Problemumgehung für die IP-Adressenzuweisung für das VLAN-Management

Ziel

Wenn der Switch in einem VLAN mit einer IP-Adresse konfiguriert ist, wird die "Fallback"-IP-Adresse in VLAN1 (192.168.1.254) freigegeben. Um die Konnektivität aufrechtzuerhalten, bevor einer VLAN-Schnittstelle eine IP-Adresse zugewiesen wird, muss das Management-VLAN *zuerst* über eine IP-Adresse verfügen. Die IP-Adresse kann über einen DHCP-Server abgerufen oder der VLAN-Schnittstelle statisch zugewiesen werden. Dieser Artikel enthält eine Problemumgehung für die VLAN-IP-Zuweisung.

Unterstützte Geräte

Switches der Serie 250

Software-Version

• 2.5.0.83

Aktivieren von SSH und Bestätigen des Switch-Status

Wenn dies nicht Ihr erstes Booten des Switches ist, fahren Sie mit Schritt 3 fort.

Schritt 1: Schalten Sie den neuen Switch ein, und melden Sie sich über den Webbrowser mit dem Standardbenutzernamen und dem Standardkennwort an.

$\left(\leftarrow \right) \rightarrow $ C $(\square $	(i) 🔏 192.168.1.254/cseb54a3e1/mts/config/log_off_page.htm							
uluulu Switch								
cisco	Application: Switch Management							
	Username: cisco							
	Password: 2							
	Language: English							
	3 Log In Secure Browsing (HTTPS)							

Hinweis: Der Standardbenutzername und das Standardkennwort beim ersten Start sind cisco/cisco.

Schritt 2: Ändern Sie den Standardbenutzernamen und das Standardkennwort. Klicken Sie auf **Apply** (Anwenden).

 $(\leftarrow) \rightarrow$ C (\triangle)

cisco SG250-26	cisco switch20abd3 Language. 26-Port Gigabit Smart Switch				
Change Default User	Change Default User				
	For security reasons, it is required to create a new administration user for device management. This will delete the default user. The minimum requirements for password are as follows: • Cannot be the same as the user name. • Minimum length is 8. • Minimum number of character classes is 3. Character classes are upper case, lower case, numeric, and special characters.				
	• User Name: admin 5/20-maracters used) Password: 9/6 2 aracters used) Confirm Password: 3 Password Strength Meter: Weak				
4	Apply Cancel				

Schritt 3: Klicken Sie nach dem Öffnen des Hauptmenüs auf **Sicherheit > TCP/UDP-Dienste** . Nach dem Laden dieser Seite **aktivieren Sie SSH** auf dem Switch. Klicken Sie auf **Apply** (Anwenden).

SG250-26 26-Port Gigabit Smart Switch								
Getting Started	TCP/UDP Services							
Dashboard								
Configuration Wizards	HTTP Service: 🕑 Enable							
Search	HTTPS Service: 🖉 Enable							
 Status and Statistics 								
 Administration 								
Port Management								
Smartport SSH Service: SSH Service: Enable								
VLAN Management								
Spanning Tree	Cancel							
	TCP Service Table							
MAC Address Tables	TCP Service Table							
MAC Address TablesMulticast	TCP Service Table Service Name Type Local IP Address Local IP Address							
 MAC Address Tables Multicast IP Configuration 	TCP Service Table Service Name Type Local IP Address Local IP HTTP TCP All							
 MAC Address Tables Multicast IP Configuration Security 	TCP Service Table Service Name Type Local IP Address Local IP HTTP TCP All HTTPS TCP All							
 MAC Address Tables Multicast IP Configuration Security RADIUS Client COD/UDD Services 	TCP Service TableService NameTypeLocal IP AddressLocal IPHTTPTCPAllHTTPSTCPAllHTTPTCP192.168.1.254							
 MAC Address Tables Multicast IP Configuration Security RADIUS Client TCP/UDP Services Port Security 	TCP Service TableService NameTypeLocal IP AddressLocal IPHTTPTCPAllIIIIIIHTTPTCPAllIIIIIIHTTPTCP192.168.1.254IIIHTTPTCP192.168.1.254IIII							
 MAC Address Tables Multicast IP Configuration Security RADIUS Client TCP/UDP Services Port Security 802.1X Authentication 	TCP Service TableService NameTypeLocal IP AddressLocal IPHTTPTCPAllIntegrationIntegrationHTTPSTCPAllIntegrationIntegrationHTTPTCP192.168.1.254IntegrationIntegrationHTTPTCP192.168.1.254IntegrationHTTPTCP192.168.1.254Integration							

Schritt 4: Melden Sie sich über SSH beim Switch an. Wir haben Putty gewählt.

Hinweis: Um zu erfahren, wie Sie über SSH oder Telnet auf einen SMB-Switch zugreifen, klicken Sie <u>hier</u>.

Schritt 5: Geben Sie den folgenden Befehl ein, um Details zur Firmware anzuzeigen und zu überprüfen, ob der Switch auf die neueste verfügbare Firmware-Version aktualisiert wird oder nicht.

Hinweis: Es wird empfohlen, die neueste Firmware auf dem Switch zu verwenden. Klicken Sie hier, um die neueste Firmware herunterzuladen.

Schritt 6: Um Informationen zu den VLAN-Einstellungen des Switches anzuzeigen, geben Sie den folgenden Befehl ein:

switch20 Created	abd3#show vlan by: D-Default,	S-Static,	G-GVRP,	R-Radius	Assigned	VLAN,	V-Voice	VLAN
Vlan	Name	Tagged	Ports	UnTago	ged Ports	C	Created k	у
1	1			gi1-2	26,Po1-4		DV	

Schritt 7: Um Informationen über die IP-Schnittstelle anzuzeigen, geben Sie Folgendes ein:

switch20abd3#show ip interface									
IP Address	I/F	I/F Status admin/oper	Туре	Directed Broadcast	Prec	Redirect	Status		
0.0.0.0/32	vlan 1	UP/UP	DHCP	disable	No	enable	Not receiv		
192.168.1.254/24	vlan 1	UP/UP	Default	disable	No	enable	Valid		

Mit dem oben genannten Befehl können Sie die aktuellen IP-Adresseinstellungen an den Schnittstellen anzeigen und entscheiden, ob Sie der neuen VLAN-Schnittstelle eine neue IP zuweisen möchten.

Beispiel: Erstellen des VLAN und Zuweisen der IP-Adresse

Hinweis: Im Folgenden sehen Sie ein Beispiel für die Schritte zum Verlust einer SSH-Sitzung. Wenn Sie den letzten Befehl eingeben, verlieren Sie den Zugriff auf den Switch, da VLAN1 keine IP-Adresse hat und alle Switch-Ports noch VLAN1 zugewiesen sind.

Um direkt zu den Workaround-Schritten zu springen, klicken Sie hier.

Schritt 8: Geben Sie im privilegierten EXEC-Modus des Switches den folgenden Befehl ein, um in den globalen Konfigurationsmodus zu wechseln:



Schritt 9: Um das VLAN 2 auf dem Switch zu konfigurieren, geben Sie Folgendes ein:

switch201bd3 (config) #vlan 2

switch20abd3#configure terminal
switch20abd3(config)#vlan 2

Schritt 10: Um die VLAN 2-Schnittstelle zu verwalten, geben Sie Folgendes ein:

switch201bd3 (config) #interface vlan 2

```
switch20abd3#configure terminal
switch20abd3(config)#vlan 2
switch20abd3(config)#interface vlan 2
```

Schritt 11: Um die IP-Adresse für die VLAN 2-Schnittstelle zu konfigurieren, geben Sie Folgendes ein:

switch201bd3 (config-if) #ip address 192.168.2.254 255.255.255.0

switch20abd3(config)#interface vlan 2
switch20abd3(config-if)#ip address 192.168.2.254 255.255.255.0

Problemumgehung: Verhinderung des Verlusts einer SSH-Sitzung

Wenn Sie der VLAN 1-Schnittstelle eine statische IP-Adresse zuweisen, bleibt die SSH-Verbindung erhalten, wenn Sie VLANs 2, 3, 4 usw. IP-Adressen zuweisen.

Um zu vermeiden, dass die Verbindung von VLAN 1 unterbrochen wird, während Sie die IP-Adresse einer anderen VLAN-Schnittstelle zuweisen, können Sie Folgendes ausführen:

Schritt 1: Geben Sie die folgenden Befehle nacheinander ein, um die statische IP-Adresse für VLAN 1 festzulegen.



Hinweis: von diesem Punkt aus können Sie IP-Adressen beliebig zuweisen.

Schritt 2: Wenden Sie den unten genannten Befehl an, um ein VLAN 2 zu erstellen und eine IP-Adresse zuzuweisen.



Hinweis: Wenn Sie im obigen Beispiel über gi2 mit dem Switch verbunden wären, würde die Verbindung unterbrochen.

Schritt 3: (Optional) Sie können jetzt die VLAN- und IP-Adresse des Switches mithilfe der folgenden Befehle überprüfen.



Fazit

Sie haben nun erfolgreich eine IP-Adresse einer anderen VLAN-Schnittstelle zugewiesen, ohne die Verbindung zu VLAN1 zu verlieren. Es ist hilfreich, eine statische IP auf der VLAN 1-Schnittstelle des Switches für Verwaltungszwecke zuzuweisen.

Sehen Sie sich ein Video zu diesem Artikel an..

Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.