

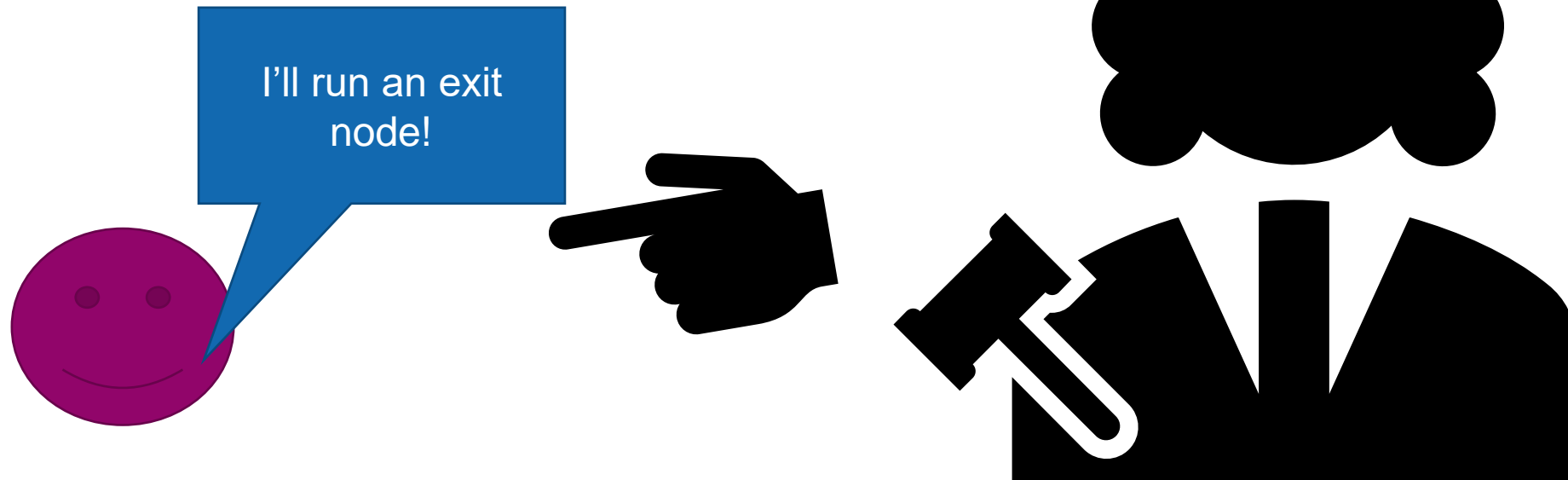
# Discussion exercise sheet 7

**Marc-Philippe Bartholomä**  
Student Assistant for Network Security 2020  
05 November 2020, At home



# Question 1 - TOR - Reprisal

- Related Material: [06-ACS](#): slide 48
- Question: Why exit policies?





# Question 1 - TOR - Reprisal

- Related Material: [06-ACS](#): slide 56
- Question: Why facebookcorewwi.onion?
  - Based on key -> Brute force
  - netsec2h4c75huw5.onion

-----BEGIN RSA PRIVATE KEY-----

```
MIICXgIBAAKBgQCvnMpqG+cFDhx8tCCIPbUMudqbmKvVW/eT8Uwz9KIk1cEVpMVGf
b//wabhhICbz1V/Todr0ucV95gEamSiAnpab2nyMlcc+8EReJ2QjBCIgyIBmxJEa
BrKdW4DF3UbHqSa1uJ6lsHuyJ0CqysOxaavPI4leFMokGI9hdyY1eP6MEQIENIG0
RwKBgAPtMEF4jKMXHG5thml1jJEM3USuOZTgWcSLNNvXebxYrFCM2dPL6pygmSod
MYZF/meaxGT93SIfRRUfnCqqVS7TwenqeKvmZPBpP9BNZ5DXsEF35lzfICl3bpQy
iA291a7Dj50a23lg3m3DjbMakwV5/lw7zv+y85uoT3+ZiBehAkEA258TnV0dS3/9
o+CYC3G2RNfyPWWOWQnSm8LmleBe/7uop+N6A0ZINro+HfSCda3RV5lqUQsgdH0b
y6SmfINoEwJBAMyzijE9XoKPPUNQIWgcWVj/oaYNrleJz3sY+9Y6YCfgo3iJukx
60zmZsCe8LISw3m3MbWWpjLITObdmRxDh8sCQDtUnrrHHiZtLjJko8AI2yffQuii
wPbmFPLAt2sN5m2iJDI89HFfMYxw0zw22rqm9ZmrT1rG2wm9I7oFPfVBgssCQQCm
ZZNLSpOfpWY0quLeq4kKhIG1mgahP1tFyKJuRCEt/B07jLU7FMgkTvRObt3yWA0N
0EOVT9UwzYfYI1YshZnLAKeApNKOVqx5bRDfGQY72mZTljBf1Qp4qBfM7NvcvD8m
wnxcT8iDU5aRKmrVbJc4Lepu6HprYLy7XaZ6tX0eqO2m/A==
```

