MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Základy sieťových technológií
Druhý deň

Agenda

- Zopár príkladov na IP kalkulácie
- Transportná vrstva
  - TCP
  - UDP
- Upper layers
  - Session, Presentation a Application
  - Príklad : Ako funguje HTTPS protokol ?
- NAT (Network Address Translation)
  - Prečo to potrebujeme ?
  - Ako to funguje ?
  - Aké sú základné typy NAT ?
- Routing
  - Statický
  - Dynamický
- Základy sieťovej bezpečnosti
  - Ako jednoducho sa dajú zneužiť existujúce protokoly ?
- Networking v Cloudoch
  - Ako fungujú siete a subnety ?
  - Ako funguje routing ?
  - Prečo je dobre pripraviť koncepty tak, aby sa sumarizovali ?

Transport layer

- je zodpovedná za doručovanie dát (údajov) do príslušného aplikačného procesu na hostiteľských počítačoch.
- Dobre známe procesy sú :
    - apache alebo nginx pre webové služby
    - openssh server pre SSH pripojenie
    - RDP server pre pripojenia vzdialenej pracovnej plochy
- Na jednom serveri môžeme mať spustených viacero služieb. Každá služba otvára iný port.
    - Príklady
        - webový server – porty 80(nezabezpečené - http) alebo 443(zabezpečené - https)
        - Mailový server – port 25 (nezabezpečené) alebo 465 (zabezpečené)
- Na transportnej vrstve je veľa dostupných protokolov, ale najdôležitejšie sú len 2 z nich :
    - TCP – Protokol riadenia prenosu
    - UDP – Protokol užívateľského datagramu

Zdrojový & Cieľový Port

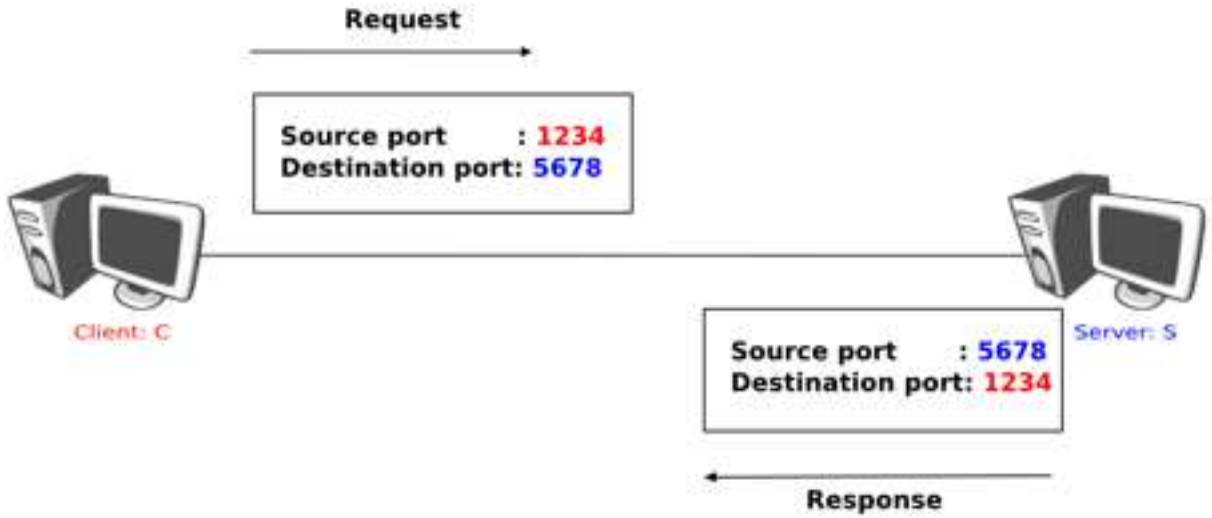
Žiadosť (z počítača na server) :

- Zdrojový port je na zdrojovom počítači definovaný ako náhodné číslo medzi 1 – 65535
    - Toto číslo sa zmení s každým novým pripojením.
    - Zakaždým, keď v prehliadači Google Chrome otvoríte novú kartu, váš počítač na to použije nový zdrojový port.
- Cieľový port je definovaný na cieľovom serveri na základe preddefinovaných hodnôt aplikácie. Tiež to môže byť číslo medzi 1 - 65535
    - Každá aplikácia má svoje vlastné preddefinované porty a protokoly, takže ich ľudia nemusia poznať.
    - Ak otvoríte novú webovú stránku, bude to port 80(ak http) alebo port 443 (ak https) a protokol TCP
    - Existuje zoznam známych portov, ktoré sa používajú pre rovnaký typ aplikácií (web, mail, atď.)
    - Cieľové porty medzi 1-1024 sú zvyčajne definované ako „statické“(definované pre nejaký typ aplikácie) a porty vyššie ako 1024 sú definované ako „vysoké porty“.

Zdrojový & Cieľový Port

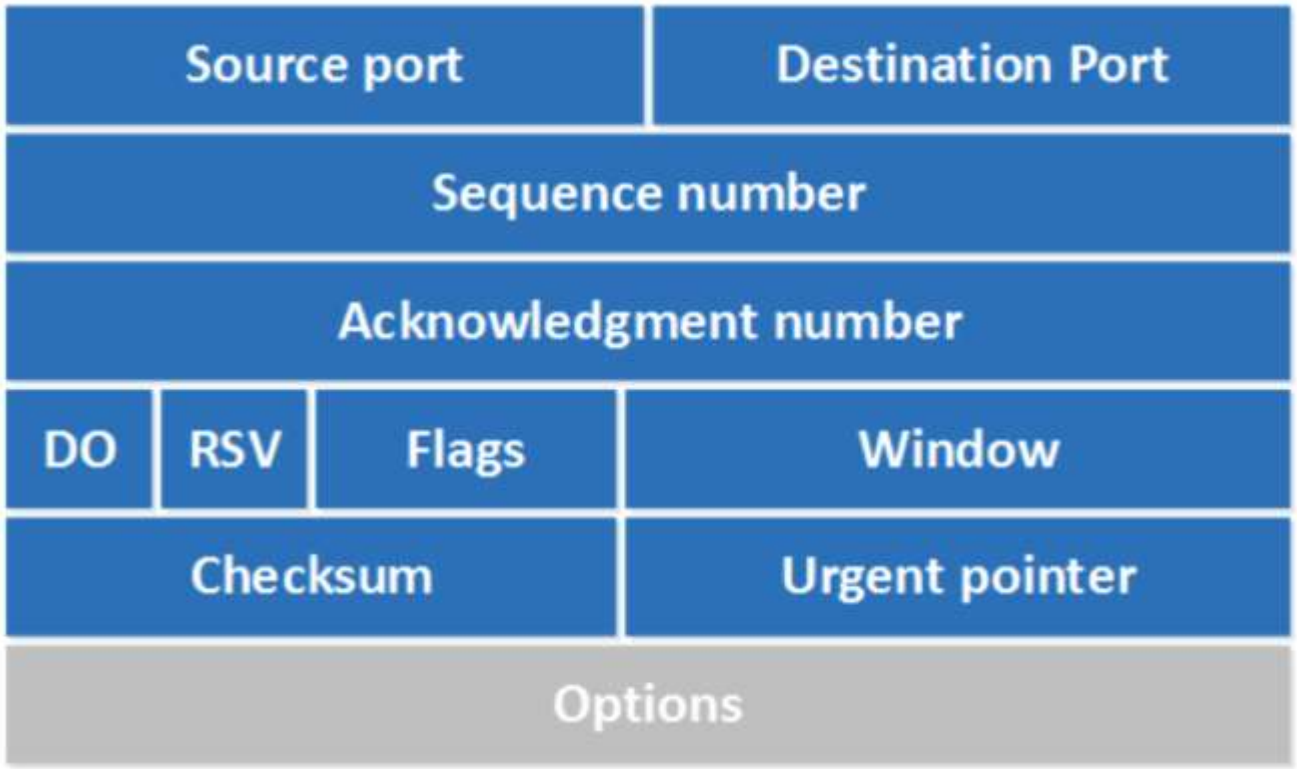
Odpoveď (zo Servera na počítač) :

- Keď webový server odpovie na vašu požiadavku, vymení si porty
  - váš pôvodný zdrojový port sa stane cieľovým portom
  - váš pôvodný cieľový port sa stane zdrojovým portom
  - váš počítač bude presne vedieť, ktorá karta Google Chrome vytvorila túto požiadavku.

