## Case Communications June 2007 Newsletter

Greetings,

Welcome to the Case Communications June Newsletter

This month we announce the launch of our new Network Management system review more security threats at Voice Over IP, and look at Linux in the embedded marketplace.

We also look at how IPV6 is to be supplied and take another look at SPAM.

We also look at additional protection for customers of Local Loop Unbundlers and at the possible merger of the CM with the British Computer Society.

### Linux is winning the race in the embedded marketplace but only has 2% of the PC market

While a lot of people have heard of Linux, to date it has not made much of an impact within the marketplace, and hasn't made a dent in **Microsoft** (nasdaq: MSFT - news - people )'s desktop PC monopoly, grabbing less than 2% of the market versus 95% for Windows.

**More**

### Linux has nailed Sun Microsystems. Could Cisco be next?

Cheap machines running Intel chips and low-cost Linux software have gutted server sales at **Sun Microsystems** (nasdaq: SUNW - news - people ) and Silicon Graphics. Now upstarts are doing the same thing in networking gear. Their target: fat and happy **Cisco** (nasdaq: CSCO - news - people ), the king of networking.

**More**

### Case Communications launch New Network Management Platform

**June 2007 – High Wycombe -**Case Communications is proud to announce the launch of its new Network Management Software called 'CaseView'England

**More**

**Case Communications June 2007 Newsletter**

**In this Issue:**

Linux is winning the race in the embedded marketplace but only has 2% of the PC market
Linux has nailed Sun Microsystems. Could Cisco be next?
Case Communications launch New Network Management Platform
Extra Protection for customers of Local Loop Unbundlers
Threats to watch out for if your considering Voip – An update to our regular Voip security watch
IPV6 to be allocated to ISP's only not to business.
An Update on the battle against SPAM
CMA theTelecoms body may merge with the British Computer Society

## Extra Protection for customers of Local Loop Unbundlers

Ofcom the Telecomms industry watchdog has announced that customers of local loop unbundlers will get extra protection.

**More**

## Threats to watch out for if your considering Voip – An update to our regular Voip security watch

Voice Over IP has been hailed as the panacea for at least the last ten years but just does not seem to have taken off, until the last couple of years when it seems no longer to just be a topic of conversation but is now actually being implemented.

**More**

## IPV6 to be allocated to ISP's only not to business.

The director of IT at the UK internet registrar, Nominet has said that, European businesses are being held back from migrating to IP version 6 due to the way IP addresses are being allocated.

**More**

## An Update on the battle against SPAM

If our readers are anything like most people, out of all the mails we receive a large percentage are SPAM and if anything its getting worse, particularly for web masters who have to check the organisations SPAM boxes to make sure a company's SPAM filter has not marked a genuine enquiry as SPAM and dumped it.

**More**

## CMA theTelecoms body may merge with the British Computer Society

The Communications Management Association (CMA) which is the only representative organisation for UK telecoms professionals is set to lose its status as an independent body.

**More**

**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:

Case Communications June 2007 Newsletter

## Linux is winning the race in the embedded marketplace but only has 2% of the PC market

Most PC makers still add Microsoft software by default. But Linux is catching on like crazy in other devices, powering the sleek new Motorola A1200 Ming smart phone, the **Sony** (nyse: SNE - news - people ) Mylo handheld computer, Linksys wireless routers and **TiVo** (nasdaq: TIVO - news - people ) digital video recorders.

and Case Communications in England have been working with Linux for years, to produce products that outperform the big name proprietary brands and also save their customers up to 75% .That's a hard deal to beat.

### Case Communications June 2007 Newsletter

**In this Issue:**

Linux is winning the race in the embedded marketplace but only has 2% of the PC market
Linux has nailed Sun Microsystems. Could Cisco be next?
Case Communications launch New Network Management Platform
Extra Protection for customers of Local Loop Unbundlers
Threats to watch out for if your considering Voip – An update to our regular Voip security watch
IPV6 to be allocated to ISP's only not to business.
An Update on the battle against SPAM
CMA theTelecoms body may merge with the British Computer Society

### 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:

Case Communications June 2007 Newsletter

## Linux has nailed Sun Microsystems. Could Cisco be next?

"The only question that remains is how much time will pass before network engineers stop paying extra for a brand like Cisco and look at alternatives that provide a lot more for less," says J.C. Utter, founder and chief of ImageStream, of Plymouth, Ind., which charges less than half Cisco's prices and has sold 30,000 Linux-based devices to customers in 75 countries.

