THE LIGHTNING FLASH

A VISION OF NETWORK WORLD ISSUE 3/99

Multi-Internet®

LIGHTNING's latest breakthrough in Networking and Security

Following it's AutoConfiguration™ 1998 breakthrough, Lightning is proud to announce a new technology, Multi-Internet®, which has been exclusively developed by Lightning's engineering staff in cooperation with leading Internet Service Providers and is now delivered on its whole range of Lightning MultiCom routers.

This exclusive new technology allows new types of ISP-supported applications, like smart Extranets, differentiated classes of Internet accesses for the same customer, or even for different customers through the same connection. Another use of Multi-Internet is to provide easy and secure on-line access for remote support of computer systems to multiple customers. Finally, it optimizes the security of the internal network, by fine-tuning its external visibility.

Continued on page 4

Dr. B. Brunner
Managing Director

France Telecom
Oléane

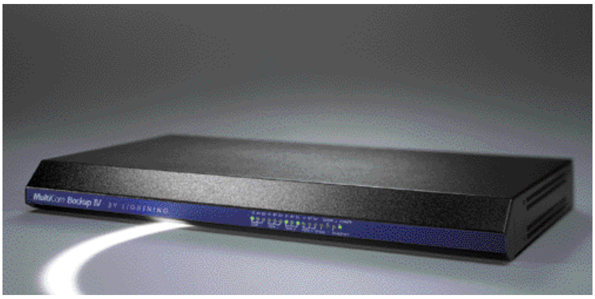
uses Lightning's MultiCom

France Télécom's subsidiary Oléane, one of the major ISPs in France, approved and now uses Lightning's Multi-Internet technology, making the Pocket MultiCom its only "Highly-Recommended" access-router for all its types of ISDN Internet and Intranet accesses.

Security & 128 bit Encryption

Security in Computer Networks

Many companies today have Intranets to exchange information throughout the company. Remote locations of such networks are connected over public networks, for example leased lines or ISDN connections provided by telecom operators. In some cases it is more cost effective to use the Internet between remote locations, which leads to so-called Virtual Private Networks.


MultiCom Backup IV: the secure solution for Virtual Private Networks.

Data exchanged on Intranets can often be very sensitive and thus a lot of attention has been given to securing these networks. Some type of data, like patient records of a hospital, have to be kept private by law. The only effective solution is to use a device which encrypts all data that leaves a local network. The data then transits in encrypted form over public wires and possibly the Internet. When it arrives at its destination it is decrypted again by a similar device. Ideally, the encryption and decryption devices are part of routers. This is particularly important in a VPN scenario. In this case, not all data leaving a local network for the Internet needs to be encrypted. You want to be able to talk to machines on the Internet which are not part of your company. Thus only the data going to a remote location of the VPN must be encrypted. Data going to a public part of the Internet should be left as it is. The decision of whether to encrypt has to be based on the destination of a data packet and is best made in the router that connects the local network to the Internet.

Security at Different Levels

If two sites of an Intranet are directly connected by ISDN or with a leased line, security can be provided at the link level. Using encryption at the link-level provides security for any type of data carried through the link.

On the other hand, if the sites of a network are connected through the Internet, then security has to be provided at the IP level, because, the data is carried over many differents links owned by different operators. In that case an encrypted data packet still needs a valid IP header. That header must be readable by any router in the Internet so that the packet can be routed correctly to its destination. Once it gets there, the payload of the packet can be decrypted again.

How Secure Is Your Encryption?

The quality or strength of an encryption depends both on the algorithm and the length of the key used. An attacker has two ways of breaking a cipher text: He can try to be clever and exploit weaknesses of the algorithm, or he can use brute force and simply try all possible keys until a useful message appears. An algorithm is considered strong if it has been public for several years and no weaknesses have been discovered. An example of such a strong public algorithm is the International Data Encryption Algorithm (IDEA) developed in Switzerland and used in many encryption systems. Another popular algorithm is the DES algorithm devised by the National Security Agency of the USA.

The only way to attack a strong algorithm is to try all possible keys. Therefore the strength of such a strong algorithm depends on the key length only. Typical key lengths are 40 and 56 bits for DES and 128 bits for IDEA.

