ISDP System Overview

With Focus on the ISDS Server and ISDP Client

Please Read

Important

Please read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

Notices

Trademark Acknowledgements

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at **www.cisco.com/go/trademarks**.

CableLabs and DOCSIS are registered trademarks of Cable Television Laboratories, Inc.

CableCARD, OCAP, and OpenCable are trademarks of Cable Television Laboratories, Inc.

DVB is a registered trademark of the DVB project.

Other third party trademarks mentioned are the property of their respective owners.

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1009R)

Publication Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing or later issued patent.

Copyright

Contents

About This Guide

Introduction

This guide provides a high-level description of the IPTV Services Delivery Platform (ISDP) service offering and provides a more detailed description of the ISDS server, Application server, and ISDP client functions.

Purpose

The purpose of this guide is to provide the following information:

- The basic concepts of the ISDP solution
- The types of applications and services supported by ISDP
- An understanding of how various hardware and software elements interact to provide IPTV services.

Scope

This guide provides only high-level descriptive information that applies to ISDP. This document does not describe how to install, configure, operate, maintain, or troubleshoot an ISDP. For more detailed descriptions, contact Cisco Services.

Audience

This guide is written for the following audiences:

- System operator marketing managers who are responsible for determining how service offerings should be packaged
- ISDP system administrators
- ISDP operators
- Cisco Services engineers
- Developers designing applications and services for the ISDP
- Other parties interested in gaining a general knowledge of ISDP

For More Information

This reference table includes a list of World Wide Web (WWW) links to technical publications containing useful information for digital systems. The links are listed alphabetically by company or feature name.

Company or Feature	Link
Widevine Technologies	www.widevine.com
ANT	***www.antlimited.com*** (http://www.scte.org)

Document Version

This is the second release of this guide

1

Introducing the ISDP Solution

Introduction

This chapter provides a brief introduction to the ISDP solution and its key components. This chapter also includes an overview of the services and benefits that the ISDP solution provides.

In This Chapter

What Is the ISDP Solution?

The IPTV Service Delivery Platform (ISDP) provides a high-performance, open architecture solution that is capable of delivering a wide range of advanced video applications using the Internet Protocol (IP) as the common communication method. Unlike other delivery methods, IP streaming enables service providers to evolve their networks over time to enable the full, connected experience of many services to many screens.

The following sections describe three basic approaches service providers can take in configuring the ISDP solution: two reference architecture approaches or a custom approach.

Reference Architecture Approaches

To facilitate the deployment of an open-architecture ISDP solution, Cisco Systems, Inc. (Cisco) has formed partnerships with other leaders in information and communications technologies. The result of this partnership is ISDP 1.0, the first release of our ISDP solution. ISDP 1.0 supports either of the following architectures:

- Standalone reference architecture
- Regional Control System (RCS) reference architecture

Standalone Reference Architecture

An ISDP standalone reference architecture supports a centralized video network.

- Cisco provides the following elements for the standalone reference architecture:
  - Video compression and encoding
  - Broadcast content grooming
  - IP streaming
  - Content delivery of Video on Demand (VOD) content to the edge network
  - Video quality control
  - System control
  - Set-top control and user experience with the reference TV navigator (RTN)
- Widevine Technologies supplies conditional access and digital rights management (DRM) for VOD content.
- Tandberg Television provides Operations Support System/Business Support System (OSS/BSS) interfaces for VOD asset management.

RCS Reference Architecture

The same partnership that provides the standalone reference architecture also provides the RCS reference architecture. The key difference is that the RCS architecture allows for central control of remote IPTV headend sites.

Service providers can begin by deploying a standalone architecture and evolve the platform over time to an RCS design as their needs change. The ISDP RCS architecture can be deployed in either of the following models:

- **Customer-operated data center** - This configuration is ideal for large systems that provide a mix of services to multiple communities. Systems with a preference for centralized management may also find this a good solution.
- **Cisco Services-managed Network Control Center (NCC)** - This configuration is a good choice for smaller systems with a goal of reducing initial capital expenses, systems that have limited operational resources for daily system management and monitoring tasks, or sites that want highly available architectures and do not want to carry the expense of these advanced configurations.

Custom Architecture Approach

The reference architectures described above illustrate two of several possible implementations for the ISDP solution. These approaches currently represent a more readily available architecture.

Alternatively, the custom architecture approach offers service providers even more flexibility by allowing them to select their own products to fulfill the following requirements of the ISDP solution:

- Control of the user experience and presentation of services (set-top client)
- Content distribution
- Conditional access
- VOD asset management (optional, required only for service providers who wish to offer VOD service)

Why Implement the ISDP Solution?

The ISDP solution allows video, voice, and data to be delivered to subscribers over an all-digital architecture that uses IP as its common communication method.

By using IP as the communication method, you can reliably deliver the standard- and high-value services that subscribers expect and also position your business to provide next-generation, mobility services available on many different devices. The ISDP solution also provides you with the benefits of its open, standards-based design and its reliable, scalable entertainment-grade network.

By implementing the ISDP solution, you can meet both current demands and fulfill new opportunities with a flexible, efficient, and high-performance network.

Foundation Services

The ISDP solution is designed to help you enter the market with the following high-quality "foundation" IPTV services:

- Basic broadcast formats
  - Standard-definition television (SDTV)
  - High-definition television (HDTV)
- Secure broadcast
  - Security with encryption and conditional access
  - Package channel plans and premium tiers, such as HBO
- Program guide
  - Software components to acquire, store, and distribute program guide data
  - Deliver using IP multicast
- Set-top based digital video recorder (DVR)
  - Manipulate live TV (pause, reverse, or fast-forward)
  - Record programs for local storage on the DVR hard drive
- Video on Demand (Optional)
  - Deliver the VOD catalog by IP multicast
  - Provide conditional access for channel application
  - Manage authorizations with VOD back office

- Emergency Alert Services (compatible with U.S. requirements)
  - Deliver emergency alert messages from the U.S. Federal Communications Commission (FCC), National Weather Service, and local authorities
  - Perform weekly and monthly tests of the U.S. Emergency Alert System (EAS)
- By using open APIs, you can deploy the following future services:
  - Games and web-based applications/portals
  - Multi-Room™ DVR (MR-DVR), which allows subscribers to extend the power and control of DVR to as many as four televisions in the home
  - Network digital video recorder (nDVR), which allows subscribers to record programming that is stored on the network instead of storing it locally on the DVR hard drive
  - Advanced client-based DVR, which allows subscribers to record programming remotely, such as from a personal computer (PC), instead of from the DVR
  - On-screen caller ID

Next-Generation Services

As your network evolves, you can offer a full, connected experience by extending services to the following devices so that subscribers can receive content wherever and whenever they desire or transfer content between the following devices:

- Personal computers (PCs)
- Mobile handsets
- Other rich-media-capable devices

Benefits

To ensure your success, our ISDP solution offers the following advantages:

- **Extreme scalability** - achieves built-in scalability using the same IP networking concepts that allow the Internet to efficiently scale from a few users to millions of users
- **Exceptional network efficiency** - employs a unique hierarchical storage design that allows carriers to maintain huge content libraries, while simplifying content storage management
- **Nonstop service availability** - advanced failover capabilities provide continuous video service, without service interruption to subscribers

- **Unmatched flexibility** - supports centralized (standalone) and distributed (RCS) networks equally effectively; service providers can begin by deploying in a standalone manner and evolve the platform over time to a RCS design
- **Rapid service velocity** - uses a modular software that employs industry-standard designs and published application programming interfaces (APIs) that allow service providers to continually evolve and incorporate new services and capabilities without complex redesigns or service outages

