* Best Current Operational Practices (BCOPs) are documents developed by the network operators community with the aim of collecting and documenting best practices to solve operational issues.
* This document[[1]](#footnote-1) is a draft for a BCOP under development by two Working Groups of The Latin American and Caribbean Network Operators Group (LACNOG[[2]](#footnote-2)), the BCOP’s Working Group[[3]](#footnote-3) and the Anti-Abuse Working Group (LAC-AAWG)[[4]](#footnote-4), in partnership with M3AAWG[[5]](#footnote-5) and LACNIC[[6]](#footnote-6).
* In order to see the proposed changes and to make comments and suggestions, it is necessary to log in to Google Docs and request permission to edit.
* Starting on "draft-02", we will build the document only in "English". After the document is completed (final version), we will translate it into Spanish and Portuguese. Comments can be made in English, Spanish and Portuguese.
* Timeline
	+ Draft-01 release for LACNIC29: 2018-04-19
	+ Draft-01 period for comments: 2018-04-19 to 2018-05-05
		- face-to-face meeting at LACNIC29: 2018-05-03 (14:00 - 16:00)
		- Web conference for discussion: 2018-06-06 (13:00 UTC)
	+ Draft-02 release: 2018-06-15
	+ Draft-02 period for comments: until 2018-07-22
	+ Draft-03 release for LACNIC30: 2018-09-19
		- Face-to-face meeting at LACNIC30: 2018-09-25 (14:00- 17:00)

Version: 3 (draft-3)

Date: September 19, 2018

Authors: Lucimara Desiderá <lucimara@cert.br>

Contributors: Christian O’ Flaherty, Ariel Weher, Cristine Hoepers, Klaus Steding-Jessen, Alexandre Giovaneli, Jordi Palet Martínez, Luciano Minuchin, Nicolas Antoniello, Fernando Quintero, Yuri Alexandro da Silva Ferreira, Italo Valcy, Carmen Denis, Eduardo Barasal Morales, Severin Walker, Nathalia Sautchuk Patrício.

State: Draft

Subject of the BCOP: Minimum security requirements for the acquisition of CPE

# Best Current Operational Practice

"Minimum security requirements for CPE acquisition"

## Index

Executive summary

Terminology

General Requirements (GR)

Software Security Requirements (SSR)

Update and Management Requirements (MR)

Functional Requirements (FR)

Initial Configuration Requirements (IR)

Vendor Requirements (VR)

List of Acronyms

Informative References

Annex I - Table of Requirements

## 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, DSL, fiber) and Wi-Fi routers, among others. CPE is on some cases managed by the ISP, and in other cases may be managed by the customer.

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

In general, common vulnerabilities have included:

* standard credentials for numerous devices;
* hardcoded credentials;
* use of well-known user names and passwords (i.e. admin / password);
* use of obsolete and insecure protocols and algorithms;
* undocumented accesses (backdoors);
* lack of secure and automated update mechanisms to address security issues;
* unnecessary and/or insecure services enabled by default;
* services that cannot be disabled;
* insecure remote management ~~and secure upgrade mechanisms~~.

This document is intended to identify a minimum set of security requirements for the purchase CPE by ISPs. The goal is to ensure that such CPE has a secure configuration and secure remote management and update mechanisms, in order to reduce the risks of compromising the provider's network, the Internet as a whole, and to attempt to minimize the cost and impact resulting from the abuse of the equipment by attackers, such as degradation or unavailability of services, technical support and rework.

Providing a list of basic requirements for IPv6 is not part of the scope of this document. However, not including such requirements as part of the general CPE purchasing document may imply in a business risk to ISPs as they may not be able to provide IPv6 connectivity to their customers neither continue to grow their network due to IPv4 address exhaustion. This document assumes that IPv6 support requirements are included as part of the general purchasing requirements document.

