ON-LINE EXPERT SUPPORT THROUGH VPN ACCESS

P. Fidry, V. Rakotomanana, C. Ausanneau

Pierre.fidry@alcatel-lucent.fr

Alcatel-Lucent, Centre de Villarceaux, 91620, Nozay, France

Abstract: As a consequence of the operation and maintenance cost reduction and quality of service improvement, and since the arrival on the market of broadband internet access using DSL (Digital Subscriber Line), a new On-line remote access service based on VPN (Virtual Private Network) has been developed.

This solution allows On-Line Expert to connect to supplier remote access platform from nearly anywhere through internet broadband access such as home, hotel or airport and then bounce to authorized customer networks.

This particular architecture could also be adapted to provide the customer with a secure remote access directly to his own system through internet access. This could reduce significantly the need to have staff on site for first level investigation or for periodic operation on the system.

1. INTRODUCTION

This paper describes the evolving customer support processes for submarine networks. New technology has enabled us to respond to requests for technical support in a much more direct way than was possible in the past. It is now possible to use VPN access to take care of customer needs.

2. TRADITIONAL SUPPORT

When submarine networks were relatively simple, two or three stations with no or low level of supervisory, the customer support was done by phone or fax .

DCN (Data Communication Network) was made of *OWE* (Order Wire Equipment) and a modem connected to Line Equipment.

2.1 System complexity

The equipments in the terminal station (*SLTE*, *PFE*, *OWE*) were connected to the local supervisory systems to enable, using an *RS232* link, analogical measurement, alarm computing, repeater interrogation and command execution. The only information exchanged between different local supervisory systems was the Supervisory Flag (Sflag) parameter for repeaters interrogation request.

2.2 Customer Support Process

After a failure, the first customer action was to replace the failed unit with a spare from the on-site store. If the problem was not solved, the customer called suppliers for technical assistance. At this stage, failure diagnosis and corrective action were done only by phone or fax. If necessary, on-site intervention was scheduled to investigate the fault .

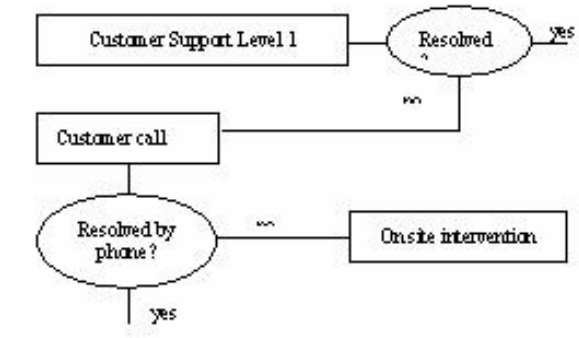

Figure 1: Traditional Process Escalation

2.2.1 Traditional Support Limitation

Due to the relatively low complexity and redundancy of equipments, the customer was able to perform the first level maintenance. Calls to suppliers were only for complex failures, but the direct on-site intervention would have sometimes been required. Cost and time resolution of such support request was high compared to the expert support developed more recently, and described in section 3.

2.4 Improvements Needed For New Systems

With new technology and the increase of the system complexity, Technical Support is a vital part of the system. It needed to be done in a better way with new tools in order to increase reactivity, and to decrease the time outage and cost associated with on-site intervention.

3. TRADITIONAL REMOTE ACCESS SUPPORT

Since the advent of computer technology and digital networks, Network Management is a very important feature, in submarine links as well as elsewhere. These systems control:

- network configuration
- traffic allocation and monitoring.

- fault handling.
- submarine fault localization
- performance and measures monitoring.

This architecture provides automatic systems which enable centralised control in a network operation centre. So the station can be unmanned with an on-call technicians.

Network control is now more complex, so that the technicians need to have knowledge about optical transmission, computer, software, routers, etc for different kind of technology.

Because problem analysis can be done remotely from a dedicated spot on a network, tools are used to make the technical support more efficient.

3.1 Tools for Remote Diagnostic - Remote Access System (RAS)

The existing RAS was designed:

- to facilitate Technical Support operations of the Network Management Elements in Terminal Stations by providing remote control and remote support to the on site customer via dedicated WAN equipment.
- to provide monitoring of the Network Elements in Terminal Stations by the use of X11 connections over IP Networks.

