
NETCO: RELIABLE ROUTING WITH UNRELIABLE ROUTERS

DISN 2016:

The 2nd International Workshop on Dependability Issues on SDN and NFV

Anja Feldmann (TU Berlin),

Philipp Heyder (TU Berlin),

Michael Kreutzer (Fraunhofer SIT),

Stefan Schmid (Aalborg University, DK & TU Berlin),

Jean-Pierre Seifert (TU Berlin & T-Labs Berlin),

Haya Shulman (Fraunhofer SIT),

Kashyap Thimmaraju (TU Berlin & T-Labs Berlin),

Michael Waidner (Fraunhofer SIT),

Jens Sieberg (Federal Office for Information Security, BSI)

AGENDA

1. SDN: Designing more dependable computer networks
2. Problem: Relying on untrusted networking hardware
3. Attacker model: Bounded-collusion stealthy adversary
4. Robust Combiners
5. NetCo approach
6. Performance
7. Conclusion

1. SDN: Designing more dependable computer networks

SDN Data Plane

- Reduced switch complexity, from “hard-coded” logic to software
=> manufacturer independence, faster innovations

Opportunities for designing more dependable computer networks:

- Switches: cheap, “dumb”, only forwarding devices
=> exchangeable, easier to secure
- Formal reasoning about the function provided by the network and its correctness
=> a crucial prerequisite of any reliable network

BUT still:

- SDN security critically depends on the correctness of the hardware
=> requires reliable switches

2. Problem: Relying on untrusted networking hardware

Cisco Blog > Security



Security

Evolution of attacks on Cisco IOS devices



Graham Holmes - October 8, 2015 - 8 Comments

While “SYNful Knock” is the latest identified malware targeting Cisco devices running Cisco IOS, we have identified and investigated six other malware incidents during the last four years that target Cisco devices running Cisco IOS. The nature of threats is evolving and Cisco will continue to adapt technology delivering trustworthy solutions that our customers can rely on. This also means that customers will need to evolve, fully utilizing the security tools that are available, as well as ensuring security best practices are in place.

2. Problem: Relying on untrusted networking hardware

Huawei HG8245 backdoor and remote access

 Posted on Dec 09 2013 | [Plain text version](#)

Summary

The Huawei HG8245 ONT, firmware version V1R006C00S100 which provides cellular services, contains 3 severe vulnerabilities: two administrator accounts enabled by default and a public administration interface exposed to the Internet.

Description

Model:	Huawei HG8245
Hardware version:	130C4600
Software version:	V1R006C00S100
Date of publication:	12/09/2013
Severity:	Very High
Solution:	Disable WAN-side HTTP and Telnet access. It is not possible to change the default web administrator's password for the user admin.

The backdoor is a web management account enabled by default and the password cannot be changed. In this version the default administrator password is:

```
admin:*6P0N4dm1nP4SS*
```

Another administrator user exists by default for the telnet service:

```
root:admin
```

2. Problem: Relying on untrusted networking hardware

IMPORTANT JUNIPER SECURITY ANNOUNCEMENT

CUSTOMER UPDATE: DECEMBER 20, 2015

Administrative Access (CVE-2015-7755) only affects ScreenOS 6.3.0r17 through 6.3.0r20. VPN Decryption (CVE-2015-7756) only affects ScreenOS 6.2.0r15 through 6.2.0r18 and 6.3.0r12 through 6.3.0r20.

