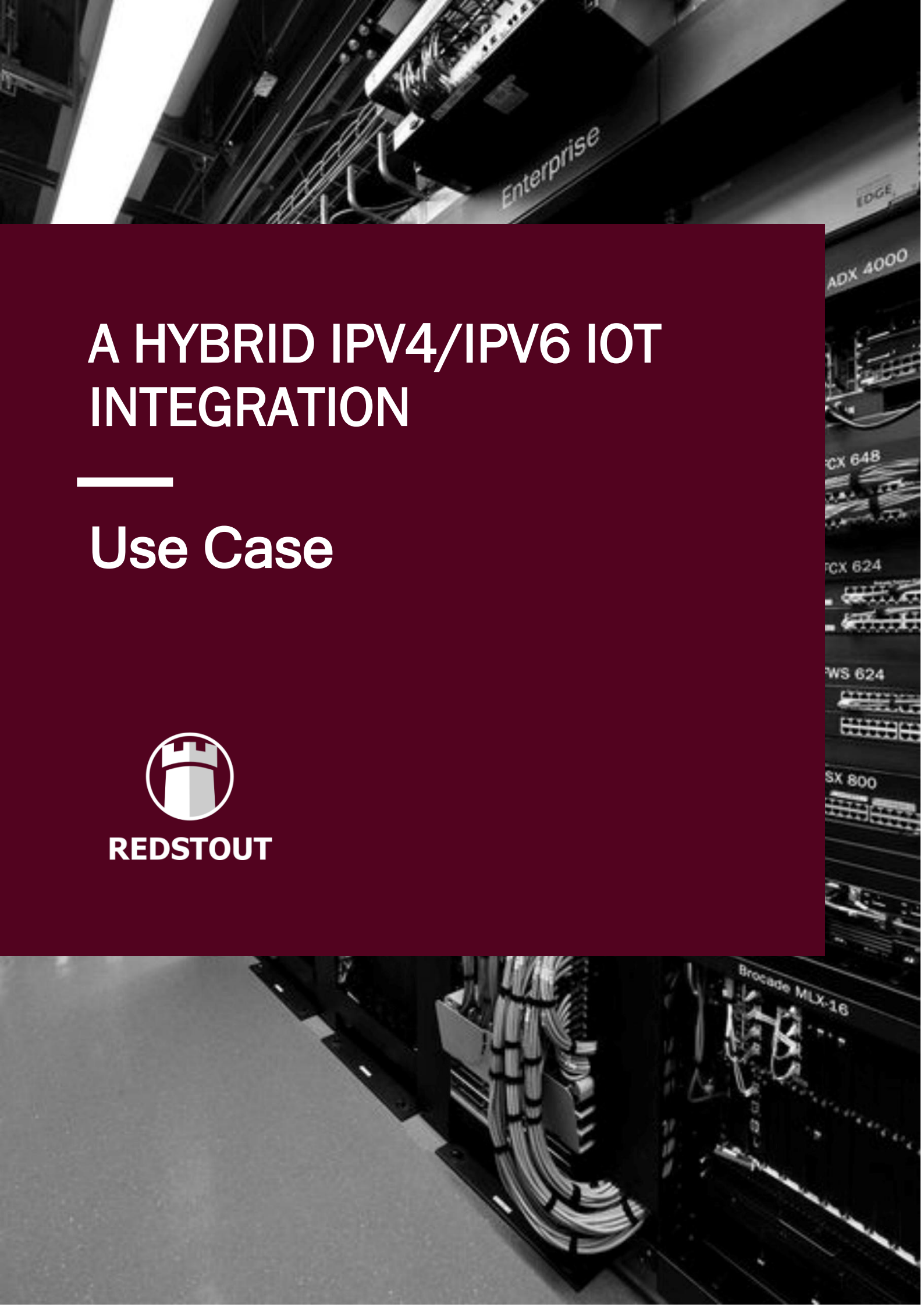


A HYBRID IPV4/IPV6 IOT INTEGRATION

Use Case

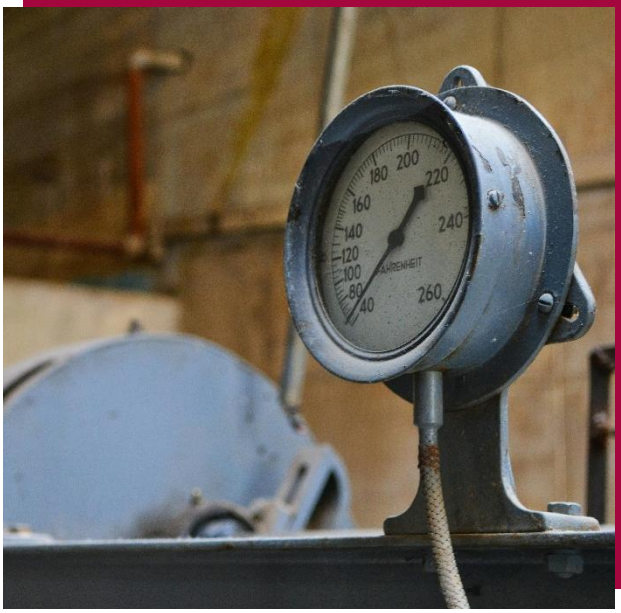
REDSTOUT

A HYBRID IPV4/IPV6 IOT INTEGRATION

REDSTOUT deployed a hybrid IPv4/IPv6 network architecture to achieve seamless integration, utilizing dual-stack configurations and translation mechanisms to ensure interoperability between the legacy IPv4 systems and the new IPv6-enabled IoT devices.

Background

A manufacturing company operated an IPv4-based enterprise network that supported critical applications, databases, and a VPN infrastructure for remote engineers. The company transformed digitally by deploying IoT devices across multiple geographically distributed facilities, including smart sensors, actuators, and real-time monitoring systems, replacing the oldest devices. These IoT devices were designed to operate on an IPv6 network due to their scalability, efficient addressing, and improved security features.



