A Management Framework for Residential Broadband Environments

Tiago Cruz, Paulo Simões,
DEI-CISUC – University of Coimbra
Coimbra, Portugal

***Abstract*— the widespread availability of broadband access technologies deeply impacted the residential LAN, reshaping its ecosystems of services and devices and changing the prevalent service delivery and usage paradigms.**

In this scenario, operators and service providers constantly face the challenge of delivering the best possible value for end-users without compromising revenue, reliability or performance. This balance can only be achieved through a comprehensive management approach, ideally capable of providing an end-to-end coverage of the critical aspects involved in the delivery process and covering the infrastructure, services and devices.

In this paper we present the main results of a PhD Dissertation that addressed the challenge of providing service providers with adequate service and device management mechanisms. First, we extended the industry *de facto* standard for remote management of devices and services on the customer's premises (the CWMP/TR069 framework), in order to increase its scope and flexibility. Afterwards, on top of those extensions, we proposed and investigated an array of innovative approaches for device, service, desktop and security management. Overall, those approaches allow operators to simplify their operations, enabling the improvement of current services as well as the introduction of novel services.

***Keywords*— Network Management, CWMP, Home Networks**

I. INTRODUCTION

The expansion of high-speed broadband access networks, with an increasing growth in the number of connected households was one of the key factors that enabled a new breed of services, such as converged n-play offers or cloud services that are contributing to displace traditional split-medium communication and service delivery models in favour of an *everything-over-IP* approach. In line with those developments, the residential LAN ecosystem has evolved to become an environment where devices as diverse as PCs, set-top-boxes, SIP telephones, smartphones, media players, smart TVs or storage devices cohabitate, providing access to a wide array of services to broadband customers. However, this scenario has a double-edged counterpart: most residential LANs have become too complex to be autonomously managed by the average customer, which frequently lacks the technical expertise to do so.

In this perspective, management is a critical matter that has a direct impact on reliability and performance, whether for operator-provided or over-the-top services. Operators are especially concerned with this situation, which is the source for a wide array of issues that can be troublesome and expensive to fix, ultimately being the cause of customer satisfaction problems, as they expect IP-based services to have equal or better performance and reliability when compared to their conventional counterparts. In some cases, this means that operators must be able to remotely manage the devices (configuration management, monitoring, etc.) and the path between them and the access network (i.e., at least a segment of the customer LAN) to ensure adequate service levels.

Still, allowing ISPs to reach the customer premises LAN contradicts the conventional centralized operator security and management models that establish a clear separation between the ISP scope (ending at the borderline equipment) and the domestic LAN premises, with the domestic customer being responsible for his own frontier equipment (such as the Residential Gateway – RGW) and everything beyond that.

With some of the key services now provided by operators (VoIP, IPTV, femtocell-based applications, etc.) heavily depending on equipment placed on the customer LAN but intended to be managed by the ISP (e.g. set-top boxes), most triple play customers already have ISP-provided devices on their LAN with customized configurations and/or firmware which they cannot control. As a result, the idea of allowing operators to manage equipment and services inside the customer's premises gains increased acceptance by both sides, creating the need for adequate management mechanisms capable of addressing the needs of service providers while safeguarding customer's autonomy and privacy concerns.

In line with such reasoning, this dissertation explores the potential for a consolidated management approach designed from the ground up to address the device and service management needs of broadband access network environments, while also supporting the creation of new managed service paradigms. Instrumental to this purpose was the development of an extensible framework for remote management of devices and services on the customer's premises, based on Broadband Forum's [1] CPE Wan Management Protocol (CWMP [2]), the *de facto* standard for management of devices located in the customer premises on broadband access network environments. As such, this framework provides a complete management solution targeted towards residential LAN environments that nevertheless, remains compatible with existing management infrastructures.

The rest of this paper is structured as such: the proposed management framework is presented on Section II, followed by the discussion of the innovative approaches it enables for device, service, desktop and security management (Sections III to VI, respectively). Section VII concludes the paper.

978-3-901882-50-0

II. Managing the Residential LAN Environment

This section presents the proposed management framework that constitutes the common building block for the research work hereafter developed. Starting with a brief introduction to the CWMP protocol, it will next delve into the design and operation of the proposed management framework.

