universal plug and play

connections

UPnP Enables Business Opportunities

Salim AbiEzzi, PhD., Microsoft Corp., Steering Committee Chair

Universal Plug and Play (UPnP) standards, in order to succeed, need to be driven by business entities. First, companies need to believe in a business opportunity that requires UPnP device standards. Then, these companies, together with their colleagues and partners, need to provide the resources and drive the development of the needed standards specifications.

It is my pleasure this quarter to report that the first such UPnP-enabled industry scenario–Internet Connection Sharing and Network Address Translation (NAT) traversal –is under deployment by several Internet gateway device vendors. Gateway devices employing NAT provide Internet connection sharing, assign port addresses to clients on a private LAN and provide home network security.

UPnP Forum member companies have worked together to create a specification in which applications or appliances running behind the gateway device can request port assignments on the gateway device and become visible and uniquely addressable from the Internet. Known as NAT traversal, this capability enables many in-home/Internet peer-to-peer networking applications, such as real-time communication and multi-player gaming, among others.

Intel Corp. and Microsoft Corp. championed this scenario to facilitate business opportunities. These companies sought a UPnP standard to enable appliances and applications on the home network to automatically discover, monitor, and control

The Internet Gateway Working Committee provided a place for participants to converge on a common specification. Forum members then created sample implementations to validate the proposed standard. The Forum's royalty-free terms and UPnP platform neutrality allow device vendors to implement the resulting specification with a low cost-of-entry.

As I write this in early June 2001, ARESCOM Inc., Buffalo Technology Inc., D-Link, Intel Corp. and Linksys Inc. have already announced support for the UPnP gateway specification in their future products. In addition, Microsoft Windows® XP will support both client and service sides of the specification so a PC running Windows XP can act as an Internet gateway and support this NAT traversal specification on behalf of applications and devices sitting behind the PC. This also means a Windows XP PC can connect to the Internet using one of these UPnP-enabled gateway devices and provide automatic connectivity support for the user. Interest in this new specification is high among gateway vendors.

Further good news is the recent announcements of UPnP software tools and device kit availability from Allegro Software Development Corp; Gatespace; Metro Link, Inc.; and Virata Corp. Each of these kits (see **www.upnp.org/resources.htm**) has unique strengths and features and usually provides support for multiple platforms. Based on indications from these tool ven-

under 128K in memory, which is an important consideration for device vendors.

The recent unanimous decision by the Consumer Electronics Association (CEA) R-7.4 Subcommittee to adopt UPnP for device discovery and control is another example of UPnP's acceptance.

Several Forum committees, including the Imaging Working Committee, have good momentum that may lead to the next industry-championed UPnP scenario. Let's work together to bring another scenario to consumers. And let's applaud the innovative progress from the Internet Gateway Working Committee and the companies supporting this Internet gateway effort! ▦

Welcome New Forum Members Since April 2001*

Allion Computer Inc.	Mobius Interactive
ARESCOM, Inc.	Netgear, Inc.
Cypress Systems Ltd.	NetTV
DH electronics GmbH	OpenGlobe, Inc.
eNabled Homes Pte Ltd.	Pioneer Research Center USA, Inc.
Gateway Inc.	PortalPlayer Inc.
Global Sun Technology Inc.	Sensormatic
Intersil	SerComm Corp.
Ipsil, Inc.	VSM Foundation (an association)
Lugh Networks	ZyXEL
Marrick Ltd.	

For a complete list of UPnP Forum members, please visit **www.upnp.org/forum/members.htm**.

* This list was accurate as of May 31, 2001, bringing total

Fifth UPnP Forum Summit– Coming October 2001

Arlene Binuya Murray, Microsoft Corp., Forum Project Manager

Please mark your calendars for the Fifth UPnP Forum Summit, currently scheduled for Thursday and Friday, October 18 and 19, 2001. Microsoft will host the event at the Microsoft Conference Center in Redmond, Washington. The UPnP Forum anticipates having several approved standards at that time. Internet Gateway Device, Digital (Security) Camera, Lighting, and Heating Ventilation and Air Conditioning (HVAC) are the strongest contenders.

The primary purpose of the event will be to provide opportunities for Forum members to broaden and deepen their understanding of UPnP for use in product development and planning. Attendees also find these events valuable for connecting with other UPnP Forum member companies on potential business opportunities.

We expect the event will showcase the UPnP products targeted for availability this holiday season and in early 2002. We also expect to be able to highlight the UPnP Certification and Logo Program at this Summit. Confirmation of the event will be broadcast to the interested community when plans are final. ▦

Third UPnP Forum Plug Fest

Arlene Binuya Murray, Microsoft Corp., Forum Project Manager

The third Forum-wide UPnP Plug Fest was held May 29 - 31, 2001. More than 40 engineering personnel from 12 companies participated in the three-day event at the Microsoft Interoperability Labs in Redmond, Washington. A critical objective was to run sample implementations of the Internet Gateway Device (IGD) against the UPnP Test Tool with the goal of arriving at Sample Test Complete (STC) status. Achieving STC will enable the Internet Gateway Working Committee to kick off the 45-day Forum-wide review period necessary for a Proposed Device Protocol (DCP) to become a standard. An additional gateway-specific Plug Fest may be held in June or July 2001 to bring the specification to STC status.