## Terminology

For purposes of this document:

1. Customer Premises Equipment (CPE): is the equipment used to connect subscribers to the Internet Service Provider (ISP) network. Other names may be used to describe this kind of devices such as Customer Edge (CE) Router and Residential Gateway (RG).
2. Backdoor: is any mechanism inserted in the system with the aim of enabling undocumented access to the system or its data. Examples of backdoor are: undocumented account/backdoor account (hardcoded account with no password, with a fixed password or password of the day); undocumented services for performing administrative functions without authentication, among others. A backdoor can be intentional (designed to guarantee later access) or accidental (used for development purposes and forgotten).
3. Appropriate encryption protocols: are open standard cryptographic algorithms/protocols published by IETF, in their current versions. The implementation must allow for the selection of up-to-date cipher suites and key sizes.
4. Service (server-type process, or *daemon*): means the server process that is active waiting for connections on a particular port, not the client software that performs queries to a service, when necessary.
5. 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.
6. DEFAULT: means a configuration set by the vendor.

General Requirements (GR)

GR-01: The descriptive information of the device SHALL include the complete identification of its main components, in particular:

1. manufacturer, model and chipset versions;
2. name and version of the firmware and the base operating system;

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

1. name, version and functionality of the firmware or operating system;
2. name, version, and factory-boot status of all applications and services installed on the device;

Software Security Requirements (SSR)

SSR-01: Authentication data (eg password, PIN, private key, etc.) MUST NOT be hardcoded. Data MUST be stored on the device and protected by appropriate cryptographic algorithms.

SSR-02: Any software tools or backdoors used for firmware or system development MUST be removed in the mass production version.

Update and Management Requirements (MR)

It is critical to have the ability to remotely apply updates and manage configurations with minimum security.

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

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

MR-03: The remote management and remote updating mechanisms:

1. MUST be authenticated,
2. SHOULD use encrypted connection, and
3. SHOULD only be accessible from specified sources.

MR-04: In the case of automated 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 of the downloaded file and if the version is correct.

MR-06: The update process MUST preserve the existing settings.

Functional Requirements (FR):

This document assumes that IPv6 support in accordance to RFC 7084 [7] is part of the general purchasing requirements document.

Features that must be supported or removed from the CPE:

FR-01: Unsafe services or applications (without support for encryption), accessible from the WAN, MUST be disabled by DEFAULT or removed, especially Telnet and FTP.

FR-02: Any management communication from WAN side to the CPE:

1. MUST be authenticated,
2. SHOULD use encrypted connection, and
3. SHOULD only be accessible from specified sources (eg. selected network segments, specified URL, etc).

FR-03: Any end user management communication from the LAN side to the CPE MUST be authenticated and MAY be encrypted.

FR-04: Any username and password MUST be changeable, including the master administration (root) password.

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

1. The initial password MUST be unique for each device;
2. At any time (eg password change or reset) password MUST NOT be null (ie, empty, blank) nor the same as the username;

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 (call home). Additionally, if there is any mechanism to send data (eg, fault logs) it MUST be disabled by DEFAULT.

FR-08: The end user MUST be able, via graphical user interface, from the LAN side only, to disable any service that is not essential to the operation or administration of the device.

FR-09: When enabling the initialization of services for the LANs, it MUST be ensured that such services will not be accessible from the WAN, in particular DNS, NTP, SSDP, UPnP or any other UDP protocol that might be used in amplification attacks.

FR-10: In order to start the SNMP service/agent:

a. the configuration of an appropriate authentication mechanism SHOULD be required and community strings with well-known default values (eg public, private) SHOULD NOT be allowed;

b. access from the WAN interface MUST be restricted to specified source(s) (eg. selected network segment).

FR-11: The device MUST implement open standard cryptographic methods, in their current versions, which 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, ie private key MUST NOT be shared (copied) among different devices.

FR-13: The CPE MUST support time synchronization through a centralized time protocol, such as NTP. Only client software is required.

FR-14: The CPE SHOULD support RFC 6092 [5] by implementing enough functionality to support the set of recommendations summarized in the Section 4.

FR-15: The CPE SHOULD support anti-spoofing filtering in accordance with BCP 38 RFC 2827 [11] for both, IPv4 and IPv6, and SHOULD be possible to disabled this feature if needed. It's out of scope of this document to determine the technique to be used for source IP address validation.

