

1

Extensions du microprogramme 2.10

Les extensions de la version 2.10 du microprogramme par rapport à la version précédente concernent les points suivants :

- *WEBconfig*
- Module SYSLOG
- Filtre pare-feu
- Module HTTP
- Client DHCP
- Etat HTTP

1.1

Configuration avec *ELSA WEBconfig*

La configuration fondamentale de l'appareil peut être effectuée au moyen d'un explorateur Web courant, même au moyen d'un explorateur orienté texte. *ELSA WEBconfig* comprend des assistants d'installation semblables à ceux de *LANconfig* et offre ainsi les conditions optimales pour une configuration confortable du *LANCOM* sous tous les systèmes d'exploitation.

Pour se connecter sur le *LANCOM*, une connexion au réseau local (LAN) doit être établie via TCP/IP. Normalement, l'accès se fait via l'adresse IP du périphérique :

```
http://<Adresse IP du LANCOM>
```

Un *LANCOM* non configuré ou réinitialisé répond même à toutes les adresses IP. Il faut toutefois que l'adresse se termine par '254' (par exemple <http://10.0.0.254>, mais aussi <http://192.168.0.254>).

Lorsqu'un serveur DHCP est déjà actif dans le réseau local, il faut adresser précisément l'adresse IP que le serveur DHCP a attribuée au LANCOM.

Une documentation complète et contextuelle sur les diverses pages et champs de *WEBconfig* est disponible dans *WEBconfig* en sélectionnant le lien 'Aide (manuel de référence)'. Les détails de la configuration de l'aide contextuelle liée à *WEBconfig* sont présentés dans le chapitre '1.4 Module HTTP'.





1.2 Le module SYSLOG

Le module SYSLOG permet de consigner les accès au *LANCOM* dans un fichier-journal. Cette fonction est en particulier intéressante pour les administrateurs du système puisqu'elle offre la possibilité d'enregistrer un historique sans lacune de toutes les activités.

Pour pouvoir recevoir les messages SYSLOG, il vous faut un démon ou client adéquat. Sous UNIX/Linux, la journalisation est effectuée par le démon SYSLOG qui est en général installé automatiquement. Ce démon s'annonce soit directement via la console ou enregistre le journal dans un fichier SYSLOG correspondant.

Sous Linux, le fichier `/etc/syslog.conf` indique quelles ressources sont déclarées dans quel fichier-journal. Vérifiez dans la configuration du démon si les connexions réseau sont explicitement surveillées.

Windows ne fournit pas de fonction système correspondante. Vous devrez installer des logiciels spécifiques qui se chargent de la fonction de démon SYSLOG.

1.2.1

Configuration du module SYSLOG

Le module SYSLOG peut être configuré de plusieurs manières :

- *WEBconfig*
Installation complète ► Setup ► Module SYSLOG, ou
Journal et trace ► Configurer le module SYSLOG
- *LANconfig*
Management ► Messages
- Telnet
/Setup/SYSLOG-module

ER

1.2.2

Exemple de configuration avec *ELSA LANconfig*

Création d'un client SYSLOG

- ① Démarrez *ELSA LANconfig*. Sélectionnez 'Management', puis l'onglet 'Messages'.
- ② Activez le module et cliquez sur **Clients SYSLOG**.
- ③ Dans la fenêtre suivante, cliquez sur **Ajouter...**
- ④ Entrez d'abord l'adresse IP du client SYSLOG, puis définissez les sources et les priorités.

Clients SYSLOG - Nouvelle entrée

Adresse IP: 10.1.0.160 [OK]

Source: [Annuler]

<input checked="" type="checkbox"/> Système	<input checked="" type="checkbox"/> Ouvertures de session
<input checked="" type="checkbox"/> Temps système	<input type="checkbox"/> Ouverture de session
<input checked="" type="checkbox"/> Connexions	<input type="checkbox"/> Comptabilisation
<input type="checkbox"/> Gestion	<input type="checkbox"/> Routeur

Priorité:

<input checked="" type="checkbox"/> Alarme	<input checked="" type="checkbox"/> Erreur
<input checked="" type="checkbox"/> Avertissement	<input checked="" type="checkbox"/> Information
<input type="checkbox"/> Débogage	

SYSLOG provient de la plate-forme UNIX dans laquelle certaines sources sont prédéfinies. Le *LANCOM* mappe ses propres sources internes (four-nies au départ usine) sur les sources prédéfinies. Celles-ci sont appelées en général des « lignes ».

Le tableau suivant fournit une liste des sources de messages disponibles dans le *LANCOM* ainsi que leur signification. En plus, la dernière colonne indique l'attribution des sources internes du *LANCOM* aux lignes SYSLOG dans la configuration au départ usine.

