



DAVIC 1.5 Specification

DAVIC Intranet

**Technical Platform Specification
(Provisional Document Structure)**

Revision 1.0

NOTICE

Use of the technologies described in this specification may infringe patents, copyrights or intellectual property rights of DAVIC Members or non-members.

This DAVIC 1.5 Specification is subject to change without notice.

Neither DAVIC nor any of its Members accept any responsibility whatsoever for damages or liability, direct or consequential, which may result from use of this specification.

This revision 1.0 of the DAVIC 1.5 Specification [DAVIC Intranet](#) document supersedes all previous versions.

© Digital Audio-Visual Council 1999.

Published by Digital Audio-Visual Council

Geneva, Switzerland

CONTENTS

1	SCOPE.....	VII
2	REFERENCES	VIII
2.1	NORMATIVE REFERENCES	VIII
2.2	INFORMATIVE REFERENCES	VIII
3	DEFINITIONS.....	IX
3.1	CLARIFICATION OF IP TERMS	IX
4	ACRONYMS AND ABBREVIATIONS.....	X
5	CONVENTIONS	XII
6	INTRODUCTION	1
7	REQUIREMENTS	2
7.1	GENERAL REQUIREMENTS	2
7.1.1	<i>Scalability</i>	2
7.1.2	<i>Pragmatism</i>	2
7.1.3	<i>Architecture flexibility</i>	2
7.1.4	<i>Multiple Client support</i>	2
7.1.5	<i>Multiple service platform</i>	2
7.1.6	<i>Billing and accounting</i>	2
7.1.7	<i>Security</i>	3
7.1.8	<i>Regulatory issues</i>	3
8	ARCHITECTURE	4
8.1	THE DAVIC INTRANET ARCHITECTURE	4
8.2	DAVIC VALUE-ADD	5
9	ADDRESSING AND NAMING	7
9.1.1	<i>Addressing Homogeneity</i>	7
9.1.2	<i>Global Addressing</i>	7
9.1.3	<i>Private Addressing</i>	7
10	NETWORK SUPPORT	8
10.1	FRAMEWORK FOR ACCESS NETWORKS.....	8
10.2	CORE NETWORKS	8
10.2.1	<i>Layer 2</i>	8
10.2.2	<i>Routing</i>	8
10.2.3	<i>Interior Routing Protocols</i>	8
10.2.4	<i>Exterior Routing Protocols</i>	9
11	MULTICAST.....	10
11.1	MULTICAST CLIENTS.....	10
11.2	MULTICAST SERVERS.....	10
11.3	DELIVERY SYSTEM.....	10
11.3.1	<i>Group Management</i>	10
11.3.2	<i>Multicast Routing Protocol</i>	10
12	QUALITY OF SERVICE	12
12.1	DIFFERENTIATED SERVICES (DIFF-SERV).....	12
12.2	RSVP PROTOCOL.....	12
12.3	JITTER	12
13	TRANSPORT	13
13.1	RTP AND RTCP	13

13.2	HTTP	13
14	SESSION DESCRIPTION AND CONTROL	14
14.1	SDP	14
14.2	RTSP	14
15	SERVICE LOCATION CAPABILITY	15
15.1	SLP	15
16	DYNAMIC FLOW DIAGRAMS FOR TV ANYWHERE AND TV ANYTIME	16
16.1	LOCAL STORAGE DISCOVERY	16
16.2	UNICAST (1-TO-1) REAL TIME	17
16.3	MULTICAST 1-TO-MANY, REAL TIME	20
16.4	EXAMPLE USAGE OF LOCAL SERVER	21
ANNEX A	: ACCESS AND HOME NETWORK TECHNOLOGY FRAMEWORK	22
A.2	HOME NETWORKS	22
A.2.1	<i>Point to Point HNs</i>	22
A.2.2	<i>Broadcast HNs</i>	23
A.3	ACCESS NETWORKS	23
A.3.1	<i>Point to Point</i>	23
A.3.2	<i>Bi-directional Broadcast</i>	23
A.3.3	<i>Unidirectional Broadcast with Back-channel</i>	23
A.4	SYSTEM FRAMEWORK	24
A.4.1	<i>Point to Point Access - Point to Point HN</i>	24
A.4.2	<i>Point to Point Access - Broadcast HN</i>	24
A.4.3	<i>Uni-directional Broadcast plus back-channel Access - Point to Point HN</i>	25
A.4.4	<i>Uni-directional Broadcast plus back-channel Access - Point to Point HN</i>	26
A.4.5	<i>Bi-directional Broadcast Access - Broadcast or Point to Point HN</i>	26
ANNEX B	: TABLE OF NORMATIVE TECHNOLOGIES	27

Foreword

About This Specification

This document contains the Technical Platform Specification for *DAVIC Intranet*.

It contains the necessary specifications to ensure service quality required for videoservices over IP based networks. The name of DAVIC Intranet comes from the fact that these specifications allow the building of islands that can be interconnected through adequate means, not using the generalInternet network for this interconnection since this cannot guarantee the QoS obtained on this Intranet..

1. Scope

This specification describes an Intranet implementation with common IETF tools. The DAVIC Intranet is defined as the system that exists between the Network and Transport Layers and therefore does not describe higher layer functionality such as the application programming interfaces. Protocols for the User and Control planes are described, however, the Management Plane is not covered. The focus of the specification is on the use of tools on the IP-layer and directly above. This includes items like stream control, routing protocol and service location protocols. It describes the use of a DAVIC Intranet for a range of applications, including the TV Anytime and TV Anywhere scenarios defined in the corresponding Document (TV AnyTime and Anywhere) It also describes the location and use of local storage devices in the DAVIC Intranet.. The applicability of the Intranet for TV Anytime and Anywhere is described in a companion document.

The specification is relevant for implementing a complete Intranet with the following features:

- The mandated use of IP multicasting tools for delivery of services on a one-to-many basis,
- The mandated use of real-time transport protocols for delivery of media streams,
- The mandated use of control and location protocols to enable local storage of audiovisual material,
- The dynamic flows and protocol mappings to support a range of applications, including TVAnywhere and TVAnytime.
- The optional use of RSVP for reservation of resources in the DAVIC Intranet,

2. References

2.1 Normative References

RFC 1771	A Border Gateway Protocol 4 (BGP-4)
RFC 1889	RTP: A Transport Protocol for Real-Time Applications
RFC 1890	RTP Profile for Audio and Video Conferences with Minimal Control
RFC 2068	Hypertext Transfer Protocol -- HTTP/1.1
RFC 2165	Service Location Protocol
RFC 2205	Resource ReServation Protocol
RFC 2236	Internet Group Management Protocol, Version 2
RFC 2327	SDP: Session Description Protocol
RFC 2326	Real time Streaming Protocol (RTSP)
RFC 2362	Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification
RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers

2.2 Informative References

RFC 1075	Distance Vector Multicast Routing Protocol (DVMRP)
RFC 1112	Host Extensions for IP Multicasting
RFC 1584	Multicast Open Shortest Path First (MOSPF)
RFC 1633	Integrated Services in the Internet Architecture: an Overview
RFC 1918	Adress allocation for private Intranets
RFC 2208	RSVP Version 1 Applicability Statement Some Guidelines on Deployment
RFC 2209	RSVP Version 1 Message Processing Rules
RFC 2210	The Use of RSVP with IETF Integrated Services
RFC 2460	Internet Protocol, Version 6 (IPv6) Specification
RFC 2475	An Architecture for Differentiated Services
	Session Announcement Protocol – IETF Work in Progress
	Session Initiation Protocol – IETF Work in Progress
	Protocol Independent Multicast : Dense Mode – IETF Work in Progress
	DAVIC 1.5 Jitter concealment tools Specification

3. Definitions

3.1 Clarification of IP terms

internet: An internet is a network of networks which are glued together using IP.

Internet: The Internet is an undimensioned, uncontrolled implementation of TCP/IP over any combination of type's of bandwidth provision technology.

Intranet: An Intranet is a dimensioned, controlled version of an internet which uses the IP protocol suite and is Internet compliant. It is an Intranet because it is under one administrative domain - and designed by one system design team. It neither implies a limited size, a corporate network, or non-Internet compliance.

DAVIC Intranet: The DAVIC Intranet is a fully Internet compliant system with added constraints and features which are defined by DAVIC.

Globally Registered IP Address (or global address) : These are addresses routable in the Public (Global) Internet. Today's Internet uses version 4 of the Internet Protocol (IPv4) which provides 32 bits for network layer addressing

Private Addresses: The address space available for private use. This means that private networks (disconnected) from the Internet can use the private address space. More than one private networks can use the same private address space as long as they are not connected between them nor with the Internet.

Network Address Translation (NAT): This is a function that attempts to overcome the limitations introduced by the use of private address space. Address Translation can be used in order to interconnect a network that uses private address space with the Internet. While address translation is addressing a real problem, its use bring so many limitations to the network that uses it that their use should be avoided when possible.