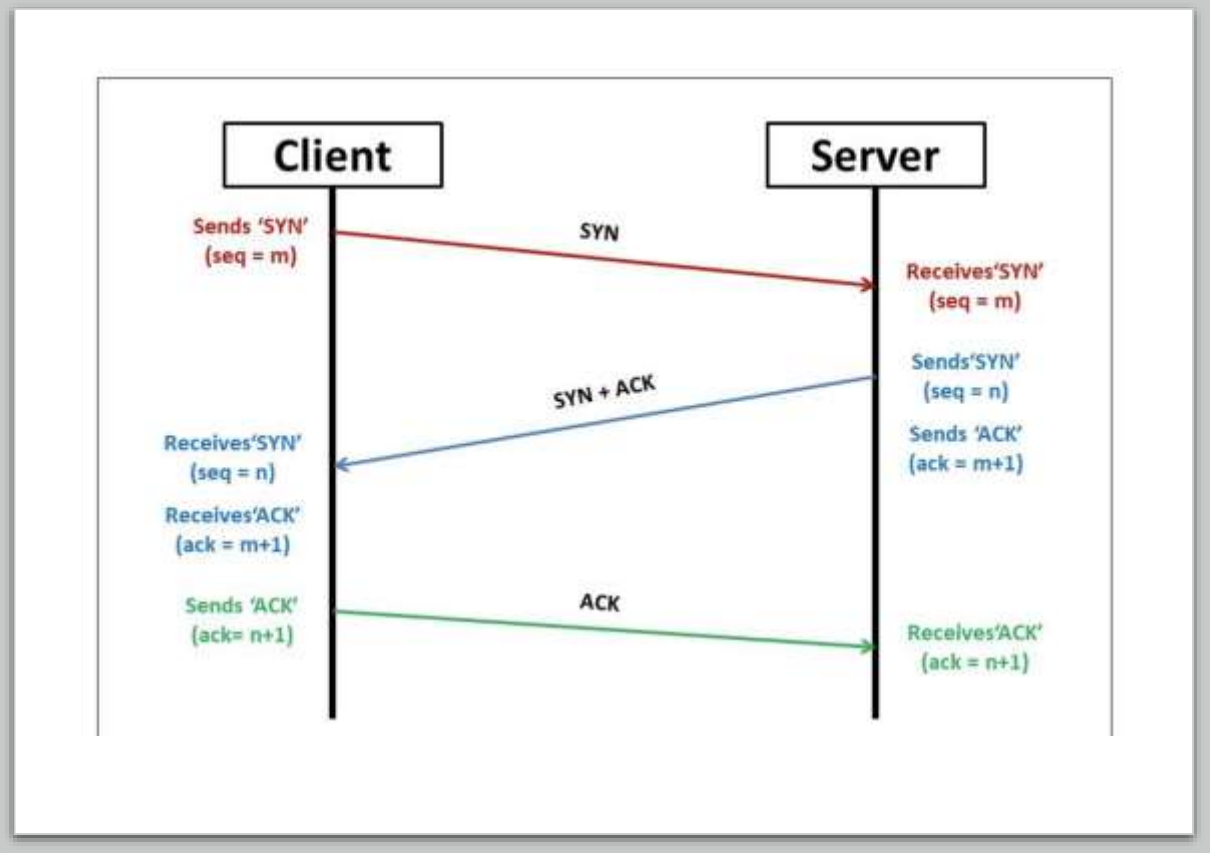


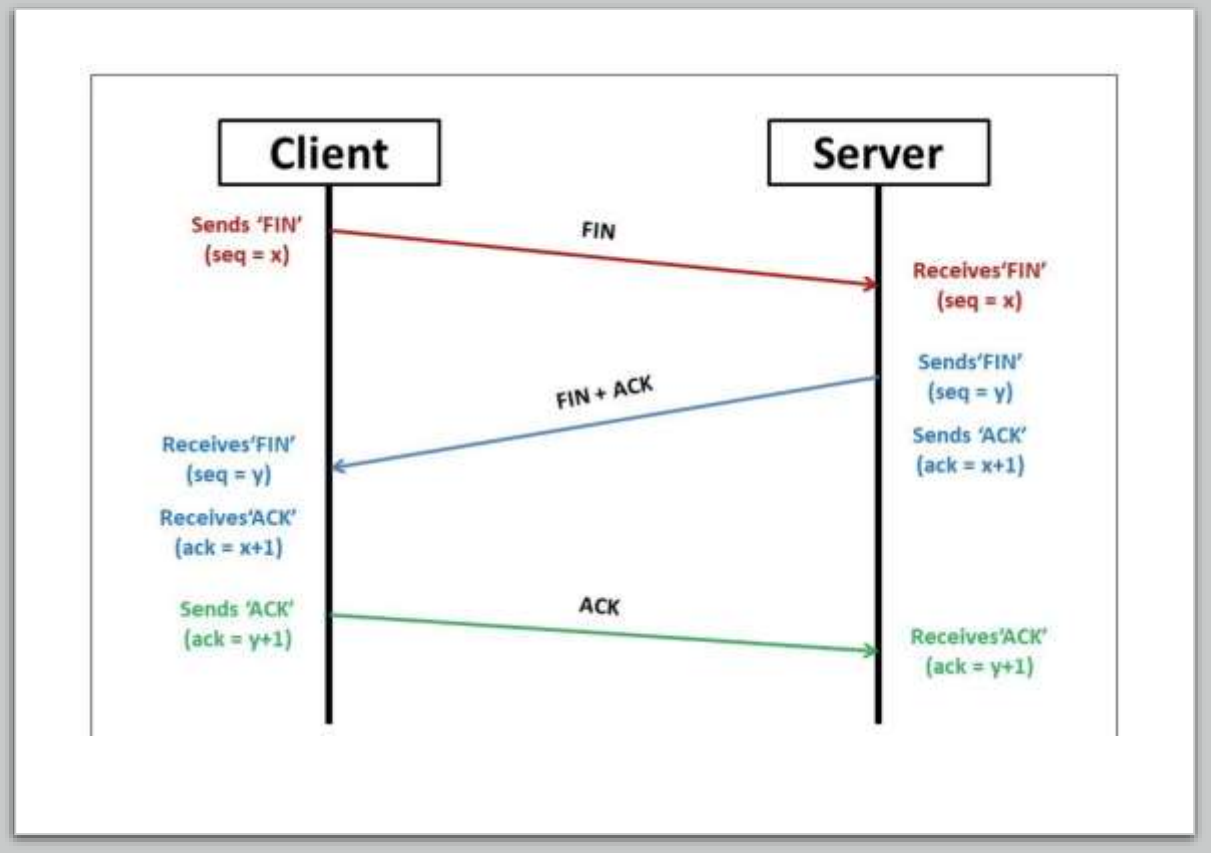
TCP – Transmission Control Protocol

- Je to protokol orientovaný na pripojenie
    - Prioritou je doručiť kompletné dáta zo servera na klienta(napr. webstránka)
- Je to pomalšie kvôli mnohým vstavaným kontrolám
    - Pri začatí komunikácie využíva 3-smerné podanie ruky
    - Používa potvrdzovanie pre každý paket.
    - Po úspešnom doručení údajov použije ukončenie podania ruky (známy ako finálne podanie ruky)
- TCP hlavička obsahuje všetky polia požadované pre všetky tieto kontroly

