LACNOG-M³AAWG Joint Best Current Operational Practices on Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition LAC-BCOP-1

May 2019

This document is available on the LACNOG website at www.lacnog.net/docs/lac-bcop-1

This document is available on the M³AAWG website at www.m3aawg.org/CPESecurityBP

This is a joint Best Current Operational Practices (BCOP) document developed by LACNOG[1] (Latin American and Caribbean Network Operators Group) and M³AAWG[2] (Messaging, Malware and Mobile Anti-Abuse Working Group). It is the product of LACNOG's original drafts by its working groups LAC-AAWG[3] (Latin American and Caribbean Anti-Abuse Working Group) and BCOP Working Group[4], in cooperation with M³AAWG members, Senior Technical Advisors and the M³AAWG Technical Committee.

Table of Contents

[1]The Latin American and Caribbean Network Operators Group (LACNOG), https://www.lacnog.net/
[2]Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), https://www.m3aawg.org/
[3]Latin American and Caribbean Anti-Abuse Working Group (LAC-AAWG), https://www.lacnog.net/lac-aawg/
[4]LACNOG BCOP Working Group, https://www.lacnog.net/wg-bcops/

Executive Summary

"Customer Premise Equipment" (CPE) is the equipment used to connect subscribers to an Internet Service Provider's (ISP) network. Examples of CPE include modems (cable, xDSL, fiber) and WiFi routers, among others.

Due to vulnerabilities in the embedded software and in default configurations, CPE has been the target of a variety of abuses, ranging from the exploitation of misconfigured services and default authentication credentials to complete compromise by malware. The purpose of many of these attacks is to conduct denial-of-service (DoS) attacks, unauthorized cryptocurrency mining, malware propagation, spamming, phishing, theft of credentials and other abuse.

In general, common vulnerabilities have included:

- Standard credentials for a large number of devices
- Credentials that cannot be changed (hard-coded)
- Use of obsolete and insecure protocols and algorithms
- Undocumented accesses (backdoors)
- Lack of automated and secure update mechanisms to address security issues
- Unnecessary and/or insecure services enabled by default
- Services that cannot be disabled
- Insecure remote management

This document is intended to identify a minimum set of security requirements that should be specified when ISPs purchase CPE to ensure that such CPE has a secure default configuration and a secure remote management and update mechanism. The goal is to reduce the risk of compromising the provider's network, and the Internet as a whole, and to minimize the costs and impact resulting from the abuse of the equipment by attackers, such as degradation or unavailability of services, technical support and repair work.

It is out of the scope of this document to provide a complete set of features or the hardware and software specifications that CPE must support[5]. For the purpose of this document, it is assumed that IPv6 and IPv4 protocols are supported, implemented and enabled.

1. Terminology

For purposes of this document:

1. Customer Premise Equipment (CPE): the equipment used to connect subscribers to the Internet Service Provider's (ISP) network. Different names may be used by others to describe this kind of devices, such as Customer Edge (CE) Router and Residential Gateway (RG).

2. Firmware: the software that runs on the CPE, including the Operating System, and may also include network interface software, software packages and services, and configurations.

3. Backdoor: any mechanism inserted into the system with the aim of enabling undocumented access to the system or its data. Examples of backdoors include an undocumented hard-coded username with no password, a fixed password or a predictable "password-of-the-day," or undocumented services for

[5] Not including requirements regarding IPv6 support and implementation as part of the CPE purchasing specification may result in a business risk for ISPs as they may not be able to provide IPv6 connectivity to their customers. This presents a business growth risk to the ISP due to IPv4 address exhaustion.

performing administrative functions without authentication, among others. A backdoor can be included intentionally (designed to guarantee later access) or accidentally (used for development purposes and then inadvertently included in general availability firmware). Backdoors can also arise as a consequence of bad programming practices.

4. Appropriate encryption/cryptography: open standard cryptographic algorithms/protocols published by the Internet Engineering Task Force (IETF) or other standards organizations in their current versions. The implementation must allow for the selection of up-to-date cipher suites and key sizes.

5. Hard-coded credentials: credentials with common values fixed in the product source code (the same for all installations of the product) that cannot be changed or disabled except by patching the source code (and consequently releasing a new binary/firmware).

6. Service (server-type process, or *daemon*): a server process that is actively waiting for connections on a particular port, not the client software that performs queries to a service, when necessary.

