

Broadband Device Web Services – An Overview

Second Draft (Version 0.8)
April 2003





Abstract

This white paper is a short overview of the business and technology challenges facing companies deploying value-added services to broadband gateways and Internet-enabled devices. Product managers and system architects are the primary audience for this document.

As with all white papers, we are plugging our own software and solutions (gasp), but offering a generalized bird's eye view of the problems and solutions. This document is also a little more tongue and cheek than what you may be used to in a white paper.

Second Draft (Version 0.8)

© Point Clark Networks 2003

Table of Contents

Abstract	2
Introduction	3
Future of Device Web Services	3
Today's Challenge	3
Market Issues	4
Increased Revenue Per Device... Really	4
Device Web Services = Increased Stickiness	4
Standards Battle Should Not Prevent Deployment	4
The Emerging Standards	5
Technology Issues	7
Device Location	7
Authentication	8
Encryption	8
Information Protection and Security	8
Infrastructure Scalability and Reliability	9
Service Creation Tools	9
Our Solution	10
Generate New Revenues and Realize Lower Costs	10
Focus on Core Competency	10
About Point Clark Networks	10



Introduction

Future of Device Web Services

There will come a day when every household, business, and organization is connected to high-speed Internet 24 hours a day. At these edges of the Internet will be broadband devices, smart servers, and other Internet-enabled devices. The future of these devices is promising; there is no doubt about it. As consumers and businesses demand more from their Internet connection, so increases the demand for an infrastructure that can deliver it. From today's content filter updates and managed VPN, to tomorrow's IP-based home alarm systems – where we want to go is easy to see, what is not so apparent is 'how are we going to get there?'

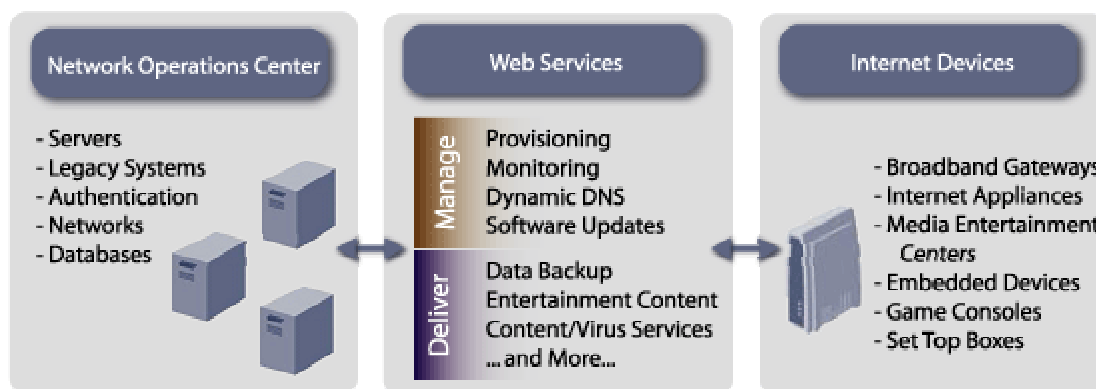
Today's Challenge

Today, the biggest category of broadband device to the home and small office – in terms of growth and volume – is the \$100-\$300 router. Whether sold through an ISP or bought directly by the end user, most of these devices are deployed without any kind of service, e.g.:

- Dynamic DNS
- Software updates
- Managed VPN
- Antivirus updates
- Content filtering updates
- Security audits
- Remote monitoring
- etc.

Of course, there are exceptions to this rule – some device/routers include basic services. For instance, SonicWall™ (<http://www.sonicwall.com>) includes antivirus subscriptions (among other services) and a "mysonicwall.com" website to manage deployed devices. As we move toward the end of the decade, the rule and the exception will change places. Most broadband devices will ship with some kind of subscription service technology – the exception will be the 'service-less' routers that we see on the store shelves today.

