Outsmarting Network Security with SDN Teleportation

KASHYAP THIMMARAJU (TU BERLIN, GERMANY)

LIRON SCHIFF (GUARDICORE LABS, ISRAEL)

STEFAN SCHMID (AALBORG UNIVERSITY, DENMARK)

IEEE EURO S&P, PARIS, FRANCE
APRIL 2017

Networking Equipment is Critical

- It forms a technological foundation for communication
- It contributes to the economy
- Vital for national security

Backdoors, exploits and 0days in Networking Equipment

(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

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

RISK ASSESSMENT —

A simple command allows the CIA to commandeer 318 models of Cisco switches

Bug relies on telnet protocol used by hardware on internal networks.

DAN GOODIN - 3/20/2017, 5:35 PM

[ovs-announce] CVE-2016-2074: MPLS buffer overflow vulnerabilities in Open vSwitch

Ben Pfaff blp at ovn.org
Mon Mar 28 17:10:13 PDT 2016

- Next message: [ovs-announce] Open vSwitch 2.4.1 and 2.3.3 Available
- **Messages sorted by:** [date] [thread] [subject] [author]

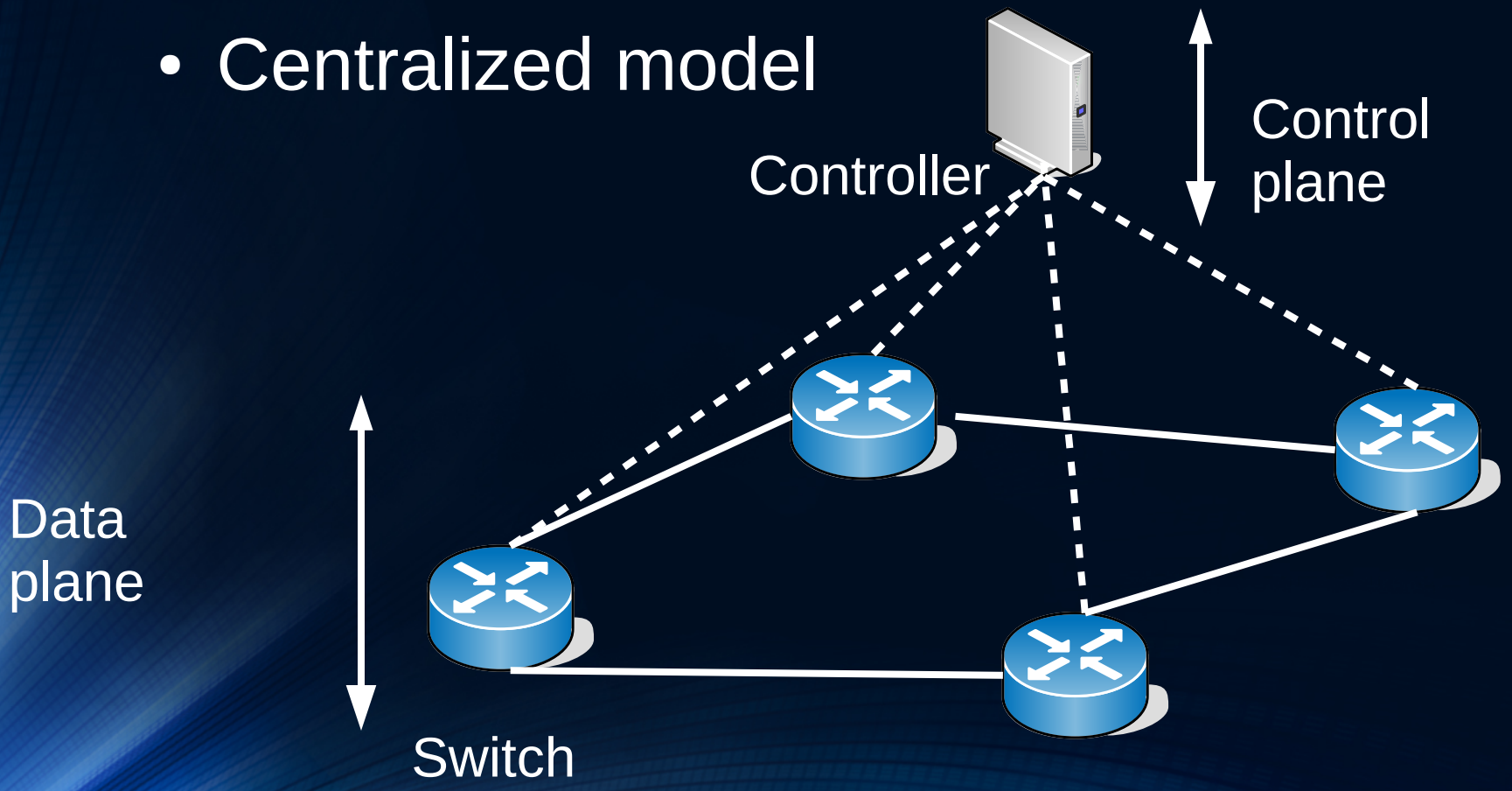
```
Description
===========

Multiple versions of Open vSwitch are vulnerable to remote buffer
overflow attacks, in which crafted MPLS packets could overflow the
buffer reserved for MPLS labels in an OVS internal data structure.
The MPLS packets that trigger the vulnerability and the potential for
exploitation vary depending on version:
```

