中国电信 CHINA TELECOM

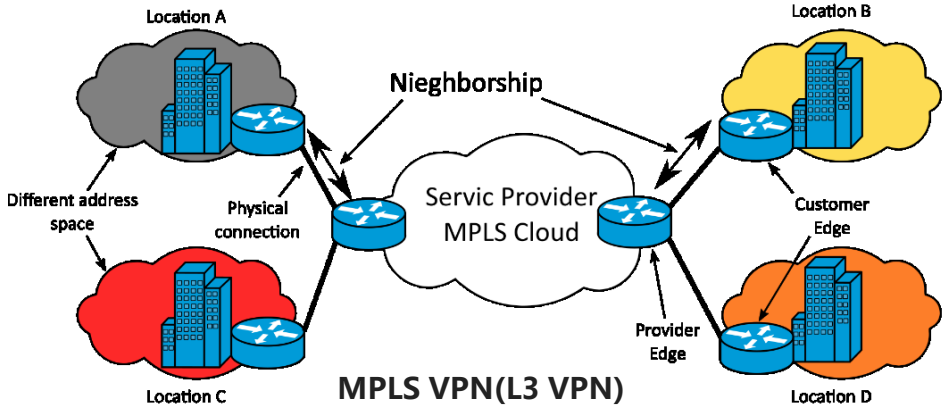
Research and Practice of Decentralized Trustworthy Network Infrastructure

Jianglong Wang
China Telecom

Lisbon，2020.1.13

Start from talking about a lease-line product

MPLS VPN, using **multiprotocol label switching** (MPLS) to create **virtual private networks** (VPNs) for enterprise customers.

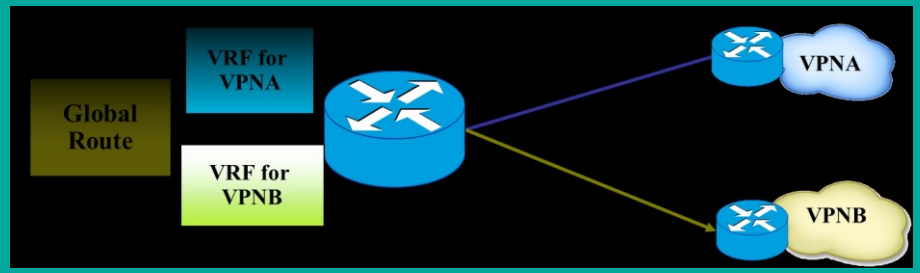


MPLS VPN(L3 VPN)

	MSTP	MPLS VPN
feature	Circuit switching	Packet switching
Encapsulation	SDH frame through GFP encapsulation	Insert an MPLS frame header
Scalability	limited by SDH ring network bandwidth	Flexible network bandwidth adjustment
QoS	End-to-end QoS	the MPLS edge router, the inbound bandwidth is limited
Technical implemention	Port-level IP, SDH core;	IP， the packet switching core.
security	**hard pipeline isolation, with high security**	**soft pipeline isolation, and the security is relatively poor.**
Applicable scenario	high security requirements and low bandwidth requirements	Integrated services with large bandwidth and complex networking

- **Is the IP protocol-based packet switching really insecure?**

  IETF RFC4381 (2006) ,MPLS VPN can be as secure as traditional layer-2 VPN services using ATM or FR



WHY Question IT ???

Multiprotocol BGP (MP-BGP) is required to utilize the service, which increases complexity of design and implementation, also introduces some insecurity

FOCUS

Network security and trustworthy

中国电信 CHINA TELECOM

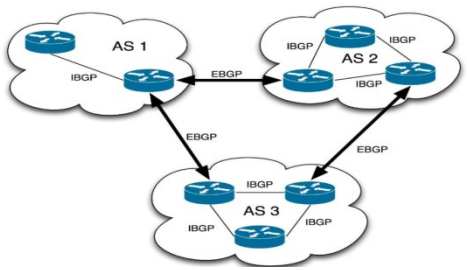
Security Problem

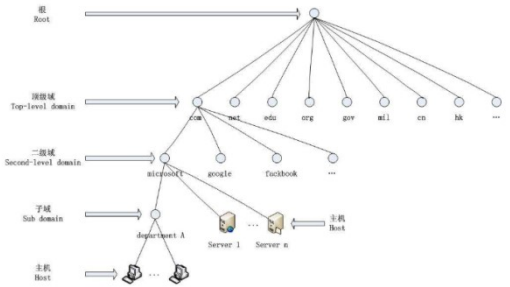
- BGP prefix Hijack
- BGP route leak

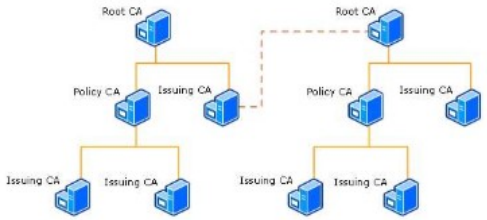
- DNS hijacking
- DDoS
- Trust anchor crisis

- Unilateral revocation of legal certificate
- Illegal certificate for identity forgery ……

Protocol







BGP | DNS | PKI

Network Infrastructure

ASN | Address | Domain Name | Public key | ID

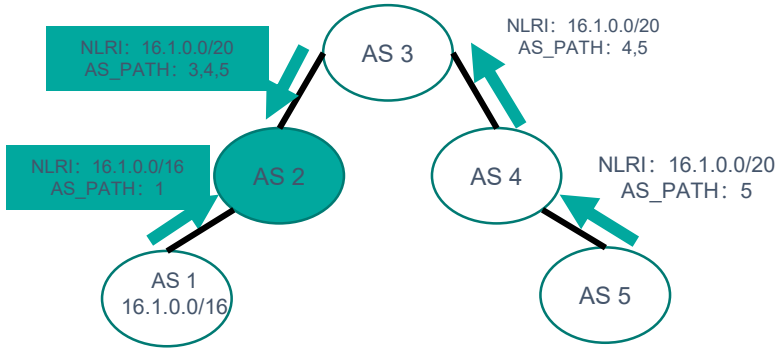
Research on the Trustworthy network infrastructure is a common concern of all countries in the world

BGP ISSUES

BGP Issues Analysis

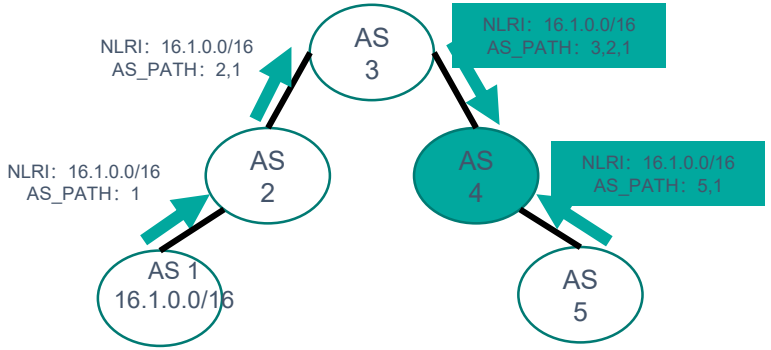
中国电信 CHINA TELECOM

Origin Hijack



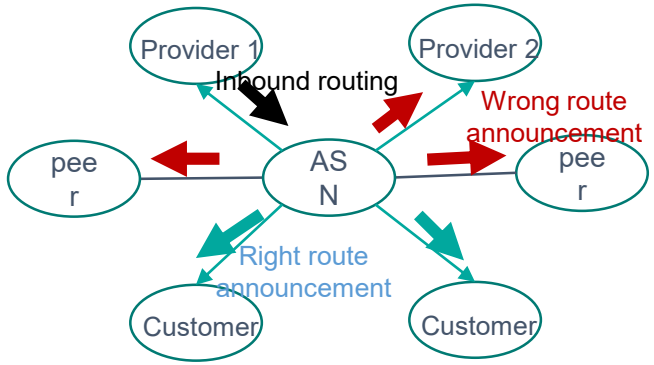
✓ Attack traffic by publishing address prefixes that are not their own

