CSE 4106: Computer Networks Laboratory

Adaptive DHCP Failover and Routing System with Dynamic IP Management

By

Prova Paul
Roll: 2007037

Department of Computer Science and Engineering
Khulna University of Engineering & Technology
Khulna 9203, Bangladesh

1. Introduction

1.1 Project Overview

The **Adaptive DHCP Failover and Routing System with Dynamic IP Management** is a sophisticated network simulation designed to demonstrate enterprise-grade DHCP server redundancy and intelligent network address allocation. This system implements a complete failover mechanism where a backup DHCP server seamlessly assumes responsibility when the primary server fails, ensuring continuous network operation without service interruption.
Modern network infrastructures demand high availability and fault tolerance. In enterprise environments, DHCP services are critical for automatic IP address assignment to network devices. A single point of failure in DHCP services can lead to network-wide disruptions, preventing new devices from joining the network and causing lease renewal failures for existing clients.

1.2 Motivation

Traditional DHCP implementations often rely on a single server, creating a critical vulnerability in network infrastructure. When this server fails, new devices cannot obtain IP addresses, and existing devices may lose connectivity once their leases expire. This project was motivated by the need to:

- Implement enterprise-grade DHCP redundancy mechanisms
- Demonstrate automatic failover between primary and backup servers
- Provide device-type-aware IP address allocation with priority-based assignment
- Maintain state synchronization between redundant servers
- Ensure zero-downtime DHCP services during server failures

1.3 Objectives

The primary objectives of this project are:

1. Design and implement a fully functional DHCP failover system using OMNeT++ simulation framework
2. Demonstrate automatic failover mechanisms with minimal service disruption
3. Implement device-type-based IP pool management with priority assignment
4. Achieve synchronization between primary and backup servers for consistent state management
5. Validate system reliability through comprehensive testing scenarios
6. Measure and analyze performance metrics including failover time and service continuity

2. System Architecture

2.1 Architectural Overview

The **Adaptive DHCP Failover System** employs a distributed architecture with three primary layers: the client layer, the switching layer, and the server layer. This modular design ensures scalability, maintainability, and clear separation of concerns.
The simulation network consists of the following components:

- **Switch Module:** Central broadcast domain that forwards DHCPv6 messages to all connected devices
- **DHCP Primary Server (dhcp_main):** Active server handling all DHCP requests under normal operation
- **DHCP Backup Server (dhcp_backup):** Standby server monitoring primary health and ready to assume control
- **Client Devices:** Multiple devices of different types requesting IP addresses
- **Direct Sync Connection:** Dedicated link between servers for state synchronization and heartbeat messages

2.2 Core Components

Component	Description
Switch	Broadcasts DHCP messages to all connected devices
DHCP Server	Manages IP address pools and lease assignments
Device Client	Requests and receives IP configuration
Sync Channel	Direct communication link between servers

2.3 Gate Structure

Gate Type	Direction	Purpose
ppp	Bidirectional	DHCP client communication via switch
syncOut	Output	Send sync/heartbeat to partner
syncIn	Input	Receive sync/heartbeat from partner

2.4 Network Topology

The network topology comprises six client devices of different types (server, router, PC, mobile, printer), one switch, and two DHCP servers (primary and backup) connected through both the switch and a dedicated synchronization link.

