The ATM Forum

Technical Committee

Policy Routing
Version 1.0

af-cs-0195.000
April 2003

Acknowledgements

The Control and Signalling working group was chaired by Gert Öster. Thomas Cornély edited the specification. The minutes at related working group meetings were recorded by Dave Paw and Andrew Dolganow.

The following people made significant technical contributions to the Policy Routing Version 1.0 specification:

Kathrin Aldinger

Sirak Bahlbi

Thomas Cornély

Andrew Dolganow

Thierry Francoz

Shawn McAllister

Gert Öster

Dave Paw

Sébastien Prouvost

Carl Rajsic

Peter Roberts

Aditya Sehgal

Ethan Mickey Spiegel

This specification uses three levels for indicating the degree of compliance necessary for specific functions, procedures, or coding. They are indicated by the use of key words as follows:

- **Requirement:** "Shall" indicates a required function, procedure, or coding necessary for compliance. The word "shall" used in text indicates a conditional requirement when the operation described is dependent on whether or not an objective or option is chosen.
- **Objective:** "Should" indicates an objective which is not required for compliance, but which is considered desirable.
- **Option:** "May" indicates an optional operation without implying a desirability of one operation over another. That is, it identifies an operation that is allowed while still maintaining compliance.

Table of Contents

List of Figures

List of Tables

1 Introduction

The terms “policy routing” or “policy based routing” have already been used for a number of years in the networking community (see [RFC 1104], [RFC 1772], and more recently, the work of the Policy WG of the IETF). In each case, the objective is to control the way data, or connections, are routed through a routing domain. Policy Routing as specified in this document achieves the same goal, without policing the routing information sent or received by a node, i.e. without the configuration of policies to control or limit advertisement (or reception) of topology, resource or reachability related information by a node. Instead, Policy Routing introduces new information that is advertised throughout a routing domain and can be considered by nodes to affect how they route connections.

Policy Routing as specified in this document gives a network administrator control over the way connections are routed across a PNNI routing domain based on network specific criterias and resource utilisation strategies. For this purpose, this specification introduces the concept of Network Service Categories. Specifically, Policy Routing allows a network administrator to manage network entity resources on a per Network Service Category basis, in addition to the per ATM Service Category basis that is already available in PNNI.

This specification does not define the semantics associated with any Network Service Category or policy. These are considered to be specific to each ATM Service Provider network and are thus beyond the scope of this document. Instead, this specification focuses on the necessary extensions to the ATM control plane to support advanced services and policies.

1.1 Scope
[Normative]

This document is an optional addendum to UNI Signalling 4.1 [SIG 4.1], PNNI 1.1 [PNNI 1.1], and AINI 1.1 [AINI 1.1]. It contains the routing and signalling specification for the support of Policy Routing.

Policy Routing is an optional feature of UNI Signalling 4.1, PNNI 1.1, and AINI 1.1.

A device supporting Policy Routing shall implement these procedures for point-to-point calls/connections, and shall implement these procedures for point-to-multipoint calls/connections if point-to-multipoint calls/connections are supported. A device shall support Policy Routing procedures for all supported connection types (SVCCs, soft PVCCs, SVPCs, or soft PVPCs). A device capable of originating a soft PVCC or soft PVPC shall be capable of originating a soft PVCC or soft PVPC, respectively, with a policy constraint. Similarly, a UNI user side at the S_B or coincident S_B/T_B reference point that is capable of originating an SVCC or SVPC shall be capable of originating an SVCC or SVPC, respectively, with a policy constraint. Specific items that a device supporting Policy Routing shall implement are specified in Sections 7.1, 7.2, 8 and 9.

Policy Routing is supported at a PNNI between different administrative domains within the same PNNI routing domain, with the constraint that the semantics associated with advertised NSCs must be consistent throughout the entire PNNI routing domain.

Policy constraints may be mapped at AINI and UNI interfaces. The criteria used to decided when to map a received policy constraint are beyond the scope of this specification.

1.1.1 Support of Policy Routing by PNNI 1.0 Nodes

A device supporting PNNI 1.0 may implement the functionality defined in this addendum by treating this addendum as if it were an optional addendum to PNNI 1.0 [PNNI 1.0], and PNNI 1.0 Errata and PICS [PNNI Err]. No new PNNI 1.1 features are required by Policy Routing.

1.1.2 Support of Policy Routing by UNI Signalling 4.0 Nodes

A device supporting UNI Signalling 4.0 may implement the functionality defined in this addendum by treating this addendum as if it were an optional addendum to UNI Signalling 4.0 [SIG 4.0]. No new UNI Signalling 4.1 features are required by Policy Routing.

1.1.3 Support of Policy Routing by AINI Nodes

A device supporting AINI may implement the functionality defined in this addendum by treating this addendum as if it were an optional addendum to AINI [AINI]. Note that interworking procedures between AINI and B-ISUP related to Policy Routing are beyond the scope of this specification. No new AINI 1.1 features are required by Policy Routing.

1.2 Motivations for Policy Routing [Informative]

In the absence of Policy Routing, PNNI allows nodes in a PNNI routing domain to route connections while taking into account the state of the resources of the links and nodes within that domain. This is achieved by providing each node with a detailed map of the available resources for each ATM Service Category (ASC) supported by each network entity. PNNI allows an ATM network operator to partition the resources on network entities per ASC, apply different overbooking factors per ASC, or even allocate different amounts of resources to different ASCs. It is even possible to preclude connections of a given ASC to be routed on certain network entities by excluding available resources for that ASC from the network entity's advertisements. This set of features is a powerful and useful capability for service providers.

However, as ATM networks evolve to support a greater variety of services, service providers need to be able to manage the resources inside their ATM network at a finer level. They also need to be able to implement certain control policies defining how connections are routed through a PNNI routing domain. A simple example is the capability for an service provider to differentiate the resources that can be accessed by end-user generated SVCs and NMS generated SPVCs. Since one of the main attributes of an SPVC service is the resiliency offered through dynamic rerouting, it is important to make sure that in a network also offering SVC service, the resources that will allow successful rerouting of SPVCs in case of a failure are not consumed by SVCs.

In the absence of Policy Routing, the policies that can be implemented in a PNNI routing domain rely primarily on the ASC as the differentiating criteria. As the previous example shows, service providers need to be able to go beyond that. This document introduces the concept of ***Network Service Categories (NSC)***. In the example of the previous paragraph, one could identify two NSCs: the SVC network service category and the SPVC network service category. Each NSC has different applications and needs to be managed differently.

One could imagine many other NSCs, like the capability to provision resources for Voice VCs (whether CBR or rt-VBR), or the capability to identify links in the network that have different physical layer resiliency capabilities (and then use this to route Premium VCs on links offering physical layer protection, while Bronze VCs would rely on ATM layer rerouting capabilities only), etc. Another possible use of NSCs is the definition of a limited number of "Virtual Backbone Networks" (VBNs). In this application, resources could be associated with NSCs that map to VBNs, setting aside resources within the service provider network to be used by connections from members of a given user group.

Following are more detailed examples showing how the Policy Routing extensions could allow a service provider to implement the services and policies mentioned in the previous paragraphs.

1.2.1 Partitioning resources between SVCs and SPVCs

The SPVC service is typically characterized by:

- Always on, long lived connections.
- High resiliency and very short restoration times (these are usually negotiated in SLAs). This typically requires capacity management and definition of restoration policies.

The SVC service is typically characterized by:

- In most cases, the end users using SVCs do not expect resiliency.
- A short restoration time is not a specific requirement (the ability to re-establish a connection that was released by the network is certainly desirable but it is not a recognized feature of SVCs).
- Because SVCs are very dynamic by nature, capacity management is more challenging.

As SVCs and SPVCs are put together on the same network infrastructures, they have to share the same resources. From a service provider's perspective, it then becomes crucial to be able to set aside resources for each service.

A particular scenario that one would want to avoid is the case of SPVC reroutes triggered by a failure in the network being rejected because the resources they should have been rerouted on (according to capacity management) are consumed by user generated SVCs.

In order to maximize successful establishment of SPVCs, resources may be set aside within the network and dedicated to SPVCs. Additionally, a service provider may want to signal that if the dedicated SPVC resources on a specific network entity cannot accommodate the SPVC setup request, it is OK to fallback and establish the connection within another set of resources on that network entity (e.g. resources that are not specifically assigned to any service).

As a result, it is desirable to:

- Be able to advertise resource partitions within network entities (links, nodes) and advertise the fact that these resources are dedicated to a specific service. In this example, network entities would at least have one resource partition dedicated to SPVCs.
- Be able to associate with a connection setup request a policy constraint that says: "this connection is allowed to use and should primarily use resources dedicated to the SPVC service; however, if such resources are not available the connection may fallback to other sets of resources, or even use unassigned resources".

1.2.2 Force connections to be <u>exclusively</u> routed on specific network entities

As service providers are moving legacy services like traditional TDM voice and TDM Private (Leased) Line Services onto their ATM networks, there is a need to be able to provide levels of resiliency comparable to what these services are normally associated with.

To provide these very high resiliency services, a service provider will want to specifically route the associated connections on links that provide some kind of high resiliency capability (SONET/SDH APS for example). As a result, it is desirable to:

- Be able to advertise the fact that a network entity supports a specific service, or has a specific capability that makes it eligible to support specific services (i.e. supports a specific NSC).
- Be able to associate with a connection setup request a policy constraint that says: "this connection must be established over links that are tagged by this specific NSC, or the connection must fail".

1.2.3 Force connections to avoid specific network entities

A service provider may want to have certain connections carrying a specific type of service to avoid specific links (for example, avoid DS3 links, VP trunks that transit specific ASP networks, MPLS tunnels, etc.).

As a result, it is desirable to:

- Be able to advertise the fact that a network entity is tagged by a specific characteristic (i.e. tagged by a specific NSC).
- Be able to associate with a connection setup request a policy constraint that says: "this connection must be established over links that are NOT tagged by this specific NSC, or the connection must fail".

1.2.4 Support Virtual Backbone Networks

Similar to being able to partition resources between SVCs and SPVCs, a service provider may want to allocate resources within its network to specific users or user-groups, providing them with a "Virtual Backbone Network". In this application, the SVCs generated by end-users of a specific user-group would preferably be established in resources of the VBN associated with that user group.

For example, a Media Gateway providing TDM Voice to VoATM interworking can be viewed as a user, and VoATM Media Gateways could constitute a user group for which a VBN could be configured. The same could be said of Frame Relay to ATM interworking functions.

VBNs could also be deployed in an ASP interconnection scenario, allowing a transit ASP to only offer a fixed amount of resources to connections coming from another specific ASP. Grouping connections within a specific VBN would enable a service provider to have separate capacity planning and therefore commit to a higher probability of successful connection establishment for VBN customers.

Supporting a limited number of VBNs essentially requires the same set of capabilities described above in Section 1.2.1 and as a result would reuse the exact same control plane mechanisms. Note that the number of VBNs that may be supported by a given implementation is limited by the number of NSCs the implementation supports.

2 References

Only the specific versions of the following referenced documents and the specific versions of the documents referenced within these documents are applicable to this specification.

[SIG 4.0] af-sig-0061.000, ATM User-Network Interface (UNI) Signalling Specification version 4.0 – July 1996

[PNNI 1.0] af-pnni-0055.000, Private Network-Network Interface Specification Version 1.0 (PNNI 1.0) – March 1996

[PNNI Err] af-pnni-0081.000, PNNI v1.0 Errata and PICS – May 1997

[AINI] af-cs-0125.000, ATM Inter-Network Interface (AINI) Specification – July 1999

[PNNI 1.1] af-pnni-0055.002, Private Network-Network Interface Specification Version 1.1 (PNNI 1.1) – April 2002

[SIG 4.1] af-sig-0061.002, ATM User-Network Interface (UNI) Signalling Specification version 4.1 – April 2002

[AINI 1.1] af-cs-0125.002, ATM Inter-Network Interface Specification Version 1.1 (AINI 1.1) – September 2002

[RFC 1104] IETF RFC 1104, “Models of Policy Based Routing”, H-W Braun – June 1989

[RFC 1772] IETF RFC 1772, “Application of the Border Gateway Protocol in the Internet”, Y. Rekhter, P. Gross – March 1995.

