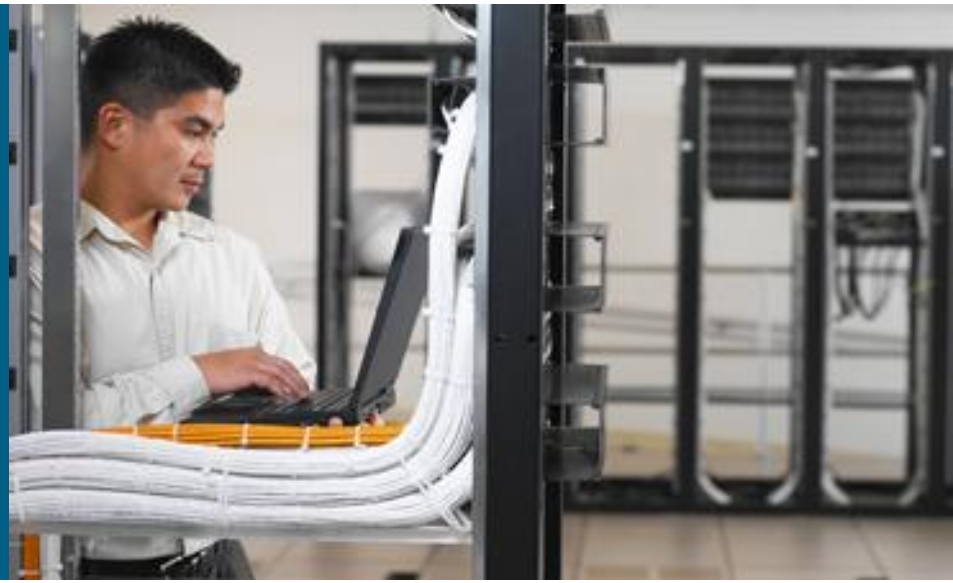
Budowa sieci:
szkielet / agregacja / dostęp

