

Konfigurieren der Wireless-Sicherheitseinstellungen auf dem WAP125 und dem WAP581

Ziel

Mit Wireless Security können Sie das Wireless-Netzwerk vor unberechtigtem Zugriff schützen. Die Access Points WAP125 und WAP581 unterstützen den statischen Wired Equivalent Protection (WEP), den Wi-Fi Protected Access (WPA) Personal und WPA Enterprise. Diese Einstellungen können pro Virtual Access Point (VAP) konfiguriert werden. Die Einrichtung dieser Einstellungen bietet Netzwerksicherheit pro VAP. Sie wird in der Regel konfiguriert, wenn der Access Point zum ersten Mal bereitgestellt wird oder wenn Aktualisierungen an den Wireless-Sicherheitseinstellungen des Netzwerks vorgenommen werden.

In diesem Artikel erfahren Sie, wie Sie die Wireless-Sicherheit auf einem WAP125 oder WAP581 Access Point konfigurieren.

Anwendbare Geräte

- WAP125
- WAP581

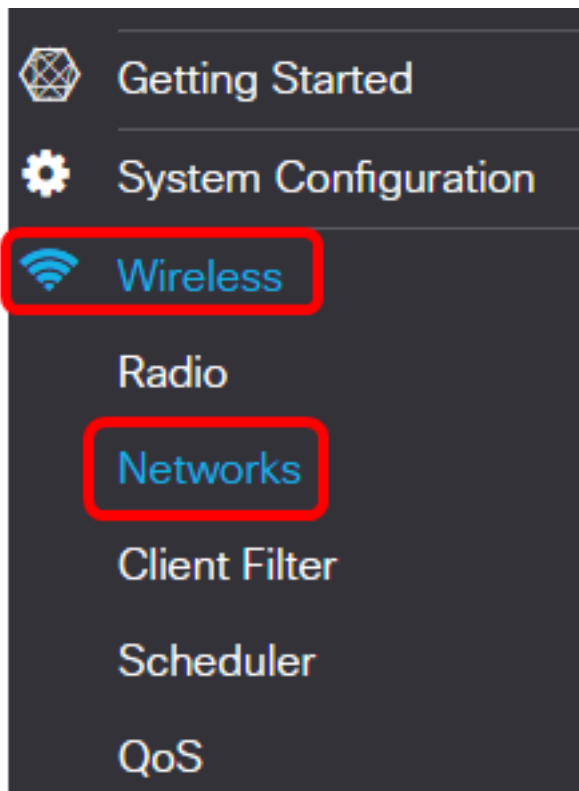
Softwareversion

- WAP125 - 1.0.0.3
- WAP581 - 1.0.0.4

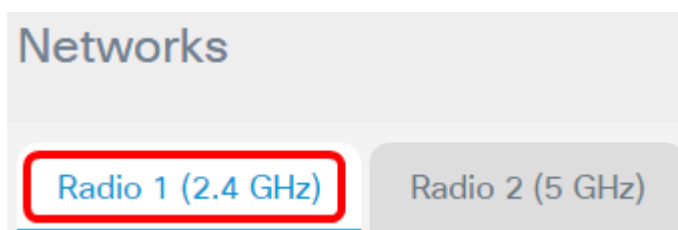
Konfigurieren der Wireless-Sicherheitseinstellungen

WPA Personal Security konfigurieren

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des WAP an, und wählen Sie **Wireless > Networks** aus.

