

# Fehlerbehebung bei Router-Angriffen

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konsole reagiert nicht.](#)

[Schritte zur Fehlerbehebung](#)

[Datenverkehr wird nicht weitergeleitet](#)

[Mögliche Ursachen](#)

[Abrufen einer Stack-Nachverfolgung von der ROM-Überwachung](#)

[Informationen, die beim Öffnen einer TAC-Serviceanfrage gesammelt werden müssen](#)

[Zugehörige Informationen](#)

## [Einleitung](#)

Dieses Dokument unterstützt Sie bei der Fehlerbehebung für ein System, das nicht reagiert. Das Dokument behandelt auch die Ursache und wie Sie das Problem beheben können.

Ein Router scheint nicht mehr zu funktionieren, wenn das System nicht auf die Konsole reagiert oder Anfragen vom Netzwerk sendet (z. B. Telnet, Simple Network Management Protocol (SNMP) usw.). Diese Probleme lassen sich in zwei große Kategorien einteilen:

- Wenn die Konsole nicht reagiert.
- Wenn der Datenverkehr nicht durchläuft.

## [Voraussetzungen](#)

### [Anforderungen](#)

Es gibt keine spezifischen Anforderungen für dieses Dokument.

### [Verwendete Komponenten](#)

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Alle Cisco IOS<sup>®</sup> Softwareversionen
- Alle Cisco Router

Dieses Dokument gilt nicht für Cisco Catalyst Switches oder MGX-Plattformen.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

## Konventionen

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

## Konsole reagiert nicht.

Konsolenprobleme treten auf, wenn der Router nicht mehr reagiert, um an den Konsolenport einzugeben. Wenn die Konsole nicht reagiert, bedeutet dies, dass ein Vorgang mit hoher Priorität den Konsolentreiber daran hindert, auf Eingaben zu reagieren.

## Schritte zur Fehlerbehebung

- Überprüfen der Kabelverbindung
- Überprüfen Sie, ob das Netzteil eingeschaltet ist.
- Überprüfen Sie den Status der Router-LED. Wenn alle LEDs nicht leuchten, ist dies höchstwahrscheinlich ein Problem mit dem Netzteil des Routers.

Wenn der Datenverkehr weiterhin über den Router fließt:

- Trennen Sie die Netzwerkschnittstellen, und prüfen Sie, ob der Router reagiert. Oft geht der Router davon aus, dass er etwas zu Wichtiges für exec-Sitzungen tut.
- Sie können auch versuchen, das Problem zu reproduzieren, nachdem Sie die folgenden Befehle ausgegeben haben: Für die Cisco Serien 7200 und 7500 gilt Folgendes:

```
configure terminal
scheduler allocate 3000 1000
^Z
```

Der **Scheduler**-Befehl garantiert CPU-Zeit für Prozesse mit niedriger Priorität. Dabei wird eine maximale Zeit für Fast-Switching (3.000 Mikrosekunden -  $\mu$ s) und Prozessswitching (1.000  $\mu$ s) pro Netzwerk-Interrupt-Kontext festgelegt. Auf allen anderen Plattformen:

```
configure terminal
scheduler interval 500
^Z
```

Der Befehl **Scheduler interval** ermöglicht die Planung von Prozessen mit niedriger Priorität alle 500 Sek., sodass einige Befehle eingegeben werden können, selbst wenn die CPU-Auslastung bei 100 % liegt. Weitere Informationen zu diesen Befehlen finden Sie unter [Grundlegende Systemverwaltungsbefehle](#) in der Cisco IOS Software-Befehlsreferenz.

- Wenn die Konsole nicht reagiert, weil die CPU-Auslastung des Routers hoch ist, ist es wichtig, die Ursache für die hohe CPU-Auslastung zu finden und zu korrigieren. Wenn beispielsweise prozessgesteuerter IP-Datenverkehr Probleme verursacht, wird dies im "IP Input"-Prozess in der Ausgabe des Befehls **show process cpu** wiedergegeben. In dieser Situation ist es wichtig, die Ausgabe von **show interfaces**, **show interfaces stat** und möglicherweise **Prozesse** zur

weiteren Diagnose des Problems zu erfassen. Um das Problem zu beheben, müssen Sie die Anzahl des IP-Datenverkehrs reduzieren, der prozessumgeschaltet wird. Weitere Informationen finden Sie unter [Fehlerbehebung bei hoher CPU-Auslastung auf Cisco Routern](#).

