

TCP/IP CONFIGURATION For Your Proxy Router

© Copyright 1998 RINGDALE Limited. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or any computer language, in any form or by any third party, without the prior written permission of RINGDALE UK Ltd.

RINGDALE UK Ltd reserves the right to revise this publication and to make changes from time to time to the contents hereof without obligation to notify any person or organization of such revision or changes. RINGDALE UK Ltd has endeavoured to ensure that the information in this publication is correct, but will not accept liability for any error or omission.

1. How to Configure the Ringdale Proxy Router

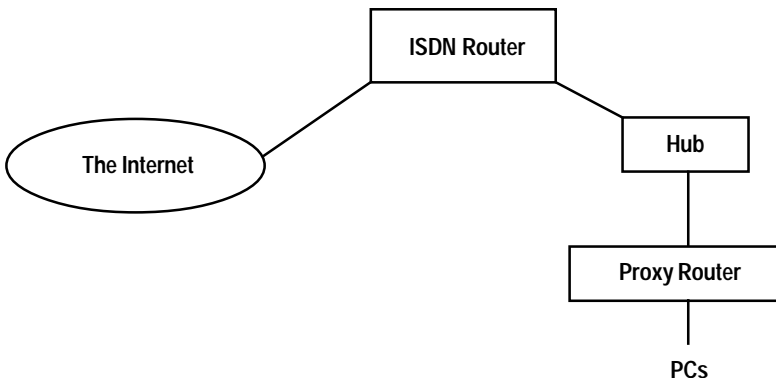
2. The Basics of TCP/IP Protocol

1. How to Configure TCP/IP for the Ringdale Proxy Router

Your network administrator should be able to supply you with the required configuration details for the Proxy Router, but if you encounter difficulties use this supplement as a reference point.

If you are unfamiliar with Internet Protocol (IP) addresses and their structure, read section two of this supplement first.

The configuration procedure for the Proxy Router will be virtually identical to setting up a PC on an Intranet or the Internet. It is important to understand that the Proxy Router itself does not supply the link to The Internet, this will be done by use of an ISDN router or similar internet routing device. Shown below is the most likely setup for your network, incorporating the Proxy Router.



Should it be required, it is possible to connect the Proxy Router directly to the ISDN router without the use of a hub. To do this it will be necessary to use a crossover RJ45 cable.

The following information will need to be configured to enable the Proxy Router to function. For details on how to enter this configuration (using the PeripheralVision® software supplied with the Proxy Router) refer to the User Manual.

Note: The **Local IP Address** and the **Local Subnet Mask** will be automatically assigned at start up and will not normally need changing.

Remote IP Address:

This is the IP address that is used to identify the Proxy Router across the network. As the router is not directly linked to the internet it does not require an IP address assigned by an Internet Service Provider (ISP), but will have an IP address consistent with other devices on the network. e.g. If other devices on the network have an IP address of:

123.456.789. *

Then the Proxy Router IP address will be:

123.456.789. + the last three digits that will be unique to the Proxy Router (for further details of IP address structure see section 2 - The Basics of TCP/IP Protocol).

TCP/IP Subnet Mask:

This will be the same as that used for the other devices on the network.

Default Gateway IP Address: This will be the IP address of the ISDN router or whatever other routing device is providing your link to the Internet.

DNS Name Server Address: This could be the IP address of the network's own DNS if it has one, but most likely this will be the IP address of the Internet Service Provider's DNS, details of which will be supplied to you by your ISP (further information on Domain Name Servers can be found in section 2).

2. The Basics of TCP/IP Protocol _____

TCP (Transmission Control Protocol) and IP (Internet Protocol) are terms that have generally become interchangeable and provide a means for individual computers and computer networks to communicate with each other. The success of TCP/IP is due to three main factors:

- 1) The range of computers it is available on makes it an attractive option for new products as manufacturers can guarantee that their products will work with lots of systems.
- 2) TCP/IP encompasses a range of extremely powerful and flexible protocols that make it suitable for just about any task you can think of.
- 3) IP is the protocol set used by the Internet.