3 Terminology

3.1 Acronyms

ABR	Available Bit Rate
ATM	Asynchronous Transfer Mode
AvCR	Available Cell Rate
ASC	ATM Service Category
ASP	ATM Service Provider
ATC	ATM Transfer Capability
AW	Administrative Weight
CAC	Connection Admission Control
CBR	Constant Bit Rate
CDV	Cell Delay Variation
CLEC	Competitive Local Exchange Carrier
CLP	Cell Loss Priority
CLR	Cell Loss Ratio
CLR_0	Cell Loss Ratio objective for CLP=0 traffic
CTD	Cell Transfer Delay
DTL	Designated Transit List
FCC	Federal Communications Commission
GCAC	Generic Connection Admission Control
GFR	Guaranteed Frame Rate
IETF	Internet Engineering Task Force
IG	Information Group
ILEC	Incumbent Local Exchange Carrier
IXC	Inter-exchange Carrier
LATA	Local Access Transport Area
LEC	Local Exchange Carrier
LGN	Logical Group Node
LSB	Least Significant Bit
MIB	Management Information Base
MSB	Most Significant Bit
NMS	Network Management System
NNI	Network-to-Network Interface
Ne-NSC	Network Entity NSC
NSC	Network Service Category
PG	Peer Group
PGL	Peer Group Leader
POP	Point Of Presence
PTSE	PNNI Topology State Element
PTSP	PNNI Topology State Packet
PNNI	Private Network-to-Network Interface
PVC	Permanent Virtual Connection
PVCC	Permanent Virtual Channel Connection
PVPC	Permanent Virtual Path Connection
QoS	Quality of Service
RAIG	Resource Availability Information Group
RCC	Routing Control Channel
Rp-NSC	Resource Partition NSC
SVC	Switched Virtual Connection
SVCC	Switched Virtual Channel Connection
TDM	Time Division Multiplex

TLV	Type, Length, Value
UBR	Unspecified Bit Rate
ULIA	Uplink Information Attribute
UNI	User to Network Interface
VBN	Virtual Backbone Network
VBR	Variable Bit Rate
VCC	Virtual Channel Connection
VCI	Virtual Channel Identifier
VoATM	Voice over ATM
VP	Virtual Path
VPC	Virtual Path Connection
VPI	Virtual Path Identifier

3.2 Definitions

Bare resources	Untagged resources, and resources of a tagged network entity that are not assigned to a specific resource partition.
Match a policy	Resources that match a policy are resources that can be considered for routing a connection after the policy has been used to prune the overall network topology map. For example, the resources that match a simple "require (single {Rp-NSC_1})" are all the resources in the network that are contained within resource partitions tagged by Rp-NSC_1. Similarly, the resources that match a simple "must avoid (single {Ne-NSC_1})" are all the bare resources in the network located on network entities which are not tagged by Ne-NSC_1.
Network entity	In the context of this specification, the term network entity is used to generically refer to a horizontal link, an uplink, a node, a spoke, a bypass or a set of reachable ATM addresses.
Network entity NSC (Ne-NSC)	An NSC that applies to the whole network entity (including all resources) and advertises properties of the network entity. Note that association of a Ne-NSC with a network entity does not prevent connections that do not request that Ne-NSC from using resources of that network entity (see the definition of bare resources).
Network Service Category (NSC)	A Network Service Category is a generic policy attribute that a service provider can use in addition to ATM Service Categories to indicate whether a network entity or a set of resources within the network entity is acceptable for carrying a given connection. When the generic acronym NSC is used, it stands for both Ne-NSCs and Rp-NSCs.
Policy	A policy is a set of requirements on network entities and resources (expressed via policy operators and lists of NSCs) that may be used to route a connection (see the definition of policy constraint). Note that when performing path selection using a policy, the topological map of the network is "pruned", leaving only the network entities and resources that match the policy. The resulting network topology map is then used during path selection.
Policy constraint	A policy constraint is an ordered list of one or more policies that must be considered during connection routing and connection establishment for a given connection.
Policy operator	A policy operator defines how a list of NSCs specified in a policy is used to "prune" a network topology map, allowing or forbidding access to network entities and resources during connection establishment. Accordingly, the supported policy operators are "*require* logical set of NSCs", or "*must avoid* logical set of NSCs".
Resource partition NSC (Rp-NSC)	An NSC that applies to a resource partition of a network entity. Note that association of a set of Rp-NSCs to a resource partition mandates that connections specify at least one of these Rp-NSCs as part of their associated policy in order to have access to resources of that partition. Those resources are then used to determine whether the resource partition is acceptable for carrying a given connection.

Tagged network entity	A network entity to which at least one Ne-NSC applies. Note that resources of a tagged network entity are considered to be tagged resources.
Tagged resources	Resources to which at least one NSC applies. Note that tagged resources are resources of a resource partition tagged by at least one Rp-NSC, or resources of a network entity tagged by at least one Ne-NSC.
Untagged network entity	A network entity that does not have any Ne-NSC associated with it. Note that an untagged network entity may contain resource partitions which in turn are tagged by one or more Rp-NSCs. As a result, an untagged network entity may contain tagged resources.
Untagged resources	Resources of an untagged network entity which are not contained in a tagged resource partition. These are resources to which no NSC can be considered to apply to. Note that by definition, resources advertised by PNNI nodes that do not support Policy Routing are untagged resources.

4 Policy Routing Overview

[Informative]

Policy Routing as specified in this document gives a network administrator control over the way connections are routed across a PNNI routing domain based on network specific criterias and resource utilisation strategies. To achieve this, Policy Routing relies on extensions to PNNI Routing and the ATM Forum signalling protocols (UNI, PNNI and AINI).

The extensions to PNNI Routing essentially allow:

- the advertisement of resource partitions within network entities, and
- the capability to tag entire network entities or only resource partitions with specific *Network Service Categories* (NSCs). Network Service Categories are sub-divided into *Network-entity NSCs* (Ne-NSCs) and *Resource-partition NSCs* (Rp-NSCs). These two terms are defined in Section 3.2.

The extensions to the signalling protocols enable a service provider or user to associate a policy constraint to a connection establishment request. The policy constraint results in the connection being routed on resources or network entities specifically tagged (or not tagged) by certain NSCs.

4.1 Advertising Network Service Categories

Resources of a network entity are advertised in PNNI Routing using RAIGs. Each RAIG advertised for a given network entity describes the resources for a given set of ASCs. Policy Routing adds an additional dimension to resource advertisement by allowing the resources advertised to be tagged by Ne-NSCs, Rp-NSCs, or both.

It is possible in PNNI to use a single RAIG to advertise resources that apply to more than one ATM Service Category. Similarly, it is possible to associate more than one NSC to a resource advertisement. For example, a link may be tagged by 2 Ne-NSCs, Ne-NSC_1 and Ne-NSC_2 (which could stand for “Physical Layer Resiliency” and “Facility Provided by XYZ”).

4.1.1 Advertising Ne-NSCs

Support of one or more Ne-NSCs by a network entity is indicated by adding the list of applicable Ne-NSCs to the resource advertisement for that network entity. This is depicted below:

Network Entity Advertisement: (without Policy Routing)	Network Entity Advertisement: (with Policy Routing)
➢ CBR resources ➢ VBR-rt resources ➢ VBR-nrt resources ➢ ABR resources ➢ UBR resources ➢ GFR resources	➢ CBR resources ➢ VBR-rt resources ➢ VBR-nrt resources ➢ ABR resources ➢ UBR resources ➢ GFR resources ➢ **List of applicable Ne-NSCs**

Figure 4-1: Advertising Ne-NSCs

4.1.2 Advertising Resource Partitions and Rp-NSCs

Policy Routing introduces the capability to define resource partitions within network entities and tag these resource partitions with one or more Rp-NSCs. Resources within a resource partition are advertised using RAIGs. The same set of rules that govern how RAIGs are used to advertise resources within a network entity in PNNI (i.e. bare resources) apply to RAIGs within a resource partition.

In the context of Policy Routing, at least one Rp-NSC is always associated with a resource partition.

In the absence of Policy Routing, PNNI allows the same physical resources to be shared (fully or partially) between multiple sets of ASCs. When this is done, these physical resources are accounted for in multiple RAIGs potentially using different overbooking factors per set of ASCs.

The same capability is expected to be supported when advertising resources of different resource partitions of a given network entity. For example, a link that has 50 Mb/s of physical cell rate could be configured with 2 resource partitions, one for SPVCs, one for SVCs, and no bare resources. Out of the total link resources, a minimum of 30 Mb/s would be reserved for SPVCs. This would result in the SPVC resource partition advertising a total of 50 Mb/s and the SVC resource partition advertising only 20 Mb/s (See Figure 4-2).

In addition, it should be possible to set the resource partition supporting SPVCs so that specific overbooking factors would apply to SPVCs, while the resource partition supporting SVCs would be configured with completely different (e.g. smaller) overbooking factors that would apply to SVCs.

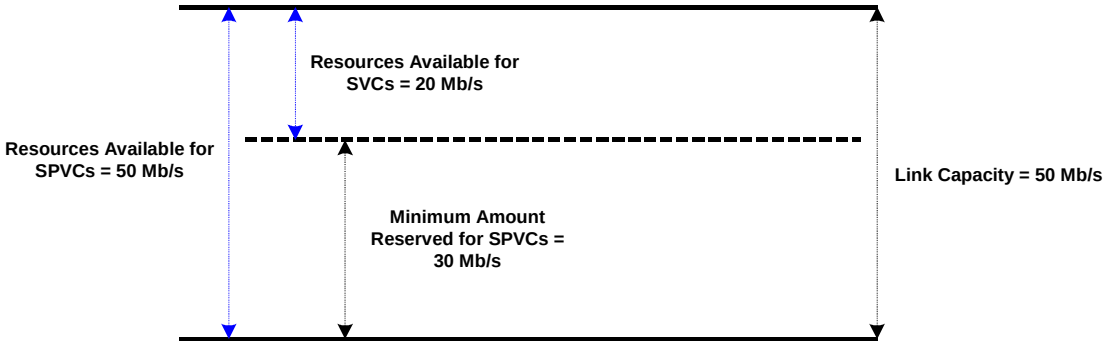


Figure 4-2: Example of Resource Partitions Sharing Physical Resources

Support of one or more resource partitions, each tagged by a set of Rp-NSCs, is indicated by introducing a hierarchy in the way resources are advertised in PNNI Routing. This is depicted below:

Network Entity Advertisement: (without Policy Routing)	Network Entity Advertisement: (with Policy Routing)
➢ CBR resources ➢ VBR-rt resources ➢ VBR-nrt resources ➢ ABR resources ➢ UBR resources ➢ GFR resources	➢ CBR resources ➢ VBR-rt resources ➢ VBR-nrt resources ➢ ABR resources ➢ UBR resources ➢ GFR resources ➢ **Resource partition 1** **List of applicable Rp-NSCs** ➢ CBR resources ➢ VBR-rt resources ➢ VBR-nrt resources ➢ ABR resources ➢ GFR resources ➢ **Resource partition 2** **List of applicable Rp-NSCs** ➢ CBR resources ➢ ABR resources ➢ GFR resources

Figure 4-3: Advertising resource partitions and Rp-NSCs

4.1.3 Advertising Ne-NSCs and Rp-NSCs within a Network Entity

A network entity may be tagged by a set of Ne-NSCs and at the same time contain a certain number of resource partitions, each tagged by a number of Rp-NSCs. Resources of such a network entity would be advertised as depicted in the figure below:

Network Entity Advertisement:

- CBR resources
- VBR-rt resources
- VBR-nrt resources
- ABR resources
- UBR resources
- GFR resources
- **List of applicable Ne-NSCs**
- **Resource partition 1**
  List of applicable Rp-NSCs
  - CBR resources
  - VBR-rt resources
  - VBR-nrt resources
  - ABR resources
  - GFR resources
- **Resource partition 2**
  List of applicable Rp-NSCs
  - CBR resources
  - ABR resources
  - GFR resources

Figure 4-4: Advertising Ne-NSCs and Rp-NSCs on a given network entity

4.1.4 Tagging all the resources of a network entity

With the resource advertising scheme defined in this specification, it is also possible to tag all the resources of a network entity, essentially dedicating it in its entirety to a specific set of network services. To achieve this, all the resources of the network entity are advertised within one or more resource partitions, tagged by the applicable Rp-NSCs.

Network Entity Advertisement:

- **List of applicable Ne-NSCs**
- **Resource partition 1**
  List of applicable Rp-NSCs
  - CBR resources
  - VBR-rt resources
  - VBR-nrt resources
  - ABR resources
  - GFR resources

Figure 4-5: Tagging all the resources of a network entity with Rp-NSCs

4.1.5 Examples of Tagged Resources, Untagged Resources and Bare Resources

These terms are defined in Section 3.2. Following are figures illustrating these definitions.

Network Entity Advertisement:	**Identification of the type of resources**
➢ CBR resources ➢ VBR-rt resources ➢ VBR-nrt resources ➢ ABR resources ➢ UBR resources ➢ GFR resources ➢ **List of applicable Ne-NSCs**	**Bare resources of a Tagged network entity**

Figure 4-6: Tagged Network entity and Bare Resources

Network Entity Advertisement:	**Identification of the type of resources**
➢ CBR resources ➢ VBR-rt resources ➢ VBR-nrt resources ➢ ABR resources ➢ UBR resources ➢ GFR resources	**Untagged resources (also, Bare resources)**
➢ **Resource partition 1** **List of applicable Rp-NSCs** ➢ CBR resources ➢ VBR-rt resources ➢ VBR-nrt resources ➢ ABR resources ➢ GFR resources	**Tagged resources**
➢ **Resource partition 2** **List of applicable Rp-NSCs** ➢ CBR resources ➢ ABR resources ➢ GFR resources	**Tagged resources**

Figure 4-7: Untagged Resources and Tagged Resources

Network Entity Advertisement:	**Identification of the type of resources**
➢ CBR resources ➢ VBR-rt resources ➢ VBR-nrt resources ➢ ABR resources ➢ UBR resources ➢ GFR resources ➢ **List of applicable Ne-NSCs**	**Bare resources of a Tagged network entity**
➢ **Resource partition 1** **List of applicable Rp-NSCs** ➢ CBR resources ➢ VBR-rt resources ➢ VBR-nrt resources ➢ ABR resources ➢ GFR resources	**Tagged resources**
➢ **Resource partition 2** **List of applicable Rp-NSCs** ➢ CBR resources ➢ ABR resources ➢ GFR resources	**Tagged resources**

Figure 4-8: Bare Resources and Tagged Resources

4.1.6 Simplifying Management of Rp-NSCs on Certain Interfaces

Policy Routing allows potentially very detailed resource management in a PNNI routing domain. Being able to define resource partitions and assign specific sets of Rp-NSCs to them on links where resources are scarce is very valuable. Still, configuring resource partitions on links, sizing them properly and assigning the right set of Rp-NSCs will very likely be a tedious process that service providers should only have to do when it is worthwhile.

