

KRNIC Update

Feb, 2026

Korea Network Information Center
Lee, Han Sang

CONTENTS

- I Internet Number Resources Statistics**
- II KRNIC's RPKI Deployment Roadmap and Activities**

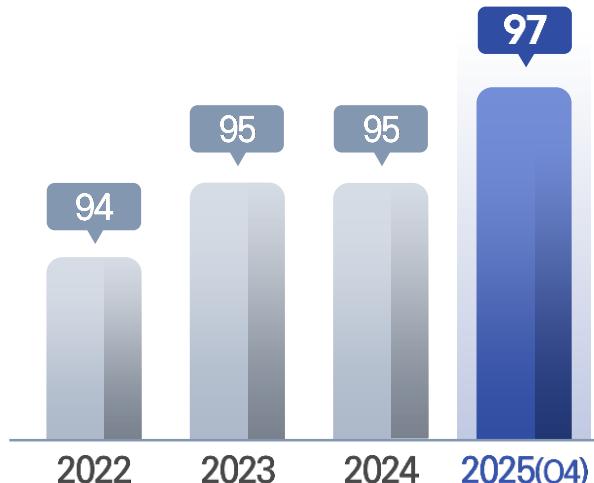
I

Internet Number Resources Statistics

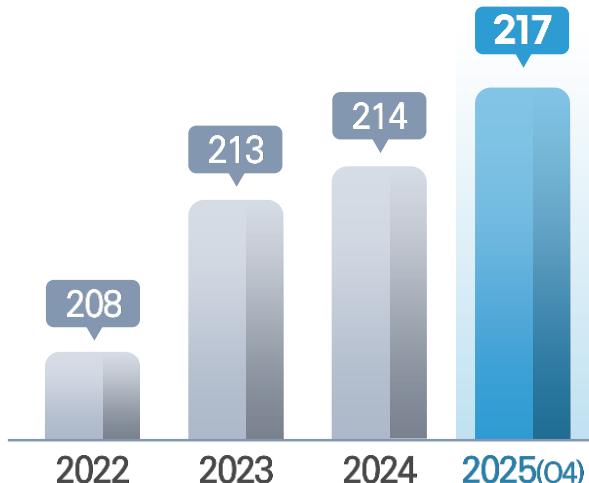
I Statistics on KRNIC Members.

Members

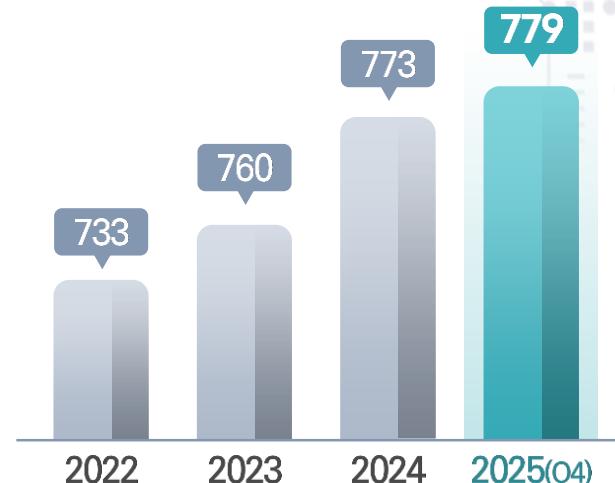
Internet Registries(ISP)