A. The CWMP protocol

Broadband Forums' CWMP protocol suite is the established standard for secure device and service management on broadband environments, being designed to enable secure auto-configuration, dynamic service provisioning, diagnostics, software/firmware management and status/performance monitoring of devices and associated services. It provides a management API of Remote Procedure Calls supported by a set of extensible data models defined by related standards such as TR-106 [3] or TR-157 [4]. The standard data model for a CWMP-capable device follows a common set of requirements for which the detailed structure, hierarchically organized like a directory tree, depends on the nature of the device. Data model information is structured using objects and parameters - each object is a container for other objects and parameters, the latter storing the configuration properties of the managed device.

The adoption of CWMP for the proposed management framework enables operators to use their already existing Operations Support Systems (OSS) to handle service and device management for the home LAN. Also, one of the characteristics that make CWMP particularly fit for management of devices and services inside the residential LAN has to do with its operation model: a managed device always initiates management sessions, either directly or by request of the management server (designated by Auto-Configuration Server, ACS). This has the benefit of better coping with firewalls and other mediation mechanisms.

B. An extensible CWMP management framework

The proposed management framework is based on a dynamic CWMP agent extensibility mechanism [5] (see Figure 1) which decouples CWMP protocol services (concentrated in a so called "Master Agent") from device/service-specific management interfaces to be provided via CWMP (distributed across "Subagents").

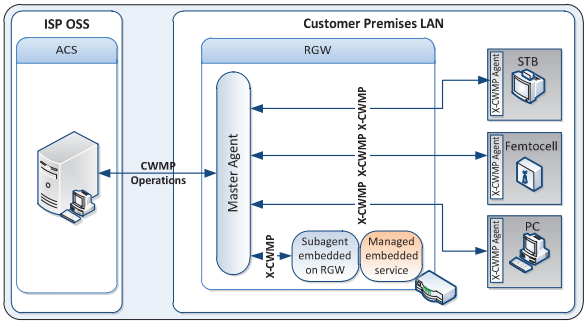

Figure 1: CWMP Extensible Agent in a Device Proxying Scenario.

Communication between the Master Agent and Subagents is based on a new protocol (X-CWMP) [5] much simpler than CWMP, based on XML messages transported over TCP/IP, with optional use of SSL. When a subagent registers on a master agent it becomes associated with the CWMP data model objects and properties for which it is responsible. The master agent acts like an orchestrator, being responsible for receiving, converting and forwarding requests – on reception of a request it identifies the subagent(s) responsible for the objects(s) involved in the operation, and forwards the request(s) to those agent(s).

Even when implementing a classic CWMP agent – contained in a single CPE – the advantages of this approach are manifold, in comparison with monolithic approaches: not only it provides an easier way to port agents to new CPE devices (as the master agent has no device-specific logic or code), but it also makes easier to add new services to a CPE, being a question of writing the corresponding interface subagents, a task not requiring detailed knowledge of CWMP. Also, managed services can be added or removed dynamically, without the need to restart the CWMP agent.

Additionally, the CWMP data model template provides support for RGWs to act as management proxies for devices inside the subscribers LAN, treating each legacy device as a data model branch of an RGW (which is also a CPE). The ACS communicates directly with the RGW and is unable to distinguish between services provided by the device itself and legacy devices. At the time of the writing of this dissertation, there were no implementations or reference guidelines taking advantage of those mechanisms – hence the novelty of this architecture, which also opens the way for less conventional configurations. For instance:

- Master agents and subagents can be located in different devices, allowing CWMP agents to proxy the access to those devices which, for some reason, might not support CWMP (see Figure 1). This eases integration of legacy devices, providing a solution for CPEs which are not powerful enough to support a full CWMP stack. Moreover, it also helps solving the CWMP NAT traversal problem, using a solution more reliable than STUN [6] (which is recommended by TR-111 [7]).
- Subagents can also be used as "Protocol Proxies" providing integration with existing LAN technologies and other protocols, such as the Universal Plug and Play framework (UPnP) [8]. This enables operators to take advantage of existing management services in the context of the internal LAN, representing valuable management information.

According to the circumstances, X-CWMP subagents constitute a generic plug-in capability allowing the CWMP stack to communicate and abstract: (i) managed services of the host device; (ii) managed services of other CPE devices; and (iii) management services provided by other protocols and associated data models.

