broadband forum

TECHNICAL REPORT

TR-131
ACS Northbound Interface Requirements

Issue: 1 Amendment 1
Issue Date: August 2015

Notice

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Broadband Forum Technical Report has been approved by members of the Forum. This Broadband Forum Technical Report is not binding on the Broadband Forum, any of its members, or any developer or service provider. This Broadband Forum Technical Report is subject to change, but only with approval of members of the Forum. This Technical Report is copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Technical Report may be copyrighted by Broadband Forum members.

THIS SPECIFICATION IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NONINFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS SPECIFICATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS SPECIFICATION.

Broadband Forum Technical Reports may be copied, downloaded, stored on a server or otherwise re-distributed in their entirety only, and may not be modified without the advance written permission of the Broadband Forum.

The text of this notice must be included in all copies of this Broadband Forum Technical Report.

Issue History

Issue Number	Approval Date	Publication Date	Issue Editor	Changes
1	November 2009		John Blackford, 2Wire Heather Kirksey, ALU William Lupton, 2Wire Anton Okmyanskiy, Cisco Hakan Westin, Tilgin	Original
1 Amendment 1	24 August 2015	11 September 2015	Sumit Singhal, Ericsson	Adds M2M Service Layer Requirements Voids inapplicable requirements from initial version Introduces requirement profiles.

Comments or questions about this Broadband Forum Technical Report should be directed to help@broadband-forum.org.

Editor	Sumit Singhal	Ericsson
BroadbandHome™ WG Chairs	John Blackford	Pace
	Jason Walls	QA Cafe

TABLE OF CONTENTS

List of Figures

Executive Summary

This Technical Report specifies requirements for the ACS Northbound Interface (NBI), which enables an integration of the Northbound Management Systems with the ACS to provision and manage devices.

This Technical Report specifies the use cases and functional requirements for the NBI, but does not specify the interface itself.

This Technical Report includes requirements for architecture, provisioning devices, device operations, file management, device grouping, events, error management, security and access control.

1 Purpose and Scope

1.1 Purpose

This Technical Report defines requirements for an ACS Northbound Interface (NBI) that allows Operational and Business Support Systems, including a Machine to Machine Service Layer, to access ACS functionality. These requirements are derived from a set of device management and service management use cases. Sections 1 through 5 of this Technical Report, which includes this introduction, use cases and key concepts, are non-normative and are provided as context for the rest of the Technical Report. Section 6 is normative and provides requirements, while 0 specifies one profile for each common ACS Northbound Management System. Other types of clients, for which no profiles are specified, can also use the ACS NBI. A profile of an ACS Northbound Management System is specified as a subset of the requirements of Section 6 which includes those requirements that must be fulfilled in order to support the interaction with the given ACS Northbound Management System.

The ACS is assumed to have the ability to support the functions outlined in Section 1.1/TR-069 [2]:

- auto-configuration and dynamic service provisioning,
- software/firmware image management,
- status and performance monitoring, and
- diagnostics

It is not assumed that the ACS itself implements features which are likely to be found in other Operational and Business Support Systems, including order fulfillment, billing, subscriber management, change management, manufacturing management, performance analytics, or service level agreement management. The ACS is likely to integrate with these systems via the NBI. Note that this is not intended to mandate that an ACS cannot implement these other functions should a company choose to build them into their product, but that their presence is not assumed. ACSes may also integrate with each other via the NBI.

The following figure illustrates the relationship between the ACS and other systems.

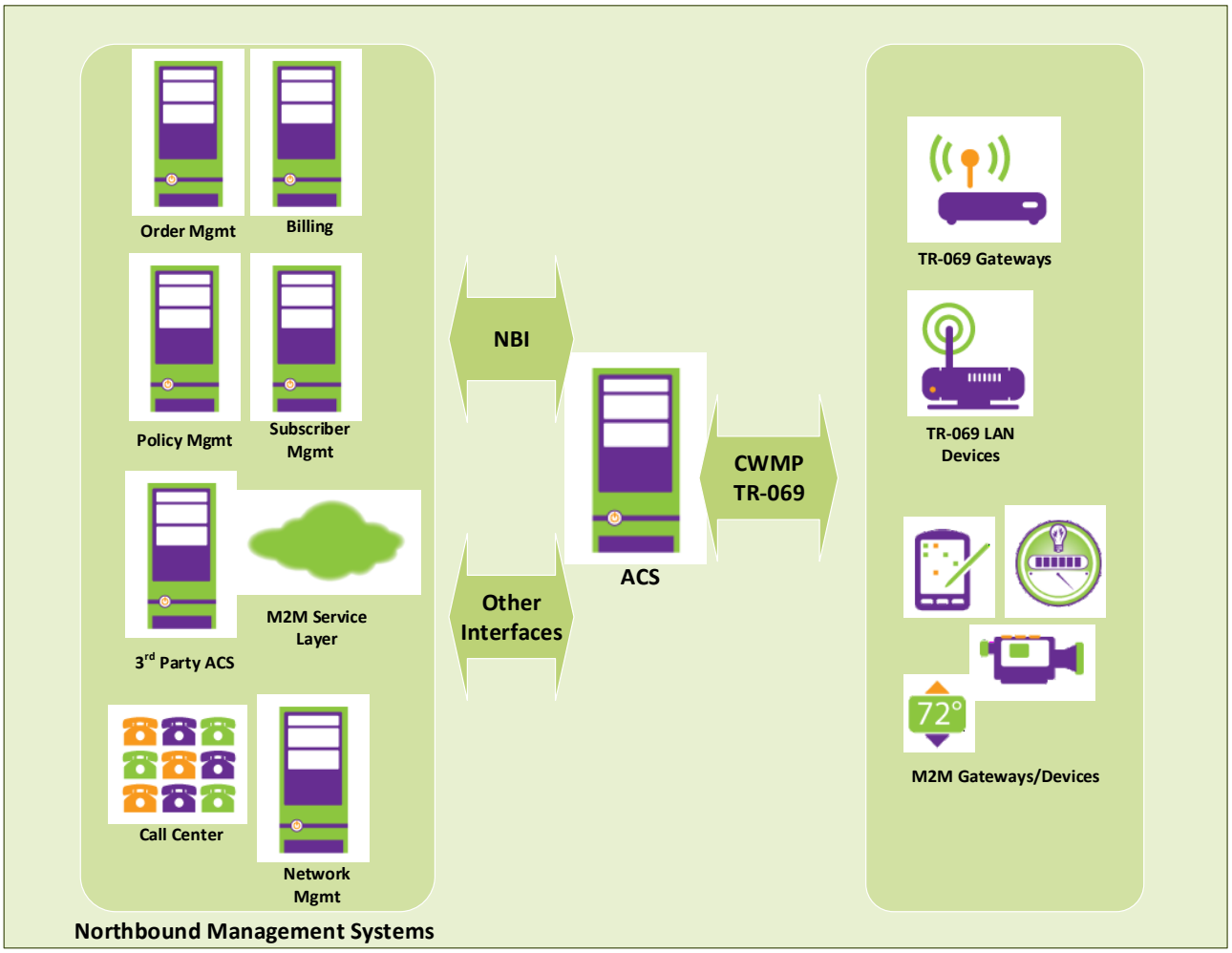

Figure 1 – ACS to Northbound Management Systems Relationships

1.2 Scope

The primary purpose of the NBI is to provide an interface for northbound Operational and Business Support Systems into the ACS for provisioning and managing any devices implementing the CWMP protocol as defined in TR-069 [2]. It also provides a messaging infrastructure to enable the communication of various Events to Operational and Business Support Systems. Devices under management by the ACS could include both those implementing InternetGatewayDevice:1 (IGD) (DEPRECATED) as defined in TR-098 [3], and/or Device:1 and Device:2 as defined in TR-181i1 [5] and TR-181i2 [6] respectively, including any embedded service objects.

The NBI additionally provides an interface for the northbound M2M Service Layer. The M2M Service Layer delegates to the ACS its operations relating to underlying networks consisting of M2M Devices, M2M Gateways and/or CPEs within a M2M Area Networks that are managed by the ACS.

An ACS may also implement alternate or proprietary southbound protocols for device management and none of the requirements expressed in this Technical Report are intended to preclude that possibility.

The NBI requirements are not intended to cover all interfaces between Northbound Management Systems and the ACS. For example, static configuration of ACS systems or ACS GUI definition is considered out of scope for this Technical Report.

This Technical Report specifies the use cases and functional requirements for the NBI, but does not specify the interface itself.

2 References and Terminology

2.1 Conventions

In this Technical Report, several words are used to signify the requirements of the specification. These words are always capitalized. More information can be found be in RFC 2119 [1].

MUST	This word, or the terms “REQUIRED” or “SHALL”, mean that the definition is an absolute requirement of the specification.
MUST NOT	This phrase, or the phrase “SHALL NOT”, means that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the adjective “RECOMMENDED”, means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications must be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase "NOT RECOMMENDED" means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
MAY	This word, or the adjective “OPTIONAL”, means that this item is one of an allowed set of alternatives. An implementation that does not include this option MUST be prepared to inter-operate with another implementation that does include the option.

2.2 References

The following references are of relevance to this Technical Report. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Technical Report are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below.
A list of currently valid Broadband Forum Technical Reports is published at www.broadband-forum.org.

[1]	RFC 2119	*Key words for use in RFCs to Indicate Requirement Levels*	IETF	1997
[2]	TR-069 Amendment 5	*CPE WAN Management Protocol*	Broadband Forum	2013
[3]	TR-098 InternetGatewayDevice:1	*Internet Gateway Device Data Model for TR-069 (DEPRECATED)*	Broadband Forum	
[4]	TR-106 Amendment 7	*Data Model Template for TR-069 Enabled Devices*	Broadband Forum	2013
[5]	TR-181 Issue 1 Device:1	*Device Data Model for TR-069*	Broadband Forum	
[6]	TR-181 Issue 2 Device:2	*Device Data Model for TR-069*	Broadband Forum	
[7]	TS-0002 Version 1.0.1	*Requirements*	oneM2M	2015
[8]	TS-0006 Version 1.0.1	*Management Enablement (BBF)*	oneM2M	2015
[9]	TS-0011 Version 1.2.1	*Common Terminology*	oneM2M	2015

2.3 Definitions

The following terminology is used throughout this Technical Report.

ACS	Auto-Configuration Server; component in the broadband network responsible for auto-configuration and management of devices.
Association	A logical link between two objects, e.g. between a subscriber and a device or between a file and a device.
BSS	Business Support System(s); this is one kind of a Northbound Management System.
Device	Customer Premises Equipment; refers to any TR-069-enabled device and therefore covers both Internet Gateways and LAN-side end devices.
Device Group	The ACS uses the Device Group concept to reference a set of devices that share something in common. Device Group membership is based on data discovered from the device, data pre-provisioned via NBI or data derived from lookups in external systems.
Device Record	The information that the ACS stores about a device.
NBI	Northbound Interface; this Technical Report specifies requirements for a standard NBI between Northbound Management Systems and the ACS: there may be other, non-standard, NBI between the same or other Northbound Management Systems and the ACS.
M2M Area Network	An M2M Area Network is a type of underlying network that minimally provides data transport services among M2M Gateway(s), M2M Device(s), including sensing and actuation devices. M2M Local Area Networks can use heterogeneous network technologies that may or may not support IP access. An M2M Area Network technology is characterized by its physical properties (e.g. IEEE_802_15_4_2003_2_4GHz), its communication protocol (e.g. ZigBee_1_0) and potentially an application profile (e.g. ZigBee_HA).
M2M Device	An M2M Device is physical equipment with communication capabilities, providing computing and/or sensing and/or actuation services. An M2M Device hosts one or more M2M Applications. In terms of CWMP, an M2M Device could be a CPE or a CPE within the M2M Area Network. The M2M Device can be managed by an M2M Service Layer that sits on top of the ACS managing the device. The NBI can provide this interface between the M2M Service Layer and the ACS to manage the M2M Device.
M2M Gateway	An M2M Gateway is physical equipment that includes, at minimum, the entities and APIs of a gateway node. The M2M Gateway can support one or more CPE behind it. The M2M Gateway can provide a pass-through mechanism for the ACS to communicate with the M2M Devices behind the M2M Gateway. The M2M Gateway can also provide a representation of the M2M Devices behind it to the ACS. The M2M Gateway can be managed by an M2M Service Layer that sits on top of the ACS. The NBI can provide this interface between the M2M Service Layer and the ACS to manage the M2M Gateway.

M2M Session	An M2M Session is a service layer communication relationship between endpoints managed via M2M Services consisting of session authentication, connection establishment/termination, transmission of information and establishment/termination of underlying network services. The NBI acts as an interface for handling M2M Sessions between the M2M Service Layer and the ACS.
M2M Service Layer	A set of M2M services provided to M2M applications.
Next Contact	The next time at which a device will contact the ACS due to any trigger such as periodic/scheduled Inform, reboot, active notification or connection request from ACS.
Operation	Method exposed by the NBI to enable interaction with one or more devices.
OSS	Operational Support System(s); this is one kind of a Northbound Management System.
Service	A collection of settings, firmware and/or software versions applied to a device to enable the delivery of some business functionality as defined by the operator.
Subscriber ID	A unique value that is chosen by the Northbound Management Systemto be able to group devices to a subscriber. This is an opaque string to the ACS and represents a billing entity rather than individual users within a subscriber's household.
Vendor Specific Operation	Vendor-specific device operations are those operations supported by a particular device that are not defined by TR-069 and adhere to the naming conventions for vendor-specific CWMP methods as dictated by Appendix A.3.1.1/TR-069.

3 Technical Report Impact

3.1 Energy Efficiency

TR-131 has no impact on energy efficiency.

3.2 IPv6

TR-131 has no impact on IPv6 support and compatibility.

3.3 Security

There are no relevant security issues relating to TR-131.

3.4 Privacy

Any issues regarding privacy are not affected by TR-131.

4 NBI Use Cases

The following NBI use cases are provided to help in the understanding of how the ACS provided NBI can be used. It is not necessarily assumed that each use case will generate a set of requirements for the standardized NBI.

4.1 Initial Device Provisioning

In this use case, a subscriber installs a device and connects it to the network for the first time. When the device is provisioned, the ACS will notify all registered Northbound Management Systems informing them that a particular device has been provisioned.

Before the device contacts the ACS, the Northbound Management Systems may add devices to the ACS data store by adding device identifiers connected to the initial desired configuration. This use case calls for the ACS to configure or re-configure the device upon bootstrap, which may involve upgrading the device firmware as well as configuring various parameters.

In addition to adding device information to the ACS, there also needs to be a clean-up feature to be able to remove unused devices.

The device management functionality can also be used by an inventory system.

4.1.1 Pre-registered Device and Unregistered Subscriber

In this use case, the subscriber installs the device before registering for service with the service provider. The ACS is pre-provisioned with sufficient data to be able to authenticate the device when it appears on the network and provide it with basic configuration. In one example usage, this basic configuration may configure the device for limited service that enables the subscriber to register for fuller service. Once the subscriber registers for service, the ACS is updated by the Northbound Management Systems with sufficient information to re-configure the device for the appropriate service(s).

4.1.2 Pre-registered Device and Pre-Registered Subscriber

In this use case, the subscriber registers for service before the device is installed. The ACS is pre-provisioned with sufficient data to be able to authenticate the device and configure it for a given service. The configuration of the device may involve upgrading device firmware as well as configuring various parameters.

4.2 Subscription to New Service

In this use case, a subscriber who has previously installed and configured their device subscribes to a new service. In this scenario, it is assumed that an order management or other Northbound Management Systems has already validated the subscriber's access to the particular service. The Northbound Management Systems may use the ACS to determine the device's capability to support the new service.

The Northbound Management Systems then instruct the ACS to execute any required changes that enable that service for the device. The ACS may change the device configuration parameters,

upgrade firmware, or install new software as appropriate. It then reports the results of the operation to the Northbound Management Systems.

4.3 Firmware/Software Management

This use case covers a couple of different firmware/software management use cases. These use cases apply to managing any software or firmware images on the device.

4.3.1 Pass-Through Firmware Management

In this use case the ACS functions as a pass-through proxy to force an upgrade of a particular device's firmware. This enables Northbound Management Systems to take direct control over firmware management as opposed to delegating such responsibilities to the ACS.

4.3.2 Firmware Reporting

In this use case, the Northbound Management Systems needs to determine the firmware currently used by a given device. The Northbound Management Systems contacts the ACS, which can query the device for its current firmware version.

4.3.3 Pass-Through Software Management

In this use case the ACS functions as a pass-through proxy to perform software management of a particular device's modular software. This enables Northbound Management Systems to take direct control over software management as opposed to delegating such responsibilities to the ACS.

4.3.4 Software Reporting

In this use case, the Northbound Management Systems needs to determine the software currently used by a given device. The Northbound Management Systems contacts the ACS, which can query the device for its currently installed software.

4.4 Device and Service Diagnostics

In this use case, a subscriber has some problem with their service and contacts the service provider's help desk to diagnose and repair the issue.

Upon the subscriber reaching the help desk, the operator identifies the customer's Subscriber ID. The tech support Northbound Management Systems then retrieves a list of devices stored in the ACS for this Subscriber ID. The Northbound Management Systems then retrieves information about each or a particular device from the ACS. This information may include data pre-provisioned into the ACS, data discovered from the device during prior interaction and stored by the ACS, and real-time data retrieved from the device if it is reachable. Additionally, the Northbound Management Systems may instruct the ACS to execute diagnostics tests supported by both the ACS and the device, and report the results. The ACS might support diagnostics tests that operate on more than one device, e.g. on all of a subscriber's devices.

Using these results the Northbound Management Systems determines the root cause of the fault and any repairs to be executed on the device or whether the problem is due to some other issue (e.g. subscriber account fault, network problem). If the problem requires changes to the device, the ACS

makes the necessary changes, validates the new settings, and reports the results to the Northbound Management Systems. The Northbound Management Systems then validates that the subscriber problem has been solved.

4.5 Device Management

In this use case, the service provider wants to manage various aspects of the service provided by the device and uses the ACS to assist in collecting the necessary information. The ACS assists the Northbound Management Systems in collecting any of the following information from the devices:

- Performance and error statistics reported by the device
- Device log files
- Results of running diagnostics tests
- Device parameters configured by the LAN-side protocols
- Any other data exposed in the device parameter model

The Northbound Management Systems may request that the data be retrieved from a given device in real-time if the device is reachable or it may request that the data be retrieved upon the next connection established by the device.

The ACS also enables the Northbound Management Systems to register for and receive any notifications supported by the device.

Finally, the ACS exposes to the Northbound Management Systems any data that has been pre-provisioned into the ACS as well as any data that the ACS discovered from the device and stored in its database.

4.6 Replacement of a Device

In this use case, a subscriber needs to return a faulty device to the service provider. The replacement device that is provided to the customer may be the same or a different model produced by the same or different manufacturer. The ACS is updated with the information about the new device. The ACS then configures the new device as in the initial installation use case. In a more advanced version of this use case, the user-modified settings stored on the device are automatically restored on the new device to the extent possible given the new device's capabilities.

5 Key Concepts

This section provides non-normative description of key NBI concepts.

The NBI provides the means for Northbound Management Systems entities to interact with devices under an ACS's management purview. Northbound Management Systems may learn device state, configure and troubleshoot it in order to enable services or satisfy management policies.

5.1 Device Groups

Because an ACS manages millions of devices, service providers are likely to wish to manage groups of devices in many scenarios rather than attempt to configure and monitor each device individually.

Device groups can be based on search criteria, which might use information discovered from the device itself. Some of this information might be static, such as make and model or device capabilities, or it might be dynamic information such as firmware version or enabled interfaces. Grouping can also use other information associated with the device, such as subscriber information.

Device groups can also consist of named collections of devices, for example a group of all devices within a specific geographic location, or devices identified as requiring enhanced monitoring. The methods by which these named groups are created or maintained is implementation specific, although the NBI provides a means to discover the available named groups as well as a way to associate a device to a group and dissociate a device from a group.

Note: This Technical Report does NOT attempt to standardize the mechanisms for defining, adding and removing device groups via the NBI. This task is best accomplished via specialized UIs provided by the ACS, which provides a key point of differentiation for ACS vendors.

5.2 Device Operations

Device operations allow any number of Northbound Management Systems to instruct the ACS to perform operations on the device.

Device operations are designed to mimic the RPCs supported by CWMP. These operations allow Northbound Management Systems to retrieve data from the device, reboot it, set parameters, etc.

Device operations may be targeted at a single device or at any of the types of device groups.

5.3 Device Connectivity

In order to execute CWMP operations against the device, the ACS must have connectivity with the device. TR-069 [2] describes multiple options for establishing the CWMP session.

If the device is reachable by the ACS, the ACS may issue a connection request to the device causing it to contact the ACS. The device, however, may not be reachable from the ACS if it is behind a NAT-enabled device, does not have an active connection or is simply not powered up. In these

situations, the ACS has to rely on the device establishing a connection on its own (or, even when the device is contactable, the ACS may choose to wait for the device to contact it). The device may establish a connection based on a variety of events such as reboot, notification, scheduled periodic contact, etc.

In order to support these situations, the NBI contains concepts both of timeliness of the operations and time span of the operations. Timeliness refers to allowing the Northbound Management System to specify whether the ACS should wait for the device's connection trigger, contact the device to establish a connection immediately, or arrange for a connection to be established at some time in the future, e.g. so that an operation will take place within a maintenance window determined by the Northbound Management System. Time span refers to the length of time it takes to reach the device, set up a session, perform the desired actions, validate their success, and report back results to the Northbound Management System. These device connection issues affect operations, responses, errors, and session timeouts throughout the NBI.

5.4 M2M Device Management

An M2M Service Layer can delegate an interaction with a CPE it manages to an ACS that is already managing the CPE. In order to support this interaction, the ACS will support M2M session establishment and maintenance mechanisms. Additionally, the M2M Service Layer might require support for multiple M2M sessions with the ACS. These multiple sessions will be based on a security model between the M2M Service Layer and the ACS.

The ACS can detect changes within CPEs it manages. If the M2M Service Layer has expressed interest in changes in a CPE but doesn't currently have a M2M Session established between the M2M Service Layer and the ACS, the ACS can notify the M2M Service Layer to establish an M2M Session. The ACS can retain any notifications or change of resources based on the provisioned event notification policy until the M2M Session is established.

The NBI can provide an interface so that discovered CPEs or resources/data of the CPE that is of interest to the M2M Service Layer can be synchronized with the ACS when the CPE or the CPE's resource/data is added, updated or removed.

6 Interface Requirements

This section contains the normative requirements of the NBI as guided by the use cases and key concepts described above.

6.1 Architecture (A)

Identifier	Requirement
A 1	The NBI MUST accommodate transactional updates of the ACS data store. This means that all data store updates MUST be done atomically, in an all-or-nothing fashion, for a single NBI method call.
A 2	The NBI MUST enable the Northbound Management System to issue an NBI operation that can lead to multiple Device Operations.
A 3	The NBI MUST document the exact transaction isolation between different operations. For example, whether or not large queries lock data. Note: this is not a run-time requirement.
A 4	Device operations MUST be designed to provide support for the full functionality of the underlying TR-069 [2] mechanisms. For example, this means that the all-or-nothing property of SetParameterValues also applies to NBI device operations. Note, though, that this all-or-nothing property applies only to a single device and, as within TR-069 [2], within the context of a single RPC; if operations are requested against multiple devices, they may succeed in one device and fail in other devices.
A 5	The NBI MUST define mechanisms to support triggering immediate updates to device configuration (when the device is available) as well as updates on device next contact. This addresses the environments in which the device cannot be contacted on demand.
A 6	The NBI MUST provide a transport binding which is based on standard technology with widely available tooling and which is programming language- and platform-neutral.
A 7	The NBI MUST provide support for standards-based security. This includes authentication of both Server and Client, authorization, link security so that it can be verified that the content has been sent from the appropriate sender and was not modified while in transit. Information should also be confidential (encryption).

Identifier	Requirement
A 8	The NBI MUST support both Point-to-Point and Publish/Subscribe notification mechanisms. A Point-to-Point notification mechanism uses a direct connection between each client and the server. A Publish/Subscribe mechanism allows the server to publish messages and each client can subscribe to the messages that it is interested in.
A 9	All NBI functions that act upon a specific device MUST use a unique device identifier to address the device. This identifier MUST be unique across all devices (under ACS management) of all vendors.
A 10	The NBI MUST be machine-readable, i.e. it MUST be possible for Northbound Management Systems to determine which NBI functions are implemented by the ACS, and details of their arguments and returned values.
A 11	The NBI MUST maintain a version number that contains both a major and minor version. The NBI MUST maintain backwards compatibility between different minor versions, except in the rare cases of known problems (errata) which MAY be corrected through a non-backwards compatible minor version. Backwards compatibility is achieved by only allowing the addition of new NBI functions and not altering or removing existing NBI functions. In the case that the NBI is changed, the current version of the NBI SHOULD be discoverable via the NBI itself.
A 12	The NBI SHOULD scale to returning millions of records in various searching and enumeration calls. The NBI MUST gracefully fail in the situations in which a particular call leads to the return of more records than the NBI can provide.
A 13	The NBI MUST provide an interface to the Northbound Management Systems to create a session (e.g. M2M Session) with the ACS.
A 14	The NBI MUST provide an interface to the Northbound Management Systems to maintain an already created session (e.g. M2M Session) with the ACS.
A 15	The NBI MUST provide an interface to the Northbound Management Systems to gracefully tear down an already created session (e.g. M2M Session) with the ACS.

Identifier	Requirement
A 16	The NBI SHOULD provide an interface to the ACS to initiate a session (e.g. M2M Session) towards the Northbound Management Systems in case a session is required and doesn't already exist between the Northbound Management Systems and the ACS.
A 17	The NBI SHOULD support establishment of multiple sessions (e.g. M2M Sessions) with the Northbound Management Systems based on the security model between the Northbound Management Systems and the ACS.

6.2 Device Data Pre-Provisioning (DDPP)

Identifier	Requirement
DDPP 1	The NBI MUST provide a primary unique identifier for each device, which includes: * Serial number * Manufacturer OUI * Product class (could be an empty string)
DDPP 2	The NBI MUST provide a mechanism to add a device record to the ACS data store.
DDPP 3	The NBI MUST provide a mechanism to manipulate (add, modify, retrieve, and delete) device data that has been provisioned into the ACS related to a specific device record.
DDPP 4	The NBI MUST allow the assignment of pre-provisioned data to a specific device by using its unique identifier.
DDPP5	The NBI MUST provide a mechanism to remove a device record from the ACS data store.

6.3 Subscriber to Device Association (SDA)

Identifier	Requirement
SDA 1	The NBI MUST provide a mechanism to associate a Subscriber ID with one or more devices. A device's association MUST NOT span more than one Subscriber ID. The NBI MAY provide a mechanism to add a Subscriber ID without an association to a device.
SDA 2	The NBI MUST provide a mechanism to dissociate a Subscriber ID from a device.
SDA 3	The NBI MUST provide a mechanism for returning the Subscriber ID for a given device identifier.
SDA 4	The NBI MUST provide a mechanism for returning a list of device identifiers for all devices that are associated with a particular Subscriber ID.
SDA 5	Void
SDA 6	The NBI MUST support the use of search filters/constraints when searching for a list of Subscriber IDs.

6.4 Device Data Retrieval (DDR)

Identifier	Requirement
DDR 1	The NBI MUST be able to differentiate between live device data and cached data from the ACS data store.
DDR 2	The NBI MUST allow the retrieval of live device state for parameters and objects, that is names, current values, and attribute settings.
DDR 3	The NBI MUST support the retrieval of data previously discovered from the device through device/ACS interactions and saved within the ACS data store. The type and quantity of data stored within the ACS is a matter of ACS implementation and Service Provider policy.
DDR 4	Void
DDR 5	The NBI MUST support the use of search filters/constraints when searching for a list of device identifiers.

6.5 Device Operations (DO)

Identifier	Requirement
DO 1	The NBI MUST allow the retrieval of TR-069 [2] device operations supported by the ACS.
DO 2	The NBI MUST support delegating device operations to the Northbound Management System. The NBI MUST support delegating the REQUIRED CPE methods as defined in TR-069 [2]. The NBI MAY support delegating the OPTIONAL CPE methods as defined in TR-069 [2].
DO 3	The NBI MAY support delegating vendor-specific device operations.
DO 4	The NBI MUST support making the results of individual device operations available upon completion. Note: this is not a synchronous requirement.
DO 5	The NBI MUST support the execution of device operations (both those defined in TR-069 [2] and vendor-defined RPCs) on an individual or group of devices governed by the execution criteria.
DO 6	The NBI MUST support making available the results of group device operations. Available results MUST include the overall success/failure for the group, individual device status, and any errors.

DO 7	Execution criteria determine when a device operation will be executed. Execution criteria MAY include
	• When to execute:
	  ○ Immediate execution
	  ○ Execution on "next device contact"
	  ○ Day/time window execution
	• Retry policy
	• Time out

DO 8	The NBI MUST allow the retrieval of all pending (not started) and running device operations for a specified device
DO 9	The NBI MUST allow the retrieval of pending (not started) and running operations for a group of devices
DO 10	The NBI MUST allow the retrieval of the status (at a summary level) of all pending (not started) and running individual and group device operations

Identifier	Requirement
DO 11	The NBI MUST allow the removal of all pending (not started) individual and group device operations. Note: Only scheduled operations that have not been started are allowed to be removed.
DO 12	The NBI MUST allow the removal of a specified pending (not started operation) device operation from a specified device. Note: Only scheduled operations that have not been started are allowed to be removed.
DO 13	The NBI MUST allow the removal of a specified pending (not started) device operation from a specified group of devices. Note: Only scheduled operations that have not been started are allowed to be removed.

6.6 File Management (FM)

Identifier	Requirement
FM 1	The NBI MUST provide a mechanism to manage device files using device pass-through operations corresponding to Download and Upload RPCs (this is really just a subset of DO2 as these 2 RPCs are already covered with that requirement). Files could be based on the File Types as defined in Section A.3.2.8 Download and Section A.4.1.5 Upload of TR-069 [2].
FM 2	The NBI MAY provide a mechanism to add files to the ACS. A file consists of metadata (e.g., manufacturer, model, type, file description, version, owner, link to file location) and optionally, file contents.
FM 3	The NBI MAY provide a mechanism for scheduling (might be immediate) the association of a file of any file type with a specified device or group of devices with the same triggering requirements as those outlined in DO7. An association means that it becomes a relation between the device and the file, the file will eventually be downloaded to the device.
FM 4	The NBI MAY provide a mechanism for deleting files from the ACS. A file consists of metadata (e.g., manufacturer, model, type, file description, version, owner, link to file location) and, optionally, file contents. Only files that have no associations can be removed.
FM 5	The NBI MAY provide a mechanism for updating files in the ACS. A file consists of metadata (e.g., manufacturer, model, type, file description, version, owner, link to file location) and, optionally, file contents. It is the responsibility of the Northbound Management System to ensure that file metadata and contents are in sync.
FM 6	The NBI MAY provide a mechanism for searching files in the ACS. A file consists of metadata (e.g. manufacturer, model, type, file description, version owner, link to file location) and, optionally, file contents. Searching can, for instance, be based on which files are associated to a given device, or which files are associated to a given device type, as well as other similar queries.
FM 7	The NBI MAY provide a mechanism for retrieving files in the ACS. A file consists of metadata (e.g., manufacturer, model, type, file description, version, owner, link to file location) and, optionally, file contents.

6.7 Events (E)

Identifier	Requirement
E 1	The NBI MUST provide a mechanism for northbound clients to subscribe to events.
E 2	The NBI MUST provide a list of events for which a northbound client can subscribe
E 3	The NBI MUST provide a mechanism for northbound clients to unsubscribe from events.
E 4	The NBI MUST provide a list of any event filters that it supports
E 5	The NBI MUST provide an event delivery mechanism.
E 6	The minimum set of events to be included in the event delivery filters MUST include: 1. CWMP event code 2. Specific parameters changing value 3. By device 4. By any combination of the above
E 7	The NBI SHOULD support retention of any notifications or changes in the managed resources based on an Event Retention Policy (for example: time, number of events).

6.8 Device Grouping (DG)

Identifier	Requirement
DG 1	The NBI MUST provide a mechanism to enable Northbound Management Systems to perform operations on collections of CPE.
DG 2	The NBI MUST allow for the targeting of groups of devices based on search criteria.
DG 3	The NBI MUST support the use of search filters/constraints when searching for groups, returning a list of currently available group names and the name of any required input arguments.
DG 4	The NBI MUST enable operations to be performed on a named group of CPEs.

Identifier	Requirement
DG 5	The NBI is NOT REQUIRED to provide a mechanism to create, update (except for group membership), or delete groups.
DG 6	The NBI MUST provide a mechanism to get a list of all device identifiers that are members of a given named group.
DG 7	The NBI MUST provide a mechanism to manage the membership of named groups.
DG 8	The NBI MUST provide a mechanism to remove a device from a named group, but only if the group is not constrained by search criteria.
DG 9	The NBI MUST provide the list of groups to which a specific device is a member of.
DG 10	The NBI MUST provide an optional mechanism to change a device from one named group to another named group.

6.9 Error Management (EM)

Identifier	Requirement
EM 1	The NBI MUST support returning an error result when a Northbound Management System makes a request with an invalid function, or invalid parameters.

6.10 Security (SE)

Identifier	Requirement
SE 1	The NBI MUST ensure the confidentiality of data exchanged between the Northbound Management Systems and the ACS.
SE 2	The NBI MUST ensure protection against security threats for sessions between the Northbound Management Systems and the ACS.
SE 3	The NBI MUST ensure the integrity of data exchanged between the Northbound Management Systems and the ACS.

6.11 Access Control (AC)

Identifier	Requirement
AC 1	The NBI MUST provide an interface to authorize Northbound Management Systems to access CPE or a group of CPE.
AC 2	The NBI MUST provide an interface for the Northbound Management Systems to discover the access management elements used to authorize and authenticate access to resources controlled by the ACS.

Annex A: Northbound Management Systems Profiles

This section specifies the requirements that are applicable to the Northbound Management Systems based on usage profile.

A.1 OSS/BSS Profile

OSS/BSS profile requires that the following requirements are supported:

1. Architecture (A1-A12)
2. Device Data Pre-Provisioning (DDPP1-DDPP5)
3. Subscriber to Device Association (SDA1-SDA4, SDA-6)
4. Device Data Retrieval (DDR1-DDR3, DDR-5)
5. Device Operations (DO1-DO13)
6. Events (E1-E6)
7. Device Grouping (DG1-DG10)
8. Error Management (EM1)
9. Security (SE1-SE3)

A.2 M2M Service Layer Profile

M2M Service Layer profile requires that the following requirements are supported:

1. Architecture (A1-A17)
2. Device Data Pre-Provisioning (DDPP1-DDPP5)
3. Subscriber to Device Association (SDA1-SDA4, SDA-6)
4. Device Data Retrieval (DDR1-DDR3, DDR-5)
5. Device Operations (DO1-DO13)
6. Events (E1-E7)
7. Device Grouping (DG1-DG10)
8. Error Management (EM1)
9. Security (SE1-SE3)
10. Access Control (AC1-AC2)

A.3 ACS File Management Profile

ACS File Management Profile requires that the following requirements are supported:

1. File Management (FM1-FM7)

Note: Requirements mentioned above, for example: A1-A17, captures inclusive support for Requirements from A1 to A17.

End of Broadband Forum Technical Report TR-131 Issue 1 Amendment 1