Direct Assignment Users

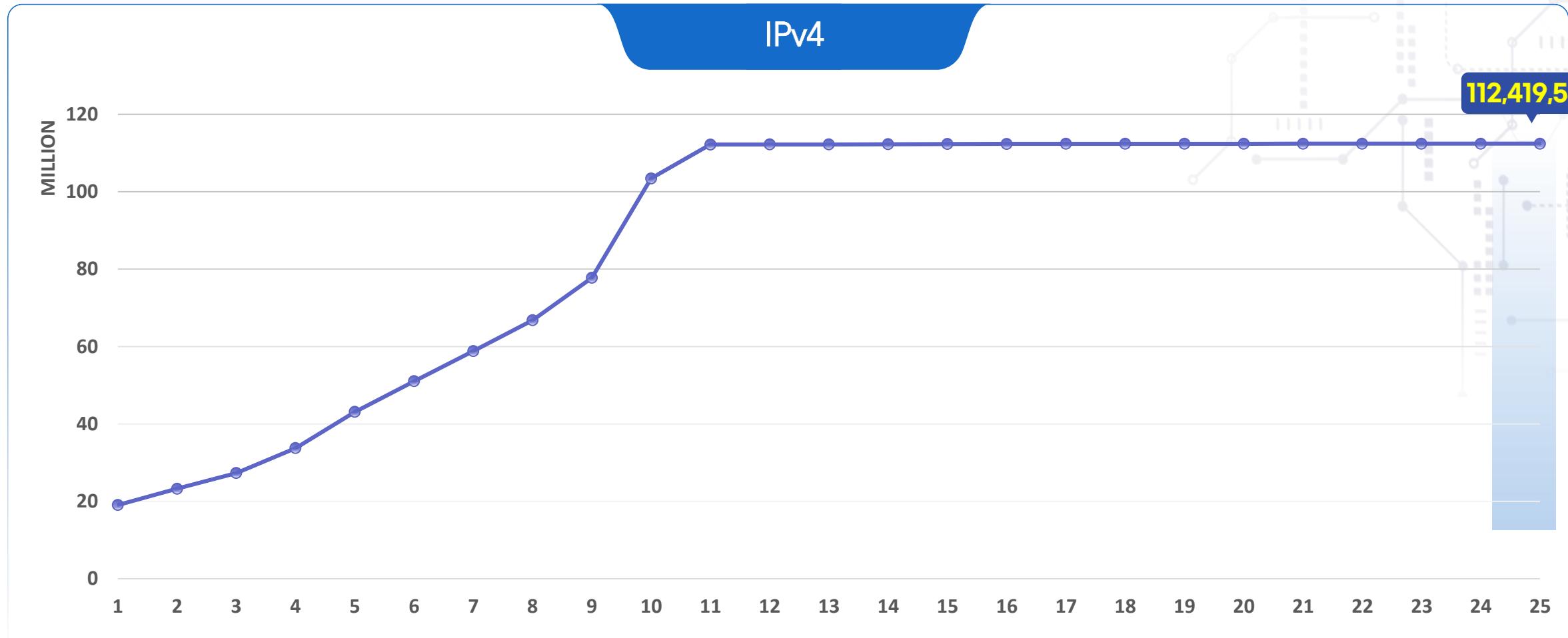


ASN Users



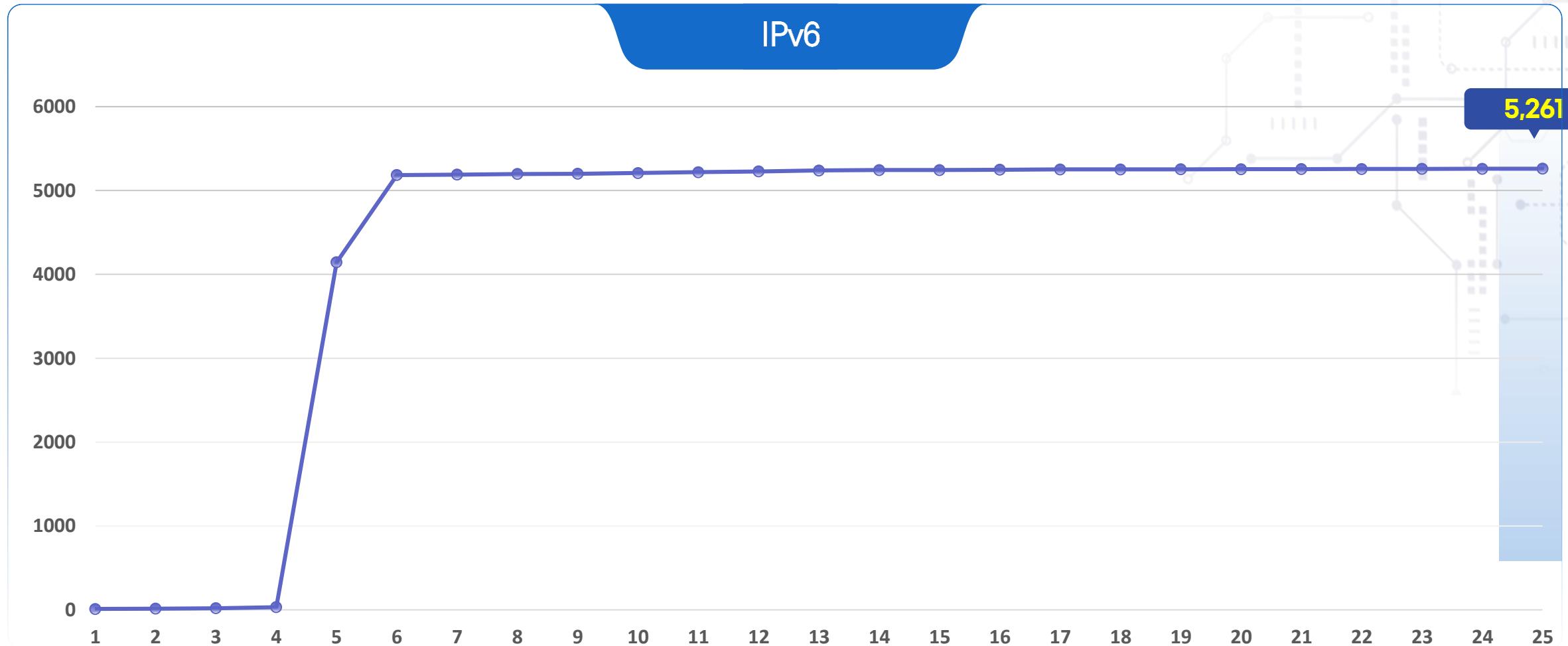
As of Q4 2025, KRNIC has a total **1,093** members.

