INTERNATIONAL STANDARD

ISO/IEC 16500-2

First edition
1999-12-15

Information technology — Generic digital audio-visual systems —

Part 2: System dynamics, scenarios and protocol requirements

Technologies de l'information — Systèmes audiovisuels numériques génériques —

Partie 2: Dynamique, scénarios et exigences de protocole des systèmes

Reference number
ISO/IEC 16500-2:1999(E)

© ISO/IEC 1999

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

© ISO/IEC 1999

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 734 10 79
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

© ISO/IEC 1999 – All rights reserved

Contents Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Definitions **1**
4 Acronyms and abbreviations **1**
5 Conventions **2**
6 Requirements for DAVIC Systems **2**
7 Implementation Procedure **2**
8 Instance Development Tool **2**
9 DAVIC System Dynamic Modeling (DSDM) and Required Protocols **3**
9.1 General 3
9.1.1 DAVIC System Dynamic Modeling 3
9.1.2 Protocols Required for System Operation 4
9.2 DSDM for VoD 4
9.2.1 Functional Entities Used in Dynamic Modeling for VoD 4
9.2.2 Alternative DAVIC Physical Scenarios for the VoD Control Functional Entities 5
9.2.3 System Dynamic Flows for VoD 7
9.2.4 Functional Entity Actions for VoD 16
9.2.5 DAVIC Dynamic Flow Parameters for VoD 22
9.2.6 Specification of the Usage of DAVIC Protocol Tools for VoD 45
9.2.7 Protocol Network Architectures for DAVIC VoD 45
9.2.8 Rationale for the Physical Scenarios for VoD 46
9.2.9 Notes on Download Protocols for VoD 46
9.2.10 Cross-Reference to DAVIC Tool Definitions for VoD 51
9.2.11 Association Between Interfaces and Network Resources for VoD 52
9.2.12 Rationale behind the selection of the DAVIC VoD dynamic systems behavior 55
9.3 DSDM for SVB (Switched Video Broadcast) 57
9.3.1 Overview 57
9.3.2 Functional Entities Used in Dynamic Modeling for SVB 57
9.3.3 System Dynamic Flows for SVB 59
9.3.4 Functional Entity Actions for DAVIC SVB 62
9.3.5 Dynamic Flow Parameters for SVB 63
9.4 DSDM for Interactive Broadcast (PSTN/ISDN Return Channel) 69
9.4.1 Overview and Description of System Behavior 69
9.4.2 Protocol Network Architecture for Interactive Broadcast 72
9.4.3 DAVIC System Dynamic Flows for Interactive Broadcast 75
9.4.4 Functional Entity Actions for Interactive Broadcast 76

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

9.5 DAVIC Architecture and DSDM for Internet Access 78
9.5.1 Overview 78
9.5.2 Direct Internet Scenario 1a 89
9.5.3 Direct Internet Scenario 1b 93
9.5.4 Direct Internet Scenario 2a 102
9.5.5 Direct Internet Scenario 2b 111
9.5.6 Internet Access Scenarios 3a and 3b 113
9.5.7 Internet Access Scenario 4 121
9.5.8 Specification of the DAVIC Protocol Tools for Internet Access 131
9.5.9 PPP Access with Broadband Broadcast and S3 Capability 133
9.5.10 Authentication and Configuration Methods for Internet Access 140
9.5.11 DAVIC server DHCP Relay Operation for Internet Access 142
9.5.12 DHCP Options for Internet Access 153
9.5.13 DAVIC Defined Resource Descriptors for Internet Access 159

10 Configuration 160

10.1 General 160
10.2 STU Configuration (Boot) 161
10.3 Service Provider System Configuration 162
10.4 Download 163
10.4.1 General 163
10.4.2 The Download service: 164
10.4.3 Download System Dynamic Flows 164
10.4.4 Download initiated at session setup: 164
10.4.5 Download initiated during active session: 166

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this part of ISO/IEC 16500 may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 16500-2 was prepared by DAVIC (Digital Audio-Visual Council) and was adopted, under the PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

ISO/IEC 16500 consists of the following parts, under the general title *Information technology — Generic digital audio-visual systems*:

— *Part 1: System reference models and scenarios*

— *Part 2: System dynamics, scenarios and protocol requirements*

— *Part 3: Contours: Technology domain*

— *Part 4: Lower-layer protocols and physical interfaces*

— *Part 5: High and mid-layer protocols*

— *Part 6: Information representation*

— *Part 7: Basic security tools*

— *Part 8: Management architecture and protocols*

— *Part 9: Usage information protocols*

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Introduction

ISO/IEC 16500 defines the minimum tools and dynamic behavior required by digital audio-visual systems for end-to-end interoperability across countries, applications and services. To achieve this interoperability, it defines the technologies and information flows to be used within and between the major components of generic digital audio-visual systems. Interoperability between these components and between individual sub-systems is assured through specification of tools and specification of dynamic systems behavior at defined reference points. A reference point can comprise one or more logical (non-physical) information-transfer interfaces, and one or more physical signal-transfer interfaces. A logical interface is defined by a set of information flows and associated protocol stacks. A physical interface is an external interface and is fully defined by its physical and electrical characteristics. Accessible reference points are used to determine and demonstrate compliance of a digital audio-visual subsystem with this international standard.

A summary of each part follows.

ISO/IEC 16500-1 (DAVIC 1.3.1a Part 2) defines the normative digital audio-visual systems technical framework. It provides a vocabulary and a Systems Reference Model, which identifies specific functional blocks and information flows, interfaces and reference points.

ISO/IEC 16500-2 (DAVIC 1.3.1a Part 12) defines system dynamic behavior and physical scenarios. It details the locations of the control functional entities along with the normative protocols needed to support the systems behavior. It is structured as a set of protocol walk-throughs, or *"Application Notes"*, that rehearse both the steady state and dynamic operation of the system at relevant reference points using specified protocols. Detailed dynamics are given for the following scenarios: video on demand, switched video broadcast, interactive broadcast, and internet access.

ISO/IEC 16500-3 (DAVIC 1.3.1a Part 14) provides the normative definition of DAVIC Technology Contours. These are strict sets of Applications, Functionalities and Technologies which allow compliance and conformance criteria to be easily specified and assessed. This part of ISO/IEC 16500 contains the full details of two contours. These are the Enhanced Digital Broadcast (EDB) and Interactive Digital Broadcast (IDB). ISO/IEC 16500-3 specifies required technologies and is a mandatory compliance document for contour implementations.

ISO/IEC 16500-4 (DAVIC 1.3.1a Part 8) defines the toolbox of technologies used for lower layer protocols and physical interfaces. The tools specified are those required to digitize signals and information in the Core Network and in the Access Network. Each tool is applicable at one or more of the reference points specified within the Delivery System. In addition a detailed specification is provided of the physical interfaces between the Network Interface Unit and the Set Top Unit and of the physical interfaces used to connect Set Top Boxes to various peripheral devices (digital video recorder, PC, printer). The physical Delivery System mechanisms included are copper pairs, coaxial cable, fiber, HFC, MMDS, LMDS, satellite and terrestrial broadcasting.

ISO/IEC 16500-5 (DAVIC 1.3.1a Part 7) defines the technologies used for high and mid-layer protocols for ISO/IEC 16500 digital audio-visual systems. In particular, this part defines the specific protocol stacks and requirements on protocols at specific interfaces for the content, control and management information flows.

ISO/IEC 16500-6 (DAVIC 1.3.1a Part 9) defines what the user will eventually see and hear and with what quality. It specifies the way in which monomedia and multimedia information types are coded and exchanged. This includes the definition of a virtual machine and a set of APIs to support interoperable exchange of program code. Interoperability of applications is achieved, without specifying the internal design of a set top unit, by a normative Reference Decoder Model which defines specific memory and behavior constraints for content decoding. Separate profiles are defined for different sets of multimedia components.

ISO/IEC 16500-7 (DAVIC 1.3.1a Part 10) defines the interfaces and the security tools required for an ISO/IEC 16500 system implementing security profiles. These tools include security protocols which operate across one or both of the defined conditional access interfaces CA0 and CA1. The interface CA0 is to all security and conditional access functions, including the high speed descrambling functions. The interface CA1 is to a tamper resistant device used for low speed cryptographic processing. This cryptographic processing function is implemented in a smart card.

ISO/IEC 16500-8 (DAVIC 1.3.1a Part 6) specifies the information model used for managing ISO/IEC 16500 systems. In particular, this part defines the managed object classes and their associated characteristics for managing the access network and service-related data in the Delivery System. Where these definitions are taken from existing standards, full reference to the required standards is provided. Otherwise a full description is integrated in the text of this part. Usage-related information model is defined in ISO/IEC 16500-9.

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

ISO/IEC 16500-9 (DAVIC 1.3.1a Part 11) specifies the interface requirements and defines the formats for the collection of usage data used for billing, and other business-related operations such as customer profile maintenance. It also specifies the protocols for the transfer of Usage Information into and out of the ISO/IEC 16500 digital audio-visual system. In summary, flows of audio, video and audio-visual works are monitored at defined usage data collection elements (e.g. servers, elements of the Delivery System, set-top boxes). Information concerning these flows is then collected, processed and passed to external systems such as billing or a rights administration society via a standardised usage data transfer interface.

Additional Information

ISO/IEC TR 16501 is an accompanying Technical Report. Further architectural and conformance information is provided in other non-normative parts of DAVIC 1.3.1a (1999). A summary of these documents is included here for information.

ISO/IEC TR 16501 (DAVIC 1.3.1a Part 1) provides a detailed listing of the functionalities required by users and providers of digital audio-visual applications and systems. It introduces the concept of a contour and defines the IDB (Interactive Digital Broadcast) and EDB (Enhanced Digital Broadcast) functionality requirements which are used to define the normative contour technology toolsets provided in ISO/IEC 16500-3.

DAVIC 1.3.1a Parts 3, 4 and 5 are DAVIC technical reports. They provide additional architectural and other information for the server, the delivery-system, and the Service Consumer systems respectively. Part 3 defines how to load an application, once created, onto a server and gives information and guidance on the protocols transmitted from the set-top user to the server, and those used to control the set-up and execution of a selected application. Part 4 provides an overview of Delivery Systems and describes instances of specific DAVIC networked service architectures. These include physical and wireless networks. Non-networked delivery (e.g. local storage physical media like discs, tapes and CD-ROMs) are not specified. Part 5 provides a Service Consumer systems architecture and a description of the DAVIC Set Top reference points defined elsewhere in the normative parts of the specification.

DAVIC 1.3.1a Part 13 is a DAVIC technical report, which provides guidelines on how to validate the systems, technology tools and protocols through conformance and / or interoperability testing.

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Information technology — Generic digital audio-visual systems — Part 2: System dynamics, scenarios and protocol requirements

1 Scope

The purpose of this part of ISO/IEC 16500 is to specify normative protocols and associated dynamic system behavior, including session and connection manipulation, configuration and download, for an ISO/IEC 16500 system. The emphasis is on the significant dynamic system entities (e.g., session control, call/connection control), the behavior of these entities (e.g., information flows, entity actions, parameters passed) and the allowable physical placement(s) of these entities in a DAVIC system (i.e., physical instances). As such, this part of ISO/IEC 16500 complements the static systems reference model described in ISO/IEC 16500-1, specifying normative dynamic behavior as well as specifying the protocol(s) required to realize this behavior.

The protocols themselves are specified primarily through the use of "Protocol Network Architecture" diagrams which visually illustrate, for each of the defined physical instances and application scenarios, the various protocol stacks which are to be used. Detailed specification of the individual protocol tools themselves (e.g., the detailed protocol messages used to realize the DAVIC dynamic flow behavior) is provided in ISO/IEC 16500-5 (mid- and higher layers) and ISO/IEC 16500-4 (lower layers) of this specification.

This results in instance specifications made up of building blocks from the DAVIC tool set organized in a manner describing a system which performs DAVIC functions.

2 Normative references

Detailed bibliographic references for the normative protocols identified in this part of ISO/IEC 16500 (e.g. in Table 9.2-28 and Table 9.2-29) are provided in ISO/IEC 16500-2 Annex E.

3 Definitions

This clause defines new terms, and the intended meaning of certain common terms, used in this part of ISO/IEC 16500. Annex A of ISO/IEC 16500-1 defines additional terms and, in some cases, alternative interpretations that are appropriate in other contexts. For convenience, the normative definitions below are included in the annex.

3.1 **call entity** or **connection entity:** user or network process which terminates S4 flow (c/c).

3.2 **functional control entities:** call/connection entity and session entity.

3.3 **functional entity:** process which terminates an information flow.

3.4 **proxy signaling agent:** signaling process performing end point signaling function on behalf of the end user. Extended definition is required if proxy is used also in hybrid network, e.g., MPEG HFC and ATM.

3.5 **Q.2931 MACRO:** single notation which summarizes the exchange of information (S4 flow) between call/connection control entities during the call set-up or release phases.

3.6 **session entity:** user or network process which terminates S3 flow (ses).

4 Acronyms and abbreviations

This clause defines the acronyms and abbreviations used in this part of ISO/IEC 16500. Annex B of ISO/IEC 16500-1 defines acronyms and abbreviations used within ISO/IEC 16500.

c/c	call/connection entity
CRM	Connection Resource Manager
DSDM	DAVIC System Dynamic Modeling
e-e cntrl	end-to-end control

--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

MPTS	Multi-Program Transport Stream (ISO/IEC 13818–1 MPEG-2 Systems)
pses	Pseudo-session control entity (used in some Internet Access scenarios)
Ses	Session control entity
SPTS	Single Program Transport Stream (ISO/IEC 13818–1 MPEG-2 Systems)

5 Conventions

The style of ISO/IEC 16500 follows the *Guide for ITU-T and ISO/IEC JTC1 co-operation. Appendix H: Rules for presentation of ITU-T | ISO/IEC common text (March, 1993).*

6 Requirements for DAVIC Systems

DAVIC systems are characterized as follows:

- The system must be built from the set of tools defined in ISO/IEC 16500.
- The system must reflect one of the allowable physical instances specified in this part of ISO/IEC 16500.
- The system must illustrate DAVIC behavior at the various reference points as defined in ISO/IEC 16500-1.
- The system must perform functionalities outlined in ISO/IEC TR 16501.
- The system dynamic behavior must be in accordance with the dynamic flow scenarios, entity actions, and parameters, and protocols specified in this part of ISO/IEC 16500, utilizing the detailed protocols specified in ISO/IEC 16500-4 and ISO/IEC 16500-5.
- The reference points must be accessible to allow effective interoperability testing at the reference points and throughout the system as appropriate.

7 Implementation Procedure

The following list defines the procedure for the description of a DAVIC system instance:

1. Define the instance in terms of the static DAVIC reference model of ISO/IEC 16500-1 and one of the allowed physical allocations of the dynamic functional entities specified in this part of ISO/IEC 16500. Identify the required protocol tools outlined in ISO/IEC 16500 from the physical instances, dynamic behavior and the protocol network architecture diagrams of this part of ISO/IEC 16500.
2. Define the identified points using the tools outlined in ISO/IEC 16500.
3. Identify the required DAVIC functionalities and demonstrate the implementation of these functions through the network instance, utilizing the system dynamic behavior as specified in the dynamic flows of this part of ISO/IEC 16500.
4. Repeat steps 2 through 3 for the various network types (i.e., for the various physical layer access technologies) to which the instance applies.

8 Instance Development Tool

The instance development tool for definition of a DAVIC system is defined with the following elements:

- Service Provider System (SPS) (e.g., the video server for the case of VoD)
- Delivery System comprising:
  - Core Network (CN)
  - Access Network (AN)
- Service User System (e.g., the Set Top Unit)
- Information Flows S1, S2, S3, S4, S5
- Reference Points A11, A10, A9, A4, A1, A0 (Note: A0 and A4 is not shown in Figure 9.1-1 below. See ISO/IEC 16500-1 for this information).
- Functional Entities: c/c, ses, content source, content sink, e-e cntrl

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

The SPS, CN, AN, SUS, Information Flows, and Reference Points are as defined in DAVIC static system reference model of ISO/IEC 16500-1.

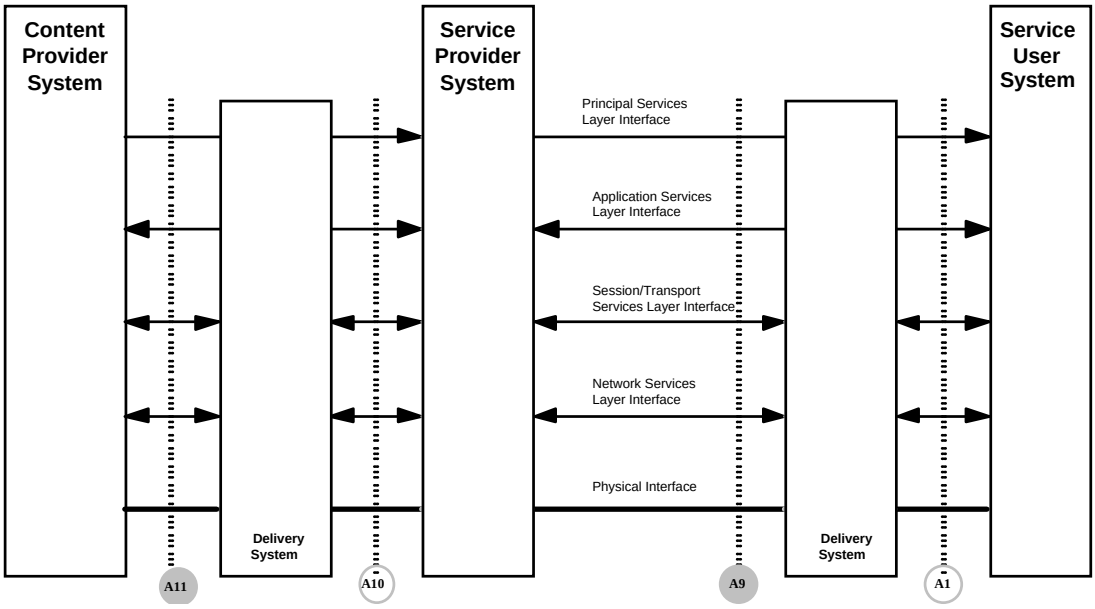


Figure 9.1-1 — DAVIC System Reference Model

The details of the relationships internal to and external to the SPS, Delivery System and SUS are as defined in the DAVIC static Systems Reference Model of ISO/IEC 16500-1.

9 DAVIC System Dynamic Modeling (DSDM) and Required Protocols

9.1 General

9.1.1 DAVIC System Dynamic Modeling

The DAVIC System Dynamic Modeling describes the following:

- Functional Entities used within the Dynamic Model(s)
- DAVIC Physical Scenarios (Physical Instances) for the allowable location(s) of the control functional entities.
- System Dynamic Flows which describe the dynamics of the DAVIC System for, e.g., the following actions, where appropriate:
  - ♦ Session & Call/connection Establishment
  - ♦ Adding Resources
  - ♦ Releasing Resources
  - ♦ Session Transfer
  - ♦ Service Transfer
  - ♦ Session & Call/connection Release
- Functional Entity Actions (performed by entities in conjunction with the dynamic flows)
- DAVIC Dynamic Flow Parameters (carried within the dynamic flows)

Collectively, these descriptive mechanisms specify the overall system dynamic behavior required of a DAVIC system for each application area (e.g., VoD, Interactive Broadcast, etc.)

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

9.1.2 Protocols Required for System Operation

The protocols required for the dynamic operation of a DAVIC compliant systems are identified in this part of ISO/IEC 16500 (for each application scenario) by means of either protocol network architecture diagrams, tables, or via descriptive text. Regardless of the means of identification, these protocols identified here are actually pointers to further detailed information specified in either ISO/IEC 16500-4 or ISO/IEC 16500-5 or in other documents as appropriate.

9.2 DSDM for VoD

9.2.1 Functional Entities Used in Dynamic Modeling for VoD

Figure 9.2-1 shows the key dynamic functional entities within a DAVIC VoD system.

- Content Source (e.g., MPEG Video Pump)
- Content Sink (e.g., Video decoder in an STU)
- e-e cntrl: entity which terminates the S2 flow and performs end-to-end control (e.g., VCR-like control: pause, fast forward, etc.)
- ses: Session Control Entities which terminate the S3 flow and coordinate the manipulation of resources, e.g., connections, in a DAVIC service instance
- c/c: call/connection control which terminate the S4 flow and set up conventional network connections

Other dynamic functional entities are introduced in the appropriate sections for the corresponding additional capabilities.

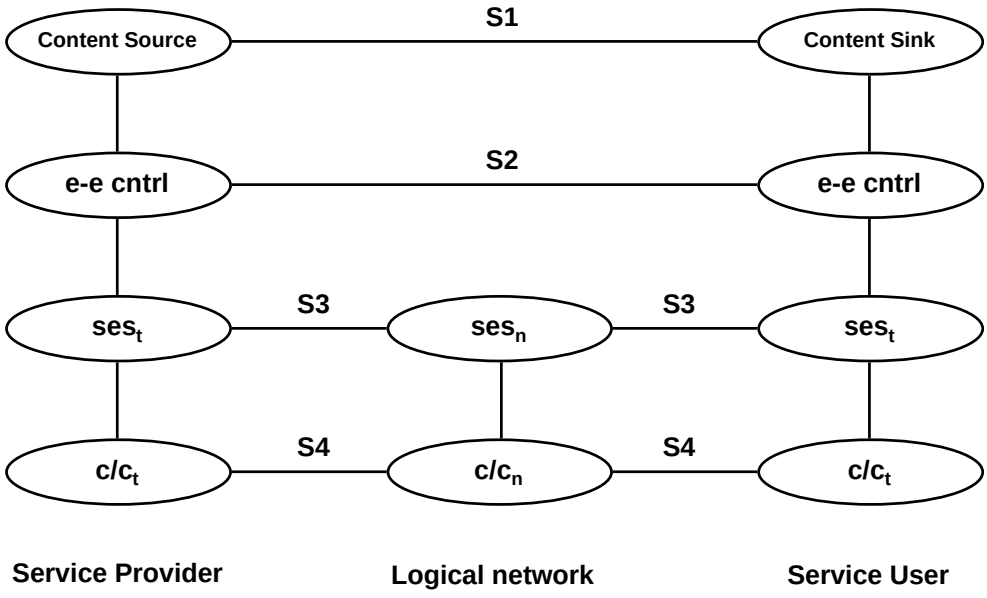


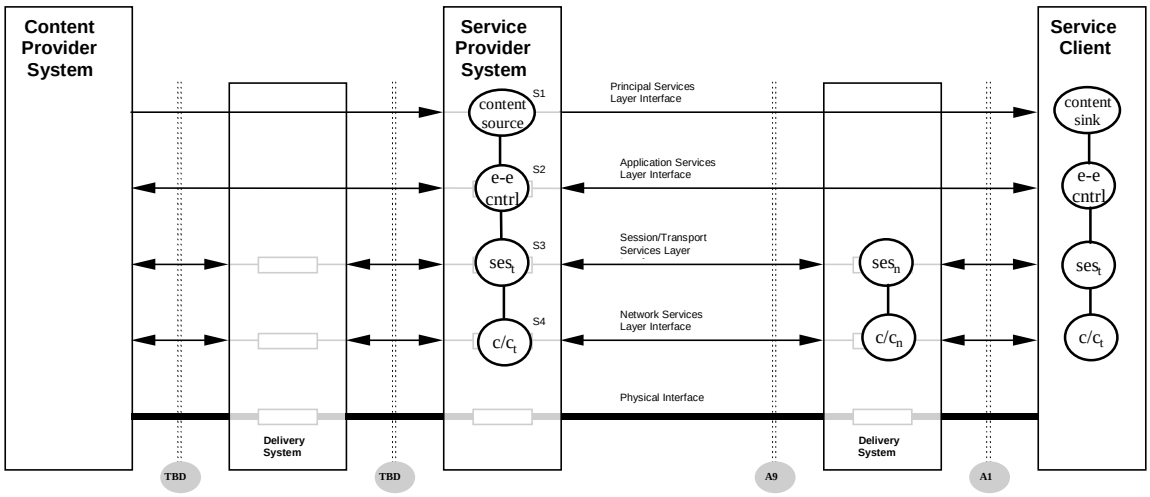
Figure 9.2-1 — Functional Entities and Relationships of a DAVIC System Instance

Figure 9.2-2 shows a mapping of the dynamic functional entities onto the DAVIC static Systems Reference Model. It should be noted that this figure illustrates, for simplicity, only the physical scenario in which the Service Client (i.e., the Set Top Unit) contains call/connection control signaling (c/c(t)). In other scenarios, as shown in Figure 9.2-3, this entity is located within the delivery system, either in the access or core network, and is called "proxy signaling".

 © ISO/IEC – All rights reserved

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale



Note: In some physical scenarios, the c/c$_t$ call/connection control entity shown in the Service Client (I.e., STU) is actually located inside the network (e.g., proxy signalling).

Figure 9.2-2 — Mapping of Dynamic Modeling Functional Entities to Systems Reference Model

9.2.2 Alternative DAVIC Physical Scenarios for the VoD Control Functional Entities

The DAVIC physical scenarios are a particular allocation of control functional entities (e.g., ses(t), ses(n), c/c(t), c/c(n)) to a specific physical entity or location within a DAVIC VoD system (e.g., STU, access network, etc.). This section also includes a physical scenario which describes the case when pre-provisioned connection resources (VP or VC) are utilized .

9.2.2.1 Physical Scenarios for Switched Connections (SVCs)

The three physical scenarios shown in Figure 9.2-3 are supported in DAVIC VoD. Physical scenario 1 is the only scenario supported for HFC when ATM is terminated in the access. All three scenarios are supported for ATM end-to-end. (Additional physical scenarios are introduced in the appropriate sections.)

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

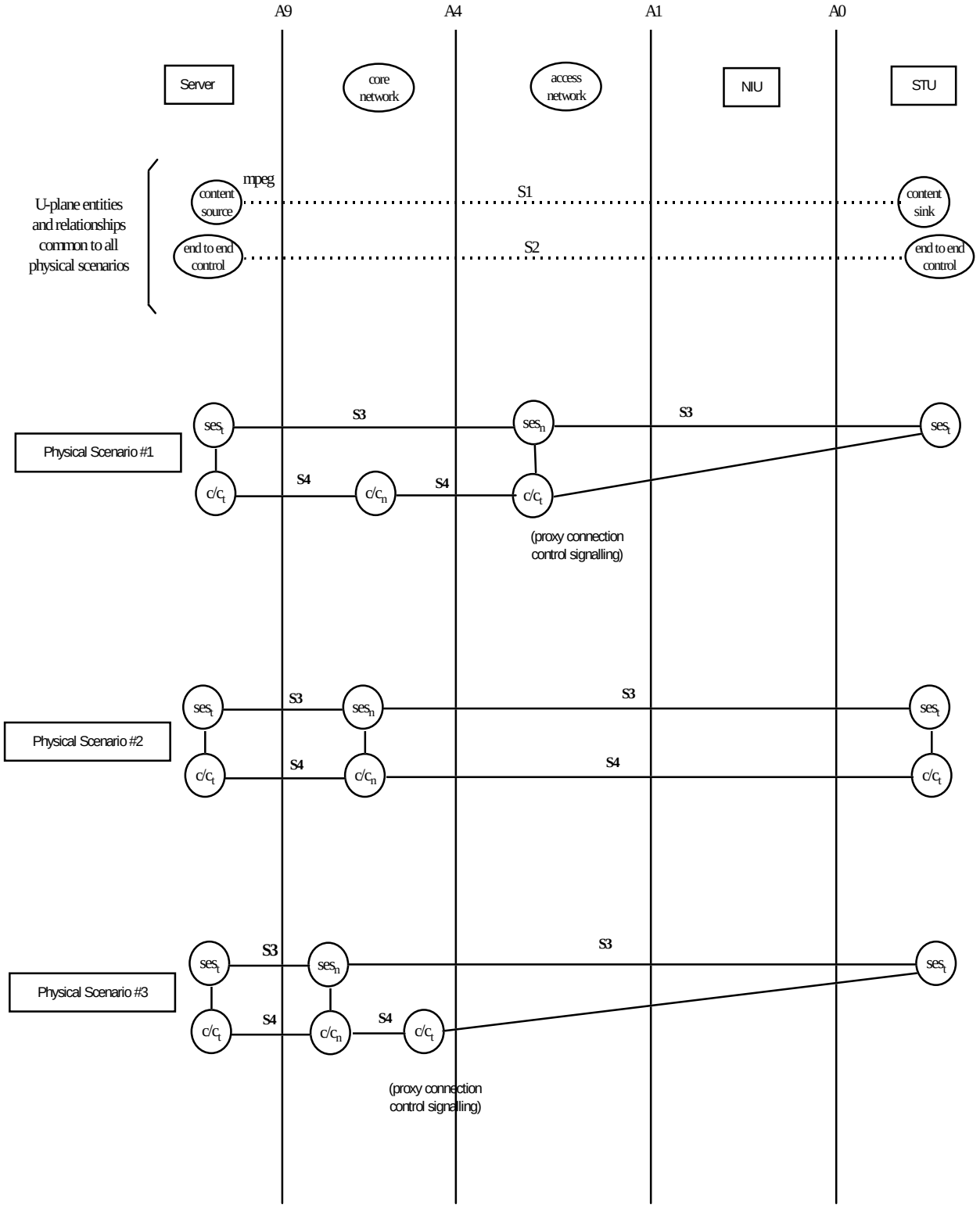


Figure 9.2-3

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

9.2.2.2 Physical Scenario 4, PVC, pre-provisioned connection resources

The physical scenario model depicted in Figure 9.2-4 shows the case where one or more than one static connection resources (VP or VC) are pre-provisioned. Case 4a shows both the ses(n) and CRM (Connection Resource Manager) located in the access whereas Case 4b shows both ses(n) and CRM located in the core network. As is the case for SVC's discussed earlier, only the Scenario 4a is supported for HFC when ATM is terminated in the access. Both 4a and 4b are supported for ATM end-to-end.

In the case of ATM access network, the connection resources may be end-to-end between the STU and the server, or the server side connection resources and the client side connection resources may be separate.

Physical Scenario 4a includes the case where the client side connection resources are not ATM connections but, rather, are HFC-specific resources providing MPEG transport streams. In this case, the CRM has the capability of establishing the connection between the ATM connections on the server side and the HFC resources on the client side.

In both of these scenario's (4a and 4b), the session manager ses(n) is co-located with a functional entity called CRM (Connection Resource Manager). CRM has knowledge about the pre-provisioned connection resources and selects an appropriate VC (and its VCI) when the ses(n) receives the request.

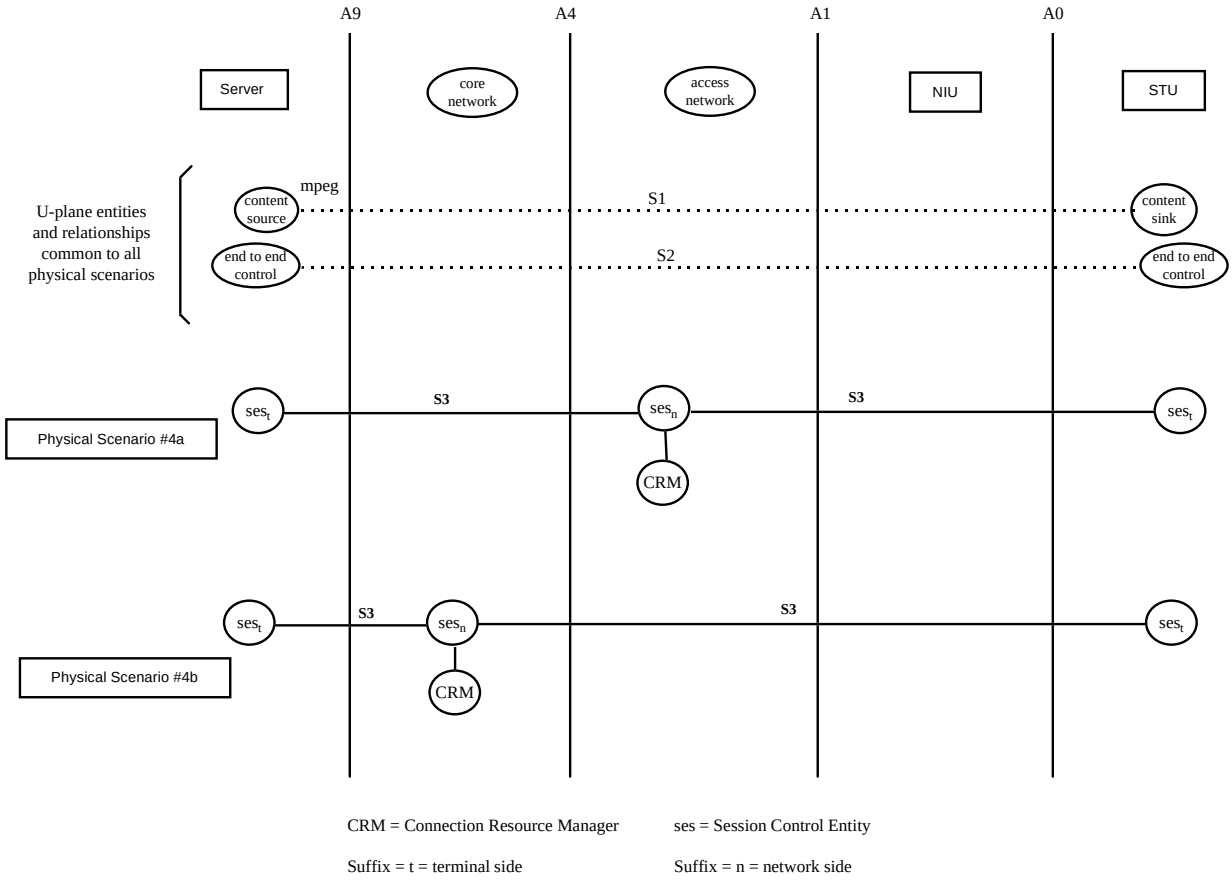


Figure 9.2-4

9.2.3 System Dynamic Flows for VoD

The dynamic behavior of a DAVIC system is described by sequences of information flows which carry information (e.g., parameters) between the control functional entities. Actions taken by functional entities as a result of the information received in these flows are described in clause 9.2.4. The parameters carried in these flows are specified in clause 9.2.5.

When interacting functional entities are located in separate physical equipment or different geographical locations, protocol messages are used to transport these parameters.

--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Figure 9.2-5 illustrates the relationships between functional entities, flows, protocol entities, and protocol messages.

Figure 9.2-6 through Figure 9.2-12 show the dynamic behavior of a DAVIC VoD system. The following dynamic flow scenarios are illustrated:

- Session & Call/Connection Setup
- Resource Add
  - STU-initiated
  - Server-initiated
- Resource Delete
  - STU-initiated
  - Server-initiated
- Transfer of Session & Call/Connections Between Servers
- Service Transfer
- Session & Call/Connection Release:
  - STU-initiated
  - Server-initiated
  - Network-initiated

It should be noted that the STU-initiated Resource Add and Resource Delete are only considered informative rather than normative DAVIC VoD system. However, they are shown here in order to illustrate completeness, consistency, and (optional) extendibility for more symmetrical DAVIC VoD and other systems.

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

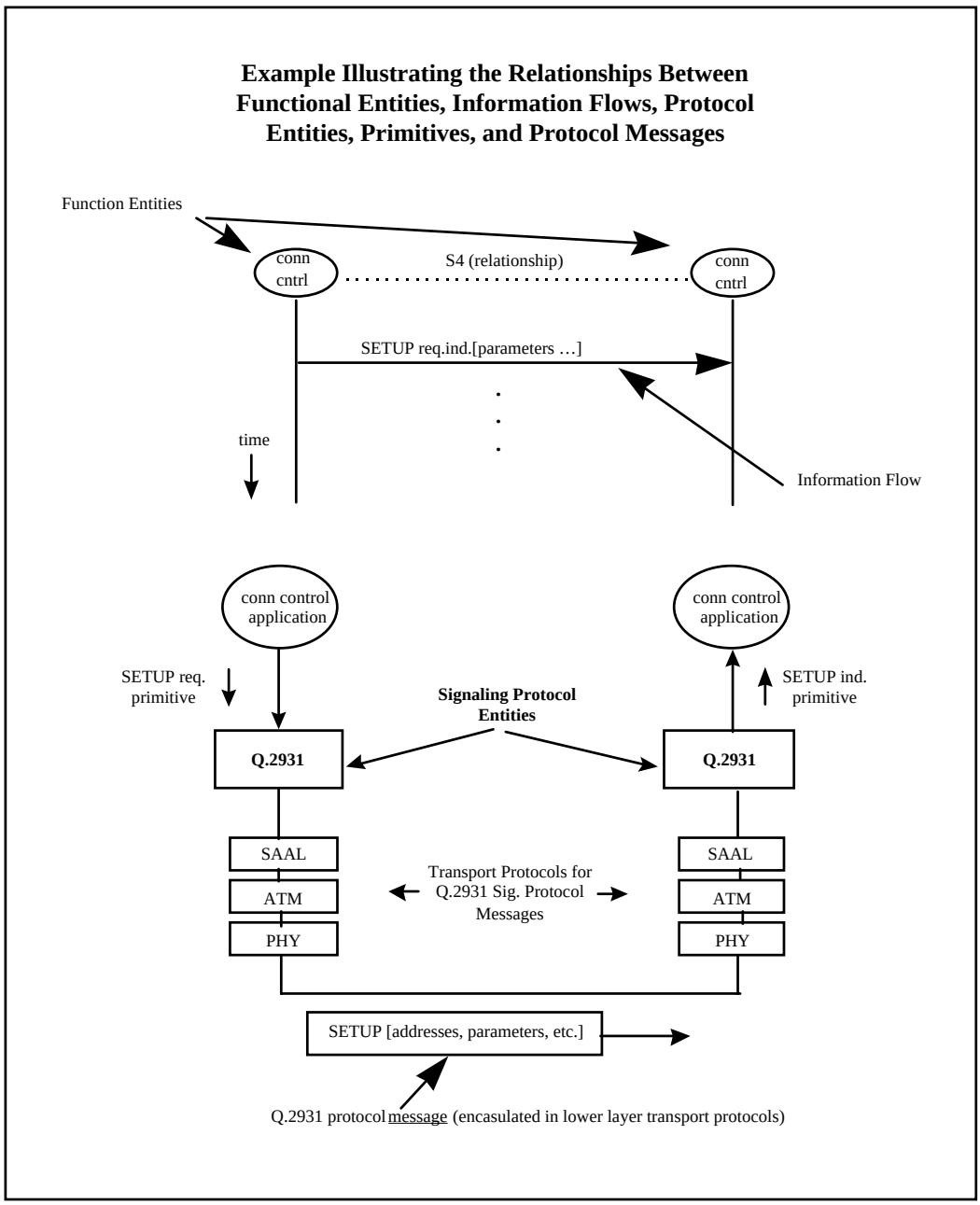


Figure 9.2-5

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

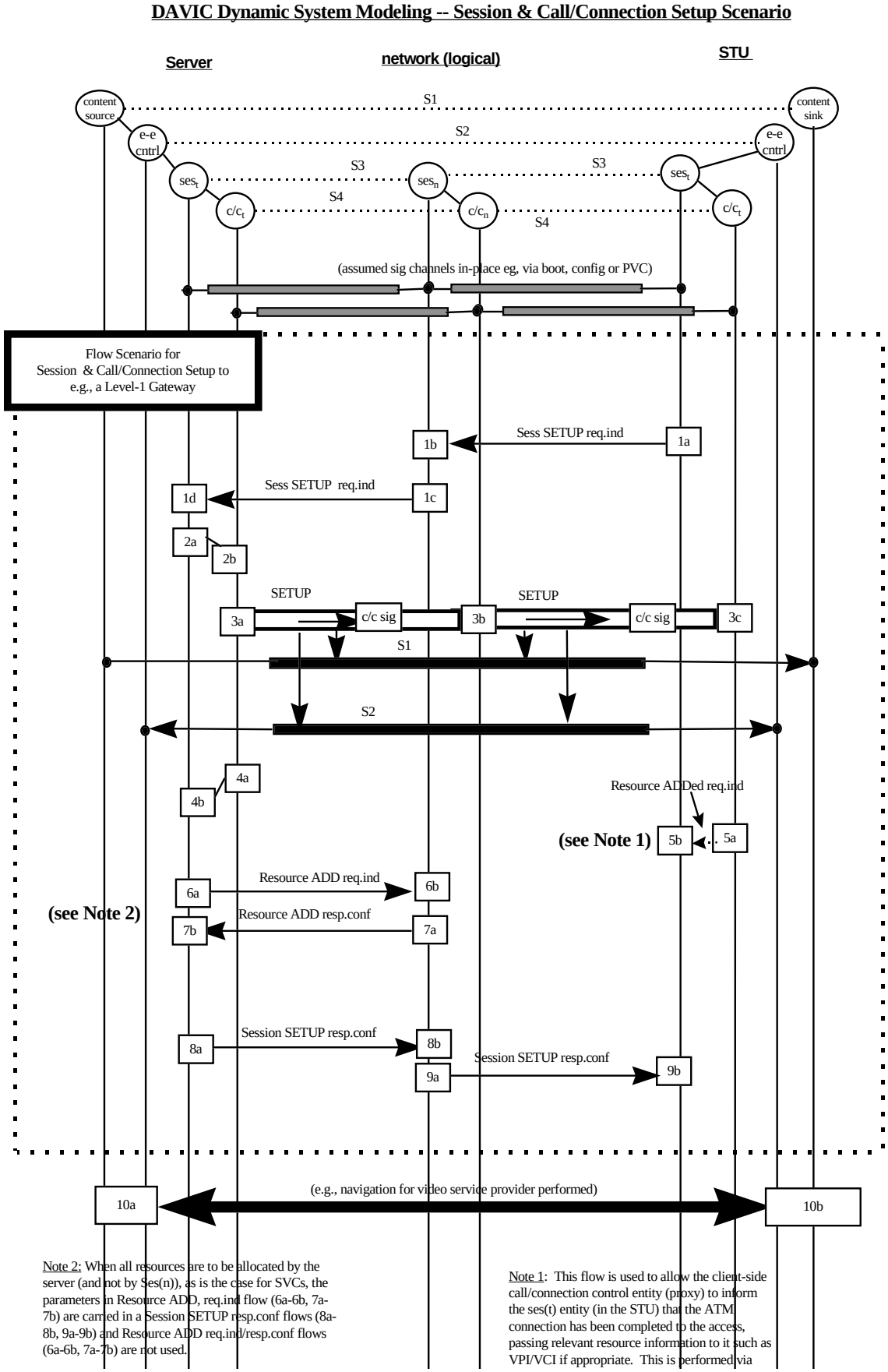


Figure 9.2-6

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

DAVIC Dynamic System Modeling -- Resource Add Scenarios

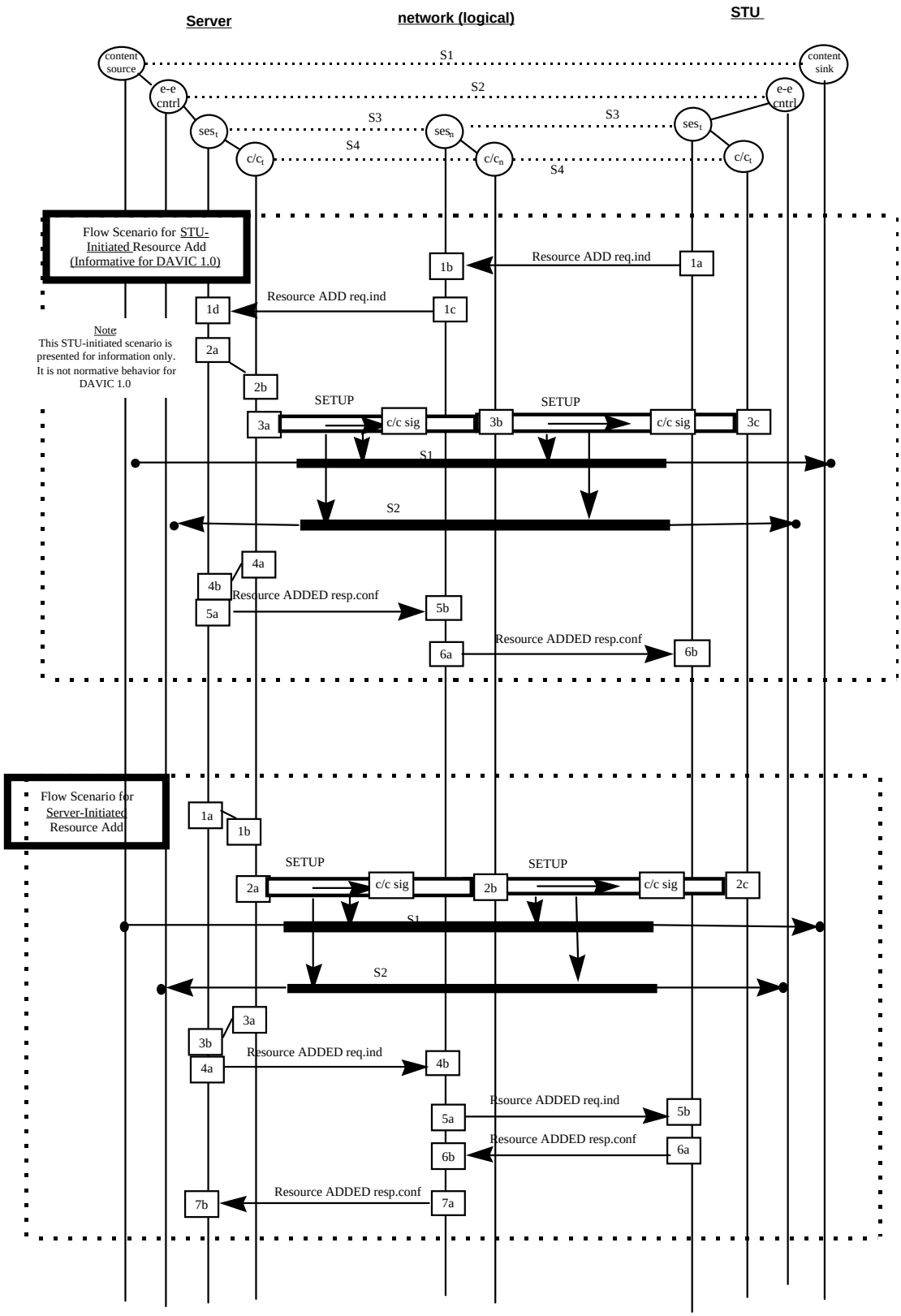


Figure 9.2-7

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

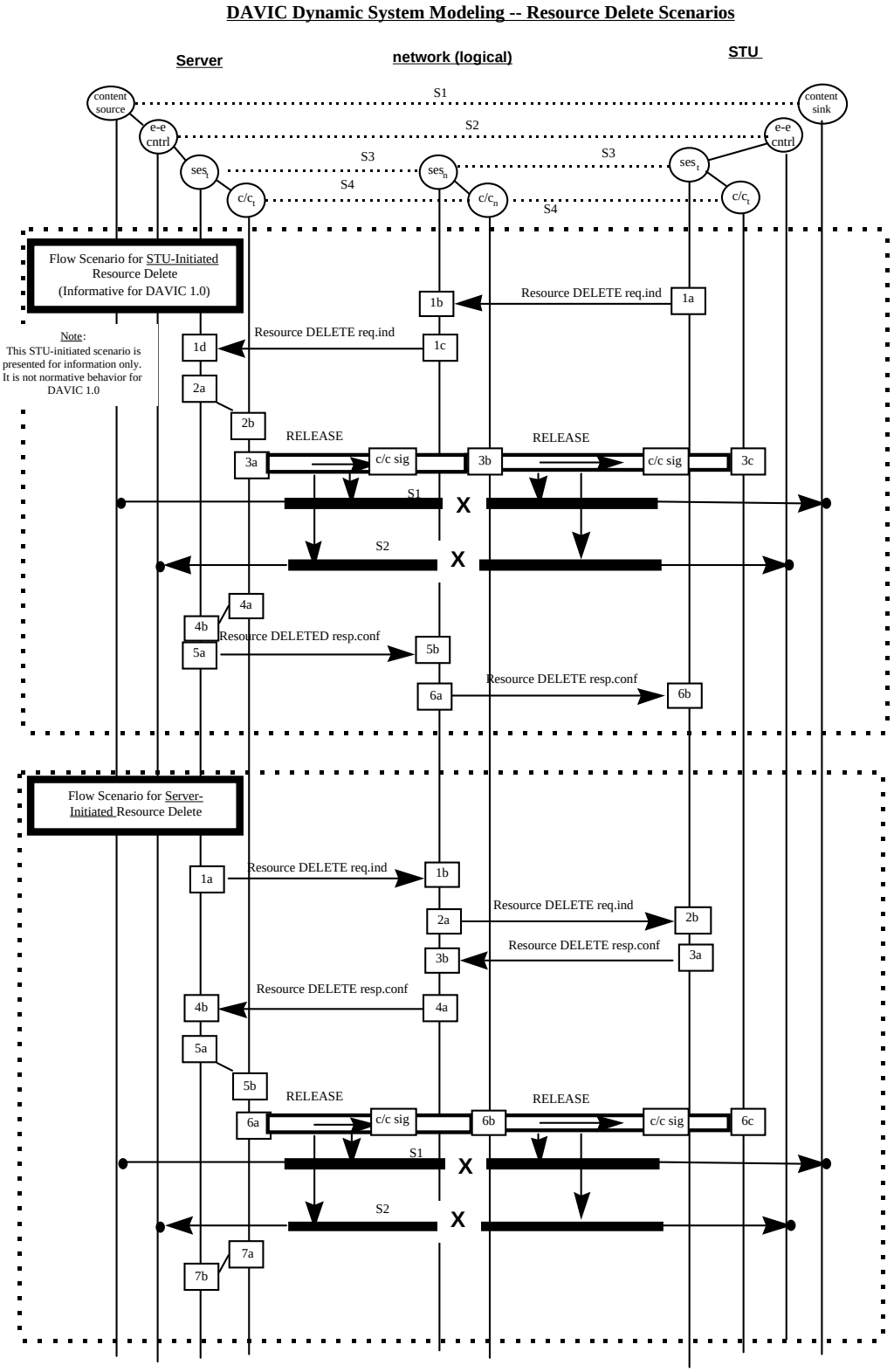


Figure 9.2-8

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

DAVIC Dynamic System Modeling -- Scenario For Transfer of Session & Call/Connections Between Servers

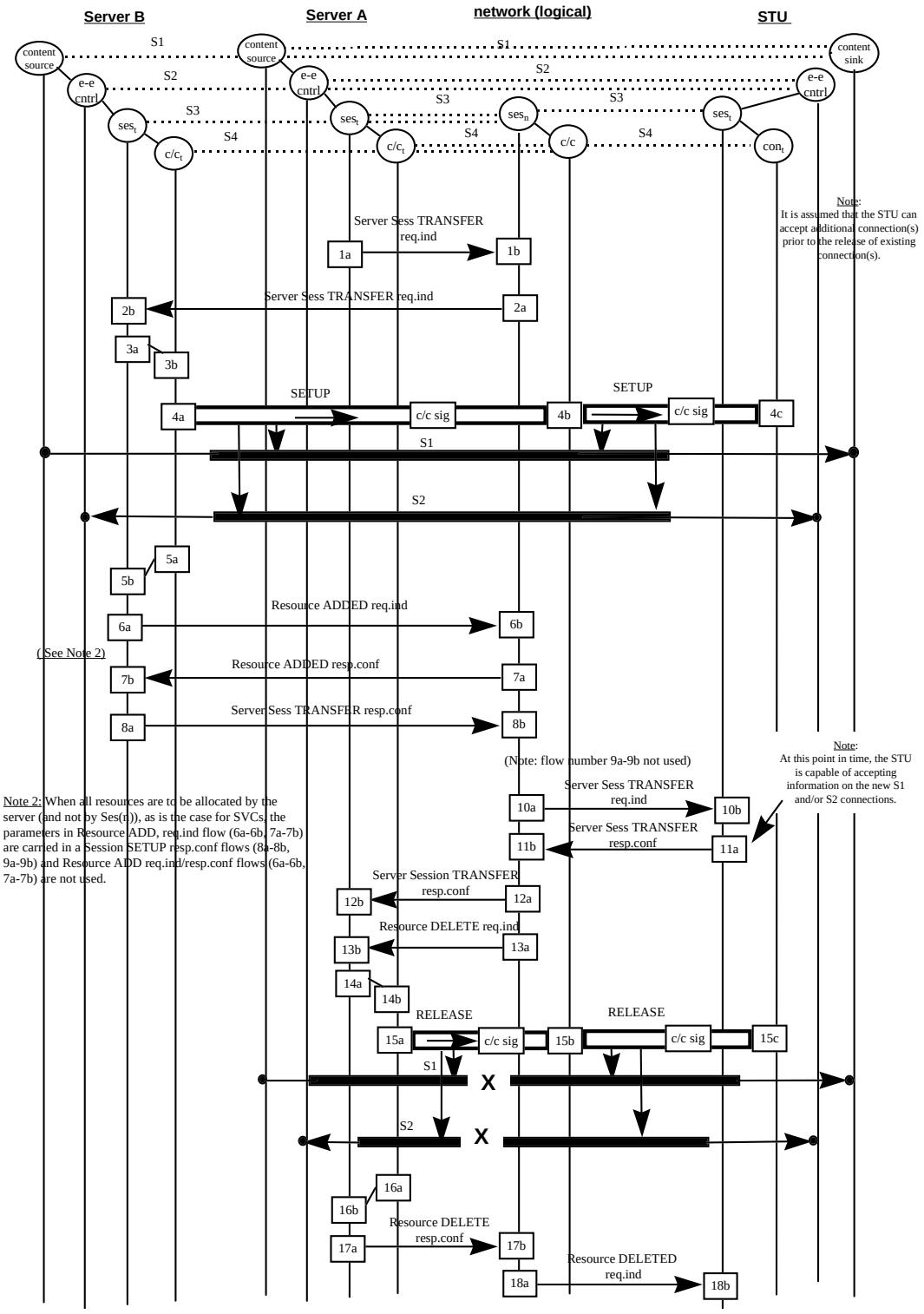


Figure 9.2-9

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

DAVIC Dynamic System Modeling -- Scenario for Service Transfer between between Servers

