Towards More Accurate and More Automatic Source Address Validation in the Internet

SAVNET@APNIC 2023.03

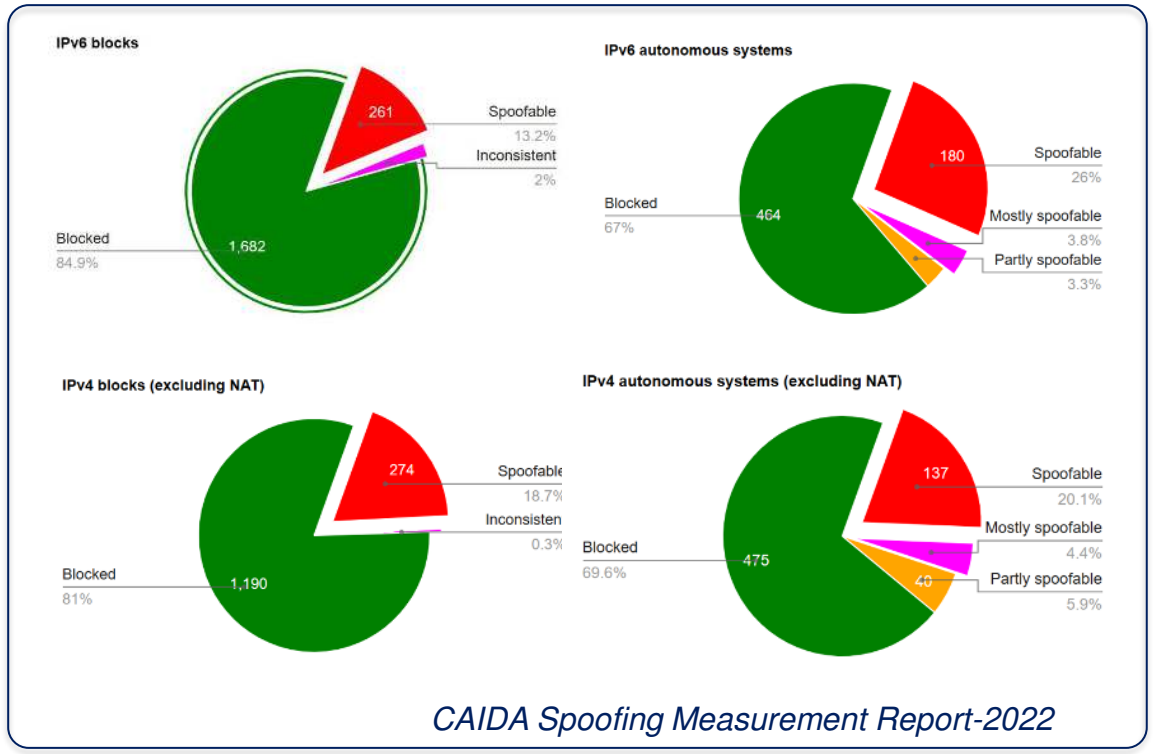
Fang Gao

Agenda

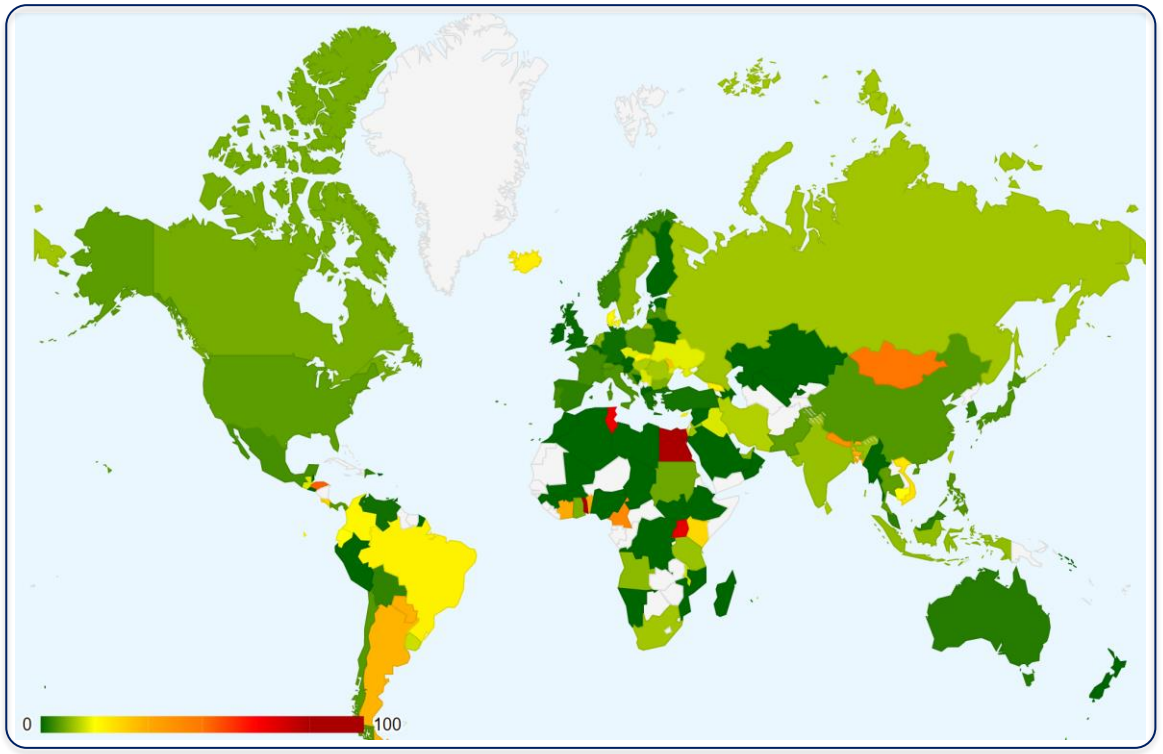
- **IP Spoofing Situation on Internet**
- Existing SAV Mechanisms and Gap Analysis
- Desired Features to Narrow Gaps
- Preliminary Architecture of compatible SAV
- SAVNET@IETF

