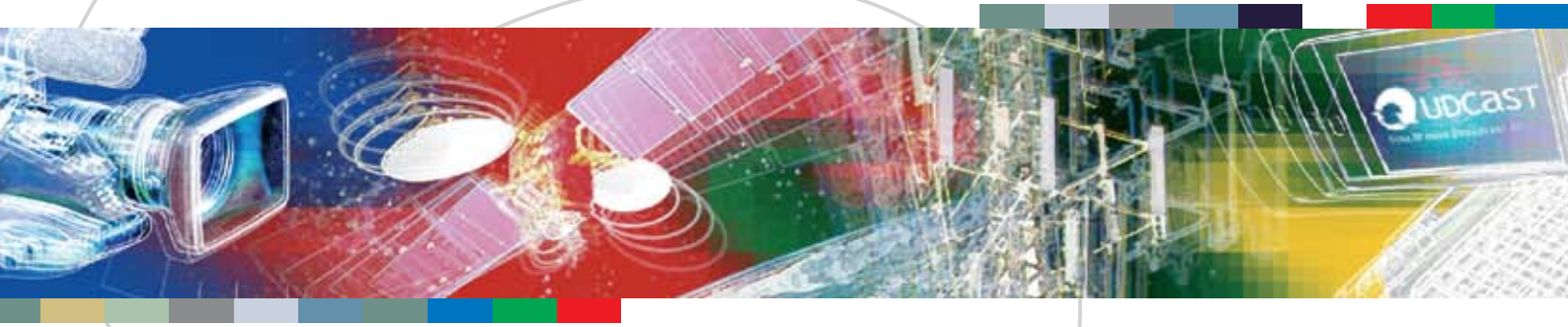


UDgateway VPN Q & A

Objective

This document is designed to answer the most frequently asked questions about UDcast's UDgateway appliance. Further information may be found on UDcast's web site www.udcast.com

UDcast

IP • BROADCAST • WIRELESS

TABLE OF CONTENTS

VPNs OVER SATELLITE: ISSUES AND SOLUTIONS

1Q: Can I run my standard VPN over a satellite connection and what will be the performances

A: Standard IPsec VPNs can run over satellite connections. However performances are often so bad that the VPN is quasi unusable. In most cases the VPN traffic is limited to around 70 to 90Kbps regardless of the satellite link speed. Hardly sufficient to meet enterprise needs.

2Q: What are the reasons for these performance problems

A: The reason for these performance problems is satellite's latency, which is not normally experienced on a terrestrial circuit. This considerably impacts transport protocols such as TCP/IP originally designed for latency free environments. Very often the latency is interpreted as congestion by the protocol, which refuses to ramp up transmission thereby leading to reduced connection speeds. In many cases performance enhancement technology, such as TCP/IP acceleration, has been implemented to be able to make full use of the satellite link capacity. However in the case of VPNs these TCP/IP accelerators have no effect.

3Q: Why doesn't my usual TCP/IP accelerator improve VPN performances

A: Standard VPNs encrypt the TCP/IP traffic with IPsec to ensure its security over the public Internet. Therefore the TCP/IP accelerator is unable to intercept the original TCP/IP header and the acceleration is disabled. In other words it is impossible to encrypt using IPsec and then accelerate meaning, that regardless of any acceleration technology a satellite system may have, VPNs cannot function.

4Q: What does UDcast do to solve VPN performance issues

A: UDcast has developed the UDgateway which resolves these problems enabling site-to-site IPsec VPNs over satellite with terrestrial like performances. The UDgateway first accelerates the traffic and then encrypts it in IPsec bringing terrestrial like performances.

UDGATEWAY FEATURES AND BENEFITS

5Q: What are the key features of the UDgateway

A: The UDgateway brings the capability of being able to offer both security and performances over satellite through one integrated appliance. The UDgateway enables the deployment of key applications such as native web (Intranet) or web enabled business applications using web-to-host architectures, as well as windows terminal server type applications.

