IST6/-/2 795 Revised

Issues relating to IDRP QoS, Security and Priority Path Attributes

Author: UK Expert

Date: 21 January, 1993

1. Introduction

This paper has been developed to discuss and provide proposed editorial changes to the following perceived problems in the DIS text of 10747:

1. The incorrect and misleading distinction between source and destination in the context of the QoS and Security path attributes.

2. The absence of support for the globally unique parameter in ISO 8473

3. Incorrect handling of multiple routes to the same destination with different priorities and/or security related information.

4. Efficiency concerns in respect of the handling of routes that contain security attributes.

5. Incorrect forwarding rules when priority and security attributes are present in an NPDU header.

These issues are discussed below with proposed editorial instructions to put into effect the identified solutions, provided in section 7.

2. Source and Destination QoS Attributes

2.1 Discussion

2.1.1 ISO 8473

ISO 8473 specifies a *Quality of Service maintenance* parameter, which may be encoded in the optional part of the ISO 8473 header. Three formats are specified for this parameter: Globally Unique, Source Address Specific and Destination Address Specific.

- The Globally Unique format permits the sender to specify a partial ranking of the service metrics: sequence preservation probability, transit delay, cost, and residual error probability. When this parameter is provided by the sender, an intermediate system that reports congestion may also set a flag bit in the parameter in order to report congestion experienced.

- The Source Address Specific format permits the sender to specify a quality of service requirement that is "unique and unambiguous in the context of the QoS Maintenance System employed by the authority responsible for assigning the source NSAP Address."

- The Destination Address Specific format permits the sender to specify a quality of service requirement that is "unique and unambiguous in the context of the QoS Maintenance System employed by the authority responsible for assigning the destination NSAP Address."

The semantics of both the source and destination specific QoS requirements are thus outside of the scope of the standard. However, these are not really different parameters. They are simply alternative methods for identifying the responsible QoS Authority, and hence the syntax and semantics of the QoS parameter.

For example, the administrator of a Routing Domain may define a syntax and corresponding semantics for a QoS Maintenance parameter. This parameter may be used whenever an NPDU originates in the RD, or has a destination address within the RD. This parameter is recognised by all systems within the RD and may also be recognised by systems outside of the RD. When an NPDU originates within the RD, the QoS Maintenance parameter is encoded as a source specific QoS Maintenance Parameter, and systems recognise it by relating the source NSAP Address to a system within the RD of the administrator that had defined the parameter. Similarly, when an NPDU originates outside the RD with a destination within the RD, the QoS Maintenance parameter is encoded as a destination specific QoS Maintenance Parameter, and systems recognise it by relating the destination NSAP Address to a system within the RD of the administrator that had defined the parameter. When the NPDU has both a source and destination within the RD, then it is arbitrary as to whether the QoS parameter is encoded as a source specific QoS Maintenance Parameter or a destination specific QoS Maintenance Parameter; it is correctly recognised in both cases

2.1.2 DIS 10747

The IDRP DIS text specifies path attributes for:

- the Transit Delay, Residual Error Probability, and Expense QoS metrics

- a Capacity metric

- Source Specific QoS

- Destination Specific QoS

The Transit Delay, Residual Error Probability, and Expense path attributes aggregate across all path segments, the maximum transit delay, etc. that may be experienced on the route. The capacity metric provides an indication of the capacity of the path segment with the lowest potential throughput.

The Transit Delay, Residual Error Probability, Expense and Capacity path attributes are all used to assist in the selection of the preferred route when two or more routes exist to the same destination and are described by the same set of distinguishing path attributes. When routes exist that are described by different sets of distinguishing path attributes then the preferred route for an NPDU may depend on the QoS Requirements expressed by the sender.

The semantics of the Source and Destination Specific QoS Path Attributes are outside of the scope of the standard.

On inspection of the above, a question that arises is, what does source and destination mean in the context of an IDRP route? There is firstly not one but possibly many destinations for a route, as to the source: that is not determinant until an NPDU is actually sent. IDRP simply copies the notion of Source and Destination QoS from ISO 8473. However, in 8473, as discussed above, the "source" and "destination" tags are no more than a means for identifying the context in which the QoS Requirements are expressed. But in the context of IDRP, such tags are meaningless.

IDRP has a similar need to identify the QoS Authority responsible for specifying a user defined QoS metric provided as a path attribute, and indeed this is actually done in the value of each of these path attributes which includes the NSAP Address Prefix which identifies the defining context. Having separate Source and Destination QoS Path attributes is simply a distraction which confuses the issue. The IDRP requirement should be to provide a mechanism for expressing additional QoS metrics and identifying the context under which they are specified. The need for this change can be understood through consideration of the following two examples.