The Latest State of IP Spoofing on Internet

CAIDA Spoofing Measurement-2022



CAIDA Spoofing Measurement Report-2022

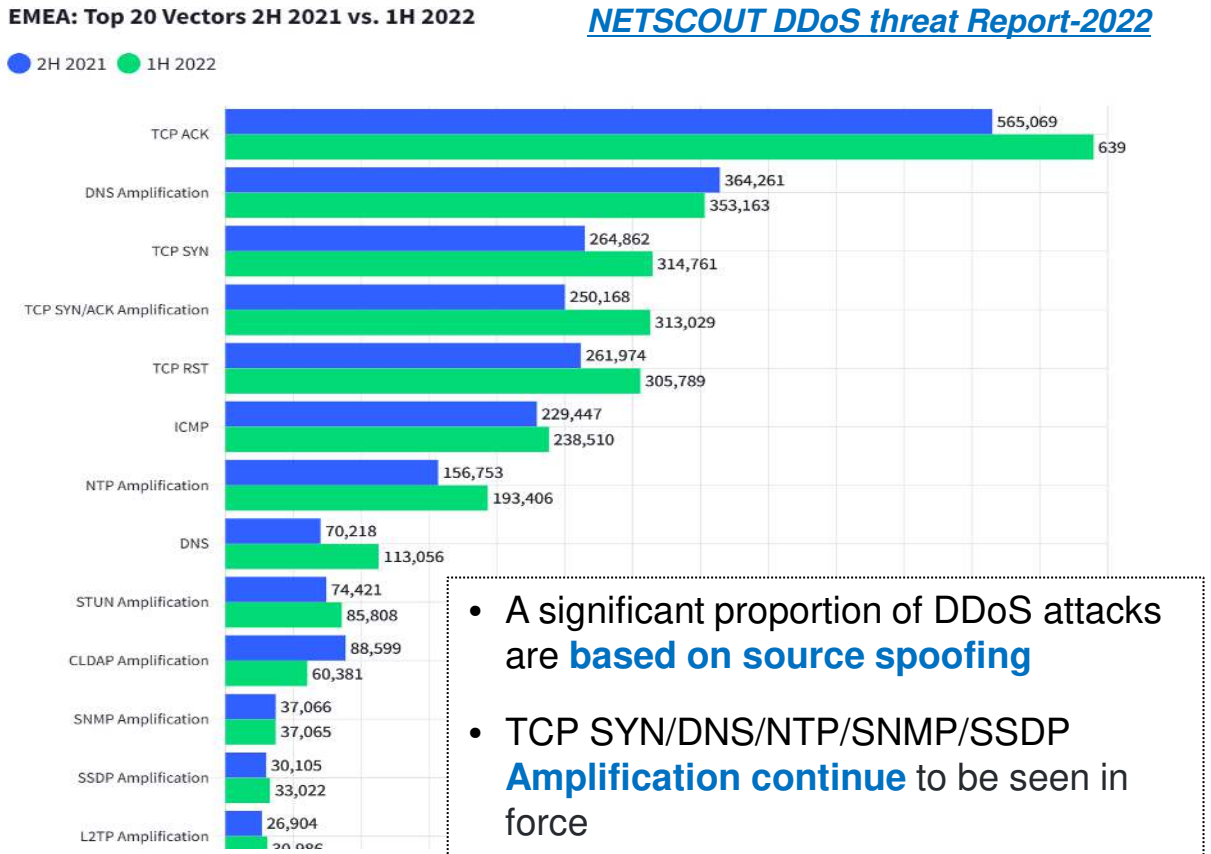


- 13.2% of IPv6 addresses and 18.7% of IPv4 addresses are spoofable
- 26% of IPv6 ASes and 20% of IPv4 ASes are spoofable
- Inbound prevention on network are deployed less than outbound

- Region: Most of South America, parts of Africa and Asia are more susceptible to spoofing
- Region: Most of Europe, America and parts of Africa is stronger on prevention against spoofing

Learning from DDoS Threat Reports

Over the years, it has become easier, cheaper, and more accessible for attackers to launch DDoS attacks based on forged source address[1]:



- A significant proportion of DDoS attacks are **based on source spoofing**
- TCP SYN/DNS/NTP/SNMP/SSDP **Amplification continue** to be seen in force

- **Google** measured a record-breaking **UDP amplification** attack reaching **2.4 Tbps** in 2017;
- **AWS** suffers **CLDAP amplification**/reflection DDoS Attack with a volume of **2.3 Tbps** in 2020;
- NETSCOUT reports **134k DDoS** in UK in 1H 2022, and most are **spoofing attacks**;
- Cloudflare reports almost **half of** all network-layer DDoS attacks were **SYN floods(in first place)** in 2022 Q4, the source IP addresses may be **spoofed** (altered) by the attacker;
- Cloudflare reports **DNS floods and amplification** attacks came **in second place** after SYN flood in 2022 Q4, accounting for ~15% of all network-layer DDoS attacks;

Detection and validation of IP Spoofing on network are very important for defending against source address spoofing attacks and allowing accurate traceback

[1] Cloudflare DDoS threat report for 2022 Q4

Agenda

- IP Spoofing Situation on Internet
- **Existing SAV Mechanisms and Gap Analysis**
- Desired Features to Narrow Gaps
- Preliminary Architecture for Compatible SAV
- SAVNET@IETF

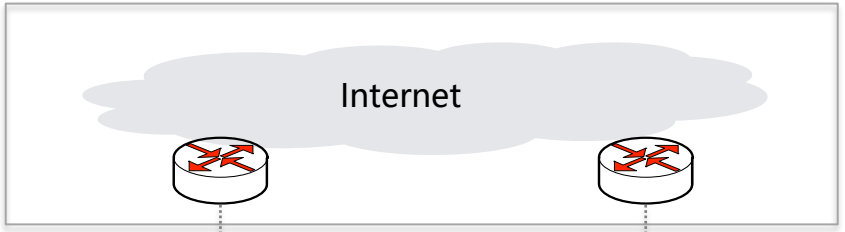
3 Levels in Current SAVA [1]

RFC 5210:

Network

SAV Functions

③ **Inter-Domain SAV**
(IP Prefixes granularity)



- **EFP-uRPF/FP-uRPF** [RFC8704]
- **Loose uRPF**[RFC3704]
- **VPN Mode-uRPF** [RFC8704]

② **Intra-Domain SAV**
(IP prefixes granularity)

Ingress filtering:
- **Strict-uRPF** [RFC3704]
- **ACL Filtering** [RFC2827]

① **Access-network SAV**
(Host granularity: IP, MAC,etc.)

