Rozdział 6: Sieci VLAN

Routing & Switching

Cisco | Networking Academy®
Mind Wide Open™

Rozdział 6

6.1 Segmentacja sieci VLAN

6.2 Implementacja sieci VLAN

6.3 Bezpieczeństwo i projektowanie sieci VLAN

6.4 Podsumowanie

Rozdział 6: Cele

- Wyjaśnienie przeznaczenia sieci VLAN w przełączanej sieci.
- Analiza, w jaki sposób przełącznik przekazuje ramki w oparciu o konfigurację sieci VLAN na wielu przełącznikach.
- Konfigurowanie portu przełącznika w taki sposób, aby przypisać go do sieci VLAN zgodnie z wymaganiami.
- Konfigurowanie na przełączniku portu trunk.
- Konfigurowanie dynamicznych protokołów trunk (DTP).
- Rozwiązywanie problemów związanych z konfiguracją sieci VLAN oraz łączy trunk w przełączanej sieci.
- Konfigurowanie funkcji bezpieczeństwa w celu ograniczenia ataków w środowisku z sieciami VLAN.
- Wyjaśnienie praktyk związanych z bezpieczeństwem dla środowiska opartego na sieciach VLAN.

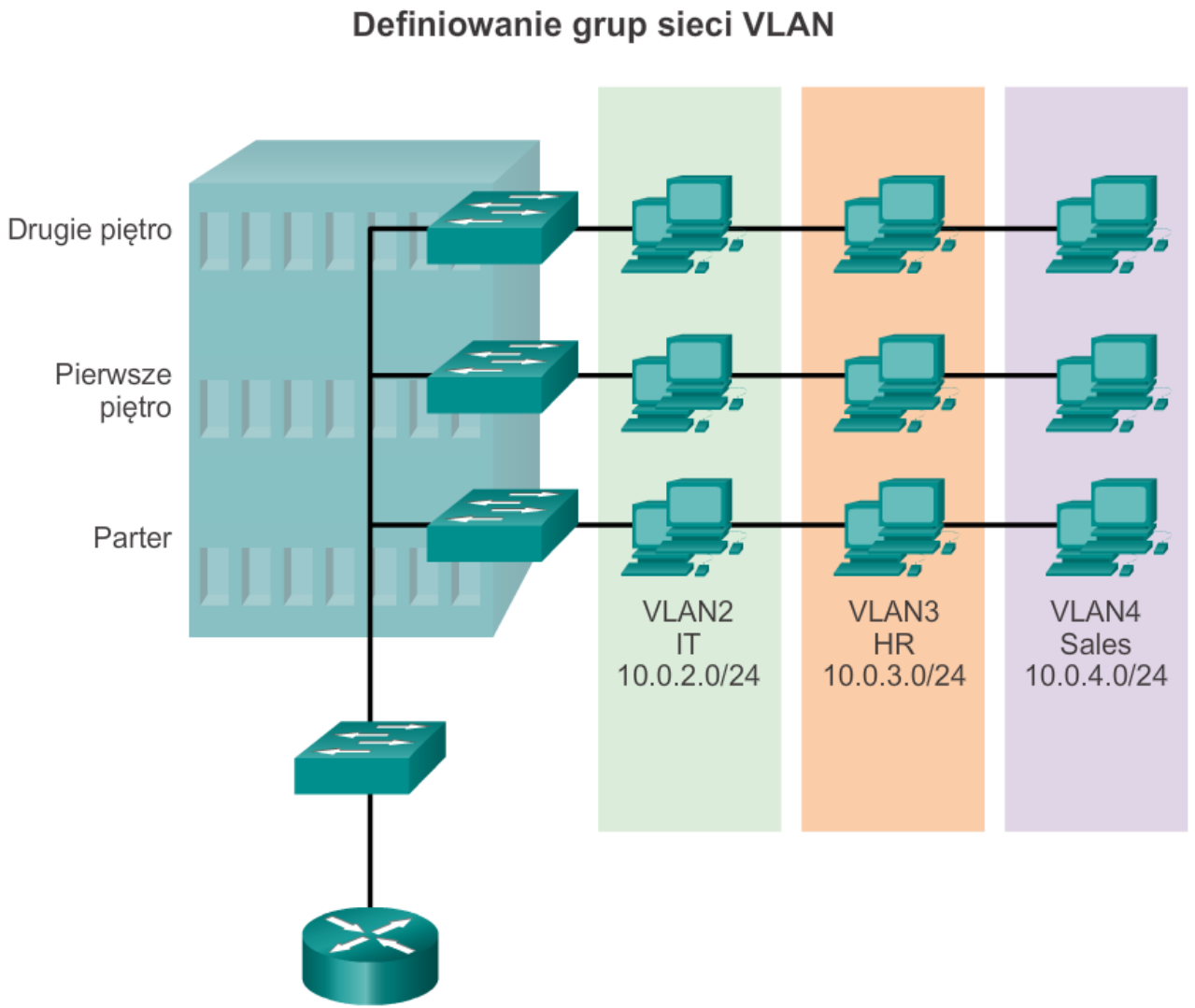
6.1 Segmentacja sieci VLAN

Cisco | Networking Academy®
Mind Wide Open™

Definicje

- Sieć VLAN jest partycją logiczną sieci w warstwie 2.
- Współistnienie wielu sieci VLAN jest możliwe przez tworzenie wielu partycji.
- Każda sieć VLAN jest domeną transmisyjną zazwyczaj z własną siecią IP.
- Sieci VLAN są wzajemnie izolowane, a pakiety mogą przechodzić tylko między nimi za pośrednictwem routera.
- Partycjonowanie warstwy 2 sieci odbywa się wewnątrz urządzenia warstwy 2 zwykle za pomocą przełącznika.
- Hosty zgrupowane w sieci VLAN nie są świadome istnienia sieci VLAN.

Definicje (cd.)



Korzyści ze stosowania sieci VLAN

- bezpieczeństwo,
- redukcja kosztów,
- lepsza wydajność,
- zmniejszenie rozmiaru domen rozgłoszeniowych,
- poprawa efektywności personelu IT,
- prostszy projekt i ułatwione wdrażanie aplikacji.

Rodzaje sieci VLAN

- Data VLAN.
- Domyślny VLAN.
- Natywny VLAN.
- Zarządzający VLAN.

Rodzaje sieci VLAN (cd.)

VLAN 1

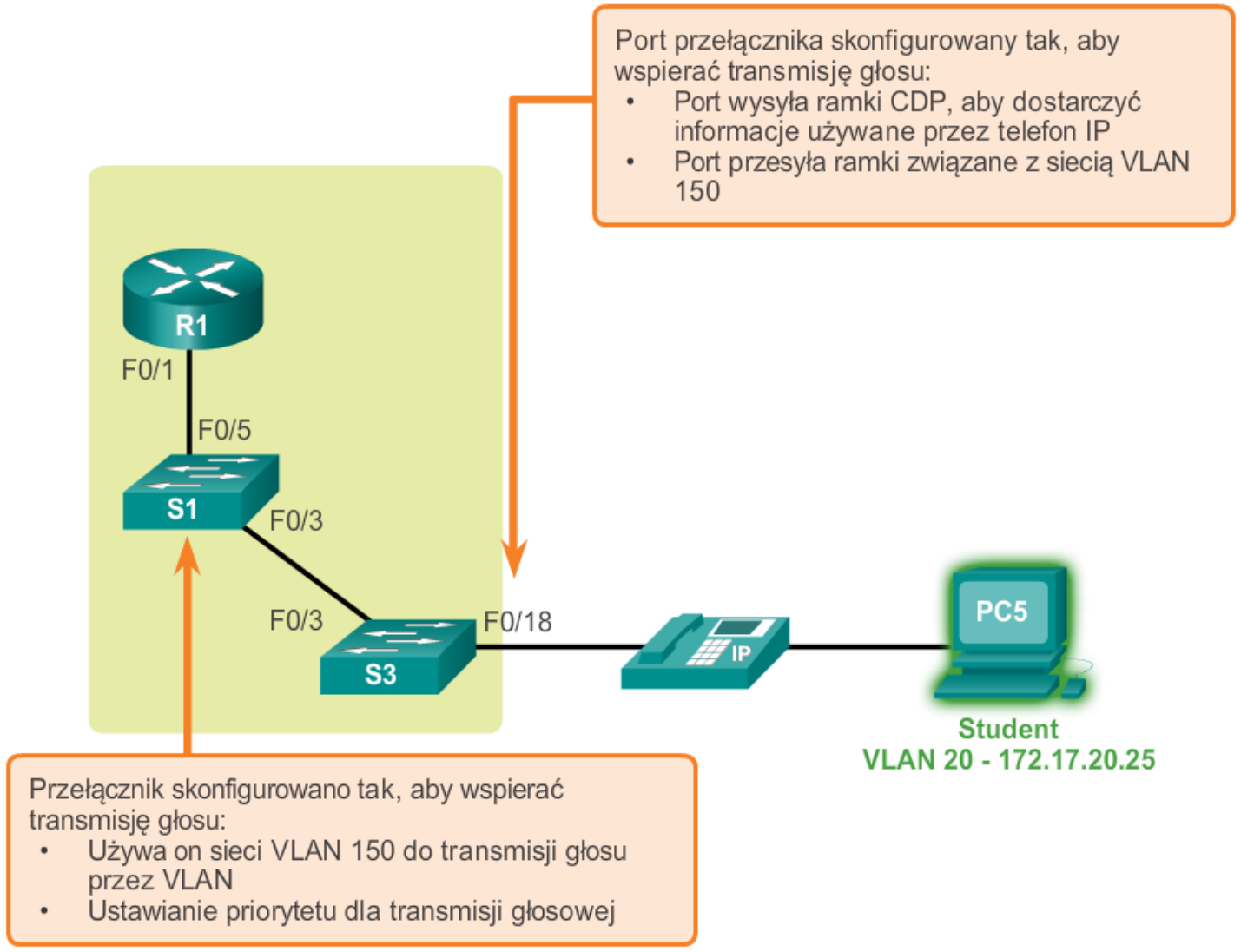
```
Switch# show vlan brief

VLAN Name                Status    Ports
---- ------------------- --------- -----------------------
1    default             active    Fa0/1,  Fa0/2,  Fa0/3,  Fa0/4
                                   Fa0/5,  Fa0/6,  Fa0/7,  Fa0/8
                                   Fa0/9,  Fa0/10, Fa0/11, Fa0/12
                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                   Gi0/1,  Gi0/2
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
```

