

By Ben Sheppard
Worldwide RGES
Marketing Manager
bsheppard@ti.com

By D'Andre Ladson
RGES Product Line Manager
dladson@ti.com

Remote Management: Critical to a New Generation of Digital Service Providers

Introduction

Increasingly, service providers are transitioning their services to Internet Protocol (IP) networks to win more customers with sophisticated leading-edge services and to increase customer loyalty by offering new services, such as bundled triple-play offerings and IP television (IPTV). Unfortunately, these new services can wreak havoc on balance sheets by driving up service and support costs.

Addressing these challenges with remote management systems can be seen as a bane or as a boon to service providers. Certainly technical challenges abound, but the savvy service provider will be able to transform the challenges into an opportunity to stand apart from the competition in an extremely competitive marketplace. And some enterprising service providers will no doubt develop a viable business model to turn their service and support programs from a cost drain into a revenue generator.

Considering the competitive situation and tighter operating margins service providers face, remote management has emerged as a critical technology for the future.

Service providers are charging headlong into uncharted waters. The broadband DSL marketplace is growing rapidly, but at a price. Specifically, pricing on DSL service is dropping to fuel continued growth and to fend off stiff competition from cable operators (MSOs), satellite TV providers and even Internet Service Providers (ISP). Tighter business margins place a greater importance on operating efficiencies. As a result, service providers are taking a close look at reducing variable operating costs in order to maintain acceptable operating margins. Of course, service and support are prime targets for cost reductions.

Simultaneous with this drive to cut costs, service providers are transitioning their services to IP networks as a way to win more customers with sophisticated leading-edge services and to increase customer loyalty by offering a so-called “triple-play”—voice, data and video services. New services like bundled triple-play offerings and IPTV are essential to service providers’ prosperity, but, unfortunately, they can wreak havoc on balance sheets by driving up service and support costs.

Telecommunications service providers are well aware of the benefits of remote management, having implemented the concept for years in the backbone public switched telephone network (PSTN). Now though, new broadband-based services are extending the purview of service providers well beyond the demarcation point and into the midst of a wide range of customer premise equipment (CPE), including residential gateways (RG), set-top-boxes (STB), Voice over IP (VoIP) phone systems, digital television sets, gaming consoles and many others. New technologies and methodologies to efficiently and remotely manage, control, configure, troubleshoot and provision the network and CPE devices are imperative.

Addressing this situation with remote management systems can be seen as a bane or as a boon to service providers. Certainly technical challenges abound, but the savvy service provider will be able to transform the challenges into an opportunity to stand apart from the competition in an extremely competitive marketplace. And some enterprising service providers will no doubt develop a viable business model to turn its service and support programs from a cost drain into a revenue generator.

These are critical times for service providers as they undergo the ultimate makeover, transforming themselves from analog voice-oriented providers to a digital world with its myriad of new and exciting service possibilities. The good news for service providers is the fact that the broadband market is undergoing explosive growth and DSL is growing faster than any other access method. According to the market research firm Point Topic and the DSL Forum, DSL services accounted for three-quarters of the worldwide growth of broadband during the first six months of 2005. Service providers want to keep this growth rate going, and they are doing all that they can to make sure it continues. Unfortunately, expanding markets attract competition but the competitive pressure service providers now face in the digital broadband world is nothing like the competitive environment of the voice-centric telecommunications marketplace in years gone by.

At the same time, new digital service offerings bring the challenge of incorporating new technologies, applications and previously unforeseen devices into the service providers' networks. Managing transport networks is something telecom service providers have done and are quite adept at, but more and more the services offered by service providers will involve operator-managed CPE equipment like RGs and STBs, connected to systems such as multimedia appliances, HD televisions, home theaters, DVD players, phone systems, personal computers and many others. Besides the effects these devices have on the performance of the network itself, consumers often turn to service providers when a device malfunctions.

Success in rapidly expanding markets with evolving technologies, fierce competition and aggressive new entrants will likely hinge on a company's operating efficiencies. The companies that can control operating costs, manage their growth effectively and maintain adequate margins will be best positioned to capitalize on marketplace opportunities.

