Case, Dowty-Case, Cray, Case Technology Legacy Products

case communications

June NEWSLETTER

LINUX

Specialists in high-speed and rugged access solutions

Case June 2010 Newsletter

Greetings,

Welcome to Case Communications June 2010 newsletter. In this edition we are pleased to announce the launch of our new Samurai 1+Mpps modular router and our Medalist range of Layer 3 Ethernet switches with performance levels up to 131 Million Packets per second, while being priced at realistic levels.

....

Case Communications launch Medalist layer 3 switches with throughput up to 131 Mpps.

Case Communications are please to announce the launch of their Medalist high performance Layer 3 Ethernet switches, with 10Gbps ports and performance levels up to 131 Million packets per second.

More

....

A British scientist says he is the first man in the world to become infected with a computer virus.

Dr Mark Gasson from the University of Reading contaminated a computer chip which was then inserted into his hand.

The device, which enables him to pass through security doors and activate his mobile phone, is a sophisticated version of ID chips used to tag pets.

More

....

Case Communications launch their new 1+ Mpps Samurai Modular routers

The Samurai Express is Case Communications 2U modular router for border, edge and colocation routing and VoiP applications.

More

....

'Hospital risk' from radio tags

Lifesaving equipment in hospitals may be switched off by radio-frequency devices used to track people and machines, Dutch

scientists claim

More

....

Few ISP's supporting IPv6

'IPv6' is version six of the 'Internet Protocol' which has been available since 1998 however it is currently only supported by a very small number of niche broadband service providers.

Courtsey of 'Think Broadband'

More

....

Mobile net 'heading for data jam'

Experts are warning that the number of people accessing the net on mobile phones could soon outstrip the capacity of networks.

More

....

'Shady' porn site practices put visitors at risk

Study suggested that visitors to porn sites are at serious risk of being exploited by cyber criminals.

More

....

Case June 2010 Newsletter

Case Communications launch Medalist layer 3 switches with throughput up to 131 Mpps.

June 2010

Case Communications have announced the launch of their Medalist range of carrier / ISP grade Ethernet switches. The Medalist switches are layer 3 switches with high levels of performance, offer a full range of fetaures and functionality and are competitively priced.

The Medalist Series Ethernet switches deliver carrier grade features and performance at a competitive price that will appeal to carriers, service providers and businesses with demanding data centres. The Medalist rnage supports comprehensive QoS, enhanced VLAN functions (VLAN VPN, Voice VLAN, Stacking VLAN), classified bandwidth control, multi-link aggregaiton, intelligent security control, which fullfills the network requirements for bandwidth control, multi link aggregation, intelligent security control, which fullfill the network requirements for Gigabit to the desk top, storage area network links, server group access and MAN high speed security access.

There are four switches in the Case Communications Medalist Ethernet switch range

1. The MS-344-GE4GC

- **Forwarding rate:** 131 Mpps
- **Switching Capability**: 176 Gbps
- **10/100/1000 TX ports:** 44
- **10 Gigabit ports:** 2 XFP Expansion slots
- **10 Gigabit ports:** 2 stack ports
- **Switching:** Layer 3

More information on MS-344-GE4GC

2. The MS-320GE-4GC

- **Forwarding rate:** 96 Mpps
- **Switching Capability**: 128 Gbps
- **10/100/1000 TX ports:** 20
- **10 Gigabit ports:** 2 XFP Expansion slots
- **10 Gigabit ports:** 2 stack ports

- **Switching:** Layer 3

[More information on MS-320GE 4GC](#)

3. MS-348-FE4GC

- **Forwarding rate:** 13.2 Mpps
- **Switching Capability**: 17.6 Gbps
- **10/100 TX ports**: 48
- **Gigabit ports**: 4 - GigE Combo (SFP / TX)
- **Switching**: Layer 3

[More information on MS-348FE-4GC](#)

4. MS-324 FE4GC

- **Forwarding rate**: 9.8 Mpps
- **Switching Capability**: 12.8 Gbps
- **10/100 TX ports**: 24
- **Gigabit ports:** 4 - GigE Combo (SFP / TX)
- **Switching:** Layer 3

[More information on MS-324FE-4GC](#)

For more information on the Case Communications Medalist Ethernet switches please follow the links under each switch or contact Case Communications via sales@casecomms.com or please call us on +44 (0)1494 880 240

A British scientist says he is the first man in the world to become infected with a computer virus.

