

Router-Based Extended ACL Security for a Three-Department Enterprise MIS Network: A Cisco Packet Tracer Case Study

Lubna Shireen R, Rahul S

Dept. of Electronics and Communication Engineering (Data Science)
SRM Institute of Science and Technology, Vadapalani Campus
Chennai, India

Abstract — Modern enterprises rely on reliable, well-segmented internal networks to support daily operations across functional departments such as Human Resources (HR), Finance, and Sales. This paper presents the design and simulation of a three-department Smart Enterprise Management Information System (MIS) Network built in Cisco Packet Tracer, using dedicated switches and a single central router without VLAN-based segmentation. The network provides centralised file storage, a payroll and employee database, a web-based Business Intelligence (BI) dashboard, and an internal e-mail system on the smartmis.com domain. Baseline reachability was first verified using ICMP ping and mail exchange, after which Cisco Extended Access Control Lists (ACLs) were introduced on the router to enforce a business-defined access matrix: HR may reach Sales data but not Finance data; Finance may reach both HR and Sales data to support payroll and revenue analysis; and Sales is restricted to its own department. Post-implementation testing confirmed that every permitted path remained functional while every denied path was blocked, demonstrating that a flat, VLAN-free enterprise network can still achieve fine-grained, department-level security through router-based traffic filtering alone.

Keywords - Enterprise network security; Management Information System (MIS); Business Intelligence dashboard; Extended Access Control List (ACL); Cisco Packet Tracer; network segmentation.

I. INTRODUCTION

Computer networks form the backbone of an organisation's daily operations, and the manner in which departments are interconnected directly affects both productivity and information security. This work considers a medium-sized enterprise composed of three functional departments — HR, Finance, and Sales — each of which must communicate internally, exchange e-mail, and, in limited and clearly defined cases, exchange data with the other departments.

Cisco Packet Tracer was selected as the simulation environment because it provides an accurate, hands-on representation of routers, switches, servers and end devices without requiring physical hardware, while allowing configuration commands to be entered exactly as on real Cisco IOS devices, making the skills learned directly transferable.

The objectives of this work are to: design a three-department enterprise topology using a single router and one switch per department, without VLANs; assign a structured IP addressing scheme with a dedicated gateway per department; deploy a File Server, a Database Server and a Web Dashboard Server

representing centralised MIS services; configure a working internal e-mail system on the smartmis.com domain; verify baseline connectivity before introducing any security policy; and translate a business-defined access policy into Cisco Extended ACLs without breaking any required communication.

II. LITERATURE SURVEY

Several published studies informed the design choices made in this work. Suman and Agrawal [1], and a related case study on a Packet-Tracer enterprise network at the University of Lagos [2], showed that an Access Control List can restrict traffic between router interfaces purely by matching source and destination addresses, protocols and ports, without requiring a separate VLAN for every trust boundary — the same underlying approach followed here for the HR–Finance–Sales boundary.

Documentation on Cisco Extended ACL configuration [4], [5] explains that, unlike Standard ACLs which filter only on source address, an Extended ACL can match on source IP, destination IP, protocol and port, and is best placed close to the traffic source so that unwanted packets are dropped early; this work applies Extended ACLs directly on the router interfaces facing each department.

Related work combining VLANs with Extended ACLs [3], [6] found that ACL rules could accurately restrict which VLAN or department could reach a given file or FTP service. Although the present design does not use VLANs, the same permit/deny-matrix principle is applied at the router-interface level.

Separately, research on Management Information Systems and Business Intelligence dashboards [7], [8] emphasises that access to reports and dashboards should be restricted by organisational role so that only authorised staff can view sensitive data such as payroll or sales figures — a principle that directly underpins the access matrix adopted in Section IV.

III. PROPOSED SYSTEM: NETWORK ARCHITECTURE AND METHODOLOGY

A. Novelty

While ACL-based segmentation in Packet Tracer has been studied in generic contexts, most existing exercises apply a simple ‘allow everything except one path’ rule or rely on VLANs as the primary segmentation mechanism. This work instead starts from a concrete business access matrix — derived from how HR, Finance and Sales actually need to interact — and maps it directly onto a small set of Extended ACL statements

applied to three router interfaces, with no VLAN dependency. It further integrates three MIS services with a working internal e-mail system, so that each ACL rule can be verified against real application traffic and not merely ping.

