
VNNIC-2023
Technical Workshop -
Advanced Routing Security
29 June 2023
Binh Lam - NTT

Cautions and Legal Disclaimer

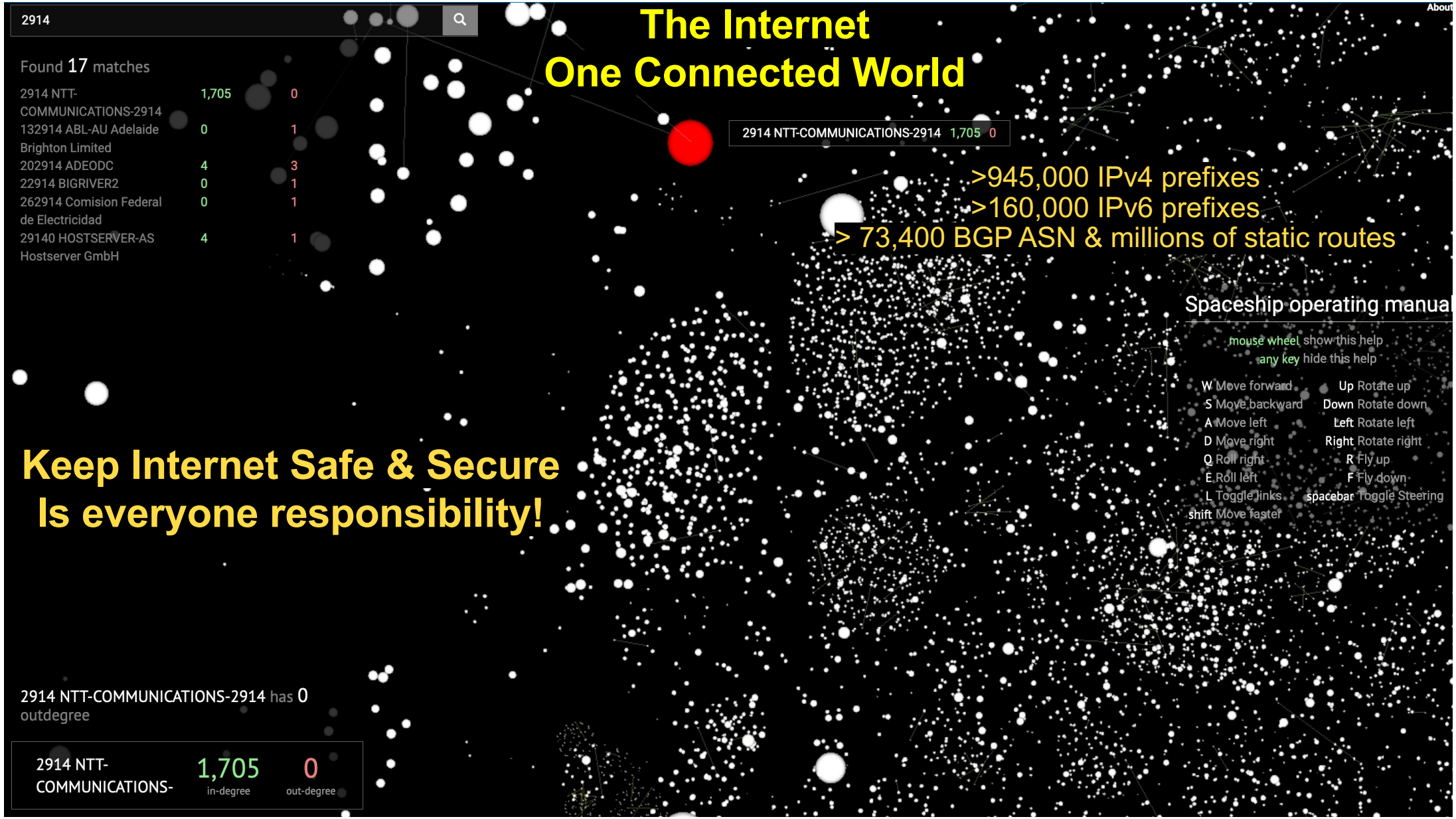
This workshop aims to educate about routing security and attack surface, with the tools and techniques discussed intended for ethical, responsible use only.

Participants must not engage in illegal activities, such as unauthorized access to computer systems or networks. Any actions taken based on workshop information are the sole responsibility of participants, and the facilitators and organizers will not be liable for any misuse or illegal actions.

By attending this workshop, you agree to uphold ethical standards and abide by all laws and regulations. We urge you to use your new knowledge responsibly, contributing positively to routing security.

Please consult the facilitators if you have any questions or concerns. Unethical actions or law violations may lead to severe legal consequences. Act responsibly, aware of your legal obligations.
We appreciate your understanding and cooperation.

whoami


2914
Found 17 matches
2914 NTT-COMMUNICATIONS-2914 1,705 0
132914 ABL-AU Adelaide Brighton Limited 0 1
202914 ADEODC 4 3
22914 BIGRIVER2 0 1
262914 Comision Federal de Electricidad 0 1
29140 HOSTSERVER-AS Hostserver GmbH 4 1
The Internet
One Connected World
2914 NTT-COMMUNICATIONS-2914 1,705 0
>945,000 IPv4 prefixes
>160,000 IPv6 prefixes
> 73,400 BGP ASN & millions of static routes
About
Spaceship operating manual
mouse wheel show this help
any key hide this help
W Move forward
S Move backward
A Move left
D Move right
Q Roll right
E Roll left
L Toggle links
shift Move faster
Up Rotate up
Down Rotate down
Left Rotate left
Right Rotate right
R Fly up
F Fly down
spacebar Toggle Steering
Keep Internet Safe & Secure
Is everyone responsibility!
2914 NTT-COMMUNICATIONS-2914 has 0 outdegree
2914 NTT-COMMUNICATIONS- 1,705 in-degree 0 out-degree

Topics

01

Identify Security Risks and Attack Surface

- Understanding Pen-testing phrases
- Understanding Vulnerability DB
- Security Risks in Core Routing Infrastructure Infrastructure
- Hands-on: Open port and Vulns Scan

02

Reduce Attack Surface

- How to Reduce Attack Surface & Protect Core Infrastructure

03

Robust Secure Routing Policies

- Identify Routing Security Flaws: Route Hijack Cases, Route Leak Cases
- What was missing?
- Lab: eBGP route leak demo
- Applying advanced Route Filter Technique

04

Tools

- BGPq4 ACL build
- Setup Route Hijack BGP Alerter

What to expect in this workshop?

01. Identify Security Threats and Attack Surfaces

Pen-Testing Approach

A systematic and controlled approach to assess the security of a system or network by simulating real-world attacks.

Pen-Testing Approach:

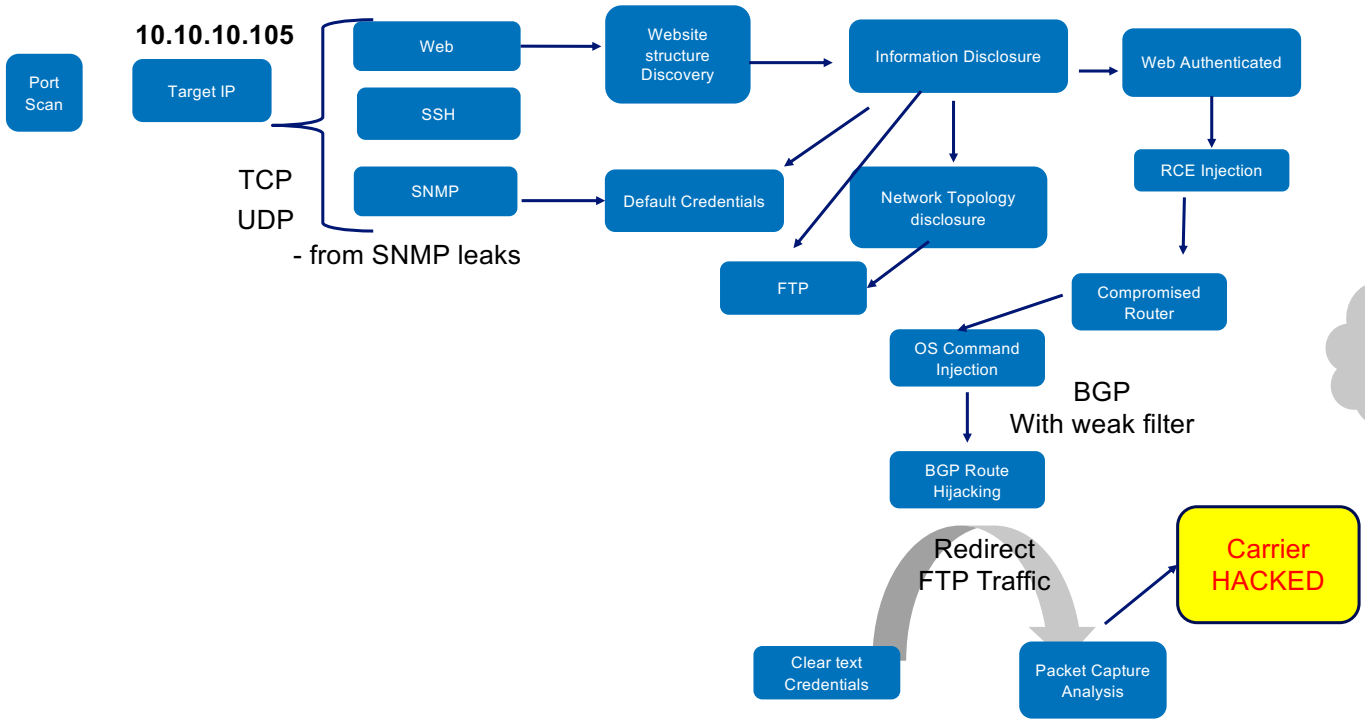
- Planning and Preparation:
  - Define objectives, scope, and rules of engagement.
  - Obtain proper authorization and permissions.
  - Gather information about the target system or network.
- Reconnaissance:
  - Collect publicly available information about the target.
  - Identify potential vulnerabilities and entry points.
- Scanning and Enumeration:
  - Utilize tools to identify open ports, services, and vulnerabilities.
  - Enumerate system details, such as user accounts and network configurations.
- Exploitation:
  - Attempt to exploit identified vulnerabilities to gain unauthorized access.
  - Test for common attack vectors, such as injection attacks or misconfigurations.
- Post-Exploitation:
  - Assess the extent of the compromise and potential impact.
  - Pivot within the network to escalate privileges or gain further access.
- Reporting and Recommendations:
  - Document findings, including vulnerabilities, exploitation details, and potential impact.
  - Provide actionable recommendations for remediation and improved security.

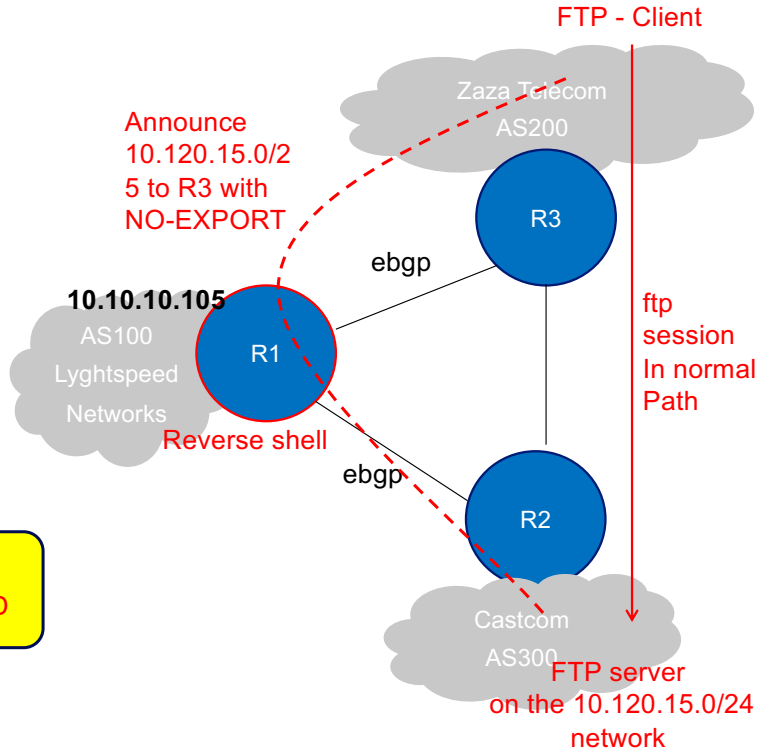
Hacking phrases

Common Pen-Testing Phrases:

- Vulnerability Assessment: Identifying and classifying vulnerabilities in a system or network.
- Exploitation Framework: A collection of tools and techniques used to exploit vulnerabilities.
- Privilege Escalation: Gaining higher levels of access beyond the initially compromised account or system.
- Pivoting: Moving laterally within a network to explore and exploit other systems or resources.
- Social Engineering Testing: Evaluating the effectiveness of security controls against social manipulation techniques.

From the Lab — Hacking “Carrier”





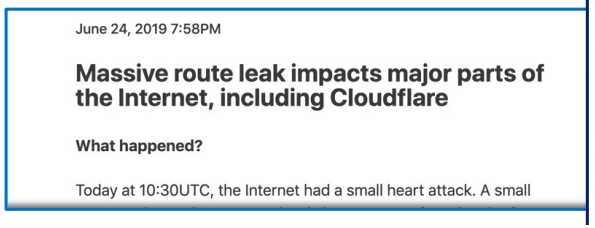
HackTheBox

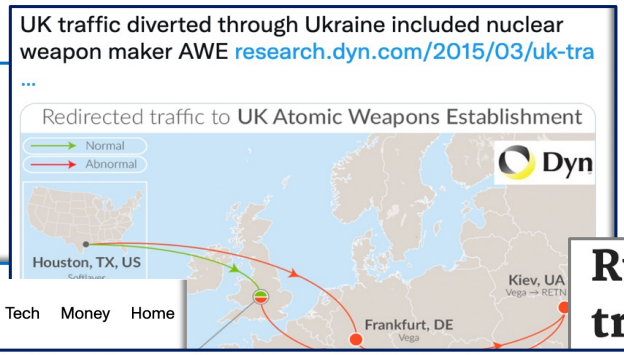
https://snowscan.io/htb-writeup-carrier/#

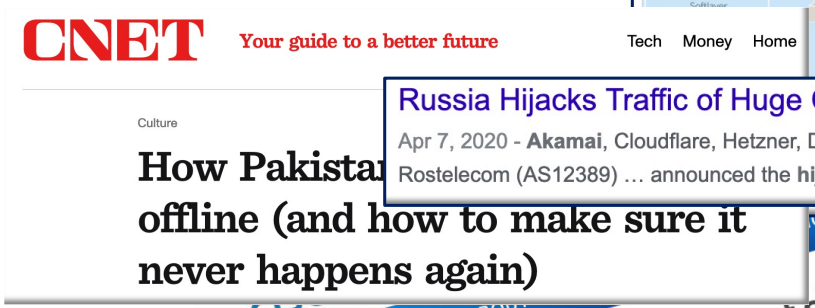
Common Attacks: BGP Route Leaks and Hijacking on the News

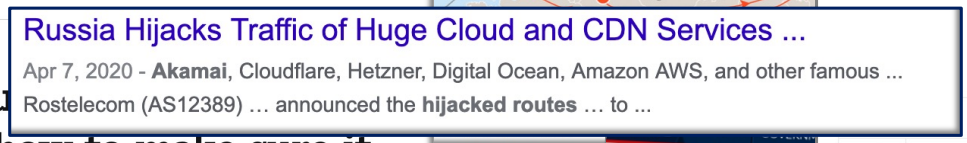
Route Hijacking:
- AS announces prefix it doesn't own to originate
- AS announces more specific prefix than what is being seen in DFZ originating from actual owner
- Packets end-up being forwarded to a wrong path of Internet

Result in: Denial-of-Service, traffic interception, or impersonating network or service









Hacking in the Real world

Y2014
BGP Route Hijack

wired.com/2014/08/isp-bitcoin-theft/

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY SIGN IN SUBSCRIBE

ANDY GREENBERG SECURITY AUG 7, 2014 1:00 PM

Hacker Redirects Traffic From 19 Internet Providers to Steal Bitcoins

Among all the scams and thievery in the bitcoin economy, one recent hack sets a new bar for brazenness: Stealing an entire chunk of raw internet traffic from more than a dozen internet service providers, then shaking it down for as many bitcoins as possible. Researchers at Dell's SecureWorks security division say they've uncovered a [...]

Y2022

KLAYSWAP|KLAYSWAP-BGP-HIJACK

Catalin Cimpanu | February 14th, 2022

KlaySwap crypto users lose funds after BGP hijack

Hackers have stolen roughly $1.9 million from South Korean cryptocurrency platform KLAYswap after they pulled off a rare and clever BGP hijack against the server infrastructure of one of the platform's providers.

The BGP hijack—which is the equivalent of hackers hijacking internet routes to bring users on malicious sites instead of legitimate ones—hit KakaoTalk, an instant messaging platform popular in South Korea.

The attack took place earlier this month, on February 3, lasted only for two hours, and KLAYswap has confirmed the incident last week and is currently issuing compensation for affected users.

BGP Hijack+ Getting More Sophisticated

25/4/2018

The Amazon Route 53 BGP Hijack to Take Over Ethereum Cryptocurrency Wallets

- BGP route hijack the prefixes where Route53 hosted
- Re-routing of Amazon's Route 53 DNS traffic towards a malicious DNS server
- User tried to access myetherwallet.com was pointed to phishing site
- Bad-Actor – Man-in-the-Middle attack
- The attackers managed to steal about $150,000 of currency from MyEtherWallet users

Amazon officials wrote: "**Neither AWS nor Amazon Route 53 were hacked or compromised.** An upstream Internet Service Provider (ISP) was compromised by a malicious actor who then used that provider to announce a subset of Route 53 IP addresses to other networks with whom this ISP was peered. These peered networks, unaware of this issue, accepted these announcements and incorrectly directed a small percentage of traffic for a single customer's domain to the malicious copy of that domain."

August 18, 2022

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

BORDER GATEWAY PROTOCOL INSECURITY —

How 3 hours of inaction from Amazon cost cryptocurrency holders $235,000

For 2nd time in 4 years, Amazon loses control of its IP space in BGP hijacking.