- Wszystkie porty przypisane do sieci VLAN 1 przesyłają dane domyślnie.
- Native VLAN jest domyślną siecią VLAN 1.
- Management VLAN jest domyślną siecią VLAN 1.
- Nazwy sieci VLAN 1 nie można zmieniać albo usuwać.

Sieci voice VLAN

- Ruch VoIP jest czuły na opóźnienia czasowe i wymaga:
  - gwarantowanej szerokości pasma zapewniającej odpowiednią jakość dźwięku,
  - priorytetu transmisji w stosunku do innych rodzajów ruchu sieciowego,
  - możliwości przekierowania z pominięciem zatorów w sieci,
  - opóźnienia mniejszego niż 150 ms w całej sieci.
- Funkcja voice VLAN umożliwia portom wykonywanie połączeń głosowych IP z telefonu IP.
- Przełącznik można podłączyć do telefonu IP Cisco 7960 i może on przenosić ruch głosowy IP.
- Jakość dźwięku w połączeniu telefonicznym IP może ulec pogorszeniu, jeśli dane są nierównomiernie wysłane; przełącznik obsługuje Quality of Service (QoS).

Sieci voice VLAN (cd.)



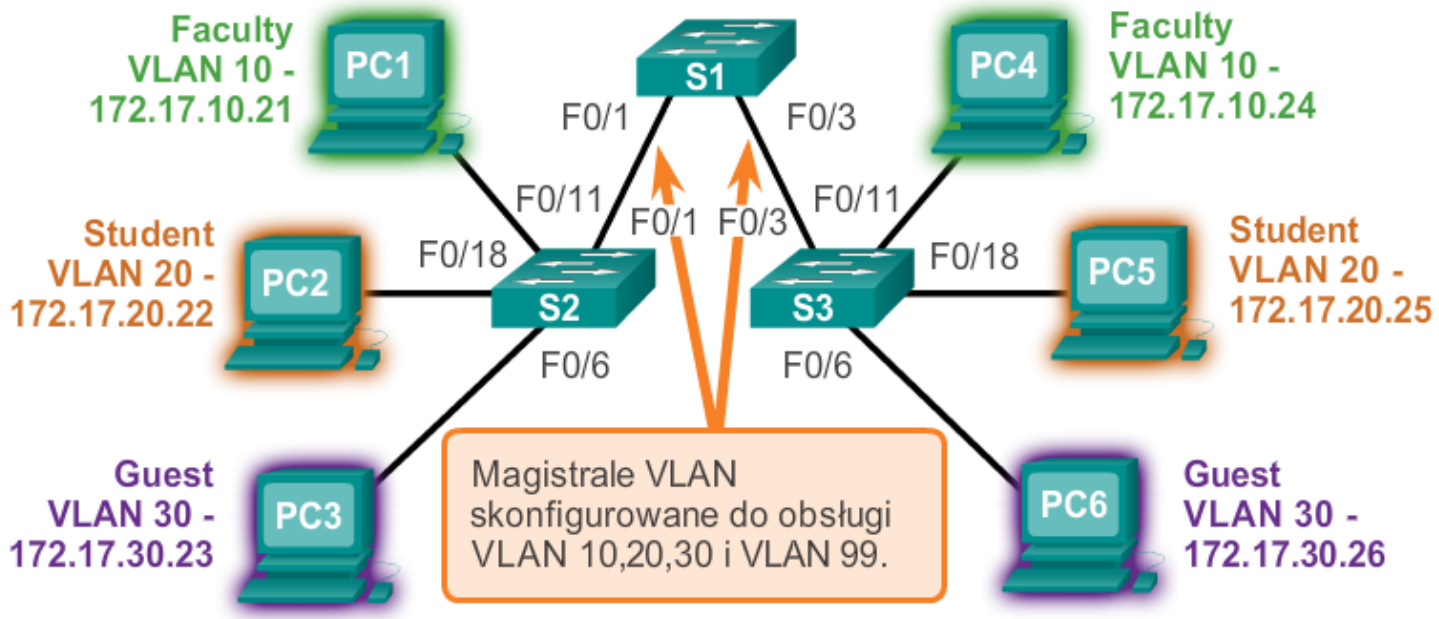
VLAN trunk

- Sieci VLAN trunk przenoszą więcej niż jedną sieć VLAN.
- VLAN trunk zostaje uruchomiona pomiędzy przełącznikami, co umożliwia komunikację urządzeniom z tą samą siecią VLAN, nawet jeśli są one fizycznie połączone z różnymi przełącznikami.
- VLAN trunk nie jest związana z żadną siecią VLAN; żaden z portów trunk nie jest wykorzystywany do ustalenia łącza trunk.
- Cisco IOS obsługuje IEEE802.1q, popularny protokół VLAN trunk.

Sieci VLAN trunk (cd.)

VLAN 10 Faculty/Staff - 172.17.10.0/24
VLAN 20 Students - 172.17.20.0/24
VLAN 30 Guest - 172.17.30.0/24
VLAN 99 Management i Native - 172.17.99.0/24

F0/1-5 są interfejsami magistral 802.1Q z pierwotną siecią VLAN 99.
F0/11-17 są w VLAN 10.
F0/18-24 są w VLAN 20.
F0/6-10 są w VLAN 30.



Domeny kontrolujące rozgłoszenie w sieciach VLAN

- Sieci VLAN mogą być stosowane w celu ograniczenia zasięgu rozgłoszenia ramek.
- Sieć VLAN sama w sobie jest domeną rozgłoszeniową.
- Ramka rozgłoszeniowa wysłana przez urządzenie w określonej sieci VLAN jest przesyłana dalej tylko w tej sieci VLAN.
- Sieci VLAN mogą pomóc kontrolować zasięg ramek rozgłoszeniowych oraz ich wpływ na sieć.
- Ramki unicast i multicast są przekazywane w ramach początkowej sieci VLAN.