4. Acronyms and Abbreviations

The following acronyms and abbreviations are used in this specification:

ARP	Address Resolution Protocol
AS	Autonomous Systems
ATM	Asynchronous Transfer Mode
ATM PVC	Asynchronous Transfer Mode Permanent Virtual Circuit
ATM SVC	Asynchronous Transfer Mode Switched Virtual Circuit
BGP	Border Gateway Protocol
DI	Davic Intranet
DHCP	Dynamic Host Configuration Protocol
Diff-Serv	Differentiated Services
DVB	Digital Video Broadcasting
DVMRP	Distance Vector Multicast Routing Protocol - RFC 1075
EDB	Enhanced Digital Broadcast
FR	Frame Relay
FTTH	Fiber To The Home
GSM	Global System Mobile
HAN	Home Area Network
HE	Head End
HN	Home Network
HTTP	HyperText Transport Protocol
IETF	Internet Engineering Task Force
IGMP	Internet Group Membership Protocol - RFC 1112
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6 (IP New Generation)
IPCDN	Internet Protocol Cable Data Networks
ISDN	Integrated Services Digital Network
ISO	International Standardization Organization
ISP	Internet Service Provider
ITU	International Telecommunications Union
L2TP	Layer 2 Transport Protocol
LAN	Local Area Network
LS	Local Server
MAC	Medium Access Control
MM	Multimedia
MOSPF	Multicast Open Shortest Path First - RFC 1584
MPEG	Moving Pictures Expert Group

DAVIC Intranet

MPLS	MultiProtocol Label Switching
NAT	Network Address Translation
NC	Network Computer
NT	Network Termination
OSPF	Open Shortest Path First
PC	Personal Computer
PDA	Personal Digital Assistant
PDH	Plesiosynchronous Digital Hierarchy
PHB	Per-Hop Behavior
PIM	Protocol Independent Multicast - RFC 2117
PIM-DM	Protocol Independent Multicast – Dense Mode
PIM-SM	Protocol Independent Multicast – Sparse Mode
POTS	Plain Old Telephone Service
PPP	Point to Point Protocol
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RPM	Reverse Path Multicasting
RS	Remote Server
RSVP	Resource reSerVation Protocol
RTCP	Real Time Control Protocol
RTP	Real-time Transport Protocol
RTSP	Real-Time Stream control Protocol
SA	Service Announcement
SAP	Session Announcement Protocol
SDH	Synchronous Digital Hierarchy
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SLP	Service Location Protocol
SReq	Service Request
TCP	Transport Control Protocol
TOS	Type of Service
TV	Television
URL	Uniform Resource Locator
VCR	Video Cassette Recorder
VLAN	Virtual Local Access Network
WAN	Wide Area Network
WWW	World Wide Web

5. Conventions

The style of this Specification 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. Introduction

The DAVIC Intranet is being designed to alleviate some of the restrictions that are valid in the current Internet. Coherence in terms of dimensioning, resource allocation, prioritization and commercial models is something that is desirable but not found in the Internet today. Examples of this added value of the DAVIC Intranet are, for example, Quality of Service (QoS) support inside and between DAVIC Intranets, multicast distribution and replication policy, security and management functions. The DAVIC Intranet should enable network providers, manufacturers, service operators and content providers with a way of delivering services that are predictable, manageable and economically feasible.

This specification will describe what the current DAVIC 1.5 Intranet system looks like, what features it has, what the limitations are and how it can be used to support, for example, the 'TV Anywhere' and 'TV Anytime' scenarios that are being defined for DAVIC 1.5. A prior knowledge of IETF protocols is assumed.

In chapter 7, the general requirements on the DAVIC Intranet are described. The architecture supporting these features is presented in chapter 8. In chapter 9, the addressing issues related with the architecture are tackled, in chapter 10 the network and routing functions are defined. In chapter 11, the quality of service functions for the DAVIC Intranet are specified. Multicast and transport of multimedia content is specified in chapters 11 and 13. Session description and service location is dealt with in chapters 14 and 15. In chapter 16 the dynamic relations between entities in the DAVIC Intranet for the TV Anytime and TV Anywhere scenarios are illustrated.

7. Requirements

7.1 General requirements

A number of requirements need to be fulfilled to make the 'DAVIC Intranet' system a success. This section will give a brief description of operator and service provider related requirements on the new DAVIC system, given the services above. The above mentioned requirements in this section will be used as part of the design parameters.

7.1.1 Scalability

Solutions for technology proposed need to be scaleable, or more than one technology needs to be chosen when scalability is not inherent in the solution. The new DAVIC Intranet must be able to run over existing and future infrastructure. This means that solutions for this technology should (if possible) run over a variety of network technologies e.g. ISDN, PSTN, xDSL, FTTH etc. There is of course an inherent quality difference of the service perceived by the user, however the chosen protocols and technology should not limit the type of infrastructure. To enable such scalability for video e.g. it may be necessary to use MPEG-4 or H.263 for the lower bit-rates and go to MPEG-2 on higher rates.

There's also the issue of scalability in numbers, DAVIC's Intranet must scale to millions of users without inherent technical difficulties.

7.1.2 Pragmatism

DAVIC solution should adhere to current (IETF) practices wherever possible. In the ideal case it has to add functionality without changing the current rules and practices in the IP-world. Specifically, DAVIC solution should utilize IETF Standard Protocols for the transport of IP packets.

7.1.3 Architecture flexibility

DAVIC's Intranet architecture needs to be flexible as to the positioning of routers, switches etc. E.g. some people might like IP-functionality in their access network, where others don't. So functionality should be physically distributable as much as possible, just like in the architecture work done for DAVIC 1.x. Also the architecture must allow for different connected DAVIC Intranets operated by different network operators.

7.1.4 Multiple Client support

In the DAVIC 1.x work, most effort on the client side was targeted at set-top based solutions connected to a television. In an IP-environment the number of clients is pluriform: there are set-tops connected to TVs, PCs, NCs, NetPC, PDAs, TV Browsers etc. Of course not all clients can access all services with their full capability, but the bare minimum should be that they can connect and have a useful exchange with a service.

7.1.5 Multiple service platform

From a network operator standpoint it is essential that the DAVIC Intranet is a platform on which an operator can build a number of services, without refitting it's entire infrastructure. The new system should support (video) telephony, multimedia (MM) retrieval services like streaming video, broadcast services and the usual Internet related data services like email, WWW-browsing etc. All these services should run on a single IP-based platform and should support guaranteed as well as relative QoS. Special consideration should be given to low-delay and low-delay variation for communicative- and video services.

7.1.6 Billing and accounting

If the option exists to have both QoS and non-guaranteed QoS services, some way of extracting information on the usage of network infrastructure needs to be done. This information must be sufficient to allow the network operator to bill for network resource usage. Billing for guaranteed QoS is essential to the success of guaranteed QoS in an IP environment.

7.1.7 Security

The DAVIC Intranet should support security functions to allow for authentication, authorization of users and encryption of content. Service providers must be able to provide secure connections to their users that may however be tapped if so required by local regulation.

7.1.8 Regulatory issues

In several domains in the world, regulations exist that impact the DAVIC Intranet. The inherent design of the DAVIC Intranet shall not be in conflict with these regulations. Some examples are:

Multiple Internet Service providers must be possible to access on an equal basis

Secure IP-traffic may have to be tapped

The DAVIC Intranet access must be open for other network providers

8. Architecture

8.1 The DAVIC Intranet Architecture

An outline of a DAVIC Intranet is shown below. It is comprised of a number of optional technical components within a single systems domain. It includes traditional DAVIC distribution networks such as ATM and MPEG WAN's, new DAVIC distribution networks such as IP over SDH and satellite, as well as Home access networks and LAN's. In addition, it includes application providers (content, third party signaling, support systems etc.) situated within the DAVIC system with both WAN and access type connectivity to support both client server and peer communications, as well as contribution systems.

Multiple, directly connected DAVIC Internets have DAVIC system interfaces defined between them such that the benefits of the system design can be exported and imported between Intranet providers, enhancing the commercial value of the DAVIC system specs. Open and flexible interfaces to non DAVIC system specifications must be supported to non-DAVIC application and service providers, Internet service providers, Internet Network Providers. It is likely that such interfaces will generally be defined by the IETF protocol component and inter-provider commercial models. The DAVIC Intranet system specs must not present barriers to the interworking and development of these interfaces. These requirements suggest that DAVIC should not adopt TCP/IP protocols developed in other standards bodies, which have not been submitted to the IETF for standardization. However, DAVIC may consider protocol specifications from outside of the IETF if they are neither direct competitors to existing IETF and Internet protocols. DAVIC may input such protocols into the IETF so that this body can decide whether the existing IETF protocols need to be updated to satisfy the DAVIC requirement.