2

Overview of the ISDP Solution

This chapter provides an overview of two different configurations of the ISDP reference architecture:

- ISDP Standalone configuration
- ISDP Regional Control System (RCS) configuration

In This Chapter

ISDP Standalone Reference Architecture Overview

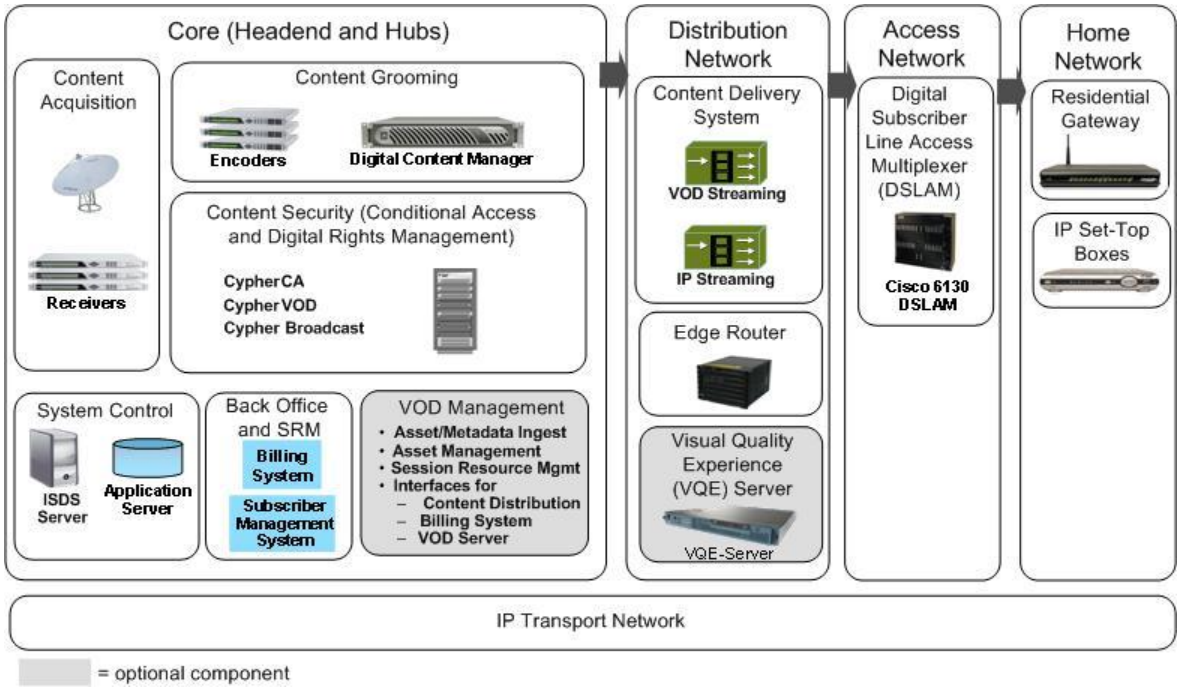
This section provides a diagram of the ISDP standalone reference architecture and describes the following major hardware components that support it:

Note: The ISDP RCS reference architecture is described later in this chapter.

- Cisco Integrated Receiver Decoders
- Cisco Encoders
- Cisco Digital Content Managers
- Cisco IP Streamers for Broadcast Content
- Cisco ISDS Server
- Cisco Application Server
- Cisco PowerKEY® Conditional Access System (optional)
- Widevine Technologies' Cypher Conditional Access System:
  - Cypher CA Core Server
  - Cypher CA EMMG Server
  - Cypher Broadcast Server
  - Cypher VOD Server
- VOD System:
  - Tandberg Catcher
  - Cisco Content Delivery System (CDS): CDS Manager and Vault and Streamer Arrays
  - Cisco CDS Streamer Arrays
  - Tandberg Business Management Server (BMS)
  - Cisco VOD Navigation Server
- Third-party external applications and interfaces, as required by the business needs of each service provider
- Cisco Edge Routers
- Cisco Visual Quality of Experience (VQE) Server (optional)
- Cisco Digital Subscriber Line Access Multiplexers (DSLAMs)
- Cisco Residential Gateways
- Cisco IP set-tops

ISDP Standalone Reference Architecture

The following diagram provides an overview of major system components along with their respective locations in the reference ISDP standalone architecture.



Core: Headend Components

The ISDP Core includes all headend components. The following table gives a high-level description of the components found in the ISDP Core network:

Content Acquisition

Components	Description
Integrated Receiver Decoder (IRD)	The receiver portion of the IRD receives a satellite signal by tuning to a single transponder frequency. The decoder takes a compressed/encoded video stream and outputs the raw, uncompressed stream. A decoder is typically used if the stream needs to be re-encoded with a more aggressive encoding scheme, or even a more aggressive version of the same encoding scheme. If re-encoding is necessary, the decoder will decode the delivered stream and pass the uncompressed stream to an encoder for re-encoding. **Note:** Because the receiver tunes to a single transponder frequency, one receiver is typically used for each transponder that contains needed content.

Content Grooming

Components	Description
Encoder	Encoder models **D9034-S** and **D9054 HDTV** advanced compression encoders are excellent choices for the ISDP solution. These encoders use advanced video-compression technologies to compress content so that a better picture quality is delivered while consuming less bandwidth.
Digital Content Manager	The **Digital Control Manager (DCM)** conditions content and processes the signals into the correct formats and to include the desired services.

System Control

Components	Description
ISDS Server	The ISDS server provides much of the video application infrastructure in an ISDP system. There is generally one ISDS (plus backup) in a standalone system. The ISDS software platform consists of the following elements: ■ Sun Solaris (UNIX-based) operating system ■ Informix relational database management system ■ X-Windows, OSF/Motif-based graphical user interfaces ■ Aprisma Management Technologies SPECTRUM enterprise management system **ISDP RCS:** When an ISDP RCS reference architecture is deployed, an RNCS server and backup are required in each remote headend. (The RNCS server is occasionally referred to as a LIONN server.)
Application Server	The Application server is an adjunct server to the ISDS which provides interactive program guide (IPG) ingest services for ISDP.

Content Security (Conditional Access and Digital Rights Management)

Components	Description
Widevine's Cypher Conditional Access (CA) System	Conditional Access for ISDP is performed using Widevine's solution, *Cypher*. Cypher system ensures that content can only be viewed by authorized subscribers. The Cypher CA system typically requires five physical servers that fulfill various roles in the CA system: ■ **Cypher CA Core server** - Provides key management, set-top key provisioning, session-key generation and Entitlement Control Messaging (ECM) generation. (Keys are used to encrypt and decrypt digital services. ECMs are specific to a particular video broadcast stream or VOD asset.) ■ **Cypher CA EMMG server** - Generates Entitlement Management Messages, or EMMs. (An EMM is used to provide keys that can only be decrypted by a specific subscriber.) ■ **Cypher EIM server** - Provides an interface to the subscriber management system and the ISDS. ■ **Cypher Broadcast server** - Provides real-time broadcast content encryption, control word (CW) generation, and ECM embedding. (A CW is one of the three keys that Cypher uses to protect and decrypt content.) ■ **Cypher VOD server** - Encrypts VOD assets during the ingest process, generates CWs, and embeds ECMs.
PowerKEY CAS (Optional, only for use in a custom architecture.)	In addition to the Cypher CA system used in an ISDP reference architecture, the ISDS also includes the PowerKEY® CA system. PowerKEY CA is the native CA of the ISDS and is available to service providers who choose to deploy an ISDP custom architecture. PowerKEY CA ensures that only approved subscribers and set-tops receive content in a readable format from the network. PowerKEY CA also provides digital rights management (DRM) to protect content once it is in a subscriber's home to ensure that the content is copied according to the copy control information assigned to the content.

