

Wann sollte Scrambling auf virtuellen ATM-Schaltungen aktiviert werden?

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Verstehen von Komplikationen](#)

[Wie aktiviere ich Scrambling?](#)

[Der Befehl zum Verschlüsseln von Zellen-Payloads in einer Zelle](#)

[Erläuterungen zu Befehlen "atm ds3-cramble" und "atm e3 cramble"](#)

[Verstehen des Befehls "crambling payload"](#)

[Bekanntes Problem: ATM-Scrambling Cell-Payload Deaktiviert beim Neuladen](#)

[Scrambling auf ATM Switch Routern](#)

[ATM Scrambling auf Packet Over SONET Links](#)

[Machen Scrambling ATM-Links sicher?](#)

[Zugehörige Informationen](#)

Einführung

ATM ist ein Layer-2-Protokoll und ein Protokoll-Stack, ähnlich wie IP ein Layer-3-Protokoll und ein Protokoll-Stack. Die [ATM-Referenzmodell](#)-Tabelle veranschaulicht den Protokollstapel für ATM.

ATM-Referenzmodell	
Höhere Schichten	
ATM Adaptation Layer (AAL)	Sublayer (Convergence Sublayer, CS) Segmentation and Reassembly (SAR)
ATM-Schicht	Generische Flow Control (GFC) Cell Header Creation and Verification Cell Virtual Path Identifier (VPI) und Virtual Channel Identifier (VCI) Translation Cell Multiplexing und Demultiplex
Physische Schichten	
Transmission Convergence (TC)-	Header Error Control (HEC) Generation and Verification Cell Delineation Cell-Rate Entkopplung Transmission Adaption

Subschicht	
Unterschicht Physical Medium Dependent (PMD)	Bit-Timing (Zeitwiederherstellung) Leitungscodierung für physisches Medium

Die physische Schicht besteht aus zwei Subschichten. Die obere Hälfte der physischen Schicht ist die TC-Unterschicht, die Funktionen wie Zellenverwürfelung und -entschlüsselung, Zelltrennung sowie HEC-Generierung und -Verifizierung implementiert.

In diesem Dokument werden die Vorteile des Scrambling und die verschiedenen Befehle erläutert, die zum Scrambling auf ATM-Schnittstellen verwendet werden, je nach dem physischen Layer-Schnittstellenmodul (PLIM).

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

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 in den [Cisco Technical Tips Conventions](#).

Verstehen von Komplikationen

Das Scrambling ist so konzipiert, dass es das Muster von Einsen und Nullen zufällig in ATM-Zellen oder im physischen Layer-Frame transportiert. Das Randomisieren der digitalen Bits kann kontinuierliche, nicht variable Bitmuster verhindern. d. h. lange Zeichenfolgen aller 1s oder 0s. Mehrere Protokolle auf physischen Ebenen basieren auf Übergängen zwischen 1s und 0s, um die Taktgebung aufrechtzuerhalten.

Ein problematisches Symptom, das sich gut für Verwürfelungen eignen kann, sind Verbindungs-Flaps, die auftreten, wenn bestimmte Dateien einen ATM-Link überschreiten. Solche Dateien können eine so lange Zeichenfolge aller 1s oder 0s erzeugen.

Wenn Sie die Scrambling-Funktion für Zell-Payloads aktivieren möchten, stellen Sie sicher, dass beide Enden eines virtuellen Kanals (VC) mit derselben Scrambling-Einstellung konfiguriert sind.

Beachten Sie, dass die meisten ATM-Schnittstellen keine standardmäßige Scrambling-Anweisung in der Konfiguration enthalten. Mit dem PA-A3-T3-Port-Adapter wird beispielsweise nur eine nicht standardmäßige Einstellung des `Cell-Payload-Scrambling` in der Konfiguration angezeigt. Im Gegensatz dazu wird in der Konfiguration für ein NM-4T1-IMA-Netzwerkmodul immer eine Scrambling-Anweisung angezeigt.

Wie aktiviere ich Scrambling?

Die Cisco IOS®-Software unterstützt drei Befehle, um das Verwürgen auf Router-ATM-Schnittstellen zu ermöglichen:

- **atm crambling cell payload** - Alle anderen ATM-Schnittstellen-Hardware (außer PA-A1).
- **atm ds3-cramble** - Nur DS-3-ATM-Schnittstellen (Digital Signal Level 3). **Hinweis:** DS-3-Schnittstellen verwenden jetzt den Befehl **atm crambling cell payload** für eine äquivalente Funktionalität.
- **Payload-Scrambling:** Nur IMA-Netzwerkmodule (2600 und 3600 Inverse Multiplexing over ATM).

In den folgenden Abschnitten werden diese Befehle ausführlicher behandelt.