-----END RSA PRIVATE KEY-----

```
time ./eschalot -v -t8 -p netsec >> netsec.txt
Running, collecting performance data...
```

```
Total hashes: 369017267, running time: 10 seconds, hashes per second: 36901726
Total hashes: 1114732814, running time: 31 seconds, hashes per second: 35959123
Total hashes: 2533180204, running time: 71 seconds, hashes per second: 35678594
Found a key for netsec (6) - netsec2h4c75huw5.onion
```

```
real    1m52.596s
```

<https://opensource.com/article/19/8/how-create-vanity-tor-onion-address>

# Question 1 - TOR - Reprisal

- Related Material: [06-ACS](#): slide 59
- Question: Why relay limit per subnet?



Might I also interest you in the book after which the attack you are performing is named?

Books > Health, Fitness & Dieting > Psychology & Counseling



## Sybil: The Classic True Story of a Woman Possessed by Sixteen Separate Personalities Mass Market Paperback – Illustrated, January 1, 1973

by [Flora Rheta Schreiber](#) (Author)

★★★★☆ 489 ratings

[See all formats and editions](#)

School & Library Binding  
\$12.92

Paperback  
\$10.19

**Mass Market Paperback**  
**\$9.99**

20 Used from \$8.94  
12 New from \$16.67

8 Used from \$7.37  
5 New from \$10.19

51 Used from \$1.92  
17 New from \$6.09

More amazing than any work of fiction, yet true in every word, it swept to the top of the bestseller lists and riveted the consciousness of the world. As an Emmy Award-winning film starring Sally Field, it captured the home screens of an entire nation and has endured as the most electrifying TV movie ever made. It's the story of a survivor of terrifying childhood abuse, victim of sudden and mystifying blackouts, and the first case of multiple personality ever to be psychoanalyzed.

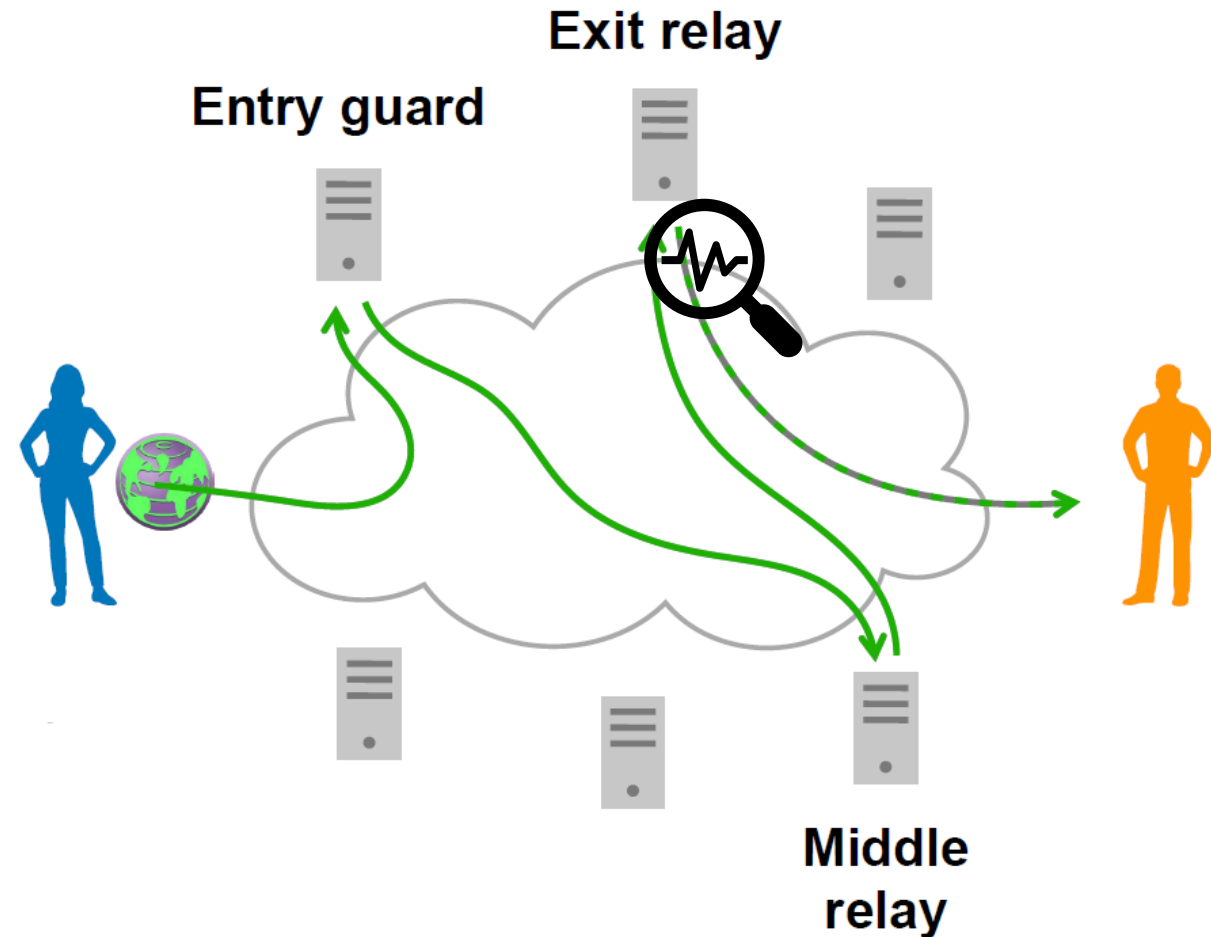
You're about to meet Sybil-and the sixteen selves to whom she played host, both women and men, each with a different personality, speech pattern, and even personal appearance. You'll experience the strangeness and fascination of one woman's rare affliction-and travel with her on her long, ultimately triumphant journey back to wholeness.