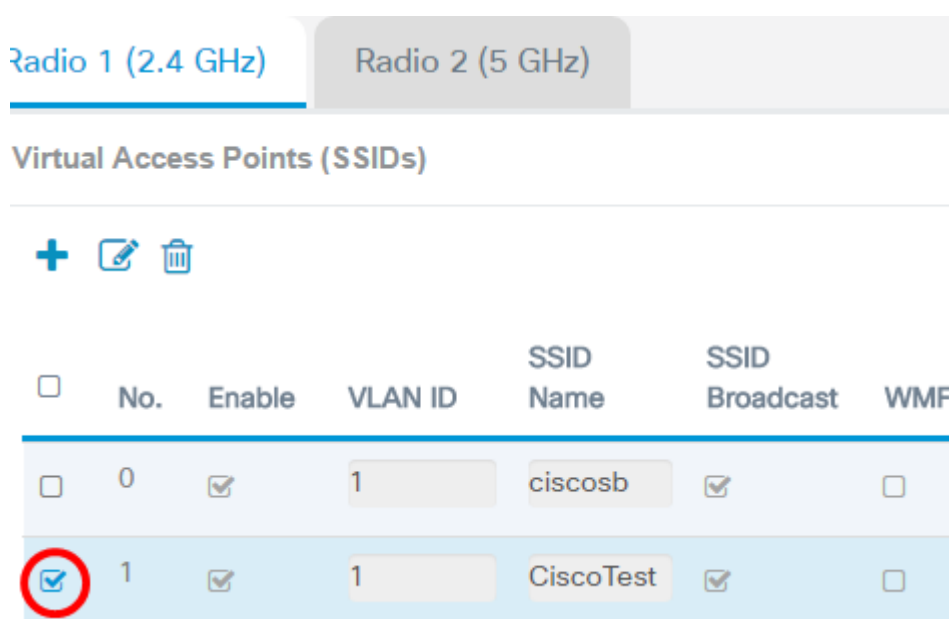


Schritt 2: Wählen Sie die Funkübertragung aus, deren Wireless-Sicherheitseinstellungen konfiguriert werden müssen.



Hinweis: In diesem Beispiel wird Radio 1 (2,4 GHz) ausgewählt.

Schritt 3: Aktivieren Sie das Kontrollkästchen für den VAP, dessen Wireless-Sicherheitseinstellungen konfiguriert werden müssen.



Hinweis: In diesem Beispiel wird VAP 1 ausgewählt.

Schritt 4: Klicken Sie auf **Bearbeiten**.

Radio 1 (2.4 GHz) Radio 2 (5 GHz)

Virtual Access Points (SSIDs)

+ [edit icon] [trash icon]

<input type="checkbox"/>	No.	Enable	VLAN ID	SSID Name	SSID Broadcast	WMF
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	ciscosb	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	CiscoTest	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Schritt 5: Wählen Sie aus der Dropdown-Liste Security (Sicherheit) einen Sicherheitsmodus aus. Folgende Optionen stehen zur Verfügung:

- None (Keine): Diese Option deaktiviert die Wireless-Sicherheitseinstellungen des ausgewählten VAP. Durch das Deaktivieren des Sicherheitsmodus wird das Wireless-Netzwerk geöffnet, und jeder Benutzer mit einem Wireless-Gerät kann eine Verbindung zu Ihrem Netzwerk und den zugehörigen Ressourcen herstellen. Dieser Modus wird zwar nicht empfohlen, kann aber für Netzwerke an entfernten Standorten nützlich sein.
- WPA Personal: Diese Option implementiert WPA-Sicherheit für das Wireless-Netzwerk. Es ermöglicht die Verwendung des Temporal Key Integrity Protocol (TKIP) oder des Advanced Encryption Standard (AES)-Algorithmus. Bei einer Mischung können Geräte, die den AES-Algorithmus nicht unterstützen, eine Verbindung zum Netzwerk herstellen. Mit WPA Personal können Sie ein alphanumerisches Kennwort mit einer Länge von bis zu 64 Zeichen verwenden. WPA Personal wird in der Regel in Büros verwendet, in denen kein RADIUS-Server (Remote Authentication Dial-In User Service) verwendet wird.
- WPA Enterprise (WPA-Enterprise): Mit dieser Option können Sie die Sicherheitsfunktionen von WPA kombinieren und gleichzeitig einen RADIUS-Server verwenden. Dies wird in der Regel in Umgebungen verwendet, in denen ein RADIUS-Server verwendet wird. Wenn Sie diese Option auswählen, klicken Sie [hier](#).

Security

WPA Personal ▼ [eye icon]

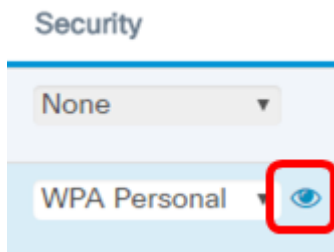
None

WPA Personal

WPA Enterprise

Hinweis: In diesem Beispiel wird WPA Personal ausgewählt.

