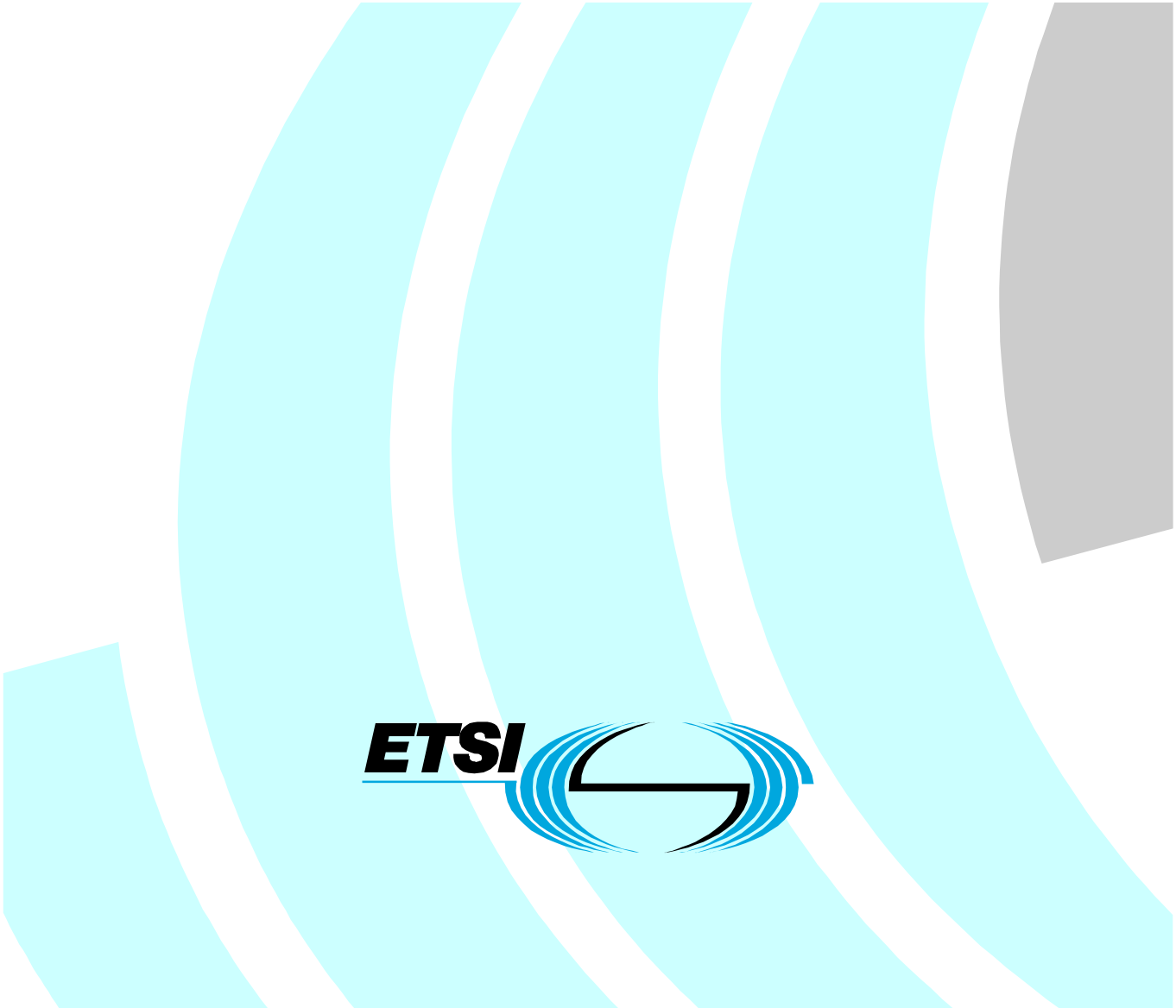
ETSI TS 102 460 V1.1.1 (2006-11)

Technical Specification

Satellite Earth Stations and Systems (SES);
Broadband Satellite Multimedia (BSM);
Address Management at the SI-SAP



Reference
DTS/SES-00100

Keywords
management, satellite, broadband, interworking, IP

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Satellite Earth Stations and Systems (SES).

Introduction

The present document discusses scenarios and architectures to provide address management functions for a BSM.

1 Scope

The present document concerns the address management functions that are required to support interworking of a BSM network with an IP network, including use as part of the general Internet, in particular the address management functions related to the BSM SI-SAP.

The SI-SAP is described in the BSM functional architecture [1] and defined in the SI-SAP specification [3]. A key element in the present document is the BSM_Identifier (BSM_ID) which is the SI-SAP address that identifies the BSM subnetwork point of attachment (SNPA). A BSM network uses the BSM_ID when sending and receiving data via the SI-SAP: the BSM_ID is an abstraction of the lower layer address that would otherwise be used.

The present document describes the relationships between IP Addresses and BSM_IDs and also describes how to create, manage, and query the BSM_IDs for the purpose of sending and receiving user data (in particular IP packets) via the SI-SAP.

NOTE 1: In some systems, requesting to pass traffic across the network also causes reservation of bandwidth. We consider this out of scope and part of QoS, but we will make some assumptions that a notification will be sent a QoS Manager.

The task divides into two parts:

- address management scenarios and architectures;
- unicast address resolution at the SI-SAP.

Lower layer address management (i.e. management of addresses below the SI-SAP) is beyond the scope of the present document.

NOTE 2: Examples of lower layer addresses that are out-of-scope include Data Link layer addresses, MAC layer addresses and Physical layer addresses.

The present document elaborates the details of the address management functions, notably the address resolution function, as defined in the SI-SAP specification TS 102 357 [3]. It also builds on several other reports:

- TR 101 984 (see bibliography);
- TR 101 985(see bibliography);
- TR 102 155 (see bibliography).

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

[1] ETSI TS 102 292: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM) services and architectures; Functional architecture for IP interworking with BSM networks".

[2] IEEE 802 (2001): "IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture".

[3] ETSI TS 102 357 (V1.1.1): "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Common Air interface specification; Satellite Independent Service Access Point SI-SAP".

3 Definitions and abbreviations

3.1 Definitions

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

Address Resolution (AR): provides a mechanism that associates L2 information with the IP address of a system

NOTE: Many L2 technologies employ unicast AR at the sender: an IP system wishing to send an IP packet encapsulates it and places it into a L2 frame. It then identifies the appropriate L3 adjacency (e.g. next hop router, end host) and determines the appropriate L2 adjacency (e.g. MAC address in Ethernet) to which the frame should be sent so that the packet gets across the L2 link.

Address Resolution Protocol (ARP): protocol defined in RFC 826 (see bibliography) that is used to associate network protocol addresses to 48 bit Ethernet addresses for transmission on Ethernet hardware

BSM Address Resolution (B-AR): provides a mechanism that associates a BSM_ID with the IP address of a system

BSM Subnetwork: infrastructure that provides transport services between STs

NOTE: The boundary of the BSM subnetwork corresponds to the SI-SAP in those STs; hence the BSM subnetwork includes elements of the STs, the Gateways and the Satellite.

BSM Network: one BSM subnetwork together with the necessary interworking functions that enable that BSM subnetwork to interwork with one or more attached networks at the STs

BSM_IDentity (BSM_ID): SI-SAP address that defines the BSM Subnetwork Point of Attachment (SNPA)

NOTE: The BSM_ID is divided into BSM Unicast IDs (BSM_UID) and BSM Group IDs (BSM_GID).

BSM Subnetwork Point of Attachment (B-SNPA): SI-SAP endpoint of the BSM data transport services

NOTE: The BSM_ID is used to address data sent to and received from the BSM Subnetwork Point of Attachment.

BSM Bearer service: transport service from one SI-SAP to one other SI-SAP (unicast service); or from one SI-SAP to one or more SI-SAPs (multicast service); within the same BSM subnetwork

dynamically assigned: assigned at a well defined point in an operation, such as at log-in

dynamically assignable: may be reassigned during normal operations

forwarding: process of relaying an IP Packet from a source to a destination through intermediate network segments and nodes

NOTE: The forwarding decision is based on information that is already available in the routing table. The decision on how to construct that routing table is the routing decision - see below.

IP datagram (datagram): IP datagram is identical to an IP packet

IP Packet (Packet): self-contained, independent entity of data that conforms to the IP protocol

NOTE: An IP packet contains sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network.

Network Access Provider (NAP): provides transmission resources to the Service Providers (SP) for accessing their subscribers

Network Address Translation (NAT): process of mapping between a set of IP addresses in one IP network to/from another set of IP addresses in another IP network

NOTE: NAT is defined in RFC 3022 (see bibliography). NAT is typically used to map between internal IP addresses and officially assigned external addresses.

Private IP address: address assigned from one of the IETF defined private addressing blocks

Queue_IDentifier (QID): SI-SAP parameter that identifies an abstract queue at the SI-SAP

NOTE: The QID is used to identify a specific lower layer resource when sending (submitting) data via the SI-SAP.

routing: process of selecting paths for packets to take based on a routing table

NOTE: The routing table can be created through different routing protocols, some of which include automatic discovery.

Satellite Network Operator (SNO): owns and is responsible for maintaining, managing, deploying and operating the Satellite Network (i.e. the BSM network) excluding terminals (STs and Hubs)

SI-SAP Instance (SAPI): specific independent instance of the SI-SAP in one ST

NOTE: A single unicast BSM_ID (UID) is associated with each instance of the SI-SAP (each SAPI). In addition one or more group BSM_IDs (GIDs) may be associated with each instance of the SI-SAP.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AM	Address Management
AR	Address Resolution
ARP	Address Resolution Protocol
B-AR	BSM Address Resolution
BAS	Broadband Access Server
B-DSPC	BSM Dynamic ST Port Configuration
BGP	Border Gateway Protocol
BSM SNPA	BSM SubNetwork Point of Attachment
BSM	Broadband Satellite Multimedia
BSM_GID	BSM Group IDentity
BSM_ID	BSM IDentity
BSM_UID	BSM Unicast IDentity
BSMS	BSM System
CHAP	Challenge HAndshake Protocol
CPE	Customer Premises Equipment
CPN	Customer Premises Network
DHC	Dynamic Host Configuration
DHCP	Dynamic Host Configuration Protocol
DVB-RCS	Digital Video Broadcasting - Return Channel via Satellite
FLSS	Forward Link SubSystem
GID	Group ID
ID	IDentity
IDU/ODU	InDoor Unit/OutDoor Unit
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Providers
L2TP	Layer 2 Tunnelling Protocol
LAA	L2TP Access Aggregation

LAN	Local Area Network
LLC	Logical Link Control
LNS	L2TP Network Server
MAC	Medium Access Control
MPE	Multi-Protocol Encapsulation
MS	Management Station
NAP	Network Access Provider
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NCC	Network Control Centre
ND	Neighbour Discovery
NHR	Next Hop Router
NMC	Network Management Centre
NMS	Network Management System
NOCC	Network Operations Control Centre
OBP	On-Board Process
OSPF	Open Shortest Path First
PAP	Password Authentication Protocol
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet
PTA	PPP Terminated Aggregation
QID	Queue IDentifier
QoS	Quality of Service
RADIUS	Remote Access Dial-In User Service
RAR	Reverse Address Resolution
RARP	Reverse Address Resolution Protocol
RCST	Return Channel Satellite Terminal
RIP	Routing Information Protocol
RLSS	Return Link SubSystem
RSGW	Regenerative Satellite GateWay
SAPI	SI-SAP Instance
SD	Satellite Dependent
SDAF	Satellite Dependent Adaptation Functions
SDU	Service Data Unit
SI	Satellite Independent
SIAF	Satellite Independent Adaptation Functions
SI-SAP	Satellite Independent Service Access Point
SLA ID	Site-Level Aggregation IDentifier
SME	Small and Medium Enterprise
SNHA	Satellite Next Hop Address
SNO	Satellite Network Operator
SOHO	Small Office - Home Office
SP	Service Provider
SPC	ST Port Configuration
ST	Satellite Terminal
UID	Unicast ID
VPN	Virtual Private Network

4 Scenarios and service requirements

The task of an ST is to forward IP packets over a BSM network to the next hop node as part of the process of forwarding the IP packet to the final destination Host for which the IP packet is intended. There may be alternative routes over the satellite network to provide link diversity or to increase the overall capacity of the satellite link.

The unicast scenario concerns a point to point link, either one-way or two way. The associated BSM Bearer Service topology can be a mesh such that two STs exchange user data directly, or a star such that the user data passes via a gateway.

Control and management information, corresponding to the C and M planes of the SI-SAP, would normally pass through a Network Control Centre (NCC) even if the user data is passed directly between STs. Systems with distributed control and management systems, i.e. where C and M plane data does not pass through the NCC, can be built but this architecture is not considered further in the present document.

4.1 Address Management (AM)

By definition (see TR 102 155 in bibliography) a BSM network is designed to transport IP packets and provides, as a minimum, the address management services required to support IP forwarding from a source BSM network node (or ingress ST) to a destination BSM network node (or egress ST).

The present document focuses on unicast address management, but the some of these functions may also be applicable to multicast address management.

This clause specifies the IP address management services required in different scenarios. In a satellite network, IP address management services are closely associated with resource management (see TR 102 155 in bibliography) and excessive traffic over the satellite network must be avoided.

NOTE 1: In the context of the present document, address management does not include any routing functions and IP routing protocols (e.g. RIP, OSPF, BGP) are not considered further in the present document.

It is assumed that protocol layers are independent and thus layer 2 addresses may be managed independently of layer 3 addresses.

NOTE 2: Layer 2 addresses may be derived from the layer 3 addresses in some cases. For example, RFC 1112 (see bibliography) defines how layer 2 group addresses may be directly derived from Layer 3 multicast addresses.

BSM IDentifier (BSM_ID) is a general term that includes both Unicast and Group Identifiers. Above the SI-SAP, BSM_IDs are associated with IP (Layer 3) addresses and below the SI-SAP BSM_IDs are typically associated with MAC (Layer 2) addresses. More specifically, the BSM Unicast ID (BSM_UID) is associated with Unicast addresses while the BSM Group Identifier (BSM_GID) is associated with multicast addresses.

As shown in figure 4.1, Address Management is used to coordinate the requirements for managing the addresses that are used for transporting user data between the ISP/Customer, Network Access Provider and Satellite Operator.

