Digi TransPort PCI Compliance Configuration Guide

Steps to Ensure the Digi TransPort follows PCI Compliance Standards

July 23, 2009

Patrick W. Brannelly, Sales Engineer

Digi International

Contents

Figures

1 Introduction

The following is a short guide to configuring the Digi TransPort according to Payment Card Industry Data Security Standards.

When configured properly, the Digi TransPort can be made part of a PCI Complaint network because it supports:

- Stateful Firewall
- Encryption via VPN
- Ability to segment networks so the credit card traffic is separate from other traffic
- MAC filtering on Ethernet ports
- Full Event Logging capabilities on device and router configuration control via Remote Manager
- Multiple users with various access levels (including read-only)

NOTE: *It is up to the user to configure any network device to be PCI DSS compliant!*

The succeeding sections will describe and show examples of the above-listed configuration options.

References: Please refer to the Digi TransPort User Guide available via http://www.digi.com/support (current link as of this writing is http://ftp1.digi.com/support/documentation/90001019_B.pdf).

2 Stateful Firewall

The Digi TransPort contains a sophisticated scripted "Stateful Firewall" and "Route Inspection" (SF/RI) engine. Stateful inspection is a powerful tool that allows the unit to keep track of a TCP/UDP or ICMP session and match packets based on the state of the connection on which they are being carried. In addition to providing sophisticated firewall functionality the SF/RI engine also provides a number of facilities for tracking the "health" of routes, marking "dead" routes as being Out Of Service (OOS) and creating rules for the automatic status checking of routes previously marked as OOS (for use in multilevel backup/restore scenarios).

Section Nine of the Digi TransPort User Guide explains the functionality and configuration syntax and is recommended reading prior to configuring the firewall.

This section shows a basic example of the script and is not intended to demonstrate complete PCI compliance as it pertains to the firewall. Full PCI compliance will depend on the type of traffic and connection specific to the user.

Configuration of the firewall consists of creating the **fw.txt** file, which contains the rules used by the TransPort router. The fw.txt file can be created in the web user interface or can be written in plain text

and imported to the router via FTP. The firewall is then enabled on the applicable interfaces by selecting the Firewall "ON" setting, shown here in figure 2-1:

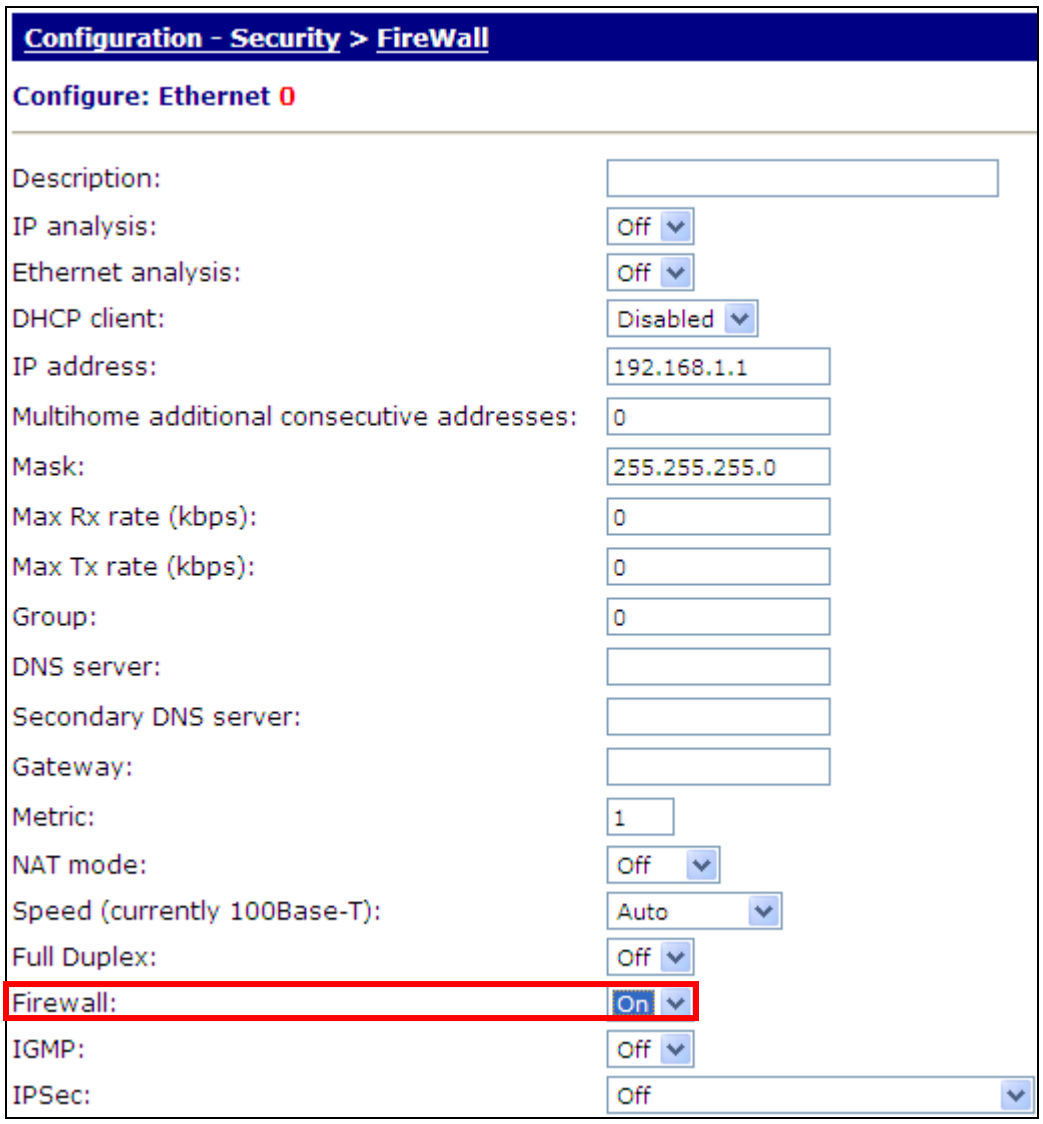

Figure 2-1: Enabling the Firewall on Eth 0

When configuring the firewall using the web interface, the rules are inserted and then saved to the fw.txt file.

In the following example, the two rules will allow certain traffic to certain Ethernet ports. Rule one allows traffic on TCP port 443 (HTTPS) through interface Eth0. Rule two allows traffic on port 80 (HTTP) through interface Eth 1. Since there is an implicit deny in place, no other traffic will pass through interface Eth 3, which in this example is the gateway. Figure 2-2 shows the rules as written in the firewall:

```
H:0 1) pass in break end on eth 3 proto tcp from any to addr-eth 0 port=443 inspect-state

H:0 2) pass in break end on eth 3 proto tcp from any to addr-eth 1 port=http inspect-state
```

Figure 2-2: Firewall Example One

Another example would be to translate the public IP address on interface Eth 3 to devices on the private LAN. In the following example, all traffic going to port 8080 (HTTP) is allowed pass. Telnet traffic is also allowed to pass. This allows the user to access the router using the web browser or Telnet software. Rules three and four translate ftp and other traffic sent to Eth 3's IP address to a device on the LAN with the IP address of 192.168.1.100. Depending on how the network is configured, this could be a DMZ, or a the device could be a member or one Local Area Network (LAN). Rule five passes all other traffic not defined in the top four rules. Figure 2-3 shows this example:

```
H:0 1) pass in break end on eth 3 from any to any port=8080 inspect-state

H:0 2) pass in break end on eth 3 from any to any port=telnet inspect-state

H:0 3) pass in break end on eth 3 proto ftp from any to addr-eth 3 port=ftpcnt -> to 192.168.1.100

H:0 4) pass in break end on eth 3 from any to addr-eth 3 -> to 192.168.1.100

H:0 5) pass break end
```

Figure 2-3: Firewall Example Two

3 VPN Encryption

VPN configuration will vary depending on the device on the end of the connection. VPN configuration varies from vendor to vendor. For specific instructions, see the applicable Application Note for the particular device and the Digi TransPort User Guide.

