Analýza síťové komunikace

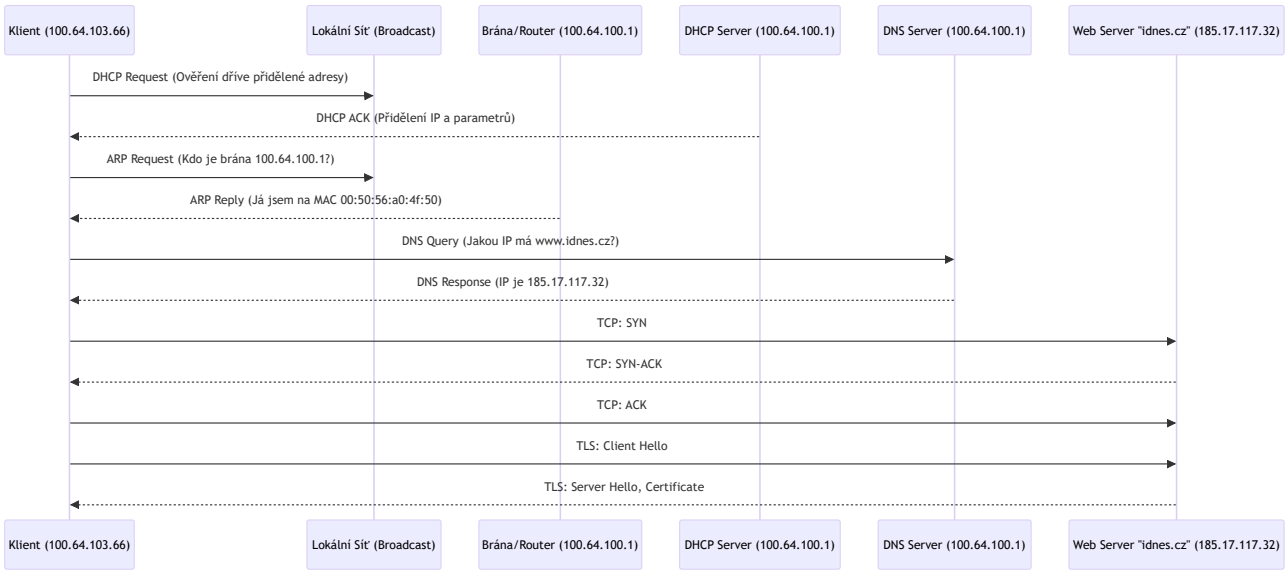
Tento MD/PDF dokument popisuje a analyzuje klíčové fáze síťové komunikace, od prvotního připojení počítače do sítě až po navázání zabezpečeného spojení s webovým serverem `www.idnes.cz`. Analýza je založena na filtrovaném záznamu síťové komunikace, který vznikl pomocí nástroje **Wireshark** a následné úpravy (zmenšení zdrojového pcapng souboru z důvodu přehlednosti) dle požadavků zadání:

```
$ tshark -r zit_ukol.pcapng -Y 'arp || bootp || dns || tcp.flags.syn==1 || tls.handshake' -w analyza_filtered.pcapng
```

V každé sekci jsou uvedeny klíčové zachycené pakety pomocí CLI ulitity `tshark`. Příklad CLI příkazu pro paket č. 2:

```
$ tshark -r analyza_filtered.pcapng -Y "frame.number == 2"
```

Prezentace komunikace: Sekvenční diagram - mermaid



Analýza komunikace

DHCP – Získání IP adresy

- **Identifikace**: Proces získání IP adresy začal v paketu č. 1 (`DHCP Request`), pokračoval žádostí v paketu č. 24 (`DHCP Request`) a byl finálně potvrzen v paketu č. 25 (`DHCP ACK`) serverem `100.64.100.1`, který přidělil následující síťové parametry: **IP adresa klienta**: 100.64.103.66, **Maska podsítě**: 255.255.252.0, **Výchozí brána (Router)**: 100.64.100.1

> Nezachytil jsem `DHCP Discover` , ani `DHCP Offer`, protože klient neprošel plným DORA cyklem (**Discover -> Offer -> Request -> ACK**), ale jen `INIT-REBOOT` (ověření dříve přidělené adresy).

- **Komentář**: DHCP (Dynamic Host Configuration Protocol) je základní služba, která automatizuje proces konfigurace síťových zařízení.

