Case Communications February 2006 Newsletter

February 2006 Newsletter

In this Issue:

Archives

Read the back issues

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe/ Unsubscribe]**

Feedback

Tell us your thoughts

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback/Enquiry]**

Welcome

Welcome to the Case Communications February 2006 Newsletter.

We have been told last week was the most depressing week of the year, so we hope we will lighten your hearts and bring you interesting news and information.

Internet Gambling grows at rapid pace

The increasing availability of Broadband has encouraged more people to have a quick flutter on line, helping Internet gambling to continue growing at a rapid pace.
[More]

New Case Communications Multi-Access Router System emulates BT digital services over Broadband and provides massive cost savings

Case Communications Router System provides massive cost savings by emulating digital services over IP networks.
[More]

Google refuses data request from Bush administration

The Bush administration subpoenaed four major search engines to hand over data in the US Governments efforts to revive anti-porn law that was rejected by the US Supreme courts and its reports three of the four obliged and handed over search data
[More]

How Secure is Voice over IP?

While VOIP is considered 'Hot' by the vendors trying to persuade customers to upgrade their Telephony systems, an area of risk cannot be ignored and should be considered by anyone being pressed to spend their budget on a new IP Telephony system and that is 'Security'
[More]

Technical Tips from Roger's Engine Room

Layer Two Tunnelling Protocol (L2TP) is an extension of the Point-to-Point Tunnelling Protocol (PPTP) used by an Internet service providers (ISP) to enable the operation of a virtual private network (VPN) over the Internet.

[More]

The Death of 0870

0870 Numbers are dead or at least they soon will be, if far-reaching changes to the UK non-geographic numbering system being proposed by Ofcom take effect

[More]

Cisco Security Alerts Serve As VoIP Wake-Up Call

First hackers targetted Microsoft and now Cisco is likely to be the target of Voice Over iP hackers, due to its marketshare

[More]

BT forced to delay QOS over Broadband due to router problems

A recent announcement by BT has stated that Quality of Service over broadband has been delayed due to problems with code on their Cisco routers.

[More]

Case Communications
Voice and data integration
Case, Dowty-Case, Cray, Case Technology Legacy Products
NEWSLETTER
making IP work for you

Case Communications February 2006 Newsletter

February 2006 Newsletter

In this Issue:

Archives

Read the back issues

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe/ Unsubscribe]**

Feedback

Tell us your thoughts

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback/ Enquiry]**

Internet Gambling grows at rapid pace

The increasing availability of Broadband has encouraged more people to have a quick flutter on line, helping Internet gambling to continue growing at a rapid pace.

Internet research company Nielsen//NetRatings, has announced that the online gambling audience in the UK has increased by 45 per cent over this time last year, with 3.2m visiting a gambling site in February. The National Lottery is the most popular gambling site for punters, with over 1.3 million visitors trying their luck from home in February 2005, making it one of the top 40 most visited sites in the UK. William Hill came in second, followed by Partypoker.com.

Nielsen//NetRatings said UK growth has been driven by a range of gambling, betting and online casino sites, and not just by the National Lottery.
Gabrielle Prior, European internet analyst at Nielsen//NetRatings, said: "We expect to see this category continue to grow as advertising attracts consumers and the sites add more and more games and prizes.

"We know from earlier survey work that UK gamblers like the speed and convenience of betting online, and as the broadband boom continues, we expect more people to try online gambling."
Three quarters of UK gamblers were using a high-speed connection, spending 20 minutes online each time. Users on slower connections spent 29 minutes online on average.

Across Europe, more than 14 million people - about 14 per cent of those online from home - visited a gambling or sweepstakes site in February.
Less than 10 Percent of Spanish and Italians log onto gamble, but the research indicated that gambling and weepstake sites were most popular with French and Swedish surfers.
The Nielsen / Net Ratings claim the following top web sites accessed by UK Gamblers fromhome are;

-The National Lottery
- William Hill
- Partypoker.com
- Ladbrokes
- Pacific Poker
- Cyberslotz
- The Gaming Club
- LoopyLotto
- Golden Palace Online Casino
- Vernons

Case Communications February 2006 Newsletter

February 2006 Newsletter

In this Issue:

Archives

Read the back issues

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe/ Unsubscribe]**

Feedback

Tell us your thoughts

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback/ Enquiry]**

New Case Communications Multi-Access Router System emulates BT digital services over Broadband and provides massive cost savings

Following the successful field trials of Case Communications Multi-Access Router the company are pleased to announce that they have officially launched their Multi-Access Router and four port HDLC Over IP card in January 2006.

