

Vladimir "vovcia" Mitiouchev <vovcia@irc.pl>

Zaawansowany sniffing, ataki typu MitM i DoS
w sieciach LAN i VLAN używając dziur w protokole STP

Spis treści:

1. Wprowadzenie
2. Krótki opis protokołu STP (Spanning Tree Protocol)
3. STP a VLAN (Virtual Local Area Network)
4. Algorytmy działania STP
5. Możliwe ataki
6. Ocena zagrożenia
7. Wykrywanie i przeciwdziałanie

1. Wprowadzenie

Wraz z rozwojem sieci lokalnych istniejące rozwiązania przestawały zaspokajać potrzeby administratorów i projektantów. O ile zaprojektowanie sieci bez pętli nie stanowiło większych problemów, problem na jednym łączy powodował rozdzielanie segmentów LANu. Kiedy zachodziła potrzeba redundancji połączenia pomiędzy segmentami LANu, trzeba było po obu stronach linków stawiać routery obsługujące lan-bridging (mostkowanie lanów) i konfigurować zapasowe łącza.

Na początku lat 90-tych XX-tego wieku powstał standard protokołu umożliwiającego działanie sieci lokalnej przy obecności nadmiarowych łączy (ANSI/IEEE 802.1D 1993 Edition). Był on dopracowywany w latach 1996 i 1998 i opierał się na przedstawieniu połączeń pomiędzy urządzeniami jako grafu w kształcie drzewa. Protokół ten nazywa się STP. W roku 2000 została stworzona nowa wersja protokołu nazywająca się RSTP (IEEE 802.1w), wprowadza ona kilka ulepszeń umożliwiających szybszą stabilizację sieci. Ulepszenia te opierają się głównie o funkcje wprowadzone wcześniej przez Cisco, takie jak Uplink Fast, Backbone Fast i Port Fast. Niestety nie poprawiają one bezpieczeństwa protokołu.

Po wprowadzeniu STP, wszystko stało się prostsze. Umożliwia on automatyczną konfigurację urządzeń wspierających ten protokół w sposób zapobiegający powstawaniu logicznych pętli. Kiedy STP wykryje nadmierowe połączenie, blokuje on port na urządzeniu tak by nie przekazywał on żadnych danych. Natomiast w momencie wykrycia przez STP problemu z łączem następuje aktywacja zapasowego łącza (o ile oczywiście takowe istnieje).

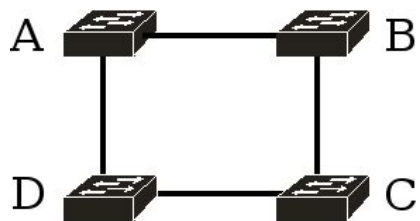
Niestety, podczas projektowania STP (standard IEEE 802.1d) nacisk położono na funkcjonalność, a nie na bezpieczeństwo. Mówiąc wprost – nie uwzględniono żadnych mechanizmów zabezpieczających przed manipulowaniem STP.

W konsekwencji stwarza on wiele możliwości ataków, poczynając od ataku typu DoS na segment sieci lub całą sieć, poprzez sniffowanie ruchu i ataki MitM (Man in the Middle – człowiek pośrodku), do rozprzestrzeniania się tych ataków na sieci VLAN.

W drugiej części omówię pokrótce sposób działania STP. W trzeciej mowa będzie o działaniu STP w środowisku VLANów. W czwartej opowiem o algorytmach kierujących budowaniem drzewa STP i wykrywaniem problemów. W piątej przedstawię znane sposoby ataków na STP. W następnej znajduje się ocena zagrożenia tymi atakami w zależności od topologii i konfiguracji sieci, a w ostatniej – siódmej – metody wykrywania i przeciwdziałania tym atakom.

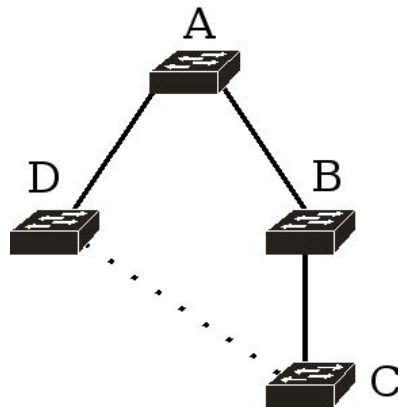
2. Krótki opis protokołu STP (Spanning Tree Protocol)

Wyobraźmy sobie sieć LAN stworzoną z 4 switchy połączonych ze sobą w następujący sposób:

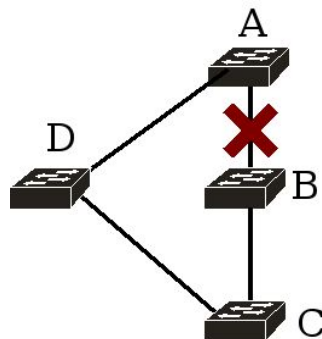


W sieci bez obsługi STP jakakolwiek ramka wpuszczona w taką sieć zaczęłaby krążyć pomiędzy switchami, doprowadzając do przeciążenia sieci i w konsekwencji

jej załamania. Natomiast gdyby sieć ta obsługiwała STP, protokół ten stworzyłby graf bez pętli w kształcie drzewa i ustalił zapasowe łącze, blokując je w trakcie normalnej pracy sieci. Graf ten mógłby wyglądać na przykład tak:



Linią punktowaną zaznaczono tu łącze skonfigurowane jako nadmiarowe, nieużywane do przesyłu danych. Jak widać powstaje struktura bez pętli. Co dzieje się gdy jedno z łączy zostanie przerwanych, można zobaczyć poniżej:



Jak widać z rysunku, w momencie gdy STP wykryje zerwany link, uaktywnia on łącze zapasowe. Czas potrzebny na wykrycie problemu zależy od zegarów ustawionych przez administratora i wynosi zwykle od kilkudziesięciu sekund do minuty (protokół RSTP w takiej sytuacji ustala stabilną konfigurację w ciągu milisekund).

3.STP a VLAN (Virtual Local Area Network)

Na początek trochę o VLANie:

- VLAN czyli Virtual LAN został stworzony by udostępnić możliwość rozdzielania LANu na grupy użytkowników znajdujących się w wirtualnie różnych sieciach i ograniczyć ruch rozgłoszeniowy
- Kolejnym zastosowaniem jest uproszczenie procedury przeprowadzki użytkownika, przy zmianie miejsca w LANie wciąż znajduje się on w swoim domowym VLANie.
- znamy 3 rodzaje VLANów: MAC-based, port-based i tag-based
- MAC-based grupuje komputery na podstawie adresów sprzętowych
- port-based grupuje porty w obrębie jednego switcha
- tag-based grupuje porty w obrębie switcha i przesyła je dalej znakując tzw. tagami, które są czytane przez switchy pośredniczące, switch końcowy przed wysłaniem ramki do komputera usuwa tag.

Niestety, większość implementacji protokołu STP w VLANie nie zachowuje się tak jakbyśmy tego od nich oczekiwali. Z reguły w obrębie całego LANu funkcjonuje jeden STP, co rozszerza wszystkie ataki opisane w tym dokumencie o atakowanie VLANów właśnie. Wszędzie tam gdzie nie jest wyraźnie zaznaczone inaczej ataki w LAN dają się analogicznie przeprowadzać również w VLAN.

4.Algorytmy działania STP

Pierwszą fazą działania protokołu STP są wybory Designated Root Bridge. Jest to urządzenie od którego zaczynamy rysowanie drzewa. Oprócz bycia logicznym początkiem nie pełni ono żadnych dodatkowych funkcji. Wybory te odbywają się w następujący sposób:

- każde urządzenie generuje ramkę BPDU zawierający Bridge Identifier, który zwykle obliczany jest na podstawie adresu MAC i ustalonego przez administratora (bądź fabrycznie) priorytetu
- po otrzymaniu zgłoszenia od kandydata (A) na Root Bridge urządzenie (B) porównuje otrzymany Bridge Identifier (A) ze swoim (B) i jeżeli kandydat (A) ma mniejsze ID to urządzenie (B) przestaje kandydować w wyborach i zaczyna

anonsować do swoich sąsiadów że A jest Designated Root Bridge.

