SMPTE PCD RP 2129:20xx

SMPTE Public Committee Draft

Inter Entity Trust Boundary

Table of Contents Page

Foreword

See AG-16 3.2 (Foreword), and ISO Directive Part 2 clause 12 (Foreword).

SMPTE (the Society of Motion Picture and Television Engineers) is an internationally-recognized standards developing organization. Headquartered and incorporated in the United States of America, SMPTE has members in over 80 countries on six continents. SMPTE"s Engineering Documents, including Standards, Recommended Practices, and Engineering Guidelines, are prepared by SMPTE"s Technology Committees. Participation in these Committees is open to all with a bona fide interest in their work. SMPTE cooperates closely with other standards-developing organizations, including ISO, IEC and ITU.

SMPTE Engineering Documents are drafted in accordance with the rules given in its Standards Operations Manual. This SMPTE Engineering Document was prepared by Technology Committee <TC-32NF>.

Normative text is text that describes elements of the design that are indispensable or contains the conformance language keywords: "shall", "should", or "may". Informative text is text that is potentially helpful to the user, but not indispensable, and can be removed, changed, or added editorially without affecting interoperability. Informative text does not contain any conformance keywords.

All text in this document is, by default, normative, except: the Introduction, any section explicitly labeled as "Informative" or individual paragraphs that start with "Note:"

The keywords "shall" and "shall not" indicate requirements strictly to be followed in order to conform to the document and from which no deviation is permitted.

The keywords "should" and "should not" indicate that, among several possibilities, one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required; or that (in the negative form) a certain possibility or course of action is deprecated but not prohibited.

The keywords "may" and "need not" indicate courses of action permissible within the limits of the document.

The keyword "reserved" indicates a provision that is not defined at this time, shall not be used, and may be defined in the future. The keyword "forbidden" indicates "reserved" and in addition indicates that the provision will never be defined in the future.

A conformant implementation according to this document is one that includes all mandatory provisions ("shall") and, if implemented, all recommended provisions ("should") as described. A conformant implementation need not implement optional provisions ("may") and need not implement them as described.

Unless otherwise specified, the order of precedence of the types of normative information in this document shall be as follows: Normative prose shall be the authoritative definition; Tables shall be next; then formal languages; then figures; and then any other language forms.

If this is a revision, a topical list of changes [should/shall] be included here.

Introduction (Optional/Conditional)

The introduction provides specific information or commentary about the technical content of the document, and about the reasons prompting its preparation. See AG-16 clause 3.3 (Introduction), AG-16 clause 4.2 (Conformance Terms), and ISO Directive Part 2 clause 13 (Introduction).

This section is entirely informative and does not form an integral part of this Engineering Document.

Linear media broadcast channel flows between Entities

Trust Boundaries

For years, Broadcasters and Media Operators (Entities) have been handing off the final composite broadcast channel output via unidirectional co-axial connections using SDI and ASI. Recently they have been migrating this traffic to IP-based network interconnections, typically using newer SMPTE standardized IP protocols such as ST 2022. Entities are learning that there are additional security and routing challenges that must be overcome when utilizing IP networking.

There are two main areas of concern for Entities when inter-connecting with others via IP networks: Security and Address space.

> The document introduces the concept of a Trust Boundary, which is a security function at the edge(s) of an Entity's IP network for broadcast composite channel delivery.
>
> It also describes some of the security, address space and firewalling challenges and makes some recommendations to address these challenges.

Trust Boundary is a security-focused function deployed at an Entity's edge that will enable all desired linear media flows in and out, while blocking all other traffic. The location of a Trust Boundary within the workflow from production to consumer is shown in 4 (Trust Boundary Concepts). Trust boundaries could be considered as media-specific firewalls.

Using private address space

Entities typically run internal networks using private IP addressing (RFC 1918, RFC 4193), and interconnect with other Entities using private subnets. The use of IP networking to interconnect multiple Entities brings a new challenge, as there is no higher-level authority managing the allocation of the (private) edge addressing as there is on the public Internet.

The choice of addressing can be agreed quickly if connections are set up between Entities on a point-to-point basis. This becomes more challenging if routing clashes, and associated service loss, are to be avoided when multiple Entities are to interconnect via a routed network.

The use of NAT to separate internal networks from those outside, and the use of multiple and separate point to point connections can help mitigate potential address clashes when multiple Entities join a meshed and routed Layer 3 (L3) network.

Section §5 is intended to describe a few of the available architectural design choices to enable linear media flows between Entities, highlight some advantages and disadvantages, and encourage Entities to select the most appropriate architecture for their needs

Broadcasters have realized that there are additional challenges around the use, and re-use of private IP address space within multiple Entities, with the associated risk of address clashing. The use of public address space to inter-connect different Entities on private network connections is not good practice.

The more Entities that are interconnected, the bigger the addressing challenge.

[Editors notes: The following paragraph will be replaced with the appropriate patent information during the SMPTE Headquarters publication process.]

At the time of publication, no notice had been received by SMPTE claiming patent rights essential to the implementation of this Engineering Document. However, attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. SMPTE shall not be held responsible for identifying any or all such patent rights.

1 Scope

The scope clearly defines the subject of the document and the aspects covered, thereby indicating the limits of applicability of the document. See AG-16 clause 3.4 (Scope), and ISO Directive Part 2 clause 14 (Scope).

This document covers the technical requirements and practices for the exchange of linear broadcast content between two or more Entities. It covers security, addressing, control and monitoring issues to achieve a desired Quality of Service.

2 Normative References

The normative references clause lists, for information, those documents which are cited normatively in the document. See AG-16 clause 3.5 (Normative References), AG-16 clause 4.3 (Normative References to Standards and Recommended Practices), and the ISO Directives Clause 15 (Normative References).

