

InJoy PPPoE 4.0

Configuration Guide



InJoy PPPoE
Broadband Network Access

Copyright © 2007, F/X Communications. All Rights Reserved. The use and copying of this product is subject to a license agreement. Any other use is strictly prohibited. No part of this publication may be reproduced, transcribed, or translated into any language, in any form by any means without the prior written consent of F/X Communications. Information in this document is subject to change without notice and does not constitute any commitment on the part of F/X Communications.

Contents

I.	Introduction to PPPoE	3
	1. INTRODUCTION	4
	1.1. DOCUMENT SCOPE	4
	2. PPPOE OVERVIEW	5
	2.1. WHAT IS PPPoE?	5
	2.2. HOW PPPoE WORKS	5
	2.3. INJOY PPPoE FEATURES	6
II.	Setting up PPPoE	8
	3. CONFIGURING PPPOE	9
	3.1. ENABLING PPPoE	9
	3.2. CONFIGURING PPPoE	10
	4. PPPOE OPERATION	17
	4.1. MANAGING PPPoE CONNECTIONS	17
	4.2. APPLYING CONFIGURATION CHANGES	18
III.	References	19
	5. MAXIMUM TRANSMISSION UNIT	20
	5.1. SOLVING THE PPPoE MTU IMPLICATIONS	20
	5.2. SETTING THE MTU VALUE	21
	6. CONFIGURATION FILES	26
	6.1. PPPoE MANDATORY PARAMETERS	26
	6.2. PPPoE OPTIONAL PARAMETERS	27

Part I

Introduction to PPPoE

1

Introduction

The PPPoE (Point to Point Protocol over Ethernet) specifies how an ISP and a remote PC can set up a session-based Internet connection on top of the session-less Ethernet protocol.

Internet Service Providers are implementing PPPoE to replace static IP addressing or DHCP systems that do not offer authentication, billing, or service differentiation.

For the end user, there are only a few changes from e.g. a DHCP served ADSL connection. Instead of having the connection automatically occur when the computer boots, the connection and authentication are established using PPPoE client software – such as the InJoy Firewall™.

It is also important to notice that because of the extra PPPoE protocol layer, the maximum IP packet size becomes smaller and we recommend that you read the "Maximum Transmission Unit" section to understand the implications.

1.1. Document Scope

Before reading this document you should be familiar with the InJoy Firewall™ and have basic knowledge of the TCP/IP protocol – i.e. know what an IP address is. Additionally, your LAN adapter should be installed and connected to your ISP hookup.

To ease your navigation, this document has been divided into several distinct parts according to the amount of information different types of readers are likely to need:

- Part I.** Introduction to PPPoE
- Part II.** Setting up PPPoE
- Part III.** References

Part II by itself contains enough information to successfully install and use the PPPoE Plugin. Users who want a better understanding of PPPoE can consult the remaining parts for additional information.

2

PPPoE Overview

This section gives you an overview of PPPoE and its capabilities.

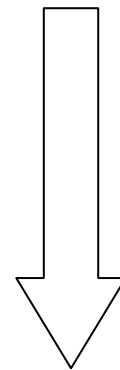
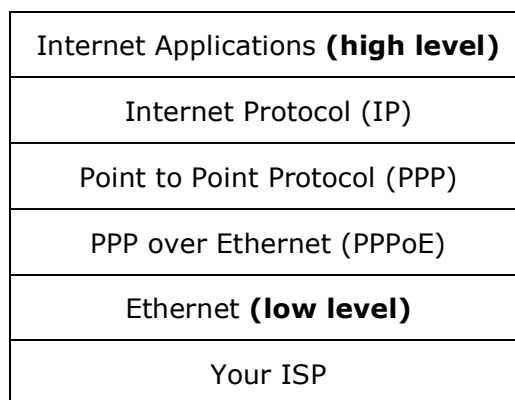
2.1. What is PPPoE?

PPPoE -- like PPP over dial-up lines -- allows connecting a machine to the Internet and is designed for simple links that transport packets between two peers; it does not support multi-destination traffic (e.g. multicast and broadcast packets). In short, PPPoE establishes a PPP session and encapsulates the traffic into PPP over an existing Ethernet line.

2.2. How PPPoE Works

Protocol Stack

PPPoE is an encapsulation technique that allows use of the PPP protocol over an Ethernet-based connection. After applying PPPoE, the layered protocol communications stack looks like this:



PPPoE Protocol

The PPPoE protocol has two distinct stages. In the first stage PPPoE discovers servers (also called Access Concentrators) and in the second stage, PPPoE negotiates a PPP connection. These two stages are named:

- PPPoE discovery phase
- PPP session phase

PPPoE Discovery Phase

This part is a stateless client-server protocol which is used when a client needs to establish a PPPoE session. The typical flow of the PPPoE discovery phase is outlined below:

- 1 First the PPPoE Client sends out a PADI (PPPoE Active Discovery Initiation) packet to the broadcast MAC address FF:FF:FF:FF:FF:FF. This packet initiates the search for PPPoE Access Concentrator(s).
- 2 One or more PPPoE servers typically respond with a PADO (PPPoE Active Discovery Offer) packet. Together with this packet is a list of services that these servers support. The PADO packet also holds a session ID derived from the initial PADI packet, which is used to uniquely identify the PPPoE session.
- 3 The PPPoE client then finds an acceptable offer and proceeds to the next exchange; the destination MAC address now correctly identifies the Access Concentrator of choice (i.e. the communication is of unicast type from now on).
- 4 The PPPoE client sends a PADR (PPPoE Active Discover Request) packet to the chosen PPPoE server which contains a session ID and other information which uniquely identifies the PADR packet.
- 5 The server responds with a session ID and then the connection enters the PPP stage.