I Statistics on IPv4 Allocations



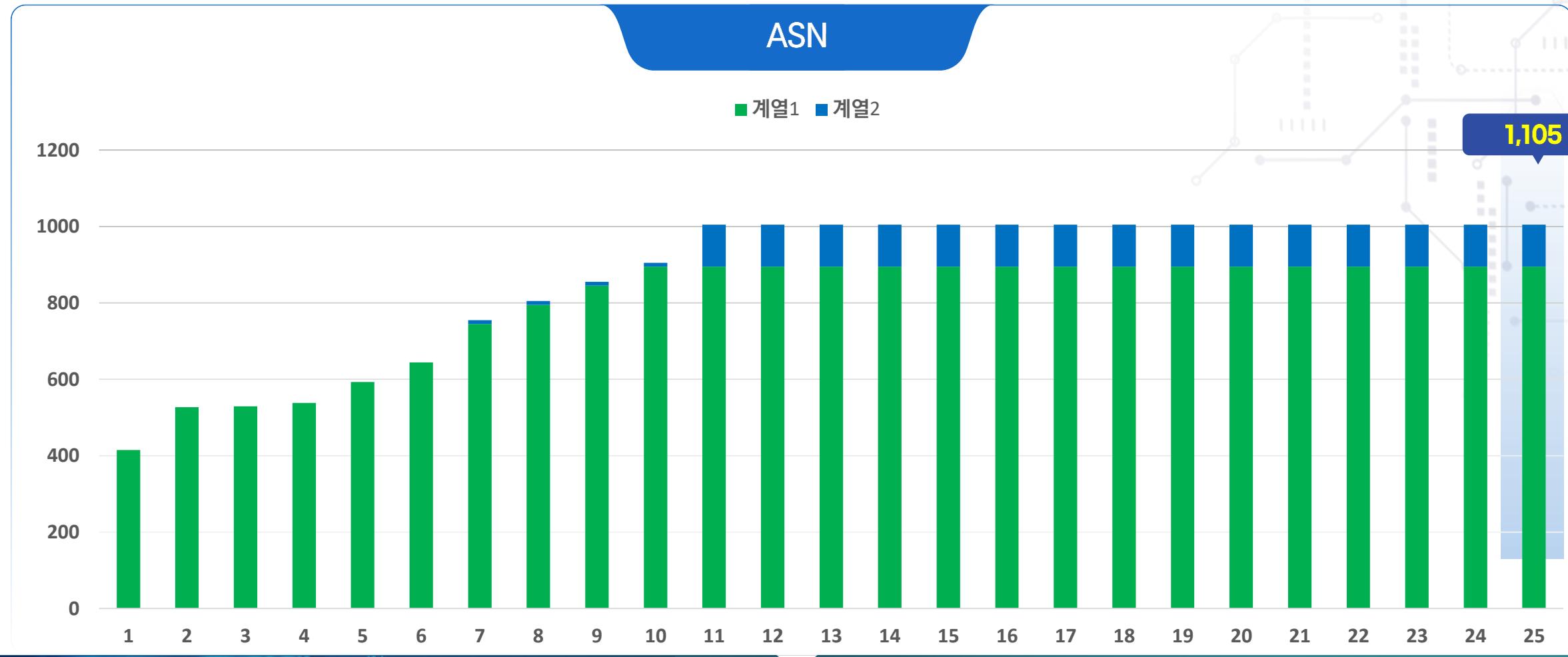
As of Q4 2025, KRNIC has allocated **112,419,584** IPv4 addresses.