The following Recommended Practice contains provisions that, through reference in this text, constitute provisions of this Recommended Practice. Dated references require that the specific edition cited shall be used as the reference. Undated citations refer to the edition of the referenced document (including any amendments) current at the date of publication of this document. All Recommended Practices are subject to revision, and users of this engineering document are encouraged to investigate the possibility of applying the most recent edition of any undated reference.

Internet Engineering Task Force (IETF) RFC 768 User Datagram Protocol [online, viewed 2021-02-10] Available at https://www.ietf.org/rfc/rfc768.txt

Internet Engineering Task Force (IETF) RFC 791 Internet Protocol [online, viewed 2021-02-10] Available at https://www.ietf.org/rfc/rfc791.txt

Internet Engineering Task Force (IETF) RFC 2460 Internet Protocol, Version 6 (IPv6) Specification [online, viewed 2021-02-10] Available at https://www.ietf.org/rfc/rfc2460.txt

Internet Engineering Task Force (IETF) RFC 1918 Address Allocation for Private Internets [online, viewed 2021-06-22] Available at https://www.ietf.org/rfc/rfc1918.txt

Internet Engineering Task Force (IETF) RFC 4193 Unique Local IPv6 Unicast Addresses [online, viewed 2021-06-22] Available at https://www.ietf.org/rfc/rfc4193.txt

Internet Engineering Task Force (IETF) RFC 3550 RTP: A Transport Protocol for Real-Time Applications [online, viewed 2021-02-10] Available at https://www.ietf.org/rfc/rfc3550.txt

Internet Engineering Task Force (IETF) RFC 1112 Host Extensions for IP Multicasting

Internet Engineering Task Force (IETF) RFC 4607 Source-Specific Multicast for IP

Internet Engineering Task Force (IETF) RFC 2236 Internet Group Management Protocol, Version 2

Internet Engineering Task Force (IETF) RFC 3376 Internet Group Management Protocol, Version 3

Internet Engineering Task Force (IETF) RFC 2710 MLD Multicast Listener Discovery (MLD) for IPv6

Internet Engineering Task Force (IETF) RFC 3810 MLD Multicast Listener Discovery Version 2 (MLDv2) for IPv6

Internet Engineering Task Force (IETF) RFC 4271 A Border Gateway Protocol 4 (BGP-4)

Internet Engineering Task Force (IETF) RFC 4594 Configuration Guidelines for DiffServ Service Classes

SMPTE ST 259:2008 SMPTE Standard - For Television — SDTV - Digital Signal/Data — Serial Digital Interface

SMPTE ST 292-1:2011 SMPTE Standard - 1.5 Gb/s Signal/Data Serial Interface

ST 2022-2:2007 SMPTE Standard - Unidirectional Transport of Constant Bit Rate MPEG-2 Transport Streams on IP Networks

ST 2022-6:2012 - SMPTE Standard - Transport of High Bit Rate Media Signals over IP Networks (HBRMT)

ISO/IEC 7498-1:1994. Information technology — Open Systems Interconnection — Basic 7-layer Reference Model

DPP-001 Live IP Profiles - Available at https://www.thedpp.com/live/live-ip

3 Terms and Definitions

The terms and definitions clause provide definitions necessary for the understanding of certain terms used in the document. See AG-16 clause 3.6 (Terms and Definitions). AG-16 clause 4.4 (Terms and Definitions), and ISO Directive Part 2 clause 16 (Terms and Definitions).

For the purposes of this document, the following terms and definitions apply:

3.1. Broadcaster

originating source of linear broadcast content

note to entry: often also the content producer

3.2. Media Operator

entity involved in the transmission of linear content from broadcaster to consumer.

3.3. Service Provider

media operator

note to entry: this is a more commonly used term in telecommunications networks for transmission provider, but is analogous to media operator for this document

3.4. Affiliate

entity associated with a broadcaster such as a service provider

3.5. Entity

business or individual

note to entry: the term Entity is used to embody different organizations, or different parts of the same organizations, typically in different geographic locations, that need to interconnect.

Entities in this document are likely to be broadcasters, media operators and service providers.

3.6. IANA Port Number Registry

list of reserved port numbers maintained by the internet assigned number authority

note to entry: a link to the register is given in the bibliography

3.7. IP

internet protocol (v4 rfc 791, v6 rfc 2460)

3.8. igmp

internet group management protocol (IP v4 : rfc 2236 [v2], rfc 3376 [v3])

3.9. MLD

multicast listener discovery (IP v6 : rfc 2710 [v1], rfc 3810 [v2])

3.10. NAT

network address translation (rfc 1631)

note to entry: packet by packet ip/udp address modification

3.11. RTP

real time protocol (rfc 3550)

note to entry: additional encapsulation on top of the IP/UDP layer, adding extra parameters (counters) that support and enhance monitoring and protection functions (if implemented in the Trust Boundary).

4 Trust boundary concepts (informative)

4.1. Security

More and more, Entities have realized that they need to increase the security of these inter-Entity IP network connections, particularly at direct interfaces, to protect internal networks and services from malicious attack or un-intentional damage.

Uni-directional, UDP only, multicast (or unicast) media traffic flows are simple to control, and mostly have a consistent payload, but have much higher bandwidths than standard IT TCP/IP traffic. Traditional IT firewalls (see Annex A2) that can handle such bandwidth are not commercially viable, and nor do they focus on filtering (and optionally, monitoring) at the media-specific payload level at those high bandwidths.

UDP-based ARQ/encryption control traffic supporting the linear media flows may also be included in this Trust Boundary concept.

In this environment Trust Boundaries are more appropriate and cost effective.

4.2. Trust

A security device, such as a firewall, forms a logical boundary, a zone, separating 'trusted' internal and 'un-trusted' external IP networks, blocking or allowing packets according to a multi-layer rule set. In the case of linear media flows the term Trust Boundary describes this transition function between the two zones.