Despite the many benefits of deploying subscription-based services, adopters recognize the obstacles to developing this kind of leading edge technology. A company must deploy what we call a **Service Delivery Network (SDN)** – a data center solution for delivering services. Even the most basic services require a sophisticated infrastructure with significant outlays in time and money. Solution providers (hint: Point Clark Networks) offer products and solutions to reduce both the time and money required to deploy an SDN. The full breakdown of what needs to be in a Service Delivery Network is shown in the figure below. We get into the details in the next few sections.





Market Issues

Is there a business case to deploy services to broadband devices? In today's economic climate, any kind of investment in new products and services must show return on investment in months, not years. Building a solution from scratch is prohibitively expensive and risky. Fortunately, a number of solution providers (read: Point Clark Networks) have developed products to significantly reduce time to market and development costs.

You will be surprised at how easy it is to build a system for managing devices, subscribers, and services. In fact, Point Clark Networks has deployed solutions for Internet Appliance developers and ISVs in less than a month.

The two key advantages	
Increased Revenue Per Device... Really The gross margins on subscription services are high (40-90%), especially when compared with the cutthroat hardware business. In some cases, the margin from a service is more than the profit from the initial sale of the hardware. As long as the development and deployment costs are kept to a minimum, the financial risk is low.	Device Web Services = Increased Stickiness Services have a tendency to increase stickiness and reduce churn. For example, simple routers without services are (gasp) commodity devices. A user can jump ship at any time and buy a competitor's product. By adding subscription services to a device (even something simple like a personalized Dynamic DNS domain), an end-user must think twice before switching. Not only does the user have to check to make sure the service is offered on competing devices, but also take the time and effort to switch services.

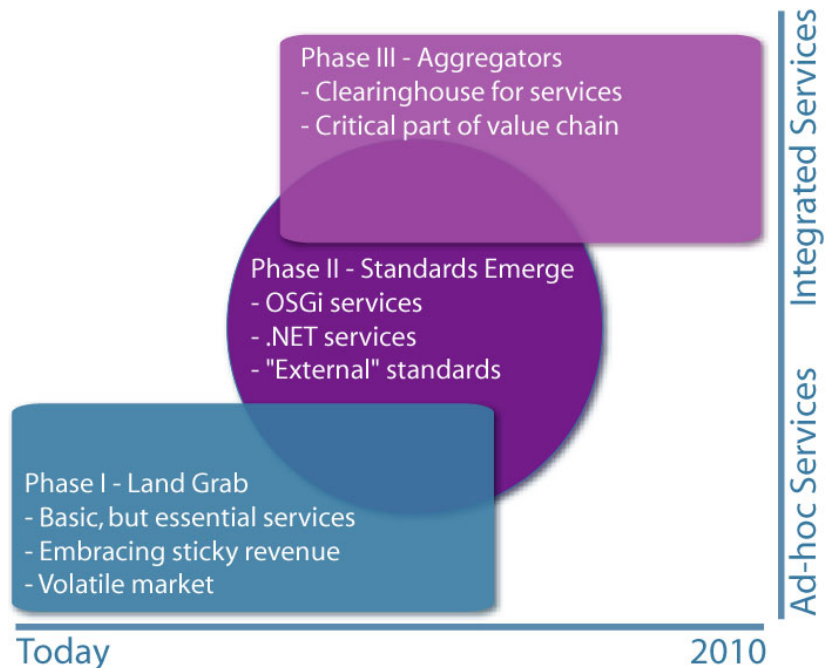
Standards Battle Should Not Prevent Deployment

The standards battle may seem like a big issue, but we feel it is a bit overblown. The winning standard for Web Services to broadband devices has not been determined. Fortunately, the whole concept behind "Web Services" is to provide a vendor/system independent way of implementing services. This means that picking the "losing" standard today is not an all-or-nothing situation. The very nature of the technology is to leave the underlying structure open to all kinds of vendors and solutions.