DAN GOODIN - 9/24/2022, 4:04 AM

The hijacked block included 44.235.216.69, an IP address hosting cbridge-prod2.celer.network, a subdomain responsible for serving a critical smart contract user interface for the Celer Bridge cryptocurrency exchange.

```
route:          44.224.0.0/11
origin:         AS16509
descr:          Amazon EC2 PDX prefix
mnt-by:         MAINT-AS16509
changed:        noc@amazon.com 20190801  #21:11:46Z
source:         RADB
rpki-ov-state:  valid


route:          44.224.0.0/11
descr:          RPKI ROA for 44.224.0.0/11 / AS16509
remarks:        This AS16509 route object represents routing data retrieved
                from the RPKI. This route object is the result of an automated
                RPKI-to-IRR conversion process performed by IRRd.
max-length:     24
origin:         AS16509
source:         RPKI  # Trust Anchor: arin


route:          44.235.216.0/24
origin:         AS16509
descr:          Amazon EC2 PDX prefix
mnt-by:         MAINT-AS16509
changed:        noc@amazon.com 20230316  #02:01:04Z
source:         RADB
rpki-ov-state:  valid
```

https://arstechnica.com/information-technology/2022/09/how-3-hours-of-inaction-from-amazon-cost-cryptocurrency-holders-235000/

Government Agency – Security Alerts

https://techcrunch.com/2022/11/07/uk-government-zero-day-scans/

Security

UK government is scanning British internet space for zero-day threats

Carly Page @carlypage_ / 12:45 AM GMT+11 • November 8, 2022 Comment

The United Kingdom's National Cyber Security Centre (NCSC), the government agency that leads the country's cyber security mission, is now ***scanning all Internet-exposed devices hosted in the UK for vulnerabilities.*** *The goal is to assess UK's vulnerability to cyber-attacks and to help the owners of Internet-connected systems understand their security posture.*

Vulnerability Database

Vulnerability Database

https://vuldb.com

https://www.cve.org/

CVE Details https://www.cvedetails.com/
The ultimate security vulnerability datasource

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

EXPLOIT DATABASE

https://www.exploit-db.com/

CVE-2023-33299: Critical Remote Code Execution Vulnerability in FortiNAC

On June 23, Fortinet published an advisory (FG-IR-23-074) that addresses a critical remote code execution vulnerability in FortiNAC, its Network Access Control solution:

CVE	Description	CVSSv3 *	Severity
CVE-2023-33299	Fortinet ForitNAC deserialization of untrusted data vulnerability	9.6	Critical

If exploited, the attacker can gain complete control of a user's account, including access to private customer data and sensitive information,"

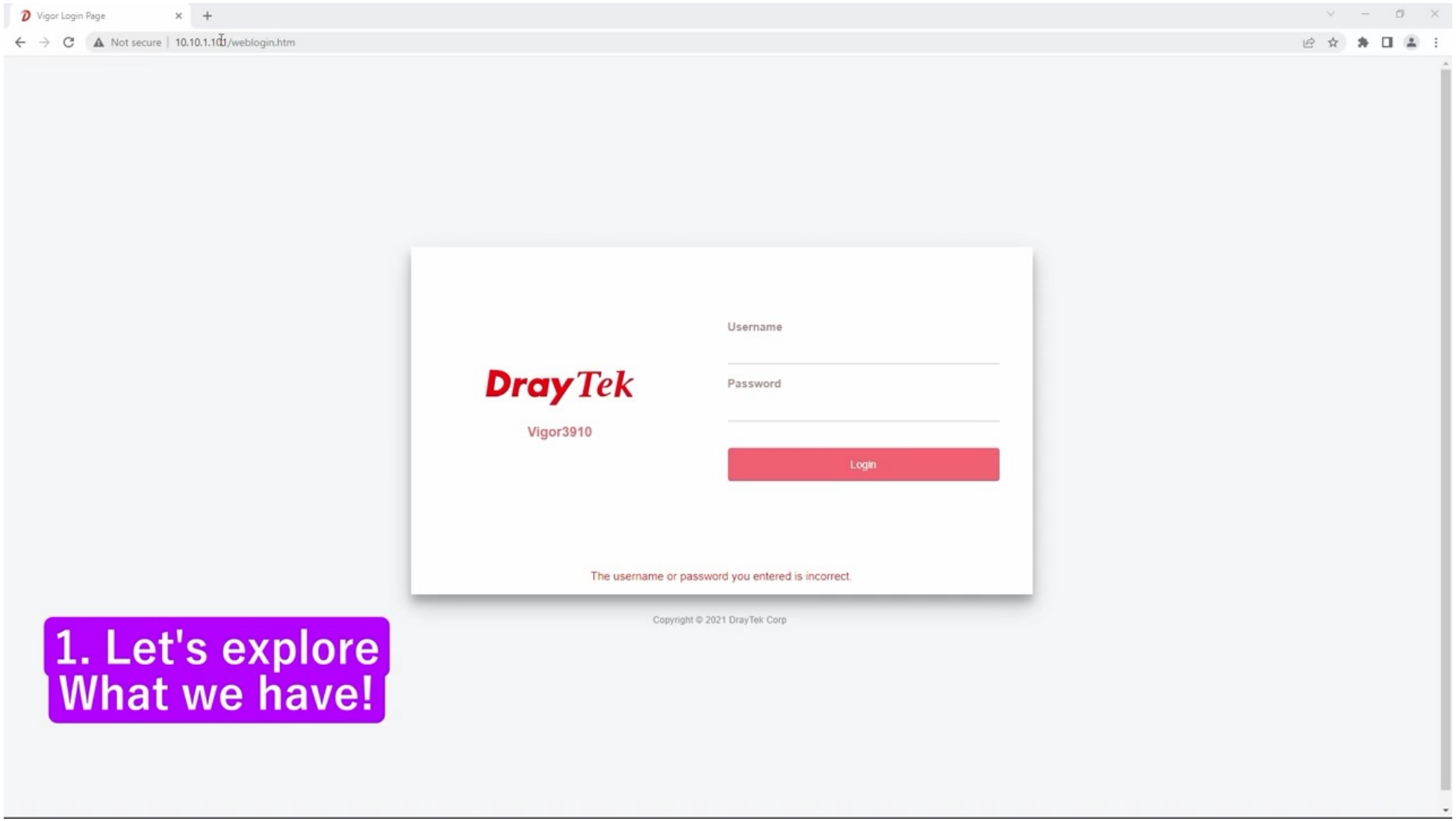
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33299
https://nvd.nist.gov/vuln/detail/CVE-2023-33299
https://www.bleepingcomputer.com/news/security/fortinet-fixes-critical-fortinac-remote-command-execution-flaw/

* The Common Vulnerability Scoring System version 3 (CVSSv3) is a set of open standards used to assess the severity of computer system security vulnerabilities.

DrayTek Router Vulnerability (CVE-2022-32548)

Successfully exploiting the vulnerability may lead to the following outcomes :

- Leaking sensitive data stored on the router such as credential keys, admin passwords
- Access to the internal systems, services and resources located in your internal network that would normally require VPN-access or be present “on the same network”
- Ransomware
- Data theft (e.g. credentials, intellectual property, personal or financial information)
- Spying on website traffic requests and other unencrypted traffic sent to the internet from your network through the router (known as Man-In-The-Middle attacks)
- Being used as part of a criminal network for ‘botnet’ activity (such hosting malicious data, attacking other IP addresses, denying services to other organisations


Vigor Login Page
Not secure | 10.10.1.1/weblogin.htm
DrayTek
Vigor3910
Username
Password
Login
The username or password you entered is incorrect.
Copyright © 2021 DrayTek Corp
1. Let's explore
What we have!

Live -

Risk Exposure to Public Internet

Security Risks To Core Routing Infrastructure

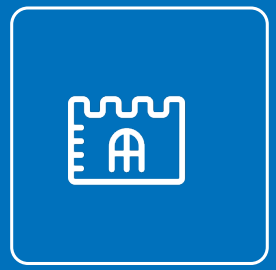
Security Risks in Core Routing Infrastructure

Unauthorized Access

Unauthorized access to network equipment, allowing malicious actors to gain control of the network

Route Leaks and Hijacks

Unauthorized access to routing information, allowing malicious actors to redirect traffic away from its intended destination



DDoS Attacks

Distributed Denial of Service attacks targeting critical network infrastructure, resulting in service disruption

Understanding the security risks associated with core routing infrastructure is essential for ISPs to ensure the safety and integrity of their networks.

Attack Surface: The Common Open Network Port Threats

We should basically assume that **any open port** on a network device **will become exploitable at some point** due either to a bug in the firmware, a misconfiguration, or a leaked or back door password.

- **Port 20 and 21 (FTP)**

  Known for being outdated and insecure, attackers frequently exploit it through brute-forcing passwords, anonymous authentication, cross-site scripting, and directory traversal attacks

- **Port 22 (SSH)**

  Secure Shell (SSH) is a TCP port for ensuring secure access to servers. Hackers can exploit port 22 by using leaked SSH keys or brute-forcing credentials

- **Port 23 (Telnet)**

  Telnet is a TCP protocol that connects users to remote computers. It is vulnerable to credential brute-forcing, spoofing and credential sniffing.

- **Port 25 (SMTP)**

  Simple Mail Transfer Protocol (SMTP) port for receiving and sending emails. Vulnerable to spoofing and spamming.

- **Port 53 (DNS)**

  Domain Name System (DNS) is a UDP and TCP port for queries and transfers, respectively. Vulnerable to DDoS attacks.

- **Ports 137 and 139 (NetBIOS over TCP) and 445 (SMB)**

  Server Message Block (SMB) uses port 445 directly and ports 137 and 139 indirectly. Vulnerable to EternalBlue exploit, capturing NTLM hashes, and brute-forcing SMB login credentials

- **Ports 80, 443, 8080 and 8443 (HTTP and HTTPS)**

  Vulnerable to cross-site scripting, SQL injections, cross-site request forgeries and DDoS attacks.

- **Ports 1433,1434 and 3306 (Used by Databases)**

  Used to distribute malware or are directly attacked in DDoS scenarios. Attackers probe these ports to find unprotected databases with exploitable default configurations

- **Port 3389 (Remote Desktop)**

  Used in conjunction with various vulnerabilities in remote desktop protocols and to probe for leaked or weak user authentication.

Commonly Targeted Ports in DDoS Attacks

UDP Flood Attacks

UDP Flood Attacks target ports 53, 123, 161, 1900, 5060, and 506

TCP SYN Flood Attacks

TCP SYN Flood Attacks target ports 80, 443, 3389, 22, 23, 25, 1433, 3306, and 808

ICMP Flood Attacks

ICMP Flood Attacks do not target specific ports as they operate at the network laye

HTTP Flood Attacks

HTTP Flood Attacks target ports 80 and 443

DDoS attacks can target various ports depending on the attack vector and the vulnerabilities present in the target system. It is important to be aware of the different types of DDoS attacks and the ports they target in order to protect your system from malicious activity

Hands-on :

Audit the open ports to the internet!!!

Helps you gain visibility into any potential network issues, allowing them to be rectified before causing downtime or impacting business performance.

Tools To Find Open Ports: Shodan & NMAP

Shodan Search Engine

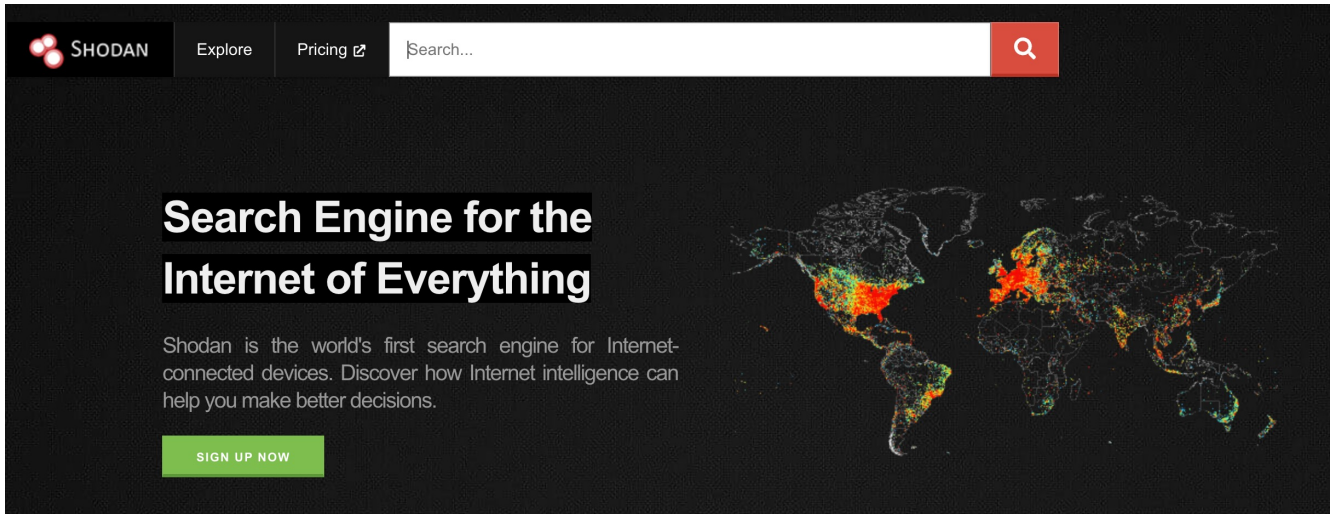
Allows users to search for specific ports and services on devices across the internet

Nmap Port Scanning

Widely used open-source network scanning tool to identify open ports on target systems

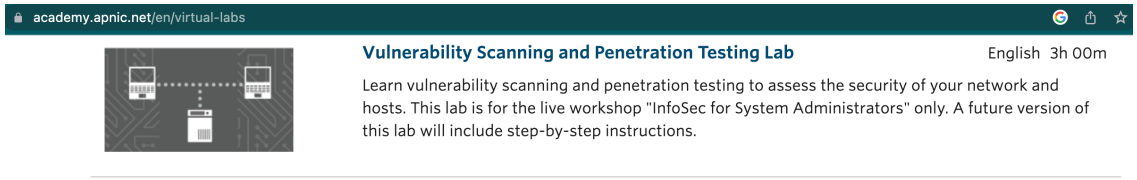
By utilizing the tools discussed in this slide, organizations can identify and address security vulnerabilities in their networks. It is important to ensure that proper authorization is obtained, and legal and ethical guidelines are followed when conducting port scans.

Passive Search: Shodan Search Engine Demo



Active Scan tool: NMAP

Homework: Further Lab resource:
https://academy.apnic.net/en/virtual-labs

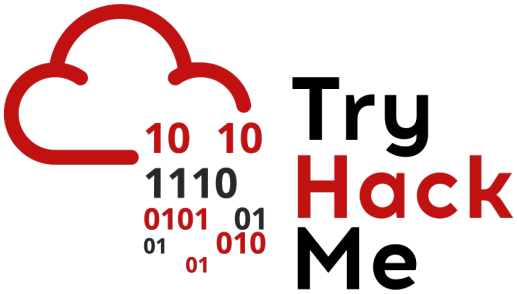


NMAP References

- https://linux.die.net/man/1/nmap
- https://nmap.org/
- https://wiki.onap.org/display/DW/Nmap

Further Study: To protect, learn the hacking technique

- Information gathering
- Vulnerability assessments and analysis
- DNS enumeration
- Service enumeration (SNMP, FTP, HTTP, SMB and a lot more)
- Port scanning
- Manual and automated vulnerability scanning
- Compiling Linux and Windows exploits
- How to work with exploits
- Web application hacking (SQL injection, Remote code Execution, local file inclusion, file upload vulnerabilities etc.)
- Privilege escalation techniques on Windows and Linux
- Password and hash attacks
- Metasploit
- And many more subjects…



https://tryhackme.com

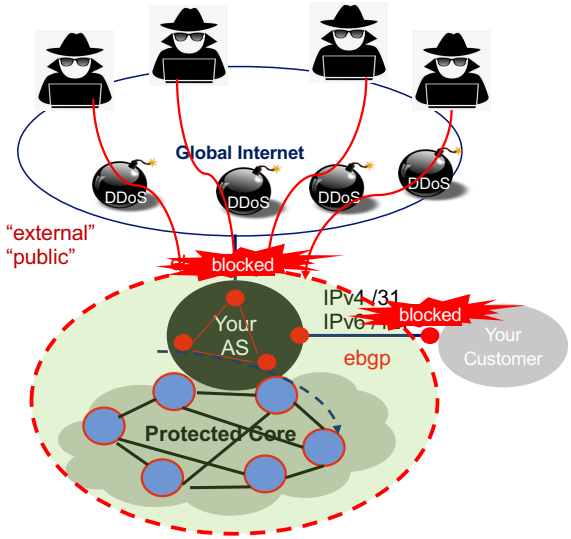
02. How To Reduce Attack Surface

Securing Ports: Best Practices for Reducing Threat Exposure

- **Limit Exposed Information**
  Conceal specifics such as software version or operating system to reduce your visibility to potential attackers.
- **Identify Open Ports & Restrict Port Access:**
  Monitor changes and document usage to create a baseline for port security. Limit access to essential IP addresses or ranges from known source
- **Disable Unused Services and Ports**
  Unless vital for operation, unnecessary open ports should be closed to reduce exposure.
- **Ingress and Egress Filtering ACL:**
  Implement ingress and egress filtering on your edge routers to prevent spoofing and DoS attacks.
- **Address Known Vulnerabilities**
  Prioritize known vulnerabilities, especially on exposed systems, to prevent exploits.
- **Secure SNMP:**
  If you are using SNMP for management, use SNMPv3 and ensure that it is configured securely filtering, and RPKI.
- **Implement BGP Security Practices:**
  Implement BGP security practices such as prefix filtering, AS path filtering, and RPKI. PLUS Reject Transit Leaks
- **Rate Limiting:**
  Implement rate limiting to prevent your router's resources from being exhausted by an attack.
- **Use Strong Authentication and Encryption:**
  For all administrative access, strong authentication methods such as two-factor authentication should be implemented. Also, ensure that all connections are encrypted (SSH instead of Telnet, for example).
- **Use VPN for Remote Access:**
  If you require remote access to the router, use a secure VPN connection.

Protecting and Securing Core Infrastructure Resources with ACLs

- Review network infrastructure and topology
  - Determine specific requirements for ACLs
- Filter in source, destination IP addresses, protocols, and port ranges
  - Assign a remark to each entry to describe its purpose or function
- Organize entries logically
  - Align with security policies
- Test ACL rules thoroughly
  - Before implementing in network
- Periodically review and update ACLs
  - Adapt to changes in network environment or security needs



Securing Your Network Through Access Control List

- Deny Bogon Source IP
  Prevent traffic from IP addresses that are not officially assigned to any organization
- Deny from Specific Source IP
  Prevent traffic from specific IP addresses or networks
- Deny to Specific Destination IP
  Prevent traffic to specific IP addresses or networks
- Allow BGP Neighbor IP
  Allow traffic from BGP neighbors for routing purposes
- Deny to BGP Linknet IP
  Prevent traffic to BGP linknets for routing purposes
- Allow to Management Plane IP
  Allow traffic to the management plane for administrative purposes
- Deny to Management Plane IP
  Prevent traffic to the management plane for administrative purposes
- Allow Trusted External to Internal Infra IP
  Allow trusted external sources access to internal infrastructure resources
- Deny to Internal Infra IP
  Prevent access to internal infrastructure resources from untrusted sources
- Limit Amplifiers IP
  Limit the use of amplifiers in order to prevent amplification attacks
- Allow Any

1. Netflow for Security Purposes

Netflow Analysis tool - Have ability to analyse traffic.