Amongst the UDgateway's features:

- Satellite system agnostic
- IPsec encryption enabling the setting up of VPNs between sites
- Two-way acceleration technology enabling the acceleration of encrypted download traffic but also upload traffic
- Designed to function over both satellite only networks and hybrid networks
- Application specific enhancements such as pre-fetch technology and caching, enabling smoother web surfing over a VPN
- Key IP functionality including
  - Firewall, antivirus and NAT
  - HTTP and DNS caching
  - HTTP prefetch and pipelining
  - SMTP mail relay
  - DHCP server
  - IP routing with split tunnelling
  - QoS
  - WANcompress: compression technique based on disk

6Q: What are the key benefits of the UDgateway for the SSP

A: The UDgateway brings several benefits to satellite service providers. In particular it enables the SSP to considerable increase revenues by reaching new markets with new services. The UDgateway enables them to:

- Develop completely new services or improve upon existing ones
- Reach new markets
- Enable premium high quality service with both performances and security over a standard satellite broadband connection
- Enable the creation of a portfolio of different services (see deployment scenarios)
- Easily integrate the appliance into existing service offerings to bring added value
- Meet customers' security and performance concerns
- Offer a flexible solution bringing value to both small and large-scale deployments
- Adapt to both SME and corporate markets
- Offer a pay as you grow solution
- Reduce satellite link cost due to data volume reduction

The UDgateway is an integrated one-stop solution facilitating:
- Seamless integration of satellite links into global enterprise networks
- Integration in various network architectures
- Service roll out
- Service maintenance

7Q: Does it only work over satellite links or also over hybrid/terrestrial networks

A: The UDgateway can be used to set up a VPN between satellite-connected sites but also where terrestrial, WiMAX or cellular sites are connected. Application enhancement provided inside the VPN makes the UDgateway ideal for networks where bandwidth is not enough for the applications to work, or where the delay makes applications working in a degraded mode.

8Q: Can I run VoIP over my VPN

A: UDcast's Gateways support DiffServ enabling priority traffic to be recognised and managed by the UDgateway's QoS mechanism. This enables UDcast to guarantee sufficient quality for applications such as voice. Secure VoIP can therefore be used over the UDgateway.

9Q: Why should SSPs create a premium service using the UDgateway

A: The UDgateway enables satellite service providers to build a premium offer. The development of a premium offer brings a number of benefits to the SSP.

Differentiation:
Satellite service providers are finding it difficult to differentiate their service other than through price. The UDgateway enables them to at last fully differentiate themselves from competitors by offering a premium service guaranteeing:

- High performances
- Embedded network security
- Simple network integration

It gives customers the choice between a low-end service and a high-end service with clear understandable differences.

Reseller sales:
By bundling a UDgateway into a package satellite service providers considerably simplify the sales effort for resellers.

- The reseller can now easily make proposals inline with each service level goal and budget.
- Minimises integration costs with pre-determined integration scenarios, reduced PC tuning etc
- Guarantee customer satisfaction through an improved end-user experience
- Add specific value such as network integration and security enforcement
- Increase revenue through value-add services such as network architecture, security plans etc

Increase Bandwidth sales:
By developing a wide range of offers and services, meeting the needs of a number of different market categories, a SSP can considerably expand its target market and boost sales. A wide range of services attracts a wide range of customers, many taking the basic service whilst others needing immediately the premium service or upgrading to it later.

Profit and margin flexibility:
By offering a range of services SSPs can strategically manage their profit and margin distribution. By fine-tuning margins on the different offerings, satellite service providers can set and achieve various goals (such as focusing on selling additional bandwidth or selling services etc).

Add more users on the same bandwidth resources with WANcompress

10Q: How is UDcast different from its competitors
A:

UDcast:
Brings satellite aware solutions to the enterprise world.
Terrestrial links can also be enhanced (by reducing bandwidth usage) and encrypted.
Looks at the end-to-end global solution.
Provides solutions that cover the totality of the network- not just the satellite portion or enterprise portion.
Makes use of standard IP protocols and practices
Seamlessly integrates satellite into the enterprise network.
Application transparent: enables transparent use of ALL applications over satellite.
Enhances the global end-user experience.

Competitors:
Tend not to look at the global picture.
Expertise limited to one specific area: either security, satellite or terrestrial.
Bring partial solutions based on their area of knowledge. Unable to provide a global solution.
Implement solutions in non-standard ways.
Considerably impact existing network architecture and management.
Non-transparent solutions impacting applications.
Only partially enhance end user experience.

UDcast are dedicated to bringing satellite aware solutions to the enterprise world. With extensive experience in both IP and satellite technology, and by looking at the end-to-end picture, UDcast provides the missing link enabling satellite to seamlessly integrate with existing terrestrial enterprise networks.

