Uživatelská dokumentace k Prototypu mikrosondy (uSondy) pro monitorování IPv6 provozu

Brno, 2015

Obsah

Protokoly pro export zachycené komunikace

Komunikaci lze exportovat 3 způsoby. Prvním je export přes TCP spojení, které zajistí, že veškeré exportované pakety budou doručeny na ukládací zařízení. Druhým způsobem je export UDP protokolem, zde hrozí možnost, že exportované pakety budou po cestě zahozeny, nebo dorazí v jiném pořadí než byly odeslány. Třetí možností je tzv. Direct export, v tomto případě jsou pakety exportovány téměř beze změny a tedy ukládací zařízení musí být připojeny přímo k uSondě, jinak exportované pakety vůbec nedorazí.

Srovnání protokolů

Protokol	Rychlost	Překročení MTU	Ztráta paketu	Poznámka
TCP	300Mb/s	NE	NE	Vhodné při záchytu filtrované komunikace
UDP	1Gb/s	ANO	ANO	Vhodné při záchytu veškeré komunikace na lince
Direct Export	1Gb/s	NE	NE	Úložné zařízení musí být připojeno přímo k uSondě

Formát dat exportovaných přes TCP

Před každý zachycený paket je vložena INI3 hlavička:

```
|     0     |    1    |      2     |     3     |
+-----------+---------+------------+-----------+
|       Blob Size     | Interface  | Reserved  |
|                Timestamp_0 (unix)             |
|                Timestamp_1 (ns přesnost)      |
|        RID_0        |          RID_1          |
```

```
Blob Size        Velikost zachyceného rámce                                    (2 bytes)
Interface        Rozhraní na kterém byl příchozí rámec zachycen                (1 bytes)
Reserved         Rezervováno pro budoucí použití                               (1 bytes)
Timestamp        Časová značka příchodu paketu ze sítě na rozhraní             (4 + 4 bytes)
RID 0/1          Identifikátor pravidla, podle kterého byl paket vybrán pro export  (2 + 2 bytes)
```

INI3 hlavička + zachycený paket tvoří tzv. superpaket. Několik superpaketů je následně spojeno dohromady a odesláno přes TCP jako aplikační data. Pozn. může dojít k situaci, kdy v 1 TCP paketu je několik superpaketů, kde poslední superpaket není celý. Zbytek tohoto superpaketu je odeslán v následujícím TCP paketu.

Formát dat exportovaných přes UDP

Před každý zachycený paket je vložena INI3 hlavička jako v případě exportu přes TCP. Následně každý odeslaný UDP paket obsahuje právě 1 superpaket. Pokud je velikost původního zachyceného paketu + velikost INI3 hlavičky větší než MTU cesty, přes kterou UDP paket musí projít, pak ho nějaký síťový prvek po cestě zahodí.

Formát Direct export protokolu

U exportovaných paketů je nahrazena zdrojová a cílová MAC adresa MACINI3 hlavičkou. Kvůli tomu je potřeba připojit ukládací zařízení přímo k mikrosondě.

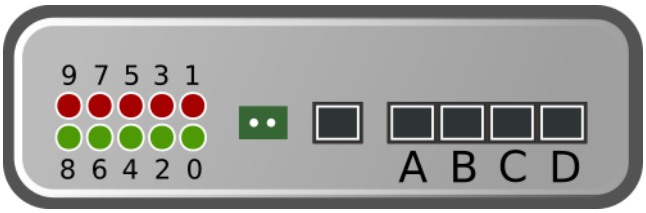
Vstupní Ethernet II rámec

```
+----+----+------+------+-----+
| DA | SA | Type | Data | FCS |
+----+----+------+------+-----+

DA          Destination MAC Address (6 bytes)
SA          Source MAC Address    (6 bytes)
Type        Protocol Type                    (2 bytes)
Data        Protocol Data                    (46 - 1500 bytes)
FCS         Frame Checksum                   (4 bytes)
```

Výstupní Ethernet II rámec

```
+----+----+------+------+-----+
 |  INI3   | Type | Data | FCS |
 +----+----+------+------+-----+
/           \
|            \_____________________________________
|                                                  \
|                      MACINI3                     |
+-----------+----------+-----------+----------+
|     0     |     1    |      2    |     3    |
+-----------+----------+-----------+----------+
|   Sequence number    | Interface | Reserved |
|               Timestamp_0 (unix)             |
|               Timestamp_1 (ns přesnost)      |

Sequence number  16B neznaménkové číslo, označuje pořadové číslo zachyceného rámce  (2 bytes)
Interface        Rozhraní na kterém byl příchozí rámec zachycen                      (1 bytes)
Reserved         Rezervováno pro budoucí použití                                     (1 bytes)
Timestamp        Časová značka příchodu paketu ze sítě na rozhraní                   (4 + 4 bytes)
```

Čelní panel uSondy



Obrázek 1: Čelní panel

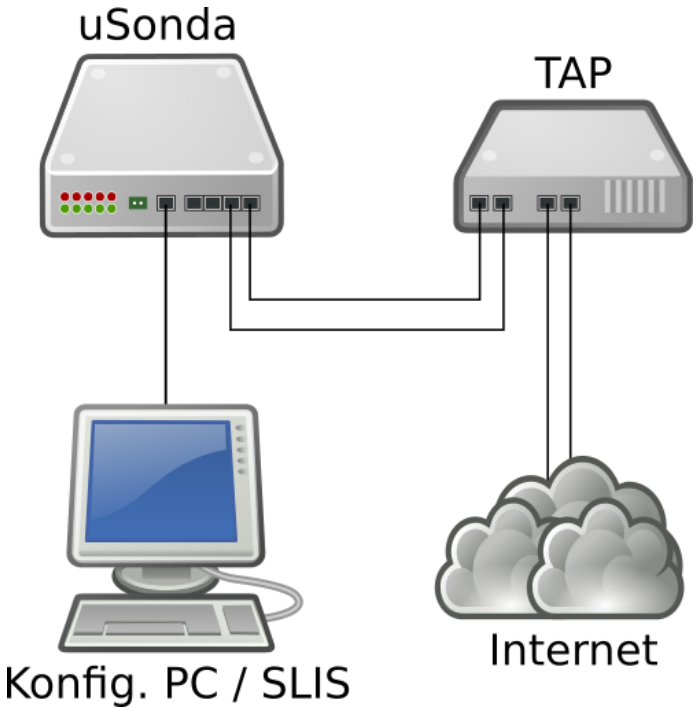
Administrační port (Neoznačený port)
Výstupní port (A)
Odposlechové vstupní porty (C,D)

Po připojení napájecího napětí pomocí externího zdroje se uSonda spustí a zhruba do 30 sekund nabootuje operační systém a automaticky se spustí všechny potřebné služby.

Zapojení

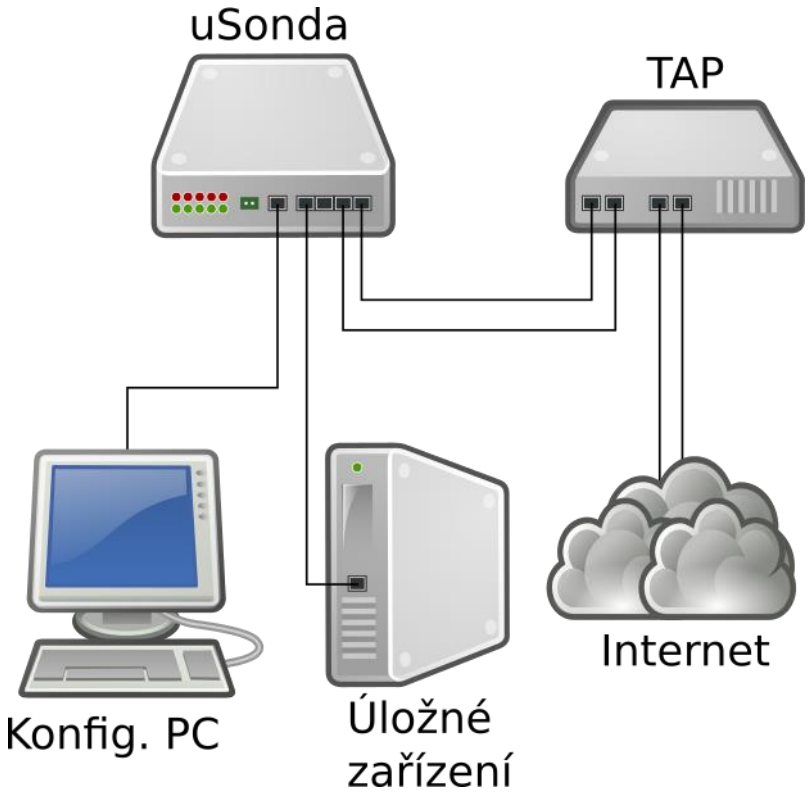
Konfigurace uSondy se provadí přes **Administrační port**. Odposlouchávaná linka je vždy připojena přes ethernetový TAP do portů **C**,**D**. Způsob připojení zařízení, na které se odchycená komunikace bude ukládat, záleží na nastavení uSondy.