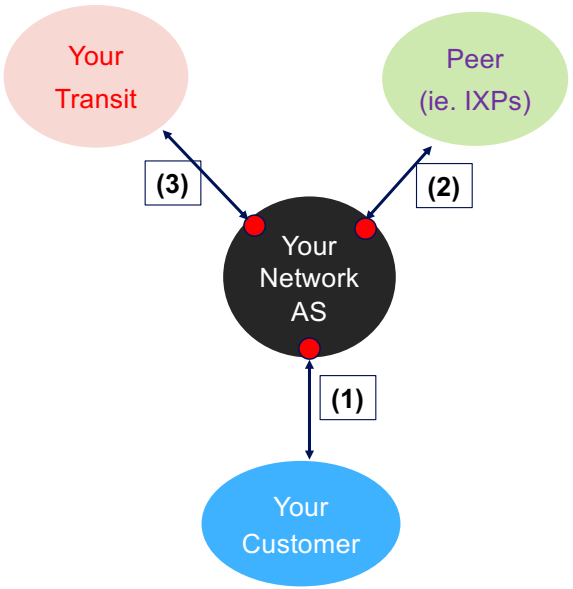
Who , What, Where, When , How

Predefined filter for known ddos attacks

Live attacks

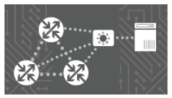
Traffic Profiles	Filter Rule
Live-udp-443	proto udp and port 443
live-chargen	proto udp and src port 19
live-LDAP	proto udp and src port 389
live-mdns-reflection	proto udp and src port 5353
live-memcached-reflection	proto udp and src port 11211
live-mssql_rs	proto udp and src port 1434
live-ntp	proto udp and src port 123
live-ssdp	proto udp and src port 1900
live-udp-0	proto udp and port 0
live-udp-80	proto udp and port 80
live-udp-3702	proto udp and src port 3702
live-udp-53	proto udp and src port 53

● : enable netflow monitoring



Further Study resource:

RFC 8195 https://tools.ietf.org/html/rfc8195

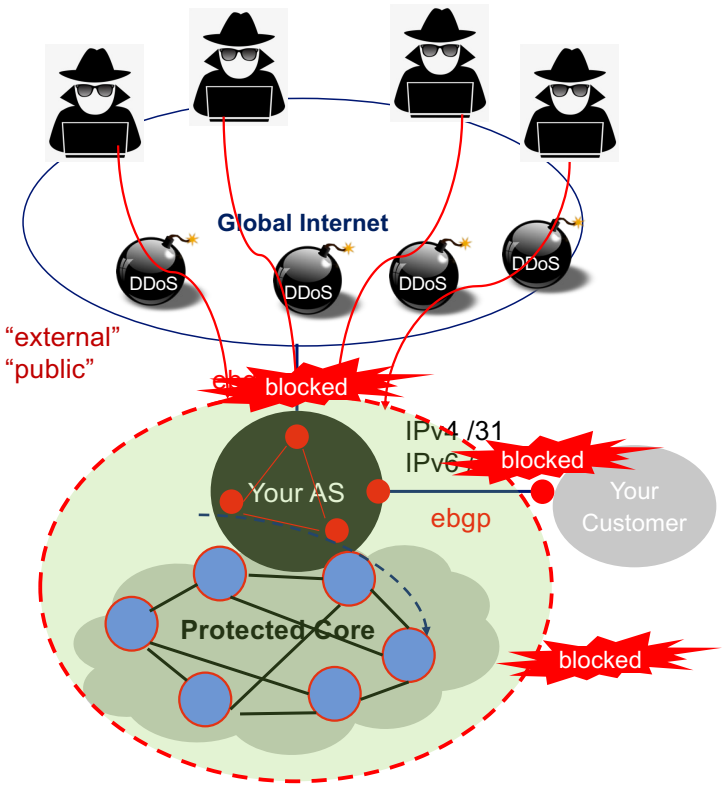


Network Management and Monitoring SNMP, LibreNMS and RRD Lab English 4h 00m

Learn step-by-step how to use open-source tools to monitor and manage a network. This virtual lab topology has been set up with one Linux machine, two Cisco Routers and one Juniper Router.

/

2. Hiding and Protect Core Infrastructure



- **Edge Interface Filter:** Hide and Protect Your Infrastructure Subnets by ACL

1. deny-bogon-source-v4
2. **deny-from-specific-source-v4**
3. deny-to-specific-destination-v4
4. allow-bgp-neigbor-v4
5. deny-to-bgp-linknet-v4
6. allow-to-management-plane-v4
7. deny-to-management-plane-v4
8. allow-trusted-external-to-internal-infra-v4
9. deny-to-internal-infra-v4
10. limit-amplifiers-v4
11. allow-any

(1) Be-Ready: Pre-defined placeholder filter

```
term deny-from-specific-source-v4 {
    from {
        source-prefix-list {
            acl-specific-source-v4;
        }
    }
    then {
        count deny-from-specific-source-v4;
        discard;
    }
}
```

```
prefix-list iacl-specific-source-v4 {
    #deny source of the attack when needed.
}
```

(2) Reduce DDoS Impact: Rate-Limit Known DDoS Attacks (Regional/Country ISP Level)

```
term limit-amplifiers-v4 {
    from {
        protocol udp;
        source-port [ 123 1900 19 11211 389 3702 ];
    }
    then {
        policer police_dos;
        count limit-amplifiers-v4;
        accept;
    }
}
```

10G Link

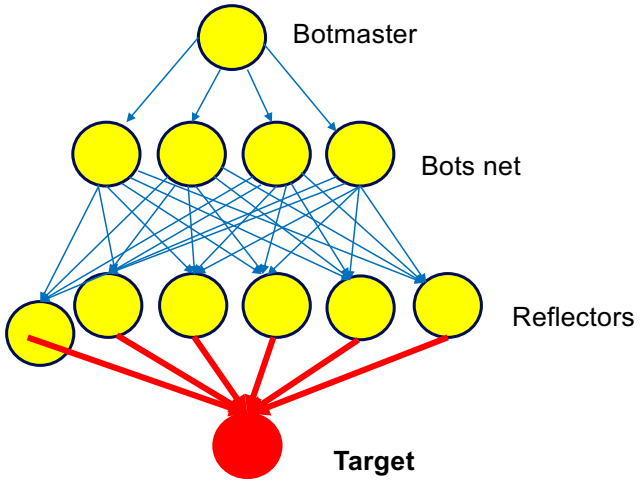
```
policer police_dos {
    if-exceeding {
        bandwidth-limit 200m;
        burst-size-limit 125k;
    }
    then discard;
}
```

ACL Edge-Filter is your first line of defense!

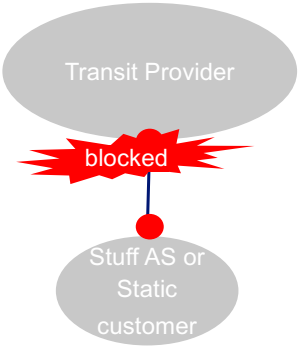
3. Use Access Control List to Stop Common DDoS Attacks

For example, this ACL can assist in stopping some common UDP amplification attacks.

```
deny udp any eq 11211 any      # This will block memcache reflection attacks
deny udp any eq 1900 any       # This will block SSDP reflection attacks
deny udp any eq 520 any        # This will block RIP reflection attacks
deny udp any eq 389 any        # This will block LDAP reflection attacks
deny udp any eq 111 any        # This will block SunRPC reflection attacks
deny udp any eq 19 any         # This will block Chargen reflection attacks
deny udp any any eq 80         # This will stop UDP directed at http
permit ip any any
```



- Such ACLs can be further tuned to make it more suitable after knowing the type of services that are running in the network.



03. Robust Secure Routing Policies

Identify Routing Security Flaws

eBGP Route Hijacks Case Study

Apple BGP Route Hijack

July 26-27 2022
Apple network traffic took a brief *12-hour* detour through the *Russian Rostelecom* network that spanned *July* 26-27

Rostelecom autonomous system (AS) 12389 network was the 17.70.96.0/19 allocated to the US tech giant.
A /19 IP block contains 8192 network addresses, and Siddiqui said the prefix is part of Apple's larger 17.0.0.0/8 allocation.
Apple does not use Route Origin Authorisation (ROA), which uses resource public key infrastructure (RPKI) cryptographically signed objects to attest that an origin AS is allowed to announce network prefixes.

Route Object (RO)

- **Current Route Object issues:**
  - Duplication, Proxy Objects, Exist but not in DFZ, expected route object in APNIC, but only found in other IRRs, etc
  - In RADB anyone pay for membership can create any route object for any prefix (if it hasn't been covered by another route object in RADB

Route Origin Authorisation

- **A Route Origin Authorisation (ROA)** is a cryptographically signed object that states which **Autonomous System (AS) is authorised to originate**

The ability to create RPKI ROAs is a service offered by the Regional Internet Registries and National Internet Registries
AFRINIC, APNIC, ARIN, NIC.BR, LACNIC, JPNIC, and RIPE NCC.

Route Object

Route ROA rigin Authorisation

Whois Route Object

```
route6:          2402:f00:2000::/38
origin:          AS23918

mnt-by:          MAINT-AU-NTT
last-modified:   2020-07-29T07:02:07Z
source:          APNIC
```

RPKI-ROV status:

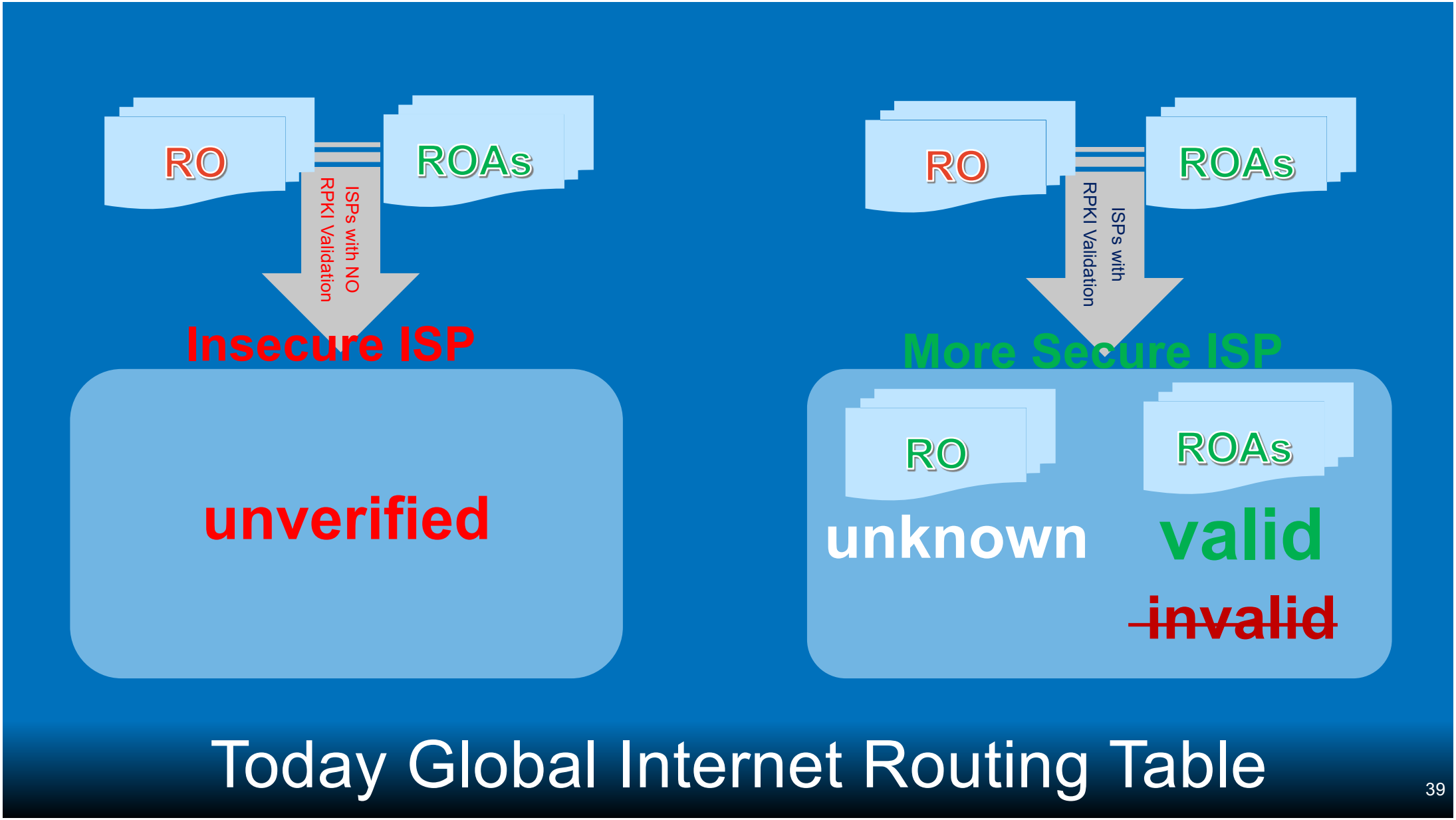
unknown

RPKI Signed ROA

```
route6:          2402:f00:2000::/38
max-length:      38
origin:          AS23918

source:          RPKI  # Trust Anchor: apnic
```

RPKI-ROV status:

valid



Today Global Internet Routing Table

Route Hijack Case 1 - With ROA Signed

18.195.44.0/24 – more specific was hijacked:

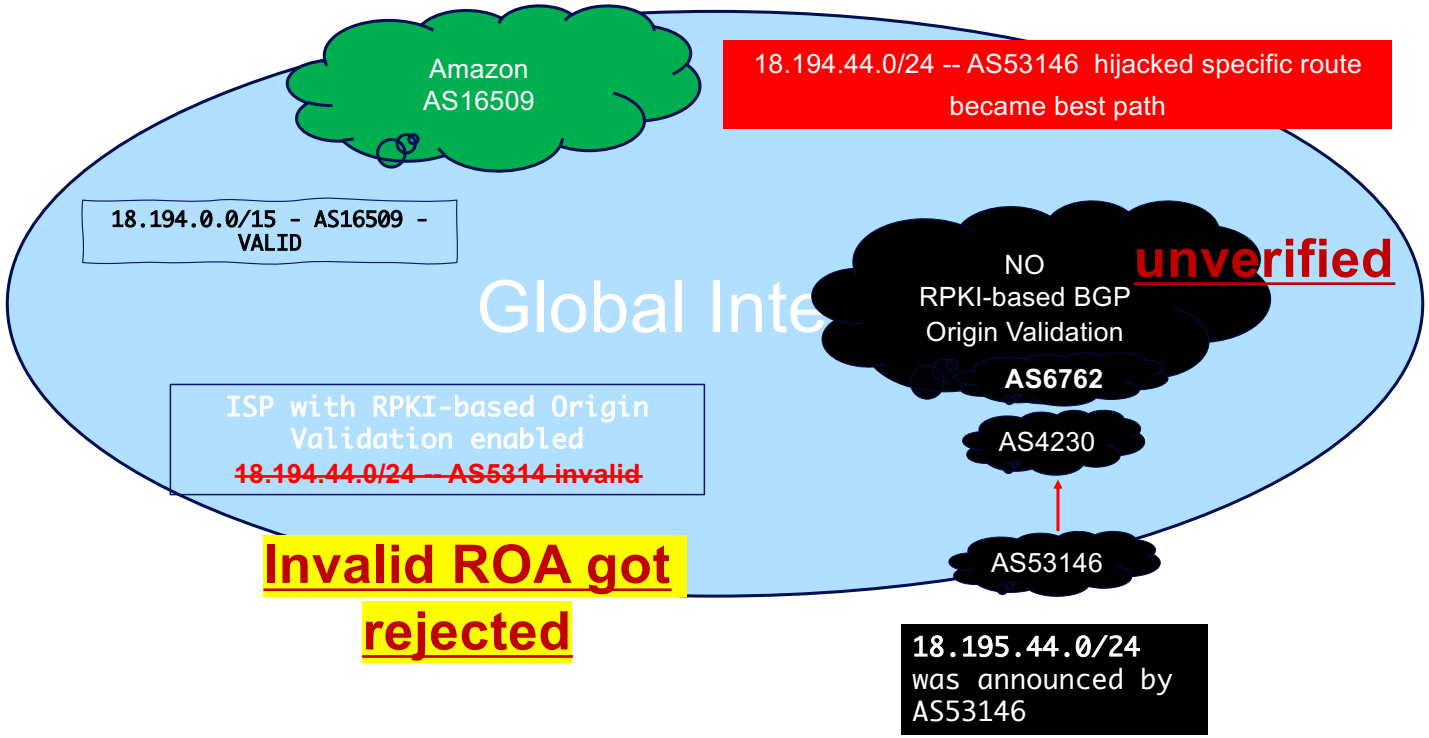
Route Origin Authorization (ROA) Objects

```
route:        18.194.0.0/15
max-length:   24
origin:       AS8987
source:       RPKI  # Trust Anchor: arin

route:        18.194.0.0/15
max-length:   24
origin:       AS14618
source:       RPKI  # Trust Anchor: arin

route:        18.194.0.0/15
max-length:   24
origin:       AS16509
source:       RPKI  # Trust Anchor: arin
```

- Secured ISPs with rpki-based BGP origin validation saw hijacked route as an invalid ROA, rejected it, and helped to stop this hijack

- Insecure ISPs without RPKI accepted route hijack

The impact was minimal!



At 2022–06–07 22:59:29

Detected by: https://bgpstream.crosswork.cisco.com/event/292121

Route Hijack Case 2 - Invalid ROA Setting

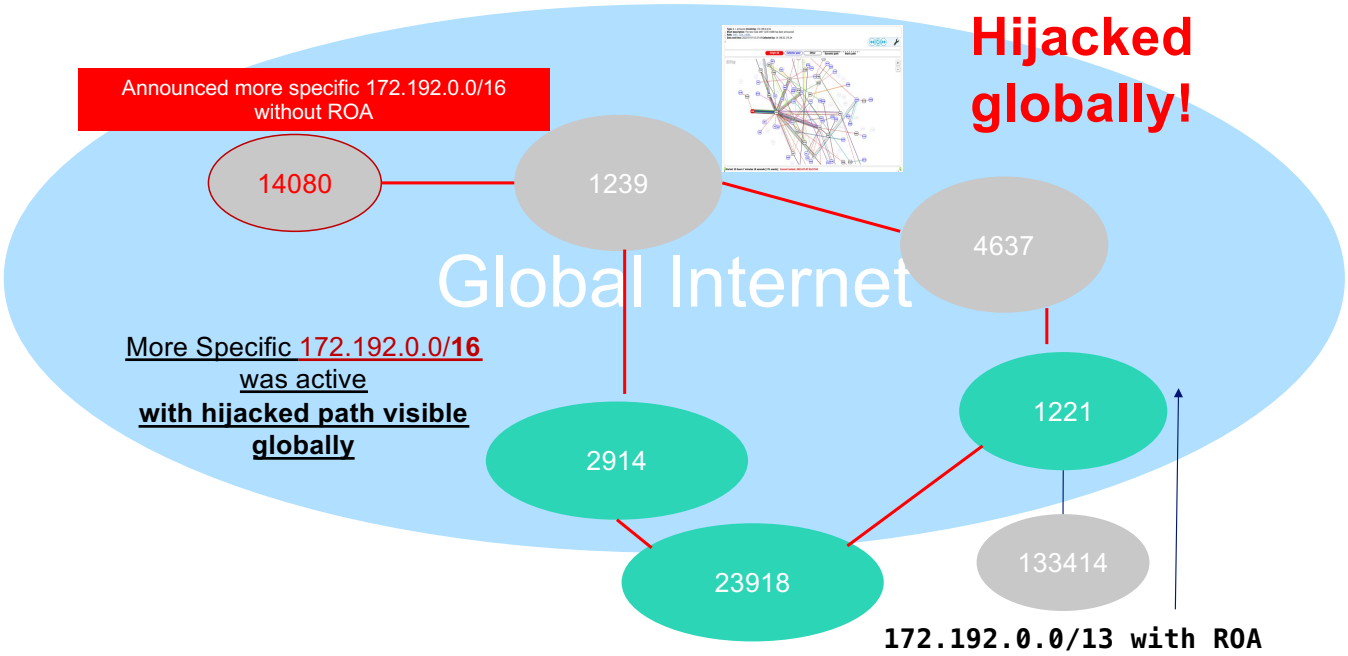
172.192.0.0/16 – has no ROA was hijacked

Route Origin Authorization (ROA) Objects

```
route:          172.192.0.0/13
descr:          RPKI ROA for
172.192.0.0/13 / AS133414
max-length:     13
origin:         AS133414
source:         RPKI  # Trust Anchor:
apnic
```

- Insecure ISPs without RPKI accepted route hijack

- Secured ISPs (with ROA rpki validation) could not verified the unknown RO, accepted route hijack.



