DOWNLOAD PDF IMPLEMENTATION OF THE BASIC COLLECTION PROTOCOL

Chapter 1 : Protocols - AARC

Approved in , the Fibre Channel Security Protocols standard (FC-SP) specifies how to protect against security breaches. This standard defines protocols for authentication, session keys, integrity and confidentiality, and policy implementation across an FC fabric. Basic FC security occurs through authentication and access control.

Network access Physical File Transfer Protocol Secure FTP passes the username and password in a plain-text form, allowing packet sniffing of the network traffic to read these values, which may then be used for unauthorized access to the server. With FTPS, data transfers take place in a way designed to allow both parties to authenticate each other and to prevent eavesdropping, tampering, and forgery on the messages exchanged. FTPS includes full support for the TLS and SSL cryptographic protocols, including the use of server-side public key authentication certificates and client-side authorization certificates. You should use FTPS when you need to transfer sensitive or confidential data between a client and a server that is configured to use SSL for secure transactions. Secure variations of FTP ensure that data cannot be intercepted during transfer and allow the use of more secure transfer of user access credentials during FTP login. However, the same certificate vulnerabilities discussed earlier in this chapter apply here, too. An alternative to this involves the use of SSL transport protocols operating on port , which creates an encrypted pipe through which HTTP traffic can be conducted securely. To differentiate a call to port 80 http: HTTP Secure HTTPS was originally created by the Netscape Corporation and used a bit RC4 stream encryption algorithm to establish a secured connection encapsulating data transferred between the client and web server, although it can also support the use of X. Now, bit encryption keys have become the accepted level of secure connectivity for online banking and electronic commerce transactions. SCP runs on port 22 and protects the authenticity and confidentiality of the data in transit. It thwarts the ability for packet sniffers to extract information from data packets. An SCP download request is server driven, which imposes a security risk when connected to a malicious server. Internet Control Message Protocol Internet Control Message Protocol ICMP is a protocol meant to be used as an aid for other protocols and system administrators to test for connectivity and search for configuration errors in a network. Ping uses the ICMP echo function and is the lowest-level test of whether a remote host is alive. The computer that sent the packet then waits for a return packet. If the connections are good and the target computer is up, the echo message return packet will be received. It is one of the most useful network tools available because it tests the most basic function of an IP network. It also shows the Time To Live TTL value and the amount of time it takes for a packet to make the complete trip, also known as round-trip time RTT , in milliseconds ms. One caveat with using ICMP: It can be manipulated by malicious users, so some administrators block ICMP traffic. If that is the case, you will receive a request timeout even though the host is available. Traceroute is a computer network diagnostic tool for displaying the route path and measuring transit delays of packets across an IP network. Traceroute outputs the list of traversed routers in simple text format, together with timing information. Traceroute is available on most operating systems. On Microsoft Windows operating systems, it is named tracert. Traceroute uses an ICMP echo request packet to find the path. It sends an echo reply with the TTL value set to 1. When the first router sees the packet with TTL 1, it decreases it by 1 to 0 and discards the packet. The source address of the ICMP error message is the first router address. Now the source knows the address of the first router. Most implementations of traceroute keep working until they have gone 30 hops, but this can be extended up to routers. Pathping is a Windows route-tracing tool that combines features of the ping and tracert commands with additional information. The command uses traceroute to identify which routers are on the path. When the traceroute is complete, pathping sends pings periodically to all the routers over a given time period and computes statistics based on the number of packets returned from each hop. By default, pathping pings each router times, with a single ping every 0. Consequently, a default query requires 25 seconds per router hop. This is especially helpful in identifying routers that cause delays or other latency problems on a connection between two IP hosts. IPv4

