ANALIZA BEZPIECZEŃSTWA SIECI MPLS VPN

Łukasz Polak
Opiekun: prof. Zbigniew Kotulski

Plan prezentacji

1. Wirtualne sieci prywatne (VPN)
2. Architektura MPLS
3. Zasada działania sieci MPLS VPN
4. Bezpieczeństwo sieci MPLS VPN
5. System do analizy bezpieczeństwa MPLS VPN

Wirtualne sieci prywatne (VPN)

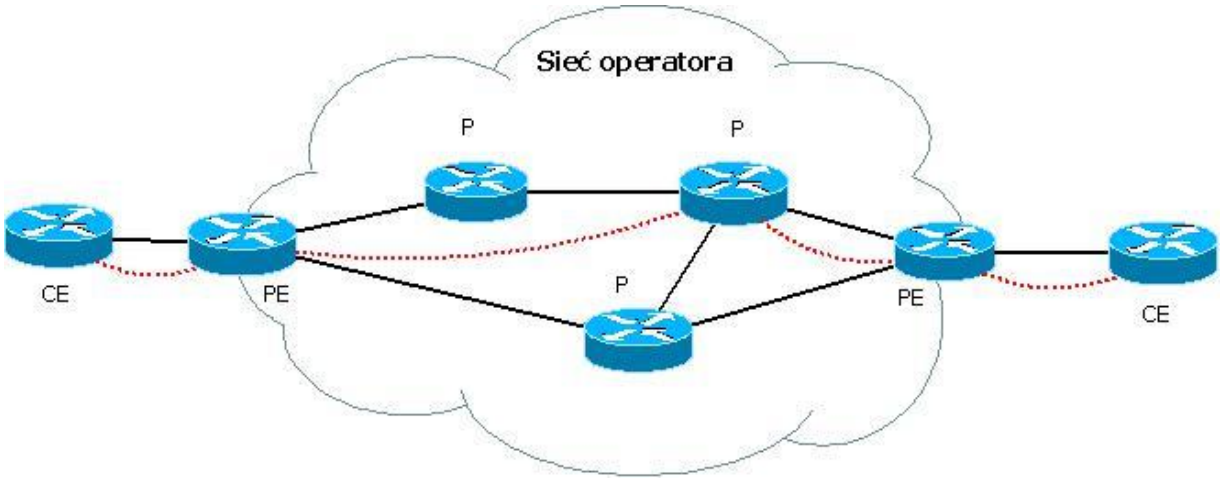
- Umożliwiają łączność pomiędzy zdalnymi lokalizacjami klienta
- Wykorzystują infrastrukturę operatora/operatorów
- Sieć operatora pozostaje transparentna dla klientów
- Tańsza alternatywa dla dzierżawionych łączy

Rodzaje sieci VPN

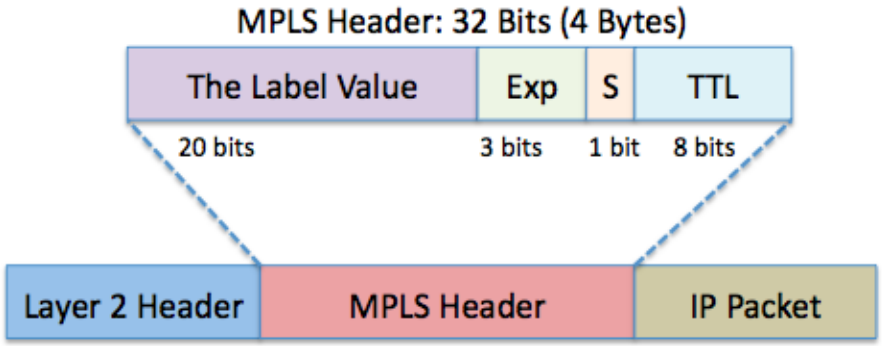
- VPN oparte o aplikacje (OpenVPN, Hamachi)
- VPN dostarczane przez operatorów (MPLS VPN)

Architektura sieci VPN

- Router brzegowy dostawcy (PE)
- Router brzegowy klienta (CE)
- Router szkieletowy (P) – niewidoczny dla klienta



