

## 1

# Ampliamento nel firmware 2.10

Gli ampliamenti della versione di firmware 2.10 in confronto con la versione precedente riguardano i seguenti punti:

- *WEBconfig*
- Modulo SYSLOG
- Filtro di firewall
- Modulo HTTP
- Client DHCP
- Stato HTTP

## 1.1

## Configurazione con *ELSA WEBconfig*

Le impostazioni di base del dispositivo possono essere effettuate tramite un qualsiasi browser Web anche a base testuale. *ELSA WEBconfig* dispone di simili assistenti per il setup come *LANconfig* ed offre in tal modo presupposti ottimali per una comoda configurazione di *LANCOM* in tutti i possibili sistemi operativi.

Per stabilire un collegamento con *LANCOM*, deve essere stabilito un collegamento LAN tramite TCP/IP. Normalmente, l'accesso avviene tramite l'indirizzo IP del dispositivo:

```
http://<Indirizzo IP del LANCOM>
```

Un *LANCOM* non configurato o resettato risponde perfino a tutti gli indirizzi IP. Il presupposto è che alla fine dell'indirizzo IP ci sia '254' (ad esempio <http://10.0.0.254>, ma anche <http://192.168.0.254> ...).

*A patto che nella LAN sia attivo un server DHCP, si deve accedere esattamente all'indirizzo IP che LANCOM ha ricevuto dal server DHCP.*

Una complessa documentazione contestuale sulle singole pagine e sui singoli campi di *WEBconfig* è raggiungibile in qualsiasi momento in *WEBconfig* tramite il link 'Guida (manuale di riferimento)'. Informazioni più precise sull'impostazione della guida contestuale collegata a *WEBconfig* si trovano nella sezione '1.4 Modulo HTTP'.





## 1.2

## Il modulo SYSLOG

Con il modulo SYSLOG si ha la possibilità di farsi protocollare gli accessi a *LANCOM*. Questa funzione è interessante in particolare per gli amministratori di sistema, poiché essa offre la possibilità di registrare una cronistoria continua di tutte le attività.

Per poter ricevere i messaggi SYSLOG, si necessita di un opportuno demon o client. In UNIX/Linux, il protocollo avviene tramite il demon SYSLOG che di solito è normalmente impostato. Questo si segnala o direttamente tramite il terminale o scrive il protocollo in un corrispondente file SYSLOG.

In Linux viene indicato nel file `/etc/syslog.conf` quali facility debbano essere scritte e in quale file di registrazione. Controllare nella configurazione del demon se c'è reazione esplicita ai collegamenti tramite rete.

Windows non mette a disposizione nessuna funzione di sistema corrispondente. Si necessita di un software speciale che faccia le funzione di un demon di SYSLOG.

## 1.2.1

### Impostazione del modulo SYSLOG

Per impostare il modulo SYSLOG, si hanno più possibilità:

- *WEBconfig*  
Configurazione completa ► Setup ► Modulo SYSLOG, o  
Log e Trace ► Configurazione modulo SYSLOG
- *LANconfig*  
Management ► Messaggi
- Telnet  
/Setup/SYSLOG-module

## 1.2.2

### Esempio di configurazione con *ELSA LANconfig*

#### Creazione del client SYSLOG

- ① Avviare *ELSA LANconfig*. In 'Management' scegliere la scheda 'Messaggi'.
- ② Avviare il modulo, e cliccare su **Client SYSLOG**.
- ③ Nella prossima finestra cliccare su **Aggiungi...**
- ④ Introdurre prima l'indirizzo IP del client SYSLOG e stabilire quindi le sorgenti e priorità.

SYSLOG proviene dal mondo UNIX nel quale determinate sorgenti sono predefinite. *LANCOM* mappa le proprie sorgenti interne dello stato al momento della fornitura su quelle predefinite. Queste prendono poi il nome generale di « Facility ».

La tabella seguente mostra una panoramica delle sorgenti di messaggi attivabili in *LANCOM* come pure il loro significato. L'ultima colonna fornisce inoltre la correlazione tra le sorgenti interne di *LANCOM* e delle facility SYSLOG nello stato al momento della fornitura.

Origine	Significato	Facility
Sistema	Messaggi di sistema (procedure di boot, sistema del timer ecc.)	KERNEL
Logins	Messaggi su login logout di un utente durante la trattativa PPP come pure gli errori che in essa si presentano.	AUTH
Orario di sistema	Messaggi sulle modifiche dell'orario di sistema	CRON
Login di terminale	Messaggi sui login di terminale (telnet, outband, ecc), logout e errori che si presentano.	AUTHPRIV
Collegamenti	Messaggi sull'attivazione e la disattivazione del collegamento come pure sugli errori che si presentano (display trace).	LOCAL0
Accounting	Informazioni di accounting dopo la disattivazione di un collegamento (utente, tempo in linea, volumi di trasferimento).	LOCAL1
Gestione	Messaggi sulle modifiche alla configurazione, comandi eseguiti remotamente ecc.	LOCAL2
Router	Statistiche a intervalli regolari sui servizi più usati (classificati secondo numero di porta) come pure messaggi sui pacchetti filtrati, errori di routing ecc.	LOCAL3

Gli otto gradi di priorità definiti in SYSLOG sono ridotti in *LANCOM* a cinque. La tabella seguente mostra la correlazione tra livello di allarme, significato e priorità di SYSLOG.

Priorità	Significato	Priorità SYSLOG
Alarm	Qui vengono raggruppati tutti i messaggi che necessitano di un'accresciuta attenzione da parte dell'amministratore.	PANIC, ALERT, CRIT
Errore	Su questo livello vengono trasmessi tutti i messaggi di errore che possono presentarsi anche durante il funzionamento normale senza che sia necessario un intervento dell'amministratore (ad esempio errori di collegamento).	ERROR
Warning	Questo livello trasmette messaggi di errore che non nuocciono al funzionamento del dispositivo.	WARNING

Priorità	Significato	Priorità SYSLOG
Informazioni	Su questo livello vengono trasmessi tutti i messaggi che hanno un carattere puramente informale (ad esempio informazioni di accounting).	NOTICE, INFORM
Debug	Questa è la priorità più bassa. I messaggi di debug non vanno mai trasmessi.	DEBUG

- ⑤ Se si sono definiti tutti i parametri, confermare le introduzioni con **OK**. Nella tabella SYSLOG viene inserito il client SYSLOG con i suoi parametri.

### Facility

Tramite il pulsante **Correlazione facility** è possibile correlare tutti i messaggi *LANCOM* ad una facility e farli scrivere in tal modo dal demon SYSLOG senza altre operazioni in uno speciale file di registrazione.

*Esempio*

Tutte le facility vengono impostate su 'local7'. In Linux vengono adesso scritte nel file '/etc/syslog.conf' tramite la voce

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

tutte le emissioni di *LANCOM* nel file '/var/log/lancom.log'.

## 1.3

### Firewall

I filtri di firewall dei dispositivi *LANCOM* offrono funzioni di filtro per singoli computer e anche per intere reti. È possibile impostare filtri sorgente e destinazione per singole porte o anche per aree di porte. È inoltre possibile filtrare singoli protocolli o qualsiasi combinazione di protocolli (TCP/UDP/ICMP).

Non appena una condizione di filtro è soddisfatta, può essere eseguita una operazione definibile.

I filtri vengono impostati con l'aiuto di due tabelle. Da un lato la lista degli oggetti nella quale si definiscono computer, reti, protocolli ecc. quali oggetti. Dall'altro la lista delle regole nella quale vengono scritte la destinazione e l'operazione con l'aiuto dei singoli oggetti. Da queste due tabelle viene generata la tabella di filtro vera e propria.

In tal modo non è più necessario creare da sé la lista di filtro e come conseguenza nella tabella di filtro non ci potranno più essere voci incongruenti.

## Lista degli oggetti

Nella lista degli oggetti possono essere definiti gli oggetti da filtrare. Oggetti possono essere:

- Protocolli
- Singoli computer
- Intere reti
- Servizi

Questi elementi possono anche essere combinati a piacere. Inoltre gli oggetti possono essere definiti con ricursione. Si possono in tal modo prima definire oggetti per i protocolli TCP e UDP. In seguito si aggiungerebbero oggetti per ad esempio FTP (= TCP + porte 20 e 21), HTTP (= TCP + porta 80) e DNS (= TCP, UDP + porta 53). Questi possono a loro volta essere raggruppati in un oggetto che contiene tutte le abilitazioni.

## La tabella delle regole

Tramite la tabella delle regole i singoli oggetti vengono combinati in regole di filtro. La tabella delle regole contiene il protocollo da filtrare, gli oggetti-sorgente, gli oggetti-destinazione come pure l'operazione di filtro da eseguire.

Il protocollo, come pure gli oggetti sorgente o destinazione possono sia essere composti da oggetti combinati, sia contenere anche descrizioni dirette (ad esempio %P6 per TCP) che vengono separate da '+' o da uno spazio. Una descrizione diretta viene contrassegnata con '%'. Possibili descrizioni sono:

Descrizione	Funzione
%A	Indirizzo IP
%M	Maschera di rete
%S	Servizio (porta)
%L	Rete locale
%H	Nome host
%P	Protocollo (TCP/UDP/ICMP ecc.)

Descrizioni dello stesso tipo possono generare delle liste separate da virgole, come ad esempio liste di host/liste di indirizzi (%A10.0.0.1, 10.0.0.2) o aree

separate da un trattino come ad esempio liste di porte (%S20-25). L'indicazione di un '0' o di una stringa vuota contrassegna l'oggetto Any:

Tutti i computer: %A0.0.0.0

Tutti i servizi: %S0

Tutti i protocolli: %P0

I nomi degli host possono essere usati solo se *LANCOM* è in grado di risolvere i nomi in indirizzi IP. A tale scopo *LANCOM* deve aver imparato i nomi tramite DHCP o NetBIOS, o la correlazione deve essere registrata in modo statico nella tabella DNS o di routing IP. (Una voce nella tabella di routing IP può in questo caso correlare ad un nome di host un'intera rete).

### La lista di filtro

Dalla tabella degli oggetti e da quella delle regole viene alla fine generata la lista di filtro. In questo caso viene costituito l'insieme di unione di tutti i filtri definiti dalle regole e dagli oggetti.

*Prestare attenzione al fatto che nel caso di una indicazione errata il filtro non può essere generato e che non vengono emessi messaggi di errore. Se si configurano i filtri a mano, bisogna controllare in ogni caso se i filtri desiderati sono stati generati.*



## 1.3.1

### Impostazione dei filtri

Per impostare un filtro firewall si hanno più possibilità:

- *WEBconfig*  
Configurazione completa ► Setup ► IP router module ► Firewall
- *LANconfig*  
Router IP ► Filtro
- Telnet  
/Setup/IP-router-module/Firewall

Particolarmente comoda è l'impostazione dei filtri con l'aiuto di *ELSA LANconfig*. In 'Filtri' si trovano le seguenti schede, con il cui aiuto si possono definire le regole di filtro:

*Prestare attenzione al fatto che nella configurazione con LANconfig, le tabelle degli oggetti che sono state impostate con telnet o con WEBconfig, dopo una riscrittura sono presenti solo in forma modificata.*



- Generale

Qui viene stabilito il nome del servizio di filtro e cosa debba accadere con i pacchetti di dati (operazione).

- Stazioni

Qui vengono stabilite le stazioni per le quali la regola di filtro debba valere come mittente o destinatario.

- Servizi

Qui viene stabilito per quali protocolli IP, porte sorgente e destinazione la regola di filtro debba valere.

## 1.4

### Modulo HTTP

Tramite il modulo HTTP si possono stabilire le radici di documento per i file di guida HTML. Nella preimpostazione il link alla guida punta sulle pagine Web ELSA. Se si desiderano salvare i file della guida localmente si può qui introdurre la cartella per tali file.



*La versione correntemente valida della guida HTML si trova per essere scaricata nelle pagine Web ELSA.*

## 1.5

### Client DHCP

Con il firmware 2.10, i dispositivi hanno anche la possibilità di prelevare automaticamente un indirizzo IP da server DHCP presente in una rete. Il punto di menù 'Setup/DHCP-module/Operating' riceve a tale scopo ulteriori funzioni:

Nello stato 'Auto' il dispositivo cerca altri server DHCP nella rete. Se ne si trova uno, il proprio server DHCP non viene attivato e il dispositivo si procura da questo un indirizzo IP. Ciò avviene però solo se il dispositivo stesso è ancora in uno stato non configurato, se cioè sia l'indirizzo Internet sia l'indirizzo di Intranet sono ancora su 0.0.0.0. Non appena lì si configura qualcosa, l'indirizzo prelevato automaticamente non è valido.



## 1.6

### Stato HTTP

Con il firmware 2.10 adesso anche la configurazione HTTP ha un menù di stato. In /Status/TCP-IP-statistics/HTTP-statistics si trovano le seguenti informazioni:

HTTP-access	Numero totale dei richiami di pagina
HTTP-not-found-errors	Numero degli accessi a pagine non presenti nel dispositivo
HTTP-authentication-errors	Numero di accessi respinti a causa di una password errata o mancante
HTTP-protocol-errors	Numero degli accessi ai quali il dispositivo non ha potuto rispondere poiché è stata inviata una richiesta HTTP sconosciuta o poiché questa forma di richiesta non era ammessa (ad esempio l'impostazione di valori tramite un collegamento read-only)

Con il comando 'Delete-values' tutti i contatori vengono reimpostati a zero. Ciò avviene anche implicitamente nel caso di un 'Delete-values' nel menù TCP/IP.