III. Device Management

As already mentioned, one of the benefits of the proposed management framework is its support for developing generic CWMP interface layers to enable interoperability with non-

compliant devices, seamlessly bridging protocol and interface gaps. In this context, two use-cases of CWMP-integrated management of "foreign" devices were explored: integration of off-the-shelf VoIP endpoints and UPnP devices.

A. VoIP device management

Fixed telephony was among the first services to be offered in converged *n-play* bundles, supported using Session Initiation Protocol (SIP) [9] signalling over IP networks. Naturally, such devices require specific configuration in order to operate – however, while Analog Telephony Adapter (ATA) devices embedded on RGWs may potentially benefit from the management mechanisms already present at the gateway-level to enable operators to remotely configure them, standalone SIP devices inside the customer LAN are a different matter. This happens because most of them were designed for corporate LANs, lacking adequate mechanisms for remote management over broadband access networks.

While CWMP-compliant SIP devices do exist, most of them correspond to ATA devices embedded on RGWs, with SIP telephones representing a small minority. Therefore, there is a need for a remote management solution for SIP endpoints capable of supporting a wider range of devices, and not only CWMP-compliant equipment.

The proposed solution [10] integrates together a CWMP frontend interface with a TFTP-based provisioning backend, using a specific integration component (see Figure 2). This component acts as module of the gateway's CWMP agent, interacting with the ISP ACS (by means of CWMP operations) and with the home gateway TFTP [11] and DHCP [12] Servers (to indirectly interface with the managed SIP devices).

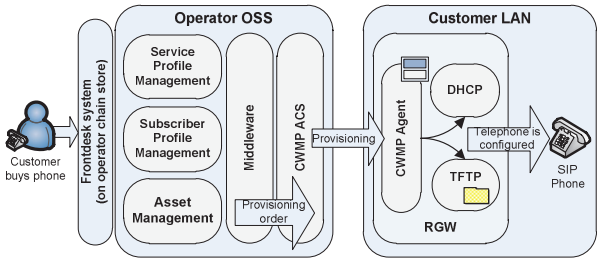

Figure 2: CWMP-integrated SIP device management.

This extension is implemented as a subagent which maps the configuration properties of SIP endpoints into the CWMP data model of a RGW, so that the operator ACS can remotely manage them using CWMP. The module will then configure the services needed for TFTP-based provisioning (TFTP and DHCP), which are embedded on the RGW and are exposed on the LAN-side interface, accordingly with its configuration.

Alternatively, this solution supports another operation model, designed to allow users to take care of the initial configuration process. This method (which is further described in [10]) allows users to buy a SIP telephone from a third-party (as long as it is included in the service provider hardware compatibility list) and take care of its provisioning in a cost-effective way, by answering a call on their newly bought telephone, using a simple and intuitive method based on an automated Interactive Voice Response (IVR) menu.

B. UPnP device management

The UPnP (Universal Plug and Play) framework was designed to simplify and/or automate device interoperability and configuration in home networks. UPnP devices use UPnP protocols to advertise, discover and access services in a seamless way, with minimum user intervention. UPnP support is popular across all classes of devices, especially media-related equipment, being supported by a wealth of devices, such as media players, "smart" TV sets or Blu-ray players, which are becoming commonplace in domestic LANs. As such, the UPnP mechanisms embedded on those devices would be of great value for remote diagnostic and configuration purposes.

However, UPnP was not designed to operate in the environment of broadband access networks, being of little or no use for remote management purposes. Also, CWMP lacks adequate mechanisms for UPnP integration – TR-157 [4] defines a profile for embedding UPnP device information on a CPE data model, but without support for device control.

To address these limitations, we developed an extension to the CWMP protocol [13] using our management framework, which allows operators to fully access and manage UPnP-compliant devices, whilst keeping compliance with the original CWMP protocol framework (see Figure 3).

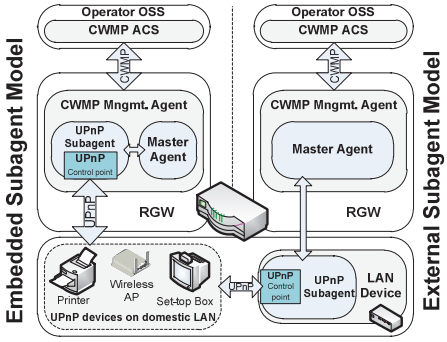

Figure 3: CWMP-integrated UPnP device management.

This UPnP-CWMP bridging extension (a subagent) maps the description of UPnP devices found on the domestic LAN on a gateway CWMP data model, also supporting UPnP eventing, integrated with CWMP asynchronous property notification mechanisms. For this purpose, the subagent embeds an UPnP control point, allowing it to interact with all UPnP devices on the domestic LAN (Figure 3). Also, the properties of our extensibility framework allow the subagent to be embedded either on the RGW or on another device on the LAN (e.g. a PC temporarily used as a protocol bridge for diagnostics).

IV. Managed Services

From the operators' perspective, added-value services are complementary to its broadband access offers, being instrumental to sustain service margins and compensate for the decreasing revenue from traditional services (like PSTN voice). In this context, an operator-managed service paradigm makes sense, even for scenarios where third-party providers or over-the-top services use the ISP infrastructure as a service carrier (with shared revenue models) – besides, it is also an

opportunity to explore and create new and innovative service paradigms. To this purpose, two operator-managed service delivery frameworks are proposed: a multimedia content delivery solution for Digital Living Network Alliance (DLNA) [14] media devices and a cloud storage service.

A. A DLNA-compliant content delivery solution

The first managed service proposal [15] consists of a solution for seamlessly delivering operator or third-party media content for media devices inside the residential LAN supporting existing protocols and media delivery frameworks, such as UPnP AV [16] (UPnP Audio Video) and DLNA (Digital Living Network Alliance). It does this by turning the RGW into a managed mediator for both operator-provided and Internet media content, provided as UPnP AV/DLNA resources visible inside the domestic LAN (see Figure 4).

The benefits of this approach are manifold: first, it helps overcome the limitations of the DLNA specifications and their core UPnP AV functionalities which were designed for use on LAN environments, being unable to properly operate across the LAN boundaries, over broadband access networks; second, it helps reducing the clutter on the residential LAN generated by the increased number of devices deployed to provide access to specific media services from Internet or content providers; finally, by adopting a standard framework for media delivery, it also becomes possible to avoid the problems arising from protocol or Application Program Interface changes for specific media services – a situation that can render devices useless until a firmware update is available, something which may never happen, depending on their support status.

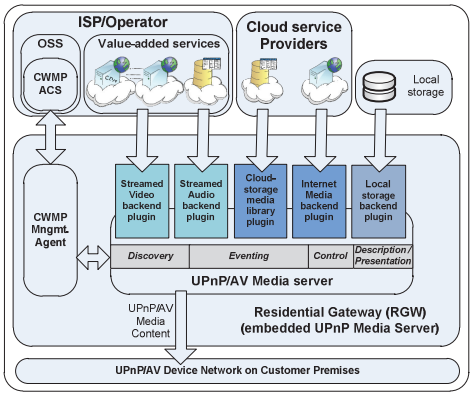

Figure 4: UPnP AV RGW server architecture.

This allows for seamless and secure media distribution to a wide range of devices that already support those protocols, without the need for pushing another protocol stack or specific device into the domestic LAN for such purpose, extending the reach of the DLNA device ecosystem beyond the LAN scope.

The media server embedded on the RGW is based on a modular architecture that makes use of plugins (which can be dynamically deployed and activated) to deliver a wide range of contents and services available outside the LAN environment – abstracted as media items residing on a regular UPnP AV media server advertised on the domestic LAN.

CWMP is used to manage the UPnP AV media server embedded on the gateway, allowing the operator to customize which specific plugins are available and the configurations of each active instance. For this purpose, a CWMP bridging subagent was developed with the purpose of mapping the configuration of the UPnP AV media server and its plugins into the CWMP data model of the RGW, so that the operator ACS can remotely manage all media server properties.

B. A managed cloud storage solution

The second managed service proposal [17] consists of an operator-managed hybrid storage solution that combines the benefits of standalone storage appliances with cloud storage. For this purpose, each RGW is transformed in a storage hub and given its own local storage resources (solid state or hard disk) whose contents are made accessible to the customer premises LAN using standard protocols such as SMB/CIFS [18], FTP [19] or HTTP(s) [20] and kept synchronized with a cloud storage container on the operator infrastructure.

There are several key advantages to this approach: first, it relieves users from the task of configuring and managing their own storage devices; second, it takes advantage of the fact that the RGW is a device which is permanently powered on (especially in triple-play environments) in order to provide connectivity services for the LAN, therefore eliminating the need for a separate appliance (and its cost of ownership); and third, it provides redundancy and reliability by replicating data to a virtual container located outside the customer premises, on the storage provider infrastructure, instead of relying on self-contained data replication methods, such as RAID (which, nevertheless, can be used for extra redundancy). Moreover, this solution has the ability to stream content to the customer premises network at LAN speeds (provided it is already synchronized), while supporting disconnected operation. Versioning is also supported, allowing the user to recover previous versions of a specific file.

Every RGW associated with the same storage service subscription is allowed to synchronize with the central repository, making this solution adequate for both multi-branch SOHO infrastructures and home users with a service subscription for a single household. Roaming users might also use native client applications to access their storage container. Figure 5 illustrates the proposed architecture.

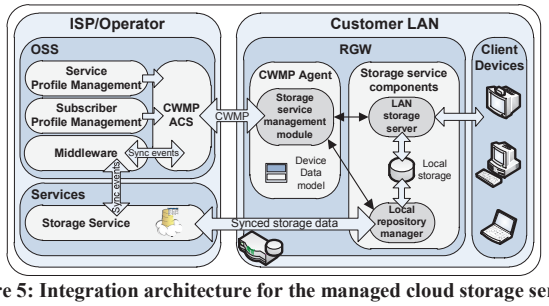

Figure 5: Integration architecture for the managed cloud storage service.

In this context, storage service management interfaces and eventing mechanisms are supported by CWMP. Each RGW incorporates a specific integration component that acts as module of the gateway CWMP agent, interacting with the ISP

ACS and with the local storage service components. On the operator side, the ACS implements the CWMP management server, which interfaces with the storage service frontend by means of a middleware layer (a message-oriented queuing system) for passing events back and forth between them.

V. Desktop Management

This section will deal with the thematic of desktop management over broadband access networks, by pursuing an approach which makes use of our management framework to propose two novel and complementing solutions to the problem: the first one targeted towards the (still predominant) windows-based PC desktop paradigm and the second one consisting on a cloud boot concept for thin-client devices which can also be used to help managing conventional PCs.

A. Operator-assisted desktop management

To deal with the lack of alternatives for the management of traditional Windows-based systems on broadband environments, we proposed a solution [21] which bridges the gap between LAN desktop management technologies – namely Windows Management Instrumentation (WMI) [22] – and the CWMP framework. This solution consists of a CWMP protocol extension that allows broadband operators to use their already existing infrastructure to remotely access and manage Windows devices, using the WMI management API. Two alternative integration scenarios are supported (see Figure 6):

- The integration is performed at the RGW. In this case the integration component is embedded on the RGW, using a CWMP/WMI subagent which remotely accesses the WMI service on the managed Windows device.
- The CWMP-WMI integration component is located in the managed device, in the form of a remote subagent accessing local WMI services. While this approach avoids restrictions such as access control mechanisms, it requires the installation of software in the Windows PC.

In either case the CWMP/WMI integration component is responsible for declaring which WMI attributes are translated into the CWMP data model, for each Windows device.

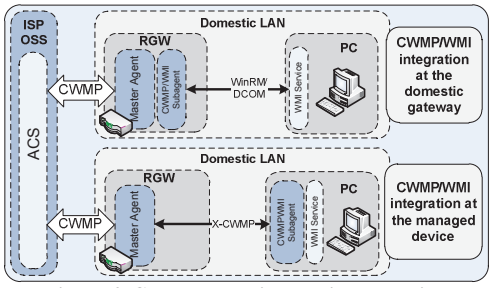

Figure 6: CWMP-WMI integration scenarios.

These two topologies are both possible thanks to our management framework, as it was designed to allow a hybrid distributed management topology where CWMP agents can proxy the access to devices that do not support CWMP, using master agents and subagents located in different devices.

Application scenarios for this solution may include operator-assisted management (for instance, an ISP may sell to domestic or SOHO customers PCs bundled with software and remote management services) or even the implementation of a Desktop Management-as-a-Service concept, where an Internet provider may provide an interface for third-party service providers specialized in desktop management. Such a service would be especially attractive for small corporations, which would be able to outsource – or cloud-source – the remote management of their desktops and Windows servers.

B. Managed cloud boot

As an alternative to the conventional desktop computing paradigm, we proposed to bring the benefits of managed desktop computing to home users, telecommuters and small businesses by providing remote OS boot capabilities on broadband access network environments [23], using the Preboot eXecution Environment (PXE) protocol [24].

PXE is the *de facto* standard for network boot firmware, allowing a PC to download and execute an agent – the Network Bootstrap Program (NBP) – over a LAN at boot time, for deployment, diagnostic or bare metal recovery. PXE can also be used to support completely stateless thin-clients [25] whose operating environment is downloaded from the network when powered up, instead of using local firmware.

In this scenario (see Figure 7), CWMP is used by the ISP ACS to configure all PXE-related parameters, mapped on the CPE/RGW data model. The CWMP agent of the RGW uses this data to configure the embedded DHCP server, so that it can provide the correct option tags to the PXE boot ROM.

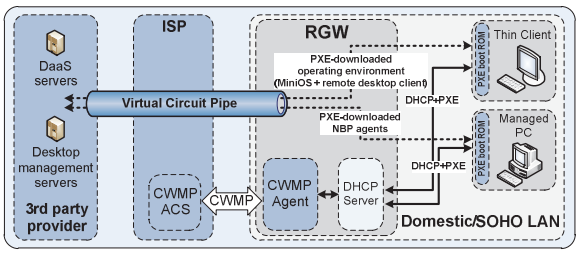

Figure 7: PXE-based broadband desktop management.

To enhance PXE operation, an ISP may also use CWMP to configure a private virtual circuit pipe in order to offer QoS guarantees to PXE, related management traffic and remote desktop services. This makes it possible to establish SLA agreements between ISPs and third-party providers of desktop services to allow end-to-end differentiation of service traffic.

Application scenarios for this solution may include the implementation of complementary recovery and diagnostics mechanisms for conventional PCs (for instance, bare metal recovery using a remote boot agent), implementation of Desktop-as-a-Service stateless thin-clients (for use as Virtual Desktop Infrastructure or web-based desktop clients) or special-purpose appliances, such as thin IPTV set-top-boxes.

VI. Security Management

From an ISP perspective, modern broadband access networks pose significant and ever increasing challenges in terms of security management. The growing number of permanently connected home networks, with a myriad of

poorly managed devices, imposes significant security risks – not only to the domestic customers, unable to defend themselves from security attacks, but also to the ISP and third-parties potentially targeted by large-scale distributed botnet attacks fed by swarms of zombie domestic PCs. In this context, the traditional delimitation of customer and ISP perimeters is no longer effective. Home networks became too complex and vulnerable to be autonomously managed by the average customer, and the scale and sophistication of distributed security attacks make it more and more difficult for the ISP to properly manage security without intervening outside the boundaries of its own network.

Considering this state of affairs, we propose an alternative approach (see Figure 8) for security management based on an increased level of integration and cooperation between the domains of the ISP infrastructure and the home network. It is based on a distributed security model that offloads some of the security functions to RGWs, taking advantage of their positioning, processing and remote management capabilities.

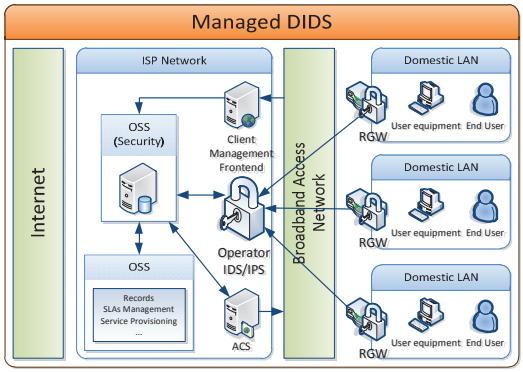

Figure 8: Proposed Managed Distributed IDS architecture.

Thus, RGWs become active security elements of a Distributed Intrusion Detection System (DIDS), being able to collect information and statistics related to network traffic that can be used as input for semi-centralized (supervised on unsupervised) training and decision inference and correlation systems, which can take actions to secure the network by distributing countermeasures to the RGWs and other network devices (like selectively filtering of network traffic in response to possible attacks). The proposed architecture includes dynamically deployable components that provide security-related services at the RGW level which are remotely managed using CWMP. Thanks to our extensible agent framework, security components might even be hosted on other LAN devices, being proxied through the RGW.

This model is not fully distributed by nature – even if it allows RGWs to embed autonomous detection and action mechanisms, all the operation is centrally orchestrated on the ISP infrastructure (see Figure 9). A management infrastructure is kept on the provider's side to coordinate the various participants on this process, orchestrating its operation based on the correlation of the pieces of information collected from the ISP network and from the different RGWs. Detection and treatment of security events may occur at two different levels:

- At local level (RGW). For efficiency, scalability and granularity reasons, the RGW may host a local event correlation engine (fed by events generated by traffic analysis tools, such as intrusion detection systems or log records) with optional reaction capabilities.
- At the ISP level. The event correlation engine that exists at the ISP level processes the events received from the multiple involved RGWs. This allows, for example, the detection of combined attacks either affecting or coming from several customers of the ISP. The provider can react to these events taking preventive measures on its network and/or adjusting the RGW configurations.

Thus, the proposed platform is able to deal with two levels of operation (RGW/microscopic, ISP/macroscopic), while covering a broad scope, from the provider's network to the entrance/exit points of the clients' network.

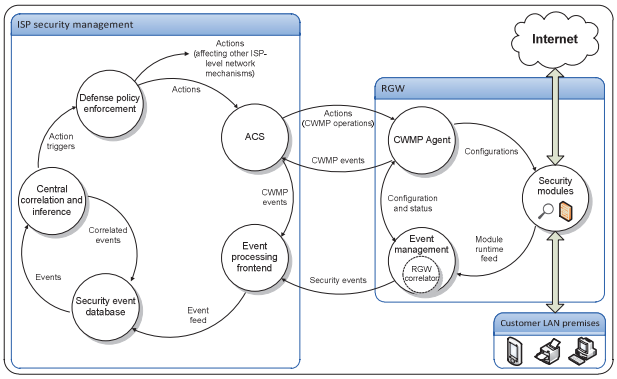

Figure 9: Generic model of the event-based decision making process.

VII. CONCLUSION

The field of device and service management in broadband access networks is surrounded by a diversity of issues, related to technologies, standards, devices and services. Ultimately, this dissertation was a reflex of all this complexity and entropy, being deemed from the start to approach a diversity of disparate subjects that, nonetheless, are somehow congregated in a common set of goals.

In global terms, we consider that this dissertation fulfilled its initial goals, demonstrating the potential of a management approach that allows the operator to reach the customer premises LAN to take care of configuration, diagnostics and troubleshooting operations. Also, this work emphasized the importance of the domestic gateway as an instrumental device in a multi-service scenario, positioned as the privileged security, management and service interface between the domestic consumer LAN and the communication and service providers. While the subject of management in broadband access networks was the pervasive topic of this dissertation, influencing all its structure, it should be nevertheless mentioned that the application scenarios that spawned from its development revealed a degree of value and consistency that made them stand out as autonomous propositions. Moreover, the development of the application scenarios was one of the most engaging and gratifying aspects of this work, mainly because of their potential to be transposed, with relative ease, to innovative market products.

VIII. Reference Material

References [10], [13], [15], [17], [21], [23], [26] and [27] refer to papers and/or articles published in the scope of this dissertation [28].

Acknowledgements

This work was partially funded by PT Inovação (Project Virtuoso) and by Project QREN ICIS (Intelligent Computing in the Internet of Services – CENTRO-07-0224-FEDER-002003).

References

[1] Broadband Forum, http://www.broadband-forum.org.
[2] Broadband Forum,"TR-069 - CPE WAN Management Protocol specification v1.2, Amendment 3", November 2010.
[3] Broadband Forum, "Data Model Template for TR-069 Enabled Device, TR-106 Amendment 4", February 2010.
[4] Broadband Forum," Component Objects for CWMP, TR-157 Amendment 3", November 2010.
[5] T. Cruz, P. Simões, et al., "CWMP Extensions for Enhanced Management of Domestic Network Services", in Proc. of LCN'2010 (The 35th IEEE Conf. on Local Computer Networks), Denver, USA, September 2010.
[6] J. Rosenberg et al., "Session Traversal Utilities for NAT (STUN)", IETF RFC 5389, October 2008.
[7] Broadband Forum, "TR-111: Applying TR-069 to Remote Management of Home Networking Devices", December 2005
[8] UPnP Forum: UPnP Device Architecture 1.1 (2008)
[9] J. Rosemberg et al., "SIP: Session Initiation Protocol", IETF RFC 3261, June 2002.
[10] T. Cruz, P. Simões, J. Almeida, J. Rodrigues, E. Monteiro, F. Bastos, A. Laranjeira, "How to Provision and Manage Off-the-Shelf SIP Phones in Domestic and SOHO Environments", in Proc. of LCN'2011 (36th IEEE Conf. on Local Computer Networks), Bonn, Germany, October 2011.
[11] K. Sollins, "The TFTP Protocol (Revision 2)", IETF RFC 1350, July 1992.
[12] R. Droms, "Dynamic Host Configuration Protocol", IETF RFC 2131, March 1997.
[13] T. Cruz, P. Simões, J. Rodrigues, E. Monteiro, F. Bastos, A. Laranjeira, "Using UPnP-CWMP Integration for Operator-assisted Management of Domestic LANs", in Proc. of CCNC 2012 (IEEE Consumer Communications and Networking Conference), Las Vegas, USA, January 2012.
[14] DLNA Consortium, "DLNA Networked Device Interoperability Guidelines", 2009.
[15] T. Cruz, P. Simões, E. Monteiro, F. Bastos, A. Laranjeira,"A Framework for Internet Media Services Delivery to the Home Environment", *Journal of Network and Systems Management*, pp. 1-29, 2012.
[16] UPnP Forum: UPnP AV Architecture:1 for UPnP Version 1.0 (2008).
[17] T. Cruz, P. Simoes, J. Rodrigues, E. Monteiro, A. Laranjeira, "Managed Hybrid Storage for Home and SOHO Environments", accepted for publication in the Proceedings of IM 2013, Ghent, Belgium, May 2013.
[18] Microsoft Corp., "Microsoft SMB Protocol and CIFS Protocol Overview", March 2011.
[19] J. Postel, et al, File Transfer Protocol, IETF RFC 959, October 1985
[20] R. Fielding et al., "Hypertext Transfer Protocol – HTTP/1.1", IETF RFC 2616, June 1999.
[21] T. Cruz, P. Simões, J. Rodrigues, E. Monteiro, F. Bastos and A. Laranjeira, "Outsourced Management of Home and SOHO Windows Desktops", in Proc. of CNSM 2011 (7th IEEE/IFIP International Conference on Network and Services Management), Paris, France, October 2011.
[22] Microsoft Corporation, "Windows Management Instrumentation Remote Protocol Specification v10.1", March 2010.
[23] T. Cruz, P. Simões, et al., "Integration of PXE-based Desktop Solutions into Broadband Access Networks", in Proc. of CNSM'2010 (The 6th IEEE/IFIP Conf. on Network and Services Management), Niagara Falls, Canada, October 2010.
[24] Intel Corporation, "Preboot Execution Environment (PXE) specification version 2.1", September 1999.
[25] T. Cruz, P. Simões, "Enabling PreOS Desktop Management", in Proc. of the IM'2003 (IFIP/IEEE Int. Symposium on Integrated Network Management), Colorado Springs, May 2003.
[26] T. Cruz, P. Simões, J. Rodrigues, E. Monteiro, F. Bastos, A. Laranjeira, "Managed Hybrid Storage for Home and SOHO Environments", Proceedings of IM 2013 (IFIP/IEEE International Symposium on Integrated Network Management), Ghent, Belgium, May 2013.
[27] T. Cruz, P. Simões, N. Reis, E. Monteiro, F. Bastos, A. Laranjeira, "An Architecture for Virtualized Home Gateways", in the Proceedings of IM 2013 Mini-conference (IFIP/IEEE International Symposium on Integrated Network Management), Ghent, Belgium, May 2013.
[28] T. Cruz, "A Management Framework for Residential Broadband Environments", Ph.D. dissertation, Dept. Informatics Engineering, University of Coimbra, Portugal, 2011.