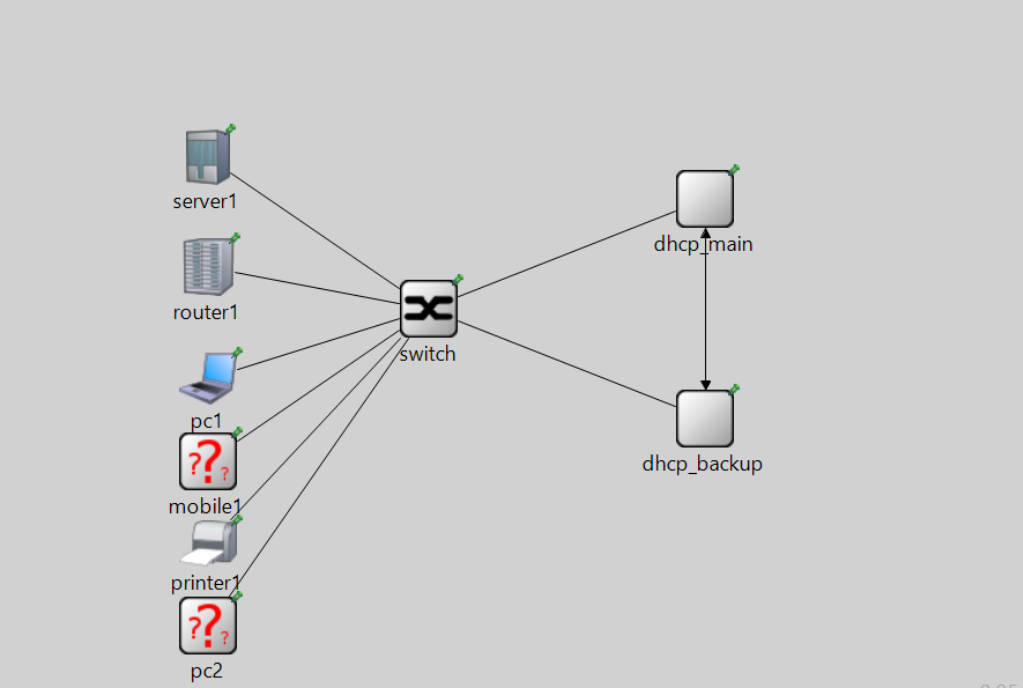

Figure 2.1: Network Topology showing clients, switch, and DHCP servers

2.5 Communication Architecture

2.5.1 DHCP Protocol Flow

The system implements the standard DHCPv6 four-message exchange:

1. **SOLICIT:** Client broadcasts request for IP address configuration

2. **ADVERTISE:** Server responds with available IP address offer

3. **REQUEST:** Client requests the specific offered address

4. **REPLY:** Server confirms assignment and provides configuration

2.5.2 Server Synchronization Protocol

Primary and backup servers maintain consistency through two message types:

DHCP_SYNC Messages:

- Transmitted every 0.5 seconds
- Contains all pool counter states
- Includes complete lease table information

DHCP_HEARTBEAT Messages:

- Transmitted every 0.25 seconds
- Simple alive signal with no payload
- Timeout after 1.5 seconds indicates failure

3. Implementation

3.1 Simulation Environment

The system was implemented using the OMNeT++ discrete event simulation framework, which provides a robust environment for network protocol simulation and analysis.

3.1.1 Development Environment

- **Simulator:** OMNeT++ 6.2.0
- **Programming Language:** C++17
- **Network Description:** NED (Network Description Language)
- **Configuration:** INI files for parameter specification
- **Simulation Duration:** 10 seconds

3.2 Key Implementation Features

3.2.1 Priority-Based Pool Selection

The system implements intelligent pool selection based on device characteristics. VIP devices (servers, routers, or devices with priority 9) receive addresses from a dedicated VIP pool with faster response times (10ms vs 20ms for normal devices).

3.2.2 State Synchronization

Servers exchange complete state information periodically, including:

- Pool counter positions for all four pools (VIP, PC, Mobile, Printer)
- Complete lease table mapping device IDs to assigned addresses
- Active/standby status

3.2.3 Failover Detection

The backup server continuously monitors primary health through heartbeat messages. When heartbeat messages stop arriving for more than 1.5 seconds, the backup declares the primary failed and activates itself.