Source	Signification	Ligne
Système	Messages système (procédures d'amorçage, système d'estampillage etc.)	KERNEL
Accès	Messages concernant les tentatives d'accès et les déconnexions d'un utilisateur pendant la négociation PPP ainsi que les erreurs survenues.	AUTH
Heure système	Messages concernant les modifications de l'heure système	CRON
Accès via consoles	Messages concernant les accès via consoles (telnet, outband, etc.), les déconnexions et les erreurs survenues.	AUTHPRIV
Connexions	Messages concernant l'établissement et la terminaison d'une connexion ainsi que les erreurs survenues (display trace).	LOCAL0
Informations sur le compte	Informations sur le compte après la terminaison d'une connexion (utilisateur, temps en ligne, volume transféré).	LOCAL1
Administration	Messages concernant les modifications de la configuration, les commandes exécutées à distance, etc.	LOCAL2
Routeur	Statistiques régulières sur les services les plus utilisés (triés par numéro de port) ainsi que des messages concernant les paquets filtrés, les erreurs de routage etc.	LOCAL3

Les huit niveaux de priorité définis dans SYSLOG ont été réduits à cinq niveaux dans le *LANCOM*. Le tableau suivant montre les liens entre le niveau d'alarme, la signification et les priorités SYSLOG.

Priorité	Signification	Priorité SYSLOG
Alarme	Ce niveau regroupe tous les messages qui requièrent l'attention particulière de l'administrateur.	PANIC, ALERT, CRIT
Erreurs	Ce niveau transmet tous les messages d'erreur qui peuvent être générés même en mode de fonctionnement normal sans qu'une intervention de l'administrateur soit nécessaire (par exemple des erreurs de connexion).	ERROR

Priorité	Signification	Priorité SYSLOG
Avertissement	Ce niveau véhicule les messages d'erreur qui ne détériorent pas le fonctionnement correct du périphérique.	WARNING
Information	Ce niveau transmet tous les messages ayant un caractère purement informatif (par exemple les informations sur le compte).	NOTICE, INFORM
Débogage	Cette priorité est la plus basse. Les messages de débogage ne devraient jamais être transmis.	DEBUG

- ⑤ Quand vous avez terminé de définir tous les paramètres, confirmez les données saisies avec **OK**. Le client SYSLOG est ajouté dans le tableau SYSLOG avec ses paramètres.

Lignes

Le bouton **Attribution de ligne** permet d'attribuer tous les messages de *LANCOM* à une ligne ; le démon SYSLOG peut ensuite les enregistrer dans un fichier-journal spécial.

Exemple

Toutes les lignes sont mises à 'local7'. Sous Linux, la commande

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

sert à enregistrer tous les messages du fichier '/etc/syslog.conf' générés par le *LANCOM* dans le fichier '/var/log/lancom.log'.

1.3

Pare-feu

Les filtres pare-feu des périphériques *LANCOM* offrent des fonctions de filtrage d'ordinateurs particuliers ou même de réseaux entiers. Les filtres source ou cible peuvent être appliqués à un port choisi ou à une série de ports. En outre, il est possible de filtrer des protocoles ou des combinaisons de protocoles (TCP/UDP/ICMP).

Dès qu'une condition de filtrage est remplie, une action définissable peut être exécutée.

Les filtres sont configurés au moyen de deux tables. Il s'agit d'une part de la liste des objets dans laquelle les ordinateurs, les réseaux, les protocoles etc. sont définis en tant qu'objets, d'autre part la liste des règles dans laquelle la source, la cible et l'action sont définies à l'aide des divers objets. C'est sur la base de ces deux tables que la table des filtres en soi est générée.

Par conséquent, il n'est plus nécessaire de créer la liste des filtres soi-même, ce qui signifie aussi que des enregistrements incohérents ne figureront plus dans cette table.

Liste des objets

La liste des objets permet de définir les objets à filtrer. Les objets peuvent être les suivants :

- Protocoles
- Ordinateur
- Réseaux entiers
- Services

Ces éléments peuvent aussi être combinés entre eux. En outre, les objets peuvent être définis de manière récursive. Par exemple, on pourrait commencer par définir des objets pour les protocoles TCP et UDP. Plus tard, on pourrait ajouter des objets par exemple pour FTP (= TCP + Ports 20 et 21), HTTP (= TCP + Port 80) et DNS (= TCP, UDP + Port 53). Tous ces objets peuvent ensuite être regroupés dans un seul objet qui contient toutes les autorisations.

La table des règles

La table des règles sert à combiner les objets pour établir des règles de filtrage. Elle contient le protocole à filtrer, les objets source, les objets cible ainsi que l'action de filtrage à exécuter.