- **SAVI** [2][RFC7039][RFC7513]
- **IPSG**

[1]SAVA: Source Address Validation Architecture
[2]SAVI: Source Address Validation Improvement

Difficult to require all access networks of all ISP and all customer to deploy SAVI effectively, effect of "Intra-domain SAV" and "Inter-domain SAV" is significant

Definition of Intra-Domain SAV and Inter-Domain SAV

Intra-Domain SAV

② ISP<->ISP Intf.

- ***Spoofed Traffic ② :***
  Blocking inbound traffic with CERNET's prefixes (P1) from other network/Internet

① ISP<->Customer Intf.

- ***Spoofed Traffic ① :***
  Preventing the outbound spoofed packets originated by the customer campus

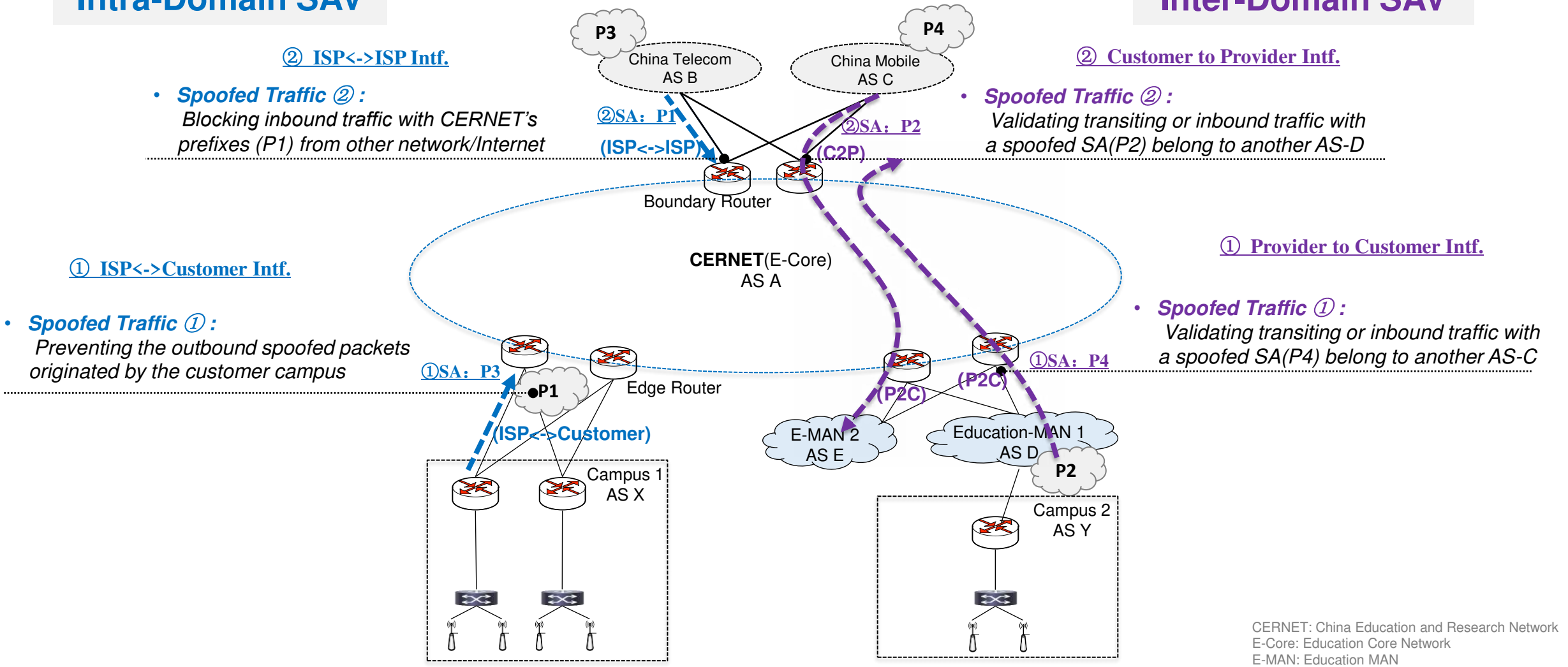
Inter-Domain SAV

② Customer to Provider Intf.

- ***Spoofed Traffic ② :***
  Validating transiting or inbound traffic with a spoofed SA(P2) belong to another AS-D

① Provider to Customer Intf.

- ***Spoofed Traffic ① :***
  Validating transiting or inbound traffic with a spoofed SA(P4) belong to another AS-C



CERNET: China Education and Research Network
E-Core: Education Core Network
E-MAN: Education MAN

Intra-domain SAV can be generate SAV rules by the network itself without collaboration between ASes;
Inter-domain SAV generate SAV rules by collaboration among ASes;