PPP Session Phase

At this point, PPP negotiations begin, which includes LCP, PAP, CHAP, IPCP and other types of payloads. PPP is encapsulated into PPPoE and all Ethernet frames are still destined for the chosen Access Concentrator.

PPPoE Standard

Additional information about the PPPoE protocol is available in the following RFCs:

- RFC 1661 "The Point-to-Point Protocol"
- RFC 1662 "PPP in HDLC-like Framing"
- RFC 2516 "A Method for Transmitting PPP over Ethernet (PPPoE)".

2.3. InJoy PPPoE Features

This section covers details of the InJoy PPPoE implementation.

Installation	<ul style="list-style-type: none"> • Installed seamlessly as part of the InJoy Firewall™ software. • Similar operation on all supported operating systems. • Plugs into the InJoy Firewall™ as a loadable module, maintaining the Firewall's superior speed and efficiency.
Configuration	<ul style="list-style-type: none"> • Multiple ISP profiles and an easy to use GUI. • Possibility of executing scripts when connecting and

	<p>disconnecting.</p> <ul style="list-style-type: none"> • For the experts (and for easy scripting), all configuration attributes are also directly editable in a plain-text file.
Performance	<ul style="list-style-type: none"> • Allows sustained utilization of all network bandwidth. • Adjustable priority allows user control of CPU utilization.
Connection	<ul style="list-style-type: none"> • Connect at start-up. • Connect on demand. • Connect manually. • Idle disconnect. • Manual disconnect. • Session timeout disconnect. • Connection loss detection. • Auto re-connect.
Diagnostics	<ul style="list-style-type: none"> • Message log. • Screen output.
Line Sharing	<ul style="list-style-type: none"> • The gateway (NAT) capability in the InJoy Firewall™ allows for sharing the PPPoE connections.
Security	<ul style="list-style-type: none"> • All the filtering and firewall capabilities of the InJoy Firewall™ are available.
VPN Support	<ul style="list-style-type: none"> • Coexists with the InJoy Firewall™ IPsec support
Documentation	<ul style="list-style-type: none"> • Complete with instructions to help both beginners and advanced users.

Part II

Setting up PPPoE

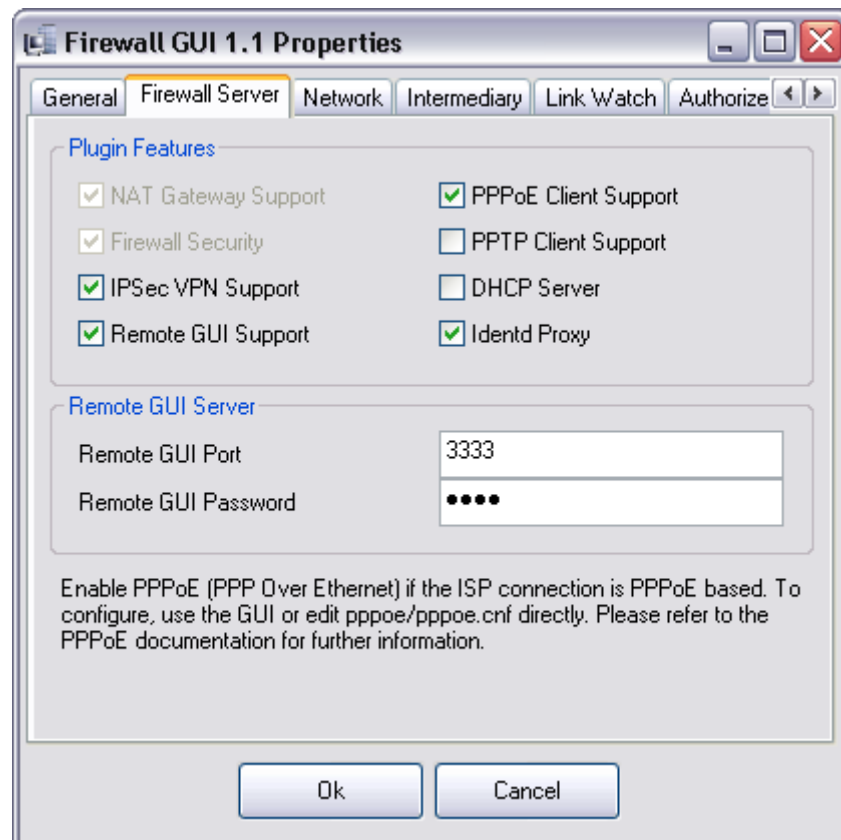
3

Configuring PPPoE

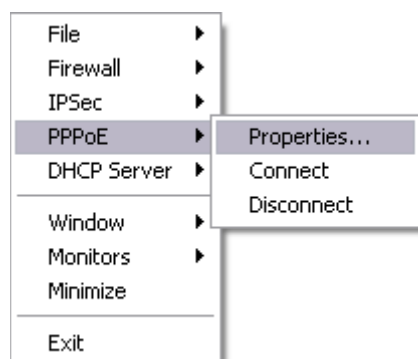
3.1. Enabling PPPoE

The PPPoE Plugin is seamlessly installed with the InJoy Firewall™ product and can be activated, if supported by the registration key.