11Q: What key messages can an SSP put forward when using the UDgateway

Amongst the key messages that a SSP can use thanks to the UDgateway are:

- The network security of a traditional IPsec VPN with enhanced performances over satellite
- The secure extension of your LAN to branch offices, partners, suppliers or customers
- Extend existing VPN coverage
- Network back up with secure network overlay
- Highly Flexible solution
  - VPN plus Internet access solution
  - Any architecture
    - . Keep existing network architecture
    - . Complete satellite VPN or VPN extension
    - . Support for satellite only networks or hybrid networks (whatever the mix of access technologies)
    - . Distributed or centralised security enforcement
    - . Distributed or centralised Internet access
    - . Any application
    - . Application server software
    - . Enterprise resource planning
    - . Collaborative suites
    - . WANcompress
    - . Reduce bandwidth consumption
    - . Enhance enterprise applications (e.g. Citrix, SAP, Oracle)

- Scalable solution
  - Unlimited number of tunnels
  - Easy addition of sites
  - Pay as you grow solution

UDGATEWAY DEPLOYMENT

12Q: Where is the UDgateway placed

A: The UDgateway is placed at either end of the desired VPN connection, between the satellite indoor unit and the LAN. In other words one UDgateway is placed at the satellite connected remote site and another at the central/HQ site. The exact positioning of the UDgateway can vary depending on the site's network and security requirements

13Q: Does the UDgateway impact the existing network

A: No the UDgateway doesn't impact the existing network. The UDgateway will seamlessly integrate with the existing network.

14Q: Does the UDgateway need to be configured specifically for various applications

A: No the Udgateway is application independent.

15Q: Is hub equipment needed

A: No equipment is needed at the hub. The hub is transparent to the VPN.

16Q: Is there a limit to the number of VPN tunnels

A: Up to 100 tunnels can be easily dealt with by the UDgateway at the central site. A 500 tunnel UDgateway is planned. Above that number UDcast has a customisable architecture which can be adapted to best meet the customers' needs.

17Q: Can the enterprise carry on using its existing VPN equipment and still benefit from two-way acceleration

A: Yes the enterprise can carry on using its existing VPN equipment (Cisco®, Checkpoint® etc). In this case the IPsec encryption within the UDgateway will be disabled and the UDgateway be placed before the third-party VPN. VPN traffic will fully benefit from the UDgateway's site-to-site two-way acceleration.

18Q: Can the enterprise still access the Internet

A: Yes the UDgateway enables full Internet access. Two scenarios can be implemented.

In high security conscious organisations all access by a remote site to the Internet is made via the main central/HQ site. In this case all Internet traffic will come via the main site and will reach the remote site via the VPN connection. Internet access via the VPN will of course benefit from the UDgateway's performance enhancement.

When security is less centralised at the HQ remote sites can access the Internet directly. In this case the UDgateway uses split tunnelling to enable at the same time VPN access and Internet access. In addition the UDgateway's firewall will protect the remote site from attack.

19Q: Can the enterprise communicate from a branch office to another branch site

A: Yes two branch offices can communicate securely by VPN by transiting through the central HQ. In June, with the launch of the Advanced UDgateway, fully meshed networks will be enabled allowing branch offices to communicate directly between themselves without passing through the HQ

20Q: Describe some deployment scenarios

A: The UDgateway can be deployed in a number of cases.

- **VPN over the Internet**
  An example of this would be an SME HQ needing secure communications with a satellite connected remote office of production site. The remote site will access the Internet directly using split tunnelling or via the HQ site.
- **Partner Interconnection**
  A satellite connected SME requiring a secure connection into a partner site in order to share applications and transfer information. In this case the SME will access the Internet directly.
- **WAN & distributed Internet**
  A company with multiple remote sites of which several use satellite connections. Those with satellite connections link into the HQ using the UDgateway. If each site is responsible for its own security (local firewalls etc) then Internet access will be made directly using split tunnelling.
- **WAN & Central Internet**
  Same as above except that security is centralised at the HQ thus barring remote sites from accessing directly the Internet. In this case all Internet access will go via the main HQ.
- **WAN Extension**
  An enterprise wishes to connect its satellite connected remote offices to its LAN thus needing VPN to ensure its WAN security.
- **Managed VPN extension**
  Terrestrial service providers with managed VPN offerings seek to offer a global uniform VPN service regardless of their customers' location and broadband connection. Through the use of UDgateway a seamless extension to their network can be made over satellite. In this case there will be a central interconnection with the service provider's terrestrial VPN network.
- **Bandwidth savings**
  Satellite technologies and also new technologies like WiMAX are suffering from lack of bandwidth or very expensive price. The UDgateway allows saving in average 50% of the bandwidth consumption, which makes enterprise applications to work in a LAN-like way.
- **WAN Backup and disaster recovery**
  Very often looked at by financial and government organisations. In the case of a terrestrial network failure (Network outage due to fire, earthquake etc) satellite is the ideal back-up network. For most organisations security is key therefore requiring the use of VPNs.