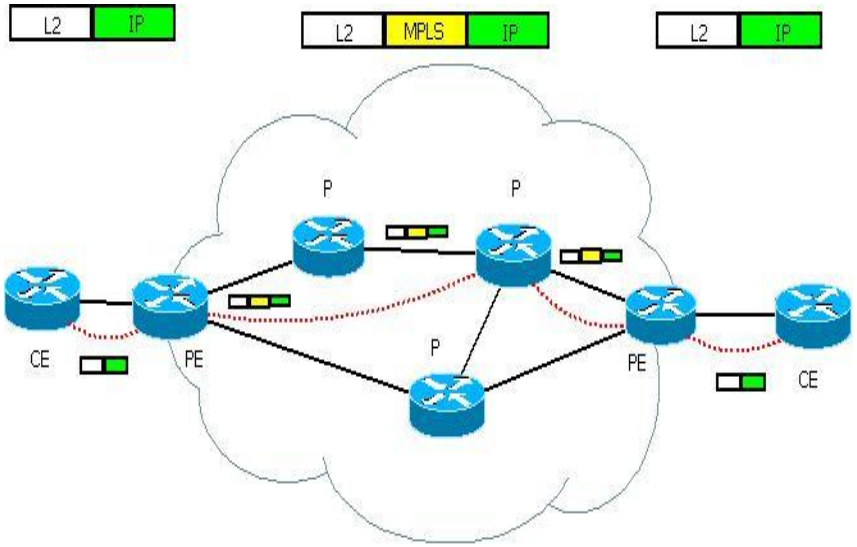
MPLS



- Mechanizm przełączania pakietów na podstawie etykiet
- Nagłówek MPLS wstawiany jest pomiędzy nagłówki 2 i 3 warstwy
- Nagłówki mogą być hierarchiczne, co pozwala realizować różne usługi (VPN, TE)
- Niezależny od stosowanych protokołów

Zasada działania MPLS

- Pakiet na brzegu sieci MPLS na podstawie zdefiniowanych kryteriów otrzymuje jedną lub więcej etykiet
- Węzły wewnątrz sieci MPLS analizują tylko najbardziej zewnętrzną etykietę i na jej podstawie kierują pakiet
- Routery MPLS mogą wykonywać jedną z operacji:
  - Zdjęcia etykiety (POP)
  - Wstawienia etykiety (PUSH)
  - Podmiany etykiety (SWAP)



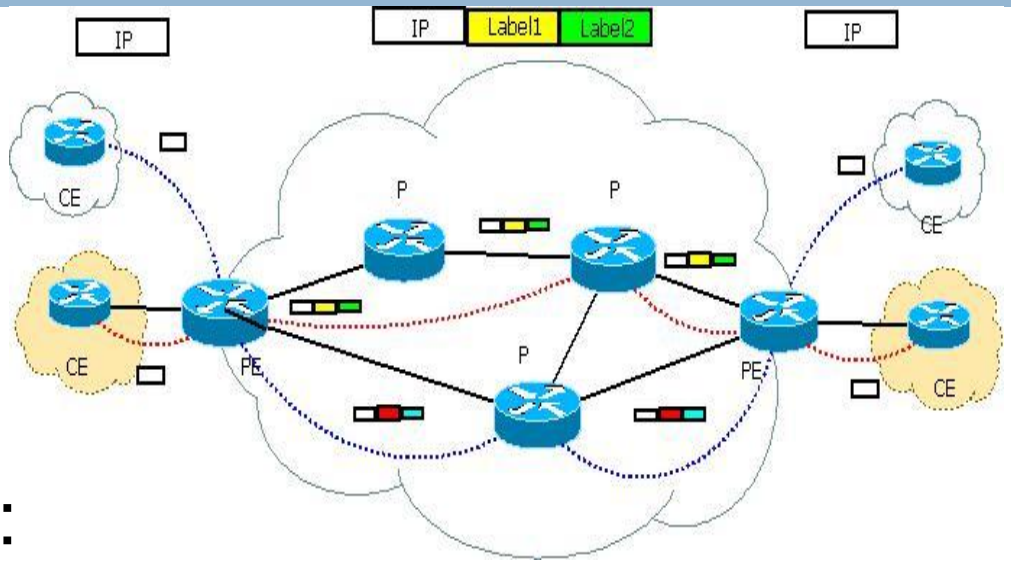
Dystrybucja etykiet

- LDP
  - Prosta konfiguracja
  - Zależny od IGP
  - Większa skalowalność
- RSVP
  - Niezależny od IGP
  - Możliwe precyzyjne definiowanie LSP
  - Inżynieria ruchowa
- MP-BGP
  - Przekazywanie informacji o etykietach pomiędzy różnymi AS-ami