DOWNLOAD PDF IMPLEMENTATION OF THE BASIC COLLECTION PROTOCOL

IPv4 is a connectionless protocol for use on packet-switched networks. It operates on a best effort delivery model, in that it does not guarantee delivery, nor does it ensure proper sequencing or avoidance of duplicate delivery. These aspects, including data integrity, are addressed by an upper-layer transport protocol, such as TCP. IPv4 currently routes the majority of Internet traffic. IPv4 is widely used in both internal and external networks throughout the world. IPv4 is susceptible to ping sweeps, port scans, and application and vulnerability scans. To mitigate sweeps and scans, filtering messages or traffic types is an acceptable solution because it is impossible to eliminate reconnaissance activity. IPv6 Because of the increased demand of devices requiring IP addresses, IPv4 could not keep up with such an expansive demand. As a result, a new method was needed to address all the new devices requiring IP addresses. The new standard, IPv6, makes several changes to the older IPv4 standard. IPv6 increases the address size from IPv4 32 bits to bits. The differences between IPv6 and IPv4 are in five major areas: Addresses are bits 16 bytes in length. Header includes a checksum and options. Header does not include a checksum, and all optional data is moved to IPv6 extension headers. ARP uses broadcast request frames to resolve an IP address to a link-layer address. Multicast Neighbor Solicitation messages are used to resolve IP addresses to linklayer addresses. IPv4 header does not identify packet flow for quality of service QoS. IPv6 header identifies packet flow for QoS. IPsec support is optional. IPv4 limits packets to 64 KB of payload. IPv6 has optional support for jumbograms, which can be as large as 4 GB. Does not require manual configuration or DHCP. In addition to the difference in the address structure in IPv6, there are IPv6 versions of protocols and commands. The following are some of the more prevalent ones: Provides stateful address configuration or stateless configuration settings to IPv6 hosts. It operates in the same manner as the IPv4 version, except that is routes IPv6 addresses. Used by IPv6 nodes to report packet processing errors and diagnostics. Used in the same capacity as Ping except for IPv6 addresses. It can be used in cloud environments as well, allowing remote resources to appear as local. Businesses choose iSCSI because of ease of installation, cost, and utilization of current Ethernet networks. IPsec provides greater levels of security and integrity, as mentioned earlier in this section. An FC infrastructure generally is more costly and complex to manage due to the separate network switching infrastructure. FC allows devices to attach through an interconnected switching system called a fabric. An FC port is not the same thing as computer port or network port. It is the node path performing data communications over the channel. The FC port manages a point-to-point connection between itself and the fabric. FC network protection is primarily security through obscurity because direct access to the FC network is not available to most users, but this does not eliminate the need for security. This standard defines protocols for authentication, session keys, integrity and confidentiality, and policy implementation across an FC fabric. Basic FC security occurs through authentication and access control. To secure FC, authentication between FC devices and other devices with whom they communicate can be established using mutual authentication. Proper access control can be achieved through port locking, hard zoning, logical unit number LUN masking, and using secure management interfaces and protocols. Because FCoE allows FC to be carried over Ethernet, the amount of equipment required in the data center can be reduced. SAN basic security flaws include weaknesses with authentication and authorization. FCoE can be secured in the manners suggested for FC but also includes control-plane protection and data-plane protection. Control-plane protection is access protection for the switches. Data-plane protection is security for traffic passing through the switches. FTP servers include many potential security issues, including anonymous file access and unencrypted authentication. Many FTP servers include the ability for anonymous access in their default installation configuration. Anonymous access is a popular method to provide general access to publicly available information. The problem with this form of access is that any user may download and potentially upload any file desired. Even when user authentication is required, FTP passes the username and password in an unencrypted plain-text form, allowing packet sniffing of the network traffic to read these values, which may then be used for unauthorized access. Using more secure variations of FTP ensures that data cannot be intercepted during transfer and allows the use of more secure transfer of user access credentials during FTP login. Unlike standard FTP, it encrypts both commands and data, preventing

passwords and sensitive information from being transmitted in the clear over the network. Either may be used within a modern enterprise network. Telnet can be used as a tool to determine whether the port on a host computer is working properly. Telnet passes the username, password, and even transacted data in an unencrypted form clear text , allowing packet sniffing of the network traffic to read these values, which may then be used for unauthorized access to the server. Telnet-type clear-text connections create the ideal situation for TCP hijacking and man-in-the-middle attacks. An HTTP message contains a header and a body. The message header of an HTTP request has a request line and a collection of header fields. All HTTP messages must include the protocol version.

Chapter 2 : Communication protocol - Wikipedia

Refworld is the leading source of information necessary for taking quality decisions on refugee status. Refworld contains a vast collection of reports relating to situations in countries of origin, policy documents and positions, and documents relating to international and national legal frameworks.

