SMPTE RECOMMENDED PRACTICE

Inter-Entity Trust Boundary

Table of Contents

445 Hamilton Ave., White Plains NY 10601, (914) 761-1100
Approved August 28, 2023

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 clause 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.

Introduction

Linear media broadcast channel flows between entities

For years, broadcasters and media operators (entities) have been handing off the final composite broadcast channel output via unidirectional coaxial 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 interconnecting with others via IP networks:

- **Security:** This 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.
- **Address space:** This document also describes some of the security, address space, and firewalling challenges and makes recommendations to address these challenges.

Trust boundaries

A 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 Clause 4 (Trust boundary concepts). Trust boundaries can 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 to 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.

Clause 6 describes 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 reuse of private IP address space within multiple entities, with the associated risk of address clashing. The use of public address space to interconnect different entities on private network connections is not good practice.

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

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

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 (QoS).

2 Normative references

The following documents contain 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 documents 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

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

SMPTE 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

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

3.1
broadcaster

originating source of linear broadcast content

Note 1 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 1 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 1 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/or service providers.

3.6
IANA Port Number Registry

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

Note 1 to entry: A link to the register is provided in the Bibliography.

3.7
IP

internet protocol

[SOURCES: v4 RFC 791, v6 RFC 2460]

3.8
IGMP

internet group management protocol

[SOURCES: IP v4:RFC 2236 [v2], RFC 3376 [v3]]

3.9
MLD

multicast listener discovery

[SOURCES: IP v6:RFC 2710 [v1], RFC 3810 [v2]]

3.10
NAT

network address translation

Note 1 to entry: Packet by packet IP/UDP address modification.

[SOURCE: RFC 1631, modified — Note 1 to entry has been added.]

3.11
RTP

real-time protocol

Note 1 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).

[SOURCE: RFC 3550, modified — Note 1 to entry has been added.]

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 unintentional damage.

Unidirectional, 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 A.2) 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 can 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 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 are 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 can 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 is at least one trusted and one untrusted interface in any trust boundary, depending on the surrounding architecture.

5 Trust boundary conformance

5.1 Conformance

5.1.1 Core conformance statements

A trust boundary requires many functions and features to be implemented. Some depend on the use case selected. 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 do not match explicitly.

f) Should separately apply NAT to every "allowed" frame: replace VLAN tags, IP source and group addressing, and UDP ports on a per-flow basis to enable maximum compatibility with third 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 5.2.2) on egress.

In addition to items a) to k) above, there are use cases that have format-specific functions or features described l) to y) 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 5.2.5).

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

This addresses 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 is not anticipated that the trust boundary will be used with other UDP-based protocols, but they are not excluded.

5.1.6 Trust boundary summary

In summary, the trust boundary becomes the edge of an entity's network, and 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 are expected to be marked 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 ought to 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 is deployed, nor what type is appropriate. Nor does it attempt to describe any need for end-point authentication. These must be considered on a per-use basis. However, it is assumed that in many cases, the use of private networks will negate the need for encryption or authentication.

Authentication might 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)

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

[1] RFC 4594 Configuration Guidelines for DiffServ Service Classes

5.2.8 L3 router NAT

It is possible to deploy L3 router devices that implement NAT with UDP flows, but they are unlikely to be RTP or media-aware and might not have the same range of functions described.

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 is 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 proves that protection is being enforced appropriately.

As suggested in 5.5, it is 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)

5.5.1 Deployment

Clause 5.5 describes where trust boundaries might fit into the edge of entities' networks.

5.5.2 Content producers

For content producer entities, trust boundaries are likely to be deployed as shown in **Figure** 1, 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).