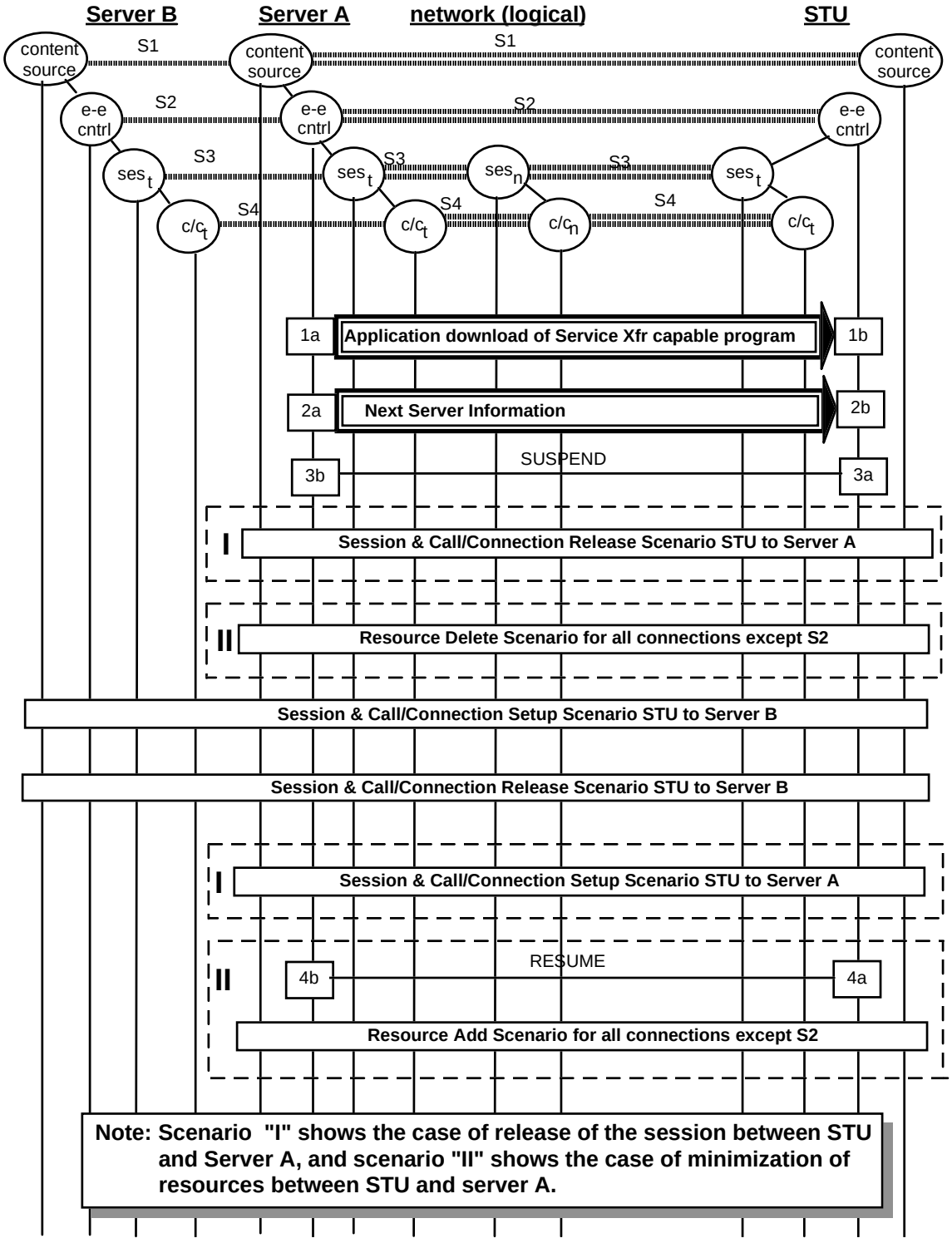


Figure 9.2-10

 © ISO/IEC – All rights reserved

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

DAVIC Dynamic System Modeling -- Session & Call/Connection Release Scenarios

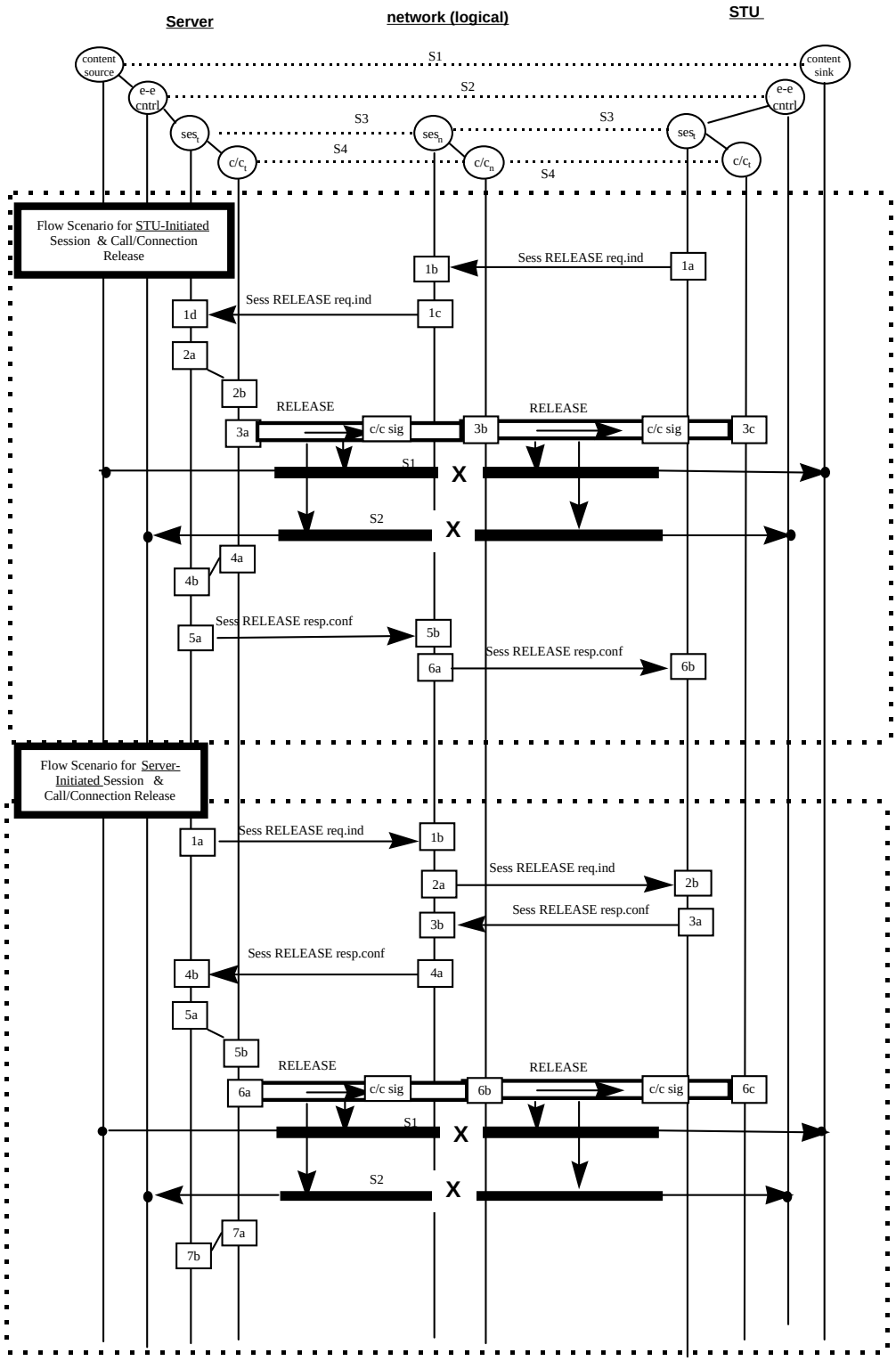


Figure 9.2-11

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

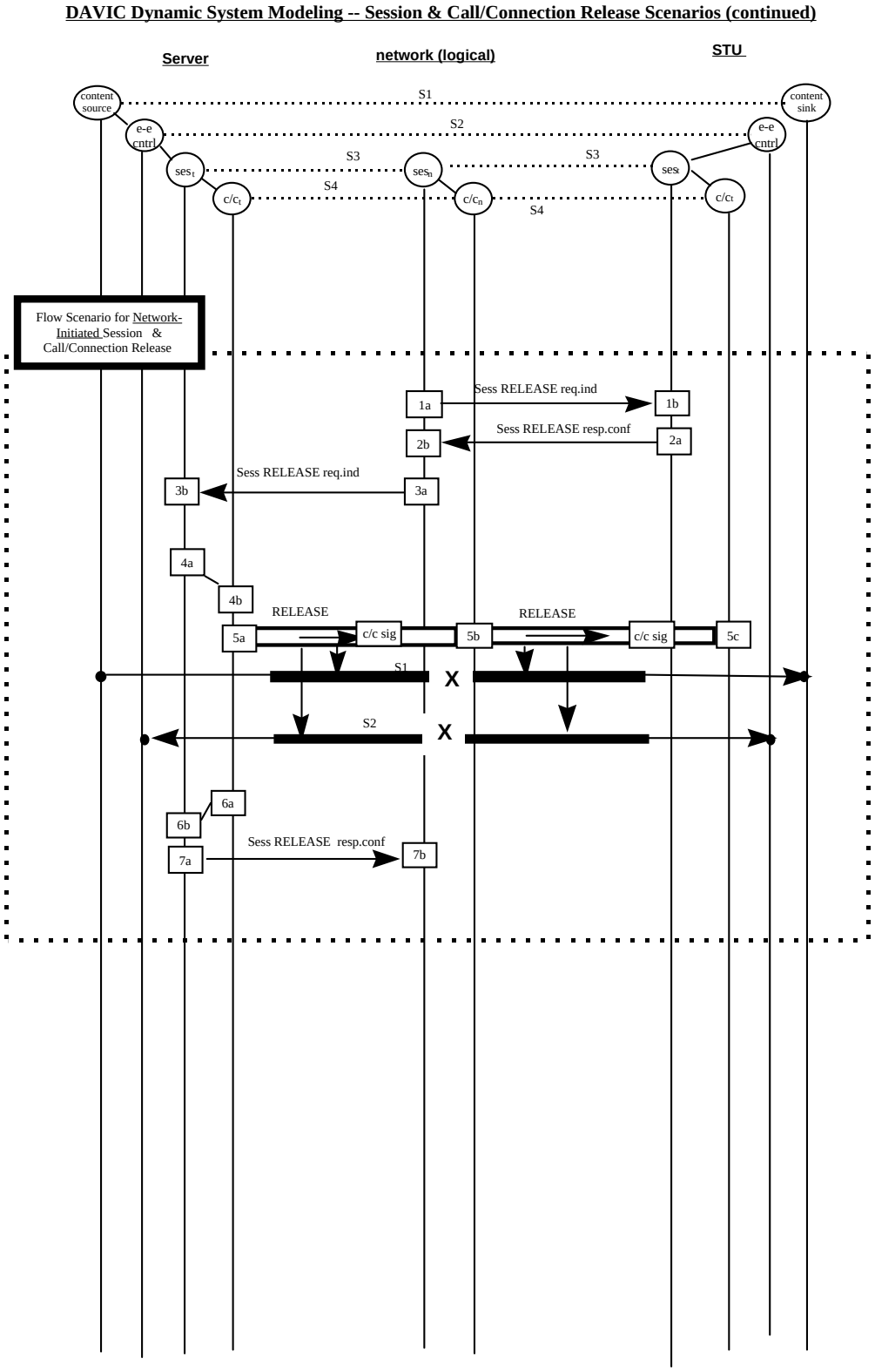


Figure 9.2-12

9.2.4 Functional Entity Actions for VoD

The Functional entity actions provide a description of the actions taken by the DAVIC control functional entities as a result of the information transferred within the ISO/IEC 16500 system flows.

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The Functional Entity Actions are described for both switched (SVC) and pre-provisioned connections (VP or VC) physical scenarios.

9.2.4.1 Functional Entity Actions for the System Flows for Physical Scenarios 1–3 (SVC)

Table 9.2-1 — Session & Call/Connection Establishment

1a–1b	The STU sends a session set-up request indication to the network session entity.
1c–1d	The network sends a session set-up request indication to the Server.
2a–2b	The Server Session entity instructs the Server call/connection entity to set-up S1 and S2 connections from the Server to the STU.
3a–3b–3c	Network connection control signaling is used to establish S2 and optionally S1. (see note 1, note 3)
4a–4b	Server call/connection entity informs the Server session entity of completion of connection establishment.
5a–5b	This flow is only used in physical scenarios 1 and 3. The client-side call/connection control entity (proxy) informs the ses(t) entity that the ATM connection has been completed to the access.
6a–6b	Server informs network of connection set-up. (see note 2)
7a–7b	Network acknowledges the server's connection set-up. (see note 2, note 3)
8a–8b	Server confirms session set-up to the Network.
9a–9b	The Network informs STU of added connection and confirms session set-up. In the physical scenario #3 ATM access network, the network informs the client of the added resources indicating their connection identifiers (VPCI and VCI).
10a–10b	U-Plane communication between STU and server via S1 and S2.

Note 1: A call/connection signaling MACRO is used for each connection establishment.

Note 2: When all resources are to be allocated by the server (and not by Ses(n)), as is the case for SVCs, the parameters in Resource ADD, req.ind flow (6a-6b, 7a-7b) are carried in a Session SETUP resp.conf flows (8a-8b, 10a-10b) and Resource ADD req.ind/resp.conf flows (6a-6b, 7a-7b) are not used.

Note 3: If the connection or resource cannot be added, then the session must be cleared.

Table 9.2-2 — Addition Of Resources (STU Initiated)

1a–1b	STU requests resource addition to Network.
1c–1d	The Network requests resource addition to the Server.
2a–2b	The Server session entity asks the Server call/connection entity to add connection to the session.
3a–3b–3c	Network connection control signaling is used to establish S2 and optionally S1. (see note)
4a–4b	The Server call/connection entity informs the Server session entity of completion of connection establishment.
5a–5b–5c	Server informs network of connection set-up.
6a–6b	The Network informs STU Session entity about added connection resource.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Table 9.2-3 — Addition of Resources (Server Initiated)

1a–1b	The Server session entity asks the Server connection entity to add connection to the session.
2a–2b–2c	Network connection control signaling is used to establish S2 and optionally S1. (see note)
3a–3b	The Server call/connection entity informs the Server session entity of completion of connection establishment.
4a–4b	Server informs network of connection set-up.
5a–5b	The Network informs STU Session entity about added connection resource. In the physical scenario #3, the network also informs the connections identifiers of the added connections.
6a–6b	The STU acknowledges the added connection notification to the Network.
7a–7b	Network acknowledges the server's added connection set-up.

9.2.4.2 Deletion of Resources

Table 9.2-4 — Deletion of Resources (STU Initiated)

1a–1b	STU requests resource deletion to Network.
1c–1d	The Network requests resource deletion to the Server.
2a–2b	The Server session entity asks the Server call/connection entity to Release connection to the session.
3a–3b–3c	Network connection control signaling is used to release S2 and optionally S1. (see note)
4a–4b	The Server call/connection entity informs the Server session entity of completion of connection release.
5a–5b	Server informs network of release of the connection.
6a–6b	The Network informs STU Session entity about the released connection resource.

Table 9.2-5 — Deletion of Resources (Server Initiated Release)

1a–1b	The Server requests release of the connection resource to the Network.
2a–2b	The Network requests release of the connection resource to the STU.
3a–3b	The STU confirms connection resource release to the Network.
4a–4b	The Network confirms connection resource release to the Server.
5a–5b	The Server Session entity requests the Server call/connection entity to Release the connection.
6a–6b 6c	Network Control Signaling is used to Release the Connections.
7a–7b	Server call/connection entity informs the Server session entity of completion of the release of the connection.

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

9.2.4.3 Session Transfer between Servers (under control of ses(n)) (Informative, pending resolution of user-user specification problems in DSM-CC)

Table 9.2-6 - Session Transfer

1a–1b	Server A Session entity requests a transfer to Server B. The request is sent to the Network session entity.
2a–2b	The Network Session entity sends a request for session transfer to Server B.
3a–3b	The Server B Session entity request the Server B call/connection entity to set-up a connection between Server B and the STU. Note: The STU is assumed to be able to accept additional connections for S1 and S2 prior to the release of existing connections for S1 and S2
4a–4b–4c	Network Control Signaling is used to set-up the connection between Server B and the STU.
5a–5b	Server B call/connection entity informs the Server B session entity of the connection establishment between Server B and the STU.
6a–6b	Server B notifies the Network of the completion of the connection establishment.
7a–7b	The Network confirms to Server B the added resources.
8a–8b	Server B acknowledges the session transfer to the Network.
9a–9b	(flow numbered 9a-9b is not used in this dynamic scenario)
10a–10b	The Network session entity informs the STU of the Session transfer request from Server A to Server B. Also, the Network informs the STU of the added connection resources. In the physical scenario #3, the network also informs the STU of the connection identifiers (VCIs) of the newly assigned connections.
11a–11b	The STU confirms Session Transfer.
12a–12b	The Network confirms to Server A the session transfer.
13a–13b	The Network requests to Server A to release the connection resources between Server A and the STU.
14a–14b	Server A session entity requests the Server A call/connection entity to release the connections between Server A and the STU.
15a–15b–15c	The network control signaling is used to release connections between Server A and the STU.
16a–16b	The Server A call/connection entity informs the Server A session entity of completion of release of the connections.
17a–17b	The Server A confirms to the Network release of connections between Server A and the STU.
18a–18b	The Network confirms the release from Server A to the STU.

9.2.4.4 Service Transfer between Servers (under control of ses(n))

Table 9.2-7 - Service Transfer

1a–1b	Server A e-e control downloads the Service Transfer capable program to the STU when or before the STU accesses the service on Server A.
2a–2b	Server A e-e control sends the next server, i.e., Server B and next Service information to the STU and prompts the Service Transfer capable program in the STU to execute a Service Transfer.
3a–3b	The STU e-e control sends a SUSPEND to the Server A e-e control indicating its preference whether it wants to release the session with Server A or wants Server A to minimize the session resources after the service suspension. Note: If the STU does not want to return to Server A, it can execute a normal session release without a suspend context.
4a–4b	In case the STU had requested Server A to minimize its session resources, its e-e control sends the RESUME to the Server A e-e control to resume to full service from the time it left off.

Note: A call/connection signaling MACRO is used for each connection establishment or release.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

9.2.4.5 Session & Call/Connection Release.

Table 9.2-8 - Session Release --STU-Initiated Release

1a–1b	STU requests the Network to Release the Session.
1c–1d	The Network requests the Server to Release the Session.
2a–2b	The Server Session entity requests the Server call/connection entity to Release the connection.
3a–3b–3c	Network Control Signaling is used to Release the Connections.
4a–4b	Server call/connection entity informs the Server session entity of completion of the release of the connection.
5a–5b	The Server confirms the Network the release of the session.
6a–6b	The Network confirms to the STU the release of the session.

Table 9.2-9 - Session Release --Server Initiated Release

1a–1b	The Server requests release of the session to the Network.
2a–2b	The Network requests release of the session to the STU.
3a–3b	The STU confirms session release to the Network. (It is mandatory that the STU perform Session Release upon receipt of flow 2a-2b.)
4a–4b	The Network confirms session release to the Server.
5a–5b	The Server Session entity requests the Server call/connection entity to Release the connection.
6a–6b 6c	Network Control Signaling is used to Release the Connections.
7a–7b	Server call/connection entity informs the Server session entity of completion of the release of the connection.

Table 9.2-10 - Session Release --Network-Initiated Release

1a–1b	The Network requests release of the session to the STU.
2a–2b	The STU confirms session release to the Network. (It is mandatory that the STU perform Session Release upon receipt of flow 1a-1b.)
3a–3b	The Network requests release of the session to the Server.
4a–4b	The Server Session entity requests the Server call/connection entity to Release the connection(s).
5a–5b-5c	Network Control Signaling is used to Release the Connections.
6a–6b	Server call/connection entity informs the Server session entity of completion of the release of the connection.
7a–7b	Server session entity informs the Network session entity of completion of the release of the Session and connection(s).

9.2.4.6 Functional Entity Actions for the Physical Scenario #4, (pre-provisioned VPs or VCs)

Note: For the physical scenario #4, only for the case where the connection resources of the both ends are pre-provisioned ATM connection resources are described.

The following amendments have been made to 9.4.1 to reflect the functional entity actions required for the Physical Scenario #4.

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Table 9.2-11 - . Session & Call/Connection Establishment (PVC Case)

6a–6b	In the physical scenario #4, the server requests connection resources.
6b–7a	In the physical scenario #4, the network selects appropriate connections for the server and the client and adds them to the session. If the server side connections and the client side connections are separate, the network connects the server side connections with the client side connections.
7a–7b	In the physical scenario #4, the network also confirms the requested resources and sends the connection identifiers (VPCI and VCI) of the resources.
9a–9b	In the physical scenario #4, the network informs the client of the added resources indicating their connection identifiers (VPCI and VCI).

9.2.4.7 Addition of Resources

Table 9.2-12 - Addition of resource (STU Initiated) (PVC)

1a–1b	The client requests resources.
1b–1c	In the physical scenario #4, the network selects the appropriate connections for the Server and the STU and adds them to the session. If the server side connections and the client side connections are separate, the network connects the Server side connections with the client side connections.
1c–1d	In the physical scenario #4, the network also informs the connections identifiers of the added connections.
2a–2b	In the physical scenario #4, this step is skipped.
3a-3b-3c	In the physical scenario #4, this step is skipped.
4a–4b	In the physical scenario #4, this step is skipped.
6a–6b	In the physical scenario #4, the network confirms the requested connections and informs the Server of the connection identifiers of the added connections.

Table 9.2-13 - Addition of resource (Server Initiated)—(PVC)

1a–1b	In the physical scenario #4, this step is skipped.
2a-2b-2c	In the physical scenario #4, this step is skipped.
3a–3b	In the physical scenario #4, this step is skipped.
4a–4b	In the physical scenario #4, the Server requests resources.
4b–5a	In the physical scenario #4, the network selects the appropriate connections for the Server and the STU and adds them to the session. If the server side connections and the client side connections are separate, the network connects the Server side connections with the client side connections.
5a–5b	In the physical scenario #4, the network also informs the connections identifiers of the added connections.
7a–7b	In the physical scenario #4, the network confirms the requested connections and informs the Server of the connection identifiers of the added connections.

9.2.4.8 Deletion of Resources

Table 9.2-14 - Deletion of resources (STU Initiated)—(PVC)

5b–6a	In the physical scenario #4, the network removes the connections from the session. If the client side connections are associated with the server side connections, the network clears this association.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Table 9.2-15 - Deletion of Resources (Server Initiated) (PVC)

3b–4a	In the physical scenario #4, the network removes the connections from the session. If the client side connections are associated with the server side connections, the network clears this association.

9.2.4.9 Session Transfer (PVC) (Informative, pending resolution of user-user specification problems in DSM-CC)

Table 9.2-16 - Session Transfer—(PVC)

6a–6b	In the physical scenario #4, the Server B requests connection resources.
6b–7a	In the physical scenario #4, the network selects appropriate connections for the Server B and the client. If the server side connections and the client side connections are separate, the network associates the client side connections and the server side connections. Some of the client side connections used in the session with the Server A may be reused in the new session with the Server B. In such cases, the network clears the association between the client side connections and the Server A side connections, and then re-associates the client side connections with the connections for the Server B.
7a–7b	In the physical scenario #4, the network confirms the connection resource request and informs the Server of the connection identifies (VCIs) of the newly assigned connections.
9a–9b	In the physical scenario #4, the network also informs the STU of the connection identifiers (VCIs) of the newly assigned connections.
12a–13a	In the physical scenario #4, the network clears the remaining association between the client side connections and the Server A side connections.

9.2.4.10 Session Release

Table 9.2-17 - Session release (STU Initiated)—(PVC)

5b–6a	In the physical scenario #4, the network removes the connections from the session. If the client side connections are associated with the server side connections, the network clears this association.

Table 9.2-18 - Session Release (Server Initiated) (PVC)

3b–4a	In the physical scenario #4, the network removes the connections from the session. If the client side connections are associated with the server side connections, the network clears this association.

9.2.5 DAVIC Dynamic Flow Parameters for VoD

The following tables show the parameters, which are included in the message flows of clause 9.3. The column "Flow" references the individual message flow as in clause 9.3, "Status" highlights whether the parameter is included in the current specification, or whether is needs further examination, "Parameter" is the name of the parameter and "Comment" identifies the value and semantics, which goes with the parameter.

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

9.2.5.1 Session & Call/Connection Setup Scenario (Normative)

Table 9.2-19

Flow	*Status*	*Parameter*	*Comment*
1a–1b Ses SETUP req.ind		session_id	uniquely assigned by STU, = device_id & arbitrary additional value, unique on this STU
		client_id	E.164 NSAP address at the A1 interface of the client.
		server_id	E.164 NSAP address at the A9 interface of the server.
		compatibility_descriptor	conveys a list of specific Hardware/Software at the STU available to the server.
		service_info	= rPathSpec, indicates to the server initial service specific information, e.g., about service selection = (initial) service name
1c–1d Sess SETUP req.ind		session_id	identical to 1a–1b
		client_id	identical to 1a–1b, with the possibility that the SESn replaces the physical address by a logical address (e.g., for reasons of privacy)
		server_id	physical NSAP E.164 address of the Server which the STU wants to establish a session with (identical to 1a–1b. If in 1a–1b a logical address was used, this address has to be replaced by the physical address for this step).
		compatibility_descriptor	identical to 1a–1b
		service_info = rPathSpec	identical to 1a–1b
2a–2b ses(t)-c/c(t) flow in Server		session_id	identical to step 1
		client_ATM_id	physical or logical E.164 address of the port, the STU is connected to, possibly including a sub-address, based on client_id of step 1c-1d.
		resource_#, resource_attribute(s)	uniquely assigned by the Server, parameters which describe the ATM connection(s) to be set up: - bandwidth - QoS - any other necessary parameters, such as AAL parameters, broadband bearer capabilities, etc.
3a–3b–3c Connection setup		all c/c signaling parameters	see ISO/IEC 16500-5, Clause 9.3.1.3
4a–4b c/c(t)-ses(t) flow in Server		session_id	identical to step 2 = 1
		resource_#	as in step 2
		status_id	indicates status and reason of requested resource (e.g., OK or failed, because of…)
		VPI/VCI	correlates ATM connection identifiers with resource identifier
5a–5b Resource ADD req.ind		session_id	identical to step 4 = 1
		VPI/VCI (as seen by STU!)	correlates ATM connection identifiers with resource identifier
		status_id	indicates status and reason of requested resource (e.g., OK or failed, because of…)
			Note: See Note 1 in Clause 9.2.1 and Note 2 on Fig. 9-6.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

6a–6b Resource ADD req.ind		session_id	identical to step 4 = 1 (However, see Note 2 in Clause 9.4.1.1)
		resource_# (as seen by the server), resource_group_tag_# resource_descriptor(s)	
		service_context_list	= connection_binding_list: indicates the "usage" of the resource in the context of the application, e.g., "S1".
7a–7b Resource ADD resp.conf		session_id	identical to step 6 = 1 (However, see Note 2 in Clause 9.4.1.1)
		resource_# (as seen by the server), resource_descriptor(s)	identical to step 6 = 1
8a–8b Session SETUP resp.conf		session_id	identical to step 7 = 1 (However, see Note 2 in Clause 9.4.1.1)
9a–9b Session SETUP resp.conf		session_id	identical to step 8 = 1 (However, see Note 2 in Clause 9.4.1.1)
		service_context_list	identical to step 6
		resource_# (as seen by the STU), resource_group_tag# resource_descriptor(s)	identical to step 6

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

9.2.5.2 Add Resource Scenario—STU initiated (Informative)

Table 9.2-20

Flow	*Status*	*Parameter*	*Comment*
1a–1b Resource ADD req.ind		session_id	uniquely assigned by STU, = device_id & arbitrary additional value, unique on this STU
		resource_# (as seen by the STU), resource_group_tag# resource_descriptor(s)	describes the resources the STU asks for.
		service_context_list	= connection_binding_list: indicates the "usage" of the resource in the context of the application, e.g., "S1".
1c-1d Resource ADD req.ind		sesson_id	see 1a-1b
		resource_# (as seen by the server), resource_group_tag# resource_descriptor	identical to 1a-1b
		service_context_list	identical to 1a-1b.
2a-2b SESSt-CONt flow in Server		session_id	identical to step 1
		client_ATM_id	physical or logical E.164 address of the port, the STU is connected to possibly including a sub-address, based upon session_id.
		resource_# resource_attribute(s)	uniquely assigned by the STU, parameters which describe the ATM connection(s) to be set up: bandwidth QoS any other necessary parameters, such as AAL parameters, broadband bearer capabilities, etc.
3a–3b–3c Connection Setup		all c/c signaling parameters	see ISO/IEC 16500-5, Clause 9.3.1.2
4a–4b CONt-SESSt flow in Server		session_id	identical to step 2 = 1
		resource_#	as in step 2
		status_id	indicates status and reason of requested resource (e.g., OK or failed, because of…)
		VPI/VCI	correlates ATM connection identifiers with resource identifier
5a–5b Resource ADDed resp.conf		session_id	identical to step 4 = 1
		resource_# (as seen by STU), resource_group_tag# resource_descriptor(s)	(Note: The resource_# is considered one element of the resource_descriptor) It still has to be clarified, at which level of detail information is needed for this flow.
		response	indicates whether the request to add resource has been successful.
6a–6b Resource ADDed resp.conf		session_id	identical to step 5 = 1

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

		resource_#, resource_descriptor(s)	identical to 5a-5b.
		response	identical to 5a-5b

 © ISO/IEC – All rights reserved

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

9.2.5.3 Add Resource Scenario—Server-initiated (Normative)

Table 9.2-21

Flow	*Status*	*Parameter*	*Comment*
1a–1b SESSt-CONt flow in Server		session_id	The identifier of the session that connections to be created are added to.
		client_ATM_id	physical or logical E.164 address of the port, the STU is connected to, possibly including a sub-address, based on client_id of step 1c-1d of Session & Call/Connection Setup Scenario within this sub-section.
		resource_#, resource_attribute(s)	uniquely assigned by the Server, parameters which describe the ATM connection(s) to be set up: - bandwidth - QoS - any other necessary parameters, such as AAL parameters, broadband bearer capabilities, etc.
2a–2b–2c Connection setup		all c/c signaling parameters	See ISO/IEC 16500-5, Clause 9.3.1.2
3a–3b CONt-SESSt flow in Server		session_id	identical to the one in step 1
		resource_#	identical to the one in step 1
		status_id	indicates status and reason of requested resource (e.g., OK or failed, because of…)
		VPI/VCI	correlates ATM connection identifiers with resource identifier
4a–4b Resource ADD req.ind		session_id	identical to the one in step 1
		resource_# (as seen by server), resource_group_tag# resource_descriptor(s)	identical to the one in step 1.
		service_context_list	=connection_binding_list: indicates the usage of the resources in the context of the application, e.g., S1. Note: DAVIC has to agree on the semantics and usage of this field.
5a–5b Resource ADDed req.ind		session_id	identical to the one in step 1
		resource_# (as seen by STU), resource_group_tag# resource_descriptor(s)	the number and the descriptor for the added resources that are visible to the client.
		service_context_list	identical to the one in step 4
6a–6b Resource ADDed req.ind		session_id	identical to the one in step 1
		resource_# (as seen by STU), resource_group_tag# resource_descriptor(s)	identical to the one in step 5 except the status code.
7a–7b Resource ADD resp.conf		session_id	identical to the one in step 1

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

		resource_# (as seen by server), resource_group_tag# resource_descriptor(s)	identical to the one in step 4 except the status code.

9.2.5.4 Delete Resource Scenario—STU-initiated (Informative)

Table 9.2-22

Flow	*Status*	*Parameter*	*Comment*
1a–1b		session_id	identifier of the session, resources shall be deleted from
		resource_id(s) (as seen by STU), (resource_count)	parameters which describe the ATM connection(s) to be deleted
2a–2b		resource_id(s) (as seen by server), (resource_count)	parameters which describe the ATM connection(s) to be deleted
3a–3b–3c		all c/c signaling parameters	see ISO/IEC 16500-5, Clause 9.3.1.2
4a–4b		resource_id(s), (resource_count)	parameters which describe the ATM connection(s) deleted
5a–5b		session_id	identical to step 1
		resource_id(s) (as seen by server), (resource_count)	parameters which describe the ATM connection(s) deleted
6a–6b		session_id	identical to step 1
		resource_id(s) (as seen by STU), (resource_count)	parameters which describe the ATM connection(s) deleted

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

9.2.5.5 Delete Resource Scenario—Server-initiated (Normative)

Table 9.2-23

Flow	*Status*	*Parameter*	*Comment*
1a–1b Resource DELETE req.ind		session_id	identifier of the session, resources shall be deleted from
		resource_id(s) seen by server), (resource_count)	parameters which describe the ATM connection(s) to be deleted
		reason	indicates the reason the connection has been requested to be released
2a–2b Resource DELETE req.ind		session_id	identical to 1
		resource_id(s) (as seen by STU), (resource_count)	parameters which describe the ATM resources to be deleted.
		reason	identical to 1
3a–3b Resource DELETE resp.conf		session_id	identical to 2
		resource_id(s) (as seen by STU), (resource_count)	identical to 2 = 1
		response	indicates the response from the STU. Possible values are specified by DSM-CC
4a–4b Resource DELETE resp.conf		session_id	identical to 3 = 1
		resource_id(s) (as seen by server), (resource_count)	identical to 1
		response	identical to 3
5a–5b SESt–c/ct RELEASE message		resource_id(s), (resource_count)	parameters which describe the ATM connection(s) to be deleted
6a–6b–6c ATM call RELEASE signaling		all c/c signaling parameters	see ISO/IEC 16500-5, Clause 9.3.1.2
7a–7b c/ct–SESt RELEASE message		resource_id(s), (resource_count)	parameters which describe the ATM connection(s) deleted

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

9.2.5.6 Session and Call/Connection Release Scenarios—STU-Initiated (Normative)

Table 9.2-24

Flow	*Status*	*Parameter*	*Comment*
1a–1b Sess RELEASE req.ind		session_id	identifier of the session to be released, obtained from Sess SETUP req.ind in Session & Call/Connection Setup Scenario within this subsection.
		reason	indicates the reason the session has been requested to be released
1c–1d Sess RELEASE req.ind		session_id	identical to 1a–1b
		reason	identical to 1a–1b
2a–2b SESt–C/Ct server internal communication		session_id	identical to 1
		resource_#(s)	identifies all the resources within the session to be released
3a–3b–3c		none	all ATM connections are released, not parameters are exchanged
4a–4b C/Ct–SESt server internal communication		session_id	identical to 2 = 1
5a–5b		session_id	identical to 4 = 1
		response	indicates the status of the session release request
5a–5b		session_id	identical to 5 = 1
		response	identical to 5 = 1

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

9.2.5.7 Session and Call/Connection Release Scenario—Server-Initiated (Normative)

Table 9.2-25

Flow	*Status*	*Parameter*	*Comment*
1a–1b Sess RELEASE req.ind		session_id	identifier of the session to be released, obtained from Sess SETUP req.ind in Session & Call/Connection Setup Scenario within this subsection.
		reason	indicates the reason the session has been requested to be released
2a–2b		session_id	identical to 1
		reason	identical to 1
3a–3b		session_id	identical to 2 = 1
		response	indicates client's response to the session release request
4a–4b		session_id	identical to 3 = 1
		response	indicates the status of the session release request
5a–5b SESt-C/Ct flow in server		resource # (s), resource_count	parameters which identify the ATM connection(s) to be released and the session the connections) are associated with.
6a–6b–6c Connection release		all c/c signaling parameters	see ISO/IEC 16500-5, Clause 9.3.1.2
7a–7b C/Ct-SESt flow in server		status_id	indicates the status of the ATM connections subsequent to the release request

© ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

9.2.5.8 Transfer of Session Between Servers (under the control of ses(n)) (Informative, pending resolution of user-user specification problems in DSM-CC)

Table 9.2-26

Flow	*Status*	*Parameter*	*Comment*
1a–1b		session_id	identifier of the session to be transferred
		server_B_id	physical or logical NSAP E.164 address of the server, the session shall be transferred to.
		service_info	information for indication to the server B initial service specific information, e.g., about service selection, user related information, e.g., authentication information
		resource_#, resource_group_tag_# resource_descriptor(s) (as seen by server)	parameters which identify the ATM resources currently (still) existing in the session
2a–2b		session_id	identical to 1
		client_id	E.164 NSAP address, which includes: AFI = 45 E.164 = E.164 (native) address of the UNI at A1, which is the physical location of the UNI of the STU. HO-DSP = IP address of STU, which is assumed to be assigned during network configuration ESI = (unique) MAC address of the STU, which is assumed to burned in by the manufacturer SEL = DAVIC reserved, default = all 0 The coding of these fields is described in ISO/IEC 8348 (See Session & Call/Connection Setup Scenario within this subsection.)
		server_A_id	logical or physical NSAP E.164 address of the Server from which the session is transferred
		resource_# , resource_group_tag_#	parameters which identify the ATM connections currently (still) existing in the session)
		resource_descriptor(s) (as seen by server)	This allows server B to derive the bandwidths and resources currently allocated to the session.
		service_info	identical to 1
3a–3b SESt-C/Ct flow in Server		session_id	identical to 1
		client_ATM_id	physical or logical E.164 address of the port, the STU is connected to, possibly including a sub-address, based on client_id of step 2a–2b.
		resource_#, resource_attribute(s)	uniquely assigned by the Server, parameters which describe the ATM connection(s) to be set up: - bandwidth - QoS - any other necessary parameters, such as AAL parameters, broadband bearer capabilities, etc.
4a–4b–4c Connection setup		all c/c signaling parameters	see ISO/IEC 16500-5, Clause 9.3.1.2 (These connections are new additional ATM connections which terminate at the STU. There may be situations, where the STU is not capable of accepting these additional connections. This will result in a session transfer reject by Server B. See step 8a–8b It)

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

5a–5b CONt-SESt flow in Server		session_id	identical to step 3 = 1
		resource_#(s)	identical to step 3
		status_id	indicates status and reason of requested resource (e.g., OK or failed, because of…)
		VPI/VCI	correlates ATM connection identifiers with resource identifier
6a–6b Resource ADD req.ind		session_id	identical to step 5 = 1
		resource_# (as seen by server), resource_group_tag# resource_descriptor(s)	
		service_context_list	= connection_binding_list: indicates the 'usage' of the resource in the context of the application, e.g., 'S1'.
7a–7b Resource ADD resp.conf		session_id	identical to step 6 = 1
		resource_# (as seen by server), resource_descriptor(s)	identical to step 6 = 1
8a–8b		session_id	identical to step 7 = 1
		response	indicates why the session transfer was accepted (or not)
9a–9b		(this 9a-9b flow is not used in this scenario)	
10a–10b		session_id	identical to step 8 = 1
		resource_# (as seen by STU) , resource_group_tag# resource_descriptor(s)	identical to step 6 = 1
		service_context_list	= connection_binding_list: indicates the 'usage' of the resource in the context of the application, e.g., 'S1'.
		reason	indicates to the STU, why the session transfer was not accepted by Server B (if this is the case), e.g., 'not sufficient resources'
11a–11b		session_id	identical to step 10 = 1
		response	indicates why the session transfer was accepted (or not) by the STU
12a–12b		session_id	identical to step 11 = 1
		response	indicates why the session transfer was accepted (or not) by the STU or server B.
13a–13b		session_id	identical to step 12 = 1
		reason	indicates the reason the session has been requested to be released.
14a–14b SESt–CONt server internal communication		session_id	identical to 13 = 1
		resource_#(s)	identifies all the resources within the session to be released
15a–15b–15c		none	all ATM connections are released, not parameters are exchanged.
16a–16b CONt–SESt server internal communication		resource_#(s)	identifies all the resources within the session to be released
17a–17b		session_id	identical to 14 = 1

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

		resource_id(s), (resource_count)	parameters which describe the ATM connection(s) deleted
18a–18b		session_id	identical to 17 = 1
		resource_id(s), (resource_count)	identical to 17

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

9.2.5.9 Flow Scenario: Service Transfer between Servers

Table 9.2-27

1a-1b Service Transfer capable program application Download			Application download is carried at the beginning when the specific service is accessed in Server A from which the transfer is initiated.
2a-2b Next Server information		server_id	this is the server_id of Server B in standard IDL format
		service_info	=rPathSpec, used below to indicate to the Server B initial service specific information, e.g., about service selection = (initial) service name.
		ticket_info	this contains an encrypted form of the ticket the STU uses when establishing a session with Server B indicating that the issuer is Server A and relates to a specific prior contract with Server B for billing and commission reimbursements. It may also include the aPrincipal (an end-user identification as received from the STU) for security.
3a-3b SUSPEND		suspend_reason	the STU indicates its preference if the UserContext on Server A must be suspended or the resources minimized. Below scenario I covers the case when the session with Server A is released and Scenario II covers the case when the session with Server A is kept but its resources are minimized
		user_context	the Server A provides the UserContext from which the service on Server A will be resumed in full when STU returns to Server A.
Scenario I Session & Call/Connection Release		parameters as in STU initiated Session and Call/Connection Release Scenario	STU releases its session with Server A after receiving the user_context from 3
Scenario II Resource Delete		parameters as in Server initiated Resource Delete Scenario	Server A minimizes all the resources in the session except for S2 information flow.
Session & Call/Connection Setup		parameters as in STU initiated Session and Call/Connection Setup Scenario	STU establishes a session with Server B and passes the service_info and ticket_info provided earlier in 2. Note: both uuData and privateData in DSM-CC userData shall be used.
Session & Call/Connection Release		parameters as in STU or Server initiated Session and Call/Connection Release Scenario	STU or Server B releases the session.
Scenario I Session & Call/Connection Setup		parameters as in STU initiated Session and Call/Connection Setup Scenario	STU re-establishes a session with Server A and passes the user_context received in 3. STU resumes the service from where it last left off.
Scenario II 4a-4b RESUME		user_context	provides user_context received in 3.
Scenario II Resource Add		parameters as in Server initiated Resource Add Scenario	Server A adds all the resources in the session except for S2 and resumes the service from where it was left of.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

9.2.5.10 Resource Descriptors used in dynamic flows for VoD

Depending on the scenario and the endpoint, there is a specific view of the session which is defined using resource descriptors which are included in the messages. This section defines the possible scenarios and the resource views (both at the Server and STU) that are associated with them.

- Download Phase, Multiple ATM SVCs
- Video Play Phase, Multiple ATM SVCs
- Single Asymmetric ATM SVC

1- Download Phase, Multiple ATM SVCs

This example uses separate ATM SVCs in order to carry the flows identified below:

- Download Data downstream
- Download Data Response upstream
- Download Control downstream
- Download Control upstream
- RPC

Two scenarios are considered:

- End-to-End ATM
  In this case the ATM SVC is maintained intact between the Server and the Client
- Core ATM network and non-ATM HFC Client access
  In this case the flows being carried on the ATM SVC are mapped to non-ATM resources through the non-ATM resource descriptors.

1-A End-to-End ATM

The top diagram in Figure 9.2-13 provides the list of resource descriptors communicated from the Server to the Network and the Network to the Client. Since it is end-to-end ATM the resource numbers and the association tags are unchanged.

In the bottom diagram in Figure 9.2-13, the flows corresponding to DownloadControl, DownloadData and RPC are carried on separate ATM SVCs, Resource Number 1, 2 and 3 respectively and use the respective Association Tags 1, 2 and 3. The bindings to the interfaces are done using the Association Tags. Through the bindings, the information format at the interfaces is expected to be in IP format.

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

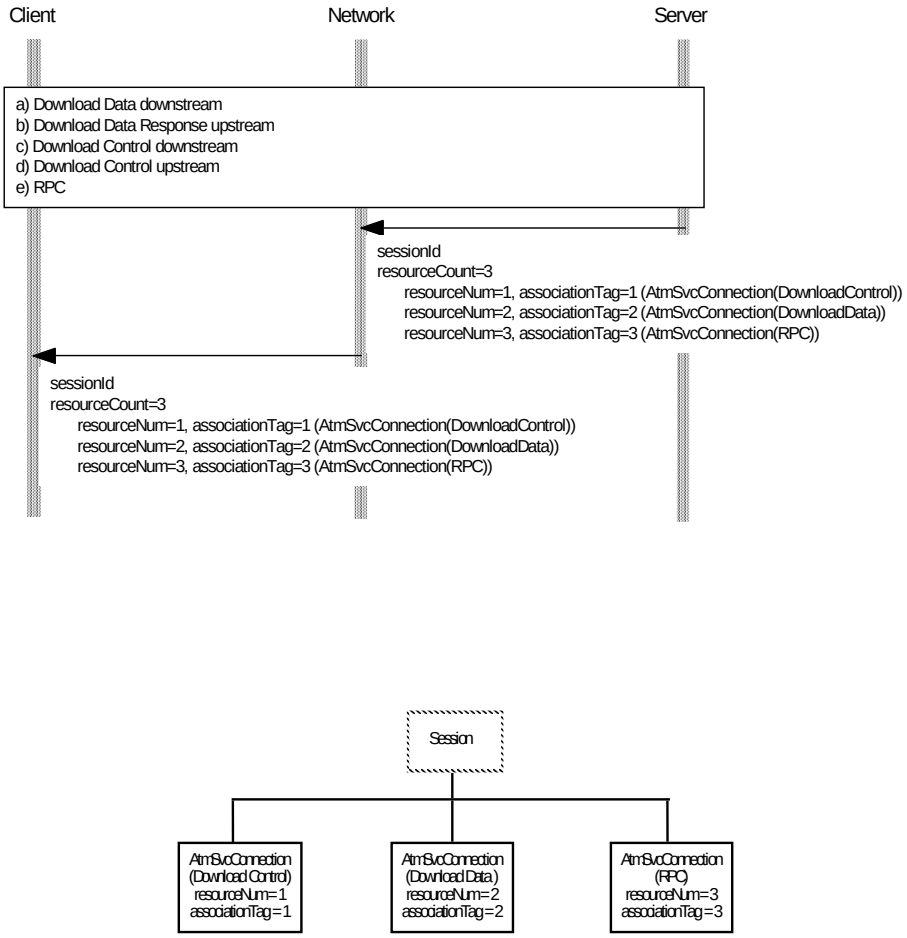


Figure 9.2-13 End-to-End ATM, Download Phase, Multiple ATM SVCs Server and Client Views

1-B Non-ATM HFC Client View

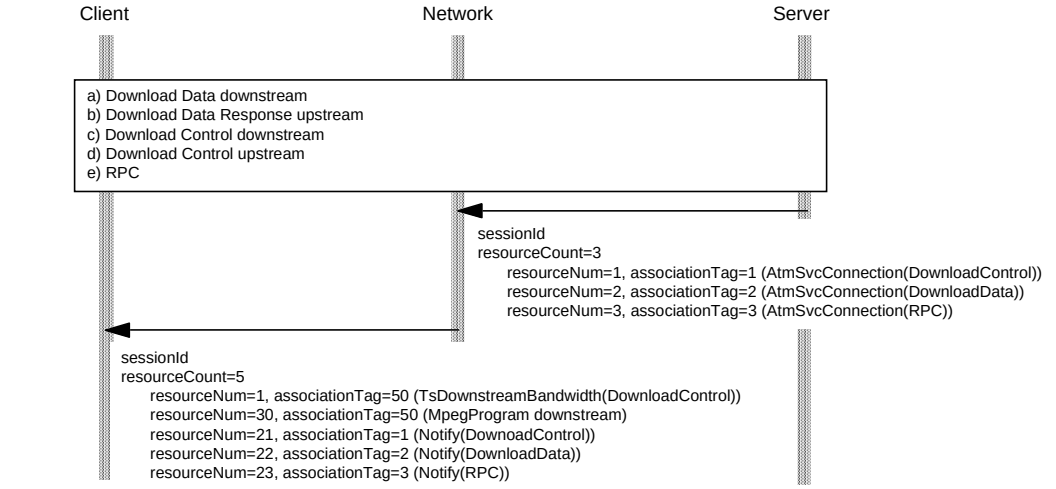
The top diagram in Figure 9.2-14 provides the list of resource descriptors communicated from the Server to the Network and the Network to the Client. Since the ATM terminates in the Network, new resources between the Network and the Client are used over the non-ATM HFC. The flows on the ATM SVC are mapped into those new non-ATM HFC resources. Although the resource numbers for each flow on the Client side are different, the association tags are kept the same.

Each of the DownloadControl, DownloadData and RPC consists of 2-way flows. The downstream flows are carried on the MPEG TS and the upstream flows are carried on TDMA referred to by the Notify resource descriptor. The bindings to the corresponding interfaces are done using the Association Tags. Through the bindings, the information format at the interfaces is expected to be in IP format.

Since the MPEG TS is carried over TsDownstreamBandwidth, Resource Number 20, the SRM assigns an Association Tag 50 to associate it with the MpegProgram Resource Number 30. The Association Tag in this instance is used to identify a stack and does not appear in interface bindings at the User-to-User level.

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale



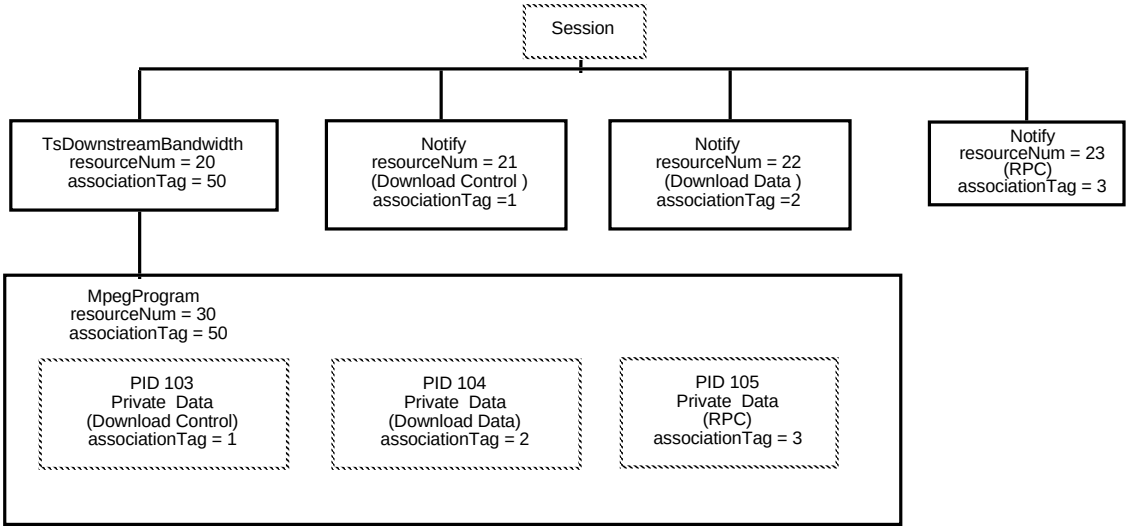


Figure 9.2-14 Non-Association TagM HFC Client View Corresponding to Download Phase, Multiple Association TagM SVCs Server and Client Views

2- Video Play Phase, Multiple Association TagM SVCs

This example uses separate Association TagM SVCs in order to carry the flows identified below:

- MPEG Audio/Video/Data downstream
- RPC

Two scenarios are considered:

End-to-End Association TagM: (In this case the Association TagM SVC is maintained intact between the Server and the Client)

Core Association TagM network and non-Association TagM HFC Client access: (In this case the flows being carried on the Association TagM SVC are mapped to non-Association TagM resources through the non-Association TagM resource descriptors.)