▼ ► Zobrazit detaily: DHCP (získání IP adresy)

Pakety: `1, 24, 25`

```
  1   0.000000      0.0.0.0 → 255.255.255.255 DHCP 358 DHCP Request  - Transaction ID 0xd628c0eb
 24   3.002096      0.0.0.0 → 255.255.255.255 DHCP 358 DHCP Request  - Transaction ID 0xd628c0eb
 25   3.003201 100.64.100.1 → 255.255.255.255 DHCP 363 DHCP ACK      - Transaction ID 0xd628c0eb
```

ARP – Zjištění MAC adresy brány

- **Identifikace**: Po získání IP adresy se klient v paketu č. 2 zeptal (`ARP Request`) na MAC adresu své brány (`100.64.100.1`). Odpověď od brány přišla v paketu č. 16 (`ARP Reply`) s MAC adresou `00:50:56:a0:4f:50`. Součástí byla i bezpečnostní kontrola v paketu č. 3 (`ARP Probe`).
- **Komentář**: ARP (Address Resolution Protocol) funguje jako překladatel mezi síťovou vrstvou (IP adresy) a linkovou vrstvou (MAC adresy) pro odeslání datového rámce v rámci lokální sítě.

▼ ► Zobrazit detaily k ARP

Pakety: `2, 3, 16`

```
2   0.019876 c8:53:09:2d:43:b3 → Broadcast    ARP 42 Who has 100.64.100.1? Tell 100.64.103.66
3   0.221220 c8:53:09:2d:43:b3 → Broadcast    ARP 42 Who has 100.64.103.66? (ARP Probe)
- Bezpečnostní kontrola, kdy se počítač ptá: "Používá někdo v síti moji budoucí IP adresu `100.64.103.66`?". Tím se brání konfliktu IP adres.
16   2.712372 VMware_a0:4f:50 → c8:53:09:2d:43:b3 ARP 60 100.64.100.1 is at 00:50:56:a0:4f:50
```

DNS – Překlad doménového jména

- **Identifikace**: V paketu č. 272 odeslal klient dotaz (`DNS Query`) na A `www.idnes.cz`. Server v paketu č. 275 odpověděl (`DNS Response`), že finální IP adresa serveru je `185.17.117.32`. Souběžně probíhala i doplňující komunikace v paketech 273 a 274.
- **Komentář**: DNS (Domain Name System) je hierarchická jmenná služba, která poskytuje IP pro doménové jméno; bez něj by klient musel znát cílovou IP.

▼ ► Zobrazit detaily k DNS

Pakety: `272, 273, 274, 275`

```
272  15.970809 100.64.103.66 → 100.64.100.1 DNS 72 Standard query 0x9bea A www.idnes.cz
273  15.971016 100.64.103.66 → 100.64.100.1 DNS 72 Standard query 0x3f24 HTTPS www.idnes.cz
274  15.971569 100.64.100.1 → 100.64.103.66 DNS 145 Standard query response 0x3f24 HTTPS www.idnes.cz CNAME c1.idnes.cz SOA ns.mafra.cz
275  15.986522 100.64.100.1 → 100.64.103.66 DNS 105 Standard query response 0x9bea A www.idnes.cz CNAME c1.idnes.cz A 185.17.117.32
```

TCP – 3-way handshake (Trojcestný handshake)

- **Identifikace**: Před přenosem dat bylo navázáno spolehlivé TCP spojení se serverem `185.17.117.32` pomocí třícestného handshake: `SYN` (paket č. 276), `SYN-ACK` (paket č. 277), `ACK` (paket č. 278)
- **Komentář**: TCP (Transmission Control Protocol) je spojově orientovaný protokol, který zaručuje, že data dorazí kompletní a ve správném pořadí. Trojcestný handshake je mechanismus, kterým se obě strany "domluví" na navázání spojení, potvrzuje obousměrnou dosažitelnost a nastavuje parametry spojení.

▼ ► Zobrazit detaily k Trojcestnému handshake

Pakety: `276, 277, 278`

```
276  15.986955 100.64.103.66 → 185.17.117.32 TCP 66 65081 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
277  15.992675 185.17.117.32 → 100.64.103.66 TCP 66 443 → 65081 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 WS=1 SACK_PERM
278  15.993118 100.64.103.66 → 185.17.117.32 TLSv1 1808 Client Hello (SNI=www.idnes.cz)
```

HTTPS (TLS) – Navázání šifrovaného spojení

- **Identifikace**: Ihned po TCP handshake byl v paketu č. 278 zahájen TLS handshake zprávou `ClientHello`. Server odpověděl v paketu č. 279 zprávou `ServerHello`, kde vybral parametry šifrování a poslal svůj certifikát.:
  - **Použité porty**: Komunikace probíhala mezi klientem (zdrojový port `65081`) a serverem (cílový port `443`).
- **Komentář**: TLS (Transport Layer Security) je kryptografický protokol, který poskytuje zabezpečení nad TCP. TLS zajišťuje důvěrnost a integritu; po výměně hello a parametrech následuje šifrovaný obsah.

▼ ► Zobrazit detaily k TLS

Pakety: `278,279`

```
278  15.993118 100.64.103.66 → 185.17.117.32 TLSv1 1808 Client Hello (SNI=www.idnes.cz)
279  16.000934 185.17.117.32 → 100.64.103.66 TLSv1.3 2974 Server Hello, Change Cipher Spec, Application Data
```