Sieci wirtualne

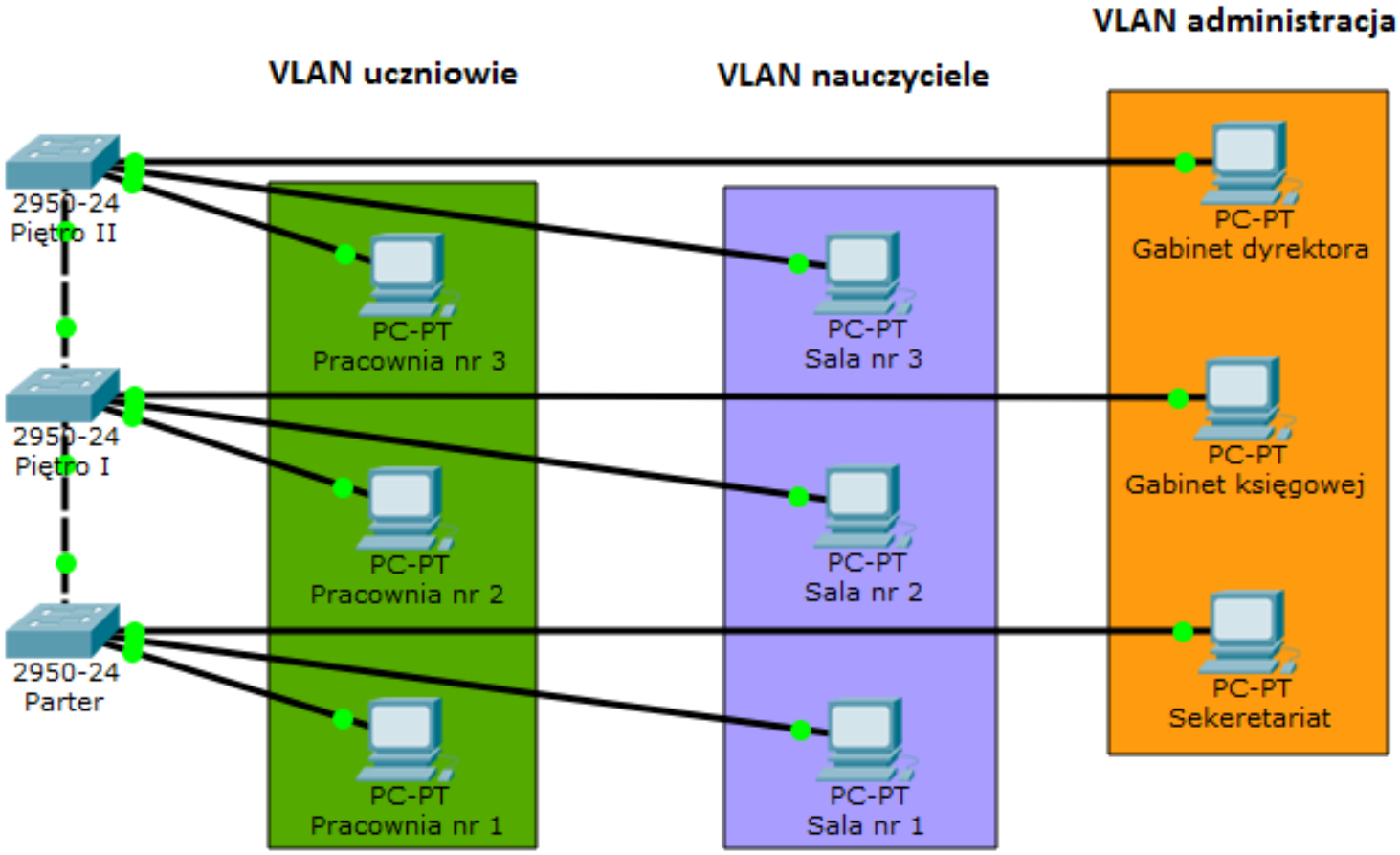
VLAN

Co to jest?