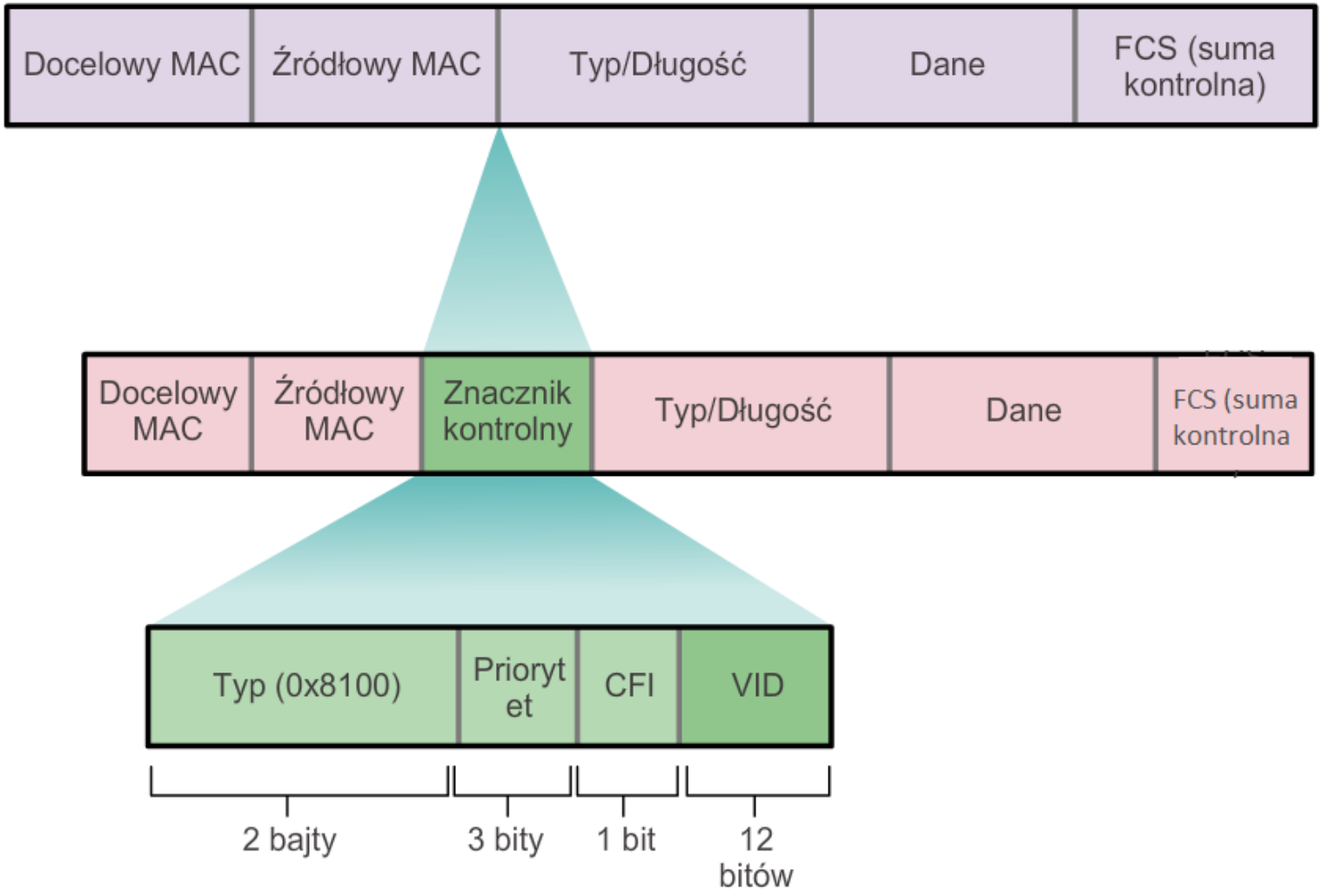
Sieci VLAN w środowisku wieloprzełącznikowym

Znakowanie ramek ethernet dla identyfikacji sieci VLAN

- Znakowanie ramek to proces, w którym do ramki dodawane są nagłówki identyfikacyjne sieci VLAN.
- Jest on używany do prawidłowego przekazywania wielu ramek VLAN za pośrednictwem łącza trunk.
- Przełączniki znakują ramki, by zidentyfikować sieć VLAN, do której należą. Istnieją różne protokoły znakowania; IEEE 802.1Q jest bardzo popularnym przykładem.
- Protokół przedstawia strukturę nagłówka znakowania dodanego do ramki.
- Przełączniki dodają znaczniki VLAN do ramek przed umieszczeniem ich w łączu trunk i usuwają znaczniki przed przekazaniem ramek przez porty non-trunk.
- Prawidłowo oznaczone ramki mogą przechodzić przez dowolną liczbę przełączników przez łącza trunk i być nadal przekazywane w ramach tego samego VLAN do miejsca przeznaczenia.

Sieci VLAN w środowisku wieloprzełącznikowym

Znakowanie ramek ethernet dla identyfikacji sieci VLAN



Natywne sieci VLAN i znakowanie 802.1Q

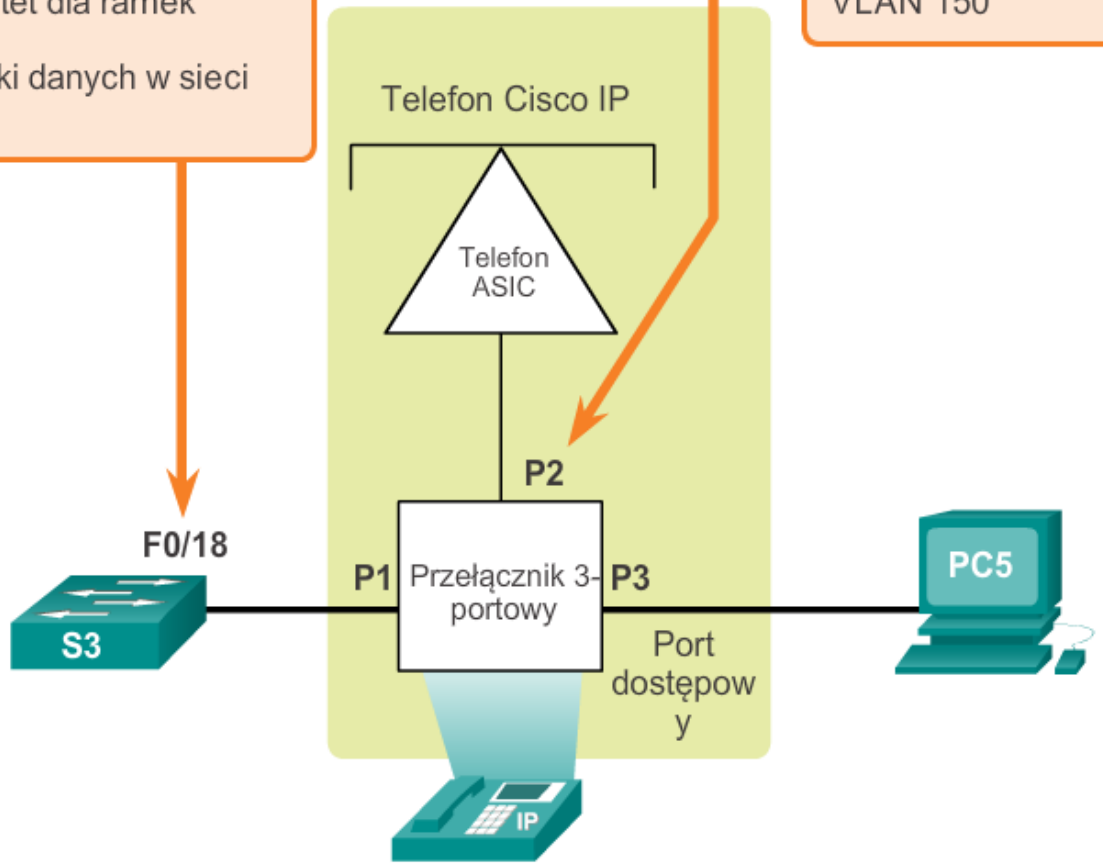
- Ramki, które należą do natywnej sieci VLAN, nie są oznaczone.
- Otrzymane nieoznaczone ramki pozostają nieoznaczone i są umieszczone w natywnej sieci VLAN podczas przekazywania.
- Jeśli nie istnieją porty związane z natywną siecią VLAN i łączem trunk, nieoznakowana ramka jest porzucana.
- W przełącznikach Cisco natywna sieć VLAN domyślnie oznakowana jest jako VLAN 1.

Sieci VLAN w środowisku wieloprzełącznikowym

Znakowanie voice VLAN

Port przełącznika jest skonfigurowany do obsługiwania transmisji głosu:
- nakazuje telefonowi oznaczyć ramkę głosową jako VLAN 150,
- ustawia priorytet dla ramek głosowych,
- przesyła ramki danych w sieci VLAN 20.

Port jest skonfigurowany do oznakowania ramek głosowych w sieci VLAN 150



6.2 Wykonanie sieci VLAN

Cisco | Networking Academy®
Mind Wide Open™

Zakresy VLAN na przełącznikach Catalyst

- Przełączniki Catalyst serii 2960 i 3560 obsługują ponad 4000 sieci VLAN.
- Sieci VLAN są podzielone na dwie kategorie:
  - normalny zakres sieci VLAN
    - sieci VLAN oznaczone numerami od 1 do 1,005,
    - konfiguracje zapisane w vlan.dat (w pamięci flash),
    - protokół VTP może tylko rozpoznać i przechowywać zakres normalnej sieci VLAN;
  - rozszerzony zakres sieci VLAN
    - sieci VLAN oznaczone numerami od 1,006 do 4,096,
    - konfiguracje zapisane w konfiguracji eksploatacyjnej (NVRAM),
    - protokół VTP nie rozpoznaje sieci VLAN z zakresu rozszerzonego.