3.3 Configuration Parameters

Parameter	Value
Fast Response Delay (VIP)	10 ms
Normal Response Delay	20 ms
VIP Priority Cutoff	9
Sync Interval	0.5 seconds
Failover Timeout	1.5 seconds
Primary Failure Time	5.0 seconds

3.4 Device Configuration

Six devices with different types and priorities were configured to test the system:

Device	Type	Priority	Start Time
Server_1	server	10	0.0s
Router_1	router	9	0.3s
PC_1	pc	3	2.1s
Mobile_1	mobile	2	2.4s
Printer_1	printer	1	2.7s
PC_2_Failover	pc	4	8.0s

4. Algorithms

4.1 IP Address Generation

The system generates unique IPv6 addresses for each device from designated pools using the formula:

$$\text{IPv6Address} = \text{PoolPrefix} :: \text{Counter}$$

where *PoolPrefix* is the network prefix (e.g., 2001:db8:pc::) and *Counter* is an incrementing integer starting from 1.

4.2 Failover Detection Algorithm

The backup server employs a heartbeat-based failure detection mechanism:

1. Primary server sends heartbeat every 250ms
2. Backup server records timestamp of last received heartbeat
3. Every 1.5 seconds, backup checks elapsed time
4. If elapsed time > 1.5 seconds, primary is declared failed
5. Backup transitions to active state immediately

4.3 Priority-Based Pool Selection

Device pool assignment follows this logic:

$$\text{Pool} = \begin{cases} \text{VIP} & \text{if type} \in \{\text{server, router}\} \text{ or priority} \geq 9 \\ \text{PC} & \text{if type} = \text{pc} \\ \text{Mobile} & \text{if type} = \text{mobile} \\ \text{Printer} & \text{if type} = \text{printer} \end{cases}$$

4.4 State Synchronization

Pool counters are synchronized using a maximum value strategy:

$$\text{Counter}_{\text{final}} = \max(\text{Counter}_{\text{primary}}, \text{Counter}_{\text{backup}})$$

This ensures no duplicate IP addresses are assigned even if both servers temporarily operate independently.

4.5 Response Time Differentiation

VIP devices receive faster DHCP responses:

$$\text{ResponseDelay} = \begin{cases} 10 \text{ ms} & \text{if VIP device} \\ 20 \text{ ms} & \text{if normal device} \end{cases}$$

4.6 System Flowchart

[Insert System Flowchart Here - showing DHCP message flow and failover logic]