Business Development manager, Massey Monfared explained, 'legacy technologies such as X.25, Frame Relay and Statistical multiplexers which run over a digital service can use our Multi-Access Router to replace those digital services with a Broadband connection costing a fraction the price of the digital service. The cost savings are tremendous, with payback periods being weeks rather than months.

Product manager Steve Law explained that at the moment the limiting factor is the speed of the broadband connection. Typically the 'uplink speed' of ADSL is 256Kbps, so to gain additional bandwidth the Multi-Access Router provides 'Link Bonding'. This allows the router to bond 2 or 3 DSL links into one high-speed pipe, and to provide much higher bandwidth than standard ADSL.

Of course customers who already have their own IP Network can simply connect the Multi-Access Router into that network and provide a path through their network for the legacy equipment.

Steve went onto explain that the company was now working on Time Division Multiplexing Over broadband, allowing PBX's and virtually any other technology to operate over a broadband connection.
For more information please go to
http://www.casecomms.com/products/routers/ip/mar6000.htm

Case Communications
Voice and data integration
Case, Dowty-Case, Cray, Case Technology Legacy Products
NEWSLETTER
making IP work for you
Case Communications February 2006 Newsletter

Archives

Read the back issues

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe/ Unsubscribe]**

Feedback

Tell us your thoughts

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback/ Enquiry]**

Google refuses data request from Bush administration

The Bush administration subpoenaed four major search engines to hand over data in the US Governments efforts to revive anti-porn law that was rejected by the US Supreme courts and its reports three of the four obliged and handed over search data.Three of four major search engines subpoenaed by the Bush administration have acknowledged that they handed over search data in the government's efforts to revive an anti-porn law that was rejected by the U.S. Supreme Court.

Microsoft Corp., which owns MSN , Yahoo Inc. and America Online said they sent data to the government, but insisted no personal information on users was given to government attorneys. The exception among major search engines was Google Inc., which said it would "vigorously" fight the government's requests.

The government had asked Google, based in Mountain View, California., for a broad amount of data, including a million random Web addresses and records of Google searches over any week, the Associated Press reported. The information came from U.S. Justice Department papers filed Wednesday in a San Jose, Calif., federal court.

Microsoft, Redmond, Wash., Yahoo, Sunnyvale, Calif., and AOL, Dulles, Va. unit of Time Warner Inc., said they provided the data without handing over personal information on subscribers.

"We did comply with their request for data in regards to helping protect children in a way that ensured we also protected the privacy of our customers," MSN spokesman Adam Sohn said in a statement. "We were able to share aggregated query data, not search results, that did not include any personally identifiable information at their request."

A Yahoo spokeswoman said, "In our opinion, this is not a privacy issue."

"We complied on a limited basis and did not provide any personally identifiable information," spokeswoman Mary Osako said in an email.

An AOL spokesman said Friday the company did not provide any information that wasn't already available on the Web.

"We did not comply with the request made in the subpoena," spokesman Andrew Weinstein said. "Instead, we gave the Department of Justice a list of aggregate anonymous search terms that did not include results or any personally identifiable information."

The high court ruled two years ago that the 1998 Child Online Protection Act requiring adults to use access codes or register with a site before receiving adult material violated free speech. The court also ruled that filtering software was adequate to protect children.

Administration lawyers are hoping that the search data will help convince a Pennsylvania federal court that technology is doing an inadequate job, the AP said.

Google said that it was not a party to the government's legal action, and felt the Justice Department was going too far in its requests.

"Google is not a party to this lawsuit and their demand for information overreaches," Nicole Wong, Google associate general counsel, said in a statement. "We had lengthy discussions with them to try to resolve this, but were not able to and we intend to resist their motion

vigorously."

At least one search expert argued that the government could test whether children can get pornography through search engines, without seeking such a huge amount of data from search engines.

