IPv6 家庭用ルータガイドライン第 2 版と TR-124i5 の比較

【第 1.0 版】

2019 年 4 月 2 日

IPv6 普及・高度化推進協議会

IPv4/IPv6 共存 WG　IPv6 家庭用ルータ SWG

変更履歴

版	改版日	摘要
1.0	2019 年 4 月 2 日	第 1 版

本書の構成

本文書の第 2 章以降の章, 節, 項は, TR-124i5 との比較, 参照がしやすいように TR-124i5 における第 4 章の Section の各階層に基づいて構成している.
また，文書内では，TR-124i5 における Section，Item，Requirements の項目を再掲し，ガイドラインとの差分を記載する形とした.

目次

1 本文書作成の背景と目的

IPv6 普及・高度化推進協議会[1] IPv4/IPv6 共存ワーキンググループ IPv6 家庭用ルータサブワーキンググループ[2]（以下，当該 SWG）では，「IPv6 家庭用ルータガイドライン第 2 版」（以下，ガイドライン）を 2010 年 7 月 29 日に公開している．

第 2 版の公開以降，当該 SWG では国際的な議論／動向に配慮し，外部団体による関連ドキュメントの調査活動を行っている．この活動は，調査対象ドキュメントとガイドラインの差異を明確にするとともに，将来的なガイドラインの改版において，対象ドキュメントの内容をガイドラインに取り込むことを目的としており，具体的には Internet Engineering Task Force[3]（以下，IETF），Broadband Forum[4]（以下，BBF）等が発行したドキュメントを対象としている．

本文書は，BBF が 2016 年 7 月に発行した TR-124 Functional Requirements for Broadband Residential Gateway Devices Issue 5 [5]（以下，TR-124i5）の内容を調査すると共に，ガイドラインと比較し，差分をまとめたものである[6]．

IPv6 家庭用ルータの最低限の仕様をまとめたガイドラインとは異なり，TR-124i5 は，装置全体の機能要件をまとめた広範囲にわたるものであるが，IPv6 に関係する部分のみを比較した．比較の結果，いくつかの部分で両文書に大きな差異があった．この差異は，主に対象機器の設置環境（地域の違い等）や IPv6 機能に関する考え方の違いに起因している．

本文書において整理した両ドキュメントの違いが，読者の理解を促進し，家庭用ルータの実装者における仕様策定，及びサービス提供者における IPv6 接続サービスの仕様策定の参考になれば幸いである．

---

[1] IPv6 普及・高度化推進協議会：http://www.v6pc.jp/
[2] IPv6 家庭用ルータ SWG：http://www.v6pc.jp/jp/wg/coexistenceWG/v6hgw-swg.phtml
[3] The Internet Engineering Task Force：https://www.ietf.org/
[4] Broadband Forum：https://www.broadband-forum.org/
[5] TR-124i5：https://www.broadband-forum.org/wp-content/uploads/2018/11/TR-124_Issue-5.pdf
[6] TR-124 Issue 2 との比較文書については，2014 年 6 月に公開している．
http://www.v6pc.jp/pdf/v6hgw_tr124i2_comparison_1.0.pdf

2 General Device Requirements

2.1 IPv6 Networking Protocols

Section	Item	Requirements	ガイドラインとの比較
GEN.NETv6.	1	The RG MUST support IP Version 6, which is defined in IETF RFC 2460.	明確に記述はないが，自明なため問題なし.
GEN.NETv6.	2	The RG MUST support enabling and disabling of IPv6.	ガイドラインは，IPv6 機能を利用する場合の基準について記述しているため，IPv6 機能を off にすることについては触れていない.

3 Wide Area Networking (WAN)

3.1 Bridging

Section	Item	Requirements	ガイドラインとの比較
WAN.BRIDGE.	1	The RG MUST be able to bridge IPv4 over Ethernet.	ガイドラインでは IPv4 ブリッジ機能については対象外.
WAN.BRIDGE.	2	The RG MUST be a learning bridge as defined in IEEE 802.1D for all logical and physical Ethernet interfaces, supporting a minimum of 272 MAC addresses.	ガイドラインでは IP4 ブリッジ機能については対象外.
WAN.BRIDGE.	3	If bridge mode is enabled for IPv4 on the RG by default for LAN connected devices, the RG MUST be able to support additional connections for TR-069 remote management addressability (using direct DHCPv4 or static IPv4, PPP, etc.), and connections for any locally terminated service that require IP (v4 or v6) addressability (e.g. gateway integrated voice ATA ports, etc.). Note that this special bridge mode that includes a device remote management session connection requires an additional WAN connection from the network. This requirement is considered conditional as a result of the network side dependency, but the RG must support this type of configuration.	TR-069 の遠隔管理が主な要件となっているため, ガイドラインでは対象外.

Section	Item	Requirements	ガイドラインとの比較
WAN.BRIDGE.	4	The RG MUST be able to bridge IPv6 over Ethernet (Ethertype 0x86DD). This includes bridging of multicast frames.	ガイドラインではブリッジ機能については触れていない．IPv6 に関連するブリッジ機能については，次版以降で検討予定．
WAN.BRIDGE.	5	The RG MUST be able to configure IPv6 bridging for a WAN interface, separate from IPv4 treatment.	ガイドラインではブリッジ機能については触れていない．IPv6 に関連するブリッジ機能については，次版以降で検討予定．
WAN.BRIDGE.	6	The RG MUST be able to configure IPv6 bridging separately for each WAN interface (if there are multiple WAN interfaces).	ガイドラインではブリッジ機能については触れていない．IPv6 に関連するブリッジ機能については，次版以降で検討予定．
WAN.BRIDGE.	7	When IPv6 bridging is enabled on a WAN interface, the RG MUST be configurable to act as a host on that WAN interface (doing SLAAC, etc.). It will not request IA_PD, since that is not a host function.	ガイドラインではブリッジ機能については触れていない．IPv6 に関連するブリッジ機能については，次版以降で検討予定．

3.2 EAP Re-authentication (ERP) for DHCPv6

Section	Item	Requirements	ガイドラインとの比較
WAN.DHCPv6.ERP	1	The RG MUST support the ERP Local Domain Name (LDN) DHCPv6 Option (RFC 6440 [136]).	ERP に関しては，国内での利用状況を調査した上で，次版への反映要否について検討する．
WAN.DHCPv6.ERP	2	The RG MUST support receiving a DHCPv6 request message from a UE client, which includes an Option Request option requesting the DHCPv6 ERP Local Domain Name option (RFC 6440 [136]). The DHCPv6 request message may be Solicit, Request, or Information Request.	ERP に関しては，国内での利用状況を調査した上で，次版への反映要否について検討する．

Section	Item	Requirements	ガイドラインとの比較
WAN.DHCPv6.ERP	3	If the RG has pre-existing knowledge of the ERP local domain name for a client (for example, from a previous AAA exchange), it SHOULD include it in an instance of the DHCPv6 ERP Local Domain Name option of the DHCPv6 message and forward it to the DHCPv6 server as a sub-option of the Relay-Supplied Options option (RFC 6422 [134]).	ERP に関しては，国内での利用状況を調査した上で，次版への反映要否について検討する．
WAN.DHCPv6.ERP	4	The RG MUST support relaying a DHCPv6 Reply Message with the DHCPv6 ERP Local Domain Name option from the DHCPv6 server to the client.	ERP に関しては，国内での利用状況を調査した上で，次版への反映要否について検討する．
WAN.DHCPv6.ERP	5	The RG MUST support configuration of the parameters for it to connect to the RADIUS or Diameter server via Web GUI or TR- 069 extension.	ERP に関しては，国内での利用状況を調査した上で，次版への反映要否について検討する．

3.3 IPv6 WAN Connection

Section	Item	Requirements	ガイドラインとの比較
WAN.IPv6.	1	The RG MUST support automated establishment of an IPv6 connection according to the flow in Annex A.2.	接続フローについて，ガイドラインに記述はないが，ガイドライン改版時に 3 章の冒頭に記述するなど参考情報として参照する．
WAN.IPv6.	2	The RG MUST support a dual stack of IPv4 and IPv6 running simultaneously, as described in section 2 of RFC 4213.	ガイドラインでは IPv6 機能に特化した要件を記述している為，本要求条件は検討の範囲外とする．

Section	Item	Requirements	ガイドラインとの比較
WAN.IPv6.	3	The RG MUST allow the IPv6 stack to be enabled / disabled.	ガイドラインは，IPv6 機能を利用する場合の基準について記述しているため，IPv6 機能を off にすることについては触れていない．
WAN.IPv6.	4	The RG MUST support DHCPv6 client messages and behavior per IETF RFC 3315. See WAN.DHCPC.5 for further specifics on IAID value.	ガイドラインでも，WAN インタフェースで DHCPv6 を実装することは必須としている．IAID についてはガイドラインでは詳述しておらず，次版での反映を検討する．
WAN.IPv6.	5	The RG MUST support the role of the CPE requesting router in RFC 3633.	ガイドラインでも，同等の記述有り．（要件 1）
WAN.IPv6.	6	The RG MUST support specifying in its DHCPv6 prefix delegation request an indication of the length of prefix it requires. If the RG supports multiple LANs, or has PD requests from its LAN, it MUST indicate a preferred prefix length that would at least enable the RG to assign a /64 prefix to each LAN it supports. Note that the delegated prefix may vary from the requested length.	ガイドラインには記述なし． サービス仕様に依存する為， 次版での反映については要検討とする．
WAN.IPv6.	7	When sending DHCPv6 messages, the RG MUST identify itself in OPTION_CLIENTID (1) (client-identifier) using the same client identifier as for IPv4 (see WAN.DHCPC.3 and .4).	ガイドラインには記述なし． RFC を超えた記述になっており， 次版での反映については要検討とする．
WAN.IPv6.	8	The RG MUST support IPv6 node requirements as a host node, per IETF RFC 6434 [135].	ガイドラインでは，RFC4294（RFC6434）そのものを参照していないが，次版での反映については要検討とする．
WAN.IPv6.	9	The RG MUST support stateless address auto-configuration (SLAAC) as a host, per IETF RFC 4862.	ガイドラインでも，同等の記述有り．（要件 4）

Section	Item	Requirements	ガイドラインとの比較
WAN.IPv6.	10	The RG MUST support receipt of route information per RFC 4191. If the RG only has one WAN connection, it does not need to place this information in its routing table, but it does need to save it (for possible forwarding on the LAN interface).	ガイドラインでは，WAN 側については RFC4191 対応に関する記述はない．次版での反映については要検討とする．
WAN.IPv6.	11	If route information is provided (RFC 4191) and the RG has multiple WAN connections, it MUST place the route information in its routing table.	ガイドラインでは，WAN 側については RFC4191 対応に関する記述はない．次版での反映については要検討とする．
WAN.IPv6.	12	If the RG does not have a globally-scoped address on its WAN interface after having been delegated a prefix, it MUST create addresses for itself from the delegated prefix. It MUST have at least one address and MAY have more. There is currently no algorithm defined for address creation. It should be assumed that different service providers will want different rules for how to create the address, how many addresses to create, and in the case of multiple addresses, how the different addresses are used.	ガイドライン(要件 6)に同様の記述があるが，後半の複数プレフィックスを取得可能な場合の記述について備考に追記する．
WAN.IPv6.	13	Requirement deleted; redundant with WAN.IPv6.3	項目が削除されている為， 対象外とする．