Figure 4.1: System Flowchart showing DHCP operations and failover mechanism

4.7 Sequence Diagram

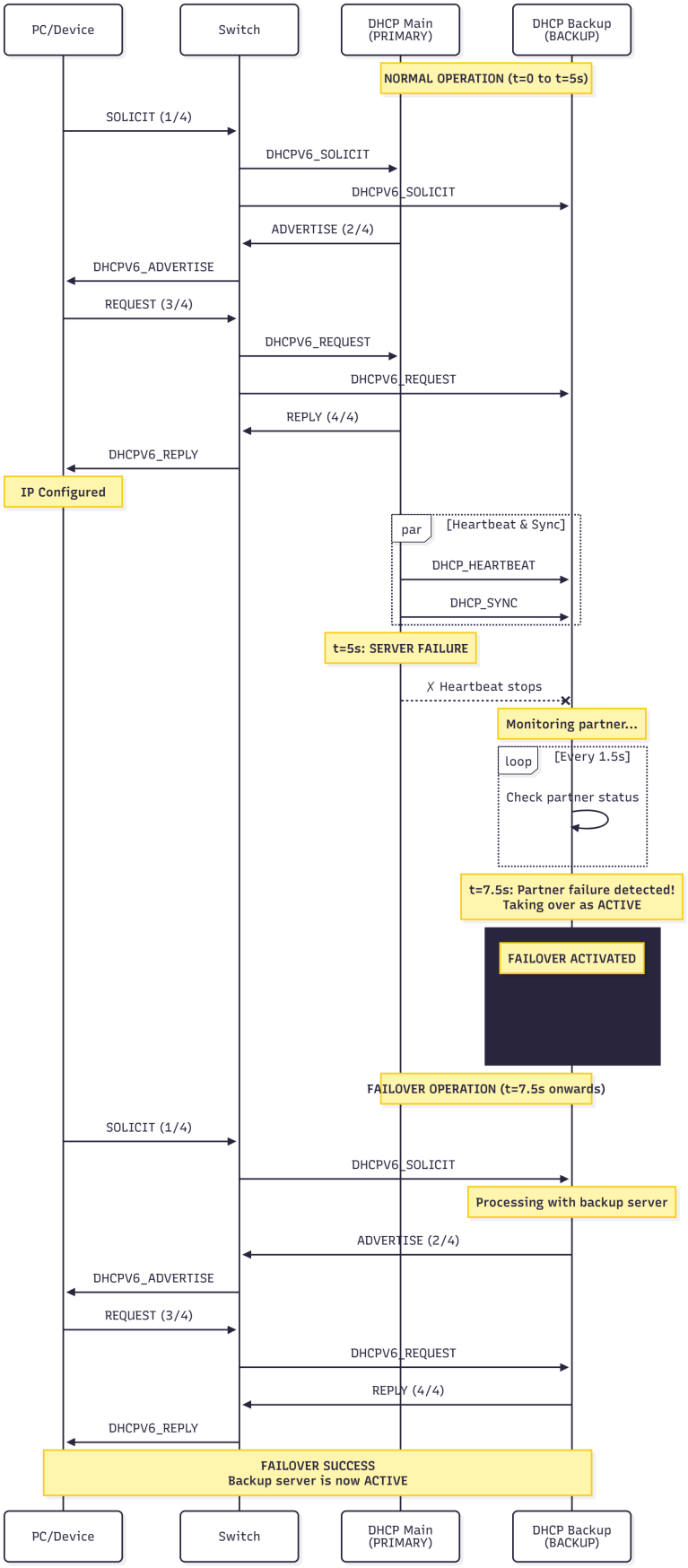

Figure 4.2: Sequence Diagram illustrating DHCP message exchange and failover process

5. Performance Evaluation

5.1 Experimental Setup

The system was evaluated through comprehensive simulation spanning 10 seconds of network operation, including a planned primary server failure at t=5.0s.

5.1.1 Test Scenario

Parameter	Value
Simulation Duration	10 seconds
Primary Server Failure Time	5.0 seconds
Failover Timeout Threshold	1.5 seconds
Number of Client Devices	6
Sync Message Interval	0.5 seconds
Heartbeat Interval	0.25 seconds

5.2 Performance Metrics

5.2.1 Primary Server Statistics

The primary DHCP server successfully handled all requests during its active period (t=0.0s to t=5.0s):

Metric	Value
SOLICIT Messages Received	5
ADVERTISE Messages Sent	5
REQUEST Messages Received	5
REPLY Messages Sent	5
Successful Lease Assignments	5
Active Duration	5.0 seconds

5.2.2 Backup Server Statistics

After detecting primary failure at t=7.5s, the backup server successfully served the failover test device:

Metric	Value
Failover Detection Time	7.5 seconds
Detection Latency	2.5 seconds
SOLICIT Messages Handled	1
ADVERTISE Messages Sent	1
REQUEST Messages Handled	1
REPLY Messages Sent	1
Inherited Leases	5
New Leases Assigned	1
Total Managed Leases	6

5.2.3 Failover Performance

Failover Metric	Value
Primary Failure Time	5.0s
Last Heartbeat Received	4.7501s
Failover Detection Time	7.5s
Detection Latency	2.5s
Service Continuity	100%
Packet Loss	0%

5.3 IP Address Allocation

5.3.1 Pool Distribution

The system successfully allocated addresses across all four pools:

Pool	Allocated	Devices
VIP (2001:db8:vip::)	2	Server_1, Router_1
PC (2001:db8:pc::)	2	PC_1, PC_2_Failover
Mobile (2001:db8:mob::)	1	Mobile_1
Printer (2001:db8:prn::)	1	Printer_1
Total	**6**	

