ReDAN: An Empirical Study on Remote DoS Attacks against NAT Networks

Xuewei Feng*, **Yuxiang Yang***, Qi Li*†, Xingxiang Zhan†, Kun Sun‡, Ziqiang Wang§, Ao Wang§, Ganqiu Du¶, Ke Xu*†

*

†

‡

§

¶

Overview

Threat Model

Background

Attack Procedure

Empirical Study

Disclosure and Mitigation

Conclusion

Threat Model

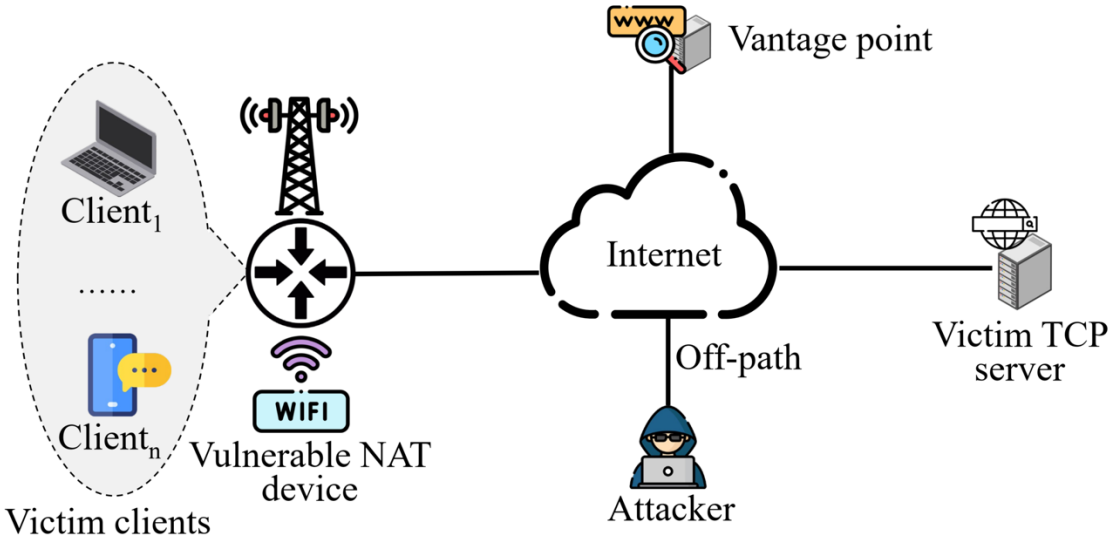
Threat Model

Consists of:

- An arbitrary victim TCP **server**
- A vulnerable **NAT device**
  - Wireless router in Wi-Fi networks
  - PDN gateway or UPF in 4G LTE/5G networks
  - a CPE gateway in IoT networks.
- A victim **client** behind the NAT device
- An off-path **attacker** capable of IP spoofing
- A **vantage point** accessible to the victim

The attacker can:

- **Identify** whether the client is behind NAT
- Launch TCP **Denial of Service (DoS)** attacks



Background

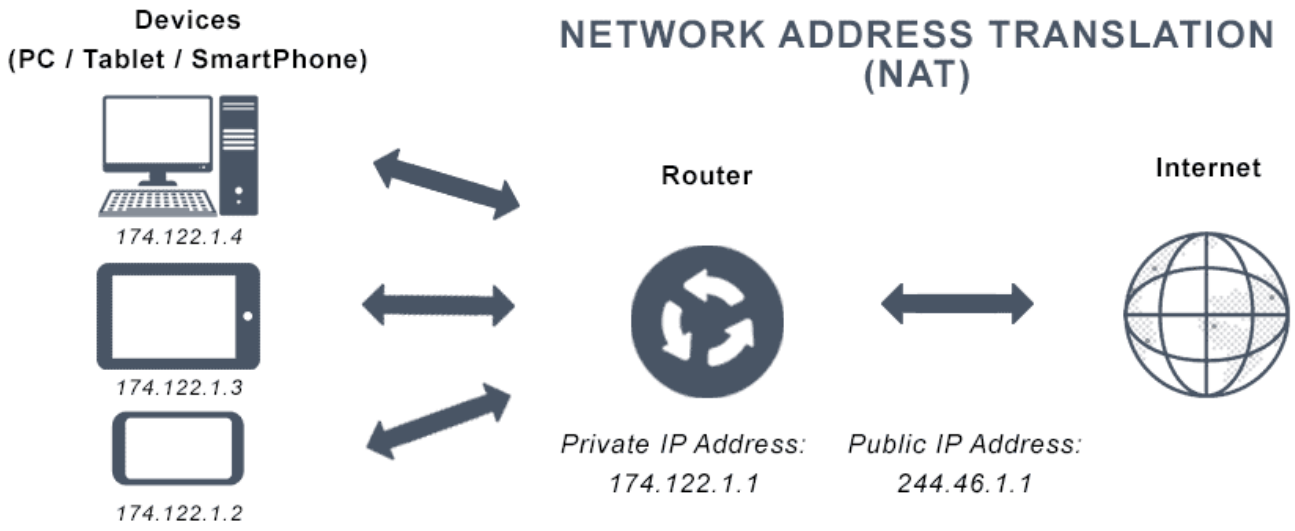
Network Address Translation (NAT)

What is NAT?

- Maps private IPs to public IPs
- Enables shared Internet among devices
- Mitigates IPv4 address exhaustion

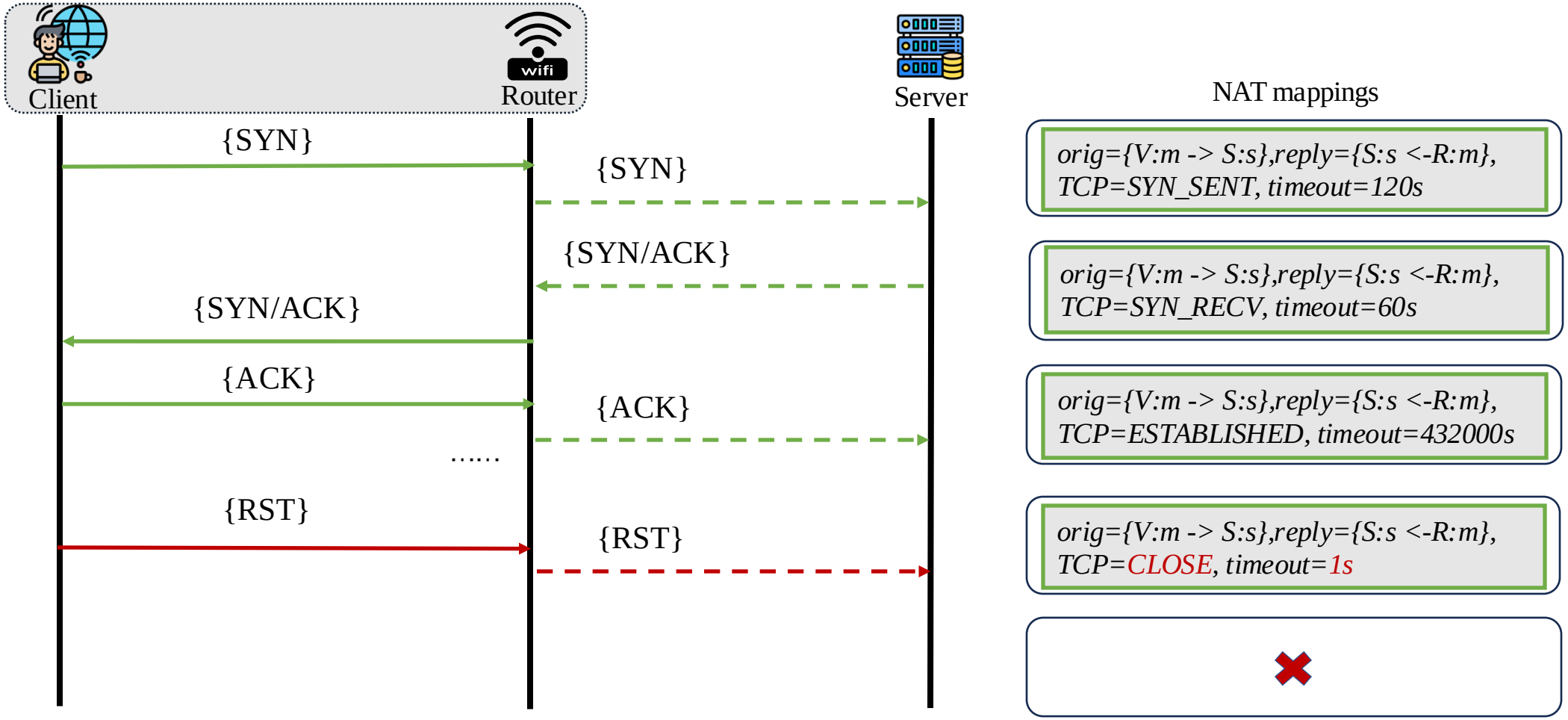
NAT Functionality

- IP Conservation: Saving public IPs.
- Security: Hides internal structure,
  Prevents direct access.



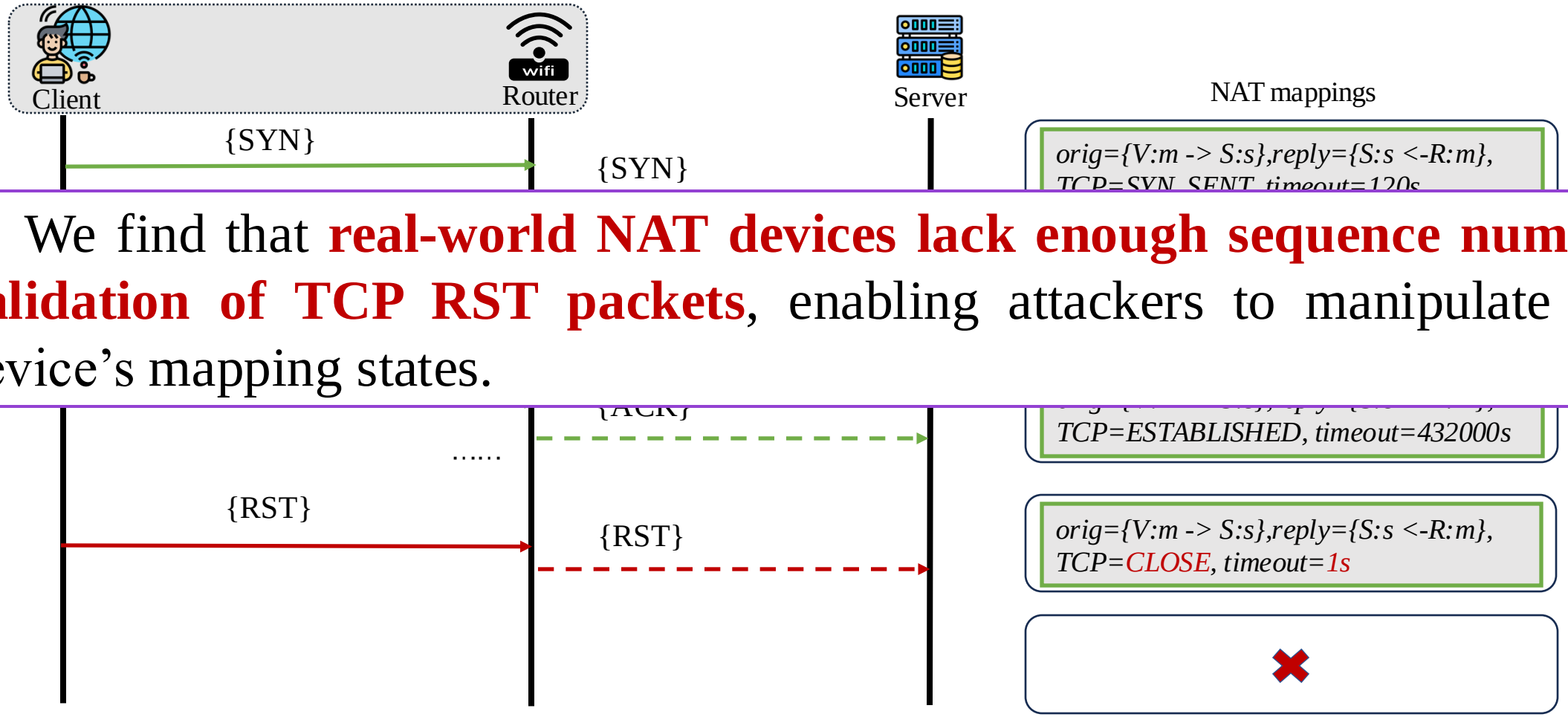
Session Mapping Tables in NAT

The key to NAT's operation is session mapping table.



