



互联网路由安全

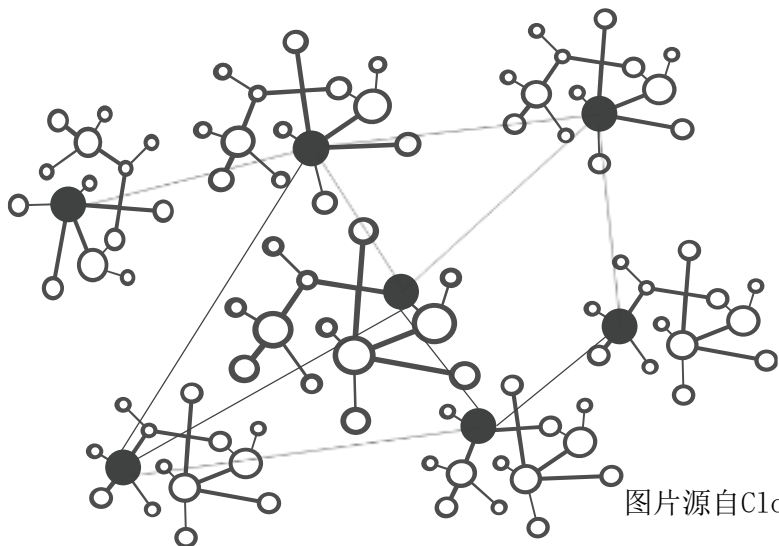
李琦

清华大学网研院



全球路由系统

The Internet
A Network of Networks

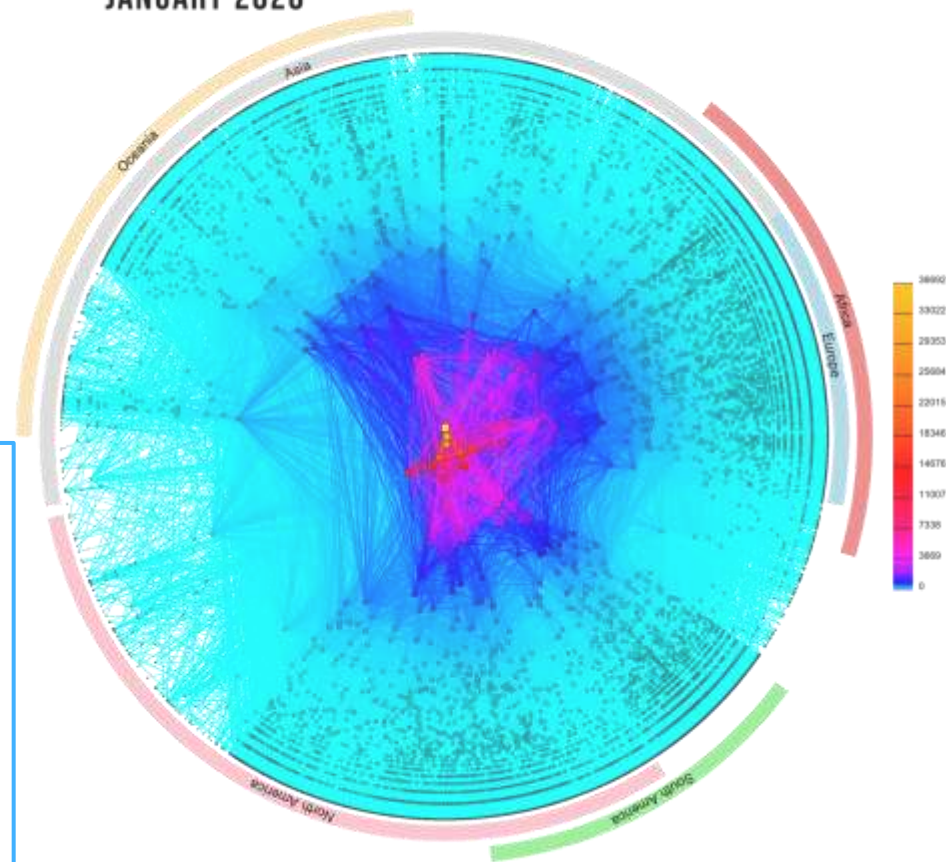


图片源自Cloudflare

截止2024年2月底，全球路由系统共包括

- 1196846条路由前缀，其中IPv4为989257，IPv6为207589
- 82470个自治系统（AS），每个拥有专属ASN（当前共分配104491个ASN）

CAIDA'S IPV4 AS CORE GRAPH
JANUARY 2020



COPYRIGHT © 2020 UC REGENTS



本章的内容组织



第一节 层次化路由体系结构

- 层次化路由
- 域内路由
- 域间路由

全球路由系统
如何工作？



第二节 路由安全问题

- 域内路由安全
- 域间路由安全

路由系统存在
什么安全问题？



第三节 路由源验证

- IRR
- RPKI
- MANRS

路由源劫持
如何防御



第四节 路径验证

- BGPsec
- FCBGP

路径劫持
如何防御



第五节 恶意路由检测

- OTC
- ASPA
- BEAM

泄露劫持
如何检测

全球路由系统各层次存在的安全问题

解决安全相关问题，构建更强健路由系统



第1节 层次化路由体系结构

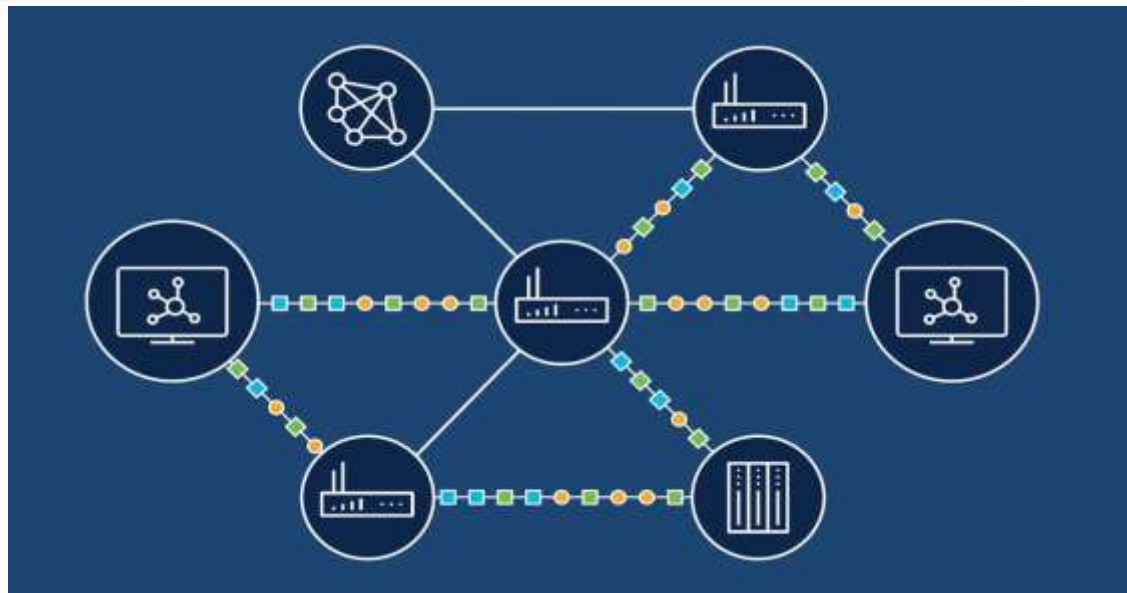
- ✓ 层次化路由
- ✓ 域内路由
- ✓ 域间路由



认识路由

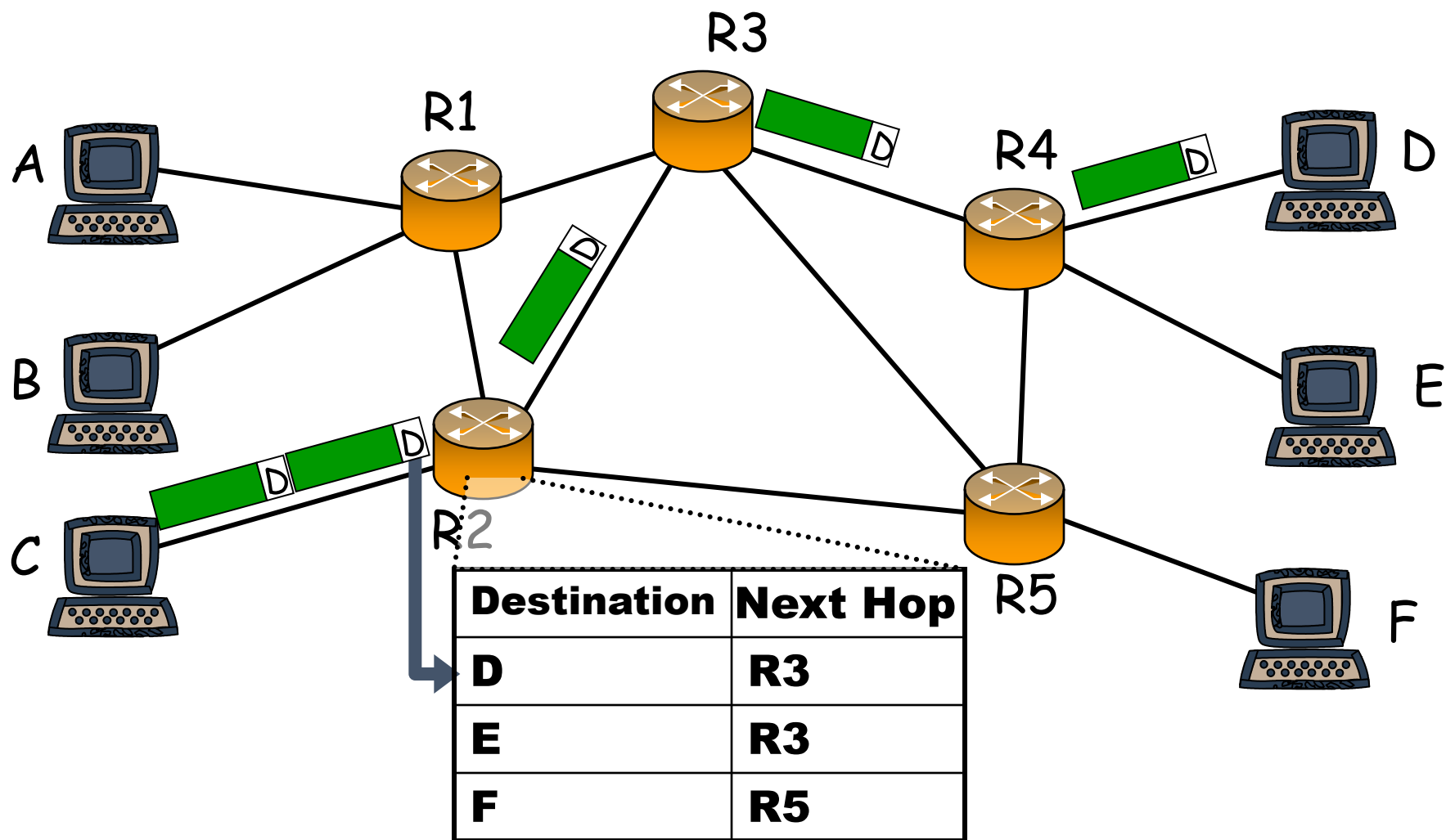
路由（routing）是通过互联的网络，把**分组从源地址传输到目的地址**。路由发生在TCP/IP协议的第三层即网络层。路由引导分组转发，从源节点出发，经过一系列中间路由器后，到达最终的目的节点

What is Routing?





认识路由





层次化路由

按域组织

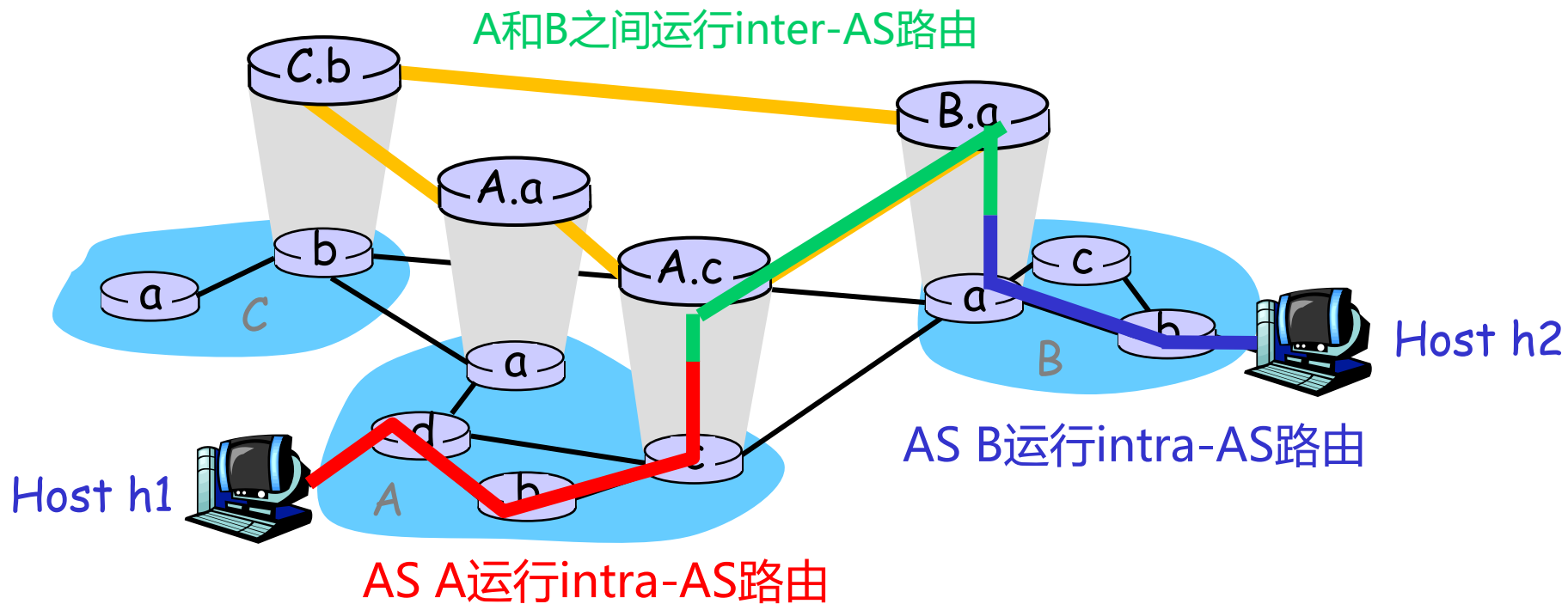
- 将路由器按区域组织、聚合，
“autonomous systems (AS)”
- 同一AS内的路由器运行同一种路由协议
 - “intra-AS” 路由协议
 - 不同AS的路由器运行不同的intra-AS路由协议

网关路由器

- 运行intra-AS路由协议与AS内的其他路由器通信
- 负责处理到本地AS之外的目的地的路由
 - 运行inter-AS路由协议，与其他的网关路由器通信



域内路由和域间路由

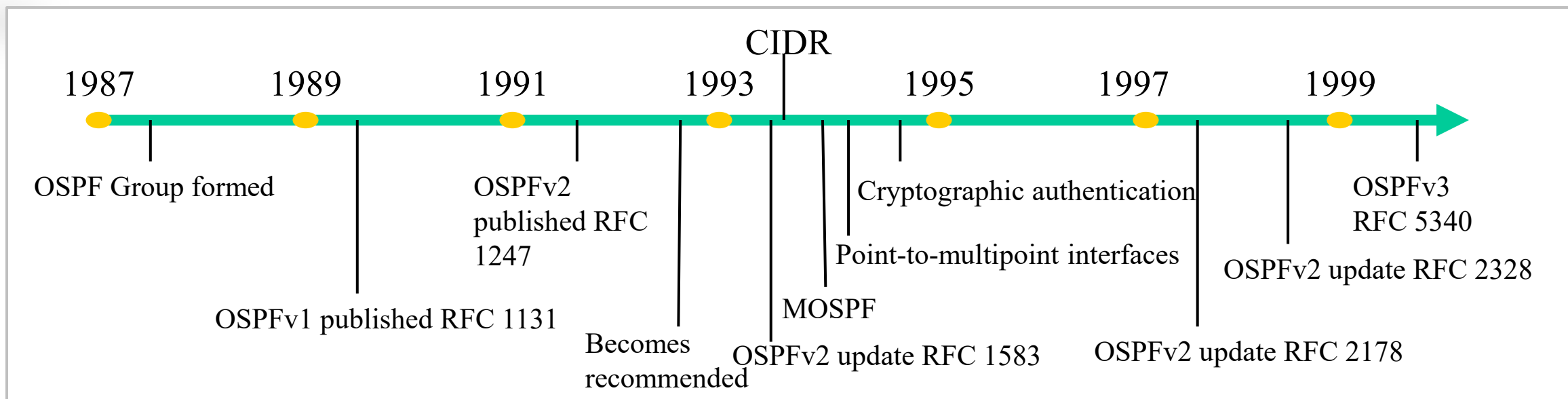


畅所欲言

域内路由协议可以有多种吗？域间路由协议呢？



OSPF的发展历史



- OSPF 使用**分布式链路状态协议** (link state protocol)
- OSPF路由器之间完整交换链路状态信息，OSPF路由器能建立一个链路状态数据库 (Link State Database, LSDB)，这个数据库实际上就是全网拓扑结构图
- 每台路由器使用LSDB中的数据，构造自己的路由表（例如，使用Dijkstra算法）



域间路由协议BGP

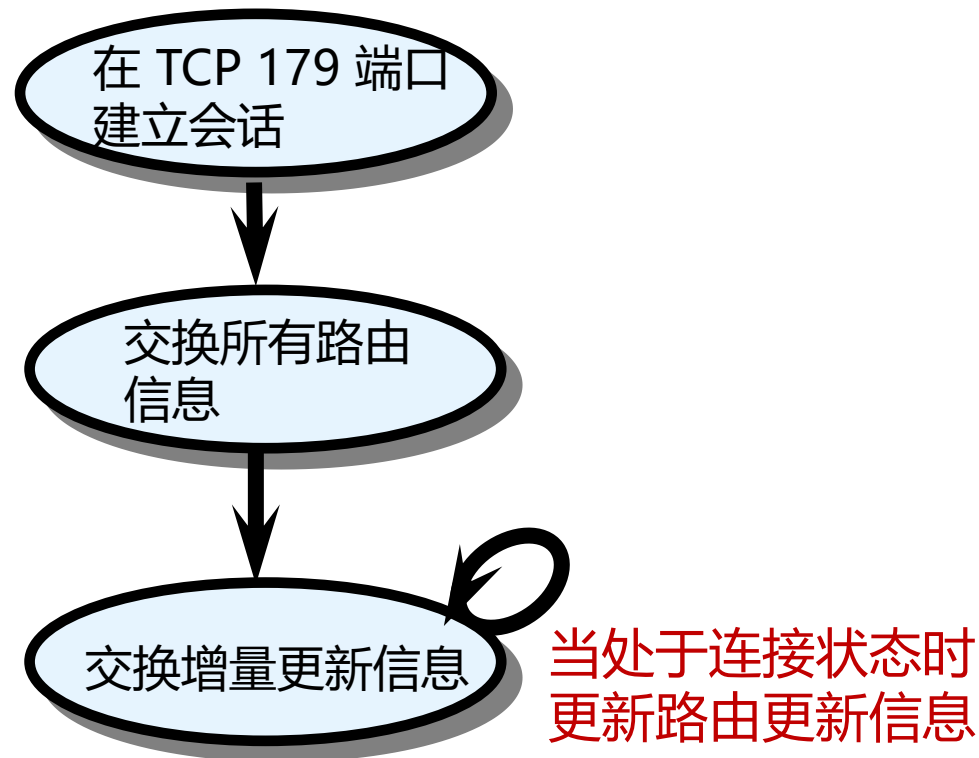
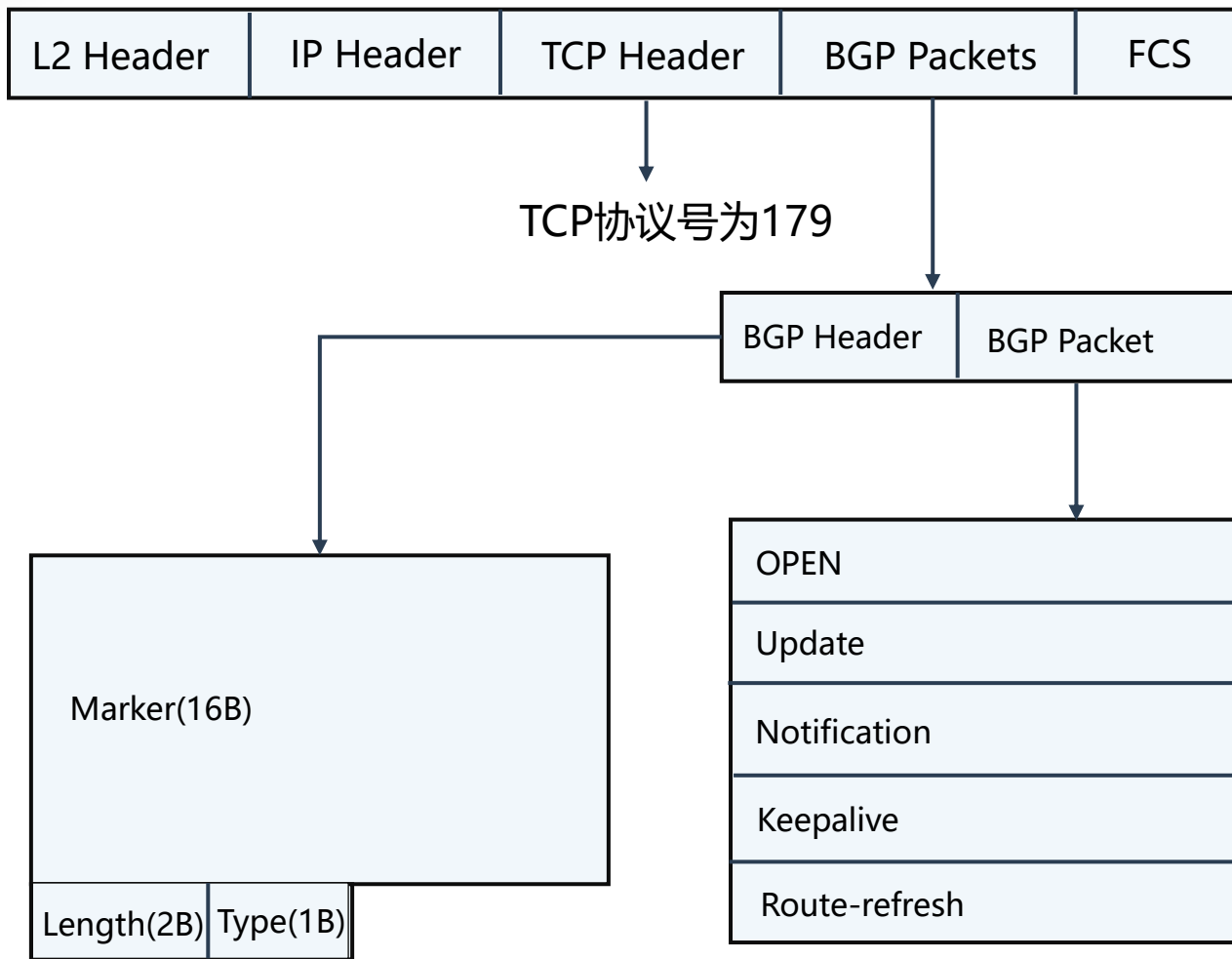
- 1989 : BGP-1 [RFC 1105]
 - Replacement for EGP (1984, RFC 904)
- 1990 : BGP-2 [RFC 1163]
- 1991 : BGP-3 [RFC 1267]
- 1995 : BGP-4 [RFC 1771]
- 2006 : BGP-4 [RFC 4271]
 - Support for Classless Interdomain Routing (CIDR)

