Remote Administration

In diesem Kapitel erfahren Sie

- wie sie Cisco Geräte remote administrieren können, d.h. von entfernten Geräte über die Application Layer Protocols telnet und SSH
- was Sie bei Telnet beachten sollten und wie Sie Telnet einrichten bzw. deaktivieren können
- wie SSH grundlegend funktioniert, wie SSH eingerichtet und verwendet wird
- wie mit Remote Sessions in den Hintergrund (der CLI) gesendet und dort verwaltet werden können
- was sie bei Remote Sessions die Logmeldungen des Geräts anzeigen lassen können

vty Lines

Eine erfolgreiche IP Konfiguration ist Voraussetzung für eine remote Konfiguration der Geräte über die TCP/IP Netzinfrastruktur. Für die Nutzung der erforderlichen Dienste auf einem Cisco Gerät (Telnet oder SSH) sind jedoch eine weitere Konfigurationseinstellungen erforderlich.

Remote Login Anfragen (via Telnet oder SSH) werden von einem Cisco Gerät gernerell auf einer virtuellen line verarbeitet, an welche die Anfrage bei Empfang an einer physikalischen Schnittstelle weitergeleitet wird: **line vty.**

Für jede Remote Login Session wird ein eigene virtuelle vty line benötigt (vty 0, vty 1, ..)

Telnet – Teletype Network

Eigenschaften
- Client/Server Dienst zur remote Admistration
- OSI 7 Protokoll.
- Verwendet TCP Port 23 zur Datenübertragung.
- Sämtliche Daten werden in Klartext übertragen.

Zur Verwendung des Telnet **Server** Dienstes, der bereits auf jedem Cisco Gerät aktiv ist, muss der Telnet Zugriff auf das Gerät – im SubConfiguration Mode der line vty - abgesichert werden:
- entweder mit einem Line Password
- oder über ein Benutzer-definiertes Login

Ohne Absicherung wird der Versuch einer Telnet Verbindung zum Gerät nur folgende Fehlermeldung verursachen: "Password required but not set".

Im übergeordneten Kommando zum Wechsel in den SubConfiguration Mode der line vty ist eine Bereichsangabe der vty Nummern möglich.
So können multiple vty lines "auf einmal" identisch konfiguriert werden.
Die Anzahl der konfigurierten vty lines definiert die Anzahl paralleler Telnet Sessions auf das Gerät. Die erste Verbindung wird auf vty 0 verarbeitet.

```
(config)# line vty start-vty-Nr [ end-vty-Nr ]
```

Beispielkonfiguration 1: Identische Konfiguration von 5 VTY Lines (Nr 0 bis 4) für 5 parallele Telnet Verbindungen, Login mit Passwort auf der Line, Automatisches Logout deaktiviert

```
(config)# line vty 0 4
(config-line)# password geheim
(config-line)# login
(config-line)# exec-timeout 0
```

Beispielkonfiguration 2: Identische Konfiguration von 5 VTY Lines (Nr 0 bis 4) für 5 parallele Telnet Verbindungen, benutzer-definiertes Login, Automatisches Logout deaktiviert

```
(config)# username admin secret geheim
(config)# line vty 0 4
(config-line)# login local
(config-line)# exec-timeout 0
```

Nach der Absicherung der vty Lines, kann via Telnet auf das Cisco Gerät zugegriffen werden.
HINWEIS: ohne konfiguriertes enable secret ist ein Wechsel vom UserEXEC Mode in den PrivilegeEXEC Mode via Telnet NICHT möglich.

Telnet Client

Cisco Geräte können nicht nur als Telnet Server arbeiten (Sessions aktzeptieren) – sondern auch als Telent **Clients** (Sessions aufbauen).

