Alibaba Group
阿里巴巴集团

阿里云基础设施网络智能运维研究

翟恩南（恩南）

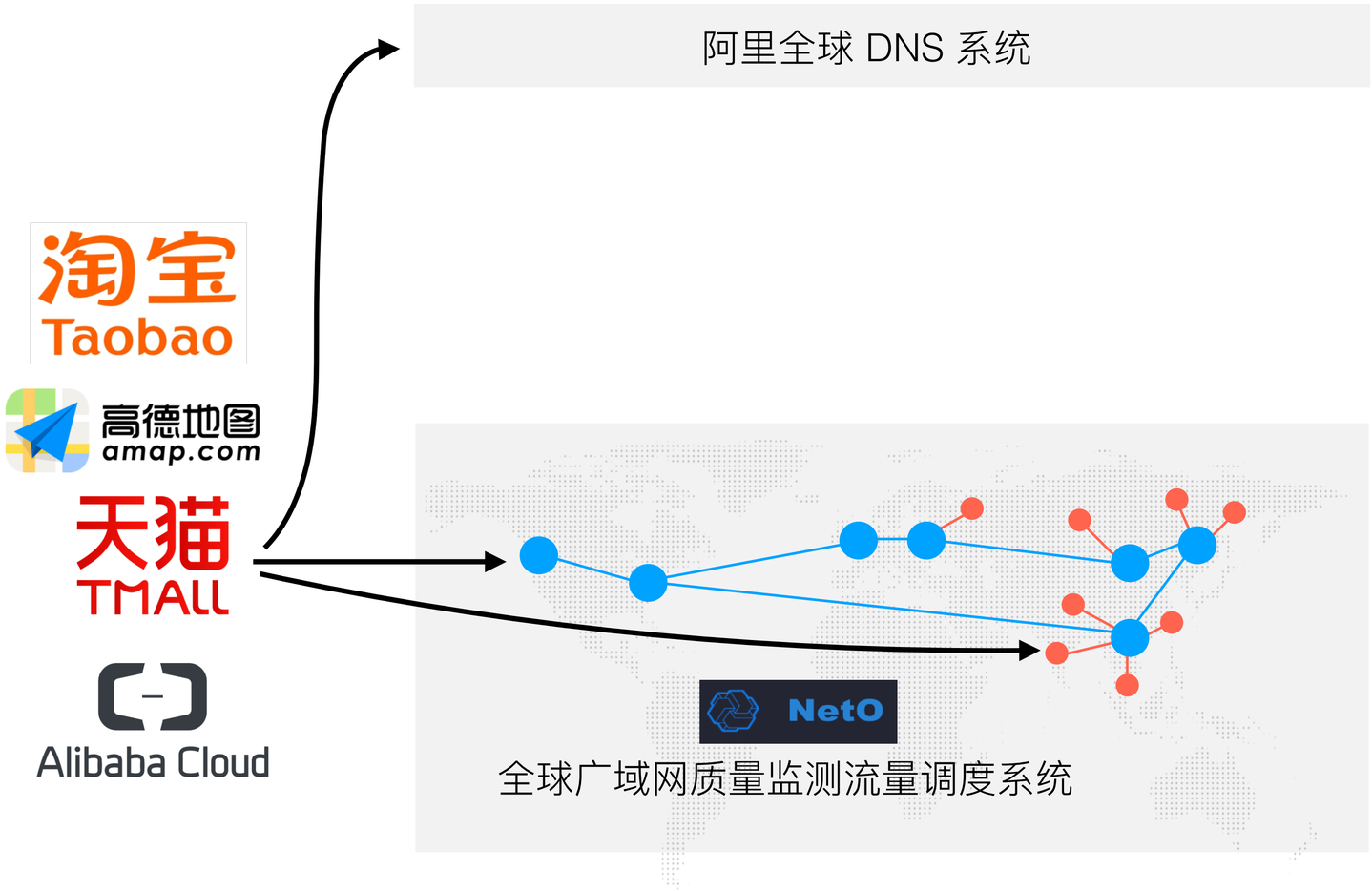
网络研究团队

目录

阿里云全球基础设施网络系统

阿里全球 DNS 系统

阿里云全球基础设施网络系统



阿里云全球基础设施网络系统

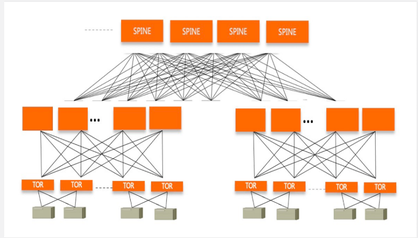
淘宝 Taobao

高德地图 amap.com

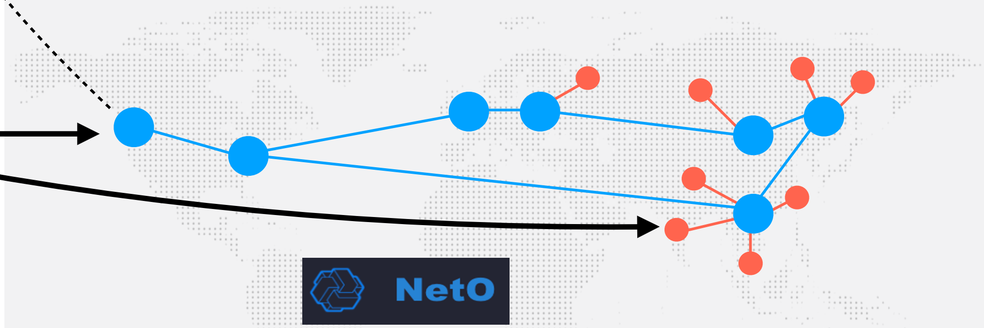
天猫 TMALL

Alibaba Cloud

阿里全球 DNS 系统



全球领先的超大规模高性能数据中心



全球广域网质量监测流量调度系统

阿里云全球基础设施网络系统

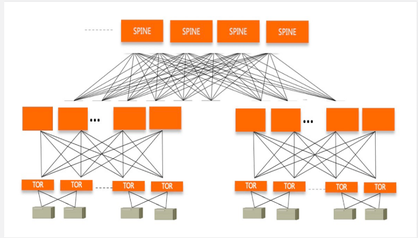
淘宝 Taobao

高德地图 amap.com

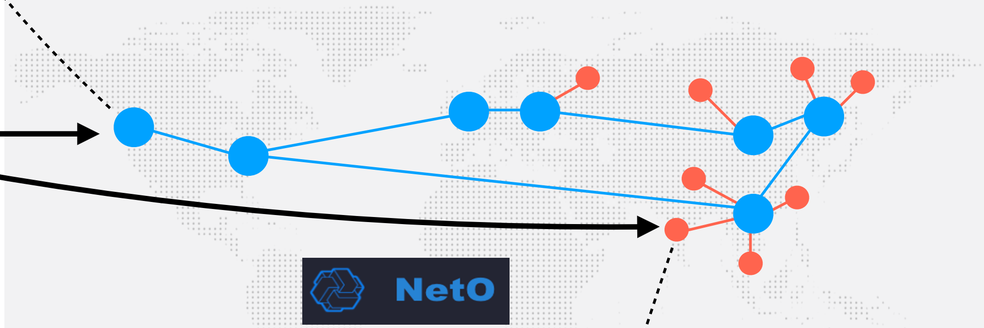
天猫 TMALL

Alibaba Cloud

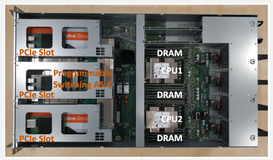
阿里全球 DNS 系统

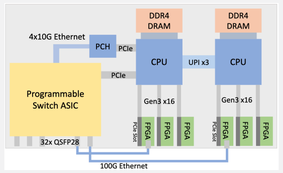


全球领先的超大规模高性能数据中心



全球广域网质量监测流量调度系统





全球最大规模部署的可编程计算网关系统

阿里云全球基础设施网络系统

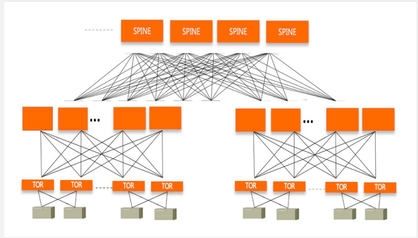
淘宝 Taobao

高德地图 amap.com

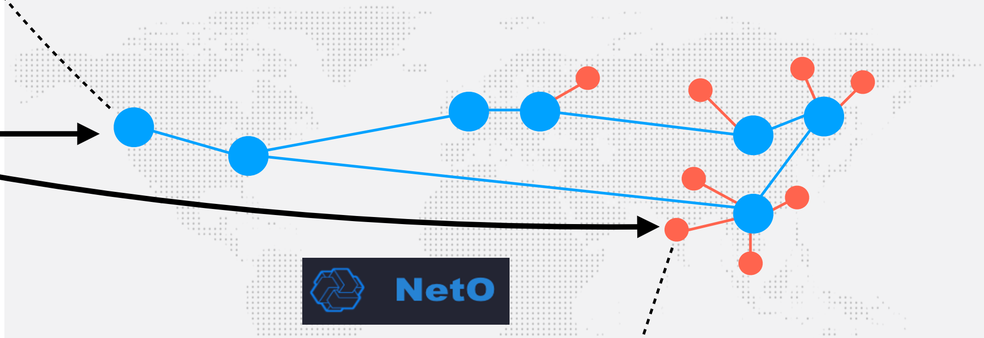
天猫 TMALL

Alibaba Cloud

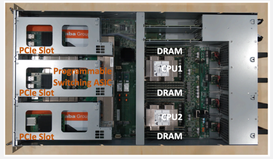
阿里全球 DNS 系统

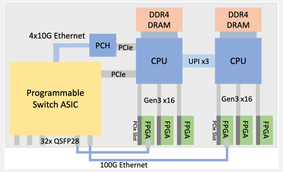


全球领先的超大规模高性能数据中心



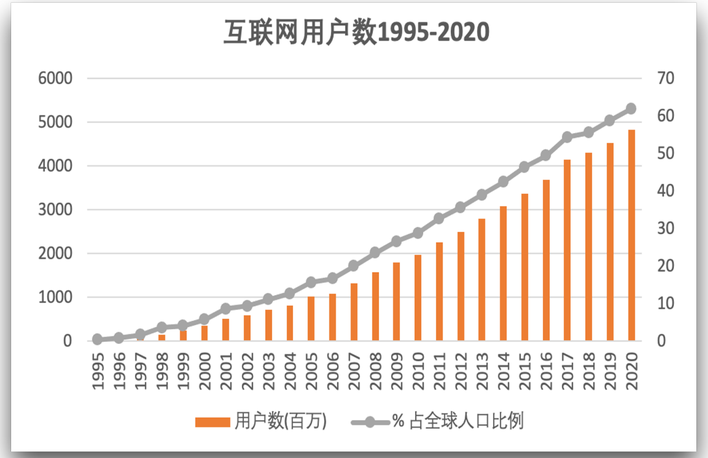
全球广域网质量监测流量调度系统





全球最大规模部署的可编程计算网关系统

网络的价值和挑战在于 **网络规模**



在网络规模持续增长的情况下，如何保证稳定性和高性能

规模驱动下带来的挑战

阿里云全球基础设施网络系统

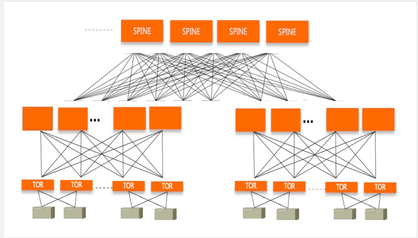
淘宝 Taobao

高德地图 amap.com

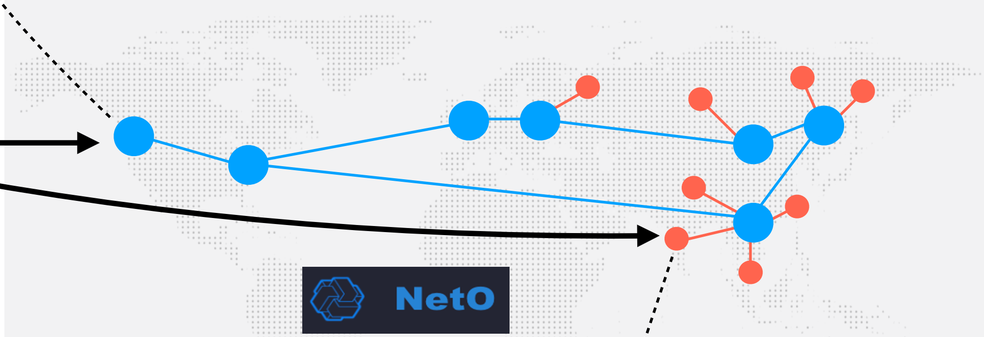
天猫 TMALL

Alibaba Cloud

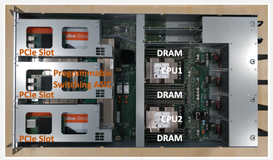
阿里全球 DNS 系统

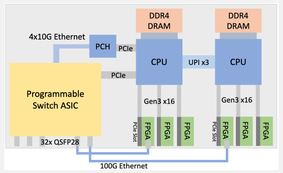


全球领先的超大规模高性能数据中心



全球广域网质量监测流量调度系统





全球最大规模部署的可编程计算网关系统

挑战1：稳定性/可靠性

挑战2：运维效率

挑战3：可预期流量调度

阿里云全球基础设施网络系统

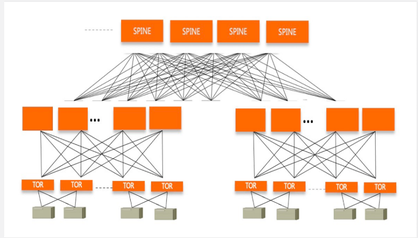
淘宝 Taobao

高德地图 amap.com

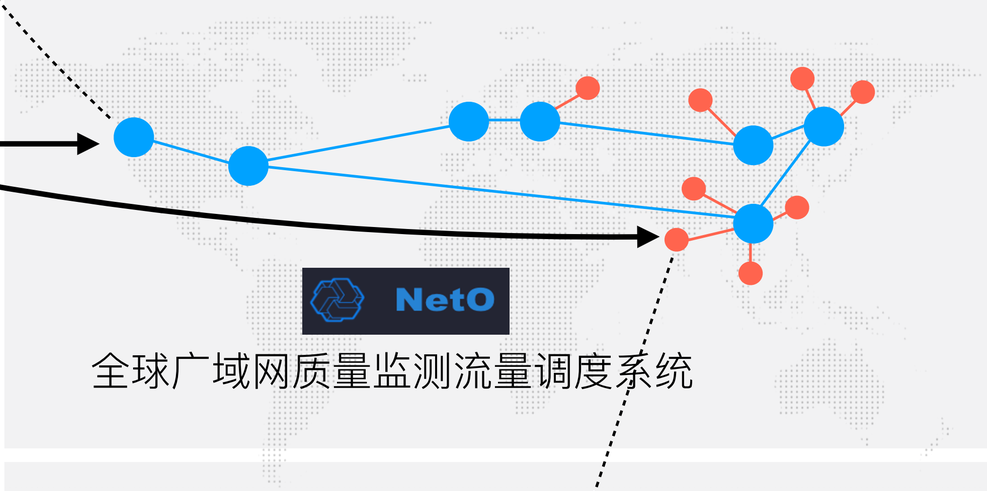
天猫 TMALL

Alibaba Cloud

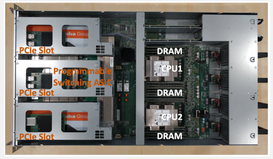
阿里全球 DNS 系统

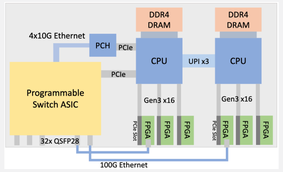


全球领先的超大规模高性能数据中心



全球广域网质量监测流量调度系统





全球最大规模部署的可编程计算网关系统

挑战1：稳定性/可靠性	仿真验证预防变更风险 [SIGCOMM'20]
	网络快速监控与故障定位
挑战2：运维效率	意图驱动体系，将运维决策从人交到系统 [SIGCOMM'19]
挑战3：可预期流量调度	细粒度应用感知的流量调度

阿里云全球基础设施网络系统

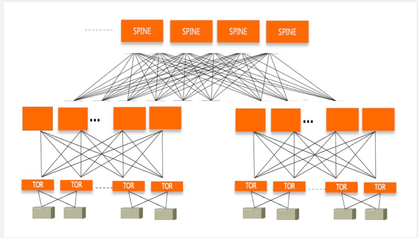
淘宝 Taobao

高德地图 amap.com

天猫 TMALL

Alibaba Cloud

阿里全球 DNS 系统

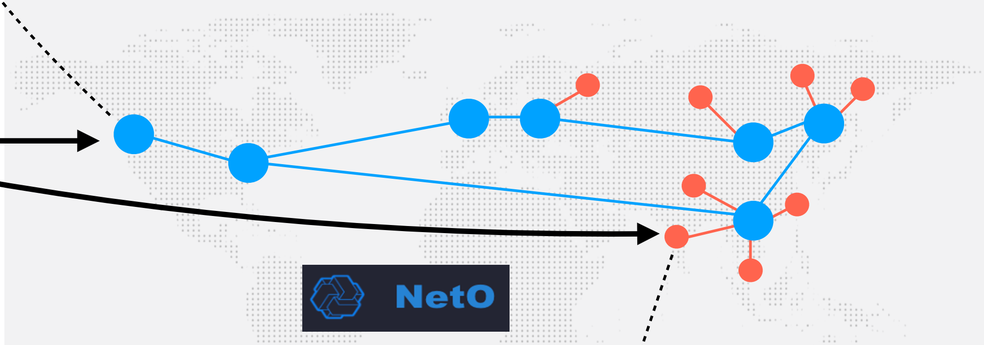


全球领先的超大规模高性能数据中心

挑战1：弹性可扩展

挑战2：稳定性/可靠性

挑战3：高性能算力



全球广域网质量监测流量调度系统

挑战1：稳定性/可靠性

仿真验证预防变更风险 [SIGCOMM'20]

