Case Communications November Newsletter

Greetings,

Welcome to the November edition of the Case Communications Newsletter. Please dont hesitate to contact us if you have any articles you would like to contribute or would like to make any comments.

Case Communications November Newsletter

In this Issue:

The Risks associated with the WEEE Directive
A guide on how to reduce your Spam
Schools dismantle wireless networks amid fears for health
A Special Notice about Polonium 210
IEEE 802.1q Unauthorised VLAN Traversal Weakness
The rush towards 10Gbps Ethernet

The Risks associated with the WEEE Directive

The UK's implementation of the Waste Electrical and Electronic Equipment (WEEE) Directive is finally set to commence next year in both the business community and the consumer. With it will come a huge increase in the collection of discarded servers and computers, many of which will be full to overflowing with information stored on hard drives.

More

A guide on how to reduce your Spam

Spam is becoming an ever-growing nuisance, and accounts for a considerable amount of wasted time, especially when you have to go through your incoming mailbox to erase Spams or go through your Spambox to retrieve good mails.

More

Schools dismantle wireless networks amid fears for health

Parents and teachers are forcing some schools to dismantle wireless computer networks amid fears that they could damage children's health.

More schools are putting transmitters in classrooms to give pupils wireless access from laptops to the school computer network and the internet.

More

A Special Notice about Polonium 210

More

IEEE 802.1q Unauthorised VLAN Traversal Weakness

Case Communications development engineers discuss a problem with the 802.1q standard, and show that it is susceptible to issues that allow attackers to send and receive packets from one VLAN to another without authorisation.

More

The rush towards 10Gbps Ethernet

It was not that long ago when the networking industry transitioned from using 10/100-Mbit/sec ports to primarily 1.0625-Gbit/sec (Gigabit Ethernet) ports. The widespread rollout of Gigabit Ethernet has caused the advent of many forms of 10-Gbit/sec Ethernet for switch backbone links.

More

Thank you for reading the Case Communications Newsletter

Thank you for taking the time to read the Case Communications Newsletter, please don't hesitate to contact Case Communications marketing department on admin@casecomms.com if you have any suggestions or would like to enter any contributions.

Case Communications November Newsletter

The Risks associated with the WEEE Directive

The UK's implementation of the Waste Electrical and Electronic Equipment (WEEE) Directive is finally set to commence next year in both the business community and the consumer. With it will come a huge increase in the collection of discarded servers and computers, many of which will be full to overflowing with information stored on hard drives.

"With the recent story of end-of-life computers from the UK being found in Nigeria with hard drives full of sensitive data, the issue of secure destruction has come to the fore of people's thinking. Despite re-use being held as the ideal under the WEEE Directive, the trend at the moment in industry is towards destruction and material recovery, which are seen very much as the most secure option.

"As a general rule, many reputable organisations are able to offer a "data wipe" service to a standard that guarantees complete clearing of the hard drive. The obvious advantage of this route is that it allows reuse of a computer, or server, within the company or sold into an external reputable market. For instance, an older server could have extra memory fitted before being redeployed in the same business saving the need for new investment in lower spec servers. However, some institutions, be they in the private or public sector, that deal with particularly sensitive data have to pursue the total destruction route, due to the nature of the information held on a server or on a hard disk.

"Therefore, what should people be looking for when it comes to secure data destruction? The first point to note is that security of information is vital and its removal must be provable. It would be difficult to exaggerate the potential damage that could be caused to any number of businesses if sensitive information were to find its way into the public domain. Although responsible companies will do their utmost to remove data before allowing computers out of their control, a second check by a specialised company will bring increased comfort.