This is the high level view of the DAVIC Intranet and its relation to other DAVIC and non-DAVIC systems. A DAVIC Intranet can be viewed as a single administrative domain with uniform network addressing.

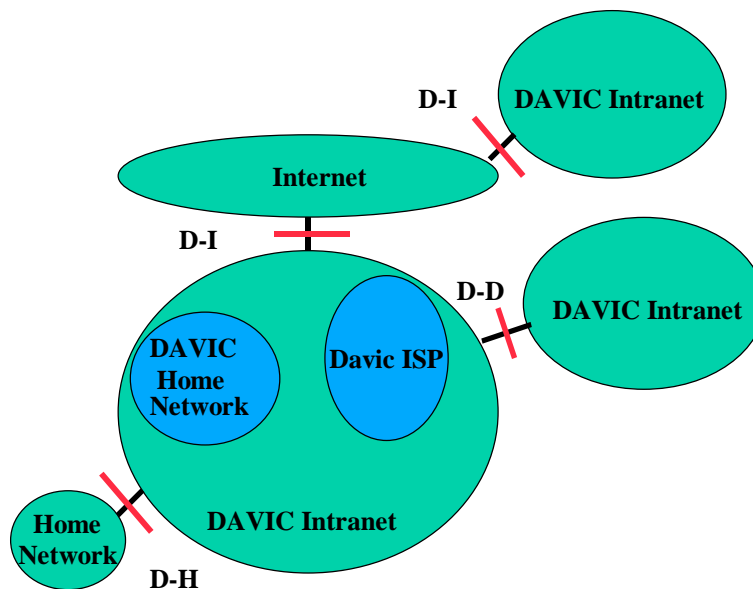


Figure 8-1: DAVIC Intranet

DAVIC Home Networks and ISPs inside the DAVIC Intranet can be interconnected in the most efficient way since they are part of a homogeneous system. Interfaces to other Intranets, non-DAVIC Home Networks and ISPs as well as the Internet itself also need to be defined.

DAVIC Intranet Interfaces:

a. D-I (DAVIC - Internet) Interface defines the tool set that is required for the connection of the DAVIC Intranet to the public Internet.

For example if private addresses are used (not recommended) in the DAVIC Intranet, Network Address Translation (NAT) may be incorporated as part of this interface in order to allow communication with the public Internet. Policy control in a number of mechanisms (multicast, QoS etc.) is also required on this Interface.

DAVIC Intranet

Note: The D-I Interface only considers the interconnection of DAVIC with the Internet. Techniques to interconnect two DAVIC Intranets over the Internet, using their D-I interfaces may be considered in the future.

b. D-D (DAVIC - DAVIC) Interface defines the tool set that is required for the direct interconnection of two DAVIC Intranets.

This interface should allow easy interconnection of DAVIC Intranets. The fact that the Interconnecting networks are DAVIC compliant should make their interconnection easy and optimum. This is because all the policy, security, quality and billing related requirement in the two systems follow the same specifications (DAVIC Intranet).

c. D-H (DAVIC - Home network) Interface defines the tool set that is required for the connection of the DAVIC Intranet to a non-DAVIC home network.

Home networks should be able to connect to DAVIC and non-DAVIC ISPs through the DAVIC Intranet.

8.2 DAVIC Value-Add

The concept of the DAVIC Intranet is useful for a number of reasons. Primarily, the network of networks paradigm of the Internet, with multiple independent system specifications within each network, inevitably results in a lack of end to end coherence in terms of dimensioning, resource allocation, prioritization and commercial models. In particular, the system interactions between transport and applications, and between different commercial roles within the system, lacks standardization. The DAVIC role exists because the IETF charter specifically excludes, discussing and satisfying the requirements of particular commercial models. More specifically, the existence of the DAVIC Intranet will allow these roles and interactions to be discussed and defined in a way that reflects the commercial interests of the DAVIC members. Examples of system specification benefits can be seen in terms of:

- multicast distribution and replication policy
- host to host differential services on an end to end basis
- application accounting;
- signaling
- contribution systems specifications
- distribution systems specifications
- definition of performance data between DAVIC Intranets
- exchange of performance data between DAVIC Intranets
- definition of security systems to control the end to end Intranet services
- definition of management systems to control the end to end Intranet services

The following figure illustrates one key example of the value added by the DAVIC Intranet concept. The top portion of the figure shows two DAVIC Intranets directly connected so that end-to-end controlled QoS is possible. The bottom figure shows how these same two DAVIC Intranets can be interconnected via "The Internet", which in general does not allow end-to-end controlled QoS. Note that in either case these interfaces are based on standard IETF protocols.

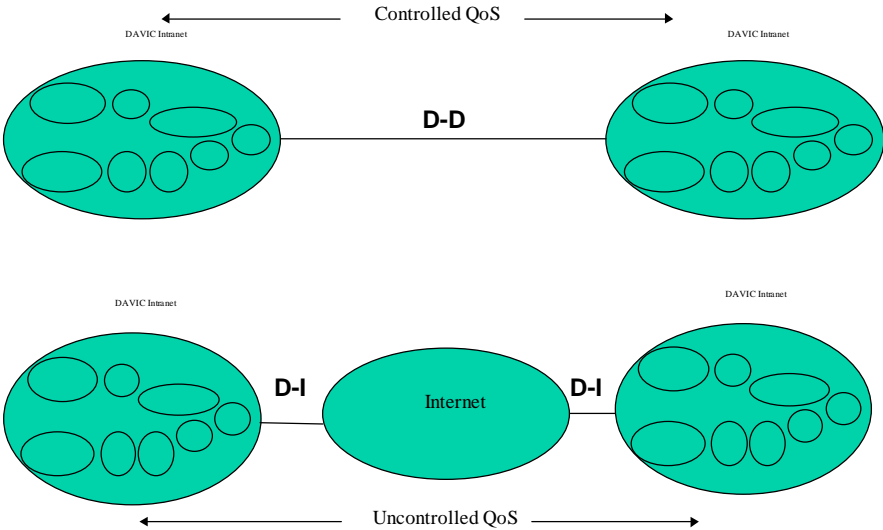


Figure 8-2: DAVIC added value example

9. Addressing and Naming

9.1. Addressing Homogeneity

Address homogeneity shall be implemented inside a single DAVIC Intranet. Addressing Homogeneity means that all network addresses in a DAVIC Intranet are routable within the Intranet.

The main advantage of address homogeneity is that no address translation is required inside a DAVIC Intranet.

9.2. Global Addressing

It is highly recommended that any DAVIC compliant system uses globally registered IP addresses when possible.

9.3. Private Addressing

If a DAVIC Intranet is not able to acquire the number of globally registered IP address required it may use private addresses. In this case special care must be taken in designing the interfaces (gateways) to the global Internet as well as other DAVIC domains.

10. Network Support

10.1 Framework for Access Networks

The DAVIC Intranet may be required to support a variety of Access Networks such as ATM, Satellite and Cable, Home Networks (HNs) such as IEEE1394 and Ethernet and different service presentations to the ISPs such as Frame relay, ATM, L2TP etc.

The following figure represents the framework based on which, we will explain most possible combinations of technologies.

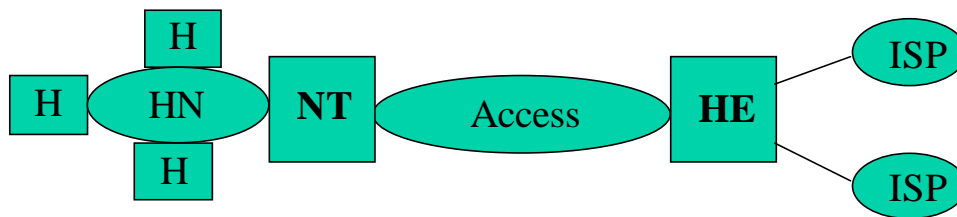


Figure 10-1: Access Framework

The HN represents functions that occur in the customer's premises, beyond the network termination (NT) on the left hand side of the above figure.

On the right hand side of the NT we have the Access Network which connects the customer to the ISP through the Head End (HE).

For an explanation of how Layer 3 is carried over a variety of Access and Home networks, refer to [Annex A : Access and Home Network Technology Framework](#)

10.2 Core Networks

10.2.1 Layer 2.

Any layer 2 that adequately supports the DAVIC Intranet may be used.

The selection of a specific layer 2 is considered to be a matter of local policy.

10.2.2 Routing.

Routing is one of the most important functions in IP technology. It is the mechanism that provides connectivity between end-points by examining the IP header of a packet going from one end to the other and forwarding it to the next router 'closer' to the destination.

10.2.3 Interior Routing Protocols

Interior Routing protocols allow routers to discover their neighbors and appropriate routes to them. They provide mechanisms for the creation of routing tables based on a number of parameters (hop count, bandwidth etc.) and the exchange of routing information between them.

The Interior routing protocol used in a DAVIC Intranet is a matter of local policy. The use of OSPF is recommended due to its better scalability but other routing protocols can also be used. Where the core comprises a number of autonomous systems (AS), inter-AS routing may use BGP.