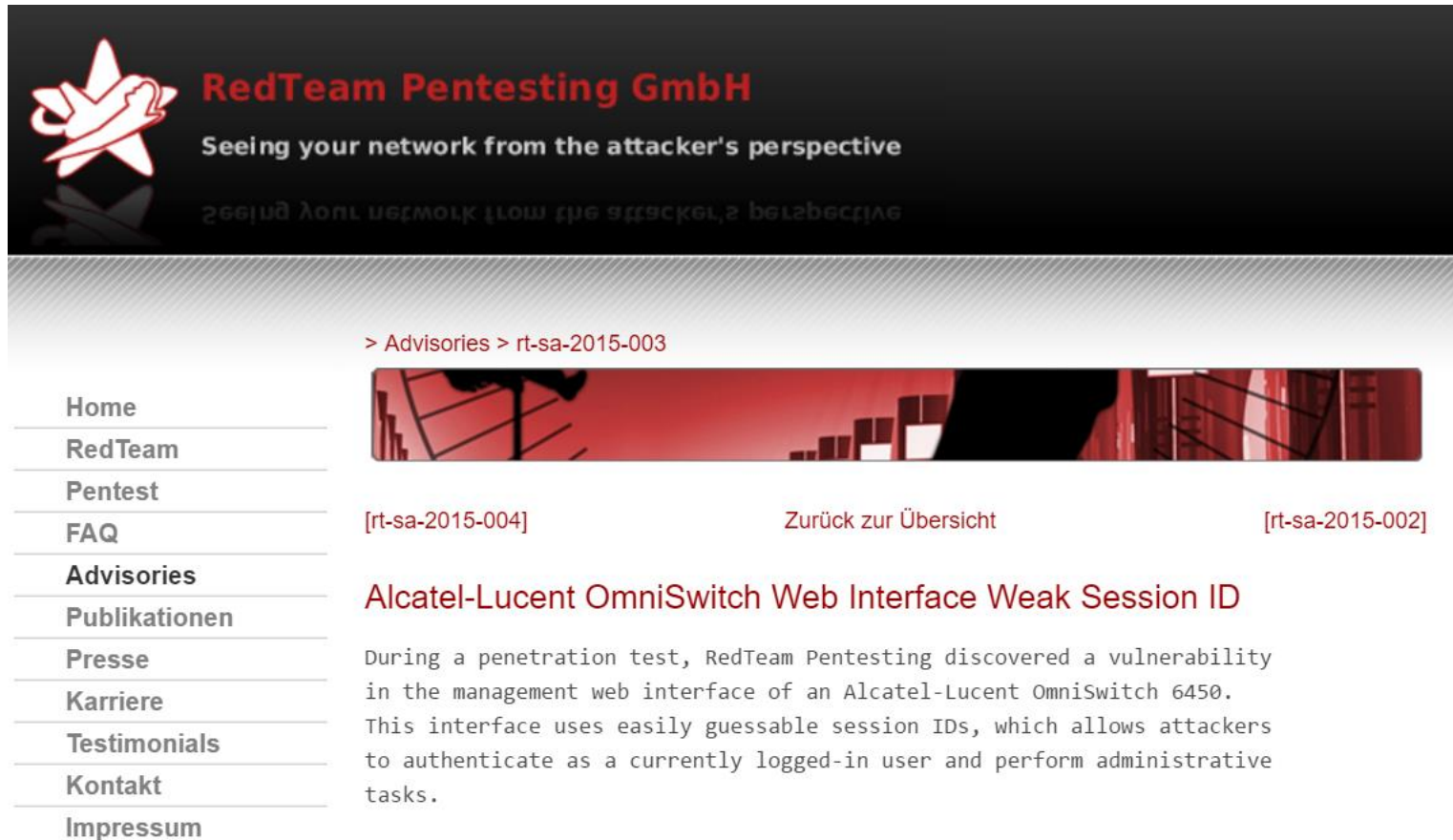
We strongly recommend that all customers update their systems and apply these patched releases with the highest priority.

POSTED BY BOB WORRALL, SVP CHIEF INFORMATION OFFICER ON DECEMBER 17, 2015

Juniper is committed to maintaining the integrity and security of our products and wanted to make customers aware of critical patched releases we are issuing today to address vulnerabilities in devices running ScreenOS® software.

During a recent internal code review, Juniper discovered unauthorized code in ScreenOS that could allow a knowledgeable attacker to gain administrative access to NetScreen® devices and to decrypt VPN connections. Once we identified these vulnerabilities, we launched an investigation into the matter, and worked to develop and issue patched releases for the latest versions of ScreenOS.

2. Problem: Relying on untrusted networking hardware



The screenshot shows the homepage of RedTeam Pentesting GmbH. The header features a red star logo and the company name in red. Below the header, a navigation menu is on the left, and a list of advisories is on the right. The selected advisory is titled 'Alcatel-Lucent OmniSwitch Web Interface Weak Session ID'.