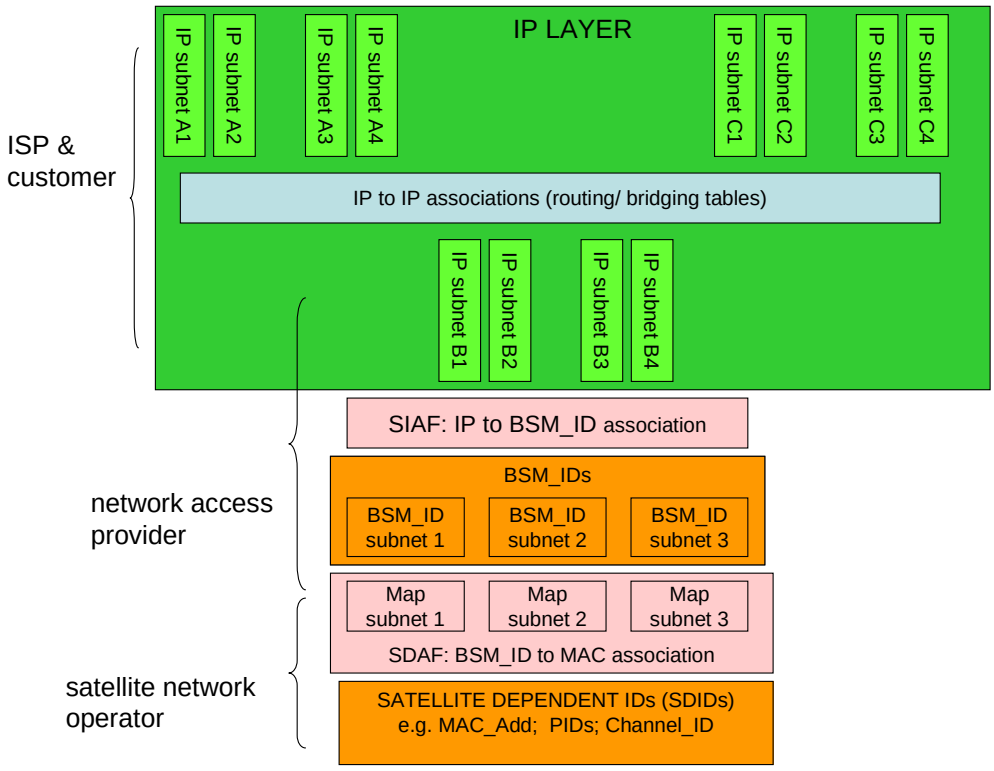


Figure 4.1: BSM Address Management layers

4.2 Address Management functions

4.2.1 IP layer Address Management functions

Figure 4.2 shows the BSM network as the middle network of three concatenated IP networks (A, B, C). In this example, the IP networks A and C are external local area networks or wide area networks, and the IP network B is the BSM Network. The IP networks A and C could be the Internet, a corporate internet, corporate intranet, a SOHO network or any enterprise network that needs to use the BSM network as an access network. Address Management will support functions consistent with IP forwarding between IP networks A and C via the BSM network.

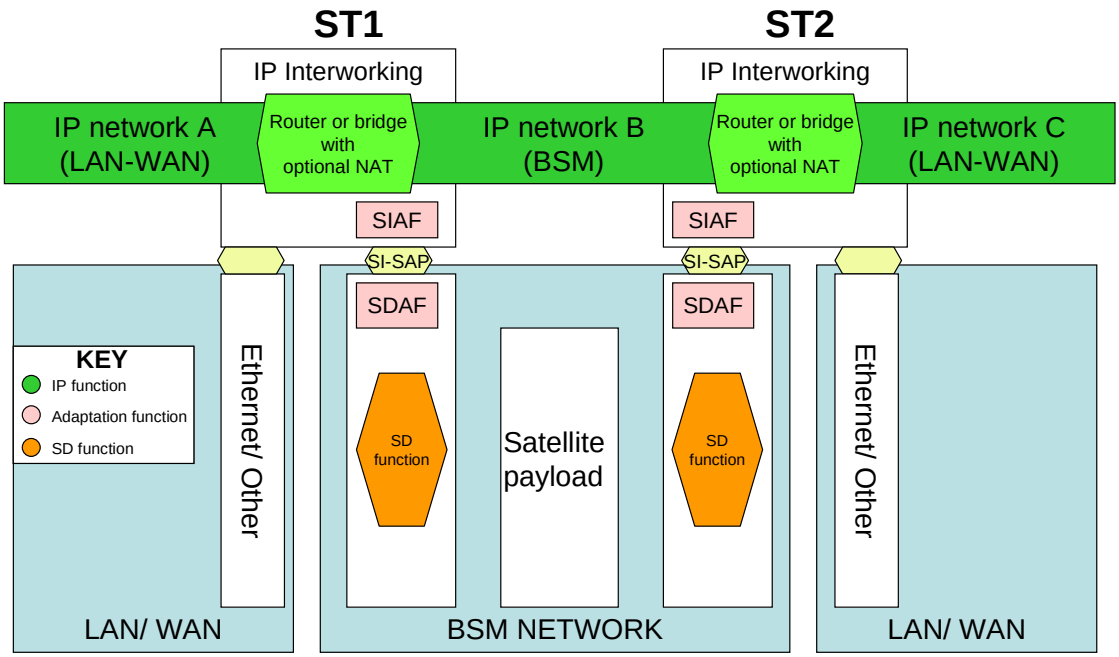


Figure 4.2: A BSM network and interworking with other IP networks

The present document considers two different cases of IP interworking within the ST:

a) **ST/ Router**: In this case, the ST interconnects the networks at the IP layer and routes IP packets between the different attached networks.

b) **ST/ Bridge**: In this case, the ST interconnects the networks at the subnetwork interface level and forwards frames between these interfaces.

NOTE: A bridge is independent of the higher layer protocol: i.e. transparent to the IP packets.

These different cases are described in more detail in annex A for the Access Network scenario.

Both customer facing and satellite facing interfaces can use either private IP addresses or globally unique IP addresses. In general, the customer facing and satellite facing ports of a given ST will have different network address ranges and to accommodate this, NAT may be required as part of the ST IP layer.

NAT can be used as part of the ST/Router case to translate between different address ranges. For example, NAT could be used to allow IP network A and/or IP network C to operate with private addresses. As a second example, NAT can allow IP network A and IP network C to have the same network addresses and may also be required because of a customer's privacy requirements as illustrated by annex D. There are several potential problems when using NAT (see for example the problems described in RFC 1631 (see bibliography)) and these problems may apply in the BSM network.

Thus the BSM Address Management IP layer services that may be required are:

- **Address Resolution (AR):** finding the next hop BSM_ID that is associated with a given next hop IP address;
- **Reverse Address Resolution (RAR):** finding the next hop IP address that is associated with a given next hop BSM_ID;
- **ST Port Configuration (SPC):** providing some autoconfiguration of the ST satellite facing port;
- **Network Address Translation (NAT):** mapping of IP addresses within the ST.

Later we will look into the infrastructure needed to support these four AM services.

4.2.2 BSM_IDs

The BSM_ID is an SI-SAP address that identifies the BSM subnetwork point of attachment (SNPA).

Each ST in the system will have one BSM_UID, associated with the SI-SAP. STs that provide a gateway function, and the Hub ST in a star network May have multiple SI-SAP instances and can therefore have one or more BSM_UIDs (one per SI-SAP). In all cases, the BSM_UID will be associated with one IP address above the SI-SAP and with a MAC address below the SI-SAP. Each SI-SAP may also be associated with zero or more BSM_GIDs.

The SI-SAP [3] specifies that the format for the BSM_ID shall be a 48 bit address (6 octets) that conforms to the IEEE 802 [2] specification for LAN MAC addresses.

4.2.3 Access network scenarios

The present document is concerned with access network scenarios. In this case, a BSM network allows the user host equipment to be directly connected to a ST or indirectly connected to a ST via a private LAN. The BSM network then acts as an Access network to provide:

- Access to one or more Internet Service Providers (ISP) network, that in turn will provide access to the Internet,
- Access to a Corporate Network (this includes linking sections of a corporate network).

Table 4.1 summarizes the types of services that can be offered based on unicast access.

Table 4.1: Types of services for consumers and SME/SOHO

Type of User	Internet Access	Corporate Access
Consumer and SOHO	Any Internet based services	Teleworking Corporate Intranet access
Corporate	Any Internet based services	Central Office access Corporate Intranet access

The network reference architecture is shown in figure A.1. It should be noted that the same network architecture supports connections to both ISP and Corporate Networks. The central element of this architecture is an Access Router or Broadband Access Server (BAS) which interconnects the Hub with external networks. The Satellite Network provides the following access services:

- IP Routing architectures:
  - Routed IP mode.
  - PPPoA router mode.
  - DHCP router mode.
- IP Bridging architectures:
  - Bridged mode.

See annex A for detailed examples illustrating this topic.

4.3 Service requirements

It is assumed that:

1) an ST has at least two IP addresses, one facing the customer network and one facing the BSM Network;

2) these IP addresses (i.e. both the customer facing IP address and the satellite facing IP address) can be either a private IP addresses or globally unique IP addresses;

3) the ST satellite facing IP address must be unique within the BSM network;

4) the IP addresses of the ST can be static and fixed through an ST internal configuration or dynamic and allocated when the ST starts;

5) NAT may be used in the ST, gateway or both.

5 Unicast architecture requirements

5.1 General requirements

A common architecture is essential for all BSM STs (see TR 102 157 in bibliography) in order to ensure their interoperability. This architecture must support the AM services discussed in clause 4. The address management functional architecture shall conform to both the BSM functional architecture [1] and the SI-SAP specification [3].

The architecture requirements include:

- the need for AM services to function by passing Address Management Primitives across the SI-SAP, thus forming an API, and messages between the BSM client and server as defined in the BSM architecture [1];
- the use of a client server architecture to provide scalability and integration into existing management structures;
- the need to interwork with IP functions dealing with address management at or below the network layer; this will ensure that the BSM function will evolve with IP protocols;
- the need to minimclause address management related traffic over the satellite link to avoid wasting satellite resources and the effects of the satellite link delay.

The unicast AM services should support all types of unicast IP packet forwarding:

- Host via ST, via BSM Network, to host via gateway.
- Host via ST, via BSM Network, to host via ST.
- Host via gateway, via BSM Network, to host via ST.

In addition, some distributed AM services may be required. To support this, the architecture should support the following elements:

- storage of AR tables (i.e. next-hop neighbour AR caches) at each ST;
- transfer of AR tables between the AR Server and the AR Clients;
- optional NAT at each ST (this includes both user/access STs and gateway STs).

5.1.1 Management of BSM_IDs in an NCC

The management of BSM_IDs involves at least two parties, a Satellite Network Operator (SNO) and a Network Access Provider (NAP) as defined in the BSM Services and Architectures (see TR 101 948 in bibliography). An SNO owns and is responsible for maintaining, managing, deploying and operating the BSM network excluding STs and gateways. A NAP provides transmission resources to the Service Providers (SP) for accessing their subscribers.

Adopting this model the following rules apply:

1) The SNO shall have responsibility for BSM_ID management over the entire BSM Network and shall therefore set the policy for allocation of BSM_IDs. In particular, the SNO shall be responsible for ensuring that the uniqueness rule is met.

2) The NAP shall be responsible for BSM_ID management over its subset of the BSM Network. The NAP shall allocate individual BSM_IDs to STs and shall also define the rules for managing the associated satellite network IP addresses.

5.1.2 Relating BSM_IDs to a BSM Network

Some address management functions could be implemented above, below or both above and below the SI-SAP. For reference, the BSM protocol stack, reproduced from TS 102 295 (see bibliography), is shown in figure 5 1. Address Resolution primitives pass across the SI-SAP in the C-plane.

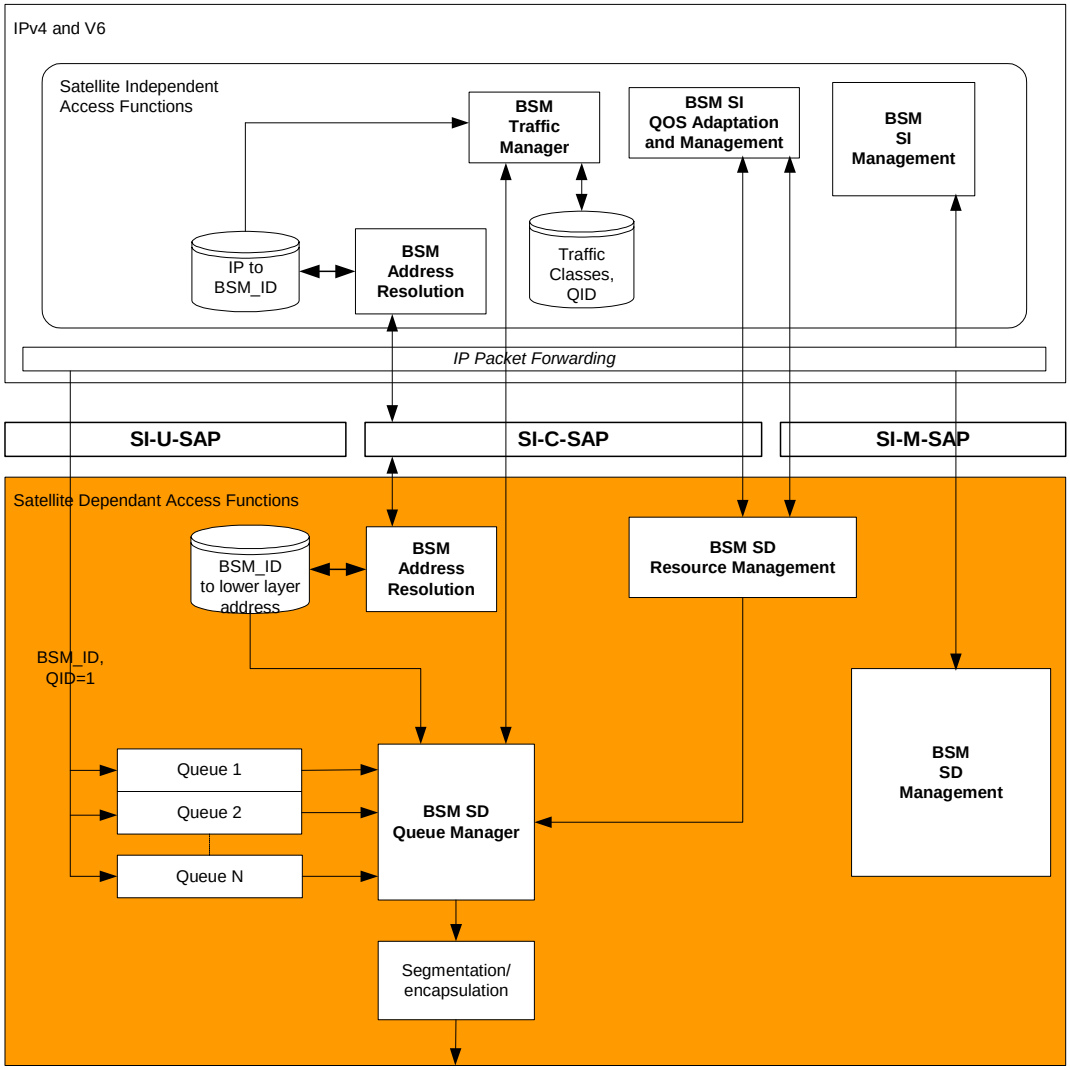


Figure 5.1: BSM protocol stack

5.1.3 BSM Address Resolution (B-AR)

BSM Address Resolution (B-AR) is defined as the function that associates a BSM_ID with the corresponding IP Address.