Um von einem Cisco Gerät eine Telnet Verbindung zu einem anderen Gerät aufzubauen, können unterschiedliche Kommandos bzw. kein Kommando verwendet werden.
Wenn als Zieladresse anstelle der IP Adresse der Hostname des Zielgeräts angegeben wird, muss eine funktionale Namensauflösung im Netzwerk existieren.

```
# telnet { IP | IPv6 | Hostname }
# connect { IP | IPv6 | Hostname }
# { IP | Hostname }
```

Aktive Telnet Verbindungen können mit **exit** wieder beendet werden.

```
home# telnet remote
remote# exit
home#
```

SSH – Secure Shell

Eigenschaften

- Client/Server Dienst zur remote Admistration und mehr (sftp, scp, ..)
- OSI 7 Protokoll.
- Verwendet TCP Port 22 zur Datenübertragung.
- Sämtliche Daten werden authentifiziert und verschlüsselt übertragen.
  - Zur **Authentifizierung** wird das asymetrische kryptografische Verfahren **RSA** (Rivest, Shamir, Adleman) verwendet. Bei der Authentifizierung des Clients mit Username und Passwort, werden diese Parameter durch den öffentlichen RSA Key des Servers verschlüsselt und können nur durch dessen privaten Schüssel wieder entschlüsselt werden. Um diese Funktionalität zu gewährleisten, sendet der Server bei erster Kontaktaufnahme eines Clients, diesem seinen öffentlichen Schlüssel, der vom Anwender akzeptiert werden muss.
  - Zur **Verschlüsselung** des weiteren Datenverkehrs (Ein- und Ausgaben) wird dann ein symetrisches Verfahren verwendet. Das symetrische Verfahren (DES, 3DES oder meist **AES**) und der entsprechende Schlüssel werden direkt nach der Authentifizierung von den Geräten automatisch ausgehandelt bzw. generiert – dazu wird der **Diffie Hellman Algoritmus** verwendet.

Zur Verwendung des SSH-Dienstes müssen folgenden **Voraussetzungen** bzw. Konfigurationseinstellungen erfüllt sein:

- IOS Image das kryptografische Features unterstützt
  - k9 im Dateinamen oder
  - Ausgabe von show version bzw. Bootmeldung beinhaltet einen Textabschnitte der wie folgt beginnt: "This product contains cryptographic features .."
- Hostname und IP Domain Name sind gesetzt – notwendig für die Generierung des RSA Key Pair
  (config)# **hostname** *name*
  (config)# **ip domain-name** *domain.topleveldomain*
- Benutzer sind angelegt (mindestens einer) und VTY Lines sind mit Benutzerkennung (login local) abgesichert – SSH erfordert ein benutzer-definiertes Login mit Benutername und Passwort.
  (config)# **username** *name* [**privilege 15**] **secret** *passwort*
  (config)# **line vty** 0 4
  (config-line)# **login local**

Um den SSH Dienst auf einem Cisco Gerät zu aktiviern, muss – wenn die Voraussetzungen erfüllt sind – lediglich ein RSA Key Pair (privater und öffentlicher RSA Schlüssel) generiert werden. Dabei sollte die Schlüssellänge (Modulo), die interaktiv abgefragt wird, mindestens 1024 betragen.

(config)# **crypto key generate rsa**

Nach erfolgreicher Generierung des RSA Key Pair wird eine Logmeldung generiert, die die Aktivierung und die Version des SSH Dienstes protokolliert. Falls die SSH Version < 2 ist, sollte sie (falls möglich) aktualisiert werden:

(config)# **ip ssh version 2**

Die Einstellung kann mit folgendem Kommandos überprüft werden:

show ip ssh

Nach vorangegangener Konfiguration ist das Cisco Gerät nun über Telnet **und** SSH erreichbar. ACHTUNG: In der default Einstellung akzeptiert das Gerät remote Verbindungen aller (möglichen) Protokolle.

Mit folgendem Kommando im SubConfiguration Moder der vty Lines kann dieses Verhalten administrativ verändert werden. Dabei werden zulässige Protokolle – durch Leerzeichen getrennt – hintereinander angegeben.
HINWEIS: in realen Umgebungen ist die Verwendung von Telnet meist aus Sicherheitgründen (alle Daten werden im Klartext übertragen) untersagt und nur die Verwendung von SSH zulässig.

```
(config)# line vty 0 4
(config-line)# transport input { protocol1 [ protocol2 .. ] | all | none }
```

Beispiel: Nur Telnet und SSH erlauben

```
(config)# line vty 0 4
(config-line)# transport input telnet ssh
```

Beispiel: Nur SSH erlauben

```
(config)# line vty 0 4
(config-line)# transport input ssh
```

RSA Key Pair Verwaltung
Der generierte öffentliche Schlüssel kann am Bildschirm ausgegeben werden

```
# show crypto key mypubkey rsa
```

Falls ein neues Schlüsselpaar generiert werden soll, muss zuerst das alte gelöscht (ausgenullt) werden – dabei wird auch der SSH Serverdienst auf dem Cisco Gerät wieder deaktiviert.

```
(config)# crypto key zeroize rsa
```

SSH Client

Cisco Geräte können nicht nur als SSH Server arbeiten (Sessions aktzeptieren) – sondern auch als SSH **Clients** (Sessions aufbauen).

Um von einem Cisco Gerät eine SSH Verbindung zu einem anderen Gerät aufzubauen, ist folgendes Kommando zu verwenden:

```
# ssh [ -l username ] { IP | IPv6 | Hostname }
```

HINWEIS: falls der Administrator als bestimmter Benutzer auf dem Gerät arbeitet, d.h. sich über ein benutzer-definiertes Login mit dem Gerät verbunden hat, wird der aktuelle Benutzername beim Aufbau der SSH Verbindung mit dem Zielgerät automatisch auch als Benutzername für die SSH Authentifizierung mitgesendet.

Aktive SSH Verbindungen können mit **exit** wieder beendet werden.

Remote Verbindungen effizient nutzen und verwalten

Telnet und SSH Verbindungen, die von einem Cisco Gerät "X" aufgebaut wurden (Cient Funktion) können mit folgender Tastenkombination in den Hintergrund (der Ein- und Ausgabe) verlagert werden:

Strg+Shift+6 → x (gleichzeitig "Strg+Shift+6", dann "x")

Die Verbindung wird – im Hintergrund - aufrechterhalten, aber Ein- und Ausgabedaten der Verbindung werden nicht mehr auf den Bildschirm geschrieben.
Anstelle dessen beziehen sich Ein- und Ausgaben wieder auf das eigentliche Cisco Gerät "X".

X# **telnet** RouterY
Y# Strg+Shift+6 → x
X#

Die in den Hintergrund verlagerten Remote Sessions können mit folgenden Kommandos verwaltet werden:

X# **show sessions**	zeigt alle im Hintergrund befindlichen Sessions inkl. der Connection Number (conn-nr) mit der unterschiedliche Sessions intern verwaltet werden. Die zuletzt verwendete Session ist mit einem * gekennzeichnet
X# ENTER	reaktiviert die * Session (wieder im Vordergrund)
X# **resume**	
X# **resume** *conn-nr*	reaktiviert die Session mit der entsprechenden Connection Number (wieder im Vordergrund)
X# **disconnect**	terminiert die * Session im Hintergrund
X# **disconnect** *conn-nr*	terminiert die Session mit der entsprechenden Connection Number im Hintergrund

Ob remote Verbindungen zum Cisco Gerät aufgebaut wurden (Server Funktion) und aktiv sind, bzw. welche Benutzer über welche Verbindung auf dem Gerät angemeldet sind, lässt sich mit folgendem Kommando ermitteln:

X# **telnet** Y
Z# **telnet** Y

Y# **show users**

Aktive remote Verbindungen (angemeldeten Benutzer) können terminiert werden.
Die line-nr für das entsprechende Kommando, kann in der ersten Spalte der Ausgabe von show users ermittelt werden (entweder numerischer Wert oder Bezeichnung der Line – z.B. entweder 67 oder vty 0)

Y# **clear line** *line-nr*

Log Meldungen bei remote Verbindungen

Die (wichtigen) Log Meldungen, die ein Cisco Gerät erzeugt, werden im Normalfall nur auf die Console geschrieben (in das Fenster einer Konsolenverbindung).

Im Fenster einer Telnet oder SSH Verbindung – dem Terminal - werden keine Log Meldungen angezeigt.

Dieses Verhalten kann durch ein einfaches "Anschalten" verändert werden. Mit folgendem ausführbaren Kommando im PrivilegeEXEC Mode, wird das "Monitoring" (Logging) für ein Termial aktiviert.

```
# terminal monitor
```

Das Kommando ist nur für die aktuelle Telnet/SSH Session und nur für die Dauer der Session gültig. Bei Ab- und erneutem Aufbau der Session ist das default Verhalten (Monitoring bzw. Logging aus) wieder aktiv.

Mit folgendem Kommando kann die Funktion während der laufenden Session wieder "abgeschaltet" werden.

```
# terminal no monitor
```

Selbstkontrolle – Aufgaben und Übungen

1. Mit welchem einzigen Kommando können Sie ermitteln, ob der SSH Dienst auf einem Cisco Gerät aktiv ist und falls ja, welche Version verwendet wird?

2. Mit welcher Tastenkombination kann eine geöffnete Telnet oder SSH Session in den Hintergrund der Anzeige verlagert werden und mit welchem Kommando lassen sich alle im Hintergrund geöffneten Sessions am Bildschirm anzeigen?

3. Welches Kommando ist für jede remote Telnet/SSH Session auf ein Cisco Gerät notwendig, damit Logmeldungen (inklusive Ausgabe von debug Kommandos) im Fenster der Verbindung dargestellt werden?

4. Notieren Sie das notwendige Kommando im SubConfiguration Moder der VTY Lines um NUR SSH als Übertragunsprotokoll zu erlauben

5. Mit welchem der folgenden Konfigurationskommandos wird SSH aktiviert?

- ○ (config)# ssh activate
- ○ (config)# ip ssh enable
- ○ (config)# ip ssh version 2
- ○ (confg)# crypto key generate rsa

6. Welche der folgenden Einstellungen sind Voraussetzung für die Aktivierung von SSH?

- ☐ (config)# hostname RTA
- ☐ (config)# ip domain name foo.bar
- ☐ (config)# username admin secret cisco
- ☐ (config-line)# password geheim
- ☐ (config-line)# login
- ☐ (config-line)# login local

7. Welche der folgenden Einstellungen sind Voraussetzung für die Nutzung von SSH nach Aktivierung?

- ☐ (config)# hostname RTA
- ☐ (config)# ip domain name foo.bar
- ☐ (config)# username admin secret cisco
- ☐ (config-line)# password geheim
- ☐ (config-line)# login
- ☐ (config-line)# login local

Selbstkontrolle – Lösungen

1. Mit welchem einzigen Kommando können Sie ermitteln, ob der SSH Dienst auf einem Cisco Gerät aktiv ist und falls ja, welche Version verwendet wird?

 # show ip ssh

2. Mit welcher Tastenkombination kann eine geöffnete Telnet oder SSH Session in den Hintergrund der Anzeige verlagert werden und mit welchem Kommando lassen sich alle im Hintergrund geöffneten Sessions am Bildschirm anzeigen?

Strg+Shift+6 → x
 # show sessions

3. Welches Kommando ist für jede remote Telnet/SSH Session auf ein Cisco Gerät notwendig, damit Logmeldungen (inklusive Ausgabe von debug Kommandos) im Fenster der Verbindung dargestellt werden?

 # terminal monitor

4. Notieren Sie das notwendige Kommando im SubConfiguration Moder der VTY Lines um NUR SSH als Übertragunsprotokoll zu erlauben

transport input ssh

5. Mit welchem der folgenden Konfigurationskommandos wird SSH aktiviert?

- O (config)# ssh activate
- O (config)# ip ssh enable
- O (config)# ip ssh version 2
- xO (confg)# crypto key generate rsa

6. Welche der folgenden Einstellungen sind Voraussetzung für die Aktivierung von SSH?

- x☐ (config)# hostname RTA
- x☐ (config)# ip domain name foo.bar
- ☐ (config)# username admin secret cisco
- ☐ (config-line)# password geheim
- ☐ (config-line)# login
- ☐ (config-line)# login local

7. Welche der folgenden Einstellungen sind Voraussetzung für die Nutzung von SSH nach Aktivierung?

- ☐ (config)# hostname RTA
- ☐ (config)# ip domain name foo.bar
- x☐ (config)# username admin secret cisco
- ☐ (config-line)# password geheim
- ☐ (config-line)# login
- x☐ (config-line)# login local