1. RM – OSI

1.1 Transportní vrstva (L4)

Slouží k adresování a značkování paketů, zajišťuje bezchybný přenos dat mezi dvěma zařízeními. Na základě typu spojení *(protokolu používaného aplikační vrstvou)* vybere buď TCP nebo UDP protokol. Realizuje end-to-end přenos aplikačních dat. Adresování na základně čísla portu, socket je označení pro IP adresu s portem *(např. 192.168.1.1:1337)*.

Provádí:

- segmentaci dat: dělení aplikačních dat na menší části a na přijímací straně opětovné složení
- multiplexování: umožňuje používání více aplikací v jednom časovém okamžiku
- zajišťuje doručení dat ve správném pořadí patřičné aplikaci
- detekuje a opravuje chyby

1.1.1 TCP

Spojově orientovaný přenos dat, doplňuje přenášená data o větší množství řídicích informací v záhlaví. Použití např. u HTTP (S), FTP. Pro sestavení spojení využívá three way handshake, pro ukončení pak two way handshake. Záhlaví o velikostit 20 B, PDU: segment.

1.1.2 UDP

Nespojově orientovaný přenos dat. Pouze základní funkce pro doručení jednotlivých datových částí mezi aplikacemi. Dochází k rychlému doručení dat bez zajištění spolehlivosti doručení všech části odeslaných dat. Vhodné především pro protokoly vyžadující malé zpoždění *(DNS, VoIP)*. Záhlaví o velikosti 8 B, PDU: datagram.

Pevně přidělené porty jsou cílové porty u serveru *(např. 80)* a většinou jsou v rozsahu 0 – 1023. **Dynamické porty** pak jsou používány na PC *(generuje je OS)* a jsou v rozsahu 1024 – 65535.

1.2 Relační vrstva (L5)

Provádí:

- vytváření, udržování a ukončování relací mezi zdrojovou a cílovou aplikací
- řízení výměny informací

1.3 Prezentační vrstva (L6)

Provádí:

- kódování a konverzi dat do binární podoby z aplikační vrstvy
- kompresi dat: snížení množství přenášených dat
- šifrování

Protokoly jako MPEG, JPEG, ASCII.

1.4 Aplikační vrstva (L7)

Programová vrstva, na této vrstvě pracují programy, které nějakým způsobem využívají připojení k síti. Funguje jako rozhraní mezi uživatelem a síti.

2. Protokoly

2.1 FTP

- TCP, porty 20 *(přenos dat)* a 21 *(přenos příkazů)*

- Slouží k přenosu souborů

2.2 SSH

- TCP, port 22
- Zabezpečená náhrada Telnetu

2.3 Telnet

- TCP, port 23
- Slouží k vzdálené správě počítačů

2.4 DNS

- TCP/UDP, port 53
- Stará se o překlad doménového jména na IP adresu

2.4.1 Typy DNS záznamů

A – přiřazení doménového jména s IPv4 adresou
AAAA – přiřazení doménového jména s IPv6 adresou
CNAME – přiřazení aliasu k doménovému jménu
MX – označení mail serveru, který doručuje e-maily pro tuto doménu
NS – označení pro autoritativní servery pro doménu
PTR – uložení reverzních záznamů
SOA – základní informace o doméně *(hlavní nameserver, e-mail na správce, expirace)*

2.4.2 Postup předkladu

- Uživatel zadá doménové jméno, které chce přeložit
- Resolver *(klient)* prohledá nejdříve vlastní paměť *(cache, obsahující již dříve vyžádané záznamy)*
- Pokud resolver nenalezne odpověď ve vlastní paměti, předá požadavek na DNS server
- DNS prohledává vlastní paměť *(autoritativní záznamy i dříve získané neautoritativní)*
- Pokud DNS server nenalezne odpověď ve své paměti, požádá o pomoc *(předáním dotazu)* jiné DNS servery
- DNS server, který obsahuje *(ne)*autoritativní záznam na dotaz, pak odešle zpět odpověď DNS serveru, který dotaz odeslal
- Získaný překlad si DNS server uloží jako neautoritativní do své paměti a zároveň jako odpověď odešle resolveru *(klientovi)*
- Odpověď je použitá aplikací, která požádala a zároveň uložena do vlastní paměti resolvera

2.5 HTTP

- TCP, port 80
- Používá se pro WWW, klient odešle dotaz na server a server odešle odpověď

2.6 HTTPS

- TCP, port 443
- Zabezpečená *(pomocí SSL nebo TLS)* verze HTTP

2.7 POP

- TCP, port 110
- Stažení e-mailů z poštovního serveru *(pošta pak nezůstává na serveru)*

