

1

Erweiterungen in der Firmware 2.10



Die Erweiterungen der Firmware-Version 2.10 im Vergleich zur Vorversion betreffen die folgenden Punkte:

- *WEBconfig*
- SYSLOG-Modul
- Firewall-Filter
- HTTP-Modul
- DHCP-Client
- HTTP-Status

1.1

Konfiguration mit *ELSA WEBconfig*

Über einen beliebigen, auch textbasierten Web-Browser können Sie die Grundeinstellungen des Gerätes vornehmen. *ELSA WEBconfig* verfügt über ähnliche Setup-Assistenten wie *LANconfig* und bietet damit optimale Voraussetzungen für eine komfortable Konfiguration des *LANCOM* unter allen möglichen Betriebssystemen.

Um eine Verbindung zum *LANCOM* herzustellen, muß ein LAN-Anschluß über TCP/IP aufgebaut sein. Normalerweise erfolgt der Zugriff über die IP-Adresse des Gerätes:

```
http://<IP-Adresse des LANCOM>
```

Ein unkonfiguriertes bzw. zurückgesetztes *LANCOM* antwortet sogar auf alle IP-Adressen. Voraussetzung ist, daß die '254' am Ende der IP-Adresse steht (z.B. <http://10.0.0.254>, aber auch <http://192.168.0.254>).

Sofern bereits ein DHCP-Server im LAN aktiv ist, muß genau die IP-Adresse angesprochen werden, die das LANCOM vom DHCP-Server zugewiesen bekommen hat.

Eine umfangreiche, kontextsensitive Dokumentation zu den einzelnen *WEBconfig*-Seiten und -Feldern ist jederzeit im *WEBconfig* über den Link 'Hilfe (Referenzhandbuch)' zu erreichen. Näheres zur Einstellung der mit *WEBconfig* verknüpften Kontext-Hilfe finden Sie im Abschnitt '1.4 HTTP-Modul'.





1.2 Das SYSLOG-Modul

Mit dem SYSLOG-Modul besteht die Möglichkeit, Zugriffe auf das *LANCOM* protokollieren zu lassen. Diese Funktion ist insbesondere für Systemadministratoren interessant, da sie die Möglichkeit bietet, eine lückenlose Historie aller Aktivitäten aufzeichnen zu lassen.

Um die SYSLOG-Nachrichten empfangen zu können, benötigen Sie einen entsprechenden Dämon bzw. Client. Unter UNIX/Linux erfolgt die Protokollierung durch den in der Regel standardmäßig eingerichteten SYSLOG-Dämon. Dieser meldet sich entweder direkt über die Konsole oder schreibt das Protokoll in eine entsprechende SYSLOG-Datei.

Unter Linux wird in der Datei `/etc/syslog.conf` angegeben, welche Facilitys in welche Logdatei geschrieben werden sollen. Überprüfen Sie in der Konfiguration des Dämons, ob auf Netzwerkverbindungen explizit gehört wird.

Windows stellt keine entsprechende Systemfunktion bereit. Sie benötigen spezielle Software, die die Funktion eines SYSLOG-Dämons erfüllt.

1.2.1

Einrichten des SYSLOG-Moduls

Sie haben mehrere Möglichkeiten das SYSLOG-Modul einzurichten:

- *WEBconfig*
Vollkonfiguration ► Setup ► SYSLOG-Modul, bzw.
Log und Trace ► SYSLOG-Modul konfigurieren
- *LANconfig*
Management ► Meldungen
- Telnet
/Setup/SYSLOG-Modul

1.2.2

Beispielkonfiguration mit *ELSA LANconfig*

SYSLOG-Client anlegen

- ① Starten Sie *ELSA LANconfig*. Unter 'Management' wählen Sie die Karte 'Meldungen'.
- ② Schalten Sie das Modul ein, und klicken Sie auf **SYSLOG-Clients**.
- ③ Im nächsten Fenster klicken Sie auf **Hinzufügen....**
- ④ Geben Sie zunächst die IP-Adresse des SYSLOG-Clients ein, und legen Sie im weiteren die Quellen und Prioritäten fest.