Section	Item	Requirements	ガイドラインとの比較
WAN.IPv6.	14	The RG MUST be able to request the following DHCPv6 options: IA_NA (RFC 3315), reconfigure accept (RFC 3315), IA_PD (RFC 3633), and DNS_SERVERS (RFC 3646).	ガイドラインには，IA_NA, IA_PD,DNS_SERVERS については，オプション名での記述がない為，次版にて追記する．Reconfigure に関しては，関連記述(要件 36)にあるが，Reconfigure Accept の追記も含め次版での記述内容について検討する．また，ISP との情報のやりとりに関わるプロトコルおよびプロトコルオプションに関する記述について全体構成の見直しを検討する．
WAN.IPv6.	15	The RG SHOULD be able to request the following DHCPv6 options: SNTP_SERVERS (RFC 4075), domain search list (RFC 3646), and Client FQDN (RFC 4704).	ガイドラインには，SNTP_SERVERS, Domain Search List については，オプション名での記述がない為，次版にて追記する．Client FQDN に関しては，国内での利用状況を調査した上で，次版への反映要否について検討する．また，ISP との情報のやりとりに関わるプロトコルおよびプロトコルオプションに関する記述について全体構成の見直しを検討する．
WAN.IPv6.	16	The RG MUST continue to use the connectivity parameters (obtained via RA or DHCP) and consider them valid until either they expire or the RG is explicitly told to use different values.	ガイドラインには記述がないが，次版での記述を検討する．
WAN.IPv6.	17	The connectivity parameters (obtained via RA and DHCPv6) MUST persist across loss of WAN connection (or lack of response from WAN connection).	ガイドラインに記述がないが，ネットワーク安定性が向上すると考えられる為，次版にて追記する．必要度については要検討．

Section	Item	Requirements	ガイドラインとの比較
WAN.IPv6.	18	The device MUST continue to use the connectivity parameters (obtained via RA or DHCP) and consider them valid until either they expire or the device is explicitly told to use different values.	ガイドラインに記述がないが，ネットワーク安定性が向上すると考えられる為，次版にて追記する．必要度については要検討．
WAN.IPv6.	19	The RG MUST NOT advertise any address prefixes on the WAN using the IPv6 neighbor discovery protocol, or advertise itself as a default router.	ガイドラインに記述なし．WAN 側インタフェースのディフォルト動作として禁止することを次版で記述する．
WAN.IPv6.	20	The RG MUST provide up to 4 instances of option-data within a single OPTION_VENDOR_OPTS (17) (RFC 3315) with IANA "ADSL Forum" Enterprise Number as the enterprise-number. Each instance will have one of the 4 sub-options from WAN.DHCPC.7 as the vendor-specific opt-code, with the corresponding value in the vendor-specific option-data. If the value of a parameter is empty for the RG, then the sub-option MUST be omitted. If there are no values to provide, the entire option MUST be omitted.	ガイドラインには記述なし．BBF における個別要件と思われる為，対象外とする．
WAN.IPv6.	21	The RG SHOULD be able to request the following DHCPv6 options: address selection policy (RFC 7078 [142]), route information (draft-ietf-mif-dhcpv6-route-option Error! Reference source not found.), and DNS selection policy (RFC 6731 [139]).	ガイドラインにて記述なし．アップリンクが複数ある場合の対応については，今後の動向次第で次版への反映を検討する．
WAN.IPv6.	22	If route information is provided (draft-ietf-mif-dhcpv6-route- option) and the RG has multiple WAN connections, it MUST place the route information in its routing table.	ガイドラインにて記述なし．アップリンクが複数ある場合の対応については，今後の動向次第で次版への反映を検討する．

Section	Item	Requirements	ガイドラインとの比較
WAN.IPv6.	23	The RG SHOULD generate address selection policy based on policies obtained from each WAN link by DHCPv6 option (draft- ietf-6man-addr-select-opt) or manually configured policy.	ガイドラインにて記述なし. アップリンクが複数ある場合の対応については, 今後の動向次第で次版への反映を検討する.

3.4 Transitional IPv6 WAN Connection

3.4.1 6rd Transition Mechanism

Section	Item	Requirements	ガイドラインとの比較
WAN.TRANS.6rd.	1	The RG MUST support the 6rd transition mechanism as described in RFC 5969. This includes being able to configure the necessary parameters via TR-069 and DHCPv4, creation of the prefix, using the created prefix as a "delegated prefix" for purpose of including one of its /64s in RA messages, and modifying the IP header for traffic that goes between the WAN and LAN devices.	2019 年 1 月時点では, 国内では IPv6 only もしくは IPv4/IPv6 Dual Stack によるネットワーク構成が主流になっており, 6rd の利用は想定されない為, ガイドラインでは対応予定なし. 但し, BBF では MUST 要件となっている.
WAN.TRANS.6rd.	2	The RG MUST support enabling and disabling of the 6rd feature on the "default" routed IPv4 connection. 6rd is not applicable to bridged WAN interfaces.	2019 年 1 月時点では, 国内では IPv6 only もしくは IPv4/IPv6 Dual Stack によるネットワーク構成が主流になっており, 6rd の利用は想定されない為, ガイドラインでは対応予定なし. 但し, BBF では MUST 要件となっている.

Section	Item	Requirements	ガイドラインとの比較
WAN.TRANS.6rd.	3	If the RG supports configuration mechanisms other than the 6rd DHCPv4 option 212 (user-entered, TR-069, etc.), the RG MUST support 6rd in "hub and spoke" mode. 6rd in "hub and spoke" mode requires all IPv6 traffic to go to the 6rd border relay. In effect, this requirement removes the "direct connect to 6rd" route defined in section 7.1.1 of RFC 5969.	2019 年 1 月時点では, 国内では IPv6 only もしくは IPv4/IPv6 Dual Stack によるネットワーク構成が主流になっており, 6rd の利用は想定されない為, ガイドラインでは対応予定なし. 但し, BBF では MUST 要件となっている.

3.4.2 Dual Stack Lite Transition Mechanism

Section	Item	Requirements	ガイドラインとの比較
WAN.TRANS.DS-LITE.	1	The RG MUST support DS-Lite (RFC 6333) with IPv4 in IPv6 encapsulation (RFC 2473).	次版にて, IPv6 移行技術の章を追加し, 要件を追記する. 但し, サービス仕様に依存する為, 必要度については要検討.
WAN.TRANS.DS-LITE.	2	This requirement replaced by requirement WAN.TRANS.DS-Lite.6.	次版にて, IPv6 移行技術の章を追加し, 要件を追記する. 但し, サービス仕様に依存する為, 必要度については要検討.
WAN.TRANS.DS-LITE.	3	The RG MUST configure a static IPv4 default route toward the DS-Lite tunnel.	次版にて, IPv6 移行技術の章を追加し, 要件を追記する. 但し, サービス仕様に依存する為, 必要度については要検討.
WAN.TRANS.DS-LITE.	4	The RG MUST deactivate the NAPT function on the DS-Lite interface.	次版にて, IPv6 移行技術の章を追加し, 要件を追記する. 但し, サービス仕様に依存する為, 必要度については要検討.

Section	Item	Requirements	ガイドラインとの比較
WAN.TRANS.DS-LITE.	5	The RG MUST support enabling and disabling of DS-Lite.	次版にて，IPv6 移行技術の章を追加し，要件を追記する． 但し，サービス仕様に依存する為，必要度については要検討．
WAN.TRANS.DS-LITE.	6	The RG MUST be able to use the DHCPv6 option to retrieve the FQDN of the AFTR element, as defined in RFC 6334.	次版にて，IPv6 移行技術の章を追加し，要件を追記する． 但し，サービス仕様に依存する為，必要度については要検討．
WAN.TRANS.DS-LITE.	7	Manual configuration on the RG of the FQDN or the IPv6 address of the AFTR element SHOULD be supported.	次版にて，IPv6 移行技術の章を追加し，要件を追記する． 但し，サービス仕様に依存する為，必要度については要検討．
WAN.TRANS.DS-LITE.	8	Remote configuration via TR-069 of the FQDN or the IPv6 address of the AFTR element SHOULD be supported.	次版にて，IPv6 移行技術の章を追加し，要件を追記する． 但し，サービス仕様に依存する為，必要度については要検討．
WAN.TRANS.DS-LITE.	9	The RG MUST support configurable precedence between the FQDN and the IPv6 address.	次版にて，IPv6 移行技術の章を追加し，要件を追記する． 但し，サービス仕様に依存する為，必要度については要検討．
WAN.TRANS.DS-LITE.	10	The RG MUST support configurable precedence between dynamic or static configuration of the IPv6 address of the AFTR element when both are available. The RG MUST use DHCPv6 by default or use an operator-specific configuration.	次版にて，IPv6 移行技術の章を追加し，要件を追記する． 但し，サービス仕様に依存する為，必要度については要検討．

3.4.3 IPv6 connectivity with content-based IPv4 release control transition mechanism

Section	Item	Requirements	ガイドラインとの比較
WAN.TRANS. v4-release-control	1	The RG MUST provide a mechanism that monitors IPv4 session/traffic.	2019 年 1 月時点では, 国内では IPv4 Release Control(IPv4 アドレスをオンデマンドで利用するサービス)[TR-242 を参照のこと]の利用は確認されていない為, ガイドラインでは対応予定なし. 但し, BBF では MUST 要件となっている.
WAN.TRANS. v4-release-control	2	The RG MUST provide a timer-based trigger for releasing an IPv4 address.	2019 年 1 月時点では, 国内では IPv4 Release Control(IPv4 アドレスをオンデマンドで利用するサービス)[TR-242 を参照のこと]の利用は確認されていない為, ガイドラインでは対応予定なし. 但し, BBF では MUST 要件となっている.
WAN.TRANS. v4-release-control	3	The RG MUST provide signaling to the BNG according to RFC 1332.	2019 年 1 月時点では, 国内では IPv4 Release Control(IPv4 アドレスをオンデマンドで利用するサービス)[TR-242 を参照のこと]の利用は確認されていない為, ガイドラインでは対応予定なし. 但し, BBF では MUST 要件となっている.
WAN.TRANS. v4-release-control	4	The RG MUST provide the (re)assignment of an IPv4 address inside a PPP session according to RFC 1332, independent of the IPv6CP status according to section 2.1/RFC 4241.	2019 年 1 月時点では, 国内では IPv4 Release Control(IPv4 アドレスをオンデマンドで利用するサービス)[TR-242 を参照のこと]の利用は確認されていない為, ガイドラインでは対応予定なし. 但し, BBF では MUST 要件となっている.

Section	Item	Requirements	ガイドラインとの比較
WAN.TRANS. v4-release-control	5	The timer that triggers the release of the IPv4 address MUST be configurable.	2019 年 1 月時点では, 国内では IPv4 Release Control(IPv4 アドレスをオンデマンドで利用するサービス)[TR-242 を参照のこと]の利用は確認されていない為, ガイドラインでは対応予定なし. 但し, BBF では MUST 要件となっている.
WAN.TRANS. v4-release-control	6	The timer that triggers the release of the IPv4 address MUST be configurable via TR-069.	2019 年 1 月時点では, 国内では IPv4 Release Control(IPv4 アドレスをオンデマンドで利用するサービス)[TR-242 を参照のこと]の利用は確認されていない為, ガイドラインでは対応予定なし. 但し, BBF では MUST 要件となっている.