[See all 3 images](#)

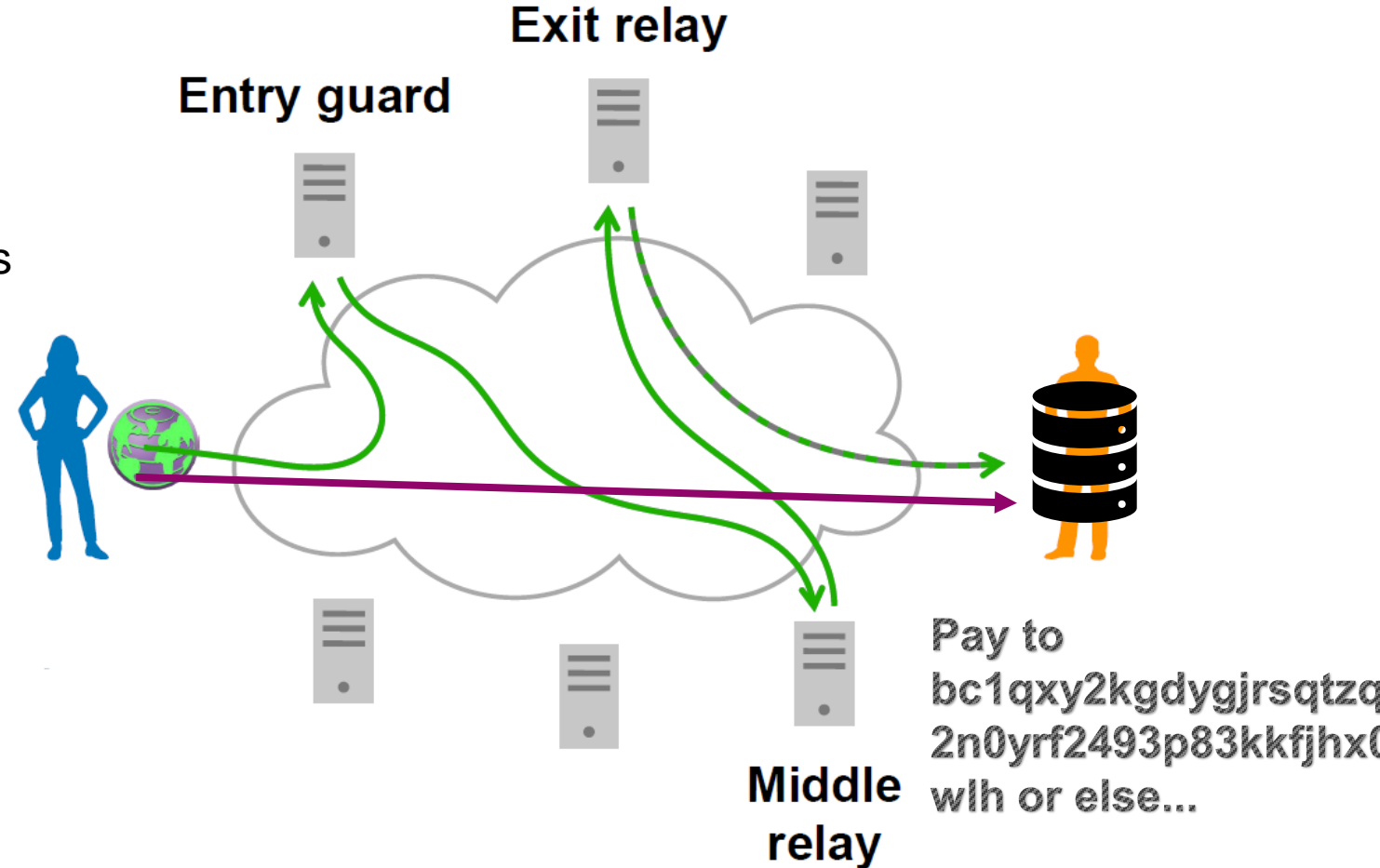
## Question 2 - TOR – Malicious Exit relays