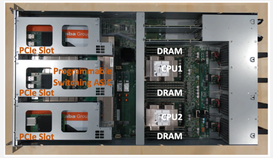
网络快速监控与故障定位

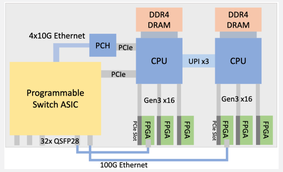
挑战2：运维效率

意图驱动体系，将运维决策从人交到系统 [SIGCOMM'19]

挑战3：可预期流量调度

细粒度应用感知的流量调度





全球最大规模部署的可编程计算网关系统

阿里云全球基础设施网络系统

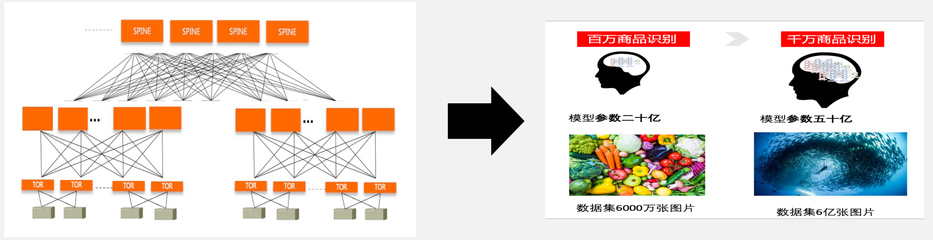
淘宝 Taobao

高德地图 amap.com

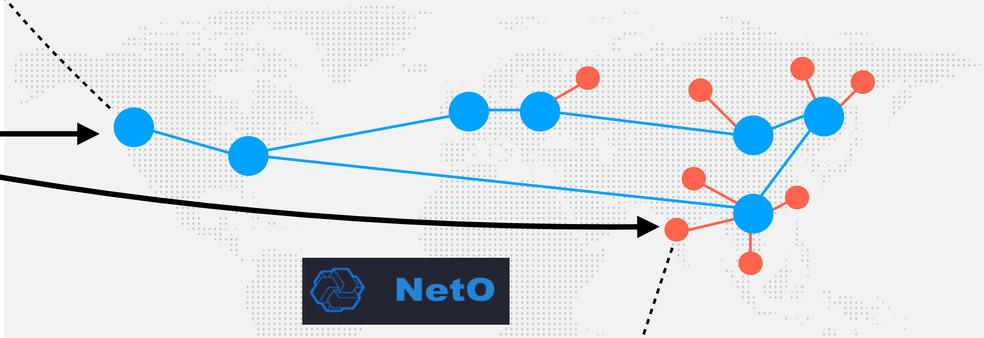
天猫 TMALL

Alibaba Cloud

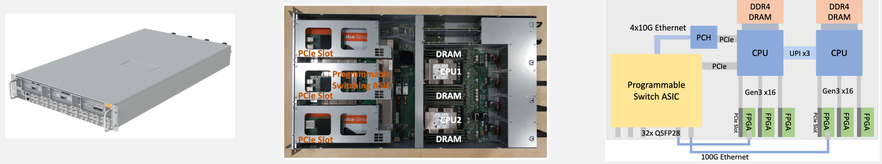
阿里全球 DNS 系统



全球领先的超大规模高性能数据中心



全球广域网质量监测流量调度系统



全球最大规模部署的可编程计算网关系统

挑战1：弹性可扩展	自研交换机，协议简化，体系化融合
挑战2：稳定性/可靠性	实时遥测精准定位故障 [SIGCOMM'20]
挑战3：高性能算力	精确反馈拥塞控制、端网协同低延时 [SIGCOMM'19, 22]
挑战1：稳定性/可靠性	仿真验证预防变更风险 [SIGCOMM'20]
	网络快速监控与故障定位
挑战2：运维效率	意图驱动体系，将运维决策从人交到系统 [SIGCOMM'19]
挑战3：可预期流量调度	细粒度应用感知的流量调度

阿里云全球基础设施网络系统

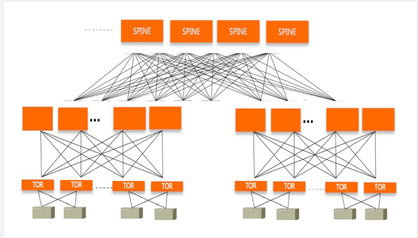
淘宝 Taobao

高德地图 amap.com

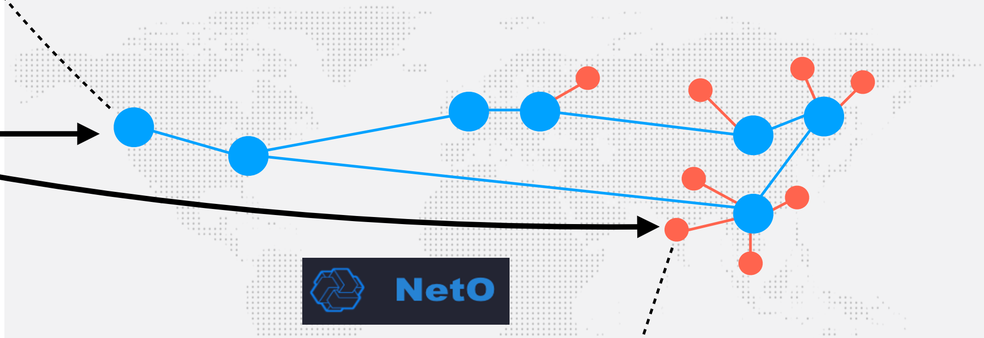
天猫 TMALL

Alibaba Cloud

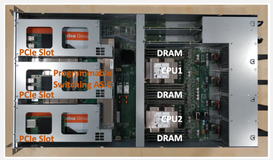
阿里全球 DNS 系统

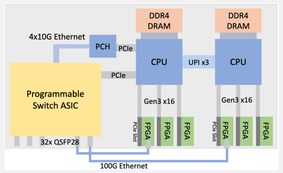


全球领先的超大规模高性能数据中心



全球广域网质量监测流量调度系统





全球最大规模部署的可编程计算网关系统

挑战1：弹性可扩展	自研交换机，协议简化，体系化融合
挑战2：稳定性/可靠性	实时遥测精准定位故障 [SIGCOMM'20]
挑战3：高性能算力	精确反馈拥塞控制、端网协同低延时 [SIGCOMM'19, 22]
挑战1：稳定性/可靠性	仿真验证预防变更风险 [SIGCOMM'20]
	网络快速监控与故障定位
挑战2：运维效率	意图驱动体系，将运维决策从人交到系统 [SIGCOMM'19]
挑战3：可预期流量调度	细粒度应用感知的流量调度
挑战1：芯片编程效率	
挑战2：芯片程序正确性	

阿里云全球基础设施网络系统

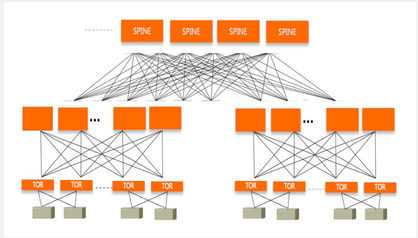
淘宝 Taobao

高德地图 amap.com

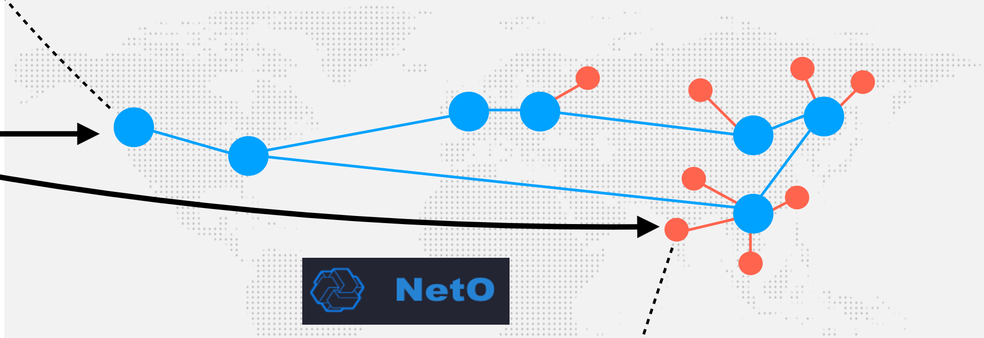
天猫 TMALL

Alibaba Cloud

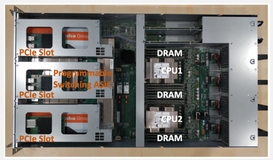
阿里全球 DNS 系统

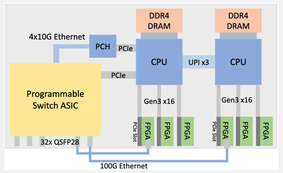


全球领先的超大规模高性能数据中心



全球广域网质量监测流量调度系统

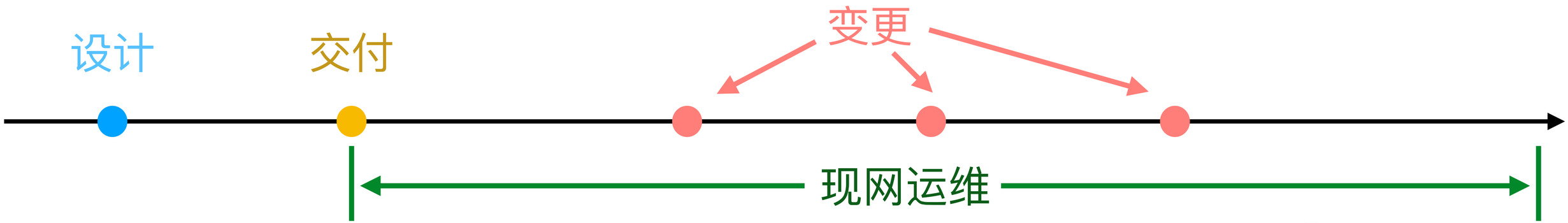




全球最大规模部署的可编程计算网关系统

挑战1：弹性可扩展	自研交换机，协议简化，体系化融合
挑战2：稳定性/可靠性	实时遥测精准定位故障 [SIGCOMM'20]
挑战3：高性能算力	精确反馈拥塞控制、端网协同低延时 [SIGCOMM'19, 22]
挑战1：稳定性/可靠性	仿真验证预防变更风险 [SIGCOMM'20]
	网络快速监控与故障定位
挑战2：运维效率	意图驱动体系，将运维决策从人交到系统 [SIGCOMM'19]
挑战3：可预期流量调度	细粒度应用感知的流量调度
挑战1：芯片编程效率	Lyra 异构芯片的程序编译 [SIGCOMM'20]
	可证明最优的芯片资源自动优化 [NSDI'22]
挑战2：芯片程序正确性	全逻辑覆盖的自动化测试生成 [SIGCOMM'22]