Address resolution includes functions both above and below the SI-SAP. Above the SI-SAP it is necessary to associate an IP address to a BSM_ID. Below the SI-SAP it is necessary to associate a BSM-ID to a lower layer address, typically a MAC address.

The BSM Architecture must provide a service where AR is supported for B-AR clients in all STs by a central B-AR server. In this content, STs includes both the Gateways (typically the Hub for a Star network) and remote STs. Each ST should also have an AR table as part of the B-AR client .

The B-AR server could, in principle, be located anywhere but it is realistic to assume that is under the control of the BSM operator since it needs knowledge of the BSM address space. Typically, the B-AR Server will be located at a Gateway or at the NCC. Having the B-AR server located at the NCC may be appropriate if the AR function is used to support traffic management, i.e. allowing and denying IP packets access to the BSM network.

B-AR is a C-plane function (see TR 102 353 in bibliography). However, two distinct processes are required for AR to function. Above the SI-SAP, a BSM_ID must be associated with an IP address. Below the SI-SAP, a BSM_ID is associated with a MAC address. The BSM_ID must be resolved to a MAC address whenever an IP packet has to be transmitted by the lower layers; this is also usually a static or pseudo static process. The process of association can store pairs of values in a table, as is the case with entities using AR over wired networks such as Ethernet. The process of resolution can examine the table, usually stored at the location where resolution occurs. Mechanisms are required to populate and update the local tables that store the associations. Updates to a local table will normally be performed by periodically transferring data from a central, or reference, table. The transferred data will either replace or enhance local data. It is highly desirable to minimclause the flow of B-AR data traversing the satellite link.

B-AR may be used whenever an IP packet is to be forwarded to a new destination across a BSM network. The BSM_ID of the next hop must be determined for the packet to be forwarded, and B-AR must be used if the BSM_ID for a given next hop IP address is not already known at that ST. There are three cases:

- star network inbound: all IP addresses resolve to the hub gateway BSM_ID. The BSM_ID associated with the hub gateway is either acquired at ST startup as part of Configuration Management by the NCC or it is pre-programmed;
- star network outbound: IP addresses resolve to specific BSM_IDs. IP address resolution may require policy decisions in connection with access management. An OBP Satellite that performs layer 2 switching may need an AR table that is at least partially managed by the B-AR server;
- mesh network: IP addresses resolve to specific BSM_IDs. IP address resolution may require policy decisions. An OBP Satellite that performs layer 2 switching may manage an AR table itself or it may be managed by the B-AR server.

In all cases a B-AR client at the sending side performs address resolution. In the first instance this should use the cached entries in the local AR table, but if there is no match the ST sends an address resolution request to a B-AR server whose address is acquired dynamically or is pre-configured.

NOTE: In contrast to Ethernet ARP a B-AR client should never send a broadcast message over the satellite link (this may not be possible in any case) and should use the address of the known B-AR server.

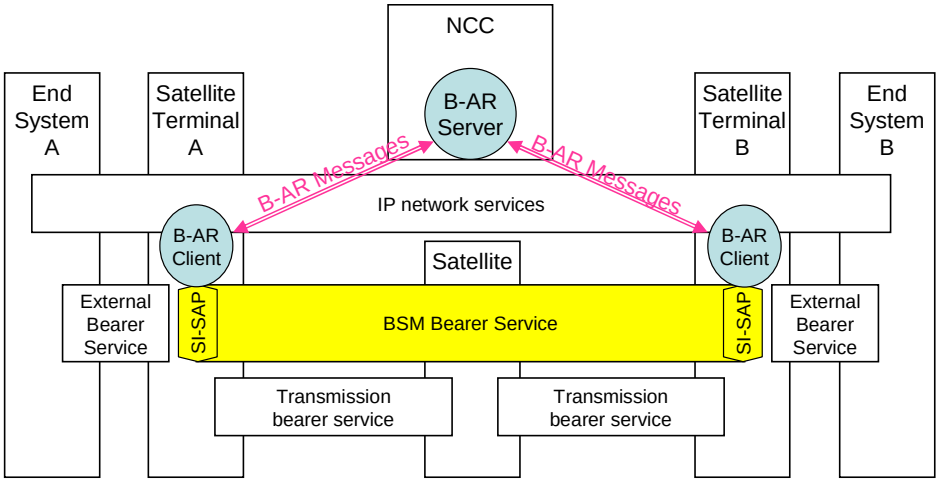


Figure 5.2: BSM AR Architecture

5.1.4 BSM Reverse Address Resolution (B-RAR)

BSM Reverse Address Resolution (B-RAR) is defined as the function that associates an IP Address with a given BSM_ID.

The corresponding wired protocol (Ethernet RARP) is now a historic (obsolete) protocol that is superseded by BOOTP; and both protocols are mostly replaced with DHCP which provides more functionality. Accordingly, it is recommended that B-RAR should not be defined for use in BSM networks and this function is therefore not elaborated further in the present document. Instead B-DSPC (as defined in clause 5.1.5) should used to provide similar functions to DHCP.

5.1.5 BSM Dynamic ST Port Configuration (B-DSPC)

B-DSPC is the process that is used to dynamically configure the satellite facing ports of STs, in particular to allocate IP addresses to these ST ports to enable them to access the satellite network.

NOTE: The equivalent function to DHCPv4 (see RFC 2131 in bibliography) for IPv4 hosts is required. Alternative functions such as DHCPv6 and ND/SEND for IPv6 hosts may also be required.

The BSM network may also be concerned with configuration of the IP address in the attached networks, as well as the configuration of the BSM satellite network IP addresses. Potential configurations are:

a) Local LAN configuration: This refers to configuration of a single local network. Typically this would be used to manage the local LAN IP addresses of the network attached to an ST (e.g. via an embedded DHCP server in the ST), This is external to and invisible to the BSM network.

b) Distributed LAN configuration: The refers to co-ordinated configuration of multiple customer premises networks, each attached to different STs, and linked together via the BSM satellite network. There are two subcases:

   1) Distributed Corporate LAN: This is used to manage LAN IP addresses within a corporate LAN, but the segments of that LAN may be at separate locations (geographically separate) and connected via a BSM network. Simply using standard DHCP could generate excessive DHCP traffic over the BSM and hence there is need for DHCP proxy servers and/or adaptation in each of the separate sites to prevent DHCP traffic from traversing the satellite network unless of specific need (e.g. the unavailability of the local DHCP proxy server) . This is still largely external to BSM and can use standard DHCP proxies/relays (see RFC 3046 in bibliography).

   2) ISP LAN configuration: This is where the ISP offers a service over the satellite network that uses L3 configuration, specifically IP address configuration using a method that is carried transparently over the satellite network (e.g. PPPoE, Bridging or VPN with DHCP. These protocols are required to operate over a satellite link (delay etc) and may require adaptation and DHCP proxies/ relays (see RFC 3046 in bibliography).

c) Satellite network configuration using B-DSPC: This is where a satellite specific protocol (B-DSPC) is used to manage the satellite facing IP addresses via a B-DSPC client in the ST and a B-DSPC server. The B-DSPC Server may be managed by either the SNO or the NSP.

All of these configurations are permitted and the choice will be network dependant.

This use of B-DSPC to configure the satellite network ports is illustrated in figure 5.3 for the case of an access network.

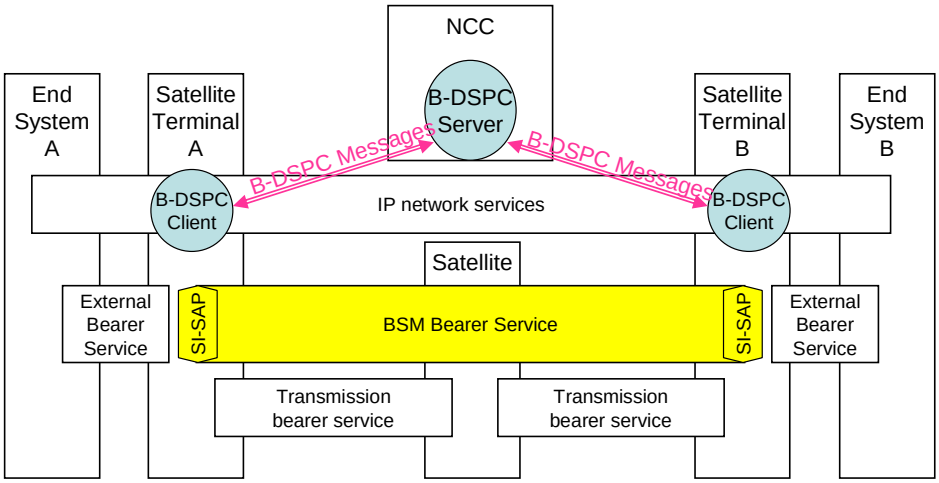


Figure 5.3: BSM B-DSPC Architecture

B-DSPC messages are exchanged between the B-DSPC clients in the STs and the B-DSPC Server, typically located in the NCC.

5.1.6 Network Address Translation (NAT)

As defined in clause 4, the Hosts connected to an ST (i.e. the Hosts within the customer premises network) can have globally unique IP addresses, or private IP addresses.

If the Hosts within the customer network use private IP addresses, but want to exchange IP packets with another private network; or want to send or receive IP packets via the Internet then Network Address Translation (NAT) will be required. Not all applications operate with NAT and non-standard workarounds may be required.

When handling ingress IP packets, the IP packets must be NATed first in order to have a BSM network IP address for transporting them through the BSM network. For egress handling, the packet must first be NATed into the next IP address and then the egress router functionality can be applied.

Three NAT cases can be considered:

1) the ST acts as a router with NAT or NAPT. Network Address and Port Translation (NAPT) is required if multiple STs appear to the BSM internal network to share a single IP address;

2) the ST acts as a bridge without NAT;

3) the ST acts as a router without NAT.

Annex A (informative): Internet access scenarios

This contribution presents some possible IP networking scenarios for providing internet access. Only unicast Internet access services are considered here.

In the first part of this annex we give a general presentation of Access Services which cover both Internet access but also VPN access. Then four typical Internet access scenarios are described, highlighting the addressing and routing configurations used.

A.1 Unicast access services

A BSM network allows a user directly connected to a Terminal or indirectly connected to a Terminal via a private LAN to:

- Access one Internet Service Providers (ISP) Network, that in turn will provide access to the Internet,
- Access a Corporate Network using a Private Network.

Subscribers can be either consumers or SOHOs or SMEs. Table A.1 summarclauses the types of services that can be offered based on unicast access.

Table A.1: Types of Services for Consumers and SME/Soho's

Type of User	Internet Access	Corporate Access
Consumer and SOHO	Any Internet based services	Teleworking Corporate Intranet access
Corporate	Any Internet based services	Central Office access Corporate Intranet access

The network reference architecture is shown on figure A.1. It should be noted that the same network architecture supports connections to both ISP and Corporate Networks. The central element of this architecture is an Access Router or Broadband Access Server (BAS) which interconnects the Hub with external networks. The Satellite Network provides the following access services:

- Routed IP mode.
- Bridged mode.
- PPPoA router mode.
- DHCP router mode.

These are the services usually found in DSL networks. This allows re-using protocols, equipment, management and business models which are already widespread in the access and service providers' market.

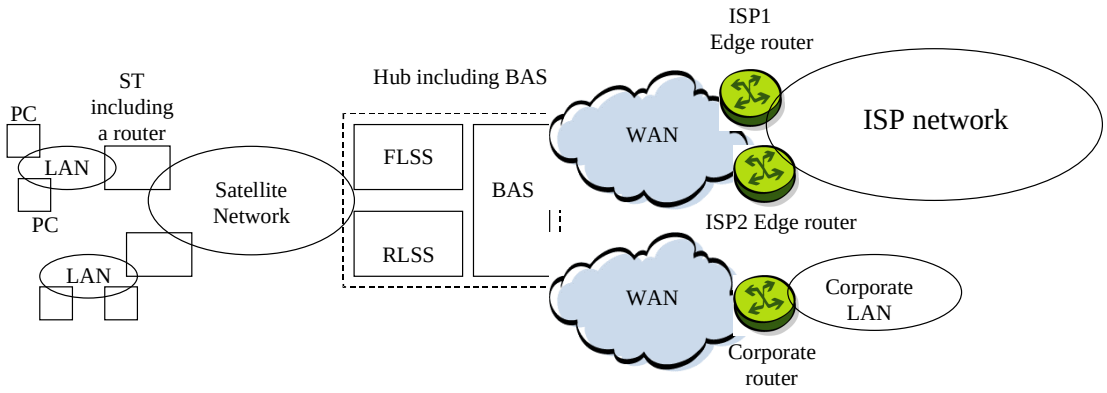


Figure A.1: BSM TSS-A1 as an Access solution

Table A.2 identifies the subscriber access modes supported by the system, and detailed in the following clauses.

Table A.2: Subscriber access modes

Access modes	Encapsulation	IP address assignment	Subscriber Management	Subscriber AAA methods
Routed IP mode	IP over ATM (IPoA)	Static	Hourly-based volume tracking	None (only the ST is authenticated at logon phase)
Bridged mode (CPE includes a PPPoE client)	PPP over Ethernet over ATM (PPPoEoA)	Dynamic through the IPCP protocol part of the PPP protocol stack	Per-PPP session volume tracking and time tracking	PAP or CHAP
PPPoA router mode	PPP over ATM (PPPoA)	Dynamic through the IPCP protocol part of the PPP protocol stack	Per-PPP session volume tracking and time tracking	PAP or CHAP
DHCP router mode	IP over Ethernet over ATM (IPoEoA)	Static or dynamic through DHCP	Hourly-based volume tracking	ST MAC address control (ST as a Router) or Subscriber Computer MAC address control (ST as a Bridge)

A.2 Routed IP access mode

A.2.1 Service architecture

This access mode enables a routed IP access service of a Subscriber LAN toward one SP backbone IP network. The SP can in turn provides Internet Access through its IP network. Both the ST and the BAS acts as IP routers. The IP address of the Satellite WAN interface of the ST can only be statically assigned.

A.2.2 Service characteristics

One Subscriber is linked to only one SP for all the contract duration. The System allows for multiple SPS connected at the Hub. Thus, a Subscriber has to select one SP among several and will be linked to the selected SP during the contract duration.

The ST acts as an IP Router:

- The IP address of the WAN IP interface is statically assigned due to the use of Classical IP over a permanent ATM VC. The PVC is a point-to-point link where an endpoint must know the IP address of the peer endpoint.
- The IP address of the LAN IP interface is also statically assigned. When the ST is configured with NAPT enabled, this interface may host a DHCP server for distributing private addresses to the LAN Computers. These LAN Computers will thus share the Internet Access using the single WAN interface public IP address.

When NAPT is disabled, the ST might route IP packets toward multiple subnets behind the LAN subnet itself thanks to a routing table that supports multiple static routing entries.