Kolejną fazą jest budowa drzewa, zasada jest podobna jak w protokołach routingu – każde urządzenie anonsuje na każdym z portów koszt połączenia do Root Bridge składający się z kosztów otrzymanych od poprzedniego urządzenia i kosztu portu z którego wysyłany jest BPDU. Należy zauważyć że BPDU nigdy nie są retransmitowane przez urządzenia podtrzymujące STP, są one interpretowane i na ich podstawie tworzone są własne BPDU.

Port który dostanie od sąsiada BPDU z najmniejszym kosztem dostępu do Root Bridge staje się Designated Root Port, co oznacza że komunikacja z resztą sieci przechodzi właśnie przez niego. Pozostałe porty z większymi kosztami dostępu są przełączane w tryb Blocking (więcej o trybach dalej). Na podobnej zasadzie wybierany jest Designated Bridge który staje się odpowiedzialny za obsługę danego segmentu LAN.

Po wszystkich wyborach następuje faza stabilności która charakteryzuje się następującymi właściwościami:

- jest tylko jedno urządzenie w sieci które regularnie ogłasza się jak Designated Root Bridge, a wszystkie pozostałe ogłaszają TO urządzenie. BPDU są wysyłane w regularnych odstępach czasu wyznaczanych przez parametr Hello Time.
- W każdym segmencie sieci jest tylko jeden Designated Root Port przez który następuje wymiana ruchu z Designated Root Bridge
- Wymiana danych poza obrębem switcha przebiega **tylko** poprzez Designated Root Port, wszystkie pozostałe porty są w stanie Blocking

Teraz krótki opis stanów w którym może znajdować się port:

- blocking: port zablokowany, ramki BPDU są otrzymywane i wysyłane, ramki użytkowe są ignorowane
- listening: pierwszy etap przygotowania do stanu Forwarding, BPDU są wysyłane i interpretowane, cała reszta – ignorancja
- learning: drugi etap: BPDU przetwarzane i wysyłane, uczenie się MACów, nie są

przekazywane żadne dane użytkowe

- forwarding: BPDU interpretowane i wysyłane, obsługa ruchu sieciowego.

Przedział czasu w jakim prot znajduje się w stanie listening i learning jest konfigurowalny i zawiera się w ramach BPDU.

Kiedy któryś z Designated Bridge wykryje zmianę w topologii sieci (np. problem w jednym z połączeń lub nowe urządzenie STP w sieci) wysyła on ramkę TCN-BPDU (Topology Change Notification BPDU) w górę drzewa. Kiedy Designated Root Bridge otrzyma taką ramkę rozsyła on TCN-BPDU do wszystkich urządzeń wymuszając rekonfigurację drzewa.

UWAGA! Opis działania STP w tym rozdziale został przedstawiony bardzo pobieżnie i ze świadomym pominięciem wielu szczegółów. Zainteresowanych dokładnym działaniem STP odsyłam do stosownego standardu IEEE odnośnik do którego znajduje się w dziale Literatura.

5. Możliwe ataki.

Ataki na STP możemy podzielić na 3 kategorie:

- ataki typu DoS na całą sieć
- ataki typu DoS na segment sieci
- ataki MitM (man in the middle)
- sniffing

Najprostszy atak który przychodzi na myśl to utrzymywanie sieci w stanie rekonfiguracji przez cały czas. Najłatwiej osiągnąć to nasłuchując zgłoszeń Designated Root Bridge i generując BPDU z Bridge Identifier niższym od aktualnego. Po timeoucie ustawianym w ramce BPDU wysyłamy kolejny BPDU z jeszcze mniejszym identyfikatorem. Przy odpowiednio dobranych timeoutach jesteśmy w stanie doprowadzić do sytuacji w której sieć przez cały czas znajduje się w stanie rekonfiguracji i nie przekazuje danych, co jest właśnie typowym atakiem typu DoS.

Innym atakiem DoS na całą sieć jest wysyłanie BPDU z Bridge ID równym 0 co powoduje wygranie wyborów, a potem **nie** wysyłanie potwierdzeń. Po upłygnięciu timeoutu nastąpi rekonfiguracja drzewa. Przy odpowiednio nisko ustawionym timeoucie sieć może przez większość czasu znajdować się w stanie rekonfiguracji. Warto zauważyć że taki atak jest łatwiejszy do przeprowadzenia ponieważ nie musimy znać parametrów Designated Root Bridge. Oprócz tego umożliwia on atakowanie w momencie gdy atakowany Bridge ID jest równy 0, ponieważ STP w momencie otrzymania dwóch zgłoszeń o tych samych Bridge ID traktuje to jako pojawienie się pętli i wyłącza albo port do którego podpięty jest ten bridge, albo port atakującego, w zależności od ich kolejności na switchu który interpretuje BPDU.

Kolejnym atakiem (hipotetycznym – brak informacji na temat możliwości jego przeprowadzenia oraz brak odpowiedniego sprzętu uniemożliwia zdobycie pewności co do jego powodzenia) jest atak na sąsiedni VLAN (typu port-based i z oddzielnymi drzewami). Polega on na wysyłaniu komunikatów BPDU od imienia urządzenia w sąsiednim VLANie. Problemem wydaje się być zdobycie jego parametrów co jest niezbędne dla powodzenia ataku – jednak przy pewnej dozie szczęścia/czasu można wmówić switchowi że w jakiś sposób oba drzewa zostały połączone co wymusi rekonstrukcję drzewa STP z udziałem obu VLANów.

Analogicznie możemy przeprowadzać ataki na część sieci, a dokładniej na połączenia pomiędzy switchem do którego jesteśmy przyłączeni a którymś z jego sąsiadów. Wmawiając naszemu switchowi że posiadamy trasę do jego sąsiada w zależności od numeru portu do którego podłączony jest ten sąsiad możemy (lub nie) odciąć część sieci. Może to być użyte w celu np. podszycia się pod serwer znajdujący się w innym segmencie.

Ogólnie rzecz ujmując, manipulując parametrami BPDU jesteśmy w stanie zmieniać przedstawienie o topologii sieci naszych bezpośrednich sąsiadów.

Kolejną klasą ataków są ataki MitM. O ile są one najbardziej niebezpieczne, o tyle są dość trudne do wykonania. Jak można się domyśleć trzeba przekonać switche które stoją na drodze między hostami które atakujemy że dysponujemy lepszym połączeniem niż one. Nie jest to łatwe zadanie, niezbędnym warunkiem jest fizyczne podłączenie do obu z nich. Można co prawda przejąć kontrolę nad dwoma hostami z różnych segmentów, powstaje jednak wtedy problem ich połączenia w celu przekazywania ramek. Wysyłając BPDU z ustawionymi mniejszymi kosztami do każdego ze switchy możemy przestawić porty je łączące w stan Blocking i przekierować ruch przez swoją jednostkę. Należy zauważyć że tego typu atak jest ekstremalnie trudny do wykrycia przez końcowego użytkownika którego atakujemy. O ile w przypadku DNS spoofing może on zobaczyć podmianę adresów IP, w przypadku ARP spoofing albo zauważy zmianę MACów, albo, co jest już praktyką powszechną ma statyczną tablicę ARP z zapisanymi adresami ważnych hostów, o tyle w przypadku STP MitM faktycznie nie ma on możliwości wykrycia faktu bycia atakowanym, jedyną wskazówką mogłoby być niewielkie zwiększenie się czasu przesyłu pakietów. Z pozycji administratora sieci zadanie jest dość proste, wystarczy obserwować dzienniki systemowe pod kątem zmian topologii STP i wyłapywać 'dziwne' sytuacje.

Kolejnym atakiem jest tzw. prowokacyjny sniffing. Znane są metody pozwalające przełączyć switch w tryb huba za pomocą zaśmiecania jego tablicy MACów. Jednak STP daje nam bardziej finezyjny sposób na wymuszenie takiego zachowania. Prowokacyjny sniffing daje nam możliwości np. przechwycenia hasła do switcha lub zgadywania TCP Sequence Number, zresztą możliwości jest tyle na ile szerokie jest nasze wyobrażenie na temat tego co można wyciągnąć z wysniffowanych danych. Sniffing taki jest wykonalny w przypadku gdy urządzenie wspiera rozszerzenie STP Portfast, które opuszcza stan Learning i od razu przekazuje ramki pomiędzy stacjami roboczymi. Haczyk tkwi w tym, że podczas zmiany konfiguracji STP switche są zobowiązane standardem do wyczyszczenia swoich tablic z adresami sprzętowymi. O ile w zwykłym STP switch w stanie Learning zdąży się nauczyć dość dużej ilości hostów, to w trybie Portfast (a propos włączony

do standardu RSTP) od razu przejdzie on do przekazywania ramek. W takiej sytuacji każda ramka która jest skierowana do stacji której switch nie ma jeszcze w swojej tablicy jest rozsyłana na wszystkie porty, co de facto oznacza że switch działa przez chwilę w trybie huba. Z drugiej strony każda ramka od nieznanego jeszcze hosta powoduje wpisanie jego adresu MAC do tablicy switcha. Zadanie atakującego sprowadza się więc do wyzerowywania tablicy MACów w switchu co najmniej dwa razy częściej niż przesyłane są pakiety między hostami które chcemy podsłuchać. W praktyce oznacza to ograniczenie skuteczności ataku gdy ruch ten jest większy niż 49% dostępnego pasma. Praktycznymi metodami zmuszania switcha do amnezji MACów jest floodowanie go pakietami BPDU sygnalizującymi zmianę topologii, co czasami ciężko wykonać bez spowodowania DoSa, oraz flood wymuszeniem wyborów jakiegokolwiek pozycji w sieci.

Konkretne algorytmy wykonywania tych ataków wykraczają poza zakres tego materiału. Dla zainteresowanych – literatura.

6. Ocena zagrożenia

Zważając na fakt że większość sieci korporacyjnych opartych jest na inteligentnych urządzeniach (switche, routery), a STP na takich urządzeniach zwykle jest domyślnie włączone, większość sieci jest bardzo podatnych na ataki opisane powyżej. Ponieważ STP jest mechanizmem właściwie samowystarczalnym i rzadko wymagającym jakiegokolwiek konfiguracji, część z administratorów może nawet nie wiedzieć że w ich sieciach jest włączony STP. Kolejni zwykle nie dotykają go zgodnie z zasadą nie ruszania działających rzeczy. Dlatego właśnie oceniam stopień zagrożenia na dość poważny. Pocięcza jedynie brak całkowicie zautomatyzowanych narzędzi do atakowania STP. Programy znane do tej pory potrafią przeprowadzać ataki typu DoS, co jest dość łatwe do wykrycia, głównie metodą interpretacji urywającego się telefonu i krzyków o niedziałającym internecie z leżącej obok popielniczki słuchawki telefonu, którą ktoś tam położył i już nigdy nie miał ochoty odkładać na miejsce.

Wykrywanie i przeciwdziałanie

Bardziej finezyjne techniki można wykrywać za pomocą analizatorów ruchu sieciowego, jednak ze względu na trudność w umiejscowieniu takich na każdym kablu proponowałbym centralne zbieranie i analizowanie logów z urządzeń obsługujących STP. Wykrywać można np. zbyt częste ramki BPDU, zmiany topologii sieci (administrator w każdym wypadku powinien się o tym dowiedzieć, niezależnie od tego czy jest to próba ataku czy losowe zdarzenie), zmiany Designated Root Bridge (robi to de facto BPDU Guard), czy też brak logów z któregoś urządzenia.

Przeciwdziałanie natomiast najłatwiej skutecznie wyłączeniem STP wszędzie tam, gdzie nie jest ono konieczne do prawidłowej pracy sieci. Jeżeli musimy mieć w sieci nadmiarowe łącza, można stosować np. technologię Link Aggregation (Intel, Avaya). Jeżeli koniecznie musimy używać STP, należy (w miarę możliwości) stosować rozwiązania typu BPDU Root i STP Portfast (który choć umożliwia sniffing zabezpiecza przed częścią ataków DoS). Można też ustawiać ręcznie identyfikatory na poszczególnych switchach, tak by Designated Root Bridge miał ID = 0, co uchroni sieć przed częścią ataków. Należy też – o ile oprogramowanie na to pozwala, włączyć STP tylko na portach połączonych z innymi urządzeniami STP. Nie jest też do końca jasne w jakiej części takie rozwiązania zabezpieczają sieć przed atakami.

Literatura:

- <http://www.bugtraq.ru/library/books/stp/index.html>
O.K. Артемьев, В.В. Мяснянкин (podziękowania)
- Media Access Control (MAC) Bridges ANSI/IEEE Std 802.1D, 1998