7. DEFAULT: a configuration set by the vendor.

8. The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 RFC 2119 [2], and RFC 8174 [3] when, and only when, they appear in all capitals, as shown here.

2. General Requirements (GR)

GR-01: The description of the device MUST include the complete identification of its main components, in particular:

a. Manufacturer, model and chipset versions

b. Name, version and date of release of the firmware and the base operating system

GR-02: The vendor MUST provide documentation that describes at minimum:

a. Name, version, date of release, and functionality of the firmware or operating system

b. Name, version, date of release, and factory-boot status (e.g. on or off by default) of all applications and services installed on the device

GR-03: The vendor MUST provide the following information for any open source software used:

a. List of all relevant licenses for each open source software used

b. Complete name and version of each open source software incorporated into the CPE system

GR-04: Contact information for vulnerability disclosure (VR-03) SHOULD be included at some point (e.g. page, tab, etc.) in the CPE graphical user interface (GUI).

GR-05: The vendor SHOULD provide information to the user if the CPE is out of the support period (see VR-01 and VR-02) and is no longer receiving firmware updates (e.g. via the graphical user interface).

3. Software Security Requirements (SSR)

SSR-01: Credentials MUST NOT be hard-coded. Also see FR-04 and FR-05.

SSR-02: Sensitive credential data (e.g. passwords, keys, and security tokens) stored on the device MUST be protected by appropriate hashing/cryptographic algorithms. Cryptographic keys SHOULD be stored in secure hardware, if available.

SSR-03: General data that is stored on the device SHOULD be protected by appropriate encryption.

SSR-04: Any software tools or backdoors used for firmware or system development MUST be removed in the mass production version.

4. Update and Management Requirements (MR)

MR-01: The CPE MUST implement a mechanism for remote management with, at minimum, remote administration using an appropriate encryption protocol. Check the table in Annex I for the list of required protocol(s).

MR-02: The CPE MUST implement a mechanism for secure remote updating. Check the table in Annex I for the list of required protocol(s).

MR-03: The remote management and administration, and remote updating mechanisms MUST support:

a. Secure authentication, and
b. Encrypted connections, and
c. Access restrictions to limit connections to specific sources (e.g. selected network segments, a specific URL, etc.), and
d. The ability to choose the connection port (i.e. support changing the port number from the DEFAULT/assigned port for the service [17]).

MR-04: In the case of automated and secure updating, a mechanism MUST be implemented to authenticate and validate the source repository.

MR-05: The CPE MUST implement a mechanism to verify – before proceeding with the actual update (typically in the flash memory) – the integrity and the authority of the downloaded file and if it is intended for that device (e.g. it is meant for the device architecture, model, version, etc.).

MR-06: The update process MUST preserve the existing settings. A vendor MAY change an existing setting if such change improves the security of the device. Such change MUST be clearly documented.

MR-07: Regarding checking for updates, CPE:

a. MUST have the ability to run periodic checks to pull updates on an automated, scheduled basis;
b. MUST allow user to initiate checking for updates.
c. SHOULD support ISP-prompted push updates on an on-demand basis.

MR-08: CPE MUST implement mechanisms to safeguard from becoming useless as result of firmware update failure (bricking). The recovery procedures MUST be clearly documented and MUST NOT require accessing internal parts of the hardware.

5. Functional Requirements (FR)

This document assumes that IPv6 support in accordance with RFC 7084 [8] is part of the general purchasing requirements document.

These features must be supported or removed from the CPE:

FR-01: CPE MUST NOT enable on the WAN BY DEFAULT services that allow the disclosure of sensitive information or can be abused to perform amplification attacks (e.g. Telnet, FTP, SOCKS, CHARGEN, SNMP, etc.)

FR-02: CPE MUST implement remote update and remote management functionalities as described in the Update and Management Requirements (MR) session of this document.

FR-03: Any end user management communication from the LAN/WLAN to the CPE MUST be authenticated[6] and SHOULD be encrypted.

FR-04: Any authentication information (e.g. passwords) MUST be changeable, including the master administration (root) password. User identifiers (e.g. usernames) SHOULD be changeable.

FR-05: Regarding the password for accessing administrative interfaces:

a. The initial password MUST be unique for each device and MUST NOT be derived from information that can be obtained via packet capture or similar methods of observation (e.g. MAC address);
b. At any time when a password is changed or reset, the password MUST NOT be null (i.e. empty, blank) nor the same as the username, and relevant best practices for password complexity MUST be followed.

FR-06: The production firmware MUST NOT have any undocumented mechanism for accessing the system or its data.

FR-07: The device MUST NOT have undocumented communication mechanisms to send data to the vendor or third parties. Any communications and data sent to the vendor or third parties MUST be explicitly documented[7].

FR-08: An authenticated end user MUST be able, via the graphical user interface:

a. To change user-specific settings as appropriate (e.g. WiFi network name, firewall/forwarding rules, etc.), and
b. To disable any service that is not essential to the operation or administration of the device.

FR-09: When enabling the operation of services for users on the CPE's LAN/WLAN interface(s), such services MUST NOT be accessible from the WAN/Internet, in particular services such as DNS, NTP, SSDP, UPnP, or any other protocol that might be used in amplification attacks.

[6] CPE may support alternative authentication mechanisms to offer a higher level of security than simply username/password.
[7] Data protection legislations in many countries/regions may put special requirements on the processing of personal data, requiring it to be detailed and explicitly documented.

FR-10: In order to use a monitoring and/or management service/agent:

a. The configuration of an appropriate authentication mechanism for setting values and/or for retrieving information/sensitive data MUST be required;

b. Access from the WAN interface(s) MUST use authentication and MUST be restricted to specific source(s) (e.g. to a selected network segment or address).

FR-11: The device MUST implement open standards-based cryptographic methods in their current versions that allow the selection of safe parameters regarding cipher suite and key sizes.

FR-12: Cryptographic services or applications involving the generation of keys and/or digital certificates for device authentication MUST generate the keys for each device; i.e. a private key MUST NOT be shared among different devices.

FR-13: The CPE MUST support time synchronization through a centralized time protocol, such as the Network Time Protocol (NTP). Only NTP client software is required. The CPE MUST NOT have a hard-coded configuration for NTP servers and MUST NOT use BY DEFAULT servers the vendor does not have permission to use.

FR-14: The CPE SHOULD support RFC 6092 "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service"[6]. In the event of a conflict between RFC 6092 and this document, the requirement of this document will prevail.

FR-15: The CPE MUST support anti-spoofing filtering in accordance with BCP 38 RFC 2827 [12] for both IPv4 and IPv6. It MUST be a selectable option enabled BY DEFAULT. It is out of the scope of this document to determine the technique to be used for source IP address validation.

FR-16: The CPE SHOULD support packet filtering for Special-Purpose IP Addresses. Addresses considered "Globally Reachable" FALSE AND "Forwardable" FALSE, in accordance with RFC 6890 [13] and RFC 8190 [14], SHOULD be filtered. In this case, CPE SHOULD be capable of being configured to include IPv4 and IPv6 addresses in accordance with the registries maintained by IANA (Internet Assigned Numbers Authority) as described in "IANA IPv4 Special-Purpose Address Registry" [15] and "IANA IPv6 Special-Purpose Address Registry" [16].

FR-17: CPE MUST NOT act as an open resolver. Regarding DNS services:

a. DNS queries received on the WAN port and destined for the CPE itself MUST NOT be permitted or responded to in any way.

b. DNS queries received on the WAN port and intended to be forwarded out the LAN port MAY be permitted as long as an explicit rule exists for this in the CPE configuration (e.g. forwarding rule, firewall rule, etc.)[8].

c. If the CPE is running a local DNS server, it SHOULD set outbound DNS queries to perform DNSSEC validation.

d. If the CPE is not running a local DNS server and is instead forwarding DNS queries to another server, then it MUST NOT remove DNSSEC validation markings from DNS queries if they exist.

[8] The CPE should not prevent the user from hosting a DNS server in the LAN. It is worth mentioning that a forwarding/firewall rule in this case makes sense only if an authoritative DNS server is running in the LAN.

FR-18: When WiFi is provided, CPE:

a. MUST implement security mechanisms with appropriate cryptography.

b. SHOULD support the latest version of the Wi-Fi Protected Access (WPA)® security features specification.

FR-19: Passwords MUST NOT be visible in clear text BY DEFAULT in any management interface. Passwords MAY be made visible when requested by the user.

FR-20: There SHOULD be a method to download the device configuration in a clear text format (ASCII or UTF-8), providing that any sensitive information (e.g. passwords, community strings, etc.) are redacted from the output.

6. Initial Configuration Requirements (IR)

Devices MUST have the following factory default settings:

IR-01: CPE MUST be restrictively configured rather than permissively configured. All services (i.e. server-type processes) that are not strictly necessary for the initial configuration process (bootstrapping) MUST be disabled, especially (if implemented) SSDP, SNMP, UPnP, SOCKS, SMB, Bandwidth Test (ergo imbedded iperf, and others). In addition, services that are enabled or can be turned on SHOULD operate in a restrictive and/or secure default mode.

IR-02: Parameters related to DNS server addresses (resolver addresses) MUST be unconfigured and the DNS Relay option (if implemented) MUST be disabled.

IR-03: The port forwarding or DMZ host option, if available, MUST be disabled BY DEFAULT.

IR-04: The initial password for accessing administrative interfaces, both graphical and command line, MUST be unique for each device and it MUST be possible to identify it visually on the device label.

IR-05: When WiFi is provided, the WiFi network(s) MUST have a unique initial password, NOT equal to the WiFi SSID, and it MUST be possible to identify the initial password(s) visually on the device label. The password(s) SHOULD be different from the DEFAULT admin password.

IR-06: When WiFi is provided, the WiFi Service Set Identifier(s)(SSIDs) DEFAULT value(s) MUST NOT be related to the vendor name nor the product model and it MUST be customizable. Check the table in Annex I for ISP customized DEFAULT values[9].

IR-07: In the case of SSH service, the server's key pair MUST NOT be pre-generated at the factory. The key MUST be generated after the first service initialization/boot and any factory reset of the device shall cause a new key to be generated. The generated key pair shall provide enough security bits to be considered secure at the time of deployment.

IR-08: Anti-spoofing filtering [FR-15] MUST be enabled BY DEFAULT.

IR-09: IPv6 transition mechanisms, tunnels, VPNs and similar services MUST be disabled BY DEFAULT.

[9] In case the ISP wants to choose how SSIDs are to be named BY DEFAULT (e.g. a single name for all devices or unique names per device), the ISP will need to describe how SSIDs MUST be named. Otherwise, the vendor may choose the DEFAULT.

7. Vendor Requirements (VR)

The vendor:

VR-01: MUST have a clear product support policy, especially regarding the availability of fixes for security vulnerabilities including the period after end-of-sale date.

VR-02: MUST provide fixes for security vulnerabilities at minimum while the device is for sale. The vendor SHOULD continue to provide security fixes for 3 (three) years from the end-of-sale date.

VR-03: MUST have a coordinated vulnerability disclosure capability, including a communication channel/point of contact that allows ISP customers, end users, and third parties (such as researchers) to report security vulnerabilities discovered in the product(s). Ideally, it SHOULD have a Product Security Incident Response Team (PSIRT).

VR-04: MUST have a publicly available support channel that does not require pre-registration or an account, at minimum, through a website in English to:

a. Inform about existing vulnerabilities, mitigation measures and security fixes associated with its product(s);
b. Provide security fixes and/or new versions of firmware or software for its product(s);
c. Provide manuals and other materials regarding device configuration, updating and security.

8. List of Acronyms

BCOP: Best Current Operational Practices

BBF: Broadband Forum

CE: Customer Edge Router

CPE: Customer Premises Equipment

CWMP: CPE WAN (Wide Area Network) Management Protocol

IANA: Internet Assigned Numbers Authority

ISP: Internet Service Provider

PSIRT: Product Security Incident Response Team

RG: Residential Gateway

SSID: Service Set Identifier

WLAN: Wireless LAN (Local Area Network)

9. Acknowledgements

Many people contributed to the development of this document, from its initiation in the Latin American and Caribbean Anti-Abuse Working Group (LAC-AAWG) to its publication.

The authors gratefully acknowledge all of the contributors for their many helpful suggestions, in some cases providing a detailed review. Contributors (in alphabetical order) include: Nicolas Antoniello, John Brown, Dennis Dayman, Carmen Denis, Yuri Ferreira, Alexandre Giovaneli, Steve Goeringer, Cristine Hoepers, Markus Lintula, Jason Livingood, Art Manion, Jordi Palet Martínez, Roney Medeiros, Luciano Minuchin, Eduardo Barasal Morales, Massimiliano Pala, Ricardo Patara, Nathalia Sautchuk Patrício, Fernando Quintero, Marcelo Batista Sarmento, Joe St Sauver, Klaus Steding-Jessen, Italo Valcy, Severin Walker, Ariel Weher, Gilberto Zorello, and Jan Žorž.

Special thanks go to:

- Lucimara Desiderá, LAC-AAWG founding co-chair, author/editor
- Christian O'Flaherty, LAC-AAWG founding co-chair
- The LACNOG BCOP Working Group community and the Chair for supporting the document development and review process
- The LACNIC WARP (Warning Advice and Reporting Point) of the Latin American and Caribbean Internet Address Registry (LACNIC) for providing infrastructure for the face-to-face meetings
- The Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG) for supporting the LAC-AAWG initiative and accepting this document for technical review

10. Informative References

[1] Abuse of Customer Premise Equipment and Recommended Actions
https://resources.sei.cmu.edu/asset_files/WhitePaper/2014_019_001_312679.pdf

[2] Key words for use in RFCs to Indicate Requirement Levels, BCP 14, RFC 2119
http://www.rfc-editor.org/info/rfc2119

[3] Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words, RFC 8174
https://tools.ietf.org/html/rfc8174

[4] Internet Security Glossary, Version 2, RFC 4949
https://tools.ietf.org/html/rfc4949

[5] Common Security Requirements for IP-Based MSO-Provided CPE - Version I01
https://apps.cablelabs.com/specification/common-security-requirements-for-ip-based-mso-provided-cpe

[6] Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service, RFC 6092
https://tools.ietf.org/html/rfc6092

[7] Data-Over-Cable Service Interface Specifications DOCSIS® 3.1, Security Specification, CM-SP-SECv3.1-I07-170111
https://apps.cablelabs.com/specification/CM-SP-SECv3.1

[8] Basic Requirements for IPv6 Customer Edge Routers, RFC 7084
https://tools.ietf.org/html/rfc7084

[9] Functional Requirements for Broadband Residential Gateway Devices, TR-124 Issue 5
https://www.broadband-forum.org/technical/download/TR-124_Issue-5.pdf

[10] CPE WAN Management Protocol, TR-069 Issue 1 Amendment 6
https://www.broadband-forum.org/technical/download/TR-069.pdf

[11] IPv4 and IPv6 eRouter Specification CM-SP-eRouter-I19-160923
https://apps.cablelabs.com/specification/ipv4-and-ipv6-erouter-specification/

[12] Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, BCP 38, RFC 2827
https://tools.ietf.org/html/rfc2827

[13] Special-Purpose IP Address Registries, BCP 153, RFC 6890
https://tools.ietf.org/html/rfc6890

[14] Updates to the Special-Purpose IP Address Registries, BCP 153, RFC 8190
https://tools.ietf.org/html/rfc8190

[15] IANA IPv4 Special-Purpose Address Registry
https://www.iana.org/assignments/iana-ipv4-special-registry

[16] IANA IPv6 Special-Purpose Address Registry
https://www.iana.org/assignments/iana-ipv6-special-registry

[17] Service Name and Transport Protocol Port Number Registry
https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

[18] Addressing the challenge of IP spoofing
https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-AntiSpoofing-20150909-en-2.pdf

[19] ISO/IEC 29147:2014 Information technology - Security techniques - Vulnerability disclosure
https://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip

[20] BSI TR-03148: Secure Broadband Router
Requirements for a secure Broadband Router Version: 1.0
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03148/TR03148.pdf?__blob=publicationFile&v=2

Annex 1 - Table of Requirements

The following table summarizes the set of requirements presented in this document and is meant to help organizations (e.g. ISPs) prepare RFPs or specify the requirements they want from vendors.

Some fields are already filled in with the recommended selection, especially when the requirement is mandatory, but a good part of the requirements require the organization to decide if it wants a given configuration or not and to define its DEFAULT setting.

It is worth noting that the items listed in this document are a minimum set of security requirements and it is highly recommended that the choices not be reduced to a lower level (e.g. from mandatory to recommended or optional implementation). Whenever possible, they should be moved to the strictest option.

General Requirements (GR)		
Requirement	**M Mandatory R Recommended O Optional**	**Default configuration**
GR-01	M	
GR-02	M	
GR-03	M	
GR-04	R	Contact information for vulnerability disclosure available in the graphical user interface
GR-05	R	Current status of updates
Software Security Requirements (SR)		
Requirement	**M Mandatory R Recommended O Optional**	**Default configuration**
SSR-01	M	
SSR-02	M	Sensitive data protected
SSR-03	R	
SSR-04	M	Software development tools and/or backdoors removed

Update and Management Requirements (MR)		
Requirement	**M Mandatory R Recommended O Optional**	**Default configuration**
MR-01	M (a)	(a)
MR-02	M (b)	(b)
MR-03	a. M b. M c. M d. M	(c)
MR-04	M	
MR-05	M	
MR-06	M	
MR-07	a. M b. M c. R	
MR-08	M	
Functional Requirements (FR)		
Requirement	**M Mandatory R Recommended O Optional**	**Default configuration**
FR-01	M	Telnet, FTP, SOCKS, CHARGEN, SNMP disabled
FR-02	M	(c)
FR-03	MUST authenticate and is RECOMMENDED to encrypt.	
FR-04	M	
FR-05	a. M b. M	Unique initial password per device
FR-06	M	
FR-07	M	
FR-08	a. M b. M	

FR-09	M	DNS, NTP, SSDP, UPnP not accessible from the WAN
FR-10	a. M b. M	(d)
FR-11	M	
FR-12	M	
FR-13	M	NTP client only. No hard-coded configuration.
FR-14	R	
FR-15	M	Anti-spoofing filtering enabled
FR-16	R	Unconfigured (e)
FR-17	a. M b. R c. R d. M	b. No forwarding rule enable
FR-18	a. M b. R	Appropriate encryption enabled
FR-19	M	
FR-20	R	

Initial Configuration Requirements (IR)

Requirement	**M Mandatory R Recommended O Optional**	**Default configuration**
IR-01	M	SSDP, SNMP, UPnP, SOCKS, SMB, Bandwidth Test disabled
IR-02	M	No pre-defined DNS addresses and DNS Relay disabled
IR-03	M	Disabled
IR-04	M	(f)
IR-05	M	(f)
IR-06	M	(g)
IR-07	M	No SSH key pre-generated
IR-08	M	Enabled
IR-09	M	Transition mechanisms, tunnels, VPN disabled

Vendor Requirements (VR)		
Requirement	**M Mandatory R Recommended O Optional**	**Default configuration**
VR-01	M	
VR-02	M	
VR-03	M	
VR-04	M	

(a) The ISP must have the ability to manage the devices remotely (e.g. for configuration). Depending on the technology used by the provider (cable, fiber, xDSL), the corresponding industry may have already specified protocols. In this item, the ISP needs to choose the protocol(s) that must be supported by the device according to its technology (e.g. BBF TR-069 CWMP for broadband), whether it should be enabled BY DEFAULT and the required default settings. If more than one protocol must be supported, the organization needs to include them all.

(b) The ISP must have the ability to update the device remotely (mostly the firmware). Depending on the technology used by the provider (cable, fiber, xDSL), the corresponding industry may have already specified protocols. In this item, the organization needs to choose the protocol(s) that must be supported by the device according to its technology (e.g. BBF TR-069 CWMP for broadband), whether it should be enabled BY DEFAULT and the required default settings. If more than one protocol must be supported, the organization needs to include them all.

(c) Not using minimum mechanisms for access control, confidentiality and integrity checking in the transactions between the CPEs and the management/updating server(s) can often result in the compromise of the provider's infrastructure. It is strongly recommended using encrypted connection (e.g. TLS/HTTPS) for all access; using authentication not based on a single, predefined username/password for all the devices; and restricting access to specified sources (e.g. to a selected network segment, specific URL, etc.).

(d) If the ISP wants a monitoring and/or management service/agent enabled BY DEFAULT, it has to provide the appropriate parameters for authentication and network access restriction.

(e) If the ISP wants to implement filtering for Special-Purpose IP Addresses directly in the CPE, it can provide the list of prefixes that may be filtered BY DEFAULT. Otherwise, the DEFAULT configuration is "unconfigured" and the CPE does not apply any filter for such prefixes.

(f) If the ISP wants to customize how the initial password is to be set, the ISP needs to inform the vendor on the password selection process. Otherwise the vendor may set random unique value(s) as the DEFAULT.

(g) If the ISP wants to customize the WiFi network name(s), it needs to inform how the WiFi Identifiers (SSIDs) should be set up. Otherwise the vendor may choose the DEFAULT value(s).

As with all documents that we publish, please check the M³AAWG website (www.m3aawg.org) or the LACNOG website (www.lacnog.net) for updates.