2.1.2.1 Example #1: Upper Bound on Expense

An Administrative Domain Administrator specifies a new QoS parameter to contain a maximum acceptable cost/kByte for data transfer; this new parameter may then, say, be defined in the context of the Administrative Domain's NSAP Addressing subdomain, and thus may be used as a source or destination QoS parameter, whenever, respectively, the source or destination NSAP Address is located in that addressing subdomain.

However, in this case the NPDU-Derived Distinguishing attribute is not a user specified IDRP QoS path attribute, but the existing IDRP path attribute EXPENSE. Furthermore, even though this path attribute is type specific, a matching rule is required, but the matching rule is not *equality* (which is the only such matching rule specified in the DIS text), but is instead, *not greater than*.

2.1.2.2 Example #2: Extension of Globally Unique QoS Maintenance Parameter

An Administrative Domain Administrator defines a new QoS parameter that is an extended version of the existing globally unique QoS parameter (ISO 8473 permits either source/destination QoS or Globally unique, but not both), perhaps to add a low "probability of duplication vs transit delay" bit. To make this effective also demands an IDRP user defined QoS path attribute (for duplication probability).

However, the corresponding NPDU-Derived Distinguishing attribute is not necessarily this new path attribute, but is instead determined from an extended version of table 4 in the DIS text, taking into account the additional "bit" and the user defined IDRP QoS path attribute, and no further matching rules are required (all the path attributes are properly type specific).

2.1.2.3 Conclusion

In neither of these examples, is the requirement met by some additional IDRP attribute with a value that matches for equality, with the corresponding ISO 8473 header parameter. The BIS needs to understand the NPDU's QoS maintenance parameter, and map it to the appropriate path attribute. This may be a "built-in" attribute, or a new user defined path attribute.

2.2 Proposed Solution

An appropriate solution would appear to be to define a single QoS path attribute ("LOCALLY DEFINED QOS") containing a QoS measurement (e.g. probability of duplication) and associated metric (i.e. the actual probability) defined in the context of some QoS Authority.

It is therefore proposed that the SOURCE SPECIFIC QOS and the DESTINATION SPECIFIC QOS path attributes are replaced by a single LOCALLY DEFINED QOS path attribute.

Consequential changes to the forwarding procedures are also required. These are discussed in 6, below.

It is also observed that the scenario discussed in 2.1.2.1 may only be realised if the QoS metric value is available in the FIB for reference during the forwarding process.

3. Source and Destination Security Attributes

3.1. Discussion

ISO 8473 specifies a *Security* parameter, which may be encoded in the optional part of the ISO 8473 header. Three formats are specified for this parameter: Globally Unique, Source Address Specific and Destination Address Specific.

- The Globally Unique format permits the sender to specify a globally unique and unambiguous security level..
- The Source Address Specific format permits the sender to specify a security level that is "unique and unambiguous in the context of the Security Classification System employed by the authority responsible for assigning the source NSAP Address."
- The Destination Address Specific format permits the sender to specify a security level that is "unique and unambiguous in the context of the Security Classification System employed by the authority responsible for assigning the destination NSAP Address."

The semantics of all formats of the Security parameter are outside of the scope of the standard.

The IDRP DIS text specifies path attributes for:

- Source Specific Security
- Destination Specific Security

The semantics of the Source and Destination Specific Security Path Attributes are outside of the scope of the IDRP standard, and may be used to reflect policy decisions that control the NPDUs permitted to traverse the route. However, IDRP does not provide a path attribute corresponding to the ISO 8473 Globally Unique format.

3.1.1. Globally Unique Security

Although there has been no internationally agreed specification for the ISO 8473 Globally Unique Security parameter, it now appears that this will change, and a specification will be developed to use this format to convey a registered object i.e. security related information specified by a registered Security Authority. A corresponding IDRP path attribute is thus required.

3.1.2. Source/Destination Security

The Source and Destination Specific Security Path Attributes are specified in much the same way as the Source and Destination Specific QoS Path Attributes, and similar comments apply. Source and Destination are meaningless terms in the context of IDRP, and only a single user specified security path attribute is necessary for support of ISO 8473 source and destination specific security parameters.

