Ćwiczenie – Wdrożenie zabezpieczenia VLAN

Topologia

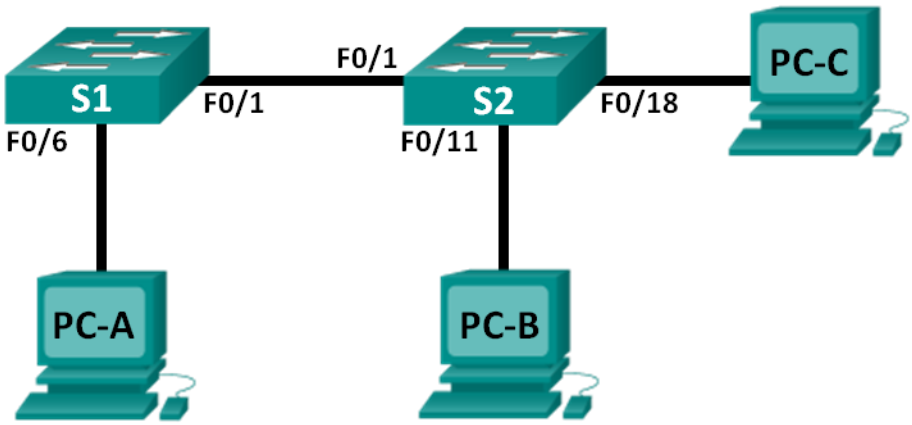

Tabela adresacji

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
S1	VLAN 99	172.17.99.11	255.255.255.0	172.17.99.1
S2	VLAN 99	172.17.99.12	255.255.255.0	172.17.99.1
PC-A	NIC	172.17.99.3	255.255.255.0	172.17.99.1
PC-B	NIC	172.17.10.3	255.255.255.0	172.17.10.1
PC-C	NIC	172.17.99.4	255.255.255.0	172.17.99.1

Przyporządkowanie sieci VLAN

VLAN	Nazwa
10	Data
99	Management&Native
999	BlackHole

Cele

Część 1: Budowa sieci i konfiguracja podstawowych ustawienie urządzeń.

Część 2: Wdrożenie zabezpieczenia VLAN na przełącznikach.

Scenariusz

Najlepsze praktyki w zarzadzaniu sieciami komputerowymi nakazują konfiguracje podstawowych ustawień zarówno dla interfejsów przełączających jak również trunkingowych. Pomaga to w zabezpieczeniu sieci zarówno przed atakami jak również transmitowanych danych przed podsłuchem. Podczas tego ćwiczenia należy skonfigurować urządzenia z podstawowymi ustawieniami, sprawdzić łączność oraz skonfigurować mocniejsze zabezpieczenia na

przełącznikach. Podczas ćwiczeń będzie można zaobserwować jak zachowują się komendy **show** w zależności od konfiguracji przełącznika.

Uwaga: Przełączniki użyte w instrukcji to Cisco Catalyst 2960s z obrazem system operacyjnego Cisco IOS wydanie 15.0(2) (lanbasek9). Do realizacji ćwiczenia mogą być użyte inne przełączniki lub wersje systemu IOS. W zależności od użytego modelu urządzenia oraz wersji IOS dostępne komendy oraz komunikaty na ekranie mogą się różnić od tych zamieszczonych w instrukcji.

Uwaga: Upewnij się, że przełączniki nie są skonfigurowane oraz nie przechowują pliku z konfiguracją startową. Jeśli nie jesteś tego pewien skontaktuj się z instruktorem.

Uwaga dla instruktorów: Procedury inicjalizacji i ponownego uruchomienia urządzeń znajdują się w instrukcji dla instruktorów.

Wymagane zasoby

- 2 przełączniki (Cisco 2960 z obrazem system Cisco IOS wydanie 15.0(2) lanbasek9 lub porównywalnym).
- 3 komputery PC (Windows 7, Vista, lub XP z za9instalowanym emulatorem terminala).
- Kabel konsolowy do konfiguracji urządzeń CISCO poprzez port konsolowy.
- Kable ethernetowe jak pokazano na rysunku topologii sieci.

Część 1: Budowa sieci i konfiguracja podstawowych ustawień urządzeń

W części 1, należy zestawić siec zgodnie z topologia I skonfigurować podstawowe ustawienia na komputerach PC oraz przełącznikach..