Der Befehl zum Verschlüsseln von Zellen-Payloads in einer Zelle

Die meisten ATM-Schnittstellen auf Cisco Routern unterstützen den Befehl zum **Verschlüsseln der Payload-Zelle**. Bestätigen Sie mit dem Befehl **show atm interface atm** die Scrambling-Einstellungen.

```
router(config-if)# atm scrambling ?
cell-payload  SONET in cell payload scrambling mode
sts-stream    SONET in sts-stream scrambling mode

7200-1# show atm interface atm 3/0

Interface ATM3/0:
AAL enabled:   AAL5 , Maximum VCs: 4096, Current VCCs: 1
Maximum Transmit Channels: 0
Max. Datagram Size: 4528
PLIM Type: SONET - 155000Kbps, TX clocking: LINE
Cell-payload scrambling: ON
sts-stream scrambling: ON
0 input, 0 output, 0 IN fast, 0 OUT fast, 0 out drop
  Avail bw = 155000
Config. is ACTIVE
```

Diese Ausgabe zeigt, dass die SONET-Schnittstellen (Synchronous Optical Network) zwei Verwürfelungsebenen unterstützen. Die erste Stufe, der ST-Stream-Scrambling-Modus, ist nach dem GR-253-Standard des Bereichs ITU-T (International Telecommunication Union Telecommunication Standardization Sector) erforderlich. Es verwendet einen $1 + x^6 + x^7$ -Algorithmus und verwirft bis auf die erste Zeile den Abschnittsüberhang des SONET-Frames. Betrachten Sie die folgende Definition der Verwendung von sts-stream-Scrambling in Abschnitt 5.1.3 von GR-253:

"SONET-Signale für optische Schnittstellen verwenden binäre Leitungskodierung und müssen daher verschlüsselt werden, um eine angemessene Anzahl von Übergängen (0 auf 1 s und 1 auf 0

s) für Zwecke wie die Wiederherstellung der Leitungsgeschwindigkeit am Empfänger sicherzustellen. Die Signale der elektrischen SONET-Schnittstellen verwenden Leitungscodes, die angemessene Übergänge gewährleisten. Sie werden jedoch auch aus Gründen der Konsistenz zwischen der elektrischen und der optischen Schnittstelle verworfen. Der Scrambler muss auf dem höchstwertigen Bit des Bytes nach dem Z0-Byte im Nten STS-1 auf '111111' zurückgesetzt werden (d. h. das Byte, das dem letzten Z0-Byte folgt). Der Scrambler muss während des gesamten verbleibenden STS-N-Frames kontinuierlich von diesem Bit aus ausgeführt werden. Beachten Sie, dass die Framing-Bytes (A1 und A2), das Section Trace-Byte (J0) und das Section Growth (Z0)-Byte nicht verschlüsselt sind."

Die zweite Stufe des Scrambling, das Scrambling von Zellen-Payloads, ist optional und in ITU-T [I.432](#), Abschnitt 4.5.3 definiert. Es verwendet ein Polynom von $1 + x^{43}$. Beim Cell-Payload-Scrambling werden die Bits nur im Payload-Teil einer ATM-Zelle randomisiert, und der 5-Byte-Header wird entschlüsselt. Zell-Payload-Scrambling ist darauf ausgelegt, eine erfolgreiche ATM-Zelltrennung sicherzustellen, d. h. den Prozess der Erkennung des Beginns jeder neuen Zelle.

Zusammenfassend ist es wichtig zu verstehen, dass das Scrambling auf SONET-Ebene oder auf STS auf jedem SONET-Gerät aktiviert sein muss. Das Verschlüsseln von Zellen-Payloads kann mit einem Konfigurationsbefehl aktiviert oder deaktiviert werden.

Beachten Sie, dass die Befehlszeile der Cisco IOS Software eine Option zum Deaktivieren des Scrambling-Streams bietet. Obwohl dieser Befehl akzeptiert wird, wird dieses Ausmaß der Verwürfelung nicht deaktiviert. [CSCdu17082](#) entfernt diesen Befehl in einer zukünftigen Version.

[Erläuterungen zu Befehlen "atm ds3-cramble" und "atm e3 cramble"](#)

Die Verschlüsselung von Leitungsprotokollen an DS-3- und E3-Schnittstellen kann von Verwürfelungen profitieren. Scrambling hilft vor allem, eine präzise Taktrückgewinnung auf der ATM-Schnittstelle sicherzustellen.

Ursprünglich verwendete die Cisco IOS Software die Befehle **ds3-Scramble** und **ATM ds3-Scramble** auf DS-3-Schnittstellen und den Befehl **ATM e3-Scramble** auf E3-Schnittstellen. In der Cisco IOS Software, Version 12.2, werden diese Befehle ausgeblendet und - sofern konfiguriert - als **ATM-Scrambling-Cell-Payload** in der Konfiguration angezeigt.

```
Router# show atm interface atm 2/0/0

ATM interface ATM2/0/0:
AAL enabled: AAL5, Maximum VCs: 4096, Current VCCs: 12
Max. Datagram Size:4528, MIDs/VC: 1024
PLIM Type:DS3 - 45Mbps, Framing is C-bit ADM,
DS3 lbo: short, TX clocking: LINE
Scrambling: OFF
227585 input, 227585 output, 0 IN fast, 0 OUT fast
Config. is ACTIVE
```

[Verstehen des Befehls "crambling payload"](#)

Das IMA-Netzwerkmodul für die Router der Serien 2600 und 3600 unterstützt den [Befehl Scrambling-Payload](#). In der Cisco IOS Software-Version 12.0(5)T und 12.0(5)XK wurde Unterstützung für das IMA-Modul und diesen Befehl eingeführt.

