UDP analyzátor

Mužík Jan

1. Zadání

Cílem práce je vytvořit grafickou aplikaci, která umožní sledování a jednoduchou tvorbu UDP packetů.

Program bude umožňovat vlastní tvorbu definice formátu packetu (struktura packetu, způsob překladu dat z binární formy do čitelné a zpět). Podle ní budou procházející packety zobrazovány a bude vytvářen formulář pro odesílání vlastních packetů.

2. Implementace

Program byl vytvořen v jazyce Python (verze 2.4) a jako grafické rozhraní byly použity wxWidgets. Pro síťovou komunikaci byly vyžadovány knihovny obsahující thready a sockety, pro ukládání dat do souboru pak knihovna cpickle, která zajišťuje jejich serializaci.

Samotná implementace byla zaměřena na operační systémy Windows, ale vzhledem k přenositelnosti jazyka a jeho komponent, měla by být kompatibilní i se systémy Linux a Solaris. Výsledkem je tedy zkompilovaná aplikace, určená pro operační systém Windows ve formátu .exe.

Z pohledu uživatele se skládá program ze dvou funkčních částí: z okna tvorby předpisu packetu, kde se tvoří definice, a z oken ovládání a sledování jednotlivých packetů.

2.1 Předpis packetu

Každý packet je definovaným tzv. předpisem packetu, který se vytváří v okně Tvůrce předpisu. Ten nese informace o samotné struktuře packetu a některé dodatečné řídící informace potřebné ke sledování a vytváření formulářů potřebných k případnému odesílaná packetu.

Předpis se skládá ze skupiny pojmenovaných proměnných, které zastupují vybrané části v packetu, a názvu packetu. Každá proměnná je tedy určena svojí pozicí v packetu, datovým typem a délkou, kterou zaujímá. Dále nese navíc řídící informaci o tom, zda je proměnná imaginární či nikoliv.

2.1.1 Proměnné

Pozice proměnné je určena v počtu bytů od počátku packetu s tím, že první bajt je považován za nultý.

Datový typ pouze označuje, jakým způsobem mají být data reprezentována při zobrazení a opět ukládána zpět do binární podoby. Je tedy jedno, zda bude úsek dat považován za číslo nebo za text - buď bude zobrazen jako číslo jako posloupnost znaků.

Jsou rozlišovány 4 datové typy:

- Číslo - jako parametr se určuje jakou zaujímá délku a to v rozmezí 1 až 4 bytů. Zobrazeno bude jako celé kladné číslo v desítkové soustavě a formulář vyžaduje, aby bylo zadáno ve stejném formátu (pouze znaky 0-9).
- Příznaky – jedná se o skupinu osmi pojmenovaných 1-bitových příznaků reprezentujících hodnoty True (1) nebo False (0). Proměnná bude zobrazována jako výčet jmen příznaků, které nabývají hodnoty True, ve formuláři jako sada zaškrtávacích polí.
- Text – reprezentuje data v čistém textovém formátu. Binární data budou zobrazena jako posloupnost příslušných znaků podle ascii tabulky.
- Hexadata – reprezentuje skupinu hexadecimálních hodnot. Při zobrazení budou data vyobrazena ve formátu *0xFF*. Při zadávání do formuláře jsou vyžadovány pouze hexadecimální znaky a to v jednom z formátů:

0xAA 0xBB 0xCC	s mezerami
AA BB CC	s mezerami
AABBCC	bez mezer

Délka proměnné je u datových typů Číslo a Příznaky určena přímo jejich vlastnostmi – Číslo je dlouhé 1 až 4B, Příznaky 1B. U ostatních datových typů je délku nutné uvést jinak bude implicitně nastavena na 1 byte. Pokud bude délka nastavena na hodnotu -1 bude uvažováno, že proměnná zasahuje až na konec packetu.

Proměnné nejsou vůči sobě kontrolovány, zda se vzájemně nepřekrývají. Pokud by k tomu docházelo, problém by nenastal při čtení – to by proběhlo v pořádku, ale při odesílání vlastního packetu. Data z jedné proměnné přepíší data (nebo jejich překrývající se část) v druhé proměnné.

Imaginární je dodatečná řícící informace, která má zabránit nechtěnému vzájemnému přepsání hodnot. Pokud je proměnná takto označena, bude sice zobrazována při čtení, ale při vytváření vlastního packetu (k odeslání) bude ignorována a ani se nezobrazí pole pro jejich zadání.

2.2 Síťová spojení

Veškeré řízení a sledování toku se kontroluje a provádí v okně Prohlížeč spojení. V levé části se vypisují příchozí a odchozí UDP packety a jsou zobrazeny způsobem, jaký je nadefinován v předpisu packetu (ten musí být nahrán přes tlačítko Nahrát předpis). V pravé části se potom nachází ovládací prvky pro řízení toku packetů a jejich zobrazení.

Nastavení spojení umožňuje základní řízení toku packetů. Umožňuje aplikaci fungovat vždy v jednom ze tří režimů:

- Client

  Aplikace se chová jako klient – dovoluje odesílat packety směrem k nastavenému vzdálenému serveru a opět je přijímat.
- Server

  Aplikace beží jako server – je definován port, na kterém jsou přijímány packety od klientů a podle nastavení můžou být i vraceny klientům zpět. V tomto režimu není možno odesílat vlastní packety.
- Man-In-Middle

  Aplikace funguje jako „muž uprostřed“. Naslouchá příchozím packetům od klientů a přeposílá je nastavenému vzdálenému serveru. Pokud server odpoví, aplikace vrátí packet správnému klientovi, kterému náleží. V tomto režimu není možno odesílat vlastní packety.

  Tato metoda funguje na předpokladu, že server pošle data zpět na stejný port, z jakého mu přišla. Po té, co jsou přijata data od klienta na standartním naslouchacím port, je vytvořen nový port určený pro komunikaci se serverem a z něj jsou data serveru poslána. Server odpoví na nový port a podle něj se rozpozná, o které „spojení“ se jedná a podle toho se data pošlou zpět správnému klientovi.

Po nastavení režimu a vyplnění potřebných dat se síť aktivuje tlačítkem Aktivovat. Jakmile je aktivována, nelze již nastavení měnit do jejího zastavení (tlačítkem Stop).

Pro správné zobrazení packetů je nutné nahrát správný předpis packetu, to se provede tlačítkem Nahrát předpis.

Pro vytvoření a odeslání vlastního packetu (pouze v režimu Client) slouží grafické tlačítko Poslat packet (). Po jeho stisknutí se zobrazí okno s formulářem pro všechny definované proměnné (které nejsou Imaginární).

Tlačítkem Smazat ( ) se smaže výpis packetů v levé části okna.

2.3 Poslání vlastního packetu

Vlastní packet lze poslat pouze v případě aktivované sítě v režimu Client. Okno Odeslat packet lze vyvolat tlačítkem v okně Síťová spojení tlačítkem Poslat ().

Okno obsahuje zobrazuje formulář podle aktuálního nahraného předpisu packetu (v okně Síťová spojení), správný předpis lze případně nahrát tlačítkem Nahrát předpis.

Dle předpisu se generuje formulář obsahuící vstup pro každou z proměnných (kromě Imaginární). Každá z proměnných vyžaduje vstup ve správném formátu (Číslo pouze číslice, hexadata pouze hexadecimální znaky). Pokud je vstup špatný, zbarví se dané pole červeně.

Po vyplnění formuláře (prázdná pole jsou povolena) se data odešlou tlačítkem Odeslat packet.