- Related Material: [06-ACS](#): slide 47
- Question: HTTP a problem?
  - Yes, MitM!
  - HTTPS works a usual



## Question 2 - TOR – Malicious Exit relays

- Related Material: [06-ACS](#): slide 47
- Question: Detection?
  - Contact with and without TOR
  - Different content proves maliciousness
  - Juicy target: bitcoin addresses

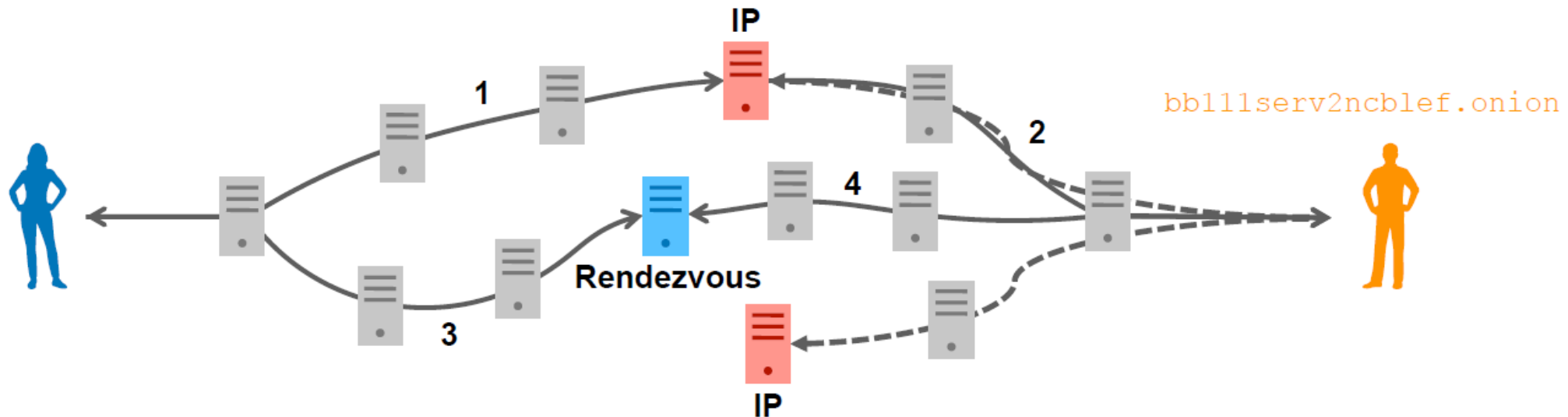


## Question 2 - TOR – Malicious Exit relays

- Related Material: [06-ACS](#): slide 55
- Question: Same with hidden service?

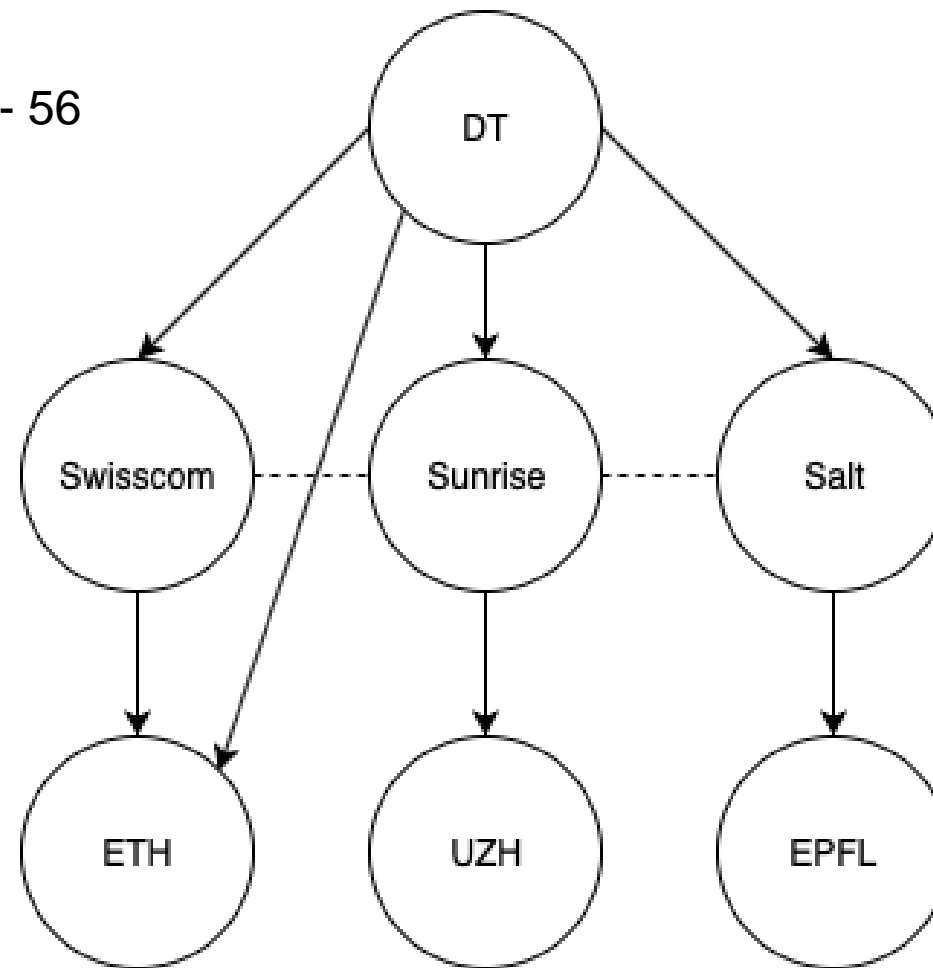
No, there is no exit relay.  
(also Hidden services  
are always encrypted)

### Hidden services



## Question 3 – BGP Relationships

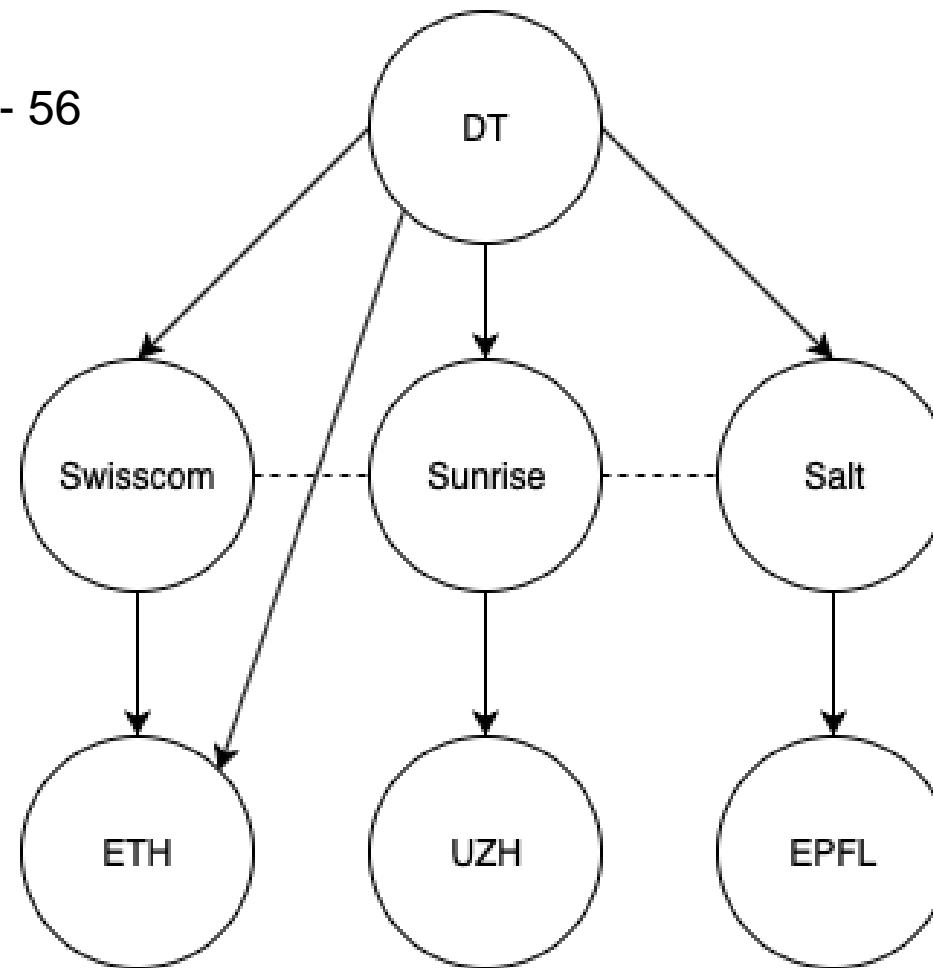
- Related Material: [01c-net-refresher](#): slide 53 - 56
- Question: ETH -> UZH?





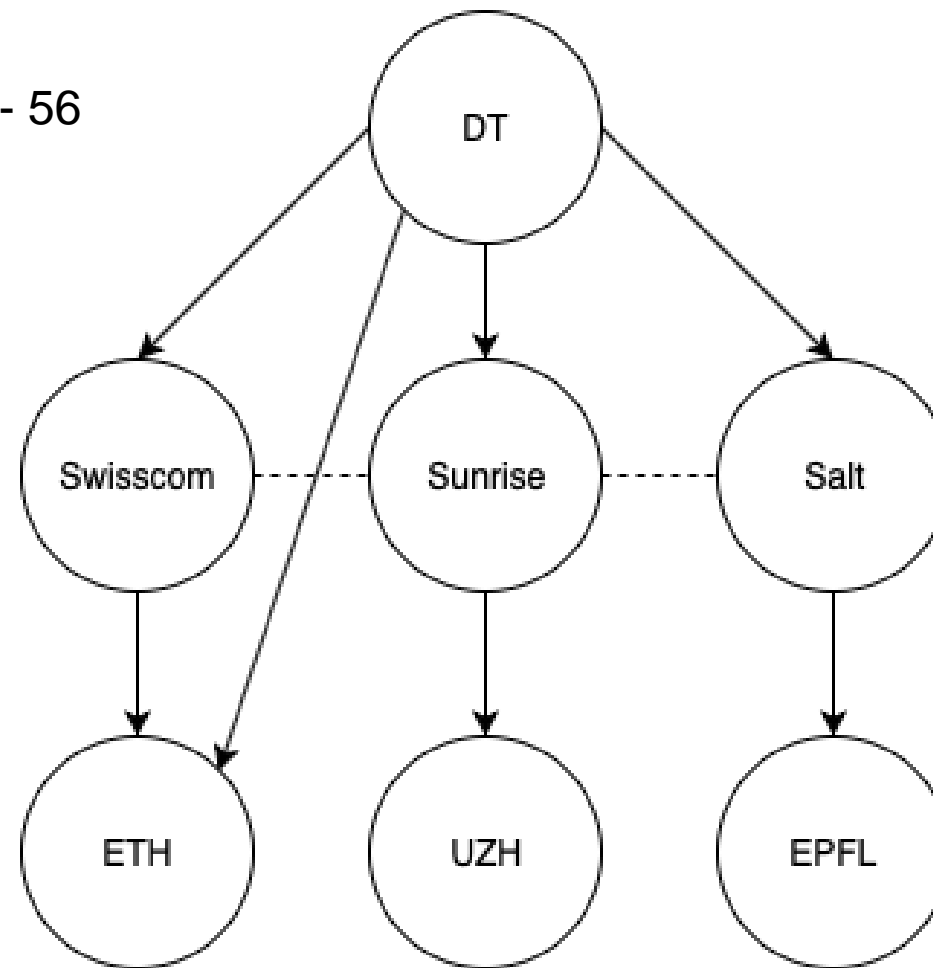
## Question 3 – BGP Relationships

- Related Material: [01c-net-refresher](#): slide 53 - 56
- Question: ETH -> EPFL?



## Question 3 – BGP Relationships

- Related Material: [01c-net-refresher](#): slide 53 - 56
- Question: ETH announces DT?
  - Swisscom to EPFL
  - Swisscom to Sunrise



# Question 4 – BGP Attacks

- Related Material: [07-BGP](#): slide 48, [RIPE article](#)
- Question: Pakistan censors Youtube?
  - [BGPlay 208.65.152.0/22](#)
  - [BGPlay 208.65.153.0/24](#)

# Question 4 – BGP Attacks

- Related Material: [07-BGP](#): slide 48, [BGPmon article](#)
- Question: AS12389 in 2017?

Starting at April 26 22:36 UTC till approximately 22:43 UTC AS12389 (PJSC Rostelecom) started to originate 50 prefixes for numerous other Autonomous systems. The 50 hijacked prefixes included 37 unique autonomous systems and the complete list of affected networks can be found below. If your organization is in this list feel free to reach out and we can provide more

3303 Swisscom (Switzerland) Ltd

30060 VeriSign Infrastructure & Operations

2559 Visa International

15632 JSC Alfa-Bank

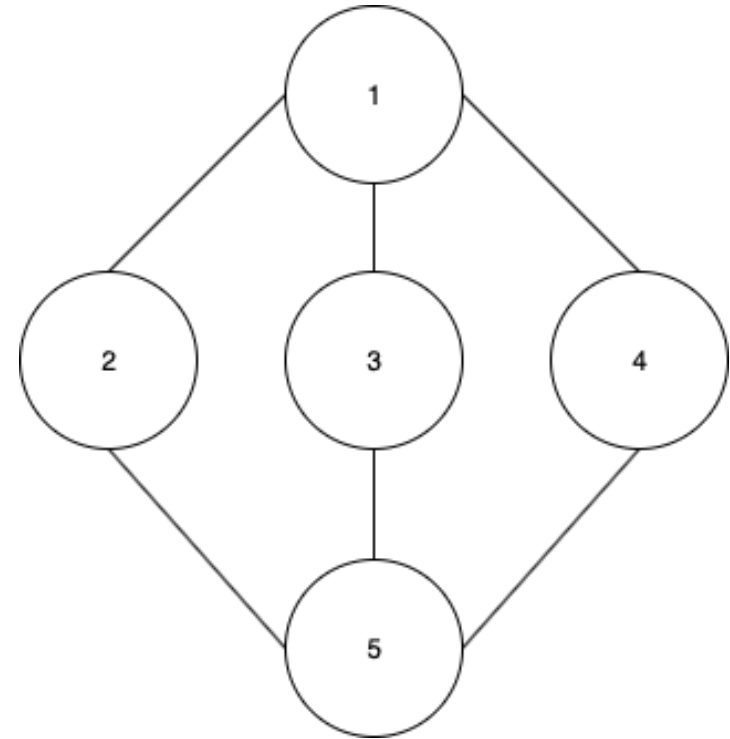
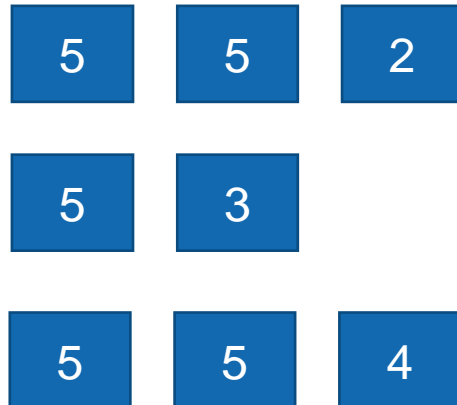
9221 HSBC HongKong

26380 MasterCard Technologies LLC

# Question 5 – Traffic Engineering

- Related Material: [07-BGP](#): slide 22 -23
- Question: Add own AS multiple times?
  - Shorter paths preferred
  - Make one path longer to signal preference

- View from 1:

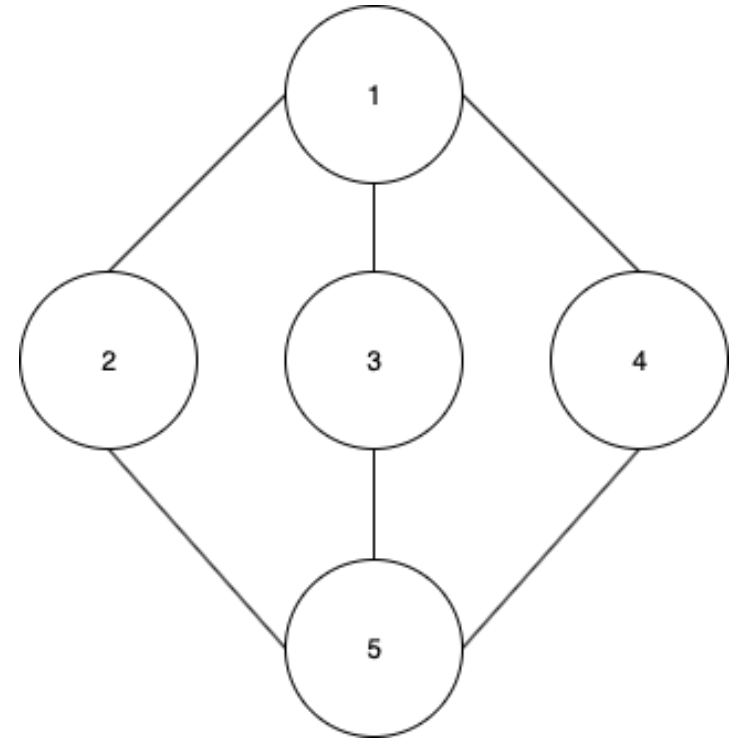
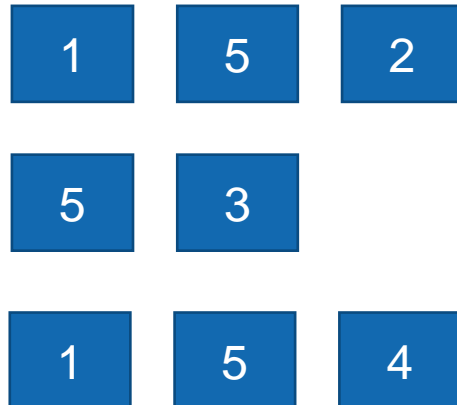




# Question 5 – Traffic Engineering

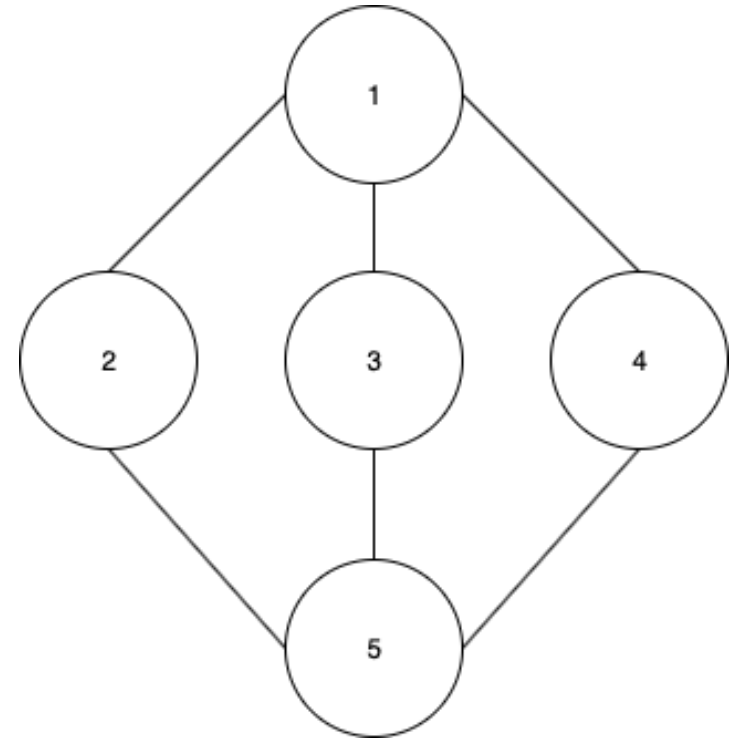
- Related Material: [07-BGP](#): slide 22 -23
- Question: Add foreign AS to path?
  - Ignored by added AS due to loop detection
  - Make one path longer to signal preference

- View from 1:



# Question 5 – Traffic Engineering

- Related Material: [07-BGP](#): slide 22 -23
- Question: 1 wants to eavesdrop 3 -> 5 and 4 -> 5?
  - Announce IP subprefix
  - Add 2 to the announcement to be able to forward to 5



# Your Questions