Cisco's prices are high in part because, like Sun, Cisco uses custom chips and custom-designed software. Cisco also pockets 65% gross margins. In the Cheap Revolution you might as well paint a target on your forehead. A Cisco spokeswoman says its custom chips and software offer a competitive advantage, and she adds that open-source alternatives have existed for a decade without harming Cisco. The San Jose, Calif. giant, with annual sales at $28 billion, holds almost 90% of the enterprise routing market, says research firm Dell'Oro Group. In telecom Cisco's share is at 56%.

Yet at the fringes some commodity newcomers are gaining traction. In the U.S. Vyatta and Lok Technology are pushing new network routers that cost a fraction of what Cisco charges. "The router business has become commoditised," says Simon Lok, founder of Lok Technology, also in San Jose.

In the telecom carrier space Cisco is under attack from a different pack of new barbarians. Cirpack, a unit of Thomson in France, generates $30 million a year selling Linux-based switches. Starting with a single four-processor IBM Linux server that costs only $10,000, Cirpack adds its own software and charges up to $2 million for a switch that can handle 250,000 phone calls simultaneously. (Traditional switches with equivalent power cost $10 million and take up 500 square meters of floor space.) Carriers in Europe are using Cirpack's cheap switches to offer "triple play" service--phone, Internet and TV--for $40 a month.

Fueling the disruption is **Intel** (nasdaq: INTC - news - people ), which has invested in outfits that build open-source switching gear and push Linux-based solutions. IBM is pushing Intel-based "blade" servers as a foundation for telecom gear. In June San Francisco venture firm Walden International vowed to invest $100 million in firms building new switches and routers on IBM blades

**Case Communications June 2007 Newsletter**

**In this Issue:**

Linux is winning the race in the embedded marketplace but only has 2% of the PC market
Linux has nailed Sun Microsystems. Could Cisco be next?
Case Communications launch New Network Management Platform
Extra Protection for customers of Local Loop Unbundlers
Threats to watch out for if your considering Voip – An update to our regular Voip security watch
IPV6 to be allocated to ISP's only not to business.
An Update on the battle against SPAM
CMA theTelecoms body may merge with the British Computer Society

## 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:

Case Communications June 2007 Newsletter

## Case Communications launch New Network Management Platform

**June 2007 – High Wycombe -**Case Communications is proud to announce the launch of its new Network Management Software called 'CaseView'England

Designed to be highly flexible and very cost effective 'CaseView' contains MIBS for Case Communications own products, and a wide variety of 3rd party products, such as Cisco, 3-Com and other less well known vendors products.

There are two versions of Caseview.

### Workgroup Edition

This is the entry-level single user version for managing small to medium sized networks. All components run on a single system, and support one user. The map database is limited to 1,000 objects.

### Enterprise Edition

The Enterprise edition is a base system for a scalable multi-user environment. The Enterprise Edition includes SNMPc Server Licence, One remote Console Licence and one remote Poller Licence. The system can be used simultaneously by two users, one at the server and one at another Remote Console system. The enterprise edition also includes a remote Access extension. It is a licence only option which allows an unlimited number of Remote Console users and Remote Polling agents. It also provides JAVA Console Support.

CaseView supports SNMP V1 and V2C and also SNMP v3 which is a secure SNMP Agent protocol, that provides authentication and privacy (encryption).

Caseview has the usual Network Management tools such as full graphical displays, the ability to up and download device configuration data, and a reactive and pro-active status reporting system, with all events and performance data logged in the system
In the event of an alarm SMS messages or e-mails can be sent to network engineers alerting them to the problem.

Management reporting allows the generation of management

**Case Communications June 2007 Newsletter**

**In this Issue:**

Linux is winning the race in the embedded marketplace but only has 2% of the PC market
Linux has nailed Sun Microsystems. Could Cisco be next?
Case Communications launch New Network Management Platform
Extra Protection for customers of Local Loop Unbundlers
Threats to watch out for if your considering Voip – An update to our regular Voip security watch
IPV6 to be allocated to ISP's only not to business.
An Update on the battle against SPAM
CMA theTelecoms body may merge with the British Computer Society

reports on network composition, inventory management and status etc.

Simon Harmonsworth Director of the Case Communications Network Management Development team said 'A Network management system is no longer about just managing your own products, its vital to manage those, but to also provide management of other vendors products, and CaseView just does that' .

For more information on CaseView please look on the Case Communications web site or contact your Case Communications account manager or reseller.