- BGP: Border Gateway Protocol
- 基于策略的路由协议
- 当今全球互联网使用的外部网关协议 (EGP)
- 支持CIDR无类域间路由

BGP使用TCP作为其传输层协议



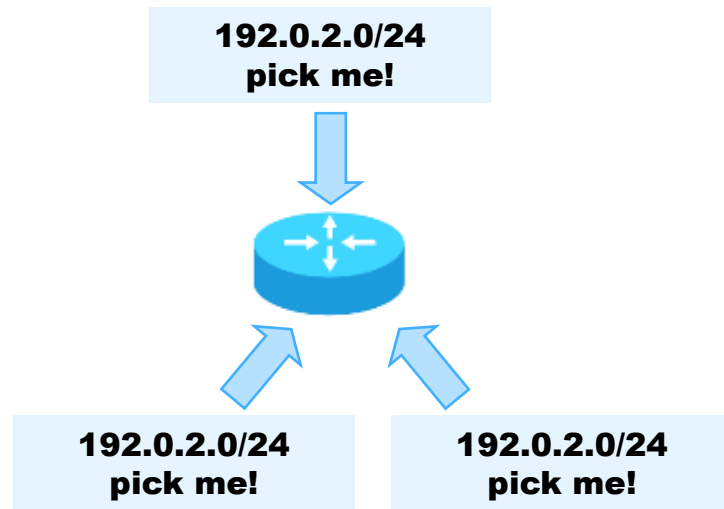
BGP的工作过程（简化版本）





BGP属性

- **公认必遵(Well-known mandatory)**: 所有BGP路由器都可以识别, 且必须存在于Update消息中
- **公认任意(Well-known discretionary)**: 所有BGP路由器都可以识别, 但不要求必须存在于Update消息中
- **可选过渡(Optional transitive)**: 在AS之间具有可传递性的属性, BGP路由器可以选择是否在Update消息中携带这种属性
- **可选非过渡(Optional non-transitive)**: BGP路由器可以选择是否在Update消息中携带这种属性

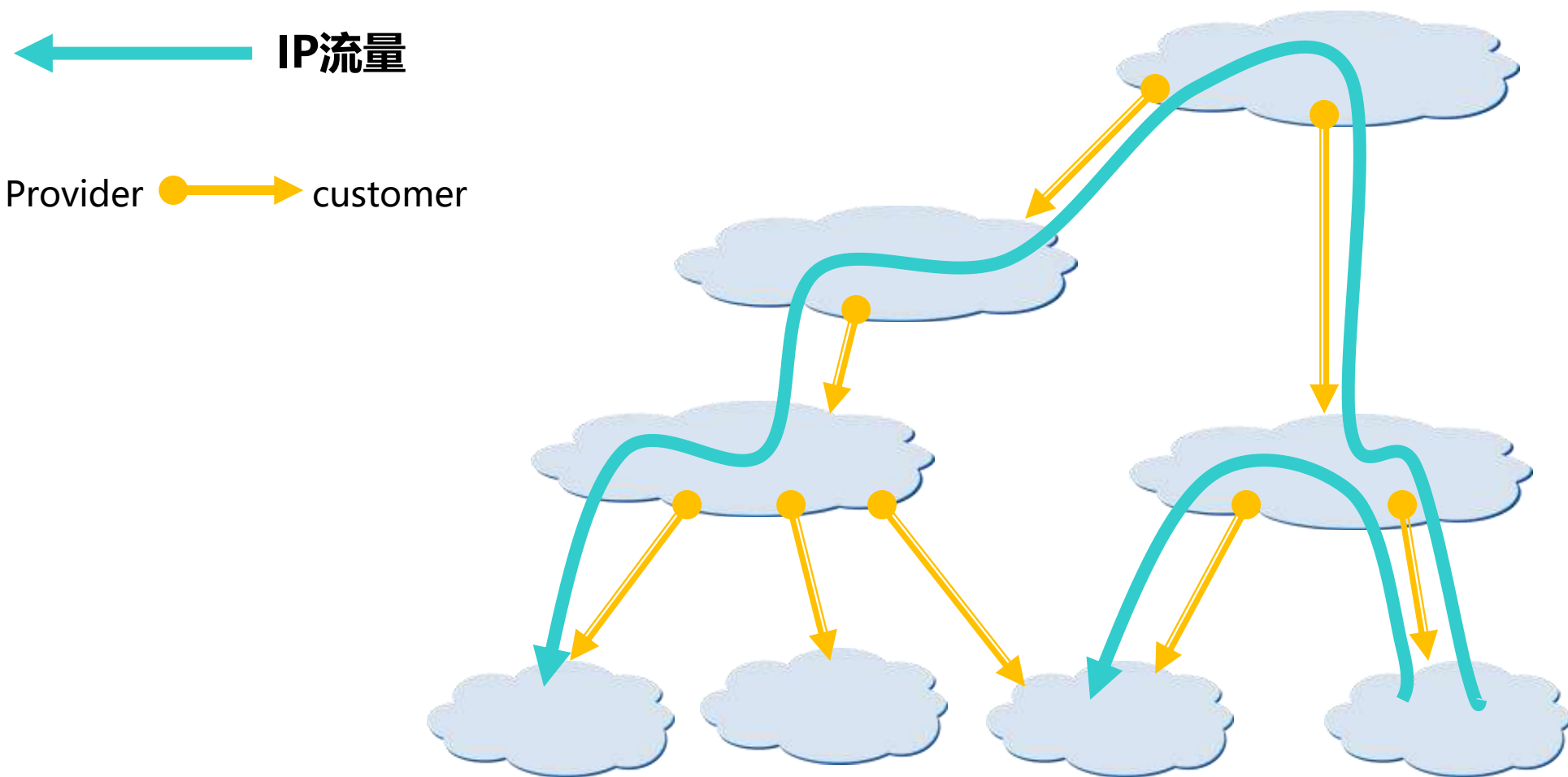


给定到同一前缀的多条路由,
一个BGP speaker 最多选择
一条最佳路线

BGP属性通常用于选择最佳路由

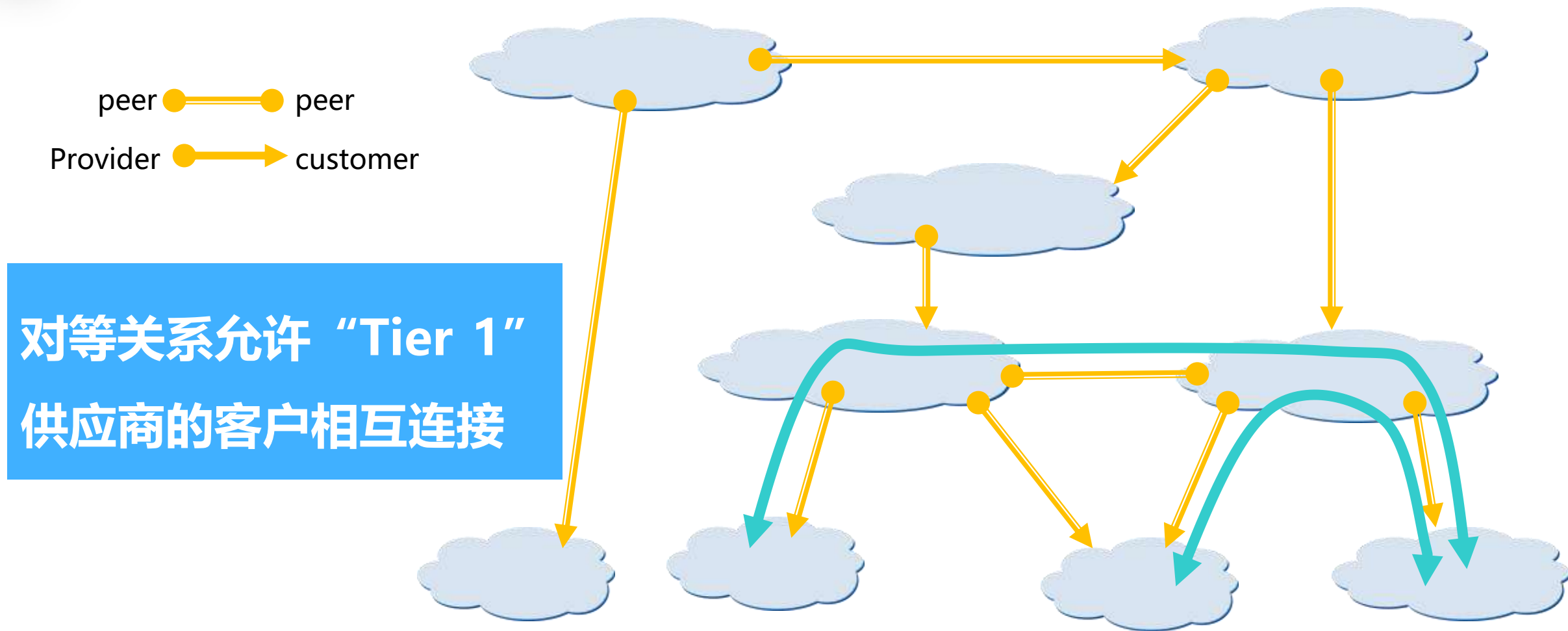


客户-提供商形成层次化结构





对等关系提供了快捷路径





纠结的对等关系

Peer

- 降低上游传输成本
- 可以提升端到端性能
- 可能是将客户连接到互联网某些地方(例如 “Tier 1”)的唯一途径

Don't Peer

- 宁愿有客户
- 对等体通常是你的竞争对手
- 对等关系可能需要定期重新协商

对等竞争是迄今为止在互联网服务领域最具争议的问题!

对等协议通常是保密的



国内ISP互联状态（历史状态）

经营性的互联单位6家

中国电信
中国网通
(称为“大网”)

中国移动
中国联通
中国铁通
(称为“中网”)

其他非经营性
互联单位
(称为“小网”)，如
CERNET

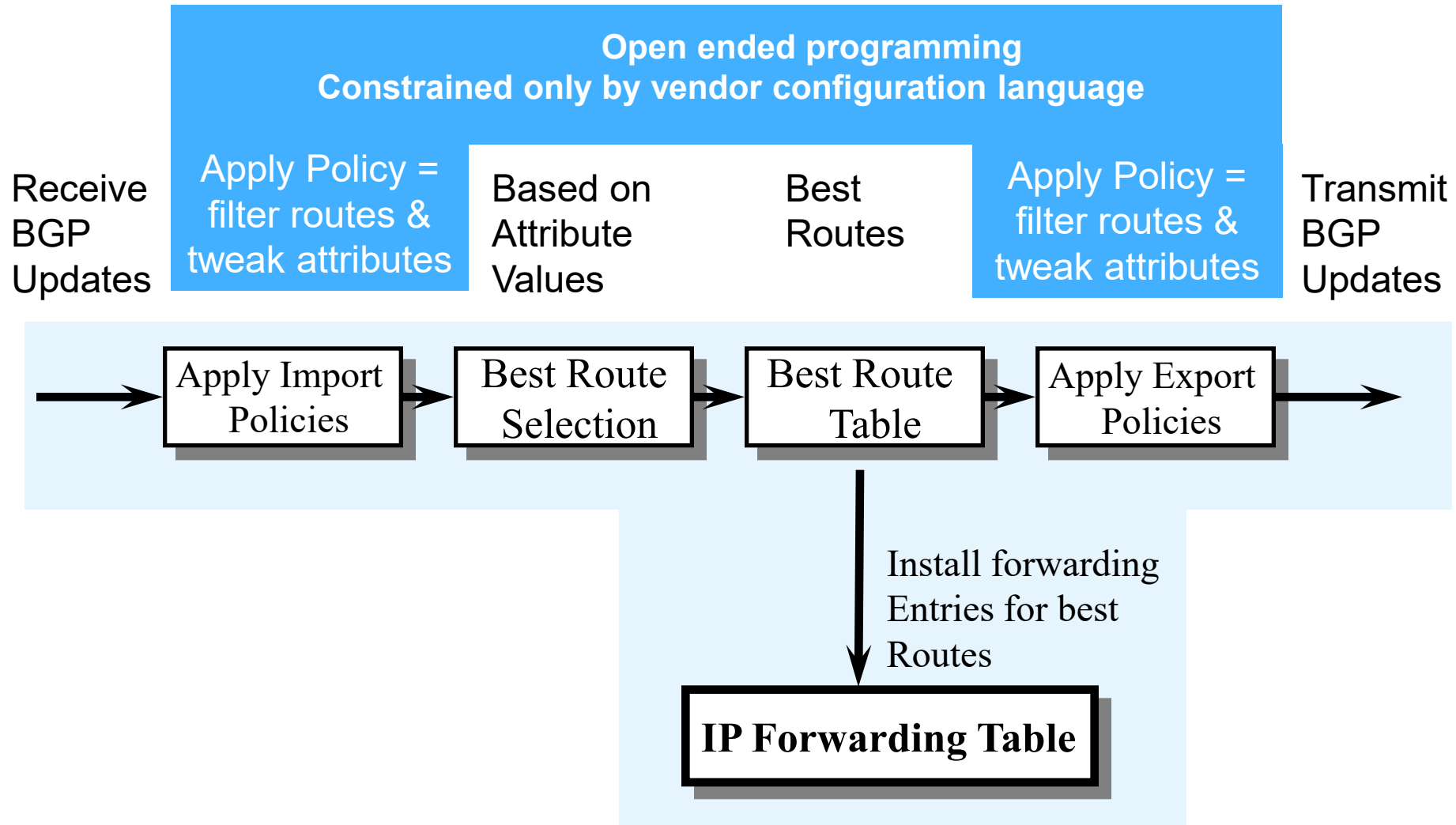
- 大网之间互不结算
- 中网与大网之间的结算方式包括直联和经NAP点转接

NAP点转接方式

- 北京、上海、广州建有国家级互联网交换中心（NAP点）
- 国家级交换中心采取政府定价，根据信息产业部2008年10月颁布的《互联网交换中心网间结算办法》，中网按照双向流量的平均值向大网交结算费
- 结算费用（元/月）= 1000（元/Mbps月）× 结算速率（Mbps） 10G带宽费用为1000万/月



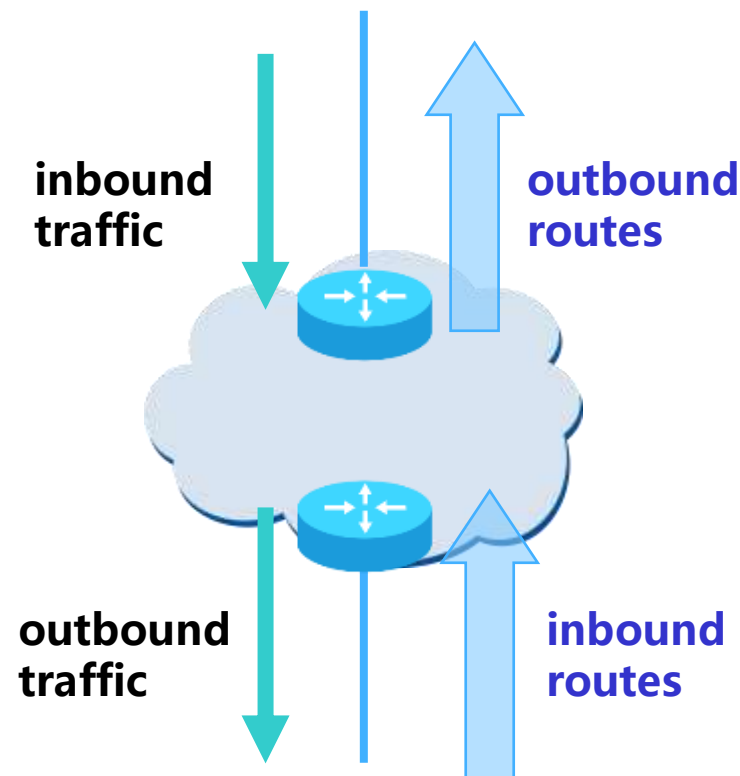
BGP 路由处理过程





如何实现策略？ 调整BGP属性

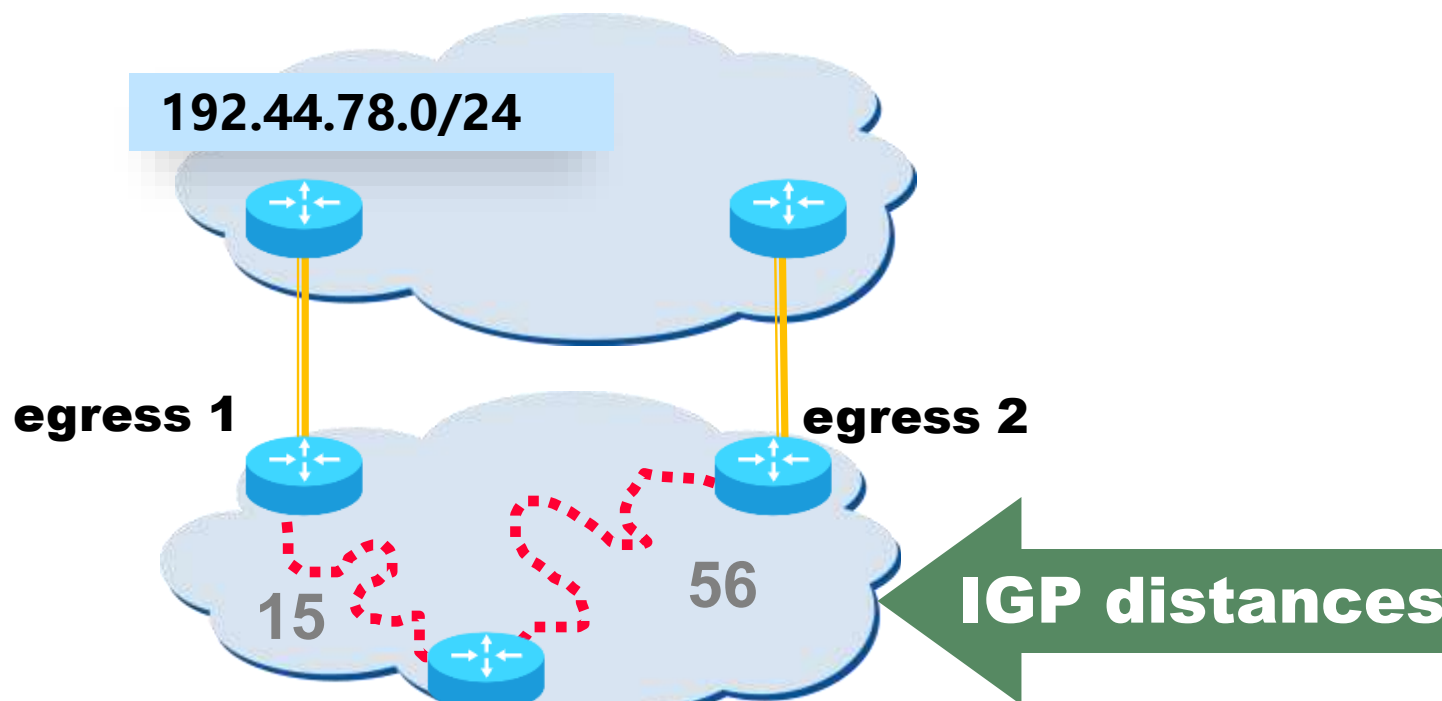
- 对于入站 (inbound) 流量
 - 过滤出站路由
 - 调整出站路由的属性，以影响邻居的最佳路由选择
- 对于出站 (outbound) 流量
 - 过滤入站路由
 - 调整入站路由的属性，以影响最佳路由选择



一般而言，AS对出站流量有更多的控制权



Hot Potato Routing: 找最近的出口



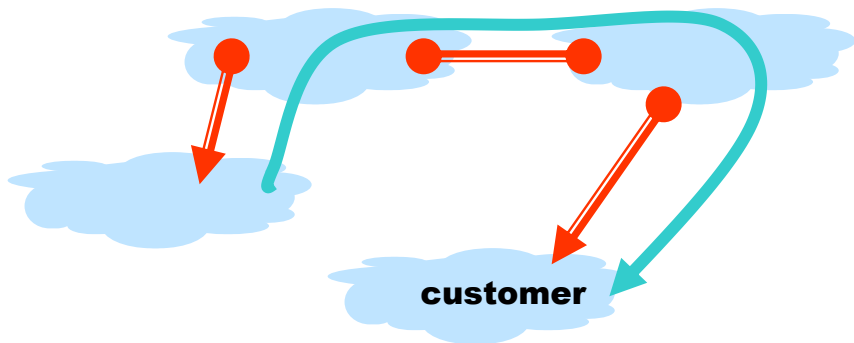
此路由器有两条通往192.44.78.0/24的BGP路由

Hot potato: 尽快将流量传输出去, 走出口1!

