Jak zbudować skalowalną i bezpieczną sieć dostępową

Marcin Szreter

Consulting Systems Engineer

szreter@cisco.com

Agenda

- **Wstęp**

  (czyli czemu w ogóle mówimy o dostępie)

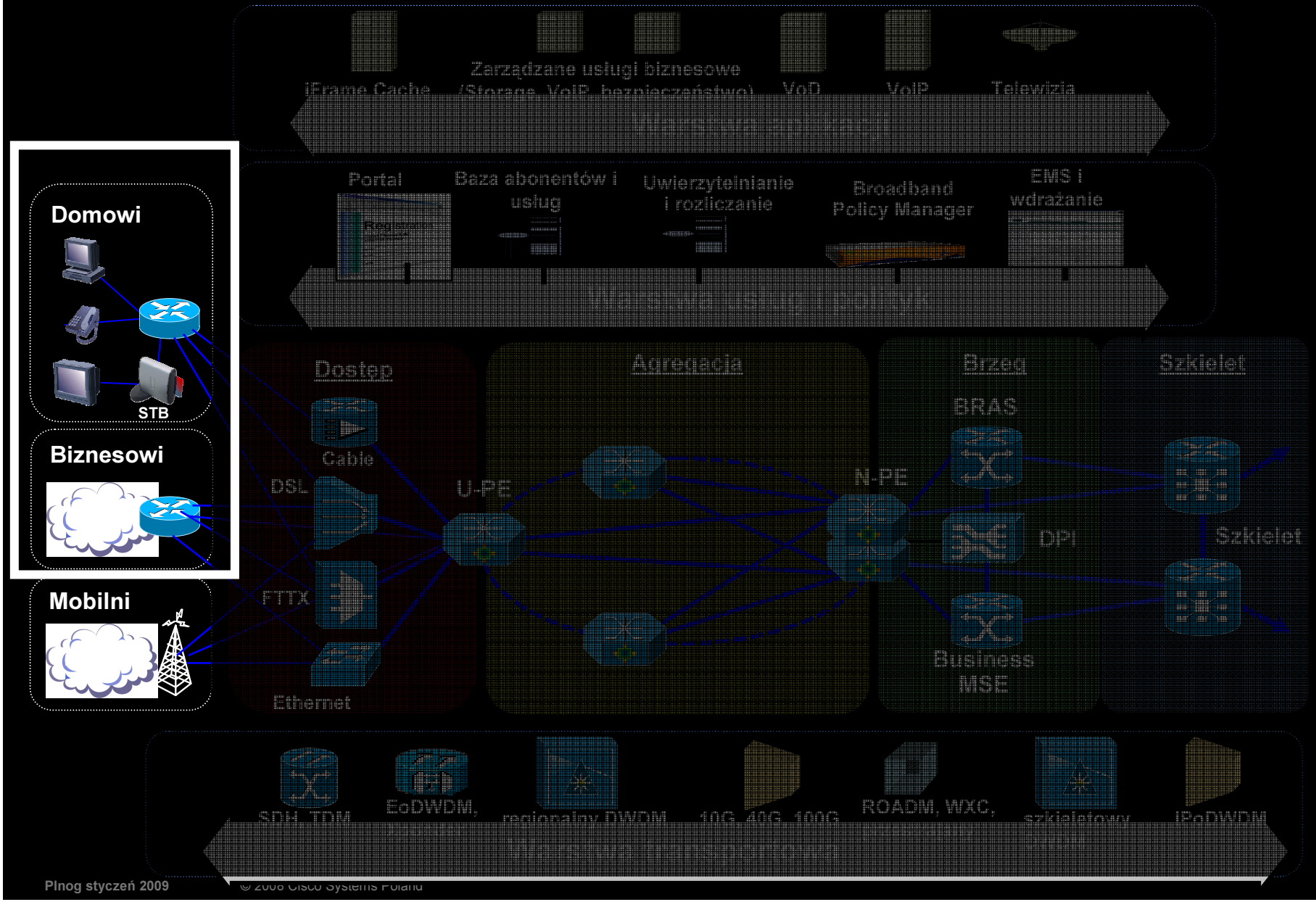
- **Technologie dostępowe**

  (czyli ktora jest lepsza, i dlaczego odpowiedz brzmi „to zależy”)

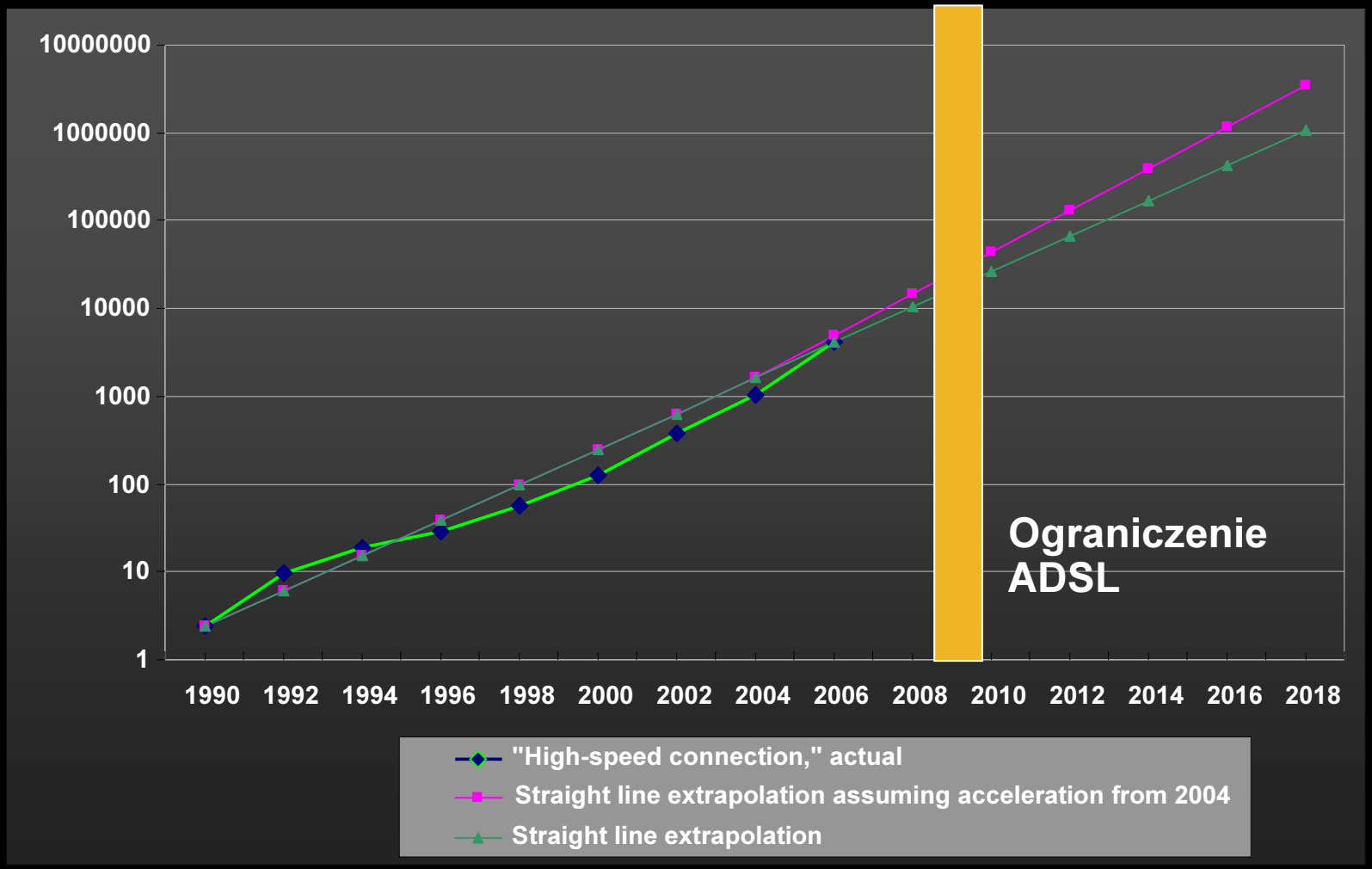
- **Architektura dostępowa w** *(ogólnych)* **szczegółach**

  (czyli jakie mechanizmy warto znać przy rozważaniu budowy sieci dostępowej)

Architektura sieci IP NGN



Wstęp
Wymagania na pasmo w niedalekiej przyszłości



Źródło: Heavy Reading "FTTH Worldwide Market & Technology Forecast, 2006-2011"

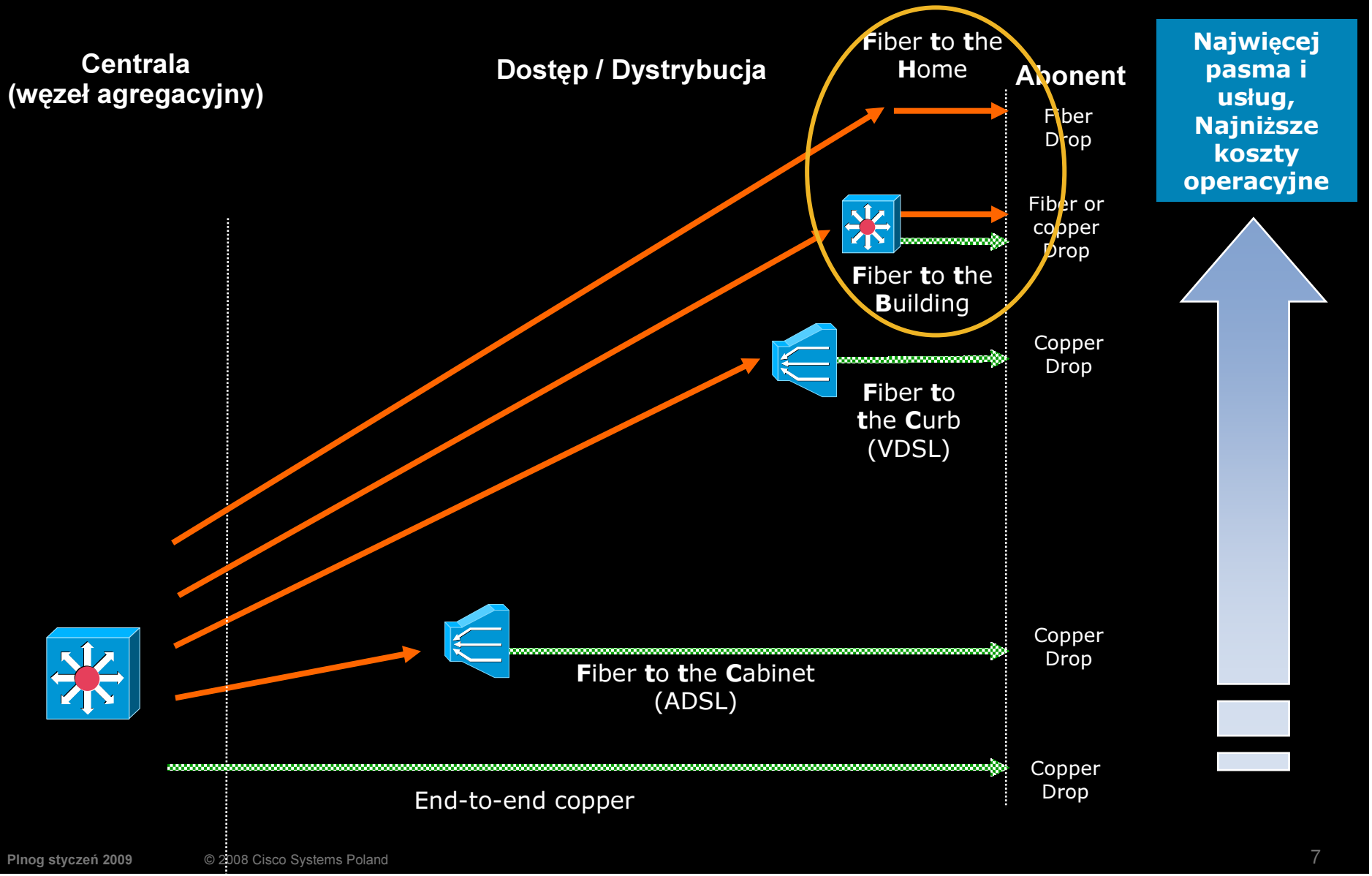
Wstęp
Wymagania dla sieci dostępowej

- **Bezpieczeństwo**
- **Skalowalność**
- **Łatwość uruchamiania nowych usług, łatwe rozwiązywanie problemów**
- **Szerokie pasmo**
- **Efektywny koszt:**
  - Niski koszt początkowy inwestycji
  - Tanie utrzymanie, administracja
  - Optymalne koszty migracji do zaawansowanych usług i większego pasma

