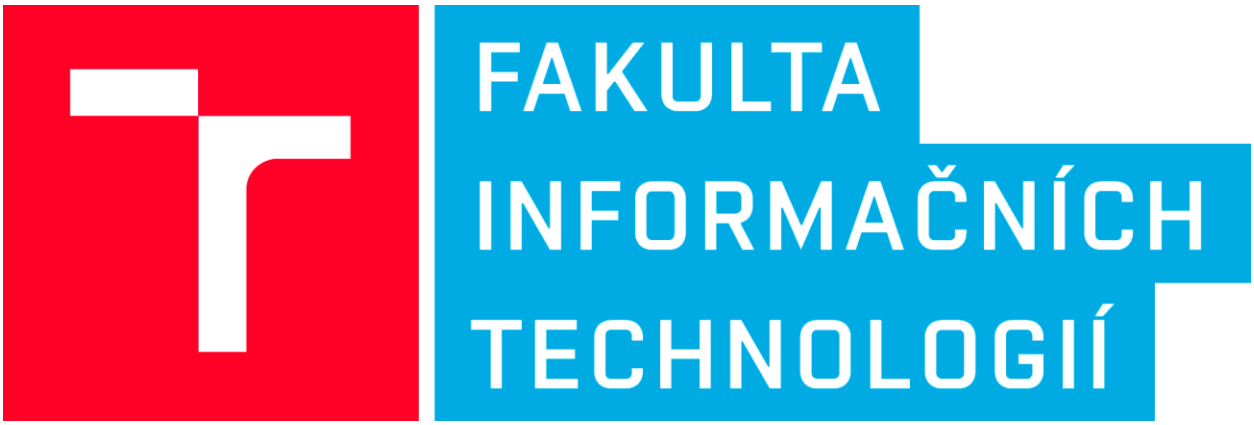
Dokumentace k projektu do předmětu ISA

Programování síťové služby

Jednoduchý monitorovací nástroj protokolů CDP a LLDP



Autor: Jan Pavlica
Login: xpavli78
Datum: 20. 11. 2016

1 OBSAH

2 ÚVOD

3 ANALÝZA PROBLÉMU

3.1 Zadání

Cílem projektu bylo vytvořit program, jež bude schopen zachytávat a analyzovat protokoly pro management sítě na druhé vrstvě na konkrétním zařízení. Jednalo se konkrétně o protokoly Cisco Discovery Protocol (dále jen CPD) a Link-Layer Discovery Protocol (dále jen LLDP). Program má za úkol nejen analyzovat zachycené packety zmíněných protokolů nýbrž i pravidelně odesílat konfigurovatelné oznámení.

3.2 Cisco Discovery Protocol

Protokol CDP je protokolem druhé vrstvy ISO/OSI modelu. Jedná se o protokol používaný výhradně síťovými prvky firmy Cisco Systems. Slouží ke sdílení informací o ostatních přímo připojených zařízeních. Nejvíce se používá s Ethernetem IEEE 802.3. V sítích IEEE 802 je závislý na mezivrstvě LLC se SNAP hlavičkou. Program pracuje pouze s tímto typem, ačkoliv CDP lze použít na linkových vrstvách Cisco HDLC nebo PPP.

Samotnému CDP packetu předchází transportní protokol, který má velikost 22 bytů. Jeho struktura je popsána níže na obrázku. Informace v ní použijeme pro filtrování packetů.

IEEE 802.3			802.2 LLC hlavička			SNAP rozšíření	
Cílová MAC	*Zdrojová MAC*	*Délka*	*DSAP*	*SSAP*	*Control*	*OUI*	*Protocol ID*
6B	6B	2B	1B	1B	1B	3B	2B
01-00-0C-CC-CC-CC	Zdrojová MAC	Délka	AA	AA	3	00000C	2000

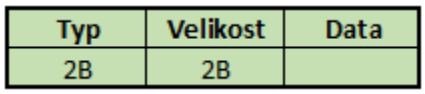
Obrázek 1 Transportní protokol pro CDP

CDP packet obsahuje povinná pole s verzí protokolu, dobou platnosti (TTL) a kontrolním součtem následována TLV záznamy.

Verze CDP	Doba platnosti	Kontrolní součet	TLV záznamy
1B	1B	2B	

Obrázek 2 Struktura CDP packetu

Type-length-value položky jsou rozepsány v následující tabulce. Pole *Type* a *Length* mají konstantní velikost a to 2 byty každá.



