

# TR-069 Interoperability: The Real Story

---

May 2005



Fine Point Technologies, Inc.  
139 Centre Street  
Sixth Floor  
New York, NY 10013 USA  
+1.212.962.7410  
[info@finepoint.com](mailto:info@finepoint.com)

© 2005 Fine Point Technologies, Inc. All rights reserved.

The information contained in this document represents the current view of Fine Point Technologies, Inc. on the issues discussed as of the date of publication. Because Fine Point Technologies must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Fine Point Technologies, and Fine Point cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. Fine Point Technologies Makes No Warranties, Express or Implied, In This Document..

Microsoft, Outlook, Windows, and Windows NT are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Fine Point Technologies, Inc. • 139 Centre Street • New York, NY 10013 • USA

## INTRODUCTION

---

We are witnessing the emergence of second generation remote CPE management systems.

The first systems were proprietary; not based on widely accepted standards and methods; meaning management systems from one vendor do not fully manage CPE from another vendor. While this offered the service provider the management capabilities they required, it locked them into CPE from a specific vendor and locked them out of competitive bidding for functionally equivalent systems.

The release of TR-069 by the DSL Forum and the wide and rapid adoption of this specification by service providers is evidence of the pent up demand for a management standard that is open and applicable to widely available, commodity hardware.

## Pain Points

The three main problems facing Service Providers in the DSL space are high customer acquisition costs, high churn rates and declining average revenue per subscriber. According to DSL industry expert Dave Burstein, the average Service Provider pays \$300 to acquire each new residential customer. A significant component of this high acquisition cost is the truck roll (where a trained technician is sent to the customer's site to install and configure the device). According to data published by Turnstone Systems, 95% of all new customers attempt to self install their equipment and while 85% of those customers, or roughly 80% of all new customers are successful, the balance require a truck roll. Burstein also reports that the industry average for customer churn rates (rumored on Wall Street to be as high as 5% per month for some providers) is 3.3% per month or almost 40% per year.

## Interoperability Questions

The promise of TR-069 is grand: Plug and play installation and activation onto the network of a wide array of complex networking and computing devices, all remotely managed by a service provider. However, with any new standard, there is a learning curve associated with it as best practices and implementations evolve. This evolution is often manifest by confusion in the market regarding implementation and interoperability.

This was shown in the early PC Clone Wars, and again in the IP Stack Wars.

There appears to be enough room in the TR-069 specification that is open to interpretation to create some interoperability issues as well.

The intent of this document is to provide some background and understanding behind the core functions of TR-069, uncover some areas of difficulty that Dimark has encountered in its work with CPE vendors, software and firmware developers, chip manufacturers and management systems developers. In addition, the steps Dimark takes to test and certify CPE to ensure the full function of the specification is supported will be discussed.

## TR-069 OVERVIEW

---

Those who have read the TR-069 specification will recognize much of the following information. However, it is important to understand the intent and resulting complexity of TR-069. It is also important to understand that while TR-069 offers significant value “out of the box,” the primary value of TR-069 is that it established a standard communications protocol to enable a wide variety of additional functionality be delivered to CPE and remotely managed and serviced.

Beyond establishing this communications structure, TR-069 supports the following primary CPE management capabilities:

- **Auto-configuration and dynamic service provisioning** - This mechanism allows CPE auto-provisioning at the time of initial connection to the broadband access network, and the ability to re-provision at any subsequent time. In short, this allows router/gateway CPE (as opposed to a simple bridge/modem CPE) to be shipped to and successfully installed by the end-user subscriber.
- **Software/firmware image management** - TR-069 provides tools to manage downloading of CPE software/firmware image files. The protocol provides mechanisms for version identification, file download initiation (ACS initiated downloads and optional CPE initiated downloads), and notification of the ACS of the success or failure of a file download.
- **Status and Performance Monitoring** - TR-069 provides support for a CPE to make available information that the ACS may use to monitor the CPE’s status and performance statistics. The protocol defines a common set of such parameters, and provides a standard syntax for vendors to define additional non-standard parameters that an ACS can monitor. It also defines a set of conditions under which a CPE should actively notify the ACS of changes.
- **Diagnostics** – TR-069 provides support for a CPE to make available information that the ACS may use to diagnose connectivity or service issues. The protocol defines a common set of such parameters and a general mechanism for adding vendor-specific diagnostic capabilities.

