



# Application Note 26

---

## Configure TransPort as an L2TP over IPsec Client

Digi Technical Support

July 2016

# Contents

1	Introduction.....	2
1.1	Outline.....	2
1.2	Assumptions.....	2
1.3	Corrections.....	3
1.4	Version and Revision History.....	3
2	L2TP Overview.....	3
3	L2TP Operation.....	3
4	Configuring L2TP/IPsec.....	4
4.1	Configuring PPP.....	5
4.2	Configuring L2TP.....	9
4.3	Configuring Ipsec.....	10
4.4	Configure the Ipsec Pre-shared key.....	13
4.5	Configuring a static route.....	14
4.6	Saving the configuration.....	14
5	Testing.....	15
6	Configuration Files.....	15
6.1	Digi Transport Configuration Files.....	15
6.2	Digi Transport Firmware Versions.....	16

## 1 INTRODUCTION

### 1.1 Outline

This document describes how to configure a TransPort to be an L2TP over IPsec client.

### 1.2 Assumptions

This guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product, and of the requirements for their specific application.

**Configuration:** This Application Note (AN) assumes that the router has a connection to the Internet using ADSL and interface PPP 1.

This AN applies to:

**Models shown:** Digi TransPort DR64 router.

**Other Compatible Models:** All Digi TransPort products.

**Firmware versions:** 5.123 and above.

**Configuration:** This AN assumes the devices are set to their factory default configurations. Most configuration commands are only shown if they differ from the factory default.

### 1.3 Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to: [tech.support@digi.com](mailto:tech.support@digi.com)

Requests for new ANs can be sent to the same address.

### 1.4 Version and Revision History

Version Number	Status
1.0	Published
1.1	Digi Transport branded
2.0	Updated for new web GUI

## 2 L2TP OVERVIEW

L2TP is a protocol-independent RFC standard protocol (RFC 2661) for encapsulating PPP data packets and passing them transparently across an IP internetwork.

L2TP has no encryption measures built into it and so it is often coupled with IPsec to provide an encrypted data tunnel across untrusted IP networks.

L2TP/IPsec has become a popular successor to PPTP in the 'Access VPN' arena, mainly due to its ability to utilise encryption and the fact that it is built into Windows 2000/XP and newer Operating Systems and available as a free option for older NT4/98/ME systems.

## 3 L2TP OPERATION

When sending data to an L2TP/IPsec host, the data is encapsulated many times in a similar way to the normal encapsulation of segments, packets and frames:

Data Description				
Plain IP Data				IP Data
				↓

IP Data inside PPP			PPP	IP Data
			↓	
PPP Data inside L2TP		L2TP	PPP	IP Data
		↓		
L2TP data encrypted inside Ipsec	Ipsec	L2TP	PPP	IP Data

We can take for example a PC wanting to send data across an L2TP/IPsec connection to a VPN host through a TransPort attached via Ethernet.

When data is seen for the subnet on the other side of the VPN tunnel, it will leave the PC via its default gateway and be routed by the TransPort to the PPP instance specified in the routing table.

This PPP instance is configured to use L2TP as its transport, and in turn L2TP will encapsulate the PPP data and forward it to the VPN host's IP address.

This L2TP data is then encrypted by IPsec as specified by an eroute which encrypts any traffic destined for the VPN host's IP address.

This encrypted data then passes to the Internet via whatever IP connection is specified either LAN/ISDN/GPRS/POTS where it can be received by the VPN host.

This example Event Log trace (to be read from the bottom up) shows the establishment of the L2TP/IPsec connection after a packet received from the PC destined for the VPN Host's network.

```

12:26:20, 17 Nov 2009, PPP 5 up
12:26:18, 17 Nov 2009, PPP 5 Start IPCP
12:26:17, 17 Nov 2009, PPP 5 Start AUTHENTICATE
12:26:14, 17 Nov 2009, PPP 5 Start LCP
12:26:14, 17 Nov 2009, PPP 5 Start
12:26:14, 17 Nov 2009, L2TP Call 0 up
12:26:13, 17 Nov 2009, L2TP Tunnel 0 up
12:26:02, 17 Nov 2009, New Ipsec SA created by 194.213.214.120
12:26:01, 17 Nov 2009, New Phase 2 IKE Session, Initiator
12:25:59, 17 Nov 2009, IKE Keys Negotiated
12:25:56, 17 Nov 2009, New Phase 1 IKE Session, Initiator
12:25:56, 17 Nov 2009, IKE Request Received From Eroute 0
12:25:55, 17 Nov 2009, GP socket connected: l_port[1701] r_ip[194.213.214.120]
r_port[1701]
12:25:55, 17 Nov 2009, IP Act_Rq to PPP 5-0: s_ip[192.168.0.1]
d_ip[192.168.10.12]