3.4.4 MAP-E Transition Mechanism

Section	Item	Requirements	ガイドラインとの比較
WAN.TRANS. MAP-E.	1	The RG MUST support mapping of address and port with encapsulation method (MAP-E) as specified in RFC 7597 [144].	次版にて, IPv6 移行技術の章を追加し, 要件を追記する. 但し, サービス仕様に依存する為, 必要度については要検討.
WAN.TRANS. MAP-E.	2	The RG MUST support the configuration for MAP-E operation by one or more methods, including TR-069, DHCPv6 with options as specified in RFC 7598 [145].	次版にて, IPv6 移行技術の章を追加し, 要件を追記する. 但し, サービス仕様に依存する為, 必要度については要検討.
WAN.TRANS. MAP-E.	3	The RG MUST support the MAP-E configuration for parameters with consistence as specified in RFC 7598 [145].	次版にて, IPv6 移行技術の章を追加し, 要件を追記する. 但し, サービス仕様に依存する為, 必要度については要検討.
WAN.TRANS. MAP-E.	4	The RG MUST support enabling and disabling of MAP-E operation.	次版にて, IPv6 移行技術の章を追加し, 要件を追記する. 但し, サービス仕様に依存する為, 必要度については要検討.

Section	Item	Requirements	ガイドラインとの比較
WAN.TRANS.MAP-E.	5	When performing NAT44 function, the RG MUST restrict the port assignment within the range per MAP-E configuration.	次版にて，IPv6 移行技術の章を追加し，要件を追記する． 但し，サービス仕様に依存する為，必要度については要検討．
WAN.TRANS.MAP-E.	6	The RG MUST support MAP-E operation in "hub and spoke" mode by forwarding IPv4-in-IPv6 packets to the MAP-E BR for distribution.	次版にて，IPv6 移行技術の章を追加し，要件を追記する． 但し，サービス仕様に依存する為，必要度については要検討．
WAN.TRANS.MAP-E.	7	The RG SHOULD be able to connect to more than one MAP-E domain.	次版にて，IPv6 移行技術の章を追加し，要件を追記する． 但し，サービス仕様に依存する為，必要度については要検討．

3.5 PPP Client

Section	Item	Requirements	ガイドラインとの比較
WAN.PPP.	1	The RG MUST support PPP and the associated protocols as defined in IETF RFCs 1332, 1334, 1661, 1877, 1994.	ガイドラインでは IPv4 PPP については対象外．
WAN.PPP.	2	Upon receipt of non-standard or unrecognized PPP extensions according to IETF RFCs 1570 and 2153 from the broadband network (e.g. vendor or proprietary), the RG MUST operate without fault.	ガイドラインでは PPP については対象外．
WAN.PPP.	3	The RG MUST support PPPoE as defined in IETF RFC 2516.	ガイドラインでは PPPoE については対象外．
WAN.PPP.	4	The RG MUST support IETF RFC 4638 in order to accommodate MTU/MRU values greater than 1492 bytes in PPPoE.	ガイドラインでは PPPoE については対象外．
WAN.PPP.	5	If the RG supports ATM, the RG SHOULD support PPP over AAL5 (PPPoA) as defined in IETF RFC 2364.	ガイドラインでは PPPoA については対象外．

Section	Item	Requirements	ガイドラインとの比較
WAN.PPP.	6	The RG MUST be able to save all logins and passwords for PPP sessions originated by the RG. Passwords MUST NOT be available outside the RG (that is, they cannot be queried or displayed).	ガイドラインでは記述がないが，実装上の要求事項として記述を次版にて追記する．要求度は SHOULD とする．(TR-124i5 では MUST であることを追記する)
WAN.PPP.	7	The RG MUST NOT immediately terminate PPPoE sessions and upper layer protocol connections when the physical connection is lost. It should defer the teardown process for two minutes. If the physical connection is restored during that time, the RG MUST first attempt to use its previous PPPoE session settings. If these are rejected, then the original PPPoE session is to be terminated and a new PPPoE session attempted.	ガイドラインでは記述がないが，サービス側の PPPoE セッション飽和を避けるために実装上の要求事項として記述を次版にて追記する．要求度は SHOULD とする．(TR-124i5 では MUST であることを追記する)
WAN.PPP.	8	The RG SHOULD incorporate a random timing delay prior to starting each IP (v4 or v6) and PPP session. This random timing delay helps to reduce connection failures when a group of users attempts to establish connections to a service provider at the same time (e.g. after power is restored to a neighborhood that had a blackout).	ガイドラインでは記述がないが，網側装置の負荷軽減をはかるために実装上の要求事項として記述を次版にて追記する．
WAN.PPP.	9	If the RG receives an authentication failure when attempting an automated PPP connection attempt, it SHOULD re-try immediately to establish the connection. After three unsuccessful attempts, the RG SHOULD wait for five minutes, then repeat the connection attempt three times. If authentication still fails, the RG SHOULD back off to thirty minute intervals between groups of three attempts.	ガイドラインでは記述がないが，網側装置の負荷軽減をはかるために実装上の要求事項として記述を次版にて追記する．

Section	Item	Requirements	ガイドラインとの比較
WAN.PPP.	10	If the RG is using the PPPoE client function actively, the RG MUST be able to forward PPPoE sessions initiated from LAN devices as additional PPPoE sessions to the WAN interface (this is sometimes known as PPPoE pass-through). Specifically, these LAN initiated PPPoE sessions MUST NOT be tunneled inside the RG's primary PPPoE client session.	ガイドラインでは記述がないが，ユーザ環境での利便性向上の為，記述を次版にて追記する.
WAN.PPP.	11	When fragmentation is required, the RG MUST fragment all PPP sessions that it originates on an access VC using MLPPP interleaving as defined in IETF RFC 1990.	ガイドラインでは PPP については対象外.
WAN.PPP.	12	If PPP is used, the RG MAY obtain an IPv4 subnet mask on its WAN interface using IPCP (IPv4) extensions. If this is done, the IPv4 subnet masks will be communicated with IPCP (IPv4) using the PPP IPCP (IPv4) option with option code 144, the length of the option being 6 and the mask being expressed as a 32-bit mask (e.g. 0xFFFFFF80), not as a number indicating the consecutive number of 1s in the mask (from 0 to 32). The learned network information MAY, but need not, be used to populate the LAN side embedded DHCP server for the RG. The learned network information is treated as a subnet and not as a collection of individual addresses. That is, the first and last addresses in the subnet should not be used. The IPv4 address negotiated SHOULD, but need not, be the one assigned to the RG.	ガイドラインでは IPv4 PPP については対象外.
WAN.PPP.	13	The RG MUST make the access concentrator name used with PPPoE connections available via the Web GUI, TR-064i2 and TR-069 interfaces for diagnostic purposes.	ガイドラインには記述なし. BBF における個別要件と思われる為，対象外とする.

Section	Item	Requirements	ガイドラインとの比較
WAN.PPP.	14	The RG MUST support RFC 3544, “IP Header Compression over PPP”.	ガイドラインには記述はないが，次版にて記述を検討する.

3.5.1 PPP Client for establishment of IPv6 connection

Section	Item	Requirements	ガイドラインとの比較
WAN.PPP.IPv6.	1	The RG MUST support IPv6 over PPP per IETF RFC 5072 and RFC 5172.	ガイドラインには記述はないが，次版にて記述を追記する.
WAN.PPP.IPv6.	2	The RG MUST support establishment of an IPv6 over PPPoE connection according to the flow in Annex A.1.	ガイドラインには記述はないが，次版にて記述を追記する. 要求度については別途検討する.
WAN.PPP.IPv6.	3	The RG MUST allow any particular PPP connection to be configurable for IPv4 only, IPv6 only, or both.	ガイドラインには記述はないが，次版にて記述を追記する. 要求度については別途検討する.
WAN.PPP.IPv6.	4	If the RG is configured for multiple PPPoE connections, it MUST be possible to configure it to use the same login and password for all, so that only the domain is unique per connection.	ガイドラインには記述はないが，次版にて記述を追記する. 要求度については別途検討する.
WAN.PPP.IPv6.	5	The RG MUST NOT tear down a shared (IPv4 and IPv6) PPP session if error conditions prevent only one IP stack (either IPv4 or IPv6) from working. The session MUST be torn down if error conditions apply to both stacks.	ガイドラインには記述はないが，次版にて記述を追記する. 要求度については別途検討する.

3.6 802.1x Client

Section	Item	Requirements	ガイドラインとの比較
WAN.dot1x.	1	The RG MUST support IEEE 802.1X acting as a supplicant.	WAN 側での IEEE 802.1X 利用に関しては，国内での利用状況を調査した上で，次版への反映要否について検討する.
WAN.dot1x.	2	The RG MUST be able to respond to an appropriate IEEE 802.1X request and provide certificate information using Extensible Authentication Protocol-Transport Layer Security (EAP/TLS).	WAN 側での IEEE 802.1X 利用に関しては，国内での利用状況を調査した上で，次版への反映要否について検討する.
WAN.dot1x.	3	The RG SHOULD support EAP-MD5 username and password type authentication.	WAN 側での IEEE 802.1X 利用に関しては，国内での利用状況を調査した上で，次版への反映要否について検討する.
WAN.dot1x.	4	The RG MUST support receiving IEEE 802.1X EAPOL frames with an individual MAC address (i.e. unicast) as well as frames with a group MAC address (i.e. multicast).	WAN 側での IEEE 802.1X 利用に関しては，国内での利用状況を調査した上で，次版への反映要否について検討する.
WAN.dot1x.	5	The RG MUST perform mutual authentication by authenticating certificate information of the requesting authenticator.	WAN 側での IEEE 802.1X 利用に関しては，国内での利用状況を調査した上で，次版への反映要否について検討する.
WAN.dot1x.	6	The RG MUST be able to store certificate information used to authenticate the authenticator.	WAN 側での IEEE 802.1X 利用に関しては，国内での利用状況を調査した上で，次版への反映要否について検討する.
WAN.dot1x.	7	The RG MUST be able to update the information used to validate the authenticator by either a firmware upgrade or via updated certificates.	WAN 側での IEEE 802.1X 利用に関しては，国内での利用状況を調査した上で，次版への反映要否について検討する.
WAN.dot1x.	8	The RG SHOULD be able to update the information used to validate the authenticator by updated certificates without a firmware upgrade.	WAN 側での IEEE 802.1X 利用に関しては，国内での利用状況を調査した上で，次版への反映要否について検討する.