There are at least two cases where having to go through this process may not be worthwhile:

1. At a network UNI. The sheer number of UNIs on a network will typically make managing Rp-NSCs on them difficult. Policy Routing being first and foremost a tool to manage how connections are routed within a network, in most cases, managing NSCs at the edges will not be worth doing.
2. In places in a network where bandwidth is not scarce (e.g. very high speed core links). While setting Ne-NSCs on high speed core links is just as valid as setting them on low speed links, setting resource partitions and Rp-NSCs on high speed core links may be unnecessary.

A resource advertisement in PNNI Routing that does not contain a Resource Partition IG (and does not contain a Ne-NSC Identifiers IG) is considered to be only advertising bare (or untagged) resources. Only connections that have a policy constraint that allows access to bare (or untagged) resources will be able to route over the interfaces associated with that advertisement. As a result, not advertising any NSCs for either of the two cases above is not acceptable since many connections may have policy constraints that do not allow access to bare (or untagged) resources.

To efficiently address the two cases identified above, Policy Routing provides the following:

- Resources associated with a reachable ATM addresses advertisement that does not contain a Ne-NSC Identifiers IG or any Resource Partition IG are always considered during path computation (i.e. they are never pruned because of a policy). Note that if a reachable ATM addresses advertisement contains either a Ne-NSC Identifiers IG or a Resource Partition IG, then the path selection rules defined in Section 6 apply.
- It is possible to efficiently advertise the fact that resources associated with an advertisement are to be considered as tagged by all Rp-NSCs by using a single flag within the information group flags (as defined in table 5-34 of [PNNI 1.1]). Note that when this flag is set, all the resources associated with the advertisement are both considered as bare resources (since they are not contained in a Resource Partition IG) and as being tagged by all Rp-NSCs (since the flag is set).

4.1.7 Recommendation on Setting Ne-NSCs and Resource Partitions on Links

The PNNI Routing extensions that allow advertising of Ne-NSC identifiers, Resource Partitions and Rp-NSC identifiers apply to a given direction of a link. From a protocol perspective, it is possible to advertise a different set of Ne-NSCs, or a different set of Rp-NSCs for each direction of the same link. Nonetheless, it is strongly recommended that service providers:

- Configure both directions of a given link with the exact same set of Ne-NSCs. This simply makes sense when considering that a Ne-NSC reflects a characteristic of the "network entity" itself. When the network entity is a link, it seems reasonable to assume that a given Ne-NSC applies equally to both directions on that link.
- Configure both directions of a given link so that overall, if a given ASC is supported for a specific Rp-NSC in one direction, that same ASC is also supported for that same Rp-NSC in the other direction. Note that this does not mean that both directions of the link necessarily have to be configured with identical Resource Partitions, tagged by the exact same set of Rp-NSCs, nor does it mean that the amount of resources set aside for a given ASC / Rp-NSC combination be identical in both directions of a link. As an example, although not recommended, one could have:
  - In one direction:
    - resource partition 1 (tagged by Rp-NSC_1, Rp-NSC_2, supporting CBR and UBR), and
    - resource partition 2 (tagged by Rp-NSC_2, Rp-NSC_3, supporting rt-VBR and ABR)
  - In the other direction:
    - resource partition 1 (tagged by Rp-NSC_2, supporting CBR, rt-VBR, UBR and ABR),
    - resource partition 2 (tagged by Rp-NSC_1, supporting CBR and UBR), and
    - resource partition 3 (tagged by Rp-NSC_3, supporting rt-VBR and ABR).

Similarly, as recommended in Sections 4.3, 7.2.5, 8.4 and 9.4, if a given direction of a link is not tagged with any NSCs (possibly because the node at the preceding side does not support Policy Routing), then the other direction should not be tagged with any NSCs either.

4.1.8 Well-Known Ne-NSCs and Rp-NSCs

Ne-NSC identifier values within the range 65000 through 65535, inclusive, are well known Ne-NSCs. Rp-NSC identifier values within the range 65000 through 65535, inclusive, are well known Rp-NSCs.

The semantics of well-known Ne-NSCs and Rp-NSCs are defined by the ATM Forum in the "ATM Forum Well-known Addresses and Assigned Codes" document which is available on the ATM Forum's web site. From a Policy Routing implementation's perspective, well-known Ne-NSCs and Rp-NSCs are handled the same as any other Ne-NSC or Rp-NSC.

4.2 Signalling Policy Constraints

4.2.1 Policy Routing and Services Definition

This specification focuses on the necessary extensions to the ATM control plane to support advanced services and policies and does not address the specific definition of these services. There may be many aspects to a service. The ability to affect how a connection is routed using a policy constraint signalled in the connection establishment request is one of the tools that a service provider may use to implement a service.

For example, to offer a "high resiliency service", a service provider could use the following two capabilities:

- SONET/SDH APS links in the PNNI routing domain
- Policy Routing to :
    1. tag links protected using SONET/SDH APS throughout the PNNI routing domain with Ne-NSC_1,
    2. associate a policy constraint with the policy "require (Ne-NSC_1)" to connection establishment request from end-users subscribed to that service.

4.2.2 What are Policy Constraints ?

A policy constraint comprises the complete set of policy information associated with a given connection in order to provide service specific "directions" for connection routing. A policy constraint consists of a single policy or a list of policies stated in order of preference. Each policy consists of a set of rules that allow access, or restrict access, to tagged resources. These rules are expressed using one or two *policy operators* (one for "require" and one for "must avoid"), each applying to one *list of NSCs* (containing a list of Ne-NSCs and/or a list of Rp-NSCs). All the rules contained in at least one of the policies listed in a policy constraint must be met during connection routing for the connection to be progressed.

When performing path selection using a policy, the topological map of the PNNI routing domain is "pruned", leaving only the network entities and resources that match the policy. Without Policy Routing, the applicable GCAC algorithm (as defined in Sections 5.13.4 and 5.13.5 of [PNNI 1.1]) for a connection is performed on a set of resources equal to the resources of the entire routing domain. With Policy Routing, GCAC for a given connection is performed on a subset of resources that match one policy in the policy constraint associated with the connection.

4.2.2.1 Syntax Used to Specify Policy Constraints

In the rest of this document, the following syntax is used to express policy constraints:

Policy constraint ::= { **Policy 1**
Ordered-OR **Policy 2**
Ordered-OR **Policy 3**
… },

Where:

- The number of policies in a policy constraint is between 1 and 6.
- When more than one policy is specified, they are always considered as comprising an "ordered or" list, where the policy at the top of the list is the most desired.
- A policy is specified as:

Policy ::= " Policy operator (**List of NSCs**) *Logical AND* Policy operator (**List of NSCs**) ",

Where:

- The number of policy operators in a single policy is either 1 or 2
- A policy operator is one of "Require" or "Must Avoid".
- A policy operator of a given type appears at most once in a single Policy.
- List of NSCs is specified as:

List of NSCs ::= (list operator {**list of Ne-NSCs**} *Logical AND* list operator {**list of Rp-NSCs**}),

Where:

- List operator is either "logical AND", "logical OR, or "Single" when only one NSC is in the list.
- A List of NSCs may contain a list of Ne-NSCs, a list of Rp-NSCs, or both.

Finally, to simplify writing policies using this syntax, all the fixed logical operators (highlighted in italics above) are denoted using a simple semi-colon ";" in the rest of this document. The meaning of a semi-colon is easily deduced from its position within a policy constraint statement.

4.2.2.2 Example of the Syntax Used to Define a Policy Constraint

A policy constraint that contains three policies:

- the most desired policy being a require that applies to a list of Rp-NSCs with a logical OR list operator and a list of Ne-NSCs with a logical AND list operator,
- the second choice policy being a require on a single Ne-NSC combined with a must avoid on another single Ne-NSC,
- the least desired policy being a must avoid on a single Ne-NSC.

Would be expressed as follows using the syntax defined above:

Policy constraint ::= {

"require (logical AND {Ne-NSC_1, Ne-NSC_5}; logical OR {Rp-NSC_1, Rp-NSC_2})"

"require (single {Ne-NSC_4}); must avoid (single {Ne-NSC_3})"

"must avoid (single {Ne-NSC_3})"

}

4.2.3 How is a Connection with no Policy Constraint Routed ?

Before going over how connections that have policy constraints associated with them are routed across a PNNI routing domain, it is necessary to understand how a connection with no policy constraint is routed and what are the resources it is allowed to use. Note that a connection originated from a user or a node that does not support Policy Routing would fall in that category.

A connection with no policy constraint associated with it is routed in bare resources (as defined in Section 3.2). If no path through bare resources exists, then the connection establishment fails. Note that resources of a network entity tagged with Ne-NSCs that are not contained in a resource partition are bare resources.

4.2.4 Policies used in Policy Routing

4.2.4.1 Policy Operators: *require* and *must avoid*

This specification defines the following policy operators:

- *Require*, which can apply to both Ne-NSCs and Rp-NSCs.
  The policy "require (single {Rp-NSC_1})" means that a connection must be routed only in resources that are tagged by Rp-NSC_1. A connection with the policy "require (single {Ne-NSC_3})" on the other hand must only be routed on bare resources of network entities that are tagged by Ne-NSC_3. If a service requires a connection to be routed in a specific resource partition (tagged by Rp-NSC_1) of specific network entities (those tagged by Ne-NSC_3), then the policy "require (single {Ne-NSC_3}; single {Rp-NSC_1})" could be used.
- *Must avoid*, which can only apply to Ne-NSCs.
  The policy "must avoid (single {Ne-NSC_3})" means that a connection must be routed in bare resources of network entities which are not tagged by Ne-NSC_3.

4.2.4.2 Policy Operators on List of NSCs

When a list of NSCs is specified in a policy, it is necessary to specify how that list shall be interpreted by nodes along the path of the connection. For the "require" policy operator, the list of NSCs may contain one list of Rp-NSCs, one list of Ne-NSCs, or both. When the list of NSCs contains both, each list is interpreted independently from the other.

Currently, there are two possible interpretations of a list of Rp-NSCs (or Ne-NSCs):

- logical AND,
- logical OR.

The precise interpretation of a list of Rp-NSCs (or Ne-NSCs) varies with the policy operator with which the list is associated:

- For the "require" policy operator:
  - A policy of "require (logical OR {list of Ne-NSCs})" means that the connection can be routed in bare resources of network entities that are tagged by any one or any combination of the listed Ne-NSCs.
  - Similarly, a policy of "require (logical OR {list of Rp-NSCs})" means that the connection must be routed in resource partitions that are tagged by any one or any combination of the listed Rp-NSCs. Note that at each traversed network entity, the resources used by a connection must come from a single resource partition (possibly affecting other resource partitions sharing the same physical resources). The logical OR is essentially a way of giving more chances for a connection to be successfully established, by giving that connection access to a bigger selection of resources. As part of a list of Rp-NSCs interpreted as a "logical OR", it is possible to indicate that bare resources should also be considered when routing and establishing the connection. This is achieved by using a special codepoint in the list, referred to as Rp-NSC_Bare in the rest of this document.
  - A policy of "require (logical AND {list of Ne-NSCs})" means that the connection must be routed in bare resources of network entities that are tagged by all the listed Ne-NSCs at the same time.

- Similarly, a policy of "require (logical AND {list of Rp-NSCs})" means that the connection must be routed in resource partitions that are tagged by all the listed Rp-NSCs at the same time. For Rp-NSCs, the option of using logical AND must be balanced against defining a new Rp-NSC that corresponds to the combination of all listed Rp-NSCs (e.g. instead of using logical AND {Rp-NSC_1, Rp-NSC_2}, one could define a Rp-NSC_3 that would tag the resources that are tagged by both Rp-NSC_1 and Rp-NSC_2). In hierarchical PNNI routing domains, defining Rp-NSCs that correspond to combinations of other Rp-NSCs is preferable to using logical AND.

- For the "must avoid" policy operator:
  - A policy of "must avoid (logical OR {list of Ne-NSCs})" means that the connection must be routed in bare resources of network entities that are not tagged by any one or any combination of the listed Ne-NSCs.
  - A policy of "must avoid (logical AND {list of Ne-NSCs})" means that the connection must be routed in bare resources of network entities that are not tagged by all the listed Ne-NSCs at the same time. Note that the connection may be routed on network entities that are tagged by a proper subset of the listed Ne-NSCs.

A policy may contain a "require" policy operator with both a list of Rp-NSCs and a list of Ne-NSCs. When such a policy is used to progress a connection, the connection is routed considering both lists, as defined above, simultaneously. As a result, if Ne-NSC_1 is "OC-3", Ne-NSC_2 is "APS 1+1" and Rp-NSC_1 is "Voice", a policy that specifies a connection to be established over OC-3 with APS 1+1 links, and is allowed access to resources reserved for Voice, would have the following definition:

"require (logical AND {Ne-NSC_1, Ne-NSC_2}; single {Rp-NSC_1})"

Note that how a node chooses which resource partition to use when establishing a connection when more than one resource partition matches the policy used for that connection, is implementation specific.

4.2.4.3 Combining Two Policy Operators Within a Single Policy

Policy Routing also allows a service provider to use two policy operators at the same time (one "require" and one "must avoid") to create a given policy.

When using such a policy, the connections are routed in resources that match both the "require" policy operator and the "must avoid" policy operator.

4.2.5 Policy Constraints Containing Multiple Policies

Specifying multiple policies in a single policy constraint allows a service provider to preferentially perform path selection and allocate resources during connection establishment using a specified set of policies.

Connections containing a policy constraint with an ordered list of policies are routed by first "pruning" the topological map of the PNNI routing domain, leaving only the network entities and resources that match the first policy in the list (i.e. the preferred policy). If possible, the connection is routed using the available resources that match the first policy. If that routing attempt fails (to be distinguished from the actual connection setup attempt failure), the second (i.e. next in order of preference) policy in the list is used to "prune" the original topological map of the PNNI routing domain. If possible, the connection is routed using the available resources that match the second policy. If that routing attempt fails, then the third policy is attempted and so on. This ordered selection of policies from a policy constraint is continued recursively, until either the connection is successfully routed, or there are no network resources available that match any of the policies defined in the policy constraint.