In fact, it is also doubtful whether such a path attribute needs to be different from one in support of globally unique security. A security parameter defined in the context of the source or destination NSAP Address, need not be any different from a security parameter defined in the context of a registered security authority. They are just different ways of identifying the responsible Security Authority and hence the syntax and semantics of the security parameter. All IDRP needs to provide is a means of identifying the Security Authority responsible for defining the security path attribute value's syntax and semantics, and a registration identifier and an NSAP Address Prefix are just simply alternative means of identifying such an authority, and could either or both be reasonably present in the same path attribute.

3.2. Proposed Solution

It is therefore proposed that IDRP defines a single security path attribute ("SECURITY") which consists of:

1. an identifier identifying the responsible Security Authority, which may be encoded as a registration identifier, an NSAP Address Prefix, or both; and

2. a security parameter providing security related information about the route.

Consequential changes to the forwarding procedures are discussed in 6, below.

4. Priority

4.2 Discussion

ISO 8473 specifies a *priority* parameter, which may be encoded in the optional part of the ISO 8473 header. This permits the sender to give each PDU a relative priority, expressed as an integer in the range 0..14. Intermediate Systems that allocate resources on a priority driven basis can then give higher preference to PDUs with a higher priority level.

The IDRP DIS text specifies a path attribute that indicates the minimum priority a PDU must possess before being permitted to use the corresponding route. The priority path attribute is used to reflect policy decisions that control the NPDUs permitted to traverse the route. It is a type specific Distinguishing path attribute.

The ISO 8473 specification for the priority path attribute is straightforward enough. Each NPDU can have a relative priority assigned to it, and that relative priority may then be used to apportion communication resources between traffic with different levels of urgency. The most obvious use of this is when different output queues are maintained for each priority level. When, say, an ISO 8208 SNDCF is employed, these queues may even lead to virtual circuits set up with a corresponding priority level. Although priority is a DTE specific parameter, there do exist examples of specially modified ISO 8208 networks which also internally assign resources to virtual circuits based on the circuit's priority level.

The routing decision can also be affected by an NPDU's priority level. This comes about when a subnetwork or data link is restricted to traffic of certain priority levels only, either during certain times of the day, or permanently.

However, in IDRP, there is a potential problem over route selection with this type of path attribute.

The IDRP protocol machine first receives each route into a *adj-RIB-in* selected according to the BIS advertising the route and the set of distinguishing path attributes present. The Decision Process then selects the preferred route out of all those available to the same destination(s) and present in *adj-*

*RIB-in*s identified by the same set of distinguishing path attributes. Each selected route is then placed in the *loc-RIB* identified by that set of distinguishing path attributes. Routes in a *loc-RIB* are used both to construct the forwarding information base and, as the basis for the routes advertised to other BISs.

In IDRP, *priority* is specified as a type specific distinguishing path attribute, and with this specification, if two or more routes with different priority levels but to the same destination(s) are present in separate *adj-RIB-in*s identified by the same set of distinguishing path attributes, then only one of these routes will be selected, typically that with the lowest priority level associated with it. The result of this is that the route reserved for urgent traffic, say, will never be used, even by data with a suitably high priority level, which seems to defeat the whole purpose of the path attribute.

4.2 Proposed Solution

One way to avoid this problem is for the priority path attribute to be redefined as a type-value specific distinguishing path attribute. However, in order for a BIS to support all priority levels (i.e. 0..14), this implies that fifteen times the number of RIB-Atts must be available between two BISs, and hence fifteen times the number of Adj-RIB-Ins, etc. This is not readily supportable.

Alternatively, the priority path attribute may retain its type specific status, which is reasonable as it is unlikely that a BIS will need to advertise multiple routes to the same destination, each with a different priorities; such routes may readily be aggregated. However, in order to counter the perceived problem, it will be necessary to permit a loc-RIB, and hence FIB, to contain more than one route to the same destination provided that they have different priority levels. The route with the highest usable priority may then be selected on a per NPDU basis. Such routes must then be aggregated before being advertised to other BISs. The need for multiple routes to exist in the same loc-RIB should only arise when the higher priority route is also the more preferable according to performance based selection criteria.

Although this proposed change seems to have significant philosophical impact on the IDRP model, it does not appear to result in any ambiguity, or cause the externally visible behaviour of a BIS to change. In fact, it is really just a trick for merging loc-RIBs and FIBs that would otherwise have to be identified by discrete RIB-Atts, and so is believed to be readily acceptable.

The current IDRP text also requires that when two routes with different values of the priority path attribute are aggregated then the highest priority level is selected. This is correct given that, in general, the destinations of the aggregated routes will be different, and not all destinations of the aggregated route with be reachable at any lower priority level. However, this needs to be changed if change is put into effect, so that the lowest priority level is selected if the destination(s) are the same.

