NFS TD 2

I Introduction

In today's TD, we will practice the infamous IPv4 mask calculation, IP routing, and take a look at a bit of cryptographic consideration.

II Mask Calculation

Here are three IPv4 addresses:

- 192.0.2.1/24
- 192.0.2.1/16
- 192.0.2.1/8

Question 1: For each of them, identify the network and host parts.

Question 2: Fill the following CIDR table

Decimal	CIDR	Binary	Addresses
255.255.255.000	/24	11111111.11111111.11111111.00000000	2^{32-24}
	/32		
	/6		
	/28		
	/29		
	/0		
	/10		
	/31		
	/7		
	/30		
	/2		
	/25		
	/27		
	/23		
	/8		
	/22		
	/1		
	/21		
	/26		
	/9		

II.1 Subnetting

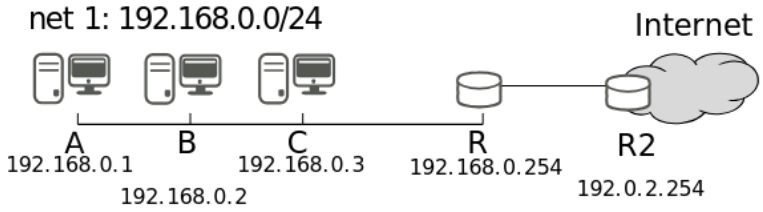
You are given the network 153.168.0.0/16 and would like to create subnets for the 6 departments of your company.

Question 3: Complete de table with all created networks.

Network	Mask	# Hosts	Range	Broadcast
_____			_____	_____
_____			_____	_____
_____			_____	_____
_____			_____	_____
_____			_____	_____
_____			_____	_____
_____			_____	_____
_____			_____	_____

II.2 Routing

II.2.1 Small Network with outbound access



In the context above:

Question 4: Write A's routing table.

Domain	Route
_____._____._____._____/___	_____
_____._____._____._____/___	_____
_____._____._____._____/___	_____
_____._____._____._____/___	_____
_____._____._____._____/___	_____

Question 5: Write R's routing table.

Domain	Route
_____._____._____._____/___	_____
_____._____._____._____/___	_____
_____._____._____._____/___	_____
_____._____._____._____/___	_____
_____._____._____._____/___	_____

II.2.2 Route prioritization

You own the 192.0.2.0/23 network, and have two routers: R1 linked to the internet Provider1, and R2 to Provider2. As the second provider is more expansive, you want to only use it if the first provider is down.

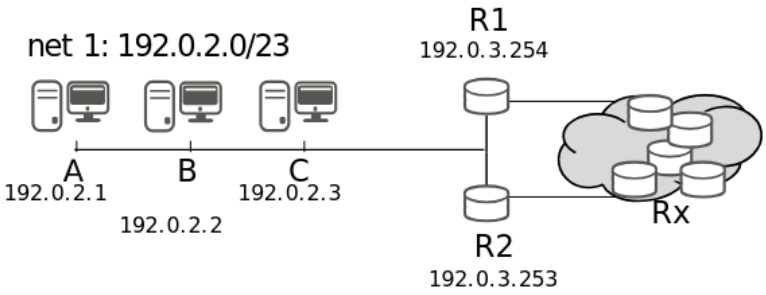


Figure 2: Network 192.0.2.0/23

Question 6: By only using network masks, complete the routing table of C to prioritize R1 over R2.

Domain	Route
_____._____._____._____/___	_____
_____._____._____._____/___	_____
_____._____._____._____/___	_____
_____._____._____._____/___	_____
_____._____._____._____/___	_____

Note: In practice, we can use metrics to indicate which road to prioritize.

III Crypto Essentials

III.1 Symmetric and Asymmetric

Question 7: Explain the main differences between symmetric and asymmetric cryptography including efficiency and key exchange problems.

III.2 Diffie-Hellman

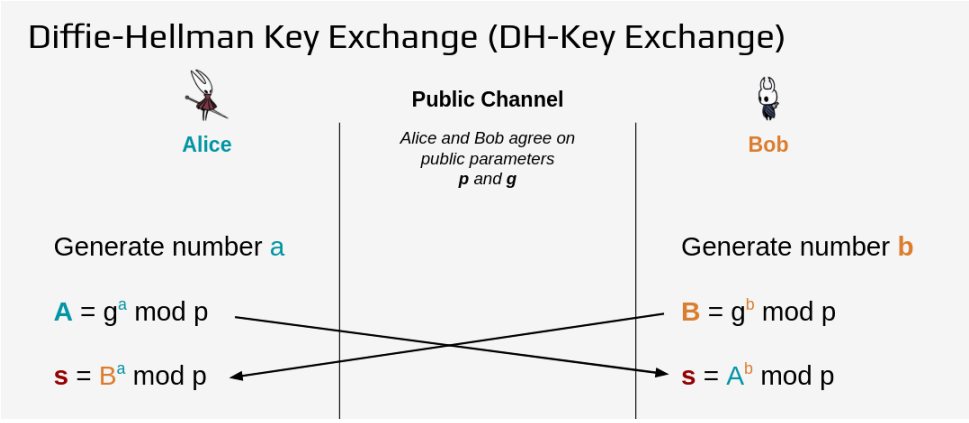


Figure 3: Simple DH.

Lets take our own numbers with:

- p = 23
- g = 5
- Alice takes a = 6
- Bob takes b = 15

Question 8: Compute Alice's and Bob's public value.

Question 9: Compute the shared secret key.

III.2.1 DH MitM

Question 10: Based on the above Diffie-Hellman key exchange, can you image a MitM attack in this setup?

Question 11: What cryptographic property could you add to this basic DH to avoid such attack?