It is easy to see why Service Providers are embracing TR-069: It immediately provides standards-based resolution of two of their primary pain-points while simultaneously enabling the use of commodity and competitively sourced CPE.

## Interoperability

For all the promise of interoperability, TR-069 implementations still have a way to go. While the specification itself is fairly well written, there is room for interpretation and error during the implementation in CPE. For example, there is a typo in the specification where a common word, used to define a field is misspelled. Does the vendor take the specification at its literal meaning, or does the vendor correct the spelling error?

Another issue is the SOAP implementation. SOAP, Simple Object Access Protocol, is the communications protocol used by TR-069. The process of remotely executing commands is called Remote Procedure Call (RPC). There are many issues involved ensuring RPC works properly and reliably. For example, transmitting data and management commands across a network to a remote device may or may not be up or responding, is tricky.

Why use SOAP, when there already are so many other standards to choose from? In one word, simplicity. Each of the other protocols does a lot more and carries a lot more overhead, which may be problematic in the limited CPU, RAM and FLASH world of CPE. If basic functionality, independent of hardware and operating system is what’s required, SOAP is the best solution.

SOAP uses XML to encapsulate the data that needs to be sent to and from the remote device. Any mode of transport can be used for SOAP calls, although HTTP will probably be the most popular, which means that TR-069 will work within the existing infrastructure and Internet security mechanisms: That's one sign of a well-designed protocol -- it can be used cleanly in new circumstances.

The TR-069 specification requires that all communications between the CPE (client) and ACS (server) are done via a persistent connection. However SOAP was designed for one way communications where the roles of client and server are clearly defined. By requiring a persistent connection, TR-069 is switching these roles during communications, something SOAP wasn't designed to do and introducing complexity to a "simple" protocol.

As a result of this shift, developers of TR-069 CPE client software are required to develop their own SOAP implementation. This has caused problems on how different SOAP implementations interpret the SOAP messages. Normally the handling functions are defined during product development and the rest is automatic. However, in the current specification it is necessary for the SOAP to be generated manually; a process highly prone to errors. [Download a TR-069 optimized client SOAP library from <http://www.dimark.com/partners/gsoap.tar.gz>].

For this reason the ACS requires cookies to maintain the identity of the client in the message stream. While it is possible for TR-069 to function without cookies, it will be at the cost of scalability and performance.

## Testing

The process we follow in validating CPE entails connecting the CPE to the ACS and testing the ability of the ACS to provision, manage and log data from the CPE.

Should any problems arise, we carefully evaluate the SOAP communications stream by intercepting the TCP data. Once the issue is identified, we forward our results to the CPE vendor and take three paths in correction:

1. If the error exists in CADM, the correction is applied to the ACS as a top engineering priority.
2. If the error exists in the CPE, but can be worked around in the ACS, we add this to the ACS. If possible, we will also move the CPE vendor to Stage 3 (benefit here is we can certify the CPE quickly instead of the slow turns that CPE vendor corrections require). We have one vendor who did not want to do any more TR-069 work; their CPE is certified for CADM through a work-around that, while outside the specifications, can be accommodated. What this does is limit that particular CPE vendor, but CADM is able to fully manage the device.
3. If the error exists in the CPE and isn't something that can be corrected by a simple work-around, we provide the CPE vendor with the SOAP structure that is at fault, an example of the expected SOAP structure, pointers to the specific chapter and verse in the specification that defines this section (to validate that we are correct in our assessment that the fault is with the CPE and not a Stage 1 correction). We then work closely with the CPE vendor to help them sort out the problems, and provide ongoing testing and expert advice. In some cases, we have corrected CPE vendor's source code.

## Results and Abilities

In light of these issues, when evaluating an ACS, it is important to consider the technical skills of the ACS vendor. Do they have the capabilities to troubleshoot and work with vendors in the CPE community? Part of this question may be answered by asking about the TR-069 client (embedded)

software component the ACS vendor has developed; if they have been able to develop a client component, they understand the issues above and are well positioned to help CPE vendors through the intricacies of TR-069.

As of the date of publication of this document, Fine Point, in conjunction with their business partner, Dimark Technologies, has tested and certified \_CPE from Belkin, D-Link, Linksys, Netgear, Westell, ZyXEL, with several others in the process. The companies also work closely with CPE OEM and ODM manufacturers in Taiwan and China to make sure many private labeled devices are TR-069 compliant; has strong technology relationships with leading chip vendors like Intel, Centillium and others, and collaborates closely with software vendors like Jungo and Intoto. Finally, Fine Point and Dimark Technologies offer a TR-069 client in source code format that has been adopted by many of the above listed organizations for integration into their products.

## CYBERADVANTAGE DEVICE MANAGER™

---

CyberAdvantage Device Manager™, a TR-069 Device Management solution, allows network devices, such as broadband gateways, 802.11 APs, VoIP gateways and integrated access devices to automatically configure and update, greatly reducing the time and cost to deploy and support these devices.

CyberAdvantage Device Manager also enables incremental and recurring post-sale revenue opportunities by providing low cost delivery, installation and configuration of a wide range of value-added services.

Configuration and management is via the TR-069 standard, with support for VoIP via WT-104. Fine Point is also extending the TR-069 standard to provide additional functionality.

The CyberAdvantage Device Manager is the server component (referred to as the ACS in TR-069) that typically runs in the broadband Service Providers' network operations center (NOC).

CyberAdvantage Device Manager is scalable, allowing it to support a virtually unlimited number of CPE devices. Expanding the number of devices supported is accomplished with more powerful server hardware and/or running the CyberAdvantage Device Manager on additional, clustered servers that may be located in different geographic locations. As CyberAdvantage Device Manager is based on the same application server and database, technologies that are used to provide massive scalability in large-scale web sites (i.e. Yahoo.com, Amazon.com, eBay.com) commonly used load balancing and clustering techniques are applicable here.

The CyberAdvantage Device Manager code is designed such that each server in a Service Provider's operation maintains the necessary information in its database to provide the proper configuration information for all the CPE it serves. This concept provides both easy expandability as well as critical redundancy.

CyberAdvantage Device Manager does not require extensive integration into the Telco's or Service Provider's systems. Instead CyberAdvantage Device Manager is installed in the provider's network and through XML communication hooks built into all OSS systems, acts as middleware to allow the provider's OSS to manage CE devices. Accordingly, there is no need for the Service Provider to change the way the sales force operates: they simply enter customer orders as before and the CyberAdvantage Device Manager will automatically extract the information required to configure the CPE from the OSS and transmits it to the client component running embedded in the CPE for action.

CyberAdvantage Device Manager also allows the provider to sell and deploy value added services with no change in the sales process and no additional effort on the part of the customer; activation is automatic with the completion of the sales order. This also allows Telcos and Service Providers to sell value-added services on a monthly or recurring basis, a revenue model they understand.

## **ABOUT FINE POINT TECHNOLOGIES**

---

Fine Point Technologies' scalable support automation solutions and technologies empower digital service providers to acquire and manage new subscribers. Since 1997, our solutions have proven to reduce technical support costs and increase service provider's profitability through the ability to provision and manage new digital services.

Our industry leading solutions that include self-installation, self-repair, and OSS service management minimize technical support costs and deliver superior subscriber experience. With solutions licensed to hundreds of service providers and deployed to over ten million subscribers worldwide, Fine Point Technologies is the proven choice for subscriber management solutions.

For more information about our solutions and technologies, visit our website at <http://www.finepoint.com>.