A.2.3 Service protocol stack

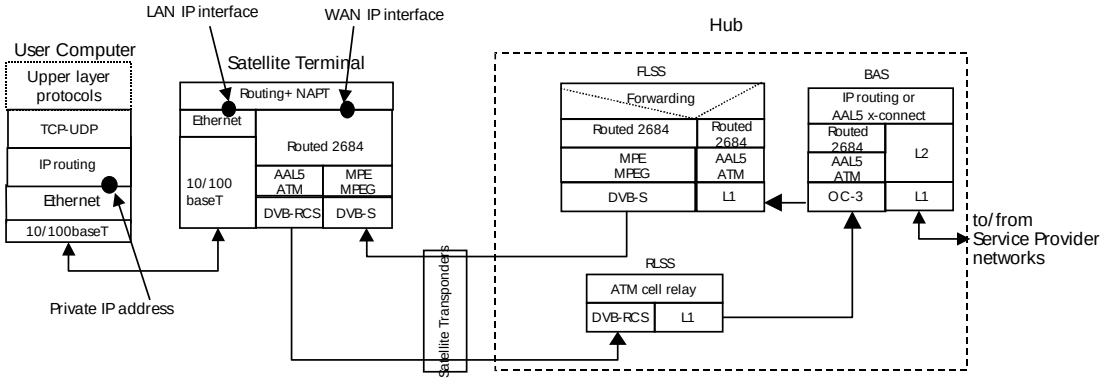


Figure A.2: Protocol stack for Routed IP mode

For the Routed IP mode, the System supports the encapsulation of IP either using VCmux or LLC. But in order to reduce at maximum bandwidth consumption, the VCmux method is strongly recommended.

A.2.4 Customer Premises configurations for Internet Access

A.2.4.1 Multi-computers LAN with its own internal private IP addressing

In this case, the Subscriber wants to keep the current private IP addressing plane of its LAN but still wants Internet access with some firewalling features.

This can be done by enabling the NAPT function of the ST. Figure A.3 shows an example of addressing configuration.

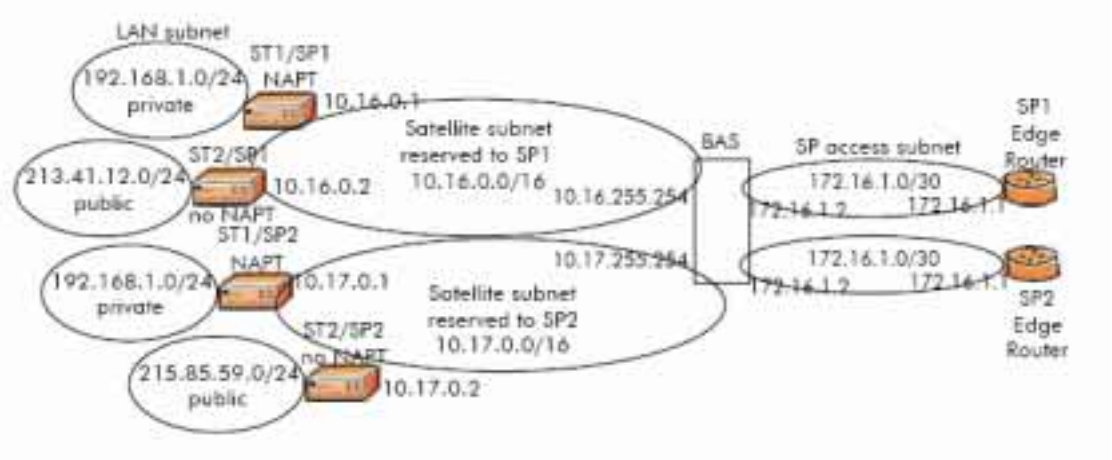


Figure A.3: IPoA Internet Access

A.3. Bridged access mode

A.3.1 Service characteristics

In bridged mode, the protocol used to connect the end-user CPE and the ISP is PPP instead of IP. As the LAN interface of the ST is Ethernet, the transport protocol between the end-user CPE and the Hub is PPP over Ethernet (PPPoE). With PPPoE, an Ethernet virtual private line is created between the end-user CPE and the Hub in order to carry the PPP session. PPP provides the following features:

- Dynamic IP addressing: the IP address is assigned dynamically using the PPP protocol in conjunction with the IPCP protocol. The IPCP selects an IP address from a pool of public addresses whenever a PPP session starts. The IP address is given back to the pool at the release of the PPP session.
- End-user authentication and authorization using PAP/CHAP protocols and the IPCP negotiation function.
- End-user accounting: with PPP, it is possible to offer time-based and volume based accounting in addition to traditional flat fee accounting.

PPPoE access services are "dial-up", i.e. the connection is established between the end-user CPE and its ISP through the satellite network at PPP session start and the user will stay connected as long as the session is not terminated. This time frame can be long enough in order that the user perceives the PPPoE access service as "always-on".

A.3.2 Service protocol stacks

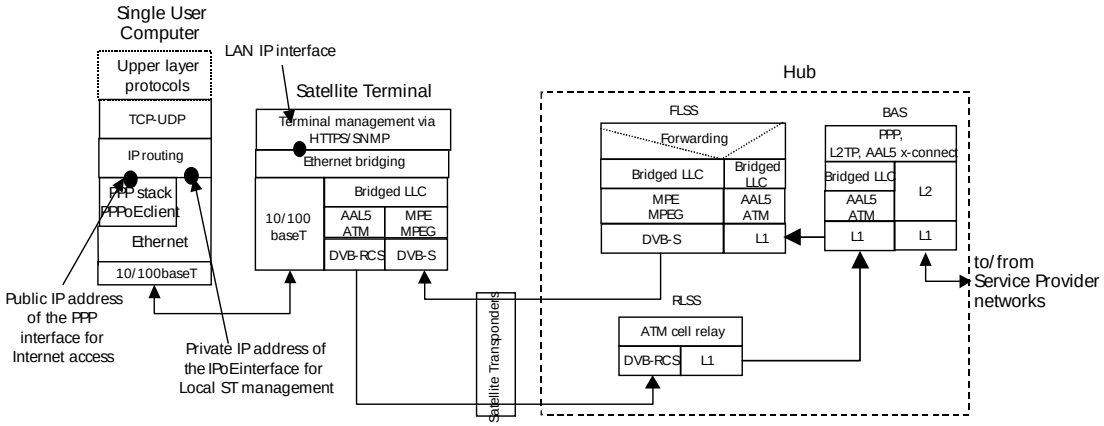


Figure A.4: Protocol stack for the bridged mode

In bridged mode, the networking functions are supported by the following elements:

- The CPE is responsible to initiate the PPP session. The CPE can be a PC or a router. The CPE or router therefore needs to include a PPPoE client. A CPE can initiate simultaneously several PPP sessions (for example to access at the same time the Internet and a Corporate network while keeping a logical independence between the two accesses).
- The ST acts as an Ethernet bridge. It transmits/receives the PPPoE frames from its Satellite interface. It can transport simultaneously several PPPoE sessions.
- The BAS supports both the "PPP open model" where the BAS forwards the end-user PPP sessions up to the requested ISP and the "PPP closed model" where the BAS terminates the subscriber PPP sessions and then routes the IP traffic to/from the relevant ISP. A third model is called "AAL5 cross-connect" where the BAS acts like an ATM cell relay from/to the relevant ISP's BAS.

A.3.3 Hub configuration

Depending on each Service Provider requirements in term of Subscriber management, Subscriber PPP sessions might be handled differently at the Hub. In particular, if a SP only wants to receive Subscriber IP traffic from the Hub, the BAS will work in PPP termination mode. If the SP wants to finish Subscriber PPP sessions at its Network Premises in order to have more accurate subscriber management, the Hub BAS may work either in LAC (L2TP Access Concentrator) mode or PVC cross-connect mode.

A.3.3.1 PPP Terminated Aggregation (PTA) mode

In this case, the BAS finishes the PPP session of each Subscriber, recovers the IP packets and routes them according to the SP routing configuration. Authentication and accounting is initiated by the Hub that acts as a RADIUS client toward the SP RADIUS server.

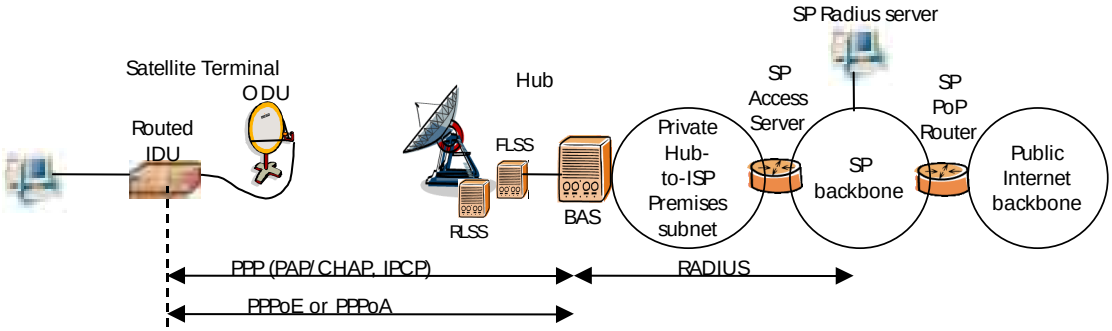


Figure A.5: PPP Terminated aggregation mode

A.3.3.2 L2TP Access Aggregation (LAA) mode

In this mode, the BAS acts as a L2TP Access Concentrator (LAC) and does not finish Subscriber PPP sessions but forwards them toward the right SP L2TP Network Server (LNS). This allows the SP to get a fine control of the Subscriber PPP session and avoid the transport of critical/internal information over the ground network between the BAS and the SP Premises.

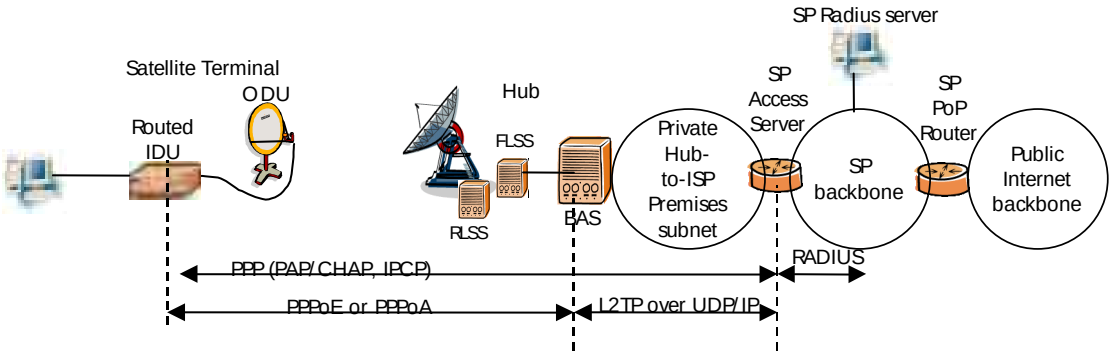


Figure A.6: L2TP Access Aggregation mode

A.4. PPP router mode

In the PPP router mode, the ST is configured as a router with NAPT enabled: this allows multiple Computers on a private LAN to share the single PPP session toward the SP. Such sharing of a single public IP address by multiple Computers with private IP addresses is entirely done by the NAPT (Network Address and Port Translation) function of the ST. On the user LAN, the addressing can be either static where the Subscriber manually configures each computer or can also be dynamic by using a DHCP server embedded in the ST and bound to the LAN IP interface.

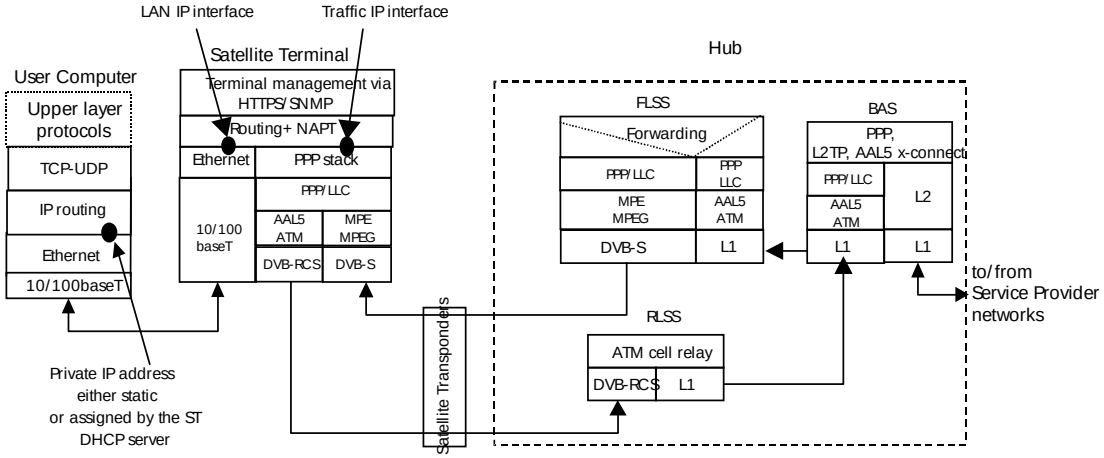


Figure A.7: Protocol stack for PPPoA Router access mode

As for the bridged access mode, three cases of ISP interconnection can be envisaged: PPP open model, PPP closed model and AAL5 cross connect model, as presented in figures A.8 and A.9.

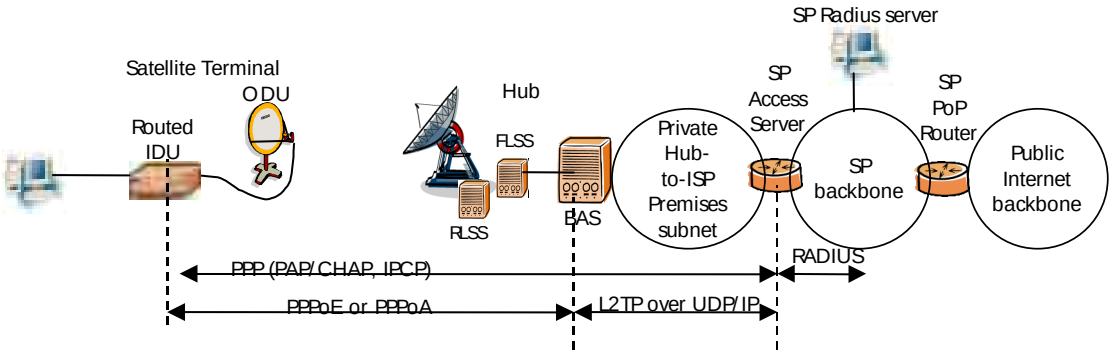


Figure A.8: PPP router access mode with Gateway in PTA mode

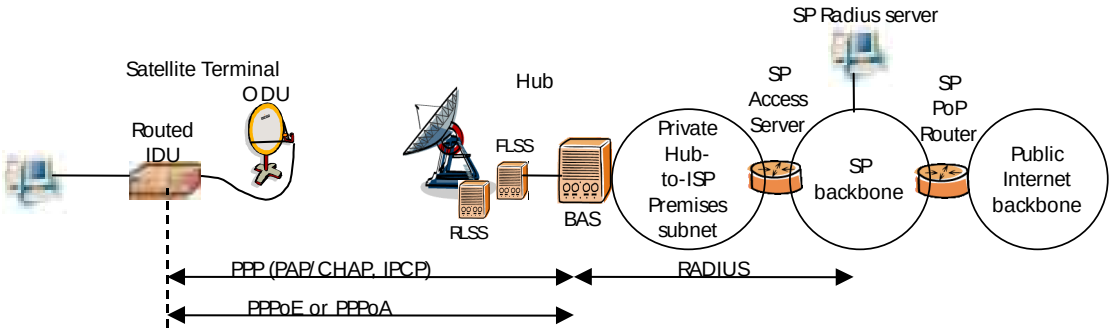


Figure A.9: PPP router access mode with Gateway in LAA mode

A.5 DHCP router mode

A.5.1 Service presentation

The DHCP router mode enables a routed IP access service of one LAN toward one SP backbone IP network. The DHCP protocol provides configuration parameters to Internet hosts. DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for allocation of network addresses to hosts.

