Document Title:	Frame Relay Risk Analysis
Document Type:	Customer Briefing
Abstract:	To discuss any risks to the Pathway solution from the introduction of frame relay as the preferred non-ISDN solution.
Status:	Approved
Distribution:	Library Anne Cooper Dave Tanner Alan D'Alvarez Horizon Library Jeremy Folkes Bob Booth Richard Smith
Author:	Barry Procter

0 Document control

0.1 Document history

Version	Date	Reason
0.1	20/04/98	Initial draft for limited internal impact
0.2	20/04/98	Updated to incorporate comments from AD'A
0.3	20/04/98	Modified to better describe the scope as solely frame relay, not the whole non-ISDN solution.
1.1	29/04/98	Modified to include questions & answers from the presentation to Horizon Technical Assurance team (at Appendix A).
1.0	21/04/98	Modified to highlight security enforcing functionality.
2.0	29/05/98	Modifications to the Conclusion to reflect the Q&A in Appendix A

0.2 Approval authorities

Name	Position	Signature	Date
Martyn Bennett	Director - Quality & Risk		
Anne Cooper	APS Project Manager		

0.3 Associated documents

No.	Reference	Vers	Date	Title	Source
[1]	TSC/TAP/01	1.0	09/07/96	Pathway Security Report	TSC

0.4 Abbreviations

ISDN	Integrated Services Digital Network

0.5 Changes in this version

The Conclusion section modified to reflect the content of Appendix A.

0.6 Table of content

1 Introduction

The Pathway solution for larger outlets in the absence of ISDN to all outlets is IP over frame relay. It is projected that during the restricted New Release 2 rollout, only a limited number of post offices will be served by frame relay. For this limited population a separate, dedicated frame relay network will be created with associated circuits and routers configured and administered by CFM (NI) as a managed service. **The introduction of frame relay will not affect the cryptographic protection of messages**.

Figure 1 illustrates the proposed design.

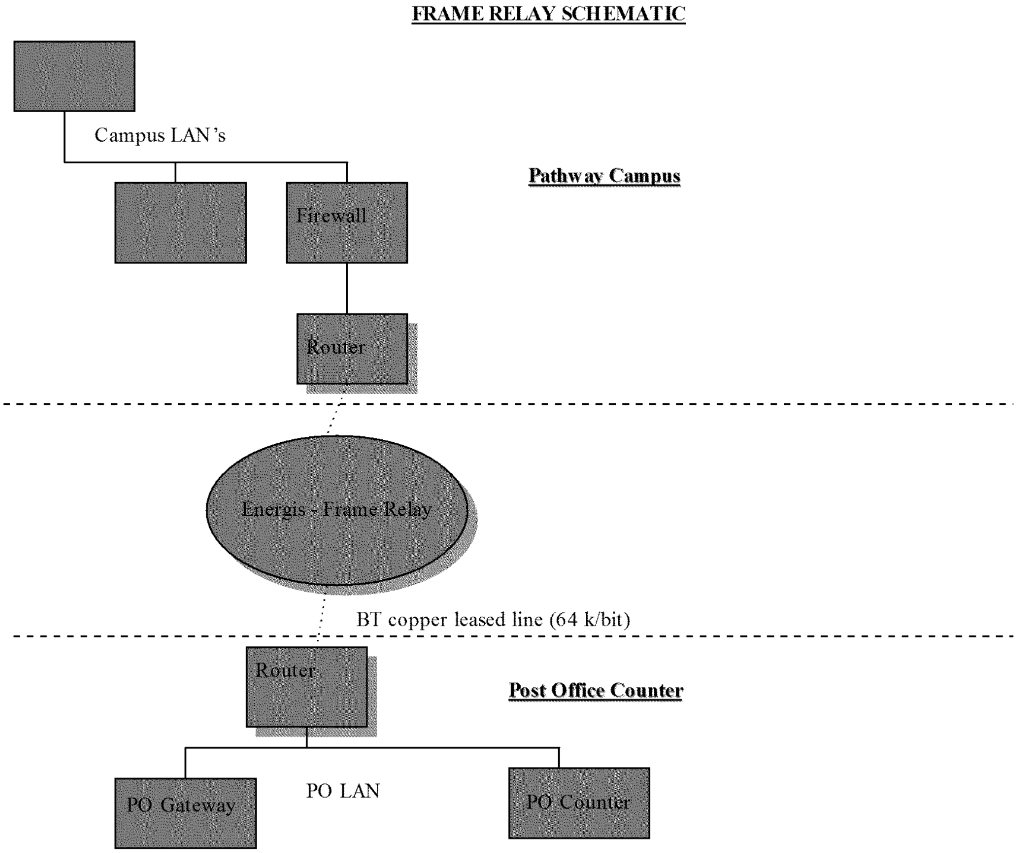

Figure 1.

