

Fakultät: Fakultät Angewandte Computer- und
Biowissenschaften

DOKUMENTATION

Programmierung I



Dokumentation: **C-Programm zur Analyse von
Cisco-Syslog-Routernachrichten**

Autoren:

Herr Philipp Dellwo (Matrikelnummer 102058)

Frau Melissa Futtig (Matrikelnummer 107813)

Studiengang:

Bachelor of Science IT-Forensik/ Cybercrime

Seminargruppe:

CC24w1-B

Dozent:

Herr Prof. Dirk Pawlaszczyk

Einreichung:

Mittweida, 30.08.2025

Inhaltsverzeichnis

1	Einleitung.....	1
1.1	Zweck des Dokuments/ Aufgabenstellung	1
1.2	Umfang des Programms.....	1
1.3	Zielgruppe.....	2
2	Grundlagen und Analyse	3
2.1	SysLog-Protokoll	3
2.2	Cisco-SysLog-Dateien	4
3	Programmentwurf	6
3.1	Diagramm/ Architektur des Programms	6
3.2	Log-Einträge/ Filterkriterien	7
3.3	Ausgabeformatierung	10
4	Implementierung und Einrichtung	13
4.4	Entwicklungsumgebung und Code-Struktur	13
4.1	Schritte zur Einrichtung.....	14
4.2	Bedienung.....	15
5	Fazit.....	17
5.1	Zusammenfassung.....	17
5.2	Limitationen.....	17

Abbildungsverzeichnis

Abbildung 1 Programmübersicht (eigene Darstellung).....	6
Abbildung 2 Hauptmenü	7
Abbildung 3 Eigene Suchbegriff-Suche.....	7
Abbildung 4 Zeitraum Verzeichnis	8
Abbildung 5 IP-Suche Verzeichnis	8
Abbildung 6 Facility-Suche Verzeichnis	9
Abbildung 7 User-Suche Verzeichnis	9
Abbildung 8 Mnemonic-Suche Verzeichnis.....	9
Abbildung 9 Severity Level Verzeichnis	10
Abbildung 10 Screenshot der Datei syslog_generic.log.....	10
Abbildung 11 Zusammenfassende Darstellung der gefundenen Logs	10
Abbildung 13 Warnhinweis (gelber Schriftzug)	11
Abbildung 14 Ausgabe Fehlermeldung	11
Abbildung 15 Fragestellung Suchergebnisspeicherung	12
Abbildung 16 Bestätigung der Suchergebnisspeicherung	12
Abbildung 17 Suchbegriff-Datei Logergebnisse.....	12
Abbildung 18 Funktion zurück in das Hauptmenü	12
Abbildung 19 Code-Struktur	13
Abbildung 20 Dashboard vor der Logdatei-Eingabe	15
Abbildung 21 Funktion „exit“	15
Abbildung 22 Hauptmenü nach der Logdatei-Eingabe.....	16
Abbildung 23 Cisco-Logdatei, Name: syslog1.log.....	VIII
Abbildung 24 Cisco-Logdatei, Name: syslog2.log.....	IX
Abbildung 25 Cisco-Logdatei, Name: syslog_generic.log.....	XI

1 Einleitung

1.1 Zweck des Dokuments/ Aufgabenstellung

Die vorliegende Belegarbeit wird im Rahmen des Moduls „Programmierung I“ des Studiengangs Bachelor of Science IT-Forensik/Cybercrime, Seminargruppe CC24w1-B, erstellt.

Das Ziel ist die Erstellung, die erfolgreiche Implementierung, die Kompilierung sowie die Dokumentation eines Kommandozeilenprogramms, das in der Programmiersprache „C“ geschrieben wird. Das Programm soll ausschließlich die Analyse von Cisco-SysLog-Router-Dateien ermöglichen.

Zunächst ist zu erwähnen, dass keine formalen Vorgaben zu den funktionalen Anforderungen des Programms oder zur Dokumentation in Schriftform vorliegen.

Dennoch soll es die Auswertung bestimmter Informationen aus den Log-Dateien wie IP-Adressen, Zeitstempel und Ereignisbeschreibungen ermöglichen. Die gewonnenen Ergebnisse sollen in einer Datei gespeichert werden können.

1.2 Umfang des Programms

In diesem Dokument wird sich mit einem Kommandozeilenprogramm befasst, das in der Sprache „C“ implementiert wird und keine grafische Benutzeroberfläche (GUI) benötigt.

Es ist darauf ausgelegt, Cisco-SysLog-Router-Dateien einzulesen und deren Inhalt zu parsen.

Das Programm enthält eine breite Palette an Filtermöglichkeiten, die es dem Nutzer ermöglichen, die Log-Einträge zum einen nach verschiedenen Kriterien zu durchsuchen und zum anderen einzugrenzen. Zudem sollen diese in einer Datei gespeichert werden.

Folgende Suchfunktionen sind implementiert:

- Eigene inhaltliche Suche (`eigenerSuchbegriff()`)
- Zeitbereichsuche (`zeitraum()`)
- IP-Adresssuche (`ipSuche()`, `ipFilterSucheEinfach()`)

- Facility Suche (facilitySuche(), eigeneFacilitySuche())
- Benutzersuche (userSuche(), eigeneUserSuche())
- Mnemonic Suche (mnemonicSuche(), eigeneMnemonicSuche())
- Severity Level Suche (severityLevel())

1.3 Zielgruppe

Zielgruppe dieses Projektes sind Personen mit einem praktischen Verständnis für die Programmierung von Analyse-Tools. Des Weiteren richtet sich das Programm an mögliche Netzwerkadministratoren sowie IT-Forensiker, die im Rahmen ihrer Tätigkeit Cisco Router SysLog-Dateien auswerten.

Zudem soll das Programm einen Mehrwert für die Studierenden des Studiengangs „IT Forensik/Cybercrime“ darstellen.

2 Grundlagen und Analyse

2.1 SysLog-Protokoll

Das Syslog-Protokoll ist ein Verfahren zur Übermittlung von System- und Ereignismeldungen in Rechnernetzen und wurde ursprünglich in den 1980er Jahren im Rahmen des Sendmail-Projekts auf BSD-Unix entwickelt [1]. Es wird von einer Vielzahl von Betriebssystemen, Netzwerkkomponenten und Anwendungen unterstützt und ist im Bereich der Ereignisprotokollierung weit verbreitet [2].

Syslog wird in der Praxis vor allem für drei Aufgaben eingesetzt: Das zentrale Monitoring von Netzwerken und Systemen, die Fehlerdiagnose durch Sammlung und Auswertung von Ereignismeldungen und die IT-Sicherheitsüberwachung, etwa durch Korrelationsanalysen in Security-Information-and-Event-Management (SIEM)-Systemen [3].

Die Standardisierung des Protokolls erfolgt durch das Dokument RFC 5424 der Internet Engineering Task Force, das das ältere RFC 3164 ersetzt. Das RFC 5424 definiert den Nachrichtenaufbau, die zulässigen Felder sowie die Prioritäts- und Schweregrade [4]. Während RFC 5424 das Nachrichtenformat spezifiziert, beschreiben RFC 5426 (UDP) und RFC 5425 (TLS) die möglichen Transportvarianten [4] [5] [6].

Eine Syslog-Nachricht nach RFC 5424 setzt sich aus den vier folgenden logischen Komponenten zusammen: Die PRI (Priority) enthält die Priorität der Nachricht, gebildet aus der Kombination von Facility (Herkunft des Ereignisses, z. B. Kernel, Mail-System, Authentifizierung) und dem Severity-Level. Der Header enthält unter anderem Versionsnummer, Zeitstempel, Hostname, Applikationsname und Prozess-ID. Die Structured Data beinhalten optionale strukturierte Zusatzinformationen in standardisiertem Format. In der letzten Komponente, MSG, steht der eigentliche Nachrichtentext.

Cisco-Router erzeugen Systemmeldungen im Syslog-kompatiblen Format und können diese an zentrale Syslog-Server weiterleiten [7]. Damit zeigen herstellerspezifische Implementierungen, dass sie auf dem Syslog-Standard aufbauen und so eine einheitliche Ereignisprotokollierung ermöglichen.

Auf den Aufbau von Cisco-Router-Logdateien wird nachfolgend eingegangen.

2.2 Cisco-SysLog-Dateien

Cisco-SysLog-Dateien sind Protokolldateien, die in diesem Fall von Cisco-Netzwerkgeräten, wie beispielsweise Routern oder Switches, automatisch erstellt werden. Diese enthalten meist zeitlich geordnete Systemmeldungen, Ereignisse, Warnungen und Fehler, die im Gesamten bestimmte Aktionen von Prozessen eines Computersystems dokumentieren [4] [7].

Nachfolgend wird beispielhaft jeweils die erste Logging-Nachricht aus den hier zu untersuchenden Cisco-Syslog-Dateien betrachtet:

Cisco-Logdatei, Name: syslog_generic.log:

```
<189>: Sep 27 2023 10:15:30.1234 UTC: %SYS-5-CONFIG_I: Configured from console by admin on Router-1
```

Cisco-Logdatei, Name: syslog1.log:

```
*Sep 14 06:04:55.610: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/8, changed state to down
```

Cisco-Logdatei, Name: syslog2.log:

```
*Mar 1 2023 08:00:00.000: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
```

Eine Cisco-IOS-Syslog-Nachricht gliedert sich grob in fünf Bereiche: Zeitstempel, Facility, Severity Level, Mnemonic und der allgemeinen Beschreibung [8].