In addition to the IGD, other device categories tested included: UPnP toolkits and SDKs, a digital (security) camera implementation, printers, and various control points. Attendees were able to test their devices against a more mature version of the UPnP Test Tool than available in previous Plug Fest events. Participants were excited to be one step closer to achieving the first UPnP standard.

The next Forum-wide Plug Fest is tentatively scheduled for September 2001 and again will be sponsored by Microsoft at the Redmond campus. Confirmation of the event will be sent to Forum members when plans are final. ▦

Events and Partner Pavilion Opportunities

Fifth Universal Plug and Play Forum Summit

www.upnp.org

October 18 - 19, 2001

Microsoft Conference Center, Redmond, WA

For: Product/tool/component vendors

Cost: $3000 for booth space, power, Internet, signage, conference passes

Contact: **upnpevnt@microsoft.com** if interested in exhibiting, speaking, or sponsorship opportunities.

Electronic House Expo

www.ehexpo.com

Conference: October 24 - 27, 2001

Exhibits: October 25 - 27, 2001

Long Beach Convention & Entertainment Center, Long Beach, CA

For: Product/tool/component vendors

Cost: TBD

Contact: **upnpevnt@microsoft.com**

If there are specific events at which a member feels it important for the UPnP Forum to host a partner pavilion or industry events where UPnP demonstrations will be on display, please let us know by contacting upnpevnt@microsoft.com.

Please additionally check www.upnp.org/calendar. htm for a regularly updated Forum

Technical Committee: UPnP Security Progress Report

Toby Nixon, Microsoft Corp. , Technical Committee Chair

Toby Nixon (tnixon@microsoft.com) was recently appointed by the Steering Committee to chair the Technical Committee, so that Jeffrey Schlimmer, chief architect for UPnP, can focus full-time on architectural issues. Toby has been with Microsoft since 1993 and has 26 years experience in networking technologies and standards activities.

The Technical Committee is actively engaged in identifying UPnP device security requirements, with the intent to develop security solutions that will be incorporated into a future update to the UPnP specifications. The accelerating rollout of always-on Internet connections such as cable modems and DSL has increased the urgency of identifying and addressing security as an integral part of UPnP.

UPnP was originally designed for the relatively benign security environment of a typical home–specifically, one that was not continuously connected to the global Internet. However, as with any Internet-based protocol, UPnP is susceptible to various security threats.

A variety of countermeasures may be employed to address security threats, including encryption, authentication (requiring users or devices to prove who they are), access control and authorization (granting permission to only particular users to do certain things), digital signatures (which ensure a message was actually sent by whomever it claims sent it) and message integrity checking (ensuring a message wasn't altered in transit), among others.

Because of its original design goals, UPnP does not directly implement these countermeasures. Instead, it assumes that measures such as network isolation (gateways, firewalls, and proxies), MAC layer encryption (provided by the network adapters), and physical access control will

be employed to protect not only UPnP traffic, but also the rest of the home network.

As work on UPnP has progressed, however, the Forum has increasingly recognized that depending on these separate measures alone may not be sufficient to address all scenarios of interest.

A variety of usage scenarios are being considered in the course of analyzing threats and identifying security requirements. These include the following:

• Preventing unauthorized persons from using home wireless powerline or telephone networks to discover which devices are in a home or to learn how to disable the burglar alarm system.

• Preventing misuse of equipment by neighbors who may have similar networks.

• Enabling users to add new, secure devices to their networks and use them immediately, without difficulty or specialized knowledge, while maintaining the ability to use unsecure devices previously installed.

• Enabling homeowners to remotely access, control, and monitor their home equipment over the Internet, while at work or on vacation, using a generic web browser such as an airport kiosk or hotel-room terminal.

• Enabling service providers such as electric utilities to securely access, control, and configure equipment, such as power meters, in the home over the Internet.

• Granting access to sensitive information and functionality to specified individuals or groups; for example, controlling the ability to view digital audio or video content based on ratings, controlling when children may access the Internet through a gateway, or restricting use to expensive resources such as high-quality photo printers.

• Allowing guests in the home to temporarily use selected equipment such as a printer, Internet connection, or video display, without exposing the entire network to discovery or use.

• Allowing equipment, such as laptop computers, to be brought from the office, where they may be part of an enterprise network security scheme, and connected to equipment in the home, such as printers and scanners.