Path Hijack



✓ Hijack traffic by publishing false path information

Route Leak



Violation of provider-to-customer policy, leading to route leaks

✓ the propagation of routing announcement(s) beyond their intended scope

Protocol design flaws : **BGP lacks a secure and reliable route authentication mechanism**. BGP will accept any route announced by the peer by default, that is, it unconditionally trust the route announcement of the peer. Even if an AS advertises a prefix not belonging to itself, it would be accepted and continue to be spread.

Events

BGP security events Overview

For two hours, a large chunk of European mobile traffic was rerouted through China

On June 6, 2019, the misconfiguration of the Swiss SafeHost company caused European traffic to be incorrectly transmitted through China Telecom for 2 hours. The incident occurred because of a BGP route leak

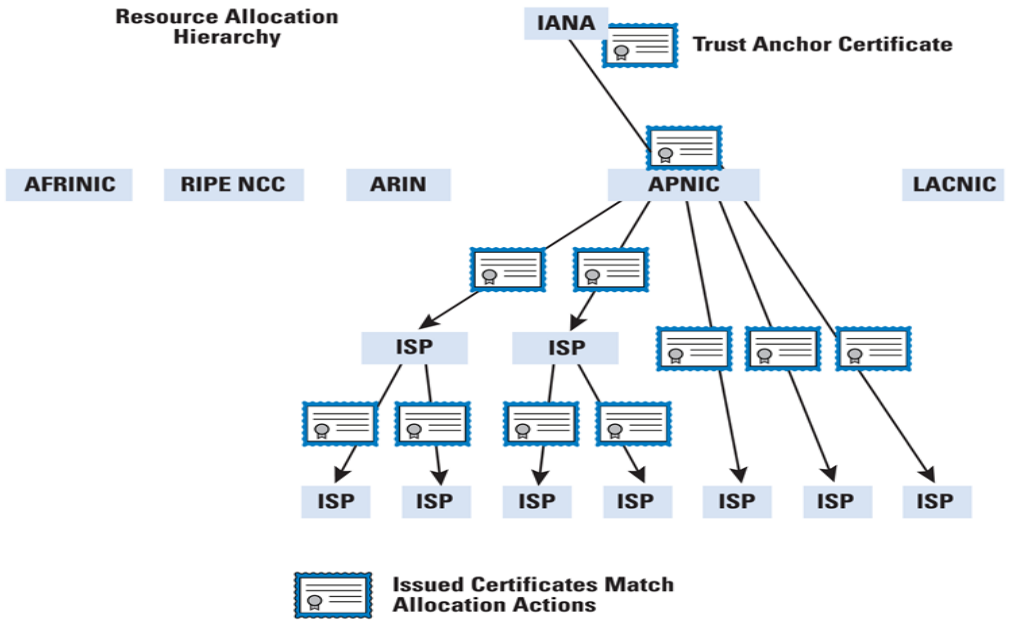
The traffic destined for some of Europe's biggest mobile providers was misdirected in a roundabout path through the China Telecom for more than two hours. We can see in the picture, a Swiss company Safe Host(data center colocation), AS21217 leaked over 70,000 routes to China Telecom (AS4134). China Telecom immediately echoed those routes rather than dropping them. In short order, a large number of big networks that connect to China Telecom began following the route. such as Cogent. The traffic is dropped in ChinaTelecom’s backbone.

Solut ion

BGP Security Protocol Solution

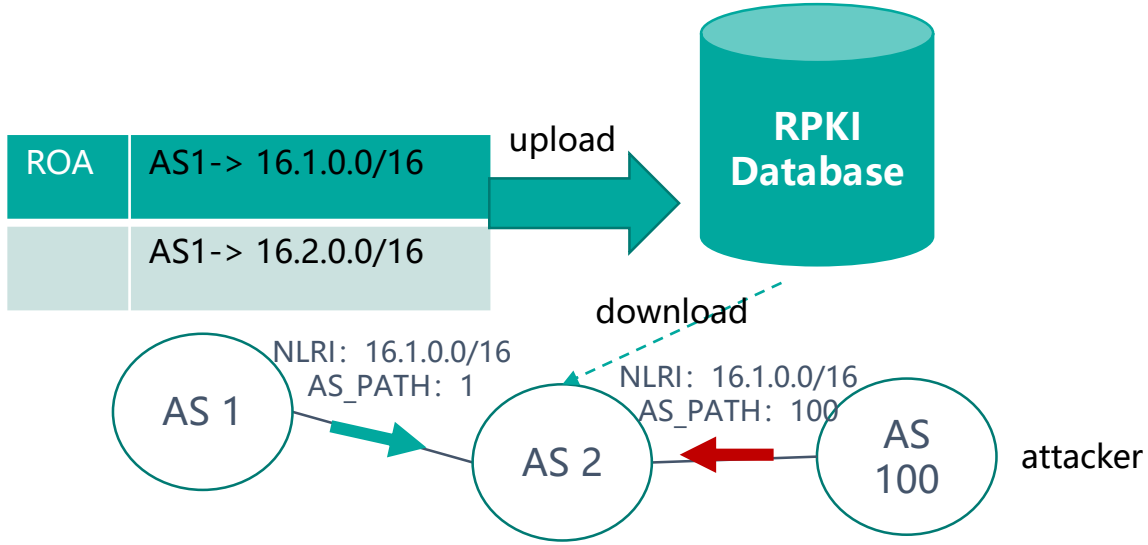
RPKI（RFC6810）

- Resource Public Key Infrastructure
- Verify the origin Autonomous Systems of BGP announcements, to deliver validated prefix origin data（Origin AS）to routers.



BGPsec（RFC8206）

- BGPsec is a BGP security extension, which is designed to provide security protection for the AS_PATH attribute in BGP update messages.
- The combination of RPKI and BGPsec can be used to verify the authenticity and integrity of BGP routes.