Schritt 6: Klicken Sie auf die Schaltfläche Ansicht, um die WPA Personal-Parameter zu konfigurieren.



Schritt 7: Wählen Sie im Bereich WPA-Versionen Ihre WPA-Version aus. Folgende Optionen stehen zur Verfügung:

- WPA-TKIP: Diese Option implementiert gemischte Sicherheit im Wireless-Netzwerk. Es eignet sich ideal für Netzwerke mit gemischten Wireless Clients. Diese Option ist standardmäßig deaktiviert.
- WPA2-AES: Diese Option implementiert die WPA2-AES-Sicherheit im Netzwerk. Dies ist ideal für Wireless-Netzwerke mit Clients, die WPA2-Sicherheit unterstützen.

Security Setting

WPA Versions: WPA-TKIP WPA2-AES

Key:

Show Key as Clear Text

Key Strength Meter: Below Minimum

Broadcast Key Refresh Rate

Hinweis: In diesem Beispiel ist WPA-TKIP aktiviert.

Schritt 8: Geben Sie das Netzwerkennwort in das Feld *Schlüssel ein*. Bei der Taste kann es sich um eine Kombination aus Buchstaben und Zahlen handeln, die 8 bis 63 Zeichen lang sein können.

Security Setting

WPA Versions:

WPA-TKIP

WPA2-AES

Key: [?](#)

Cisco!@#\$\$%^&*()

Show Key as Clear Text

Key Strength Meter:



Below Minimum

Broadcast Key Refresh Rate [?](#)

86400

OK

cancel

Hinweis: In diesem Beispiel wird Cisco!@#\$\$%^&*() eingegeben.

Schritt 9: (Optional) Aktivieren Sie das Kontrollkästchen **Schlüssel als Klartext anzeigen**, um den Schlüssel im Klartext anzuzeigen.

Security Setting

WPA Versions:

WPA-TKIP

WPA2-AES

Key: [?](#)

Cisco!@#\$\$%^&*()

Show Key as Clear Text

Key Strength Meter:



Below Minimum

Broadcast Key Refresh Rate [?](#)

86400

OK

cancel

Hinweis: In diesem Beispiel ist Show Key as Clear Text (Schlüssel als Klartext anzeigen) aktiviert.

Schritt 10: Geben Sie die Anzahl der Sekunden ein, bis Ihr Sicherheitsschlüssel im Feld *Aktualisierungsrate* des *Sendeschlüssels* durch einen neu generierten Schlüssel ersetzt wird. Der Standardwert ist 86400.

Security Setting

WPA Versions:

WPA-TKIP

WPA2-AES

Key: [?](#)

Cisco!@#\$\$%^&*()

Show Key as Clear Text

Key Strength Meter:



Below Minimum

Broadcast Key Refresh Rate [?](#)

86400

OK

cancel

Schritt 11: Klicken Sie auf **OK**.

Security Setting

WPA Versions:

WPA-TKIP

WPA2-AES

Key: [?](#)

Cisco!@#\$\$%^&*()

Show Key as Clear Text

Key Strength Meter:



Below Minimum

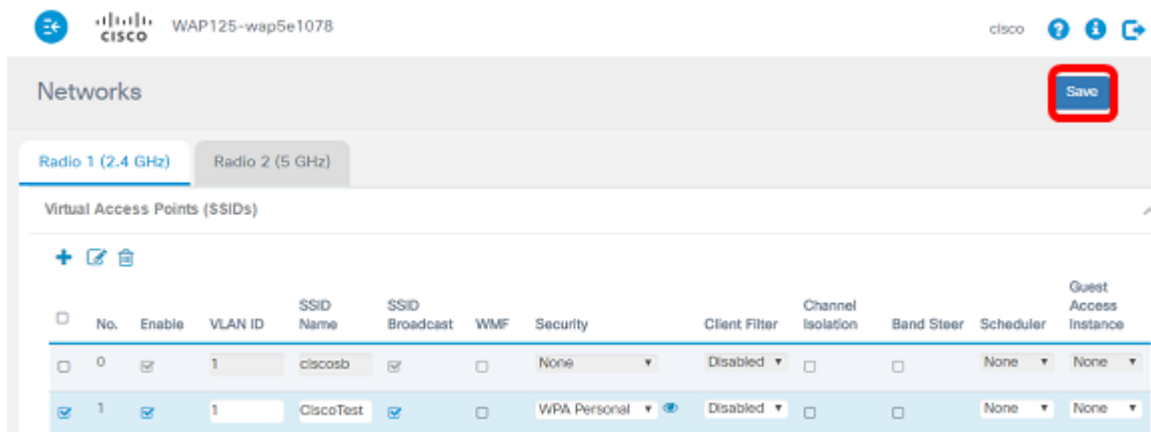
Broadcast Key Refresh Rate [?](#)