Der Zeitstempel wird folgendermaßen dargestellt: „*Sep 14 06:04:55.610“. Dieser gibt das Datum und die genaue Uhrzeit des jeweiligen Ereignisses an. Dabei besteht die Möglichkeit, dass die Nachricht anstatt mit einem „*“, mit einer Zahl in spitzen Klammern

beginnt. Ein Beispiel hierfür ist: „<189>:“. Der genannte Zeitstempel bedeutet, dass am 14. September um 06:04 Uhr und 55.610 Sekunden ein Ereignis stattgefunden hat [9].

Die Facility gibt die Subsystem- oder Prozessbezeichnung an, aus der die Nachricht stammt. Es ist eine Art der internen Absendererkennung. In diesem Zusammenhang zeigt „%LINEPROTO“ das momentane Line Protocol Subsystem an. Das Konzept der Facilities stammt ursprünglich aus UNIX-Systemen. Cisco hingegen verwendet eigene Bezeichnungen wie beispielsweise LINEPROTO, LINK und KERNEL, die auf die jeweiligen internen Module beziehungsweise Prozesse verweisen [9].

Die zusätzlich enthaltenen Severity Level sind sogenannte Schweregrade, die bei Cisco standardisiert von 0 bis 7 geordnet werden. Dabei stellt die niedrigste Zahl die höchste Dringlichkeit dar. Folgende Beschreibungen treffen auf die unterschiedlichen Zahlen zu:

- 0 – *Emergencies*: Das System ist unbrauchbar
- 1 – *Alerts*: Sofortiges Eingreifen erforderlich
- 2 – *Criticals*: Kritische Zustände
- 3 – *Error*: Fehlerhafte Bedingungen/ Zustände
- 4 – *Warning*: Warnmeldungen
- 5 – *Notification*: Normale, aber wichtige Meldungen
- 6 – *Informational*: Informative Meldungen
- 7 – *Debugging*: Debugging-Meldungen, die typischerweise nur temporär verwendet werden, da sie sehr viele Logs generieren können und die Systemleistung beeinträchtigen können [10].

Mnemonics, wie zum Beispiel CONFIG_I oder UPDOWN, sind kurze Bezeichner, die den eigentlichen Inhalt der Meldung beschreiben. Sie sind Schlüsselwörter, die die Art des Ereignisses darstellen und sich an die Severity Levels anlehnen [9].

3 Programmentwurf

3.1 Diagramm/ Architektur des Programms

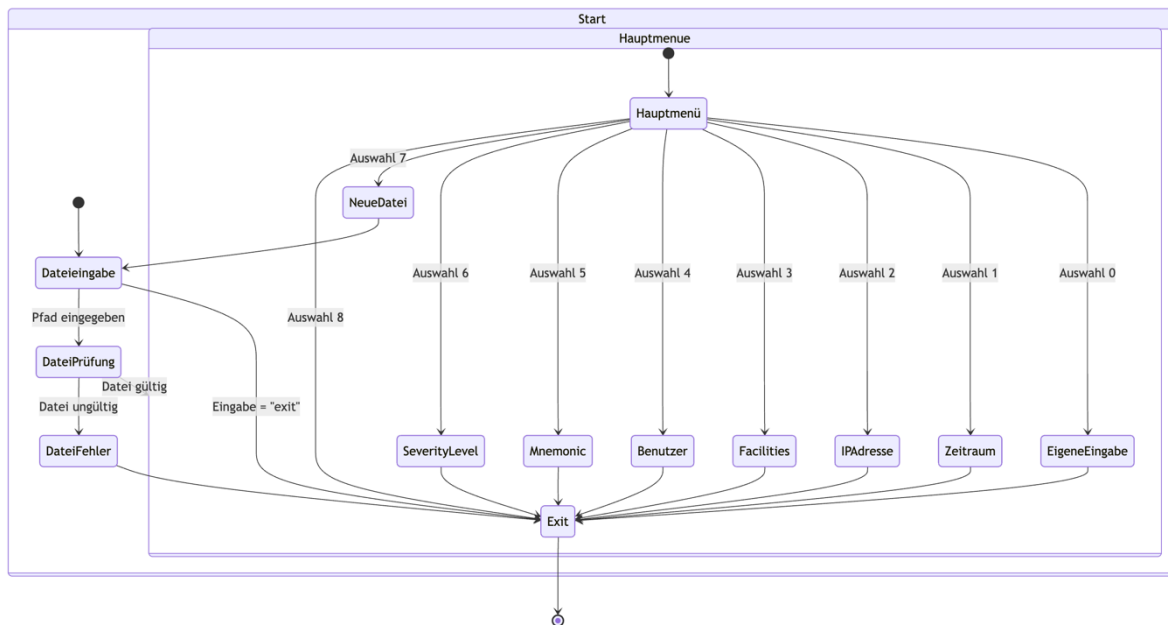


Abbildung 1 Programmübersicht (eigene Darstellung)

Das in Abbildung 1 dargestellte Diagramm stellt eine grobe Programmübersicht dar. Dabei werden die Funktionen des Programms in einem Zustandsdiagramm veranschaulicht.

Der Nutzer muss zu Beginn das Programm initialisieren und seinen Dateipfad eingeben. Daraufhin erfolgt die Prüfung nach einer gültigen Datei. Ist diese nicht gültig, gibt der Nutzer erneut den Dateipfad ein, bis dieser korrekt ist. Das Programm beendet sich automatisch, sobald der Nutzer dreimal eine falsche Eingabe tätigt. Ist der Dateipfad korrekt, wird der Nutzer in das Hauptmenü geleitet und kann sich eine der dort gelisteten Optionen aussuchen. Zusätzlich hat er immer die Möglichkeit, das Programm zu beenden und neu zu starten.

3.2 Log-Einträge/ Filterkriterien

Nachfolgend werden die Log-Einträge beziehungsweise Filterkriterien erläutert.

Abbildung 2 zeigt das Hauptmenü, das das erste Abfrageverzeichnis darstellt. Dort werden alle Such-/Filtermöglichkeiten des Programms aufgelistet. Der Nutzer hat die Möglichkeit, über eine der vor den Begriffen stehenden Ziffern auszuwählen, um in den jeweiligen Filtermodus zu gelangen. Wird keine Zahl zwischen 0 und 8 eingegeben, sondern ein Buchstabe oder ein anderes Zeichen, erhält der Nutzer eine Fehlermeldung. Auf dieses Thema wird im Rahmen der Ausgabenformatierung detaillierter eingegangen.

```
Bitte wählen Sie einen Suchbegriff aus:
0: Eigene Eingabe
1: Zeitraum
2: IP-Adresse
3: Facilities
4: User
5: Mnemonic
6: Severity Level
7: Neue Datei auswählen
8: Programm beenden

Auswahl (0-8):
```

Abbildung 2 Hauptmenü

Anschließend ist zu erwähnen, dass durch den Benutzer, wie in Abbildung 3, über „Eigene Eingabe“ ein beliebiger Suchbegriff eingegeben werden kann, bei dem nicht zwischen Groß- und Kleinschreibung unterschieden wird. Das Programm durchsucht die gesamte Logdatei nach dem Vorkommen des eingegebenen Begriffs und gibt die entsprechenden Zeilen aus. Auch hier prüft das Programm, ob der Nutzer wirklich einen Inhalt eingibt oder ob er nur mit der Enter-Taste eine leere Eingabe tätigt. Tritt letzteres auf, wirft das Programm einen Fehler aus und bittet den Nutzer, die Eingabe zu wiederholen.

```
Bitte geben Sie einen beliebigen Suchbegriff ein:
```

Abbildung 3 Eigene Suchbegriff-Suche

Weiterhin ist es möglich, mit dem Zeitraumfilter die Logeinträge zeitlich einzugrenzen (siehe Abbildung 4). Zur Verfügung stehen die Optionen „Meldungen ab einem bestimmten Zeitpunkt“, „Bis zu einem Zeitpunkt“ oder „Zeitraum zwischen der ersten und zweiten Zeit“. Dies erleichtert die Analyse von Ereignissen, die zu einem konkreten Zeitpunkt aufgetreten sind. In diesem Verzeichnis wählt der Nutzer erneut eine der ersten

drei Ziffern aus und gibt im Anschluss die entsprechenden Zeiten ein. Es muss zuerst der Tag (DD), dann der Monat (MMM), das eventuell vorhandene Jahr (YYYY) und zum Schluss die genaue Uhrzeit (HH:MM:SS) eingegeben werden. Falls eine Logdatei kein Jahr enthält, wird dem Nutzer während der Abfrage diese Information mitgeteilt, sodass eine Eingabe nicht erforderlich ist.

```
Wie wollen Sie die Logs betrachten?  
1: Ab der ersten eingegebenen Zeit.  
2: Bis zur ersten eingegebenen Zeit.  
3: Zeitraum zwischen der ersten und zweiten Zeit.  
4: Zurück ins Hauptmenü  
5: Programm beenden.  
  
Auswahl (1-5):
```