Remote management—the ability of a service provider to manage or, at the very least, monitor CPE devices connected to the network—will be critical for service providers who must realize highly efficient service, support and maintenance operations in order to compete effectively. Besides managing devices like RGs that are connected directly to their broadband networks, service providers must also be concerned about managing or monitoring consumer electronic (CE) devices connected to the RG or whatever sort of hub there is in the home network. As a result, any remote management standard must be able to identify and manage many different types of CE devices that were simply purchased in retail outlets. In addition, the service provider's remote management standard also must be able to work with any of several home networking management methodologies.

Other important service provider issues for an industry-accepted standard for remote management are the openness of any such standard, its security and its scalability. An open remote management standard would draw on other open standards that service providers have accepted and deployed, such as SOAP, XML, HTTP and, of course, TCP/IP. The security of any mechanism that has access to private home networks and the devices connected to them is of paramount importance. Encryption algorithms, security protocols, key management techniques, authentication methods and other aspects of air-tight security must all be considered in the development of a remote management standard. And certainly service providers who plan on growing their subscriber base by offering new IP-based services will be concerned about the scalability of their remote management technologies.

Fortunately, the industry is addressing the issue of remote management with efforts like the DSL Forum's DSLHome initiative and the TR-069 standard, its extensions and other technologies. Much has been learned over the years from related technologies such as the transport-oriented Simple Network Management Protocol (SNMP) and the PC-centric/local networking Universal Plug 'n Play (UPnP) technology, even though these methodologies do not provide the same kind of end-to-end visibility and control that is needed by service providers. The future of open, interoperable remote management clearly is centered on TR-069 and its related standards.

Extending the Hockey Stick

At a time when telecom service providers can celebrate the rapid growth of DSL, they also face the discomfoting realization that revenues from their more traditional services like wireline voice and long distance have stagnated or are falling. Mobile wireless telephone service is making serious inroads into these areas. Providers are trying to reverse this revenue trend by launching new services based on digital broadband and IP technologies. The big question is: How will this rapid shift in services and technologies affect the service providers' business model?

In the broadband access marketplace, service providers are running into significant competition from cable operators, satellite TV providers and ISPs. Traditional telecom companies are taking a number of actions to not only retain, but also expand their market share. One area of expansion is IPTV services. Unfortunately, formidable competitors like Google and Yahoo! also have stated that they intend to enter the IPTV marketplace as well. All of these events and eventualities have significant implications for service providers' business models.

Restructured Pricing

To compete aggressively while expanding the size of the marketplace, many service providers are restructuring their subscription rates. Other technology markets have shown that early adopters of new products and services are more willing to absorb higher costs. By lowering prices, service providers are reaching out to an entirely new audience for their DSL services. In addition, the early adopters of broadband services were in all likelihood more technically adept than most consumers. This new group of consumers for whom broadband DSL is now economically available will require a higher level of support and hand-holding since they are less knowledgeable. Moreover, by lowering the cost of admission to the broadband DSL market, providers will be adding subscribers who may be less loyal because they are more value-conscious. New consumers drawn into the market will be more apt to switch service providers at the first hint of dissatisfaction.

Bundles of New Services

Rather than calling it a “triple-play”, it might be more accurate to call bundled voice, data and video service offerings a home run for service providers. Providers hope that triple-play bundles solidify their position in the home to the exclusion of other broadband operators like the cable companies who are trespassing on the telecom providers’ turf by offering VoIP services. Assuming consumer satisfaction remains relatively high, triple-play offerings can improve subscriber loyalty, reduce churn and increase the average revenues per user (ARPU), reversing the slippage in ARPU providers have suffered in recent years. Of course, much of this logic hinges on whether service providers can maintain high customer satisfaction. Deploying real-time, bandwidth-hungry applications such as video and IPTV raise Quality-of-Service (QoS) issues for providers. No consumer would remain with a provider for long if voice calls were dropped every time a television was turned on in the house.

Boxes, Boxes Everywhere...