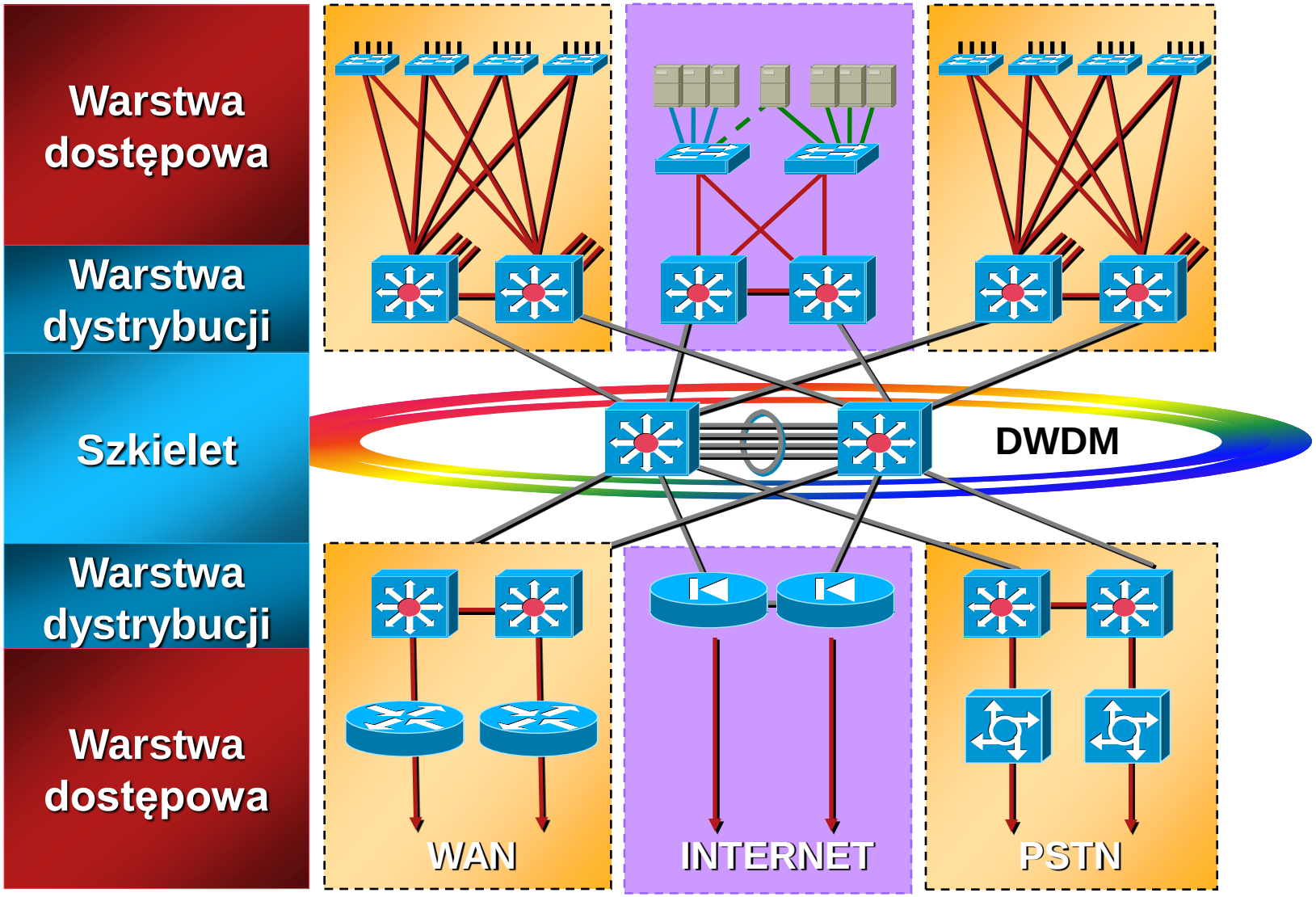


Marcin Aronowski
maaronow@cisco.com

Warszawa, marzec 2011

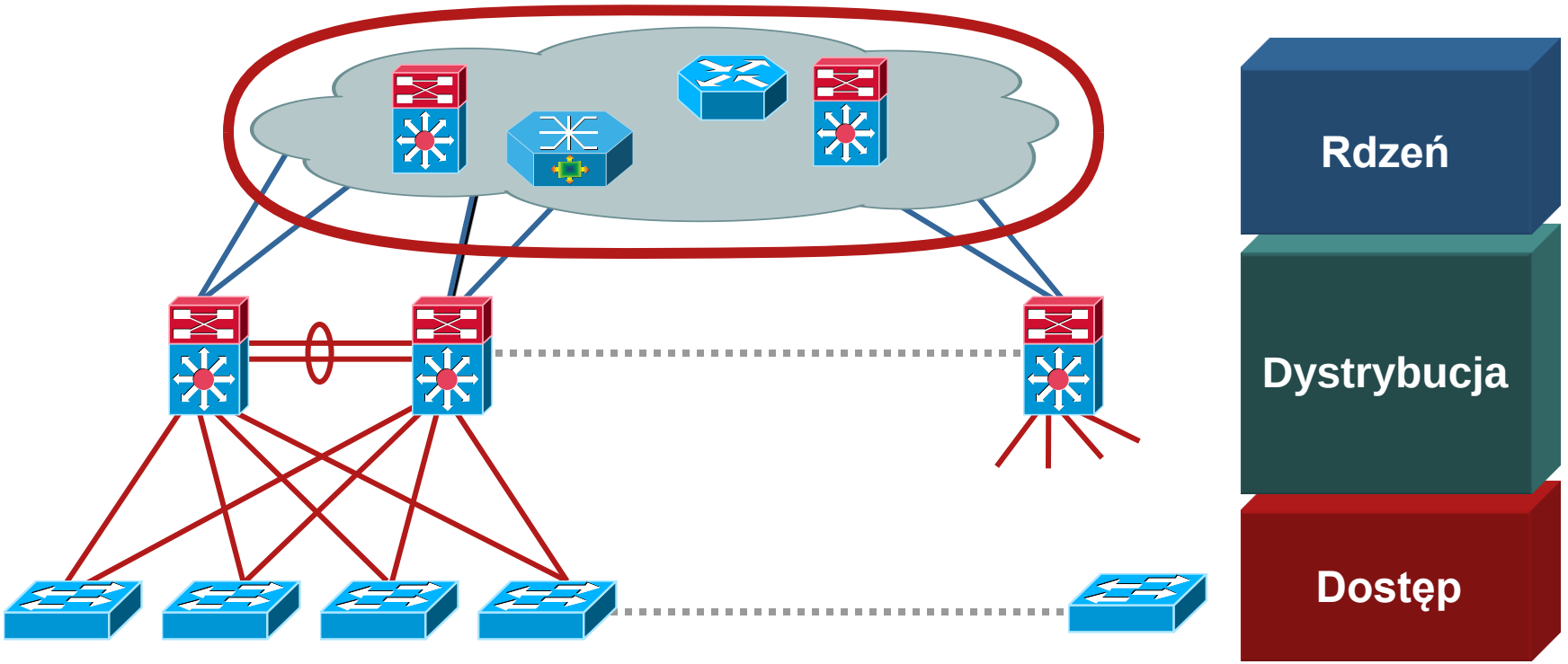
Hierarchia w LAN

Hierarchiczny model sieci LAN



Definicja rdzenia sieci

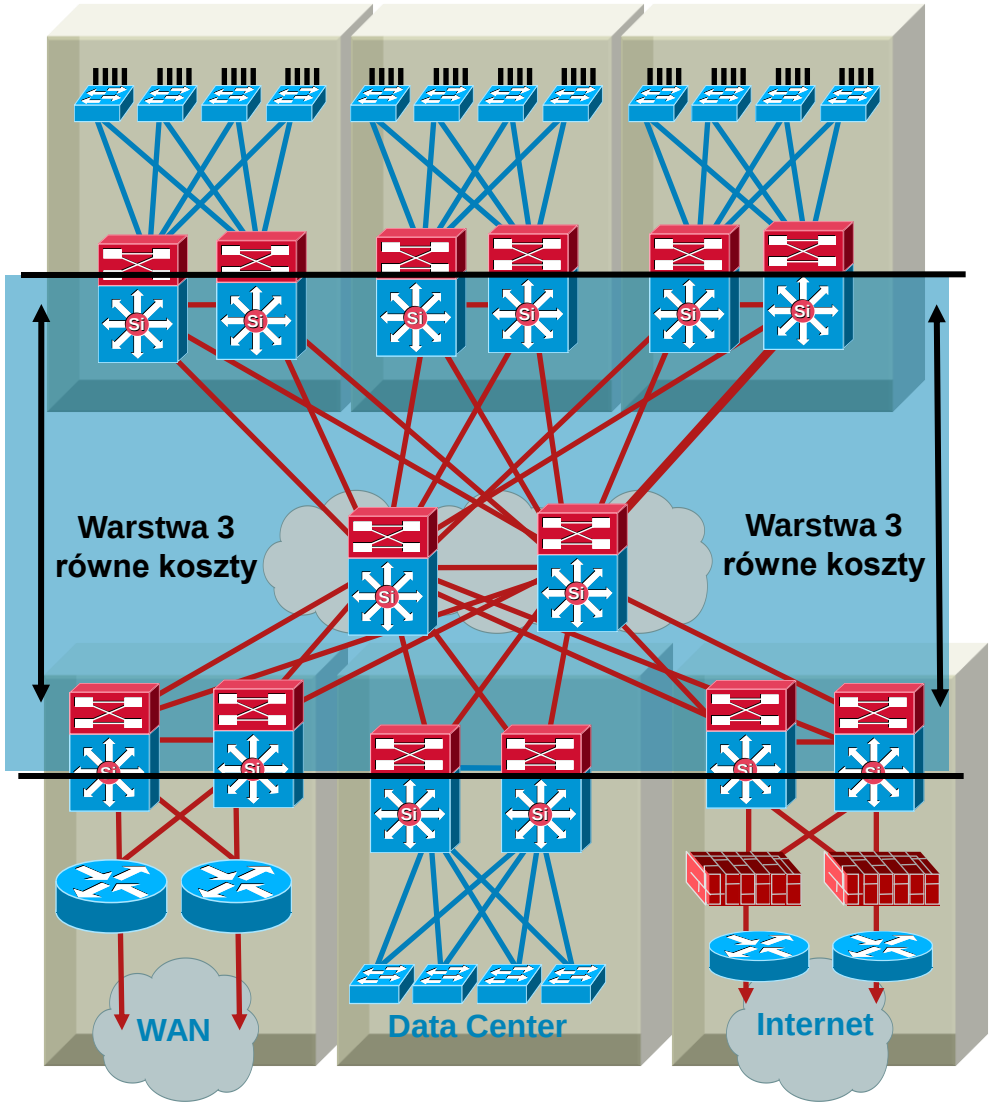
Skalowalność, niezawodność, szybka zbieżność



- Szkielet dla całej sieci – łączy poszczególne bloki funkcjonalne
- Wydajność i stabilność a złożoność
- Agregacja dla warstwy dystrybucji
- Dedykowany rdzeń pozwala na łatwiejszą rozbudowę sieci

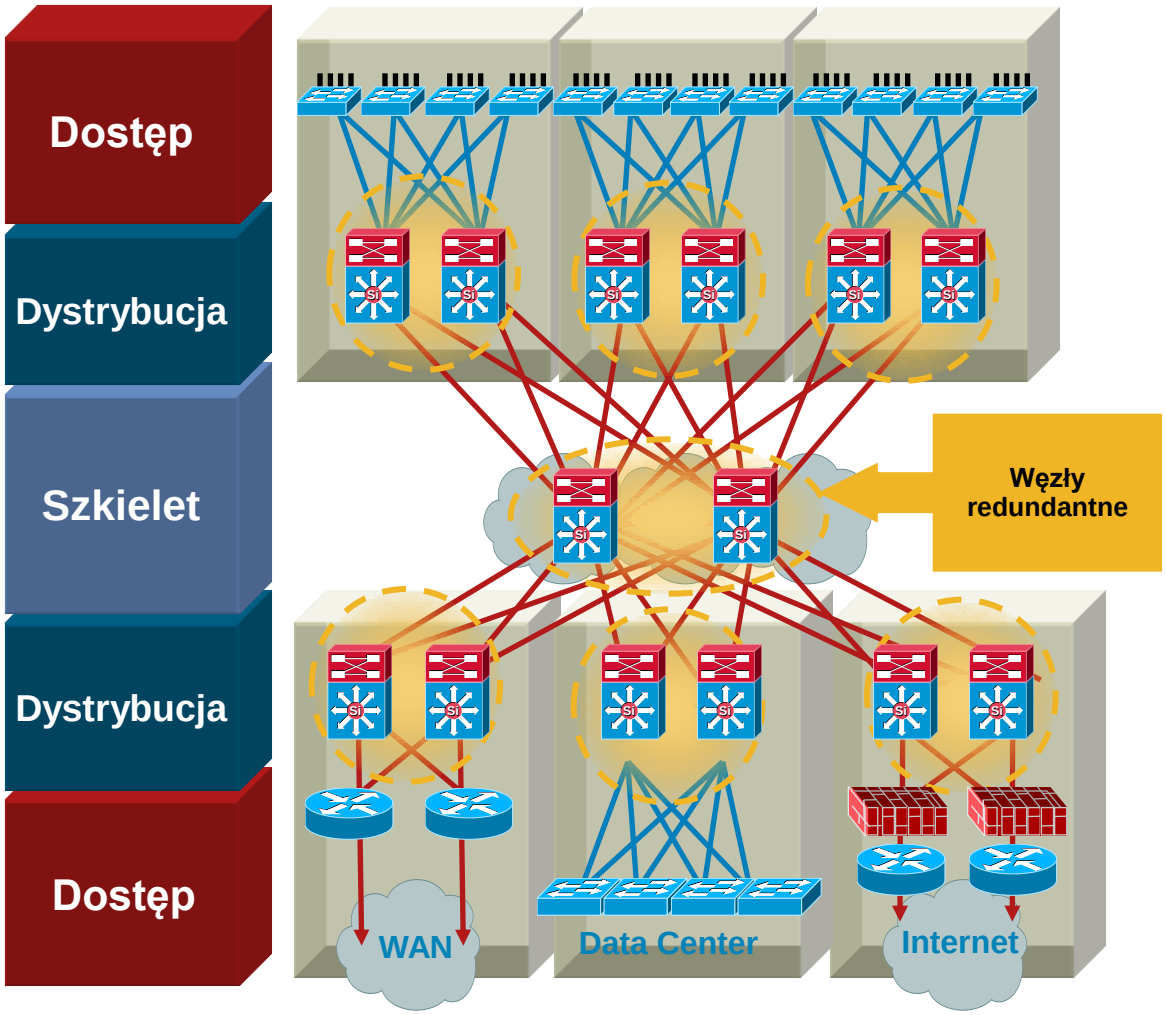
Rdzeń sieci – L3

- Zasadniczo pomiędzy dystrybucją i rdzeniem oraz w ramach rdzenia sieci
- Szybka zmiana trasy w przypadku awarii
- Lepiej budować „trójkąty” niż „czworokąty” – przewidywalna zbieżność
- Redundantne połączenia L3, aby uniknąć „czarnych dziur”
- Sumaryzacja w stronę rdzenia ogranicza zapytania EIGRP oraz propagację LSA OSPFa
- Tuning mechanizmów przesyłania (np. CEF) L3/L4 pozwala na pełne wykorzystanie łączy

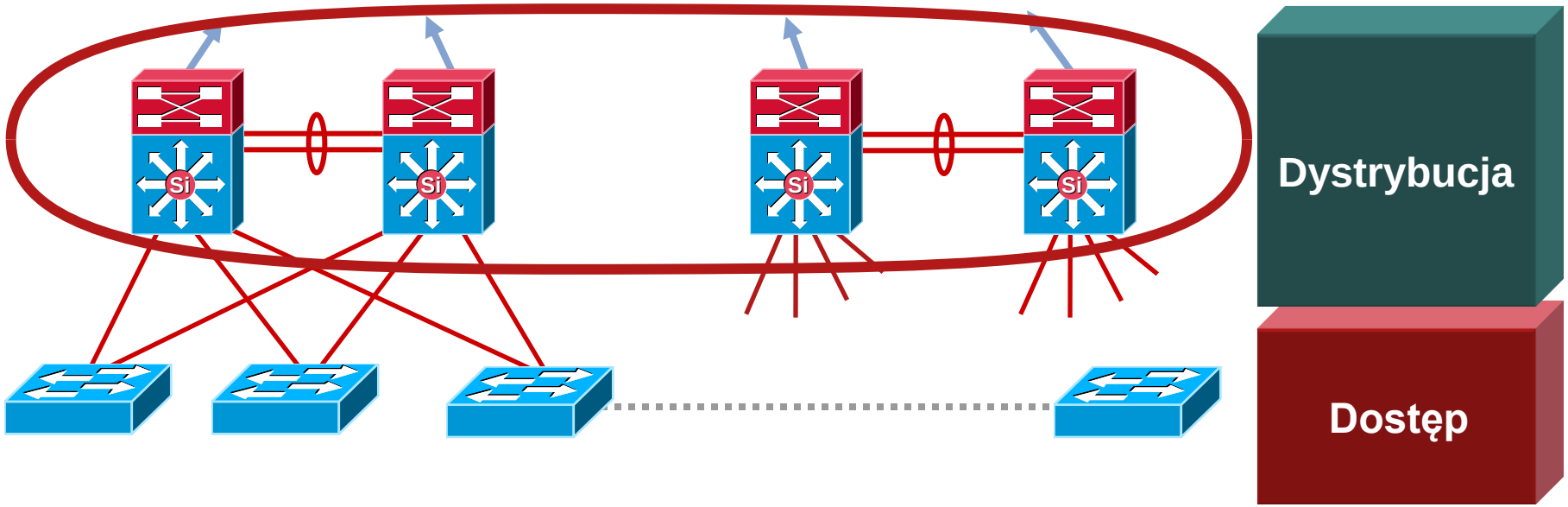


Rdzeń sieci – redundancja NSF/SSO

- W momencie wystąpienia awarii modułu zarządzającego ruch jest nadal przekazywany – zapasowy Supervisor tylko odświeża a nie odbudowuje tablicę FIB
- NSF = Non-Stop Forwarding
- SSO = Stateful SwitchOver



Definicja warstwy dystrybucyjnej
Zbieżność, QoS i duża niezawodność

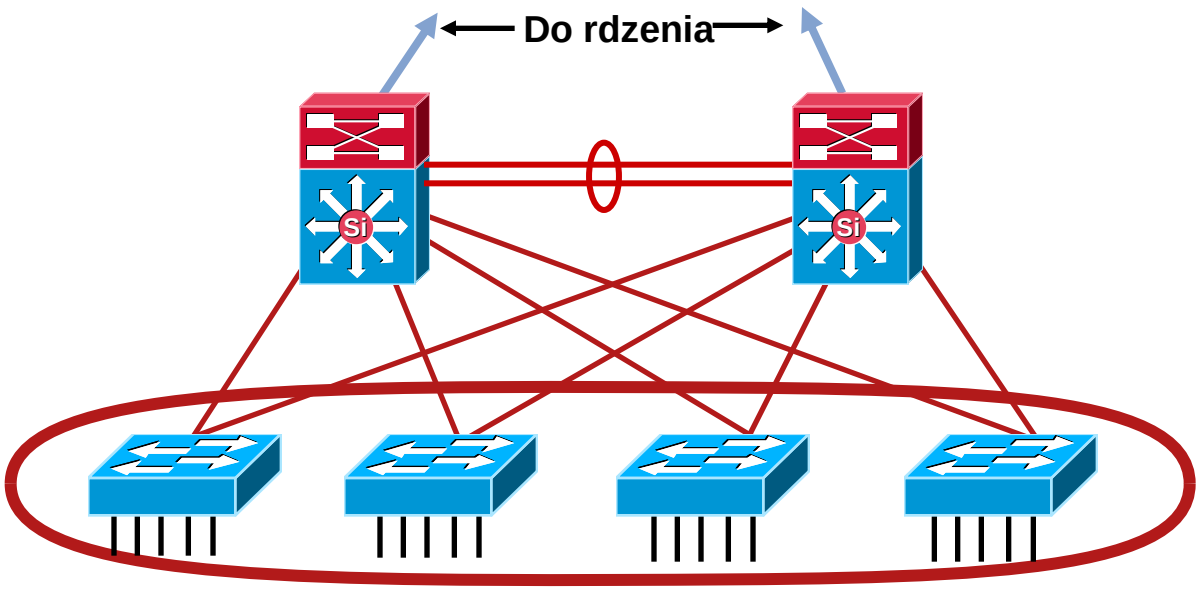


- Niezawodność, równoważenie ruchu, QoS
- Agregacja ruchu z warstwy dostępowej i połączenie do rdzenia
- Przełączanie w warstwie 3
- Chroni rdzeń przed problemami warstwy dostępowej

- Spanning Tree:
  - Tylko wówczas, gdy konieczne: ustawić STP Root, Root Guard Rapid PVST+—Per VLAN 802.1w
- Sumaryzacja, szybka zbieżność, redundantne ścieżki, równoważenie ruchu
- HSRP lub GLBP dla zapewnienia redundancji

Definicja warstwy dostępowej

Wiele funkcjonalności – to nie tylko łączność

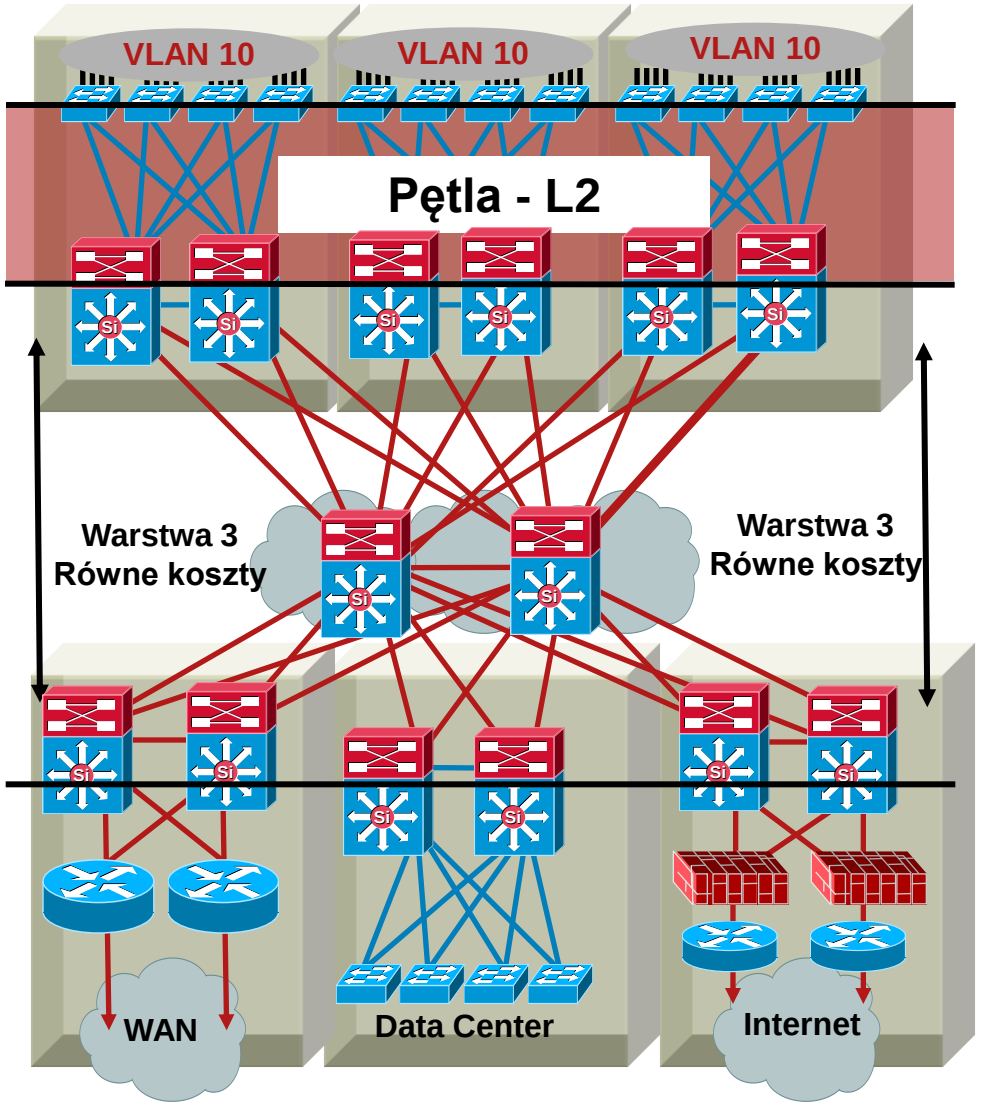


- Agreguje urządzenia
- Funkcjonalności warstwy 2 i 3; zbieżność, niezawodność, bezpieczeństwo, QoS, IP multicast, ...
- Inteligentne usługi: QoS, granica zaufania, ograniczanie broadcastów, IGMP snooping
- Inteligentne usługi sieciowe: PVST+, Rapid PVST+, DTP, PAgP/LACP, UDLD, ...
- Catalyst® - zintegrowane bezpieczeństwo IBNS (802.1x), (CISF): port security, DHCP snooping, DAI, IPSG, ...
- Wykrywanie telefonów IP, zasilanie poprzez Ethernet, prywatne VLANy, ...
- Spanning Tree: Portfast, UplinkFast, BackboneFast, LoopGuard, BPDUGuard, BPDUFilter, RootGuard, ...

Warstwa dostępowa – Spanning Tree

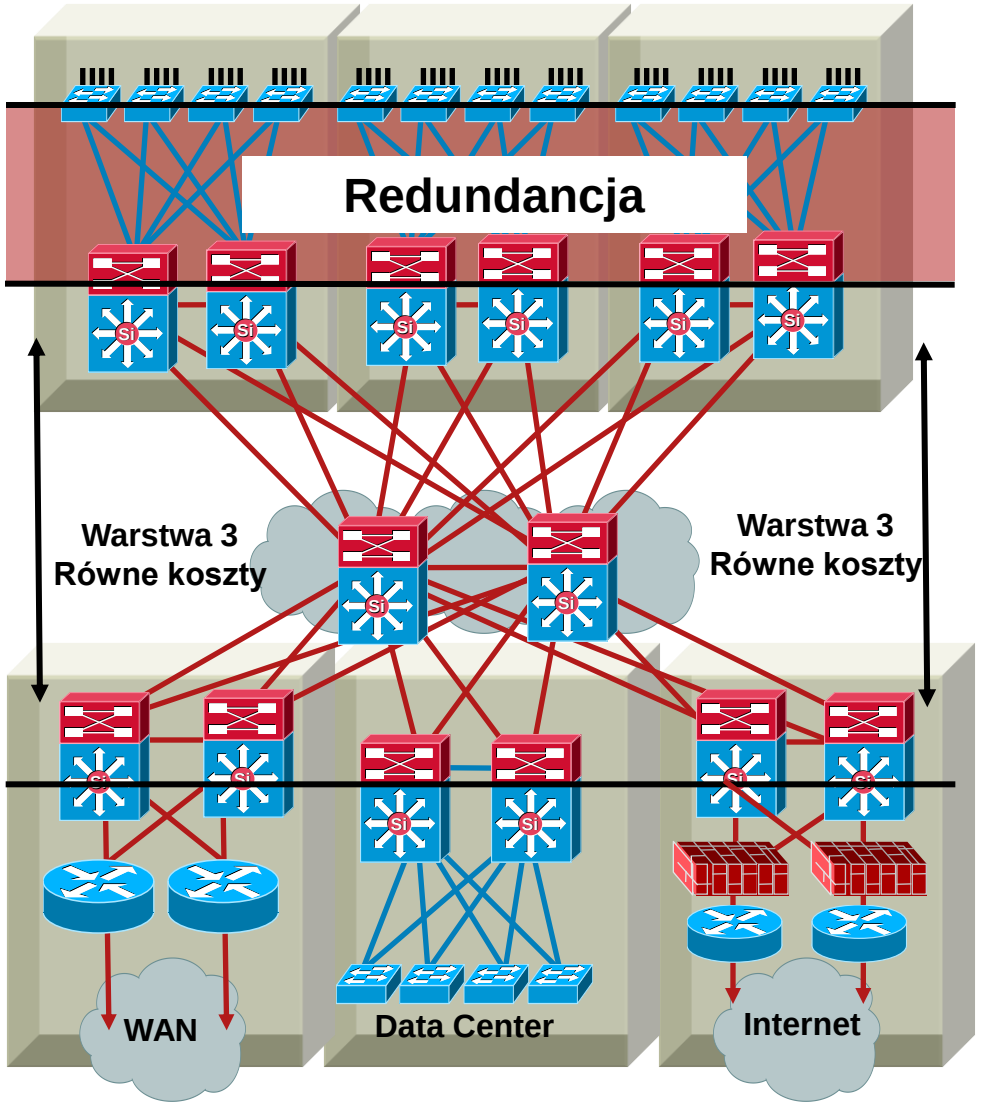
- TYLKO jeśli to konieczne!
- REP, FLEXLink, vPC są lepsze ☺
- Wymagane by uniknąć pętli po stronie użytkownika
- Rapid PVST+ zapewnia lepszą zbieżność
- Należy wykorzystać wszystkie możliwe narzędzia Spanning Tree

  również bezpieczeństwa!



Warstwa dostępowa – redundancja

- Zawsze osiągalny adres bramy domyślnej
- HSRP, VRRP lub GLBP
- VRRP, gdy kilku producentów
- GLBP gwarantuje możliwość równoważenia ruchu



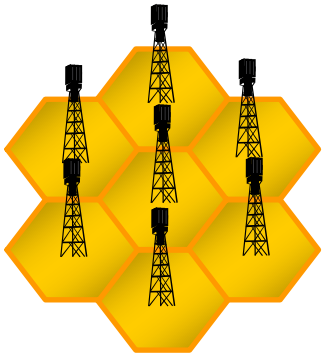
Sieć kampusowa

Wysoka dostępność - narzędzia

poziom aplikacji	**Global Server Load Balancing, Stateful NAT, Stateful IPSec, DNS, DHCP, IP SLA, Netflow**
protokoły warstw wyższych	**NSF/SSO, HSRP, VRRP, GLBP, Graceful Restart (GR): BGP, ISIS, OSPF, EIGRP, OER, BGP Multipath, Fast Polling, BFD, Incremental SPF**
warstwa łącza	**SONET APS, RPR, DWDM, Etherchannel®, 802.1d, 802.1w, 802.1s, PVST+, Portfast, BPDU Guard, PagP, LacP, UDLD, Stackwise, mPPP**
poziom sprzętowy	**Redundantne Procesory (RP), Switch Fabric, karty (LC), Porty, Zasilanie, CoPP, ISSU, Config Rollback**

A jak to zrobić “głębiej” w sieci?

Skalowanie sieci all-IP



Dostęp RAN

Ethernet

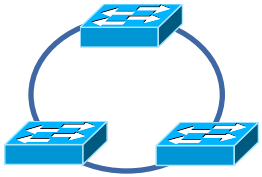
Agregacja RAN

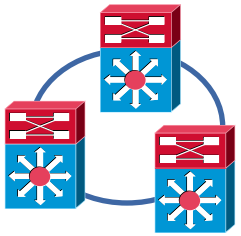
IP/MPLS 10/100GE lub DWDM

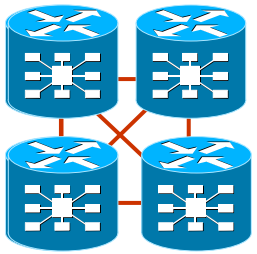
Szkielet IP

IP/MPLS DWDM

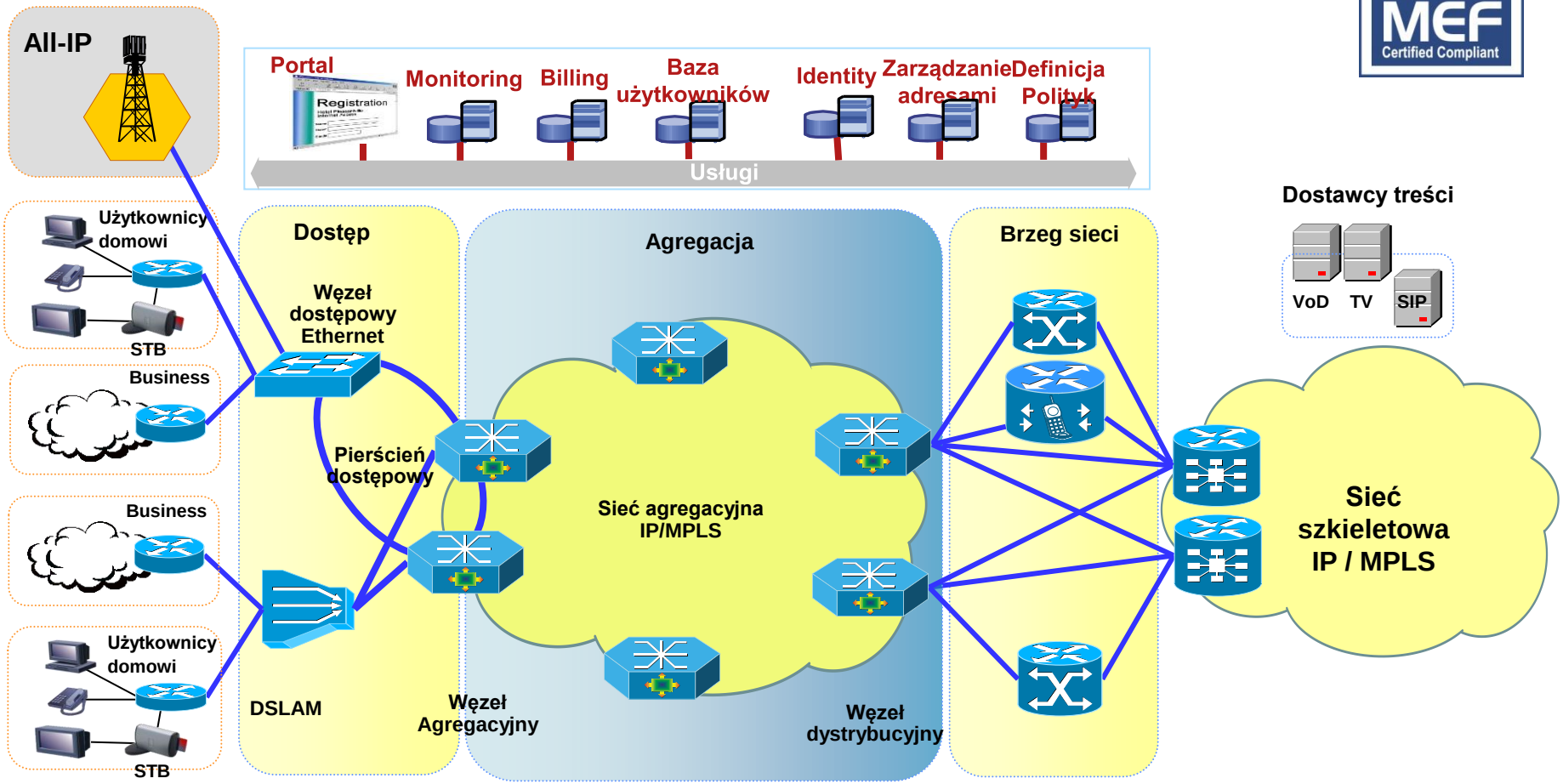
20 Mbps x50 1Gbps x20 20 Gbps x10-50 0.2-1 Tbps







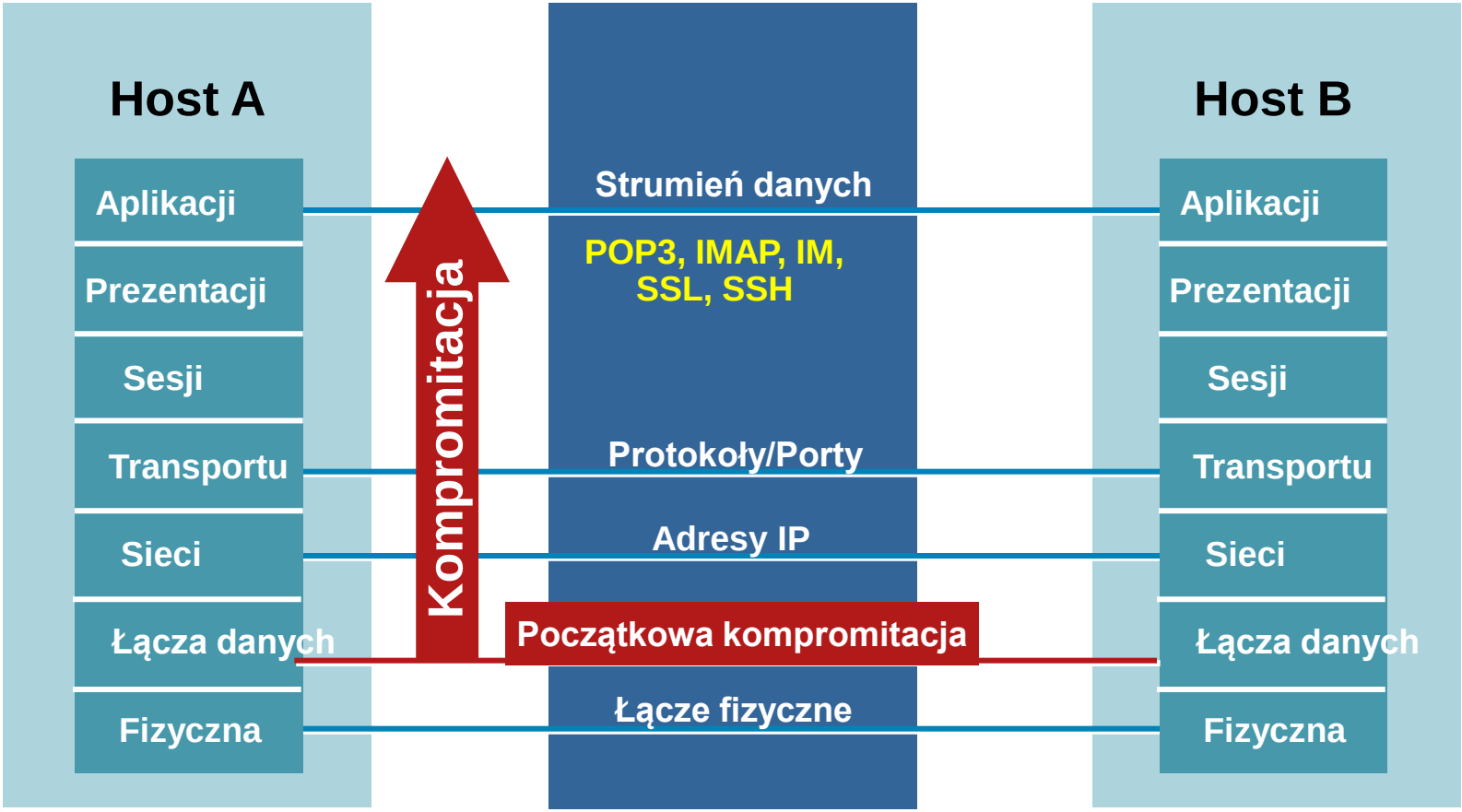
Sieć operatorska



Przykładowa analiza - Bezpieczeństwo L2

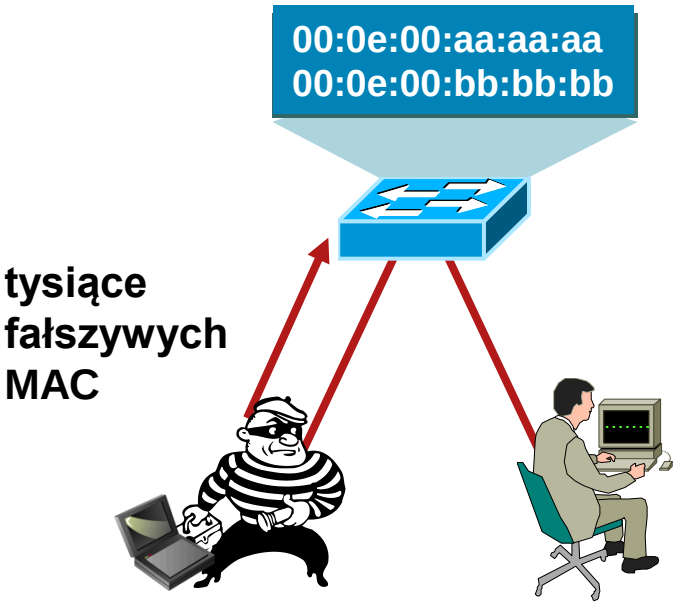
Warstwy niższe OSI wpływają na wyższe

- Kompromitacja warstwy niższej otwiera wyższe na atak – nie są tego świadome
- Bezpieczeństwo jest tak dobre, jak najsłabsze ogniwo architektury
- Warstwa 2 może być bardzo słabym ogniwem



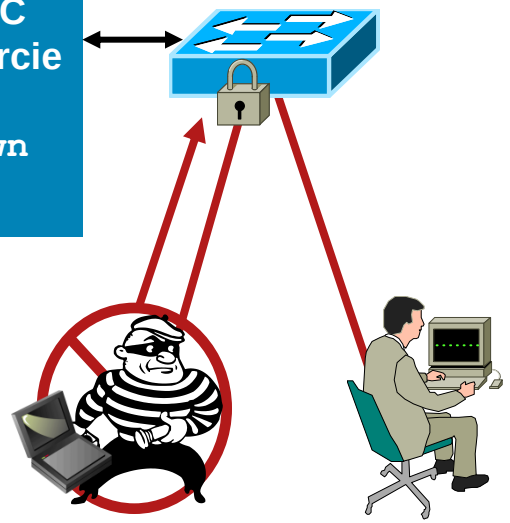
Obrona przed atakami na tablicę CAM

Port Security ogranicza ilość adresów MAC na interfejsie



Tylko jeden MAC dozwolony na porcie

Akcja: `shutdown`

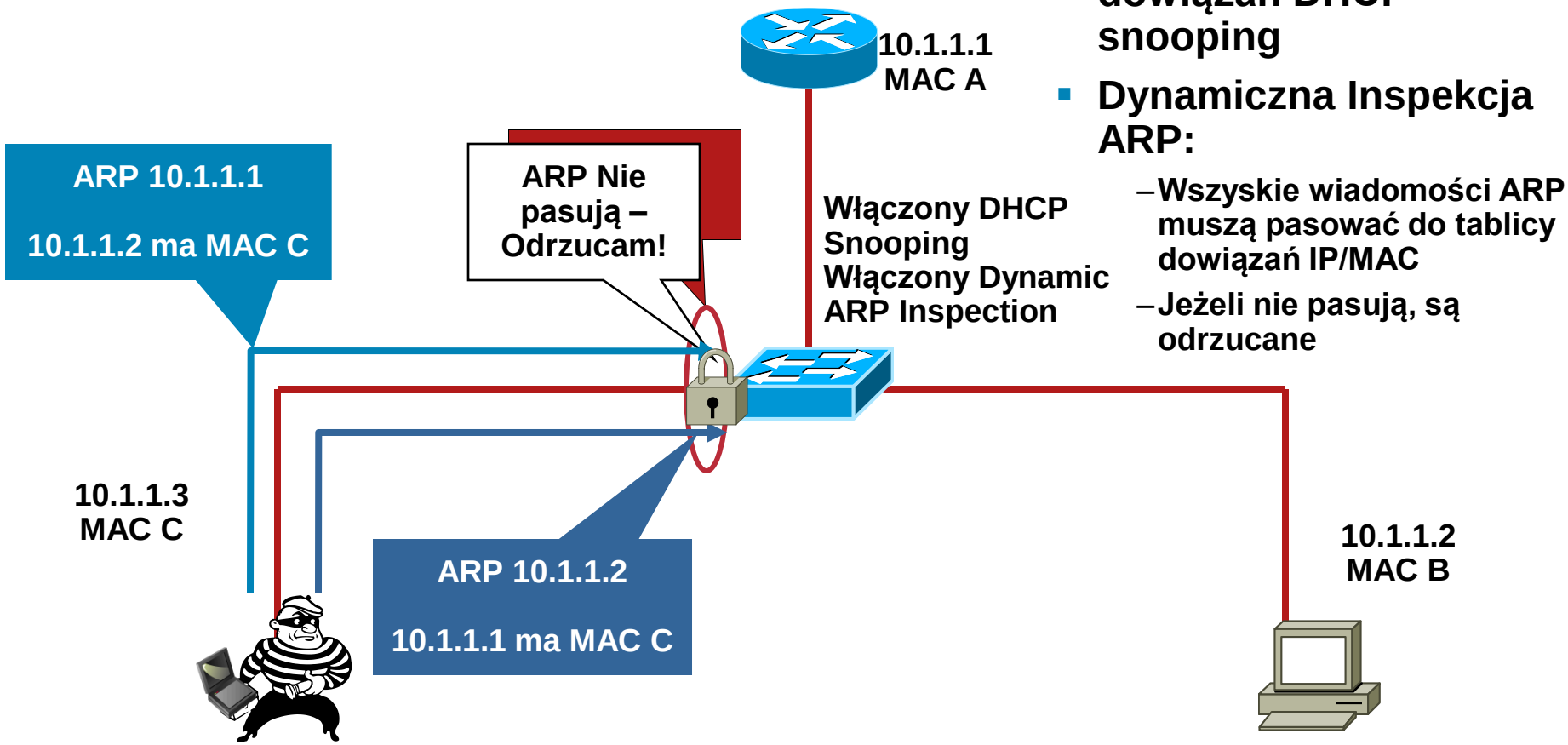


Rozwiązanie:

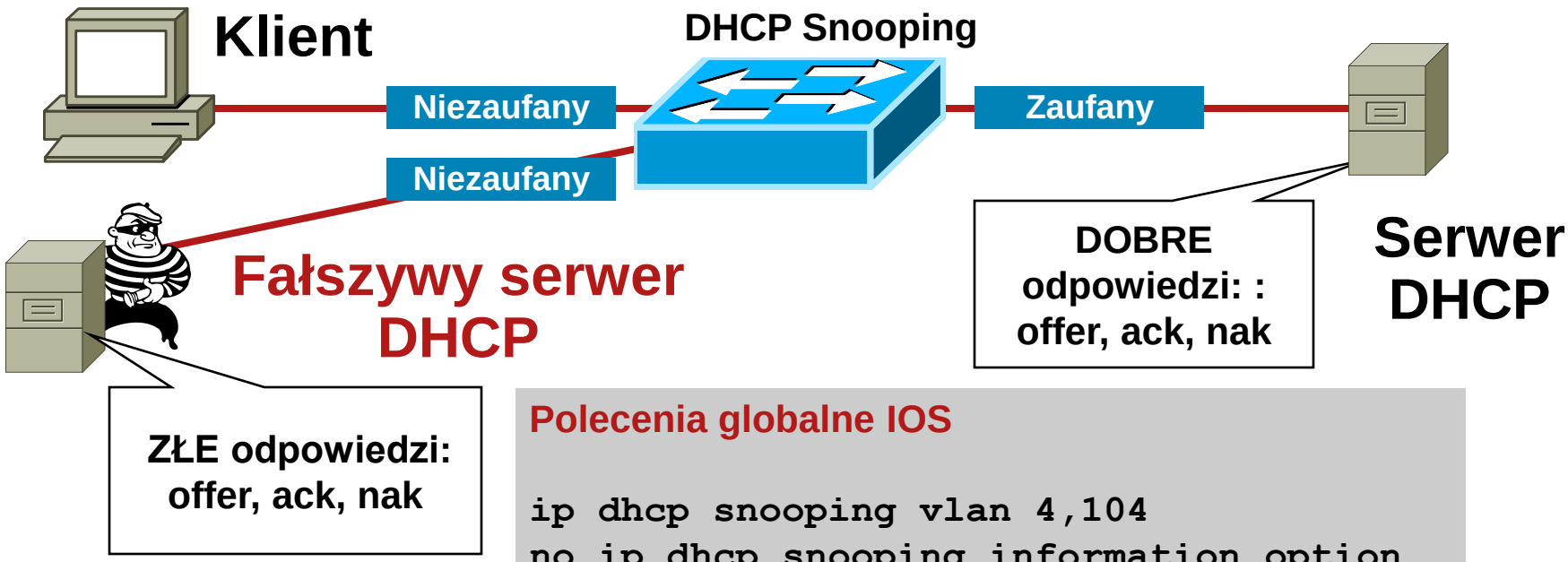
- Mechanizm Port security ogranicza atak MAC flood, wysyła wiadomość SNMP i wyłącza port

Ataki na ARP – ARP snooping

- **Wykorzystuje tablicę dowiązań DHCP snooping**
- **Dynamiczna Inspekcja ARP:**
  - **Wszyskie wiadomości ARP muszą pasować do tablicy dowiązań IP/MAC**
  - **Jeżeli nie pasują, są odrzucane**



Ataki na DHCP – DHCP snooping



Polecenia globalne IOS

```
ip dhcp snooping vlan 4,104
no ip dhcp snooping information option
ip dhcp snooping
```

DHCP Snooping – port niezaufany

Polecenia na porcie niezaufanym

```
no ip dhcp snooping trust (Default)
ip dhcp snooping limit rate 10 (pps)
```

DHCP Snooping – uplink lub serwer

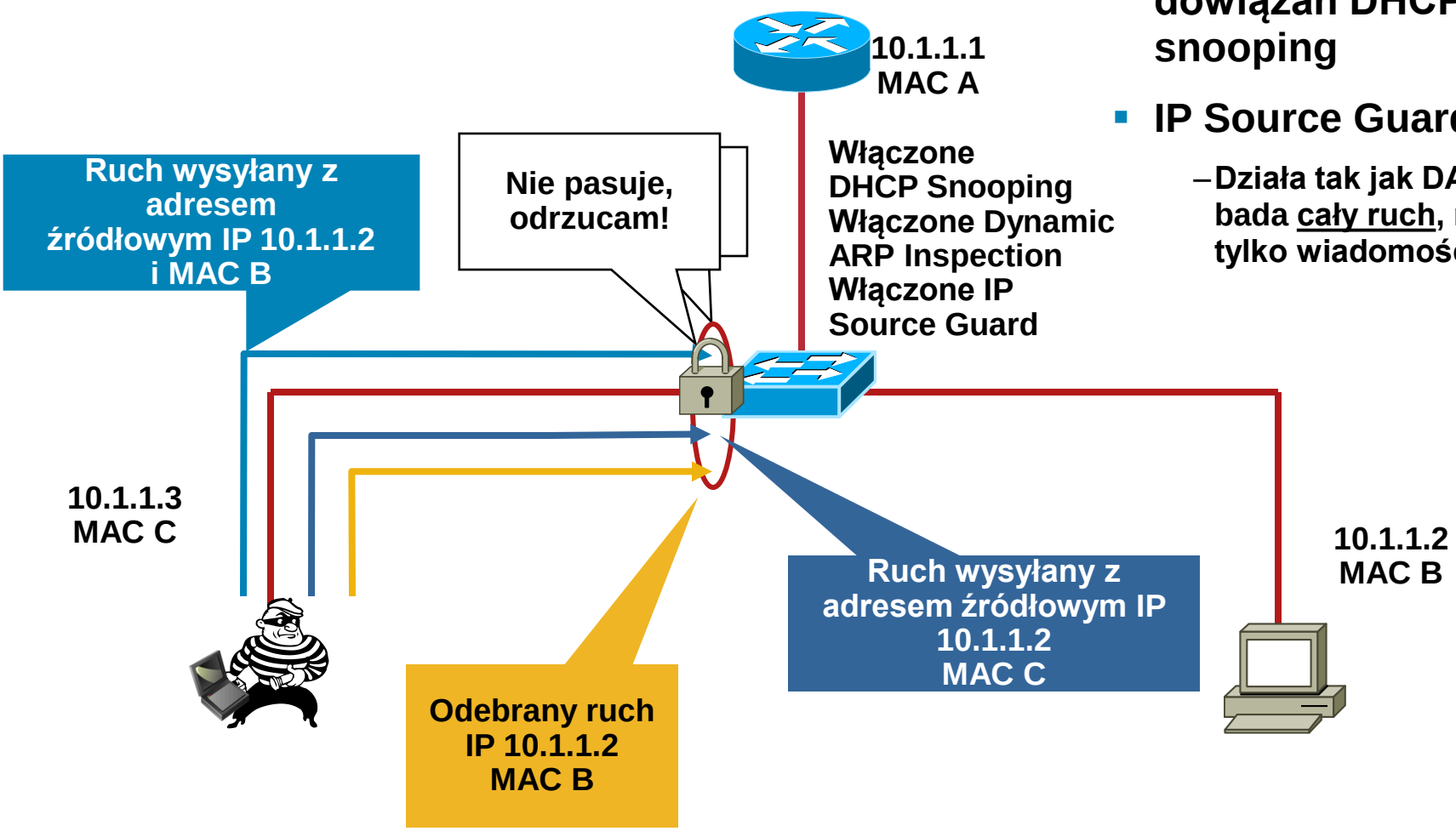
Polecenia na porcie zaufanym

```
ip dhcp snooping trust
```

- **Domyśnie wszystkie porty w VLANie są niezaufane**

Ataki na sieć - IP Source Guard

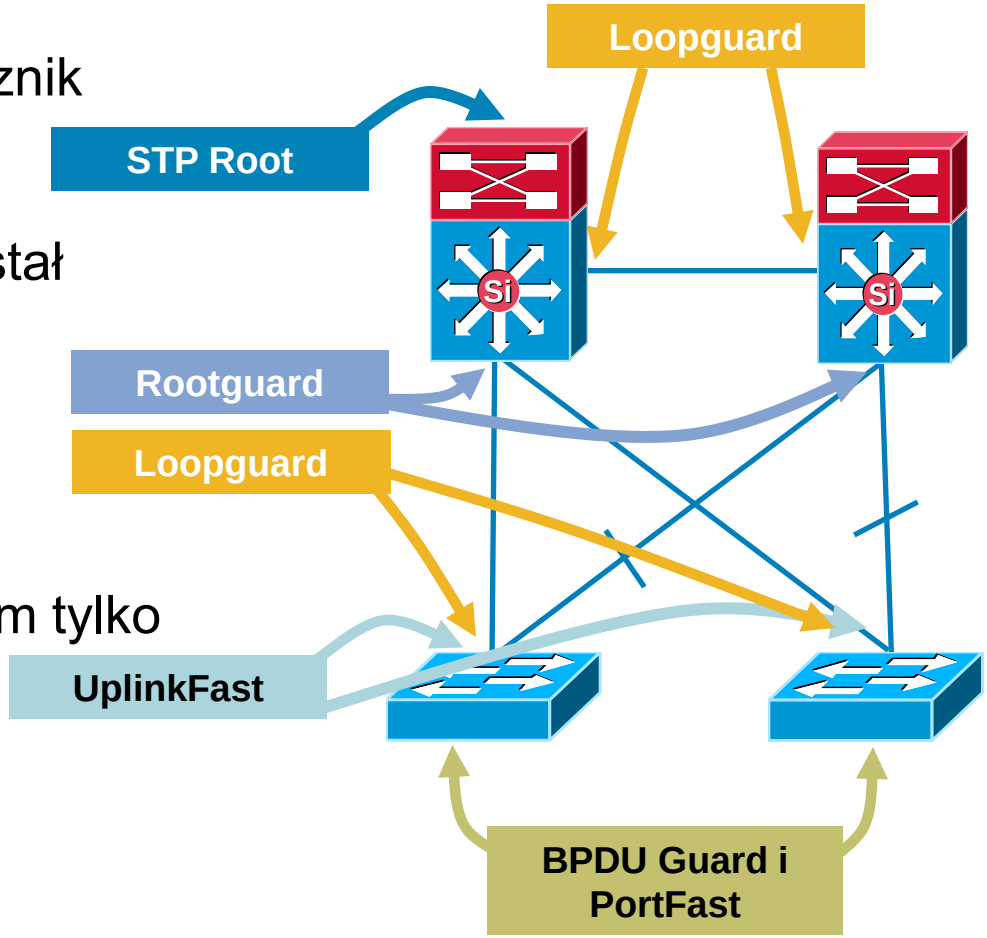
- **Wykorzystuje tablicę dowiązań DHCP snooping**
- **IP Source Guard**
  - **Działa tak jak DAI, ale bada cały ruch, nie tylko wiadomości ARP**



Atak na Spanning Tree

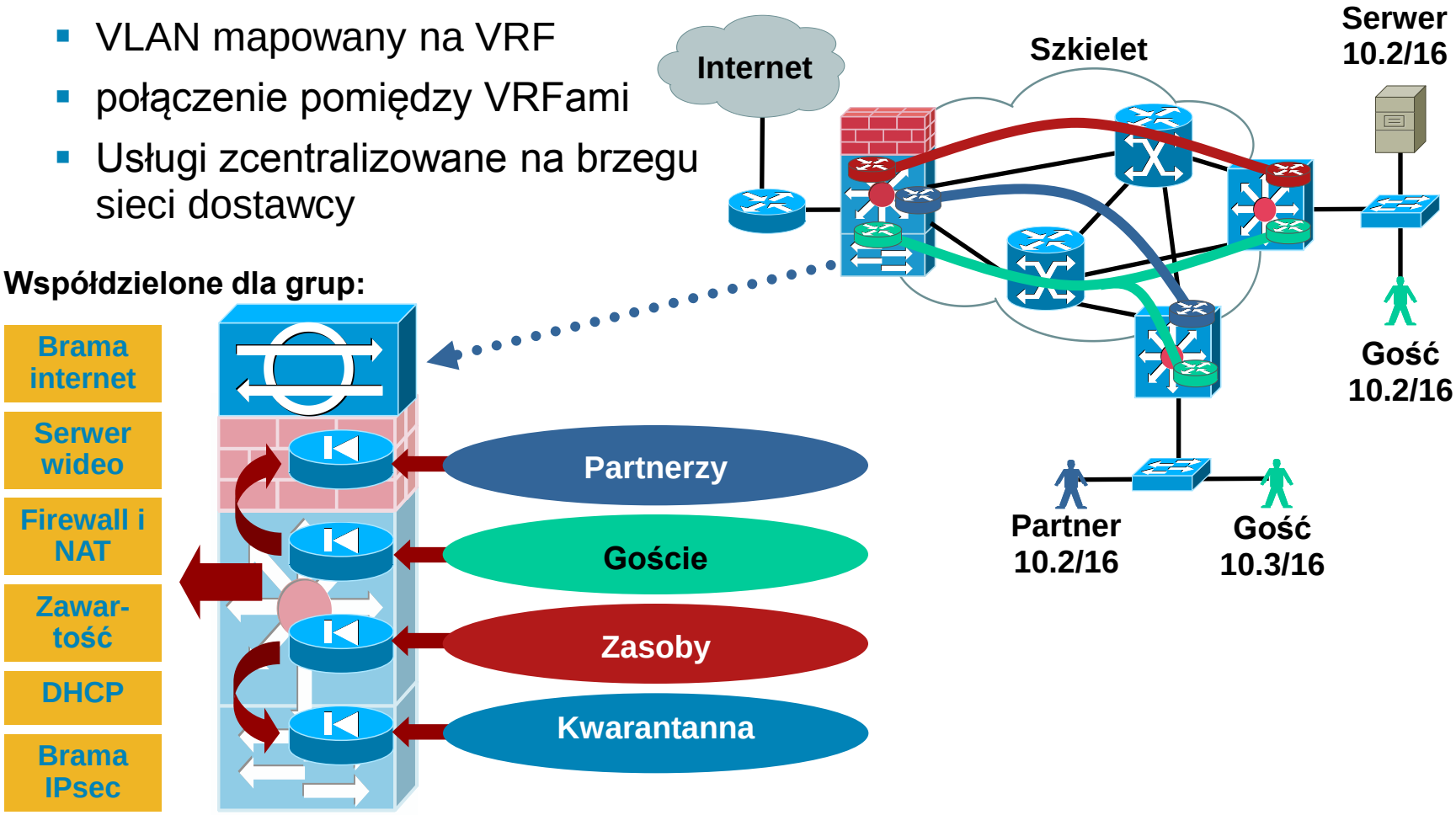
Świadoma budowa i zabezpieczenie sieci

- Należy zdefiniować przełącznik Root
  - –Root Podstawowy/Zapasowy
- Root zawsze tam, gdzie został zdefiniowany:
  - –Rootguard
  - –Loopguard
  - –UplinkFast
  - –UDLD
- Na przełączniku dostępowym tylko ruch od klientów:
  - –BPDU Guard
  - –Root Guard
  - –PortFast
  - –Port-Security
  - –DAI/IP Source Guard

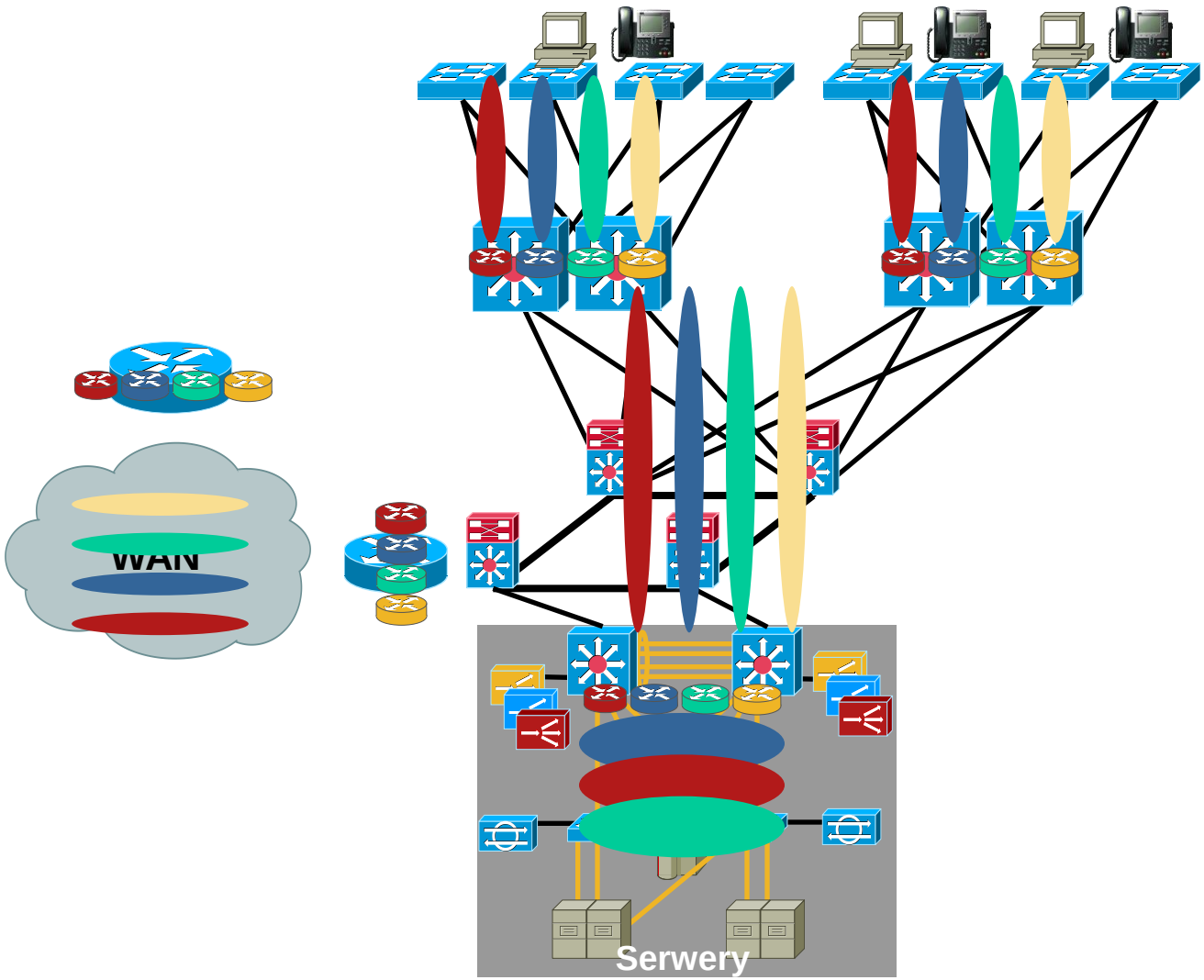


Dynamiczne pozycjonowanie użytkowników

- Użytkownik przydzielany do VLANu
- VLAN mapowany na VRF
- połączenie pomiędzy VRFami
- Usługi zcentralizowane na brzegu sieci dostawcy



Separacja ruchu



Identyfikajca
(per Port lub 802.1x)

Role per-użytkownik
VLANy (L2)

VRFy (L3)

802.1Q + VRFy
MPLS,
GRE (PBR/VRF),
L2TPv3

Zwirtualizowane
usługi

Farmy serwerów
podzielone
na VLANy

Podsumowanie

Podsumowanie

- Hierarchizacja nie rozwiązuje wszystkich problemów sieciowych, ale…
  - Pozwala dokładnie dopasować urządzenia do ich funkcji w sieci
  - Ułatwia planowanie rozwoju
  - Ułatwia utrzymanie sieci


CISCO