Session Mapping Tables in NAT

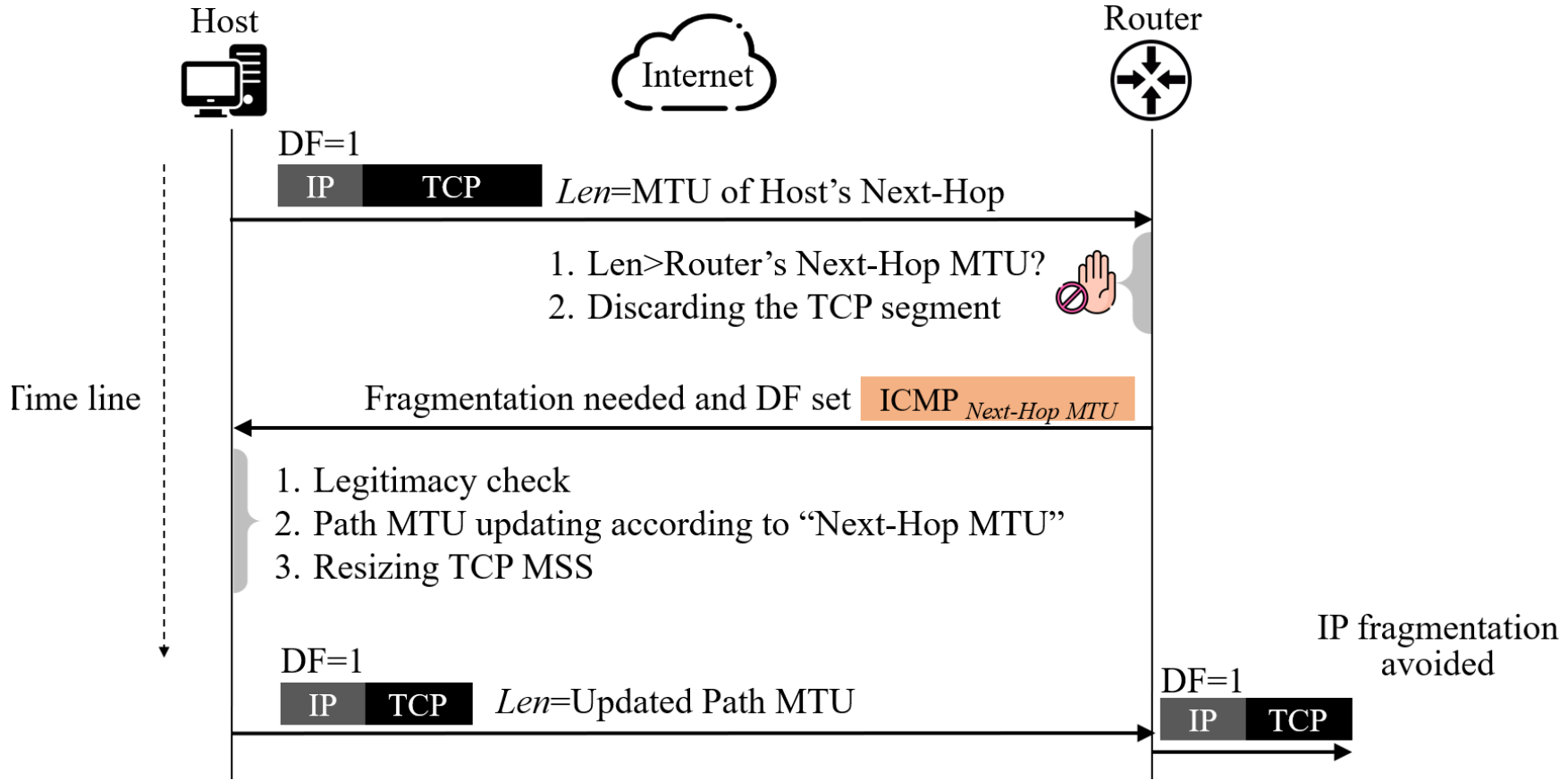
The key to NAT's operation is session mapping table.



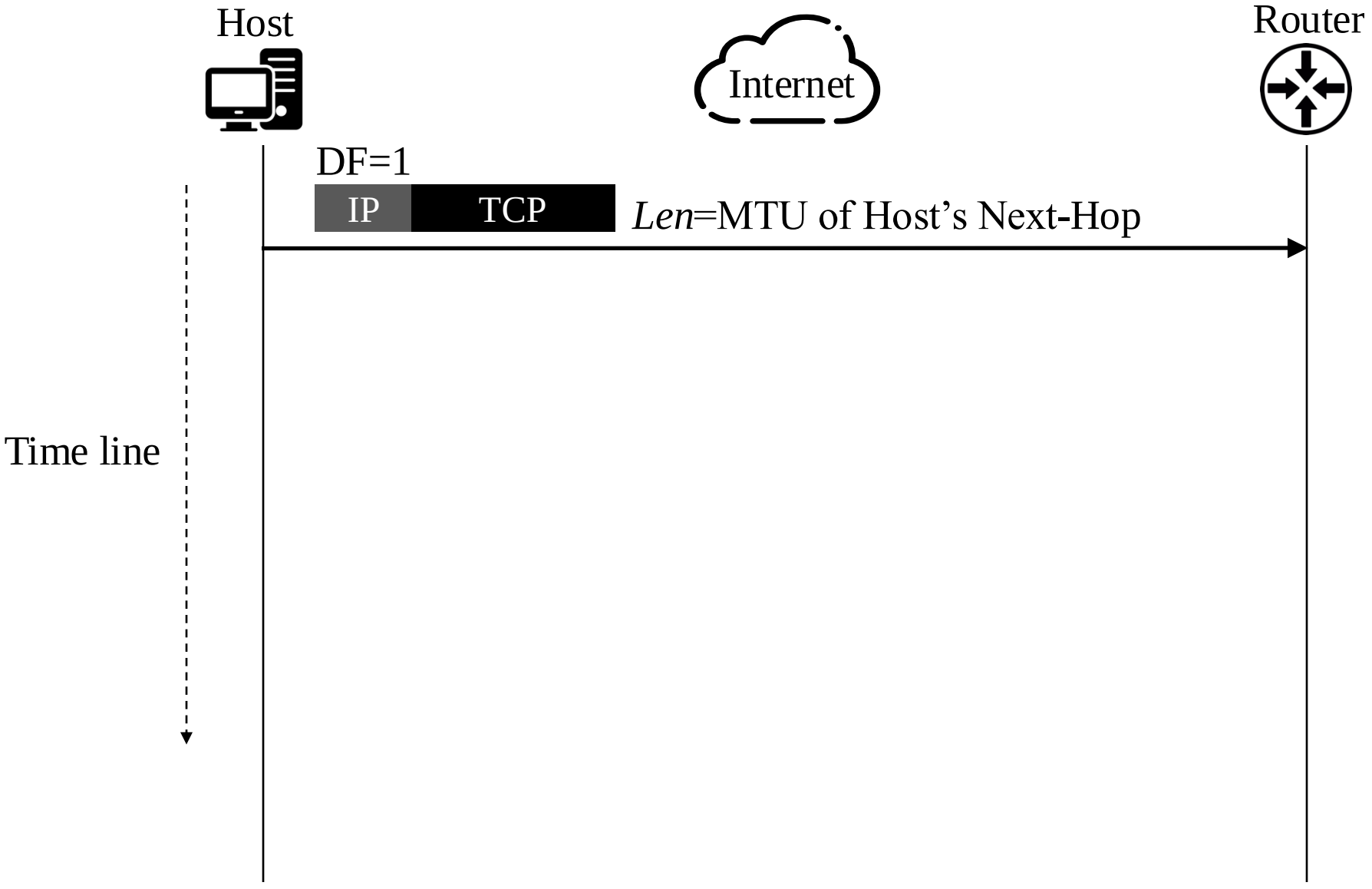
We find that **real-world NAT devices lack enough sequence number validation of TCP RST packets**, enabling attackers to manipulate the device's mapping states.

Path MTU Discovery (PMTUD)

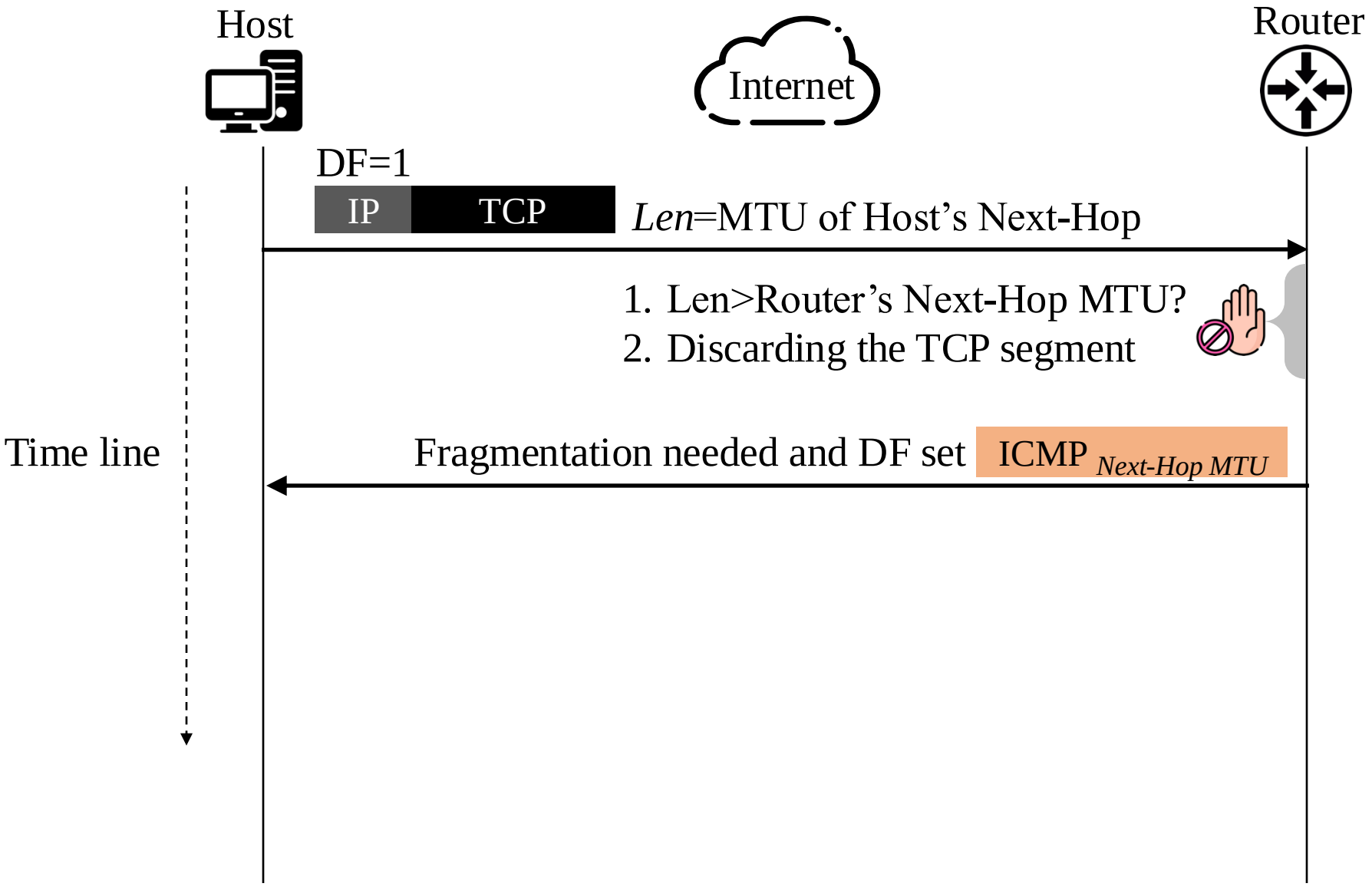
PMTUD is designed to **prevents IP fragmentation** by dynamically determining the maximum packet size supported along a network path.



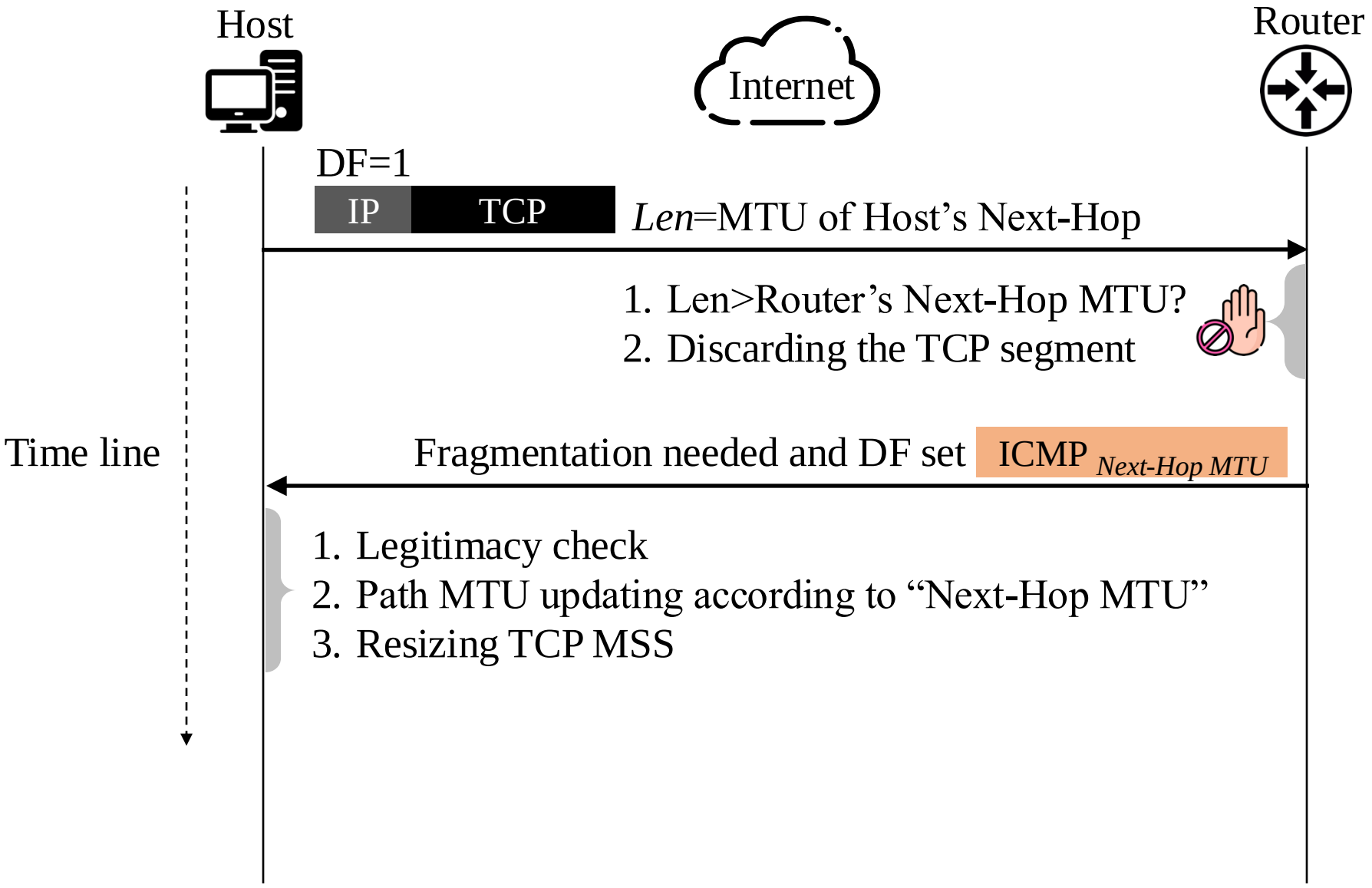
Path MTU Discovery (PMTUD)