Danny Sullivan, editor for Search Engine Watch, said "If you want to measure how much porn is showing up in searches, try searching for it yourself rather than issuing privacy alarm sounding subpoenas. It would certainly be more accurate".

Case Communications February 2006 Newsletter

February 2006 Newsletter

In this Issue:

Archives

Read the back issues

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe/ Unsubscribe]**

Feedback

Tell us your thoughts

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback/ Enquiry]**

How Secure is Voice over IP?

While VOIP is considered 'Hot' by the vendors trying to persuade customers to upgrade their Telephony systems, an area of risk cannot be ignored and should be considered by anyone being pressed to spend their budget on a new IP Telephony system and that is 'Security' Security risks abound in current commercial VoIP solutions, including Denial of Service (DoS) attacks, eavesdropping, and a host of new vectors for intrusion and malware propagation. As it stands now, the benefits of VoIP--cheaper phone bills and converged voice and data applications--may not be worth the risks.

Migrating to VOIP exposes you to serious security risks.
When you migrate voice from a circuit-switched medium to a packet-switched one, you expose that voice traffic to a pair of serious security risks: DoS attacks and eavesdropping.
Unlike traditional uses of IP networks (think downloading files), VoIP is ultrasensitive to latency. Seemingly small delays of 150ms can transform a high-quality call into unintelligible gobbledygook. Jitter, a phenomenon where network-induced delays cause packets to arrive out of sequence, can also be problematic. Losing a single packet isn't a big deal because VoIP packets are small and contain only 12 to 62ms worth of data. But packet loss as low as 1 percent can make a call hard to understand, and a 5 percent loss turns VoIP into a very difficult to use system.
The upshot is that VoIP networks are easy prey for DoS attacks. Network architects should strongly consider the business impact of a simple attack that can completely derail both data applications and phone service in one fell swoop. And note that not all DoS problems are packet-based. A simple power outage will silence a VoIP dial tone as effectively as any black hat.
VoIP also makes it easier for attackers to eavesdrop.

The kind of physical access to a line or a switch required to tap a phone isn't required to tap a VoIP call. Common network sniffing tools, including Ethereal, and tcpdump have plug-ins for both the Session Initiation Protocol (SIP) and H.323. The hilariously named vomit tool (an acronym for Voice Over Misconfigured Internet Telephones, converts tcpdump files into .wav files that can be played on any PC.
To protect against eavesdropping, VoIP users can use SSL/TLS, a VPN, or possibly IPSec. However, packet size, ciphering latency, and a lack of cryptographic engines designed for packet throughput efficiency and ordering affect the trade-off. In its present form, cryptography introduces a severe and unworkable bottleneck in most VoIP systems.

The ease of building exploits.
As with other elements of computer security, software exploits present a real problem for VoIP. Network architects should assume that software exploiters can obtain VoIP software, disassemble it, build exploits, and even make malicious modifications. In addition, a number of academics have uncovered and published SIP

implementation flaws that, when exploited, allow remote code execution, unauthorized access, and software failure, all through malformed packets. Finally, H.323 systems make use of ASN.1 parsing, which has been particularly hard hit by software exploits.
Most VoIP network installations involve many parts, from endpoints to proxies to location servers and registrars. Because many of these nodes include or support dynamically configurable parameters, attackers are presented with a large set of potential targets, just as in a normal data network. Cordless unit systems exacerbate this risk by adding IEEE 802.11 wireless security issues to the mix.
While Voice over IP is an interesting technology, which can offer organisations a wide range of benefits, the security risks are very real. Network managers and architects considering a VOIP Solution must take these risks into account when designing networks for VOIP. If VOIP is important for you, it may be too early for your enterprise to be using VOIP.

Case Communications February 2006 Newsletter

February 2006 Newsletter

In this Issue:

Archives

Read the back issues

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe/ Unsubscribe]**

Feedback

Tell us your thoughts

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback/ Enquiry]**

Technical Tips from Roger's Engine Room

Case Communications Head of development Roger Holden provides a brief overview of L2TP.

Layer Two Tunnelling Protocol (L2TP) is an extension of the Point-to-Point Tunnelling Protocol (PPTP) used by an Internet service providers (ISP) to enable the operation of a virtual private network (VPN) over the Internet.