RedTeam Pentesting GmbH
Seeing your network from the attacker's perspective

> Advisories > rt-sa-2015-003

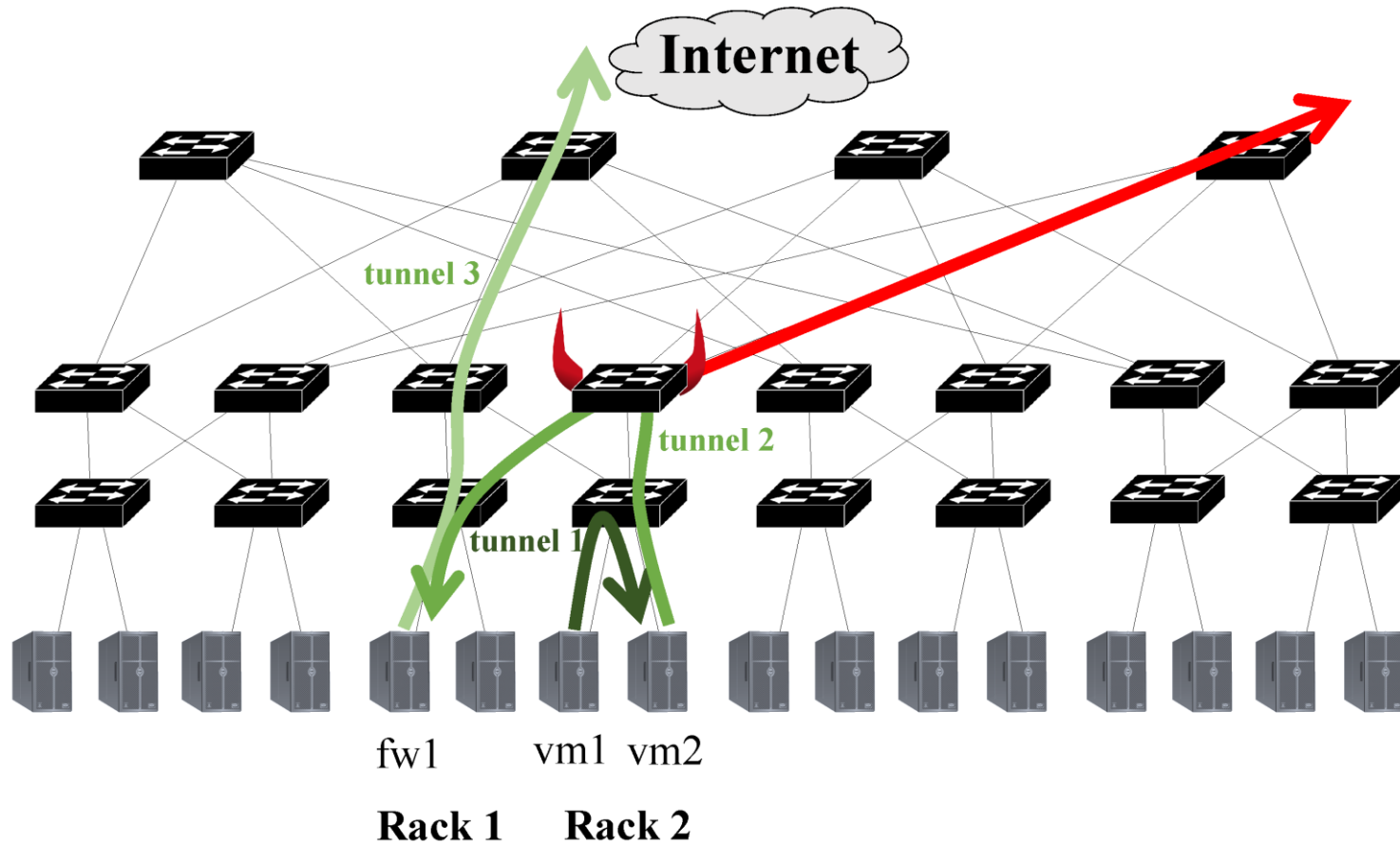
[Home](#)
[RedTeam](#)
[Pentest](#)
[FAQ](#)
[Advisories](#)
[Publikationen](#)
[Presse](#)
[Karriere](#)
[Testimonials](#)
[Kontakt](#)
[Impressum](#)

[\[rt-sa-2015-004\]](#) [Zurück zur Übersicht](#) [\[rt-sa-2015-002\]](#)