Zapojení - TCP export



Obrázek 2: TCP export

Zapojení - UDP/Direct export



Obrázek 3: UDP/Direct export

Nastavení IP adresy po spuštění

Na SD kartě uSondy je soubor **settings**, ve kterém je možné nastavit IP adresu, která se přiřadí **Administračnímu portu (Neoznačený port)**. Výchozí obsah souboru:

```
#This option set default IP adress
# Examples
# IPADDRESS=10.10.10.10/24 - after boot on ETH1 will be set IP 10.10.10.10 255.255.255.0
# IPADDRESS=dhcp - after boot IP adress on ETH1 will be received from DHCP server

IPADDRESS=dhcp
```

Pozn. řádky začínající # jsou komentáře a na funkčnost nemají vliv

Položku **IPADRESS** je možné nastavit na řetězec dhcp, kdy IP adresa se získá přes dhcp protokol. Alternativně je možné nastavit konkrétní IP adresu s délkou prefixu (např. 192.18.0.1/24)

Nastavení uSondy

uSonda má dostupné webové rozhraní přes na **Administračním portu**. IP adresa tohoto portu je nastavitelná viz Nastavení IP adresy po spuštění.

Přístupové údaje na webové rozhraní:

```
Uživatelské jméno: admin
            Heslo: R6sataJpuj
```

Konfigurace způsobu exportování a nastavení času na uSondě se provádí v nabídce **Configure**. Nastavení filtrovacích pravidel pro záchyt komunikace je dostupné na stránce **Interceptions**.

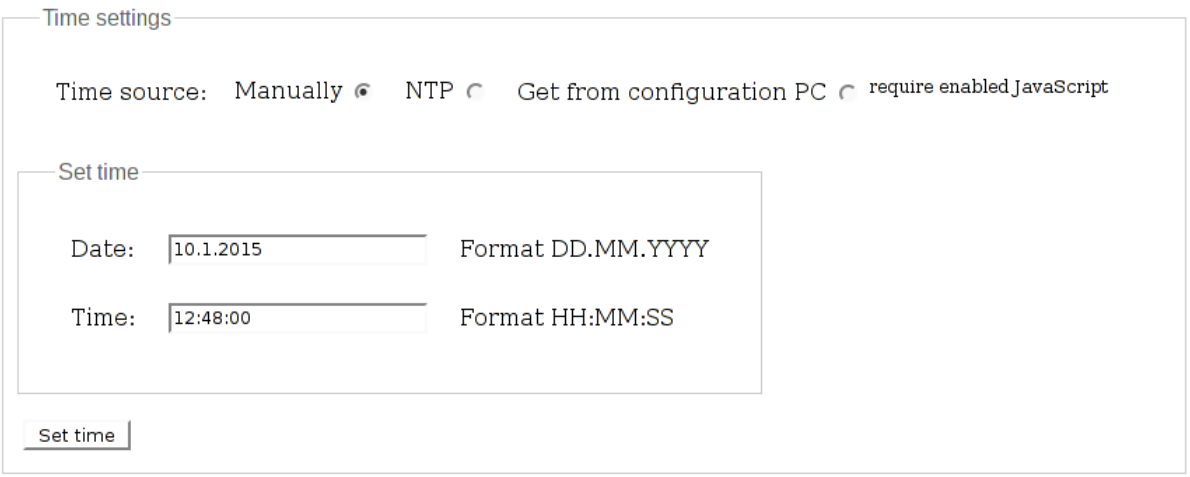
Nastavení času

Po zapnutí je potřeba nastavit aktuální čas, tak aby časová razítka, která se přidělují zachyceným paketům, odpovídali skutečnosti. Všechny časové údaje, které uSonda používá jsou v **UTC+0**.

Čas je možné nastavit 3 způsoby:

- **Manuální (Manually)** - Ruční nastavení data a času
- **NTP** - Čas se získá ze vzdáleného NTP serveru (vyžaduje funkční připojení k Internetu skrz port neoznačený port)
- **Automatické (Get from configuration PC)** - Použije se aktuální čas, který je nastaven na počítači, ze kterého se právě uSonda konfiguruje

Nastavení se provede stiskem tlačítka **Set time.**



Obrázek 4: Příklad manuálního nastavení data a času

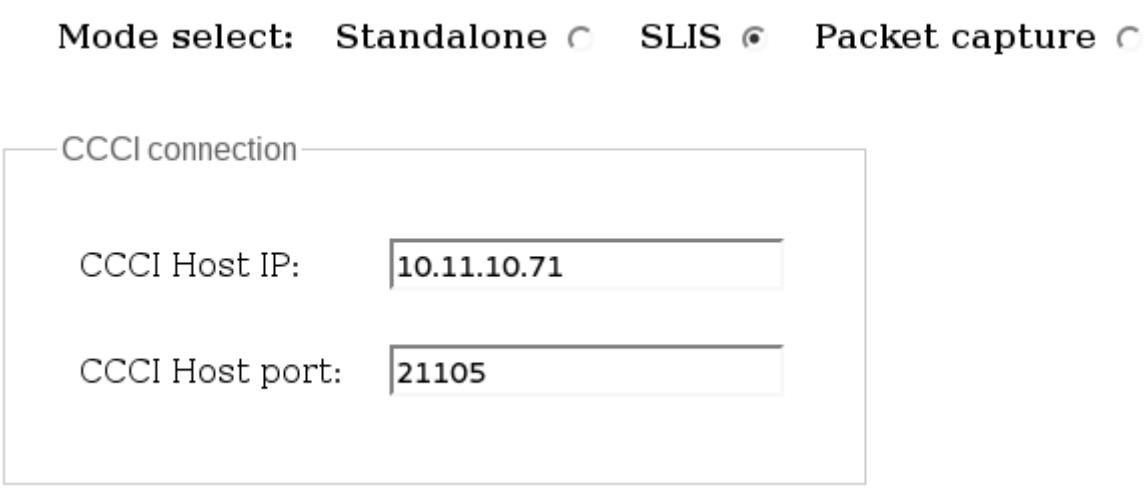
Konfigurace módu

uSonda lze nakonfigurovat do jednoho ze 3 režimů.

- **Standalone** - Zachycení komunikace, která odpovídá nakonfigurovaným filtrovacím pravidlům. Konfigurace filtrovacích pravidel se provádí přímo na uSondě.
- **SLIS** - uSonda se připojí k systému SLIS, na kterém jsou nakonfigurovány odposlechy. uSonda zachycená data odešle na zpracování zpět na server se SLISem.
- **Packet capture** - U zachycené komunikace neprobíhá filtrování a tedy veškerý zachycený síťový provoz je vyexportován na úložné zařízení.

Každý mód umožňuje export pomocí protokolů TCP a UDP. Direct export je možný použít pouze v režimu Standalone a Packet capture.