21Q: When accessing the Internet directly from the remote site will the enterprise benefit from performance enhancement

A: Yes. In all cases the users will benefit from smoother web surfing thanks to the UDgateway's web pre-fetch technology. To benefit from UDcast's TCP/IP acceleration enabling fast file download the satellite hub needs to be equipped with an UDstation.

22Q: When accessing the Internet directly from the remote site can the enterprise use performance enhancement technology which may already be included in the IDU

A: Some IDUs already have performance enhancement technology enabling fast file download. In this case UDcast's TCP/IP acceleration can be deactivated removing the need for an UDstation at the hub. The enterprise will still benefit from UDcast's additional performance enhancement technology: Web pre-fetch and caching making for considerably smoother web surfing.

23Q: How do VPNs for mobile users work over satellite

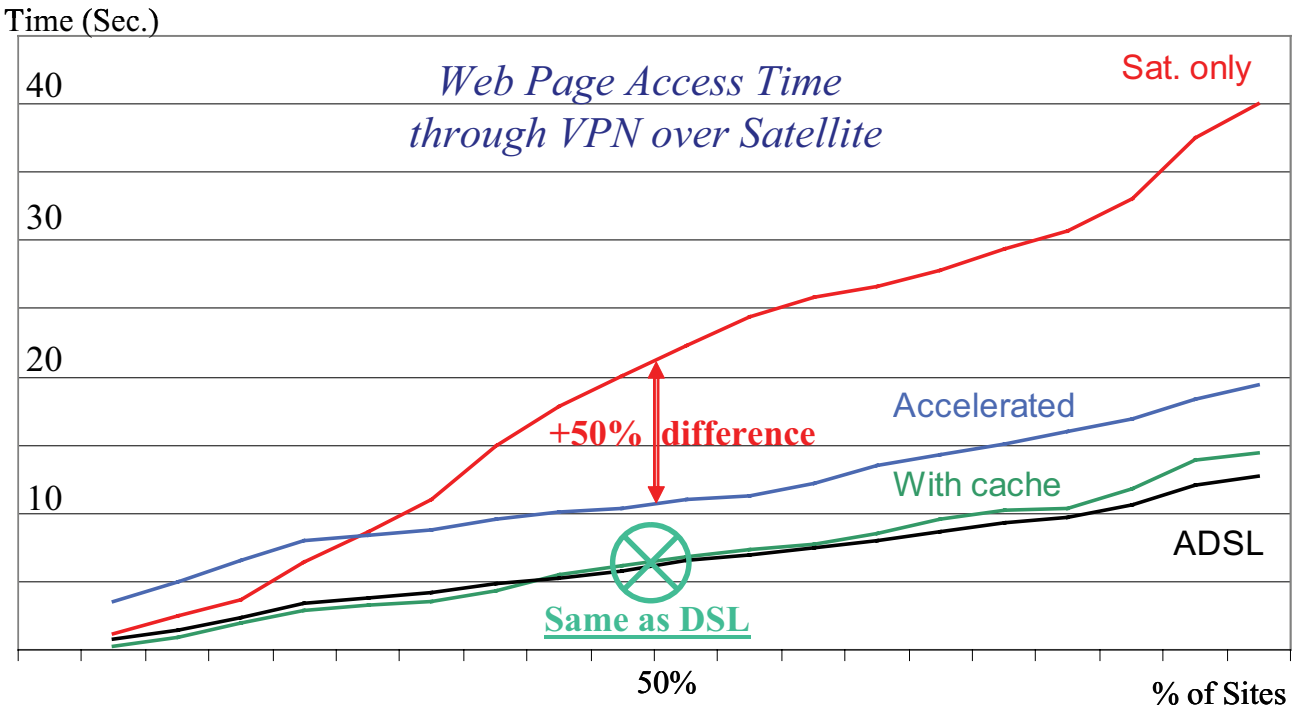
A: SSL based VPNs should experience no difficulties over satellite connections. However those with IPsec based solutions on their devices there will be performance problems. There are currently no solutions resolving this whilst remaining IPsec based

24Q: What performances can the enterprise expect using a UDgateway over satellite

A: For web based applications such as native web (Intranet) or web enabled business applications using a web-to-host architecture, the UDgateway enables performances identical to those expected of an equivalent DSL connection (with cache enabled).
For file downloads from the central site performances are improved on average by 2 (for large files). In general full use is made of the available bandwidth in both ways.