16.1.0.0/16, AS 1 legal
16.1.0.0/16, AS 100 illegal

RISK

The centralized trust model of the Internet

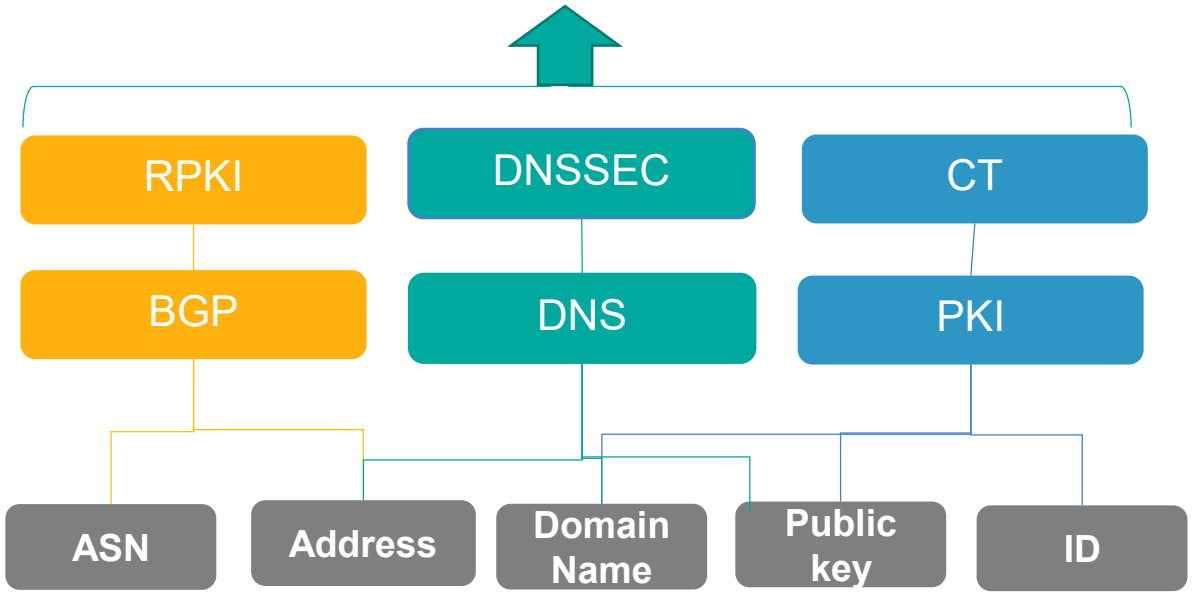
中国电信 CHINA TELECOM

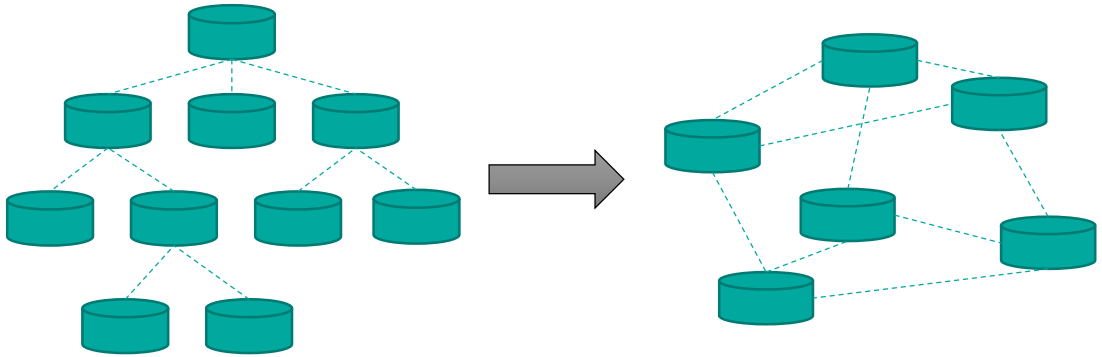
RISK & Problem

- **Depending on the centralized trust model, once the Authority node is misconfigured or attacked, it raises security issues and is difficult to avoid from the mechanism.**
- **Does not solve the route leakage problem**

What we focus on?

- explore an innovative architecture of trusted network system, from technical security to mechanism security. We try to change our mind from centralized network to decentralized network, concentrating on a new trustworthy network architecture.





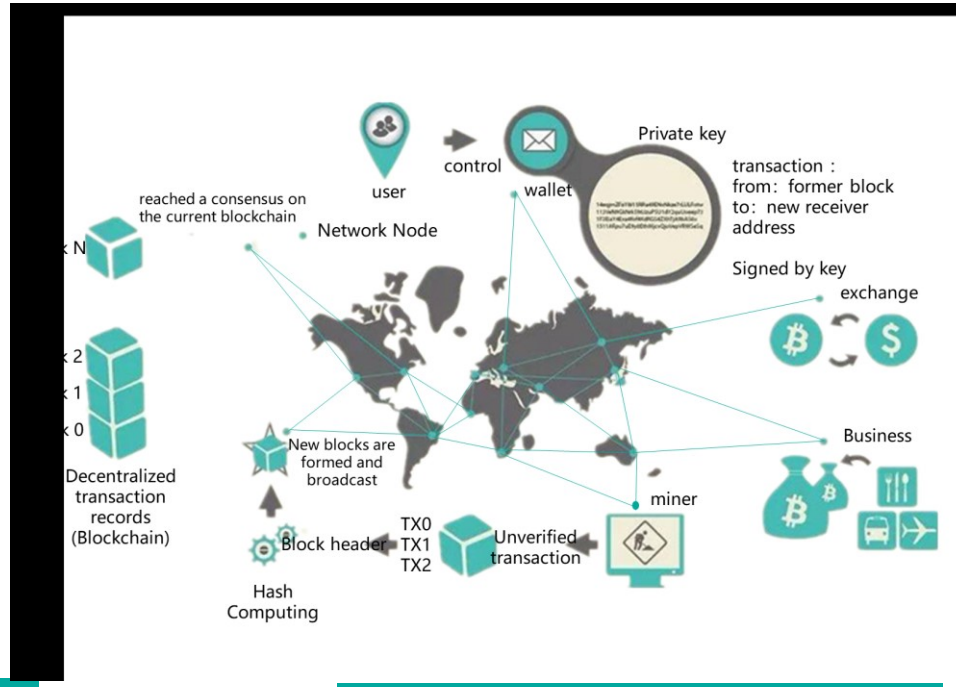
centralized

decentralized

Key Tech

Block Chain

- **Block Chain is a distributed database that maintains a continuously-growing list of data records hardened against tampering and revision.** The data storage, transaction verification, and data transmission in the blockchain system are all decentralized



Public chain

- A public blockchain has absolutely no access restrictions. Anyone with an Internet connection can send transactions to it as well as become a validator (i.e., participate in the execution of a consensus protocol).

Private chain

- A private blockchain is permissioned. One cannot join it unless invited by the network administrators. Participant and validator access is restricted.