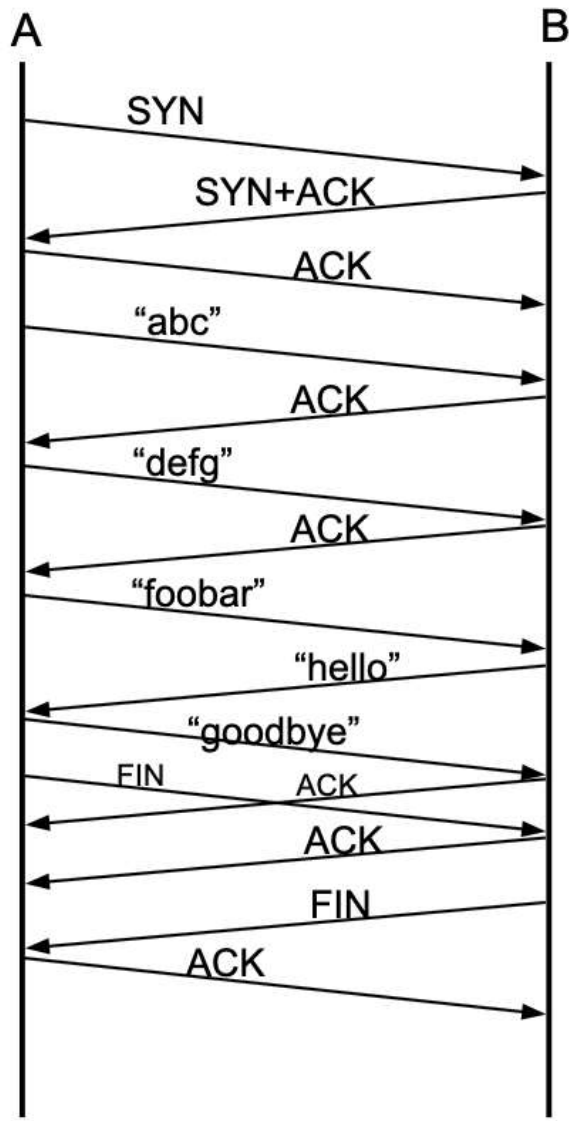


TCP – Handshakes



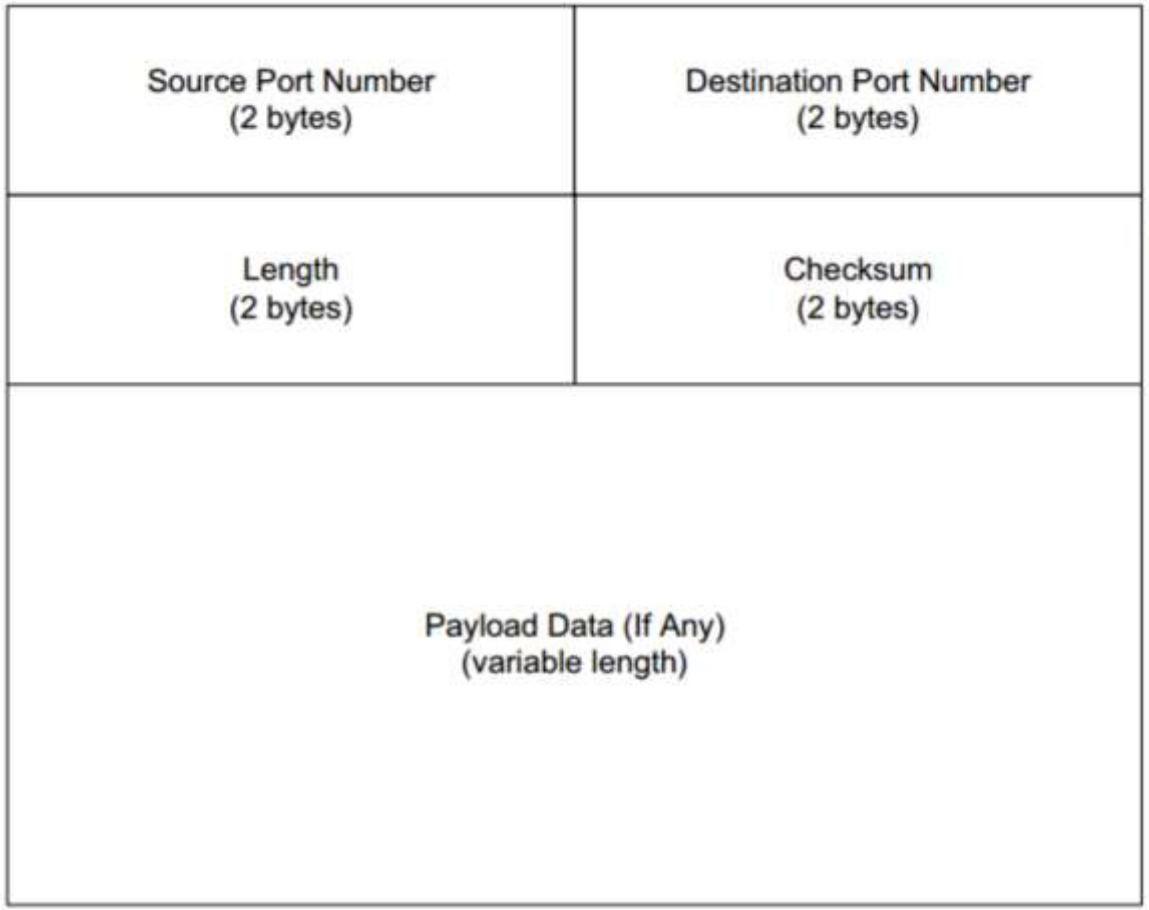


TCP – Data transfer

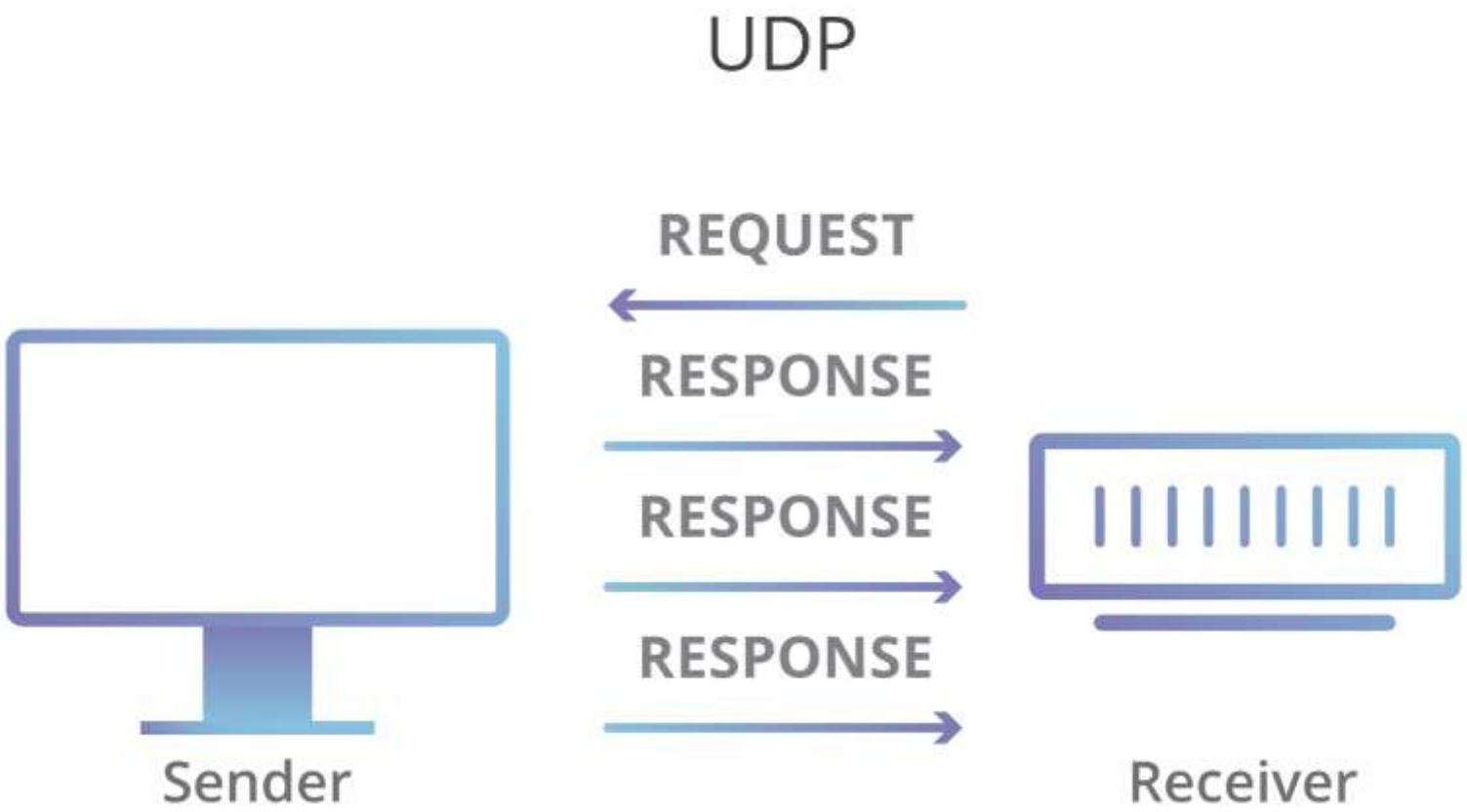


UDP – User Datagram Protocol

- Je to protokol bez spojenia
  - Nie každý paket je prioritou, prioritou je dátový tok
  - Keď telefonujeme – je lepšie stratiť niektoré pakety, ale nechať hovor otvorený, ako prerušiť hovor, keď sa jeden paket niekde stratí
- Je oveľa rýchlejší ako TCP
  - Neexistujú žiadne vstavané kontroly na potvrdzovanie paketov
  - Zdroj môže odosielať údaje v prúde
- Hlavička UDP obsahuje iba polia potrebné na prenos dát



UDP stream




MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY
Upper layers (Application)
Layer 5 – Session Layer
Layer 6 – Presentation Layer
Layer 7 – Application Layer

Upper layers

Funkcie všetkých 3 našich vrchných vrstiev sa vzťahujú na aplikáciu(napr. Google Chrome)

Application vrstva

- Je to GUI (grafické používateľské rozhranie) vašej aplikácie – predná časť
- Príklad: Google Chrome, Outlook alebo akákoľvek iná aplikácia

Presentation vrstva

- Je to pozadie aplikácií. Definuje formát údajov a šifrovanie.
- Príklad: ASCII, UNICODE, JPEG, GIF, TLS, SSL a iné

Session vrstva

- Poskytuje mechanizmus na otváranie, zatváranie a manažovanie relácie medzi aplikáciou koncového používateľa a službou bežiacou na serveri.

DNS – Domain Name System

Čo je DNS a prečo ho potrebujeme?

- DNS je veľká sieť serverov umiestnených po celom svete, ktoré obsahujú distribuovanú databázu názvov domén a IP adries. DNS, často označovaný ako internetový adresár, spája názvy domén s IP adresami. Keď teda do prehliadača zadáte adresu URL stránky, DNS nájde IP adresu, ktorá sa zhoduje s názvom domény. Váš prehliadač potom môže kontaktovať správny server a načítať webovú stránku a jej obsah.

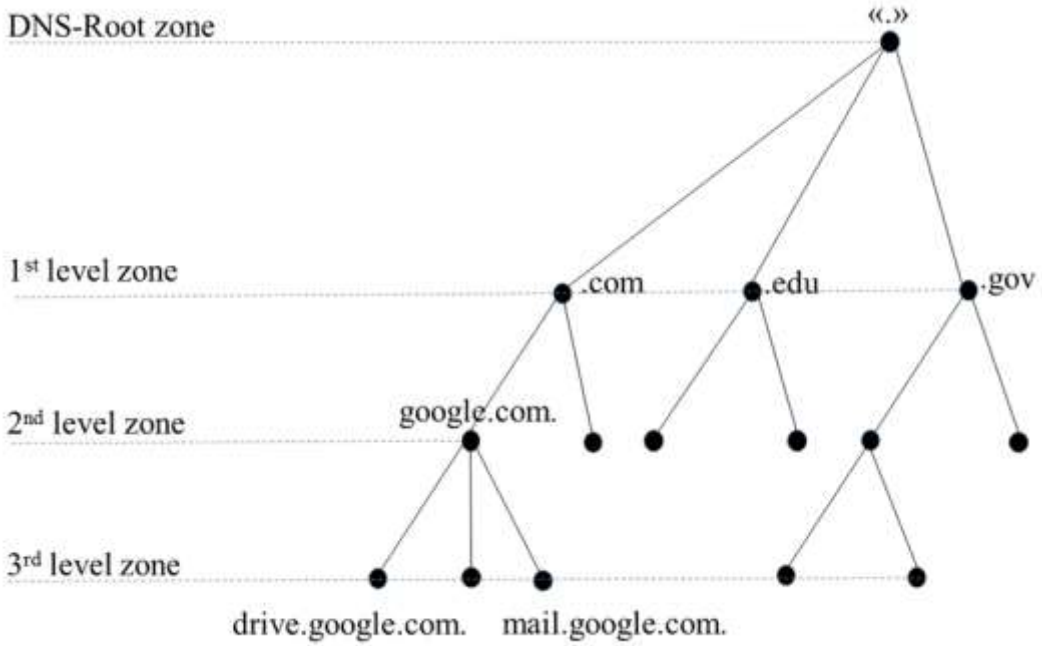
- Potrebujeme to, pretože si nemôžeme zapamätať všetky IP adresy (ktoré sa dynamicky menia) pre každý server, ktorý by sme chceli dosiahnuť.
- DNS umožňuje load balancing medzi servermi na rovnaký účel (facebook, google, atď.). Bez DNS bude mimoriadne ťažké poskytovať celosvetové služby.

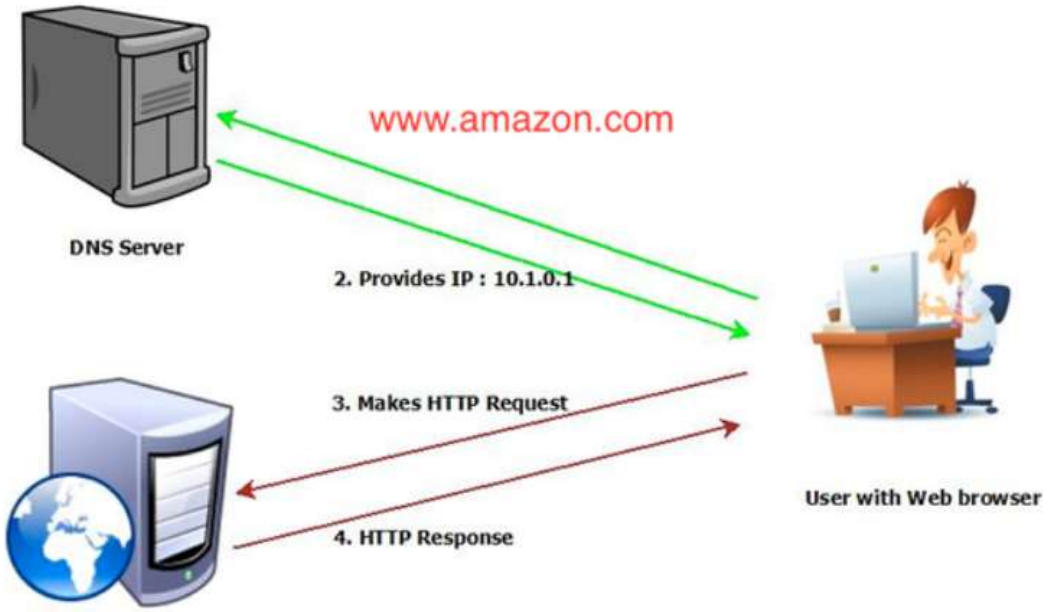
Ako funguje DNS ?

- Na vašom PC vždy získate konfiguráciu DNS servera ako súčasť DHCP
  - Ľudia nevedia, ako funguje vytváranie sietí, preto je to automatické.
  - IP servera DNS je väčšinou váš router, ale iba posiela vaše požiadavky DNS smerom k ISP alebo koreňovým serverom DNS.
  - Najznámejšie DNS servery sú : 8.8.8.8 (google) a 1.1.1.1 (Cloudflare)
- Keď sa chcete dostať na stránku www.facebook.com, váš počítač tomu nerozumie. Môže pristupovať iba k cieľovým IP adresám – nie k reťazcom.
  - Počítač odošle požiadavku DNS na váš server DNS
    - Jednoduchý dopyt, kde je len webová stránka, na ktorú by ste sa chceli dostať.
    - Používa UDP (rýchly) protokol s portom 53 (UDP_53), pretože potrebujeme rýchlu odozvu.
    - Ide o čistú textovú komunikáciu, takže ak niekto sedí v jej strede – vidí, aké webové stránky si prezeráte!
  - Server odošle odpoveď s IP adresou
  - Môžete to simulovať pomocou CLI : nslookup www.facebook.com
    - Skontrolujte to viackrát, uvidíte, že IP sa niekoľkokrát zmení.
- Potom bude nasledovať už známu cestu pomocou smerovania IP adresy smerom k internetu.
- Youtube video (2:24) vysvetlenie je tu : https://youtu.be/Ersp-jvfWpc

DNS in pictures

- Existuje len niekoľko koreňových serverov DNS
- Na celom svete však existujú stovky serverov DNS zóny 1 úrovne. Len aby sa zabezpečilo, že DNS bude dostupné pre každého.
- Sú synchronizované a majú svoju lokálnu vyrovnávaciu pamäť, do ktorej na nejaký čas ukladajú odpovede DNS (predvolené 24 hodín)





NAT – Network Address Translation

Prečo nemáme na všetkých zariadeniach verejnú IP ?