The issue of how to strengthen implementation of the Convention and the Protocol relating to the Status of Refugees has twice recently been a separate item on the agenda of the Sub-Committee of the Whole on International Protection the Sub-Committee. At the most recent inter-sessional meeting of the Sub-Committee, held from April , UNHCR was requested to submit for further discussion certain basic questions concerning implementation which have emerged in the course of these various debates and which, among others, would benefit from more detailed analysis. The present note responds to this request by placing before the Sub-Committee the following four issues which it might wish to consider: Promotion and monitoring of implementation covering points a and b 3. The utmost importance of effective implementation has been repeatedly stressed by the Executive Committee. The Convention and its Protocol together are the most comprehensive instruments adopted to date on a universal level to safeguard the fundamental rights of refugees and to regulate their status in countries of asylum. As such, they are fundamental to the international regime of refugee protection. They help in ensuring that refugees are granted basic humanitarian treatment. UNHCR has been mandated by the international community with the particular responsibility to ensure effective implementation of the Convention and Protocol within the overall framework of its protection responsibilities. The Office is specifically called upon, pursuant to paragraph a a of its Statute, inter alia, to supervise the application of international conventions for the protection of refugees. The Note also recognized, as a first step, the need for more States to respond to the questionnaire on implementation. It is also clear, however, that discussion would benefit from going beyond mere restatement of this commitment to identifying practical suggestions to strengthen implementation. Accordingly, the Sub-Committee is invited to reconsider the suggestions put to the forty-second session. Other ideas which might, at the same time, be considered could include periodic meetings of States Parties to review problems and progress on implementation. There might also be appropriate steps taken at the regional level to harmonize interpretation and application of the Convention among neighbouring countries, including giving existing regional human rights commissions, or courts, certain refugee-related responsibilities. Regional bodies are the obvious interlocutors in pursuing regional approaches to ensure respect for protection standards and to achieve harmonized approaches. Improving monitoring arrangements, as suggested in previous paragraphs, would considerably facilitate better implementation. At the same time, however, there are a number of obstacles impeding full and proper implementation which monitoring will not necessarily remove. They are more appropriately addressed through clearly targeted promotion campaigns. Legal obstacles to proper implementation include the clash of, or inconsistencies between, existing national laws and certain Convention obligations; failure to incorporate the Convention into national law through specific implementing legislation; or implementing legislation which defines not the rights of the individuals but rather the powers vested in refugee officials. As to the latter, this means that protection of refugee rights becomes an exercise of powers and discretion by officials, rather than enforcement of specific rights identified and guaranteed by law. Where the judiciary has an important role in protecting refugee rights, restrictive interpretations can also be an impediment to full implementation. Finally, the maintenance of the geographic limitation by some countries is a serious obstacle to effective implementation. At another level, there are bureaucratic obstacles, including unwieldy, inefficient or inappropriate structures for dealing with refugees, a dearth of manpower generally or of adequately trained officials, and the non-availability of expert assistance for asylum-seekers. Finally, there are certain problems of perception at the governmental level, including that the grant of asylum is a political statement and can be an irritant in inter-state relations. Strengthened training, promotion and public

information activities are required to overcome these various problems. A promotion campaign could be built around implementation of the Convention which would, inter alia, address these difficulties and would involve intensified training of officials and other key groups journalists, lawyers, the judiciary, non-governmental organizations NGOs and opinion-makers generally. In addition there is a need to build up local support bases for fair treatment of refugees, in accordance with Convention standards. One possibility in this regard is the creation of National Refugee Councils, consisting of senior Government administrators, NGO representatives and those of religious groups, as well as other prominent individuals, to sensitize national public opinion and enable UNHCR to receive counsel and advice from a broader range of interlocutors. Difficulties in fulfilling Convention obligations covering point c Replies received to the questionnaire show clearly that some States have difficulties in fulfilling all of their obligations under the Convention. This is understandable, since the Convention contains comprehensive provisions concerning the rights of refugees in a number of diverse areas. Even under the best of circumstances, States may occasionally find that public opinion does not understand, or support, efforts undertaken on behalf of refugees. When States are suffering from adverse economic conditions, lack of development or high unemployment, it can become all the more difficult to guarantee the basic needs of refugees, especially when those of the national population are not able to be fully met. Nonetheless, although States may face constraints in implementing the Convention completely, there are certain provisions which are so fundamental to refugee protection that any deviation from them is always a matter of paramount concern to UNHCR. One such provision is Article 33 which enshrines the principle of non-refoulement. Article 33 of the Convention and its prohibition on return of individuals to situations threatening life or liberty is a fundamental guarantee of refugee protection. It must be read together, in particular, with Articles 31 non-penalization for illegal entry and 32 limits to expulsion: This is the case as regards the refugee definition Article 1 , non-discrimination Article 3 , freedom of religion Article 4 , non-penalization of refugees unlawfully in the country of refuge Article 31 , expulsion Article 32 and the prohibition of refoulement Article Other provisions of the Convention, such as those defining the economic and social rights of refugees, are more relevant to refugees who have been granted durable asylum by a contracting State and are intended to facilitate their integration in their asylum country. There will be large-scale influx situations which may fall within the parameters of the Convention but because of their massive character and the clear feasibility of return in safety at some point, repatriation not integration is the appropriate approach. Varying interpretations and selective application of the definition covering Point d The imprecision of the language to some extent facilitates selective interpretation or application. As some States Parties have observed, the Convention does not, for example, contain a definition of persecution. The Convention sets no time limits as to when the persecution should have arisen. What sort of post-flight situations should be regarded as sufficient to serve as a foundation for a fear of persecution is not fully clear. Where the Convention is not precise, the courts or Refugee Boards have moved to fill the gaps. In this process, as the numbers of asylum-seekers continue to rise, divergence is apparent between the profiles of a percentage of the asylum-seekers and the classical concept of refugee. This approach is often revealed in decisions on refugee status which narrow the meaning of the terms persecution and well-founded fear. Examples which have come to the attention of the Office include refusal to regard severe or repeated discrimination or harassment as persecution; reluctance to recognize situations of group persecution; rejection of draft evasion or desertion for valid reasons of conscience as a basis for a claim; little or no consideration of the situation of women as a particular social group; limiting the notion of "agents of persecution" to the authorities of the country of origin; and setting of arbitrary time limits on how recently the persecution must have occurred. With respect to well-founded fear, negative decisions are taken based on subjective assessments of general credibility, with a growing inclination to see uncorroborated testimony as inherently self-serving and without acknowledging the reality that, as has always been the case, many refugees will not have been able to bring forward independent evidence to substantiate their claim. Other troubling cases include denials based on irregularities in the manner of entry, even if such an entry was the only means of escape, and rejection of