In order to evaluate any threats unique to the Pathway frame relay solution, it is necessary to understand the protection that is present in the Pathway ISDN implementation, and that which is afforded by the Frame Relay solution.

2 Scope

This document is restricted to any risks associated with the Pathway frame relay solution.

3 Existing Protection of Post Office ISDN links

There is no link related protection of operational data, but CHAP initial connection authentication is provided, with refresh, supplemented by CLI authentication of the Post Offices from the ICL Pathway campus. CHAP re-authentication is applied to all calls (however initiated).

Specific security controls include:

- CHAP Authentication - where a Challenge Handshake Authentication Protocol (CHAP) challenge is issued on inbound and outgoing calls when the connection is established.

- Call screening - where a list of valid callers is configured in the central Router and all other calls are rejected. The list of valid caller information is subject to access controls and maintained using Tivoli.

An ISDN adapter is installed in the gateway workstation at every Post Office location which uses ISDN. The interface between Windows NT and the adapter is provided by a Network Device Interface Specification (NDIS) adapter which is supplied by EICON.

The NDIS adapter provides the following security enforcing functionality:

- It will only accept incoming calls from phone numbers for which entries exist in an incoming allowed list.
- It will only call phone numbers which exist in the NDIS configuration data.
- It only passes network traffic at the IP level.
- It acts as a CHAP authenticator on every call.
- It reissues the CHAP challenge every n seconds where n is a configurable parameter stored in the NDIS configuration data.
- It stores the CHAP secret in the NDIS configuration data using a symmetric encryption algorithm.
- It protects the NDIS configuration information.

All NDIS configuration data is stored in the Windows NT Registry. The files used are protected by the Windows NT access controls and filestore encryption.

4 Proposed Protection of Post Office Frame Relay links

A dedicated network comprising:

- A Closed User Group (CUG) definition.
- Dedicated frame relay routers at each end of the circuit to filter traffic on IP address.
- Firewalls to further thwart unauthorised access to the Pathway Data Centres.

The Frame Relay proposal provides the following security enforcing functionality:

- A Closed User Group (CUG).
- Firewall protection on user name, password, application and port number.
- Firewall protection will reject and report ‘foreigns’.
- It only passes network traffic at the IP level.
- Proactive monitoring by Energis.
- Security of routers provided by TACACS (username and password).

5 Conclusion

The major change introduced with the Frame Relay solution is that authentication between the routers only occurs at initialisation, whereas with the ISDN solution, CHAP authentication is invoked at each connection and periodically thereafter during the connection. The Permanent Virtual Circuit (PVC) once established between a Post Office Outlet router and a Data Centre router will not ‘drop’ unless an error condition occurs and as such no further authentication will take place. To overcome this, security is provided by the firewall environment at the Data Centre which prevents unauthorised access to the campus. There is no equivalent protection at Post Office Outlet so the risk is that an attacker spoofs a post office into thinking it is talking to a genuine Pathway correspondence server. The initial risk analysis [1], identified three cases for consideration:

1. The centre acknowledging receipt of encashment data from a post office.

   “If the protocol consisted of the post office simply sending encashment data to the centre, with only simple acknowledgement of receipt then it would perhaps not be too difficult to spoof this……but what would the subsequent fraud be? It would be difficult to make a foreign encashment work despite this confusion.”

1. The centre sending payment authorisations.

   “Payment authorisations are signed and cannot be spoofed, so provided reply protection of payment authorisations is provided this fraud would not work.”

1. Spoofing the response to foreign encashment requests

   “This could be done provided the protocol is understood by the attacker, but unless a small post office is chosen so there is no other traffic to the centre, the complexity of the task would be daunting."

The proposed frame relay solution provides adequate protection of the link with the utilisation of CUG and dedicated frame relay routers . The absence of CHAP and CLI has been mitigated by the inclusion of additional firewalls which are actively monitored by CFM (NI).

