IP Telephony Over Internet Virtual Private Network (VPN)

Case Study

Panasonic Communications Company UK Ltd
Version: 0.0.2

IP Telephone Over Internet Virtual Private Network (VPN)

DISCLAIMER

This document has been prepared by Panasonic Communications Company UK (PCCUK) Ltd., as part of its commitment to provide relevant information technology (IT) educational documents. PCCUK reserves the right to revise and make necessary changes to this manual without the obligation to notify any person or organization of such revisions or changes. All reasonable precautions have been taken in the production and preparation of this material, including both technical and non-technical proofing. However, PCCUK assumes no responsibility for any errors or omissions. No warranties are made, expressed or implied with regard to this material. PCCUK shall not be responsible for any direct, incidental or consequential damages arising from the use of any material contained either in this or any associated documents. All third party trademarks used in this document belong to the respective trademark owners.

Contributing Author(s): Syed Ahmad
Contact: syed.ahmad@eu.panasonic.com

Table of Contents

Audience

This document is intended for those familiar with Panasonic KX-TDA PBX programming and installations and are trying to educate themselves with knowledge of IP technology and data networking concepts so as to be able to perform better sales and support of IP technology based advanced business telephony solutions.

This document is part of a series of information technology (IT) educational documents prepared by Panasonic Communications Company UK (PCCUK) Ltd., as part of its commitment to providing helpful educational materials to help those selling and supporting Panasonic PBXs.

Some of the concepts and information discussed in this document may be basic to some of the readers, however it is recommended to be read in its entirely. It is assumed that an end-to-end reading of this document should give the reader enough information to be able to understand some of the issues around setting up VoIP (Voice over IP) based telephony solutions.

It is assumed that the reader has read and reviewed the document titled "Understanding IP Ports – An Introduction" before studying this document.

Managers and Sales/Marketing personnel are encouraged to read atleast the following sections:

- **Introduction**
- **Broadband Internet Access**

The rest of the document is geared towards those involved in actual installation of Panasonic IP telephony systems.

Goal

The goal of this document is to provide an advanced level of knowledge that is necessary to be able to:

a. Understand the basics of Broadband Internet.
b. Understand the basics of Setting up a DSL Broadband Internet Connection
c. Learn how to setup a Panasonic IP Phone over an Internet IP VPN link

Using these techniques together with relevant TDA PBXs (TDA100, TDA200, & TDA600) should help in installing and implementing advanced VoIP Telephony solutions.

Introduction

IP Telephony or Voice Over IP (VoIP) is a technology where voice signals are converted into IP packets and transported over IP networks. Once the packets reach the destination – they are converted back into voice signals for human listening and understanding.

As Internet has become the primary source of most forms of communications – **Internet Service Providers (ISPs)** have implemented various technologies to provide higher bandwidth access to the Internet for relatively low cost. This has resulted in affordable highspeed Internet commonly termed **Broadband Internet** for most users around the world.

IP Telephone Over Internet Virtual Private Network (VPN)

Panasonic IP Telephony Solutions such as the KX-NT136 IP phones combined together with easy and affordable Broadband Internet access services and low-cost IP VPN Routers are a compelling way for Small to Medium size businesses to allow employees to not only connect back to their office remotely for email and data communications but at the same time companies with Panasonic TDA PBXs can now offer employees the ability to use IP telephones over the same high speed Broadband Internet access. Deploying Panasonic IP telephony solution addresses the needs of businesses by empowering remote employees with easy and convenient access to all the feature rich capabilities of the Panasonic TDA PBXs – regardless of their geographic location.

It should be noted that since Internet is an unmanaged IP network – in order to ensure that the data and voice communication over Internet is reliable as well as secure – an IP Virtual Private Network (IP VPN) **must** be established over the Broadband Internet access.