status for persons fleeing from war or other armed conflict or violence, without investigating the possibility of persecution which may well exist in such situations. The Office has been particularly concerned about a number of recent cases involving individual refugee status applicants whose claims have been denied essentially because they have been viewed as victims of armed conflicts rather than of specifically targeted persecution. Even where it has been accepted by the determining authorities that an individual has suffered serious human rights abuses, that he or she has a genuine fear and that there is a distinct likelihood of arrest and detention on return, the position has been taken that these factors are not attributable to any intention on the part of the authorities to persecute the individual concerned on account of one of the recognized grounds and that, accordingly, there is no issue of refugee status involved. There is nothing in the definition itself which would exclude its application to persons caught up in civil war who meet the definition. The interest of the Government neither explains nor excuses the use of torture or arbitrary punishment, or the discriminatory singling out of certain individuals or groups for punishment. It should also be noted that, in accordance with the Vienna Convention on the Law of Treaties, States should interpret the Convention in a way which is consistent with its object and purpose. The object and purposes of the Convention are clear from the context in which the Convention was negotiated. It was an instrument designed to assure refugees the widest possible exercise of their rights, and to provide a framework within which to structure the exercise by States of their discretion to receive refugees and accord them those rights. In its consideration of this issue, the Sub-Committee might judge it useful to encourage all States Parties to approach interpretation of Article 1 in a manner consistent with the object and purposes of the Convention.

DOWNLOAD PDF IMPLEMENTATION OF THE BASIC COLLECTION PROTOCOL

Chapter 3 : calendrierdelascience.com Namespace | Microsoft Docs

The Standard Operating Protocol was the primary reference document for hospitals and Lead Technical Agencies (LTAs) participating in the WHO High5s project.

At the most recent inter-sessional meeting of the Sub-Committee, held from April , UNHCR was requested to submit for further discussion certain basic questions concerning implementation which have emerged in the course of these various debates and which, among others, would benefit from more detailed analysis. The present note responds to this request by placing before the Sub-Committee the following four issues which it might wish to consider: Promotion and monitoring of implementation covering points a and b 3. The utmost importance of effective implementation has been repeatedly stressed by the Executive Committee. The Convention and its Protocol together are the most comprehensive instruments adopted to date on a universal level to safeguard the fundamental rights of refugees and to regulate their status in countries of asylum. As such, they are fundamental to the international regime of refugee protection. They help in ensuring that refugees are granted basic humanitarian treatment. UNHCR has been mandated by the international community with the particular responsibility to ensure effective implementation of the Convention and Protocol within the overall framework of its protection responsibilities. The Office is specifically called upon, pursuant to paragraph a a of its Statute, inter alia, to supervise the application of international conventions for the protection of refugees. The Note also recognized, as a first step, the need for more States to respond to the questionnaire on implementation. It is also clear, however, that discussion would benefit from going beyond mere restatement of this commitment to identifying practical suggestions to strengthen implementation. Accordingly, the Sub-Committee is invited to reconsider the suggestions put to the forty-second session. Other ideas which might, at the same time, be considered could include periodic meetings of States Parties to review problems and progress on implementation. There might also be appropriate steps taken at the regional level to harmonize interpretation and application of the Convention among neighbouring countries, including giving existing regional human rights commissions, or courts, certain refugee-related responsibilities. Regional bodies are the obvious interlocutors in pursuing regional approaches to ensure respect for protection standards and to achieve harmonized approaches. Improving monitoring arrangements, as suggested in previous paragraphs, would considerably facilitate better implementation. At the same time, however, there are a number of obstacles impeding full and proper implementation which monitoring will not necessarily remove. They are more appropriately addressed through clearly targeted promotion campaigns. Legal obstacles to proper implementation include the clash of, or inconsistencies between, existing national laws and certain Convention obligations; failure to incorporate the Convention into national law through specific implementing legislation; or implementing legislation which defines not the rights of the individuals but rather the powers vested in refugee officials. As to the latter, this means that protection of refugee rights becomes an exercise of powers and discretion by officials, rather than enforcement of specific rights identified and guaranteed by law. Where the judiciary has an important role in protecting refugee rights, restrictive interpretations can also be an impediment to full implementation. Finally, the maintenance of the geographic limitation by some countries is a serious obstacle to effective implementation. At another level, there are bureaucratic obstacles, including unwieldy, inefficient or inappropriate structures for dealing with refugees, a dearth of manpower generally or of adequately trained officials, and the non-availability of expert assistance for asylum-seekers. Finally, there are certain problems of perception at the governmental level, including that the grant of asylum is a political statement and can be an irritant in inter-state relations. Strengthened training, promotion and public information activities are required to overcome these various problems. A promotion campaign could be built around implementation of the Convention which would, inter alia, address these difficulties and would involve intensified training of officials and other key groups journalists, lawyers, the judiciary, non-governmental organizations NGOs and opinion-makers generally. In addition there is a need to build up local support bases