5. Efficient Secure Routing

5.1. Discussion

A BIS may receive several routes, to the same destination, from different BISs, and each distinguished by the value of the SECURITY attribute (i.e. defined with reference to the same security authority, but containing different security related information). Each of those routes may not necessarily be suitable for the same NPDUs, and each one needs to be made available to the forwarding process. This is because security considerations do not necessarily partition routes into a strict hierarchy. Routes may provide differing degrees of protection, and have non-overlapping access restrictions.

The present specification does permit each such route to be made available to the forwarding process. This is because each discrete value of a SECURITY attribute distinguishes a RIB-Att.

However, under many Security Policies, the number of possible values of a Security Label could be large, resulting in an even larger number of RIB-Atts given the different combinations of Security, Priority and QoS attributes possible. The feasibility of this has to be questioned.

5.2. Proposed Solution

The solution proposed, is essentially to use the same "trick" as for priority. Firstly, the specification is changed so that only the Security Authority Identifier is used to disambiguate different RIB-Atts. Secondly, more than one route to the same destination may appear in a single loc-RIB/FIB provided that such routes have different security related information. Such routes must then always be aggregated before being advertised to other BISs.

The security related information is then referenced during the forwarding process as discussed in 6 below.

6. The Forwarding Process

6.1. Discussion

6.1.1. Derivation of the NPDU-Derived Distinguishing attributes for the QoS Maintenance Parameter

Clause 8.3 of the DIS text provides rules for determining the NPDU-Derived Distinguishing attributes, and provides additional matching rules if the NPDU-Derived Distinguishing attributes are type-value specific. In the case of source/destination QOS, the NPDU-Derived Distinguishing attributes are the Source and Destination QoS path attributes (which are type-value specific) and match only if equal. However, this appears to ignore likely user requirements for use of, say, source/destination QoS in ISO 8473, as illustrated by the examples in 2.1.2.

These examples illustrate that the relationship between ISO 8473 QoS Requirements and IDRP QoS Path Attributes is not something that can necessarily be fixed by the base standard and needs, like Routing Policy, to be something that can be expressed as a set of rules which the describe the effective QoS Maintenance System. Then it will be possible to define additional QoS parameters for ISO 8473 that make reference to the standard set of QoS Metrics specified by the IDRP base standard; to both the standard set and additional QoS metrics; or to additional QoS metrics alone.

The DIS text already recognises that insofar as route aggregation and the updating of attributes are concerned, a BIS must have knowledge of the semantics of user defined QoS attributes. It seems perverse then to try and implement the forwarding process without assuming similar knowledge.

The principle should be that an Intermediate System only interprets QoS parameters for which it understands the semantics. The DIS text should be amended to state that whenever an NPDU contains a source or destination QoS parameter then the derivation of the NPDU-Derived Distinguishing path attributes and the corresponding matching rule (if any) is as specified by the QoS Authority (as implied by the source or destination NSAP Address, respectively) responsible for the specification of the QoS parameter . If the parameter is unrecognised then the default of no QoS NPDU-Derived Distinguishing path attributes should be used, which is in line with ISO 8473 clause 6.16.

6.1.2. The NPDU-Derived Distinguishing Attributes for the Security Attribute

The DIS text currently requires that the SOURCE SPECIFIC SECURITY path attribute is used as the NPDU-Derived Distinguishing Attribute if the source specific security parameter is present in the NPDU header, and, similarly, that the DESTINATION SPECIFIC SECURITY path attribute is used as the NPDU-Derived Distinguishing Attribute if the destination specific security parameter is present in the NPDU header. A FIB is then selected only if the corresponding path attribute is present in the RIB-Att and its value matches that of the NPDU's security parameter.

Even if the above is amended to refer to a single SECURITY attribute, as with QoS, matching for equality is unlikely to meet the user requirement.

The security related information present in an NPDU may be a protection requirement and/or a Security Label which may used to express a protection requirement and used for access control purposes. In IDRP, the security related information in a route may be an indication of the protection provided and/or a set of Security Labels that can be used both to indicate the suitability of a route (c.f. protection) as well as the limitations of use (c.f. access control).

If the security related information was limited to explicit indications of protection required and provided, then matching for equality may well suffice. However, the rules for matching Security Labels are both potentially complex and generally specific to a Security Policy.