Section	Item	Requirements	ガイドラインとの比較
WAN.dot1x.	9	The RG MUST be able to authenticate a minimum of eight authenticators.	WAN 側での IEEE 802.1X 利用に関しては，国内での利用状況を調査した上で，次版への反映要否について検討する．
WAN.dot1x.	10	When used with IPv4 over Ethernet and DHCPv4, if the RG already has a connection when receiving an IEEE 802.1X request, the RG SHOULD subsequently perform a DHCPv4 lease renewal upon successful 802.1X authentication.	WAN 側での IEEE 802.1X 利用に関しては，国内での利用状況を調査した上で，次版への反映要否について検討する．
WAN.dot1x.	11	Each RG MUST have a unique factory-installed private/public key pair and an embedded ITU-T X.509 version 3 / IETF RFC 5280 [125] certificate that has been signed by the RG vendor's certificate authority.	WAN 側での IEEE 802.1X 利用に関しては，国内での利用状況を調査した上で，次版への反映要否について検討する．
WAN.dot1x.	12	The RG certificate MUST have a validity period greater than the operational lifetime of the RG.	WAN 側での IEEE 802.1X 利用に関しては，国内での利用状況を調査した上で，次版への反映要否について検討する．
WAN.dot1x.	13	When used with IPv6 over Ethernet and DHCPv6, if the RG already has a connection when receiving an IEEE 802.1X request, the RG SHOULD subsequently perform a DHCPv6 CONFIRM upon successful 802.1X authentication.	WAN 側での IEEE 802.1X 利用に関しては，国内での利用状況を調査した上で，次版への反映要否について検討する．

3.7 Denial of Service Prevention

Section	Item	Requirements	ガイドラインとの比較
WAN.DoS.	1	The RG MUST provide denial of service (DOS) protection for itself and all LAN CPE including protection from ping of death, SYN flood, LAND and variant attacks. The extent of this protection will be limited when the RG is configured as a bridge in which only PPPoE traffic is bridged. This protection MUST be available when the RG terminates IP (v4 or v6) or bridges IPv4.	ガイドラインに記述がないが，攻撃の定義や性能要件が曖昧な為，要件として記述することは困難と考える． 次版にて，TR-124i5 では MUST 要件であることおよび記述が困難な理由を追記する． （ルータ性能限界と対コストとのバランスに依存する等）
WAN.DoS.	2	The RG MUST reject packets from the WAN with source MAC addresses of devices on the local LAN or invalid IP (v4 or v6) addresses (e.g. broadcast addresses or IP (v4 or v6) addresses matching those assigned to the LAN segment).	ガイドラインに記述がないが，MAC アドレスについてはリジェクトせずに通常動作することも可能であると考える為，対応予定なし．IP アドレスについては次版にて追記するが，不正な IP アドレスの定義について検討が必要．
WAN.DoS.	3	The RG MUST reject any unidentified Ethernet packets (i.e. any packet that is not associated with IP (v4 or v6) or PPPoE protocols).	ガイドラインに記述がないが，unidentified の定義が曖昧な為，要件として対応予定なし．次版にて，TR-124i5 では MUST 要件であることおよび記述が困難な理由を追記する．（ルータ性能限界と対コストとのバランスに依存する等）
WAN.DoS.	4	The RG MUST perform anti-spoofing filtering for IPv6. All IPv6 traffic sent to the WAN from the LAN MUST have an IPv6 source address with a prefix assigned to the LAN by the RG, that was delegated from the WAN (through DHCPv6 or configuration).	ガイドラインには記述はないが，次版にて追記する．要求度については RFC7084 にて MUST から SHOULD に格下げされた経緯があり，要検討．
WAN.DoS.	5	Because the RG must perform anti-spoofing filtering for IPv6, until it has an IPv6 LAN prefix delegation it MUST filter all upstream IPv6 traffic from the home.	ガイドラインに記述はないが，次版にて追記する．

3.8 Quality of Service

Section	Item	Requirements	ガイドラインとの比較
WAN.QoS.	1	The RG MUST support classification of WAN directed LAN traffic and placement into appropriate queues (or discard) based on any one or more of the following pieces of information: (1) destination IP (v4 or v6) address(es) with subnet mask, (2) originating IP (v4 or v6) address(es) with subnet mask, (3) source MAC address, (4) destination MAC address, (5) protocol (TCP, UDP, ICMP, IGMP, …) (6) source TCP/UDP port and port range, (7) destination TCP/UDP port and port range, (8) IEEE 802.1Q Ethernet priority, (9) FQDN (fully qualified domain name) of WAN session, (10) Diffserv codepoint (IETF RFC 3260), (11) Ethertype (IEEE 802.3) length/type field), (12) traffic handled by an ALG, (13) IEEE 802.1Q VLAN identification. (14) Wi-Fi SSID and, (15) LAN type (Ethernet, WiFi, etc.).	ガイドラインには記述なし. QoS は, 網側の機能, サービスとあわせて考える必要があり, また, ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため, 対象外とする.
WAN.QoS.	2	The RG SHOULD support classification of WAN directed LAN traffic and placement into appropriate queues (or discard) based on any one or more of the following pieces of information: (1) packet length (note: to be used with caution to avoid re-ordering packets), and (2) LAN-side physical port.	ガイドラインには記述なし. QoS は, 網側の機能, サービスとあわせて考える必要があり, また, ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため, 対象外とする.

<table>
<tr><th>Section</th><th>Item</th><th>Requirements</th><th>ガイドラインとの比較</th></tr>
<tr><td>WAN.QoS.</td><td>3</td><td>The RG MUST support the differentiated services field (DS field) in IP (v4 or v6) headers as defined in IETF RFC 2474.</td><td>ガイドラインには記述なし. QoS は, 網側の機能, サービスとあわせて考える必要があり, また, ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため, 対象外とする.</td></tr>
<tr><td>WAN.QoS.</td><td>4</td><td>The RG MUST by default recognize and provide appropriate treatment to packets marked with recommended Diffserv codepoints, whose values and behavior are defined in IETF RFCs 2474, 2475, 2597, 3246, and 3260. Specifically, the values shown in the DSCP column of the table below MUST be supported, except Cs0-7, which are optional.
<table>
<tr><th>Class</th><th>Description</th><th>DSCP marking (name)</th><th>DSCP marking (decimal value)</th></tr>
<tr><td>EF</td><td>Realtime</td><td>ef</td><td>46</td></tr>
<tr><td>AF4 – in-contract</td><td>Premium class4 (in)</td><td>af41</td><td>34</td></tr>
<tr><td>AF4 – out-of-contract</td><td>Premium class4 (out)</td><td>af42, af43</td><td>36, 38</td></tr>
<tr><td>AF3 – in-contract</td><td>Premium class3 (in)</td><td>af31</td><td>26</td></tr>
<tr><td>AF3 – out-of-contract</td><td>Premium class3 (out)</td><td>af32, af33</td><td>28, 30</td></tr>
<tr><td>AF2 – in-contract</td><td>Premium class2 (in)</td><td>af21</td><td>18</td></tr>
<tr><td>AF2 – out-of-contract</td><td>Premium class2 (out)</td><td>af22, af23</td><td>20, 22</td></tr>
<tr><td>AF1 – in-contract</td><td>Premium class1 (in)</td><td>af11</td><td>10</td></tr>
<tr><td>AF1 – out-of-contract</td><td>Premium class1 (out)</td><td>af12, af13</td><td>12, 14</td></tr>
<tr><td>DE/BE</td><td>Default / Best Effort</td><td>be</td><td>0</td></tr>
<tr><td>Cs0 (optional)</td><td>Class Selector 0</td><td>cs0</td><td>0</td></tr>
<tr><td>Cs1 (optional)</td><td>Class Selector 1</td><td>cs1</td><td>8</td></tr>
<tr><td>Cs2 (optional)</td><td>Class Selector 2</td><td>cs2</td><td>16</td></tr>
<tr><td>Cs3 (optional)</td><td>Class Selector 3</td><td>cs3</td><td>24</td></tr>
<tr><td>Cs4 (optional)</td><td>Class Selector 4</td><td>cs4</td><td>32</td></tr>
<tr><td>Cs5 (optional)</td><td>Class Selector 5</td><td>cs5</td><td>40</td></tr>
<tr><td>Cs6 (optional)</td><td>Class Selector 6</td><td>cs6</td><td>48</td></tr>
<tr><td>Cs7 (optional)</td><td>Class Selector 7</td><td>cs7</td><td>56</td></tr>
</table></td><td>ガイドラインには記述なし. QoS は, 網側の機能, サービスとあわせて考える必要があり, また, ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため, 対象外とする.</td></tr>
<tr><td>WAN.QoS.</td><td>5</td><td>The RG MUST be able to mark or remark the Diffserv codepoint or IEEE 802.1Q Ethernet priority of traffic identified based on any of the classifiers supported by the RG.</td><td>ガイドラインには記述なし. QoS は, 網側の機能, サービスとあわせて考える必要があり, また, ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため, 対象外とする.</td></tr>
</table>

Section	Item	Requirements	ガイドラインとの比較
WAN.QoS.	6	Requirement relocated to WAN.QoS.VLAN.1	ガイドラインには記述なし. QoS は, 網側の機能, サービスとあわせて考える必要があり, また, ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため, 対象外とする.
WAN.QoS.	7	Requirement relocated to WAN.QoS.VLAN.2	ガイドラインには記述なし. QoS は, 網側の機能, サービスとあわせて考える必要があり, また, ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため, 対象外とする.
WAN.QoS.	8	Requirement relocated to WAN.QoS.VLAN.3	ガイドラインには記述なし. QoS は, 網側の機能, サービスとあわせて考える必要があり, また, ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため, 対象外とする.
WAN.QoS.	9	The RG MUST support one best effort (BE) queue, one expedited forwarding (EF) queue and a minimum of four assured forwarding (AF) queues.	ガイドラインには記述なし. QoS は, 網側の機能, サービスとあわせて考える必要があり, また, ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため, 対象外とする.

Section	Item	Requirements	ガイドラインとの比較
WAN.QoS.	10	The RG MUST duplicate the set of queues for each access session (e.g. L2 PVC, VLAN). This can be done logically or physically.	ガイドラインには記述なし. QoS は, 網側の機能, サービスとあわせて考える必要があり, また, ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため, 対象外とする.
WAN.QoS.	11	The RG SHOULD support the appropriate mechanism to effectively implement Diffserv per-hop scheduling behaviors. The RG SHOULD be able to configure each queue defined in WAN.QoS.9 for strict priority or weighted round robin scheduling. SP queues are served with priority over all other queues. A strict priority scheduler is preferred for EF. WRR queues are served on the basis of configurable weights, provided with a mechanism to prevent starvation (WRR queue minimum bandwidth)	ガイドラインには記述なし. QoS は, 網側の機能, サービスとあわせて考える必要があり, また, ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため, 対象外とする.
WAN.QoS.	12	The RG MUST support aggregate shaping of upstream traffic across all access sessions (e.g. L2 PVC, VLAN).	ガイドラインには記述なし. QoS は, 網側の機能, サービスとあわせて考える必要があり, また, ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため, 対象外とする.
WAN.QoS.	13	The RG MUST support per-class shaping of upstream traffic. Classes are defined in WAN.QoS.4.	ガイドラインには記述なし. QoS は, 網側の機能, サービスとあわせて考える必要があり, また, ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため, 対象外とする.

Section	Item	Requirements	ガイドラインとの比較
WAN.QoS.	14	The RG MUST support the capability to fragment IP traffic on sessions that it originates, in order to limit the effect of large packets on traffic delay.	ガイドラインには記述なし. QoS は, 網側の機能, サービスとあわせて考える必要があり, また, ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため, 対象外とする.
WAN.QoS.	15	The packet size threshold before fragmenting AF and BE packets MUST be configurable.	ガイドラインには記述なし. QoS は, 網側の機能, サービスとあわせて考える必要があり, また, ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため, 対象外とする.
WAN.QoS.	16	The RG MUST handle all telephone service-related network traffic by a high priority queue to avoid congestion, delay, jitter, or packet loss.	ガイドラインには記述なし. QoS は, 網側の機能, サービスとあわせて考える必要があり, また, ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため, 対象外とする.
WAN.QoS.	17	The RG MAY handle all telephone service-related network traffic by a dedicated WAN interface to avoid congestion, delay, jitter, or packet loss.	ガイドラインには記述なし. QoS は, 網側の機能, サービスとあわせて考える必要があり, また, ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため, 対象外とする.