In this mode, the ST acts as an IP router. Its WAN IP address is dynamically assigned via DHCP (RFC 2131, see bibliography). Thanks to the Ethernet layer between IP and ATM, the DHCP client is able to automatically detects a DHCP server managed by the SP (through a DHCP relay or not). This is the advantage of the DHCP router mode compared to the Routed IP mode. The IP address of the LAN IP interface of the ST is statically assigned. Since the ST is configured with NAPT enabled, this interface hosts a DHCP server for distributing private addresses to the LAN Computers. These LAN Computers will thus share the Internet Access using the single WAN interface public IP address retrieving through DHCP.

A.5.2 Service characteristics

One Subscriber is linked to only one SP for all the contract duration. The System allows for multiple SPS connected at the Hub. Thus, a Subscriber has to select one SP among several and will be linked to the selected SP during the contract duration.

The ST acts as an IP Router:

- the IP address of the WAN IP interface is either statically assigned or dynamically assigned by activating a DHCP client bound to this WAN IP interface. Thanks to the Ethernet layer between IP and ATM, the DHCP client is able to automatically detects a DHCP server managed by the SP (through a DHCP relay or not).
- the IP address of the LAN IP interface is statically assigned. When the ST is configured with NAPT enabled, this interface may host a DHCP server for distributing private addresses to the LAN Computers. These LAN Computers will thus share the Internet Access using the single WAN interface public IP address retrieving though DHCP.

When NAPT is disabled, the ST might route IP packets toward multiple subnets behind the LAN subnet itself thanks to a routing table that supports multiple static routing entries.

A.5.3 Service protocol stacks

Figure A.10 presents the protocol stack for the DHCP router mode.

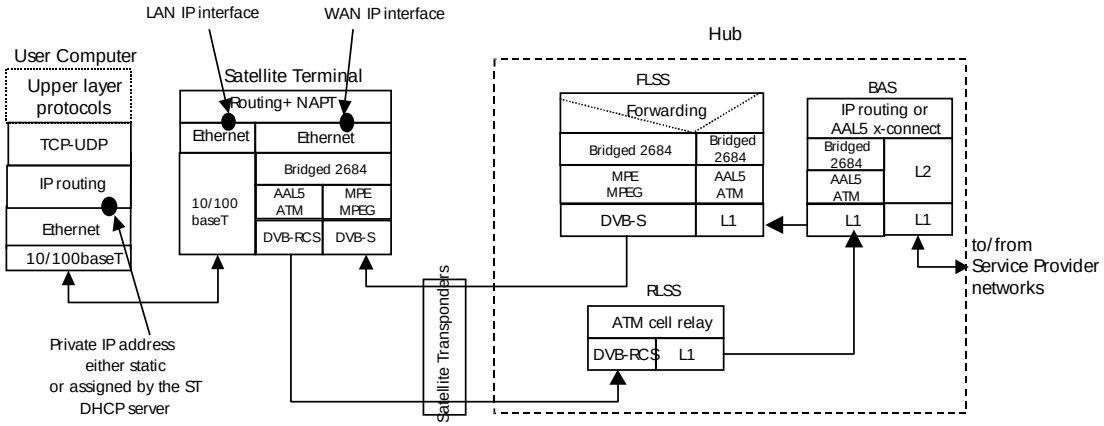


Figure A.10: DHCP router mode protocol stacks

Annex B (informative): Address Management network topology

B.1 Address Management SI-SAP model

A definition of the Address Management network topology will help to define some of the requirements, functions, and scenarios. For a BSM network, all IP packets pass through a Satellite Terminal (ST).

The ST Address Management is based on the SI-SAP architecture defined in TS 102 292 [1] and reproduced in figure B.1.

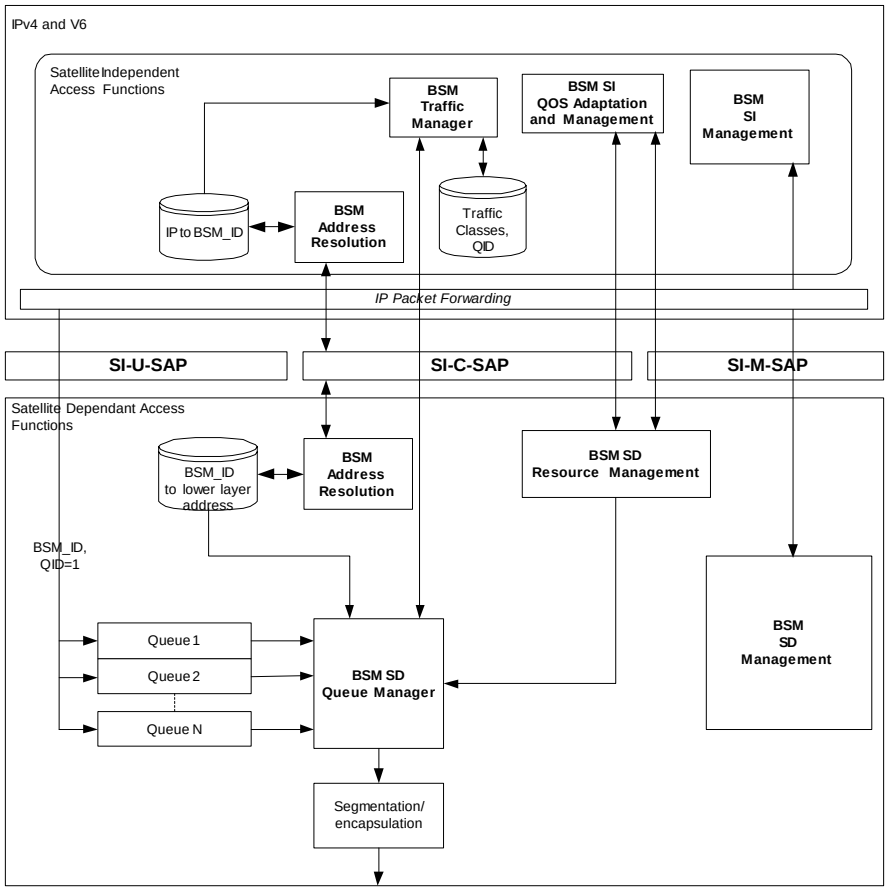


Figure B.1: ST SI-SAP model

Figure B.1 shows a logical ST and generally how IP packets cross vertically from the IP layer to the satellite dependent lower layers. Concentrating on the Address Resolution functions above and below the SI-SAP, each of these elements has a "cache" associated with it. At the SIAF layer, BSM Address Resolution involves associating a next-hop IP address with the corresponding next-hop BSM_UID.

Address management is concerned with the BSM_IDs that are needed by any given BSM network and how they are used to forward IP datagrams from one SI-SAP point of attachment to another including mapping BSM_IDs to MAC addresses, sets of addresses for translation, and the next-hop destination addresses (both BSM_ID and IP addresses).

B.2 BSM network models

Figure B.2 shows the customer premises network, the BSM Network, and the BSM SI-SAP and BSM Subnetwork.

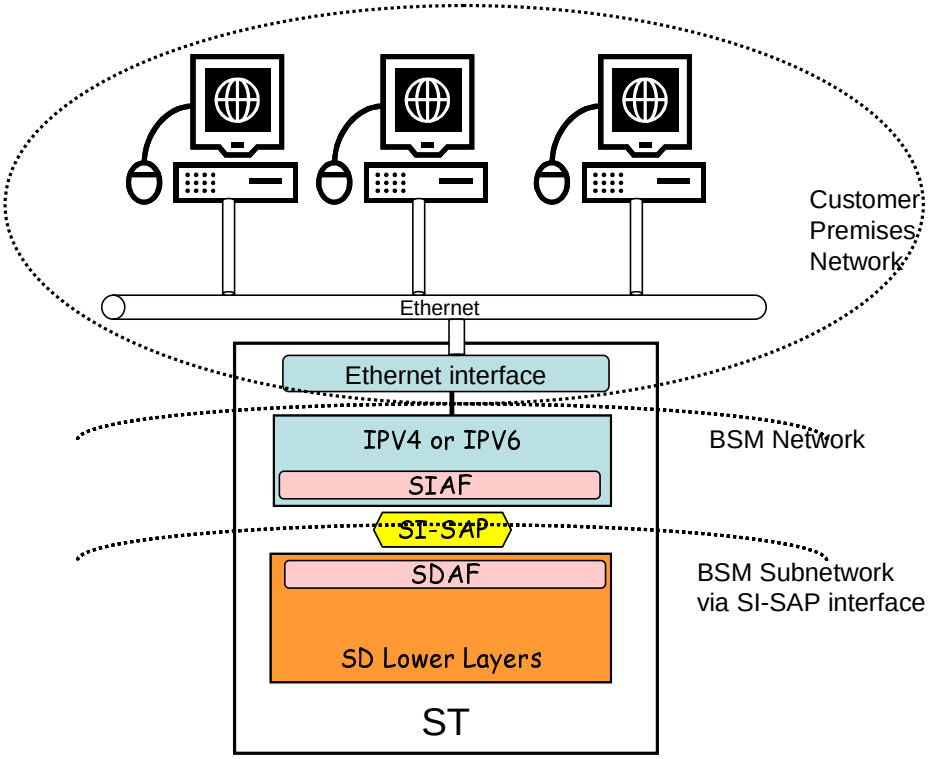


Figure B.2: BSM Network and SI-SAP point of attachments

Host PC are shown as an example of customer premises equipment and from an IP networking viewpoint these are end hosts having IP addresses. All IP traffic between the customer premises and the BSM network equipment is via the Ethernet IP interface.

Referring to figure B.2, which shows the customer premises network, the BSM Network, and the BSM SI-SAP and BSM Subnetwork, we can show the relationship between them.

Customer Premises Networks can be the following:

- private address that are not routable outside of the customer premises network and require NAT to a local routable address to allow forwarding to another local customer premises network;
- private address that are routable to other customer premises network within the BSM Network but require NAT to a global unique (public) IP address;
- public globally unique and globally routable IP address.

Taking the first bullet point as the most involved case, figure B.3 shows the relationship between different points of attachments when there are multiple STs and multiple Customer Premises Networks.

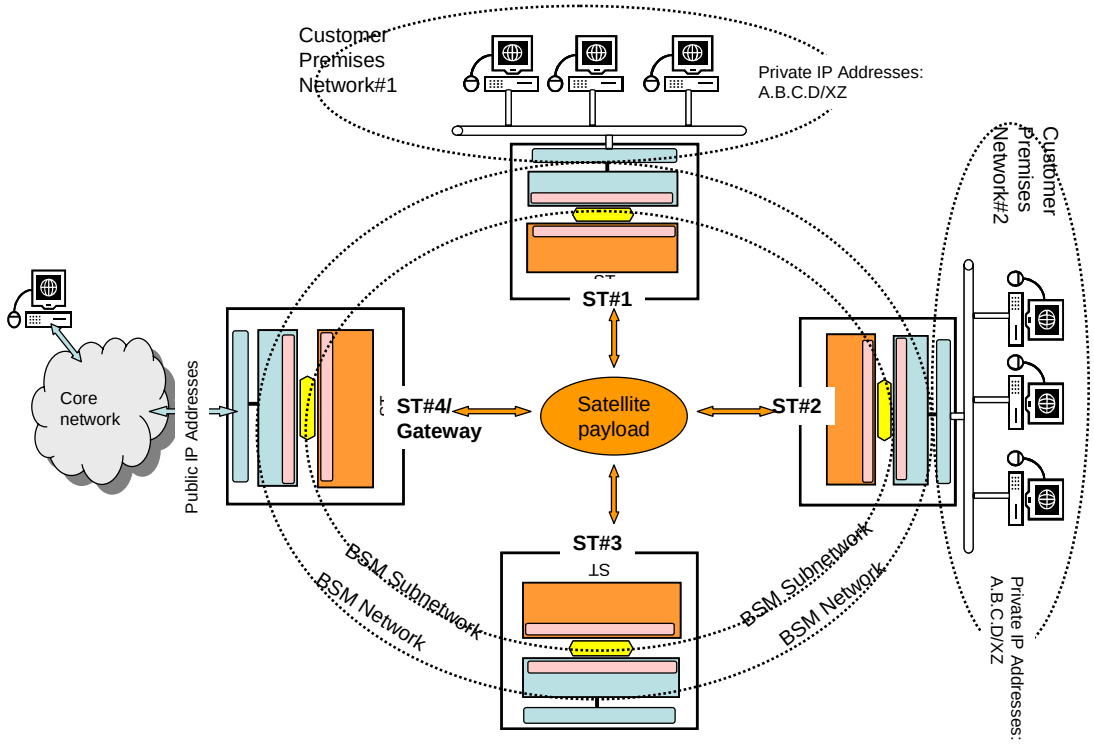


Figure B.3: BSM Network with multiple Customer Premises Networks

Part of this figure shows two Customer Premises Network (CPN), both with the identical network address (IP address and netmask). To route a package from one CPN(1) to another CPN(2) the IP packet will need to have knowledge of the routable addresses assigned to CPN(2) and CPN(2) will need to know the routable addresses of CPN(1). The scopes of these routable addresses are global or unique within the BSM network (BSM local). A worked example using double NAT is given in annex C.

Within the BSM Network, IP addresses must be routable at least to another ST or GW. The destination ST/GW must be able to translate to a destination address routable for the attached network (Public or Customer Premises).

Since there is a one to one correspondence from ST to BSM_ID, for routing to work the BSM_ID must be unique within a BSM network; this uniqueness of BSM_ID enables routing within the BSM subnetwork from GW/ST to ST. This property is vital: the BSM STs send data via the SI-SAP: each data transfer is labelled with the BSM_ID (i.e. a specific destination BSM_ID). For ingress IP packets, this BSM_ID is translated to a satellite dependent lower layer address which is then used to transport the data from one SI-SAP point of attachment to another. For egress IP packets, the destination BSM_ID may be used to query how to process the packet for exit from the BSM subnetwork.