4.2.6 Addition, Replacement, Discard of Policy Constraints

Policy Routing allows each side of a UNI, or AINI interface to:

- Add a policy constraint to a SETUP or ADD PARTY message that was received without one.
- Replace a policy constraint received in a SETUP or ADD PARTY message with another one. Note that the specific criteria used to decide whether a policy constraint needs to be replaced or not are outside the scope of this specification.
- Discard a policy constraint received in a SETUP or ADD PARTY message and forward that message without one.

A PNNI interface cannot add a policy constraint to a SETUP or ADD PARTY message that does not contain one. Similarly, a PNNI interface cannot modify or discard a received valid policy constraint.

4.2.7 NSC Report List Capability

In addition to the ability to associate policy constraints to connections, the signalling extensions allow a calling end user to request a policy related report. A report consists of a list of Ne-NSC identifiers, or a list of Rp-NSCs identifiers, or both, returned in the CONNECT or ADD PARTY ACKNOWLEDGE message of the connection or party, respectively, for which a report was requested.

4.2.7.1 Types of Reports and Example Applications

There are different types of reports that can be requested during connection or party establishment:

1. Reports containing all the Rp-NSC identifiers that both tag the resource partitions in which the connection was established, and were part of “require” policies used to progress it.
2. Reports containing all the Ne-NSC identifiers that both tag the network entities over which the connection was established, and were part of “require” policies used to progress it.
3. Reports containing all the Ne-NSC identifiers that tag network entities over which the connection was established.
4. Some combinations of the above.

One application that could utilize the NSC Report List capability is “diverse routing”. Each link in the network could be tagged with a unique Ne-NSC in a “network wide” predefined range of “link Ne-NSCs”. A report of the third type can then be used to collect all Ne-NSC identifiers tagging links supporting a connection. A subsequent connection establishment could then be made with a policy constraint of “must avoid” and the list of the “link Ne-NSCs” reported by the first connection establishment, guaranteeing that the second connection would not be established on links that were used by the first one.

Another application of the NSC Report List capability is one combining a report request with a policy constraint that either contains multiple policies, or contains a policy with a policy operator on a list of NSCs. With such a policy constraint, a connection may be established in resources that are tagged by different NSCs in different parts of the PNNI routing domain.

In such a scenario, the NSC Report List capability can be used to provide a basic indication to the calling user or PNNI routing domain point of entry of the type of resources in which the connection was established. The CONNECT message returned to the calling user for a connection that was established using policies containing a “require” policy operator could contain the list of the Rp-NSCs as well as the list of the Ne-NSCs that were both listed in the policies used to establish the connection and tag any of the resources in which the connection was established. This report provides the calling user a “high level” indication of the type of resources on which the connection sits within the PNNI routing domain.

One application of such a report is the case of a connection with the following policy constraint:

{
"require (single {Rp-NSC_1})"
"require (logical OR {Rp-NSC_1, Rp-NSC_2})"
}

where the resources tagged by Rp-NSC_2 are less desirable, and provided more as "back-up" than anything else. Typically, the service provider has engineered its network so that the connection will be established in resources tagged by Rp-NSC_1, and includes Rp-NSC_2 within the second policy to allow the connection to stay up (potentially while being sub-optimally routed) in case of failures in the network.

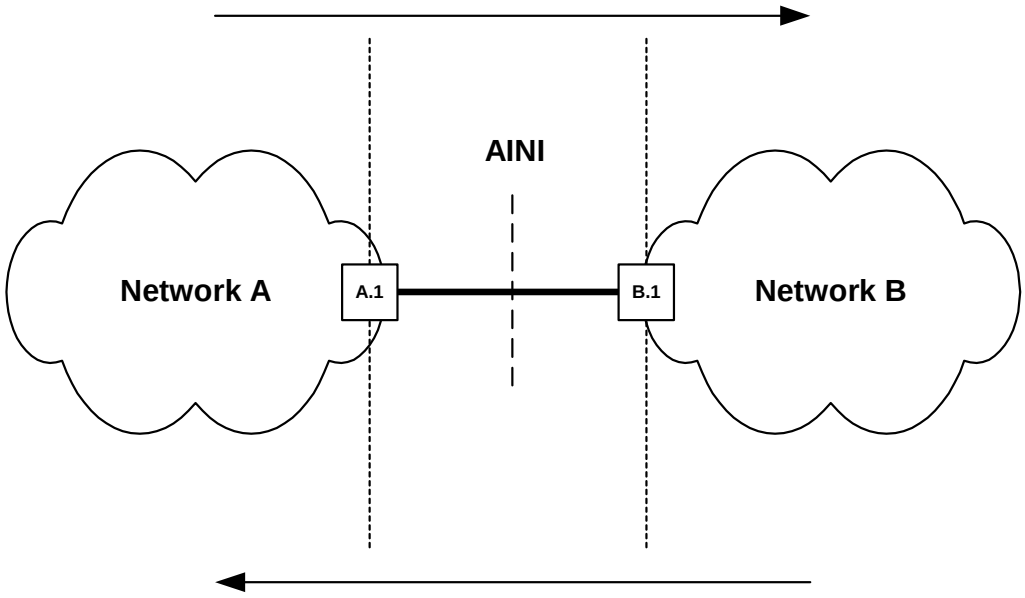
In such a scenario, a service provider could use a report returned in the CONNECT message to confirm that the connection was routed as it should (i.e. only through resources tagged by Rp-NSC_1), or not. The presence of Rp-NSC_2 in the report could be used as an indication that the connection was established using less desirable resources and may need to be moved at a later point in time.

4.2.7.2 Scope of a Report

For a point to point connection within a PNNI routing domain, a received report contains information on at least the portion of the connection's path that is contained within that PNNI routing domain.

At an interface where the policy constraint contained in the connection's SETUP message was either added, replaced, or discarded, a received report is typically "reset". This is a consequence of the fact that the meaning of NSCs is network specific, and that Ne-NSC_1 may be associated with completely different services in different networks. As a result, a node or end-user can only receive a report listing NSCs that make sense to that node or end-user. An example scenario where a report is "reset" at an AINI is depicted in Figure 4-9.

In the SETUP message, node A.1 replaces the policy constraint received from Network A (PCA) with another one (PCB), associated with the service desired from Network B. Both policy constraints contained a report request.



The CONNECT message received by node A.1 contains a report that was based on PCB, and applies to the resources within Network B. Node A.1 removes that report from the CONNECT message and starts a brand new one, based on PCA.

Figure 4-9: Example of a Report being "Reset" at an AINI

For a point to multipoint connection, the report returned in an ADD PARTY ACKNOWLEDGE message only gives an indication of the NSCs that tag the resources used to forward the connection from the branching point (where the ADD PARTY message was converted to a SETUP message) to the called party. It does not provide any indication of the NSCs tagging the resources supporting the connection between the root and the branching point.

4.3 Backwards Compatibility with Nodes not supporting Policy Routing

Since all resources of nodes that do not support Policy Routing are considered as untagged resources, connections with a policy constraint may be established over PNNI and AINI interfaces which do not support this feature if the policy constraint allows the connection to be routed on untagged resources.

Whether a Policy constraint information element should be passed along by nodes that do not support Policy Routing will vary with the signalled policy constraint. Typically, a Policy constraint information element allowing routing on untagged resources should be passed along by nodes not supporting Policy Routing. Similarly, connections that are not allowed to be routed on untagged resources should be released by nodes not supporting Policy Routing. As a result, the setting of the IE instruction field of the Policy constraint information element in a SETUP or ADD PARTY message will vary and should be set by the node or end-user originating the connection on a connection by connection basis. In a CONNECT or ADD PARTY ACKNOWLEDGE message however, the Policy constraint information element should always be passed along.

Requesting that a Policy constraint information element be passed on by nodes that do not support Policy Routing may result in connections being misrouted in hierarchical PNNI routing domains where border nodes do not support Policy Routing. One example could be the routing of a connection with the policy "must avoid (single {Ne-NSC_1})". If that connection is received by an entry border node that does not support Policy Routing, that entry border node will compute a path through the peer group ignoring the policy constraint, potentially routing the connection on intermediate links that are tagged by Ne-NSC_1. In such a scenario, a node at the preceding side of a link tagged by Ne-NSC_1 would then crankback the connection, causing the border node to "try again". Based on this observation, it is recommended that upgrade of a peer group to support Policy Routing is done starting with the border nodes.

Policy Routing provides a mechanism to identify within a PNNI routing domain nodes that do support Policy Routing from nodes that do not. A node that supports Policy Routing will include in its Nodal IG a Policy Version IG that advertises the policy version it supports. Consequently, a node that does not advertise a Policy Version IG is considered to not support Policy Routing.

When a connection is routed through bare resources, it is important that the report returned in the CONNECT message contains an indication that the connection was established through what may be less desirable resources. The report is updated by each node as the CONNECT message is progressed through the network. When a connection is routed through a node that does not support Policy Routing, that node will simply forward the received report unchanged (assuming the pass along request bit of the Policy constraint information element is set as recommended above). So there is a risk that a connection is established through bare resources without the report returned in the CONNECT message reflecting it.

To protect a PNNI routing domain from such a scenario, it is strongly recommended that service providers apply the following rule when configuring their network for Policy Routing: if a node A that supports Policy Routing is connected to a node B that does not support Policy Routing, all the resources of the connecting links in the direction from node A to node B should be left untagged. This is the same as saying that if a link has one end on a node that does not support Policy Routing, then the resources in both directions of that link should be left untagged.

With this rule in place, the only way a connection with a policy constraint can reach a node that does not support Policy Routing is if a node that does support Policy Routing established that connection in untagged resources. This will automatically result in the report list returned in the CONNECT message containing an indication that bare resources were used.

4.4 Modeling Considerations for the Signalling Procedures

The signalling procedures of Sections 7.2.3, 7.2.4, 8.2, 8.3, 9.2 and 9.3 use the basic model described in Section 6.1 of [PNNI 1.1]. In addition, in order to relate path, link and resource selection with the processing of a connection setup message, it is assumed that:

- the succeeding side of an interface is responsible for selecting the resource partition and the resources allocated to a connection in the backward direction on that interface. The corresponding procedures are specified as part of the succeeding side procedures, using the policy constraint in the "indication" primitive sent to the Call Control entity.
- Although Call Control can be considered to be the entity responsible for selecting the path (if applicable) and the link to be used as the next interface; in this specification, the corresponding procedures are described as part of the succeeding side procedures, using the policy constraint in the "indication" primitive sent by the succeeding side.
- the preceding side of an interface is responsible for selecting the resource partition and the resources allocated to a connection in the forward direction on that interface. The corresponding procedures are specified as part of the preceding side procedures, using the policy constraint in the "request" primitive sent by the Call Control entity.

Note that from the Call Control entity's perspective, the policy constraint in the "request" primitive is always identical to the one in the "indication" primitive. Adding, replacing, and discarding policy constraints always occurs either at the succeeding side or the preceding side, not in Call Control.

This is depicted in Figure 4-10 below:

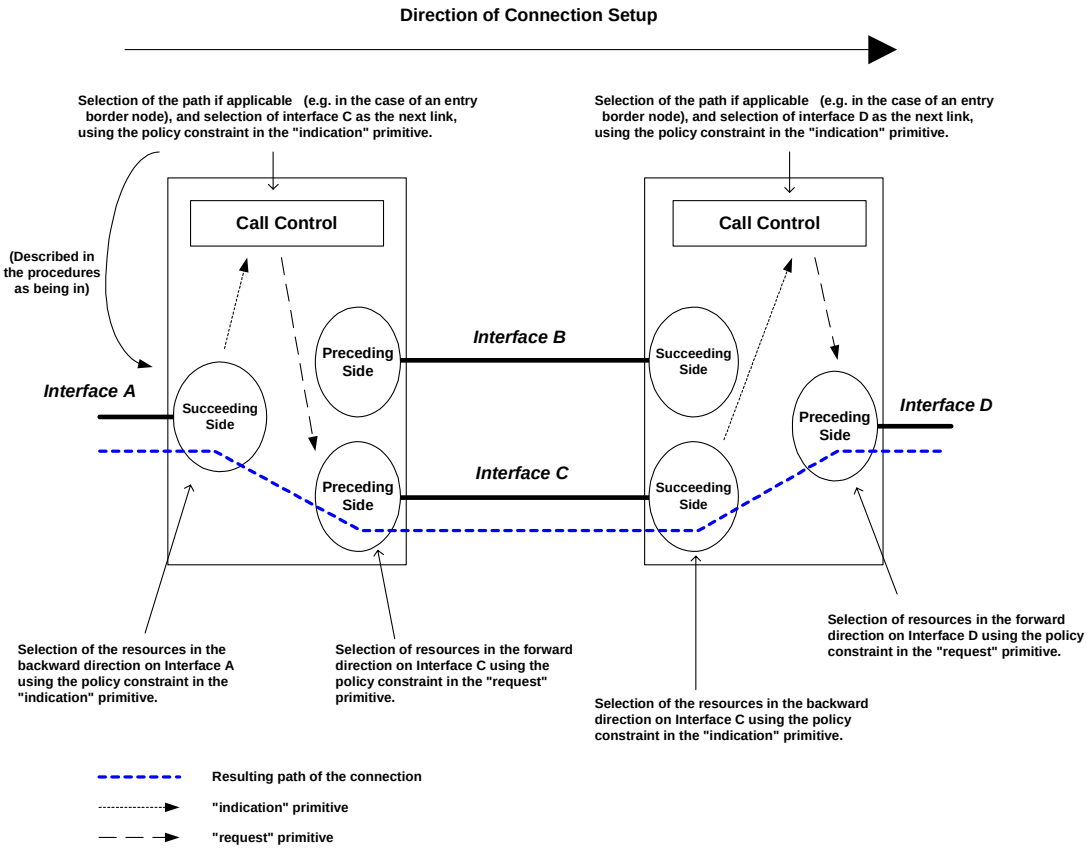


Figure 4-10: Modeling Assumptions Related to Path, Link and Resource Selection

These modeling assumptions do not restrict where specific tasks are performed within an implementation, as long as its external behavior matches this model.

