ETH zürich

Discussion exercise sheet 1

Marc-Philippe Bartholomä
Student Assistant for Network Security 2020
23 September 2020, HG F1

Exercise Sessions for Network Security 2020

	Exercise	24.09.2020	Introduction to Project 1: ACME Client Discussion exercise sheet 1
week 3	**Lecture**	29.09.2020	TLS [KP]
	Exercise	01.10.2020	Guest: Nico Schottelius, Ungleich, "Security Aspects of IPv6" Discussion exercise sheet
week 4	**Lecture**	06.10.2020	TLS [KP]
	Exercise	08.10.2020	Discussion exercise sheet Question hour

Online; submit questions in advance

- Assumption: You have solved (or at least looked at) the exercise sheet!
- Feel free to ask questions anonymously!

Question 1

- Related Material: 01b-crypto-refresher: slides 3 – 6
- Question: Security property and example

- Ed wants to prove to Laura that the is the sender of a message.
  - Integrity or Authentication?
  - Example: digital signatures or HMACs

- Ed wants to send a secret message to Glenn.
  - Confidentiality or Secrecy?
  - Example: asymmetric encryption

Question 1

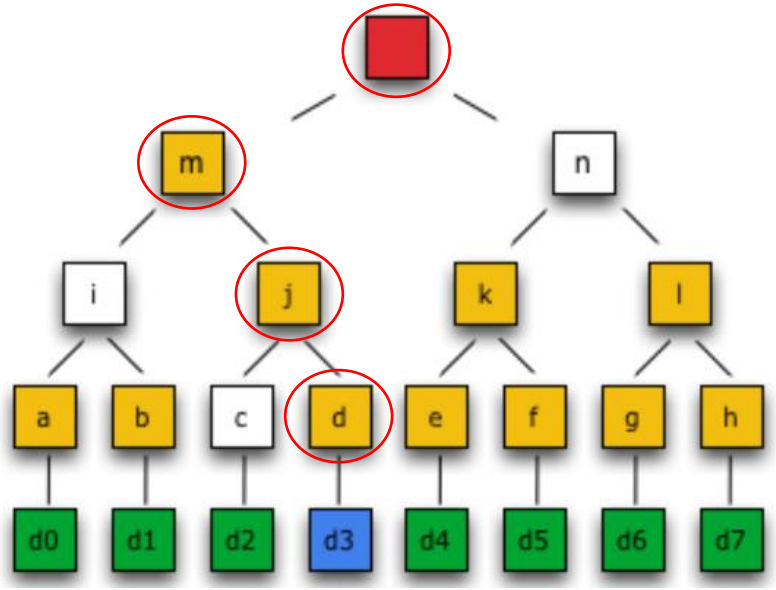
- Related Material: 01b-crypto-refresher: slides 3 – 6
- Question: Security property and example

- Ed wants to store records and ensure that they won't be altered
  - Integrity or Data authentication?
  - Example: TLS or IPsec

- Chelsea wants to share documents without being identified.
  - Anonymity or Privacy?
  - Example: TOR

Question 2

- Related Material: 01b-crypto-refresher: slides 47 – 48
- Question: Recomputation cost for updating a leaf in a Merkle Hash Tree



$O(\log_2 n)$

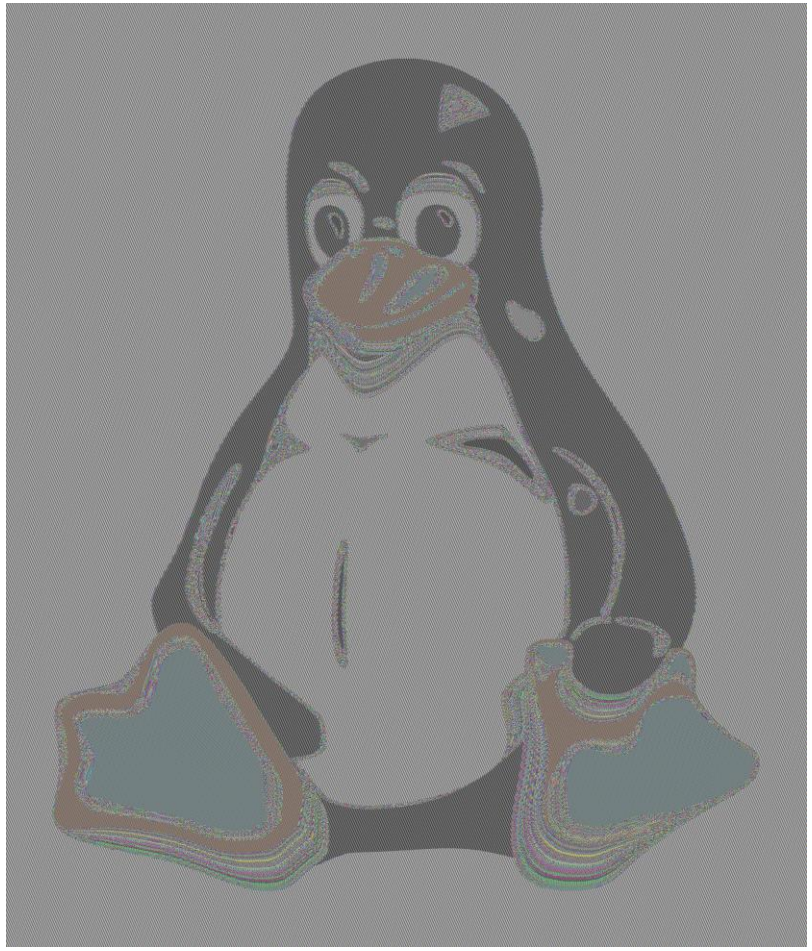
Source: 02-PKI: slide 47

Question 3

- Related Material: 01b-crypto-refresher: slides 16 – 17
- Question: Usage of AES-ECB on image

The Zoom transport protocol adds Zoom's own encryption scheme to RTP in an unusual way. By default, all participants' audio and video in a Zoom meeting appears to be encrypted and decrypted with a single AES-128 key shared amongst the participants. The AES key appears to be generated and distributed to the meeting's participants by Zoom servers. Zoom's encryption and decryption use AES in ECB mode, which is well-understood to be a bad idea, because this mode of encryption preserves patterns in the input. Industry standard protocols for encryption of streaming media (e.g., the SRTP standard) recommend the use of AES in Segmented Integer Counter Mode or f8-mode, which do not have the same weakness as ECB mode.

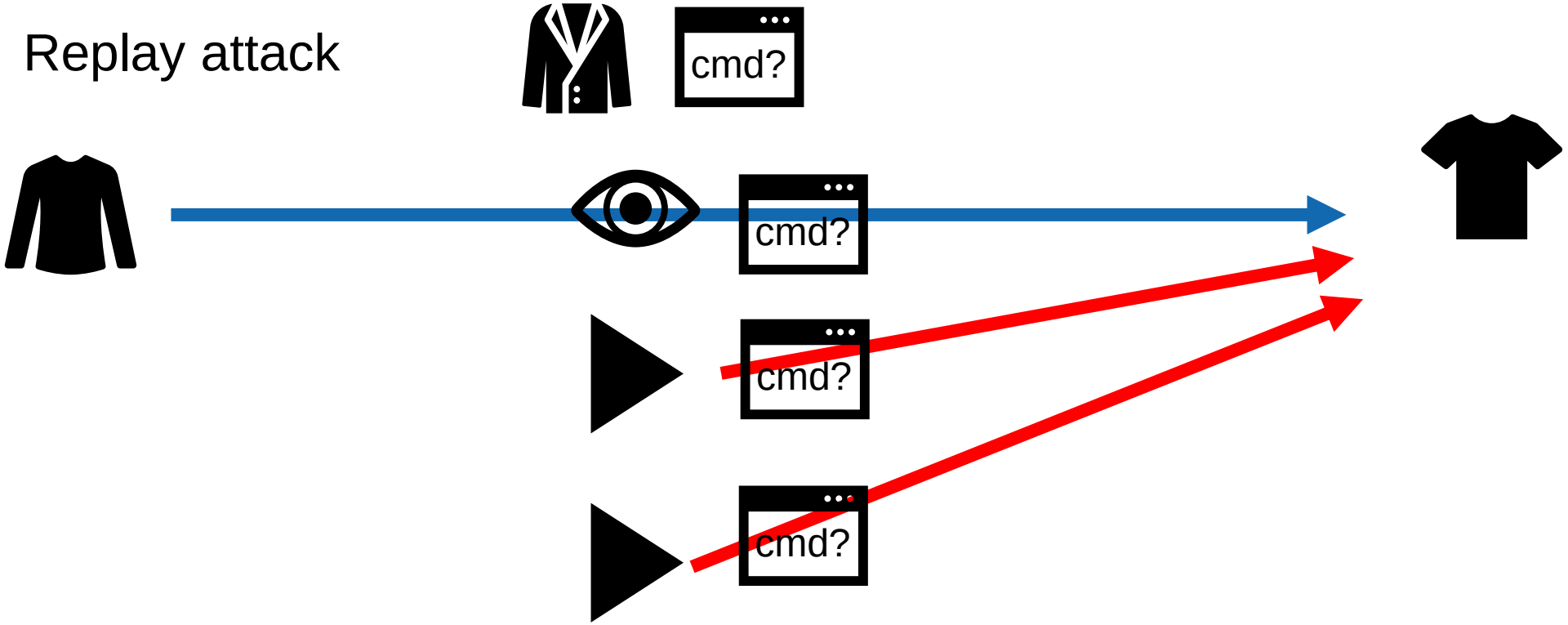
https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/