Krok 1: Połącz okablowanie zgodnie z topologią sieci.

Krok 2: Zainicjuj przełączniki i przeładuj je jeśli to konieczne.

Krok 3: Skonfiguruj adresy IP na PC-A, PC-B i PC-C.

Skorzystaj z do tabeli adresacji.

Krok 4: Skonfiguruj podstawowe ustawienia na każdym przełączniku.

a. Wyłącz automatyczne zapytania DNS (DNS lookup).
b. Skonfiguruj nazwę urządzenia jak to pokazano na schemacie.
c. Przypisz **class** jako hasło do trybu uprzywilejowanego EXEC.
d. Przypisz **cisco** jako hasło konsoli i vty i włącz logowanie do konsoli i vty.
e. Skonfiguruj **logging synchronous** dla wejścia konsolowego i vty

Krok 5: Utwórz sieci VLANs, na każdym przełączniku.

a. Utwórz i nazwij sieci VLAN zgodnie z tabelą przyporządkowania sieci VLAN.
b. Utwórz adres IP na podstawie Tabeli adresacji i przypisz go do VLAN 99 na obu przełącznikach.
c. Skonfiguruj interfejs F0/6 na przełączniku S1 jako port dostępowy i przypisz go z VLAN 99.
d. Skonfiguruj interfejs F0/11 na przełączniku S2 jako port dostępowy i przypisz go z VLAN 10.

e. Skonfiguruj interfejs F0/18 na przełączniku S2 jako port dostępowy i przypisz go z VLAN 99.

f. Wydaj komendę **show vlan brief** aby zweryfikować VLAN-y oraz przyporządkowanie portów.

```
S1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, 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
10   Data                             active
99   Management&Native                active    Fa0/6
999  BlackHole                        active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

S2# 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
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
10   Data                             active    Fa0/11
99   Management&Native                active    Fa0/18
999  BlackHole                        active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Do którego VLAN powinien należeć interfejs nieprzypisany, na przykład F0/8 na przełączniku S2?

_____

Wszystkie porty domyślnie są przypisane do VLAN1.

Krok 6: Skonfiguruj podstawowe zabezpieczenia na przełączniku.

a. Skonfiguruj baner MOTD aby ostrzegał użytkowników, że nieautoryzowany dostęp jest zabroniony b. Zaszyfruj wszystkie hasła.

b. Administracyjnie wyłącz wszystkie nieużywane interfejsy na przełączniku.

c. Wyłącz podstawowe serwisy WEB uruchomione domyślnie na przełącznikach.

```
S1(config)# no ip http server
```

```
S2(config)# no ip http server
```

d. Skopiuj konfiguracje bieżącą do konfiguracji startowej.

Krok 7: Sprawdź łączność pomiędzy urządzeniami i informacje na temat VLAN-ów.

a. Z linii komend komputera PC-A (wywołaj CMD z menu), pinguj adres IP sieci zarzadzania na przełączniku S1. Czy test łączności zakończył się sukcesem? Dlaczego?

_____

_____

Tak, wynik polecenia ping – udany. Komputer PC-A jest w tej samej sieci VLAN co adres zarządzający przełącznika.

b. Z przełącznika S1, pinguj adres zarzadzania na przełączniku S2. Czy test łączności zakończył się sukcesem? Dlaczego?

_____

_____

Nie wynik polecenia ping – negatywny. Adresy zarządzające przełączników S1 i S2 są w tej samej sieci VLAN ale interfejs Fa0/1 na obu przełącznikach nie jest ustawiony w tryb trunk. Port Fa0/1 nadal przynależy do sieci VLAN 1 a nie do VLAN 99

c. Z linii komend komputera PC-B, pinguj adres zarządzający na przełącznikach S1 i S2 i adres IP PC-A i PC-C. Czy test łączności zakończył się sukcesem? Dlaczego?

_____

_____

Wyniki polecenia ping do S1, S2, PC-A, i PC-C z PC-B były negatywne. PC-B jest w sieci VLAN 10 a S1, S2, PC-A, i PC-C są w sieci VLAN 99. Nie ma pomiędzy nimi żadnego urządzenia warstwy trzeciej, któreby rutowało między tymi sieciami.

d. Z linii komend komputera PC-C, pinguj adres zarządzający na przełącznikach S1 i S2. Czy test łączności zakończył się sukcesem? Dlaczego?

_____

_____

Sukces częściowy. PC-C jest w tym samej sieci VLAN co S1 I S2. PC-C pinguje adres zarządzający przełącznika S2 wciąż nie osiąga przełącznika S1 nie został jeszcze ustanowiony trunk pomiędzyS1 a S2.

Uwaga: Może być konieczne wyłączenie ściany ogniowej na komputerach PC.

Część 2: Implementacja zabezpieczeń sieci VLAN na przełącznikach

Krok 1. Skonfiguruj interfejsy trunkingowe na S1 i S2.

a. Skonfiguruj interfejs F0/1 na przełączniku S1 jako trunk.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
```

b. Skonfiguruj interfejs F0/1 na przełączniku S2 jako trunk.

```
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
```


c. Sprawdź trunki na S1 and S2. Wydaj komendę **show interface trunk** na obu przełącznikach.

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,99,999
```

Krok 2. Zmień natywny VLAN dla portów trunkingowych S1 i S2.

Zmiana natywnego VLAN-u dla portów trunkingowych z VLAN 1 do innego VLAN-u jest dobrą praktyką w zakresie bezpieczeństwa.

a. Jaki jest natywny VLAN dla przełącznika S1 i S2 na interfejsie F0/1?

_____

VLAN 1 ijest natywnym VLANem dla obu przełączników

b. Skonfiguruj natywny VLAN na S1 i interfejsie Trunk F0/1 na Management&Native VLAN 99.

```
S1# config t
S1(config)# interface f0/1
S1(config-if)# switchport trunk native vlan 99
```

c. Poczekaj kilka sekund. Na konsoli przelacznika S1 powinny pojawiać się komunikaty o błędzie. Co oznacza wiadomość %CDP-4-NATIVE_VLAN_MISMATCH:?

_____

To jest wiadomość CDP (Cisco Discovery Protocol) wskazująca, że natywne sieci VLAN przełączników S1 I S2 nie są takie same. S2 ma natywny VLAN 1 a S2 ma natywny VLAN 99

d. Skonfiguruj natywny VLAN na S2 i interfejsie trunkingowym F0/1 na Management&Native VLAN 99.

```
S2(config)# interface f0/1
S2(config-if)# switchport trunk native vlan 99
```

e. Sprawdź, że natywnym VLAN-em jest teraz VLAN 99 na obu przełącznikach. Odpowiedź przełącznika S1 podana jest poniżej

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-4094
```

```
Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999

Port          Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,999
```

Krok 3. Sprawdź czy ruch przez łącze trunk jest poprawny.

a. Z linii komend komputera PC-A (wywołaj CMD z menu), pinguj adres IP sieci zarzadzania na przełączniku S1. Czy test łączności zakończył się sukcesem? Dlaczego?

_____

_____

Tak . Pingi się powiodły . PC-A jest w tym samej sieci VLAN co adres zarządzający switcha.

b. Z przełącznika S1, pinguj adres zarzadzania na przełączniku S2. Czy test łączności zakończył się sukcesem? Dlaczego?

_____

_____

.Tak . Pingi się powiodły. Połączenie typu trunk zostało stworzone a oba switche są w sieci VLAN 99.

c. Z linii komend komputera PC-B, pinguj adres zarządzający na przełącznikach S1 i S2 i adres IP PC-A i PC-C. Czy test łączności zakończył się sukcesem? Dlaczego?

_____

_____

Pingi do S1, S2, PC-A I PC-C z PC-B się nie powiodły. PC-B jest w sieci VLAN 10 a S1, S2, PC-A I PC-C są w sieci VLAN 99. Nie ma pomiędzy nimi żadnego urządzenia warstwy trzeciej, które by rutowało między tymi sieciami.

d. Z linii komend komputera PC-C, pinguj adres zarządzający na przełącznikach S1 i S2. Czy test łączności zakończył się sukcesem? Dlaczego?

_____

_____

Tak . Pingi się powiodły. PC-C jest w tej samej sieci VLAN co S1 I S2 I PC-A.

Uwaga: Może być konieczne wyłączenie ściany ogniowej na komputerach PC.

Krok 4. Wyklucz użycie DTP na przełącznikach S1 i S2

Cisco wykorzystuje własny protokół znany jako dynamiczny protokół Trunkingowy (DTP) na swoich przełącznikach. Niektóre porty automatycznie negocjują między sobą tryb trunkingu. Dobrą praktyką jest wyłączenie auto negocjacji. Domyślne zachowanie się interfejsu można sprawdzić wydając następującą komendę:

```
S1# show interface 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
```

```
<Output Omitted>
```

a. Wyłącz negocjacje na S1.

```
S1(config)# interface f0/1
S1(config-if)# switchport nonegotiate
```

b. Wyłącz negocjacje na S2.

```
S2(config)# interface f0/1
S2(config-if)# switchport nonegotiate
```

c. Sprawdź czy auto negocjacja jest wyłączona wydając komendę **show interface f0/1 switchport** na S1 and S2.

```
S1# show interface 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: Off
<Output Omitted>
```

Krok 5. Włącz ochronę portów dostępowych na S1 i S2.

Nawet jeśli wyłączyć nieużywane porty na przełącznikach, jeśli urządzenie jest podłączone do jednego z tych portów, a interfejs jest włączony, może wystąpić połączenie trunkingowe. Ponadto domyślnie wszystkie porty są w sieci VLAN 1. Dobrą praktyką jest umieszczenie wszystkich nieużywanych portów w VLAN "czarna dziura". W tym kroku należy wyłączyć trunking na wszystkich nieużywanych portach. Można również przypisać nieużywane porty do sieci VLAN 999. W tym ćwiczeniu, tylko interfejsy od 2 do 5 zostaną skonfigurowane na obu przełącznikach.

a. Wydaj polecenie **show interface f0/2 switchport** na S1. Zwróć uwagę na tryb administracyjny i stan negocjacji protokołu trunkingowego

```
S1# show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
<Output Omitted>
```

b. Wyłącz trunking na interfejsach dostępowych S1.

```
S1(config)# interface range f0/2 – 5
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 999
```

c. Wyłącz trunking na interfejsach dostępowych S2.

```
S2(config)# interface range f0/2 – 5
S2(config-if-range)# switchport mode access
```

```
S2(config-if-range)# switchport access vlan 999
```

d. Sprawdź, że F0/2 jest ustawiony w tryb dostępowy S1.

```
S1# show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 999 (BlackHole)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
<Output Omitted>
```

e. Sprawdź, że jest prawidłowe przyporządkowanie portów na obu przełącznikach do VLAN-ów. Wynik z przełącznika S1 jest pokazany poniżej.

```
S1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
-- 1    default                          active    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
10   Data                             active
99   Management&Native                active    Fa0/6
999  BlackHole                        active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
1002 fddi-default                       act/unsup
1003 token-ring-default                 act/unsup
1004 fddinet-default                    act/unsup
1005 trnet-default                      act/unsup Restrict VLANs allowed on
     trunk ports.
```

Domyślnie wszystkie sieci VLAN mogą być przenoszone przez łącze trunkingowe. Ze względów bezpieczeństwa, jest dobrą praktyką, aby umożliwić komunikację przez trunki tylko pożądanych sieci VLAN a nie wszystkich.

f. Ogranicz połączenie trunkingowe na interfejsie F0/1 na S1 tylko do przenoszenia sieci VLAN 10 i 99.

```
S1(config)# interface f0/1
S1(config-if)# switchport trunk allowed vlan 10,99
```

g. Ogranicz połączenie trunkingowe na interfejsie F0/1 na S1 tylko do przenoszenia sieci VLAN 10 i 99

```
S2(config)# interface f0/1
S2(config-if)# switchport trunk allowed vlan 10,99
```

h. Sprawdź dopuszczone do komunikacji VLAN-y. Wydaj komendę **show interface trunk** w trybie uprzywilejowanym EXEC na obu przełącznikach S1 i S2.

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       10,99

Port        Vlans allowed and active in management domain
Fa0/1       10,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,99
```

Jaki jest rezultat?

Tylko sieci VLAN 10 I 99 są dozwolone do przejscia przez trunk pomiędzy S1 I S2

Do przemyślenia

1. Jakie, jeśli w ogóle, występują problemy z bezpieczeństwem na przełącznikach CISCO dla ustawień domyślnych?

Fakt, że domyślnie wszystkie porty przełącznika są przypisane do sieci VLAN1 to podstawowy problem bezpieczeństwa. Następny to taki, że na większości przełączników Cisco tryb pracy trunk jest ustawiony w pozycji autonegocjacji, więc połączenia typu trunk moga być przestawione przez naszej wiedzy, gdy tylko niepowołany switch zostanie wpięty do naszej sieci, Inna możliwa odpowiedź to, taka że hasła konsoli I vty są przesyłane domyślnie jawnym tekstem I serwer HTTP jest domyślnie włączony.

Switch S1

```
S1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------
1    default                           active    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
10   Data                              active
99   Management&Native                 active    Fa0/6
```

```
999  BlackHole                      active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

S1#sh run
Building configuration...

Current configuration : 3821 bytes
!
ersion 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10,99
 switchport mode trunk
 switchport nonegotiate
!
```

```
interface FastEthernet0/2
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/3
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/4
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/5
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/6
 switchport access vlan 99
 switchport mode access
!
interface FastEthernet0/7
 shutdown
!
interface FastEthernet0/8
 shutdown
!
interface FastEthernet0/9
 shutdown
!
interface FastEthernet0/10
 shutdown
!
interface FastEthernet0/11
 shutdown
!
interface FastEthernet0/12
```

```
 shutdown
!
interface FastEthernet0/13
 shutdown
!
interface FastEthernet0/14
 shutdown
!
interface FastEthernet0/15
 shutdown
!
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
 shutdown
!
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
 shutdown
!
interface FastEthernet0/20
 shutdown
!
interface FastEthernet0/21
 shutdown
!
interface FastEthernet0/22
 shutdown
!
interface FastEthernet0/23
 shutdown
!
interface FastEthernet0/24
 shutdown
!
interface GigabitEthernet0/1
 shutdown
```

```
!
interface GigabitEthernet0/2
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan99
 ip address 172.17.99.11 255.255.255.0
!
no ip http server
ip http secure-server
!
banner motd ^CWarning. Unauthorized access is prohibited.^C
!
line con 0
 password 7 070C285F4D06
 logging synchronous
 login
line vty 0 4
 password 7 070C285F4D06
 logging synchronous
 login
line vty 5 15
 password 7 070C285F4D06
 logging synchronous
 login
!
end
```

Switch S2

```
S2#show vlan brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------
------
1    default                             active    Fa0/6, Fa0/7, Fa0/8,
Fa0/9
                                                    Fa0/10, Fa0/12, Fa0/13, Fa0/14
                                                   Fa0/15, Fa0/16, Fa0/17, Fa0/19
```

```
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gi0/1, Gi0/2
10   Data                                       active    Fa0/11
99   Management&Native                          active    Fa0/18
999  BlackHole                                  active    Fa0/2, Fa0/3, Fa0/4,
Fa0/5
1002 fddi-default                               act/unsup
1003 token-ring-default                         act/unsup
1004 fddinet-default                            act/unsup
1005 trnet-default                              act/unsup

S2#sh run
Building configuration...

Current configuration : 3852 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S2
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
```

```
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10,99
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0/2
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/3
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/4
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/5
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/6
 shutdown

interface FastEthernet0/6
 shutdown
!
interface FastEthernet0/7
 shutdown
!
interface FastEthernet0/8
 shutdown
!
interface FastEthernet0/9
 shutdown
!
```

```
interface FastEthernet0/10
 shutdown
!
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/12
 shutdown
!
interface FastEthernet0/13
 shutdown
!
interface FastEthernet0/14
 shutdown
!
interface FastEthernet0/15
 shutdown
!
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
 shutdown
!
interface FastEthernet0/18
 switchport access vlan 99
 switchport mode access
!
interface FastEthernet0/19
 shutdown
!
interface FastEthernet0/20
 shutdown
!
interface FastEthernet0/21
 shutdown
!
interface FastEthernet0/22
 shutdown
```

```
!
interface FastEthernet0/23
 shutdown
!
interface FastEthernet0/24
 shutdown
!
interface GigabitEthernet0/1
 shutdown
!
interface GigabitEthernet0/2
 shutdown
!
interface Vlan1
 no ip address
!
interface Vlan99
 ip address 172.17.99.12 255.255.255.0
!
no ip http server
ip http secure-server
!
banner motd ^CWarning. Unauthorized access is prohibited.^C
!
line con 0
 password 7 00071A150754
 logging synchronous
 login
line vty 0 4
 password 7 00071A150754
 logging synchronous
 login
line vty 5 15
 password 7 070C285F4D06
 logging synchronous
 login
!
end
```