for fair treatment of refugees, in accordance with Convention standards. One possibility in this regard is the creation of National Refugee Councils, consisting of senior Government administrators, NGO representatives and those of religious groups, as well as other prominent individuals, to sensitize national public opinion and enable UNHCR to receive counsel and advice from a broader range of interlocutors. Difficulties in fulfilling Convention obligations covering point c Replies received to the questionnaire show clearly that some States have difficulties in fulfilling all of their obligations under the Convention. This is understandable, since the Convention contains comprehensive provisions concerning the rights of refugees in a number of diverse areas. Even under the best of circumstances, States may occasionally find that public opinion does not understand, or support, efforts undertaken on behalf of refugees. When States are suffering from adverse economic conditions, lack of development or high unemployment, it can become all the more difficult to guarantee the basic needs of refugees, especially when those of the national population are not able to be fully met. Nonetheless, although States may face constraints in implementing the Convention completely, there are certain provisions which are so fundamental to refugee protection that any deviation from them is always a matter of paramount concern to UNHCR. One such provision is Article 33 which enshrines the principle of non-refoulement. Article 33 of the Convention and its prohibition on return of individuals to situations threatening life or liberty is a fundamental guarantee of refugee protection. It must be read together, in particular, with Articles 31 non-penalization for illegal entry and 32 limits to expulsion: This is the case as regards the refugee definition Article 1 , non-discrimination Article 3 , freedom of religion Article 4 , non-penalization of refugees unlawfully in the country of refuge Article 31 , explusion Article 32 and the prohibition of refoulement Article Other provisions of the Convention, such as those defining the economic and social rights of refugees, are more relevant to refugees who have been granted durable asylum by a contracting State and are intended to facilitate their integration in their asylum country. There will be large-scale influx situations which may fall within the parameters of the Convention but because of their massive character and the clear feasibility of return in safety at some point, repatriation not integration is the appropriate approach. Varying interpretations and selective application of the definition covering Point d The imprecision of the language to some extent facilitates selective interpretation or application. As some States Parties have observed, the Convention does not, for example, contain a definition of persecution. The Convention sets no time limits as to when the persecution should have arisen. What sort of post-flight situations should be regarded as sufficient to serve as a foundation for a fear of persecution is not fully clear. Where the Convention is not precise, the courts or Refugee Boards have moved to fill the gaps. In this process, as the numbers of asylum-seekers continue to rise, divergence is apparent between the profiles of a percentage of the asylum-seekers and the classical concept of refugee. This approach is often revealed in decisions on refugee status which narrow the meaning of the terms persecution and well-founded fear. Examples which have come to the attention of the Office include refusal to regard severe or repeated discrimination or harassment as persecution; reluctance to recognize situations of group persecution; rejection of draft evasion or desertion for valid reasons of conscience as a basis for a claim; little or no consideration of the situation of women as a particular social group; limiting the notion of "agents of persecution" to the authorities of the country of origin; and setting of arbitrary time limits on how recently the persecution must have occurred. With respect to well-founded fear, negative decisions are taken based on subjective assessments of general credibility, with a growing inclination to see uncorroborated testimony as inherently self-serving and without acknowledging the reality that, as has always been the case, many refugees will not have been able to bring forward independent evidence to substantiate their claim. Other troubling cases include denials based on irregularities in the manner of entry, even if such an entry was the only means of escape, and rejection of status for persons fleeing from war or other armed conflict or violence, without investigating the possibility of persecution which may well exist in such situations. The Office has been particularly concerned about a number of recent cases involving individual refugee status applicants whose claims have been denied essentially because they have been viewed as victims of armed conflicts rather than of specifically targeted

persecution. Even where it has been accepted by the determining authorities that an individual has suffered serious human rights abuses, that he or she has a genuine fear and that there is a distinct likelihood of arrest and detention on return, the position has been taken that these factors are not attributable to any intention on the part of the authorities to persecute the individual concerned on account of one of the recognized grounds and that, accordingly, there is no issue of refugee status involved. There is nothing in the definition itself which would exclude its application to persons caught up in civil war who meet the definition. The interest of the Government neither explains nor excuses the use of torture or arbitrary punishment, or the discriminatory singling out of certain individuals or groups for punishment. It should also be noted that, in accordance with the Vienna Convention on the Law of Treaties, States should interpret the Convention in a way which is consistent with its object and purpose. The object and purposes of the Convention are clear from the context in which the Convention was negotiated. It was an instrument designed to assure refugees the widest possible exercise of their rights, and to provide a framework within which to structure the exercise by States of their discretion to receive refugees and accord them those rights. In its consideration of this issue, the Sub-Committee might judge it useful to encourage all States Parties to approach interpretation of Article 1 in a manner consistent with the object and purposes of the Convention.