4.3. Trust Boundary Concept

A Trust Boundary is a virtual concept, where functionality is deployed at the demarcation point between two Entities that will monitor, manage and control all linear media traffic between two Entities, filtering out unwanted traffic. Typically, the desired traffic will be IP multicast (or unicast) SMPTE linear media flows.

Operators of a Trust Boundary shall be free to choose whatever protocol or format is appropriate for their use case, and will select a vendor implementation that supports that functionality.

The Trust Boundary is expected to primarily function at the network level, but enhanced features may also enable additional payload-specific functionality, like monitoring.

4.4. Trust Boundary Interfaces

The Trusted interface connects to the Entity's own internal networks and address space, and the Untrusted interface connects to other Entity's networks, as shown in figure 2, configured to be in a different IP address space. There will be at least one Trusted and one Untrusted interface on any Trust Boundary function, depending on the surrounding architecture.

5 Trust Boundary Conformance

A Trust Boundary requires many functions and features to be implemented. Some will depend on the use case selected.

5.1.1. Core conformance statements

In all cases, a Trust Boundary implementation

a) Shall have one or more Trusted interfaces, and one or more Untrusted interfaces
b) Shall drop all IP packets arriving at the Untrusted (outside) interface, unless one or more 'firewall' rules, or templates, are applied to enable desired packets to pass through the function to egress out of the Trusted (inside) interface.
c) Shall apply separate 'firewall' rules, or templates, to flows from the Trusted to Untrusted interface, and drop (block) all other packets,
d) Should operate UDP only
e) Should filter every packet based on source and unicast destination or multicast group addressing, UDP ports, VLAN tags against the Layer 2, Layer 3 and Layer 4 rules, and drop all packets that don't match explicitly.
f) Should separately NAT every 'allowed' frame: replace VLAN tags, IP source and group addressing, UDP ports on a per-flow basis to enable maximum compatibility with 3rd parties
g) Should enforce per-flow accurate packet rate-control on ingress
h) Should maintain RTP headers from ingress to egress, where present.
i) Should connect with network equipment at standard network interface rates (1Gb/s (SFP), 10Gb/s (SFP+), 25Gb/s (SFP28)) on both Trusted and Untrusted interfaces.
j) Should support static and IGMP/MLD multicast joins (IGMP v3 / MLD v2preferred)

k) Should mark QoS appropriately (see 5.2.3) on egress

In addition to the above there are some different use cases that will have format-specific functions or features described below that may be implemented, based on the protocol(s) of the linear media flow.

Note that for each use case, a successful connection will depend on matching capabilities at both ends of the connection.

5.1.2. Use Case 1: UDP/RTP SMPTE 2022, 2110, AES 67 flows

This is the simplest use case, typically selected for use on private, managed networks where FEC and ARQ are not required.

In addition to the core requirements:

l) Shall support SMPTE standard payloads: ST 2022 and ST 2110 and future variants.
m) May filter every packet based on RTP payload type (typically 33 for ST 2022-2, 98 for ST 2022-6, 96 for ST 2110-20, 97 for ST 2110-30 etc.), discarding all other packets.
n) Should monitor each UDP/RTP flow (see monitoring section in next paragraph)
o) May enable (ST 2110) essence timing adjustment.
p) May enable (ST 2110) datagram spacing management.
q) May enable flow duplication, to support ST 2022-7 merge downstream.
r) May enable ST 2022-7 flow protection.
s) May enable alarm-based flow protection.
t) May enable payload standard translation (for example between ST 2110 (component) and ST 2022 (composite))
u) Should support recommended DPP flow profiles

5.1.3. Use Case 2: SMPTE / AES flows with FEC.

For networks where the operator selects FEC as a flow protection mechanism for SMPTE-based or AES-based flows.

In addition to the core requirements and those in Use Case 1:

v) should support additional UDP-based FEC flows to enable packet recovery

5.1.4. Use Case 3: ARQ (NACK) flows with optional FEC

This is typically selected for unmanaged networks (Internet) where ARQ flow protection is required. Authentication and encryption are usually part of the implementation and should be supported.

In addition to the core requirements and those in Use Case 1:

w) should enable additional UDP-based control flows to support ARQ packet recovery
x) should enable additional UDP-based FEC flows to support packet recovery
y) should support authenticated and encrypted flows

5.1.5. Use case 4: Other protocols

It's not anticipated that the Trust Boundary will be used with other UDP-based protocols, but they are not excluded.

In summary, the Trust Boundary becomes the edge of an Entity's network, from an addressing and routing perspective, blocks all unwanted traffic in both directions, and could also provide valuable RTP and payload monitoring at the demarcation point.

5.2. Contributing Factors (informative)

5.2.1. IP v4/v6

The choice of IP v4/v6 will be implementation specific, and agreed by the interconnecting Entities. If v6 is chosen, then the Trust Boundary must support it.

5.2.2. QoS (quality of service, priority)

All linear media flows should be marking with a high priority flag, such as Expedited Forwarding (DSCP 46)[1], but within a Trust Boundary, which is exclusively passing these flows, and blocking all other traffic, support of incoming QoS is less important. Marking egress packets appropriately should be an important part of the Trust Boundary implementation. Re-mark to comply with your own rules.

Of course, correct QoS marking of flows through the rest of the network is important, where traffic is mixed.

5.2.3. ARQ/NACK Transport Protection protocols

The decision to use an ARQ/NACK-based Transport Protection protocol, or UDP/RDP is a choice for the implementor, and is outside the scope of this document. Typically Transport Protection will only be deployed on unmanaged networks.

5.2.4. Encryption and authentication

This document does not attempt to define whether link encryption should be deployed, nor what type is appropriate. Nor does it attempt to describe any need for end-point authentication. These must be considered on per-use basis. However, it's assumed that in many cases, the use of private networks will negate the need for encryption or authentication.

Authentication may be necessary in some cases to help ensure that a particular flow is the correct one with the desired content.