86400

OK

cancel

Schritt 12: Klicken Sie auf **Speichern**.

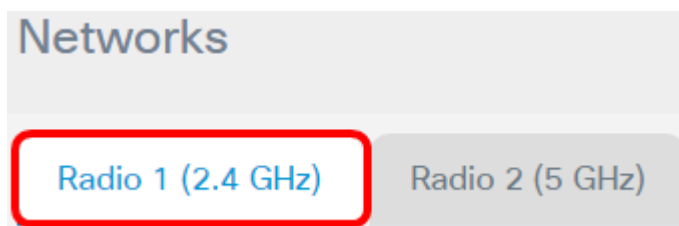


Schritt 13: Klicken Sie auf **OK**.

Die WPA Personal Wireless Security-Einstellungen wurden jetzt auf dem WAP125 konfiguriert.

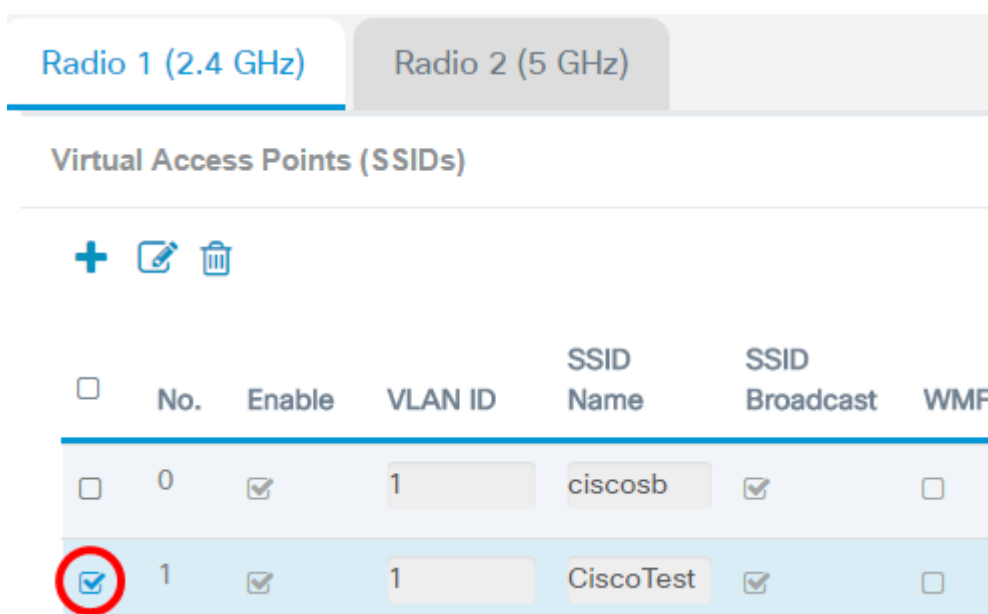
WPA Enterprise Security konfigurieren

Schritt 1: Wählen Sie die Funkübertragung aus, deren Wireless-Sicherheitseinstellungen konfiguriert werden müssen.



Hinweis: In diesem Beispiel wird Radio 1 (2,4 GHz) ausgewählt.

Schritt 2: Aktivieren Sie das Kontrollkästchen für den VAP, dessen Wireless-Sicherheitseinstellungen konfiguriert werden müssen.





Hinweis: In diesem Beispiel wird VAP 1 ausgewählt.