Konfigurace SLIS režimu



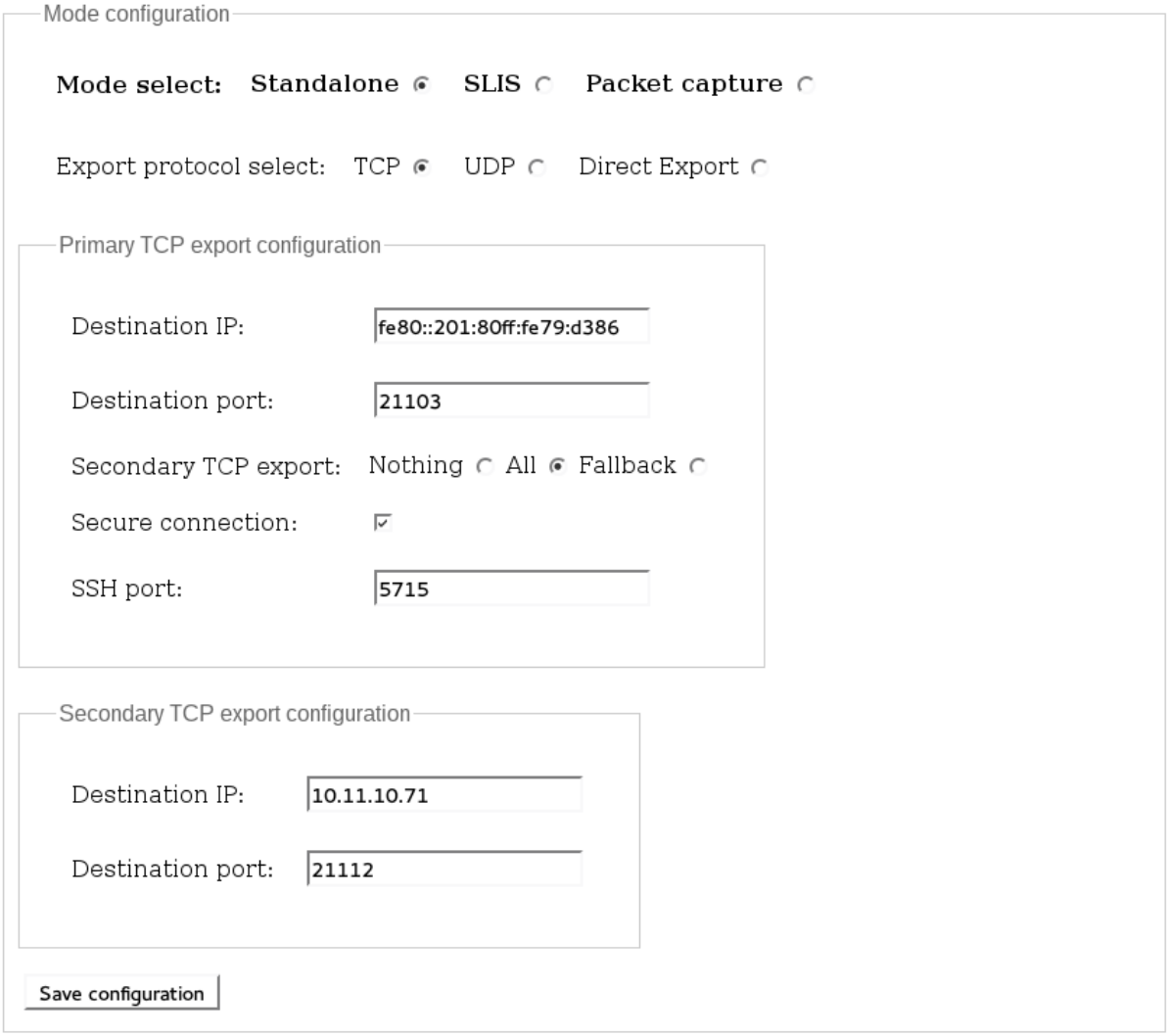
Obrázek 5: Úkázka nastavení režimu SLIS

V tomto režimu je zapotřebí nakonfigurovat spojení se systém SLIS.

CCCI connection - Toto spojení slouží pro získávání filtrovacích pravidel od systému SLIS

- CCCI Host IP - IP adresa, na které je SLIS přístupný
- CCCI Host port - TCP port, na kterém SLIS naslouchá pro příchozí spojení

Konfigurace TCP exportu



Obrázek 6: Úkázka nastavení pro komunikaci přes TCP

Primary TCP export configuration - Primární nastavení TCP exportu, kam bude zachycená komunikace odesílána

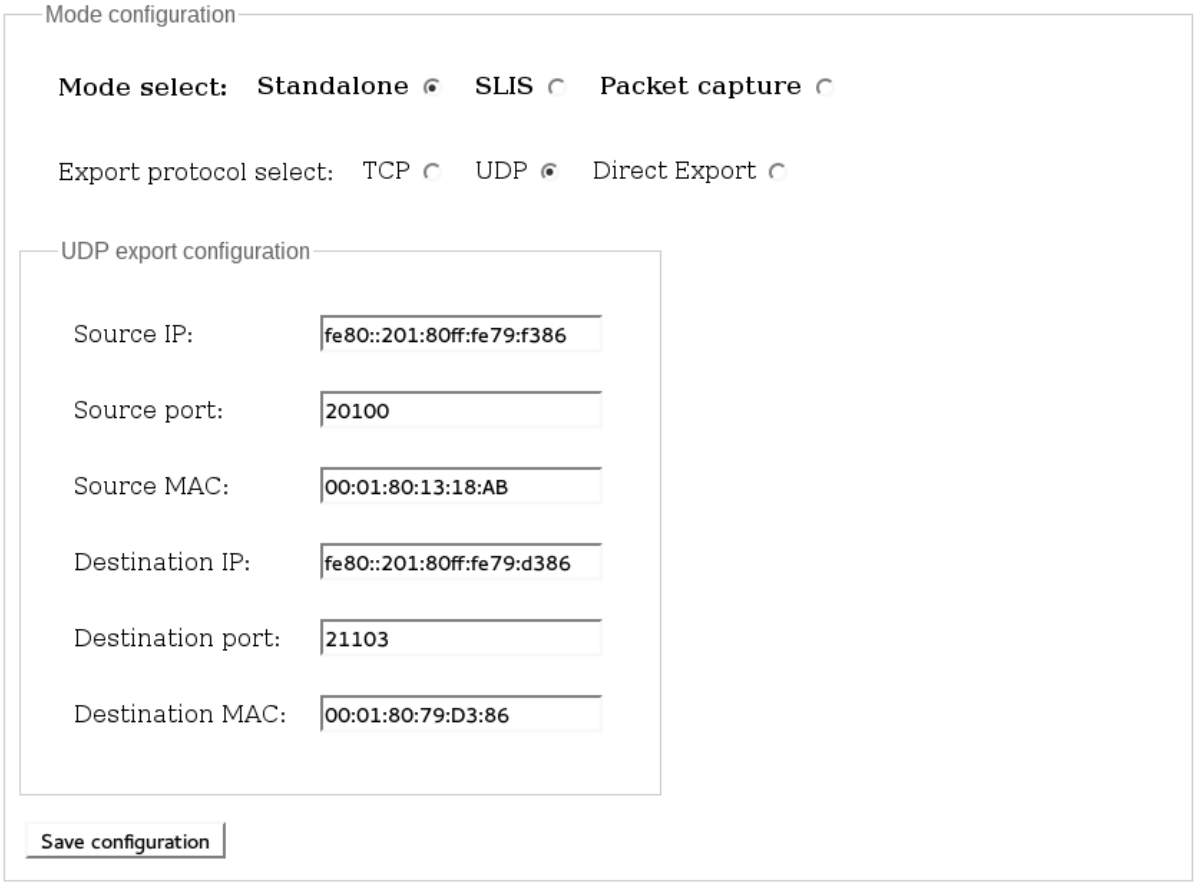
- Destination IP - IP adresa zařízení, které bude komunikaci ukládat
- Destination port - TCP port, na kterém ukládací zařízení naslouchá
- Secondary TCP export
  - Nothing - sekundární ukládání je vypnuto
  - All - kopie dat, které se zasílají do SLISu, jsou odeslána na nastavený HDD (konfigurace HDD exportu je stejná jako u režimu Standalone a Packet capture)
  - Fallback - na nastavený HDD se začnou odesílat zachycené rámce pouze pokud dojde ke ztrátě spojení s SLISem
- Secure connection - vytvoří zabezpečené spojení se serverem, na který se odesílají zachycená data

- Na serveru je potřeba mít uživatele **slis**
- Uživatel **slis** umožňuje vzdálené přihlášení pomocí SSH certifikátů
- Soubor */home/slis/.ssh/authorized_keys* obsahuje záznam s dodaným veřejným klíčem

Secondary TCP export configuration - Sekundární nastavení TCP exportu, kam bude zachycená komunikace odesílána (aktivace se odvíjí od nastavení *Secondary TCP export*

- Destination IP - IP adresa zařízení, které bude komunikaci ukládat
- Destination port - TCP port, na kterém ukládací zařízení naslouchá

Konfigurace UDP exportu



Obrázek 7: Úkázka nastavení pro komunikaci přes UDP

UDP export configuration

- Source IP - IP adresa, která bude ve výstupním paketu uvedena jako zdrojová
- Source port - UDP port, který bude ve výstupním paketu uveden jako zdrojový
- Source MAC - MAC adresa, která bude ve výstupním paketu uvedena jako zdrojová
- Destination IP - IP adresa zařízení, které bude komunikaci ukládat
- Destination port - UDP port, na kterém ukládací zařízení naslouchá
- Destination MAC - MAC adresa následujícího síťového zařízení, který leží na cestě k úložnému zařízení

Uložení výchozí konfigurace

Po zapnutí uSondy je vždy načtena výchozí konfigurace. Pro úpravu této konfigurace slouží tlačítko **Save active configuration as default** na stránce **Configure**. Po stisknutí tohoto tlačítka se uloží aktuálně používaná konfigurace jako výchozí.