- **Bezpečnostné dôvody:** ak všetky PC, notebooky, mobilné telefóny a ďalšie zariadenia (TV, Xbox, PS, IoT zariadenia) budú mať verejnú IP adresu (bez akejkoľvek ochrany) – budeme sa môcť priamo pripojiť z jedného zariadenia k druhému. To nechceme – ľudia nevedia, ako nastaviť svoje zariadenia.

- **Počet IP adries:** Štandard IPv4 bol vytvorený v roku 1981 s viac ako 4,3 miliardami dostupných adries IPv4. Koncom 80. rokov to už nestačilo. Len si predstavte všetky počítače a zariadenia IoT, ktoré sa dnes pripájajú na internet. Teraz si predstavte všetky internetové služby a ich komplexnosť. (nslookup www.facebook.com) Jednoducho nemáme dostatok IPv4 adries pre každého.

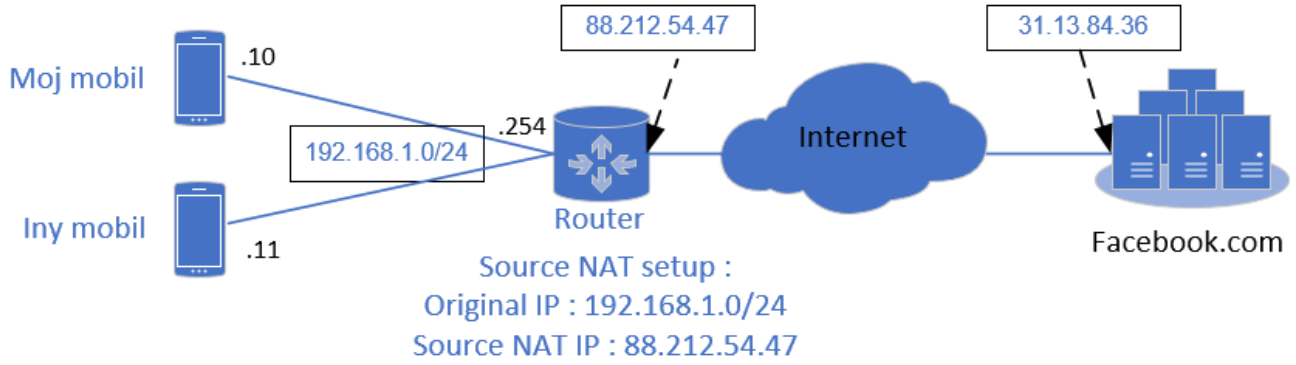
Private IP addresses

- **Privátne IP adresy:** v roku 1996 bolo riešenie publikované ako štandard. V rámci tohto dokumentu boli 3 nezávislé prefixy IPv4 vyhradené len na súkromné použitie. Tie nie sú smerované do vnútra internetu – takže jednoducho, ak máte iba tieto IP adresy – ste nedosiahnuteľní z vonkajšieho sveta.
  - 10.0.0.0/8
  - 192.168.0.0/16
  - 172.16.0.0/12
- Môžu byť použité pre jedného nájomníka (zákazníka), takže väčšina z vás má rovnaké IP adresy vo svojich domácich sieťach (napr. 192.168.1.0/24)
- Otázkou však je – ak máme všetci na svojich zariadeniach len súkromné adresy IP, ako je možné, že sa všetci dostaneme k internetovým službám (napr. facebook) ?

NAT ako riešenie

- Ako to funguje ?
  - Všetci používatelia, ktorí nepotrebujú verejné IP adresy (väčšinou domáci používatelia), budú predvolene dostávať iba súkromné IP adresy.
  - ISPs (Internet Service Providers – Poskytovatelia internetových služieb ako napr. Telekom, Antik, atď.) budú mať svoje vlastné verejné IP adresy. (Sú veľmi drahé – a ich cena stúpa!)
  - Poskytovatelia internetových služieb sú zodpovední za svoju verejnú IP podsieť, ich zákazníci sú zodpovední za svoju súkromnú IP podsieť.
  - Domáce routre sú vopred nakonfigurované tak, aby vykonávali jeden typ NAT – existuje však viac typov.
  - Váš domáci router jednoducho skryje vaše súkromné rozsahy IP doma pre jednu jedinú adresu IP.
    - Na to použije tabuľku NAT, kde je možné spätne sledovať každé spojenie.
    - Každé pripojenie má svoju životnosť, preto by sa tabuľka mala obnoviť, keď sa odpojíte od internetovej služby (napr. facebook, keď zatvoríte kartu na počítači – pripojenie je ukončené)
- Koľko relácií vieme skryť za jednu verejnú IP ?
  - Približne 65 000, závisí to od výrobcu zariadenia a jeho konfigurácie

Hide NAT(Network Address Translation)



Hide NAT (Port Address Translation) table on router							
Original packet				Translated packet			
Source IP address	Source port	Destination IP	Destination port	Source IP address	Source port (1-65535)	Destination IP	Destination port
192.168.1.10	11653	31.13.84.36	443	88.212.54.47	1	31.13.84.36	443
192.168.1.11	22423	31.13.84.36	443	88.212.54.47	2	31.13.84.36	443

- Čo sa stane, keď komunikácia príde z internetu na našu verejnú IP a cieľový port, ktorý nie je v tabuľke? – upustí sa.
- Z tohto dôvodu väčšina škodlivého softvéru iba otvára relácie na internete.

NAT (Network Address Translation)

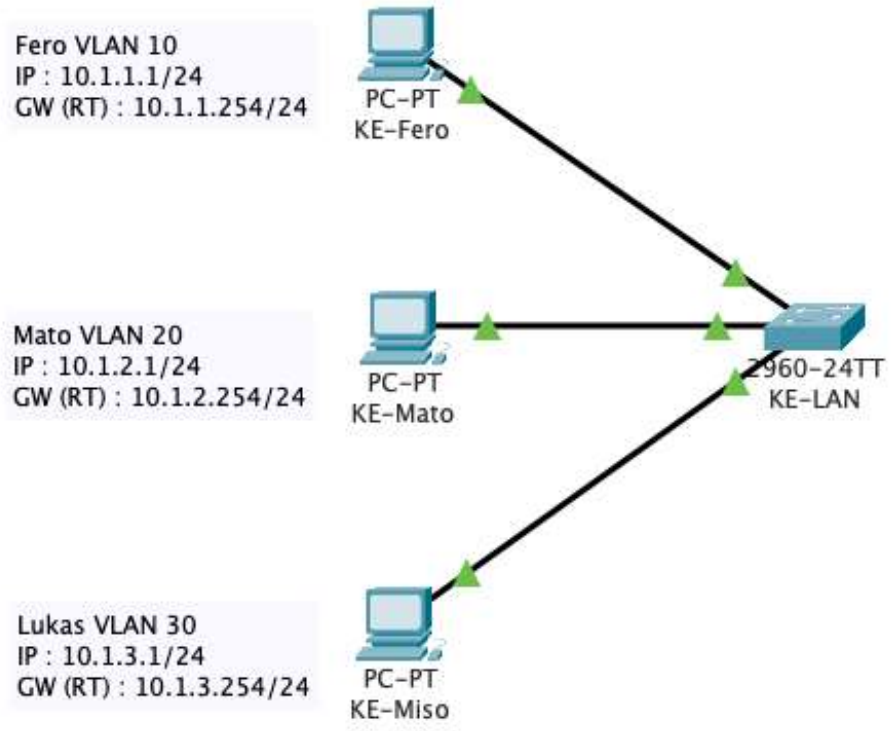
- Hide NAT – PAT (f.e. Antik internet)
  - Jeden zákazník alebo skupina zákazníkov je skrytá za jednu verejnú IP adresu
  - Pretože tento koncept sa môže použiť viac krát za sebou, môžeme mať jednu domácnosť, ktorú skrývame za jednu privátnu IP a potom všetky tieto privátne IP skrývame ďalej za jednu (alebo viac) verejných IP.
- Dynamic public NAT (for free with Telekom VDSL)
  - Je pod-typom Hide NAT, kde ale na interface vášho domáceho routra dostanete buď priamo verejnú IP, alebo privátnu IP, ktorá bude NAT-ovaná spôsobom 1:1 za nejakú verejnú.
  - Táto IP sa môže zmeniť každým reštartom routra.
- Static public NAT – 1:1 NAT (extra paid service)
  - Toto sa používa ak si kúpite verejnú IP od ISP (Internet Service Providera)
  - Potrebujete mať ale zariadenie, ktoré podporuje konkrétne nastavenia ktoré je aj potrebné vykonať.


MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Routing

VLAN & Subnet separation

- Why is separation important
  - Security – we don't want to have everyone in the same VLAN
    - Broadcast (f.e. ARP) messages are flying around and all PCs mu at least read them
      - CPU overhead (PCs are listening)
      - Network overhead
    - Within one VLAN there are many ways to attack one PC to another
      - On our last lesson I would like to show you some examples
- Therefore, we have
  - home segmentation :
    - Each flat in a block has their own VLAN
  - company / school segmentation
    - Each group of people will have their own VLAN – examples :
      - Students
      - Teachers
      - Head office
      - Administrator (Engineering)
- But question is – if we will do the separation and everyone will have his own VLAN, how can we connect from one VLAN to another ?



Router on a Stick

How do we interconnect VLANs ?

- The only way how to inter-connect VLANs is using device on L3 or higher layer.
  - Router
  - Firewall
- Easiest way to configure interfaces on router is just to connect physical interface per-VLAN. But because routers mostly don't have too much interfaces – we have to think about it

What is router on a stick ?