5 Information Element Coding for Policy Routing

[Normative]

5.1 Policy Constraint Information Element

The purpose of the Policy constraint information element is to carry any policy routing related information associated with a connection.

When this information element is included in a SETUP (or ADD PARTY) message, it contains:

- the policy constraint that must be used to route and establish the connection (respectively, party), or
- the request for a report to be returned in the CONNECT (respectively, ADD PARTY ACKNOWLEDGE) message for that connection (respectively, party), or
- both.

A policy constraint can contain up to six policies. Each policy is in turn defined as the combination of one or two policy operators ("require" or "must avoid") each applying to a Ne-NSC list and /or a Rp-NSC list. Ne-NSC lists and Rp-NSC lists each contain a list operator defining how the list must be interpreted ("single", "logical AND", "logical OR"). A simple policy constraint will contain a single policy. When multiple policies are contained, they are considered as an ordered list, the policy appearing first in the information element being the most desirable.

When this information element is included in a CONNECT or an ADD PARTY ACKNOWLEDGE message, it contains a report comprised of:

- a list of Ne-NSC identifiers, or
- a list of Rp-NSC identifiers, or
- both.

Unless specified otherwise, high level octet groups and octet groups within octet groups in the Policy constraint information element are position independent, i.e. they need not appear in a certain order within the information element.

At a PNNI, or an AINI that would grant a pass along request to a Policy constraint information element, the information element content validation rules specified in Section 10 shall apply. At any other type of interface, normal information element content validation rules shall be followed.

To allow for future extensions of the Policy constraint information element, an unrecognized octet group identifier shall always be assumed to be immediately followed by a one octet length field indicating the length of the octet group's contents, excluding the two octets used for the identifier and the length. Note that a length of zero is allowed.

The number of instances of this information element in a message is limited to one.

Bits 8	7	6	5	4	3	2	1	Octets
Policy constraint information element identifier								
1	1	1	1	1	0	0	0	1
ext. 1	Coding standard		IE instruction field					2
Length of Policy constraint information element contents								3
								4

Policy Identifier								5 * (Notes 1, 2)
0	0	0	0	0	0	0	1	
Policy Length								5.1 *
Policy Operator Identifier								5.2 * (Notes 3, 4)
0	0	0	0	0	0	1	0	
Policy Operator Length								5.2.1 *
Policy Operator								5.2.2 *
Ne-NSC List Identifier								5.2.3 *
0	0	0	0	0	0	1	1	
Ne-NSC List Length								5.2.3.1 *
Ne-NSC List Operator								5.2.3.2 *
Ne-NSC Identifier Value								5.2.3.3 * (Note 6) 5.2.3.4 * (Note 6)
Rp-NSC List Identifier								5.2.4 * (Note 5)
0	0	0	0	0	1	0	0	
Rp-NSC List Length								5.2.4.1 *
Rp-NSC List Operator								5.2.4.2 *
Rp-NSC Identifier Value								5.2.4.3 * (Note 7) 5.2.4.4 * (Note 7)
Report Request Identifier								6 * (Note 8)
0	0	0	0	0	1	0	1	
Report Request Length								6.1 *
Report Request Indicator								6.2*
Report Identifier								7 * (Note 9)
0	0	0	0	0	1	1	0	
Report Length								7.1 *
Ne-NSC Report List Identifier								7.2 * (Note 10)
0	0	0	0	0	1	1	1	
Ne-NSC Report List Length								7.2.1 *
Ne-NSC Identifier Value								7.2.2 * (Note 11) 7.2.3 * (Note 11)
Rp-NSC Report List Identifier								7.3 * (Note 10)
0	0	0	0	1	0	0	0	
Rp-NSC Report List Length								7.3.1 *
Rp-NSC Identifier Value								7.3.2 * (Note 12) 7.3.3 * (Note 12)
Report Gap Identifier								7.4 * (Note 10)
0	0	0	0	1	0	0	1	
Report Gap Length (set to 0)								7.4.1 * (Note 13)

Note 1 - Octet group 5 shall only be included if the Policy constraint information element is contained in a SETUP or an ADD PARTY message.

Note 2 - Octet group 5 may appear up to 6 times. When octet group 5 appears more than once, each occurrence shall be considered as being part of an ordered list of policies where the first occurrence (first policy in the list) is considered more desirable than the second occurrence (second policy in the list), which is more desirable than the third occurrence (third policy in the list), etc. As such, the order in which multiple occurrences of octet group 5 appear in this information element shall not be modified by nodes along the path of the connection.

Note 3 - Octet group 5.2 with octet 5.2.2 set to the “require” operator shall contain:

- a single octet group 5.2.3, or
- a single octet group 5.2.4, or
- a single octet group 5.2.3 and a single octet group 5.2.4

Octet group 5.2 with octet 5.2.2 set to the “must avoid” operator shall contain a single octet group 5.2.3.

Note 4 - Octet group 5.2 shall appear at least once and may appear up to 2 times within a single policy (i.e. within octet group 5).
When octet group 5.2 appears twice within a single policy, one occurrence shall have octet 5.2.2 set to the “require” operator, while the other occurrence shall have octet 5.2.2 set to the “must avoid” operator.

Note 5- Octet group 5.2.4 may not be contained in an octet group 5.2 with octet 5.2.2 set to the “must avoid” operator.

Note 6 - Octets 5.2.3.3 and 5.2.3.4 may be repeated within octet group 5.2.3, subject to the Policy constraint information element not exceeding its maximum length.

Note 7 - Octets 5.2.4.3 and 5.2.4.4 may be repeated within octet group 5.2.4, subject to the Policy constraint information element not exceeding its maximum length.

Note 8 - Octet group 6 may only be included if the Policy constraint information element is contained in a SETUP or an ADD PARTY message. It is included to request that a report be returned in the CONNECT (or ADD PARTY ACKNOWLEDGE) message for that connection (or party).

Note 9 - Octet group 7 may only be included if the Policy constraint information element is contained in a CONNECT or ADD PARTY ACKNOWLEDGE message.

Note 10 - May appear at most once as part of octet group 7.

Note 11 - May be repeated multiple times within octet group 7.2, subject to the Policy constraint information element not exceeding its maximum length.

Note 12 - May be repeated multiple times within octet group 7.3, subject to the Policy constraint information element not exceeding its maximum length.

Note 13 - The Report Gap length is always set to zero.

Figure 5-1: Policy constraint information element

Coding standard (octet 2)

Bits	Meaning
7 6	
1 1	ATM Forum specific

Policy Length (octet 5.1)

Length of the Policy contents in octets, i.e. excluding the octets used for the Policy length and the identifier.

Policy Operator Length (octet 5.2.1)

Length of the Policy Operator contents in octets, i.e. excluding the octets used for the Policy Operator length and the identifier.

Policy Operator (octet 5.2.2)

Bits								Meaning
8	7	6	5	4	3	2	1	
0	0	0	0	0	0	0	0	"require" Operator
0	0	0	0	0	0	0	1	"must avoid" Operator
All other values								Reserved

Ne-NSC List Length (octet 5.2.3.1)

Length of the Ne-NSC list contents (including octet 5.2.3.2) in octets, i.e. excluding the octets used for the Ne-NSC list length and the identifier.

Ne-NSC List Operator (octet 5.2.3.2)

Bits								Meaning
8	7	6	5	4	3	2	1	
0	0	0	0	0	0	0	0	Single Ne-NSC
0	0	0	0	0	0	0	1	Logical AND
0	0	0	0	0	0	1	0	Logical OR
All other values								Reserved

Ne-NSC Identifier Value (octets 5.2.3.3 and 5.2.3.4; octets 7.2.2 and 7.2.3)

The Ne-NSC Identifier is a 2 octet binary value used to identify a specific Ne-NSC.

The minimum value of a Ne-NSC Identifier is 1.

Rp-NSC List Length (octet 5.2.4.1)

Length of the Rp-NSC list contents (including octet 5.2.4.2) in octets, i.e. excluding the octets used for the Rp-NSC list length and the identifier.

Rp-NSC List Operator (octet 5.2.4.2)

Bits								Meaning
8	7	6	5	4	3	2	1	
0	0	0	0	0	0	0	0	Single Rp-NSC
0	0	0	0	0	0	0	1	Logical AND
0	0	0	0	0	0	1	0	Logical OR
All other values								Reserved

Rp-NSC Identifier (octets 5.2.4.3 and 5.2.4.4; octets 7.3.2 and 7.3.3)

The Rp-NSC Identifier is a 2 octet binary value used to identify a specific Rp-NSC.

The minimum value of an Rp-NSC Identifier is 0. The Rp-NSC Identifier value 0 is referred to as Rp-NSC_Bare and identifies "bare resources".

Report Request Length (octet 6.1)

Length of the Report Request contents in octets, i.e. excluding the octets used for the Report Request length and identifier.

Report Request Indicator (octet 6.2)

Bits								Meaning
8	7	6	5	4	3	2	1	
0	0	0	0	0	0	0	1	Report all required NSCs (Note 1)
0	0	0	0	0	0	1	0	Report required Ne-NSCs (Note 2)
0	0	0	0	0	0	1	1	Report required Rp-NSCs (Note 3)
0	0	0	0	0	1	0	0	Report all Ne-NSCs (Note 4)
0	0	0	0	0	1	0	1	Report all Ne-NSCs and required Rp-NSCs (Note 5)
All other values								Reserved

Note 1 - With such a request, the report contained in the CONNECT or ADD PARTY ACKNOWLEDGE message will list the Ne-NSC and Rp-NSC identifiers that both tag the resources in which the connection was established, and were part of “require” policies used to progress the connection or party, respectively.

Note 2 - With such a request, the report contained in the CONNECT or ADD PARTY ACKNOWLEDGE message will list the Ne-NSC identifiers that both tag the resources in which the connection was established, and were part of “require” policies used to progress the connection or party, respectively.

Note 3 - With such a request, the report contained in the CONNECT or ADD PARTY ACKNOWLEDGE message will list the Rp-NSC identifiers that both tag the resources in which the connection was established, and were part of “require” policies used to progress the connection or party, respectively.

Note 4 - With such a request, the report contained in the CONNECT or ADD PARTY ACKNOWLEDGE message will list all the Ne-NSC identifiers that tag entities supporting the connection or new branch, respectively.

Note 5 - With such a request, the report contained in the CONNECT or ADD PARTY ACKNOWLEDGE message will list:

- all the Ne-NSC identifiers that tag entities supporting the connection or new branch, respectively; and
- the Rp-NSC identifiers that both tag the resources in which the connection was established, and were part of “require” policies used to progress the connection or party, respectively.

Report Length (octet 7.1)

Length of the Report contents in octets, i.e. excluding the octets used for the Report length and the identifier.

Ne-NSC Report List Length (octet 7.2.1)

Length of the Ne-NSC report list contents in octets, i.e. excluding the octets used for the Ne-NSC report list length and the identifier.

Rp-NSC Report List Length (octet 7.3.1)

Length of the Rp-NSC list contents in octets, i.e. excluding the octets used for the Rp-NSC list length and the identifier.

Report Gap Length (octet 7.4.1)

Length of the Report Gap is always set to zero.

6 Path Selection with Policy Routing

[Normative]

Policy Routing reduces the set of resources on which path selection, PNNI GCAC (as defined in Section 5.13 of [PNNI 1.1]), local link selection and actual CAC are performed:

- Without Policy Routing, the applicable PNNI GCAC algorithm for a connection is performed on a set of resources equal to the resources of the entire routing domain. With Policy Routing, GCAC for a given connection is only performed on the subset of resources that match a policy within the policy constraint associated with the connection.
- Similarly, in PNNI and AINI, actual CAC is performed on all the available resources of links leading to the next node on the path of the connection. With Policy Routing, actual CAC for a given connection is performed on the subset of those resources that match a policy within the policy constraint associated with the connection.

A policy shall apply to both directions of a connection.

For each policy defined in this specification, this section specifies which resources a node shall consider when it computes a path and performs local link and resource selection using that policy.

6.1 Path Selection for a Connection with no Policy Constraint

Path selection for a connection with no policy constraint shall be performed considering only bare resources. If no acceptable path through bare resources exists, then the connection shall be released, following applicable procedures. If the interface is a PNNI or an AINI, the connection may be cranked back, as specified in Annex B of [PNNI 1.1] or Annex A of [AINI 1.1], respectively.

6.2 Path Selection for a Connection with a Policy Constraint Containing a Single Policy

Path selection for a connection with a policy constraint containing a single policy shall be performed using that policy, as defined in this section. When performing path selection using a policy, the topological map of the PNNI routing domain shall be "pruned", leaving only the network entities and resources that match the policy.

When performing path selection using a given policy, a node shall ensure that nodes along the path of the connection will be able to understand (or can safely ignore) that policy. Specifically:

- If the policy allows routing on untagged resources, then the selected path may go through nodes that do not support Policy Routing (i.e. nodes that do not advertise a Policy Version IG).
- If the policy is a "newer" policy that:
  1. does not allow routing on untagged resources, and
  2. is using syntax of policy version "x" that is not supported in previous policy versions,

  then the node doing the path selection shall ensure that nodes along the path of the connection will understand the signalled policy; i.e. that node shall prune nodes that do not advertise a supported policy version of "x" or higher from its topological map of the PNNI routing domain.