Backdoors in SDN equipment

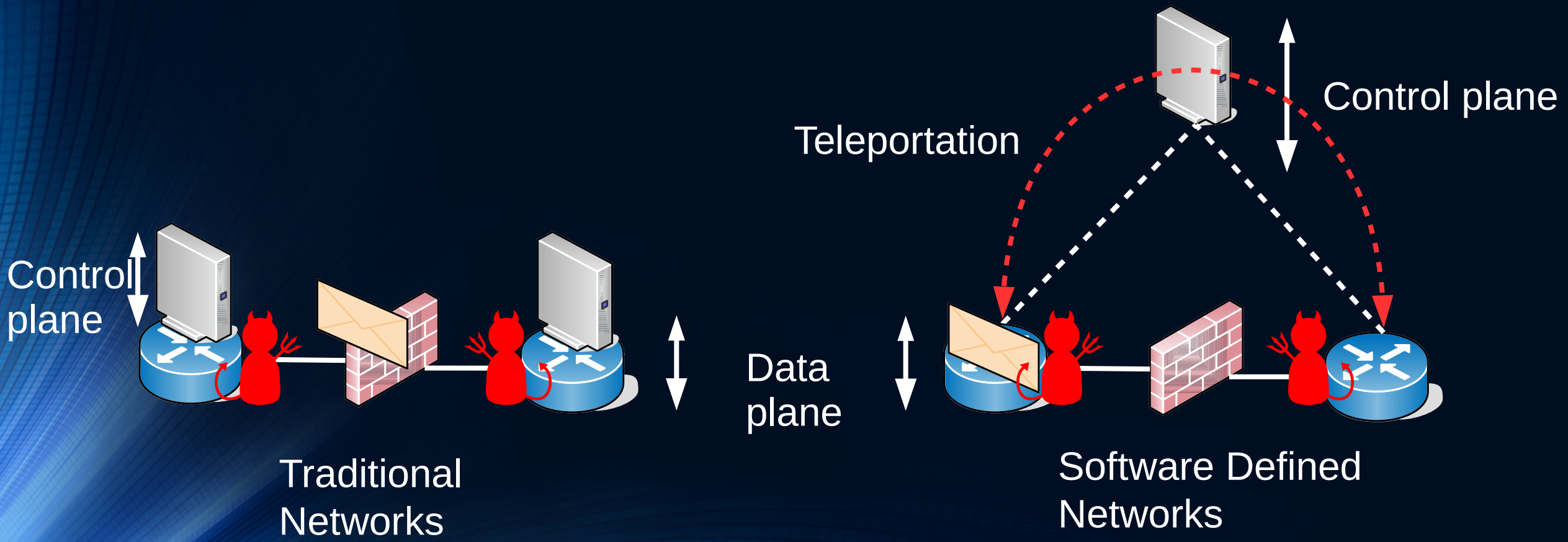
- Does that introduce new attacks?
- Can we detect backdoor activity?