#Normal Path:

172.192.0.0/13 *

AS path: 1221 133414 ?, **validation-state: valid**

#Hijack Path was active in **unknown** state:

172.198.0.0/16 *

AS path: **2914 1239** 14080 I, **validation-state: unknown**

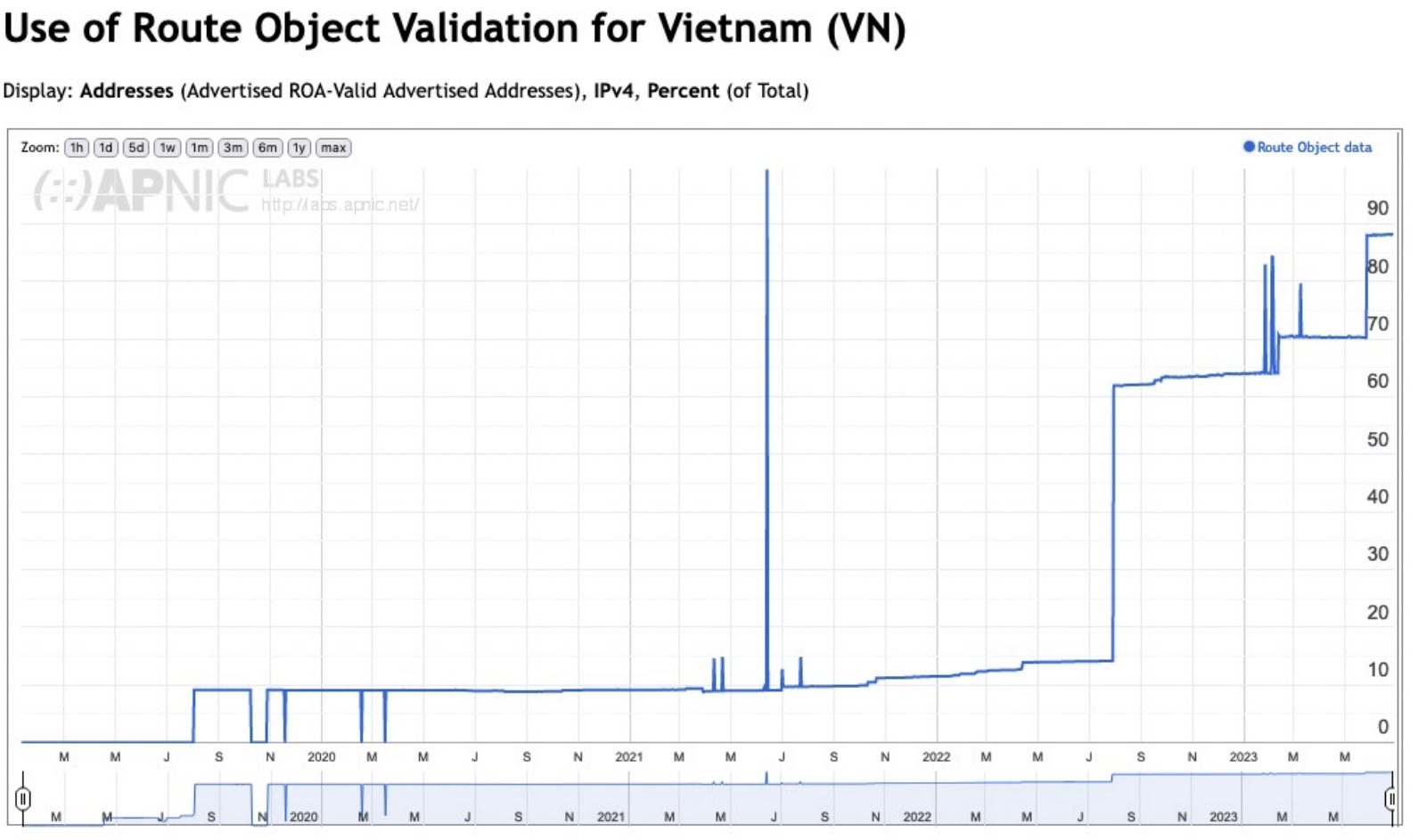
AS path: **1221 4637 1299 1239 14080** I, **validation-state: unknown**

at 2022-07-07 03:36:50

Detected by: https://bgpstream.crosswork.cisco.com/event/293015

IPv4 ROA - VN

https://stats.labs.apnic.net/roas

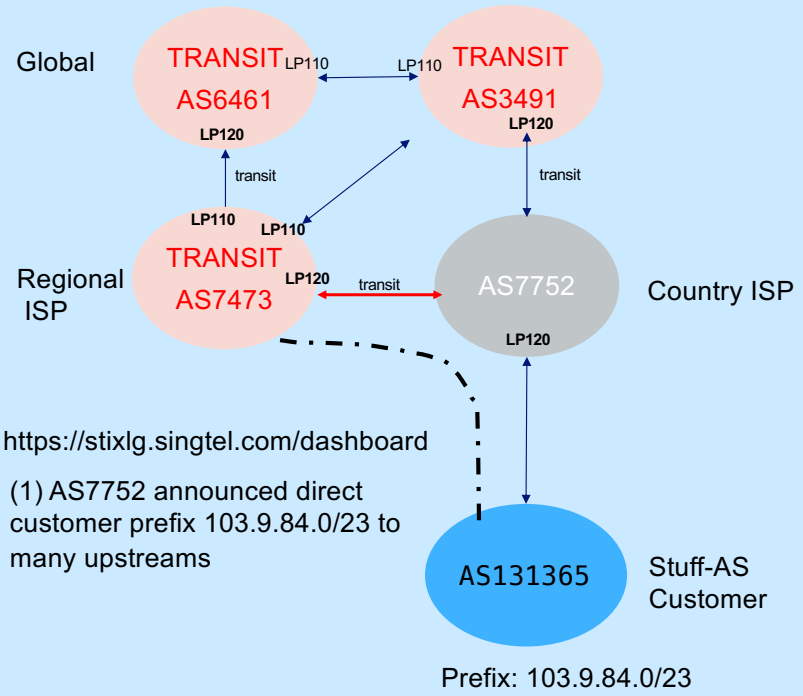


Analyse the eBGP Route Leak Cases

Exact-match Route Filter - Is secure enough?

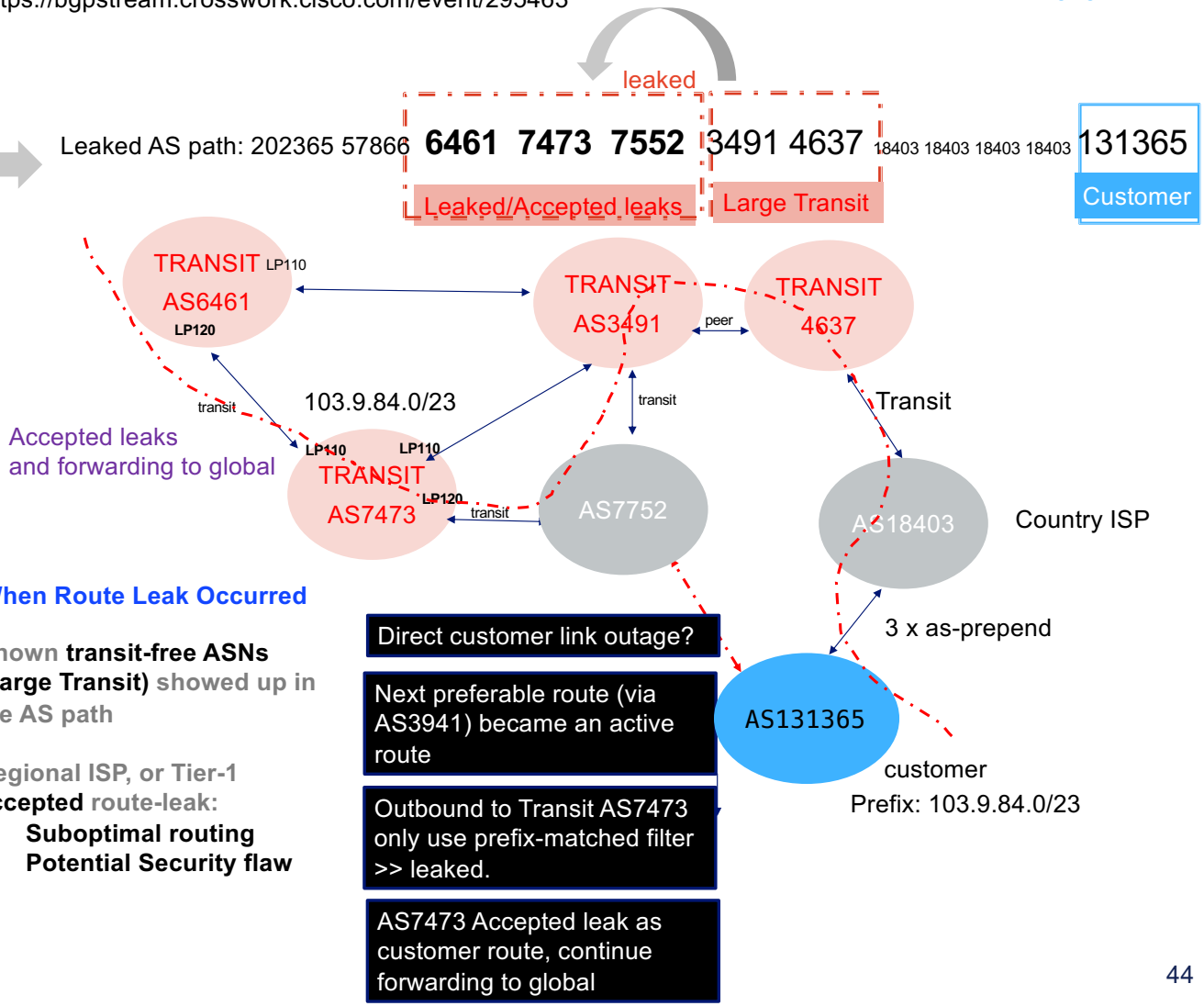
: Customer
: ISP
: Peer
: Transit

Prefix: 103.9.84.0/23
One of normal AS best paths: **7473 7752 131365**



Leaked prefix: 103.9.84.0/23

2022-08-21 05:16:59 UTC, we detected a possible BGP Leak
https://bgpstream.crosswork.cisco.com/event/295463



When Route Leak Occurred

Known **transit-free ASNs (Large Transit)** showed up in the AS path

Regional ISP, or Tier-1 **accepted** route-leak:
- **Suboptimal routing**
- **Potential Security flaw**

Direct customer link outage?

Next preferable route (via AS3941) became an active route

Outbound to Transit AS7473 only use prefix-matched filter >> leaked.

AS7473 Accepted leak as customer route, continue forwarding to global

Small Route Leak – A Sign of Routing Security Flaw

https://bgpstream.crosswork.cisco.com/event/

Start time	Event ID	Leaked AS path:	Large Transit Accepted Leak as customer route	Regional ISP Accepted Leak as customer route	Leaked by	Large Transit in the path
2022-08-21 05:16:59 UTC	295463	202365 57866 6461 7473 7552 3491 4637 18403 18403 18403 18403 131365	6461	7473	7552	3491 4637
2022-08-21 08:59:24 UTC	295470	53432 13994 7029 6461 4637 38442 38442 38442 6939 1299 4648 132528 45355 135647	7029 6461	4637	38442	6939 1299 4648
2022-07-28 08:49:17 UTC	293993	35710 48200 6762 4637 7552 7552 7552 7552 7552 7552 7552 7552 7552 7552 7552 1299 174 132876 136255	6762	4637	7552	1299 174
2022-08-20 21:12:39 UTC	295449	202365 206499 50629 3356 4637 4637 4637 31712 31712 31712 31712 286 174 42466 42466 42466	6461 (ZAYO-6461, US) 3356 (LEVEL3, US) 701 (UUNET, US) 6762 (SEABONE-NET	4637	31712	286 174

Small leaks

Case Studies Leak Pattern 3

Large Leaks were not on the News

2022-03-29 08:10:14 UTC **Over 300 leaks accepted/detected**

https://bgpstream.crosswork.cisco.com/

Accepted leaks **leaked** **Large Transit**

Leak AS path: 263525 **3549 3356 3257** 5511 49666 197207

Tier-1 peer

Live - Examples

https://bgpstream.crosswork.cisco.com/

Possible BGP hijack

Beginning at 2023-06-03 17:18:24 UTC, we detected a possible BGP hijack.
Prefix 130.137.28.0/24, is normally announced by AS16509 AMAZON-02, US.
But beginning at 2023-06-03 17:18:24, the same prefix (130.137.28.0/24) was also announced by ASN 58319.
This was detected by 2 BGPMon peers.

Expected
Start time: 2023-06-03 17:18:24 UTC
Expected prefix: 130.137.28.0/24
Expected ASN: 16509 (AMAZON-02, US)

Event Details
Detected advertisement: 130.137.28.0/24
Detected Origin ASN 58319 (KAZAKOV-AS, RU)
Detected AS Path 63956 3491 58453 209141 43727 34602 58319

Routes found on all for '130.137.28.0/24'

map | plain text | permalink | renew

Prefix: 130.137.28.0/24 2

IRR Explorer | WHOIS

1 SENTIAAMS5-v4

AS-Path	8315 6774 16509 via next-hop 185.74.76.8
Origin validation state	not-found
ASPA validation state	unknown
Only To Customer (OTC)	yes, ASN: 8315
Origin	IGP
MED	0
Last update	2023-06-04 11:58:37 UTC (00:05:29 ago)
Large communities	8315:32:6 8315:32:6774 (Route learned through BIC...)

BGP Leak

Beginning at 2023-06-02 16:37:36 UTC, we detected a possible BGP Leak
Prefix 1.65.248.0/21, Normally announced by AS4760 HKTIMS-AP HKT Limited, HK
Leaked by AS7552 VIETEL-AS-AP Viettel Group, VN
This was detected by 10 BGPMon peers.

Leak Details

Start time: 2023-06-02 16:37:36 UTC

Leaked prefix: 1.65.248.0/21 (AS4760 HKTIMS-AP HKT Limited, HK)

Leaked By: AS7552 (VIETEL-AS-AP Viettel Group, VN)

Leaked To:
7473 (SINGTEL-AS-AP Singapore Telecommunications Ltd, SG)

Example AS path: 200005 13237 6461 7473 7552 131429 131429 131429 131429 131429 131429 131429 131429 131429 131429 45896 18403 4229 3491 4760 4760 4760 4760 4760

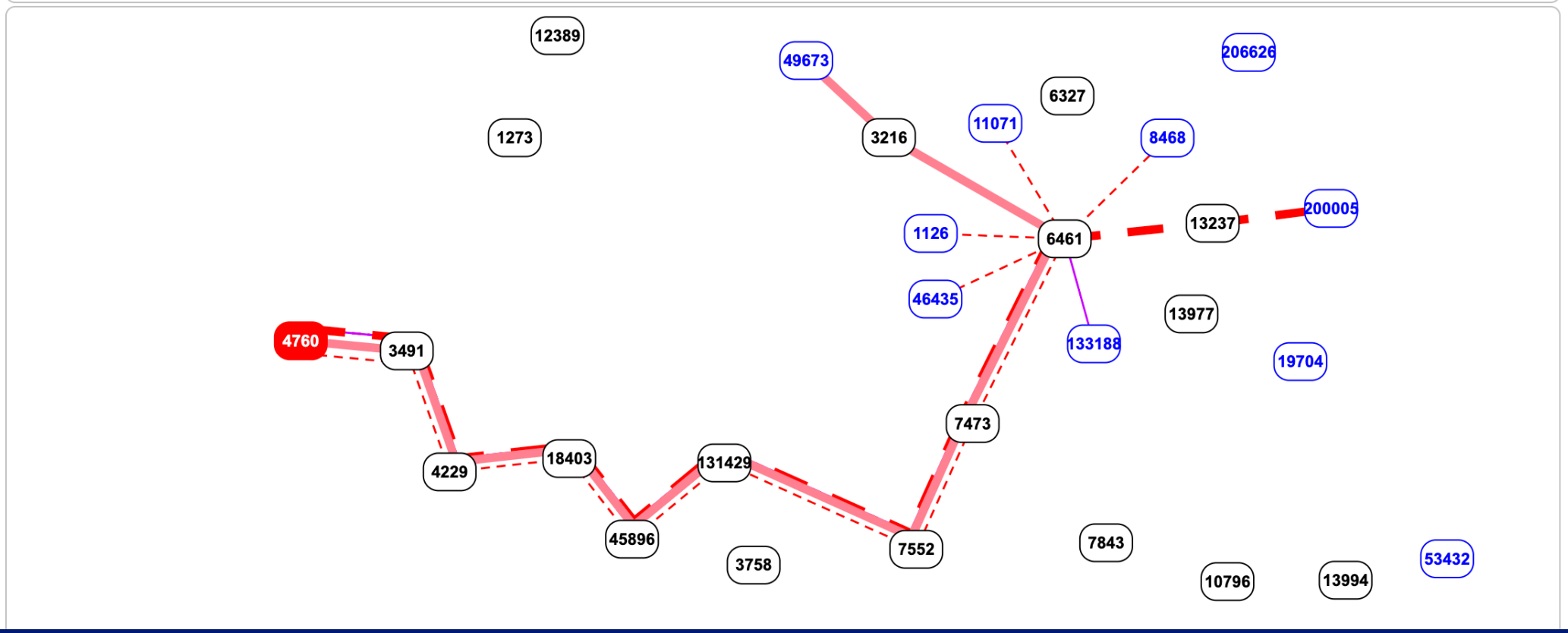
Number of BGPMon peers that saw it: 10

Watch the replay of this event

Type: A > announce **Involving:** 1.65.248.0/21
Short description: The new route 46435 6461 7473 7552 131429 131429 131429 131429 131429 131429 131429 131429 131429 131429 45896 18403 4229 3491 4760 4760 4760 4760 4760 has been announced
Path: 46435, 6461, 7473, 7552, 131429, 45896, 18403, 4229, 3491, 4760,
Date and time: 2023-06-02 16:35:47 **Collected by:** 00-74.118.17.220

Info

Origin AS | Collector peer | Other | Dynamic path | Static path



https://bgpstream.crosswork.cisco.com/event/305428

BGP Leak

Beginning at 2023-03-16 08:54:17 UTC, we detected a possible BGP Leak
Prefix 45.119.240.0/24, Normally announced by AS131418 VIETNAMESPORTS-AS-VN Vietnam Esports Development Joint Stock Company, VN
Leaked by AS7552 VIETEL-AS-AP Viettel Group, VN
This was detected by 11 BGPMon peers.