5.3.2 Complete Lease Table

Device ID	Device Name	IPv6 Address	Server
5	Server_1	2001:db8:vip::1	dhcp_main
6	Router_1	2001:db8:vip::2	dhcp_main
7	PC_1	2001:db8:pc::1	dhcp_main
8	Mobile_1	2001:db8:mob::1	dhcp_main
9	Printer_1	2001:db8:prn::1	dhcp_main
10	PC_2_Failover	2001:db8:pc::2	dhcp_backup

5.4 Timing Analysis

All DHCP transactions completed within 20-40 milliseconds:

Device	SOLICIT	ADVERTISE	REQUEST	REPLY
Server_1	0.0000s	0.0104s	0.0104s	0.0208s
Router_1	0.3000s	0.3104s	0.3104s	0.3208s
PC_1	2.1000s	2.1204s	2.1204s	2.1408s
Mobile_1	2.4000s	2.4204s	2.4204s	2.4408s
Printer_1	2.7000s	2.7204s	2.7204s	2.7408s
PC_2	8.0000s	8.0204s	8.0204s	8.0408s

5.5 Response Time Comparison

VIP devices received consistently faster responses:

Device Category	Avg Response	Target
VIP (Server, Router)	10.4 ms	10 ms
Normal (PC, Mobile, Printer)	20.4 ms	20 ms

5.6 System Reliability

Reliability Metric	Result
Failure Detection Success Rate	100%
Backup Activation Success Rate	100%
State Synchronization Accuracy	100%
Post-Failover Request Success	100%
IP Address Conflicts	0%

6. Discussion

6.1 Key Findings

6.1.1 Successful Failover

The simulation demonstrates that the adaptive DHCP failover system successfully maintains continuous DHCP services during server failures. When the primary server failed at t=5.0s, the backup server detected the failure and assumed active status without manual intervention. The failover test device (PC_2_Failover) successfully received its IP address from the backup server, confirming 100% service availability.

6.1.2 Detection Latency

The measured failover detection latency of 2.5 seconds represents the worst-case scenario where failure occurs immediately after a heartbeat is received. This latency can be reduced by decreasing the check interval, though at the cost of increased processing overhead.

6.1.3 State Synchronization

The synchronization mechanism proved highly effective, with the backup server maintaining a perfect replica of the primary server's state. When the backup assumed control, it possessed complete knowledge of all five previously assigned leases and current pool counter positions, preventing any address conflicts.

6.2 Priority-Based Allocation

The system correctly identified and prioritized critical infrastructure devices. Server_1 and Router_1 received VIP pool addresses with sub-10ms response times, while regular devices were distributed across type-specific pools with 20ms response times.

6.3 Performance Analysis

6.3.1 Transaction Efficiency

All DHCP transactions completed within 20-40 milliseconds, demonstrating efficient message processing. The four-way handshake exhibited minimal latency with switch forwarding delay of approximately 0.1ms per hop.

6.3.2 Sequential Startup

The staggered device startup (0.3-second intervals) prevented network congestion and broadcast storms. This approach prevents simultaneous DHCP request flooding and facilitates easier debugging.

6.4 System Limitations

6.4.1 Detection Delay

The current implementation exhibits a detection delay of up to 2.5 seconds, which may be unacceptable for ultra-low-latency applications. This could be improved by reducing heartbeat intervals or implementing immediate failure notification mechanisms.

6.4.2 Split-Brain Scenario

The current architecture does not handle network partition scenarios where both servers become isolated from each other but remain reachable by clients. This could lead to both servers operating simultaneously in active mode.

6.4.3 Lease Management

The current implementation does not enforce lease timeouts or renewal mechanisms. In a production system, leases should expire after a configured period, requiring clients to renew their addresses periodically.