Obrázek 8: Tlačítko pro uložení výchozí konfigurace

Nastavení odposlechů

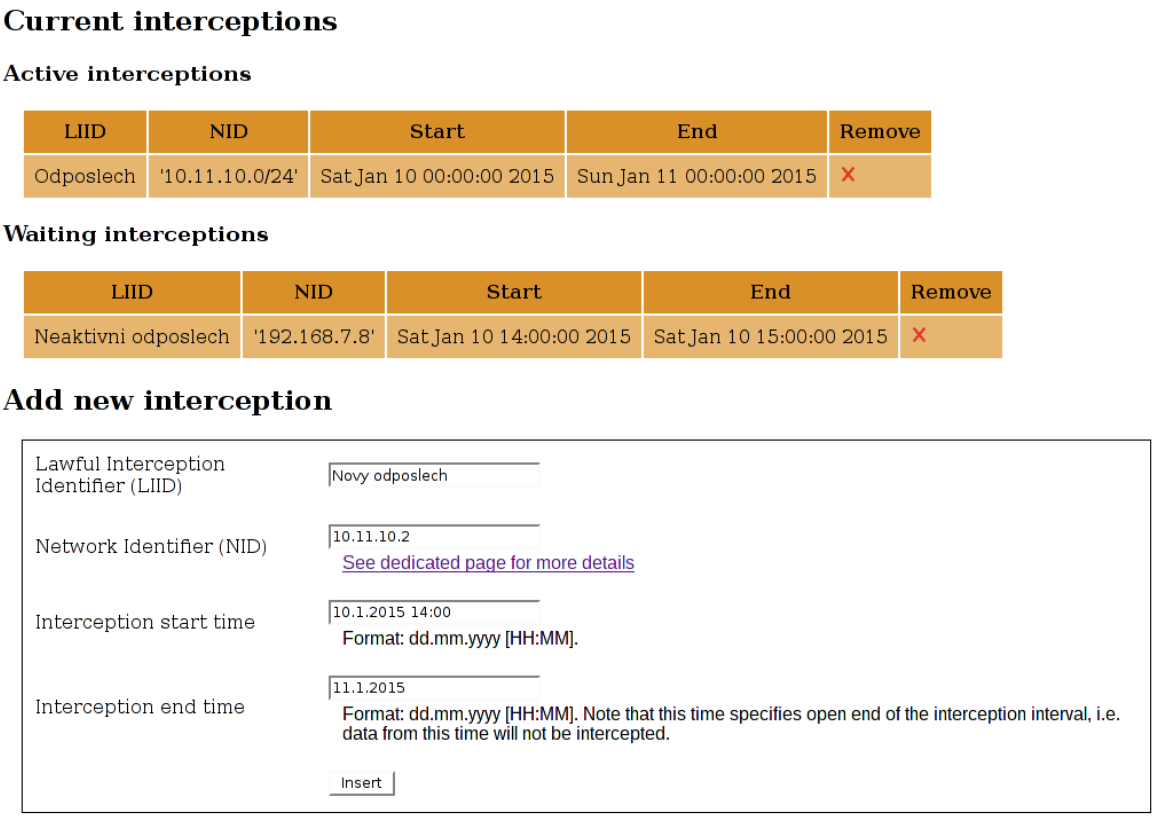
Nastavení odposlechů se provádí na stránce **Interceptions.**

Přidání odposlechu

- Lawful Interception Identifier - textový identifikátor odposlechu (nesmí se shodovat s již probíhajícími, či naplánovanými odposlechy)
- Network Identifier - IPv4/IPv6 adresa (případně rozsah zadaný pomocí masky) určující, které pakety budou zachyceny
- Interception start time - datum a čas, od kdy bude odposlech se zadanou IPv4/IPv6 adresou platný (formát dd.mm.rrrr [hh:mm])
- Interception end time - datum a čas, kdy zadané pravidlo pozbude platnosti a odposlech bude ukončen (formát dd.mm.rrrr [hh:mm])
- **Pozor**: předpokládá se čas zadaný v **UTC+0**

Odstranění odposlechu

- Nahoře na stránce s odposlechy je možné vidět aktivní odposlechy, případně odposlechy čekající na aktivaci, pro odstranění takového odposlechu stačí kliknout na ikonu křížku ve sloupci Remove



Obrázek 9: Ukázka nastavení odposlechů

Statistiky

Na stránce **Statistics** jsou dvě kategorie statistik:

Ethernet statistics - Informuje o počtu přijatých/odeslaných rámců

- Interface 0 = D
- Interface 1 = C
- Output Interface = A

Filter statistics - Udává počet paketů, které zpracovával filtr

- Allowed - počet paketů, které byly vyexportováný
- Denied - pakety, které byly vyfiltrovány
- Total - počet všech paketů, které vstoupily do filtru

Ethernet statistics

Interface 0	
Received bytes	76390
Received frames	1067
Send bytes	0
Send frames	0

Interface 1	
Received bytes	60650592480
Received frames	882538637
Send bytes	0
Send frames	0

Output interface	
Received bytes	0
Received frames	0
Send bytes	60653038893
Send frames	882575286

Filter statistics

Interface 0	
Allowed	1067
Denied	0
Total	1067

Interface 1	
Allowed	882613410
Denied	0
Total	882613410

Obrázek 10: Ukázka statistik

LED diody na čelním panelu

LED	Funkce
0	uSonda je nastavena
1	uSonda se nastavuje
2	uSonda je nastavena
3	uSonda se nastavuje
4	uSonda je nastavena
5	uSonda se nastavuje
6	uSonda je nastavena
7	uSonda se nastavuje
8	uSonda je nastavena
9	uSonda se nastavuje

Tlačítko na čelním panelu

Při podržení tlačítka cca 10s dojde k restartování uSondy.

Zachycení dat z uSondy

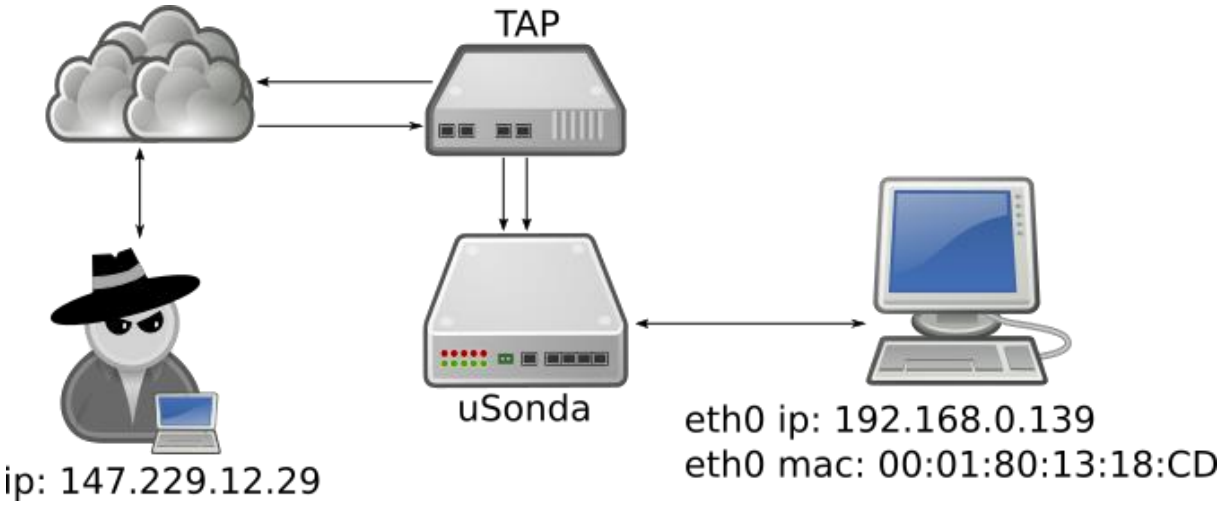
Pokud je export uSondy nastaven v režimu Direct export, je možné na rozhraní **A** připojit PC a pomocí Wiresharku zobrazit/uložit rámce, které uSonda exportuje. Pro lepší zobrazení a analýzu zachycených paketů je možno využít také plug-in o programu Wireshark. Dostupný je zde: http://www.fit.vutbr.cz/research/view_product.php?id=398