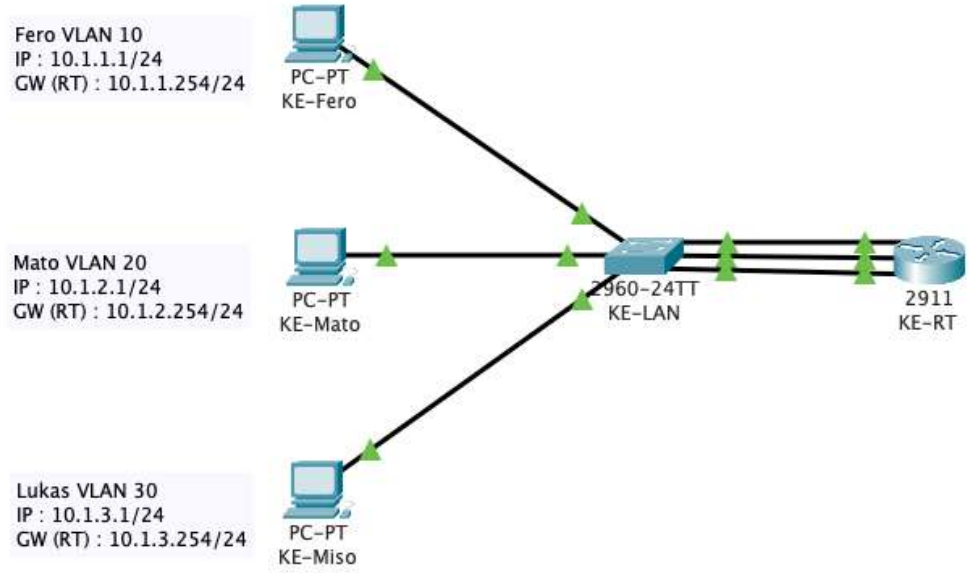
- This name is used when router is connected to a switch with only one physical connection, configured as trunk with multiple allowed VLANs

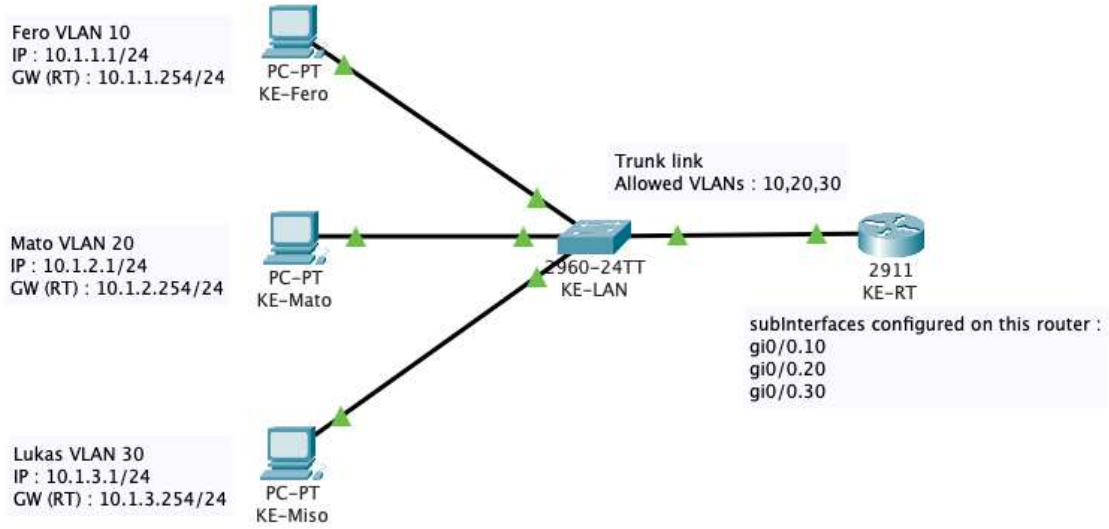
How does it work ?

- On router we will configure subinterfaces as an edge of some VLAN
- It is a logical interface with
  - Interface name
  - IP address from that VLAN
  - VLAN ID

In both cases we are calling those networks (VLANs) directly connected to this router.

- Router on a stick configuration is more used and configuration from router perspective is very similar



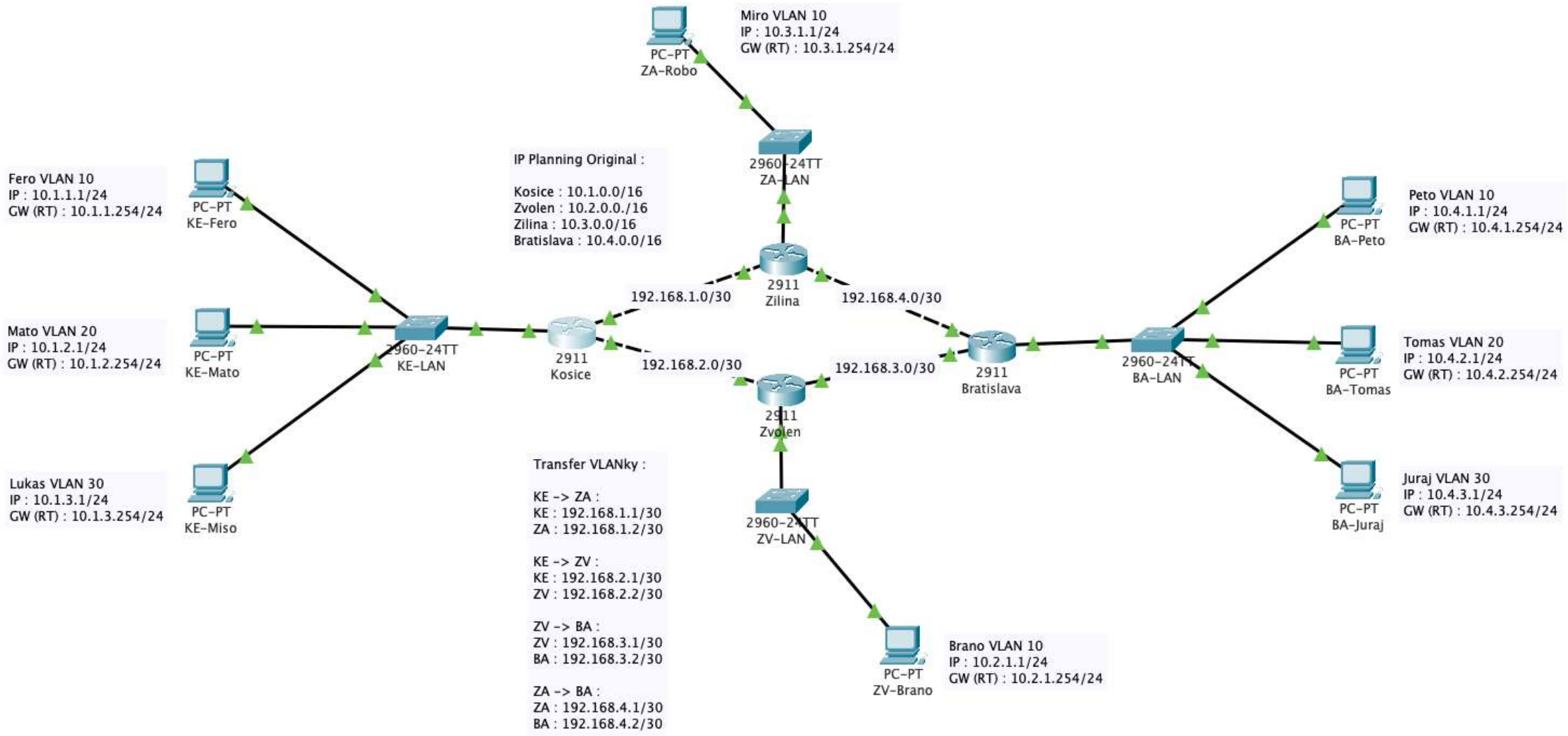


Router & Switch configuration for VLAN separation

```
# Switch configuration

! Now let's create VLANs
vlan 10
name Fero
vlan 20
name Mato
vlan 30
name Lukas

! Now let's configure access interfaces
interface FastEthernet0/1
description VLAN10-Fero
switchport mode access
switchport access vlan 10

interface FastEthernet0/2
description VLAN20-Mato
switchport mode access
switchport access vlan 20

interface FastEthernet0/3
description VLAN30-Lukas
switchport mode access
switchport access vlan 30

! Now let's configure trunk interface towards router
interface GigabitEthernet0/1
description Kosice_gi0/0
switchport mode trunk
switchport trunk allowed vlan 10,20,30

! And finally just save the configuration
end
write
```

```
# Router configuration

! Second let's just enable physical interface
! by default all interfaces on a router are shutdown
interface gigabitEthernet 0/0
no shutdown

! Last let's configure VLAN SubInterfaces
interface gigabitEthernet 0/0.10
encapsulation dot1Q 10
ip address 10.1.1.254 255.255.255.0
description VLAN10-Fero

interface gigabitEthernet 0/0.20
encapsulation dot1Q 20
ip address 10.1.2.254 255.255.255.0
description VLAN20-Mato

interface gigabitEthernet 0/0.30
encapsulation dot1Q 30
ip address 10.1.3.254 255.255.255.0
description VLAN30-Lukas

! Exit config mode and save configuration
end
write
```

Static routing



Static routing

What with all those networks that are not just directly connected to our router ?

- By default, router don’t know where to send traffic.
- If he don’t know – he will drop the traffic as you can see on our example here.
- How to configure static route :

ip route 10.4.0.0 255.255.0.0 192.168.2.2

What is default route ?

- All traffic that doesn’t match other routes will be send to a given destination.
- How to configure default route :

ip route 0.0.0.0 0.0.0.0 192.168.2.2

```
Kosice#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C       10.1.1.0/24 is directly connected, GigabitEthernet0/0.10
L       10.1.1.254/32 is directly connected, GigabitEthernet0/0.10
C       10.1.2.0/24 is directly connected, GigabitEthernet0/0.20
L       10.1.2.254/32 is directly connected, GigabitEthernet0/0.20
C       10.1.3.0/24 is directly connected, GigabitEthernet0/0.30
L       10.1.3.254/32 is directly connected, GigabitEthernet0/0.30
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/30 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/30 is directly connected, GigabitEthernet0/2
L       192.168.2.1/32 is directly connected, GigabitEthernet0/2

Kosice#
Kosice#show ip route 10.4.1.1
% Subnet not in table
```

Dynamic routing

What is good about static routes ?

- Administrator is the only responsible person who can make changes in his network.

What is bad about static routes ?

- Response time – if link between two routers goes down, administrator will be informed, and he will have to correct it.
- Because of this, we are using static routes only in very small networks.
- If we have redundant links – we can't wait for administrator to correct it. What if he will be on vacation ? Half of Slovakia won't have Internet connection until he will be back ?

What is dynamic routing ?

- Set of functions on a router that allow communication between routers. They will tell each other which directly connected networks they have, and this information is propagated between them.
- There are many different protocols (f.e. OSPF, BGP, EIGRP, e.t.c.) that will provide you this function in a different way. But all of them are dynamic and all of them support convergence in case of failure in a network.
- If link between Kosice and Zvolen will go down for any reason, dynamic routing will detect and change routing to Zvolen subnet via Zilina and Bratislava.

Routing decision in detail

Which route type has the highest priority on a router ?

- The **most specific route** for a given IP subnet always wins against larger network
  - If we have two routes for 10.1.1.1 in this two subnets :
    - 10.0.0.0/8 via path A
    - 10.1.1.0/24 via path B = this will win, because it is more specific

- If there are 2 routes for the same network, each route has 2 values that are used for this decision :
  - **Administrative distance (AD)** – lower is better
  - **Metric** – lower is better, but it is only checked when two routes have the same AD
    - This value can be setup with static routes, or can be calculated with dynamic routing protocols

- **Administrative distance** is **different** for each **type of route** :
  - **Directly connected** (f.e. : Router on a Stick) – value is 0
    - There can be just one directly connected network with a given IP range !
  - **Static route** – value is 1
  - **Dynamic route** – different per routing protocol (example : OSPF value is 110)

Routing decision simple

How router is doing decision based on priority :

1. Which is the **most specific route** for given IP ?
    1. If there is just one route for this most specific subnet – it will be routed based on this entry (no other checks are needed!)

2. **If I have 2 identical** ranges routed via different input (directly connected, static route, dynamic route) :
    1. What is the **Administrative distance** of this route input ?
        1. **Lowest** always wins !

    2. **If I have 2 identical ranges** routed via the same input (static route, dynamic route)
        1. What is the **Metric number** ?
            1. **Lowest** always wins !

Network Security

Network Security Basics

What CIA means in the world of Network Security ?

- **Confidentiality**
  - assurance that the information is accessible only to those authorized to have access
- (Data) **Integrity**
  - the trustworthiness of data or resources in terms of preventing improper and unauthorized change
- **Availability**
  - assurance that the system responsible for delivering, storing, and processing information are accessible when required by the authorized person

Network Security Vocabulary

Just few of them, but there are many more :

Vulnerability
- Existence of weakness, design, or implementation error that can lead to an unexpected event compromising the security of the system

Exploit
- a breach of IT system security through vulnerabilities

Acceptable risk
- Vendor/s will accept, that risk of exploiting this vulnerability is not so high, or it will significantly lower down usability of feature. Therefore, it will be accepted as possible risk without fix.

Zero-Day Vulnerability / Attack
- an attack or vulnerability that affects application before the software developer releases a patch for it

Phishing
- claiming to be from a legitimate site in an attempts to acquire a user's personal or account information

Man-In-The-Middle Attack
- Attack type, when attacker sits between victim and his destination server to see the traffic

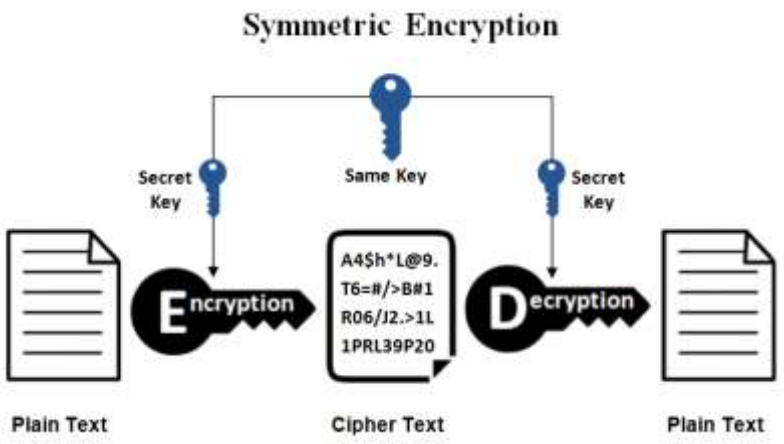
Symmetrical vs Asymmetrical encryption

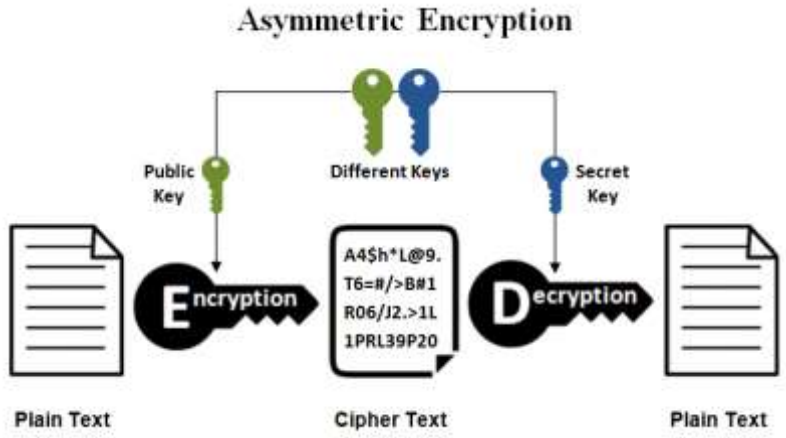
Symmetrical encryption

- Symmetric encryption uses a single key
- Friendly to CPU usage
- Not so secure – you need to exchange the key & used algorithm.

Asymmetrical encryption

- Uses pair of keys
  - Private – we will never share this!
  - Public – we will share with others
- Mathematical logic is applied – you cannot calculate private from public and other way around.
- If data are encrypted with one key – they can be decrypted only with the second key.

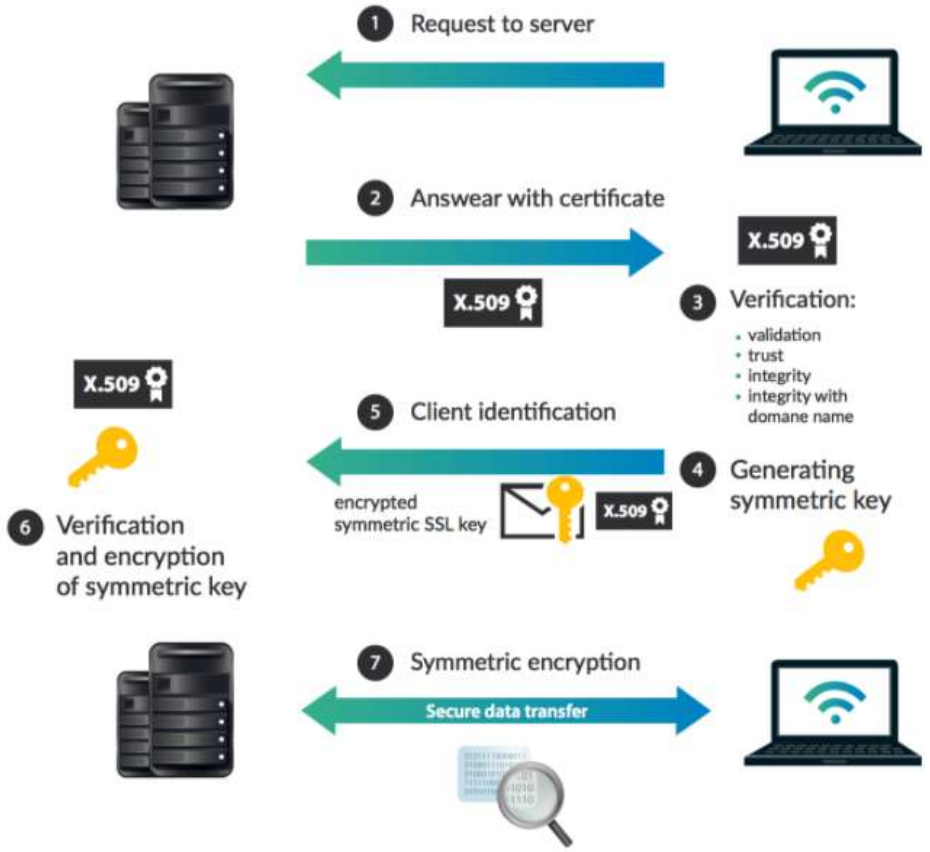




How HTTPs works ?

- It is using classic HTTP method, but in encrypted way.
  - 2 protocols that are mostly used : SSL or TLS
- For encryption – it is using combination of symmetric & asymmetric encryption
  - Asymmetric – to exchange key and used algorithms
  - Symmetric – for all further communication

- Important part is Verification of server's certificate
  - How can I trust this server ?
    - It was signed by Certification Authority, that I trusted.
    - If we will translate it in human language – we can check ID card or passport, because we trust the organization that issued it.

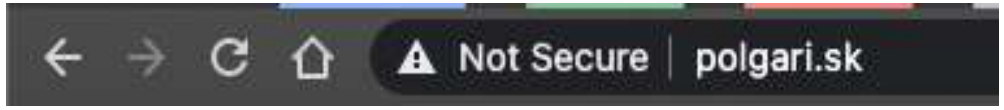


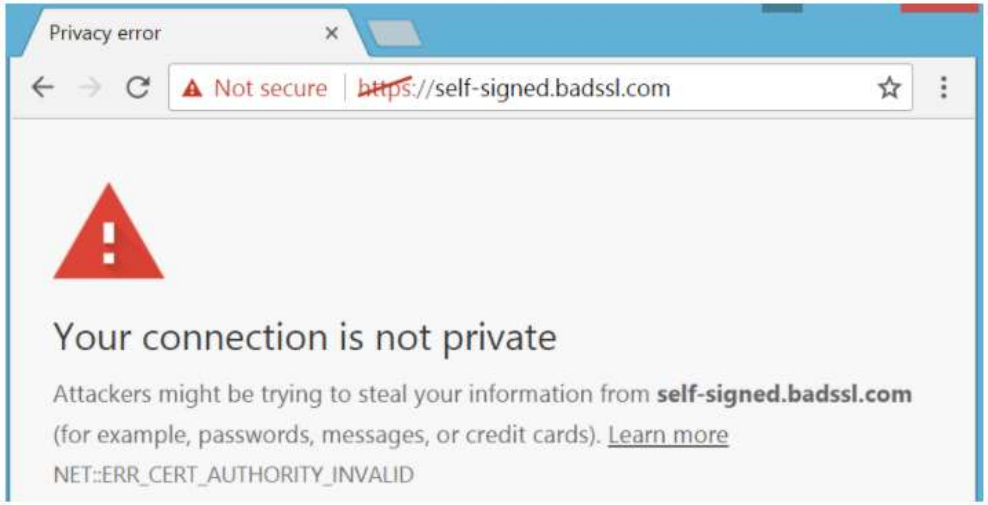
How to check if page is valid ?

Before entering any information on any web page, always check this :

- Is this the domain I should be on ?
  - If web page is asking you to enter some data or login information – always check if the page is really the one you are looking for.
    - Example : am I on facebook or facbook ?

- Does it have a valid certificate ?
  - Do not enter any information to HTTP page – always use HTTPS instead. If page doesn't have HTTPS version, don't use it.
  - If you are on page using HTTPS - browser will show warning message if certificate is invalid.
    - In this case – do not enter this page !