Obrázek 3 Struktura TLV záznamu u CDP

TLV	Typ	Popis
Device-ID	0x0001	Obsahuje jméno zařízení.
Address	0x0002	Seznam adres zařízení.
Port-ID	0x0003	Identifikace portu.
Capabilities	0x0004	Popisuje vlastnosti a funkce zařízení.
Version	0x0005	Verze softwaru, který běží na zařízení.
Platform	0x0006	Popisuje hardwarovou platformu.
IP Network Prefix	0x0007	Obsahuje IP prefixy adres.
VTP Management Domain	0x0009	Jméno pro VTP.
Native VLAN	0x000A	Indikuje předpokládaný VLAN pro neoznačené packety.
Full/half Duplex	0x000B	Popisuje, zda je zařízení full nebo half duplexní.

Tabulka 1 Seznam TLV záznamů pro CDP

3.3 Link-Layer Discovery Protocol

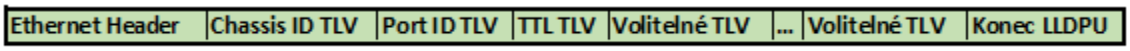
LLDP je stejně jako CDP protokol linkové vrstvy. Výhodou je, že je standardizován (IEEE 802.1AB-2009 a IEEE 802.3-2012) a je tedy využíván mnoha výrobci. Stejně jako CDP protokol odesílá informace okolním připojeným zařízením. Na rozdíl do CDP není třeba využívat LLC a SNAP, jelikož je možné specifikovat protokol v Ethernetovém rámci.

Ethernetová hlavička LLDP paketu má velikost 14 bytů a obsahuje jako cílovou MAC adresu speciální multicastovou adresu, která není přeposílána MAC mosty. Nejvíce používanou cílovou adresou je 01-80-C2-00-00-0E. Dále hlavička obsahuje MAC adresu odesílatele a položku typu Ethernetu, která pro LLDP pakety vždy nabývá hodnoty 88-CC.

Cílová MAC	*Zdrojová MAC*	*Ethernet Type*
6B	6B	2B
01-80-C2-00-00-0E	Zdrojová MAC	88-cc

Obrázek 4 Ethernetová hlavička u LLDP

Za hlavičkou následují data LLDP packetu složené z TLV položek z nichž 4 jsou povinné. Jedná se o první 3 a poslední ukončující. Konkrétně pak *Chassis ID*, *Port ID* a *TTL* na začátku a označení *konce LLDPU* na konci. Mezi těmito položkami může být opět libovolné množství TLV záznamů.



Obrázek 5 Struktura LLDP packetu

Na rozdíl od CDP TLV záznamů, kde zabírá pole *Type* a *Length* pouze 2 byty dohromady. Konkrétně pole *Type* zabírá 7 bitů a pole *Lenght* 9 bitů. To je pak následováno samotnými daty vázajícími se k danému TLV záznamu.

Typ	Velikost	Data
7 bitů	9 bitů	

Obrázek 6 Struktura TLV záznamu u LLDP

Seznam TVL položek:

- Chassis ID TLV (Type = 1)
- Port ID TLV (Type = 2)
- Time To Live TLV (Type = 3)
- End of LLDPDU TLV (Type = 0)
- Port Description TLV (Type = 4)
- System Name TLV (Type = 5)
- System Description TLV (Type = 6)
- System Capabilities TLV (Type = 7)
- Management Address TLV (Type = 8)

4 ŘEŠENÍ PROBLÉMU

4.1 Analýza packetů

Při implementaci byla použita knihovna `libpcap`. Pro získávání packetů je použit následující filtr

(ether[12:2] <= 1500 && ether[14:2] == 0xAAAA && ether[16:1] == 0x03 && ether[17:2] == 0x0000 && ether[19:1] == 0x0C && ether[20:2] == 0x2000) or ether proto 0x88cc

Modrá část slouží pro filtrování CDP packetů a hnědá pro LLDP packety. Jádrem je pak cyklus while, který obsahuje funkci `pcap_next_ex` ze zmiňované knihovny. V případě zachycení packetu jsou data přeposlána do funkce pro její vytisknutí. Třídění dat probíhá ve switchi.

4.2 Odesílání packetů

V případě, že je požadováno odesílání packetů dojde k odeslání prvotních CDP a LLDP oznámení, a pak jejich opakované odesílání v intervalech 30 vteřin pro LLDP a 60 vteřin pro CDP. Abych se vyhnul vytváření nových procesů nebo vláken porovnávám čas s kontrolním a pokud je překročen požadovaný interval je odeslán packet za pomocí `raw socket`.