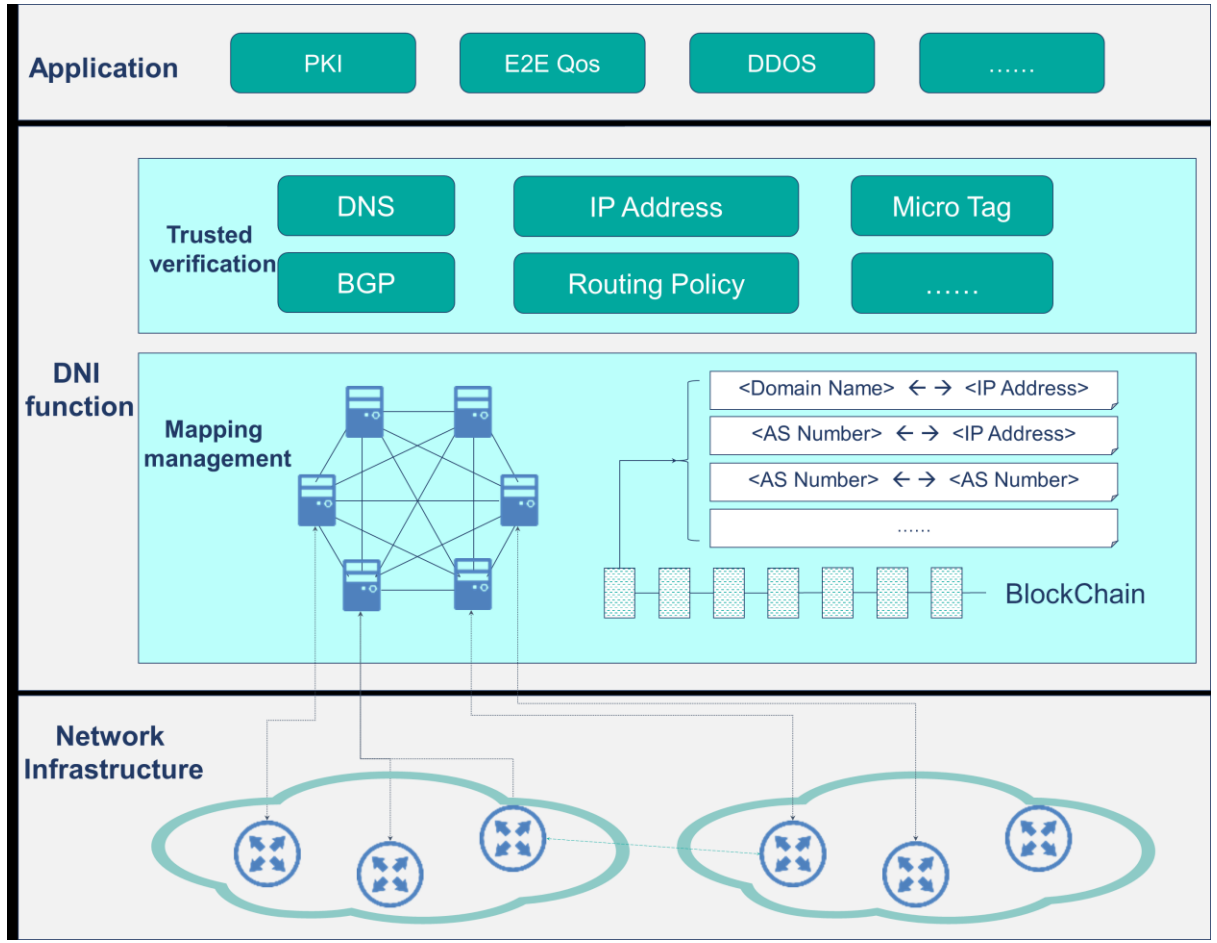
consortium blockchain

- The consortium blockchain is a hybrid between the 'low-trust' offered by public blockchains and the 'single highly-trusted entity' model of private blockchains.
- participation in consensus can be controlled through authorization.

Decentralized Trustworthy Network Infrastructure

ITU-T SG13 Y.DNI-fr《Framework and Requirements of Decentralized Trustworthy Network Infrastructure》

——China Telecom、Huawei、 China Unicom、 China Information Communication



Application Layer

An open application layer that supports and promotes innovative, trusted, decentralized network applications

- Decentralized PKI platform, DDoS defence services

Name Space Management Layer

Trusted name space ownership and mapping

- IP & ASN: Trusted routing system
- IP &Domain name: Trusted DNS resolution system
- Other name spaces: host identifier, content name, IoT ID…

Distributed Ledger Layer

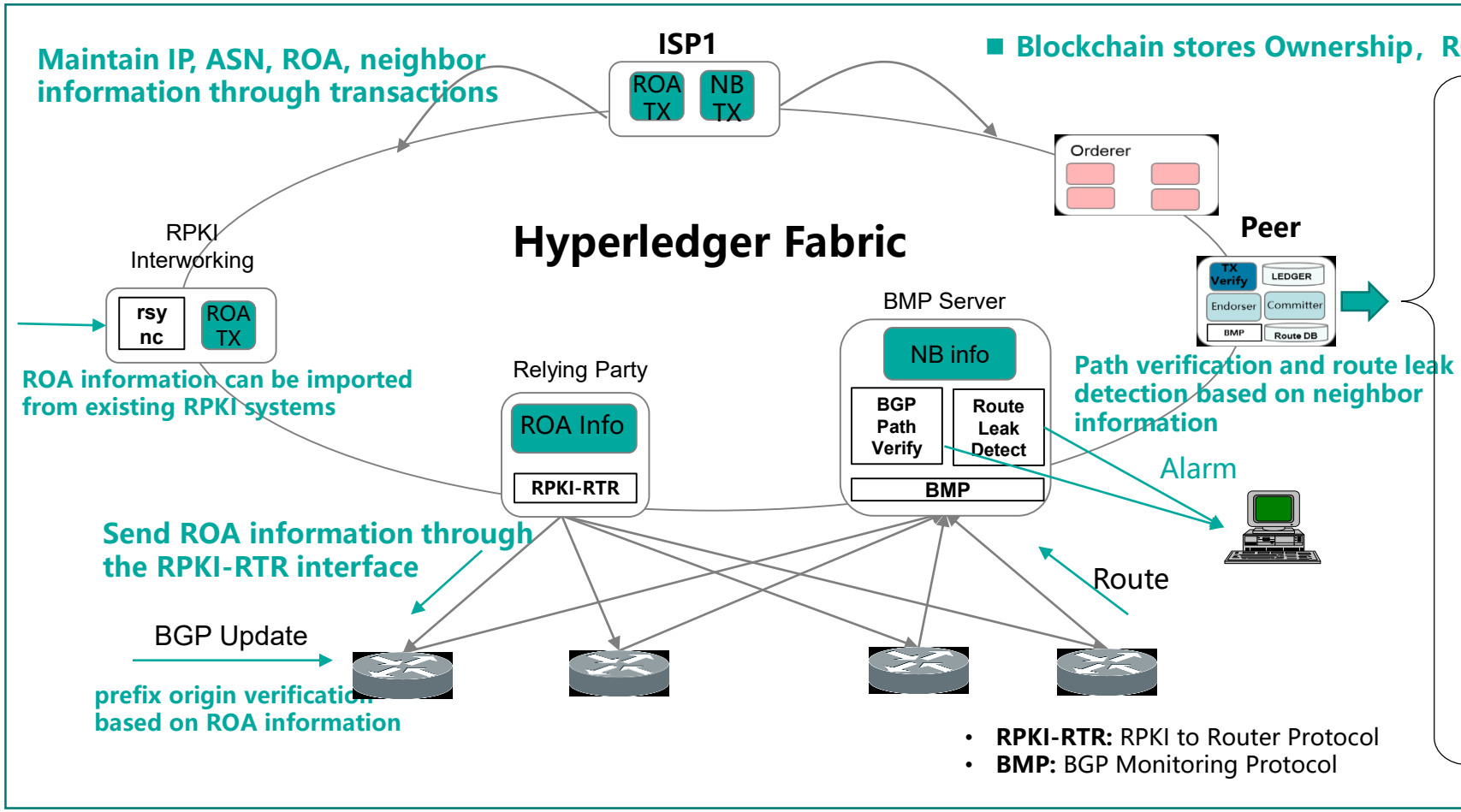
The basis of decentralized network infrastructure. It is in charge of providing the following functions

- Providing decentralized system structure
- Providing distributed consensus mechanism
- Guarantee of trustable trade

Test bed

DNI-based Testbed

The testbed is based on Hyperledger Fabric. Blockchain stores Ownership，ROA and neighbor information，providing Internet resource management, BGP security (prefix origin verification, route path verification, route leak detection).