3.2 Network Design considerations

The main requirements which have guided the design of the Platform were:

- The Platform was able to connect to any remote site in the world at any time, if it had been initially configured for RAS
- The platform was able to permit the process of multiple windows sessions
- The design was scalable enough to accommodate additional traffic.

3.3 Hardware design

3.3.1 Remote Access Platform design

The *Remote Access Platform* consisted of several routers interconnected to the same Ethernet LAN. The WAN access was performed by *Basic ISDN* (Integrated Service Digital Network*)* lines connected to the Basic Rate Interface (*BRI*) of each router . *PSTN* (Public Switched Telephone Network) access was possible when *ISDN* Network cannot be used..

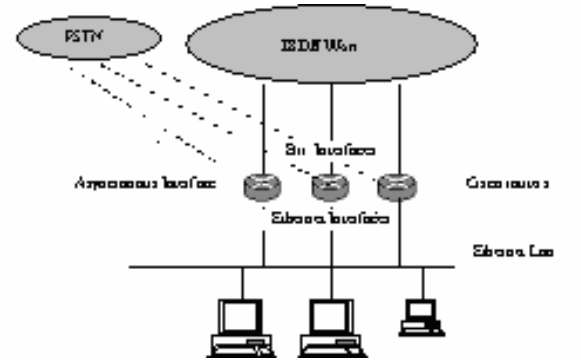

Figure 2: Hardware Design of the Remote access Platform

3.1.2 Remote Site Design

Access to the remote site was achieved by the installation of a dedicated router in the Terminal Station. This dedicated router was directly connected to the *LAN* through its Ethernet Interface. Every dedicated router was configured with a *BRI* Interface for the *ISDN* Network and with an asynchronous Interface for *PSTN* access.

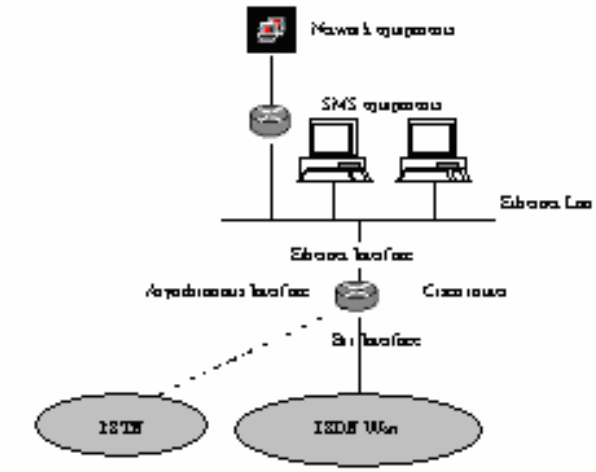

Figure 3: Hardware Design for the remote router

4. VPN REMOTE ACCESS

Compared to the current solution, based on ISDN, which has proven to be a powerful tool to meet customers needs in term of Technical Support, the new solution, based on *VPN* (Virtual Private Network) remote access, compensates for the *ISDN* drawbacks :

- fixed access points (which is a lack of flexibility in having heavy frozen infrastructure and operational procedure).
- single entry point access (when *ISDN* line is up, no other external connections are possible).
- expensive connections costs.

- obsolete or non-existent technology in some countries.
- narrow bandwidth (limited usually to a maximum of 128kbits/s).

4.1 New Tools for Remote Diagnostic – Virtual Private Network

The VPN is designed :

- to provide the same functionalities of the RAS (remote support and monitoring on network elements through network management systems via a dedicated WAN equipment).
- to be more flexible for interventions that take place outside of business hours (to connect from any broadband internet access).
- to give the possibility for several customer or supplier technical support experts to connect anytime from anywhere on all their submarine systems simultaneously.
- to reduce significantly the operation cost to a fixed one (it is no more linked to the time spent).
- all countries involved in submarine business are able to provide in a very short delay a DSL access.
- DSL access provides a bandwidth starting from 1Mb/s to 20Mb/s. This will also extensively speed up the data transfer rates therefore increase the expert efficiency in solving issues.

4.2 New Network Design Considerations

The following considerations influenced the new design of this network :

- Traffic considerations
- Network equipment considerations
- Scalability and multi-access considerations
- Media selection
- Application protocol requirements
- Network address considerations
- Performance considerations

4.2.1 Traffic Considerations

An analysis of the anticipated traffic has indicated that the Platform supports with a 1Mb/s bandwidth a minimum of 20 X sessions simultaneously.