Gap Analysis of Existing SAV Mechanisms on CERNET

Intra-Domain SAV

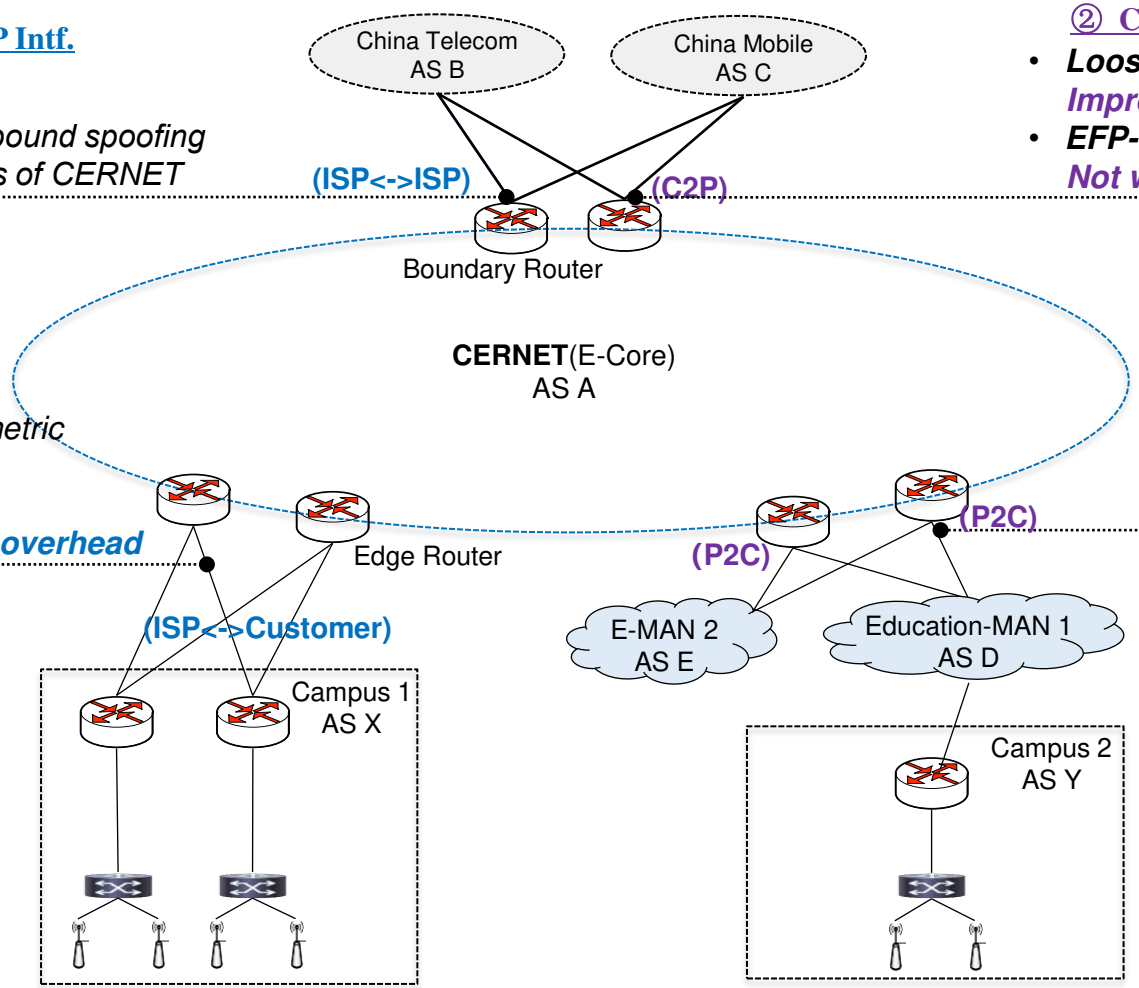
Inter-Domain SAV

② ISP<->ISP Intf.

- ***Loose uRPF:***
  Improper permit *for "inbound spoofing traffic" forging IP address of CERNET*

② Customer to Provider Intf.

- ***Loose uRPF:***
  Improper permit
- ***EFP-uRPF:***
  Not working *on Provider direction*



① ISP<->Customer Intf.

- ***Strict-uRPF:***
  Improper Block *in multi-homing /asymmetric routing scenario*
- ***ACL-based ingress filtering:***
  Manual *configuration &* ***high maintains overhead***

① Provider to Customer Intf.

- ***EFP-uRPF:***
  Improper Block *in BGP "No Export" scenario from AS-Y;*
  Improper Block *for Hidden prefix in DSR*

CERNET: China Education and Research Network
E-Core: Education Core Network
E-MAN: Education MAN

Intra-domain SAV can be generate SAV rules by the network itself without collaboration between ASes;
Inter-domain SAV generate SAV rules by collaboration among ASes;

Agenda

- IP Spoofing Situation on Internet
- Existing SAV Mechanisms and Gap Analysis
- **Desired Features to Narrow Gaps**
- Preliminary Architecture of Compatible SAV
- SAVNET@IETF

Desired Features to Narrow Gaps

Intra-Domain SAV

② ISP<->ISP Intf.

- *Generate rules for IP prefixes of CERNET network for inbound SAV*

① ISP<->Customer Intf.

- *Generate SAV rules in asymmetric scenario/ multi-homing automatically*
- *Update SAV rules dynamically in real time according to changes*