In trials, Dr Gasson showed that the chip was able to pass on the computer virus to external control systems.
If other implanted chips had then connected to the system they too would have been corrupted, he said.

Medical alert

Dr Gasson admits that the test is a proof of principle but he thinks it has important implications for a future where medical devices such as pacemakers and cochlear implants become more sophisticated, and risk being contaminated by other human implants.

"With the benefits of this type of technology come risks. We may improve ourselves in some way but much like the improvements with other technologies, mobile phones for example, they become vulnerable to risks, such as security problems and computer viruses."

However, Dr Gasson predicts that wider use will be made of implanted technology.

"This type of technology has been commercialised in the United States as a type of medical alert bracelet, so that if you're found unconscious you can be scanned and your medical history brought up."

Professor Rafael Capurro of the Steinbeis-Transfer-Institute of Information Ethics in Germany told BBC News that the research was "interesting".

"If someone can get online access to your implant, it could be serious," he said.

Cosmetic surgery

Professor Capurro contributed to a 2005 ethical study for the European Commission that looked at the development of digital implants and possible abuse of them.

"From an ethical point of view, the surveillance of implants can be both positive and negative," he said.

"Surveillance can be part of medical care, but if someone wants to do harm to you, it could be a problem."

In addition, he said, that there should be caution if implants with surveillance capabilities started to be used outside of a medical setting.

However, Dr Gasson believes that there will be a demand for these non-essential applications, much as people pay for cosmetic

surgery.

"If we can find a way of enhancing someone's memory or their IQ then there's a real possibility that people will choose to have this kind of invasive procedure."

Dr Gasson works at the University of Reading's School of Systems Engineering and will present the results of his research at the International Symposium for Technology and Society in Australia next month. Professor Capurro will also talk at the event.

(Courtsey of the BBC)

Case Communications launch their new 1+ Mpps Samurai Modular routers

....

The Samurai Express is Case Communications 2U router for border, edge and co-locations routing and VoiP applications. The 2U chassis includes PCI Express expansion slots.

The Chassis has a locking front door, with two removable drive bays to support applications like Web caching and VoiP gateway / auto-attendant than can benefit from adding a hard drive to our routers.

The chassis supports options for redundant AC or redundant -48VDC power supplies and its design will require all wiring to be connected inside the rack at the back panel.
The Samurai Express has one x 16 PCIe slot, one x 4 PCIe slot and two PCI slots. The two PCI slots reside on dedicated PCI buses, enabling the capacity of two PCI buses.

The Samurai Express uses Linux which provides support for NAT, Firewall, VPN's, Quality of Service (QoS), VLANs, VRRP Failover, dynamic routing, packet filtering, bridging, peer-to-peer traffic control, lawful intercept, Voip gateway Web filtering with Netsweeper, and more.

The distribution also leverages the powerful and scalable 'Inetics 'driver component architecture. 'Inetics 'supports WAN protocols including PPP, Cisco HDLC, Frame Relay, ATM and best-in-class E1/T1 solutions that run Any Port, Any protocol. Inetics even simplifies trouble shooting for LAN and WAN connections with real-time port status and performance monitoring.

The Samurai Express can be used as an Internet gateway, and in the network core or edge. It delivers superior performance and reliability in a 2U package that works where most Cisco 2800, 3800 and 7200 routers are used.
The Samurai Express is Case Communications lowest cost router for applications requiring redundant power including high-speed multi-homed networks, DSL aggregation and a wide range of other mid-range routing applications.

For more information please contact please look on our web site at http://www.casecomms.com/products/routers/industrial/samurai.htm or contact Case Communications.

'Hospital risk' from radio tags

Radio frequency identification devices (RFIDs) are on the rise in healthcare, helping identify patients, and reveal the location of equipment.

The Journal of the American Medical Association study found they could interfere with machines.

But NHS computer specialists said RFIDs could eventually make patients safer

There are two types of RFID, one which transmits information, and another, "passive", device which can be "read" by a powered machine when it is held nearby.

They are small and cheap enough to be in everyday use in society, in everything from security and travel cards - such as London Transport's Oystercard, to anti-theft devices on goods in shops, and hospitals are starting to become aware of their potential.

At Heartlands Hospital in Birmingham, patients heading for the operating theatre wear an RFID wristband, so that even when anaesthetised, their full identity, including a picture, can be downloaded into a PDA held nearby.

Turned off

The latest research, conducted at Vrije University in Amsterdam, tested the effect of holding both "passive" and powered RFID systems close to 41 medical devices, including ventilators, syringe pumps, dialysis machines and pacemakers.

A total of 123 tests, three on each machine, were carried out, and 34 produced an "incident" in which the RFID appeared to have an effect - 24 of which were deemed either "significant" or "hazardous".

In some tests, RFIDs either switched off or changed the settings on mechanical ventilators, completely stopped the working of syringe pumps, caused external pacemakers to malfunction, and halted dialysis machines.

The device did not have to be held right up to the machine to

make this happen - some "hazardous" incidents happened when the RFID was more than 10 inches away.

Patient safety

Dr Donald Berwick, from the Institute of Healthcare Improvement in Cambridge, Massachusetts, said: "Design in isolation is risky - even the most seductive technology will interact in the tightly-coupled healthcare world in ways physicians and other members of the healthcare team had better understand, or they and their patients may pay a dear price."

A spokesman for NHS Connecting for Health, which manages various IT projects across the health service, said that RFIDs had the potential to deliver big improvements in patient safety, reducing mistakes caused by the wrong identification of patients.

She said: "Any product such as this which is for use in a healthcare setting has to meet a standard which means it is very unlikely to interfere with medical equipment.

"This risk is more likely to come from RFID tags from other sources - such as a travel card, a tag on clothing, or on another retail item."

A spokesman for the Medicines and Healthcare Products Regulatory Agency said that, as for mobile phone use, individual Trusts needed to make risk assessments about the use of RFIDs.

He said: "Despite much debate in the literature on the subject of electromagnetic interference (EMI) of medical devices by mobile telephones and other sources of radiofrequency transmission, the MHRA has received very few reports of adverse events caused by this problem over the last seven years or so.

"Of those incidents reported, only a very small number have been proven to be as a direct result of EMI."

Few ISP's supporting IPv6

It is important that service providers can support IPv6 as the available address space we currently use ('IPv4') is projected to run in 2011. After this, it will not be possible to allocate new IPv4 addresses which are used to identify each computer on the Internet, and whilst it will take some time before the effects are truly felt by consumers, it will start to divide the Internet.

IP addresses are like phone numbers and as the telephone network expanded, it was necessary to make them longer to make space for new numbers, for example by changing London's area code from '01', to '071', then '0171' and finally '020' in April 2000. The good news for consumers is that because we use domain names rather than IP addresses when going to websites, you will be able to continue to type www.google.com into your web browser, and it will take you to Google in exactly the same way whether it uses IPv4 or IPv6.

Mainstream operating systems such as Microsoft Windows and Apple's OS X have supported IPv6 for some time now, and even companies like google have been IPv6 enabled since 2008, but only a small number of broadband service providers and router manufacturers are ready. It seems that those offering IPv6 are the niche providers.

The current IPv4 address space contains 4.3 billion addresses, but as more users and companies come online in countries like China, we're fast running out of them. The number of addresses offered by IPv6 is 340,282,366,920,938,000,000,000,000,000 billion (2 to the power of 128) which means that the size of the Internet could double every year and we would still have enough IPv6 addresses for the next 96 years.

We called 17 broadband service providers a few weeks ago to ask if they supported IPv6 and we were quite surprised by the results, not because we expected it to be supported by many of them, but because of the inaccurate information we were provided. Several larger providers took 20 minutes to give us a definitive answer, and even then we believe 3 of them got it wrong.

Here are some of the interesting responses to a question asked by 'Think Broadband' to some Internet Service providers "Do you support IPv6?"

"Is it Internet Explorer 6?"

"I know quite a bit about computers but I've never heard that before."

"Never been asked. I'm just looking at Wikipedia right now"

"Is that voice over Internet?"

"[IPv6] has not been released in the market"

"We support IP version 5, but I'm not too sure about 6"

"Is that a TV channel?"

"[We] would advise you to use version 4 [..] Version 6 never always works"

Mobile net 'heading for data jam'

According to mobile analyst firm Informa, Mobile data traffic looks set to rise 25 fold by 2012.

The boom could present operators with problems as revenues generated by those using such mobile data services will only double over the same time period.

Mobile network experts warn that operators need to take action to avoid imminent data traffic jams.

"Revenues from data are increasing much slower than traffic," said Dimitris Mavrakis, mobile network analyst from Informa. "Where operators are experiencing exploding data traffic, revenues are not following them."

The "decoupling" of revenues from traffic presented operators with a problem, said Mr Mavrakis, because it deprived the phone firms of cash at a time when their networks were in need of upgrading.

This was compounded, he said, by the fact that hardware to build next-generation mobile networks that can handle high data rates will not be widely available until late 2010.

Graham Carey, a spokesman for network optimisation firm Bytemobile, said the history of mobile networks also made it harder to handle the always-on nature of many smartphones and laptops.

"Radio networks today have been designed to have very short sessions for telephone-type calls," he said.

He added that flat-rate pricing made it hard for mobile operators to recover enough cash to cope.

Such payment plans made it hard to persuade users to be parsimonious with their data browsing.

"As far as users are concerned, they do not see the need to manage their consumption," he said.

"The consumption rate is far outweighing the network improvement rate," he said. "There's a crunch point coming."

Already many mobile networks were turning to optimisation schemes that shrink the size of files that people download.

Typically these involve using software centrally to look at what people are downloading and shrink them where possible. For instance, web pages with a lot of white space can be shrunk with little or no effect on the quality of a site seen by end users.

John Spindler, vice president of product management at network optimisation firm ADC, said operators were also struggling to cope with sudden spikes in mobile data use.

Heavy users of mobile data were not spread equally around an operator's network, he said.

"When you start looking at data applications, if you look at laptops or mobile handsets, a lot of that is not happening on the street corner," he said. "It is happening in conference rooms and convention centres."

"Today the primary use for wireless is happening indoors," he said.

"What's going to happen if carriers do not respond appropriately? They are going to crush the user experience."

Case June 2010 Newsletter

'Shady' porn site practices put visitors at risk

It found that many sites harboured malware or used "shady" practices to squeeze money out of their visitors.

By creating their own porn sites researchers found that many consumers were vulnerable to known bugs and loopholes.

Competition among porn sites makes the online adult industry ripe for abuse by hi-tech criminals.

"They have almost inadvertently created a whole ecosystem that's easy to abuse for cyber crime on a large scale," said Dr Gilbert Wondracek, a computer security expert from the International Secure System Lab, which led the study.

Hidden danger

Dr Wondracek said the team embarked on the study to find out the truth of the widely held view that porn sites are dangerous to visit.

"There are studies looking at the profitability and economics of the industry but we are the first to come at it from a security and more technical point of view," he said.

Statistics suggest that approximately 12% of all websites offer pornography of one sort or another and that 70% of men under 24 browse these sites.

As a first step the researchers trawled pornographic sites to classify what they found and how the industry was structured.

The big distinction was between free sites and those that charge for access. Typically pay sites produce content they give to free sites to drum up traffic.

More than 90% of the 35,000 pornographic domains analysed in the study were free sites.

The researchers analysed the 269,000 websites hosted on the 35,000 domains to see which hosted malicious software. About 3.23% of these sites were booby-trapped with adware, spyware and viruses.

Many others used "shady" practices to keep visitors onsite. These included javascript catchers that made it hard for people to leave a page.

Others use scripts that re-direct visitors so when they click on a link they do not see the video or image they were expecting but are passed to an affiliate site.

The vast majority of sites engage in this trading of traffic or clicks, said Dr Wondracek.

"Visitors are being abused as click bots," he said.

As most sites were free, the only resource they could exploit as a revenue source was this traffic.

"It's cut-throat competition," said Dr Wondracek. "Everybody tries to get as much traffic as possible."

Finding victims

Traffic is used in many different ways. Popular sites sell it to those looking for an audience, some is used to direct visitors to affiliates who provide content and sometimes it is used to boost rankings in search engine indexes.

It could also be a great way for hi-tech criminals to get a ready source of victims, said Dr Wondracek.

To test this idea the researchers created two adult sites of their own, populated them with free content from porn producers and spent $160 (£108) to get traffic piped to these sites.

Analysis of the 49,000 visitors sent to their sample sites showed that 20,000 were using a computer and browser combination that was vulnerable to at least one known exploit.

"As an attacker you want to make your life easier," said Dr Wondracek. "If you can have these 20,000 people come to a place instantly, why not?"

With many porn sites appearing in the top 100 most popular sites on the web this could mean that huge numbers of people are caught out when they browse for adult content.

While relatively few porn sites were infecting visitors, it is difficult to spot good from bad, he said.

"For the average user it might be hard to tell an honest porn site from a dishonest porn site until you click on something," he said.

Dr Wondracek recommended that anyone visiting porn sites keep their security software up to date and use the "safe browsing"

modes found in many browsing programs.

The researchers presented their results at the Workshop on the
Economics of Information Security held at Harvard from 7-8 June