Section	Item	Requirements	ガイドラインとの比較
WAN.QoS.	18	The RG MUST provide counters in terms of dropped and emitted packets/bytes for each queue. Statistics SHOULD be collected from the time of last counter reset or on a configurable sample interval.	ガイドラインには記述なし. QoS は, 網側の機能, サービスとあわせて考える必要があり, また, ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため, 対象外とする.
WAN.QoS.	19	The RG MUST provide information about queue occupancy in terms of packets and peak percentage. Statistics SHOULD be collected from the time of last counter reset or on a configurable sample interval.	ガイドラインには記述なし. QoS は, 網側の機能, サービスとあわせて考える必要があり, また, ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため, 対象外とする.
WAN.QoS.	20	The RG MUST support classification of WAN-directed internally-generated traffic and placement into appropriate queues based on any one or more of the following pieces of information: (1) destination IP address(es) with subnet mask, (2) originating IP address(es) with subnet mask, (3) protocol (TCP, UDP, ICMP, …), (4) source TCP/UDP port and port range, (5) destination TCP/UDP port and port range, (6) Diffserv codepoint (IETF RFC 3260), (7) physical port, in case of voice packets.	ガイドラインには記述なし. QoS は, 網側の機能, サービスとあわせて考える必要があり, また, ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため, 対象外とする.
WAN.QoS.	21	The RG SHOULD support classification of WAN directed internally generated traffic and placement into appropriate queues based on any one or more of the following pieces of information: (1) packet length.	ガイドラインには記述なし. QoS は, 網側の機能, サービスとあわせて考える必要があり, また, ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため, 対象外とする.

Section	Item	Requirements	ガイドラインとの比較
WAN.QoS.	22	The RG MUST be able to learn classification keys (MAC address and IP address) through the following option of the DHCP client requests on the LAN that it serves: (1) DHCP Option 60 (Vendor Class ID), (2) DHCP Option 61 (Client Identifier), (3) DHCP Option 77 (User Class ID), and (4) DHCP Option 125 (Vendor Specific Information).	ガイドラインには記述なし. QoS は, 網側の機能, サービスとあわせて考える必要があり, また, ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため, 対象外とする.
WAN.QoS.	23	The RG SHOULD be able to learn classification keys (MAC address and IP address) for trusted DLNA devices as they are recognized on the LAN.	ガイドラインには記述なし. QoS は, 網側の機能, サービスとあわせて考える必要があり, また, ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため, 対象外とする.

3.8.1 VLAN based QoS

Section	Item	Requirements	ガイドラインとの比較
WAN.QoS.VLAN.	1	The RG MUST support sending the following frame types: untagged frames, priority-tagged frames, and VLAN-tagged frames in the upstream direction. This satisfies TR-101 R-01.	ガイドラインには記述なし. WAN インタフェースにおける VLAN タグの付与等は，網側の機能，サービスとあわせて考える必要があり，また，ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため，対象外とする.
WAN.QoS.VLAN.	2	The RG MUST support setting the priority tag and VLAN ID values. This satisfies TR-101 R-03.	ガイドラインには記述なし. WANにおけるVLANタグの付与等は，網側の機能，サービスとあわせて考える必要があり，また，ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため，対象外とする.
WAN.QoS.VLAN.	3	The RG MUST support receiving untagged and VLAN-tagged Ethernet frames in the downstream direction, and MUST be able to strip the VLAN tagging from the ones received tagged. This satisfies TR-101 R-04.	ガイドラインには記述なし. WANにおけるVLANタグの付与等は，網側の機能，サービスとあわせて考える必要があり，また，ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため，対象外とする.

3.8.2 Quality of Service for Tunneled Traffic

Section	Item	Requirements	ガイドラインとの比較
		This module only applies when the RG is an endpoint for a tunnel to the WAN. This module applies to IPv6 if it is used as either the tunneled or the tunneling protocol.	
WAN.QoS.TUNNEL.	1	The RG MUST be able to mark or remark the Diffserv codepoint of traffic that will be placed over a tunnel, based on classification of that traffic (prior to placing it on the tunnel) using any of the classifiers supported by the RG. This only applies when the traffic is going from LAN to WAN.	ガイドラインには記述なし. QoS 機能は，ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため，対象外とする.
WAN.QoS.TUNNEL.	2	The RG MUST be able to mark the Diffserv codepoint of the underlying tunnel or the IEEE 802.1Q Ethernet priority of Ethernet that is transporting the tunnel, based on classification of the tunneled traffic using any of the classifiers supported by the RG. This only applies when the traffic is going from LAN to WAN.	ガイドラインには記述なし. QoS 機能は，ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため，対象外とする.
WAN.QoS.TUNNEL.	3	When the RG receives tunneled traffic from the WAN, it MUST be able to mark or remark the Diffserv codepoint of that traffic, based on classification of the tunneled traffic using any of the IP-layer or higher layer classifiers supported by the RG.	ガイドラインには記述なし. QoS 機能は，ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため，対象外とする.
WAN.QoS.TUNNEL.	4	When the RG receives tunneled traffic from the WAN, it MUST be able to mark the IEEE 802.1Q Ethernet priority of the LAN Ethernet frame, based on classification of the tunneled traffic using any of the IP-layer or higher layer classifiers supported by the RG.	ガイドラインには記述なし. QoS 機能は，ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため，対象外とする.

Section	Item	Requirements	ガイドラインとの比較
WAN.QoS.TUNNEL.	5	When the RG receives tunneled traffic from the WAN, it MUST be able to mark or remark the Diffserv codepoint or mark the IEEE 802.1Q Ethernet priority of the LAN Ethernet frame, based on classification of the WAN Ethernet, using any of the Ethernet-layer classifiers supported by the RG.	ガイドラインには記述なし. QoS 機能は，ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため，対象外とする.
WAN.QoS.TUNNEL.	6	When the RG receives tunneled traffic from the WAN, it SHOULD be able to mark or remark the Diffserv codepoint or mark the IEEE 802.1Q Ethernet priority of the LAN Ethernet frame, based on classification of the underlying tunnel, using any of the IP-layer classifiers supported by the RG.	ガイドラインには記述なし. QoS 機能は，ガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため，対象外とする.

3.9 IPsec VPN peer to peer

Section	Item	Requirements	ガイドラインとの比較
WAN.IPsecClient.	1	The RG MAY support peer to peer IPSec VPN, as defined in IETF RFCs 4301, 4303, 5996.	ガイドラインには記述なし. IPsec 機能に関してはガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため，対象外とする.
WAN.IPsecClient.	2	If the RG supports IPSec VPN, it MUST support encapsulating security payload (ESP), as defined in IETF RFC 4303.	ガイドラインには記述なし. IPsec 機能に関してはガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため，対象外とする.

Section	Item	Requirements	ガイドラインとの比較
WAN.IPsecClient.	3	If the RG supports IPSec VPN, it MUST support the IKEv2 key exchange protocol as defined in RFC 5996.	ガイドラインには記述なし. IPsec 機能に関してはガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため，対象外とする.
WAN.IPsecClient.	4	If the RG supports IPSec VPN, it MUST support IPSec VPN in tunnel mode, which is defined in section 3.2 of RFC 4301.	ガイドラインには記述なし. IPsec 機能に関してはガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため，対象外とする.
WAN.IPsecClient.	5	If the RG supports IPSec VPN, it MUST support dead peer detection (DPD), which is defined in RFC 5996.	ガイドラインには記述なし. IPsec 機能に関してはガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため，対象外とする.
WAN.IPsecClient.	6	If the RG supports IPSec VPN, it must support configuring the IPSec VPN via web GUI or TR-069 extension.	ガイドラインには記述なし. IPsec 機能に関してはガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため，対象外とする.
WAN.IPsecClient.	7	If the RG supports IPSec VPN, it MUST support that the source address in the IPSec is configured to be either an IP address or a TR-069 instance of WAN interface.	ガイドラインには記述なし. IPsec 機能に関してはガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため，対象外とする.

Section	Item	Requirements	ガイドラインとの比較
WAN.IPsecClient.	8	If the RG supports IPSec VPN, it MUST support that the destination address in the IPSec is configured to be either an IP address or a dynamic domain name.	ガイドラインには記述なし. IPsec 機能に関してはガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため，対象外とする.
WAN.IPsecClient.	9	If the RG supports IPSec VPN, it MUST support querying the status of child security associations (SA) via TR-069 extension.	ガイドラインには記述なし. IPsec 機能に関してはガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため，対象外とする.

3.10 L2tp VPN Remote Access

Section	Item	Requirements	ガイドラインとの比較
WAN.L2tpClient.	1	The device MAY support L2TPv2 VPN, as defined in IETF RFC 2661 [73].	ガイドラインには要件としての記述なし. L2TP 機能に関してはガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため，対象外とする.
WAN.L2tpClient.	2	The device SHOULD support L2TPv3 VPN, as defined in IETF RFC 3931 [97].	ガイドラインには要件としての記述なし. L2TP 機能に関してはガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため，対象外とする.
WAN.L2tpClient.	3	If the device supports L2TP VPN, it SHOULD support L2TP Disconnect Cause Information, as defined in RFC 3145 [81].	ガイドラインには要件としての記述なし. L2TP 機能に関してはガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため，対象外とする.

Section	Item	Requirements	ガイドラインとの比較
WAN.L2tpClient.	4	If the device supports L2TP VPN, it MUST support L2TP/IPSec VPN connection.	ガイドラインには要件としての記述なし. L2TP 機能に関してはガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため, 対象外とする.
WAN.L2tpClient.	5	If the device supports L2TP VPN, it MUST support LNS functions, as defined in IETF RFC 2661 [73] or IETF RFC 3931 [97].	ガイドラインには要件としての記述なし. L2TP 機能に関してはガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため, 対象外とする.
WAN.L2tpClient.	6	If the device supports L2TP VPN, it MUST support configuring the L2TP VPN via Web GUI or TR-069 extension.	ガイドラインには要件としての記述なし. L2TP 機能に関してはガイドラインの主旨である「最低限必要とされる機能を有するもの」に該当しない機能と考えるため, 対象外とする.

3.11 Port Control Protocol

Section	Item	Requirements	ガイドラインとの比較
WAN.PCP.	1	The RG MUST support Port Control Protocol (PCP) Client as specified in RFC 6887 [140].	ガイドラインには要件としての記述なし. ここでのユースケースは, IPv4 サービスにおいて網側の CGN のポートを PCP で操作するものである. IPv4 向けの機能については, ガイドラインの対象外とする.
WAN.PCP.	2	The RG MUST support Port Control Protocol (PCP) Extension for Port Set Allocation as specified in Error! Reference source not found.. 注:上記リファレンスは, RFC7753 [147] である.	ガイドラインには要件としての記述なし. ここでのユースケースは, IPv4 サービスにおいて網側の CGN のポートを PCP で操作するものである. IPv4 向けの機能については, ガイドラインの対象外とする.