An attacker has two ways of breaking a cipher text

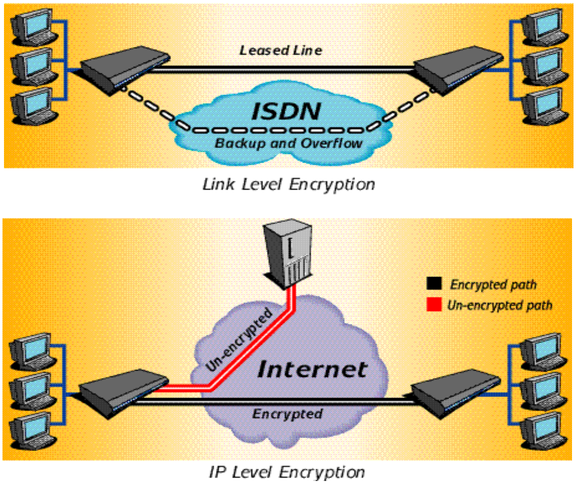
With 40 bits there are 1100 billion possible keys. The number of keys grows exponentially. With 128 bits there are not 3 times more key but 0.3 billions of billions of billions more keys than with 40 bits!

The DES algorithm, which has a 56 bit key, has lately been cracked on a 250’000$ special purpose machine in 56 hours. Cracking a 40 bit key is thus a matter of seconds. Luckily we have many years in front of us before we will see machines that break 128 bit keys.

Export restrictions

“So”, you may ask, “why doesn’t everybody use 128 bit keys for encryption?”. Some countries have regulatory limitations on export of cryptography. For example the US law only allows unrestricted export of “security” products with 40 bit keys. Systems with longer keys may be exported upon approval and for special, well defined purposes only. Systems with a key escrow, a back-door which gives the authorities full access to the data that is being encrypted, are easier to export but still need to be approved.

Switzerland has no such export restrictions for encryption devices, which is why Swiss companies like Lightning can offer products with strong 128 bit encryption algorithms and no back-doors.



Link Level Encryption

IP Level Encryption

Figure: Simple link-level and IP level encryption

Keep it private

Intranets are an important communication tool for companies. They increase the efficiency and can provide a competitive advantage. If your Intranet runs unencrypted over public lines or even the Internet, anybody with the right tools can have a peek at your company’s data.

Many routers on the market now do not even have the possibility to be upgraded with a strong encryption option with 128 bit keys. Choosing a router with 128 bits encryption option makes sure that nobody will be able to crack the encryption and lets you keep your business private.

success story

Major Banks use Lightning’s Secure Routers

Lightning is proud to count among its prestigious customers quite a few leading banking and finance institutes. This report outlines the variety of applications that these banks have setup using Lightning MultiCom routers.

Application 1:
Customer Connections

Some of Lightning’s banking clients connect their customers directly to the bank’s facilities. This not only improves customer service and satisfaction, it also significantly reduces the bank’s ongoing costs. It allows the bank to create a comprehensive portfolio of electronic corporate banking and Internet banking. New financial products can be delivered with a very fast time-to-market, thanks to a direct TCP/IP networking connection with their customer, assuring application compatibility. Banks often choose the LIGHTNING MultiCom LAN Access Centers with 128 bits encryption option and ISDN Primary Rate interface for the central location, while Pocket MultiCom Secure ISDN Routers are preferred for customer premises and the Series IV for branches.

One customer bank’s Vice-President says that *“For linking all of our major customers to our bank and reliably providing them with their mission-critical data, in a secure way, we needed a “bullet-proof” solution. LIGHTNING provided an integrated solution, with the Pocket MultiCom. We are now equipping new customers in minutes instead of days.”*

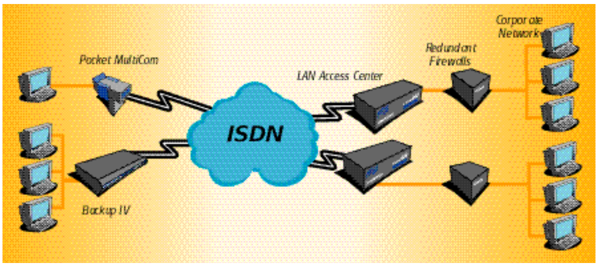


Figure: Typical MultiCom setup scheme for banking applications

Application 2:
Branch Offices

Other banking customers connect their branch offices to their main offices. While ISDN with the Pocket MultiCom is the right choice for small offices, leased lines using Classic MultiCom or MultiCom Series IV are preferred for larger locations with almost permanent traffic.

Application 3:
Bank-to-Bank and Finance-Institutes connections

Banks are also often using MultiCom encrypting routers to link with their partner banks and finance institutes, enabling the use of networked applications across banks.

Application 4:
Backup Sites

ISDN is very well suited to interconnect backup computing sites in case of emergencies. In this situation, a MultiCom Backup IV, with its 8 ISDN B-channels, which can be bundled and 128-bit IDEA™ encryption option, proves to be the best choice. Some of the leading European private banks use this setup.

Application 5:
Tele-Working, Tele-Maintenance

In a competitive world, banking networks need to run around-the-clock with an optimal security. Network Managers need to have secure, encrypted, remote access to the bank network from home or from geographically distant locations. Corporate managers also need to be able to follow the banks operations from home. For these situations, the Pocket MultiCom with Encryption option proved many times to be the right choice.