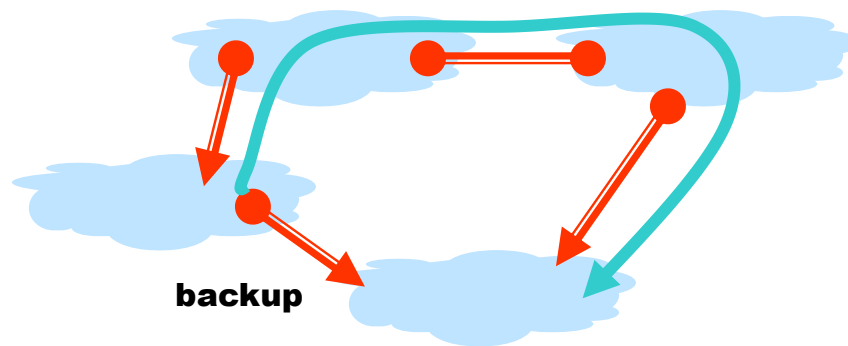


策略有时候效果很奇怪

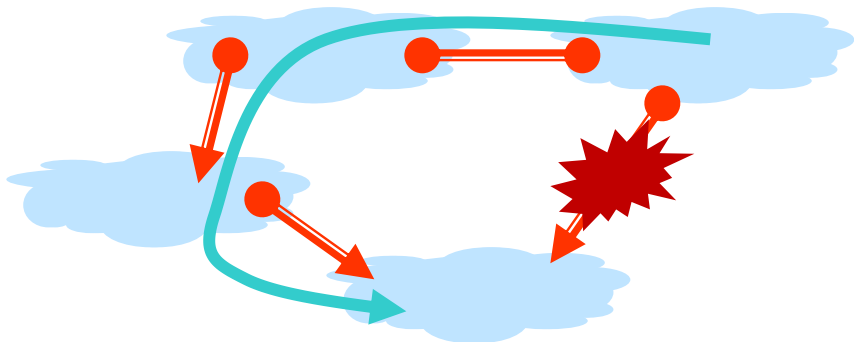
“路由粘连 (Route Pinning)” 示例



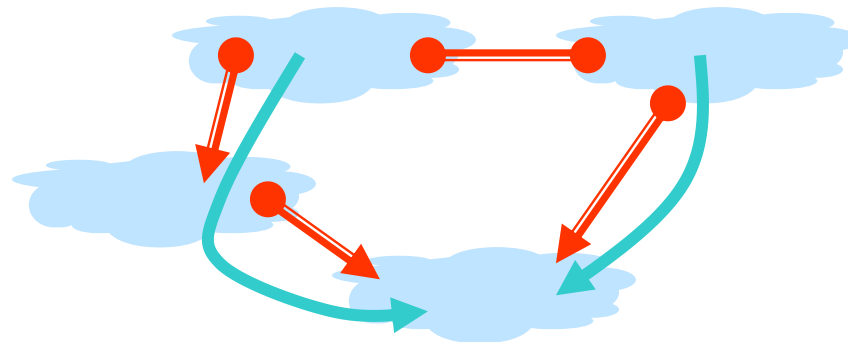
1



2 使用community建立备份链路



3 主链路发生故障，备份链路启用



4 主链路已恢复，但一些流量仍被锁定在备份链路上



请注意...

BGP不能保证收敛到稳定的路由

策略交互可能导致“livelock” 协议振荡

推论：BGP不能保证从网络故障中恢复



区分动态语义和静态语义

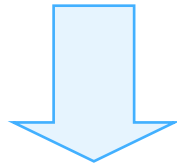
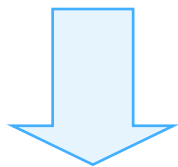
静态语义

动态语义

BGP Policies

BGP

Booo Hooo,
Many, many
complications...



**Stable Paths
Problem (SPP)**

SPVP

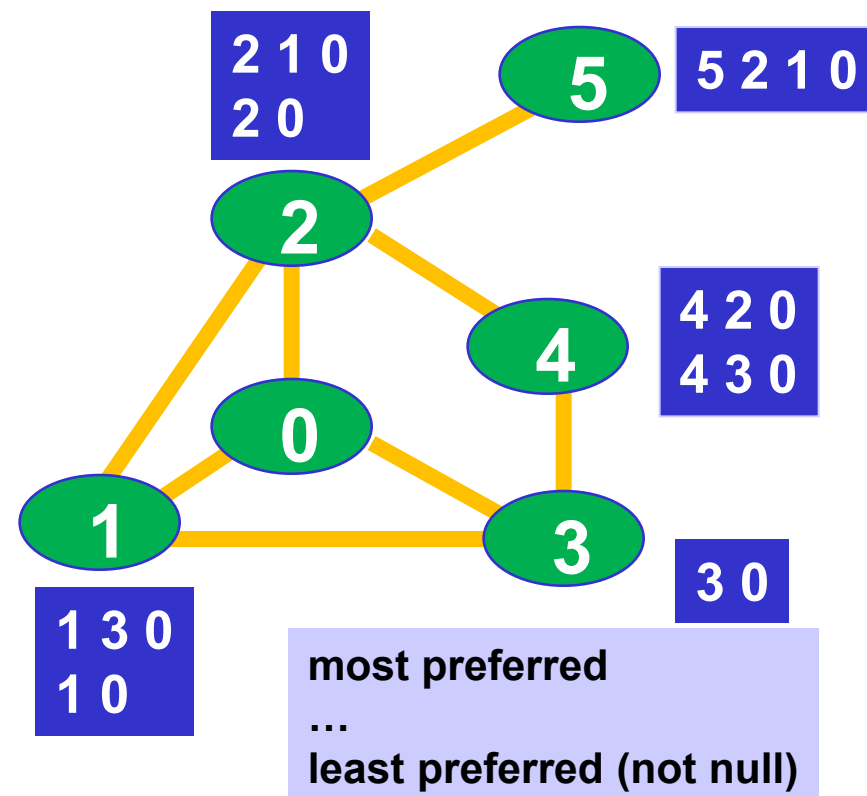
SPVP = Simple Path
Vector Protocol = a
distributed algorithm
for solving SPP

The stable paths problem and interdomain routing. IEEE/ACM Trans. Netw. 10(2): 232-243 (2002)



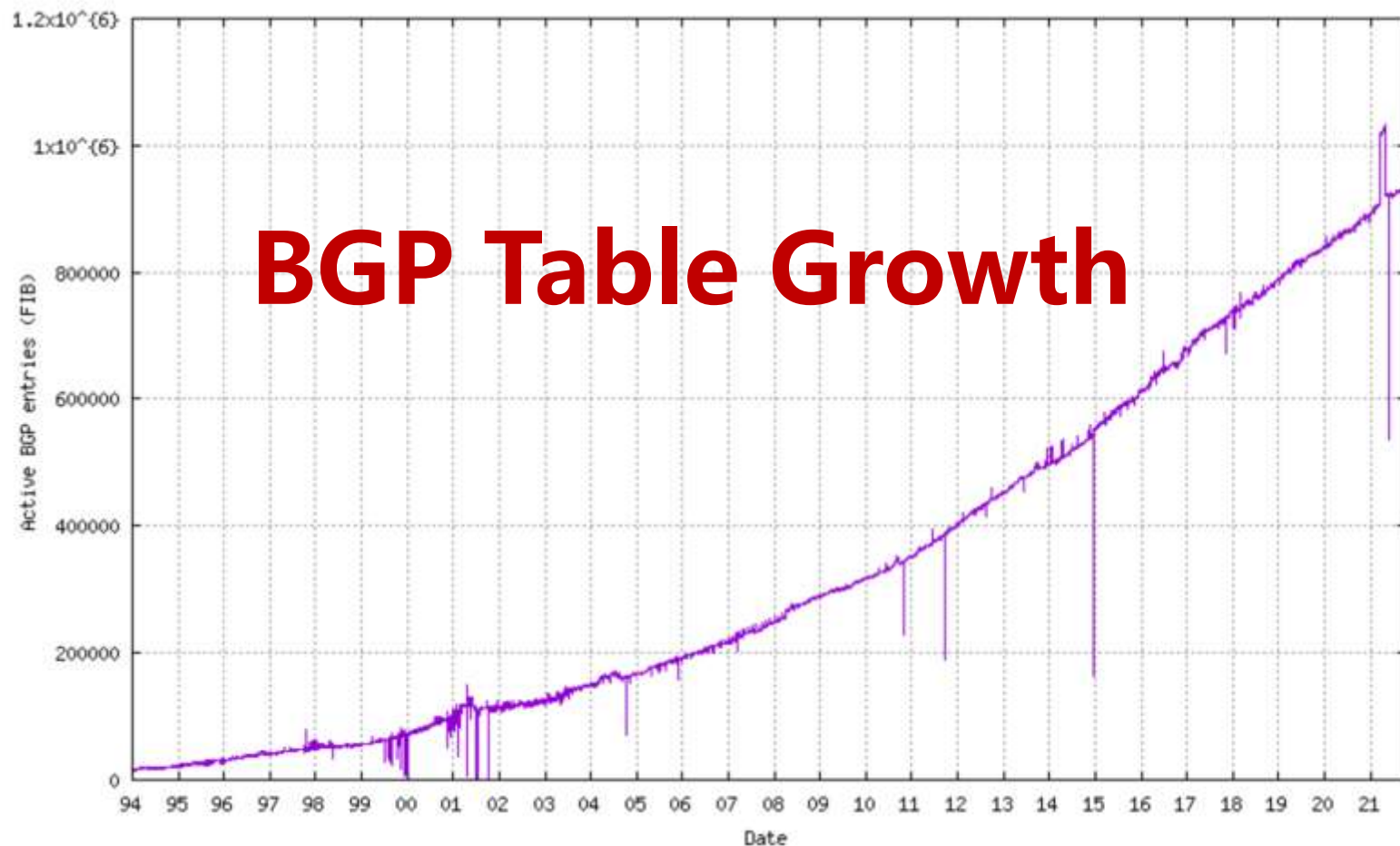
Stable Paths Problem 实例

- 由节点和边组成的图
- 节点0，称为原点
- 对于每个非零节点，都有指向原点的一组允许路径。这个集合总是包含“空路径”，路径优先性自上而下越来越低
- 空路径总是优先级最低的





BGP系统很大，而且正在变得更大



FIB / RIB Table Reports (plots)	Data Sets(txt)
Active BGP entries (FIB)	932266
All BGP entries (RIB)	27107687
RIB/FIB ratio (27107687/932266)	29.0772
Valid entries	27107687
Suppressed RIB entries	0
Damped entries	0
History entries	0

<http://bgp.potaroo.net/as6447/> BGP data obtained from AS6447



BGP路由表太大一定有危害

- 路由表必须存储最佳路由和备用路由
- 对于具有许多备选路由(例如路由反射器)的路由器来说，负担可能很大
- 众所周知，路由器会死机
- 增加CPU负载，特别是在会话重置期间

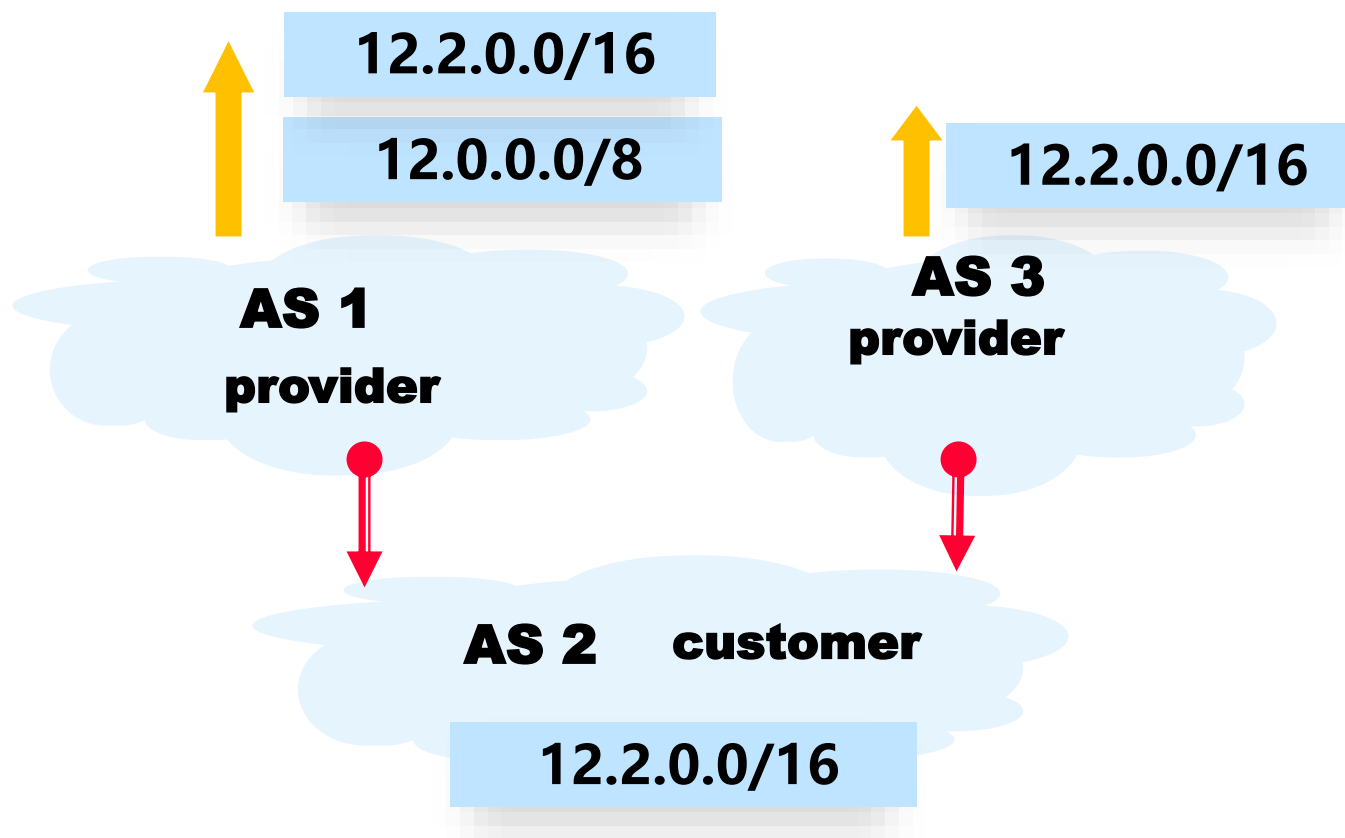
理论上，摩尔定律可能会拯救我们，但实际上这意味着需要花钱升级装备.....



Multihoming 是路由表增大的主要原因

如果 AS 1 没有公布更具体的前缀，则到 AS 2 的大部分流量将通过 AS 3，因为它的匹配掩码更长

AS 2 is
“punching a hole” in
The CIDR block of AS 1





第2节 路由安全问题

- ✓ 域内路由安全
- ✓ 域间路由安全



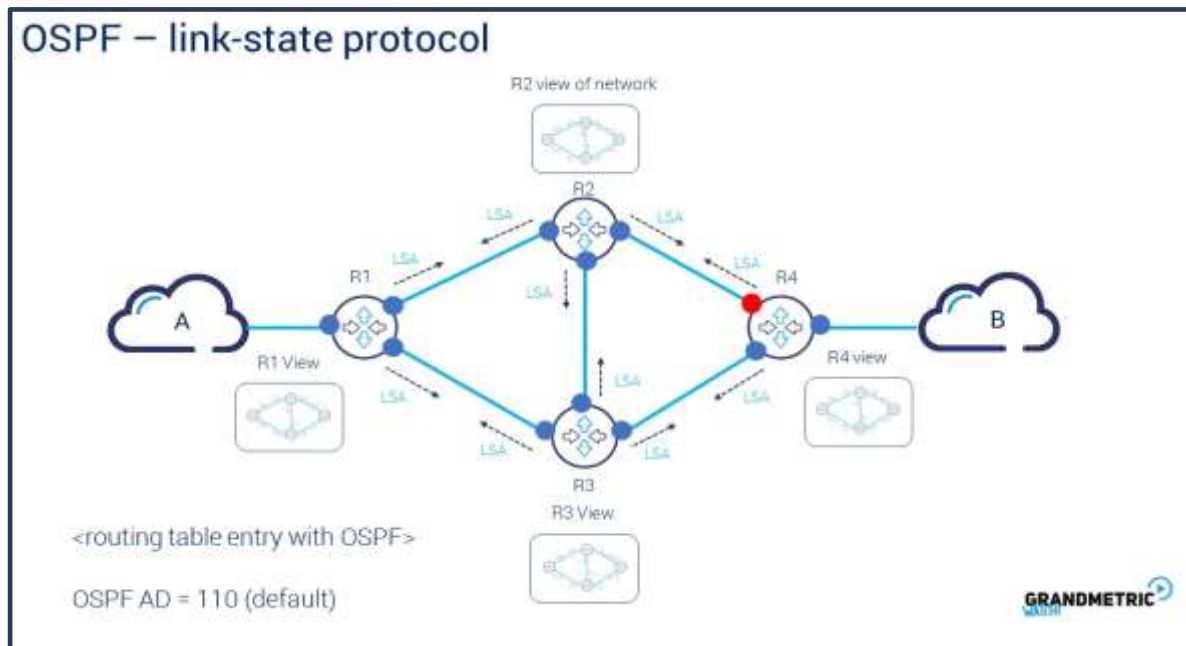
域内路由安全

OSPF协议是目前使用最广泛的域内路由协议，因此针对域内路由的威胁攻击，也主要是针对OSPF协议展开



OSPF攻击基本原理：

攻击者通常假装成合法的域内路由器，伪造OSPF协议的LSA报文并广播出去，迷惑其他路由器，干扰路由表的计算

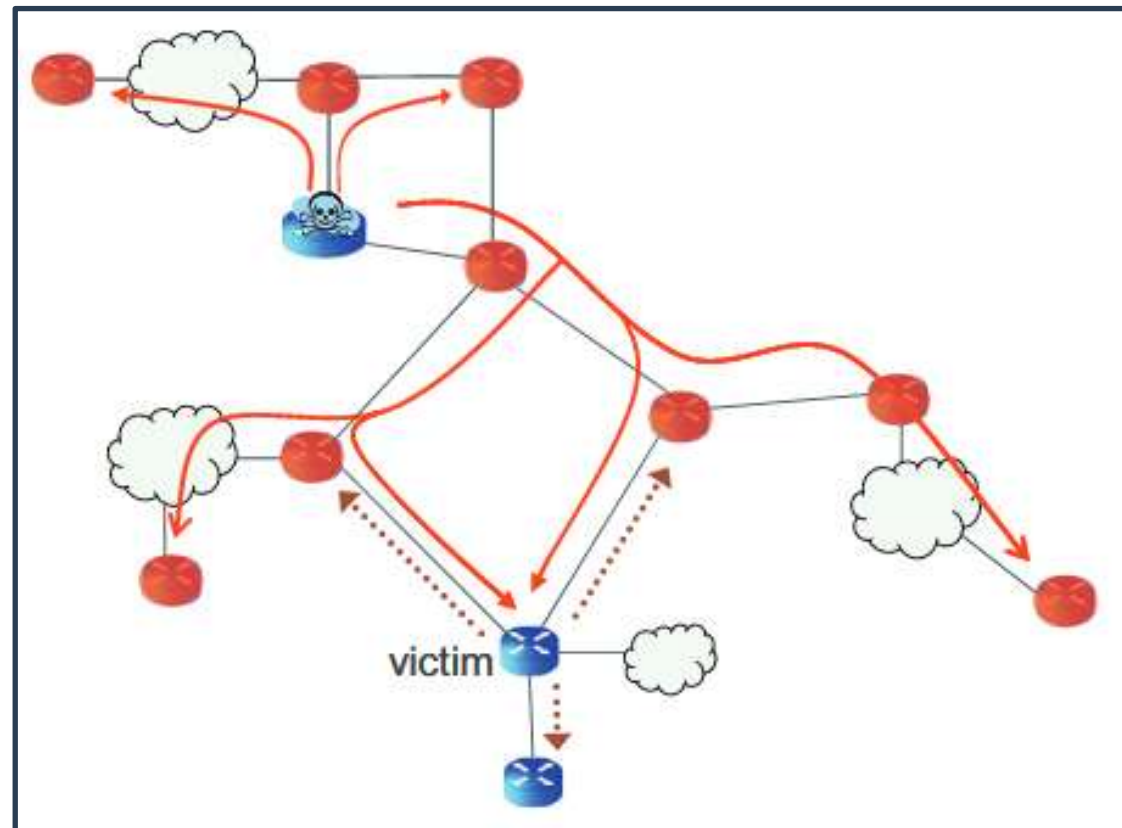




域内路由安全

Periodic injection 攻击

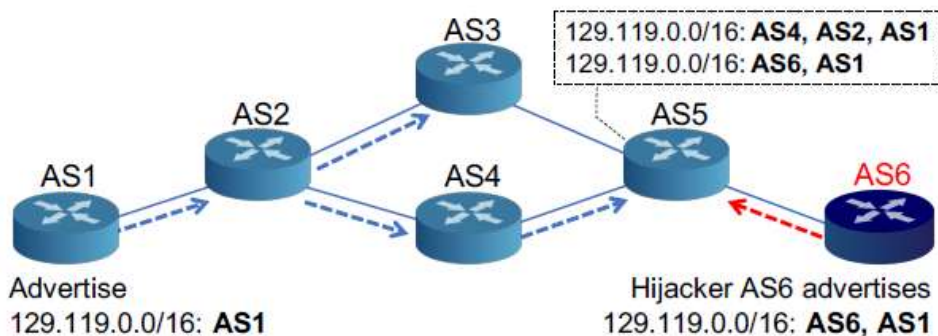
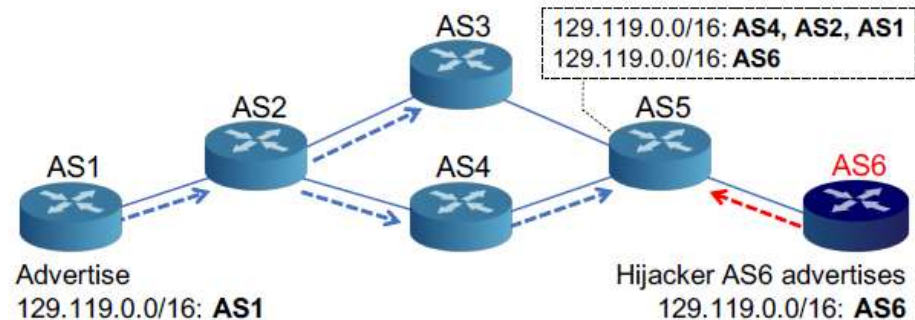
- (1) Fight-back纠正报文的通告是有时限的，路由器LSA报文的通告不能小于5秒
- (2) 如果攻击者发送伪造LSA的间隔小于5秒，源合法路由器发现伪造的LSA与当前时刻小于5秒，会阻止当前的fight-back动作
- (3) 等待时钟到达5秒后再发送，但是当真的再过5秒后，下一个伪造的LSA又会到达，则源合法路由器又会继续等待，从整体效果来看，整个fight-back动作被抑制了