Leak Details

Start time: 2023-03-16 08:54:17 UTC

Leaked prefix: 45.119.240.0/24 (AS131418 VIETNAMESPORTS-AS-VN Vietnam Esports Development Joint Stock Company, VN)

Leaked By: AS7552 (VIETEL-AS-AP Viettel Group, VN)

Leaked To:
7473 (SINGTEL-AS-AP Singapore Telecommunications Ltd, SG)

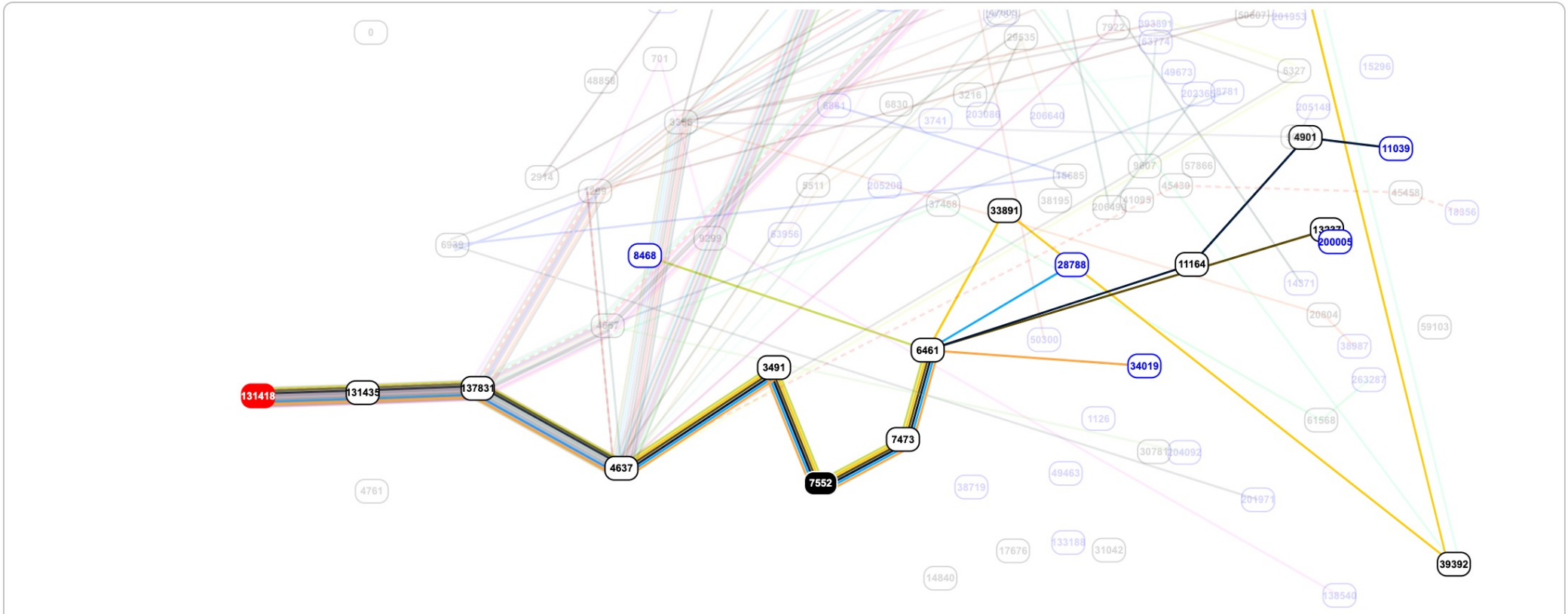
Example AS path: 200155 39392 33891 6461 7473 7552 3491 4637 137831 131435 131418

Watch the replay of this event

Node ID: 7552
AS: 7552
Owner: VIETEL-AS-AP Viettel Group, VN

Info

Origin AS | Collector peer | Other | Dynamic path | Static path



https://bgpstream.crosswork.cisco.com/event/303438

What was missing?

- Lock Large Transit Leaks
- Route-tag for Route filter

Internet Service Provider The Fundamentals

- Global Default Free Zone
- Internet Tiers and Peering Relationships
- Common Routing Policies with Best Path Selection

Global Internet Routing - Default Free Zone

In Internet routing, the **default-free zone** (**DFZ**) is the collection of all Internet autonomous systems (AS) that do not require a default route to route a packet to any destination. Conceptually, DFZ routers have a "complete" Border Gateway Protocol table, sometimes referred to as the **Internet routing table**, **global routing table** or **global BGP table.**.

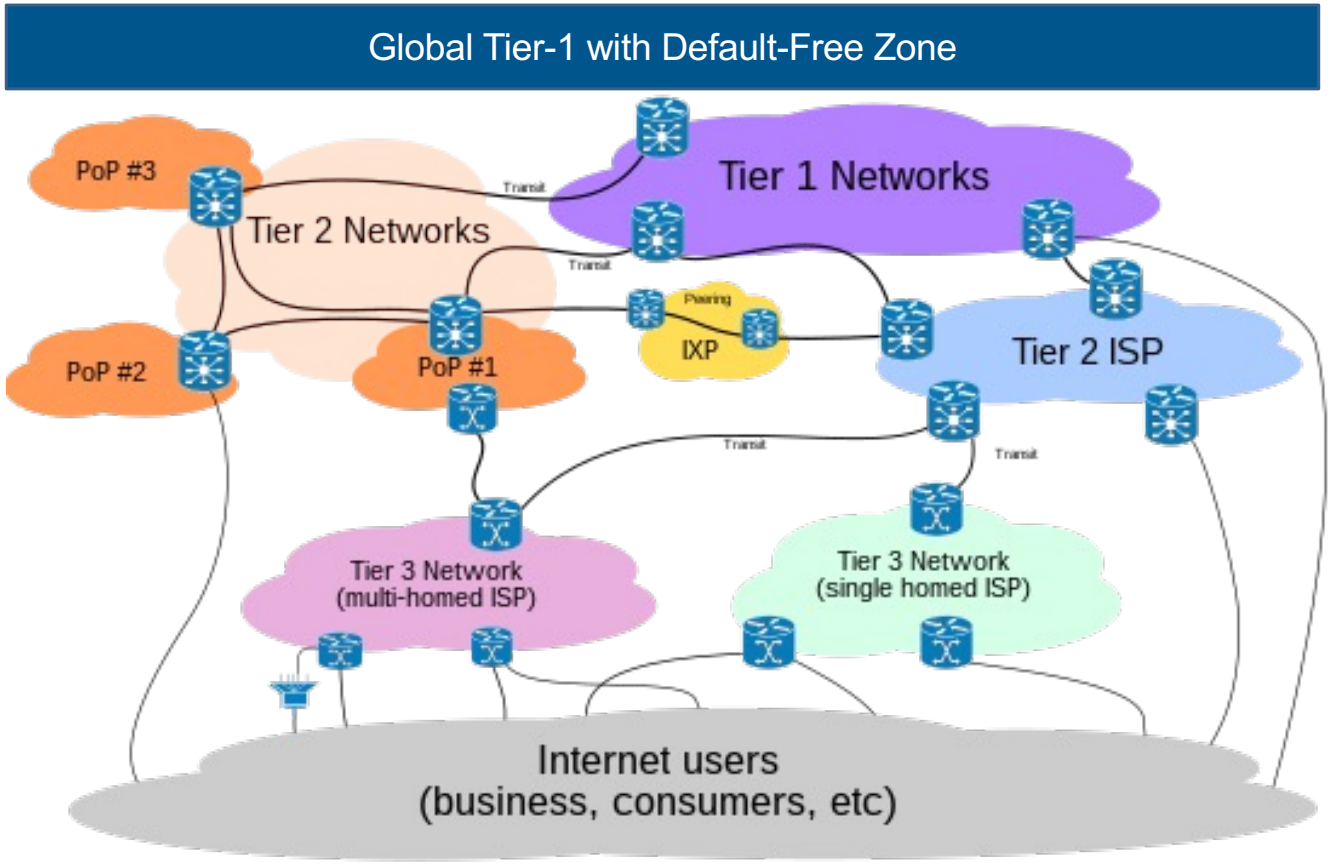
https://en.wikipedia.org/wiki/Default-free_zone

eBGP Relationships

A **Tier 1 network** is an Internet Protocol (IP) network that can reach every other network on the Internet solely via settlement-free interconnection (also known as settlement-free peering).

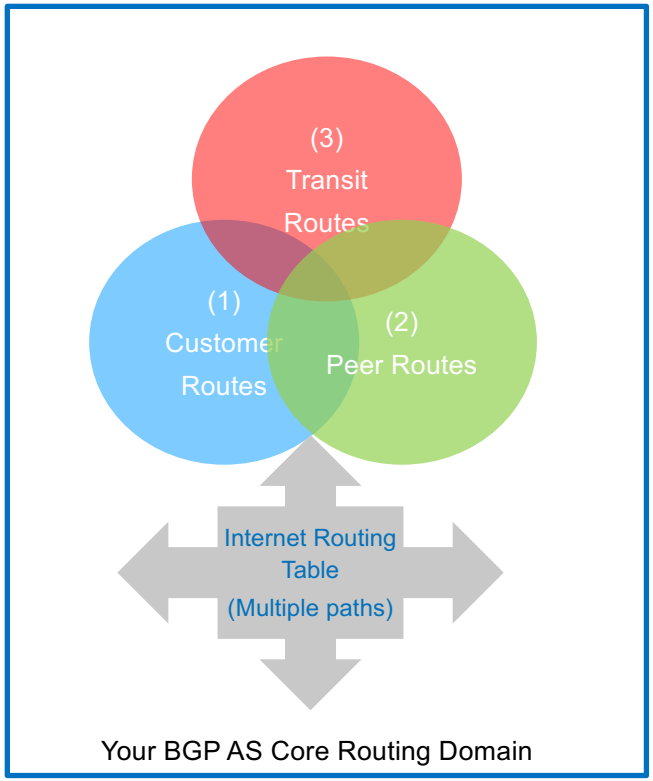
Tier 1 networks can exchange traffic with other Tier 1 networks without paying any fees for the exchange of traffic in either direction

In contrast, some Tier 2 networks and all Tier 3 networks must pay to transmit traffic on other networks



Source: https://en.wikipedia.org/wiki/Tier_1_network

Common Routing Table



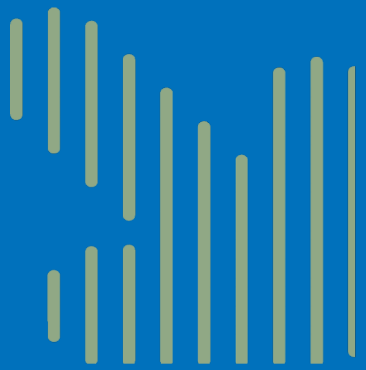
Route4/route6:

- minimum routable ip block of IPv4 is /24, IPv6 is /48
- One route contains multiple paths

Path Selection:

The 1st Rule: The longest prefix match wins it all.

Path Selection			
	Attribute	Description	Preference
1	**Weight**	Administrative preferfence	Highest
2	**Local Preference**	Communicated between peers within an AS	Highest
3	**Self-originated**	Prefer paths origninated locally	True
4	**AS Path**	Minimize AS hops	Shortest
5	**Origin**	Prefer IGP-learned routes over EGP, and EGP over unknown	IGP
6	**MED**	Used externally to enter an AS	Lowest
7	**External**	Prefer eBGP routes over iBGP	eBGP
8	**IGP Cost**	Consider IGP metric	Lowest
9	**eBGP Peering**	Favour more stable routes	Oldest
10	**Router ID**	Tie breaker	Lowest

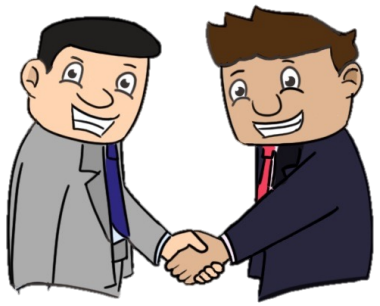


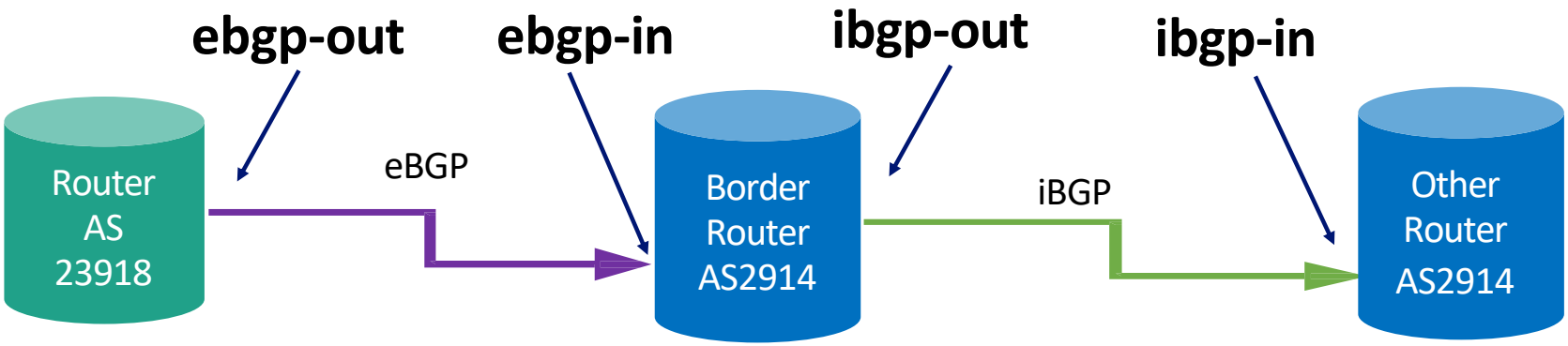
Design Robust Routing Policies

- Enable - ROA RPKI Validation
- Lock Large Transit Leaks
- Using BGP communities for Routing Policies & Route filters

BGP Filter – Attachment Points

- Route Filter Attachment points
- Route Advertisement Direction

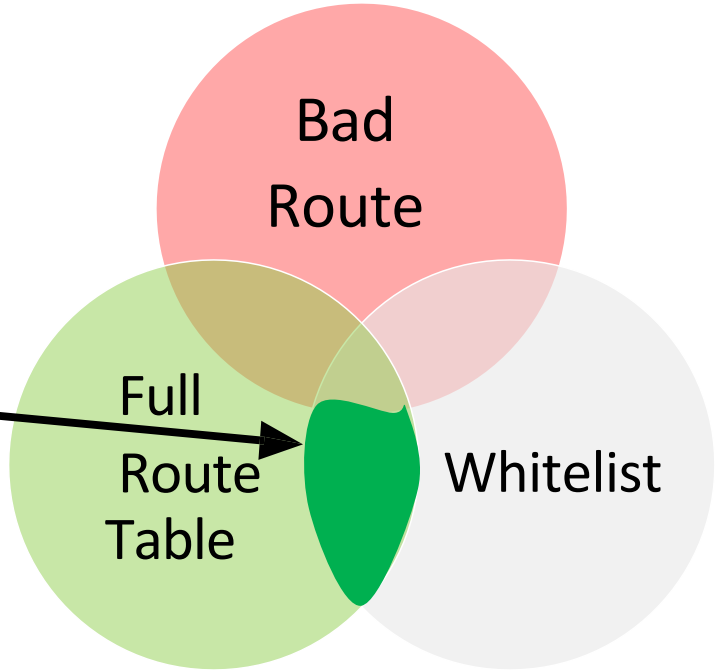




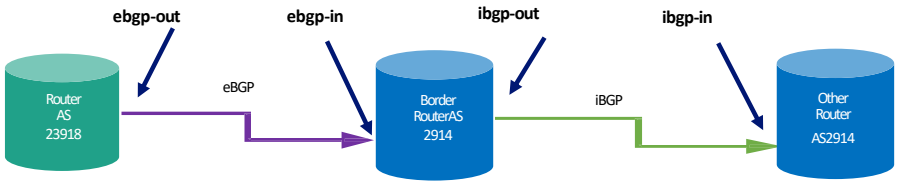
"ebgp-in" Rejecting *Bad Routes*

- Bogon or Private ASNs
- Bogon or Private Prefixes
- Large Leaks (example: NTT seeing Lumen via Orange)
- RPKI Invalid announcements
- Your own space and more-specifics

The good route to be accepted in



Routing Policies: How to use BGP communities?



- ***Classification*** on the **ebgp-in**

"`set community XXX`"

Common Classifiers

- "learned from transit customer"
- "route via peering partner"
- "learned from upstream provider"
- "route learned in Singapore"
- "route learned in Sydney"

- Execution - **ebgp-out** attachment point

"`match community YYY`"

Common Execution Outcomes

- Announce to this EBGP neighbor
- Do not announce
- Prepend AS_PATH once

Further Study resource:
RFC 8195 https://tools.ietf.org/html/rfc8195

What is a BGP community?

"A community is a group of destinations which share some common property." – RFC1997

"An Application of the BGP Community Attribute i in simplifying the implementation and configuration of routing policies in the multi-provider Internet." – RFC1998

Further Study resource:
RFC 1997: https://tools.ietf.org/html/rfc1997
RFC 1998: https://tools.ietf.org/html/rfc1998

Define Route Propagation Policies Via eBGP and BGP Community Tags

Import Rule \ Export Rule	ebgp-out to **customer**	eBGP-out to peers	eBGP-out to upstream transit
Learnt from **Customer** > tag customer routes	**ACCEPT**	**ACCEPT**	**ACCEPT**
Learnt from **peer** > tag peer routes	**ACCEPT**	**Reject**	**Reject**
Learnt from **upstream** > tag transit routes	**ACCEPT**	**Reject**	**Reject**
No-Tags (safe guard)	**Reject**	**Reject**	**Reject**

1. Reject Large Transit AS

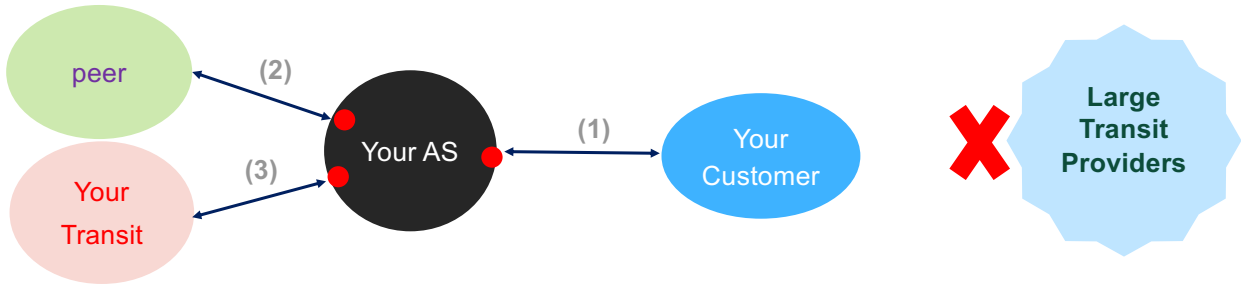
In from Customers, or Peers – and Out to Upstream

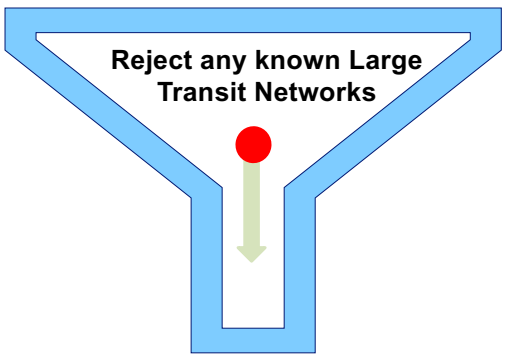
Large Transit Providers

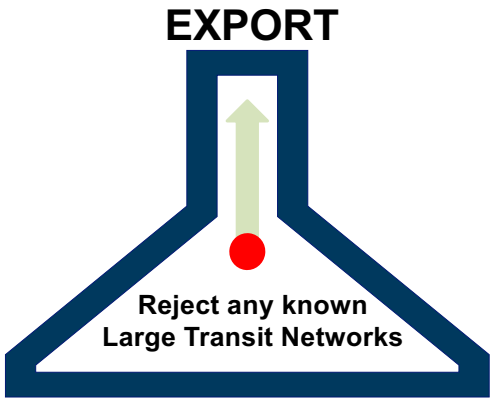
Reference Policy statement: Junos Style:

```
policy-options as-path lock-large-transit-in  ".*
(174|209|701|1239|1273|1299|2828|2914|3257
|3320|3356|3491|3549|3949|4713|5511|6453|6
461|6762|6830|6939|7018|7922|15169) .* "

#customise-it
```

