

Uppbyggnad av Acreos referensplattform

Basboxmiljön

av

Elisabeth Modin

med hjälp av
Hans Eric Sandström
och
Rickard Lindström

Rev A
2007-05-29



1. Innehållsförteckning

1. Innehållsförteckning.....	2
2. Inledning	3
3. Basboxmiljöns komponenter	4
4. Systemens interaktion med varandra	5
5. Kanalmottagning.....	6
6. Säkerhet och "Conditional Access"	7
7. Funktion hos "middleware"	8
8. Portalfunktionen	9
9. Set-Top Boxen	10
10. Provisioneringssystem.....	11
11. Anslutning till Acreos referensplattform	12
12. Systemspecifikation	14
13. Uttryck i IPTV-världen.....	15
14. Förkortningar	16

2. Inledning

Att oberoende av leverantör och med bara en set-top box under TV-apparaten kunna se vilka kanaler man själv vill, utnyttja vilka tjänster man själv vill och göra detta när man själv vill, har hittills inte varit möjligt i Sverige. Ett steg på vägen mot detta oberoende är basboxmiljön.

Syftet med detta dokument är att beskriva hur Acreo har implementerat basboxmiljön och hur den ser ut i dagsläget. Det visar vilka system som valts och förklarar även varför i vissa fall. Det visar på ett grundläggande sätt hur basboxmiljön är uppbyggd och syftet med densamma.

I slutet av dokumentet förklaras olika uttryck som florerar i IPTV-världen och en sammanställning av alla förkortningar i dokumentet finns också där.

3. Basboxmiljöns komponenter

För att bygga upp en basboxmiljö krävs ett antal olika system. I Acreos referensplattform används just nu:

- Streamingserver: iXanon
- Middleware: Modulation, görs av Northport
- Portal: Modulation, görs av Northport
- Krypteringssystem: Latens
- Bootserver för STB: Infocast (Kreatel), mcastbootd (Amino), (Tilgin)
- Provisioneringssystem: Netadmin
- Set-Top Box: Kreatel, Amino, Tilgin
- Dessutom tillkommer parabol på taket, router m m.