- Eine weitere mögliche Ursache für einen scheinbaren Auflegen ist ein Speicherzuweisungsfehler. d. h., entweder der Router hat alle verfügbaren Speicher verwendet, oder der Speicher wurde in so kleine Teile zerlegt, dass der Router keinen geeigneten verfügbaren Block finden kann. Weitere Informationen finden Sie unter [Beheben von Speicherproblemen](#).
- Der Router kann aufgrund eines Sicherheitsproblems wie Wurm oder Virus nicht mehr reagieren. Dies ist besonders dann der Fall, wenn in letzter Zeit keine Änderungen am Netzwerk vorgenommen wurden, z. B. ein Router-IOS-Upgrade. In der Regel kann eine Konfigurationsänderung, z. B. das Hinzufügen zusätzlicher Zeilen zu Ihren Zugriffslisten, die Auswirkungen dieses Problems mindern. Die Seite [Cisco Security Advisories and Notices](#) enthält Informationen zur Erkennung der wahrscheinlichsten Ursachen und spezifischer Problemumgehungen. Weitere Informationen finden Sie unter: [100 Fragen und Antworten zu Bedrohungen aus dem InternetCisco Bedrohungskontrolle](#)
- Wenn der Router während des Startvorgangs nicht mehr reagiert, kann dies auf eine falsch konfigurierte Funktion oder einen Softwarefehler in einer konfigurierten Funktion zurückzuführen sein. Dies wird häufig durch das Auftreten einer Warnung oder Fehlermeldung auf der Konsole unmittelbar vor dem Einfrieren des Routers deutlich. Um dieses Problem zu umgehen, starten Sie den Router in ROMMON, umgehen die gespeicherte Konfiguration und konfigurieren Sie sie dann erneut. Führen Sie diese Schritte aus: Schließen Sie ein Terminal bzw. einen PC mit Terminal-Emulation an den Konsolenport des Routers an. Verwenden Sie diese Terminaleinstellungen: Baudrate 9600 Keine Parität 8 Datenbits 1 Stoppbit Keine Flusssteuerung Starten Sie den Router neu, und brechen Sie den ROMMON ein, indem Sie innerhalb von 60 Sekunden nach dem Einschalten auf die **Unterbrechungstaste** der Tastatur drücken. Wenn die Unterbrechungssequenz nicht funktioniert, finden Sie weitere Tastenkombinationen [während der Kennwortwiederherstellung](#) unter [Standardtastenkombinationen](#). Ändern Sie das Konfigurationsregister in 0x2142, und setzen Sie den Router zurück. Dazu führen Sie den Befehl **confreg 0x2142** an der Eingabeaufforderung `rommon 1>` aus. Geben Sie dann **reset** an der Eingabeaufforderung `2>` ein. Dadurch wird der Router von Flash gestartet, ohne die Konfiguration zu laden. Geben Sie **no** nach jeder Einrichtungsfrage ein, oder drücken Sie Strg-C, um die Ersteinrichtung zu überspringen. Geben Sie **enable** bei der Eingabeaufforderung `Router>` ein. Sie befinden sich im **Aktivierungsmodus** und sehen die Eingabeaufforderung `Router#`. Jetzt können Sie eine leere Konfiguration speichern (alle Befehle entfernt). Geben Sie den Befehl **copy running-config startup-config** ein. Wenn Sie den Verdacht haben, dass ein bestimmter Befehl das Problem verursacht, können Sie auch die Konfiguration bearbeiten. Führen Sie dazu den Befehl **copy startup-config running-config** aus. Geben Sie dann **configure terminal** ein, und nehmen Sie die Änderungen vor. Wenn Sie fertig sind, setzen Sie die Konfigurationsregistrierung auf 0x2102 zurück. Geben Sie hierfür **config-register 0x2102** ein. Geben Sie den Befehl **copy running-config startup-config** ein, um die Änderungen zu bestätigen.