4.2.2 Network Equipment Considerations

A simple solution based on commercially available firewall routers is adequate for the technical architecture of the Platform at a reasonable cost.

4.2.3 Scalability and multi-access Considerations

The solution of a single firewall router is enough scalable as the multi-access is tuned by software.

Additionally, the large DSL bandwidth can easily stand multiple connections on the network.

4.2.4 Media selection

The *VPN* over Digital Subscriber Line (*DSL*) has been chosen for the following reasons:

- Availability : *DSL* is available at almost all of the remote sites.
- Bandwidth : the X sessions processed through the Network cause a large amount of data to be transferred between the remote sites and the Platform.
- Cost savings : It allows the use of a shared medium to enable private communications between two or more parties. This sharing allows subscribers to realize significant cost savings over installing private lines.
- Security : Communication content is secured so it is not read by unintended parties, modified; and, is verified that it actually came from the person identified as sending it. These security measures are characterized in terms of information privacy, integrity, and authenticity.

4.2.5 Application Protocol Requirements

The remote workstations run Network applications that use the process of the Internet Protocol (*IP*). Given this requirement, the technical choice leads to an equipment that provides Ethernet, *DSL*, data encryption and authentication software, and that supports the IP Protocol and moreover is able to create a secure IP tunnel.

4.2.6 Network Address Requirements

The remote routers, central-site access routers or remote access workstations should be connected to the Internet Network, so that the *IP* addresses will be provided by the local internet service providers. Then, the remote login software manages the creation of the dedicated secured connection.

4.2.7 Performances Considerations

A specific application used for the compression of the X traffic generated on the *WAN* during the session should be added into the *VPN* logical architecture.

4.3 Hardware Design

4.3.1 Remote Access Design

4.3.1.1 VPN remote Access Platform

VPN Remote Access Platform is the adaptation and the evolution of the existing *ISDN* Remote Access Platform described in section 3.1.1.

There are two evolving options :

- To install a direct router firewall to Internet.
- To install a router firewall connected to the intranet of the supplier**.**

The first option is easy and fast to be set up. It is very flexible and is mostly used for testing or on emergency request.

The second option is the most secure as it uses the high grade security infrastructure of the intranet of the supplier (maintenance resources, state of the art security…).

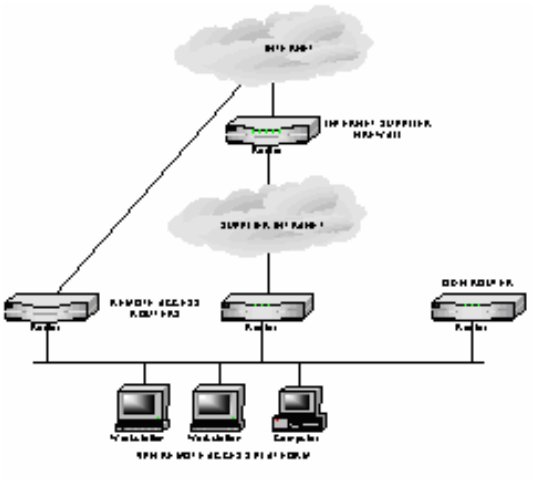

Figure 4: Hardware Design for the VPN Remote Access Platform

4.3.1.2 VPN Access to Remote Access Platform

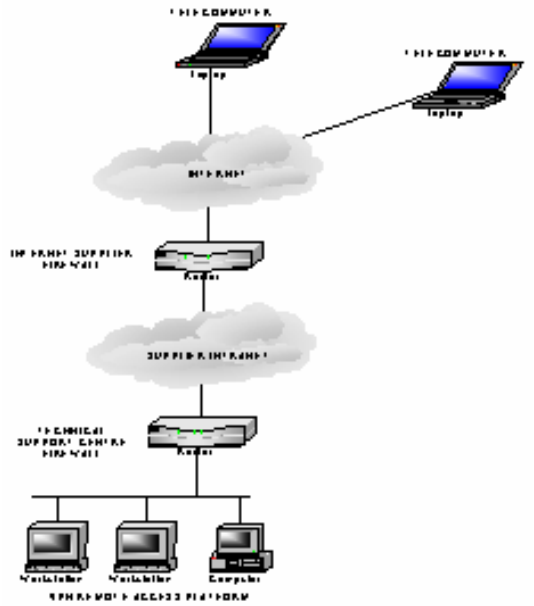

Figure 5: Hardware Design for the VPN remote access on VPN Remote Access Platform

For telecommuters (supplier technical support expert outside the office, at home, airport, hotel, etc.) *VPN* access, the Remote Access Platform is connected to the intranet of the supplier.