Question 4

- Related Material: 01b-crypto-refresher: slides 18 – 19
- Question: Network protocol to control your server using AES-CBC

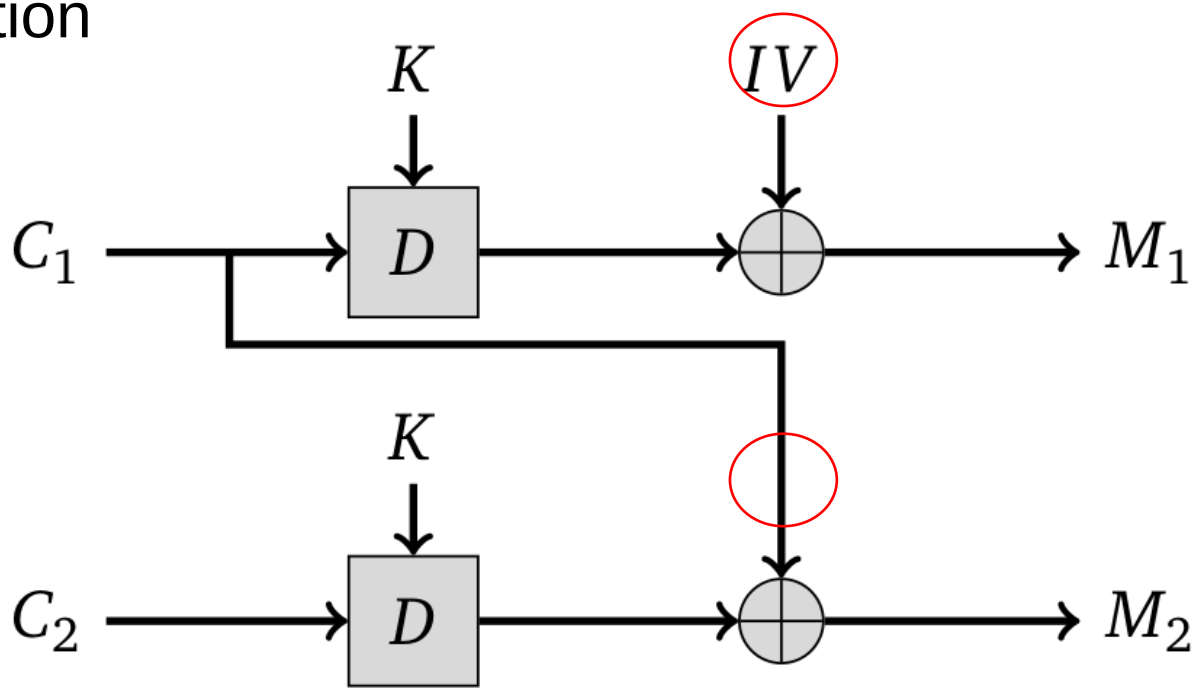
Replay attack



Question 4

- Related Material: 01b-crypto-refresher: slides 18 – 19
- Question: Network protocol to control your server using AES-CBC

Manipulation



Question 4

- Bonus Material: RFC 2315
- Question: Network protocol to control your server using AES-CBC **with MAC and padding**

Background: PKCS #7 Padding

1 byte to pad:	0x??	0x??	0x??	0x??	0x??	0x??	0x??	**0x01**
2 bytes to pad:	0x??	0x??	0x??	0x??	0x??	0x??	**0x02**	**0x02**
3 bytes to pad:	0x??	0x??	0x??	0x??	0x??	**0x03**	**0x03**	**0x03**

Question 4

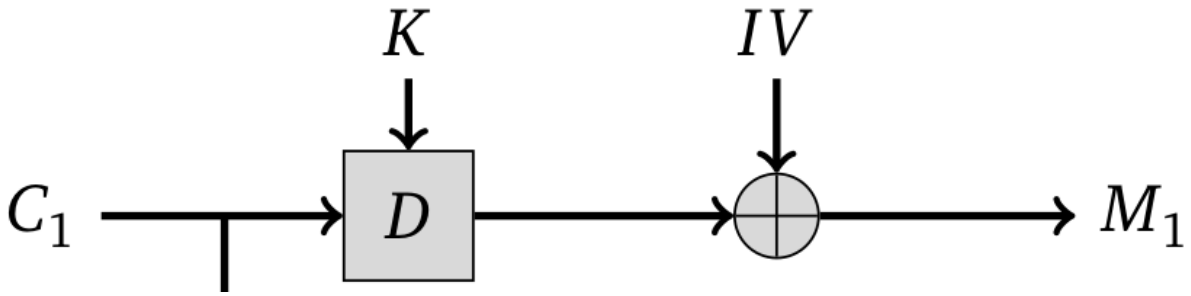
- Bonus Material: [blog post by Ron Bowes]
- Question: Network protocol to control your server using AES-CBC **with MAC and padding**

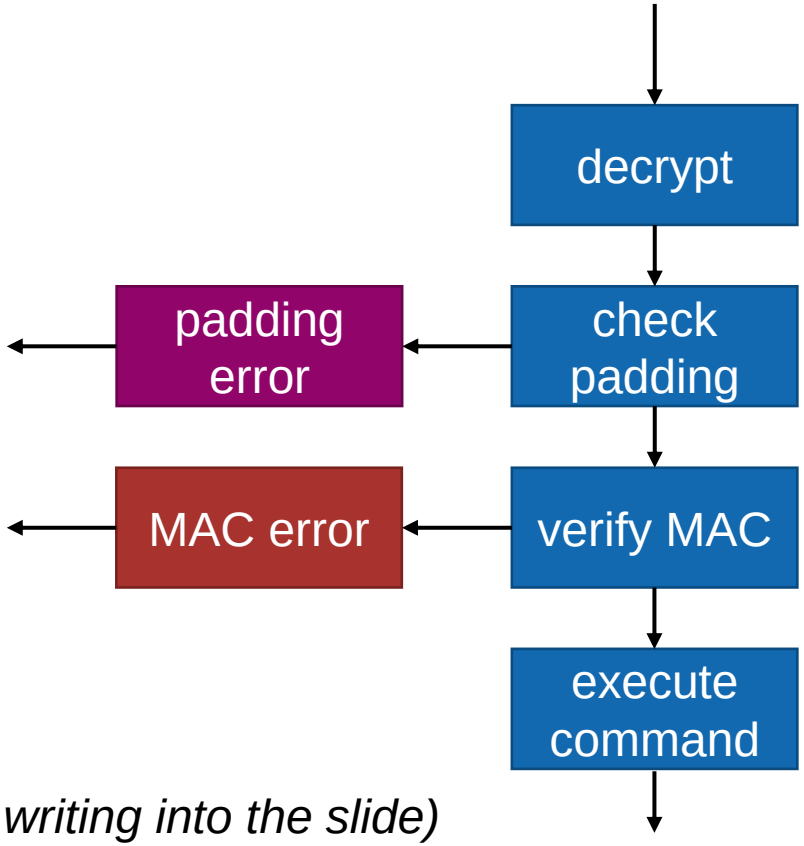
Padding Oracle Attack

Ciphertext Block

0x??	0x??	0x??	0x??