■ Blockchain stores Ownership，ROA and neighbor information

IPList

IP	Owner	Exp date
1.1.1.1/32	ISP1	19/10

ASNList

ASN	Owner	Exp date
100	ISP1	19/10

ROAList（IP->ASN）

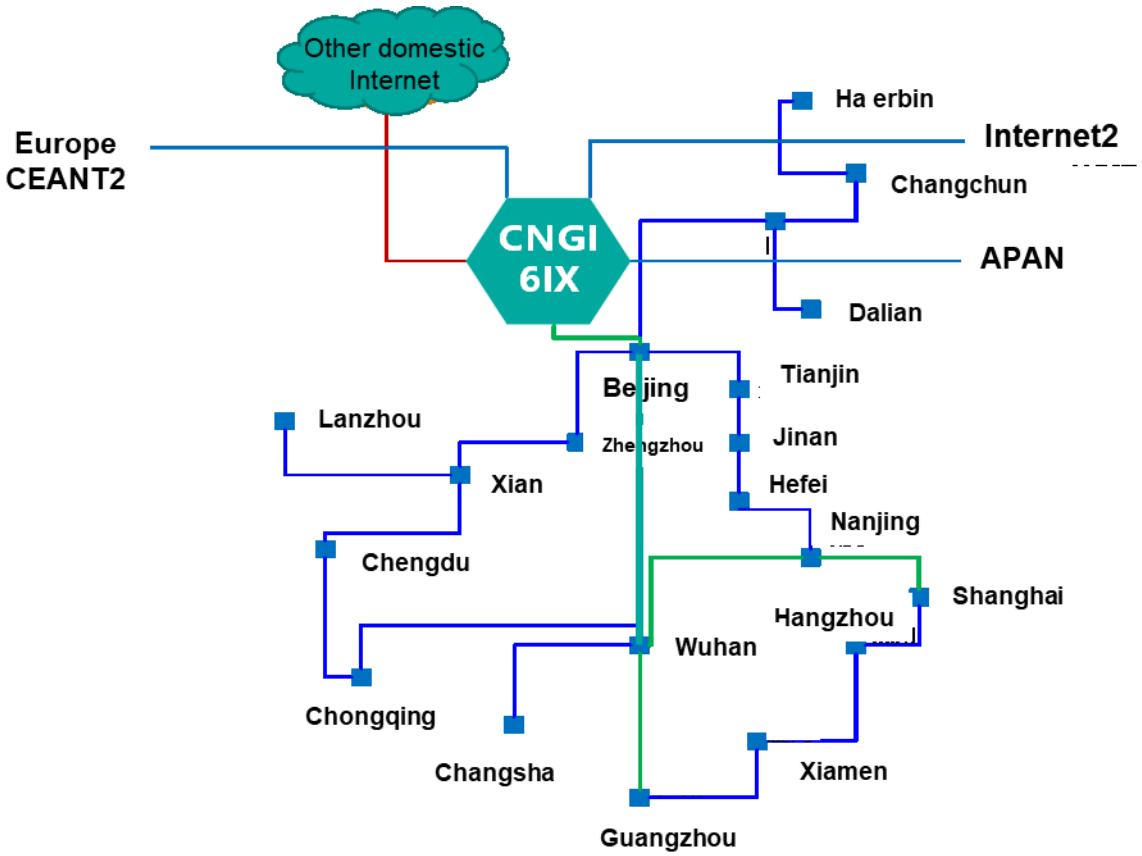
IP	Maxlength	ASN
1.1.1.1/32	32	100

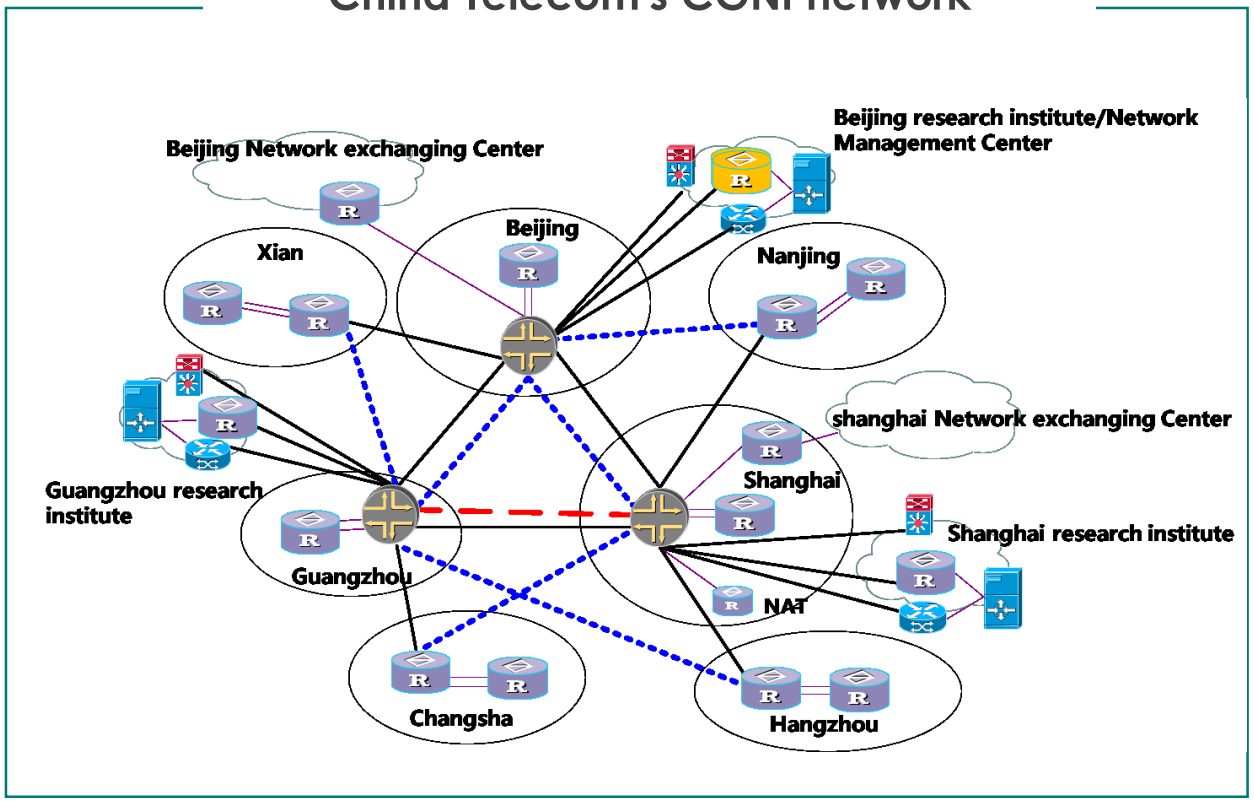
NeighborList（ASN->ASN）

Source	Target	Type
AS1	AS2	P2C
AS2	AS3	P2P

CNGI Introduction

CNGI，China‘s Next Generation Internet，which is the world’s first IPv6-only network. The whole network construction and management is jointly responsible by six companies in China.