Reachability information differs from other topological data provided by PNNI Routing in that it must be available to first identify the target of a path computation. For this reason, resources associated with a reachable ATM addresses advertisement (either an Internal Reachable ATM Addresses IG or an Exterior Reachable ATM Addresses IG) that:

- has its "Tagged by all Rp-NSCs" flag set to zero, and
- does not contain a Ne-NSC Identifiers IG, and
- does not contain any Resource Partition IG,

are always considered during path computation, regardless of the policy used. Note that if a reachable ATM addresses advertisement either has its "Tagged by all Rp-NSCs" flag set to one or contains either a Ne-NSC Identifiers IG or a Resource Partition IG, then the rules defined in the following sections apply to the resources associated with that advertisement.

When performing path selection for a connection with a policy constraint containing a single policy, if no acceptable path that satisfies this policy is available, then the connection shall be released, following applicable procedures. If the interface is a PNNI or an AINI, the connection may be cranked back, using the appropriate crankback cause, as specified in Annex B of [PNNI 1.1] or Annex A of [AINI 1.1], respectively.

A PNNI node that complies with Policy Routing Version 1.0 shall be capable of performing path selection considering all policies defined in all the following sub-sections.

6.2.1 Path Selection for a Connection with a Policy on a Single NSC

6.2.1.1 Policy "require (single {NSC})"

Path selection for a connection with the policy "require (single {NSC_1})" shall be performed considering only the resources that are tagged with NSC_1. Note that the resources considered may also be tagged by other NSCs.

The above shall apply whether NSC_1 is a Ne-NSC or a Rp-NSC.

6.2.1.2 Policy "must avoid (single {Ne-NSC})"

Path selection for a connection with a policy "must avoid (single {Ne-NSC_1})" shall be performed considering only bare resources of network entities that are not tagged by Ne-NSC_1. Note that this does not exclude network entities that are tagged by other Ne-NSCs.

6.2.2 Path Selection for a Connection with a "require" Policy on a List of NSCs

6.2.2.1 Policy "require (logical OR {list of Ne-NSCs})"

Path selection for a connection with a policy "require (logical OR {list of Ne-NSCs})" shall be performed considering the bare resources of network entities that are tagged by any one or any combination of the listed Ne-NSCs. Note that the network entities considered may also be tagged by other Ne-NSCs.

6.2.2.2 Policy "require (logical OR {list of Rp-NSCs})"

Path selection for a connection with a policy "require (logical OR {list of Rp-NSCs})" shall be performed considering the resources in resource partitions that are tagged by any one or any combination of the listed Rp-NSCs. Note that the resource partitions considered may also be tagged by other Rp-NSCs. In addition, when Rp-NSC_Bare is part of the list of Rp-NSCs, bare resources shall also be considered in path selection.

6.2.2.3 Policy "require (logical AND {list of Ne-NSCs})"

Path selection for a connection with a policy "require (logical AND {list of Ne-NSCs})" shall be performed considering only the bare resources of network entities that are tagged by all the listed Ne-NSCs at the same time. Note that the network entities considered may also be tagged by other Ne-NSCs.

6.2.2.4 Policy "require (logical AND {list of Rp-NSCs})"

Path selection for a connection with a policy "require (logical AND {list of Rp-NSCs})" shall be performed considering only the resources in resource partitions that are tagged by all the listed Rp-NSCs at the same time. Note that the resource partitions considered may also be tagged by other Rp-NSCs.

If Rp-NSC_Bare is part of the list of Rp_NSCs, then the policy shall be treated as an unrecognized Policy octet group as defined in Section 10.

6.2.2.5 Require Policy on a list of Ne-NSCs and a list of Rp-NSCs

Path selection for a connection with a "require" policy containing a list of Rp-NSCs and a list or Ne-NSCs shall be performed considering the resource partitions that match the "require" policy on the list of Rp-NSCs, within network entities that match the "require" policy on the list of Ne-NSCs.

This is equivalent to considering such a policy as a logical AND between a "require" on the list of Ne-NSCs, and another "require" on the list of Rp-NSCs.

6.2.3 Path Selection for a Connection with a "must avoid" Policy on a List of Ne-NSCs

6.2.3.1 Policy "must avoid (logical OR {list of Ne-NSCs})"

Path selection for a connection with a policy "must avoid (logical OR {list of Ne-NSCs})" shall be performed considering only the bare resources of network entities that are not tagged by any one of the listed Ne-NSCs. Note that the network entities considered may be tagged by any other Ne-NSCs.

6.2.3.2 Policy "must avoid (logical AND {list of Ne-NSCs})"

Path selection for a connection with a policy "must avoid (logical AND {list of Ne-NSCs})" shall be performed considering only the bare resources of network entities that are NOT tagged by all the listed Ne-NSCs. The connection may be routed on network entities that are tagged by some (and not all) of the listed Ne-NSCs. Note that the network entities considered may also be tagged by other Ne-NSCs.

6.2.4 Path Selection for a Connection with a Policy containing both "require" and "must avoid" Operators

Path selection for a connection with a policy containing both "require" and "must avoid" policy operators shall be performed considering only resources that satisfy both policy operators at the same time. As a result, instead of considering the full PNNI routing domain as the input to the "must avoid" part of the policy, the input of the "must avoid" shall be the subset comprising the resources that match the "require" part of the policy.

6.3 Path Selection for a Connection with a Policy Constraint Containing Multiple Policies

A policy constraint that contains multiple policies shall be considered to contain an ordered list of policies, where the policy appearing first is the most desirable, while the policy appearing last is the least desirable.

Path selection for a connection with a policy constraint containing an ordered list of policies shall be performed by first considering all the resources of the PNNI routing domain that match (as defined in Section 6.2) the first recognized policy (as defined in Section 10) in the list. If no acceptable path can be found (to be distinguished from an actual connection setup attempt failure), then path selection shall be performed considering all the resources of the PNNI routing domain that match the second (i.e. next in order of preference) recognized policy in the list. If no acceptable path can be found, then path selection shall be performed considering all the resources of the PNNI routing domain that match the third recognized policy in the list, if present.

These path selection attempts shall be performed until either an acceptable path is found, or all the recognized policies in the policy constraint have been considered. If no acceptable path is available, the connection shall be released, following applicable procedures. If the interface is a PNNI or an AINI, the connection may be cranked back, using the appropriate crankback cause, as specified in Annex B of [PNNI 1.1] or Annex A of [AINI 1.1], respectively.

A PNNI node that complies with Policy Routing Version 1.0 shall be capable of performing path selection considering an ordered list of 6 policies.

6.4 Local Link and Resource Selection during Connection Establishment

Selection of the local link over which to forward a connection with a policy constraint shall be performed according to the procedures in Sections 6.2 and 6.3.

During actual CAC, selection of the resource partition in which to establish a connection with a policy constraint shall be performed according to the procedures related to Rp-NSCs in Sections 6.2 and 6.3.

When multiple parallel links or resource partitions match the same policy, selection of the link or the resource partition in which to establish the connection is an implementation specific issue.

6.5 Alternate Routing Following Crankback

During crankback of a connection with a policy constraint, any node that attempts to find an alternate path for that connection shall follow the procedures of Section 6.2 and 6.3.

7 PNNI support of Policy Routing

[Normative]

7.1 PNNI Routing Extensions

A total of three new PNNI Routing information groups are introduced by Policy Routing:

- The Policy Version information group. This information group is used to advertise the fact that a node supports a specific policy version.
- The Ne-NSC Identifiers Information Group. This information group is used to advertise the Ne-NSCs that tag a given network entity.
- The Resource Partition Information Group. This information group is used to advertise the resources of a given resource partition, along with the Rp-NSCs that tag them.

In addition to these information groups, bit 15 of the information group flags (as specified in Table 5-34 of [PNNI 1.1]) is defined as the "tagged by all Rp-NSCs" flag. This flag is used to advertise the fact that resources associated with a given advertisement are to be considered as bare resources as well as resources tagged by all Rp-NSCs.

A PNNI node that complies with Policy Routing Version 1.0 shall be capable of:

- Advertising the Policy Version information group,
- Advertising at least two resource partitions per network element, each tagged by at least two Rp-NSCs,
- Advertising network elements tagged by at least two Ne-NSCs, and
- Advertising and interpreting the "Tagged by all Rp-NSCs" information group flag.

7.1.1 Changes to Existing PNNI 1.1 Sections

7.1.1.1 Updates to PNNI 1.1 Information Group Summary Tables

In order to specify the allowed nesting of PNNI Routing IGs in conjunction with the new Policy Version IG, the Ne-NSC Identifiers IG and the Resource Partition IG, Tables 5-18/PNNI 1.1 "Information Group Summary" and 5-19/PNNI 1.1 "Information Groups in PNNI Packets" are modified as follows:

- In the first Table 5-18/PNNI 1.1, add three rows for the Ne-NSC Identifiers, Resource Partition and Policy Version information groups and update other rows as follows:

Type	IG Name	Contains IGs one level down
34	Uplink information attribute	Outgoing resource availability (128), Ne-NSC identifiers (140), Resource partition (141), System capabilities (640), Security (641)
…		
96	Nodal state parameters	Outgoing resource availability (128), Ne-NSC identifiers (140), Resource partition (141), System capabilities (640), Security (641)
97	Nodal information group (Note 1)	Next higher level binding information (192), Outside nodal hierarchy list (36), Policy version (142), System capabilities (640), Security (641)
…		

140	Ne-NSC identifiers	System capabilities (640), Security (641)
141	Resource partition	Outgoing resource availability (128), Incoming resource availability (129), System capabilities (640), Security (641)
142	Policy version	System capabilities (640), Security (641)
…		
224	Internal reachable ATM addresses	Outgoing resource availability (128), Incoming resource availability (129), Ne-NSC identifiers (140), Resource partition (141), System capabilities (640), Security (641)
256	Exterior reachable ATM addresses	Outgoing resource availability (128), Incoming resource availability (129), Ne-NSC identifiers (140), Resource partition (141), Transit network ID (304), System capabilities (640), Security (641)
288	Horizontal links	Outgoing resource availability (128), Ne-NSC identifiers (140), Resource partition (141), System capabilities (640), Security (641)
289	Uplinks	Uplink information attribute (34), Outgoing resource availability (128), Ne-NSC identifiers (140), Resource partition (141), System capabilities (640), Security (641)

- In the second Table 5-18, add three rows for the Ne-NSC Identifiers, Resource Partition and Policy Version information groups, and update other rows as follows:

Type	**IG Name**	**Contained in IGs one level up**	**Contained in packets**
128	Outgoing resource availability	Uplink information attribute (34), Nodal state parameters (96), Resource partition (141), Internal reachable ATM addresses (224), Exterior reachable ATM addresses (256), Horizontal links (288), uplinks (289)	Hello (1), PTSP (2)
129	Incoming resource availability	Resource partition (141), Internal Reachable ATM Addresses (224), Exterior reachable ATM addresses (256)	PTSP (2)
140	Ne-NSC identifiers	Uplink information attribute (34), Nodal state parameters (96), Internal reachable ATM addresses (224), Exterior reachable ATM addresses (256), Horizontal links (288), uplinks (289)	Hello (1), PTSP (2)
141	Resource partition	Uplink information attribute (34), Nodal state parameters (96), Internal reachable ATM addresses (224), Exterior reachable ATM addresses (256), Horizontal links (288), uplinks (289)	Hello (1), PTSP (2)
142	Policy version	Nodal information group (97)	PTSP (2)

- Modify Table 5-19/PNNI 1.1 “Information Groups in PNNI Packets” as follows:

Type	Packet Name	Contains Igs
1	Hello	Aggregation token (32), Nodal hierarchy list (33), Uplink information attribute (34), LGN horizontal link extension (35), Outgoing resource availability (128), Ne-NSC identifiers (140), Resource partition (141), Optional GCAC parameters (160), Optional BeCR parameter (161), AccBCT parameter (162), System capabilities (640), Security (641)
2	PTSP	PTSE (64), Outside nodal hierarchy list (36), Nodal state parameters (96), Nodal information group (97), Outgoing resource availability (128), Ne-NSC identifiers (140), Resource partition (141), Policy version (142), Incoming resource availability (129), Next higher level binding (192), Optional GCAC parameters (160), Optional BeCR parameter (161), AccBCT parameter (162), Internal reachable ATM addresses (224), Exterior reachable ATM addresses (256), Horizontal links (288), Uplinks (289), Transit network ID (304) , System capabilities (640), Security (641), PAR service (768), PAR VPN ID (776), PAR IPv4 service definition (784), PAR IPv4 OSPF service definition (800), PAR IPv4 MOSPF service definition (801), PAR IPv4 BGP4 service definition (802), PAR IPv4 DNS service definition (803), PAR IPv4 PIM-SM service definition (804)
3	PTSE ACK	Nodal PTSE Ack (384) , System capabilities (640), Security (641)
4	DBSummary	Nodal PTSE summaries (512) , System capabilities (640), Security (641)
5	PTSE Request	Requested PTSE header (513) , System capabilities (640), Security (641)

7.1.1.2 Updates to PNNI 1.1 Information Groups

- Add rows at the end of Table 5-24/PNNI 1.1 “The Uplink Information Attribute” as follows:

• Any additional optional IGs needed to describe the reverse direction of the uplink.
• Optional Ne-NSC Identifiers information group (type = 140) to advertise the Ne-NSCs tagging the reverse direction of the uplink.
• Optional information groups to advertise resource partitions and the Rp-NSCs tagging them. Repeat for each resource partition configured in the reverse direction of the uplink: • Resource Partition information group (type = 141). Each Resource Partition information group contains all Outgoing resource availability information groups (type = 128) to describe the reverse direction of the uplink.