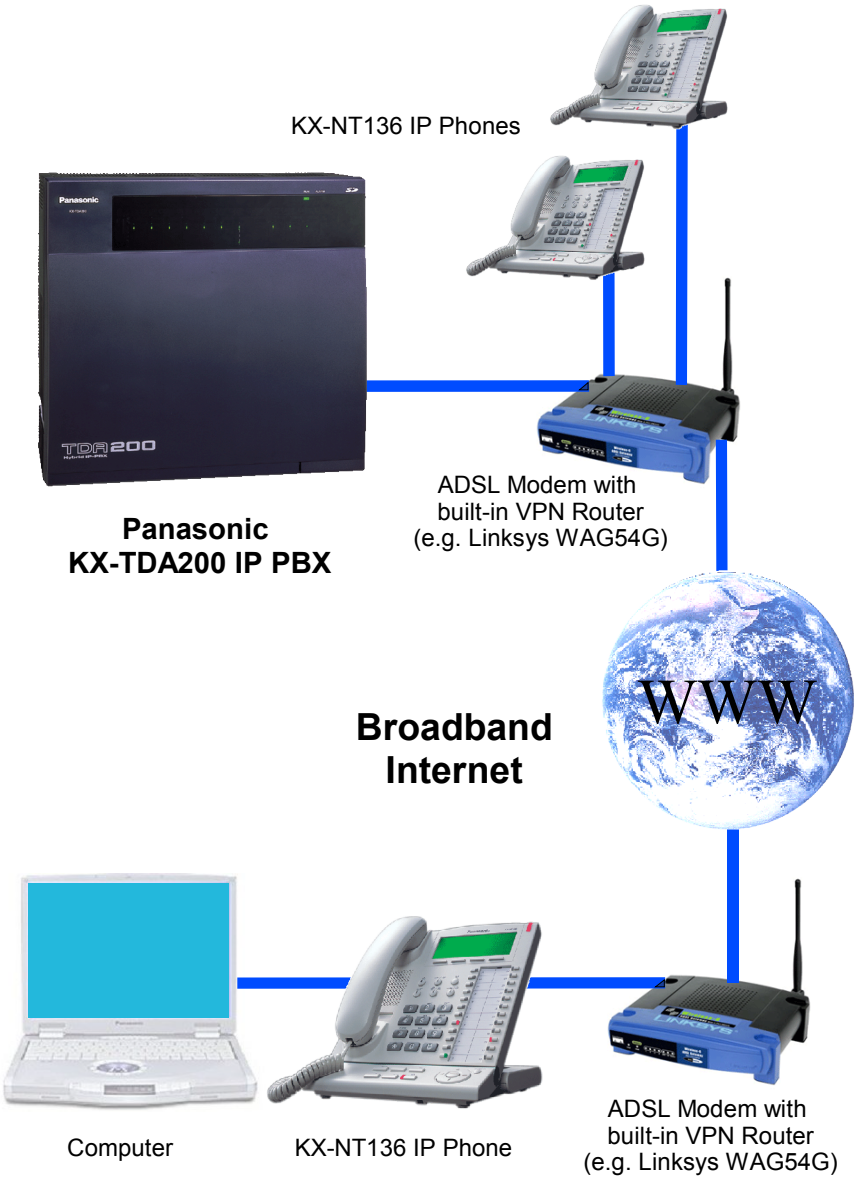


Illustration 1- IP Telephony Over Broadband Internet Connection

Broadband Internet Access

The term **Broadband Internet Access**, often shortened to "broadband Internet" or just "broadband" is a high data-transmission rate Internet connection. Although the **International Telecommunication Union (ITU-T)** has defined broadband as a transmission capacity that is faster than primary rate ISDN (i.e. More than 1.5 to 2 Mbit/s), in general - any Internet access that is 256 kbit/s (0.256 Mb/s) or more is considered as broadband.

Access technologies that most commonly are used by individuals or companies for Broadband access are:
a. Cable (or more specifically Hybrid Fiber Coax), and
b. DSL (Digital Subscriber Line)

Cable Internet Access:

Broadband Internet over Coaxial Cable is basically provided by using unused bandwidth over Cable Television Network infrastructure that provides Cable Television transmission to individual user's homes.

A weakness generally seen in Cable Internet access is that users in a neighborhood share the available bandwidth provided by a single coaxial cable line. Based on sharing of bandwidth on the local network – access speeds can vary depending on the number of users using the service at the same time as well as the type of content being downloaded. Another perception of weakness of cable networks is the risk of loss of privacy, especially considering the easy availability of network sniffing and hacking tools.

However these initial concerns have mostly been addressed by the Cable Internet access providers using bandwidth control, privacy features and encryption mechanisms.

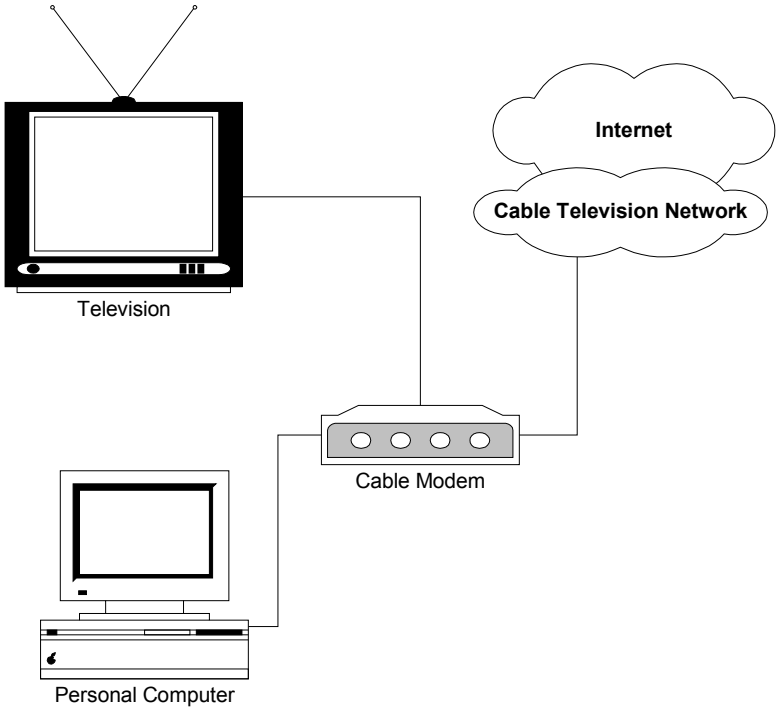


Figure 1- A Typical Cable Modem Broadband Access Setup

IP Telephone Over Internet Virtual Private Network (VPN)

Data over Cable travels from the subscriber to a device called a CMTS (Cable Modem Termination System) or simply Headend. This devices separates the TV signals from the IP Data packets – which are then passed on to the IP network of the Internet Service Provider (ISP).

From an IP Telephony point of view - the Broadband Internet service offered over Cable is just as good as the Broadband Internet service provided over DSL infrastructure.

DSL Broadband Access:

Digital Subscriber Line, or DSL, is a family of technologies that provide a digital connection over copper wires used to provide local analog telephone service by the telephone companies. By using a higher carrier frequency and modulating digital data – unused frequency spectrum is used to achieve high speed data transmission rates. This allows an ordinary phone line to provide digital communication without blocking access to voice services.

At the subscriber end – equipments like Computers, LAN Switches, IP Telephones etc are connected via a DSL modem to the DSL Broadband access network. The DSL modem establishes a high speed transmission over which data is transported.

In addition the subscriber may need to install a passive electronic filter (sometimes called a "micro-filter" or "splitter") if they want to continue to use standard telephones on the same line. The filter ensures that the DSL modem receives the high frequency data signal while the analog telephone receives the proper low frequency signals required to handle voice. Once the data reaches the telephone exchange office (commonly called a **CO**) a device called Digital Subscriber Line Access Multiplexer (DSLAM) terminates the DSL circuits, combines the data streams, separates voice and connects the data to the Internet.