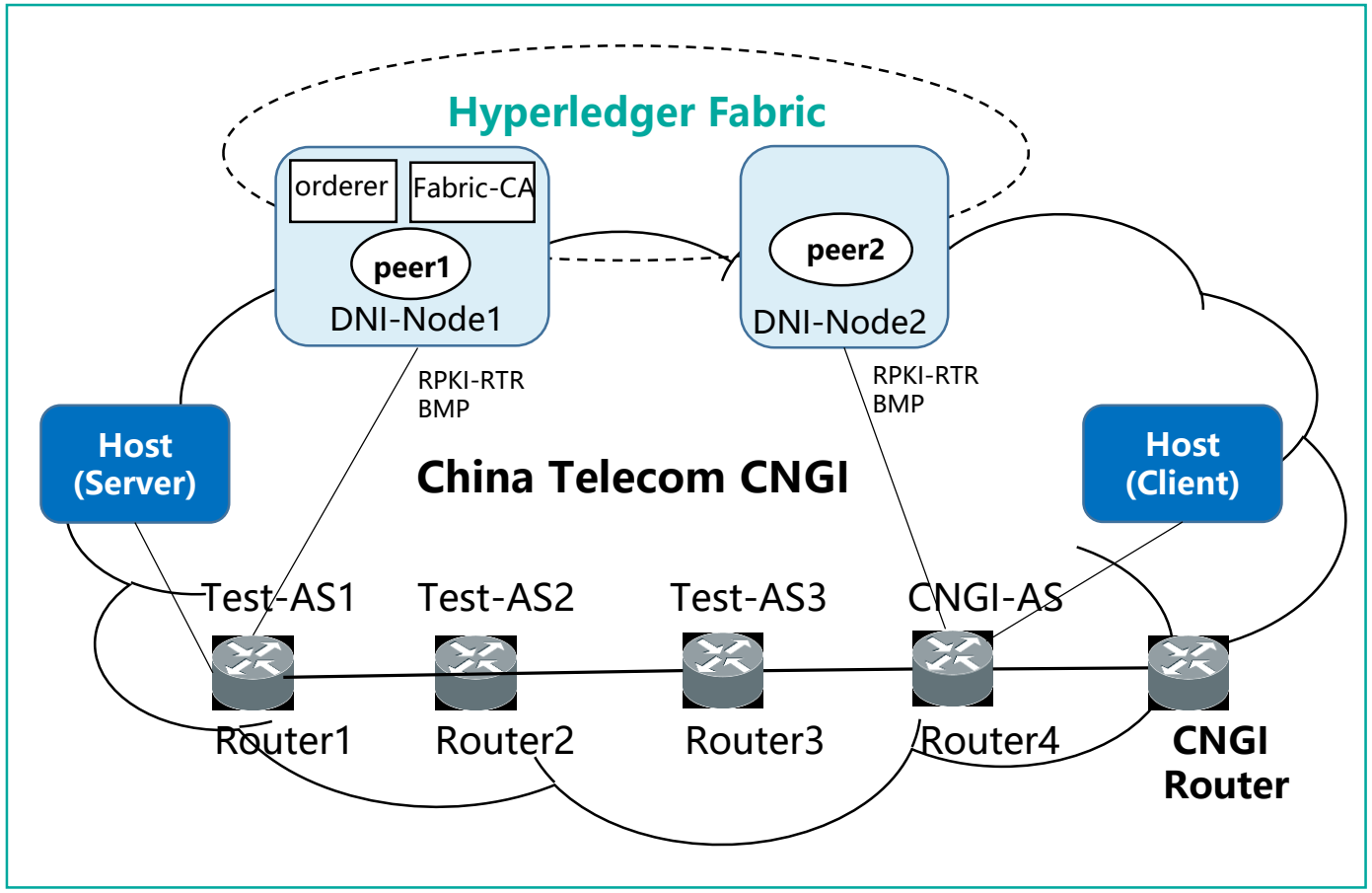


DNI-CNGI

DNI Testbed based on CNGI

中国电信 CHINA TELECOM

The current phase of test environment is provided by China Telecom CNGI network. The whole system is includes a block chain system based on the Hyperledger Fabric, open source distributed ledger, several border routers, 2 servers.



1 the existing network deployment

- Add 4 new routers to connect to the CNGI Router.
- Router 4 is connected to CNGI's network ,Configuring CNGI ‘s AS number.

2 Incremental deployment

- Newly deployed 2 servers and 2 VM
- Server: Video Server and Client for traffic testing. VM: Orderer(Kafka*4+Zookeeper*3), Peer, Fabric CA, Relying Party, BMP Server

