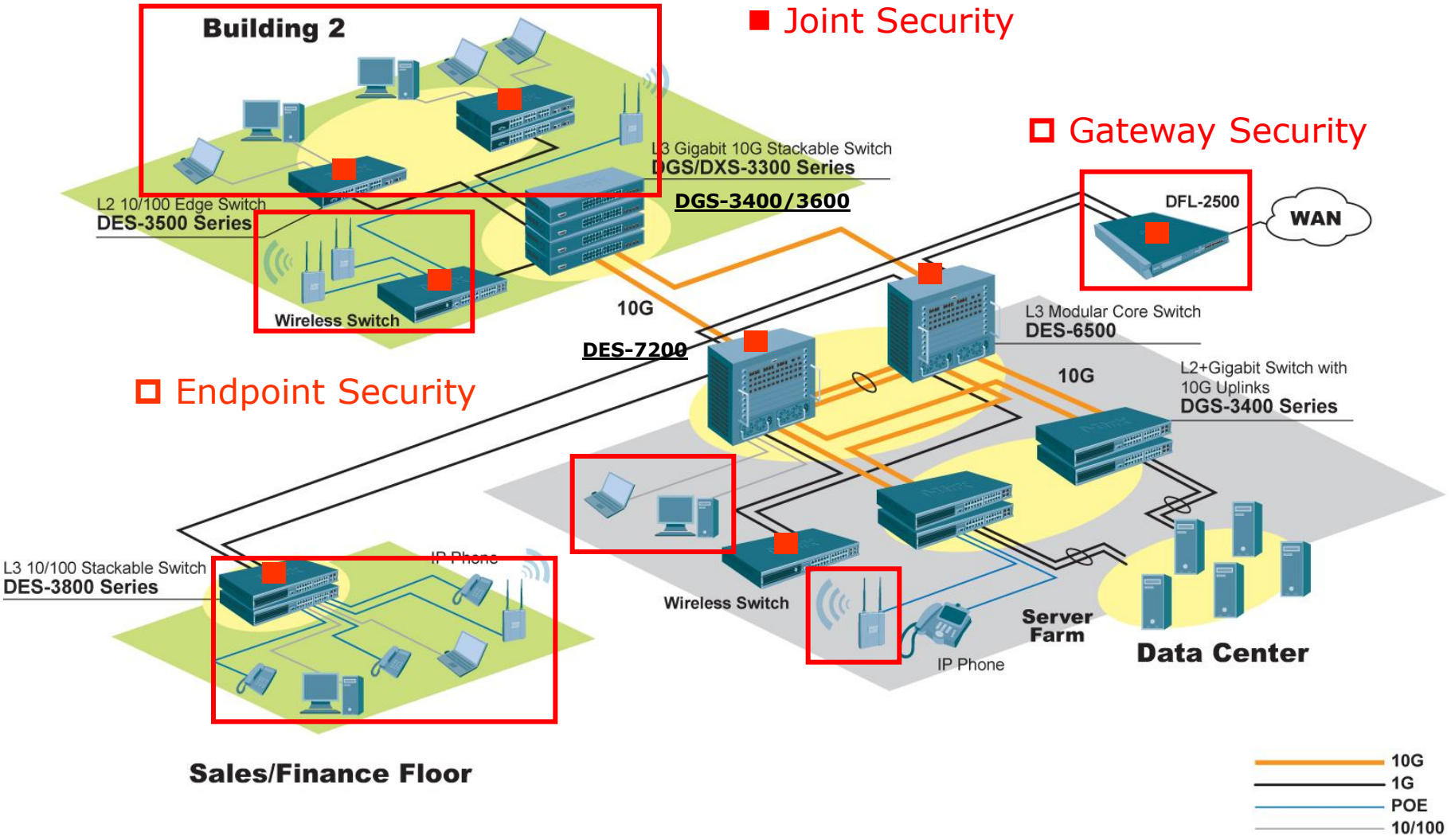
D-Link Business

Rozwiązania sieciowe dla dostawców usług telekomunikacyjnych i multimedialnych

Marcin Wójcik
PreSales Engineer
D-Link (Polska)

End-to-End Security (E2ES)



Przełączniki - portfolio

Features

DES-7200 Series

XSTACK

DES-3500 / DES3800 / DGS-3400 / DGS-3600 Series

Chassis Switches

- 6 / 10 Slots
- 10/100, Gigabit & 10G Ethernet
- 19" Rack Mountable Chassis
- Modular Resiliency
- Advanced IP Route
- IPv6 Support
- Maximum Network Uptime
- Comprehensive Security Features
- Application Awareness Enabled
- Comprehensive QoS Control
- Full Management Featured

DES-3000 / DGS-3100 Series

xStack Switches

- 24/ 48 Port
- 10/100, Gigabit & 10G Ethernet
- 19" Rack Mountable
- L2+/ L3+
- Full Management Featured
- D-Link SIM Support
- Complete Security Features
- Comprehensive QoS Control
- Safeguard Engine embedded
- ZoneDefense with NetDefend Firewall

DES / DGS-1200 Series

Entry-Level Managed Switches

- 8* /16 / 24 / 48 Port
- 10/100 Mbps & Gigabit Ethernet
- 11" * / 19" Rack Mountable
- Web / CLI / SNMP Manageable
- Single IP Management *
- Physical Stacking **

DES/DGS-1000

Web Smart Switches

- 16 / 24 / 48 Ports
- 10/100 Mbps & Gigabit Ethernet
- 19" Rack Mountable
- Web Manageable
- Unmanaged price / Management features

Unmanaged Switches

- 5/ 8/ 16/ 24/ 48 port
- 10/100 & Gigabit Ethernet
- Quality & Stable
- Desktop size, 11"/ 19" rack mountable
- Cable Diagnostic Support
- Green Ethernet for Gigabit

dlinkgreen

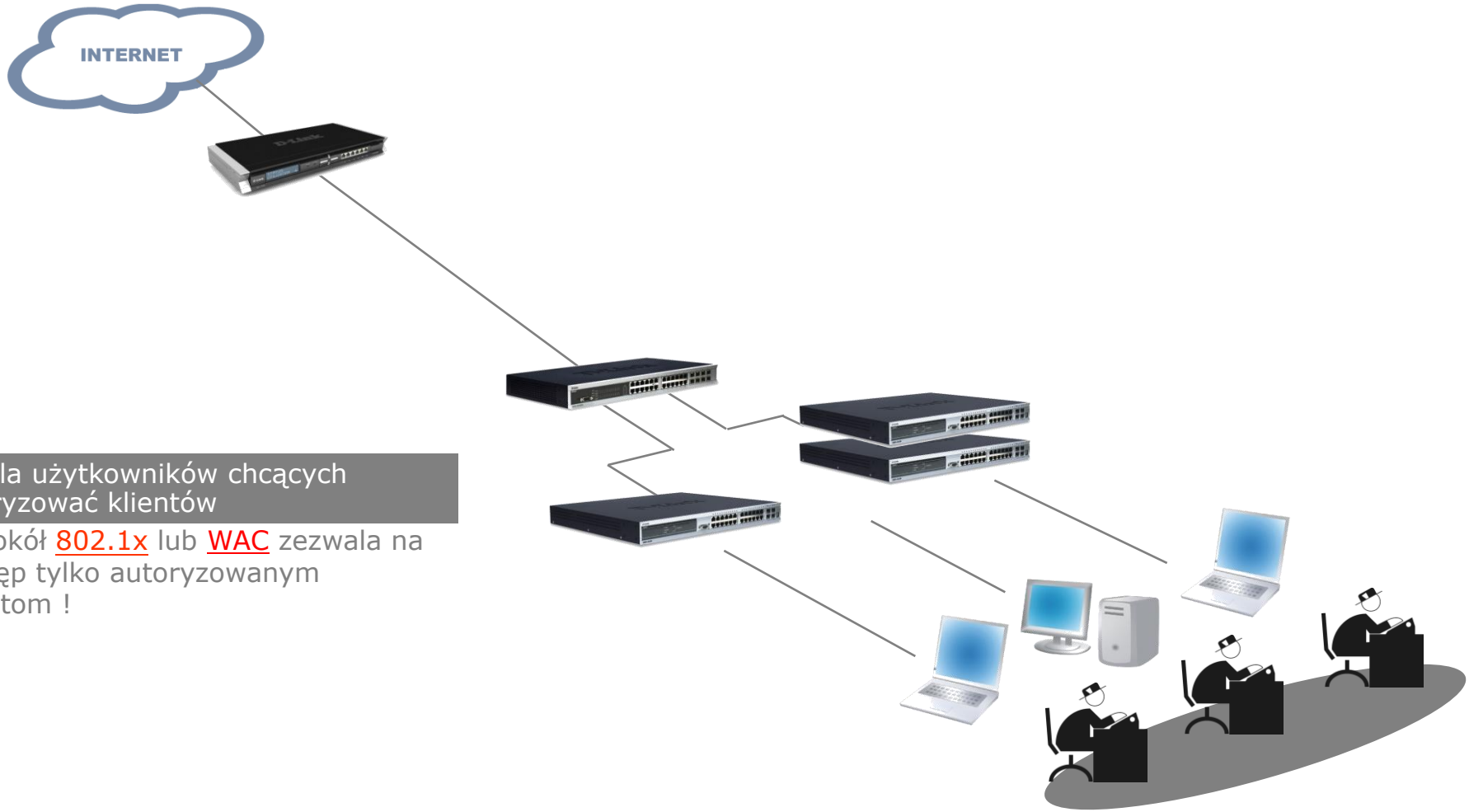
DGS-3200

Network Complexity

dlinkgreen

D-Link
Building Networks for People

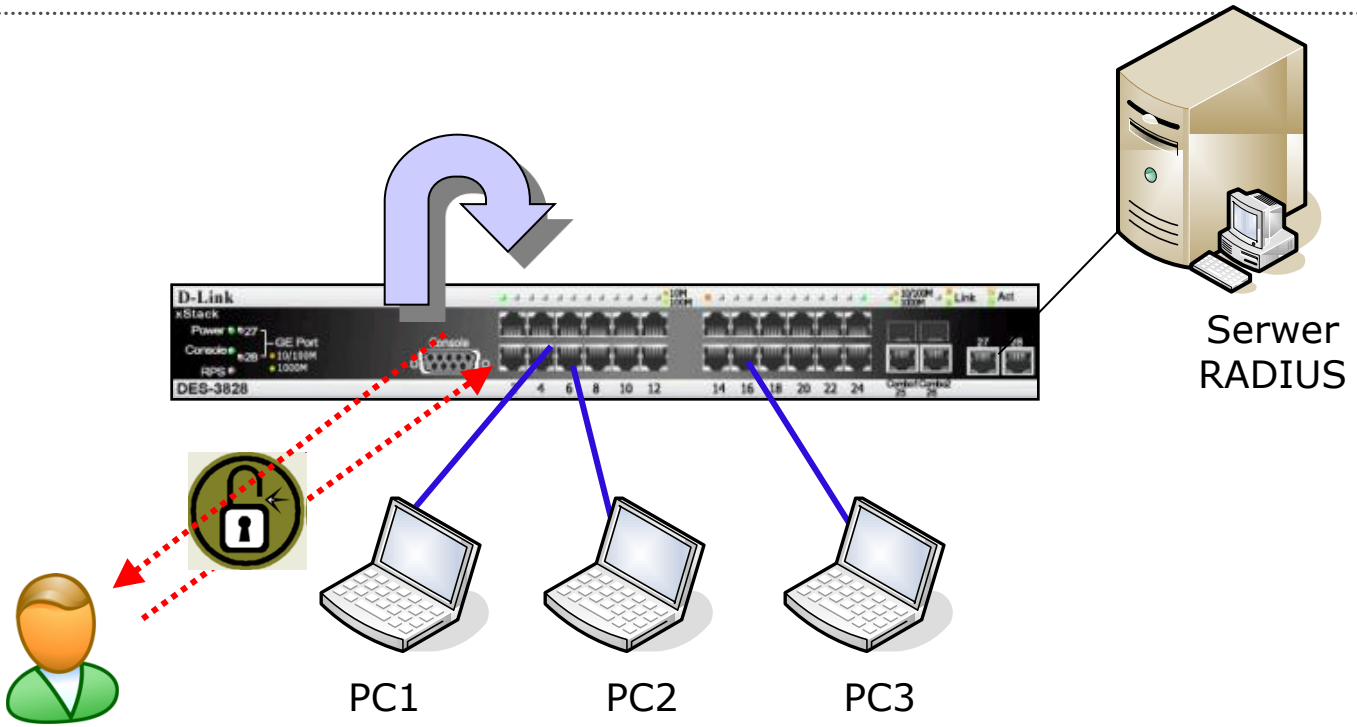
Zintegrowany system ochrony sieci



#1 Dla użytkowników chcących autoryzować klientów

Protokół 802.1x lub WAC zezwala na dostęp tylko autoryzowanym klientom !

Uwierzytelnianie 802.1x



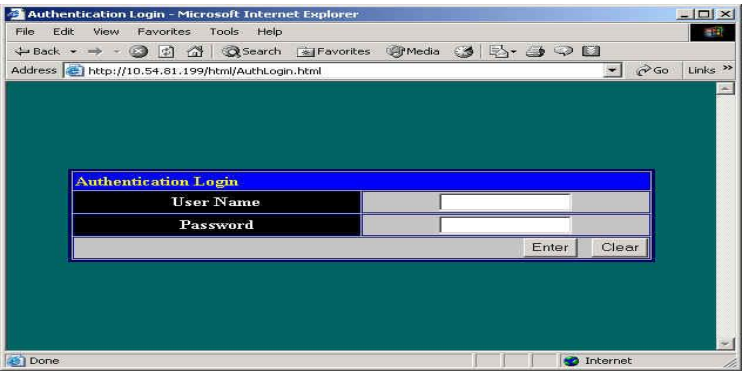
użytkownik korzysta z klienta 802.1x

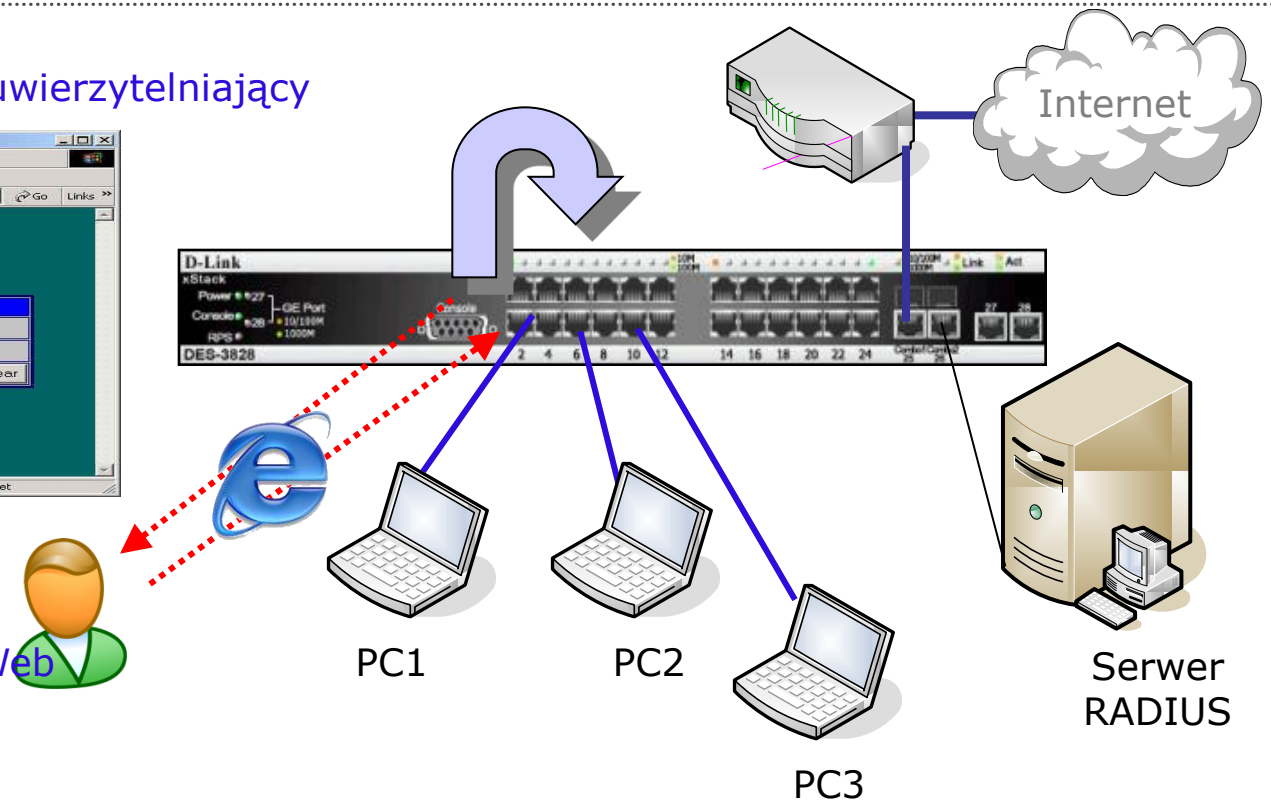
Użytkownik musi posiadać zainstalowaną aplikacje uwierzytelniającą (klienta 802.1x)

Możliwość współdziałania z funkcjonalnością Guest VLAN

Web-Based Access Control (WAC)

2. przełącznik wyświetla ekran uwierzytelniający

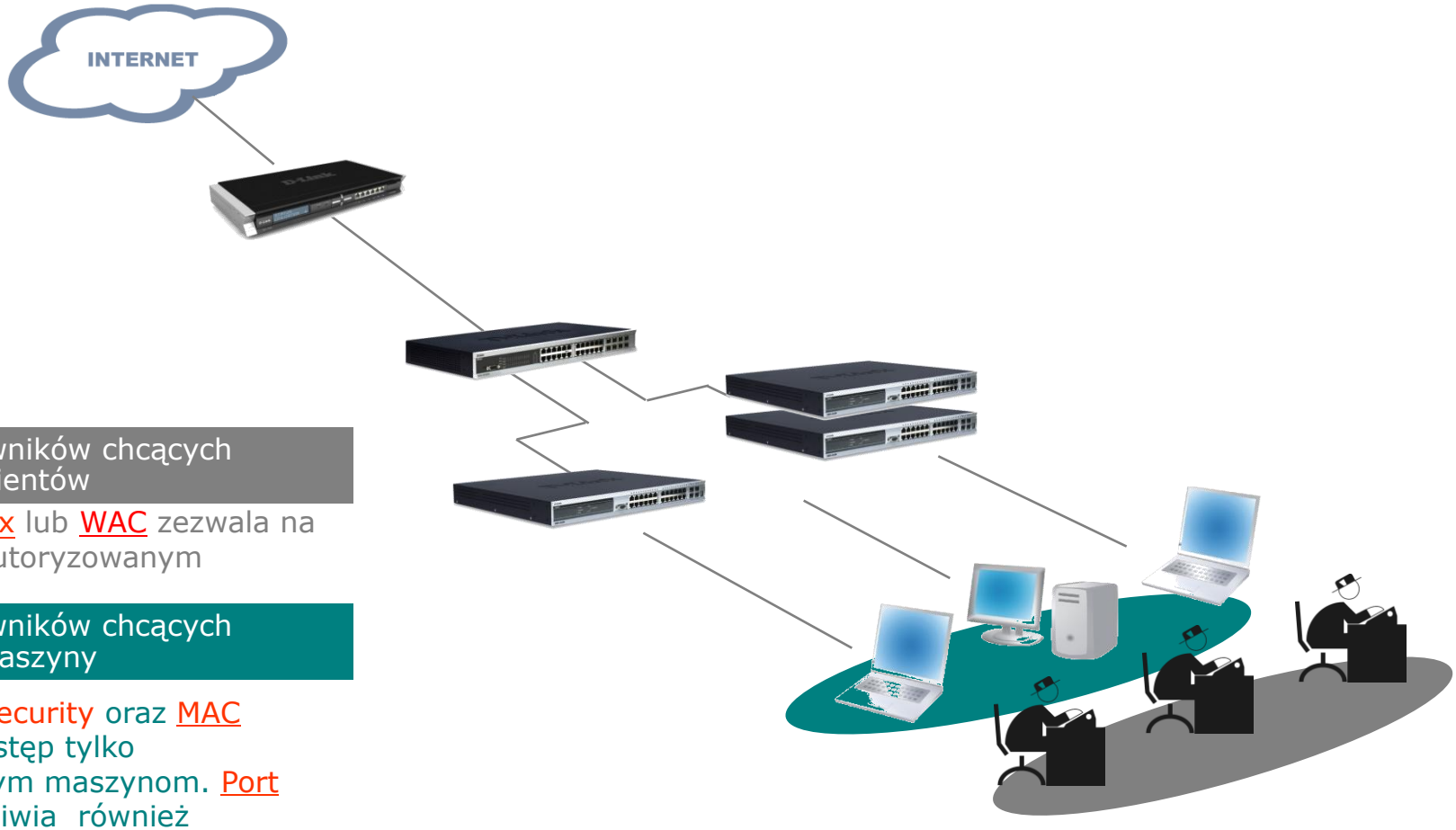




1. Użytkownik otwiera stronę Web

Możliwość współdziałania z funkcjonalnością Guest VLAN

Zintegrowany system ochrony sieci



#1 Dla użytkowników chcących autoryzować klientów

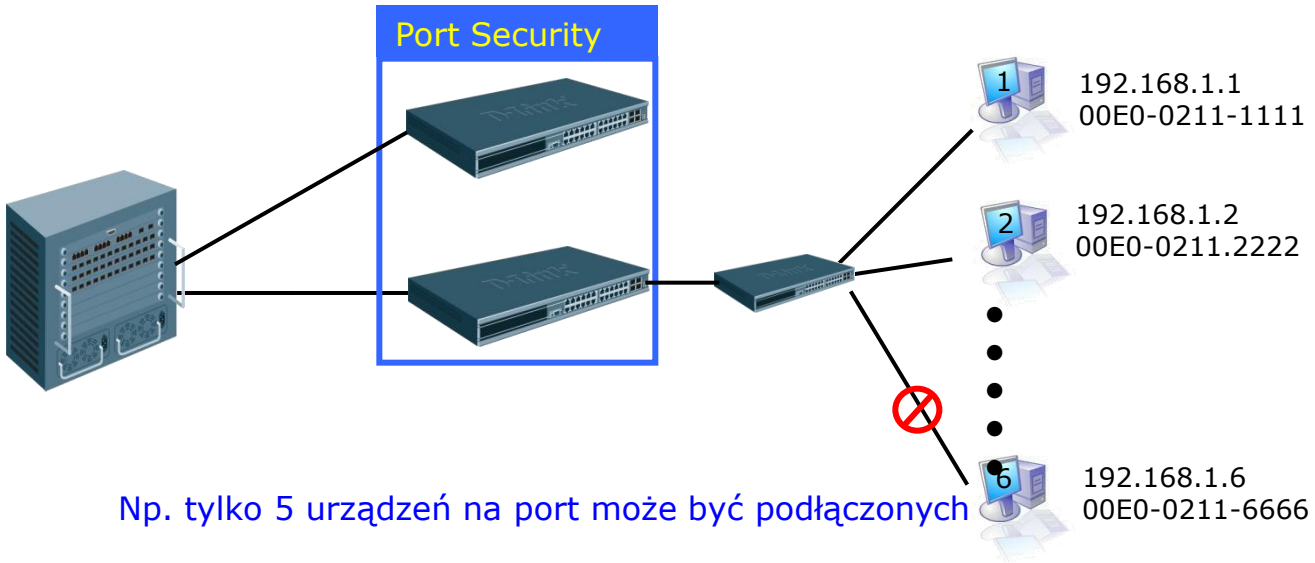
Protokół 802.1x lub WAC zezwala na dostęp tylko autoryzowanym klientom !

#2 Dla użytkowników chcących autoryzować maszyny

Funkcja Port Security oraz MAC pozwala na dostęp tylko zarejestrowanym maszynom. Port Security umożliwia również limitowanie liczby maszyn na każdym porcie !

Port security

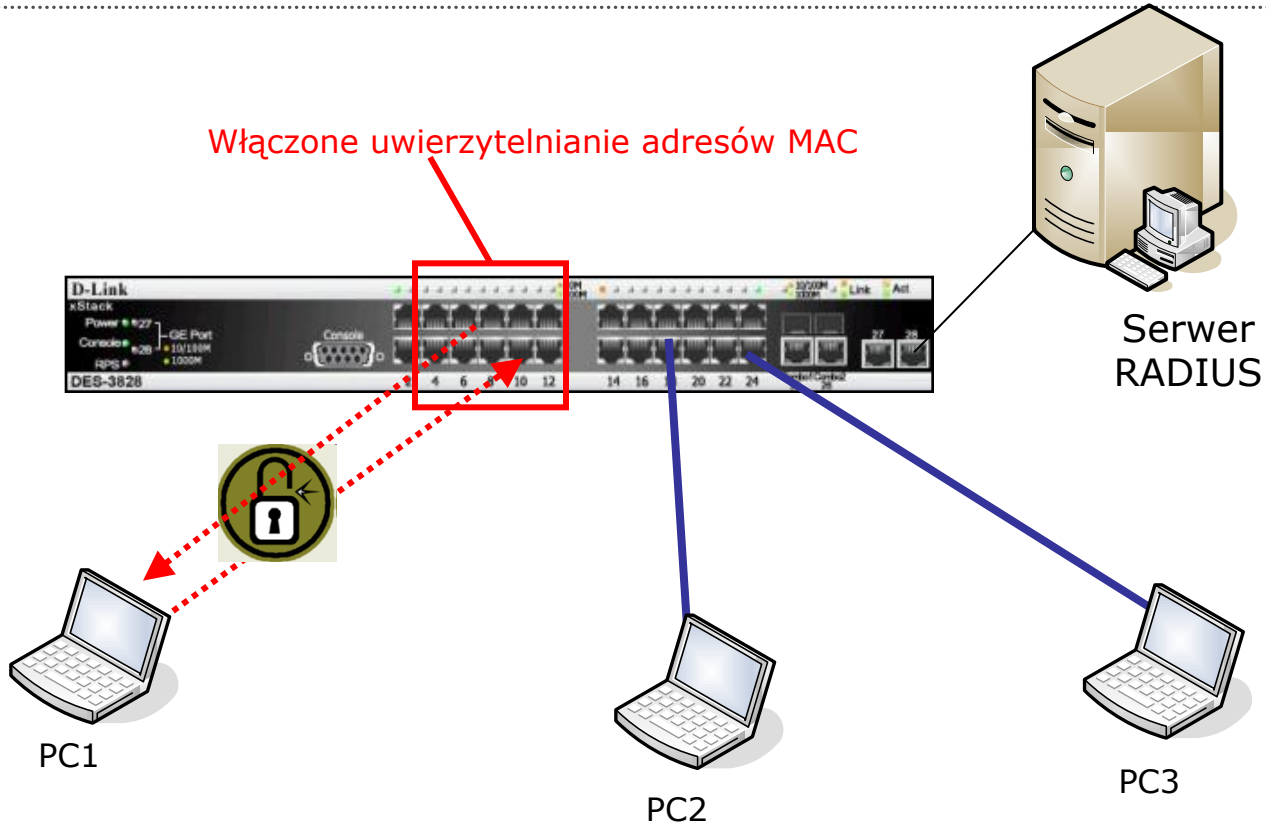
- Limitowanie ilości użytkowników per port
  - Często stosowane w projektach ISP FTTH/ETTH czy akademikach
  - Ochrona przed atakiem MAC Flooding



Np. tylko 5 urządzeń na port może być podłączonych

DGS-3200-24: max 64 MAC

MAC-Based Access Control (MAC)

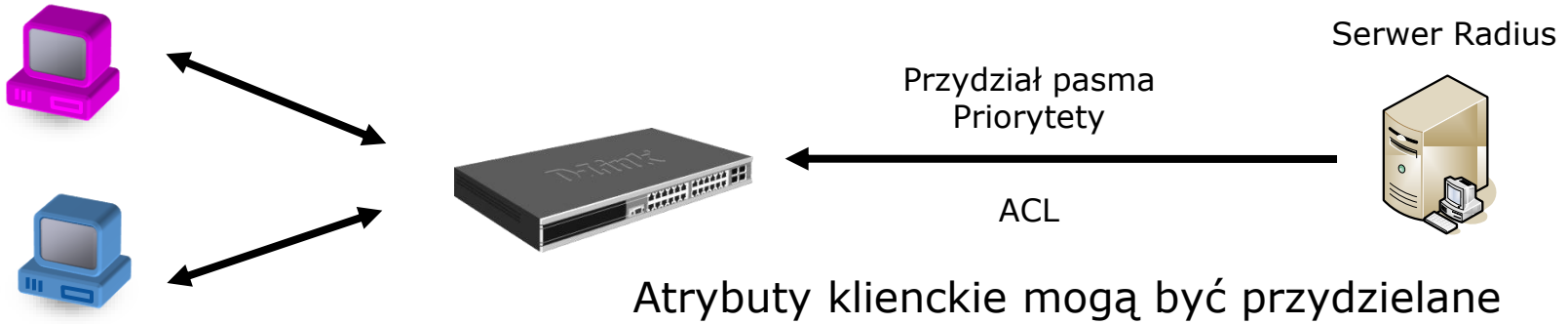


PC1 musi się uwierzytelnić aby otrzymać dostęp do sieci.
Adres MAC PC1 musi być zarejestrowany w bazie danych.

Możliwość współdziałania z funkcjonalnością Guest VLAN

Kontrola wejścia: uprawnienia

- Rozwiązanie D-Linka:
  - Dynamiczne przydzielanie do VLANów
  - Guest VLAN (sieć wyodrębniona/zastrzeżona)
  - Parametryzacja portu klienckiego
    - Kontrola pasma per port
    - Priorytety 802.1p
    - ACL identyfikująca użytkownika dostarczana jako zestaw kilku usług*



Atrybuty klienckie mogą być przydzielane przez serwer RADIUS po poprawnej autentykacji

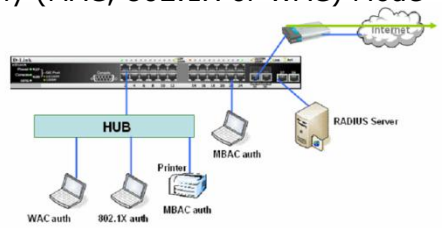
- Reguły bezpieczeństwa bazujące na tożsamości zapewniają właściwy poziom dostępu do sieci dla różnych użytkowników

* W przygotowaniu

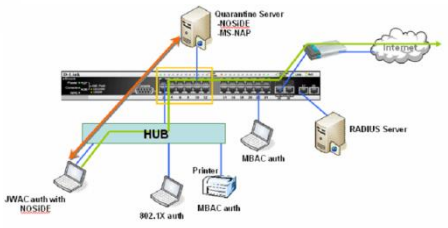
Multiple (Compound) Authentication

- Wiele równoczesnych metod uwierzytelniania na porcie
  - 802.1X
  - MAC-based Access Control (MBAC)
  - Web-based Access Control (WAC)
  - Japan Web-based Access Control (JWAC)
  - IP-MAC-Port Binding (IMPB)

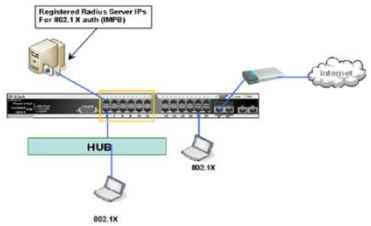
Any (MAC, 802.1X or WAC) Mode



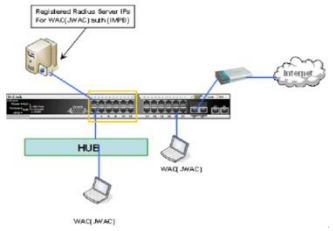
Any (MAC, 802.1X or JWAC) Mode



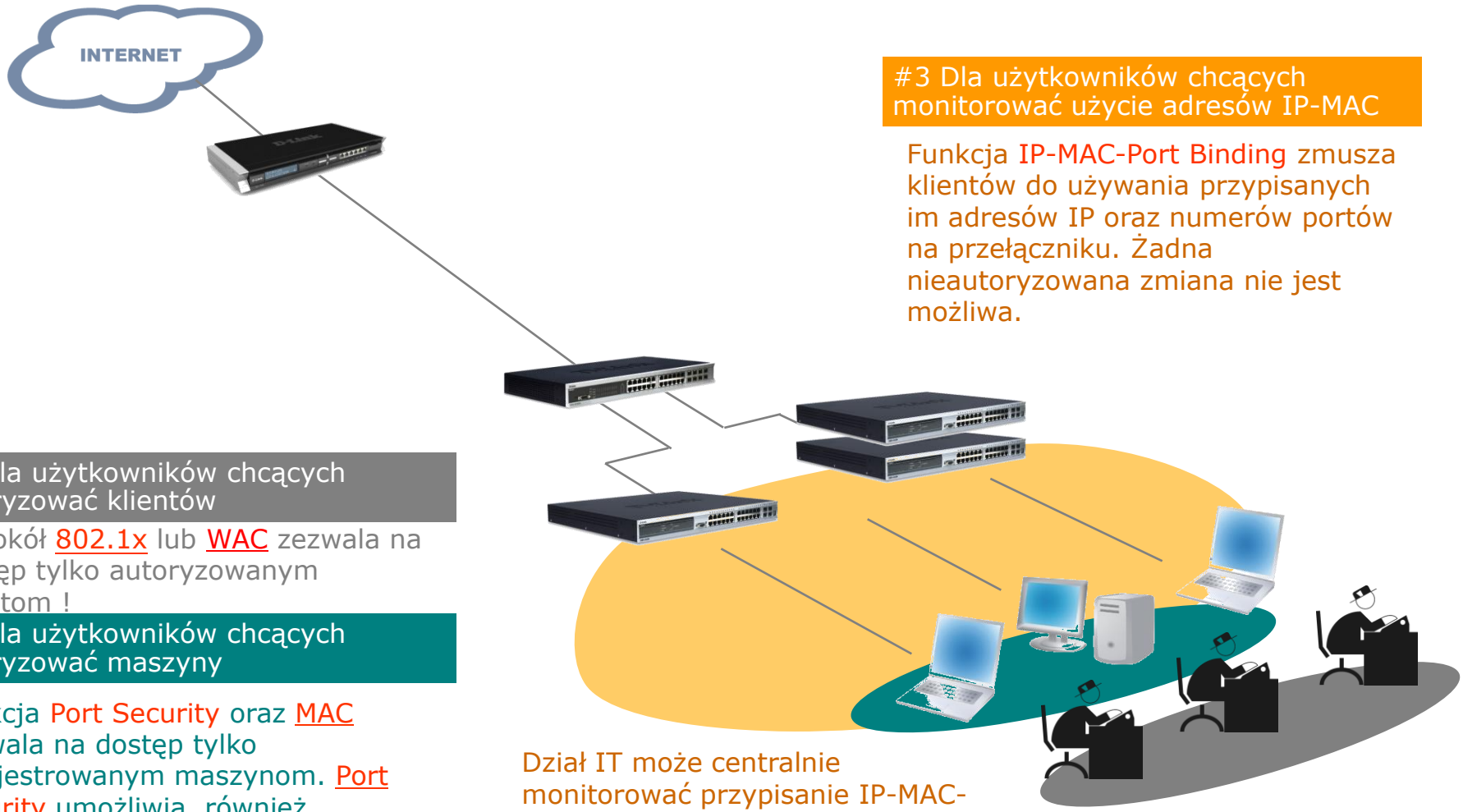
802.1X & IMPB Mode



IMPB & WAC/JWAC Mode



Zintegrowany system ochrony sieci



#3 Dla użytkowników chcących monitorować użycie adresów IP-MAC

Funkcja IP-MAC-Port Binding zmusza klientów do używania przypisanych im adresów IP oraz numerów portów na przełączniku. Żadna nieautoryzowana zmiana nie jest możliwa.