Section	Item	Requirements	ガイドラインとの比較
WAN.PCP.	3	The RG MUST support configuring the PCP Client via web GUI or TR-069 extension.	ガイドラインには要件としての記述なし．本要件は，PCP 利用時における要件であり，ガイドラインの対象外とする．
WAN.PCP.	4	The RG MUST be able to use the DHCP option to retrieve Server name(s) as defined in RFC 7291 [143].	ガイドラインには要件としての記述なし．本要件は，PCP 利用時における要件であり，ガイドラインの対象外とする．
WAN.PCP.	5	For the DS-Lite case, if PCP is enabled and no PCP server is configured, the RG MUST consider that the AFTR is the PCP server.	ガイドラインには要件としての記述なし．DS-Lite を含む CGN における PCP の利用は，国内サービスにおいて例がない為，対象外とする．
WAN.PCP.	6	The PCP client of the RG MUST support invocations from applications on the RG, from the Web GUI or from TR-069 extensions.	ガイドラインには要件としての記述なし．本要件は，PCP 利用時における要件であり，ガイドラインの対象外とする．
WAN.PCP.	7	The RG MUST embed an interworking function to ensure interworking between the UPnP IGD (Internet Gateway Device) used by CPE LAN devices in the LAN and PCP as defined in RFC 6970 [141].	ガイドラインには要件としての記述なし．本要件は，PCP 利用時における要件であり，ガイドラインの対象外とする．
WAN.PCP.	8	The RG MUST embed a PCP proxy function as defined in the IETF document “Port Control Protocol (PCP) Proxy Function” Error! Reference source not found..	ガイドラインには要件としての記述なし．本要件は，PCP 利用時における要件であり，ガイドラインの対象外とする．
WAN.PCP.	9	Static (i.e. configured) PCP mappings MUST be stored on the RG across reboot or power off situations.	ガイドラインには要件としての記述なし．本要件は，PCP 利用時における要件であり，ガイドラインの対象外とする．

4 Local Area Networking (LAN)

4.1 General LAN Protocols

Section	Item	Requirements	ガイドラインとの比較
LAN.GEN.	1	The RG MAY support SOCKS as defined in IETF RFC 1928 for non-ALG access to the public address.	ガイドラインでは IPv6 機能に特化した要件を記述している為，検討の範囲外とする．
LAN.GEN.	2	Both NetBios and zero config naming mechanisms MAY be used to populate the DNS tables.	ガイドラインでは IPv6 機能に特化した要件を記述している為，検討の範囲外とする．
LAN.GEN.	3	The RG MAY act as a NETBIOS master browser for that name service.	ガイドラインでは IPv6 機能に特化した要件を記述している為，検討の範囲外とする．
LAN.GEN.	4	The RG MUST support multiple subnets being used on the local LAN.	次版では，LAN 側の章に BBF の MUST 機能として記述されていることを記述した上で，MAY の要件度として記述する．

4.2 LAN IPv6 Addressing

Section	Item	Requirements	ガイドラインとの比較
LAN.ADDRESSv6.	1	The RG MUST create a Link Local (LL) address for its LAN interface, and perform Duplicate Address Discovery (DAD), per RFC 4862. It MUST always use the same LL address, even after reboot or power failure.	ガイドラインには記述なし． 次版以降にて，リンクローカルアドレス付与については明記する．リンクローカルアドレスの変更については記述の是非に関して検討する．
LAN.ADDRESSv6.	2	The RG SHOULD try alternate LL addresses, if DAD fails. The RG vendor can define the algorithm to be used in this case.	ガイドラインには記述なし． 次版以降で記述の是非を検討する．

Section	Item	Requirements	ガイドラインとの比較
LAN.ADDRESSv6.	3	The RG MUST have a ULA prefix (RFC 4193). It MUST always maintain the same prefix, even after reboot or power failure, unless this prefix is changed through configuration, in which case it MUST maintain the changed value.	次版では，LAN 側の章に BBF の MUST 機能として記述されていることを記述した上で，要求度も含め，記述内容を検討する.
LAN.ADDRESSv6.	4	The RG MAY allow its ULA prefix to be changed through configuration.	次版では，LAN 側の章に BBF の MUST 機能として記述されていることを記述した上で，要求度も含め，記述内容を検討する.
LAN.ADDRESSv6.	5	The RG MUST support the ability to enable or disable advertising a /64 from its ULA prefix through Router Advertisement. When enabled, this /64 will be included in RA messages, with L=1, A=1, and reasonable timer values.	ガイドラインに同等の記述有り（3.3.4） 次版では，LAN 側の章に BBF の MUST 機能として記述されていることを記述した上で，要求度も含め，記述内容を検討する.
LAN.ADDRESSv6.	6	The RG MUST support RFC 4861 section 6.2, Router specification requirements.	ガイドランには記述なし. 次版では，LAN 側の章に記述を追加する.
LAN.ADDRESSv6.	7	The RG MUST support configuration of the following elements of a Router Advertisement: M and O flags (RFC 4861), route information (RFC 4191), and default router preference (Prf) (RFC 4191).	ガイドラインに関連する記述有り（6.1.1 と 7.2.2） 次版では，LAN 側の章に BBF の MUST 機能として記述されていることを記述した上で，RFC4191 の要求度および他のオプションの必要性も含め，記述内容を検討する.
LAN.ADDRESSv6.	8	The RG SHOULD support configuration of the following elements of a router advertisement: MTU (RFC 4861).	ガイドラインに同一の記述有り（6.3.1）

Section	Item	Requirements	ガイドラインとの比較
LAN.ADDRESSv6.	9	The RG MUST advertise (in RA) a /64 prefix from all prefixes delegated via the WAN interface. This will have L=1, A=1, and lifetimes per the received (from the WAN) delegation.	ガイドラインに関連する記述有り(6.1.1) 次版では，委譲された全ての Prefix から/64 を広告することの是非，L フラグを 1 とすることの是非を検討した上で，同等の記述内容とする．要件 7，8 との関係についても整理する．
LAN.ADDRESSv6.	10	The RG SHOULD advertise DNS server using the RDNSS option in Router Advertisements (RFC 6106).	ガイドラインに同一の記述有り(6.2.1) 次版では，RFC8106 を参照した上で，オプション毎の要求度について再検討する．

4.3 DHCPv6 Server

Section	Item	Requirements	ガイドラインとの比較
LAN.DHCPv6S.	1	The RG MUST support DHCPv6 server messages and behavior per RFC 3315.	ガイドラインでは，RFC3315 のメッセージ交換や振る舞いに関する記述はない． 要求度について検討した上で記述の追加を検討する．(サポートするオプションに応じて対応するメッセージや振る舞いが異なる為，SHOULD 要件とすることを検討)
LAN.DHCPv6S.	2	The RG MUST support and be configurable to enable/disable address assignment using DHCPv6.	ガイドラインには，必須機能ではないがアドレス配布が可能であることのみ記述あり(6.1.2)．
LAN.DHCPv6S.	3	The RG MUST either have an algorithm or allow configuration (or both) as to which /64 prefix to use, from any received WAN prefixes or its own ULA prefix.	ガイドラインでは，アドレス配布に関連する事項として記述している(3.3.2,3.3.3, 3.3.4)為，本要件は包含されている．

Section	Item	Requirements	ガイドラインとの比較
LAN.DHCPv6S.	4	The RG SHOULD be configurable to support rules as to which host devices will be assigned addresses through DHCPv6. That is, it should be possible for a service provider to place its own host devices at the customer premises and have the RG only support DHCPv6 address assignment to those devices. Note that this does not require use of the RA "M" flag, as the service provider host devices can be configured to always use DHCPv6 for address assignment. The DUID may help to identify host devices.	サービス仕様に依存するため，対応予定なし.
LAN.DHCPv6S.	5	The RG MUST be configurable to enable/disable prefix delegation via DHCPv6.	ガイドラインには，設定の有効・無効に関する記述はない. 次版では，LAN.DHCPv6S.7 と併せて検討する.
LAN.DHCPv6S.	6	The RG MUST support delegation of any received WAN prefix and its own ULA prefix, that is shorter than /64, using mechanisms of RFC 3633.	ガイドラインには，必須機能ではないがプレフィックス配布が可能であることのみ記述あり(6.1.2). 次版では，LAN 側の章に BBF の MUST 機能として記述されていることを記述した上で，MAY の要件度として記述する.
LAN.DHCPv6S.	7	The WAN / ULA prefixes that an RG is allowed to further delegate SHOULD be configurable.	ガイドラインには，必須機能ではないがプレフィックスの再配布が可能であることの記述あり(要件 37). 次版では，ユーザ環境での利便性向上の為，記述を追記する.
LAN.DHCPv6S.	8	The RG MUST support DHCPv6 Information_request messages.	ガイドラインには，同様の記述あり(要件 39).

Section	Item	Requirements	ガイドラインとの比較
LAN.DHCPv6S.	9	The RG MUST support the following DHCPv6 options: IA_NA (RFC 3315), IA_PD (RFC 3633), and DNS_SERVERS (RFC 3646).	ガイドラインには，同様の記述があるが(要件 39,要件 40)，必要度については検討する.
LAN.DHCPv6S.	10	The RG SHOULD support Reconfigure Accept (RFC 3315) and pass the additional set of DHCP options received from the DHCP client on its WAN interface to IPv6 hosts.	ガイドラインには，同様の記述があるが(要件 41)，必要度については検討する.
LAN.DHCPv6S.	11	The options that the RG will provide via DHCPv6 MUST be configurable.	ガイドラインには記述なし．次版にて追記を(必要度についても含めて)検討する.
LAN.DHCPv6S.	12	If address selection policy option is requested in a DHCPv6 request from hosts, the RG SHOULD advertise the generated address selection policy (see WAN.IPv6.21).	ガイドラインには記述なし. 今後の動向次第で次版への反映を検討する.

4.4 Naming Services (IPv6)

Section	Item	Requirements	ガイドラインとの比較
LAN.DNSv6.	1	The RG MUST act as a DNS server for IPv6-capable LAN devices by supporting IPv6 (AAAA) records in its DNS server (per RFC 3596) and allowing these records to be queried using either IPv4 or IPv6 transport (RFC 3901).	ガイドラインには，トランスポートに関して関連する記述あり(5.1). AAAA RR は記述なし. 次版で追加を検討する.
LAN.DNSv6.	2	The RG MUST attach all known (for the host device) globally scoped IPv6 addresses to the DNS record for a particular host device (see LAN.DNS.6), as AAAA records for that device.	ガイドラインには記述なし. CPE ルータとしては必要ないと思われるため対応しない予定.

Section	Item	Requirements	ガイドラインとの比較
LAN.DNSv6.	3	The RG SHOULD support dynamic DNS (DDNS) for devices to provide their own DNS information. This would override any DNS entries the RG might have created for the IP addresses included in the DDNS request.	ガイドラインに関連する記述(3.2.1)はあるが，対応しない予定.
LAN.DNSv6.	4	The RG MUST be able to query for A and AAAA records using either IPv4 or IPv6 transport to DNS recursive name servers in the WAN.	ガイドラインに記述あり(5.1.1).
LAN.DNSv6.	5	The RG SHOULD use a DNS recursive name server obtained through DHCPv6 option 23 (OPTION_DNS_SERVERS) to query for AAAA records to the WAN, as its first choice.	「AAAA RR の query を行う場合，DHCPv6 で取得した DNS サーバを最優先として使用する」という記述は，ガイドラインに記述されていない．日本におけるサービスの条件下では，この要件は必ずしも必須とはならないため，対応しない.
LAN.DNSv6.	6	When the RG is proxying DNS queries for LAN devices, it SHOULD use IPv6 transport regardless of the transport mode used by the LAN device, when querying to the WAN. This is only possible if the RG has IPv6 addresses for DNS recursive name servers on the WAN.	TR-124i5 では「IPv6 での query が可能な場合には，IPv6 で聞く（SHOULD）」ことになっているが，ガイドラインでは「トランスポートは可能な限り合わせる（MAY）」と記述されている．対応しない予定.
LAN.DNSv6.	7	The RG MUST support receiving at least 2 DNS recursive name server IPv6 addresses from the network through DHCPv6 option 23 (OPTION_DNS_SERVERS) (RFC 3646).	ガイドラインでは記述なし. 2 つ以上の Nameserver を受け取ることが可能であることを，次版以降で追加予定.