**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:

Case Communications June 2007 Newsletter

## Extra Protection for customers of Local Loop Unbundlers

Ofcom the Telecomms industry watchdog has announced that customers of local loop unbundlers will get extra protection. From this week, consumers who get their voice or broadband from LLU companies can expect the same protection as customers of traditional fixed-line voice providers.

Unbundlers will now need to comply with a code of practice that prevents activities such as 'slamming' - transferring a customer from one provider to another without their knowledge.

According to Ofcom, there have been 1,200 complaints regarding telecoms misselling in the first three months of this year. Since the code of practice was introduced in 2005, Ofcom has opened 11 misselling investigations into telecoms providers including the Post Office and Tesco.

Ofcom is also looking at the issue of misselling and switching providers across the whole range of communicaitons medium, from Mobile to cable, to see if a standard approach to switching could be adopted which covers all technologies, and provides better protection for customers.

### Case Communications June 2007 Newsletter

**In this Issue:**

Linux is winning the race in the embedded marketplace but only has 2% of the PC market
Linux has nailed Sun Microsystems. Could Cisco be next?
Case Communications launch New Network Management Platform
Extra Protection for customers of Local Loop Unbundlers
Threats to watch out for if your considering Voip – An update to our regular Voip security watch
IPV6 to be allocated to ISP's only not to business.
An Update on the battle against SPAM
CMA theTelecoms body may merge with the British Computer Society

### 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**

Case Communications June 2007 Newsletter

## Threats to watch out for if your considering Voip – An update to our regular Voip security watch

Case Communications Newsletters have looks at IP Telephony and Voice Over IP pitfalls on a regular basis, and we thought it wastime to look at the latest worries

According to market researchers AMI Partners, worldwide SME spending on VoIP solutions topped £1.5bn in 2006, up 26 per cent over 2005, with small and medium-sized enterprises proving the keanest to move to the new technology. AMI predicts that most SMEs will choose to move to VoIP over the next five years.
The bulk of VoIP calls currently being made are still not properly secured and this is leaving businesses open to attack, and many organisations overlook the security implications in their rush to adopt the technology.
As increasing numbers of users adopt VoIP, more hackers and criminals will be enticed to capitalise on the weaknesses in the technology. This short article looks at the major threats businesses of any size face when adopting VoIP.

### 'Normal Data' attacks will also affect voice.

The benefit of converged networks is that voice over IP is 'just' another application running on the data network, and saving carriers a huge amount in not having two infrastctures to support, and the enterprise significant amounts by beign bale to use the same dat apaths they use for their IT systems, for voice.
Unfortunately from a security viewpoint, this means that it will also be affected by all the attacks that cripple data networks, even if they are not deliberately targeting voice over IP.

### Denial of Service (DOS) attacks

The most significant specific threat to VoIP is denial of service (DoS) because this can bring a data network to its knees and shut down all applications running on it - including VoIP. This means your employees could be without phone service until the network is back up.

### Vulnerabilities within Asterisk

Security bugs that plague data applications will also affect VoIP users. For instance, security company Core Security Technologies discovered a vulnerability in the popularVoIP Asterisk PBX application which runs under Linx and is used as the core of a large number of commercial PBX products. The Asterisk PBX

**Case Communications June 2007 Newsletter**

**In this Issue:**

Linux is winning the race in the embedded marketplace but only has 2% of the PC market
Linux has nailed Sun Microsystems. Could Cisco be next?
Case Communications launch New Network Management Platform
Extra Protection for customers of Local Loop Unbundlers
Threats to watch out for if your considering Voip – An update to our regular Voip security watch
IPV6 to be allocated to ISP's only not to business.
An Update on the battle against SPAM
CMA theTelecoms body may merge with the British Computer Society

allowed hackers to create buffer overflows for a denial of service attack. Any bugs in similar apps you are using could make your network vulnerable to malicious users.

**SIP vulnerabilities**

The increasing adoption of session initiation protocol (SIP) for VoIP is expected to open up a whole new front in the security war. SIP is a relatively new protocol which offers little inherent security. Some of its characteristics also leave it vulnerable to hackers, such as using text for encoding and SIP extensions that can create security holes.

Examples of hacks for SIP include registration hijacking, which allows a hacker to intercept incoming calls and reroute them; message tampering, which allows a hacker to modify data packets travelling between SIP addresses; and session tear-down, which allows a hacker to terminate calls or carry out a VoIP-targeted DoS attack by flooding the system with shutdown requests.