Abbildung 4 Zeitraum Verzeichnis

Außerdem wurde, wie in Abbildung 5 eine IP-Adresssuche implementiert, die mehrere Varianten bietet: Der Benutzer kann eine bestimmte IPv4-Adresse manuell eingeben oder automatisch nach privaten bzw. öffentlichen IP-Adressen filtern. Entscheidet sich der Nutzer für die erste Option, muss er eine beliebige IP-Adresse eingeben. Hierbei prüft das Programm besonders die Art der Schreibweise. Gültig sind ausschließlich IPv4-Adressen. Da die Logdateien (Cisco-Logdatei, Name: syslog1.logCisco-Logdatei, Name: syslog2.log, Cisco-Logdatei, Name: syslog_generic.log) keine IPv6-Adressen beinhalten, wurde diesbezüglich keine Filteroption erstellt.

```
Bitte wählen Sie die Art der IP-Suche:  
1: Manuelle Eingabe einer IP-Adresse  
2: Nur private IP-Adressen anzeigen  
3: Nur öffentliche IP-Adressen anzeigen  
4: Zurück in das Hauptmenü  
5: Programm beenden  
  
Auswahl (1-5):
```

Abbildung 5 IP-Suche Verzeichnis

Über den Facility-Filter wie in Abbildung 6 kann nach dem Subsystem gesucht werden, aus dem die Meldung stammt (z. B. LINK, STP, DHCP). Hier ist sowohl eine manuelle Eingabe eines Facility-Namens als auch die Auswahl aus allen in der entsprechenden Datei befindlichen Facilities möglich. Entscheidet sich der Nutzer für die zweite Option, werden ihm zu Beginn alle existierenden Facilities angezeigt. Dabei legt das Programm den Fokus darauf, ob sich die Facilities tatsächlich in der Logdatei befinden. Im Anschluss

werden alle verfügbaren Logs angezeigt, aus denen der Nutzer auswählen kann. Schließlich wird das Suchergebnis angezeigt.

```
Bitte wählen Sie die Art der Facility-Suche:
1: Eigene Suche nach Facility-Begriff
2: Alle vorhandenen Facilities anzeigen und auswählen
3: Zurück in das Hauptmenü
4: Programm beenden

Auswahl (1-4):
```

Abbildung 6 Facility-Suche Verzeichnis

In Abbildung 7 ist ersichtlich, dass die Möglichkeit besteht, nach Benutzernamen (User) zu filtern. Dabei unterstützt das Programm sowohl die direkte Eingabe eines Namens als auch die Anzeige aller in der Logdatei enthaltenen Benutzer mit anschließender Auswahl. Auf diese Weise lassen sich Aktivitäten bestimmter Benutzer nachvollziehen.

```
Bitte wählen Sie die Art der User-Suche:
1: Eigene Suche nach User
2: Alle User anzeigen und auswählen
3: Zurück in das Hauptmenü
4: Programm beenden

Auswahl (1-4):
```

Abbildung 7 User-Suche Verzeichnis

Das Mnemonic-Filterkriterium aus Abbildung 8 ermöglicht die Suche nach den Kennungen für Ereignisse wie beispielsweise CONFIG_I oder UPDOWN. Analog zur Facility-Suche und der Suche nach Usern ist eine freie Eingabe und die Auswahl aus allen in der Log-Datei enthaltenen Mnemonics möglich.

```
Bitte wählen Sie die Art der Mnemonic-Suche:
1: Eigene Suche nach Mnemonic
2: Alle vorhandenen Mnemonics anzeigen und auswählen
3: Zurück in das Hauptmenü
4: Programm beenden

Auswahl (1-4):
```

Abbildung 8 Mnemonic-Suche Verzeichnis

Wie in Kapitel 2.2 Cisco-SysLog-Dateien bereits erwähnt, sind Severity Level sogenannte Schweregrade, die bei Cisco standardisiert von 0 bis 7 geordnet werden. Im Programm hat der Nutzer die Möglichkeit, wie in Abbildung 9 sichtbar, eines der Severity Levels auszuwählen und alle Logzeilen anzeigen zu lassen, die dieses enthalten.

```

Bitte wählen Sie ein Severity Level aus.

0: EMERGENCIES - Ein System ist unbenutzbar
1: ALERTS - Sofortiges Handeln erforderlich
2: CRITICALS - Kritische Zustände
3: ERRORS - Errorwarnungen
4: WARNINGS - Warnhinweise
5: NOTIFICATIONS - Normale, aber signifikante Zustände
6: INFORMATIONAL - Informierende Nachrichten/Logs
7: DEBUGGING - Debugging Nachrichten/Logs
8: Zurück in das Hauptmenü
9: Programm beenden

Auswahl (0-9):

```

Abbildung 9 Severity Level Verzeichnis

3.3 Ausgabeformatierung

3.3.1 Logergebnis-Ausgabe

Die Ausgabe der Ergebnisse erfolgt über die Konsole. Jeder gefundene Logeintrag wird wie in Abbildung 10 in seiner ursprünglichen Form dargestellt und zusätzlich mit der entsprechenden Zeilennummer versehen. Dies ermöglicht eine Nachvollziehbarkeit innerhalb der ursprünglichen Logdatei.

```

Zeile 2: <184>: Sep 27 2023 10:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
Zeile 7: <184>: Sep 27 2023 11:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to down
Zeile 12: <184>: Sep 27 2023 12:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/3, changed state to up
Zeile 17: <184>: Sep 27 2023 13:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/4, changed state to down
Zeile 22: <184>: Sep 27 2023 14:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/5, changed state to up
Zeile 27: <184>: Sep 27 2023 15:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/6, changed state to up
Zeile 32: <184>: Sep 27 2023 16:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/7, changed state to down
Zeile 37: <184>: Sep 27 2023 17:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/8, changed state to up
Zeile 42: <184>: Sep 27 2023 18:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/9, changed state to down
Zeile 47: <184>: Sep 27 2023 19:16:45.6789 UTC: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
Zeile 52: <184>: Sep 27 2023 20:16:45.6789 UTC: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to down
Zeile 57: <184>: Sep 27 2023 21:16:45.6789 UTC: %LINK-3-UPDOWN: Interface Serial0/0/1, changed state to up
Zeile 62: <184>: Sep 27 2023 22:16:45.6789 UTC: %LINK-3-UPDOWN: Interface Serial0/0/2, changed state to down
Zeile 67: <184>: Sep 27 2023 23:16:45.6789 UTC: %LINK-3-UPDOWN: Interface Serial0/0/3, changed state to up
Zeile 72: <184>: Sep 27 2023 00:16:45.6789 UTC: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to down
Zeile 77: <184>: Sep 27 2023 01:16:45.6789 UTC: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to up
Zeile 82: <184>: Sep 27 2023 02:16:45.6789 UTC: %LINK-3-UPDOWN: Interface FastEthernet0/4, changed state to down
Zeile 87: <184>: Sep 27 2023 03:16:45.6789 UTC: %LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to up
Zeile 92: <184>: Sep 27 2023 04:16:45.6789 UTC: %LINK-3-UPDOWN: Interface FastEthernet0/6, changed state to down

```

Abbildung 10 Screenshot der Datei syslog_generic.log

Nach Abschluss einer Suche erfolgt eine zusammenfassende Darstellung. Dabei wird entweder die Gesamtzahl der gefundenen Treffer angegeben oder es wird explizit darauf hingewiesen, dass keine passenden Logeinträge vorhanden sind (siehe Abbildung 12 und Abbildung 13). Auf diese Weise wird der Benutzer über das Ergebnis der jeweiligen Suche oder Filterung informiert.

```

In der analysierten Log-Datei wurden 19 Logs für Facility 'LINK' gefunden.

```

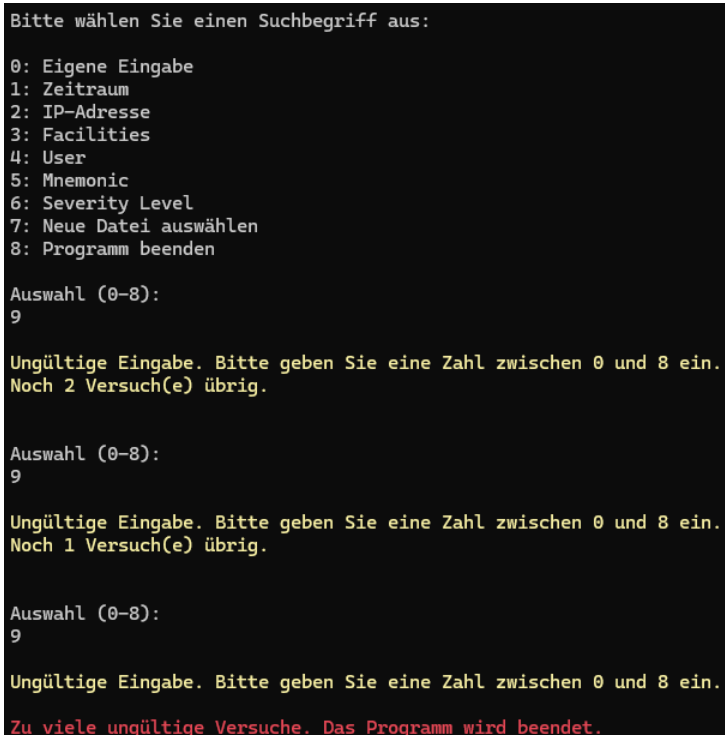
Abbildung 11 Zusammenfassende Darstellung der gefundenen Logs



Abbildung 12 Warnhinweis (gelber Schriftzug)

3.3.2 Warnungen und kritische Fehlermeldungen

Bei fehlerhaften Eingaben gibt das Programm entsprechende Rückmeldungen an den Nutzer. Warnungen werden dabei in gelber Schrift in der Konsole dargestellt und machen auf ungültige oder unvollständige Eingaben aufmerksam. Kritische Fehlermeldungen erscheinen hingegen in roter Schrift. In diesem Fall wird das Programm automatisch beendet und muss neu gestartet werden (siehe Abbildung 13). Die farbliche Kennzeichnung trägt zur besseren Lesbarkeit bei und verdeutlicht die Bedeutung der jeweiligen Meldungen.



```
Bitte wählen Sie einen Suchbegriff aus:
0: Eigene Eingabe
1: Zeitraum
2: IP-Adresse
3: Facilities
4: User
5: Mnemonic
6: Severity Level
7: Neue Datei auswählen
8: Programm beenden

Auswahl (0-8):
9

Ungültige Eingabe. Bitte geben Sie eine Zahl zwischen 0 und 8 ein.
Noch 2 Versuch(e) übrig.

Auswahl (0-8):
9

Ungültige Eingabe. Bitte geben Sie eine Zahl zwischen 0 und 8 ein.
Noch 1 Versuch(e) übrig.

Auswahl (0-8):
9

Ungültige Eingabe. Bitte geben Sie eine Zahl zwischen 0 und 8 ein.
Zu viele ungültige Versuche. Das Programm wird beendet.
```

Abbildung 13 Ausgabe Fehlermeldung

Normale Meldungen und die Ausgabe der Kommunikation verbleiben in der Standardfarbe. Die Ausgabe der Logs erscheint in grüner Schrift (Abbildung 11). Die farbliche Differenzierung erleichtert eine schnelle visuelle Einordnung und Bewertung der Ergebnisse, sodass der Nutzer Fehler sofort erkennt.

3.3.3 Logergebnis-Speicherung

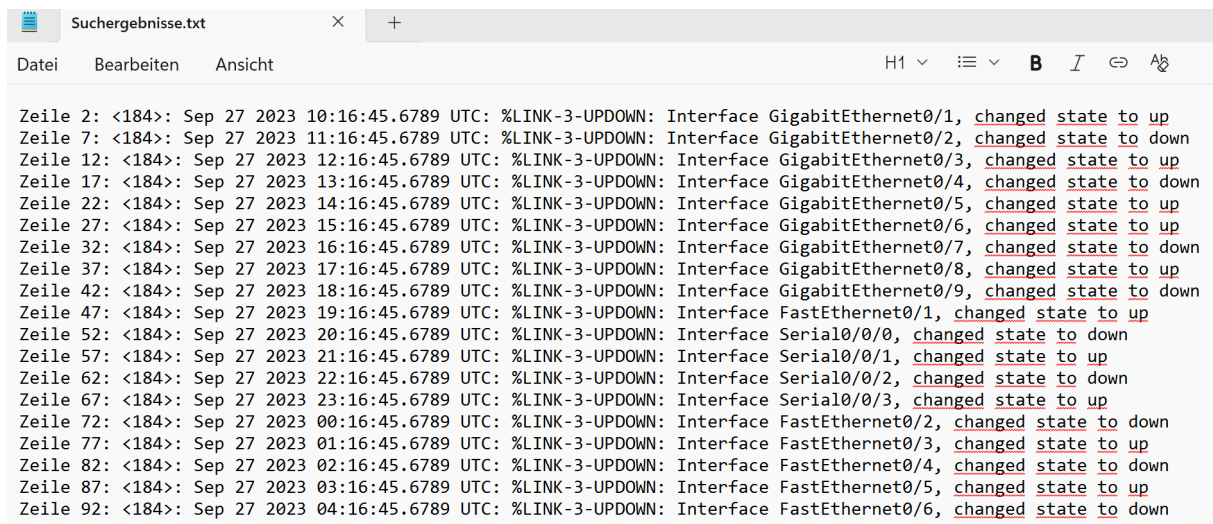
Darüber hinaus besteht die Möglichkeit, die Ergebnisse in einer Ausgabedatei (Suchergebnisse.txt) zu speichern. Die Treffer werden dort im gleichen Format wie in der Konsole gespeichert (siehe Abbildungen 14, 15 und 16).

```
Möchten Sie die Ergebnisse in einer Datei speichern? (j/n):
j
```

Abbildung 14 Fragestellung Suchergebnisspeicherung

```
Die Ergebnisse wurden in der 'Suchergebnisse.txt' Datei gespeichert.
```

Abbildung 15 Bestätigung der Suchergebnisspeicherung



```
Suchergebnisse.txt
Datei  Bearbeiten  Ansicht  H1  ≡  B  I  ↶  ↷

Zeile 2: <184>: Sep 27 2023 10:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
Zeile 7: <184>: Sep 27 2023 11:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to down
Zeile 12: <184>: Sep 27 2023 12:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/3, changed state to up
Zeile 17: <184>: Sep 27 2023 13:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/4, changed state to down
Zeile 22: <184>: Sep 27 2023 14:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/5, changed state to up
Zeile 27: <184>: Sep 27 2023 15:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/6, changed state to up
Zeile 32: <184>: Sep 27 2023 16:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/7, changed state to down
Zeile 37: <184>: Sep 27 2023 17:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/8, changed state to up
Zeile 42: <184>: Sep 27 2023 18:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/9, changed state to down
Zeile 47: <184>: Sep 27 2023 19:16:45.6789 UTC: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
Zeile 52: <184>: Sep 27 2023 20:16:45.6789 UTC: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to down
Zeile 57: <184>: Sep 27 2023 21:16:45.6789 UTC: %LINK-3-UPDOWN: Interface Serial0/0/1, changed state to up
Zeile 62: <184>: Sep 27 2023 22:16:45.6789 UTC: %LINK-3-UPDOWN: Interface Serial0/0/2, changed state to down
Zeile 67: <184>: Sep 27 2023 23:16:45.6789 UTC: %LINK-3-UPDOWN: Interface Serial0/0/3, changed state to up
Zeile 72: <184>: Sep 27 2023 00:16:45.6789 UTC: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to down
Zeile 77: <184>: Sep 27 2023 01:16:45.6789 UTC: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to up
Zeile 82: <184>: Sep 27 2023 02:16:45.6789 UTC: %LINK-3-UPDOWN: Interface FastEthernet0/4, changed state to down
Zeile 87: <184>: Sep 27 2023 03:16:45.6789 UTC: %LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to up
Zeile 92: <184>: Sep 27 2023 04:16:45.6789 UTC: %LINK-3-UPDOWN: Interface FastEthernet0/6, changed state to down
```

Abbildung 16 Suchbegriff-Datei Logergebnisse

3.3.4 Rückkehr in das Hauptmenü

Nach jeder Suche und Filterung wird der Benutzer zudem aufgefordert, über das weitere Vorgehen zu entscheiden. Dabei kann die Suche wiederholt, in das Hauptmenü zurückgekehrt oder das Programm beendet werden (siehe Abbildung 17).

```
Was möchten Sie tun?

1: Suche wiederholen
2: Zurück ins Hauptmenü
3: Programm beenden

Auswahl (1-3):
```

Abbildung 17 Funktion zurück in das Hauptmenü

4 Implementierung und Einrichtung

4.4 Entwicklungsumgebung und Code-Struktur

Eine Entwicklungsumgebung wird in englischer Sprache auch als Integrated Development Environment (IDE) bezeichnet. Diese ist ein Werkzeug der Softwareentwicklung, in der der Quellcode eines zukünftigen Programms verfasst wird. Die hier genutzte Umgebung ist Visual Studio Code (VSC). Grund dafür sind die unterstützenden Plug-Ins, die zur Kompilierung und Fehlererkennung während der Entwicklung nützlich sind. Durch die Nutzung von VSC lässt sich der Code übersichtlich darstellen und eine gute Struktur erkennen [11] [12].

Abbildung 18 verdeutlicht den blockweisen Aufbau.

```
| — Bibliotheken
| — _CRT_SECURE_NO_WARNINGS
| — <stdio.h>
| — ...
| — Farbcodes
| — RED
| — YELLOW
| — RESET
| — Plattformdefinition
| — _WIN32
| — strcasecmp_stricmp
| — Variablendeklaration
| — FILE* datei
| — int stunde
| — ...
| — Funktionendefinition
| — void hauptmenue
| — ...
| — Methodendeklaration
| — int exitEingabe
| — ...
| — Main-Methode
```

Abbildung 18 Code-Struktur

Bereits in Abbildung 1 wird der Aufbau des Codes veranschaulicht. Zu Beginn wurden die benötigten Bibliotheken eingefügt. Anschließend erfolgte die Variablendeklaration.