I Statistics on IPv6 Allocations



As of Q4 2025, KRNIC has allocated **5,261** IPv6 addresses. (/32)

I Statistics on ASN Allocations



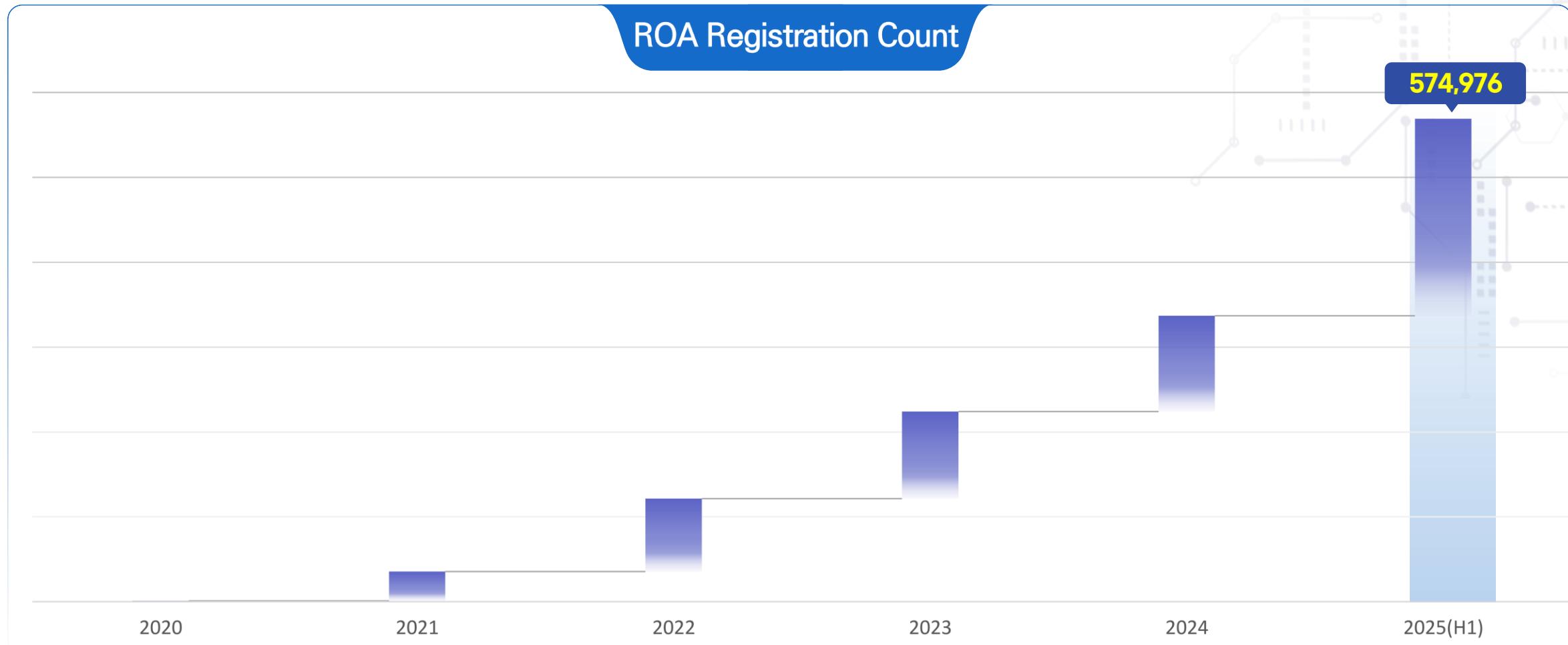
As of Q4 2025, KRNIC has allocated **1,105** ASNs. (2-byte: 895, 4-byte: 210)