For example, an NPDU Security Label may indicate a classification of, say, RESTRICTED in a typical hierarchical security system, with a security category of "blue eyes". A route's Security Label may indicate a classification of, say, SECRET, and a security category (caveat on use) of "brown eyes only". Under the effective Security Policy, the route may provide sufficient protection (its suitable for up to SECRET traffic), but the NPDU is not actually permitted to use the route, because it is for "brown eyes only". If the NPDU had a category of "brown eyes" instead of "blue eyes" then it would have been able to use the route. These kind of rules cannot be implemented with a simple matching criteria, unless perhaps all possible Security Labels were enumerated in the route. But this becomes prohibitive when the Security Policy identifies many different security categories.

As with QoS, it is wrong for the base standard to try and identify matching rules for security. Matching rules, and indeed, route aggregation and update rules, must be specified by the Security Authority that specifies the security related information used in the path attribute. They cannot be part of the base standard.

6.2 Proposed Solution

The specific of addition QoS attributes in IDRP or of ISO 8473 source/destination QoS Maintenance parameters implies a "QoS Policy" that is additional to that described by the base standard. The above analysis implies that this QoS Policy has to be understood by a BIS if it is to properly forward NPDUs under such a QoS Policy. A BIS already has a Policy Information Base in order to hold the effective Routing Policy, and it appears correct that this should be extended to hold the rules that comprise the QoS Policy as they relate to route aggregation and update and NPDU forwarding.

Similarly, a BIS needs to understand the effective Security Policy if routes are to be advertised and NPDUs forwarded in line with that Security Policy. To some extent the PIB already contains rules related to the Security Policy in respect of route advertisement. This needs to be extended to cover route aggregation and update and NPDU forwarding.

It should be noted that the DIS text already recognises that for source/destination QoS and Security attributes, the BIS must understand their semantics in order to perform aggregation and update of these attributes, but does not identify where these rules are held.

7. Proposed Editorial Changes

The proposed editorial changes are as follows.

7.1. Clause 5.2 Routeing Policy

Append to this clause:

The set of rules that comprises the Routing Policy enforced by a BIS are held in an Information Base separate from the RIB, and known as the Policy Information Base (PIB). Depending on local Security and QoS requirements, the PIB may also contain:

1. rules for the aggregation of routes including the SECURITY and LOCALLY DEFINED QOS path attributes (see clause 7.18.2)

2. rules for enforcing local QoS Maintenance Policies and the effective Security Policy, during NPDU forwarding

3. rules for updating SECURITY and LOCALLY DEFINED QOS path attributes in routes that are re-advertised to external RDs.

7.2. Table 1

Add to FIB "contains" list:

- a minimum priority associated with this subnetwork hop, when the RIB-Att contains a PRIORITY attribute

- security related information associated with this subnetwork hop, when the RIB-Att contains a SECURITY attribute

- the QoS metric value, when the RIB-Att contains a RESIDUAL ERROR, TRANSIT DELAY, EXPENSE, CAPACITY or LOCALLY DEFINED QOS attribute

7.3. Clause 6.2 OPEN PDU

Top of page 13, second bullet beginning "a type-value specific distinguishing attribute.........". Replace this bullet with:

- a type-value specific distinguishing attribute (see clause 7.11.2) is encoded as a triple <type, length, value>, using the type code for the attribute, the length in octets of the subsequent value, and the value itself, being encoded as follows for each such distinguishing attribute:

    i. **SECURITY:** the value shall comprise either the NSAP Address Prefix or the Security Registration Identifier, or both, that identifies the Security Authority for which security related information is supported by this RIB-Att, encoded identically to the encoding of the SECURITY attribute specified in clause 6.3 including length fields, but with a zero length security information.

ii. **LOCALLY DEFINED QOS:** the value shall comprise the NSAP Address Prefix of the QoS Authority and the QoS value that identifies the QoS measurement, encoded identically to the encoding of the LOCALLY DEFINED QOS attribute specified in clause 6.3 including length fields, but with a zero length metric.

7.4. Clause 6.3.*l* SOURCE SPECIFIC QOS

Change title to "LOCALLY DEFINED QOS"

Replace first paragraph with:

This is a well-known discretionary attribute whose variable length field contains the parameters associated with a QoS related path attribute defined by a QoS Authority that is outside of the scope of this international standard. The parameters of this attribute identify the QoS Authority, the name of the QoS measurement, and, optionally, a metric associated with that measurement.

