
Introduction to Intelligent Grouping and Resource Sharing (IGRS) A Technical White Paper

1. Goals of IGRS

We are incorporating more and more digital devices into our daily activities to enhance productivity. These devices are divided into three worlds of “Information Islands” – the Internet, Broadcast, and Communication – providing three categories of services (called the “3C” categories):

- 1) **Computing:** Internet world – computers and other computing peripherals;
- 2) **Consumer Electronics:** Broadcast world – TV, hi-fi audio, set-top box, etc.;
- 3) **Communication:** Communication world – mobile phone, PDA, and laptops, etc.

There is very limited interoperability among these categories because of incompatible technologies. Nevertheless, there is a growing market demand for integrated systems that span these categories. The IGRS communications system was developed to meet this demand by enabling digital devices to interoperate with shared resources and service collaboration. All of this is accomplished with an efficient communications system appropriate for the cost-constraints typical of consumer electronics.

IGRS specifies a communications protocol that device manufacturers can incorporate easily to enable new applications, services, and features through device interactions. The addition of IGRS interfaces facilitates new IGRS products and improves existing products. IGRS-equipped products are differentiated from the competition by providing users with novel applications.

The IGRS protocol is specifically designed for user simplicity through resource virtualization. Consumers do not need to worry about the technical complexities of the devices they purchase such as drivers, ports, and network configuration. They may freely choose among many devices made by different manufacturers with the assurance that their 3C devices will interoperate seamlessly. In essence, devices with built-in IGRS protocol will automatically discover one another by various physical connection methods such as WLAN, Ethernet and Bluetooth, establish different logical resource groups and execute service collaboration based on specific application demands. If one of the devices/services in the group fails or goes offline, then its services and capabilities are distributed and maintained among several other similar devices across different networks or platforms such that the consumer will not notice any decline in user experience.

2. Development of IGRS

The Intelligent Grouping and Resource Sharing (IGRS) working group, also known as the IGRS Alliance, was established on July 10, 2003 by five of the largest leading IT and consumer electronics companies in China: Lenovo, TCL, Konka, Hisense, and Great Wall. This working group is an open standards organization that developed the IGRS specifications. The mission of IGRS is to foster 3C convergence and enable seamless intelligent grouping, resource sharing, and service collaboration among devices for communication terminals, computers, and consumer electronics for users at *home*, *office* and *public areas*. The IGRS working group has defined a dynamic networking architecture, especially for wireless environments, and has created a new collaborative application model among

digital devices. This new application model maximizes the resource usage of each device and the interoperability among devices.

On June 29, 2005, the IGRS Standard was formally approved by the Ministry of Information Industry as a Chinese National Industry Standard. Currently, the IGRS Alliance has 113 members worldwide including many major international corporations such as Philips, LG Electronics, Cisco-Linksys, and STMicroelectronics. The Alliance members have already launched various IGRS-compliant products including IGRS-equipped TVs, PCs, laptop computers, projectors, audio systems, printers, mobile phones, and wireless audio access points. IGRS chips and modules that will further reduce R&D cost have been introduced. With these recent rapid industrialization efforts, the IGRS Standard is poised to impact our lives significantly in the near future.

3. IGRS framework

The IGRS standard framework provides a common set of protocols to enable network resource discovery, invocation, and management capabilities. The IGRS technical framework includes three components: IGRS Core Protocol, IGRS Application Profile, and IGRS Basic Applications. These elements of IGRS define dynamic device discovery, ID, management and message routing, device and service data advertisement and sharing mechanisms, distributed device grouping, and various application-specific profiles. The IGRS core protocol defines IGRS device grouping and the interaction mechanism between client and service. Based on the IGRS core protocol, the IGRS Application Profile defines service description and interaction logic for IGRS applications. Various IGRS applications are standardized and implemented based upon corresponding IGRS Application Profiles to ensure interoperability.

The key innovations in IGRS emphasize network resource virtualization and service/application convergence. The IGRS specifications are designed around a unique **device grouping** concept that allows the content and computing resources to link and collaborate dynamically with little or no reliance on various network elements such as configuration, scalability, and complexity. This feature of device grouping is not found in any existing international industry specification that addresses terminal device and service interoperability. IGRS supports a device grouping-based system architecture that fully integrates the resource organization framework, control model, service discovery, as well as a security mechanism, as shown in Figure 1.

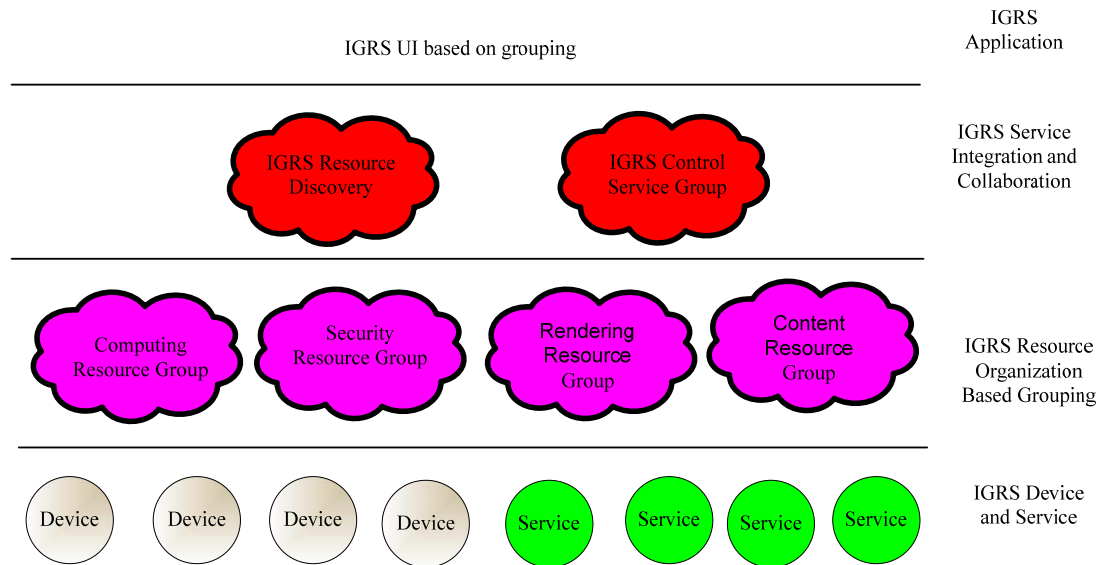


Figure 1: IGRS system architecture

In this figure, the control service group handles the negotiation among different resource groups such as the content, computing, and rendering resource group and so on. Data flows from the content resource group, through the computing resource group, to the rendering resource group. The security resource group is enabled in all control and transport paths to ensure data integrity.

4. Resource organization framework

In addition to supporting the simple peer-to-peer model, IGRS emphasizes the virtualization of resources. The services offered by separate physical devices can be organized into logical groups (IGRS Device Groups) to simplify the management of a diverse network of devices. A virtualized resource organization system can dynamically coordinate different resources and separate the closely coupled relationship between specific device and service to realize transparent and flexible computing system architecture. This concept enables the creation of a flexible multi-application-based computing environment that uses the aggregation of computing resources located across multiple devices. This grouping improves the efficiency of resource utilization and allows services from a variety of resources to be marshaled into customized user services on demand in order to satisfy the progressive application requirements of the digital home.

In the IGRS resource organization framework, the device grouping model provides the technical foundation to enable the dynamic resource allocation. The IGRS specification defines a device group in multiple dimensions to ensure maximum adaptability. For instance, IGRS currently supports hierarchical device groups such as peer-to-peer and centralized (master-slave) groups. In addition, IGRS allows device groups to be categorized by the application/service cluster or by the physical property of devices.

By definition, IGRS device groups permit the implementation of a “virtual device” – a composition of logical devices and services of different types operating on different physical devices. This joint

device or service set is treated as a virtual resource to the devices that are not a part of this group. Device grouping simplifies the external invocation process even when services may be located on different physical devices across the network. By creating these dynamic virtual devices in the digital home, IGRS expands beyond the traditional resource sharing among the local devices and services to support many “resource clouds” consist of devices and services from across different networks and platforms. The net result of the IGRS technology is enhanced reliability and fault tolerance.

To an application, the device grouping approach greatly improves the efficiency of resource discovery and simplifies the interaction process by concealing the lower layer device and service network complexities, especially in a heterogeneous network. For example, if a user wishes to play video games with a group of users, he/she only needs to connect with a virtual gaming device representing a group of users.

In Figure 2, we use a typical Audio/Video (AV) application scenario in the home to demonstrate the device-grouping concept.

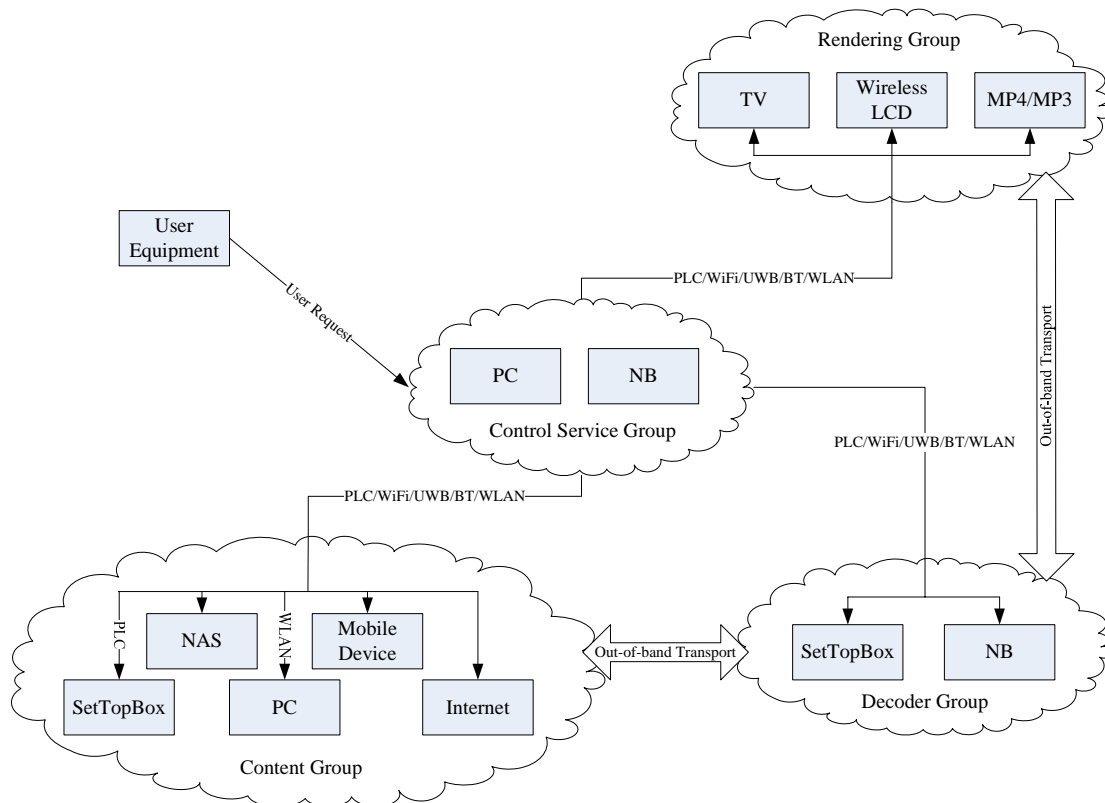


Figure 2: A typical AV application in the home

From the service perspective, this scenario includes the content group, decoder group, rendering group and control service group. These device groups all appear as a single virtual device to the devices and networks outside these groups. The devices in the content group store AV media sources that are accessible via various physical means such as Power Line Communication (PLC), WiFi, Ultra Wideband (UWB), Bluetooth, and Ethernet. The typical devices in the content group are set-top boxes, Network Attached Storage (NAS), PC, mobile devices, or even devices on the Internet. The decoder

group provides computing resources to decode media data for rendering. The typical decoder devices are set-top boxes, PCs, and notebooks. The rendering group consists of devices such as TVs, wireless LCDs, and MP4/MP3 players that are capable of handling various multimedia contents. The control service group is responsible for providing control services to the application. The typical devices include notebooks, PCs, or other capable devices that can respond to various types of user requests.

In this application scenario, user equipment invokes the application services through interactions with the control service group only. It does not need to know the details of data flow or device configurations such as where the contents are stored or how the multimedia data are processed. For example, once a PLAY service request is received by the control service group, the media contents in the content group will be transferred via PLC to the decoding group for decoding. The decoded data are then pushed to a wireless TV or projector in the rendering group for viewing. All of the above device actions are triggered without the resource burden of requiring every device to discover every other device in all device groups. This capability saves execution time and is found only in IGRS.

This scenario fully demonstrates the flexibility and distributed virtual resource organization capabilities provided by the IGRS device grouping feature that enables intelligent grouping and resource sharing.

5. Discovery mechanism

IGRS service discovery and event subscription mechanisms also support the device grouping architecture described above. For multiple devices in the same device group, the existence of device discovery, device advertisement, and event subscription based on IGRS device grouping provides dynamic information about the device and group capabilities that offer more flexibility and efficiency compared to other similar home networking technologies since fewer messages are required to relay the same amount of information. Moreover, the IGRS protocol has minimum impact on the overall network performance while offering better scalability and adaptability support, especially in a complex network environment with many active devices.

In contrast to other service discovery mechanisms, IGRS supports service discovery based on the “device pipe.” Any service discovery mechanism in a digital home must be able to operate in a complex environment consisting of heterogeneous devices, services, and communication techniques. The IGRS device pipe enables transparent service discovery by effectively encapsulating the security mechanism while shielding the transport layer communications with a cross-platform discovery and service invocation call simpler than found elsewhere. IGRS service discovery adheres consistently with the resource virtualization design theme and thus is no longer limited to a small network or application scale.

The device-grouping model enables IGRS to support the discovery-by-proxy method. For instance, in an IGRS peer-to-peer or centralized device group, the master node can act as a proxy to send and receive service advertisements for all member nodes of the device group in order to save communication and computing resources. This mechanism can be easily extended to provide service proxy for devices from different device groups. Furthermore, an IGRS proxy device can serve as the

service advertisement proxy to interconnect successfully among different heterogeneous networks. Silent network devices can also be supported by this method because the proxy node can delegate operations such as service advertisement instead of the device itself. Finally, the IGRS proxy mechanism even enables some non-standard devices to connect to the IGRS networks so that the user with legacy devices can enjoy the benefit of system upgrades.

6. Control model

IGRS supports a distributed collaborative control model that is significantly different from the traditional point-to-point or single-point centralized control model. The traditional model is adequate for a simple control network where a single node contains all control services. The IGRS control model is based on the control service group concept of building a “virtual control point” supported by multiple device groups that aggregate all relevant control services. Control is accessed as a single logical unit even if it is distributed among many devices. An IGRS control network with multiple control elements can efficiently separate each functional module and integrate different services on the “resource cloud” according to each application demand such as balancing bandwidth load, managing Quality of Service (QoS), and simplifying device implementation. The IGRS control model provides the user with the following functions: 1) User interfaces to the “resource cloud,” 2) dynamic service directories, and 3) aggregated resource control service management such as dynamic resource monitoring, control, and load balancing.

In the IGRS control network, each node serves a specified control function such as access control or security authentication. Therefore, through collaboration, these control service nodes in the IGRS control service group can be organized to appear as a single “unit” for users to control based on specific application demand. The user can simply connect to a virtual control service through the provided user interface in order to access the application. However, unknown to the user is the fact that this virtual service is actually supported by a group of services rather than by a single service or server. The complexity of backend service and device integration is completely shielded from the user with this approach. For example, in the resource organization scenario described in Figure 2, the notebook in the control service group can handle all access control services. The PC can connect to the Internet and manage multimedia content authentication. External devices treat the control service network as a virtual control point in that every service request is forwarded by the control service group to the relevant service control node for processing according to the request type.

IGRS has adopted this aggregated service control architecture to manage resources efficiently, to improve the scalability of services and applications, and to enhance fault tolerance and disaster recovery capacities.

7. Security mechanism

IGRS supports multiple widely-used security encryption mechanisms. These encryption methods are combined with the IGRS device pipe concept to provide a unique transparent security service implementation. This combination hides the lower transport layer details to reduce the complexity of embedding security mechanism into a digital home network system.

The IGRS protocol requires that each device negotiate security encryption policies upon connection via a device pipe to ensure that the same and most secure mechanism is used by the devices sharing the pipe. The five security mechanisms used by IGRS are categorized below by the following levels of complexity from the lowest to the highest complexity: 0) No security (NULL), 1) Identity authentication and message authentication mechanism based on symmetric-key cryptosystem (PreSharedKey_MAC), 2) Identity authentication, encrypted message transmission and message authentication mechanism based on symmetric-key cryptosystem (PreSharedKey_Cipher_MAC), 3) Identity authentication, encrypted message transmission and message authentication mechanism based on public-key cryptosystem (PKICertificate_Cipher_MAC), 4) Identity authentication, encrypted message transmission and message signature mechanism based on trusted third party (3rdPartyAuthenService). In this system, every IGRS device must implement the null security mechanism. The other four mechanisms are optional. However, if a device implements a security level above 0, it must implement all lower-complexity levels. For example, a device that implements PKICertificate_Cipher_MAC must also implement PreSharedKey_Cipher_MAC, PreSharedKey_MAC, and NULL mechanisms. Moreover, IGRS also supports multiple encryption techniques such as SHA-1, SHA-256, 3DES, AES128 to provide the security appropriate for various applications. Please refer to the IGRS standard series part 1: Core Protocol [1] for more details.

8. The benefits of IGRS

IGRS technologies will bring new values and benefits to consumers, device manufacturers, and content providers alike. Consumers reap the benefits of simple network configuration. Manufacturers can create devices and applications that are economic and easy to build and that operate efficiently. IGRS-enabled device integration and service collaboration is driving technology developments in areas such as user security authentication, high-quality media streaming, and content protection. A network of IGRS-equipped devices enables content providers to offer users expanded access to any content services at anytime, anywhere.

References

- [1] ISO/IEC (FCD Draft) 14543-5-1: *Information technology – Home Electronic System (HES) architecture – Part 5-1: Intelligent grouping and resource sharing for HES Class 2 and Class 3 – Core protocol*
- [2] IETF RFC 1510: *The Kerberos Network Authentication Service (V5)*
- [3] IETF RFC 3447: *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*
- [4] ISO/IEC 9594-8:2001, *Information technology – Open System interconnection – The directory: Public-key and attribute certificate*
- [5] ISO/IEC 10118-3:2004, *Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions*
- [6] ISO/IEC 18033-3: *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*