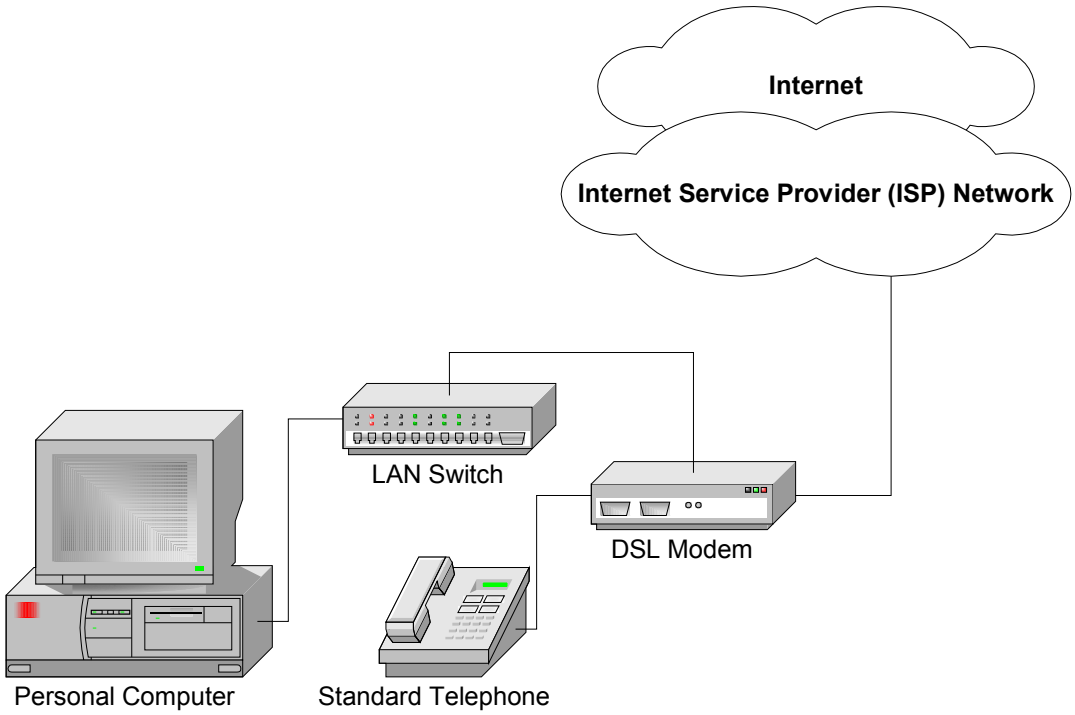


Figure 2- A Typical DSL Modem Broadband Access Setup

Various different DSL technologies (generally called xDSL) are available from Internet Service Providers. The common types include:

IP Telephone Over Internet Virtual Private Network (VPN)

- **ADSL (Asymmetric Digital Subscriber Line)**
- **HDSL (High Bit Rate Digital Subscriber Line)**
- **RADSL (Rate Adaptive Digital Subscriber Line), and**
- **SDSL (Symmetric Digital Subscriber Line, a standardised version of HDSL)**

Out of these xDSL access technologies - the most common type available is ADSL. The term Asymmetric in ADSL means that the download and upload available bandwidth are different. In practice the bandwidth for download is much higher than the bandwidth available for uploads with typically a 1Mbps service providing speeds of 1.024Mbps for download and 256Kbps for uploads.

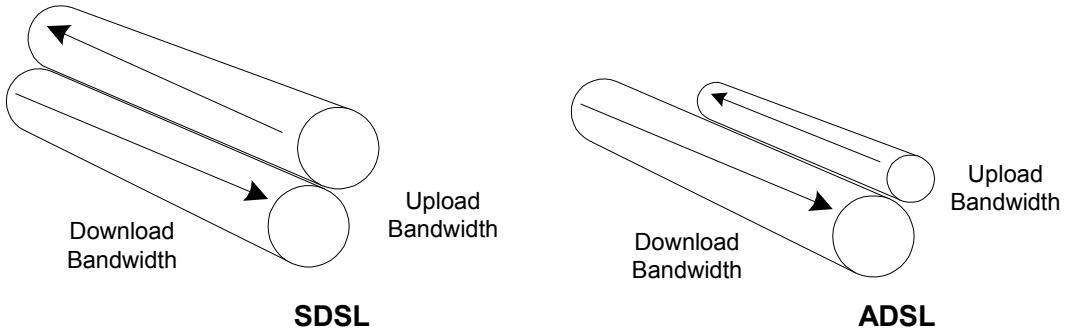


Figure 3 - Bandwidth Comparison between ADSL vs SDSL

It should be noted that all ISPs share fixed bandwidth between users. For home users the typical contention ratio is around 50:1 while for office users it is approximately 20:1. This means that under worst case scenario – an ADSL home user is sharing their 1 M service with 49 other home users of same service for a worst case download speed of 1.024Mbps/50 = 20.48 Kbps. In reality the average download speeds are more closer to around the middle of the service offering.

NOTE: Customers planning to use IP Telephony over standard ADSL service for homes should realize that **voice quality can potentially be severely affected** because of higher bandwidth sharing due to 50:1 contention ratio. Hence it is recommended to use business ADSL service that has a much better and lower contention ratio of 20:1.

Since data network like Internet were designed to carry data – which is not time sensitive - having different upload and download bandwidth is typically not a problem when dealing with emails, websurfing, downloading music etc. As ADSL has more downstream bandwidth than upstream, if you take the same size data file — you could download it more quickly than you could upload it. The same affect happens for voice packets when going over ADSL. Since voice is time sensitive in both directions – it is important to understand that having different bandwidth for uploading and downloading can easily cause voice degradation.

A much better and recommended service specially for business users and IP Telephony is SDSL. The term Symmetric in SDSL means that the bandwidth available for both downloading and uploading is the same (see Figure above). This means that a typical 1Mbps SDSL service provides 1.024 Mbps each for downloads and uploads. This means that Voice (VoIP) packets travel much more effeciently over SDSL and there is much less change of any voice degradation.

ADSL Broadband Setup

In Europe the most common form of Broadband Internet access provided by ISPs is ADSL. Since ADSL is provided over standard telephone connection – this service is physically provided over normal telephone connection provided by your local telephone company.

