# Protokoły warstwy łącza danych i ich słabe punkty

**Seminarium: Protokoły komunikacyjne**
dr Sławomir Lasota, dr hab. Jerzy Tyszkiewicz
[ 1000-2D02PK ], SOCRATES: 11304

**2006-10-10**

**Tomasz Andrzej Nidecki**
tomasz.nidecki@students.mimuw.edu.pl
nr indeksu 136413

Uniwersytet Warszawski
Wydział Matematyki, Informatyki i Mechaniki

# Plan ogólny referatu

- Przypomnienie funkcji warstwy łącza danych.
- Możliwe konsekwencje słabości protokołów łącza danych.
- Protokół STP (Spanning Tree Protocol) i jego wady.
- Protokół CDP (Cisco Discovery Protocol) i jego wady.
- Protokół DTP (Dynamic Trunking Protocol) i jego wady.
- Protokół IEEE 802.1Q i jego wady.
- Protokół VTP (VLAN Trunking Protocol) i jego wady.
- Podsumowanie.

# Warstwa łącza danych

- Druga warstwa w modelu ISO/OSI.
- Stanowi połączenie między warstwą sieci (np. protokół IP), a warstwą fizyczną.
- Zapewnia mechanizmy funkcyjne i proceduralne do przesyłania danych między elementami sieci.
- Przykładowe protokoły: Ethernet, PPP, SLIP, Frame Relay, ATM.
- Urządzenia sieciowe standardu Ethernet niektórych producentów (a szczególnie Cisco) wyposażone są w dodatkowe protokoły przydatne w dużych sieciach.
- Przyjrzymy się, do czego służą te protokoły oraz jakie są najpopularniejsze luki w nich i do czego może doprowadzić ich wykorzystanie.

# Spanning Tree Protocol (STP)

- Protokół zdefiniowany jako część standardu IEEE 802.1D.
- Oparty na algorytmie wymyślonym przez Radię Perlman (DEC).
- **Funkcja**: unikanie zapętlenia ramek w mostkowanych sieciach lokalnych.
- **Sposób działania**: utworzenie drzewa rozpinającego i deaktywację nadmiarowych połączeń między urządzeniami.
- **Niebezpieczeństwa**: możliwość przeprowadzenia ataku DoS.
- Opiera się na pakietach zwanych BPDU (*Bridge Protocol Data Unit*). Istnieją dwa rodzaje BPDU: *Configuration* i TCN (*Topology Change Notification*).

# Spanning Tree Protocol (STP)

- Budowa pakietu typu *Configuration*:
  - **PID** (2b): protokół [0]
  - **Wersja** (1b): wersja STP [0 = STP, 1 = RSTP, 3 = MSTP)
  - **Typ komunikatu** (1b): typ BPDU [0x00 = configuration, 0x80 = TCN]
  - **Znaczniki** (1b): ustawienia portów dla RSTP
  - **ID korzenia** (8b): identyfikator korzenia drzewa
  - **Koszt ścieżki do korzenia** (4b)
  - **Identyfikator mostu** (8b): identyfikator nadawcy BPDU
  - **Identyfikator portu** (2b): numer portu (IEEE lub Cisco STP BPDU) z którego wysłano BPDU
  - **Wiek wiadomości** (2b): ilość czasu od wysłania przez korzeń komunikatu, na którymoparto obecny
  - **Maksymalny wiek** (2b): czas po którym komunikat powinien zostać usunięty
  - **Czas powitania** (2b): czas po którym ma być wysłany kolejny BPDU typu Configuration
  - **Opóźnienie przekazywania** (2b): czasy jaki mosty powinny odczekać przed przejściem do nowego stanu po zmianie topologii

# Spanning Tree Protocol (STP)

- Uproszczony opis działania:
  - Przy włączeniu sieci wszystkie obecne w niej przełączniki wysyłają BPDU Configuration, uczestnicząc w wyborach korzenia.
  - Na podstawie ich identyfikatorów wybierany jest korzeń (urządzenie o najmniejszym adresie MAC), a każdy przełącznik oblicza koszty dróg połączenia z korzeniem i wybiera tę o najniższym koszcie.
  - Łącza nadmiarowe są deaktywowane.
  - Po podłączeniu urządzenia o ID niższym niż korzeń następują ponowne wybory korzenia.
  - Po odłączeniu urządzenia struktura drzewa jest przebudowywana od nowa.
  - Za pomocą BPDU typu TCN przełącznik “informuje” korzeń o zmianie działania portów (np. odłączeniu sąsiada) i konieczności przeliczenia dróg. Po otrzymaniu TCN korzeń rozsyła BPDU typu Configuration z bitem “Change” ustawionym na 1 (w polu Znaczniki), co powoduje że pozostałe urządzenia przeliczają wszystkie ścieżki od nowa.

# Spanning Tree Protocol (STP)

- Słabości:
  - Brak uwierzytelnienia. Każde urządzenie w sieci może wysyłać pakiety BPDU.
- Możliwe ataki:
  - Wysyłanie przez napastnika dużej ilości pakietów BPDU (Configuration lub TCN) z losowo wygenerowanymi polami. Powoduje to, iż pozostałe urządzenia w sieci przebudowują wciąż drzewa połączeń. Duża ilość takich danych powoduje paraliż sieci.
  - Przejęcie roli korzenia. Wystarczy przechwycić BPDU z identyfikatorem korzenia, a następnie wysłać BPDU z mniejszym adresem MAC, by stać się nowym korzeniem. Jeśli co chwila wysyłane są BPDU z coraz mniejszymi adresami MAC, następuje permanentny stan wyborów.
- Konsekwencje:
  - Niestabilność sieci. Przez konieczność ciągłego przeliczania ścieżek efektywność sieci jest znacznie zmniejszona, a niektóre ramki mogą ginąć.
- Jak temu zaradzić:
  - Najlepiej wyłączyć STP lub użyć rozszerzeń protokołu zwanych “guard enhancement”.

# Spanning Tree Protocol (STP)

- Więcej informacji:
  - *http://pl.wikipedia.org/wiki/Protokół_drzewa_rozpinającego*
  - *http://en.wikipedia.org/wiki/Spanning_tree_protocol*
  - *http://www.javvin.com/protocolSTP.html*
  - *http://www.cisco.com/univercd/cc/td/doc/product/lan/trsrb/frames.htm#xtocid61*
  - *http://www.cisco.com/warp/public/473/146.html*
  - *http://www.cisco.com/warp/public/473/17.html*
  - *http://www.cisco.com/warp/public/473/65.html (Portfast BPDU Guard Enhancement)*
  - *http://www.cisco.com/warp/public/473/74.html (Root Guard Enhancement)*

# Cisco Discovery Protocol (CDP)

- Protokół własny Cisco, wykorzystywany jednak czasem przez urządzenia innych producentów (np. HP).
- **Funkcja**: służy do wymiany informacji o innych bezpośrednio podłączonych urządzeniach Cisco, np. wersji systemu operacyjnego lub adresu IP. Może być też wykorzystany do wymiany informacji o rutingu na żądanie, co umożliwia uniknięcie konieczności użycia dynamicznych protokołów rutingu w małych sieciach.
- **Sposób działania**: pakiety rozgłoszeniowe CDP są wysyłane na adres multicast 01:00:0C:CC:CC:CC co 60 sekund.
- **Niebezpieczeństwa**: możliwość ataku DoS lub udawania realnego urządzenia.

# Cisco Discovery Protocol (CDP)

- Budowa pakietu CDP:
  - **Wersja** (1b): wersja protokołu [zazwyczaj 1 lub 2]
  - **TTL** (1b)
  - **Suma kontrolna** (2b)
  - **TLV** (różnej długości): zestawy *Type (2b) Length (2b) Value*, zawierające przeróżne informacje, np.:
    - wersja systemu operacyjnego
    - nazwa hosta
    - adresy skonfigurowane dla portu (np. adres IP)
    - typ i model urządzenia
    - ustawienia duplexu
    - domena VTP
    - i inne.

# Cisco Discovery Protocol (CDP)

- Słabości:
  - Brak uwierzytelnienia. Każde urządzenie w sieci może wysyłać pakiety CDP.
- Możliwe ataki:
  - W starszych wersjach systemu IOS występuje podatność na DoS. W przypadku wysłania dużej ilości pakietów CDP z różnymi identyfikatorami (adresami MAC) w urządzeniu wyczerpuje się pamięć i musi być restartowane, by działać poprawnie.
  - Jeśli administrator używa CDP by orientować się w swojej sieci, pojawienie się dużej ilości nowych fikcyjnych urządzeń może utrudnić mu pracę.
- Konsekwencje:
  - Niestabilność sieci w przypadku urządzeń z podatnością w IOS. Zdenerwowanie administratora.
- Jak temu zaradzić:
  - Wyłączyć CDP (polecenie: no cdp run). Protokołu nie ulepszono pod względem bezpieczeństwa.

# Cisco Discovery Protocol (CDP)

## Przykładowy atak:

```
00:06:08: %SYS-2-MALLOCFAIL: Memory allocation of 224 bytes failed from 0x800118D0, alignment 0
Pool: Processor  Free: 0  Cause: Not enough free memory
Alternate Pool: I/O  Free: 32  Cause: Not enough free memory
-Process= "CDP Protocol", ipl= 0, pid= 26
-Traceback= 801DFC30 801E1DD8 800118D8 80011218 801D932C 801D9318
00:06:08:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:09:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:10:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:11:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:12:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:13:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:14:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:15:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:16:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:17:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:18:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:19:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:20:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:21:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:22:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:23:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:38: %SYS-2-MALLOCFAIL: Memory allocation of 140 bytes failed from 0x801E28BC, alignment 0
Pool: Processor  Free: 0  Cause: Not enough free memory
Alternate Pool: I/O  Free: 32  Cause: Not enough free memory
```

# Cisco Discovery Protocol (CDP)

- Więcej informacji:
  - *http://pl.wikipedia.org/wiki/Cisco_Discovery_Protocol*
  - *http://en.wikipedia.org/wiki/Cisco_Discovery_Protocol*
  - *http://www.cisco.com/univercd/cc/td/doc/product/lan/trsrb/frames.htm#xtocid12*
  - *http://www.phenoelit.de/stuff/CiscoCDP.txt (podatność odkryta przez FX)*

# Dynamic Trunking Protocol (DTP)

- Protokół własny Cisco, wykorzystywany do dynamicznego nawiązywania łącz typu *trunk*.
- Łącze typu *trunk* pozwala kierować ruch z wielu VLAN-ów przez pojedyncze połączenie fizyczne.
- **Funkcja**: nawiązanie łącza typu *trunk* między dwoma urządzeniami.
- **Sposób działania**: pozwala na ustalenie typu hermetyzacji (*encapsulation*): np. IEEE 802.1Q lub ISL (własny standard Cisco) oraz chęci nawiązania łącza typu *trunk* między dwoma urządzeniami.
- **Niebezpieczeństwa**: pozwala podszywać się pod urządzenie i dzięki temu przeprowadzać ataki na 802.1Q i VTP. Pozwala podsłuchiwać dane przesyłane przez VLAN.

# Dynamic Trunking Protocol (DTP)

- Budowa pakietu DTP:
  - **Domena** (32b): ciąg ASCII zgodny z domeną VTP
  - **Status** (1b): status portu [włączony, wyłączony, zezwalający na DTP, automatyczny; domyślnie zezwlający na DTP]
  - **Typ** (1b): typ obsługiwanej hermetyzacji [ISL, 802.1Q, negocjowany lub własny]
  - **Identyfikator sąsiada** (6b): identyfikator urządzenia, które wysyła pakiet, zazwyczaj adres MAC portu.
- Urządzenie wysyła najpierw trzy pakiety (jeden na sekundę) wskazujące status łącza oraz wymagany typ hermetyzacji. Następnie pakiety wysłane są co 30 sekund.

# Dynamic Trunking Protocol (DTP)

- Słabości:
  - Brak uwierzytelnienia i domyślna aktywacja na wszystkich portach w urządzeniach Cisco. Każde urządzenie w sieci może uczestniczyć w negocjacji łącz typu *trunk* za pomocą pakietów DTP.
- Możliwe ataki:
  - Uczestnictwo w negocjacji łącz za pomocą pakietów DTP umożliwia podszycie się pod nieistniejące urządzenie uczestniczące w łączu typu *trunk*. Przez to można uzyskać dostęp do przesyłanych przez *trunk* danych i zaatakować protokoły wykorzystywane do hermetyzacji tych danych.
- Konsekwencje:
  - Niepowołany dostęp do danych. Możliwość wykorzystania protokołu do ataków na inne protokoły.
- Jak temu zaradzić:
  - Wyłączyć automatyczne nawiązywanie łącz typu *trunk* (polecenie: switchport mode access). Wtedy jednak administrator musi ręcznie zakładać każde łącze.

# Dynamic Trunking Protocol (DTP)

- Więcej informacji:
  - *http://www.netcraftsmen.net/welcher/papers/switchvtp.html*

# IEEE 802.1Q

- Format pakietów przesyłanych przez łącza typu *trunk* (VLAN).
- **Funkcja**: oznaczanie danych przesyłanych przez łącza typu *trunk* – określanie, do którego VLAN-u należą przesyłane dane.
- **Sposób działania**: po otrzymaniu ramki, przełącznik dodaje znacznik 802.1Q (4 bajty) i przesyła ramkę dalej. W polu VID określone jest, do jakiego VLAN-u należy pakiet.
- **Niebezpieczeństwa**: ataki Man-in-the-Middle, podsłuchiwanie komunikacji, wstrzykiwanie danych do “nieswoich” VLAN-ów.

# IEEE 802.1Q

- Słabości:
  - Brak uwierzytelnienia. Każde urządzenie może udawać, iż wysyła pakiety należące do określonego VLAN-u.
  - Możliwość dodania podwójnego nagłówka, co powoduje kierowanie ramki do VLAN-u z drugiego nagłówka po usunięciu tego pierwszego.
- Możliwe ataki:
  - Wysyłanie dowolnych danych do innego VLAN-u. Atak *proof of concept* (raczej nieszkodliwy).
  - Połączenie z techniką *ARP spoofing* i możliwość podsłuchiwania danych przesyłanych między wybranymi urządzeniami.
- Konsekwencje:
  - Niepowołany dostęp do danych.
- Jak temu zaradzić:
  - Jak w przypadku DTP: wyłączyć automatyczne nawiązywanie łącz typu *trunk* (polecenie: switchport mode access). Wtedy jednak administrator musi ręcznie zakładać każde łącze.

# IEEE 802.1Q

- Więcej informacji:
  - *http://en.wikipedia.org/wiki/IEEE_802.1Q*
  - *http://standards.ieee.org/getieee802/download/802.1Q-2003.pdf*

# VLAN Trunking Protocol (VTP)

- Format własny Cisco, służący do centralnego zarządzania łączami VLAN.
- Umożliwia np. automatyczne skonfigurowanie sieci VLAN na wszystkich przełącznikach należących do tej samej domeny VTP.
- **Funkcja**: centralne zarządzanie łączami VLAN.
- **Sposób działania**: pozwala przekazywać automatycznie między przełącznikami informacje o dodawaniu, usuwaniu lub zmianie nazwy VLAN-ów.
- **Niebezpieczeństwa**: destabilizacja sieci, np. przez nieautoryzowane usuwanie VLAN-ów.

# VLAN Trunking Protocol (VTP)

- Słabości:
  - Pozwala wykorzystywać hasła do zarządzania, ale nie są one domyślnie włączone.
  - W sytuacji, gdy nie są wykorzystywane hasła, każdy może dodać, usunąć lub zmienić nazwę VLAN-u.
- Możliwe ataki:
  - Usunięcie istniejącego VLAN-u lub wszystkich znalezionych w sieci VLAN-ów.
  - Dodanie własnego VLAN-u (raczej *proof-of-concept*).
- Konsekwencje:
  - Urządzenia różnie reagują na usunięcie VLAN-u, do którego są podłączone. Mogą np. utracić łączność z siecią na dobre lub tylko do momentu ponownego utworzenia VLAN-u.
- Jak temu zaradzić:
  - Jak w przypadku DTP: wyłączyć automatyczne nawiązywanie łącz typu *trunk* (polecenie: switchport mode access). Wtedy jednak administrator musi ręcznie zakładać każde łącze. Można też używać hasła VTP dla wszystkich przełączników w danej domenie.

# VLAN Trunking Protocol (VTP)

- Więcej informacji:
  - *http://en.wikipedia.org/wiki/VTP*
  - *http://www.cisco.com/warp/public/473/21.html*

# Podsumowanie

- Większość protokołów w warstwie łącza danych stosowanych np. w urzarzeniach Cisco nie ma żadnych mechanizmów bezpieczeństwa.
- Choć ataki nie są zbyt groźne i z racji charakterystyki warstwy wymagają bezpośredniego dostępu do sieci wewnętrznej, mogą mieć niemiłe konsekwencje w dużych sieciach i utrudnić pracę administratorom.
- Przed wieloma atakami nie ma ochrony innej, niż wyłączenie protokołu.

- *Referat opracowano na podstawie badań Davida Barroso Berruety i Alfredo Andrésa Omelli, twórców narzędzia Yersinia: http://www.yersinia.net/*