2.8 SMTP

- TCP, port 25
- Odesílání e-mailů od klienta na server *(nebo mezi servery)*

2.9 IMAP

- TCP, port 143
- Práce s e-maily online *(pošta zůstává na serveru)*

2.10 DHCP

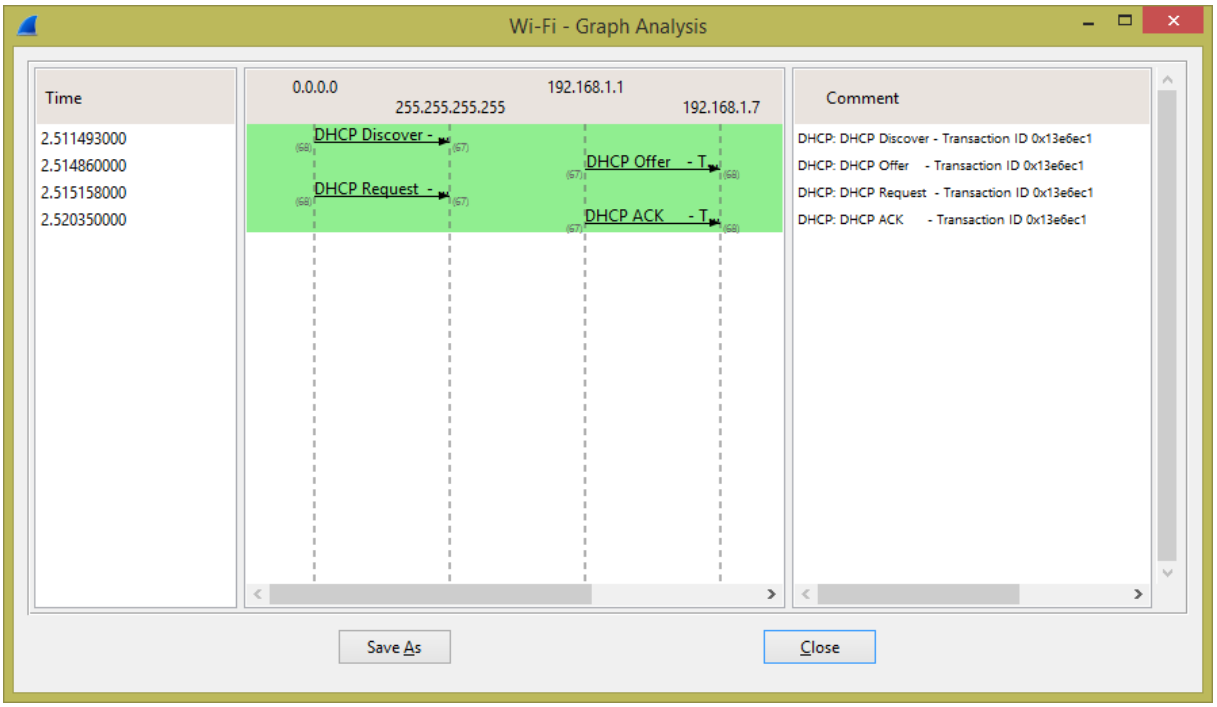
- UDP, porty 67 a 68
- Zajišťuje připojení hosta do sítě *(automatické přidělení síťových parametrů)*

2.10.1 DHCP analýza

No.	Time	Source	Destination	Protocol	Length	Info
42	2.51149300	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x13e6ec1
43	2.51486000	192.168.1.1	192.168.1.7	DHCP	342	DHCP Offer - Transaction ID 0x13e6ec1
44	2.51515800	0.0.0.0	255.255.255.255	DHCP	357	DHCP Request - Transaction ID 0x13e6ec1
45	2.52035000	192.168.1.1	192.168.1.7	DHCP	357	DHCP ACK - Transaction ID 0x13e6ec1

Ze zachyceného průběhu lze vidět DHCP konverzaci, která je tvořena 4 zprávami *(2 od klienta, 2 od serveru)*. Po připojení do sítě klient *(0.0.0.0)* odešle broadcastově *(255.255.255.255)* do sítě zprávu **DHCP Discover**. Pokud se v síti nalézá DHCP server *(nebo servery, 192.168.1.1)* tak na zprávu odpoví – zpráva **DHCP Offer**.

Klient si následně vybere z odpovědí, které mu přišly a požádá o přidělení zaslaných parametrů – zpráva **DHCP Request**. Následně server potvrdí zprávou **DHCP ACK** klientovi *(192.168.1.7)* síťové parametry a klient začíná pod nimi v síti vystupovat. Vše jde vidět ještě v níže uvedeném flow grafu.