Basbox referensplattform och referensnät

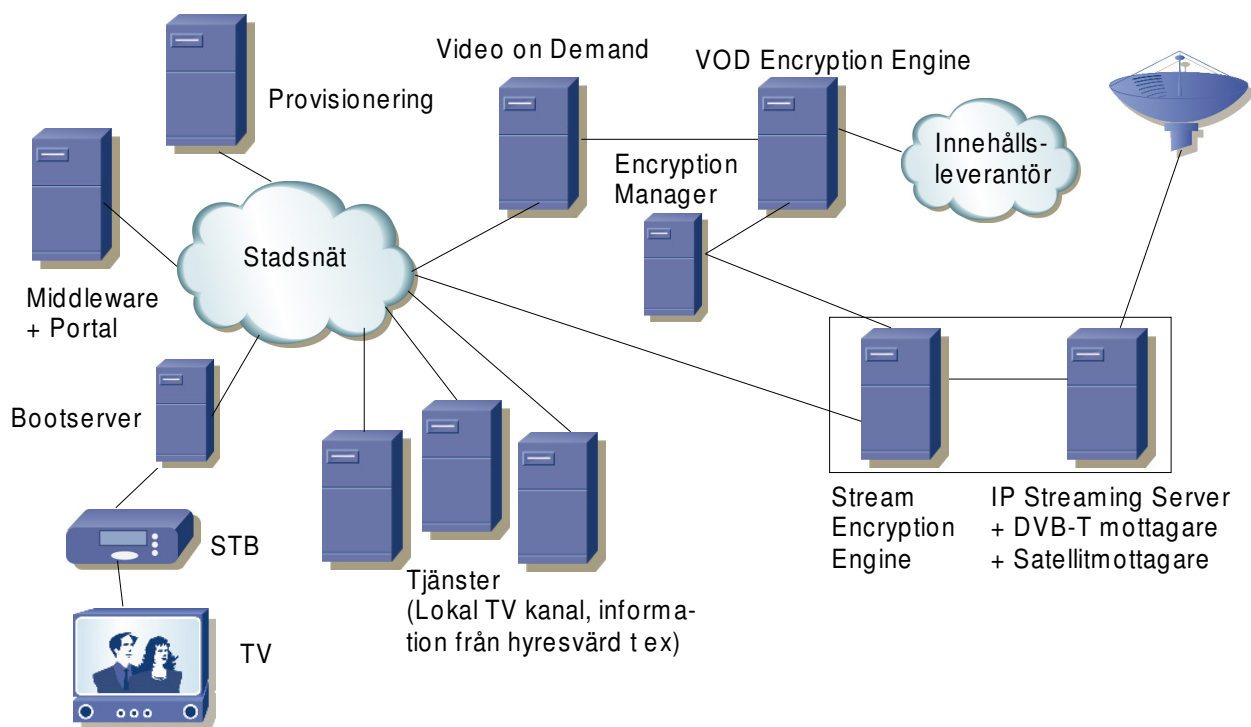


Bild 1

4. Systemens interaktion med varandra

Kanaler tas emot från satelliter, via kabel eller via antenn (när det gäller det marksända nätet), konverteras till IP och förs efter kryptering vidare till Set-Top boxar (STB) i hemmen. (Se bild 1, föregående sida).

För att få sända kanaler ut till konsumenter krävs att rättigheter finns. Acreo har för närvarande sina rättigheter via AB Svensk Programagentur (SPA) och de tillhandahåller en lista med information om på vilka frekvenser och satelliter kanalerna finns. Denna information kan även fås via Internet.

För att ta emot och sända vidare kanalerna använder sig Acreo idag av ett antal kombinerade mottagare och sändare från iXanon. De har mottagare för satellit- och markbaserade sändningar som kombineras med IP Streaming. Konfigureringen görs med hjälp av en lista över frekvenser och kanaler och varje kanal konfigureras som en egen multicastgrupp.

Kanalströmmen som kommer från streamingservern är inte krypterad. Detta gör att den kan ses med streamingläsare (t ex VLC eller TSReader), förutsatt att rätt multicastadress och portnummer anges.

För att få tillåtelse att sända kanalerna vidare till konsumenternas STB måste kanalerna krypteras och göras oåtkomliga för alla och en var. Detta görs med hjälp av ett Conditional Access system (CA system), som läser in kanalerna via multicast, krypterar IP-strömmen och sänder ut den på en ny multicastadress.

Alla STBar måste vara registrerade i Modulution, som är det middleware och portal som Acreo valt att använda sig av. De STB som ska visa krypterat kanalutbud måste även vara registrerade i CA systemet.

Den lokal där allt detta är installerat och driftas kallas för Head-End.

Se bild 1 på föregående sida.

5. Kanalmottagning

Man börjar med att ta reda på från vilken satellit och på vilken frekvens kanalen sänds. Detta görs enklast på Internet genom att söka efter information om kanal. Några bra sidor att starta på kan vara:

<http://www.satcodx1.com/sve/>

<http://www.lyngsat.com/>

<http://se.kingofsat.net/>

Marksända kanaler som t ex SVT och TV4 tas emot via TV-antenn. Detaljerad kanal- och frekvenslista för det marksända nätet finns på

<http://www.teracom.se/?page=5883>

Dessutom finns en lista från SPA som visar på vilka frekvenser de tar ner sina kanaler. Det är dock inte alltid som dessa frekvenser är de som passar Acreo bäst. Det är via SPA Acreo har vidareändringsrättigheter och korten för avkodning kommer från dem.

Acreo har tre parabolerna på taket, som är riktade mot olika satelliter (Thor, Sirius och Hotbird). Varje parabol har fyra huvuden, vilket ger tolv mottagare totalt. Dessutom finns vanlig TV-antenn. Parabolerna tar emot satellitkanaler av typen DVB-S och TV-antennen tar emot marksända kanaler av typen DVB-T.

Inomhus finns tre streamingservrar som var och en har sex ingående interface, ett marksänt och fem satellit. Varje interface är utrustat med en kortläsare (CA modul). På varje interface kan en satellit- eller marksänd frekvens användas. Antalet kanaler på varje frekvens kan variera och de kan vara endera Free To Air (FTA) eller kodade. För de kodade kanalerna måste ett kort sättas i CA modulen för att avkoda. Detta gör att bara en kodad kanal kan tas emot på varje interface om inte kortet kan avkoda flera kanaler. På vissa interface tas en kanal emot och på andra fyra-fem stycken.