For direct Internet access from the remote satellite connected site, performances are improved by a factor of two leading to a greatly improved web surfing experience.
For direct file download performances can be improved by up to 8 times (when no other accelerator is in place). In general full use is made of the available bandwidth on downloads.

These are the results for tests over an operational Internet service 1Mbps/256Kbps. Through the use of the UDgateway, performances may be brought in line with those obtained over a DSL link with equivalent bandwidth.



25Q: What bandwidth saving can be expected using a UDgateway over satellite

A: The UDgateway provides TCP ACK suppression in order to save bandwidth on the return link when downloading files. This is key on VPN as the ACK is tunnelled, adding extra weight per ACK. Within the UDgateway's current implementation, only 24Kbps is used to acknowledge a transfer at any rate. Thus, at 2Mbps, 80Kbps is saved on the expensive return channel (28Kbps at 1Mbps).

26Q: What is the performance difference between accessing the Internet via the HQ or directly

A: Accessing the Internet via the VPN to the HQ may have lower performances than accessing the Internet directly. This is difficult to measure because of the sheer number of different possible cases.

27Q: What other VPN solutions may your competitors offer

A: There are very few solutions, which solve the problems of VPN over satellite. The UDgateway is the only one that enables the seamless integration of satellite links into enterprise networks. This is mainly based on bundling security - IPsec based site-to-site VPN - and performance enhancement - two-way acceleration and application specific optimizations. Most solutions are either partial, solving only half the problem, or intervene at an application level and use some form of proprietary non-IPsec encryption behind TCP-IP headers impacting security.

- **Partial VPN solution**
  This involves collocating equipment at the satellite provider's hub as well as at the two sites communicating via VPN. An encryption mechanism is used between the remote site and the satellite hub. This encryption is not standard and usually keeps the TCP headers which reduces the level of security with destination addresses, emission addresses as well as the traffic type clearly visible There is a break in the VPN at the hub and then an IPsec based VPN relays the data to the central HQ. The acceleration is therefore only one way between the remote site and the hub, and high security through the use of IPsec is only present on the terrestrial portion of the network. This approach does not provide end-to-end security, thus not answering current enterprise requirements.

- **Application layer VPN**
  This approach involves a software client on every PC operating at an application layer or a CPE that spoofs the TCP session in order to encrypt traffic before sending it with clear TCP/IP headers. A proprietary tunnelling mechanism is used. As the data is then injected into the TCP/IP session, TCP/IP acceleration systems which may or may not be available over the satellite system will accelerate the encrypted application data. Acceleration is only one-way. This solution does not provide global private network at IP level, thus does not answer to current enterprise requirements.

Both these approaches also mean that it is impossible to use existing VPN equipment such as Nortel® Contivity or Cisco® VPN 3000 or firewalls such as Checkpoint® or Cisco® PIX. And in both cases by not being IPsec site to site they do not enable seamless enterprise network integration.

28Q: What can the service operator offer a client who doesn't yet need a VPN but yet still requires performance enhancement

A: The UDgateway brings all the necessary performance enhancement technology and can be upgraded at a later date when the end client requires a VPN.

GENERAL VPN QUESTIONS

29Q: What is a VPN

A: Virtual private networking allows organisations to securely connect remote offices and remote users through cost-effective third-party Internet access, rather than expensive dedicated WAN links. VPNs are an alternative to expensive Frame Relay and leased-line WAN infrastructures to provide secure network connectivity for branch offices, business partner extranets... In other words VPNs enable the setting up of secure connections over the public Internet infrastructure.

30Q: What is a site-to-site VPN

A: A site-to-site VPN is a secure connection between two trusted sites over the public Internet. Site-to-site VPNs usually use the IPsec protocol.