However, the company's infrastructure remained heavily dependent on IPv4, creating interoperability challenges between the legacy systems and the newly deployed IPv6-based IoT ecosystem. A hybrid networking approach was required to ensure seamless communication, secure remote access, and uninterrupted data flow across the enterprise.

Challenges and Requirements

IPv4/IPv6 Interoperability

Ensuring IPv4 and IPv6 Communication for Legacy Systems

Traditional legacy applications and databases were initially designed to operate exclusively on IPv4 networks. However, with the proliferation of IPv6-enabled IoT devices, these systems faced interoperability challenges, requiring robust mechanisms to ensure seamless data exchange across differing network protocols.

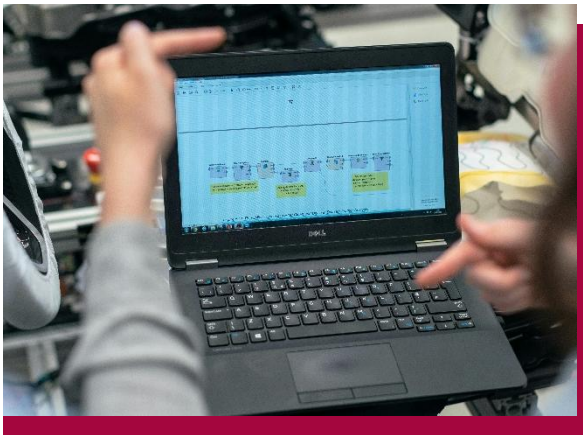
The network needed to enable seamless, bidirectional communication between IPv4-based enterprise services and IPv6-enabled IoT devices, ensuring interoperability without necessitating extensive modifications to existing applications.

Secure Remote Access for IPv6 Devices

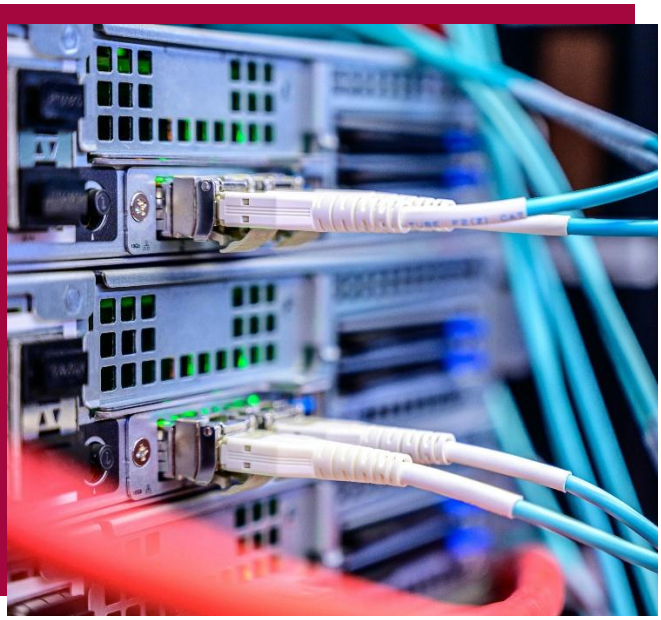
IPv6 Access for IPv4-Connected Engineers

The solution enabled IPv4-connected engineers to securely monitor, diagnose, and troubleshoot IPv6-enabled IoT devices, ensuring seamless operational oversight and maintenance.

Engineers and technicians remotely accessed the network through an IPv4-based VPN, ensuring secure connectivity while maintaining compatibility with legacy infrastructure.



Network Traversal Over an IPv4 Backbone



IPv6 Traffic Support on an IPv4 Backbone

The company's backbone network operated exclusively on IPv4 and needed to support the seamless transmission of IPv6 traffic without requiring major infrastructure overhauls.

IoT device data must be efficiently transmitted to centralized servers and cloud-based analytics platforms, ensuring real-time processing and actionable insights.

IPv4/IPv6 interoperability, secure remote access, and efficient IPv6 traffic traversal over an IPv4 backbone without major infrastructure changes.

The solution enabled seamless **IPv4/IPv6 interoperability**, allowing legacy IPv4 applications to communicate with IPv6-enabled IoT devices without significant modifications. It provided **secure remote access**, allowing IPv4-based VPN users to monitor and troubleshoot IPv6 devices. Additionally, it supported **IPv6 traffic traversal over an IPv4 backbone**, ensuring efficient data transmission to centralized servers and cloud platforms without requiring extensive infrastructure changes.

Solution Architecture

REDSTOUT designed a hybrid networking strategy to address these challenges, incorporating dual-stack infrastructure, protocol translation, and tunneling mechanisms.

Deploying Dual-Stack Gateways

Dual-stack routers and gateways were deployed at each remote site to bridge IPv4 and IPv6 networks, enabling communication, optimizing traffic flow, and ensuring compatibility with legacy and modern systems.

These devices supported advanced IPv4 and IPv6 routing capabilities, ensuring seamless interoperability between IPv6-enabled IoT devices and IPv4-based services while optimizing performance, maintaining security, and enabling efficient traffic management across the network.

Ensuring IPv4 and IPv6 Communication for Legacy Systems

Network segmentation was implemented to effectively isolate IPv4 and IPv6 traffic, enhancing security, optimizing performance, and reducing potential conflicts. It also enabled controlled and necessary logical cross-communication to maintain seamless interoperability between both network protocols.

NAT64 and DNS64 for Protocol Translation

NAT64 and DNS64 were deployed to enable IPv6-to-IPv4 translation and service discovery, ensuring interoperability between legacy IPv4 applications and IPv6-enabled IoT devices without requiring modifications or disrupting network efficiency.

NAT64 was deployed at network edge gateways to seamlessly translate IPv6 traffic from IoT devices into IPv4 packets, ensuring full compatibility with legacy services while maintaining network efficiency and minimizing latency.

DNS64 was implemented to dynamically generate synthetic IPv6 addresses for IPv4-based resources, enabling seamless service discovery and connectivity for IPv6-enabled IoT devices while reducing the need for manual configurations.

This approach ensured that existing IPv4 applications could continue operating without requiring modifications while simultaneously enabling smooth communication with IPv6 devices, preserving infrastructure investments, and future-proofing the network for gradual IPv6 adoption.

IPv4 VPN Integration with IPv6 Networks

The IPv4 VPN infrastructure was extended and fortified with NAT64, DNS64, and advanced security policies, enabling remote engineers to securely access and manage IPv6-based IoT devices while maintaining seamless interoperability and strict access control.

The existing IPv4 VPN infrastructure was enhanced and extended to support remote engineers securely accessing IPv6-based IoT devices, ensuring seamless connectivity without requiring major network reconfigurations.

Edge gateways equipped with NAT64 and DNS64 facilitated transparent communication between VPN-connected engineers and IPv6-enabled IoT devices, enabling effortless interaction while preserving compatibility with legacy systems.

Robust VPN policies and firewall rules were meticulously configured to enforce strict access control, segment network traffic, and implement advanced security measures, ensuring that only authorized engineers could securely access and manage IoT devices.

Tunneling IPv6 Traffic Over an IPv4 Backbone

A tunneling mechanism utilizing 6in4 encapsulation was implemented to enable seamless, secure end-to-end IPv6 communication over the company's IPv4-only backbone.

Given that the company’s backbone network was exclusively IPv4, an efficient tunneling mechanism was implemented to seamlessly transport IPv6 traffic, ensuring interoperability without major infrastructure overhauls.

6in4 tunnels were strategically deployed to encapsulate IPv6 packets within IPv4, enabling reliable, end-to-end IPv6 communication across the existing IPv4 backbone while minimizing latency and maintaining network performance.

This approach ensured that IoT data from remote sites could securely traverse the IPv4 backbone and reach centralized processing systems and cloud environments, eliminating the need for an immediate full-scale IPv6 migration while maintaining

Implementation Considerations

REDSTOUT designed a hybrid networking strategy to address these challenges, incorporating dual-stack infrastructure, protocol translation, and tunneling mechanisms.

Security and Access Control

1. Firewall policies were updated to filter and inspect IPv4 and IPv6 traffic, ensuring network security.

2. Access control lists (ACLs) were configured on dual-stack gateways to restrict unauthorized traffic between IPv4 and IPv6 segments.

3. VPN authentication mechanisms (e.g., MFA, certificate-based authentication) were enforced for remote engineers accessing IoT devices.

Network Performance Optimization

1. Traffic monitoring and QoS policies were established to ensure efficient handling of IPv6 IoT traffic without affecting legacy applications.

2. Load balancing was implemented across dual-stack gateways to prevent bottlenecks in protocol translation.

Scalability and Future Readiness

1. The hybrid architecture allowed for incremental IPv6 adoption, ensuring the company could transition to full IPv6 at a controlled pace.

2. Additional IoT devices and smart infrastructure were seamlessly integrated without network reconfiguration.

3. As cloud-based services increasingly adopted IPv6, the architecture ensured long-term compatibility.

Conclusions

A robust hybrid IPv4/IPv6 architecture enabled interoperability, secure remote access, and efficient IoT data transmission, ensuring a scalable, secure, and future-proof foundation for digital transformation and IoT expansion.

By implementing a robust hybrid IPv4/IPv6 architecture incorporating dual-stack gateways, NAT64/DNS64 translation, VPN integration, and 6in4 tunneling, the manufacturing company successfully modernized its operations while preserving the stability of existing services.

This comprehensive solution enabled seamless interoperability between legacy applications and IPv6-enabled IoT devices, facilitated secure and efficient remote access for engineers, and ensured reliable transmission of IoT data across the IPv4-only backbone network.

Additionally, advanced network segmentation, strict access controls, and optimized traffic management enhanced security, performance, and scalability. This approach established a resilient, future-proof foundation for ongoing digital transformation, supporting the company’s long-term IoT expansion and technological innovation.