10.2.4 Exterior Routing Protocols

Exterior routing protocols are similar to interior routing protocols with the difference that the routing information that is created and exchanged is mostly based on policy rather than network topology and/or connection characteristics.

BGP4 shall be used for exterior routing between DAVIC Intranets.

11. Multicast

For live content over unicast networks, bandwidth efficiency and server dimensioning issues can be reduced through the use of an IP multicast tree. The user and application provider QoS requirements will need to be supported by the underlying internetwork components. The content provider can then view the distribution network as a broadcast network

For DAVIC's IP-based multimedia applications/services, it is equally important to support not only QoS-guaranteed point-to-point applications/services but also multicast applications/services. Some DAVIC applications may require QoS-based multicasting and some may consider reliability as a first priority. Therefore, it is very important to provide these multicasting functionalities that satisfy the requirements from various applications/services. These multicasting functionalities can be realized in transport layer and/or network layer or even by some other means. For example multicasting functionalities could be efficiently mapped into ATM multicasting capabilities for the IP over ATM scenario.

11.1 Multicast Clients

In contrast to IP unicast services, IP multicast uses Class D addresses that are reserved for groups rather than individual hosts. These addresses can be dynamically allocated from a pool and reused. With IP multicast, a single source sends a stream of IP packets to multiple destinations simultaneously. It enables applications to significantly reduce the load on network resources. IP multicast is supported by IGMP (Internet Group Membership Protocol - RFC 1112), which works between the router and attached clients.

Clients shall support the IGMP protocol to enable clients to join and leave the multicast group.

11.2 Multicast Servers

IGMP enables clients to join and leave a multicast session dynamically by sending notifications to the router.

Servers that offer multicast type services shall support IGMP to enable servers to join or leave a multicast group.

11.3 Delivery System

11.3.1 Group Management

The Delivery System (network) shall support IGMP to enable clients to join and leave the multicast group.

11.3.2 Multicast Routing Protocol

In addition to IGMP mentioned previously, IP multicast is also supported by a routing protocol, such as PIM (Protocol Independent Multicast - RFC 2117, including PIM-Dense Mode and PIM-Sparse Mode), or DVMRP (Distance Vector Multicast Routing Protocol - RFC 1075) or MOSPF (Multicast Open Shortest Path First - RFC 1584). These protocols all use the source-based tree techniques.

Routing protocols for multicast	Main features
DVMRP	Constructs source-based multicast delivery trees using the Reverse Path Multicasting (RPM) algorithm.
MOSPF	Maintains a current image of the network topology through the unicast OSPF link-state routing protocol and uses IGMP to monitor multicast membership on direct-attached subnetwork, then determines the local routers' responsibility for delivering multicast datagrams.
PIM-DM and PIM-SM	They are more independent than others and allows data streams to be broadcast to multiple receivers using as little network bandwidth as possible.

Table 11-1 Multicast Routing Table

Multicast routing protocols can also be divided in terms of the expected demography of the multicast group membership. Explicit join protocols (PIM-SM) use a single shared s tree for all sources, centered at an elected rendezvous point in the network and are optimized for sparsely populated spanning trees. For densely populated trees, a broadcast and prune mechanism is used (DVMRP, MOSPF, PIM-DM).

As PIM supports both paradigms, this is the selected multicast routing protocol.

Delivery Systems shall support PIM for the multicast routing protocol.

12. Quality of Service

The Internet currently supports ‘best endeavors’ for data transmission, which does not encourage the commercial development of high value services due to the unpredictable Quality of Service (QoS). Methods of implementing QoS must be identified to enable differentiated services to be delivered.

The current DAVIC Intranet supports two types of QoS mechanisms defined in this section. In the future DAVIC may add or extend the tools to support additional QoS requirements.

Admission policies employed for the QoS services should be left to the freedom of the DAVIC Intranet operators.

12.1 Differentiated Services (Diff-Serv)

The IETF is currently in the process of standardizing the semantics of 6 bits of the IP TOS field, in the IP header, to give 64 values or ‘codepoints’ that can be used to define per-hop behaviors (PHBs). PHB semantics are defined in terms of relative characteristics such as low delay, high reliability, high bandwidth etc.

If the codepoints defined by the IETF are not fully satisfactory, DAVIC may make use of codepoints assigned for local/experimental use and possibly propose its use to the IETF

The mechanisms to support these, such as scheduling algorithms, priority queuing etc. at this stage are left to the router manufacturers. The Diff-Serv mechanisms should always be used in combination with appropriate dimensioning of the network resources.

DAVIC Intranets should support differentiated service mechanisms, when they are sufficiently mature and DAVIC has determined their exact use.

12.2 RSVP Protocol

DAVIC Intranets may have the capability to reserve resources between two end-points that can communicate over a path that is DAVIC compliant.

In that case Resource reSerVation Protocol (RSVP) shall be used on:

- **the edge routers of every DAVIC intranet as well as**
- **the end-hosts/applications that require resource reservations.**

Resource reservation inside a DAVIC Intranet is left to local policy as long as RSVP can run end-to-end and the correct resources can be reserved according to the RSVP reservation messages. It is possible that a network may support RSVP on all its Layer 3 devices or that the resource reservation is handled by different mechanisms such as MPLS (MultiProtocol Label Switching)

RSVP will satisfy the bandwidth and delay requirements; additional mechanisms, however, will also be required in order to satisfy applications with very strict delay variance (jitter) requirements. More information can found in the "DAVIC 1.5 Jitter concealment tools specification".

12.3 Jitter

Existing IP QoS components such as RSVP and Diff-Serv are not directly dealing with jitter. Due, however, to the strict requirements imposed by a number of real time services, the jitter problem on IP networks has to be dealt with. (DAVIC 1.5 Jitter concealment tools specification)

13. Transport

13.1 RTP and RTCP

In the IP world, RTP (Real-time Transport Protocol) provides end-to-end delivery services to support applications transmitting real-time data over DAVIC Intranets. RTP services include payload type identification, sequence numbering, and time stamping. Its header provides the timing information necessary to synchronize and display audio/video data. It also provides optional data delivery monitoring and controlling by means of an integrated control protocol -- RTCP. RTCP introduces some scalability issues when used in large scale multicast communication because of the large amount of Receiver Reports that are sent to the server (multicast sender).

DAVIC Intranet clients and servers shall support the RTP protocol.

RTP will be used for the real time transport of content and in particular A/V content in DAVIC Intranets.

DAVIC Intranet clients and servers shall support the RTCP protocol.

The application will determine if RTCP is to be used or not and if so, how it will be applied. Future specifications of DAVIC will address this issue.

13.2 HTTP

HTTP (HyperText Transport Protocol) was originally intended for transactional services and is currently also used for file transfer.

DAVIC Intranet clients shall support the HTTP v1.1 protocol.

HTTP will be used for the non real time transport of content in DAVIC Intranets.

14. Session Description and Control

14.1 SDP

SDP is designed to describe multimedia sessions for the purposes of session announcement, session invitation, and other forms of multimedia session initiation. Note that SDP cannot describe multiple methods for receiving the same stream. To enable this, multiple SDP descriptions are required, one for each method for receiving the same stream.

DAVIC Intranets shall support SDP as the protocol for describing sessions.

SDP descriptions can be transported using various protocols and mechanisms including SAP and HTTP.

The jitter document (*reference*) describes the RQRP scheme for dealing with jitter. In order to use this scheme the SDP <transport> sub-field of the 'm=' parameter will have to be <RQRP/RTP/AVT>. The default Audio/Video profile [RFC1890] still applies.

14.2 RTSP

RTSP (Real-Time Stream control Protocol) is used in the Internet to initiate and control (play, record etc) audio, video and other RTP-based streams. Although RTSP can be used to provide basic Video Cassette Recorder (VCR) control, advanced functionalities, such as delayed recording (setting up recording parameters for a session that is going to be available in the future) are not currently supported by the RTSP specification.

DAVIC Intranet clients and local servers shall support the RTSP protocol for the control of streams.

DAVIC Intranet servers shall support the RTSP protocol for the control of unicast streams

15. Service Location Capability

15.1 SLP

SLP (Service Location Protocol) provides a framework for the discovery and selection of network services. Using this protocol, computers accessing the Internet need little or no static configuration of network services for network based applications. SLP allows devices such as Local Servers to announce themselves and their capabilities to clients, as well as allows clients to request specific services from the network.

DAVIC Intranet clients shall support the SLP protocol.

SLP may be used for the discovery of services in the Home Network (HN). SLP is not to be used to discover services outside the home network.

Local Servers that are used in the HN shall support the SLP protocol.

Local Servers shall use SLP in order to advertise services internal to the HN.

For the purposes of the DAVIC Intranet design a new 'service' definition is required in the SLP protocol.