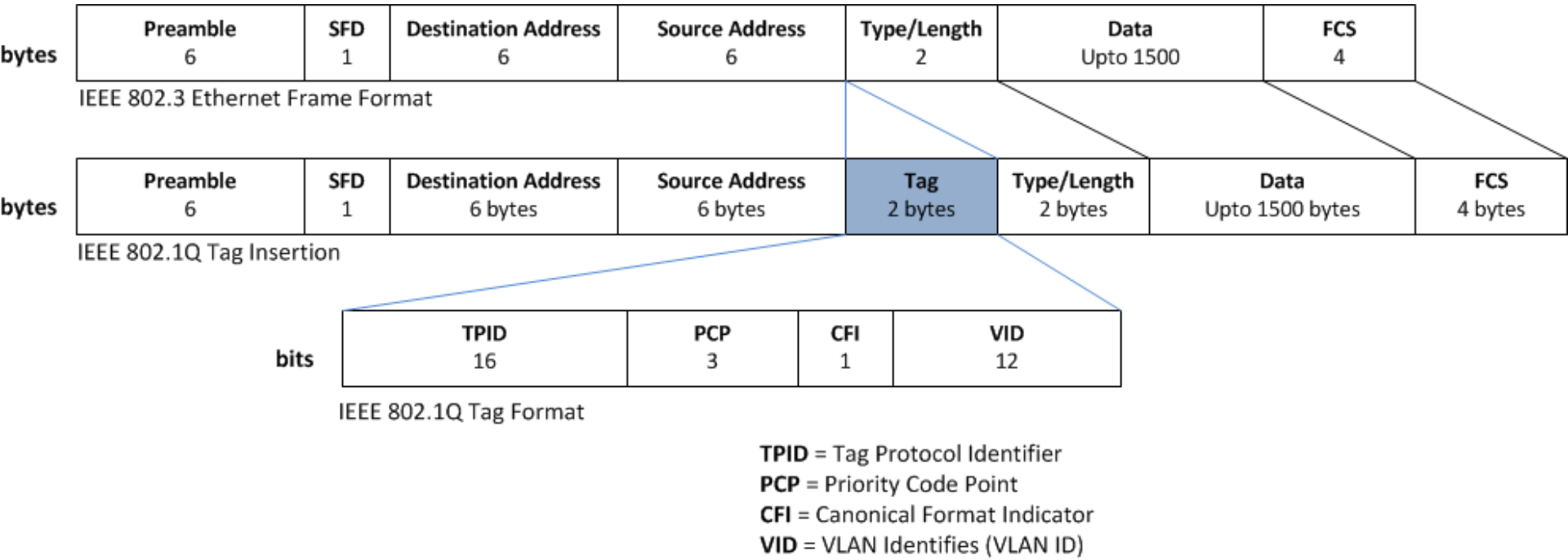
VLAN (czyli formalnie Virtual Local Area Network) to technologia pozwalająca na podzielenie portów w przełączniku w logiczne odizolowane grupy.

Dzięki temu możemy podzielić nasz przełącznik posiadający np. 48 portów na dwie grupy po np. 24 portów każda.

Zastosowanie VLAN



Standard **IEEE 802.1Q**



TPID = Tag Protocol Identifier
PCP = Priority Code Point
CFI = Canonical Format Indicator
VID = VLAN Identifies (VLAN ID)

Podział przełączników

- **Przełączniki niezarządzalne Passthrough VLAN** – Przepuszczają ramki 802.1Q – ale nie pozwalają na zdefiniowanie żadnego VLANu. Zasadniczo tak zachowuje się niemalże każdy prosty switch za kilkadziesiąt złotych.
- **Przełączniki niezarządzalne „z dipswitchem”** – W nich VLANy ustawiane są za pomocą przełącznika, ale nie wspierają w pełni „tagowanych” VLANów w standardzie 802.1Q. Ich funkcjonalność często ogranicza się tylko do izolacji portów między sobą.
- **Przełączniki zarządzalne z obsługą VLAN jako Port Based** – najczęściej są to kompaktowe przełączniki zarządzalne – popularne WebSmarty- które obsługują tworzenie grup VLANowych, ale często bez obsługi tagowania ramek zgodnie z 802.1Q.
- **Przełączniki zarządzalne z pełną obsługą 802.1Q** – czyli najbardziej uniwersalne przełączniki, które pozwalają na przenoszenie ramek ethernetowych wraz z tzw. tagami.