2.11 Souhrn

Protokol	Port	Protokol L4
FTP	20, 21	TCP
SSH	22	TCP
Telnet	23	TCP
SMTP	25	TCP
DNS	53	UDP/TCP
DHCP	67, 68	UDP
HTTP	80	TCP
POP	110	TCP
IMAP	143	TCP
HTTPS	443	TCP

3. Bezpečnost

ACL je seznam pravidel, která řídí přístup k nějakému objektu. Jedná se o základní síťovou bezpečnost k blokování/povolení provozu, může být využít i ke kontrole šířky pásma nebo k identifikaci či klasifikaci provozu.

ACL je řazený seznam pravidel povolit a zakázat. K identifikaci můžeme použít jméno anebo číslo seznamu. Nové pravidla se řadí na konec, seznam se prochází od začátku ke konci a v případě shody se již dále neprochází. Každý neprázdný seznam má na konci defaultní pravidlo zakazující vše, prázdný seznam povoluje vše. Vždy je nutné povolit/zakázat i zpětný směr.

- Povolte do Internetu protokoly DNS a HTTP(S)

Odchozí směr

Pořadí položky	Povolit / zakázat	Protokol	Zdrojová IP	Zdrojový port	Cílová IP	Cílový port
1	povolit	UDP	*	*	*	53
2	povolit	TCP	*	*	*	53
3	povolit	TCP	*	*	*	80
4	povolit	TCP	*	*	*	443
5	zakázat	IP	*		*	

Příchozí směr

Pořadí položky	Povolit / zakázat	Protokol	Zdrojová IP	Zdrojový port	Cílová IP	Cílový port
1	povolit	UDP	*	53	*	*
2	povolit	TCP	*	53	*	*
3	povolit	TCP	*	80	*	*
4	povolit	TCP	*	443	*	*
5	zakázat	IP	*		*	

4. Směrování

Směrování je proces nalezení vhodné cesty k cíli a směrování provádí routery. Směrování se provádí na základně IP adresy cíle, uvedeného v záhlaví IP paketu a směrovací tabulky, kterou si tvoří router.

Mezi beztřídní směrovací protokoly patří RIPv2, EIGRP, OSPF. Tyto směrovací protokoly odesílají v aktualizačních zprávách kromě síťové adresy taky informaci o masce. Beztřídní směrovací protokoly jsou nezbytné pro použití sumarizace cest *(propagování souvislého rozsahu adres jako jedné s kratší maskou)*.

4.1 Statické směrování

Statický směrovací záznam je jeden ze způsobů jak přidat do směrovací tabulky informace o vzdálených sítích – typické použití v malých sítích anebo jak výchozí cesty k jednomu ISP.

Minimálně zatěžuje, CPU, snadná konfigurace. Nevýhody jako časově náročná konfigurace i údržba, možnost vzniku chyb, nutná úprava při změně topologie.

4.2 Dynamické směrování

Dynamické směrování funguje automaticky a router získává informace o vzdálených sítích od ostatních routerů.

Při přidání či odebrání sítí je minimum úprav, protokoly na změny reagují automaticky. Dynamické směrovací protokoly však zatěžují CPU, paměť i šířku pásma na linkách.

4.2.1 Distance vektor

Každá cesta je inzerována jako vektor vzdálenosti a směr. Vzdálenost je definována termíny z metriky *(např. počet hopů)* a směr jako následující směrovač *(např. next hop router)*.

Některé DV protokoly posílají periodicky kompletní směrovací tabulky všem připojeným sousedním směrovačům. Nejlépe pracují v jednoduchých sítích, mají však pomalý čas konvergence. Příkladem toho protokolu je RIP.

4.2.2 Link state

Pomocí LS protokolů získává směrovač informace na základně, kterých si vytváří kompletní mapu topologie. Všechny směrovače v síti používají stejnou mapu topologie, dle které pak vybírají nejlepší cestu k cíli.

Směrovací informace si LS protokoly vyměňují do doby, než dojde ke konvergenci v síti *(ta je rychlejší než u DV protokolů)*. Další informace se posílají pouze v případě změny v topologii. Typický představil je OSPF.

5. NAT

- Překlad zdrojové nebo cílové IP adresy *(na L3 prvcích)* – typicky překlad mezi veřejnými a privátními adresami
- Překládá se na základě překládací tabulky, která je tvořena staticky nebo dynamicky *(automaticky)*
- Skrytí vnitřní struktury sítě