**Spam Over Internet Telephony (SPIT)**

This threat is the voice incarnation of SPAMs in e-mail and stands for 'spam over internet telephony'. Spammers are already targeting users of all IM systems with ‘spim’ (spam over instant messaging) and the fact many accounts include demographic information such as user location or age helps them target users.

Up to now there have not been a great many instances of VoIP spam but there is great potential for it to become a major problem. Spit could be generated in a similar way to email spam with botnets targeting millions of VoIP users from compromised machines.

The real-time nature of voice calls will make dealing with spit much more challenging than email spam. While emails can sit on a server for an extra hour to go through a spam filter, calls must be routed to the recipient instantly.

An innovative solution has been recently demonstrated by Japanese tech company NEC. A technology it has dubbed VoIP Seal defends against spit using a range of techniques including a Turing test. The technology claims to be able to correctly identify 99 per cent of spit by looking at communications patterns and stopping the call before it is connected to the user.

**Vishing**

Just as in the email world, tipping dodgy stock and selling Viagra is only part of spit, it can also be used to commit serious fraud. Vishing uses telephony to glean information such as account details directly from users.

One of the first reported cases affected the phishers' favourite target PayPal. The scam was a true multi-channel attack. Victims first received an email purporting to come from PayPal which asked them to verify their credit card details on a phone line. Those who called the number were then asked to enter their

credit card number using the telephone. Once the credit card number had been entered, the fraudsters were free to siphon money from their victim's account.

Scams like this are not just a danger for voice over IP users but the much lower cost of making VoIP calls will make them much more popular than they would be with standard phone systems. Because users still trust the telephone more than the web, criminals are able to make themselves very convincing by spoofing the correct telephone numbers. And through spamming techniques they can call thousands of people for very little outlay.

**VoIP hacking**

Like any IP system, a VoIP network is at serious risk of being hacked. This can affect anyone who uses VoIP - from the home user through enterprises to service providers. A US fraud case in 2006 heard how hackers broke into VoIP service providers' systems using the common 'brute force' hack to identify holes in their networks.

VoIP service providers use a prefix on the IP packets to identify their own calls, so the hackers sent millions of fake test calls to find out which prefixes were admitted to the network. Once they had determined the prefix they were able to send calls through those service providers' networks, and sell these minutes on through two front companies.

**Man in the middle attacks to Eavesdrop**

Hackers can eavesdrop on media streams and intercept VoIP packets to obtain sensitive information by reassembling the packets into speech.

One way for hackers to do this is through a man-in-the-middle attack, where a third party spoofs the MAC addresses of the two speaking parties, to force the IP packets to flow through the hackers' system.

While eavesdropping on telephone conversations is not just a risk for VoIP conversations, the nature of IP networks makes access to the phone conversations much easier. Eavesdroppers will no longer need to physically put a tap into a phone line, they can simply get access from a laptop loaded with the right tools connected to the internet. Other compromises are also possible with VoIP, such as intercepting a genuine call to a bank and rerouting it to a bogus bank teller.

Although extensive, all of these threats can be prevented by proper security procedures and technology.

**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:

Case Communications June 2007 Newsletter

## IPV6 to be allocated to ISP's only not to business.

The director of IT at the UK internet registrar, Nominet has said that, European businesses are being held back from migrating to IP version 6 due to the way IP addresses are being allocated. IPv6 will succeed the current version, IPv4, and because it uses a longer string of numbers for identification it promises many more IP addresses than are possible in IPv4. ( Its said that every grain of sand on this planet can be given an IP address with IP V6).

The American Registry for Internet Numbers (ARIN) argues that because only 19 per cent of IPv4 address space remains available - and it is running out faster than expected - it was, for the first time, "compelled to advise the internet community that migration to IPv6 is necessary for any applications that require ongoing availability of contiguous IP number resources".

(We would not be facing this dilema if the world had chosen to adopt the more sophisticated OSI (Open Systems Interconnection) protocol rather than the simpler IP back in the 1990's. OSI was technically superior and for a while it seemed sense would prevail as Governments Worldwide formed GOSIP (Government Open System Interconnection Profile) which in effect stated that Goverments would only purchase IT equipment which conformed to OSI.However the complexitiy of OSI, and then the fact IP was given away free with Unix machines, meant IP became dominant, and todays limitations are a result of that decision.

Dave Passmore, research director at Burton Group, said: "This issue will significantly affect all enterprise organisations with applications that require the ongoing availability of public IP addresses."
However, concerns have been raised about the way IPv6 addresses are currently allocated by RIPE, (the European equivalent of ARIN), and it appears that this situation will not change for at least four months.