L2TP merges the best features of two other tunnelling protocols: PPTP from Microsoft and L2F from Cisco Systems. The two main components that make up L2TP are the L2TP Access Concentrator (LAC), which is the device that physically terminates a call and the L2TP Network Server (LNS), which is the device that terminates and possibly authenticates the PPP stream.

The Point to Point Protocol (PPP) defines a means of encapsulation to transmit multiprotocol packets over layer two (L2) point-to-point links. Generally, a user connects to a network access server (NAS) through ISDN, ADSL, dialup POTS or other service and runs PPP over that connection. In this configuration, the L2 and PPP session endpoints are both on the same NAS.

L2TP uses packet-switched network connections to make it possible for the endpoints to be located on different machines. The user has an L2 connection to an access concentrator, which then tunnels individual PPP frames to the NAS, so that the packets can be processed separately from the location of the circuit termination. This means that the connection can terminate at a local circuit concentrator, eliminating possible long-distance charges, among other benefits. From the user's point of view, there is no difference in the operation.

Case Communications
Voice and data integration
Case, Dowty-Case, Cray, Case Technology Legacy Products
NEWSLETTER
making IP work for you
Case Communications February 2006 Newsletter

Archives

Read the back issues

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe/ Unsubscribe]**

Feedback

Tell us your thoughts

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback/ Enquiry]**

The Death of 0870

Contribution by Henry Newrick - Managing Director of Team Telecom (Europe)

0870 Numbers are dead or at least they soon will be, if far-reaching changes to the UK non-geographic numbering system being proposed by Ofcom take effect.Spurred by media campaigns and wide ranging public criticism Ofcom has for some time been looking at the future of non-geographic numbers and in particular 0870. In the process it has consulted widely with industry as well as ordinary members of the public, The result is one of the biggest phone numbering shake-ups seen for a long time in the telecomms industry.When they were first introduced in the UK about 9 years ago, 0870 numbers, costing the same as a BT Long distance call , were called national rate numbers. At that time the standard BT rate for calling long distance within the UK was 6.73p a minute plus VAT. 0870 numbers provided a non-geographic alternative to standard geographic numbers and brought many advantages including the ability to be moved anywhere in the UK.

From a consumers viewpoint there was no disadvantage in calling an 0870 number because the cost was the same regardless of whether they called 0870 or the geographic code.Over the past few years the telecomms marketplace has become increasingly competitive with the result that rates have been dropping steadily so that now its possible to make long distance calls to geographic numbers from one end of the country to the other for under 1p. Yes 0870 numbers have remained unchanged at 6.73p. It has not escaped public attention.

It is also well known among the public that many companies are receiving a share of the call revenue that arises from these higher priced 0870 calls. This in itself wouldn't be so bad if call waiting times were short, but many large companies and government departments with their sophisticated call queuing systems routinely keep callers on hold for up to an hour or more with endless repetitions of that bland message 'Your call is important to us. Please Hold'. In the same way as speed cameras are seen as revenue generators for government, so too are 0870 numbers perceived as revenue generators for many companies and call centres. Under the Ofcom proposals there are to be a number of changes to 0870 which, if adopted will be effective from early 2007. These are:

1. An end to revenue share. No longer will BT be required to share revenue with carriers who supply 0870 numbers to their clients or resellers.

2. 0870 Numbers are to be charged at the same rate as geographic numbers - offered by various carriers. Therefore if a carriers national geographic rate is 2p per minute then it must also charge 2p per minute to call an 0870 number unless the call is preceded by a recorded announcement telling the caller tat the call is cost 7.9p a minute (6.73p plus VAT).The caller will then have the opportunity to cancel the call. The inescapable conclusion to this is

that we are likely to see the demise of 0870 numbers as companies move either back to geographic numbers or to cheaper non-geographic alternatives such as 0845 (local call) which Ofcom has said will remain untouched for at least 2 years. One of the principal reasons for leaving 0845 untouched at this stage is that many ISP's use 0845 numbers for dial up internet access, and the small revenue share they receive is critical to maintaining their business models.