Przyporządkowanie sieci VLAN

Tworzenie sieci VLAN

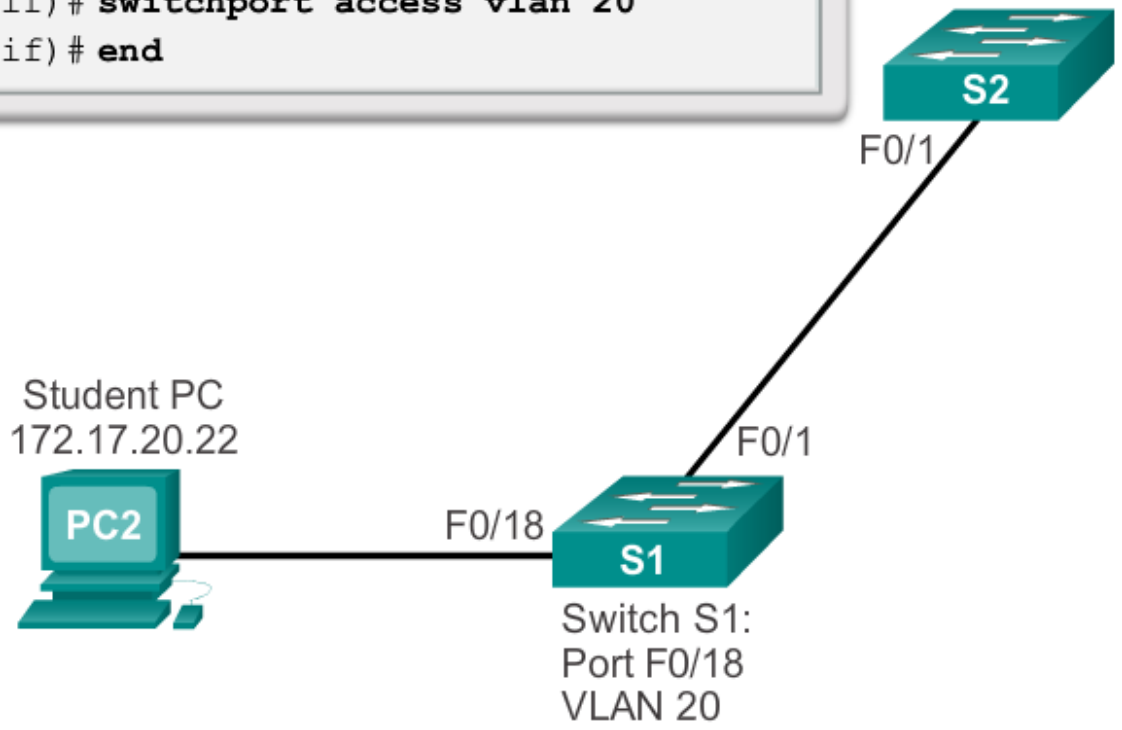
Polecenia IOS dla przełącznika Cisco	
Przejdź do trybu konfiguracji globalnej.	`S1# configure terminal`
Utwórz VLAN z poprawnym numerem vlan-id.	`S1(config)# vlan vlan-id`
Ustaw unikalną nazwę identyfikującą sieć VLAN.	`S1(config-vlan)# name vlan-name`
Wróć do trybu uprzywilejowanego EXEC.	`S1(config-vlan)# end`

Przyporządkowanie portów do sieci VLAN

Polecenia IOS dla przełącznika Cisco	
Przejdź do trybu konfiguracji globalnej.	`S1# configure terminal`
Przejdź do trybu konfiguracji interfejsu dla SVI.	`S1(config)# interface interface_id`
Ustaw port w trybie dostępu (access mode).	`S1(config-if)# switchport mode access`
Przypisz ten port do sieci VLAN.	`S1(config-if)# switchport access vlan vlan_id`
Powróć do trybu uprzywilejowanego EXEC.	`S1(config-if)# end`

Przyporządkowanie portów do sieci VLAN (cd.)

```
s1# configure terminal
s1(config)# interface F0/18
s1(config-if)# switchport mode access
s1(config-if)# switchport access vlan 20
s1(config-if)# end
```



Przyporządkowanie sieci VLAN

Zmiana przynależności portu do sieci VLAN

```
S1(config)# int fa0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
S1# show vlan brief

VLAN Name                Status    Ports
---- ----------------- ------- -------------------------------
1    default              active  Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                  Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                  Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                  Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                  Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                  Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                  Gi0/1, Gi0/2
20   student              active
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
S1#
```

Zmiana przynależności portu do sieci VLAN (cd.)

```
S1# config t
S1(config)# int F0/18
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
S1#
S1# show vlan brief

VLAN Name                 Status     Ports
---- -------------------- --------- -------------------------------
1    default              active     Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                     Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                     Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                     Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                     Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                     Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                     Gi0/2
20   student              active     F0/11
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
S1#
```

Przyporządkowanie sieci VLAN

Usuwanie sieci VLAN

```
S1# conf t
S1(config)# no vlan 20
S1(config)# end
S1#
S1# sh vlan brief

VLAN Name                 Status    Ports
---- ----------------     --------- -------------------------------
1    default              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                    Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                    Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                    Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                    Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                    Gi0/2
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
S1#
```

Weryfikacja informacji z sieci VLAN

```
S1# show vlan name student

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------
20   student                           active    Fa0/11, Fa0/18

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
20   enet  100020     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------

S1# show vlan summary
Number of existing VLANs              : 7
Number of existing VTP VLANs          : 7
Number of existing extended VLANS     : 0

S1#
```

Przyporządkowanie sieci VLAN

Weryfikacja informacji z sieci VLAN (cd.)

```
S1# show interfaces vlan 20
Vlan20 is up, line protocol is down
  Hardware is EtherSVI, address is 001c.57ec.0641 (bia
001c.57ec.0641)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Przyporządkowanie sieci VLAN

Konfigurowanie łączy trunk IEEE 802.1q

Polecenia IOS dla przełącznika Cisco

Przejdź do trybu konfiguracji globalnej.	`S1# configure terminal`
Przejdź do trybu konfiguracji interfejsu dla SVI.	`S1(config)# interface interface_id`
Ustaw łącze w trybie pracy magistrali.	`S1(config-if)# switchport mode trunk`
Określ pierwotną sieć VLAN dla nieoznakowanych połączeń przechodzących przez magistrale 802.1Q.	`S1(config-if)# switchport trunk native vlan vlan_id`
Określ listę sieci VLAN, które mogą przechodzić przez łącze magistrali.	`S1(config-if)# switchport trunk allowed vlan vlan-list`
Powróć do trybu uprzywilejowanego EXEC.	`S1(config-if)# end`

```
S1(config)# interface FastEthernet0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30
S1(config-if)# end
```

Przyporządkowanie sieci VLAN

Przywracanie łącza trunk do ustawień domyślnych

```
S1(config)# interface f0/1
S1(config-if)# no switchport trunk allowed vlan
S1(config-if)# no switchport trunk native vlan
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<output omitted>
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<output omitted>
```

Przywracanie łącza trunk do ustawień domyślnych (cd.)

Przywróć port do trybu dostępu (access mode).

```
S1(config)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
```

Weryfikowanie konfiguracji łącza trunk

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<output omitted>
```

Dynamiczny protokół trunk

Wprowadzenie do DTP

- Porty przełącznika można skonfigurować ręcznie, tworząc łącza trunk.
- Porty przełącznika można również skonfigurować tak, by negocjowały i nawiązywały połączenie trunk z połączonym równouprawnionym urządzeniem.
- Dynamiczny protokół trunk (DTP) zarządza negocjacją łącza trunk.
- DTP to własny protokół Cisco i jest włączony domyślnie w systemie Cisco Catalyst 2960 i 3560 przełączników.
- Jeśli port na przełączniku sąsiada jest skonfigurowany w trybie trunk, który obsługuje DTP, to on zarządza negocjacją.
- Domyślną konfiguracją dla przełączników Catalyst serii 2960 i 3560 jest tryb dynamic auto.

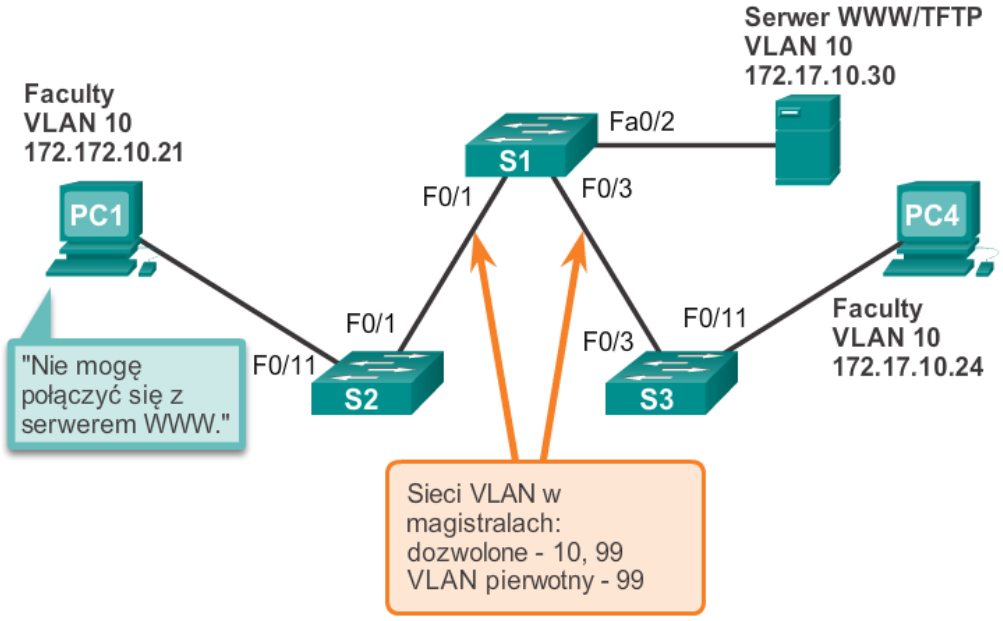
Negocjacyjne tryby interfejsu

- Przełączniki Catalyst serii 2960 i 3560 obsługują następujące tryby trunk:
  - switchport mode dynamic auto,
  - switchport mode dynamic desirable,
  - switchport mode trunk,
  - switchport nonegotiate.