2-A End-to-End Association TagM

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The top diagram in Figure 9.2-15 provides the list of resource descriptors communicated from the Server to the Network and the Network to the Client. Since it is end-to-end Association TagM the resource numbers and the association tags are unchanged.

In the bottom diagram in Figure 9.2-15, the flows corresponding to MPEG Audio/Video/Data downstream and RPC are carried on separate Association TagM SVCs, Resource Number 1 and 3 respectively and use the respective Association Tags 1 and 3. The Association Tag 4 identifies a stack and is not used in the bindings. The bindings to the corresponding interfaces are done using the Association Tags 10. 11. 6 and 3. Through the Association Tag 3 binding the information format at the interface is expected to be in IP format.

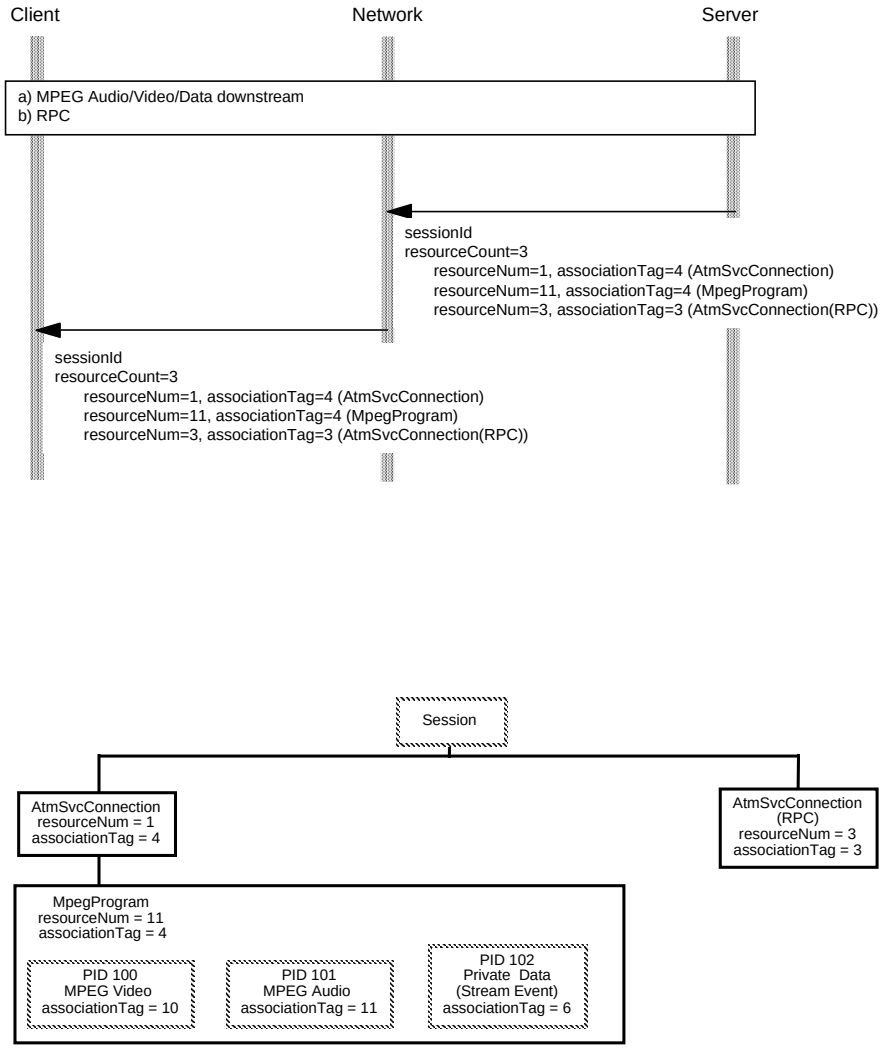


Figure 9.2-15 End-to-End Association TagM, Video Play Phase, Multiple Association TagM SVCs Server and Client Views

2-B Non-Association TagM HFC Client View

The top diagram in Figure 9.2-16 provides the list of resource descriptors communicated from the Server to the Network and the Network to the Client. Since the Association TagM terminates in the Network, new resources between the Network and the Client are used over the non-Association TagM HFC. The flows on the Association TagM SVC are mapped into those new non-Association TagM HFC resources. Although the

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

resource numbers for each flow on the Client side are different, the association tags are kept the same.

In the bottom diagram of Figure 9.2-16, the MPEG Audio/Video/StreamEvent consist of only downstream flows, the RPC consists of 2-way flows. Both MPEG Audio/Video/StreamEvent and RPC downstream flows are carried on the MPEG TS and the RPC upstream flow is carried on TDMA referred to by the Notify resource descriptor. The bindings to the corresponding interfaces are done using the Association Tags.

Since the MPEG TS is carried over TsDownstreamBandwidth, Resource Number 20, the SRM assigns an Association Tag 50 to associate it with the MpegProgram Resource Number 11. The Association Tag in this instance is used to identify a stack and does not appear in interface bindings at the User-to-User level.

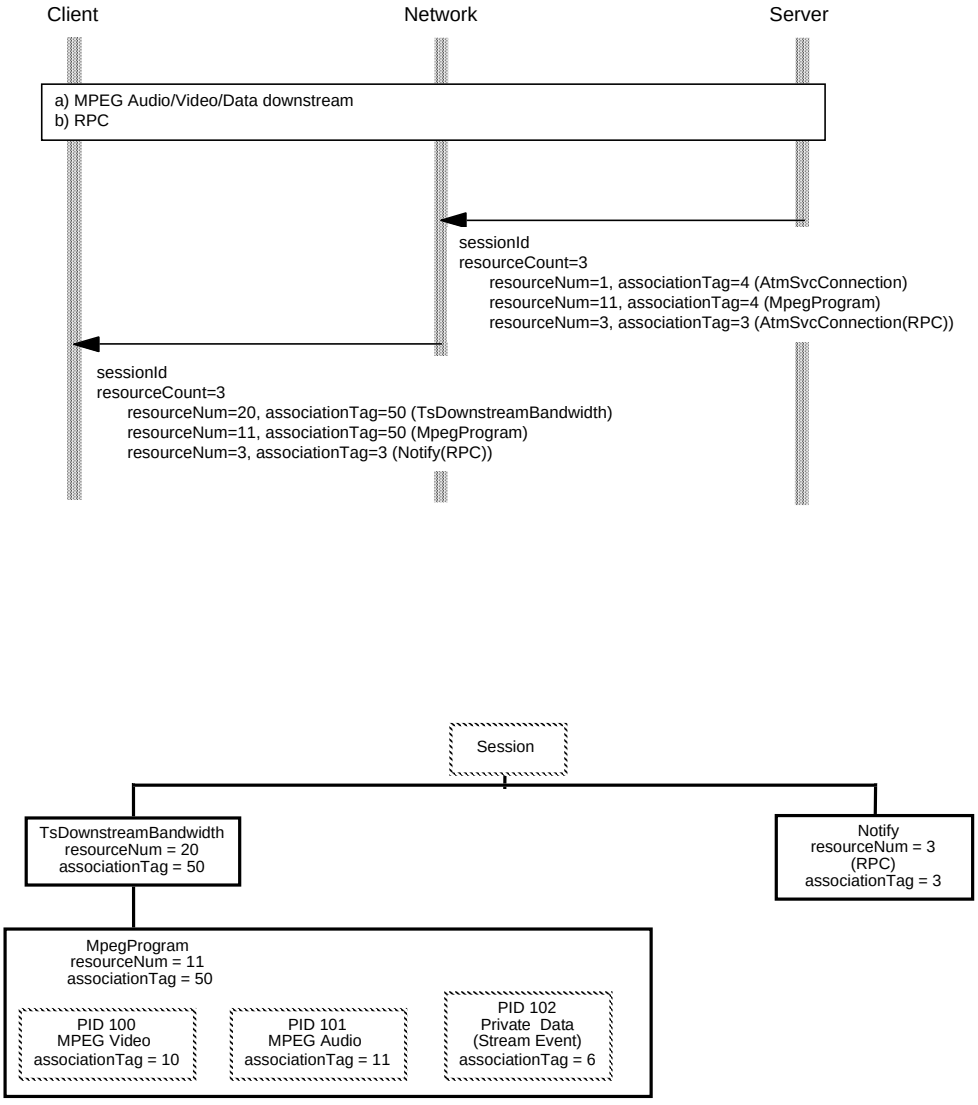


Figure 9.2-16 Non-Association TagM HFC Client View Corresponding to Video Play Phase, Multiple Association TagM SVCs Server View

3- Single Asymmetric Association TagM SVC

This example uses a single asymmetric Association TagM SVC in order to carry the flows identified below:

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

- MPEG Audio/Video/Data downstream
- RPC over TCP/IP downstream flow over private data on MPEG TS
- RPC over TCP/IP upstream flow over Association TagM
- Download Control and Data downstream flow in TCP/IP over private data on MPEG TS
- Download Control and Data Response upstream flow over Association TagM

Note: The use of TCP/IP in Download data will be reviewed for replacement by UDP/IP over the reflector for the June meeting.

Two scenarios are considered:

End-to-End Association TagM: (In this case the Association TagM SVC is maintained intact between the Server and the Client)

Core Association TagM network and non-Association TagM HFC Client access: (In this case the flows being carried on the Association TagM SVC are mapped to non-Association TagM resources through the non-Association TagM resource descriptors.)

Note: In case of TCP/IP, while the SVC connection is established, the TCP/IP connection is not. In step 8a-8b the IP resource descriptor is sent. The Download service at the server immediately begins to listen at the specified port. the TCP/IP connection is made by the STU Download service after receiving the IP resource descriptor in 9a–9b.

3-A End-to-End Association TagM

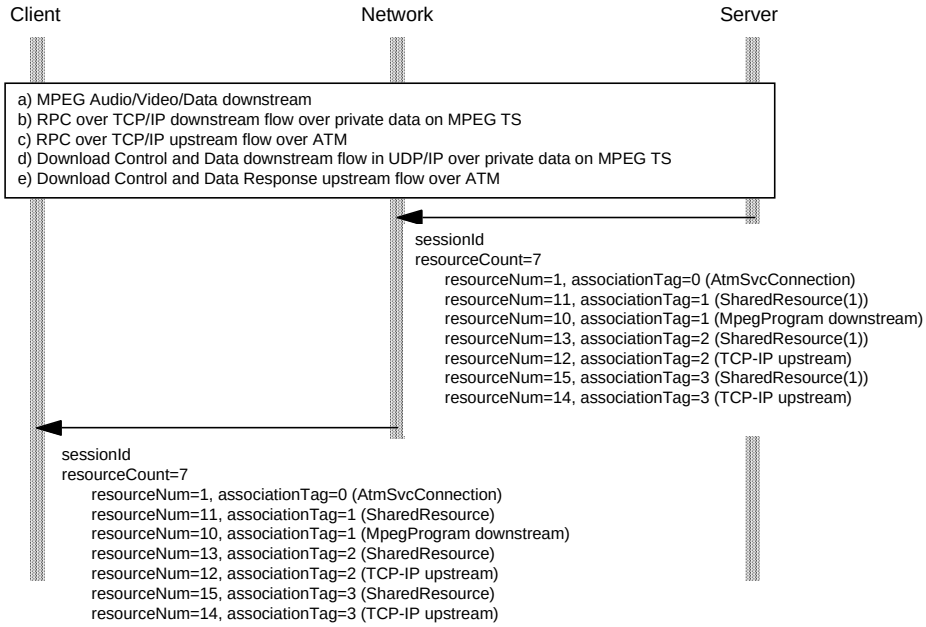
The top diagram in Figure 9.2-17 provides the list of resource descriptors communicated from the Server to the Network and the Network to the Client. Since it is end-to-end Association TagM the resource numbers and the association tags are unchanged.

The bottom diagram in Figure 9.2-17 shows how the SharedResource descriptor is used to share the AtmSvcConnection between the MpegProgram and Ip descriptors.

The MPEG Transport Stream Resource number, Resource Number 10, through SharedResource, Resource Number 11 shares the AtmSvcConnection, Resource Number 1 with the other IP connections. The link between the MPEG TS and the SharedResource is maintained through the Association Tag, Association Tag 1. The Audio, the Video and the StreamEvent carried in PIDs 100, 101 and 102 respectively are assigned the Association Tags 10, 11 and 6 respectively.

Since the RPC consists of 2-way flows, the downstream is carried on the MPEG TS, PID 204 and the upstream is carried on the IP connection Resource Number 12. Association Tag 2, links the two directions to the same interface. The SharedResource, Resource Number 13 also is tagged at Association Tag 2. Similarly the PID, Resource Number 14 and Resource Number 15 for Download are tagged at Association Tag 3.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale



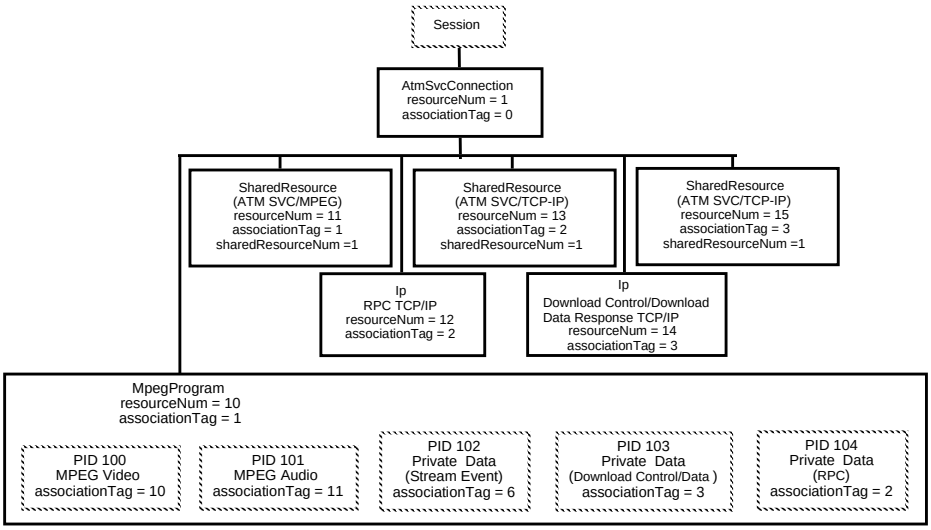


Figure 9.2-17 End-to-End Association TagM, Single Asymmetric Association TagM SVC Server and Client Views

3-B Non-Association TagM HFC Client View

The top diagram in Figure 9.2-18 provides the list of resource descriptors communicated from the Server to the Network and the Network to the Client. Since the Association TagM terminates in the Network, new

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

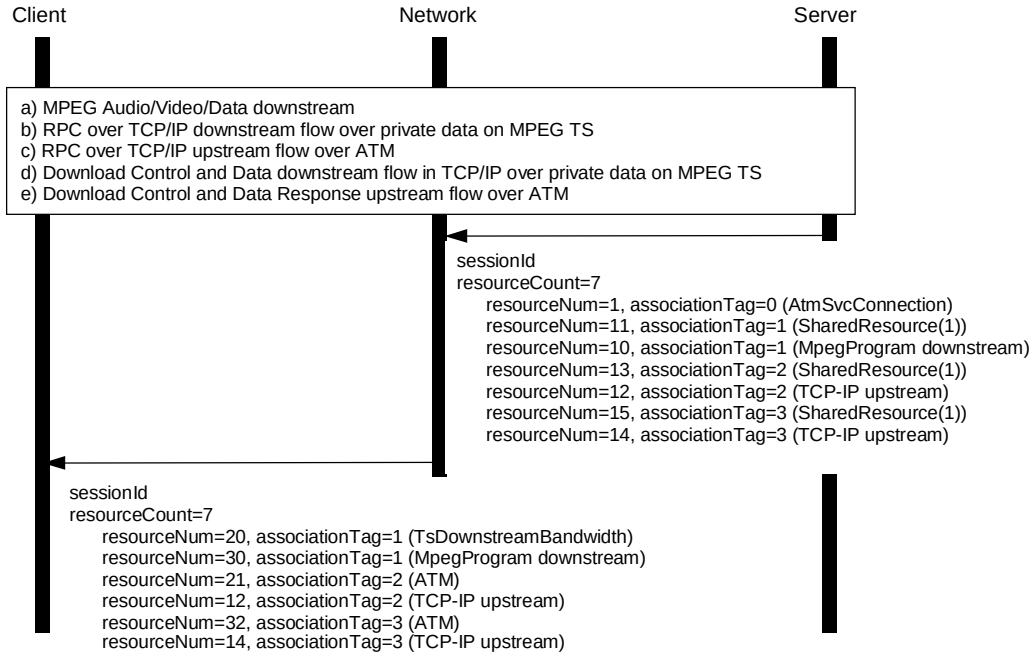
resources between the Network and the Client are used over the non-Association TagM HFC. The flows on the Association TagM SVC are mapped into those new non-Association TagM HFC resources. Although the resource numbers for each flow on the Client side are different, the association tags are kept the same.

The bottom diagram in Figure 9.2-18 shows two upstream connections each referred to by a Notify resource descriptor, which carry the DownloadControl/Data and the RPC upstream flows. Since the TsDownstreamBandwidth only carries the MPEG TS then both descriptors share the same Association Tag 1.

The MPEG Transport Stream Resource number, Resource Number 30 carries the Audio, the Video and the StreamEvent in PIDs 100, 101 and 102 respectively, assigned the respective Association Tag numbers 10, 11 and 6.

Since the RPC consists of 2-way flows, the downstream is carried on the MPEG TS, PID 204 and the upstream is carried on the IP connection Resource Number 12. The Association Tag 2, links the two directions to the same interface. The SharedResource, Resource Number 31 also share the Association Tag 2. Similarly the PID, Resource Number 14 and Resource Number 32 for Download are share the Association Tag 3.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale



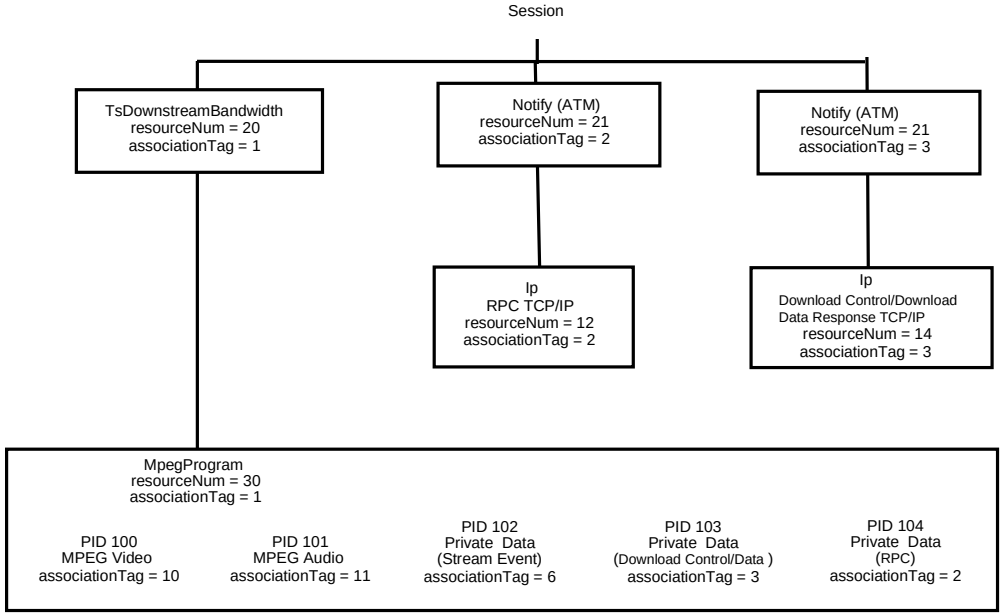


Figure 9.2-18 - Non-ATM HFC Client View Corresponding to Single Asymmetric ATM SVC Server Views

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

4- Single Asymmetric ATM PVC

The example with PVC is similar to the example in 1 “Single Asymmetric ATM SVC” except AtmSvcConnection is replaced by AtmConnection and SVC is replaced by PVC in the text.

5- Download Phase, Multiple ATM PVCs

The example with PVC is similar to the example in 2 “End-to-End ATM, Download Phase, Multiple ATM SVCs” except AtmSvcConnection is replaced by AtmConnection and SVC is replaced by PVC in the text.

6- Video Play Phase, Multiple ATM PVCs

The example with PVC is similar to the example in 3 “End-to-End ATM, Video Play Phase, Multiple ATM SVCs” except AtmSvcConnection is replaced by AtmConnection and SVC is replaced by PVC in the text.

7- Use of sharedResourceRequest Descriptors

In scenarios 1 through 6 above the resource numbers are assigned by the originator of the request. If the resource numbers are assigned by the Network, then the sharedResourceRequest Descriptor replaces the SharedResource Descriptor at every instance of its occurrence in examples 1 through 6 and correspondingly the sharedResourceNum is replaced by sharedResourceRequestId. In the request message, from the originator to the Network, the ResourceNums are filled with “0”s. In the confirm message from the Network to the originator, the ResourceNums take their actual values assigned by the Network..

9.2.6 Specification of the Usage of DAVIC Protocol Tools for VoD

This section describes the protocol stacks and network architectures that are used to implement the S1 through S4 information flows required by the dynamic functional entities for DAVIC VoD. These protocol stacks are described here in terms of network or topology diagrams for each of the defined Physical Scenarios, with the various physical layer (PHY) technology options illustrated via tables.

The relationships between the logical information flows (S1, S2 etc.), the functional entities, and the protocols that support them are also illustrated, in accordance with Figure 9.2-5.

Cross references between the protocols and their normative definitions elsewhere in the Davic VoD Specification are provided in Tables 12.1 and 12.2.

9.2.7 Protocol Network Architectures for DAVIC VoD

The three Scenarios shown in Figure 9.2-19, Figure 9.2-20, and Figure 9.2-21 represent end-to-end DAVIC systems illustrating the control functional entities (e.g., c/c, ses) and their supporting protocol stacks in a network or geographical view. Each Scenario illustrates a slightly different physical allocation of these entities in order to accommodate different DAVIC physical scenarios reflecting network deployment strategies and alternative access technologies. Both ATM end-to-end and ATM terminated in the access are shown.

The three scenarios described within this section utilize switched connections (SVCs), while yet another scenario, that for the use of permanent virtual circuits (PVCs), is described earlier.

Scenarios 2 & 3 illustrate the cases where the session manager is between A4 and A9:

In Scenario. 2, the STU contains call/connection control (e.g., Q.2931, etc.) and applies only to the ATM end-to-end case.

In contrast, Scenario 3 shows the use of proxy signaling (i.e., Q.2931 is moved out of the STU in order to simplify the STU. This scenario is also used only for ATM end-to-end.

Scenario 1 is similar to Scenario 3 in that proxy signaling is used. ATM can either be end-to-end or terminated in the access. However, in Scenario 1, the session manager (i.e., network side session entity) is located in the access network, connecting to the network via a standard UNI. Typically, this location will be at or near the location of the proxy signaling agent and possibly at the place ATM terminates (if ATM is not end-to-end).

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Scenario 1 is the only scenario supported in the DAVIC 1.3.1 Specification for HFC for ATM terminated in the access.

In all cases (Scenarios 1,2, & 3), the same combinations and alternatives of physical layer (PHY) technologies are supported. These alternative PHY protocols are not illustrated on these Protocol Network Architecture diagrams but, rather, are described in Table 12.2.

9.2.8 Rationale for the Physical Scenarios for VoD

Scenario 2 is the most general and flexible architecture, and it scales well geographically. It corresponds to the standard B-ISDN view: An ATM terminal containing, for example, Q.2931 call/connection control signaling is assumed, and the session manager is located in the service control within the core network (perhaps in an intelligent network entity).

Scenario 2 scales well and is readily extensible to other broadband services such as video conferencing, distance learning, etc. In addition, this approach appears to be well-suited for multi-network, multi-operator DAVIC because of the ability to distribute the network-side session entity among the various networks involved in the session.

Scenario 3 differs from Scenario 2 in that call/connection control signaling (e.g., Q.2931) resides outside of the STU(i.e., proxy signaling) . This potentially simplifies the STU and accommodates non-ATM end-to-end viewpoints. For the DAVIC VoD Specification, the proxy signaling entity is considered to be part of the core network along with the Ses(n) entity. This removes the need for any protocols and messages between these two entities for the DAVIC VoD Specification.

However, from core network and SRC (Service Related Control) point of view, it is the same as Scenario 2, thus allowing for the same distributed session capabilities for multi-network DAVIC.

Scenario 1 allows for rapid, localized equipment deployment and potentially simplifies the STU's. The difference between Scenario 1 and Scenario 3 is that the session manager entity is moved out of the core network into the access, connecting to the network via a standard UNI. Proxy signaling is used to simplify the STU's, and ATM can either be end-to-end or ATM can terminate in the access.

9.2.9 Notes on Download Protocols for VoD

The download protocol stacks shown in Figure 9.2-19, Figure 9.2-20, and Figure 9.2-21indicate that download of data can optionally utilize AAL5 without using the MPEG TS MUX/DEMUX mechanism. This is seen to be useful, for example, in the case where the server is not supplying an MPEG stream function. It is for further study whether or not TCP/UDP and IP are needed in this case. Or, is the direct use of AAL5 sufficient.

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

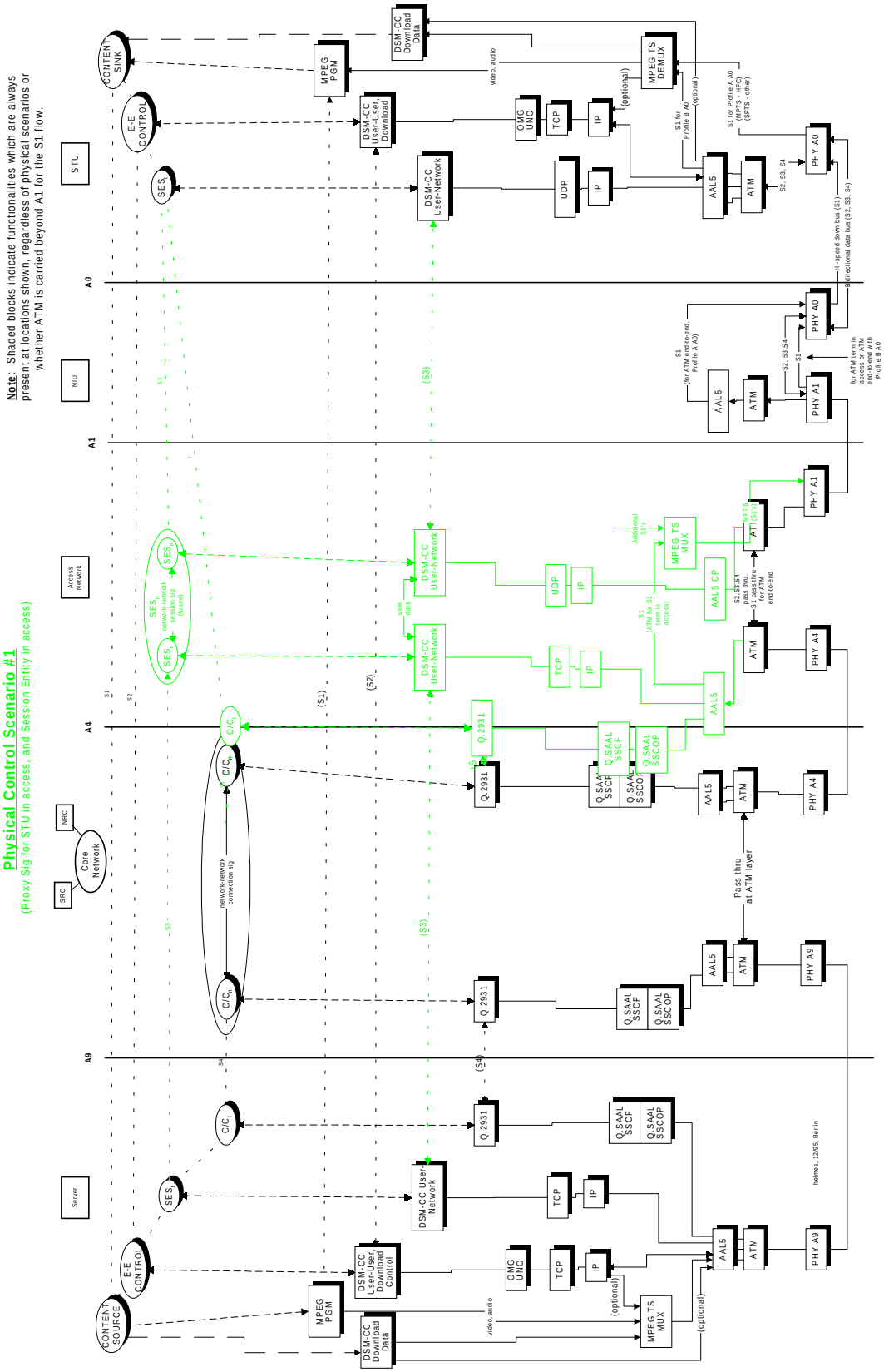


Figure 9.2-19

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

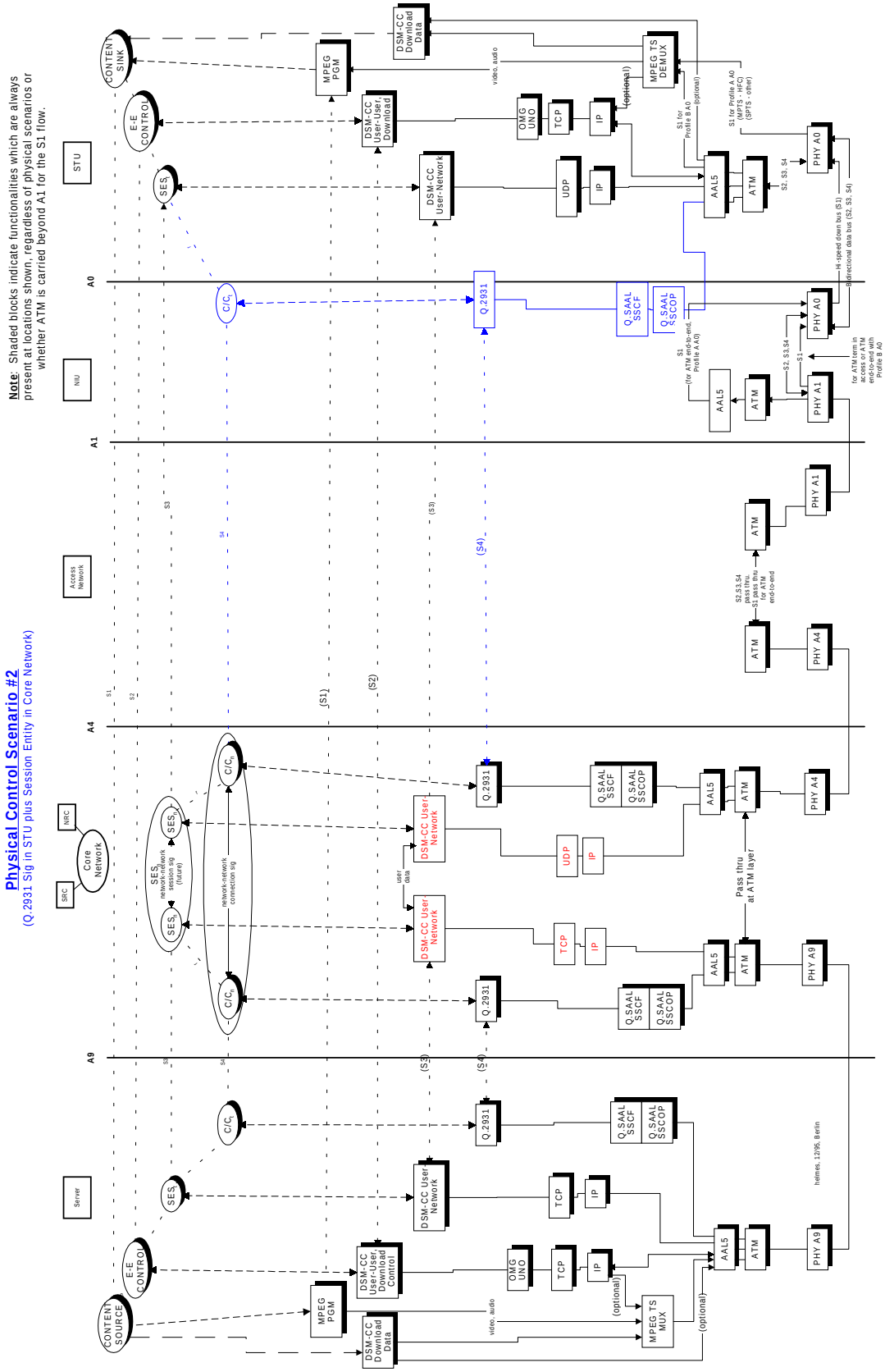


Figure 9.2-20

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

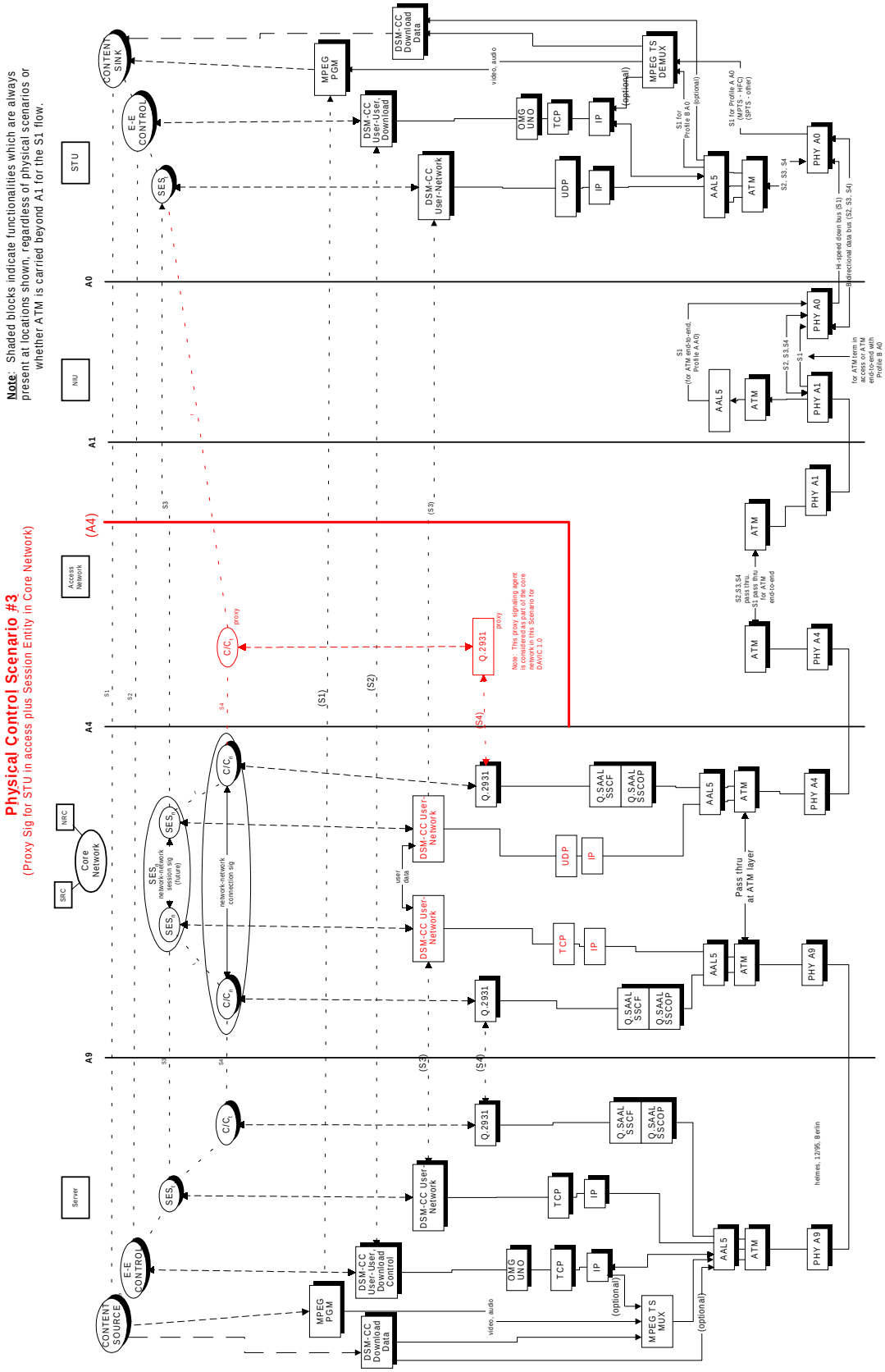


Figure 9.2-21

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Blank Page

 © ISO/IEC – All rights reserved

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

9.2.10 Cross-Reference to DAVIC Tool Definitions for VoD

Table 9.2-28 and Table 9.2-29 provide a cross-reference of the protocols specified for use within a DAVIC VoD system (as shown in Figure 9.2-19, Figure 9.2-20, and Figure 9.2-21) to their detailed descriptions and references described elsewhere within this Specification.

Table 9.2-28 - Cross-Reference to DAVIC Tool Definitions for VoD

DAVIC Tool Name (as shown in Figure 9.2-19, Figure 9.2-20, and Figure 9.2-21)	*ISO/IEC 16500 Part Number*	*Clause Number*	*Notes*
AAL5	5	11.4	(references ITU-T Rec. I. 363.5)
ATM	5	11.5	(references ITU-T Rec. I. 361)
DSM-CC User-Network	5	8.3	(references ISO/IEC 13818–6)
DSM-CC User-User, Download Control	5	7	(references ISO/IEC 13818–6)
DSM-CC Download Data	5	6	(references ISO/IEC 13818–6)
IP	5	11.3	(references RFC 791)
MPEG PGM	5	6	MPEG program information (e.g., video, audio) . Stored on Server as a SPTS. (references ISO/IEC 13818–1, -2, -3)
MPEG TS DEMUX	5	6	This refers to the Transport Stream Demultiplexing functionality of MPEG-2 Systems (ISO/IEC 13818–1)
MPEG TS MUX	5	6	This refers to the Transport Stream Multiplexing functionality of MPEG-2 Systems (ISO/IEC 13818–1)
OMG GIOP/IIOP	5	7.2.2 and 7.3	Includes OMG's CDR (Common Data Representation), OMG UNO's RPC mechanism, and CORBA 2.1's IIOP based on TCP/IP (default).
PHY A0	4 5	8. 12.	
PHY A1	4		A number of physical layer technologies are supported for the access. These are summarized in Table 9.2-29, but specified in detail or referenced in ISO/IEC 16500-4.
PHY A4	4	6.	
PHY A9	4	6.	
Q.2931	5	9.3.1	(specifies subset of ITU-T Q.2931)
Q.SAAL SSCF	5	9.3.2	(specifies ITU-T Q.2130 (SSCF-UNI)
Q.SAAL SSCOP	5	9.3.2	(specifies ITU-T Q.2110 (SSCOP)
TCP	5	11.1	(references RFC 793)
UDP	5	11.2	(references RFC 768)

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Table 9.2-29 - PHY Layer Cross-Reference to DAVIC Tool Definitions for VoD

PHY A1 Variant	*Name (in the Davic Specification)*	*ISO/IEC 16500-4 Clause Number*	*Common, Informal, or Previous Name*	*Referenced or Spec. Included?*	*ATM End-to-end? (across A1)*
#1	Low-Speed Symmetrical PHY on the PSTN	7.1	(modem on POTS line)	ref. V.22bis	no
#2	Low-Speed Symmetrical PHY on the ISDN	7.2	N-ISDN	ref. I.430	no
#3	Long-Range Baseband Asymmetrical PHY on copper	7.3	ADSL	ref. ANSI T1E1.4	some
#4	Medium-Range Baseband Asymmetrical PHY on copper	7.4	VDSL	ref. ANSI T1E1.4	yes
#5	Short-Range Baseband Asymmetrical PHY on copper and coax	7.5	FTTC	spec. included in this DAVIC Specification	yes
#6	Passband Unidirectional PHY on coax	7.6	HFC #1	spec. included in this DAVIC Specification	some
#7	Passband Bi-directional PHY on coax	7.7	HFC #2	spec. included in this DAVIC Specification	some
#8	Passband Unidirectional PHY on Satellite	7.8	Satellite Broadcast (DVB)	ref. ETS 300 421 plus DAVIC-specific deltas	no
#9	Baseband Symmetrical PHY on copper	7.9	ATM Forum's 25 Mbs on UTP	ref. ATM Forum	yes
#10	Baseband Symmetrical PHY on fiber	7.10	FTTH/SDH	ref. I.432.1, I.432.2	yes

9.2.11 Association Between Interfaces and Network Resources for VoD

Background:

The Digital Storage Media Command & Control initiative, which this specification references, provides two elements to a solution: a) the session protocol which instructs the settop about network resources for a session, and b) service interfaces which the settop invokes to interact with services. The session protocol deals with network resources; the protocol is oblivious to the interface (that is, the semantics) above the resources. The service interfaces deal with services; the interface is oblivious to the network resources below. The separation is one reason applications on the settop interacts with consistent interface, even though the network to which the settop attaches often differs.

It is still necessary, however, to relate interfaces with resources. The Digital Storage Media Command & Control initiative provides the framework. This section presents the specialization for distinct services and distinct networks. The mechanism is a structure which accompanies the object reference for the service. The structure allows the service to bind an interface name, known to the application code on the settop, to shorthand for network resources, known to the session code on the settop.

The shorthand is known as the association tag. The value has end-to-end significance. If the connection which carries the media stream changes at the access gateway, for example, the resource descriptors visible to the service and the resources visible to the settop would differ. The association tag, however, would not. The service would assign it and list the network resources it encapsulates. The ses(n) element preserves the value. If the media stream connection changes, the ses(n) element would forward the value, along with the network resources visible to the settop.

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Since the service does not know, nor wish to know, the network visible to the settop, the service shall always assign association tags. It then provides the list which binds interfaces to resources (to be precise binds to association tags) with an object reference.

Interface Support:

The question which remains is which interfaces and which resources should the settop expect to encounter. We first consider the interfaces. The service domain can be thought to divide into services which do not provide a media stream (for example ServiceGateway) and those which do provide a media stream (for example Stream). If the service does not produce a media stream, the settop shall support the interfaces shown in Table 9.2-30.

Table 9.2-30

Description	*Classification*	*Direction*
Service Request	Request	Settop-to-Service
Service Reply	Reply	Service-to-Settop
Download Control Request	Request	Settop-to-Service
Download Control Reply	Reply	Service-to-Settop
Download Data Confirm	DataAck	Settop-to-Service
Download Data	Data	Service-to-Settop

(In the interest of comprehension, the descriptions above differ slightly from the list found in the Digital Storage Media Command & Control initiative. The correspondence, however, is obvious.)

The implication of the above list is that the settop should expect that download might occur. If the download phase is not necessary, the download service cancels the phase.

If the service does produce a media stream, the settop should also expect the interface shown in Table 9.2-31.

Table 9.2-31

Description	*Classification*	*Direction*
Mpeg Downstream	MpegPid	Service-to-Settop
StreamEvent	MpegPid	Service-to-Settop

(While the complete list of the Digital Storage Media Command & Control initiative includes a media stream in the upstream (settop-to-service) direction, the default is just transport of media stream from the service to the settop.)

Note that the settop can subscribe to stream events, which appear as private data in the mpeg stream. The implication is that the service must describe the resource, that is the elementary stream, in which the event data will be found. (See resource for this case below.)

Resource Support:

The companion question to which interfaces to support is the question of which resources to bind to the interfaces. The answer depends on the perspective. From the perspective of the service, either MPEG TS stream or ATM with or without IP could be used for download. In the case of end-to-end ATM the carriage of the download is for further study.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Table 9.2-32

Description	*Classification*	*Direction*	*ResourceDescriptor*
DownloadControlRequest	Request	Settop-to-Service	ATMIp
DownloadControlReply	Reply	Service-to-Settop	AtmIp
DownloadDataConfirm	DataAck	Settop-to-Service	AtmIp
DownloadData	Data	Service-to-Settop	AtmIp
ServiceRequest	Request	Settop-to-Service	AtmIp
ServiceReply	Reply	Service-to-Settop	AtmIp
MpegDownstream	Stream	Service-to-Settop	AtmMpegAudio
			AtmMpegVideo
StreamEvent	Private Data	Service-to-Settop	AtmMpegStrmEvnt

Table 9.2-33 describes the situation where the service delivers a media stream. Note that the download data is found in the media stream. Note also that stream event data appears as private data in the media stream.

Table 9.2-33

Description	*Classification*	*Direction*	*ResourceDescriptor*
DownloadControlRequest (When not carried over uuData)	Request	Settop-to-Service	TcpAtm
DownloadControlReply (When not carried over uuData)	Reply	Service-to-Settop	TcpAtm
DownloadDataResponse	DataAck	Settop-to-Service	For Further Study
DownloadData	Data	Service-to-Settop	For Further Study
ServiceRequest	Request	Settop-to-Service	TcpAtm
ServiceReply	Reply	Service-to-Settop	TcpAtm
MpegDownstream	Stream	Service-to-Settop	MpegAudioAtm
			MpegVideoAtm
StreamEvent	PrivateData	Service-to-Settop	MpegStrmEvntAtm

If the settop and the service both agree, it is feasible to embed data in the media stream. The technique is known as tunneling. If both sides elect to adopt the technique, the interface vs resource list becomes as shown in Table 9.2-34.

Table 9.2-34

Description	*Classification*	*Direction*	*ResourceDescriptor*
DownloadControlRequest (When not carried over uuData)	Request	Settop-to-Service	TcpAtm
DownloadControlReply (When not carried over uuData)	Reply	Service-to-Settop	TcpMpegAtm
DownloadDataResponse	DataAck	Settop-to-Service	For Further Study
DownloadData	Data	Service-to-Settop	For Further Study
ServiceRequest	Request	Settop-to-Service	TcpAtm
ServiceReply	Reply	Service-to-Settop	TcpMpegAtm
MpegDownstream	Stream	Service-to-Settop	MpegAudioAtm
			MpegVideoAtm
StreamEvent	PrivateData	Service-to-Settop	MpegStrmEvntAtm

From the perspective of the settop, there is a comparable list. The resource field of the list, however, depends on the delivery technique. In the case of ATM to the settop, the above lists apply. In the case of HFC, the list in Table 9.2-35 applies.

 © ISO/IEC – All rights reserved

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Table 9.2-35

Description	*Classification*	*Direction*	*ResourceDescriptor*
DownloadControlRequest (When not carried over uuData)	Request	Settop-to-Service	TcpHfcUpStrm
DownloadControlReply (When not carried over uuData)	Reply	Service-to-Settop	TcpHfcDnStrm
DownloadDataResponse	DataAck	Settop-to-Service	For Further Study
DownloadData	Data	Service-to-Settop	For Further Study
ServiceRequest	Request	Settop-to-Service	TcpHfcUpStrm
ServiceReply	Reply	Service-to-Settop	TcpMpegHfcDnStrm
MpegDownstream	Stream	Service-to-Settop	MpegAudioHfcDnStrm
			MpegVideoHfcDnStrm
StreamEvent	PrivateData	Service-to-Settop	MpegStrmEvntHfcDnStrm

There are, in fact, separate descriptors for the Permanent Virtual Circuit versus Switched Virtual Circuit cases. From the perspective of the settop, however, the descriptors can be thought to be the same.

9.2.12 Rationale behind the selection of the DAVIC VoD dynamic systems behavior

A) Conclusions reached:

Usage of DSM-CC User-Network protocol are defined as follows:

- The assignor of the sessionId shall be the STU.
- The assignor of the resourceNum shall be the Server.
- The clientId sent to the Server, e.g., in Sess SETUP req.ind, shall represent the ATM address with which the Server may use to request an ATM call/connection with the STU.

B) Rational:

(1) The preferred method for ATM call/connection establishment for S1 and S2 is for the Server to be the calling party.

Reasons for (1):

1.1 In the case where the proxy signaling agent for the STU (c/c(t)) resides in the Access Network and the ses(n) resides in the core domain (between A4 and A9), some messages would have to cross the A4 interface if ses(n) triggered c/c(t) to originate the ATM call/connection setup from the STU side. This is due to the fact that the network cannot itself initiate a connection establishment outwards from a point within the network.

2.2 In the case where the network operator offers a session-based tariff service, it is risky to allow end-users (STU) to request ATM call/connections, because some end-users might try to illegally access the network by, e.g., requesting a call with a false resourceId embedded in the call request message. The network would have to check whether the resourceId in the call request message is valid or not. This real-time authentication operation would be difficult to perform.

(2) Given (1) and that the definition of the Resource ADD req.ind flow means that the resources contained within the message have been allocated, the call/connect request by the Server must occur before Resource ADD req.ind flow (if used) or before the Session SETUP resp.conf flow for the case of end-to-end ATM SVC's.

(3) Given (2), the assignor of the resourceNum (and hence resourceId) shall be the Server.

(4) DAVIC shall support the AddResource sequence embedded within the STU-Initiated Session Setup flow sequence in order to enable the fastest start-up for User-User interactions. This means that, in the end-to-end SVC case, the STU receives the call/connections associated with the requested session before receiving Session SETUP resp.conf flow. As such, the STU needs to know the sessionId before this in order to correlate the ATM call/connection with the session. Therefore, the assignor of the sessionId shall be the STU.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

(5) Given (1) and (4), the Server has to know the ATM address for the STU (the address with which the ATM network can route call/connections to the STU) at the time of ServerSessionSetupIndication. To perform this without requiring a translation function in the Server, the clientId delivered to the Server shall indicate the ATM address for the STU.

All the above rationales described above are associated with the end-to-end ATM with SVC case. The same line of reasoning applies to the ATM-terminated-in-the-access and PVC cases.

 © ISO/IEC – All rights reserved

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

9.3 DSDM for SVB (Switched Video Broadcast)

9.3.1 Overview

Two main realization models are provided for the SVB:

- SVB without prior session establishment (SVB Realization 1)
- SVB with prior session establishment (SVB Realization 2)

Intermediate realizations can comprise of elements from each. These models vary in their realizations of the flows described below:

Table 9.3-1 - Realization of functional flows in the SVB models

Functional Flows	SVB Realization 1	SVB Realization 2
1- Broadcast Program Configuration	Through administrative means, outside the scope of DAVIC	Through dynamic Continuous Feed establishment using Continuous Feed Sessions
2- Client Service Profile Transfer to Broadcast Control Unit	Through administrative means, outside the scope of DAVIC	Through Switched Video Service Session Establishment, see 4 below.
3- Broadcast Program Guide Transfer to the Client	Through administrative means, outside the scope of DAVIC	Broadcaster Service provider specific through download in conjunctions with channel change control application program or private data at resource allocation time and/or Replication Unit specific by the Network Service Provider through private data at session establishment.
4- Switched Video Service Session Establishment	Session numbers are predefined as connection numbers at STU configuration time implying that no session establishment is required for SVB.	Session numbers are assigned in the normal course of session establishment in conjunction with session numbers for access to other services such as Interactive Video.
5- Client Initiated Channel Changes	Uses Channel Change Protocol	Uses Channel Change Protocol
6- Network Initiated Channel Changes	Not applicable	Used for presubscribed programs such as Pay TV
7- Switched Video Service Session Establishment	Not applicable. The Client is connected to the SVB service as part of the interface initialization when the STU is powered up.	Terminates the Client's SVB service.