Wenn der Datenverkehr nicht durch den Router fließt:

- Wenn der Datenverkehr nicht mehr durch den Router fließt und die Konsole nicht reagiert, besteht möglicherweise ein Problem mit dem System. Im Allgemeinen bedeutet dies, dass der Router in einer durchgehenden Schleife gefangen oder an einer Funktion festgehalten wird. Dies wird fast immer durch einen Fehler in der Software verursacht. Installieren Sie die

neueste Wartungsversion der Cisco IOS-Softwareschulung, die Sie aktuell ausführen. Bevor Sie eine Serviceanfrage beim Cisco TAC erstellen, [rufen Sie eine Stapelüberwachung vom ROM Monitor ab](#). Wenn Sie während eines Problems Stack-Traces erhalten, können Sie feststellen, wo im Code der Router Schleifen oder fixiert ist.

## Datenverkehr wird nicht weitergeleitet

Datenverkehrsprobleme treten auf, wenn die Konsole weiterhin reagiert, der Datenverkehr jedoch nicht über den Router fließt. In diesem Fall reagiert ein Teil des Datenverkehrs oder ein Teil der Schnittstellen nicht. Dieses Verhalten kann auf verschiedene Ursachen zurückzuführen sein. Wenn dieses Problem auftritt, können Informationen über den Konsolenport vom Router gesammelt werden. Die Ursachen für diese Datenverkehrsprobleme reichen von Schnittstellenfehlern bis hin zu Software- und Hardwareproblemen.

### Mögliche Ursachen

- **Routingproblem** - Änderungen in der Netzwerktopologie oder in der Konfiguration einiger Router könnten sich auf die Routing-Tabellen ausgewirkt haben.
- **Hohe CPU-Auslastung** - Führen Sie den Befehl **show process cpu aus**. Wenn die CPU über 95 % liegt, kann die Leistung des Routers beeinträchtigt werden, und Pakete können verzögert oder verworfen werden. Weitere Informationen finden Sie unter [Fehlerbehebung bei hoher CPU-Auslastung auf Routern](#).
- **Schnittstelle ausgefallen** - Eine der Router-Schnittstellen kann ausgefallen sein. Es gibt mehrere Ereignisse, die dies verursachen können, die von einem falschen Konfigurationsbefehl bis zu einem Hardwarefehler der Schnittstelle oder des Kabels reichen können. Wenn einige Schnittstellen bei Ausgabe des Befehls **show interfaces** nicht angezeigt werden, versuchen Sie herauszufinden, was die Schnittstelle verursacht hat.
- **Hochbekannte Schnittstellen** - Dies ist ein besonderer Fall von Pufferlecks, die dazu führen, dass die Eingangswarteschlange einer Schnittstelle bis zu dem Punkt gefüllt ist, an dem sie Pakete nicht mehr akzeptieren kann. Laden Sie den Router neu. Dadurch wird diese Eingabewarteschlange freigegeben und der Datenverkehr wiederhergestellt, bis die Warteschlange wieder voll ist. Je nach Schweregrad des Lecks kann dies zwischen wenigen Sekunden und einigen Wochen dauern. Der einfachste Weg, eine verheiratete Schnittstelle zu identifizieren, ist, einen Befehl **show interfaces** zu erstellen und nach etwas Ähnlichem zu suchen:

```
Output queue 0/40, 0 drops; input queue 76/75, 27 drops
```

Detaillierte Richtlinien und Beispiele finden Sie unter [Troubleshooting Buffer Leaks](#) (Fehlerbehebung).

## Abrufen einer Stack-Nachverfolgung von der ROM-Überwachung

*K-trace* bezeichnet die Prozedur, mit der eine Stapelüberwachung vom Router aus ROM Monitor abgerufen wird. Auf Routern mit älterem ROM Monitor-Code wird eine Stapelüberwachung mit dem Befehl **k** abgerufen. Auf Routern, die einen neueren ROM Monitor-Code ausführen, kann auch der **Stapel**-Befehl verwendet werden.