Software Defined Networking (SDN) is a networking paradigm

- Separated planes
- Centralized model



SDN Teleportation:
An attack previously not possible



SDN Teleportation poses several threats

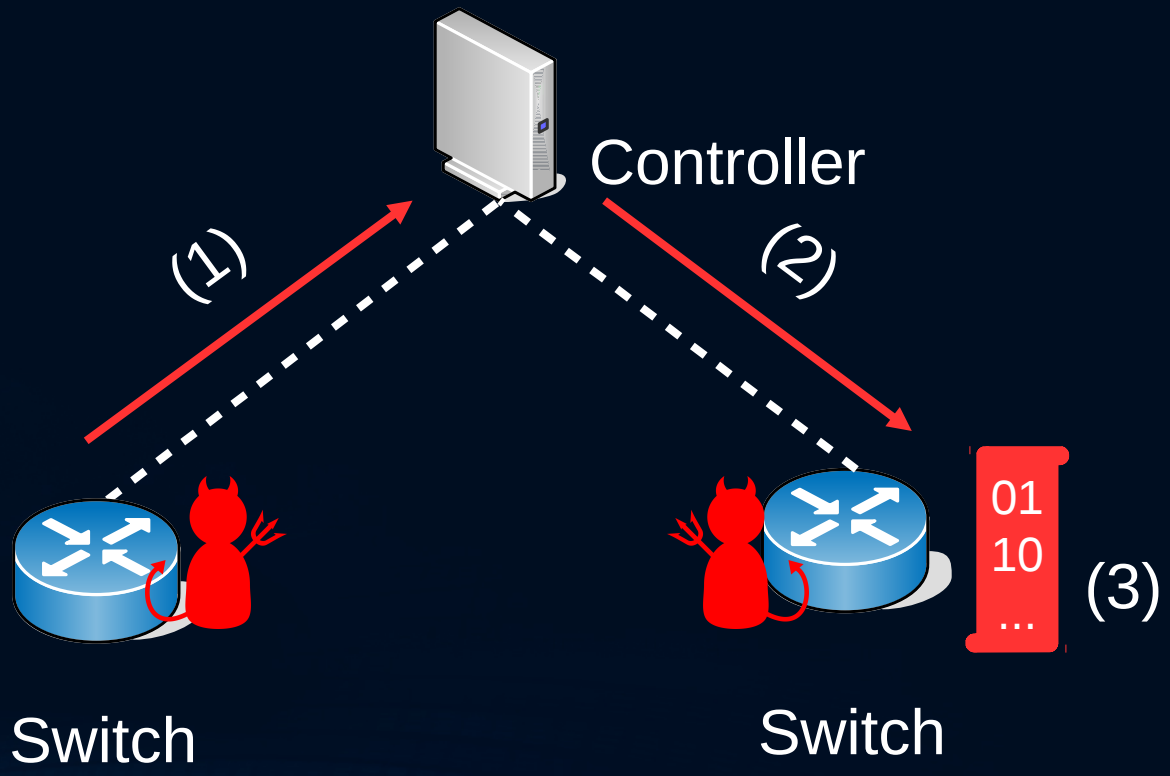
- Bypass security mechanisms
- Attack coordination
- Exfiltration
- Eavesdrop