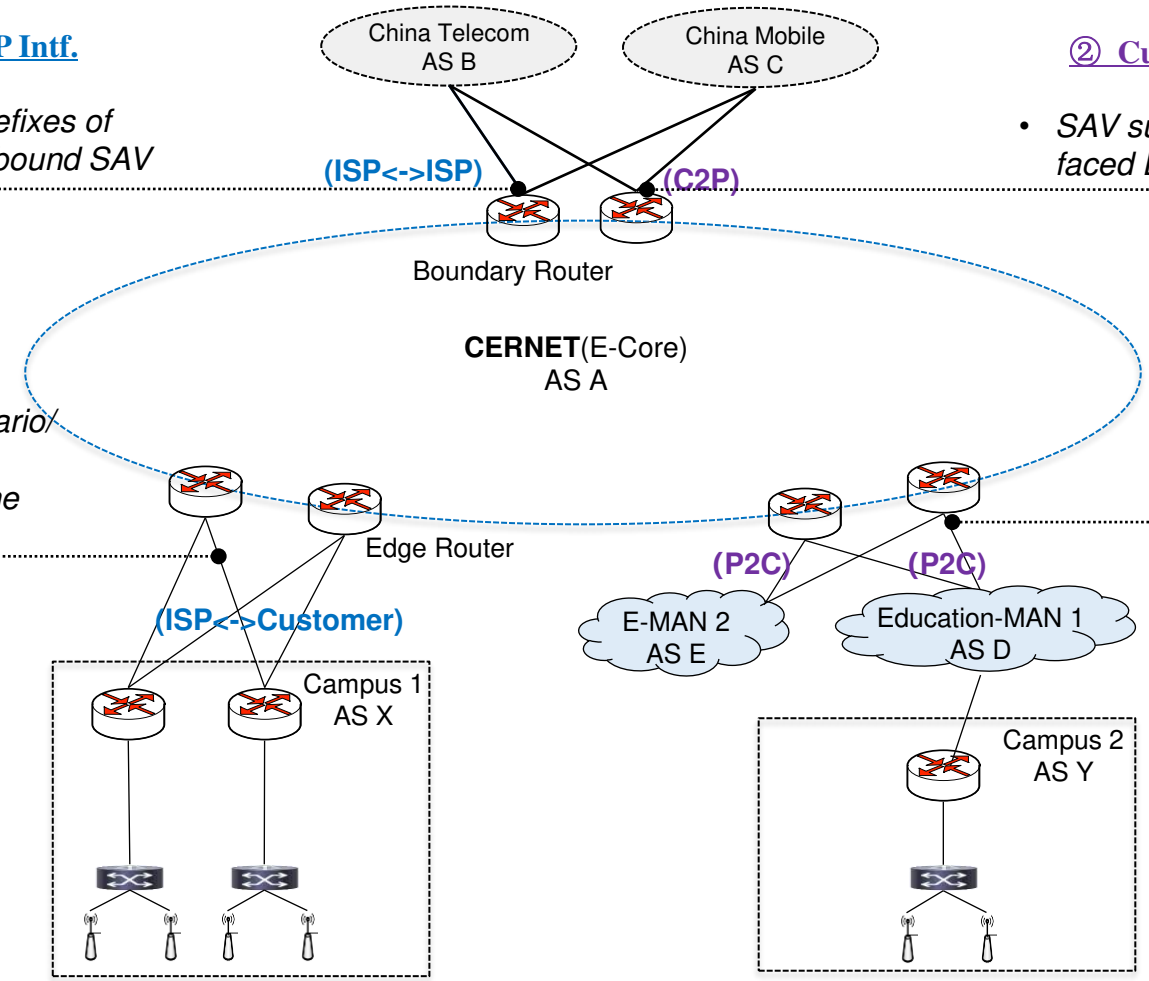
Inter-Domain SAV

② Customer to Provider Intf.

- *SAV supported on Provider/Peer faced Directions*

① Provider to Customer Intf.

- *Accurate SAV in typical BGP "No Export" Scenario*
- *Accurate SAV for Hidden prefixes in DSR*

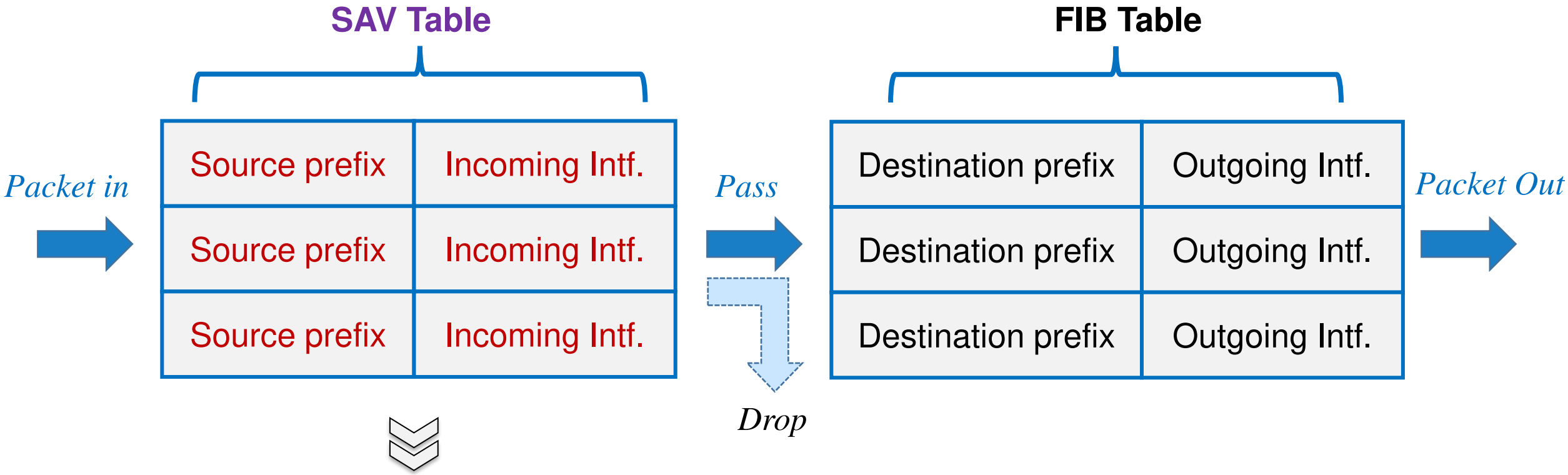


Try to Automatically generate Accurate SAV rules on all-directions in both asymmetric network and dynamic network.