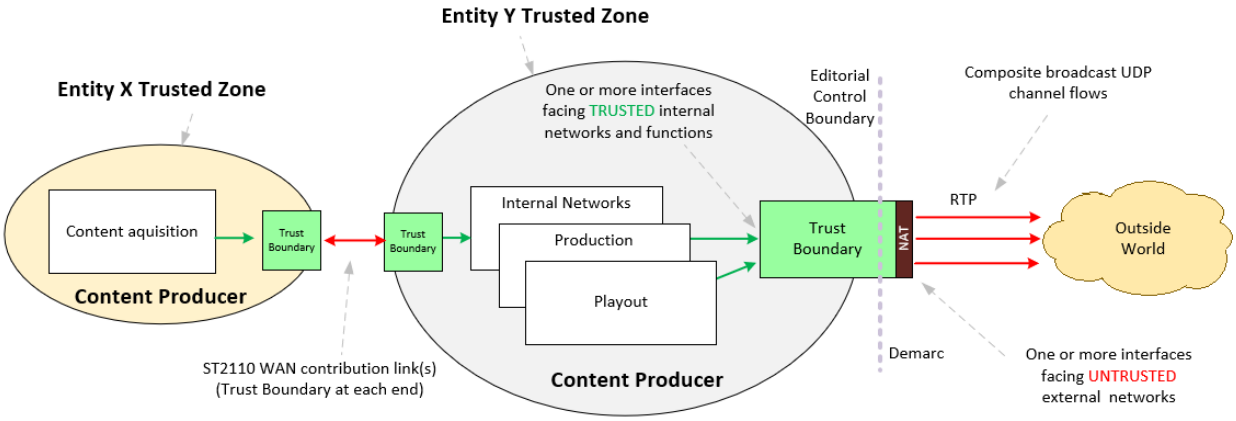

Figure 1 — Trust boundaries as typically deployed by content producers

[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 A.

5.5.3 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.

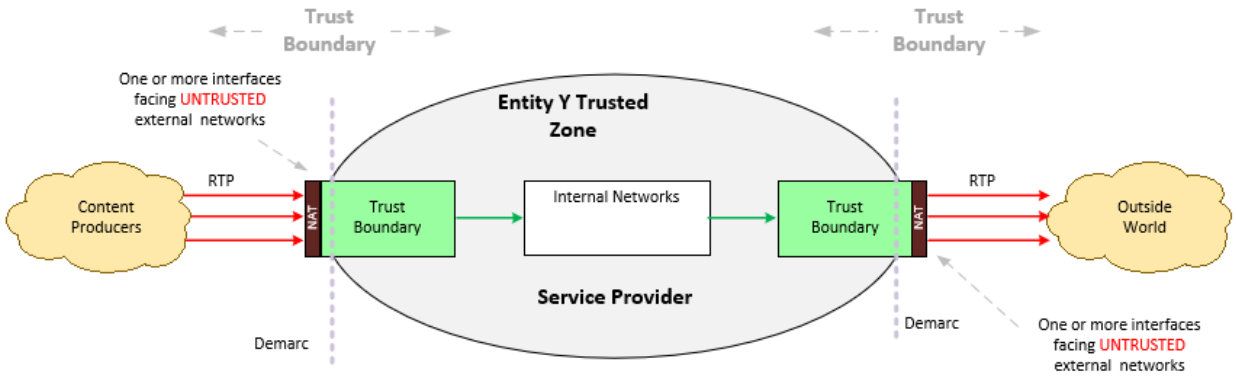

Figure 2 — Trust boundaries as typically deployed by linear pass-through service providers

"Pass-through" service providers are likely to need trust boundary functions at both ends of the service delivery chain.

5.5.4 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 at the left side at the ingress point, as shown in Figure 3.

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.