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Ograniczona komunikacja
Access	Access	Access	Ograniczona komunikacja	Access

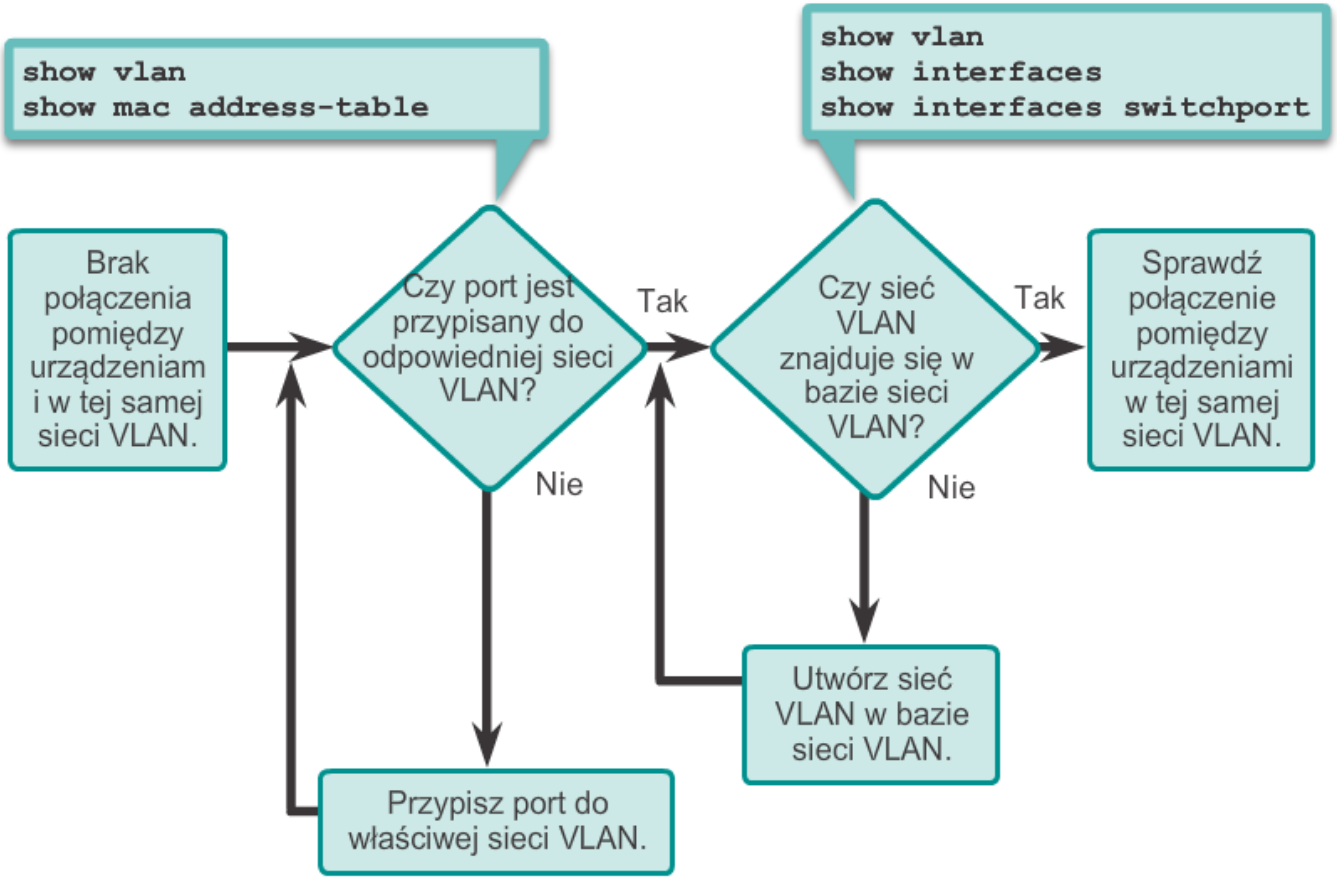
Problematyka adresowania IP w VLAN

- Powszechną praktyką jest kojarzenie sieci VLAN z siecią IP.
- Ponieważ różne sieci IP komunikują się tylko za pośrednictwem routera, wszystkie urządzenia w sieci VLAN muszą być częścią tej samej sieci IP, by mogły się komunikować.
- Rysunek pokazuje, że PC1 nie może komunikować się z serwerem, ponieważ ma skonfigurowany zły adres IP.

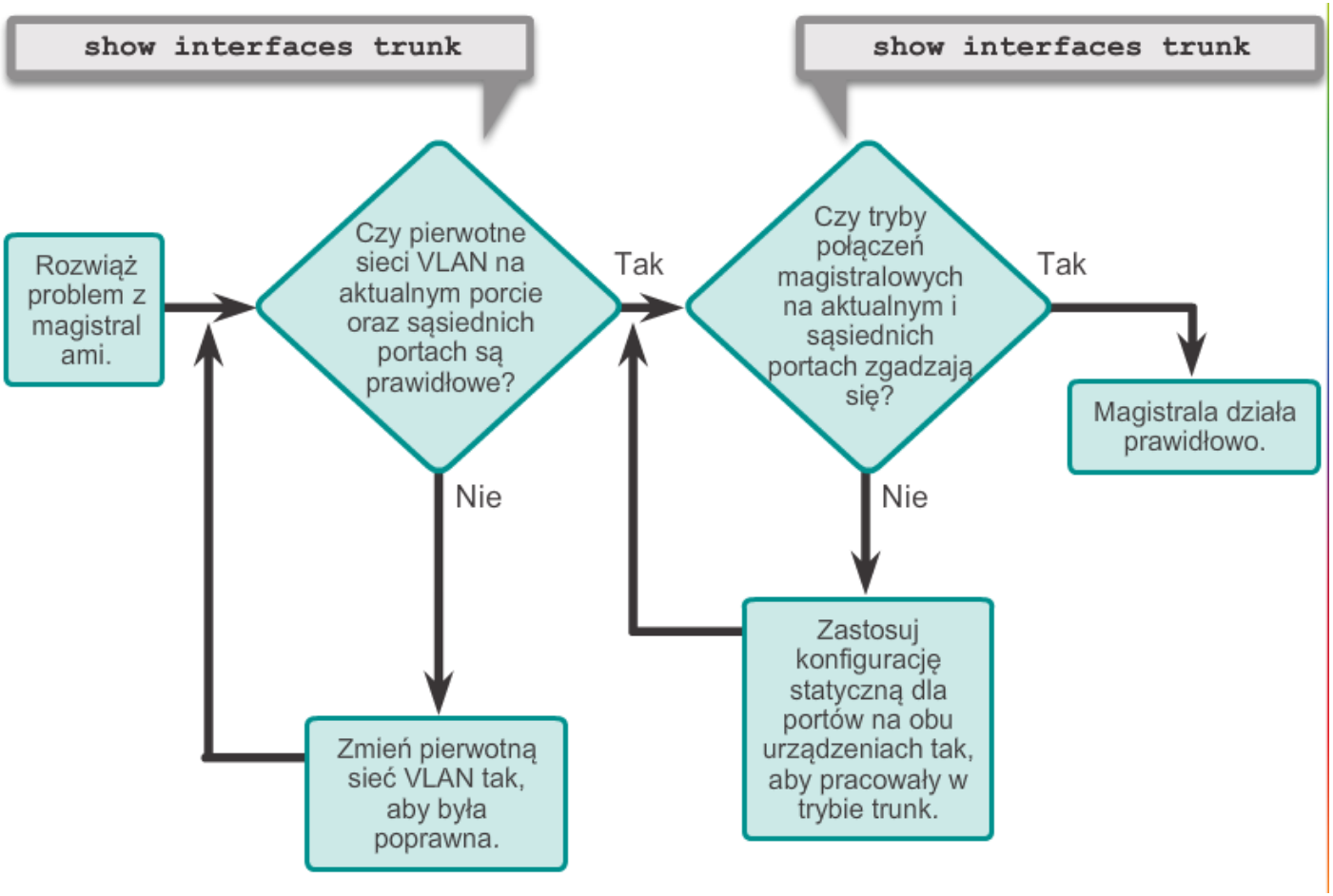


Brakujące sieci VLAN

- Jeśli wszystkie adresy IP zostały dopasowane, ale urządzenie nadal nie może się podłączyć do sieci, należy sprawdzić, czy na przełączniku istnieje sieć VLAN.



Wprowadzenie do rozwiązywania problemów z łączami trunk



Najczęściej występujące problemy z łączami trunk

- Problemy z połączeniami trunk zazwyczaj wynikają z niepoprawnej konfiguracji.
- Najczęściej występujące błędy w konfiguracji połączeń trunk to:
  1. niedopasowanie natywnej sieci VLAN,
  2. niedopasowanie trybu trunk,
  3. dozwolone sieci VLAN na połączeniach trunk.
- Jeśli zostanie wykryty problem z połączeniem trunk, wytyczne dotyczące najlepszych praktyk polecają rozwiązać problem w kolejności podanej wyżej.