For this new service, the 'service type' (RFC2165) string shall be: <DLS> for the DAVIC local server.

16. Dynamic Flow Diagrams for TV anywhere and TV anytime

This section contains implementation examples for the DAVIC Intranet application scenarios.

The DAVIC 1.5 Intranet architectural model is shown in [Figure 16-1](#). It shows the relations between the different functional elements that are being used in the DAVIC 1.5 Intranet System. The identified functional elements for DAVIC 1.5 are a DAVIC Intranet server, a DAVIC Intranet client and a local storage server. These elements are connected through the DAVIC Intranet (this includes the home network).

The DAVIC Intranet server is a device that is capable of streaming 'real-time' audiovisual material to a client or a local storage server. The DAVIC Intranet client is able to decode and display this audiovisual stream in real time. The client may also instruct the local server to record a real-time or non-real time stream coming from the DAVIC Intranet server. It may also ask the local storage server to play any audiovisual streams that are on the disk. The relationships between these entities are being indicated by the numbered dotted lines.

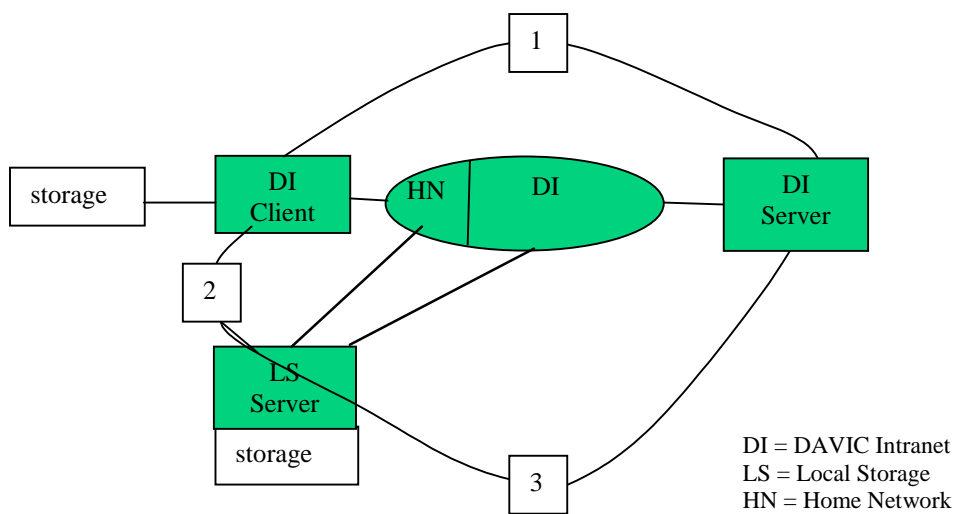


Figure 16-1 DAVIC 1.5 Intranet Architecture

The DAVIC 1.5 architectural model is a simplified version of the DAVIC Intranet model, where more DAVIC Intranets can be combined and also other internetworking may be taking place.

The following sections contain the flow diagrams that highlight the temporal relationships between the different entities.

The flow diagrams presented in this section are not exhaustive. They are here to help the implementers of the specification to understand the possible sequence of events during the control and retrieval of content.

16.1 Local Storage Discovery

If the HN includes a Local Server (LS), Local Storage device with Server capabilities, the Service Location Protocol can be used in two ways in order to automate the clients' configuration.

The LS periodically announces its presence by multicasting a Service Announcement (SAnn) message on the Home Network using the well known SLP multicast address. Clients that must be configured to listen to this address for service announcements will pick-up the announcement.

Clients can explicitly request a specific service by multicasting a Service Request (SReq) message on the Home Network using the well known SLP multicast address. LSs must be configured to listen to this address for service requests and reply by sending a unicast SAnn message to the requesting client.

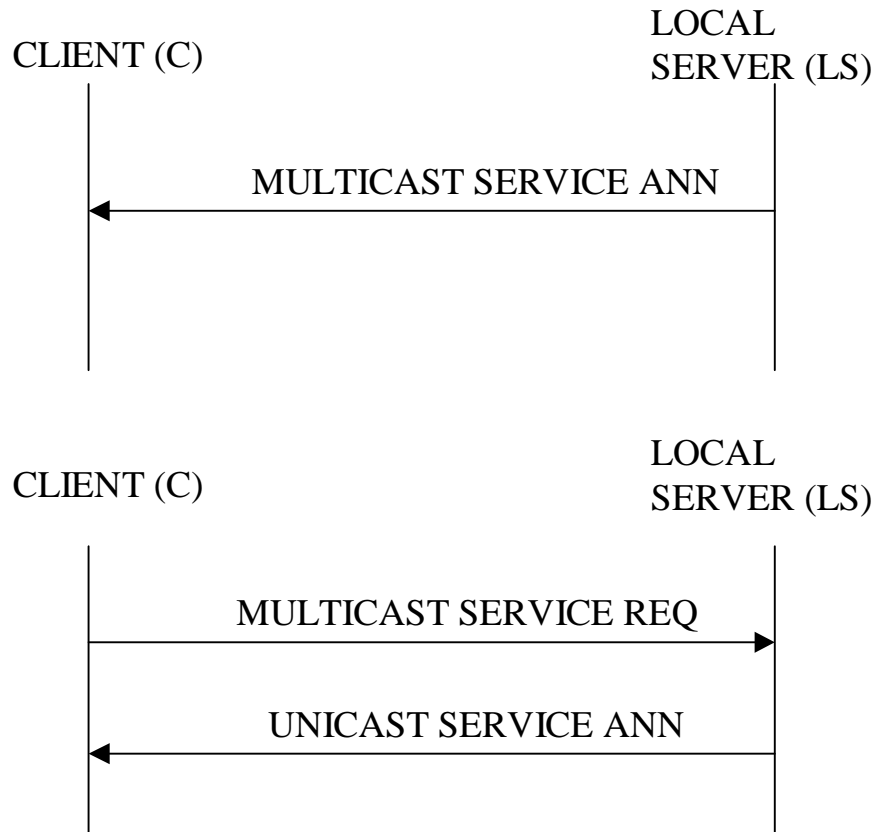


Figure 16-2 Local Server Discovery

16.2 Unicast (1-to-1) Real Time

Client C requests a movie from Remote Servers RS (DAVIC.server.com). The media description is for example, stored on a web server, for simplification, also located in a RS. The media description contains descriptions of the presentation and all its streams, including the codecs that are available, dynamic RTP payload types, the protocol stack, bandwidth requirements etc.

Note that the data stream is transmitted over unicast in this case. This is particularly required for the implementation of the TV anytime application scenario.

