TeamWork

Manual do Utilizador

(v1.2 – 12 Agosto 2005)

PTPrime -N.º de Suporte Técnico ao Cliente : 800 20 20 22
TMN - Atendimento Especializado de Serviços de Dados : 12030

Prime
Soluções Empresariais

ÍNDICE

1 - O serviço TeamWork

A sua conta TeamWork permite-lhe :

- aceder à sua VPN,
- com segurança através de um túnel IPSec,
- utilizando um PC com sistema operativo Windows,
- a partir da Internet ou
- a partir da rede WiFi da PT ou
- a partir da rede GPRS / TeamWork da TMN.

Presentemente o serviço tem os seguintes condicionalismos:

- Não é utilizável a partir de PDAs ou outros dispositivos que não sejam PCs com Windows;

Para utilizar o serviço TeamWork deverá realizar os seguintes passos :

1. Aceder ao Concentrador de Túneis IPSec da PTPrime (IP 62.48.130.254)
2. Correr no seu PC o programa que estabelece o túnel IPSec até à VPN (TeamWork VPN Client).

Nota : O TeamWork VPN Client poderá ser instalado no seu PC correndo o ficheiro **TeamWork_setup.exe** que encontrará no CD **TeamWork** ou no site da PTPrime - ver pontos 2 e 3.

Depois de ter completado com êxito estas duas etapas deverá ter no seu PC um endereço IP da gama privada da VPN e ter conectividade IP aos *hosts* autorizados.
Nos capítulos seguintes descrevemos detalhadamente estas duas etapas de utilização do serviço e apresentamos uma metodologia de resolução de problemas.

Os requisitos mínimos para a instalação do Cliente Contivity são os seguintes:

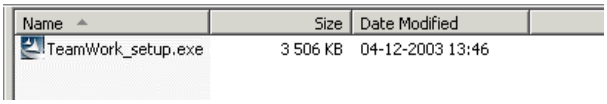
- Windows 95 ou posterior
- Pentium a 200 MHz
- 64 MB RAM
- 10 MB de espaço livre em disco

O acesso à Internet (entre o utilizador remoto e o terminador de túneis L2TP no backbone da PTPrime) deve permitir a passagem dos ports **udp** 500, 10001 e dos protocolos **icmp**, **esp** e **ah**. A reconfiguração de *firewalls* ou outros mecanismos de restrição, que eventualmente bloqueiem estes portos ou protocolos, deverá ser tratada entre os Clientes e os ISP envolvidos. A PTPrime não intervirá neste assunto.

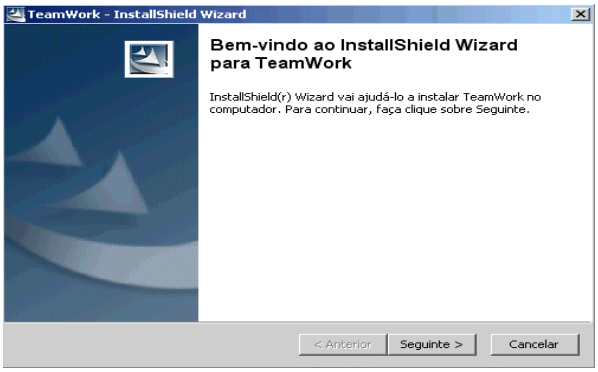
Em caso de dúvidas ou problemas técnicos pode contactar o Número de Suporte ao Cliente: **800 20 20 22**. No caso de dúvidas ou problemas com o acesso GPRS ao serviço TeamWork pode contactar com o Atendimento Especializado de Serviços de Dados da TMN – **12030.**

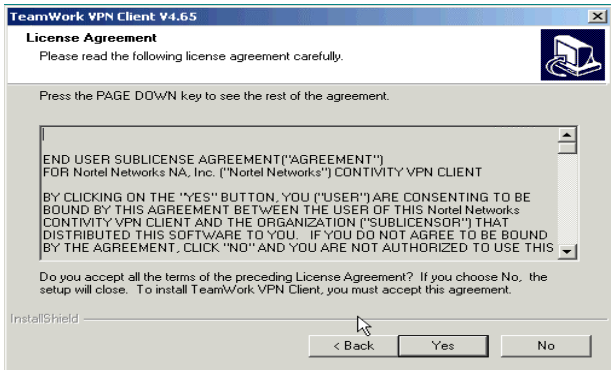
2 - Instalação do TeamWork VPN Client

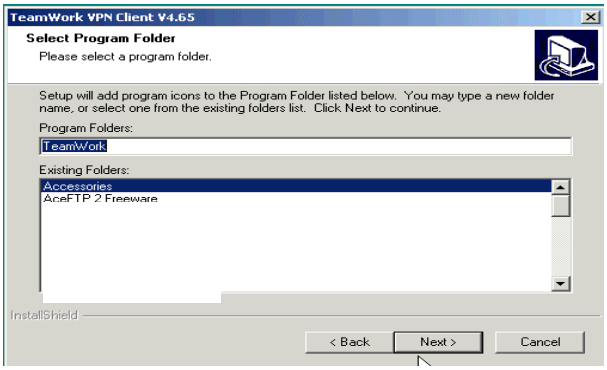
O TeamWork VPN Client é o software que implementa os túneis IPSec entre o PC e o Concentrador de Túneis IPSec da PTPrime. Para instalar este software no seu PC deverá executar o ficheiro **TeamWork_setup.exe** que encontra no CD de distribuição do serviço TeamWork ou no site da PTPrime.

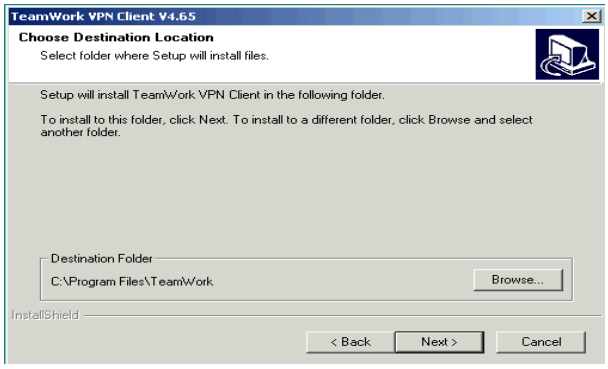


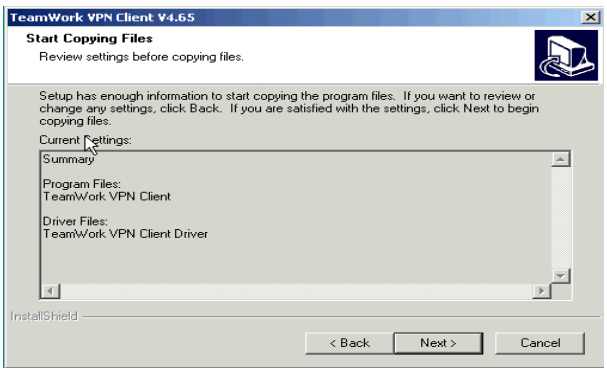
As etapas da instalação são as seguintes:

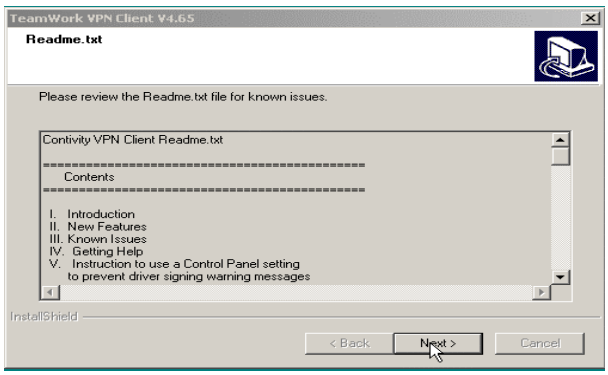












Após a instalação do TeamWork VPN Client deverá ter no seu Desktop o seguinte *shortcut*

No VPN Client que acabou de instalar estão parcialmente pré-configuradas 2 contas que lhe podem facilitar a utilização do serviço TeamWork. A seguir indicamos a utilização de cada uma das contas e a personalização que deve fazer para as activar.

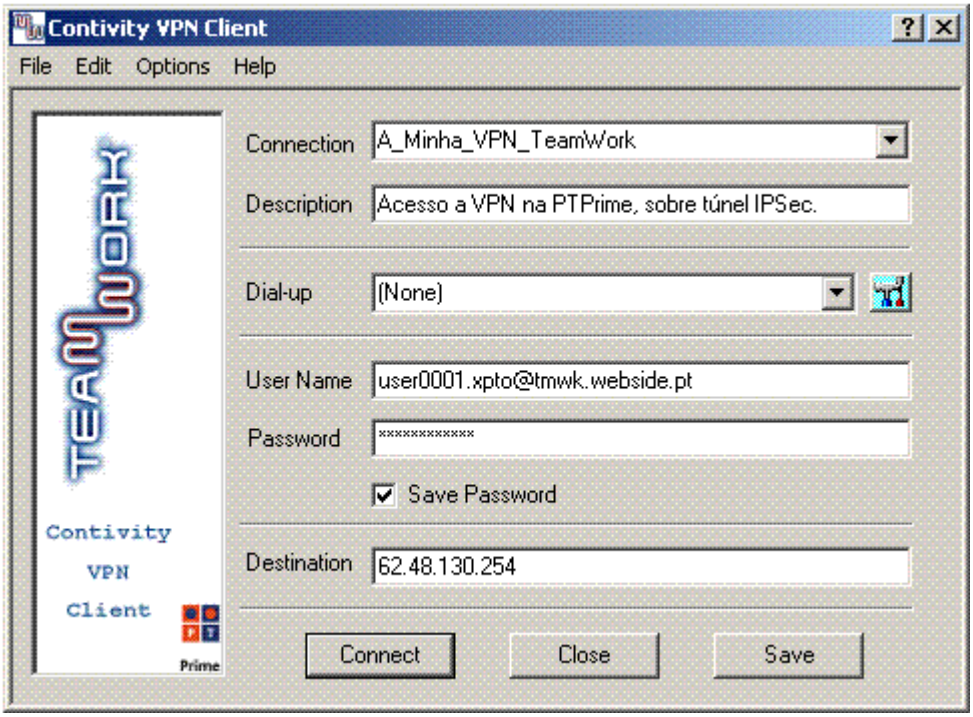
Conta : A_Minha_VPN_TeamWork

Utilização

Esta é a sua conta TeamWork que lhe permitirá aceder à sua VPN.