The Digi TransPort supports IPSec, PPTP and L2TP VPNs. Under IPSec, it supports the following:

1. Pre-shared key:

   A pre-shared key requires both the remote and host system (initiator and responder) share a secret key, or password, that can be matched by the responder to the initiator calling in.

2. RSA Signatures (X.509 Certificates):

   Certificates provide a mechanism like pre-shared keys, but without the need to manually enter or distribute secret keys. A user's certificate acts a little like a passport providing proof that the user is who they say they are and enclosing details of how to use that certificate to decrypt data encoded within. To prove the certificate has been properly issued and hasn't been changed, the user's name is embedded in code in a long string of numbers.

3. XAUTH:

   A single pre-shared key can be used for many remote VPN users but each user can have their own username and password. When using XAUTH, the head-end unit can be configured to authorize the username and password against a local table or an external device using RADIUS or TACACS for example.

3.1 VPN Configuration

In this example, the Digi TransPort will create an IPsec tunnel to a remote VPN device and is designated as the VPN Initiator. As such it will be configured to match the parameter ranges of the VPN Responder.

The steps for configuration are:

1. Configure the IKE 0 (Initiator)
2. Configure the Eroute (IPsec tunnel)
3. Configure any settings pertaining to the authentication method:
   a. Pre-shared Key uses a user account which acts as the pre-shared key
   b. RSA signatures invoke the use of X.509 certificates (an explanation and configuration instructions can be found in Section 7 of the Digi TransPort User Guide)

3.1.1 Configure IKE

The IKE instance is set with the parameters of the VPN tunnel, and figure 3-1 shows an example. Some settings, such as "Aggressive Mode" are added, but are not always necessary. For troubleshooting

purposes, it is a good idea to enable debugging at level “Very High” when trying to connect the first time. It can be disabled later, if debugging is no longer needed. This configuration page is located at ***Configuration - VPN>IPSec >IKE>IKE 0.***

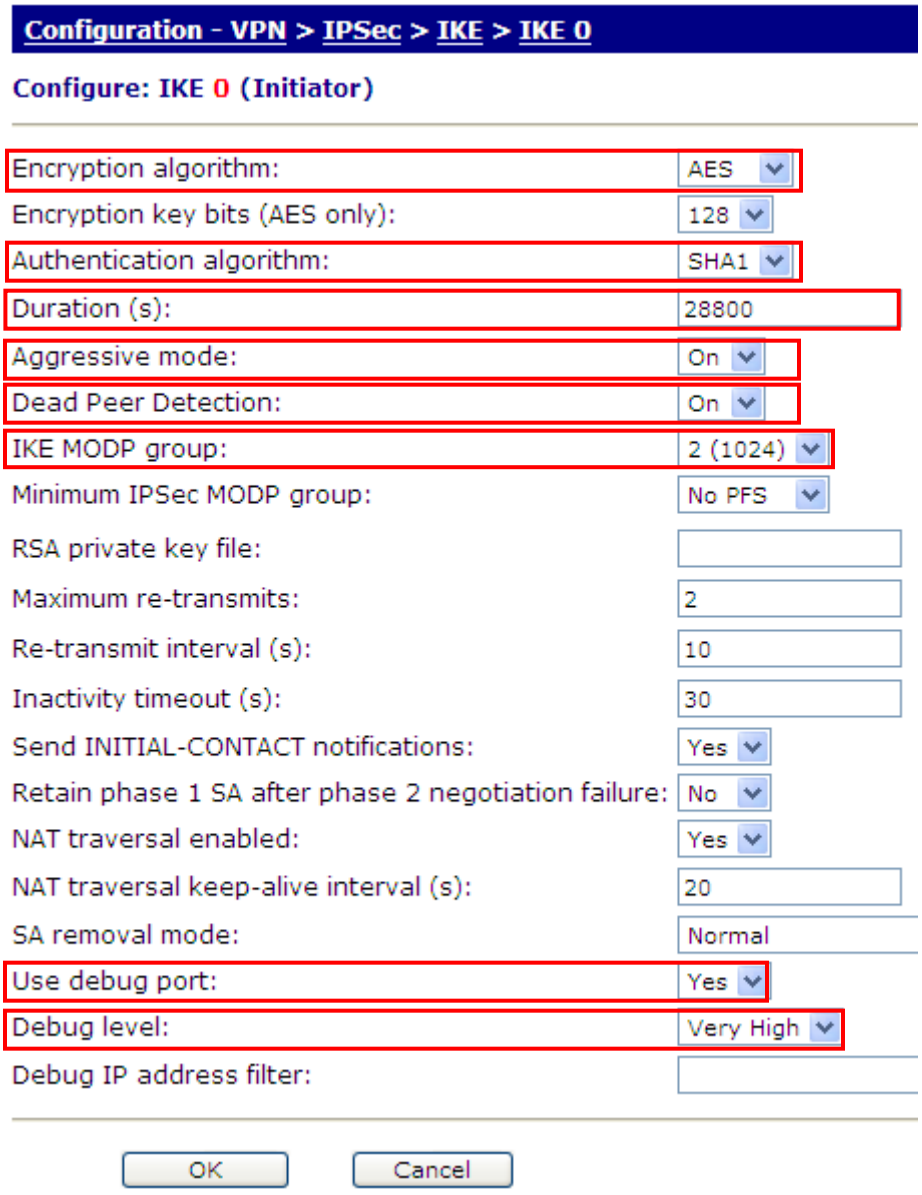

Figure 3-1: IKE Responder Configuration

3.1.2 Configure Eroute 0

The Eroute is where the Peer IP, Peer ID, local and remote subnets, etc. are configured. The following is a list of most common parameters with example settings:

1. Peer IP
2. Peer ID

3. Our ID:
4. Local Subnet IP address
5. Local Subnet mask
6. Remote Subnet IP address
7. Remote Subnet mask
8. Mode: Tunnel
9. ESP authentication algorithm
10. ESP encryption algorithm
11. Duration (s): 28800
12. Duration (kb): 0
13. No SA Action: Use IKE
14. Create SA's automatically: Yes. Route with matching interface required (for Always-on settings)
15. Authentication method

The configuration page is located at ***Configuration - VPN > IPSec > IPSec Eroutes > Eroute 0 - 9 > Eroute 0*** and Figure 3-2 shows these settings:

Configuration - VPN > IPSec > IPSec Eroutes > Eroute 0 - 9 > Eroute 0

Configure: IPSec EROUTE 0

Description:	
Peer IP/hostname:	67.177.44.106
Backup peer IP:	
Peer ID:	digivc7400
Our ID:	digitransportsr
XAUTH ID:	
RSA private key file:	
Send our ID as FQDN:	No
Interface to use for local subnet IP address:	None
Interface # to use for local subnet IP address:	0
Local subnet IP address:	172.16.2.0
Local subnet mask:	255.255.255.0
Local subnet IP address to negotiate (if different from above):	
Local subnet mask to negotiate (if different from above):	
Negotiate virtual local IP address using MODECFG (initiators only):	No
Remote subnet IP address:	192.168.1.0
Remote subnet mask:	255.255.255.0
Remote subnet ID:	
Local port:	0
Remote port:	0
TX packets with these TOS values through this eroute:	
First local port (IKEv2 only):	0
Last local port (IKEv2 only):	65535
First remote port (IKEv2 only):	0
Last remote port (IKEv2 only):	65535
Mode:	Tunnel
AH authentication algorithm:	Off