To enable the PPPoE Plugin, go into the Firewall GUI Properties and enable the “PPPoE Client Support” checkbox - as shown below:



Press the **OK** button and restart the InJoy Firewall™ as directed. After restarting the Firewall, the Firewall GUI pop-up menu should include a PPPoE submenu, as shown below:



3.2. Configuring PPPoE

The PPPoE configuration is divided into ISP profiles that can be edited via the Firewall GUI or by using a simple plain-text editor (the configuration is stored in PPPOE\PPPOE.CNF).

This section guides you through the PPPoE configuration using the Firewall GUI. You can find information about editing the PPPoE configuration with a plain-text editor later in this document.

The Configuration Notebook

To configure PPPoE graphically, right click the InJoy Firewall™ GUI and select "**PPPoE | Properties**" from the pop-up menu. Four separate configuration pages appear:

Login

The Login tab contains the required account information for logging on with your ISP. This screen also presents you with the controls needed to maintain a list of ISP profiles and an option for setting the active ISP.

TCP

The TCP tab contains the settings pertinent to TCP/IP, including IP addresses and DNS servers.

Link

The Link tab contains the settings that control and monitor the link, such as keep-alive timers, demand connectivity, and tracing.

About

The about tab contains the PPPoE Plugin logo.

Login Parameters

The PPPoE Plugin supports multiple ISP configurations, which are easily maintained through the Login dialog. The dialog contains buttons for creating,

modifying and deleting ISP profiles. A drop-down list of ISP profiles gives you a quick overview of those profiles.



ISP

This is the list of ISP profiles. Each profile is a logical identifier that refers to the parameters for a connection.

You can create new or delete existing profiles by clicking the buttons on the right of the ISP drop-down list. You cannot edit the connection names in the drop-down list – use **ISP Name** for this.

ISP Name

The ISP Name is the name of the connection being modified/created/deleted. This field accepts characters only the following characters: 0-9, A-Z, and `-'`.

User ID

Enter the user ID as assigned to you by your ISP. The format is typically "user-id@isp.com". For example, if your user ID is **joe** and your ISP is Sympatico, then enter the following: "joe@sympatico.ca".

Password

Enter the password assigned to you by your ISP. Please note that passwords are typically case-sensitive and the state of the CAPS LOCK key and the OS language should be checked.

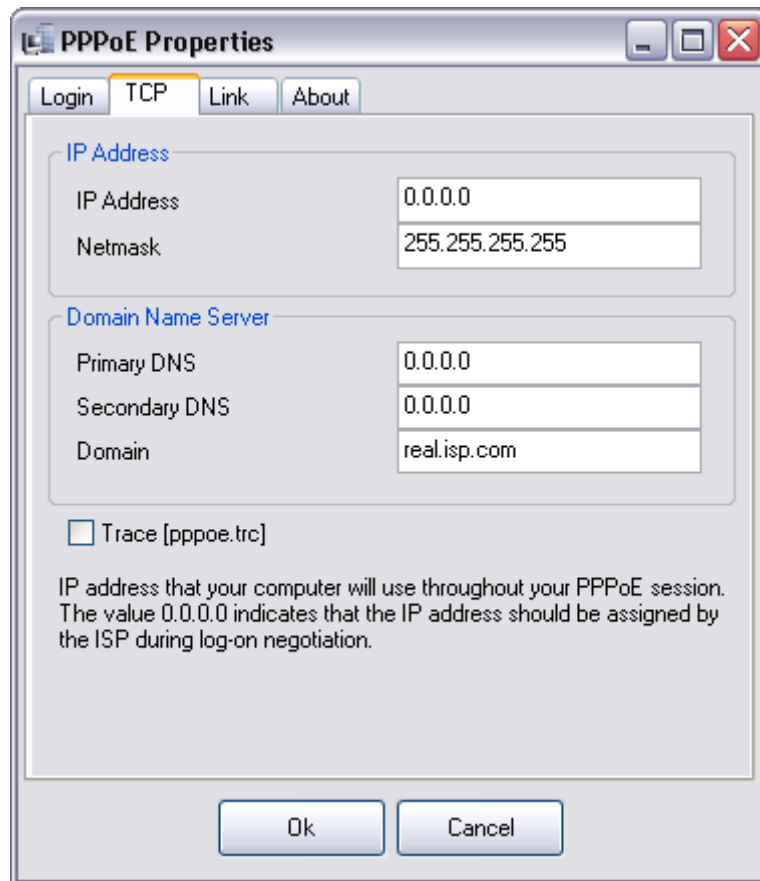
Default Profile

Only one ISP can be marked active at a time. Marking an ISP active will automatically turn this flag off in all other ISP profiles.

The default ISP profile is the one selected at startup. Other flags determine whether a connection will be automatically set up.

TCP Parameters

To connect successfully with a PPPoE ISP, both ends of the connection must define some basic parameters to control the PPPoE negotiation.



IP Address

This is the Internet Protocol (IP) address that your computer will use throughout your session.

The value 0.0.0.0 means that PPPoE should obtain the actual IP address from the ISP server during PPP negotiation. Obtaining the IP address from the server is the standard way of assigning IP addresses using PPPoE.

It is possible to specify an IP address when the server will not dynamically assign one.

Netmask

The netmask specifies the IP addresses which are supposed to go through your PPPoE connection. If you did not receive an assigned netmask from your ISP then leave it as set (255.255.255.255).

Primary DNS / Secondary DNS

The Primary and Secondary DNS (Domain Name Server) are IP addresses of your preferred name servers.

If your ISP supports "server assigned DNS addresses" (RFC 1877), then enable the automatic negotiation by entering 0.0.0.0 in the DNS server fields. Only DNS server fields containing 0.0.0.0 will be negotiated. Note that you can mix the 0.0.0.0 value with a static specification of a DNS server. For example, the primary DNS server could be specified as 0.0.0.0 (i.e. to have the ISP assign the value), while the secondary DNS server is specified as a static value (i.e. the IP address of your own DNS server).

Domain

This is the domain in which your computer exists on the Internet. You should specify the symbolic name that you have received from your ISP. For example, "sympatico.ca" and "ibm.net" are valid domain names.

Trace

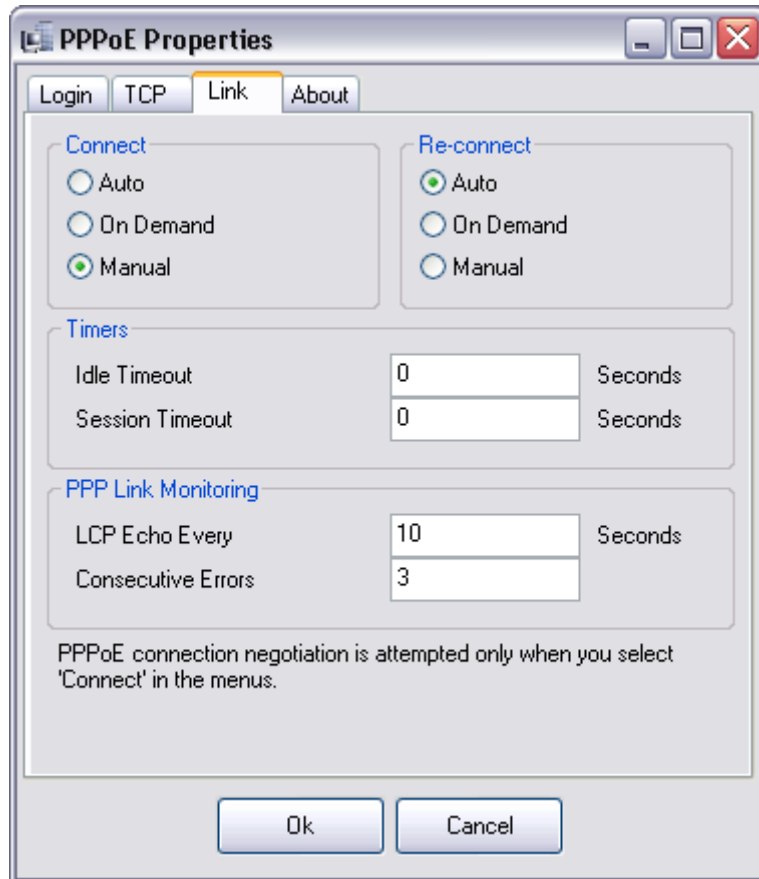
Enable this option if you need to trace a PPPoE connection. The trace information is written to the file LOGS\PPPOE.TRC.

If you have problems connecting to the ISP, this is the file that will help the F/X support crew (support@fx.dk) to get you online.

When running in a stable environment, it is recommended to turn OFF the tracing, as it results in significantly lower performance.

Link Parameters

The link parameters define when connections are to be established or brought down. Additionally, the link dialog offers functionality for timeout, link loss and trace monitoring.



Connect

This allows you to define when the initial PPPoE connection is to be established:

- **Auto**
A PPPoE connection is negotiated immediately at ISP profile selection. The default ISP profile is selected automatically at startup.
- **On Demand**
Connect on Demand (a.k.a. Dial on Demand - DoD) allows for automatic connections when an application on your computer or a NAT LAN client needs it; auto-disconnecting when the connection is idle (using the idle timeout feature), and auto-dialing again at the next need/demand.

Sometimes you will find it useful to go back and see what packet triggered the connection demand. You can do this as the triggering packet is saved to 'DOD.DMP'. This file uses a format which can be decoded by the IPFORMAT utility included in the InJoy Firewall™. To get a nicely formatted dump of the trigger packet, issue the command 'IPFORMAT DOD.DMP'.

- **Manual**

Connection negotiation is attempted when the user selects "Connect" in the InJoy Firewall™ pop-up menu.

Re-connect

This option specifies the action to be taken when a connection is terminated. As with the above option, you can choose to re-connect automatically, on demand or manually.

Idle Timeout

Specifies how long the connection may remain idle (i.e. nothing being received) before PPPoE will automatically disconnect. The Idle Timeout is specified in seconds.

A note of caution is in order here. Some users set the idle timeout to five minutes or so, and walk away from the computer after beginning a long download/upload... knowing that when finished the connection will be dropped, as the idle timer reaches zero.

Be careful: many hosts periodically send "dummy" packets in order to avoid unintentional disconnects. If you are paying for your connection by the minute you might want to ensure the line is dropped within a reasonable time after data flow has stopped (see the Session Timeout).

To completely disable the idle timeout, specify a value of zero. In that case, the line will never be dropped due to inactivity.

Session Timeout

This timer specifies how long PPPoE may stay connected before it will automatically disconnect, irrespective of traffic.

The timeout is specified in seconds.

This function is much like the one on your VCR or TV that enables you to automatically turn it off e.g. after half an hour, without worrying about the TV starting a fire during the night.

In the same way this can go wrong for a television, it can for PPPoE. If PPPoE has a problem disconnecting, there is nothing it can do. To completely disable the timeout, specify a value of zero. In this case, the line will never be dropped for exceeding a preset time on line.

LCP Echo Every

A standard feature of PPP is the ability to probe the link by sending out echo packets and watching for responses. This feature is valuable with PPPoE as the endpoints are physically connected but there is no guarantee that the logical connection is working.

To enable this feature and detect disconnects, set this parameter to a non-zero value. The value should be the number of seconds between sending out the LCP Echo blocks. When setting the time between each outgoing echo, consider that the ISP should have enough time to reply to the previous echo before PPP sends out a new echo packet.

When a lost connection is detected, it is reported to the PPPoE control code and depending on the "Re-connect" setting, an action will be taken.

Specify zero to disable this feature.

Consecutive Errors

Packets can be lost on a PPPoE link without being critical to the connection. However, if several packets in sequence are lost, then it is normally a sign that the logical PPP connection is lost.

This option allows you to specify the number of consecutive lost packets that are required in order to declare the link dead.

4

PPPoE Operation

4.1. Managing PPPoE Connections

The Connection

PPPoE transforms a physical LAN-to-LAN connection into a logical connection.

Once “connected” using a PPPoE client, your connection will look the same as your current TCP/IP connection. When you disconnect, your PPPoE connection is terminated and you will need to reconnect to use the Internet again. InJoy PPPoE can monitor the link and automatically reconnect. It is your choice whether this is done immediately or on demand. In NAT environments this interruption is transparent.

Connecting

A connection can be triggered manually, automatically or on demand.

Using the Firewall GUI, you can manually trigger a connection by selecting “**PPPoE | Connect**” from the RMB (Right Mouse Button) pop-up menu.

Disconnecting

Disconnections can be triggered manually, by timers or by the ISP.

Using the Firewall GUI, you can manually disconnect by selecting “**PPPoE | Disconnect**” from the RMB (Right Mouse Button) pop-up menu.

Reconnecting

As previously mentioned in the configuration section, the re-connect flag allows you to determine when, how and if a PPPoE connection is to be reconnected at connection loss.

If you wish to maintain a full time PPPoE connection, then set the re-connect flag to “auto” and InJoy will automatically reconnect when the connection loss is detected. This makes InJoy the perfect choice for keeping a connection alive 24 hours a day.

Setting the re-connect flag to “demand” allows for automatic reconnects when your TCP/IP applications require Internet connectivity.

Connection details

When a PPPoE connection has been successfully established, the file CONNECT.TXT is immediately created. This file includes characteristics about your current connection. The following is an example of the contents of a typical CONNECT.TXT file:

```
194.234.160.52
194.234.160.8
Host.....: Sympatico
Modem connect.: void
Line speed...: unknown
DNS (Primary)..: 194.234.160.2
DNS (Backup)...: 194.234.160.3
```

CONNECT.TXT is not a semaphore file, so don't use it to determine if you are connected at any moment.

This file is also found in the InJoy Dialer™ product and the same file format is maintained between products.

4.2. Applying Configuration Changes

At start-up and with each connect attempt, the ISP profiles are automatically scanned for the active profile. Once found, the active profile is read and the new settings are put into action. There is no need to manually re-load the configuration each time it is changed (unlike the IPsec and DHCP Server Plugins).

Part III

References

5

Maximum Transmission Unit

This section provides you with the background information to understand and solve the MTU issues that arise from using the PPPoE protocol.

The problems are likely to be of different importance in various organizations and there is no single perfect work-around available. As a general approach, it is recommended that you start out by using the MSS fix described below and only continue to update the MTU on internal machines if it proves necessary for your application suite.

While this section delivers a comprehensive introduction to the possible MTU issues, a complete description of the MTU is beyond the scope of this document.

5.1. Solving the PPPoE MTU Implications

Understanding the PPPoE MTU Problem

Typically, packets on your network have a maximum size of 1500 bytes, which is the default MTU (Maximum Transmission Unit) on Ethernet.

Packets of 1500 bytes are larger than the maximum possible PPPoE packet size and therefore it is typically recommended that all machines which send data over the PPPoE connection MUST have their MTU set to a smaller value (for example 1492 bytes, which is 1500 bytes less the 8 bytes PPPoE header).

On a larger network with many different OS platforms, it can however be a resource demanding task to change the MTU on all internal PCs. Adding to this complexity are other protocols, such as IPSec or PPTP, which also enlarges IP packets.

The TCP/IP protocol includes its own technology to allow big packets to traverse smaller pipes. This technology is known as packet fragmentation and it is supported by the InJoy Firewall™.

Packet fragmentation splits up big packets into several small packet fragments and once the fragments arrive at their final destination they are defragmented into a complete packet. The packet fragmentation can somewhat solve the PPPoE MTU problem, however, it introduces an extra hit on performance and worse, certain applications require packets to reach their destination without the use of fragmentation.

Identifying MTU problems

MTU problems are distinct and easy to detect.

If you have an MTU misconfiguration, you will experience problems especially when you download larger web pages, fetch e-mails and use ftp. Very small e-mails, certain web pages and small files on ftp may download just fine, while others just stall.

Maximum Segment Size (MSS) - A Quick Fix

The Maximum Segment Size is the maximum portion of data (in a single IP packet) that can pass over a TCP connection. By default, the MSS is automatically set by the TCP/IP stack, based on the interface MTU. For example, if the MTU is 1500 bytes, the MSS is typically 1460 bytes – calculated as 1500 minus the 40 bytes used by the TCP/IP headers.

The InJoy Firewall™ has a feature to automatically change the MSS value for every new TCP connection, thereby tricking the opposite end of the connection to send smaller packets. In practice, this effectively solves the MTU problems for all TCP connections (but not for UDP, ICMP and other protocols).

When using PPPoE, it is recommended that you start by setting the MSS-Adjust value in the InJoy Firewall™, "**File | Properties | Intermediary**" to a low value – for example in the range 1000-1200 (1200 is the default and it should be okay).

You can read more about the MSS-Adjust feature in the InJoy Firewall™ "Getting Started" documentation.

5.2. Setting the MTU Value

On different Operating Systems, different ways exist to edit the MTU values of network interfaces.

It is often a complicated procedure to adjust the MTU values and whenever possible, it is recommended that you use the MSS-Adjust feature to solve the PPPoE inflicted MTU problems.

If you however find that you must update the MTU values to ensure proper operation, you will find the procedure to edit the MTU on OS/2, eComStation, Windows 2000/XP and RedHat Linux 7.2+ below.

Setting the MTU on OS/2 and eComStation

There are several ways to change to the MTU in OS/2, but they all evaluate to a simple parameter to the ifconfig statements in:

```
\MPTN\BIN\SETUP.CMD
```

Example:

```
route -fh
arp -f
ifconfig lo 127.0.0.1 mtu 1492
ifconfig lan0 192.168.1.1 netmask 255.255.255.0 mtu 1492
```

```
...
```

TCP/IP 4.1 has been known to ignore MTU values at the end of ifconfig lines. The solution is to set the MTU on separate lines.

Example:

```
route -fh
arp -f
ifconfig lo 127.0.0.1
ifconfig lo mtu 1492
ifconfig lan0 192.168.1.1 netmask 255.255.255.0
ifconfig lan0 mtu 1492
...
```

Reboot the OS/2 Machine.

Setting the MTU on Windows 2000/XP

Changing the MTU in Windows requires use of the registry editor.

START > RUN > type **regedit** and press Enter.

Export your current registry to back it up into a temporary directory.

Then add these registry keys in the following sections (if they are not there already). If they are already present, then modify them to these values:

```
HKEY_LOCAL_MACHINE
\SYSTEM\CurrentControlSet\Services\\Parameters\Tcpip
MTU="1492"
```

(Make sure MTU is a DWORD VAR and NOT a STRING)

Windows 2000/XP has a registry setting at the TCP/IP level that tells TCP/IP to ignore explicit NIC MTU values and instead rely on detection of the maximum packet size. The settings that turn this on are presented below:

```
HKEY_LOCAL_MACHINE\
SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
"TcpWindowSize"="63990" (DWORD VAR)
DefaultTTL="128" (DWORD VAR)
EnablePMTUDiscovery="1" (DWORD VAR)
EnablePMTUBHDetect="0" (DWORD VAR)
```

Setting the MTU on Windows 98

Changing the MTU in Windows requires use of the registry editor.

START > RUN > type **regedit** and hit Enter.

[Export your current registry to back it up into a temporary directory.](#)

Then add these registry keys in the following sections (if they are not there already). If they are already present, then modify them to the new values.

The following keys should be set for your Ethernet adapter. When you go to the registry and look through the 000n folders in Nettrans (as shown below) you will know you found the right folder when you find the IP address of the Win95 client. In that 000n device folder add this:

```
HKEY_LOCAL_MACHINE\  
System\CurrentControlSet\Services\Class\NetTrans\000n  
  
MaxMTU="1492" (STRING VAR)
```

The following keys are also recommended, but only the PMTUDiscovery is mandatory for the PPPoE operation.

```
DefaultRcvWindow="362610" (FOR WIN98 USERS ONLY, STRING VAR)  
DefaultTTL="128" (STRING VAR)  
PMTUDiscovery="0" (DWORD)  
PMTUBlackHoleDetect="0" (DWORD )
```

Reboot the Win98 Machine.

Setting the MTU on Windows 95

Changing the MTU in Windows requires use of the registry editor.

START > RUN > type **regedit** and hit Enter.

[Export your current registry to back it up into a temporary directory.](#)

Then add these registry keys in the following sections (if they are not there already). If they are already present, then modify them to the new values.

The following keys should be set for your Ethernet adapter. When you go to the registry and look through the 000n folders in Nettrans (as shown below) you will know you found the right folder when you find the IP address of the Win95 client. In that 000n device folder add this:

```
HKEY_LOCAL_MACHINE\  
System\CurrentControlSet\Services\Class\NetTrans\000n  
  
MaxMTU="1492" (STRING VAR)  
  
HKEY_LOCAL_MACHINE\  
System\CurrentControlSet\Services\VxD\MSTCP  
  
DefaultRcvWindow="63990" (STRING VAR)  
DefaultTTL="128" (STRING VAR)  
PMTUDiscovery="0" (DWORD VAR),  
PMTUBlackHoleDetect="0" (DWORD VAR)
```

Reboot the Win95 Machine.

Setting the MTU on Windows NT

Changing the MTU in Windows requires use of the registry editor.

START > RUN > type **regedit** and hit Enter.

[Export your current registry to back it up into a temporary directory.](#)

Then add these registry keys in the following sections (if they are not there already). If they are already present, then modify them to these values:

```
HKEY_LOCAL_MACHINE  
\SYSTEM\CurrentControlSet\Services\<<Adapter Name>\Parameters\Tcpip  
  
MTU="1492" (Make sure it's a DWORD VAR and NOT a STRING)
```

Now add:

```
HKEY_LOCAL_MACHINE\  
SYSTEM\CurrentControlSet\Services\Tcpip\Parameters  
  
DefaultTTL="128" (DWORD VAR)  
EnablePMTUDiscovery="0" (DWORD VAR)  
EnablePMTUBHDetect="0" (DWORD VAR)
```

Reboot the NT Machine.

Setting the MTU on Linux Red Hat 7.2+

On Linux systems there are few ways to change the MTU, but the most widely used is to set it at start-up. This can be achieved by editing the file **/etc/sysconfig/network-scripts/ifcfg-XXXX**, where XXXX is interface name.

The setting that controls the MTU size is called "MTU" and it is represented in bytes. An example of valid **ifcfg-fx0** file is below:

```
DEVICE=fx0
ONBOOT=yes
MTU=1492
```

Another way to change the MTU value on-the-fly is to issue the following command:

```
ifconfig XXXX mtu 1492
```

Where XXXX is the interface name (e.g. fx0).

6

Configuration Files

The PPPoE Plugin uses the following configuration files:

- PPPOE/PPPOE.CNF – ISP profiles and their parameters
- TEMPLATE/PPPOE.CNF – default values for PPPoE configuration file. It is recommended that you do not edit this file!

The following section is divided into two parts. The first part deals with those parameters that MUST be entered in order for PPPoE to function. The second part deals with parameters for which the defaults should be sufficient. However, please review these parameters to ensure that possible ISP specific ISP parameters are not overlooked.

For parameters that are not already in PPPOE/PPPOE.CNF, simply copy & paste from PPPOE.CNF in the TEMPLATE directory.

Characters following '#' and ';' are comments and are ignored by the PPPoE Plugin.

The sample PPPOE/PPPOE.CNF file below illustrates the format of the configuration file:

```
# Real ISP profile
#
real-isp
    User-Id = "johndoe@real.isp.com",
    Password = "-73098811821c8917932bb726b4",
    Domain-Name = "real.isp.com",
    Default-Profile = Yes
```

For more details about the individual configuration attributes, please refer to the tables below.

6.1. PPPoE Mandatory Parameters

The following parameters should be defined by the user, as defaults values may not work.

Parameter	Permissible Values	Description
Domain-Name	String	This is the domain name of your ISP. DEFAULT : "[domain.com]" Enclosed in quotation marks

		e.g. "Sympatico.ca".
Password	String	This is the password provided by your ISP. DEFAULT : "" Enclosed in quotation marks e.g. "xyz123abc"
User-Id	String	This is the User-ID provided by your ISP. DEFAULT : "[user@isp.com]" Enclosed in quotation marks e.g. "joe@sympatico.ca"

6.2. PPPoE Optional Parameters

The following parameters are optional, defaults should function.

Parameter	Permissible Values	Description
AC-Name	String	This option allows you to select among several "Access Concentrators" for your ISP. Currently rarely used. However, usage will increase in the future as more PPPoE servers are deployed. Change ONLY if specifically instructed by your ISP. DEFAULT : "" Enclosed in quotation marks.
Connect	Auto On Demand Manual	This defines how the initial connection is to be initiated. AUTO The connection will be made using the ACTIVE ISP profile when the Gateway is executed. ON DEMAND (a.k.a. DoD) Connect the ACTIVE profile when a system process (Application or NAT LAN) requests, and close connection when process

		ends (using the Idle Timer). MANUAL Connect using the mouse RMB to select "CONNECT" in the Firewall GUI environment. DEFAULT : Manual Quotation marks NOT used
Default-Profile	Yes No	Indicates whether this ISP profile is the default profile, i.e. the one selected at start-up or at a connect event. DEFAULT : No Quotation marks NOT used
DNS-1 DNS-2	Valid TCP/IP Address	These are provided by your ISP. If your ISP supports server assigned DNS addresses per RFC 1877 then enable the negotiation by entering 0.0.0.0 in these fields. Change ONLY if specifically instructed by your ISP. DEFAULT : DNS-1 = "0.0.0.0" DNS-2 = "0.0.0.0" Enclosed in quotation marks e.g. "205.101.251.1"
Idle-Timeout	Seconds 0 – 99999	Specifies how long the connection may remain idle (i.e. nothing being RECEIVED) before automatically disconnecting. 0 - disables the feature DEFAULT : 0 Quotation marks NOT used
LCP-Echo	Seconds 0 – 99999	This will trigger echo packets to be sent at the specified interval in order to detect connection loss. Incoming IP packets reset the timer.

		<p>When a lost connection is detected, PPPoE will respond according to the Re-connect setting for the profile.</p> <p>0 - disables the feature</p> <p>DEFAULT : 10</p> <p>Quotation marks NOT used</p>
LCP-Consecutive-Errors	Counter 0 – 99999	<p>Packets can be lost on a PPPoE link without that being critical to the connection. However, if several packets in sequence are lost, then it is normally a sign that the logical PPP connection is lost. This option allows you to specify the number of consecutive lost packets that are required in order to declare the connection lost. PPPoE will respond according to the "Re-connect" setting for the profile.</p> <p>0 - disables the feature</p> <p>DEFAULT : 3</p> <p>Quotation marks NOT used</p>
Local-IP	Valid TCP/IP Address	<p>This is the Internet Protocol (IP) address that your computer will use throughout the current session.</p> <p>The value 0.0.0.0 means that PPPoE should obtain the actual IP address from the ISP server during log on negotiation. This is the normal mode used by PPPoE.</p> <p>Change ONLY if specifically instructed by your ISP</p> <p>DEFAULT : "0.0.0.0"</p> <p>Enclosed in quotation marks e.g. "0.0.0.0"</p>
Netmask	Valid TCP/IP Address	<p>If you were not assigned a special net mask from your ISP then use the net mask</p>

		255.255.255.255. DEFAULT : "255.255.255.255" Enclosed in quotation marks e.g. "255.255.255.255"
Peer-IP	Valid TCP/IP Address	This address is normally assigned by the ISP during the log on process. However, some providers specify a fixed IP address that you should enter here. Change ONLY if specifically instructed by your ISP Enclosed in quotation marks DEFAULT : "0.0.0.0"
MTU	Packet Size 1 – 1500	This is the MTU size that will be used when negotiating with the ISP. The MTU should be no bigger than 1492 bytes. Once negotiated, the MTU controls the maximum size of packets that are to traverse the PPPoE connection. Ethernet has a Max packet size of 1500 bytes, of which 8 bytes are required for the packet header. Therefore, unless directed by your ISP, you should use 1492 DEFAULT : 1492 Quotation marks NOT used
Lock-MTU	Yes No	The Lock MTU feature allows you to override the MTU value that the ISP wants you to use. Lock MTU will instead cause the MTU you specified to be used. DEFAULT : No Quotation marks NOT used
Re-Connect	Auto On Demand	This defines what is to happen if a connection is lost.

	Manual	<p>AUTO Attempt re-connection using the ACTIVE profile automatically.</p> <p>ON DEMAND (a.k.a. DoD) Attempt to re-connect when a system process (Application or NAT LAN) requests.</p> <p>MANUAL Do not attempt a re-connect.</p> <p>DEFAULT : Auto Quotation marks NOT used</p>
Restart-Timer	mS (1/1000th) 0 - 99999	<p>This is ONLY used in the opening PPPoE negotiation, and resends requests at the specified interval until negotiation is successful. If the opening negotiation seems slow adjust this setting. Note that too small a value can also slow the process down as the server needs time to respond.</p> <p>Note that this only applies to the initial login, once the connection is established this timer is dormant.</p> <p>The smaller you can set this timer and still reliably login, the faster PPPoE negotiates.</p> <p>DEFAULT : 300 Quotation marks NOT used</p>
Restart-Timer-Aut	mS (1/1000th) 0 - 99999	<p>This is ONLY used in the opening PPPoE negotiation, specifically the user/password authentication process and resends blocks at the specified interval until authentication is successful. If the opening negotiation seems slow, adjust this setting.</p>

		<p>Note that too small a value can also slow the process down as the server needs time to respond.</p> <p>Note that this is only applies to the initial login, once the connection is established this timer is dormant.</p> <p>DEFAULT : 1000 Quotation marks NOT used</p>
Service-Name	String	<p>For future use. Change ONLY if specifically instructed by your ISP</p> <p>DEFAULT : "" Enclosed in quotation marks</p>
Session-Timeout	Seconds 0 – 99999	<p>Specifies how long the connection may remain active, irrespective of activity, before automatically disconnecting.</p> <p>0 - disables the feature</p> <p>DEFAULT : 0 Quotation marks NOT used</p>
Trace	Yes No	<p>Enable this option if you need to trace a PPPoE connection. The trace information is written to the file "PPPOE.TRC" in the home directory. It is recommended to disable trace, unless troubleshooting, as it significantly reduces performance.</p> <p>DEFAULT : No Quotation marks NOT used</p>