SYSLOG-Clients - Neuer Eintrag

IP-Adresse:

Quelle:

<input checked="" type="checkbox"/> System	<input checked="" type="checkbox"/> Logins
<input checked="" type="checkbox"/> Systemzeit	<input type="checkbox"/> Konsolen-Logins
<input checked="" type="checkbox"/> Verbindungen	<input type="checkbox"/> Accounting
<input type="checkbox"/> Verwaltung	<input type="checkbox"/> Router

Priorität:

<input checked="" type="checkbox"/> Alarm	<input checked="" type="checkbox"/> Fehler
<input checked="" type="checkbox"/> Warning	<input checked="" type="checkbox"/> Information
<input type="checkbox"/> Debug	

SYSLOG kommt aus der UNIX-Welt in der bestimmte Quellen vordefiniert sind. *LANCOM* mappt seine eigenen internen Quellen im Auslieferungszustand auf die vordefinierten. Diese heißen dann allgemein Facilities.

Die folgende Tabelle gibt eine Übersicht über die im *LANCOM* schaltbaren Nachrichtenquellen sowie deren Bedeutung. Zusätzlich gibt die letzte

Spalte die Zuordnung zwischen den internen Quellen des *LANCOM* und den SYSLOG-Facilities im Auslieferungszustand an.

Quelle	Bedeutung	Facility
System	Systemmeldungen (Bootvorgänge, Timersystem etc.)	KERNEL
Logins	Meldungen über Login und Logout eines Users während der PPP-Verhandlung sowie dabei auftretende Fehler	AUTH
Systemzeit	Meldungen über Änderungen der Systemzeit	CRON
Konsolen-Logins	Meldungen über Konsolen-Logins (Telnet, Outband, etc), Logouts und dabei auftretende Fehler	AUTHPRIV
Verbindungen	Meldungen über den Verbindungsauf- und -abbau sowie dabei auftretende Fehler (Display-Trace)	LOCAL0
Accounting	Accounting-Informationen nach dem Abbau einer Verbindung (User, Onlinezeit, Transfervolumen)	LOCAL1
Verwaltung	Meldungen über Konfigurationsänderungen, remote ausgeführte Kommandos etc.	LOCAL2
Router	Regelmäßige Statistiken über die am häufigsten genutzten Dienste (nach Portnummern aufgeschlüsselt) sowie Meldungen über gefilterte Pakete, Routing-Fehler etc.	LOCAL3

Die im SYSLOG definierten acht Prioritätsstufen sind im *LANCOM* auf fünf Stufen reduziert. Die nachfolgende Tabelle zeigt die Zuordnung zwischen Alarmlevel, Bedeutung und SYSLOG-Prioritäten.

Priorität	Bedeutung	SYSLOG-Priorität
Alarm	Hierunter werden alle Meldungen zusammengefaßt, die der erhöhten Aufmerksamkeit des Administrators bedürfen.	PANIC, ALERT, CRIT
Fehler	Auf diesem Level werden alle Fehlermeldungen übermittelt, die auch im Normalbetrieb auftreten können, ohne daß ein Eingriff des Administrators notwendig wird (z.B. Verbindungsfehler).	ERROR
Warning	Dieser Level übermittelt Fehlermeldungen, die den ordnungsgemäßen Betrieb des Geräts nicht beeinträchtigen.	WARNING
Information	Auf diesem Level werden alle Nachrichten übermittelt, die rein informellen Charakter haben (z.B. Accounting-Informationen).	NOTICE, INFORM

Priorität	Bedeutung	SYSLOG-Priorität
Debug	Dies ist die niedrigste Priorität. Debug-Meldungen sollten niemals übermittelt werden.	DEBUG

- ⑤ Wenn Sie alle Parameter definiert haben, bestätigen Sie die Eingaben mit **OK**. In der SYSLOG-Tabelle wird der SYSLOG-Client mit seinen Parametern eingetragen.

Facilities

Über die Schaltfläche **Facility-Zuordnung** können alle *LANCOM*-Meldungen einem Facility zugeordnet und dadurch vom SYSLOG-Dämon ohne zusätzlichen Aufwand in eine spezielle Log-Datei geschrieben werden.