• Allowing UPnP-enabled equipment, such as digital cameras, from the home to be taken to the office and used with computers there, without interfering with enterprise security or becoming visible to others on the network.

• Allowing use of UPnP-enabled equipment in public facilities, such as printer kiosks in airports, protecting the service providers from fraudulent use and protecting sensitive information on the UPnP equipment.

The Technical Committee is studying specific countermeasures mentioned above in order to identify those most appropriate for use with UPnP, taking into consideration the unique characteristics and limitations of many UPnP devices–such as severe constraints on computational power, memory, and bandwidth–the need for simplicity in installation and management, backward compatibility, the use of well-known and accepted standards, and favorable intellectual property rights.

Some areas of security have been deemed outside the scope of UPnP and will not be addressed in this work. These include digital rights management (copyright protection of media content), and security of the platforms on which UPnP devices or control points may be implemented (e.g., validation of executable code). These areas may be addressed in relevant device control protocols or left to the implementer. ▓

Forum member companies made several important UPnP-related product announcements this quarter, including a number of announcements related to UPnP support for Internet gateway devices that are scheduled for commercial availability in 2001. These efforts represent solid progress in the adoption of UPnP and toward the goal of making "it just works" a mainstream reality in home networking.

Study after study indicates that sharing a common connection to the Internet remains the primary reason why people establish a home network. Because of this, it is especially important that UPnP provide value in this scenario by enabling Network Address Translation (NAT) traversal.

Here is a summary of news, in alphabetical order by company name.

ARESCOM to Include UPnP Support

Ken Wang, ARESCOM Inc., Forum Member

ARESCOM, a global provider of broadband infrastructure equipment for telecommunications carriers, ISPs, small office/home office, and multi-tenant units, announced plans to include UPnP support in its DSL and cable gateway products beginning in the second half of 2001.

For more information please visit www.arescom.com.

Buffalo Technology to Include UPnP Support in its Wireless Gateway

Kenny Lam, Buffalo Technology Inc., Forum Member

Buffalo Technology Inc. (USA), developer of AirStation wireless networking and Internet sharing devices for home, small office/home office and small business, has announced support of UPnP, targeting availability in October 2001. The company's AirStation WLAR-L11-L access point will support the UPnP standard, enabling a much easier set up process, particularly for AirStation units installed in conjunction with Microsoft Windows® XP operating system.

UPnP-enabled Internet gateways will help home and small business broadband customers seamlessly run multi-user network gaming, real-time communications experiences such as Windows Messenger, remote PC assistance, and other peer-to-peer applications by uniquely identifying PCs or devices sharing a broadband connection.

For more information please visit www.buffalotech.com.

Consumer Electronics Association (CEA) R-7.4 Chooses UPnP as Automation Protocol

Robert Lembree, Metro Link, Inc., CEA R-7.4 Working Group 6 Chair, Forum Member

The Consumer Electronics Association (CEA) Joint CEA/VESA (R-7.4) Subcommittee has chosen UPnP as the base protocol in its Versatile Home Network (VHN) specification. UPnP brings a rich set of features to VHN that are crucial to home networking. Handling all aspects of addressing, device discovery, eventing and control, UPnP will serve as a foundation for VHN's more advanced features.

The CEA has a cohesive strategy for compatibility of various home networking protocols, with the VHN as the centerpiece tying clusters together. The choice of UPnP as the base protocol allows VHN to leverage the strengths of UPnP and achieve compatibility with UPnP devices and control points. In return, VHN will provide standards that build upon UPnP, particularly in the areas of distributed audio and video, network security and network architecture.

The CEA R-7.4 Working Group 6 (WG6) is chartered with the task of integrating UPnP into the VHN specification, which is expected to be completed by Fall 2001.

VHN specifies media, bridges, and access points, as well as other network components. VHN has chosen IEEE 1394b over CAT 5 or fiber as the backbone for the home network, taking advantage of various network media features, such as IEEE 1394b's ability to guarantee bandwidth to an application.

VHN adds to UPnP the security, network management, user interface, and streaming Quality of Service (QoS) layers needed to access outside services and distribute entertainment in the home.

The ability for all VHN devices to interoperate with UPnP devices brings a significant convergence to the home networking industry, which is driven by Internet access and entertainment opportunities. VHN and UPnP together provide manufacturers, software developers and service providers the necessary tools, stability and direction to begin developing their products with confidence in the standards implemented by their products.

With over 600 members, the CEA is accredited by ANSI and authorized to write American National Standards. CEA is the only open, consensus-based standards developing organization (SDO) that is actively engaged in home networking standards.

For more information please visit www.ce.org.