TAG – znakowane ramki

W sieciach **VLAN** możemy oznaczać poszczególne ramki Ethernetowe za pomocą znaczników. Odbywa się to zgodnie ze standardem **802.1Q** – który definiuje dwa dodatkowe pola w ramce Ethernet o łącznej długości 4 bajtów. Pola te nazywają się po kolei **TPID** (Tag Protocol Identifier) oraz **TCI** (Tag Control Information).

Pole TPID jest zasadniczo zawsze stałe i reprezentowane przez wartość szesnastkową 0x8100. Pole TCI zawiera przede wszystkim 12 bitowy identyfikator VLANu. Pozostałe bity zarezerwowane są na dodatkowe informacje o technologii oraz priorytecie – gdyż dane z poszczególnych VLANów mogą być również odpowiednio z określonym priorytetem przełączane przez switcha.

Z uwagi, że do dyspozycji posiadamy 12 bitów przeznaczonych na określenie identyfikatora VLANu – do dyspozycji mamy sumarycznie 4096 znaczniki, z czego wartość 0 i 4096 nie może być używana. Stąd do dyspozycji mamy 4094 różne VLANy.

Czym różni się Port Based od 802.1Q ?

W przypadku 802.1Q ramki są oznaczane TAGiem i mogą one z takim znacznikiem opuszczać przełącznik.

W przypadku trybu Port Based VLANy są tworzone tylko w konfiguracji przełącznika.

Tryby pracy portu

Przełączniki zwykle mają za zadanie odpowiednio kierować ramki Ethernetowe do odpowiednich portów – stąd znaczniki ramek są odpowiednio dodawane lub usuwane w zależności czy dana ramka przychodzi na dany port (**Ingress**) czy też opuszcza port (**Egress**).

W przypadku kiedy ramki przychodzą na port – switch może domyślnie „otagować” ramkę jeśli ta nie jest już wcześniej oznaczona (tryb ACCESS i GENERAL). Kiedy ramka ma zostać wysłana na konkretny port ramka może zostać pozbawiona znacznika (tryb ACCESS) lub może zostać oznaczona odpowiednim znacznikiem (tryb TRUNK lub GENERAL).

Tryby pracy portu

- **ACCESS** – W tym trybie przełącznik akceptuje zwykle wszystkie nietagowane ramki i nadaje im znacznik z góry zdefiniowany za pomocą pola PVID. Jeśli dane mają zostać wysłane na port w trybie ACCESS – znacznik zostaje usunięty. Warto tutaj zaznaczyć, że w przypadku trybu ACCESS przypisać możemy tylko jeden wybrany VLAN.
- **GENERAL** – Ten tryb pracy jest najbardziej uniwersalny, gdyż oferuje możliwość odbierania ramek nietagowanych i tagowanych. W przypadku ramek nietagowanych możemy oczywiście nadać im odpowiedni PVID. W przypadku ramek tagowanych możemy wskazać jakie ramki chcemy zaakceptować – w tym celu dopisujemy w konfiguracji przełącznika jakie VLANy mają być przypisane do danego portu.
- **TRUNK** – Ten tryb w zależności od producenta przełącznika zwykle definiowany jest jako port którym „przepychane” są wszystkie VLANy jakie znajdują się w obrębie przełącznika. W przypadku switchy Cisco Catalyst port ustawiony w trybie TRUNK akceptuje wszystkie ramki tagowane i również wysyła wszystkie VLANy. W przypadku nowszych switchy Cisco czy też nawet TP-Linków – w konfiguracji należy zdefiniować jakie VLANy akceptujemy. Więc funkcjonalność portu w trybie TRUNK nie różni się wiele w odróżnieniu od trybu GENERAL – jednak port w takim trybie nie będzie akceptował nietagowanych ramek.