Schritt 3: Klicken Sie auf **Bearbeiten**.

Radio 1 (2.4 GHz) Radio 2 (5 GHz)

Virtual Access Points (SSIDs)


+  

<input type="checkbox"/>	No.	Enable	VLAN ID	SSID Name	SSID Broadcast	WMF
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	ciscosb	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	CiscoTest	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Schritt 4: Wählen Sie WPA Enterprise aus der Dropdown-Liste Security (Sicherheit) aus.

Security

None

WPA Enterprise 

None


WPA Personal

WPA Enterprise

Schritt 5: Klicken Sie auf die Schaltfläche Ansicht, um die WPA Enterprise-Parameter zu konfigurieren.

Security

None

WPA Enterprise 

None

WPA Personal

WPA Enterprise

Schritt 6: Wählen Sie im Bereich WPA-Versionen Ihre WPA-Version aus. Folgende Optionen stehen zur Verfügung:

- WPA-TKIP: Diese Option implementiert gemischte Sicherheit im Wireless-Netzwerk. Es eignet sich ideal für Netzwerke mit gemischten Wireless Clients. Diese Option ist standardmäßig deaktiviert.
- WPA2-AES: Diese Option implementiert die WPA2-AES-Sicherheit im Netzwerk. Dies ist ideal für Wireless-Netzwerke mit Clients, die WPA2-Sicherheit unterstützen.

Security Setting



Hinweis: In diesem Beispiel ist WPA-TKIP aktiviert.

Schritt 7: (Optional) Aktivieren Sie das Kontrollkästchen **Vorauthentifizierung aktivieren**, um die Funktion zu aktivieren. Wenn diese Option aktiviert ist, werden die Vorauthentifizierungsinformationen vom WAP weitergeleitet, dass der Wireless-Client derzeit mit dem Ziel-WAP verbunden ist. Durch die Aktivierung dieser Funktion kann die Authentifizierung für Roaming-Clients beschleunigt werden, die mit mehreren Access Points verbunden sind. Wenn der Sicherheitsmodus deaktiviert ist, ist diese Option ebenfalls deaktiviert und kann nicht bearbeitet werden.

Security Setting



Schritt 8: (Optional) Deaktivieren Sie das Kontrollkästchen Globale RADIUS-Servereinstellungen verwenden, um einen anderen Satz von RADIUS-Servern angeben zu können. Standardmäßig verwendet jeder VAP die für den WAP definierten globalen RADIUS-Einstellungen.

Security Setting

WPA Versions:

WPA-TKIP

WPA2-AES

Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type:

IPv4 IPv6

Server IP Address-1: [?](#)

192.168.1.1

Server IP Address-2: [?](#)

Key-1: [?](#)

.....

Key-2: [?](#)

Enable RADIUS Accounting

Active Server:

Server IP Address-1 ▼

Broadcast Key Refresh Rate: [?](#)

86400

Session Key Refresh Rate: [?](#)

0

OK

cancel

Hinweis: In diesem Beispiel ist die Option Globale RADIUS-Servereinstellungen verwenden nicht aktiviert. Wenn diese Option aktiviert ist, fahren Sie mit [Schritt 17](#) fort.

Schritt 9: (Optional) Wählen Sie einen Server-IP-Adresstyp aus. Folgende Optionen stehen zur Verfügung:

- IPv4: Mit dieser Option kann der WAP den IPv4-RADIUS-Server kontaktieren.
- IPv6 - Mit dieser Option kann der WAP den IPv6 RADIUS-Server kontaktieren.

Security Setting

WPA Versions: WPA-TKIP WPA2-AES

Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: Pv4 IPv6

Server IP Address-1:

Server IP Address-2:

Key-1:

Key-2:

Enable RADIUS Accounting

Active Server:

Broadcast Key Refresh Rate:

Session Key Refresh Rate:

OK

cancel

Hinweis: In diesem Beispiel wird IPv4 ausgewählt.

Schritt 10: (Optional) Geben Sie die IP-Adresse des primären RADIUS-Servers für den VAP im Feld *Server-IP-Adresse -1* ein.