Personalização a fazer :

1. Pode mudar o nome da conta (Opcional)
2. Substituir o **meu_username** pelo Username correcto da sua conta TeamWork. Normalmente os Usernames tem o formato **userxxxx.<nome_vpn>@tmwk.webside.pt**
1. Inscrever a Password correspondente à sua conta.
2. Fazer Save desta conta



Conta : Teste_TeamWork

Utilização

Acesso à VPN de Teste. A utilizar para facilitar o diagnóstico de problemas no serviço TeamWork.

Personalização a fazer :

1. Substituir os **?** por um dígito (**0** a **9**) de forma a seleccionar uma das 10 contas de teste disponíveis (**teste? showroom@tmwk.webside.pt**.
2. Inscrever a Password correspondente a esta conta de teste com o mesmo dígito (**teste?**).
3. Fazer Save desta conta.

3 - Configuração do TeamWork VPN Client

Antes de utilizar o TeamWork VPN Client tem de o configurar, definindo alguns parâmetros para cada uma das contas, nomeadamente :

Obrigatórios - A fornecer pela PTPrime

- User Name
- Password
- Seleccionar a opção de "Group Security Authentication"
- Seleccionar a opção "Group Password Authentication"
- Group ID
- Group Password

Opcionais

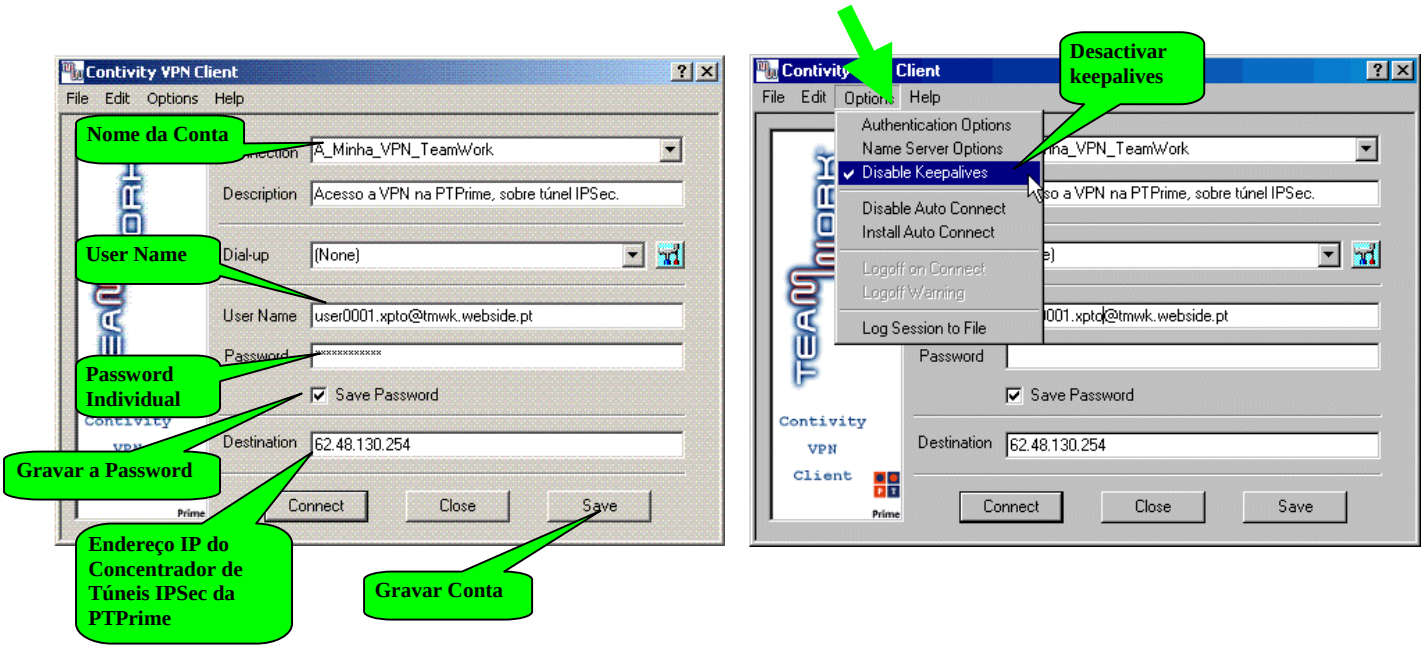
- DNS (Só necessário se a VPN tiver serviço DNS)
- WINS (Só necessário se a VPN tiver serviço WINS)
- Nome do Domínio

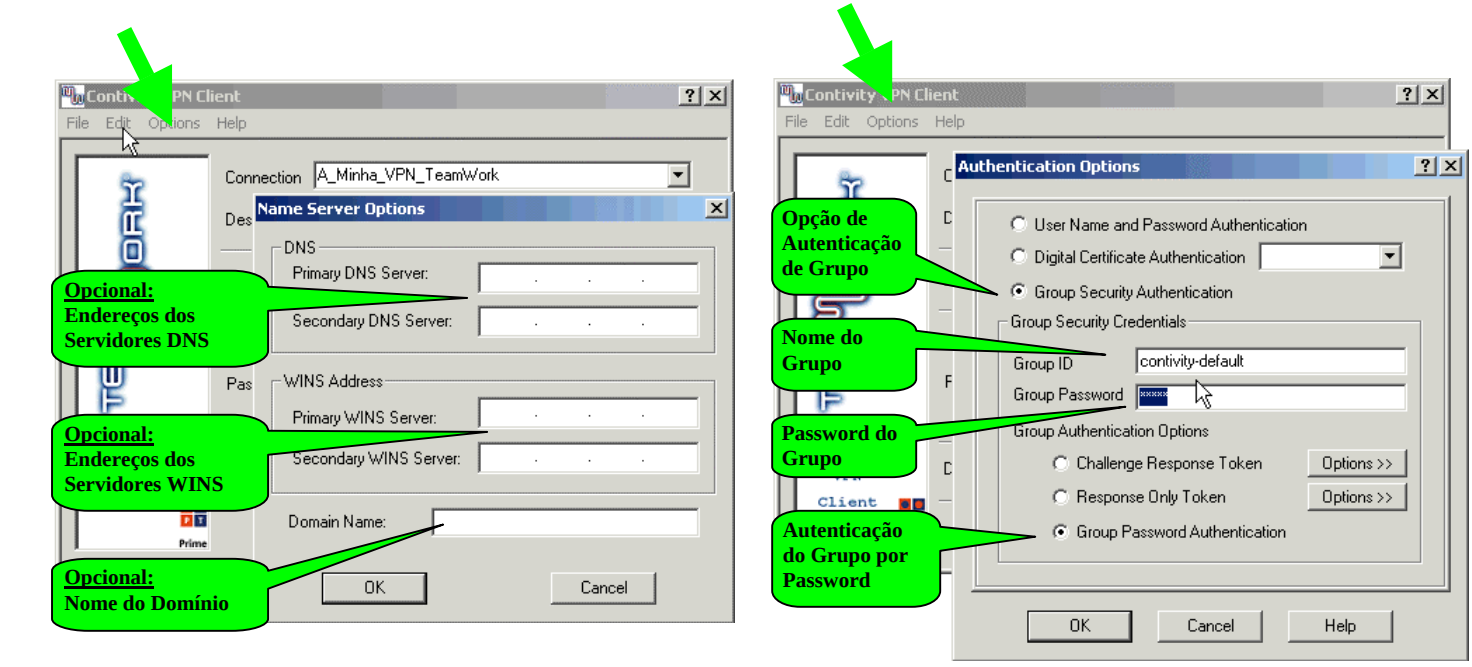
Nota : Cada conta deverá ter um nome, a ser atribuído livremente pelo utilizador.

Deverá também desactivar os "Keepalives" (Cancelar o **!**). Pode activar a opção de "Gravar a Password" da conta. Esta opção só deve ser activada se tiver garantias de que o seu PC nunca irá ser utilizado por outras pessoas que possam aceder ilicitamente à VPN.

Deverá gravar a configuração de cada conta antes de passar para a seguinte ou de fechar o VPN Client.

Nas quatro figuras seguintes indicamos onde deve efectuar cada uma destas acções. Pode encontrar mais informação, em inglês, no "Help" do VPN Client.





O Grupo define um conjunto de parâmetros que são válidos para todos os Utilizadores pertencentes a esse Grupo. Existem alguns Grupos genéricos pré-definidos na VPN mas o Cliente pode acordar com a PTPrime a definição de grupos específicos.

4 - Acesso ao Concentrador de Túneis IPSec

O acesso ao concentrador de túneis IPSec da PTPrime pode ser feito de diferentes formas. Examinaremos em seguidas as mais comuns.

4.1 Acesso por linha telefónica/RDIS ou por ADSL (monoposto)

O seu ISP (**I**nternet **S**ervice **P**rovider) deverá ter-lhe fornecido um *username* e uma *password* que lhe permitem ligar-se à Internet. Utilizando esse username/password e o programa de ligação adequado (por exemplo o *dialer* do Windows) deverá receber, no caso de ser bem sucedido, uma indicação de que está ligado à Internet.
Pode verificar se tem acesso à Internet tentando, por exemplo, aceder a um site seu conhecido. Opcionalmente poderá fazer *ping* para o Concentrador de Túneis IPSec da PTPrime (62.48.130.254).

Poderá depois lançar o **TeamWork VPN Client.** Se já o instalou, deverá ter no Desktop o seguinte *shortcut* :

Se ainda não instalou o TeamWork VPN Client, deverá seguir as instruções do **Capítulo 2 – Instalação do TeamWork VPN Client**.