```

It is possible to use a TransPort as an L2TP client to an existing Access VPN service such as Microsoft 2003 Server RAS service, although you will need to enable the standard CHAP-MD5 authentication rather than the Microsoft proprietary MS-CHAP authentication.

## 4 CONFIGURING L2TP/IPSEC

There are four steps to configuring the TransPort as an L2TP/IPsec client.

1. Configuring a PPP Instance to use.
2. Configuring an L2TP instance.
3. Configuring an IPsec Eroute.

4. Configuring a static route.

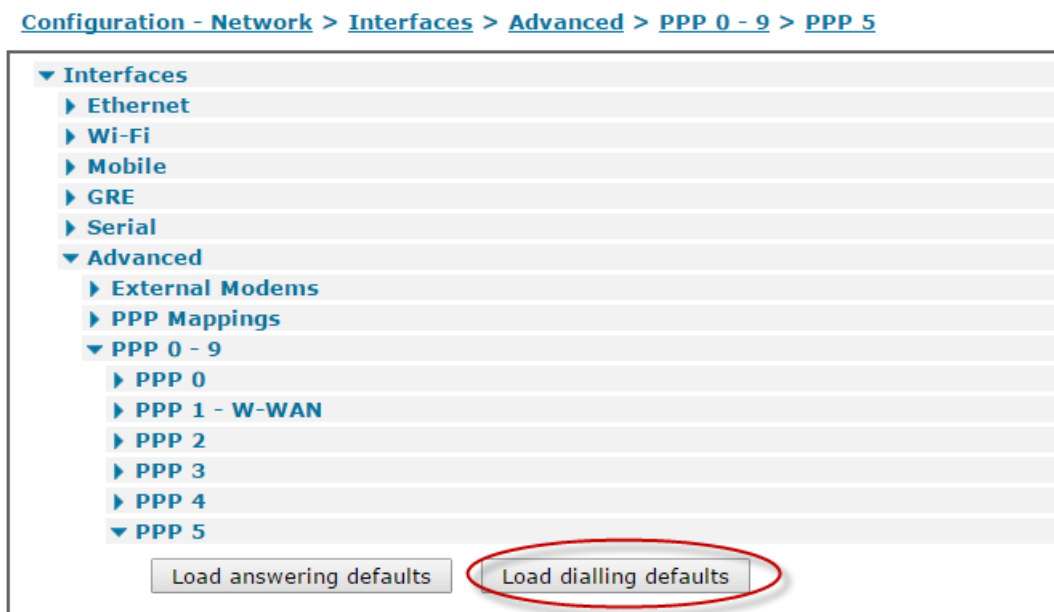
## 4.1 Configuring PPP

Choose a PPP instance for the L2TP connection to use. Note that this should be separate from any other PPP instances such as those used to dial an ISP.

Ideally choose PPP 5 or higher since lower numbered PPP instances are preconfigured for other interfaces.

Navigate to **Configuration – Network > Interfaces > Advanced > PPP 0 – 9 > PPP 5**

Click on **Load dialling defaults** then scroll down and click **Apply**.



Then return to the PPP settings and enter the following parameters:

[Configuration - Network > Interfaces](#)

The screenshot shows a configuration page for PPP interfaces. The left sidebar lists various interface types: Ethernet, Wi-Fi, Mobile, GRE, Serial, and Advanced. Under Advanced, there are sub-sections for External Modems, PPP Mappings, and PPP 0-9. The PPP 5 section is expanded, showing fields for dial out numbers, prefix, username, password, and confirm password. The values entered are 012345, an empty field, vpn.user.id, and two masked password fields. There are also buttons for 'Load answering defaults' and 'Load dialling defaults', and a 'Description:' field.