If this situation were analogous to the VHS and Beta standards battle, then you would be the video store owner. Regardless of which VCR standard emerges, you would still need a store, staff, shelves, accountants, lawyers, (well... maybe not lawyers) etc. Switching your inventory from Beta to VHS would be a pain and cost a little, but nothing more. Similarly for Web Services, you still need the billing, customer relationship management, databases, networks, data centers, information security protection, server OS, switches, etc. As the standards battle ebbs and flows, only a low layer of software will require some rework.



We have put together a chart (adjacent) to show how we see the standards and market emerge. As we move toward the end of the decade, a standard will become dominant and the ad-hoc services of today will turn into industry standards of tomorrow. Keep in mind that the very nature of today's technology and IP-based networks puts Web Service deployment on a solid foundation. In a way, future proofing is already built-in.



The Emerging Standards

First, we are using the term “standard” quite loosely. The following are not approved by official standards organizations, but are simply tools and techniques that are common in the industry. We are assuming that you know about the following standards already – if not, the website address is given for convenience. Here are the players in the standards battle:

OSGi (<http://www.osgi.org>) – The scope of the original OSGi specification did not cover the aspects of the infrastructure required in the data center – or what we call the Service Delivery Network. For the most part, the specification concentrates on many aspects of the local network: Bluetooth™, CAL, CEBus, Convergence, emNET, HAVi™, HomePNA™, HomePlug™, HomeRF™, Jini™ technology, LonWorks, UPnP, etc. That is a perfectly good place to scope the standard, but it does not help with Web Services deployment. This is certainly not a criticism of the specification; we are just pointing out OSGi only touches the surface of what is required in the data center. Future versions of the specification may expand on this part of service deployment, so we have included it in this list of standards.

Microsoft's .NET (<http://www.microsoft.com/net/>) – Despite the confusion surrounding Microsoft's .NET, it does include a framework for delivering Web Services. Specifically, SOAP and XML technologies are used to transfer data and run procedures across a network. This is certainly not a new concept – RPC, XML-RPC, and CORBA are all acronyms (and solutions) that have been around for years. Once again, Microsoft did a great job bringing a ‘geek-only’ concept to the hearts and minds of the technology masses.

As the .NET framework matures, it may become the dominant standard for Web Services to devices. It took Java 5+ years to get a solid foothold in the enterprise. Expect .NET (if successful) to have a similar beak-in period. It would be unwise to bet against Microsoft, so hedging your bets is a smart policy!



SOAP et al (<http://www.w3.org/TR/SOAP/>) – SOAP is a standard that has been adopted by the World Wide Web Consortium – the same group that publishes standards for HTML and many other web-related matters. SOAP is more of a protocol than a full-on standard for Web Services. To give you an example, if the National Weather Service decided to publish weather data via a Web Service, they would have to add some glue to make it into a real standard. Part of the .NET framework is based on SOAP, and other standards may include it in the future (e.g. OSGi may include some kind of SOAP framework in future versions).

Vendor Driven – We must not leave out the possibility that a big vendor will come along (IBM, Sony, etc.) and dictate the future standards for this market. It has happened before, and it will happen again.

We will now take a look at some of the technology issues.



Technology Issues

The shift from simple devices to service-enabled devices brings with it new technology challenges. The challenges and solutions are outlined in the table below. We use a combination of off-the-shelf solutions and – of course – our own software to meet these challenges. We are not necessarily peddling our solution (but we are); the important lessons here are recognizing the challenges.

Challenge	Solution	Service Delivery Network
Device Location	Our Dynamic DNS provides a solution to track IP addresses of Internet devices.	
Authentication	Leveraging the strength of customizable RSA based Public Key Infrastructure (PKI) and the US Government's Advanced Encryption Standard (AES), our Suva technology provides flexibility and tiny resource footprints without giving an inch on security.	
Encryption		
Information Protection and Security	Denial of Service (DoS) attacks, and other information security issues are a way of life on the Internet. We have developed tools to mitigate the risk.	
Infrastructure Reliability	Our distributed server system is a high-level solution for managing scalability and reliability.	
Service Creation Tools	Our Software Development Kit (SDK) provides an environment for creating value-added services for Internet-enabled devices.	

