuration supports effective communication across geographically dispersed teams.

7 FTP Access Rules

FTP services are organized into directories with clear access permissions to protect sensitive data:

- Directory structure includes `/software`, `/documentation`, `/marketing`, and `/resources`.
- Only William, an administrator located on the Data Center subnet, has write access to FTP directories.
- Other users can read files and submit uploads via email, ensuring controlled content management.

This carefully balanced approach safeguards critical resources while enabling necessary collaboration.

8 Telnet Access Design

Telnet access policies are strictly defined per location, supporting secure remote management:

Location	Devices	Admin Access Protocols
Office A	Router, Email Server, Web Server, 4 Switches	Telnet via Router
Office B	Router, Email Server, DNS Server, 4 Switches	Telnet via Router
Data Center	Router, Email Server, Web Server, 4 Switches	Telnet via Router

This centralized Telnet approach simplifies administration while ensuring robust access control.

9 VLAN Access Control & Segmentation

Network segmentation via VLANs enhances security and traffic management. Inter-VLAN routing is disabled to enforce strict isolation; ACLs are optionally deployed to reinforce segmentation.

Office	Floor	Department 1	VLAN	Department 2
A	1	HR	10	Customer Service (20)
A	2	R&D	30	Marketing (40)
B	1	Finance	50	Sales (60)
B	2	IT	70	Operations (80)

This segmented design prevents unauthorized lateral movement and restricts broadcast domains effectively.

10 Testing Summary

Extensive testing verified ACL enforcement, VLAN isolation, and Telnet accessibility to ensure policy compliance and operational integrity.

10.1 ACL Verification

Test ID	**Source Destination**	**Protocol**	**Expected Outcome**
TC01	External 192.168.1.100	ICMP	Blocked
TC02	Internal DNS/Web Server	IP	Permitted

10.2 VLAN Isolation

Test ID	**Source VLAN Destination VLAN**	**Result**
TC09	HR Customer Service	Denied
TC10	R&D Marketing	Denied

10.3 Telnet Access

Test ID	Device	Origin	Expected Result
TC15	Office A Router	Admin Device	Allowed
TC16	Office B Email Server	Non-Admin	Denied

Test outcomes confirm the network adheres to the intended security policies and access controls.

11 Conclusion

The designed network infrastructure for JbSolutions delivers a secure, scalable, and robust environment tailored to enterprise needs. Comprehensive subnet planning and VLAN segmentation effectively isolate departmental traffic, while ACLs enforce strict security boundaries. DNS-based load balancing optimizes service availability, and controlled Telnet access maintains administrative security. The Packet Tracer simulations confirm the network meets connectivity and segmentation requirements. Future enhancements may include integrating dynamic routing protocols, implementing detailed traffic logging for auditing, and further ACL optimizations to adapt to evolving security landscapes.