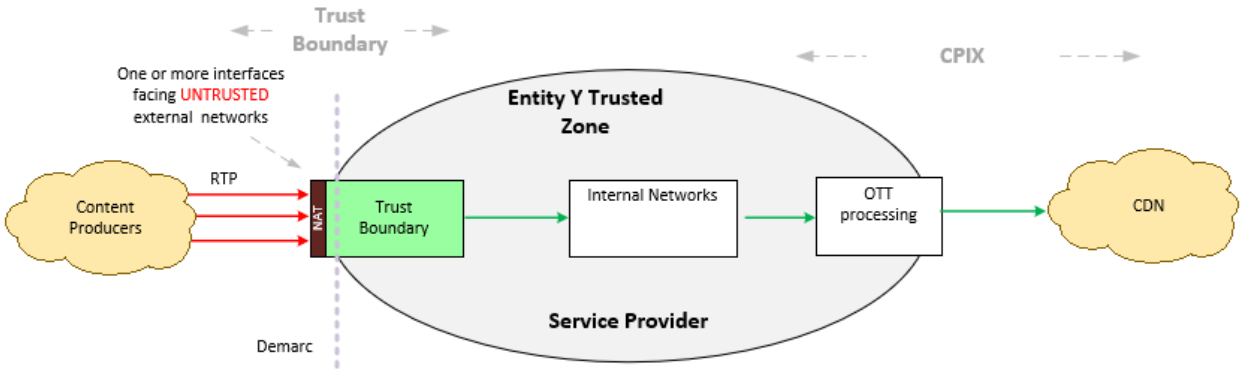

Figure 3 — Trust boundary as typically deployed by OTT service providers

Figure 3 shows the likely location of a trust boundary for an entity that is responsible for turning a linear RTP flow (as an example) into an OTT service.

6 Network topology (informative)

6.1 Connecting entities

The remainder of this 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 advantages and disadvantages, which are explored in Clause 6.

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

6.2 Dual and diverse

The use of dual and diverse connections between entities to improve service resilience is outside the scope of this document. Clause 6.3 and Clause 6.4 describe only one side of any connection of the specified connection type.

6.3 Demarcation points

Broadcasters and telecommunications service providers have slightly different views of the location of an entity's demarcation point.

- In the broadcast industry, the service provider connects to the customer, and the customer (often) assigns the IP addresses.
- In the telecommunications industry, it is the customer's responsibility to connect to the service provider, and the service provider assigns IP addresses.

This has implications for the ownership and responsibility for that interconnecting red line, as shown in Figure 4 and Figure 5.

In Figure 4 and Figure 5, the red line could represent a fibre run between two racks in a facility.

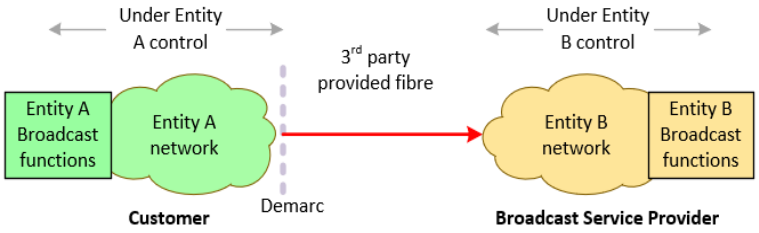

Figure 4 — Broadcaster model

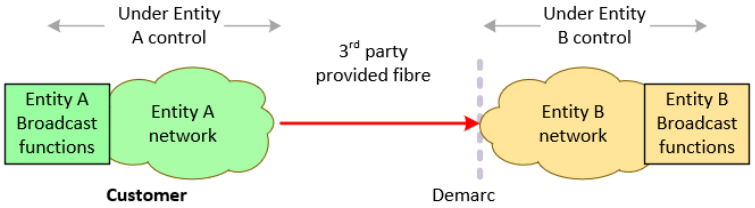

Figure 5 — Telecommunications model

In the telecommunications industry, the customer and service provider naming is more about a commercial relationship, not about the direction of traffic.

6.4 Interconnecting entities

6.4.1 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.

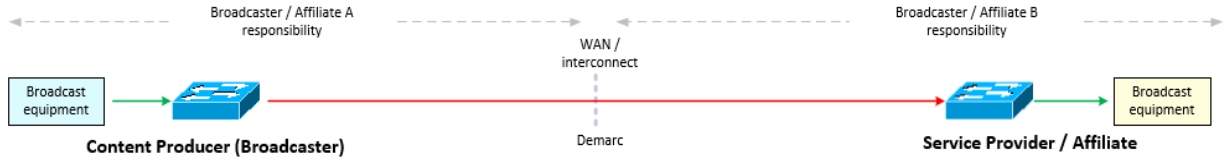

Figure 6 — Basic point-to-point connection without trust boundary

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

For completely isolated interconnections, 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.