"And security, when it comes to the destruction of data, starts at the moment the server is 'unplugged', before it leaves the building. Companies should make sure that their reprocessing partner utilises transportation and logistics systems that are completely secure, including using specialised containers. In addition, the onward journey of WEEE, before it is processed, should always be completed on the same day, without any overnight stops. Indeed, if the information being carried is

Case Communications November Newsletter

In this Issue:

The Risks associated with the WEEE Directive
A guide on how to reduce your Spam
Schools dismantle wireless networks amid fears for health
A Special Notice about Polonium 210
IEEE 802.1q Unauthorised VLAN Traversal Weakness
The rush towards 10Gbps Ethernet

particularly sensitive, the journey's key moments, such as the start and the end, should be available to be witnessed by the client. Furthermore, once assets have been transported, the processing facility that they arrive at should also be secure and be able to offer a witnessed destruction upon arrival service.

"The processing facility should offer complete hardware destruction, which is often favourable over processes like eventual data wiping, which can be both time consuming and have associated risks. However, there should also be the option from a reprocessor of wiping data from machines at a client's facility, prior to the transportation of equipment for destruction. And one step on from this, some companies may need to witness the physical destruction of units for themselves – and a reprocessing partner should be able to facilitate this.

"Companies should also look at the actual destruction process used by potential reprocessing partners. The standard destruction of equipment will involve pre-shredding to forty millimetre strips before secondary granulation down to twenty millimetre "flakes". Good processors should be able to offer a final granulation of material to pieces as small as six millimetres in size for when security is even more vital. Again, if it is warranted by the client, the customer should be able to witness destruction at first hand or receive suitable evidence, such as photographs or film footage, of the server's demise. Finally, all computer waste emanating from the process should be disposed of in accordance with the criteria laid down in the legislation.

"If destruction of equipment such as servers and hard drives is the route decided upon by companies, businesses must choose a partner of integrity with clearly auditable systems for their peace of mind. Recyclers and dismantlers not offering such a system as part of the refurbishment or recycling process should be avoided under all circumstances."

Case Communications November Newsletter

A guide on how to reduce your Spam

Reduce your risk of being 'Harvested'

Certainly if you're the owner of a web site you can attract a lot of unwanted mails and the way to reduce this is by not displaying your e-mail address in public more than necessary, at least not in a way 'Scavenger bots' (programmes that spammers use to collect e-mail addresses.

One useful tip is not to put your e-mail address in a click to e-mail. It means people have to cut-and-paste your address than than e-mailing you with a single, click, makes more work for them, but saves a lot of Spam.

Rather than putting your email address on every page of your site, it may be better to have it on only one page, with links to it. Many spammers don't even bother to remove duplicates from their lists. If your address appears on a very well-indexed site you might want to use one of the many common tactics to disguise it to fool scavenger bots, (such as splitting the components of the address), or inserting HTML code in the middle of the address.

If you post to Usenet or chat, consider disguising your address. There are dozens of ways of doing this so that humans who really want to contact you can figure out how to do so: look at a few postings and choose one you like. We have heard reports that some harvesters are already wise to addresses such as me@nospam.myisp.com so try a variation on the nospam. There are plenty of adjectives that could be added.

An alternative is getting a free forwarding address from companies who include free filtering facilities.

A harvesting technique called 'dictionary spamming' will pick up more common user names and will generate more Spam to those names than the less common names. So for example if your user name is jbrown you will get more Spams than if your user name is jb49rwn, particularly at large ISP,s. A name with a letter late in the alphabet also gets less Spam because many lists are sold sorted in alphabetic order and Spamming sessions are often terminated before they complete.

Check your browsing isn't giving you away

Case Communications November Newsletter

In this Issue:

The Risks associated with the WEEE Directive
A guide on how to reduce your Spam
Schools dismantle wireless networks amid fears for health
A Special Notice about Polonium 210
IEEE 802.1q Unauthorised VLAN Traversal Weakness
The rush towards 10Gbps Ethernet

In a very small number of cases, your email address may be discovered by a web site you visit. This has occurred through bugs in places such as Web-based email services. Early versions of some browsers gave away email addresses routinely. A quick and easy way to check for this is to visit 'Junkbuster' privacy check page that displays these headers. If your address is being disclosed, reconfigure your browser or use a free product such as Internet Junkbuster to block it.

Check that your ISP or company isn't running the identd demon, a background program that Web servers can ask for your user ID while you wait for a page. It was originally intended to restrict access to authorized users, but spamming sites can use it to guess your email address.

Requesting anonymity from sources of addresses

If you use an on-line service that offers a member directory, opt out of it; they are favourites of spammers.

Some larger companies sell or give away email addresses. Most have policies and terms that prohibit use of their information for spamming, but this doesn't seem to stop some spammers.

You can tell email lookup services such as those listed in Yahoo to remove your name and email address.

Some of the giant companies that sell mailing lists to catalog companies are now also selling email addresses. Most of these don't have Web-based ``opt-out'' forms, but JUNK*BUSTERS* gives you an easy way to draft physical letters to them.
DECLARATION

Reporting spammers to ISPs and email providers

The instructions given in spam to have your name removed from the spammer's lists are often bogus. The address may not exist: if it doesn't mailing to it will only result in another piece of email saying it wasn't delivered. One spammer has even included the URL for this page in fake instructions for removal.

A free service that does the sleuthing and complaining for you is Spamcop. [Wired on Spamcop]

If the spam asks invites responses to an address at one of the major online providers or at a ``disposable'' address such as the free accounts provided by Hotmail or Juno, your course is clear: simply forward the spam to the postmaster at the company named. All these companies have strict policies against spam and should terminate the account promptly, if it is really being used by a spammer. If not, they may decide to track down and cut off or sue the spammer.

Reporting spammers to law enforcement

There are various law enforcement agencies where you can report spam.

1. If the spam involves fraudulent or deception practices, you can forward it to uce@ftc.gov for the Federal Trade Commission to add to their database.
2. If a Nigerian says they have millions of dollars waiting for you to collect, forward the email with the subject "419 sample - no financial loss" to 419.fcd@usss.treas.gov for the US Secret Service to investigate. Nigerian Advance Fee Fraud (also called 419 Fraud) has been going on since the 80's with faxes, and has recently become common with email.

What about removal services?

Be cautious also about sites where you can register to have your email address removed from spammer's lists. Some are ineffective; some actually *add* your address to other spammers' lists.

Some services say they will not giving addresses to spammers: they have to submit their lists for ``cleansing.''

Some large service providers sue spammers to protect their customers and in the USA the Federal Trade Commission has said they will go after Spammers who fraudently use tactics such as fake removal addresses.

Its difficult for the average person to stop spammers, but one tactic which seems to be working in the USA, is to provide a carefully worded ‘offer such as shown in the paragraph below.

I do not want to receive uninvited solicitations by email (``Junk Email''). I am unwilling to receive Junk Email freely because it costs me time and money. If you send me any Junk Email other than on the terms of the offer set out in the following nine points, I will take this to mean that you plan to use what I offered you without paying for it. If you ever try to do this I reserve my right to take any action available to me without further reference to you. Actions available to me include taking proceedings against you for negligence or breach of contract, which may result in substantial damages being awarded against you by a court. The unauthorized use of my computing facilities may even be a crime.

1. *I offer to receive all further email from you on the terms set out below. If you send me any solicitation by email without my express prior written consent this will be taken as your acceptance of this offer.*

2. *For the purposes of points 3 and 4, you will be taken to have sent any email sent by any entity apparently associated with you for the purpose of sending email solicitations.*

3. *You must pay me ten US dollars for each such item of email that you send me.*

4. *You must pay me ten US dollars for each copy of each email solicitation that you send to anybody or any email address referred to below, even if you don't send a copy to me. You may also have to pay other persons as well if they have sent you a similar offer.*

5. *I may join with any of those persons for the purpose of efficiently collecting your payments.*

6. *You must mail payment by certified check to me within five working days of the transmission of the email. If you do not know where to send payment, you must state this in the email and give me an easy way to tell you.*

7. *Each email item must be uniquely identified, and each payment must clearly identify the relevant item or items.*

8. *You must tell me your name and full business and residential addresses in each email message.*

9. *I may vary the terms of or terminate this offer at any time (even after you have accepted it). Any new terms will apply to all email you send after you have been notified of a variation.*

Some large online providers do sue spammers to protect their customers, and the Federal Trade Commission has said that they will go after spammers who use fraudulent tactics such as fake remove addresses. But what can the average person do to stop a persistent spammer?

Other commonly used legal threats include claims that spam is an unsolicited fax under the *Telephone Consumer Protection Act,* and statements that spam will be interpreted as an order for proofreading services.

Parts of this article are kindly reproduced from 'Junkbusters'

Case Communications November Newsletter

Schools dismantle wireless networks amid fears for health

Health fears lead schools to dismantle wireless networks

- **Radiation levels blamed for illnesses**
- **Teacher became too sick to work**

Parents and teachers are forcing some schools to dismantle wireless computer networks amid fears that they could damage children's health.
More schools are putting transmitters in classrooms to give pupils wireless access from laptops to the school computer network and the internet.

But many parents and some scientists fear that low levels of microwave radiation emitted by the transmitters could be harmful, causing loss of concentration, headaches, fatigue, memory and behavioural problems and possibly cancer in the long term. Scientific evidence is inconclusive, but some researchers think that children are vulnerable because of their thinner skulls and developing nervous systems.

At the Prebendal School, a prestigious preparatory in Chichester, West Sussex, a group of parents lobbied the headteacher, Tim Cannell, to remove the wireless network last month. Mr Cannell told The Times: "We listened to the parents' views and they were obviously very concerned. We also did a lot of research. The authorities say it's safe, but there have been no long-term studies to prove this.

"We had been having problems with the reliability of it anyway, so we decided to exchange it for a conventional cabled system."

Vivienne Baron, who is bringing up Sebastian, her ten-year-old grandson, said: "I did not want Sebastian exposed to a wireless computer network at school. No

Case Communications November Newsletter

In this Issue:

The Risks associated with the WEEE Directive
A guide on how to reduce your Spam
Schools dismantle wireless networks amid fears for health
A Special Notice about Polonium 210
IEEE 802.1q Unauthorised VLAN Traversal Weakness
The rush towards 10Gbps Ethernet

real evidence has been produced to prove that this new technology is safe in the long term. Until it is, I think we should take a precautionary approach and use cabled systems."

At Ysgol Pantycelyn, a comprehensive in Carmarthenshire, parents aired their concerns to the governors, who agreed to switch off its wireless network. Hywel Pugh, the head teacher, told The Times: "The county council and central government told us that wireless networks are perfectly safe, but as there were concerns we listened to them and decided that the concerns of the parents were of greater importance than our need to have a wireless network."

Judith Davies, who has a daughter at the school, said: "Many people campaign against mobile phone masts near schools, but there is a great deal of ignorance about wireless computer networks. Yet they are like having a phone mast in the classroom and the transmitters are placed very close to the children."

Stowe School, the Buckinghamshire public school, also removed part of its wireless network after a teacher became ill. Michael Bevington, a classics teacher for 28 years at the school, said that he had such a violent reaction to the network that he was too ill to teach.

"I felt a steadily widening range of unpleasant effects whenever I was in the classroom," he said. "First came a thick headache, then pains throughout the body, sudden flushes, pressure behind the eyes, sudden skin pains and burning sensations, along with bouts of nausea. Over the weekend, away from the classroom, I felt completely normal."

Anthony Wallersteiner, the head teacher of Stowe School, said that he was planning to put cabled networks in all new classrooms and boarding houses.

Professor Sir William Stewart, chairman of the Health Protection Agency, said that evidence of potentially harmful effects of microwave radiation had become more persuasive over the past five years. His report said that while there was a lack of hard information of damage to health, the approach should be precautionary.

A DfES spokesman said: "It's up to individual schools to decide on this."

Reproduced courtesy of 'Times Online'

Case Communications November Newsletter

A Special Notice about Polonium 210

A SPECIAL NOTICE ABOUT POLONIUM-210

With the recent news of Polonium-210 being used as a poison, a good deal of incorrect information has been passed around (primarily by the media) concerning the Polonium isotope and radioactive materials in general. It's important to get the facts correct.

The amount of Plonium-210, is an 'exempt quantity' amount. These quantities of radioactive material are not hazardous - this is why they are permitted by the Nuclear Regulatory Commission (NRC) to be sold to the general public without any sort of license.

The exempt quantity amount of Polonium-210, or any of the radioactive isotopes sold is so small that they are essentially invisible to the human eye.
In the case of needle sources, the radioactive material is electroplated on the inside of the eye of a needle.

You would need about 15,000 of our Polonium-210 needle sources at a total cost of about $1 million - to have a toxic amount.

In comparison, Amercium-241 is a similar toxic Alpha radiation emitter.
Instead of a half life of 138 days like Polonium-210 has, it has a half life of over 450 years. It is far more toxic - and there is 10 times more than the 'exempt quantity' amount in every smoke detector in your home.

If you really wanted to poison someone, you would of course have to come up with a way to remove the invisible amount of material from the exempt sources - which is just about physically impossible and combine them together. Of course you would also need that 15,000 exempt sources.

In addition, there are dozens of other far more toxic materials, such as Ricin and Abrin, both of which can easily be made, and are also undetectable as a poison and untraceable.

Although it obviously works, Polonium-210 is a poor choice for a poison.

Another point to keep in mind is that an order for 15,000 sources would look a tad suspicious, considering we sell about 1 or 2 sources every 3 months.

Make sure you are truly knowledgeable about a subject before you start repeating and spreading potentially incorrect information related to it.

Gamma-only radiation emitters

ISOTOPE	ACTIVITY	HALF-LIFE	ENERGIES (KeV)

Case Communications November Newsletter

In this Issue:

The Risks associated with the WEEE Directive
A guide on how to reduce your Spam
Schools dismantle wireless networks amid fears for health
A Special Notice about Polonium 210
IEEE 802.1q Unauthorised VLAN Traversal Weakness
The rush towards 10Gbps Ethernet

Cadmium^{109}	1uCi	453 days	88.0
Barium^{133}	1uCi	10.7 years	81.0, 276.3, 302.7, 355.9, 383.7
Cobalt^{57}	1uCi	270 days	122.1, 136.4
Manganese^{54}	1uCi	312 days	834.8
Sodium^{22}	1uCi	2.6 years	511.0, 1274.5
Zinc^{65}	1uCi	244 days	1115.5

Beta-only radiation emitters

ISOTOPE	ACTIVITY	HALF-LIFE	ENERGIES (KeV)
Strontium^{90}	0.1uCi	28.5 years	546.0
Thallium^{204}	1uCi	3.78 years	763.4

Alpha-only radiation emitter

ISOTOPE	ACTIVITY	HALF-LIFE	ENERGIES (KeV)
Polonium^{210}	0.1uCi	138 days	5304.5

Case Communications November Newsletter

IEEE 802.1q Unauthorised VLAN Traversal Weakness

IEEE 802.1q Unauthorised VLAN Traversal Weakness

By spoofing various Ethernet frame fields such as the source or destination MAC addresses, IP addresses, and VLAN tags, attackers may cause packets to traverse from one VLAN to another, and possibly back again. Attackers may also add multiple VLAN tags to packets to cause multiple routers to decapsulate the packets in unexpected ways, aiding the attacker in traversing VLANs.

This issue allows attackers to traverse from one VLAN to another in an unauthorized fashion. As some users may utilize VLANs to segregate network segments containing differing security properties, this may have various consequences.

This issue may be exacerbated by utilizing attacker-controlled external network hosts to bounce packets between VLANs.

1. Modification of the double-tagging VLAN jumping attack.

The attacker tags his malicious data with two 802.1q tags and sends the packet with a spoofed source IP of a host under his or her control. This can be any host to which a valid route from the target VLAN is present, including an external host on the Internet. The first tag gets stripped by the switch the attacker is plugged into and the packet is forwarded to the next switch. The remaining tag contains a different VLAN number, to which the packet is sent. So, data is forced to pass between the VLANs. The receiving host will check the source IP of the arriving packet and send the reply to this IP, which is a host that belongs to the attacker.

This attack can be launched using Yersinia (http://sourceforge.net/projects/yersinia/).

2. Modification of the MAC spoofing PVLAN jumping attack.

The attacker sends a packet with a valid source MAC but a

Case Communications November Newsletter

In this Issue:

The Risks associated with the WEEE Directive
A guide on how to reduce your Spam
Schools dismantle wireless networks amid fears for health
A Special Notice about Polonium 210
IEEE 802.1q Unauthorised VLAN Traversal Weakness
The rush towards 10Gbps Ethernet

spoofed source P of a host under his or her control. This can be any host to which a valid route from the target PVLAN is present, including an external host on the Internet. The target MAC address is replaced with the one of a gateway router. A switch would forward such packet to the router, which will then look at the IP and direct the packet to the target. Of course, the source MAC of the packet will be replaced by the one of the router, which would then direct the reply packet from the target to the host that belongs to the attacker.

Note: Such attacks can be used for different purposes from portscanning to communicating with a backdoor on a different VLAN or PVLAN.

Risk Factor: Medium

Workarounds: There are no direct workarounds. Implement strict egress filtering against the spoofed packets described.

Case Communications November Newsletter

The rush towards 10Gbps Ethernet

A few years ago most Enterprise customers were content to use one or two Gigabit upklinks, now the cry is for all 10/100/1000 ports on the switch and uplinks to be 10Gbps.

A large number of switches now consists of two or more 10-Gbit/sec ports. Higher-end switches have dozens of 10-Gbit/sec ports as well as some trunk multi-port backbone links.

Today in the interconnect industry, there is a rush to win 10-Gbit/sec single end-user, horizontal-building, and data-center design-ins. This article looks at some of the current activities with copper and optical standards, products, applications, and interconnect components.

IEEE 802.3an, also known as 10GBase-T, is a newly released Ethernet copper specification for the four-lane x 2.5-Gbit/sec per pair electrical signaling intended for twisted-pair cable assemblies with Category 6A or better rating. Purposely, there is no connector or cable assembly specification within this new standard. Current Category 6 unshielded twisted-pair (UTP) interconnect products seem to work only for 37-meter link lengths, not the usual 100 meters for horizontal wiring.

Alien Cross Talk Risks

Alien crosstalk and other factors make foil-shielded Category 6A and dual-shielded cables like Category 7 a lower-risk design-in choice. The Category 7 IEC connector is not RJ-45, but is based on The Siemon Co.'s TERA connector and cabling system. Some suppliers are still working to improve the RJ-45 performance range.

IEEE 802.3ak, also known as 10GBase-CX4, uses the SFF-8470 copper connector for its 4-lanes x 3.125-Gbit/sec per pair, for a total of 12.5 Gbits/sec. This standard does have a connector and cable assembly specification section. Various stacked 4x multi-receptacle connectors are providing increased density across "pizza boxes" and blades. The XAUI-2-based chips with 6 Gbits/sec per differential pair upgrade products have been popular, and still work to 15+ meters. Tiny, active low-cost equalizer chips embedded in cables or receptacles, or feed-through connectors, allow performance to 50+ meters for CX4 current applications. A cable assembly with one 12x connector fanout to six Category 6A receptacles or plugs is a new six-port density solution.

Case Communications November Newsletter

In this Issue:

The Risks associated with the WEEE Directive
A guide on how to reduce your Spam
Schools dismantle wireless networks amid fears for health
A Special Notice about Polonium 210
IEEE 802.1q Unauthorised VLAN Traversal Weakness
The rush towards 10Gbps Ethernet

CX4 cable assembly products vary in performance. Some new-generation CX4 interconnect engineering prototypes have been demonstrated to 17 and 25 Gbits/sec per pair, while the majority of design-in is in the 4, 5, 6, or 8.5-Gbit/sec range. There is also a quickly growing 10- and 12.8-Gbit/sec design-in range because of the requirement to have multi-generational capability and many custom backbone I/O product design-ins.

Some 100-Gbit/sec Ethernet CX early developers are looking at using a 12x InfiniBand connector with 12 lanes running at 10 Gbits/sec per pair in a serial aggregation architecture. Some may want a smaller connector supporting the 24 different pairs, yet other OEMs may consider staying with the 4x connector by supporting four lanes x 25-Gbits/sec per pair for 100 Gbits/sec.

IEEE 802.3ap, also known as 10-Gbit Backplane Ethernet, is a new specification for running either four lanes x 3.125 Gbits/sec and/or one lane x 10.5 Gbits/sec. This specification covers signaling running from chips, through boards and multiple connectors, but does not specify what connectors or boards to use. High-speed cabled backplane expander assemblies are longer solutions compared to current FR-4 printed circuit boards.

CompactPCI and VME specifications support various Ethernet signaling running through the hard metric 2-mm connectors (frequently referred to as 2 mm HM). New 2-mm cabling fanout systems with Category 6A or Category 7 connectors and raw cables are a popular upgrade product for a large installed base within the military/aerospace and telephony market segments.

A collaboration

IEEE 802.3's liaison work group and the INICTS-T11 Fibre Channel physical layer committee are working to complete a jointly supported one-lane SFP+ interconnect specification for 10.5 Gbits/sec and 8.5 Gbits/sec one-lane links. Besides the market offering of several SFP+ optical transceivers for very long links, another popular solution will be SFP+ copper to same or in fanout (sometimes called "octopus") configurations using a 12x InfiniBand-style connector as a multiport single connector. A portion of the storage area network and data-communications switch markets likely will use SFP+ versus dedicated optical with LC cables and copper enhanced HSSDC-2 connector and cabling systems used in IEEE-802.3z Gigabit Ethernet.

Ethernet observers are also looking closely at the development of a new multi-source agreement (MSA) consortium that is also working with the InfiniBand consortium. The Quad SmallFormfactor Pluggable (QSFP) proposed from *www.qsfpmsa.org* is a four-lane optical multimode transceiver using a wider version of the current SFP shield cage and PCB edge connector. A copper-plugged QSFP cable assembly could be competing with CX4 in the data-center environment, as could the 8-fibered MTP/MPO assemblies.

TIA-568 cabling standards have been upgraded to cover Category 6A applications and installations for building wired infrastructures. Wiring cabinet proprietary block products are declining in design-ins and TAM (total available market) versus RJ-45 interconnects.

Whats to come?

The chip technology and supporting interconnect that offers the lowest power consumption and cooling requirements, and higher-density footprint, likely will be holding major TAM design-in percentage. Ethernet, InfiniBand, and Fibre Channel cross-compatibility are key for winning chip and interconnect product design-ins.

Some Ethernet 10GBase-T evangelists would like to see a higher-density and higher-speed copper connector versus the current Category 6A and Category 7 connectors. There seems to be a need for the Category 7 connector to have the enhanced IEEE 802.3ah Power over Ethernet (PoE) capabilities that are available with Category 6 RJ-45 receptacles. Will there be a future IEC Category 8 copper cabling specification?

Multiple 1-Gbit Ethernet signals have been proven to work within the new MiniRJ-21 connector that is replacing the very old delta-ribbon style 50-position RJ-21 connector. Can the MiniRJ-21 handle 802.3an 2.5-Gbit/sec signals as well as CX-4 3.125-Gbit/sec signals, or will a new connector become either an industry or a *de facto* standard?

Will there be a need for environmentally hardened SFP or Category 7 plugs and cables, as there has been for Gigabit Ethernet within overmolding and circular metal shells using RJ-45 Category 5e connectors?

10-Gbits/sec has been a multi-technology and standard-interfaces roadmap crossover point. How will the Ethernet community compete with developing 4 lanes x 10 for 40 Gbit/sec ATM, and 160 Gbit/sec SONET standards and products?

Heat, power, and density factors within chips and modules will continue to drive the design for smaller, high-performance connectors and provide major TAM to the standard that has the best price/density solution set. CX4 chips have had a best overall heat/power/size story, so CX4 forecasting remains healthy for the data center for now.