Sodann erfolgt die Funktions- und Methodendefinition, die das eigentliche Herzstück des Programms darstellen. In diesem Programm stellen diese beispielsweise die Filter- und Suchfunktionen dar.

Abschließend wird die Main-Methode implementiert, die den Einstiegspunkt des Programms darstellt, das Programm startet und die Variablen sowie die Funktionen und Methoden nutzt.

Das Programm umfasst eine Größe von 90 KB und 2090 Code-Zeilen.

4.1 Schritte zur Einrichtung

Die Einrichtung des Programms muss in mehreren aufeinanderfolgenden Schritten erfolgen. Zu Beginn muss ein entsprechender Compiler installiert werden, der den Quellcode des Programms, der in Form einer .c-Datei vorliegt, auf dem jeweiligen Betriebssystem kompilieren kann. Im Anschluss wird die Kompilierung über die Kommandozeile mit dem Befehl `gcc -o main.c` durchgeführt, die eine ausführbare Datei mit dem Namen „main“ erzeugt. Vor der Ausführung der erzeugten Datei ist sicherzustellen, dass auf die zu untersuchende .log-Datei zugegriffen werden kann. Das Programm kann dann ebenfalls in der Kommandozeile mit dem Befehl `main` (Windows) bzw. `./main` (macOS) ausgeführt werden.

Damit das Programm auf Windows-Systemen problemlos ausgeführt werden kann, müssen folgende Code-Zeilen eingefügt werden:

- `#define _CRT_SECURE_NO_WARNINGS`: Diese Präprozessor-Direktive unterdrückt Warnungen in der Entwicklungsumgebung Microsoft Visual Studio, die als zu „unsicher“ gelten könnten. Dabei sind Beispiele „scanf“ und/ oder „strcpy“.
- `#ifdef _WIN32 #define strcasecmp _stricmp #endif`: Diese Makro-Definition sorgt dafür, dass der Funktionsname „strcasecmp“, der in Windows nicht existiert, durch „_stricmp“ ersetzt wird. Auf macOS bzw. den UNIX-Systemen ist „strcasecmp“ standardmäßig implementiert. Die Funktion beschreibt den Vergleich von zwei Zeichenfolgen [13].
- `#ifdef _WIN32 system(„cls“); ,else system(“clear”);`: Hierbei wird geprüft, ob der Code unter Windows läuft und wenn ja, wird die Konsole geleert. Wenn der Code unter einem anderen Betriebssystem läuft, wird mit dem anderen Befehl die Kommandozeilenhistory gelöscht. Für macOS (und Linux) wird für die Funktionsfähigkeit kein weiterer Code benötigt. Alle Standardbibliotheken sind bereits kompatibel. Auch die „strcasecmp“-Funktion ist wie bereits erwähnt auf macOS/ UNIX vorhanden, sodass eine Umleitung nicht notwendig ist.

- SetConsoleOutputCP(CP_UTF8): Diese Funktion stellt die Ausgabe der Windows-Konsole auf UTF-8 um, damit Sonder- und Unicode-Zeichen korrekt dargestellt werden. Gleichzeitig muss die Bibliothek <windows.h> eingefügt werden.

4.2 Bedienung

Im folgenden Abschnitt wird auf die konkreten Bedienungsmöglichkeiten des Programms eingegangen. Nach dem Start des Programms wird der Benutzer zunächst aufgefordert, den Pfad zu der Datei mit der Endung .log einzugeben, in der später gesucht oder gefiltert werden soll (siehe Abbildung 19).

```
#####
Auswertungsprogramm für CISCO-Logdateien
#####

Hinweise: Das Programm kann jederzeit mit der Eingabe von 'exit' beendet werden.
Alle Eingaben müssen mit der Enter-Taste bestätigt werden.

Bitte geben Sie den Dateipfad ein (.log-Datei):
```

Abbildung 19 Dashboard vor der Logdatei-Eingabe

Der Nutzer hat im gesamten Programm, unabhängig von der Eingabe, die Möglichkeit, mit dem Befehl “exit“ das Programm und seine Eingabe zu beenden (siehe Abbildung 20). Vertippt sich der Nutzer, erhält er eine Warnung und kann eine korrigierte Version eingeben.

```
Bitte wählen Sie einen Suchbegriff aus:

0: Eigene Eingabe
1: Zeitraum
2: IP-Adresse
3: Facilities
4: User
5: Mnemonic
6: Severity Level
7: Neue Datei auswählen
8: Programm beenden

Auswahl (0-8):
exit

Programm wird beendet.

C: .exe (Prozess "46944") wurde mit Code "0" (0x0) beendet.
Drücken Sie eine beliebige Taste, um dieses Fenster zu schließen.
```

Abbildung 20 Funktion „exit“

Wird eine gültige Datei angegeben, lädt das Programm diese und öffnet anschließend das Hauptmenü. Ist die Datei ungültig oder der Pfad nicht korrekt, zeigt das Programm eine Fehlermeldung an und der Nutzer erhält erneut die Möglichkeit, den Pfad einzugeben.

Die Bedienung des Hauptmenüs erfolgt über eine nummerierte Auswahl, bei der durch die Eingabe der entsprechenden Zahl der Benutzer einen Such- oder Filtervorgang starten kann (siehe Abbildung 21).



```
Aktuelle Logdatei: C:\...log
Bitte wählen Sie einen Suchbegriff aus:
0: Eigene Eingabe
1: Zeitraum
2: IP-Adresse
3: Facilities
4: User
5: Mnemonic
6: Severity Level
7: Neue Datei auswählen
8: Programm beenden
Auswahl (0-8):
```

Abbildung 21 Hauptmenü nach der Logdatei-Eingabe

An dieser Stelle wird auf die unter Punkt 3.2 beschriebenen Such- und Filterkriterien verwiesen. Nach der Durchführung einer Suche oder Filterung gibt das Programm die Ergebnisse direkt auf der Konsole aus und es besteht die Möglichkeit der Speicherung. Der Nutzer wird gefragt, ob die entstandenen Ergebnisse der Filterung in einer Datei gespeichert werden sollen. Auf die weiteren Bedienmöglichkeiten nach einer Suche/Filterung wurde bereits unter Punkt 3.3 eingegangen.

5 Fazit

5.1 Zusammenfassung

In der vorliegenden Belegarbeit wurde ein Kommandozeilenprogramm in der Programmiersprache C zur Analyse von Cisco-Syslog-Dateien entwickelt. Das Programm ermöglicht neben einer allgemeinen Begriffssuche die Suche nach IP-Adressen, Zeitstempeln, Benutzern, Facilities, Mnemonics und Severity-Levels. Die Ergebnisse werden auf der Konsole ausgegeben und können durch den Benutzer zusätzlich in einer Ausgabedatei gespeichert werden. Das Programm dürfte aufgrund seiner Funktionen für den Einsatz in der Netzwerkanalyse und IT-Forensik geeignet sein und die Aufgabenstellung erfüllen.

5.2 Limitationen

Das Programm setzt die korrekte Formatierung der Logdateien voraus. Abweichungen vom erwarteten Cisco-Syslog-Format könnten zu Fehlermeldungen oder unvollständigen Ausgaben führen. Des Weiteren ist es momentan nicht möglich nach IPv6-Adressen zu suchen – ausschließlich die Suche nach IPv4-Adressen ist möglich.

Das Entwickeln auf unterschiedlichen Betriebssystemen (Windows und MacOS) führt zu Kompilierungsunterschieden. Während Windows bei der Implementierung von Funktionen und Methoden und der Deklaration von Variablen teilweise über die Reihenfolge hinweg schaut, orientiert sich das macOS-System an den ISO/IEC 9899:1999-Standard. Dieser ist ein für die Programmiersprache C entwickelter Standard, der sich besonders mit der Syntax und Semantik eines Programmes beschäftigt [14].

Literaturverzeichnis

- [1] C. Lonvick, "datatracker," 08 2001. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc3164>. [Accessed 17 08 2025].
- [2] Y. Q. Q. Z. P. L. a. J. X. J. Zhou, "DeepSyslog: Deep Anomaly Detection on Syslog Using Sentence Embedding and Metadata," 2022, pp. 3051-1061.
- [3] K. K. a. M. Souppaya, "National Institute of Standards and Technology," 09 2006. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-92.pdf>. [Accessed 17 08 2025].
- [4] R. Gerhards, "datatracker," 03 2009. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc5424>. [Accessed 17 08 2025].
- [5] A. Okmianski, "datatracker," datatracker, 03 2009. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc5426>. [Accessed 17 08 2025].
- [6] Y. M. J. S. F. Miao, "datatracker," 03 2009. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc5425>. [Accessed 17 08 2025].
- [7] Cisco, "Cisco Secure Firewall ASA Series Syslog Messages," 30 01 2019. [Online]. Available: <https://www.cisco.com/c/en/us/td/docs/security/asa/syslog/asa-syslog/about.html>. [Accessed 26 08 2025].
- [8] Cisco, "System Management Configuration Guide, Cisco IOS XE 17.x – System Logging Message Formatting," [Online]. Available: https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/syst-mgmt/b-system-management/m_esm-syslog.html. [Accessed 25 08 2025].
- [9] "Cisco," Cisco, [Online]. Available: <https://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SysMsgLogging.html#wp1055064>. [Accessed 26 08 2025].
- [10] "Cisco docs," Cisco, [Online]. Available: https://docs.manage.security.cisco.com/cdfmc/c_severity_levels.html. [Accessed 26 08 2025].
- [11] "pi-informatik," PI Informatik GmbH, [Online]. Available: <https://www.pi-informatik.berlin/pi-lexikon/softwareentwicklung/was-ist-eine-entwicklungsumgebung/>. [Accessed 19 08 2025].

-
- [12] "Visual Studio Code," Visual Studio Code, [Online]. Available: <https://code.visualstudio.com/>. [Accessed 19 08 2025].
- [13] "Linux-Console.net," [Online]. Available: <https://de.linux-console.net/?p=38950>. [Accessed 26 08 2025].
- [14] American National Standards Institute, "datat," 12 01 1999. [Online]. Available: <https://dotat.at/tmp/iso-iec-9899.pdf>. [Accessed 25 08 2025].

Anhang

Syslog1.log

```
*Sep 14 06:04:55.610: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/8, changed state to down
*Sep 14 06:04:56.611: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/8, changed state to down
*Sep 14 06:04:59.782: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/8, changed state to up
*Sep 14 06:05:00.782: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/8, changed state to up
*Sep 14 06:05:05.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/8, changed state to down
*Sep 14 06:05:06.926: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/8, changed state to down
*Sep 14 06:05:10.855: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/8, changed state to up
*Sep 14 06:05:11.855: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/8, changed state to up
*Sep 14 06:05:25.666: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/0/48, changed state to down
*Sep 14 06:05:26.669: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/48, changed state to down
*Sep 14 06:05:30.762: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/48, changed state to up
*Sep 14 06:05:31.762: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/0/48, changed state to up
*Sep 14 06:06:00.178: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/8, changed state to down
*Sep 14 06:06:01.178: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/8, changed state to down
*Sep 14 06:06:04.842: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/8, changed state to up
*Sep 14 06:06:05.843: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/8, changed state to up
*Sep 14 06:06:48.087: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/8, changed state to down
*Sep 14 06:06:49.086: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/8, changed state to down
*Sep 14 06:06:49.618: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/0/48, changed state to down
*Sep 14 06:06:50.619: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/48, changed state to down
*Sep 14 06:06:52.283: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/8, changed state to up
*Sep 14 06:06:53.282: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/8, changed state to up
*Sep 14 06:06:53.747: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to up
*Sep 14 06:06:54.659: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/48, changed state to up
*Sep 14 06:06:54.745: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up
*Sep 14 06:06:55.658: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/0/48, changed state to up
*Sep 14 06:11:38.066: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, changed state to down
*Sep 14 06:11:39.067: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/6, changed state to down
*Sep 14 06:11:41.749: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/6, changed state to up
*Sep 14 06:11:42.750: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, changed state to up
*Sep 14 06:12:07.247: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, changed state to down
*Sep 14 06:12:08.246: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/6, changed state to down
*Sep 14 06:12:11.395: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/6, changed state to up
*Sep 14 06:12:12.394: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, changed state to up
*Sep 14 06:12:39.799: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, changed state to down
*Sep 14 06:12:40.798: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/6, changed state to down
*Sep 14 06:12:44.166: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/6, changed state to up
*Sep 14 06:12:45.166: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, changed state to up
*Sep 14 06:15:19.051: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, changed state to down
*Sep 14 06:15:20.051: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/6, changed state to down
*Sep 14 06:15:22.819: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/6, changed state to up
*Sep 14 06:15:23.819: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, changed state to up
*Sep 14 06:15:47.766: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, changed state to down
*Sep 14 06:15:48.769: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/6, changed state to down
*Sep 14 06:15:52.126: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/6, changed state to up
*Sep 14 06:15:53.127: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, changed state to up
*Sep 14 06:16:32.707: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, changed state to down
*Sep 14 06:16:33.707: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/6, changed state to down
*Sep 14 06:16:36.741: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/6, changed state to up
*Sep 14 06:16:37.742: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, changed state to up
*Sep 14 06:18:10.538: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, changed state to down
*Sep 14 06:18:11.543: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/6, changed state to down
*Sep 14 06:18:14.277: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/6, changed state to up
*Sep 14 06:18:15.279: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, changed state to up
*Sep 14 06:18:39.319: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, changed state to down
*Sep 14 06:18:40.322: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/6, changed state to down
*Sep 14 06:18:43.415: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/6, changed state to up
*Sep 14 06:18:44.415: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, changed state to up
*Sep 14 06:19:10.158: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, changed state to down
```

```
*Sep 14 06:19:11.157: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/6, changed state to down
*Sep 14 06:19:14.259: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/6, changed state to up
*Sep 14 06:19:15.259: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, changed state to up
*Sep 14 06:19:29.955: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, changed state to down
*Sep 14 06:19:30.954: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/6, changed state to down
*Sep 14 06:19:34.219: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/6, changed state to up
*Sep 14 06:19:35.219: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, changed state to up
*Sep 14 06:19:52.386: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to down
*Sep 14 06:19:53.386: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to down
*Sep 14 06:19:56.874: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to up
*Sep 14 06:19:57.875: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up
*Sep 14 06:25:05.502: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/24, changed state to down
*Sep 14 06:25:06.503: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/24, changed state to down
*Sep 14 06:25:10.674: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/24, changed state to up
*Sep 14 06:25:11.675: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/24, changed state to up
*Sep 14 06:25:36.191: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/24, changed state to down
*Sep 14 06:25:37.190: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/24, changed state to down
*Sep 14 06:25:40.377: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/24, changed state to up
*Sep 14 06:25:41.379: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/24, changed state to up
*Sep 14 06:25:54.563: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/24, changed state to down
*Sep 14 06:25:55.563: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/24, changed state to down
*Sep 14 06:25:58.686: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/24, changed state to up
*Sep 14 06:25:59.685: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/24, changed state to up
*Sep 14 06:26:01.310: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/24, changed state to down
*Sep 14 06:26:02.314: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/24, changed state to down
*Sep 14 06:26:05.433: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/24, changed state to up
*Sep 14 06:26:06.435: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/24, changed state to up
*Sep 14 06:26:44.350: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to down
*Sep 14 06:26:45.350: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to down
*Sep 14 08:54:29.614: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to up
*Sep 14 08:54:30.614: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up
*Sep 14 08:54:38.035: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to down
*Sep 14 08:54:39.034: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to down
*Sep 14 08:54:42.318: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to up
*Sep 14 08:54:43.318: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up
*Sep 14 08:56:24.678: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to down
*Sep 14 08:56:25.679: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to down
*Sep 14 08:56:29.125: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to up
*Sep 14 08:56:30.126: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up
*Sep 14 08:56:45.822: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/24, changed state to down
*Sep 14 08:56:46.826: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/24, changed state to down
*Sep 14 08:56:49.551: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/24, changed state to up
*Sep 14 08:56:50.550: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/24, changed state to up
*Sep 14 08:57:14.242: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/24, changed state to down
*Sep 14 08:57:15.243: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/24, changed state to down
*Sep 14 08:57:18.322: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/24, changed state to up
*Sep 14 08:57:19.322: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/24, changed state to up
*Sep 14 08:57:32.751: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/24, changed state to down
*Sep 14 08:57:33.754: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/24, changed state to down
*Sep 14 08:57:36.827: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/24, changed state to up
*Sep 14 08:57:37.834: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/24, changed state to up
*Sep 14 08:57:39.631: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/24, changed state to down
*Sep 14 08:57:40.631: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/24, changed state to down
*Sep 14 08:57:43.789: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/24, changed state to up
*Sep 14 08:57:44.791: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/24, changed state to up
*Sep 14 08:57:59.385: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to down
*Sep 14 08:58:00.391: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to down
*Sep 14 09:34:05.903: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: datacadm] [Source: 172.16.100.188] [localport: 22] at
09:34:05 UTC Thu Sep 14 2023
*Sep 14 09:36:44.722: %SYS-6-LOGOUT: User datacadm has exited tty session 2(172.16.100.188)
*Sep 14 12:14:45.876: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart License Utility (CSLU) : Unable
to resolve server hostname/domain name
*Sep 14 13:11:51.274: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to up
*Sep 14 13:11:52.275: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up
*Sep 14 13:13:21.503: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: datacadm] [Source: 172.16.100.187] [localport: 22] at
13:13:21 UTC Thu Sep 14 2023
```


*Sep 14 13:13:55.033: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/25, changed state to down
*Sep 14 13:13:55.352: %SYS-5-CONFIG_I: Configured from console by datacadm on vty0 (172.16.100.187)
*Sep 14 13:14:08.649: %SYS-6-LOGOUT: User datacadm has exited tty session 2(172.16.100.187)
*Sep 14 13:14:22.418: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to down
*Sep 14 13:14:23.422: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to down
*Sep 14 13:14:32.154: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/25, changed state to up
*Sep 14 13:14:33.155: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/25, changed state to up
*Sep 14 13:26:43.830: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/25, changed state to down
*Sep 14 13:26:44.831: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/25, changed state to down
*Sep 15 12:14:54.887: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart License Utility (CSLU) : Unable to resolve server hostname/domain name
*Sep 16 12:15:03.906: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart License Utility (CSLU) : Unable to resolve server hostname/domain name
*Sep 17 12:15:12.919: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart License Utility (CSLU) : Unable to resolve server hostname/domain name
*Sep 18 12:15:21.935: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart License Utility (CSLU) : Unable to resolve server hostname/domain name
*Sep 19 12:00:43.984: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart License Utility (CSLU) : Communications failure
*Sep 19 12:15:30.947: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart License Utility (CSLU) : Unable to resolve server hostname/domain name
*Sep 20 12:15:39.960: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart License Utility (CSLU) : Unable to resolve server hostname/domain name
*Sep 21 12:15:48.975: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart License Utility (CSLU) : Unable to resolve server hostname/domain name
*Sep 22 12:15:57.987: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart License Utility (CSLU) : Unable to resolve server hostname/domain name
*Sep 23 12:16:07.004: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart License Utility (CSLU) : Unable to resolve server hostname/domain name
*Sep 24 12:16:16.016: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart License Utility (CSLU) : Unable to resolve server hostname/domain name
*Sep 25 12:16:25.026: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart License Utility (CSLU) : Unable to resolve server hostname/domain name
*Sep 26 12:00:44.411: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart License Utility (CSLU) : Communications failure
*Sep 26 12:16:34.038: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart License Utility (CSLU) : Unable to resolve server hostname/domain name
*Sep 27 04:44:54.133: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: datacadm] [Source: 172.16.100.188] [localport: 22] at 04:44:54 UTC Wed Sep 27 2023

Abbildung 22 Cisco-Logdatei, Name: syslog1.log

Syslog2.log

```
*Mar 1 2023 08:00:00.000: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Mar 1 2023 08:05:00.000: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (192.168.1.10)
*Mar 1 2023 08:10:00.000: %SEC-6-IPACCESSLOGP: IP access denied via ACL from 192.168.2.20 to 10.0.0.1
*Mar 1 2023 08:15:00.000: %BGP-5-ADJCHANGE: BGP neighbor 172.16.0.2 Up
*Mar 1 2023 08:20:00.000: %STP-2-BRIDGE_FORWARDING: Interface GigabitEthernet0/1, changed state to forwarding
*Mar 1 2023 08:25:00.000: %CDP-4-DUPLEX_MISMATCH: Duplex mismatch discovered on GigabitEthernet0/2 (not half duplex), with
switch SW2
*Mar 1 2023 08:30:00.000: %OSPF-5-ADJCHG: Process 100, Nbr 192.168.3.30 on GigabitEthernet0/3 from FULL to DOWN
*Mar 1 2023 08:35:00.000: %HSRP-4-ACTIVE: GigabitEthernet0/4 is now the active router for HSRP group 1
*Mar 1 2023 08:40:00.000: %SNMP-3-AUTHFAIL: Authentication failure for SNMP request from 192.168.4.40
*Mar 1 2023 08:45:00.000: %RADIUS-4-RADIUS_ERR_RESPONSE: RADIUS server 10.1.1.1 sent an invalid response
*Mar 1 2023 17:55:00.000: %IP-4-DUPADDR: Duplicate address 192.168.1.10 on GigabitEthernet0/0, sourced by 00:1A:2B:3C:4D:5E
*Mar 1 2023 18:00:00.000: %SYS-5-RELOAD: Reload requested by admin on console
Abbildung 23 Cisco-Logdatei, Name: syslog2.log
```

Syslog_generic.log

```
<189>: Sep 27 2023 10:15:30.1234 UTC: %SYS-5-CONFIG_I: Configured from console by admin on Router-1
<184>: Sep 27 2023 10:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
<190>: Sep 27 2023 10:17:12.3456 UTC: %SEC-6-IPACCESSLOGP: IP access violation detected: 10.0.0.1 -> 192.168.1.1
<187>: Sep 27 2023 10:18:00.9876 UTC: %BGP-5-ADJCHANGE: Neighbor 192.168.2.2 Down due to BGP Notification received
<188>: Sep 27 2023 10:19:18.4321 UTC: %SYS-4-CPUHOG: CPU hog detected on Router-1, process: HOG_PROCESS
<189>: Sep 27 2023 11:15:30.1234 UTC: %SYS-5-CONFIG_I: Configured from console by admin on Router-2
<184>: Sep 27 2023 11:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to down
<190>: Sep 27 2023 11:17:12.3456 UTC: %SEC-6-IPACCESSLOGP: IP access violation detected: 10.0.0.2 -> 192.168.1.2
<187>: Sep 27 2023 11:18:00.9876 UTC: %BGP-5-ADJCHANGE: Neighbor 192.168.2.3 Down due to BGP Notification received
<188>: Sep 27 2023 11:19:18.4321 UTC: %SYS-4-CPUHOG: CPU hog detected on Router-2, process: HOG_PROCESS
<189>: Sep 27 2023 12:15:30.1234 UTC: %SYS-5-CONFIG_I: Configured from console by admin on Router-3
<184>: Sep 27 2023 12:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/3, changed state to up
<190>: Sep 27 2023 12:17:12.3456 UTC: %SEC-6-IPACCESSLOGP: IP access violation detected: 10.0.0.3 -> 192.168.1.3
<187>: Sep 27 2023 12:18:00.9876 UTC: %BGP-5-ADJCHANGE: Neighbor 192.168.2.4 Down due to BGP Notification received
<188>: Sep 27 2023 12:19:18.4321 UTC: %SYS-4-CPUHOG: CPU hog detected on Router-3, process: HOG_PROCESS
<189>: Sep 27 2023 13:15:30.1234 UTC: %SYS-5-CONFIG_I: Configured from console by admin on Router-4
<184>: Sep 27 2023 13:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/4, changed state to down
<190>: Sep 27 2023 13:17:12.3456 UTC: %SEC-6-IPACCESSLOGP: IP access violation detected: 10.0.0.4 -> 192.168.1.4
<187>: Sep 27 2023 13:18:00.9876 UTC: %BGP-5-ADJCHANGE: Neighbor 192.168.2.5 Down due to BGP Notification received
<188>: Sep 27 2023 13:19:18.4321 UTC: %SYS-4-CPUHOG: CPU hog detected on Router-4, process: HOG_PROCESS
<189>: Sep 27 2023 14:15:30.1234 UTC: %SYS-5-CONFIG_I: Configured from console by admin on Router-5
<184>: Sep 27 2023 14:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/5, changed state to up
<190>: Sep 27 2023 14:17:12.3456 UTC: %SEC-6-IPACCESSLOGP: IP access violation detected: 10.0.0.5 -> 192.168.1.5
<187>: Sep 27 2023 14:18:00.9876 UTC: %BGP-5-ADJCHANGE: Neighbor 192.168.2.6 Down due to BGP Notification received
<188>: Sep 27 2023 14:19:18.4321 UTC: %SYS-4-CPUHOG: CPU hog detected on Router-5, process: HOG_PROCESS
<189>: Sep 27 2023 15:15:30.1234 UTC: %SYS-5-CONFIG_I: Configured from console by admin on Router-6
<184>: Sep 27 2023 15:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/6, changed state to up
<190>: Sep 27 2023 15:17:12.3456 UTC: %SEC-6-IPACCESSLOGP: IP access violation detected: 10.0.0.6 -> 192.168.1.6
<187>: Sep 27 2023 15:18:00.9876 UTC: %BGP-5-ADJCHANGE: Neighbor 192.168.2.7 Down due to BGP Notification received
<188>: Sep 27 2023 15:19:18.4321 UTC: %SYS-4-CPUHOG: CPU hog detected on Router-6, process: HOG_PROCESS
<189>: Sep 27 2023 16:15:30.1234 UTC: %SYS-5-CONFIG_I: Configured from console by admin on Router-7
<184>: Sep 27 2023 16:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/7, changed state to down
<190>: Sep 27 2023 16:17:12.3456 UTC: %SEC-6-IPACCESSLOGP: IP access violation detected: 10.0.0.7 -> 192.168.1.7
<187>: Sep 27 2023 16:18:00.9876 UTC: %BGP-5-ADJCHANGE: Neighbor 192.168.2.8 Down due to BGP Notification received
<188>: Sep 27 2023 16:19:18.4321 UTC: %SYS-4-CPUHOG: CPU hog detected on Router-7, process: HOG_PROCESS
<189>: Sep 27 2023 17:15:30.1234 UTC: %SYS-5-CONFIG_I: Configured from console by admin on Router-8
<184>: Sep 27 2023 17:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/8, changed state to up
<190>: Sep 27 2023 17:17:12.3456 UTC: %SEC-6-IPACCESSLOGP: IP access violation detected: 10.0.0.8 -> 192.168.1.8
<187>: Sep 27 2023 17:18:00.9876 UTC: %BGP-5-ADJCHANGE: Neighbor 192.168.2.9 Down due to BGP Notification received
<188>: Sep 27 2023 17:19:18.4321 UTC: %SYS-4-CPUHOG: CPU hog detected on Router-8, process: HOG_PROCESS
<189>: Sep 27 2023 18:15:30.1234 UTC: %SYS-5-CONFIG_I: Configured from console by admin on Router-9
<184>: Sep 27 2023 18:16:45.6789 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet0/9, changed state to down
<190>: Sep 27 2023 18:17:12.3456 UTC: %SEC-6-IPACCESSLOGP: IP access violation detected: 10.0.0.9 -> 192.168.1.9
<187>: Sep 27 2023 18:18:00.9876 UTC: %BGP-5-ADJCHANGE: Neighbor 192.168.2.10 Down due to BGP Notification received
<188>: Sep 27 2023 18:19:18.4321 UTC: %SYS-4-CPUHOG: CPU hog detected on Router-9, process: HOG_PROCESS
<189>: Sep 27 2023 19:15:30.1234 UTC: %SYS-5-USER_LOGOUT: User admin logged out from Router-10
<184>: Sep 27 2023 19:16:45.6789 UTC: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
<190>: Sep 27 2023 19:17:12.3456 UTC: %SEC-6-IPACCESSLOGP: IP access violation detected: 10.0.0.10 -> 192.168.1.10
<187>: Sep 27 2023 19:18:00.9876 UTC: %VPN-4-IKMP_NO_SA: IKE message from 203.0.113.1 has no SA, deleting
<188>: Sep 27 2023 19:19:18.4321 UTC: %INTERFACE-6-ERROR_DISABLED: Interface GigabitEthernet0/0/1 disabled due to excessive errors
<189>: Sep 27 2023 20:15:30.1234 UTC: %SYS-5-CONFIG_I: Configured from console by admin on Router-11
<184>: Sep 27 2023 20:16:45.6789 UTC: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to down
<190>: Sep 27 2023 20:17:12.3456 UTC: %SEC-6-IPACCESSLOGP: IP access violation detected: 10.0.0.11 -> 192.168.1.11
<187>: Sep 27 2023 20:18:00.9876 UTC: %OSPF-5-ADJCHG: OSPF neighbor 192.168.3.1 went down
<188>: Sep 27 2023 20:19:18.4321 UTC: %SYS-4-LOGGING: Logging to host 192.168.4.1 failed - Host unreachable
<189>: Sep 27 2023 21:15:30.1234 UTC: %SYS-5-CONFIG_I: Configured from console by admin on Router-12
<184>: Sep 27 2023 21:16:45.6789 UTC: %LINK-3-UPDOWN: Interface Serial0/0/1, changed state to up
<190>: Sep 27 2023 21:17:12.3456 UTC: %SEC-6-IPACCESSLOGP: IP access violation detected: 10.0.0.12 -> 192.168.1.12
<187>: Sep 27 2023 21:18:00.9876 UTC: %EIGRP-5-ADJCHANGE: Neighbor 192.168.5.1 went up
<188>: Sep 27 2023 21:19:18.4321 UTC: %SYS-4-RESTART: System restarted
<189>: Sep 27 2023 22:15:30.1234 UTC: %SYS-5-CONFIG_I: Configured from console by admin on Router-13
<184>: Sep 27 2023 22:16:45.6789 UTC: %LINK-3-UPDOWN: Interface Serial0/0/2, changed state to down
```

<190>: Sep 27 2023 22:17:12.3456 UTC: %SEC-6-IPACCESSLOGP: IP access violation detected: 10.0.0.13 -> 192.168.1.13
<187>: Sep 27 2023 22:18:00.9876 UTC: %VRRP-6-STATECHANGE: VRRP Group 1 state changed to Backup
<188>: Sep 27 2023 22:19:18.4321 UTC: %SYS-4-SW2BASIC: Switching from advanced to basic mode
<189>: Sep 27 2023 23:15:30.1234 UTC: %SYS-5-CONFIG_I: Configured from console by admin on Router-14
<184>: Sep 27 2023 23:16:45.6789 UTC: %LINK-3-UPDOWN: Interface Serial0/0/3, changed state to up
<190>: Sep 27 2023 23:17:12.3456 UTC: %SEC-6-IPACCESSLOGP: IP access violation detected: 10.0.0.14 -> 192.168.1.14
<187>: Sep 27 2023 23:18:00.9876 UTC: %HSRP-4-STATECHANGE: FastEthernet0/1 Grp 1 state Standby -> Active
<188>: Sep 27 2023 23:19:18.4321 UTC: %SYS-4-STACKT: Stack unit 2 switched to new master
<189>: Sep 27 2023 00:15:30.1234 UTC: %SYS-5-CONFIG_I: Configured from console by admin on Router-15
<184>: Sep 27 2023 00:16:45.6789 UTC: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to down
<190>: Sep 27 2023 00:17:12.3456 UTC: %SEC-6-IPACCESSLOGP: IP access violation detected: 10.0.0.15 -> 192.168.1.15
<187>: Sep 27 2023 00:18:00.9876 UTC: %VLAN-6-PORT_UP: VLAN 20, port FastEthernet0/2 is up
<188>: Sep 27 2023 00:19:18.4321 UTC: %SYS-4-TIMER: Timer 1 has expired on Router-15
<189>: Sep 27 2023 01:15:30.1234 UTC: %SYS-5-CONFIG_I: Configured from console by admin on Router-16
<184>: Sep 27 2023 01:16:45.6789 UTC: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to up
<190>: Sep 27 2023 01:17:12.3456 UTC: %SEC-6-IPACCESSLOGP: IP access violation detected: 10.0.0.16 -> 192.168.1.16
<187>: Sep 27 2023 01:18:00.9876 UTC: %SNMP-6-AUTHFAIL: SNMP authentication failure from host 192.168.10.1
<188>: Sep 27 2023 01:19:18.4321 UTC: %SYS-4-ROUTERBOOT: Router-16 is booting up
<189>: Sep 27 2023 02:15:30.1234 UTC: %SYS-5-CONFIG_I: Configured from console by admin on Router-17
<184>: Sep 27 2023 02:16:45.6789 UTC: %LINK-3-UPDOWN: Interface FastEthernet0/4, changed state to down
<190>: Sep 27 2023 02:17:12.3456 UTC: %SEC-6-IPACCESSLOGP: IP access violation detected: 10.0.0.17 -> 192.168.1.17
<187>: Sep 27 2023 02:18:00.9876 UTC: %PORTSEC-6-VIOLATION: Security violation on interface FastEthernet0/4
<188>: Sep 27 2023 02:19:18.4321 UTC: %SYS-4-STACKM: Stack unit 3 has been added to the stack
<189>: Sep 27 2023 03:15:30.1234 UTC: %SYS-5-CONFIG_I: Configured from console by admin on Router-18
<184>: Sep 27 2023 03:16:45.6789 UTC: %LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to up
<190>: Sep 27 2023 03:17:12.3456 UTC: %SEC-6-IPACCESSLOGP: IP access violation detected: 10.0.0.18 -> 192.168.1.18
<187>: Sep 27 2023 03:18:00.9876 UTC: %ACL-6-IPDENY: IP deny from host 10.0.0.19 to 192.168.1.19
<188>: Sep 27 2023 03:19:18.4321 UTC: %SYS-4-PORTFLAP: Port FastEthernet0/5 flapping between up and down states
<189>: Sep 27 2023 04:15:30.1234 UTC: %SYS-5-CONFIG_I: Configured from console by admin on Router-19
<184>: Sep 27 2023 04:16:45.6789 UTC: %LINK-3-UPDOWN: Interface FastEthernet0/6, changed state to down
<190>: Sep 27 2023 04:17:12.3456 UTC: %SEC-6-IPACCESSLOGP: IP access violation detected: 10.0.0.20 -> 192.168.1.20
<187>: Sep 27 2023 04:18:00.9876 UTC: %DHCP-6-ADDRESS_ASSIGN: IP address 192.168.20.1 assigned to client 00:0A:BC:DE:F0:01
<188>: Sep 27 2023 04:19:18.4321 UTC: %SYS-4-INTERFACECHANGE: Interface GigabitEthernet0/0/2 changed state to administratively down

Abbildung 24 Cisco-Logdatei, Name: syslog_generic.log

Selbstständigkeitserklärung

„Wir versichern hiermit an Eides statt, dass wir die vorliegende Arbeit selbstständig verfasst, ganz oder in Teilen noch nicht als Prüfungsleistung vorgelegt und keine anderen als die angegebenen Hilfsmittel benutzt haben. Sämtliche Stellen der Arbeit, die benutzten Werke im Wortlaut oder dem Sinn entnommen sind, haben wir durch Quellenangaben kenntlich gemacht. Dies gilt auch für Zeichnungen, Skizzen, bildliche Darstellungen und dergleichen sowie für Quellen aus dem Internet. Uns ist bewusst, dass es sich beim Plagiarismus um akademisches Verhalten handelt, dass sanktioniert werden kann.“

Philipp Dellwo

Melissa Futtig

Konz, den 30.08.2025

Wiesbaden, den 30.08.2025