3 Interface configuration

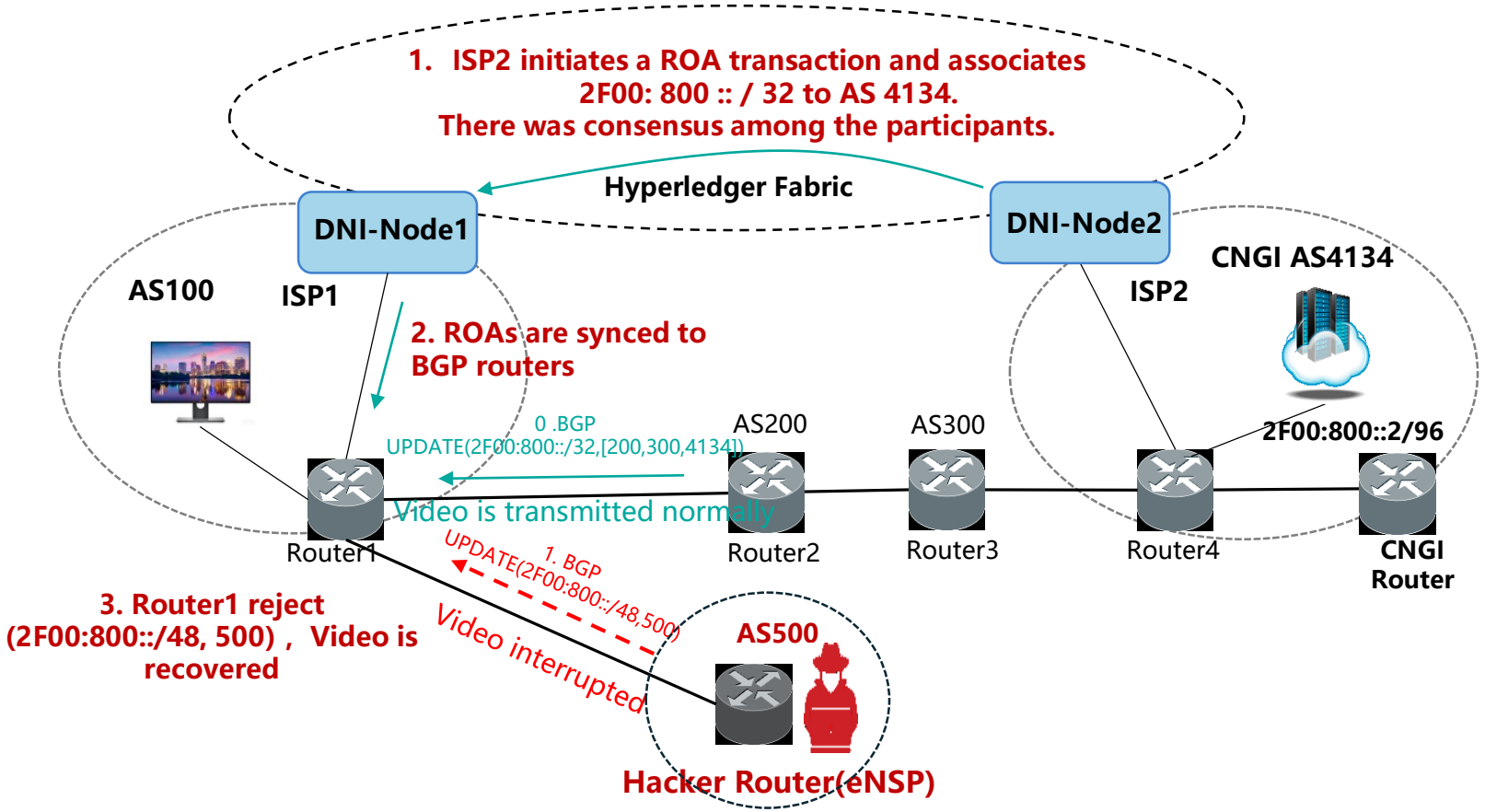
- RPKI-RTR and BMP interfaces are configured between routers and DNI-nodes.
- **RPKI-RTR :** ROA data synchronization.
- **BMP:** synchronize routing information to DNI-nodes

CASE 1

DNI-based BGP Origin Verification

中国电信 CHINA TELECOM

- A hacker launched a prefix-hijacking attack on the IP address in the operator's AS4134 domain, which caused normal video service interruption. The operator initiates ROA transaction through the DNI system. The entire network reached consensus and synchronized ROA information. The prefix-hijacking attack failed.



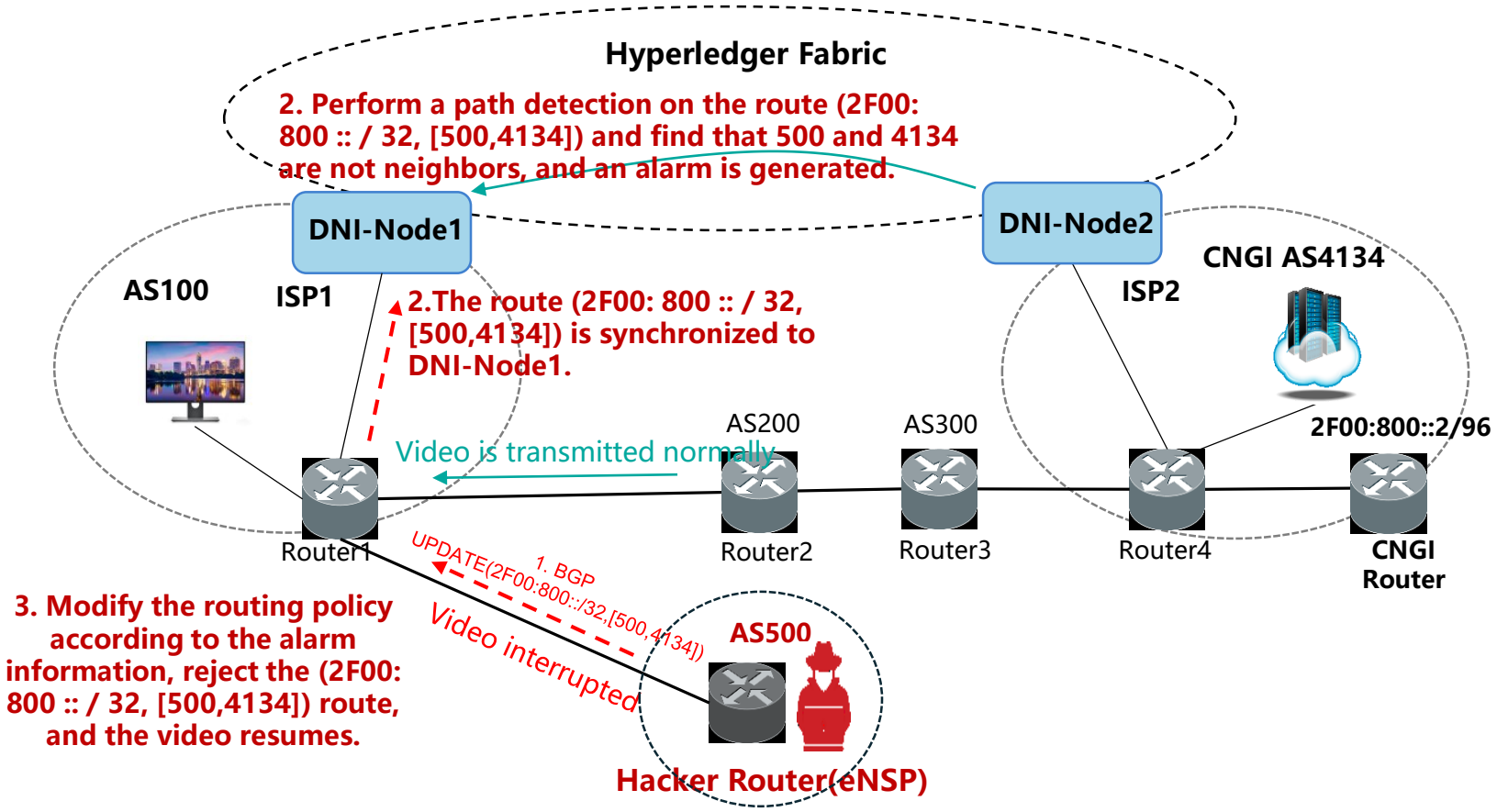
- in this scenario, the video client is in the AS100 domain, the video server is in the AS4134, the AS4314 announces the right route to the AS100.so the video clients can access to the server with this IPv6 address 2F00:800::2, and watch video normally.
- we simulate a hacker to imitate AS500 to launch a longer prefix hijack by using the IP prefix(2F00: 800 :: / 48,500). AS500 announces it to AS100. AS100 will forward this route sent by AS500 based on the “longest prefix matching” principle, which means that AS500 initiates a prefix hijacking on AS100, the video service interrupted.
- ISP2 finds that the prefix is hijacked, issues ROA transactions through the DNI system, associates the right route to AS4134. After the AS reaches a consensus, the ROA information is synchronized to the router. Router1 rejects the hijack routes according to the ROA information. The prefix-hijacking attack failed and the video service is restored.