Konfigureringen av kanalerna och interfacen i iXanonservern görs via Secure Shell (SSH). iXanon tillhandahåller några program för att söka efter kanaler. De är dvbtskan för marksända nätet (DVB-T) och dvbsscan för satellit (DVB-S). (I framtiden kommer all konfigurering att ske via webgränssnittet men för tillfället har det lösts på det här sättet.)

Via webgränssnittet ses exakt vilka kanaler som finns på varje interface, vilken multicastadress varje kanal sänds ut på samt hur mycket bandbredd den tar (uppdatering var 5:e sekund).

6. Säkerhet och "Conditional Access"

Conditional Access (CA) = Skydd av innehåll genom att begära att särskilda kriterier uppnås innan tillåtelse ges, s k villkorad access. Detta används för att skydda data från att spridas fritt.

Acreo använder idag ett CA system som heter Latens. Detta system sköter krypteringen av IP-strömmarna, använder sig av mjuka nycklar och har stöd för ETSI-standarden Simulcrypt¹.

Krypteringen görs genom att multicastströmmen med aktuell kanal krypteras via en Stream Encryption Engine (SEE) och sänds ut i nytt format på en ny multicastström. Dekrypteringen av kanalen sker i STB hemma hos kunden. STB måste således vara registrerad i systemet som en godkänd STB, annars kommer ingen dekryptering att ske. Om det handlar om VoD används istället en VoD Encryption Engine (VEE), som gör samma sak som en SEE fast inte i realtid. Där sker omkrypteringen innan materialet läggs upp på VoD-servern. Sedan hämtar man det krypterade materialet vid behov.

För tillfället måste varje STB läggas in manuellt i Latens. Där skrivs MAC-adressen på STB in och vilka behörighetsbevis (entitlements) den ska ha. Entitlements är en form av kanallista som säger vilka kanaler varje STB har tillåtelse att dekryptera och visa.

Systemet använder sig av "mjuka nycklar", vilket innebär att kunden inte behöver ha ett s k Smartcard i sin box.

Anledningen till att det görs på detta sätt är att uppgraderingar går mycket smidigare och hanteringen av kort undviks. När krypteringsnyckeln görs om, görs det i mjukvaran och kommer automatiskt till boxen vid omstart. Dessutom blir systemet säkrare eftersom nya nycklar sänds ut oftare och således inte hinner knäckas. I Latens CA-system genereras nya nycklar var 10:e sekund.

För att administrera hela systemet finns en CA Manager där boxar och kanaler läggs in och grupperas för distribution till kunder.

För en djupare förståelse för hur Latens som system fungerar, se vidare i dessa dokument:

Latens_CAS_OAM_rel3.0
Encryption Overview Rev2

¹ Se Uttryck i IPTV-världen på sidan 15

7. Funktion hos ”middleware”

Middleware är ett system som sammanfogar andra system till en enhet. Det kan kallas ett lim mellan andra mjukvarukomponenter.

Middleware kan ses som det ”centrala nervsystemet” i basboxmiljön. Acreo har för tillfället Northport som leverantör av middleware.

I middleware måste alla kanaler läggas in och sorteras upp i paket som sedan distribueras till kunderna. Dessutom måste alla STB registreras här med sina MAC-adresser. Om en STB inte finns registrerad i middleware visas ett meddelande vid uppstart som säger att kunden ska ta kontakt med sin leverantör.

Acreo har valt Northports middleware som heter Modulation, eftersom det tillåter att man har olika fabrikat av STB vilket är ett grundkrav för basboxmiljön. Northports gränssnitt mot STB (Hardware Abstraction Layer (HAL)) anpassas efter de olika boxarna och utjämnar skillnader i t ex browser och javascript API. Detta gör att STB ser likadana ut ur tjänsteleverantörernas (TL) synpunkt. Det underlättar för TL eftersom de inte behöver anpassa sin produkt till olika STB.

Andra anledningar till valet av middleware är att TL är separerade från varandra och att de får tillgång till ett gemensamt API-gränssnitt.