Our Service Delivery Network runs on Java technology (Servlets and/or J2EE). As the .NET framework matures, we may also provide support for the platform.

Device Location

Imagine FedEx attempting to deliver a package to a mailing address that might change every hour. This is analogous to how many parts of the Internet are built: broadband and dial-up users do not always receive the same Internet Protocol (IP) address on every connection, sometimes changing in the middle of a session. This has worked acceptably in the era of strict client/server relationships, for example HTTP and FTP. But the tasks of pushing media, timely information and software updates requires the ability to know where an Internet-enabled device is at all times.

Furthermore, direct control by end users – such as disabling an alarm system from a remote location or retrieving real time device status – requires that the IP address information be as up-to-date as possible. If not, an IP address change would cause the device to simply ‘disappear’ from the network.



Point Clark Networks debuted its device location service in November 2000, and now has thousands of devices using the service. It consists of a simple client that determines when the IP address has changed, and a server-side system to register that change within seconds. In addition, the server-side publishes the IP addresses of the devices via standard DNS (a feature typically called Dynamic DNS), allowing anyone, anywhere, to find the device in question using a simple domain name (e.g. bob-smith.pointclark.net).

Finding a device is a mundane, but crucial, component in delivering Web Services. Point Clark has had a solution that has been field-tested and is reliable, leaving you free to concern yourself with the more interesting tasks.

Authentication

With power comes responsibility. Images of the future have everything from the family's home security system to a remote oil well hooked up to the Internet. The question quickly goes from 'what can we do with this technology' to 'what could happen if this fell into the wrong hands?' Our core technology – **Suva** – was designed with this concern first and foremost in mind.

In the final analysis, authentication means that no one can do anything on a Suva-enabled device without proving, without a doubt, who they are. The method for obtaining this certainty comes from a technology well known and trusted in the security community – the RSA algorithm, which is used by such protocols such as SSH and PGP. Invented in 1977, the RSA algorithm has withstood the test of time in the rapidly changing field of cryptography, and is still considered the premiere asymmetric key encryption scheme.

Authentication is a fundamental part of Suva, and has been there since the earliest beta versions.

Encryption

After authentication, both parties can trust each other. With this trust comes the ability to send and receive sensitive information. The Internet is the Wild West of networks, nothing and no one can be trusted, and the nature of networking means that information is copied again and again. The most reliable way of making sure that information stays in the right hands is to make it meaningless to everyone except the intended recipient.

Point Clark Networks is focused on building reliable, secure and flexible software for delivering services to broadband devices.

This is what we do everyday.

The Suva framework accomplishes this using another trusted encryption scheme: the Advanced Encryption Standard (AES). The process for selecting the cipher for AES began in 1997, and in 2001 it was made an official standard by the US government for general strong encryption purposes.

Using our solution, a software developer only has to flip a single bit, and all subsequent communication is automatically encrypted using a 128-bit key (rotated every five minutes). Like authentication, data encryption has been part of Suva from the very beginning.

Information Protection and Security

Deploying any kind of Internet infrastructure requires dedicated resources for managing information protection. It is not a matter of 'if', but 'when' a security issue rears its ugly head. The procedures and processes for handling situations must be planned and deployed. What do you do when confronted with a sophisticated distributed denial of service attack? We have



answered many of these types of questions and put protection tools in place to mitigate risks and downtime.

Infrastructure Scalability and Reliability

Uptime is important to end users; if they paid for it, they expect it to be there at two in the morning or on a long weekend. And nothing can affect total cost of ownership more than a Web Service that keeps failing (editors note: we have first hand knowledge of this effect).

While the quest for 100% uptime is never finished, our Service Delivery Network has been designed from the beginning to have a head start. The solution was designed with location transparency in mind, which facilitates distributed failover and load balancing capabilities. Point Clark Networks has developed considerable support technologies to deliver the promise of continued service in even the most catastrophic circumstances. The technology makes our Service Delivery Network scalable, reliable and robust.