Le protocole, les objets source et les objets cible peuvent aussi bien être formés par des objets confectionnés que contenir des descriptions directes (par exemple %P6 pour TCP) qui sont séparées par '+' ou des caractères d'espacement. Une description directe est caractérisée par le signe '%'. Les descriptions possibles sont les suivantes :

Description	Fonction
%A	Adresse IP
%M	Masque de réseau
%S	Service (port)
%L	Réseau local
%H	Nom d'hôte
%P	Protocole (TCP/UDP/ICMP etc.)

Des descriptions similaires peuvent être générées par des listes à séparateur virgule, par exemple des listes d'hôtes/listes d'adresses (%A10.0.0.1, 10.0.0.2) ou par des sélections séparées par un trait d'union telles que des listes de ports (%S20-25). Un '0' ou une chaîne vide désigne l'objet 'any' :

tous les ordinateurs : %A0.0.0.0

tous les services : %S0

tous les protocoles : %P0

Les noms d'hôtes ne peuvent être utilisés que si le *LANCOM* peut convertir les noms en adresses IP. A cet effet, les noms doivent avoir été déclarés au *LANCOM* via DHCP ou NetBIOS, ou les liens doivent être enregistrés de façon statique dans la table DNS ou de routage IP. (Un enregistrement dans la table de routage IP peut affecter un réseau entier à un nom d'hôte.)

La liste des filtres

La liste des filtres est formée sur la base de la table des objets et de la table des règles. Elle est la conjonction de tous les filtres définis par les règles et les objets.



Nous attirons votre attention sur le fait que les filtres ne sont pas générés en cas de saisie incorrecte et qu'aucun message d'erreur ne vous en avertit. Si vous configurez les filtres manuellement, vérifiez ensuite si les filtres souhaités ont été générés.

1.3.1

Configuration des filtres

Les filtres pare-feu peuvent être configurés de plusieurs manières :

- *WEBconfig*
Installation complète ► Setup ► IP router module ► Firewall
- *LANconfig*
Routeur IP ► Filtre
- Telnet
/Setup/IP-router-module/Firewall

La configuration des filtres à l'aide de *ELSA LANconfig* est particulièrement conviviale. Le menu 'Filtre' vous permet d'accéder aux onglets ci-dessous servant à définir les règles de filtrage.



Notez que dans le cas de la configuration avec LANconfig, les tables d'objets qui ont été configurées avec telnet ou avec WEBconfig ont une forme modifiée après l'enregistrement des données.

- Général

Le nom du service de filtrage est fixé ici, ainsi que l'action appliquée aux paquets de données.

- Stations

Cet onglet sert à indiquer les stations émettrices ou de destination auxquelles la règle de filtrage doit s'appliquer.

- Services

Les protocoles IP ainsi que les ports source et cible auxquels la règle de filtrage doit s'appliquer sont fixés ici.

1.4

Module HTTP

Le module HTTP permet de fixer la racine des documents pour les fichiers d'aide HTML. Par défaut, le lien de l'aide renvoie aux pages Web d'ELSA. Pour déposer les fichiers d'aide sur un disque local, entrez le répertoire de ces fichiers.



La version à jour de l'aide HTML peut être téléchargée depuis le site Web d'ELSA.

1.5

Client DHCP

Avec la version 2.10 du microprogramme, les périphériques peuvent aussi obtenir une adresse IP automatiquement d'un serveur DHCP installé dans le réseau. Le menu 'Setup/DHCP-module/Operating' contient à cet effet des fonctions supplémentaires :

En mode 'Auto', le périphérique recherche d'autres serveurs DHCP dans le réseau. Lorsqu'il en trouve un, le propre serveur DHCP n'est pas activé et le périphérique obtient une adresse IP du serveur trouvé. Mais ceci n'est le cas que si le périphérique lui-même n'est pas encore configuré, c'est-à-dire si aussi bien l'adresse Internet que l'adresse Intranet sont encore 0.0.0.0. Dès qu'une opération de configuration est effectuée, l'adresse attribuée automatiquement n'est plus valable.

1.6

Etat HTTP

Avec la version 2.10 du microprogramme, la configuration de HTTP est également dotée d'un menu d'état. Sous /Status/TCP-IP-statistics/HTTP-statistics, vous trouverez les informations suivantes :

HTTP-access	Nombre total d'accès aux pages
HTTP-notfound-errors	Nombre d'accès à des pages inexistantes sur le périphérique
HTTP-authentication-errors	Nombre d'accès refusés en raison d'un mot de passe manquant ou erroné
HTTP-protocol-errors	Nombre d'accès auxquels le périphérique n'a pas pu répondre en raison d'une requête HTTP inconnue ou non valable (par exemple l'envoi de valeurs via une connexion en lecture seule)

La commande 'Delete-values' remet tous les compteurs à zéro. Cette action est aussi exécutée implicitement dans le cas d'un 'Delete values' dans le menu TCP/IP.