Se já instalou o TeamWork VPN Client mas ainda não configurou a sua conta TeamWork, deverá seguir as instruções do **Capítulo 3 – Configuração do Teamwork VPN Client**.

Se tiver dúvidas sobre se está ou não ligado à Internet ou sobre o acesso ao Concentrador de Túneis IPSec da PTPrime poderá seguir as instruções do **Capítulo 5 – Resolução de Problemas**.

4.2 Acesso a partir de uma LAN (*routers* ADSL, RDIS ou outros)

Nota importante: A configuração deste tipo de acesso pressupõe alguma experiência de comunicações de dados IP e pode exigir o acesso ao *router*, pelo que é aconselhável que receba apoio de alguém com responsabilidade na administração da LAN.
Em alguns routers quando existe NAT é feito o mapeamento (*bind*) directo dos portos dos protocolos IKE e ESP. Esta funcionalidade, denominada em alguns casos de "NAT Transparent", serve para fazer IPSec a partir de endereços privados sem que o router altere os respectivos portos.
O VPN Contivity Client espera que o porto seja alterado de modo a fazer IPSec sobre o porto UDP 10001 (funcionalidade de "NAT Traversal).

Assim é necessário, em alguns casos, desactivar o mapeamento acima referido de forma a permitir o "NAT Traversal". No CD de instalação do TeamWork existe o ficheiro “TeamWork em Routers ADSL.pdf” onde poderá ver um exemplo da configuração necessária para resolver este tipo de problema. Em caso de dificuldade contacte o N.º de Suporte Técnico ao Cliente da PTPrime (800 20 20 22).
Em caso de dificuldade contacte o N.º de Suporte Técnico ao Cliente da PTPrime (800 20 20 22).

No caso de estar a utilizar um PC ligado a uma LAN deve verificar se tem acesso à Internet tentando, por exemplo, aceder a um site seu conhecido. Opcionalmente poderá fazer ping para o Concentrador de Túneis IPSec da PTPrime (IP 62.48.130.254).

Deve certificar-se também que o seu PC tem um endereço IP público, vendo as **Propriedades** da **Ligação à Rede Local**. Normalmente são públicos os endereços IP que não têm os seguintes formatos: **192.168.x.y**, **172.16.x.y** ou **10.x.y.z,** onde **x y z** são números entre 0 e 255.

Nota: NAT significa **N**etwork **A**ddress **T**ranslation e é a forma de o *router* traduzir os endereços IP privados (válidos na rede privada) em endereços IP públicos (válidos na Internet).

Poderá depois lançar o **TeamWork VPN Client.** Se já o instalou, deverá ter no Desktop o seguinte *shortcut* :

Se ainda não instalou o TeamWork VPN Client, deverá seguir as instruções do **Capítulo 2 – Instalação do TeamWork VPN Client**.

Se já instalou o TeamWork VPN Client mas ainda não configurou a sua conta TeamWork, deverá seguir as instruções do **Capítulo 3 – Configuração do Teamwork VPN Client**.

Se tiver dúvidas sobre se está ou não ligado à Internet ou sobre o acesso ao Concentrador de Túneis IPSec da PTPrime poderá seguir as instruções do **Capítulo 5 – Resolução de Problemas**

4.3 Acesso por Wireless LAN (PT-WiFi)

4.3.1 Resumo

Para poder aceder ao serviço TeamWork através da rede PT WiFi, deverá:

1. Ter recebido da PTPrime duas contas diferentes: uma para o acesso WiFi e outra para o serviço Teamwork. A conta do acesso WiFi tem o formato **userxxxx.<Nome_VPN>@wifi.webside.pt.**
   Nota: Apenas as contas PTPrime WiFi permitem o acesso ao serviço TeamWork.

2. Estar na zona de cobertura de um dos *hotspots* desta rede e ter um dispositivo de acesso (por exemplo uma placa PCMCIA compatível com o standard IEEE 802.11b) devidamente instalado no PC. Pode consultar a lista dos hotspots em http://www.ptwifi.pt.

3. Detectar a presença da rede WiFi e verificar/seleccionar no dispositivo de acesso o SSID (Nome da Rede WiFi) **PT-WIFI.** O protocolo de encriptação **WEP** deve estar desactivado (Ver 4.3.3).

4. Activar um browser (por exemplo o Internet Explorer). Se tentar aceder a alguma página WEB será redireccionado para o portal do *hotspot* que lhe mostrará a página de boas vindas. Pode então fazer *login* utilizando o seu *username* e a *password* da conta WiFi.
   Nota: Deverá a selecção de *proxy* no *browser* antes de se conectar (ver instruções mais adiante - Ver 4.3.2).

Depois de se ter *logado* com sucesso no portal do *hotspot* WiFi, ficará com acesso ao Concentrador de Túneis IPSec da PTPrime (62.48.130.254), mas **não terá** acesso à Internet.

Poderá então lançar o **TeamWork VPN Client**. Se já o instalou, deverá ter no Desktop o seguinte *shortcut* :

Se ainda não instalou o TeamWork VPN Client, deverá seguir as instruções do **Capítulo 2 – Instalação do TeamWork VPN Client**.

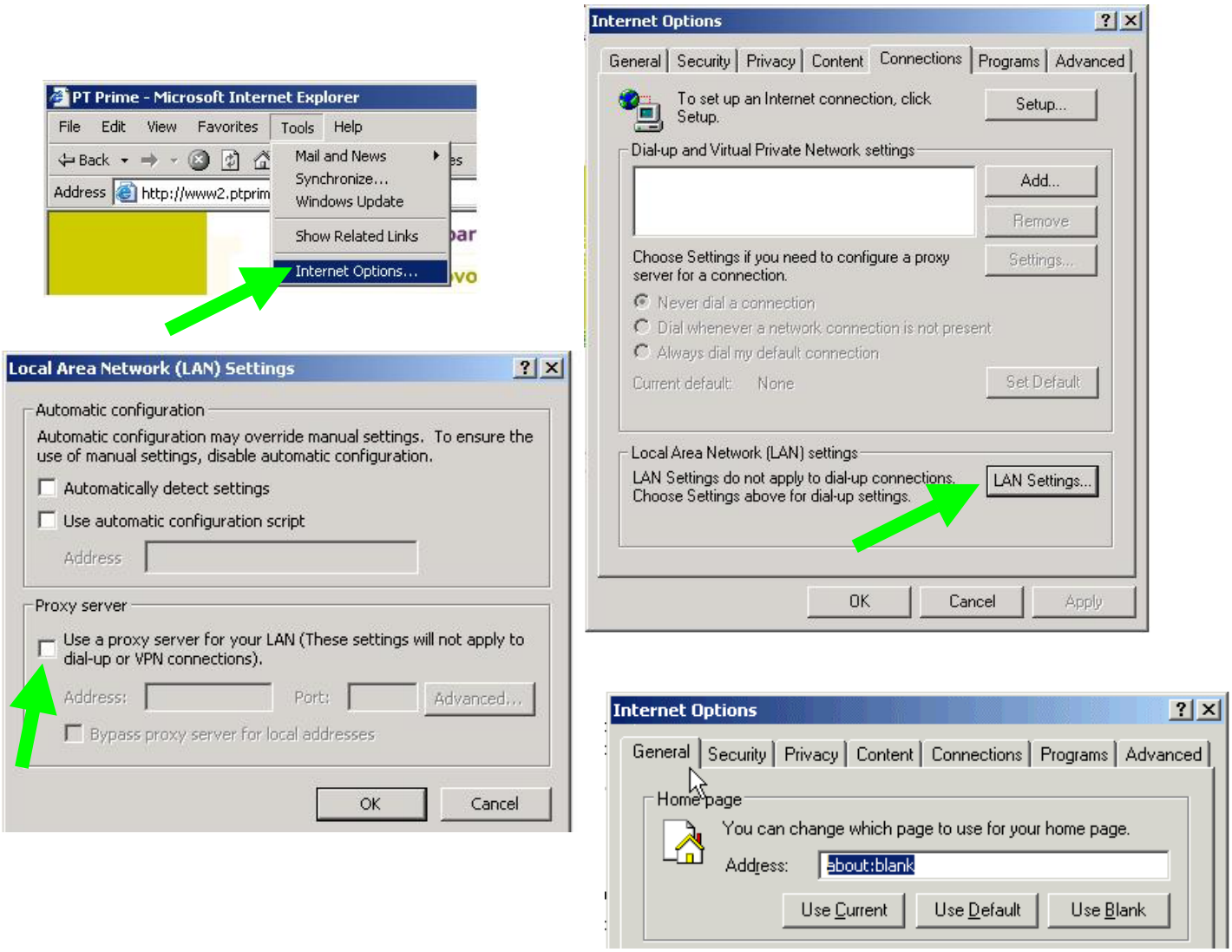
Se já instalou o TeamWork VPN Client mas ainda não configurou a sua conta TeamWork, deverá seguir as instruções do **Capítulo 3 – Configuração do Teamwork VPN Client**.

Se tiver dúvidas sobre o acesso ao Concentrador de Túneis IPSec da PTPrime, poderá seguir as instruções do **Capítulo 5 – Resolução de Problemas**

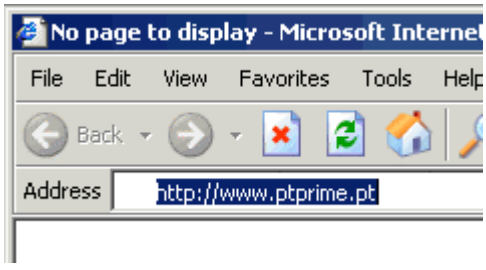
4.3.2 Configuração do browser

Para aceder a um *hotspot* deverá ter um *browser* instalado no seu PC (por exemplo o Microsoft Internet Explorer v.5 ou superior ou o Netscape v.4.7 ou superior).

É necessário que desactive a opção de utilização do *proxy*, como a seguir se mostra.



O *hotspot* redirecciona o acesso inicial do seu *broswer* para o respectivo portal, dando-lhe as boas vindas e permitindo que faça *login* no serviço WiFi. Se tiver a *home page* do seu *browser* configurada como "*about:blank*" não haverá nenhuma tentativa de acesso quando activar o *browser* e o portal do *hotspot* não poderá ser mostrado.