Selecting the best end-to-end exportable solution

Thanks to Lightning's extensive Security technology, solid customer references, and excellent reputation, the selection process is often accelerated, reducing cost and lead-time to installation.

The fact that the Lightning routers and encryption technology have been developped and manufactured in Switzerland, and thus are not subject to US encryption export law, provides customers with an easy export.

All-in-one: Reducing acquisition and installation costs

Using the secure remote access solution from Lightning, banks significantly reduce their acquisition and installation costs by leveraging their data network and eliminating the need for additional dedicated encryption and security units.

"*After testing a number of potential solutions, it became clear that separate solutions for network and security could not meet our needs for high network availability and enhanced network Security*" says the Manager of a customer integration project of a leading bank. Its Network Manager adds: "*The ability to integrate access routing and security and deliver applications with outstanding performance is one of the strongest appeals of the MultiCom end-to-end solution. Dynamic bandwidth allocation gives us much greater availability with lower cost. Only the MultiCom product family provides the functionality that we require for today's and tomorrow's services in a compact device*". The Vice-President of the same bank adds: "*Lightning has provided highly qualified support and reacted promptly to our wishes for new features, which are now available and maintained in all their standard products.*"

The Pocket MultiCom lets the managers follow the bank operations from home with absolute security

Year 2000 compliance

The declared and tested Year 2000 compliance of Lightning's MultiCom secure routers also helps greatly to reduce the overall compliance tests which have to be carried out for mission-critical banking applications, such as the ones in which the Lightning MultiCom are being used.

Non-stop Growth and New Opportunities

Most of Lightning's banking and finance customers extend the uses of MultiCom routers to new fields of applications and scale of uses, not envisioned before, proving their right choice. ■

MultiCom secure routers link key customers to UBS

In 1996 UBS was looking for an internationally available, highly secure, remote access solution for its key customers in Switzerland, as well as for its small branches worldwide. As a result of a through selection process, with extensive lab and field tests, UBS chose LIGHTNING's MultiCom encrypting routers.

Up to the end of 1998, UBS deployed five MultiCom LAN Access Centers in its central dial-in locations and approximately 220 Pocket MultiCom Secure ISDN Routers at key customer premises as well as at selected foreign branch office locations. Additional new key customers will be connected in 1999. UBS's key customers and branches enjoy the convenience of the new services, which changed the way they do business and has reduced the transactions and service cost.

MultiCom secure links to branches of Axus

Axus is a subsidiary of Ford Financial Services Group and supplies customers with cars from every vehicle manufacturer, from ten wholly owned locations: UK, France, Germany, Spain, Italy, Belgium, Netherlands, Luxembourg, Finland and Denmark. Axus manages fleets for leading organizations throughout Europe. Currently 80'000 vehicles are under contract.

Last year, Axus Finland has been looking to secure the communication between their different locations. Classic and Pocket MultiCom routers have been deployed to secure these links. The implementation has been very successful and MultiCom Secure Encryption Routers will be now used to encrypt other branches of the group around Europe.

DISTRIBUTORS NEWS

Belgium
Alfa Systems NV
Mechelseweg 24 - 2811 Hombeek
Tel. +32 15 45 11 60 - Fax +32 15 45 11 65
www.alfasys.be

Call Consult Service
Avenue Molière 77 - 1190 Bruxelles
Tel. 0032 2346 9150 - Fax 0032 2346 9155

Switzerland
Commcare AG
Turmstrasse 8 / Gaswerk Nord - 8952 Schlieren
Tel. +41 1 738 61 11 - Fax +41 1 738 61 10
www.commcare.ch

Germany
Comtes GmbH
Osterdeich 110/112 - 28205 Bremen
Tel. +49 421 49 99 20-Fax +49 421 49 99 280
www.comtes.net

Sweden
DataNät AB
Box 532 - Rallarvägen 17B - 18425 Akersberga
Tel. +46 8 544 10 600 - Fax +46 8 544 10 644
www.datanat.se

Netherlands
- DDN - Dacom Distributie Nederland
Bongerd 6a - 7642 DA Wierden
Tel. +31 546 58 00 58 - Fax +31 546 58 00 59
www.ccg.nl/ddn/

Denmark
NetDesign A/S - Gammelgardsvej 91
3520 Farum
Tel. +45 42 95 38 88 - Fax +45 42 95 38 44
www.netdesign.dk

Italy
Siemens Nixdorf Technologies SRL
Via nuova ponente 1/A-B - 41012 Carpi
Tel. +39 59 63 77 11 - Fax +39 59 63 77 22
www.snt.it