II

KRNIC's RPKI Deployment Roadmap and Activity

I Number of ROA-Registered IPv4 in Korea



Korea's ROA-Registered Count is very low (2%)

II KRINC's RPKI Deployment Roadmap

Step 1 (2026)

Step 2 (2027)

Step 3 (2028~)

Preparation & Foundation

Pilot & Implementation

Expansion & Global Collaboration



RPKI Testbed System

Establishment & Preparation

Development & Pilot Operation

Expansion & Advancement

ISMP for RPKI System

Mgmt & Operation Pilot RPKI System

Wider Adoption for Service Providers



RPKI Deployment & Management

Promotion with Large ISPs

Expansion to SMEs & Cooperation

Global Collaboration

Promote & Expand RPKI, Connecting NOGs

III KRNIC's RPKI Routing Security Testbed

What is the RPKI Routing Security Testbed?

The RPKI Routing Security Testbed is a “virtual proving ground” where you can safely test routing security technologies before deploying them on the live Internet, preventing attackers from tampering with routing information like road signs on a highway.

It provides a controlled lab environment to emulate real-world Internet routing conditions and to validate that RPKI-based protection works as intended without impacting production traffic.



The RPKI Routing Security Testbed provides test equipment and full configuration support for routing security technologies like RPKI. It creates a structured environment to systematically validate RPKI deployment, performance evaluation, and incident response readiness.



01. Provision of a virtualized testbed infrastructure that reflects the global standard RPKI architecture



02. Simulation of realistic route hijacking attack scenarios to verify the effectiveness of RPKI deployment



03. Hands-on practice in building ROA registration and validation servers tailored to the domestic environment, enabling a safe transition to RPKI



04. Delivery of quantitative analysis reports based on empirical test data to support the definition of objective operational targets



05. Reservation and administrative support for the testbed, with priority given to organizations mandated to adopt RPKI

Purpose of the RPKI Routing Security Testbed

The testbed is designed to support reliable and secure adoption of RPKI through realistic mock deployments and systematic evaluation.

By enabling pre-deployment design, configuration, and assessment, it helps operators reduce the risk of misconfiguration, route hijacking, and other routing incidents when rolling out RPKI in production networks.



Securing stable RPKI deployment capabilities through pre-validation testing

Hands-on RPKI implementation practice in a virtual lab environment builds the technical expertise needed for reliable rollout.



Identifying RPKI deployment failure points and operational caveats

Through pre-production testbed simulations, operators can proactively detect and eliminate potential exception scenarios and latent failure factors before live deployment.



Support for establishing performance metrics and maintenance objectives

Leveraging performance and stability validation data from testbed experiments, operators can define optimized performance indicators and efficient maintenance targets tailored to their production environments.

III KRNIC's RPKI Routing Security Testbed

RPKI Routing Security Experiment Application Process

This portal enables organizations to request and track access to a secure virtual environment for safely testing RPKI, the critical technology that protects Internet routing paths from hijacking and manipulation.

Experiment Application Workflow

Home > Experiment Application and Status > Experiment Application

Experiment Application

RPKI Application Steps: Step 1 Schedule, Step 2 Objectives, Step 3 Operation Method, Step 4 Description

Step 1 / Step 4

Experiment Schedule

Select experiment dates: 2026-01-16 ~ 2026-01-19

Cancel Next

Step 1: Select Experiment Schedule

RPKI Application Steps: Step 1 Schedule, Step 2 Objectives, Step 3 Operation Method, Step 4 Description

Step 2 / Step 4

Experiment Objectives

What is the purpose of the experiment?

RPKI Practice
 RPKI Fault Response Training
 BGP Hacking Response Training

Cancel Back Next

Step 2: Define Experiment Objectives

RPKI Application Steps: Step 1 Schedule, Step 2 Objectives, Step 3 Operation Method, Step 4 Description

Step 3 / Step 4

Experiment Operation Method

Select the experiment operation method!