Niedopasowanie trybu trunk

- Jeśli port połączenia trunk skonfigurowany jest do pracy w trybie trunk niezgodnym z portem po drugiej stronie połączenia, to między tymi dwoma przełącznikami połączenie nie zestawi się.
- Użyj polecenia **show interface trunk**, aby sprawdzić stan portów trunk na przełącznikach.
- Aby rozwiązać ten problem, należy skonfigurować interfejsy z odpowiednimi trybami trunk.

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Ograniczona komunikacja
Access	Access	Access	Ograniczona komunikacja	Access

Nieprawidłowa lista VLAN

- W połączeniach trunk sieci VLAN muszą być dozwolone, zanim ich ramki będą mogły być przekazywane łączem.
- Użyj polecenia **switchport trunk allowed vlan** w celu określenia, które sieci VLAN mają dostęp do połączenia trunk.
- Użyj polecenia **show interface trunk**, aby upewnić się, czy prawidłowe sieci VLAN są dopuszczone w połączeniu trunk.

6.3 Bezpieczeństwo i projektowanie sieci VLAN

Cisco | Networking Academy®
Mind Wide Open™

Atak typu fałszowanie przełącznika

- Istnieje wiele różnych rodzajów ataków na sieć VLAN w nowoczesnych przełączanych sieciach; VLAN Hopping jest jednym z przykładów.
- Domyślną konfiguracją portu przełącznika jest tryb dynamic auto.
- Poprzez konfigurację hostu, aby działał jako przełącznik i tworzył połączenie trunk, dokonujący ataku może uzyskać dostęp do dowolnej sieci VLAN w całej sieci.
- Ponieważ dokonujący ataku jest obecnie w stanie uzyskać dostęp do innych sieci VLAN, jest to tzw. atak VLAN hopping.
- Najlepszym sposobem na uniemożliwienie tego podstawowego rodzaju ataku podszywania się jest wyłączenie trybu trunk na wszystkich portach przełącznika z wyjątkiem tych, które rzeczywiście mają zestawić połączenia trunk.

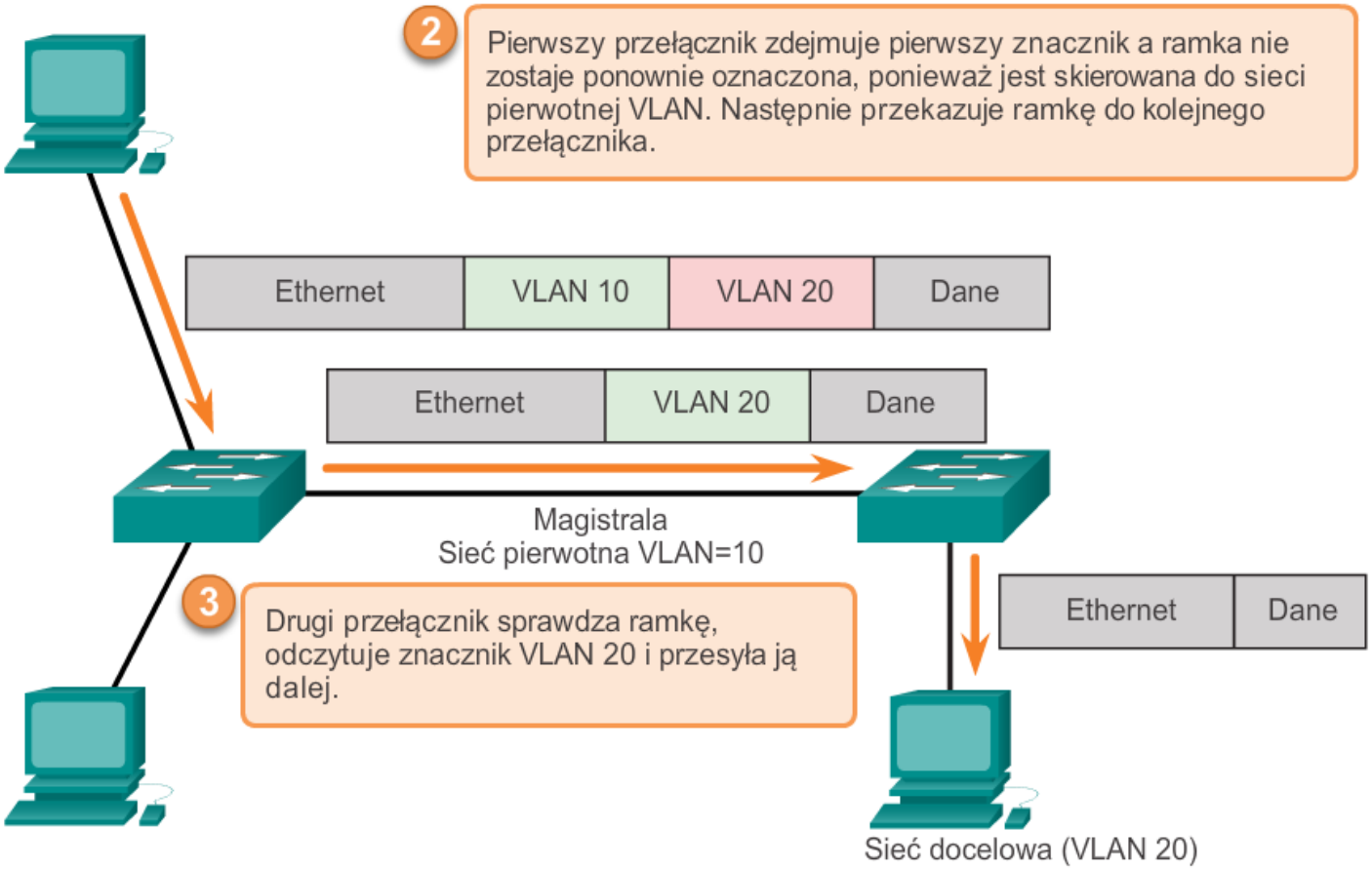
Atak podwójnego oznaczania

- Atak podwójnego oznaczania wykorzystuje sposób, w jaki sprzęt na większości przełączników dekapsuluje znaczniki 802.1Q.
- Większość przełączników wykonuje tylko jeden poziom 802.1Q dekapsulowania, co pozwala dokonującemu osadzić drugi, nieautoryzowany nagłówek w ramce.
- Po usunięciu pierwszego i legalnego nagłówka 802.1Q, przełącznik przekazuje ramkę do sieci VLAN, określonej w nieautoryzowanym nagłówku 802.1Q.
- Najlepszym sposobem na uniknięcie podwójnego znakowania jest upewnienie się, że VLAN natywny na portach trunk jest inny od sieci VLAN wszystkich użytkowników.

Ataki na sieci VLAN

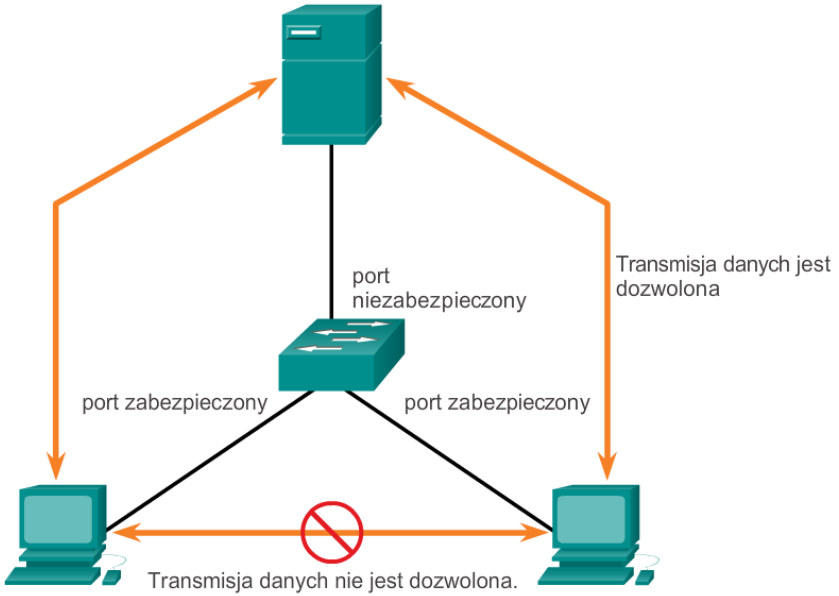
Atak podwójnego oznaczania (cd.)

1. Atakujący znajduje się w sieci VLAN 10. Wstawia on do ramki znacznik dla sieci VLAN 10 oraz wstawia dodatkowy znacznik dla sieci VLAN 20.



PVLAN Edge

- Opcja konfiguracyjna prywatnych sieci VLAN (PVLAN), znana również jako tryb chroniony, zapewnia, że nie ma wymiany żadnego rodzaju ruchu, komunikacji jednostkowej, rozgłoszeniowej czy grupowej między chronionymi portami na przełączniku.
- Wyłącznie znaczenie lokalne.
- Wymiana ruchu występuje tylko pomiędzy chronionym portem i portami niezabezpieczonymi.
- Wymiana ruchu nie występuje pomiędzy chronionym portem i innym chronionym portem.



Wytyczne projektowania sieci VLAN

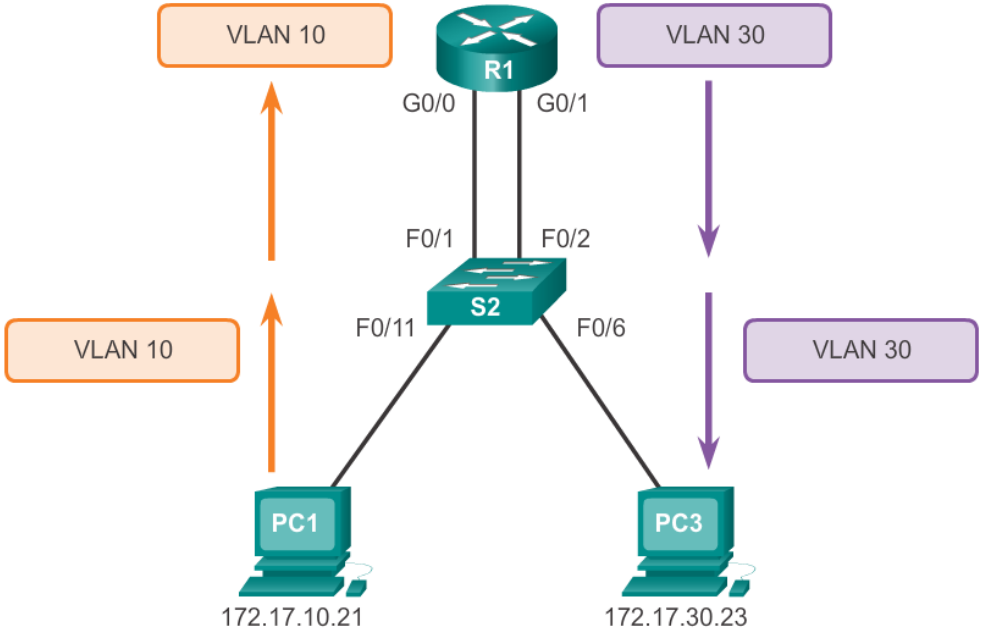
- Przenieś wszystkie porty z sieci VLAN 1 i przypisz je do sieci VLAN nieużytkowej.
- Zamknij wszystkie nieużywane porty przełączników.
- Rozdziel ruch zarządzający i ruch danych użytkownika.
- Zmień zarządzającą sieć VLAN na inną niż VLAN 1 (To samo dotyczy natywnej sieci VLAN).
- Upewnij się, że tylko urządzenia w zarządzającej sieci VLAN można podłączyć do przełączników.
- Przełącznik powinien akceptować tylko połączenia SSH.
- Wyłącz automatyczne uzgadnianie na portach trunk.
- Nie korzystaj z trybów automatycznego lub pożądanego portu przełącznika.

6.4 Konfigurowanie routingu między sieciami VLAN

Cisco | Networking Academy®
Mind Wide Open™

Co to jest routing między sieciami VLAN?

- Przełączniki warstwy 2 nie mogą przesyłać ruchu między sieciami VLAN bez pomocy routerów.
- Routing między sieciami VLAN realizowany na routerze jest procesem przekazywania ruchu sieciowego z jednej sieci VLAN do innej sieci VLAN.



Tradycyjny routing między sieciami VLAN

W przeszłości:

- do routowania między sieciami VLAN używane były rzeczywiste routery;
- każda sieć VLAN była podłączona do innego interfejsu routera;
- pakiety przychodziły do routera na jednym interfejsie, były routowane i wychodziły innym interfejsem;
- z powodu tego, że interfejsy routera były podłączone do różnych sieci VLAN i miały adresy należące do tych sieci, routing między nimi był możliwy;
- duże sieci z wielką ilością sieci VLAN wymagały olbrzymiej ilości interfejsów routerów.

„Router na patyku” w routingu między sieciami VLAN

- Rozwiązanie zwane „routerem na patyku” wykorzystuje różne trasy do routowania między sieciami VLAN.
- Jeden z fizycznych interfejsów routera jest skonfigurowany jako port trunk 802.1Q, więc może rozumieć znaczniki sieci VLAN.
- Tworzone są logiczne podinterfejsy, jeden na każdą sieć VLAN.
- Każdy podinterfejs skonfigurowany jest z adresem IP sieci VLAN, do której należy.
- Hosty znajdujące się w sieci VLAN mają jako bramę główną podany adres odpowiedniego podinterfejsu routera.
- Tylko jeden interfejs fizyczny routera jest używany.

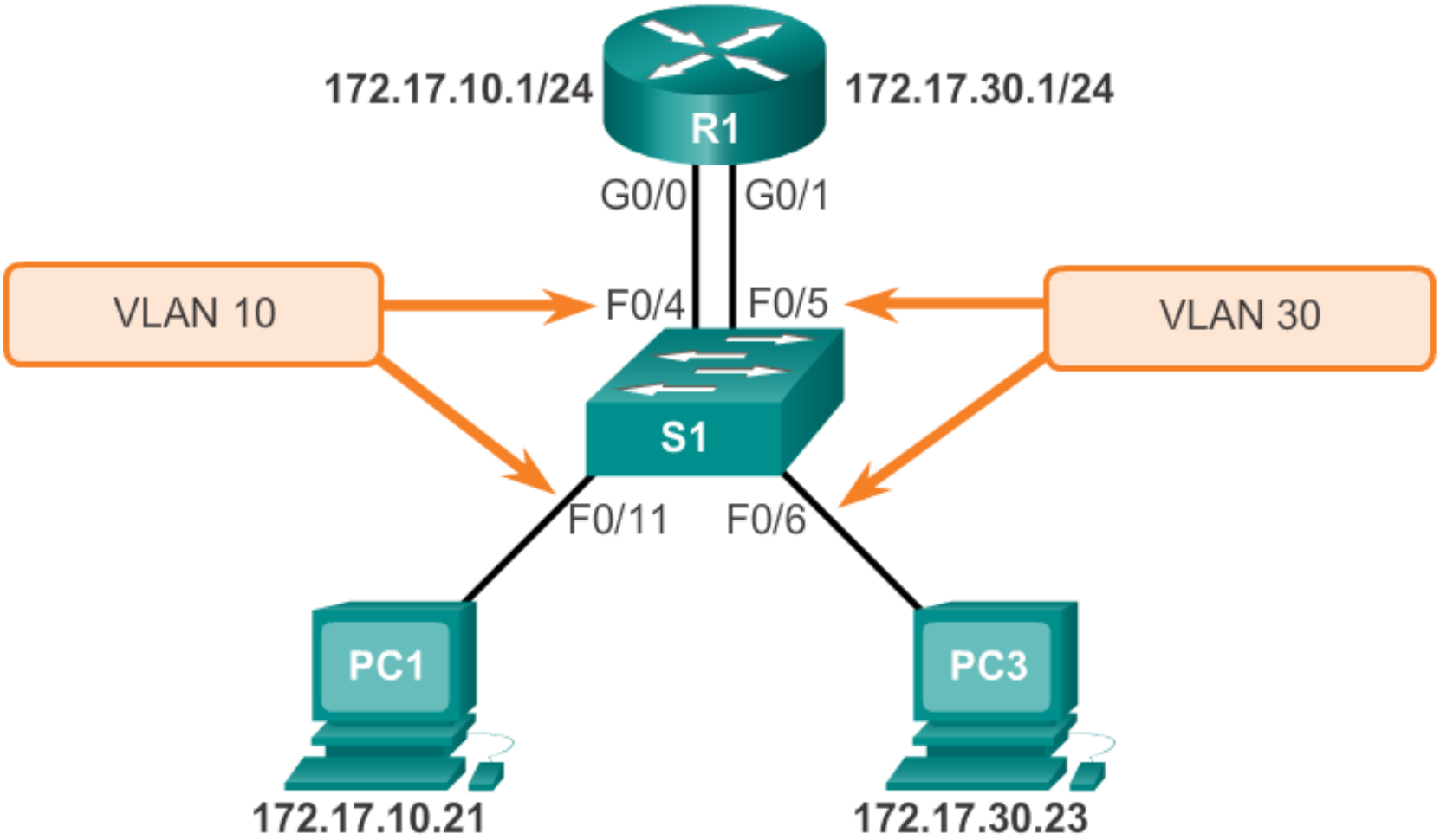
Działanie routingu między sieciami VLAN
Przełącznik wielowarstwowy jako router między sieciami VLAN

- Wielowarstwowe przełączniki mogą wykonywać zarówno operacje warstwy 2, jak i 3, zastępując konieczność wykorzystania dedykowanego routera.
- Przełączniki wielowarstwowe wspierają zarówno routing dynamiczny, jak i routing między sieciami VLAN.
- Przełącznik warstwy 3 musi mieć także włączony routing.
- Wirtualny interfejs przełącznika (SVI) domyślnie istnieje dla VLAN 1. Na wielowarstwowym przełączniku interfejs logiczny (warstwa 3) może być skonfigurowany adresem z dowolnej sieci VLAN.
- Przełącznik rozumie PDU warstwy sieci i może routować między swoimi interfejsami SVI dokładnie tak, jak router pomiędzy swoimi interfejsami.
- W przełączniku wielowarstwowym ruch jest routowany wewnętrznie na urządzeniu.
- Taki proces routingu jest odpowiedni i skalowany.

Przygotowanie

- Tradycyjny routing między sieciami VLAN wymaga, żeby router miał kilka fizycznych interfejsów.
- Każdy z interfejsów fizycznych routera podłączony jest do innej sieci VLAN.
- Każdy interfejs jest również skonfigurowany adresem IP podsieci konkretnej sieci VLAN.
- Urządzenia sieciowe używają routera jako bramy do urządzeń podłączonych do innych sieci VLAN.

Przygotowanie (cd.)



Konfiguracja tradycyjnego routingu między sieciami VLAN

Konfiguracja przełącznika

```
S1(config)# vlan 10
S1(config-vlan)# vlan 30
S1(config-vlan)# interface f0/11
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/4
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/6
S1(config-if)# switchport access vlan 30
S1(config-if)# interface f0/5
S1(config-if)# switchport access vlan 30
S1(config-if)# end
*Mar 20 01:22:56.751: %SYS-5-CONFIG_I: Configured from console by
console
S1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Konfiguracja tradycyjnego routingu między sieciami VLAN

Konfiguracja interfejsu routera

```
R1(config)# interface g0/0
R1(config-if)# ip address 172.17.10.1 255.255.255.0
R1(config-if)# no shutdown
*Mar 20 01:42:12.951: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
changed state to up
*Mar 20 01:42:13.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
R1(config-if)# interface g0/1
R1(config-if)# ip address 172.17.30.1 255.255.255.0
R1(config-if)# no shutdown
*Mar 20 01:42:54.951: %LINK-3-UPDOWN: Interface GigabitEthernet0/1,
changed state to up
*Mar 20 01:42:55.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
R1(config-if)# end
R1# copy running-config startup-config
```

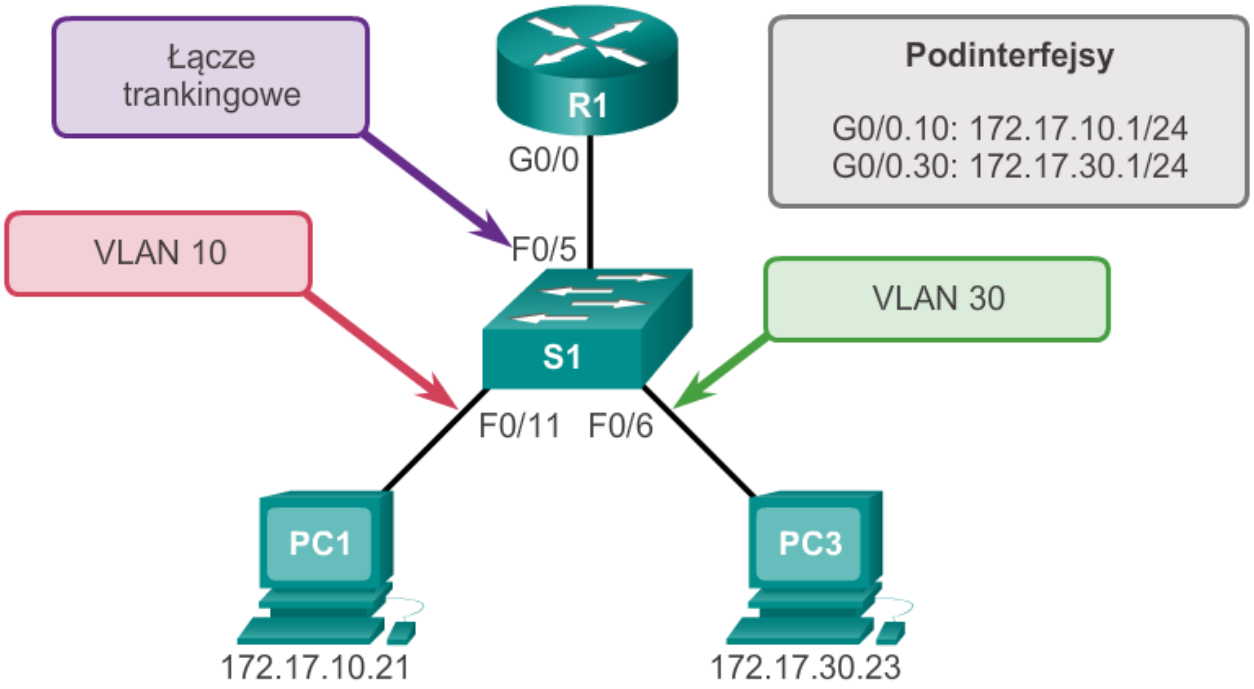
Konfiguracja „routera na patyku”

Przygotowanie

- Alternatywą dla tradycyjnego routingu między sieciami VLAN jest użycie połączenia trunk i podinterfejsów.
- Połączenie trunk umożliwia pojedynczemu fizycznemu interfejsowi routera routować ruch dla wielu sieci VLAN.
- Fizyczny interfejs routera musi być połączony do połączenia trunk przełącznika.
- Na routerze tworzone są podinterfejsy dla każdej sieci VLAN.
- Każdy podinterfejs ma skonfigurowany adres IP należący do jednej z sieci VLAN i również ma skonfigurowane znakowaniem ramek, identyfikatorem tej konkretnej sieci VLAN.

Konfiguracja „routera na patyku”

Konfiguracja przełącznika




```
S1(config)# vlan 10
S1(config-vlan)# vlan 30
S1(config-vlan)# interface f0/5
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1#
```

Konfiguracja „routera na patyku”

Konfiguracja podinterfejsu routera

```
R1(config)# interface g0/0.10
R1(config-subif)# encapsulation dot1q 10
R1(config-subif)# ip address 172.17.10.1 255.255.255.0
R1(config-subif)# interface g0/0.30
R1(config-subif)# encapsulation dot1q 30
R1(config-subif)# ip address 172.17.30.1 255.255.255.0
R1(config)# interface g0/0
R1(config-if)# no shutdown
*Mar 20 00:20:59.299: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
 changed state to down
*Mar 20 00:21:02.919: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
 changed state to up
*Mar 20 00:21:03.919: %LINEPROTO-5-UPDOWN: Line protocol on
 changed state to down
*Mar 20 00:21:02.919: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
 changed state to up
*Mar 20 00:21:03.919: %LINEPROTO-5-UPDOWN: Line protocol on
 Interface GigabitEthernet0/0, changed state to up
```

Konfiguracja „routera na patyku”

Sprawdzenie podinterfejsów

```
R1# show vlans
 <output omitted>
Virtual LAN ID:  10 (IEEE 802.1Q Encapsulation)

  vLAN Trunk Interface:    GigabitEthernet0/0.10

  Protocols Configured:  Address:      Received:   Transmitted:
          IP             172.17.10.1          11              18
<output omitted>
Virtual LAN ID:  30 (IEEE 802.1Q Encapsulation)

  vLAN Trunk Interface:    GigabitEthernet0/0.30

  Protocols Configured:  Address:      Received:   Transmitted:
          IP             172.17.30.1          11               8
<output omitted>
```

Konfiguracja „routera na patyku”

Sprawdzenie podinterfejsów (cd.)

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
       B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF,
       IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
            type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1,
       L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default,
       U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP,
       l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

   172.17.0.0/16 is variably subnetted, 4 subnets, 2 masks
C     172.17.10.0/24 is directly connected, GigabitEthernet0/0.10
L     172.17.10.1/32 is directly connected, GigabitEthernet0/0.10
C     172.17.30.0/24 is directly connected, GigabitEthernet0/0.30
L     172.17.30.1/32 is directly connected, GigabitEthernet0/0.30
```

Sprawdzenie routingu

Dostęp do zdalnych urządzeń, znajdujących się w innej sieci VLAN, może być testowany za pomocą komendy **`ping`** .

- Polecenie **`ping`** wysyła na adres docelowy żądanie ECHO request protokołu ICMP.
- Kiedy host otrzymuje żądanie ICMP echo request, odpowiada przez wysłanie ICMP echo reply.
- Narzędzie tracert służy do poznania trasy między dwoma urządzeniami.

Rozdział 3: Podsumowanie

Rozdział ten:

- dotyczyi sieci VLAN oraz z ich typów,
- opisał połączenia pomiędzy sieciami VLAN i domenami rozgłaszania,
- przybliżył zagadnienie znakowania ramek IEEE 802.1Q i sposób umożliwiający odróżnianie ramek ethernet związanych z różnymi sieciami VLAN, gdyż przemierzają one wspólne łącza trunk,
- przedstawił konfigurowanie, sprawdzanie sieci VLAN oraz rozwiązywanie problemów z sieciami VLAN i połączeniami trunk przy wykorzystaniu wiersza poleceń systemu Cisco IOS. Przybliżył również podstawowe techniki planowania i zabezpieczania.