The Teleportation Model

1)Switch to Controller

2)Controller to Switches

3)Destination Processing

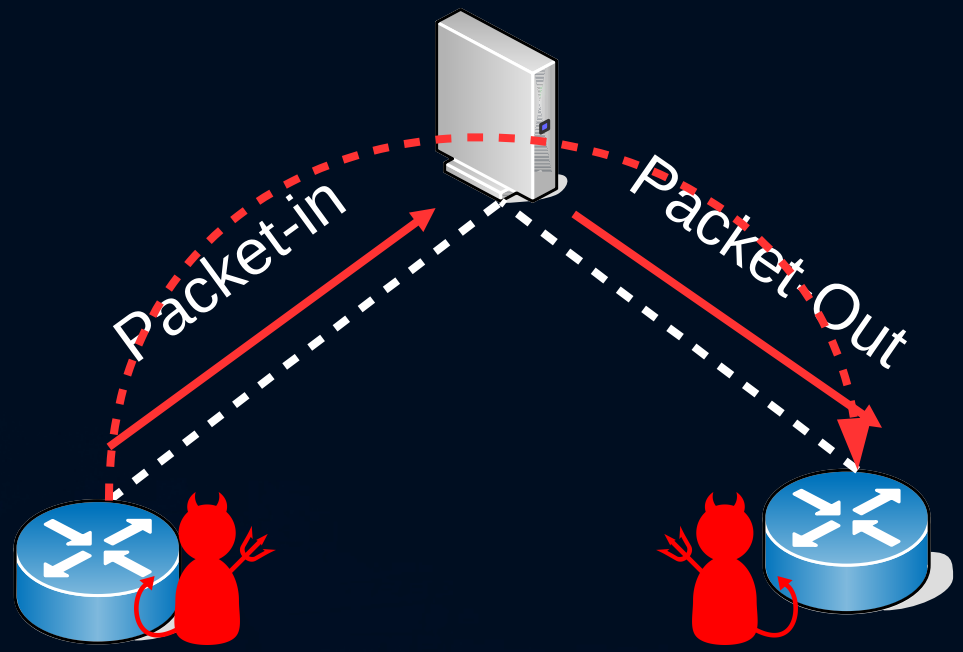


Teleportation Techniques

- Out-of-band Forwarding
- Flow (re-)configurations
- Switch Identification

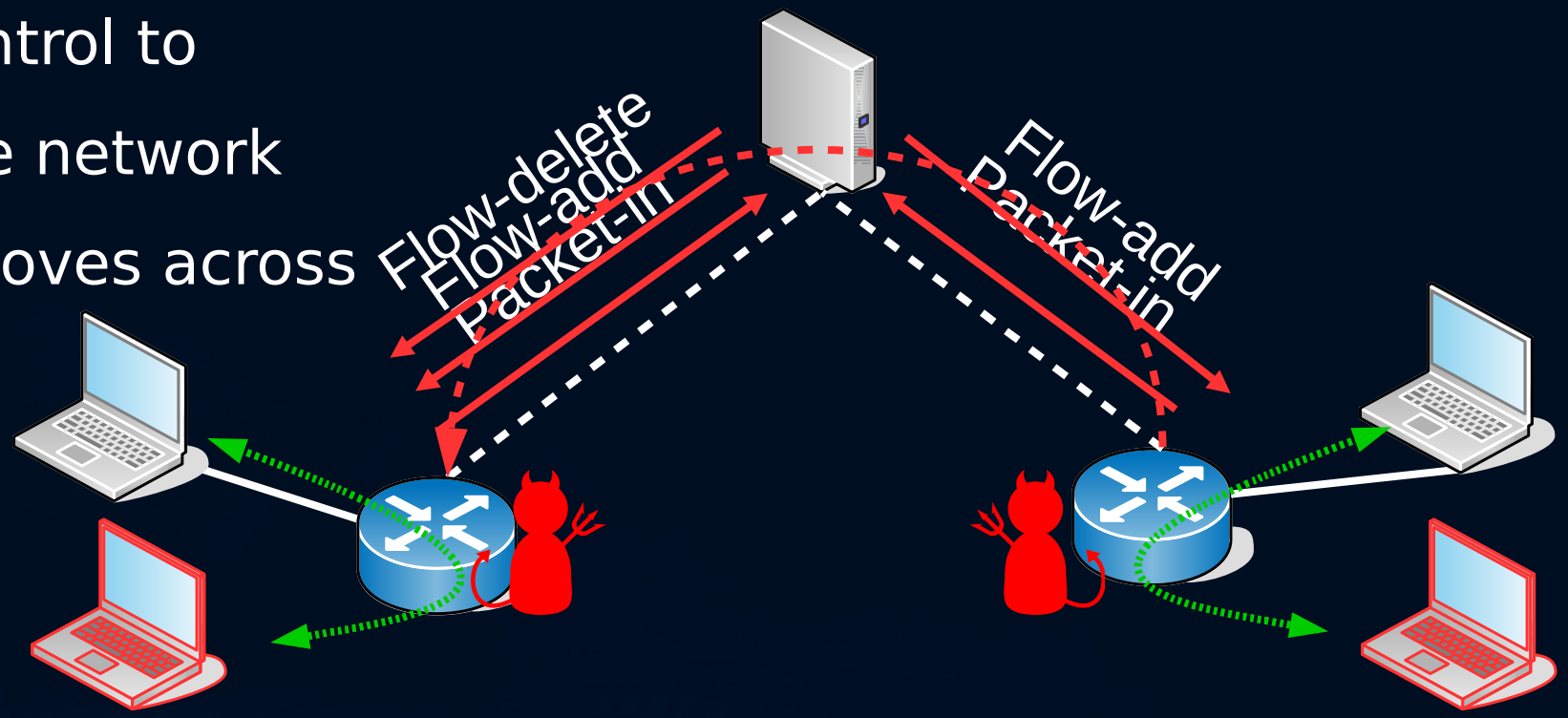