Increasingly, service providers’ broadband pipes will terminate into home networks connected to a wide variety of devices, including new types of digital media appliances and players, voice systems, consumer electronic products like gaming consoles, TV sets, MP3 players, digital still cameras and home theaters, desktop and laptop computers, and many others. Once the service provider’s support and service mechanisms are in place, a new business model centered on supporting home networks could emerge as a viable revenue generator. Of course, the viability of such a model will depend upon the efficiencies of

the provider's service and support programs. High-touch, manually-intensive support services could not be priced at a level to attract the new wave of value-conscious subscribers entering the marketplace.

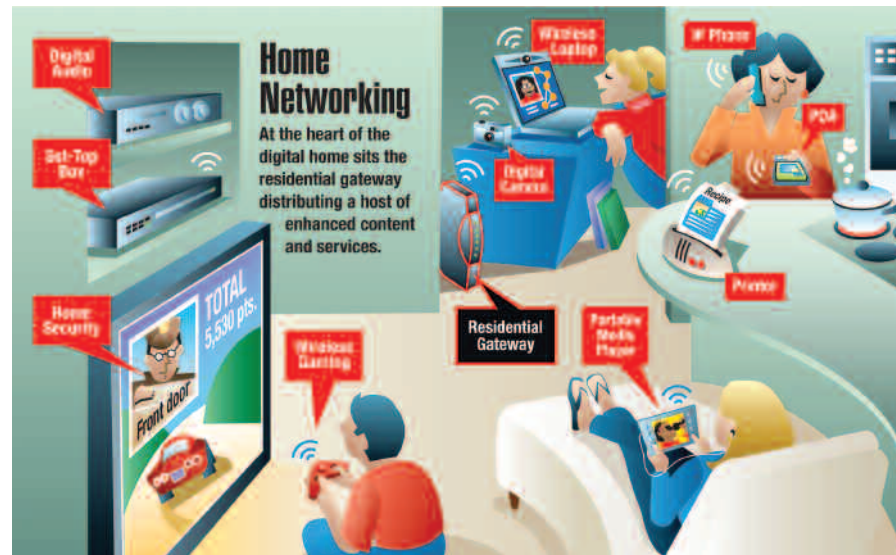


Figure 1

Another Dimension to Remote Management

Remote management as an integral concept for telecommunications service providers is not new. Indeed, it has been around for many years. What has changed is the digital nature of the networks, the myriad of new types of devices that have joined telephones on service providers' networks and the desire by service providers to expand in terms of number and reach into the home or place of business the services they offer. In the case of IPTV and VoIP, for example, service providers are responsible for services well beyond the demarcation point where the broadband pipe enters the home or office.

Considering the competitive situation and the tighter operating margins service providers face, remote management has emerged as a critical technology for the future. Moreover, the revenue growth potential for broadband services as well as the new media services they deliver increase the stakes exponentially. The opportunity is too big to miss.

Just as service providers are transitioning from a world dominated by analog to the contemporary digital world, so too the role of established remote management technologies is transitioning as they become complementary to newer, more comprehensive technologies, such as those based on the DSL Forum's TR-069 specification and its extensions.

Transitioning

For IP-based transport networks, the SNMP had been deployed extensively to monitor the performance, load and other operating parameters of switches, routers, servers and systems that are essential to the backbone of the Internet as well as large enterprise-wide virtual private networks (VPN). SNMP-generated data can be very useful to network administrators

who wish to evaluate a network's performance and identify traffic bottlenecks or potential bottlenecks. This type of information is also helpful in designing or re-designing networks.

Because SNMP was first specified in the late 1980s during the early days of the Internet, the security mechanisms built into Version 1 were not particularly strong or effective. Subsequent versions of SNMP have improved its security features and performance.

At the other end of the scale from the backbone of the Internet, small-scale IP-based networks in the home often employ UPnP as a control mechanism. Originally envisioned for transparently connecting peripheral devices to PCs, UPnP has evolved into a peer-to-peer architecture. Part of the beauty of UPnP is its ease-of-use for consumers. New devices automatically join a home or small office network and they are "discovered" by the other devices already participating in the network. Some UPnP networks are unmanaged in the sense that there is no Dynamic Host Configuration Protocol (DHCP) server present on the network. When this is the case, a device joining a UPnP network must assign itself an IP address. Security, or lack thereof, can also be a vulnerability in UPnP-based home networks.

For service providers who need remote management tools that traverse the Internet and give visibility into home networks all the way to termination devices, SNMP is seen as inadequate. To some degree, it could complement the capabilities of TR-069, but it doesn't provide the control, configuration and management features that are required now or in the future. On the other hand, UPnP is limited to control issues on local area networks (LAN), not wide area transport networks.

End-to-End Remote Management

The name of the DSL Forum's TR-069 specification, "CPE WAN Management Protocol," clearly states that it has been defined to provide management mechanisms that span the operator's wide area network (WAN) and provide a bridge to CPE devices, many of which will be located on a home or small office LAN. In general, the capabilities provided by TR-069 include secure auto-configuration and management functions for the DSL CPE device. The specification is an open standard and, as such, it is agnostic to the type of end device and its manufacturer. Specifications complementary to TR-069 are being developed to accommodate management and control functionality beyond the broadband access device to another layer of CPE devices connected directly to the broadband access device or to a LAN.

Specifically, the primary functionalities provided by TR-069 include the following:

- Auto-configuration and dynamic service provisioning
- Software/firmware image management
- Status and performance monitoring
- Diagnostics

The architecture of TR-069 includes an Auto-Configuration Server (ACS), which communicates with the DSL CPE using the TR-069 protocols (Figure 2). With TR-069, the DSL CPE can be provisioned when it is first connected to the broadband network. Later, it can be re-provisioned remotely over the network as-needed.

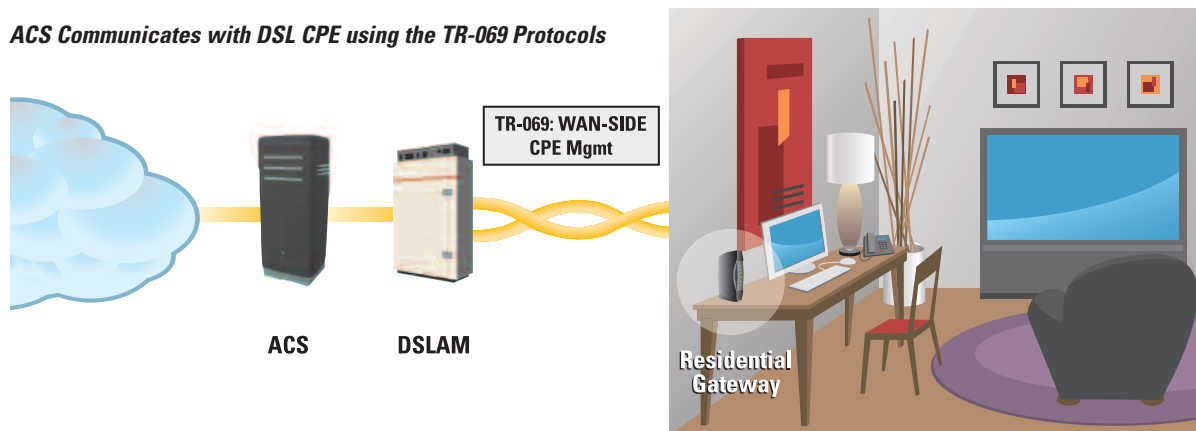


Figure 2

Should a service provider wish to monitor the performance or service status of the DSL CPE, TR-069 supports functionality whereby the DSL CPE can send statistics to the ACS. TR-069 defines a broad set of operational parameters for these purposes, or vendors and network operators can add their own parameters. These parameters can also be applied to diagnostic applications, which attempt to determine the cause of connectivity malfunctions or service degradations. In addition, operators are able to define certain conditions that will trigger a notification from a DSL CPE to the ACS, should changes occur in the DSL CPE's performance or its operating environment.

Managing deployed software or firmware can be a costly and time-consuming process for service providers. TR-069 includes functionality for downloading software images to individual DSL CPEs or, in a broadcast mode, to multiple CPEs at once. In addition to checking the version of the software or firmware already in place, this mechanism will also notify the ACS whether the download was accomplished successfully or if it failed. As an added degree of security, providers can also require that any download be digitally "signed" before it is loaded into a CPE system. This process is intended to authenticate that the download is coming from the service provider and not a hacker or intruder of some sort.

TR-069 security measures can also be scaled to the devices connected to the DSL CPE. If the resources of less robust devices would be severely taxed by complex security algorithms, simpler security measures can be deployed. For robust devices where sensitive personal information is more likely to be stored, stronger and more complex security measures can be implemented.

The TR-069 specification also includes a number of optional tools for managing services or applications involving connected devices and payment processes that require extra strong security measures. TR-069 defines so-called digital “vouchers” which can be used to authenticate the parties to a transaction. Other security measures are designed to prevent tampering and theft of CPE boxes, and to maintain the confidentiality of communications between the ACS and any CPE system.

A number of extensions to the TR-069 specification are currently under development by the DSL Forum. These documents define how certain types of devices can be remotely managed with TR-069 through the DSL CPE. Services such as auto-configuration and management functions included in TR-069 will be able to pass through the DSL CPE to connected devices such as VoIP phones and systems (TR-104 and TR-110), STB and gaming consoles.

DSL Leadership

Texas Instruments (TI) has been a longtime leader in the development of the TR-069 specification and other standards of the DSL Forum. The company’s current DSL solution—AR7, and its next-generation architecture, UR8—both conform to the requirements of TR-069 and its extensions.

The UR8 architecture serves as the foundation for an entire family of residential gateway solutions that support the remote management capabilities needed by service providers as they transition to new business models. The UR8 architecture is an open platform with exceptional voice capabilities, high-performance data communications, and advanced multimedia and video processing.

In addition, TI has applied its many years of experience working with service providers and their equipment suppliers to develop PIQUA™ technology, an advanced system of quality management elements that gives service providers and network management vendors real-time information on the functioning of IP networks at every level. Because TI silicon, software and intellectual property are embedded throughout IP networks from CPE systems through the switches and routers that make up the IP network, TI can play a critical role in helping to remotely manage these networks. The information from PIQUA technology gives service providers the ability to effectively manage both their QoS and the efficiency of their operations. With PIQUA technology, operators have a new level of visibility into their IP networks and connected CPE systems.

TI’s Residential Gateway Solutions: www.ti.com/ar7

TI’s PIQUA technology: www.ti.piqua

Piqua is a trademark of Texas Instruments.
All other trademarks are the property of their respective owners.

© 2006 Texas Instruments Incorporated
Printed in the U.S.A.
♻️ Printed on recycled paper.



SPAY026

IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, modifications, enhancements, improvements, and other changes to its products and services at any time and to discontinue any product or service without notice. Customers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All products are sold subject to TI's terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its hardware products to the specifications applicable at the time of sale in accordance with TI's standard warranty. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by government requirements, testing of all parameters of each product is not necessarily performed.

TI assumes no liability for applications assistance or customer product design. Customers are responsible for their products and applications using TI components. To minimize the risks associated with customer products and applications, customers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any TI patent right, copyright, mask work right, or other TI intellectual property right relating to any combination, machine, or process in which TI products or services are used. Information published by TI regarding third-party products or services does not constitute a license from TI to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

Reproduction of information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. Reproduction of this information with alteration is an unfair and deceptive business practice. TI is not responsible or liable for such altered documentation.

Resale of TI products or services with statements different from or beyond the parameters stated by TI for that product or service voids all express and any implied warranties for the associated TI product or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

Following are URLs where you can obtain information on other Texas Instruments products and application solutions:

Products		Applications	
Amplifiers	amplifier.ti.com	Audio	www.ti.com/audio
Data Converters	dataconverter.ti.com	Automotive	www.ti.com/automotive
DSP	dsp.ti.com	Broadband	www.ti.com/broadband
Interface	interface.ti.com	Digital Control	www.ti.com/digitalcontrol
Logic	logic.ti.com	Military	www.ti.com/military
Power Mgmt	power.ti.com	Optical Networking	www.ti.com/opticalnetwork
Microcontrollers	microcontroller.ti.com	Security	www.ti.com/security
Low Power Wireless	www.ti.com/lpw	Telephony	www.ti.com/telephony
		Video & Imaging	www.ti.com/video
		Wireless	www.ti.com/wireless

Mailing Address: Texas Instruments
Post Office Box 655303 Dallas, Texas 75265