FR-16: The CPE MAY support packet filtering for Special-Purpose IP Addresses. Addresses considered "Globally Reachable" FALSE AND "Forwardable" FALSE, in accordance with RFC 6890 [12], MAY 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 as described in “IANA IPv4 Special-Purpose Address Registry” [14] and “IANA IPv6 Special-Purpose Address Registry” [15].

FR-17: DNS queries from WAN to LAN MUST NOT be forwarded unless there is an explicit port forwarding rule set for that.

FR-18: CPE MUST support WPA3.

FR-19: Passwords MUST not be visible in clear text in any management interface.

Initial Configuration Requirements (IR)

Devices MUST have the following factory default settings:

IR-01: All services (ie, server-type processes) that are not strictly necessary for the initial configuration process (bootstrapping) MUST be disabled, especially (if implemented), SSDP, SNMP, UPnP.

IR-02: Parameters related to DNS server addresses (resolver address) 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.

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

IR-05 Wi-Fi SSIDs MUST be unique for each device and MUST NOT be related to the vendor name nor equal to the password.

IR-06: Wi-Fi networks MUST have a unique initial password and it MUST be possible to identify it visually on the device label.

IR-07: In the case of SSH service, the cryptographic key 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.

IR-08: Anti-spoofing filtering (FR-15) SHOULD be enabled by DEFAULT.

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

Vendor Requirements (VR)

The vendor:

VR-01: MUST have a clear product support policy, especially regarding the availability of fixes for security vulnerabilities.

VR-02: MUST provide fixes for security vulnerabilities for at least 5 (five) years from the end of sale date.

VR-03: MUST have a communication channel/point of contact that allows customers and third parties (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 support channel, at least a website in English, to:

1. inform about existing vulnerabilities, mitigation measures and security fixes associated with its product(s);
2. provide security fixes and/or new versions of firmware or software for its product(s);
3. provide manuals and other materials regarding device configuration, updating and security.

List of Acronyms

BCOP: Best Current Operational Practices

BBF: Broadband Forum

CE: Customer Edge Router

CPE: Customer Premises Equipment

IANA: Internet Assigned Numbers Authority

ISP: Internet Service Provider

PSIRT:Product Security Incident Response Team

RG: Residential Gateway

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] | 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> |
| [5] | Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service, RFC 6092<https://tools.ietf.org/html/rfc6092> |
| [6] | 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> |
| [7] | Basic Requirements for IPv6 Customer Edge Routers, RFC 7084<https://tools.ietf.org/html/rfc7084> |
| [8] | Functional Requirements for Broadband Residential Gateway Devices, Issue 5<https://www.broadband-forum.org/technical/download/TR-124_Issue-5.pdf> |
| [9] | TR-069 - CPE WAN Management Protocol, Issue: 1 Amendment 6<https://www.broadband-forum.org/technical/download/TR-069.pdf> |
| [10] | IPv4 and IPv6 eRouter Specification /CM-SP-eRouter-I19-160923<https://apps.cablelabs.com/specification/ipv4-and-ipv6-erouter-specification/> |
| [11] | Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, BCP 38, RFC 2827<https://tools.ietf.org/html/rfc2827> |
| [12] | Special-Purpose IP Address Registries, BCP 153, RFC 6890<https://tools.ietf.org/html/rfc6890> |
| [13] | Updates to the Special-Purpose IP Address Registries, BCP 153, RFC 8190<https://tools.ietf.org/html/rfc8190> |
| [14] | IANA IPv4 Special-Purpose Address Registry<https://www.iana.org/assignments/iana-ipv4-special-registry> |
| [15] | IANA IPv6 Special-Purpose Address Registry<https://www.iana.org/assignments/iana-ipv6-special-registry> |
| [16] | Addressing the challenge of IP spoofing<https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-AntiSpoofing-20150909-en-2.pdf>  |

Annex I - table of requirements

The following table summarizes the set of requirements presented in this document, and it is meant to help organizations (e.g. ISPs) to prepare RFPs or to 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 demands the organization to make decisions on whether it wants a given configuration or not, as well as the definition of what will be its default setting.