IV





(Explained by writing into the slide)

Question 5

- Related Material: 01c-networking-refresher: slides 68 - 76
- Question: Bandwidth allocation

- Explain:
  - Way of allocating total available bandwidth to senders
  - Efficient: capacity used but no congestion
  - Fair: every sender gets a reasonable share

Question 5

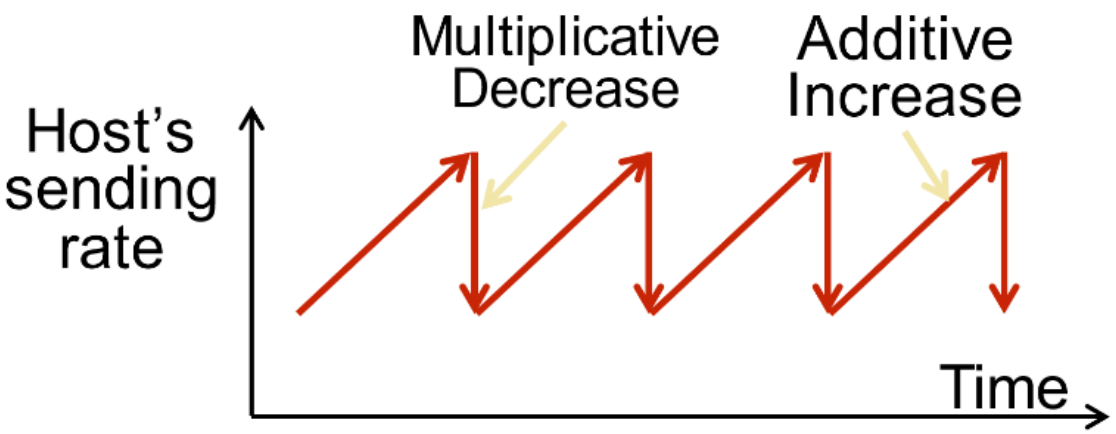
- Related Material: 01c-networking-refresher: slides 68 - 76
- Question: Bandwidth allocation
- What UDP does:

Source: https://http.cat/404

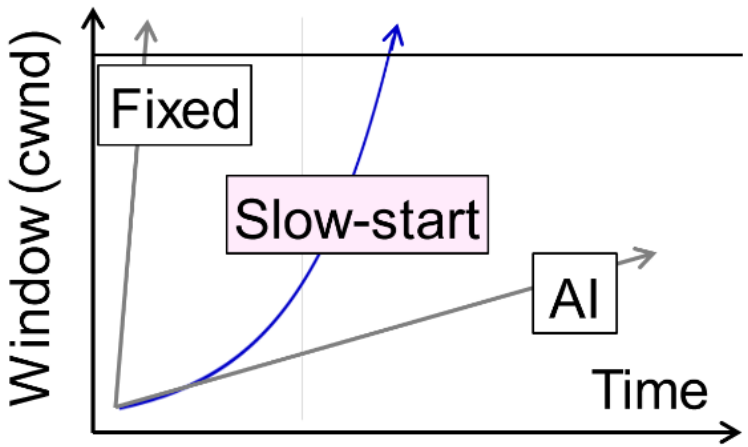
Question 5

- Related Material: 01c-networking-refresher: slides 68 - 76
- Question: Bandwidth allocation

- What TCP does:



+



Question 5

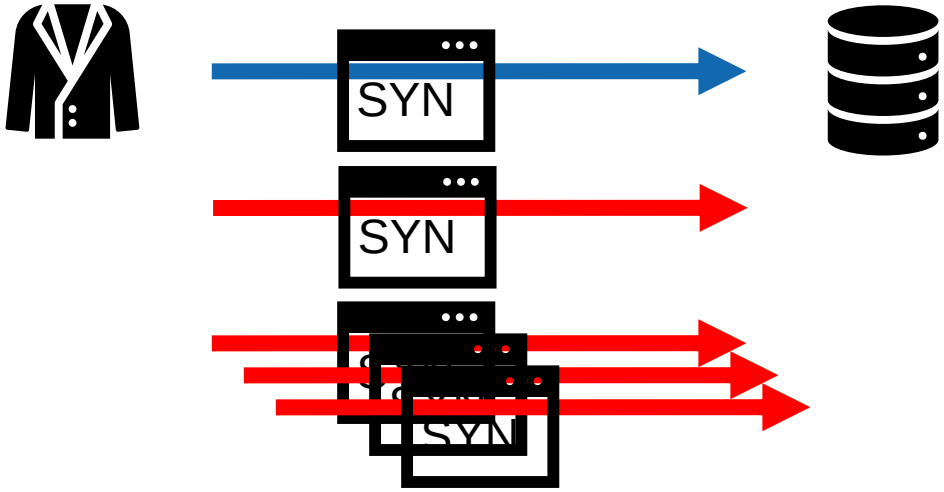
- Related Material: 01c-networking-refresher: slide 76
- Question: UDP & TCP

- When is UDP still useful?
  - When some features of TCP aren’t required
  - e. g. no reliability needed

Question 5

- Related Material: [01c-networking-refresher](): slides 60 - 62
- Question: UDP & TCP

- TCP requires server resources per open connection. Attack?

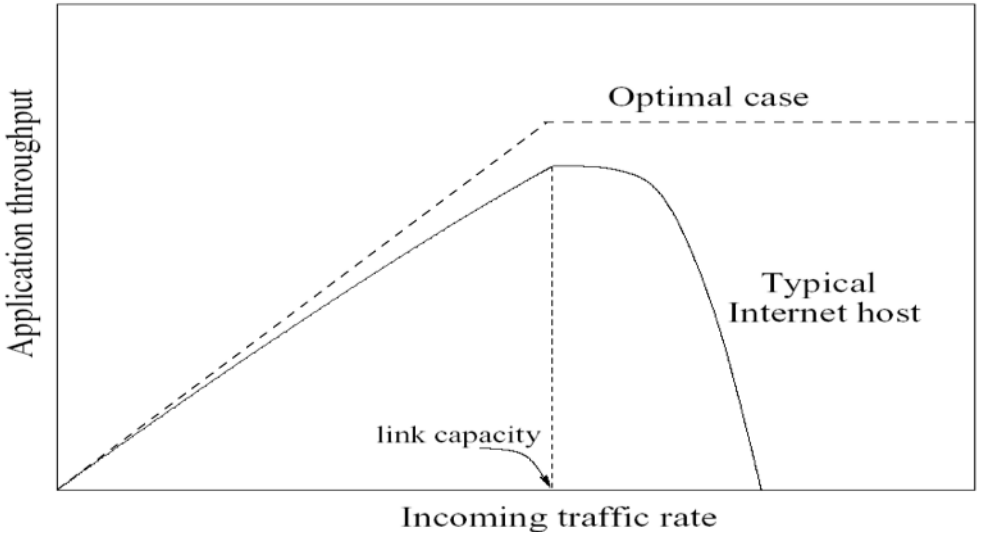


Con 1									
Con 2									
Con 3									
Con 4									
Con 5									

Question 6

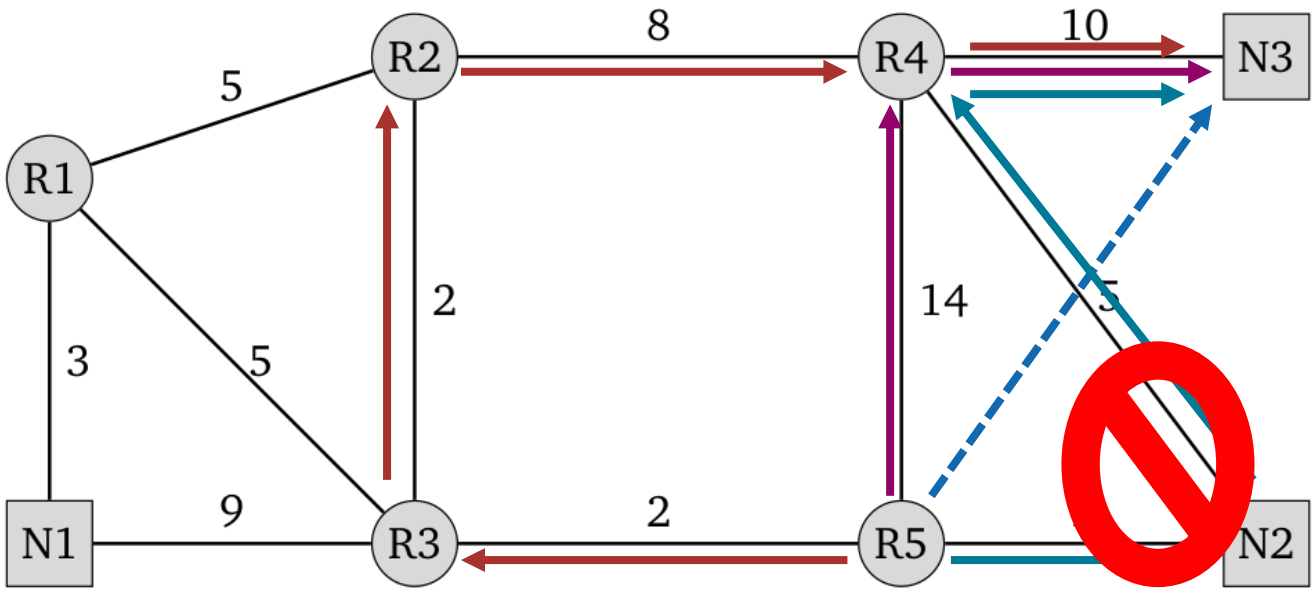
- Related Material: not available
- Question: Congestion

Congestion Collapse



Question 7

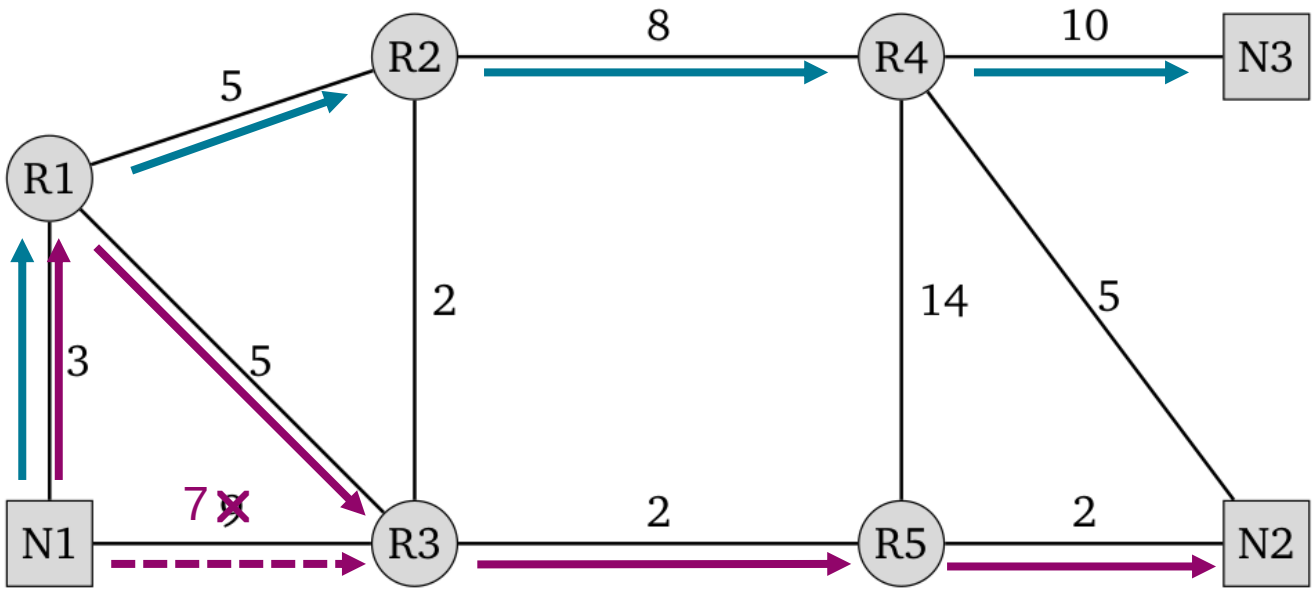
- Related Material: 01c-networking-refresher: slides 27, 29
- Question: OSPF
- From R5 to N3?
  - Answer R5 -> R3 -> R2 -> R5 -> N3



Illegal path!
Can’t route through network!

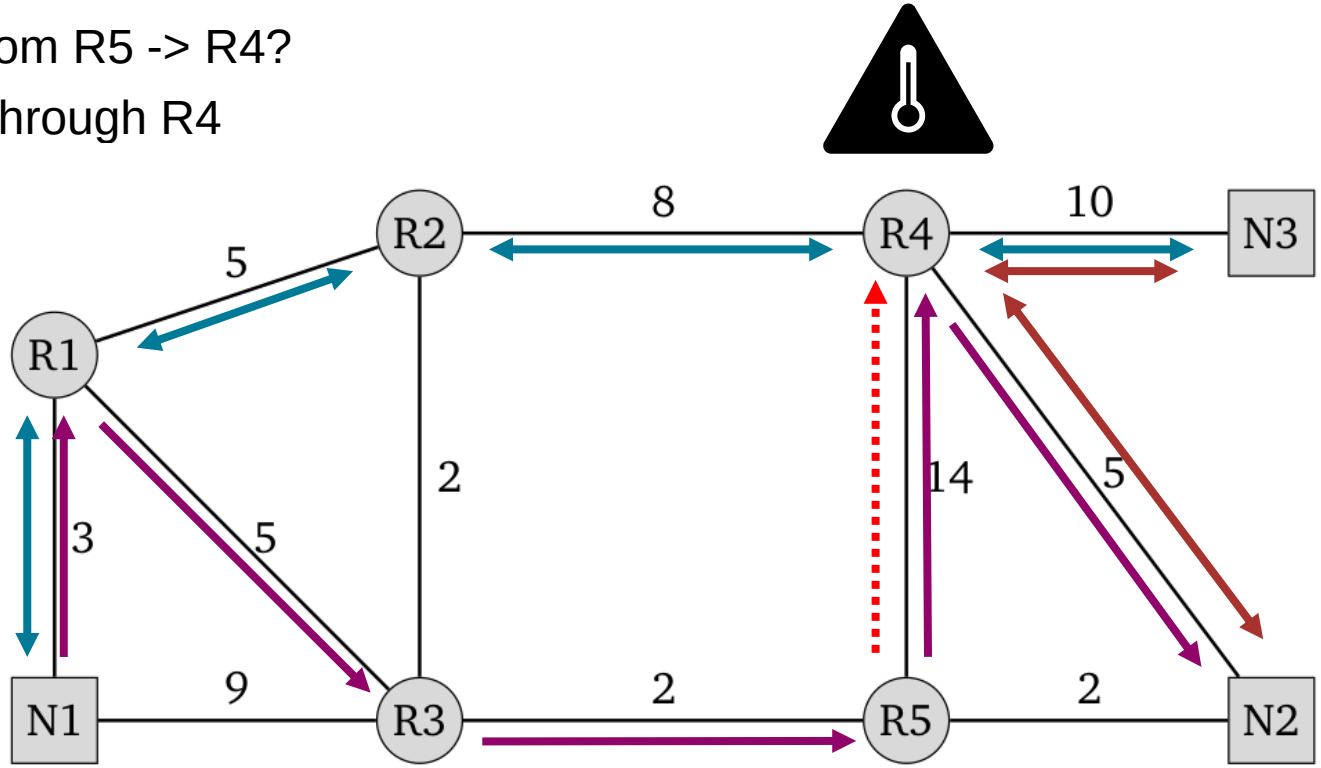
Question 7

- Related Material: 01c-networking-refresher: slides 27, 29
- Question: OSPF
- Are N1 -> N3 and N1 -> N2 disjoint?
  - No, change N1 <-> R3



Question 7

- Related Material: 01c-networking-refresher: slides 27, 29
- Question: OSPF
- Static Route from R5 -> R4?
  - More goes through R4



Your Questions