DOWNLOAD PDF IMPLEMENTATION OF THE BASIC COLLECTION PROTOCOL

Chapter 4 : The Collection Interface (The Javaâ„¢ Tutorials > Collections > Interfaces)

The protocol underlying this Java-only implementation is known as Java Remote Method Protocol (JRMP). In order to support code running in a non-JVM context, programmers later developed a CORBA version.

Overriding Swift Protocol Extension Default Implementations How to avoid unexpected behavior when subclassing types which conform to protocols. Swift encourages protocol oriented development and default implementations provide a powerful tool for composing types. Using these tools in combination with class inheritance has some surprising consequences which can result in unexpected behavior. You can also find these examples as an Xcode Playground. Most of the time I want to use some common default configuration. So I extend the protocol with a default implementation to specify that default configuration file: When I create Configurable structs this works great. My types get the default implementation but can also provide their own version: I can also create Configurable classes. At first this works fine: Problems appear When I subclass a Configurable class suddenly I have a problem: Here my parent baseView class is using self to invoke the default implementation of a Configurable method. Solutions One workaround is to drop the default implementation. If we have a small number of classes adopting Configurable this might be fine. However when we have lots of Configurable types this becomes less satisfying. The swift evolution mailing list suggests two additional workarounds. If classes always implement protocol methods and call any default implementations then they will always use dynamic dispatching and be able to invoke overrides from subclasses. Calling default implementations can be a little tricky as well. One option is to avoid default implementations of methods declared in the protocol. Unfortunately this means that when we implement a class we need to remember to check the protocol extension and implement every method found there, even though they do not appear in the protocol declaration. A second option is to define a wrapper type which can use a statically dispatched call to the default implementation. This allows us to include function declarations in our protocol definition but a large protocol with many required methods requires a large wrapper class. This causes confusing behavior where a subclass can implement protocol methods only to discover that they are never called from behavior inherited from a superclass. This can be a source of confusing bugs and identifying the root cause requires inspecting the behavior of all our parent classes. Something that can be especially difficult if we were to subclass a framework provided class. To avoid creating types which are likely to introduce bugs in the future we should do one of the following: Use only value types with behaviors composed from protocol default implementations. Use classes and restrict ourselves to adopting protocols without default implementations. Use final classes when adopting protocols with default implementations so we cannot have problematic subclasses. When defining a non-final class which implements protocols with default implementations reimplement those protocol methods and call the default implementation. In my current work at Good Eggs I chose option number 2. I needed class types but it was reasonable for us to implement our shared behavior on a base class and use class inheritance rather than protocol conformance to compose types. If I were publishing a framework containing reference types then I would use options 3 and 4 to protect consumers of my types. Subclass with caution and happy coding. Good Eggs connects people who love food, directly with people who make it. We deliver the most incredible food, straight to Bay Area homes. If you are inspired by our mission is to grow and sustain local food systems worldwide, find out how you can help.

DOWNLOAD PDF IMPLEMENTATION OF THE BASIC COLLECTION PROTOCOL

Chapter 5 : Java remote method invocation - Wikipedia

Overriding Swift Protocol Extension Default Implementations. How to avoid unexpected behavior when subclassing types which conform to protocols. Swift encourages protocol oriented development and default implementations provide a powerful tool for composing types. Using these tools in combination with class inheritance has some surprising consequences which can result in unexpected behavior.

Support for other audio and video codecs is optional. Collectively, terminals, multipoint control units and gateways are often referred to as endpoints. While not all elements are required, at least two terminals are required in order to enable communication between two people. They might exist in the form of a simple IP phone or a powerful high-definition videoconferencing system. The diagram, figure 1, depicts a complete, sophisticated stack that provides support for voice, video, and various forms of data communication. In reality, most H. Multipoint control units[edit] A multipoint control unit MCU is responsible for managing multipoint conferences and is composed of two logical entities referred to as the Multipoint Controller MC and the Multipoint Processor MP. The most significant difference, however, is that H. Some MCUs also provide multipoint data collaboration capabilities. What this means to the end user is that, by placing a video call into an H. Gateways[edit] Gateways are devices that enable communication between H. If one party in a conversation is utilizing a terminal that is not an H. Gateways are widely used today in order to enable the legacy PSTN phones to interconnect with the large, international H. Gateways are also used within the enterprise in order to enable enterprise IP phones to communicate through the service provider to users on the PSTN. Gateways are also used in order to enable videoconferencing devices based on H. Most of the third generation 3G mobile networks deployed today utilize the H. Gatekeepers[edit] A Gatekeeper is an optional component in the H. Those services include endpoint registration, address resolution, admission control, user authentication, and so forth. Of the various functions performed by the gatekeeper, address resolution is the most important as it enables two endpoints to contact each other without either endpoint having to know the IP address of the other endpoint. Gatekeepers may be designed to operate in one of two signaling modes, namely "direct routed" and "gatekeeper routed" mode. Direct routed mode is the most efficient and most widely deployed mode. In this mode, endpoints utilize the RAS protocol in order to learn the IP address of the remote endpoint and a call is established directly with the remote device. In the gatekeeper routed mode, call signaling always passes through the gatekeeper. While the latter requires the gatekeeper to have more processing power, it also gives the gatekeeper complete control over the call and the ability to provide supplementary services on behalf of the endpoints. Likewise, gatekeepers use RAS to communicate with other gatekeepers. A collection of endpoints that are registered to a single Gatekeeper in H. This collection of devices does not necessarily have to have an associated physical topology. Rather, a zone may be entirely logical and is arbitrarily defined by the network administrator. Gatekeepers have the ability to neighbor together so that call resolution can happen between zones. Neighboring facilitates the use of dial plans such as the Global Dialing Scheme. Border elements and peer elements[edit] Figure 2 - An illustration of an administrative domain with border elements, peer elements, and gatekeepers Border Elements and Peer Elements are optional entities similar to a Gatekeeper, but that do not manage endpoints directly and provide some services that are not described in the RAS protocol. The role of a border or peer element is understood via the definition of an " administrative domain ". An administrative domain is the collection of all zones that are under the control of a single person or organization, such as a service provider. Within a service provider network there may be hundreds or thousands of gateway devices, telephones, video terminals, or other H. The service provider might arrange devices into "zones" that enable the service provider to best manage all of the devices under its control, such as logical arrangement by city. Taken together, all of the zones within the service provider network would appear to another service provider as an "administrative domain". The border element is a signaling entity that generally sits at the edge of the administrative domain and communicates with another administrative domain.

This communication might include such things as access authorization information; call pricing information; or other important data necessary to enable communication between the two administrative domains. Peer elements are entities within the administrative domain that, more or less, help to propagate information learned from the border elements throughout the administrative domain. Such architecture is intended to enable large-scale deployments within carrier networks and to enable services such as clearinghouses. The diagram, figure 2, provides an illustration of an administrative domain with border elements, peer elements, and gatekeepers. The syntax of the protocol is defined in ASN. Below is an overview of the various communication flows in H. Setup and Setup acknowledge.

DOWNLOAD PDF IMPLEMENTATION OF THE BASIC COLLECTION PROTOCOL

Chapter 6 : Overriding Swift Protocol Extension Default Implementations

data collection measures that will be used during the baseline data collection phase of the FBA (i.e., data collected before the intervention is designed and implemented). For example, if the.

Communicating systems[edit] The information exchanged between devices through a network or other media is governed by rules and conventions that can be set out in communication protocol specifications. The nature of a communication, the actual data exchanged and any state -dependent behaviors, is defined by these specifications. In digital computing systems, the rules can be expressed by algorithms and data structures. Protocols are to communication what algorithms or programming languages are to computations. This communication is governed by well-understood protocols, which can be embedded in the process code itself. Transmission is not necessarily reliable, and individual systems may use different hardware or operating systems. This framework implements the networking functionality of the operating system. At the time the Internet was developed, abstraction layering had proven to be a successful design approach for both compiler and operating system design and, given the similarities between programming languages and communication protocols, the originally monolithic networking programs were decomposed into cooperating protocols. Instead they use a set of cooperating protocols, sometimes called a protocol suite. The protocols can be arranged based on functionality in groups, for instance there is a group of transport protocols. The functionalities are mapped onto the layers, each layer solving a distinct class of problems relating to, for instance: The selection of the next protocol is accomplished by extending the message with a protocol selector for each layer. The data received has to be evaluated in the context of the progress of the conversation, a protocol therefore must include rules describing the context. These kind of rules are said to express the syntax of the communication. Other rules determine whether the data is meaningful for the context in which the exchange takes place. These kind of rules are said to express the semantics of the communication. Messages are sent and received on communicating systems to establish communication. Protocols should therefore specify rules governing the transmission. In general, much of the following should be addressed: The bitstrings are divided in fields and each field carries information relevant to the protocol. Conceptually the bitstring is divided into two parts called the header and the payload. The actual message is carried in the payload. The header area contains the fields with relevance to the operation of the protocol. Bitstrings longer than the maximum transmission unit MTU are divided in pieces of appropriate size. The addresses are carried in the header area of the bitstrings, allowing the receivers to determine whether the bitstrings are of interest and should be processed or should be ignored. A connection between a sender and a receiver can be identified using an address pair sender address, receiver address. Usually some address values have special meanings. An all-1s address could be taken to mean an addressing of all stations on the network, so sending to this address would result in a broadcast on the local network. The rules describing the meanings of the address value are collectively called an addressing scheme. This is referred to as address mapping. On the Internet, the networks are connected using routers. The interconnection of networks through routers is called internetworking. Detection of transmission errors Error detection is necessary on networks where data corruption is possible. In a common approach, CRCs of the data area are added to the end of packets, making it possible for the receiver to detect differences caused by corruption. The receiver rejects the packets on CRC differences and arranges somehow for retransmission. Acknowledgements are sent from receivers back to their respective senders. To cope with this, under some protocols, a sender may expect an acknowledgement of correct reception from the receiver within a certain amount of time. Thus, on timeouts , the sender may need to retransmit the information. Exceeding the retry limit is considered an error. This is known as media access control. Arrangements have to be made to accommodate the case of collision or contention where two parties respectively simultaneously transmit or wish to transmit. As a result, pieces may arrive out of sequence. Retransmissions can result in duplicate pieces. By marking the pieces with sequence information at the sender,

the receiver can determine what was lost or duplicated, ask for necessary retransmissions and reassemble the original message. Flow control can be implemented by messaging from receiver to sender. Design of complex protocols often involves decomposition into simpler, cooperating protocols. Such a set of cooperating protocols is sometimes called a protocol family or a protocol suite, [10] within a conceptual framework. Communicating systems operate concurrently. An important aspect of concurrent programming is the synchronization of software for receiving and transmitting messages of communication in proper sequencing. Concurrent programming has traditionally been a topic in operating systems theory texts. Mealy and Moore machines are in use as design tools in digital electronics systems encountered in the form of hardware used in telecommunication or electronic devices in general. In analogy, a transfer mechanism of a protocol is comparable to a central processing unit CPU. The framework introduces rules that allow the programmer to design cooperating protocols independently of one another. Protocols are to computer communication what programming languages are to computation. In modern protocol design, protocols are layered to form a protocol stack. Layering is a design principle which divides the protocol design task into smaller steps, each of which accomplishes a specific part, interacting with the other parts of the protocol only in a small number of well-defined ways. Layering allows the parts of a protocol to be designed and tested without a combinatorial explosion of cases, keeping each design relatively simple. Layering also permits familiar protocols to be adapted to unusual circumstances. For example, the mail protocol can be adapted to send messages to aircraft by changing the V. The communication protocols in use in the Internet are designed to function in diverse and complex settings. This model was expanded to four layers by additional protocols. However, the Internet protocol development has not focussed on the principle of layering as mandatory recipe for communication, rather it evolved as a convenient description of modularity and protocol cooperation. A different model is the OSI seven layer model , which was developed internationally as a rigorous reference model for general communication, with much stricter rules of protocol interaction and a rigorous layering concept of functionality. Typically, application software is built upon a robust data transport layer. Underlying this transport layer is a datagram delivery and routing mechanism that is typically connectionless in the Internet. Packet relaying across networks happens over another layer that involves only network link technologies, which are often specific to certain physical layer technologies, such as Ethernet. Layering provides opportunities to exchange technologies when needed, for example, protocols are often stacked in a tunneling arrangement to accommodate connection of dissimilar networks. Protocol layering[edit] Figure 3. Message flows using a protocol suite. Black loops show the actual messaging loops, red loops are the effective communication between layers enabled by the lower layers. Protocol layering now forms the basis of protocol design. The Internet protocol suite consists of the following layers: Computations deal with algorithms and data and communication involves protocols and messages, so the analog of a data flow diagram is some kind of message flow diagram. The systems both make use of the same protocol suite. The vertical flows and protocols are in system and the horizontal message flows and protocols are between systems. The message flows are governed by rules, and data formats specified by protocols. The blue lines therefore mark the boundaries of the horizontal protocol layers. The horizontal protocols are layered protocols and all belong to the protocol suite. Layered protocols allow the protocol designer to concentrate on one layer at a time, without worrying about how other layers perform. This can be achieved using a technique called Encapsulation. The pieces contain a header area and a data area. The result is that at the lowest level the piece looks like this: This rule therefore ensures that the protocol layering principle holds and effectively virtualizes all but the lowest transmission lines, so for this reason some message flows are coloured red in figure 3. To ensure both sides use the same protocol, the pieces also carry data identifying the protocol in their header. The design of the protocol layering and the network or Internet architecture are interrelated, so one cannot be designed without the other. The Internet offers universal interconnection, which means that any pair of computers connected to the Internet is allowed to communicate. Each computer is identified by an address on the Internet. All the interconnected physical networks appear to the user as a single large network. This interconnection scheme is

called an internetwork or internet. The netid identifies a network and the hostid identifies a host. The term host is misleading in that an individual computer can have multiple network interfaces each having its own Internet address. An Internet Address identifies a connection to the network, not an individual computer. The mapping is called address resolution. This way physical addresses are only used by the protocols of the network interface layer. Message flows in the presence of a router Physical networks are interconnected by routers. Routers forward packets between interconnected networks making it possible for hosts to reach hosts on other physical networks. The message flows between two communicating systems A and B in the presence of a router R are illustrated in figure 4. Datagrams are passed from router to router until a router is reached that can deliver the datagram on a physically attached network called direct delivery. The table consists of pairs of networkids and the paths to be taken to reach known networks.