9.3.2 Functional Entities Used in Dynamic Modeling for SVB

The functional entities specific to SVB are:

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

- Broadcast Control Unit - This unit terminates the S3 flow which controls the selection of the broadcast channel.
- Replication Unit - This unit terminates the S1 flow on which the broadcast channels are transmitted. Content sources are provided to the Replication Unit either through satellite pick up at the unit or through ATM PVC/SVC connection to the source which can be either off satellite, a content service server with continuous broadcasting capability or a live source.

The location of the above functional units are either in the access or in the core.

 © ISO/IEC – All rights reserved

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

9.3.3 System Dynamic Flows for SVB

Broadcast Program Configuration Using Continuous Feed Session Establishment

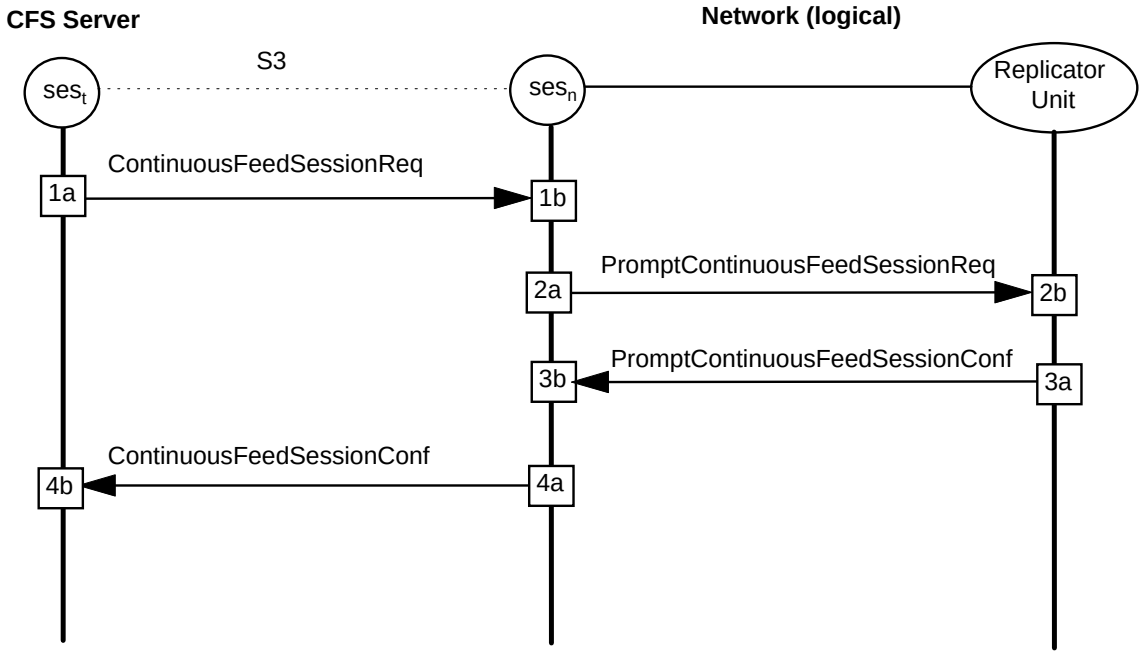
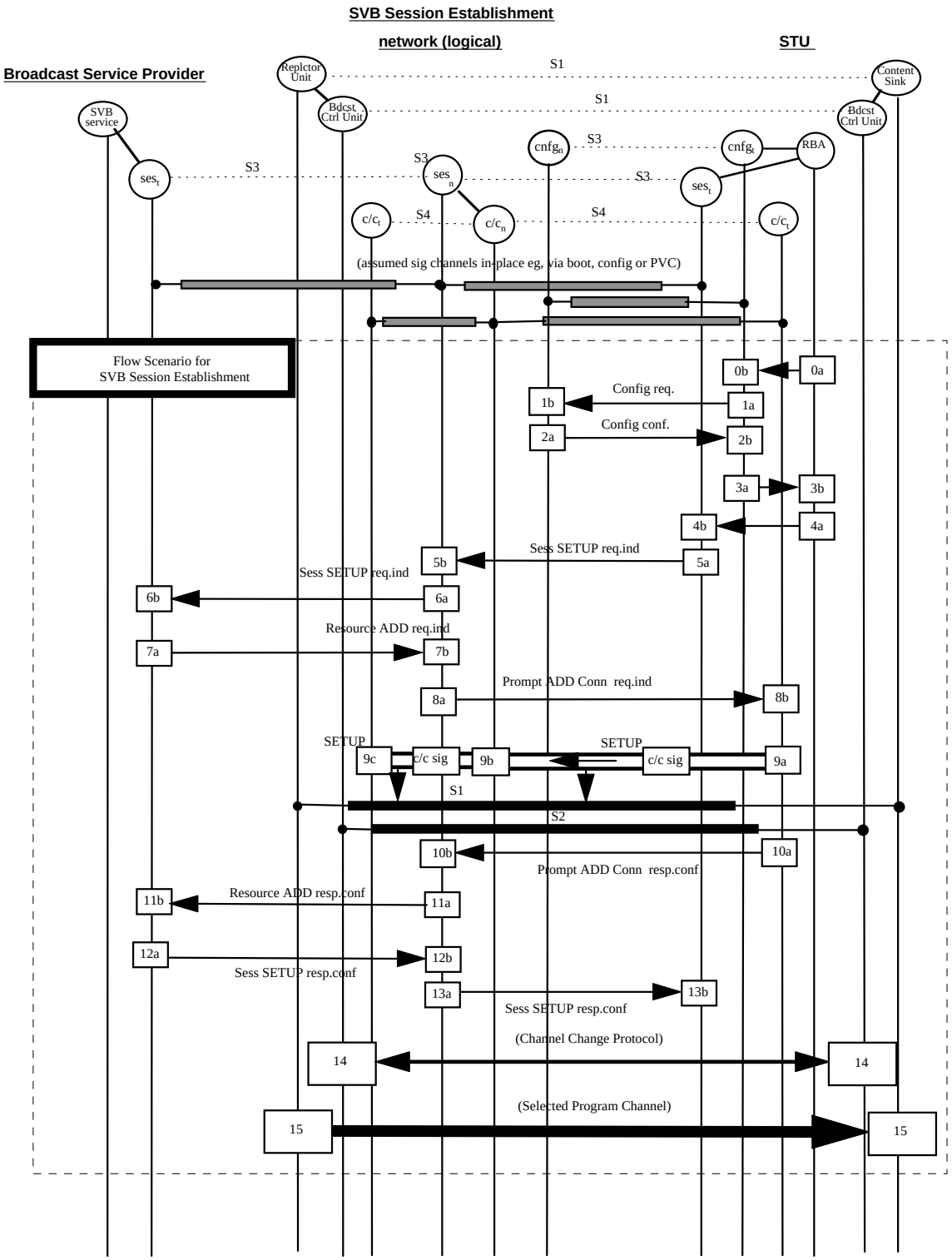


Figure 9.3-1

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale



Note : This dynamic flow scenario is used for Physical Scenario #1 (both ses(n) and the proxy signalling agent c/c(t) are colocated). In this case, flows 8a-8b and 10a-10b are actually internal. In Physical Scenario #2, c/c(t) (I.e., Q.2931) is located in the STU and can therefore be directly prompted by the STU application to initiate the connection to the router.

Figure 9.3-2

Note: The physical channel for the Channel Change Protocol may not be established via Q.2931, but it could be a PVC.

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Client Initiated Channel Change

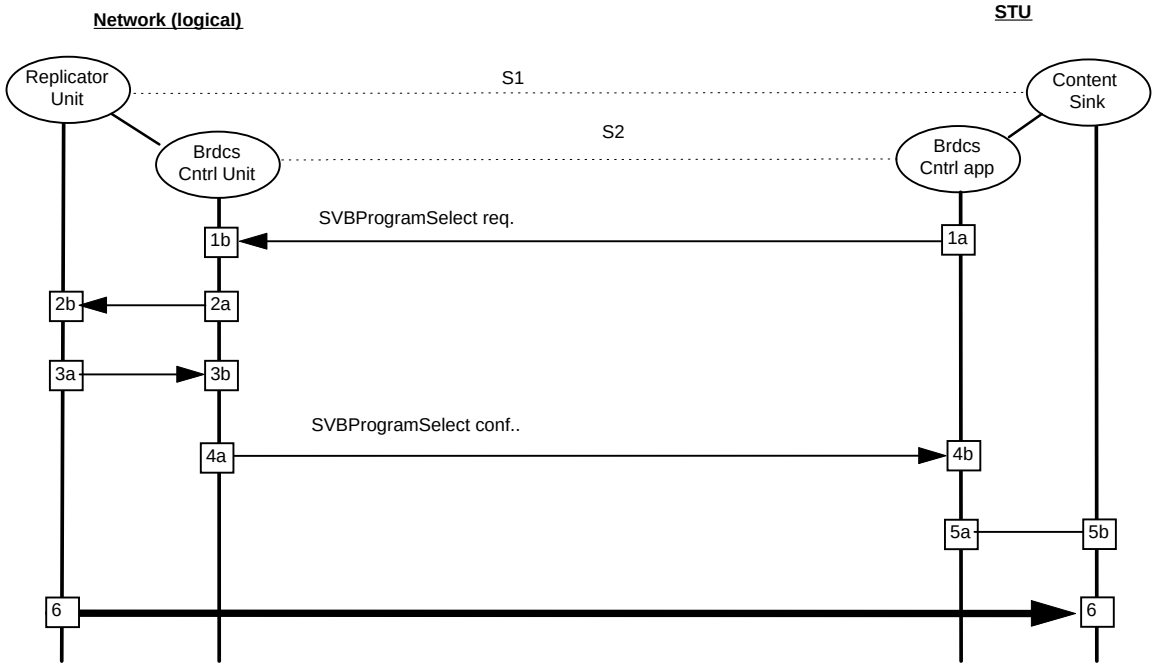


Figure 9.3-3

Network Initiated Channel Change

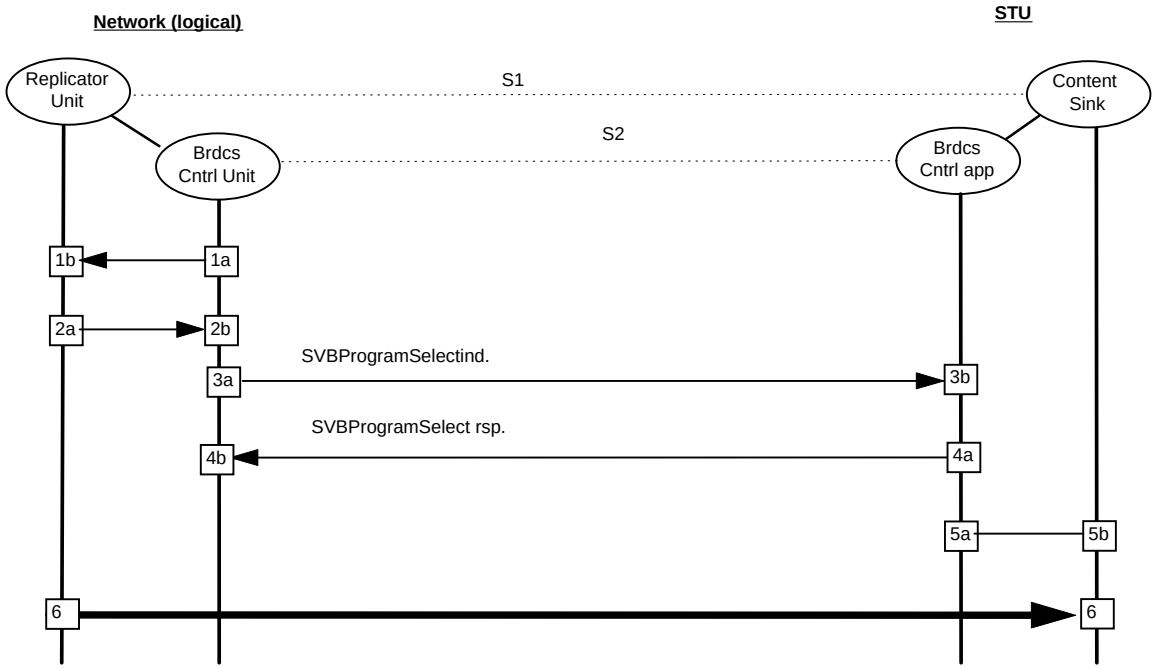


Figure 9.3-4

The SVB Session release is identical to the DAVIC VoD session release.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

9.3.4 Functional Entity Actions for DAVIC SVB

Table 9.3-2 - Broadcast Program Configuration Using Continuous Feed Session Establishment

1a–1b	Continuous Feed Server sends a ContinuousFeedSesskonReq to establish program channel feeds with the Replication Unit
2a–2b	For each broadcast program ses_n assigns a broadcast program ID and provides the Replication Unit with the association between the broadcast program ID and the Replication Unit's view of the connection resource that carries the broadcast program
3a–3b	The Replication Unit acknowledges the presence of the broadcast program on the resource
4a–4b	Ses_n indicates the broadcast program ID assigned to the broadcast program

Table 9.3-3 - Functional Entity Actions - SVB Session Establishment

0a – 0b:	The STU is powered up and the Resident Base Application invokes the User-to-Network Configuration process.
1a – 1b:	STU Config send the Network Config a Config req.
2a – 2b:	Network Config sends the STU a Config conf. including the server_id of the Broadcast Service Provider
3a – 3b	STU Config invokes the Resident Base Application with the message content of Config conf.
4a – 4b	The Resident Base application requests the establishment of a session with the Broadcast Service Provider. Note: It is also possible to select a Broadcast Service Provider at an intermediate default Broker Server provided at U-N configuration time. These steps are not shown for reasons of brevity.
5a – 5b	the STU ses_t sends a Sess. SETUP req.ind to ses_n
6a – 6b	Ses_n sends a Sess. SETUP req.ind to the Broadcast Service Server ses_t
7a – 7b	The Broadcast Service Server ses_t sends Resource ADD req.ind to ses_n
8a – 8b	Ses_n prompts the STU proxy C/C_t to establish the connections for : Channel Change Protocol from the STU to the Broadcast Control Unit Program viewing from the STU to the Replication Unit Note 1: In case of PVC both of these connections could be pre-established. Note 2: In case if more than one SVB session is established at the STU the Channel Change Protocol resource is shared among all the SVB sessions at the STU.
9a – 9b – 9c	Connections establishment
10a – 10b	C/C_t prompts the ses_n with the result of connection establishment e.g., VPI/VCI
11a – 11b	Ses_n sends Resource ADD resp.conf to the Broadcast Service Server ses_t
12a – 12b	The Broadcast Service Server ses_t sends Sess. SETUP resp.conf to ses_n
13a – 13b	Ses_n sends Sess. SETUP resp.conf to the STU ses_t

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

14a – 14b	The Resident Base application is prompted with the results of the establishment of the connection e.g., VPI/VCI to the both the Broadcast Control Unit and the Replication. The Resident Base Application passes the resource association to the Broadcast Control Application. Note: Connection may also be established to the Broadcast Service Server to download the Broadcast Control Application and in turn the latter could download the Electronic Program Guide. These steps are not shown above for reasons of brevity.
15	At this point the Channel Change Protocol can begin to operate
16	The selected program channel is carried in the downstream direction.

Table 9.3-4 - Client initiated channel change

1a–1b	Based on the Electronic Program Guide and input from the hand held control the Broadcast Control Application request and SVB program selection
2a–2b	The Broadcast Control Unit passes the selection to the Replication Unit
3a–3b	The Replication Unit provides information regarding the availability of the program and adequate network resources to the Broadcast Control Unit
4a–4b	The Broadcast Control Unit passes on the program channel tuning parameters to the Broadcast Control Application
5a–5b	The Broadcast Control Application passes the program channel tuning information to the Content Sink
6	The program channel tuning is completed ant the Client begins the viewing

Table 9.3-5 - Network initiated channel change

1a–1b	Based on pre-subscription the Broadcast ControlUnit selects a program channel passes the selection to the Replication Unit just prior to the start of the event.
2a–2b	The Replication Unit provides information regarding the availability of the program and adequate network resources to the Broadcast Control Unit
3a–3b	The Broadcast Control Unit passes on the program channel tuning parameters to the Broadcast Control Application
4a–4b	The Broadcast Control Application acknowledges the correct reception of the information
5a–5b	The Broadcast Control Application passes the program channel tuning information to the Content Sink
6	The program channel tuning is completed ant the Client begins the viewing

9.3.5 Dynamic Flow Parameters for SVB

Table 9.3-6 - Broadcast Program Configuration Using Continuous Feed Session Establishment

Flow	Status	Parameter	Comment
1a–1b ContinuousFeedSession req.		session_id	A unique value assigned by the Continuous Feed Server

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

		server_id	E.164 NSAP address at the A9 interface of the server
		sdb_id	is the specific basket assigned by the network provider to which the programs are added
		program_id(s)	this field is left blank for the ses_n to assign a value
		association_tag(s)	corresponds to each program_id and associates it to a resource_descriptor association_tag
		resource_descriptor(s)	contains an association_tag which corresponds to the program which it carries
2a–2b ses_n-Replication Unit		program_id(s)	as assigned by the ses_n
		association_tag(s)	corresponds to each program_id and associates it to a resource_descriptor association_tag
		resource_descriptor(s)	contains an association_tag which corresponds to the program which it carries
3a–3b Replication Unit - ses_n		program_id(s)	same as in 2
		association_tag(s)	same as in 2=1
		resource_descriptor(s)	same as in 2=1
		status_id	indicates the status of the requested program_id(s) (e.g., OK or failed because of...)
4a–4b ContinoudFeed Session conf.		session_id	same as 1
		server_id	same as 1
		sdb_id	same as 1
		program_id(s)	same as 3=2
		association_tag(s)	same as 3=1
		resource_descriptor(s)	same as 3=1
		status_id	same as 3

Table 9.3-7 - SVB Session Establishment

Flow	Status	Parameters	Comments
0a-0b The STU is powered up, Resident Base App - $Cnfg_t$			

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

1a-1b Config req.		device_id	this is the device_id of the STU.
2a-2b Config conf.		device_id	the same as in 1
		network_config_parametrs	provides the Broadcast Service Server server_id and optionally the service_info which includes an SdbId as primary_saved_context
3a-3b $Cnfg_t$ – Resident Base App		server_id	the Admin Server server_id from 2
		service_info	identical to step 2
4a – 4b Resident Base App – Ses_t		server_id	the Admin Server server_id from 3 = 2
		service_info	identical to step 3 = 2
5a – 5b Sess SETUP req.ind		session_id	uniquely assigned by the STU = device_id & arbitrary additional value, unique on this STU
		client_id	E164 NSAP address at the A1 interface of the client.
		server_id	the Broadcast Service Server server_id from 4 = 2
		service_info	identical to step 4 = 2
6a – 6b Sess SETUP req.ind		session_id	identical to step 5
		client_id	identical to step 5
		service_info	identical to step 5 = 2

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

7a – 7b Resource ADD req.ind		resource # (as seen by the server) association_tag (end-to-end) resource_descriptor(s)	describes the connections between the Broadcast Conrol Unit and the Replication Unit and the STU and contains - physical E.164 address of the port, on both the Broadcast Control Unit and the Replication Unitparameters which describe the ATM connection to be set up: - bandwidth - QoS - any other necessary parameters, such as AAL parameters, broadband bearer capabilities, etc. A list of broadcast program Ids for the Client's entitlement within the established session. Provision is made for inclusion of programs in addition to the regular programs specified in the sdbId or for exclusion of some programs as the need may arise. However it is expected that the sdbId will be adjusted in time or new sdbId created to avoid unnecessary use of inclusions. Note: It is also possible to assign the Channel Change Control Protocol through the Interface Initialization protocol, in which case he Broadcast Server will be notified through the compatibility parameters in 5 and accordingly not request the establishment of the resource. The ses_n allocates the resource needed to support the control channel and a nominal resource for initial program viewing based on the Client entitlements for the SDB Session in the SdbFeed. Note that the ses_n may need to request the resources from the Replication Unit and the Broadcast Control Unit at this point, and may communicate Client entitlement information to the Replication Unit.
8a – 8b ses_n - c/c_t		STU_id	This contains the E164 NSAP address of the STU
		broadcast_ATM_id	provided by the network if connection is ATM SVC
		replicator_ATM_id	provided by the network if connection is ATM SVC
		resource_attribute(s)	derived from the resource descriptor in 7
9a – 9b – 9c		all c/c signaling parameters	see ISO/IEC 16500-5
10a – 10b c/c_t – ses_n		session_id	identical to step 5
		VPI/VCI (as seen by the STU A1)	
		status_id	indicates status and reason of the requested resource (e.g., OK or failed because of ...)

 © ISO/IEC – All rights reserved

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

11a – 11b Resource ADD resp.conf		resource #	identical to 7
		status_id	The status field is set to “ASSIGNED” if all resources could be successfully allocated, and is set to “FAILED” if not.
12a – 12b Sess SETUP resp.conf		session_id	identical to step 8 = 5
		status_id	indicates if the request has been successful or not
		resource_# (as seen by the server)	provides the client view of the resource which corresponds to the server view in step 7.
13a – 13b Sess SETUP resp.conf		session_id	identical to 12 = 5
		status_id	identical to 12
		resource # (as seen by the STU) association_tag (end-to-end) resource_descriptor	as generated by ses_n in 10.
14a – 14b ses_t to Resident Base App		association_tag resource_descriptor	the association_tag is identical to 9 = 5. The resource_descriptor presents the Client view and is identical to 9.
15		Channel Change Protocol	For detail on the operation CCP see the Client or Broadcast control initiated channel change system dynamics.
16		Selected program channel	At this point the client begins watching the selected program channel

Table 9.3-8 - Client initiated channel change

Flow	Status	Parameter	Comment
1a–1b SVBProgramSelect req.		session_id	In case of SVB realization 1 this is a connection number from the set of connection numbers obtained through U-N Config In case of SVB realization 2 this is the session_id of the session established by the client session
		broadcast_program_id	Is the program channel id of the requested program obtained from the EPG
2a–2b		broadcast_program_id	same as 1

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

3a–3b		tuning_descriptor	In case of ATM this is the VCI/VPI of the channel if static programchannel VPI/VCI mapping is used
		status_id	provides an indication of success or failure and the reason in case of failure
4a–4b SVBProgramSelect conf		session_id	same as in 1
		broadcast_program_id	same as in one or a different barter channel
		tuning_descriptor	same as in 3
		status_id	provides an indication of success or failure and the reason in case of failure
5a–5b		tuning_descriptor	same as in 4=3
6		MPEG TS	The MPEG program is decoded and the Client begins the viewing

Table 9.3-9 - Network initiated channel change

Flow	Status	Parameter	Comment
1a–1b		broadcast_program_id	This is presubscribed
2a–2b		tuning_descriptor	In case of ATM this is the VCI/VPI of the channel if static programchannel VPI/VCI mapping is used
		status_id	provides an indication of success or failure and the reason in case of failure
3a–3b SVBProgramSelect.ind		session_id	In case of SVB realization 2 this is the session-id of the client established SVB session
		broadcast_program_id	same as in 1
		tuning_descriptor	same as in 2
		reason	indicates the reason for the channel change
4a–4b		session_id	The Broadcast Control Application acknowledges the correct reception of the information
		broadcast_program_id	same as in 4=1
		response	provides an indication of success or failure and the reason in case of failure
5a–5b		tuning_descriptor	same as in 3=2
6		MPEG TS	The MPEG program is decoded and the Client begins the viewing

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

9.4 DSDM for Interactive Broadcast (PSTN/ISDN Return Channel)

9.4.1 Overview and Description of System Behavior

9.4.1.1 Allocation of telephone numbers

No assumptions or constraints are made about the allocation of telephone numbers in the enhanced broadcast scenario. Service Providers and/or application writers may chose to allocate 1 or more telephone numbers to users. More than one telephone number may be allocated by an application on the basis of varying levels of quality of service. Telephone numbers may be allocated to any size of the population, from individuals, to anyone wishing able to receive the broadcast or enter it into a suitable STU worldwide.

9.4.1.2 Use of the interaction channel

There are two cases when a interaction channel shall be used in the interactive broadcast scenario:

1. In order to access services as part of a “sign on” to a service provider
2. For interactive participation within an application.

(1) As part of a *sign-on* (initial access) to a service provider:

- A telephone number shall be communicated to the user outside the domain of DAVIC. The number may be obtained from any number of sources, but typically the number shall have been notified to the user using a medium outside the scope of DAVIC. For example: on a smart card mailed directly to the user, or in an advert in a newspaper.
- The user enters the number into the STU. For the interactive broadcast scenario, a smart card (provided by the service provider) could be inserted into a suitable socket on the STU, or a screen based menu (provided as part of the bootstrap application) could instruct the user to enter the number using point and click number selection.
- The user should be offered the opportunity to modify the number. Thus the number should be presented to the user on a screen-based form. allowing him to change any codes implicit in the number, for example: the number could be modified to match the user’s configuration.

(2) From within an interactive application (after start-up):

- The initiation of a interaction channel during an application at (or shortly before) the point where interaction is expected, allows that application to control the semantics regarding the use of the interaction channel. It is expected that this would be done with the approval of the user, either explicitly or implicitly during the application, or by reference to configuration parameters for interaction channel use.
- Because the interaction channel is being used in the known semantics of an application (for example: to place an order within a home shopping application) the telephone number can be automatically acquired by the STU. The number provided in this context may still be modified (either manually by the user or by reference to configuration data) to use the core network routing preferred by the user.

When the interaction channel is already in use for a different telephone number:

- An application may wish to use the interaction channel when the interaction channel is already in use (either with another application running on the same STU or because the PSTN/ISDN/wireless connection is already in use).
- When another application on the same STU is using the interaction channel, any priority for using the channel must be reconciled between the two applications both wishing to use the channel. If necessary, the user can be informed of the problem and asked to choose between which application he wishes to take priority in using the channel.

9.4.1.3 Configuring the Data Link

After a STU is connected through PSTN/ISDN/PLMN to the server, the PPP configuration process is proceeded. This configuration process is constructed by following three phases:

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

(1) Link Control Protocol (LCP) is used to establish data link connection.

(2) PAP / CHAP (RFC 1334) is used to authenticate the STU(optional).

(3) IPCP (RFC1332) is used to configure the IP address and compression type.

In phase (1) and (3), both of “Configure-Request” and “Configure-Ack” packet are sent and received. In phase (3), a STU sends a Configure-Request packet that includes IP Address configuration fields at the beginning. In this case, PPP facilitates the transfer of an IP address from the interactive service provider during the initialization phase of PPP. Note that PPP specifies the IPCP NCP method of getting an IP address into the STU as part of the initialization of the PPP link.

9.4.1.4 Data Transfer and Download

- Data transfer and download describe two techniques of loading data into the STU.

These two techniques map to two DSM-CC User-User facilities available to the application control software in the STU. Data transfer can be provided by User-User interaction. Download is to be provided by the DSM-CC download protocol.

The download and data transfer mechanism can be categorized by the following two cases:

9.4.1.4.1 Synchronized Data Transfer or download

A synchronized data transfer (one where data is requested and specifically provided by the service provider in response to that request) can use:

- a response sent over the interaction channel
- a response sent over the interaction channel which refers to data to be transmitted over a private stream in a broadcast MPEG-TS.

For a requested download where a small amount of data is requested data may be transferred across the interaction channel from the server to the STU. The data is transferred in a DSM-CC User -User message in the response to an RPC from the STU-Top Unit.

For larger data transfer the response sent over the interaction channel to the STU contains DSM-CC User-User BIOP information that uniquely identifies an object in a particular broadcast stream in a particular broadcast network. A timeout is also set, after which time, the requested object shall no longer be broadcast.

9.4.1.4.2 Unsynchronized Data Download or data transfer

Data requested by the STU can be transmitted on a longer term basis than for the ‘synchronized’ download case. The user accesses or is granted access to the data transmission by first receiving a response from the server control data which is transmitted to the user. One example of long-term data transmission is to use ‘object carousels’, which repeatedly broadcast data.

The DSM-CC User-User download protocol includes a negotiation phase to establish the requirements for the download, followed by the download. The DSM-CC User-User download protocol informs the STU of a unique identity of the required data, the location of the required data, and the period of time over which it can be accessed. It may be necessary to supply the user with any access control mechanisms required to read the data, such as decryption keys.

Depending on the success of the download, it may be necessary to repeat some or all of the download. Any repetition of the download shall be coordinated between the service provider and STU. The DSM-CC User-User download protocol allows retransmission of selected blocks which have failed to download successfully.

Example DSM-CC U-U scenario 1: STU requesting data for point to point delivery .

1a) Data sent over broadcast channel to STU

- RPC request containing DSM-CC U-U primitives from STU to server
- RPC reply from server to STU RPC O.K. Reply identifies the network, MPEG-TS, channel, object (using DSMCC BIOP) which is to be delivered over the broadcast channel, together with a timeout for the receipt of the object by the STU.
- Content transmitted over the MPEG private data channel to STB.
- 1b) Data sent over the interaction channel

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

- RPC request from STU to server
- RPC reply from server to STU RPC O.K. including the Content/Data embedded in the response DSM-CC U-U primitive response.
- Example DSM-CC U-U Scenario 2 STU requests a download.
- 2a) Data sent over broadcast channel to STU
- Request containing DSM-CC Download Control from STU to server
- DSM-CC download control dialogue between STU and server. During the download control dialogue the server informs the STU of the identity of the download data block(s) to be delivered over the broadcast channel. The BIOP identifies the download data block messages in which the requested data is to be sent over the broadcast channel.
- Content transmitted over the MPEG private data channel to IP address of STB.
- 2b) Data sent over the interaction channel
- Request containing DSM-CC Download Control from STU to server
- DSM-CC download control dialogue between server and STU. The Dialogue includes the Content/Data embedded in a response.
- User compatibility fields in DownloadInfoResponse allow the STU and server to identify what download capability (hardware and software) the STU has.

9.4.1.5 Session control (reason for absence of)

Apart from signaling, no core network resources have been identified which affect the DAVIC end-to-end scenario, hence the S3 flow is not needed. A characteristic of the interactive broadcast scenario is that the broadcast channel is assumed to function properly. To introduce the ability to automatically report errors in broadcast transmission would swamp the broadcast service provider with error reports should a transmission error occur.

9.4.1.6 Interaction channel Configuration

Screen-based controls provided by a usage configuration application can allow the user to configure how the STU shall react when using an automatically loaded telephone number intended for use as part of an interactive broadcast service. The automatic dialing of a telephone number without prior user approval is not recommended. For example, in a multiple network environment the user may choose to modify the number in order to access a specific network between the STU and the server. A usage configuration application may also offer the user screen-based prompting prior to setting up the interaction channel.

The user may be able to manually close the interaction channel at any time, using a screen-based control application.

Configuration rules about the duration of inactivity on the interaction channel before it is cleared down may also be entered as part of a usage configuration application.

9.4.1.7 International Distribution

Some broadcast services (such as those using satellite) have a large international footprint by nature. Thus, international growth of such services is likely. To prevent customers having to interact via international PSTN/ISDN links, or even long distance national connections, the Interactive Service Provider may choose to provide local or national service access points. The details of these access points, telephone numbers etc. can be carried in the broadcast object carousels as part of the application and displayed on the TV screen using the MHEG-Java tools, to enable the customer to choose the access server. This approach can also be used to solve language problems in the customer-service interaction.

Setting up local or national access points should not be a pre-requisite for interactive broadcast services. Intelligent network control of charging and address resolution can be used to avoid forcing the user into paying for a connection over the physical distance between the user and the interactive service provider. This permits alternative sources of funding (e.g. advertising) to be used to pay for the interaction channel

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

9.4.2 Protocol Network Architecture for Interactive Broadcast

See Figure 9.4-1 – *Interactive Broadcast Scenario using a PSTN/ISDN interaction channel*, and Figure 9.4-2 – *Interactive Broadcast Scenario using a PLMN interaction channel at A1*.

 © ISO/IEC – All rights reserved

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

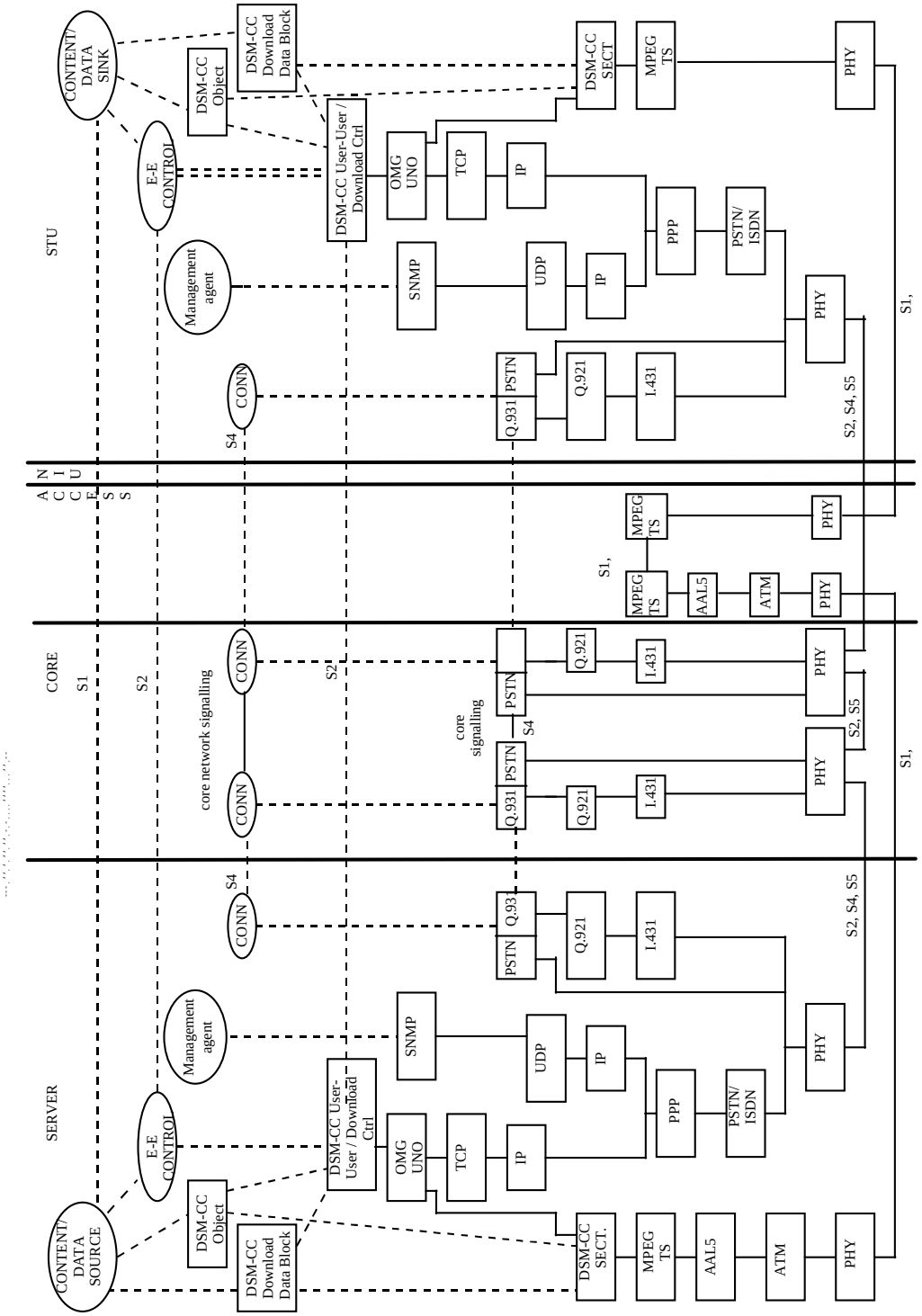


Figure 9.4-1 - Interactive Broadcast scenario using a PSTN/ISDN interaction channel

(Note: The audio/visual S1 content has been removed because of a lack of space)

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

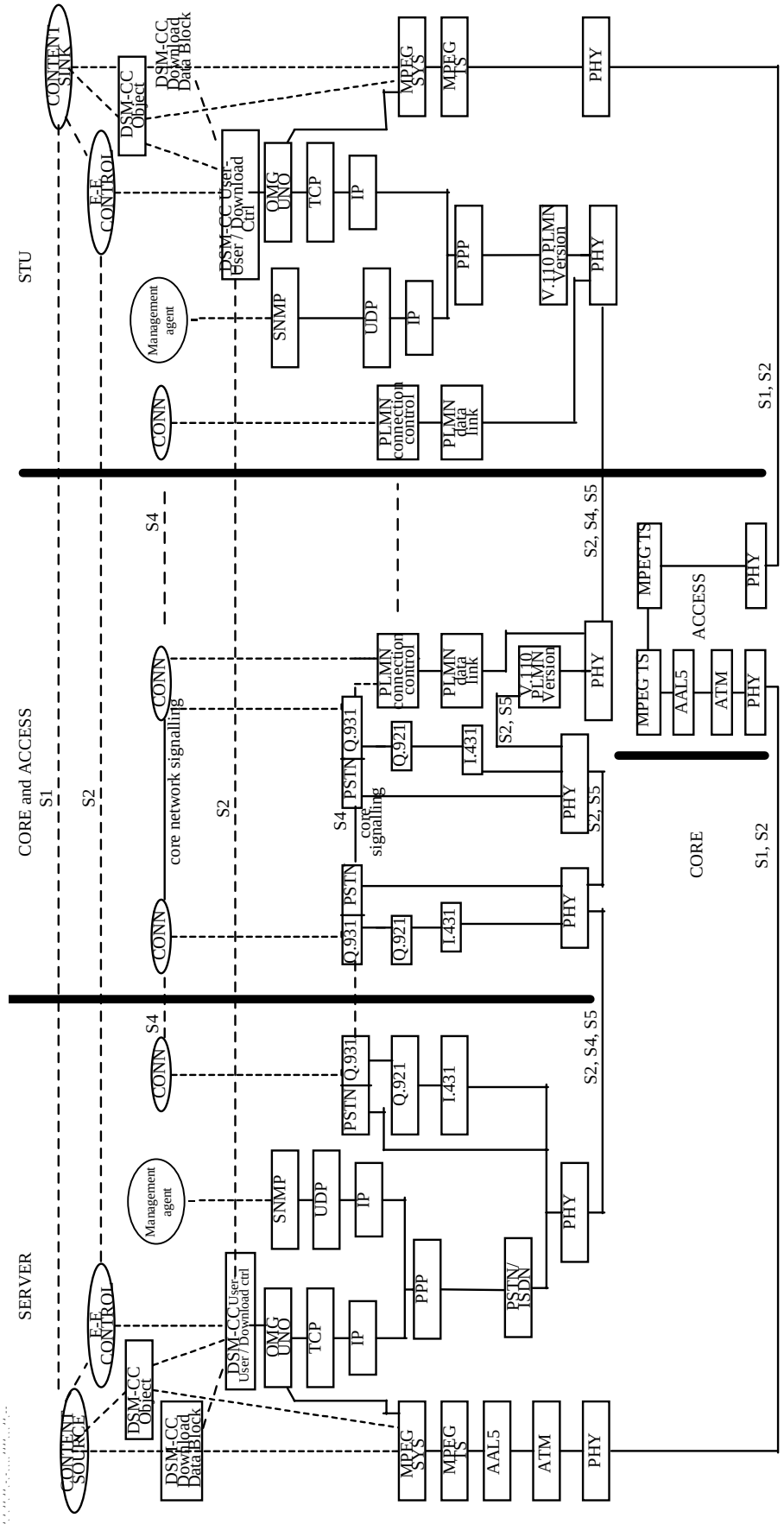


Figure 9.4-2 - Interactive Broadcast scenario using a PLMN interaction channel at A1

(Note: The audio/visual S1 content has been removed because of a lack of space)

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

9.4.3 DAVIC System Dynamic Flows for Interactive Broadcast

9.4.3.1 Interaction Channel Call/Connection Setup

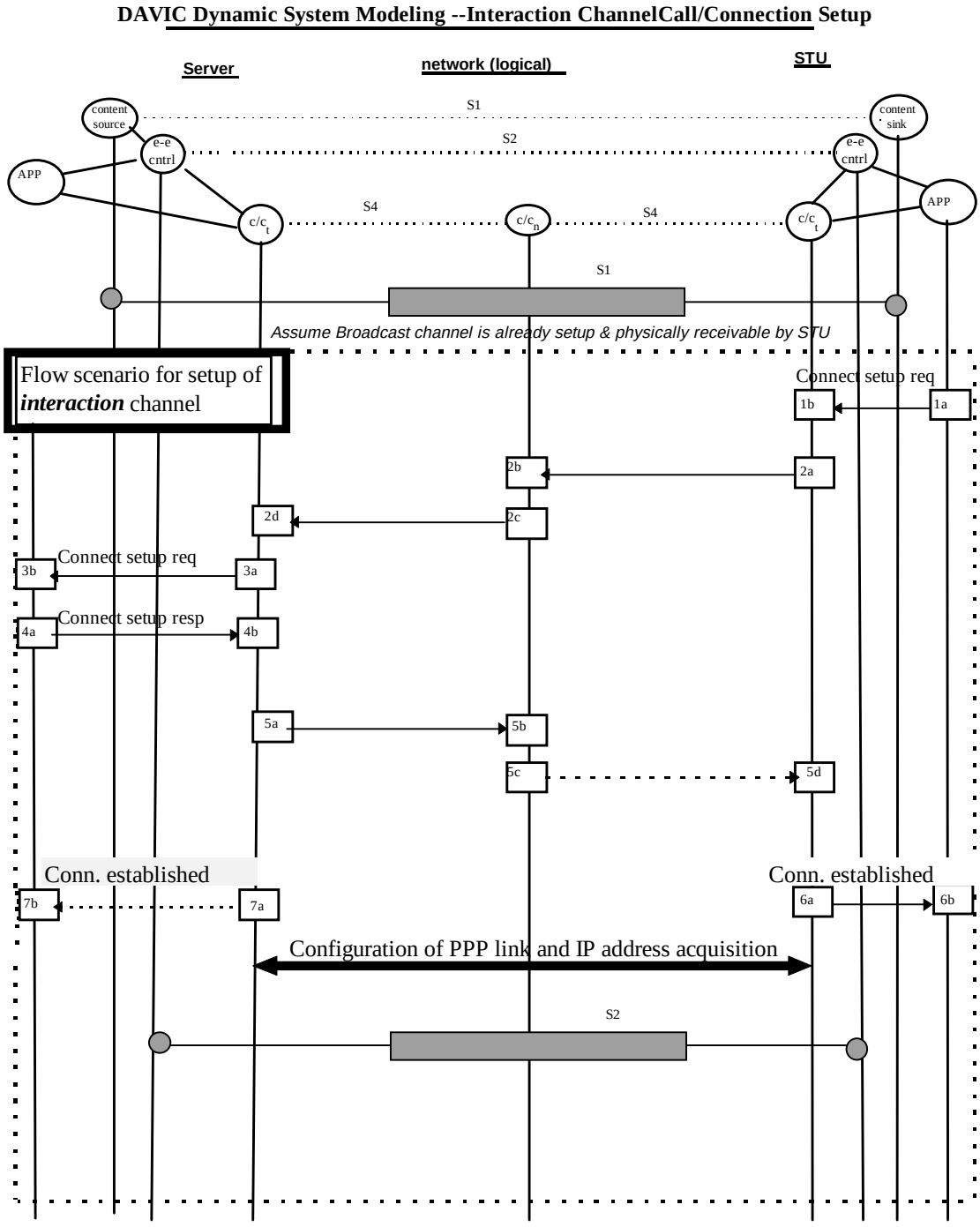


Figure 9.4-3

9.4.3.2 Release Sequences (STU and Server Initiated)

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

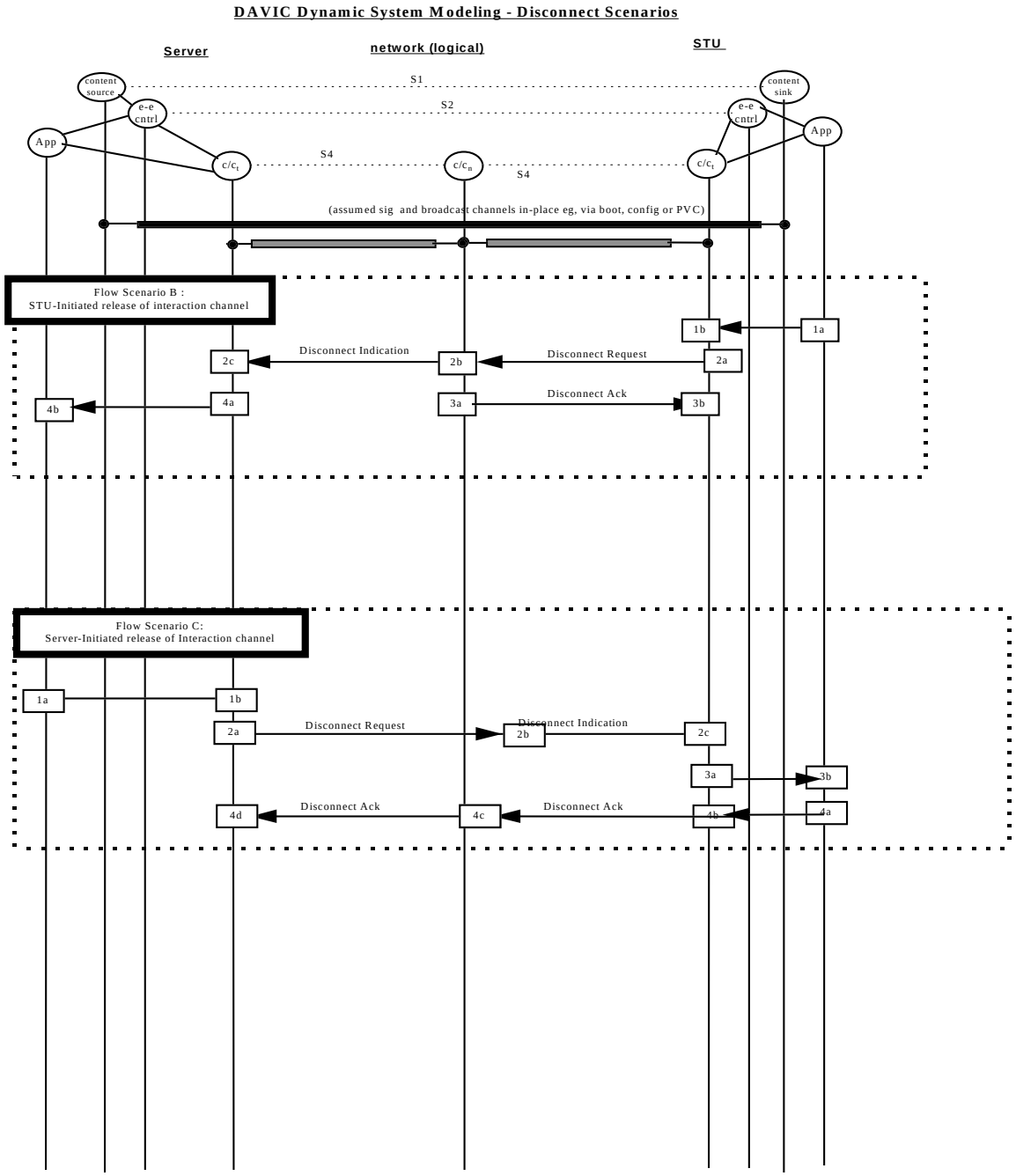


Figure 9.4-4

9.4.4 Functional Entity Actions for Interactive Broadcast

9.4.4.1 Interaction Channel Call/Connection Setup

Table 9.4-1 – Interaction Channel Call/Connection Setup

1a – 1b	The application initiates a connection request using an E164 number which has either been provided over the broadcast channel or a source outside DAVIC, e.g. a newspaper advert.
2a – 2b - 2c – 2d	A circuit switched connection is established between the STU and Server using the PSTN/ISDN.

 © ISO/IEC – All rights reserved

--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

3a – 3b	An incoming call indication is received by the Server.
4a – 4b	The Server application entity instructs the connection entity to accept the connection.
5a – 5b *5c – 5d	The Server's acceptance of the incoming call is signaled to the network. * In the ISDN case this acceptance is signaled to the STU's connection entity. In the PSTN case acceptance is recognized by the opening of the circuit switched path over which the modems begin to sync.
6a – 6b	The STU application receives confirmation that the connection has been established. Either resulting from the synchronized modems or via the ISDN altering response message.
7a – 7b	The Server application receives confirmation that the connection has been established. As a result of the synchronization of the modems (PSTN case only). A PPP connection is initiated between the server and the STU, during which the server selects an IP address and sends it to the connection entity.

Notes:

Where there are no available ports on the server, the STU may retry establishing the connection, or it may choose to use different servers (if other numbers have been included as part of the interaction channel control software application).

Ultimately, if an interaction channel cannot be setup, then it may be necessary to inform the user (via the TV screen) that interaction with broadcast services is not possible at the present time.

9.4.4.2 Release Sequences (STU and Server Initiated)

Table 9.4-2 - Sequence A: STU Initiated Release.

1a - 1b	The application initiates a disconnect request to the network by issuing a close connection command. This causes the network interface to issue the relevant protocol command to the network.
2a - 2b - 2c	The disconnection command is passed between the network nodes involved in the connection.
3a - 3b	The network acknowledges the disconnection request.
4a - 4b	The client application receives an indication that the Set-Top has cleared the connection and updates interaction channel management data where necessary.

Table 9.4-3 - Sequence B: Server-Initiated Disconnect

1a - 1b	The server application initiates a disconnect request to the network by issuing a close connection command. This causes the network interface to issue the relevant protocol command to the network.
2a - 2b - 2c	The disconnection command is passed between the network nodes involved in the connection.
3a - 3b	The network acknowledges the disconnection request.
4a - 4b	The client application receives an indication that the Server has cleared the connection and makes changes to the application software where necessary.

9.4.4.3 Release Sequence (Forced Disconnect)

Where the network releases the connection, this will be detected by both the client and server end-points of the interaction channel. If necessary, the client application software shall inform the user that a problem has occurred with the interactive channel. Attempts by both end-points to reestablish the channel shall be possible. In order that both channels don't simultaneously attempt to call each other, application software shall be written to coordinate the re-establishment of the interaction channel between the client and server. Alternatively, whoever (client or server) was originally responsible for setting up the disconnected interaction

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

channel should be responsible for reestablishing it. The choice of these sets of actions should be agreed between the client and server soon after set-up of the interaction channel.

9.5 DAVIC Architecture and DSDM for Internet Access

9.5.1 Overview

9.5.1.1 Introduction

DAVIC Direct Internet Access is used to provide the end-user with either "full" or "client" Internet access (RFC 1775) using PC connected to an STU or a standalone STU. The assumption is that no additional software will be required on the PC or the Router for Direct Internet Access beyond what is required at present for Internet access.

A number of tools for Direct Internet Access are possible, each with its own characteristics. A Internet access tool may or may not co-exist with other tools in the same STU.

Note, when Internet access is the only tool in a STU, the STU "appears" like a modem to the user but is still called a STU in this specification in order to maintain compatibility with the DAVIC model.

9.5.1.2 Why DAVIC Internet Tools?

The DAVIC Internet tools allow DAVIC equipment to bind physical addresses of devices at a home, such as PCs, to IP addresses. This binding is achieved through a DAVIC STU in the home interacting with network based DAVIC equipment using Internet services, such as ARP and Inverse ARP. In the following sections, DAVIC subsystems are used, within a series of scenarios, to give PCs increasingly more freedom of access to Internet Service Providers.

A single PC is connected to an Internet Service Provider:

(1) A single PC at the home is bound to a fixed Internet Service Provider through an Internet Service Access Provider (ISAP) Router, as shown in Figure 9.5-1. The STU shields the network dependency.