XABA Datacommunications s.r.l.
74 Via dell'Imbrecciato - 00149 Roma
Tel. 0039 06 55 03 778 - Fax 0039 06 55 14 628
www.xaba.it

Korea
Daesin Computer & Communication Co. Ltd
Young Hwa Bldg
193-8 Youn Hee-Dong Seo Dae Mun-Gu
Tel. +82 2 322 41 41 - Fax +82 2 322 29 00
www.daesincomm.co.kr

CALENDAR OF EVENTS

CommunicAsia 99
Singapore - 22.-25.06.99

Networld+Interop 99
Paris - 15.-17.09.99

Telecom 99
Geneva - 10.-17.10.99

THE LIGHTNING FLASH
Issue No. 2 - March 1999
Editor: Dr. B. Brunner,
Managing director

LIGHTNING InstrumentationSA
Av. des Boveresses 50 - 1010 Lausanne
Switzerland
Tel. +41 21 654 2000
fax +41 21 654 2001
Internet: www.lightning.ch
Email: info@lightning.ch

highlight

Multi-Internet® Technology Overview

Multi-Internet® brings key competitive advantages to ISPs and corporate customers

Lightning's Multi-Internet Technology consists of five major inter-working components:

- Multi-PAT,
- Multi-NAT,
- built-in SecureWall™ firewall,
- dynamic IP-address handling,
- fully classless TCP/IP routing.

This smart combination allows to virtually assign any internal (Intranet) IP-address to any external (Internet or Extranet) IP-address, including dynamically allocated addresses. Even groups of Intranet IP addresses can be assigned to Internet-addresses. The above figure illustrates the possible combinations and their applications.

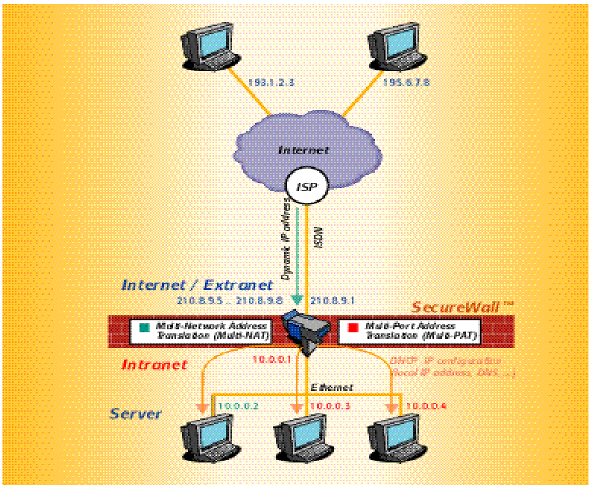


Figure: Example of a Multi-Internet access.

To be fully effective, Lightning's Multi-Internet-capable MultiCom routers must be used in the remote location, while a Multi-Internet-aware ISP setup should be made at the central location, either using Lightning routers or existing equipment from third parties.

This new technology will allow ISPs to efficiently differentiate their offering by providing new services with high added value.

Application 1
Extranets and VPNs

Translating specifical groups of Intranet computers to corresponding external Internet addresses, routed into an Extranet over the Internet, allows ISPs with an Extranet infrastructure to very simply connect Intranets together, while providing Internet access to the rest of the internal network.

This application is useful in a variety of situations: multinational companies with distributed departments, communities of companies working together, schools with administration and education networks, and so on.

Application 2:
Differentiated Internet Access

Sometimes, different parts of a company need different Quality of Service (QoS) for their Internet or Intranet access. Bundling different groups of computers from the same location into distinct Internet or Extranet addresses can allow the provision of differentiated Priority, Bandwidth and Quality of Service: all costly features, which can now be applied only to the parts of the company really needing them. Typical examples include Internet and Intranet Servers, dedicated high-quality Extranet services of ISPs.

Application 3
Linking multiple customers or even ISPs

Sometimes, industrial buildings host multiple companies, which may want to share a single access line to an Internet access. With Lightning's Multi-Internet technology, this is now possible, providing each company with a dedicated Internet access and own Internet addresses, but using the same access line, be it ISDN or a leased line. ISPs are also users of this new technology.

Application 4:
Remote Maintenance and Support

For all branch-specific, customer-adapted, software applications, like Enterprise Resource Planning (ERP) applications, the service company, which installed the application, may also provide remote maintenance service. The new Lightning Multi-Internet technology allows to route and translate incompatible IP addresses of the customers into IP addresses compatible with the service company's internal network, providing on-line network-based remote maintenance to all customer's servers and computers. All kinds of companies are interested in this new Lightning technology.

Multi-Internet is available as a standard feature on all members of the MultiCom family in software release 2.5. ■