- Add rows at the end of Table 5-33/PNNI 1.1 “The Nodal State Parameters IG” as follows:

12	4	Output Port ID	
Repeat for each (set of) service category(ies):			
Outgoing resource availability information group (type = 128)			
• Optional Ne-NSC Identifiers information group (type = 140) to advertise the Ne-NSCs tagging the entity in the outgoing direction.			

• Optional information groups to advertise resource partitions and the Rp-NSCs tagging them. Repeat for each resource partition configured in the outgoing direction:
  • Resource Partition information group (type = 141). Within each Resource Partition information group, repeat for each (set of) service category(ies):
  • Outgoing resource availability information group (type = 128)

- Add one row at the end of Table 5-35/PNNI 1.1 "The Nodal IG" as follows:

130	2	*Reserved*	
Optional Policy Version information group (type = 142) to advertise the policy version supported by this node.			

- Add rows at the end of Table 5-37/PNNI 1.1 "The Internal Reachable ATM Address IG" as follows:

Optional TLV groups for resource availability information, repeat for each (set of) service category(ies): • Outgoing resource availability information group (type = 128) • Incoming resource availability information group (type = 129) If present, the resource availability information groups apply to all present reachable address prefixes, and are to be combined directly with PNNI internal service category parameters.
• Optional Ne-NSC Identifiers information group (type = 140) to advertise the Ne-NSCs tagging the entity. The Ne-NSCs listed in this information group apply to all present reachable address prefixes, in both directions.

• Optional information groups to advertise resource partitions and the Rp-NSCs tagging them. Each advertised resource partition applies to all present reachable address prefixes. Repeat for each resource partition configured:
  • Resource Partition information group (type = 141). Within each Resource Partition information group, repeat for each (set of) service category(ies):
  • Outgoing resource availability information group (type = 128)
  • Incoming resource availability information group (type = 129)

- Add rows at the end of Table 5-38/PNNI 1.1 "The Exterior Reachable ATM Address IG" as follows:

• Optional TLV groups for resource availability information, repeat for each (set of) service category(ies). If present, the resource availability information groups apply to all present reachable address prefixes, and are to be combined directly with PNNI internal service category parameters:
  • Outgoing resource availability information group (type = 128)
  • Incoming resource availability information group (type = 129)
• Additional optional TLV groups
  • Transit network ID (type = 304).

• Optional Ne-NSC Identifiers information group (type = 140) to advertise the Ne-NSCs tagging the entity. The Ne-NSCs listed in this information group apply to all present reachable address prefixes, in both directions.
• Optional information groups to advertise resource partitions and the Rp-NSCs tagging them. Each advertised resource partition applies to all present reachable address prefixes. Repeat for each resource partition configured: • Resource Partition information group (type = 141). Within each Resource Partition information group, repeat for each (set of) service

category(ies): • Outgoing resource availability information group (type = 128) • Incoming resource availability information group (type = 129)

- Add rows at the end of Table 5-39/PNNI 1.1 "The Horizontal Links IG" as follows:

• Repeat for each (set of) service category(ies):   • Outgoing resource availability information group (type = 128)
• Optional Ne-NSC Identifiers information group (type = 140) to advertise the Ne-NSCs tagging the entity in the outgoing direction.

• Optional information groups to advertise resource partitions and the Rp-NSCs tagging them. Repeat for each resource partition configured in the outgoing direction:
  • Resource Partition information group (type = 141). Within each Resource Partition information group, repeat for each (set of) service category(ies):
  • Outgoing resource availability information group (type = 128)

- Add rows at the end of Table 5-40/PNNI 1.1 "The Uplinks IG" as follows:

• Repeat for each (set of) service category(ies):   • Outgoing resource availability information group (type = 128) • Uplink Information Attribute (type = 34)
• Optional Ne-NSC Identifiers information group (type = 140) to advertise the Ne-NSCs tagging the entity in the outgoing direction.

• Optional information groups to advertise resource partitions and the Rp-NSCs tagging them. Repeat for each resource partition configured in the outgoing direction:
  • Resource Partition information group (type = 141). Within each Resource Partition information group, repeat for each (set of) service category(ies):
  • Outgoing resource availability information group (type = 128)

7.1.2 New Information Groups Encoding

7.1.2.1 The Ne-NSC Identifiers Information Group

The Ne-NSC Identifiers information group is used to advertise the set of Ne-NSCs that tag the containing advertised network entity. By definition, Ne-NSCs apply to all resources of the network entity to which they are associated.

The Ne-NSC Identifiers are advertised using a list of two octet binary values, allowing a range of 1 to 65535. Ne-NSC identifier value 0 is reserved. A Ne-NSC Identifiers IG shall contain a minimum of one Ne-NSC identifier.

A Ne-NSC Identifiers IG advertised by a node that does not advertise a Policy Version IG in its Nodal information group shall be ignored during state-significant computations (as defined in Section 5.14.9.4 of [PNNI 1.1]) and during path computations. Similarly, a node receiving an IG containing more than one Ne-NSC Identifiers IG shall only consider the first occurrence during state-significant computations and path computations.

For backwards compatibility, the information group tags of the Ne-NSC Identifiers IG shall be set to optional, summarizable and non-transitive. As a result, in accordance to the definitions of Section 5.14.2.6 of [PNNI 1.1], the information group tags shall be set to all zeroes.

Table 7-1: The Ne-NSC Identifiers Information Group

Offset	Size (Octets)	Name	Function/Description
0	2	Type	Type = 140 (Ne-NSC Identifiers)
2	2	Length	
4	1	*Reserved*	
5	1	Ne-NSC count	Ne-NSC count (*nc*) is the number of Ne-NSC Identifiers contained in the information group.
Repeat (*nc*) times			
	2	Ne-NSC Identifier	
		Padding	0-2 octets Note: The size of the Padding field is calculated so that the length of the IG is a multiple of 4, using the formula: [6 + (nc * 2)] modulus 4

7.1.2.2 The Resource Partition Information Group

The Resource Partition information group is used to advertise the resources associated with a given resource partition and the set of Rp-NSCs tagging this resource partition.

The Resource Partition IG contains a list of the Rp-NSC identifiers tagging the resources of the resource partition. The Rp-NSC identifiers are advertised using a list of two octet binary values, allowing a range of 1 to 65535. Rp-NSC identifier value 0 shall not be advertised since it corresponds to Rp-NSC_Bare in signalling. A Resource Partition IG shall contain a minimum of one Rp-NSC identifier.

Resources within a Resource Partition IG are advertised using RAIGs, in the exact same manner that RAIGs are used in PNNI Routing to advertise resources of a network entity. This implies that the same PNNI 1.1 rules covering how RAIGs are included in reachable ATM addresses, horizontal link, uplink, nodal state parameters, or ULIA IGs shall apply at the Resource Partition IG level. Specifically, if a service category appears in multiple RAIGs within a given Resource Partition IG, then only the first RAIG in which this service category appears applies for this service category in state-significant computations.

A Resource Partition IG advertised by a node that does not advertise a Policy Version IG in its Nodal information group shall be ignored during state-significant computations (as defined in Section 5.14.9.4 of [PNNI 1.1]) and during path computations.

For backwards compatibility, the information group tags of the Resource partition IG shall be set to optional, summarizable and non-transitive. As a result, in accordance to the definitions of Section 5.14.2.6 of [PNNI 1.1], the information group tags shall be set to all zeroes.

Table 7-2: The Resource Partition Information Group

Offset	Size (Octets)	Name	Function/Description
0	2	Type	Type = 141 (Resource Partition)
2	2	Length	
4	1	*Reserved*	
5	1	Rp-NSC count	Rp-NSC count (*nc*) is the number of Rp-NSC Identifiers contained in the information group.
Repeat (*nc*) times			
	2	Rp-NSC Identifier	
		Padding	0-2 octets Note: The size of the Padding field is calculated so that the length of the IG is a multiple of 4, using the formula: [6 + (nc * 2)] modulus 4
Repeat for each (set of) service category(ies) supported in the resource partition: • Outgoing resource availability information group (type = 128) • Incoming resource availability information group (type = 129). Incoming resource availability information groups may only be included if such information groups are allowed in the information group one level up (See Table 5-18/PNNI 1.1). The resource availability information groups specify the supported service categories, routing metrics and attributes that apply to the resources of the resource partition.			

7.1.2.3 The Policy Version Information Group

The Policy Version information group is used to advertise the specific policy version supported by a node. The policy version identifies the syntax of the policies and policy constraints that a node is able to signal and use during path selection.

A lowest level node supporting Policy Routing shall advertise its highest supported policy version by including the Policy Version information group with that version number in its Nodal IG. It is expected that all future versions of Policy Routing will be backwards compatible and that by advertising the highest supported policy version, a node will implicitly advertise support for all policy versions, up to and including the advertised version.

For logical group nodes, the specific policy version advertised shall be locally configurable by the service provider (See Section 7.1.5.1 for guidelines). By default, a logical group node shall advertise support for the lowest policy version that is supported by nodes in its child peer group.

A node that does not advertise a Policy Version IG shall not:

- advertise any Ne-NSC Identifiers IGs or Resource Partition IGs in PTSEs that it originates, or
- set the “Tagged by all Rp-NSCs” flag in any information group it originates.

A node receiving a Nodal IG containing more than one Policy Version IG shall only consider the first occurrence for state-significant computations (as defined in Section 5.14.9.4 of [PNNI 1.1]) and during path computations.

For backwards compatibility, the information group tags of the Policy Version IG shall be set to optional, summarizable and non-transitive. As a result, in accordance to the definitions of Section 5.14.2.6 of [PNNI 1.1], the information group tags shall be set to all zeroes.

Table 7-3: The Policy Version Information Group

Offset	Size (Octets)	Name	Function/Description
0	2	Type	Type = 142 (Policy Version)
2	2	Length	
4	1	Policy version	Specifies the policy version supported by this node. The policy version identifies the syntax of the policies and policy constraints that the node is able to signal and use during path selection. This specification specifies policy version: 1.
5	3	*Reserved*	

7.1.3 New Information Group Flag Definition

- Modify Table 5-34 of [PNNI 1.1] "Flags" as follows:

Bit ID:	bit 16 (MSB)	bit 15	bits 14...1
Bit Name:	VP Capability Flag	Tagged by all Rp-NSCs	*Reserved*

- Add the following at the end of Section 5.14.9.1.1 of [PNNI 1.1]:

  The "Tagged by all Rp-NSCs" flag is set to one to simply advertise that all the resources associated with a given advertisement are tagged by all Rp-NSCs.

  When the resources associated with a given advertisement (e.g. a Nodal State Parameters IG, an Internal Reachable ATM Addresses IG, an Exterior Reachable ATM Addresses IG, a Horizontal Links IG or an Uplinks IG) are to be considered as being tagged by all Rp-NSCs, bit 15 of the information group flags contained in the advertisement shall be set to one. Note that when bit 15 is set to one, all the resources associated with the advertisement that are not contained in a Resource Partition IG are considered both as bare resources (since they are not contained in a Resource Partition IG) and as resources being tagged by all Rp-NSCs (since bit 15 is set to one).

  As the result of this definition, an IG that contains resource advertisements for both directions of a link (e.g. an Uplinks IG, an Internal Reachable ATM Addresses IG or an Exterior Reachable ATM Addresses IG) and has the "Tagged by all Rp-NSCs" flag set to one shall be understood as meaning that the resources in both directions that are not contained in a Resource Partition IG are tagged by all Rp-NSCs. For example, if an Uplinks IG has its "Tagged by all Rp-NSCs" flag set to one, then all resources advertised within contained RAIGs and ULIAs and not contained in a Resource Partition IG shall be considered tagged by all Rp-NSCs.

  If a node receives an IG that has its "Tagged by all Rp-NSCs" flag set to one and contains a Resource Partition IG, the node shall consider that only the resources advertised within the resource partition are tagged by the Rp-NSCs explicitly listed in that Resource Partition IG. Only resources advertised within the containing IG and not within a Resource Partition IG shall be considered tagged by all Rp-NSCs.

  The setting of the "Tagged by all Rp-NSCs" flag in information groups advertised by a node that does not advertise a Policy Version IG in its Nodal information group shall be treated as if it was set to zero during state-significant computations (as defined in Section 5.14.9.4 of [PNNI 1.1]) and during path computations.

7.1.4 Significant Change Rules on Policy Routing Information Groups

Any change to:

- a contained Policy Version IG, or
- the "Tagged by all Rp-NSCs" flag, or
- a contained Ne-NSC Identifiers IG, or
- a contained Resource Partition IG

shall constitute a significant change to the containing IG. See Section 5.8.5.1 of [PNNI 1.1] for more information on what results from a significant change.

7.1.5 Advertising Policy Information in a Hierarchical PNNI Routing Domain

This section contains guidelines on how policy information should be advertised in a hierarchical PNNI routing domain. It also identifies issues and tradeoffs that must be considered when enabling Policy Routing in a hierarchical PNNI routing domain.

Because Policy Routing changes the way connections are routed through a PNNI routing domain, having logical group nodes advertise relevant policy information is necessary. There are three types of policy information that a logical group node may advertise:

1. The policy version that it supports.
2. The Ne-NSCs that are supported by a given set of resources (either aggregated link, reachable ATM addresses, radius or exception)
3. The Rp-NSCs that are supported by a given set of resources (either aggregated link, reachable ATM addresses, radius or exception)

7.1.5.1 The Policy Version advertised by an LGN

A logical group node shall advertise the policy version it supports. This indicates to nodes outside of its child peer group that they can route connections with a policy constraint up to the advertised version through this logical group node.

The specific version advertised by a given logical group node shall be locally configurable by the service provider. By default, a logical group node shall advertise support for the lowest policy version supported by nodes in its child peer group.