Delete the last sentence of the definition of the NSAP (address) prefix length. *This is because only ISO 8348 can be the addressing authority for all NSAP Addresses.*

Replace the last sentence of the definition of the NSAP (address) prefix with:

This field identifies the QoS Authority and comprises an NSAP Address Prefix when the QoS Authority is also an NSAP Addressing Authority (see ISO 8473 clauses 7.5.6.1 and 7.5.6.2); the NSAP Address Prefix is that of the QoS Authority's Addressing Subdomain. When the QoS Authority is not also an NSAP Addressing Authority, then this field contains an NET that uniquely identifies the QoS Authority.

7.5. Clause 6.3.*m* DESTINATION SPECIFIC QOS

Delete this clause.

7.6. Clause 6.3.*p* SOURCE SPECIFIC SECURITY

Change title to "SECURITY"

Replace this clause with:

This is a well-known discretionary attribute whose variable length field contains the parameters associated with a security related path attribute defined by a Security Authority that is outside of the scope of this international standard. The parameters of this attribute identify the Security Authority, and some security related information, which may identify the protection provided by the route, a set of Security Labels associated with the route, or both. The syntax and semantics of the security related information are outside the scope of this international standard, and are specified by responsible Security Authority. The encoding of the attribute is as follows:

NSAP Address Prefix Length (1 octet)
NSAP Address Prefix (variable)
Security Registration ID Length (1 octet)
Security Registration ID (variable)
Length (2 octets)
Security Information (variable)

The use and meaning of the fields is as follows:

1) NSAP Address Prefix Length

   The length field indicates the length in bits of the NSAP Address Prefix (see 7.1.2.1) encoded in the following field. This field may be set to zero if the Security Authority is identified by a Security Registration Identifier, and no NSAP Address Prefix is provided.

2) NSAP Address Prefix

   If the Length field...........octet boundary. This field identifies the Security Authority and comprises an NSAP Address Prefix when the Security Authority is also an NSAP Addressing Authority (see ISO 8473 clauses 7.5.3.1 and 7.5.3.2); the NSAP Address Prefix is that of the Security Authority's Addressing Subdomain. When the Security Authority is not also an NSAP Addressing Authority, then this field contains an NET that uniquely identifies the Security Authority.

3) Security Registration ID Length

   This field contains the length in octets of the Security Authority's Security Registration Identifier. This field may be set to zero if the Security Authority is identified by an NSAP Address Prefix, and no Security Registration ID is provided. When both an NSAP Address Prefix and a Security Registration ID are present then they shall identify the same Security Authority.

4) Security Registration ID

   This variable length field contains the Security Registration Identifier of the Security Authority responsible for defining the following security information. The Security Registration Identifier is defined by ISO ????

5) Length

   This field contains the length in octets of the Security Information, as a non-zero unsigned integer. A value of zero is not permitted.

6) Security Information

This variable length field contains an integral number of octets comprising security related information specified by the Security Authority identified above. The syntax and semantics of this information are outside of the scope of this international standard.

7.7. Clause 6.3.𝓰 DESTINATION SPECIFIC SECURITY

Delete this clause.

7.8. Clause 7.11.2 Handling of Distinguishing Attributes

Replace list items (b) and (c) with:

b) Can include the SECURITY path attribute

c) can contain at most one of the distinguishing attributes: RESIDUAL ERROR, TRANSIT DELAY, EXPENSE, CAPACITY and LOCALLY DEFINED QOS .

7.9. Clause 7.11.3 Equivalent Distinguishing Attributes

Replace sentence beginning "Others can not be disambiguated..." with :

Others can not be disambiguated based solely on their type, but require knowledge of both their type, and a subset of the fields that comprise their value - namely SECURITY and LOCALLY DEFINED QOS.

7.10. Clause 7.12.12 SOURCE SPECIFIC QOS

Change title to "LOCALLY DEFINED QOS"

Replace first four paragraphs (i.e. all the clause except for the ordered list) with:

LOCALLY DEFINED QOS is a well known discretionary attribute that enables a QoS Authority to specify a QoS measurement that is not included in the set of QoS measurements specified in this international standard. The QoS Measurement is identified within the context of the QoS Authority, which is also responsible for specifying its name (QoS Value) and its semantics. A QoS Authority may specify as many QoS measurements as necessary, each distinguished by the QoS Value field.

When a BIS supports a LOCALLY DEFINED QOS measurement, this may be signalled to adjacent BISs in a RIB-Att as specified in clause 6.2. When support of a LOCALLY DEFINED QOS measurement is indicated in a RIB-Att, then the BIS shall support the adj-RIB-ins, adj-RIB-outs and a loc-RIB and a FIB corresponding to this RIB-Att. A BIS may only include a LOCALLY DEFINED QOS measurement in a RIB-Att when its PIB contains the rules necessary to support this measurement.