TCP/IP describes two protocols. TCP offers a guaranteed delivery service on top of IP, the core datagram service.

Developments in TCP/IP are fast and more functionality is constantly being added. This is what makes it so powerful, but it has the side effect that what many people term as IP actually comprises a whole range of protocols and functionality. Moreover, because it is required to work in such a wide range of environments, some configuration is needed to get it running on a given network, i.e. a server name and a couple of network numbers are required. For bigger networks the only real network configuration required is to ensure that each network segment has a unique number. With IP, however, there are several server processes that may be required to, for example, tell new workstations about the network configuration, or provide translation services between host names and their IP addresses.

The IP Address and the Subnet Mask

The core of TCP/IP is the host address, also known as the *IP address* of a machine. Every machine on your network that is running IP needs a unique host address and there is no distinction between workstations, printers, routers or servers - they are all IP hosts. If you are used to local networks then you will know that each workstation and server also has a unique address, but this is set automatically. With IP you have to do it yourself. There is a similar and equally important idea in IP called the *subnet address*, but this is less obviously identified - rather than typing in a network number the address of the subnet to which a machine is attached is embedded in its IP address. All IP addresses are currently 32 bits, i.e. four bytes long. IP addresses are usually written in decimal format, e.g.

192.130.159.163

Associated with a particular IP address is the *subnet mask*. This is used to tell you how many of the leading bits in a given IP address denote the subnet address, e.g. the typical subnet mask of

255.255.255.0

means that the first three bytes of an IP address denote the subnet address, and the last byte identifies a particular host on that subnet. So with an IP address of:

192.130.159.163

and a subnet mask of:

255.255.255.0

the subnet address is:

192.130.159

and the host identifier is:

163

Such a subnet address is known as a *Class C* network and it means that you can have up to 255 different host addresses on that subnet (although using 0 and 255 is a bad idea as they can conflict with other network services. In practice it is best to stick to a range of 1 to 254, giving 253 total addresses). *Class B* networks use a subnet mask of:

255.255.0.0

giving two bytes' worth of addresses (65,536) that can be used. There are also *Class A* networks with a subnet mask of:

255.0.0.0

giving three bytes' worth of addresses.

If your TCP/IP network is never going to be connected to anything else, you can use whatever subnet mask and IP addressing structure that you want. Do not use IP addresses with 0 or 255 in them as these are used by network services, as is 127.x.x.x. But typically you will want to attach your network to the Internet via an ISP (Internet Service Provider).

To do this you generally arrange with the ISP to get them to supply you with a unique *Class C* address - they will give you a three byte address which you can use with a subnet mask of:

255.255.255.0

and then you can use the remaining byte of the address to identify the hosts on your network. If you have more than 255 hosts then you could ask for a *Class B* address, but these are fast running out so you would have to put a good case to get one. Instead you would

probably have to settle for two or more Class C addresses. Class A addresses are reserved for organisations such as the US Department of Defense.

Domain Name Servers

If you have used the World Wide Web (WWW), you will know that most sites have a name. But although all you need to know is the name of a host, the IP stack itself needs to know the host's address. The translation between the host name and its IP address (and vice versa) is provided by a DNS (Domain Name Server). The DNS is a software process running on a machine somewhere on the network that provides a look-up service for IP protocol stacks.

There are utilities that allow you to query a DNS directly, but generally it is all behind the scenes. If your network is completely stand-alone then you will need to have your own DNS somewhere on your network. If instead you have an Internet connection, then your ISP will have at least one DNS on your side of the Internet connection to add resiliency and reduce the amount of traffic over the Internet connection. A single DNS, even one for an ISP, will not have the names and relevant IP addresses for every host on the Internet - they number in the millions. Therefore, you configure your hosts with a list of several DNS services in them - your ISP can provide you with a list. If the host cannot find the address it is looking for in the first listed DNS (typically your local one) it goes to the next one in the list and so on until it either finds the address or gives up and tells you that it cannot be found.

Notes

Notes