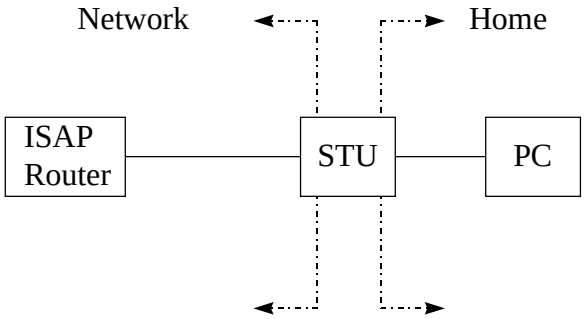


Figure 9.5-1

(2) A single PC is provided access to an Internet Service Provider, chosen on demand by the end user, as illustrated in Figure 9.5-2

 © ISO/IEC – All rights reserved

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

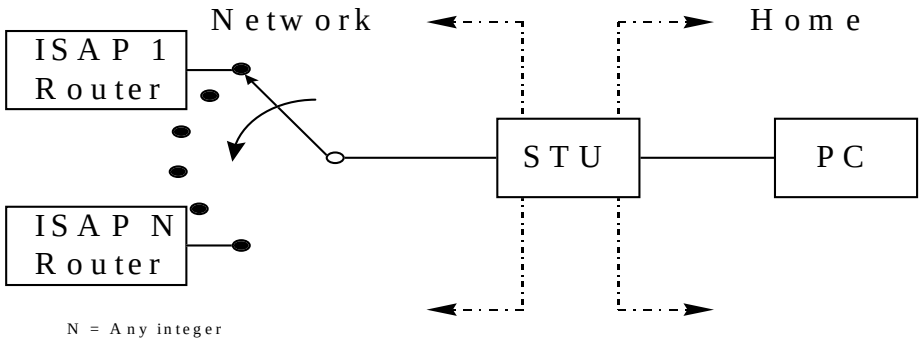


Figure 9.5-2

(3) Any PC, of a number of PCs connected to a STU, is provided access to a chosen ISAP by the user of the PC as shown in Figure 9.5-3.

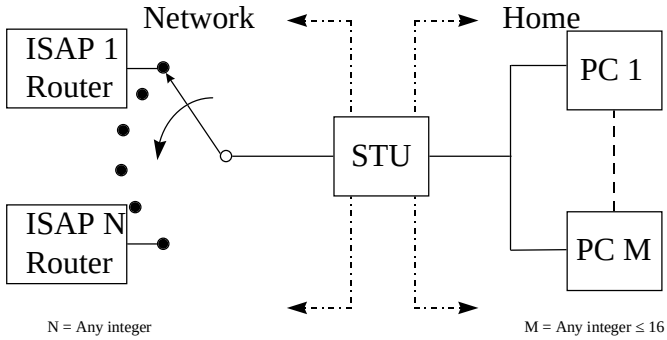


Figure 9.5-3

DAVIC provides a user the benefit of leveraging already available broadband access facilities, e.g., ADSL, FTTC, HFC and Hertzian for broadband Internet access using existing off the shelf protocols.

9.5.1.3 Categories of Tools for DAVIC Direct Internet Access:

The categories below are selected in order to enable PCs increased freedom of access to Internet Service Providers. The increased features are obtained through incremental addition of subsystems from one category to the next.

Category 1-- Static/null session, Internet Service Access Provider (ISAP) is fixed and pre-agreed between the Network Provider and end user. Two scenarios are supported in this category:

Scenario 1a: Connection to ISAP is pre-established by the Network Service Provider through ATM PVC's and/or Channel ID and optionally a MPEG PID.

Scenario 1b: Connection to ISAP can be established dynamically using ATM SVC's (including a section using non-ATM HFC). Both proxy signaling and Q.2931 resident in STU are supported.

Category 2 – Dynamic DAVIC/DSM-CC session, Internet Service Access Provider (ISAP) is fixed and pre-agreed between the Network Provider and end user. The connection to the ISAP Router is established on demand. Two scenarios are supported in this category:

Scenario 2a: Connection (ATM PVC or ATM SVC including a section using non-ATM HFC) is established through a DAVIC session to a DAVIC server.

Scenario 2b: Same as scenario 2a except a physical DAVIC server is not required. The server functionality is physically co-located with the DAVIC SES(n) entity (and with the proxy signaling entity (SES(t)) for Physical Scenarios 1 & 3.

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Category 3-- Dynamic DAVIC/DSM-CC session, Internet Service Access Provider (ISAP) can be selected by the end user. The connection to the ISAP Router is established on demand. Two scenarios are supported in this category:

Scenario 3a: Connection is established through a DAVIC session to a DAVIC server which also acts as a Web server.

Scenario 3b: Same as scenario 3a except a physical DAVIC server is not required. The server functionality is physically co-located with the DAVIC SES(n) entity (and with the proxy signaling entity (SES(t)) for Physical Scenarios 1 & 3.

Category 4-- Dynamic DAVIC/DSM-CC session, Internet Service Access Provider (ISAP) can be selected by the end user. Connections to a single ISAP may be established at a time. One scenario is supported in this category:

Scenario 4: Connections are established to multiple ISAPs through a DAVIC session to a DAVIC server.

The tools in the following tables are supported in all Physical Scenarios shown in the VoD section of this part of ISO/IEC 16500. It is assumed that use of proxy signaling or PVC is used in DAVIC Physical Scenarios 1, 3 or 4. In case of Physical Scenario 2, the proxy is replaced by Q.2931 signaling resident in the STU to establish connection to the ISAP.

Table 9.5-1 - Summary DAVIC Internet Access Scenarios., Category 1

DAVIC Direct Internet Configuration	Description	Subsystems
Category 1	Static/null session, Internet Service Access Provider (ISAP) is fixed and pre-agreed between the Network Provider and end user	Scenario 1a • PC • STU • DSM-CC U-N Config Server • ISAP Router for static IP assignment or capable of relaying DHCP/BOOTP in case of dynamic IP assignment • DHCP/BOOTP server in case of dynamic IP address assignment • Server for Internet Service
		Scenario 1b • PC • STU • DSM-CC U-N Config Server Pseudo-session control for 1b • Signaling Proxy Agent for Physical Scenarios 1 & 3, Q.2931 resident in STU for Physical Scenario 2. • ISAP Router for static IP assignment or capable of relaying DHCP/BOOTP in case of dynamic IP assignment • DHCP/BOOTP server in case of dynamic IP address assignment Server for Internet Service

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table 9.5-2 - Summary DAVIC Direct Internet Access Scenarios, Category 2

DAVIC Direct Internet Configuration	Description	Subsystems
Category 2	Dynamic DAVIC/DSM-CC session, Internet Service Access Provider (ISAP) is fixed and pre-agreed between the Network Provider and end user. The connection to the ISAP Router is established on demand.	<u>Scenario 2a</u> • PC • STU • DAVIC SES(n) (e.g., in a DSM-CC SRM) • DSM-CC U-N Config Server • Signaling Proxy Agent for Physical Scenarios 1 & 3, Q.2931 resident in STU for Physical Scenario 2. • Network Provider Admin DAVIC Server is physical server • ISAP Router for static IP assignment or capable of relaying DHCP/BOOTP in case of dynamic IP assignment • DHCP/BOOTP server in case of dynamic IP address assignment • Server for Internet Service
		<u>Scenario 2b</u> • subsystems are the same as for scenario 2a above except the Admin server code is co-located with SES(n) and proxy signaling agent, if used (e.g., in a DSM-CC SRM)

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Table 9.5-3 - Summary DAVIC Internet Access Scenarios, Categories 3a, 3b & 4

DAVIC Internet Scenario	Description	Subsystems
		•
3a and 3b	Dynamic DAVIC/DSM-CC session, Internet Service Access Provider (ISAP) can be selected by the end user. The connection to the ISAP Router is established on demand	• Integrated or separate STU and PC • DSM-CC U-N Config Server • DAVIC SES(n) (e.g., a DSM-CC SRM) • Signaling Proxy Agent for Physical Scenarios 1 & 3, Q.2931 resident in STU for Physical Scenario 2. • Network Provider Admin dual DAVIC-Web Server is physical server for 3a. (Note: in case of 3b the Admin server code is co-located with SES(n) and proxy signaling agent, if used (e.g., in a DSM-CC SRM) • ISAP Router(s) • IP server(s)
4	Dynamic DAVIC/DSM-CC session, Internet Service Access Provider (ISAP) can be selected by the end user. Connections to a single ISAP may be established at a time.	• Integrated or separate STU and PC • DSM-CC U-N Config Server • DAVIC SES(n) (e.g., a DSM-CC SRM) • Signaling Proxy Agent • Directory Server • ISAP DAVIC Server • ISAP Router(s) • IP server(s)

Figure 9.5-4 and Figure 9.5-5 provide the system level connectivity for each of the tools.

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

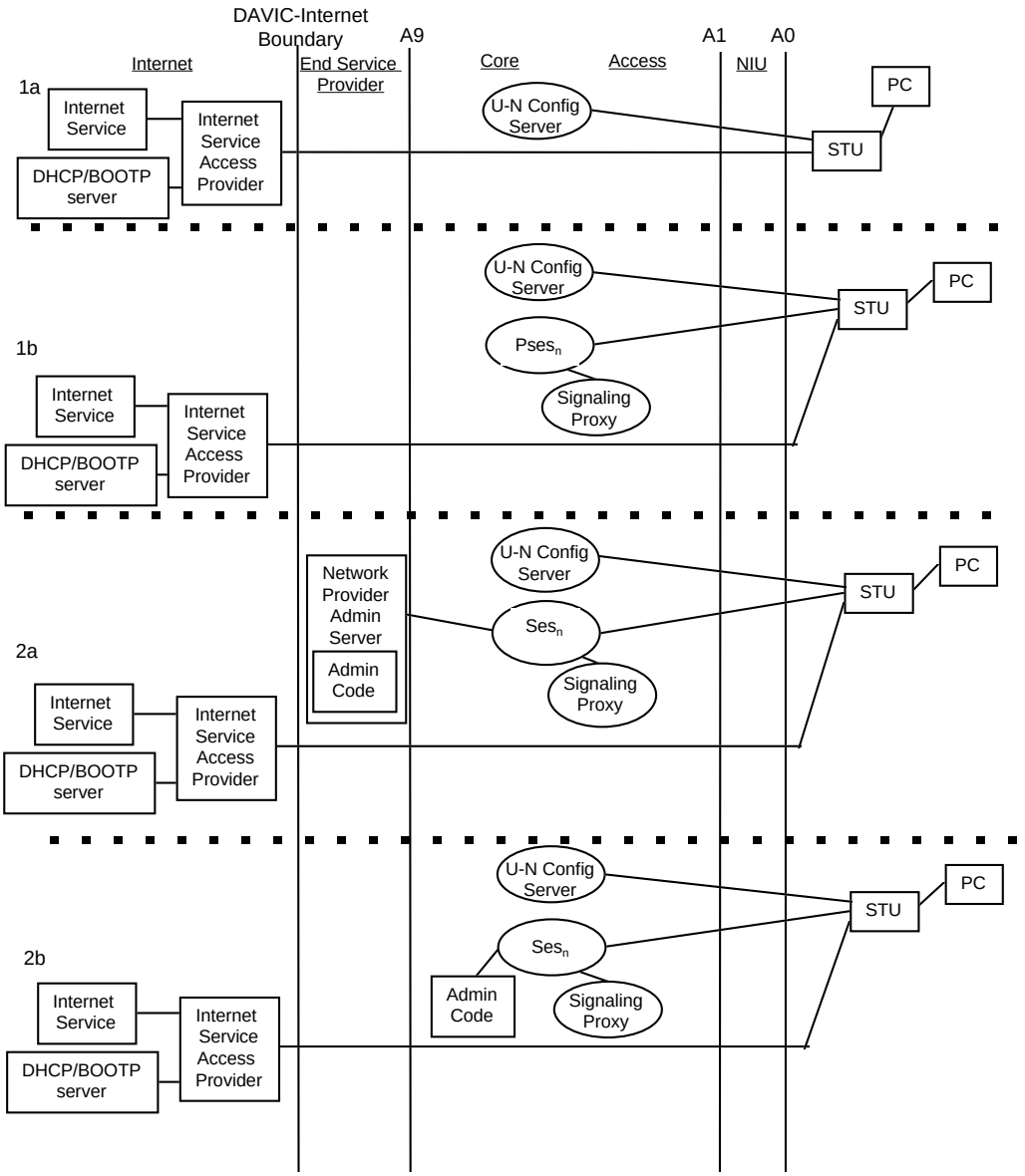
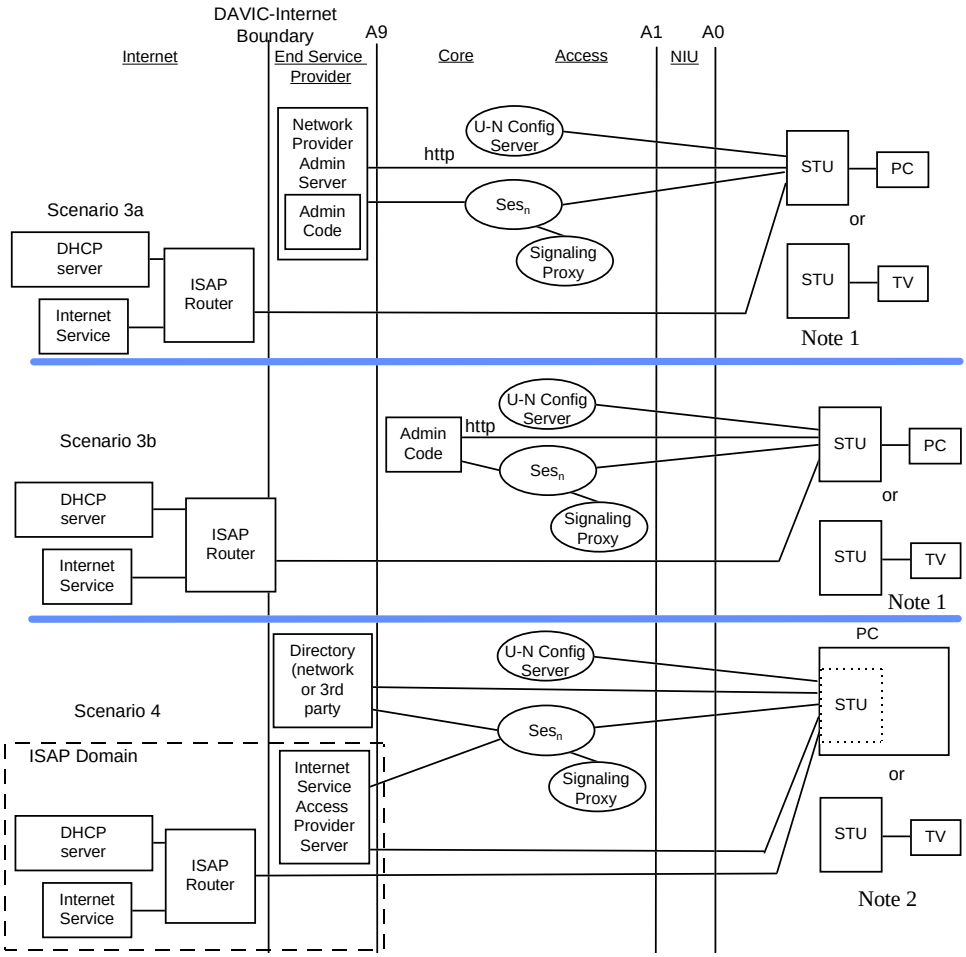


Figure 9.5-4 - System level Connectivity for DAVIC Direct Internet Access Scenario Options

Note: In Figure 9.5-4, only the case where proxy signaling is used is illustrated. For Physical Scenario 2, Q.2931 connection control signaling is located in the STU and the proxy agent is not used.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale



Note 1: Other arrangemets not shown are PC subsuming STU and PC subsuming NIU and STU
Note 2: Other arrangemets not shown are separate STU and PC, and PC subsuming NIU and STU

Figure 9.5-5 - System level Connectivity for DAVIC Internet Access Scenario Options

9.5.1.4 Assumptions and Definitions:

ISAP Router:

- Any of the IP routers belonging to an ISAP. An STU gains access to the Internet by connecting to a designated ISAP Router. The following assumptions apply:
- The ISAP Router ports to which STU's can be connected use the inATMARP function of the classical IP on ATM (RFC 1577 and RFC 1293).
- The ISAP Router ports use the LLC/SNAP encapsulation option of RFC 1483.
- In case the ISAP supports DHCP then ISAP selection can be used otherwise the IP shall be statically assigned and limited to scenarios 1a, 1b, 2a and 2b.
- The Router shall obtain the IP address of the PC through inATMARP via the STU. As noted below under PC behavior and STU Data Switcher assumptions, the PC shall obtain its IP address using DHCP or BOOTP via DSM-CC DHCP relay (see section on Internet Access DAVIC server DHCP Relay Operation) or Access Router relay. The STU shall obtain the IP address from the PC through the Ethernet ARP or derive it from the first IP packet arriving from the PC. Other methods of dynamic address resolution, such as using IPCP, are not precluded once the appropriate standards for operation over ATM are established.
- It is assumed that the ISAP Router can configure its ports to support the MTU size of the STU Dataport such that no IP fragmentation is required in the STU. The incoming side of the router towards the STU is configured for MTU 1500 bytes. The outgoing side from the STU supports IEEE 1394 MTU 2024 bytes

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

(Baseline document # 41). The MTU Discover (RFC 1191) shall be implemented at the PCs connected to the STU through the IEEE 1394 port.

- All ISAP Router ports which can be connected to the STU are ATM SVC's or PVC's. The connection is bound to the IP address through inATMARP from which the router can infer the IP address of the PC attached to the STU.

STU Data Switcher:

- The STU Data Switcher channels the packets (e.g., in the case of Internet access IP packets) received from the Dataport to a DAVIC network connection resource (e.g., the PVC or SVC). A DAVIC network resource consists of a connection to the ISAP Router for each PC. The connection may be over ATM, PPP operating over PSTN/NISDN/PLMN and may include, in the downstream direction, MPEG2-TS in the access network. In case of PPP the STU contains MTU Discover (RFC 1191) functionality to reduce the size of the MTU to the one used in PPP.
- A binding is made between an interface (towards the ISAP Router) on the one hand and the PC on the other hand. Depending on the scenario, different methods are used:

Scenario 1a

- In case of multiple PCs to a STU there are as many PVC's provisioned per STU as there are PCs connected to the STU. The Data Forwarder is replaced with a Data Switcher. Access to a different ISAP for each PC is not permitted in scenario 1a.
- In case the IP address is preassigned and manually entered into the PC, then the first IP packet from the PC will be used by the STU to create the binding with a non-assigned PVC. In case a DHCPDISCOVER is received from a PC the STU chooses a connection and logically binds it to the MAC address of the PC.
- When PVC connections are used at the ISAP Router, the possibility exists that the router sends a packet downstream to the STU before STU or Access Router learns the IP address of the PC. The STU or the Access Router may either discard the packet, or optionally the STU can send an Ethernet ARP, for the destination IP address indicated in the packet, to learn the PC Ethernet MAC address. If the PC responds, the STU learns the IP & MAC address of the PC. The STU thus establishes a logical link between the connection on which the IP was received and the MAC address of the PC. Any IP messages coming from that PC will from there on be sent over the logically bound PVC and the same will happen for the IP packets in reverse arriving on the PVC from the ISAP router.

Scenario 1b:

- Access to a different ISAP for each PC is not permitted in scenario 1b.
- The Data Forwarder is replaced by a Data Switcher.
- If a DHCPDISCOVER or Ethernet ARP or IEEE 1394 ARP is received from a PC the STU begins a new pseudo-session SetUp and logically binds the resulting connection to the ISAP router to the MAC address of the PC. Any IP messages coming from that PC will from there on be sent over the logically bound connection and the same will happen for the IP packets in reverse arriving on the connection from the ISAP router.
- The Data Switcher supports DHCP Relay functionality where a DHCPDISCOVER initiates a pseudo-session and reports back the DHCPOFFERs received through the SessionSetUpResponse message DHCP resource descriptor. The DHCPRESPONSE and DHCPACK messages are passed through to and from the established connection to the ISAP Router unaltered.

Release of Connection to the ISAP

- STU power-down, reset or session release
  With the power down of the STU the connection bindings disappear. $pSes_n$ can also request a Session Release (which affects one PC) or STU Reset. In those situation the end-user of a connected PC is not explicitly notified, the result however will be a delay experienced by the WWW Service in the PC since a subsequent receipt of IP packet from the PC will establish a new psess and connection with the ISAP.
- PC prompted connection release
  In a graceful shutdown, when DHCP is used, the PC sends a If DHCPRELEASE, the Data Switcher in the STU monitors the message and sends the message to the router and the Main Resident Application (MRA). The MRA proceeds to release the pseudo-session corresponding to the PC.
- STU initiated release
  As an example of a mechanism that could be used, the STU monitors the IP flow from each PC. After a

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

period of inactivity of 2 minutes, the STU proceeds by sending an Ethernet ARP at each 2 minute interval using the IP address of the PC, if no response is received after 3 such attempts the STU proceeds to release the psession. If an ARP Reply is not received from the PC, the psession shall be released if IP packet inactivity from the PC persists for a duration of Trel specified at UN Config time. A subsequent receipt of IP packet from the PC will establish a new psess and connection with the ISAP.

Scenarios 2a and 2b:

- Access to a different ISAP for each PC is not permitted in scenarios 2a and 2b.
- The Data Forwarder is replaced by a Data Switcher.
- If a DHCPDISCOVER or Ethernet ARP or IEEE 1394 ARP is received the STU begins a new session SetUp and logically binds the resulting connection to the ISAP router to the MAC address of the PC. Any IP messages coming from that PC will from there on be sent over the logically bound connection and the same will happen for the IP packets in reverse arriving on the connection from the ISAP router.
- The Data Switcher supports DHCP Relay functionality where a DHCPDISCOVER initiates a session and reports back the DHCPOFFERs received through the SessionSetUpResponse message DHCP resource descriptor. The DHCPRESPONSE and DHCPACK messages are passed through to and from the established connection to the ISAP Router unaltered.

Release of Connection to the ISAP

- STU power-down, reset or session release
  With the power down of the STU the connection bindings disappear. Ses_n can also request a Session Release (which affects one PC) or STU Reset. In those situation the end-user of a connected PC is not explicitly notified, the result however will be a delay experienced by the WWW Service in the PC since a subsequent receipt of IP packet from the PC will establish a new session and connection with the ISAP
- PC prompted connection release
  In a graceful shutdown, when DHCP is used, the PC sends a DHCPRELEASE, the Data Switcher in the STU monitors the message and sends the message to the router and the Main Resident Application (MRA). The MRA proceeds to release the session corresponding to the PC.
- STU initiated release
  As an example of a mechanism that could be used, the STU monitors the IP flow from each PC. After a period of inactivity of 2 minutes, the STU proceeds by sending an Ethernet ARP at each 2 minute interval using the IP address of the PC, if no response is received after 3 such attempts the STU proceeds to release the session. If an ARP Reply is received from the PC, the session shall be released if IP packet inactivity from the PC persists for a duration of Trel specified at UN Config time. A subsequent receipt of IP packet from the PC will establish a new session and connection with the ISAP.

Scenarios 3a and 3b:

- The STU is connected to a Network Service Provider Admin Server which has an IP address within the domain assigned to the Network Service Provider. Each of the PCs connected to the STU will have a browser bookmark for the Network Services Provider Admin Web Server.
- It is permitted each PC to access a different ISAP. During the ISAP selection it is ensured that the selected ISAPs do not have conflicting network domain addresses. The checking is carried out at selection time in the http Admin server.
- The Data Switcher supports IP initialization function. A way to do this is that it responds to DHCPDISCOVER with a DHCPOFFER containing a dummy IP address with a lease time of 2 s and will complete the cycle of DHCPREQUEST and DHCPACK. At this stage of the state table in the STU a session is not initiated as in 4 below. However this permits the PC to establish a connection with the Admin http server for a choice of an ISAP.
- In case of an http packet is received from a PC with the configured address of the Network Service Provider Admin Web server, the Data Switcher will substitute the source PC IP address (assigned a dummy address as above) by its own STU IP address and PC's MAC address to the http as input to the Web server.(i.e., http://<location>/<path>?<PC's MAC address>). As a result of the PC MAC address the Admin Web Server will present a directory of ISAPs from which the PC can make its choice. The Admin Web Server then sends a PassThrough message to the STU carrying the MAC address. The STU initiates a session for the PC and the Data Switcher binds the connection to the MAC address of the PC. Any IP messages coming from that PC (including the DHCPDISCOVER) will from there on be sent over

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

the logically bound connection and the same will happen for the IP packets in reverse arriving on the connection from the ISAP router.

- The Data Switcher supports DHCP Relay functionality where a DHCP Discover initiates a session and reports back the DHCPOFFERs received through the SessionSetUpResponse message DhcpOffer resource. The DHCPRESPONSE and DHCPACK messages are passed through to and from the established connection to the ISAP Router unaltered.

Release of Connection to the ISAP

- STU power-down, reset or session release
  With the power down of the STU or STU Reset by ses_n the connection bindings disappear. Ses_n can also request a Session Release (which affects one PC). In those situation the end-user of a connected PC is not explicitly notified, the result however will be a delay experienced by the WWW Service in the PC since a subsequent receipt of IP packet from the PC will establish a new session and connection with the ISAP. Release can also be:
- PC prompted connection release
  In a graceful shutdown, when DHCP is used, the PC sends a DHCPRELEASE, the Data Switcher in the STU monitors the message and sends the message to the router and the Main Resident Application (MRA). The MRA proceeds to release the session corresponding to the PC.
- STU initiated release
  As an example of a mechanism that could be used, the STU monitors the IP flow from each PC. After a period of inactivity of 2 minutes, the STU proceeds by sending an Ethernet ARP at each 2 minute interval using the IP address of the PC, if no response is received after 3 such attempts the STU proceeds to release the session. If an ARP Reply is not received from the PC, the session shall be released if IP packet inactivity from the PC persists for a duration of Trel specified at UN Config time. A subsequent receipt of IP packet from the PC will be ignored and the PC needs to start the ISAP selection process from the beginning.

Scenario 4:

- Scenario 4 allows the use of an integrated Server platform where DAVIC and Internet services coexist. Integrated or separate STU and PC can be used. The full Data Switcher functionality is reduced to the functionality of STU DHCP relay only. In the STU DHCP Relay a DHCP Discover initiates a session and reports back the DHCPOFFERs received through the SessionSetUpResponse message DhcpOffer resource descriptor (Appendix B - Internet Access DAVIC server- DHCP Relay Operation). The DHCPRESPONSE and DHCPACK messages are passed through to and from the established connection to the ISAP Router unaltered. When other PCs are connected to the STU or the PC using the integrated platform through the IEEE 1394 and/or 10BaseT the connected PCs will not be working on an integrated platform. In those cases the full Data Switcher functions will be implemented on the integrated platform and 8will operate for the connected PCs according to scenario 3a/3b while the integrated platform will operate according to scenario 4. Multiple STU's or PCs using integrated platform can be connected to the NT through A1* interface.

Access Router:

- It contains DHCP relay function through which it can extract the IP address of the PC and use the information to logically bind the PC to the connection based on the source IP.
- It performs the routing functions of the IP packets received from the network to the MPEG Access Control and the PPP access Control based on the destination STU IP's and the mode of operation using PPP downstream only, MPEG TS only or both for the specific session indicated on the GIT (Generic Identifier Transport) of the Q.2931 of the ATM connection as indicated by ses_n. through the A7 interface, see Figure 34- IWU Functional Components.
- It routes the IP's received from the MPEG Access Control and the PPP access Control based on the source IP address and the destination IP address.

MPEG TS Access Control:

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

- It chooses a PID and sends datagram_sections using the STU MAC address, to the STU. The MAC address is derived from the PCs IP address from a table built by the Access Router using STU Client ID information from ses_n.
- It prepares the client view of the resource descriptor for the Sip and sends it to the ses_n over A7 coupled with locally generated resource ID.

PPP Access Control:

- It assigns a port number to the IP received from DAVIC servers. S3 and http connections are assigned well known port numbers. No port numbers for the connections to the ISAP routers are assigned since these are differentiated by the IP of the destination PC connected to the STU.
- The assigned port number is communicated to the ses_n over A7 coupled with locally generated resource ID together with an association tag shared with the MPEGTS descriptor if it is used for the downstream IP path.

PC Behavior:

- In scenarios 3a/b and 4 the PC shall use DHCP to get its IP address.
- Shall implement MTU Discover RFC 1191 in case IEEE 1394 is used in the data port or PPP is used in the access.

Dataport:

- IEEE 1394 is normative and 10Base T is optional.
- PCs connected to IEEE 1394 can communicate with each other, but are not required to communicate with PCs connected to 10BaseT and vice versa.

Integrated STU PC Package:

Two examples of packaging STU with the PC are provided Figure 9.5-6 below:

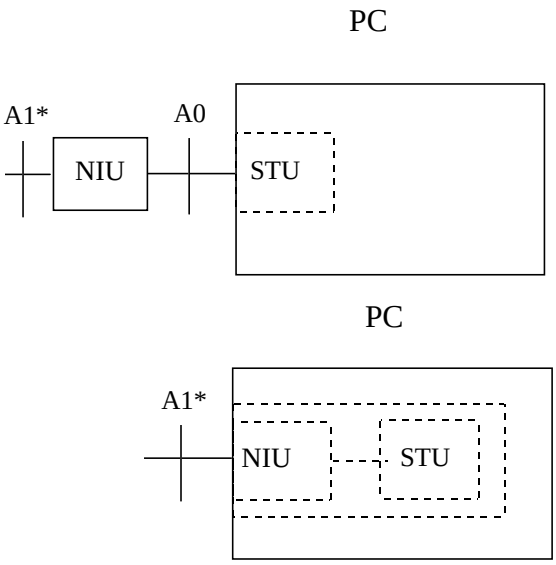


Figure 9.5-6

Configuration 1 scenario characteristics:

- No TV required
- End-user not explicitly notified of the STU access to ISAP
- Dedicated STU security
- Predetermined access QoS per ISAP per STU
- Pre-established connections to the ISAP for scenario 1a
- On demand connections to the ISAP for scenario 1b

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Configuration 2 scenario characteristics:

- No TV required
- User not explicitly notified of the STU access to ISAP
- Dedicated STU security
- Predetermined access QoS per ISAP per STU
- On demand connections to the ISAP
- DAVIC/DSM-CC download supported in scenario 2a only.

Configuration 3 scenario characteristics:

- does not provide a common Service domain for DAVIC and Internet services
- user not explicitly notified of the STU access to ISAP
- access security for Physical Scenarios 1 & 3 ensured through the Signaling Proxy Agent, the use of a token required for Q.2931 (this is an open issue)
- predetermined access QoS per ISAP per STU
- on demand connections to a user selected ISAP
- equal access to Internet Service Access Providers
- download only in 3a

Configuration 4 scenario characteristics:

- Both DAVIC and Internet services may reside on a common DAVIC Service Domain
- Equal access to Internet Service Access Providers
- Selection of an ISAP can be carried out as a DAVIC service
- Ability to download network related software.

9.5.2 Direct Internet Scenario 1a

9.5.2.1 Synopsis

The U-N Config server shall give the STU a pre-established connection for it to access the ISAP Router. The connection can be assigned dynamically to an STU at the U-N configuration time and reassigned at a later time through network initiated U-N configuration while the STU is active.

9.5.2.2 Applicability

Applicable when there is exactly one ISAP available per STU. This ISAP is associated with the device_id of the STU through administrative means outside the scope of DAVIC. This association shall apply until there is an administrative change that associates the STU to another ISAP. The STU can be ported between different locations as long as this association can be accessed through the U-N Config.

9.5.2.3 Configuration of Scenario 1a

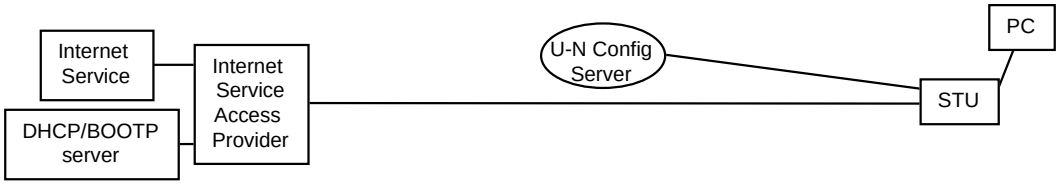


Figure 9.5-7 – System level Connectivity for Direct Internet Scenario 1a

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

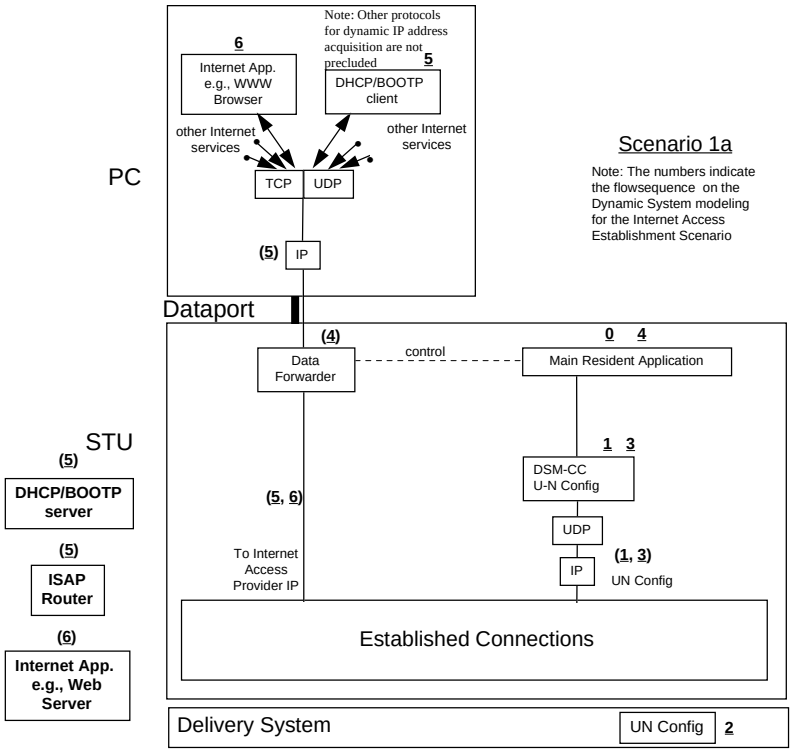


Figure 9.5-8 – STU and PC Level Entities for Direct Internet Access Scenario 1a

A Internet tool access may or may not co-exist with other tools in the same STU. Note, when Internet access is the only tool in a STU, the STU "appears" like a modem to the user but is called a STU in order to maintain compatibility with the DAVIC model.

Data Forwarder:

- Channels the packets (e.g., in the case of Internet access IP packets) received from the Dataport to the DAVIC network resource. Note: See previous section – Assumptions and Definitions – STU Data Switcher – for description of multiple PC operation.

DSM-CC U-N Config:

- Provides the protocol for DSM-CC U-N Configuration

Established Connections:

- Represents function for establishing connections

ISAP Router:

- Internet Service Access Provider router

Internet app, e.g., WWW Browser

- Any browser capable of navigating the Web

IP:

- formats IP packets

Main Resident Application:

- An application which comes with the STU

TCP:

- Establishes TCP connections and formats TCP packets

UDP:

- Formats UDP packets

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Internet app. e.g., Web Server:

- Provides Web services

9.5.2.4 Connection Establishment with the Internet Service Access Provider (ISAP)

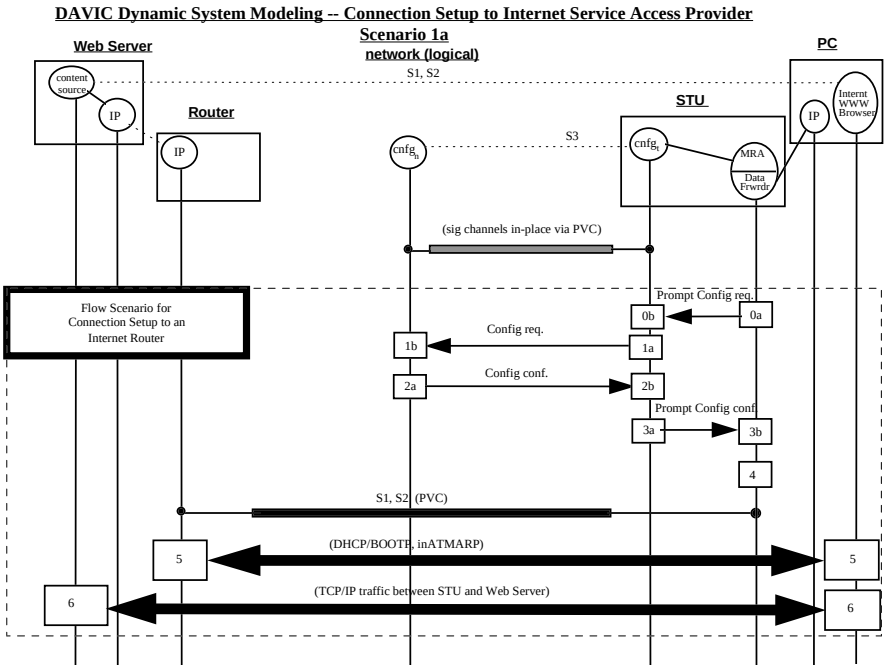


Figure 9.5-9 – DAVIC Dynamic System Model – Establishment of Direct Access to Internet for Direct Internet Access Scenario 1a

Table 9.5-4 - Functional Entity Actions – Establishment of Direct Access to Internet for Scenario 1a

Establishment of Direct Access to Internet	
0a - 0b:	The STU is powered up and the Main Resident Application invokes the User-to-Network Configuration process.
1a - 1b:	STU Config send the Network Config a Config req.
2a - 2b:	Network Config send the STU a Config conf.
3a - 3b	STU Config invokes the Main Resident Application with the message content of Config conf.
4	The Main Resident application passes the channel and optionally the Conditional Access to the Data Forwarder for connectivity to the Internet Access Service Provider's router.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

5	The PC obtains its dynamic IP address or is manually configured with its static IP address. The STU updates the ARP cache in the Data Forwarder. The STU is required to respond to ARP request messages with an ARP response message (RFC 826). An example operation with DHCP is provided below: PC gets its IP address (in case of DHCP) PC powers up and broadcasts an Ethernet packet containing DHCP (RFC1541) DHCPDISCOVER STU receives it remembers src-enet address and forwards request to router The ISAP Router returns DHCPOFFER, the STU creates enet packet and sends to PC The PC broadcasts a DHCPREQUEST and the appropriate DHCP server responds with DHCP ACK message which includes the PC's IP address PC sends its first IP packet PC sends ARP to get enet MAC address to use for future transmissions of IP packets to specified IP address (i.e., the IP address included in the ARP response) and also informs the STU of its own configured (or manually entered) IP address. STU learns the PC IP address and responds to ARP. The ARP response tells the PC to send any packets for that IP address to the STU Ethernet address. The Data Forwarder sends an inATMARP on the designated VPI/VCI which triggers the ISAP Router to bind the IP to the VPI/VCI PC sends the IP data packets to the ISAP router via STU MAC address ISAP Router sends IP data packets to STU, which forms Ethernet packet with correct dst-enet address for PC.
6	Internet app. e.g., WWW Server shall now begin to receive the IP packets from the Browser

Table 9.5-5 - Dynamic Flow Parameters - Establishment of Direct Access to Internet for Scenario 1a

Flow	Status	Parameters	Comments
0a-0b The STU is powered up, Main Resident App - $Cnfg_t$			
1a-1b Config req.		device_id	this is the device_id of the STU. Optionally it may be encrypted for increased security when shared access media is used.
2a-2b Config conf.		device_id	the same as in 1
		STU view of connection parameters e.g., channel_id in HFC plus VPI/VCI in case of ATM or MPEG PID	the channel assigned to the STU dedicated to the Internet Service Access Provider (ISAP)by the Network Service Provider. The QoS of the VPI/VCI is preassigned by the ISAP under contract with the Network Service Provider.

 © ISO/IEC – All rights reserved

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

		encapsulation	RFC 1483 for ATM or MPEG TS ISO/IEC 13818-6. RFC-1483 LLC/SNAP is the default. Each of the encapsulation types specified by RFC-1483 may also be supported.
3a-3b Main Resident App - $Cnfg_t$		VPI/VCI	as in 2
4			the Data Forwarder now forwards any data received from the STU Data Port to the VPI/VCI provided in 3.
5		PC_IP	the PC obtains its dynamic IP address and notifies the ISAP that it is connected to the network. For detail see table 2 row 5.
6			the IP packets from the PC now reach Internet WWW server, the TCP is established and communication begins with the Internet WWW browser. Any other Internet Service on the PC can be operated.

9.5.2.5 Release of Connection to ISAP

With the power down of the STU the connection binding to the VPI/VCI disappears. The binding is re-established again when the STU is powered up. In case of change of the connection, the network initiates a U-N configuration to an active STU and the Data Forwarder makes use of this other connection. The ATM rate used for Internet is UBR therefore no resource penalty is incurred when the connection remain inactive. The total number of VPI/VCIs is 64,000 per physical connection which makes it sufficient to assign each STU sharing the physical connection its own VPI/VCI for the connection.

9.5.3 Direct Internet Scenario 1b

9.5.3.1 Synopsis

In this scenario, the STU initiates an SVC connection directly upon receiving a DHCP or equivalent packet from the PC. It utilizes Functional Entities (FE), $pses_n$ and $pses_t$, which originate and terminate the appropriate flows. These Fe's can be viewed as a limited subset of ses_n and ses_t respectively. However, $pses_n$ is always co-located with the client-side connection control signaling entity (c/c_t) (see physical scenarios Figure 5).

9.5.3.2 Applicability

Applicable when there is exactly one ISAP available per STU. This ISAP is associated with the device_id of the STU through administrative means outside the scope of DAVIC. The end user may change this ISAP by an administrative request. This association shall apply until there is an administrative change that associates the STU to another ISAP. The STU can be ported between different locations as long that this association can be accessed through the U-N Config.

The advantages are:

- the client_id shall be verified at the $pses_n$ before the connection is established with the ISAP Router.
- capability to work with non-ATM HFC since the $pses_n$ shall interact with the access network to provide the proper interworking between the ATM core and the non-ATM HFC.

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

9.5.3.3 Configuration of Scenario 1b

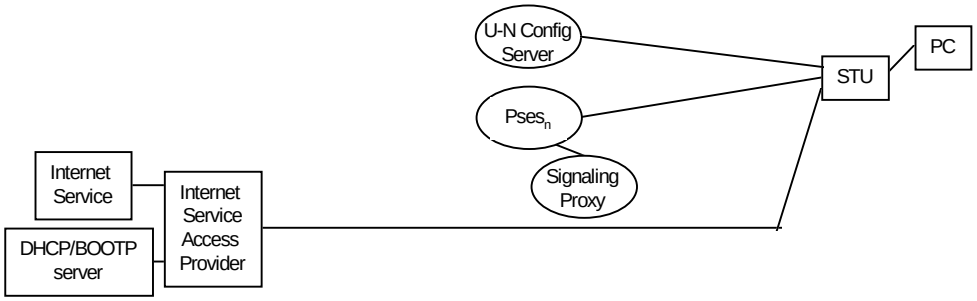


Figure 9.5-10 - System level Connectivity for Direct Internet Scenario 1b

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

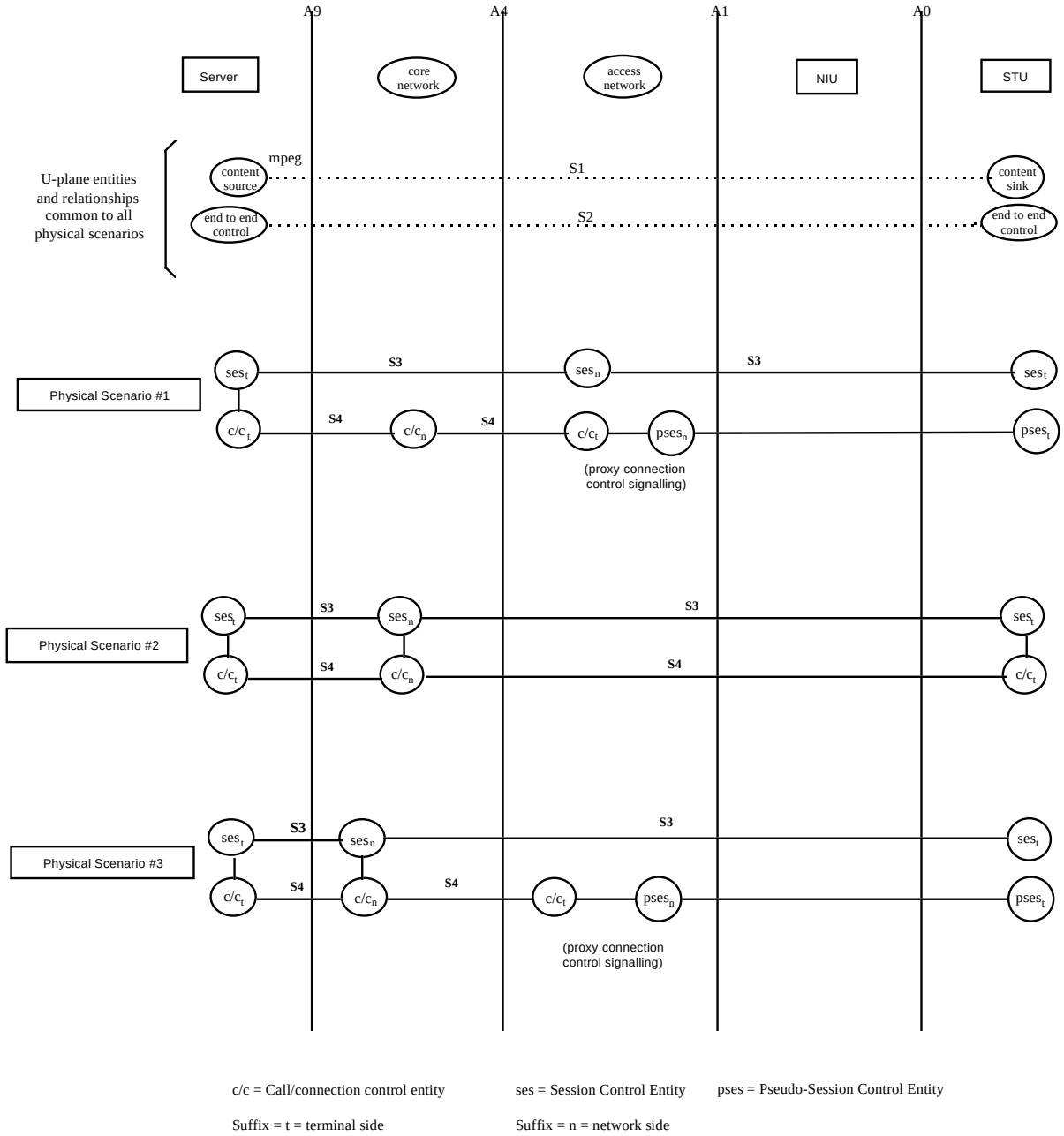


Figure 9.5-11 - Integration of Pseudo-Session Control Entities in the DAVIC Physical Scenarios for Switched Connections (SVCs)

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

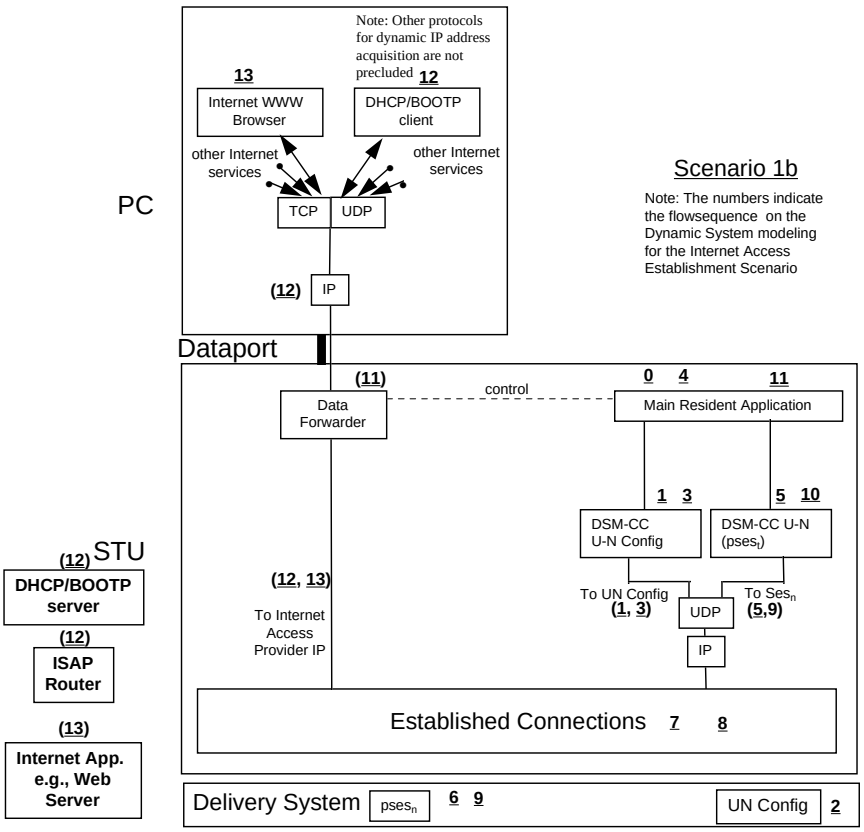


Figure 9.5-12 - STU and PC Level Entities for Direct Internet Access Scenario 1b

Data Forwarder: Channels the packets (e.g., in the case of Internet access, IP packets) to the DAVIC network resource. Note: See previous section – Assumptions and Definitions – STU Data Switcher – for description of multiple PC operation.

DSM-CC U-N Config: Provides the protocol for DSM-CC U-N Configuration

DSM-CC U-N ($pses_t$): Provides subset of protocols for pseudo-session set-up and release from the DSM-CC U-N protocols

Established Connections: Represents function for establishing connections

ISAP Router: Internet Service Access Provider router

Internet app. e.g., WWW Browser: Any browser capable of navigating the Web

IP: formats IP packets

Main Resident Application: An application which comes with the STU

TCP: Establishes TCP connections and formats TCP packets

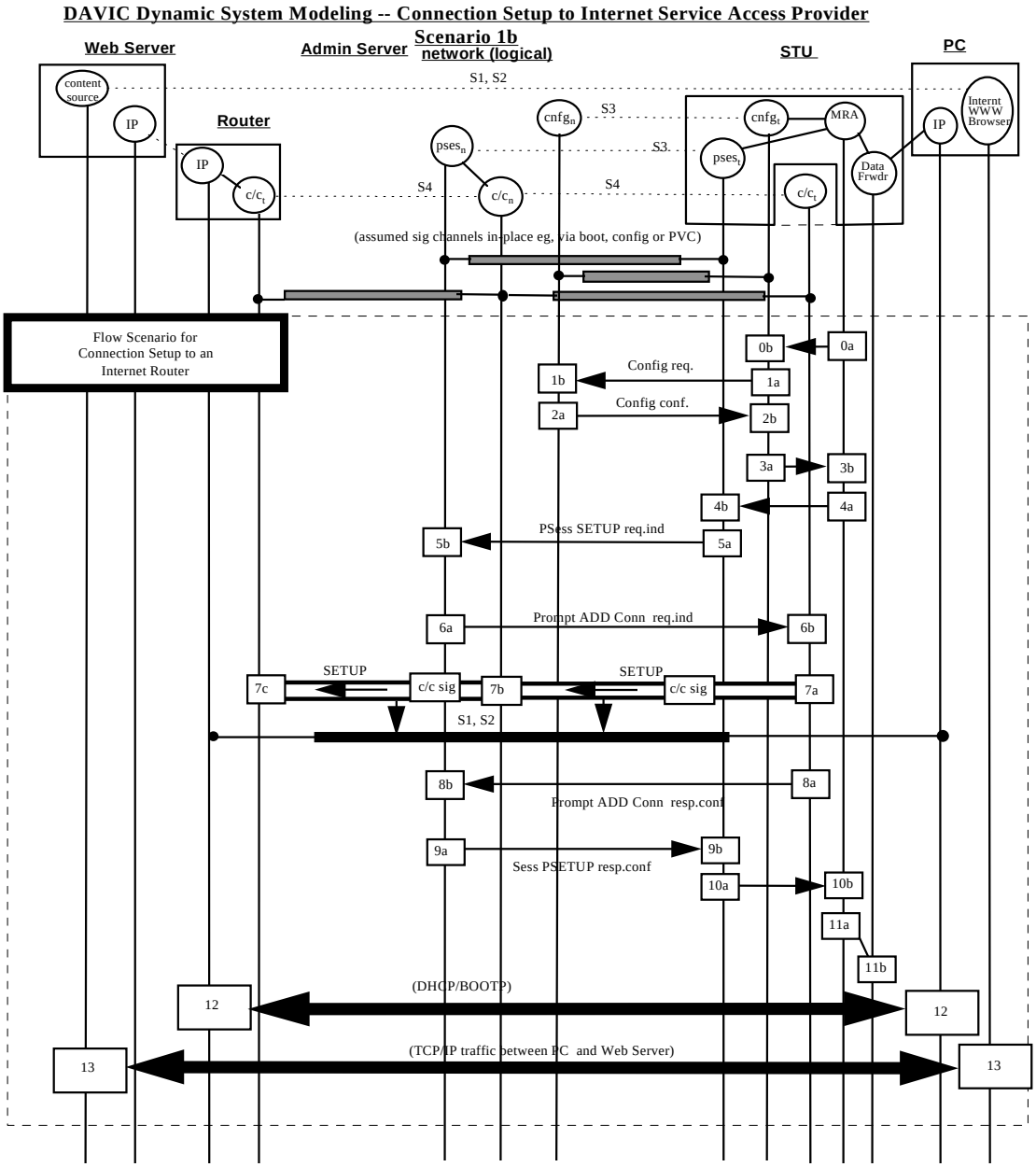
UDP: Formats UDP packets

Internet app. e.g., Web Server: Provides Web services

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

9.5.3.4 Connection Establishment with the Internet Service Access Provider (ISAP)



Note : This dynamic flow scenario is used for Physical Scenario #1 (both $pses_n$ and the proxy signalling agent c/c(t) are colocated). In this case, flows 6a-6b and 8a-8b are actually internal. In Physical Scenario #2, c/c(t) (I.e., Q.2931) is located in the STU and can therefore be directly prompted by the the STU application to initiate the connection to the router.