#1 Dla użytkowników chcących autoryzować klientów

Protokół 802.1x lub WAC zezwala na dostęp tylko autoryzowanym klientom !

#2 Dla użytkowników chcących autoryzować maszyny

Funkcja Port Security oraz MAC pozwala na dostęp tylko zarejestrowanym maszynom. Port Security umożliwia również limitowanie liczby maszyn na każdym porcie !

Dział IT może centralnie monitorować przypisanie IP-MAC-Port za pośrednictwem SNMP oraz łatwo zlokalizować każdą maszynę

Ochrona przed ARP Spoofing

- Rozwiązanie D-Linka: Gratuitous ARP
  - Pakiet gratuitous ARP jest specjalnym rodzajem pakietu ARP, w którym

    - source IP i **destination IP** są adresami IP nadawcy

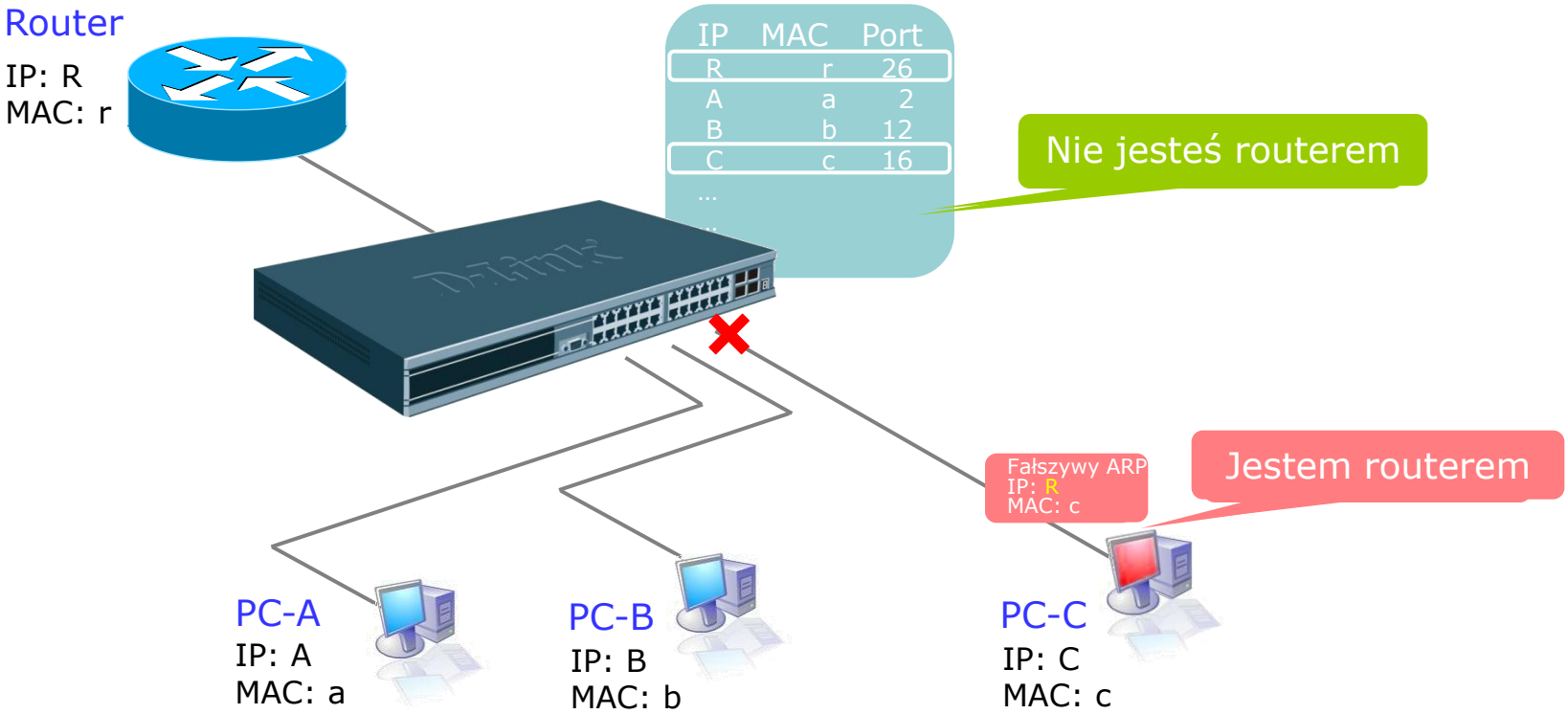
    - source MAC jest adresem MAC nadawcy a **destination MAC** jest adresem broadcasowym FF:FF:FF:FF:FF:FF

  Prewencyjne informowanie o fakcie, że dany IP jest pod danym MAC

- Jak przebiega rozsiewanie Gratuitous ARP:
  - Przełącznik D-linka okresowo wysyła pakiety Gratuitous ARP do wszystkich PC w sieci
  - Po otrzymaniu pakietu Gratuitous ARP, wszystkie PC w sieci automatycznie uaktualniają swoją własną tablicę ARP poprawnym wpisem MAC/IP

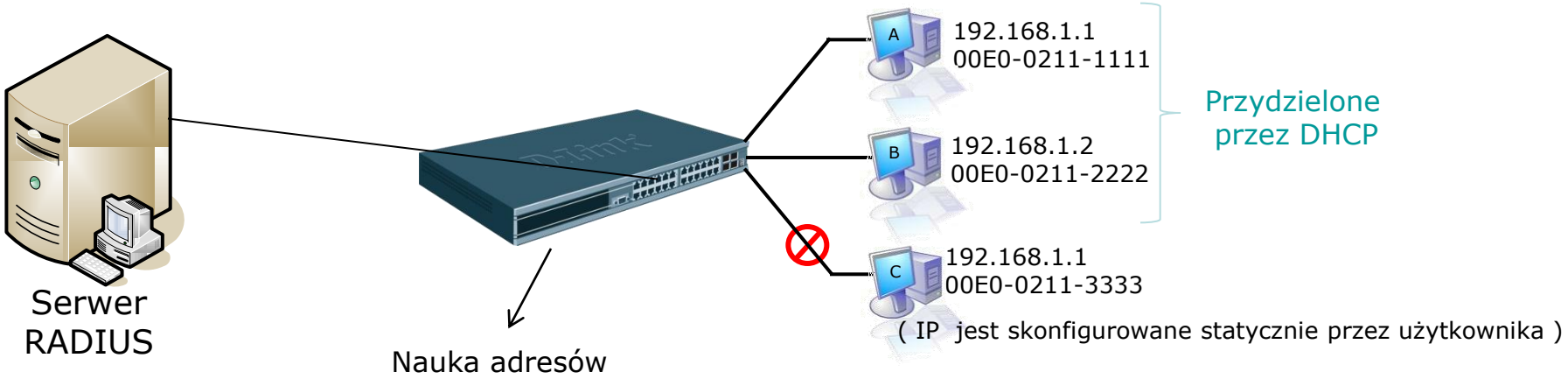
Ochrona przed ARP Spoofing

- Rozwiązanie: IP-MAC-Port Binding
  - ✓ Stworzenie bazy powiązań pomiędzy IP, MAC i portem fizycznym przełącznika
  - ✓ Przełącznik blokuje niedozwoloną próbę dołączenia się do portu natychmiast, gdy wykryty zostanie niepasujący pakiet ARP.



IMP (IP-MAC-Port) Binding v3

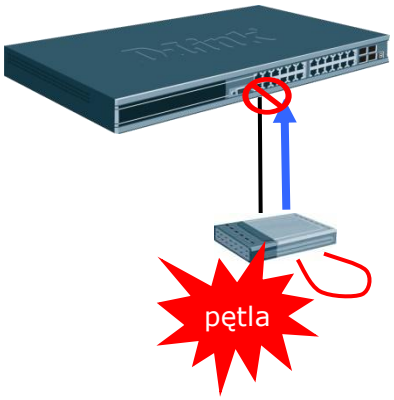
- IMP Binding v3 (DHCP Snooping)
  - ✓ IMP Binding v3 automatycznie zapamiętuje pary IP-MAC w lokalnej bazie danych
  - ✓ Tylko ramki z adresacją odpowiadającą parom na „białej liście” mogą przejść przez port przełącznika
  - ✓ Blokada ruchu ARP i IP
  - ✓ Ochrona ARP DOS



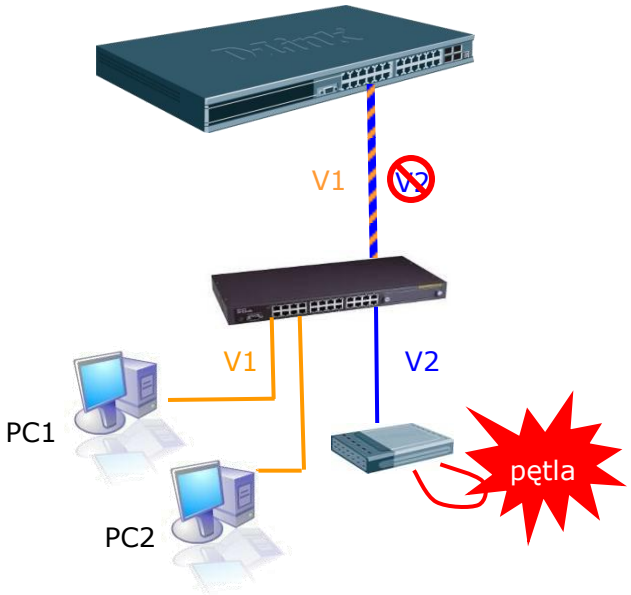
White List		
192.168.1.1	00E0-0211-1111	Port1
192.168.1.2	00E0-0211-2222	Port2

Loopback Detection (LBD v4.0)

- ✓ Niezależne od STP (Spanning Tree Protocol)
  - Niezarządzane przełączniki zwykle nie mają funkcji STP
  - Rozwiązanie D-Linka może wykryć zapętlone połączenia nawet jeśli nieobecne/wyłączony jest protokół STP
- ✓ Elastyczne ustawienia dla ochrony przed pętlami w sieci
  - Port-based lub
  - VLAN-based



1. Port-based LBD
- Port zamknięty, ruch jest niedozwolony

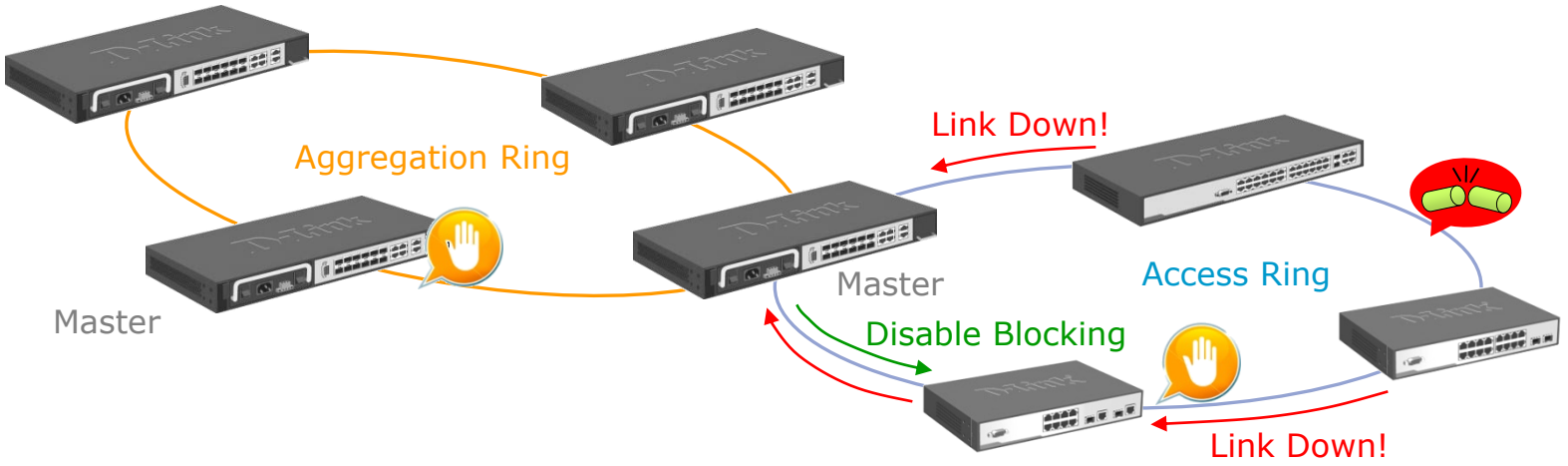


2. VLAN-based LBD
- Blokada ruchu tylko dla VLAN gdzie wystąpiła pętla bez wyłączania portu uplink

RERP-Switching (RERP-S)

	STP	RSTP	RERP-S
Topologia	dowolna	dowolna	pierścień
Czas odtworzenia	30-50 sek	1 sek	**50-200 ms!**

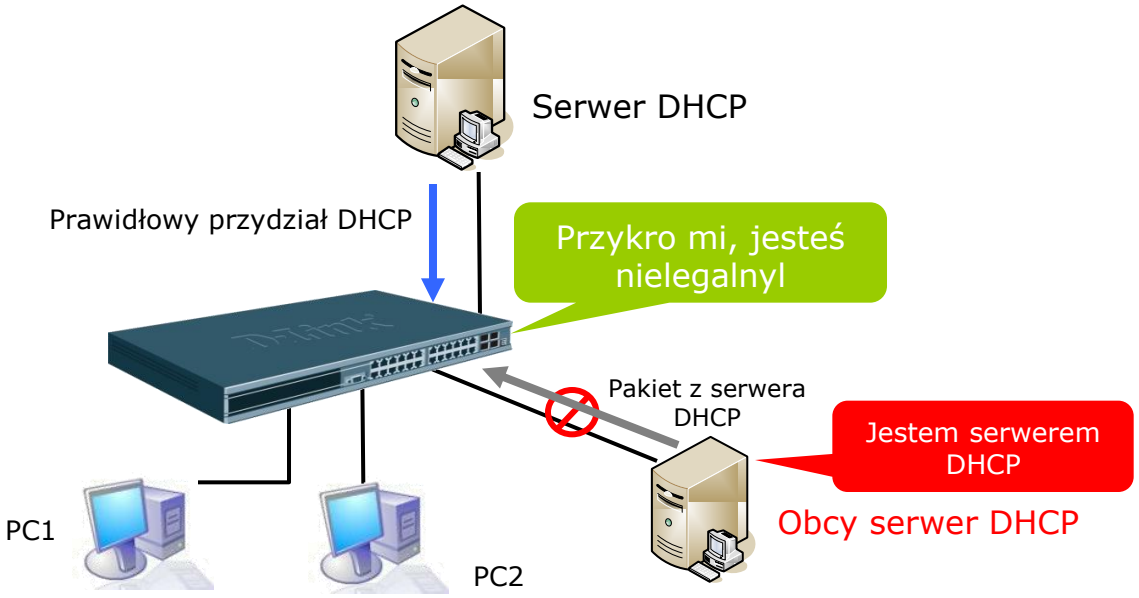
- standard (ITU-T G.8032) dla Ethernet Ring Protection switching
- Wsparcie dla aplikacji w wieloma pierścieniami
- 50ms na odbudowę w pierścieniu z 16 urządzeniami w pętli <1200 m