Agenda

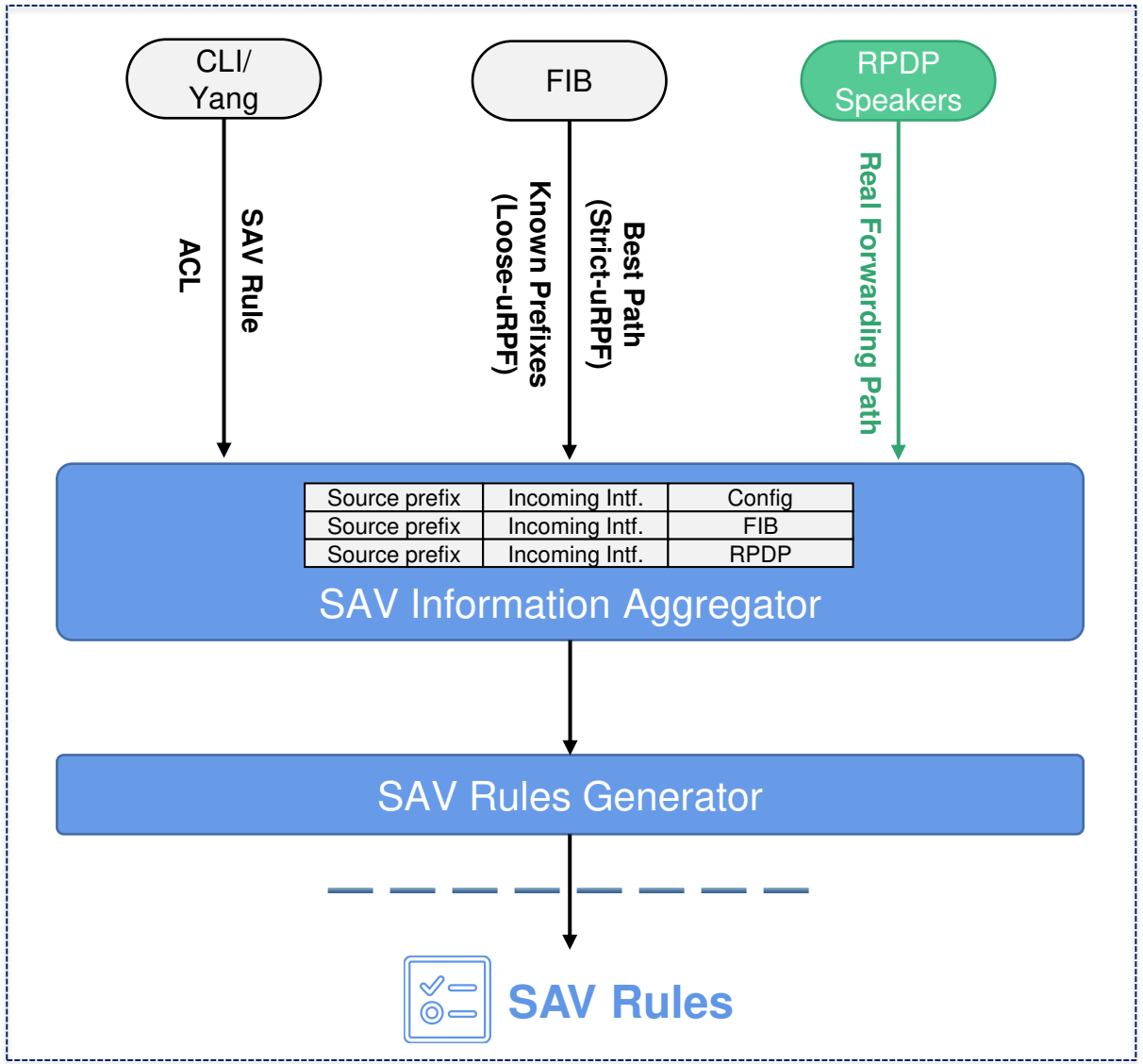
- IP Spoofing Situation on Internet
- Existing SAV Mechanisms and Gap Analysis
- Desired Features to Narrow Gaps
- **Preliminary Architecture of Compatible SAV**
- SAVNET@IETF

Candidate Structure on Data Plane



- **SAV Rule:** The rule that indicates valid incoming interfaces for a specific source prefix
- **SAV Table:** The table or data structure that implements the SAV rules
- Different actions-“Pass/Drop”, ”Qos CAR” or ”NetFlow-Sampling” cloud be executed by design.

Candidate Architecture of Intra-Domain SAVNET



*RPDP: Real Path Discovery Protocol

Integrated SAVNET System

- Multiple Source Information: mitigate improper block issue of incomplete prefixes set on accuracy :

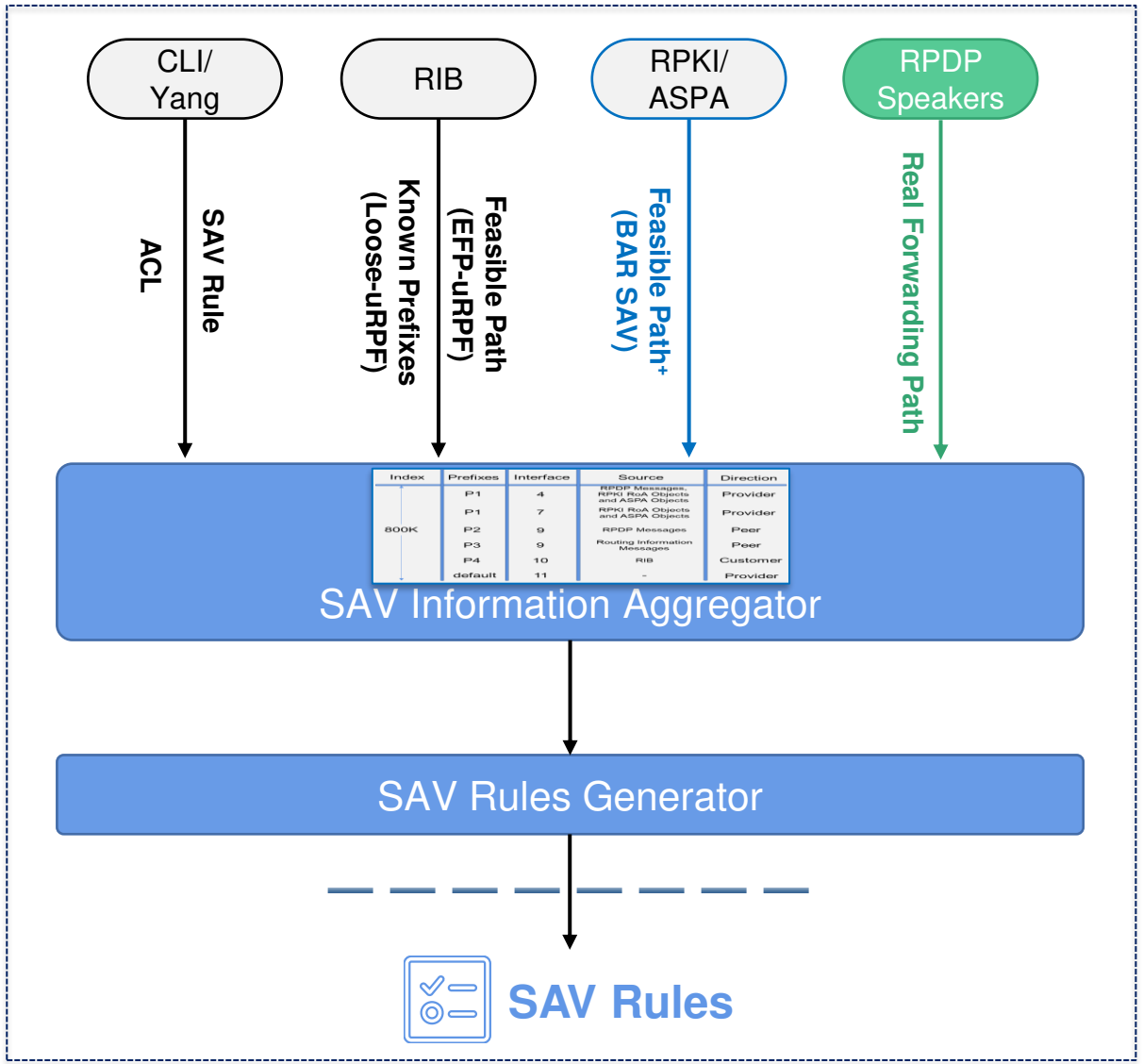
Info Source --→	CLI/yang	FIB	RPDP
ACL	✓		
Strict-uRPF		✓	
Loose-uRPF		✓	
SAVNET	✓	✓	✓

- Real Path Discovery Protocol :

  Discover accurate real path automatically among routers, to avoid improper block in asymmetric routing scenario and minimize improper permitting

- RPDP: Reduce operating overhead via generating SAV rules by corporation between Routers on control-plane.

Candidate Architecture of Inter-Domain SAVNET



*RPDP: Real Path Discovery Protocol

Integrated SAVNET System

- Multiple Source Information: Mitigate improper block issue of incomplete prefixes set on accuracy :

Info Source →	CLI/yang	RIB	ASPA/RPKI	RPDP
ACL	✓			
EFP-uRPF		✓		
Loose-uRPF		✓		
BAR SAV		✓	✓	
SAVNET	✓	✓	✓	✓

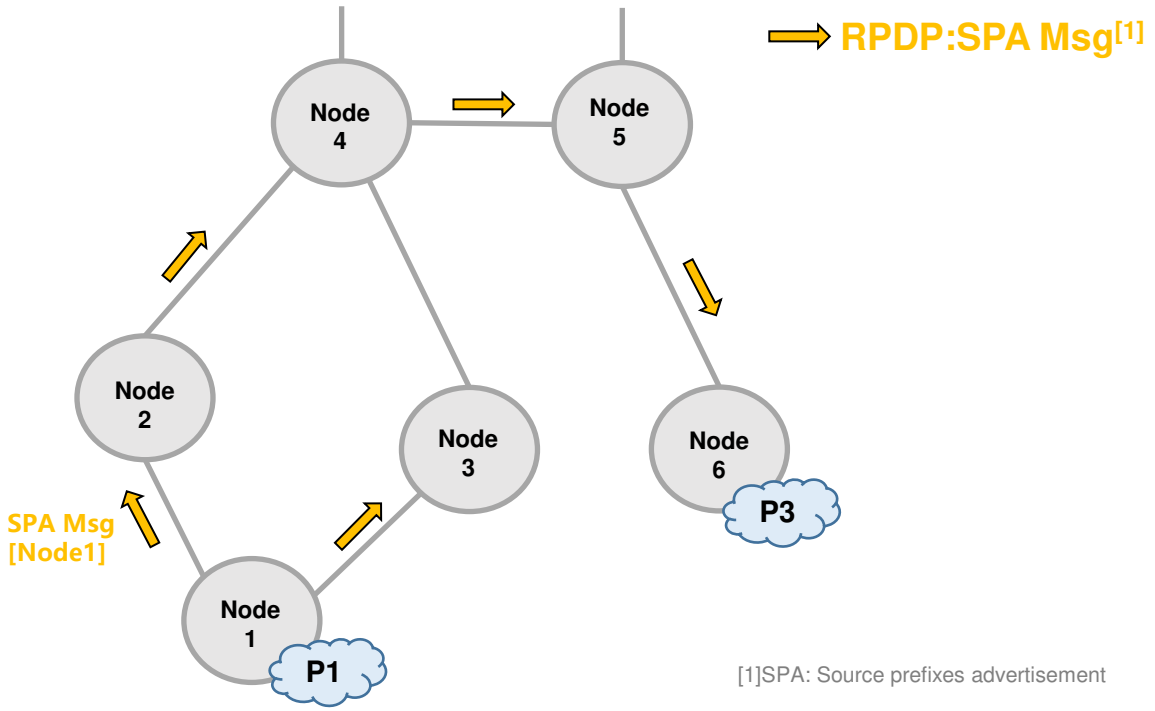
- Real Path Discovery Protocol :

  Discover accurate real path automatically among ASes, to avoid improper block in asymmetric routing scenario and minimize improper permitting

- RPDP: Reduce operating overhead via generating SAV rules by corporation between ASes on control-plane.

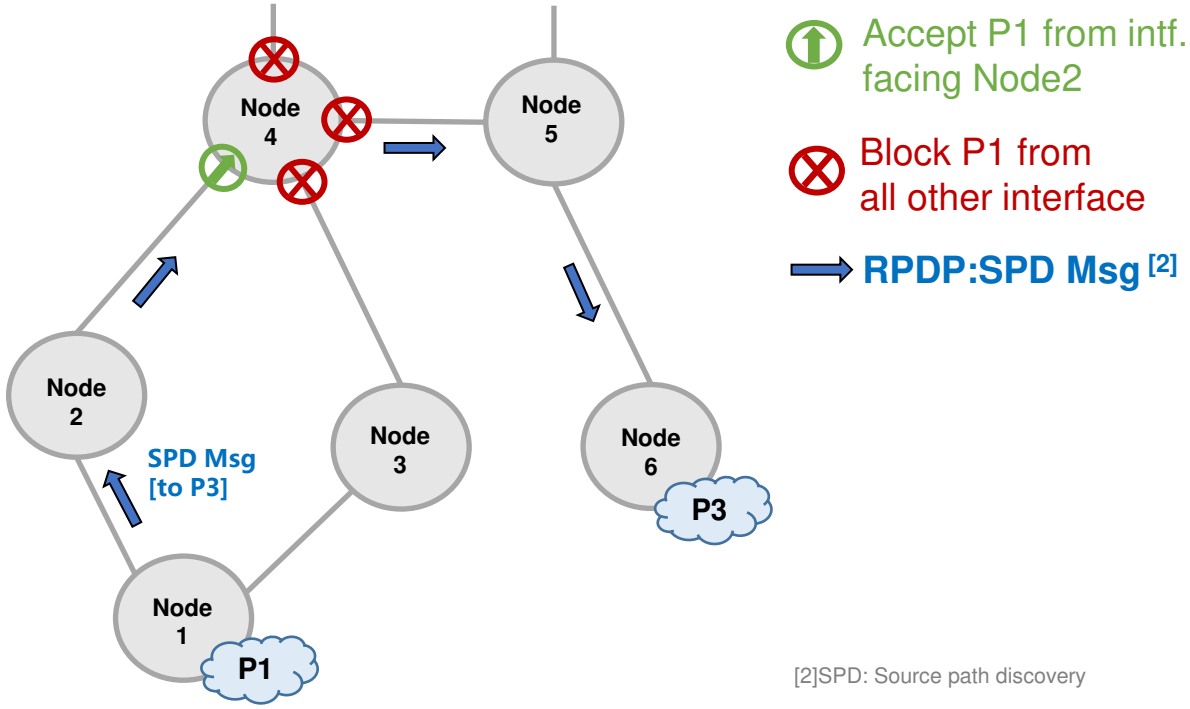
Real Forwarding Path Discovery Protocol (RPDP)

Step1：Source Prefixes Advertisement



[1]SPA: Source prefixes advertisement

Step2：Source Path Discovery



[2]SPD: Source path discovery

Main idea

① Origin Node advertises its all prefixes to other Nodes by RPDP-SPA message

② Other Nodes learn the source prefixes of origin Node through received RPDP-SPA messages

Main idea

① Origin Node advertises its RPDP-SPD message on preferred paths to other Node according to real data-plane information

② Other Nodes learn the incoming interface of origin Node through received RPDP-SPD messages

Agenda

- IP Spoofing Situation on Internet
- Existing SAV Mechanisms and Gap Analysis
- Desired Features to Narrow Gaps
- Preliminary Architecture of Compatible SAV
- **SAVNET@IETF**

IETF SAVNET WG: A Platform of SAV

- **SAVNET BOF, IETF 113**, Mar 24, 2022
- **SAVNET WG, formed in Jun 17**, 2022
  - Name: Source Address Validation in Intra-domain and Inter-domain Networks
  - Acronym: savnet
  - Area: Routing Area (RTG)
  - Mailing list: savnet@ietf.org
  - WG Charter: https://datatracker.ietf.org/wg/savnet/about/
- **SAVNET WG Meeting, IETF 114**, Jul 25, 2022
  - Intra-domain SAVNET Gap, Analysis, Problem stement and Requirement
  - Intra-domain SAVNET method
  - Intra-domain SAVNET method

IETF SAVNET WG: A Platform of SAV

- **SAVNET WG Meeting, IETF 115**, Nov 11, 2022
  - **SAV Table** Abstraction and Application
  - **Intra-domain** Source Address Validation (SAVNET-RPDP) **Architecture**
  - **Inter-domain** Source Address Validation (SAVNET-RPDP) **Architecture**
  - **BAR-SAV** Approach -- Lowering Improper Block and Improper Admit
  - Analysis of SAV **Data Plane Performance**

- **SAVNET WG Meeting, IETF 116, Mar** 25, 2023

  Under planning

Proposed Solutions in SAVNET WG

Submitted Solutions:

① SAVNET-RPDP Architecture;

Source Address Validation Using Real Path Discovery Protocol

② BAR-SAV

Source Address Validation Using BGP UPDATEs, ASPA, and ROA

› ***More…***

Waiting for your sharing & contribution

Documents & Draft

Document
Related Internet-Drafts (10 hits)
draft-cui-savnet-anti-ddos-00 **SAVA-based Anti-DDoS Architecture**
draft-huang-savnet-sav-table-00 **Source Address Validation Table Abstraction and Application**
draft-li-savnet-dataplane-performance-00 **Analysis of Source Address Validation Data Plane Performance**
draft-li-savnet-intra-domain-architecture-00 **Intra-domain Source Address Validation (SAVNET) Architecture**
draft-li-savnet-intra-domain-problem-statement-05 **Source Address Validation in Intra-domain Networks (Intra-domain SAVNET) Gap Analysis, Pr**
draft-lin-savnet-lsr-intra-domain-method-01 **Intra-domain SAVNET method**
draft-qin-savnet-incentive-03 **The Incentive Consideration for Defense Against Reflection Attacks**
draft-sriram-sidrops-bar-sav-02 **Source Address Validation Using BGP UPDATEs, ASPA, and ROA (BAR-SAV)**
draft-wu-savnet-inter-domain-architecture-00 **Inter-domain Source Address Validation (SAVNET) Architecture**
draft-wu-savnet-inter-domain-problem-statement-05 **Source Address Validation in Inter-domain Networks (Inter-domain SAVNET) Gap Analysis, Pr**

Thank you !