网络规划和运维的复杂



复杂

- 繁多的路由协议
- 路由重策略繁多

异构

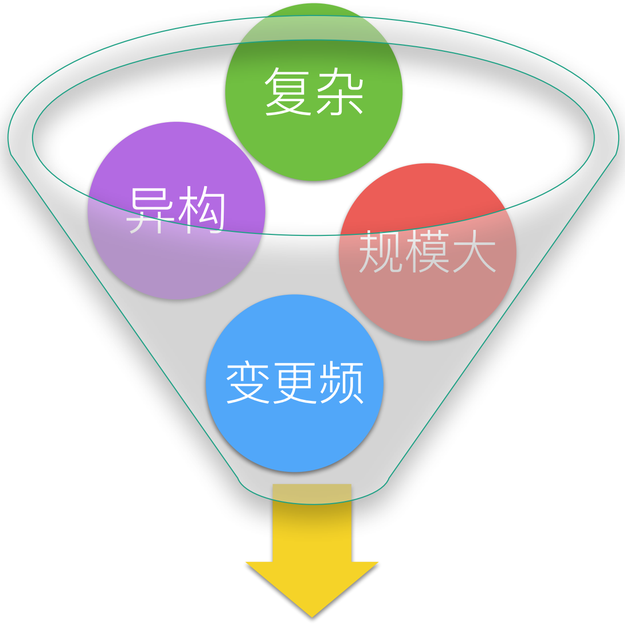
- 细节参数繁多
- 厂商差异性

规模大

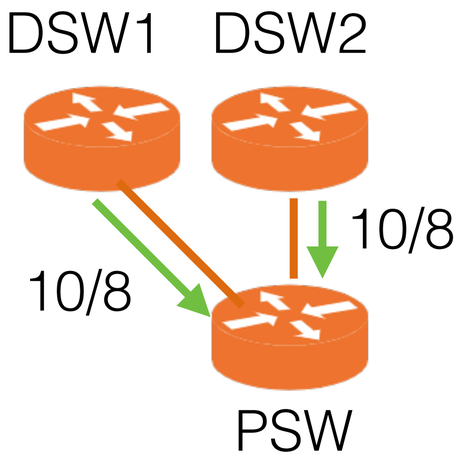
- 大量设备分布协同
- 万行配置/设备

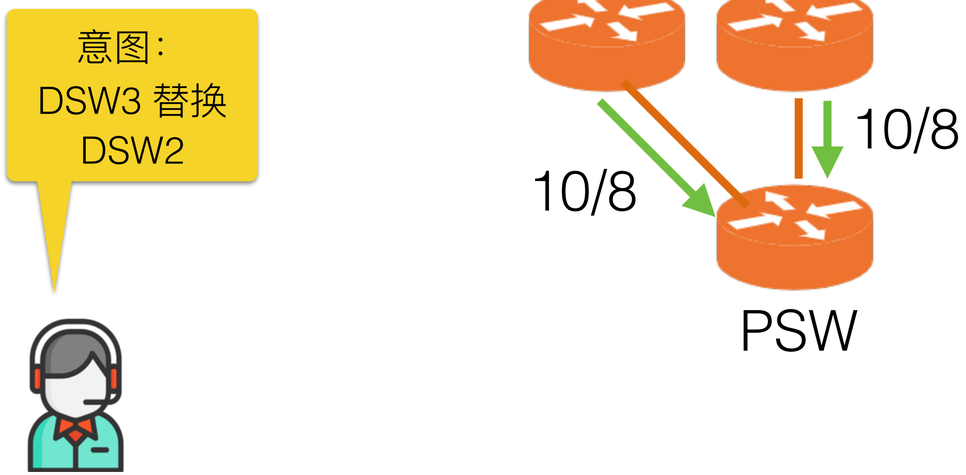
变更频

- 万次变更每年
- 需求多样化



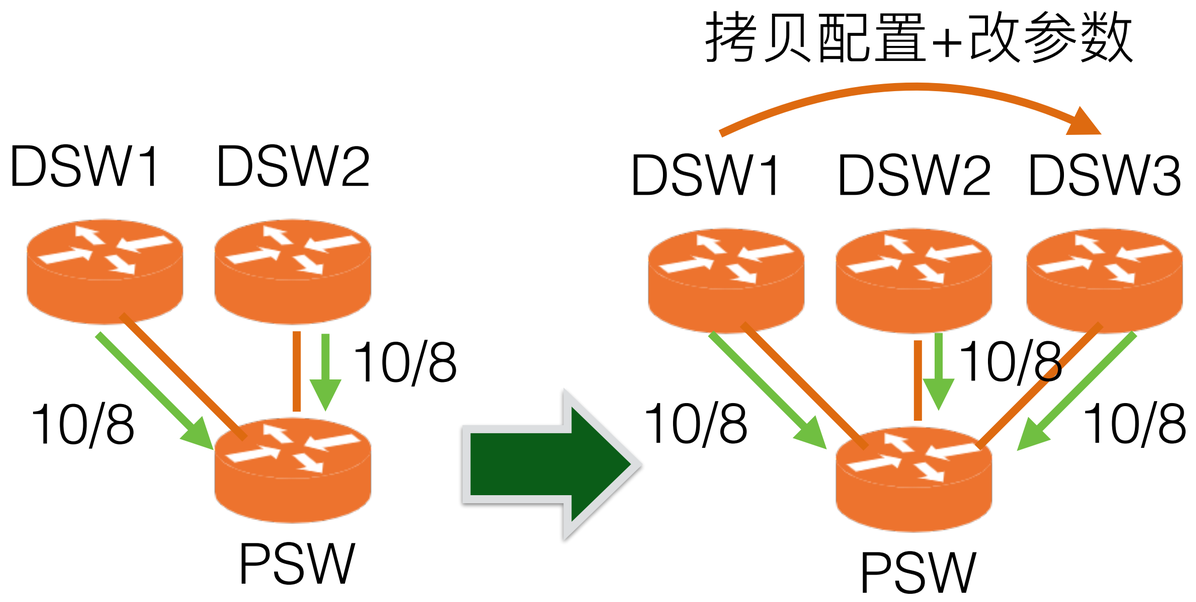
靠人的 “小心谨慎” 是
无法避免的


DSW1
DSW2
10/8
10/8
PSW

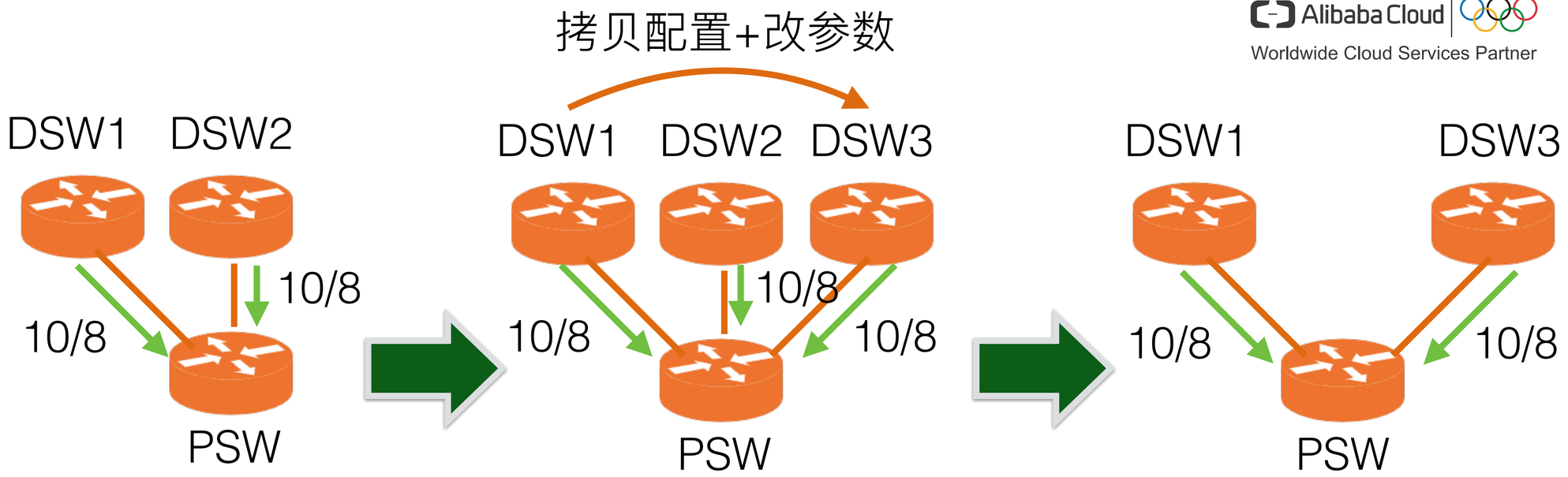

意图：
DSW3 替换
DSW2

DSW1
DSW2
10/8
10/8
PSW

意图：
DSW3 替换
DSW2

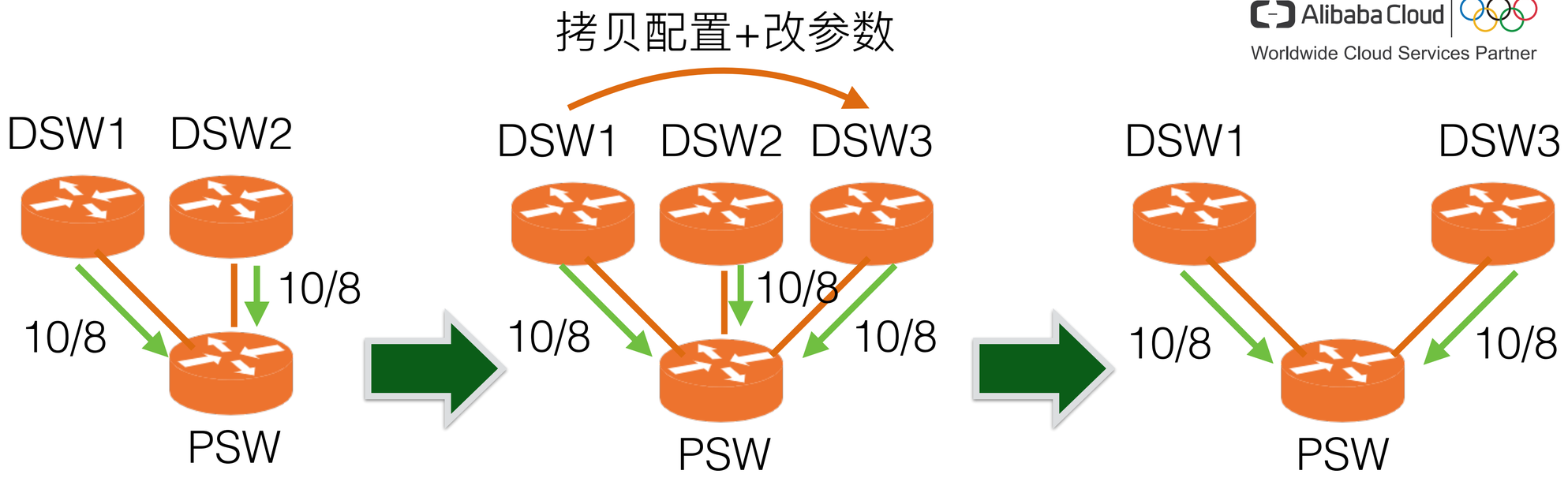


意图：
DSW3 替换
DSW2



意图：
DSW3 替换
DSW2

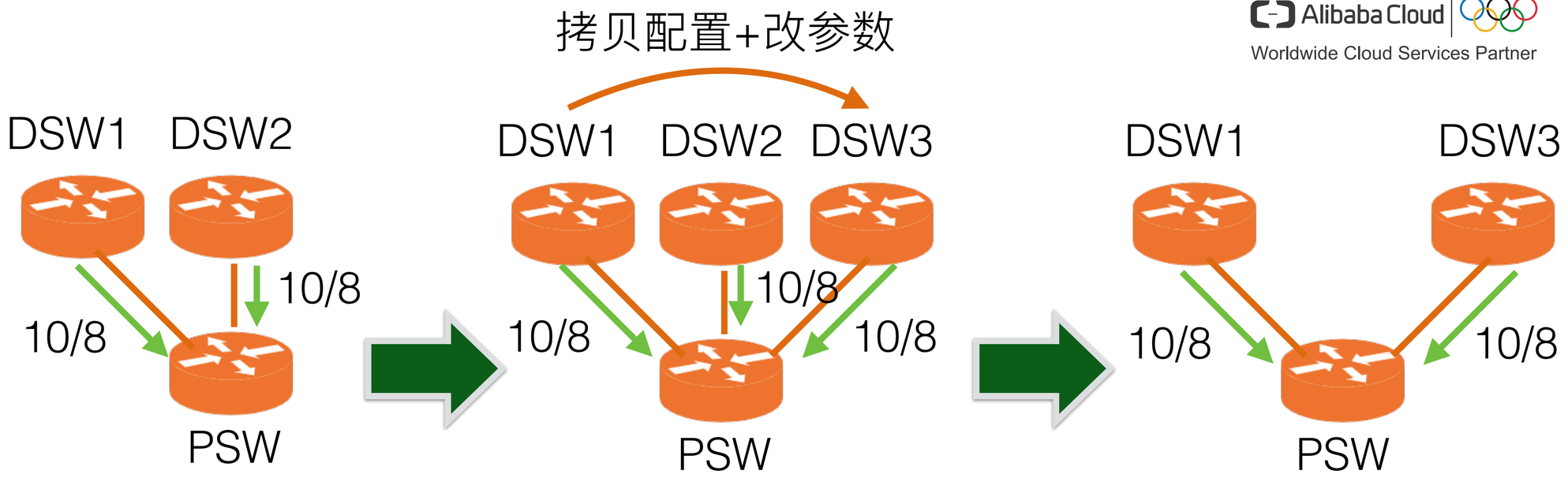
我们认为



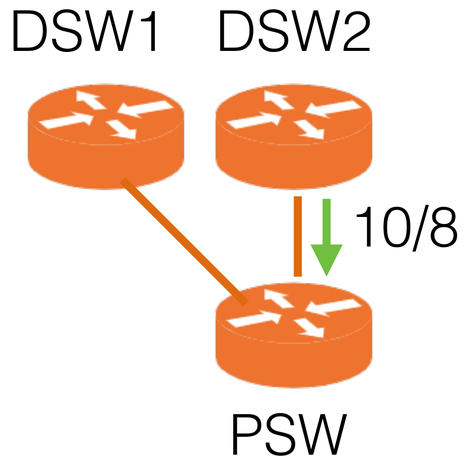
实际情况

意图：
DSW3 替换
DSW2

我们认为

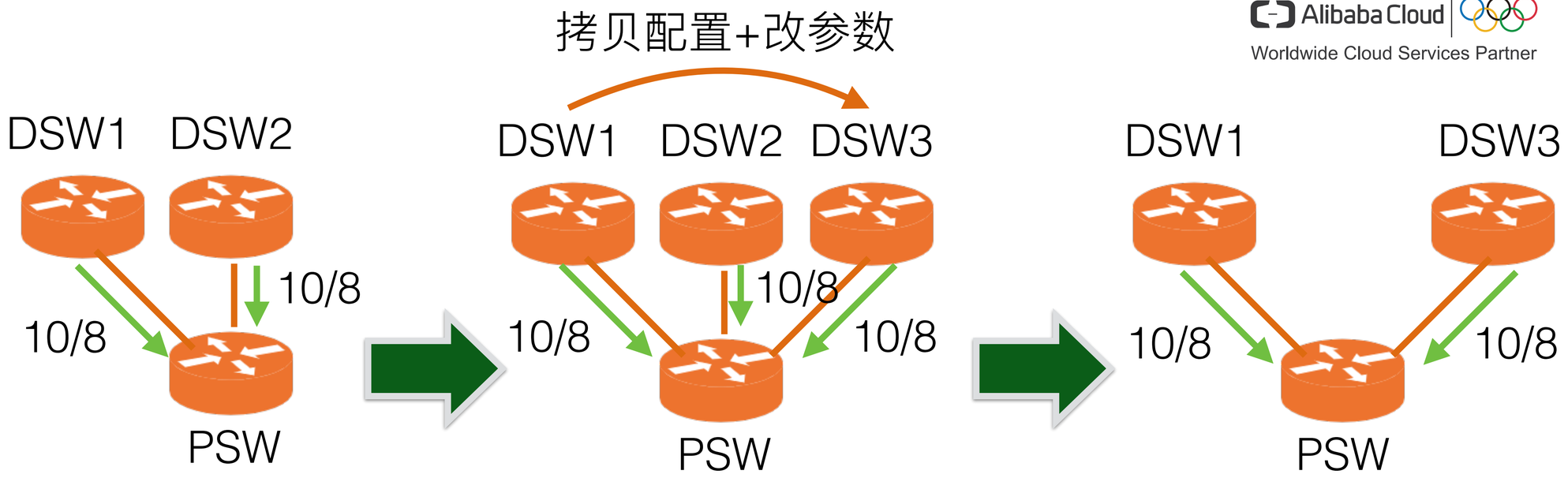


实际情况

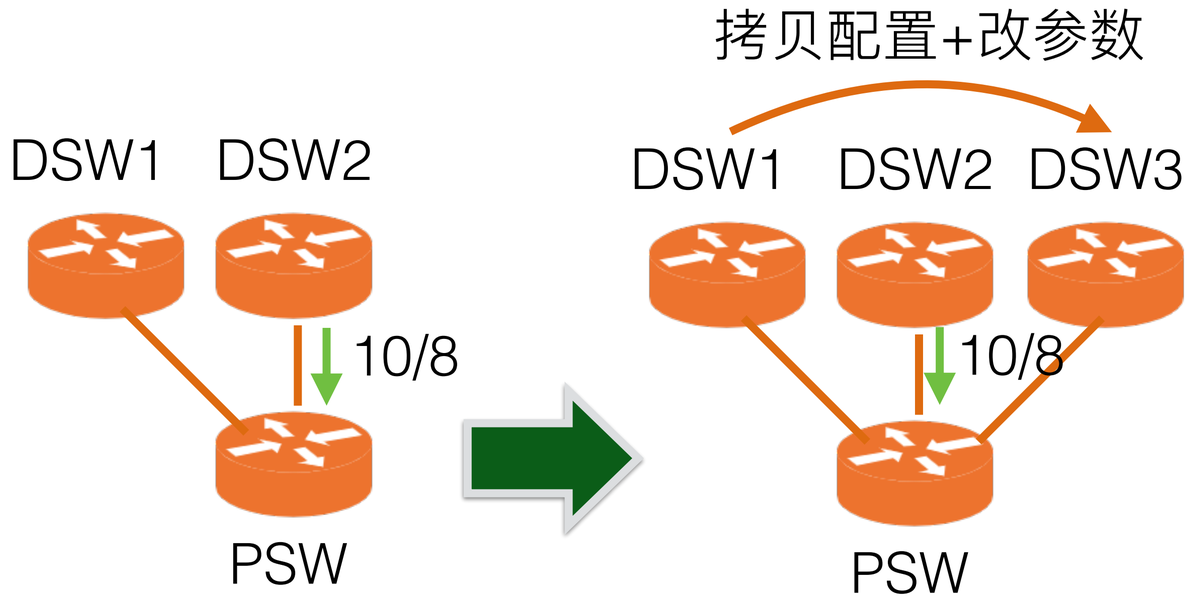


意图：
DSW3 替换
DSW2

我们认为

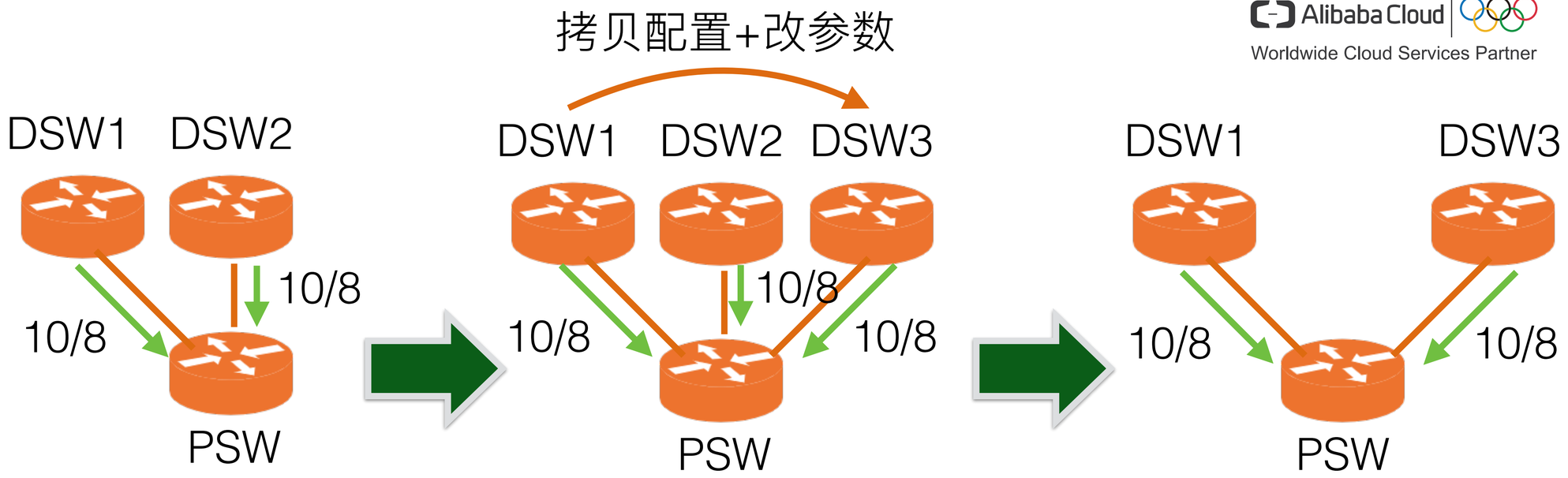


实际情况

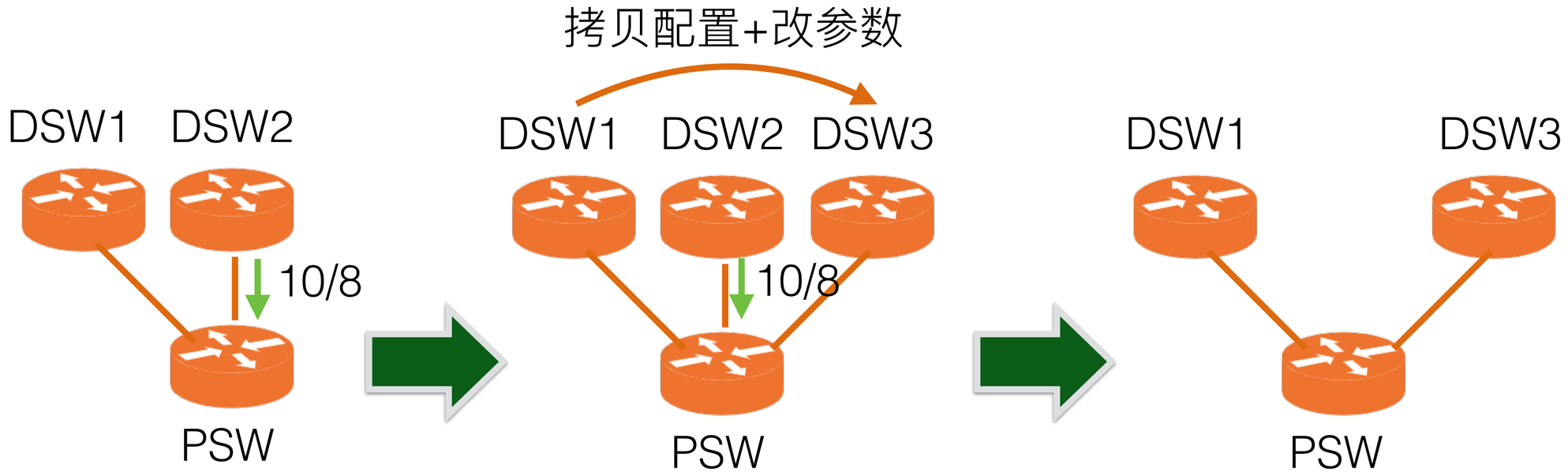


意图：
DSW3 替换
DSW2

我们认为



实际情况



目录

传统基于配置的思想

设计

Intent -> 现网配置

现网配置 -> Intent

交付

Intent -> 现网配置

现网配置 -> Intent

变更

Intent -> 现网配置

现网配置 -> Intent

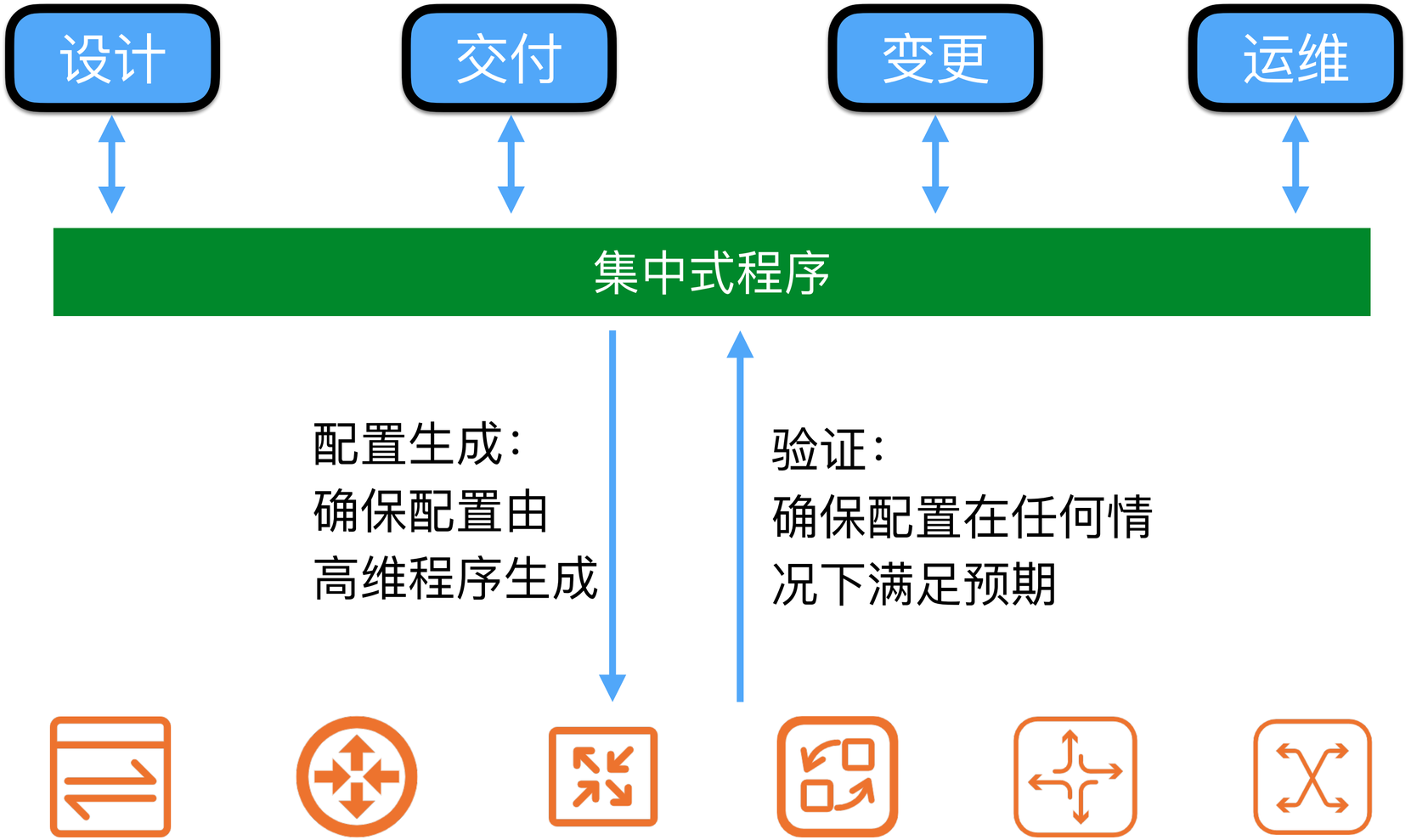
运维

Intent -> 现网配置

现网配置 -> Intent

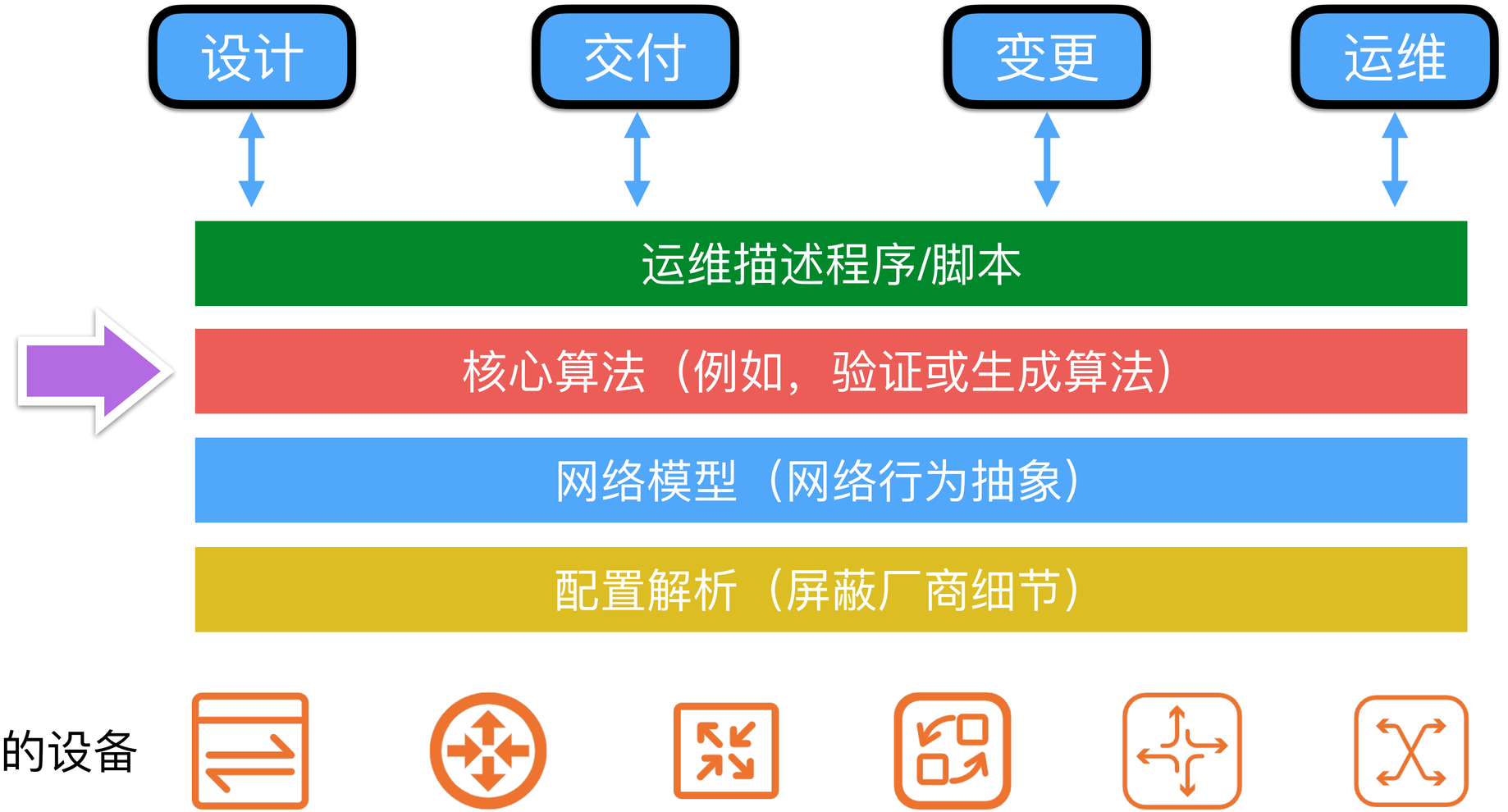
不同厂商的设备

IBN 思想：高级抽象



IBN 思想

集中式网络规划体系

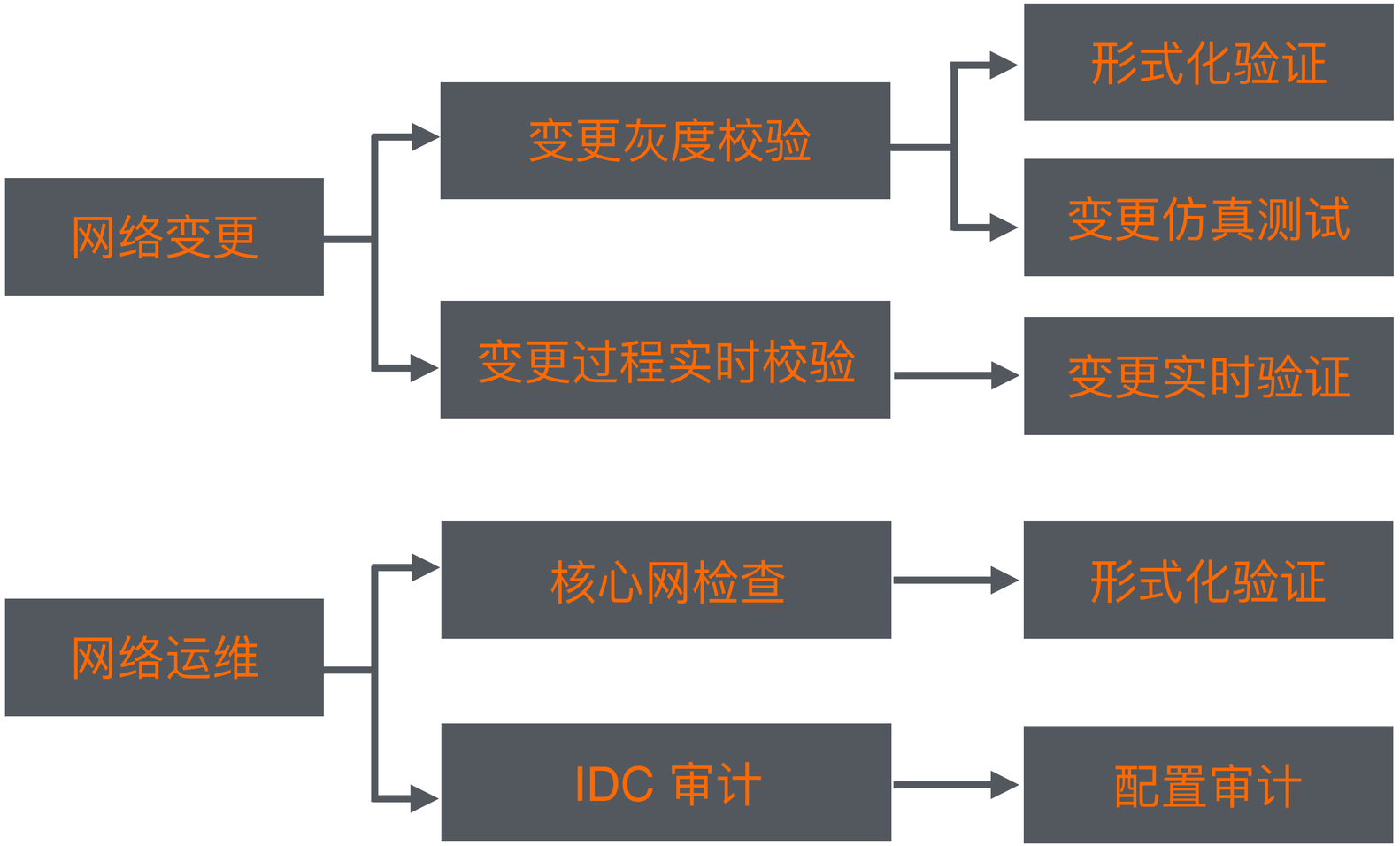


不同厂商的设备

核心技术之一：验证

挑战1：有多准?

挑战2：有多快?



目录

Network configuration verification in Alibaba

Alibaba Cloud
Worldwide Cloud Services Partner

Monkey King: Fire & Golden Eye
(The ability to see the truth)

火眼 金睛

3:30 - 3:45 pm EDT & 2:30 - 2:45 am EDT

Accuracy, Scalability, Coverage – A Practical Configuration Verifier on a Global WAN
Fangdan Ye *(Tsinghua University)*; Da Yu *(Brown University)*; Ennan Zhai, Hongqiang Harry Liu *(Alibaba Group)*; Bingchuan Tian *(Nanjing University)*; Qiaobo Ye, Chunsheng Wang, Xin Wu, Tianchen Guo, Cheng Jin, Duncheng She, Qing Ma, Biao Cheng, Hui Xu, Ming Zhang *(Alibaba Group)*; Zhiliang Wang *(Tsinghua University)*; Rodrigo Fonseca *(Brown University)*

Abstract: This paper presents Hoyan-- the first reported large scale deployment of configuration verification in a global-scale wide area network (WAN). Hoyan has been running in production for more than two years and is currently used for all critical configuration auditing and updates on the WAN. We highlight our innovative designs and real-life experience to make Hoyan accurate and scalable in practice. For accuracy under the inconsistencies of devices' vendor-specific behaviors (VSBs), Hoyan continuously discovers the flaws in device behavior models, thus aiding the operators in fixing the models. For scalability to verify our global WAN, Hoyan introduces a "global-simulation & local formal-modeling" strategy to model uncertainties in small scales and perform aggressive pruning of possibilities during the protocol simulations. Hoyan achieves near-100% verification accuracy after it detected and fixed O(10) VSBs on our WAN. Hoyan has prevented many potential service failures resulting from misconfiguration and reduced the failure rate of updates of our WAN by more than half in 2019.

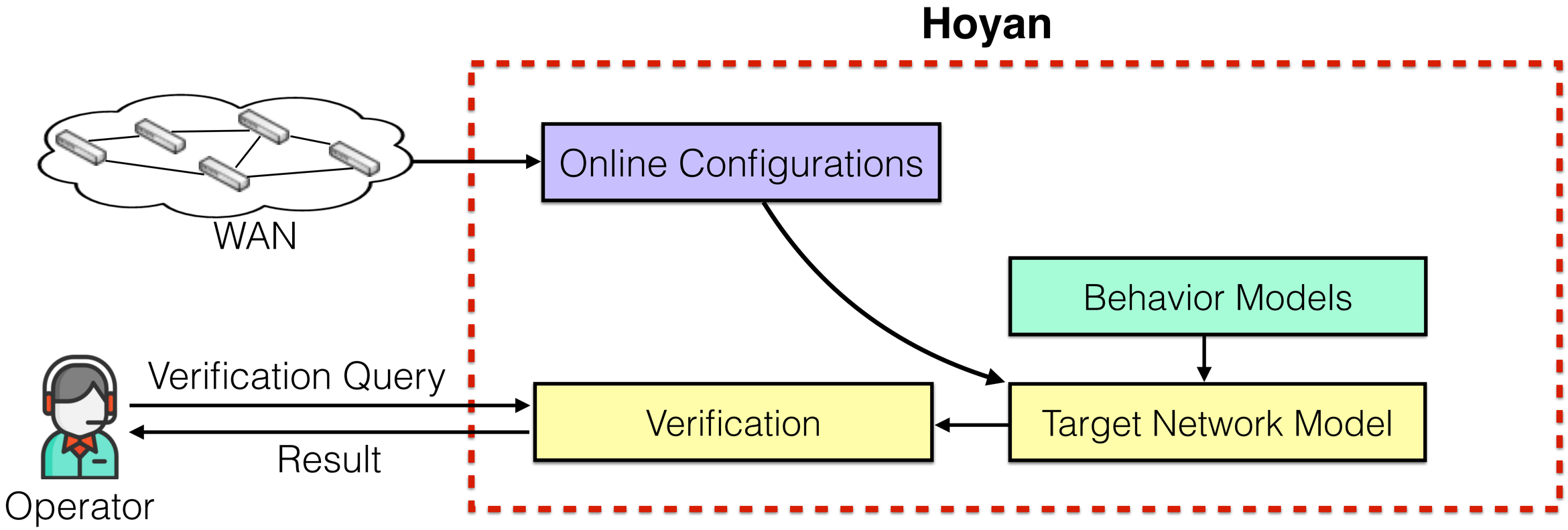
Hoyan (火眼)
Routing configuration verification
[ACM SIGCOMM'20]

Safely and Automatically Updating In-Network ACL Configurations with Intent Language
Bingchuan Tian *(Nanjing University)*, Xinyi Zhang *(University of California Santa Barbara)*, Ennan Zhai, Hongqiang Harry Liu, Qiaobo Ye, Chunsheng Wang, Xin Wu, Zhiming Ji, Yihong Sang, Ming Zhang *(Alibaba Group)*, Da Yu *(Brown University)*, Chen Tian *(Nanjing University)*, Haitao Zheng, Ben Y. Zhao *(University of Chicago)*

Abstract: In-network Access Control List (ACL) is an important technique in ensuring network-wide connectivity and security. As cloud-scale WANs today constantly evolve in size and complexity, in-network ACL rules are becoming increasingly more complex. This presents a great challenge to the updating process of ACL configurations: network operators are frequently required to update "tangled" ACL rules across thousands of devices to meet diverse business requirements, and even a single ACL misconfiguration may lead to network disruptions. Such increasing challenges call for an automated system to improve the efficiency and correctness of ACL updates. This paper presents Jinjing, a system that aids Alibaba's network operators in automatically and correctly updating ACL configurations in Alibaba's global WAN. Jinjing allows the operators to express in a declarative language, named LAI, their update intent (e.g., ACL migration and traffic control). Then, Jinjing automatically synthesizes ACL update plans that satisfy their intent. At the heart of Jinjing, we develop a set of novel verification and synthesis techniques to rigorously guarantee the correctness of update plans. In Alibaba, our operators have used Jinjing to efficiently update their ACLs and have thus prevented significant service downtime.

Jinjing (金睛)
In-Network ACL verification
[ACM SIGCOMM'19]

Hoyan

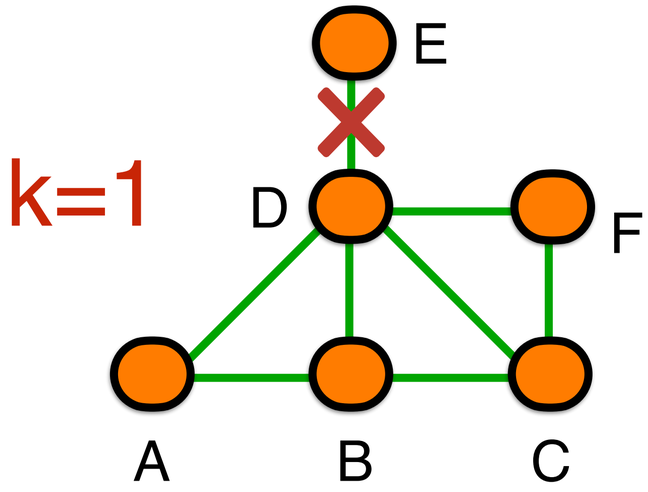


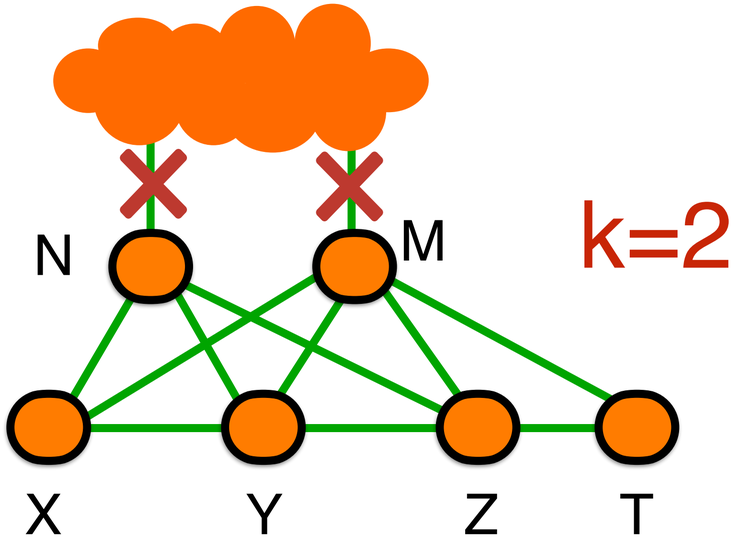
Technical challenges

Challenge 1: Scalability with failure coverage in our global WAN

Technical challenges

Challenge 1: Scalability with failure coverage in our global WAN

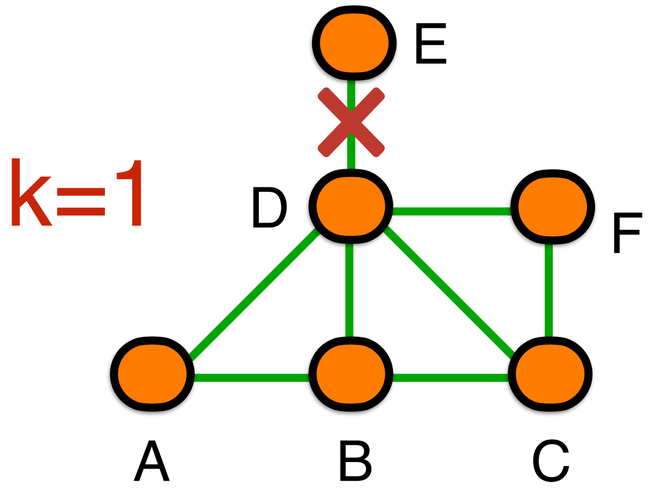


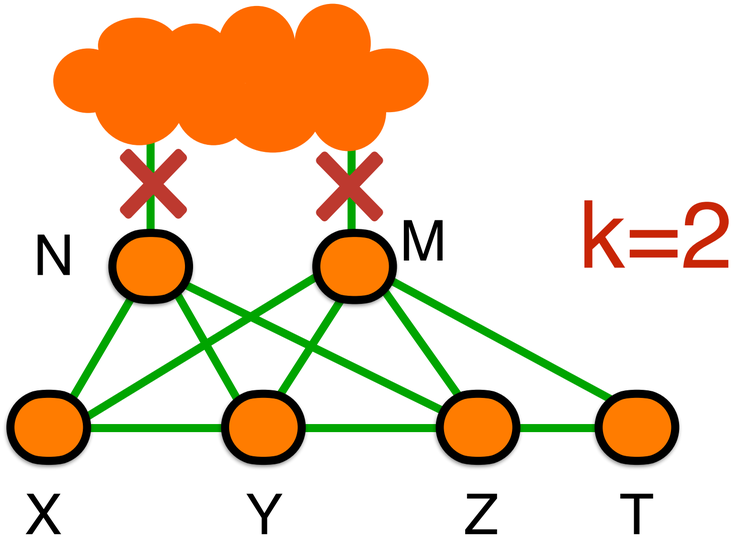


Technical challenges

Challenge 1: Scalability with failure coverage in our global WAN

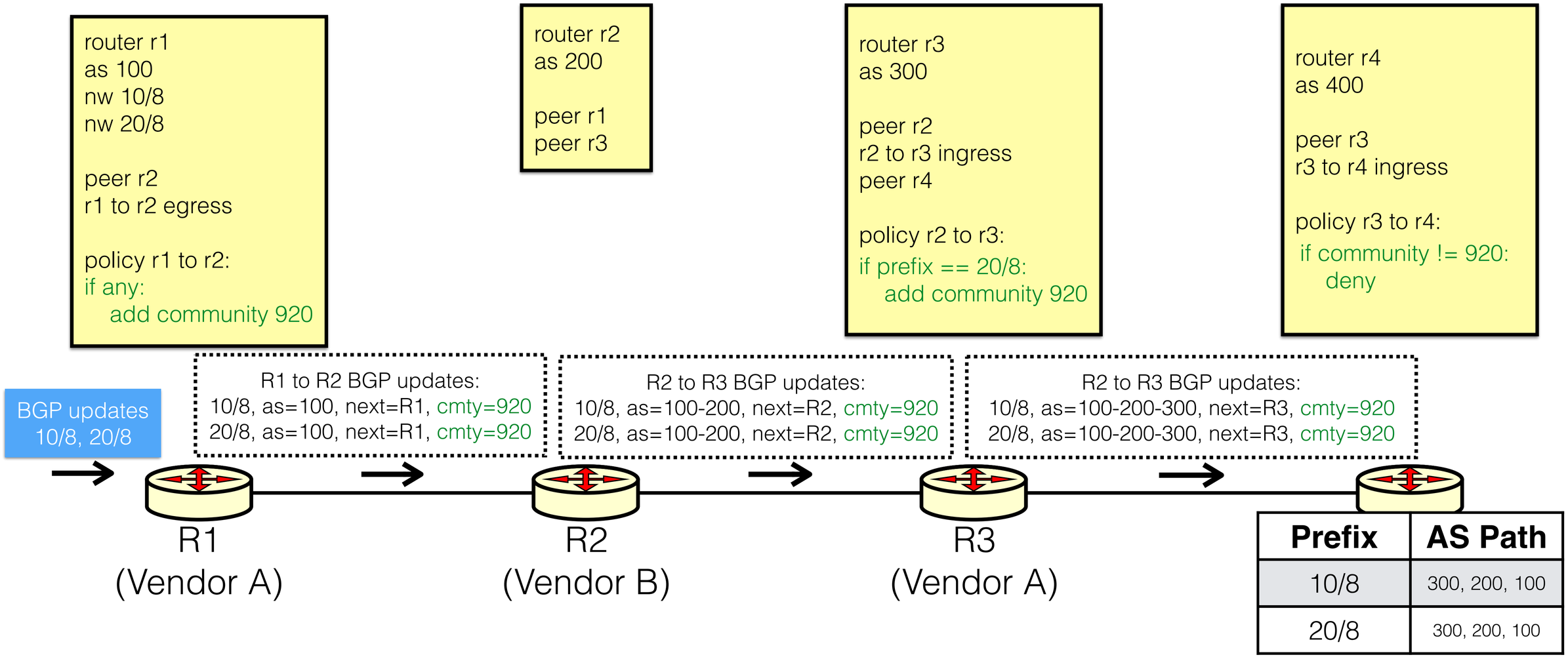
- Simulation-based verification efforts, e.g., Batfish, need to enumerate C_n^k cases for checking under arbitrary ***k*** failures out of ***n*** links
- Formal model approaches, e.g., Minesweeper, are not scalable since a large WAN generates a huge SMT formula
- Asymmetry of our WAN invalidates symmetry-based simplification approaches





Technical challenges

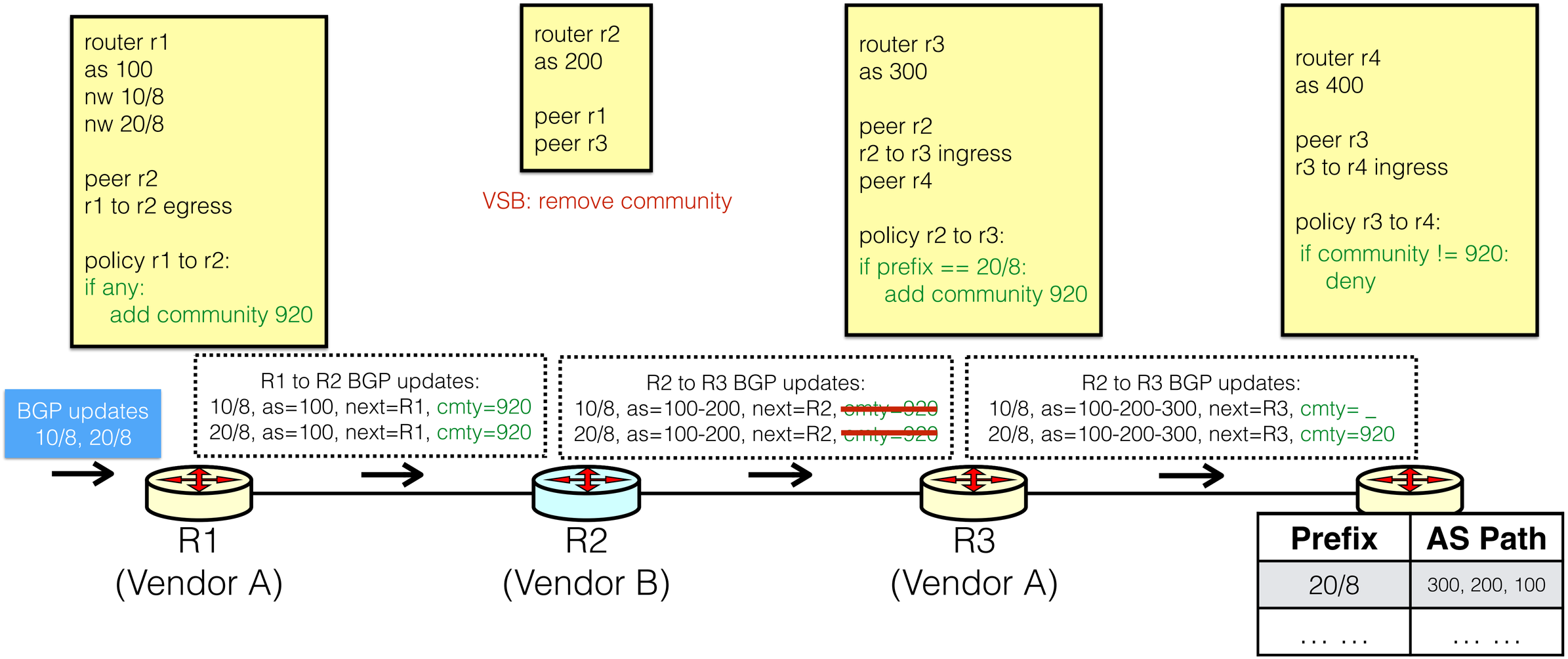
Challenge 2: Faithfulness of device behavior model



Prefix	AS Path
10/8	300, 200, 100
20/8	300, 200, 100

Technical challenges

Challenge 2: Faithfulness of device behavior model

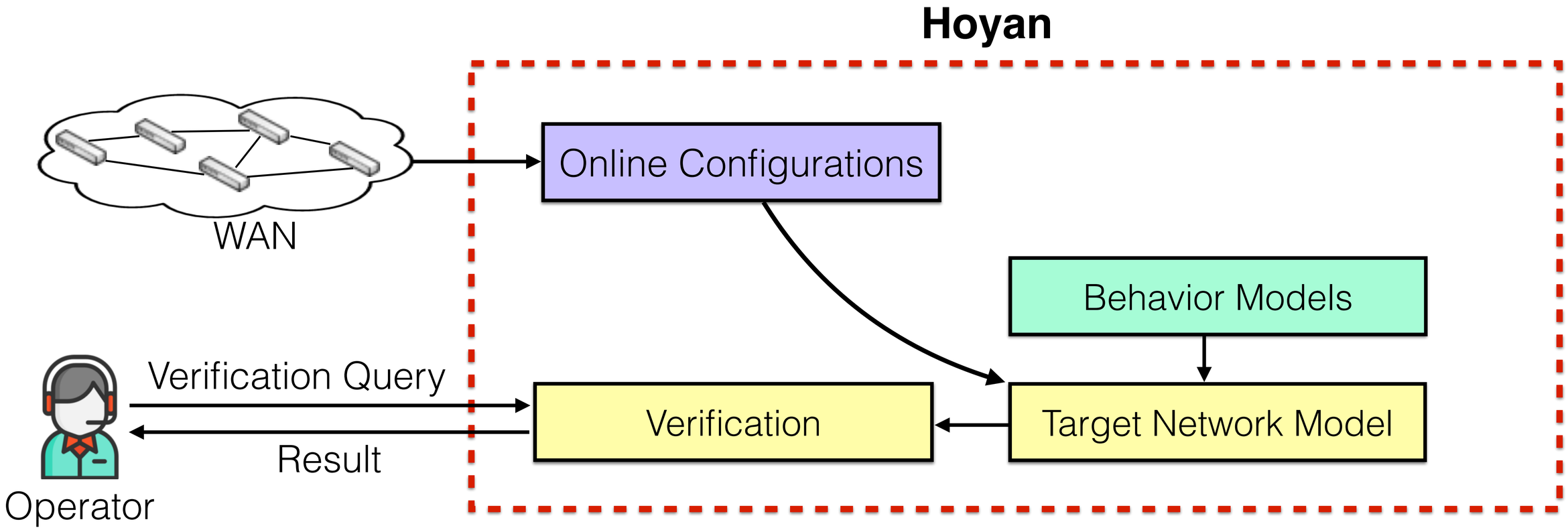


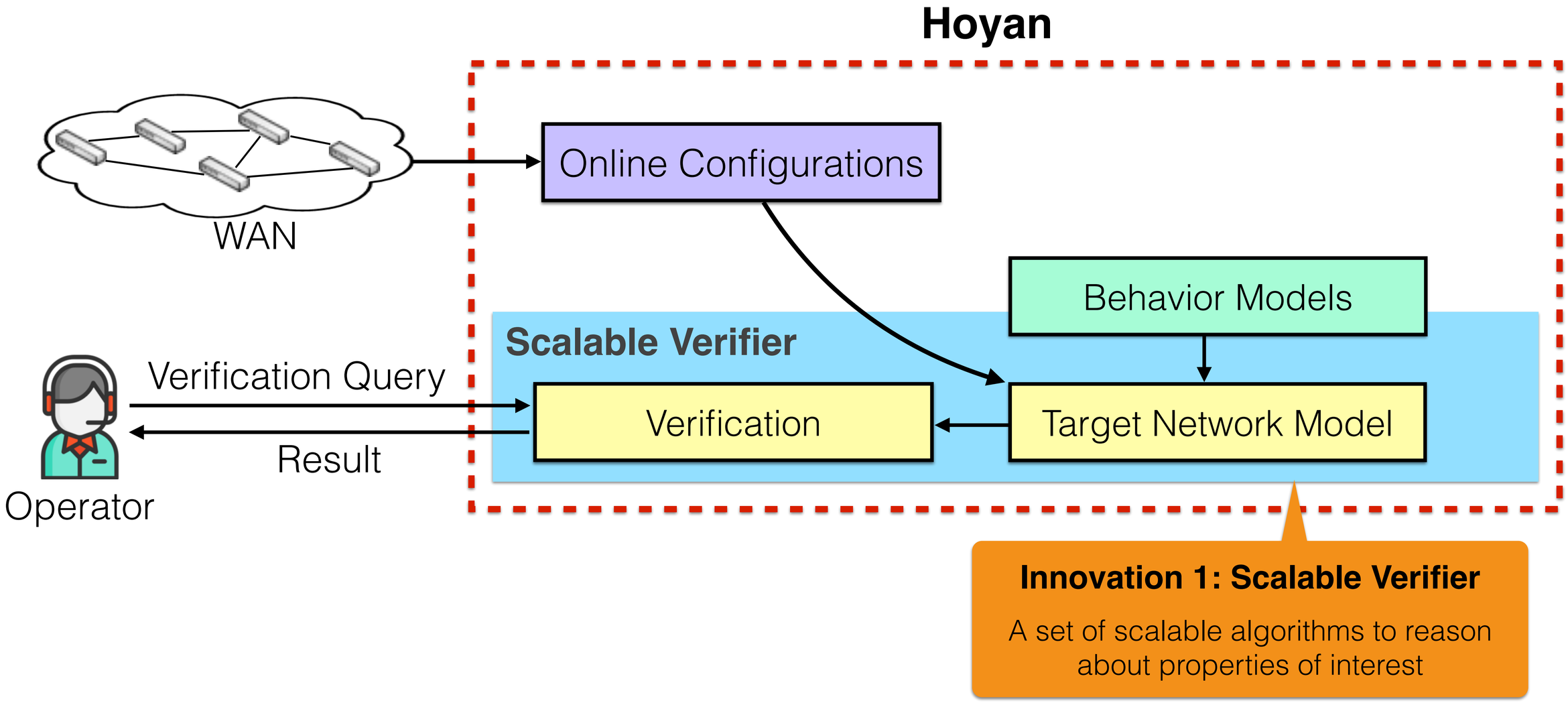
Technical challenges

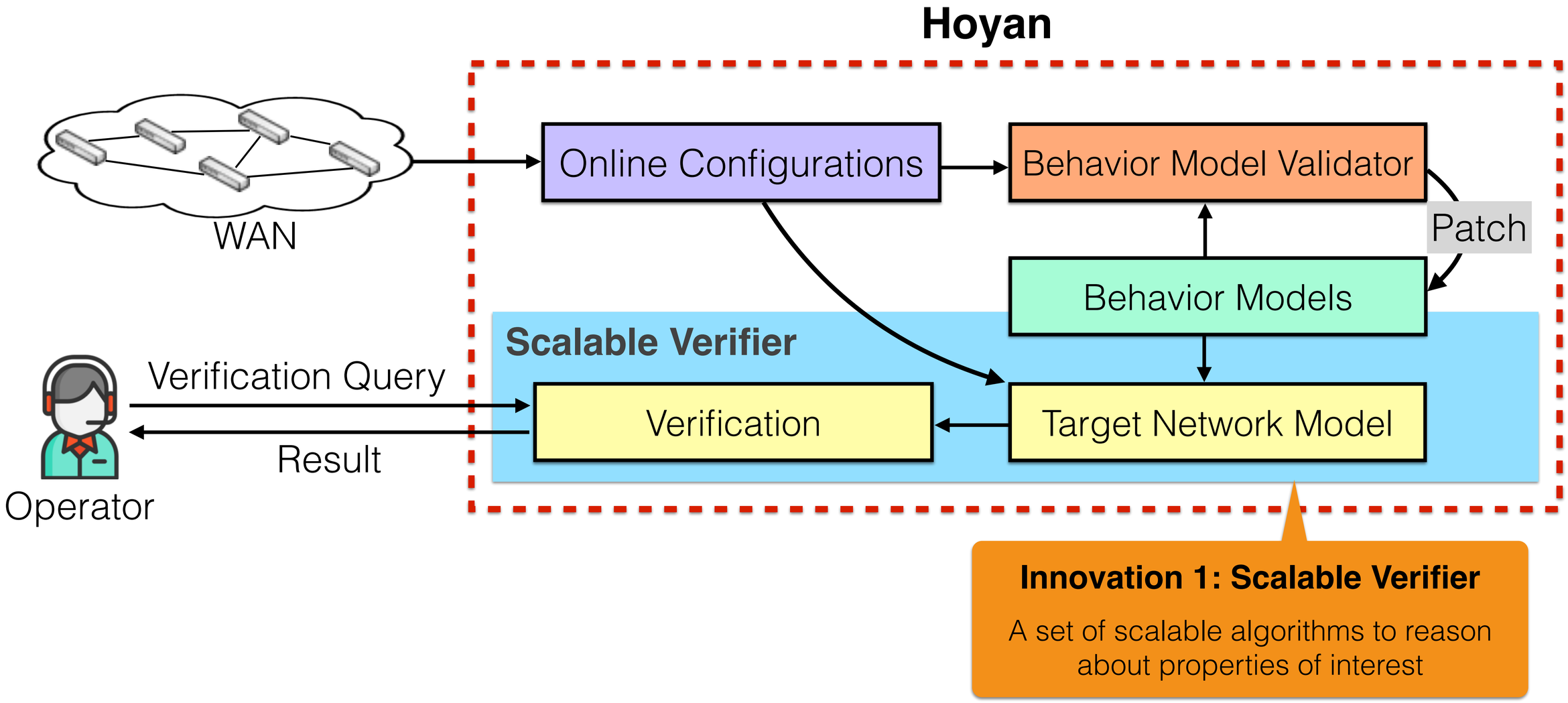
Challenge 2: Faithfulness of device behavior model

- Vendors implemented the same protocols in various ways due to the ambiguity of RFC
- Vendor-specific behaviors (VSBs) significantly affect the accuracy of network modeling
- No existing efforts can detect or tune the VSBs in network model

Hoyan

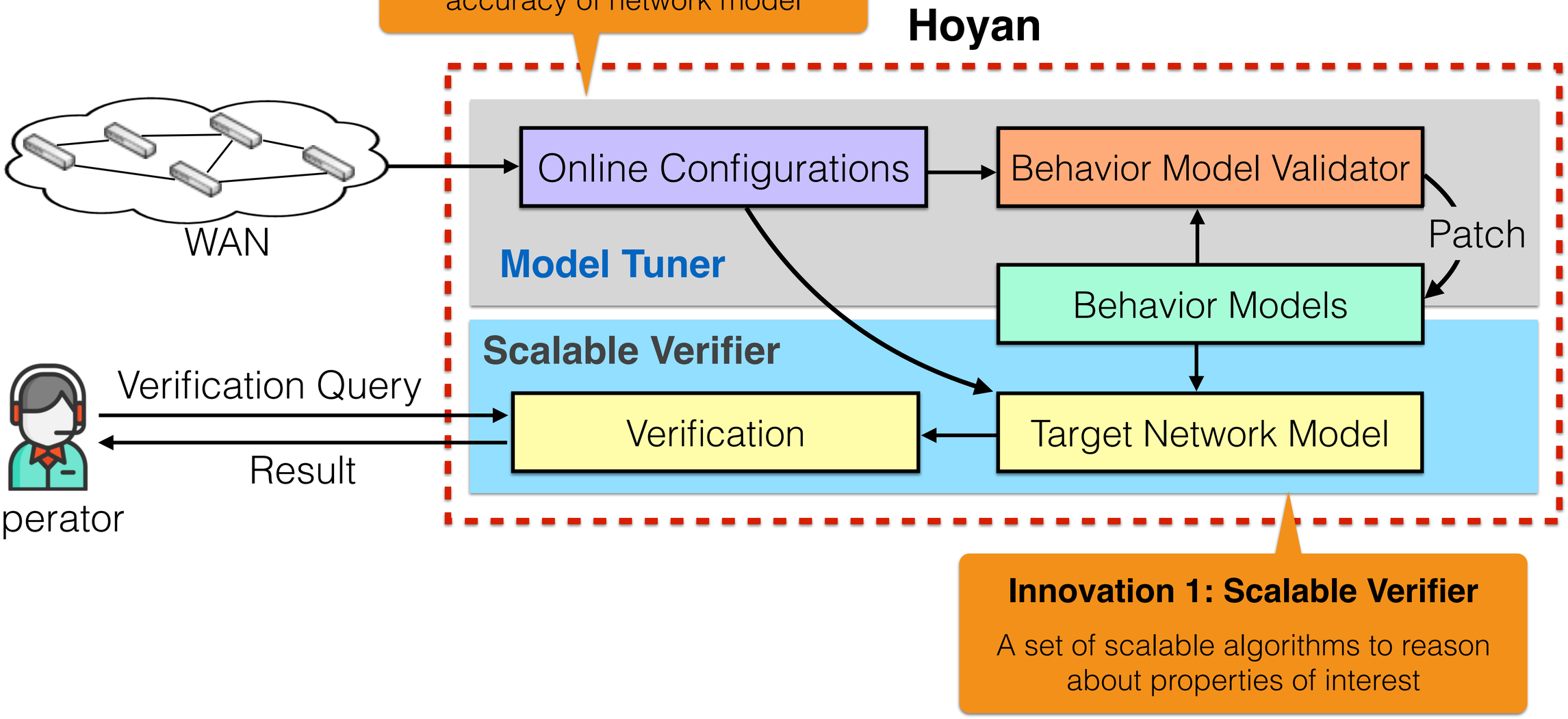



Hoyan
WAN
Online Configurations
Behavior Models
Scalable Verifier
Verification Query
Result
Verification
Target Network Model
Operator
Innovation 1: Scalable Verifier
A set of scalable algorithms to reason about properties of interest


Hoyan
WAN
Online Configurations
Behavior Model Validator
Patch
Behavior Models
Scalable Verifier
Verification Query
Result
Verification
Target Network Model
Operator
Innovation 1: Scalable Verifier
A set of scalable algorithms to reason about properties of interest

Innovation 2: Model Tuner

A systematic way to tune the accuracy of network model



Innovation 1: Scalable Verifier

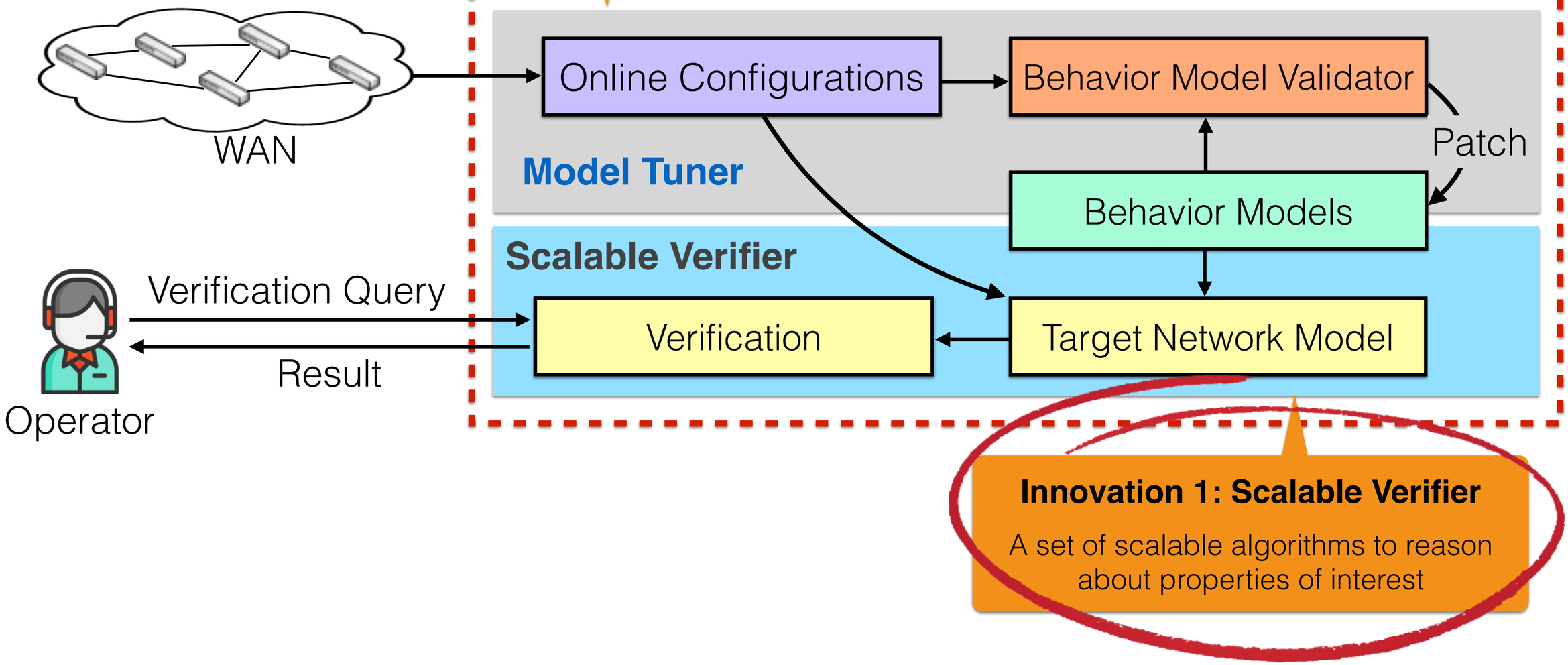
A set of scalable algorithms to reason about properties of interest

Hoyan

Alibaba Cloud
Worldwide Cloud Services Partner

Innovation 2: Model Tuner

A systematic way to tune the accuracy of network model



Innovation 1: Scalable Verifier

A set of scalable algorithms to reason about properties of interest

How to address the scalability challenge?

Key insight:

- Simulation-based approaches are scalable but fail to cover all possible cases
- Formal model approaches can encode all possibilities and conditions as a formula but are not scalable because solving such a huge formula is expensive

How to address the scalability challenge?

Key insight:

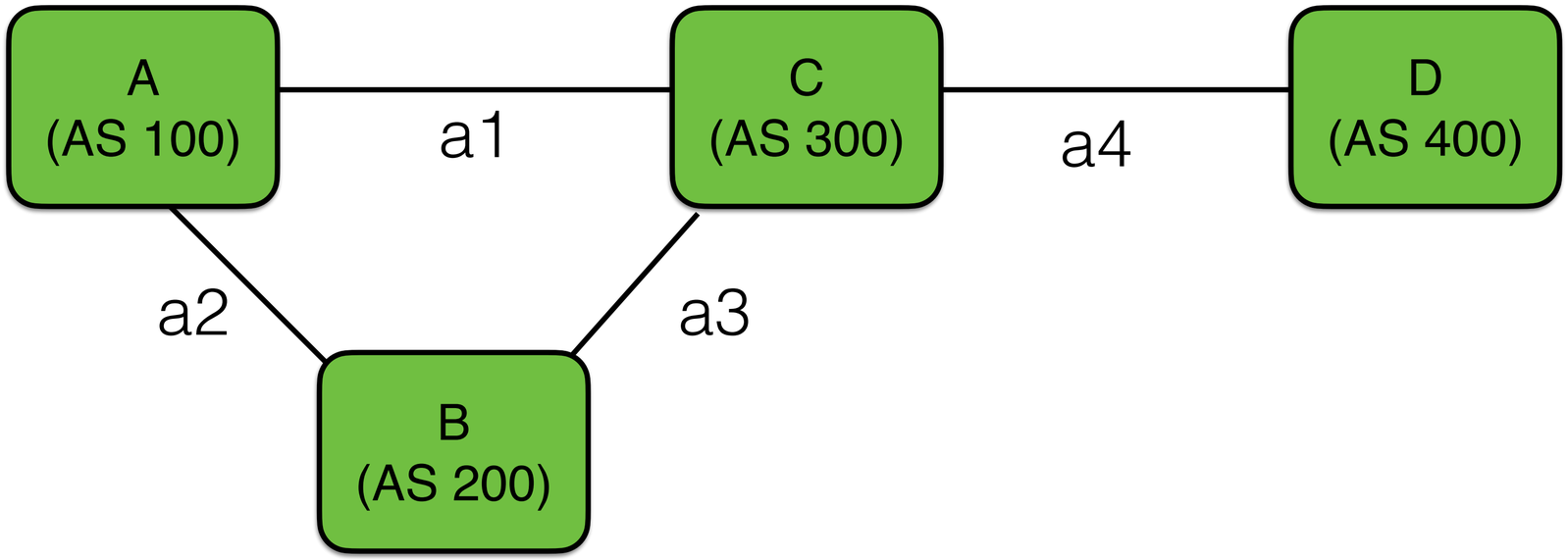
- Simulation-based approaches are scalable but fail to cover all possible cases
- Formal model approaches can encode all possibilities and conditions as a formula but are not scalable because solving such a huge formula is expensive

Solution: Global simulation & locally formal modeling approach

- We run overall simulation for global scalability
- Each router node locally encodes its all possible routing conditions that are transmitted along with the simulation process

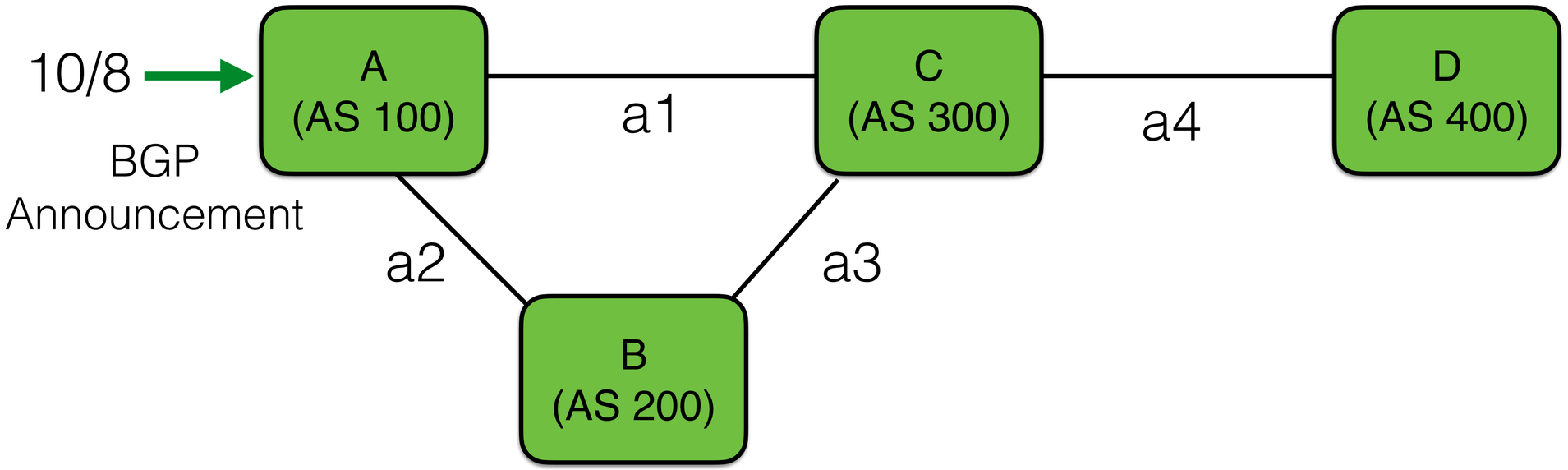
Global simulation & local formal-modeling

Checking k-failure tolerance between A and D

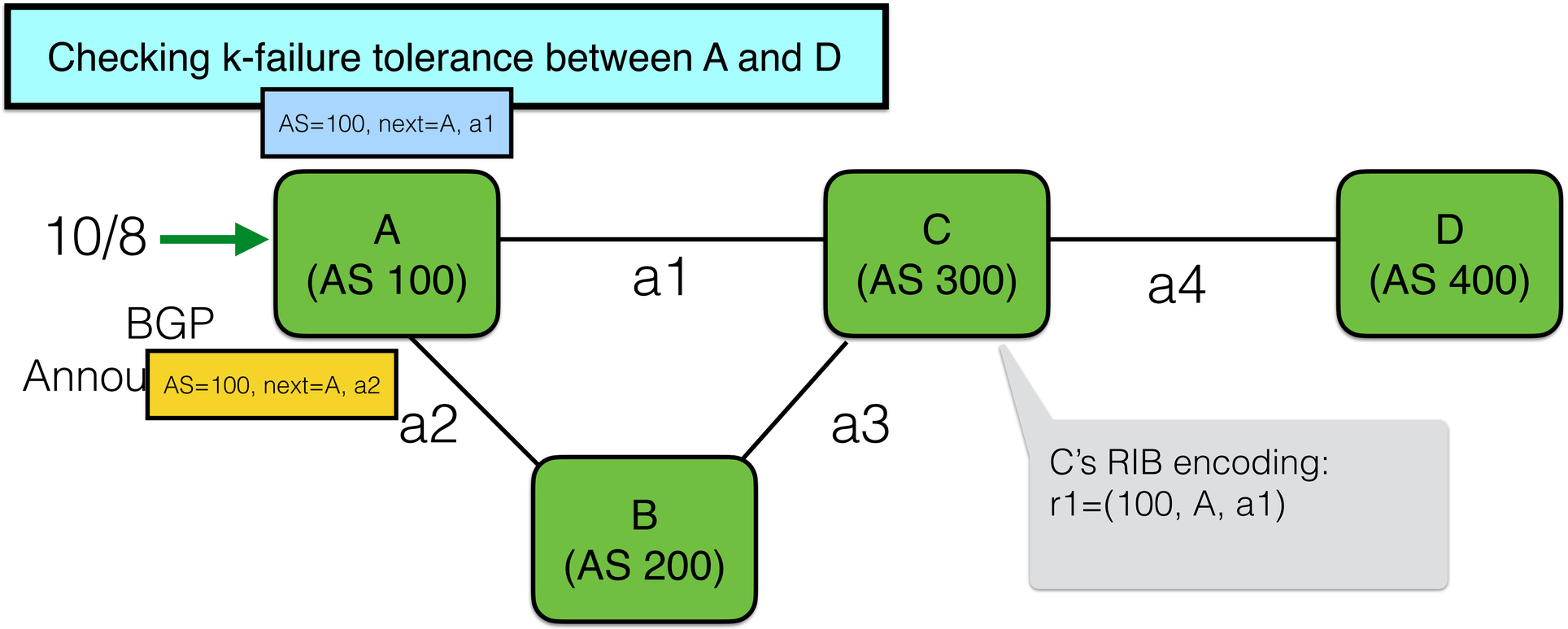


Global simulation & local formal-modeling

Checking k-failure tolerance between A and D

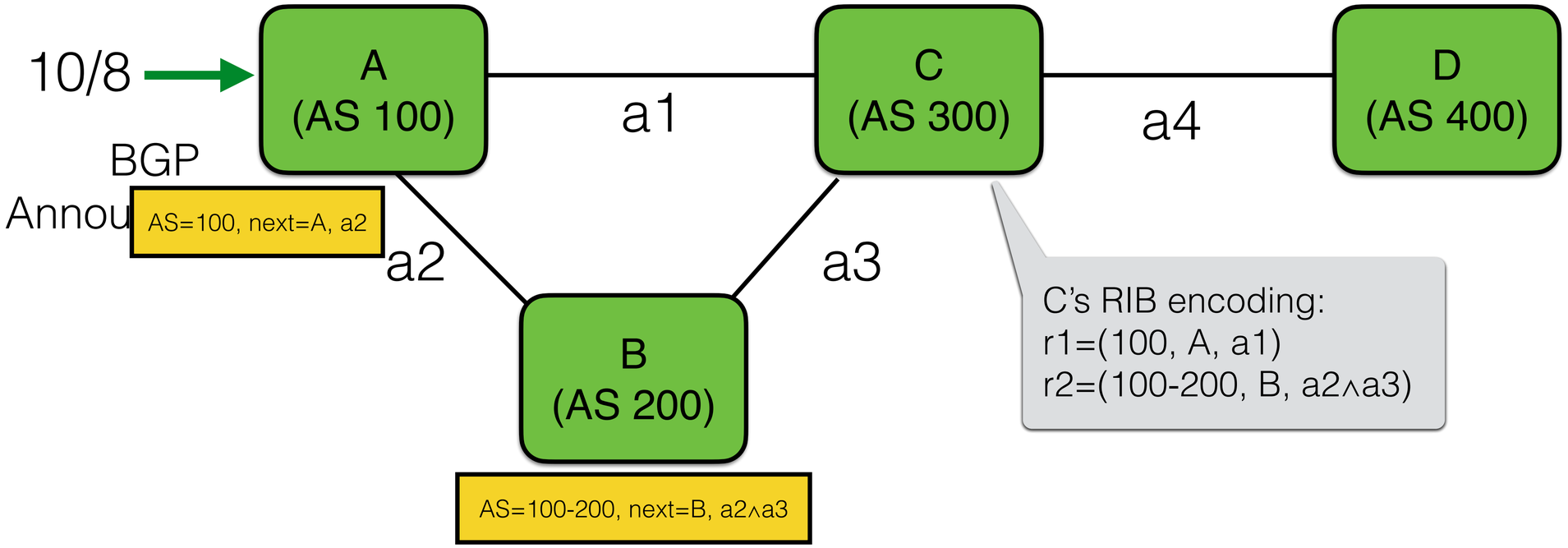


Global simulation & local formal-modeling

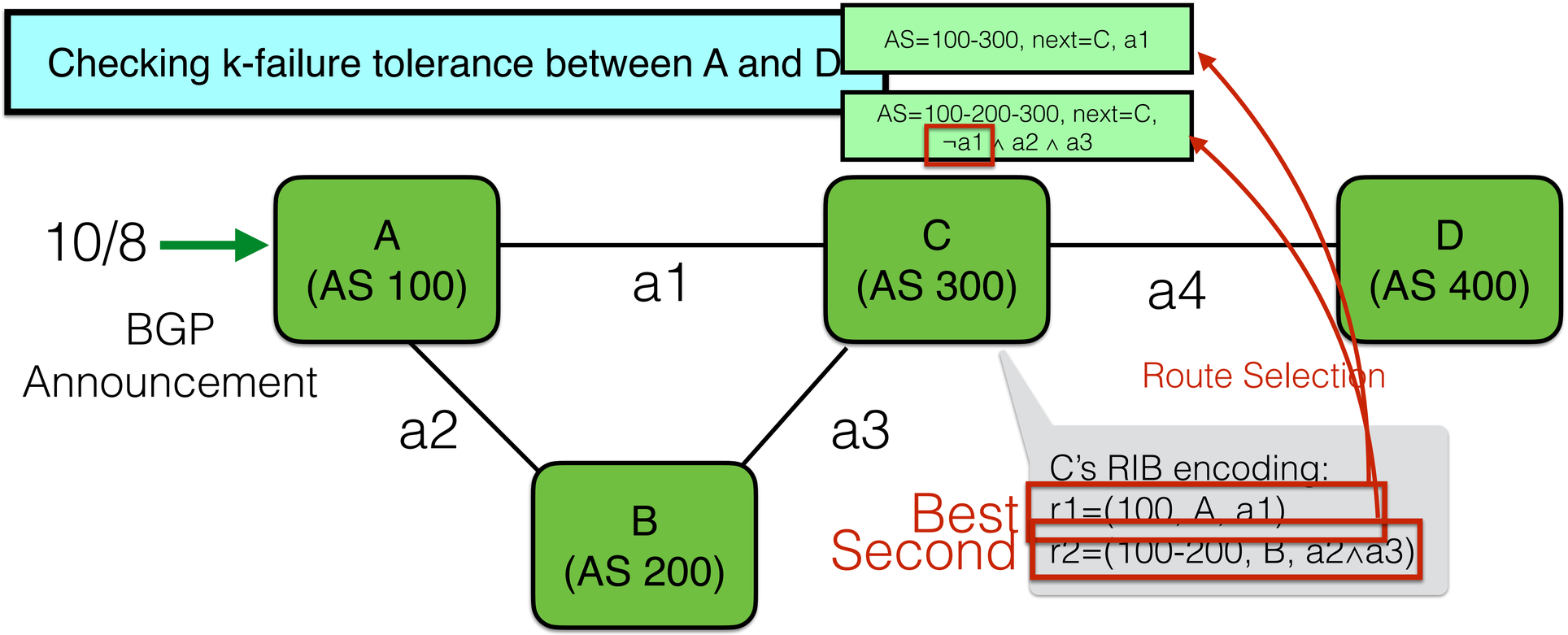


Global simulation & local formal-modeling

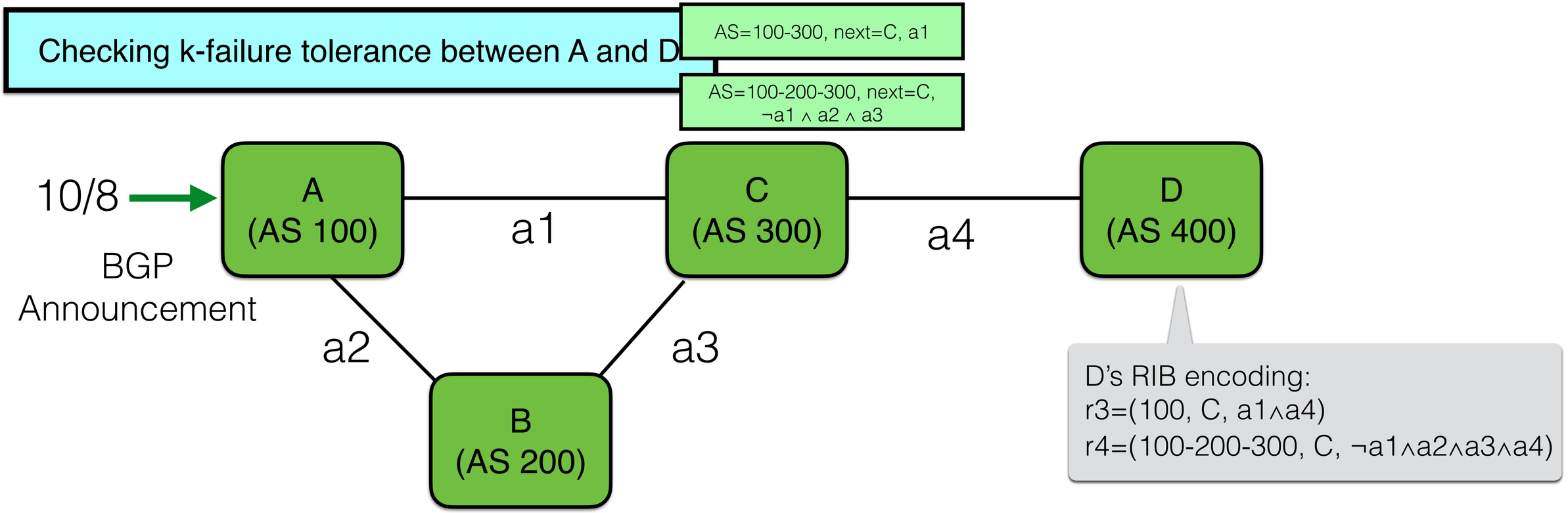
Checking k-failure tolerance between A and D



Global simulation & local formal-modeling

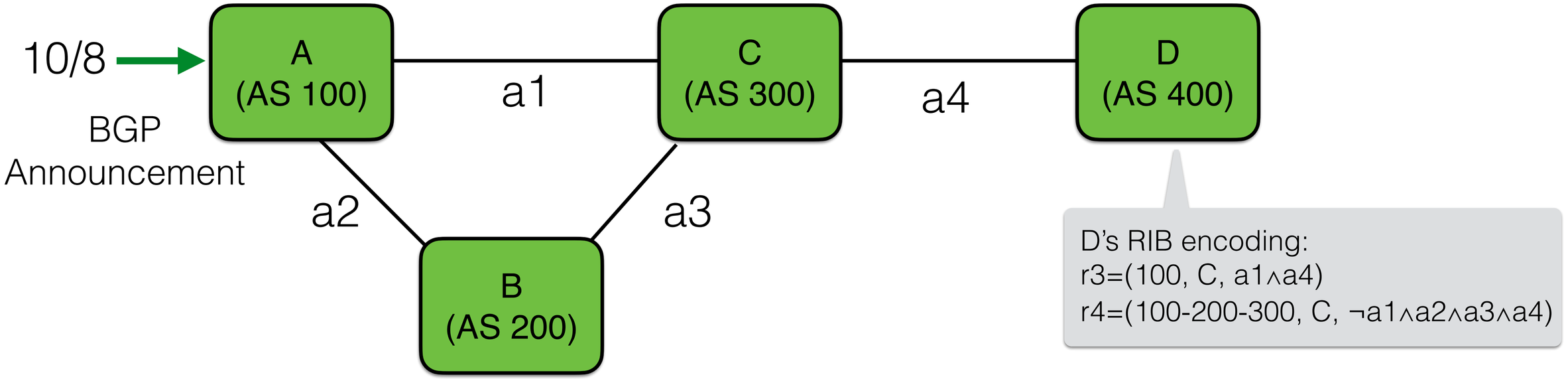


Global simulation & local formal-modeling



Global simulation & local formal-modeling

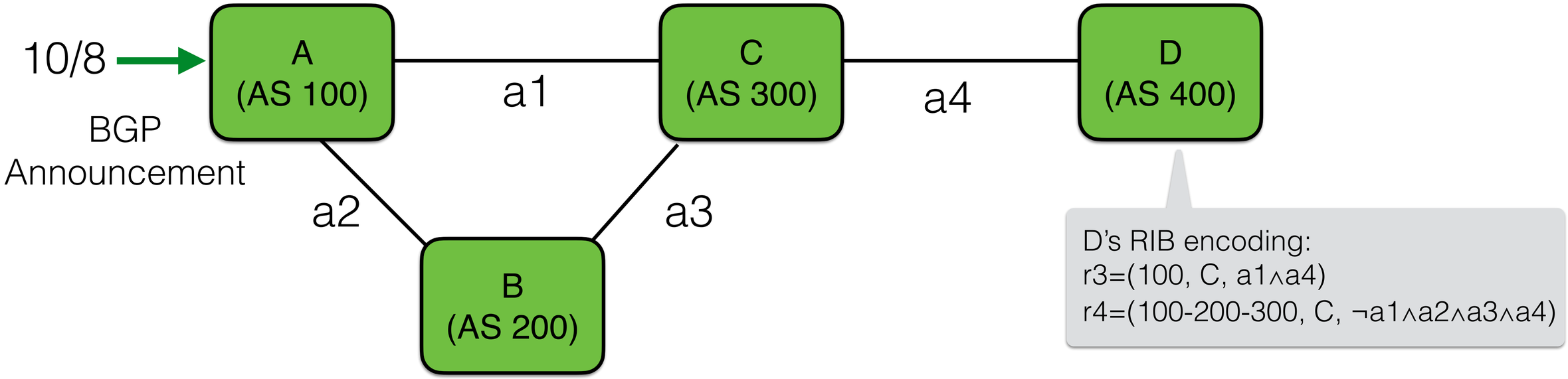
Checking k-failure tolerance between A and D



The local formula of "route of A reach D" is $(a1 \wedge a4) \vee (\neg a1 \wedge a2 \wedge a3 \wedge a4)$ ← $\neg a4$

Global simulation & local formal-modeling

Checking k-failure tolerance between A and D



The good scalability comes from:

- Dropping more than k cases
- Dropping impossible cases
- Simplifying logical formulas

Comparing Hoyan, Batfish and Minesweeper

A sub-network: 80 routers with thousands of lines of configurations

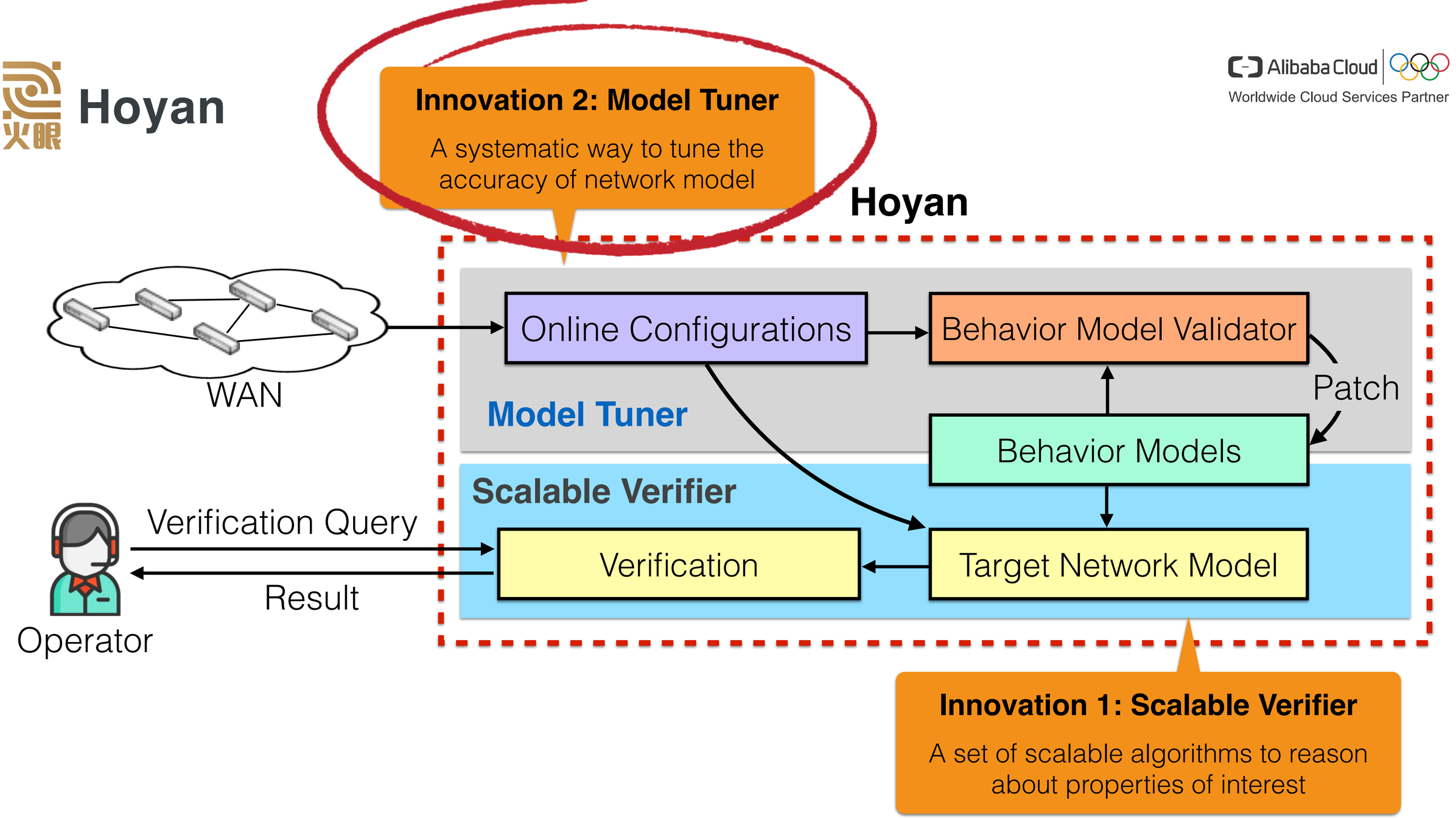
Network Properties		Hoyan	Minesweeper	Batfish
Reachability	k=0	14 seconds	84,043 seconds	683 seconds
	k=1	22 seconds	> 24 hours	> 24 hours
	k=2	43 seconds	> 24 hours	> 24 hours
	k=3	1176 seconds	> 24 hours	> 24 hours
Role Equivalence		4 seconds	> 24 hours	-

Hoyan

Alibaba Cloud
Worldwide Cloud Services Partner

Innovation 2: Model Tuner

A systematic way to tune the accuracy of network model



Innovation 1: Scalable Verifier

A set of scalable algorithms to reason about properties of interest

How to address the model faithfulness challenge?