Click the **Apply** button to confirm these settings.

Parameter	Setting	Description
Dial out using numbers	012345	A Dummy Value
Username	vpn.user.id	VPN Username
Password	vpn.user.pass	VPN Password

### Optional PPP configuration for IP addressing:

**NOTE:** If unsure, do not configure this. Allow the VPN responder to assign an IP address.

If you are going to be using a fixed IP address to the VPN host instead of a negotiated one, enter it in the following fields:

[Configuration - Network](#) > [Interfaces](#) > [Advanced](#) > [PPP 0 - 9](#) > [PPP 5](#)

Serial

Advanced

External Modems

PPP Mappings

PPP 0 - 9

PPP 0

PPP 1 - W-WAN

PPP 2

PPP 3

PPP 4

PPP 5

Load answering defaults Load dialling defaults

Description:

This PPP interface will use

Dial out using numbers:

Prefix:  to the dial out number

Username:

Password:

Confirm password:

Allow the remote device to assign a local IP address to this router

Try to negotiate to use  as the local IP address for this router

Use  as the local IP address for this router (i.e. not negotiable)

Use mask  for this interface

Click **Apply** to confirm these settings.

Parameter	Setting	Description
local IP address	192.168.10.1	Fixed IP address example <b>(Optional)</b>
mask	255.255.255.0	Fixed mask example <b>(Optional)</b>

Next, select L2TP as the transport for this PPP instance:

[Configuration - Network](#) > [Interfaces](#) > [Advanced](#) > [PPP 0 - 9](#) > [PPP 5](#)

- ▼ Interfaces
  - ▶ Ethernet
  - ▶ Wi-Fi
  - ▶ Mobile
  - ▶ GRE
  - ▶ Serial
  - ▼ Advanced
    - ▶ External Modems
    - ▶ PPP Mappings
    - ▼ PPP 0 - 9
      - ▶ PPP 0
      - ▶ PPP 1 - W-WAN
      - ▶ PPP 2
      - ▶ PPP 3
      - ▶ PPP 4
      - ▼ PPP 5

Description:

This PPP interface will use L2TP

Click the **Apply** button to confirm these settings.

Parameter	Setting	Description
Layer 1 Interface	L2TP	
Layer 1 Interface #	0	



## 4.2 Configuring L2TP

Navigate to **Configuration – Network > Virtual Private Networking (VPN) > L2TP > L2TP 0**

[Configuration - Network > Virtual Private Networking \(VPN\) > L2TP > L2TP 0](#)

The screenshot shows the configuration page for L2TP 0. The left sidebar lists navigation options: Interfaces, DHCP Server, Network Services, DNS Servers, Dynamic DNS, IP Routing/Forwarding, and Virtual Private Networking (VPN). Under VPN, there are sub-sections for IPsec, L2TP, and L2TP 0. The main content area contains the following settings:

- Act as a listener only
- Enable Server mode
- Initiate connections to:  (circled in red)
- Use  as a backup
- Bring this tunnel up:  All the time (circled in red),  On demand
- Bring this tunnel down if it is idle for:  hrs  mins  secs (circled in red)
- L2TP Window Size:  ▼
- Route UDP packets over interface:  ▼
- Source Port:  Normal,  Variable
- Name:
- Authentication:  Off,  Secret

At the bottom, there is an **Advanced** section and an **Apply** button.

Click the **Apply** button to confirm these settings.

Parameter	Setting	Description
Initiate connections to	194.213.214.120	IP Address of VPN Host (example)
Bring this tunnel up	All the time	All the time – Permanent Internet connection On demand – GPRS / Dial-on-demand connection
Bring this tunnel down if it is idle for	0 hrs 0 mins 0 secs	0 hrs 0 mins 0 secs – Permanent Internet connection 0 hrs 1 mins 0 secs – GPRS / Dial-on-demand connection

## 4.3 Configuring IPsec

Navigate to **Configuration – Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE 0**

The settings for IKE 0 are the factory defaults and do not need to be changed.

**Configuration – Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE 0**

- ▶ Interfaces
- ▶ DHCP Server
- ▶ Network Services
- ▶ DNS Servers
- ▶ Dynamic DNS
- ▶ IP Routing/Forwarding
- ▼ Virtual Private Networking (VPN)
  - ▼ IPsec
    - ▶ IPsec Tunnels
    - ▶ IPsec Default Action
    - ▶ IPsec Groups
    - ▶ Dead Peer Detection (DPD)
    - ▼ IKE
      - ▶ IKE Debug
      - ▼ IKE 0

Use the following settings for negotiation

Encryption:  None  DES  3DES  AES (128 bit)  AES (192 bit)  AES (256 bit)

Authentication:  None  MD5  SHA1

Mode:  Main  Aggressive

MODP Group for Phase 1:

MODP Group for Phase 2:

Renegotiate after  hrs  mins  secs

▼ **Advanced**

Retransmit a frame if no response after  seconds

Stop IKE negotiation after  retransmissions

Stop IKE negotiation if no packet received for  seconds

Enable Dead Peer Detection

NAT Traversal Mode:

Send INITIAL-CONTACT notifications

Retain phase 1 SA after failed phase 2 negotiation

RSA private key file:

SA Removal Mode:

Delete SAs when invalid SPI notifications are received

Click the **Apply** button to confirm these settings.

Navigate to **Configuration – Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0**

Choose the first available Eroute (in this case Eroute 0) and enter the following parameters:

**Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0**

**IPsec 0**

Description:

The IP address or hostname of the remote unit

Use  as a backup unit

Local LAN	Remote LAN
<input checked="" type="radio"/> Use these settings for the local LAN	<input checked="" type="radio"/> Use these settings for the remote LAN
IP Address: <input type="text"/>	IP Address: <input type="text" value="194.213.214.120"/>
Mask: <input type="text" value="255.255.255.255"/>	Mask: <input type="text" value="255.255.255.255"/>
<input type="radio"/> Use interface <input type="text" value="PPP"/> <input type="text" value="0"/>	<input type="radio"/> Remote Subnet ID: <input type="text"/>

Use the following security on this tunnel

Off  Preshared Keys  XAUTH Init Preshared Keys  RSA Signatures  XAUTH Init RSA

Our ID:

Our ID type  IKE ID  FQDN  User FQDN  IPv4 Address

Remote ID:

Use  encryption on this tunnel

Use  authentication on this tunnel

Use Diffie Hellman group

Use IKE  to negotiate this tunnel

Use IKE configuration:

Bring this tunnel up

All the time  
 Whenever a route to the destination is available  
 On demand

If the tunnel is down and a packet is ready to be sent

Bring this tunnel down if it is idle for  hrs  mins  secs

Renew the tunnel after

hrs  mins  secs

KBytes of traffic

**Advanced**

IPsec mode  Transport  Tunnel

Use  AH authentication on this tunnel

Use  compression on this tunnel

Delete SAs when this tunnel is down

Replay detection window

Delete SAs when Ethernet  is not a VRRP master

Go out of service if automatic establishment fails

Disconnect the configured interface after  consecutive auto-negotiation failures

This tunnel can only use

Link tunnel with interface

Inhibit this IPsec tunnel when IPsec tunnels  are up

Inhibit this IPsec tunnel unless IPsec tunnel  is up

IKE negotiation source IP address is taken from the

- Interface
- Secondary IP address
- Interface

Tunnel this IPsec tunnel inside another tunnel < / div >

NAT-Traversal Keepalive timer  seconds

Allow  IP protocol(s) in this tunnel

IP packets with ToS values  must use this tunnel

Only tunnel IP packets with

- local TCP/UDP port
- remote TCP/UDP port

Insert remote subnet into routing table with metric

Click the **Apply** button to confirm these settings.

Parameter	Setting	Description
The IP address or hostname of the remote unit	194.213.214.120	IP Address of VPN Host (example)
Local LAN – IP Address		Leave Blank
Local LAN – Mask	255.255.255.255	Subnet Mask
Remote LAN – IP Address	194.213.214.120	IP Address of VPN Host (example)
Remote LAN – Mask	255.255.255.255	Subnet Mask
Use the following security	Preshared Keys	Authentication Method

on this tunnel		
Our ID	194.213.214.120	IP Address of VPN Host (example)
Our ID type	IPv4 Address	
Use ___ encryption on this tunnel	3DES	ESP Encryption Algorithm
Use ___ authentication on the tunnel	MD5	ESP Authentication Algorithm
Bring this tunnel up	On demand	
If the tunnel is down...	Bring the tunnel up	
Renew the tunnel after (time)	1 hour	This has to match the VPN Host (example)
Renew the tunnel after (traffic)	0 Kbytes	This has to match the VPN Host (example)
IPsec mode	Transport	
Allow ___ IP protocol(s)...	UDP	L2TP is UDP
local TCP/UDP port	1701	Source port (L2TP uses port 1701)
remote TCP/UDP port	1701	Destination port (L2TP uses port 1701)

#### 4.4 Configure the IPsec Pre-shared key

Navigate to **Configuration - Security > Users > User 0 - 9** and select an available User ID to enter the IPsec Pre-shared key. In this example, **User 5** will be used.



Click the **Apply** button to confirm these settings.

Parameter	Setting	Description
-----------	---------	-------------

Username	194.213.214.120	IP Address of VPN Host (example)
Password	*****	Value for Pre-shared Key
Confirm Password	*****	Value for Pre-shared Key
Access Level	None	Level of router administration access

## 4.5 Configuring a static route

Navigate to **Configuration - Network > IP Routing/Forwarding > Static Routes > Routes 0 - 9 > Route 0**

If Static route 0 is in use, choose the first available static route and enter:

[Configuration - Network > IP Routing/Forwarding > Static Routes > Routes 0 - 9 > Route 0](#)

The screenshot shows the configuration page for Route 0. The left sidebar contains a tree view with the following items: Interfaces, DHCP Server, Network Services, DNS Servers, Dynamic DNS, IP Routing/Forwarding (expanded), IP Routing, and Static Routes (expanded). Under Static Routes, there is a sub-section for Routes 0 - 9, and under that, Route 0. The main content area shows the configuration for Route 0. The Description field is empty. The Destination Network field contains 192.168.10.0 and the Mask field contains 255.255.255.0. Below these fields is a 'via' label, followed by a Gateway field (empty), an Interface dropdown menu set to PPP, and an Interface # field set to 5. Below the Interface # field is a 'Use PPP sub-configuration' checkbox (checked) and a Metric field set to 1. At the bottom of the configuration area is an 'Advanced' link. At the very bottom of the page is an 'Apply' button.

Click the **Apply** button to confirm these settings.

Parameter	Setting	Description
Destination Network	192.168.10.0	LAN Subnet of VPN Host (example)
Mask	255.255.255.0	Subnet Mask of VPN Host (example)
Interface	PPP	
Interface #	5	The Number of the PPP interface configured (example)

## 4.6 Saving the configuration

Navigate to **Administration - Save configuration**

## Administration - Save configuration

Save current configuration to Config **0 (power up)**

**Save**

Save all configuration. This includes the following

- Save the current configuration to config 0
- Save the current firewall
- Save all registers on all ports to profile 0
- Save all PAD parameters on all PADs to profile 0

Save All

Click the **Save** button to save the settings.

## 5 TESTING

To test the link, you will need to send data to the remote network (example: ping 192.168.10.1). You should then be able to see in the Event Log the L2TP traffic being encrypted in an IPsec tunnel and then sent using PPP 2 to the remote network.

```
12:26:20, 17 Nov 2009, PPP 5 up
12:26:18, 17 Nov 2009, PPP 5 Start IPCP
12:26:17, 17 Nov 2009, PPP 5 Start AUTHENTICATE
12:26:14, 17 Nov 2009, PPP 5 Start LCP
12:26:14, 17 Nov 2009, PPP 5 Start
12:26:14, 17 Nov 2009, L2TP Call 0 up
12:26:13, 17 Nov 2009, L2TP Tunnel 0 up
12:26:02, 17 Nov 2009, New IPsec SA created by 194.213.214.120
12:26:01, 17 Nov 2009, New Phase 2 IKE Session, Initiator
12:25:59, 17 Nov 2009, IKE Keys Negotiated
12:25:56, 17 Nov 2009, New Phase 1 IKE Session, Initiator
12:25:56, 17 Nov 2009, IKE Request Received From Eroute 0
12:25:55, 17 Nov 2009, GP socket connected: l_port[1701] r_ip[194.213.214.120]
r_port[1701]
12:25:55, 17 Nov 2009, IP Act_Rq to PPP 5-0: s_ip[192.168.0.1] d_ip[192.168.10.1]
```

Once the tunnel is up, the traffic can be routed and a reply to your ping should be seen.