CASE 2

DNI-based BGP AS Path Verification

中国电信 CHINA TELECOM

- The hacker launched a path-hijacking attack on the operator. The DNI system sends an alarm after detecting the path-hijacking attack. The operator modifies the routing policy, the path hijacking attack failed, and the video service is restored.



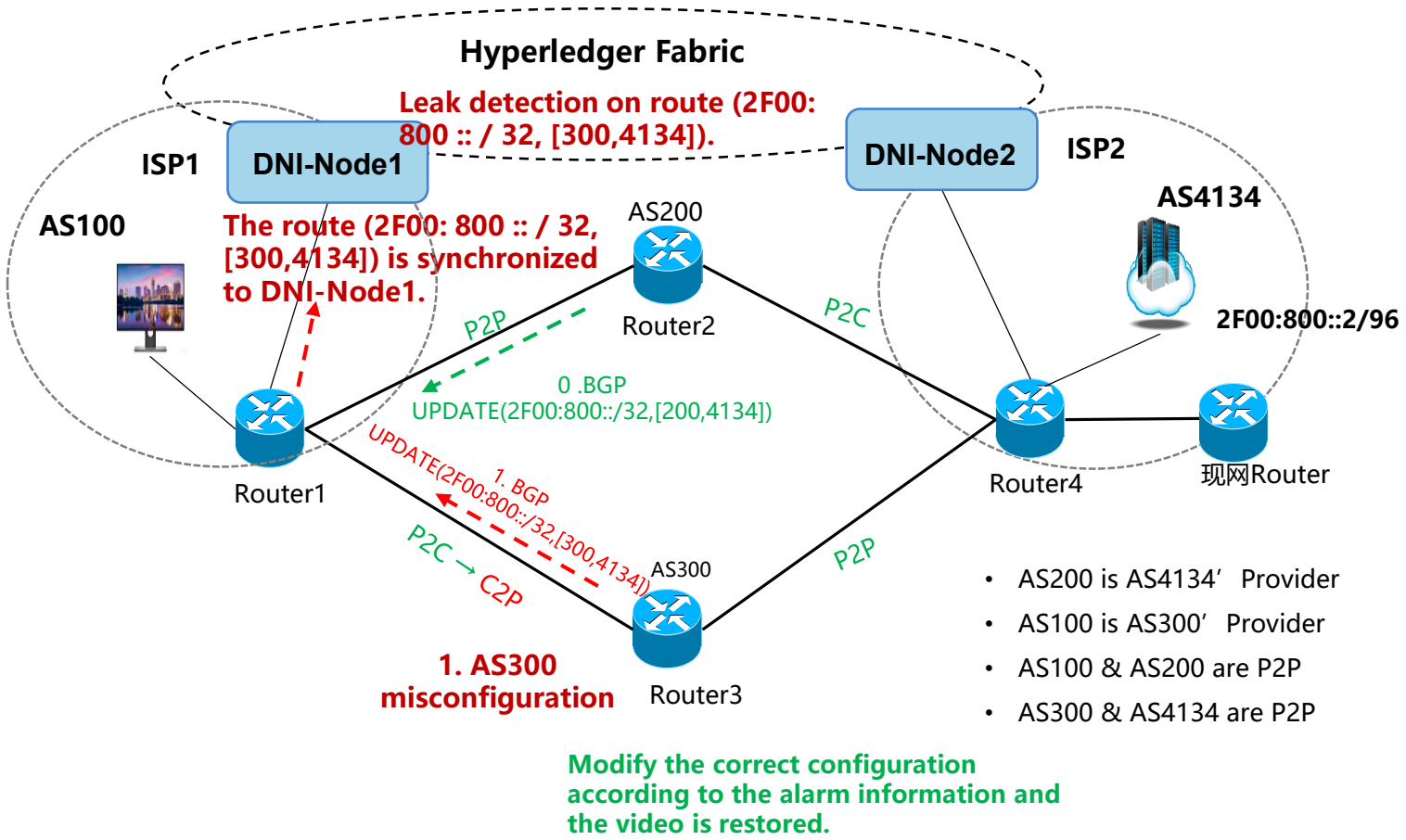
- Each AS publish its neighbor information in the ledger, and the neighbor information will be used for AS path verification in BGP announcement.
- The Relaying Party (RP) get neighbor information from the ledger and synchronize the information to routers.

CASE 3

DNI-based BGP Route Leak Protection

中国电信 CHINA TELECOM

- The route leak is due to the misconfiguration of the operator. The DNI system triggered an alarm after detecting the route leak. The operator handled the misconfiguration based on the alarm information and the video service was restored.



- In this scenario, AS100-AS300, AS200-AS4134 are P2C relationship, AS100-AS200 , AS300-AS4134 are P2P relationship. The relationship between AS300 and AS100 is misconfigured, the route (2f00: 800 :: / 32, [300,4134]) was leaked to AS100. According to the "customer first" principle, AS100 will select the route sent by AS300.but AS300 is not a transit AS, it will drop the traffic and interrupt the video service.

- DNI-Node perform a route leak detection and found that it violated the route leak rule. At this time, DNI-Node sends a route leak alarm. AS300 checks the alarm information and changes back to the correct configuration according to the alarm information. After the configuration is corrected, this route is no longer leaked to AS100. Video service is restored.

Test result

DNI-CNGI Test Result

中国电信 CHINA TELECOM

The test results prove that the DNI architecture can achieve endogenous security from the network architecture layer

- ✓ Adaptive: Automatically solve abnormal problems in the network and carry out corresponding approaches to automatically restore services to normal
- ✓ Autonomy: Operators are producers and users of the block chain content. we can establish independent security capabilities from our own security needs and business

Test case	introduction	result
BGP security	Prefix origin verification, Route path verification, Route leak detection	pass
IP address management	ISP users apply for, transfer, authorize, and recall IP addresses	pass
ASN management	ISP users and terminal users apply for and transfer ASN	pass
ROA	Creation and deletion of ROA	pass
AS neighbor	AS neighbor relationship creation, deletion and conflict detection	pass
Alarm information	Alarm information management and removal	pass
User management	ISP user and terminal user registration and login	pass

ROA

Alarm information

IP address management

Next Step

More cooperation and research

In the future, we will forward to introducing more resources to expand the platform.

中国电信 CHINA TELECOM

- **For NET2030：** Considering the security and trustworthy requirements of future network services, it is meaningful to consider the endogenous security network architecture and implementation mechanism in the future network architecture towards 2030. The decentralized trusted network based on blockchain is a new idea, which is worthy of further research.
- **You are welcome to participate in this project**, to establish a multi-node testbed for further verification together.

Thank You

Jianglong Wang
wangjl50@chinatelecom.cn