In some countries a representative of your local ISP may visit your home or office to setup the ADSL service. However as ADSL becomes more common - most ISPs now assume that an end-user is able to setup the ADSL service on their own. The steps below indicate a typical ADSL setup and have been provided here for information purposes only. Please note that in your particular case – the steps may be slightly different based on the type of ADSL modem as well as the service provided by your local ISP:

Connecting ADSL Modem to a PC to configure it:

1. Connect a standard telephone cable to the wall-jack with ADSL Service.
2. Find a telephone jack on the ADSL modem labeled commonly as "Line", or "Internet" and connect the other end of the telephone cable to the ADSL Modem. Typically ADSL modems are provided by your ISP – however in some cases you may have to buy your own.
3. To avoid interference, you may need to place a microfilter or splitter between the phone cable and wall jack – before the ADSL modem.
4. Connect one end of a straight through RJ45 Ethernet Cable on the ADSL Modem. If your ISP has not provided you with an ADSL modem that has an RJ45 port – you will need to get an ADSL modem that has atleast 1 RJ45 port. It is common to have an ADSL modem with a built-in LAN Switch.
5. Connect the other end of the RJ45 Cable to your PC – making sure that the IP settings on your PC is set to DHCP. This will ensure that after connecting to the ADSL modem when you turn on your PC – it will automatically get the proper IP address from the ADSL Modem. (Note: Almost all ADSL Modems have a built-in DHCP Server that can assign local IP addresses)
6. Turn on the ADSL Modem – wait for a few seconds and then power on the PC connected to the ADSL Modem. If your PC requires a login, please enter the proper login details – e.g. Your PC's User ID and password.

Configuring the ADSL Modem to access Internet via your local ISP:

1. Collect the information provided by your ISP for setting up your ADSL modem as well as your Broadband Internet. These are needed to configure and setup your ADSL modem.
2. Open the browser on the PC connected to the ADSL modem and type in the URL address field of your browser the local IP address of the ADSL modem. Typically this would be an IP address in the format 192.168.x.y. and provided by either you ISP or ADSL modem manufacturer. For this example – we will assume that this address is **192.168.1.1.** Please write down this IP address as it will be required when configuring the IP-EXT16 card and the IP phones.
3. A window may popup asking you to enter a User ID and Password to access the configuration section of the ADSL modem. This should have been provided either by your ISP, or by the manufacturer of the ADSL modem. Once the User ID and Password is properly entered – a web based configuration page would open.
4. Enter all the information provided by your ISP to configure the ADSL modem and click to save settings. These settings would typically include the following type of information (see figure below):
    - **Encapsulation Type**
    - **Virtual Circuit (VPI - Virtual Path Identifier, and VCI - Virtual Channel Identifier)**
    - **Username and Password for ADSL account (if required by ISP).**

- **Select "Keep Alive" if you are not charged to stay connected to Broadband Internet.**
- **Hostname (if required by ISP)**
- **Domain name (if required by ISP)**

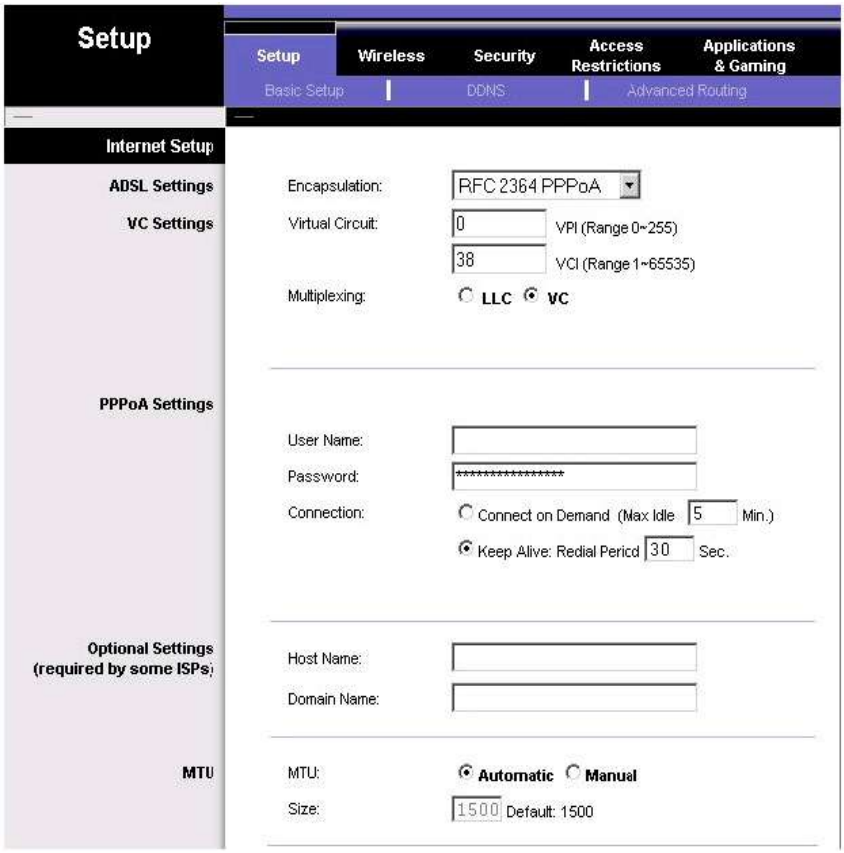


Figure 4- A Linksys WAG54G ADSL Modem setup screen

Check to make sure that your PC has the proper DNS settings provided by your ISP and your Browser is properly configured to access the Internet. Then open your browser and type a favorite website – e.g. http://www.panasonic.co.uk to make sure that your Internet connection is working ok.

NOTE: When planning to connect ADSL in the office where the TDA Hybrid IP PBX is located, please make sure that you order a Fixed IP address from your ISP. Fixed IP address is also sometimes called Static IP address, or Fixed Public IP address and your ISP may bill you an additional monthy charge for this service.

