به نام خدا

HW3

Computer network

Dr. Jafari

Sara Azarnoush

98170668

## Contents

1

SDN (Software-Defined Networking) is a network architecture technique that allows networks to be intelligently and centrally controlled, or 'programmed,' using software applications.

Regardless of the underlying network technology, this allows operators to manage the entire network uniformly and holistically.

Reasons:

- Increased control with greater speed and flexibility:

  Instead of manually programming multiple vendor-specific hardware devices, developers can control the flow of traffic over a network simply by programming an open standard software-based controller. Networking administrators also have more flexibility in choosing networking equipment, since they can choose a single protocol to communicate with any number of hardware devices through a central controller.

- Customizable network infrastructure:

  With a software-defined network, administrators can configure network services and allocate virtual resources to change the network infrastructure in real time through one centralized location. This allows network administrators to optimize the flow of data through the network and prioritize applications that require more availability.

- Robust security:

  A software-defined network delivers visibility into the entire network, providing a more holistic view of security threats. With the proliferation of smart devices that connect to the internet, SDN offers clear advantages over traditional networking. Operators can create separate zones for devices that require different levels of security, or immediately quarantine compromised devices so that they cannot infect the rest of the network.

Models:

- Open SDN:

  Network administrators use a protocol like OpenFlow to control the behavior of virtual and physical switches at the data plane level.

- SDN by APIs

  Instead of using an open protocol, application programming interfaces control how data moves through the network on each device.

- SDN Overlay Model:

Another type of software-defined networking runs a virtual network on top of an existing hardware infrastructure, creating dynamic tunnels to different on-premise and remote data centers. The virtual network allocates bandwidth over a variety of channels and assigns devices to each channel, leaving the physical network untouched.

- Hybrid SDN:

  This model combines software-defined networking with traditional networking protocols in one environment to support different functions on a network. Standard networking protocols continue to direct some traffic, while SDN takes on responsibility for other traffic, allowing network administrators to introduce SDN in stages to a legacy environment.

Benefits:

Many of today's services and applications, especially when they involve the cloud, could not function without SDN. SDN allows data to move easily between distributed locations, which is critical for cloud applications.

Additionally, SDN supports moving workloads around a network quickly. For instance, dividing a virtual network into sections, using a technique called network functions virtualization (NFV), allows telecommunications providers to move customer services to less expensive servers or even to the customer's own servers. Service providers can use a virtual network infrastructure to shift workloads from private to public cloud infrastructures as necessary, and to make new customer services available instantly. SDN also makes it easier for any network to flex and scale as network administrators add or remove virtual machines, whether those machines are on-premises or in the cloud.

Finally, because of the speed and flexibility offered by SDN, it is able to support emerging trends and technologies such as edge computing and the Internet of Things, which require transferring data quickly and easily between remote sites.

Resources:

https://www.vmware.com/topics/glossary/content/software-defined-networking.html

https://www.ciena.com/insights/what-is/What-Is-SDN.html

https://en.wikipedia.org/wiki/Software-defined_networking

## 2

### a)

Telegram does support E2E encryption for two types of communications: Secret Chats, and voice calls. Secret Chats are chats that are not stored on Telegram servers, and are only accessible to the devices involved in the chat. Secret Chats should be as secure as MTProto, but users need to remember to turn them on. Voice calls are automatically E2E encrypted, likewise making them as secure as MTProto allows.

The concern about Telegram's E2E encryption is that it is not applied by default. Most chats (Cloud chats) on Telegram are securely encrypted while in transit between your devices and Telegram's servers. Once chat messages arrive at the Telegram servers, they are encrypted using MTProto while at rest on the servers. However, Telegram can read chat data since it handles the encryption/decryption of messages at the servers.

Other secure messaging services such as Signal, apply E2E encryption on all communications by default. The service cannot read those messages. Only the sender and the recipient can read E2E encrypted messages. In other words, any service that uses E2E encryption for all their messages will be more secure than Telegram.