5.2.5. Monitoring

Monitoring the linear media flows for health, status, network and payload levels is operationally important. Useful features include :

a) Tracking RTP missing sequence numbers
b) Tracking RTP inter-arrival time (IAT), packet delivery variation / jitter (PDV)
c) Packet rate (in Mb/s)

[1] RFC 4594 Configuration Guidelines for DiffServ Service Classes

5.2.6. Rate limiting

To protect downstream networks from overrating, some form of rate limiting can be applied to flows through the Trust Boundary

5.2.7. Protection switching

It may be desirable to add functionality to switch between two flows for service protection. This may be alarm-based (payload layer), or hitless merge, based on ST 2022-7 (network layer)

5.2.8. L3 router NAT

It's possible to deploy L3 router devices that will NAT UDP flows, but they are unlikely to be RTP or media-aware and may not have the same range of functions described above.

5.3. Choosing a Trust Boundary.

This document is not about which vendor's product to buy, or how to configure it, but is a set of recommendations and information to help with the choice.

5.4. Testing Trust Boundary Security

It's the responsibility of each Entity deploying a Trust Boundary to ensure sufficient security testing is performed to satisfy the Entity's internal guidelines. Standard InfoSec PEN testing principles should be applied when testing the inside (trusted) and outside (untrusted) interfaces of the Trust Boundary function. This testing should prove protection is being enforced appropriately.

As suggested below, it's anticipated that two interconnecting Entities will each have a Trust Boundary facing the other, so that the security responsibility is internal only.

See also Annex A.

5.5. Deploying Trust Boundaries (informative)

The next few paragraphs are intended to describe where Trust Boundaries might fit into the edge of Entities networks.

5.5.1. Content Producers

For Content Producer Entities, Trust Boundaries are likely to be deployed as shown in Figure 1 below. Firstly between Entity X and Entity Y, becoming the network security edge function, and also after the Editorial Control Boundary[2], typically for the permanent, composite broadcast RTP stream (in this example).

[2] The Editorial Control Boundary is a DPP definition, representing the end of the production chain, where component essence flows are combined into a final, broadcast composite mix. See Annex Reference.

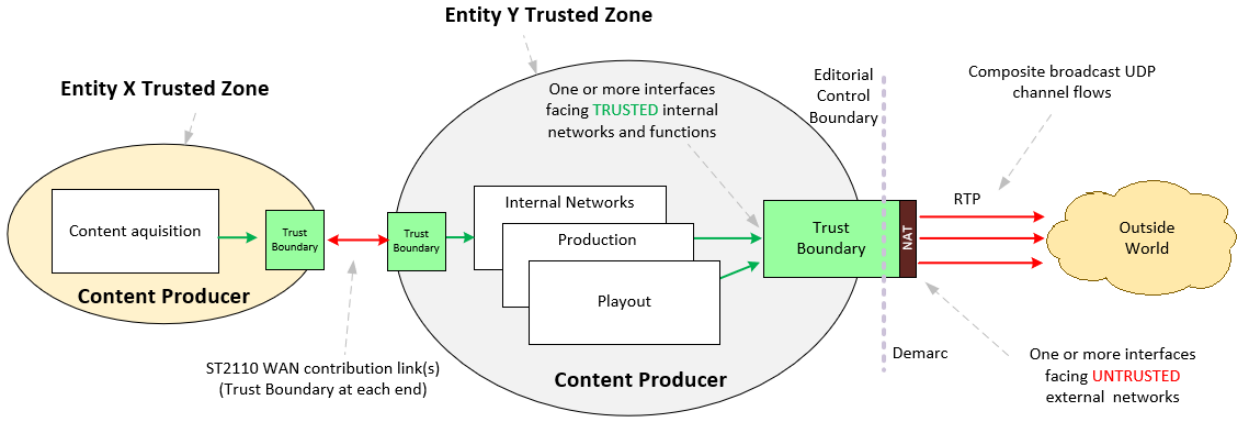

Figure 1.

5.5.2. Service providers – linear pass through

For Service Provider Entities, Trust Boundaries are likely to be deployed as shown in Figure 2, again using UDP/RTP as an example.

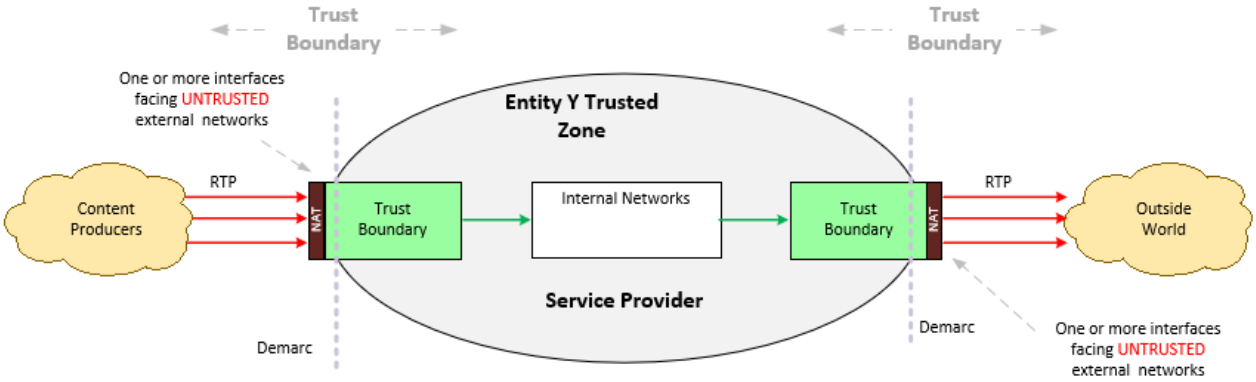

Figure 2.

'Pass-through' Service Providers are likely to need Trust Boundary functions at both ends of the service delivery chain.