Annex C (informative): Example of a double NAT network topology

C.1 Double NAT network scenario

Double NAT applies when you purposely use overlapping private address ranges in a network. This is done when your private/company network is larger than the public IP addresses allocated to your system. Shown below are two networks using private IP address range 192.168.150.0/16. Two additional IP ranges are needed to allow transport between the two ranges using 192.168.150.0/16; this is done commonly since the other option is to use the scarce assigned public IP addresses.

Take the example from sending from HOST 192.168.150.12 to HOST 192.168.150.22; this message will never leave Premises Network. This same example can occur separately in both of the premises networks that are using the same 192.168.150.0/16 address range: in both cases the packets will only be routed within the local premise network.

In order to route packets between these two premises network, with their overlapping address ranges, we need to use NAT. The following examples show why double NAT is required.

As a second example consider sending traffic from HOST 192.168.150.13 to HOST 192.168.190.23 and assume the 192.168.180.0/16 NAT is not present; this second message will leave the customer premises network and arrive at the 192.168.190.0/16 NAT and forward this message to destination 192.168.150.23. The second message requires a reply and this reply will have the original source address as its reply address 192.168.150.13; as a result this third message never leave the premises PC and is sent to the wrong PC.

Now start a fourth message with the 192.168.180.0/16 NAT working; this message will be sent to 192.168.190.45 from 192.168.150.45 arriving at the 192.168.180.0/16 NAT. This fourth message will have the source address changed to 192.168.180.45 and forwarded to the 192.168.190.0/16 NAT where the destination is changed to 192.168.150.45. This fourth message requires a reply to 192.168.180.45 and has no routing problems because of the double NAT'ing.

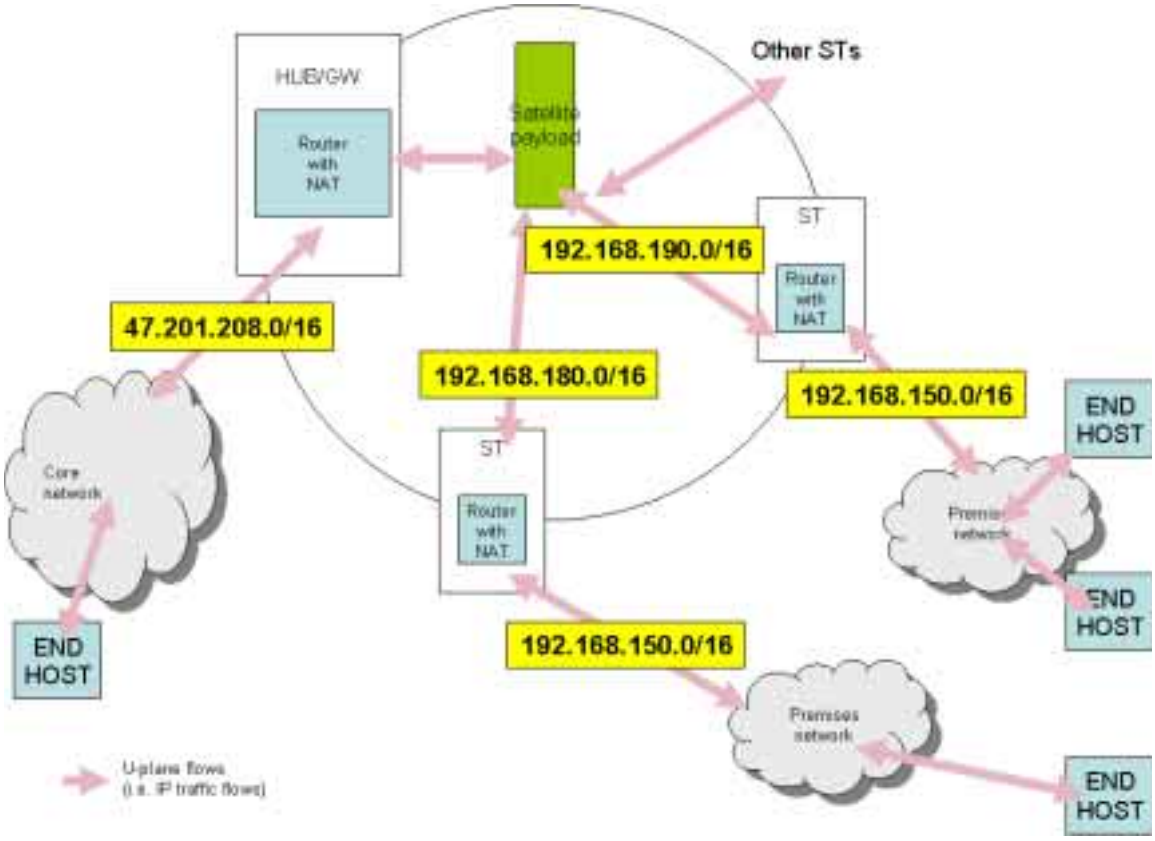


Figure C.1: BSM Network with two Customer Premises Networks

The last example is sending traffic from 192.168.150.65 to 64.236.24.20. This will only work if the destination address is changed to, for example, first 192.168.190.65, and then 47.201.208.51. For the reply message the routers will to know the public address to send, the Hub/GW will need to translate to a 192.168.190.65 (since 192.168.150.65 is ambiguous at this router). The 192.168.190.0/16 NAT will forward the reply to 192.168.150.65.

NOTE: See http://www.strongswan.org/uml/testresults/double-nat-net/ and http://www.netfilter.org/documentation/HOWTO/netfilter-double-nat.html for more examples of double nat.

C.2 Premises network routing

The above examples are a specific implementation but in the BSM Network the following is true.

The premises networks IP ranges can be one of three cases for routing:

1) Public; globally routable.

2) Private, routable only within the BSM Network.

3) Private Non-routable.

C.2.1 Public Routable Networks

A public address is an address that is routable globally in the Internet. If the END HOSTs have public IP addresses, no need for NAT'ing is needed to enable routing between the two.

C.2.2 Private Non-Routable Network

A private address is defined by the IANA as:

1) 10.0.0.0 to 10.255.255.255 (10/8 prefix);

2) 172.16.0.0 to 172.31.255.255 (172.16/12 prefix);

3) 192.168.0.0 to192.168.255.255 (192.168/16 prefix).

Addresses of this range are not typically routed among network domains. To enable routing, router filters and/or NAT tables are needed to allow the traffic to pass.

C.3 Double NAT'ing Requirements

Assumptions:

1) A Premises Networks attached to the BSM Network and sending IP traffic to another attachment point.

2) The traffic must pass through the BSM Network.

3) The BSM Network address range is larger than the size of all attached ST for private addresses

4) The BSM Network is configured for STs with public addresses.

These are the cases that make double NAT'ing a requirement between two BSM networks:

1) A Premises Networks with non-routable addresses is sending traffic to another Premises Network with non-routable addresses.

2) One Premises Network is only routable within that Premises Network and is accessing the public internet (via the BSM Network).

3) Any two Customer Premises Networks use the same IP address range.

Annex D (informative): RSM-B IP routing

D.1 RSM-B overview

The BSM Regenerative Satellite Mesh - B (RSM-B) system architecture is configured to fit both Star and Mesh topologies. The RSM-B network is based on DVB-RCS specification for the return channel (uplink) and DVB-S specification for the forward channel (downlink) communications.

The RSM-B network provides broadband data services and access to terrestrial networks, mainly IP network and PSTN through gateways, star communications. RSM-B system may also be seen as a broadband multimedia platform oriented to mesh communications based in only one hop, indicated for those scenarios where broadband services and real-time communications are desired in a single and unique offer.

The RSM-B Network includes the following elements:

- The On-Board Processor (OBP).
- The Management Station (MS): composed of two main elements:
  - The Network Management Center (NMC) is in charge of the management of all network elements, and the network and service provisioning.
  - The Network Control Center (NCC) in charge of the control of the network to serve the satellite access requests from the users of the system and manage the OBP configuration.
- Regenerative Satellite GateWay (RSGW) that provides the interface with external networks.
- Return Channel Satellite Terminal (RCST) that interfaces RSM-B network with external users of terrestrial networks.

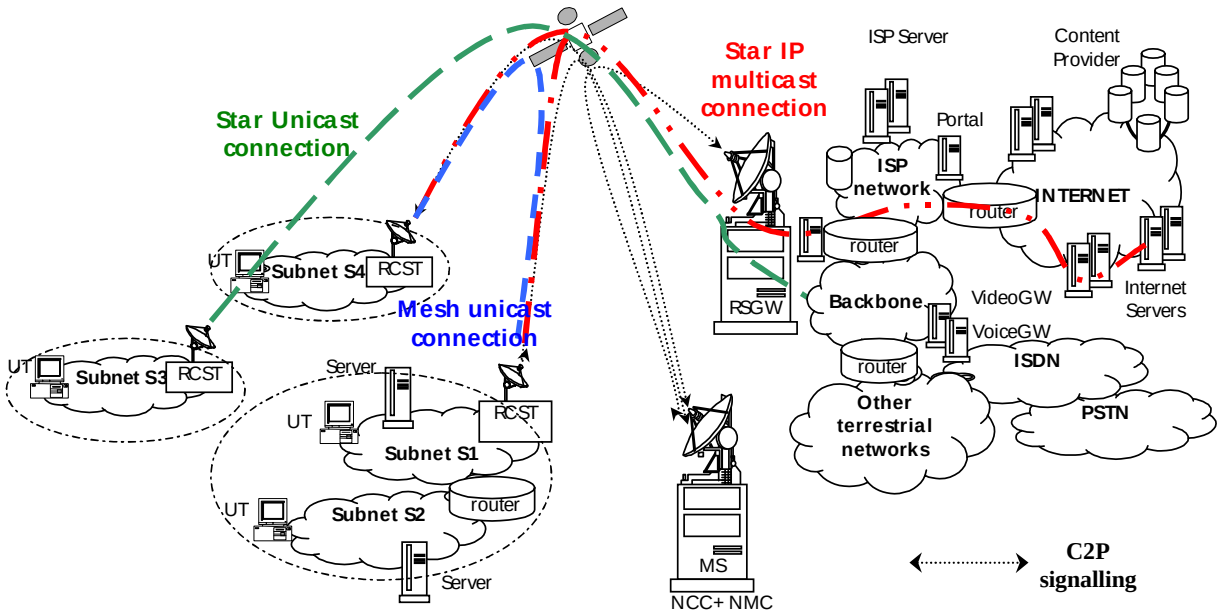


Figure D.1: RSM-B Network

D.2 RSM-B routing

The RSM-B routing function is organized as a "decentralized router". Part of the routing functions are located in the RCSTs/RSGWs and the other part of them within the NCC, in a client/server like architecture. The NCC is the routing server and the RCSTs/RSGWs the clients. Each time a client needs to route an IP packet, it asks the server for the information required to route this packet. The routing information sent by the server, is saved in the client. Each client must also be configured with some "overall" subnet prefixes authorized for this client.

Each time an IP packet arrives at the RSM-B system, the RCST or the RSGW must first determine where to send the packet, the final target of this process is to determine the destination equipment MAC address. The RCST or the RSGW look within their routing table and, if the route on the satellite path does not exist, it issues an AR toward the NCC, through the C2P(Connection Control Protocol) connection request message.

RSM-B system is a connection oriented network. C2P is the protocol used for NCC and RCST/RSGW communication. C2P provides embedded AR, plus a dynamic control of the set of communicating parties in RSM-B system for both mesh and star topology.

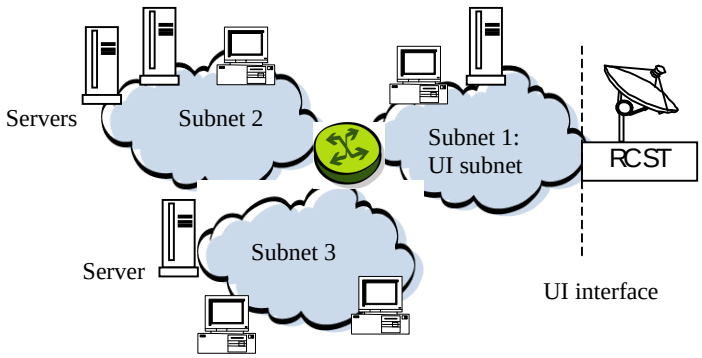


Figure D.2: Several subnets at RCST user interface side

D.3 IP routing and address resolution function

The RCST performs IP routing. Each time an IP packet enters the RCST, this one determines where to send the packet, aiming to get either the destination equipment MAC address or the Next Hop Router (NHR) MAC address.

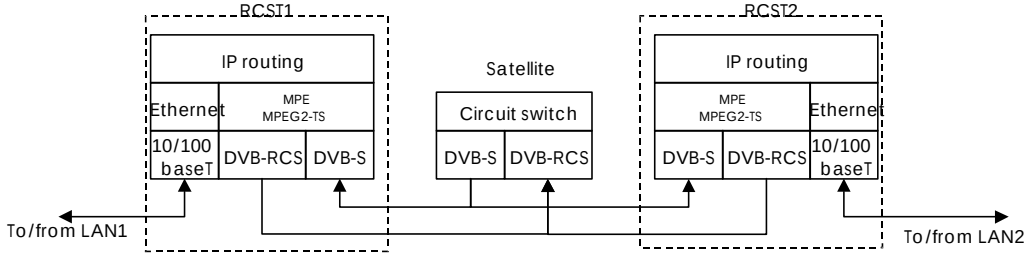


Figure D.3: RCST RSM-B IP routing function

There exists a close interaction between the routing and addressing functions, and the connection control and management. The connection interconnects distant points across the RSM-B network as a route across any type of network. And as for a route, the connection between end points is not possible without the knowledge of transit and end points (address), and paths linking these points (routing information).

All this information is centralized in the NCC, which alone makes possible the connection between end points. The end point can be any user equipment hosted on a sub-net located behind a RCST (User Interface side). These equipment are identified by a unique IP address belonging to one of the sub-net masks attached to the RCST. However, since the transmission across RSM-B is based upon the MPEG-2 TS packet format, the knowledge of MPE MAC addresses of end RCSTs is mandatory to establish a connection. That means that the NCC provides the mechanisms required to associate the IP address of a user equipment into the MPE MAC address corresponding to the hosting RCST (mechanism referred as "address resolution").

In order to speed-up the connection establishment procedure, the AR function and the connection establishment is simultaneous: the connection establishment request from the RCST includes an AR request, and the NCC response contains both AR response (destination MAC address, and subnets) and connection parameters. There is only one step and one message sent in each direction.

The RCST routing table consists in two parts:

- The first part of the routing table is configured with routes depending on the subscription.
- The second part dynamically modifiable through C2P.

The configured entries may not be modified or removed by C2P but only through management (such as through SNMP or local management interface). The Next Hop information in the corresponding line of the routing table, for these entries, are configured empty (dash) so that the RCST issues an AR toward the NCC.