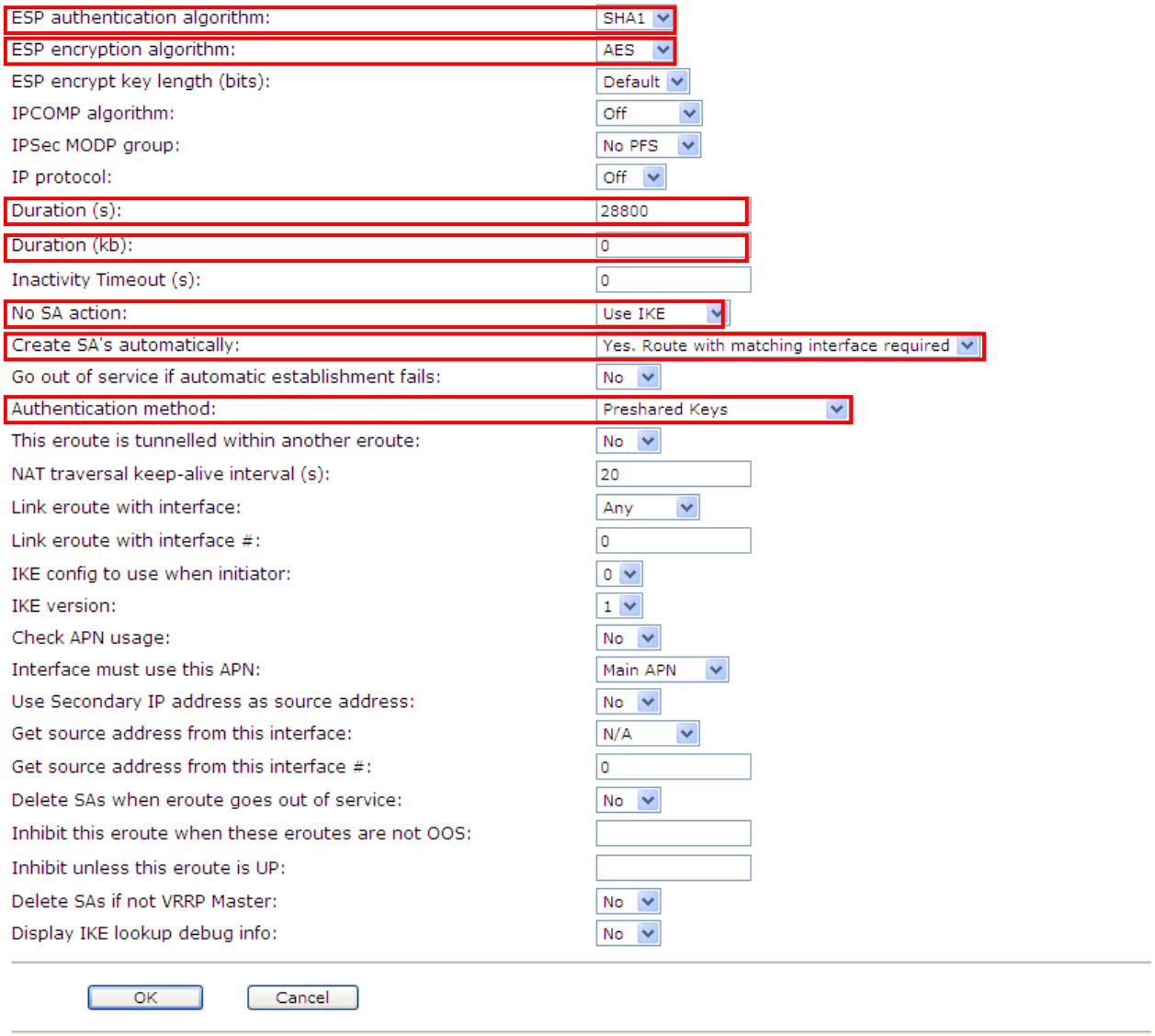

Figure 3-2: Eroute 0 Configuration

3.1.3 Configure the User/Pre-shared Key

The Digi TransPort uses a user account for the pre-shared key. In this example, User 10 was used. The page is located at ***Configuration - Security > Users > User 10 - 19 > User 10***. The steps are to configure the name, password and access level. The name is the peer ID and the password is the pre-shared key and the access level is "None".

In a normal setting, it is advisable to use a pre-shared key of at least 10 characters, ideally with random upper and lower case characters. Use of a dictionary word could potentially be cracked in a matter of seconds. The password in this example is for simplicity, and is not recommended in a production environment.

For this application note, the name is “digivc7400” and the password is “transport”. Figure 3-5 demonstrates this:

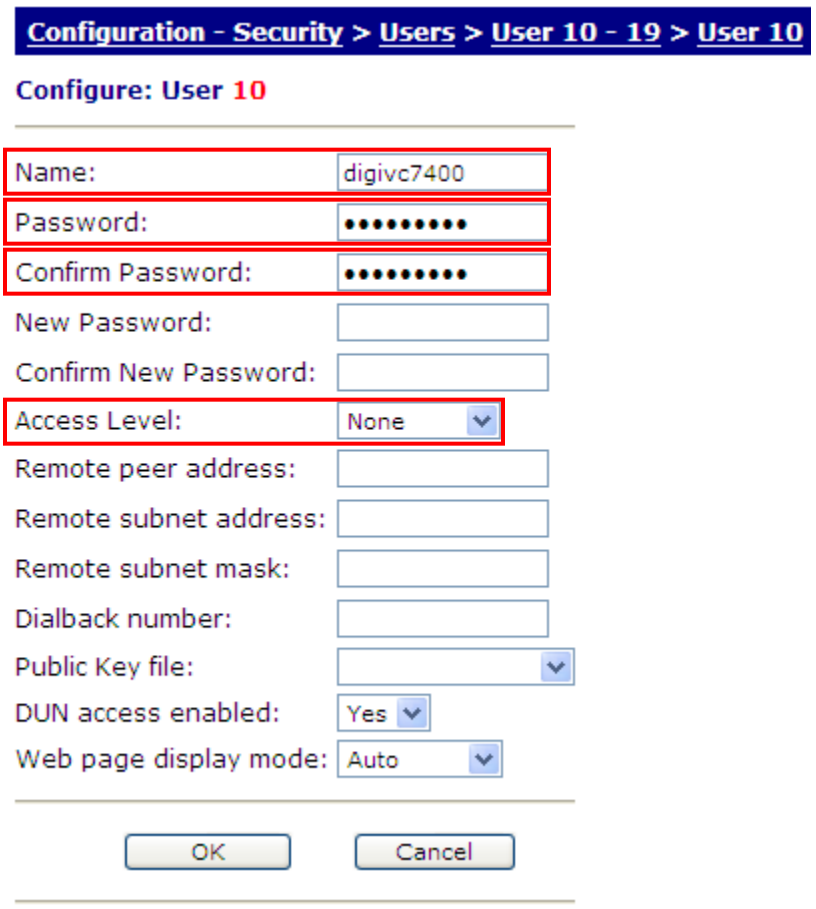

Figure 3-3: User 10/Preshared Key Configuration

3.1.4 Using X.509 Certificates

Certificates are held in non-volatile files on the unit. Any private files are named privxxxx.xxx and cannot be copied, moved, renamed, uploaded or typed. This is to protect the contents. They can be overwritten by another file, or deleted.

Two file formats for certificates are supported:

• PEM – Privacy Enhanced MIME

• DER – Distinguished Encoding Rules

Certificate and key files should be in one of these two formats, and should have an extension of “.pem” or “.der” respectively.

The unit maintains two lists of certificate files. The first is a list of “Certificate Authorities” or CAs. Files in this list are used to validate public certificates sent by remote users. Public certificates must be signed

by one of the certificates in the CA list before the unit can validate them. Certificates with the filename CA*.PEM and CA*.DER are loaded into this list at start-up time. In the absence of any CA certificates, a public certificate cannot be validated.