When a BIS re-distributes a route which has been learnt in an UPDATE PDU that contains a LOCALLY DEFINED QOS path attributes, then the new UPDATE PDU shall contain the same QoS Value and NSAP Address Prefix fields in the LOCALLY DEFINED QOS path attribute, and the metric fields (if present) shall be modified in the following way:

In last phrase of list item (b) replace "are not within the scope of IDRP" with "shall be specified in the PIB".

7.11. Clause 7.12.13 DESTINATION SPECIFIC QOS

Delete this clause.

7.12. Clause 7.12.16 SOURCE SPECIFIC SECURITY

Change title to "SECURITY"

Replace whole clause with:

SECURITY is a well known discretionary attribute that enables a Security Authority to specify security related information concerning a route. The security related information is identified within the context of the Security Authority, which is also responsible for specifying its semantics. Only one security attribute may be included in each route.

When a BIS is able to interpret and act on security related information specified by a given Security Authority, this may be signalled to adjacent BISs in a RIB-Att as specified in clause 6.2. When support of the SECURITY attribute is indicated in a RIB-Att, then the BIS shall support the adj-RIB-ins, adj-RIB-outs and a loc-RIB and a FIB corresponding to this RIB-Att. A BIS may only include a SECURITY distinguishing attribute in a RIB-Att when its PIB contains the rules necessary to interpret and act on the security related information for the identified Security Authority.

When a BIS re-distributes a route which has been learnt in an UPDATE PDU that contains a SECURITY distinguishing attribute, then the new UPDATE PDU shall contain the same Security Authority identification fields, and the security related information shall be modified according to the rules specified in the PIB. Any such modification may only reduce the protection level indicated, or add additional restrictions on access to the route.

7.13. DESTINATION SPECIFIC SECURITY

Delete this clause

7.14. Clause 7.16.2 Phase 2: Route Selection

Insert after third para ordered list:

When RIB-Att includes the priority attribute then all routes with the same NLRI shall be copied to the loc-RIB unless their computed preference is less than another such route with the same or lower priority.

When the RIB-Att includes the SECURITY attribute then all routes with the same NLRI shall be copied to the loc-RIB unless their computed preference is less than another such route which the applicable PIB Security Policy rules identify as providing equivalent or poorer protection and are usable by the same or more NPDUs.

7.15. Clause 7.16.3 Phase 3: Route Dissemination

Insert after para 4:

Routes with identical NLRI extracted from the same loc-RIB shall always be aggregated before being copied to an Adj-RIB-in, and may be aggregated with other routes according to the local Routing Policy.

7.16. Clause 7.18.2.3 Path Attribute Aggregation

Insert after third paragraph:

Routes that contain the LOCALLY SPECIFIED QOS attribute shall only be aggregated if their LOCALLY SPECIFIED QOS attributes have an identical NSAP Address Prefix field and an identical QoS Value field.

Routes that contain the SECURITY attribute shall only be aggregated if their SECURITY attributes identify the same Security Authority.

Replace paragraphs on **SOURCE SPECIFIC QOS** and **DESTINATION SPECIFIC QOS** with:

LOCALLY SPECIFIED QOS: The rules for determining the value of the metric field of each such LOCALLY SPECIFIED QOS attribute of the aggregated route are specific for each QoS Value and are specified by the responsible QoS Authority. They shall be held in the PIB. If no suitable rule exists in the PIB then the routes shall not be aggregated.

Replace paragraphs on **SOURCE SPECIFIC SECURITY** and **DESTINATION SPECIFIC SECURITY** with:

SECURITY: The rules for determining the value of the SECURITY attribute of the aggregated route are specified by the responsible Security Authority. They shall be held in the PIB. If no suitable rule exists in the PIB then the routes shall not be aggregated.

Replace paragraph on PRIORITY with:

PRIORITY: The value of the PRIORITY attribute of the aggregated route shall be equal to the maximum value of the values of the PRIORITY attributes of the routes being aggregated, unless the NLRI of component routes are identical when the value of the PRIORITY attribute of the aggregated route shall be the minimum value of the values of the PRIORITY attributes of the routes being aggregated.