The following sequence presents the successive steps associated to a new point-to-point bi-directional connection set-up between two end points (other parameters than the addressing type are omitted for simplicity):

1) First of all, the calling RCST (hosting the calling equipment) needs to determine if a new connection should be requested or not as shown in figure D.4.

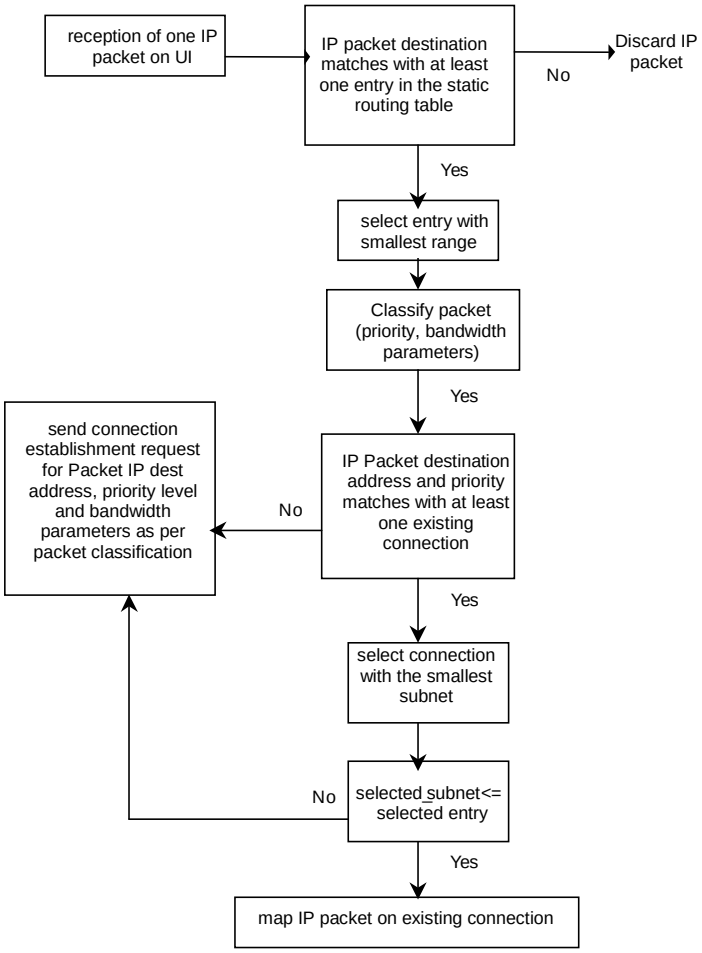


Figure D.4: RCST RSM-B routing and connection set-up

2) If the results is positive, the calling RCST propagates towards the NCC the request containing the called IP address to query the MPE MAC address of the corresponding end RCST (hosting the called equipment). The source RCST also transmits the IP address of the calling user equipment, the priority level and a requested bandwidth for the connection.

3) The NCC propagates the calling MPE MAC address and adds the mask addresses of the sub-net associated to the calling RCST. This mask contains the IP address of the calling user equipment.

4) The NCC replies to the request with the called RCST MPE MAC address of the corresponding end RCST (hosting the called equipment) and the mask addresses associated to called RCST. This mask obviously contains the IP address of the called user equipment, confirmation of the priority level and bandwidth requested for the connection.

5) Each RCST caches the called MAC MPE address/IP sub-net masks pair avoiding to reiterate requests at each new incoming IP packet with an IP address belonging to one of the sub-net masks.

6) All the sub-nets prefix attached to one RCST are transmitted to the other RCST.

7) Once the calling RCST queried the called RCST MPE MAC address, it can encapsulate the data over MPEG-2 TS with the right MPE header and transmit the IP packets on the connection so established.

In case of multicast connection, the destination MPE MAC address is a multicast or broadcast MAC address.

D.4 Default route

The RCST routing table is configured with:

- one or several prefixes covering all the private IP address ranges of all the subscribers of the satellite network;
- one or several prefixes identifying the public IP address ranges allowed in the satellite network (this may also be specific to each RSCT);
- optionally, a default route.

Depending on the satellite network-addressing plan, the RCST may have a default route or not. A single default route is authorized per RCST. The usage to the default routing entry will depend on the type of services supported by the RCST:

- The routing table of a RCST involved in an Internet access subscription is configured with a default route toward a RSGW of the ISP.
- The routing table of a RCST involved in a corporate access is configured with a default route toward the RSGW of the telecom operator.
- The routing table of a RCST involved in a LAN interconnection access (VPN) may be configured with a default route toward another RCST of the same satellite network.

Annex E (informative): RSM-A Address Resolution

E.1 Introduction

Address Resolution is the means by which a network layer (IPv4 or IPv6) address is resolved to a link layer (RSM-A or Ethernet) address.

Address resolution is performed after the router interface is determined and makes use of an AR cache, which keeps AR entries for resolving the network address. The AR cache may be populated by a network protocol associated with the router interface. This clause identifies the protocols used for AR, Satellite Address Resolution Protocol (S-ARP). In addition, static AR entries may also be configured under certain conditions. This clause does not describe how the static AR entries are configured and the likely scenarios for doing so.

This annex presents the design for AR for customer networks as well as for the RSM-A Management Network.

E.1.1 AR for customer networks

As it relates to customer networks supported by RSM-A, the ST has two link layer interfaces: satellite and terrestrial.

E.1.1.1 AR at Terrestrial Interface for customer networks

For the Ethernet interface, the ST will use ARP (Address Resolution Protocol), RFC 826 (see bibliography), for resolving IPv4 addresses and ND (Neighbour Discovery), RFC 2461 (see bibliography), for resolving IPv6 addresses. The ST shall support an AR cache for its Ethernet interface(s); the size of this cache is dependent on the number of hosts/routers that are connected to the LAN segment. For example, it is expected that the larger gateway terminals will maintain a much larger cache than the smaller user terminals.

The AR cache supporting IPv6 and the Ethernet link may contain only a portion of the IPv6 address. If the SLA ID (for Global Unicast addresses) or the Subnet ID (for Site Local addresses) are mapped uniquely to an Ethernet interface, then the AR cache entry may use the 64 bit Interface ID or Station ID to identify the network address to be resolved.

E.1.1.2 AR at Satellite Interface for customer networks

Because RSM-A is a shared resource where many subnets all use a single communication link, the IP address that is assigned to the satellite interface of the ST must be unique in order to resolve to the RSM-A MAC address. Region wide uniqueness is required because the Wholesaler facility (NOCC) is used to perform address resolution. This design introduces a new term that is used from a system design perspective for solving the lack of uniqueness problem. An address called the Satellite Next Hop Address (SNHA) is introduced to provide the uniqueness required for routing and address resolution across RSM-A. The Satellite Next Hop Address is found in route table entries and is the address that comes out of the route lookup process.

The Satellite Next Hop Address is used irrespective of ST type. For ST Gateway STs, the Satellite Next Hop Address is associated with the satellite interface of the Access Gateway; for standalone STs, it is associated with the satellite interface of the UP. This same address is also in the AR cache for the satellite interface and is used to resolve to the RSM-A Destination MAC Address.

The STs AR cache for the satellite interface is composed of at least the following parameters:

- Satellite Next Hop Address.
- RSM-A Destination MAC Address.
- Static AR entry indicator.
- Pending AR entry indicator.

- Stale AR entry indicator.
- AR pass/fail indicator.
- AR entry timer value.

AR cache entries for the satellite link will be configured by the NOCC or learned by the ST using Satellite ARP. Configured cache entries will have the "Static AR entry" indicator set and will not be timed out. A likely scenario for using static cache entries is for the case when the remote (ST) is configured with a default route pointing to its hub Access Gateway. In such a case, a static AR entry ought to be configured to resolve the network address of the Access Gateway.

If an ST is configured to use Satellite ARP and an entry is not found in the AR cache associated with the STs satellite interface, then the ST participates in the Satellite ARP to resolve the Satellite Next Hop Address to the RSM-A Destination MAC address. The ST may insert the Satellite Next Hop Address into the AR cache entry and set the Pending AR entry indicator while it is waiting for a response from the NOCC for the Satellite ARP request. Once the Satellite ARP response is returned to the ST, entries learned by way of Satellite ARP are inserted into the AR cache along with the pre-configured cache timeout value. The Pending AR entry indicator is cleared and the AR pass/fail indicator is set according to the value returned in the Satellite ARP Response. When the AR entry times out, the stale AR entry indicator is set. If the Satellite Next Hop Address cannot be resolved to the RSM-A Destination MAC Address, then the ST drops the IP packet.

E.1.1.3 Satellite ARP Description

The ST and the NOCC participate in the Satellite AR protocol. The NOCC provides an AR server that contains a database of all RSM-A Destination MAC addresses assigned to all customer networks supported by RSM-A for each satellite in a given region. The RSM-A Destination MAC address is unique to a specified RSM-A satellite link. Associated with the Satellite Next Hop Address is a RSM-A Destination MAC Address.

The ST will query the AR server for the address resolution information for forwarding the IP packet, and after validating the query, the AR server would return an AR entry. The ST will insert this entry into the AR cache associated with the satellite interface and use it to forward the IP packet to another ST across the satellite link. The IP packet which triggered the Satellite ARP request (and subsequent IP packets to the same subnet) is queued. The current requirement is that the NOCC shall respond to an address resolution query within 2 seconds over the space link.

The two messages necessary for this mechanism are Satellite ARP Request and Satellite ARP Response. The Satellite ARP Request has the following information:

- Satellite ARP Version Number.
- Satellite ARP Message Type (Satellite ARP Request).
- Satellite Next Hop Address.
- Satellite ARP Request ID.
- The Satellite ARP response has the following information:
- Satellite ARP Version Number.
- Satellite ARP Message Type (Satellite ARP Response).
- Satellite Next Hop Address.
- RSM-A Destination MAC address.
- Satellite ARP Response Status.
- Satellite ARP Request ID.

When the NOCC receives a Satellite ARP request, it performs an access check before returning the Satellite ARP Response. The tables containing the address resolution between Satellite Next Hop Address and RSM-A Destination MAC Address will be populated as part of the configuration process of an ST. A Satellite ARP response status is returned for error conditions or when access restrictions prevent communication. The NOCC returns the Satellite ARP Request ID to the ST in the Satellite ARP Response message.

There are some Satellite ARP Response Status values which indicate that the Satellite Next Hop Address was not resolved by the NOCC for some reason which is transient in nature. In these cases, the ST will not insert the responses in the AR cache, but will retry at an interval which is typically much shorter than the AR cache timeout value.

There may be situations when the NOCC may want to send an unsolicited AR entry to one or more STs. In these cases, the NOCC sends an Unsolicited Satellite ARP Response with the following information:

- Satellite ARP Version Number.
- Satellite ARP Message Type (Unsolicited Satellite ARP Response).
- Satellite Next Hop Address.
- RSM-A Destination MAC address.
- Satellite ARP Response Status.

The behaviour of the ST in handling the Unsolicited Satellite ARP Response is the same as the Satellite ARP Response, except for the Satellite ARP Request ID. The NOCC will region-cast to every ST of a satellite the Unsolicited Satellite ARP message for a particular AR entry. There will be a field in the Unsolicited Satellite ARP message indicating that if the AR entry is found, it is to be removed.

E.2 State diagram

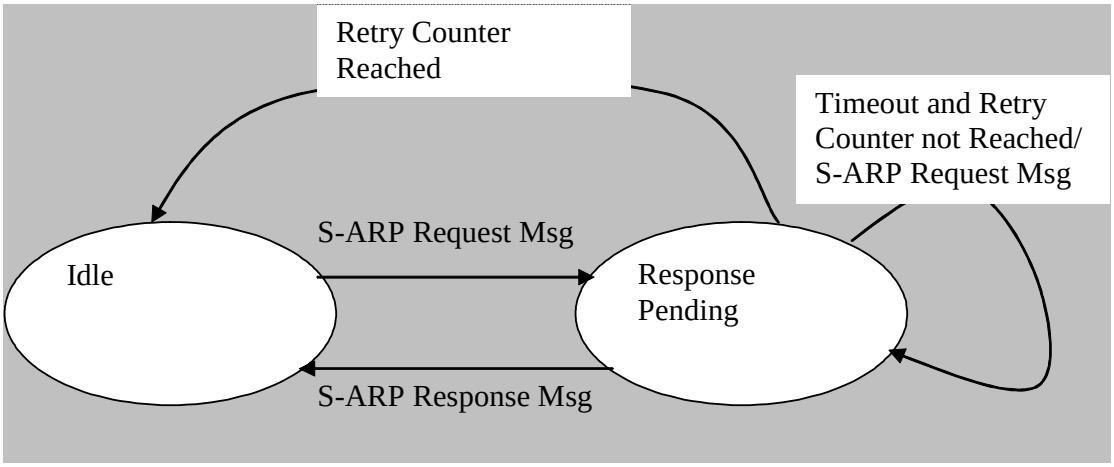


Figure E.1: S-ARP state diagram at ST virtual port

E.3 Procedures

The following ladder diagram shows a S-ARP request exchange between an ST virtual port and the NOCC for the purpose of Address Resolution.

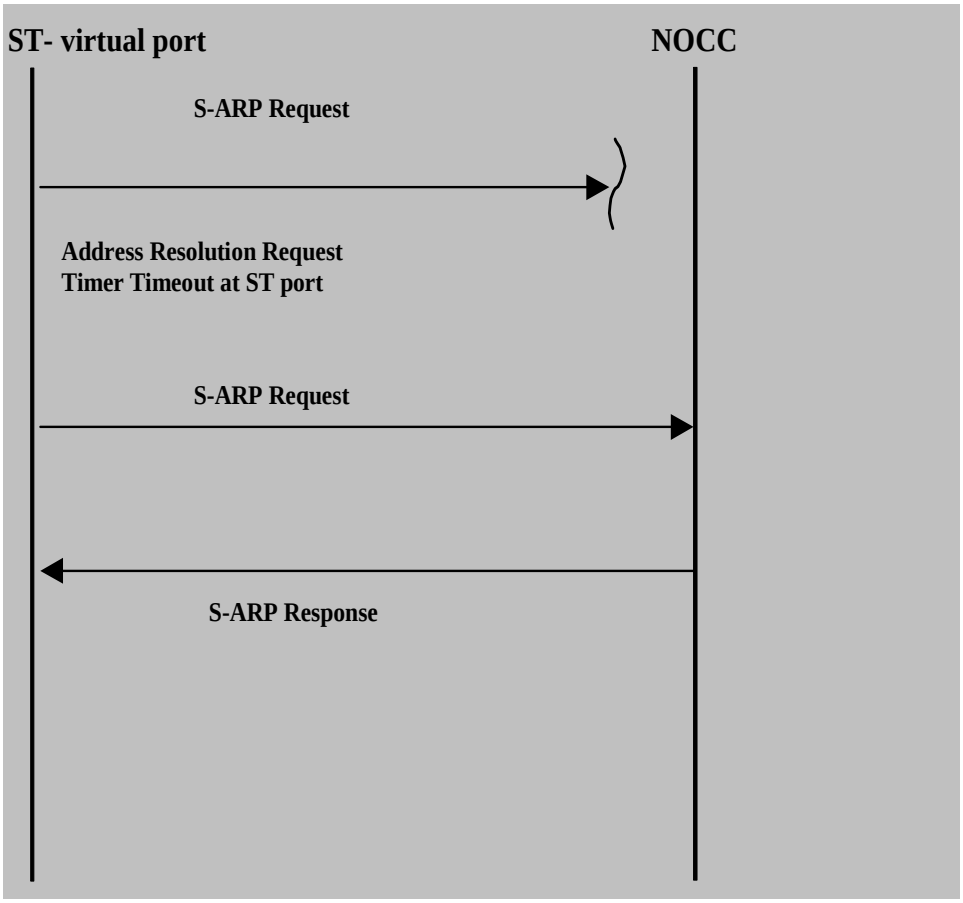


Figure E.2: S-ARP requests and response

Annex F (informative): Description of SI-SAP AR Primitives

F.1 C-Plane AR Primitives

Primitives for all three planes (C, U and M) were identified in [3] "Satellite Independent Service Access Point (SI-SAP)". The C-Plane AR primitives are reproduced below for reference with some suggested parameters.