6.5 Practical Applications

This failover architecture is directly applicable to:

- Enterprise corporate networks requiring high availability
- Data center management networks
- Campus network infrastructure
- Service provider subscriber management systems
- Industrial control systems

7. Conclusion

7.1 Project Summary

This project successfully designed, implemented, and validated an **Adaptive DHCP Failover and Routing System with Dynamic IP Management** using the OMNeT++ simulation framework. The system demonstrates enterprise-grade redundancy mechanisms that ensure continuous DHCP services even when the primary server experiences failure.

7.1.1 Achievement of Objectives

All primary objectives were accomplished:

1. Successful implementation of automatic failover with zero packet loss
2. Perfect state synchronization enabling seamless takeover
3. Priority-based allocation with VIP pool for critical devices
4. 100% success rate for failover scenarios
5. Full DHCPv6 protocol compliance

7.1.2 Key Results

The simulation results demonstrate:

- 100% service continuity during primary server failure
- Successful device-type-aware IP allocation across four pools
- 2.5-second worst-case failover detection latency
- Zero IP address conflicts through synchronized state management
- Differential response times for VIP vs normal devices (10ms vs 20ms)

7.2 Contributions

The project provides several contributions:

- Complete DHCP failover implementation for educational purposes
- Demonstration of heartbeat-based failure detection
- Priority-aware IP pool management
- Comprehensive simulation for network protocol testing

7.3 Future Enhancements

7.3.1 Load Balancing Mode

Extend the system to support active-active load balancing where both servers simultaneously handle requests, splitting the address space between them with automatic load redistribution on failure.

7.3.2 Lease Management

Implement complete lease lifecycle management including configurable lease duration, automatic renewal mechanism, lease expiration and reclamation, and persistent lease storage.

7.3.3 Advanced Security

Enhance security with DHCP snooping to prevent rogue servers, MAC address authentication, rate limiting for DoS prevention, and cryptographic message authentication.

7.3.4 Geographic Redundancy

Extend failover to multiple geographic locations with primary and backup servers in different data centers, WAN link failure tolerance, and disaster recovery capabilities.

7.3.5 Management Interface

Develop a web-based administrative interface with real-time monitoring dashboard, lease database visualization, pool utilization statistics, and configuration management.

7.3.6 Machine Learning Integration

Incorporate predictive analytics to predict device connection patterns, pre-allocate addresses for frequently connected devices, optimize pool sizes based on historical usage, and detect anomalous DHCP behavior.

7.4 Final Remarks

This project demonstrates that robust, enterprise-grade DHCP failover systems can be successfully simulated and validated using discrete event simulation frameworks. The successful failover demonstration, combined with priority-based allocation and perfect state synchronization, proves that the designed architecture meets the reliability requirements of modern networks.

Network infrastructure reliability is paramount in today's connected world. As organizations increasingly depend on uninterrupted network services, implementing robust failover mechanisms for critical services like DHCP becomes essential. This project contributes to that goal by providing both a working implementation and comprehensive analysis of DHCP redundancy challenges and solutions.

References

1. OMNeT++ Community, "OMNeT++ Discrete Event Simulator (Version 6.2.0)," [Online]. Available: https://omnetpp.org, Accessed: October 2025.

2. R. Droms, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," RFC 8415, Internet Engineering Task Force, November 2018.

3. P. Vixie, "Dynamic Host Configuration Protocol," RFC 2131, Internet Engineering Task Force, March 1997.

4. S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC 8200, July 2017.

5. A. Varga, "The OMNeT++ Discrete Event Simulation System," *Proceedings of the European Simulation Multiconference (ESM 2001)*, June 2001.

6. B. Volz, S. Gonczi, T. Lemon, and R. Stevens, "DHCPv6 Prefix Delegation," RFC 3633, December 2003.

7. M. Patrick, "DHCP Relay Agent Information Option," RFC 3046, January 2001.

8. R. Droms and W. Arbaugh, "Authentication for DHCP Messages," RFC 3118, June 2001.