It's worth remembering that the items listed in this document were thought to be a minimum set of security requirements, so it is highly recommended that the choices on the requirements are not relaxed to a lower level (e.g. from mandatory to recommended or optional implementation) and whenever possible, move to the strictest option.

|  |
| --- |
| General Requirements (GR) |
| Requirement | M MandatoryR RecommendedO Optional | Default configuration |
| GR-01 | M |   |
| GR-02 | M |   |
| Software Security Requirements (SR) |
| Requirement | M MandatoryR RecommendedO Optional | Default configuration |
| SR-01 | M |   |
| SR-02 | M |   |
| Management Requirements (MR) |
| Requirement | M MandatoryR RecommendedO Optional | Default configuration |
| MR-01 | M (a) | (a) |
| MR-02 | M (b) | (b) |
| MR-03 | a. Mb. R c. R  | (c) |
| MR-04 | M |   |
| MR-05 | M |   |
| MR-06 | M |   |
| Functional Requirements (FR) |
| Requirement | M MandatoryR RecommendedO Optional | Default configuration |
| FR-01 | M | Telnet and FTP disabled |
| FR-02 | a. Mb. R c. R  | (c) |
| FR-03 | M |   |
| FR-04 | M |   |
| FR-05 | M |   |
| FR-06 | M |   |
| FR-07 | M | Disabled |
| FR-08 | M | Web admin interface only from the LANs |
| FR-09 | M |   |
| FR-10 | a. Rb. M | SNMP Disabled (d) |
| FR-11 | M |   |
| FR-12 | M |   |
| FR-13 | M | NTP client only |
| FR-14 | R |   |
| FR-15 | R | Implemented and enabled |
| FR-16 | O | Unconfigured (e) |
| FR-17 | M |   |
| FR-18 | M |  |
| FR-19 | M |  |
| Initial Configuration Requirements (IR) |
| Requirement | M MandatoryR RecommendedO Optional | Default configuration |
| IR-01 | M | SSDP, SNMP, UPnP disabled |
| IR-02 | M | DNS addresses unconfigured and DNS Relay disabled |
| IR-03 | M | Disabled |
| IR-04 | M | (f) |
| IR-05 | M | (g) |
| IR-06 | M | (f) |
| IR-07 | M | No SSH key pre-generated |
| IR-08 | R | Enabled |
| IR-09 | M | Transition, tunnels, VPN, disabled |
| Vendor Requirements (VR) |
| Requirement | M MandatoryR RecommendedO 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 protocols already specified. 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 for broadband), that it should be enabled by default and the default settings required for that. 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 protocols already specified. 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 for broadband), that it should be enabled by default and the default settings required for that. 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 CPE and the management/updating server(s) can largely facilitate the compromise of the provider’s infrastructure. It’s strongly recommended to use encrypted connection (e.g. TLS/HTTPS) and authentication not based in a single predefined username/password for all the devices.

(d) Provide the appropriate parameters for SNMP authentication and network access restriction if the ISP intends to enable the corresponding service.

(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) The ISP needs to decide how it wants the unique passwords to be generated, if completely random or based in some device ID, or a combination of unique and fixed information.

(g) The ISP needs to inform how the Wi-Fi Identifiers (SSIDs) should be named.

1. Link to this document <https://docs.google.com/document/d/1\_Sa8ZEnKXiAnh\_xRc-J44VXadUGdr98MT\_MZrA5sALc/edit?usp=sharing> [↑](#footnote-ref-1)
2. The Latin American and Caribbean Network Operators Group (LACNOG) <http://www.lacnog.net/> [↑](#footnote-ref-2)
3. LACNOG BCOP’s Working Group <http://www.lacnog.org/wg-bcops/> [↑](#footnote-ref-3)
4. LACNOG Anti-Abuse Working Group (LAC-AAWG) <https://www.m3aawg.org/news/rel-LAC-AAWG-Formed-2017-05> [↑](#footnote-ref-4)
5. Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) <https://www.m3aawg.org/> [↑](#footnote-ref-5)
6. Latin America and Caribbean Network Information Center (LACNIC) <http://www.lacnic.net/> [↑](#footnote-ref-6)