6.4.2 Adding trust boundaries to a point-to-point connection

A better solution, shown in Figure 7, is to deploy one (or two for 1+1 flows) media-specific trust boundary function, as described in 6.4.1 above, facing the other entity's network. This specialist function improves on the security and adds value by including further media-related processing and monitoring.

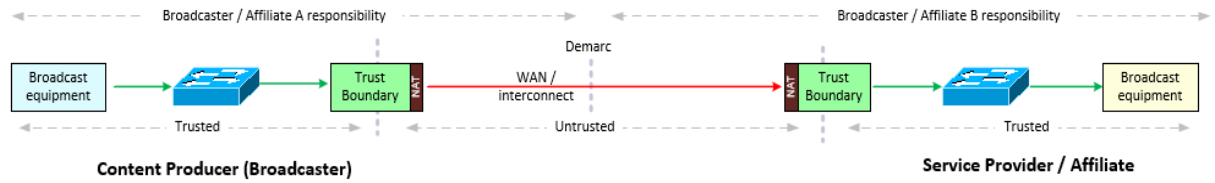

Figure 7 — Point-to-point connection with trust boundaries

Using trust boundaries has an additional advantage, in that the NAT function at each end means that the effective edge of each entity's 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 need to agree only on the small subnet to be used on the interconnect.

6.4.3 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, directly facing the untrusted public Internet. The senders and receivers could be additional functions within the trust boundary concept.

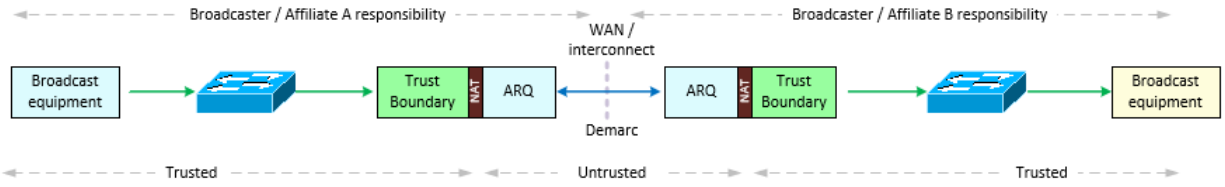

Figure 8 —Transport protection for public interconnection

6.4.4 IGMP or static joins

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

6.4.5 L2 or L3

The remainder of Clause 6 describes alternative architectures.

6.4.6 Multiple direct connections at Layer 2

In many cases, as shown in the examples in 6.3 and 6.4, a point-to-point connection is the simplest to deploy.

However, if an entity has multiple connections to other entities, then there is a variety of options.

An entity can have multiple connections to other entities that might be achieved with multiple physical (NIC) or logical (VLAN) interfaces on the trust boundary functional block, as shown in Figure 9.