The second list is a list of public certificates that the unit can use to obtain public keys for decrypting signatures sent during IKE exchanges. Certificates with a filename CERT*.PEM and CERT*.DER are loaded into this list when the unit is powered on or rebooted. Certificates in this list will be used in cases where the remote unit does not send a certificate during IKE exchanges. If the list does not contain a valid certificate communication with the remote unit cannot take place.

Both the host and remote units must have a copy of a file called CASAR.PEM. This file is required to validate the certificates of the remote units.

In addition, the host unit should have copies of the files CERT02.PEM (which allows it to send this certificate to remote units) and PRIVRSA.PEM. Note that before it can send this certificate, the "Responder ID" parameter in the ***Configuration - VPN > IPSEC > IKE*** page must be set to "host@Digi.co.uk".

The remote unit must have copies of CERT01.PEM and PRIVRSA.PEM. In addition, any Eroutes that are going to use certificates for authentication should be configured as follows:

3.1.4.1 Our ID

The "Our ID" setting should be set to "info@Digi.co.uk". This is the same as the subject "Altname" in certificate CERT01.PEM which makes it possible for the router to locate the correct certificate to send to the host.

> ***Note:*** *The equivalent filename extension for .PEM files in Microsoft Windows is ".CER". By renaming ".PEM" certificate files to ".CER", it is possible to view their makeup under Windows.*

3.1.4.2 Authentication Method

The authentication method should be set to RSA Signatures. This indicates to IKE that RSA signatures (certificates) are to be used for authentication.

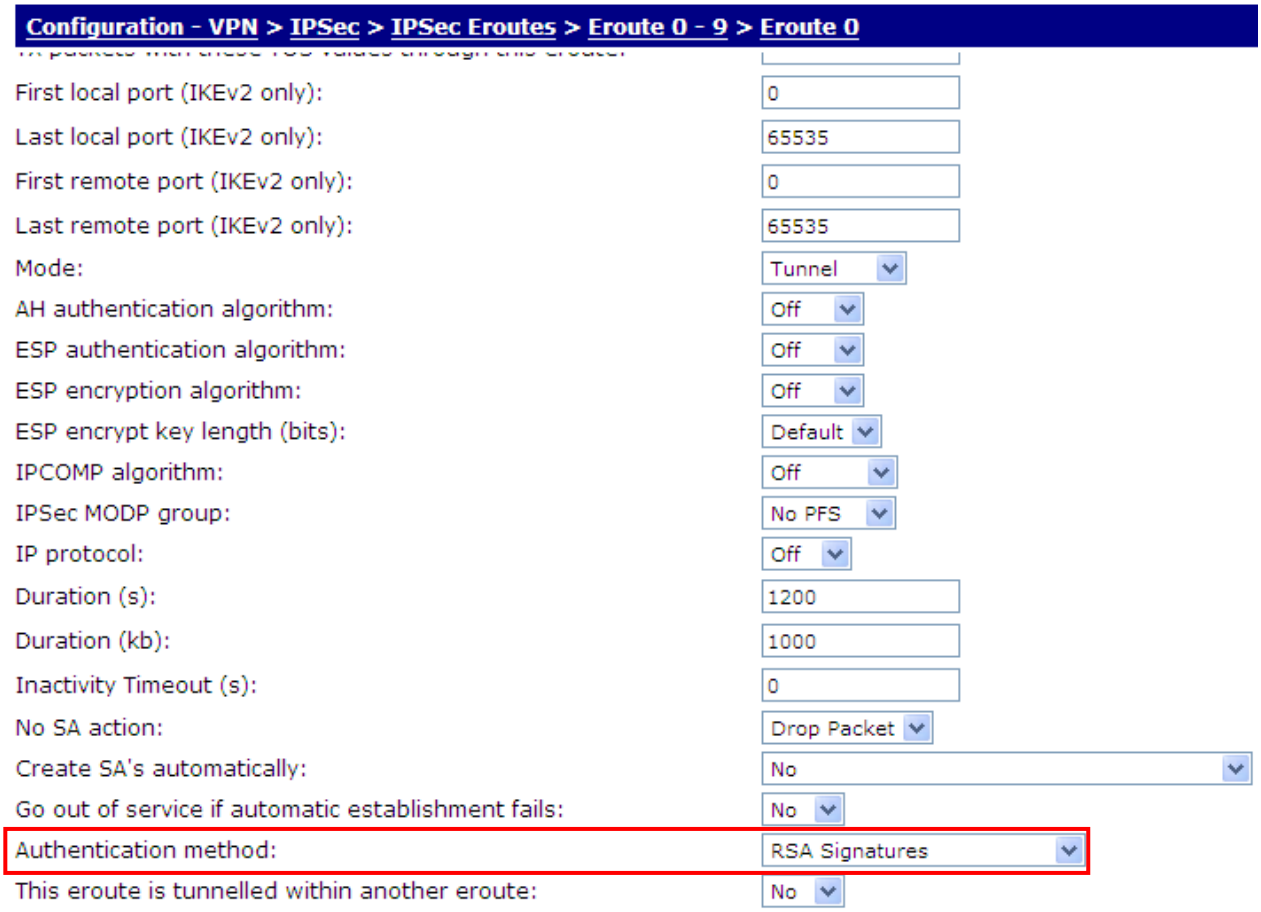

Figure 3-4: RSA Signature Authentication

When IKE receives a signature from a remote unit, it needs to be able to retrieve the correct public key so it can decrypt the signature and confirm the signature is correct. The certificate must either be on the FLASH file system, or be provided by the remote unit as part of the IKE negotiation. The ID provided by the remote unit is used to find the correct certificate to use. If the correct certificate is found, the code then checks it has been signed by one of the certificate authority certificates (CA*.PEM) existing on the unit. The code first checks the local certificates, then the certificate provided by the remote (if any). IKE will send a certificate during negotiations if it is able to find one containing the subject "AltName" matching the ID being used. If it is not able to locate the certificate, the remote must have local access to the file so the public key can be retrieved.

A typical set-up may be the host unit has a copy of all certificates. This means the remote units only require the private key and the Certificate Authority certificate. This eases administration as any changes to certificates need only be made on the host. Because typically they do not have a copy of their certificate, remote units rely on the host having a copy. An alternative however, is the remote units all have a copy of the certificate, the private key and certificate authority certificate, and the host only has its own certificate. This scenario requires the remote unit send its certificate during negotiations. It can validate the certificate because it has the certificate authority certificate.

4 Network Segmentation

The Digi TransPort supports three methods of network segmentation, or in other words, the ability to separate the different streams of traffic passing through the router. They are:

1. VLANs
2. Groups
3. Port Isolate Mode

NOTE: Groups and Port Isolation are only available on Digi TransPort routers with multiple Ethernet ports. VLAN tagging is supported on all models.

4.1 VLANs

The Digi TransPort supports 802.1q Virtual Local Area Networks (VLAN).