Gehen Sie wie folgt vor, um Stapelspuren von einem Router abzurufen, der nicht reagiert:

1. Aktivieren Sie die Unterbrechungssequenz. Ändern Sie dazu den Wert für das Konfigurationsregister. Der achte Bit-Wert muss auf Null gesetzt werden, damit Unterbrechungen nicht ignoriert werden. Ein Wert von 0x2002 funktioniert.

```
Router#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)#config-register 0x2002
```

2. Laden Sie den Router neu, sodass der neue Wert für das Konfigurationsregister verwendet wird.
3. Senden Sie die Unterbrechungssequenz, wenn das Problem auftritt. Die ROM Monitor-Eingabeaufforderung ">" oder "rommon 1 >" muss angezeigt werden.
4. Erfassen einer Stapelüberwachung Hierzu müssen Sie die Ausgabe entweder von den Befehlen **k 50** oder **stack 50** erfassen. Fügen Sie **50** zum Befehl hinzu, um eine längere Stapelüberwachung zu drucken.
5. Geben Sie den Befehl **c** oder **cont** ein, um fortzufahren.
6. Wiederholen Sie die letzten drei Schritte mehrmals, um sicherzustellen, dass mehrere Punkte in einer kontinuierlichen Schleife erfasst wurden.
7. Nachdem Sie mehrere Stack-Traces erhalten haben, starten Sie den Router neu, um den ausgefallenen Zustand zu beheben.

Hier ein Beispiel für dieses Verfahren:

```
User break detected at location 0x80af570
rommon 1 > k 50
Stack trace:
PC = 0x080af570
Frame 00: FP = 0x02004750      RA = 0x0813d1b4
Frame 01: FP = 0x02004810      RA = 0x0813a8b8
Frame 02: FP = 0x0200482c      RA = 0x08032000
Frame 03: FP = 0x0200483c      RA = 0x040005b0
Frame 04: FP = 0x02004b34      RA = 0x0401517a
Frame 05: FP = 0x02004bf0      RA = 0x04014d9c
Frame 06: FP = 0x02004c00      RA = 0x040023d0
Frame 07: FP = 0x02004c68      RA = 0x04002e9e
Frame 08: FP = 0x02004c78      RA = 0x040154fe
Frame 09: FP = 0x02004e68      RA = 0x04001fc0
Frame 10: FP = 0x02004f90      RA = 0x0400c41e
Frame 11: FP = 0x02004fa4      RA = 0x04000458
Suspect bogus FP = 0x00000000, aborting
rommon 2 > cont
```

Wiederholen Sie diese Prozedur mehrmals, wenn ein Systemproblem auftritt, um mehrere Instanzen der Stapelüberwachung zu erfassen.

Wenn ein Router nicht reagiert, ist dies fast immer ein Softwareproblem. Sammeln Sie in diesem Fall so viele Informationen wie möglich, einschließlich der Stapelüberwachung, bevor Sie eine TAC-Serviceanfrage öffnen. Es ist auch wichtig, die Ausgabe der Befehle **show version**, **show run** und **show interfaces** einzuschließen.

## [Informationen, die beim Öffnen einer TAC-Serviceanfrage gesammelt werden müssen](#)

Wenn Sie eine TAC-Serviceanfrage öffnen, fügen Sie
--

**Ihrer Anfrage zur Fehlerbehebung von Router-Änderungen die folgenden Informationen bei:**

- Fehlerbehebung vor dem Öffnen des Gehäuses durchgeführt
- Ausgabe **des technischen Supports anzeigen** (wenn möglich im Aktivierungsmodus)
- **Protokollausgabe** oder Konsolenaufzeichnungen **anzeigen**, falls verfügbar
- [Stapelverfolgung vom ROM Monitor](#)

Bitte fügen Sie die gesammelten Daten in einem nicht zippierten Textformat (.txt) an Ihr Ticket an. Sie können Informationen zu Ihrem Ticket hinzufügen, indem Sie es mit dem [TAC Service Request Tool](#) hochladen (nur [registrierte](#) Kunden). Wenn Sie nicht auf das TAC Service Request Tool zugreifen können, können Sie die entsprechenden Informationen an Ihr Ticket anhängen, indem Sie die Ticketnummer in der Betreffzeile Ihrer Nachricht an [attach@cisco.com](mailto:attach@cisco.com) senden.

**Hinweis:** Wenn die Konsole reagiert, laden Sie den Router nicht manuell neu oder schalten Sie ihn ein, bevor Sie die oben genannten Informationen sammeln. Es sei denn, Sie müssen eine Fehlerbehebung bei Fehlern des Routers durchführen. Dies kann dazu führen, dass wichtige Informationen verloren gehen, die zur Bestimmung der Ursache des Problems erforderlich sind.

## [Zugehörige Informationen](#)

- [Befehl show process](#)
- [Standardkombinationen für die Break-Key-Sequenz während der Kennwortwiederherstellung](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)