B. Network Topology

The network is built around a single Cisco 2911 router acting as the inter-department gateway, with three Cisco 2960 switches — one per department — each connected to a dedicated router interface (Fig. 1). Each department hosts its own server and two client PCs; the HR switch additionally serves a Manager PC that requires reachability into all three departments for oversight.

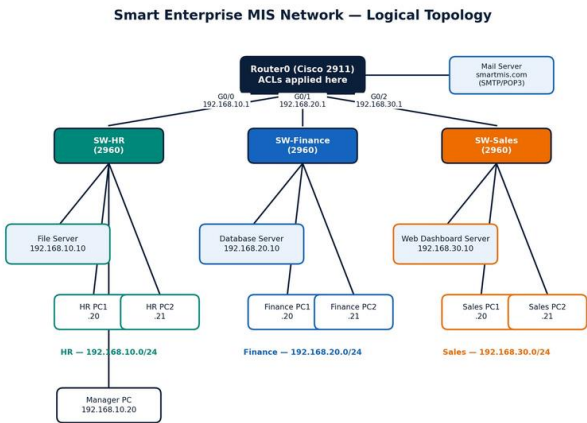


Fig. 1. Logical topology of the Smart Enterprise MIS Network.

C. IP Addressing Plan

Each department is assigned its own /24 subnet, with the router interface acting as the default gateway for all hosts and the server in that department (Table I). The Manager PC is addressed as 192.168.10.20 on the HR subnet.

TABLE I. IP ADDRESSING PLAN

Dept.	Subnet	Gateway	Server IP
HR	192.168.10.0/24	G0/0 – .1	File Srv – .10
Finance	192.168.20.0/24	G0/1 – .1	DB Srv – .10
Sales	192.168.30.0/24	G0/2 – .1	Web Srv – .10

D. MIS Services

Table II summarises the three centralised MIS services deployed, one per department. In addition, an internal Mail Server on the smartmis.com domain provides SMTP and POP3 services to seven mailboxes (manager, hr1, hr2, fin1, fin2, sales1, sales2), enabling every PC to send and receive e-mail as part of normal MIS operation.

TABLE II. MIS SERVICES

Server	Role	Dept.
File Server	Employee records & dept. files	HR
Database Server	Payroll & employee master data	Finance
Web Dashboard Srv	BI dashboard for performance reporting	Sales

E. Baseline Connectivity Testing

Before any ACL was configured, the network was validated end-to-end: the Manager PC reached all three subnets, HR/Finance/Sales could ping one another in every direction,

PC1 and PC2 within each department reached one another and their local server, and all seven mailboxes exchanged e-mail successfully. Only after this baseline was confirmed did the project introduce Extended ACLs, so that any later communication failure could be attributed to the new security policy rather than a pre-existing fault.

IV. SECURITY IMPLEMENTATION: EXTENDED ACCESS CONTROL LISTS

A. Business Access Matrix

The business requirement is that HR may consult Sales figures (to plan recruitment) but must never see Finance data; Finance may consult both HR and Sales data (to run payroll and analyse revenue); and Sales must be confined strictly to its own department, as summarised in Fig. 2.

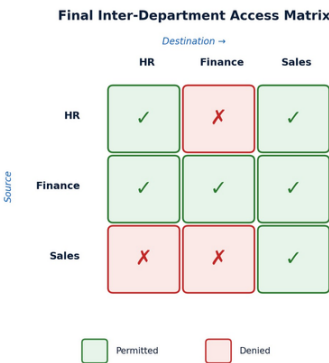


Fig. 2. Final inter-department access matrix enforced by the router ACLs.

B. Packet-Filtering Logic

Every Extended ACL on Router0 is evaluated using the same logic: incoming packets are compared against each Access Control Entry (ACE) from top to bottom, and the first matching rule’s action is applied immediately; if no rule matches, an implicit deny ip any any at the end of the list silently drops the packet (Fig. 3). Extended ACLs are placed as close as possible to the traffic source, so each department’s outbound restriction is applied inbound on its own router interface — e.g., the Sales-to-HR and Sales-to-Finance denials are applied on G0/2, closest to where that traffic originates.

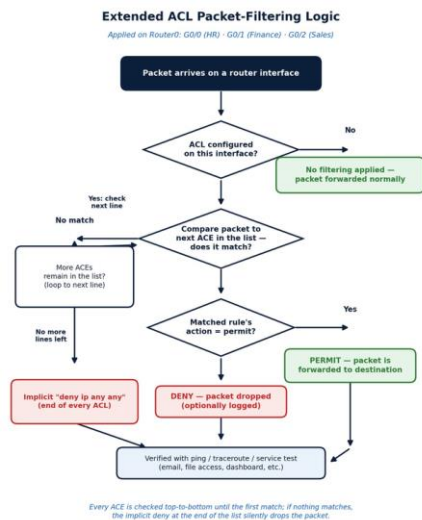


Fig. 3. Extended ACL packet-filtering decision flow, applied on G0/0, G0/1 and G0/2.