Příklady použití

Použité nástroje:

- uSonda verze 1.2
- PC+Linux
- Wireshark 1.12 (https://www.wireshark.org/)
    - INI3 plugin (http://www.fit.vutbr.cz/research/prod/index.php?id=398)
    - INI3SEQ plugin (http://www.fit.vutbr.cz/research/prod/index.php?id=398)
- INI3 dump (http://www.fit.vutbr.cz/research/prod/index.php?id=398)

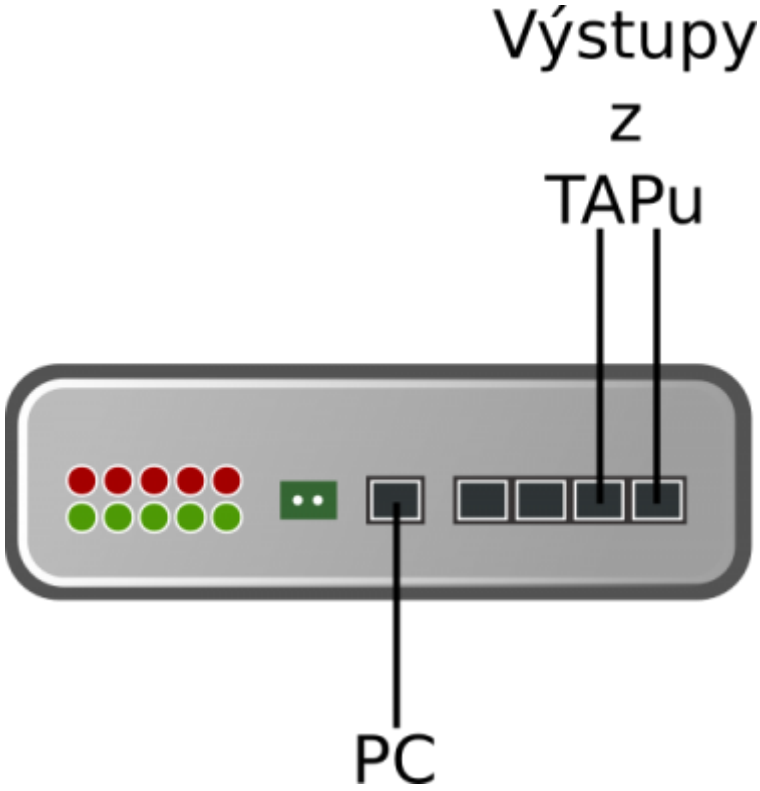
Topologie



Obrázek 11: Topologie sítě

Příklad 1 - zachycení veškeré komunikace, export přes TCP

V tomto příkladu bude ukázáno jak zachytit veškerý provoz, který je do uSondy poslán. Provoz bude uložen na připojeném počítači ve formě pcapu včetně INI3 hlaviček. Export bude prováděn za použití TCP.

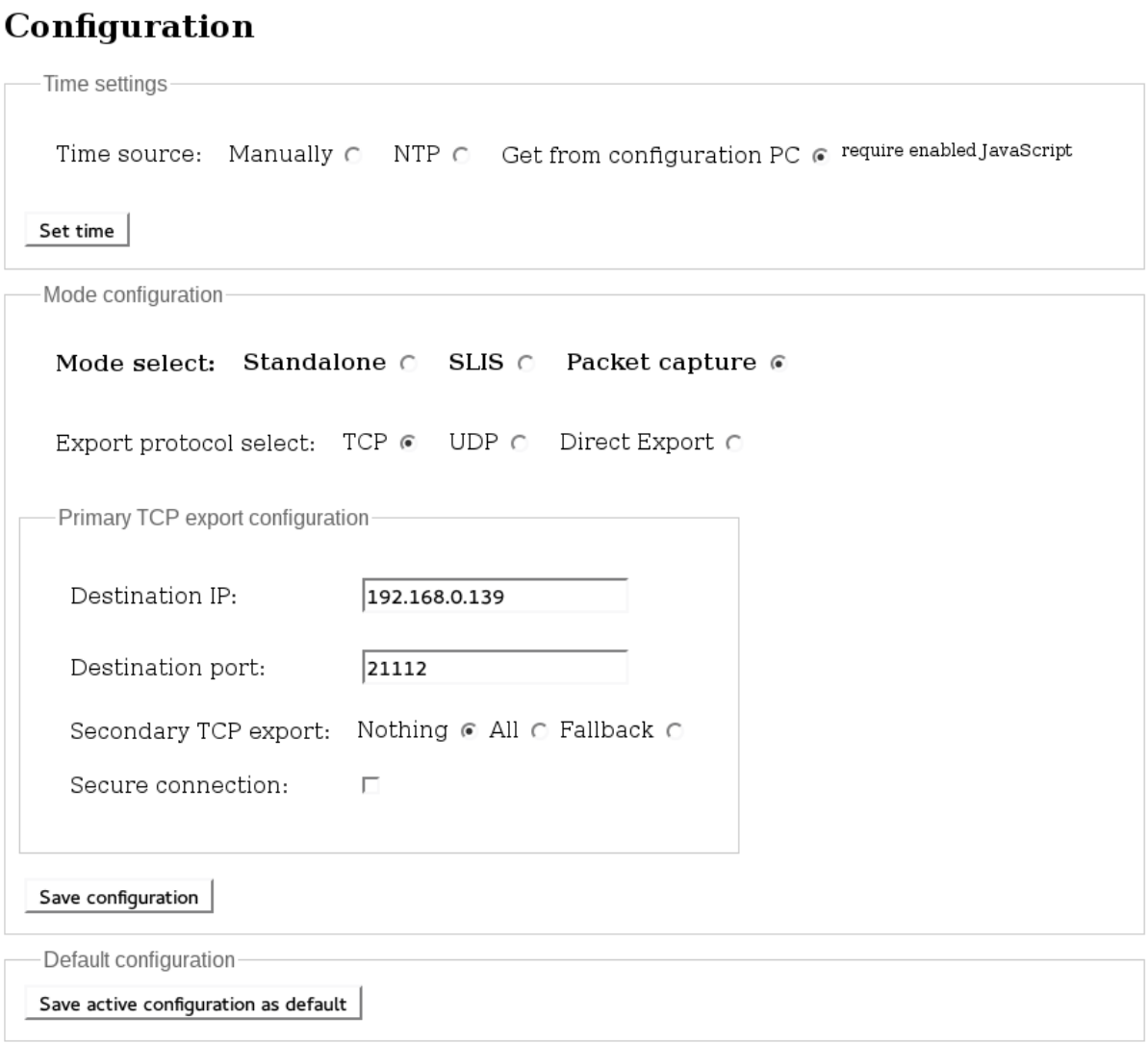


Obrázek 12: Zapojení uSondy

Konfigurace

Po zapnutí uSondy se připojíme na webové rozhraní. Na stránce **Configuration** pokud není vybráno **Get from configuration PC**, tak ho zvolíme a klikneme na tlačítko **Set time**. Nyní je na uSondě nastaven aktuální čas.

Stále na stránce **Configuration** v sekci **Mode configuration** zvolíme **Packet capture**. Tato volba zajistí, exportování veškeré příchozí komunikace. Aby bylo možné navázat TCP spojení s PC, na kterém bude síťový provoz uložen, Export protokol vybereme TCP. Do pole **Destination IP** vložíme 192.168.0.139 a **Destination port** nastavíme na 21112. Secondary TCP export a SSH tunelovaní necháme vypnuté. Nyní klikneme na tlačítko **Save configuration**.