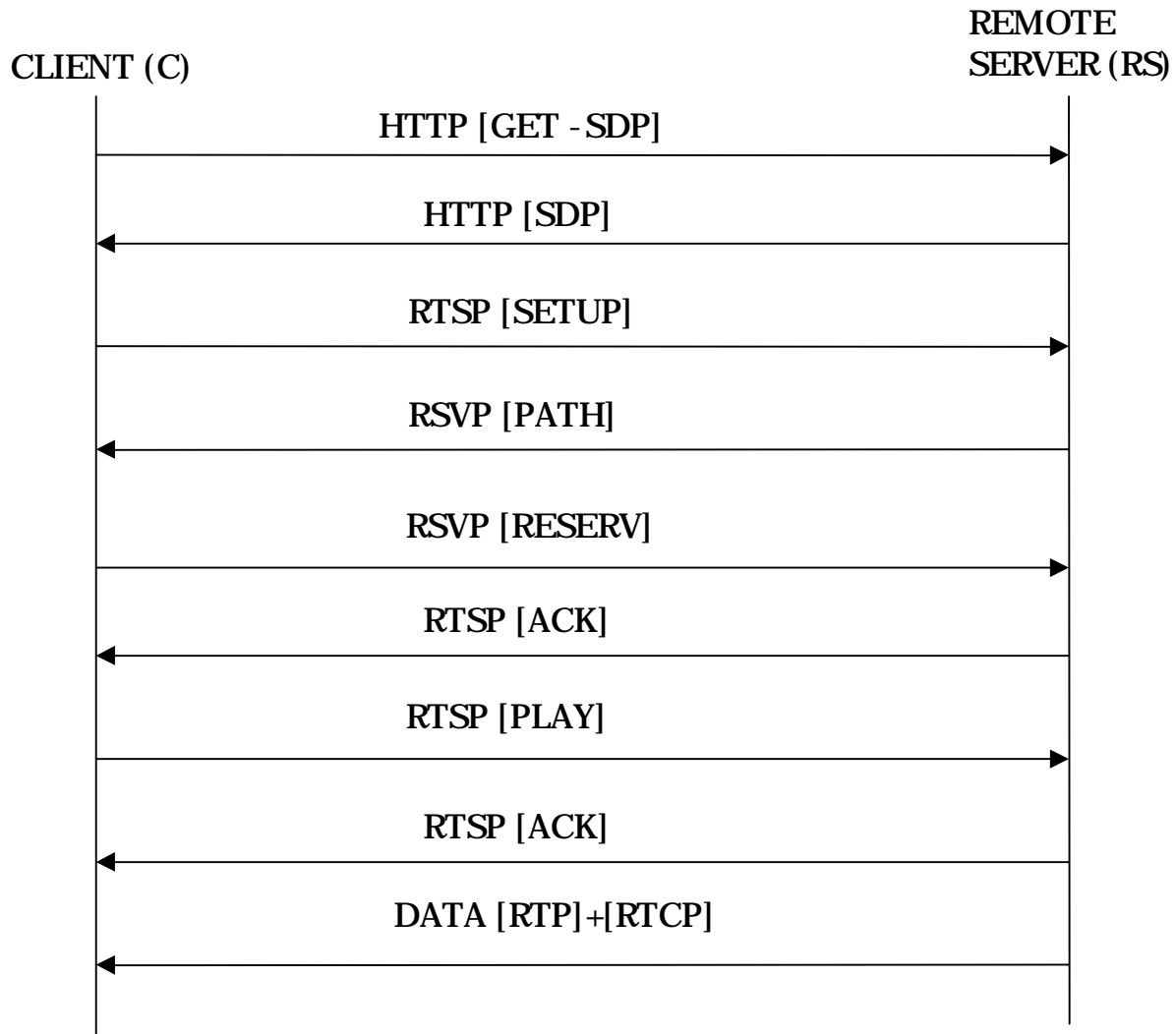


Figure 16-3 Unicast Real Time Streaming

C is sending an HTTP (GET) command in order to retrieve SDP information for some content. The Web Server sends the SDP information also using HTTP. By parsing the SDP information, C finds an RTSP URL indicating where the content resides and how it can be retrieved. An RTSP (SETUP) message is sent to the correct RTSP server which also triggers RSVP reservation if QoS is required. Note that SDP information include bandwidth (b=) parameter that can be used by RSVP. If the reservation succeeds an RTSP (ACK) message is sent by RS. C can now send an RTSP (PLAY) message in order to retrieve the stream. RS acknowledges the request and sends the data using RTP/RTCP, as indicated by the SDP information.

The RTSP session will have to be Torn-Down by the client.

The fact that HTTP is used to retrieve SDP information is incidental. The same information could be retrieved by other means; e.g.: via Session Announcement Protocol (SAP), e-mail or something else.

The following walk through provides some more detailed information on the use of the selected protocols for the implementation of the above flow diagram.

```

C->RS: GET /DAVIC-video.sdp HTTP/1.1
      Host: www.DAVIC.org
      Accept: application/sdp
RS->C: HTTP/1.0 200 OK
      Content-Type: application/sdp
  
```

DAVIC Intranet

```
v=0          -Version
o=- 2890844526 2890842807 IN IP4 192.16.24.202 -session ID
s=DAVIC Session      -Session Name
m=video 49100/2 RTP/AVP 33(<-MPEG2TS)      -media
b=AS:6000          -bandwidth
a=control:rtsp://DAVIC.server.com/video -attributes
C->RS: SETUP rtsp://DAVIC.server.com/video RTSP/1.0
      CSeq: 1
      Transport: RTP/AVP/UDP;unicast;client_port=3058-3059
```

RSVP reservation should be dealt with at this stage

```
RS->C: RTSP/1.0 200 OK
      CSeq: 1
      Session: 23456789      -Session ID
      Transport: RTP/AVP/UDP;unicast;client_port=3058-3059;
                server_port=49100-49101
C->RS: PLAY rtsp://DAVIC.server.com/video RTSP/1.0
      CSeq: 2
      Session: 23456789
      Range: smpte=0:10:00-      -Relative timestamp
RS->C: RTSP/1.0 200 OK
      CSeq: 2
      Session: 23456789
      Range: smpte=0:10:00-0:20:00
      RTP-Info: url= rtsp://DAVIC.server.com/video;
                seq=12312232;rtptime=78712811
```

Video Streaming Phase

```
C->RS: TEARDOWN rtsp://DAVIC.server.com/video RTSP/1.0
      CSeq: 3
      Session: 23456789
```

Client should now remove any RSVP reservation

```
RS->C: RTSP/1.0 200 OK
      CSeq: 3
```

16.3 Multicast 1-to-Many, Real Time

Client C attempts to retrieve a stream. The media description of the stream is transmitted over SAP, which is the default announcement protocol for multicast sessions. The media description contains descriptions of the presentation and all its streams, including the codecs that are available, dynamic RTP payload types, the protocol stack, bandwidth requirements etc. It may also give an indication about the timeline of the movie.

Note that the data stream is transmitted over multicast in this case. This is particularly useful for the implementation of the TV anywhere application scenario.

Note: SAP when it's completed by the IETF is a possible way to get the SDP information to the client. Depending on the application, other means may be more appropriate. Other solutions, not involving multicast of SDP could be considered.

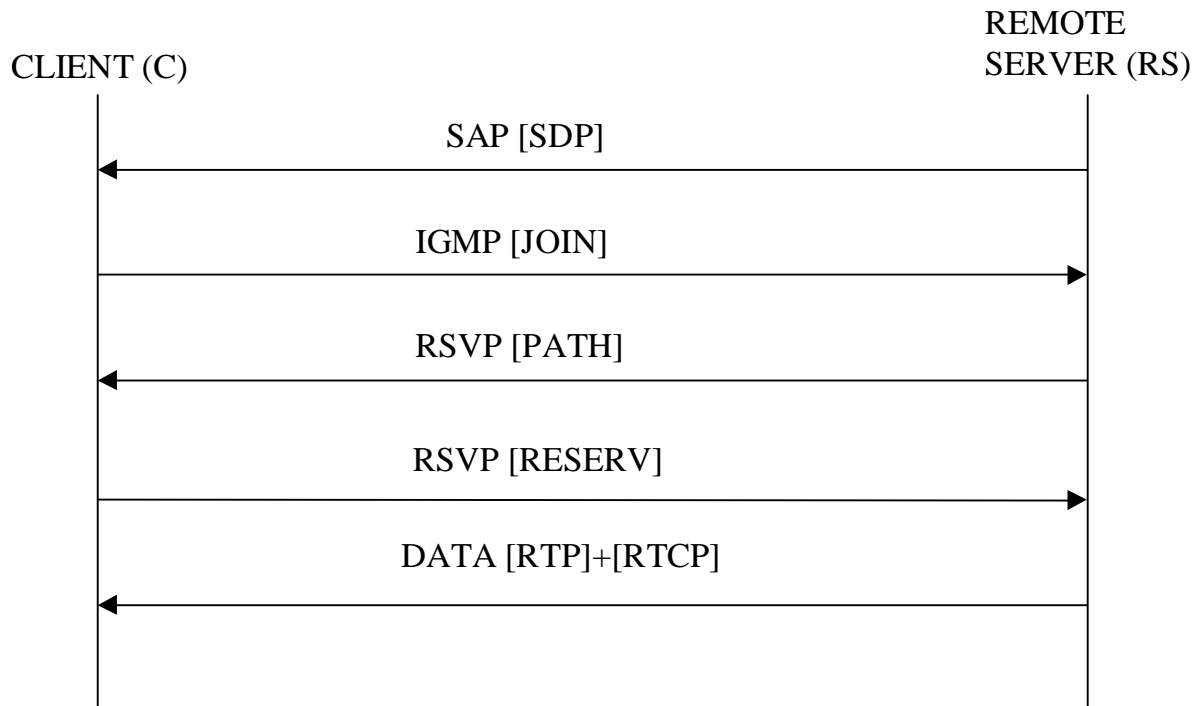


Figure 16-4 Multicast Streaming

C is listening on the designated multicast address for Session Announcements. Session announcements are received and they include SDP information. By parsing the SDP information, C finds the multicast group that it has to join in order to receive the selected stream. An IGMP (JOIN) message is sent to the correct multicast group which also triggers RSVP reservation if QoS is required. Note that SDP information include bandwidth (b=) parameter that can be used by RSVP. If the reservation succeeds C starts receiving the stream over RTP.

16.4 Example Usage of Local Server

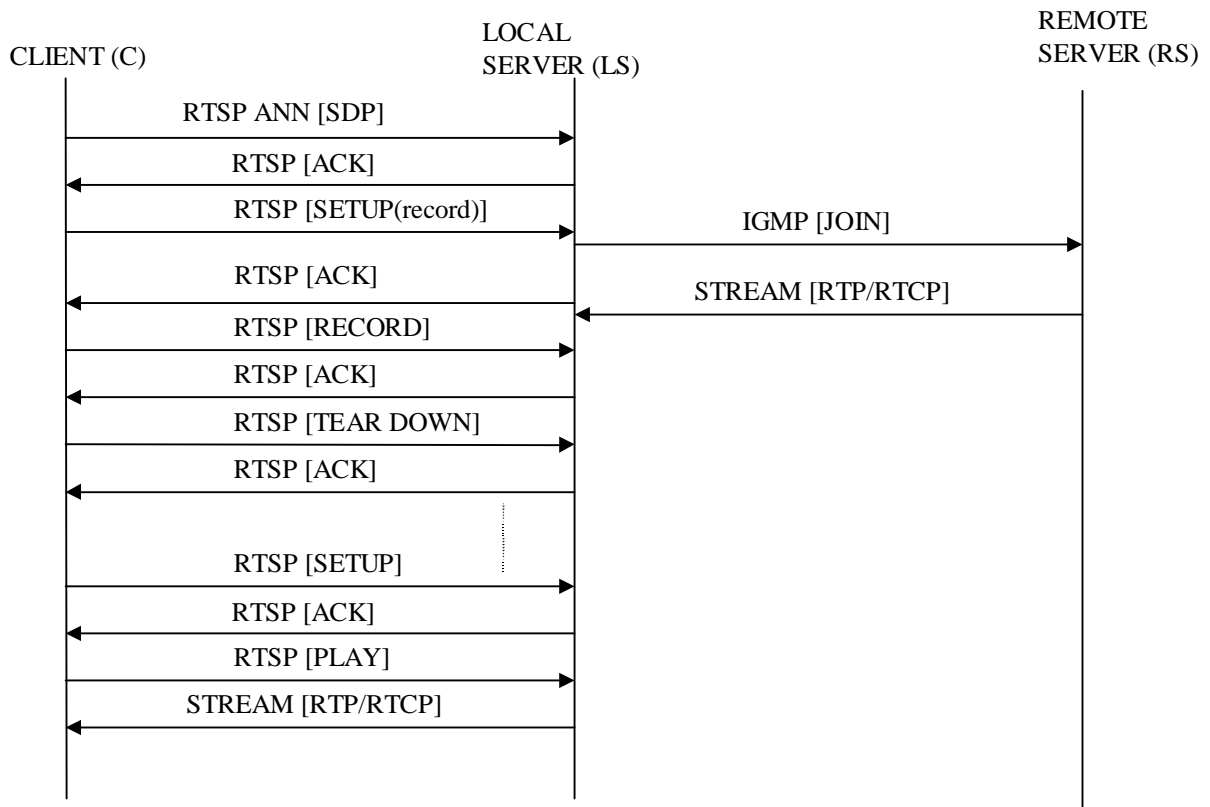


Figure 16-5 Real time streaming with a local server

In this example a client controls a Local Server in order to record a real time stream and play it back in a way similar to that of a conventional VCR.

The client opens an RTSP session with the LS and sends the SDP description of the session to be recorded. This makes the LS to join the multicast that the SDP description dictates. The LS can now start recording the session after appropriate command from the client and the client can play it back at any time after that.

Annex A : Access and Home Network Technology Framework

The following sections will break down each part of the Home and Access network framework as being either "Point to Point" or "Broadcast" based. This in order to cover the maximum number of technology combinations in a generic way.

A.1. Home Networks

The Home Networks divide into Point to Point and Broadcast, the assumptions that need to be made and the features required are different for each.

A.1..1. Point to Point HNs

These are configurations in which the end-points have individual and independent point to point connections to the NT. This may be materialized in two ways.

a) Real Point to Point connections

By this we refer to HN Layer 2 technologies that are fundamentally point to point, such as ATM shown in the low left corner of the figure.

b) Emulated point to Point connections

By this we refer to HN Layer 2 technologies that are fundamentally not point to point (e.g.: broadcast) but point to point connections are emulated somehow between the end-points and the NT. In the top left corner of figure we see an Ethernet based HN with L2TP connections between the end-points and the NT that makes the HN look to higher layer protocols like a point to point network, much like its ATM counterpart in (a).

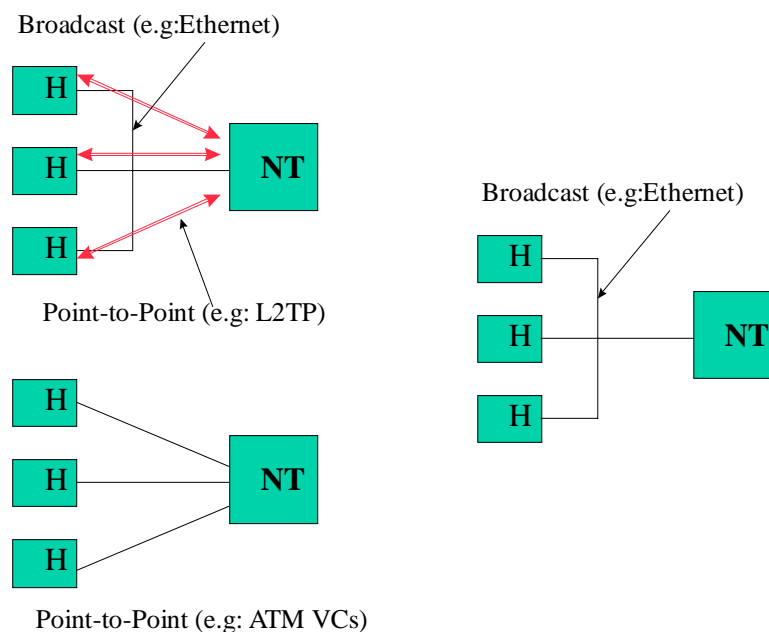


Figure A-1: Home Networks

A.1..2. Broadcast HNs

These are HNs that are based on a broadcast Layer 2 technology such as Ethernet. Note that there might also be fundamentally point to point Layer 2 HNs that emulate broadcast connectivity using for example VLAN techniques.

A.2. Access Networks

There are three kinds of Access Networks and these are a) Point to Point, b) Bi-directional Broadcast and c) Unidirectional Broadcast with Back-channel. There are also a number of flavors of the above but after close study all come done to one of the above three variants.

Again, keep in mind that some of the above may be emulated by different kind of technologies. For example an IP based access network using L2TP technology to connect NTs to the ISPs is not fundamentally Point to Point, but it emulates Point to Point with L2TP tunnels.

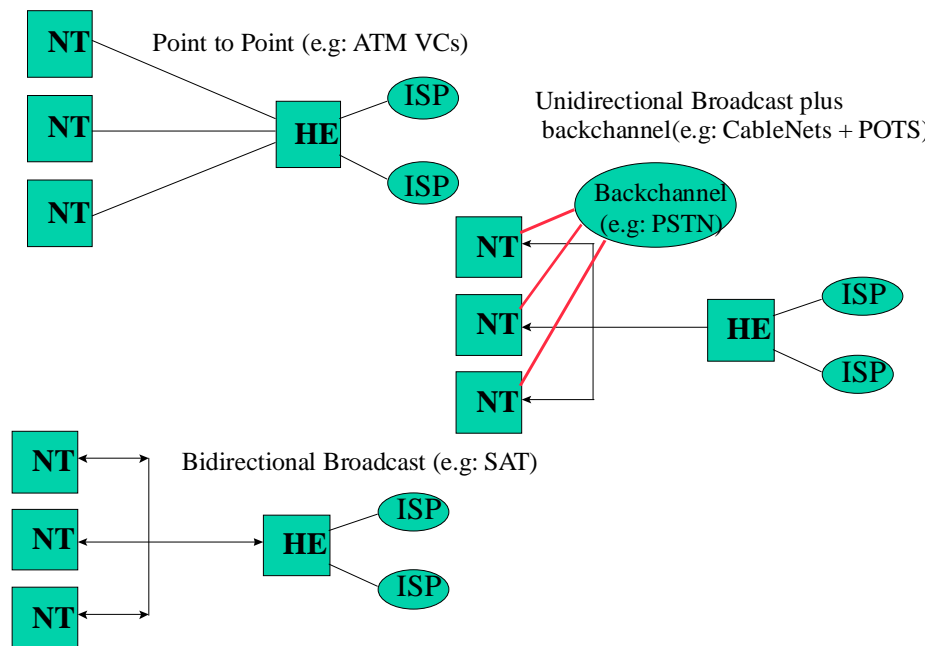


Figure A-2: Access Networks

A.2..1. Point to Point

These are Access Networks which use point to point links to connect NTs to HEs (and thus ISPs).

A.2..2. Bi-directional Broadcast

These are networks such as satellites, where the NT is also a satellite transmitter or Cable Networks where the NT has a point to point connection to the HE but the Layer 2 technology emulates a broadcast network..

A.2..3. Unidirectional Broadcast with Back-channel

These are networks such as sidelight with one way broadcast (HE to NT) and a back channel from NT to HE that may use different media such as PSTN to create a point to point link back to the HE.

A.3. System Framework

We are going to combine the different HN and Access configurations in order to examine a number of complete access scenarios.

To limit the number of combinations we are going to examine each of the Access configurations in combination with all the HN configurations at the same time.