Key insight:

- Using production network RIBs as a reference to debug simulated model

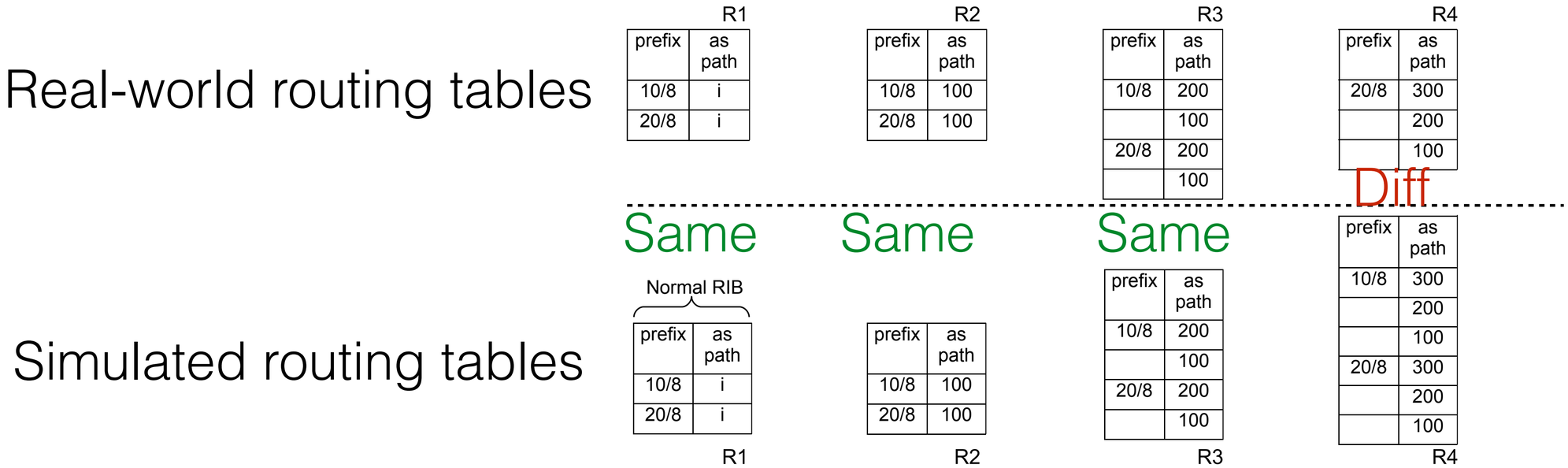
How to address the model faithfulness challenge?

Key insight:

- Using production network RIBs as a reference to debug simulated model

Strawman solution:

- Localizing vendor-specific behaviors by comparing real and simulated RIBs



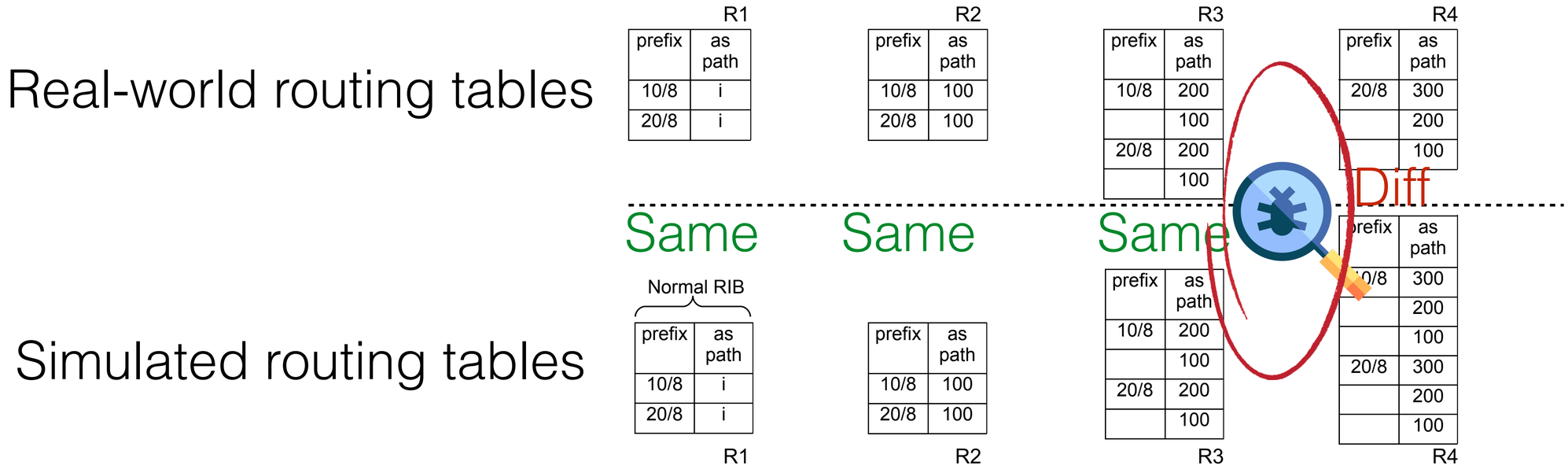
How to address the model faithfulness challenge?

Key insight:

- Using production network RIBs as a reference to debug simulated model

Strawman solution:

- Localizing vendor-specific behaviors by comparing real and simulated RIBs



How to address the model faithfulness challenge?

Key insight:

- Using production network RIBs as a reference to debug simulated model

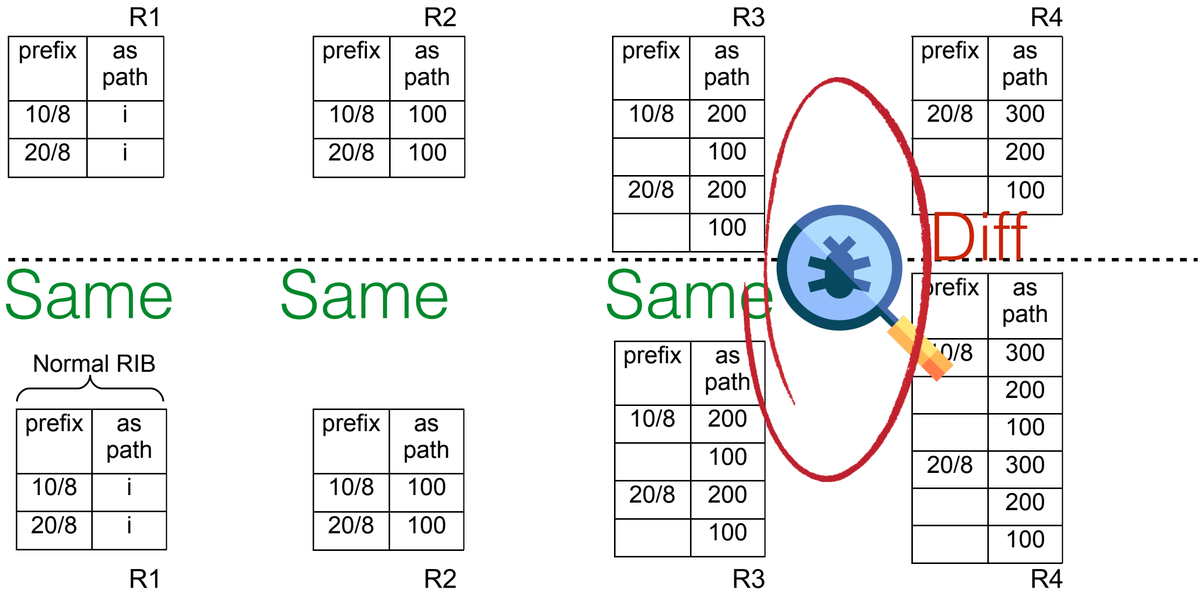
Strawman solution:

- Localizing vendor-specific behaviors by comparing real and simulated RIBs

Real-world routing tables

However, using normal RIBs cannot localize the correct VSBs!

Simulated routing tables



How to address the model faithfulness challenge?

Key insight:

- Using production network RIBs as a reference to debug simulated model

Our solution:

- Hoyan combines all the attributes of a route relevant for routing into an extended RIB
- The first mismatch between real and simulated ext-RIBs is vendor-specific behavior

Real-world routing tables

R1

prefix	as path	community
10/8	i	-
20/8	i	-

R2

prefix	as path	community
10/8	100	920
20/8	100	920

R3

prefix	as path	community
10/8	200	-
	100	-
20/8	200	920
	100	-

R4

prefix	as path	community
20/8	300	920
	200	-
	100	-

Simulated routing tables

Ext-RIB

Normal RIB

R1

prefix	as path	community
10/8	i	-
20/8	i	-

R2

prefix	as path	community
10/8	100	920
20/8	100	920

R3

prefix	as path	community
10/8	200	920
	100	-
20/8	200	920
	100	-

R4

prefix	as path	community
10/8	300	920
	200	-
	100	-
20/8	300	920
	200	-
	100	-

How to address the model faithfulness challenge?

Key insight:

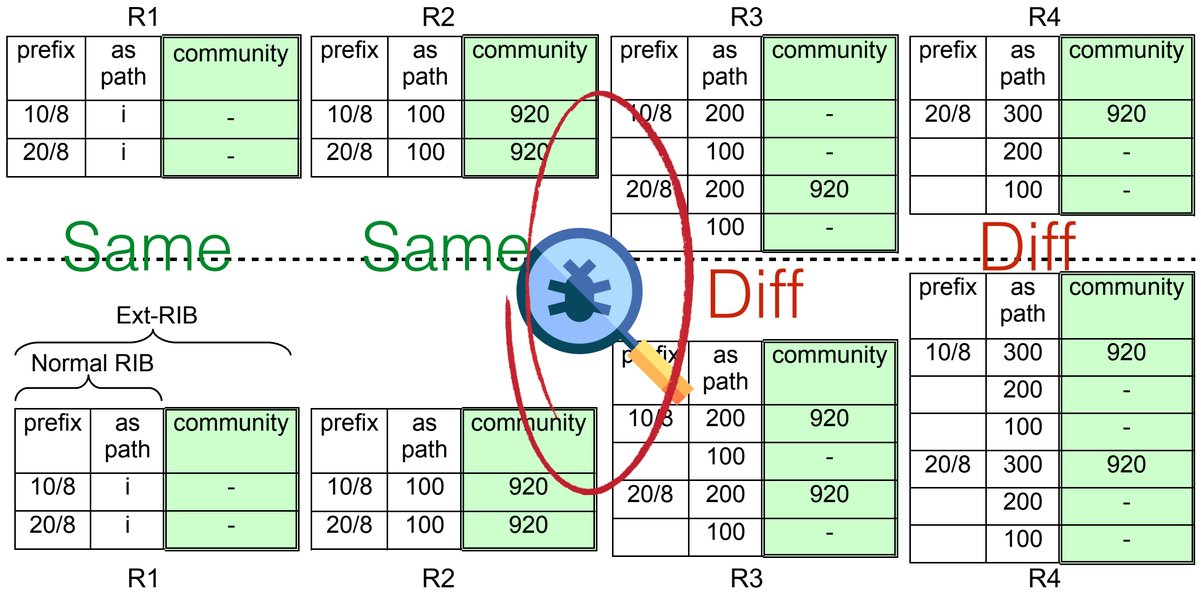
- Using production network RIBs as a reference to debug simulated model

Our solution:

- Hoyan combines all the attributes of a route relevant for routing into an extended RIB
- The first mismatch between real and simulated ext-RIBs is vendor-specific behavior

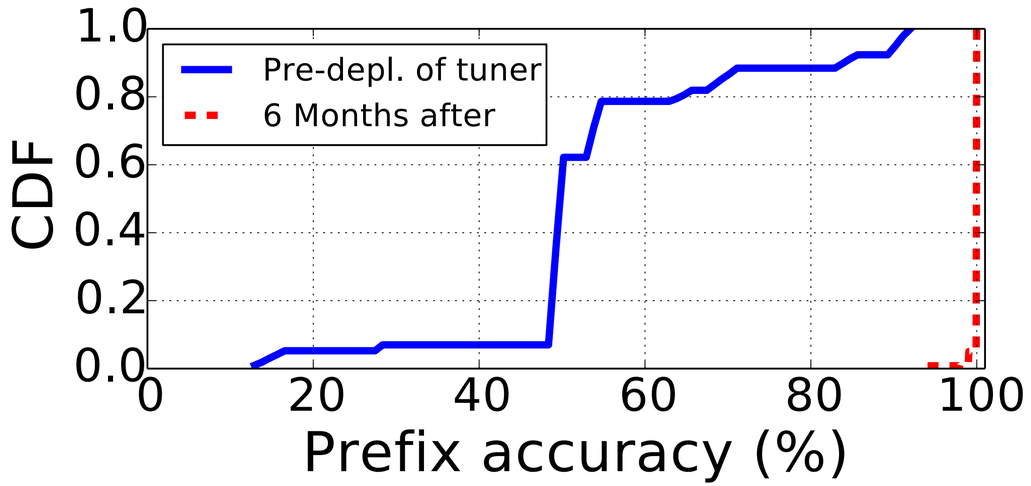
Real-world routing tables

Simulated routing tables



Device behavior model tuner

- Eight VSBs detected
  - Default ACL, route policy, removing private AS, etc.;
  - VSB localization within 10 lines of configuration



Hoyan: Deployment experience

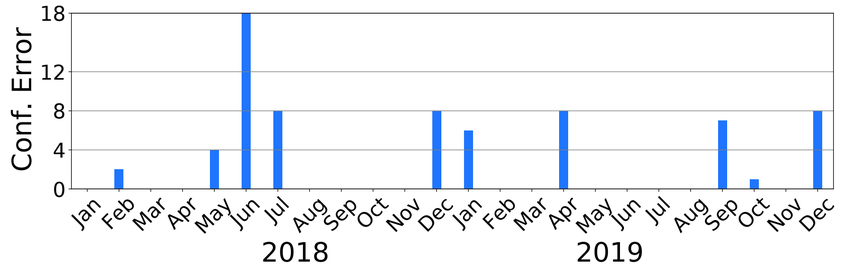
The overall rate of update-triggered network incidents was cut by more than half in the second year of Hoyan's deployment.

Hoyan: Deployment experience

Alibaba Cloud
Worldwide Cloud Services Partner

The overall rate of update-triggered network incidents was cut by more than half in the second year of Hoyan's deployment.

- Configuration auditing verification (Jan 2018 - Dec 2019)

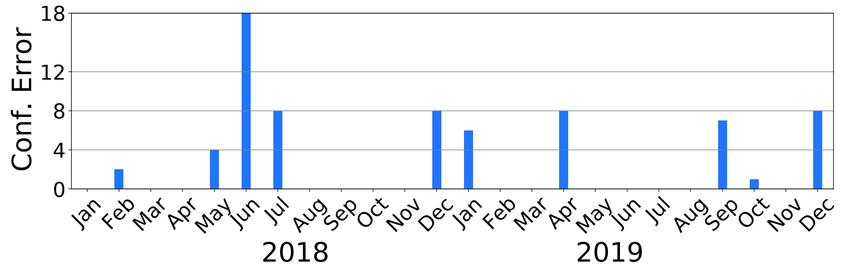


Hoyan: Deployment experience

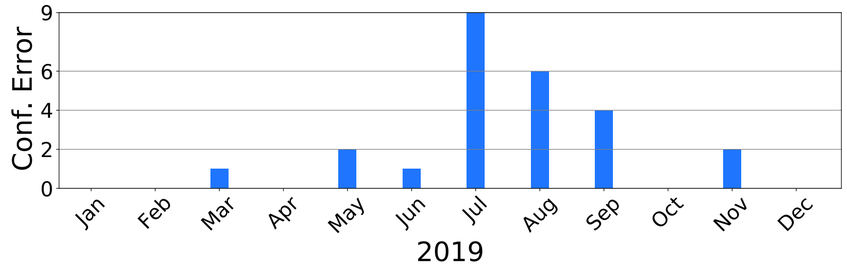
Alibaba Cloud
Worldwide Cloud Services Partner

The overall rate of update-triggered network incidents was cut by more than half in the second year of Hoyan's deployment.

- Configuration auditing verification (Jan 2018 - Dec 2019)



- Configuration update verification (Jan 2019 - Dec 2019)



Hoyan’s verification capability summary

Alibaba Cloud
Worldwide Cloud Services Partner

What protocols are covered by Hoyan?

- BGP (eBGP and iBGP), IGP (IS-IS and OSPF), static routes, route redistribution and ACL

Hoyan's verification capability summary

What protocols are covered by Hoyan?

- BGP (eBGP and iBGP), IGP (IS-IS and OSPF), static routes, route redistribution and ACL

What properties can Hoyan verify?

- Reachability (route and packet reachability)
- K-failure tolerance
- Non-deterministic routing update race
- Multipath consistency (equality)

目录

Our lessons and open questions

- Verification on WAN is more needed than DCNs
  - WAN is more complex than DCNs in routing policies and dependencies
  - WAN is not symmetric and configuration is not such “modular”
  - Tricky errors, e.g., non-deterministic issues

Our lessons and open questions

- Verification on WAN is more needed than DCNs
  - WAN is more complex than DCNs in routing policies and dependencies
  - WAN is not symmetric and configuration is not such “modular”
  - Tricky errors, e.g., non-deterministic issues

- Expressing intent and intent extraction
  - Multiple security domains and implicit business needs
  - Does example-based specification help? e.g., example spec verification or synthesis

Our lessons and open questions

- Misconfiguration repairing
  - There are multiple ways to repair a misconfiguration. Which one is the best?
  - How to avoid side effects, i.e., new problems after fixing the target bug?
  - How to express the fixing purpose?

Our lessons and open questions

- Misconfiguration repairing
  - There are multiple ways to repair a misconfiguration. Which one is the best?
  - How to avoid side effects, i.e., new problems after fixing the target bug?
  - How to express the fixing purpose?

- Vendor diversity
  - Vendor diversity can prevent cascading failures
  - How to quantify diversity? How to detect my network diversity is low?
  - Can we transform a “non-diverse” network to a diverse network?

集中式网络规划体系

设计　交付　变更　运维

程序怎么写？（语言设计）

属性描述（语言设计）

运维描述程序/脚本

配置的生成（synthesis）

核心算法（例如，验证或生成算法）

变更生成（synthesis）

网络模型（网络行为抽象）

配置解析（屏蔽厂商细节）

不同厂商的设备

THANKS