Zastosowanie MPLS

- Inżynieria ruchowa
- Integracja różnych technologii sieciowych
- Wirtualne sieci prywatne

MPLS VPN



- Rodzaje:
  - L3VPN
  - L2VPN
  - VPLS
- Zasada działania:
  - Pakiet otrzymuje 2 etykiety: zewnętrzna określa router PE do którego jest kierowany ruch, wewnętrzna definiuje VPN do którego powinien trafić pakiet
  - W przypadku L3VPN routery PE posiadają oddzielne tablice routingu dla wszystkich klientów (VRF)

Bezpieczeństwo MPLS VPN

- Ruch w sieci MPLS nie jest szyfrowany
- Routery PE są zazwyczaj współdzielone
- MPLS nie dostarcza żadnych dodatkowych mechanizmów bezpieczeństwa

Ataki na sieć MPLS VPN

- Podział ataków na sieć VPN ze względu na:
  - Miejsce z którego następuje atak:
    - Z zewnątrz sieci MPLS (Internet, inny VPN)
    - Z wewnątrz sieci MPLS
  - Rodzaj ataku:
    - DoS
    - Nieuprawniony dostęp
    - DoQoS

Ataki spoza sieci MPLS VPN

- Zgodnie z RFC 2547 routery PE nie powinny wpuszczać z zewnątrz do sieci MPLS pakietów posiadających etykietę – zapobiega to możliwości wstrzyknięcia spreparowanych etykiet
- Routery wewnątrz sieci MPLS nie analizują adresów IP – podmiana adresu nie przyniesie atakującemu korzyści
- Routery P powinny być niewidoczne z zewnątrz
- Wniosek: jedynym możliwym atakiem na sieć MPLS z zewnątrz jest atak typu DoS na routery PE

Ataki z wewnątrz sieci MPLS VPN

- Możliwe wszystkie rodzaje ataków, w szczególności nieuprawniony dostęp – przechwycenie/wstrzyknięcie ruchu poprzez atak na protokoły dystrybucji etykiet (LDP, RSVP, MBGP)
- Modyfikacja etykiet pozwala na przekierowanie w sposób niezauważony ruchu poza VPN
- Ataki na protokół RSVP mogą uniemożliwić szybkie zestawianie LSP o określonych parametrach i uniemożliwić poprawne działanie mechanizmów TE (DoQoS)
- W transparentnych sieciach L2VPN/VPLS możliwe do wykonania są klasyczne ataki na protokoły L2 poprzez „chmurę MPLS”:
  - MAC flooding
  - ARP spoofing
  - Ataki na STP, VTP

Cel pracy

- Implementacja systemu do analizy sieci MPLS VPN i przeprowadzania ataków na sieć MPLS
- Przetestowanie systemu w sieci laboratoryjnej

System do analizy bezpieczeństwa sieci MPLS VPN

- Założenia:
  - Dostęp do łącza wewnątrz sieci MPLS VPN
  - Brak wiadomości na temat przyporządkowanych etykiet (możliwość przeprowadzenia ataku bez wcześniejszej wiedzy)
- Dostępne funkcje:
  - Skanowanie ruchu (przechowywanie mapowania etykieta/IP)
  - Przechwycenie/przekierowanie ruchu poprzez zmianę etykiet
  - Modyfikacja sesji MPBGP w celu przekierowania ruchu
  - Ataki na QoS
  - Ataki na L2 poprzez sieć MPLS
- Testy na sprzęcie (planowane):
  - Cisco 7200
  - Juniper 2320

Implementacja

- Język Python 2.6
- W chwili obecnej zaimplementowane przeze mnie zostało skanowanie ruchu i podmiana etykiet
- Do symulacji ataków L2 planuję wykorzystać program *yersinia*

Dziękuję za uwagę

Pytania