5.5.3. OTT Service Providers

For service providers that have a linear flow as an input at the demarcation point, but convert the linear mezzanine into an OTT service, the Trust Boundary function will only be required on the left hand side (in the diagram below) at the ingress point

The work done by CPIX will cover the requirements of all aspects of the OTT delivery, and is complementary to the concept of Trust Boundary.

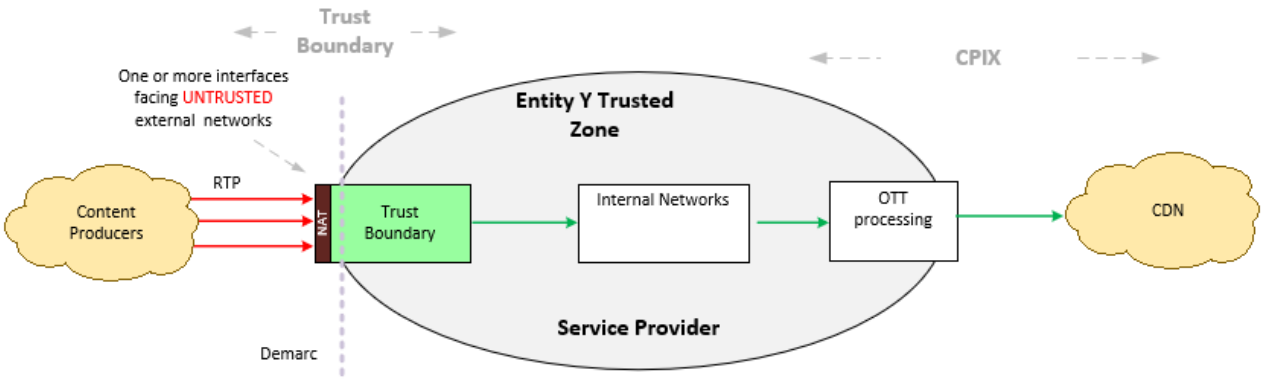

Figure 3.

Figure 3 shows the likely location of a Trust Boundary for an Entity that's responsible for turning a linear RTP flow (as an example) into an OTT service.

6 Network topology (informative)

This second part of the document describes different network topologies that could be implemented to interconnect Media Entities.

There are choices to be made about the way linear media multicast flows are set up to flow across a network, and Entities need to agree on the topology of the interconnection between each other. Each choice has some advantages and disadvantages, which will be explored below.

Network routing technologies are outside the scope of this document, but some references are made.

6.1. Dual and diverse.

The use of dual and diverse connections between Entities to improve service resilience is outside the scope of this document. Each paragraph and diagram below only represents one side of any connection of that type.

6.2. Demarcation points

It may be worth stating that Broadcasters and Telecommunications Service Providers have a slightly different view of where an Entity's demarcation point is . In the Telecommunications industry, it's the customer's responsibility to connect to the Service Provider, and the Service Provider hands out IP addresses. In the Broadcast industry, it's the Service Provider who connects to the customer, and the Customer who (often) hands out the IP addressing.

This has implications for the ownership and responsibility for that interconnecting red line in the figure below.

In the diagram below, the red line could represent a fibre run between two racks in a facility.

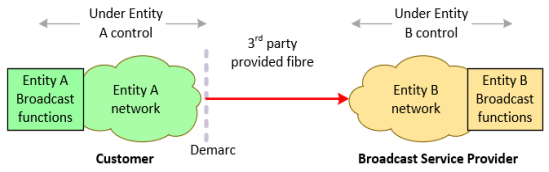

Figure 4 Broadcaster model

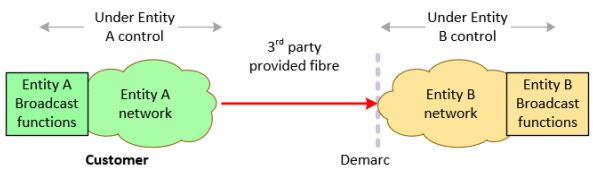

Figure 4 Telecommunications model.

In the Telecommunications industry, the Customer and Service Provider naming is more about a commercial relationship, not about the direction of traffic.

6.3. Interconnecting Entities

6.3.1. Basic point to point connection

Today, many private interconnections between Entities are deployed without any form of Trust Boundary, based on point-to-point connections between L2 network devices, where some security is imposed by configuring the external interfaces to block unwanted traffic.

Typical examples would be contribution networks between a Broadcaster and an Affiliate.

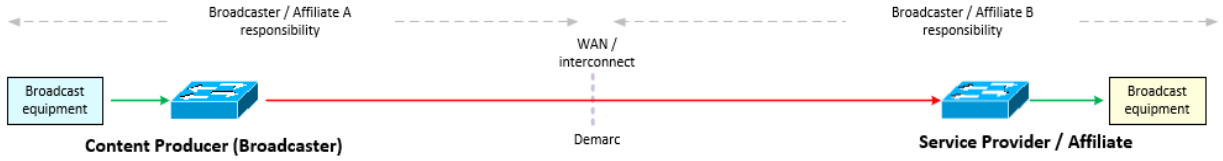

Figure 6.

The security between the two Entities in figure 6 is not optimal, and there is little or no media-specific monitoring.

For completely isolated inter-connections, there are no serious challenges, but if other networks extend away from the switches at either end, a conversation needs to take place between the two Entities to ensure that the routable private address space used on both sides do not overlap. Alternatively, a L2 VLAN could be used to extend one network subnet inside the other, with the associated security risks.

6.3.2. Adding Trust Boundaries to point-point

A better solution, shown in figure 7 below, is to deploy one (or two for 1+1 flows) media-specific Trust Boundary function, as described above, facing the other Entity's network. This specialist function will improve on the security and add value by including further media-related processing and monitoring.

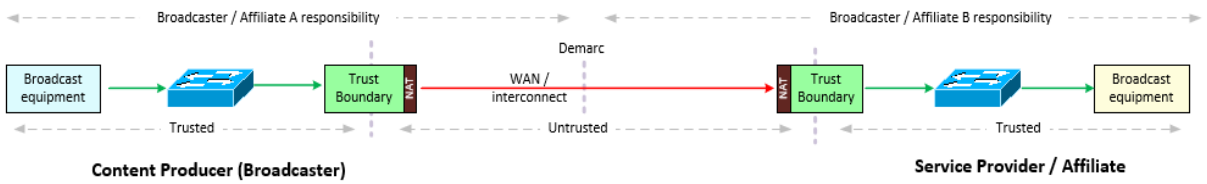

Figure 7

Using Trust Boundaries as shown above has an additional advantage, in that the NAT function at each end means that the effective edge of each Entities network is within the Trust Boundary, and does not extend across the interconnection. Each Entity can use the same internal addressing without compromise.

The two Entities only need to agree on the small subnet to be used on the interconnect.

6.3.3. Transport Protection

For interconnections that are via Public connections (the Internet), ARQ/FEC-based Transport Protection is likely to be deployed, as shown in Figure 8 below, directly facing the untrusted public Internet. The Senders and Receivers could be an additional function within the Trust Boundary concept defined above.

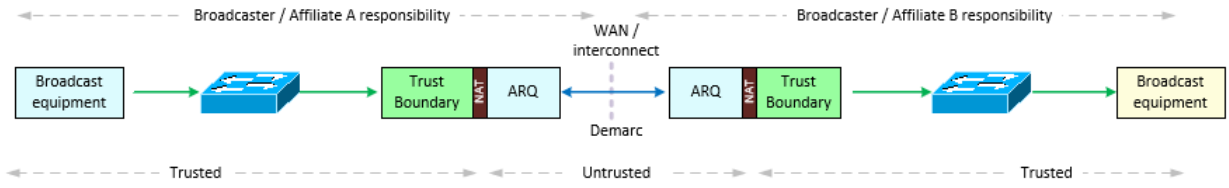

Figure 8

6.3.4. IGMP or static joins

The choice of IGMP or static L2 multicast joins is out of scope.

6.3.5. L2 or L3

In the remaining paragraphs some alternative architectures will be discussed.

6.3.6. Multiple direct connections at Layer 2

In many cases, as shown in the examples above, a point to point connection is the simplest to deploy.

However, if an Entity has multiple connections to other Entities, then there are choices to be made.

This can be achieved with multiple physical (NIC) or logical (VLAN) interfaces on the Trust Boundary functional block, as shown in Figure 9 below.

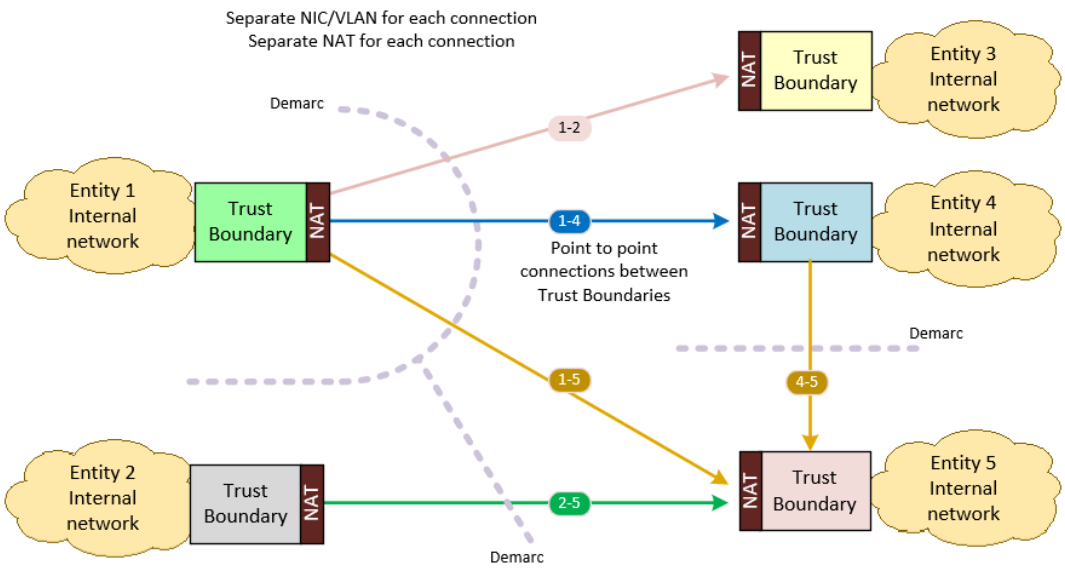

Figure 9

In the example above, each colored block represents a Trust Boundary configured and managed by a separate Entity, with direct connections (L2 etc.) between each Trust Boundary.

Trust Boundaries enable complete network separation between all interconnected Entities, overcoming the challenge of clashing IP address ranges within each of the different Entities.

The allocation of each interconnection can be agreed independently between each pair of Entities without any restrictions imposed by other Entities.

6.3.7. Routed network

In some circumstances, there may be a requirement to deploy a routed network in between the Trust Boundary functions, as shown in Figure 10 below.

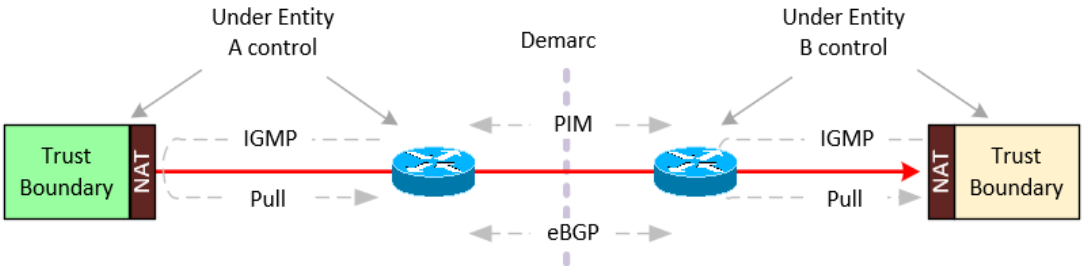

Figure 10

In a routed network, IGMP and PIM are likely to be deployed within an Entities internal network to enable multicast flows to/from the edge router, and eBGP + PIM most likely deployed on the network segment between the Entities. Choices need to be made around the use of which AS numbers to use, whether they be private or publicly assigned to the entity. See Annex.

This routed architecture is more complicated than the L2 alternative in figure 14, as there is another network segment across the demarcation point, and the NAT function in the Trust Boundary is now inside the Entities routed network.

6.3.8. Multiple connections via routed network (Layer 3)

Typically, interconnections between Entities are configured using private addresses from the ranges defined in RFC 1918, so there is no higher-level authority controlling what addresses each Entity shall use when connecting with another. When only two Entities interconnect, it is easy to agree on a suitable subnet for the interconnect.

If the routed network example in figure 10 (above) is expanded to include multiple Entities, as shown below in Figure 11, it becomes more complicated to arrange the assortment of subnet address ranges to avoid clashing between any or all of them. The Trust Boundary function will isolate all the internal subnets from this inter-Entity network, but there will still need to be a dialogue between every single Entity to successfully interconnect them all. The diagram below imagines that the L3 devices (A, B, C etc.) cannot NAT[3].

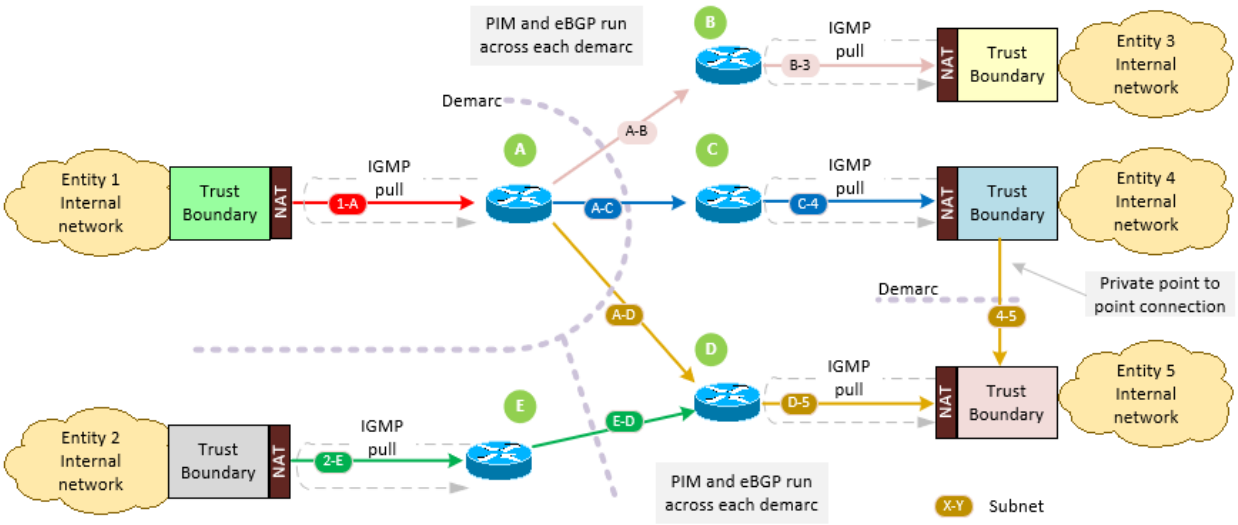

Figure 11

Figure 11 above illustrates the challenge when extra interconnects are provisioned via private inter-Entity networks. If the subnets either side of routers A, B, C or D have clashing address space, that will be a problem with this architecture. If routers A and E have clashing address spaces, that will be a problem for router D. However, the Trust Boundaries NAT functionality will isolate every Entity's internal network, simplifying the challenge of clashing IP address space.

Care will need to be taken to avoid the risk of one of the Entities setting the address/subnet of the external Trust Boundary interface to clash with one from another, possibly disrupting an existing flow.

[3] Some L3 routers can NAT flows at wire-speed, but there should only be one NAT function at the edge of the Entity's network, and it's proposed that NAT is best implemented in the Trust Boundary.

Figures 9 and 11 represent two opposite ends of a spectrum of interconnection opportunities.

6.3.9. Link aggregation across inter-Entity connections.

It's expected that in many cases, multicast flows will be duplicated and delivered via separate and diverse paths (RED and BLUE, A and B), but it's also good practice to use dual connections within facilities between Entities, to avoid the delay while a failed link is fixed, and the redundancy is restored.

The choice of protocol or configuration for these dual links needs to be carefully considered, as load-sharing across two links is undesirable, as it can add to packet jitter and cause re-ordering. The dual links should be for link protection or redundancy only.

6.3.10. ASM or SSM?

Multicast flows can be configured without a Source address or port. This "Any Source Multicast" (ASM) is flexible but can be less reliable in practice. Source-specific multicast (SSM), where the Source address and port ARE defined, is preferred and recommended in all deployments.

7 Network topology and implementation Conformance points

When different Entities interconnect, the following recommendations are important.

Entities should use private IP address ranges when using inter Trust Boundary private links. (see Annex A2)

Entities should use private ASN numbers when inter-connecting via Layer 3 on private links (see Annex A3)

Entities should use UDP ports above 1024 for both source and destination addressing. (see Annex A4).

Entities should consider using point-to-point connections to reduce the risk of IP routing failures (and service loss), as more Entities join the private routed network without sufficient consultation.

Entities should use NAT to eliminate overlapping IP address ranges.

Entities should use SSM and avoid ASM.

8 Conclusion

There are several different ways that an 'inter-Entity' connection can be built and configured, as demonstrated above. The architecture that is chosen will be influenced by each Entity's focus on security, flexibility, orchestration, and cultural choice of software-defined networking (SDN) vs traditional networking.

The capabilities of, and functionality within, is at the discretion of the implementer, but operational testing is recommended to prove the business objectives are fulfilled.

Direct connections between Trust Boundaries offer the highest security and eliminate the risk of service loss due to other Entities joining a routed network incorrectly, but without a network device in the signal path, the number of direct connections will be limited to the number of available interfaces on the Trust boundary.

Adding network devices in the signal path could add extra jitter to each flow, which may be important if the end receiving device is intolerant of large jitter.

Ultimately it will be down to the two Entities to agree how each interconnection shall be provisioned and configured.

Annex A (Informative)

The annex heading shall be followed by the indication “(normative)” or “(informative)”, and by the title.

See AG-16 clause 3.8 (Annexes), and ISO Directive Part 2 clause 20 (Annexes).

A.1 Separation of traffic types

There are established standards and technologies that cover interconnection of non-linear, data-orientated TCP/IP networks for standard IT traffic and any such traffic should be steered down such networks and not via any Trust Boundary implementations. Typically, IT firewalls would be deployed at the edge of these bi-directional data networks to control and limit TCP/IP data traffic with its huge range of ports and data types.

A.2 Private address space RFC 1918 (IP v4), RFC 4193 (IP v6)

3 separate ranges of the available IPV4 addressing space were defined by RFC 1918 as suitable to be used inside a private network, and more importantly, that it would never be routed across any public network.

These ranges are

10.0.0.0 – 10.255.255.255 (RFC 1918, IP v4)

172.16.0.0 – 172.31.255.255 (RFC 1918, IP v4)

192.168.0.0 – 192.168.255.255 (RFC 1918, IP v4)

fc00::/7 address block = RFC 4193 IP v6 Unique Local Addresses (ULA)

All Entities use IP addressing and subnets freely within their private networks, but there are no rules to stop these networks clashing when Entities inter-connect.

A.3 Use of Autonomous System Numbers (ASN) in inter-Entity L3 connections

Each public facing Entity is allocated one or more Public Autonomous System Numbers (ASN) to use when inter-connecting to other Entities at Internet Exchanges. For private connections, such as those described above, use of AS numbers in a private range, is recommended. See RFC 6996.

A.4 UDP port usage

The IANA Port Number Registry states that ports 0-1024 are ‘system’, ports 1024-49151 are ‘user’, therefore use UDP ports from the ‘user range. This includes the ‘source’ port.

There is no technical reason not to use system ports for multicast media flows, 0 included, but then you run the risk of downstream devices not working correctly, depending on how the vendor has implemented their network stack.

In the 2nd paragraph of section 5.1 of RFC 8085, it says:

A UDP sender SHOULD NOT use a source port value of zero. A source port number that cannot be easily determined from the address or payload type provides protection at the receiver from data injection attacks by off-path devices. A UDP receiver SHOULD NOT bind to port zero.

A.5 InfoSec requirements

The assurance of security within each Trust Boundary implementation shall be assessed via a penetration test conducted by CHECK, CREST, or TIGER accredited testers and third parties. The results of such tests shall evidence that any of the core security functions have been met and could not be circumvented or breached by an adversary.
It's also worth considering the recommendations defined in the EBU security documents listed below in the Bibliography.

A.6 Software Defined Networking (SDN)

The path that packets take through a network is normally automatically set by a number of Ethernet and IP (routing) protocols running within and between switches and routers. An alternative mode of operation, often called Software-defined networking, disables many of those automatic protocols running on the routers and switches, and instead calculates paths in software at a higher level, which are then imposed on the switches.

Bibliography (Conditional) (Informative)

Useful documents that are not required to implement this Recommended Practice. See AG-16 clause 3.9 (Bibliography), and ISO Directive Part 2 clause 21 (Bibliography).

IANA Service Name and Transport Protocol Port Number Registry. Continually updated at https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

Internet Engineering Task Force (IETF) RFC 8085 UDP Usage Guidelines [online, viewed 2021-07-28] Available at https://www.ietf.org/rfc/rfc8085.txt

EBU R 148 Minimum Security Tests for Networked media Equipment

EBU R 143 Cybersecurity for media vendor systems, software & services

Information for Document Editors (this page is to be deleted prior to FCD ballot)

The following documents have useful reference material for document editors.

SMPTE AG 16:2018 -- SMPTE Engineering Document Style Guidelines

International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC), Directives, Part 2:2016-05, Principles and rules for the structure and drafting of ISO and IEC documents, 7.0

Warning: Only copy-and-paste plain text from other documents; otherwise this style set may be corrupted.

The following styles are available for SMPTE document editors:

- Annex – For annex headings and subheadings
- Headings – For clause headings and subheadings; These are red if too deep
- Hyperlink – No underline as recommended
- NOTE – A single note; Additional paragraphs need a tab char for proper spacing
- NOTE 1 – For numbered notes; use for a group of (numbered) notes
- NOTE n continued – Used for additional paragraphs in a numbered note.
- S XML – For XML snippets
- S pseudo code – For pseudo code or Programming language code segments
- MathVariable – A single math variable
- MathVariableSubscriptSuperscript – A subscript or superscript for a single math variable
- SMPTE boiler plate – Prose that should not be altered or deleted.
- SMPTE notes and hints – Prose that can be deleted when the document editor wishes.
- Terms and Defs – Used for numbering definitions in the terms and definitions clause.
- TermAcronym– Used for acronyms (under a term) in the terms and definitions clause.
- Title – Section headings; these are not numbered and are included in the Table of Contents
- Subtitle – Subsection headings; these are not numbered and are included in the Table of Contents
- FigureCaption – Used for captions for figures
- TableTitle – Used for title above a table