As a matter of fact, the intranet of the supplier is connected to the internet through a firewall equipped with token authentication devices.

There is a second level of security to protect the Remote Access Platform with a second firewall that only allows on call registered technical support experts. This simplifies the management in real time of telecommuter turnover.

These steps are necessary for the supplier to guarantee its customers that only chosen experts will be able to connect on their systems and that their systems can not be hacked.

4.3.2 Remote Site Design

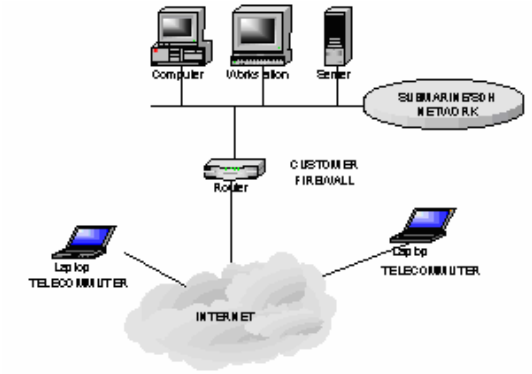

Figure 6: Hardware Design for the remote site

Remote site design is also based on the architecture of the traditional remote access described in section 3.1.2.

It consists in replacing the old router and the ISDN line access by a *DSL* internet access and a router firewall only able to create *IP* tunnel with declared *VPN* remote access platform of the suppliers or with declared telecommuters who are identified as customer technical experts. This is preventing any unwanted intrusion in the system.

4.4 Safe and Secure Process

The challenge in migrating to a VPN is protecting customer network from attack and securing traffic configuration transported over the public IP network. Securing these assets necessitates a comprehensive approach to address application, platform, network architecture, and physical security.

A comprehensive security plan begins with defining security policies that identify at-risk assets protection specification including protection type and level needed based on risk assessment. Following the security policies is designing a secure network architecture and implementing physical security controls with security operations procedures and practices.

This application note outlines a network architecture design that:

- Secures the network infrastructure and host systems from unwanted intrusions.
- Ensures the privacy, integrity, and authenticity of data transported over the public network

The design is based on strategic placement and implementation of VPN routers and VPN firewalls.

Moreover, to achieve information security objectives, a set of standards and protocols called the Internet Security Protocol (IPSec) is used to implement VPNs. IPSec uses encryption to ensure message privacy and secure hashing to ensure message integrity. Digital certificates authenticate the sender and destination.

In the past, a simple approach to securing the network infrastructure was to place a packet-filtering firewall at the network perimeter, at the point where it accesses the Internet or the *ISP* (*Internet Service Provider*) network. While adequate for certain low-risk sites, this is not appropriate for sites needing higher levels of protection such as submarine and *SDH (Synchronous Digital Hierarchy*) networks management system. Sophisticated hacker tools and techniques for scanning, footprinting, enumerating, and spoofing networks, reveal vulnerable systems and available ports where attacks may be launched through firewalls with ports open to support in-bound services protocols, such as http, smtp, and ftp. Normally the first target of this network fingerprinting process is the firewall. The designed VPN platforms used are bridge level (Layer 2) devices, unresponsive to hacker information gathering and detection techniques. And they block traffic suspected of finger printing or scanning the network.

As an ultimate security feature to keep control of their own network, customers can switch off the router firewall and start it only on suppliers or telecommuters requests.

5. CONCLUSIONS

With this new technology, the operators can use complex computer systems and software to monitor the network. A remote diagnostic contract is offered to the customer as a service. It allows:

- active and fast contact with experts
- down time reduction
- safe and secure access for network integrity
- cost reduction for on site intervention
- preventive maintenance
- software patch installation

This solution could be also extended, on the customer side, to replace leased line used for *ROPs* (Remote Operator Position), *NOC* (Network Operating Centre), *DCN* (Data Communication Network) backup or for geographical redundancy by reducing drastically the operational cost

To conclude, the *VPN* is the optimum solution available on the market.