Wstęp
Technologie dostępowe

- HFC *(Hybrid Fiber Coaxial) DOCSIS 2.0, 3.0,* D-PON
- ADSL, xDSL (x!='A' *HDSL, SHDSL, itp)*
- WiMax / WiFi
- Optyczne sieci pasywne PON – Passive Optical Networks (B-PON, E-PON, G-PON, WDM-PON, 10GE-PON)
- ETTx - Ethernet Point-to-Point

Wstęp
FTTx - opcje



Agenda

- **Wstęp**

  (czyli czemu w ogóle mówimy o dostępie)

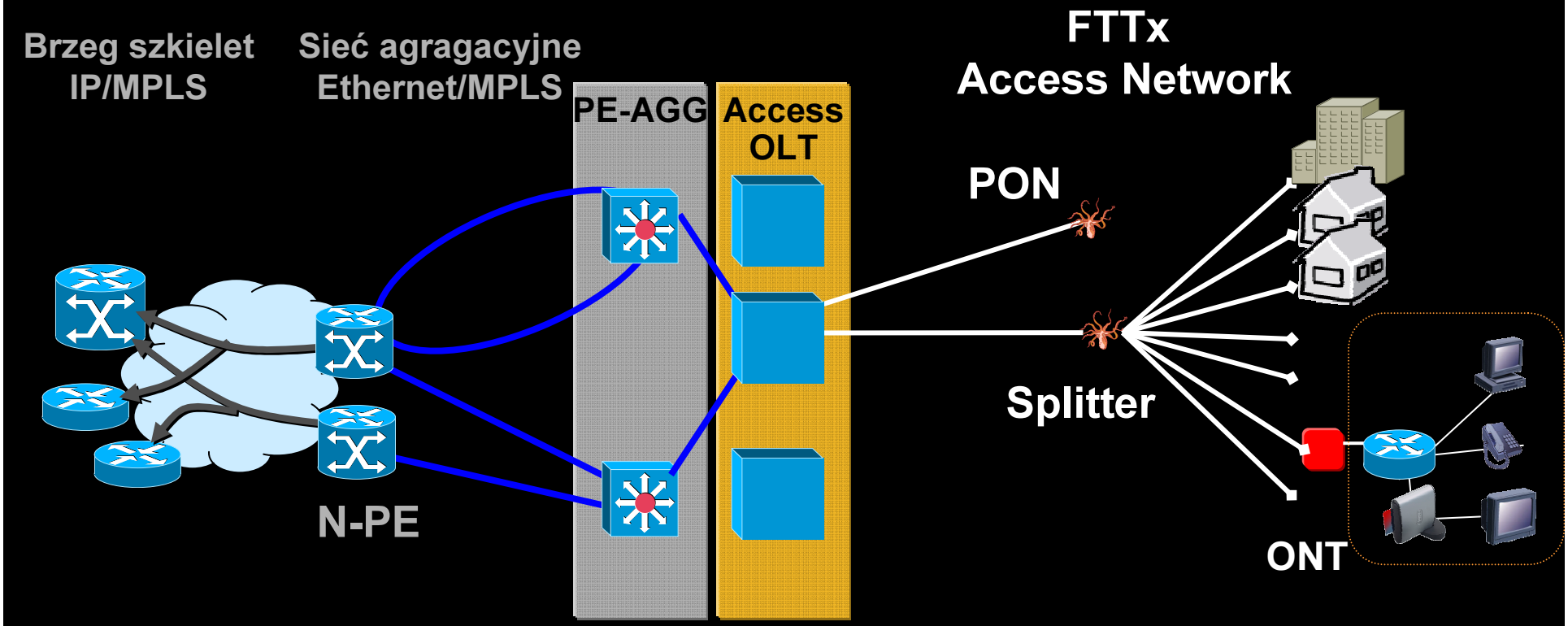
- **Technologie dostępowe**

  (czyli ktora jest lepsza, i dlaczego odpowiedz brzmi „to zależy”)

- **Architektura dostępowa w** *(ogólnych)* **szczegółach**

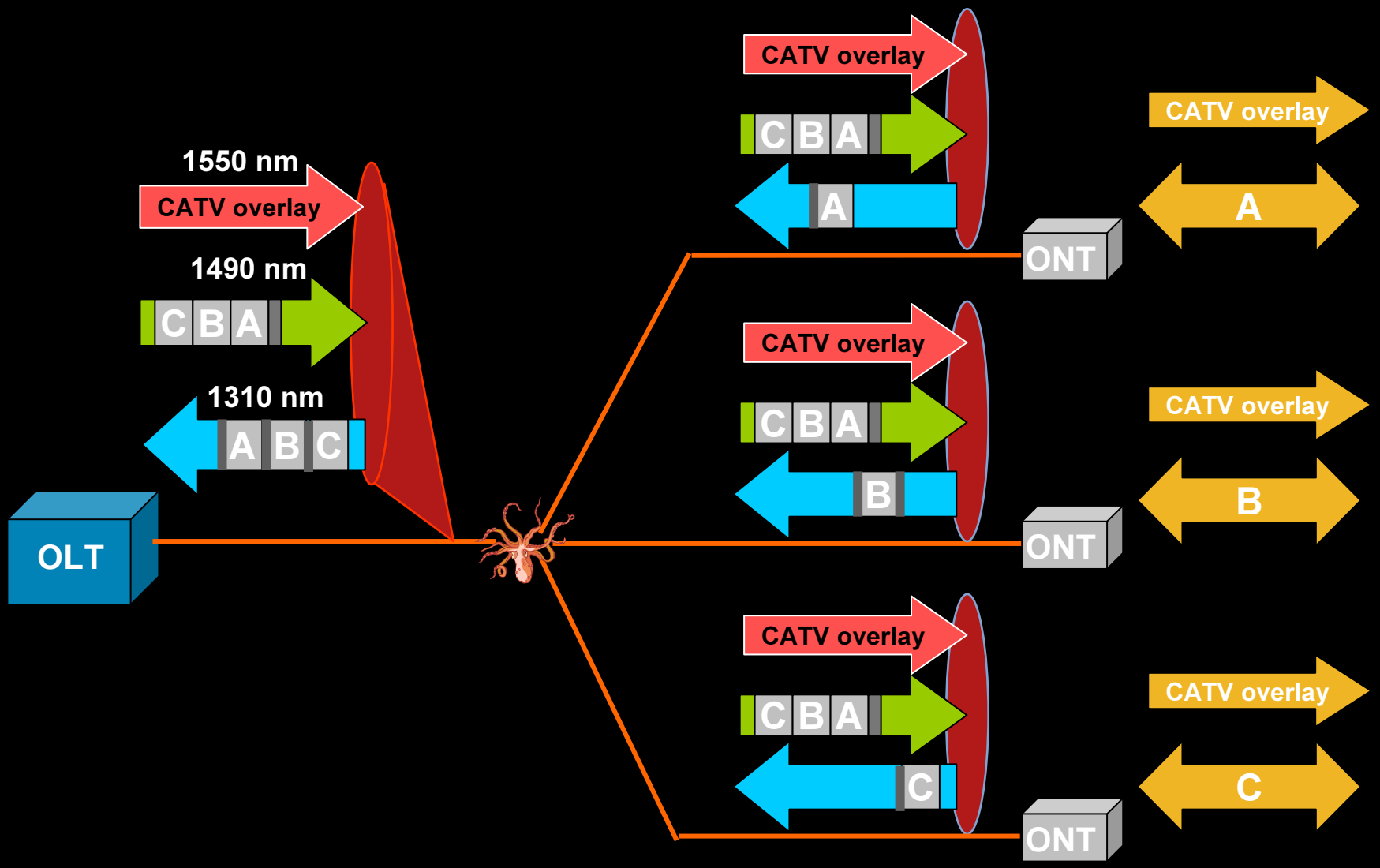
  (czyli jakie mechanizmy warto znać przy rozważaniu budowy sieci dostępowej)

Passive Optical Networks (PON)
Architektura



ONT - Optical Network Termination
ONU - Optical Network Unit
OLT – Optical Line Termination

Passive Optical Networks (PON)
Komunikacja



Passive Optical Networks (PON)
Cechy *(1/2)*

- **Oszczedności światłowodów pomiedzy CO/POP**

  Istotne w sytuacji, gdy można wykorzystać istniejace, niewielkie ilości światłowodów lub gdzie możliwość implementacji nowych wiązek jest ograniczona

  Mało istotne w nowych implementacjach: koszt światłowodu jest niewielki w stosunku do kosztów robót ziemnych, instalacyjnych, itp.

- **Oszczędność ilości portów optycznych w CO/POP**

  PON ma mniejsze wymagania na ilość portów na których terminowane są łącza klienckie

- **Brak implementacji aktywnych urządzeń poza POP**

  W zależności od regionu ten argument może nie być istotny: w Europie często pętle są na tyle krótkie (w obszarach miejskich) że implementacja ethernetu point-2-point też nie wymaga instalacji urządzeń aktywnych poza PoP

CO – central office
PoP – point of presence

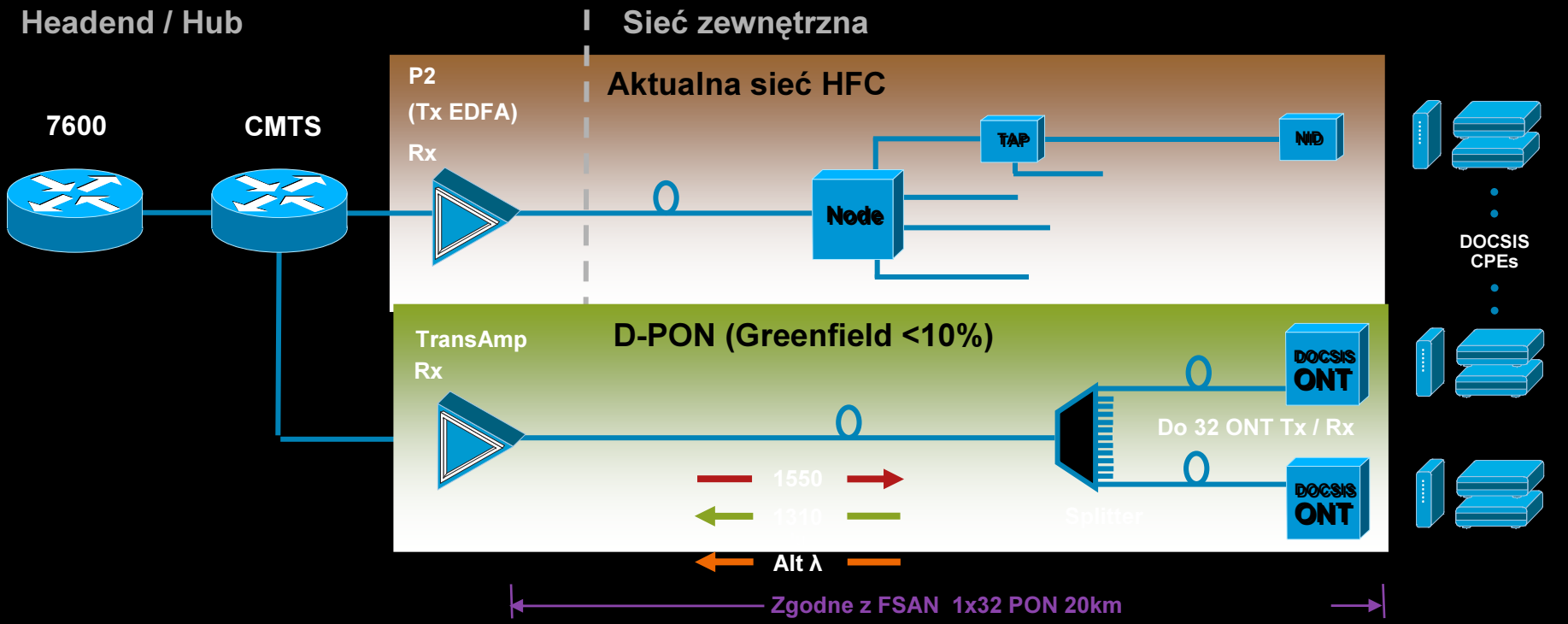
Passive Optical Networks (PON)
Cechy *(2/2)*