Service Creation Tools

The whole point of creating a reliable Service Delivery Network is to deliver a valuable service to an Internet-enabled device. When developing services, flexibility is key, and the distance between concept and rollout is critical. Our development environment has tools to help.

Services, by definition, are composed of either delivering information, or controlling functionality on the end device. The classic way of accomplishing both in the most flexible way is to use a RPC (Remote Procedure Calling) protocol. Popular RPCs include SOAP, D-COM and Java's RMI.

The two RPCs that Suva currently supports natively are SOAP and a lightweight internal protocol called Ono. In addition, Suva supports the creation of authenticated and encrypted TCP/IP tunnels. This means that protocols not natively supported by Suva can still work transparently. You can find more details in the Technology Overview on our website – <http://www.pointclark.net>.



Our Solution

This document was a brief introduction to the challenges of deploying Web Services to Internet devices. Whether you are looking for a turnkey system or consulting services to build your own solution, we can help. Why would you want to outsource? The answers are found in the table below.

	Point Clark Networks Solution	In-House Solution
Authentication & Security	<ul style="list-style-type: none">• Public key infrastructure• Follows US government standards	<ul style="list-style-type: none">• Security mechanisms must be built from scratch
Support	<ul style="list-style-type: none">• Redundancy through multiple locations• Proven technology and service record• 24/7 monitoring and support	<ul style="list-style-type: none">• Development and beta testing period may cause downtime
Rapid Development	<ul style="list-style-type: none">• Architecture already in place• Rapid application development• Cross-language development	<ul style="list-style-type: none">• Few similar off-the-shelf alternatives available
Ongoing Development	<ul style="list-style-type: none">• It is our core product!	<ul style="list-style-type: none">• Not a core business activity• Software engineers required to maintain and upgrade systems
Footprint	<ul style="list-style-type: none">• Built from the ground-up to be small: under 150 Kb	<ul style="list-style-type: none">• Alternative solutions may require significant computing resources
Cost	<ul style="list-style-type: none">• Reduce the costly and time-consuming work of re-inventing the wheel.	<ul style="list-style-type: none">• Expensive

Generate New Revenues and Realize Lower Costs

Companies that build their own Service Delivery Networks end up creating and maintaining the underlying platform themselves. This work can involve four to ten full-time engineers on an ongoing basis – more if the Web Services and integration are complex. This represents an engineering investment of \$400,000 to \$1,000,000 per year. Our solution realizes substantial cost savings.

Focus on Core Competency

More important than the cost in dollars is the less tangible cost in lost focus on core competencies. Our solution lets you focus on differentiating your products and services without having to worry about maintaining the underlying service delivery platform. These differentiators are the critical drivers of the success of a Web Services deployment – after all, the end user cares about features and reliability, not the servers in the back room.

About Point Clark Networks

Point Clark Networks started as a concept on the back of a napkin on the campus of Carnegie Mellon University. In May 2000, the company moved from concept to reality and started



developing solutions for the broadband server/device market. Point Clark Networks has built a great team around our core competencies. The technical backgrounds of half our team come directly from Internet/network infrastructure fields, and half of the staff are licensed Professional Engineers in Ontario, Canada.

The first version of our Device Web Services solution was launched in late 2000. This initial release included a basic software update service along with a dynamic DNS service. Today, our solution includes dozens of unique services to help consumers and businesses get the most out of their Internet-based devices. Everyday, we see new devices appear on our network as we continue to deliver services to thousands of installed systems across 40 countries. Our customers not only include end users, but also ISPs, Internet appliance manufacturers, and ISVs.

In addition, Point Clark Networks has developed *ClarkConnect* - a do-it-yourself Linux-based broadband device solution. Users can download the open-source product and transform a standard PC into a full-featured Internet device. Through the *ClarkConnect* project, Point Clark Networks understands what it takes to support and maintain a broadband Internet device. The project also gives us a unique environment to build, test and deploy our infrastructure.

Contact

Point Clark Networks
<http://www.pointclark.net>
info@pointclark.net
416.977.0574