A further reason that 0870 numbers are likely to disappear is that many companies may move to take up 0844 numbers where calls cost just 4 or 5p a minute at all times. With 0844 numbers a small revenue share is still likely. However, if this number range came into widespread use, then in due course there is the possibility of unfavourable media attention - especially once revenue sharing became known.
While the biggest impact of the recent OFCOM review is clearly on 0870 numbers, other number ranges are also referred to. As previously note d0845 numbers are to remain untouched for two years at which point they too will be reviewed. It is proposed that 0871 calls come under the jurisdiction of ICSTIS the agency responsible for policing premium rate 09 numbers. Adult calls made on 0871 numbers (where revenue share can be up to 6p per minute) are likely to be moved to premium rate 09 numbers.
Severely affected will be companies that have invested heavily in building their brand or business around a particular phone number. Apart from the obvious benefits to the consumer in terms of lower call charges, printers and sign writers will also do well for the next few years as businesses set about changing their stationery and signage.
Henry Newrick is the Managing Director of Team Telecom (Europe) Ltd, a company specialising in Sourcing non geographic numbers for clients throughout the UK and overseas.

Henry can be reached on henry.newrick@telecomsolutions.co.uk

or 0845 222 0033

Case Communications February 2006 Newsletter

February 2006 Newsletter

In this Issue:

Archives

Read the back issues

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe/ Unsubscribe]**

Feedback

Tell us your thoughts

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback/ Enquiry]**

Cisco Security Alerts Serve As VoIP Wake-Up Call

First hackers targetted Microsoft and now Cisco is likely to be the target of Voice Over iP hackers, due to its marketshare. A Synergy Research Group Synergy issues a report last week which indicated that Cisco's IP telephony technology accounted for 18% of the office-telephone-system market over the past year, with more than 30,000 customers and 7 million phones sold since it entered the market six years ago.

Another danger lies in IT staff inexperience: Voice over IP hasn't been much of a target for hackers, and gaining the security know-how to protect those networks may not be top of mind during deployments, says chief technology officer Ofir Arkin of network-management company Insightix Ltd. and a board member of the Voice over IP Security Alliance, a collection of networking and security vendors, researchers, and academics. "To knock off a voice-over-IP infrastructure is easier than traditional calls," he adds. "We all need to take these as very serious things, because if you want to dial 911, and you can't, this is life-threatening."Most VoIP attacks to date have been against specific phones and directed at stealing service or altering configurations to make the phones act strangely. Last July, Internet Security Systems Inc.'s X-Force research team posted an alert that Cisco CallManager included bugs that attackers could exploit to create what's known as a heap overflow to crash a system or gain unauthorized access. In 2002, vulnerabilities emerged in several Pingtel Corp. Session Initiation Protocol-based phones that allowed denial-of-service attacks, manipulation of SIP signaling, and unauthorized remote access to phones.Be PreparedBusinesses can help protect their VoIP networks by segmenting their voice and data traffic using a virtual LAN, says Kevin Flynn, senior manager for Cisco IP communications and wireless security technology marketing. "If an attack occurs on the data network and there's good segmentation, the voice traffic will be fine," he says. The problem with a virtual LAN, however, is that virtual segmentation won't protect data and voice traffic if the networking equipment itself is attacked and taken down. These concerns are only beginning to be felt among businesses using VoIP.

Case Communications February 2006 Newsletter

February 2006 Newsletter

In this Issue:

Archives

Read the back issues

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe/ Unsubscribe]**

Feedback

Tell us your thoughts

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback/ Enquiry]**

BT forced to delay QOS over Broadband due to router problems

A recent announcement by BT has stated that Quality of Service over broadband has been delayed due to problems with code on their Cisco routers.

The implementation of the Differentiated Services Code Point (DSCP) Class of Service (CoS) capability on Digital Subscriber Line (DSL) accesses to BT's UK IPVPN products has been delayed owing to non availability of a robust router code to support the feature on our network.

We are well aware of the importance of this particular development and our Development Team has been working hard to resolve the issue and put in place this additional capability. The new launch date is now expected to be mid May 06, however we are trying hard to bring this forward if possible.

Some competitors currently offering a form of CoS over DSL with Cisco routers will be experiencing the functionality and reliability problems we have delayed launch to avoid. Whilst there are other Cisco routers available that do not present this problem, these are not in line with our requirements