域间路由安全

- 恶意攻击者宣告一个**实际上并不控制的IP地址前缀**或者宣告**到达合法AS的非法路径**，进行虚假路由宣告。如果虚假路由宣告未被有效过滤，就有可能发生路由劫持攻击
- 路由劫持想要成功，恶意攻击者的宣告必须满足以下条件：
 - (1) 宣告比以前其他 AS **更具体的 IP 地址范围**，这被称为源劫持
 - (2) 提供一条通往目标IP 地址的**较短路径**，这被称为路径劫持
- 要发生 BGP 劫持，通常需要运营商权限

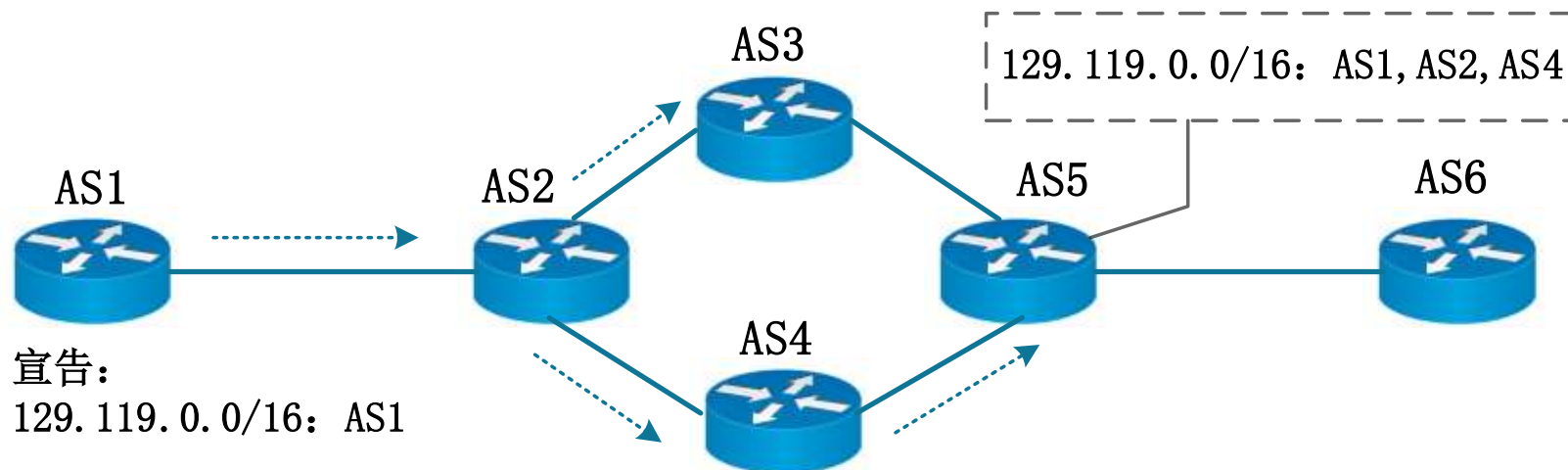




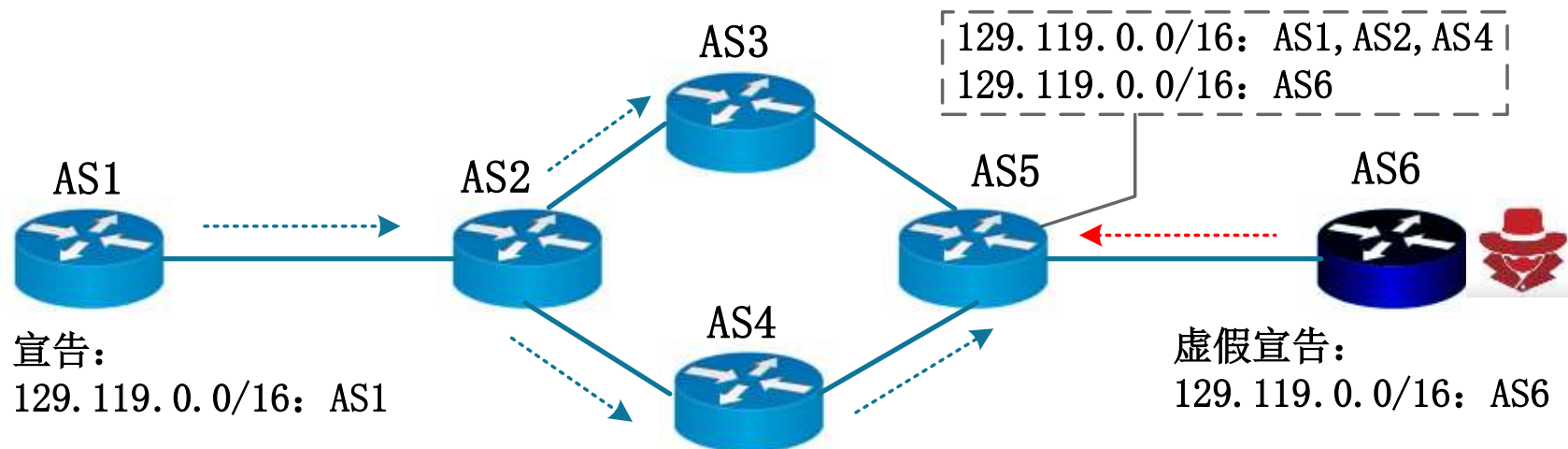
域间路由安全

前缀劫持

劫持前



劫持后





域间路由安全

Oracle 互联网分析部门主管Doug Madory最先报告了此事件，他所做的路由跟踪，复现了流量传输路径究竟绕了多大的圈子。右图显示了从弗吉尼亚州的谷歌云服务器开始的流量通过中国电信的骨干网络传输，最终传输到位于奥地利维也纳的目标IP地址

```
tracert from Google (Ashburn, VA) to ACOnet (Vienna, Austria) at 09:57 Jun 06, 2019
```

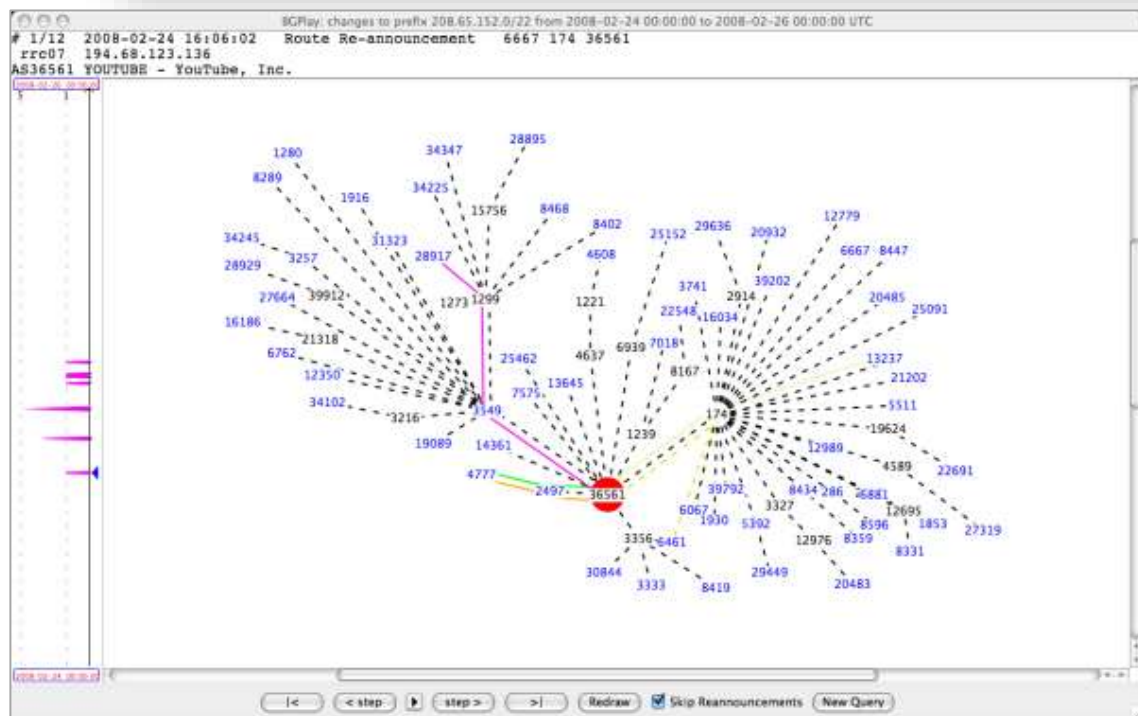
1	*			0.0
2	195.219.50.2	if-ae-7-2.tcore1.fnm-frankfurt.as6453.net	Frankfurt Germany	86.451
3	*			0.0
4	*			0.0
5	118.85.205.233	CHINANET BACKBONE NETWORK	Amsterdam Netherlands	265.544
6	*			0.0
7	202.97.52.65	CHINANET backbone network	Frankfurt am Main Germany	387.218
8	118.85.205.90	CHINANET BACKBONE NETWORK	China	340.859
9	80.80.225.142	vlan24.cs2.gva.safehost.net	Genève Switzerland	297.579
10	80.80.225.211	Safe Host Network Geneva	Genève Switzerland	309.027
11	80.80.225.193	ge-3-1.ds4.gva.safehost.net	Genève Switzerland	308.962
12	83.137.83.1	euNetworks GmbH	Vevey Switzerland	222.019
13	80.86.163.17	Loopbacks and P2P links Switzerl	Braunschweig Germany	219.624
14	217.71.96.37	ae6.irt1.fra44.de.as13237.net	Frankfurt am Main Germany	218.007
15	217.71.96.6	ae4.irt1.mun02.de.as13237.net	Munich Germany	213.565
16	217.71.96.110	ae1.400.irt1.vie08.at.as13237.net	Vienna Austria	222.668
17	193.171.255.33	ACOnet Services Network	Vienna Austria	221.573

此次事件中，有超过**1,300个**荷兰路由前缀被暴露，并且有**470条**KPN路线通过了中国电信的网络。同样的情况也发生在64条Swisscom路由上，有**200个**瑞士路由前缀被暴露

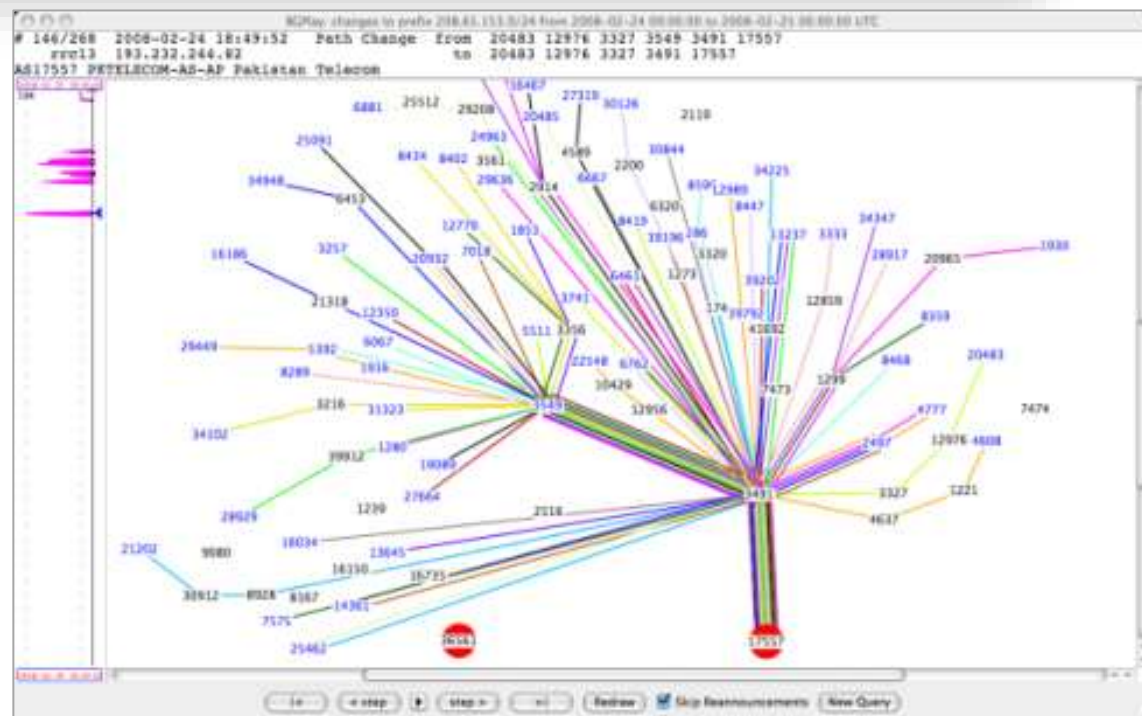


域间路由安全

2008年，巴基斯坦电信劫持YouTube流量，导致YouTube断网2小时，全球很多用户无法访问



AS36561 (YouTube) 通告208.65.152.0/22



AS17557 (Pakistan Telecom) 通告208.65.153.0/24
劫持YouTube流量



第3节 路由源验证

- ✓ Internet Routing Registry
- ✓ Resource Public Key Infrastructure
- ✓ Mutually Agreed Norms for Routing Security



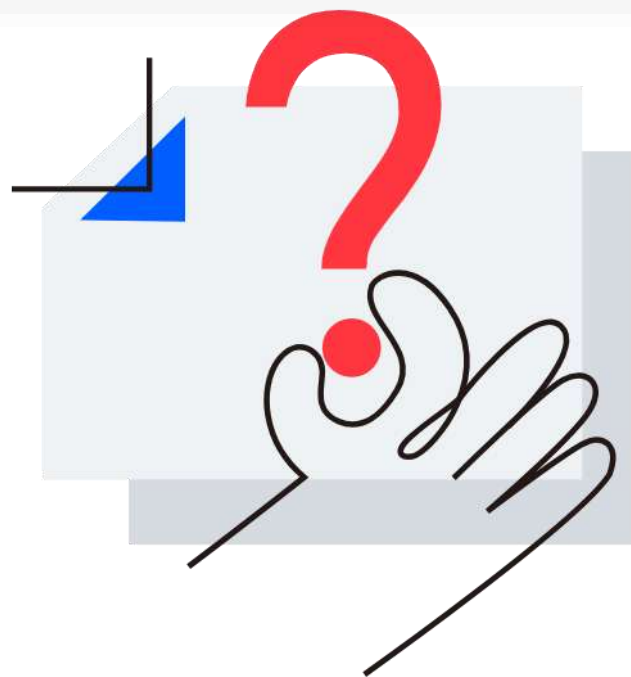
路由防劫持

BGP缺陷

- BGP假设运营商都是可信的，缺乏内建安全机制，没有检查路由是否正确
- 无法有效抵御恶意攻击（路由劫持/路由泄漏），且无法识别配置错误

如何保障路由安全，避免路由劫持/泄漏和配置错误？

- **可靠的IP前缀和自治系统的绑定关系和策略**
- 全球互联网路由选择的稳定性、一致性和安全性
- 路由过滤，防止意外或恶意的路由声明

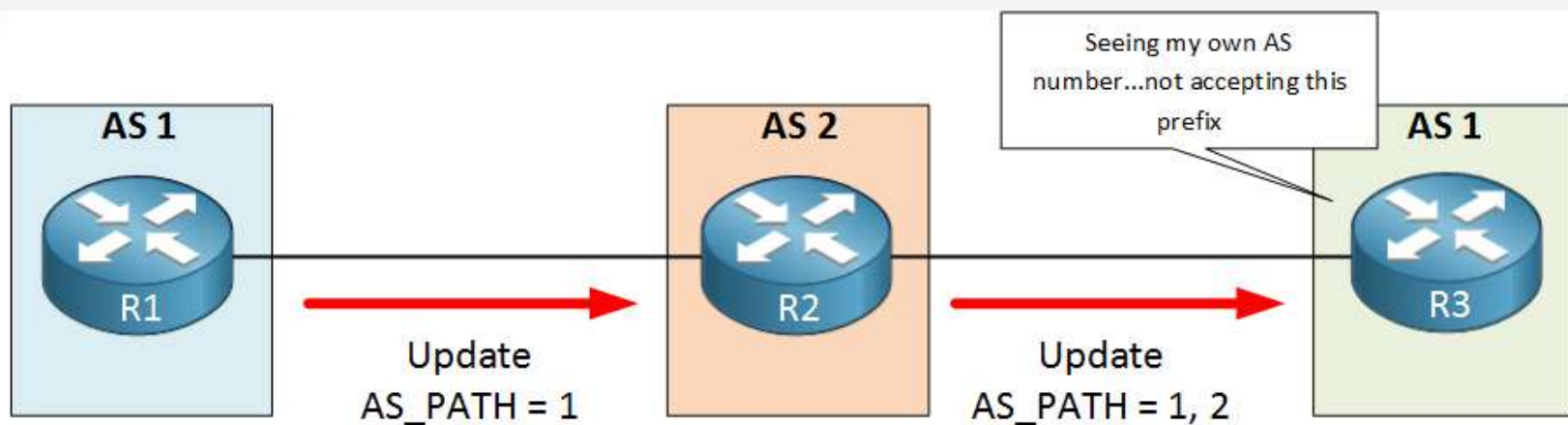




路由过滤

路由过滤 - 决定在路由表或网络中允许哪些路由，以及向邻居宣布哪些路由：

- 不接受BOGON ASN
- 不接受BOGON 前缀
- 不接受自己的前缀
- 不接受前缀长度大于24的前缀
- 不接受AS PATH太长的前缀等





认识IRR：全球路由策略分布式数据库

IRR标准化工作开始于1995年，旨在：

- 保证全球互联网路由的稳定与一致性(RFC 2622)
- 排除路由问题，查询对等协议(RFC 2650)
- 自动配置骨干路由器(RFC 2650)

RFC-1786: RIPE-181

RFC-2622: Routing Policy Specification Language

RFC-2650: Using RPSL in Practice

RFC-2726: PGP Authentication for RIPE Database Updates

RFC-2725: Routing Policy System Security

RFC-2769: Routing Policy System Replication

RFC-4012: Routing Policy Specification Language next generation (RPSLNg)



Internet Routing Registry (IRR) : 全球路由策略分布式数据库
<http://www.irr.net>



Routing Policy Specification Language

```
route:
descr:
origin:
remarks:
remarks:
remarks:
notify:
mnt-by:
changed:
source:
last-modified:
1.0.7.0/24
Proxy route object registered by AS2764
AS38803
This route object was created by AAPT on behalf of a customer.
As some of AAPT's upstream networks filter based on IRR objects,
this route object has been created to ensure that the advertisement
of this prefix is not rejected.
routing.shared@aapt.com.au
MAINT-AS2764
nobody@aapt.com.au 20210408
RADB
2023-11-13T16:16:49Z
```

属性

属性值

```
as-set:
descr:
members:
mnt-by:
changed:
source:
last-modified:
AS151000:AS-MAXCLOUD
Maxcloud Customer
AS151000,AS140389,AS138865,AS140476
MAINT-AS151000
heru@maxcloud.id 20240207 # 0404Z
RADB
2024-02-07T04:04:12Z
```

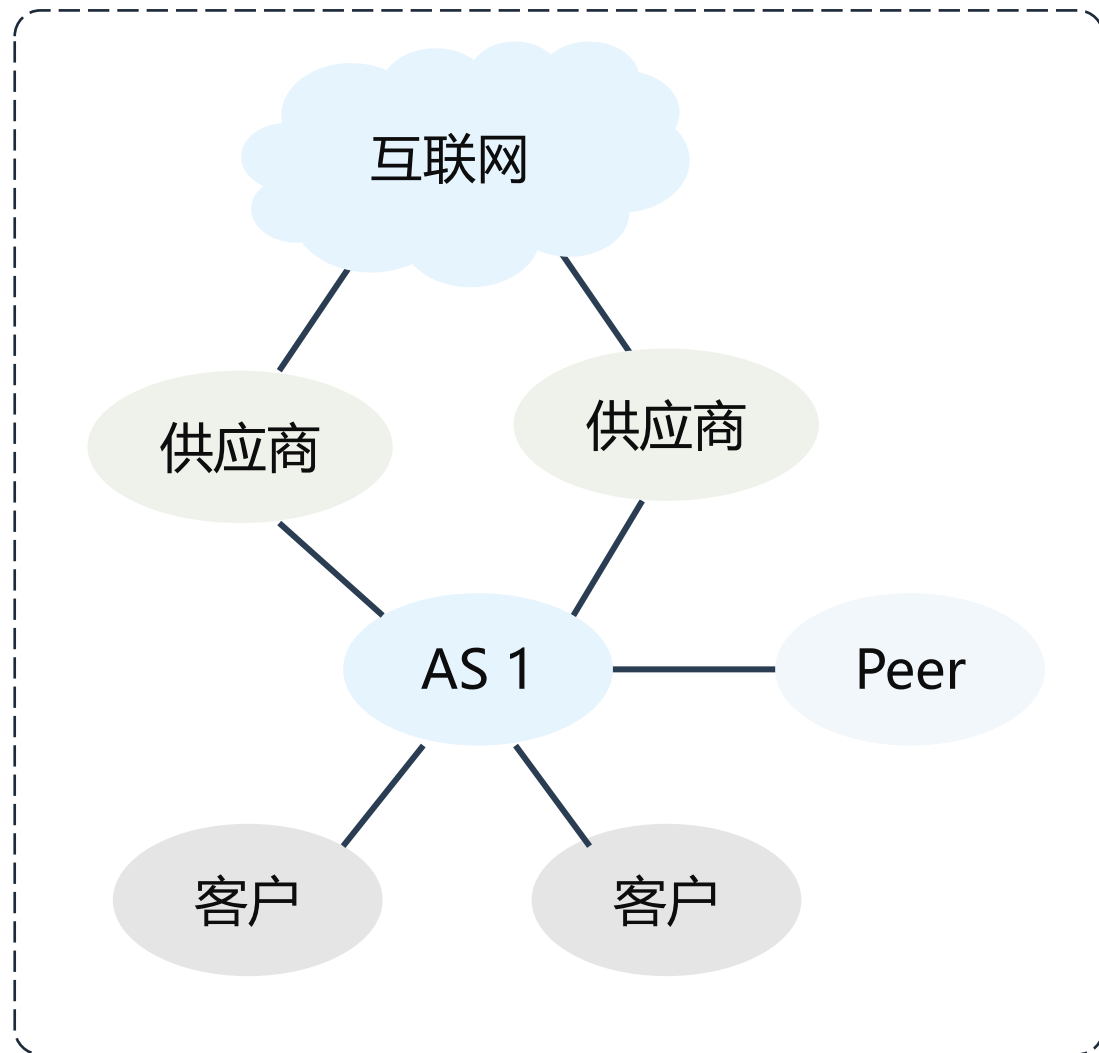
- RPSL基于RIPE-181, 定义了IRR 数据的语法和格式
- 路由信息通过一个或多个对象之间关系表达
- 独立于供应商, 可进行扩展