C. Access Control Entries by Interface

Table III lists the ACEs required on each interface. Rule order is critical: more specific deny statements must precede the final permit statement, or they will never be reached. Each ACL is bound to its interface in the inbound direction using ip access-group <name> in, so filtering happens as each department's traffic first enters the router.

TABLE III. EXTENDED ACL ENTRIES BY INTERFACE

Interface	Required ACEs (in order)
G0/0 (HR)	1. Deny HR→Finance 2. Permit HR→Sales 3. Permit HR→any
G0/1 (Fin.)	1. Permit Fin→HR 2. Permit Fin→Sales 3. Permit Fin→any
G0/2 (Sales)	1. Deny Sales→HR 2. Deny Sales→Fin 3. Permit Sales→any

V. RESULTS AND ANALYSIS

After applying the Extended ACLs, the network was re-tested against the baseline checklist plus a set of negative tests confirming that denied paths were actually blocked rather than merely unconfigured (Table IV). Every previously working path that the business rules permit continued to work, and every path the business rules forbid was blocked, without needing VLANs or additional hardware.

TABLE IV. POST-ACL TEST RESULTS

Test	Expect.	Observed
HR → Sales Dashboard	Permit	Reachable
HR → Finance DB	Deny	Blocked
Finance → HR File Srv	Permit	Reachable
Finance → Sales Dashboard	Permit	Reachable
Sales → HR File Srv	Deny	Blocked
Sales → Finance DB	Deny	Blocked
Intra-dept. PC/server traffic	Permit	Unaffected
E-mail, all 7 mailboxes	Permit	Unaffected

A. Common Pitfalls Observed

- Placing the final permit ip any any statement before a specific deny statement silently defeats that deny rule, since the first match wins.

- Forgetting the implicit deny at the end of every ACL can unexpectedly block legitimate traffic (e.g. e-mail) if no explicit permit statement covers it.
- Binding the ACL to the wrong direction (out instead of in) changes which traffic the ACL actually inspects.
- Using the wrong wildcard mask for a /24 subnet (0.0.0.255) instead of a standard subnet mask causes rules to silently match the wrong address range.

VI. CONCLUSION

This work has designed, built and secured a three-department Smart Enterprise MIS Network in Cisco Packet Tracer. Starting from a fully operational, unrestricted network with working file, database and dashboard services plus a complete internal e-mail system, Extended ACLs were introduced to enforce a business-defined access matrix between HR, Finance and Sales without disrupting any previously verified communication path. The results show that router-based Extended ACLs are sufficient to achieve fine-grained, department-level security in a flat enterprise topology, and that a business access policy can be translated directly and verifiably into a small, ordered set of ACL statements — providing a complete, testable and explainable model suitable for an academic viva-voce demonstration.

ACKNOWLEDGMENT

The authors thank the Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Vadapalani Campus, for the guidance and laboratory facilities provided during this work.

REFERENCES

- S. Suman and A. Agrawal, "IP traffic management with access control list using Cisco Packet Tracer," ResearchGate, 2016.
- "Design and simulation of a secured enterprise network using Cisco Packet Tracer: A case study of the Faculty of Engineering, University of Lagos," ResearchGate.
- O. J. Usior and E. Sediyo, "Simulasi Extended ACL pada jaringan VLAN menggunakan aplikasi Cisco Packet Tracer," AITI Journal, vol. 20, no. 1, pp. 32–47, 2023.
- R. Parthasarathy et al., "Configuration of access control list applications: Route filtering and traffic control for enterprise network design using Cisco Packet Tracer simulation tool," Sci. Int. (Lahore), vol. 33, no. 3, pp. 265–271, 2021.
- IPCisco, "Cisco extended ACL configuration with Packet Tracer — 3 steps," 2018.
- "Implementation of VLAN and ACL for network security," Journal of Electrical Engineering and Computer (JEECOM).
- "Management information system for effective and efficient decision making: A case study," ResearchGate.
- W. Presthus and C. Canales, "Business intelligence dashboard design: A case study of a large logistics company," Semantic Scholar.