5 TESTOVÁNÍ

K testování bylo použito programu ***mausezahn*** pro generování CDP packetů a ***lldpd*** pro zasílání LLDP packetů. Dále byly odchyceny packety po přehrání pcap souborů programem *tcpreplay*. Výstupy všech zachycených packetů byly porovnány s výstupy aplikace *Wireshark*.

6 POUŽITÍ PROGRAMU

Program je třeba pouštět s patřičným oprávněním. Samotné spuštění probíhá následovně.

./myL2monitor -i <rozhraní> {--send-hello {--ttl <sekundy>} {--duplex [full|half]} {--software-version <verze>} {--device-id <identifikátor>} {--platform <platforma>} {--port-id <rozhraní>} {--capabilities <integer>} {--address <IPv4>}}

Význam parametrů a jejich hodnot:

- *-i <rozhraní>*: Povinný parametr. Specifikuje lokální identifikátor rozhraní v operačním systému (např. eth0), na kterém bude aplikace naslouchat a případně odesílat zprávy;
- *--send-hello*: Volitelný parametr. Pokud přítomen tento parametr není, tak aplikace jen naslouchá na rozhraní a vypisuje obsahy CDP a LLDP zpráv. Pokud je přítomen, tak aplikace i pravidelně generuje CDP oznámení, přičemž obsah TLV políček je specifikován následujícími volitelnými parametry.
- *--ttl <sekundy>*: Volitelný parametr, výchozí číselná hodnota 180s.
- *--duplex [full|half]*: Volitelný parametr, může nabývat dvou řetězcových hodnot, a to "half" či "full", výchozí hodnota odpovídá full-duplexnímu označení vlastnosti rozhraní.
- *--platform <platforma>*: Volitelný parametr, výchozí řetězcová hodnota bude odpovídat výstupu příkazu "uname" na spouštěném OS.
- *--software-version <verze>*: Volitelný parametr, výchozí řetězcová hodnota bude odpovídat výstupu příkazu "uname -a" na spouštěném OS.
- *--device-id <identifikátor>*: Volitelný parametr, výchozí řetězcová hodnota bude odpovídat výstupu příkazu "hostname" na spouštěném OS.
- *--port-id <rozhraní>*: Volitelný parametr, výchozí řetězcová hodnota bude odpovídat hodnotě parametru *-i <rozhraní>*.
- *--capabilities <integer>*: Volitelný parametr, výchozí číselná hodnota bude odpovídat Host capability ze specifikací.
- *--address <IPv4>*: Volitelný parametr, výchozí hodnota přijde do TLV Addresses, kde se očekává právě jedna (primární) IPv4 rozhraní specifikovaného parametrem *-i <rozhraní>*.

7 ZÁVĚR

Při řešení projektu se nevyskytl závažnější komplikace. Snažil jsem se splnit všechny požadavky vyplívající ze specifikace zadání. Aplikace nepodporuje některé podtypy či neformátuje jejich hodnoty do smysluplné podoby. Nicméně všechny důležité a často používané podtypy jsou zpracovány. Aplikace byla vyvíjena na operačním systému Linux Ubuntu 16.04.

8 LITERATURA

Cisco Discovery Protocol (CDP). *The Wireshark Wiki* [online]. 2013-05-0 [cit. 2016-11-20]. Dostupné z: https://wiki.wireshark.org/CDP

Link Layer Discovery Protocol (LLDP, IEEE 802.1AB). *The Wireshark Wiki* [online]. 2014 [cit. 2016-11-20]. Dostupné z: https://wiki.wireshark.org/LinkLayerDiscoveryProtocol

Filtering LLDP and CDP packets with Wireshark. *It must be the network.*. [online]. 2016-4-8 [cit. 2016-11-20]. Dostupné z: https://subnetwork.me/2011/04/08/filtering-lldp-and-cdp-packets-with-wireshark/

LLDP a CDP aneb kde se v síti schovává tučňák. *Root.cz* [online]. 2014-10-1, **2014**(10) [cit. 2016-11-20]. ISSN 1212-8309. Dostupné z: https://www.root.cz/clanky/lldp-a-cdp-aneb-kde-se-v-siti-schovava-tucnak/

CDP Implemantation: Final Report. *The Computer Communication Lab (236340)* [online]. 2003 [cit. 2016-11-20]. Dostupné z: http://www.cs.technion.ac.il/Courses/Computer-Networks-Lab/projects/spring2003/cdp2/web_cdp2/web_cdp2/cdp2_report.htm

IIE 802.2 LLC [online]. [cit. 2016-11-20]. Dostupný z WWW: http://standards.ieee.org/getieee802/download/802.1AB-2005.pdf

Cisco Discovery Protocol Version 2. *Cisco* [online]. 2016-6-3 [cit. 2016-11-20]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cdp/configuration/15-mt/cdp-15-mt-book/nm-cdp-discover.html

9 PŘÍLOHY

9.1 Výstup CDP packetu

```
root@izolacezmleka:/home/izolacezmleka/skola/5_semestr/ISA# ./myL2monitor -i wlp2s0
wlp2s0
*****************************************************
                        CDP
*****************************************************
Dest MAC Address : 01:00:0c:cc:cc:cc
Source MAC Address : aa:bb:cc:00:01:30
Verze: 2
Time to live: 180
Checksum: 34945
Device name: MUNI
Version: Cisco IOS Software, Linux Software (I86BI_LINUX-ADVENTERPRISEK9-M), Version 15.4(2)T4,
DEVELOPMENT TEST SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Thu 08-Oct-15 21:21 by prod_rel_team
Platform: Linux Unix
Address:
        Address count: 1
                Protocol type: NLPID
                Protocol field length: 1
                Protocol: IP
                IP address: 192.168.13.1
Port-ID: Ethernet0/3
Capabilities: 00000000000000000000000000000101
        ........ ........ ........ .......1 - Is a Router
        ........ ........ ........ ......0. = Not a Transparent Bridge
        ........ ........ ........ .....1.. = Is a Source Route Bridge
        ........ ........ ........ ....0... = Not a Switch
        ........ ........ ........ ...0.... = Not a Host
        ........ ........ ........ ..0..... = Not IGMP capable
        ........ ........ ........ .0...... = Not a Repeater
IP prefixes:
        147.251.1.0/24
        147.251.2.0/24
        172.16.3.0/24
        172.16.23.0/30
        172.16.23.4/30
        172.16.23.8/30
Duplex: Half

*****************************************************
                       LLDP
*****************************************************
Dest MAC Address : 01:80:c2:00:00:0e
Source MAC Address : aa:bb:cc:00:01:30
Protocol : 0x88cc
Chassis ID:     MAC Address : aa:bb:cc:00:01:00
Port-ID: Et0/3
Time to live: 120
System name: MUNI
System desription: Cisco IOS Software, Linux Software (I86BI_LINUX-ADVENTERPRISEK9-M), Version 1
5.4(2)T4, DEVELOPMENT TEST SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
```

9.2 Výstup LLDP packetu

```
*******************************************************
                        LLDP
*******************************************************
Dest MAC Address : 01:80:c2:00:00:0e
Source MAC Address : aa:bb:cc:00:01:30
Protocol : 0x88cc
Chassis ID:     MAC Address : aa:bb:cc:00:01:00
Port-ID: Et0/3
Time to live: 120
System name: MUNI
System desription: Cisco IOS Software, Linux Software (I86BI_LINUX-ADVENTERPRISEK9-M), Version 1
5.4(2)T4, DEVELOPMENT TEST SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Thu 08-Oct-15 21:21 by prod_rel_te
Port desription: Ethernet0/3
Capabilities:
        Capabilities: 0000000000010100
                ........ .......0 - Other: Not Capable
                ........ ......0. - Repeater: Not Capable
                ........ .....1.. = Bridge: Capable
                ........ ....0... = WLAN access point:: Not Capable
                ........ ...1.... = Router: Capable
                ........ ..0..... = Telephone: Not Capable
                ........ .0...... = DOCSIS cable device: Not Capable
                ........ 0....... = Station only: Not Capable
        Capabilities enabled: 0000000000010000
                ........ .......0 - Other: Not Enabled
                ........ ......0. - Repeater: Not Enabled
                ........ .....0.. = Bridge: Not Enabled
                ........ ....0... = WLAN access point:: Not Enabled
                ........ ...1.... = Router: Enabled
                ........ ..0..... = Telephone: Not Enabled
                ........ .0...... = DOCSIS cable device: Not Enabled
                ........ 0....... = Station only: Not Enabled
Management Address
         Address String Length: 5
         Address Subtype: IPv4 (1)
         Management Address: 192.168.13.1
         Interface Subtype: ifIndex (2)
         Interface Number: 4
         OID String Length: 0
```

9.3 Zakreslení topologie ze zadání