- **Pasmo jest współdzielone pomiędzy abonentami**
- **Mocna enkrypcja jest wymagana by zabezpieczyć ruch kliencki i ograniczyć możliwość podsłuchiwania**
- **Każda końcówka (OLT, ONT) musi pracować z pasmem zagregowanym**

  Np. GPON ONT dostarczające pasmo abonenckie 100 Mbit/s musi pracować z pasmem 2.5 Gbit/s od strony sieciowej
- **Znacząco wyższa moc optyczna jest wymagana niż w innych technologiach**
- **Niższa dostępność** – uszkodzone CPE może spowodować niedostępność całego drzewa
- **Zagłuszanie sygnału jest łatwe** - wystarczy transmitować silne światło w kierunku OLT: trudne do wykrycia
- **W przypadku zmiany technologii wszystkie urządzenia terminujące muszą zostać wymienione**

D-PON

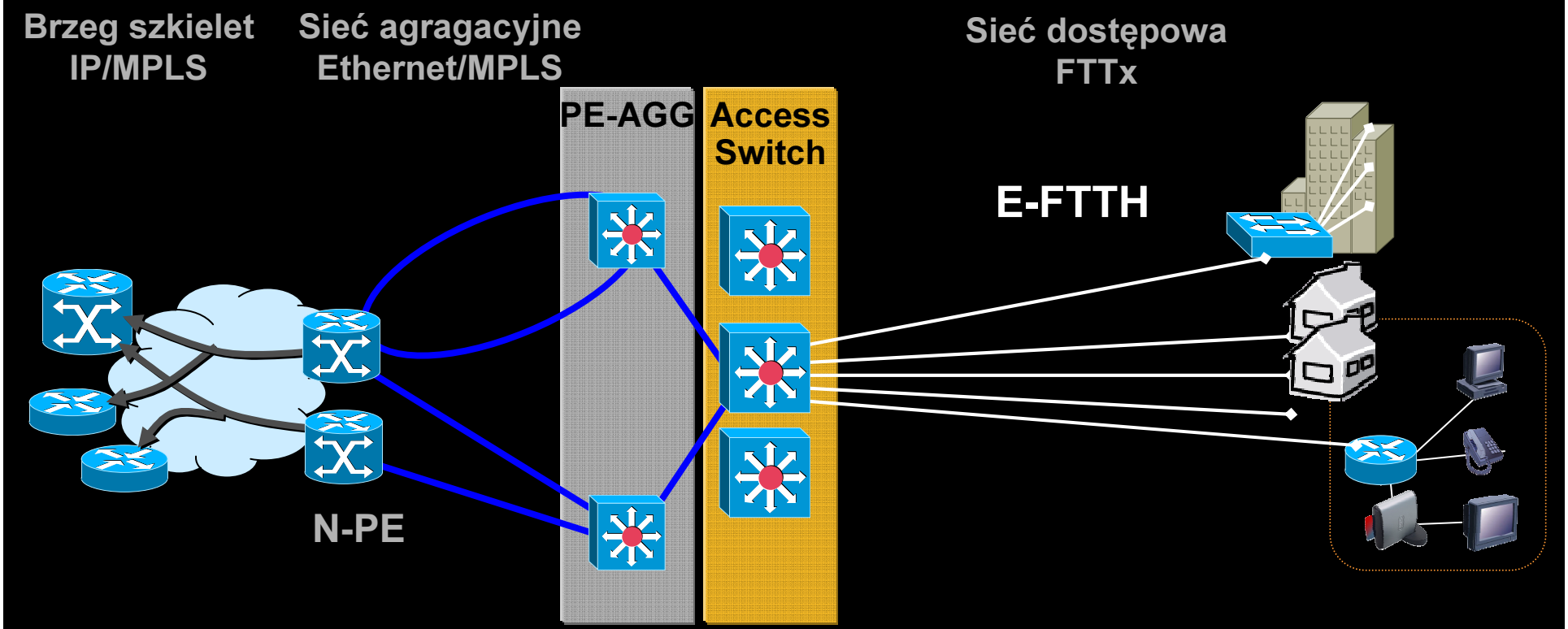
Lub jak wdrożyć FTTH jakby było siecią HFC



- Rynkiem docelowym dla D-PON są sieci typu „greenfield” gdzie operator używa zarządzania DOCSIS
- Rozwiązanie D-PON pozwala na przyszłościowy rozwój architektury zachowując aktualną infrastrukturę back-office

Rozwiązanie D-PON istnieje równolegle dla sieci HFC

Point-to-point Ethernet
Architektura



ETTx Point-to-point Ethernet
Cechy

- **Bezpośredni dostęp optyczny do klientów indywidualnych (np bloki mieszkalne, apartamenty)**
  - Przełączniki dostępowe w PoP operatora
- **Zbiorcze implementacje dla klientów indywidualnych, małych i dużych przedsiębiorstw**
  - Przełączniki dostępowe w piwnicach budynków; last drop poprzez kabel Cat5/6/7, swiatłowód, EoVDSL
- **Większa liczba światłowodów podłączonych do CO/POP niż w PON**
- **Elastyczna architektura, umożliwiająca nieograniczone pasmo**
- **Inwestycje w miare wzrostu sieci**
- **Migracja do nowych technologii lub wyzszych przepustowości następuje per abonent.**
- **Relatywnie tanie i proste CPE**

Agenda

- **Wstęp**

  (czyli czemu w ogóle mówimy o dostępie)

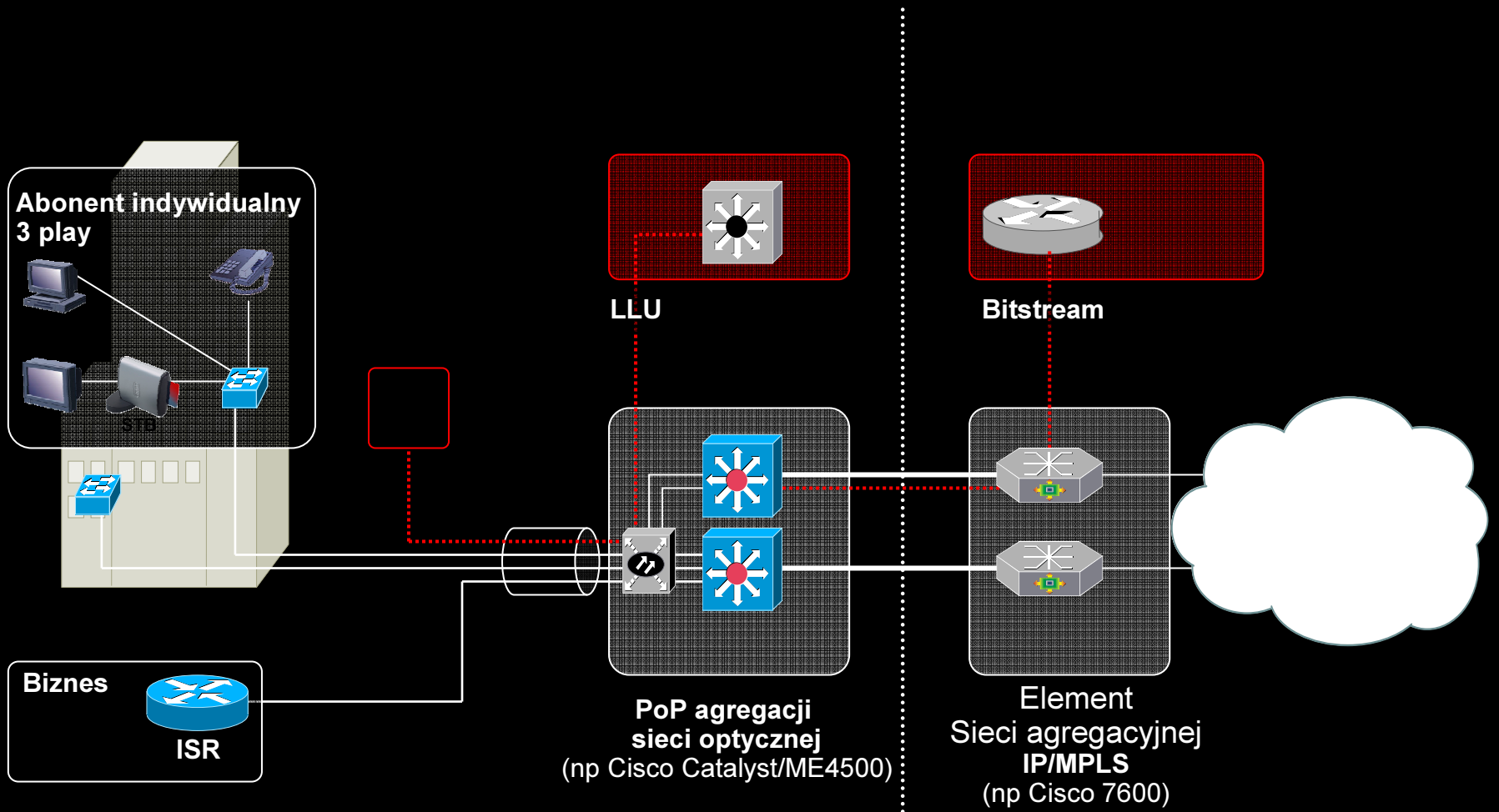
- **Technologie dostępowe**

  (czyli ktora jest lepsza, i dlaczego odpowiedz brzmi „to zależy”)

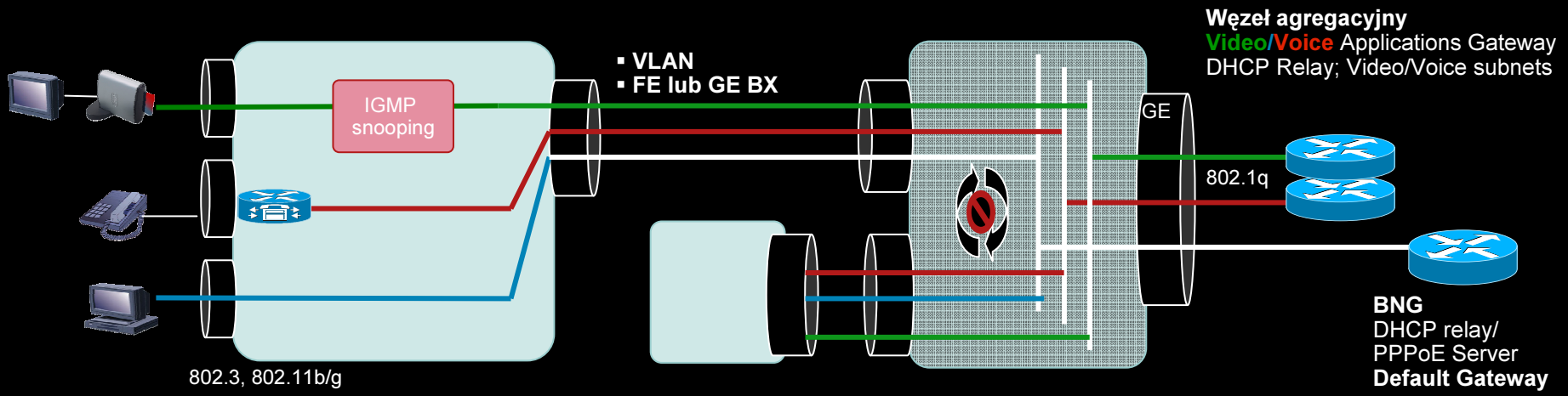
- **Architektura dostępowa w** *(ogólnych)* **szczegółach**