Beispiel

Alle Facilities werden auf 'local7' gesetzt. Unter Linux werden nun in der Datei '/etc/syslog.conf' durch den Eintrag

```
local7.* /var/log/lancom.log
```

alle Ausgaben des *LANCOM* in die Datei '/var/log/lancom.log' geschrieben.

1.3

Firewall

Die Firewall-Filter der *LANCOM*-Geräte bieten Filterfunktionen für einzelne Rechner und auch ganze Netze. Es ist möglich, Quell- und Zielfilter für einzelne Ports oder auch Portbereiche aufzusetzen. Zudem können einzelne Protokolle oder beliebige Protokollkombinationen (TCP/UDP/ICMP) gefiltert werden.

Sobald eine Filterbedingung zutrifft, kann eine definierbare Aktion ausgeführt werden.

Die Filter werden mit Hilfe zweier Tabellen eingerichtet. Zum einen die Objektliste, in der Rechner, Netze, Protokolle etc. als Objekte definiert werden. Als zweites die Regelliste, in der Quelle, Ziel und Aktion mit Hilfe der einzelnen Objekte beschrieben werden. Aus diesen beiden Tabellen wird die eigentliche Filter-Tabelle erzeugt.

Dadurch ist es nicht mehr erforderlich, die Filterliste selber zu erstellen, wodurch keine inkonsistenten Einträge in der Filter-Tabelle mehr auftauchen können.

Objektlist

In der Objektliste können die zu filternden Objekte definiert werden. Objekte können sein:

- Protokolle
- Einzelne Rechner
- Ganze Netze
- Dienste

Diese Elemente lassen sich auch beliebig kombinieren. Zudem können Objekte rekursiv definiert werden. So könnten zunächst Objekte für die Protokolle TCP und UDP definiert werden. Später kämen dann Objekte z.B. für FTP (= TCP + Ports 20 und 21), HTTP (= TCP + Port 80) und DNS (= TCP, UDP + Port 53) hinzu. Diese könnten dann wiederum zu einem Objekt zusammengefaßt werden, das alle Freigaben enthält.

Die Regeltabelle

Über die Regel-Tabelle werden die einzelnen Objekte zu Filterregeln kombiniert. Die Regel-Tabelle enthält das zu filternde Protokoll, die Quell-Objekte, die Ziel-Objekte sowie die auszuführende Filteraktion.

Das Protokoll sowie die Quell- bzw. Ziel-Objekte können sowohl aus zusammengestellten Objekten bestehen als auch direkte Beschreibungen (z.B. %P6 für TCP) beinhalten, die durch '+' oder Leerzeichen getrennt werden. Eine direkte Beschreibung wird durch '%' gekennzeichnet. Mögliche Beschreibungen sind:

Beschreibung	Funktion
%A	IP-Adresse
%M	Netzmaske
%S	Dienst (Port)
%L	lokales Netz
%H	Hostname
%P	Protokoll (TCP/UDP/ICMP etc.)

Gleichartige Beschreibungen können durch Komma getrennte Listen, wie z.B. Host-Listen/Adresslisten (%A10.0.0.1, 10.0.0.2) oder durch Bindestrich

getrennte Bereiche wie z.B. Portlisten (%S20-25) erzeugen. Die Angabe einer '0' oder eines Leerstrings bezeichnet das Any-Objekt:

alle Rechner: %A0.0.0.0

alle Dienste: %S0

alle Protokolle: %P0

Hostnamen können nur dann verwendet werden, wenn *LANCOM* die Namen in IP-Adressen auflösen kann. Dafür muß *LANCOM* die Namen über DHCP oder NetBIOS gelernt haben, oder die Zuordnung muß statisch in der DNS- oder IP-Routing-Tabelle eingetragen sein. Ein Eintrag in der IP-Routing-Tabelle kann dabei einem Hostnamen ein ganzes Netz zuordnen.

Die Filter-Liste

Aus Objekt-Tabelle und Regel-Tabelle wird schließlich die Filter-Liste aufgebaut. Dabei wird die Vereinigungsmenge aller durch die Regeln und Objekte definierten Filter gebildet.

Beachten Sie bitte, daß Filter bei einer Fehlangebe nicht erzeugt und auch keine Fehlermeldungen ausgegeben werden. Wenn Sie die Filter manuell konfigurieren, sollten Sie in jedem Fall überprüfen, ob die gewünschten Filter erzeugt wurden.



1.3.1

Einrichten der Filter

Sie haben mehrere Möglichkeiten die Firewall-Filter einzurichten:

- *WEBconfig*
Vollkonfiguration ► Setup ► IP-Router-Modul ► Firewall
- *LANconfig*
IP-Router ► Filter
- Telnet
/Setup/IP-Router-Modul/Firewall

Besonders komfortabel ist die Einrichtung der Filter mit Hilfe von *ELSA LANconfig*. Unter 'Filter' finden Sie die folgenden Karteikarten, mit deren Hilfe Filterregeln definiert werden können.

Bitte beachten Sie, daß bei der Konfiguration mit LANconfig, Objekttabellen, die mit Telnet oder WEBconfig eingerichtet wurden, nach einem Zurückschreiben nur in veränderter Form vorliegen.



- Allgemein
Hier wird der Name des Filterdienstes festgelegt und was mit den Datenpaketen geschehen soll (Aktion).
- Stationen
Hier werden die Stationen festgelegt, für die die Filterregel als Absender oder Adressat gelten soll.
- Dienste
Hier wird festgelegt, für welche IP-Protokolle, Quell- und Zielports die Filterregel gelten soll.

1.4

HTTP-Modul

Über das HTTP-Modul können Sie die Dokumentenwurzel für die HTML-Hilfedateien festlegen. In der Voreinstellung verweist der Hilfe-Link auf die ELSA-Web-Seiten. Wenn Sie die Hilfedateien lokal ablegen möchten, können Sie hier das Verzeichnis für diese Dateien eintragen.



Die jeweils aktuelle Version der HTML-Hilfe finden Sie zum Download auf den ELSA-Web-Seiten.

1.5

DHCP-Client

Mit der Firmware 2.10 erhalten die Geräte auch die Möglichkeit, von einem im Netz vorhandenen DHCP-Server automatisch eine IP-Adresse zu beziehen. Der Menüpunkt 'Setup/DHCP-Modul/Operating' erhält dazu weitere Funktionen:

Im Zustand 'Auto' sucht das Gerät nach anderen DHCP-Servern im Netz. Wird einer gefunden, wird der eigene DHCP-Server nicht aktiviert, und das Gerät beschafft sich von diesem eine IP-Adresse. Letzteres passiert aber nur, wenn das Gerät selber noch im unkonfigurierten Zustand ist, d.h. sowohl Internet- als auch Intranet-Adresse noch auf 0.0.0.0 stehen. Sobald dort etwas konfiguriert wird, ist die automatisch bezogene Adresse ungültig.

1.6

HTTP-Status

Mit der Firmware 2.10 bekommt jetzt auch die HTTP-Konfiguration ein Statusmenü. Unter /Status/TCP-IP-Statistik/HTTP-Statistik finden Sie folgende Informationen:

HTTP-Zugriffe	Gesamtzahl Seitenabrufe
HTTP-nichtgefunden-Fehler	Anzahl Zugriffe auf nicht im Gerät vorhandene Seiten
HTTP-Authentisierungs-Fehler	Anzahl Zugriffe, die aufgrund eines fehlenden oder falschen Paßwortes abgelehnt wurden
HTTP-Protokollfehler	Anzahl Zugriffe, die vom Gerät nicht beantwortet werden konnten, weil eine unbekannte HTTP-Anfrage geschickt wurde oder diese Form der Anfrage nicht zulässig war (z.B. das Setzen von Werten über eine Read-Only-Verbindung)

Mit dem Befehl 'Werte-loeschen' werden alle Zähler auf Null zurückgesetzt. Dies erfolgt auch implizit bei einem 'Werte-loeschen' im TCP/IP-Menü.