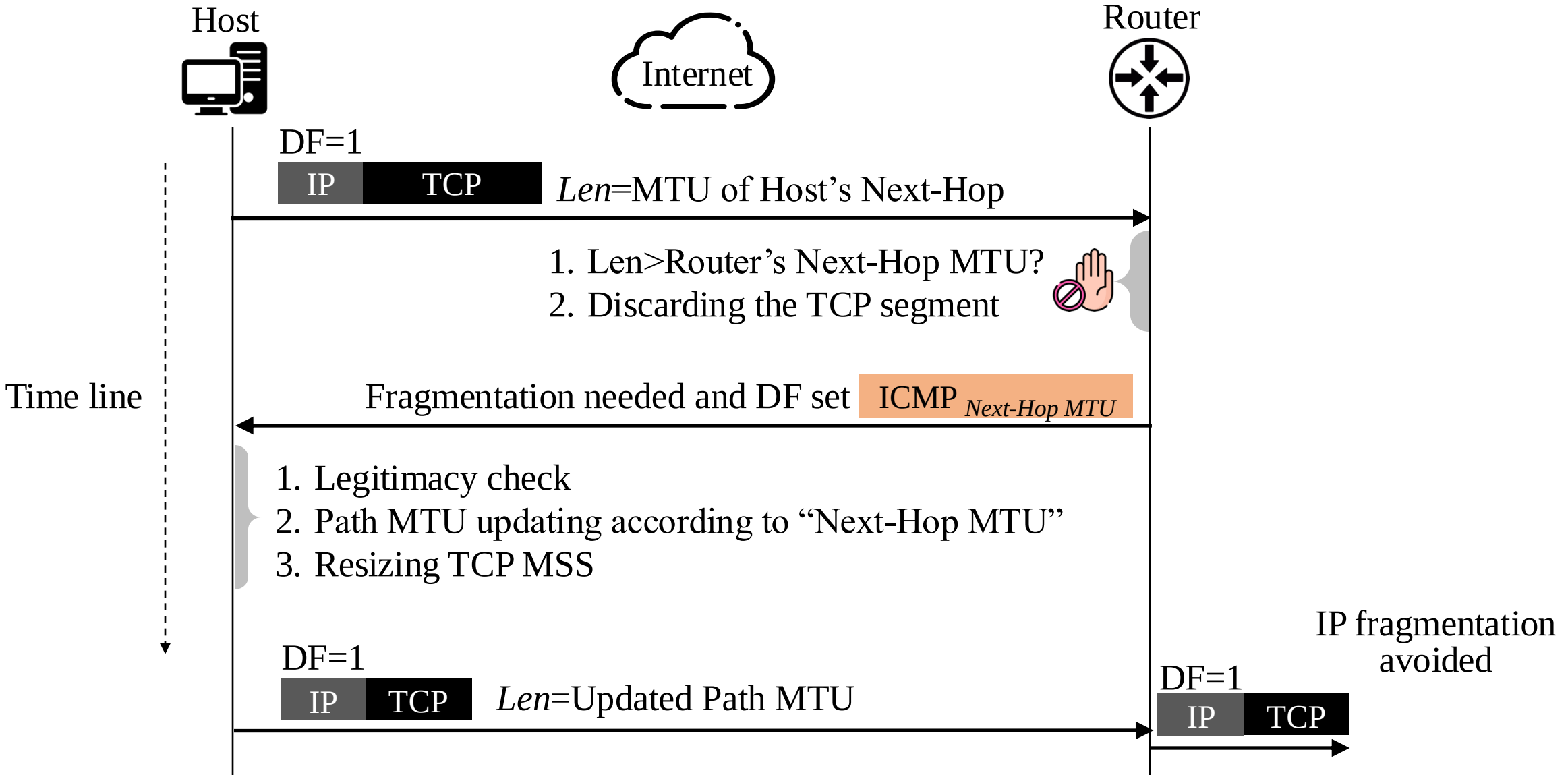
Path MTU Discovery (PMTUD)



Path MTU Discovery (PMTUD)



Path MTU Discovery (PMTUD)



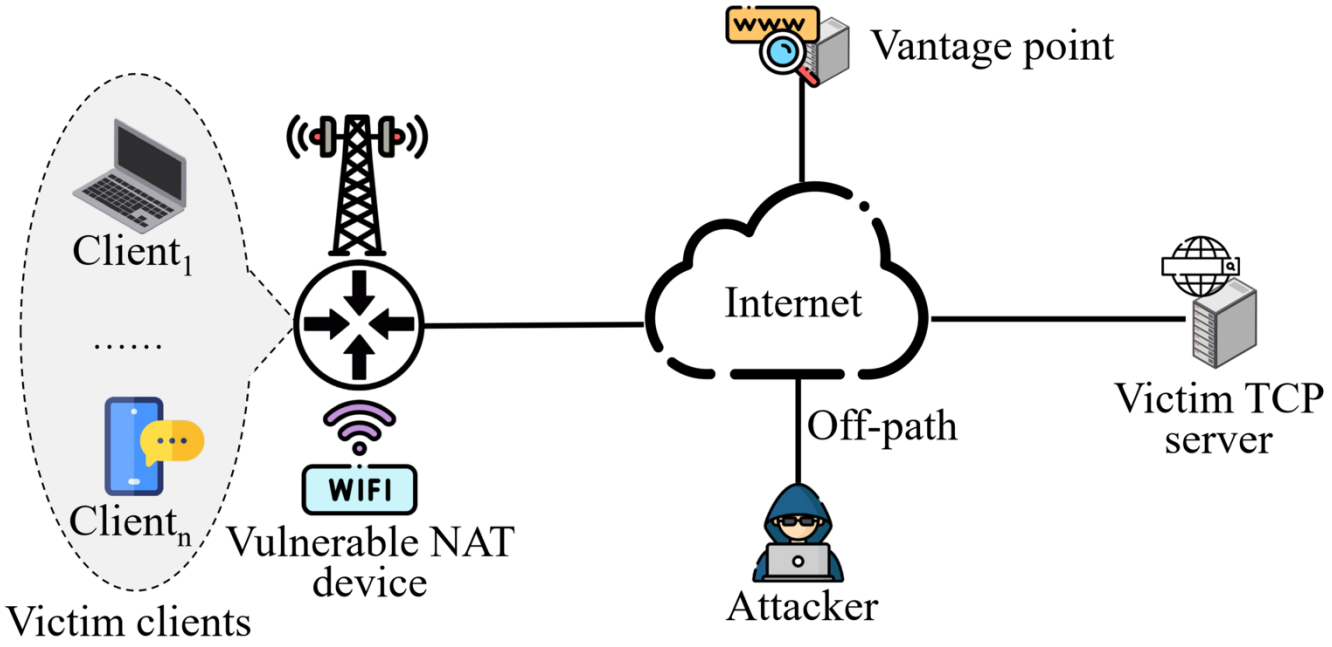
ATTACK PROCEDURE

Attack Overview

We show that off-path attacker posses the capability to **remotely identify a NAT device** and **terminate TCP connections** initiated from the device.

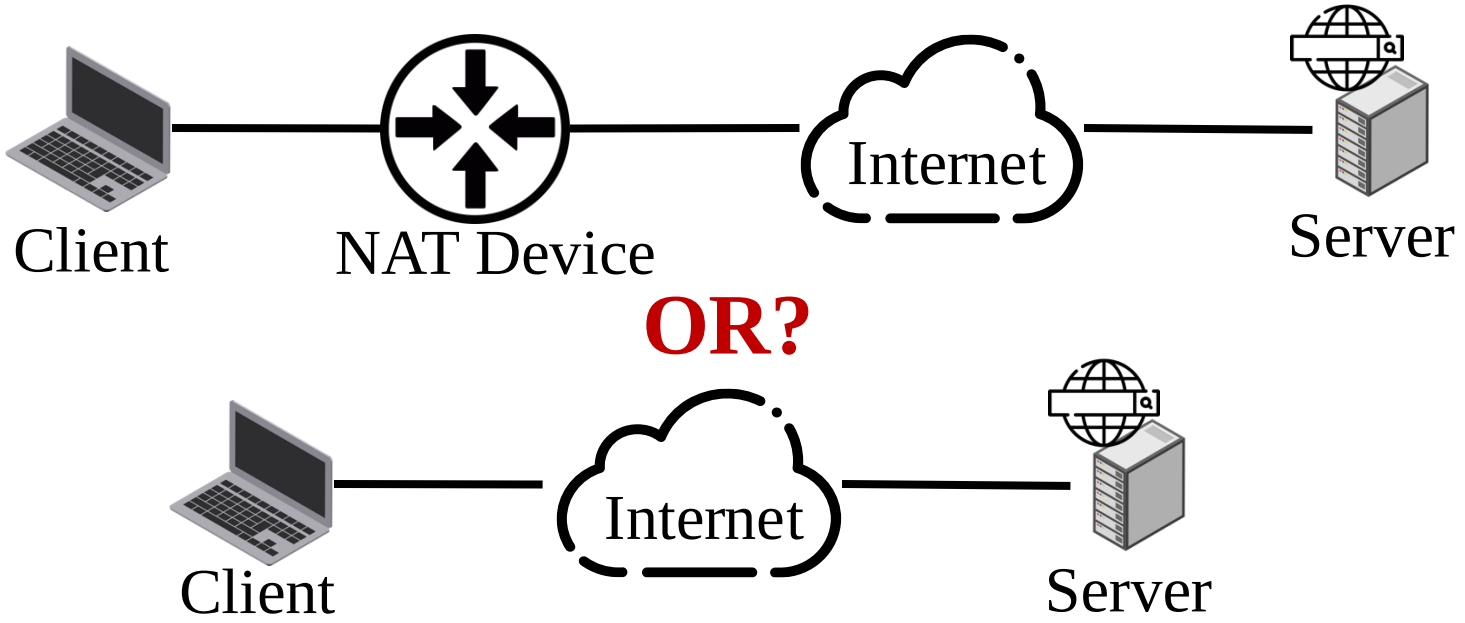
Attack Steps：

- Step 1: Identifying NAT Devices. (Leveraging a new side channel.)
- Step 2: Conducting DoS Attacks. (By crafting RST packets.)



Step 1: Identifying NAT Devices

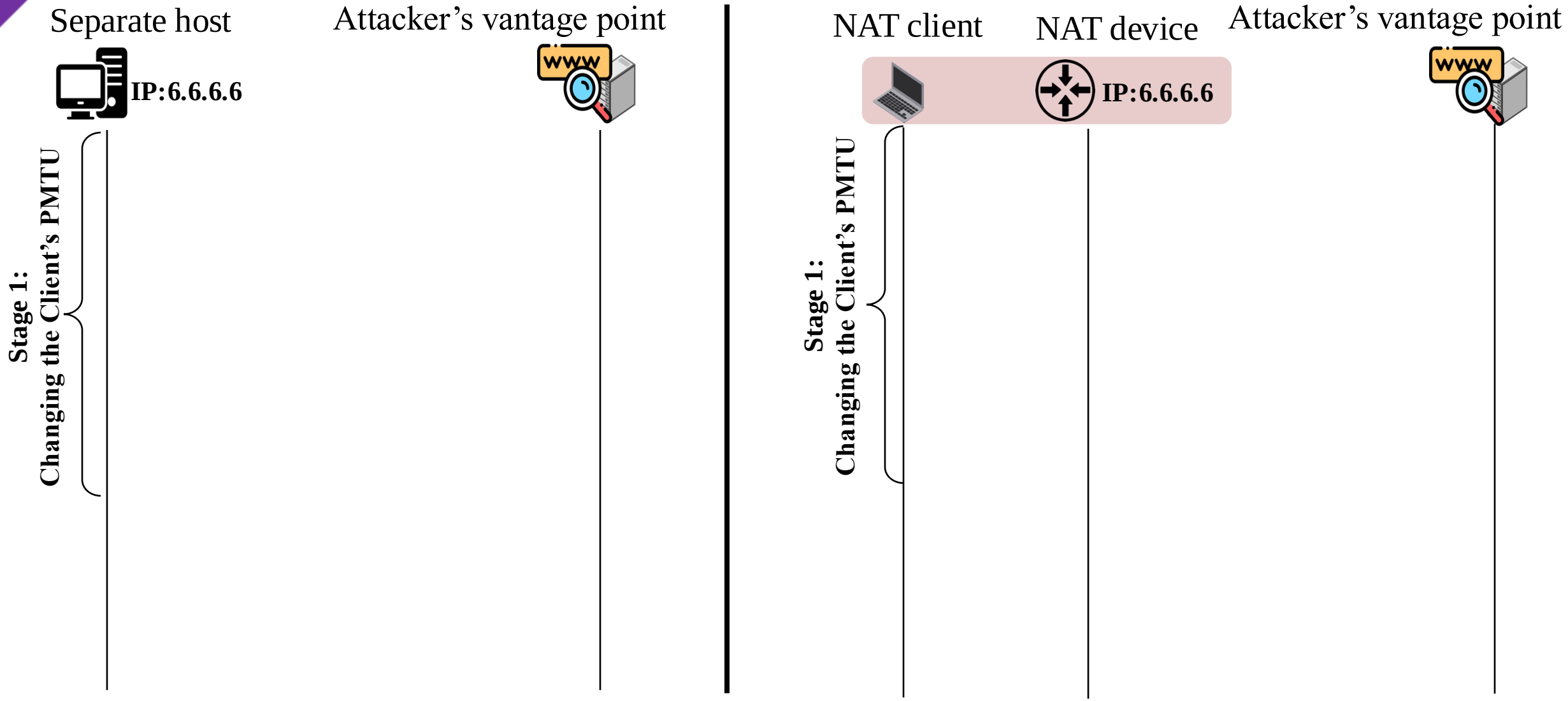
Goal: Determine if a specific target host is behind a NAT device.



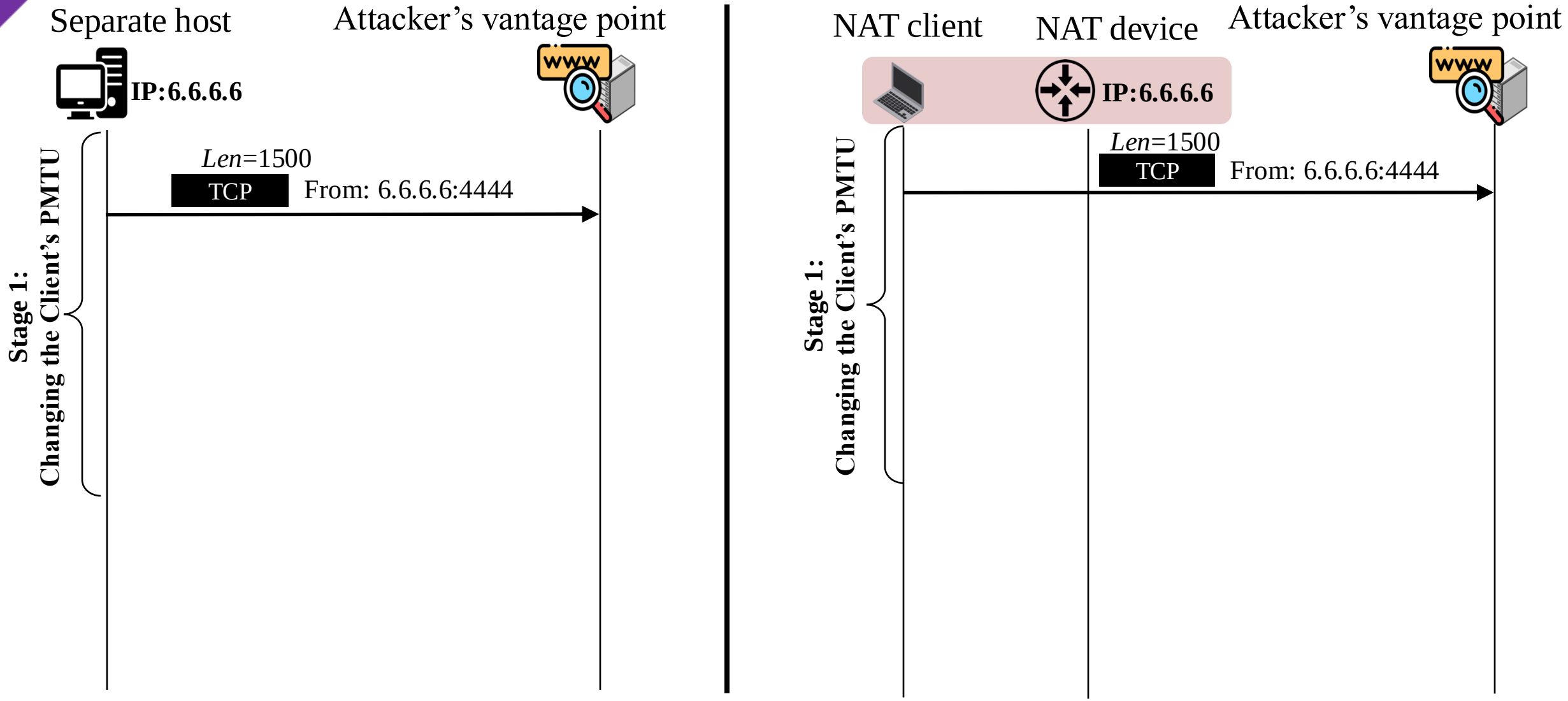
By a new side channel:

- Leveraging **discrepancies in Path MTU values** between NAT devices and internal clients.

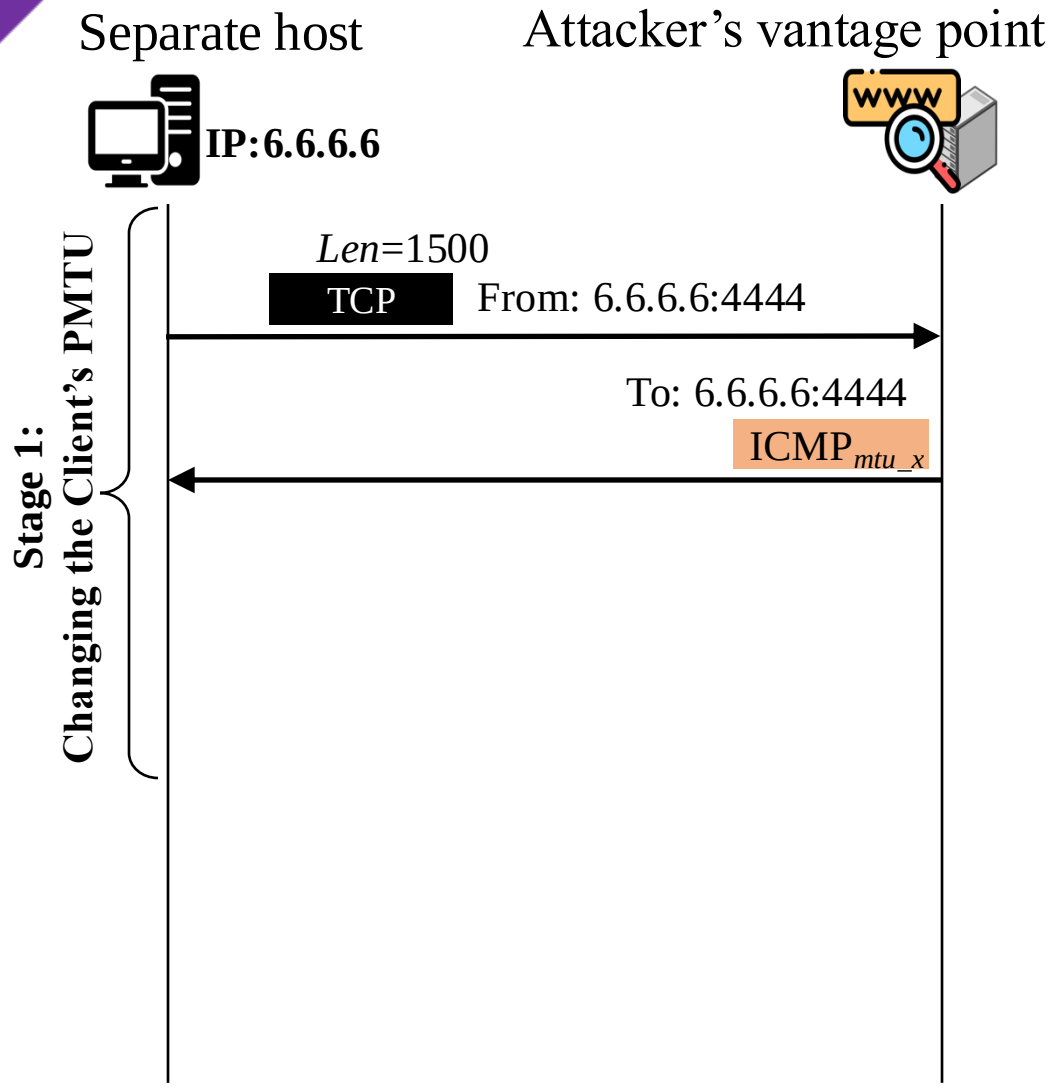
Changing Client's Path MTU

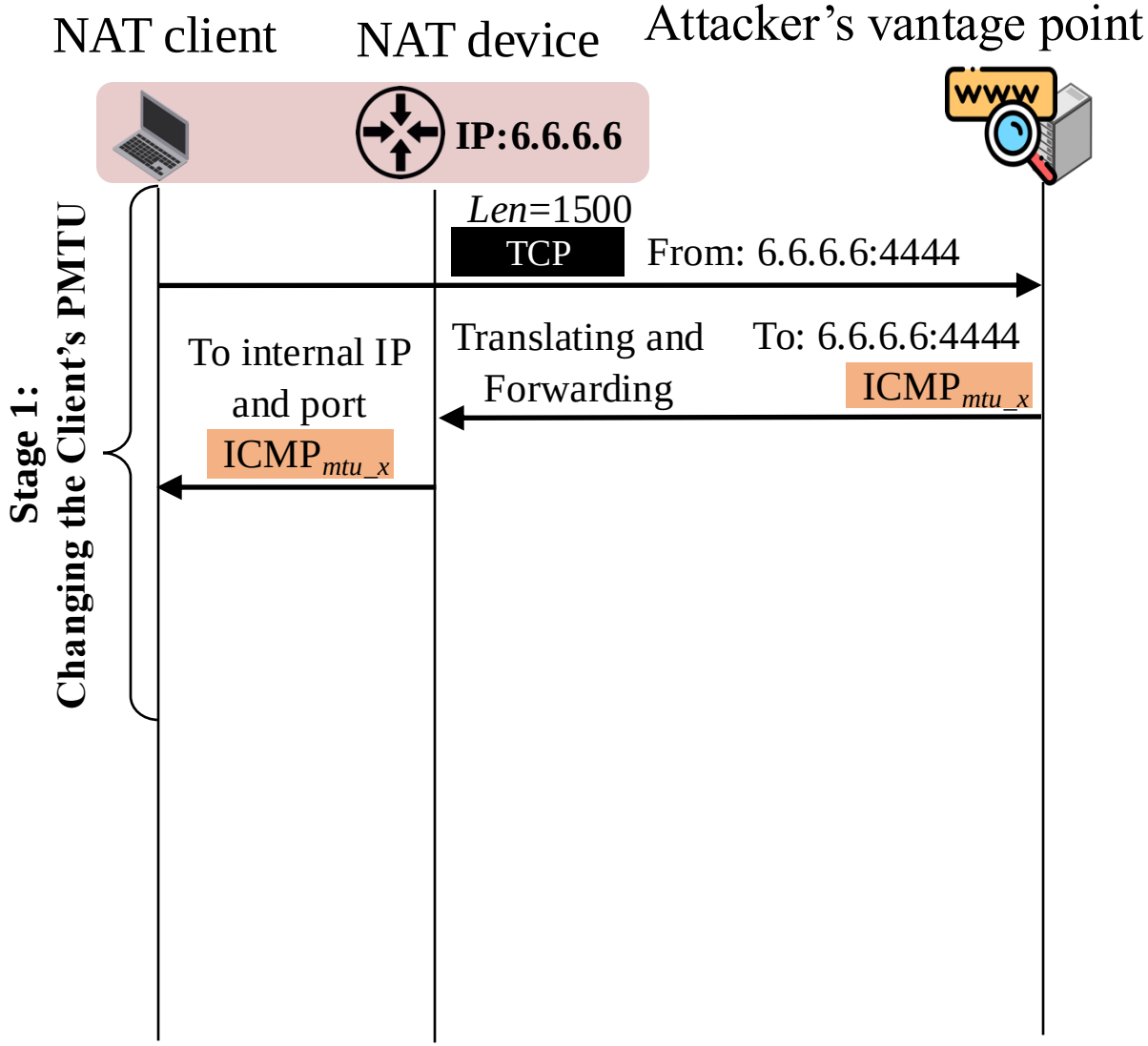


Changing Client's Path MTU

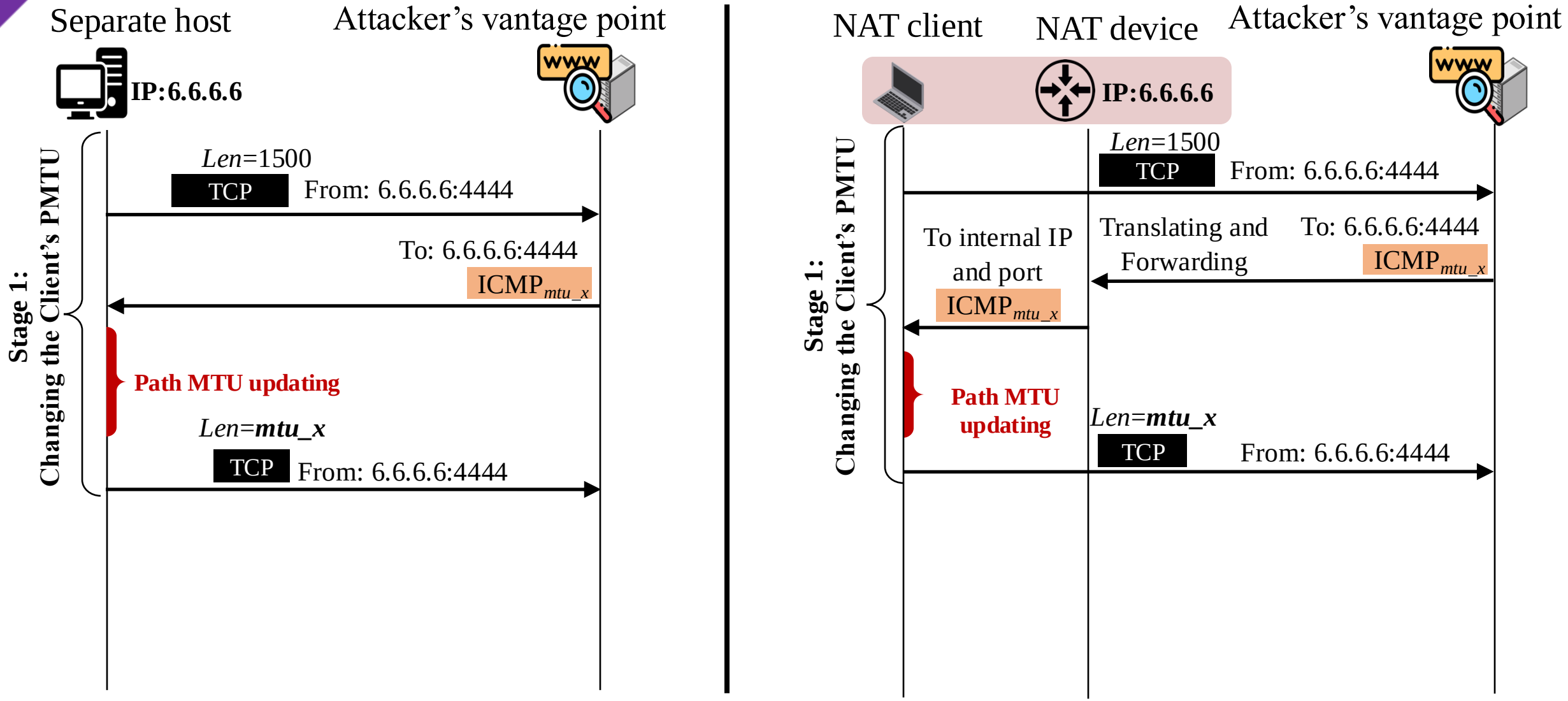


Changing Client's Path MTU

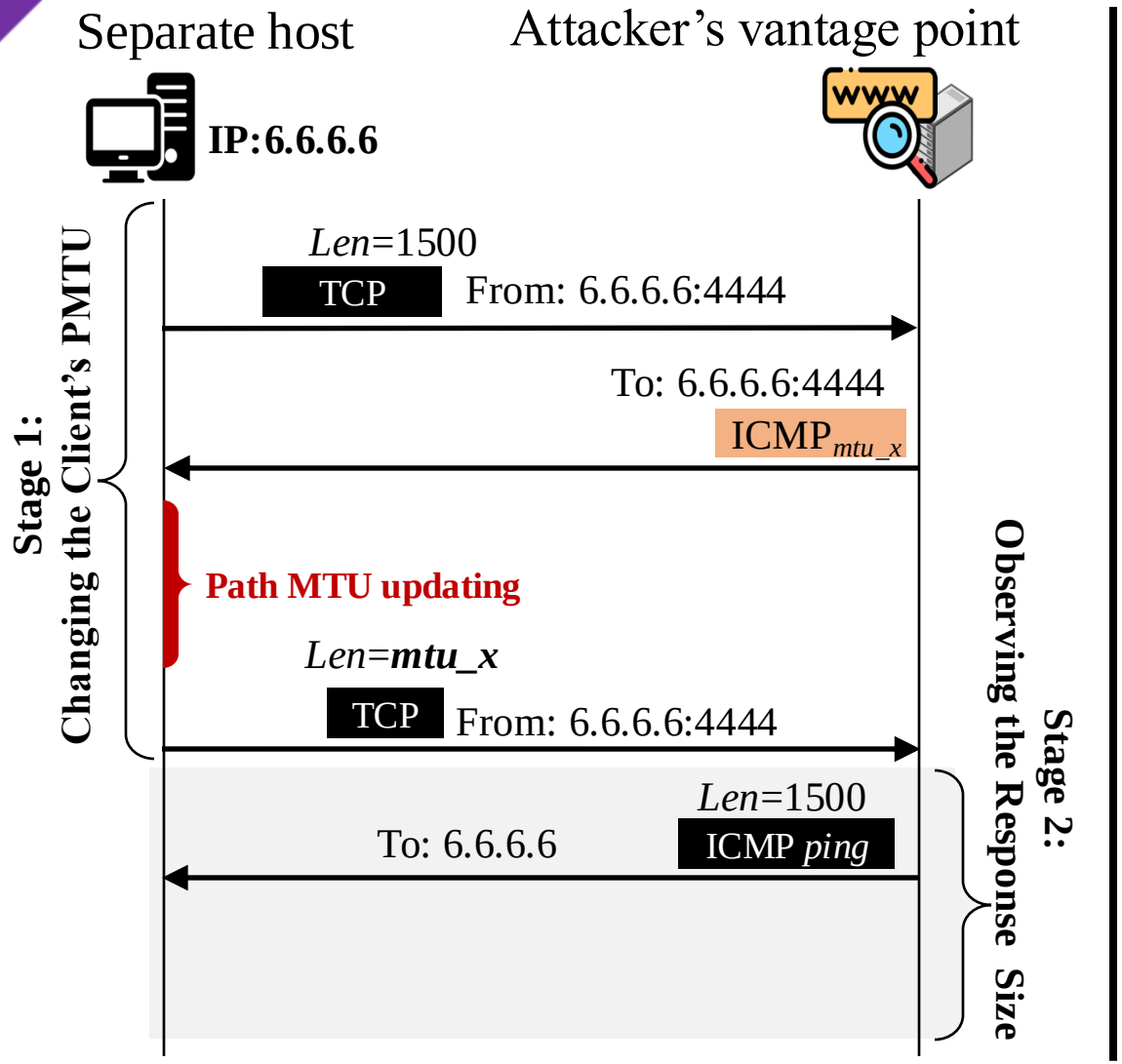


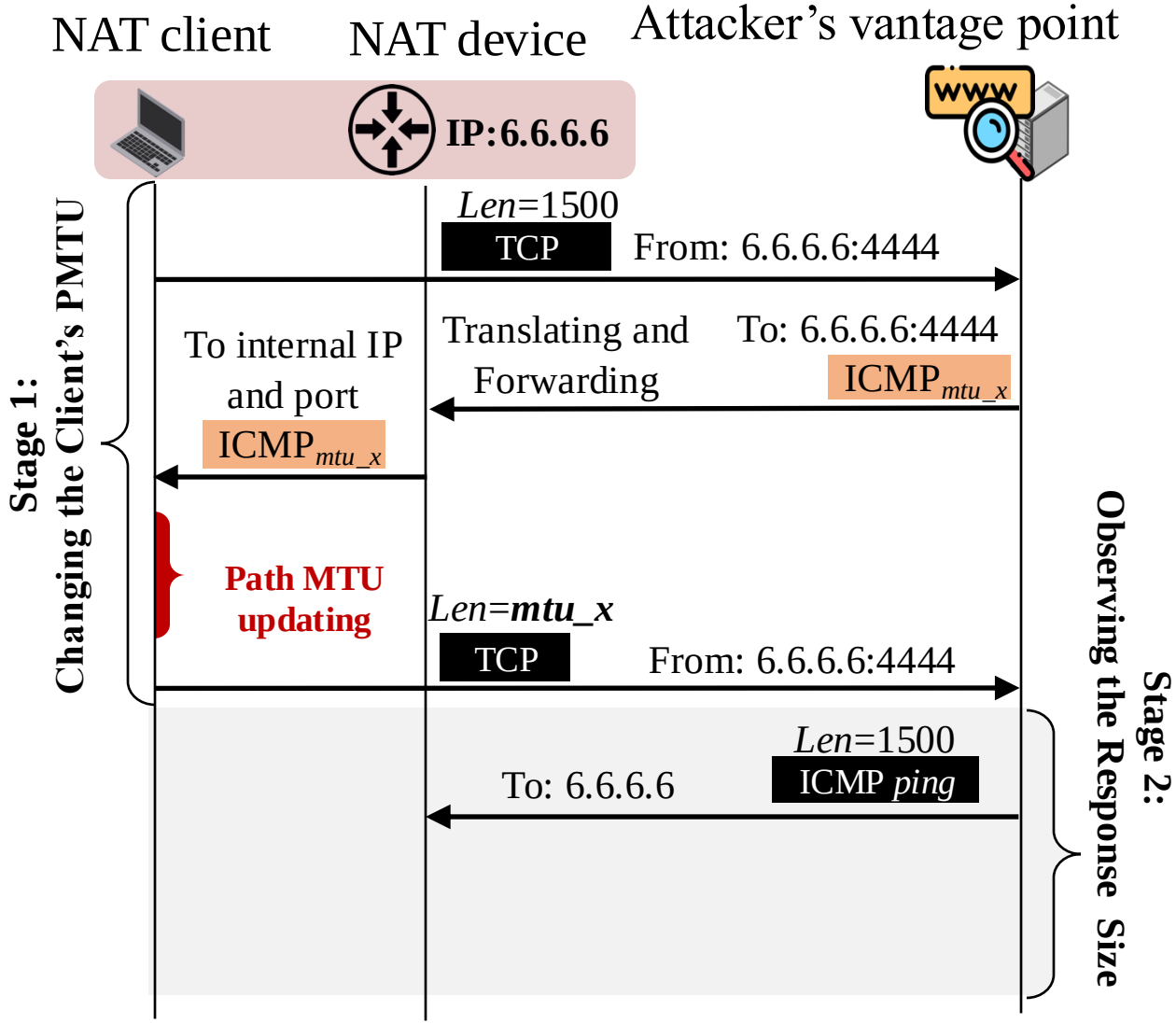


Changing Client's Path MTU

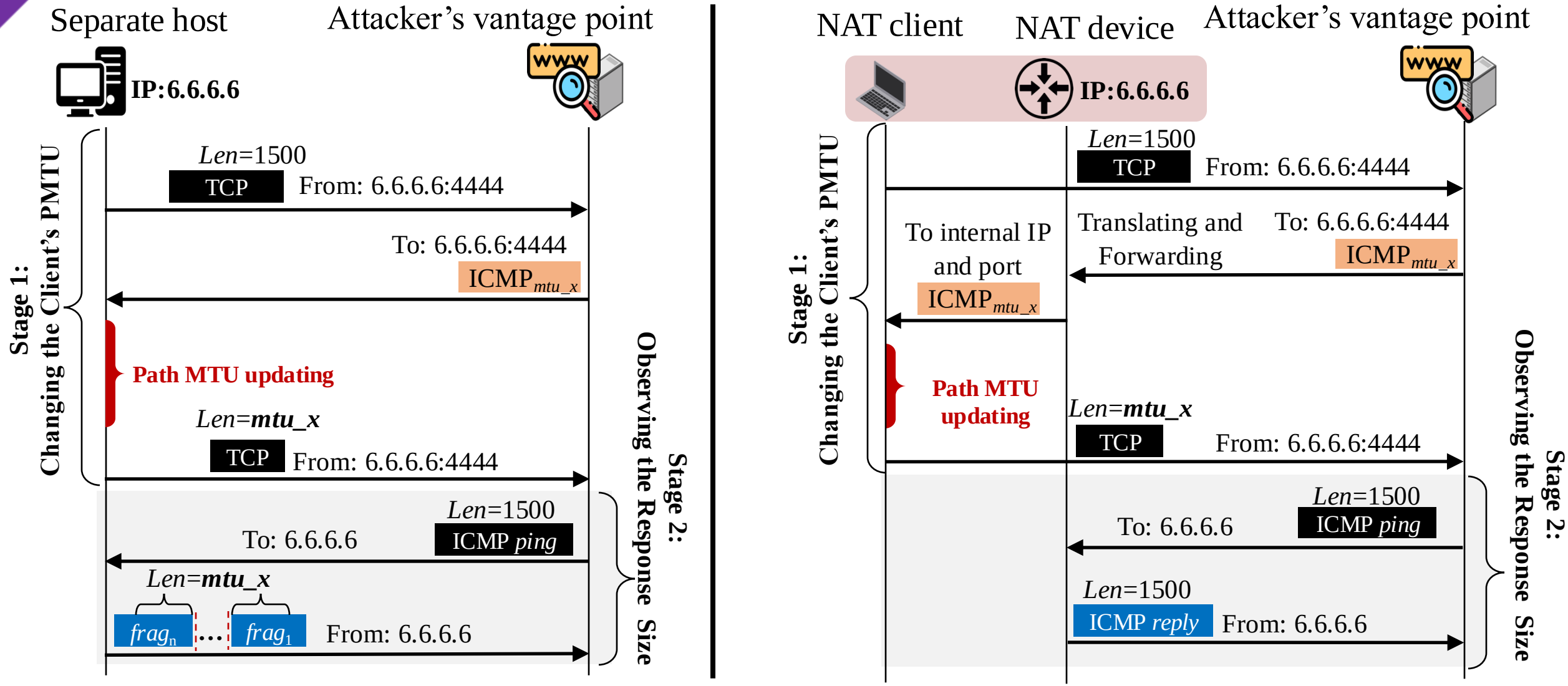


Observing Response Sizes



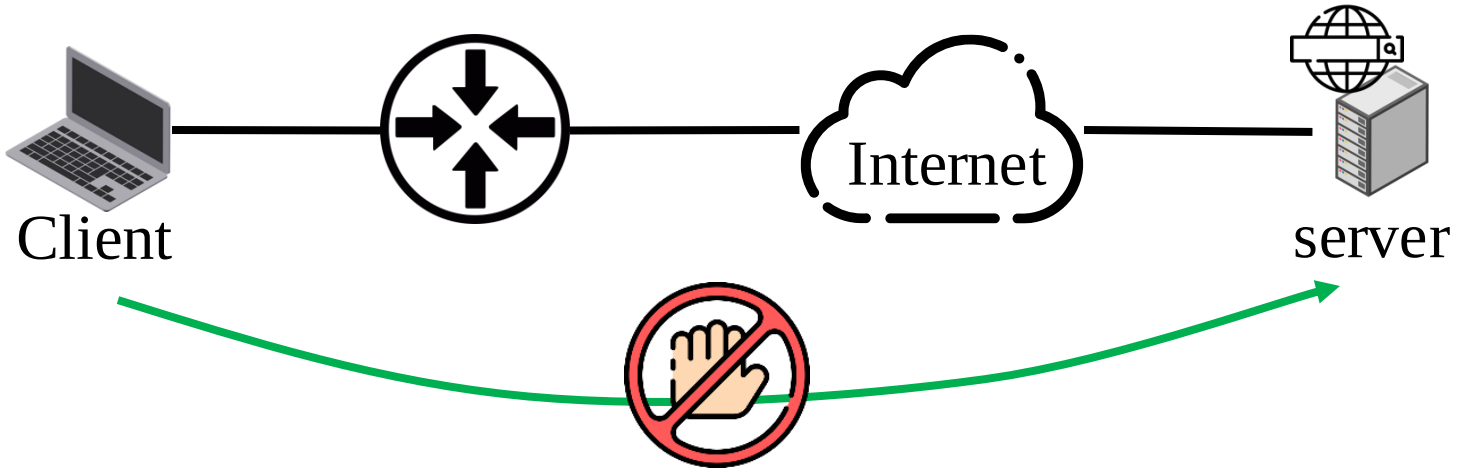


Observing Response Sizes



Step 2: Conducting DoS Attacks

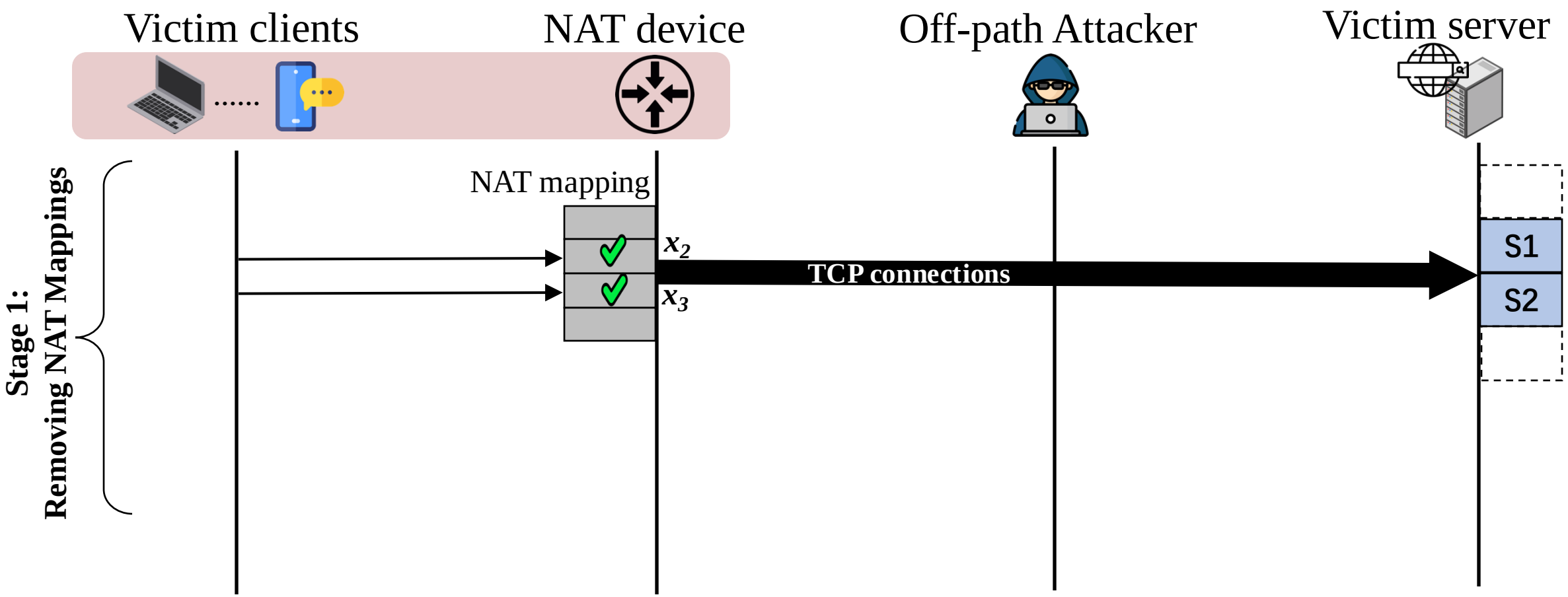
Goal: Terminate TCP connections between victim client and server



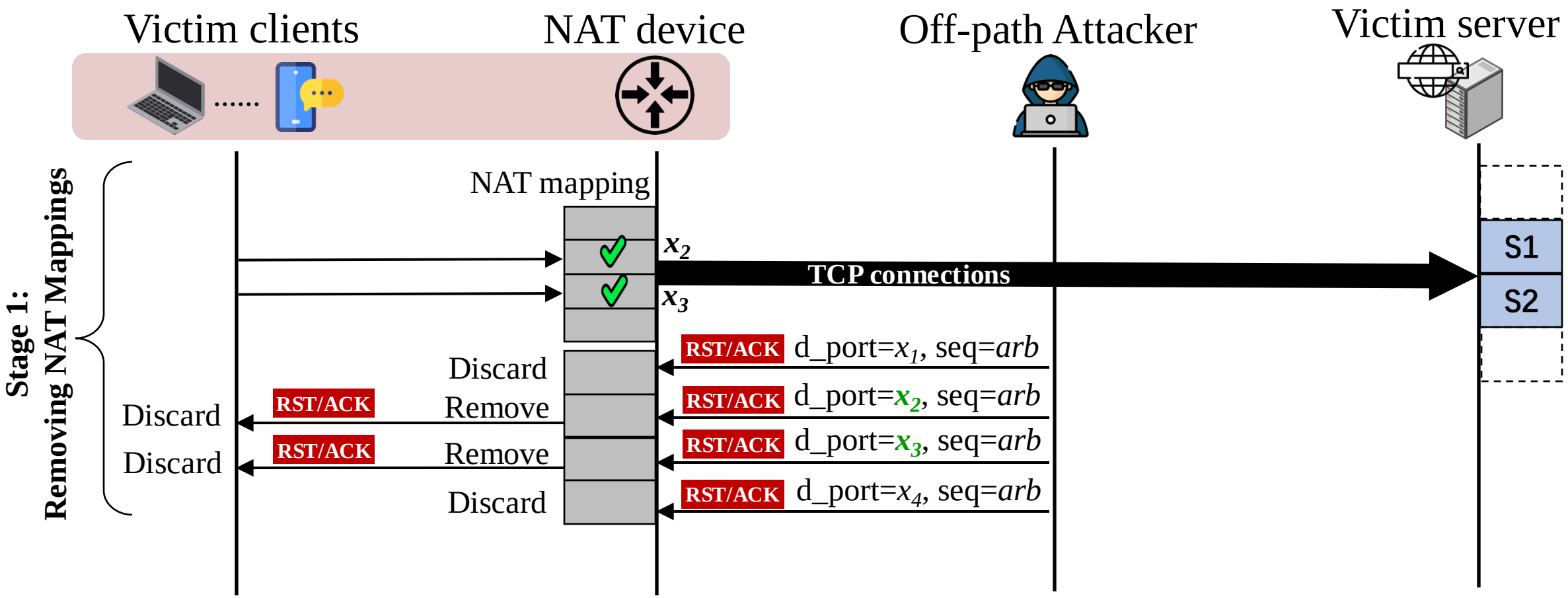
By crafted RST packets:

- Real-world NAT devices (public Wi-Fi/5G/cloud gateways) often **lack enough sequence checks** of **TCP RSTs**.

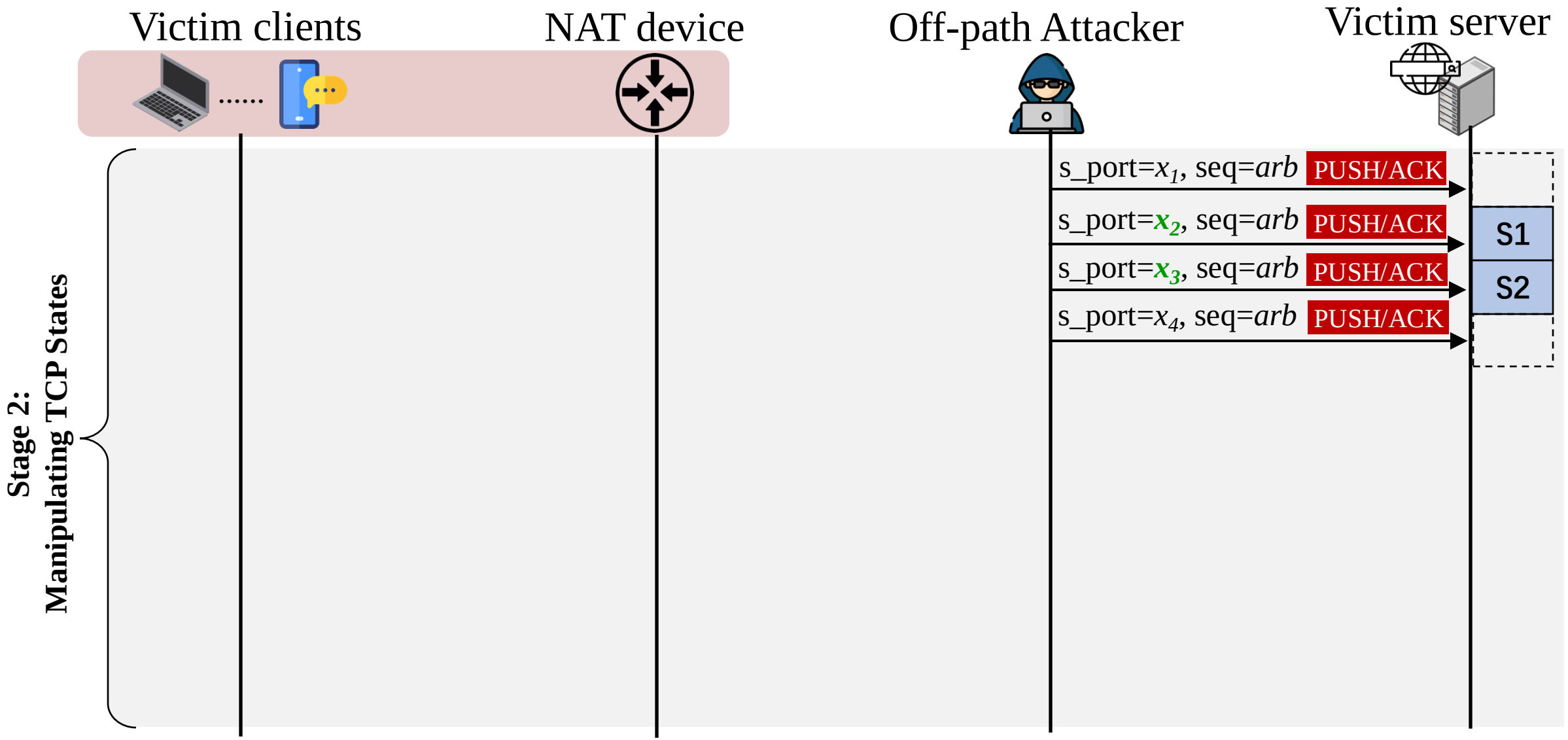
Removing NAT Mappings



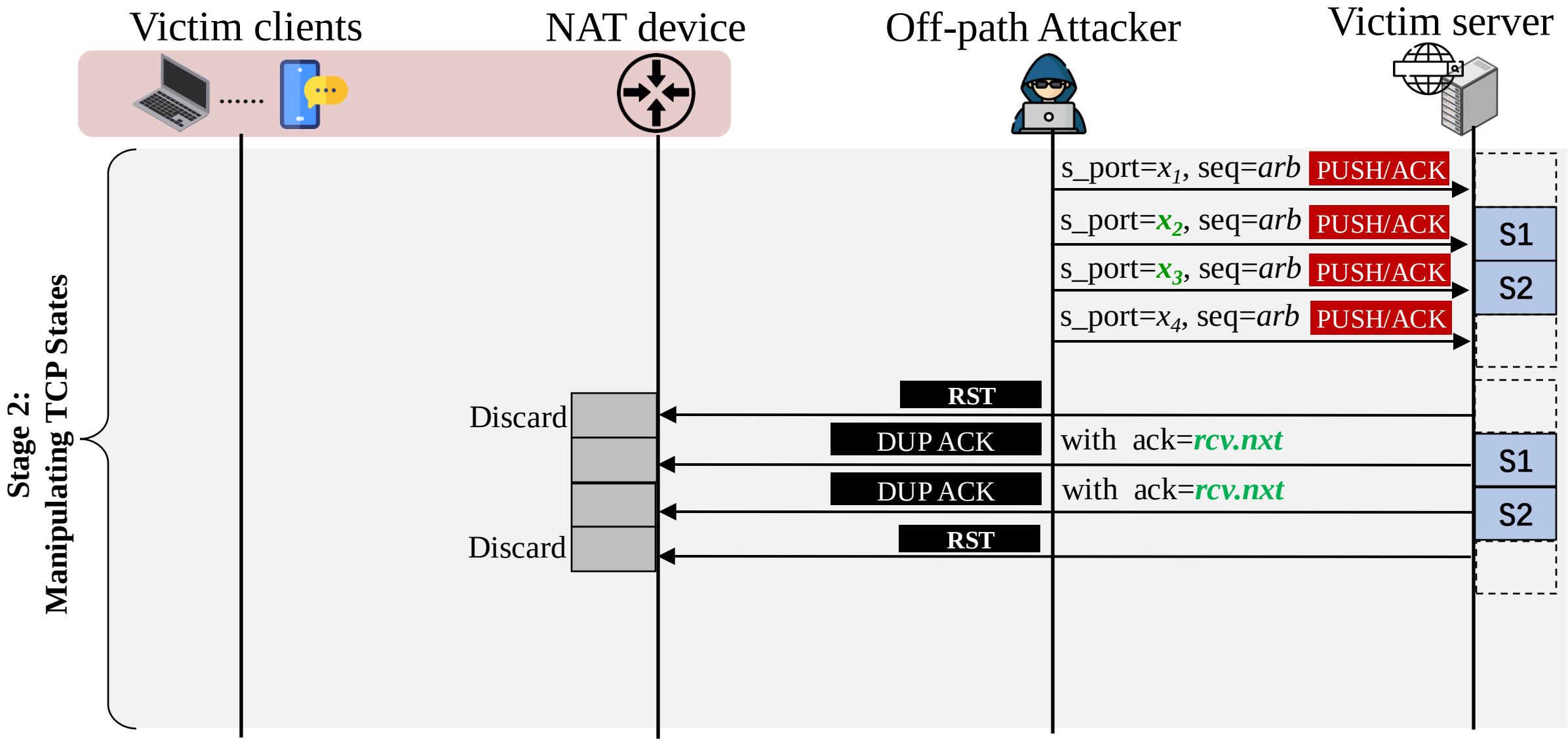
Removing NAT Mappings



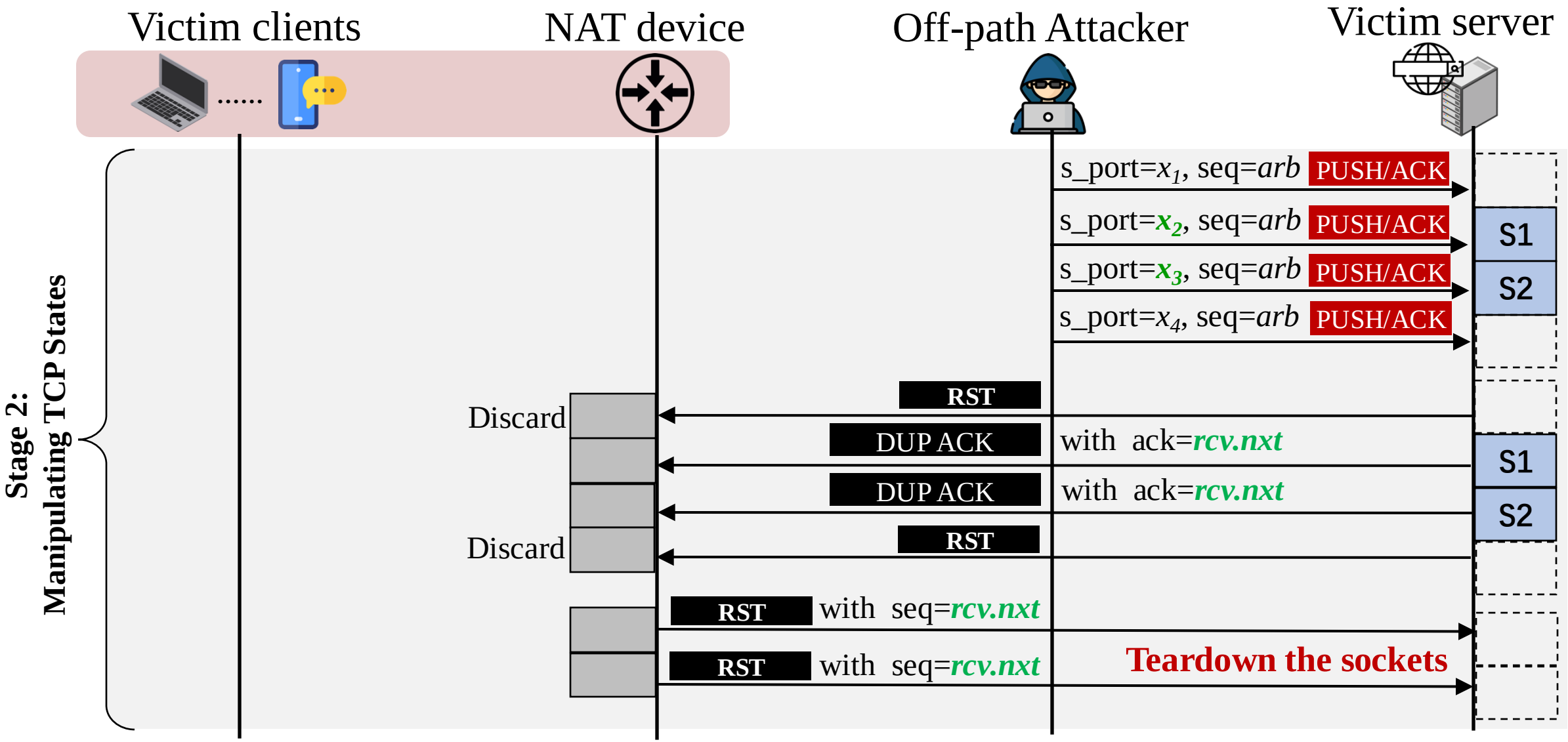
Manipulating TCP States



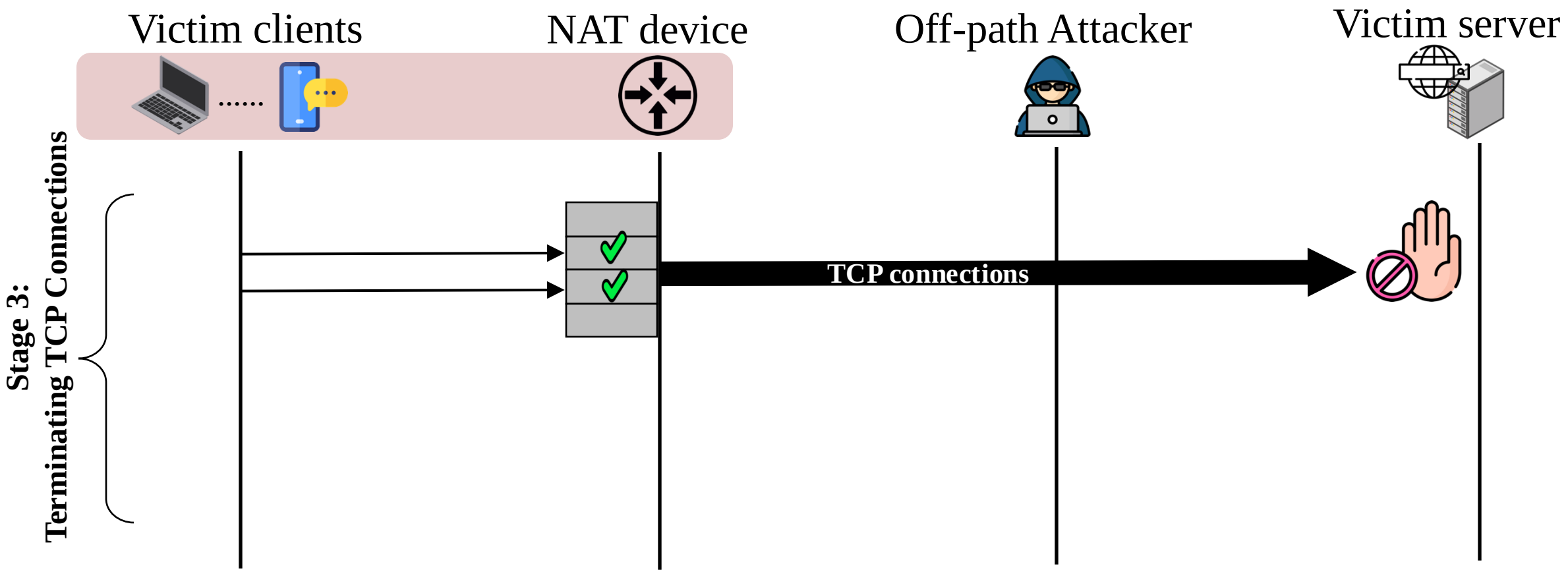
Manipulating TCP States



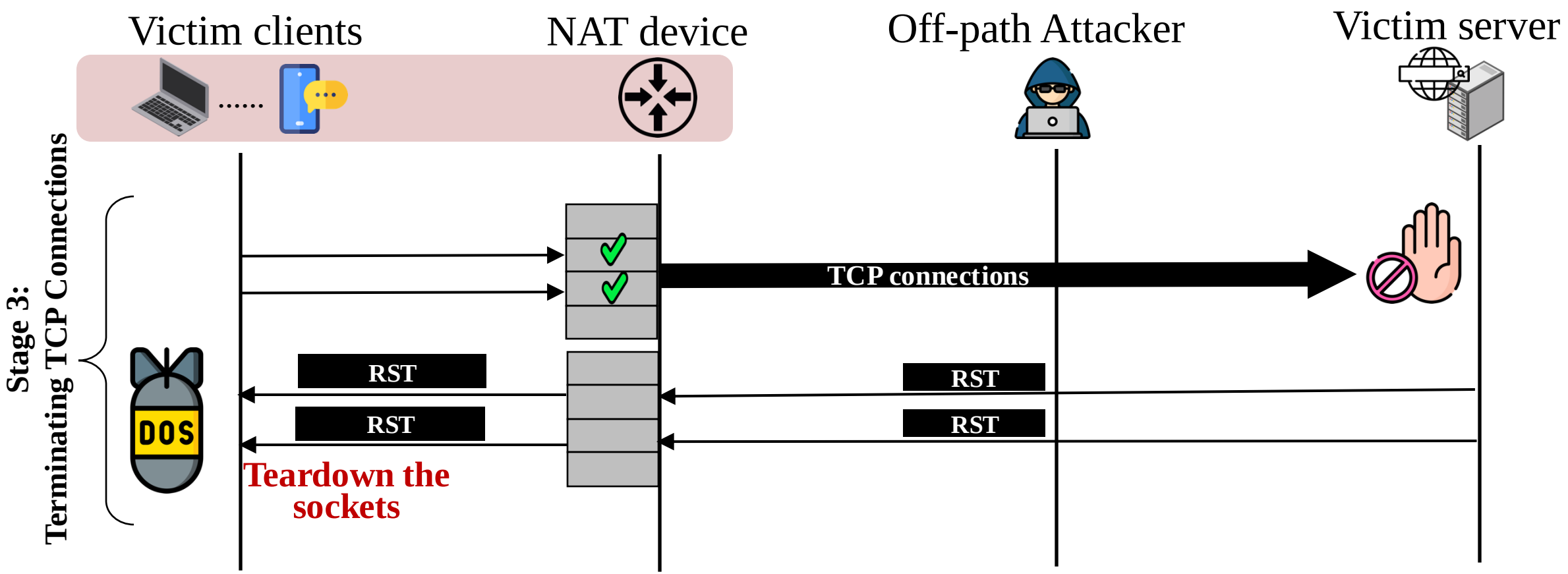
Manipulating TCP States



Terminating TCP Connections



Terminating TCP Connections



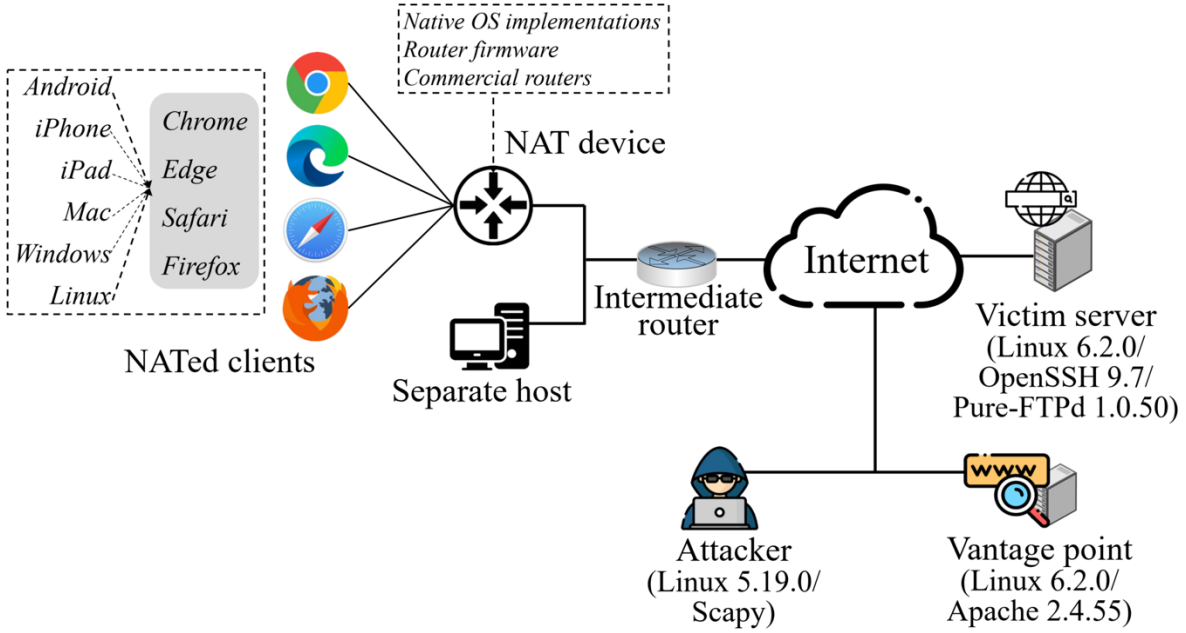
Empirical Study

End-to-end Evaluation

We conduct end-to-end evaluations of the methods with:

- NAT devices: **6 native OSes**, **8 types of router firmware** implementations, **30 commercial routers**
- NATed clients: varied configurations, using **different OSes and browsers**.

1. Whether NATed clients can be identified via the PMTUD side channel.
2. Whether NAT mappings of the NAT devices can be manipulated.
3. Case studies on SSH and FTP DoS.



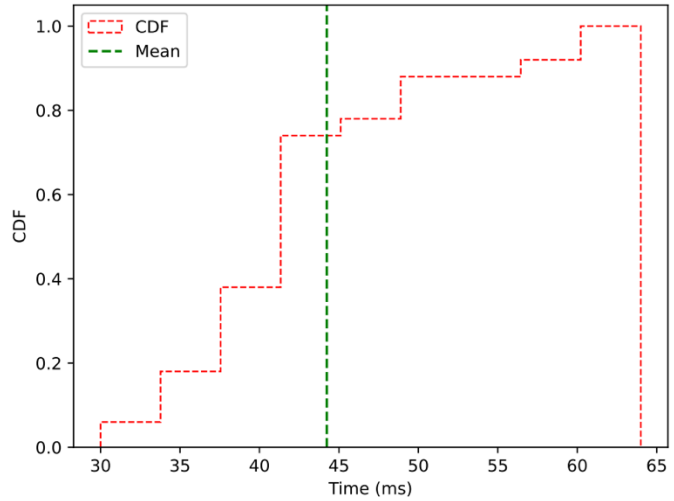
End-to-end Evaluation Results

✎ **Effective Identification**: PMTUD side channel can reliably identify NATed clients. More **effective** than **Javascript-based** and **timing-based** methods.

	Chrome	Edge	Safari	Firefox
Android 12	✔—✔	✔—✔	N/A	✘—✔
iOS 16.3	✘—✔	✘—✔	✘—✔	✘—✔
iPadOS 16.61	✘—✔	✘—✔	✘—✔	✘—✔
MacOS 13.0	✘—✔	✘—✔	✘—✔	✘—✔
Windows 10	✘—✔	✘—✔	N/A	✘—✔
Linux 6.2.0	✘—✔	✘—✔	N/A	✘—✔

✔means the JavaScript-based method works.
✘means the JavaScript-based method fails.
✔means our side channel-based method works.

Comparison with Javascript-based methods



Comparison of time costs with timing-based methods.

End-to-end Evaluation Results

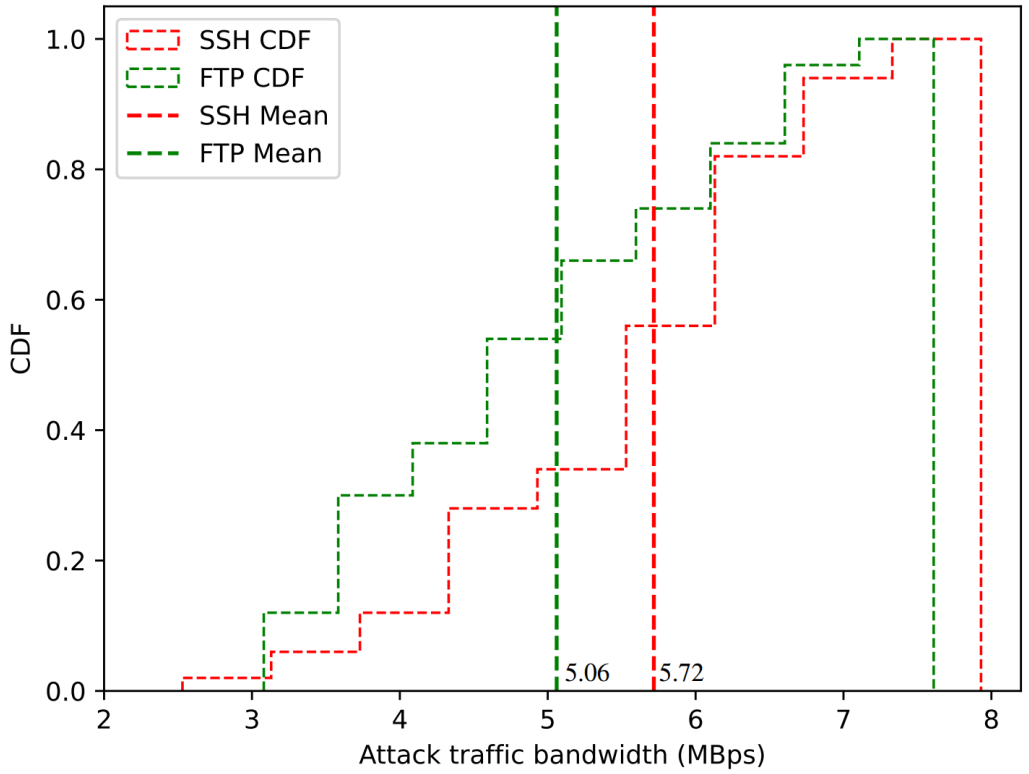
- **Effective Identification**: PMTUD side channel can reliably identify NATed clients. More **effective** than **Javascript-based** and **timing-based** methods.
- **Widespread Vulnerability**: **2 of the 6 native OSes**, **6 of the 8 router firmware**, and **29 of 30 commercial routers** are susceptible to mapping manipulation via crafted RST packets.

NAT Setup	OS/Firmware /Router	Version /Vendor	Release Date*	Vulnerable
Native OS	FreeBSD	13.2 and earlier	04/2023	✔
	Linux	5.0 and earlier	05/2019	✔
	Linux	5.1 and beyond	05/2019	✘
	OpenBSD	5.0 and beyond	11/2011	✘
	macOS	13.2.1	02/2023	✘
	Windows	10	07/2015	✘
		11	10/2021	
Router Firmware	OpenWrt	22.03 and earlier	05/2023	✔
	AsusWrt	3.0.0.4.386 and earlier	10/2022	✔
	pfSense	2.7.0 and earlier	06/2023	✔
	OPNsense	23.7 and earlier	07/2023	✔
	iKuai	3.7.6 and earlier	09/2023	✔
	VxWorks	5.5.1	09/2002	✔
	VyOS	1.4 and beyond	11/2020	✘
	RouterOS	6.49 and beyond	08/2021	✘
Commercial Router	RAX20	Netgear	10/2020	✔
	RAX50	Netgear	02/2020	✔
	E5600	Linksys	03/2020	✔
	E9450	Linksys	05/2022	✔
	RT-AX57	ASUS	02/2023	✔
	RT-AX89X	ASUS	10/2020	✔
	AR6140E-9G-2AC	Huawei	05/2023	✔
	AX3 Pro	Huawei	09/2020	✔
	WS5200	Huawei	—	✔
	TC7102	Huawei	04/2020	✔
	TL-R473GP-AC	TP-Link	04/2021	✔
	TL-R4239GP	TP-Link	06/2022	✔
	TL-XDR6020	TP-Link	01/2022	✔
	TL-AC1200	TP-Link	12/2020	✔
	TL-WDR7620	TP-Link	—	✔
	Magic R100	H3C	01/2020	✔

TCP session mapping removal via crafted RST.

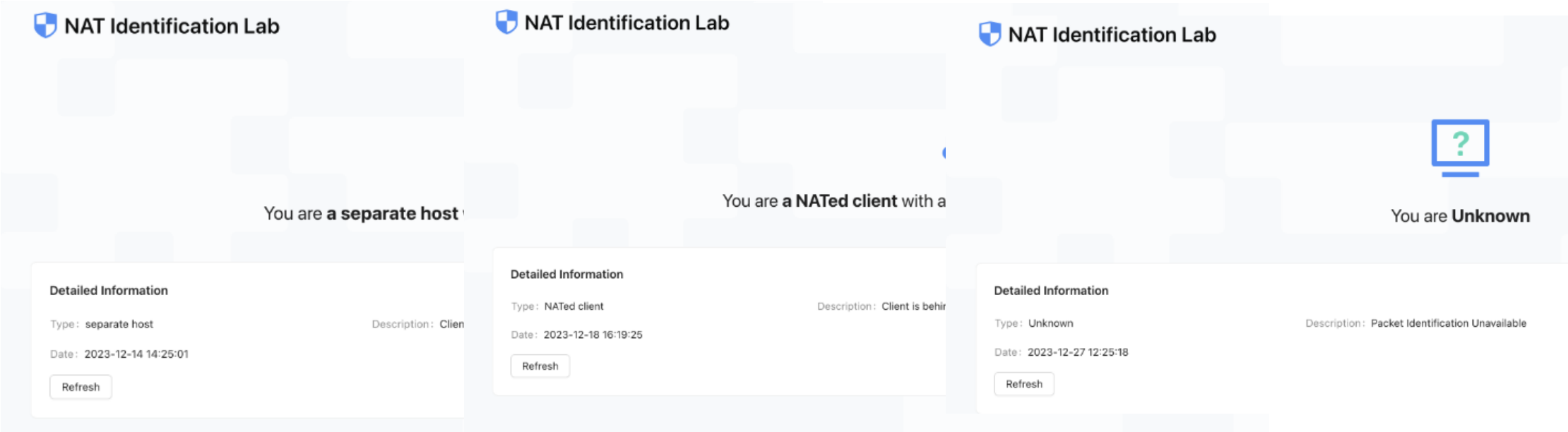
End-to-end Evaluation Results

- **Effective Identification**: PMTUD side channel can reliably identify NATed clients. More **effective** than **Javascript-based** and **timing-based** methods.
- **Widespread Vulnerability**: **2 of the 6 native OSes**, **6 of the 8 router firmware**, and **29 of 30 commercial routers** are susceptible to mapping manipulation via crafted RST packets.
- **Low-Bandwidth DoS**: The attacker can **terminate established TCP connections** or **prevent the establishment of new** SSH & FTP **connections** with low traffic (< 6 MBps on average).



Real-World Experiments

- We **deployed 7 vantage points** in 5 ASes and **tested the PMTUD method** to determine whether the client requesting for our vantage point is a NATed client or a separate IP host.
- We **shared the URLs** for accessing our vantage points via **seeking voluntary users** to participate in our NAT identification in 11 months.



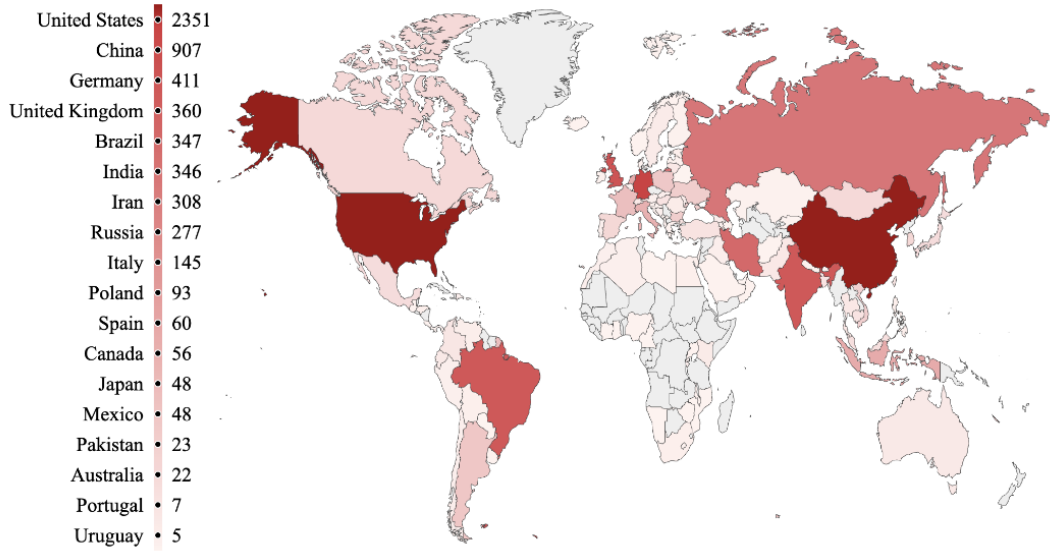
Real-World Experiment Results

EXPERIMENTAL RESULTS OF IDENTIFYING NAT DEVICES ON THE INTERNET.

	Frankfurt	Virginia	California	Jakarta	Bangkok	Beijing	São Paulo	Total	
Request	14,487	14,428	15,690	9,102	13,114	10,328	14,312	91,461	
Denial	7,936	8,235	9,617	4,808	8,001	5,832	7,370	51,799	
Approval	6,551	6,193	6,073	4,294	5,113	4,496	6,942	39,662	
Clients	5,616	5,045	3,458	3,536	3,883	3,184	5,432	30,154	
NAT	1,416 (486A / 84C)	1,158 (386A / 87C)	804 (275A / 68C)	927 (316A / 66C)	994 (334A / 75C)	863 (275A / 68C)	1,443 (491A / 84C)	7,605 (1,289A / 124C)	25.22%
Separate IP	2,449	2,408	1,650	1,636	1,819	1,361	2,425	13,748	45.59%
Unknown	1,751	1,479	1,004	973	1,070	960	1,564	8,801	29.19%

"A" means ASes where the identified NAT devices reside, and "C" means countries that the identified NAT devices belong to.

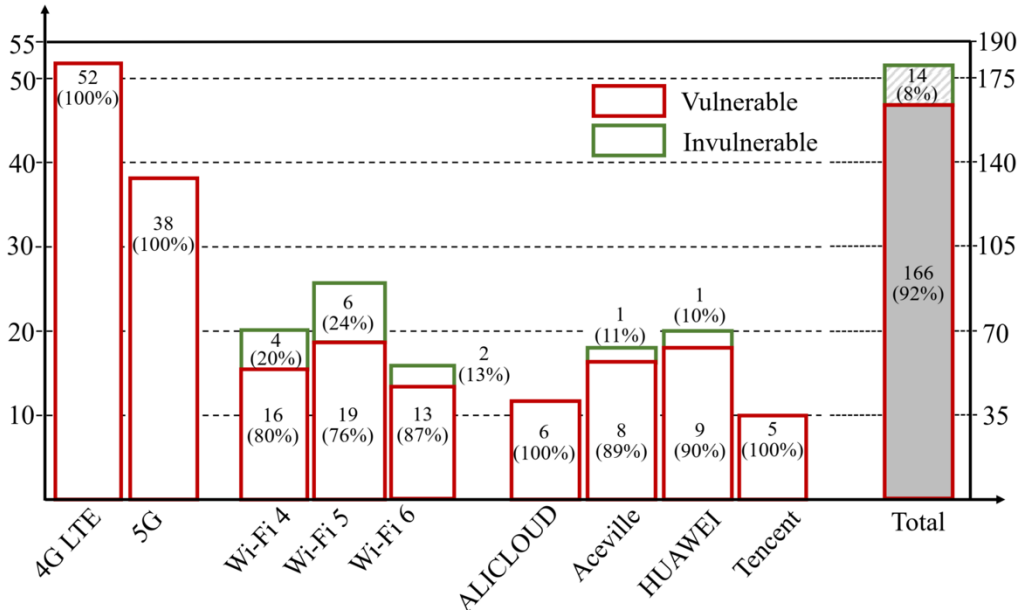
- Out of the 30,154 clients who sent requests, we **successfully identified** more than 7,600 public IPv4 addresses used by **NAT devices** on the Internet.
- We **take a thoroughly analysis** on scenarios of failure cases and possible influences of middle boxses or VPNs.



Distribution of the identified NAT devices.

Real-World Experiment Results

- We randomly selected **180 NAT networks** from three popular network scenarios, including 90 **4G LTE/5G networks**, 60 **Wi-Fi networks**, and 30 **cloud networks**.
- All of the 90 4G/5G networks, 48 of the 60 Wi-Fi networks, 28 of the 30 cloud networks are vunerable to the DoS attacks. Out of **the 180 NAT networks, 166 are vulnerable** to our attacks, causing a **vulnerable proportion** of **more than 92%.**



No.	Public IP address	CIDR	NAT Scenario	Region	Organization	Success Rate
1	*.216.177.*	/20	4G LTE	Virginia, United States	Verizon Business	9/10
2	*.60.40.*	/16	4G LTE	Canarias, Spain	VODAFONE ESPANA S.A.U.	10/10
3	*.30.41.*	/24	4G LTE	Dhaka, Bangladesh	Grameenphone Limited	10/10
4	*.139.100.*	/19	4G LTE	Guizhou, China	China Telecom	9/10
5	*.144.207.*	/21	4G LTE	Xinjiang, China	China Mobile	10/10
6	*.254.3.*	/24	5G	Beijing, China	China Unicom Beijing	10/10
7	*.108.164.*	/13	5G	Chongqing, China	China Telecom	9/10
8	*.139.124.*	/15	5G	Shannxi, China	China Unicom Shannxi	10/10
9	*.104.41.*	/22	5G	Guangdong, China	China Mobile	10/10
10	*.144.139.*	/23	5G	Sichuan, China	China Mobile	9/10
11	*.88.63.*	/18	VM in cloud	California, United States	ALICLOUD	10/10
12	*.74.95.*	/19	VM in cloud	New South Wales, Australia	ALICLOUD	9/10
13	*.51.98.*	/22	VM in cloud	Ontario, Canada	Aceville	10/10
14	*.130.146.*	/19	VM in cloud	Virginia, United States	Aceville	10/10
15	*.135.216.*	/19	VM in cloud	São Paulo, Brazil	Aceville	10/10
16	*.163.199.*	/19	VM in cloud	Tokyo, Japan	Aceville	10/10
17	*.138.165.*	/20	VM in cloud	Johannesburg, South Africa	HUAWEI CLOUDS	9/10
18	*.44.39.*	/20	VM in cloud	Istanbul, Turkey	HUAWEI CLOUDS	10/10
19	*.46.221.*	/17	VM in cloud	Beijing, China	HUAWEI CLOUDS	10/10
20	*.195.177.*	/18	VM in cloud	Shandong, China	Tencent Cloud	10/10
21	*.36.245.*	/16	Wi-Fi	Virginia, United States	Verizon Business	10/10
22	*.66.18.*	/16	Wi-Fi	Virginia, United States	Verizon Business	10/10
23	*.198.141.*	/22	Wi-Fi	Washington, United States	Cox Communications Inc.	10/10
24	*.223.36.*	/15	Wi-Fi	California, United States	Comcast Cable Communications, LLC	9/10
25	*.58.21.*	/16	Wi-Fi	Burnaby, Canada	Simon Fraser University	9/10
26	*.138.139.*	/10	Wi-Fi	Hesse, Germany	Deutsche Telekom AG	8/10
27	*.92.167.*	/20	Wi-Fi	Kerala, India	Bharat Sanchar Nigam LTD	10/10
28	*.129.63.*	/18	Wi-Fi	Beijing, China	China Unicom Beijing	10/10
29	*.47.33.*	/24	Wi-Fi	Dhaka, Bangladesh	Link3 Technologies Limited	10/10
30	*.114.95.*	/14	Wi-Fi	Yunnan, China	China Telecom	10/10

Disclosure and Mitigation

Disclosure and Mitigation

- Ethical disclosure
  - Acknowledgment from the **FreeBSD** community, **OpenWrt/Asuswrt** firmware platforms, **3 major Chinese ISPs**, **3 cloud providers** and **4 router vendors**.
  - 5 CVE/CNVD identifiers (CVE-2023-6534, CVE-2023-31635, CNVD-2023-60783, CNVD-2023-30194, CNVD-2023-30193)
- Mitigation
  - Fixing the Side Channel in PMTUD.
  - Enforcing More Strict Checks on TCP

Conclusion

- We **uncover novel vulnerabilities and propose methods** to identify NAT devices and launch remote DoS attacks.
- We conduct **extensive evaluations** on various NAT implementations and real-world networks.
- We **responsibly disclose** the vulnerabilities and **propose** corresponding **countermeasures.**

Thank you !