  (czyli jakie mechanizmy warto znać przy rozważaniu budowy sieci dostępowej)

ETTx
Model referencyjny



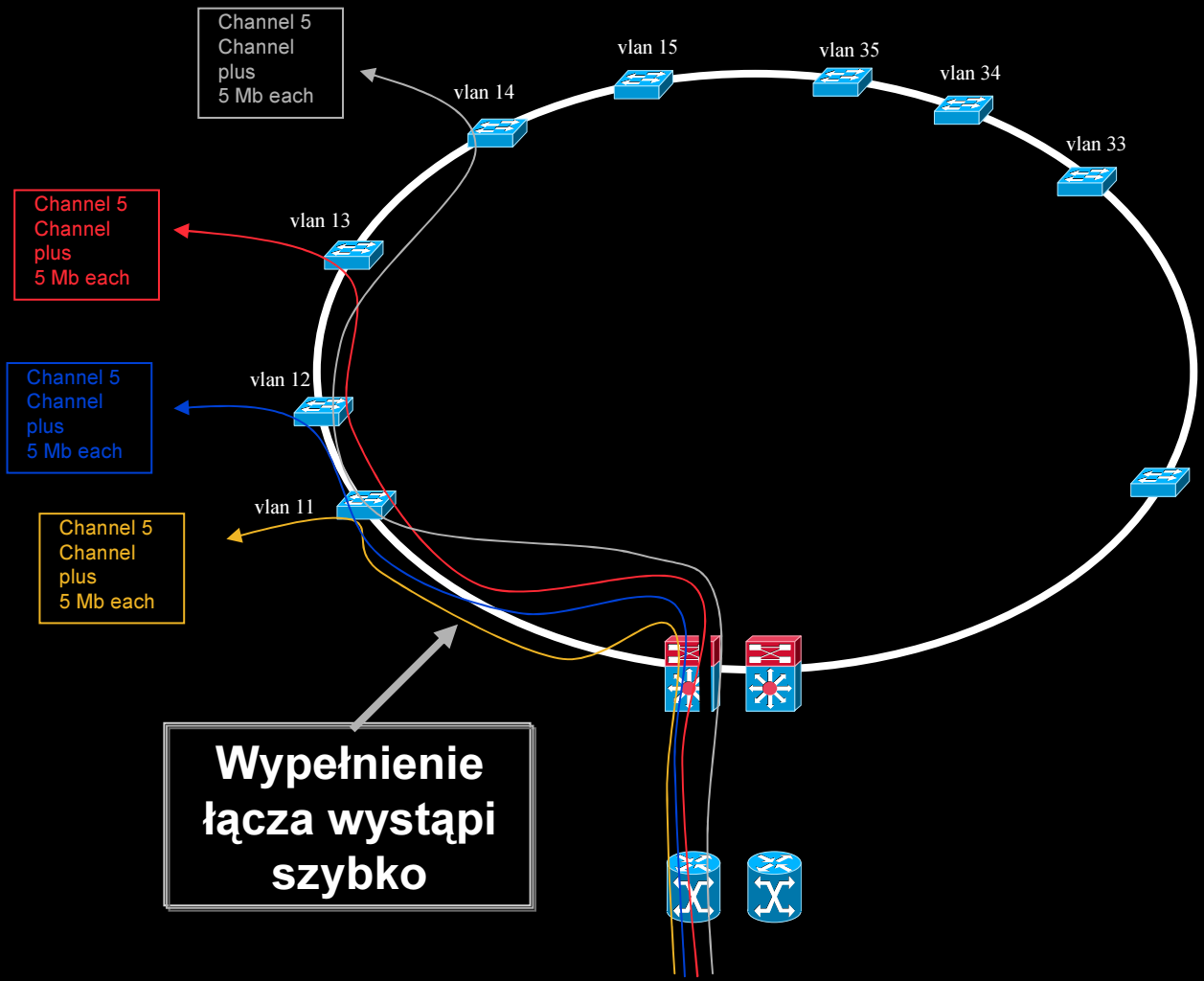
ETTx
Podłaczenie usług



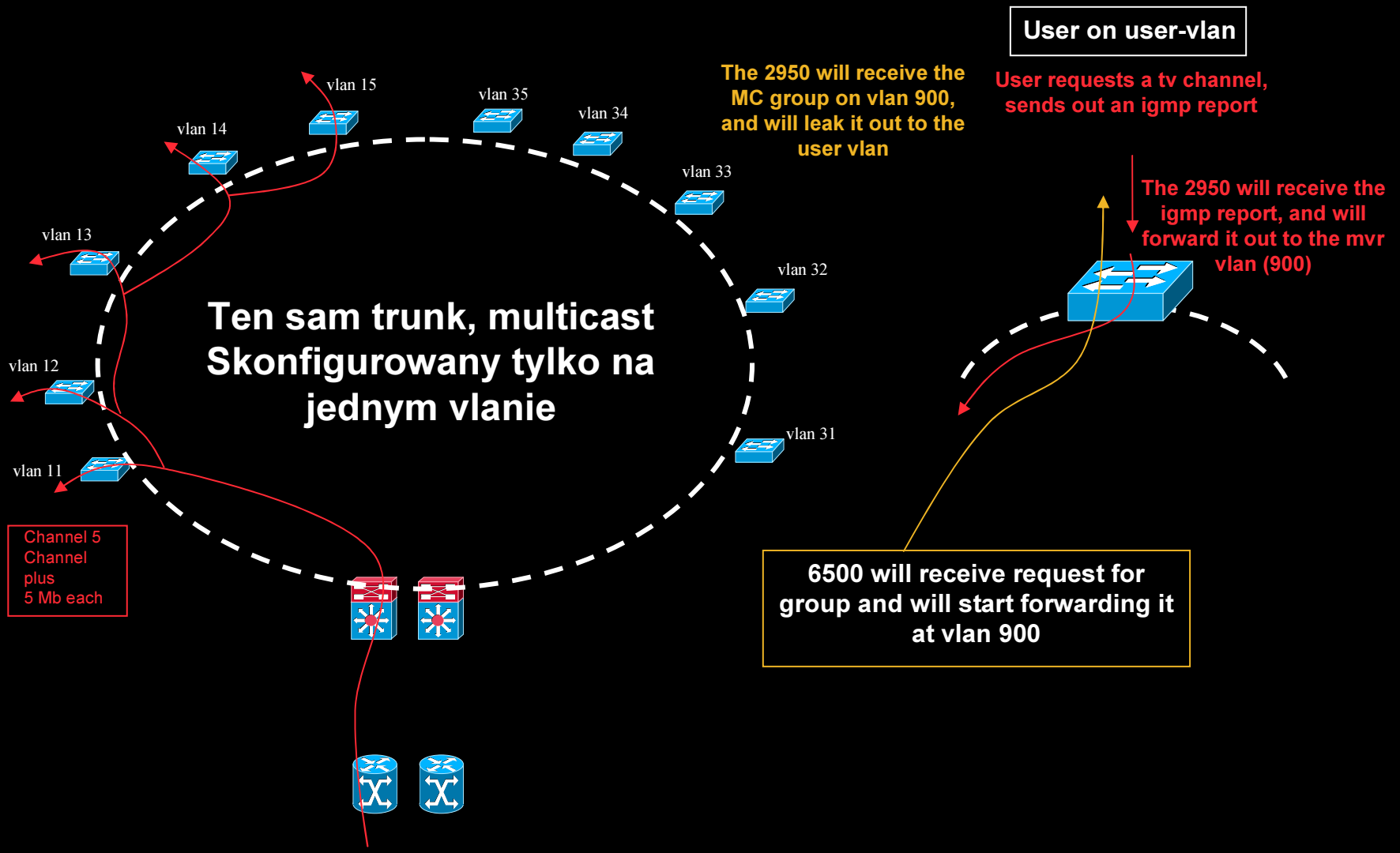
- **Podłaczenie i przełączanie usług**
  - Pojedyńczy VLAN per usługa
  - Ograniczone przełączanie na podst. MAC
  - IGMP Snooping
- **Priorytetyzacja usług**
  - Oparta na Class of Service

- **Podłaczenie i przełączanie usług**
  - Dostęp do internetu: przełączany do vlanu internet (model N:1)
  - Voice: przełączany do vlanu voice (model N:1)
  - Video: przełączany do vlanu video (model N:1)
- **Priorytetyzacja usług na styku UNI**
  - Oparta na Class of Service
- **Priorytetyzacja usług na styku NNI**
  - Oparta na Class of Service

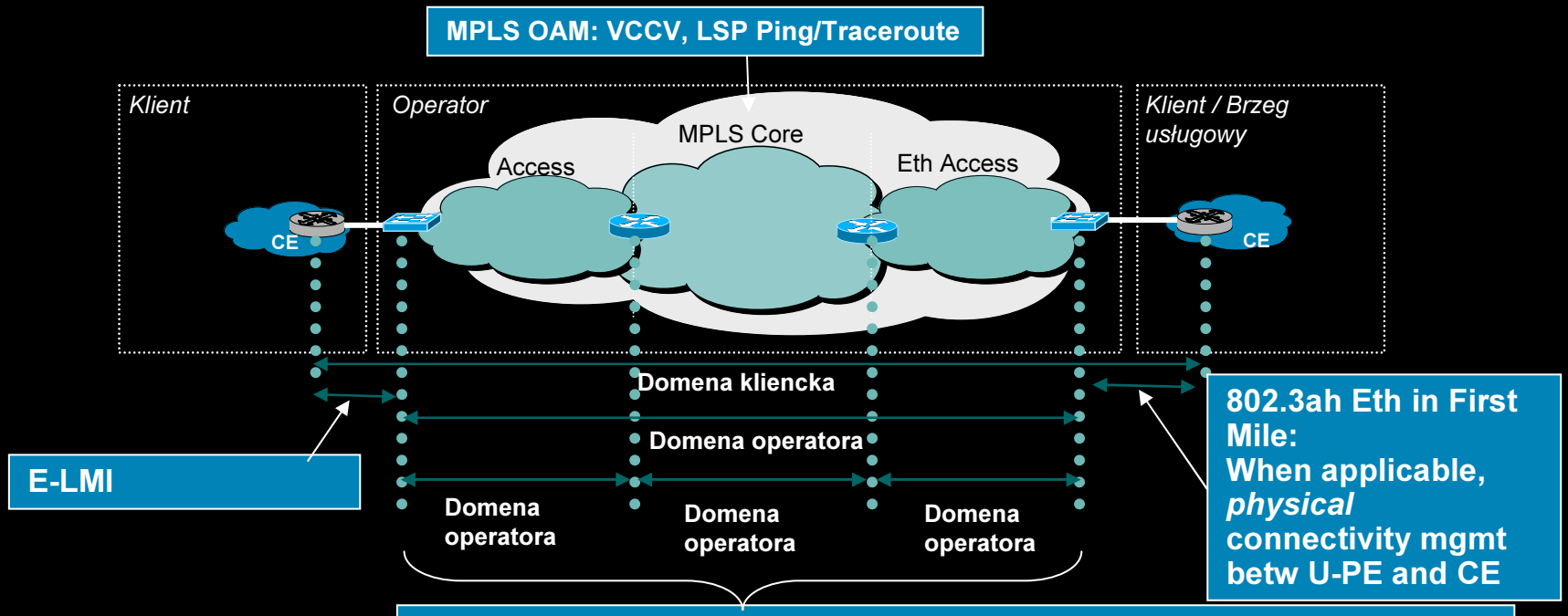
Multicast w ETTx – *problem?*
Typowa instalacja ETTx



Multicast w ETTx - *po problemie:*
MVR *(Multicast Vlan Registration)*



ETTx - utrzymanie
Zarządzanie jakością usług - Ethernet OAM

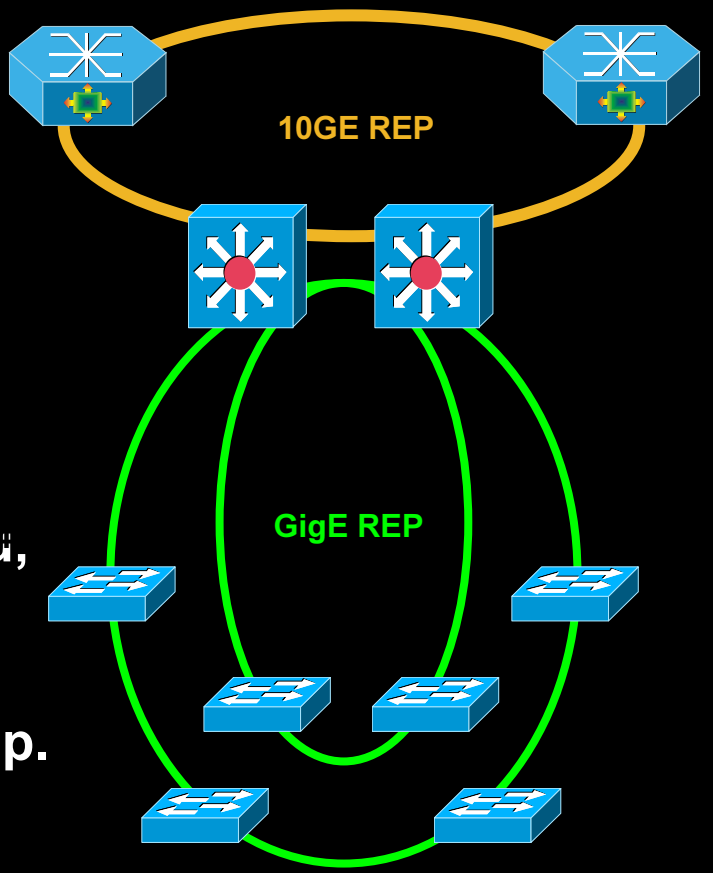


802.1ag - Kontrola połączeń

Zapewnia wykrywanie awarii i sprawdzanie działania usługi
- **Trzy rodzaje pakietów: Continuity Check, L2 Ping, L2 Traceroute**

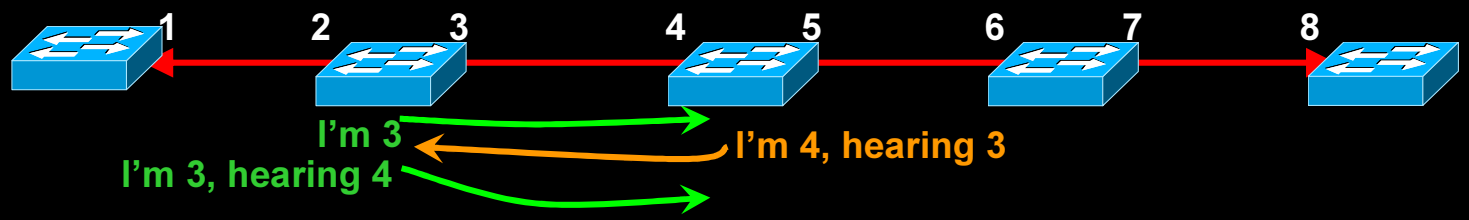
ETTx - dostępność
REP - Resilient Ethernet Protocol

- Zabezpieczenie pierścienia (< 200ms przerwy)
- GigE lub 10GE
- Bez Spanning Tree
- Sieć podzielona na segmenty, możliwa hierarchia segmentów
- Każdy z przełączników posiada informacje o topologii całego segmentu, relacje sąsiedztwa pomiędzy przełącznikami
- Możliwa współpraca ze spanning tree np. w nadrzędnych pierścieniach



ETTx - dostępność

REP Dostępność łącz sprawdzana *hop-by-hop*

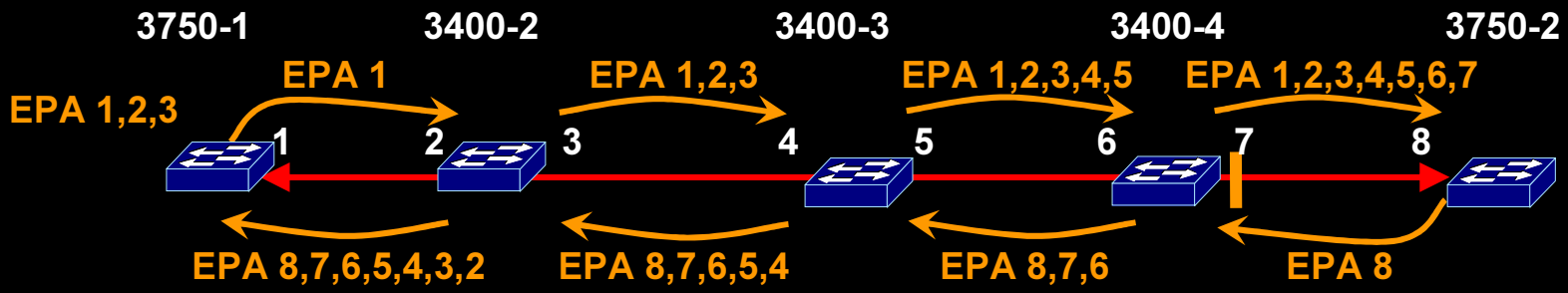


- Porty w segmencie wysylają hello na adres BPDU, i formują stosunki sąsiedztwa z przełącznikami z którymi są połączone bezpośrednio.
- Jesli sąsiedztwo jest wadliwe (sąsiad nie odpowiada, więcej niż jeden sąsiad, wtedy port jest umieszczany w stanie 'blocking'

ETTx - dostępność
REP – budowanie topologii

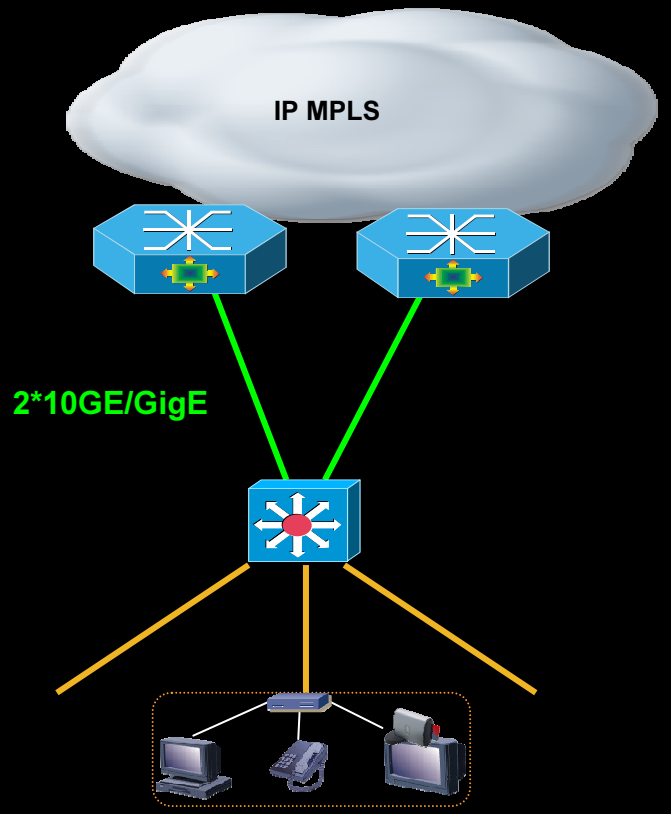
- Porty na obu końcach segmentu wysyłają End Port Advertisements (EPA) co 4 sekundy
- Te wiadmomości są przesyłane przez kolejne porty
- Poprzez agregację komunikatów EPA otrzymanych z każdej strony, port buduje baze o topologii segmentu

```
3750-1# show rep topology
REP Segment 1
BridgeName PortName Edge Role
---------------- ---------- ---- ----
3750-1 Gi1/1/1 Pri   Open
3400-2 Gi0/2         Open
3400-2 Gi0/1         Open
3400-3 Gi0/2         Open
3400-3 Gi0/1         Open
3400-4 Gi0/2         Open
3400-4 Gi0/1         Alt
3750-2 Gi1/1/2 Sec Open
```



ETTx – Dostępność
Redundancja połączeń – FlexLink+

- Zabezpieczenie w topologii Hub & Spoke (<200msec przerwy)
- GigE lub10GE
- Zabezpieczenie 1:1 z rozłożeniem ruchu



ETTx
Bezpieczeństwo

- *Dostępowa sieć ethernetowa działa tak samo jak korporacyjna, tylko więcej w niej potencjalnych atakujących*

- Rodzaje ataków w sieci ETTx:

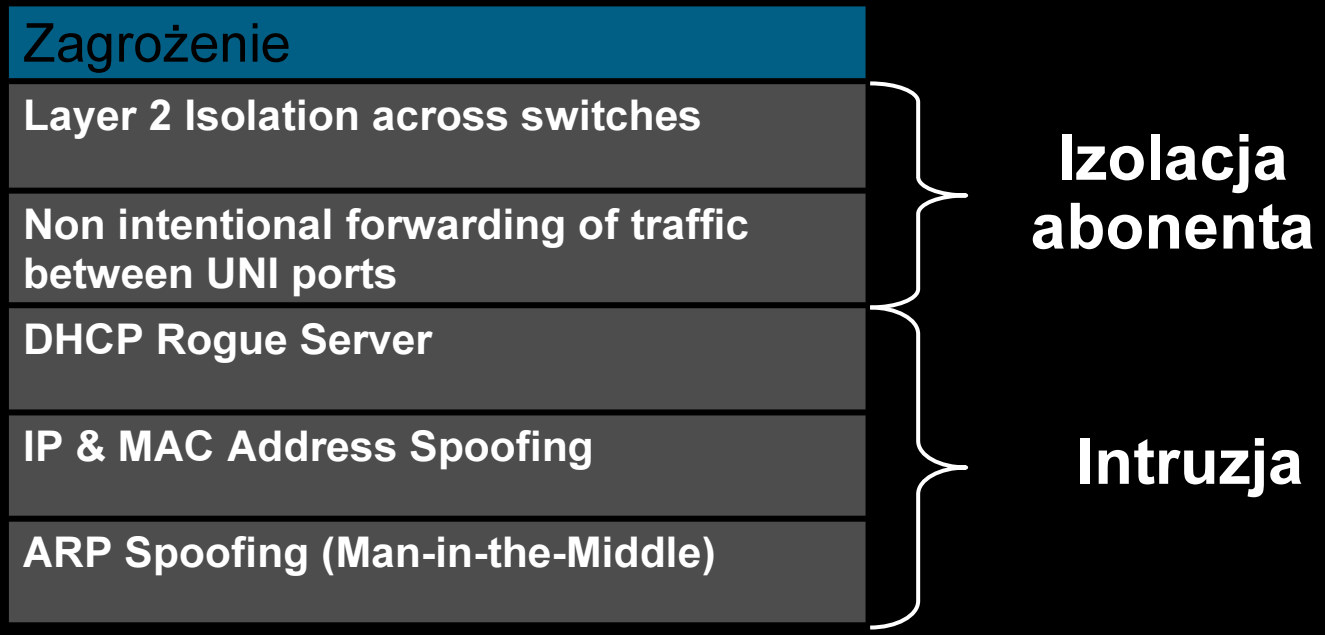
  Ataki na abonentów *(np. IP/MAC spoofing, ARP spoofing)*

  Ataki na przełączniki *(np. przepełnianie tablic MAC)*

  Ataki na infrastrukture *(np. man-in-the-middle dla ruchu zarządzającego)*

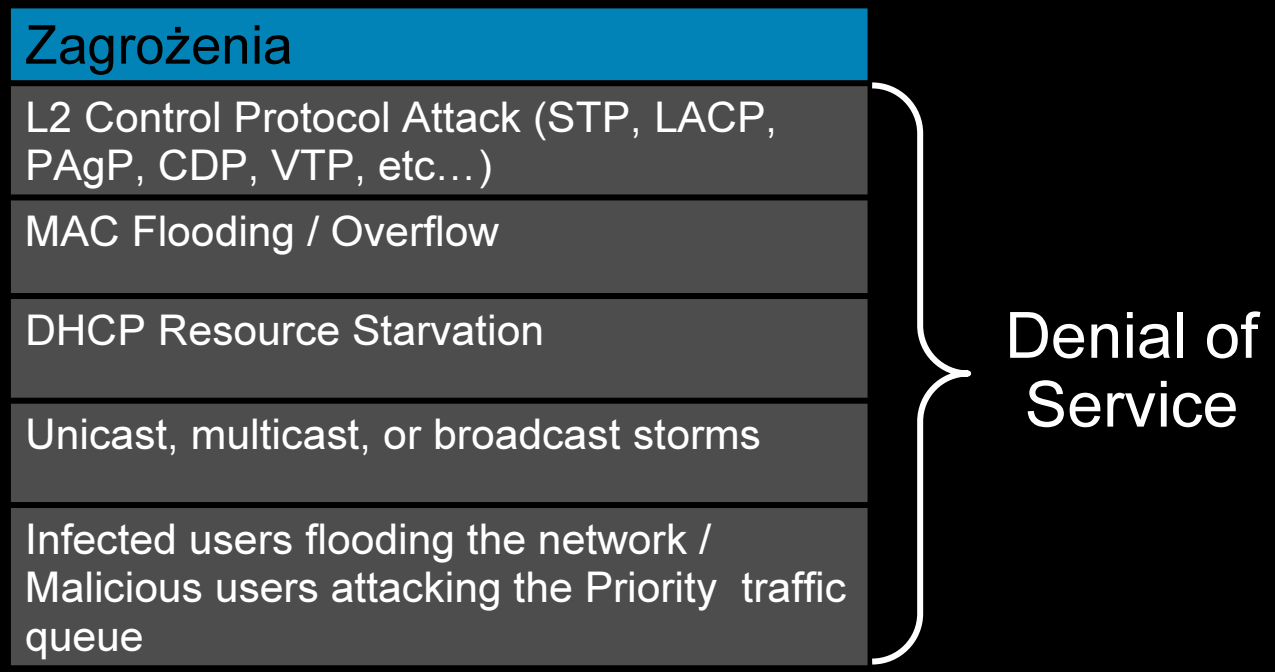
ETTx
Bezpieczeństwo abonentów

- Jednym z najważniejszych aspektów bezpieczeństwa w sieciach dostępowych jest zapobieganie wpływi jednego abonenta na drugiego



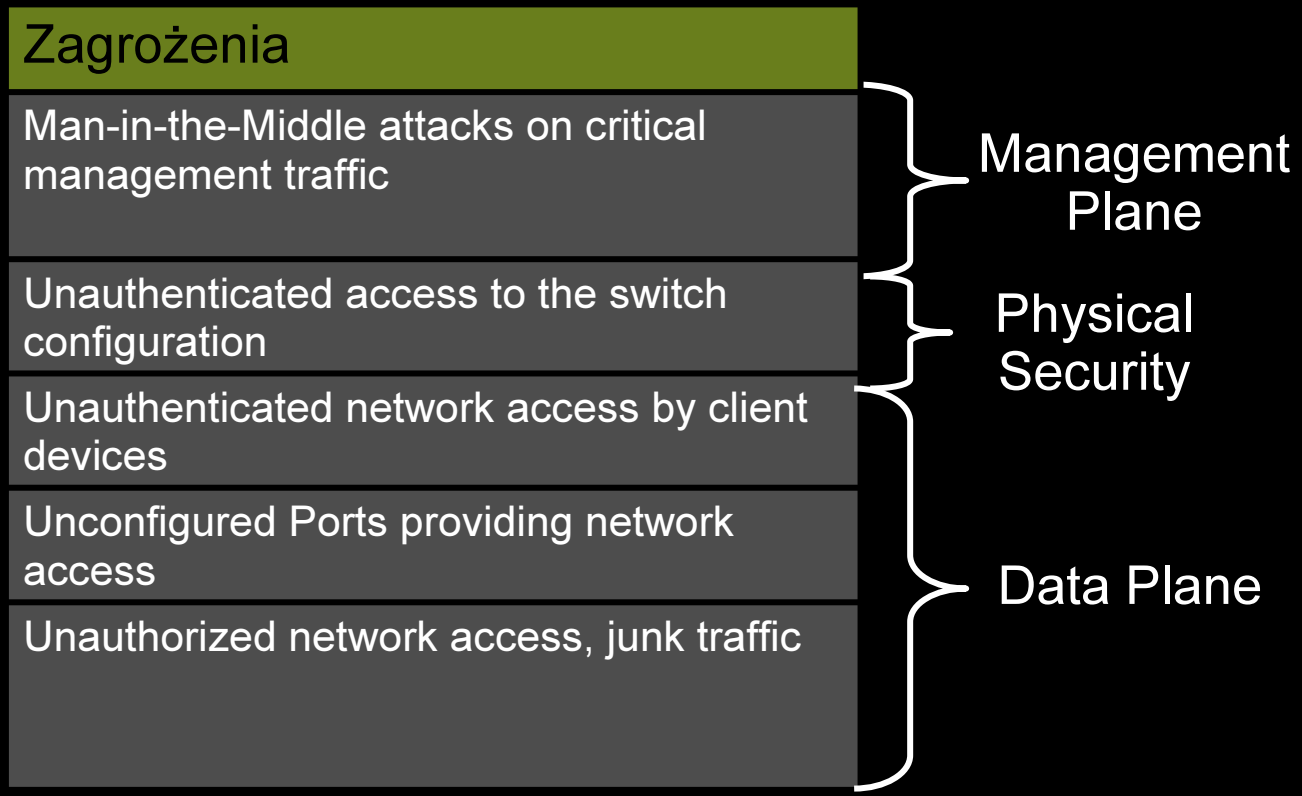
ETTx
Bezpieczeństwo przełączników

- Najczęściej spotykane ataki na przełączniki to ataki typu DoS

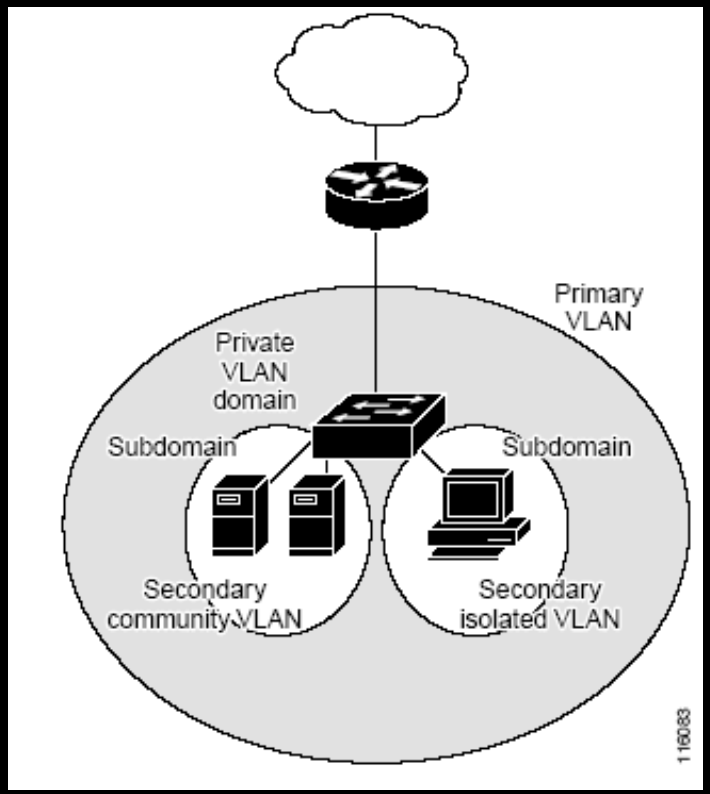


ETTx
Bezpieczeństwo infrastruktury

- Ataki infrastrukturalne wykorzystują słabość data, control plane i warstwy zarządzania a także fizyczne bezpieczeństwo



Bezpieczeństwo abonentów
Private VLAN



Działanie:

- Zapewnienie izolacji pomiędzy portami należącymi do tego samego vlanu
- Dwa rodzaje vlanów:
  - Isolated VLAN – porty nie mogą się ze sobą komunikowac na L2.
  - Community VLAN – Porty w ramach community mogą komunikować się ze sobą ale nie moga z innimi portami w innych communities

Zysk:

- Zapewnienie separacji L2

Bezpieczeństwo abonentów
Private VLAN - konfiguracja

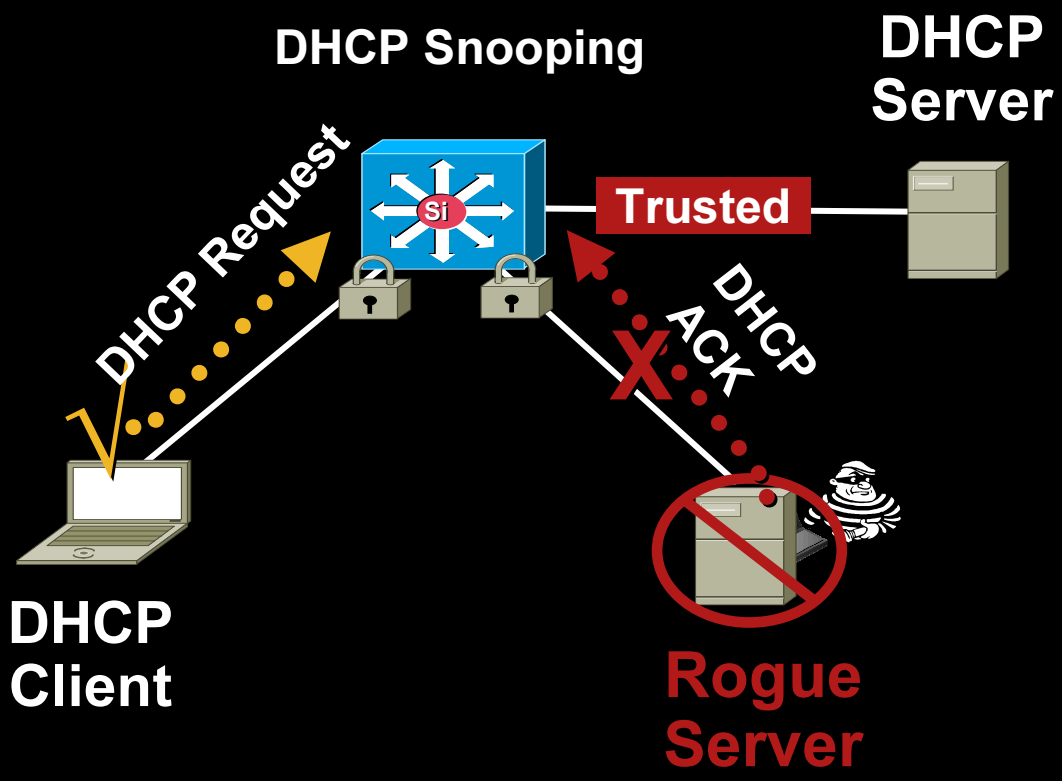
Przykład:

```
(config)vlan 10
(config-vlan) uni-vlan isolated
(config-vlan) vlan 20
(config-vlan) uni-vlan community
```

```
Switch#sh vlan uni-vlan type

Vlan Type
---- ----------------
10   UNI isolated
20   UNI community
```

Bezpieczeństwo abonentów
DHCP Snooping



Działanie:
Przełączanie tylko request'ów DHCP z portów untrusted, pozostałe rodzaje ruchu DHCP są blokowane

- Pozwala na relay pakietów DHCP tylko portom zaufanym
- Buduje tablice 'DHCP binding' zawierającą adres IP, MAC, port, VLAN klienta

Zysk:
- Eliminuje możliwość działania nieautoryzowanych serwerów DHCP

Bezpieczeństwo abonentów
DHCP Snooping

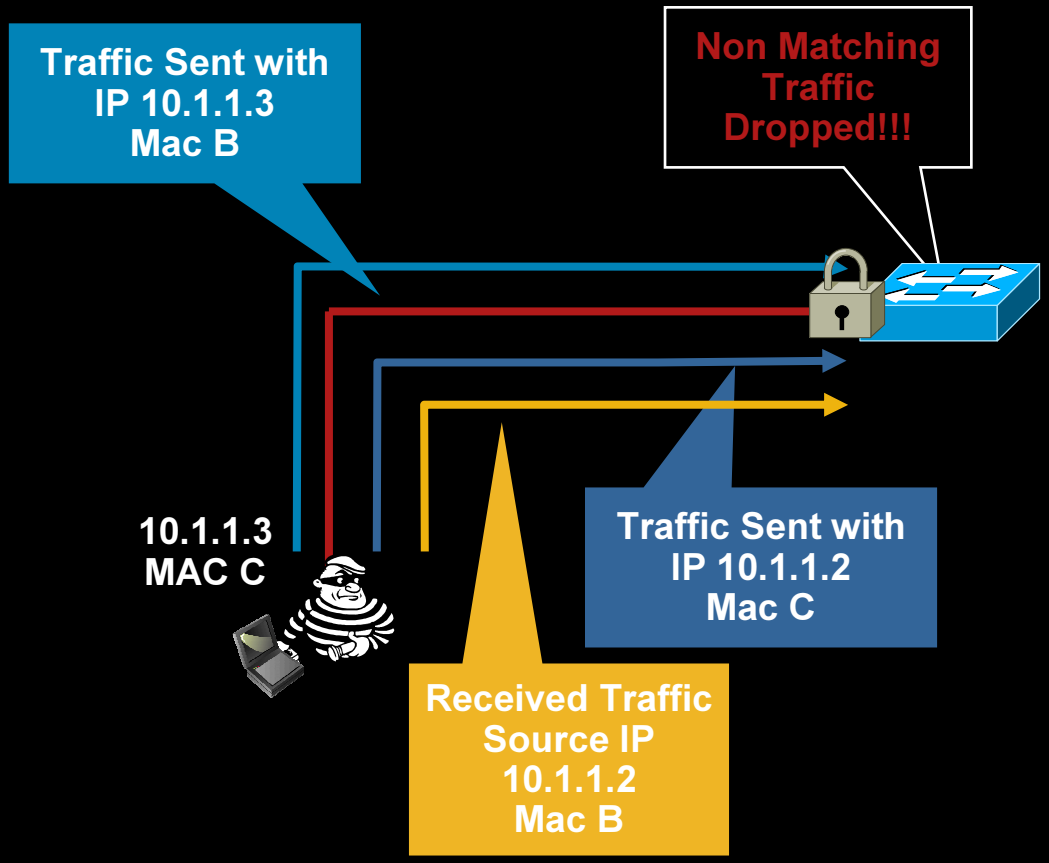
DHCP Snooping Binding Table

```
sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:03:47:B5:9F:AD   10.120.4.10      193185      dhcp-snooping  4     FastEthernet3/18
```

- Wpisy pozostają w tablicy do zakończenia dhcp lease
- Tablica może być zapisana na bootflash, ftp, rcp, slot0, tftp

```
ip dhcp snooping database tftp://172.26.168.10/tftpboot//4500-dhcpdb
ip dhcp snooping database write-delay 60
```

Zabezpieczenie przed atakami spoofingowymi
IP Source Guard



- IP SG łączy adres IP, MAC, VLAN, Port klienta

Działanie:

- Wykorzystanie tablicy DHCP snooping
- Jeśli klient otrzymał adres IP z DHCP przełącznik blokuje cały ruch wysyłany z portu klienta z innymi adresami IP

Zysk:

- Uniemożliwia klientowi używania adresu, ktory nie jest do niego przypisany.

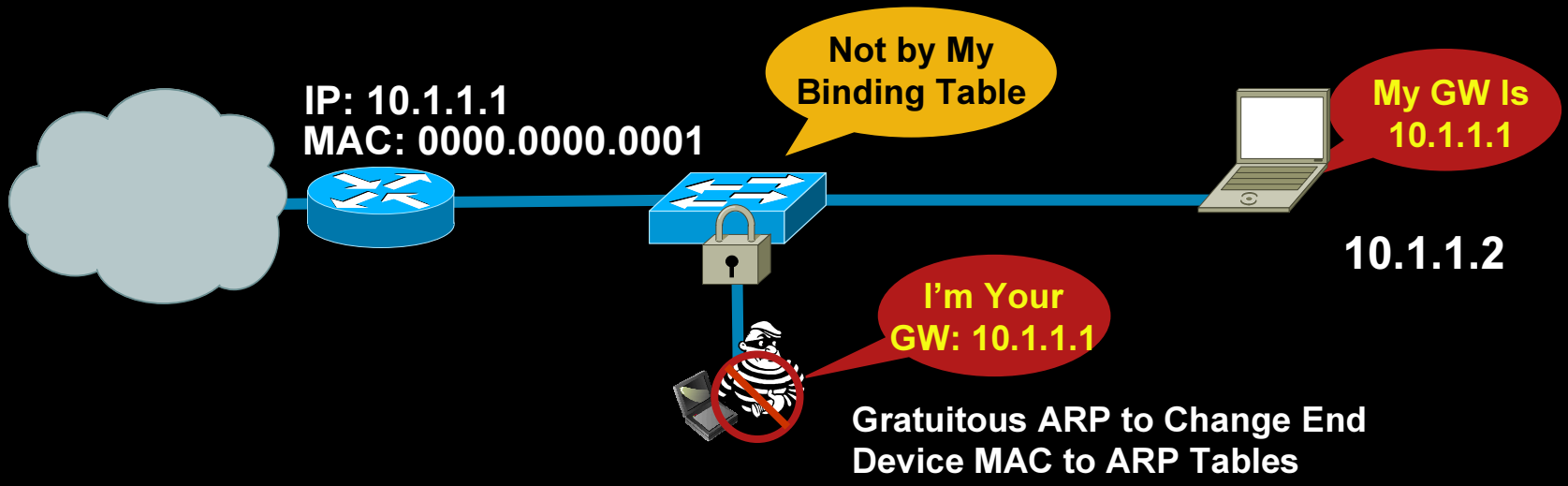
Zabezpieczenie przed atakami ARP
Dynamic ARP Inspection

Działanie

- Inspekcja pakietów ARP – kasowanie pakietów z niewłaściwym mapowaniem IP-do-MAC
- Wykorzystuje tablice DHCP binding, tworzoną automatycznie przy przejściu pakietu DHCP-offer przez przełącznik

Zysk:

Efektywnie blokuje ataki typu “man-in-the-middle” i “ARP Spoofing”



Zabezpieczenie przed atakami ARP
Dynamic ARP Inspection

IOS
Global Commands
```
ip dhcp snooping vlan 4,104
no ip dhcp snooping information option
ip dhcp snooping
ip arp inspection vlan 4,104
ip arp inspection log-buffer entries 1024
ip arp inspection log-buffer logs 1024 interval 10
```
Interface Commands
```
ip dhcp snooping trust
ip arp inspection trust
```

IOS
Interface Commands
```
no ip arp inspection trust (default)
ip arp inspection limit rate 15 (pps)
```

Zabezpieczenie przed atakami ARP
Dynamic ARP Inspection - wpisy statyczne
(gdy nie ma w sieci serwera DHCP)

IOS
Global Commands
```
ip source binding 0000.0000.0001 vlan 4 10.0.10.200 interface fastethernet 3/1
```

IOS
Show Commands
```
show ip source binding
```

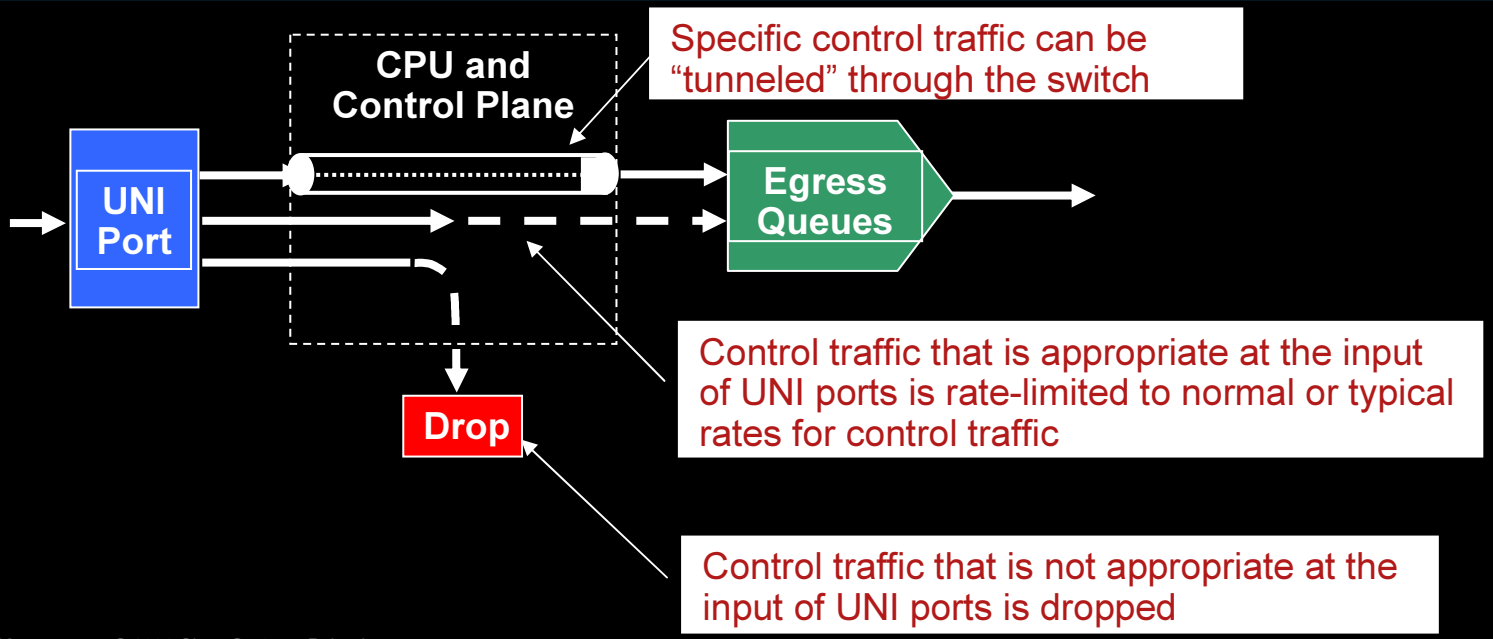
Zabezpieczenie przełączników
Control Plane Security

Działanie

- **By default**, wszystkie pakiety kontrolne protokołów STP, VTP, CDP, DTP, PAgP and LACP są kasowane na UNI
- W niektórych sytuacjach można tunelować i ograniczać pakiety dochodzące do CPU

Zysk:

- Zapewnia zabezpieczenie przed atakami DoS z wykorzystaniem pakietów kontrolnych