31Q: What other types of VPN exist: What is the difference between an IPsec based VPN and a SSL VPN

A: In addition to IPsec VPNs you will also come across SSL VPNs. IPsec VPNs are built upon the network layer and provide access to corporate resources for remote offices/branches. In some cases they are also used for mobile workers in which case the download of software onto the worker's PC is needed.
However in most cases for VPN access from a mobile environment SSL VPNs have been developed. Using an SSL VPN the connection between the mobile user and the internal resource happens as a web connection, at the application layer, making it ideal for mobile users because:

- SSL doesn't need to be downloaded onto the device used
- SSL doesn't need to be configured by the end user
- SSL is available wherever there is a standard web browser, so users don't need a company laptop.

The question is not to choose between an IPsec VPN and a SSL VPN. They are complimentary in that within a same organisation both will be used: IPsec for always-on remote branch site-to-site VPNs and SSL VPNs for mobile VPN access.

32Q: What categories of VPN are available on the market

A: Enterprises have 3 main choices when adopting a VPN.

- **Do it yourself VPN (DIY VPN)**

In this case the enterprise will purchase its VPN CPE equipment and manage its deployment and service itself. In other words the enterprise will manage its own WAN. According to IDC this category will continue to see strong growth.

- **CPE based managed VPNs**

In this case the service provider is responsible for running the network as well as the CPE. The demarcation point with the enterprise is at the Ethernet connection to the LAN. The VPN tunnel starts at the CPE. The service provider can guarantee network quality with SLAs covering transit time, maximum drop rates as well as service availability.

- **Network based VPNs**

Here the VPN is created and managed at the backbone and extended to the CPE. The service provider once again provides an SLA covering transit times, drop rates, service availability, security etc. As all the VPN is controlled within the backbone, QoS can be provided with associated SLAs.

33Q: How are VPNs implemented (IPsec, MPLS etc)

A: VPNs can be constructed with a variety of protocols including IPsec, MPLS, PTTP, L2TP...
The two dominant protocols are IPsec and MPLS.
For CPE based VPNs IPsec is the most common protocol with encryption, authentication, data integrity,... For network based VPNs MPLS is increasingly being used instead of IPsec tunnels.

34Q: Why install a VPN

A: Security is becoming increasingly important with the number of attempted security breaches constantly increasing. The cost of not being security conscious can be extremely high as demonstrated by a survey amongst 538 US security professionals:

Average dollar amount lost per organisation per year by type of security breach (Source: Computer Security Institute/ FBI, March 2001)

Financial fraud: $8.0million
Theft of proprietary information: $2.9million
System penetration by outsiders $454 000
Unauthorised insider access: $276 000

The increasing real-time exchange of mission-critical information such as procurement, supply-chain management, sales and customer relationship management, online business transactions, online access to financial institutions etc makes security over the Internet paramount.