8. Portalfunktionen

Portalen är en del av middleware och kan ses som användargränssnittet.

Detta gränssnitt kan skräddarsys för varje enskild kund. Via portalen får kunden tillgång till de olika tjänsterna.

I Acreos portal som finns tillgänglig för test finns följande funktioner:

- TV
 - TV-Nära tjänster
 - Tjänster
 - Abonnemang
 - Inställningar
 - Informationssidor
 - Hjälp
-
- **TV** är precis som titeln säger. Tryck på OK eller TV-ikonen på fjärrkontrollen för att se TV.
 - **TV-Nära tjänster** är t ex Electronic Program Guide (EPG) som är en programtablå över vad som sänds på TV just nu och vad som ska komma. Det finns även en demonstration av avancerad EPG. Denna visar upp sex kanaler samtidigt. Det finns Paus-TV där en bild eller ett videoklipp (t ex en brasa) kan väljas för att ha som tavla när ingen använder TV-apparaten. Här finns även tillgång till Internet.
 - **Tjänster** är olika tjänster som ett antal tjänsteleverantörer bidrar med. Det är t ex spel, filmer, dokumentärer och ljudböcker.
 - **Abonnemang** är hantering av inställningar för abonnemang.
 - **Inställningar**: Här ställs bildformat in, språk väljs och ljud ställs in m m. Här kan även information om systemet och nätverket ses.
 - På **informationssidorna** kan vilken information som helst ges, men i Acreo portal finns det information om Acreo, Fiber Optic Valley och andra företag och organisationer som Acreo samarbetar med.
 - Under **Hjälp** ska man få det som namnet anger.

9. Set-Top Boxen

En STB är med avsikt enkel i sin funktionalitet. Den innehåller en webbläsare och får all sin information via portalen. Bootservern för STB tillhandahåller dess operativsystem och styr hur den ska starta. Det är via servern som den får sin första sida, vilka ikoner som ska visas och deras funktioner. Själva uppstartsfilerna konfigureras via terminalfönster direkt på servern. Inom Acreos testbädd används för tillfället tre olika STB; Kreatel (Motorola), Amino och Tilgin.

Det är Set-Top boxen som identifieras mot CA-systemet och middleware så att alla kanaler kan ses. Detta görs genom att STBns MAC-adress registreras både i Modulation och i CA-systemet samt tilldelas olika entitlements (se avsnittet om kryptering).

Olika modeller av STB har olika funktionalitet. Som exempel kan nämnas de Kreatel (Motorola) boxar som finns i Acreos testbädd. Modell 1510 visar vanlig TV. Modell 1550 kan dessutom visa HD-TV med MPEG2 kryptering och 1910-modellen HD-TV med MPEG4 kryptering.

Vilka system som STBn har kontakt med syns i bild 2.