Server IP Address Type: IPv4 IPv6

Server IP Address-1:

Server IP Address-2:

Key-1:

Key-2:

Hinweis: In diesem Beispiel wird 192.168.1.1 eingegeben.

Schritt 11: (Optional) Geben Sie im Feld *Server IP Address -2* (*Server-IP-Adresse -2*) die IP-Adresse des Backup-RADIUS-Servers für den VAP ein.

Server IP Address Type: IPv4 IPv6

Server IP Address-1:

Server IP Address-2:

Key-1:

Key-2:

Hinweis: In diesem Beispiel wird keine Backup-IP-Adresse eingegeben.

Schritt 12: (Optional) Geben Sie im Feld *Key-1* ein Kennwort für die Adresse des primären Servers ein.

Server IP Address Type: IPv4 IPv6

Server IP Address-1:

Server IP Address-2:

Key-1:

Key-2:

Schritt 13: (Optional) Geben Sie im Feld *Key-2* ein Kennwort für die Adresse des Backup-Servers ein.

Server IP Address Type: IPv4 IPv6

Server IP Address-1:

Server IP Address-2:

Key-1:

Key-2:

Hinweis: In diesem Beispiel wird kein Kennwort eingegeben.

Schritt 14: (Optional) Aktivieren Sie das Kontrollkästchen **RADIUS Accounting aktivieren**. Diese Option verfolgt und misst die Ressourcen, die ein bestimmter Benutzer beansprucht hat, z. B. Systemzeit und Menge der übertragenen und empfangenen Daten. Wenn diese Funktion aktiviert ist, wird sie für die primären und Backup-Server aktiviert.

Enable RADIUS Accounting

Active Server:

Broadcast Key Refresh Rate:

Session Key Refresh Rate:

Hinweis: In diesem Beispiel ist Enable RADIUS Accounting aktiviert.

Schritt 15: (Optional) Wählen Sie einen aktiven Server aus der Dropdown-Liste "Active Server" aus.

Server IP Address Type: IPv4 IPv6

Server IP Address-1:

Server IP Address-2:

Key-1:

Key-2:

Enable RADIUS Accounting

Active Server:

Broadcast Key Refresh Rate:

Session Key Refresh Rate:

Hinweis: In diesem Beispiel wird die Server-IP-Adresse-1 ausgewählt.

Schritt 16: (Optional) Geben Sie die Anzahl der Sekunden ein, bis Ihr Sicherheitsschlüssel im Feld *Aktualisierungsrate* für den *Broadcast-Schlüssel* durch einen neu generierten Schlüssel ersetzt wird. Der Standardwert ist 86400.

Active Server:

Broadcast Key Refresh Rate:

Session Key Refresh Rate:

Hinweis: In diesem Beispiel wird die Aktualisierungsrate für den Broadcast-Schlüssel auf dem Standardwert belassen.

Schritt 17: Geben Sie das Intervall ein, in dem der WAP die Sitzungsschlüssel für jeden dem VAP zugeordneten Client aktualisiert. Der Wert kann zwischen 30 und 86.400 Sekunden liegen.

Active Server:

Broadcast Key Refresh Rate:

Session Key Refresh Rate:

Schritt 18: Klicken Sie auf **OK**.

Active Server:

Broadcast Key Refresh Rate:

Session Key Refresh Rate:

Schritt 19: Klicken Sie auf **Speichern**.

WAP125-wap5e1078

Networks Save

Radio 1 (2.4 GHz) Radio 2 (5 GHz)

Virtual Access Points (SSIDs)

No.	Enable	VLAN ID	SSID Name	SSID Broadcast	WMM	Security	Client Filter	Channel Isolation	Band Steer	Scheduler	Guest Access Instance
0	<input type="checkbox"/>	1	ciscosb	<input type="checkbox"/>	<input type="checkbox"/>	None	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	None	None
1	<input checked="" type="checkbox"/>	1	CiscoTest	<input checked="" type="checkbox"/>	<input type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	None	None

Sie sollten jetzt die WPA Enterprise-Sicherheit in Ihrem Wireless-Netzwerk konfiguriert haben.

Sehen Sie sich ein Video zu diesem Artikel an..

[Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.](#)