35Q: What is this security risk

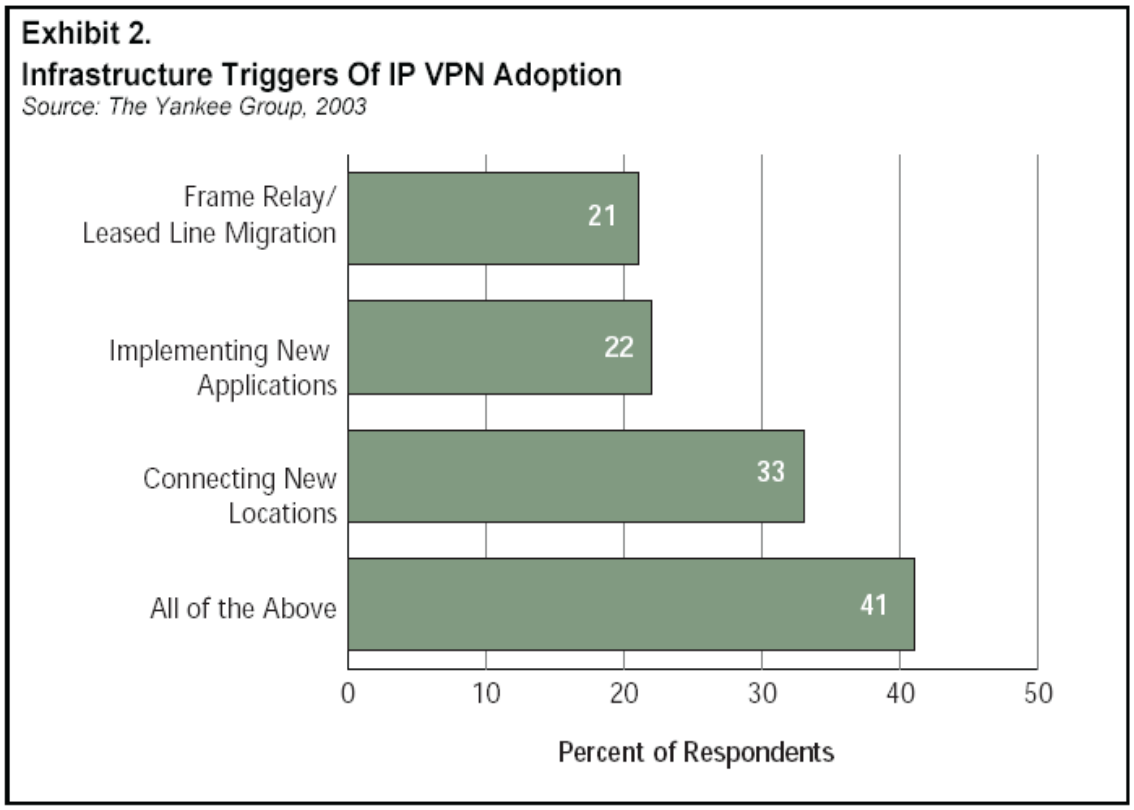
A: Within an IP packet one can find-

- User data:
  Passwords, user IDs, credit card information, and confidential information.
- Information useful to hackers:
  Other headers contain info used by hackers to attack an enterprise's web sites.
- Source and destination addresses:
  By capturing these addresses, a hacker can learn the addresses of target servers and try to set up unauthorised communications with them. A hacker can also learn the addresses of authorised users and use these addresses to impersonate authorised clients.

There are two ways of protecting data. The first is to use private networks between sites - leased lines or Frame Relay - costly and with limited geographic coverage. The second is through the use of VPNs - setting up a private network over the public Internet be it a dial up connection, ISDN, ADSL, satellite etc. In other words VPNs provide a secure and affordable private network over public infrastructure.

36Q: What are the common triggers for adopting VPNs (other than being security conscious)

A:



As the cost of broadband decreases more and more companies are moving away from Frame Relay and leased lines and adopting VPN to secure their public Internet access. Now with the possibility of site-to-site IPsec VPNs over satellite we may see an increase in the migration away from leased lines and Frame Relay not only to ADSL but also to satellite.

Implementing new applications: see next question

Connecting new locations: Every time a company adds a new site it needs to be connected securely to the existing corporate LAN.

37Q: Which type of applications trigger VPN adoption

A: Enterprises are implementing an increasing number of applications which are highly dependant on the exchange of vital information. This information naturally needs to be fully secured triggering a need for VPNs. In addition once a VPN is deployed, enterprises are likely to look at a second wave of IP applications (VoIP, IP telephony, unified messaging, IP conferencing, collaborative working tools -file sharing, Net meeting).

Applications that drive IP VPN Take-up:

Application	What does it do	Typical users	Network implications
Applications server software such as Citrix®	Enables business critical applications to be accessed via any enterprise device	Greatest benefits to remote workers and smaller offices	Requires low latency to ensure effective communications to users
Enterprise resource planning such as SAP® *More and more web enabled*	Used for the majority of business functions: financial, order management, manufacturing processes, planning, and procurement	Different departments throughout an organisation	Required across majority of PCs. Need for more flexible networking, although data information may be centralised/decentralised depending on level of control required
Collaborative suites such as Lotus Notes, Microsoft® Exchange	Main form of communication for most companies	Majority of staff use e-mail, attachments are increasing dramatically	Although e-mail is not mission critical it contributes to a significant proportion of corporate traffic which needs to be managed. MPLS based IP VPNs help prioritise traffic across the network

ABOUT UDCAST

UDcast is a leading software company providing IP broadcast solutions for the delivery of content to a broad range of devices over existing and emerging wireless networks worldwide. UDcast's Mobile TV technology is a key component in the end-to-end solutions from major systems providers including Motorola, Nokia, NSN, Alcatel-Lucent, Tandberg-Ericsson, Cisco-Scientific Atlanta, Harris Broadcasting and others. UDcast's satellite-aware IP appliances are widely deployed at thousands of sites around the globe. The Company was recognized in 2007 as a leading European technology company by the prestigious Red Herring Hot 100 award. The Company maintains its global headquarters in Sophia-Antipolis, France with offices in Algeria, Italy and Spain. For more information, visit www.udcast.com.