Figure 9.5-13 - DAVIC Dynamic System Model - Establishment of Direct Access to Internet for Direct Internet Scenario 1b

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Table 9.5-6 - Functional Entity Actions - Establishment of Direct Access to Internet for Direct Internet Scenario 1b

Establishment of Direct Access to Internet	
0a – 0b	The STU is powered up and the Main Resident Application invokes the User-to-Network Configuration process.
1a – 1b	STU Config send the Network Config a Config req.
2a – 2b	Network Config send the STU a Config conf. including the ISAP access service on the Network Service Provider's Admin Server as a default service
3a – 3b	STU Config invokes the Main Resident Application with the message content of Config conf.
3'	At this point, no action is taken until the first packet is received. This packet is held in the Main Resident Application (MRA) until a connection is established. Any subsequent packets received during connection establishment may also be stored in the MRA. On Buffer overflow the oldest packets are discarded.
4a – 4b	The Main Resident application requests the establishment of a pseudo-session with the pses(t) with a connection resource descriptor which was passed along the U-N Config Conf.
5a – 5b	the STU $pses_t$ sends a pSess. SETUP req.ind to $pses_n$
6a – 6b	$pSes_n$ prompts the STU proxy C/C_t to establish the connection from STU to the ISAP
7a – 7b – 7c	Connection establishment between STU and ISAP
8a – 8b	C/C_t prompts the $pses_n$ with the result of connection establishment e.g., VPI/VCI
9a – 9b	$Pses_n$ sends pSess. SETUP resp.conf to the STU $pses_t$
10a – 10b	The Main Resident application is prompted with the results of the establishment of the connection to the ISAP e.g., VPI/VCI
11a – 11b	The Main Resident application passes the channel to the Data Forwarder for connectivity to the ISAP's router

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

12	The PC is configured manually with its static IP or can obtain its IP using DHCP. The STU updates the ARP cache in the Data Forwarder. The STU is required to respond to ARP request messages with an ARP response message (RFC 826). An example operation with DHCP is provided below: PC gets its IP address (in case of DHCP) PC powers up and broadcasts an Ethernet packet containing DHCP (RFC1541) DHCPDISCOVER STU receives it remembers src-enet address and forwards request to router The ISAP Router returns DHCPOFFER, the STU creates enet packet and sends to PC The PC broadcasts a DHCPREQUEST and the appropriate DHCP server responds with DHCP ACK message which includes the PC's IP address PC sends its first IP packet PC sends ARP to get enet MAC address to use for future transmissions of IP packets to specified IP address (i.e., the IP address included in the ARP response) and also inform the STU of its own configured IP address. STU copies the PC IP address and responds to ARP. The ARP response tells the PC to send any packets for that IP address to the STU Ethernet address. The Data Forwarder sends an initiates psess setup which results in the connection being established with the ISAP Router. This triggers the ISAP Router to send inATMARP from which it binds the IP to the VPI/VCI PC sends the IP data packets to the ISAP Router via STU MAC address ISAP Router sends IP data packets to STU, which forms Ethernet frames with correct dst-enet address for PC.
13	The Internet WWW Server will now begin to receive the IP packets from the Browser
14	Dynamic connection release During the UN Config process the STU receives a session aging timer Trel which could be set by the user at subscription time or could be defaulted to 15 minutes. As an example of a mechanism that could be used, the STU monitors the IP flow. After a period of inactivity of 2 minutes, the STU proceeds by sending an Ethernet ARP at each 2 minute interval using the IP address of the PC, if no response is received after 3 such attempts the STU proceeds to release the psession. If an ARP Reply is received from the PC, the psession shall be released if IP packet inactivity from the PC persists for a duration of Trel. At the first packet received after the psession is released the procedure in 12 is followed where the ARP packet is replaced by the first IP packet.

Table 9.5-7 - Dynamic Flow Parameters - Establishment of Direct Access to Internet for Direct Internet Access

Flow	Status	Parameters	Comments
0a-0b The STU is powered up, Main Resident App - $Cnfg_t$			

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

1a-1b Config req.		device_id	this is the device_id of the STU. Optionally it may be encrypted for increased security when shared access media is used.
2a-2b Config conf.		device_id	the same as in 1
		user_config_parametrs	connection resource descriptor for the connection to be established with the ISAP Router.
		encapsulation	RFC 1483 for ATM or MPEG TS ISO/IEC 13818-6. RFC-1483 LLC/SNAP is the default. Each of the encapsulation types specified by RFC-1483 may also be supported.
		STU_timers	session release timer Trel
3a-3b $Cnfg_t$ – Main Resident App		server_id	the Admin Server connection resource descriptor from 2
3’			At this point, no action is taken until the first packet is received. This packet is held in the Main Resident Application (MRA) until a connection is established. Any subsequent packets received during connection establishment are also stored in the MRA.
		service_info	identical to step 2
4a – 4b Main Resident App – $Pses_t$			
		connection_resource_descriptor	identical to step 3 = 2
5a – 5b pSess SETUP req.ind		session_id	uniquely assigned by the STU = device_id & arbitrary additional value, unique on this STU Note: One session is permitted at a time in this scenario.
		client_id	E164 NSAP address at the A1 interface of the client.
		Connection_resource_descriptor	identical to step 4 =2

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

		resource # (as seen by the server) association_tag (end-to-end) resource_descriptor	describes the connection between the required ISAP and the STU and contains - physical or logical E.164 address of the port, the inap router is connected to. parameters which describe the ATM connection to be set up: - bandwidth - QoS - any other necessary parameters, such as AAL parameters, broadband bearer capabilities, etc. Note: This is the resource_descriptor for the connection which terminates on the ISAP.
6a – 6b $pses_n$ _ c/c_t		STU_id	This contains the E164 NSAP address of the STU
		isap_ATM_id	derived from the resource descriptor in 7
		resource_attribute(s)	derived from the resource descriptor in 7
7a – 7b – 7c		all c/c signaling parameters	see ISO/IEC 16500-5 *Note: In order to guarantee that the connection delivered to the ISAP Router is a connection sanctioned by the $pses_n$, an identifier for the $pses_n$ may be required with a time dependent or encrypted security code as part of the Q.2931 SETUP message. This information could be passed in the GIT and could be checked by the ISAP for acceptance of the incoming connection.*
8a – 8b c/c_t – $pses_n$		session_id	identical to step 5
		VPI/VCI (as seen by the STU A1 or the access A4)	Note: In case of non-ATM HFC access the $pses_n$ shall also establish a connection to the STU and will generate the associated client view resource_descriptor.
		status_id	indicates status and reason of the requested resource (e.g., OK or failed because of ...)
9a – 9b pSess SETUP resp.conf		session_id	identical to 8 = 5
		status_id	identical to 8
		resource # (as seen by the server) association_tag (end-to-end) resource_descriptor	as generated by $pses_n$ in 7.
10a – 10b ses_t to Main Resident App		association_tag resource_descriptor	the association_tag is identical to 6 = 5. The resource_descriptor presents the Client view and is identical to 6.

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

11a – 11b			The Data Forwarder establishes a binding between its outgoing port and the channel described by the resource descriptor.
12		PC_IP	Packets stored in MRA are sent on the connection. Typically these will be initialization messages for DHCP.
13 WWW Client – Web Server		http protocol	At this point the IP packets can begin to flow between the Internet WWW Client and the Internet Service Provider Web Server
14			Dynamic release, see release table

9.5.3.5 Release of Connection to the ISAP

With the power down of the STU the connection binding disappears. $pSes_n$ can also request a Connection Release or STU Reset. In those situation the user is not explicitly notified, the result however will be the loss of connection detected by the WWW Service in the PC. A subsequent receipt of IP packet will establish a new psess aqnd connection with the ISAP. Release can also be:

PC prompted connection release:

- In a graceful shutdown, when DHCP is used, the PC sends a DHCPRELEASE, the Data Forwarder in the STU monitors the message and sends the message to the router and the MRA. The MRA proceeds to release the pseudo-session.

STU initiated release:

- As an example of a mechanism that could be used, the STU monitors the IP flow. After a period of inactivity of 2 minutes, the STU proceeds by sending an Ethernet ARP at each 2 minute interval using the IP address of the PC, if no response is received after 3 such attempts the STU proceeds to release the psession. If an ARP Reply is received from the PC, the psession shall be released if IP packet inactivity from the PC persists for a duration of Trel. At the first packet received after the psession is released the procedure in Table 38 row12 is followed where the ARP packet is replaced by the first IP packet

9.5.4 Direct Internet Scenario 2a

9.5.4.1 Synopsis

The U-N Config server will give the STU a default server_id, primary_service and saved_service_context. These will be used by the STU to access the service on the Network Service Provider Admin Server which will establish the connection to the ISAP Router.

9.5.4.2 Applicability

Applicable when there is exactly one ISAP available per STU. This ISAP is associated with the device_id of the STU through administrative means outside the scope of DAVIC. This association will apply until there is an administrative change that associates the STU to another ISAP. The STU can be ported between different locations as long that this association can be accessed through the U-N Config.

The advantages are:

- the client_id will be verified both at the ses_n and the Network Service Provider Admin Server before the connection is established with the ISAP Router.
- capability to work with non-ATM HFC since the ses_n will interact with the access network to provide the proper interworking between the ATM core and the non-ATM HFC.
- capability for the Network Service Provider Admin to download the Data Forwarder code.

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

9.5.4.3 Configuration of Scenario 2a

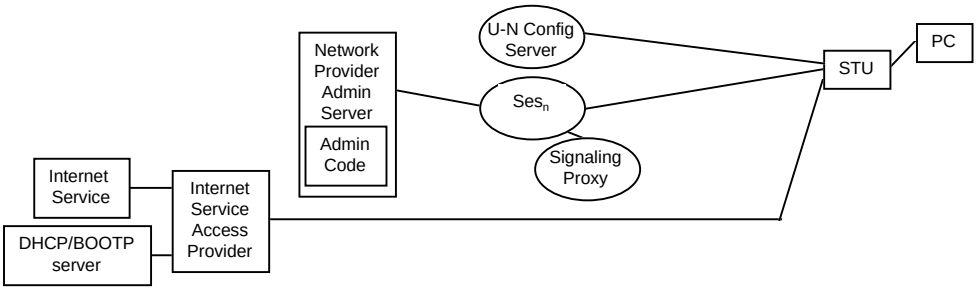


Figure 9.5-14 - System level Connectivity for Direct Internet Scenario 2a

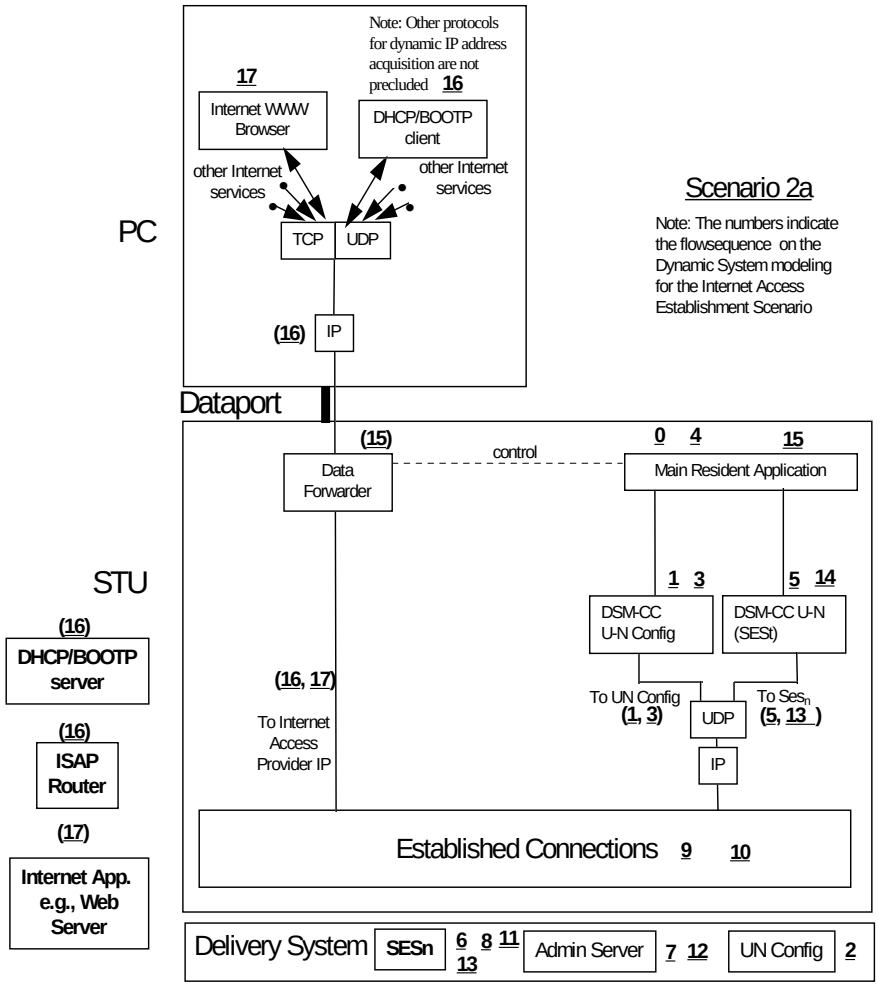


Figure 9.5-15 - STU and PC Level Entities for Direct Internet Access Scenario 2a

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Data Forwarder: Channels the packets (e.g., in the Internet case, IP packets) to the DAVIC network resource. Note: See previous section – Assumptions and Definitions – STU Data Switcher – for description of multiple PC operation.

DSM-CC U-N Config: Provides the protocol for DSM-CC U-N Configuration

DSM-CC U-N: Provides the protocol for DSM-CC U-N protocols

Established Connections: Represents function for establishing connections

ISAP Router: Internet Service Access Provider router

Internet app. e.g., WWW Browser: Any browser capable of navigating the Web

IP: formats IP packets

Main Resident Application: An application which comes with the STU

TCP: Establishes TCP connections and formats TCP packets

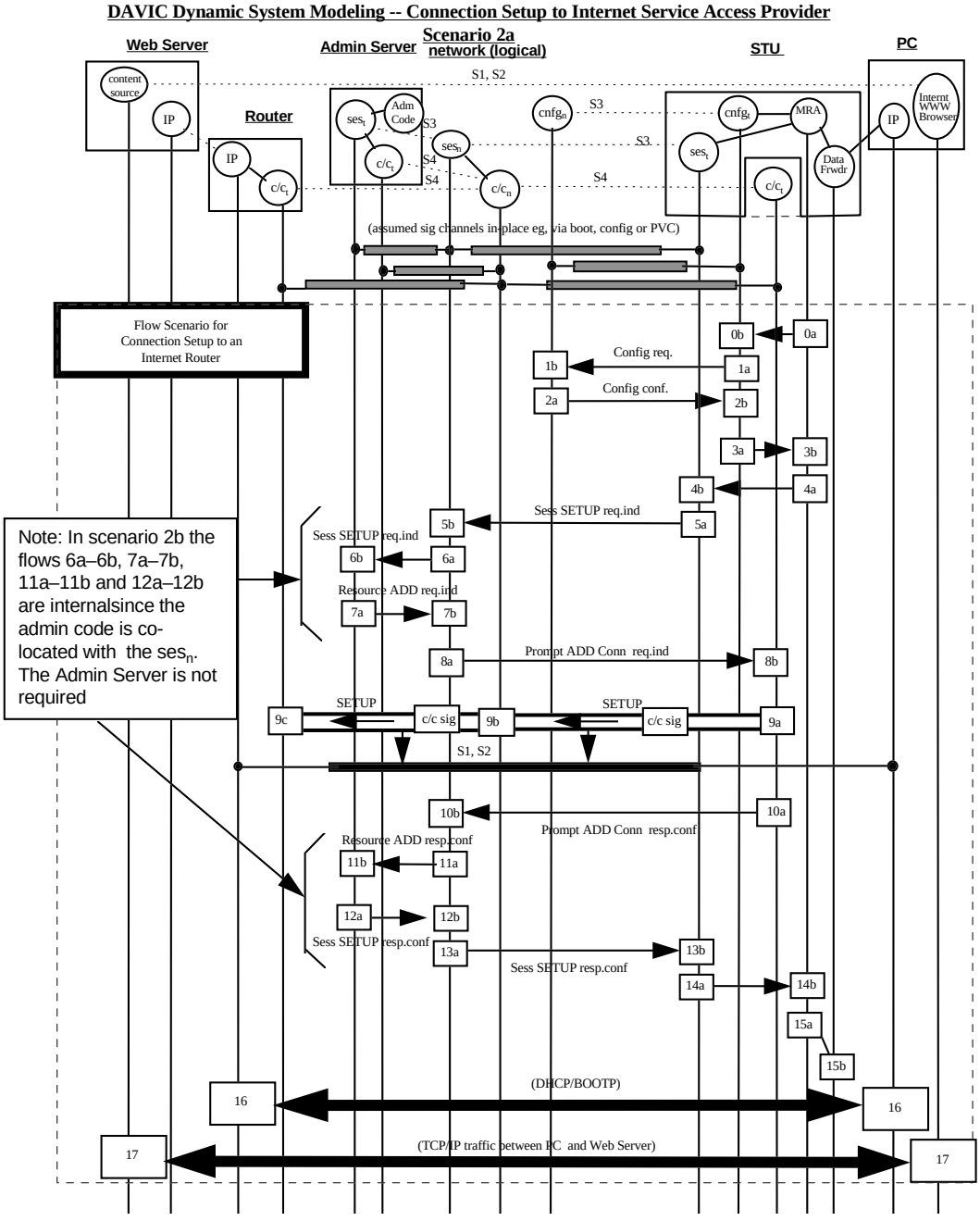
UDP: Formats UDP packets

Internet app. e.g., Web Server: Provides Web services

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

9.5.4.4 Connection Establishment with the Internet Service Access Provider (ISAP)



Note : This dynamic flow scenario is used for Physical Scenario #1 (both ses(n) and the proxy signalling agent c/c(t) are colocated). In this case, flows 8a-8b and 10a-10b are actually internal. In Physical Scenario #2, c/c(t) (I.e., Q.2931) is located in the STU and can therefore be directly prompted by the STU application to initiate the connection to the router.

Figure 9.5-16 - DAVIC Dynamic System Model - Establishment of Direct Access to Internet for Direct Internet Scenario 2a

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table 9.5-8 - Functional Entity Actions - Establishment of Direct Access to Internet for Direct Internet Access

Establishment of Direct Access to Internet	
0a – 0b:	The STU is powered up and the Main Resident Application invokes the User-to-Network Configuration process.
1a – 1b:	STU Config send the Network Config a Config req.
2a – 2b:	Network Config send the STU a Config conf. including the ISAP access service on the Network Service Provider's Admin Server as a default service
3a – 3b	STU Config invokes the Main Resident Application with the message content of Config conf.
3'	At this point, no action is taken until the first packet is received. This packet is held in the Main Resident Application (MRA) until a connection is established. Any subsequent packets received during connection establishment may also be stored in the MRA. On Buffer overflow the oldest packets are discarded.
4a – 4b	The Main Resident application requests the establishment of a session with the Network Service Provider's Admin Server with the default service which was passed along the U-N Config Conf.
5a – 5b	the STU ses_t sends a Sess. SETUP req.ind to ses_n
6a – 6b	Ses_n sends a Sess. SETUP req.ind to the Admin Server ses_t
7a – 7b	The Admin Server ses_t sends Resource ADD req.ind to ses_n
8a – 8b	Ses_n prompts the STU proxy C/C_t to establish the connection from STU to the ISAP
9a – 9b – 9c	Connection establishment between STU and ISAP
10a – 10b	C/C_t prompts the ses_n with the result of connection establishment e.g., VPI/VCI
11a – 11b	Ses_n sends Resource ADD resp.conf to the Admin Server ses_t
12a – 12b	The Admin Server ses_t sends Sess. SETUP resp.conf to ses_n
13a – 13b	Ses_n sends Sess. SETUP resp.conf to the STU ses_t
14a – 14b	The Main Resident application is prompted with the results of the establishment of the connection to the ISAP e.g., VPI/VCI
15a – 15b	The Main Resident application passes the channel to the Data Forwarder for connectivity to the ISAP's router

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

16	The PC is configured manually with its static IP or can obtain its IP using DHCP. The STU updates the ARP cache in the Data Forwarder. The STU is required to respond to ARP request messages with an ARP response message (RFC 826). An example operation with DHCP is provided below: PC gets its IP address (in case of DHCP) PC powers up and broadcasts an Ethernet packet containing DHCP (RFC1541) DHCPDISCOVER STU receives it remembers src-enet address and forwards request to router The ISAP Router returns DHCPOFFER, the STU creates enet packet and sends to PC The PC broadcasts a DHCPREQUEST and the appropriate DHCP server responds with DHCP ACK message which includes the PC's IP address PC sends its first IP packet PC sends ARP to get enet MAC address to use for future transmissions of IP packets to specified IP address (i.e., the IP address included in the ARP response) and also inform the STU of its own configured IP address. STU copies the PC IP address and responds to ARP. The ARP response tells the PC to send any packets for that IP address to the STU Ethernet address. The Data Forwarder initiates sess setup which results in the connection being established with the ISAP Router. This triggers the ISAP Router to send inATMARP from which it binds the IP to the VPI/VCI PC sends the IP data packets to the ISAP Router via STU MAC address ISAP Router sends IP data packets to STU, which forms Ethernet frames with correct dst-enet address for PC.
17	The Internet WWW Server will now begin to receive the IP packets from the Browser
18	Dynamic connection release During the UN Config process the STU receives a session aging timer Trel which could be set by the user at subscription time or could be defaulted to 15 minutes. As an example of a mechanism that could be used, the STU monitors the IP flow. After a period of inactivity of 2 minutes, the STU proceeds by sending an Ethernet ARP at each 2 minute interval using the IP address of the PC, if no response is received after 3 such attempts the STU proceeds to release the session. If an ARP Reply is received from the PC, the session shall be released if IP packet inactivity from the PC persists for a duration of Trel. At the first packet received after the session is released the procedure in 16 is followed where the ARP packet is replaced by the first IP packet.

Table 9.5-9 - Dynamic Flow Parameters - Establishment of Direct Access to Internet for Direct Internet Access

Flow	Status	Parameters	Comments
0a-0b The STU is powered up, Main Resident App - $Cnfg_t$			

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

1a-1b Config req.		device_id	this is the device_id of the STU. Optionally it may be encrypted for increased security when shared access media is used.
2a-2b Config conf.		device_id	the same as in 1
		network_config_parametrs	provides the Admin Server server_id and the service_info which includes ISAP access as the default_primary_service and the specific ISAP as primary_saved_context
		encapsulation	RFC 1483 for ATM or MPEG TS ISO/IEC 13818-6. RFC-1483 LLC/SNAP is the default. Each of the encapsulation types specified by RFC-1483 may also be supported.
		STU_timers	session release timer Trel
3a-3b $Cnfg_t$ – Main Resident App		server_id	the Admin Server server_id from 2
3’			At this point, no action is taken until the first packet is received. This packet is held in the Main Resident Application (MRA) until a connection is established. Any subsequent packets received during connection establishment are also stored in the MRA.
		service_info	identical to step 2
4a – 4b Main Resident App – Ses_t		server_id	the Admin Server server_id from 3 = 2
		service_info	identical to step 3 = 2
5a – 5b Sess SETUP req.ind		session_id	uniquely assigned by the STU = device_id & arbitrary additional value, unique on this STU Note: One session is permitted at a time in this scenario.
		client_id	E164 NSAP address at the A1 interface of the client.
		server_id	the Admin Server server_id from 4 = 2
		service_info	identical to step 4 = 2
6a – 6b Sess SETUP req.ind		session_id	identical to step 5
		client_id	identical to step 5
		server_id	derived from step 5
		service_info	identical to step 5 = 2

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

7a – 7b Resource ADD req.ind		inap_ATM_id	provided by the Admin Server based on client_id value and contractual agreement with the ISAP.
		resource # (as seen by the server) association_tag (end-to-end) resource_descriptor	describes the connection between the required ISAP and the STU and contains - physical or logical E.164 address of the port, the inap router is connected to. parameters which describe the ATM connection to be set up: - bandwidth - QoS - any other necessary parameters, such as AAL parameters, broadband bearer capabilities, etc. Note: This is the resource_descriptor for the connection which terminates on the ISAP.
8a – 8b ses_n _ c/c_t		STU_id	This contains the E164 NSAP address of the STU
		inap_ATM_id	derived from the resource descriptor in 7
		resource_attribute(s)	derived from the resource descriptor in 7
9a – 9b – 9c		all c/c signaling parameters	*Note: In order to guarantee that the connection delivered to the ISAP Router is a connection sanctioned by the ses_n, an identifier for the ses_n may be required with a time dependent or encrypted security code as part of the Q.2931 SETUP message. This information could be passed in the GIT and could be checked by the ISAP for acceptance of the incoming connection.*
10a – 10b c/c_t – ses_n		session_id	identical to step 5
		VPI/VCI (as seen by the STU A1 or the access A4)	Note: In case of non-ATM HFC access the ses_n shall also establish a connection to the STU and will generate the associated client view resource_descriptor.
		status_id	indicates status and reason of the requested resource (e.g., OK or failed because of ...)
11a – 11b Resource ADD resp.conf		resource #	identical to 7
		status_id	indicates if the end-to-end connection has been successful or not.
12a – 12b Sess SETUP resp.conf		session_id	identical to step 8 = 5
		status_id	indicates if the request has been successful or not

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

		resource_# (as seen by the server)	provides the client view of the resource which corresponds to the server view in step 7.
13a – 13b Sess SETUP resp.conf		session_id	identical to 12 = 5
		status_id	identical to 12
		resource # (as seen by the server) association_tag (end-to-end) resource_descriptor	as generated by ses_n in 10.
14a – 14b ses_t to Main Resident App		association_tag resource_descriptor	the association_tag is identical to 9 = 5. The resource_descriptor presents the Client view and is identical to 9.
15a – 15b			The Data Forwarder establishes a binding between its outgoing port and the channel described by the resource descriptor.
16		PC_IP	Packets stored in MRA are sent on the connection. Typically these will be initialization messages for DHCP.
17 WWW Client – Web Server		http protocol	At this point the IP packets can begin to flow between the Internet WWW Client and the Internet Service Provider Web Server
18			Dynamic release, see release table

9.5.4.5 Release of Session and Connection to ISAP

With the power down of the STU the connection binding disappears. Ses_n can also request a Connection Release or STU Reset. In those situation the user is not explicitly notified, the result however will be the loss of connection detected by the WWW Service in the PC. A subsequent receipt of IP packet will establish a new session and connection with the ISAP. Release can also be:

- PC prompted connection release:

  In a graceful shutdown, when DHCP is used, the PC sends a DHCPRELEASE, the Data Forwarder in the STU monitors the message and sends the message to the router and the MRA. The MRA proceeds to release the session.

- STU initiated release:

  As an example of a mechanism that could be used, the STU monitors the IP flow. After a period of inactivity of 2 minutes, the STU proceeds by sending an Ethernet ARP at each 2 minute interval using the IP address of the PC, if no response is received after 3 such attempts the STU proceeds to release the psession. If an ARP Reply is received from the PC, the psession shall be released if IP packet inactivity from the PC persists for a duration of Trel. At the first packet received after the psession is released the procedure in Table 40 row16 is followed where the ARP packet is replaced by the first IP packet

 © ISO/IEC – All rights reserved

--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

9.5.5 Direct Internet Scenario 2b

9.5.5.1 Synopsis

This is similar to scenario 2a, except that the Admin Server is replaced by pre-packaged code residing at the $ses_{n.}$

9.5.5.2 Applicability

The same applicability as in scenario 2a, except that the download capability is absent.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

9.5.5.3 Configuration of DI Scenario 2b

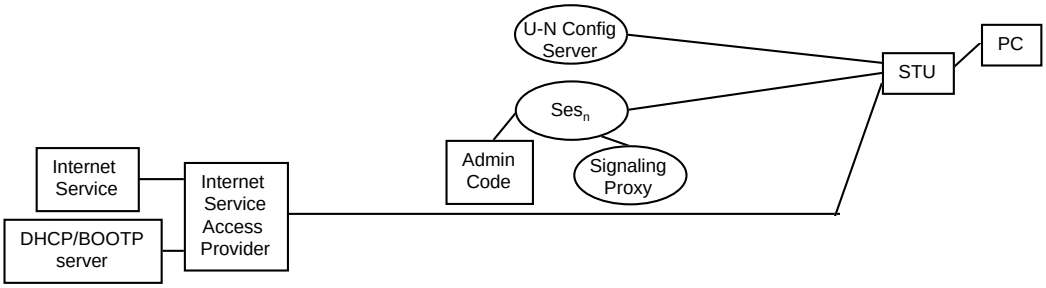


Figure 9.5-17 - System level Connectivity for Direct Internet Scenario 2b

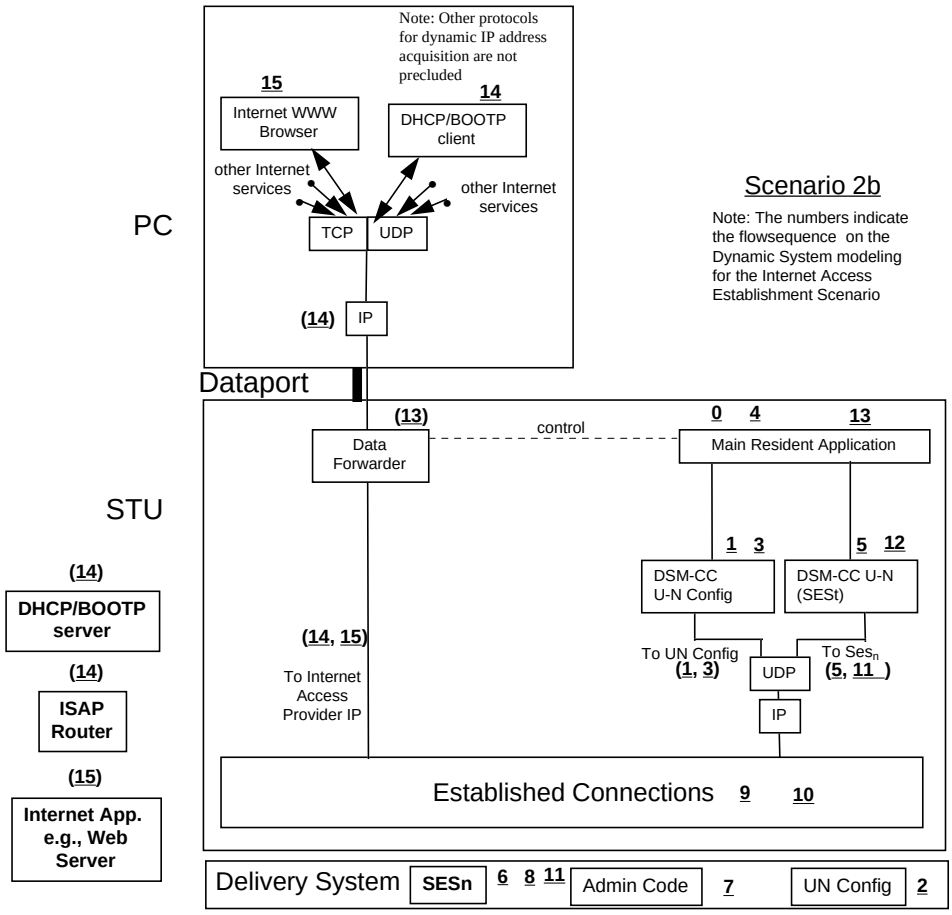


Figure 9.5-18 - STU and PC Level Entities for Direct Internet Access Scenario 2b

Data Forwarder: Channels the packets (e.g., in case of Internet access, the IP packets) to the DAVIC network resource. Note: See previous section – Assumptions and Definitions – STU Data Switcher – for description of multiple PC operation.

DSM-CC U-N Config: Provides the protocol for DSM-CC U-N Configuration

DSM-CC U-N: Provides the protocol for DSM-CC U-N protocols

Established Connections: Represents function for establishing connections

 © ISO/IEC – All rights reserved

--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ISAP Router: Internet Service Access Provider

Internet app. e.g., WWW Browser: Any browser capable of navigating the Web

IP: formats IP packets.

Main Resident Application: An application which comes with the STU

TCP: Establishes TCP connections and formats TCP packets

UDP: Formats UDP packets

Internet app e.g., Web Server: Provides Web services

9.5.5.4 Connection Establishment with the Internet Service Access Provider (ISAP)

See the note in Figure 9.5-16 against flows 6 and 7. Likewise functional action entities are shown in Table 9.5-8 and Dynamic Flow Parameters are shown in Table 9.5-9 with flows 6 and 7 now becoming internal to ses_n

9.5.5.5 Release of Connection to ISAP

The release is similar to scenario 2a.

9.5.6 Internet Access Scenarios 3a and 3b

9.5.6.1 Synopsis

The U-N Config provides information for connecting to the Network Service Provider's Admin dual Web-DAVIC Server. After a choice of ISAP by the end-user on the Admin Web Server, the Admin DAVIC Server uses a DSM-CC Pass-Through message to prompt the STU to set up a session with it in order to give the STU access to the ISAP router. The ISAP does not require to own a DAVIC server.

9.5.6.2 Applicability

The end-user requires a full choice of ISAPs (and indeed to any other (non-Internet) data network since the Data Switcher can be downloaded).

For end-user who already have the STU for DAVIC services but wish to access to the ISAP. PC users can select and make an ISAP connection without the use of TV to set up the connection.

The advantages are:

- the client_id will be verified both at the ses_n and the Network Service Provider Admin Server before the connection is established with the ISAP router.
- capability to work with non-ATM HFC since the ses_n will interact with the access network to provide the proper inter-working between the ATM core and the non-ATM HFC or PPP Access with Broadband Broadcast and S3 Capability Section 9.19.8.
- capability for the Network Service Provider Admin to download code e.g., for the Internet stack along with the DSM-CC application.
- the ability to select from a full list of ISAPs

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

9.5.6.3 Configuration of DAVIC Internet Scenario 3a

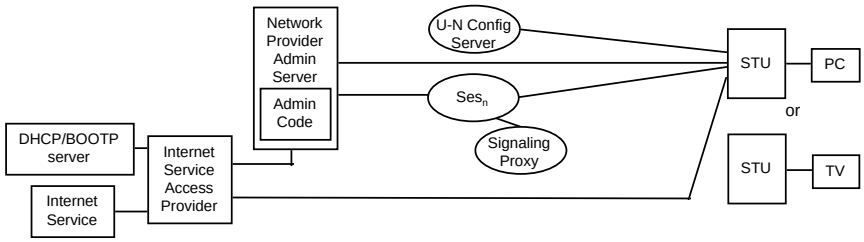


Figure 9.5-19 - System level Connectivity for Direct Internet Scenario 3a

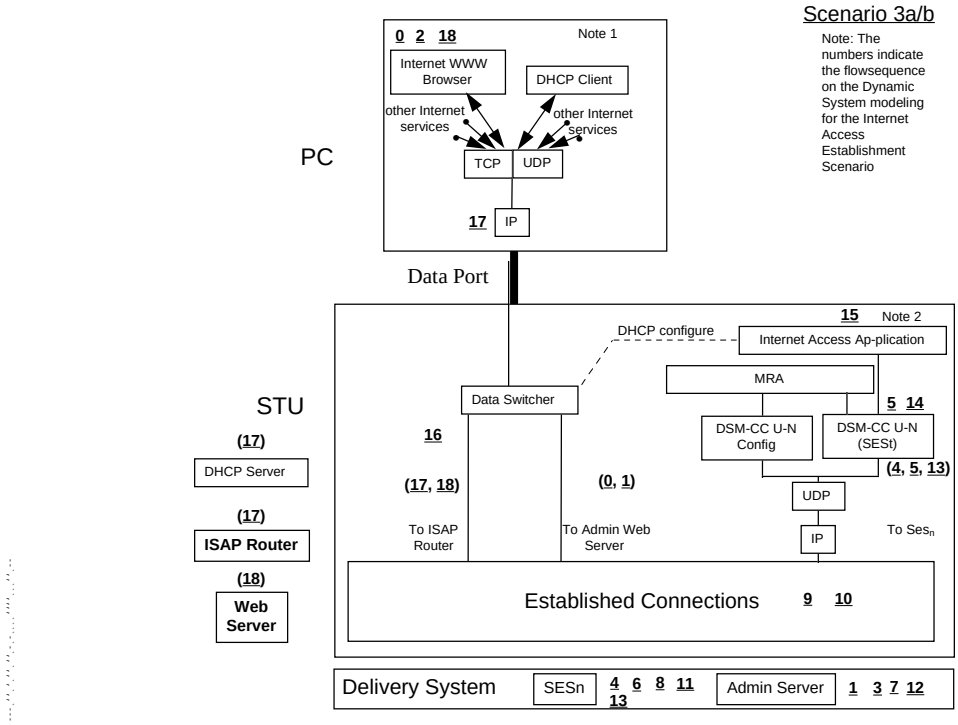


Figure 9.5-20 - STU and PC Level Entities for Direct Internet Access Scenario 3a/b

Admin Server: Owned by the Network Services Provider, provides information for selecting and routing to ISAPs.

Data Switcher Performs logical associations between PCs and connections, IP initialization and DHCP Relay functions

DHCP: Dynamic Host Configuration (RFC 1541)

DSM-CC U-N: Provides the protocol for DSM-CC U-N protocols

Established Connections: Represents connections and functions for establishing connections

ISAP: Internet Service Access Provider

Internet WWW Browser: Any commercial browser capable of navigating the Web

IP: formats IP packets. Also performs ARP, ICMP administrative tasks

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Internet Access Application: An application is used to establish the session for access to ISAP

MRA: Main Resident Application, is an STU resident boot application

TCP: Establishes TCP connections and formats TCP packets

UDP: Formats UDP packets

Web Server: Provides Web services

Note 1: Used only with Authentication and Configuration method 1 (See subclause 9.5.10).

Note 2: Could cover authentication and Configuration see method 2 (See subclause 9.5.10).

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

9.5.6.4 Connection Establishment with the Internet Service Access Provider (ISAP)

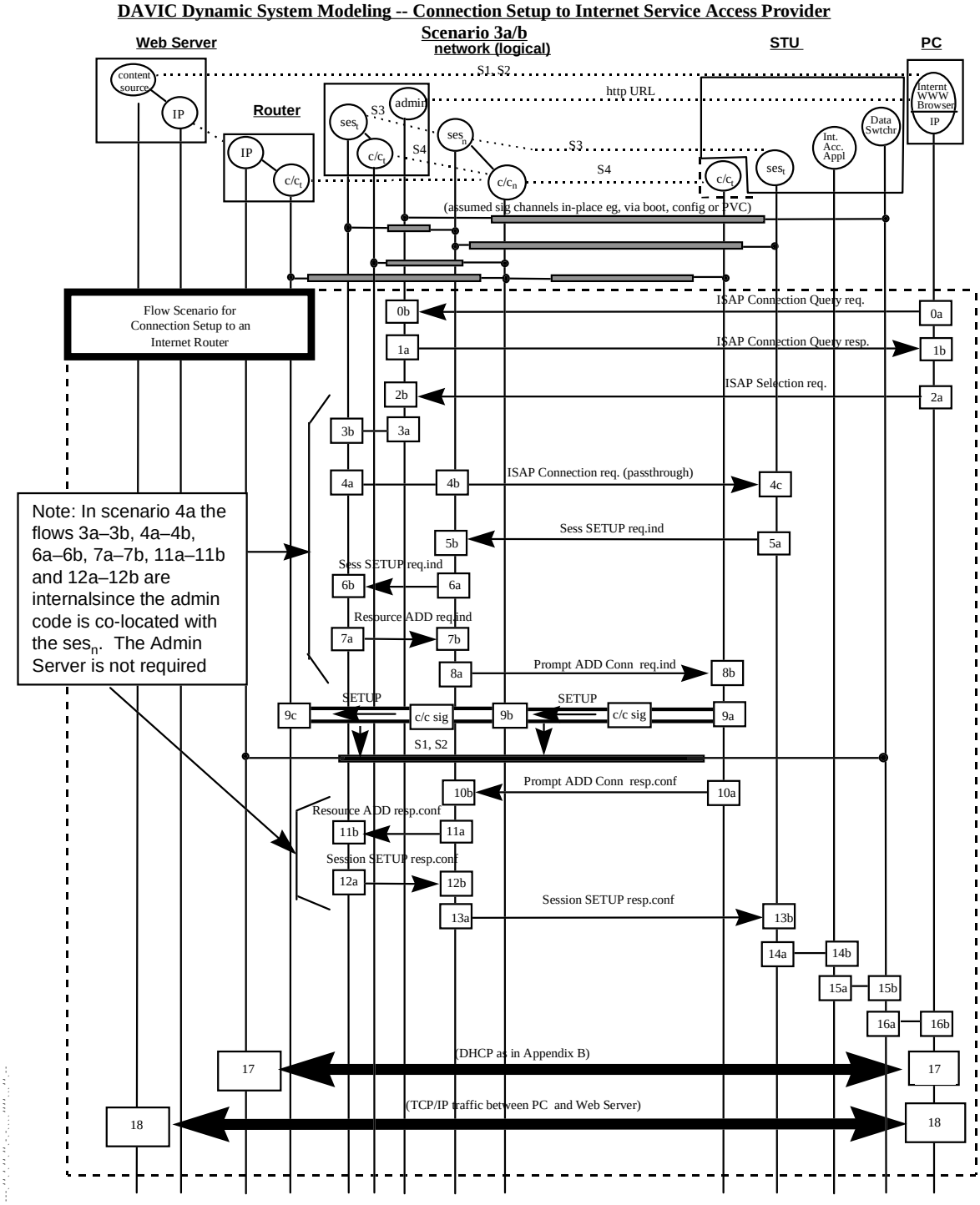


Figure 9.5-21 - DAVIC Dynamic System Model - Establishment of Direct Access to Internet for Internet Access Scenarios 3a and b

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table 9.5-10 - Functional Entity Actions - Establishment of Direct Access to Internet for Direct Internet Access Scenarios 3 a and b

Establishment of Direct Access to Internet	
0a – 0b:	The PC or STU has been powered up in advance (possibly for interactive VoD). This is typically described in steps 0 through 3 in Table 47- Dynamic Flow Parameters - Initiating a session SetUp from a PC. At this point the STU is given its IP address. From the Internet Web Browser the ISAP connect bookmark is selected. The Admin server receives the Connect URL. Note: At the beginning, the PC portion of the separate or integrated STU and PC, uses the DHCP client to get a dummy IP address e.g., 0.0.0.0. from the Network Services Provider DHCP server with an expiration time of e.g., 2 seconds. Up to 16 dummy addresses are available for a maximum number of 16 PC's being connected to a STU. When the ISAP selection bookmark is activated on the browser, the http packet IP destination address is monitored in the STU and the source IP address is substituted by the STU IP address assigned by the Network Service provider. This will allow the reverse http IP packets to reach the STU which then passes them to the PC portion using its client hardware address as its destination.
1a – 1b:	The Admin server sends the html Web page for ISAP access selection to the Internet Web Browser
2a – 2b:	The http URL is sent to the Admin Web server based on the ISAP selected for access.
3a – 3b	The Admin server invokes the ses_t with the information to access the selected ISAP
4a – 4b – 4c	The Admin Server ses_t sends a DSM-CC Pass-Through carrying the selected ISAPs access information
5a – 5b	When the IP address of the PC expires the PC sends a DHCPREQUEST. The STU after receiving the Pass-Through will ignore this request. This will trigger the PC to send a DHCPDISCOVER which in turn will trigger the Ses_t of the STU to send a Sess. SETUP req.ind to ses_n.
6a – 6b	Ses_n sends a Sess. SETUP req.ind to the Admin DAVIC Server ses_t. The Server broadcasts the DHCPDISCOVER see Appendix B - Internet Access DAVIC server DHCP Relay Operation
7a – 7b	The Admin DAVIC Server ses_t sends Resource ADD req.ind to ses_n
8a – 8b	Ses_n prompts the STU proxy C/C_t to establish the connection from the STU to the ISAP
9a – 9b – 9c	Connection establishment between STU and ISAP. At this point the ISAP Router send out an inATMARP message on the connection. This will be ignored by the STU until it obtains the PC IP address from the DHCPACK in response to the DHCPREQUEST sent in 17 below
10a – 10b	C/C_t prompts the ses_n with the result of connection establishment e.g., VPI/VCI
11a – 11 b	Ses_n sends Resource ADD resp.conf to the Admin DAVIC Server ses_t
12a – 12b	Ses_t of the Admin DAVIC Server sends a Sess. SETUP resp.conf to Ses_n carrying the collected DHCPOFFERs in DhcpOffer Resource Descriptors see DAVIC server DHCP Relay Operation for Internet Access.
13a – 13b	Ses_n sends a Sess. SETUP resp.conf carrying the collected DHCPOFFERs in a DhcpOffer Resource Descriptors, to ses_t of the STU
14a – 14b	The Internet Access Application is sent DhcpOffer Resource Descriptors and the binding information for the connection to the ISAP e.g., VPI/VCI

--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

15a – 15b	The ISAP access application passes the bindings information and the DHCPOFFER parameters in case of method 2 of DAVIC server DHCP Relay Operation for Internet Access.
16a – 16b	Data Switcher establishes the PC Internet bindings with the connection resource and passes the DHCPOFFER parameters to the PC.
17	The PC responds to the DHCPOFFER with a DHCPREQUEST. This message is passed through on the established connection to the ISAP Router and subsequently the selected DHCP server. The DHCP now responds with DHCPACK which goes through the STU to the PC. The PC issues an ARP which contains it's IP address. The PC IP address is captured by the STU which then responds to the inATMARP sent by the ISAP router.
18	The IP packets begin to flow between the Internet WWW Server and the Web Browser after the user selects the WWW Server bookmark.

Table 9.5-11 - Dynamic Flow Parameters - Establishment of Direct Access to Internet for Direct Internet Access Scenarios 3a and b

Flow	Status	Parameters	Comments
0a-0b ISAP Connection Query req.		the path to the Web page on the Admin Server device_id	Prior to this step the PC or the STU had been brought up (e.g., independently for VoD interaction). From the Internet Web Browser on the PC or the STU the ISAP connect is selected. This sends out the ISAP Connection Query req. with an http URL format containing //<location>/<path>?<device_id> location = Admin server location path = path to the web page device_id = the MAC of the PC or the STU
1a-1b ISAP Connection Query resp.		isap_connections	The end-user is sent a web page containing the subscribed isap_connections as http URLs
2a-2b ISAP Selection req.		isap_connection	selected from the list given in 1 //<location>/<path>?<isap_connection>
3a – 3b		saved_context	The saved_context corresponds to the isap_connection in step 2. The saved_context contains Admin DAVIC Server server_id and the service_info which includes ISAP access as the default_primary_service and the specific ISAP as primary_saved_context
4a – 4b – 4c		saved_context	The Admin Server ses_t requests a session with the connection specified in the saved_context identical to 3.
5a – 5b Sess SETUP req.ind		session_id	uniquely assigned by the PC or the STU = device_id & arbitrary additional value, unique on this STU Note: One session may be permitted at a time based on the contractual agreement with the

 © ISO/IEC – All rights reserved

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

			selected ISAP.
		client_id	E164 NSAP address at the A1 interface of the client.
		server_id	E164 NSAP address of the Admin Web Server at the A9 interface.
		compatibility_descriptor	conveys a list of specific Hardware/Software at the STU available to the server
		service_info	= saved_context, indicates to the server initial service specific information. In this case the ISAP Directory service and the context from which the service can be started in a manner that the end-user will not be asked to make further selection.
6a – 6b Sess SETUP req.ind		session_id	identical to step 5
		client_id	identical to step 5
		service_info	identical to step 5 = 2
7a – 7b Resource ADD req.ind		inap_ATM_id	provided by the Admin Server based on client_id value and contractual agreement with the ISAP.
		resource # (as seen by the server) association_tag (end-to-end) resource_descriptor	describes the connection between the required ISAP and the STU and contains - physical or logical E.164 address of the port, the ISAP Router is connected to. Parameters which describe the ATM connection to be set up: - bandwidth - QOS - any other necessary parameters, such as AAL parameters, broadband bearer capabilities, etc. Note: This is the resource_descriptor for the connection which terminates on the ISAP.
8a – 8b ses_n _ c/c_t		STU_id	This contains the E164 NSAP address of the STU
		inap_ATM_id	derived from the resource descriptor in 7
		resource_attribute(s)	derived from the resource descriptor in 7
9a – 9b – 9c		all c/c signaling parameters	*Note: In order to guarantee that the connection delivered to the ISAP Router is a connection sanctioned by the ses_n, an identifier for the ses_n may be required with a time dependent or encrypted security code as part of the Q.2931 SETUP message. This information could be passed in the GIT and could be checked by the ISAP for acceptance of the incoming connection.*
10a – 10b		session_id	identical to step 5

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

c/c_t – ses_n			
		VPI/VCI (as seen by the STU A1 or the access A4)	Note: In case of non-ATM HFC access or PPP over PSTN/NISDN/PLMN, Section 9.19.8, the ses_n shall also establish a connection to the STU and will generate the associated client view resource_descriptor.
		status_id	indicates status and reason of the requested resource (e.g., OK or failed because of ...)
11a – 11b Resource ADD resp.conf		resource #	identical to 7
		status_id	indicates if the end-to-end connection has been successful or not.
12a – 12b Sess SETUP resp.conf		session_id	identical to step 8 = 5
		status_id	indicates if the request has been successful or not
		resource_# (as seen by the server)	provides the client view of the resource which corresponds to the server view in step 7.
13a – 13b Sess SETUP resp.conf		session_id	identical to 12 = 5
		status_id	identical to 12
		resource # (as seen by the server) association_tag (end-to-end) resource_descriptor	as generated by ses_n in 10.
14a – 14b		association_tag resource_descriptor	the association_tag is identical to 22. The resource_descriptor present the Client view and are identical to 10.
15		connection_binding_list DHCPOFFERs include: MTU_size IP_address subnet_mask DNS_address default_router_address	The collected DHCPOFFER information are passed to the Data Switcher and depending on the authentication configuration method used if it is 2 IP configuration information MTU_size, IP_address, subnet_mask, DNS_address, default_router_address is also passed, see Authentication and Configuration Methods for Internet Access.
16a – 16b		connection_binding_list DHCPOFFERs	The Data Switcher establishes a binding between its outgoing port and the channel described by the resource descriptor. It passes along the DHCPOFFERs to the PC. The implementation choice is between method 1or 2, see DAVIC server DHCP Relay Operation for Internet Access.

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

17		DHCPREQUEST DHCPACK inATMARP request inATMARP reply	the PC responds to the DHCPOFFERs with a DHCPREQUEST and once the IP address is confirmed then the STU informs the ISAP Router with the PC address in the inATMARP reply message.
18 WWW Client – Web Server		http protocol	At this point the IP packets can begin to flow between the Internet WWW Client and the Internet Service Provider Web Server

9.5.6.5 Release of Connection to ISAP

The end user performs a normal release of the session with the Admin DAVIC server as outlined in DAVIC VoD section on Session & Call/Connection Release.

9.5.7 Internet Access Scenario 4

9.5.7.1 Synopsis

This heralds the merging of both the DAVIC and Internet services. Maximum benefit is gained when an integrated PC and STU platform is used to gain access to an integrated ISAP Internet and DAVIC server, but non integrated STU and PC configurations are also permitted. The limitation is that the integrated platform can access Internet services off one ISAP at a time. An end-user accesses the directory of integrated ISAPs through a session on a 3rd party Directory Server.