IRR使用Routing Policy Specification Language (RPSL/RPSL- NG) 定义对象



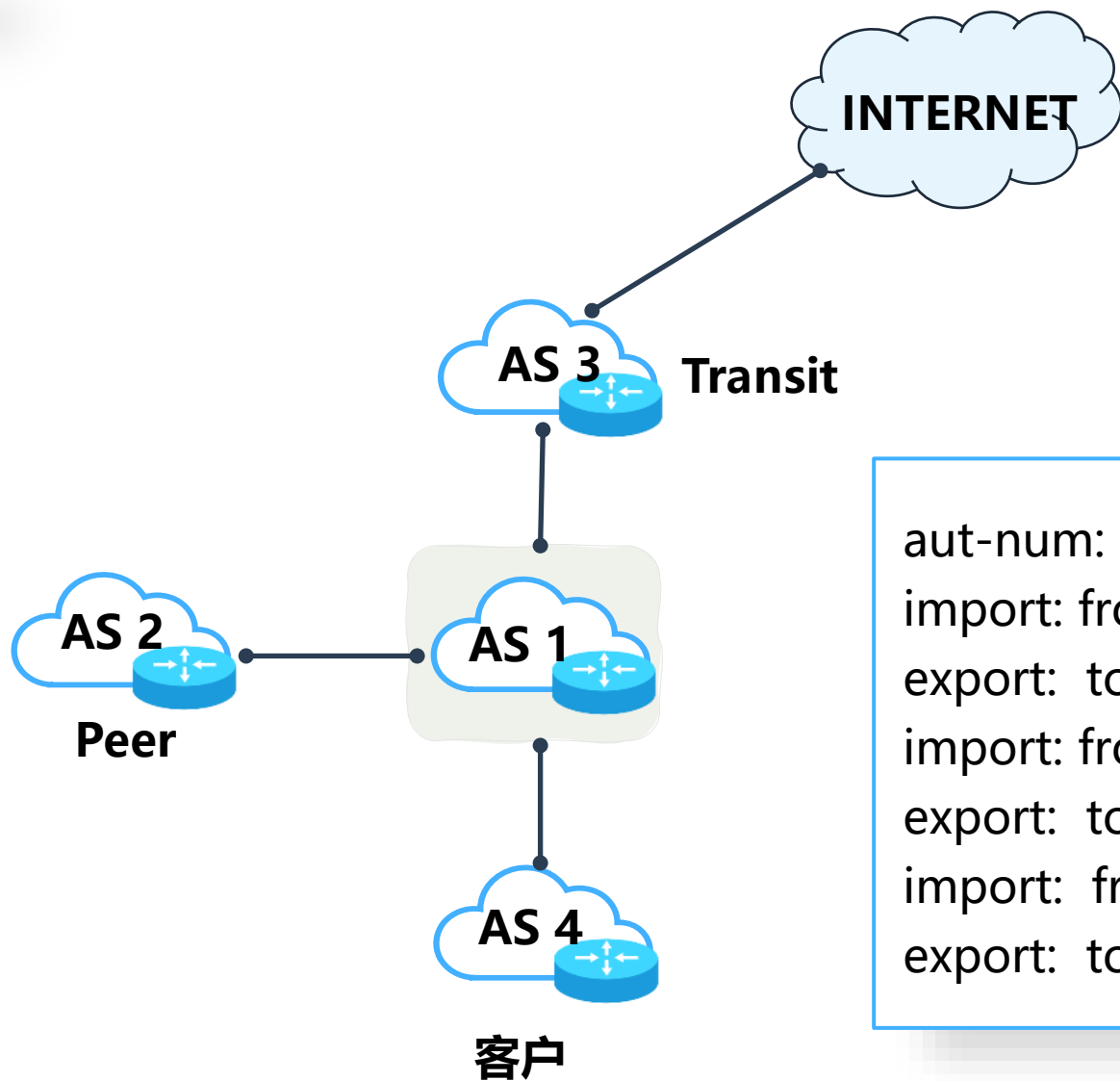
路由策略

- 与哪些AS连接，BGP Peer包括哪些
- 与他们的BGP关系：
 - 客户
 - 供应商
 - Peer
- 针对每类关系/AS的路由决策：
 - 接收哪些前缀
 - 宣告哪些前缀
 - 如果有多条路由，哪个前缀优先





路由策略



aut-num:

import: from AS3 accept ANY

export: to AS3 announce AS1 AS4

import: from AS4 accept AS4

export: to AS4 announce ANY

import: from AS2 accept AS2

export: to AS2 announce AS1 AS4

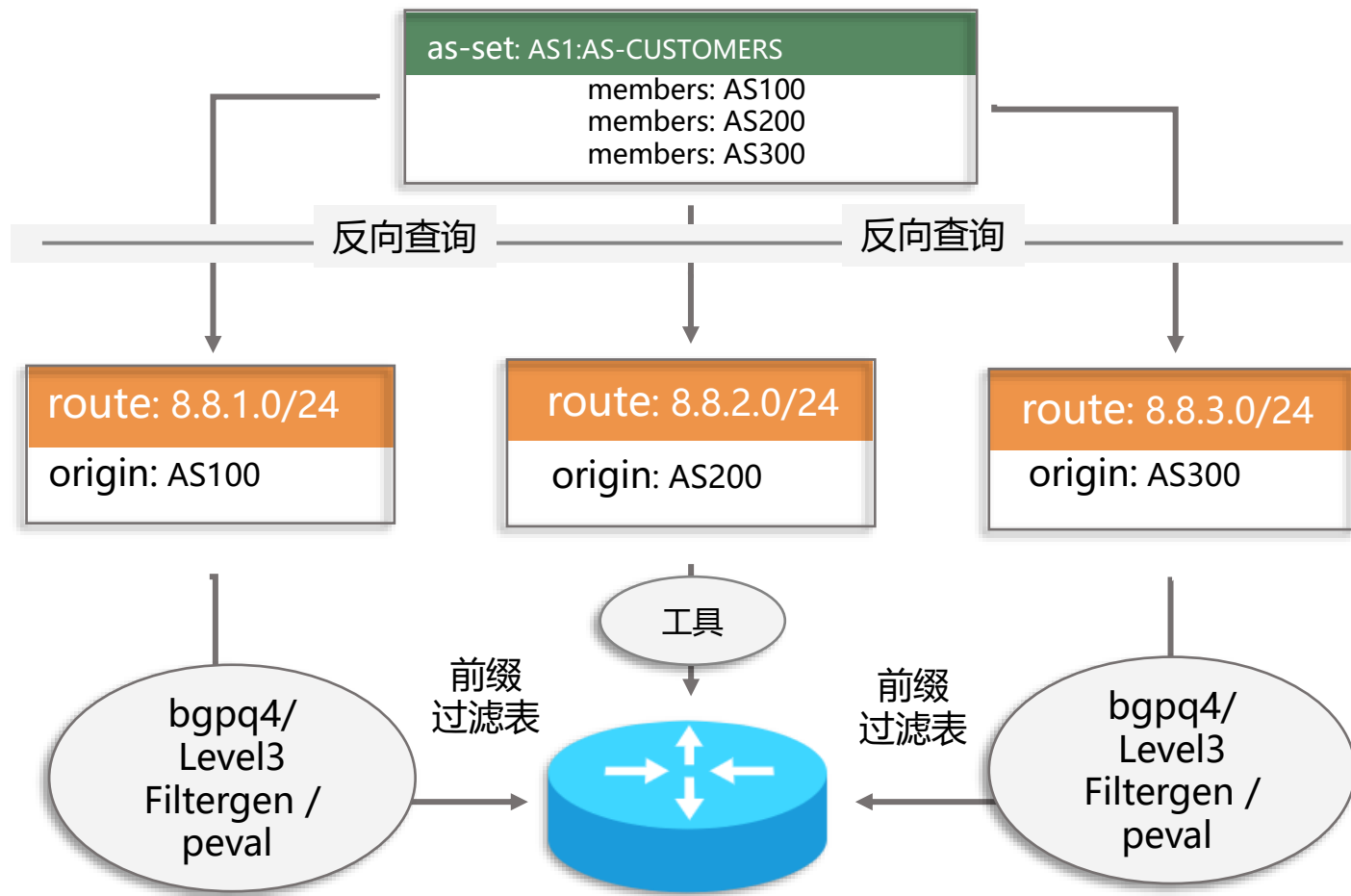
Transit供应商

下游客户

Peer



生成过滤表

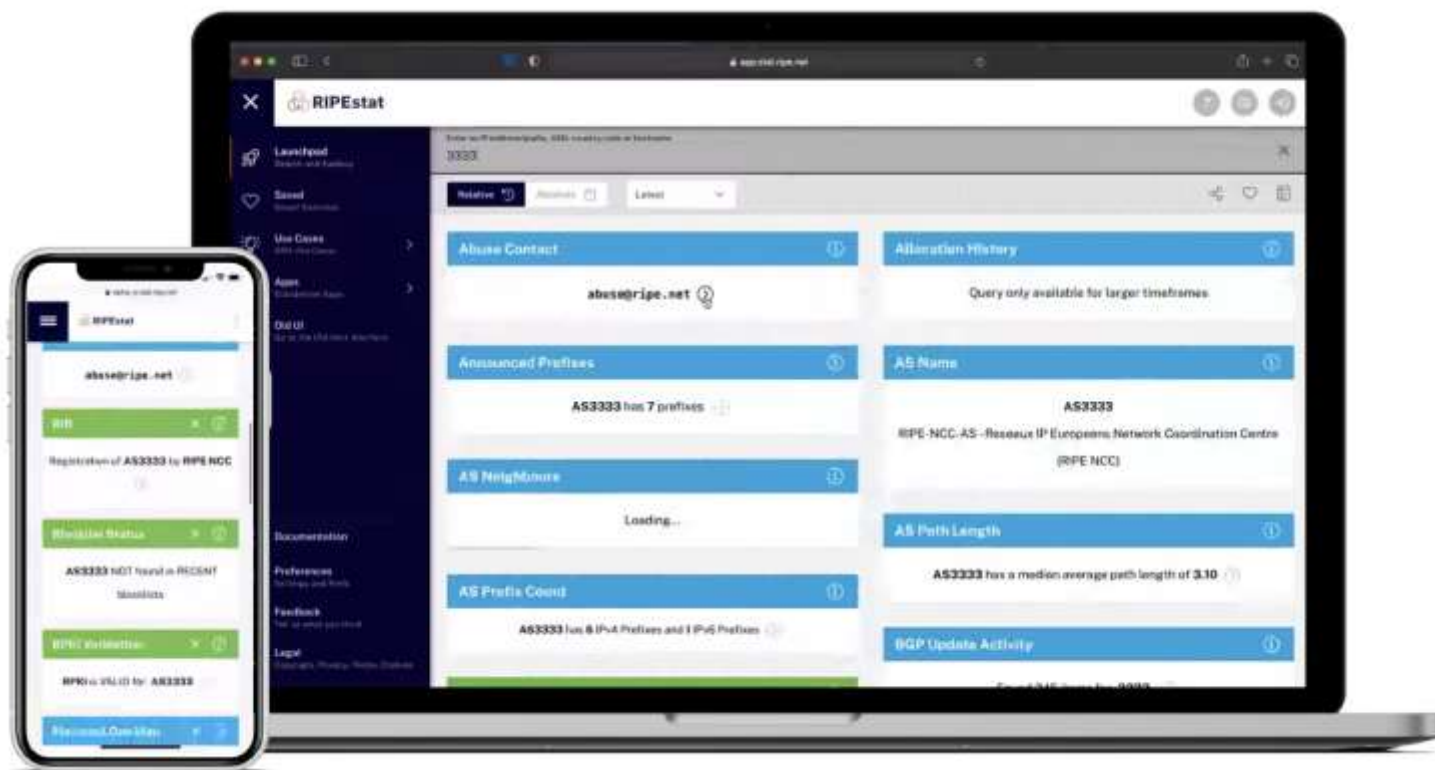


图中IP Prefix仅限于举例说明，并非真实分配

基于route对象和as-set对象，借助自动化IRR工具，生成路由过滤表



查看IRR状态平台/工具



<https://irrexplorer.nlnog.net/>

<https://stat.ripe.net/>



IRR存在问题

数据的准确性问题

IRR中的数据依赖于网络管理员和ISP主动更新和维护，但很多组织未及时更新或提供准确的信息，导致数据可能不准确或过时

缺乏统一标准

IRR缺乏统一的标准和规范，导致不同的IRR数据库之间存在差异和不一致，使得数据的比对和交换变得困难

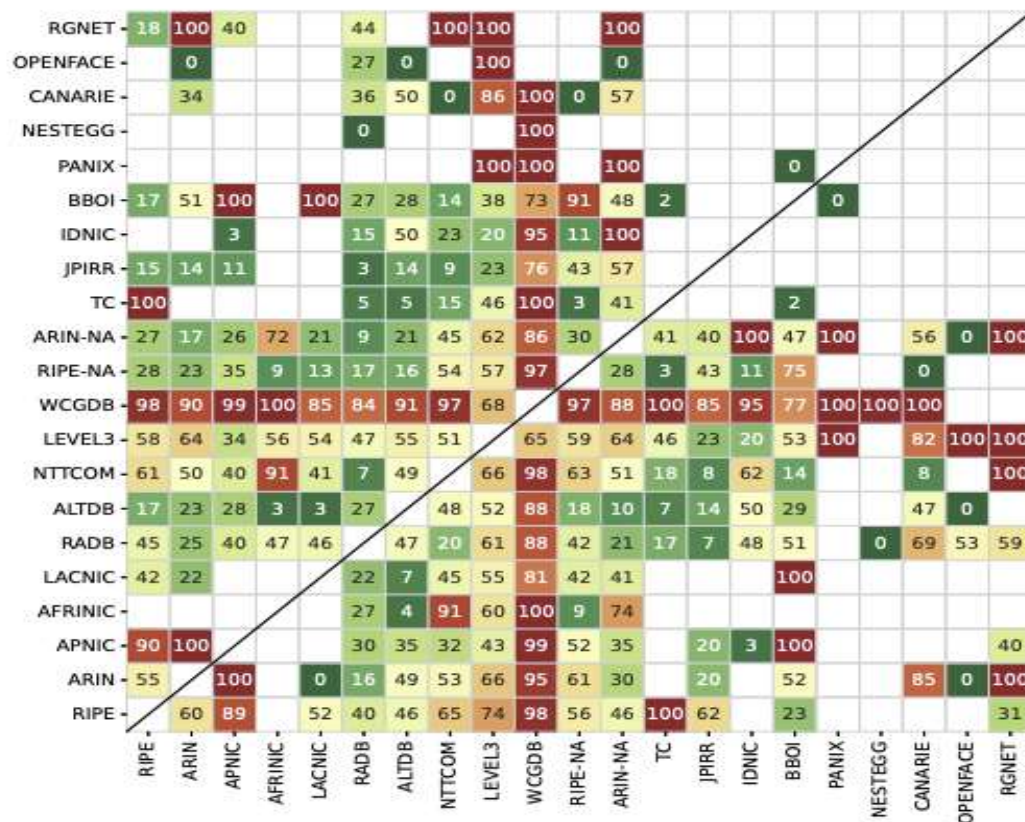
数据的可信性问题

IRR中的数据可以被任何人修改和更新，缺乏验证机制，容易受到恶意篡改或误操作的影响，导致可信性受到质疑

管理和维护的复杂性

IRR的管理和维护需要网络管理员和ISP主动参与，但这需要一定的技术知识和时间投入

IMC '23, October 24–26, 2023, Montreal, QC, Canada



BEN DU, KATHERINE IZHIKEVICH, SUMANTH RAO, 等. IRRegularities in the internet routing registry[C/OL] //Proceedings of the 2023 ACM on internet measurement conference. New York, NY, USA: Association for Computing Machinery, 2023: 104-110.

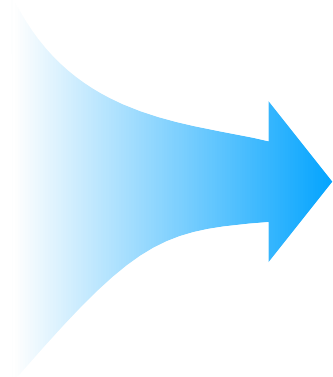





认识RPKI

RPKI



- IRR数据不可以被完全信任
 - 准确性
 - 不完整数据
 - 可维护性
- 第三方数据库广泛使用
- 缺乏验证



-  将IP地址和ASN使用公钥绑定
-  遵循注册时的层次结构
-  资源持有者的授权声明
 - ASN X被授权使用我的前缀Y
 - 签名

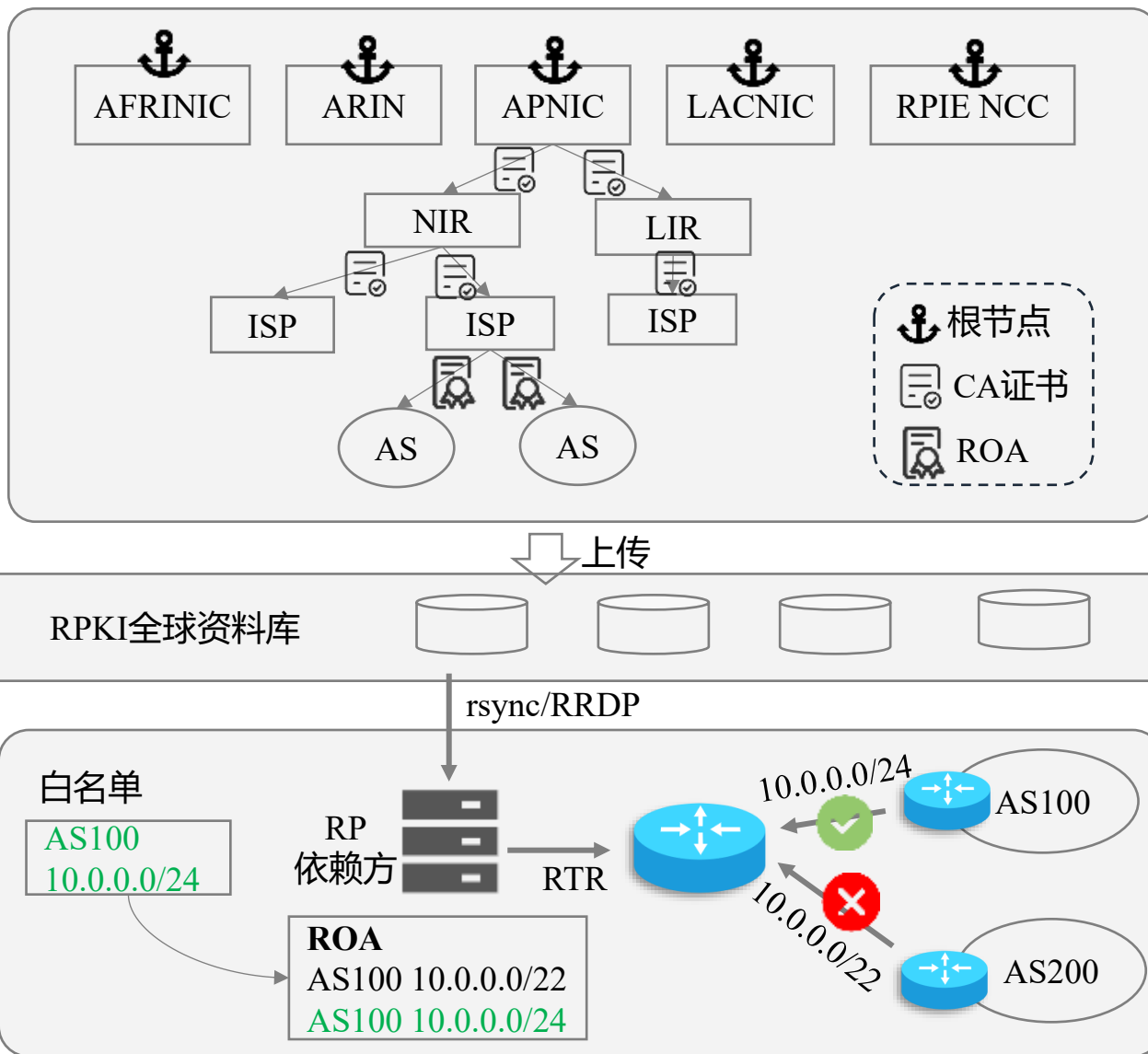


RPKI整体架构

RPKI是一种数字证书系统，对码号资源提供密码学证书

ROA是指某个IP地址所有者将IP地址授权给某个AS

RPKI依赖方(RP) 是连接RPKI与互联网域间路由的桥梁



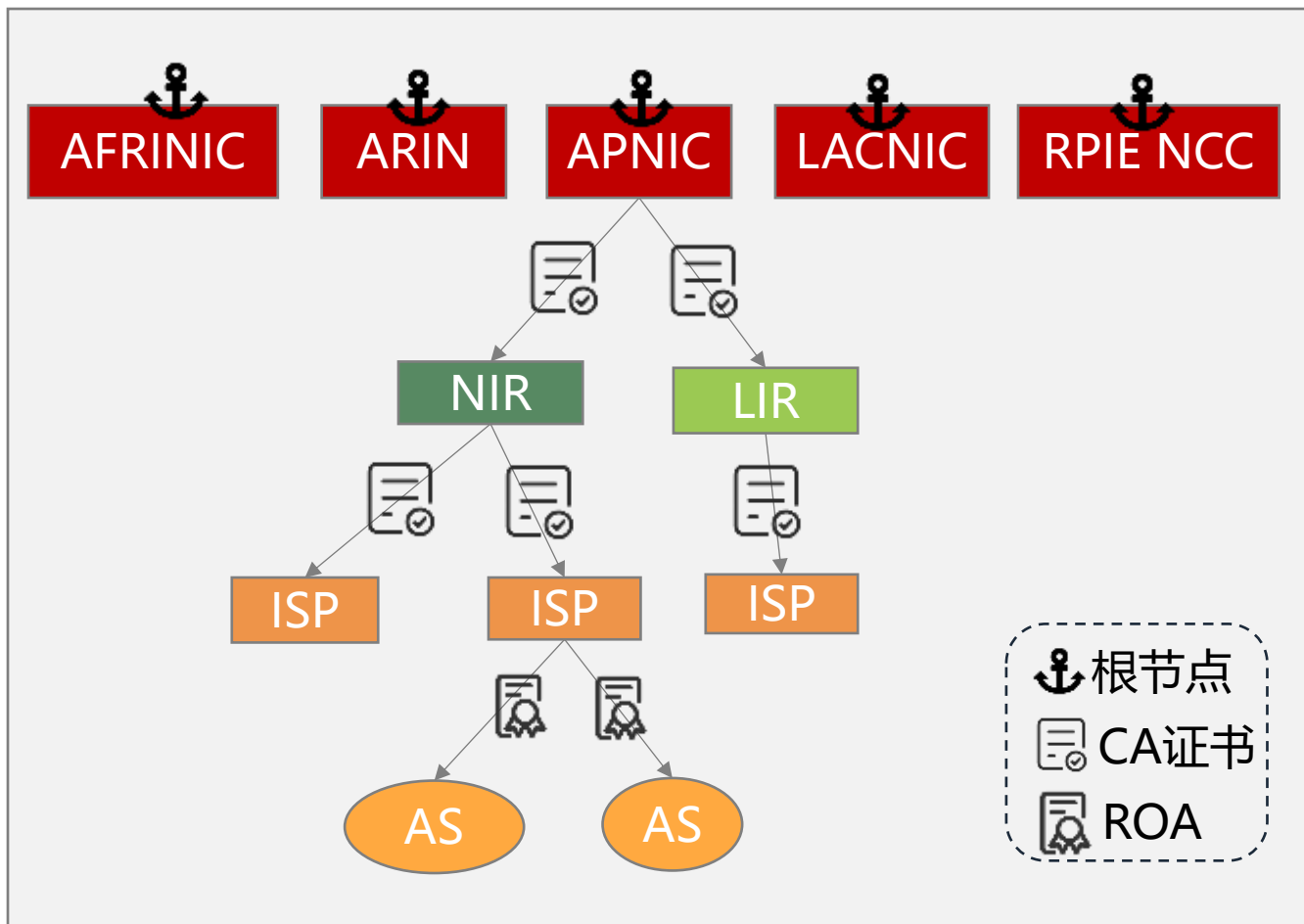
RPKI**证书**包括CA和EE，CA证书用来担保IP和AS分配。EE证书用于路由源授权

RPKI资料库是储存证书和签名的数据库

互联网资源分配机构，自上而下包括IANA、RIR、NIR、LIR、ISP



RPKI证书签发体系



RPKI通过逐级签发数字证书

- RIR签发自签名的根证书
- RIR使用根证书为NIR/LIR/ISP签发资源证书
- 逐级签发.....
- ISP使用自己EE证书签发ROA, 将AS与IP前缀绑定在一起



什么是ROA

Route
Origin
Authorization

Prefix

正在为其创建ROA的网络

Origin
ASN

应该发起BGP宣告的ASN

Max
Length

ROA被授权可以宣告的最大前缀长

ROA对象是经过加密签名的对象，在RPKI框架中用于声明AS被授权发起的IP前缀

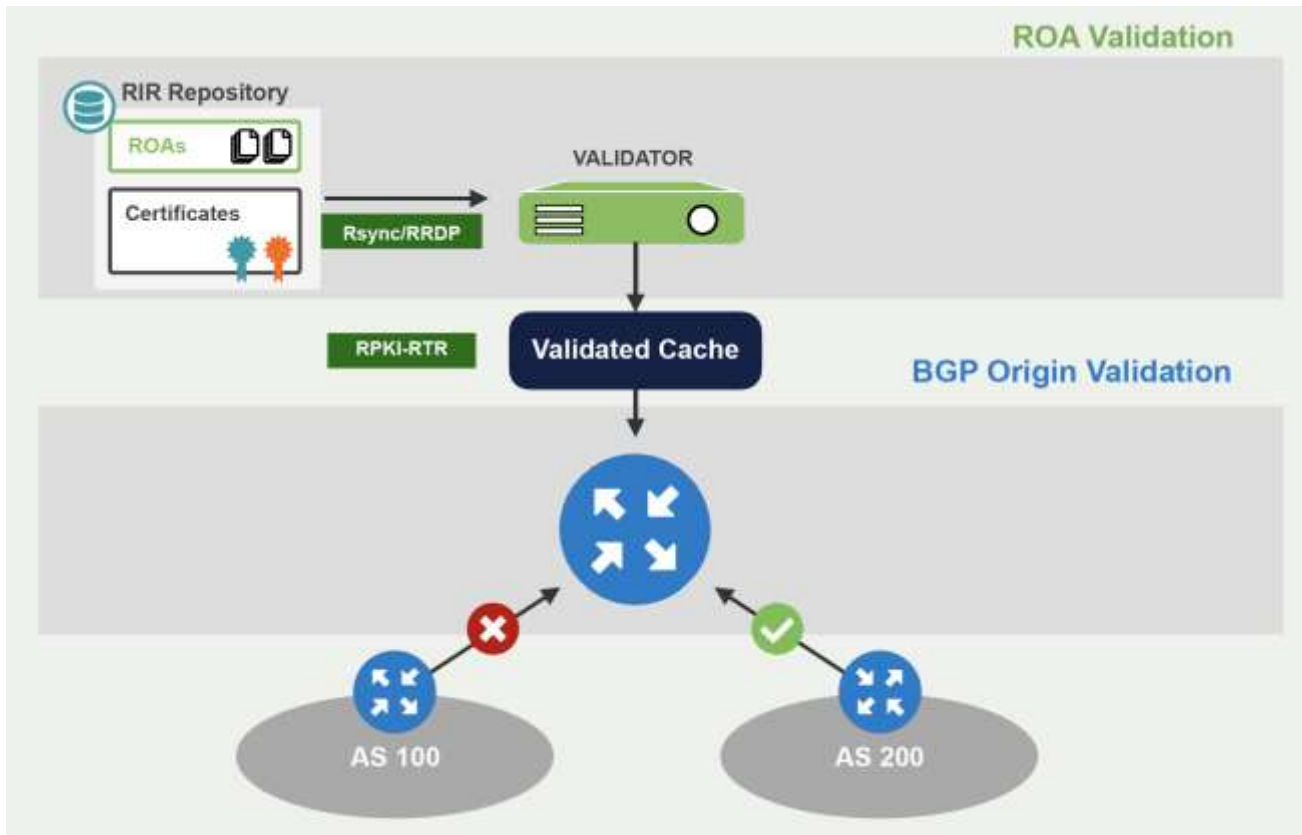
Route Origin Authorization (ROA)

Origin ASN:	17771
Not Valid Before:	2010-12-07 00:00:00
Not Valid After:	2011-12-07 23:59:59
Prefixed:	2405:le00::/32 (max length /48) 202.63.96.0/19 (max length /24) 49.238.32.0/19 (max length /32)





ROA验证

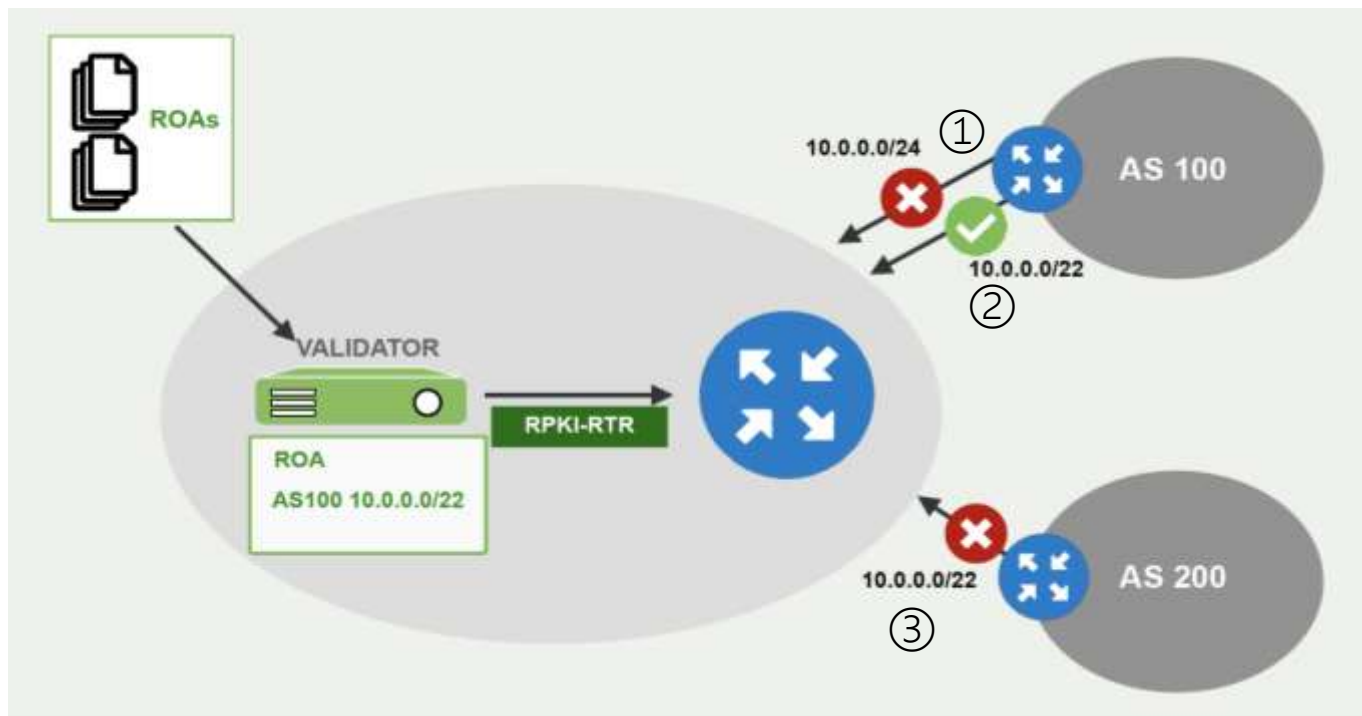


ROA同步与验证

- 定时通过Rsync/RRDP协议，从各RIR仓库同步证书及签名对象
- 沿证书链验证ROA有效性
- 生成最佳的路由过滤表
- 通过RTR协议下发到边界路由器



路由源验证

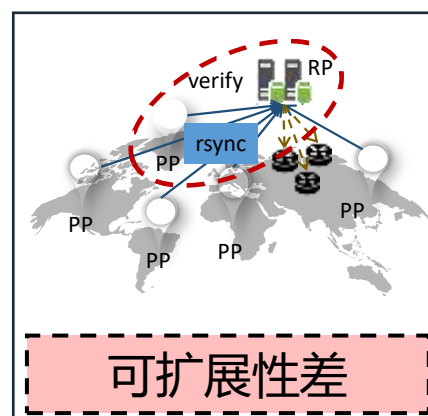
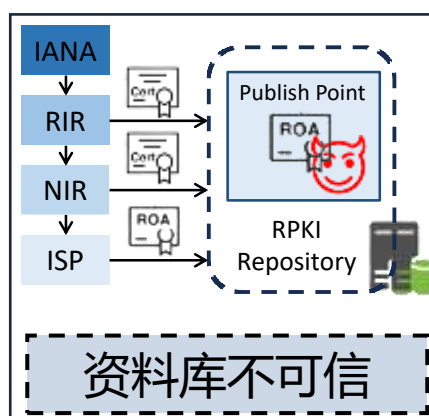
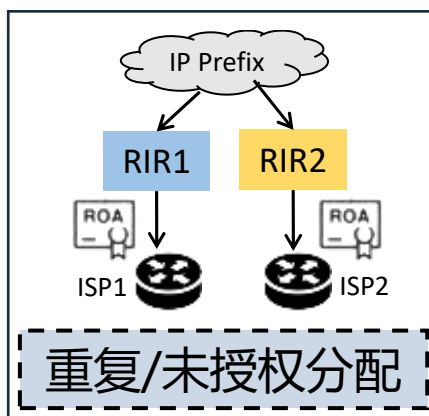
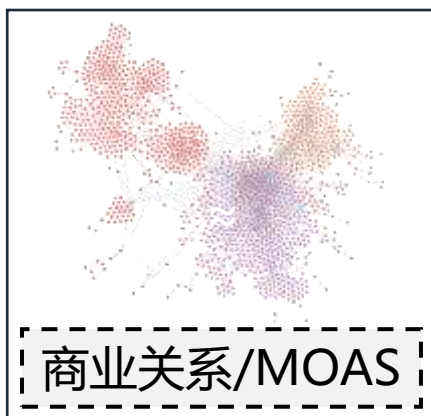
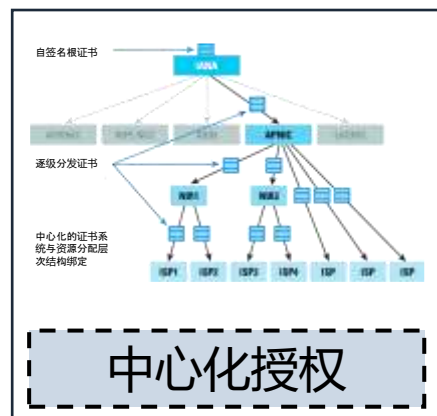
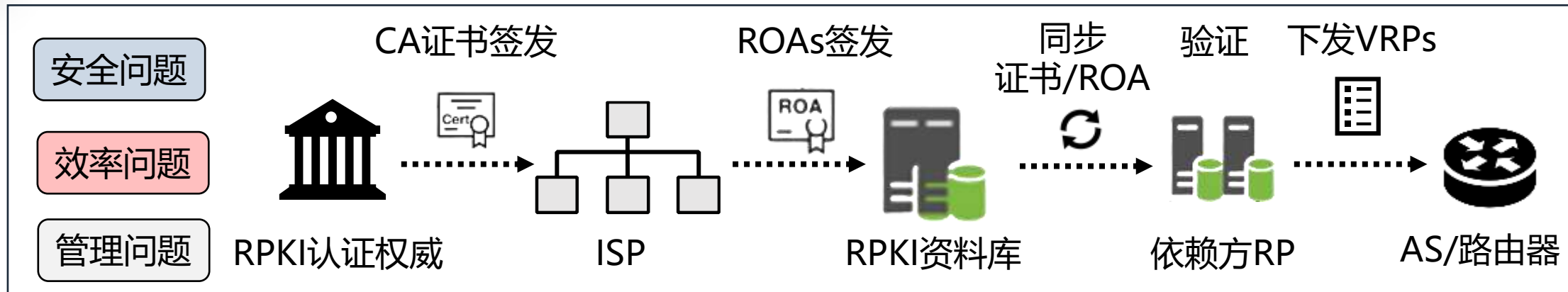


根据RFC6811，ROV根据注册授权的相关信息，对路由宣告进行验证，包括以下几种状态：

- 前缀未匹配
- 前缀匹配，源未匹配，图中情况③
- 前缀、源匹配，宣告前缀长度 $>$ Max Length，图中情况①
- 前缀、源、Max Length均匹配，图中情况②



RPKI 局限性

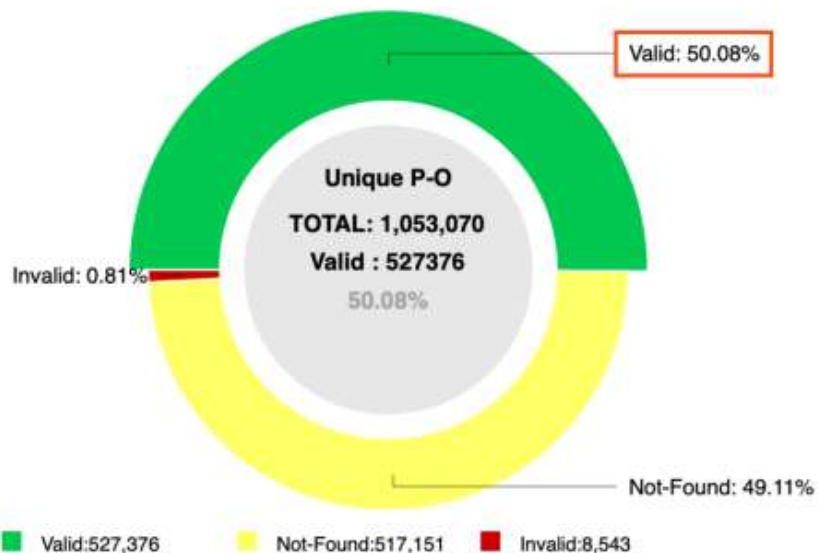


体系结构的固有缺陷+尚处于部署初期存在未暴露的安全隐患



RPKI 部署进展

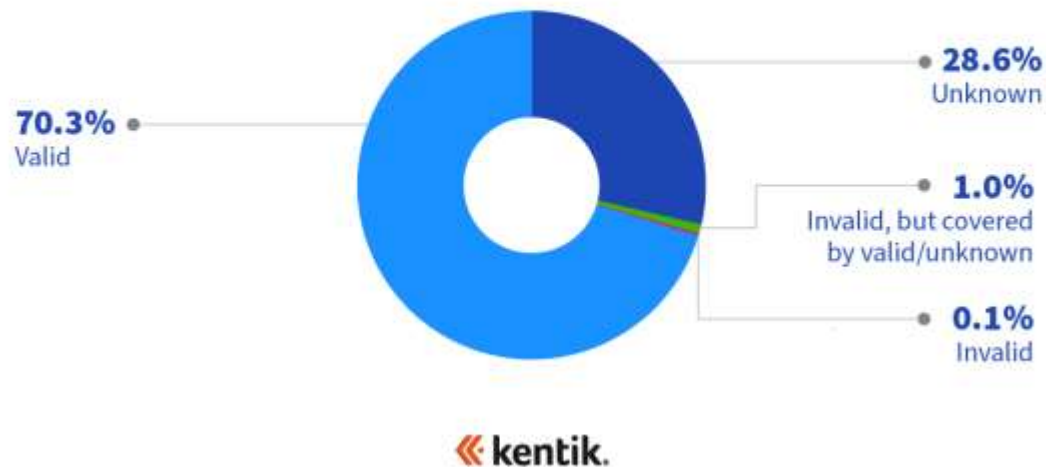
RPKI-ROV analysis of unique prefix-origin pairs (IPv4)



NIST RPKI Monitor: RPKI-ROV Analysis Protocol: IPv4 RIR: All Date: 2024-05-01 00:00

Internet traffic volume by RPKI evaluation

May 2024



2024年5月1日，互联网IPv4地址RPKI部署率第一次超过50%
承载流量比例已经超过70%



为什么路由安全那么难

成因分析

- 每个网络都有责任实施基本的路由安全实践来应对威胁
- 但是，实施最佳实践并不能带来很多立竿见影的好处。它需要花费时间和金钱，而且网络可能无法为此收取额外费用
- 即使做的一切都是正确的，安全仍然掌握在其他网络手中
- 导致大家注册/更新可靠路由源意愿较低



- 网络运营商有责任确保全球路由基础设施的稳健和安全
- 网络安全取决于路由基础架构，它能清除对互联网造成破坏的不良行为者和意外错误配置
- 网络运营商合作得越多，事故就会越少，造成的破坏也就越小

责任与安全



Mutually Agreed Norms for Routing Security (MANRS)

- MANRS 以参与者之间的协作和对互联网基础设施的共同责任为基础，提高了全球互联网路由系统的安全性和可靠性
- MANRS则分别针对四类参与者，创建了相关项目

网络运营商

CDN和云提供商

互联网交换节点

设备厂商



网络运营商项目

网络运营商项目作为首个项目，也是MANRS最重要的项目，于 2014 年发起，当前共有928个参与方。目标包括：

- 提高对路由安全问题的认识，并鼓励实施能够解决这些问题的行动
- 促进对互联网全球路由系统的安全性和弹性承担集体责任的文化
- 展示互联网行业解决路由安全问题的能力
- 为网络运营商提供一个框架，以更好地理解与解决与互联网全球路由系统的安全性和弹性有关的问题





其它项目

CDN和云提供商

于2020年推出，要求出口路由控制，防止安全事件

目标：

- 创建安全对等互联环境
- 鼓励改善路由状态
- 展示责任行为
- 提升对等互联效率



IXPs

于 2018 年推出，通过一套单独的 MANRS 行动来解决 IXP 的独特需求和关切

IXPs 可以实施一些行动来证明其对路由安全的承诺，并显著改善其对等互联关系的弹性和安全性



设备厂商

最新开展的项目，向全球网络提供设备支持和培训指导

目标：

- 作为激励因素
- 对行业产生积极影响，促进对路由安全的认识和支持





MANRS意义与局限性



MANRS 是一个重要步骤

- 安全是一个过程，而不是一种状态
- MANRS 为解决互联网面临的安全问题提供了一种结构和一致的方法
- MANRS 是网络应考虑的最高限度，风险低、成本效益高

MANRS 不是解决互联网所有路由问题的一站式方案，但它是迈向全球强大安全路由基础设施的重要一步

manrs.org



第4节 路径验证



BGPsec



FC-BGP



威胁模型

假设

- 参与全球路由的自治系统均**接入**了互联网范围的**路由源验证**系统，例如RPKI，其中存储了关于自治系统ASN与合法前缀以及可验证公钥的映射信息
- 这样的互联网路由，足够安全吗**

遗憾的是，**答案是否定的！**

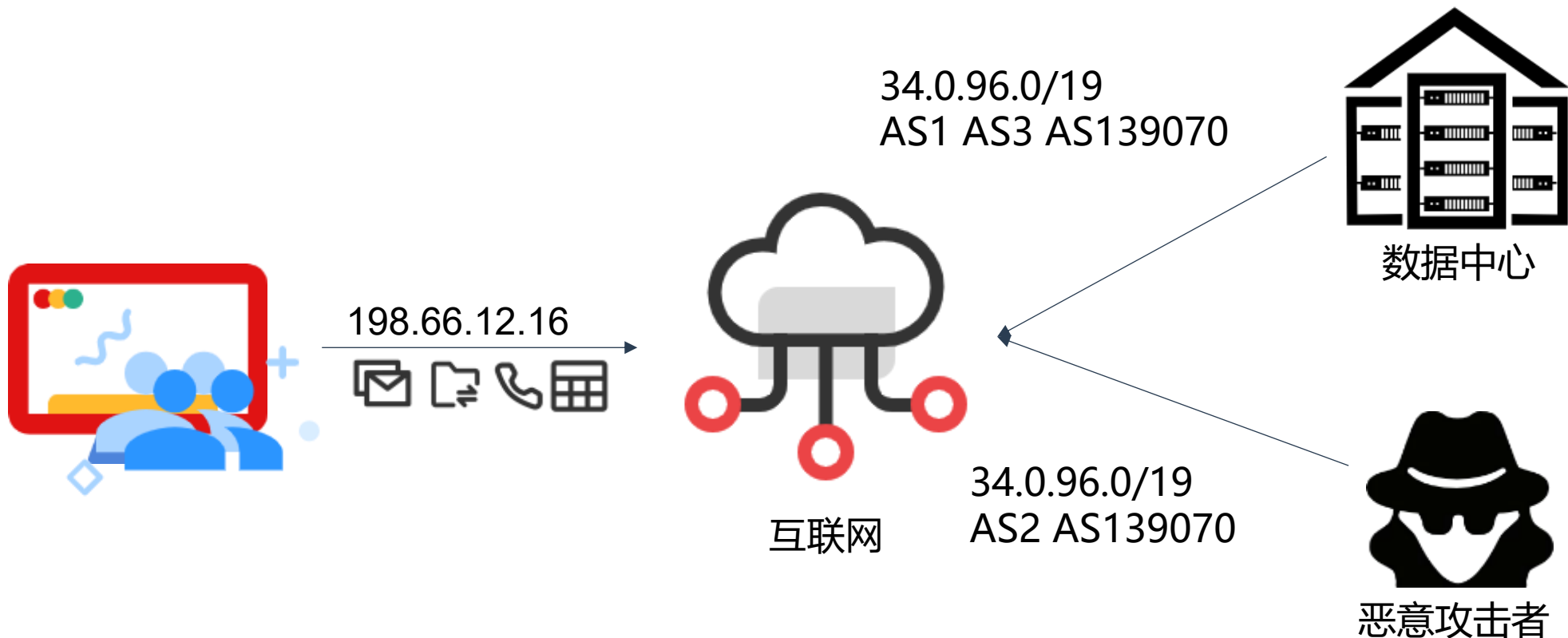
因为，基于RPKI的起源验证：

- 既**不**加密保证（公告未签名）
- 也**不**保证公告的AS_PATH





为什么需要路径验证



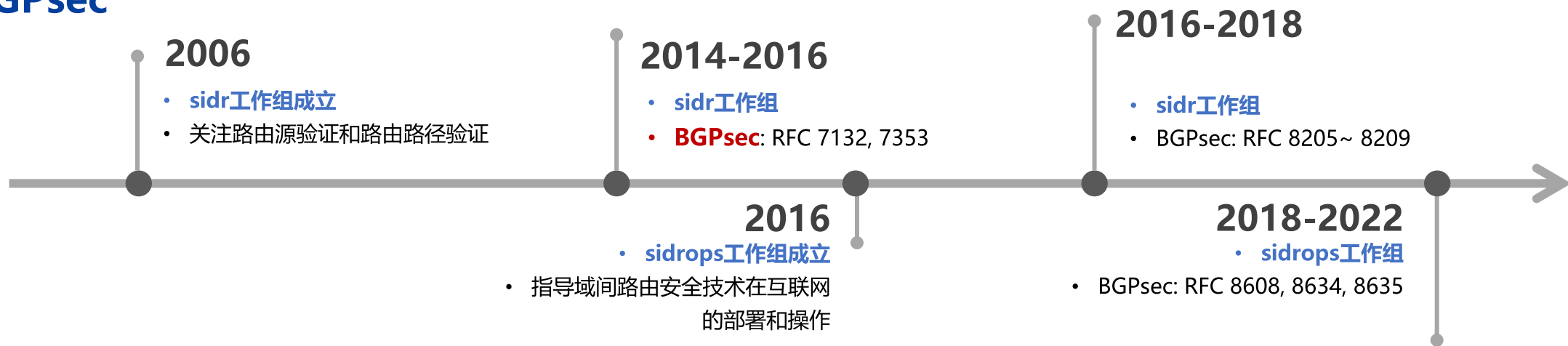
攻击者伪装自己有到正确源ASN的更短路径，**绕过路由源验证**

由于其具有更短的AS_PATH长度，因此最佳路由将指向恶意攻击者



认识BGPsec

BGPsec



RPKI已存在，为什么还需要：

RPKI提供资源分配认证，用于源验证

BGPsec则用于路径验证

RFC7132: BGP路径威胁模型

RFC7353: BGP路径验证安全需求

RFC8205\8206: 协议说明

RFC8207: 运行注意事项

RFC8208\RFC8608: 算法、密钥格式和签名格式

RFC8209: 路由器证书、证书吊销列表和认证请求

RFC8635: 路由器密钥

BGPsec旨在解决域间路由的AS路径篡改问题



BGPsec

BGPsec理念在于**保护AS路径**的传播过程

- 防止恶意插入有效起源
- 防止路径劫持

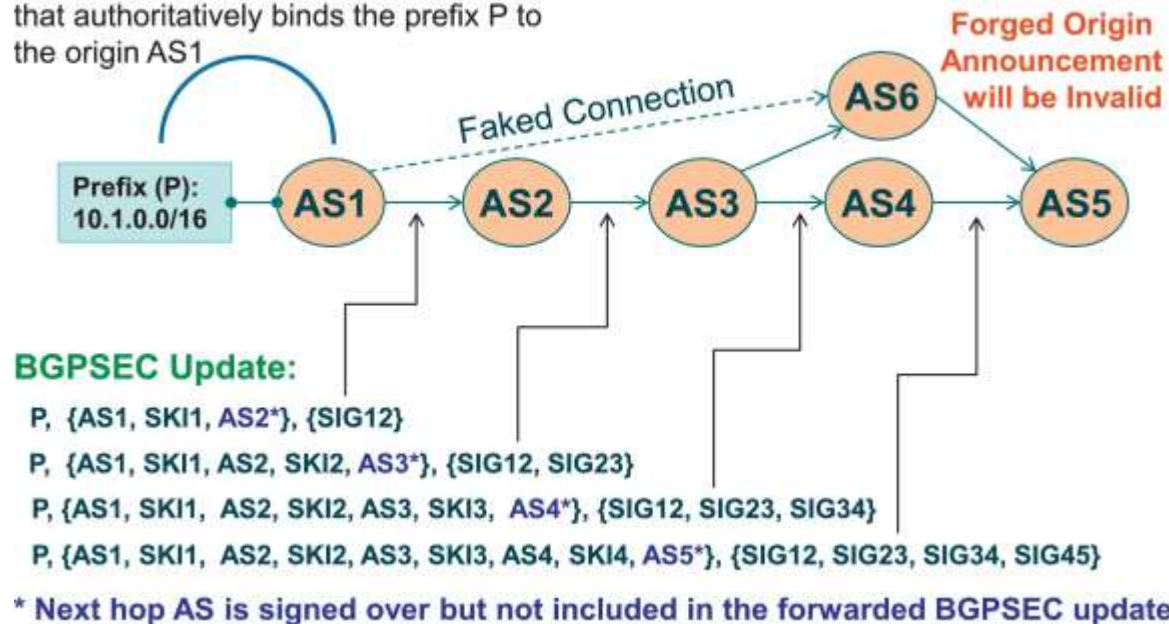
对接收到的所有内容进行签名

- 包括发送给AS，防止通过剪切/粘贴创建已签名路径

BGPsec引入**新的属性和能力**

- 仅向能处理该属性的邻居发送

Route Origin Authorization (ROA) exists that authoritatively binds the prefix P to the origin AS1

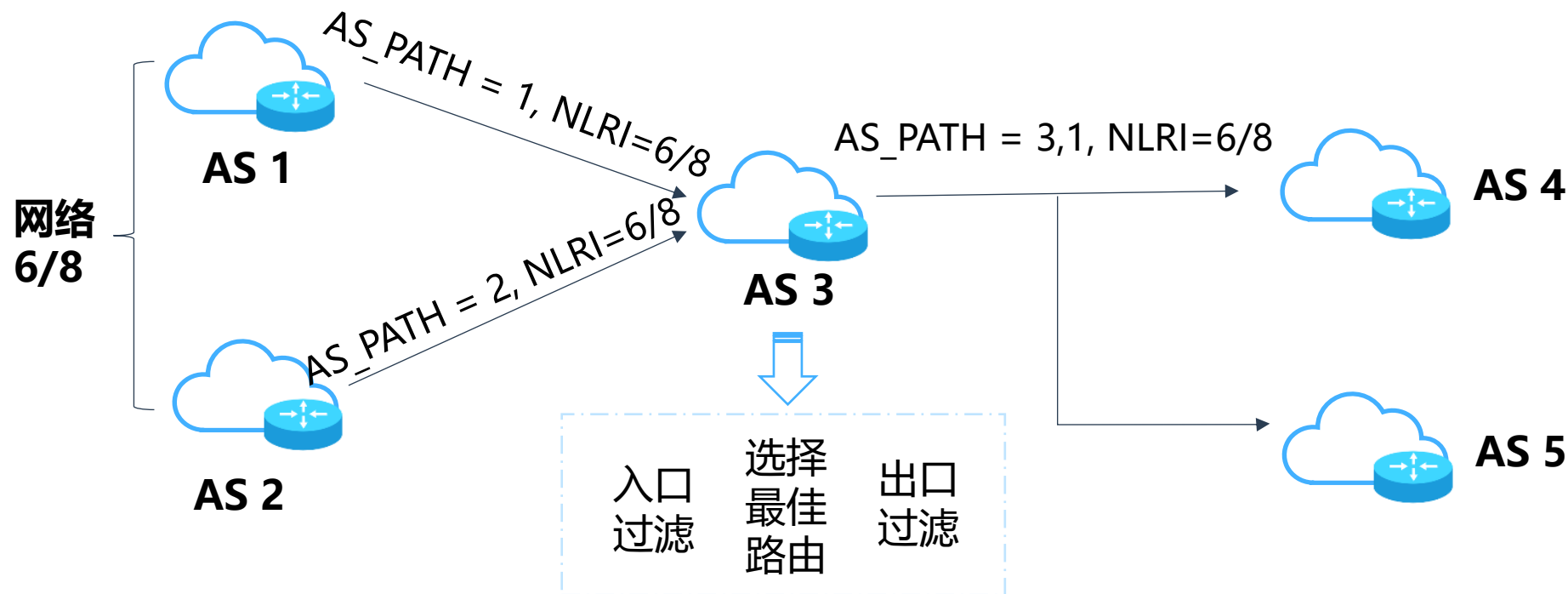


引用: SRIRAM V K, MONTGOMERY D. Design and analysis of optimization algorithms to minimize cryptographic processing in BGP security protocols[J/OL]. Computer Communications, 2017, 106: 75-85..

例如：如果 AS6 假装有到 AS1 的单跳连接，公告前缀P，将不会成功。因为它从未直接从 AS1 收到签名的前缀P的公告报文



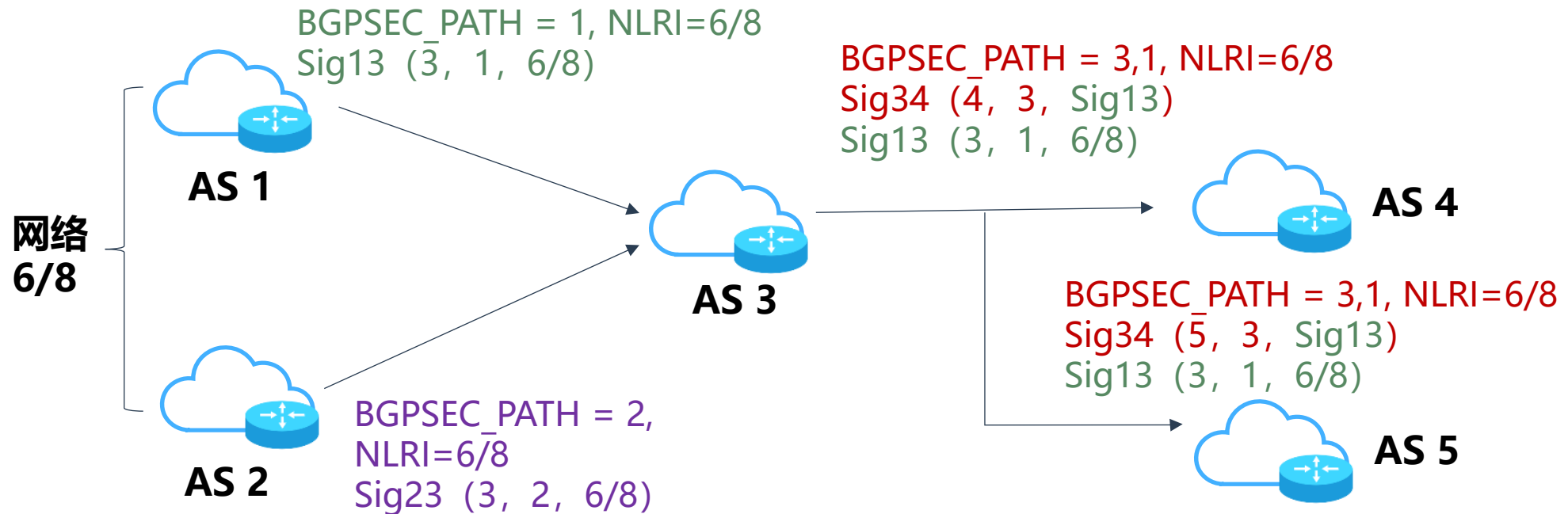
BGP流程 (未部署BGPsec)



- BGP可能从不同路由器接收同一IP前缀
- 入口过滤：决定处理哪些路由
- 根据路由规则，选择一条最佳路由
- 出口过滤：决定发送Update的邻居



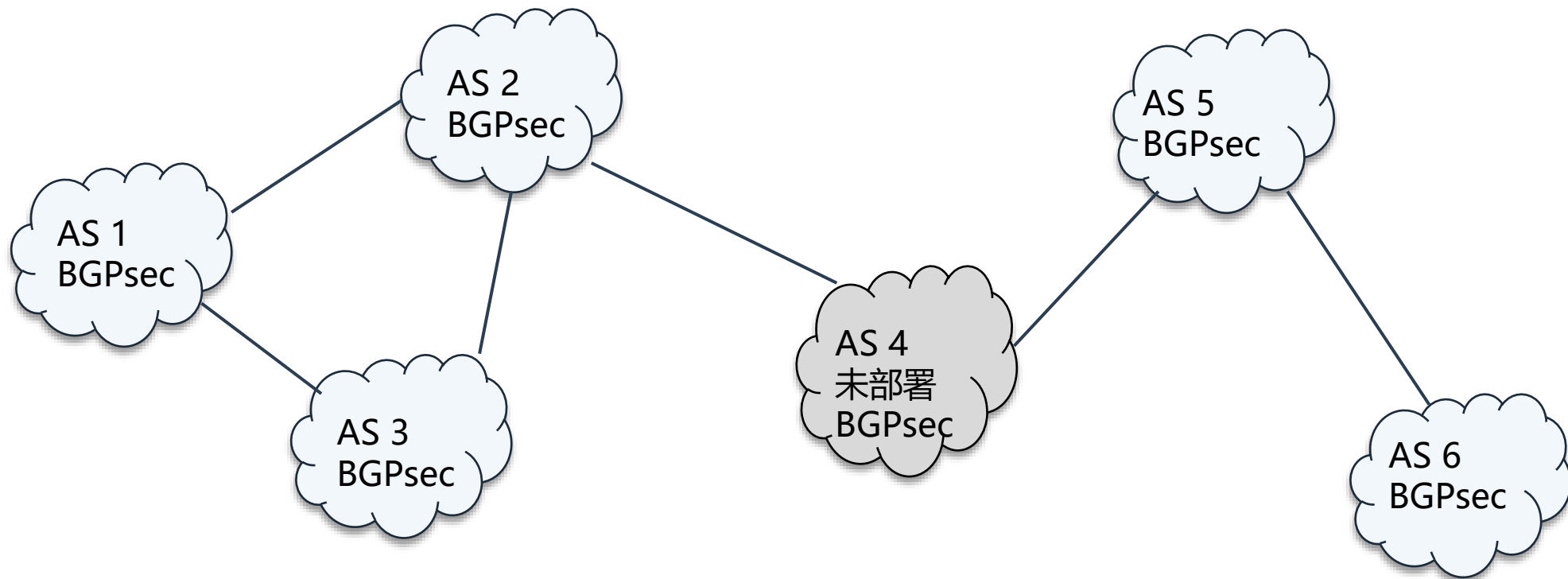
BGPsec流程



- 每个Update均有 BGPsec_PATH 中每个 AS 的签名
 - 每个签名包括到该点的BGPsec_PATH, 以及要发往的AS
- 在入口处, 检查所有签名
- 在出口处, 添加AS时, 在列表中添加新签名
- AS_PATH, 在 BGPsec_Path属性中编码



BGPsec安全性分析



非BGPsec Speaker无法传递BGPsec属性，该路径无法被保护



BGPsec局限性

- **部署率低**
 - BGPsec需要大量资源，现实部署困难
 - 由于需要验证BGPsec的签名，路由器需要具有更强控制面
- **部分部署安全收益问题**
 - 签名验证链断裂，难以确保整条路径真实性
- **安全问题**
 - 暴露签署update的AS和实际路由器
 - BGPsec完全部署仍面临wormhole以及篡改等攻击

acmqueue Why Is It Taking So Long
to Secure Internet Routing?

Routing security incidents can still slip past deployed security defenses

Sharon Goldberg, Boston University

Sharon Goldberg在ACM Queue撰文指出目前的BGP安全机制部署困难，大多无法增量部署

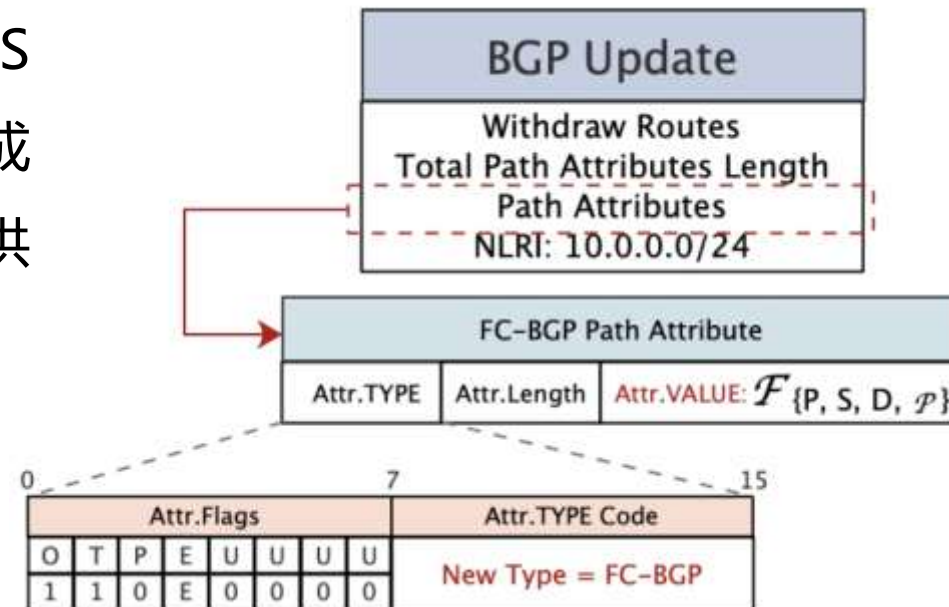




如何改进：FC-BGP

假设AS B收到一个BGP Update报文：P: $S \leftarrow A \leftarrow B$ ，AS B决定将此路由继续传播给自己的邻居AS C。AS B将生成如下的FC (Forwarding Commitment) 来向其它AS提供可公开验证的路由意愿

$$\mathcal{F}_{\{A,B,C,\mathcal{P}\}} = \left\{ \mathcal{H}(A, B, C, \mathcal{P})_{\text{Sig}_B} \parallel A \parallel B \parallel C \right\},$$



- FC-BGP设计了一种逐段验证路由宣告路径的机制，相比以BGPsec为代表的全路径验证机制，具备以下优势：
 - ✓ 完全部署时相同的安全收益，与更低的验证开销
 - ✓ 兼容部分部署场景，提供此场景下明确的安全收益
- FC并不会造成额外的路由策略隐私泄漏



FC-BGP核心设计：分段验证



BGP路由场景与语义信息：AS A向AS B宣告前缀P，AS B准备将此路由宣告给AS C

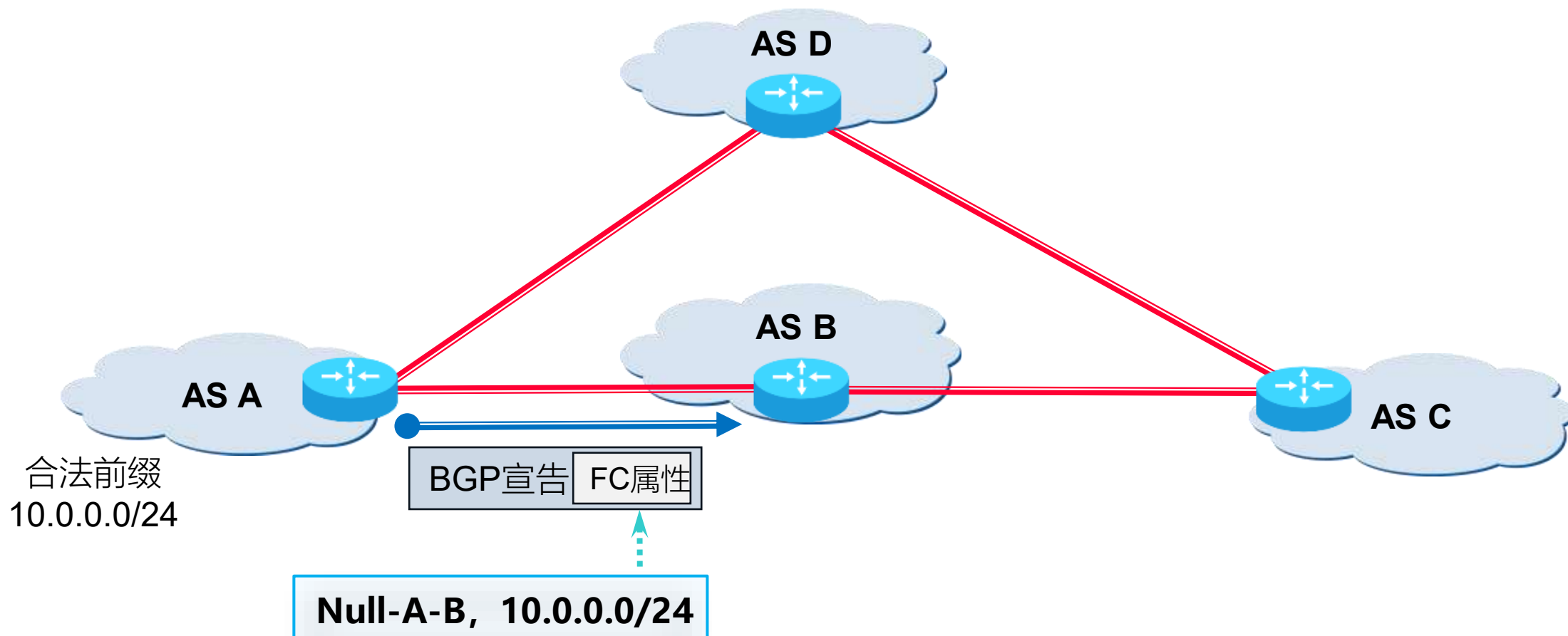
拼接 (A, B, C, P) ，并用AS B私钥签名，保障BGP路由语义的完整和不可篡改

可传递的BGP路径属性FC (Forwarding commitment)

$$\mathcal{F}_{\{A, B, C, P\}} = \left\{ \mathcal{H}(A, B, C, P)_{\text{Sig}_B} \parallel A \parallel B \parallel C \right\},$$

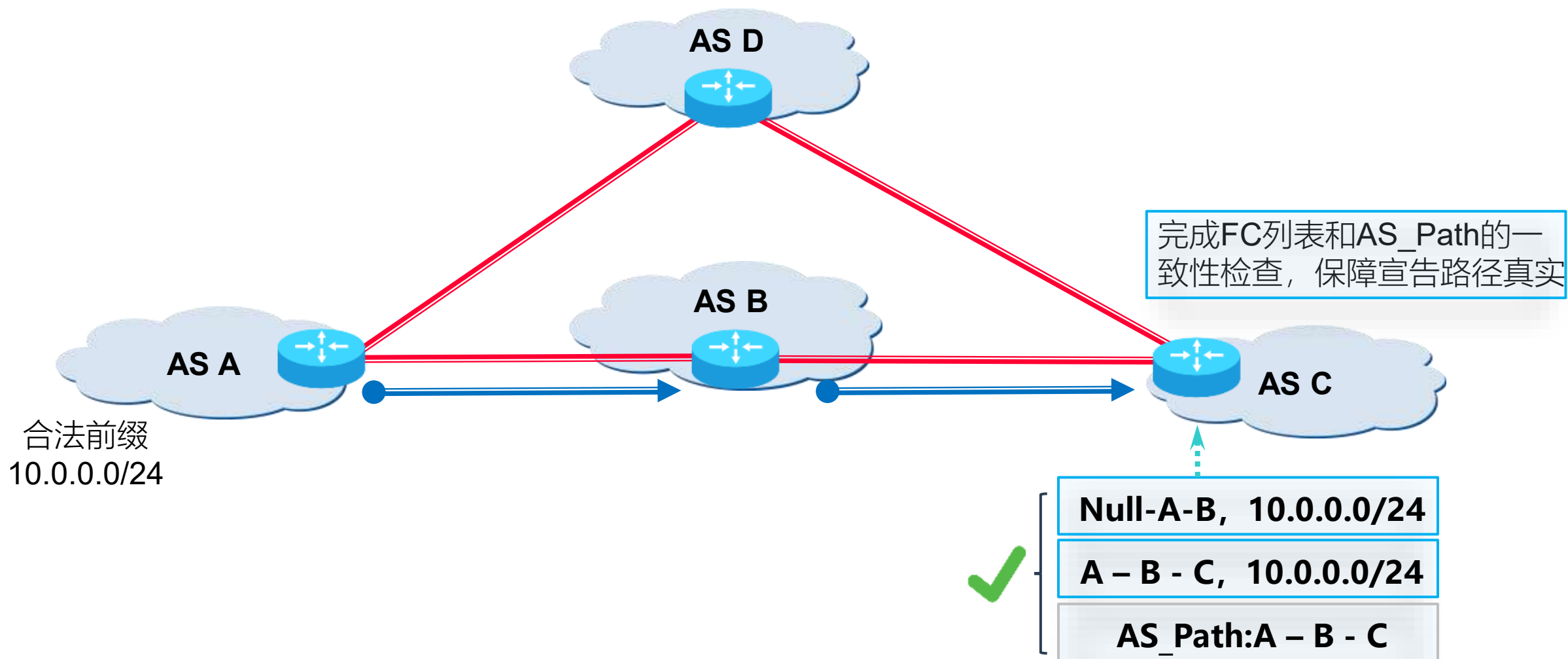


路由宣告路径验证



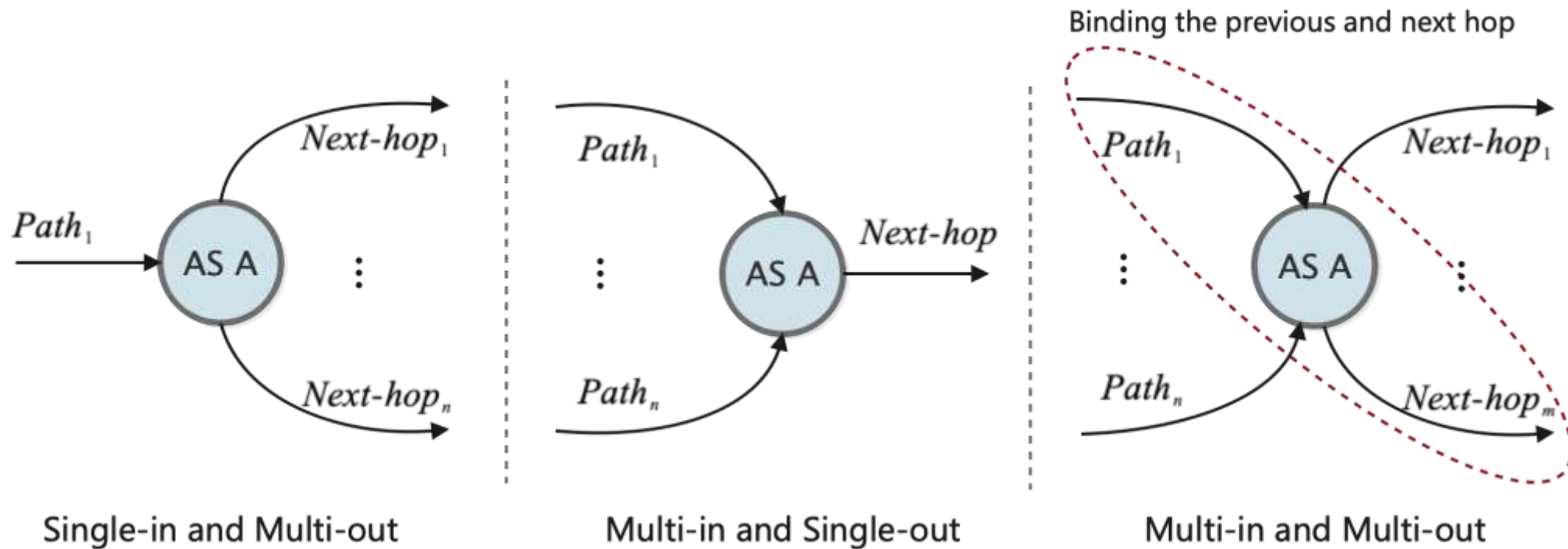


路由宣告路径验证





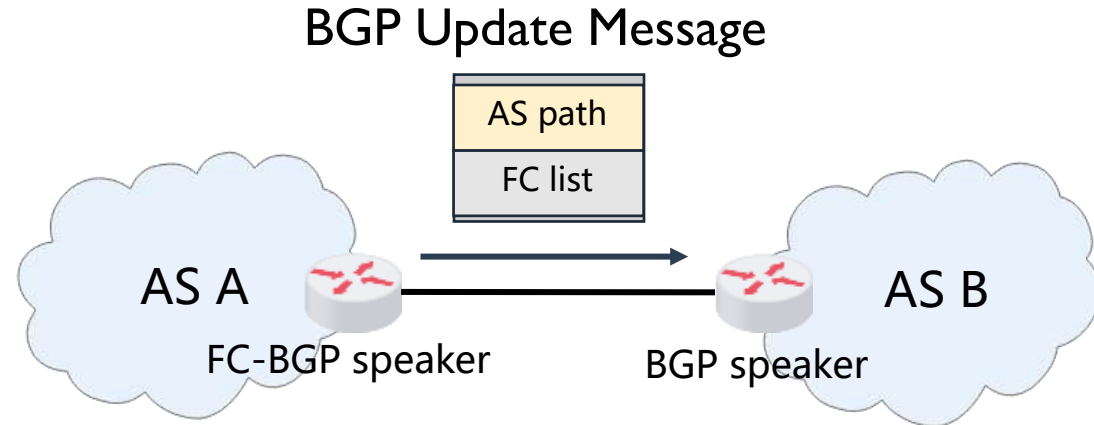
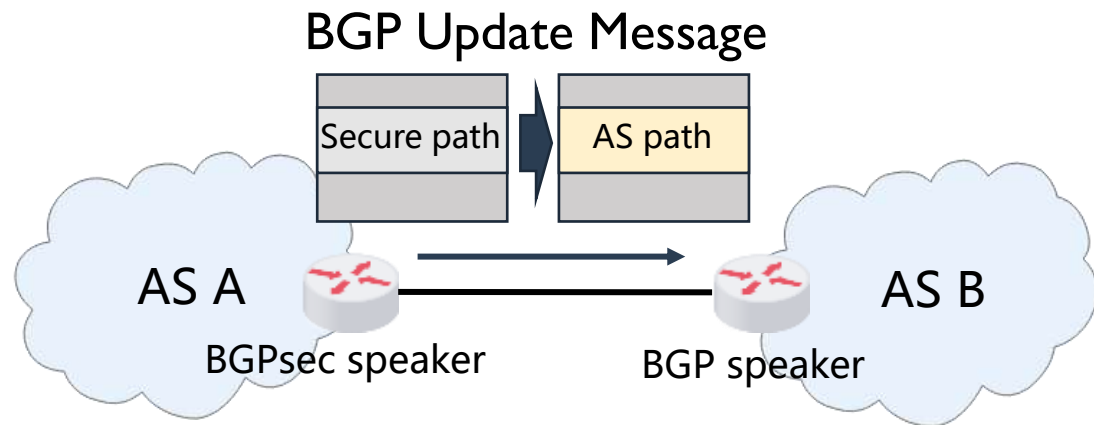
FC-BGP的安全性分析



- FC-BGP安全性的核心在于如何避免通过拼凑合法FC构造一条非法路径
- 节点私钥的安全性保证了FC无法被伪造
- 拼凑合法FC仅可能出现在多条路径的交汇点，“单进多出”和“多进单出”均无法拼凑，仅有“多入多出”可能将前后两部分进行拼接。但FC绑定前一跳和后一跳的结构，使得“多入多出”也无法将分别属于两条路径的FC进行拼接。由此保证FC-BGP的安全性



部分部署的兼容性



- 与BGPsec不同，FC-BGP并不修改标准BGP Update报文中的AS Path字段，而是增加一个新的可传递路径属性，用来携带路径对应的FC列表
- 因此，FC-BGP具备对标准BGP协议的原生兼容性，避免了AS Path字段替换为Secure Path的额外操作和协商



标准化工作



“...FC-BGP I love it, I absolutely love it. And not because it is an ASPA replacement because it is a possibility of source address validation. Which I think is something that we solely lacking in routing security...”

- 目前，研究组正在积极推动FC-BGP的标准化工作
- 2023年9月参加APNIC 56会议，FC-BGP得到了广泛关注和好评
- 2023年11月参加IETF 118会议，idr组内讨论了FC-BGP，受到广泛关注，得到BGPsec作者Sriram、idr主席Jeff和Keyur等的积极评价与建议



第5节 恶意路由检测

- ✓ 路由泄露：OTC
- ✓ 路由劫持：BEAM



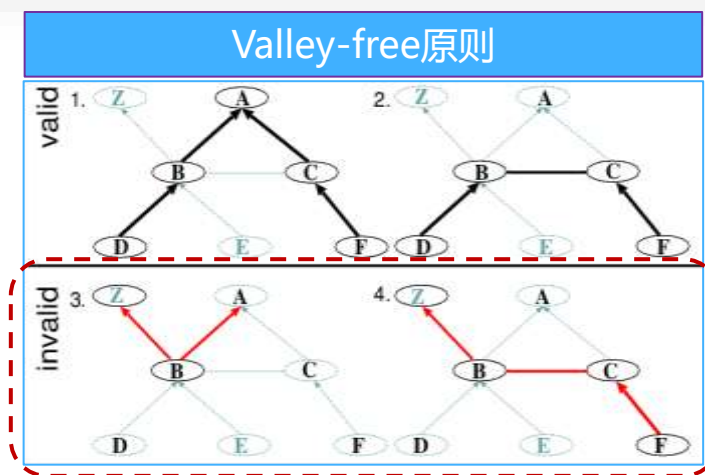
路由宣告原则

原则

- 根据商业利益，AS在出站策略中遵循**Gao-Rexford**的原则：向Provider或Peer宣告时，AS可以导出其自身的路由和Customer路由，但通常不导出其提供商或对等网络的路由
- 在向客户或同级自治系统宣告时，AS可以导出其自身的路由和客户路由，以及其提供商或对等网络的路由
- **AS路径应该是无谷的**

违反传播原则的因素：

- 路由配置错误/缺失
- AS之间缺乏协调机制

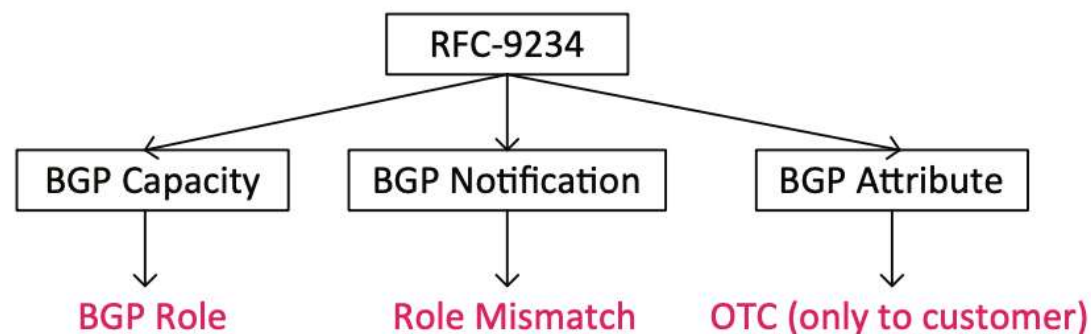


违反valley-free原则



BGP角色确认机制

- 五种角色：Provider、Customer、Route Server(RS)、RS-Client、Peer



- BGP Role描述了建立连接的eBGP speaker 之间的关系，接收端路由器会根据合法的商业关系规则匹配双方角色

- **Only to Customer**
- 进一步增强路由防护

OTC属性值等于本地的ASN

- Update报文中 Path Attribute 字段的一个**可选的且可传递的**属性

OTC引入**新的属性和能力**

- 强制规定路由一旦发送到客户、对等方或路由服务器客户端，随后只能发送给客户



路由劫持检测

技术方法

- 传统检测方法：控制面手机异常公告、ping指令探测可达性
- 基于learning检测：学习异常路由的特征

技术评价

- 传统检测方法：依赖大量的人工调研和配置
- 基于learning检测：需要大规模的数据标记和特征构建

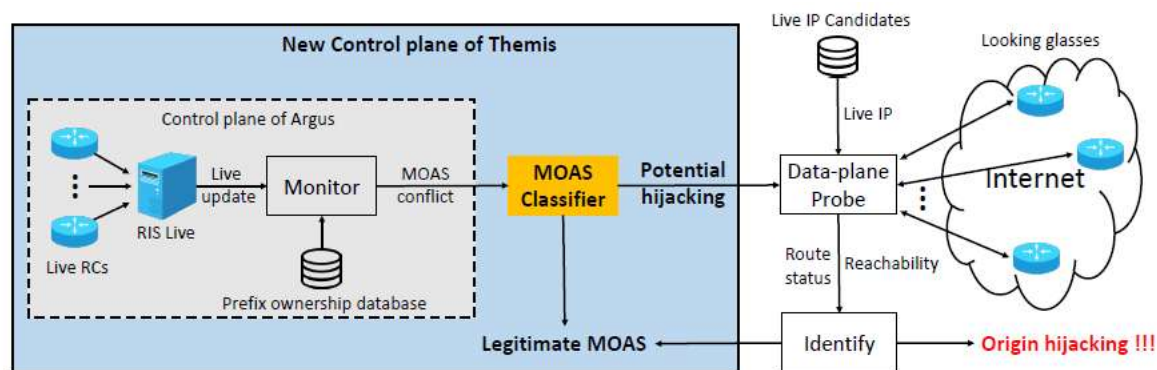
BGP Origin Hijacks

Detected BGP hijack events originated by any ASN

Detected Origin	Expected Origin(s)	Start Time	Duration	BGP Messages	Prefixes	Confidence	Tags
AS40844	AS10096	Mon, 24 Apr 2023 22:24	—	1 msg (1 peers)	148.59.204.0/24	Medium	NEW ORIGIN
AS21491	AS327734 AS3236662	Mon, 24 Apr 2023 22:24	—	14 msgs (14 peers)	302.68.124.0/24	Medium	NEW ORIGIN, NEW OLD ORIGIN, NEW OLD
AS43831	AS31296	Mon, 24 Apr 2023 22:16	—	1 msg (1 peers)	2401.8180.132	Medium	NEW ORIGIN, NEW OLD ORIGIN
AS61139	AS934	Mon, 24 Apr 2023 22:00	—	1 msg (1 peers)	188.102.11.0/24	Medium	NEW ORIGIN
AS263288	AS36913	Mon, 24 Apr 2023 22:02	14 minutes	8 msgs (8 peers)	140.99.90.0/24	High	NEW ORIGIN, NEW ORIGIN, NEW OLD ORIGIN, NEW OLD
AS29802	AS61317	Mon, 24 Apr 2023 22:19	—	4 msgs (4 peers)	64.292.300.0/24	Low	NEW ORIGIN, NEW OLD ORIGIN, NEW OLD
AS209552	AS198962	Mon, 24 Apr 2023 22:01	—	1 msg (1 peers)	194.40.242.0/24	High	NEW ORIGIN
AS212607	AS16731	Mon, 24 Apr 2023 21:30	—	2 msgs (2 peers)	794.87.23.0/24	High	NEW ORIGIN
AS50283	AS60169	Mon, 24 Apr 2023 21:15	—	22 msgs (15 peers)	193.52.46.0/24 ... 3 more	High	NEW ORIGIN, NEW ORIGIN
AS30485	AS212384	Mon, 24 Apr 2023 21:18	2 seconds	4 msgs (4 peers)	181.215.37.0/24	High	NEW ORIGIN

< > Page 1 of 15

前缀劫持事件



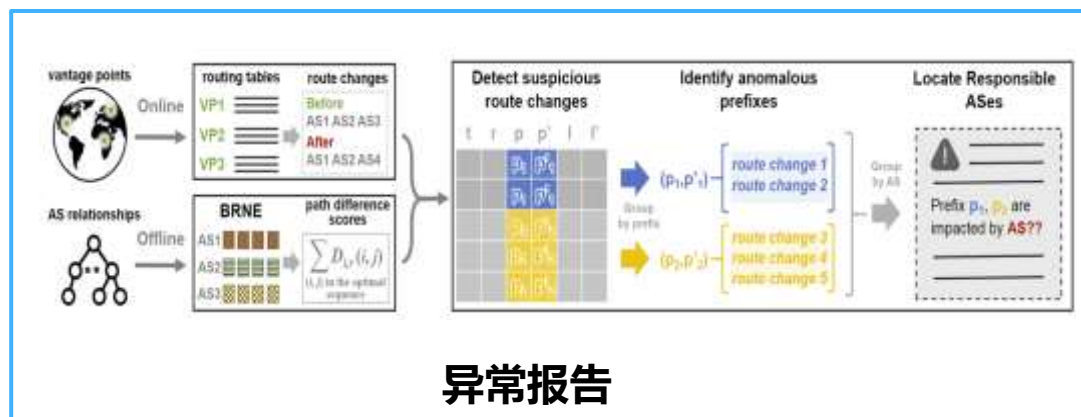
Themis架构



路由劫持检测

代表性方案—BEAM

- 设计实现基于网络表示学习的路由异常检测系统和可视化监测平台
 - ✓ 开发路由异常检测系统和可视化平台，实时输出检测结果，覆盖劫持、泄漏详细事件解释，实现路由安全态势感知，及时通告给运维人员



监测平台



第6节 总结和展望



总结



第一节

层次化路由体系结构

- 层次化路由
- 域内路由
- 域间路由

域内路由：OSPF
等协议
域间路由：BGP
等协议



第二节

路由安全问题

- 域内路由安全
- 域间路由安全

路由系统面临着
路由劫持、路由
泄漏等安全问题



第三节

路由源验证

- IRR
- RPKI
- MANRS

通过提供可靠
的源-前缀映
射关系，避免
路由源劫持



第四节

路径验证

- BGPsec
- FCBGP

在源验证基
础上，通过
签名等保护
路由路径



第五节

恶意路由检测

- OTC
- ASPA
- BEAM

增加AS协
商机制，
学习AS关
系语义



展望

网络空间命运共同体为构建更健壮的全球路由系统提供新机会



- **多方协作、多源融合、灵活合作机制**推动形成全球一致、可验证的路由源
- **渐进部署收益**的路由验证方案逐渐标准化，鼓励更多人采用路由验证机制，推动构建更安全、更稳健的全球路由系统