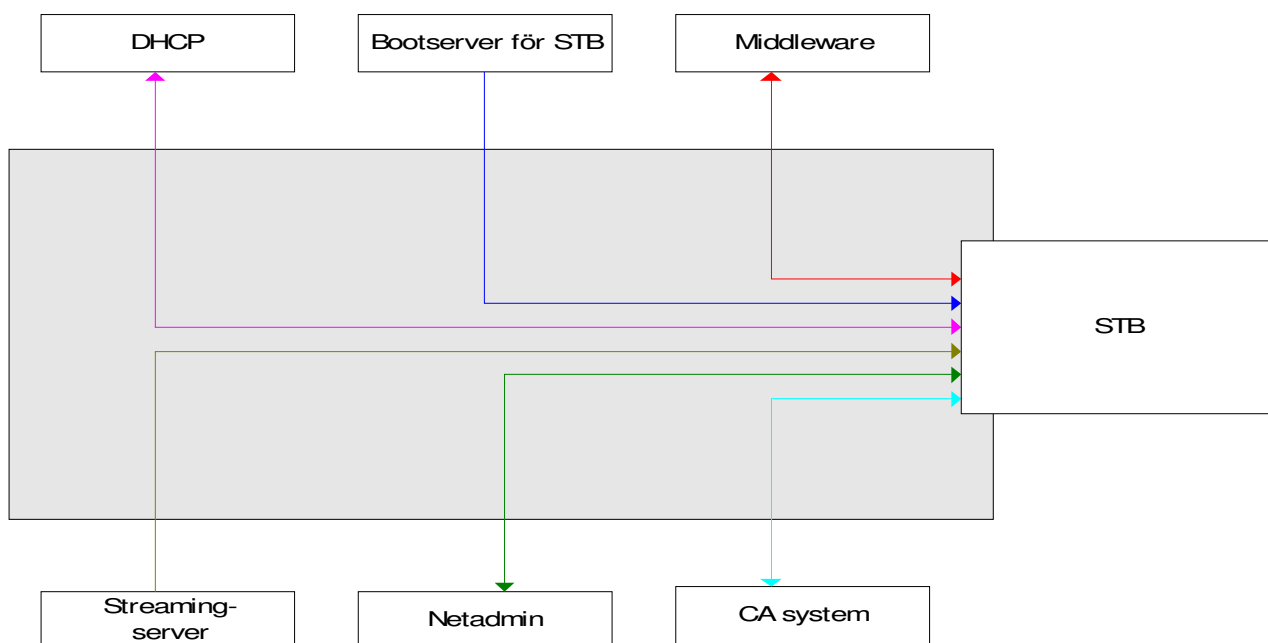


Bild 2: In- och utströmmar till/från en STB. STB har envägskommunikation med Bootservern och Streamingservern, då dessa bara sänder information till STB. Det grå fältet är nätet.

10. Provisioneringssystem

Provisioneringssystemet finns för att sammanlänka olika ekonomiska och administrativa uppgifter.

Genom ett sådant system ska det administrativa arbetet som nu utförs för hand i hög utsträckning automatiseras. Det ska fungera så att kunden kan gå in i en affär och köpa en STB, den registreras på kunden och registrering sker automatiskt i både Latens och Northport. Dessutom ska faktureringsystemet automatiskt kopplas in. Detta gör att när kunden kommer hem och kopplar in sin STB i nätet ska allt fungera.

Det provisioneringssystem Acreo använder idag är NETadmin.

Här är deras egen definition av provisionering:

”The process of providing users with access to data and technology resources. Provisioning can be thought of as a combination of the duties of the human resources and IT departments in an enterprise, where users are given access to data repositories or granted authorization to systems, applications and databases based on a unique user identity, and users are appropriated hardware resources, such as computers, mobile phones etc. The process implies that the access rights and privileges are monitored and tracked to ensure the security of an enterprise's resources.”

11. Anslutning till Acreos referensplattform

För att få ut basboxmiljön till stadsnäten så att de kan testa miljön, krävs ett kontrollerat sätt att koppla ihop IP-nät för utbyte av tjänster.

I vårt fall kallas denna Basbox IX (Ip eXchange), är av märket Cisco och finns placerad i Operatörshotellet (OPH) i Guldsmeden, Hudiksvall. Dessutom finns det en i Stockholm, på Tulegatan hos Stokab.

Mot denna kopplar stadsnäten upp sig och får sedan åtkomst till Acreos basboxmiljö. För att få koppla upp sig måste ett antal krav uppfyllas. Bland annat måste protokollen BGP och MSDP implementeras och vissa IP-adresser låsas.

Med dessa Basbox-IXar kan 24 stadsnät kopplas upp (tolv från Hudiksvall och tolv från Stockholm).

Den mjukvara som är installerad på Basbox IXarna heter METROIPACCESS och ger den funktionalitet som behövs för att sända strömmande media.

Säkerhetsmässigt ges skydd på tre nivåer: kund-, switch- och nätverksnivå. På kundnivån behövs olika system som hindrar kunder att störa varandra, medvetet eller omedvetet. Switchen behöver skyddas från attacker utifrån och nätverket från att okända IP-adresser försöker ta sig in m m.

För mer detaljer kring hur inkopplingen till Acreos basboxmiljö går till, se detta dokument: "Inkoppling till Acreos Basbox IX" av Rickard Lindström 2007-03-01

Hur flödet ser ut visas i bild 3.

