

# Router an Router Verschlüsselung von DLSw-Datenverkehr

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Konfigurationen](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Befehle debuggen und anzeigen](#)

[Zugehörige Informationen](#)

## [Einführung](#)

In der Beispielkonfiguration in diesem Dokument sind zwei Router mit Data-Link Switching (DLSw)-Peers zwischen ihren Loopback-Schnittstellen eingerichtet. Der gesamte DLSw-Datenverkehr wird zwischen ihnen verschlüsselt. Diese Konfiguration funktioniert für jeden vom Router selbst generierten Datenverkehr.

In dieser Konfiguration ist die Crypto-Zugriffsliste allgemein gehalten. Der Benutzer kann spezifischer sein und DLSw-Datenverkehr zwischen den beiden Loopback-Adressen zulassen. Im Allgemeinen wird nur DLSw-Datenverkehr von der Loopback-Schnittstelle an die Loopback-Schnittstelle übertragen.

## [Voraussetzungen](#)

### [Anforderungen](#)

Für dieses Dokument bestehen keine speziellen Anforderungen.

### [Verwendete Komponenten](#)

Diese Konfiguration wurde mit den folgenden Software- und Hardwareversionen entwickelt und getestet:

- Cisco IOS® Softwareversion 12.0. Diese Konfiguration wurde mit 12,28T getestet.

- Cisco 2500-is56i-l.120-7.T
- Cisco 2513

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## [Konventionen](#)

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

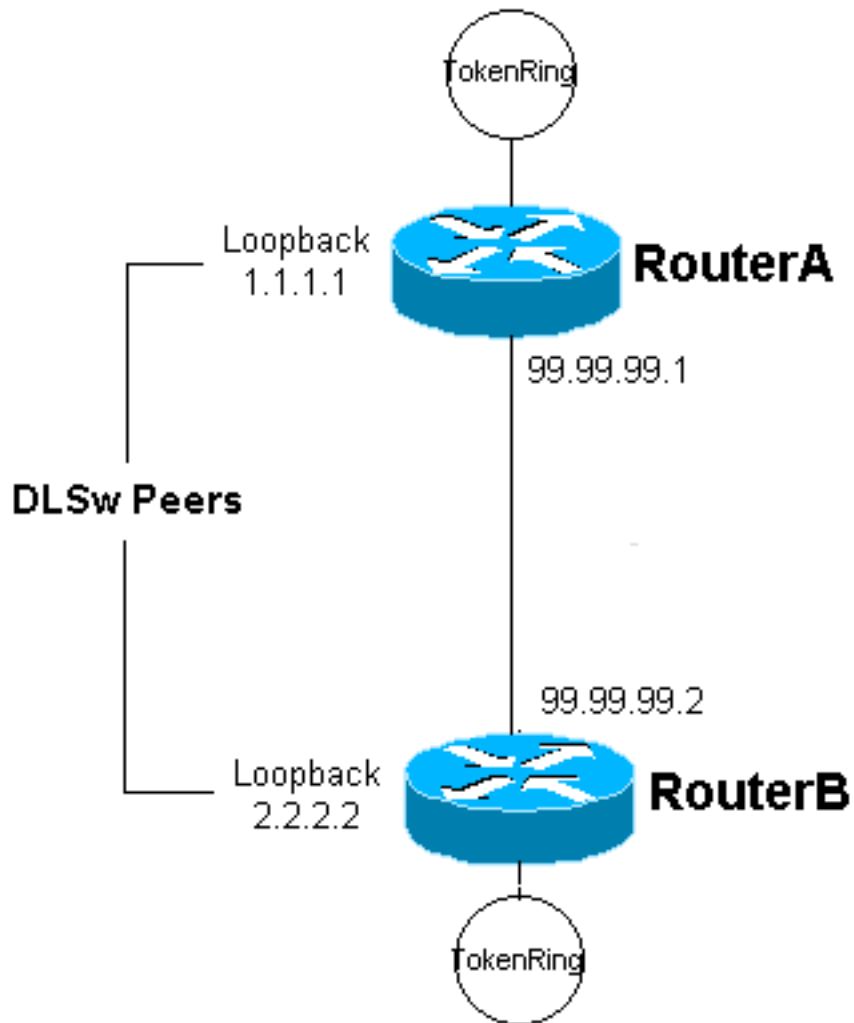
## [Konfigurieren](#)

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

**Hinweis:** Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten.

## [Netzwerkdiagramm](#)

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



## Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- Router A
- Router B

### Router A

Current configuration:

```

!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!
enable secret 5 $1$7WP3$aEqtNjvRJ9Vy6i41x0RJf0
enable password ww
!
ip subnet-zero
!
cns event-service server

```

```

source-bridge ring-group 20
dlsw local-peer peer-id 1.1.1.1
dlsw remote-peer 0 tcp 2.2.2.2
!
crypto isakmp policy 1
  hash md5
  authentication pre-share
crypto isakmp key cisco123 address 99.99.99.2
!
crypto ipsec transform-set dlswset esp-des esp-md5-hmac
!
crypto map dlswstuff 10 ipsec-isakmp
  set peer 99.99.99.2
  set transform-set dlswset
  match address 101
!
!
interface Loopback0
  ip address 1.1.1.1 255.255.255.0
  no ip directed-broadcast
!
interface TokenRing0
  ip address 10.2.2.3 255.255.255.0
  ring-speed 16
  source-bridge 2 3 20
  source-bridge spanning
  no ip directed-broadcast
  no mop enabled
!
interface Serial0
  ip address 99.99.99.1 255.255.255.0
  no ip directed-broadcast
  crypto map dlswstuff
!
ip classless
ip route 0.0.0.0 0.0.0.0 99.99.99.2
no ip http server
!
access-list 101 permit ip host 1.1.1.1 host 2.2.2.2
!
line con 0
  transport input none
line aux 0
line vty 0 4
  password ww
  login
!
end

```

## Router B

Current configuration:

```

!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterB
!
enable secret 5 $1$7WP3$SaEqtNjvRJ9Vy6i41x0RJf0
enable password ww

```

```

!
ip subnet-zero
!
cns event-service server

source-bridge ring-group 10
dlsw local-peer peer-id 2.2.2.2
dlsw remote-peer 0 tcp 1.1.1.1
!
crypto isakmp policy 1
  hash md5
  authentication pre-share
crypto isakmp key cisco123 address 99.99.99.1
!
crypto ipsec transform-set dlswset esp-des esp-md5-hmac
!
crypto map dlswstuff 10 ipsec-isakmp
  set peer 99.99.99.1
  set transform-set dlswset
  match address 101
!
!
interface Loopback0
  ip address 2.2.2.2 255.255.255.0
  no ip directed-broadcast
!
interface TokenRing0
  ip address 10.1.1.3 255.255.255.0
  ring-speed 16
  source-bridge 2 3 10
  source-bridge spanning
  no ip directed-broadcast
  no mop enabled
!
interface Serial0
  ip address 99.99.99.2 255.255.255.0
  no ip directed-broadcast
  crypto map dlswstuff
!
ip classless
ip route 0.0.0.0 0.0.0.0 99.99.99.1
no ip http server
!
access-list 101 permit ip host 2.2.2.2 host 1.1.1.1
!
line con 0
  transport input none
line aux 0
line vty 0 4
  password ww
  login
!
end

```

## Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

## Fehlerbehebung

In diesem Abschnitt finden Sie eine Fehlerbehebung für Ihre Konfiguration.

## Befehle debuggen und anzeigen

Das [Output Interpreter Tool](#) (nur [registrierte](#) Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show** **anzuzeigen**.

**Hinweis:** Beachten Sie [vor der](#) Verwendung von **Debug**-Befehlen die [Informationen](#) zu [Debug-Befehlen](#).

- **debug crypto ipsec** - Dieser Befehl zeigt die IP Security Protocol (IPSec)-Aushandlungen von Phase 2 an.
- **debug crypto isakmp** - Dieser Befehl zeigt die ISAKMP-Verhandlungen (Internet Security Association and Key Management Protocol) von Phase 1 an.
- **debug crypto engine** - Dieser Befehl zeigt den verschlüsselten Datenverkehr an.
- **show crypto ipsec sa** — Zeigt die Sicherheitszuordnungen für Phase 2 an.
- **show crypto isakmp sa** — Dieser Befehl zeigt die Sicherheitszuordnungen für Phase 1 an.
- **show dlsw peer** - Dieser Befehl zeigt den DLSw-Peer-Status und den Verbindungsstatus an.

## Zugehörige Informationen

- [IPSec-Support-Seite](#)
- [DLSW-Support-Seite](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)