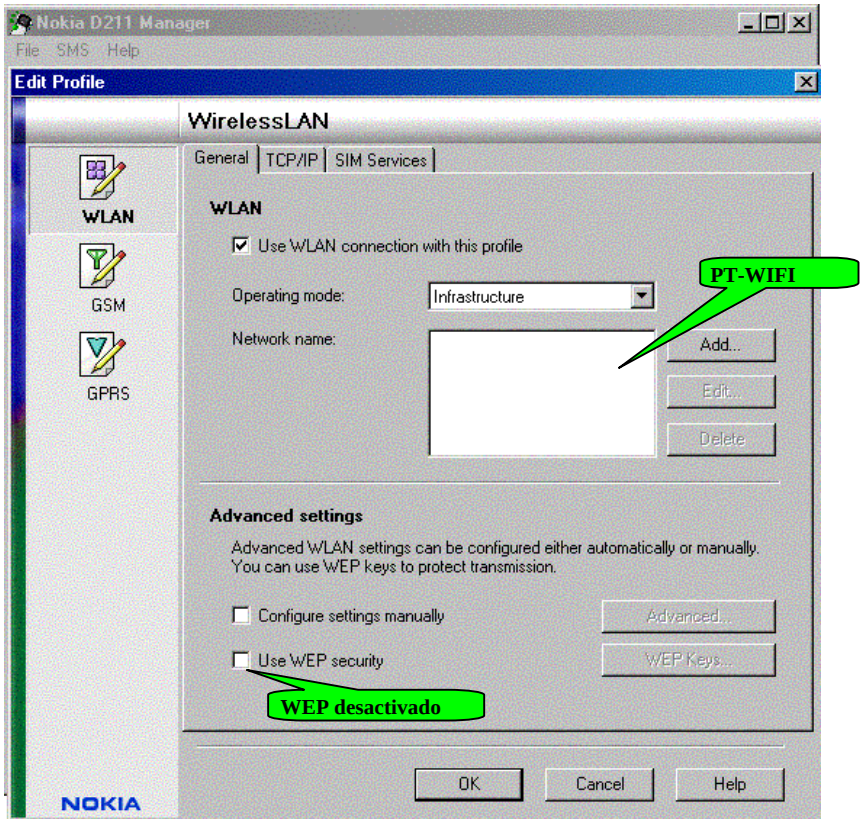
Nesse caso deverá tentar aceder a um site na Internet, por exemplo http://www.ptprime.pt, de forma a ser redireccionado para o portal

4.3.3 Ligação a um *hotspot* PT-WIFI

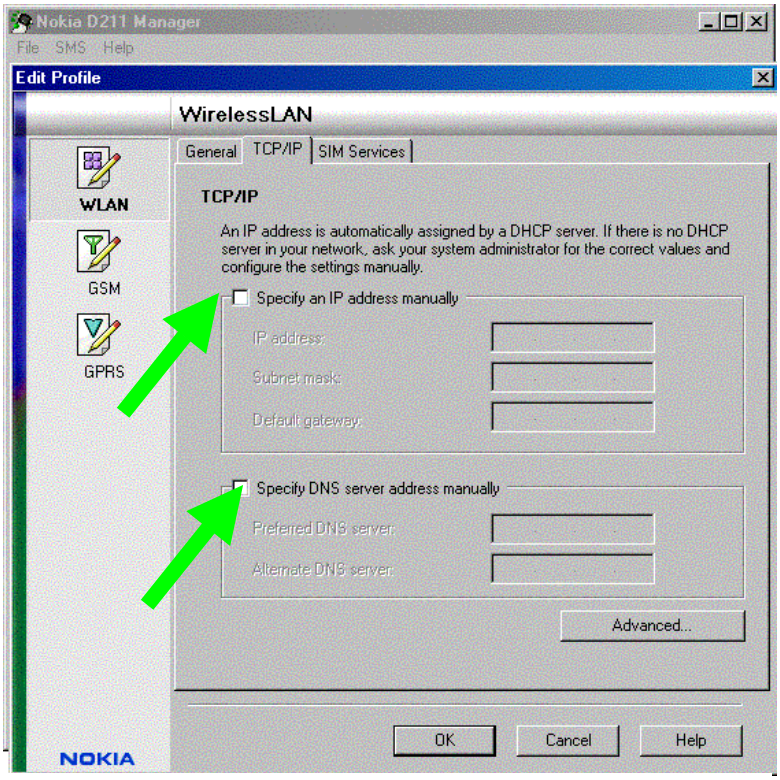
Os diversos dispositivos de acesso a Wireless LANs apresentam, naturalmente, menus de utilização e de configuração diferentes uns dos outros. Deverá consultar o manual do dispositivo que equipa o seu PC e configurá-lo de forma adequada.

A título de exemplo apresentamos os menus de uma placa PCMCIA que suporta o standard 802.11b, relevantes para o serviço PT WI-FI.

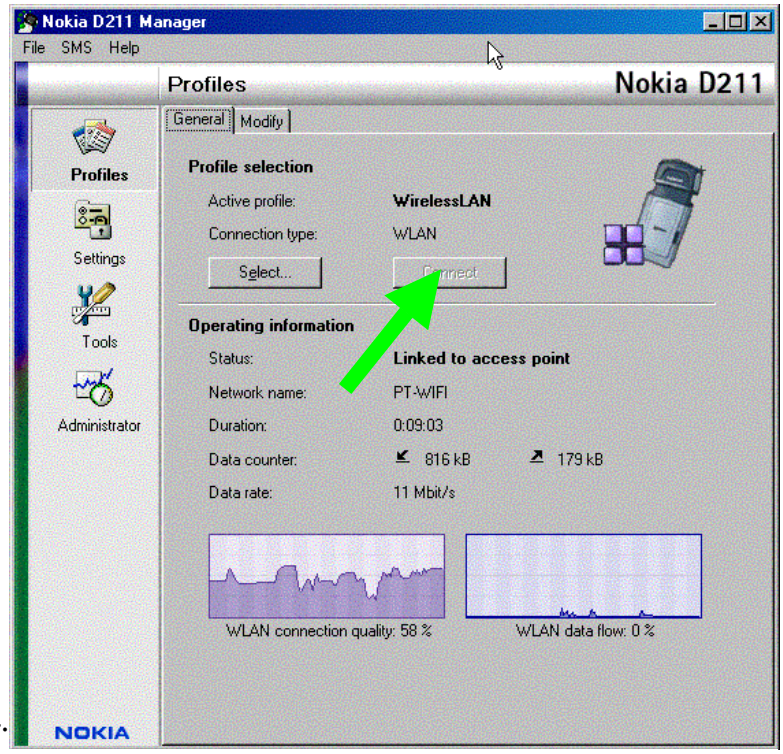
O endereço IP do PC e do DNS deverão ser definidos pela rede WiFi.
O nome da rede a seleccionar (SSID) é **PT-WIFI**