D-Link Supports UPnP in Residential Gateways through Windows XP

Brad Bester, D-Link Systems, Inc., Forum Member

D-Link will incorporate UPnP technology to make home networking and broadband Internet sharing easier than ever, expanding the security, ease of use, and Internet sharing capabilities of its residential gateway products. D-Link will offer this UPnP technology as a free upgrade to its currently available gateway models later this year and as an added feature to future products beginning in September 2001.

The upgrade will be optimized to take advantage of new home networking enhancements included in the Microsoft Windows® XP operating system. By adhering to the UPnP Device Architecture version

1.0 guidelines, D-Link will provide a new class of residential gateway that will leverage the UPnP support in Windows XP to create a more enjoyable home networking experience for users.

Both the industry and users will benefit from this new D-Link technology as it expands the market for home networking past the early adopter to the general consumer.

For more information please visit **www.dlink.com.** ⊞

Intel Offers UPnP DSL Gateway Device

Roger Chandler, Intel Corp., Forum Member

Intel Corporation, a leading manufacturer of networking and communications solutions, will offer a UPnP-enabled DSL Gateway product scheduled to begin shipping in July 2001. The new product, Intel AnyPoint™ DSL Gateway Model 4200, will help service providers improve the customer installation experience, lower installation costs, reduce ongoing support costs, and increase revenue streams. Optimized for home and small office environments, the gateway will provide greatly simplified setup and usage via UPnP and other technologies.

Intel will continue to de-mystify networking for home users through UPnP. Future residential gateway products from Intel will enable users to transparently add new devices to a home network and share network resources. Users will be able to easily share a broadband connection between multiple PCs and other connected devices for real time communications, digital entertainment and gaming.

Intel currently chairs the Internet Gateway Working Committee and has helped to promote industry adoption through sponsorship of UPnP Plug Fest events and industry education. Last year the Intel Architecture Labs released a free, open source UPnP SDK for Linux-based connected device manufacturers incorporating UPnP into their products.

For more information please visit **www.intel.com/home/dsl/dslgateway.htm.** ⊞

developer tools

UPnP Used to Assist Persons with Disabilities

Mike Friedman, Microsoft Corp., Forum Member

"Victoria" is the Microsoft™ codename for a technology that improves the accessibility of UPnP devices for persons with disabilities. The new technology facilitates the use of a custom user interface – text-based, speech-based, Braille-based, or other–hosted on a device such as a Personal Digital Assistant (PDA) or other computer.

Created by the Microsoft Accessible Technology group, "Victoria" is based on the idea of Universal Console (UC) software. UC software appears to the target UPnP device as a UPnP V1.0 control point. The software controls UPnP devices at home, at work, and while traveling.

In the UPnP architecture, the target device directs a control point to the URL of the service's user interface. Under the "Victoria" paradigm, the URL points to an XML document that contains an abstract representation of the service's user interface. The UC software transforms the abstract user interface into a concrete user interface accessible to the person with disabilities.

Manufacturers will find "Victoria" easy to implement–a manufacturer commissions an author/developer to create a single XML document for a UPnP service. The resulting document can serve customers with a wide variety of disabilities and combinations of disabilities. An operating system could include a basic UC that accommodates common disabilities. Vendors can create full-featured UCs for specialized markets. A custom UC can be developed for an individual with an unusual combination of disabilities.

"Victoria" works with conventional UPnP devices, as well as ATMs, kiosks, and other devices and software applications. Microsoft has submitted a draft standard based on the Victoria technology to the National Committee for Information Technology Standards (NCITS).

The Microsoft Accessible Technology group is seeking a variety of UPnP devices to use in prototyping "Victoria," with potential commercial availability of "Victoria"-enabled products in 2002.

For more information please contact **vicprj@microsoft.com.** ⊞

Gatespace Builds Bridge Between UPnP and OSGi

Staffan Truve, Gatespace , Forum Member

Gatespace, a provider of open standards-based distributed service platforms for developing and delivering network-based services, announced at Parks Connections 2001 in May that the company is adding support for UPnP to its portfolio of OSGi-based (Open Services Gateway Initiative) products. The Gatespace platform now allows service gateways to discover and control UPnP-enabled devices on local networks. At the same time, UPnP devices can discover and control OSGi-based services executing on a service gateway.

The Gatespace OSGi/UPnP connectivity product allows service developers to provide distributed services that securely and reliably tie together UPnP devices and OSGi services on different gateways and local networks. This approach simplifies the development of many services focused on content delivery, network-based storage, and remote management, among others.

For more information please visit **www.gatespace.com** or call **650-846-6580.** ⊞

Virata Releases EmWebUPnP for Networked Devices

Philip Poulidis, Virata Corp., Forum Member

Virata has released EmWeb®UPnP, a turnkey multi-platform UPnP software for embedded devices. Based upon the highly-efficient and patented EmWeb architecture, EmWebUPnP allows system developers to easily add cutting-edge network control to products, while saving development time and expense.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.

fastcase
Smarter legal research.