The ***Configuration - Interfaces > Ethernet > VLANs*** page contains a table that contains VLAN IDs, Ethernet Instances, IP Addresses and Subnet Masks with which to base VLAN tagging. Figure 7 shows the VLAN configuration page and each parameter is described below:

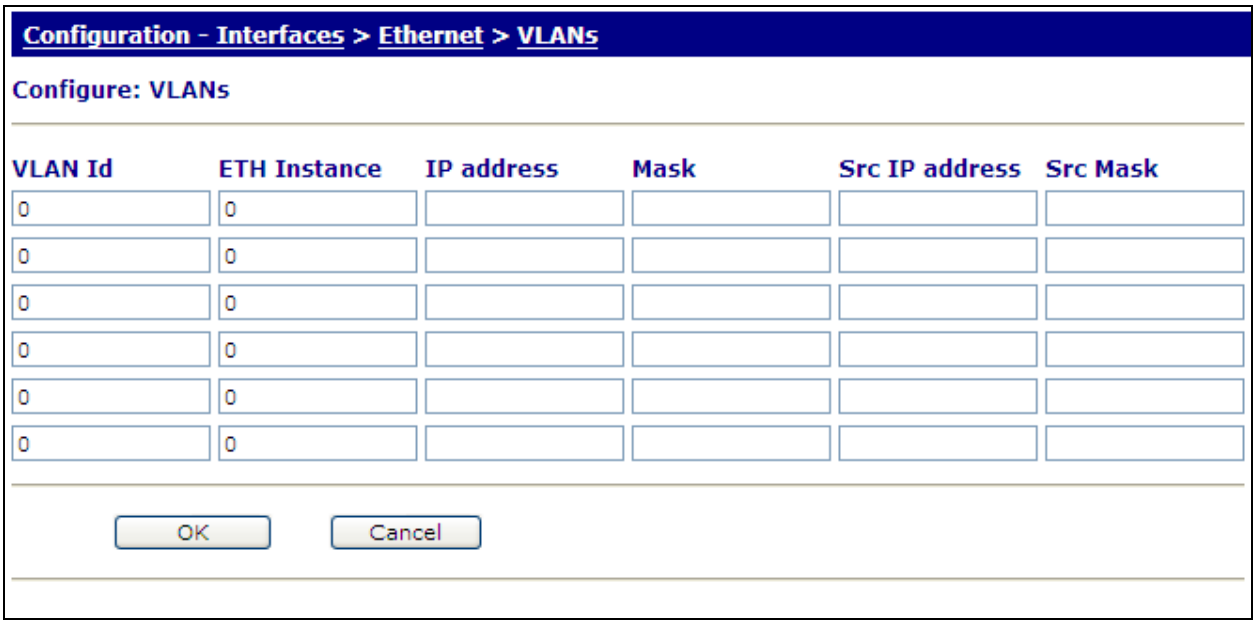

Figure 4-1: VLAN Configuration

VLAN ID: The ID of the Virtual LAN. This parameter is used in the TCP header to identify the destination VLAN for the packet.

ETH Instance: The Ethernet port that will tag the outgoing packets. Only packets sent from this interface will have VLAN tagging applied.

IP Address: The destination IP address. If this field is filled in, only packets destined for this IP address will have VLAN tagging applied.

Mask: The destination IP subnet mask. If this field is filled in, only packets destined for this IP subnet mask will have VLAN tagging applied.

Src IP Address: The source IP address. If this field is filled in, only packets from this IP address will have VLAN tagging applied.

Src Mask: The source IP subnet mask. If this field is filled in, only packets from the network range/space specified by the combination of the specified Src Address and Src Mask will have VLAN tagging applied.

For the VLANs to take effect, VLAN tagging must be enabled on the applicable interfaces. This is done by setting the VLAN parameter to "ON" on the interface configuration page. Figure 8 demonstrates this:

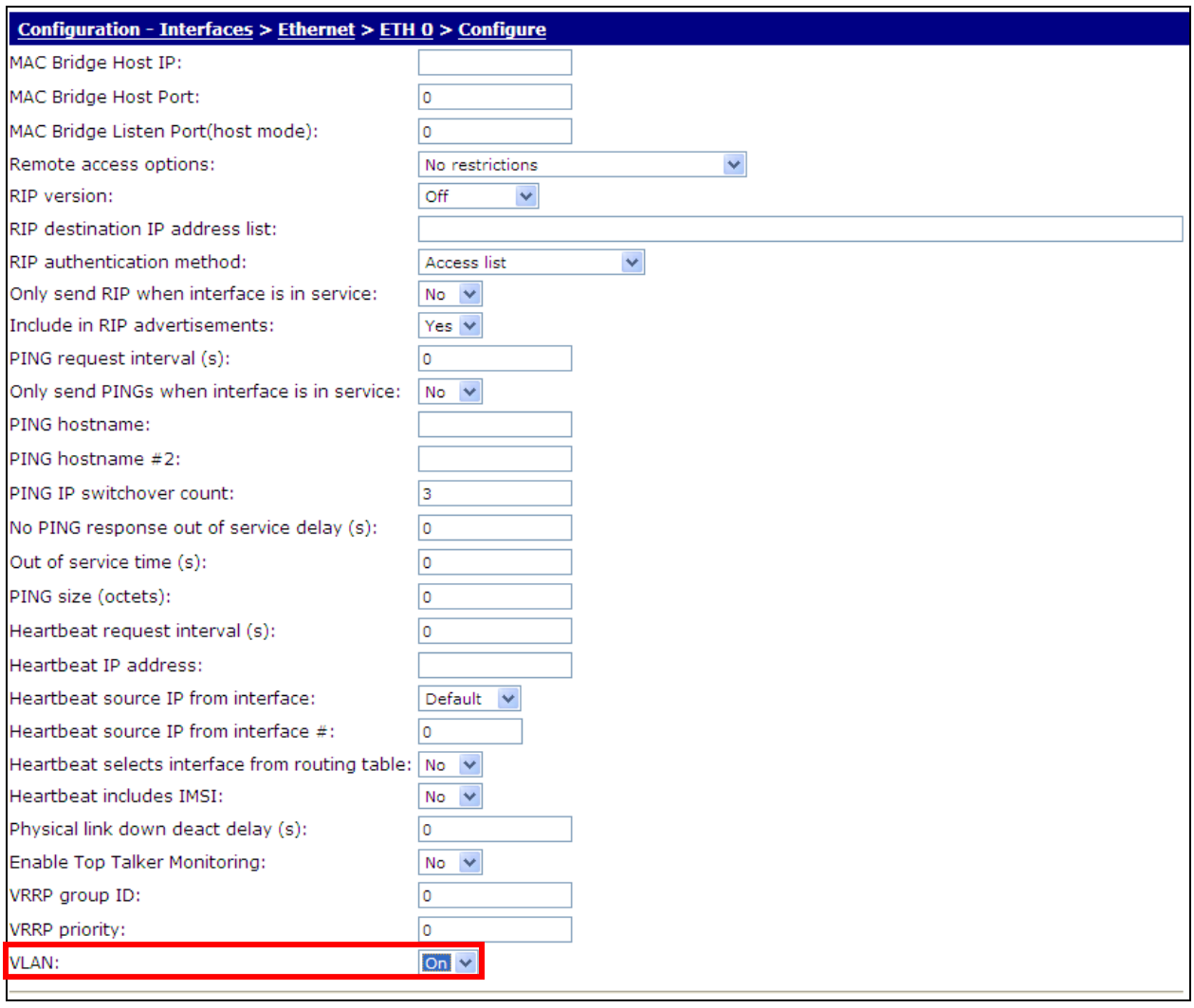

Figure 4-2: ETH 0 VLAN Parameter

4.2 Groups

The Group parameter for each port is normally set to 0. This means that all ports belong to the same switch. If required, the Group parameter may be used to isolate specific ports to create separate switches. For example, if Ethernet 0 and Ethernet1 are set to Group 0 whilst Ethernet 2 and Ethernet 3 are set to 1, the unit will in effect be configured as two 2-port switches instead of one 4-port switch. This means that traffic on physical ports "LAN 0" and "LAN 1" will not be visible to traffic on physical ports "LAN 2" and "LAN 3" (and vice versa). For the two groups to communicate, routing between them must be configured.

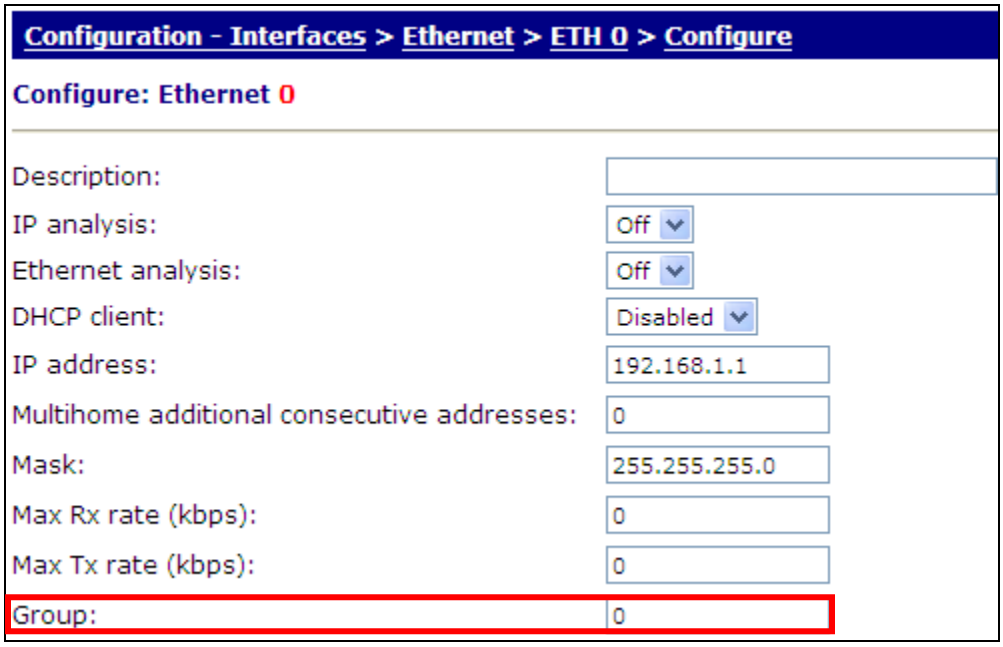

Figure 4-3: ETH 0 Group Configuration

This parameter is not available on the web page when the unit is configured for VLAN operation or is set to Port Isolate mode.

4.3 Port Isolate

On TransPort routers with more than one physical Ethernet port, the Ethernet instances refer to the different physical Ethernet ports. These units can be configured for either "HUB" mode or "Port Isolate" mode.

In HUB mode all the Ethernet ports are linked together and behave like an Ethernet hub or switch. This means that the router will respond to all of its Ethernet IP addresses on all of its ports (as the hub/switch behavior links the ports together).

In Port Isolate mode, as shown in figure 4-4 below, the router will only respond to its Ethernet 0 IP address on physical port "LAN 0", its Ethernet 1 IP address on physical port "LAN 1", etc. The router will not respond to its Ethernet 1 address on port "LAN 0" unless routing has been configured appropriately.

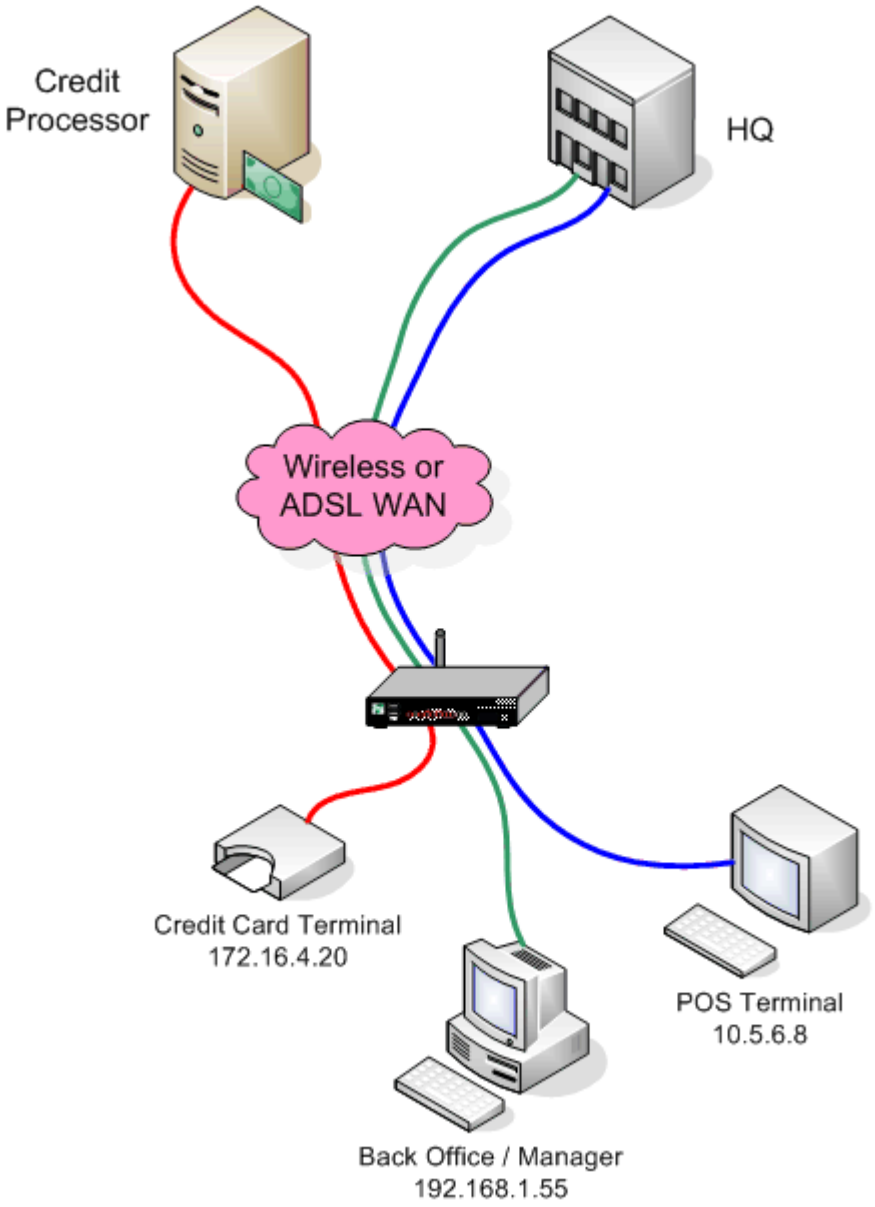

Figure 4-4: Port Isolation

In HUB mode all the Ethernet ports are linked together and behave like an Ethernet hub or switch. This means that the router will respond to all of its Ethernet IP addresses on all of its ports (as the hub/switch behavior links the ports together).

In Port Isolate mode the router will only respond to its Ethernet 0 IP address on physical port “LAN 0”, its Ethernet 1 IP address on physical port “LAN 1”, etc. The router will not respond to its Ethernet 1 address on port “LAN 0” unless routing has been configured appropriately.

When configured for HUB mode it is important that no more than one of the router's ports is connected to another hub or switch on the same physical network otherwise an Ethernet loop can occur. The default behavior is "HUB" rather than "Port Isolate".

To set the mode to either "HUB" or "Port Isolate", select the button at the bottom of any of the Ethernet configuration pages. When the router is in "HUB" mode, it will say "Change to Port Isolate Mode" on the button and vice versa. After selecting the mode change, the router must be rebooted before the change can take effect. Figure 4-4 shows an example of what the bottom of the Ethernet configuration page looks like in HUB mode and Figure 4-5 shows Port Isolate Mode

Figure 4-5: HUB Mode

Figure 4-6: Port Isolate Mode

5 MAC Filtering

MAC Filtering refers to a security access control methodology whereby the 48-bit address assigned to each network card is used to determine access to the network.

MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of lists.

MAC Filtering is configured in two areas of the web page:

Configuration–Interfaces>Ethernet>MAC Filters>

Configuration-Interfaces>Ethernet>

When MAC addresses are entered on the MAC Filters page, only these MAC addresses can access an Ethernet port where MAC filtering is enabled. The configuration page is as follows:

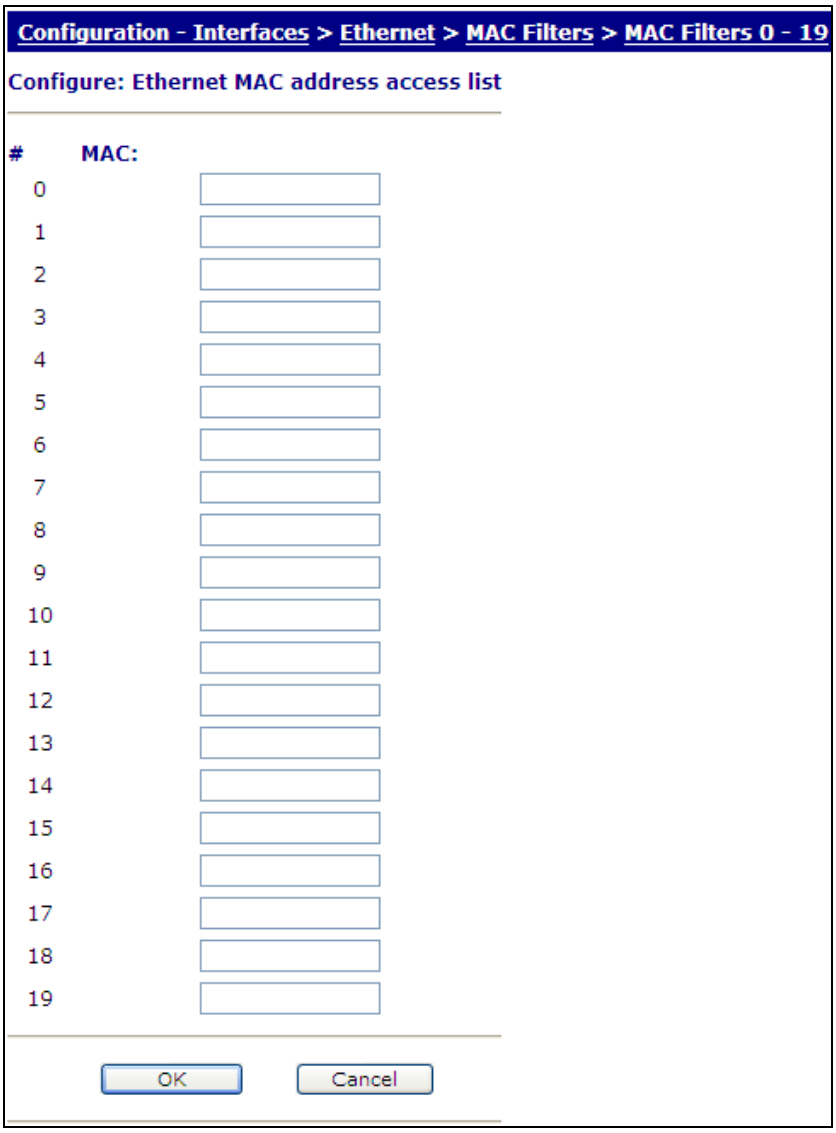

Figure 5-1: MAC Filter List

Enabling MAC filtering is accomplished changing the MAC Address Filtering setting to “ON” on the Ethernet port’s configuration page as shown below:

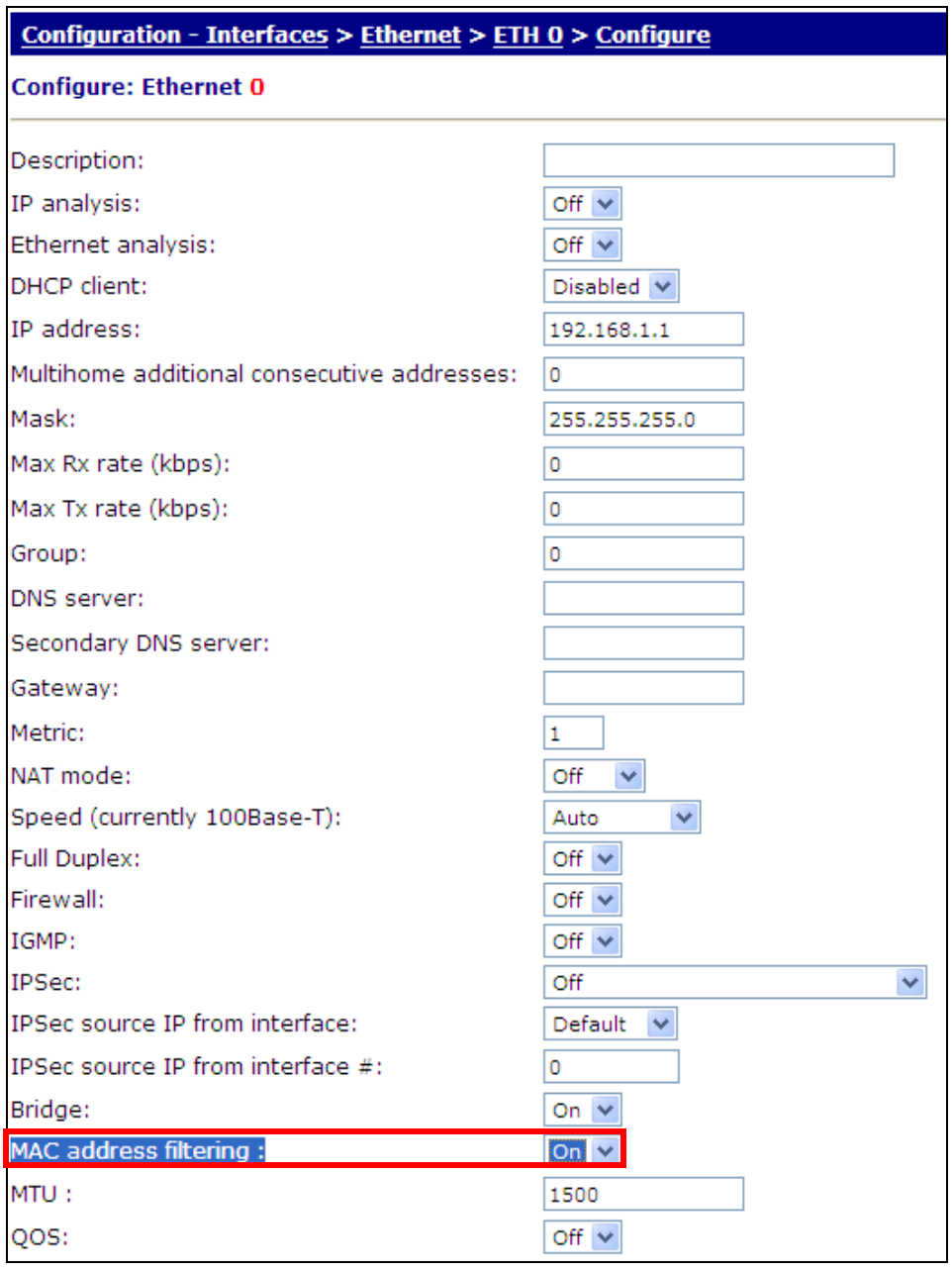

Figure 5-2: MAC Filter Enable

MAC filtering can also be accomplished in the CLI by using the macfilt command. *`macfilt 0 mac 00059a3c7800`* for example, would allow a device with the MAC address of 00059a3c7800 to access Ethernet 0. The next step is to enable MAC filtering by typing *macfilt ON*.

It is possible to allow a range of addresses by specifying only the significant portion of the MAC address in the table, e.g. *macfilt 0 mac 00042d* to allow packets from Digi units.