Standardmäßig ist das Payload-Scrambling für T1-Verbindungen und E1-Verbindungen

deaktiviert. Die standardmäßige binäre 8-0-Substitution (B8ZS)-Leitungscodierung für T1-Verbindungen reicht normalerweise für eine ordnungsgemäße Zelltrennung aus. Die Scrambling-Einstellung muss mit dem Gegenstück übereinstimmen.

Verwenden Sie die Befehle **show atm interface atm** oder **show controller atm**, um den Status des Scrambling auf den IMA-Schnittstellen anzuzeigen.

```
router# show controller atm 0/2
```

```
Interface ATM0/2 is administratively down
```

```
Hardware is ATM T1
```

```
!--- Output suppressed. SAR Scheduling channels: -1 -1 -1 -1 -1 -1 -1 -1 Part of IMA group 3  
Link 2 IMA Info: group index is 1 Tx link id is 2, Tx link state is unusableNoGivenReason Rx  
link id is 99, Rx link state is unusableFault Rx link failure status is fault, 0 tx failures, 3  
rx failures Link 2 Framer Info: framing is ESF, line code is B8ZS, fdl is ANSI cable-length is  
long, Rcv gain is 26db and Tx gain is 0db, clock src is line, payload-scrambling is disabled, no  
loopback
```

[Bekanntes Problem: ATM-Scrambling Cell-Payload Deaktiviert beim Neuladen](#)

Die ATM-Netzwerkprozessormodule für die 4x00-Router-Serie verwenden den Befehl **atm scrambling cell payload**, um Payload-Scrambling zu konfigurieren. [CSCds42723](#) löst eine Bedingung auf, in der der Router den Befehl zum Scrambling der Payload entfernt und beim erneuten Laden eine `no-scrambling`-Anweisung in die aktuelle Konfiguration eingibt.

Hinweis: Der standardmäßige Scrambling-Status dieser Module ist `kein Scrambling`.

[Scrambling auf ATM Switch Routern](#)

Die ATM-Switches der Serien LS1010 und Catalyst 8500 unterstützen beide SONET-Scrambling-Modi. Beide Modi sind auf SONET-Schnittstellen standardmäßig aktiviert.

```
ls1010# show controllers atm 12/0/3
```

```
IF Name: ATM12/0/3    Chip Base Address: A8E0E000  
Port type: OC3      Port rate: 155 Mbps    Port medium: SM Fiber  
Port status:Good Signal Loopback:None    Flags:8308  
TX Led: Traffic Pattern  RX Led: Traffic Pattern  
TX clock source: network-derived  
Framing mode: sts-3c  
Cell payload scrambling on  
Sts-stream scrambling on
```

Das Scrambling nach Zellen ist standardmäßig auf DS-3-Schnittstellen deaktiviert und ist standardmäßig für E3-Schnittstellen aktiviert.

Verwenden Sie den Befehl **show controller atm**, um Konfigurationsänderungen an diesen Standardeinstellungen zu bestätigen.

[ATM Scrambling auf Packet Over SONET Links](#)

Packet over SONET (POS)-Schnittstellen unterstützen das Payload-Scrambling im ATM-Stil über

den SPE-Teil eines SONET-Frames, um eine ausreichende Bitübergangsdichte sicherzustellen. Diese Scrambling ist standardmäßig deaktiviert und mit dem Befehl **pos scramble-atm** aktiviert.

```
Router(config)# interface pos 3/0
```

```
Router(config-if)# pos scramble-atm
```

Hinweis: Scrambling ändert den Wert des C2-Bytes im Pfad-Overhead. Die beiden Werte sind **16** für Scrambling aktiviert und **CF** für Scrambling deaktiviert. Bei Verwendung mit ATM over SONET-Links ändert das Scrambling das C2-Byte nicht.

Machen Scrambling ATM-Links sicher?

Zellenverschlüsselung bietet keine Sicherheit. Verwenden Sie diese Methode, um das Datenmuster über eine virtuelle Verbindung zuzusprechen. Für sichere ATM-Verbindungen sollte die Implementierung von Sicherheitsfunktionen auf höherer Ebene oder mithilfe eines Verschlüsselungssystems in Betracht gezogen werden.

Zugehörige Informationen

- [Support-Seiten für ATM \(Asynchroner Transfermodus\)](#)
- [Tools und Dienstprogramme - Cisco Systems](#)
- [Technischer Support - Cisco Systems](#)