Address resolution query primitives are used to enable the upper SI-layers to determine the appropriate destination BSM_ID (lower layer address) for a given destination network address (IP address).

Address resolution information primitives are used to enable the SD-layer to supply unsolicited address resolution information.

F.2 Primitives

F.2.1 SI-C-AR_QUERY

The SI layer requests an Address Resolution update using the SI-C-AR_QUERY-REQ primitive containing the Network Address of the destination.

The SD layer should respond to the request using the SI-C-AR_QUERY-CFM primitive which contains the BSM_ID associated with that Network Address.

Table F.1: SI-C-AR_QUERY primitives

PRIMITIVE NAME	SI-C-AR_QUERY-***
FUNCTION	Request and receive address resolution information

Primitive parameters:	**-req**	**-cfm**	**-ind**	**-res**	**Comments**
AR Query Handle	M	M	M	M	Used to match request and confirm
Network Address Type	M	M	M	M	Defines the format of the Network Address
Network Address	M	M	M	M	Network address for AR
BSM_ID		M		M	Next-hop BSM_ID; validity indicated by cause code
BSM Multicast Flag		M		M	Flag that indicates if the BSM_ID is a multicast address
Cause code		M		M	Indicates whether AR was successful, and gives cause in case of failure
Status	O	M	O	M	Indicates status for forwarding to this destination

F.2.1 SI-C-AR_INFO

The SD layer may supply unsolicited AR information (i.e. Network Address/ BSM_ID pairs) at any time using the SI-C-AR_INFO-IND primitive. This primitive can be used to announce the existence of multicast groups.

The SI layer should respond to unsolicited AR information using the SI-C-AR_INFO-RES primitive to acknowledge receipt of the AR information.

Table F.2: SI-C-AR_INFO primitives

PRIMITIVE NAME	SI-C-AR_INFO-***
FUNCTION	Receive and acknowledge unsolicited address resolution information

Primitive parameters:	**-req**		**-ind**	**-res**	**Comments**
AR Info Handle	M		M	M	Used to match indication and response
AR Info Type	M		M	M	Indicates whether the AR info is set or cancelled
Network Address Type	M		M		Defines the type of the Network Address.
Network Address	M		M		Network address for AR
BSM_ID	M		M		Next-hop BSM_ID; validity indicated by cause code
BSM Multicast Flag	M		M		Flag that indicates if the BSM_ID is a multicast address
Status	M		M		Allow or Drop this kind of traffic

F.3 Parameters

F.3.1 AR query handle

A local label that is used to identify a given AR_QUERY request. The ID handle is used to label all primitives associated with a given request.

F.3.2 AR info handle

A local label that is used to identify a given AR_INFO indication. The ID handle is used to label all primitives associated with a given indication.

F.3.3 AR info type

A flag that indicated whether the AR_INFO primitive is setting or clearing the associated AR entry.

Parameter	**Value**	**Comment**
AR Info Type; Boolean	True = "Set"	New AR entry; add or replace existing value in cache
	False = "Cancel"	AR entry cancelled; remove existing value in cache

F.3.4 Network address

The network address corresponds to the "next-hop" address for the higher layers. The address shall be unique within the satellite network.

A network address that is context dependent, for example an IPv4 next-hop address (which may be subject to NAT) shall include an additional context field to differentiate all overlapping (ambiguous) address domains within the satellite network.

F.3.5 Network address type

The Network address type defines the format of the Network Address using the IEEE defined Ethertype parameter.

NOTE: This parameter has the same definition as the SDU Type parameter: the SDU Type parameter is defined in the SI-SAP specification [3] as part of the SI-U-UNITDATA primitives.

F.3.6 Status

Parameter	Value	Comment
Type; Boolean	True = "Allow"	Allow this network range to pass the SI-SAP
	False = "Drop"	Drop this network range at the SI-SAP

F.3.7 BSM_ID

The BSM_ID is the SI-SAP address that can be used to send data to the wanted destination ST. A given Network Address shall only be associated with one BSM_ID. See clause 5.1.3.

F.3.8 BSM multicast flag

A flag that indicates whether the network address in the AR_QUERY or the AR_INFO primitive is a BSM multicast ID.

Parameter	Value	Comment
Multicast flag; Boolean	True	Address is a multicast ID
	False	Address is not a multicast ID

Annex G (informative): Examples of AR function usage

The Address Management for AM functions will contain a summary of Address Resolution, Dynamic Host Configuration assignments, and associated NAT.

G.1 Suggestion for data stored in AR caches

1) BSM_ID.
2) Next hop IP address.
3) List IP addresses for searching for next hop addresses each having:
   a) IP addresses.
   b) IP address scope (Private BSM Network, Private ST Local, Public Routable Address).
   c) Status (accept/deny) (optional).

G.2 SI-C-AR_INFO Function

This message is used to provide unsolicited information to configure or update an AR entry. These should be used typically for allowing or dropping IP traffic at an SI-SAP interface; updates would be more in mesh topology where t he initial packets are sent to a default location and then the NCC will configuration a more efficient path for the data.

Figure G.1 shows two examples of SI-C-AR_INFO primitive usage.

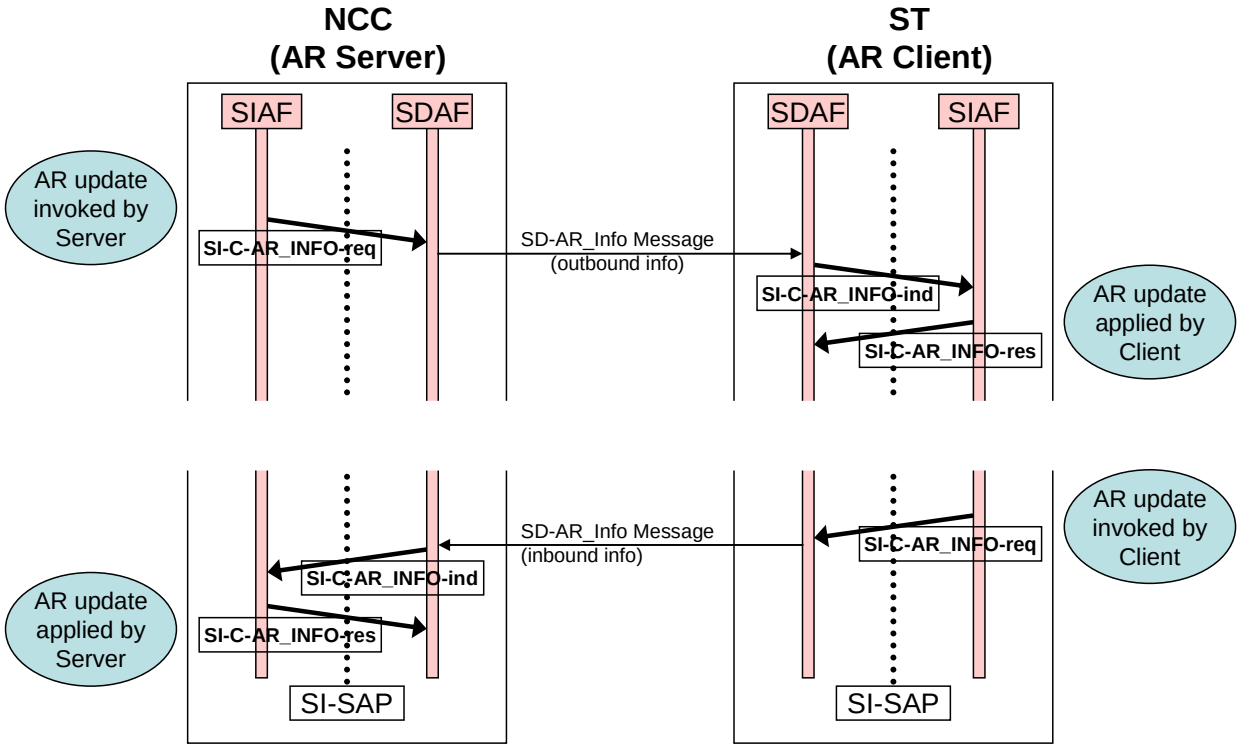


Figure G.1: Example of use of SI-C-AR_INFO primitives

In the case of a Star topology, the ST includes both Remote ST and the central Hub/Gateway ST. In both cases, the ST is assumed to contain an AR client function that exchanges AR data with an AR server.

The upper sequence in figure G.1 shows an Outbound information sequence:

- The SIAF at the Server side invokes the request by submitting a SI-C-AR_INFO-request primitive.
- This request triggers a SD message to the Client.

NOTE: This SD message may be a multicast or broadcast message to multiple or all Clients.

- The request emerges at the Client(s) in a SI-C-AR_INFO-indication primitive.
- Each Client should update its local AR Tables with the new AR information.

The lower sequence in figure G.1 shows an Inbound information sequence:

- The SIAF at the Client side invokes the request by submitting a SI-C-AR_INFO-request primitive.
- This request triggers a SD message to the Server.
- The request emerges at the Server in a SI-C-AR_INFO-indication primitive.
- The Server should update its central AT Tables with the new AR information.

G.3 SI-C-AR_QUERY

The B-AR server will store the BSM_ID and associated IP addresses. These IP addresses will have a status associated to them of allow or deny access to the BSM Network. The server can be preconfigured by the Network Operator with allowed IP addresses. Optionally the server can be dynamically updated with allowed addresses.

The ST AR Client can invoke on-demand queries to the AR Server at any time using the SI-C-AR_QUERY primitives. Typically an AR client would invoke this request when a packet arrives for a new destination and the ST does not have valid AR information available for that IP destination.

As noted above, the ST includes both a Remote ST and the central Hub/Gateway ST in the case of a Star topology. The ST and Hub/Gateway can dynamically update the B-AR server with SI-C-AR_INFO Primitives using the lower sequence shown in clause G.2 if received IP packets cannot be processed at the destination correctly.

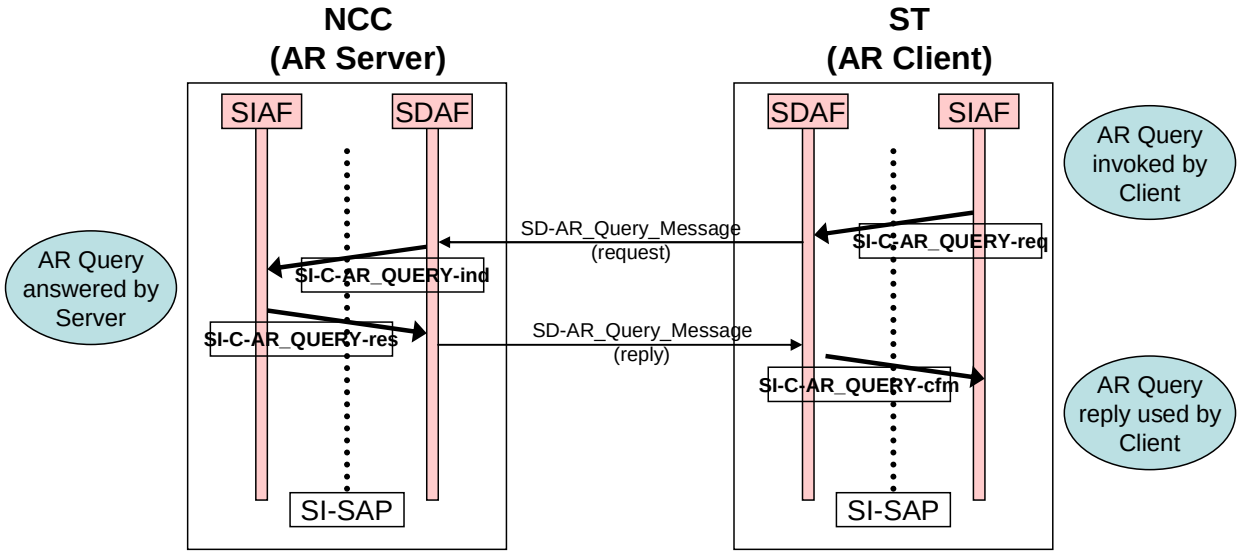


Figure G.2: Example of use of SI-C-AR_QUERY primitives

Figure G.2 shows one example of the use of these primitives:

- The SIAF at the Client side invokes the request by submitting a SI-C-AR_QUERY-request primitive.
- This request triggers a SD message to the Server.
- The request emerges at the Server in a SI-C-AR_QUERY-indication primitive.
- The Server replies to the Query in a SI-C-AR_QUERY-response primitive.
- This response triggers a SD message back to the Client.
- The reply emerges at the Client in a SI-C-AR_QUERY-confirm primitive.

Annex H (informative): Bibliography

ETSI TR 101 984: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia; Services and Architectures".

ETSI TR 101 985: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia; IP over Satellite".

ETSI TS 102 295: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM) services and architectures; BSM Traffic Classes".

ETSI TR 102 353: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Guidelines for the Satellite Independent Service Access Point (SI-SAP)".

IETF RFC 1112: "Host extensions for IP Multicasting".

ETSI TR 102 157: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia; IP Interworking over satellite; Performance, Availability and Quality of Service".

ETSI TR 102 155: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia; IP interworking over satellite; Addressing and routing".

IETF RFC 3022: "Traditional IP Network Address Translator (Traditional NAT)".

IETF RFC 826: "An Ethernet Address Resolution Protocol: or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware".

IETF RFC 2131: "Dynamic Host Configuration Protocol".

IETF RFC 3046: "DHCP Relay Agent Information Option".

IETF RFC 1631: "The IP Network Address Translator (NAT)".

IETF RFC 2461: "Neighbor Discovery for IP Version 6 (IPv6)".

History

Document history		
V1.1.1	November 2006	Publication