It should be noted, however, that within [1] both CHAP and CLI are described as providing minimal protection which does not defend against proficient attacks on the circuits between the Data Centres and the outlets ; "We see CHAP and CLI making a very hard life slightly harder for the hi-tech masquerader but not making it impossible". It further states "Our general conclusion is that, except for the use of CLI at roll-out, the CHAP and CLI measures proposed provide a useful backstop to other defences but are not essential".

This has been acknowledged within Pathway who are investigating more secure alternatives for all outlets for implementation at a future release.

6 Appendix A

The following section addresses the questions raised by the Horizon Technical Assurance Team.

1) What protection exists against attack to the "local loop" at the post office end, i.e. the private circuit from office to the Energis switch (via the BT infrastructure)? What mechanisms prevent an attacker, armed with the right Cisco router, from spoofing the office or from spoofing the host by attaching to the line?

The Cisco routers proposed for the outlets incorporate a username and password authentication mechanism to prevent spoofing of the host. Calls to the Data Centres will be authenticated by TACACS to prevent spoofing of the outlet.

2) What protection exists against an attack by a legitimate Energis Frame Relay customer (or Energis employee who has authorised access to the FR network)? Can someone with such access gain access (at IP level) to the link?

a) Attacks from within the Frame Relay Network are prevented by the provision of Closed User Groups (CUG).

a) As above - CUG's plus the username and password protection inherent in the routers

3) What protection exists against unauthorised access to the Data Centres through attachment to the office LAN, noting that in the proposed FR solution the router is physically attached to the LAN, whereas in the ISDN solution the router is installed within the gateway PC? [That is, in the FR the cable to the router is easily identified and accessed; in the ISDN solution there is no such external cable].

PCs on the local LAN, (Gateway PC or counter) are connected to the mini hub which is enclosed within the comms cabinet, The router is located inside the comms cabinet. If a non-Pathway PC is connected on the LAN, scenarios to consider :

Riposte *- Neighbour replication at the Post Office Outlet, and Riposte replication to or from a Correspondence server is via the Gateway PC only, therefore not a* *security issue as non-Pathway PC will not be able to communicate with Riposte locally or remote.*

Others *- Firewalls validate the IP address and application port number (specific port number for Tivoli and Migration server) at the Data Centres prior to allowing onward routing within the Data Centres. Therefore a non-Pathway PC will be 'blocked' by the firewall and a security alarm raised.*

4) The ISDN CHAP/CLI solution, we understand, involves two way authentication (i.e. office to host and vice versa) using CHAP and checks for both inbound and outbound calls - i.e. the CLI is checked for both a host-office and office-host call. Given the reliance in the FR solution on "firewall protection on user name, password.....", please confirm that the authentication is "both way" - in other words that the office is protected against a rogue inbound 'call'.

The Frame Relay routers at the Data Centres and the PO Outlets establish Private Virtual Circuits (PVC's) and as such there is not the concept of a call either way - the link is a permanent connection once established within the Frame Relay Closed User Group (CUG).

5) CHAP involves a periodic re-authentication of a link, in addition to the authentication when the link is set up. The username/password firewall check was described as being only at set-up (which might be very infrequent, given that the link may never be downed, except through power failure). What mitigates against this lack of periodic re-authentication?

The Frame Relay routers at the Data Centres and the PO Outlets establish Private Virtual Circuits PVC's and as such there is not the concept of a call either way - the link is a permanent connection once established within the Frame Relay Closed User Group (CUG) . Authentication between the router takes place at initialisation, however the proposed Frame Relay Firewall environment at the Data Centres will monitor and validate all packets from the source address prior to onward transmission to the destination address.

6) Generally, we would benefit from a fuller description of the username/password mechanism, to include:

a) how are the names/passwords generated and installed

a) what protocol used for the authentication (eg is this info passed in clear)

a) how are the names/passwords stored (i.e. can someone gain access to this security info by reading the memory card)

a) what quality of names/passwords

(basically the standard access control and key management questions)

a) Usernames and Passwords for routers destined for the Frame Relay PO Outlets are generated to Pathway standards. The Username & Password for this router along with Username & Password for Data Centre Frame Relay routers are input by WTL during configuration. On installation of the router at a PO Outlet the Username /Password is input to the Frame Relay routers at the Data Centres .

a) Usernames are clear, Passwords are encrypted

a) Usernames & Passwords stored in NVRAM *a) Pathway security standards for Username & Password allocation.*