7.17. Clause 7.19 Maintenance of the FIBs

In first para, replace last sentence following the colon with:

a) the NET of the next-hop BIS,

b) the local SNPA used by the local BIS to forward traffic to the next-hop BIS,

c) the minimum priority supported by this subnetwork hop, if the FIB's RIB-Att contains the PRIORITY attribute

d) security related information associated with this subnetwork hop, if the FIB's RIB-Att contains the SECURITY attribute

e) if available, the SNPA in the next-hop BIS to which NPDUs will be forwarded.

f) the QoS metric value if the FIB's RIB-Att contains the RESIDUAL ERROR, TRANSIT DELAY, EXPENSE, CAPACITY or LOCALLY DEFINED QOS attribute.

Append at end of clause:

d) **priority:** the minimum priority that an NPDU shall have for it to be forwarded over this subnetwork hop. If omitted, then the NPDU may have any priority.

e) **security related information:** identifies the protection available over the subnetwork hop and the NPDUs that may use it with reference to a known Security Policy.

f) **QoS Metric:** provides the value of the route's QoS metric for the corresponding QoS distinguishing path attribute, for use in additional matching rules during the NPDU forwarding process.

7.18. Clause 8.2 Determining the NPDU-Derived Distinguishing Attributes

Replace the second and third bullets with:

- The first two bits of the ISO 8473 security parameter are decoded. If they equal '01' then the responsible Security Authority is identified by the NPDU's source NSAP Address; if they equal '10' then the responsible Security Authority is identified by the NPDU's destination NSAP Address. The corresponding NPDU-Derived Distinguishing attribute is then a SECURITY attribute identifying the same Security Authority.

- The first two bits of the ISO 8473 QoS Maintenance parameter are decoded.

    i. If they equal '01' then the responsible QoS Authority is indicated by the source NSAP Address, and the NPDU-Derived Distinguishing attribute is determined using the remaining octets of the QoS Maintenance parameter and by applying the rules specified by the QoS Authority and contained in the PIB for selection of the NPDU-Derived Distinguishing attribute. If no such rules exist then no NPDU-Derived Distinguishing attribute shall be associated with this QoS Maintenance parameter.

    ii. If they equal '10' then the responsible QoS Authority is indicated by the destination NSAP Address, and the NPDU-Derived Distinguishing attribute is determined using the remaining octets of the QoS Maintenance parameter and by applying the rules specified by the QoS Authority and contained in the PIB for selection of the NPDU-Derived

Distinguishing attribute. If no such rules exist then no NPDU-Derived Distinguishing attribute shall be associated with this QoS Maintenance parameter.

iii. If they equal '11' then the NPDU-Derived Distinguishing attribute is as shown in table 4.

7.19. Clause 8.3 Matching RIB-Att to NPDU-Derived Distinguishing Attributes

Replace (c) with:

c) Each instance of a type-value specific attribute in the NPDU-Derived Distinguishing Attributes has a corresponding instance in an FIB's RIB-Att, and, depending on the type of the NPDU-Derived Distinguishing Attribute:

LOCALLY DEFINED QOS: The NSAP Address prefixes and QoS Values are identical.

SECURITY: The same Security Authority is identified in each case.

Replace last paragraph with:

Provided that such a RIB-Att can be found then the contents is inspected to find an entry such that:

a) the NLRI contains the NPDU's destination NSAP Address, or an NSAP Address prefix which is a prefix of the NPDU's destination NSAP Address;

b) the subnetwork hop's priority, if present, is less than or equal to the NPDU's priority

c) with reference to the applicable Security Policy rules contained in the PIB, the subnetwork hop provides sufficient protection for the NPDU, and the NPDU is permitted to use the subnetwork hop.

d) when a type specific NPDU-Derived Distinguishing Attribute has been selected by a rule specified by a QoS Authority from a source or destination specific QoS Maintenance parameter, then an additional matching rule may also be specified that determines whether the value of the QoS metric is acceptable.

If such a RIB-Att or entry cannot be found, then, in the order specified:

a) if the NPDU's security parameter does not express a requirement for protection, the SECURITY attribute may be removed from the NPDU-Derived Distinguishing attributes, and the above procedures repeated in order to find a match.

b) the PRIORITY attribute may be removed from the NPDU-Derived Distinguishing attributes, and the above procedures repeated in order to find a match.

c) Both the PRIORITY attribute and the SECURITY attribute, if the NPDU's security parameter does not express a requirement for protection, may be removed from the NPDU-Derived Distinguishing

```
attributes, and the above procedures repeated in order to find
a match.
```

7.20. Table 4

Delete entries for SOURCE SPECIFIC QOS and DESTINATION SPECIFIC QOS.