9.5.7.2 Applicability

Allows an end-user to home on a number of service domains (IP or non-IP networks) providing the ability to provide synergy between a DAVIC service and IP or non-IP service.

The advantages are:

- maximum service benefit is derived for the end-user through the integration of the DAVIC and Internet services on one platform.
- the client_id will be verified at the ses_n and the ISAP Server before the connection is established with the ISAP router.
- capability to work with non-ATM HFC since the ses_n will interact with the access network to provide the proper inter-working between the ATM core and the non-ATM HFC or PPP Access with Broadband Broadcast and S3 Capability (Section 9.5.9).
- capability for the Network Service Provider Admin to download code e.g., for the Internet stack along with the DSM-CC application.
- the ability to select from a full list of ISAPs

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

9.5.7.3 Configuration of DAVIC Internet Scenario 4

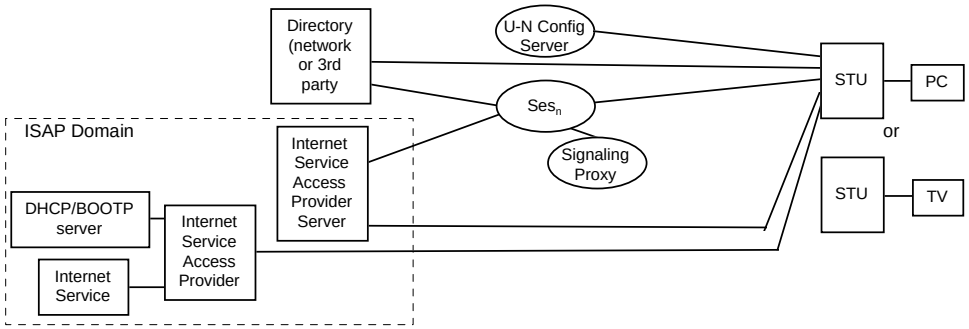


Figure 9.5-22 - System level Connectivity for Integrated Internet Scenario 4

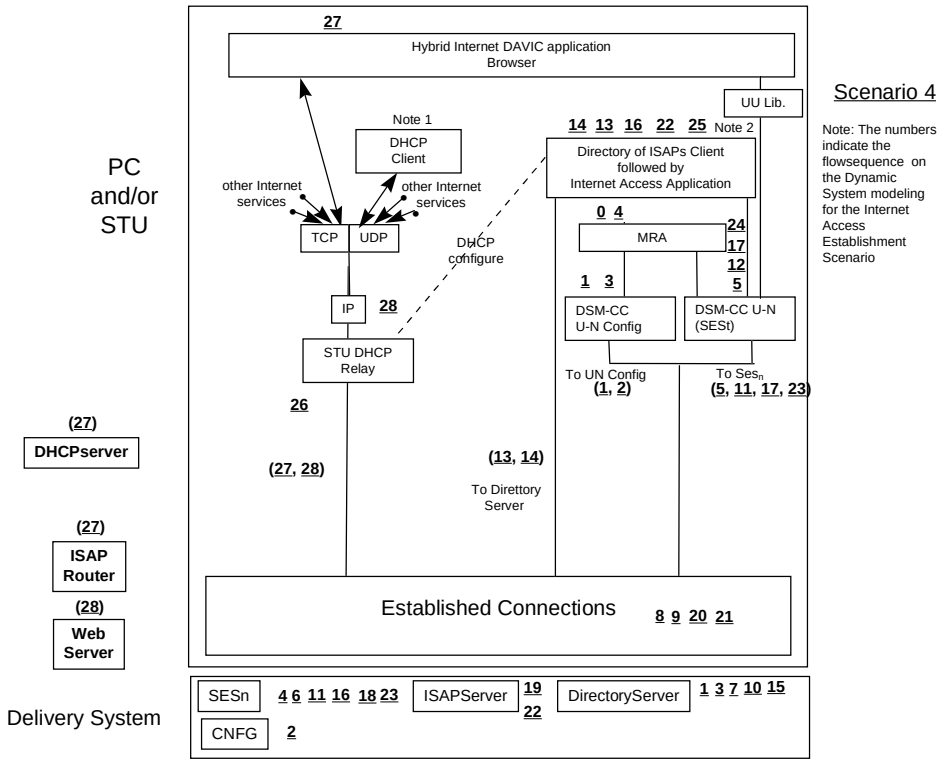


Figure 9.5-23 - STU and PC Level Entities for Direct Internet Access Scenario 4

Directory Server: Owned by the Network Services Provider, provides information for selecting ISAPs.

DHCP: Dynamic Host Configuration (RFC 1541)

DSM-CC U-N: Provides the protocol for DSM-CC U-N protocols

Established Connections: Represents connections and function for establishing connections

ISAP: Internet Service Access Provide

ISAP Server: This is a DAVIC server owned by the ISAP capable of providing IP service destinations and downloads

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ISAP Router: This is a router owned by the ISAP closest to the end-user

Directory OF ISAPs: A program on the PC (downloaded on the STU) which allows the selection of an ISAP

Internet WWW Browser: An instance of commercial browser capable of navigating the Web

IP: An instance of a stack that formats IP packets. Also performs ARP, ICMP administrative tasks

Internet Access Application: An application is used to establish the session for access to ISAP

STU DHCP Relay: DHCPDISCOVER initiates a session and reports DHCPOFFERs through Internet Access Application, DHCPREQUEST and DHSCPACK are passed through to the appropriate connection

TCP: Establishes TCP connections and formats TCP packets

UDP: Formats UDP packets

Web Server: Provides Web services

Note 1: Used only with Authentication and configuration method 1 (See subclause 9.5.10).

Note 2: Could cover authentication and configuration see method 2 or authentication only, with method 2 (See subclause 9.5.10).

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

9.5.7.4 Connection Establishment with the Internet Service Access Provider (ISAP)

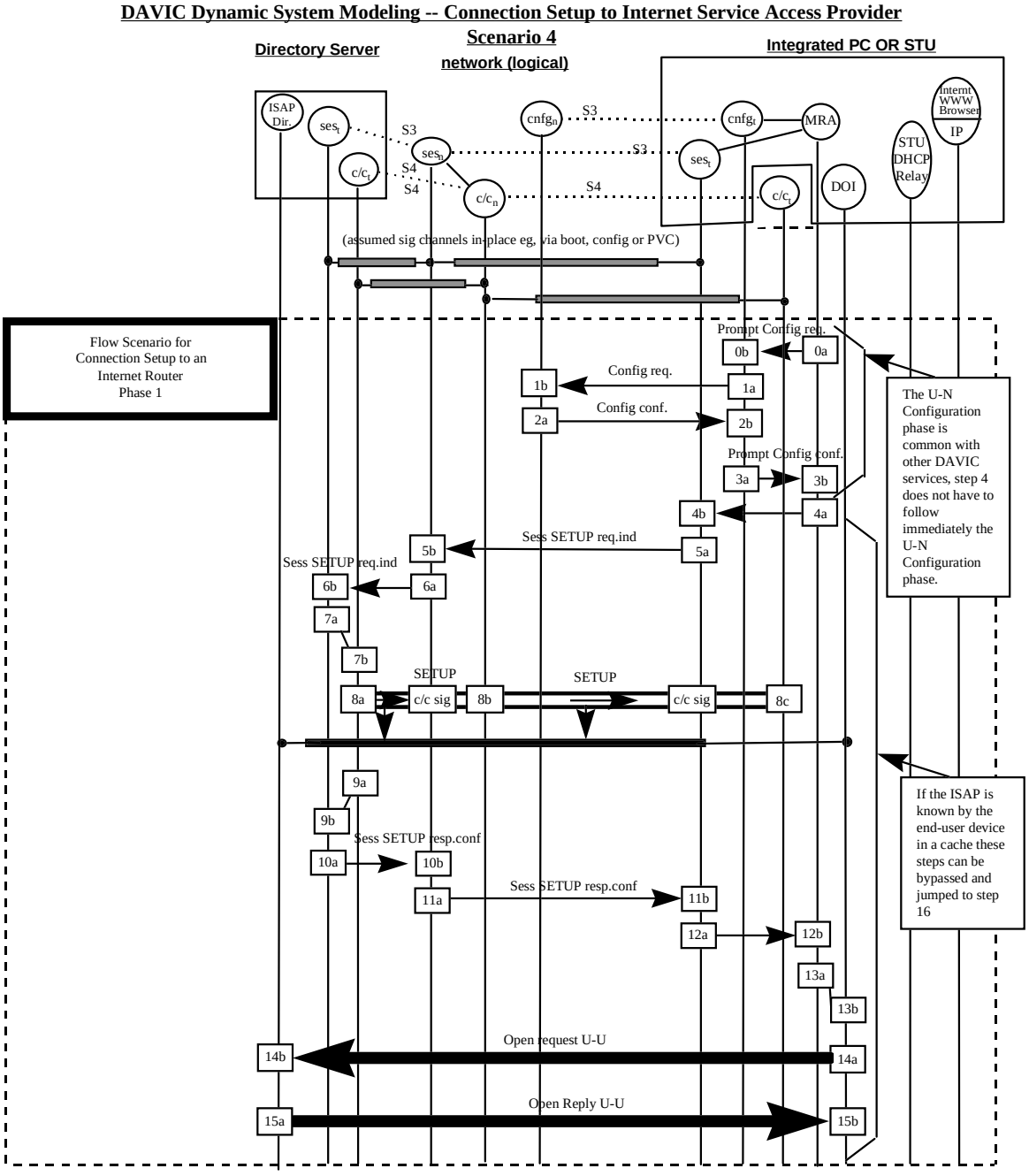
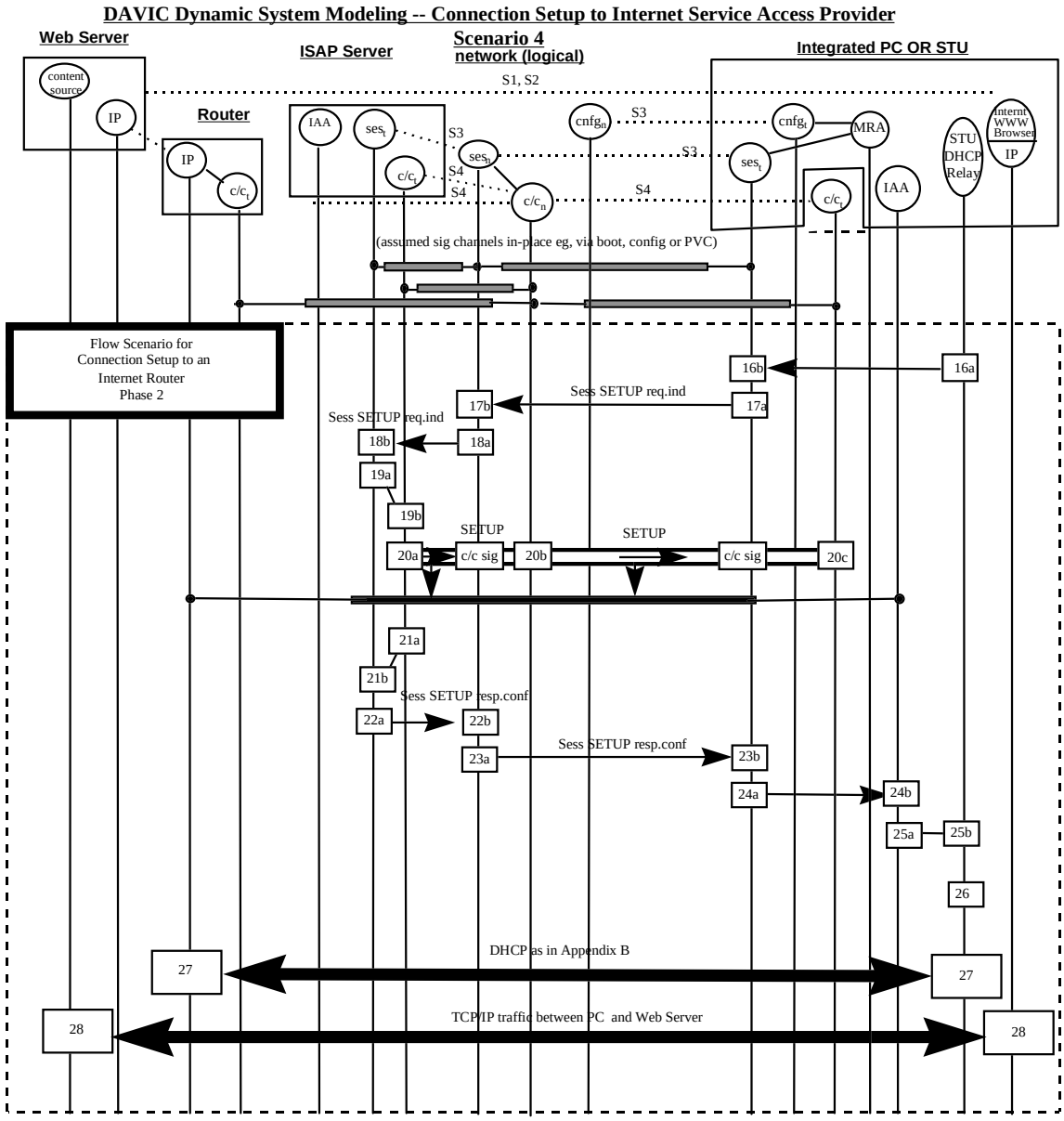


Figure 9.5-24 - Phase 1 of Scenario 4

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale



Note : This dynamic flow scenario is used for Physical Scenarios #1 and #3 (both ses(n) and the proxy signalling agent c/c(t) are colocated). In this case, flows 19a-19b and 21a-21b are actually internal. In Physical Scenario #2, c/c(t) (I.e., Q.2931) is located in the STU and can therefore be directly prompted by the STU application to initiate the connection to the router.

Figure 9.5-25 - Phase 2 of Scenario 4

Table 9.5-12 - Functional Entity Actions - Establishment Access to Internet for Scenario 5

Establishment of Direct Access to Internet	
Phase 1, see Figure 31	
0a – 0b:	The STU is powered up the Main Resident Application begins the configuration process.
1a – 1b:	The Config req is sent to the Config server

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

2a – 2b:	The Config server responds with Config conf
3a – 3b	The configuration parameters are passed on to the Main Resident Application.
4a – 4b	The Main Resident Application requests the ses_t a Session set up to the Directory Server.
5a – 5b	The STU ses_t issues a Sess SETUP req.ind to ses_n
6a – 6b	The ses_n issues a Sess SETUP req.ind to the Directory Server ses_t
7a – 7b	The Directory Server ses_t after checking with the Service Gateway and launching the ISAP Directory may request the c/c_t connections for the download and for the Client portion of the Directory of ISAPs (to be downloaded to the STU). In this scenario without the loss of generality it is assumed that the Directory of ISAPs is already present at the Client side. This is particularly likely if the device is a PC.
8a – 8b – 8c	Connection establishment for use between the Client side and the server side of the Directory of ISAPs application.
9a – 9b	c/c_t prompts the Ses_n with the result of connection establishment s.
10a – 10b	Directory Server Ses_t sends Sess SETUP resp.conf to Ses_n
11a – 11b	Ses_n sends Sess SETUP resp.conf to the STU Ses_t
12a – 12b	The STU Ses_t informs the Main Resident Application the connection binding
13a – 13b	The Main Resident Application passes on the connection resource established for the ISAP Directory
14a – 14b 15a – 15b	The Directory of ISAPs client-server User to User communication results in the selection of the ISAP.
16a – 16b	The Directory of ISAPs arms the STU DHCP Relay Agent which when it receives DHCPDISCOVER requests the ses_t a Session set up to the ISAP Server. At this stage IAA is not yet downloaded.
17a – 17b	The STU ses_t issues a Sess SETUP req.ind to ses_n
18a – 18b	The ses_n issues a Sess SETUP req.ind to the ISAP Server ses_t
19a – 19b	The ISAP Server after checking with the Service Gateway and launching the ISAP service may request the download of Internet Access Application (IAA) software and an IP stack plus any other necessary Integrated Internet DAVIC services application code. The ISAP Server ses_t requests the c/c_t connections between the ISAP Router and the IP stack. Also it broadcasts the DHCPDISCOVER, collects the DHCPOFFERs and prepares the DhcpOffer Resource Descriptors.
20a – 20b – 20c	Connection establishment between the ISAP Router and the STU DHCP Relay.
21a – 21b	c/c_t prompts the ISAP Server's ses_t with the result of connection establishments.
22a – 22b	ISAP Server's Ses_t sends Sess SETUP resp.conf to Ses_n
23a – 23b	Ses_n sends Sess SETUP resp.conf to the STU Ses_t
24a – 24b	The STU Ses_t informs the IAA the connection binding and passes along the DhcpOffer Resource Descriptor parameters.
25a – 25b	The ISAP access application passes the bindings information and the DHCPOFFER parameters in case of method 2 Appendix A.
16a – 16b	The STU DHCP Relay establishes the PC Internet bindings with the connection resource and passes the DHCPOFFER parameters to the PC.

 © ISO/IEC – All rights reserved

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

27	The PC responds to the DHCPOFFER with a DHCPREQUEST. This message is passed through on the established connection to the ISAP Router and subsequently the selected DHCP server. The DHCP now responds with DHCPACK which goes through the STU to the PC. The PC issues an ARP which contains it's IP address. The PC IP address is captured by the STU which then responds to the inATMARP sent by the ISAP router.
28	The IP packets begin to flow between the Internet WWW Server and the Web Browser after the user selects the WWW Server bookmark.

Table 9.5-13 - Dynamic Flow Parameters - Establishment of Access to Internet for Scenario 4

Flow	Status	Parameters	Comments
0a-0b The STU is powered up			The Resident Base Application requests the $Config_t$ to begin the configuration
1a-1b Config req.		device_id	this is the device_id of the STU. Optionally it may be encrypted for increased security when shared access media is used.
2a-2b Config conf.		device_id	the same as in 1
		response	indicates the status of the configuration request
		dsmccConfigurationParameters	provides DSM-CC parameter values: messageTimer, messageRetryCount, sessionIdAssignor, resourceIdAssignor, maximumForwardCount
		encapsulation	RFC 1483 for ATM or MPEG TS ISO/IEC 13818-6. RFC-1483 LLC/SNAP is the default. Each of the encapsulation types specified by RFC-1483 shall also be supported.
		networkConfigurationParameters	provides initial default server which may be 3rd party Directory Server.
3a-3b $Config_t$ – Main Resident App		server_id	This consists the initial server_id for user selection one of which is default. The Resident Base Application may either choose the default or display to the user for the selection of an initial service. In either case the ISAP Directory Service is selected.
4a – 4b Main Resident App – Ses_t		server_id	this is the Admin Server server_id
5a – 5b Sess SETUP req.ind		session_id	uniquely assigned by the STU = device_id & arbitrary additional value, unique on this STU
		client_id	E164 NSAP address at the A1 interface of the client.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

		server_id	identical to step 4
		compatibility_descriptor	conveys a list of specific Hardware/Software at the STU available to the server
		service_info	=rPathSpec, indicates to the server initial service specific information. In this case the Directory of ISAPs service
6a – 6b Sess SETUP req.ind		session_id	identical to step 5
		client_id	identical to step 5
		service_info	identical to step 5 = 2
7a – 7b ses_t – c/c_t		STU_id	This contains the E164 NSAP address of the STU
		resource # (as seen by the server) association_tag (end-to-end) resource_descriptor	describes the connection between the required DOI server and the STU and contains - physical or logical E.164 address of the port, the ISAP Router is connected to. Parameters which describe the ATM connection to be set up: - bandwidth - QOS - any other necessary parameters, such as AAL parameters, broadband bearer capabilities, etc.
8a – 8b – 8c		all c/c signaling parameters	see DAVIC 5
9a – 9b c/c_t – ses_t		session_id	identical to step 5
		VPI/VCI (as seen by the STU A1 or the access A4)	Note: In case of non-ATM HFC access or PPP over PSTN/NISDN/PLMN, Section 9.19.8, the ses_n shall also establish a connection to the STU and will generate the associated client view resource_descriptor.
		status_id	indicates status and reason of the requested resource (e.g., OK or failed because of ...)
10a – 10b Sess SETUP resp.conf		session_id	identical to step 7 = 5
		status_id	indicates if the request has been successful or not
		resource_# (as seen by the server)	provides the client view of the resource which corresponds to the server view in step 7.
11a – 11b Sess SETUP resp.conf		session_id	identical to 10 = 5

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

		status_id	identical to 10
		resource # (as seen by the server) association_tag (end-to-end) resource_descriptor	as generated by ses_t in 7.
12a – 12b		resource_# (as seen by the client) association_tag resource_descriptor connection_binding_list	from step 11
13a – 13b		connection_binding_list	same as in 12=10
14a – 14b			User-to-User RPC message exchange which culminates in the selection of an ISAP. Note: If the ISAP is known in advance and stored in a cache then jump to step 16.
15a – 15b DOI – DOI		next_service_location	this includes the server_id, and optionally the PathName and SavedContext of the service on the selected ISAP server
16a – 16b DOI App – Ses_t		server_id	this is the ISAP Server server_id
		selected_service	this is the ISAP service
17a – 17b Sess SETUP req.ind		session_id	uniquely assigned by the PC/STU = device_id & arbitrary additional value, unique on this STU
		client_id	E164 NSAP address at the A1 interface of the client.
		server_id	identical to step 16 = 15
		compatibility_descriptor	conveys a list of specific Hardware/Software at the STU available to the server
		service_info	=rPathSpec, indicates to the server initial service specific information. In this case the Internet access service
18a – 18b Sess SETUP req.ind		session_id	identical to step 17
		client_id	identical to step 17
		service_info	identical to step 17 = 15
19a – 19b ses_t _ c/c_t		STU_id	This contains the E164 NSAP address of the STU
		resource # (as seen by the server) association_tag (end-to-end) resource_descriptor	describes the connection between the required ISAP and the STU and contains - physical or logical E.164 address ofthe port, the ISAP Router is connected to.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

			Parameters which describe the ATM connection to be set up: - bandwidth - QOS - any other necessary parameters, such as AAL parameters, broadband bearer capabilities, etc. Note: This is the resource_descriptor for the connection which terminates on the ISAP.
20a – 20b – 20c		all c/c signaling parameters	see 5 of this specification
21a – 21b c/c_t – ses_t		session_id	identical to step 5
		VPI/VCI (as seen by the STU A1 or the access A4)	Note: In case of non-ATM HFC access or PPP over PSTN/NISDN/PLMN, Section 9.19.8, the ses_n shall also establish a connection to the STU and will generate the associated client view resource_descriptor.
		status_id	indicates status and reason of the requested resource (e.g., OK or failed because of ...)
22a – 22b Sess SETUP resp.conf		session_id	identical to step 18 = 17
		status_id	indicates if the request has been successful or not
		resource_# (as seen by the client)	provides the client view of the resource which corresponds to the server view in step 19.
23a – 23b Sess SETUP resp.conf		session_id	identical to 22 = 17
		status_id	identical to 22
		resource # (as seen by the server) association_tag (end-to-end) resource_descriptor	as generated by ses_t in 19.
24a – 24b		resource_# (as seen by the client) association_tag resource_descriptor connection_binding_list	from step 22
25a – 25b		connection_binding_list DHCPOFFERs include: MTU_size IP_address	The collected DHCPOFFER information are passed to the Data Switcher and depending on the authentication configuration method used if it is 2 IP configuration information MTU_size, IP_address, subnet_mask, DNS_address, default_router_address is also passed, see

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

		subnet_mask DNS_address default_router_address	Authentication and Configuration Methods for Internet Access.
26a – 26b		connection_binding_list DHCPOFFERs	The Data Switcher establishes a binding between its outgoing port and the channel described by the resource descriptor. It passes along the DHCPOFFERs to the PC. The implementation choice is between method 1or 2, See subclause 9.5.10
27		DHCPREQUEST DHCPACK inATMARP request inATMARP reply	the PC responds to the DHCPOFFERs with a DHCPREQUEST and once the IP address is confirmed then the STU informs the ISAP Router with the PC address in the inATMARP reply message.
28 WWW Client – Web Server		http protocol	At this point the IP packets can begin to flow between the Internet WWW Client and the Internet Service Provider Web Server

9.5.7.5 Release of Connection to ISAP

The release of the connection can be done by releasing the Session with the ISAP Server. This can be effected by the STU or the It follows the procedures described in DAVIC VoD section.

9.5.8 Specification of the DAVIC Protocol Tools for Internet Access

This section specifies the protocol stacks to be used for Internet Access in a DAVIC conformant system. All Physical Scenarios of DAVIC VoD are to be supported, if applicable. It is assumed that proxy signaling or PVC is used in DAVIC Physical Scenarios 1,3, and 4. In the case of Physical Scenario 2, the proxy connection control signaling entity is replaced by Q.2931 signaling resident in the STU in order to establish the connection to the ISAP Router.

Figure 9.5-26 shows the protocol stacks for upstream (all cases) and downstream (for end-to-end ATM).

Figure 9.5-27 shows the downstream protocol stacks for the case where ATM terminates in the access (HFC, non-end-to-end ATM).

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

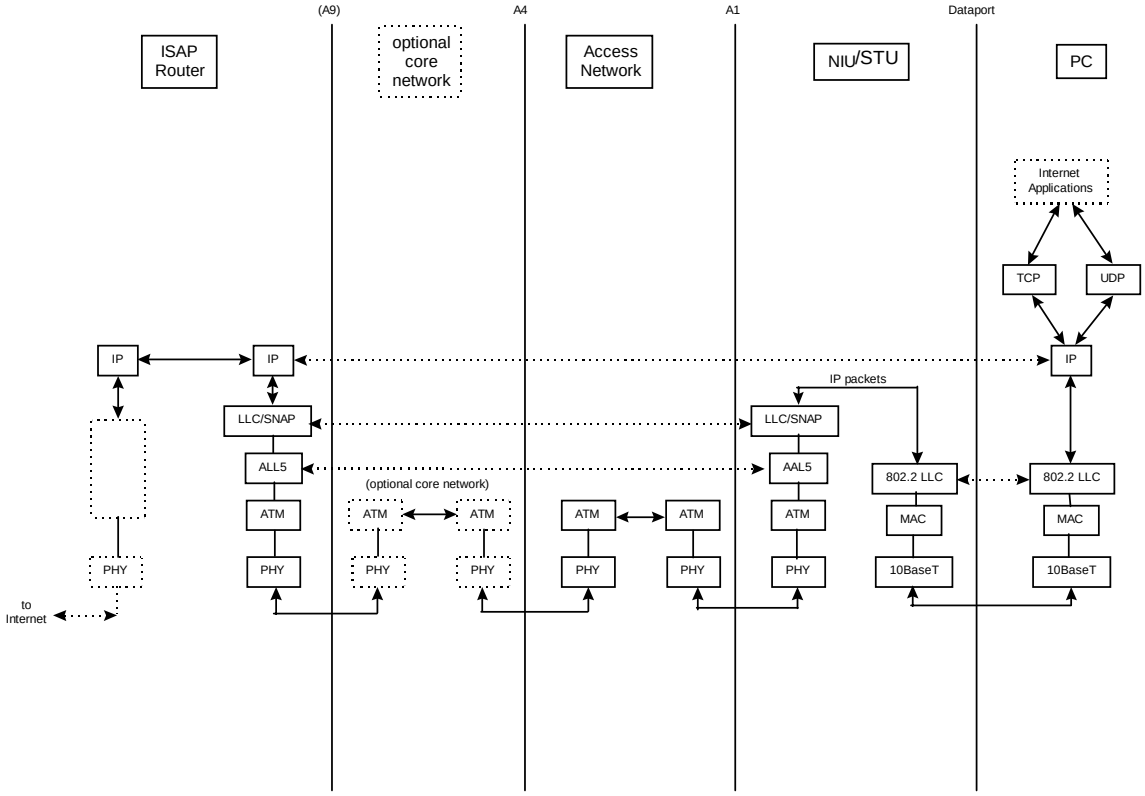


Figure 9.5-26 - Protocol Stacks for Upstream (All Cases) and Downstream (for ATM end-to-end)

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

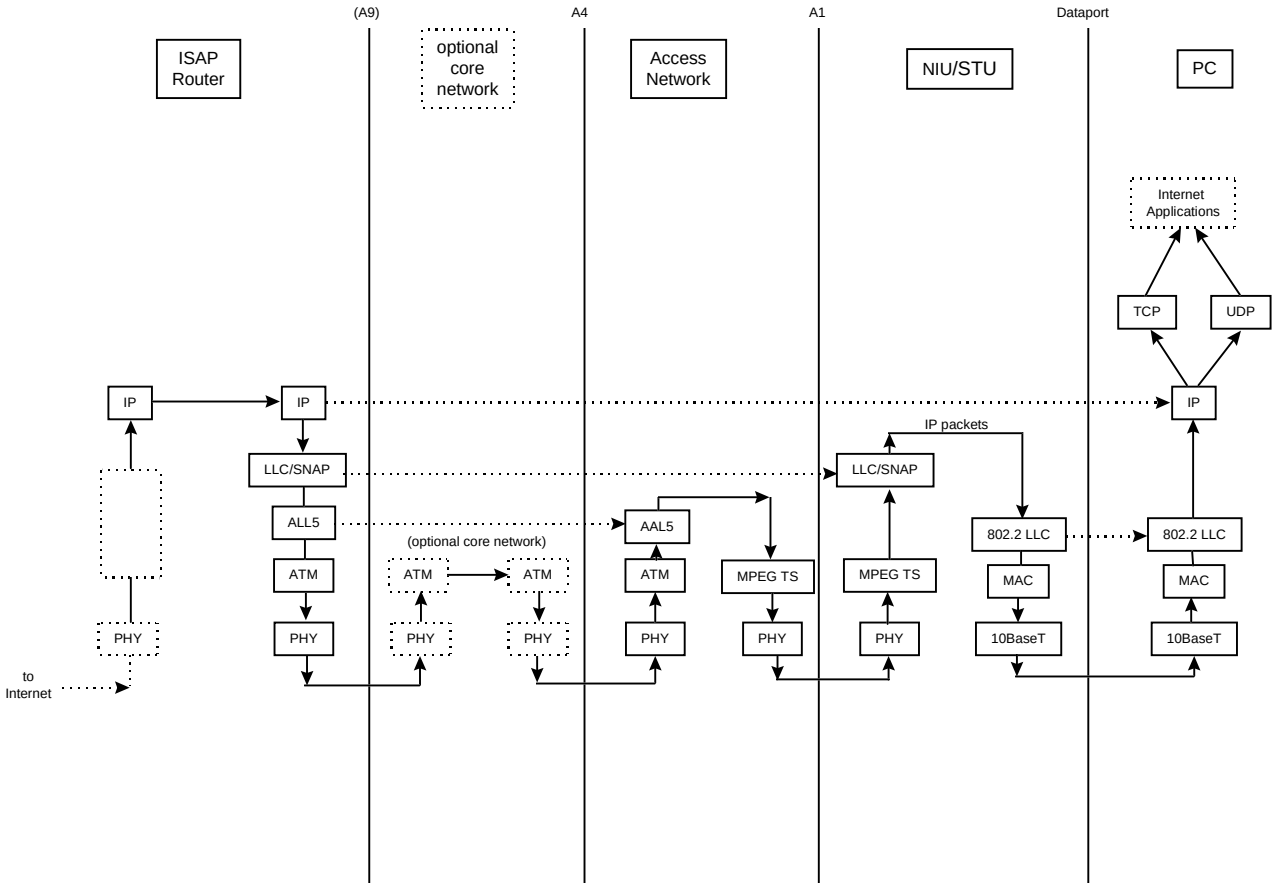


Figure 9.5-27 - Protocol stacks for the case where ATM terminates in the access (HFC, non-end-to-end ATM).

9.5.9 PPP Access with Broadband Broadcast and S3 Capability

9.5.9.1 Synopsis

A STU connected to a broadband delivery network and a narrowband return channel (PSTN/ISDN/PLMN) is used for accessing Internet services. DAVIC/DSM-CC session is used for signaling the necessary parameters of the transport. This scenario is independent of the IP address allocation for the PC. However, the scenario supports using the S3 messages for transmitting this information.

9.5.9.2 Physical network model

In the physical network model, the access network consists of a broadband broadcast network and a narrowband return channel. The S3 flow is carried in the narrowband channel in both directions. The upstream part of the Sip flow is always carried through the narrowband channel. The downstream part of Sip may be carried over the broadband network, the narrowband channel or both the broadband and narrowband channels can be combined.

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

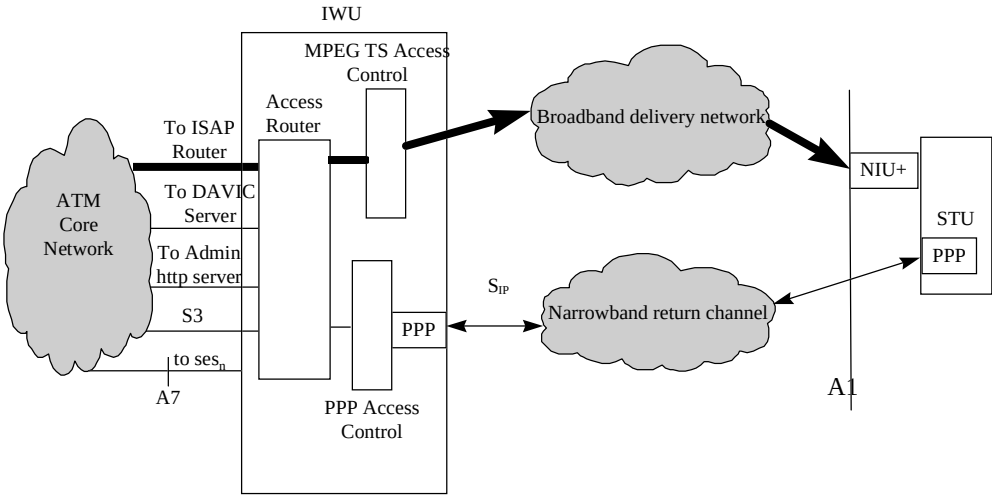


Figure 9.5-28 - IWU Functional Components

Figure 9.5-28 shows the overall configuration of the PPP Access with Broadband Broadcast and S3 Capability. The PPP connection is established over PSTN/NISDN/PLMN Upon request from the STU over a separate connection bypassing the A0 interface. The Broadband connection is established over the A0 interface through the NIU. It may consist of straight MPEG or MPEG over ATM using HFC or satellite transmission. The IWU is connected to the core through which ATM connections are established over PVC or SVC to the ISAP Router, the DAVIC server, the Admin http server and ses_n. In addition to these connections the IWU is connected to the ses_n through A7 for exchange of connection control information. The functions of each functional component in the IWU are described below:

Access Router:

- It contains DHCP relay function through which it can extract the IP address of the PC and use the information to logically bind the PC to the connection based on the source IP.
- It performs the routing functions of the IP packets received from the network to the MPEG Access Control and the PPP access Control based on the destination STU IP's and the mode of operation using PPP downstream only, MPEG TS only or both for the specific session indicated on the GIT (Generic Identifier Transport) of the Q.2931 of the ATM connection as indicated by ses_n. through the A7 interface.
- It routes the IPs received from the MPEG Access Control and the PPP access Control based on the source IP address and the destination IP address.

MPEG TS Access Control:

- It chooses a PID and sends datagram_sections using the STU MAC address, to the STU. The MAC address is derived from the PCs IP address from a table built by the Access Router using STU Client ID information from ses_n.
- It prepares the client view of the resource descriptor for the Sip and sends it to the ses_n over A7 coupled with locally generated resource ID.

PPP Access Control:

- It assigns a port number to the IP received from DAVIC servers. S3 and http connections are assigned well known port numbers. No port numbers for the connections to the ISAP routers are assigned since these are differentiated by the IP of the destination PC connected to the STU.
- The assigned port number is communicated to the ses_n over A7 coupled with locally generated resource ID together with an association tag shared with the MPEGTS descriptor if it is used for the downstream IP path.

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

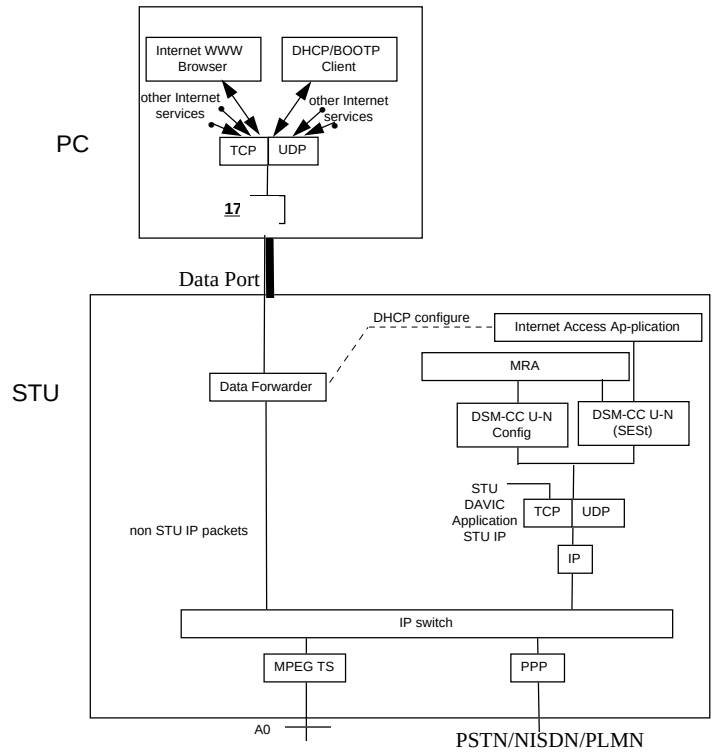


Figure 9.5-29 - STU and PC level of entities for PPP/Broadband Access and S3

Figure 9.5-29 shows the entities within the STU. The IP switch separates those IP packets which are not STU IPs and forwards them to the Data Forwarder. The STU IP packets which are used with the DAVIC server are assigned a port number communicated by ses_n to the STU through the IP resource descriptors.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

9.5.9.3 Protocol Stacks

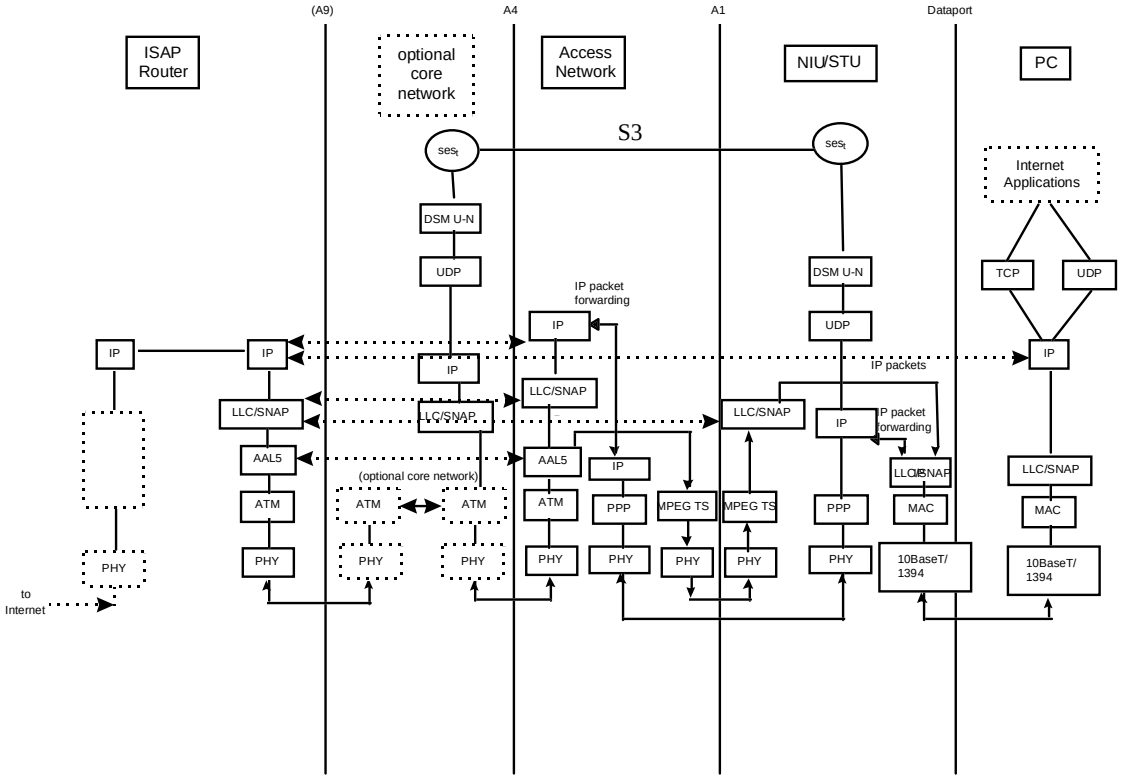


Figure 9.5-30 – Protocol Stacks for PPP Access with Broadcast and S3 Capability

9.5.9.4 Broadband MPEG TS encapsulation format and filtering

Each datagram is encapsulated in one datagram_section, which is to the DSMCC_section format for private data defined in ISO/IEC 13818-6 (DSM-CC). The mapping of the section into MPEG-2 Transport Stream packets is defined in ISO/IEC 13818-1 (MPEG-2 Systems).

The syntax and semantics of the datagram_section are defined below. Because of this encapsulation specification the MTU is 4080 bytes.

The syntax of the datagram is fully aligned with the DVB specification for Data Broadcasting.

Table 9.5-14 - Syntax of datagram_section

Syntax	No. of bits	Mnemonic
datagram_section() {		
table_id	8	uimsbf
section_syntax_indicator	1	bslbf
private_indicator	1	bslbf
reserved	2	bslbf
section_length	12	uimsbf

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

MAC_address_byte_6	8	uimsbf
MAC_address_byte_5	8	uimsbf
reserved	2	bslbf
payload_scrambling_control	2	bslbf
address_scrambling_control	2	bslbf
LLCSNAP_header_flag	1	bslbf
payload_compression_flag	1	bslbf
section_number	8	uimsbf
last_section_number	8	uimsbf
MAC_address_byte_4	8	uimsbf
MAC_address_byte_3	8	uimsbf
MAC_address_byte_2	8	uimsbf
MAC_address_byte_1	8	uimsbf
if (LLC_SNAP_flag==‘1’) {		
LLCSNAP()		
} else {		
for (j=0;j<N;j++) {		
IP_datagram_data_byte	8	bslbf
}		
}		
for (k=0;k<M;k++) {		
stuffing_byte	8	bslbf
}		
if (section_syntax_indicator ==‘0’) {		
checksum	32	uimsbf
} else {		
CRC_32	32	rpchof
}		
}		

The semantics of the datagram_section are as follows:

table_id : this is an 8-bit field which shall be set to 0x3E (DSM-CC sections with private data).

section_syntax_indicator : this field shall be set as defined by ISO/IEC 13818-6.

private_indicator : this field shall be set as defined by ISO/IEC 13818-6.

reserved: this is a 2-bit field that shall be set to ‘11’.

section_length : this field shall be set as defined by ISO/IEC 13818-6.

MAC_address_byte_[1..6] : this 48-bit field contains the MAC address of the destination. The MAC address is fragmented in 6 fields of 8-bits, labeled MAC_address_byte_1 to MAC_address_byte_6. The MAC_address_byte_1 field contains the most significant byte of the MAC address, while MAC_address_byte_6 contains the least significant byte. Figure 9.5-31illustrates the mapping of the MAC

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

address bytes in the section fields. Note that the order of the bits in the bytes is not reversed and that the most significant bit of each byte is still transmitted first.

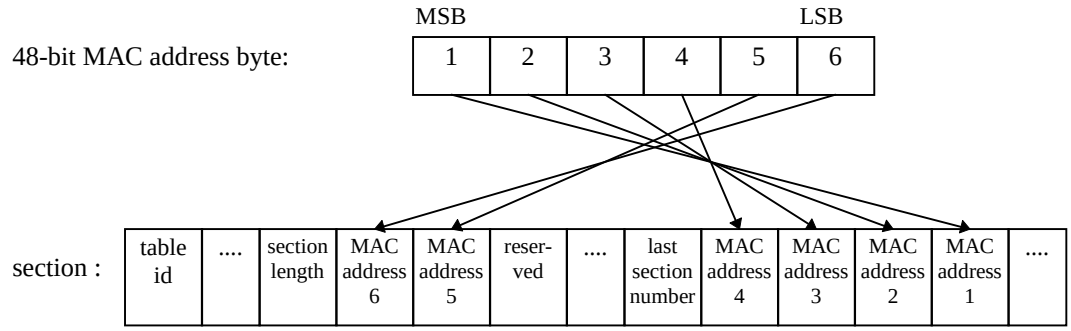


Figure 9.5-31 - Mapping of MAC address bytes to section fields

The MAC_address fields contain either a clear or a scrambled MAC address as indicated by the address_scrambling_control field.

payload_scrambling_control : this 2-bit field defines the scrambling mode of the payload of the section. This includes the payload starting after the MAC_address_byte_1 but excludes the checksum or CRC32 field. If both compression and scrambling are performed, the compression shall be done before scrambling. See Table 9.5-15. The scrambling method applied is user private.

Table 9.5-15 - Coding of the payload_scrambling_control field

value	payload scrambling control
00	unscrambled
01	defined by service
10	defined by service
11	defined by service

address_scrambling_control - this 2-bit field defines the scrambling mode of MAC address in this section. See Table 9.5-16. This field enables a dynamic change of MAC addresses. The scrambling method applied is user private.

Table 9.5-16 - Coding of the address_scrambling_control field

value	address scrambling control
00	unscrambled
01	defined by service
10	defined by service
11	defined by service

LLCSNAP_header_flag: this is a 1-bit flag. If this flag is set to '1' the payload carries an LLCSNAP encapsulated datagram following the MAC_address_1 field. The LLCSNAP header structure shall indicate

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

the type of the datagram conveyed. If this flag is set to '0', the section shall contain an IP datagram without an LLCSNAP encapsulation.

payload_compression_flag: this is a 1-bit flag. If this flag is set to '1' the payload of the section is compressed which includes the payload starting after the MAC_address_byte_1 but excludes the checksum or CRC32 field. If both compression and scrambling are performed, the compression shall be done before scrambling. If set to '0' the payload is not compressed.

reserved: this is a 2-bit field that shall be set to '11'.

section_number: this 8-bit field shall have the value 0x00. The usage of other values is reserved for future use.

last_section_number: this 8-bit field shall be set to the value of 0x00. The usage of other values is reserved for future use.

LLCSNAP() - this field shall contain the encapsulated datagram according to the ISO/IEC 8802-2 Logical Link Control (LLC) and ISO/IEC 8802-1a SubNetwork Attachment Point (SNAP) specifications. If the payload of the section is scrambled (see payload_scrambling_mode), these bytes are scrambled. If the payload of the section is compressed (see payload_compression_flag), these bytes are compressed.

IP_datagram_data_byte - these bytes contain the data of the IP datagram. If the payload of the section is scrambled (see payload_scrambling_mode), these bytes are scrambled. If the payload of the section is compressed (see payload_compression_flag), these bytes are compressed.

stuffing_type: this is a 8-bit field that shall be set to 0xFF.

checksum - This field shall be set as defined by ISO/IEC 13818-6. It is calculated over the entire datagram_section.

CRC_32 - This field shall be set as defined by ISO/IEC 13818-6. It is calculated over the entire datagram_section.

9.5.9.5 Resource descriptors

The PID and the physical parameters of the channel carrying the MPEG TS are transported using the resource descriptors in the DAVIC VoD portion of this specification.

Interactive Broadcast descriptor covering the following modes is defined in the later section, Internet Access DAVIC Defined Resource Descriptors, with:

1 = with MPEG TS and PSTN/NISDN/PLMN Downstream and PSTN/NISDN/PLMN Upstream

2 = with MPEG TS Downstream and PSTN/NISDN/PLMN Upstream

3 = PSTN/NISDN/PLMN Downstream and Upstream

9.5.9.6 S3 signaling via PSTN/ISDN/PLMN return channel

The Interactive Broadcast Scenario defines the physical tools for using the PSTN/ISDN/PLMN channel as a return channel with PPP link. However, it does not specify how the S3 signaling should be done in that case.

Difference between the PPP link and the normal DAVIC return channel scenarios is that the PPP link provides a connection to an IP network instead of ATM as all other DAVIC scenarios. When the S3 flow shall be carried over the PPP link, the IP address of the ses_n entity shall be well known to the STU. DSM-CC U-N messages shall be sent using normal UDP/IP over the PPP link instead of the dedicated ATM virtual circuit used in other DAVIC scenarios.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

In this case the protocol stack looks like this:

DSM-CC U-N
UDP
IP
PPP
Phy

It should be noted that in this case the STU needs an IP address for itself in addition to the possible other IP address given to the PC. This IP address will be assigned to the STU using IPCP during the PPP link SetUp. The IP address for the STU does not need to be a real Internet address; it can be taken from a address space which is defined to be private address space in RFC1597 (i.e. packets from those addresses will not be routed to the Internet, but they can be used for internal communication in the subnet.)

9.5.9.7 DHCP with PPP access network

The STU has to operate as a DHCP forwarder as defined in RFC 1542 and forward the DHCP calls to the actual DHCP server. This operation is different than in ATM networks since the STU has to know the IP address of the DHCP server and send the request directly to it.

9.5.10 Authentication and Configuration Methods for Internet Access

The following authorization and configuration methods can potentially be used with the scenarios described in this contribution:

DSM-CC based authentication and DHCP based configuration, Figure 9.5-32.