- Secret Chats are end-to-end encrypted
  Massages are client-to-client encrypted
- Secret Chats are device-specific
  Stored on the device not telegram cloud.
- Secret Chats cannot be forwarded
  It synchronized between sender and receiver
- Secret Chats messages can be time bounded
  Can set time and after it finished it disappeared

Resources:

https://medium.com/@pichsenmeister/a-glimpse-into-telegram-s-security-bbf3eaa58aab

https://core.telegram.org/techfaq

https://www.gadgetsnow.com/social/telegram-secret-chat-how-it-is-different-from-regular-chats/articleshow/80280228.cms

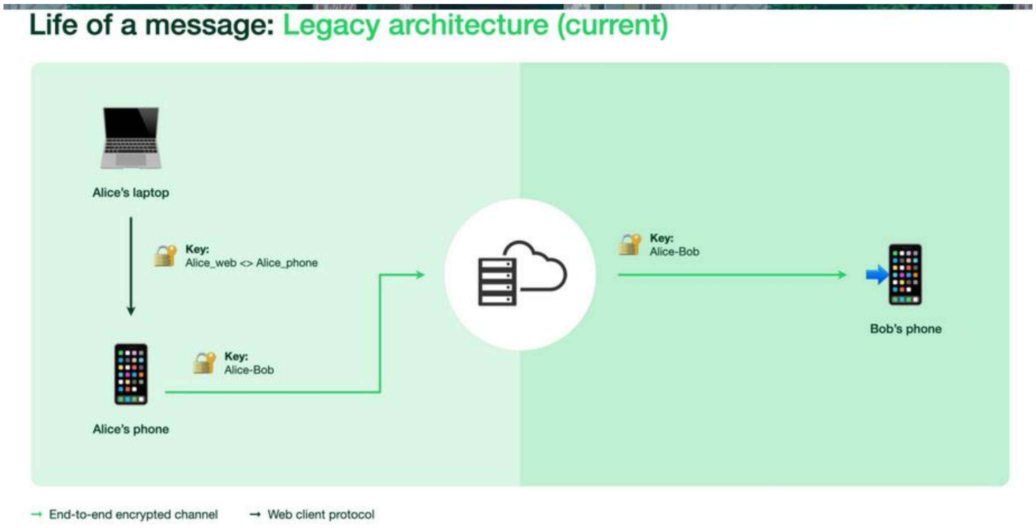
### b)

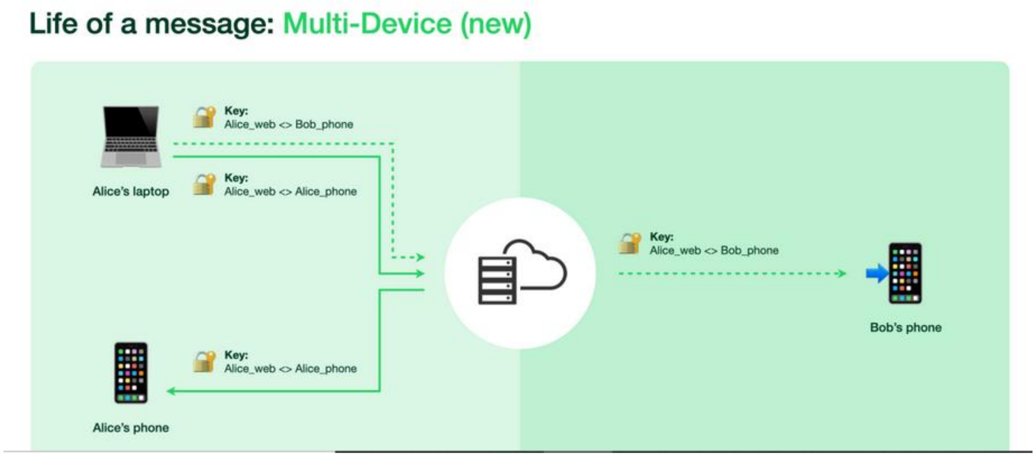
everything in Whatsapp utilizes a server. The amount of overhead that would occur if Whatsapp was P2P would be high. Also there will be very high CPu usage as there would be multiple encrypted connections happening simultaneously, which would mean high battery usage. Thus Whatsapp is not P2P but utilizes a server.