A.3..1. Point to Point Access - Point to Point HN

In this case both the HN and the access are point to point based

The following components are required for internet access:

PPP (Point to Point Protocol)

Since there is a point to point Layer2 link from the Home End-point to the ISP, PPP is going to be used for negotiation of the IP parameters, link speed, framing etc. Note that by using PPP, a number of point to point technologies can be supported (ATM VCs, ISDN, FR etc.).

No IP on the NT

Due to PPP running across the NT, the NT itself does not require IP awareness; it can simply be an ISDN type modem or a switch.

iii. The IP addresses may be Statically (not recommended) or Dynamically allocated to the end-points using DHCP. In this case the DHCP server is going to be located in the ISP.

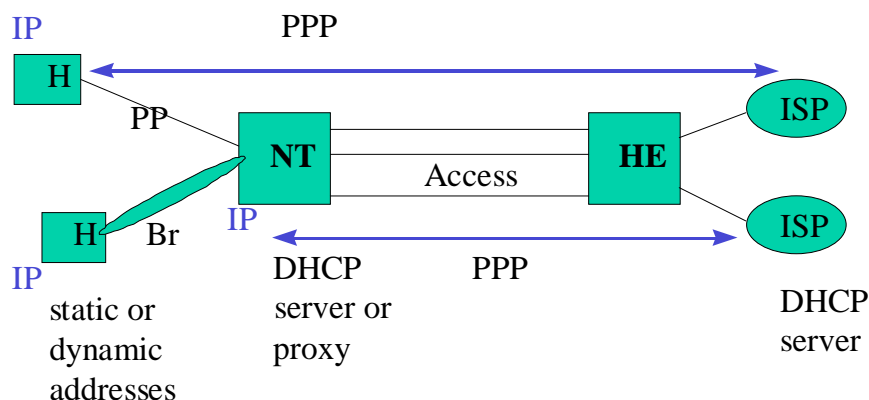


Figure A-3: Point to Point Access

A.3..2. Point to Point Access - Broadcast HN

In this case the HN is Broadcast based and the access is point to point based

The following components are required for internet access:

PPP (Point to Point Protocol)

Since there is a point to point Layer2 link from the NT to the ISP, PPP is going to be used for negotiation of the IP parameters, link speed, framing etc. Note that by using PPP, a number of point to point technologies can be supported (ATM VCs, ISDN, FR etc.).

IP on the NT

Due to PPP running from the NT, the NT itself requires to have IP awareness in order to terminate PPP and understand the IP parameters allocated by the ISP. The NT requires at least a minimum amount of routing capabilities.

iii. The IP addresses may be Statically (not recommended) or Dynamically allocated to the end-points using DHCP. In this case a DHCP server located at the ISP may be accessed directly from the home end-points or by a proxy DHCP on the NT which in its turn will provide DHCP services to the Home Network.

A.3.3. Uni-directional Broadcast plus back-channel Access - Point to Point HN

In this case the HN is Point to Point based and the access has a Broadcast channel from the HE to the NTs while the NTs connect back to the HE with a separate bi-directional point to point link.

The following components are required for internet access:

i. IP on the NT

The NT requires to be IP aware since the Broadcast channel terminates on it and routing is then required in order to send the traffic to the correct end-point.

PPP on the back-channel

Depending on the exact scenario Home end-points require a point to point link (possibly running PPP) over the back-channel and to their ISPs

iii. ARP

The end-points need to be able to communicate the MAC address of the NT in order for the HE to send to them traffic on the correct layer2 address. Note that such a mechanism does not exist at the moment.

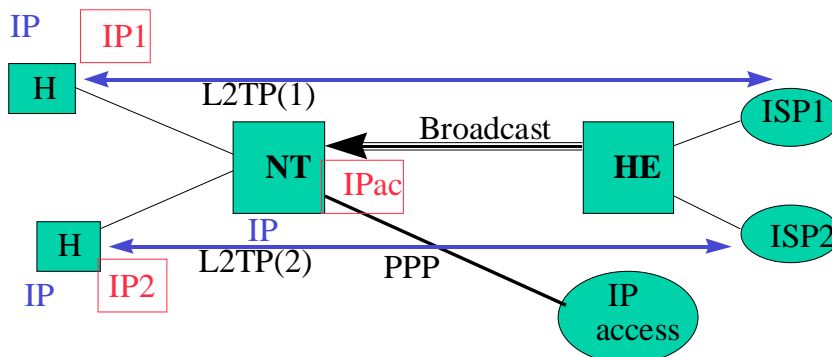


Figure A-4: Broadcast Access + Point to Point HN

A.3..4. Uni-directional Broadcast plus back-channel Access - Point to Point HN

In this case the HN is Point to Point based and the access has a Broadcast channel from the HE to the NTs while the NTs connect back to the HE with a separate bi-directional point to point link.

The following components are required for internet access:

i. IP on the NT

The NT requires to be IP aware since the back-channel starts from it

PPP on the back-channel

Depending on the exact scenario NTs require a point to point link running PPP over the back-channel and to their ISPs

DHCP

The NT can also play the role of proxy DHCP if this is required

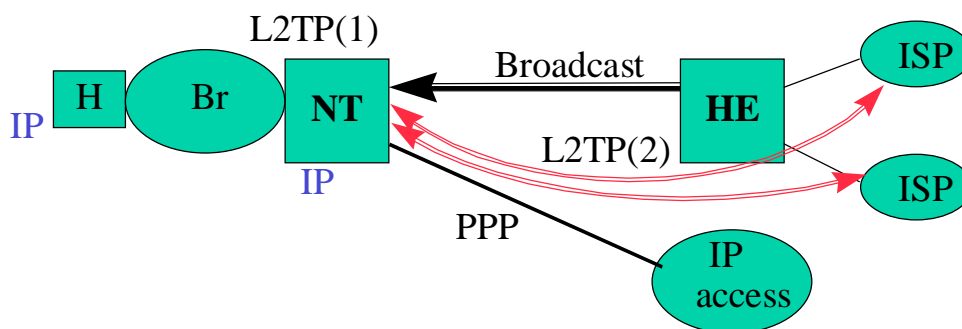


Figure A-5: Broadcast Access + Broadcast HN

A.3..5. Bi-directional Broadcast Access - Broadcast or Point to Point HN

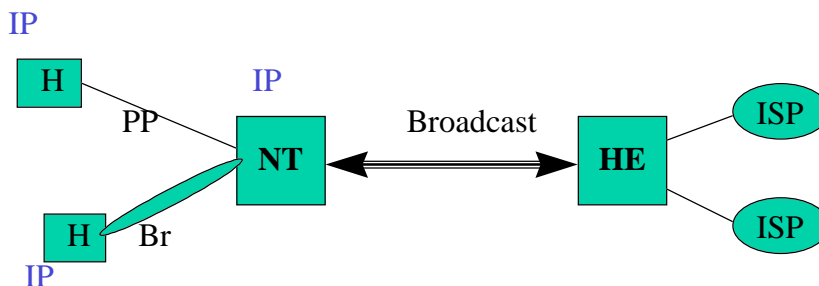


Figure A-6: Bi-directional Broadcast Access

Annex B : Table of Normative Technologies

Section	Requirement
9.1.1	Address homogeneity shall be implemented inside a single DAVIC Intranet. Addressing Homogeneity means that all network addresses in a DAVIC Intranet are routable within the Intranet.
10.2.3	BGP4 shall be used for exterior routing between DAVIC intranets.
11.1	Clients shall support the IGMP protocol to enable clients to join and leave the multicast group.
11.2	Servers that offer multicast type services shall support IGMP to enable servers to join or leave a multicast group.
11.3.1	The Delivery System (network) shall support IGMP to enable clients to join and leave the multicast group.
11.3.2	Delivery Systems shall support PIM for the multicast routing protocol.
12.2	<p>In that case Resource reSerVation Protocol (RSVP) shall be used on:</p> <ul style="list-style-type: none"> • the edge routers of every DAVIC intranet as well as • the end-hosts/applications that require resource reservations.
13.1	<p>DAVIC Intranet clients and servers shall support the RTP protocol.</p> <p>DAVIC Intranet clients and servers shall support the RTCP protocol.</p>
13.2	DAVIC Intranet clients shall support the HTTP v1.1 protocol.
14.1	DAVIC Intranets shall support SDP as the protocol for describing sessions.
14.2	<p>DAVIC Intranet clients and local servers shall support the RTSP protocol for the control of streams.</p> <p>DAVIC Intranet servers shall support the RTSP protocol for the control of unicast streams</p>
15.1	<p>DAVIC Intranet clients shall support the SLP protocol.</p> <p>Local Servers that are used in the HN shall support the SLP protocol.</p> <p>Local Servers shall use SLP in order to advertise services internal to the HN.</p> <p>For this new service, the ‘service type’ (RFC2165) string shall be: <DLS> for the DAVIC local server.</p>