Obrázek 13: Nastavení uSondy

Export do PCAPu

Na konfiguračním stroji spustíme nástroj ini3_dump:

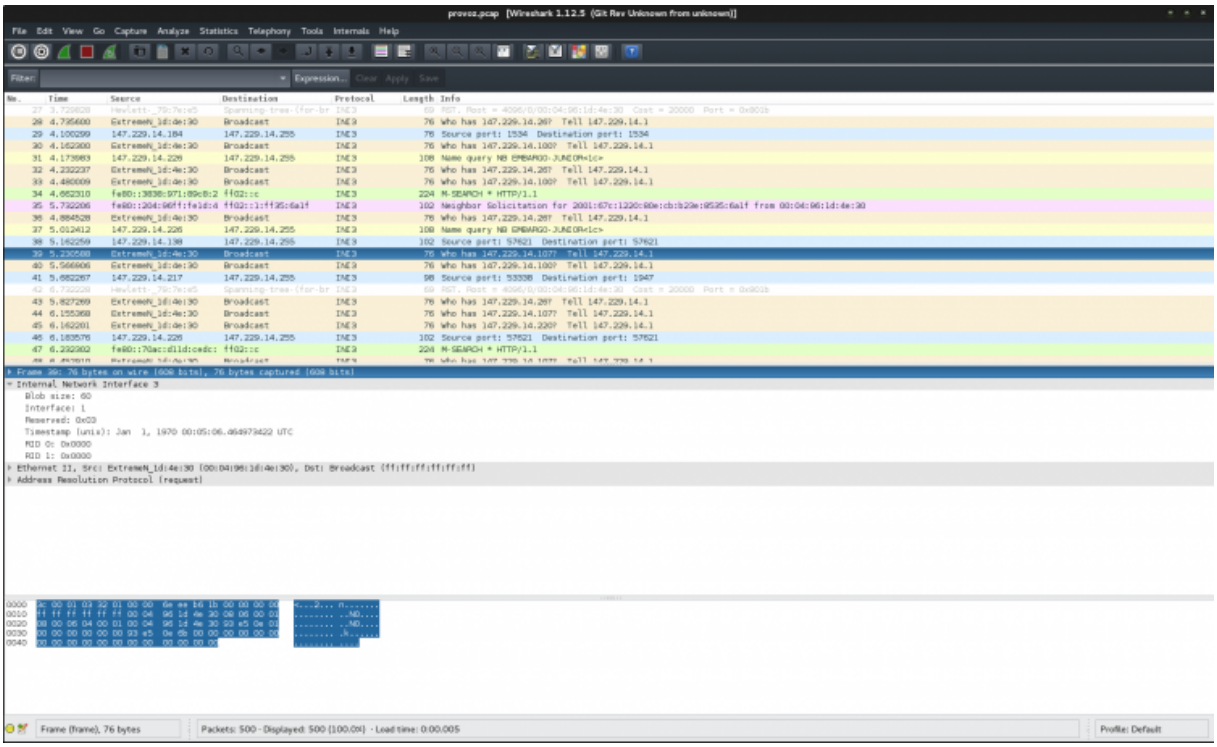
```
./ini3_dump -p 21112 -f provoz
```

Parametr -p aktivuje příjem zachycené komunikace z uSondy na TCP portu 21112 (tento port byl nastaven v konfiguraci uSondy). Parametr -f zajistí, že komunikace bude uložena do souboru *provoz.pcap*. Když máme odchycen dostatek paketů, aplikaci ukončíme stisknutím Ctrl+C.

Prozkoumání zachycené komunikace

Protože zachycená komunikace je uložena včetně INI3 hlaviček není možné tento pcap otevřít běžnými nástroji. Pro tento případ byl vytvořen plugin do Wiresharku, který umožňuje takto vytvořený soubor otevřít a zpracovat. Pokud je již ve Wiresharku plugin nainstalován, soubor stačí přímo otevřít bez dalších kroků.

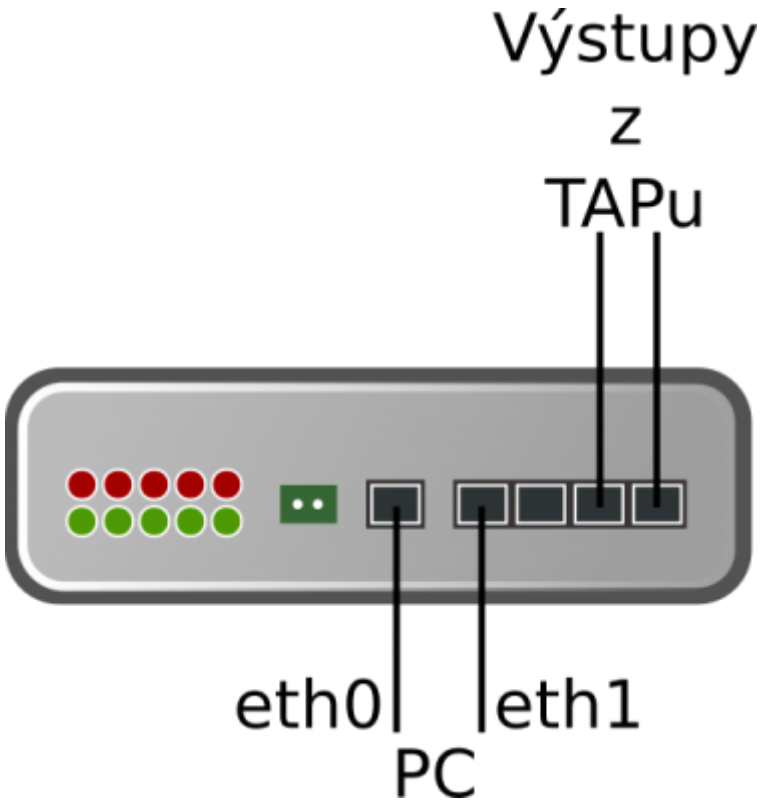
Při vybrání libovolného paketu lze v podrobnostech vidět jednotlivé položky INI3 hlavičky následovaný původním rámcem.



Obrázek 14: Screenshot wiresharku se zachycenými daty

Příklad 2 - zachycení konkrétní IP

V tomto případě bude uložen jen vybraný provoz, který bude určen IP adresou odposlouchávaného. Zachycená komunikace bude exportována v protokolem **Direct export**.

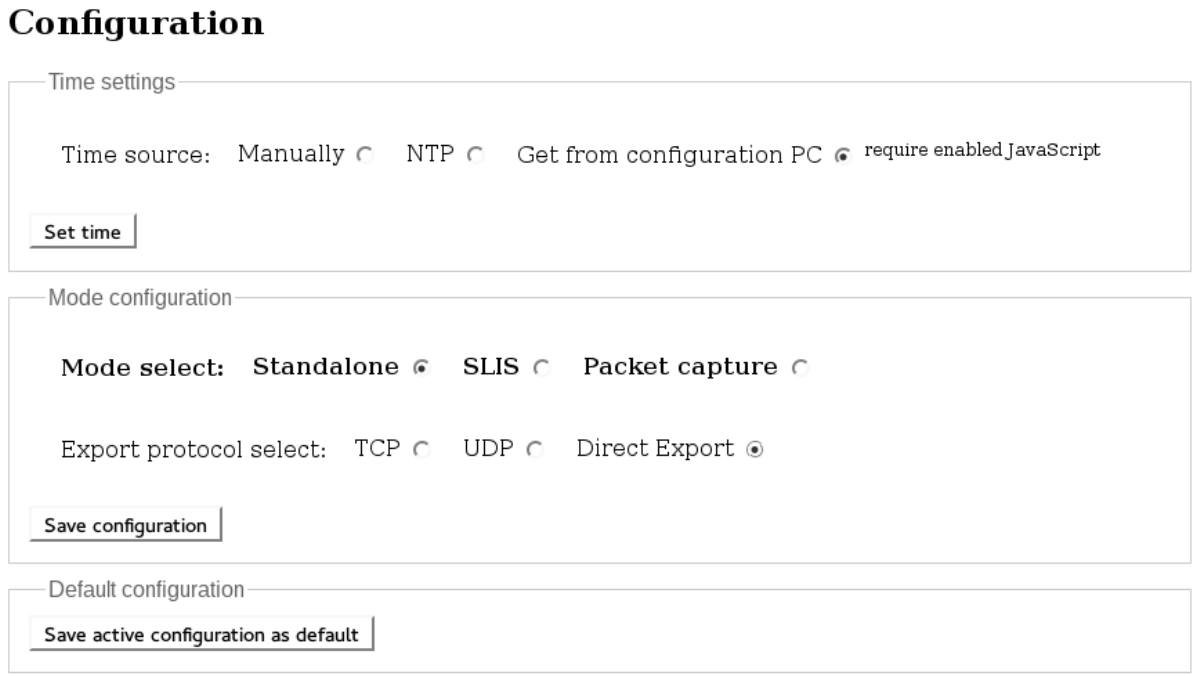


Obrázek 15: Zapojení uSondy

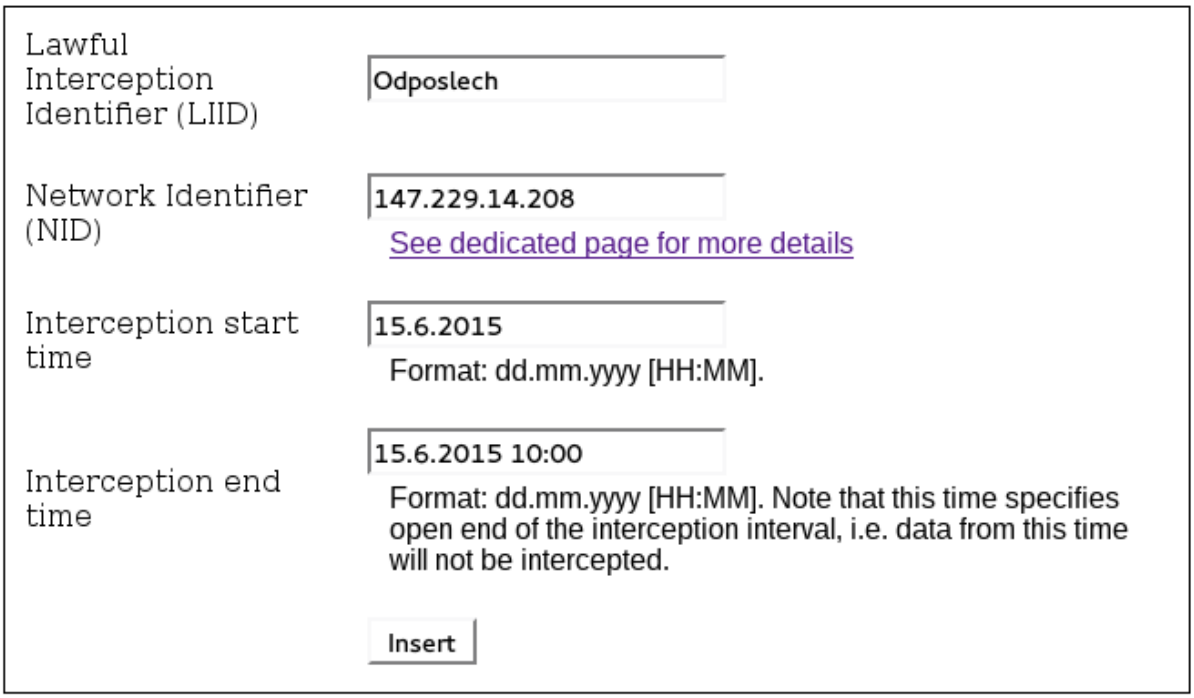
Konfigurace

Po zapnutí uSondy se připojíme na webové. Na stránce **Configuration** pokud není vybráno **Get from configuration PC**, tak ho zvolíme a klikneme na tlačítko **Set time**. Nyní je na uSondě nastaven aktuální čas.

Stále na stránce **Configuration** v sekci **Mode configuration** zvolíme **Standalone**. Tato volba zajistí, exportování pouze takové komunikace, která je nastavena. **Export protocol** bude **Direct export**. Nyní klikneme na tlačítko **Save configuration**.



Obrázek 16: Nastavení uSondy



Obrázek 17: Nastavení odposlechu na uSondě

Export do PCAPu

Na konfiguračním stroji spustíme nástroj ini3_dump:

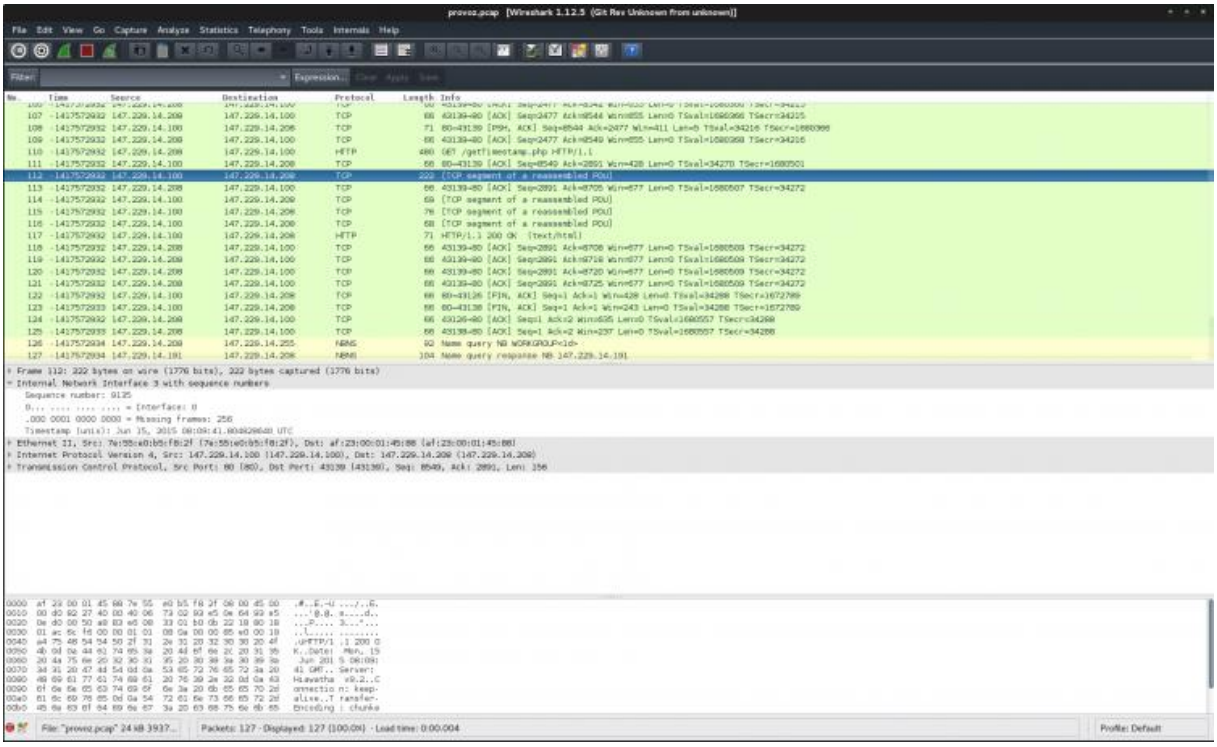
```
./ini3_dump -d eth1 -f provoz
```

Parametr -d aktivuje ukládání všech paketů, které přijdou na rozhraní eth1. Předpokládá se, že uSonda je přímo připojen k PC (bez použití switche/routeru). Parametr -f zajistí, že komunikace bude uložena do souboru *provoz.pcap*. Když máme odchycen dostatek paketů, aplikaci ukončíme stisknutím Ctrl+C.

Prozkoumání zachycené komunikace

V režimu **Direct export** jsou exportované pakety mírně upraveny, tak že původní MAC adresy jsou přepsány speciální INI3 hlavičkou (detailně viz dokumentace uSondy). I když je teoreticky možné vytvořený soubor otevřít normálními nástroji, které pracují s PCAP soubory, doporučuje se zkoumat soubor otevřený ve Wiresharku s pluginem INI3SEQ. Pokud je již ve Wiresharku plugin nainstalován, soubor stačí přímo otevřít bez dalších kroků.

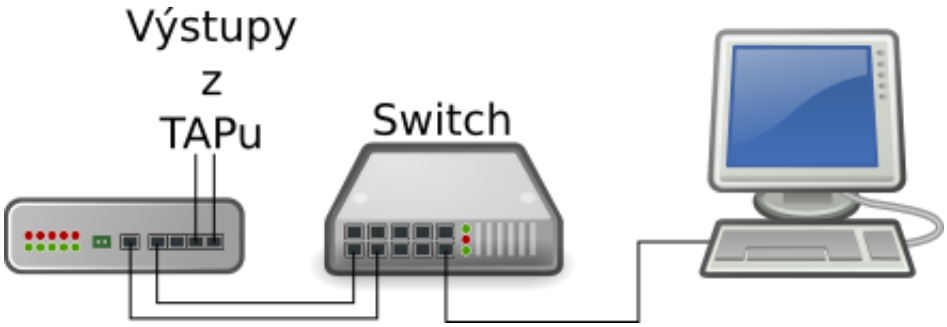
Při vybrání libovolného paketu lze v podrobnostech vidět jednotlivé položky INI3 hlavičky následovaný původním rámcem.



Obrázek 18: Screenshot wiresharku se zachycenými daty

Příklad 3 - zachycení veškeré komunikace, export přes UDP

V tomto příkladu bude ukázáno jak zachytit veškerý provoz, který je do uSondy poslán. Provoz bude uložen na připojeném počítači ve formě pcapu **bez** INI3 hlaviček. Export bude prováděn za použití UDP.

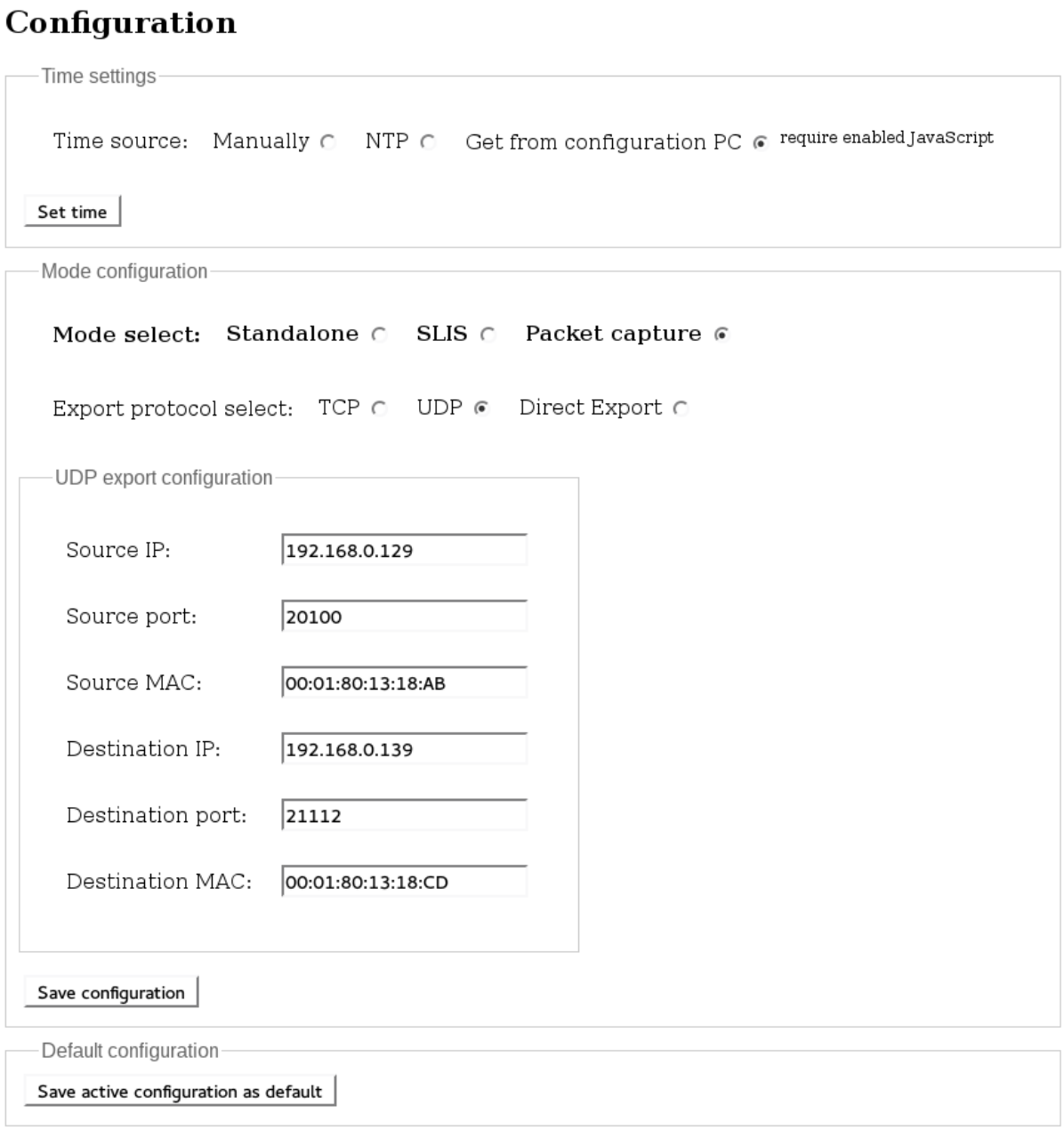


Obrázek 19: Zapojení uSondy

Konfigurace

Po zapnutí uSondy se připojíme na webové rozhraní. Na stránce **Configuration** pokud není vybráno **Get from configuration PC**, tak ho zvolíme a klikneme na tlačítko **Set time**. Nyní je na uSondě nastaven aktuální čas.

Stále na stránce **Configuration** v sekci **Mode configuration** zvolíme **Packet capture**. Tato volba zajistí, exportování veškeré příchozí komunikace. **Export protocol** bude UDP. Jednotlivá pole nastavíme stejně jako na obrázku a konfiguraci uložíme.



Obrázek 20: Nastavení uSondy

Export do PCAPu

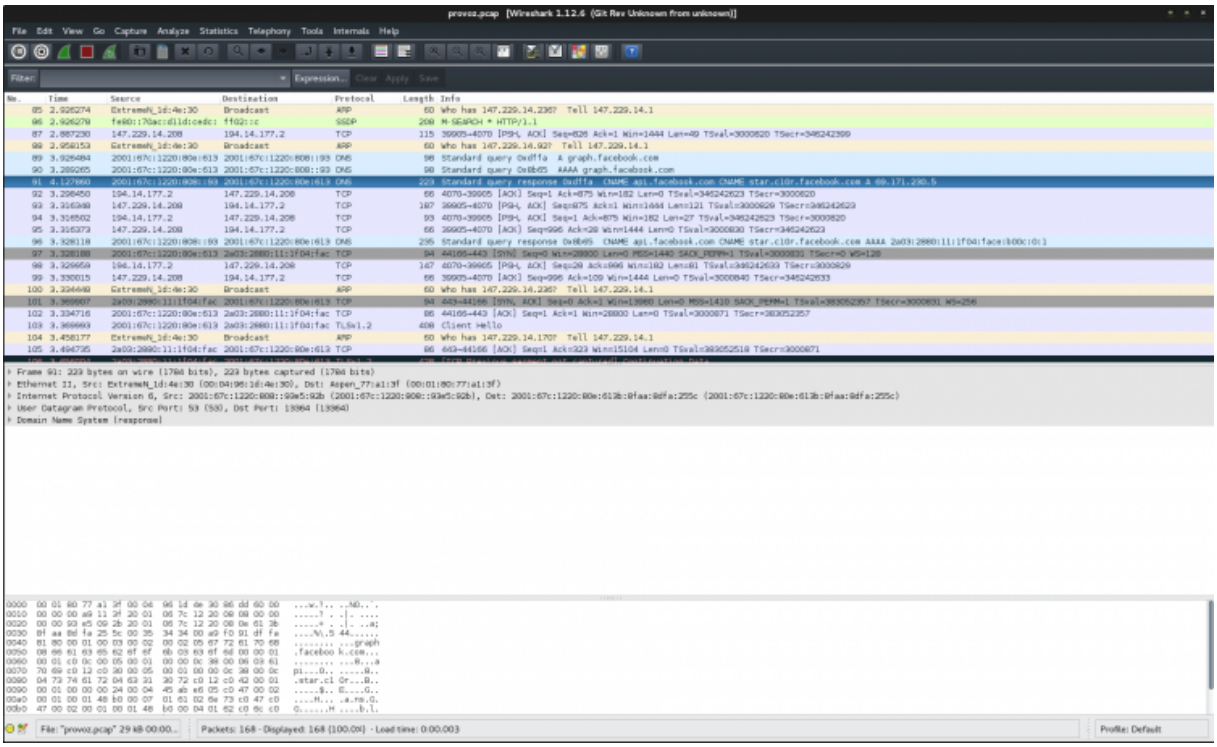
Na konfiguračním stroji spustíme nástroj ini3_dump:

```
./ini3_dump -u -p 21122 -f provoz -m
```

Kombinace Parametrů -u a -p aktivuje příjem zachycené komunikace z uSondy na UDP portu 21122 (tento port byl nastaven v konfiguraci uSondy). Parametr -f zajistí, že komunikace bude uložena do souboru *provoz.pcap*. Parametr -m zapíná oříznutí INI3 hlaviček a tedy vytváří standardní PCAP soubor. Když máme odchycen dostatek paketů, aplikaci ukončíme stisknutím Ctrl+C.

Prozkoumání zachycené komunikace

Soubor *provoz.pcap* normální soubor typu PCAP a tedy je možné jej otevřít běžně dostupnými nástroji, jako je například Wireshark.



Obrázek 21: Screenshot wiresharku se zachycenými daty