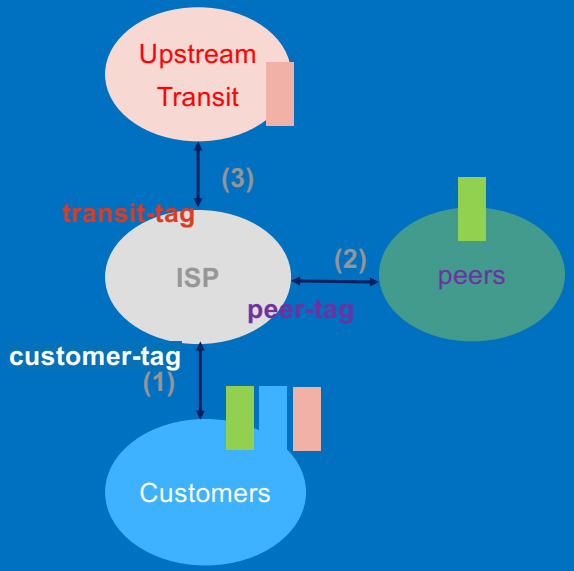
No known transit-free ASNs should show up in a given valid AS_PATH from customers, or Peer







2. Import – Set route-tag Export – Filter based on route-tag

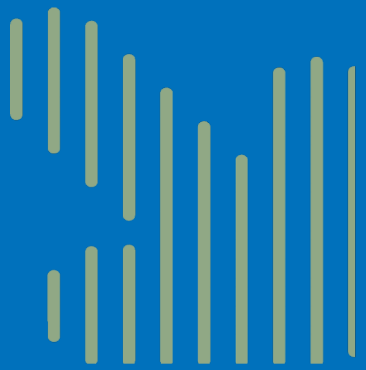


Route import, TAG it

1. Tag Customer's route
2. Peer's route
3. Transit's route

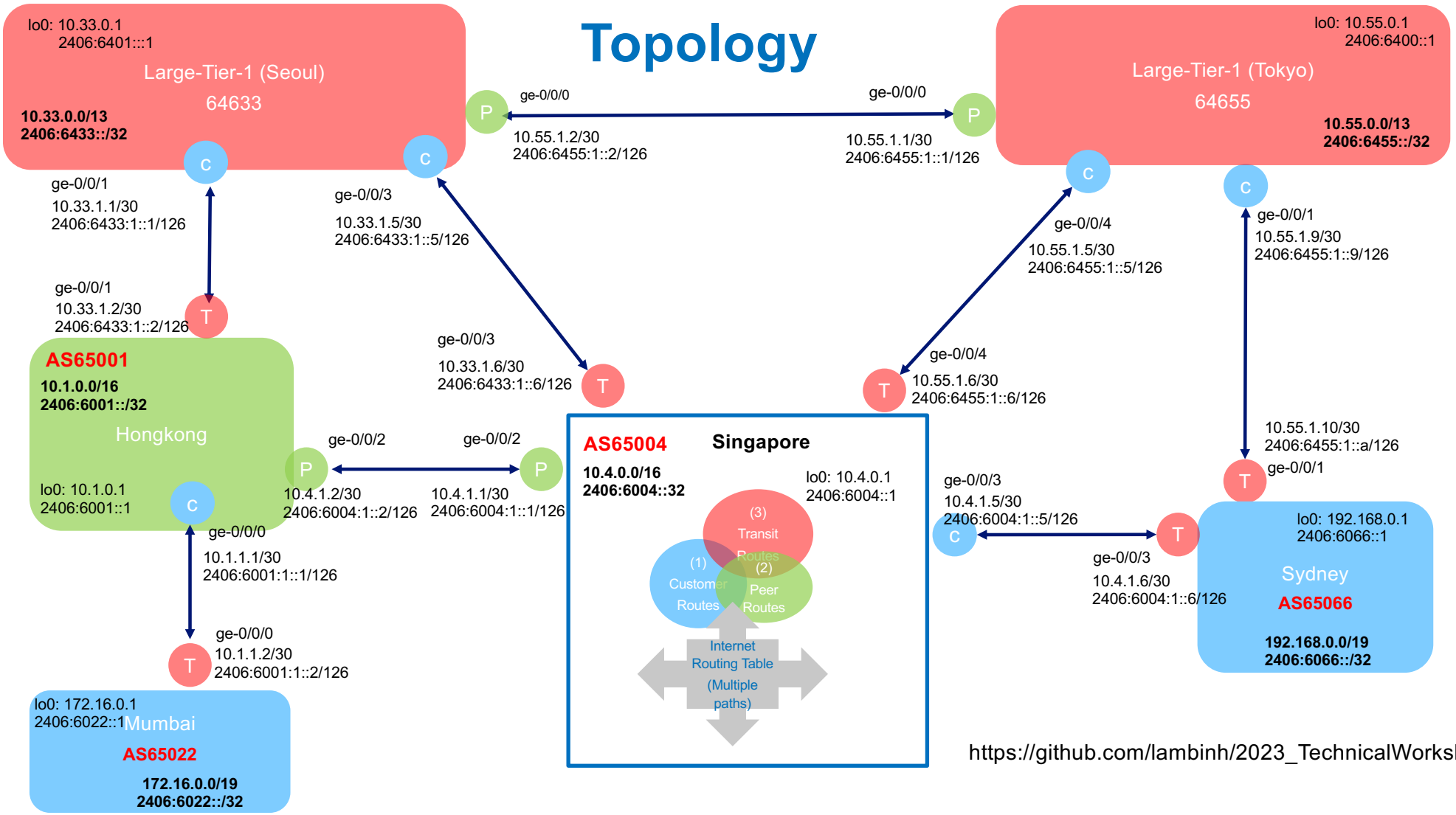
eBGP Route Filter

Import From \ Export To	Customer	Peer	Upstream Transit
Customer ➢ tag **customer-tag**	Allow **customer-tag**	Allow **customer-tag**	Allow **customer-tag**
Peer ➢ tag **peer-tag**	Allow **peer-tag**	Reject ~~**peer-tag**~~	Reject ~~**peer-tag**~~
Upstream ➢ tag **transit-tag**	Allow **transit-tag**	Reject ~~**transit-tag**~~	Reject ~~**transit-tag**~~
No-Tags (**safe guard**)	Reject	Reject	Reject

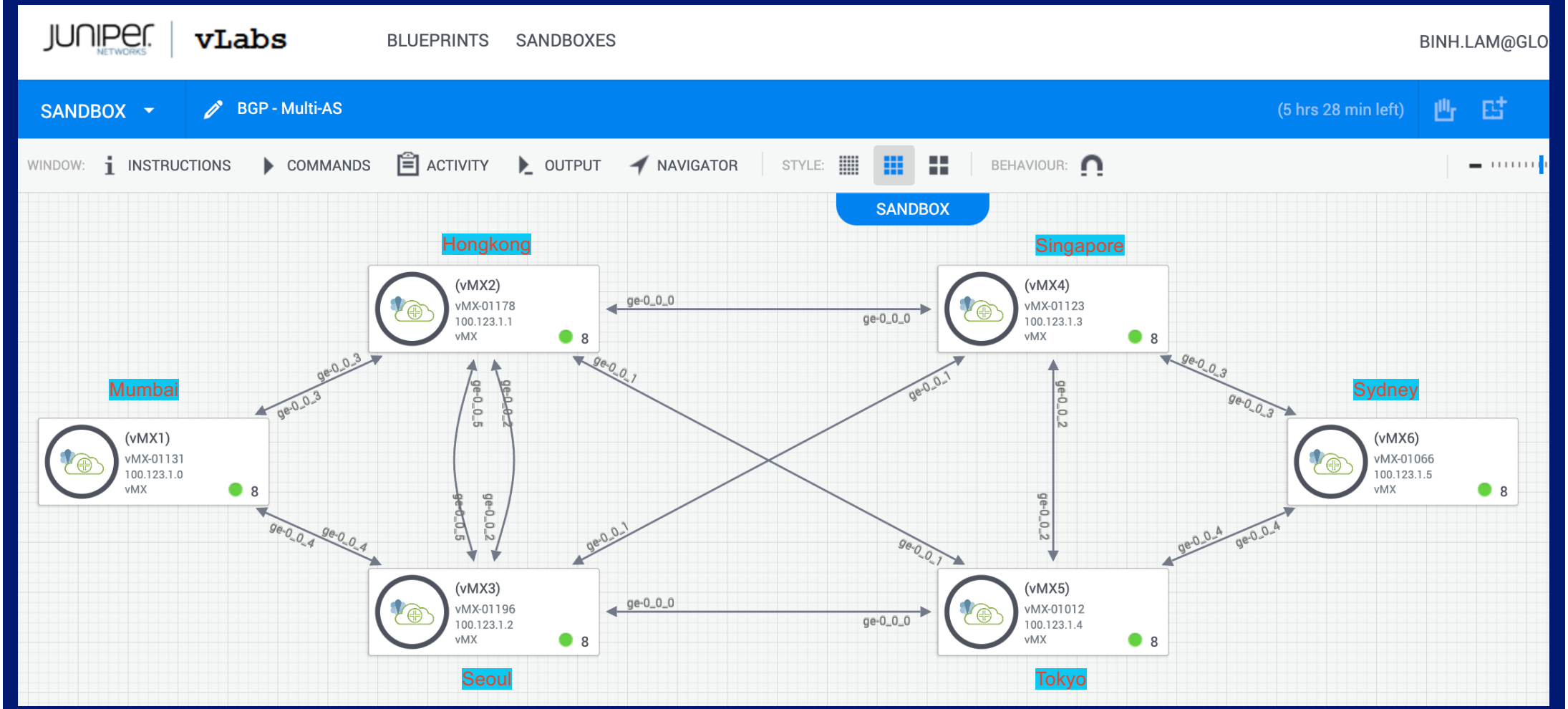


Demo Lab Topology

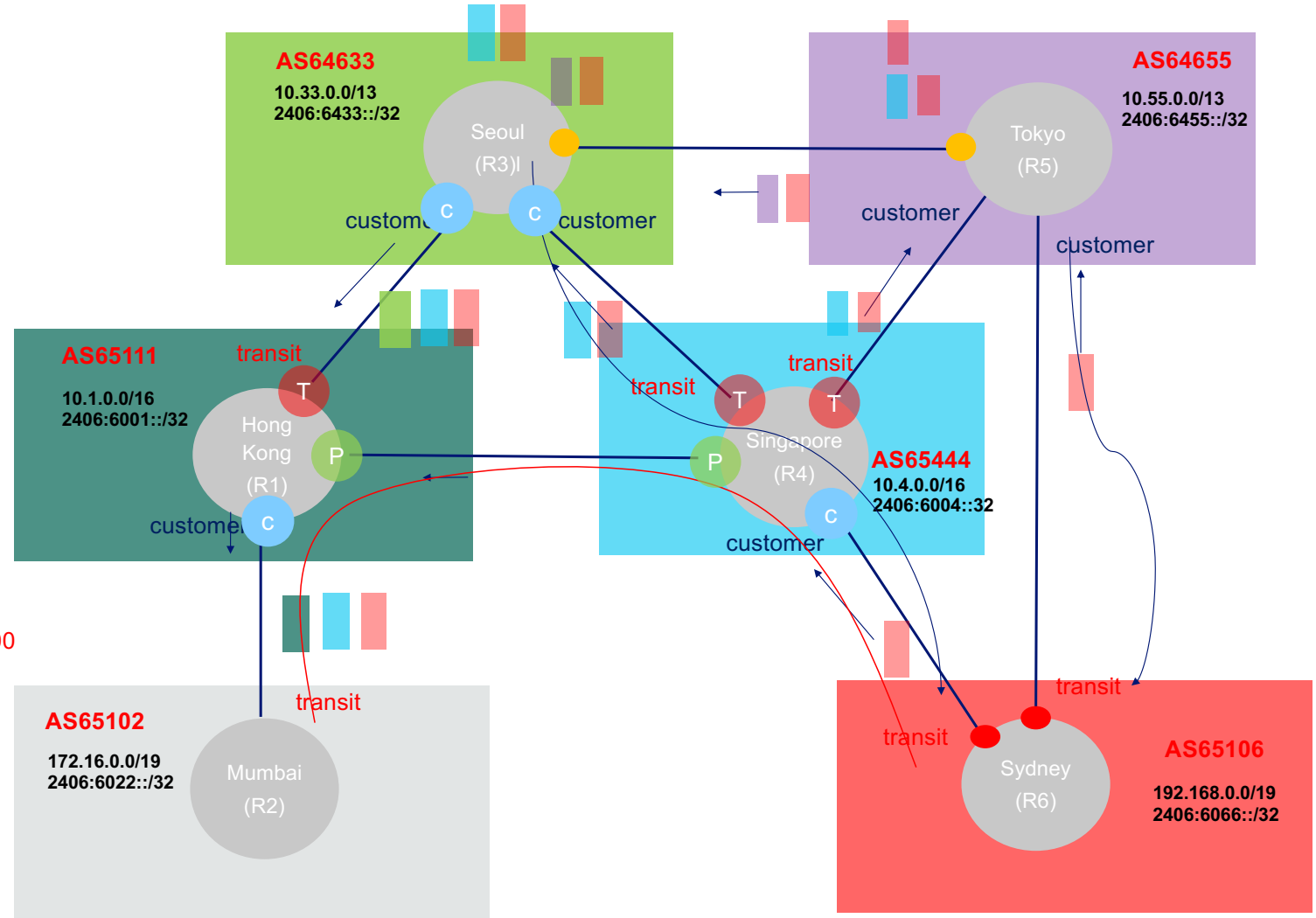
APNIC vSRX Sandbox Topology



https://github.com/lambinh/2023_TechnicalWorkshop


JUNIPER NETWORKS
vLabs
BLUEPRINTS
SANDBOXES
BINH.LAM@GLO
SANDBOX
BGP - Multi-AS
(5 hrs 28 min left)
WINDOW:
INSTRUCTIONS
COMMANDS
ACTIVITY
OUTPUT
NAVIGATOR
STYLE:
BEHAVIOUR:
SANDBOX
Hongkong
(vMX2)
vMX-01178
100.123.1.1
vMX
8
Singapore
(vMX4)
vMX-01123
100.123.1.3
vMX
8
Mumbai
(vMX1)
vMX-01131
100.123.1.0
vMX
8
Sydney
(vMX6)
vMX-01066
100.123.1.5
vMX
8
(vMX3)
vMX-01196
100.123.1.2
vMX
8
Seoul
(vMX5)
vMX-01012
100.123.1.4
vMX
8
Tokyo
ge-0_0_0
ge-0_0_1
ge-0_0_2
ge-0_0_3
ge-0_0_4
ge-0_0_5

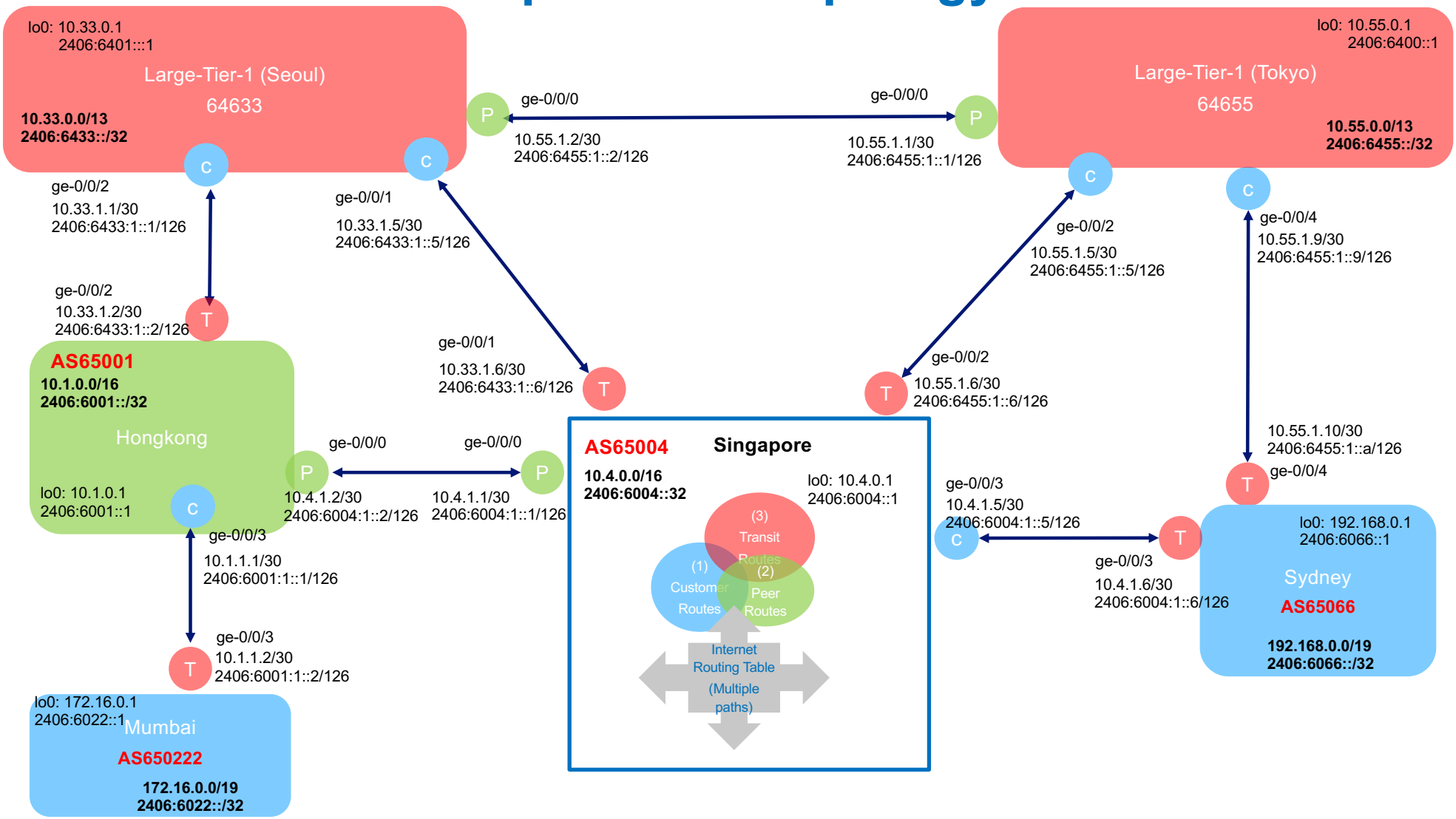
VNNIC2023 LAB Topo – Juniper vLabs



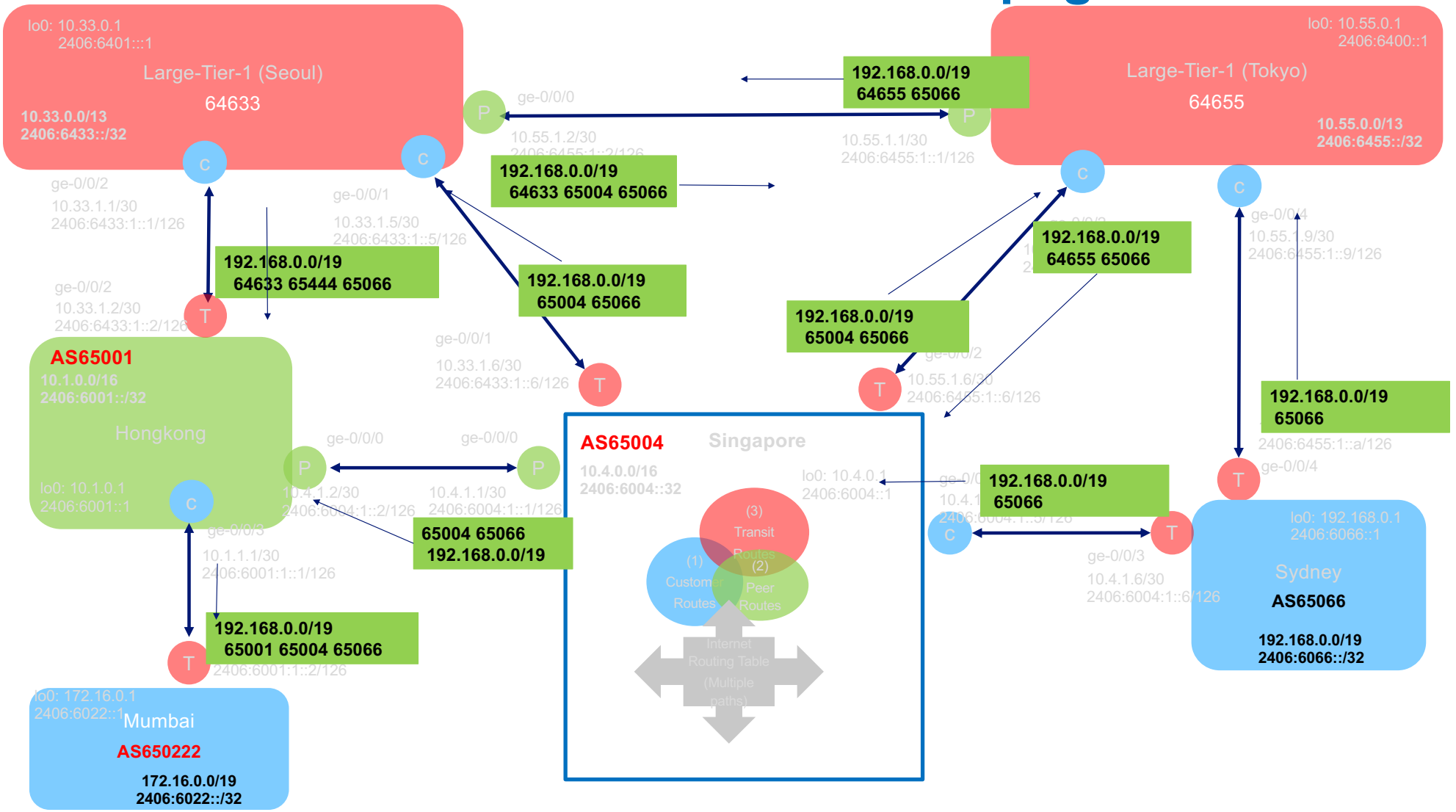
Routing Policies:

- Customer: LP120
- Peer route: LP110
- Transit Route: LP100

Juniper vLab Topology



192.168.0.0/19 Route Propagation



Active Routing table to prefix 192.168.0.0/19

```
@R3_Seoul> show route 192.168.0.0/19

inet.0: 15 destinations, 17 routes (15 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.168.0.0/19     *[BGP/170] 00:20:03, localpref 120
                      AS path: 65004 65066 I, validation-state: unverified
                    >  to 10.33.1.6 via ge-0/0/1.0
                    [BGP/170] 00:20:04, localpref 100
                      AS path: 64655 65066 I, validation-state: unverified
                    >  to 10.55.1.1 via ge-0/0/0.0
```

```
@R5_Tokyo> show route 192.168.0.0/19

inet.0: 15 destinations, 18 routes (15 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.168.0.0/19     *[BGP/170] 00:04:53, localpref 120
                      AS path: 65066 I, validation-state: unverified
                    >  to 10.55.1.10 via ge-0/0/4.0
                    [BGP/170] 00:03:53, localpref 120
                      AS path: 65004 65066 I, validation-state: unverified
                    >  to 10.55.1.6 via ge-0/0/2.0
                    [BGP/170] 00:02:16, localpref 100
                      AS path: 64633 65004 65066 I, validation-state:
unverified
                    >  to 10.55.1.2 via ge-0/0/0.0
```

```
R1_Hongkong> show route 192.168.0.0/19

inet.0: 16 destinations, 18 routes (16 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.168.0.0/19     *[BGP/170] 00:20:48, localpref 110
                      AS path: 65004 65066 I, validation-state: unverified
                    >  to 10.4.1.1 via ge-0/0/0.0
                    [BGP/170] 00:20:54, localpref 100
                      AS path: 64633 65004 65066 I, validation-state: unverified
                    >  to 10.33.1.1 via ge-0/0/2.0
```

```
R4_Singapore> show route 192.168.0.0/19

inet.0: 19 destinations, 26 routes (19 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.168.0.0/19     *[BGP/170] 00:18:03, localpref 120
                      AS path: 65066 I, validation-state: unverified
                    >  to 10.4.1.6 via ge-0/0/3.0
                    [BGP/170] 00:18:15, localpref 100
                      AS path: 64655 65066 I, validation-state: unverified
                    >  to 10.55.1.5 via ge-0/0/2.0
```

```
R2_Mumbai> show route 192.168.0.0/19

inet.0: 11 destinations, 12 routes (11 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.168.0.0/19     *[BGP/170] 00:22:36, localpref 100
                      AS path: 65001 65004 65066 I, validation-state: unverified
                    >  to 10.1.1.1 via ge-0/0/3.0
```

Outage Simulation

1) In Normal BGP Routing – No outage

```
R4_Singapore> show bgp summary
…
Peer                 AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn State|#Active/Received/Accepted/Damped...
10.4.1.2             65001      69         67       0       0       29:13 Establ
  inet.0: 2/2/2/0
10.4.1.6             65066      72         79       0       0       31:29 Establ
  inet.0: 1/1/1/0
10.33.1.5            64633      74         68       0       0       29:52 Establ
  inet.0: 1/4/4/0
10.55.1.5            64655      77         72       0       0       31:41 Establ
  inet.0: 1/5/5/0
2406:6004:1::2       65001      68         66       0       0       29:07 Establ
  inet6.0: 2/2/2/0
2406:6004:1::6       65066      73         79       0       0       31:31 Establ
  inet6.0: 0/1/0/0
2406:6433:1::5       64633      74         67       0       0       29:41 Establ
  inet6.0: 1/5/5/0
2406:6455:1::5       64655      77         71       0       0       31:30 Establ
  inet6.0: 2/5/5/0
```

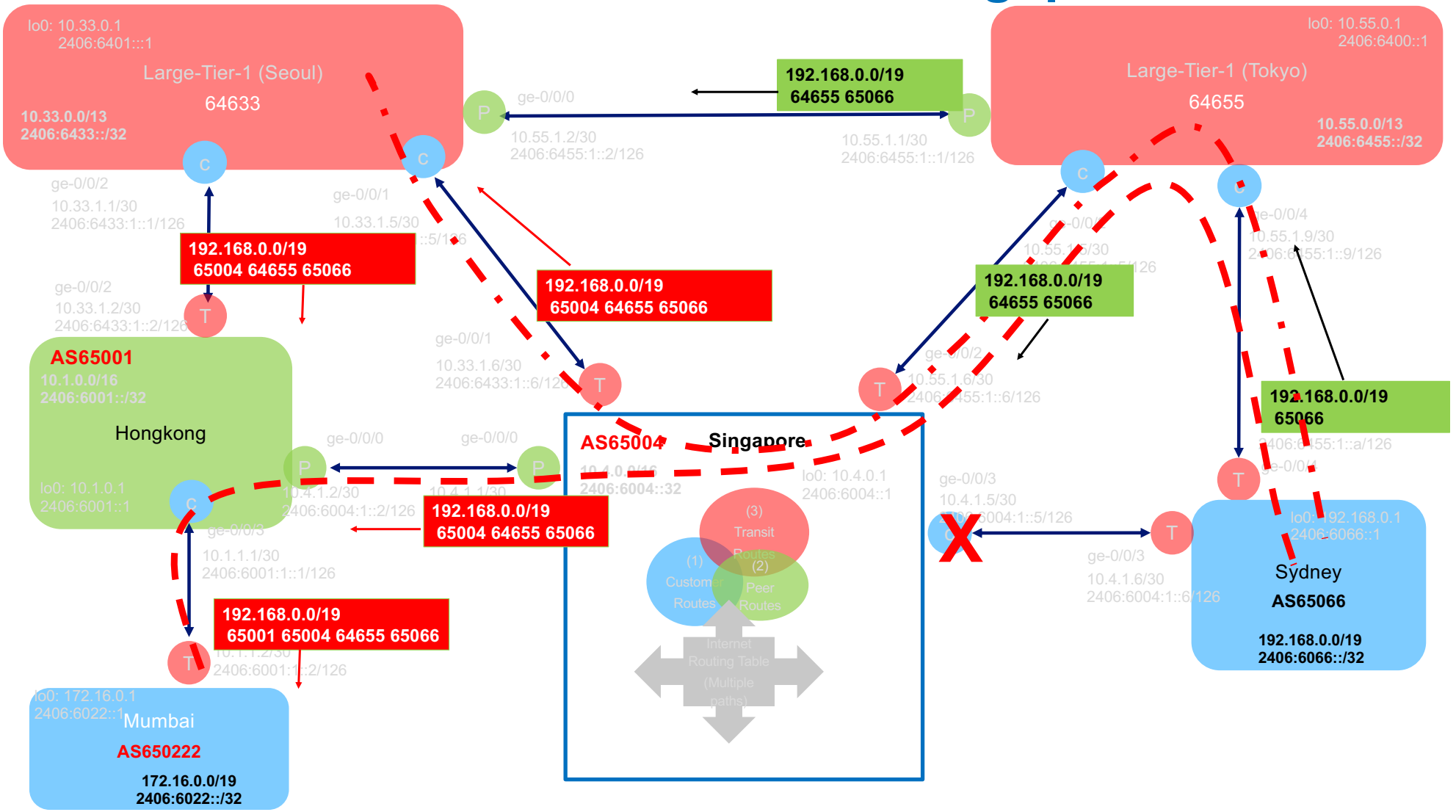
2) Shutting the Singapore – Sydney Link Down:

```
jcluser@R6_Sydney# run show interfaces descriptions
Interface      Admin Link Description
ge-0/0/3       up    up   Connection to R4_Singapore
ge-0/0/4       up    up   Connection to R5_Tokyo
lo0            up    up   *** Loopback ***

[edit]
jcluser@R6_Sydney# set interfaces ge-0/0/3 disable

[edit]
jcluser@R6_Sydney# top commit
commit complete

[edit]
jcluser@R6_Sydney# run show interfaces descriptions
Interface      Admin Link Description
ge-0/0/3       down  down Connection to R4_Singapore
ge-0/0/4       up    up   Connection to R5_Tokyo
lo0            up    up   *** Loopback ***
```

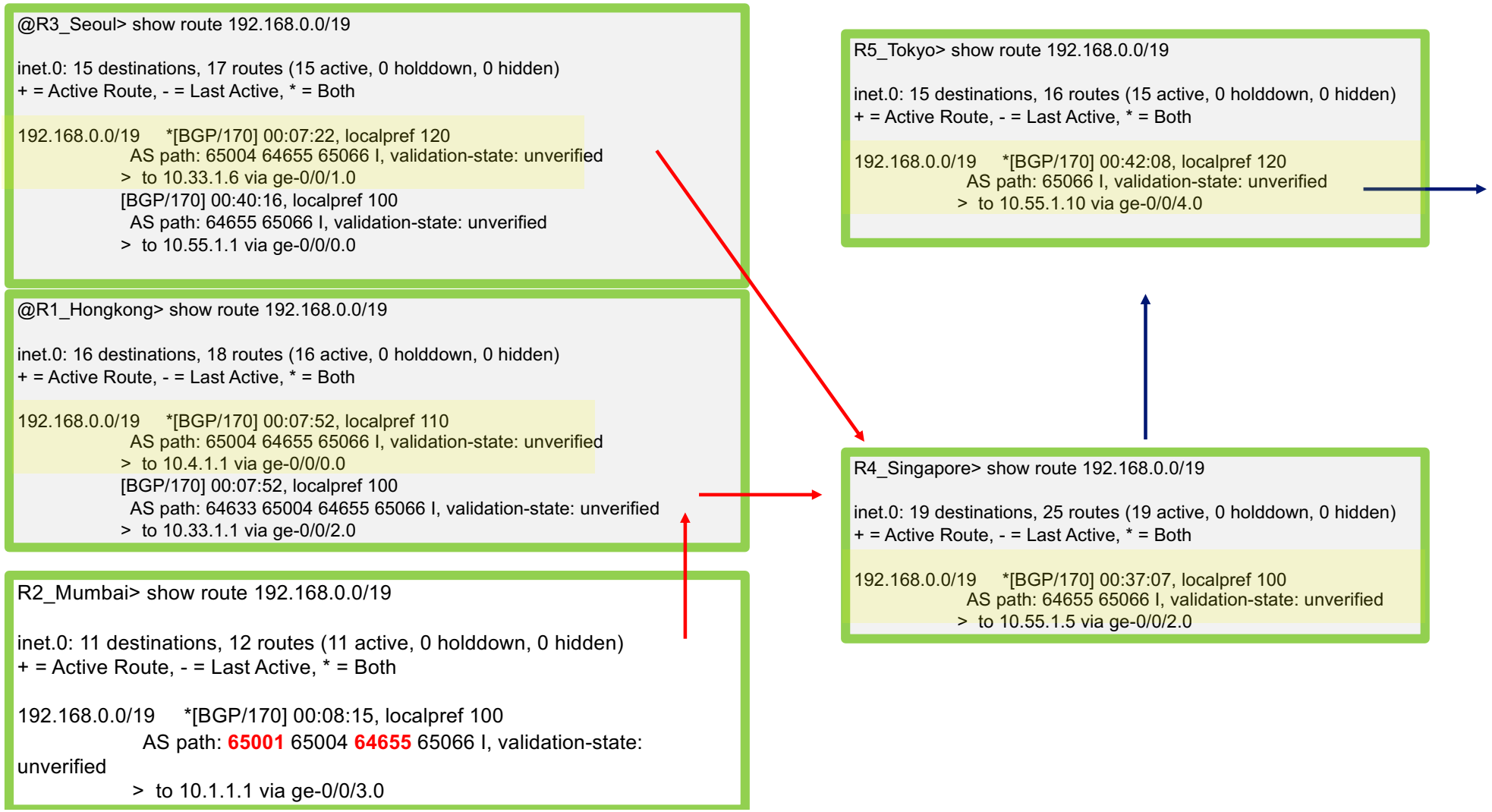
3) Singapore – has Sydney Route via Upstream AS64655

```
jcluser@R4_Singapore> show bgp summary | match 65066
10.4.1.6             65066          0          0       0       1        1:49 Connect
2406:6004:1::6       65066          0          0       0       1        1:25 Connect

jcluser@R4_Singapore> show route 192.168.0.0/19

inet.0: 19 destinations, 25 routes (19 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.168.0.0/19     *[BGP/170] 00:37:07, localpref 100
                      AS path: 64655 65066 I, validation-state: unverified
                    >  to 10.55.1.5 via ge-0/0/2.0
```

Route Leak occurred at Singapore AS



Active Routing table to prefix 192.168.0.0/19



Active Routing table to prefix 192.168.0.0/19

Routing at Mumbai Router seeing 192.169.0.0/19 via leak path

```
jcluser@R2_Mumbai> show route 192.168.0.0/19

inet.0: 11 destinations, 12 routes (11 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.168.0.0/19     *[BGP/170] 00:03:28, localpref 100
                      AS path: 65001 64633 65004 64655 65066 I, validation-state: unverified
                    >  to 10.1.1.1 via ge-0/0/3.0
```

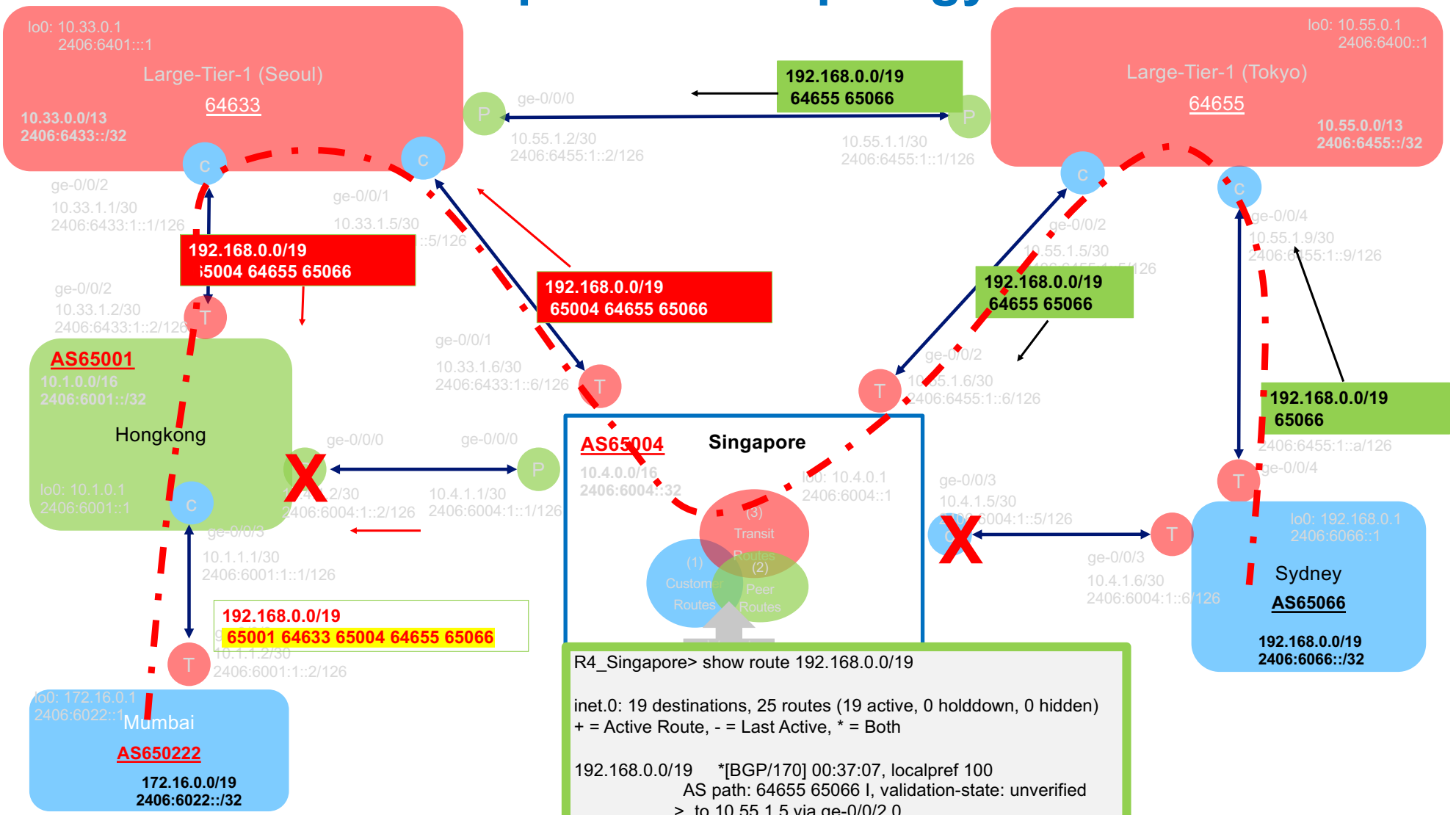
When the Hongkong– Singapore Link outage

```
@R2_Mumbai> traceroute 192.168.0.1 as-number-lookup
traceroute to 192.168.0.1 (192.168.0.1), 30 hops max, 52 byte packets
 1  10.1.1.1 (10.1.1.1) [AS  65001]  3.063 ms  1.820 ms  1.660 ms
 2  10.33.1.1 (10.33.1.1) [AS  64633]  2.389 ms  2.160 ms  2.815 ms
 3  10.33.1.6 (10.33.1.6) [AS  64633]  3.531 ms  2.731 ms  3.074 ms
 4  10.55.1.5 (10.55.1.5) [AS  64655]  9.671 ms  8.081 ms  3.615 ms
 5  192.168.0.1 (192.168.0.1) [AS  65066]  8.085 ms  4.773 ms  4.622 ms
```

```
R1_Hongkong# run show interfaces descriptions
Interface       Admin Link Description
ge-0/0/0        up    up   Connection to R4_Singapore
ge-0/0/2        up    up   Connection to R3_Seoul
ge-0/0/3        up    up   Connection to R2_Mumbai
lo0             up    up   *** Loopback ***

[edit]

jcluser@R1_Hongkong# set interfaces ge-0/0/0 disable

[edit]
jcluser@R1_Hongkong# top commit
commit complete

[edit]
jcluser@R1_Hongkong# run show bgp summary | match 65004
10.4.1.1            65004        103        103       0       1          26 Idle
2406:6004:1::1      65004        102        103       0       1          26 Idle
```

```
R1_Hongkong# run show bgp summary | match 65004
10.4.1.1            65004        103        103       0       1          26 Idle
2406:6004:1::1      65004        102        103       0       1          26 Idle

[edit]
jcluser@R1_Hongkong# run show route 192.168.0.0/19

inet.0: 15 destinations, 15 routes (15 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.168.0.0/19     *[BGP/170] 00:14:35, localpref 100
                      AS path: 64633 65004 64655 65066 I, validation-state: unverified
                    >  to 10.33.1.1 via ge-0/0/2.0
```