01. Will you operate the Validator (Relying Party) yourself?
 Yes No

02. Do you have an AS (Autonomous System) in operation?
 Yes No

03. Please enter the ASN of the AS you are operating!

Cancel Back Next

Step 3: Review Experiment Operations

RPKI Application Steps: Step 1 Schedule, Step 2 Objectives, Step 3 Operation Method, Step 4 Description

Step 4 / Step 4

Write Experiment Description

Please write the experiment details!

Describe the experiment's objective

Cancel Back Submit Application

User Portal : Experiment Application & Status Dashboard

Routing Security Validation Service

Experiment Application and Status

ROUTING SECURITY TESTBED
BGP HACKS DEFENSE SIMULATION
RPKI VALIDATION ACTIVE

Experiment Application and Status

Enter search terms

Experiment Application

Reservation Number	Experiment Start Date	Experiment End Date	Application Status	Experiment Status
5	2025-03-01	2025-03-17	Rejected	Rejected
4	2025-03-01	2025-03-15	Pending	Pending
3	2025-03-01	2025-03-10	Approved	In Progress
2	2025-03-05	2025-03-10	Approved	Ended
1	2025-03-07	2025-03-08	Approved	Ended

KISA

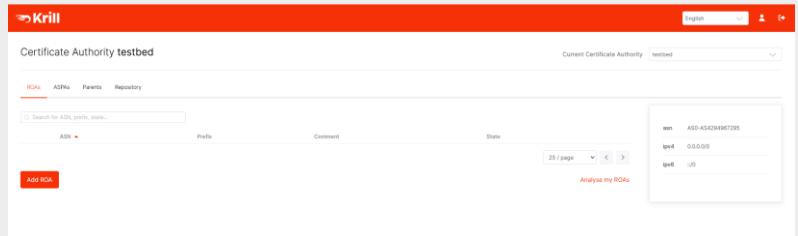
12

III KRNIC's RPKI Routing Security Testbed

ROA Issuance in Test Environment

Designates which networks are authorized to use specific IP address blocks, generating Route Origin Authorization(ROA) records to establish legitimate path ownership.

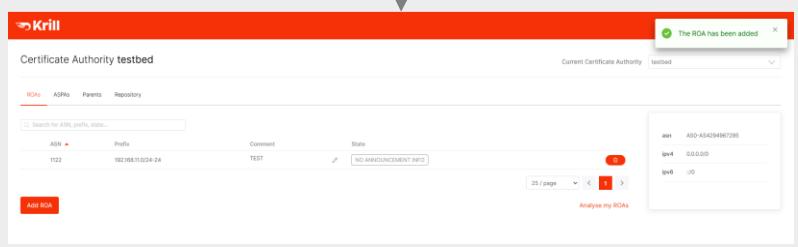
ROA Registration Workflow



[Pre-ROA Registration]



[ROA Registration]

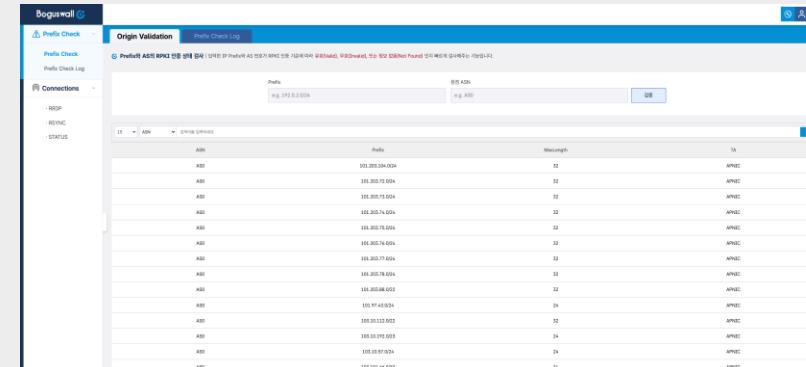


[ROA Registration Complete]

Test Environment Relying Party(RP) Deployment

Deploys Relying Party(RP) software to validate BGP route legitimacy, integrating with routers to activate the full RPKI security framework.

RP Deployment Screens(using Boguswall Commercial RP Solution)



[Relying Party(RP) Installation]

CISCO terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router# config terminal
Router(config)# router bgp 65001
Router(config-router)# bgp rpki server 192.168.10.100 port 3323 refresh 60
Router(config-router)# address-family ipv4
Router(config-router-af)# bgp bestpath prefix-validate allow-invalid
Router(config-router-af)# end
Router#
#SYS-5-CONFIG_I: Configured from console by console
Router# show ip bgp rpki servers

Server	Port	State	Rcvd	Refr	Last
192.168.10.100	3323	ESTAB	14500	60	00:05:21

VyOS
vyos@vyos:~\$ show ip bgp ... x0_64
vyos@vyos:~\$ configure
[edit] vyos@vyos:~# set protocols rpki cache 192.168.10.100 port '3323'
vyos@vyos:~# set protocols rpki cache 192.168.10.100 preference '10'
vyos@vyos:~# set protocols rpki [protocols rpki]
Starting RPKI...
vyos@vyos:~# save
Saving configuration to '/config/config.boot'...
Done
vyos@vyos:~# exit
exit
vyos@vyos:~\$ show rpki cache-connection
Connected to group 192.168.10.100(3323)
Type : TCP
State : Up
Entries : 14500
Preference: 10

Juniper terminal
Edit mode
[edit] root@mx-router# set routing-options validation group RPKI-MAIN session 192.168.10.100 port 3323
root@mx-router# set routing-options validation group RPKI-MAIN session 192.168.10.100 refresh-time 60
root@mx-router# commit
root@mx-router# exit
Exiting configuration mode
root@mx-router# show validation session
Session 192.168.10.100 State up Flaps 0 Uptime 00:01:23 #IPv4/IPv6 14500/0

[Pre-Router RP Configuration Dashboard]

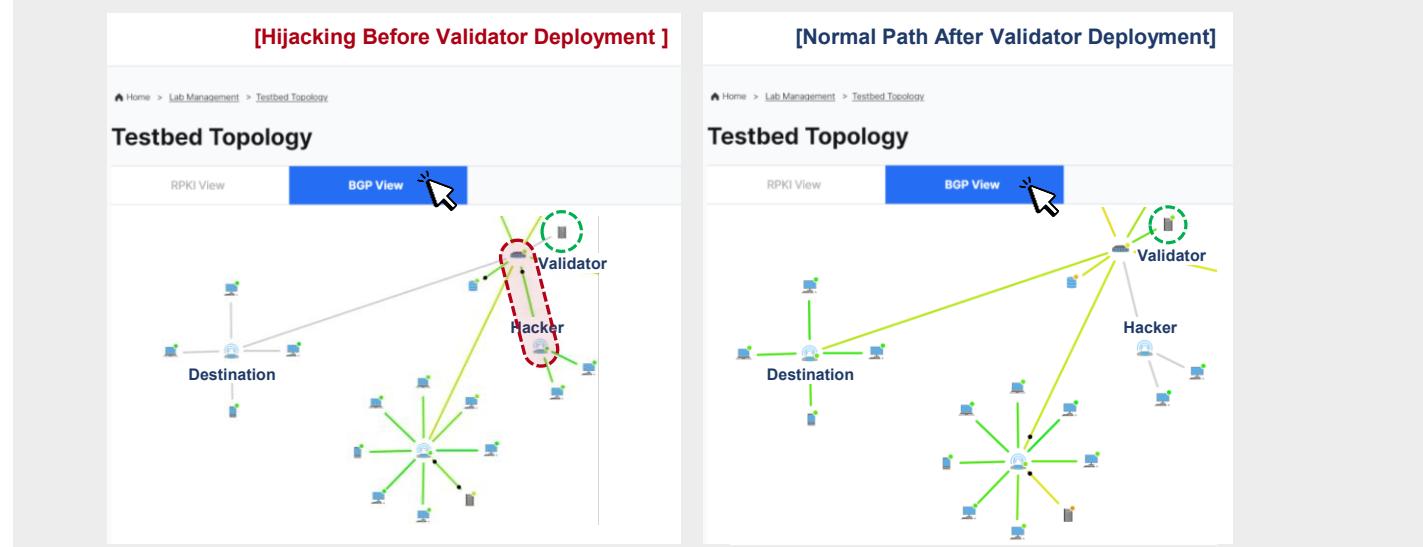
III KRNIC's RPKI Routing Security Testbed

BGP Hijacking Response Experiment

Interactive Visualization Dashboard

Designates which networks are authorized to use specific IP address blocks, generating Route Origin Authorization(ROA) records to establish legitimate path ownership.

Experiment Topology View(Testbed)
– BGP Perspective
BGP Hijacking scenario: Before & After RPKI deployment

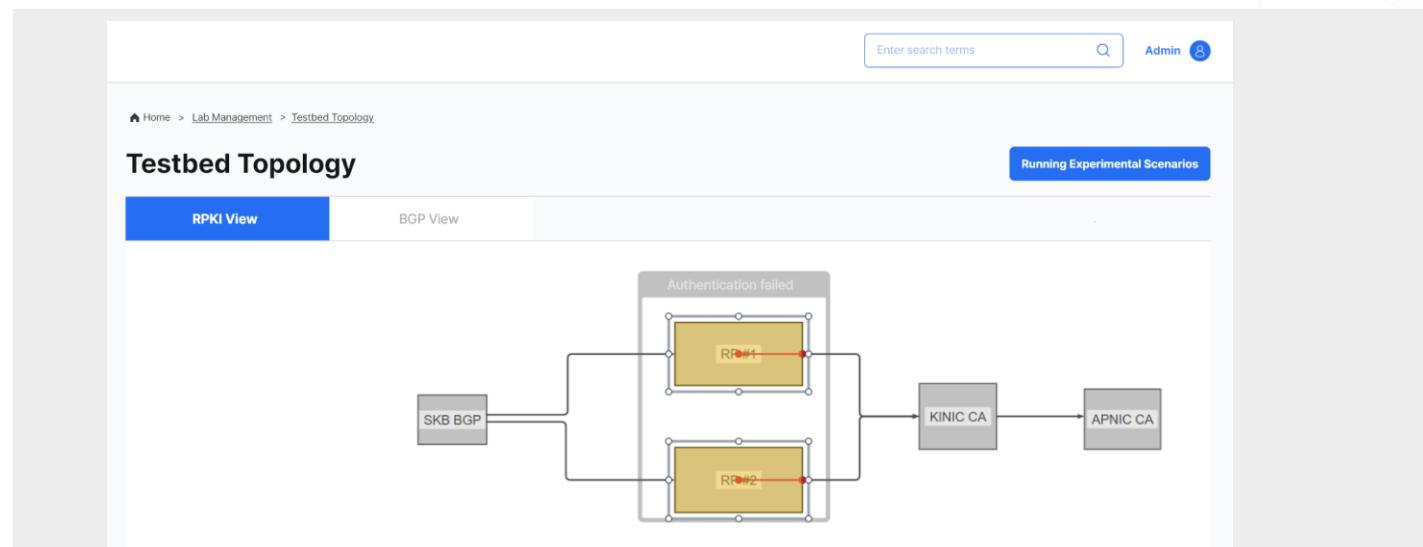


RPKI Routing Security Monitoring Practice

Real-time Validation Dashboard

Monitors whether your network (AS) is properly registered in RPKI and displays route validation status (Valid/Invalid/Unknown)

Experiment Topology View(Testbed)
– RPKI Perspective



III KRNIC's RPKI Routing Security Testbed

Results Report

Provides pass/fail reporting across 20 evaluation criteria covering key RPKI deployment procedures, enabling comprehensive learning and competency assessment of the RPKI implementation process

A faint, light-gray network diagram with various nodes (represented by circles) and lines (represented by dashed lines) forming a complex web, serving as a background for the report's content.

[Home](#) > [Experiment Monitoring](#) > [Experiment Result Report](#)

Experiment Result Report

[Summary Report](#) [Detailed Experiment Results](#)

Practice Items

ROA Registration

01. Did you accurately enter the ROA information?	00.00.00.00/00	00 AS00000 etc. (4 items)	●
02. Did you verify the validity period after ROA registration?		Not Checked	●
02. Did you check the time taken for the ROA to be applied within the RPKI system?		1 minute 22 seconds	●

RP (Relying Party) Configuration

01. Did you verify the TAL (Trust Anchor Locator) settings?	Checked	●
02. Did you check the ROA linkage status?	Checked	●

RP (Relying Party) Configuration

01. Did you verify the BGP Hijacking results without RPKI applied?	Checked	●
02. Did you verify the BGP Hijacking results after applying RPKI?	Checked	●

Q&A