Section	Item	Requirements	ガイドラインとの比較
LAN.DNSv6.	8	The RG SHOULD allow the user to specify that the network-learned or user-specified DNS recursive name server addresses be passed back to the LAN devices in DHCPv6 responses instead of the RG's address itself as the DNS recursive name server(s).	ガイドラインに Nameserver のアドレス配布自体の記述はある(6.2.2). ただし，配布する Nameserver のアドレスの選択に関する記述はないため，次版以降で検討予定．要求度については要検討.
LAN.DNSv6.	9	When the RG learns DNS name server addresses from multiple WAN connections, the RG SHOULD make recursive query to the DNS name server specified with DNS selection policy that is obtained through DHCPv6 (draft-ietf-mif-dns-server-selection) or manually configured DNS selection policy.	ガイドラインでは記述なし. 複数 WAN 接続環境における要件としてガイドラインに追記する.

4.5 Port Forwarding (IPv6)

Section	Item	Requirements	ガイドラインとの比較
LAN.PFWDv6.	1	The RG MUST support security mechanisms described in RFC 6092.	ガイドラインでは関連記述があるが詳細について言及していない．次版にて記述追加を検討する.
LAN.PFWDv6	2	Individual port forwarding rules MUST be associated with a LAN device, not the IPv6 address of the LAN device, and follow the LAN device should its IPv6 address change.	ガイドラインにはセキュリティの章があるが，該当する記述がない. ポートフォワーディング機能は次版以降で追記を検討する.

Section	Item	Requirements	ガイドラインとの比較
LAN.PFWDv6	3	The port forwarding mechanism of the RG SHOULD be easy to configure for common applications and user protocols (e.g. ftp, http, etc.) by specifying a protocol name or application name in a "Common Applications Names List" instead of a port number and protocol type. A partial list of applications for potential inclusion appears in Appendix I.	ガイドラインにはセキュリティの章があるが，該当する記述がない． ポートフォワーディング機能は次版以降で追記を検討する．
LAN.PFWDv6	4	The RG SHOULD NOT apply RFC 6092 security mechanisms to traffic associated with prefixes it has delegated to other routers inside the LAN.	次版以降で追記を検討する．

4.6 MLD and Multicast in Routed Configurations (IPv6)

Section	Item	Requirements	ガイドラインとの比較
LAN.MLD.ROUTED.	1	The RG MUST support MLDv2 as defined in IETF RFC 3810.	ガイドラインに記述あり(7.3.2)
LAN.MLD.ROUTED.	2	The RG MUST support functionality as described for IGMP in requirements LAN.IGMP.ROUTED. 1, 3-5, 7, 9, 11, 14-16, 18-23	IPv6 マルチキャスト機能は一般的に利用するサービスに依存しているため，ガイドラインにおいては対応予定なし．
LAN.MLD.ROUTED.	3	The RG SHOULD support functionality as described for IGMP in requirements LAN.IGMP.ROUTED. 6, 10, 17	IPv6 マルチキャスト機能は一般的に利用するサービスに依存しているため，ガイドラインにおいては対応予定なし．
LAN.MLD.ROUTED.	4	The RG MUST be configurable to prevent sending MLD messages to the WAN interfaces for specified multicast addresses or scopes.	IPv6 マルチキャスト機能は一般的に利用するサービスに依存しているため，ガイドラインにおいては対応予定なし．

Section	Item	Requirements	ガイドラインとの比較
LAN.MLD.ROUTED.	5	The RG MUST default to not sending MLD messages for scope of 0 through 8.	IPv6 マルチキャスト機能は一般的に利用するサービスに依存しているため，ガイドラインにおいては対応予定なし.

4.7 Firewall (Basic)

Section	Item	Requirements	ガイドラインとの比較
LAN.FW.	1	The RG MUST drop or deny IPv4 access requests from WAN side connections to LAN side devices and to the RG itself except in direct response to outgoing traffic or as explicitly permitted through configuration of the RG (e.g. for port forwarding or management).	RFC6092 との関連を確認した上で，次版への追記を検討する.
LAN.FW.	2	The RG MUST support a separate firewall log to maintain records of transactions according to firewall rules.	RFC6092 との関連を確認した上で，次版への追記を検討する.
LAN.FW.	3	The firewall log file MUST be able to hold at least the last 100 entries or 10 Kbytes of text.	RFC6092 との関連を確認した上で，次版への追記を検討する.
LAN.FW.	4	Firewall log entries SHOULD NOT be cleared except when the RG is reset to its factory default settings.	RFC6092 との関連を確認した上で，次版への追記を検討する.
LAN.FW.	5	The RG MUST timestamp each firewall log entry.	RFC6092 との関連を確認した上で，次版への追記を検討する.
LAN.FW.	6	The RG MUST support the definition of IPv6 firewall rules separate from IPv4.	RFC6092 との関連を確認した上で，次版への追記を検討する.

4.8 Firewall (Advanced)

Section	Item	Requirements	ガイドラインとの比較
		This module applies to IPv6 as well as IPv4, but only if the RG has an IPv6 stack.	
LAN.FW.SPI.	1	The RG MUST support a more robust firewall, such as one that provides a full OSI 7 layer stack stateful packet inspection and packet filtering function.	RFC6092 との関連を確認した上で，次版への追記を検討する.
LAN.FW.SPI.	2	The RG SHOULD provide protection for the following: – Port scans – Packets with same source and destination addresses – Packets with a broadcast source address – Downstream packets with a LAN source address – Invalid fragmented IP (v4 or v6) packets – Fragmented TCP packets – Packets with invalid TCP flag settings (NULL, FIN, Xmas, etc.) – Fragmented packet headers (TCP, UDP and ICMP) – Inconsistent packet header lengths – Packet flooding – Excessive number of sessions – Invalid ICMP requests – Irregular sequence differences between TCP packets The extent of this protection will be limited when the RG is configured as a bridge in which only PPPoE traffic is bridged. This protection MUST be available when the RG terminates IP (v4 or v6) or bridges IPv4.	RFC6092 との関連を確認した上で，次版への追記を検討する.
LAN.FW.SPI.	3	Each type of attack for which protection is provided SHOULD be configurable on the RG and be on by default.	RFC6092 との関連を確認した上で，次版への追記を検討する.

Section	Item	Requirements	ガイドラインとの比較
LAN.FW.SPI.	4	The RG MUST support passing and blocking of traffic by user-defined and TR-069 configurable rules.	RFC6092 との関連を確認した上で，次版への追記を検討する.
LAN.FW.SPI.	5	The RG MUST support setting firewall rules by the TR-069 ACS that cannot be altered by the user. If firewall rules are set via security policies in TR-181i2 profiles, or via other mechanisms such as TR-069 file download, the rules MUST NOT be able to be overridden by user firewall rules.	RFC6092 との関連を確認した上で，次版への追記を検討する.
LAN.FW.SPI.	6	The RG MUST support the user temporarily disabling specific user-defined rules or all user defined rules, that is, without deleting the rules.	RFC6092 との関連を確認した上で，次版への追記を検討する.
LAN.FW.SPI.	7	The RG MUST support the user specifying the order in which firewall rules are processed. Note: not all firewall rules need be included under the scope of this requirement.	RFC6092 との関連を確認した上で，次版への追記を検討する.

Section	Item	Requirements	ガイドラインとの比較
LAN.FW.SPI.	8	The RG SHOULD support specification of any of the following in a firewall rule: – destination IP (v4 or v6) address(es) with subnet mask – originating IP (v4 or v6) address(es) with subnet mask – source MAC address – destination MAC address – protocol (0–255, or by alias: TCP, UDP, ICMP, IP, IGMP, eigrp, gre, ipinip, pim, nos, ospf, …) – source port – destination port – IEEE 802.1Q user priority – FQDN (fully qualified domain name) of WAN session – DiffServ codepoint (IETF RFC 3260) – Ethertype (IEEE 802.3) length/type field) – Traffic matching an ALG filter – IEEE 802.1Q VLAN identification – packet length – TCP flags (urg, ack, psh, rst, syn, fin) – IP option values (potentially name aliases) – logical interface of source – logical interface of destination	RFC6092 との関連を確認した上で，次版への追記を検討する．
LAN.FW.SPI.	9	The RG MAY support filtering based on other fields unique to specific protocols.	RFC6092 との関連を確認した上で，次版への追記を検討する．

Section	Item	Requirements	ガイドラインとの比較
LAN.FW.SPI.	10	The RG SHOULD support firewall rules that support generic pattern matching against the header or data payload of traffic. Logically this can be envisioned as: match(header[offset[,length|max]],condition) match(payload[offset[,length|max]], condition) where condition is (relationship, data) such as (=, ne, all, one, and, or) for a hex field (=, ne, gt, ge, lt, le) for a decimal/hex field (=, ne, contains) for a string field	RFC6092 との関連を確認した上で，次版への追記を検討する.
LAN.FW.SPI.	11	The RG SHOULD support a set of predefined rules to which the user can set or reset the firewall settings.	RFC6092 との関連を確認した上で，次版への追記を検討する.
LAN.FW.SPI.	12	If a set of predefined rules has been set on the RG, the RG rule set SHOULD be able to be used as the basis for a user maintained set of firewall rules.	RFC6092 との関連を確認した上で，次版への追記を検討する.
LAN.FW.SPI.	13	In addition to blocking or passing traffic identified by a firewall filter, the RG MUST support other actions as well, including but not limited to: – logging on success or failure, – notification on success or failure (to email or pager if supported), – sending notification to a PC monitor application (either originator and or centralized source), and – requesting verification from a PC monitor application.	RFC6092 との関連を確認した上で，次版への追記を検討する.
LAN.FW.SPI.	14	The RG MUST allow for configuration of global firewall values.	RFC6092 との関連を確認した上で，次版への追記を検討する.

Section	Item	Requirements	ガイドラインとの比較
LAN.FW.SPI.	15	The RG firewall SHOULD be either ICSA certified (www.icsalabs.com) or be able to display all the attributes necessary for ICSA certification for the current version of either the Residential category or the Small/Medium Business (SMB) category.	RFC6092 との関連を確認した上で，次版への追記を検討する.
LAN.FW.SPI.	16	Unless configured otherwise, DOS, port blocking and stateful packet inspection MUST be provided to all LAN devices receiving traffic from the WAN interface.	RFC6092 との関連を確認した上で，次版への追記を検討する.

4.9 Captive Portal with Web Redirection

Section	Item	Requirements	ガイドラインとの比較
LAN.CAPTIVE.	1	The device and the ACS MUST support a redirect function, which, when enabled, intercepts WAN destination IP (v4 or v6) HTTP requests and responds to these by substituting a specified URL in place of the web page request. The URL, as well as a list of locations for which this redirect would be bypassed (i.e., white list), MUST be set through the TR-069 interface. The actual captive portal to be redirected to may be established at the time the white list is defined or the white list defined first and the captive portal specified at a later time.	ガイドラインには記述なし. 次版への追記を検討する.
LAN.CAPTIVE.	2	The redirection function and associated fields MUST NOT be modifiable by the subscriber.	ガイドラインには記述なし. 次版への追記を検討する.
LAN.CAPTIVE.	3	The device MUST support turning on and off the redirect function when the captive portal URL field is populated and cleared respectively by the TR-069 ACS.	ガイドラインには記述なし. 次版への追記を検討する.
LAN.CAPTIVE.	4	All port 80 traffic, excluding that associated with the white list, MUST be redirected when the redirect function is turned on in the device.	ガイドラインには記述なし. 次版への追記を検討する.