It is a good idea to write down the public IP address of your ADSL Modem. This information will be needed when you setup an Internet IP VPN over your Broadband connection. To find this – check the information provided by your ISP, or you can also find this by accessing any of the public websites that can provide this information. Two such websites that you may find useful are:

1. http://www.mywanip.com/
2. http://www.whatismyip.com/

For this example setup – we assume that the Office site with the TDA Hybrid IP PBX populated with the IP-EXT16 card has a fixed IP address **81.158.176.57** while the remote

site with the Panasonic IP telephone connected over ADSL has a dynamic (i.e. can change over time) IP address.

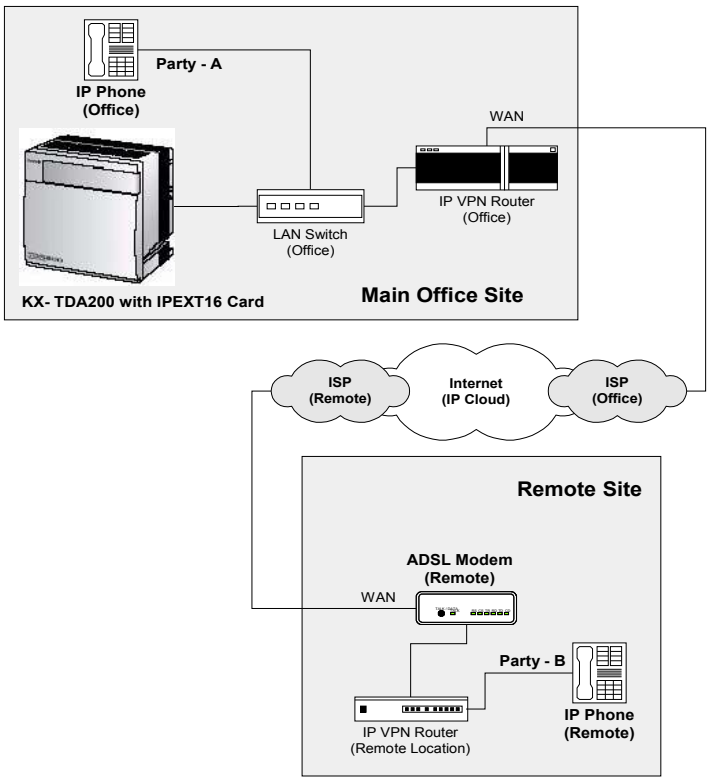
IP Telephony over Broadband

For simplicity – this document shows how to setup a single Panasonic IP phone at a remote site over ADSL to connect back to a TDA PBX in main office. For this example – we assume that both Main Office site as well as the Remote Site are connected to the Internet over Broadband Internet using ADSL. For this setup to work - the following minimum equipment is required:

Equipment Needed at Main Office Site:
- KX-TDA100 (or KX-TDA200) Hybrid IP PBX
- KX-TDA0470 IP-EXT16 Card
- KX-NT136 IP Phone - (1)
- ADSL Modem with RJ45 LAN port and built-in IP VPN Router (e.g.: Linksys WAG54G)
- Broadband Internet Connection with 1 Fixed Publically Addressable IP Address
- Necessary RJ45 Straight through LAN Cables

Equipment Needed at Remote Site:
- KX-NT136 IP Phone - (1)
- ADSL Modem with RJ45 LAN port and built-in IP VPN Router (e.g.: Linksys WAG54G)
- Broadband Internet Connection (Dynamically Assigned IP address is acceptable)
- Necessary RJ45 Straight through LAN Cables

It is assumed that the installer is already familiar with:
1. Installing and setting up Panasonic KX-TDA200 Hybrid IP PBX
2. Installing and configuring an IP-EXT16 card
3. Installing, registering and setting up an NT-136 IP phone



IP Telephone Over Internet Virtual Private Network (VPN)

A typical simplified network for setting up remote IP Telephony over ADSL modem is shown above.

For this example we have used the Linksys WAG54G ADSL modem. This modem has built-in LAN Switch, Firewall/NAT, DHCP Server, as well as IP VPN Router with ability to support upto 5 serapate IP VPN tunnels.

Setup TDA PBX and IP Phones in Main Office Site:

1. Remember that the Local and Public IP addresses for the ADSL modem (mentioned above) are

Local IP Address = 192.168.1.1
Public IP Address = 81.158.176.57

Main Office Site ADSL Modem IP Settings

2. Install the TDA200 in the main office
3. Install and configure an IP-EXT16 card. Use the following settings for configuring the IP-EXT16 card. Note that the Gateway Address for the IP-EXT16 Card is the same as the Local IP Address for the IP VPN Router – which is part of the ADSL Modem

IP Address = 192.168.1.10
Subnet Mark = 255.255.255.0
Gateway Address = 192.168.1.1

IP-EXT16 Card IP Settings

4. Using Ethernet RJ-45 LAN Cables, connect the IP-EXT16 card and the two NT-136 IP Phones using the LAN Switch part of the ADSL Modem.
5. Assign the following IP address, Subnet Mask, Default Gateway IP address, and PBX IP Address to the two NT-136 IP phone. Note that the Default Gateway Address for the IP Phones is the same as the Local IP Address for the IP VPN Router – which is part of the ADSL Modem, while the PBX IP Address is the same as the IP Address for the IP-EXT16 Card.

Phone Setting for Party A:
IP Address = 192.168.1.12
Subnet Mark = 255.255.255.0
Default Gateway = 192.168.1.1
PBX IP Address = 192.168.1.10

Phone Setting for Party B:
IP Address = 192.168.1.13
Subnet Mark = 255.255.255.0
Default Gateway = 192.168.1.1
PBX IP Address = 192.168.1.10

IP Settings for NT-136 IP Phones

6. Connect the PC on the same network making sure it is assigned an IP address in the same range yet different from all the other devices (e.g. 192.168.1.20). Use the PC to confirm that all the devices are accessable over the IP network by pinging each IP address.
7. Register the two phones with the IP-EXT16 Card using TDA PC Maintenance Console software. When the IP phones are registered, the PBX automatically assigns phone numbers. For this example we assume the two phone numbers as follows:

IP Telephone Over Internet Virtual Private Network (VPN)

Party A Telephone Number: 217

Party B Telephone Number: 218

Assigned Telephone Numbers

8. Make a call between the two IP phones to make sure that you have clear audio communication between the two phones in both direction.