Juniper vLab Topology



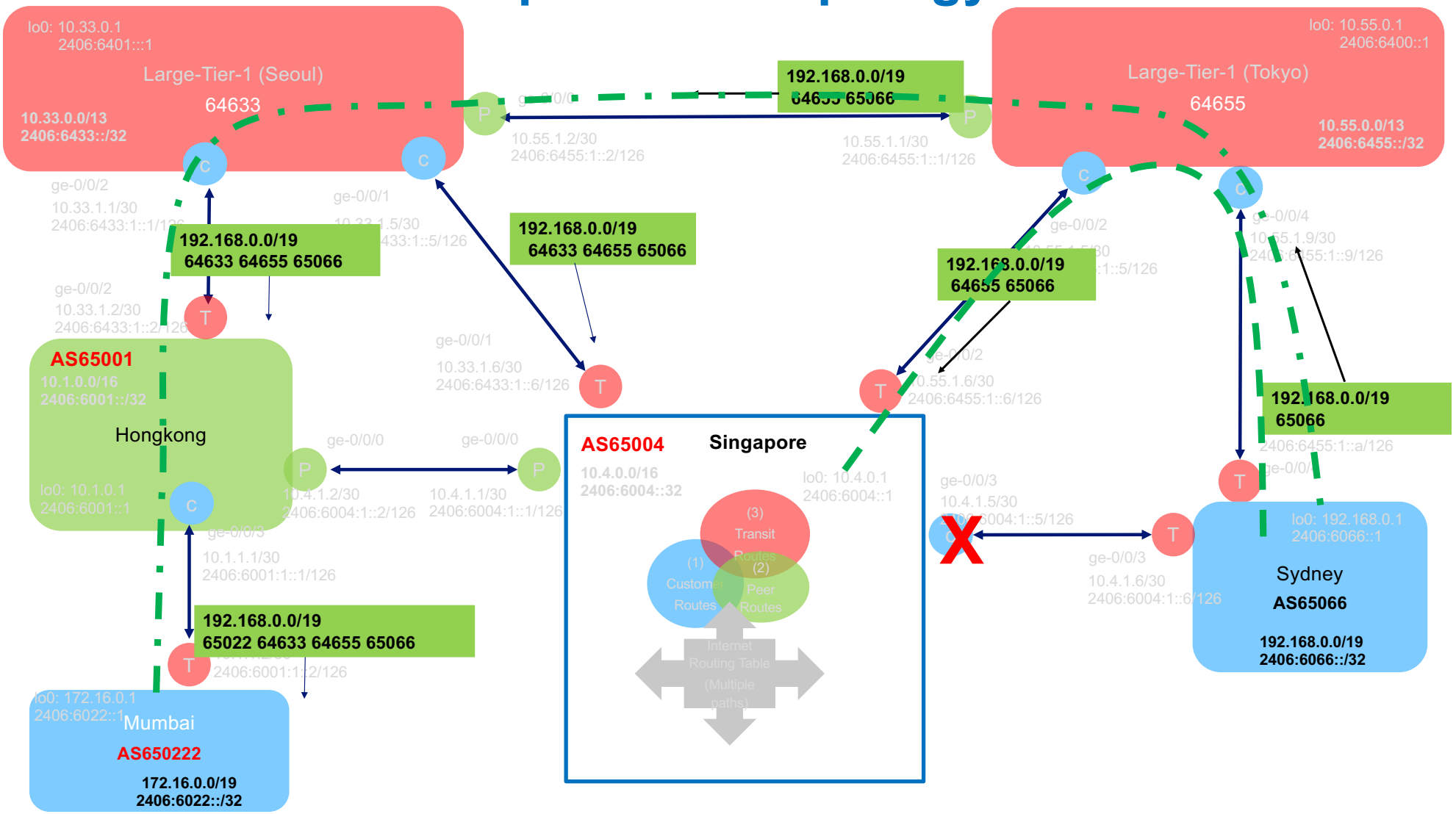
```
R4_Singapore# run show configuration protocols bgp group eBGP-to-transits
type external;
export [ lock-peer-out drop-bogons static-or-connected next-hop-self final-filter ];
neighbor 10.55.1.5 {
    description "Transit AS64655 Tokyo";
    import [ drop-bogons AS64655-route-mark set-transit-in final-filter ];
    export [ lock-peer-out drop-bogons static-or-connected AS64655-v4-transit-out next-hop-
self ];
    peer-as 64655;
}
```

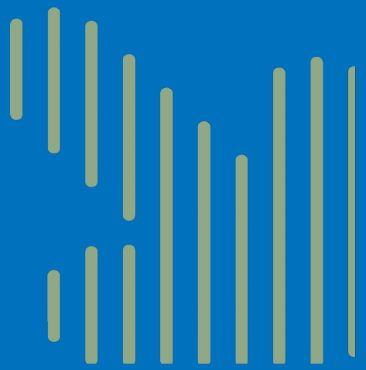
```
@R4_Singapore# show policy-options policy-statement set-transit-in
term set-transit {
    from community comm-transit;
    then {
        local-preference 100;
        next policy;
    }
}

R4_Singapore# show policy-options community comm-transit
members 65004:333
```

```
R4_Singapore# show policy-options policy-statement lock-peer-out
term deny {
    from community [ comm-peer comm-transit ];
    then reject;
}
then next policy;
```

```
@R4_Singapore# run show route 192.168.0.0/19 detail

inet.0: 19 destinations, 26 routes (19 active, 0 holddown, 0 hidden)
192.168.0.0/19 (2 entries, 1 announced)
        *BGP    Preference: 170/-101
                Next hop type: Router, Next hop index: 625
                Address: 0xc4b5d54
                Next-hop reference count: 7
                Source: 10.55.1.5
                Next hop: 10.55.1.5 via ge-0/0/2.0, selected
                Session Id: 0x140
                State: <Active Ext>
                Local AS: 65004 Peer AS: 64655
                Age: 1:18:54
                Validation State: unverified
                Task: BGP_64655.10.55.1.5
                Announcement bits (2): 0-KRT 3-Resolve tree 3
                AS path: 64655 65066 I
                Communities: 65004:333 65004:64655
                Accepted
                Localpref: 100
                Router ID: 10.55.0.1
                Thread: junos-main
        BGP     Preference: 170/-101
                Next hop type: Router, Next hop index: 581
                Address: 0xc4b63d4
                Next-hop reference count: 6
                Source: 10.33.1.5
                Next hop: 10.33.1.5 via ge-0/0/1.0, selected
                Session Id: 0x143
                State: <Ext Changed>
                Inactive reason: AS path
                Local AS: 65004 Peer AS: 64633
                Age: 2:32
                Validation State: unverified
                Task: BGP_64633.10.33.1.5
                AS path: 64633 64655 65066 I
                Communities: 65004:333 65004:64633
                Accepted
                Localpref: 100
                Router ID: 10.33.0.1
                Thread: junos-main
```

Juniper vLab Topology





Hands-on: BGPQ4

Bgpq4 example:

IPv4 exact-match filter from AS-SET

```
bgpq4 -Jl AS23918-exact-in AS23918:AS-GLOBAL
policy-options {
replace:
 prefix-list AS23918-exact-in {
…..
```

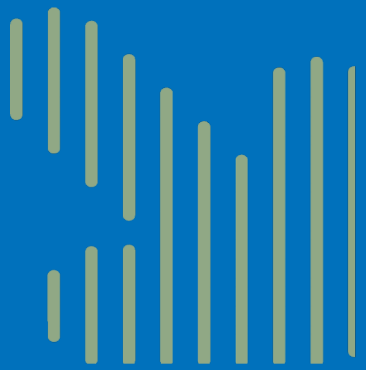
IPv6 exact-match filter from AS-SET

```
 bgpq4 -J6l AS23918v6-exact-in AS23918:AS-GLOBAL
policy-options {
replace:
 prefix-list AS23918v6-exact-in {
…..
```

For Cisco we can use aggregation (-A) flag to make this prefix-filter more compact:

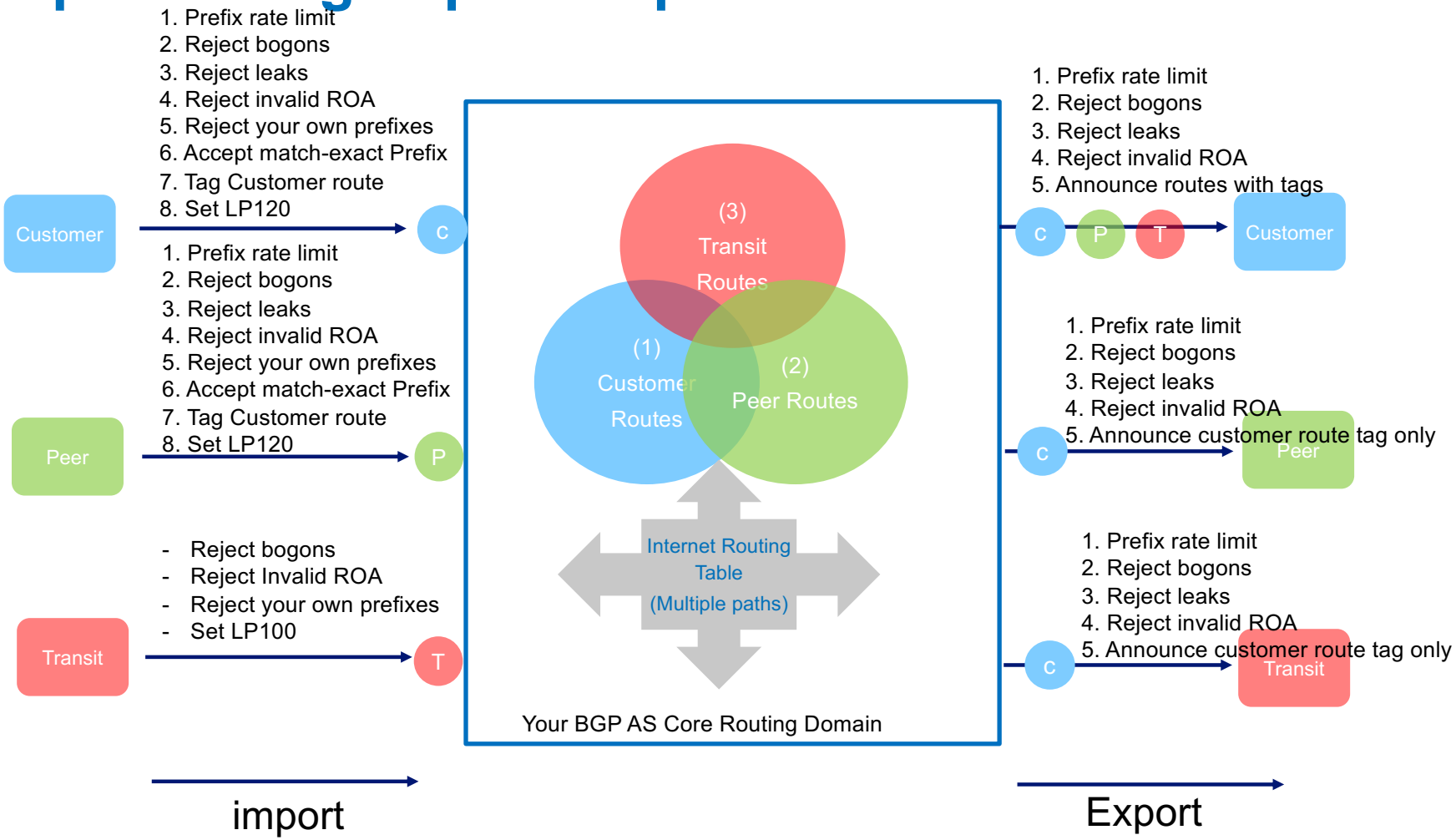
```
bgpq4 -Al AS23918-in AS23918:AS-GLOBAL
no ip prefix-list AS23918-in
ip prefix-list AS23918-in permit 5.187.16.0/20
…..
```

```
bgpq4 -A6l AS23918v6-in AS23918:AS-GLOBAL
no ipv6 prefix-list AS23918v6-in
ipv6 prefix-list AS23918v6-in permit
2401:4700:3000::/48
```

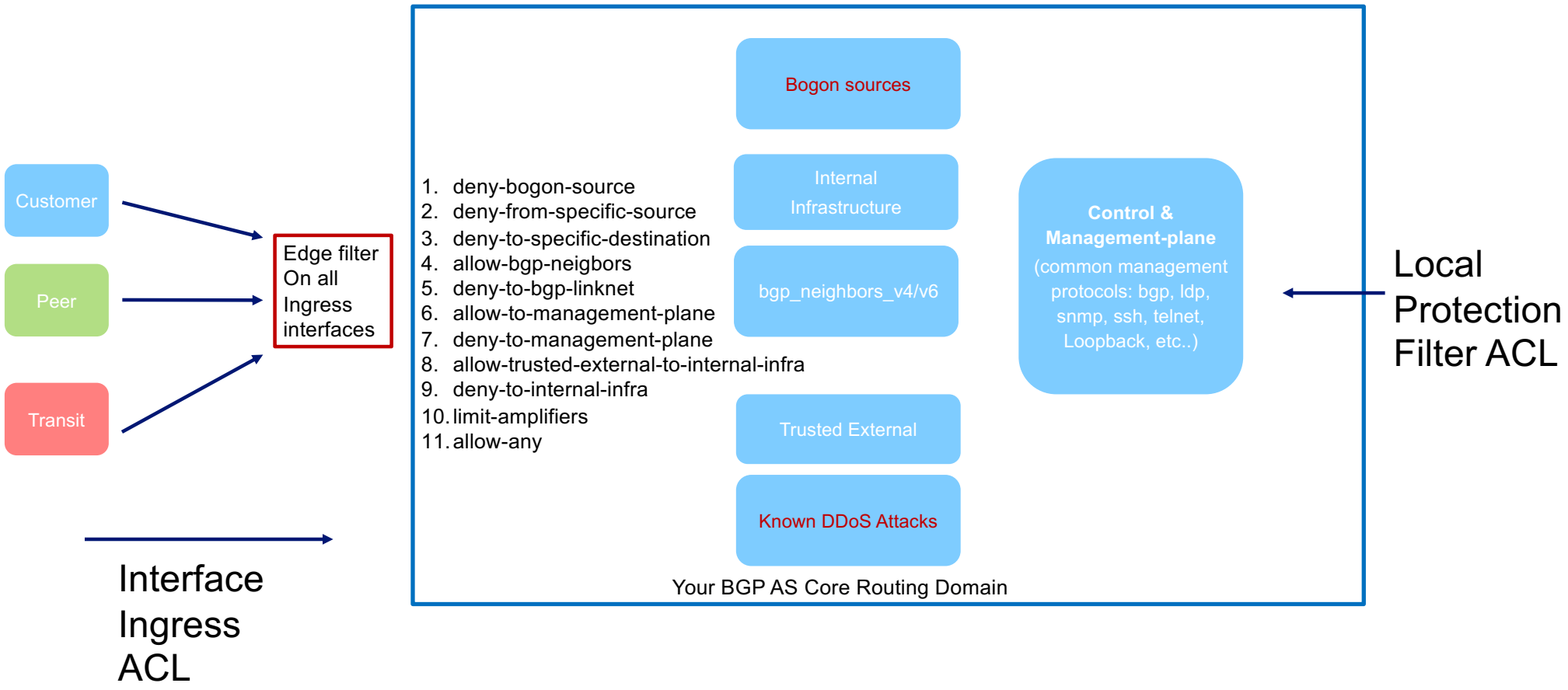


BGP Alerter

Recap: Routing Import/Export Policies



Recap: ACL Core Protection



Secure Internet Routing – is your eBGP filter up-to-date?

Inbound Filter Checklist

	Ingress	Customer	Peer	Transit
1	A max-prefix Limit + 10% for growth	✓	✓	✓
2	Reject You Own Prefixes	✓	✓	✓
3	Reject Bogon Prefixes	✓	✓	✓
4	Reject Default Routes	✓	✓	✓
5	Reject Bogon ASN	✓	✓	✓
6	rpki validation	✓	✓	✓
7	Lock Large Transit AS-PATH Leaks	✓	✓	NA
8	Accept only /24 IPv4, /48 IPv6 or Shorter	NA	✓	✓
9	Accept valid Prefixes against IRR/ROA Validation	✓	✓	✓
10	Mark route-type with BGP communities	Cust-route	Peer-route	Transit-route
11	Apply BGP features: blackholing, traffic engineering, etc	✓	NA	NA
12	Enable MD5 Session Authentication	✓	✓	✓

Outbound Filter Checklist

	Egress	Customer	Peer	Transit
1	Remove Private AS	✓	✓	✓
2	Reject Bogon prefixes	✓	✓	✓
3	Reject Default Routes		✓	✓
4	Reject Bogon ASN	✓	✓	✓
5	Lock Large Transit AS-PATH Leaks	NA	✓	✓
6	Accept only /24 IPv4, /48 IPv6 or Shorter	NA	✓	✓
7	Accept valid Prefixes against IRR/ROA Validation	✓	✓	✓
8	Match Cust-route comm tags	Allow	Allow	Allow
9	Match Peer-route, Transit-route comm tags	✓	Reject	Reject
10	Apply BGP features: as-prepend, etc..	✓	✓	✓
11	Reject Any	✓	✓	✓

Tools and Reference Sites

https://tryhackme.com/hacktivities#network-rooms

https://www.shodan.io

https://nvd.nist.gov/vuln/detail/CVE-2021-23017

https://isc.sans.edu/podcastdetail.html?id=8392

https://bgpstream.crosswork.cisco.com/

https://lg.ring.nlnog.net/

https://packetvis.com/

https://github.com/lambinh/2023_TechnicalWorkshop

https://github.com/lambinh/netsec-training

Thank you!