CONTACT UDCAST

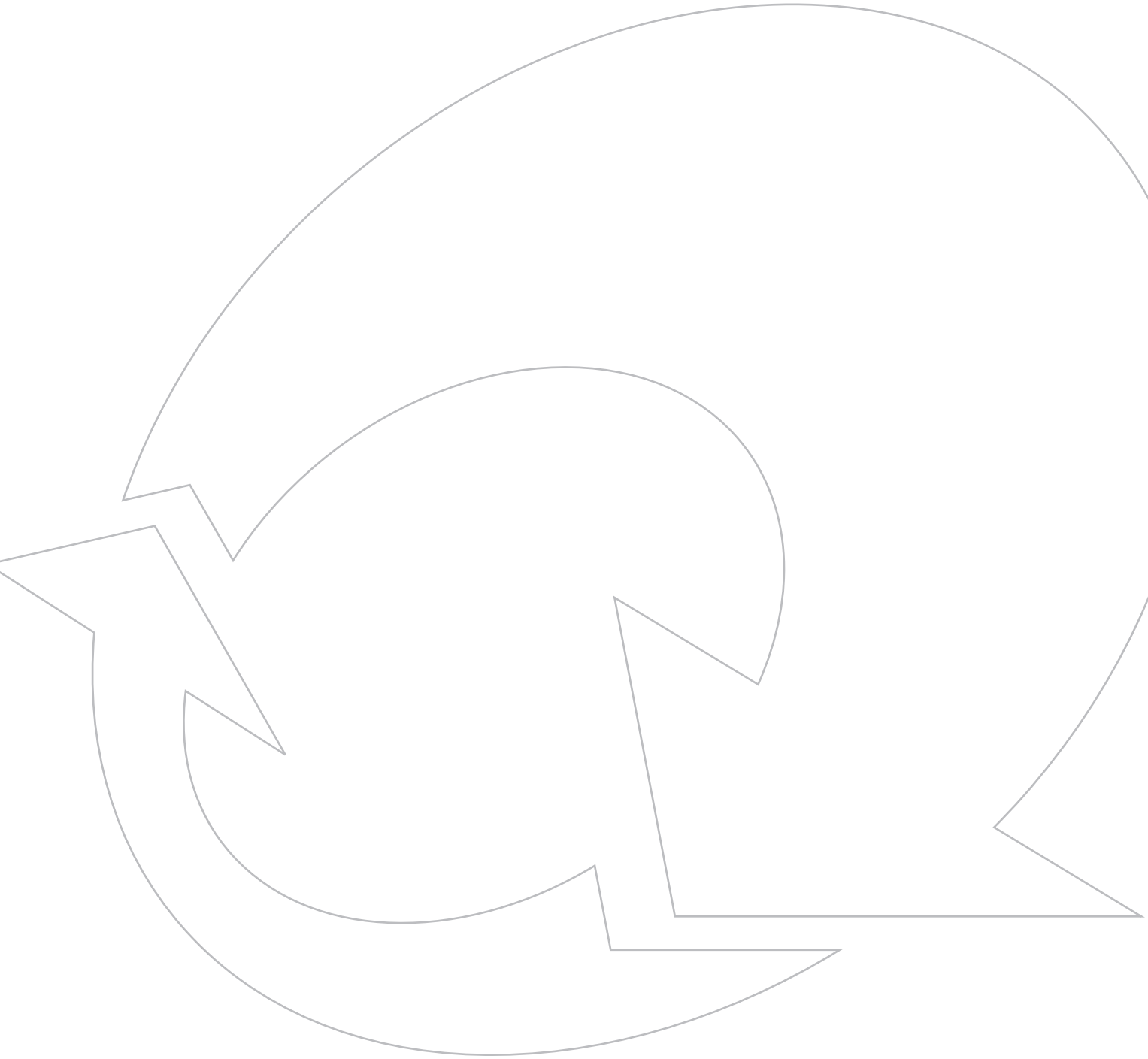
Headquarters:
2455 route des Dolines
BP 355
06906 Sophia Antipolis
Cedex
FRANCE

Tel. +33 (0)493 001 660
Fax. +33 (0)493 001 661

contact@udcast.com

For more information please visit our website:

www.udcast.com



UDcast

IP • BROADCAST • WIRELESS