## 6 CONFIGURATION FILES

### 6.1 TransPort Configuration Files

This is the relevant configuration from the router:

```
l2tp 0 remhost "194.213.214.120"

route 0 IPAddr "192.168.10.0"
route 0 ll_ent "PPP"
route 0 ll_add 5

eroute 0 peerip "194.213.214.120"
eroute 0 ourid "194.213.214.120"
```

```

eroute 0 ouridtype 3
eroute 0 locmsk "255.255.255.255"
eroute 0 remip "194.213.214.120"
eroute 0 remmsk "255.255.255.255"
eroute 0 mode "Transport"
eroute 0 ESPauth "MD5"
eroute 0 ESPenc "3DES"
eroute 0 proto "UDP"
eroute 0 locport 1701
eroute 0 remport 1701
eroute 0 ltime 3600
eroute 0 authmeth "PRESHARED"
eroute 0 nosa "TRY"

ppp 5 l1iface "L2TP"
ppp 5 phonenum "012345"
ppp 5 username "vpn.user.id"
ppp 5 epassword "Li94FFBfQk4cTUAORQ==" #This is the enciphered password
ppp 5 r_addr OFF
ppp 5 l_addr ON
ppp 5 l_pap OFF
ppp 5 l_chap OFF

user 5 name "194.213.214.120"
user 5 epassword "Li94FFVfTBJGWFIIJ"
user 5 access 4

#Optional PPP 5 configuration from page 6, if unsure, do not use:
ppp 5 IPaddr "192.168.10.1"
ppp 5 mask "255.255.255.0"
ppp 5 L_addr OFF

```

## 6.2 TransPort Firmware Versions

This is the firmware \ hardware information from the unit:

```

ati5
Digi TransPort WR44v2-U8G1-WE2-XX Ser#:291603
Software Build Ver 5.2.12.5 Nov 2 2015 05:02:14 LW
ARM Bios Ver 7.56u v45 800MHz B995-M1003-F80-01000140,2 MAC:00042d047313
Power Up Profile: 0
Async Driver           Revision: 1.19  Int clk
Wi-Fi                  Revision: 2.0
Ethernet Hub Driver    Revision: 1.11
Firewall               Revision: 1.0
EventEdit              Revision: 1.0
Timer Module           Revision: 1.1
AAL                    Revision: 1.0
ADSL                   Revision: 1.0
(B)USBHOST             Revision: 1.0
L2TP                   Revision: 1.10
PPTP                   Revision: 1.00
TACPLUS                Revision: 1.00
MySQL                  Revision: 0.01
LAPB                   Revision: 1.12
X25 Layer              Revision: 1.19
MACRO                  Revision: 1.0
PAD                    Revision: 1.4
X25 Switch             Revision: 1.7
V120                   Revision: 1.16
TPAD Interface         Revision: 1.12
SCRIBATSK             Revision: 1.0

```



BASTSK	Revision: 1.0
ARM Sync Driver	Revision: 1.18
TCP (HASH mode)	Revision: 1.14
TCP Utils	Revision: 1.13
PPP	Revision: 1.19
WEB	Revision: 1.5
SMTP	Revision: 1.1
FTP Client	Revision: 1.5
FTP	Revision: 1.4
IKE	Revision: 1.0
POLLANS	Revision: 1.2
PPPOE	Revision: 1.0
BRIDGE	Revision: 1.1
MODEM CC (Telit LTE)	Revision: 5.2
FLASH Write	Revision: 1.2
Command Interpreter	Revision: 1.38
SSLCLI	Revision: 1.0
OSPF	Revision: 1.0
BGP	Revision: 1.0
QOS	Revision: 1.0
RADIUS Client	Revision: 1.0
SSH Server	Revision: 1.0
SCP	Revision: 1.0
CERT	Revision: 1.0
LowPrio	Revision: 1.0
Tunnel	Revision: 1.2
OVPN	Revision: 1.2
TEMPLOG	Revision: 1.0
OK	