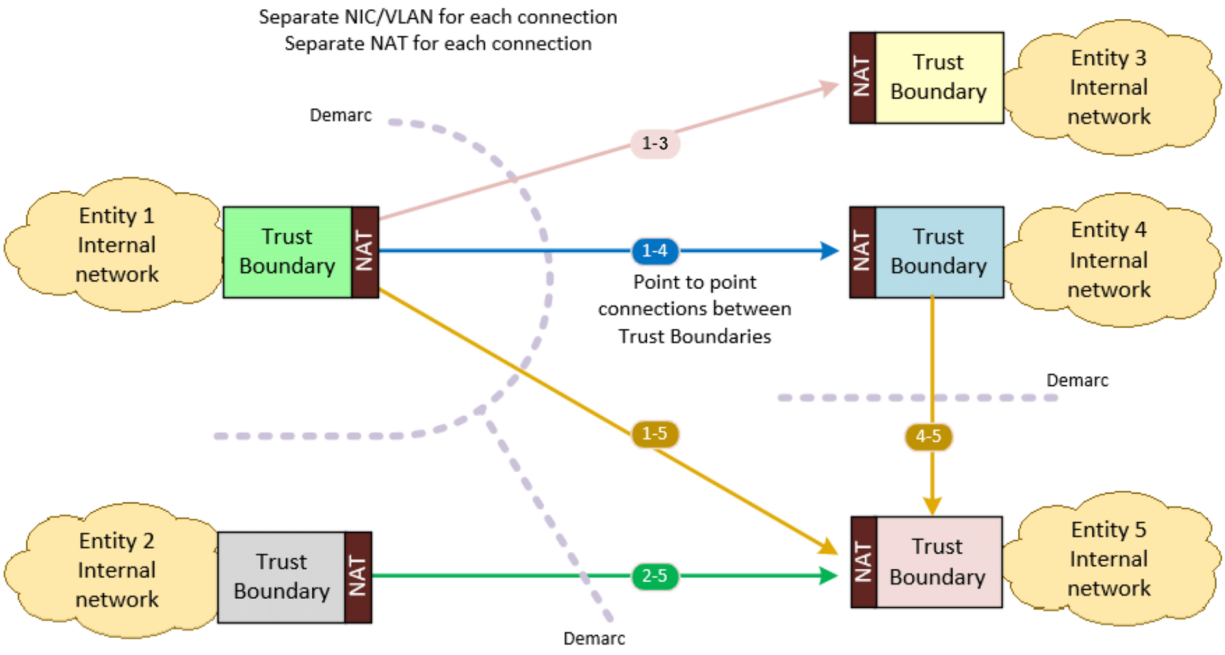

Figure 9 — Multiple direct connections at Layer 2

In Figure 9 and Figure 10, 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.

6.4.7 Routed network

In some circumstances, there might be a requirement to deploy a routed network in between the trust boundary functions, as shown in Figure 10.

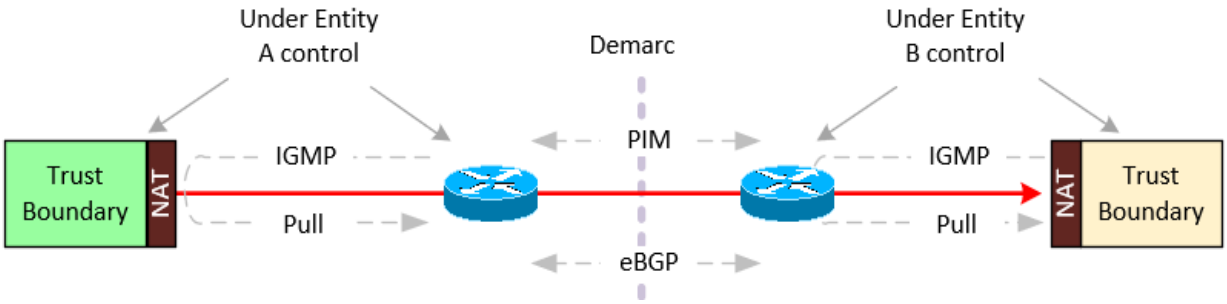

Figure 10 — Routed network in between trust boundaries

In a routed network, IGMP and PIM are likely to be deployed within an entity's 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 Autonomous System Numbers (ASNs) to use, whether they be private or publicly assigned to the entity. See Annex A.

This routed architecture is more complicated than the L2 alternative in Figure 9, as there is another network segment across the demarcation point, and the NAT function in the trust boundary is now inside the entity's routed network.

6.4.8 Multiple connections via routed network at 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 must use when connecting to 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 is expanded to include multiple entities, as shown in Figure 11, it becomes more complicated to arrange the assortment of subnet address ranges to avoid clashing among 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. Figure 11 shows an instance in which the L3 devices (A, B, C, etc.) cannot apply NAT[3].