6 Event Handling

6.1 Event Logging

The unit maintains a log of certain types of event in the "EVENTLOG.TXT" pseudo file. When an event of a specified level (or higher) occurs, it can be configured to automatically generate and send an email alert message, or on W-WAN models an SMS alert message, to a pre-defined address.

All events can be appended to a second log file stored on a USB flash disk; this is useful for capturing a very large log file over an extended period. The size of the secondary log file is only limited by the size of the USB flash drive attached to the router.

The event log displays the contents of the "EVENTLOG.TXT" file with the most recent events listed at the top of the log. Each event log entry consists of the time and date of the event followed by a brief description. The information can be very useful in tracing and diagnosing fault conditions.

Event logging does not require configuration, although using the debug feature on the different interfaces, VPN tunnels, protocols, etc. can provide more information.

To view the event log in the web user interface, the page is Diagnostics-Event Log. It can also be viewed in the CLI by typing the command: *type eventlog.txt.* Finally, it can also be downloaded via FTP.

Figure 6-1 shows an example of the Event Log. In this example, the PPP1 interface is connected and then there are three login events, two are successful and one is a failure:

```
00:50:21, 13 Jul 2009,WEB Login OK by username lvl 0
00:50:13, 13 Jul 2009,Login failure by username: WEB
00:30:22, 13 Jul 2009,WEB Login OK by username lvl 0
00:22:48, 13 Jul 2009,WEB Login OK by username lvl 0
00:20:38, 13 Jul 2009,WEB Login OK by username lvl 0
00:18:54, 13 Jul 2009,PPP 1 up
00:18:54, 13 Jul 2009,PPP 1 Start IPCP
00:18:54, 13 Jul 2009,PPP 1 Start AUTHENTICATE
00:18:54, 13 Jul 2009,PPP 1 Start LCP
00:18:54, 13 Jul 2009,PPP 1 Start
```

Figure 6-1: Event Log Example

6.2 Syslog

The TransPort may be configured to deliver Syslog messages when events of a suitable priority occur. Up to five Syslog servers can be configured.

The TransPort supports the standard priority and facility selections:

Priority Selections:	Facility Selections:
0=Emergency 1=Alert 2=Critical 3=Error 4=Warning 5=Notice 6=Info 7=Debug	0=Kernel 1=User 2=Mail 3=System 4=Auth 5=Syslog 6=Lptr 7=Nnews 8=Uucp 9=Clock 10=Auth2 11=FTP 12=NTP 13=LOGAUDIT 14=LOGALERT 15=CLOCK2 16=LOCAL0 17=LOCAL1 18=LOCAL2 19=LOCAL3 20=LOCAL4 21=LOCAL5 22=LOCAL6 23=LOCAL7

7 Multiple User Configuration

The Digi TransPort allows up to 30 authorized users, which varies depending on the software build the unit is running. Each user has a password and an access level which determines access to the various facilities:

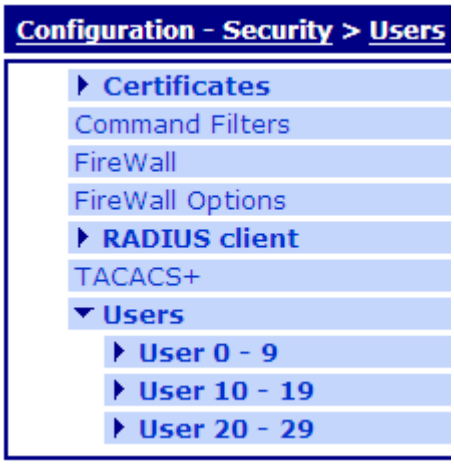

Figure 7-1: TransPort User Accounts

The *Configure* > *Users* > *User n* pages display the user settings:

Name: Enter a username of up to 14 characters.

Password: Enter a password for the user of up to 14 characters.

Confirm Password: Re-enter the Password in this field to confirm it.

New Password: When IKE is the initiator, the responder supplied HASH is checked using the normal password and the new password if that fails. The initiator will remember which password was successful, and use that password to create the HASH if it becomes the responder of some new negotiation. If the IKE becomes responder and IKE negotiations fail after supplying the HASH, the other password will be used during the next negotiation.

Confirm New Password: Re-enter the Password in this field to confirm it.

Access Level: Select the access level for the User. "Super" allows full access to all facilities.

"**Super**" is the highest level and gives the user administrative rights

"**High**" allows users to change some settings such as the time & date and to reconfigure the general operation of the unit. However, a High level user cannot change User settings.

"**Medium**" allows minimal ability to change settings and access to read-only commands.

"**Low**" allows the user access only the most basic and read-only commands.

"**None**" prohibits access to commands. It is used for pre-shared keys where only VPN authentication is needed and not access to the device itself.

"**Read-only**" give the user only rights to see the configuration, but make no changes.

"**Remote Peer Address & Remote Subnet Address**" In the event multiple PPP instances are enabled for answering and multiple remote routers can dial into the local router, static routes cannot always be used to ensure that packets which should be routed to the remote network are sent through the correct PPP interface. These parameters can be used in conjunction with the IP mask parameter to associate a network address with a user.

"**Remote subnet mask**" The remote subnet mask parameter is used in conjunction with the remote peer address parameter above to fully qualify the network address for the user.

"**Dialback number**" This parameter is used to specify a telephone number for the user in the event that "dial-back" is required.

"**Public Key file**" This parameter contains the filename of the file containing the public key for that user. If the public key matches the client supplied public key, the user is allowed access.

"**Web page display mode**" This parameter selects the default web view for a user.

Figure 7-2 demonstrates User 1's configuration:

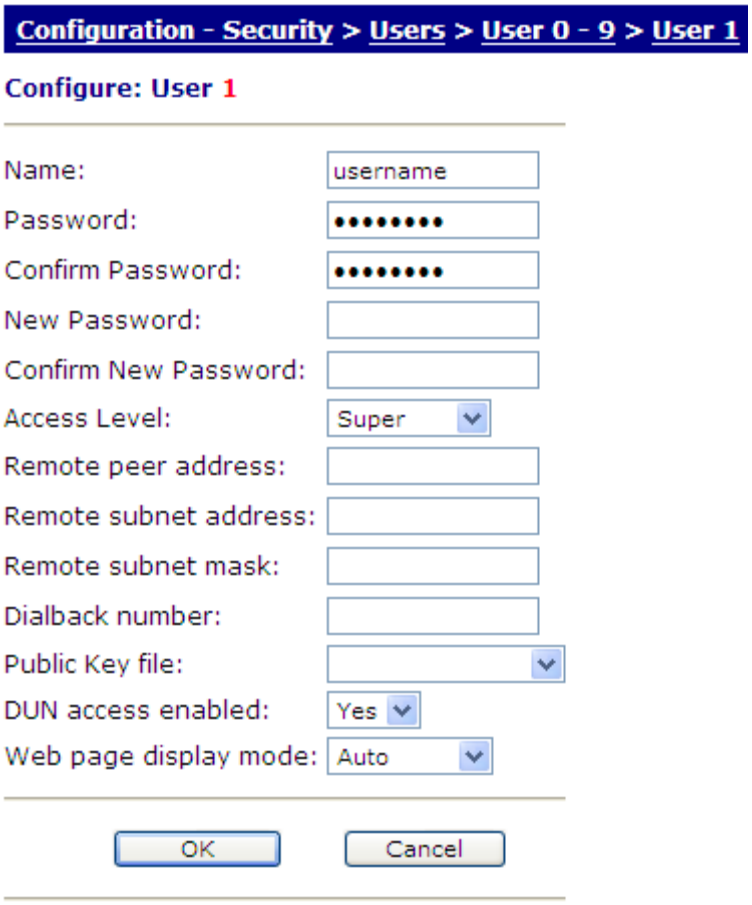

Figure 7-2: User 1 Configuration