

BalticNOG 2025

Wednesday, September 24, 2025 - Thursday, September 25, 2025

AC Hotel by Marriott Vilnius

Scientific Program

Network Security

BGP Security, Hijacks, and Route Leaks

Explores vulnerabilities in the Border Gateway Protocol, focusing on incidents of route hijacking and leaks, and discusses mitigation strategies to enhance routing security.

DDoS Mitigation and Cybersecurity Trends

Addresses the latest trends in cybersecurity, with an emphasis on Distributed Denial of Service attacks, their evolving tactics, and effective defense mechanisms.

Internet Protocols and Deployment

IPv6 Deployment and Transition Strategies

Covers methodologies for transitioning from IPv4 to IPv6, including deployment planning, addressing architecture, and overcoming common challenges in adoption.

Internet Routing and Interconnection

Focuses on the dynamics of internet routing, inter-AS relationships, and strategies to optimize interconnection for improved performance and resilience.

IP Leasing, RPKI, and Resource Management

Discusses the practices of IP address leasing, the implementation of Resource Public Key Infrastructure for route validation, and effective management of IP resources.

Network Automation and Emerging Technologies

Network Automation and AI in Networking

Explores the integration of automation tools and artificial intelligence in network management, aiming to enhance efficiency, reduce human error, and enable self-optimizing networks.

Data Center and Cloud Networking

Examines the architectures and technologies underpinning modern data centers and cloud environments, including virtualization, software-defined networking, and scalability solutions.

Connectivity and Infrastructure

Peering, IXPs, and Regional Connectivity

Investigates the role of peering agreements, Internet Exchange Points, and strategies to enhance regional connectivity, aiming to improve latency and bandwidth for end-users.

Policy and Regulation

Regulatory and Policy Developments

Analyzes recent changes in telecommunications policies and regulations, assessing their impact on network operations, data privacy, and the broader internet ecosystem.

Cybersecurity and Network Resilience in Conflict Zones

Cyber Warfare and Infrastructure Protection Amidst the Conflict Areas

This track examines cybersecurity challenges in regions facing armed conflicts, focusing on cyber warfare tactics, critical infrastructure protection, and strategies to enhance network resilience based on lessons learned from recent incidents.