End-to-end encrypted messages are stored on your device and not WhatsApp servers after they are delivered.

immediately after linking a companion device, the primary device end-to-end encrypts a copy of messages from recent chats The primary device will also include a copy of the user's stored public identity key when copying messages for one-to-one chats This process, called Messaging History Syncing, generates bundles of the end-to-end encrypted messages and other data for the chat using the same mechanism of encryption as described in the "Transmitting Media and Other Attachments" section

Telegram only has full secure end-to-end encryption for "Secret chats". This is the only client-client end-to-end encrypted functionallity in Telegram, whereas the rest is client-server/server-client. So group messaging goes over Telegram's cloud infrastructure, where you send once and Telegram forwards to 100 people.





Resources:

https://security.stackexchange.com/questions/231879/is-group-call-for-whatsapp-p2p-or-through-server-like-zoom https://www.whatsapp.com/security/

https://scontent-bru2-1.xx.fbcdn.net/v/t39.8562-6/271639644_1080641699441889_2201546141855802968_n.pdf?_nc_cat=108&ccb=1-7&_nc_sid=ad8a9d&_nc_ohc=tWxo3KVk_uwAX9KXryu&_nc_ht=scontent-bru2-1.xx&oh=00_AT9tb6UGBwBaNUN-bPe2V18i7F7SiBYRs1zclxYPldLkWA&oe=62B7087D

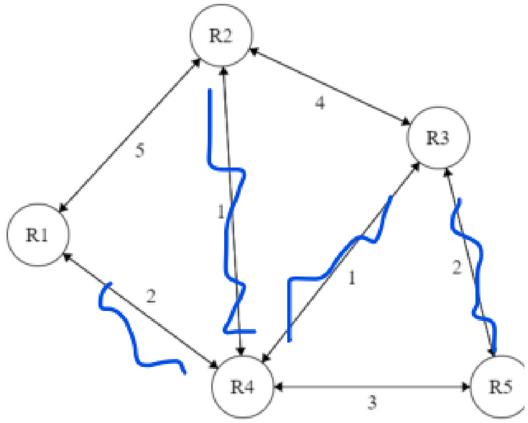
https://engineering.fb.com/2021/07/14/security/whatsapp-multi-device/

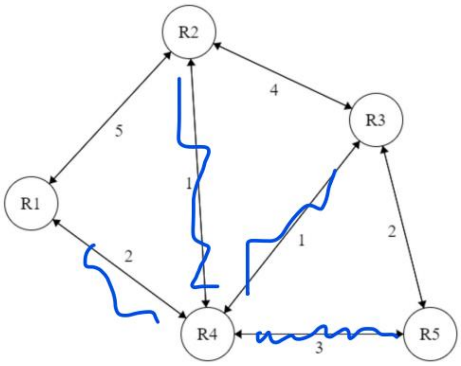
https://www.quora.com/Is-whatsapp-peer-to-peer-like-skype-If-yes-How-am-i-able-to-send-offline-message-to-other-people-If-not-wont-it-be-better-to-make-it-peer-to-peer-since-it-will-remove-server-connection-overhead

3

a)

| step | | R2 | R3 | R4 | R5 |
|---|---|---|---|---|---|
| 1 | R1 | 5 | inf | 2 | inf |
| 2 | R1R4 | 3 | 3 | - | 5 |
| 3 | R1R4R2 | - | 3 | - | 5 |
| 4 | R1R4R2R3 | - | - | - | 5 |
| 5 | R1R4R2R3R5 | - | - | - | - |





b)
R1R4R2R3R5

Step1:

Combine all 5 table in 1 table(only 1 column is ok other are inf)

| | R1 | R2 | R3 | R4 | R5 |
|---|---|---|---|---|---|
| R1 | 0 | 5 | inf | 2 | inf |

| | | | | | |
|---|---|---|---|---|---|
| R2 | 5 | 0 | 4 | 1 | inf |
| R3 | inf | 4 | 0 | 1 | 2 |
| R4 | 2 | 1 | 1 | 0 | 3 |
| R5 | inf | inf | 2 | 3 | 0 |

Choose R4

Step2:

| R1 | R1 | R2 | R3 | R4 | R5 |
|---|---|---|---|---|---|
| R1 | 0 | 3 | 3 | 2 | 5 |
| R2 | 5 | 0 | 4 | 1 | inf |
| R3 | inf | inf | inf | inf | inf |
| R4 | 2 | 1 | 1 | 0 | 3 |
| R5 | inf | inf | inf | inf | inf |

| R2 | R1 | R2 | R3 | R4 | R5 |
|---|---|---|---|---|---|
| R1 | 0 | 5 | inf | 2 | inf |
| R2 | 3 | 0 | 2 | 1 | 4 |
| R3 | inf | 4 | 0 | 1 | 2 |
| R4 | 2 | 1 | 1 | 0 | 3 |
| R5 | inf | inf | inf | inf | inf |

| R3 | R1 | R2 | R3 | R4 | R5 |
|---|---|---|---|---|---|
| R1 | inf | inf | inf | inf | inf |
| R2 | 5 | 0 | 4 | 1 | inf |
| R3 | 3 | 2 | 0 | 1 | 2 |
| R4 | 2 | 1 | 1 | 0 | 3 |
| R5 | inf | inf | 2 | 3 | 0 |

| R4 | R1 | R2 | R3 | R4 | R5 |
|---|---|---|---|---|---|
| R1 | 0 | 5 | inf | 2 | inf |
| R2 | 5 | 0 | 4 | 1 | inf |
| R3 | inf | 4 | 0 | 1 | 2 |
| R4 | 2 | 1 | 1 | 0 | 3 |
| R5 | inf | inf | 2 | 3 | 0 |

| R3 | R1 | R2 | R3 | R4 | R5 |
|---|---|---|---|---|---|
| R1 | inf | inf | inf | inf | inf |
| R2 | inf | inf | inf | inf | inf |
| R3 | inf | 44 | 0 | 1 | 2 |
| R4 | 2 | 1 | 1 | 0 | 3 |
| R5 | 5 | 4 | 2 | 3 | 0 |

Step3:

All the same

| | R1 | R2 | R3 | R4 | R5 |
|---|---|---|---|---|---|
| R1 | 0 | 3 | 3 | 2 | 5 |
| R2 | 3 | 0 | 2 | 1 | 4 |
| R3 | 3 | 2 | 0 | 1 | 2 |
| R4 | 2 | 1 | 1 | 0 | 3 |
| R5 | 5 | 4 | 2 | 3 | 0 |

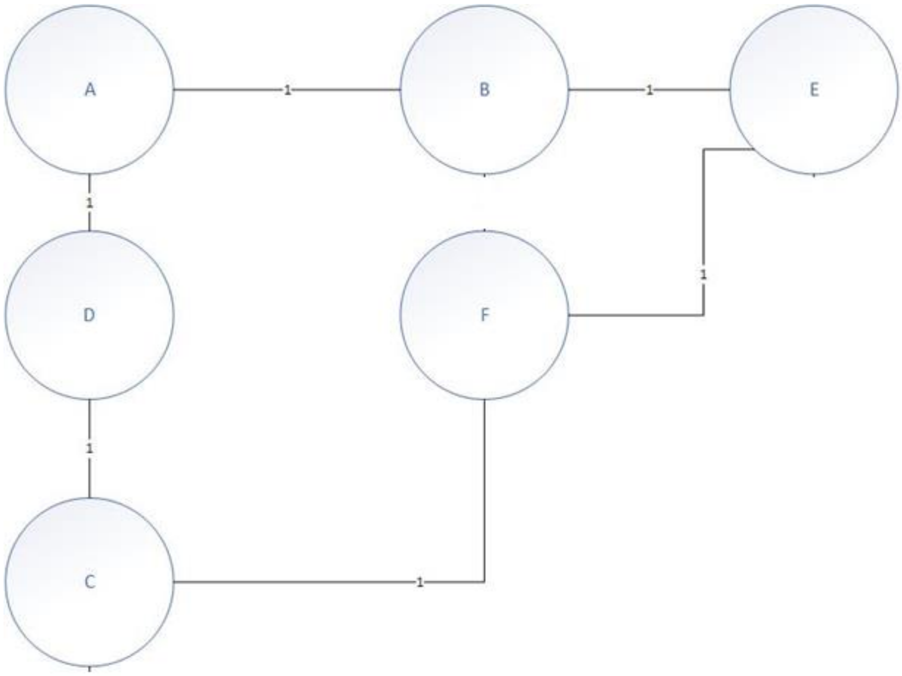
The main issue with Distance Vector Routing (DVR) protocols is Routing Loops since Bellman-Ford Algorithm cannot prevent loops. This routing loop in the DVR network causes the Count to Infinity Problem. Routing loops usually occur when an interface goes down or two routers send updates at the same time.

Poison Reverse is used to tackle the count-to-Infinity problems and one can imagine it as a reverse of the Split Horizon method. With the help of poison reverse, we can advertise the route advertisement which would be suppressed by a split-horizon with a distance of infinity.

In the Autonomous system, every router must have information about all the networks in the autonomous system which is possible if every router manages to get the information of its neighboring routers. Hence each router shares its whole routing table with its neighboring one.

1. We don’t have to wait until time out for breaking a loop
2. Split horizon with poison reverse is way more secure than route poisoning.

4



a)

DCF -> 2

b)

ABEF -> 5

5

Facebook, Instagram, and WhatsApp were down on Monday October 4th due to an interruption in communication between company data centers. The interruption is said to be caused by configuration changes on the routers that coordinate traffic between the data centers. Disruption of network traffic had a cascading effect on the way Facebook's data centers communicate, which brought all services to a halt. Social media quickly burst into flames, reporting what our engineers rapidly confirmed too. Facebook and its affiliated services WhatsApp and Instagram were, in fact, all down. Their DNS names stopped resolving, and their infrastructure IPs were unreachable. It was as if someone had "pulled the cables" from their data centers all at once and disconnected them from the Internet. This wasn't a DNS issue itself, but failing DNS was the first symptom we'd seen of a larger Facebook outage.

According to reports, The Facebook outage was due to a misconfiguration of the border gateway protocol (BGP) that snowballed beyond its control. Somehow, as part of routine maintenance, a command was launched that accidentally disconnected all of Facebook's data centers. Facebook's DNS servers realized its network backbone was no longer communicating with the internet and stopped sending out BGP advertisements. To users, it appeared as if Facebook was sending a message for everyone to take its servers off its "internet maps".

security experts identified the problem as a Border Gateway Protocol (BGP) withdrawal of the IP address prefixes in which Facebook's Domain Name servers were hosted, making it impossible for users to resolve Facebook and related domain names, and reach services. Iran done the same thing and resolve ips.

Resources:

https://www.theguardian.com/technology/2021/oct/05/facebook-outage-what-went-wrong-and-why-did-it-take-so-long-to-fix

https://en.wikipedia.org/wiki/2021_Facebook_outage

https://www.searchenginejournal.com/facebook-outage-2/422000/#close

https://www.facebook.com/business/news/update-about-the-october-4th-outage

https://blog.cloudflare.com/october-2021-facebook-outage/