Basbox referensplattform med Basbox IX

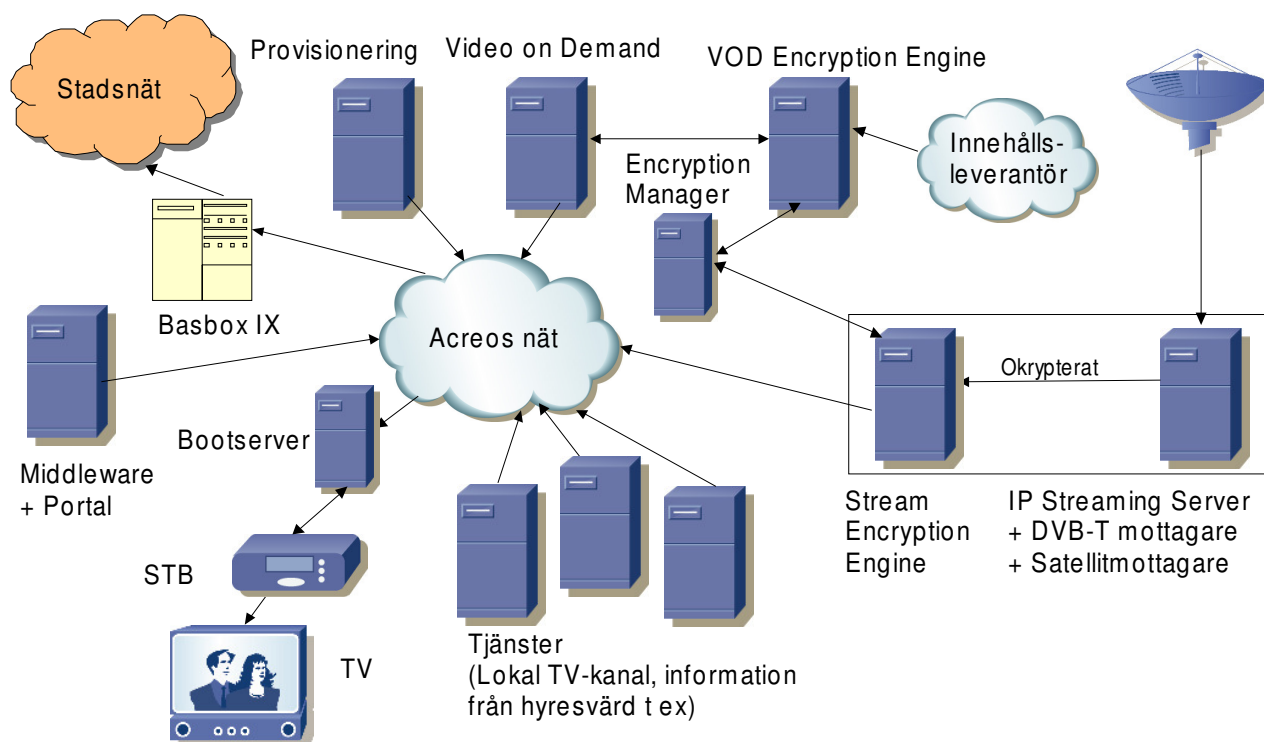


Bild 3: Krypterade kanaler kommer från Stream Encryption Engine, krypterad VoD via VoD Encryption Engine samt tjänster från olika leverantörer. Provisionering, middleware och portal förs in i Acreos nät. STB loggar upp sig mot en bootserver och tar sedan emot signalerna från nätet och sänder dem vidare till TV. Via Basbox IX kopplas stadsnäten in och kan få tillgång till Acreos portal.

12. Systemspecifikation²

Streamingsserver:

iXanon dvbstreamerd version 1.1.6

Middleware:

Northport Modulation v 1.8.0

Portal:

Northport Modulation v 1.8.0

CA-System:

Latens v 1.0

Bootserver:

Motorola Infocast Server v1.15

Provisioneringssystem:

NETadmin v 8.1

Set-Top box:

Motorola 1510 version 3.2

1550 version 3.2

Utgångsport:

Basbox IX: Cisco ME3400

Mjukvara: Cisco IOS Software, ME340x Software (ME340x-METROIPACCESSK9-M), Version 12.2(35)SE2, RELEASE SOFTWARE (fc1)

Protokoll: BGP ver 4
MSDP

Video-On-Demand

Bitband

² Giltig 2007-05-02

13. Uttryck i IPTV-världen

Triple-play	Ett uttryck som används för att benämna en pakettjänst innehållande: IP-telefoni, bredband och IPTV
Middleware	En mjukvara som fungerar som en mellanhand och länkar samman andra system
Portal	Det gränssnitt som är synligt för kunden. Ligger ovanpå ett middleware
MPEG-2	En standard för komprimering av digitalt ljud och bild. Den standard som används på alla DVD:er samt för överföring av video via satellit. Fungerar bättre än den tidigare standarden MPEG-1 vad gäller högre bithastigheter (över 2 Mbit/s)
MPEG-4	En ännu mer flexibel standard som är designad för att stödja alla de möjligheter som nu erbjuds med IP-baserade tjänster. Kallas även H.264 och finns i flera varianter. H.264-AVC komprimerar ungefär dubbelt så bra som MPEG-2. (4 Mbit/s med MPEG-2 ger 1.8 Mbit/s med MPEG-4)
Blu-ray	Ett format för digital lagring av video och spel. Använder sig av blå laser i stället för röd som vanliga DVD-läsare gör, vilket gör att data kan komprimeras mer och det får plats mycket mer data på en skiva.
HD-DVD	Konkurrent till Blu-ray ovan och fungerar på ungefär samma sätt
PVR	Personal Video Recorder. Video utan band. Man spar till en hårddisk istället. Termen inkluderar också fristående STB och mjukvara för PC som möjliggör in- och uppspelning till och från en disk.
DVR	Digital Video Recorder. Samma som PVR.
MUX	Multiplex. Gruppering av kanaler och strömmar. Varje MUX är en kanal med inbäddade bild- och ljudfiler, eventuell textning och andra medskickade strömmar (som till exempel EPG).
Multicast	Att skicka en enda mediaström som sedan delas upp i en router och sänds till intressenter.
Simulcast	Att skicka samma mediaström med olika kodningar samtidigt. T ex att skicka TV-signalen både analogt och digitalt.
Simulcrypt	Innefattar dels att konsumentens mottagare kan förstå och hantera olika system för villkorad tillgång, dels att programbolag kan kryptera programsignalen med parallella system för villkorad tillgång vid utsändning.
Head End	Den plats där all hårdvara som behövs för att sända ut IPTV finns.

14. Förkortningar

DVB-S	Digital Video Broadcasting – Satellite (standard för digital television)
DVB-T	Digital Video Broadcasting – Terrestrial (standard för marksänd television)
STB	Set Top Box
VoD	Video on Demand
CA	Conditional Access
IP	Internet Protocol. Det protokoll som används på Internet
VLC	VLC Media Player, en gratis mediaspelare för PC (förkortningen stod en gång för VideoLan Client men det gäller inte längre)
CA modul	Conditional Access Module, en kortplats i digital-TV-mottagaren (streamingservern) som är avsedd för programkort innehållande ett specifikt programpaket
SEE	Stream Encryption Engine (kryptering i realtid)
VEE	VoD Encryption Engine (kryptering för senare utsändning)
EPG	Electronic Program Guide
FTA	Free-To-Air, okodade kanaler som är fria att sända. Te x BBC World, SVT-kanalerna och TV4
SPA	AB Svensk Programagentur
BGP	Border Gateway Protocol är ett routingprotokoll som används för att binda samman IP-nät
MSDP	Multicast Source Discovery Protocol: Syftet med MSDP är att separera olika domäner från varandra och göra nätet mer robust. Varje nät blir en egen värld som har koppling till alla andra, men klarar sig själv
ETSI	European Telecommunications Standards Institute. Ett europeiskt standardiseringsorgan
HD-TV	High Definition TeleVision, högupplösnings-TV, TV-sändning med bättre bildkvalitet
DHCP	Dynamic Host Configuration Protocol: det protokoll som delar ut IP-adresser och annan nödvändig information till nya klienter på ett nätverk
API	Application Programming Interface. En uppsättning subrutiner, protokoll eller funktioner som program kan anropa för att utföra någonting
HAL	Hardware Abstraction Layer. Den del i operativsystemet som sköter kommunikationen mellan hårdvara och applikationer
MAC-adress	Media Access Control. En unik identifierare som varje enhet som har kontakt med ett nätverk har. T ex har varje nätverkskort och varje STB en unik MAC-adress