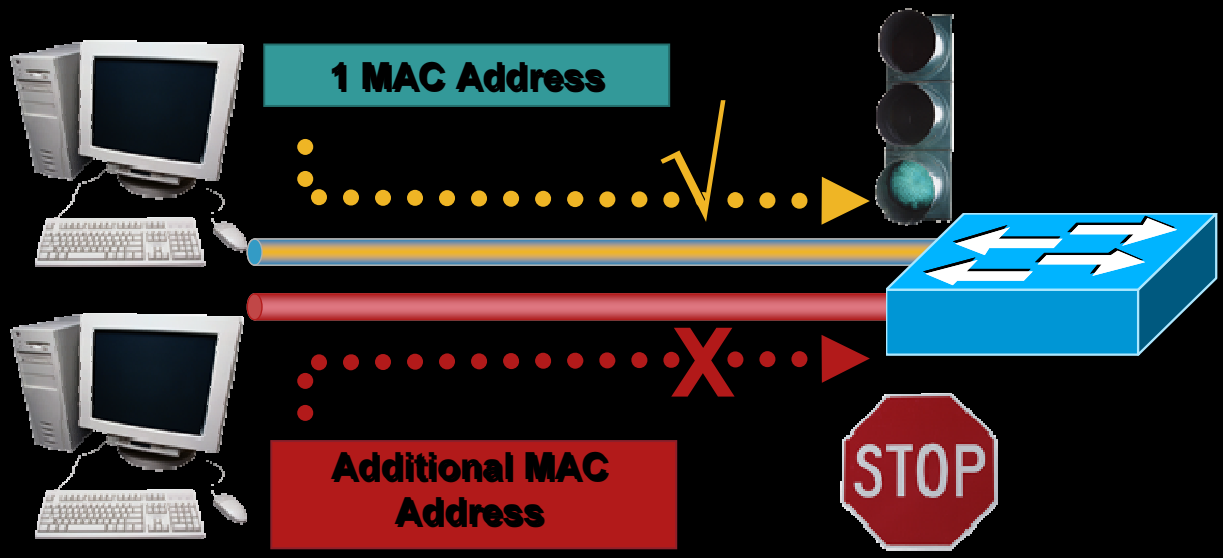
Zabezpieczenie przed MAC floodingiem
Port Security

Działanie:

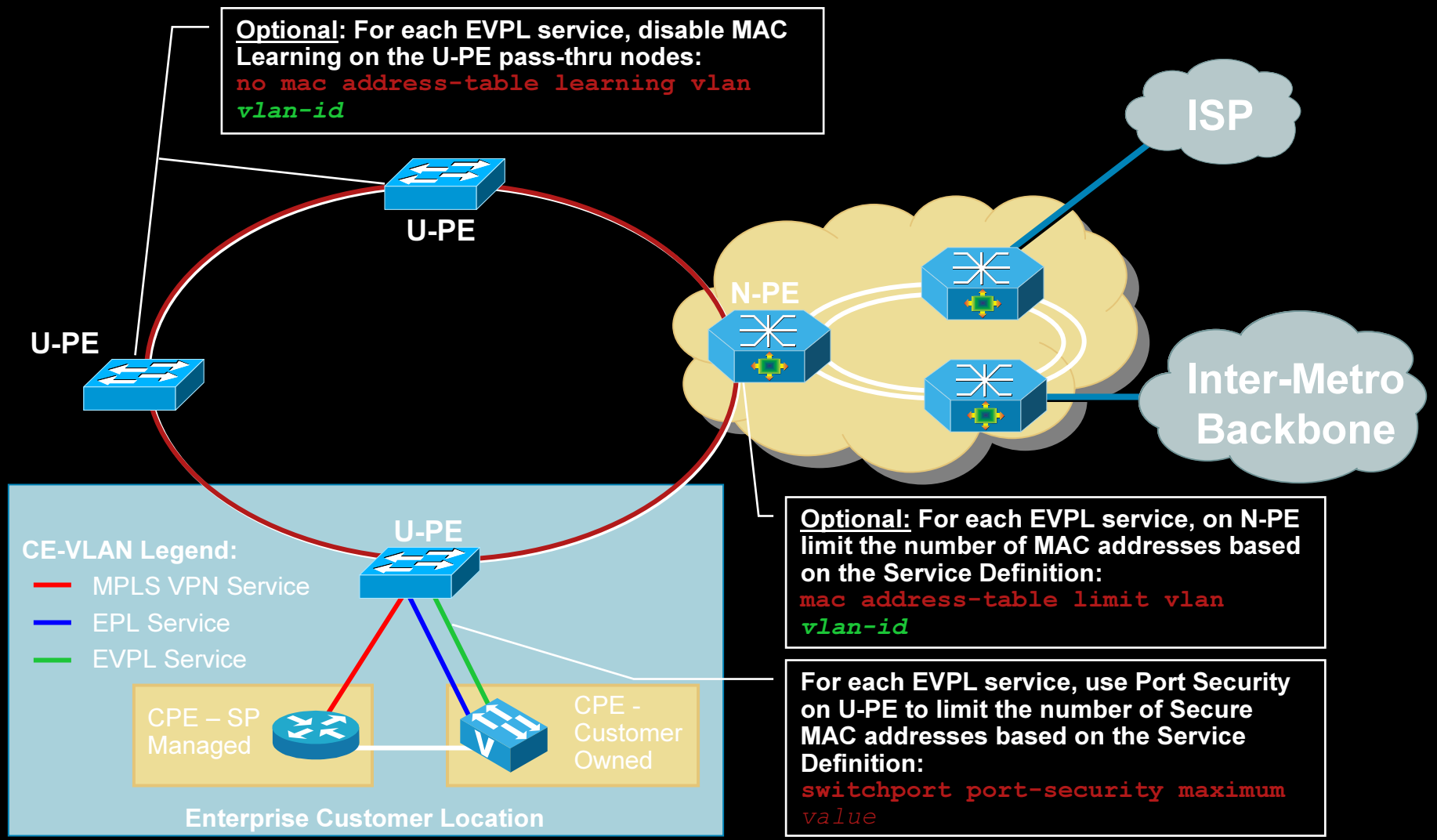
- Ograniczenie ilości adresów MAC na interfejsach

Zysk:

- Zabezpieczenie przed atakami MAC Flooding
- Zapewnia że tylko autoryzowani abonenci mogą korzystać z usług *(secure MAC entries)*



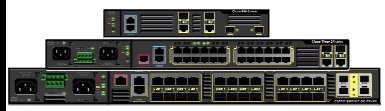
Zabezpieczenie przed MAC floodingiem
Port Security i per VLAN mac learning



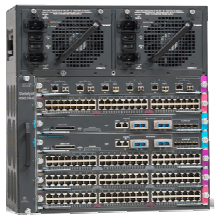
Dodatkowe mechanizmy

- **Zabezpieczenie Spanning Tree** – rootguard, bpdu guard
- **Zapobieganie zalewaniu ruchem:** storm control
- **Bezpieczeństwo fizyczne** - „password recovery disable”
- **Zarządzanie poprzez SSH, SNMPv3 żeby uniknąć ataków typu man-in-the-middle**

Cisco ETTx – platformy sprzętowe
Przełączniki Cisco serii ME *(1/3)*

Cisco ME2400		Usługi L2	ETTx, *UPE, CPE*
Cisco ME3400		Usługi L2/3	ETTx *UPE, CPE, IED*
Cisco ME3400E		Usługi L2/3	ETTx *UPE, CPE, IED*
Cisco ME3750		Usługi premium L2/3 z hQoS i MPLS	ETTB *UPE, CPE*

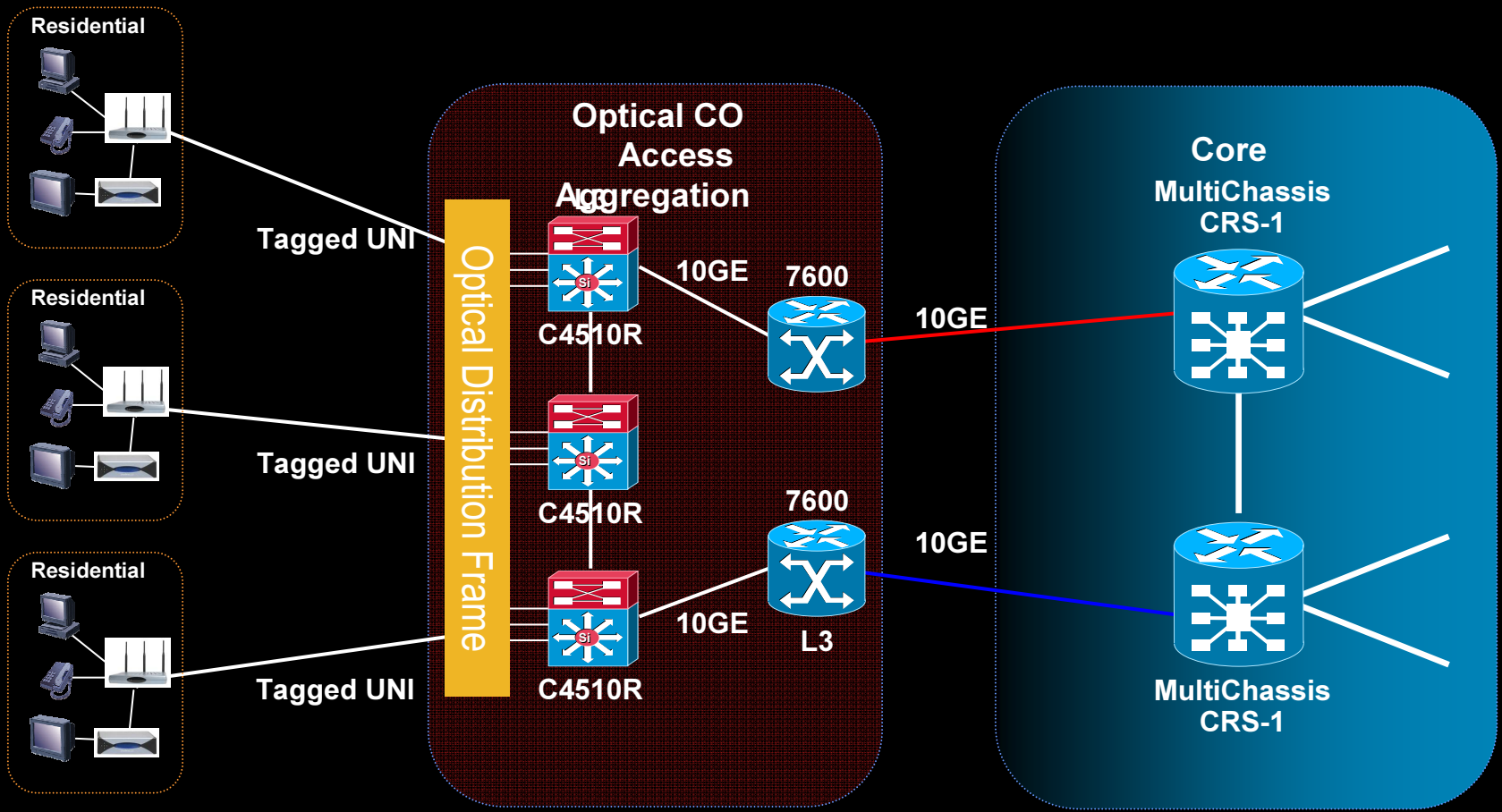
Cisco ETTx - platformy sprzętowe
Przełączniki Cisco serii ME *(2/3)*

Cisco Cat / ME 4500		Usługi L2/L3, multicast L3, HQoS	ETTx, *UPE*
Cisco ME4924-10GE		Usługi L2/L3, multicast L3	ETTx, *UPE*
Cisco 4948-10GE		Usługi L2/L3, multicast L3	ETTx, *UPE*
Cisco 4900M		Usługi L2/L3, multicast L3, IPv6	ETTx, *UPE*
Cisco ME6528		Usługi L2/L3, multicast L3, MPLS, EoMPLS, L3VPN, IPv6	ETTx, *UPE*

Cisco ETTx - platformy sprzętowe
Przełączniki Cisco serii ME *(3/3)*

- Opracowane z myślą o rynku operatorów telekomunikacyjnych
- Lista funkcjonalności przygotowana pod implementacje w sieci operatorskiej *(ograniczone funkcje czysto enterprise, wsparcie sprzętowe dla funkcji SP)*
- Bezpieczeństwo – mechanizmy zapewniające bezpieczeństwo abonentom, oraz zabezpieczenie urządzeń przed atakami
- Mechanizmy dostępności: REP – Resilient Ethernet Protocol, FlexLink
- Zarządzanie: E-OAM, IP SLA

Cisco ETTx
Przykład implementacji *(duży francuski operator)*



szreter@cisco.com