Modo de operação - Infraestruture
WEP – Desactivado
SSID – PT-WIFI

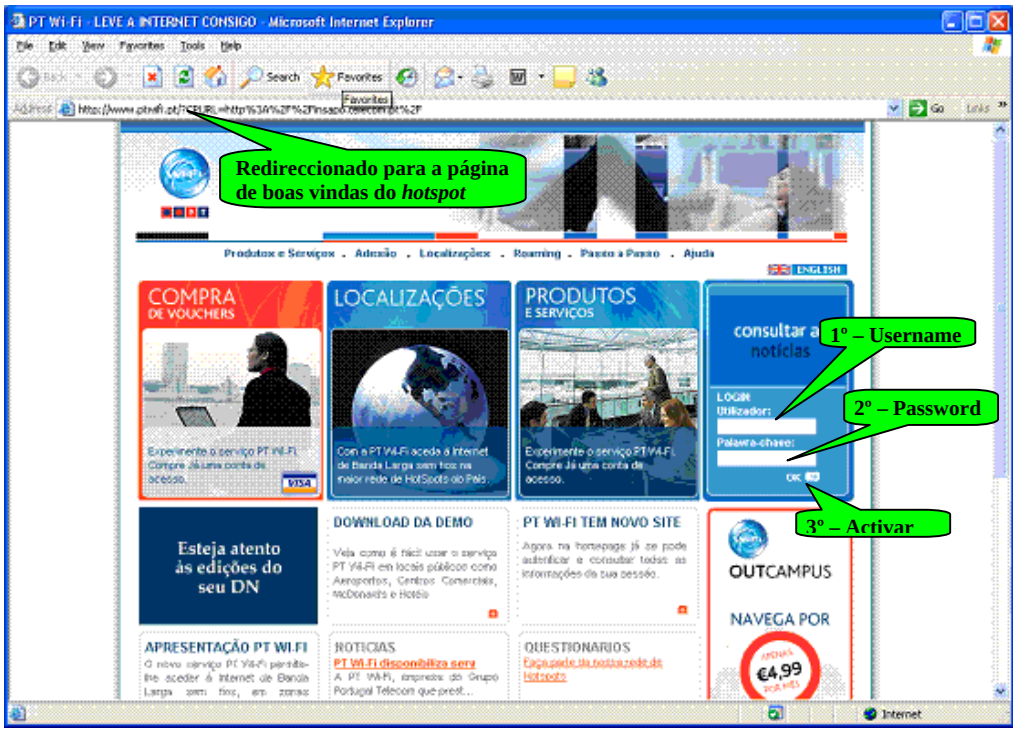


IP - Definido pela rede
DNS - Definido pela rede

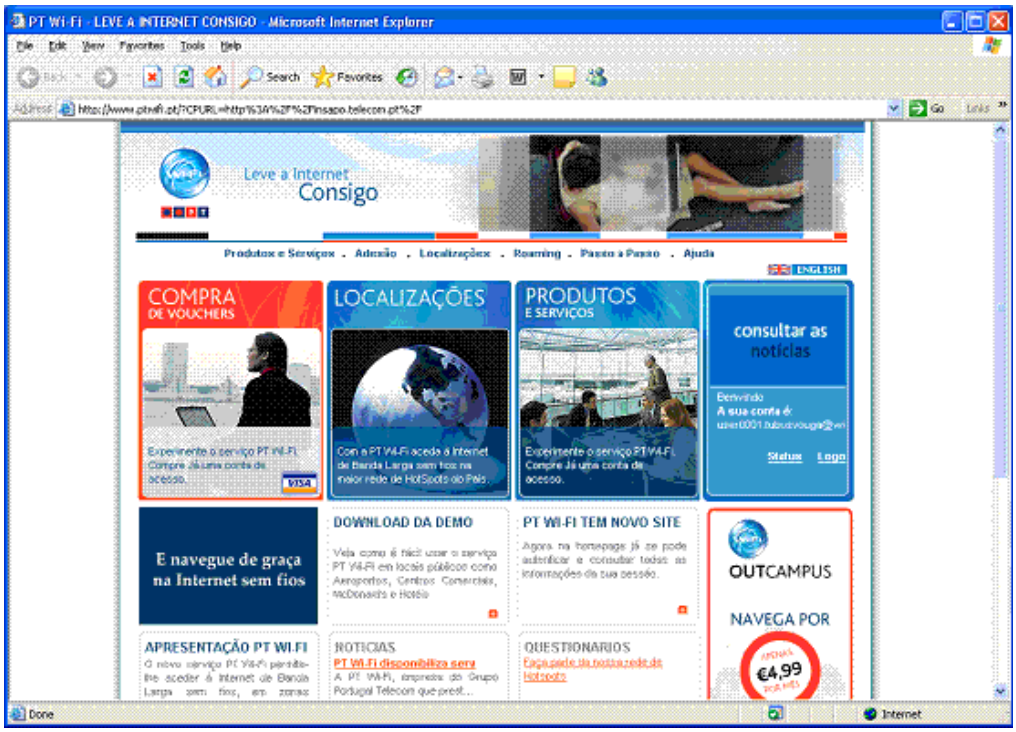
4. 

Em operação / Ligação

Sessão no Portal PT Wi-Fi

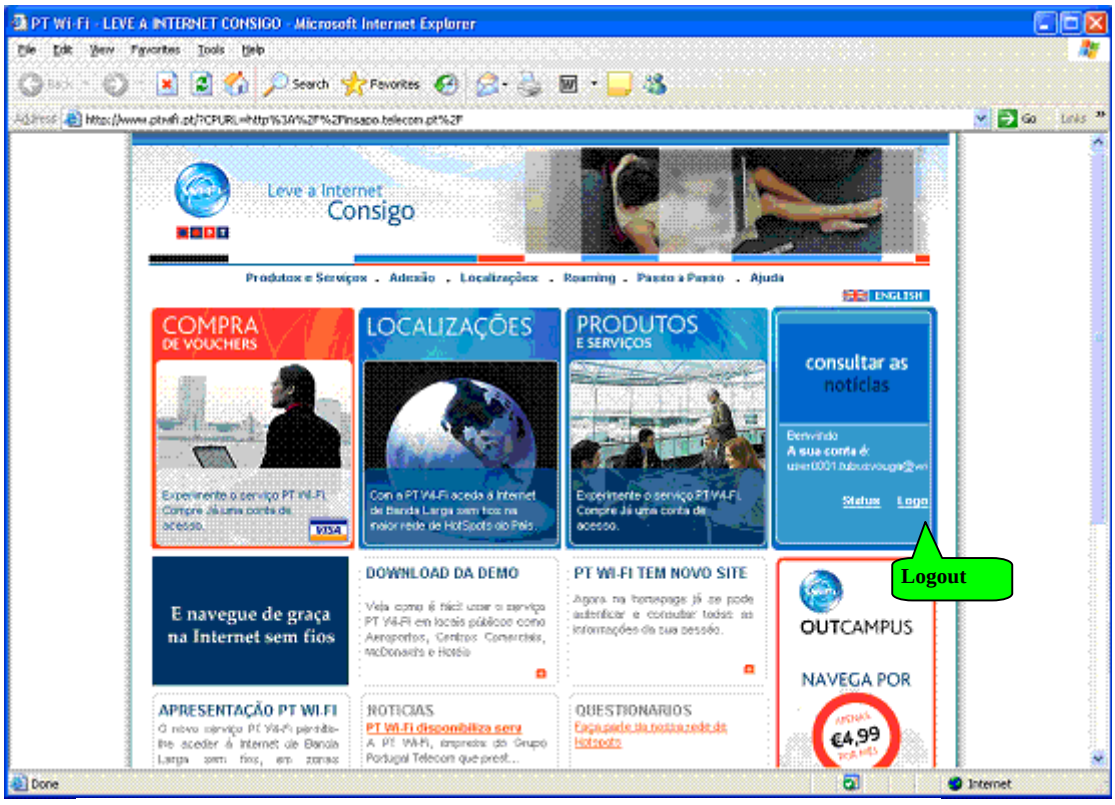


Login no Portal PT Wi-Fi



Boas vindas no Portal PT Wi-Fi, depois de login com sucesso. Pode activar o TeamWork VPN Client.

Informação sobre a Sessão



Logout

4.4 Acesso por GPRS / TMN

4.4.1 Resumo

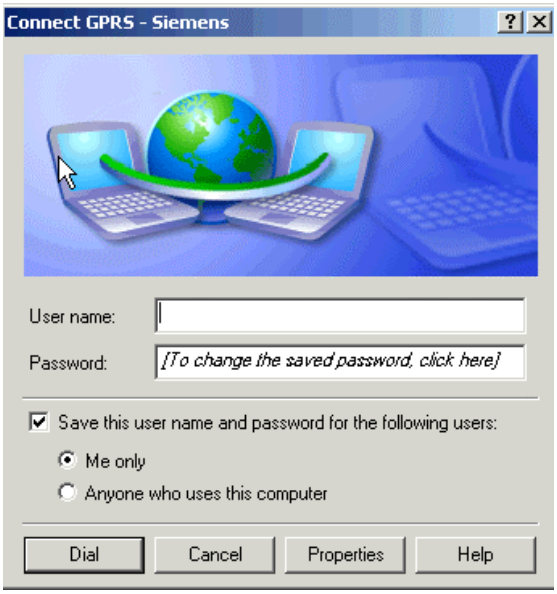
Para poder aceder ao serviço TeamWork através da rede GPRS da TMN deverá:

1. Ter o cartão SIM (Subscriber Identification Module) registado na APN (Access Point Name) **primesec.tmn.pt**
   Nota: Este registo deverá ter sido pedido à TMN na altura da activação do serviço TeamWork.

2. Estar na zona de cobertura GPRS da TMN (ou de um dos operadores com os quais a TMN tem acordo de *roaming*) e ter um dispositivo de acesso (placa PCMCIA, telemóvel ou outro) devidamente instalado ou ligado no PC. Pode consultar a lista dos operadores com *roaming* GPRS em http://www.tmn.pt.

3. Configurar o modem GPRS com a APN correcta. Normalmente isso é feito através de uma *string* de inicialização aditional, com o seguinte formato: **+cgdcont=1,"ip","primesec.tmn.pt".**
   (Ver informação mais adiante - Ver 4.4.2)

4. Aceder à rede GPRS utilizando o *dialer* do Windows, **sem** *username* e **sem** *password*.



5. Depois de se ter ligado com sucesso à rede GPRS/TeamWork da TMN deverá receber um endereço IP privado (da gama 10.35.x.y.) e ficará com acesso ao Concentrador de Túneis IPSec da PTPrime (62.48.130.254), mas **não terá** acesso à Internet. Pode verificar o acesso fazendo um *ping*.

6. Poderá então lançar o TeamWork VPN Client. Se já o instalou deverá ter no Desktop o seguinte *shortcut* :

Nota: O GPRS TMN de acesso à Internet (APN = **internet**) não suporta o serviço Teamwork. Deverá utilizar a APN = **primesec.tmn.pt**

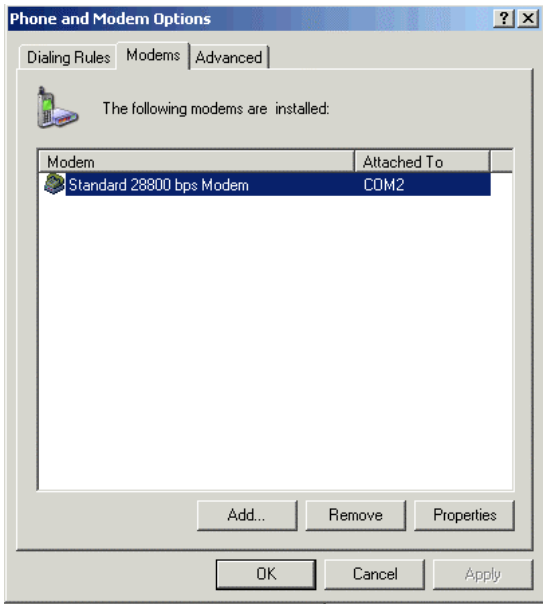
Se ainda não instalou o TeamWork VPN Client, deverá seguir as instruções do **Capítulo 2 – Instalação do TeamWork VPN Client**.

Se já instalou o TeamWork VPN Client mas ainda não configurou a sua conta TeamWork, deverá seguir as instruções do **Capítulo 3 – Configuração Teamwork VPN Client**.

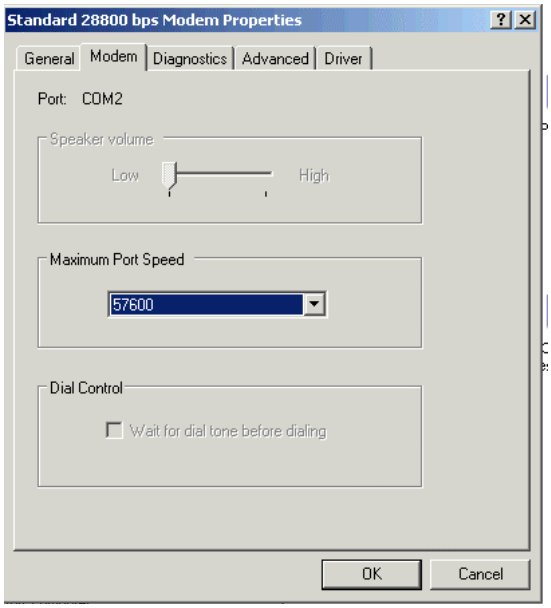
Se tiver dúvidas sobre o acesso ao Concentrador de Túneis IPSec da PTPrime, poderá seguir as instruções do **Capítulo 5 – Resolução de Problemas**

4.4.2 Configuração de modem GPRS

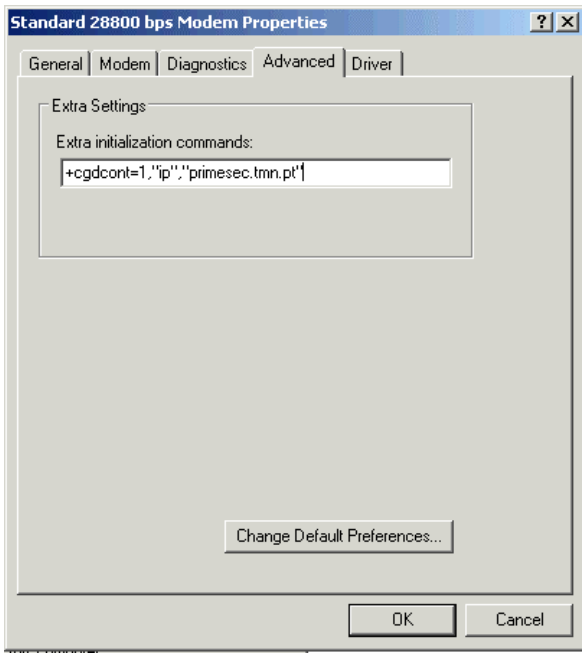
Os diversos dispositivos de acesso GPRS apresentam, naturalmente, menus de utilização e de configuração diferentes uns dos outros. Deverá consultar o manual do dispositivo que equipa o seu PC e configurá-lo de forma adequada.
A título de exemplo apresentamos os menus de modem externo genérico, utilizável em alguns telemóveis que suportam GPRS



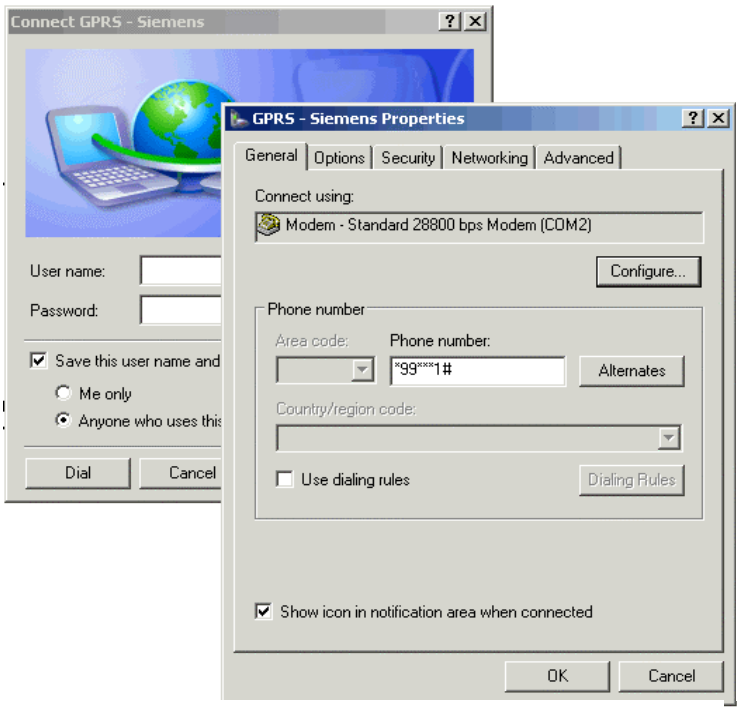
Selecção do Modem Externo



Alteração da Velocidade da porta COM2



String adicional de inicialização (definição APN) :
+cgdcont=1,"ip","primesec.tmn.pt".



Número a marcar pelo telemóvel (***99***1#**)
(Nota : depende da configuração do telemóvel)

O contacto da TMN para suporte a este serviço é o Atendimento Especializado de Serviços de Dados – **12030**

5 - Utilização do Teamwork VPN Client

Para utilizar o VPN Client e aceder à sua VPN deverá:

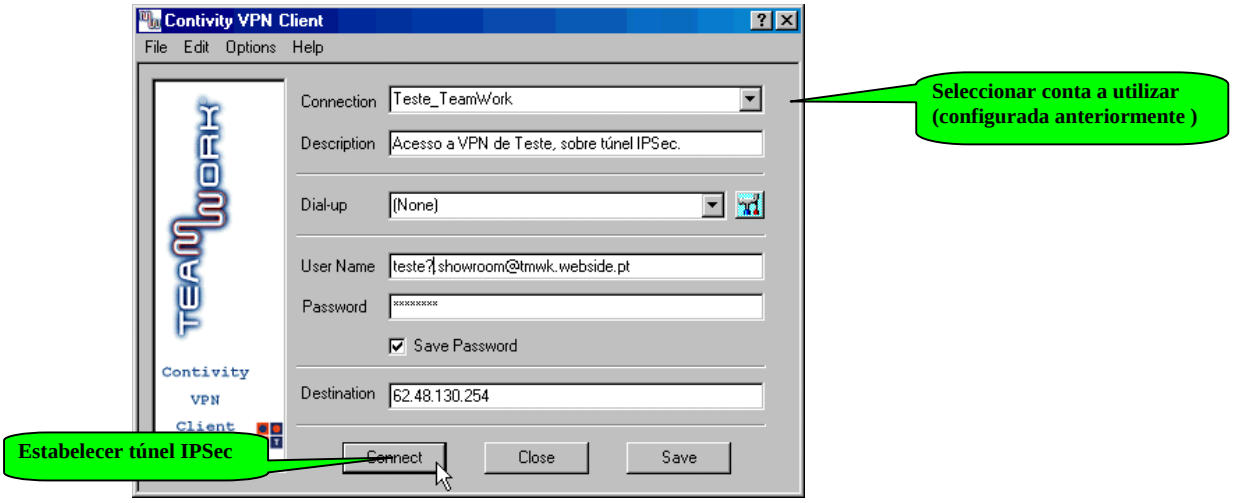
1. Ter configurado anteriormente a conta que vai usar
   (Ver 3 - Configuração do TeamWork VPN Client.
   Nota: O **?** pode ser qualquer dígito de 1 a 9)

2. Estabelecer o acesso ao Concentrador de Túneis da PTPrime
   (Ver 4 - Acesso ao Concentrador de Túneis IPSec)

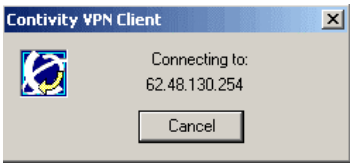
3. Activar o VPN Client utilizando o *shortcut* existente no Desktop

ou correndo o ficheiro que normalmente deverá ter sido instalado em "C:\Program Files\TeamWork\Extranet.exe"

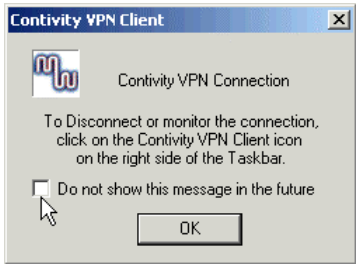
4. Seleccionar a conta pretendida e fazer a ligação (Ver figura seguinte)



Na sequência da ligação ao Concentrador de Túneis deverão surgir as seguintes mensagens :



Ligação a ser estabelecida

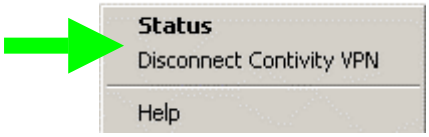


Ligação estabelecida

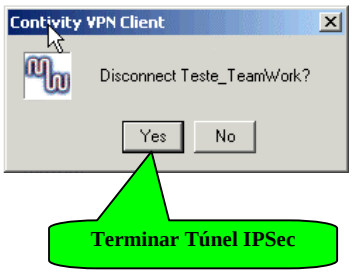
"Ligação estabelecida",
na Notification Area / Task Bar

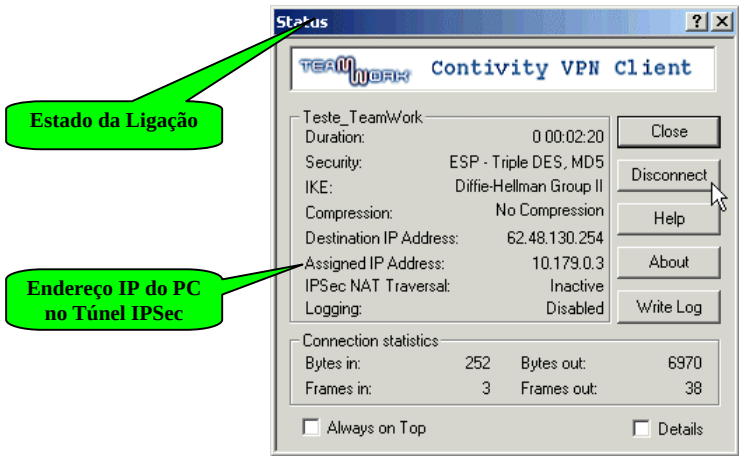
"Ligação estabelecida, com tráfego ",
na Notification Area / Task Bar

Pode ver detalhes da ligação IPSec colocando o cursor sobre o *icon* da ligação na "Notification Area" da Task Bar e clicando no botão direito do rato. Pode então terminar o túnel IPSec ou ver o seu estado.



Visualizar *Status* do túnel IPSEc





Nota : Ao estabelecer o túnel IPSec, o PC recebe um outro endereço IP da gama da VPN, fixamente associado ao username. O PC fica assim com dois endereços IP, um do acesso (Internet, GPRS ou WiFi) e outro do túnel. Para efeitos de comunicação com a VPN, o endereço IP que conta é o do túnel IPSec.

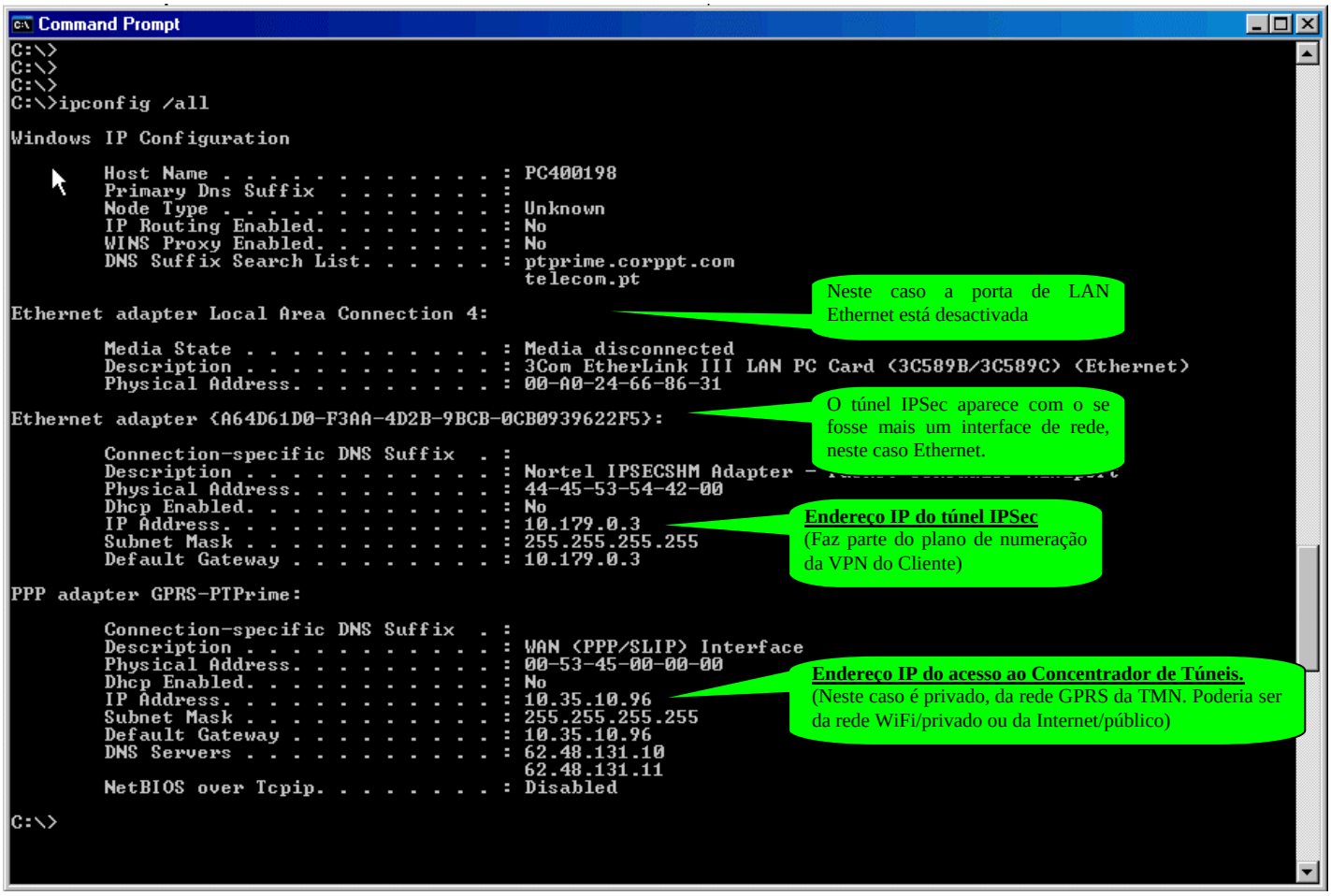
6 - Resolução de problemas

Há diversos programas normalmente disponíveis nos PCs que podem auxiliar na resolução de problemas que eventualmente surjam na utilização do serviço TeamWork. Dependendo da experiência e do tipo de problema em causa, poderá ou não ser possível a sua resolução pelo próprio utilizador. Em caso de necessidade, pode sempre recorrer ao N.º de Suporte ao Cliente (**800 20 20 22**), parte integrante do serviço TeamWork que a PTPrime presta aos seus Clientes.

Neste capitulo apresentamos algumas sugestões que poderão ser-lhe úteis.

6.1 Verificar acesso (Internet, WI-FI, GPRS) e IP obtido

Na linha de comando do DOS (Command Prompt) executar o comando **ipconfig /all**:



(Exemplo no caso de um PC portátil ligado à VPN de teste através de GPRS)

Normalmente são públicos os endereços IP que **não têm** os seguintes formatos: **192.168.x.y**, **172.16.x.y** ou **10.x.y.z,** onde **x**, **y** e **z** são números entre 0 e 255.

No caso de aceder directamente à Internet, o PC tem de receber um IP público. Se não o receber deve verificar a conta do ISP, as configurações, o modem, etc. No caso de se ligar à Internet através de uma LAN remota poderá ter um endereço privado ou público.

No caso do acesso via GPRS/TMN o utilizador deve configurar o telemóvel ou a carta PCMCIA com a APN do serviço TeamWork – **primesec.tmn.pt.** Ao ligar-se ao serviço GPRS (sem username/password), deverá receber um endereço IP da gama 10.35.9.1 a 10.35.9.254 ou da gama 10.35.10.1 a 10.35.10.254.

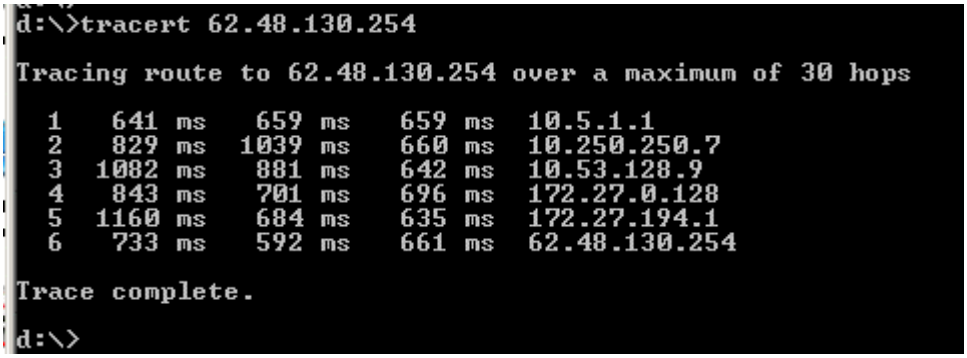
Se não receber o endereço IP correcto, deverá verificar as configurações do telemóvel ou da carta GPRS, nomeadamente a APN configurada. Deverá também certificar-se, junto da PTPrime ou da TMN, se o seu número de cartão SIM (96xxxxxxx) está inscrito na APN **primesec.tmn.pt**. O contacto da TMN para suporte a este serviço é o Atendimento Especializado de Serviços de Dados - **12030**

No caso de acesso WI-FI, a conta de acesso tem o formato **userxxxx.<Nome_VPN>@wifi.webside.pt** e o endereço IP recebido é privado da gama 172.23.x.x. Se não receber o endereço IP correcto, deve verificar se há cobertura WiFi, as configurações da placa WI-FI e a conta do cliente (username/password).

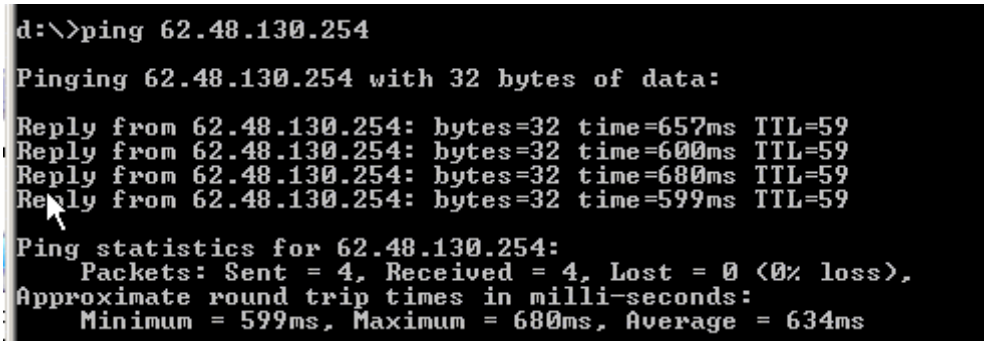
6.2 Verificar se o PC tem acesso ao Concentrador de Túneis

Depois de verificar que está ligado à Internet ou às redes GPRS/TMN ou PT-WIFI, poderá testar a conectividade com o Concentrador de Túneis, utilizando o *ping*.

A seguir apresentamos um exemplo de *ping* feito a partir de um PC portátil, via GPRS.



No caso de contactar com o Suporte ao Cliente (**800 20 20 22**) da PTPrime ou o Atendimento Especializado de Serviços de Dados da TMN (**12030**), poderá ser solicitado a fazer um "trace route" a partir do seu PC. A seguir apresentamos o resultado de um comando **tracert 62.48.130.254**.



6.3 Estabelecimento do Túnel IPSec

Tendo conseguido estabelecer uma ligação IP ao Concentrador de Túneis, pode agora tentar estabelecer um túnel IPSec. Para tal deverá ter configurado uma conta no VPN Cliente, e pressionado o botão "Connect".

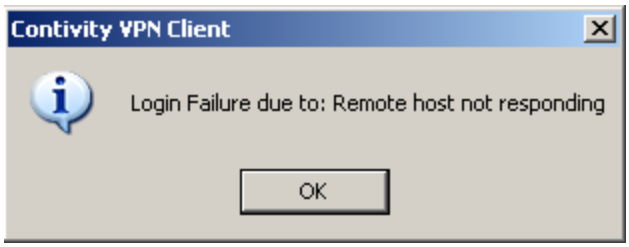
Em caso de insucesso, deverá receber uma mensagem do VPN Client que o auxiliará a diagnosticar o problema:

Mensagem :

Causa provável :
O VPN Client não conseguiu negociar o Túnel. Isto significa que, embora haja conectividade (testada antes) entre o PC e o Concentrador de Túneis, não é possível estabelecer o túnel IPSEC. Este problema pode ocorrer mais frequentemente em acessos feitos a partir de LANs remotas e é devido a *Firewalls* ou *access-lists* (provavelmente na LAN remota) que não permitem o tráfego IPSEC ,

Acção : Deverá contactar o administrador da LAN remota onde está ligado.

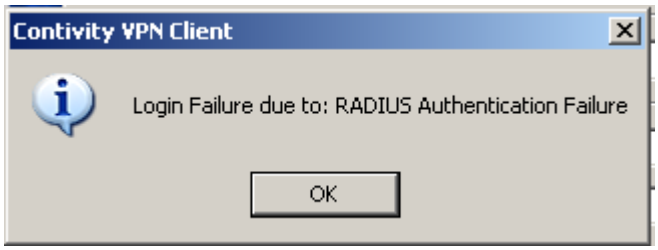
Mensagem :



Causa provável :
Problemas com o NAT/PAT. Se existir PAT (NAT N:1 ou de 1:1 mas com PAT) o VPN Client não funciona.

Acção : Deverá contactar o administrador da LAN remota onde está ligado.

Mensagem :



Causa provável : Username ou password errada

Acção : Verificar e corrigir o Username individual, o GroupID e as respectivas passwords.

6.4 Acesso à VPN de Teste

Depois de estabelecido o túnel pode ver o respectivo estado *clicando* no ícone "Ligação estabelecida" na "Notification Area" da "Task Bar" do Windows. Está agora ligado à VPN por meio de um túnel IPSec e deverá poder aceder a todos os recursos aos quais o endereço IP que recebeu lhe dá direito.

Uma forma de testar o acesso é fazer *ping* para o endereço IP do servidor que pretende atingir. O facto de não receber resposta pode significar que não tem conectividade até esse servidor ou que ele não está autorizado a responder a *pings*.

Se conseguiu estabelecer o túnel e não tem acesso aos recursos que pretende atingir deverá certificar-se junto do administrador da rede Informática da que está autorizado para tal.

A PTPrime disponibiliza uma VPN de teste à qual poderá aceder. Nessa VPN existe um servidor HTTP (um site WEB) e um servidor FTP (anonymous / só download) que responde a pings.

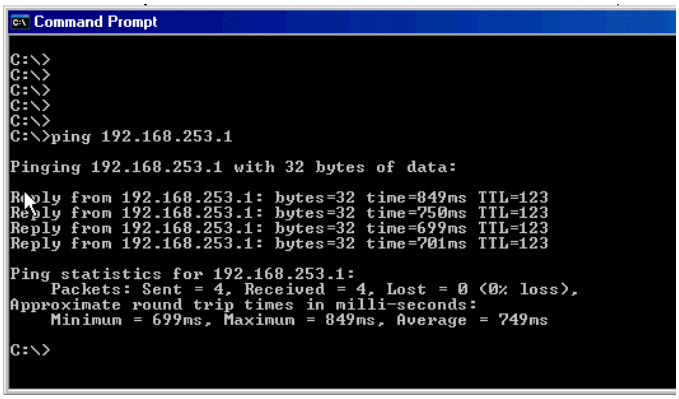
Actualmente as contas TeamWork desta VPN tem os seguintes usernames e passwords (**?** pode ser qualquer dígito de 1 a 9):

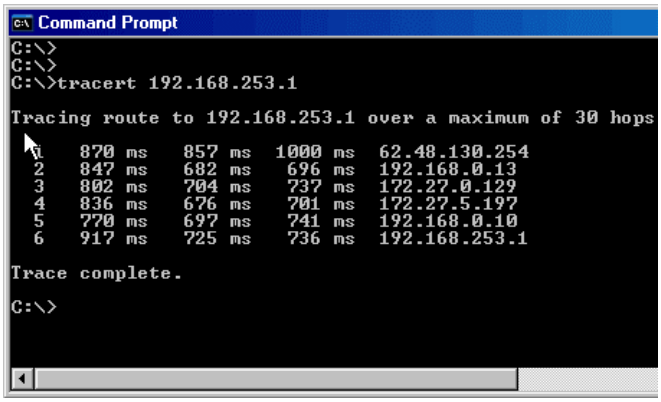
- Username : **teste?.showroom@tmwk.webside.pt**
- Password : **teste?**
- GroupID : **contivity-default**
- Group Password : **ipsec**

O endereço do servidor é 192.168.252.2.

Pode aceder ao site escrevendo no *browser* o seguinte URL : **http://192.168.252.2**

Pode fazer *ping* ou *trace route* escrevendo na linha de comando do DOS (Command Prompt) o comando **ping 192.168.252.2** ou o comando **tracert 192.168.252.2**. A seguir apresentamos exemplos destes comandos, com o acesso via GPRS.





Para fazer o *download* de um ficheiro do servidor FTP existente no mesmo endereço, deverá utilizar um programa FTP (que pode obter na Internet) ou executar na linha de comando do DOS (Command Prompt) o comando **ftp 192.168.252.2.**

6.5 Utilização de TeamWork em LANs

A configuração deste tipo de acesso pressupõe alguma experiência de comunicações de dados IP e pode exigir o acesso ao router, pelo que é aconselhável que receba apoio de alguém com responsabilidade na administração da LAN.

Em alguns routers quando existe NAT é feito o mapeamento (bind) directo dos portos dos protocolos IKE e ESP. Esta funcionalidade, denominada em alguns casos de "NAT Transparent", serve para fazer IPSec a partir de endereços privados sem que o router altere os respectivos portos.

O VPN Contivity Client espera que o porto seja alterado de modo a fazer IPSec sobre o porto UDP 10001 (funcionalidade de "NAT Traversal).

Assim é necessário, em alguns casos, desactivar o mapeamento acima referido de forma a permitir o "NAT Traversal". No CD de instalação do TeamWork existe o ficheiro "**TeamWork em Routers ADSL.pdf**" onde poderá ver um exemplo da configuração necessária para resolver este tipo de problema. Em caso de dificuldade contacte o N.º de Suporte Técnico ao Cliente da PTPrime (800 20 20 22).

7 - Glossário

Access-lists – Lista de autorizações ou proibições que definem quais os endereços e quais os protocolos autorizados a aceder a determinado ponto da rede.

Access Point (AP) - Equipamento que serve de ponto de ligação dos utilizadores *wireless* à infra-estrutura WiFi.

ADSL - Asymmetric Digital Subscriber Line

AH - Authentication Header protocol .

APN - Access Point Name. Identifica uma Rede de Dados com Comutação de Pacotes no âmbito de um operador GPRS

DNS - Domain Name Service

ESP - Encapsulating Security Payload protocol

Firewall – Dispositivo que vigia o tráfego de entrada e saída numa rede, de forma a implementar as regras de segurança definidas para essa rede. Analisa os endereços de origem e destino e os protocolos utilizados.

FTP - File Transfer Protocol

GPRS - General Packet Radio Service

Hot Spot - Local com acesso a uma rede *wireless* pública

HTML - HyperText Markup Language

HTTP - Hypertext Transfer Protocol

ICMP - Internet Control Message Protocol

IEEE - Institute of Electrical and Electronics Engineers

IEEE 802.11b - Standard para LANs wireless a 11 Mbps, elaborado pelo IEEE.

> **Modo Ad-hoc -** Os utilizadores *wireless* comunicam directamente entre si
>
> **Modo Infrastructure -** Os utilizadores *wireless* comunicam entre si através de Access Points.

IP - Internet Protocol

IPSec - Internet Protocol Security

Keepalives - Pequenas mensagens que servem para manter uma ligação activa mesmo na ausência de tráfego real.

LAN - Local Area Network

NAT - Network Address Translation

PCMCIA - Personal Computer Memory Card International Association .

PAT - Port Address Translation

ping - Programa que testa o acesso a um dado endereço IP enviando uma mensagem e aguardando a resposta.

Proxy - Agente, intermediário. Equipamento que recebe uma solicitação de acesso a uma página WEB da parte de um PC, faz ele mesmo o acesso à página WEB e devolve ao PC inicial a informação que recolheu.

RADIUS - Remote Authentication Dial-In User Service

RDIS - Rede Digital com Integração de Serviços

Roaming - Funcionalidade que permite o utilizador mudar de rede *wireless* (WiFi , GSM, GPRS,..) e continuar a ter acesso ao serviço que contratou no seu operador de origem.

SSID - Service Set Identifier. Nome da rede WiFi.

trace route - Programa que permite traçar a rota de comunicação entre um utilizador e um outro computador identificado por um endereço IP. Devolve uma lista de todos endereços IP por onde a comunicação passa.

UMTS - Universal Mobile Telecommunications System

UDP - User Datagram Protocol

URL – Universal Resource Locator. Identificação de site na Internet.

VPN - Virtual Private Network

VPN Client - Programa que corre no PC do utilizador (ou num router de uma LAN remota) e que permite estabelecer um túnel de acesso a uma VPN, atravessando com segurança a infra-estrutura pública de comunicações.

WAN - Wide Area Networking

Web Browser - Software que permite aceder a documentos HTML (Páginas WEB)

WEP - Wired Equivalent Privacy. Protocolo de segurança para redes *wireless*

WIFI - (Wireless Fidelity). Designação comum das comunicações *wireless* baseadas no standard IEEE 802.11b.

WINS - Windows Internet Naming Service

Wireless - Tecnologia de comunicações em que os utilizadores acedem "sem fios" à infra-estrutura fixa do operador. Além do WiFi, também o GPRS, o UMTS e outros são *wireless*.

WPA - WiFi Protected Access. Protocolo de segurança para redes *wireless.*