Nominet's IT director Jay Daley indicated that, unlike ARIN, RIPE was allowing only ISPs access to IPv6 addresses, leaving enterprises out in the cold.
He said: "We, for example, have our own IPv4 address allocation from RIPE but we are unable to get an IPv6 allocation because their current allocation policy means we must be an ISP who

**Case Communications June 2007 Newsletter**

**In this Issue:**

Linux is winning the race in the embedded marketplace but only has 2% of the PC market
Linux has nailed Sun Microsystems. Could Cisco be next?
Case Communications launch New Network Management Platform
Extra Protection for customers of Local Loop Unbundlers
Threats to watch out for if your considering Voip – An update to our regular Voip security watch
IPV6 to be allocated to ISP's only not to business.
An Update on the battle against SPAM
CMA theTelecoms body may merge with the British Computer Society

gives addresses out to at least 200 customers. We don't give addresses to customers - we are an enterprise, in the same way that a large enterprise might want their own address space for local management of internet connectivity."

Tim Chown, systems administrator for the University of Southampton's school of electronics and computer science and a member of the UK's IPv6 taskforce, agreed. He said that although the bulk of the hardware and software needed for IPv6 was already available, companies were currently unable to avoid being tied to an ISP when migrating to IPv6.

**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:

Case Communications June 2007 Newsletter

## An Update on the battle against SPAM

If our readers are anything typical of most business users of e-mail, out of all the mails we receive a large percentage are SPAM and if anything its getting worse, particularly for web masters who have to check the organisations SPAM boxes to make sure a company's SPAM filter has not marked a genuine enquiry as SPAM and dumped it.

While we still have the plethora of SPAMS offering Viagra and medication, SPAM e-mails have developed further, but you will be pleased to know it is not a new problem. We have had junk mail for as long as we have had letterboxes, and that is exactly what spam is: junk mail, although unlike junk mail spam has got cleverer in the way it tries to trap you. Whereas the junk that falls through your letterbox rarely does more than try to sell you another credit card or fast food, the kind of junk that we see in our inbox has got way more sophisticated, although apparently the naming of these things has taken a backward step.

### Pump-and-dump

"Pump-and-dump is a type of spam," said Mark Sunner from Messagelabs, "and it's one of the most prevalent things that's going on at the moment. Essentially the bad guys are sending out, in huge volumes, messages that purport to be a hot stock tip.

"Ironically, because enough people fall for this, we can see, by tracking these shares, that they do elevate very slightly.

"It's not a huge bump but the bad guys will have taken a slice of these penny shares and then they get out quickly, usually within a 24-hour period, as the price rises. Then people are left with something which is going to be worthless."

So how do they come up with the e-mail addresses?

"Brute force, in e-mail terms," explained Mr Sumner. "Someone can create an e-mail account called, say, abcd1234@. It's not a name, so how would anyone guess that?" And yet it still starts receiving spam.

"The answer is that there are many programs out there that are working their way through all permutations of letters and numbers, but starting with names; for instance things like asmith@, bsmith@, csmith@ etc, will be at the top of the algorithms that are targeting a particular domain.

"They have no concept of who might be behind that address, but by performing a brute force attack starting with real names there's a high likelihood that they're going to get real addresses."

**Case Communications June 2007 Newsletter**

**In this Issue:**

Linux is winning the race in the embedded marketplace but only has 2% of the PC market
Linux has nailed Sun Microsystems. Could Cisco be next?
Case Communications launch New Network Management Platform
Extra Protection for customers of Local Loop Unbundlers
Threats to watch out for if your considering Voip – An update to our regular Voip security watch
IPV6 to be allocated to ISP's only not to business.
An Update on the battle against SPAM
CMA theTelecoms body may merge with the British Computer Society

**Open invitation**

Did you know you were not supposed to even open up a spam e-mail? "When you receive a spam message in your Inbox," said Phil Watts of SoftScan, "my advice to you is please don't click on it. "The double click is like opening a Word document, which means it opens that document into your Inbox, releases the software that's inside it, and it inserts itself into your directory or wherever it needs to go. And it could be sending out messages to your e-mail list, for example."

But it gets worse, as Thierry Karsenti from CheckPoint revealed. "By opening the e-mail you're automatically downloading images or whatever makes the e-mail attractive to you, but by doing that you give the spammer the information that you're actually reading the e-mail."