DHCP Server Screening

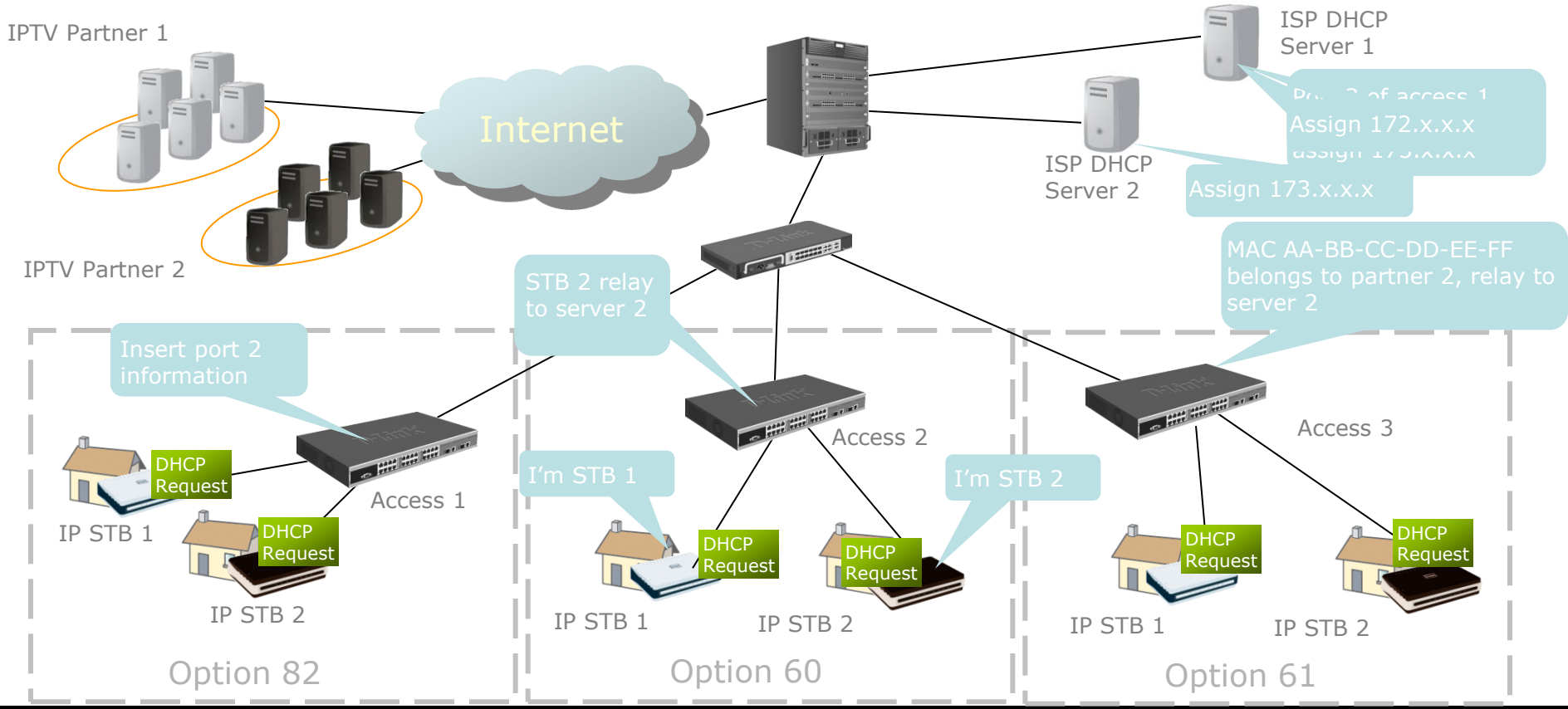
- Problem: Użytkownicy wstawiają w sieć swój własny serwer DHCP
  - ✓ Nieprawidłowe przydzielanie IP
  - ✓ Problemy ze stabilnością działania sieci

- Rozwiązanie: DHCP Server Screening
  - ✓ Skanuje i blokuje pakiety DHCP pochodzące ze strony portów klienckich (unthrusted) aby chronić przed nieprawidłowym przydziałem IP w sieci



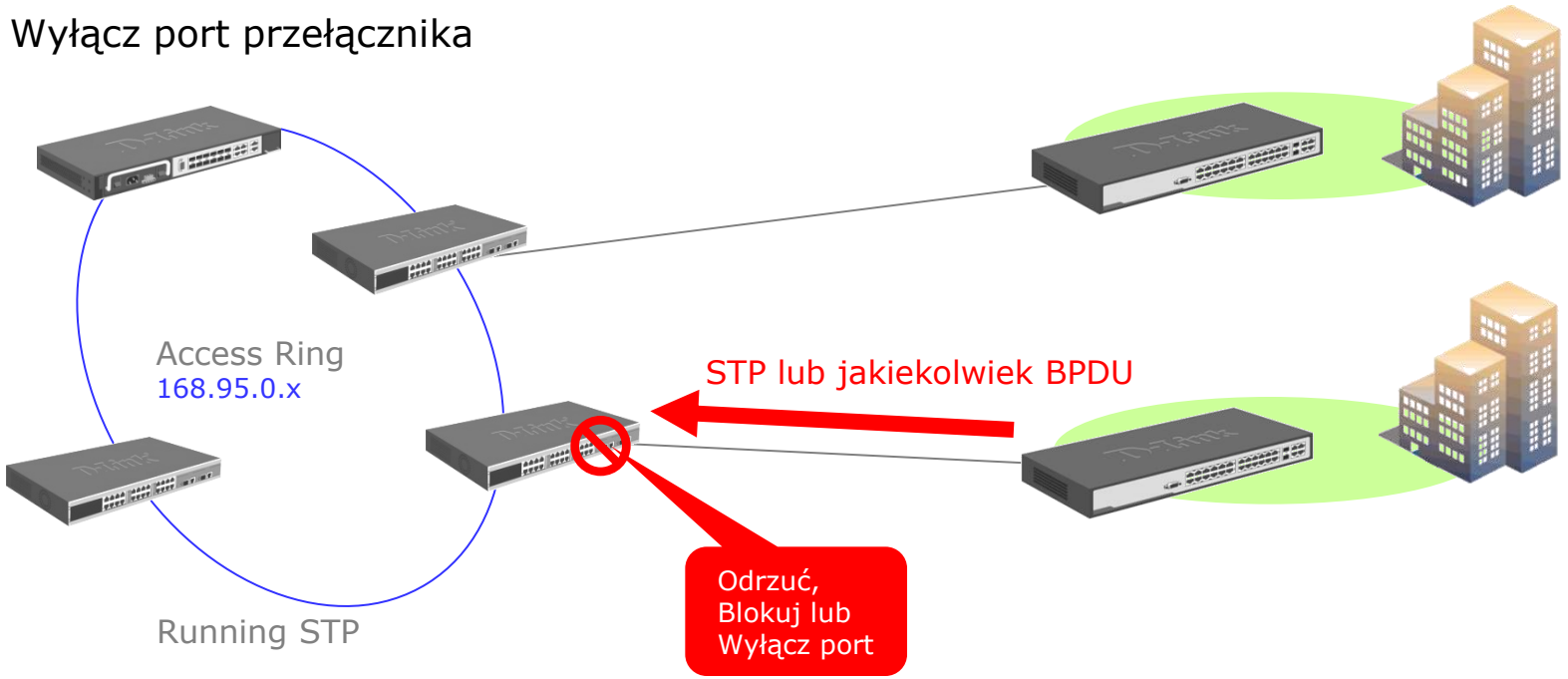
DHCP Relay

- DHCP option 82: przydział IP bazując na ID obwodu (VLAN, port, adres MAC przełącznika)
- DHCP option 60: przydział IP bazując na zdefiniowanym stringu
- DHCP option 61: przydział IP bazując na adresie MAC lub zdefiniowanym stringu



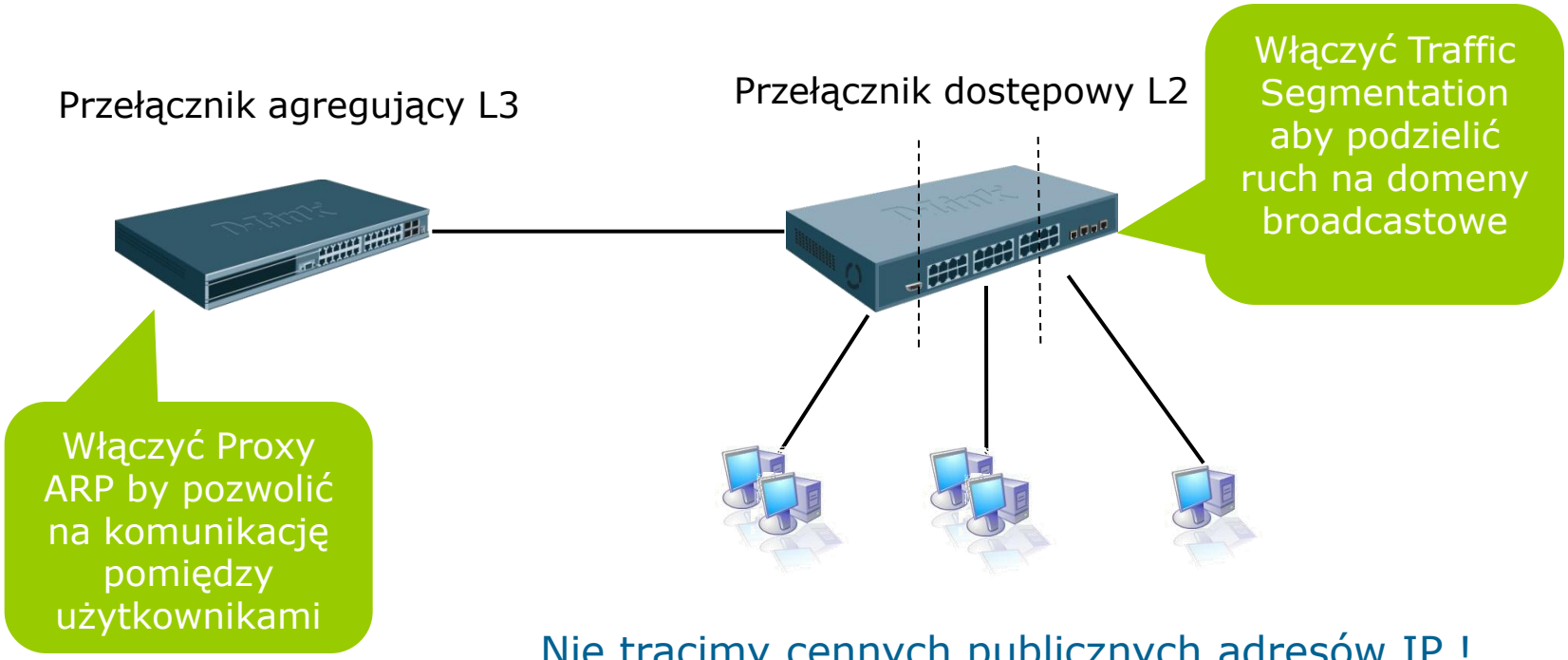
Ochrona przed atakiem BPDU

- Klienci biznesowi mogą spowodować wyciek pakietów BPDU Spanning Tree do sieci operatora i zakłócić jego usługi sieciowe
- BPDU Attack Protection oferuje 3 akcje w razie gdy przełącznik wykryje pakiety BPDU:
  - Odrzuć pakiety BPDU
  - Wyblokuj cały ruch przychodzący
  - Wyłącz port przełącznika



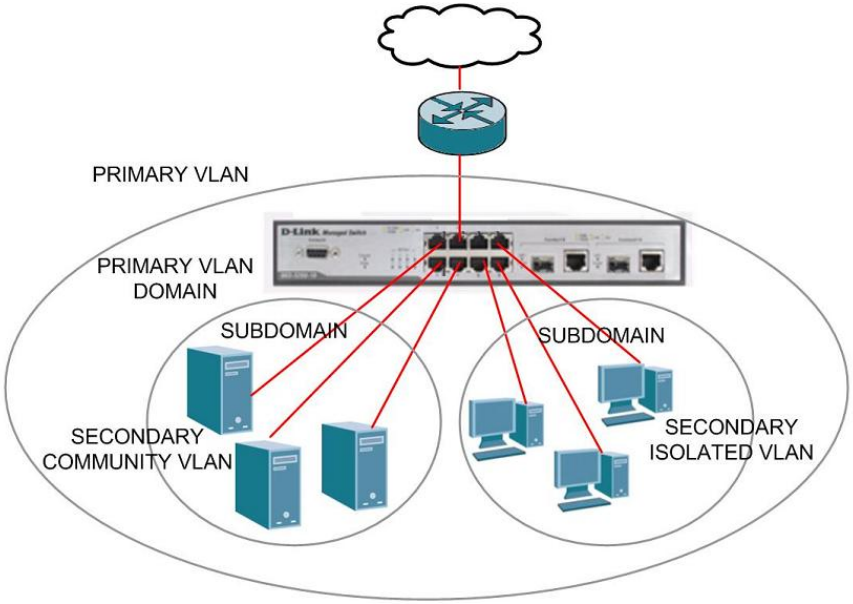
Traffic Segmentation + Proxy ARP

- Wymaganie: Segregacja ruchu użytkowników
  - ✓ Zwykle pod projekty ISP ETTH
  - ✓ Użytkownicy podłączeni do tego samego przełącznika są w innych domenach broadcast'owych, ale mogą komunikować się ze sobą, gdy zachodzi taka potrzeba.
- Rozwiązanie : Traffic Segmentation + Proxy ARP



Nie tracimy cennych publicznych adresów IP !

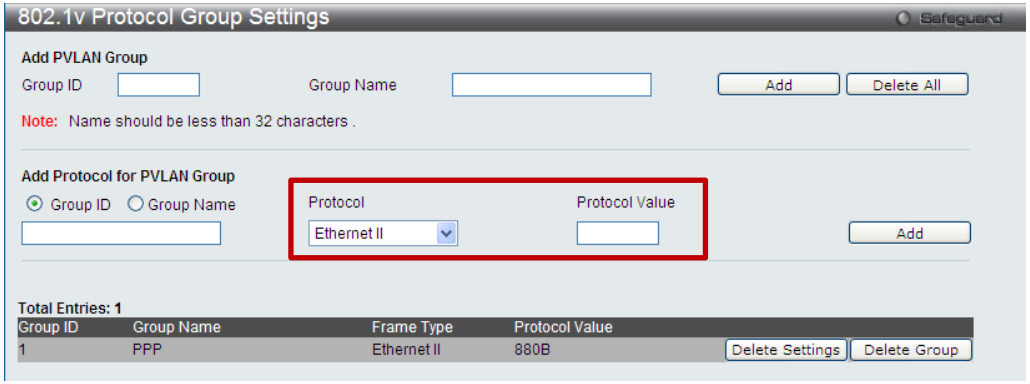
Private VLAN

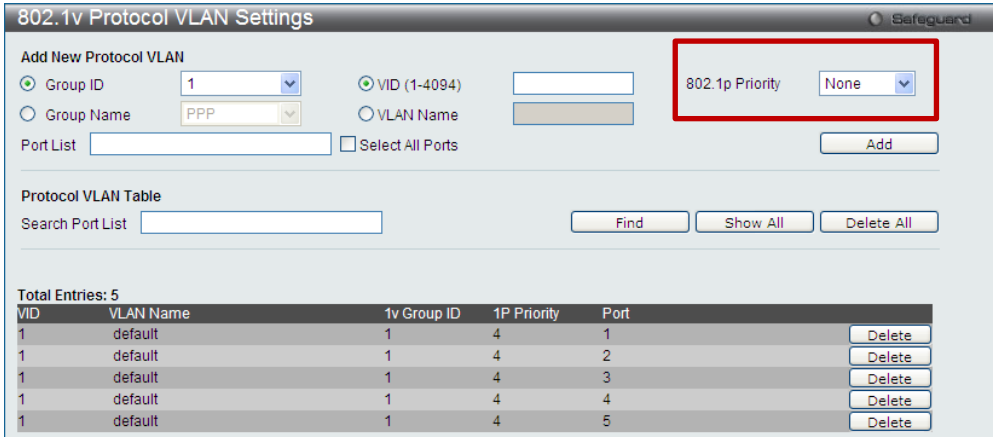


- Dla ISP, którzy chcą przydzielić unikatowe VLANy swoim klientom.
- Porty mogą być w 3 stanach:
  - Promiscuous: widzi wszystkie porty
  - Isolated: widzi tylko port Promiscuous
  - Community: widzi porty w subdomenie i port Promiscuous

VLAN 802.1v

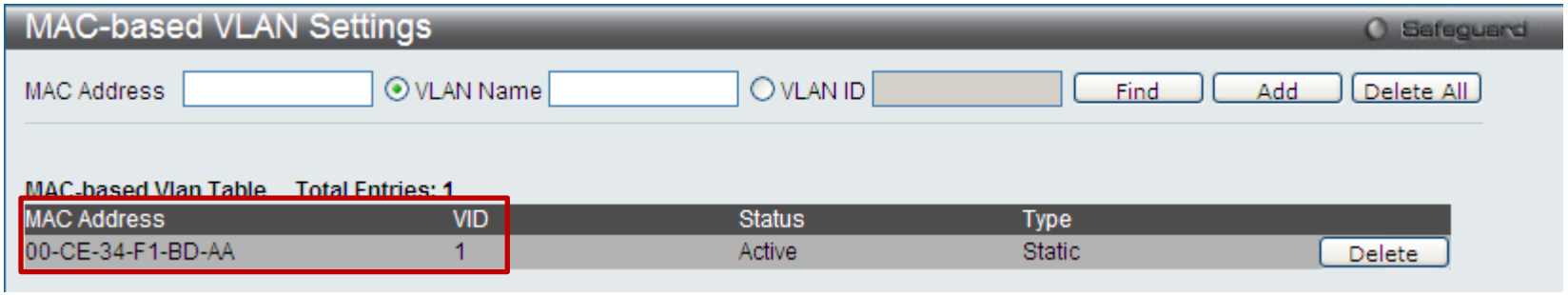
- Automatyczne „wkładanie” ramek do VLAN na podstawie wartości protokołu (Ethernet II, SNAP, LLC)





MAC-based VLAN

- Przypinanie ramek do VLAN na podstawie adresu MAC

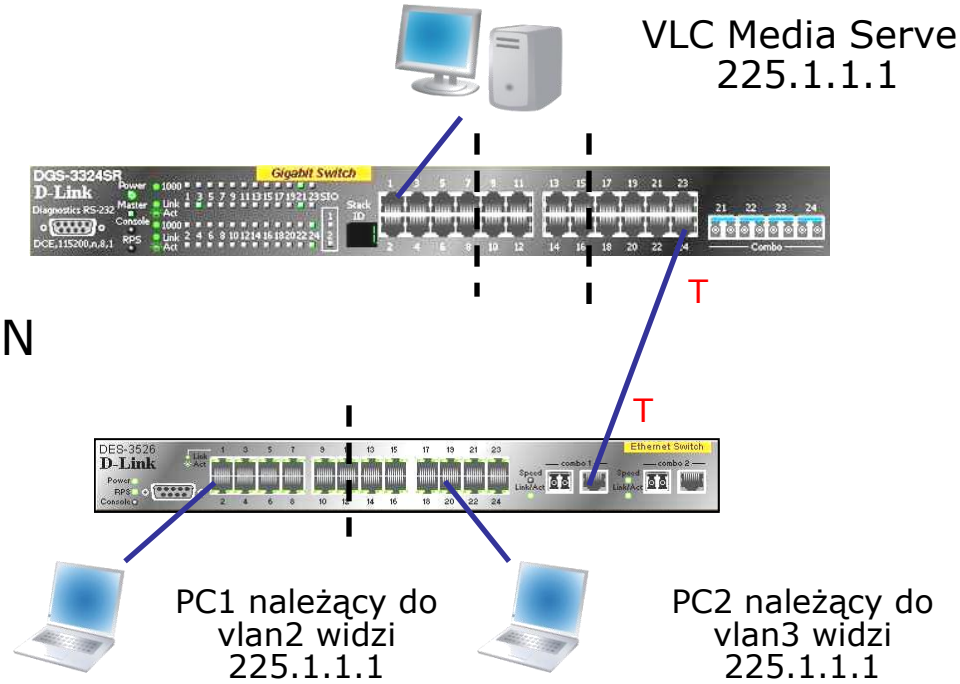


IGMP Snooping Multicast (ISM) VLAN

- Mechanizm wykorzystywany często w przypadku świadczenia usług Triple-Play: użytkownik w ramach abonamentu chce oglądać TV na kilku odbiornikach: np. telewizorze i na każdym komputerze

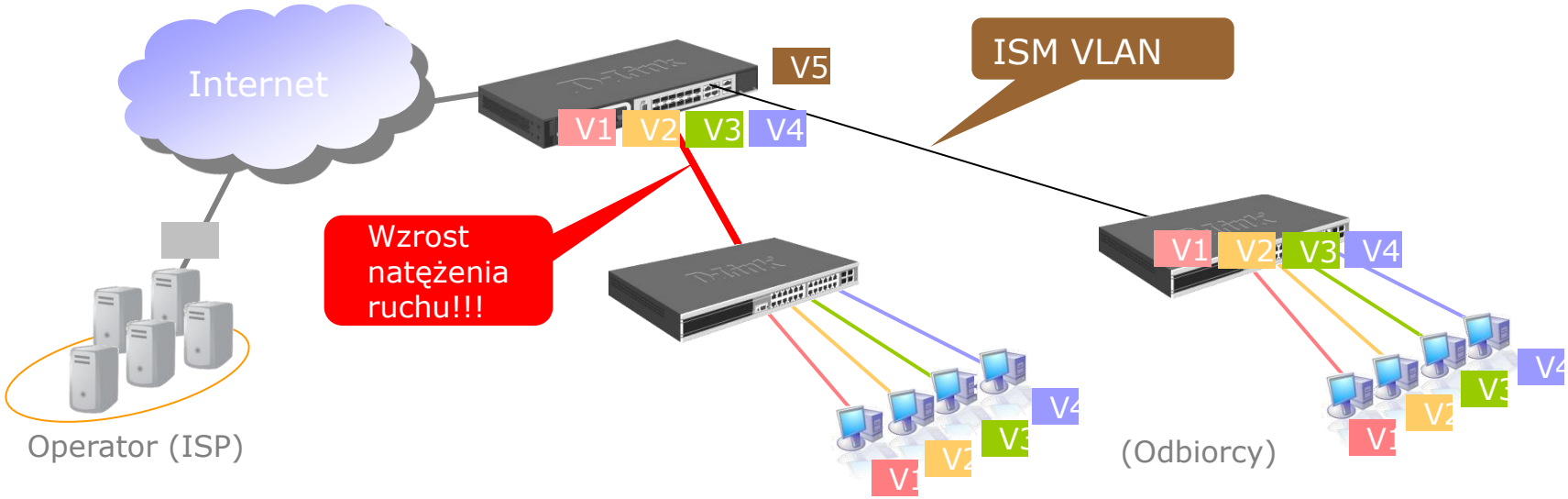
- **Jeden strumień multicastu zamiast wielu obciążających sieć kopii**
- Cisco **MVR** (Multicast VLAN Registration) – **Leaky VLAN**

D-Link **ISM** VLAN

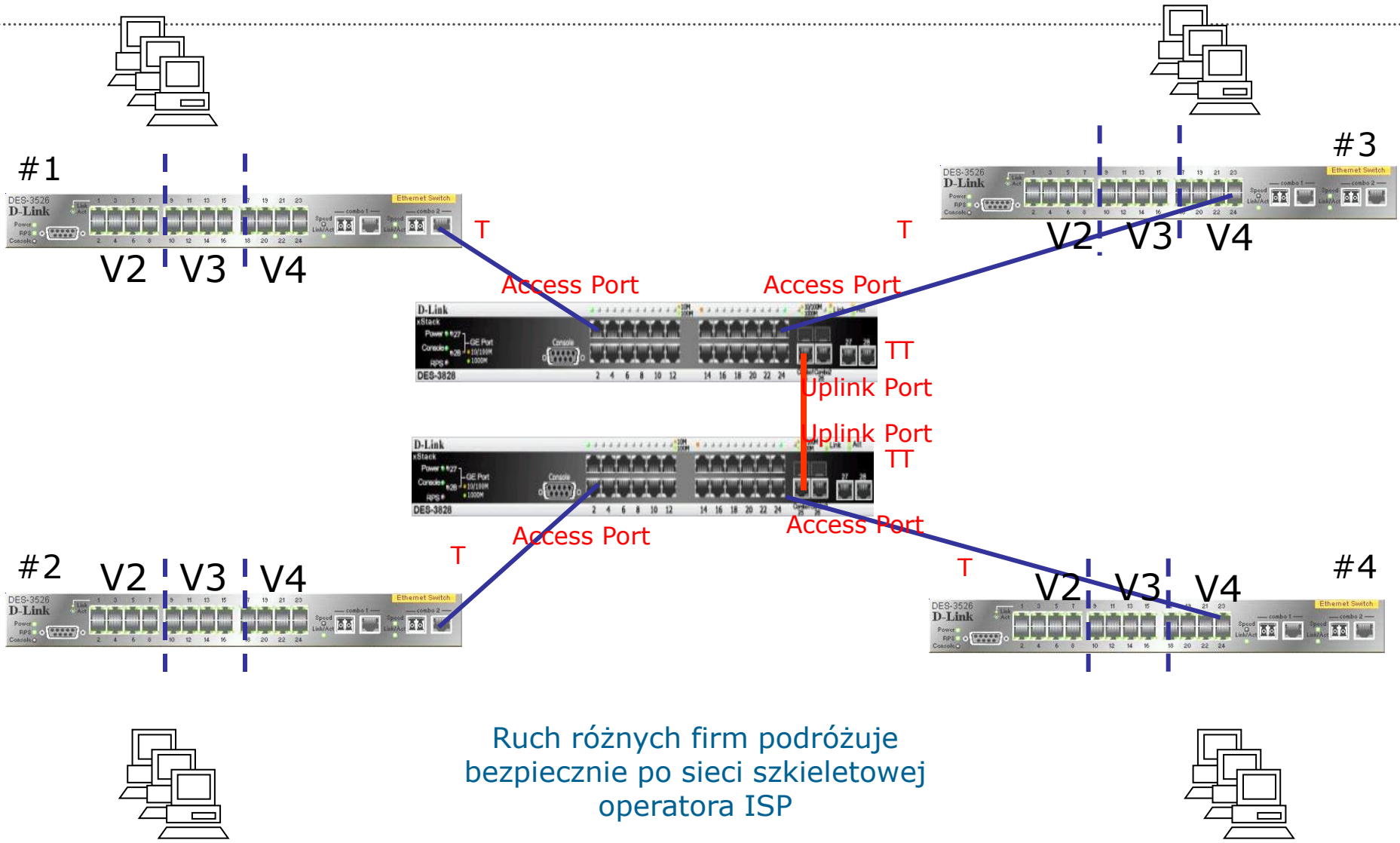


ISM VLAN

- Ze względu na bezpieczeństwo ISP izolują strumienie dla różnych odbiorców przez wprowadzenie ich w VLANy.
- Aplikacje wymagają ciągłego strumienia multicastu, który powoduje drastyczny wzrost ruchu na interfejsie uplinkowym switcha dostępowego L2.
- ISM VLAN rejestruje strumień multicastu dla abonenckich VLAN, co oszczędza pasmo na interfejsie uplinkowym.

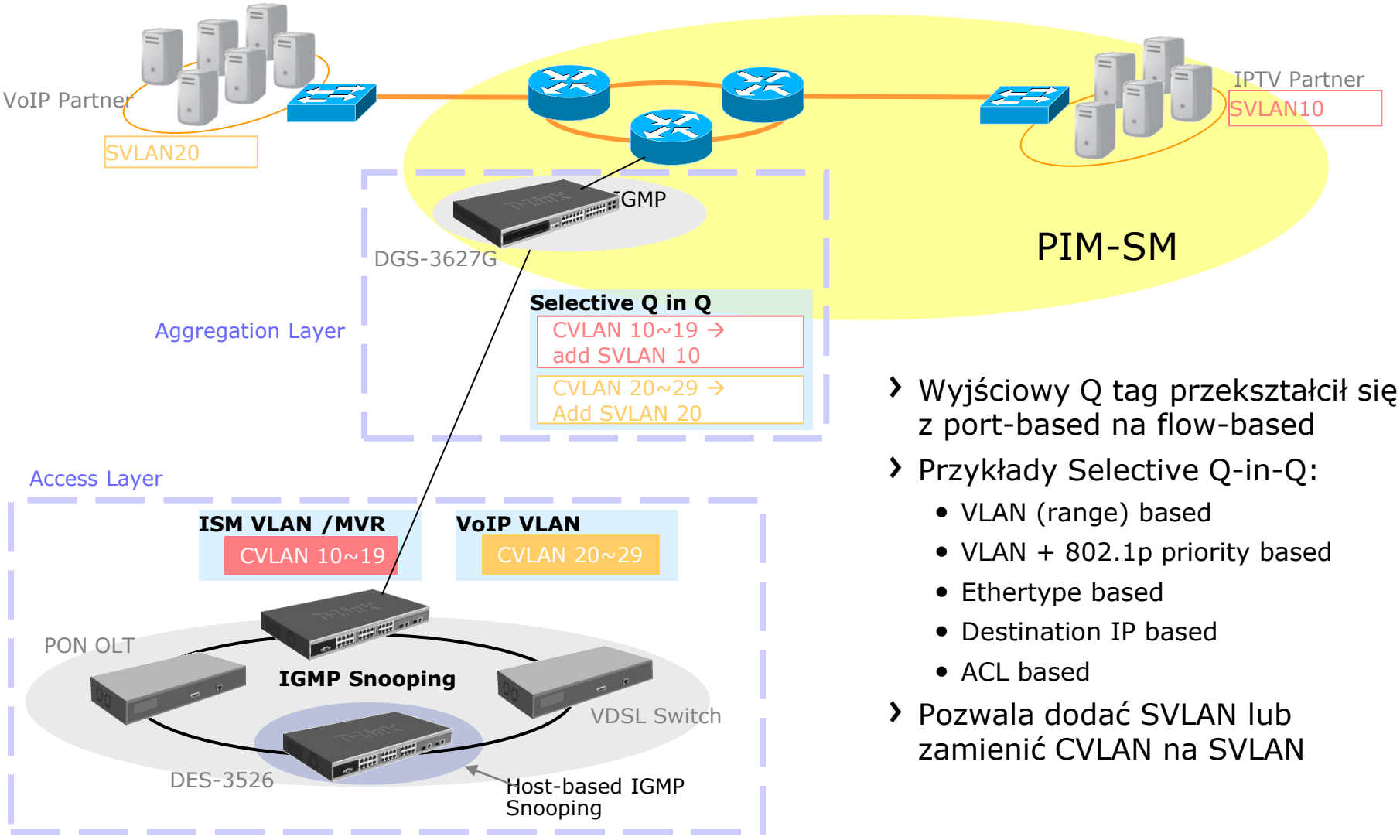


Double VLAN (Q-in-Q tagging)



Ruch różnych firm podróżuje bezpiecznie po sieci szkieletowej operatora ISP

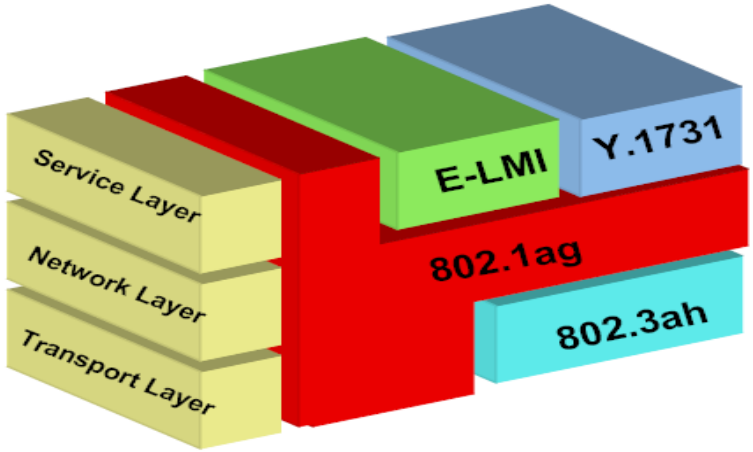
Selective Q-in-Q (VLAN Translation)



- Wyjściowy Q tag przekształcił się z port-based na flow-based
- Przykłady Selective Q-in-Q:
  - VLAN (range) based
  - VLAN + 802.1p priority based
  - Ethertype based
  - Destination IP based
  - ACL based
- Pozwala dodać SVLAN lub zamienić CVLAN na SVLAN

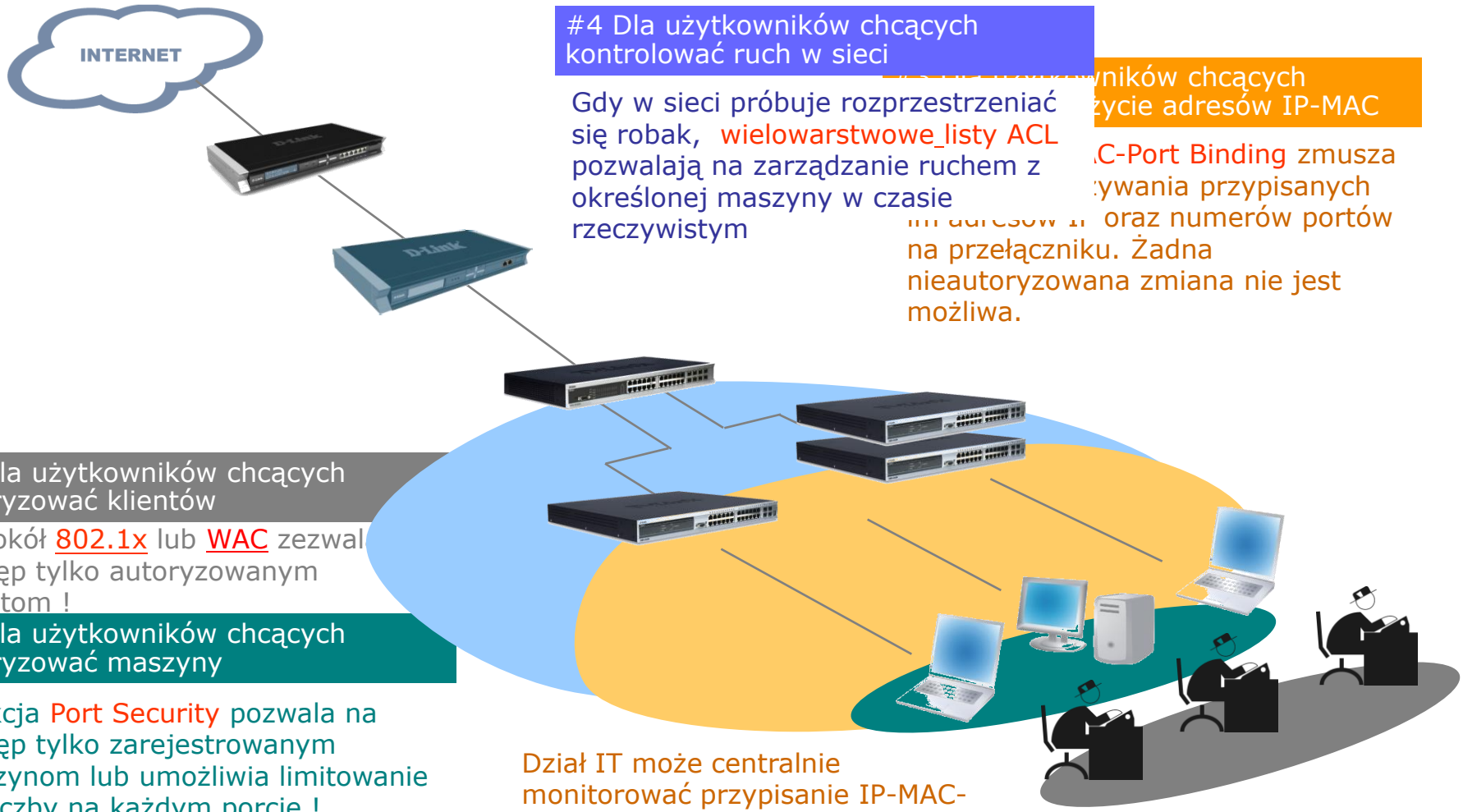
Funkcjonalności Metro Ethernet

- L2 VPN: QinQ, L2PT, VLAN Translation
- Zaawansowane usługi IPTV : Multicast VLAN i profile kanałów, Multicast Reporting, Host-based Multicasting, ISM VLAN (MVR)
- Stabilność/odporność: E-RPS, LBD
- Silne zabezpieczenia: DHCP/ARP/MIM/DDOS Attack Prevention, Microsoft NAP
- Kontrola dostępu: Bandwidth Control, CIR, QoS
- OAM: 802.1ag, 802.3ah, Y.1731*, Cable Diagnostics, Optical Transceiver DDM
- Certyfikat MEF 9,14, IPv6 Ready*



* - trwają prace

Zintegrowany system ochrony sieci



#4 Dla użytkowników chcących kontrolować ruch w sieci

Gdy w sieci próbuje rozprzestrzeniać się robak, wielowarstwowe_listy ACL pozwalają na zarządzanie ruchem z określonej maszyny w czasie rzeczywistym

...ników chcących
...życie adresów IP-MAC

...C-Port Binding zmusza
...ywania przypisanych
...oraz numerów portów
na przełączniku. Żadna nieautoryzowana zmiana nie jest możliwa.

#1 Dla użytkowników chcących autoryzować klientów

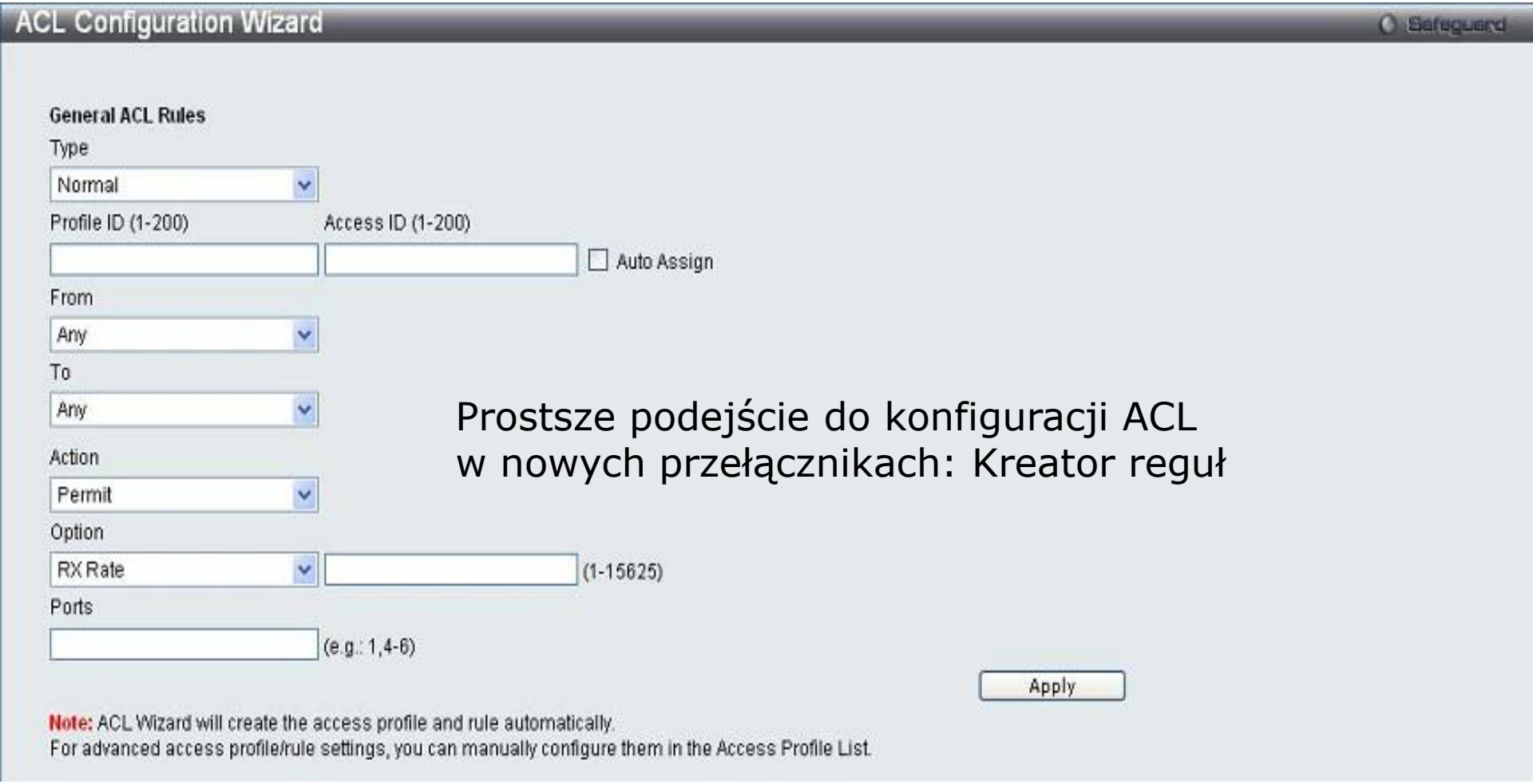
Protokół 802.1x lub WAC zezwal... dostęp tylko autoryzowanym klientom !

#2 Dla użytkowników chcących autoryzować maszyny

Funkcja Port Security pozwala na dostęp tylko zarejestrowanym maszynom lub umożliwia limitowanie ich liczby na każdym porcie !

Dział IT może centralnie monitorować przypisanie IP-MAC-Port za pośrednictwem SNMP oraz łatwo zlokalizować każdą maszynę

Access Control List (ACL)

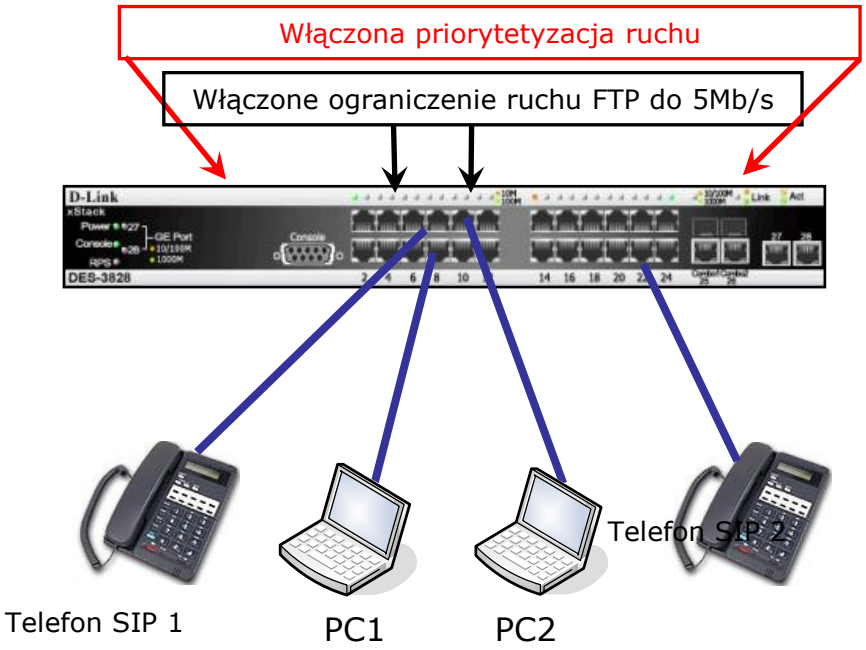


Prostsze podejście do konfiguracji ACL w nowych przełącznikach: Kreator reguł

Kształtowanie ruchu „per flow”

- Jeden użytkownik/usługa na port, z limitem pasma
  - Port-based Bandwidth Control

- Wielu użytkowników/usług na port, z limitem pasma
  - Flow-based Bandwidth Control (ingress ACL)

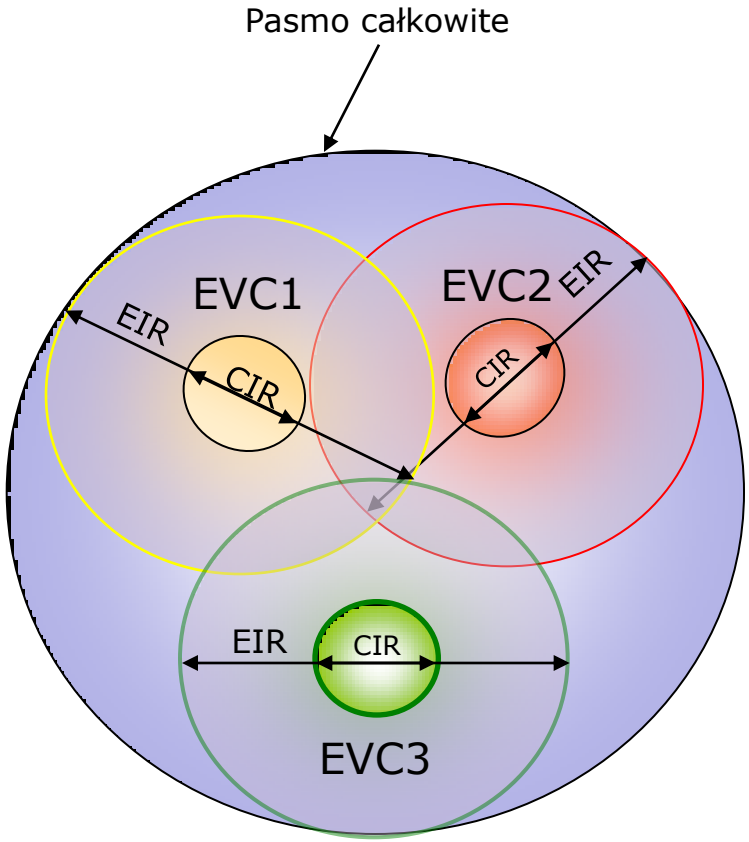


Kształtowanie ruchu „per flow”

- Wiele użytkowników/usług na port, z limitem i gwarancją pasma

  - SrTCM – Single rate, 3 Color Marking
  - TrTCM – Two rate, 3 Color Marking

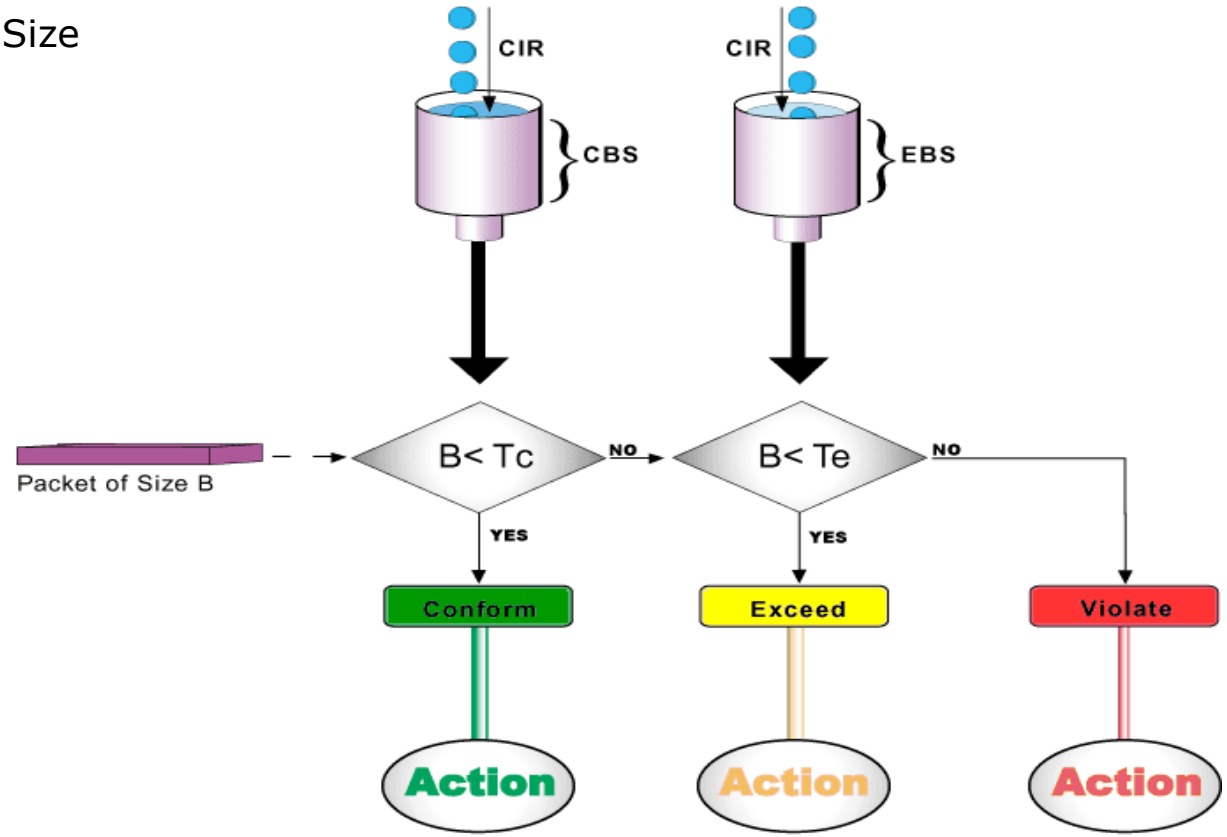
    - CIR – Committed Information Rate
    - EIR – Excess Information Rate
    - CBS, EBS - size of burst (ms) dla danych CIR/EIR



Single-Rate Three Color Marker

- Zastosowanie: szybkie wyłuskanie pakietów trzymających CIR

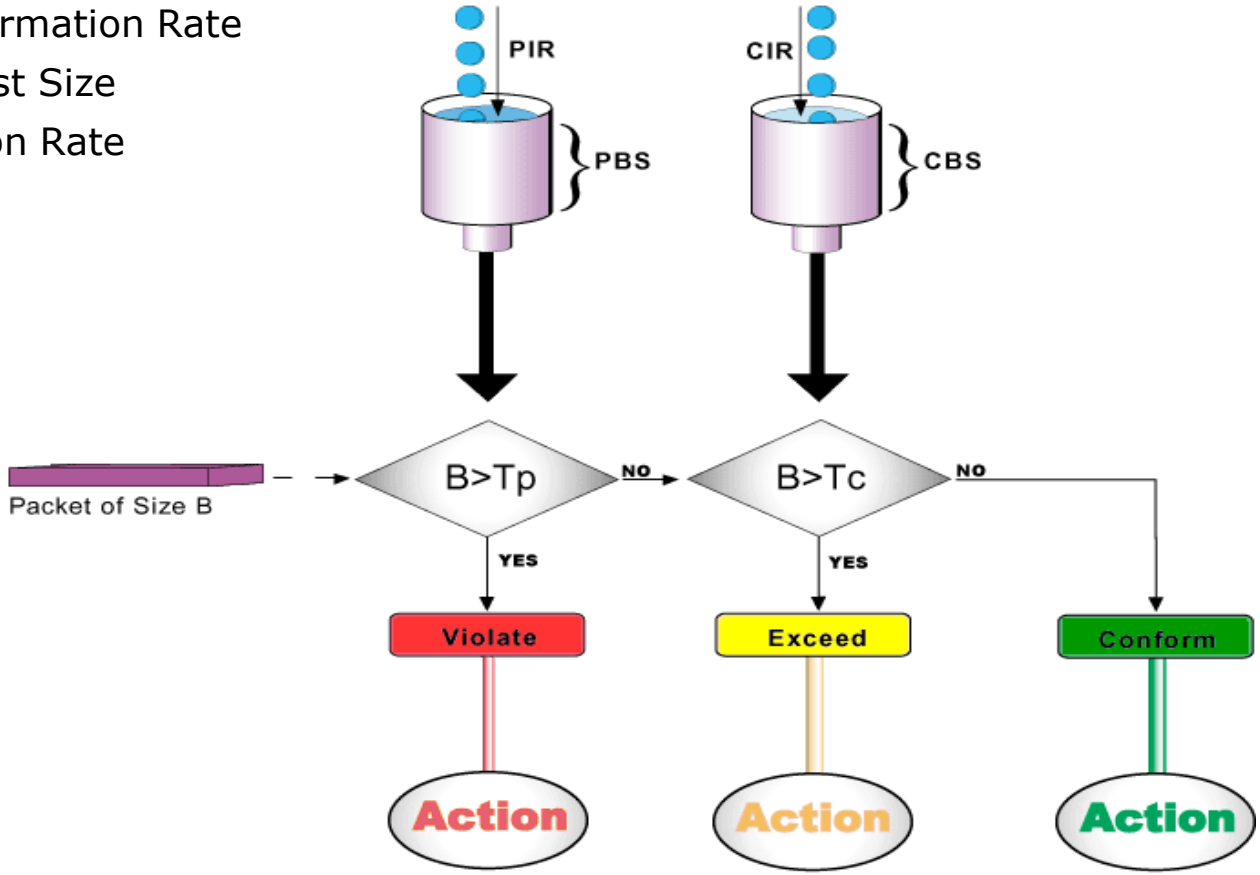
  - **CIR**: Committed Information Rate
  - **CBS**: Committed Burst Size
  - **EBS**: Excess Burst Size



Two-Rate Three Color Marker

- Zastosowanie: aby osobno przetwarzać pakiety > CIR i PIR

  - **CIR**: Committed Information Rate
  - **CBS**: Committed burst Size
  - **PIR**: Peak Information Rate
  - **PBS**: Peak burst Size



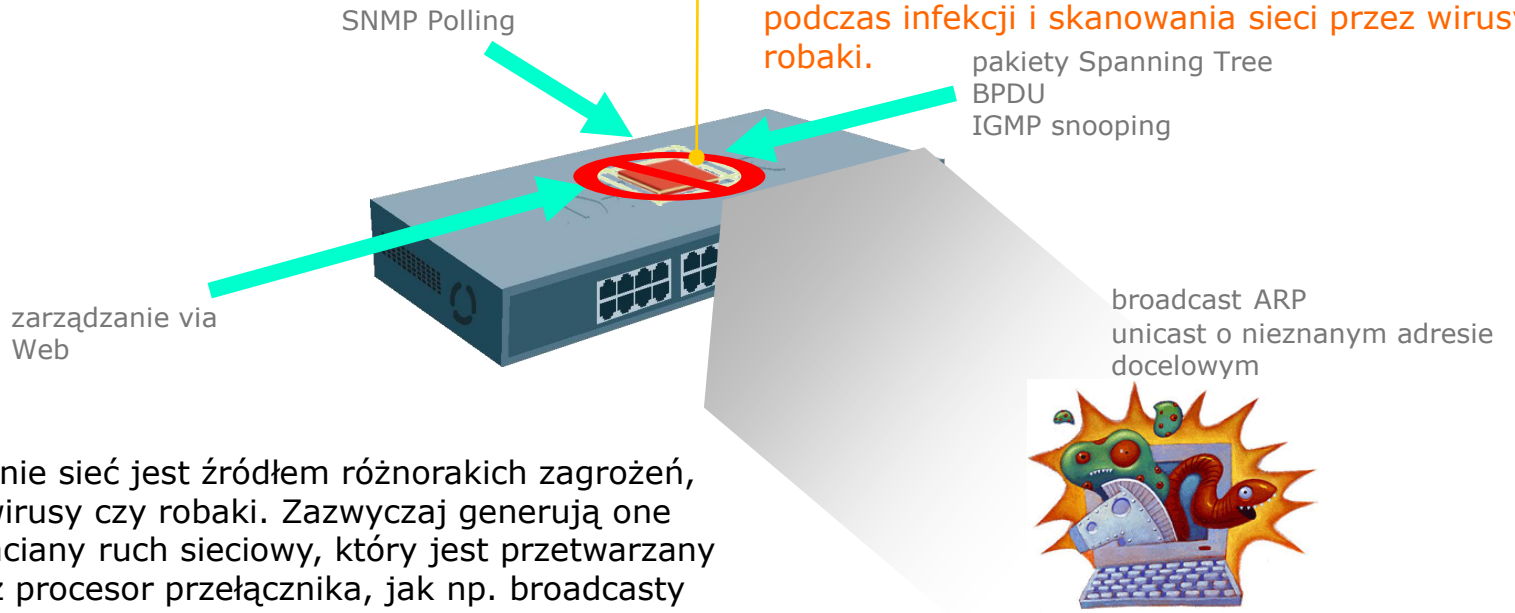
D-Link Safeguard Engine

Safeguard Engine jest mechanizmem pozwalającym zwiększenie odporności przełącznika na nienormalny ruch pozwalając na podwyższenie niezawodności i dostępności całej sieci.

Powoduje to, że procesor jest przeciążony i nie jest w stanie przetwarzać innych zadań, jak zarządzanie, STP, SNMP polling...

Safeguard Engine identyfikuje i priorytetyzuje ruch aby utrzymywać liczbę niechcianych pakietów docierających do przełącznika na akceptowalnym poziomie i umożliwiać niezawodną pracę przełącznika.

Zalety tego mechanizmu będą widoczne zwłaszcza podczas infekcji i skanowania sieci przez wirusy i robaki.



Obecnie sieć jest źródłem różnorakich zagrożeń, jak wirusy czy robaki. Zazwyczaj generują one niechciany ruch sieciowy, który jest przetwarzany przez procesor przełącznika, jak np. broadcasty ARP.

Obsługa IPv6

- W sieciach korporacyjnych, IPv6 oferuje większe bezpieczeństwo, mobilość, QoS i skalowalność
- D-Link zaimplementował IPv6 w Gigabit xStack i przełącznikach Chassis
- D-Link posiada przełączniki IPv6 certyfikowane wg wytycznych fazy 1 i 2.

Cert IPv6 faza 1

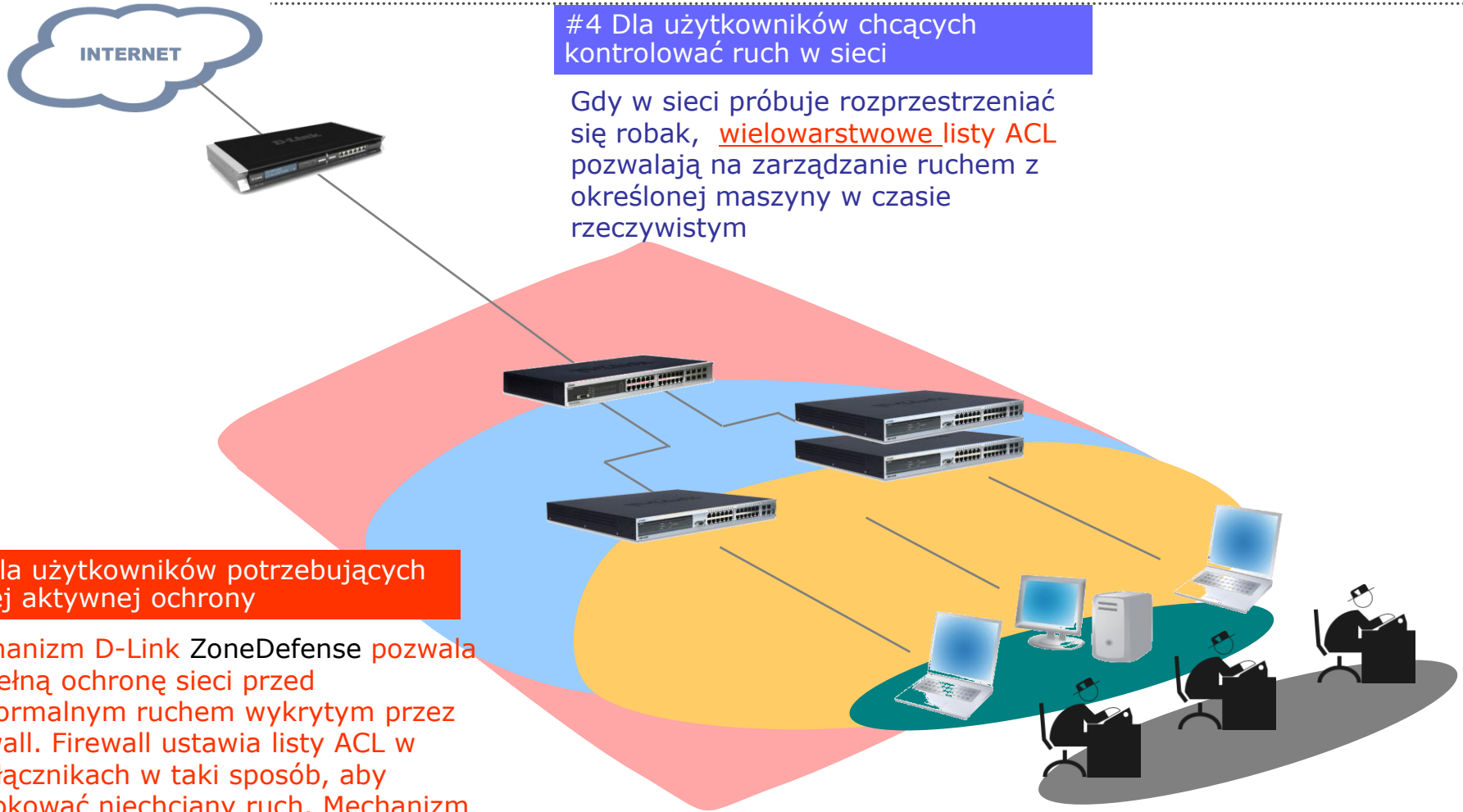
Cert IPv6 faza 2

Seria DES-7200: funkcjonalność

Bezpieczeństwo	Usługi	Routing
Access Control – 802.1x Access Control – MAC Authentication – L2/3/4 Advanced ACL's – IP/MAC/Port Binding Robust Infrastructure – Anti-DDoS Attack – Protocol Verification Traffic Management – CPP (CPU Protection Policy) – L3 Protocol Authentication – Bandwidth Rate Limiting – Port Mirror / Traffic Redirect Secure Management – SNMPv3 Management – SSH v2 Secure Shell Client	– Traffic Classification – Advanced QoS – Bandwidth Control (minimum granularity 64Kbps) – Hardware Multicast Routing (lower latency) – PIM-SM, PIM-DM – **IPFIX*** – **LPM** (L3 switching of Longest Prefix Matching) – **VRF** (Virtual Routing and Forwarding)	– IPv6 Ready (H/W based) – **BGP4+** – **Policy Based Route** – VRRP – OSPF v2/v3 – **ECMP, WCMP** (Equal-cost multi-path routing, Weight-Cost Multipath Routing) – **RERP** (Rapid Ethernet Ring Protection 50~200ms convergence) – **MPLS** – **VPLS*** – **NAT/Firewall***

*-trwają prace

Zintegrowany system ochrony sieci



#4 Dla użytkowników chcących kontrolować ruch w sieci

Gdy w sieci próbuje rozprzestrzeniać się robak, wielowarstwowe listy ACL pozwalają na zarządzanie ruchem z określonej maszyny w czasie rzeczywistym

#5 Dla użytkowników potrzebujących pełnej aktywnej ochrony

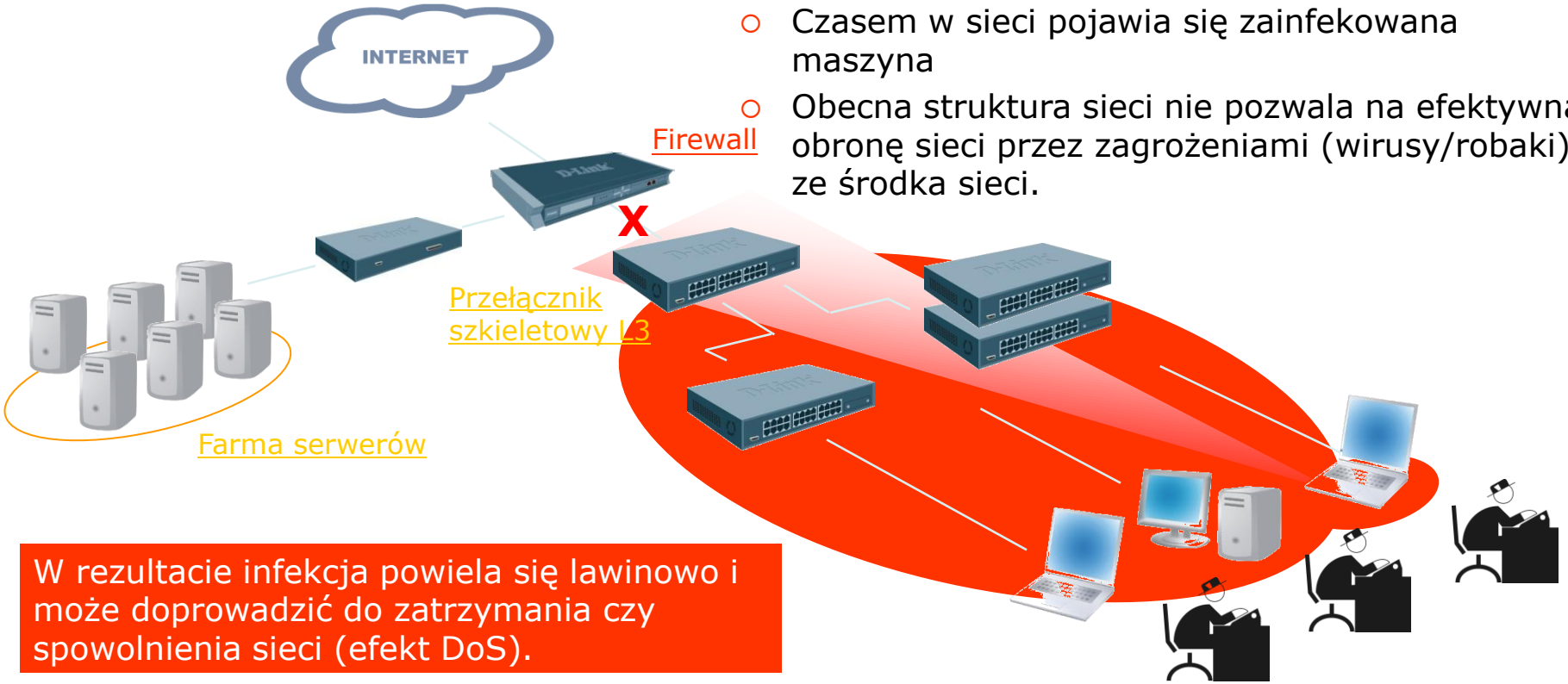
Mechanizm D-Link ZoneDefense pozwala na pełną ochronę sieci przed nienormalnym ruchem wykrytym przez firewall. Firewall ustawia listy ACL w przełącznikach w taki sposób, aby zablokować niechciany ruch. Mechanizm Safeguard Engine chroni dodatkowo sam przełącznik przed niepożądanym ruchem typu broadcast.

Joint Security

MECHANIZMY DOPEŁNIAJĄCE E2ES

Technologia ZoneDefense

- Wyzwania dla bezpieczeństwa obecnych sieci

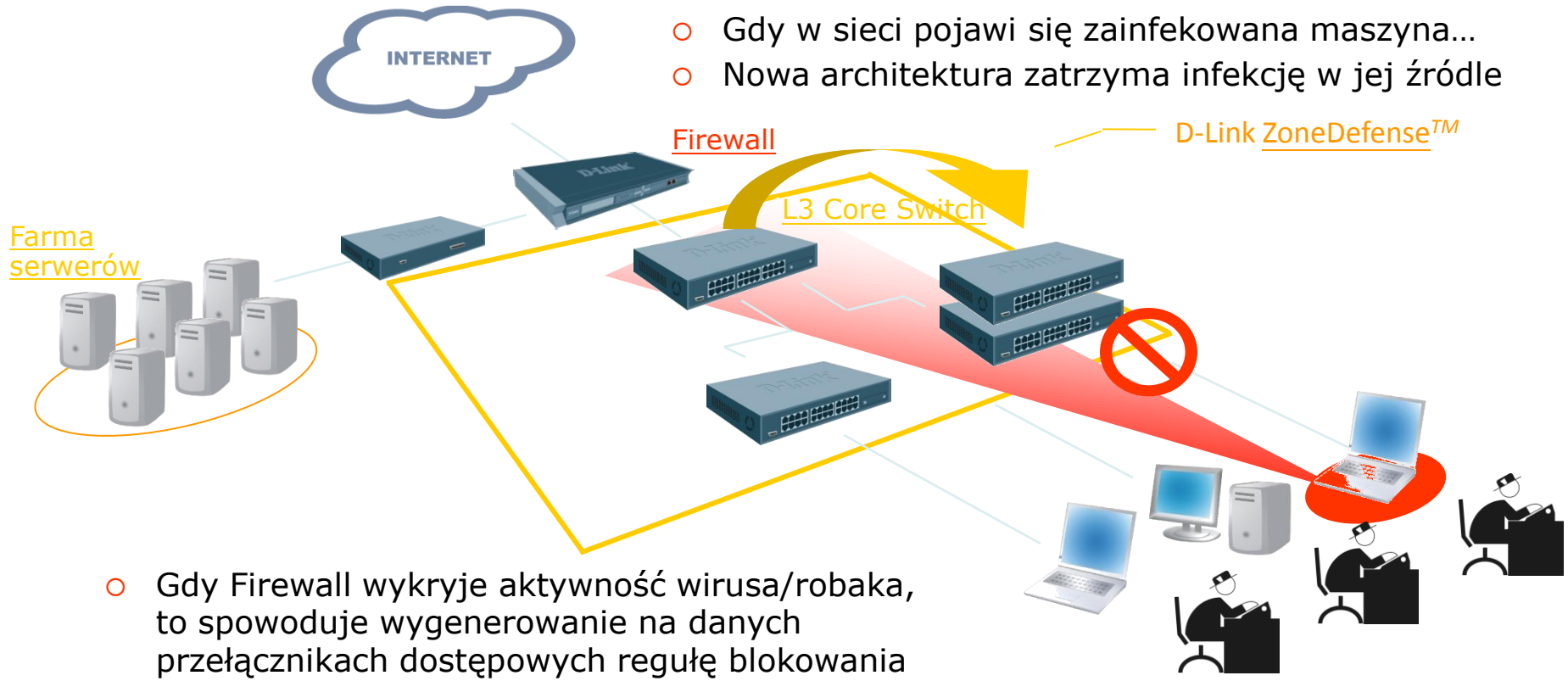


- Tradycyjne zapory mają ograniczoną ilość portów oraz wydajność, zatem routing L3 wciąż oparty jest na przełącznikach warstwy 3.
- Czasem w sieci pojawia się zainfekowana maszyna
- Obecna struktura sieci nie pozwala na efektywną obronę sieci przez zagrożeniami (wirusy/robaki) ze środka sieci.

W rezultacie infekcja powiela się lawinowo i może doprowadzić do zatrzymania czy spowolnienia sieci (efekt DoS).

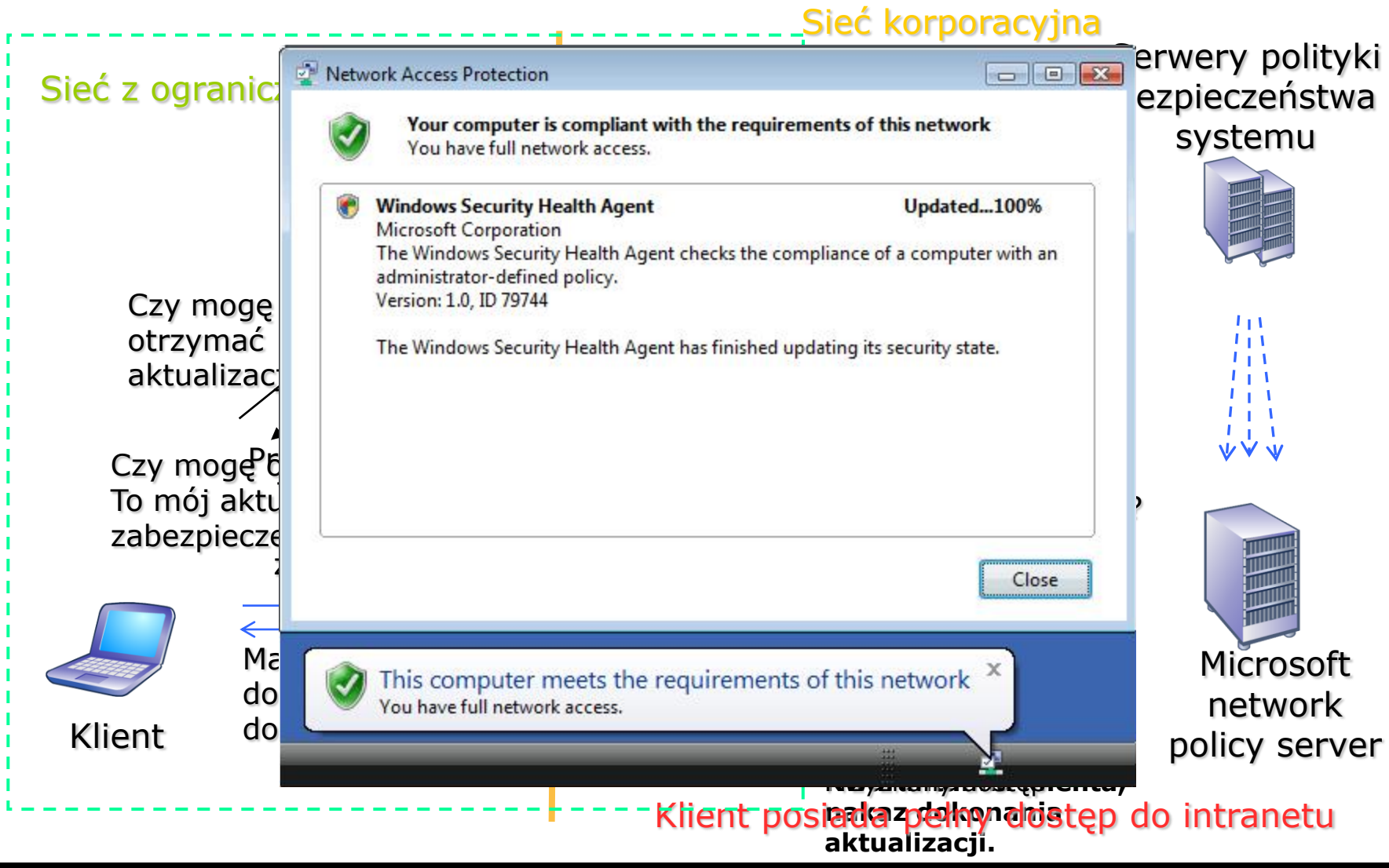
Technologia ZoneDefense

- Nowa bezpieczna architektura sieci
  - Nowe, wieloportowe i wydajne zapory sieciowe są w stanie przejąć przełączanie w warstwie 3 i umożliwiają ustalenie bezpiecznych reguł przejścia ruchu pomiędzy podsieciami.
  - Gdy w sieci pojawi się zainfekowana maszyna…
  - Nowa architektura zatrzymа infekcję w jej źródle



  - Gdy Firewall wykryje aktywność wirusa/robaka, to spowoduje wygenerowanie na danych przełącznikach dostępowych regułę blokowania podejrzanego ruchu, co zaowocuje szybkim stłumieniem infekcji.

Microsoft NAP



DHCP NAP

- Niezależnie od integracji z Microsoft NAP (802.1X), D-Link wspiera **DHCP NAP** dla rynku SMB
  - Przed przydziałem adresu IP, Network Policy Server (NPS) sprawdzi „status zdrowia” klienta NAP
  - Jeśli jest ok, klient zostanie wpuszczony ze standardowym adresem IP
  - Jeśli nie jest ok, to wtedy dostanie adres ze specjalnej puli bez przydzielonej bramy domyślnej
- Opcje dodane przez D-Linka:
  - **Integracja z IMPB w celu ochrony przed ręczną zmianą adresacji**
  - **Ochrona przed działalnością obcych serwerów DHCP przy pomocy mechanizmu DHCP Server Screening**
- Korzyści dla użytkownika
  - Zbędna konfiguracja klienta 802.1X – łatwa konfiguracja i zarządzanie
  - Całkowicie przeźroczyste dla użytkowników
  - Wysoka integracja z siecią bez dodatkowych kosztów

D-Link Green

- Sprawdzanie stanu końcówki: śpi czy pracuje
- Sprawdzanie długości skrętki pomiędzy portem a końcówką
- Elektroniki przełączników wykonane w najnowszej technologii miniaturyzacji – mały pobór mocy
- Brak potrzeby stosowania wentylatorów lub wentylatory auto włączane i wyłączane
- Praca portów PoE wg harmonogramu użytkownika

dlink green™

DGS-3200 jest pierwszym z serii xStack wykonanym w technologii GreenEthernet

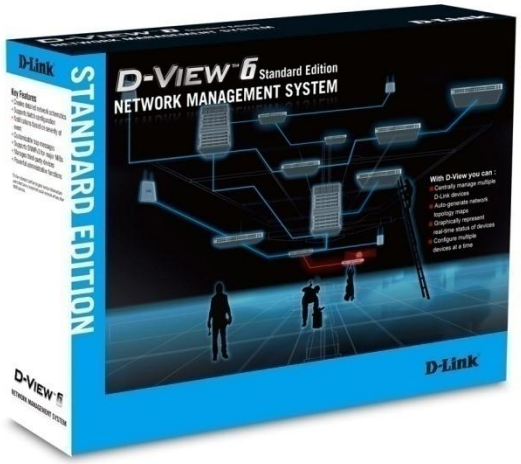
Network Management System

D-View 6.0

D-Link®
Building Networks for People

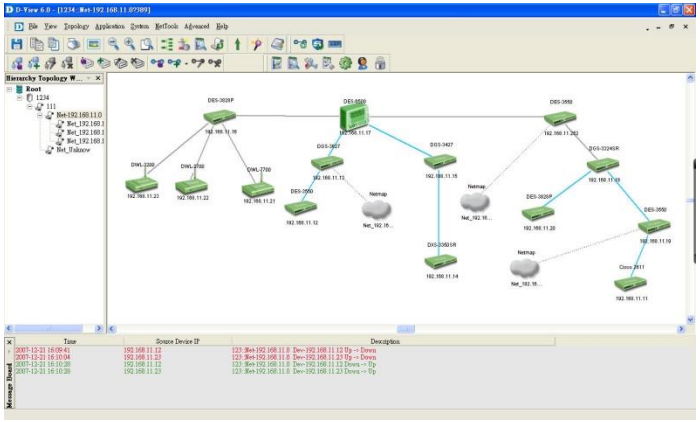
D-View 6.0 – NMS

- D-View 6.0 Standard Edition (**DV-600S**):
  - dla SMB
  - wspiera do 1000 końcówek klienckich
  - bazuje na wbudowanej bazie danych Microsoft Access



- D-View 6.0 Professional Edition (**DV-600P**):
  - dla dużych przedsiębiorstw, telekomów oraz ISP
  - wspiera ponad 1000 końcówek klienckich
  - limit górny stanowi pojemność zewnętrznej bazy danych Microsoft SQL

- Pełnofunkcjonalny trial 30 dni wersji std
  - Dodawany także do przełączników xStack
- Obsługuje urządzenia SNMP innych producentów
- Budowa modularna (Plugin'y)



D-View 6.0 – budowa modułowa

D-View 6.0

- Mapa topologii
- Auto wykrywanie zmian topologii
- konfiguracja grupy urządzeń
- Personalizowane alarmy/powiadomienia
- Rozproszona architektura

D-View 6.0
E2ES Console Plug-in

- IP MAC Port Binding
- ACL batch configuration
- ZoneDefense
- Loopback Detection
- Port Security
- RADIUS Server

Service Pack 2

- Scheduling
- Support Windows Vista (Standard Version)
- Multiple mailing list
- L3 topology map
- Inventory Management
- Link color will change when connection problem occurred
- Be able to configure trap notification by port

D-View 6.0
Wireless Plug-in

- Multiple DWS Management
- Unified AP Management
- Fat AP Management

D-View 6.0
NetDefend Plug-in

- Batch Configuration
- Central Pattern Update Server
- Reporting
- Fault / Alarm Management

D-View 6.0
Reporting Plug-in (Free)

- Professional supports full function
- Standard provides templates
- Collect specific MIB data
- Query the history report

Phase I Phase II Phase III Phase IV

Case Study

WDROŻENIA W POLSCE

Case Study: Śląska Grupa Telekomunikacyjna, operatorzy skupieni wokół projektu jambox.pl

- Sieć dostępowa dla klientów operatorów ETTH
- Core: Cisco Catalyst 6500 i D-Link DGS-36XX,
- Dystrybucja: DGS-36XX
- Agregacja: DES-31XX
- Access: DES-35XX, DES-30XX
- Usługi: TriplePlay, Internet
- Aplikacje: DHCP Relay, PIM
- Wykorzystywane funkcjonalności przełączników D-Link:
  - SNMP (monitoring pracy)
  - IGMP (IPTV, multicasting)
  - ACL, IP-MAC-Port Binding, QOS, DHCP Snooping
  - VLANs
- Dlaczego D-Link?
  - Dobry stosunek cena/możliwości
  - Pozytywne testy w „żywej” infrastrukturze

SGT
ŚLĄSKA GRUPA TELEKOMUNIKACYJNA

Case Study: Stream Communication Sp. z o.o.

- Sieć dostępowa dla klientów osiedlowych
  - sygnał rozchodzi się po budynkach po światłowodach lub miedzi
  - okablowanie: w blokach miedź, dojście światłowód
- Core: Cisco i DGS-3627G
- Access: DES-3028
  - Przydział adresu IP na podstawie portu na switchu (DHCP opcja 82) bez kontroli adresu MAC
  - Kontrola pakietów jak najbliżej klienta: ustawianie pasma wielkości oraz ewentualne blokady (np. porty 25, 135-139). Część kontroli odbywa się globalnie na DGS-3627
- Usługi: TriplePlay
- Wykorzystywane funkcjonalności przełączników D-Link:
  - QoS - uproszczony: 1 – management 2 – VoIP 3 - reszta ruchu
  - SNMP (monitoring pracy), IGMP (IPTV, multicasting)
  - ACL, IP-MAC-Port Binding, QOS, Bandwith Control, VLANs
- Dlaczego D-Link?
  - Dobry stosunek cena/możliwości
  - Pozytywne testy w „żywej” infrastrukturze
  - Dobre referencje z rynku polskiego

Case Study: TVK Hajnówka Sp.j

- Sieć dostępowa dla klientów osiedlowych
  - okablowanie: w blokach miedź 1G, dojście światłowód (m.konwerter DMC-810SC)
- Core: przełącznik Cisco
- Access: DXS-3350SR, DES-3526, DGS-1216T
- Usługi: VoIP
- Wykorzystywane funkcjonalności przełączników D-Link:
  - SNMP (monitoring pracy)
  - ACL, IP-MAC-Port Binding, QOS
  - VLANs
- Dlaczego D-Link?
  - Dobry stosunek cena/możliwości
  - Pozytywne testy w „żywej” infrastrukturze
  - Dobre referencje z rynku polskiego

Case Study: Internetia Sp. z o.o.

- Sieć dostępowa dla klientów osiedlowych
  - okablowanie: w blokach miedź, dojście światłowód
- Core: 3Com seria 5500G-EI oraz D- Link DXS-3326 i DGS-3600
- Access: seria DES-3500 i DES-3226
- Usługi: Internet, VoIP, iptv w testach
- Wykorzystywane funkcjonalności przełączników D-Link:
  - SNMP – monitoring
  - ACL - generator konfiguracji połączony z bazą danych o klientach który potrafi: zatrzasnąć klienta (MAC i IP) na porcie, przyciąć ilość MAC per port, zablokować komunikację DHCP z portu klienckiego
  - VLAN – osiedla „zamknięte” w VLAN, ogromna elastyczność sieci
  - LACP - agregacja kilku łączy radiowych (STM1)
  - Bandwith Control
- Dlaczego D-Link?
  - Bardzo dobry stosunek cena/możliwości
  - Bardzo dobry serwis (FixIT)
  - Działa !!! ☺

netia
WOLNOŚĆ WYBORU

Case Study: Internet Solutions/Tarnów

- Sieć miejska (~7000 portów D-Link)
  - okablowanie: w blokach miedź, dojście światłowód
- Core: przełącznik Cisco 6500, **4x** D-Link DGS-3627(G) [stack]
- Access: ponad **250** przełączników DES-35xx, miedziane porty abonenckie, uplinki optyczne na wkładkach SFP 1Gbps
- Usługi: TriplePlay
- Wykorzystywane funkcje przełączników D-Link:
  - SNMP (monitoring pracy), SNMPv3 (zarządzanie – system autorski)
  - Agregacja L2, terminowanie L3 po 10GE w Cisco
  - IGMP (IPTV, multicasting)
  - ACL, IP-MAC-Port Binding, QoS, Bandwith Control, Packet Content Filter [hardware]
  - Loopback detection, broadcast/multicast storm control
  - LACP, STP, Stacking, VLANs
- Dlaczego D-Link?
  - Sprzętowe Packet Content Filter [do 86 bajtów nagłówka IP]
  - Stabilność oraz niska awaryjność, bardzo dobry stosunek cena/możliwości
  - Support techniczny, dobry serwis gwarancyjny

internet solutions

Internet Telefon Telewizja

Case Study: IST S.C.

- Sieć miejska
  - okablowanie: w blokach miedź, dojście światłowód
- Core: HP Procurve
- Access: przełączniki D-Link: FE L2, uplinki 1GE FO: DES-3526 i DES-3550
- Agregacja: DGS-3627G
- Usługi: Internet, Telefonia VOIP jako oddzielny VLAN, IPTV Multicast - usługa niekomercyjna w fazie testów
- Wykorzystywane funkcje przełączników D-Link:
  - SNMP (monitoring pracy)
  - IGMP (IPTV, multicasting)
  - ACL, IP-MAC-Port Binding, QOS 802.1p, DHCP Snooping
  - VLAN 802.1q,
  - PIM - w fazie testów
- Dlaczego D-Link?
  - bardzo dobry stosunek cena/możliwości

Case Study: Zeto S.A.

- Sieć dostępowa dla klientów osiedlowych
  - okablowanie: w blokach miedź 1G (porty 100 MB), dojście światłowód
- Core: przełącznik Cisco
- Access: przełączniki D-Link: FE L2, uplinki 1GE FO
- Usługi: Triple Play
- Wykorzystywane funkcjonalności przełączników D-Link:
  - SNMP (monitoring pracy)
  - IGMP (IPTV, multicasting)
  - ACL, IP-MAC-Port Binding, QOS
  - VLANs
- Dlaczego D-Link?
  - Dobry stosunek cena/możliwości
  - Pozytywne testy w „żywej” infrastrukturze
  - Dobre referencje z rynku polskiego
  - *„Pomijam, że pewnie gdzieś podświadomie przeczuwałem, że będę współpracował z Panią Agatą Malarczyk, a to jest argument nie do odparcia:)”*

Dziękuję za uwagę

Pytania?

mwojcik@dlink.pl
amalarczyk@dlink.pl