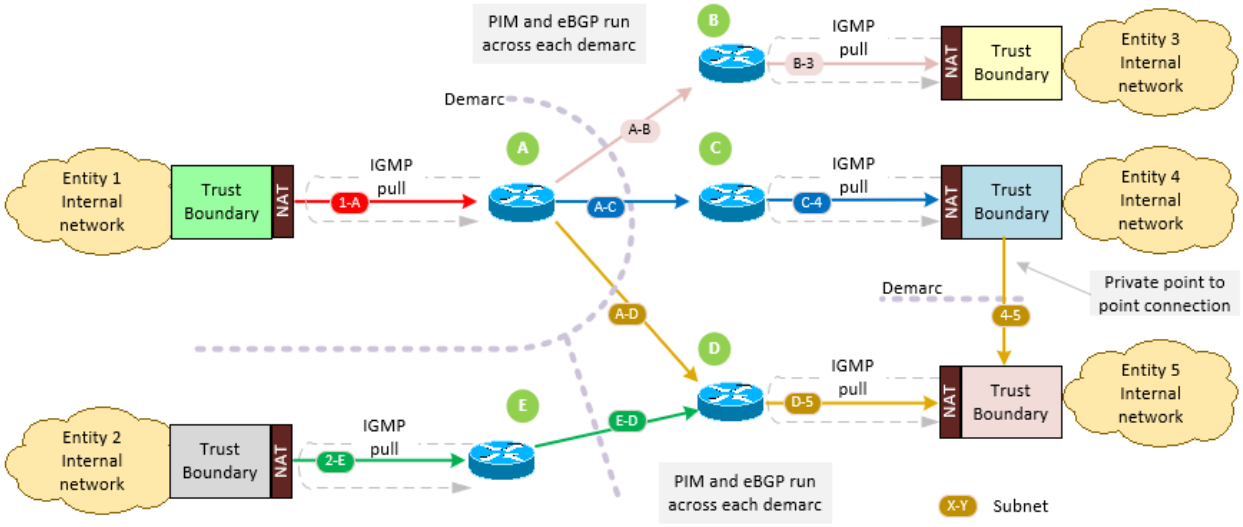

Figure 11 — Multiple connections via routed network at Layer 3

Figure 11 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, then that will cause a problem with this architecture. If routers A and E have clashing address spaces, then that will cause 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.

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

[3] Some L3 routers can apply NAT flows at wire-speed, but it is recommended that there be only one NAT function at the edge of the entity's network, and it is proposed that NAT is best implemented in the trust boundary.

6.4.9 Link aggregation across inter-entity connections.

It is expected that in many cases, multicast flows will be duplicated and delivered via separate and diverse paths (e.g., RED and BLUE, A and B), but it is 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. Dual links ought to be employed for link protection or redundancy only.

6.4.10 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 A.2).
- Entities should use private ASNs when interconnecting via Layer 3 on private links (see A.3).
- Entities should use UDP ports greater than 1024 for both source and destination addressing (see A.4).
- 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 ways that an inter-entity connection can be built and configured, as described in this document. The selected architecture 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, are at the discretion of the implementer, but operational testing is recommended to confirm that 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 might become important if the end receiving device is intolerant of large jitter.

Ultimately, it is down to the two entities to agree on the provisioning of each interconnection.

Annex A
(informative)

Additional information

A.1 Separation of traffic types

There are established standards and technologies that cover interconnection of non-linear, data-oriented TCP/IP networks for standard IT traffic, and any such traffic needs to be steered down such networks and not via any trust boundary implementations. Typically, IT firewalls would be deployed at the edge of these bidirectional data networks to control and limit the huge range of ports and data types that TCP/IP data traffic allows.

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

Three 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 as follows:

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 interconnect.

A.3 Use of Autonomous System Numbers (ASNs) in inter-entity L3 connections

Each public facing entity is allocated one or more public Autonomous System Numbers (ASNs) to use when interconnecting to other entities at Internet exchanges. For private connections, such as those described in A.2, use of ASNs in a private range is recommended. See RFC 6996.

A.4 UDP port usage

The IANA Port Number Registry states that ports 0-1023 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.

RFC 8085 Section 5, Paragraph 2 states: "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 must be assessed via a penetration test conducted by CHECK, CREST, or TIGER accredited testers and third parties. The results of such tests must provide evidence that any of the core security functions have been met and could not be circumvented or breached by an adversary.

It is also worth considering the recommendations defined in the EBU security documents listed 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 (informative)

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