Out-of-band Forwarding Teleportation

- Complete packets from one switch are teleported to another switch



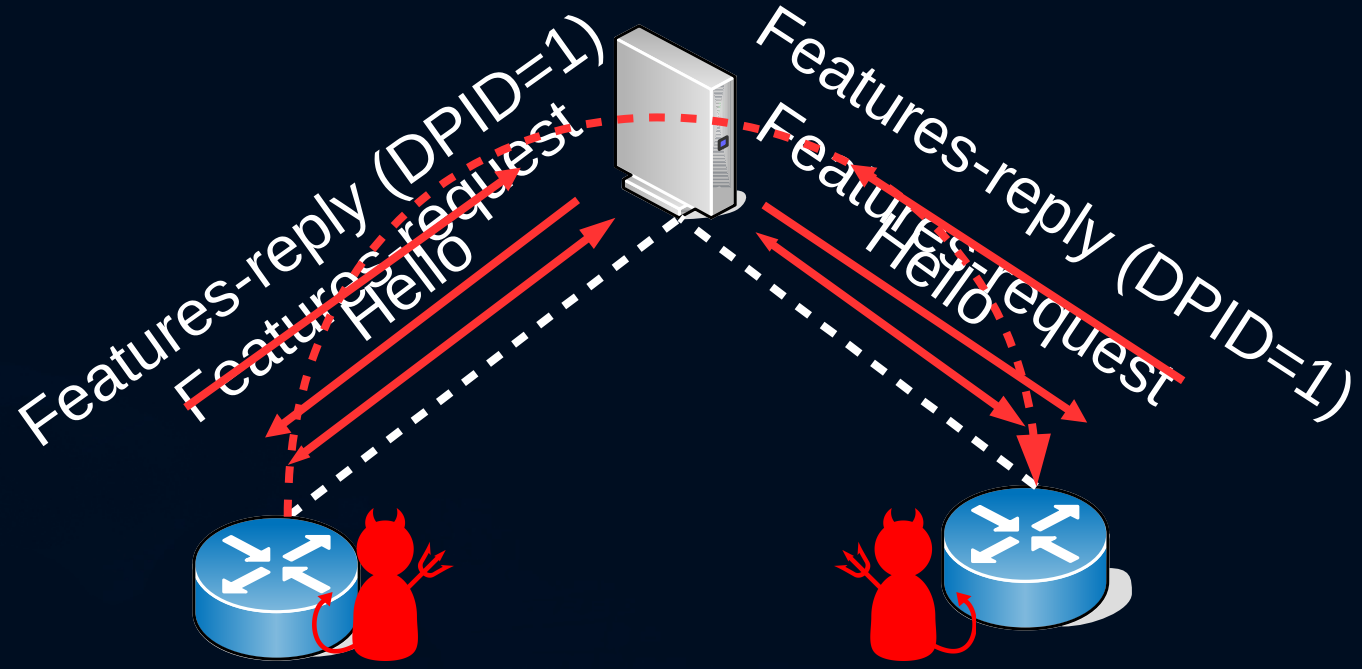
Flow (Re-)Configuration Teleportation

- Exploit the controllers centralized control to reconfigure the network when a host moves across the network



Switch Identification Teleportation

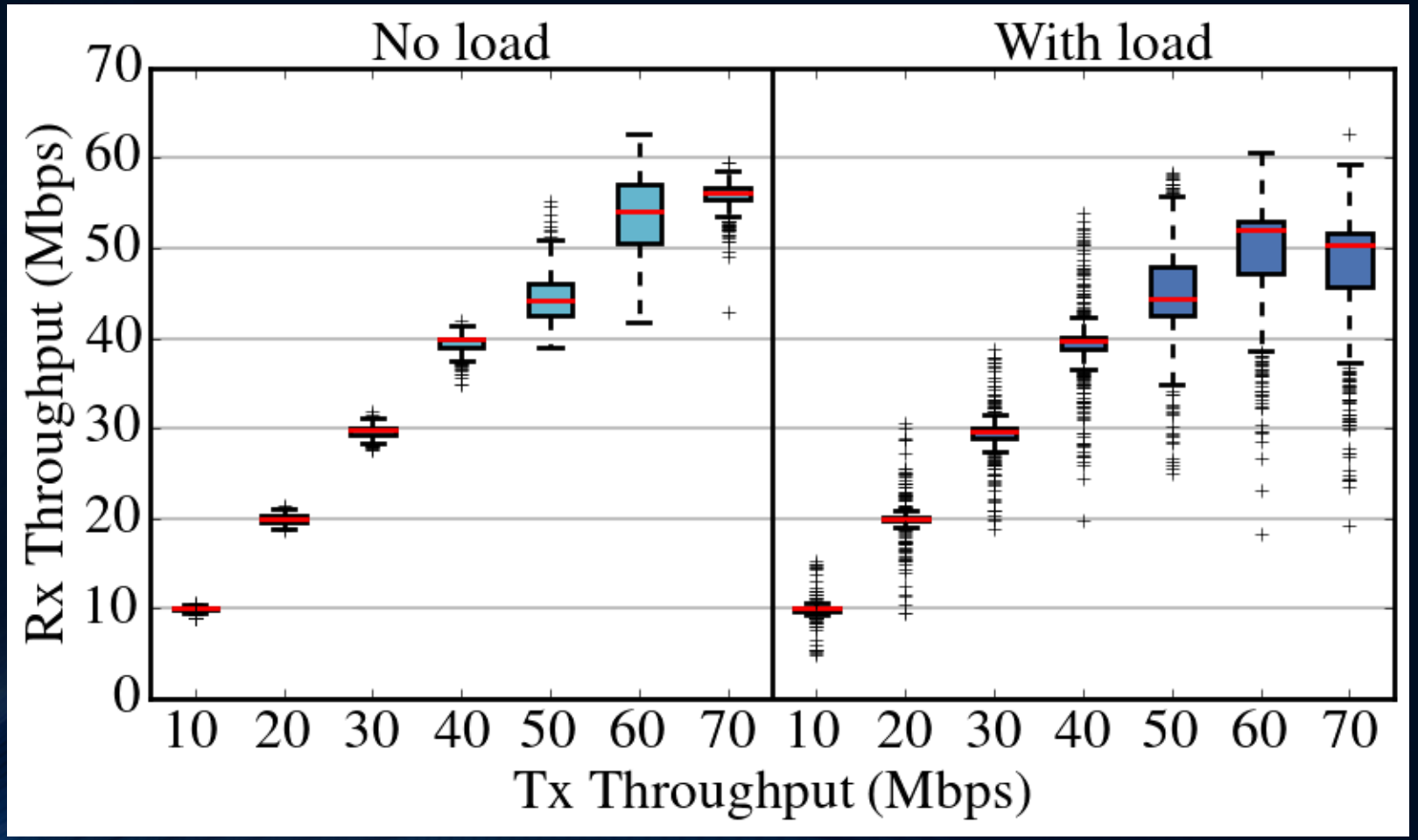
- Impersonate the Datapath-ID to communicate information



Attacks using Teleportation

- Bypass firewalls, IDS and IPS
- Exfiltration
- Man-in-the-middle
- Rendezvous/Attack coordination

Teleportation Bandwidth



Countermeasures

- Packet-in-Packet-Out Watcher
- Audit-Trails and Accountability
- Enhanced IDS with Waypoint Enforcement

Conclusions

- Introduced a conceptually novel SDN attack
- Teleportation enables several attacks
- Teleportation has high quality and throughput
- Suggested Teleportation countermeasures

Questions