Components	Description
PowerKEY CAS (Optional, only for use in a custom architecture.), continued	The PowerKEY CAS interfaces with the following components of the PowerKEY CAS: ■ **Transaction Encryption Device (TED)** - The PowerKEY TED is responsible for set-top key management. The TED is an EMM Generator (EMMG) that uses set-top public keys and generates entitlement messages for set-tops. PowerKEY EMMs are delivered to the set-top devices over an out-band channel. PowerKEY Conditional Access System Gateway (PCG) performs real-time PowerKEY entitlement control Message (ECM) generation and distribution. ■ **PowerKEY Conditional Access Gateway (PCG) server** - PCG is a server that performs real-time PowerKEY ECM generation. The PCG is a DVB® SimulCrypt compliant ECM Generator (ECMG). ■ **PowerKEY Encryption Server (PKES)** - The VOD content is encrypted by the PKES in a manner that is similar to PowerKEY's session-based encryption solution. However, under PowerKEY's session-based encryption solution, each time someone orders an event, a new encryption key is generated. That encryption key is used once by the subscriber and then never used again. For the pre-encryption solution, implemented by the PKES, the entire VOD library is assigned a single entitlement ID. Set-tops are then authorized and de-authorized for VOD assets through standard PowerKEY EMMs. ■ **Harmonic ProStream encryptor** - The PowerKEY CAS management encrypts content using the Harmonic ProStream encryptor to provide real-time scrambling of broadcast services. (PKES provides the pre-encryption scrambling function for VOD services.) ■ **Session Resource Manager (SRM) module** - The ISDS SRM module keeps track of all the session information in a database and informs the PowerKEY CA module whenever a session is created, deleted, or queried. The SRM module processes requests for session creation or deletion and routes the CA requests, such as requests to deliver ECMs, to the appropriate modules.

Back Office and Session Resource Manager

Components	Description
Operations Support System/Business Support System (OSS/BSS)	**Tandberg OpenStream BMS** - Performs the core of the VOD backoffice functions. It acts as a metadata repository, performs entitlement checks, activates and retires content, interfaces to the billing system, and provides historical purchase data for reporting. A software application called the Enterprise Session Resource Manager (eSRM) is responsible for VOD session setup. When a subscriber selects a VOD asset for purchase, the Tandberg VOD client sends a session setup request to the eSRM using real time streaming protocol (RTSP). Then the eSRM coordinates the allocation of server and network resources and the user is authenticated through the billing system. The eSRM also communicates with the CA system resulting in the necessary EMM being delivered to the set-top for decryption of the specific asset stream.

VOD Management

Components	Description
VOD System **Note:** A VOD System is included as part of the ISDP Reference Architecture.	The VOD system handles all the following components to deliver movies on demand and subscription VOD services. ■ **Tandberg Catcher** - Receives VOD content from satellite or terrestrial links. It encrypts the content and transfers it to the VOD server. (This process is called VOD ingest). ■ **Cisco CDS Vault Arrays** -The vault stores all the VOD assets until they expire. Vaults are always deployed in a redundant configuration (minimum of two appliances) called a vault array. All vaults in an array automatically mirror content among themselves. The vault serves up content in blocks to the streamer. ■ **Cisco CDS Manager -** A browser-based application for administering configuration, monitoring, and reporting for all content distribution engines network-wide. CDS Manager is usually located in the headend ■ **Cisco VOD Navigation Server** - Keeps track of titles and metadata and presents the catalog for subscribers. (Metadata provides information about the movies such as actors, year, and ratings.)

Components	Description
Third-Party Applications **Note:** Other third-party applications and interfaces can be deployed according to the needs of each service provider.	Each service provider can install additional applications and data that are provided and installed by third-party vendors. Applications and data most commonly provided by third-party vendors include the following: ■ Billing Systems ■ IPG Data ■ Emergency Alert System (required in the United States) ■ Network Management System

Distribution Network Components

The following table gives a high-level description of the components found in ISDP Distribution network:

Components	Description
Content Delivery System ■ VOD streaming ■ IP streaming	In the ISDP reference architecture that is used as an example in this guide, the **Cisco Content Delivery System (CDS)** is used to aggregate, store and distribute VOD content to the edge router for the set-tops to access. Currently, the CDS is not used for broadcast content. The CDS consists of the following components: ■ **Cisco CDS Streamer Arrays** - The stream provides the actual media stream along with stream control to the set-top. The streamer acts as a multistage cache for content. Instead of requesting entire assets from the vault, the streamer uses a cache-fill algorithm to the request 64k blocks from the fault. ■ **Cisco Continuum DVP™ Advanced Headend Processor model D9655 IP Streamer** -Allows distribution of a multiple program transport stream over a high-speed IP network or backbone toward multiple regional headends or hub sites. It supports both unicast and multicast and has two 1 gigabit Ethernet network interfaces (main and backup). In a reference architecture, the IP steamer is used for broadcast content. It is not used for VOD content.

Components	Description
Edge Router	The **Cisco 7606 Edge Router** is a router used in hubs that serve subscriber homes. When a subscriber served by a hub requests a channel change, the edge router will then send the selected stream to the home and the digital set-top will "join" the multicast session.
Visual Quality of Experience (VQE) Server (optional)	The **VQE Server** (VQE-S) software is hosted on a **Cisco CDE-110** appliance running a standard Linux operating system. The Cisco CDE-110 comes with the required software pre-installed: VQE-S, VQE-S Application Monitoring Tool, Linux, Apache web server, and other software. The VQE server improves the quality of IPTV services and subscribers' viewing experiences. VQE technology detects if packets are missing from a video stream for retransmission or receiver-report services

Access Network

The following table gives a high-level description of the components found in the ISDP Access network:

Components	Description
DSL Access Multiplexer	In the ISDP reference architecture that is used as an example in this guide, the **Cisco 6130** functions as the DSL access multiplexer and provides broadband connections to subscribers. This device is responsible for selecting content from the Distribution Network using standard IP and delivering it to the subscriber using a DSL "last mile" network. DSLAMs work with DSL modems inside subscribers' homes.
Network Router/Switches	The **Cisco 6500 Series** routers act as a router/switch for all of the ISDP traffic, both to and from the set-tops.

Home Network

The following table gives a high-level description of the components found in the ISDP Home network:

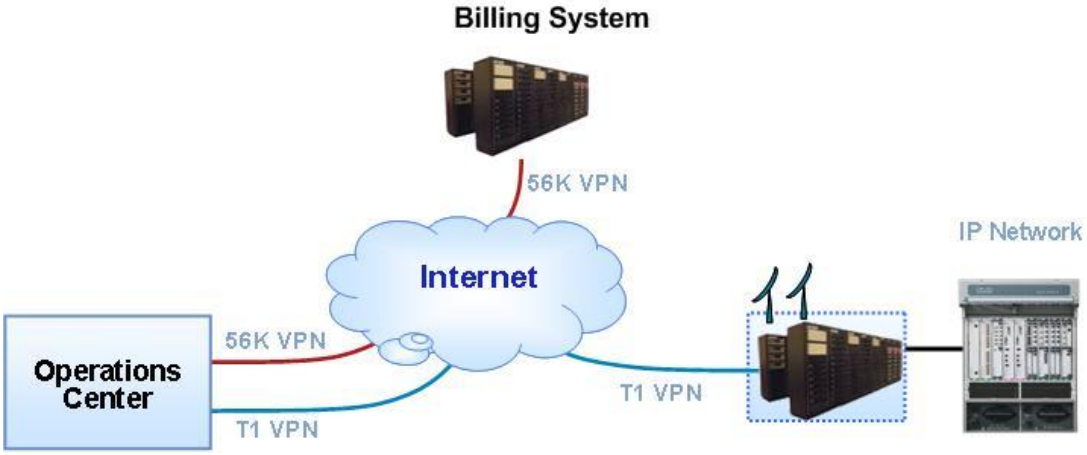
Components	Description
Residential Gateway	Residential gateways connect the home's local area network (LAN) to multiple broadband services, taking advantage of IP network architectures. These devices have integrated IP routing and multicasting, and allow consumers to request access to and receive content from the Aggregate network. Cisco offers two high-performance gateways that integrate a DSL data gateway with an IP-over-Coax adapter, facilitating seamless distribution of data, voice and IPTV within the home: **DDR 2200** and the **DDR 2300**.
IP Set-Tops	Cisco set-tops easily manage the two-way communication that ISDP demands. In addition, they offer flexible and open architecture facilitating seamless integration of the set-tops into an end-to-end IPTV system. They deliver high definition (HD) content, personal video recording capabilities, advanced security solutions, and the ability to stream content to multiple televisions. These IP set-tops support the following high-definition set-top models for North American markets: ■ **CIS330** ■ **CIS430 -** includes a DVR ■ **CIS2000**

Components	Description
IP Set-Tops, continued	ISDP supports the following high-definition set-tops for European markets: ■ **CIS 2001** ■ **CIS 5020** - includes a DVR ■ **CIS 5100** - includes a Digital Video Broadcasting-Terrestrial (DVB-T) tuner ■ **CIS 5220** - includes a DVR and DVB-T tuners **Note:** If the optional VQE server is used, the VQE client is integrated into select Cisco set-tops.

ISDP RCS Architecture Overview

In addition to the ISDP Standalone architecture, the ISDP solution can also be deployed with a Regional Control System (RCS). This configuration allows service providers to control remote headend sites from a central ISDS operations center.

As the following illustration indicates, systems for billing and provisioning connect through a simple 56K VPN, and a T1-equivalent circuit is required for RNCS command and control.



Benefits of the ISDP RCS Solution

The ISDP RCS solution provides a competitive advantage to providers that serve several remote sites across a wide geographical area. By allowing service providers to consolidate management of remote headend sites, operations costs are reduced because the RCS does not require a separate ISDS operator at each remote site.

ISDP RCS Option

The ISDP RCS architecture can be deployed in either of the following ways:

- **Customer-operated data center** - This configuration is ideal for large systems that provide a mix of services to multiple communities. Systems with a preference for centralized management may also find this a good solution.
- **Cisco Services-managed Network Control Center (NCC)** - This configuration is a good choice for smaller systems with a goal of reducing initial capital expenses, systems that have limited operational resources for daily system management and monitoring tasks, or sites that want highly available architectures and do not want to carry the expense of these advanced configurations.

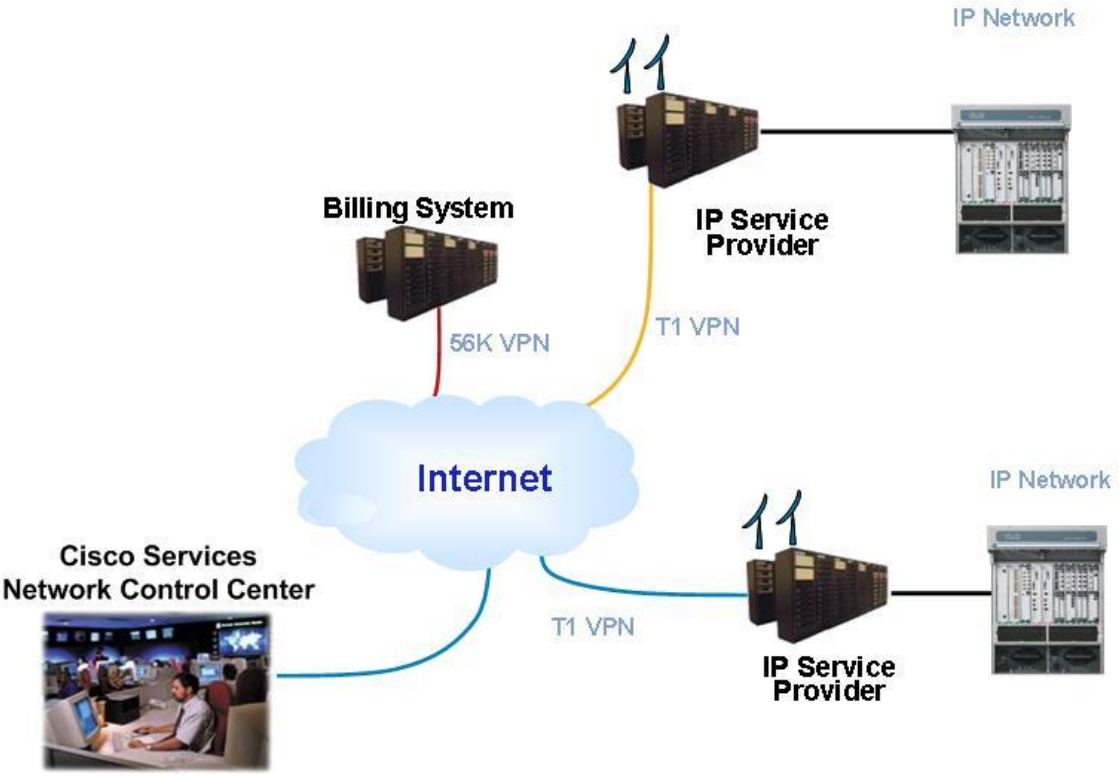
Customer-Operated Data Center Solution

When a customer-operated configuration is deployed, customers are able to manage multiple IPTV headends from an RCS located at the customer's central operations center.

Cisco Services-Managed Network Control Center Solution

When a Cisco Services-managed NCC configuration is deployed, Cisco Services professionals manage multiple IPTV headends from an RCS located at the Cisco Services office in Atlanta, Georgia. Cisco Services provides the technical resources to help customers meet their business and technical needs.

The following figure provides a high-level view of an ISDP RCS solution with the Cisco Services-managed NCC configuration.



Cisco Service professionals at the NCC perform the following operational support services:

- All basic operational tasks
- 24-hour system monitoring
- Change control and system upgrade activities
- 24-hour, year-round emergency support
- Instant-Hit: Re-sends authorization information to a set-top
- Staging-Hit: Re-creates staging information and sends it to set-tops; used for special administrative purposes
- Reboot: Reboots the specified set-top
- View the current packages (authorizations) of a specified set-top
- Verify your billing server is properly sending transactions to the Controller in the NCC

3

Key ISDP Elements

This chapter provides details about the key elements that are at the core of the ISDP solution.

For information on other portions of the ISDP solution, refer to the appropriate vendor documentation.

In This Chapter

Overview of ISDP Software

This section provides an overview of the major software components that support the ISDP solution.

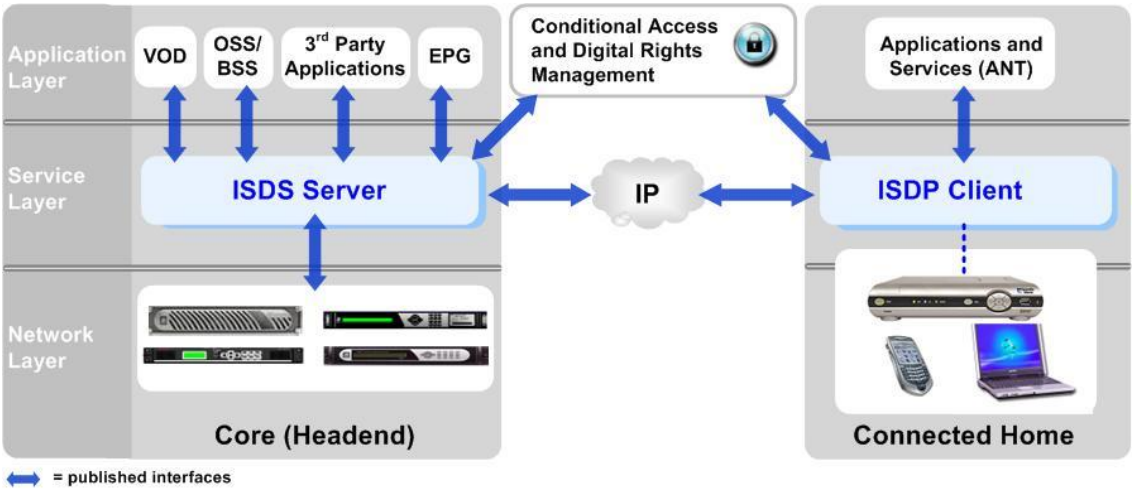
ISDP Software Component Overview

In its most basic description, the ISDP consists of two major software components, which are shown in the Service Layer in the following illustration:

- **ISDS server software** - ISDS software version 1.0 resides on the ISDS server. The ISDS server leverages our experience from years of deploying large cable networks. It is a proven, scalable system that supports millions of set-tops on a single Sun server. The ISDS adds to the DNCS appropriate functions and standards to support IP networks, such as Internet group management protocol (IGMP), unicast, multicast, and so on.

  Note: The ISDP Application server is an adjunct server to the ISDS server. The Application server provides interactive program guide (IPG) ingest services for the ISDP solution.

- **ISDP client software** - The ISDP client operates across a variety of Cisco set-top types from SDV through HDTV to DVR. The client platform provides the necessary foundation to help deliver robustness, reliability, and scalability of the software platform. It enables a range of services layers to be supported thorough a published application programming interfaces (APIs).



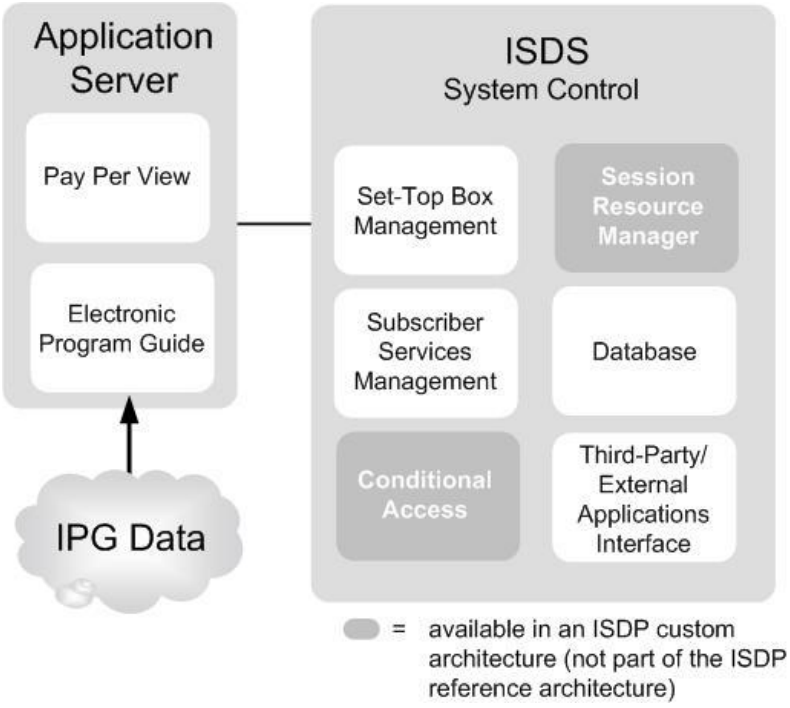
ISDS Server and Application Server Software

The software platform for the ISDS server consists of the following elements:

- Sun Solaris (UNIX-based) operating system
- Informix Relational Database Management System
- X-Windows, OSF/Motif-based graphical user interfaces
- Aprisma Management Technologies SPECTRUM Enterprise Management System
- Apache and Tomcat web servers

Cisco's ISDS Software Approach

The primary function of ISDS is to perform system control for the ISDS. As indicated in the following illustration, the Application server assists with system control. Like the ISDS server, the Application server is a Sun Solaris (UNIX-based) operating system.



ISDS Software Functions

This section describes the following major ISDS software components:

- Set-top management
- Subscriber services management
- Enterprise session manager
- Conditional access
- Database
- Third-party/external applications interface
- Emergency Alert System

Set-Top Management

Set-top management includes sign-on and registration for each set-top in the system, administrative and configuration settings, software downloads (including updates and upgrades), plus diagnostics and logging.

The system uses multiple flows to communicate with set-tops:

- **System-Wide flow** - As the highest level flow, the system-wide flow contains IP names or address of the various video application servers in the system and a code verification table (CVT), which tells the set-tops in the system when to upgrade boot code. All set-tops join the system-wide flow during the boot process and just after the boot process. The system-wide flow resides at a well-known IP multicast address. The IP names or addresses are provided on the system-wide flow using DSM-CC UNConfigIndicator messages.
- **Hub flow** - Provides the system information (SI) table, which contains service parameters for each service in the system. A hub is a logical grouping of clusters across that provide the same tuning information (SI). Each hub-specific flow that an operator defines is associated with a unique multicast IP address. The operator may choose to define one or more SI flows for the system
- **Cluster flow** - The lowest level in the hierarchy is the cluster. A cluster is a collection of IP subnets. The set-tops acquire the address of the site, hub and cluster flows during the registration process (in the UNConfigConfirm message).

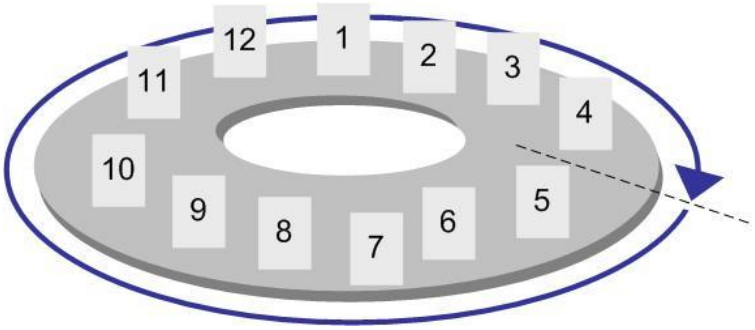
Each set-top is assigned to a cluster, each cluster to a hub, and each hub to a site by the operator in the ISDS. Since there is only one system-wide flow, a well known multicast address is used (224.0.23.42). The Hub and Cluster flows employ user-defined addresses.

Multicast Carousels

The ISDP system needs a way to send configuration and information files needed by the set-top and each video application to millions of set-tops in the system. A mechanism called multicast carousels fills this need by sending files to all set-tops in a system. Multicast carousels use IP multicast to send the same data to many endpoints. The use of IP multicast allows the server to send, and the network to transport, a single copy of each piece of data that can be consumed by any or all set-tops in the system.

The files are presented to the set-top and the video client applications as a virtual file system (called the Broadcast File System or BFS). Presenting the files to the set-top as a virtual file system makes application programming easier because common file access paradigms can be used. The files are separated into groups called carousels. The files in a given carousel are broken into blocks and transmitted with sequence numbers in IP multicast streams. When all blocks in a carousel have been transmitted, the process starts over with the first block. This rotating transmission algorithm, which gives the carousel its name, allows a set-top to join the IP multicast stream corresponding to the carousel at an arbitrary point in time. The set-top need only listen for one rotation cycle (assuming no packets are dropped) to receive all blocks in the carousel.

Consider the simplified example shown in the following diagram. The set-top would know that the carousel had 12 total blocks from the Directory Carousel. If, for example, the set-top joined in the middle of block 4, the set-top would ignore the remainder of block 4 because it cannot receive the full block. The set-top would receive block 5 up through block 12. The carousel would then restart with block 1. The set-top would continue to listen through block 4. Once block 4 is received, the set-top would have received all 12 blocks in the carousel having only had to join the carousel for one complete rotation.



The Broadcast File System provided by the ISDS allows applications to place files on a virtual file system accessible by all set-tops in a system while making the most efficient use of network bandwidth using multicast and placing minimal load on the ISDS and application servers.

NAT/STUN Services

One of the functions of the residential gateway in a typical Service Provider network is to "hide" the customer's home network from the network. This process, which is referred to as Network Address Translation or NAT2, mimics a single end point to the network by rewriting the source IP address in all outbound packets. Since servers outside the home see all devices inside the home as a single IP address, all traffic destined for devices in the home are sent back to the single outside IP address of the gateway. As applications contact servers outside the home, the gateway keeps a mapping table for each flow. The gateway uses the mapping table to ensure that return traffic goes to the correct host inside the subscriber's home.

This causes a problem for the ISDS which must initiate unsolicited flows to set-tops inside the home. Since the ISDS sees all set-tops inside the home as a single IP address and the flow is unsolicited, the gateway has no way of knowing which set-top is the intended recipient of the flow. To allow the gateway to determine which set-top is to receive a specific flow, the ISDS uses a STUN (Simple Traversal of UDP through NATs) server. A STUN server allows the set-top to send a test flow on a specific UDP port number and get a response from the STUN server telling what outside address and port mappings would be used for flows on that port number. The set-top then sends this mapping information to the ISDS with the UNCR registration message.

Subscriber Services Management

ISDP uses both a channel and a walled-garden application paradigm to select services or applications. The ISDS generates a system information (SI) table which contains the mapping of all video applications in the system. Each video application is usually mapped to one or more virtual channel numbers that show up in the program guide. The set-top will obtain this SI table from the ISDS on the hub flow. As the end user selects the various services in the program guide, the set-top uses this mapping to call the various video applications resident on the set-top.

Database

The ISDS keeps a master database for equipment and services used in the ISDP system, including the following:

- Set-top records and authorizations
- Network element records
- Service definitions
- Channel maps
- Package (service tier) definitions
- Mapping of the NATed IP addresses along with the associated NATed UDP/TCP ports and original port of the application in question

Third-Party/External Applications Interface

To give service providers flexibility to differentiate their services, applications and data provided and installed by third-party vendors can be part of the ISDP reference architectures or the custom architecture. Interfaces for the following applications are typically included as part of the ISDP solution:

- Billing Systems
- IPG data for populating the guide
- Emergency Alert System (EAS), required in United States
- Network Management System (NMS)
- VOD

  Note: The ISDS includes interfaces to Tandberg Television's OpenStream platform for both ISDP reference architectures. For the ISDP custom architecture, the ISDS includes interfaces to the selected VOD platform.

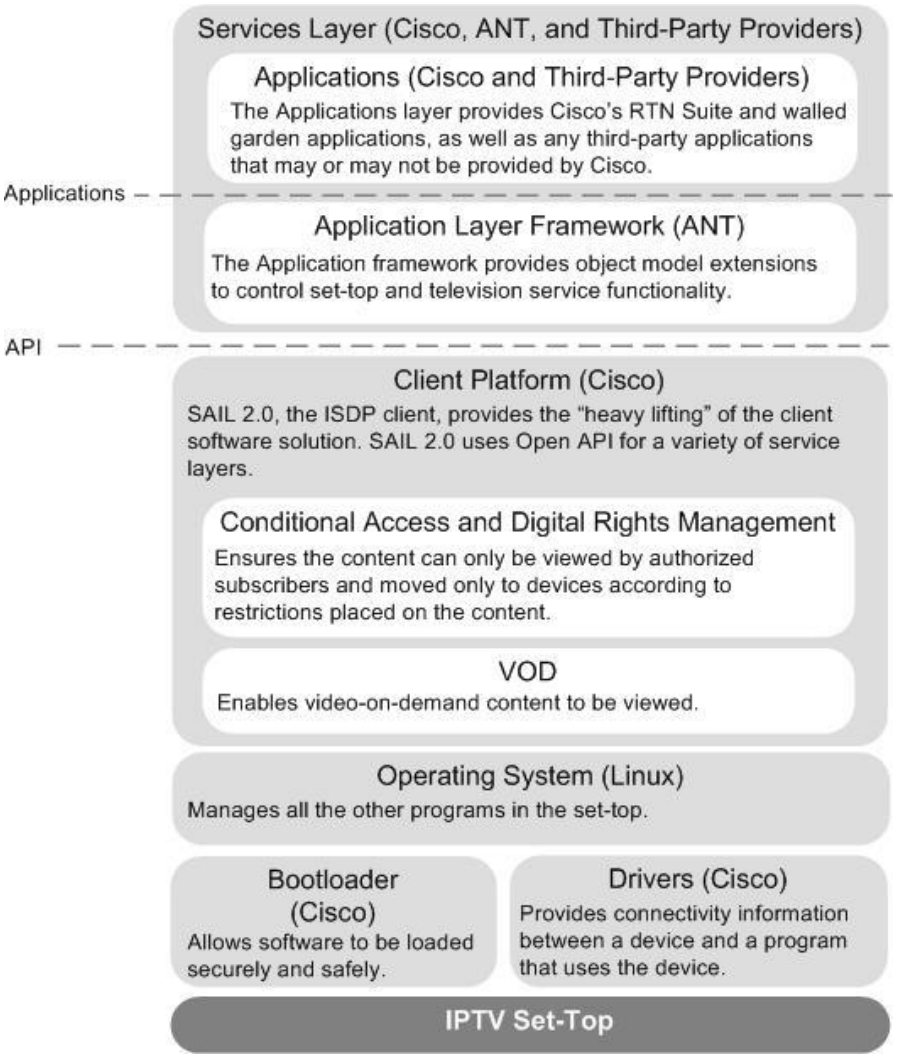
Application Server Software Functions

The Application server is an adjunct server to the ISDS. The Application server is controlled through the ISDS using the administrative console software. The Application server provides programs that enable set-tops to inform subscribers of service offerings. It comes with the following standard applications:

- Interactive Program Guide (IPG)
- VOD

ISDP Client Software Functions

The ISDP client platform (Cisco Abstraction IPTV Layer 2.0, or SAIL 2.0) comes pre-loaded on Cisco IP set-tops. SAIL provides the necessary foundation to help deliver robustness, reliability and scalability for the ISDP solution. It also enables a range of services layers to be supported through a published API, as shown in the following illustration.



Client Reference Services Layer

The client reference services layer utilizes W3C technology for applications to define the presentation and control of digital TV and networked CE devices. It consists of the following components:

- **Applications Layer** - provides resident applications that are part of the resident image and supports downloadable applications that can be web hosted
- **Application Layer Framework** - enables the W3C application framework

Applications Layer

The Applications layer provides the following:

- The Reference TV Navigator (RTN) Suite which includes the following applications:
  - **Miniguide/Zapper application** - Displays a banner at the bottom of live TV to provide basic program information, such as the channel number, name, and program title, of the program currently viewed.
  - **IPG (Interactive Program Guide) application** - Provides an on-screen display of channel names and associated program data. The IPG allows users to scan the available channels list and tune to current programs by using the remote control to select specific program listings.
  - **VOD application** - Provides an on-screen display of VOD assets available for purchase and allows users to select and control a VOD asset.
  - **DVR application** - Provides on-screen controls that allow the user to control live television and to schedule and manage recordings.
  - **Settings application** - Provides an on-screen display that allows users to customize set-top settings, such as a list of favorites.
  - **Portal application** - Provides an on-screen directory of services, which is often the user's main starting point to the set-top application.
  - **Support for a Caller ID application** - Provides an on-screen display that offers information about the current telephone caller, such as the caller telephone number and name.
- Support for third-party applications that may or may not be provided by Cisco.
- Support for a portal to provide a walled garden application.

The RTN Suite uses open licensing and includes two skins that the operator can use as-is, modify, or use the source code to create completely customized skin. The RTN Suite supports the following:

- **AJAX** (Asynchronous JavaScript and XML) - increases the responsiveness, speed, functionality and usability of web-based applications. AJAX is the face of Web 2.0 applications. It is based upon open standards and allows for cross-platform and cross-browser compatibility.
- **HTML** (Hypertext Markup Language) - coding language that provides web browsers with instructions on how to display web pages. Pages written in HTML define both the structure and content of the document as well as the formatting, or presentation, of the pages.
- **XML** (Extensible Markup Language) - allows designers to create interactive pages, allows the subscriber to customize those pages, and makes creating e-commerce applications more intuitive.
- **XHTML** (Extensible Hypertext Markup Language Specification) - a coding language that combines the flexibility of HTML with the extensibility of XML.
- **CSS** (Cascading Style Sheets) - used to define the format or presentation of a web page.
- **JavaScript** - allows for cross-browser support, validation of data on the client, and enables the creation of sophisticated user interface.
- **DOM** (Document Object Model) - supports the navigation and modification of XML documents. It allows for the delivery of targeted content.

Application Layer Framework

The ANT Galio Browser and the ANT Connected Device Framework collectively enable the W3C application framework by providing object model extensions to control set-top and television service functionality. It accomplishes this via a set of open and published JavaScript extensions for the set-top environment.

SAIL 2.0

SAIL provides public interface to the client platform. SAIL is a focused set of APIs using ANSI C definition that enables rapid prototyping and deployment for "service velocity" and supports a large range of options. It provides a consistent implementation across a range of service layers. The "heavy lifting" functionality it offers includes the following:

- Unicast RTSP client
- Multicast IGMP
- MPEG program stream support
- Conditional access and DRM
- SI acquisition and management
- IPG acquisition and management
- Content protection (CCI, etc.)
- Closed Captioning
- DVR
- SNMP
- Diagnostics

SAIL provides the following:

- IPG database
- Channel List database
- PPV Event database

Conditional Access and Digital Rights Management

The ISDP client supports both Widevine Cypher CA used in the reference architecture and PowerKEY CA, which may be used in a custom architecture.

Widevine Conditional Access System

Conditional Access for ISDP is performed using Widevine's solution, Cypher. Cypher system ensures that content can only be viewed by authorized subscribers. The Cypher CA system typically requires five physical servers that fulfill various roles in the CA system:

- Cypher CA Core server - Provides key management, set-top key provisioning, session-key generation and Entitlement Control Messaging (ECM) generation. (Keys are used to encrypt and decrypt digital services. ECMs are specific to a particular video broadcast stream or VOD asset.)
- Cypher CA EMMG server - Generates Entitlement Management Messages, or EMMs. (An EMM is used to provide keys that can only be decrypted by a specific subscriber.)
- Cypher EIM server - Provides an interface to the subscriber management system and the ISDS.
- Cypher Broadcast server - Provides real-time broadcast content encryption, control word (CW) generation, and ECM embedding. (A CW is one of the three keys that Cypher uses to protect and decrypt content.)
- Cypher VOD server - Encrypts VOD assets during the ingest process, generates CWs, and embeds ECMs.

Bootloader

The bootloader software module is part of the ISDP client platform and provides software integrity for IP set-tops. Bootloader is responsible for booting up a set-top and making sure it has the correct software and information to perform in an ISDP network. It also leverages the multicast delivery of code updates and helps to provide a scalable and cost-effective solution.

Drivers

The set-top device drivers are written to the operating system in use on the IPTV platform and provide an interface through which higher level software can address the hardware resources on the set-top.

Overview of Key ISDP Hardware

This section describes the following hardware devices that are at the core of the ISDP solution:

- ISDS server
- Application server
- Residential gateways
- IP set-tops

Key Headend Hardware

The ISDS server resides in the headend. A Sun Fire V445 server provides the hardware platform for the ISDS server. There is typically one ISDS server, plus a backup server, in a system.

Key Hardware for the Home Network

Cisco provides the following hardware for the home:

- Residential gateways
- IP set-tops

Residential Gateways

Cisco offers the following high-performance gateways that integrate a DSL data gateway with an IP-over-Coax adapter. They facilitate seamless distribution of data, voice, and IPTV within the home.

- **DDR 2200** - ADSL2+ Pair-Bonded
- **DDR 2300** - Dual Mode: VDSL/ADSL2+

Common features for both models include the following:

- WAN: DSL RJ-11 Optional: RJ-45 10/100 Ethernet (for FTTP)
- Integrated HPNAv3 (Coax + TP)
- 4-port 10/100 Mbps Ethernet Switch
- USB PC & Device Support
- Wireless: 802.11g
- IP QoS for IPTV
- Multicasting Support IGMPv2/3

- Manageability: Web GUI and TR-69 (Remote) + TR-64 (Local)
- Built-In NAT/Firewall
- Flexible service mapping options
- VoIP (SIP, 2-Ports, Optional)

IP Set-Tops

Cisco IP set-tops deliver high-definition (HD) and standard-definition (SD), personal video recording capabilities, advanced security capabilities, and the ability to stream content to multiple televisions. They also provide two-way communications required for IP communications.

ISDP client software supports the following NTSC set-top models for North America:

- CIS330
- CIS430 - includes a DVR
- CIS2000

ISDP client software supports the following DVB-T set-top models for Europe:

- CIS2001
- CIS5020 - includes a DVR
- CIS5100
- CIS5220 - includes a DVR

Service Provider Benefits

All of Cisco's IPTV set-tops provide the following benefits to service providers:

- Allow the use of a wide range of video codecs, including MPEG-2, MPEG-4 Part 10/H.264, and VC-1 in both standard-and high-definition formats
- Support open middleware platforms (the Services Layer), enabling a high degree of control, creativity, and differentiation in solutions development
- Select open, renewable security solutions, including downloadable CA systems and DRM
- Use existing coaxial wiring in the home to deliver IPTV service

Consumer Services Provided

Cisco's IPTV set-tops allow consumers to enjoy the following features:

- Pause, watch, and record live television, while recording other programming simultaneously
- Create personalized channel line-ups
- Select different viewing angles, where available

4

Customer Information

If You Have Questions

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

Access your company's extranet site to view or order additional technical publications. For accessing instructions, contact the representative who handles your account. Check your extranet site often as the information is updated frequently.

A

Pre-Installation Planning for Key ISDP Components

Introduction

This appendix provides an overview of the installation planning necessary for installing the ISDS server and application server and interfaces to those devices.

Note: For assistance with the remaining portion of the ISDP network, contact the appropriate provider.

- Application Service Layer with UI - When the reference architecture is used, Cisco Systems, Inc. (The service provider may elect to use their own custom RTN.)
- Content Distribution and Network Integrity - Cisco Systems, Inc.
- Operations Support System/Backoffice Support system interfaces for billing and VOD asset management - Tandberg Television
- Content Protection - Widevine Technologies

In This Appendix

General Preparations

Cisco Services engineers use this site survey to initiate successful deployments of the ISDS server and application server within an ISDP. The site survey is used to establish the following:

- Points of contact
- A baseline system environment
- Network requirements
- Expectations for the ISDP solution and the customer's installation site.

The site survey is one in a series of documents to be provided for integration of the ISDS server and application server within an ISDP. To assure a successful outcome, Cisco Services engineers expect to gain a working knowledge of the customer's installation site and network with information obtained from the site survey.

Site Survey

The site survey begins with contact information. Cisco Services engineers require contact information (a name and telephone number) for the following personnel to ensure a successful installation:

- **Cisco router network manager**. We recommend that this person be available to answer questions during the time of installation. Most of the devices Cisco Services will install require their own IP address and network range.
- **VQE server manager**. In order to broadcast video from the VQE server, the ISDP system requires correct information from the VQE server. Consequently, Cisco Services requires that the VQE server manager be available during the installation and configuration.
- **DCM/video content manager**. To ensure the best quality possible, Cisco Services requires that this manager be available to match the settings for the video source that the ISDS system receives.
- **ISDP network manager**. Because the ISDP solution provides flexibility for customizing certain variables to the service provider's preference, Cisco Services requires the ISDP network manager be present during installation and configuration.
- **CDS/MIDAS/VOD network manager**. To ensure a successful installation, Cisco Services requires that the personnel responsible for managing these systems be available to ensure that these devices are correctly configured and functioning appropriately.

Network Management Planning

DHCP Server: Set-tops require a DHCP server to provide them with their IP address. The preferred device is a Cisco 4948 router. Other Cisco routers may be used as long as they meet the minimal requirements. The router must be capable of multicast streaming as multicast streaming is the delivery system used for an ISDP network. When designing network flow, keep in mind that the physical ports located on the router can limit the number of devices that can be attached to the network

Please verify the router you wish to use with Cisco Services.

1. Verify the existence of the DHCP server on the access network for set-top IP provisioning.
   - **a** Is this router capable of multicast streaming?
   - **b** If this is a single router configuration, does it have the following required ports?
     - **i** Three ports for dncs
     - **ii** Three ports for appserver
     - **iii** 2/5 2 ports for Widevine lab 5
     - **iv** Enough ports for the set-tops (The number of ports required equals tea number of set-tops that are directly connected to the router.)
     - **v** Enough ports for video sources (varies by customer)

       Note: At this time, we do not have a set number of ports for Tandberg and CDS devices.
2. Provide IP addresses for the ISDS server and the Application server network interfaces, as shown in the following examples:
   - Network IP address: 10.253.0.x 255.255.255.0 (This is the Cisco Services default IP scheme. We recommend that you adopt this scheme.)
   - Management IP address: 10.192.0.x 255.255.255.0 (This is the Cisco Services default IP scheme. We recommend that you adopt this scheme.)
   - Corporate IP address: 10.90.128.x 255.255.255.x

   Note: An outline of the network should be performed prior to deployment for installation. Using the correct IP addresses in the diagram will increase the efficiency of the installation process.
3. Determine the set-top IP address scheme throughout the access layer, such as in this example: **10.18.x.x 255.255.x.x**

   Note: The set-top IP range will need to be large enough to encompass the number of set-tops that will be sued. This range can be any range you wish to use. A Cisco Services installer will only use this IP range at the end of installation to perform routine tests of the set-top. Having the set-top IP range prior to installation allows a more accurate network diagram to be completed for the site.

4 Provide IP address information for third-party servers, such as Widevine servers, VOD servers, or other pertinent application servers. (We recommend that a subnet of 13 IP addresses be reserved.)

Note: Widevine in a lab environment typically requires only two IP addresses on the same network. The VQE requires an IP address for each server that is to be used.

Video Source

Video source information is required for provisioning of active services. IPG information must match exactly what is coming in from the IPG source. Channel map can be arranged according to the needs of the service provider; however, we require that the channel map list be submitted prior to installation. Source ID schema is a generic, unique number that he ISDS uses to tag each source. This enables the ISDS to control, pass, and track each source as needed. A Cisco Services installer uses a generic source ID, unless the system is installed alongside a pre-existing Digital Network Control System (DNCS). If a DNCS exists, the new sources must be unique.

1 The following service provisioning information is required:

- Service application manager (SAM) information, including long and short descriptions
- Channel mapping information
- Source ID schema

2 The following IP source definition information is required for each source:

Note: The DCM or encoder used to supply the video source determines the value required for each of the following specifications:

- Source device type and IP address
- Multicast destination IP address
- Destination UDP port
- Video encoding type
- Video encapsulation type
- Video data rate
- Video frame rate
- Video resolution
- Audio encoding type

3 Verify the content delivery mode required for both the current and future needs of the system (for example, IP, RF, or both IP and RF).

Note: Currently, the IP and RF mode is currently under development.

4 The following IPG provider information is required:

Important: This information allows the ISDS to download current IPG information from the IPG source. Without this information, IPG will fail. With the current test version of ISDS, set-tops will not boot without up-to-date IPG information. If you foresee this as a possible issue, please contact Cisco Services for assistance.

- IPG service provider FTP server address
- IPG service provider user name and password
- IPG service provider file name format

ISDP System Information

1. Provide the following cluster parameters: Group Destination address

   Note: Clusters break up a network into manageable parts. Each cluster that is established requires its own group destination IP address. The group destination IP address for subscribers is as follows: 233.0.2.1, 233.0.2.2, 233.0.2.3, and so on.

2. A list of the localizations and localization codes that the network uses are required.

   Note: Localization codes break a cluster down into even more manageable parts. Currently, we recommend that for a domestic system, that localization codes correspond with a target area's zip code.

3. Provide the approximate number of set-tops that the system will support.

   Note: At the time of installation, a rough estimate is used to ensure the system that is being installed is capable of handling the amount of volume required for quality delivery.

VPN

1. Will a virtual private network (VPN) tunnel be made available to Cisco Services engineers during the installation?

   Note: VPN access allows Cisco Services to assist its on-site installation team. It also provides customer support after the installation is complete and Cisco Services engineers are no longer on site. Because the VPN allows an installer to receive expert-level support in resolving unique situations that may occur during installation, a VPN tunnel increases the efficiency of the installation and provides a more satisfactory installation.

2. Will a VPN tunnel be made available for Widevine service monitoring?

   Note: Widevine requires 24-hour monitoring of their server through a VPN tunnel.

VQE Servers

1. List the sources that will be filtered through VQE.

   Note: At the time of installation, a list of all sources filtered through VQE should be provided to the installer. The list should indicate the VQE server through which the source is being filtered.

2. Provide the number of VQE servers to be set up on site.

   Note: The number of VQE servers is dependent upon the number of sources that will use the VQE server.

CDS

1. Provide the MIDAS set-top side IP address
2. Provide the BMS set-top-side IP address

Cisco Systems, Inc.
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

678 277-1120
800 722-2009
www.cisco.com

[month] 2012 Printed in USA

Part Number 4017607 Rev B