Setup IP VPN Tunnel at Main Office Site:

1. Connect a PC to the IP VPN Router/ADSL Modem – by typing **192.168.1.1** into your browser's URL address field. Once connected and logged in – click on the Security tab and then click on VPN to setup an IPSec based IP VPN tunnel. See Figure 6 below.
2. Make sure to set **IPSec Pass-Through** to **enabled**
3. To Create an IP Sec based VPN Tunnel, set **IPSec VPN Tunnel** to **enabled** and assign a name/label to the VPN tunnel. You can use any name that you like (i.e. **myipvpntunnel**) . Note that the name you assign for the VPN Tunnel at the Main Office does not have to be identical to the name that you assign for the VPN Tunnel at the Remote Site.
4. Set **IP Range** for **Local Secure Group** to 192.168.1.1 ~ 100. This would allow all IP devices in this range to be able to communicate over the VPN Tunnel.
5. Set **IP Range** for **Remote Secure Group** to 192.168.2.1 ~ 10. This would allow all IP devices in the local IP Range to communicate with all IP devices at the remote site within the Remote Secure Group IP Range.
6. For **Remote Security Gateway** – set the Main Office IP VPN Router to **Any**. This is because in this example setup – the IP VPN/ADSL modem at the Remote Site has a dynamically assigned IP address. If in your case the remote site also has a fixed IP address – please enter that value here instead of setting the Remote Security Gateway to **Any**.
7. Set your preferred **Encryption** and **Authentication** type.
8. Under the section for **Key Management**, select **Auto. IKE** (Internet Key Enchange Protocol) and set **PFS** (Perfect Forward Secrecy) to **enabled** and enter an alphaneumeric value for the **Pre-shared Key**. This could be any value – however the longer it is the more secure the VPN tunnel will be. Further, it should be noted that Pre-shared Key value MUST be the same at the Main Office and the Remote Site. If multiple IP VPN is created – one for each different remote site – then the Pre-shared Key for each Tunnel could be different, however for each pair of VPN Tunnel between the Main Office and Remote Site – it must be the same.
9. Click **Advanced** and under **Other Settings** check **Keep-Alive**. This will keep your VPN Tunnel up – and even if for some reason it is disconnected – the IP VPN Router will reconnect the VPN Tunnel automatically.
10. Save all your settings. At this point the status of your IP VPN Tunnel will show **Disconnected**. Once the IP VPN is properly setup at the remote site – the status will change to **Connected**.

IP Telephone Over Internet Virtual Private Network (VPN)

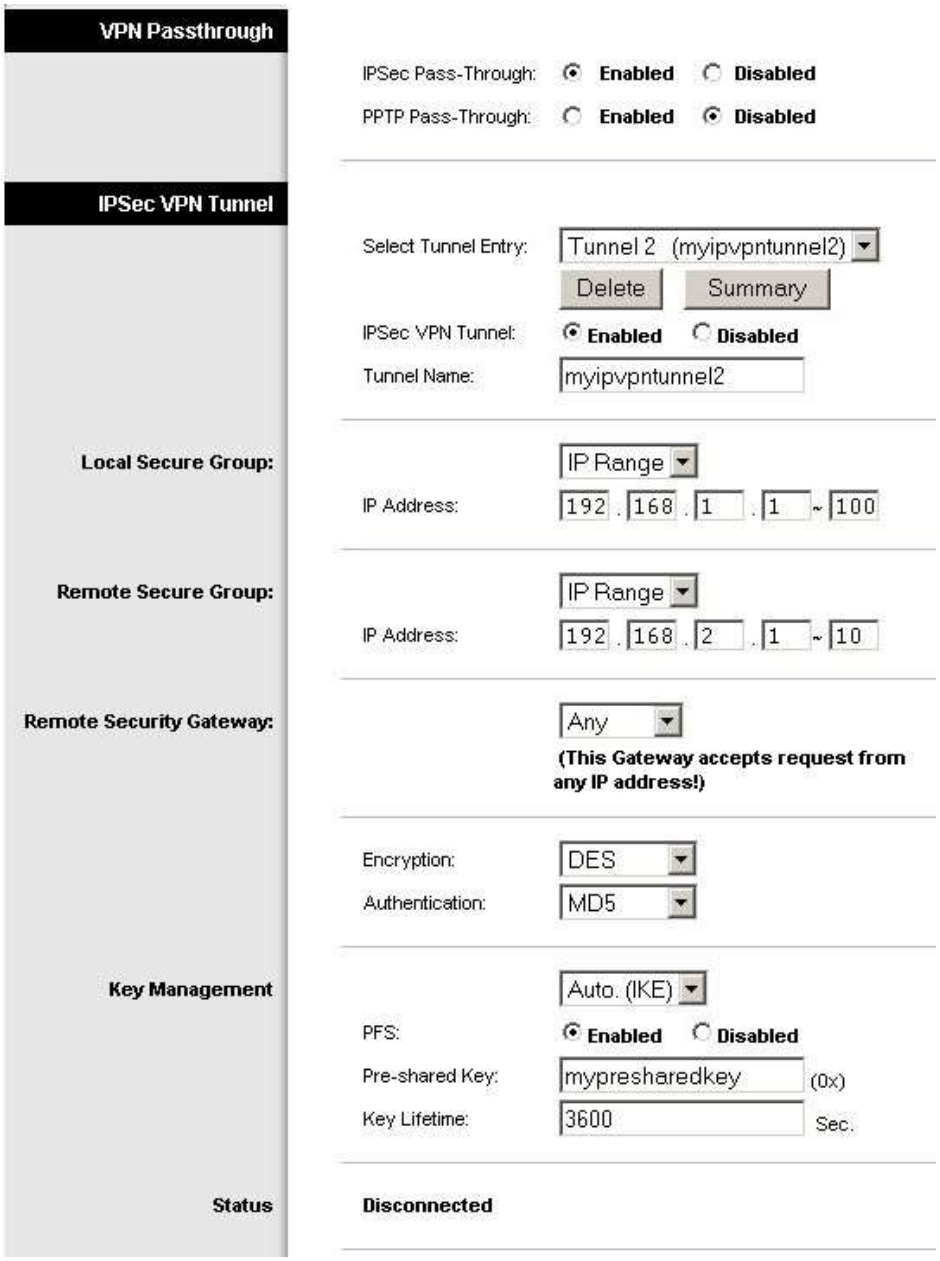


Figure 6- IPSec IP VPN Setting for Main Office Site

IP Telephone Over Internet Virtual Private Network (VPN)

Setup IP VPN Tunnel at Remote Site:

Visit the Remote Site – taking the IP Phone (Ext 218) already registered with the IP-EXT16 card in the Main Office. It is assumed that the installer has already installed and configured the ADSL modem at the Remote Site (see section titled **ADSL Broadband Setup** above). For this example – it is assumed that the ADSL modem at Remote Site has the following IP settings

Local IP Address = 192.168.2.1
Public IP Address = Dynamically Assigned

Remote Site ADSL Modem IP Settings

In order to Setup an IPSec based IP VPN tunnel at the remote site – follow the same process as described above for setting up IP VPN for the Main Office and use the settings as mentioned in the Figure below.

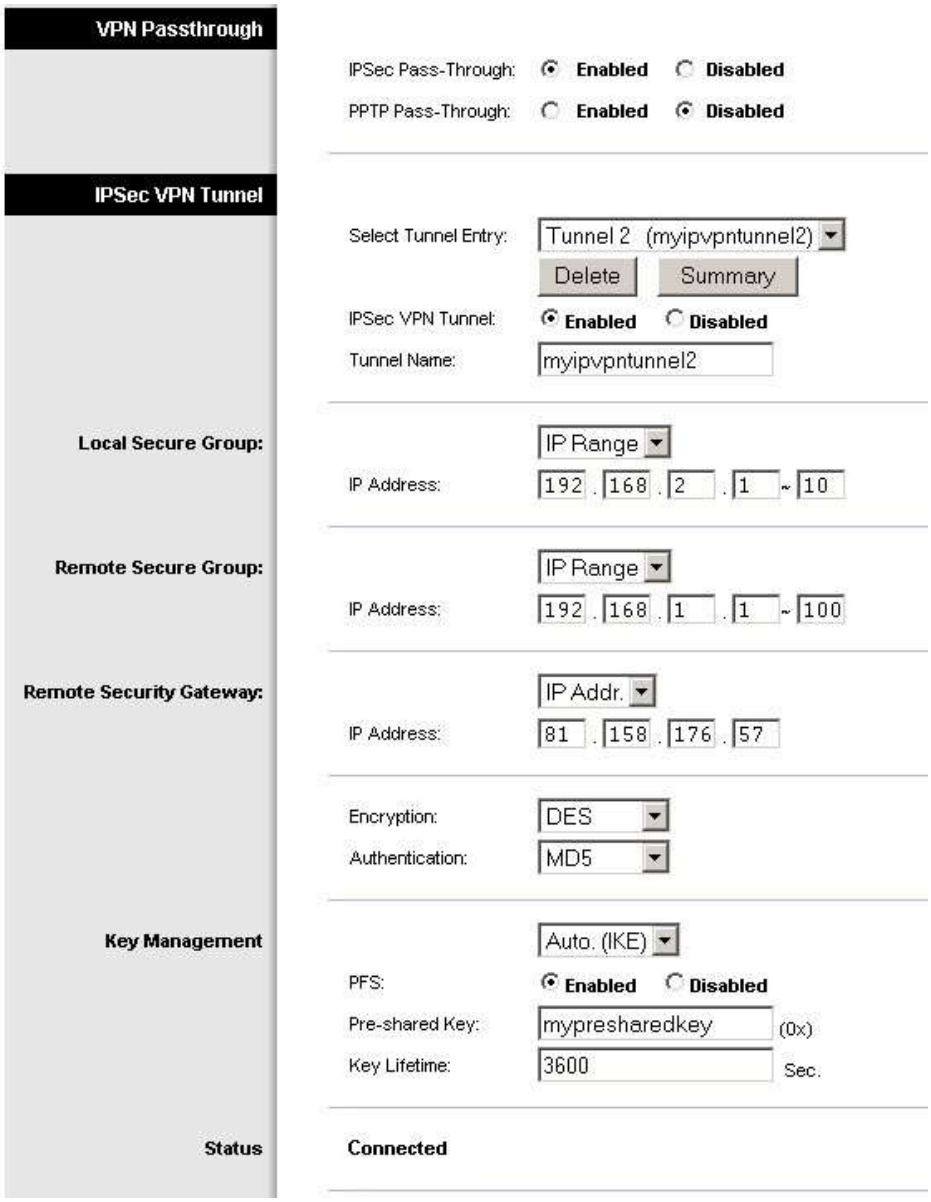


Figure 7- IPSec IP VPN Setting for Remote Site

IP Telephone Over Internet Virtual Private Network (VPN)

When setting IP VPN Tunnel at the Remote Site, make sure to:

1. Set **IP Range** for **Local Secure Group** and **Remote Secure Group** such that it is opposite to the settings for the IP VPN Router in the Main Office. This would allow all IP devices in the range to be able to communicate over the VPN Tunnel.
2. For **Remote Security Gateway** – enter the Fixed Public IP Address of the ADSL Modem at the Main Office. Remember that this was **81.158.176.57**. This will allow the Remote VPN Router to find the VPN Router located at Main Office Site and establish an IPSec based VPN Tunnel.
3. Click **Advanced** and under **Other Settings** check **Keep-Alive**. This will keep your VPN Tunnel up – even if for some reason it gets disconnected.
4. Save all your settings and click **Connect**. After a few seconds the Status of the VPN Tunnel should change to **Connected**.
5. You can click on the button labeled **Summary** under the **Select Tunnel Entry** field to see the detailed status of the VPN Tunnel.

Setting IP Phone at Remote Site:

1. Using Ethernet RJ-45 LAN Cables, connect the NT-136 IP Phone to the LAN Switch part of the ADSL Modem.
2. Change the IP settings of the IP Phone (Ext 218) by assiging the following IP address, Subnet Mask, Default Gateway IP address, and PBX IP Address to the NT-136 IP phone. Note that the Default Gateway Address for the IP Phone is the same as the Local IP Address for the IP VPN Router – which is part of the ADSL Modem, while the PBX IP Address is the same as the internal IP Address for the IP-EXT16 Card.

Phone Setting for Party B:
IP Address = 192.168.2.12
Subnet Mark = 255.255.255.0
Default Gateway = 192.168.2.1
PBX IP Address = 192.168.1.10

IP Settings for NT-136 IP Phones

3. Please note that once an IP Phone is already registered with the IP-EXT16 card on the TDA Hybrid IP PBX, it does not need to be re-registered even when the IP address of the IP Phone is changed. This is because as part of the registration process – the IP Phone sents its own MAC addess to the IP-EXT16 card which then stores the phone's MAC address in the PBX database. Since the MAC address is independent of the IP Address, when the same IP phone is assigned a different IP address – the PBX can recognize the MAC address of the IP Phone and thereby does not need for it to be re-registered.
4. The IP Phone should automatically register and come online.
5. Go Off-hook to make sure that you can hear the dial-tone. Hearing the dial tone is an indication that the IP Phone has been properly installed and configured at the remote site.

At this point you should be able to go Off-hook and make a call between Party B and Party A making sure that there is audio communication between the two IP phones.

You have now successfully completed installing an NT-136 IP Phone at a Remote Site over Broadband ADSL connection.

For the complete network setup diagram for the entire network – please see Figure 8 on the following page.

IP Telephone Over Internet Virtual Private Network (VPN)

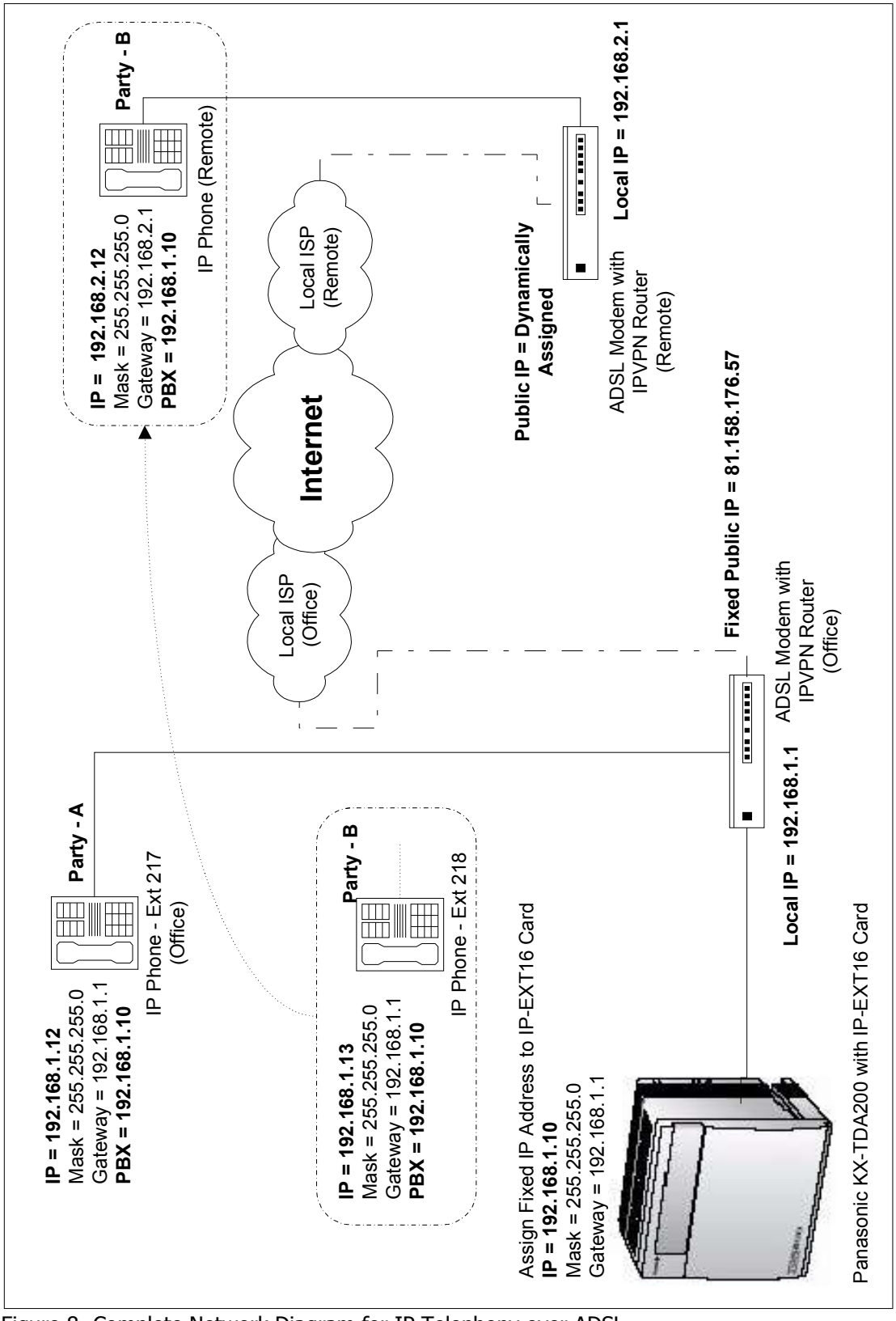


Figure 8- Complete Network Diagram for IP Telephony over ADSL