1. DSM-CC based authentication and configuration through DHCP Relay, Figure 9.5-33.

The choice of the method used is an implementation and deployment matter

 © ISO/IEC – All rights reserved

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

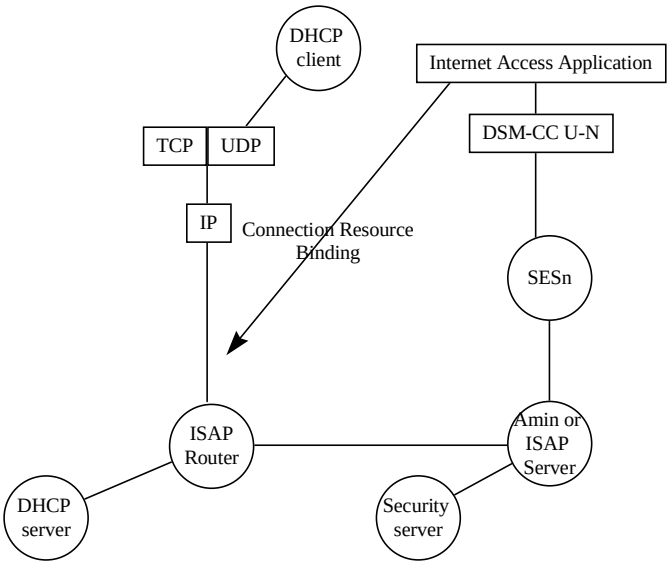


Figure 9.5-32 - Authentication using DSM-CC and Configuration using DHCP

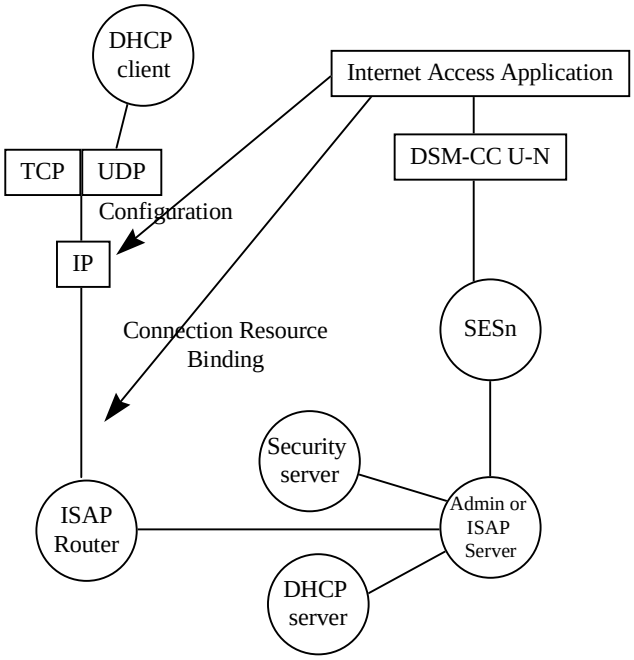


Figure 9.5-33 - Both authentication and Configuration done using DSM-CC

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

9.5.11 DAVIC server DHCP Relay Operation for Internet Access

This section provides the procedure of DHCP relay operation over DSM-CC:

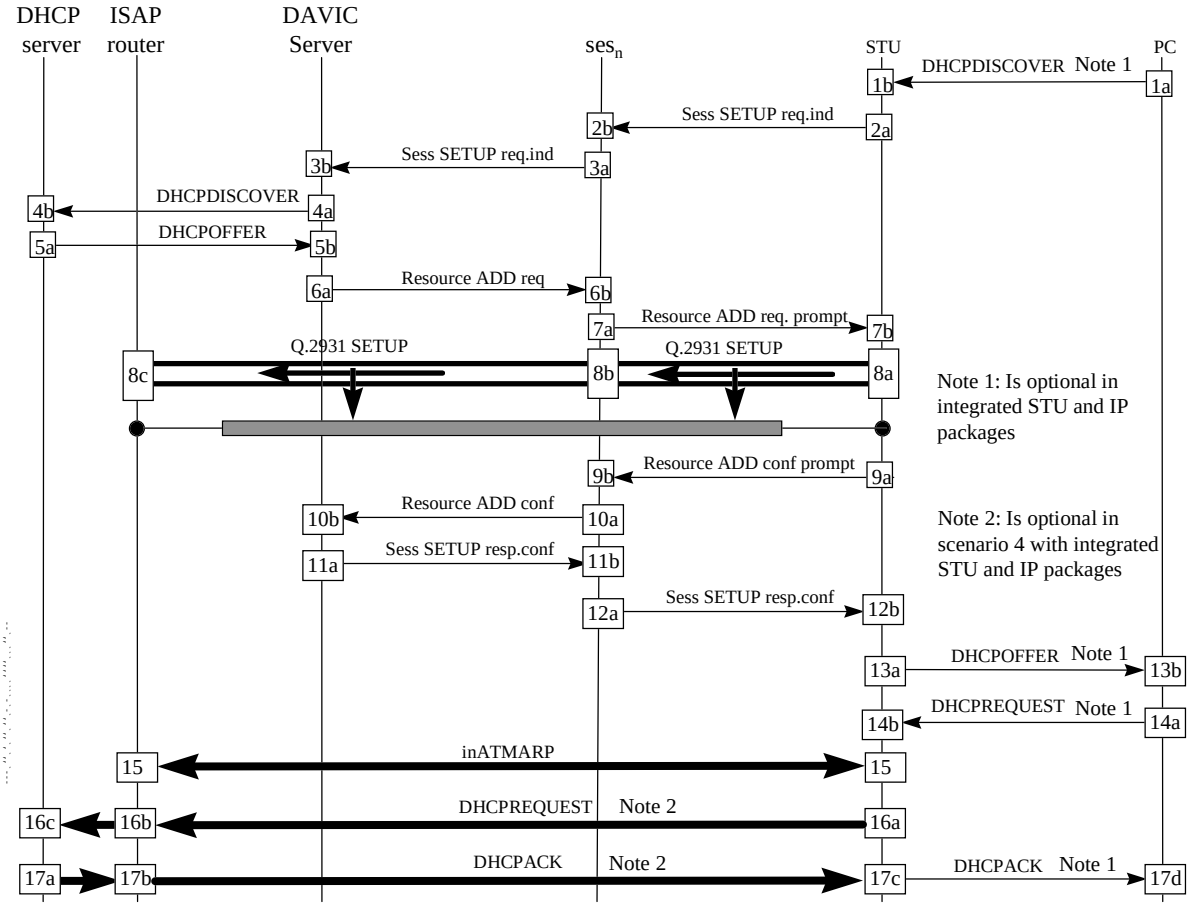


Figure 9.5-34 - DHCP initiated Internet session SetUp

Table 9.5-17 - Functional Entity Actions - Initiating a session SetUp from a PC

Establishment of Direct Access to Internet	
1a - 1b:	PC sends DHCPDISCOVER IP message over Ethernet
2a - 2b	Upon receiving DHCPDISCOVER the STU initiates a Sess SETUP req.ind to ses$_n$
3a - 3b	ses$_n$ sends Sess SETUP req.ind to the DAVIC Server
4a - 4b	The DAVIC Server broadcasts DHCPDISCOVER as a DHCP relay agent
5a - 5b	A DHCPOFFFER is received from a DHCP server responding to the DHCPDISCOVER with DHCPOFFER
6a - 6b	The DAVIC Server sends a Resource ADD req. to establish a connection with a specific QoS between the STU and the ISAP router.
7a - 7b	ses$_n$ requests the STU Proxy Signaling Agent (PSA) to initiate a connection

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

8a - 8b - 8c	In the case of ATM SVC an SVC connection is established
9a - 9b:	The PSA reports the success of connection establishment
10a - 10b	ses_n sends Resource ADD conf to the DAVIC Server
11a - 11b	The DAVIC Server collects the DHCPOFFERs received from the responding DHCP servers into an DHCP resource descriptor and associates it to the SVC using a Shared_Resource resource descriptor. It sends the resource descriptors in Sess SETUP resp.conf to ses_n
12a - 12b	ses_n adds the ATM SVC resource descriptor to the Sess SETUP resp.conf and sends it to the STU
13a - 13b	The STU extracts the DHCPOFFERs from the DHCP resource descriptor in the Sess SETUP resp.conf and sends them to the PC on the IEEE 1394 port or Ethernet
14a - 14b	The PC sends a DHCPREQUEST to a specific DHCP server confirming its IP address plus some of the offered parameters and requesting for modification other parameters.
15	The STU extracts the PC IP address from the DHCPREQUEST and responds to the inATMARP repeatedly sent by the ISAP router since connection establishment. (Alternatively in case of PVC the STU triggers the ISAP inATMARP by issuing an inATMARP of its own at step 13)
16a - 16b - 16c	To STU now passes through the DHCPREQUEST message which is broadcast at the ISAP router to all the DHCP servers including the selected server. The selected DHCP server binds the parameters while the other DHCP servers release them (if they were temporarily reserved)
17a - 17b - 17c	The selected DHCP server responds to the DHCPREQUEST with DHCPACK

Table 9.5-18 - Dynamic Flow Parameters - Initiating a session SetUp from a PC

Flow	Status	Parameters	Comments
1a-1b DHCPDISCOVER		htype	Hardware address type = 1 for 10mb Ethernet
		hlen	= 6 for 10mb Ethernet
		hops	= 0
		xid	Transaction ID, a random number chosen by the client, used by the client and server to associate messages and responses between a client and a server
		secs	(opt.)
		flags	Set 'BROADCAST' flag if client requires broadcast reply 0
		ciaddr	= 0
		yiaddr	= 0
		siaddr	= 0
		chaddr	Client hardware address
		giaddr	Relay agent IP address, used in booting via a relay-agent = 0 .

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

		sname	options, if indicated in 'sname/file' option; otherwise unused
		file	options, if indicated in 'sname/file' option; otherwise 'generic' name or null
		options	Requested IP address - MAY IP address lease time - MAY Use 'file'/'sname' fields - MAY DHCP message type - DHCPDISCOVER Client identifier - MAY Class identifier - SHOULD Server identifier - MUST NOT Parameter request list - MAY Maximum message size - MAY Message - SHOULD NOT Site-specific - MAY All others - MUST NOT See Appendix A
2a - 2b Sess SETUP req.ind		session_id	uniquely assigned by the STU
		client_id	E.164 NSAP address at the A1 interface of the client.
		server_id	E.164 NSAP address at the A9 interface of the server.
		compatibility_discriminator	conveys a list of specific Hardware/Software at the STU available to the server.
		service_info	indicates specific information about service selection it includes the selected ISAP and the options from 1
3a - 3b Sess SETUP req.ind		session_id	identical to 2
		client_id	identical to 2, with the possibility that the ses_n replaces the physical address by a logical address (e.g., for reasons of privacy)
		server_id	physical E.164 NSAP address of the Server which the STU wants to establish a session with (identical to 2, if logical address was used, this address has to be replaced by the physical address for this step)
		compatibility_descriptor	identical to 2
		service_info	identical to 2
4a-4b DHCPDISCOVER		htype	identical to 1

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

		hlen	identical to 1
		hops	identical to 1
		xid	identical to 1
		secs	identical to 1
		flags	identical to 1
		ciaddr	identical to 1
		yiaddr	identical to 1
		siaddr	identical to 1
		chaddr	identical to 1
		giaddr	On the ISAP net IP address, of the DAVIC Server .
		sname	identical to 1
		file	identical to 1
		options	identical to 1
5a-5b DHCPOFFER. (RFC 1541 RFC 1533)		htype	identical to 4=1
		hlen	identical to 4=1
		hops	identical to 4=1
		xid	identical to 4=1
		secs	= 0
		ciaddr	= 0
		yiaddr	IP address offered to client
		siaddr	IP address of next bootstrap server
		flags	if 'giaddr' is not 0 then 'flags' from client message else 0
		chaddr	identical to 4=1
		giaddr	identical to 4
		sname	Server host name or options
		file	Client boot file name or options
		options	Requested IP address - MUST NOT IP address lease time - MUST Use 'file'/'sname' fields - MAY DHCP message type - DHCPOFFER Parameter request list - MUST NOT Message - SHOULD Client identifier - MUST NOT Class identifier - MUST NOT Server identifier - MUST

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

			Maximum message size - MUST NOT All others - MAY See Appendix A
6a - 6b Resource ADD req		session_id	identical to 3=2
		resource_number association_tag AtmSvcConnection	assigned by the server assigned by the server to be bound to the Data Forwarder interface as in the SETUP signaling message (e.g., Q.2931, ATM UNI 3.1 or 4.0). The values are based on the client's subscription and Network Service Provider's network
		status_id	indicates status and reason of the requested resource
7a - 7b		session_id	identical to 6=2
		resource_number association_tag AtmSvcConnection	identical to step 6 identical to step 6 identical to step 6
		status_id	indicates status and reason of the requested resource
8a - 8b - 8c			ATM SVC connection established
9a - 9b		session_id	identical to 7=2
		resource_number association_tag AtmSvcConnection	identical to 7=6 identical to 7=6 established values
		status_id	indicates status and reason of the requested resource
10a - 10b Resource ADD conf		session_id	identical to step 9=2
		resource_number association_tag	identical to step 6 identical to step 6

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

		AtmSvcConnection	identical to step 9
		status_id	indicates the status and the reason of the confirm
11a - 11b Sess SETUP resp.conf		session_id	identical to step 3=2
		server_id	identical to step 3=2
		resource_number association_tag DhcpOfferResource	STU view used in binding the resource in the STU to the Data Forwarder interface contains the different options by DHCPOFFER received at the DAVIC Server, see the section on DAVIC Defined Resource Descriptors for Internet Access.
		resource_number association_tag SharedResource	STU view the same as for the resource it brings into the shared resource relates to the SVC connection in step 6
		status_id	indicates the status and the reason of the resp.conf
12a - 12b Sess SETUP resp.conf		session_id	identical to step 11=2
		server_id	identical to step 11=2 (Note: this assumes session forward is not used)
		resource_number association_tag AtmSvcConnection	identical to step 10
		resource_number association_tag DhcpOfferResource	identical to step 11
		resource_number association_tag	identical to step 11

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

		SharedResource	
		status_id	indicates the status and the reason of the resp.conf
13a-13b DHCPOFFER. (RFC 1541 RFC 1533)		htype	same as in 1
		hlen	identical to step 5=1
		hops	identical to step 5=1
		xid	identical to step 5=1
		secs	identical to step 5=1
		ciaddr	identical to step 5=1
		yiaddr	identical to step 5
		siaddr	identical to step 5
		flags	identical to step 5=1
		chaddr	identical to step 5=1
		giaddr	identical to 1
		sname	identical to step 5
		file	identical to step 5
		options per each DHCPOFFER	identical to step 5
14a-14b DHCPREQUEST (RFC 1541 RFC 1533)		htype	Hardware address type = 1 for 10mb Ethernet
		hlen	= 6 for 10mb Ethernet
		hops	0
		xid	selected by client
		secs	(opt.)
		flags	Set 'BROADCAST' flag if client requires broadcast reply
		ciaddr	previously allocated network address from step 13
		yiaddr	0
		siaddr	0
		giaddr	0
		chaddr	client's hardware address
		sname	options, if indicated in 'sname/file' option; otherwise unused
		file	options, if indicated in 'sname/file' option; otherwise 'generic' name or null

 © ISO/IEC – All rights reserved

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

		options	Requested IP address - MUST NOT IP address lease time - MAY Use 'file'/'sname' fields - MAY DHCP message type - DHCPREQUEST Client identifier - MAY Class identifier - SHOULD Server identifier - MUST (after DHCPDISCOVER), MUST NOT (when renewing) Parameter request list - MAY Maximum message size - MAY Message - SHOULD NOT Site-specific - MAY All others - MUST NOT See Note below See Appendix A Usually, the requested parameters will match those returned to the client in the DHCPOFFER message; however, the client may choose to request a different lease duration. Also, there is no requirement that the server cache the parameters from the DHCPOFFER message. The server must simply check that the parameters requested in the DHCPREQUEST are acceptable. If the parameters are acceptable, the server records the new client binding and returns a DHCPACK message to the client.
15 invATMARP		PC_IP	The STU extracts the PC_IP from the ciaddr in step 13 and responds to the invATMARP
16a - 16b - 16c DHCPREQUEST			the Data Forwarder now forwards any IP data received from the STU Data Port to the VPI/VCI provided in 12, including the DHCPREQUEST from 14 which is broadcast to all the DHCP servers on the ISAP network to which the DAVIC Server is connected as a DHCP relay agent.
17a - 17b - 17c - 17d DHCPACK (RFC 1541 RFC 1533)		htype	Hardware address type = 1 for 10mb Ethernet
		hlen	= 6 for 10mb Ethernet
		hops	0
		xid	'xid' from client DHCPREQUEST message step 16
		secs	0
		ciaddr	'ciaddr' from DHCPREQUEST step 16

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

		yiaddr	IP address assigned to client
		siaddr	IP address of next bootstrap server
		flags	0
		giaddr	0
		chaddr	'chaddr' from client DHCPREQUEST message step 16
		sname	Server host name or options
		file	Client boot file name or options
		options	Requested IP address -- MUST NOT IP address lease time -- MUST Use 'file'/'sname' fields - MAY DHCP message type -- DHCPACK Parameter request list - MUST NOT Message -- SHOULD Client identifier -- MUST NOT Class identifier -- MUST NOT Server identifier -- MAY Maximum message size -- MUST NOT All others -- MAY

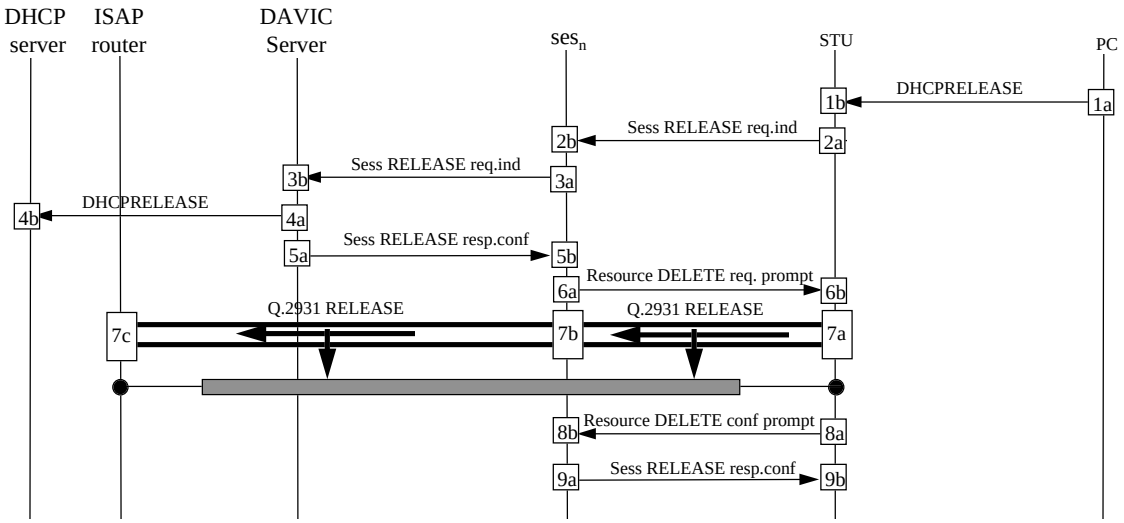


Figure 9.5-35 - Using DHCP for normal termination of an Internet Session

Table 9.5-19 – Functional Entity Actions – Initiating a session release from a PC

Graceful Release of Access to Internet	
1a – 1b:	PC sends DHCPRELEASE IP message over Ethernet

 © ISO/IEC – All rights reserved

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

2a – 2b	Upon receiving DHCPRELEASE the STU initiates a Sess RELEASE req.ind to ses_n
3a – 3b	ses_n sends Sess RELEASE req.ind to the DAVIC Server
4a – 4b	The DAVIC Server sends DHCPRELEASE as a DHCP relay agent to the DHCP server identified by the server identifier
5a – 5b	The DAVIC Server sends Sess RELEASE resp.conf to ses_n
6a – 6b	ses_n requests the STU Proxy Signaling Agent (PSA) to release the connection
7a – 7b – 7c	The connection is released between the ISAP router and the STU
8a – 8b	The PSA reports the success of connection release
9a – 9b	ses_n proceeds to send Sess RELEASE resp.conf to the STU

Table 9.5-20 - Dynamic Flow Parameters – Initiating a session release from a PC

Flow	Status	Parameters	Comments
1a-1b DHCPRELEASE		htype	Hardware address type '1' = 10mb Ethernet
		hlen	'6' for 10mb Ethernet
		hops	= 0
		xid	Transaction ID, a random number chosen by the client, used by the client and server to associate messages and responses between a client and a server
		secs	= 0
		ciaddr	IP address of the client
		yiaddr	= 0
		siaddr	= 0
		giaddr	= 0 .
		chaddr	the client's hardware address
		sname	unused
		file	unused
		options	unused
2a - 2b Sess RELEASE req.ind		session_id	identifier of the session to be released, obtained from Sess SETUP req.ind in Session & Call/Connection SetUp Scenario
		DAVIC_data	DAVIC defined DHCPRELEASE parameters *Note: Need to define format for DAVIC_data*
		reason	indicates the reason the session has been requested to be released In this case a user defined reason by DAVIC indicates that the DAVIC_data carries

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

			DHCPRELEASE parameters
3a - 3b Sess RELEASE req.ind		session_id	identical to 2
		DAVIC_data	identical to 2
		reason	identical to 2
4a - 4b DHCPRELEASE		htype	identical to 1
		hlen	identical to 1
		hops	identical to 1
		xid	identical to 1
		secs	identical to 1
		ciaddr	identical to 1
		yiaddr	identical to 1
		siaddr	identical to 1
		giaddr	DAVIC Server IP address
		chaddr	identical to 1
		sname	identical to 1
		file	identical to 1
		options	identical to 1
5a - 5b Sess RELEASE resp.conf		session_id	identical to 3=2
		response	indicates the status of the session release request
6a - 6b Resource DELETE req. prompt		session_id	identical to 5=2
		resource_#s	identifies the resources within the session to be released
7a - 7b - 7c			the ATM SVC connection is released
8a - 8b Resource DELETE conf. prompt		session_id	identical to 6=2
		status	indicates success or failure
5a - 5b Sess RELEASE resp.conf		session_id	identical to 5=2

 © ISO/IEC – All rights reserved

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

		response	identical to 5=2

9.5.12 DHCP Options for Internet Access

All Subnets are Local Option:

This option specifies whether or not the client may assume that all subnets of the IP network to which the client is connected use the same MTU as the subnet of that network to which the client is directly connected. A value of 1 indicates that all subnets share the same MTU. A value of 0 means that the client should assume that some subnets of the directly connected network may have smaller MTUs.

ARP Cache Timeout Option:

This option specifies the timeout in seconds for ARP cache entries. The time is specified as a 32-bit unsigned integer.

Boot File Size Option:

This option specifies the length in 512-octet blocks of the default boot image for the client. The file length is specified as an unsigned 16-bit integer.

Broadcast Address Option:

This option specifies the broadcast address in use on the client's subnet.

Class-identifier:

This option is used by DHCP clients to optionally identify the type and configuration of a DHCP client. The information is a string of n octets, interpreted by servers. Vendors and sites may choose to define specific class identifiers to convey particular configuration or other identification information about a client. For example, the identifier may encode the client's hardware configuration. Servers not equipped to interpret the class-specific information sent by a client MUST ignore it (although it may be reported).

Client-identifier:

This option is used by DHCP clients to specify their unique identifier. DHCP servers use this value to index their database of address bindings. This value is expected to be unique for all clients in an administrative domain. It is expected that this field will typically contain a hardware type and hardware address, but this is not required.

Cookie Server Option:

The cookie server option specifies a list of RFC 865 cookie servers available to the client. Servers SHOULD be listed in order of preference.

DHCP Message Type:

This option is used to convey the type of the DHCP message.

Domain Name:

This option specifies the domain name that client should use when resolving host names via the Domain Name System.

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Domain Name Server Option:

The domain name server option specifies a list of Domain Name System (STD 13, RFC 1035) name servers available to the client. Servers SHOULD be listed in order of preference.

Default IP Time-to-live:

This option specifies the default time-to-live that the client should use on outgoing datagrams. The TTL is specified as an octet with a value between 1 and 255.

Ethernet Encapsulation Option:

This option specifies whether or not the client should use Ethernet Version 2 (RFC 894) or IEEE 802.3 (RFC 1042) encapsulation if the interface is an Ethernet. A value of 0 indicates that the client should use RFC 894 encapsulation. A value of 1 means that the client should use RFC 1042 encapsulation.

Extensions Path:

A string to specify a file, retrievable via TFTP, which contains information which can be interpreted in the same way as the 64-octet vendor-extension field within the BOOTP response, with the following exceptions:

- the length of the file is unconstrained;

- all references to Tag 18 (i.e., instances of the BOOTP Extensions Path field) within the file are ignored.

Host Name Option:

This option specifies the name of the client. The name may or may not be qualified with the local domain name. See RFC 1035 for character set restrictions.

Impress Server Option:

The Impress server option specifies a list of Imagen Impress servers available to the client. Servers SHOULD be listed in order of preference.

Interface MTU Option:

This option specifies the MTU to use on this interface. The MTU is specified as a 16-bit unsigned integer. The minimum legal value for the MTU is 68.

IP Address Lease Time:

A DHCP server uses this option to specify the lease time it is willing to offer. The time is in units of seconds, and is specified as a 32-bit unsigned integer.

This option is also used to allow the client to request a lease time for the IP address. The time is in units of seconds, and is specified as a 32-bit unsigned integer.

IP Forwarding Enable/Disable Option:

This option specifies whether the client should configure its IP layer for packet forwarding. A value of 0 means disable IP forwarding, and a value of 1 means enable IP forwarding.

Log Server Option:

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

The log server option specifies a list of MIT-LCS UDP log servers available to the client. Servers SHOULD be listed in order of preference.

LPR Server Option;

The LPR server option specifies a list of RFC 1179 line printer servers available to the client. Servers SHOULD be listed in order of preference.

Mask Supplier Option:

This option specifies whether or not the client should respond to subnet mask requests using ICMP. A value of 0 indicates that the client should not respond. A value of 1 means that the client should respond.

Maximum Datagram Reassembly Size;

This option specifies the maximum size datagram that the client should be prepared to reassemble. The size is specified as a 16-bit unsigned integer. The minimum value legal value is 576.

Maximum DHCP Message Size:

This option specifies the maximum length DHCP message that it is willing to accept. The length is specified as an unsigned 16-bit integer.

Note: The MTU depends on the Dataport protocol being used e.g., 10BaseT or 1394

Merit Dump File:

This option specifies the path-name of a file to which the client's core image should be dumped in the event the client crashes. The path is formatted as a character string consisting of characters from the NVT ASCII character set.

Name Server Option:

The name server option specifies a list of IEN 116 name servers available to the client. Servers SHOULD be listed in order of preference.

NetBIOS over TCP/IP Name Server Option:

The NetBIOS name server (NBNS) option specifies a list of RFC 1001/1002. NBNS name servers listed in order of preference.

NetBIOS over TCP/IP Datagram Distribution Server Option;

The NetBIOS datagram distribution server (NBDD) option specifies a list of RFC 1001/1002 NBDD servers listed in order of preference. The code for this option is 45. The minimum length of the option is 4 octets, and the length must always be a multiple of 4.

NetBIOS over TCP/IP Node Type Option:

The NetBIOS node type option allows NetBIOS over TCP/IP clients which are configurable to be configured as described in RFC 1001/1002.

NetBIOS over TCP/IP Scope Option:

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

The NetBIOS scope option specifies the NetBIOS over TCP/IP scope parameter for the client as specified in RFC 1001/1002.

Network Information Servers Option:

This option specifies a list of IP addresses indicating NIS servers available to the client. Servers SHOULD be listed in order of preference.

Network Information Service Domain Option:

This option specifies the name of the client's NIS domain. The domain is formatted as a character string consisting of characters from the NVT ASCII character set.

Network Time Protocol Servers Option:

This option specifies a list of IP addresses indicating NTP servers available to the client. Servers SHOULD be listed in order of preference

Non-Local Source Routing Enable/Disable Option:

This option specifies whether the client should configure its IP layer to allow forwarding of datagrams with non-local source routes. A value of 0 means disallow forwarding of such datagrams, and a value of 1 means allow forwarding.

Option Overload:

This option is used to indicate that the DHCP "sname" or "file" fields are being overloaded by using them to carry DHCP options. A DHCP server inserts this option if the returned parameters will exceed the usual space allotted for options. If this option is present, the client interprets the specified additional fields after it concludes interpretation of the standard option fields.

Parameter Request List;

This option is used by a DHCP client to request values for specified configuration parameters. The list of requested parameters is specified as n octets, where each octet is a valid DHCP option code as defined in this document. The client MAY list the options in order of preference. The DHCP server is not required to return the options in the requested order, but MUST try to insert the requested options in the order requested by the client.

Path MTU Aging Timeout Option:

This option specifies the timeout (in seconds) to use when aging Path MTU values discovered by the mechanism defined in RFC 1191 [12]. The timeout is specified as a 32-bit unsigned integer.

Path MTU Plateau Table Option:

This option specifies a table of MTU sizes to use when performing Path MTU Discovery as defined in RFC 1191. The table is formatted as a list of 16-bit unsigned integers, ordered from smallest to largest. The minimum MTU value cannot be smaller than 68.

Perform Mask Discovery Option:

This option specifies whether or not the client should perform subnet mask discovery using ICMP. A value of 0 indicates that the client should not perform mask discovery. A value of 1 means that the client should perform mask discovery

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Perform Router Discovery Option:

This option specifies whether or not the client should solicit routers using the Router Discovery mechanism defined in RFC 1256 [13]. A value of 0 indicates that the client should not perform router discovery. A value of 1 means that the client should perform router discovery.

Policy Filter Option:

This option specifies policy filters for non-local source routing. The filters consist of a list of IP addresses and masks which specify destination/mask pairs with which to filter incoming source routes. Any source routed datagram whose next-hop address does not match one of the filters should be discarded by the client.

Rebinding (T2) Time Value:

This option specifies the time interval from address assignment until the client transitions to the REBINDING state. The value is in units of seconds, and is specified as a 32-bit unsigned integer.

Renewal (T1) Time Value:

This option specifies the time interval from address assignment until the client transitions to the RENEWING state. The value is in units of seconds, and is specified as a 32-bit unsigned integer.

Requested IP Address:

This option is used to allow the client to request that a particular IP address be assigned.

Resource Location Server Option:

This option specifies a list of RFC 887 Resource Location servers available to the client. Servers SHOULD be listed in order of preference.

Root Path:

This option specifies the path-name that contains the client's root disk. The path is formatted as a character string consisting of characters from the NVT ASCII character set.

Router Option:

The router option specifies a list of IP addresses for routers on the client's subnet. Routers SHOULD be listed in order of preference.

Router Solicitation Address Option:

This option specifies the address to which the client should transmit router solicitation requests.

Server Identifier:

DHCP servers include this option in the DHCPOFFER in order to allow the client to distinguish between lease offers. The identifier is the IP address of the selected server.

Also, DHCP clients indicate which of several lease offers is being accepted by including this option in a DHCPREQUEST message. The identifier is the IP address of the selected server.

Static Route Option:

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

This option specifies a list of static routes that the client should install in its routing cache. If multiple routes to the same destination are specified, they are listed in descending order of priority. The routes consist of a list of IP address pairs. The first address is the destination address, and the second address is the router for the destination. The default route (0.0.0.0) is an illegal destination for a static route.

Subnet Mask:

The subnet mask option specifies the client's subnet mask as per RFC 950

Swap Server:

This specifies the IP address of the client's swap server.

TCP Default TTL Option:

This option specifies the default TTL that the client should use when sending TCP segments. The value is represented as an 8-bit unsigned integer. The minimum value is 1.

TCP Keepalive Interval Option:

This option specifies the interval (in seconds) that the client TCP should wait before sending a keepalive message on a TCP connection. The time is specified as a 32-bit unsigned integer. A value of zero indicates that the client should not generate keepalive messages on connections unless specifically requested by an application.

TCP Keepalive Garbage Option:

This option specifies the whether or not the client should send TCP keepalive messages with an octet of garbage for compatibility with older implementations. A value of 0 indicates that a garbage octet should not be sent. A value of 1 indicates that a garbage octet should be sent.

Time Offset:

The time offset field specifies the offset of the client's subnet in seconds from Coordinated Universal Time (UTC). The offset is expressed as a signed 32-bit integer.

Time Server Option:

The time server option specifies a list of RFC 868 time servers available to the client. Servers SHOULD be listed in order of preference.

Trailer Encapsulation Option:

This option specifies whether or not the client should negotiate the use of trailers (RFC 893) when using the ARP protocol. A value of 0 indicates that the client should not attempt to use trailers. A value of 1 means that the client should attempt to use trailers.

Vendor Specific Information:

This option is used for vendor-specific information. In case of clients, the information is an opaque object of n octets, presumably interpreted by vendor-specific code on the clients. The definition of this information is vendor specific. The vendor is indicated in the class-identifier option. Clients which do not receive desired vendor-specific information SHOULD make an attempt to operate without it, although they may do so (and announce they are doing so) in a degraded mode. In case of servers the information is an opaque object of n octets, presumably interpreted by vendor-specific code on the servers. The definition of this information is

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

vendor specific. The vendor is indicated in the class-identifier option. Servers not equipped to interpret the vendor-specific information sent by a client MUST ignore it (although it may be reported)

X Window System Font Server Option:

This option specifies a list of X Window System Font servers available to the client. Servers SHOULD be listed in order of preference.

X Window System Display Manager Option:

This option specifies a list of IP addresses of systems that are running the X Window System Display Manager and are available to the client. Addresses SHOULD be listed in order of preference.

9.5.13 DAVIC Defined Resource Descriptors for Internet Access

9.5.13.1 Interactive Broadcast Descriptor

The Interactive Broadcast descriptor covers the following modes:

1 = with MPEG TS and PSTN/NISDN/PLMN Downstream and PSTN/NISDN/PLMN Upstream

2 = with MPEG TS Downstream and PSTN/NISDN/PLMN Upstream

3 = PSTN/NISDN/PLMN Downstream and Upstream

9.5.13.2 The DhcpOffer descriptor covers the following parameters (RFC 1541 RFC 1533):

Table 9.5-21

htype	Hardware address type = 1 for 10mb Ethernet
hlen	= 6 for 10mb Ethernet
hops	= 0
xid	Transaction ID, a random number chosen by the client, used by the client and server to associate messages and responses between a client and a server
secs	= 0
ciaddr	= 0
yiaddr	IP address offered to client
siaddr	IP address of next bootstrap server
flags	if 'giaddr' is not 0 then 'flags' from client message else 0
chaddr	identical to 4=1
giaddr	identical to 4
sname	Server host name or options
file	Client boot file name or options
options	Requested IP address - MUST NOT IP address lease time - MUST

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

	Use 'file'/'sname' fields - MAY DHCP message type - DHCPOFFER Parameter request list - MUST NOT Message - SHOULD Client identifier - MUST NOT Class identifier - MUST NOT Server identifier - MUST Maximum message size - MUST NOT All others - MAY

10 Configuration

10.1 General

This section describes configuration and initialization behavior for both STU Boot and Service (i.e., Server) Boot. Figure 10.1-1 provides an overview of the flows for interface initialization. It illustrates the relationships between the initial A0 flows, the DIIP flows, and finally, the DSM-CC UN Configuration flows.

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

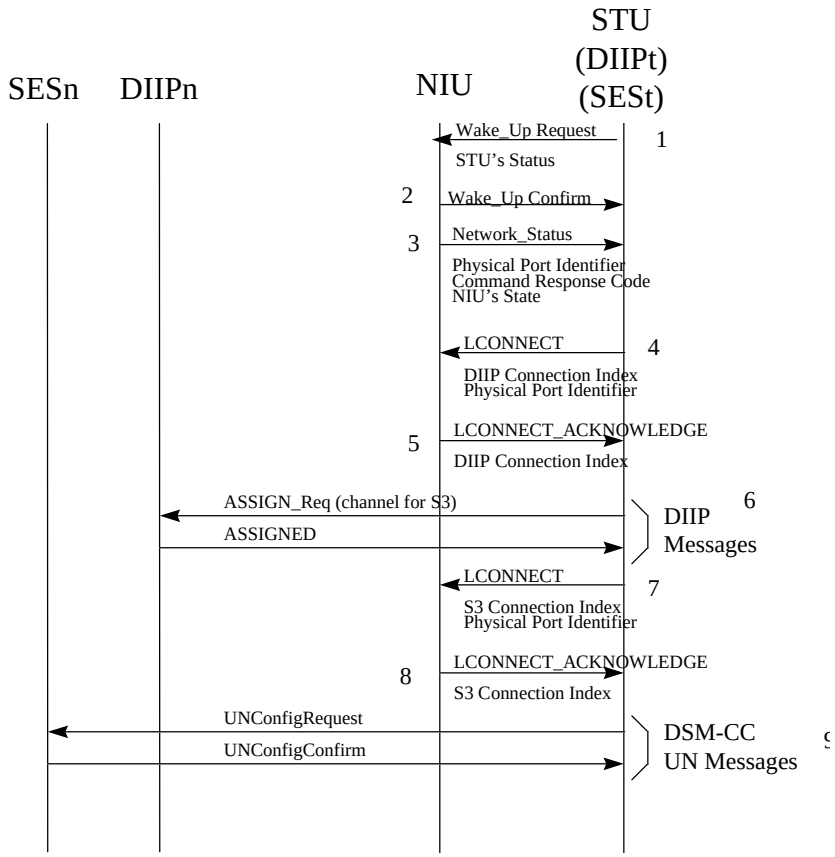


Figure 10.1-1

Note: Figure 10.1-1 shows the case when a PVC is used to carry the S3 flow (DSMCC U-N message). When an SVC is used to carry the S3 flow, Q.2931 is required to establish the S3 channel.

10.2 STU Configuration (Boot)

Before starting establishment, the STU shall meet the following preconditions:

- The STU has an assigned channel with the SESn for session control signaling.
- The STU knows its clientId.
- The STU knows the serverId assigned to the server to be connected with.
- The STU knows the following input parameters of DSM ServiceGateway attach:
- rPathSpec
- rClientRef
- rClientProfile
- aEndUser

The complete specification for a method of meeting the above preconditions is not specified in this DAVIC Specification. However, in order to facilitate the future specification, the Specification requires the use of DSM-CC U-N configuration protocol. The appropriate DSM-CC parameters will be set as follows:

- sessionIdAssign or in dsmccConfigurationParameters shall be 1.
- resourceIdAssign or in dsmccConfigurationParameters shall be 1.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

- serverId in networkConfigurationParameters() shall indicate the server with which the STU performs any download which may be required subsequent to the DSM-CC U-N configuration, such as O.S. updates.
- networkParameter DataBytes in ConfigurationParameters() in UnConfigurationConfirm shall follow the syntax as specified in Table 10.2-1.

Table 10.2-1 - Syntax for networkParameters (networkParameterDataBytes)

Syntax	*Number of Bytes*

networkParameters(){
numberingPlanIndicator
/* the rest of this field is not specified in this Specification */
}
	1

ClientId and serverId are based on the E.164 NSAP. The ClientId E.164 NSAP address HO-DSP contains the IP address used in setting the TCP connection for the S2 information flow. However, for end-to-end communication that traverses the public ATM network, routing in the public ATM network (the called number) may be based on either native E.164 (ISDN numbering plan) or E.164 NSAP. The actual method will be assigned by the network provider using the DSM-CC U-N configuration protocol. To accommodate this function, DAVIC stipulates the DSM-CC U-N configuration protocol will contain the numberingPlanIndicator parameter, as defined in Table 10.2-2, in the networkConfigurationParameters() data bytes.

Table 10.2-2 - Values for numberingPlanIndicator

numberingPlan	*Value*
reserved	0x00
ISDN numbering plan (E.164 Native)	0x01
E.164 NSAP	0x02
reserved	0x03–0xff

The transport mechanism of DSM-CC U-N configuration messages depends on the underlying network and is not specified in this Specification.

10.3 Service Provider System Configuration

The discussion presents the service configuration phase. The configuration phase is the exchange between the Session Gateway, which resides in the Service Domain, and the Session & Resource Manager, which resides in the network. (Note: The SRM (Session & Resource Manager) is not a DAVIC entity, but rather a term used in the DSM-CC specification. It corresponds to the ses(n) entity of this specification for the case of Physical Instance #1 where this entity is located in the access network. This specification refers to the element which terminates the session protocol on the service side as the ses(t) and the element which terminates the session protocol on the network side as the ses(n).)

The solution is the configuration protocol of the Digital Storage Media Command & Control initiative. The discussion visualizes the element which implements the configuration protocol and the element which implements the session protocol as distinct elements. It is thought that there is private interface between the configuration element and the session element on the service side. It is thought that there is private interface between the configuration element and the session element on the network side. In both cases the session element forwards values to the configuration element before the configuration phase, and the configuration element returns values to the session element after the configuration phase. The specification of the interactions, however, is out of scope.

The configuration element on the service side understands the network address to associate with the configuration element on the network side through convention. The configuration element on the service side initiates the exchange. The data which it provides in the first message is:

- Configuration Network Address: This is the network address to which the DSM-CC network shall send DSM-CC U-N configuration messages.

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

- Session Network Address: This is the network address to which the DSM-CC network shall send DSM-CC U-N session messages.
- Session Profile: The session profile shall indicate the subset of DSM-CC U-N session primitives supported by the server.
- Resource Profile: The resource profile shall indicate the subset of DSM-CC U-N resources that the server expects the network to provision for a service.
- Default Service: The default service is defined as the service to be selected if the set-top does not indicate the desired service during the DSM-CC U-N session establishment.
- Default Service Profile: Just as the settop can provide a client profile which articulates features which affect interpretation, it is thought a service could provide a service profile which articulates features which affect interpretation. (The field is optional. The Digital Storage Media Command & Control initiative does not describe the field. It is a placeholder which empowers a proactive network to present services known to be interoperable.)

The configuration code on the network side returns the data shown below. It initializes the context of the ses(t) element (also known as the Session Gateway) in the service domain.

- Session & Resource Manager Network Address: The configuration phase initializes the network address to which the service side will send session protocol. It is E.164 NSAP.
- Session Profile: The profile identifies the subset of the session protocol which the Session & Resource Manager supports.
- Resource Profile: The profile identifies the resources which the Session & Resource Manager can allocate for a service. The data includes the type field of the resource descriptor.
- Resource Allocation Option: There are two options. The service can provision network resources and inform the network, or the service can request that the network establish network resources on its behalf.
- SessionId Option: The SessionId is a unique value which identifies a session. The Session & Resource Manager instructs the ses(t) element as to whether it is to assign the value.
- Maximum Session Forward Count: The protocol which relates to session forward includes a count which increments with each attempt to forward the session. This is the maximum count.
- Maximum Message Retry Count: The session elements resend a message up to this count. (See the Digital Storage Media Command & Control specification for the state machine.)
- Message Timeout. The session protocol elements resend a message if the response does not arrive before the timeout.

10.4 Download

10.4.1 General

In DAVIC, download refers to the function of transferring data objects from a server to an STU. There are four possible methods for downloading this information:

- Download control messages piggybacked on the Sess SETUP req.ind and Sess SETUP resp.conf as user-to-user data and Download data and Download data response over asymmetrical connection with Download data carried over S1 in downstream (not necessarily using MPEG TS) and Download response over S2 in upstream. The MPEG TS is used when operating with level “A” A0 interface if such a connection is created at the outset otherwise the speed for download data for level “A” A0 interface is limited to 2.048 Mbit/s.
- Download control messages over a connection for S2 flows and Download data and Download data response over asymmetrical connection with Download data carried over S1 in downstream (not necessarily using MPEG TS) and Download response over S2 in upstream. This method is used during an active session. The MPEG TS is used when operating with level “A” A0 interface.
- Download control messages, Download data and Download data response over asymmetrical connection with the downstream portion of the Download control and the Download data carried over S1 in downstream using MPEG TS and the upstream portion of the Download control and the Download response carried over S2 in upstream This method is used during an active session and with level “A” A0 interface.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

- Download carousel over S1 with no control messages. This method is used when there is no bi-directional S2 path.

The DSM-CC download protocol shall be used to perform download. This protocol is defined in ISO/IEC13818-6. The method used for download shall be chosen by the down load service which performs the download of data to the STU (based on the STU capabilities and the established connections).

10.4.2 The Download service:

The download service covers both functions of control and data transfer and is shown at the tops of Table 10.4-1 and Table 10.4-2.

10.4.3 Download System Dynamic Flows

There are two instances of download operations within a session: 1) download occurs at session set-up, and 2) download occurs part way though the session. In the following, both of those instances are described.

10.4.4 Download initiated at session setup:

Figure 10.4-1 shows the case of a download initiated at session setup. When download is being initiated at session setup the control information is carried as part of the session SETUP req.ind flow [1]. Therefore, there is no requirement for a connection to carry Download control messages . In contrast, a connection is needed to carry Download data downstream and Download data response upstream. Table 10.4-1 shows the Download functional entity actions.

Table 10.4-1 - Download initiated at session set-up

1a–1b	The download service is active
2a–2b	The STU sends a session set-up request indication to the network. This contains the download request and compatibility information to be carried user-to-user.
2b-2c	The network sends a session set-up request indication to the Server. This contains the download request and compatibility information to be carried user-to-user.
3a–3b	The download service is given the download request parameters.
4a–4b	The download service provides the download response parameters.
5a–5b	A connection is requested with a bandwidth appropriate for Download data
An end-to-end connection is established to carry the download data.	
6a–6b 7a–7b	Optional Resource ADD req.ind used for PVC when Sesn is does the resource allocation.
8a–8b	The Server sends a session set-up response confirm to the network carrying the download response as user-to-user information.
8b–8c	The network sends a session set-up response confirm to the STU carrying the download response as user-to-user information.
9a–9b	The download parameters are passed to the download service.
10a–10b	The STU requests start of data download.
11(1-n)a– 11(1-n)b	Server downloads the data blocks.
12a–12b	As negotiated in 4a–4b and 6a–6b, after a number of download blocks the STU sends an Ack message.

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

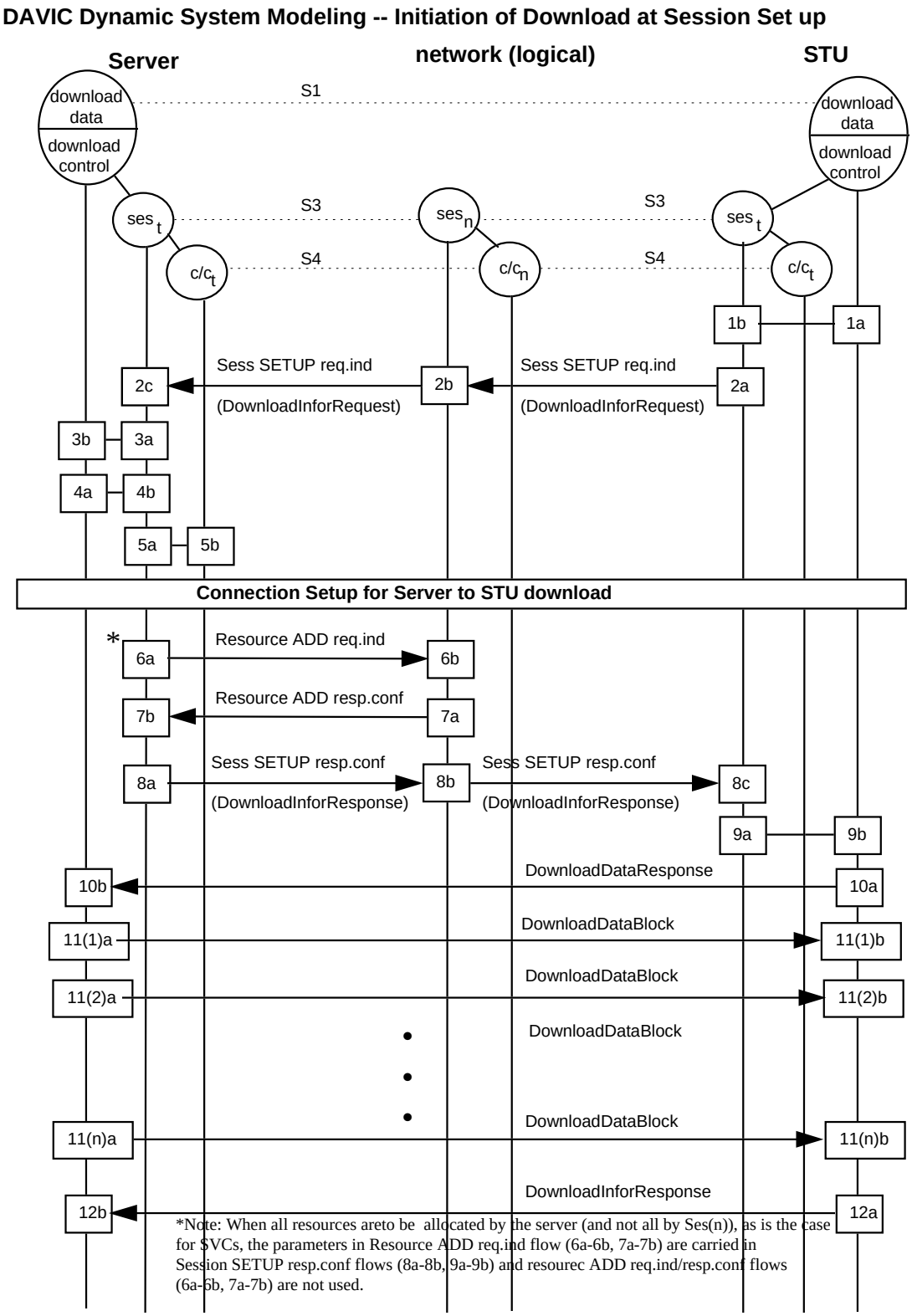


Figure 10.4-1 - Download initiated at session setup

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

10.4.5 Download initiated during active session:

Figure 10.4-2 shows the case when download is initiated during active session. In contrast to Figure 10.4-1, connections are required both for control flow (S2) and for Download data and Download data response (S1). In this case the download server may prompt the STU to begin the process of download, however this is optional because it depends on the logic of the application running on the client. The process then continues as in Figure 10.4-1. However the Download info request and reply are no longer piggy backed on the Sess SETUP req.ind and Sess SETUP resp.conf. Table 10.4-2 shows the Download functional entity actions.

Table 10.4-2 - Download initiated post session set-up

1a–1b	User chooses a new service or application
End-to-end connections are established if required to carry the Download control, Download data and Download data response, otherwise existing connections are reused. Note: It may be required to rebind the connection for control and data. This information must be passed between the Service Gateways (Serv gwy) at both the Server and the STU using the RPC (S2) and not the user-to-user field in the resource ADD flows. Doing so covers the case if a connection is reused and new resource ADD flows are not required to be sent.	
2a–2b	The download service is initiated by the server (optional) and the connection bindings are provided for the Download Service.
3a–3b	The download service is given the signal to proceed.
4a–4b	The STU sends download request to the server.
5a–5b	The download parameters are passed from the server to the STU download service.
6a–6b	The STU requests start of data download.
7(1-n)a–7(1-n)b	Server downloads the data blocks.
8a–8b	As negotiated in 6a–6b after a number of download blocks the STU sends an Ack message.

 © ISO/IEC – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

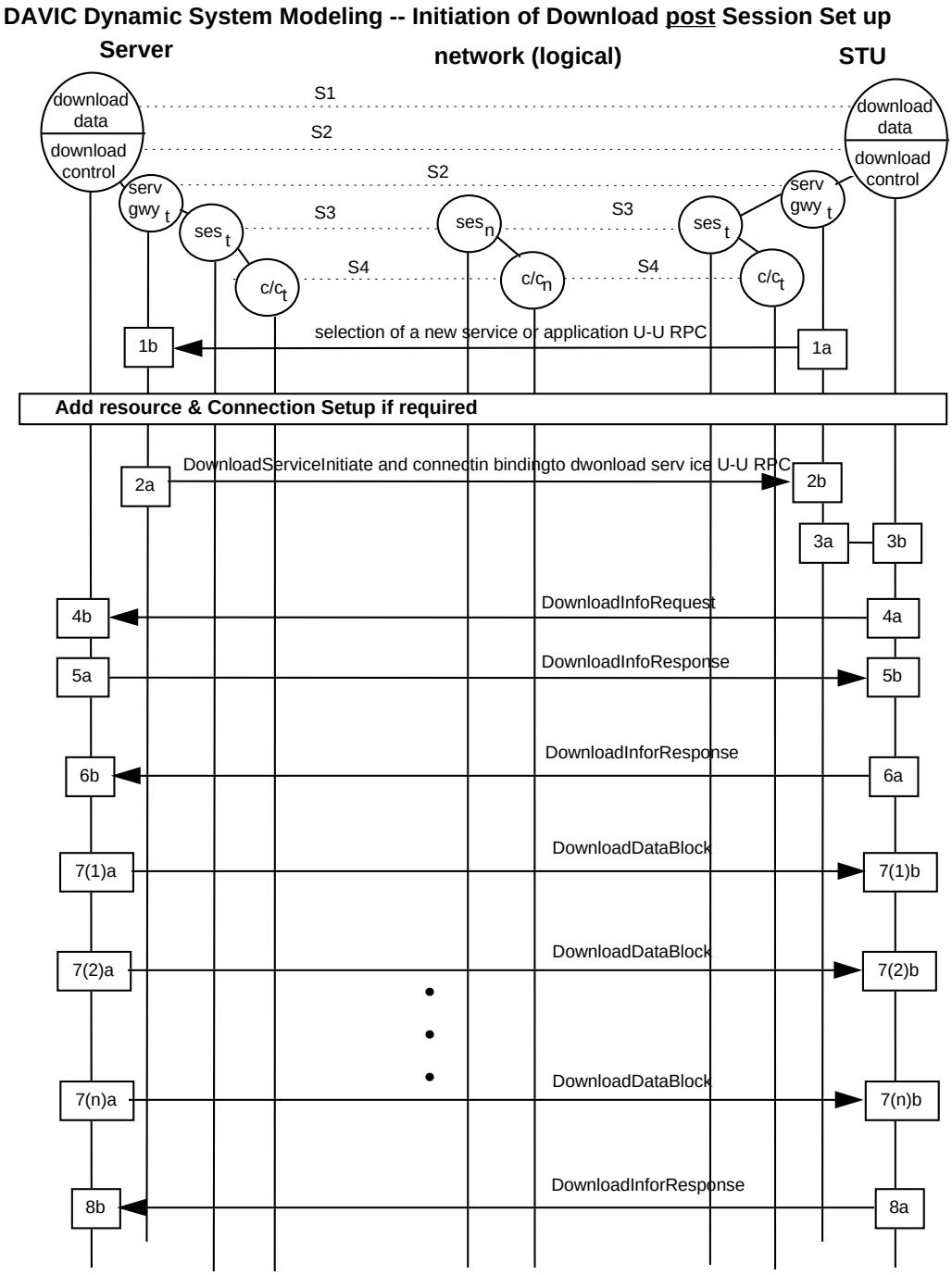


Figure 10.4-2 - Download initiated post session setup

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ICS 35.040

Price based on 166 pages

© ISO/IEC 1999 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale