

Syslog

Verschiedenes

- RFC 3164, RFC 5424
- Serverport: UDP 514

Ziele von Syslog-Messages auf Cisco-Gerät

- logging buffer (RAM)
- console line
- terminal line
- Syslog Server

Severity Level (Schwere des Fehlers)

Level	Name	Erklärung	Bedeutung
0	Emergencies	System Unusable	Message about malfunction
1	Alerts	Immediate Action Needed	
2	Critical	Critical Condition	
3	Errors	Error Condition	
4	Warnings	Warning Condition	
5	Notifications	Normal, but Significant Condition	z.B. interface up/down, system restart
6	Information	Informational Message	z.B. booting
7	Debugging	Debugging Message	debug command

Syslog Facility (= Funktion)

IF (interface), IP, OSPF, SYS (Betriebssystem), IPSEC, ...

Message Format

```
*Mär 01, 00:37:41.3737: %SYS-5-CONFIG_I: Configured from console by console
```

```
Mär 01, 00:37:41.3737      Timestamp
SYS                        Sylog reporting facility
5                          Severity level
CONFIG_I                   Mnemonic
Configured from console by console  Description
```

Cisco-Router/Switch als Syslog-Client

```
Router(config)# logging host 1.2.3.4 # IP-Adresse des Servers
Router(config)# logging trap debugging # Alles mit Level ≤ 7 mitloggen
Router(config)# service timestamps log datetime msec # Zeit mitloggen
```