**Choosing an e-mail account**

Chris Long and Dan Simmons from the BBC carried out some research and thought they would try an experiment to see how much unwanted e-mail they would attract simply by setting up some e-mail accounts. Would spam simply flood in? Would it make much of difference who they signed up with, or what they signed up for?

First of all they set up three e-mail accounts with AOL.

Number one was their secret account - not to be used or disclosed by anyone. Number two - was set up for social networking. They registered on MySpace, Bebo, and a dating site called FriendFinder.

Finally, number three was used to sign up for just about anything they could think of: free TV and film sites, national online newspapers, beauty products, voucher schemes, all sorts.

To make sure they were not being biased we set up similar free accounts with MSN's Hotmail, and Google's mail service.

With each account they accepted the provider's default spam settings. For each site they signed up to, if they were given an option to avoid third party e-mails, they took it.

**Experiment results**

After seven days they returned to our inboxes.

Their secret accounts, the ones they had just set up and kept completely hush about, had been untouched by spammers. Each of the number one accounts had just one e-mail in - welcoming them to that service. So far so good.

The number two accounts, used for social networking sites, attracted more e-mails - mainly to verify their registration. But there was nothing here they did not ask for. No third parties have been in touch. So no spam so far.

And so to the sign-up-to-anything accounts. They chose six sites at random and used their number three e-mail addresses to register. Would they attract spam inside a week of being used?

AOL was clean. There was nothing in the spam folder and all 10 messages have come from their six sites. Half of them come from a site they signed up to called Secret Satellite, all pushing the

company's web TV service.

Their Hotmail account did not attract uninvited e-mails either, but it decided to treat two of Secret Satellites' messages as spam. They appear to come from Oliver, adding a personal touch to the site's repetitive pitch. Hotmail also decided that the e-mail from beautyexpert.co.uk confirming their registration was junk too.

Google seemed more cut-throat about what constitutes spam. Again there was nothing from strangers - but this time every e-mail from Secret Satellite went into the spam bin.

Which begs the question: are repeated e-mails from a service you have signed up for spam? You will have to decide, and all of these services "learn" what you think is spam depending on where you file messages.

Certainly in the short term they were not deluged with unsolicited e-mails simply because they set up e-mail accounts. Spam is a little more complicated than that.

Of course their experiment is only seven days in. But they plan to return to their inboxes to find out more the next time Click tackles spam.

We acknowledge and thank the BBC for information contained within this story, taken from an original story from BBC NEWS:

Published: 2007/04/27 14:42:44 GMT

© BBC MMVII

**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:

Case Communications June 2007 Newsletter

## CMA theTelecoms body may merge with the British Computer Society

The Communications Management Association (CMA) which is the only representative organisation for UK telecoms professionals is set to lose its status as an independent body.

The (CMA) will, pending approval by its members, be swallowed by the British Computer Society (BCS), a much larger organisation which represents UK IT professionals.

The organisations argue the proposal is essential because IT and telecoms technology have converged and so there is no need for two separate user organisations.

If the proposal is passed, it will mean the end of the CMA's 49-year history as an independent organisation.

The CMA grew in popularity, from its establishment in the 1950s until the height of the dot-com boom, as the use of telecommunications rocketed.

But in 2001 its fortunes took a turn for the worse as funding drained from the industry. As a result, its annual exhibition and conference in Brighton collapsed and its membership base shrank rapidly.

Case Communications attended the last TMA exhibition in Brighton as an exhibitor and could see the writing on the wall. There were few visitors and many empy stands, and shows such as 'BT's Broadband show' due to start at 3pm had no visitors and just a handleful of BT staff were seen sleeping in their audiences seats.

Acceptance of the new proposal, which will be presented to members at the CMA's AGM in July, would see the association become a subsidiary of the BCS.

Both organisations would continue to sign members separately - with members of one organisation being granted affiliate membership of the other.

The BCS will establish a communications forum, which will be run by the CMA. The CMA will retain its headquarters in Leatherhead and its chief executive Glenn Powell, but its direction will be driven by a new strategic board.

### Case Communications June 2007 Newsletter

**In this Issue:**

Linux is winning the race in the embedded marketplace but only has 2% of the PC market
Linux has nailed Sun Microsystems. Could Cisco be next?
Case Communications launch New Network Management Platform
Extra Protection for customers of Local Loop Unbundlers
Threats to watch out for if your considering Voip – An update to our regular Voip security watch
IPV6 to be allocated to ISP's only not to business.
An Update on the battle against SPAM
CMA theTelecoms body may merge with the British Computer Society

### 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: