Ambient Networking Solutions for Anytime, Anywhere, Anyplace Communication
IST Results (06/20/06)

The WWI Ambient Networks project has developed a proof of concept demonstrator that suggests seamless connectivity of different wireless and mobile networks could become a reality. The cooperation of the different networks would enable end users to select the best network for a particular service or multimedia content, regardless of their location. The IST-funded project has developed Smart Multimedia Routing and Transport technology, a prototype that is also designed to provide operators with the network configuration and management necessary to support such flexibility. "The comprehensive prototype will include multi-access technologies that will give the user or networks the choice of using the appropriate radio technology automatically, such as switching between different flavors of Universal Mobile Telecommunications System, Wideband Code Division Multiple Access, Code Division Multiple Access, the Wireless LAN, Bluetooth or a forthcoming 4G radio," says project coordinator H. Abramowicz at Ericsson. "Users will be able to instantly connect without a commercial contract." As the industry comes to agreement on ambient networking concepts, mobile network service providers will have new business opportunities in integrating user networks.

Groups Push Alternate Net Neutrality Proposals
IDG News Service (06/20/06), G. Gross

Two days in advance of the Senate Commerce Committee's debate on the net neutrality issue, the Center for Democracy and Technology (CDT) and New Yorkers for Fair Use have released their own net neutrality proposals, which aim to force broadband providers to treat all content equally on the public Internet while permitting them to reserve portions of their network for specialized offerings. CDT executive director L. Harris says her organization would prefer a "narrowly tailored" series of net neutrality regulations, though big broadband providers claim such measures are unnecessary because there is no evidence of content discrimination. Harris says the scarcity of broadband competition presents a "significant risk" for such abuse. Under the CDT plan, Congress would be authorized to watchdog the Internet for signs of discrimination, and broadband providers would be allowed to offer tiered services such as broadband video while maintaining equal treatment for all public Internet content and services. New Yorkers for Fair Use member S. Johnson's net neutrality proposal, endorsed by D. Reed and others, would also permit the provision of tiered services, but their categorization as Internet services would be disallowed if they discriminate against rival content. In an e-mail, the Johnson group said Congress has to elucidate the definition of Internet connectivity. "IP-layer neutrality is not a property of the Internet. It is the Internet," they wrote.

Interview: Why DNS Defences Need Bolstering
IT Week (06/19/06), P. Muncaster

A. Gouyet, the vice president of marketing for Nominum, describes the security threats to the Domain Name System (DNS), which tend to be overlooked, he says. The security threats to

the DNS have the potential to erode users' trust in the Internet, which will affect the visible Web presences of governments and companies, Gouyet says. There are new DNS vulnerabilities being exploited each quarter, and companies "don't spend enough time reviewing [the DNS] like they do auditing the network security layer," he says. These threats can be mitigated with DNSsec, which authenticates IP addresses. The Swedish government is implementing DNSsec for the .se domain name, and the United States is also looking to adopt DNSsec. DNSsec requires an upgrade to the DNS servers and it takes multiple levels of cooperation in order to work properly. "You must have people sign their domain names, and DNS service providers must upgrade their servers to recognize when the signatures are there and when they are not," Gouyet says.

Keeping the Trust While Under Attack
Government Technology (06/20/06), K. Asborno

Information security threats such as identity theft, fraud, and malware were discussed during a NASCIO teleconference, keynoted by E. Spafford at Purdue University. More than $100 billion is spent every year to fight these attacks. Government legislation such as the Real ID Act and Help America make it even easier for information to be exposed on the Web. Spafford weighed in on the alarming statistics and what proactive methods need to be implemented to safeguard networks. "In 2003-2004 we saw about 4,000 vulnerabilities reported in those [commonly used software packages]," said Spafford. "In 2005 it jumped up to about 4,600, and so far this year we are averaging about 20 per day. That's an incredible load to try to keep up with." Spafford suggested that vendors need to release more products to businesses and the government that can be trusted and he insists that firewalls are not an effective solution. Organized crime, rather than terrorism is the biggest threat to the government and it is getting worse in Eastern Europe and Africa, according to Spafford. A long-term plan that consists of policymaking, education, and enforcement is the best solution for businesses and government to fend off attacks, said Spafford. Business and the government should consider how and where information is being stored and limit connectivity.

ICANN Needs to Clamp Down on Domain Name Abuse
CNet (06/21/06), D. Isenberg

A debate over the purpose of the Whois database is quietly taking place, with one side arguing that the database is essential to conducting business on the Internet and another side arguing that, for privacy reasons, domain name registrants should not be forced to enter personal information into the database. Meanwhile, ICANN, which meets in Morocco June 26-30, is also pondering the issue. ICANN requires that domain name registrars collect personal information about domain name registrants, including their names and contact data, and enter it into the publicly accessible Whois database so that cybersquatters, phishers, and other online crooks can be forced out of the shadows and identified. Ensuring that the information in the Whois database remains publicly accessible is important to protecting company brands and, by extension, consumers on the Internet, but others argue that the Whois database creates privacy risks. Some cybersquatters provide false Whois information to registrars--the registrant of one particular domain name is listed as "Meow," a cat--and it can be surmised that these domain owners are up to no good. Many cybersquatters now call themselves "domainers," and an entire industry of domain name "monetization" services has allowed domainers to make money off of parked domains, many of which are suggestive of well-known brands. These monetization services, along with other dubious practices such as "domain tasting," are causing economic damage to legitimate businesses, which must spend money and resources to

protect their intellectual property on the Internet. If ICANN decides to place additional restrictions on the Whois system, these companies and their consumers will suffer even greater harm, and the integrity of the Internet will be compromised, writes attorney and WIPO domain name panelist Doug Isenberg.

RFID Tags: Driving Toward 5 Cents
EDN (06/08/06) Vol. 51, No. 12, P. 69; C. Murray

Radio Frequency IDentification (RFID) tags have not reached the nickel per tag price point partly out of manufacturers' hesitancy, since lower-priced tags may be less capable than higher-priced ones. "We've been talking about the mythical 5-cent price point for years. Is it possible? Yes. But it may not necessarily be the type of tag you're looking for," says Venture Development's M. Liard. The upshot of the lack of enthusiasm for pursuing 5-cent tags is the employment of current tags in previously undreamed of applications while makers simultaneously improve RFID technology and reduce costs at about 5-10% annually. Experts expect RFID tags to be embedded in everyday items, while their non-line-of-sight capability can thwart theft and forgery by facilitating the gathering of location information without individual handling. There is also confidence among experts that an "Internet of things," in which nearly all conceivable items are networked together, will be facilitated by RFID technology. This would allow the instant identification of all products by anyone anywhere. Researchers expect everyday objects to feature RFID via integration within the corrugate of cardboard boxes during manufacture, instead of on sticky tags. MIT mechanical engineering professor S. Sarma believes RFID technologies will proliferate when production volume hits a tipping point, reducing costs enough to encourage RFID tagging of everyday objects. Sarma says, "The question now is the tipping point. When do you get to the percentage that causes you to say, 'I'm going to put the tag inside the corrugate?' In the next year, we could see it happen."

Debugging ZigBee Applications
Sensors (06/06) Vol. 23, No. 6, P. 16; A. Wheeler

The complexity of ZigBee wireless sensor networks lessens the effectiveness of traditional debugging methods, but new tools are emerging that can help. Greater numbers of sensors and a wider distance between them makes the collection of information via standard techniques increasingly cumbersome, which can give rise to inaccurate readings of where a malfunction is taking place, or can cause new faults to crop up. Most issues with a ZigBee HVAC system can be attributed to information overload or the failure to obtain required information because of the size of the system. Information overload can be minimized by network analyzers, which come with traditional packet sniffer capabilities in addition to support for multiple data sources and sophisticated packet activity analysis tools. Replacing traditional in-circuit debug and serial printing functions with analyzers calls for close links between the tools and a vendor's hardware, and ZigBee nodes use MCUs and radios that feature direct hardware support for network debugging. This allows for the creation of tools that can resolve many problems associated with sniffer-based tools, as well as the enablement of access to more traditional network debugging methods; the debugging integration can be executed through the use of ZigBee systems-on-chip. Among the challenges that are still unmet is the provision of processor halt/step debugging functionality in a network, and the creation of new techniques for the presentation and filtering of data collected by debugging tools as network size expands.