Alcatel-Lucent OmniSwitch Web Interface Weak Session ID

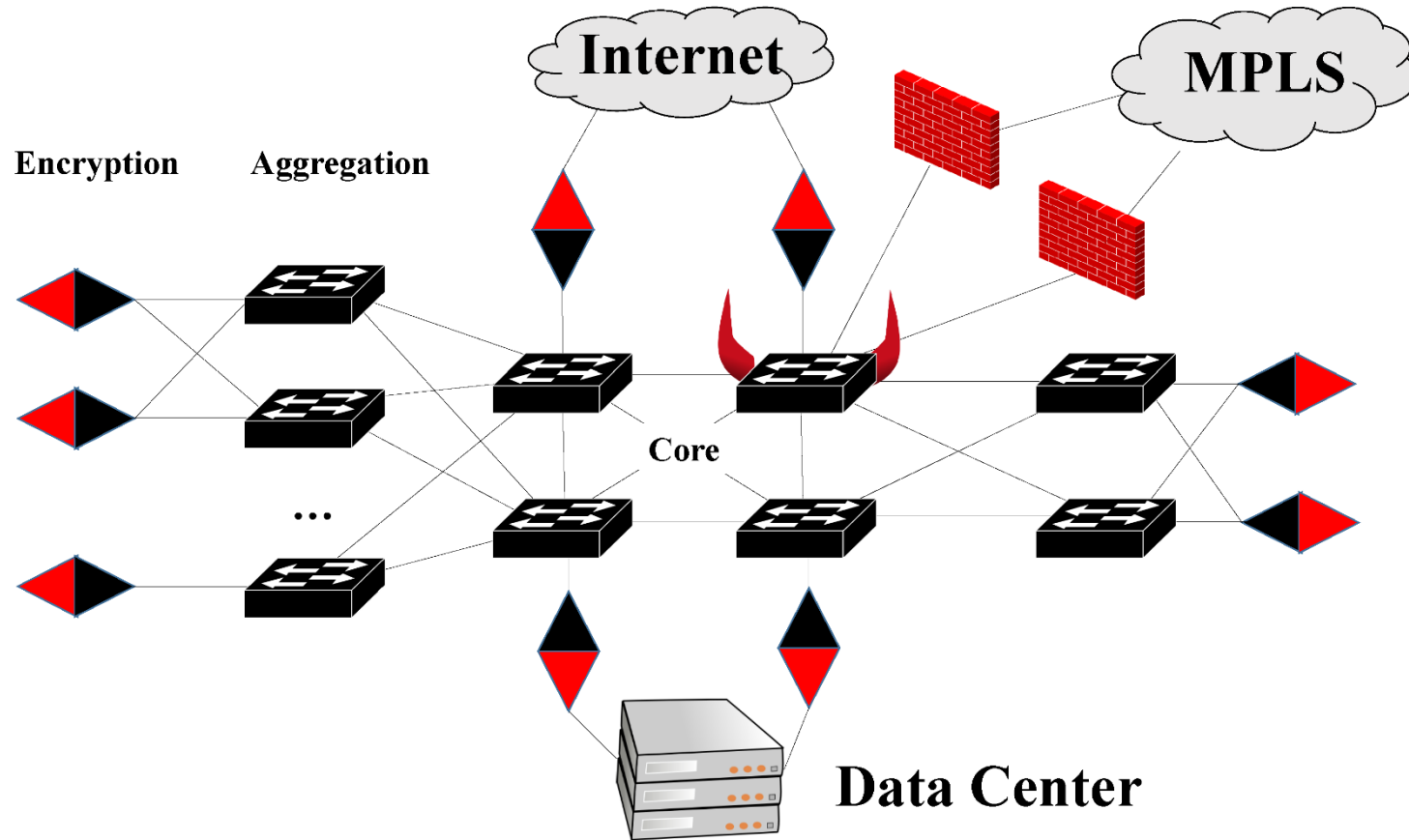
During a penetration test, RedTeam Pentesting discovered a vulnerability in the management web interface of an Alcatel-Lucent OmniSwitch 6450. This interface uses easily guessable session IDs, which allows attackers to authenticate as a currently logged-in user and perform administrative tasks.

2. Problem: Relying on untrusted networking hardware



Datacenter Scenario with fat tree topology

2. Problem: Relying on untrusted networking hardware



Crypto Transport Scenario

3. Attacker model: Bounded-collusion stealthy adversary

Adversarial switch may perform the following attacks:

- Rerouting
- Mirroring
- Packet Modification
- Stealthy Denial-of-Service (DoS)

4. Robust Combiners

- Inspired by the robust combiner concept known from cryptography

Tolerant Combiners: Resilient Cryptographic Design

Amir Herzberg

Computer Science Department, Bar Ilan University, Ramat Gan, Israel

herzbea@cs.biu.ac.il

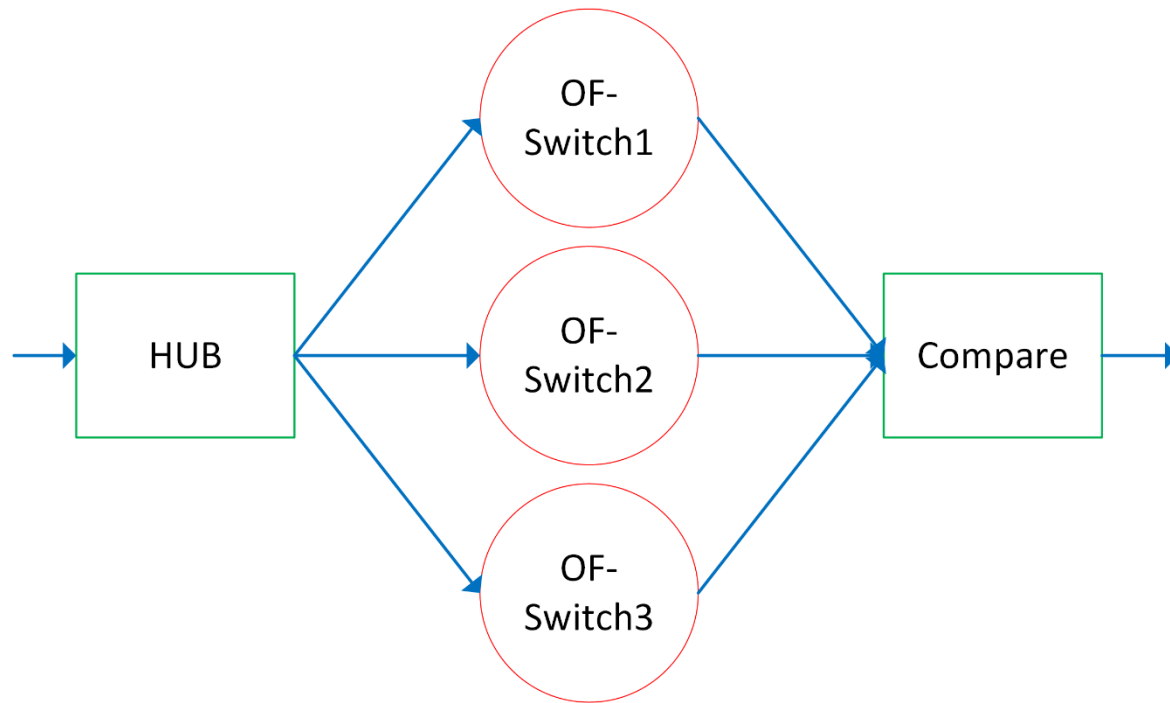
<http://AmirHerzberg.com>

Abstract. Cryptographic schemes are often designed as a combination of multiple component cryptographic modules. Such a combiner design is *tolerant* for a (security) specification if it meets the specification, provided that a sufficient subset of the components meet their specifications. The archtypical combiner is *cascade*, and we show that it is indeed a tolerant combiner for encryption schemes, under chosen plaintext

Received 29 Aug 2002, published @ CT-RSA 2005

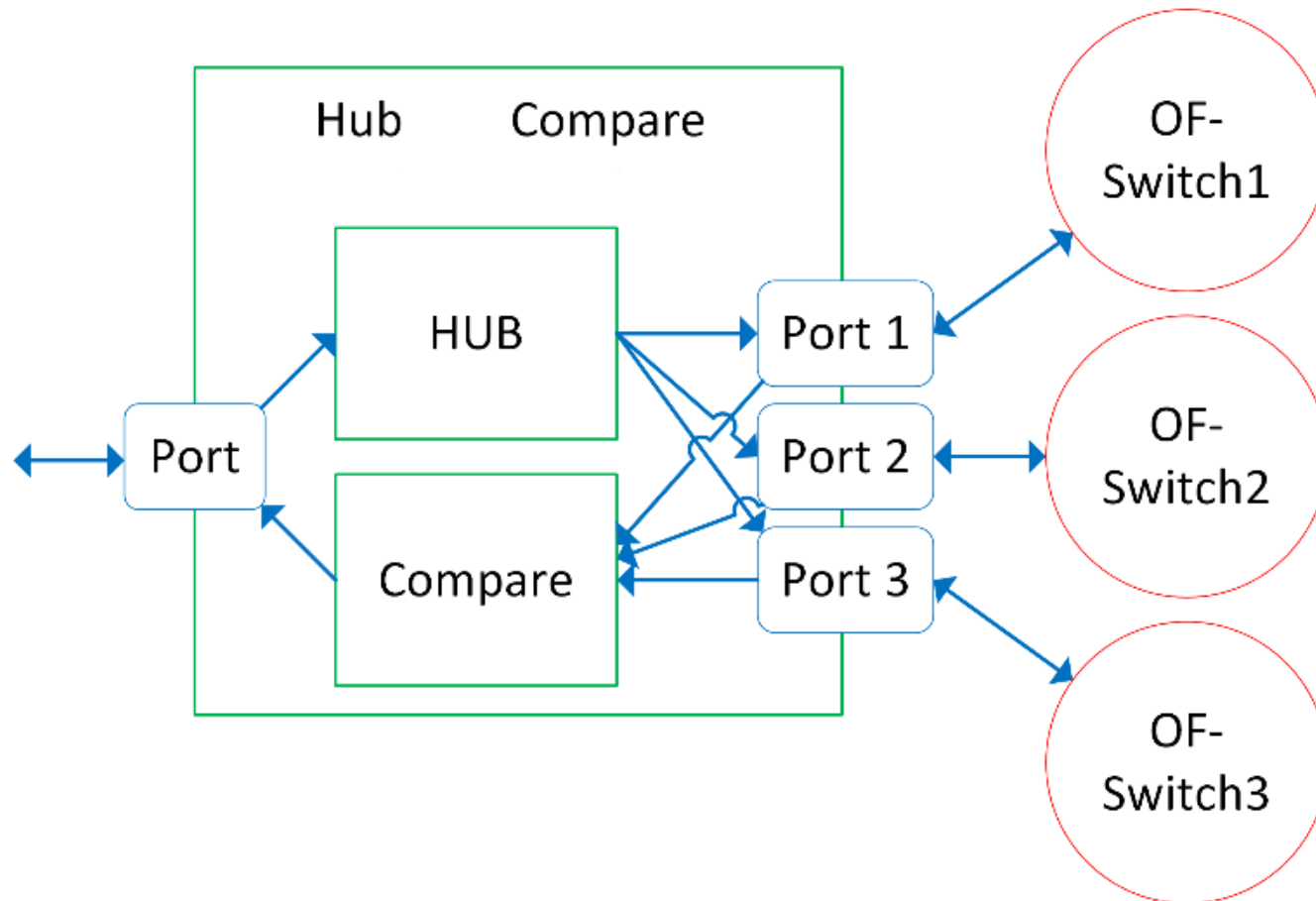
5. NetCo approach

- Constructions allowing to detect malicious behaviour and prevent it



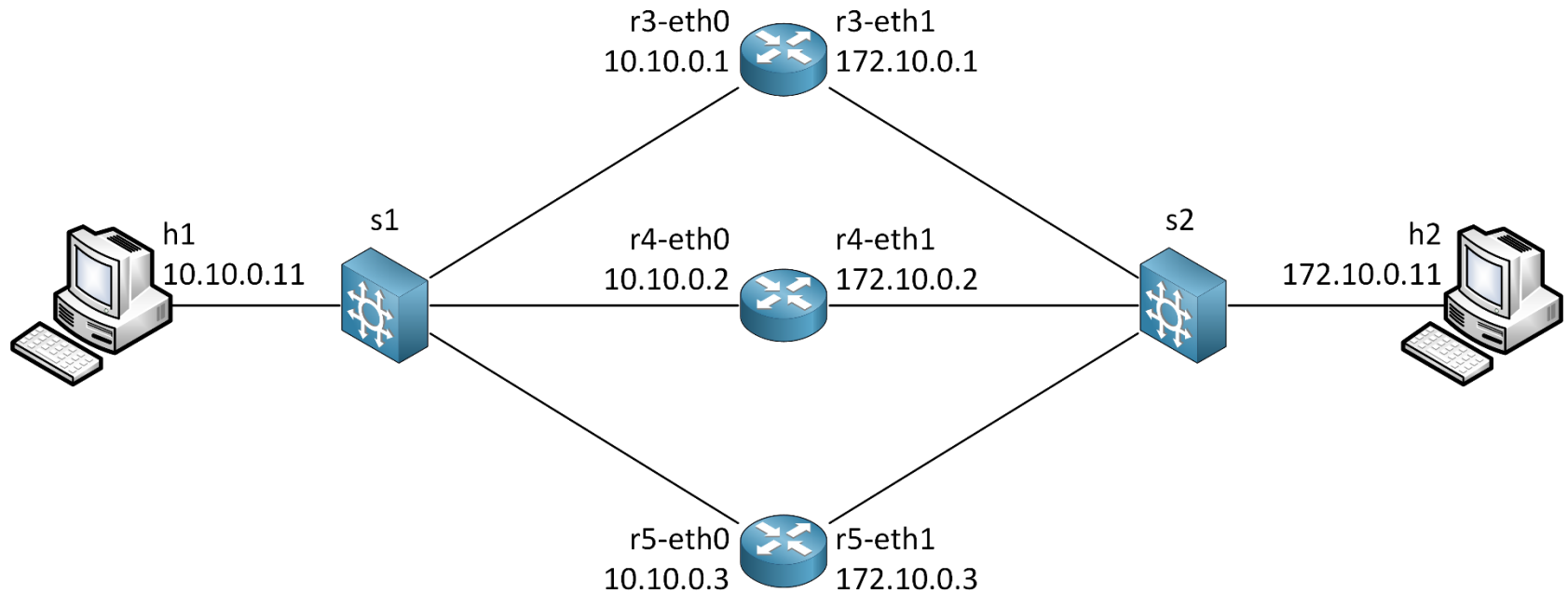
Only for exemplification: Unidirectional schematic representation

5. NetCo approach



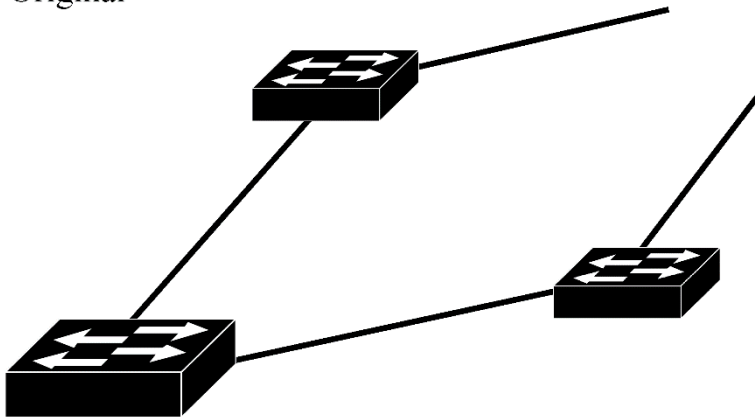
Exemplification: Port-centric bidirectional schematic representation

5. NetCo approach

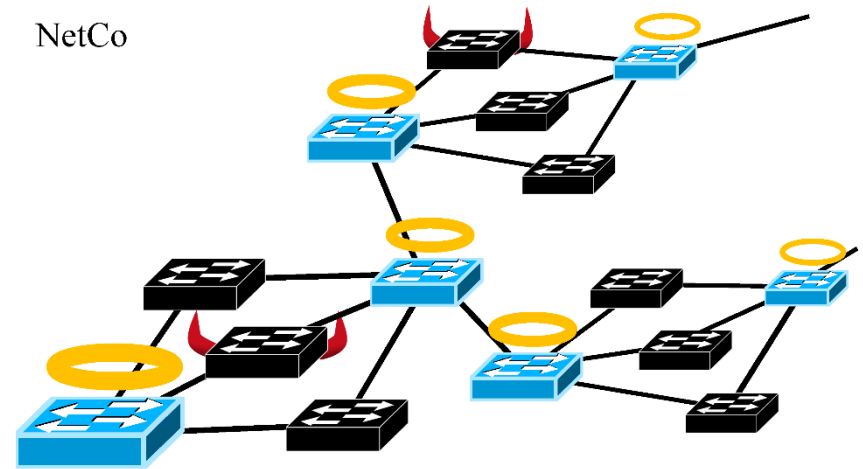


5. NetCo approach

Original



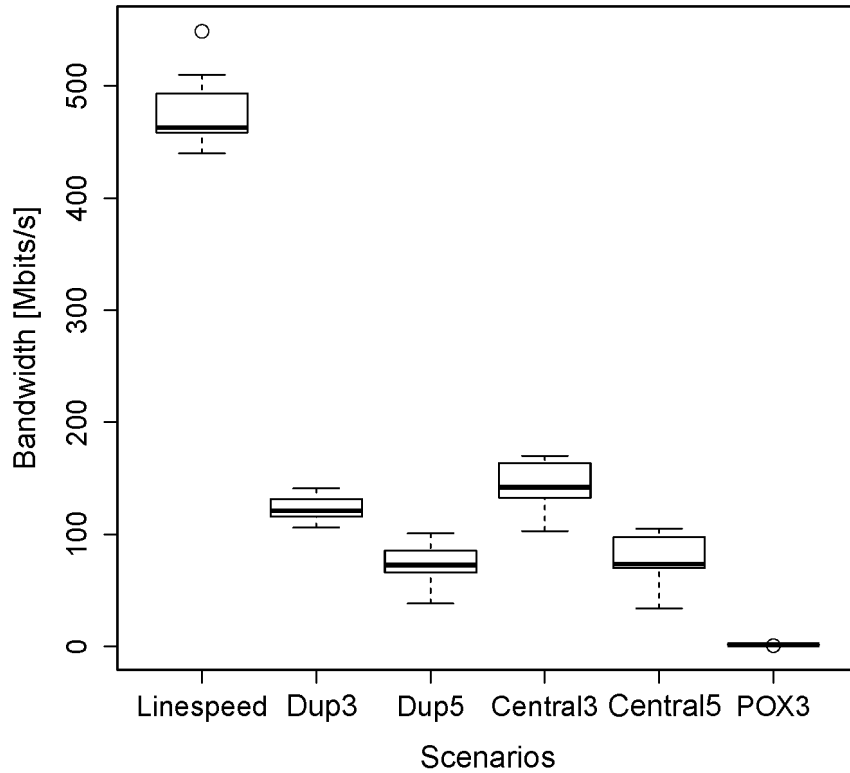
NetCo



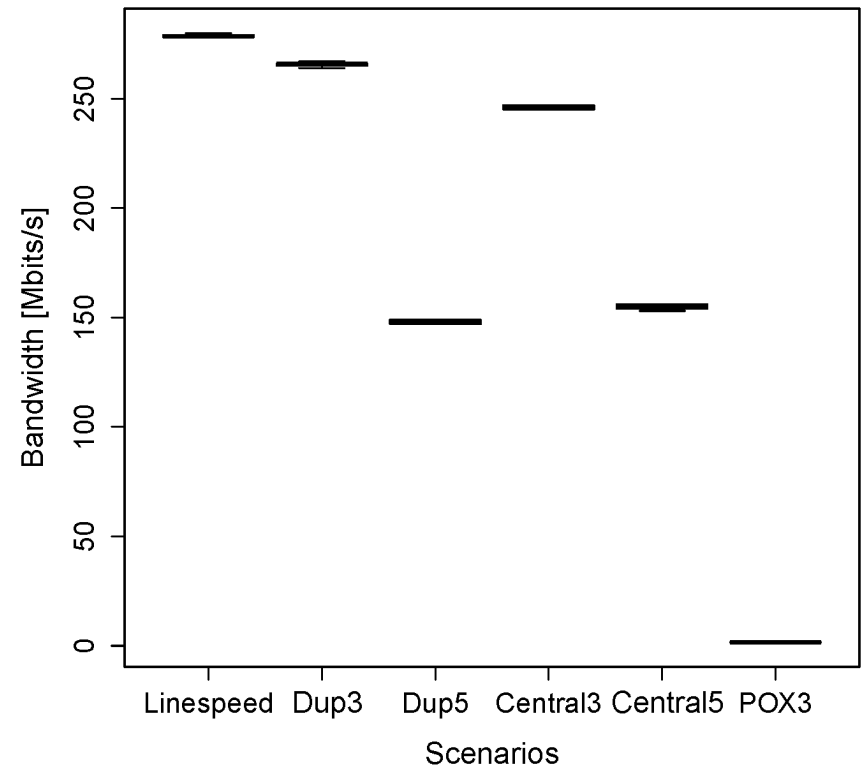
6. Performance

- **Linespeed:** The simplest abstraction of our testing topology features only h1, s1, r3, s2 and h2. A benchmark for the ideal performance, which informs our expectations.
- **Central3:** The full prototype implementation, featuring $k = 3$ test routers.
- **Central5:** The full prototype implementation, featuring $k = 5$ test routers.
- **POX3:** A reference implementation of NetCo as a SDN application running on the POX controller
- **Dup3:** Nodes s1 and s2 act as hubs, duplicate packets are not removed. Three test routers are put in a parallel circuit.
- **Dup5:** Nodes s1 and s2 act as hubs, duplicate packets are not removed. Five test routers are put in a parallel circuit.

6. Performance



TCP throughput



UDP throughput

7. Conclusion: Four examples reloaded

- CISCO
- Huawei
- Juniper
- Alcatel-Lucent

7. Conclusion: Reliable routing on unreliable networks

- Detection and prevention: bounded-collusion stealthy adversary
- Prototype: Very early stage of NetCo
- Robust combiner concept: create efficient, low-cost yet resilient networks, from untrusted network devices

Contact

- Dr. Michael Kreutzer
Fraunhofer SIT
Rheinstraße 75
64295 Darmstadt

+49 6151- 869 348
michael.kreutzer@sit.fraunhofer.de