Section	Item	Requirements	ガイドラインとの比較
LAN.CAPTIVE.	5	The captive portal that traffic is redirected to MUST be defined as an IP (v4 or v6) address or a URL with a maximum length of 2,000 characters.	ガイドラインには記述なし. 次版への追記を検討する.
LAN.CAPTIVE.	6	The redirect white list MUST support 512 separate list entries which can be individual IP (v4 or v6) addresses, a range of IPv4 addresses, an IPv6 prefix, or any combination thereof. For a range of IPv4 addresses a subnet mask is required.	ガイドラインには記述なし. 次版への追記を検討する.
LAN.CAPTIVE.	7	Variable length subnet masking (VLSM) MUST be supported in the redirect white list. For example: – Individual IPv4 Address: ipaddress or ipaddress/32 or ipaddress 255.255.255.255 – Range of　64 IPv4 addresses ipaddress/26 or ipaddress　255.255.192.0	ガイドラインには記述なし. 次版への追記を検討する.
LAN.CAPTIVE.	8	The device MUST support only one set or captive portal and redirect settings as a time. If new settings are needed, the ACS will submit these to overwrite the existing values within the device.	ガイドラインには記述なし. 次版への追記を検討する.
LAN.CAPTIVE.	9	A valid set of redirect settings MUST be enabled in a device within five seconds of the redirect URL being sent from the ACS.	ガイドラインには記述なし. 次版への追記を検討する.
LAN.CAPTIVE.	10	The redirect function MUST be disabled on the device within five seconds of the captive portal string being cleared in a device by an empty redirect URL being sent from the ACS.	ガイドラインには記述なし. 次版への追記を検討する.
LAN.CAPTIVE.	11	Incremental packet delay through the device due to white list lookup MUST NOT exceed 5 ms.	ガイドラインには記述なし. 次版への追記を検討する.

5 Management & Diagnostics

5.1 UPnP

Section	Item	Requirements	ガイドラインとの比較
MGMT.UPnP.	1	The RG MUST support UPnP device architecture 1.0. This specification is available for download at http://www.upnp.org.	ガイドラインには記述なし. 次版への追記を検討する.
MGMT.UPnP.	2	The RG MUST support UPnP device identification in accordance with the UPnP device architecture. The RG MUST display itself as a network device with the following information: – Manufacturer name – RG name – Model number – Description (e.g. VendorName Wireless Gateway) – Device address (e.g. http://192.168.1.254)	ガイドラインには記述なし. 次版への追記を検討する.

5.1.1 UPnP IGD

Section	Item	Requirements	ガイドラインとの比較
MGMT.UPnP. IGD.	1	This requirement has been replaced by MGMT.UPnP.IGD.4.	(MGMT.UPnP.IGD.4 項を参照)
MGMT.UPnP. IGD.	2	The RG MUST allow the user to enable logging of all UPnP IGD actions and events.	ガイドラインには記述なし. 次版への追記を検討する.
MGMT.UPnP. IGD.	3	The user SHOULD be warned upon enabling UPnP IGD that this may allow applications to configure the box and allow unintended access to local devices.	ガイドラインには記述なし. 次版への追記を検討する.
MGMT.UPnP. IGD.	4	At a minimum, the RG MUST support UPnP InternetGatewayDevice:2 device template version 1.01 standardized DCP. This specification is available for download at http://www.upnp.org.	ガイドラインには記述なし. 次版への追記を検討する.

5.1.2 UPnP IGD to allow Connection Request Forwarding

Section	Item	Requirements	ガイドラインとの比較
MGMT.UPnP.IGD.ACRF.	1	The RG MUST support UPnP Internet Gateway Device:2 root device as defined in [176]. This specification is available for download at http://upnp.org/specs/gw/UPnP-gw-InternetGatewayDevice-v2-Device.pdf	ガイドラインには記述なし. 次版への追記を検討する.
MGMT.UPnP.IGD.ACRF.	2	The RG MUST support IGD specific security as defined in section 2.3 Security Policies of UPnP InternetGatewayDevice:2 [176]	ガイドラインには記述なし. 次版への追記を検討する.
MGMT.UPnP.IGD.ACRF.	3	Across resets or reboots, the RG MUST remove port mappings and pinholes.	ガイドラインには記述なし. 次版への追記を検討する.

5.1.3 UPnP IGD to allow Connection Request Forwarding through the Firewall of the device

Section	Item	Requirements	ガイドラインとの比較
MGMT.UPnP.IGD.ACRF.IPv6.	1	The RG MUST have a WANIPv6FirewallControl:1 service as specified in [179]. The specification is available for download at http://upnp.org/specs/gw/UPnP-gw-WANIPv6FirewallControl-v1-Service.pdf	ガイドラインには記述なし. 次版への追記を検討する.
MGMT.UPnP.IGD.ACRF.IPv6.	2	The RG MUST allow Inbound Pinhole management (InboundPinholeAllowed set to "1").	ガイドラインには記述なし. 次版への追記を検討する.

5.2 Remote Management (Web Browser)

Section	Item	Requirements	ガイドラインとの比較
MGMT.REMOTE.WEB.	1	The device MUST be able to allow temporary manual remote access to its Web GUI remotely from the WAN interface.	ガイドラインには記述なし．昨今のセキュリティ事情と比較して，推奨すべき要件ではないと考えられる為，対象外とする．
MGMT.REMOTE.WEB.	2	When temporary WAN side remote access is enabled to the device, the remote access session MUST be started within 20 minutes and the activated session MUST time out after 20 minutes of inactivity.	ガイドラインには記述なし．昨今のセキュリティ事情と比較して，推奨すべき要件ではないと考えられる為，対象外とする．
MGMT.REMOTE.WEB.	3	The user MUST be able to specify that the temporary WAN side remote access is a read only connection or one which allows for updates. The default MUST be read only.	ガイドラインには記述なし．昨今のセキュリティ事情と比較して，推奨すべき要件ではないと考えられる為，対象外とする．
MGMT.REMOTE.WEB.	4	Temporary WAN side remote access MUST NOT allow for changing the device password.	ガイドラインには記述なし．昨今のセキュリティ事情と比較して，推奨すべき要件ではないと考えられる為，対象外とする．
MGMT.REMOTE.WEB.	5	Temporary WAN side remote access MUST be disabled by default.	ガイドラインには記述なし．昨今のセキュリティ事情と比較して，推奨すべき要件ではないと考えられる為，対象外とする．
MGMT.REMOTE.WEB.	6	Temporary WAN side remote access SHOULD be through HTTP over TLS (i.e., https using TLS).	ガイドラインには記述なし．昨今のセキュリティ事情と比較して，推奨すべき要件ではないと考えられる為，対象外とする．

Section	Item	Requirements	ガイドラインとの比較
MGMT.REMOTE.WEB.	7	The device SHOULD use a randomly selected port for temporary WAN side remote access to prevent hacking of a well known port.	ガイドラインには記述なし．昨今のセキュリティ事情と比較して，推奨すべき要件ではないと考えられる為，対象外とする．
MGMT.REMOTE.WEB.	8	If a default port is used for temporary WAN side remote access, it MUST be 51003.	ガイドラインには記述なし．昨今のセキュリティ事情と比較して，推奨すべき要件ではないと考えられる為，対象外とする．
MGMT.REMOTE.WEB.	9	The user MUST specify a non-blank password to be used for each temporary WAN side remote access session. This information MUST not be saved across sessions.	ガイドラインには記述なし．昨今のセキュリティ事情と比較して，推奨すべき要件ではないと考えられる為，対象外とする．
MGMT.REMOTE.WEB.	10	The User ID for all temporary WAN side remote access sessions, if required based on the method of implementation, MUST be "tech" by default.	ガイドラインには記述なし．昨今のセキュリティ事情と比較して，推奨すべき要件ではないと考えられる為，対象外とする．
MGMT.REMOTE.WEB.	11	The user MUST be able to change the User ID for all temporary WAN side remote access sessions.	ガイドラインには記述なし．昨今のセキュリティ事情と比較して，推奨すべき要件ではないと考えられる為，対象外とする．
MGMT.REMOTE.WEB.	12	The device MUST allow only one temporary WAN side remote access session to be active at a time.	ガイドラインには記述なし．昨今のセキュリティ事情と比較して，推奨すべき要件ではないと考えられる為，対象外とする．

Section	Item	Requirements	ガイドラインとの比較
MGMT.REMOTE.WEB.	13	All other direct access to the device from the WAN side MUST be disabled and blocked by default.	ガイドラインには記述なし．昨今のセキュリティ事情と比較して，推奨すべき要件ではないと考えられる為，対象外とする．

5.3 Network Time Client

Section	Item	Requirements	ガイドラインとの比較
MGMT.NTP.	1	The RG MUST support an internal clock with a date and time mechanism.	ガイドラインでは IPv6 機能に特化した要件を記述している為，本要求条件は検討の範囲外とする．
MGMT.NTP.	2	The RG clock MUST be able to be set via an internal time client from an Internet source using IETF RFC 1305.	ガイドラインでは IPv6 機能に特化した要件を記述している為，本要求条件は検討の範囲外とする．
MGMT.NTP.	3	The RG MUST support the use of time server identification by both domain name and IP (v4 or v6) address.	ガイドラインには記述なし． 次版への追記を検討する．
MGMT.NTP.	4	If the RG includes default time server values, they SHOULD be specified by domain name and not by IP (v4 or v6) address.	ガイドラインでは IPv6 機能に特化した要件を記述している為，本要求条件は検討の範囲外とする．
MGMT.NTP.	5	The RG SHOULD allow configuration of the primary and alternate time server values in addition to or in place of any default values.	ガイドラインでは IPv6 機能に特化した要件を記述している為，本要求条件は検討の範囲外とする．
MGMT.NTP.	6	If the RG includes default time server values or if time server values are identified in documentation, these values SHOULD be selected using industry best practices for NTP and SNTP clients, as published in section 10 of IETF RFC 4330.	ガイドラインでは IPv6 機能に特化した要件を記述している為，本要求条件は検討の範囲外とする．

Section	Item	Requirements	ガイドラインとの比較
MGMT.NTP.	7	The time client SHOULD support DNS responses with CNAMEs or multiple A or AAAA records.	ガイドラインには記述なし. 次版への追記を検討する.
MGMT.NTP.	8	The default frequency with which the RG updates its time from a time server MUST NOT be less than 60 minutes, or use an operator-specific configuration.	ガイドラインでは IPv6 機能に特化した要件を記述している為，本要求条件は検討の範囲外とする.
MGMT.NTP.	9	The default frequency with which the RG updates its time from a time server MUST NOT be greater than 24 hours, or use an operator-specific configuration.	ガイドラインでは IPv6 機能に特化した要件を記述している為，本要求条件は検討の範囲外とする.
MGMT.NTP.	10	The frequency with which the RG updates its time from a time server SHOULD be able to be configured.	ガイドラインでは IPv6 機能に特化した要件を記述している為，本要求条件は検討の範囲外とする.

6 検討メンバー

下記に検討メンバーを示す．所属の 50 音順に従っている．

所属	氏名
エヌ・ティ・ティ・コミュニケーションズ株式会社	藤崎 智宏（部会長）
ＮＥＣプラットフォームズ株式会社	川島 正伸（部会長）
株式会社インターネットイニシアティブ	佐原 具幸（部会長）
エヌ・ティ・ティ・コミュニケーションズ株式会社	鈴木 聡介
株式会社アイ・オー・データ機器	田畑 敬司
株式会社ネクステック	大石 憲且
株式会社バッファロー	山田 大輔
ヤマハ株式会社	下薗 大樹
ヤマハ株式会社	里吉 一浩
ヤマハ株式会社	藤田 尚吾
ヤマハ株式会社	太田 将博