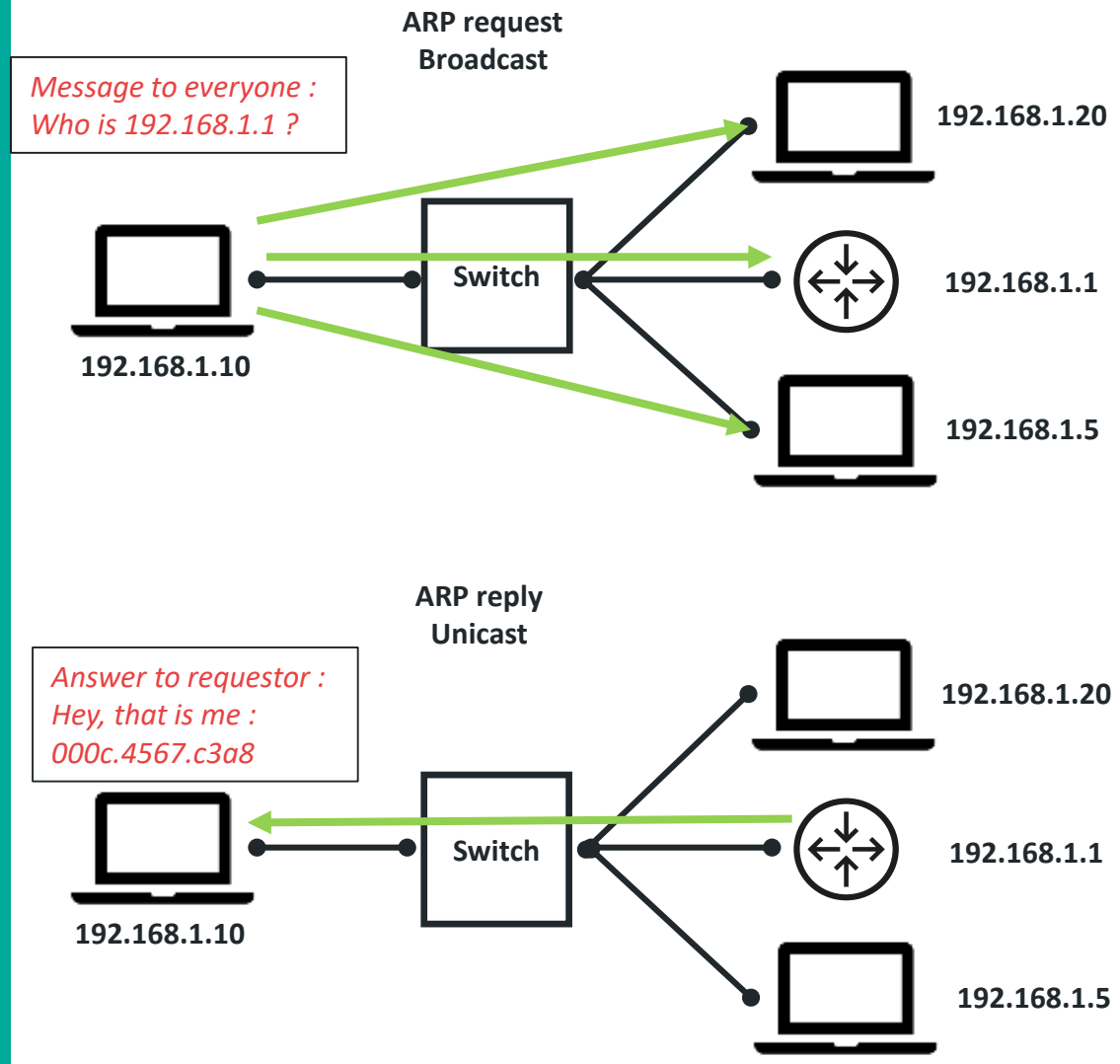


How ARP works ?

It is a very simple protocol that uses cleartext traffic within one network to translate IP address into MAC address.

It consist of 2 messages :

- ARP request :
  - Broadcast message to everyone in the same network with a question
  - This is a frequent question based on endpoint setup
- ARP reply :
  - Unicast message from the destination back to the source.
  - If ARP reply is sent by destination without request – it is called gratuitous ARP
    - This one is used in case new device is introduced with the same IP – f.e. : you have network with 3 available IP addresses, and you will disconnect one laptop from it and connect a new one. It will ”introduce itself” to his default gateway.



Man-In-The-Middle Attacks

A man-in-the-middle (MitM) attack is when an attacker intercepts communications between two parties either to secretly eavesdrop or modify traffic traveling between the two. Attackers might use MitM attacks to steal login credentials or personal information, spy on the victim, or sabotage communications or corrupt data.

- It is an attack category and there are many types of MitM attacks.
  - you can achieve this using different protocols and vulnerabilities – or using physical interception of a wire between victim PC and router

What is ARP poisoning ?

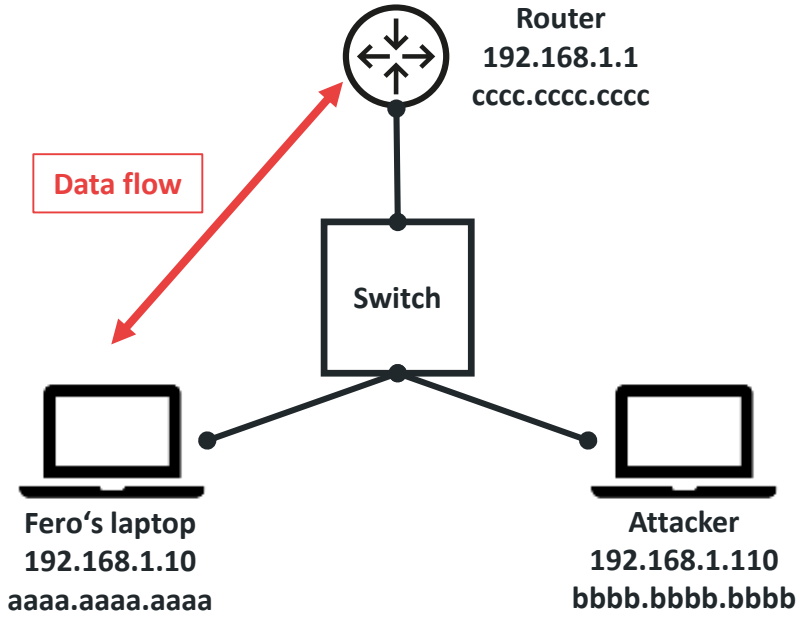
This is a MitM attack type, using ARP protocol.

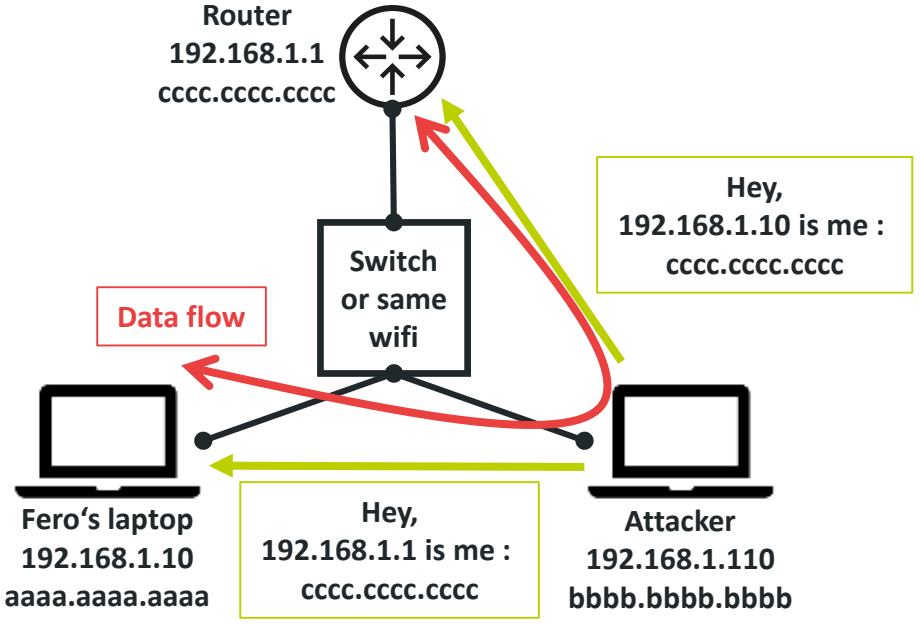
ARP works in the same way in your local network and in public wireless network (f.e. school, bus station, hotel, e.t.c.)

How ARP poisoning attack work ?

- It is using (**gratuitous)** ARP reply message from attacker PC – so normal "trust traffic".
- It is a MITM attack type, where attacker will lie to you and default GW of the network that he is the right MAC address behind the IP
- All the traffic will afterwards go from your PC to destination (f.e. facebook) without you realizing it.
- All cleartext traffic can be simply shown on attacker PC.
- This is the simple reason why to follow security recommendations on slide 7

It is highly recommended not to login to any page on public wireless network if it is not necessary.





ARP poisoning demo

Before attack :

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : fc00:10:200:2::f:1
   Link-local IPv6 Address . . . . . : fe80::a590:ff5a:b832:3691%11
   IPv4 Address. . . . . . . . . . . : 10.200.2.110
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::a5b:eff:fefd:bcbc%11
                                       10.200.2.1

C:\Users\ahyben>arp -a

Interface: 10.200.2.110 --- 0xb
  Internet Address      Physical Address      Type
  10.200.2.1            08-5b-0e-fd-bc-bc     dynamic
  10.200.2.255          ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

C:\Users\ahyben>
```

ARP cache before & after attack :

```
C:\Users\ahyben>arp -a

Interface: 10.200.2.110 --- 0xb
  Internet Address      Physical Address      Type
  10.200.2.1            08-5b-0e-fd-bc-bc     dynamic
  10.200.2.255          ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

C:\Users\ahyben>arp -a

Interface: 10.200.2.110 --- 0xb
  Internet Address      Physical Address      Type
  10.200.2.1            12-1a-7f-68-8a-aa     dynamic
  10.200.2.2            12-1a-7f-68-8a-aa     dynamic
  10.200.2.255          ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

Phishing attacks

Phishing is a general term that refers to any cyber attack where a hacker disguises themselves as a trusted source in order to acquire sensitive information.

- There are many types of phishing attack, but mostly used is scam e-mail.
  - Do you remember that Nigerian king that would like to save some gold on your account – it is not real ☹
- In general, it works in a way that someone will send you a message from an institute you trust, asking you to use their link to access your bank account and they will get access to it.
- Some of them are not so intelligent and will just ask you for some money with some pretty story about : gold in Africa, lost cousin in problems.
  - In Slovak language we have word “smejdi” for this. They can operate in real world or online.

Next steps in Network Security

There are many companies that provides dedicated trainings for this field, but all those trainings have pre-requisites of basic Networking, Linux & Virtualization skills.

Most of them require at least basic python skills.

Vendor neutral trainings :

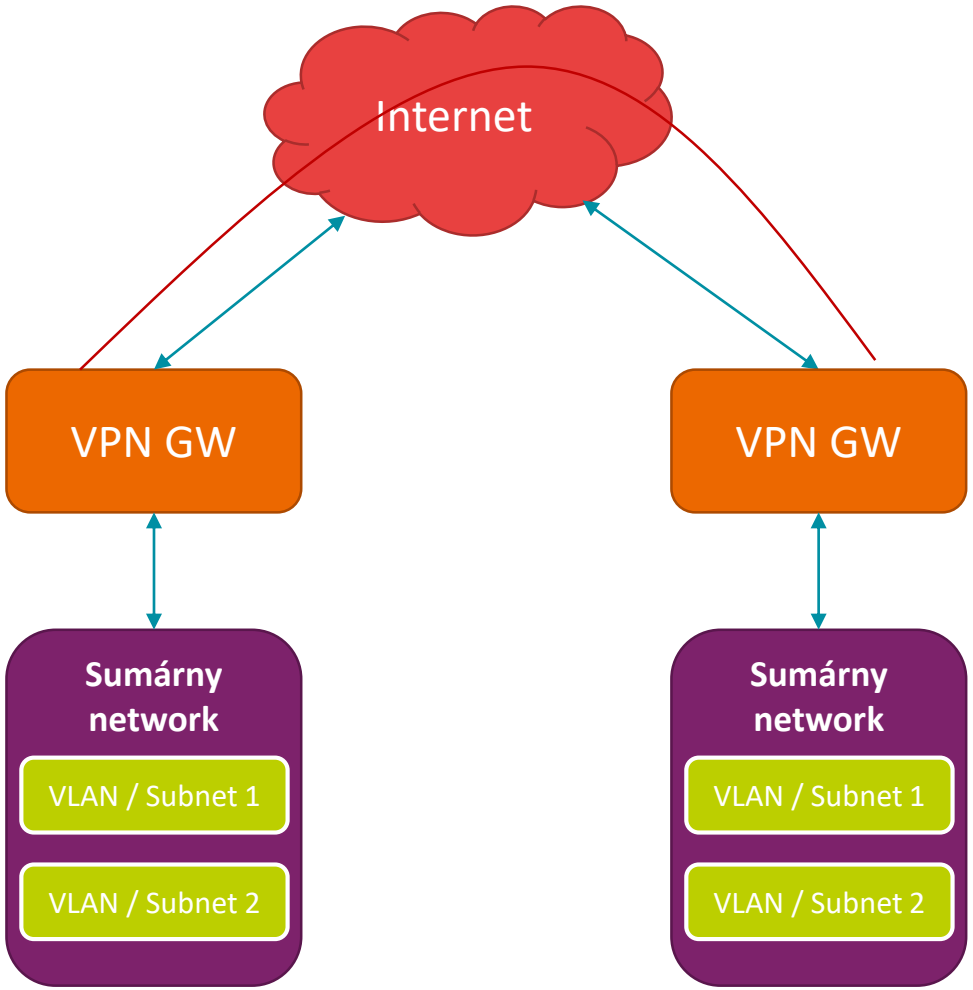
- CompTIA
- ISC^2
- EC-Council

Vendor specific (just example, there are many more) :

- Cisco
- FortiNet
- Juniper

Gateway – Gateway / IPSEC VPN

- IPsec VPN je bezpečný spôsob pripojenia dvoch alebo viacerých sietí cez internet, ktorý zabezpečuje šifrovanie a autentifikáciu dát prenášaných medzi sieťami.
- Tento typ VPN využíva IPsec (Internet Protocol Security) protokoly na zabezpečenie komunikácie medzi bránami, čím chráni dáta pred možným odpočúvaním alebo zmenou.
- IPSEC VPN umožňuje vzdialeným sieťam komunikovať tak, akoby boli priamo pripojené cez súkromnú sieť, čo je užitočné pre spojenie pobočkových kancelárií, výrobných závodov alebo distribučných centier.
- Každá brána v sieti má svoje vlastné unikátne identifikačné údaje, vrátane preddeleného kľúča, ktorý sa používa na autentifikáciu a zabezpečenie spojenia.
- Skladá sa z dvoch fáz :
  - 1. Fáza vytvorí kontrolné tunely medzi bránami, aby brány vedeli vytvoriť bezpečné dátové tunely
  - 2. Fáza vytvorí priamo dátové tunely, ktoré prenášajú dáta medzi lokáciami.



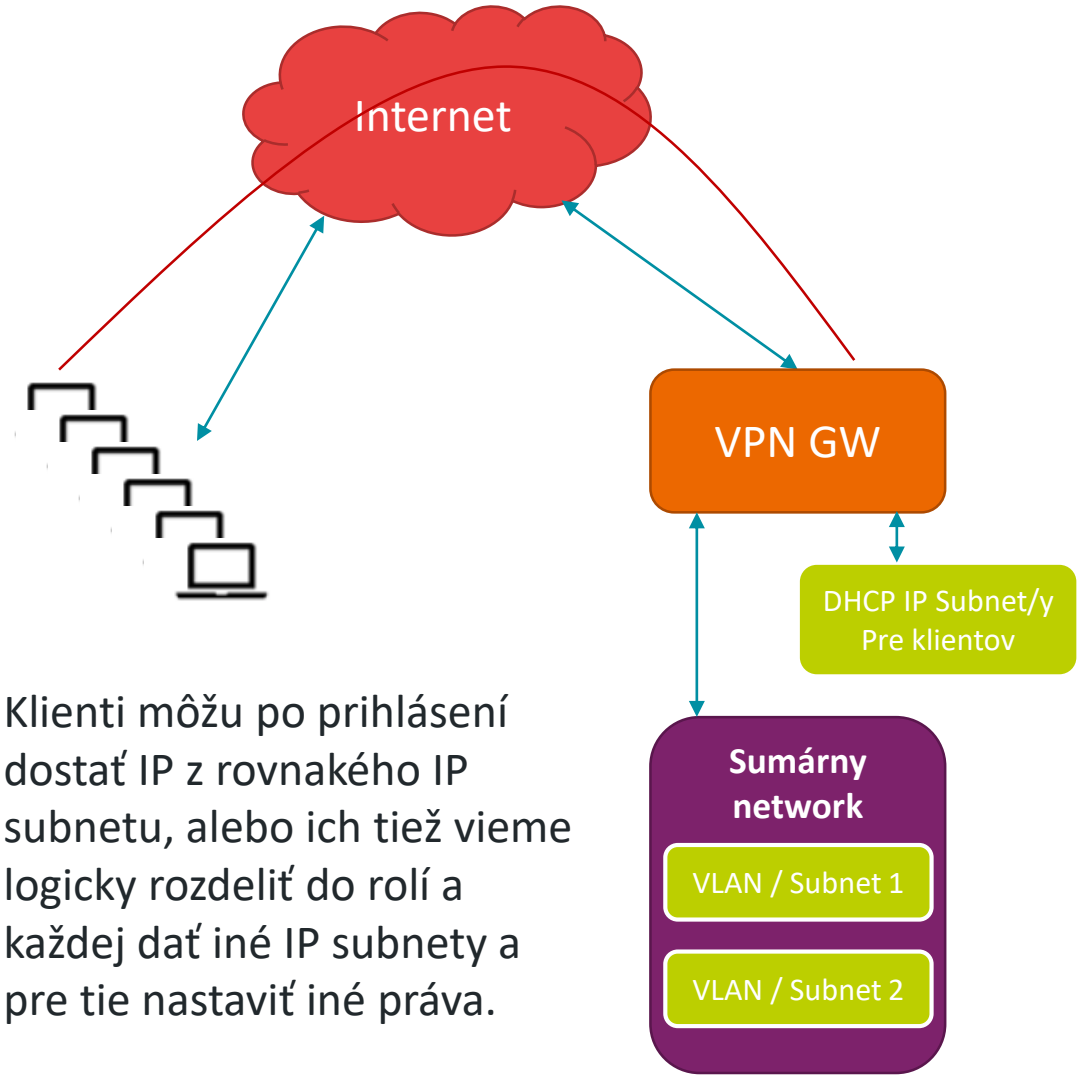
Príklad :

- Na lokácií 1 budeme mať 10.1.0.0/16
- Na lokácií 2 budeme mať 10.2.0.0/16

Subnety v oboch lokáciach môžeme mať rôzne menšie podsiete

Client – Gateway / SSL VPN

- Client-to-Gateway / SSL VPN je typ bezpečného pripojenia, ktorý umožňuje jednotlivým zariadeniam alebo užívateľom vzdialene pripojiť sa k sieti organizácie cez internet.
- Tento typ VPN zabezpečuje šifrovanie a autentifikáciu dát prenášaných medzi zariadením užívateľa (client) a bránou organizácie (gateway), čím chráni komunikáciu pred neoprávneným prístupom.
- Client-to-Gateway VPN je obzvlášť užitočný pre vzdialených zamestnancov, ktorí potrebujú pristupovať k firemnej sieti z rôznych lokalít alebo z domu.
- môže byť konfigurovaný pre rôzne typy autentifikácie, vrátane užívateľských mien a hesiel, dvojfaktorovej autentifikácie alebo certifikátov, čo zabezpečuje prispôsobiteľnosť podľa špecifických potrieb organizácie.
- Po úspešnej autentifikácií, dostane klient na svojom koncovom zariadení (PC, mobil, tablet), nový virtuálny interface, na ktorom prideluj IP adresu VPN gateway pomocou DHCP. Táto IP je následne použitá na komunikáciu do VPNky.
- Pri client-gateway VPNkach vieme hovoriť o 2 typoch routingu :
  - routing všetkého do VPN (čiže aj ked idete na facebook, či voláte cez MS Teams, ide to cez VPNku)
  - split-tunnel (do VPNky posielate len komunikáciu relevantnú pre biznis, všetko co má ísť do internetu tam aj naďalej ide)



Klienti môžu po prihlásení dostať IP z rovnakého IP subnetu, alebo ich tiež vieme logicky rozdeliť do rolí a každej dať iné IP subnety a pre tie nastaviť iné práva.

Cloud Networking

- Včera sme sa dozvedeli, že na segmentáciu sietí na menšie časti používame VLANky.
- Tiež sme sa dozvedeli, že limit na počet VLAN je 4096, čo asi nemôže byť dostačujúce pre počet v multi-tenant prostredí public cloudu.
- Ako to teda robia ?
  - Každému zákazníkovi, ktorý si vytvorí network (u rôznych operátorov sú iné názvy – napr. Vnet, VCN, VPC) vytvorí vlastný virtuálny switch. Nie VLANku – ale switch, ktorý môže mať rôzne VLANky.
  - V každom networku môže zákazník nastavovať VLANky, tieto ale môžu byť len z rovnakého IP range-u ako network (menšia sub-sieť), aby si ušetrili problémy s routingom.
  - Zákazníkovi dajú možnosť prepájať si tieto switche a ich VLANky cez rôzne virtuálne routre ale do internetu ide každý zákazník samostatne.
  - Ak niekto spravuje multi-tenant prostredie, musí sa pripraviť na 2 veľké challenges :
    - On-premise datacentrá s ich rozsahmi
    - Nevôla / Neschopnosť zákazníkov používať IP range, ktorý chceme.