Following are two examples of how a service provider could configure the policy version advertised by a logical group node:

- A service provider could set the version advertised by an LGN to the highest policy version supported by any given node within its child peer group. By having the LGN advertise the highest supported policy version, a service provider will cause nodes outside of the LGN's child peer group to attempt to go through it. This has the drawback of connections possibly being cranked back if they enter the child peer group via a border node that does not support the signalled policy constraint (See Section 7.2.3.2 and 7.2.5).
- A service provider could set the version advertised by an LGN to the lowest policy version supported by any given node within its child peer group. This can also translate into not advertising support for Policy Routing at all if at least one node in the child peer group does not support it. This approach minimizes the risk of having to crankback connections that reach the child peer group, at the cost of potentially causing connections to be routed around the child peer group (if possible), even though they could have been established through it without problems.

7.1.5.2 Policy Information Aggregation during Topology Aggregation

The following applies equally to link aggregation and nodal aggregation. In both cases, what is called "policy information aggregation" is performed.

Policy information aggregation shall be performed when advertising:

- Outside links and uplinks that are to be aggregated by a border node that supports Policy Routing.
- Links between logical group nodes that are to be aggregated by a logical group node advertising support for Policy Routing.
- The radius or an exception for a logical group node advertising support for Policy Routing.
- Reachability information that results from address summarization.

Policy information aggregation is defined as the operation that, starting with the policy information (Ne-NSC Identifiers and Resource partitions) of an "input" set of entities, results in the policy information associated with the advertised aggregated entity. In the case of link aggregation, the "input set" contains available resources of links. In the case of nodal aggregation, the "input set" contains information on available resources within the child peer group (e.g. paths between 2 ports of the logical group node).

The following paragraphs contain examples of what an LGN may do during policy information aggregation.

When performing policy information aggregation, the aggregated entity may be tagged by the result of a logical OR of all the Ne-NSC identifiers associated with the entities of the "input set". This type of aggregation behavior can be considered "aggressive", since it tags the aggregated entity with a given Ne-NSC as long as one of the entities within the "input set" was tagged by that Ne-NSC.

In an environment where resource partitions within the "input set" have different contents in terms of supported ATM Service Category (e.g. one partition supports only CBR, while another supports only ABR, another supports CBR, VBR and ABR, etc.), policy information aggregation for resource partitions and Rp-NSCs can very easily explode into an intractable problem. To avoid running into such a problem, it may be beneficial to change the focus of Rp-NSC advertisements when dealing with aggregated entities. While for lowest level nodes and links, the focus is to carve the resources of a network entity into resource partitions and then tag those resource partitions with sets of Rp-NSCs, during policy information aggregation, it is recommended instead:

- To focus on advertising all the Rp-NSC Identifiers supported within the child peer group rather than on the correct set of resources associated with these Rp-NSCs. Advertising meaningful RAIGs for the resource partitions of aggregated entities will typically be challenging anyway.
- To only advertise a limited number of resource partitions.

For example, one could advertise one resource partition per ASC supported in the "input set" in addition to the usual bare resources. This would limit the number of resource partitions to be advertised to at most the number of different ASCs supported by entities in the "input set". Each of those ASC specific resource partitions would then be tagged by the Rp-NSCs that were tagging resource partitions containing resources for that ASC within the "input set". The RAIGs contained in those resource partitions would be derived following existing PNNI algorithms.

However, in an environment where the number of Rp-NSCs tagging the resource partitions in the "input set" is limited and repetitive (e.g. each entity in the "input set" contains one resource partition tagged by Rp-NSC_1 and Rp_NSC_4, another resource partition tagged by Rp-NSC_2, Rp_NSC_6 and Rp-NSC_3, etc.) it may be possible to continue advertising the same number of resource partitions (tagged by the same sets of Rp-NSCs) while simply updating the RAIGs contained in those resource partitions (following existing PNNI algorithms).

The above makes a strong case for service providers to be careful when configuring resource partitions in a hierarchical PNNI routing domain. Specifically, the service provider should configure consistent sets of resource partitions, tagged by consistent sets of Rp-NSCs throughout a peer group in order to allow the latter scheme to be applied. It is worth pointing out that by defining services throughout a network and defining them consistently, it is very likely that a well engineered network will meet the requirements that allow the latter scheme to apply.

Finally, it is worth noting that in some cases, it may be more efficient to simply tag a complete Internal / Exterior Reachable ATM Addresses, Nodal State Parameters, Horizontal links or Uplinks IG with the "Tagged by all Rp-NSCs" flag. Note however that while doing this could greatly simplify the task of policy information aggregation, it also increases the risk of crankbacks.

7.1.5.3 Policy Information Aggregation and Policies Based on the Logical AND List Operator

When looking at how policy information aggregation works, it is obvious that at the level of a logical group node, a given set of resources is more likely to be tagged by multiple Ne-NSCs and / or Rp-NSCs. This will occur even though resources within the child peer group may never be tagged by multiple NSCs at a given time.

The above can cause excessive crankbacks when policy constraints containing policies on a list of NSCs with a logical AND operator are to be routed through the PNNI routing domain. From the information advertised by the logical group node, it may seem that the child peer group supports a logical AND on certain NSCs, causing connections to be routed through it. It is only when the border node of the child peer group receives the connection that it will find that in fact, at the child peer group level, no path matching that policy exists.

Such problems are inherent to the logical AND list operator within hierarchical PNNI routing domains. To avoid such problems, it is always possible to define new NSCs that essentially correspond to a given logical AND. For example, if a connection with a "require (logical AND {Ne-NSC_1; Ne-NSC_2})" results in too many crankbacks, it may be necessary to define a new Ne-NSC in the routing domain (e.g. Ne-NSC_3) that would tag all network entities that are already tagged by both Ne-NSC_1 and Ne-NSC_2 and then route connections using the policy: "require (single {Ne-NSC_3})".

This observation does not take away the value of the logical AND list operator in non hierarchical PNNI routing domains.

7.2 PNNI Signalling Extensions

A PNNI Signalling implementation that complies with Policy Routing Version 1.0 shall be capable of:

- Supporting and processing up to six policies per Policy constraint information element,
- Supporting and processing all types of report requests defined in this specification,
- Signalling and processing all policies defined in this specification.

7.2.1 Additions to PNNI Signalling Messages

- The following row is added to Table 6-5 in Section 6.4.5.1 of [PNNI 1.1]:

Table 7-4: Additional Information Element used in PNNI

Bits 8 7 6 5	Bits 4 3 2 1	Information Element	Max Length	Min Length	Max no. of Occurrences
1 1 1 1	1 0 0 0	Policy constraint	253 (1)	6 (2)	1

Note 1 - The maximum length of the Policy constraint information element was computed to allow signalling of:

- a policy constraint containing 6 policies, each consisting of a "require" policy operator followed by a list of 4 Ne-NSCs and a list of 4 Rp-NSCs, and a "must avoid" policy operator followed by a list of 4 Ne-NSCs. And,
- a report request.

Note 2 - The minimum length of the Policy constraint information element in the SETUP and ADD PARTY messages is 7.

7.2.1.1 CONNECT

- The following row is added to Figure 6-5 in Section 6.3.1.3 of [PNNI 1.1]:

Information Element	Reference	Type	Length
Policy constraint	5.1	O (1)	6-253

Note 1 - May be included in the CONNECT message if the SETUP message contained a report request .

7.2.1.2 SETUP

- The following row is added to Figure 6-8 in Section 6.3.1.6 of [PNNI 1.1]:

Information Element	Reference	Type	Length
Policy constraint	5.1	O	7-253 (1)

Note 1 - The maximum length of the Policy constraint information element was computed to allow signalling of:

- a policy constraint containing 6 policies, each consisting of a "require" policy operator followed by a list of 4 Ne-NSCs and a list of 4 Rp-NSCs, and a "must avoid" policy operator followed by a list of 4 Ne-NSCs. And,
- a report request

7.2.1.3 ADD PARTY

- The following row is added to Figure 6-19 in Section 6.3.4.1 of [PNNI 1.1]:

Information Element	Reference	Type	Length
Policy constraint	5.1	O	7-253 (1)

Note 1 - The maximum length of the Policy constraint information element was computed to allow signalling of:

- a policy constraint containing 6 policies, each consisting of a "require" policy operator followed by a list of 4 Ne-NSCs and a list of 4 Rp-NSCs, and a "must avoid" policy operator followed by a list of 4 Ne-NSCs. And,
- a report request.

7.2.1.4 ADD PARTY ACKNOWLEDGE

- The following row is added to Figure 6-5 in Section 6.3.4.2 of [PNNI 1.1]:

Information Element	Reference	Type	Length
Policy constraint	5.1	O (1)	6-253

Note 1 - May be included in the ADD PARTY ACKNOWLEDGE message if the ADD PARTY message contained a report request.

7.2.2 Additions to PNNI Information Elements

- The following Crankback cause value is added to Section 6.4.6.3 of [PNNI 1.1]:

Bits 8 7 6 5 4 3 2 1	Number	Meaning	Diagnostics
1 1 0 0 0 0 0 0	192	Unrecognized policy constraint	

7.2.3 Signalling Procedures for Point to Point Connections

The procedures for basic call/connection control as specified in [PNNI 1.1] shall apply. This section contains additional procedures that apply when Policy Routing is supported.

7.2.3.1 Procedures at the Preceding Side

Whenever local resource selection occurs for a setup request that contains a policy constraint, the policy constraint shall be taken into account as specified in Section 6.4.

If the setup request received by the preceding side contains a Policy constraint information element and the connection is progressed, the preceding side shall include this Policy constraint information element unchanged in the SETUP message sent to the succeeding side.

When the preceding side receives the CONNECT message, if the SETUP message contained a report request and either:

- that report request was not recognized, or
- a policy with a "require" policy operator was used to select the link and resources at this interface, or
- this interface is tagged with at least one Ne-NSC,

then:

- If the received CONNECT message contains a Policy constraint information element with invalid content (as defined in Section 10), then the preceding side shall:
  - discard the received Policy constraint information element, and
  - replace it with one containing a Report octet group with a report gap, and
  - the remaining procedures of this section shall not apply.
- If the received CONNECT message contains a Policy constraint information element with valid content (as defined in Section 10) and more than one recognized Report octet group, then the following procedures shall only apply on the first recognized occurrence of the Report octet group.
- If a received Policy constraint information element is recognized and the CONNECT message is progressed, any unrecognized octet group it might contain shall be included in the forwarded Policy constraint information element, in the same position (with regards to other received octet groups) it was received in.
- If the received CONNECT message does not contain a Policy constraint information element, the preceding side shall insert one containing a report in the connect indication forwarded to Call Control.
- If the received CONNECT message contains a Policy constraint information element that does not contain a report, the preceding side shall insert a Report octet group in that Policy constraint information element.
- If the SETUP message contained an unrecognized report request, then:
  - the preceding side shall add a report gap in the connect indication, if one is not already present, and
  - the remaining procedures of this section shall not apply.
- If
  - the "require" policy operator used when forwarding the SETUP message contained a Rp-NSC list, and
  - the SETUP message contained a report request set to either "Report all required NSCs", "Report required Rp-NSCs", or "Report all Ne-NSCs and required Rp-NSCs", and
  - the received CONNECT message does not contain a Rp-NSC report list,

  then such a list shall be included in the report contained in the forwarded connect indication.
- If
  - the "require" policy operator used when forwarding the SETUP message contained a Ne-NSC list, and
  - the SETUP message contained a report request set to either "Report all required NSCs" or "Report required Ne-NSCs", and
  - the received CONNECT message does not contain a Ne-NSC report list,

  then such a list shall be included in the report contained in the forwarded connect indication.

- If
  - this interface is tagged with at least one Ne-NSC, and
  - the SETUP message contained a report request set to either “Report all Ne-NSCs” or “Report all Ne-NSCs and required Rp-NSCs”, and
  - the received CONNECT message does not contain a Ne-NSC report list,

  then such a list shall be included in the report contained in the forwarded connect indication.
- If present in the forwarded connect indication, the Rp-NSC report list shall contain all the Rp-NSCs that were contained in the received CONNECT message, if any. In addition, the Rp-NSC report list shall contain all the Rp-NSCs that were listed in the policy used when forwarding the SETUP message and which tag the resource partition into which the connection was established by this node. If the connection was established on a network entity with its “tagged by all Rp-NSCs” flag set to one, the Rp-NSC report list shall contain all the Rp-NSCs that were listed in the policy used when forwarding the SETUP. A given Rp-NSC may only appear once in the Rp-NSC report list forwarded in the connect indication. Note that if the connection was established in bare resources and Rp-NSC_Bare was contained in the policy used to forward the SETUP message, then Rp-NSC_Bare must be included in the forwarded Rp-NSC report list.
- If present in the forwarded connect indication, the Ne-NSC report list shall contain all the Ne-NSCs that were contained in the received CONNECT message, if any. In addition:
  - If the SETUP message contained a report request set to “Report required Ne-NSCs” or “Report all required NSCs”, then the Ne-NSC report list shall contain the Ne-NSCs that were listed within the “require” Policy Operator octet group of the policy used when forwarding the SETUP message and which tag the network entity over which the connection was established by this node.
  - If the SETUP message contained a report request set to “Report all Ne-NSCs” or “Report all Ne-NSCs and required Rp-NSCs”, then the Ne-NSC report list shall contain all the Ne-NSCs that tag this interface.

  A given Ne-NSC may only appear once in the Ne-NSC report list forwarded in the connect indication.
- If, as a result of the procedures above, the length of the Policy constraint information element to be included in the connect indication would exceed the information element maximum length minus two octets, then the preceding side shall include a report gap if one is not already present. The preceding side may also include as much of the information from the steps above as can fit in the information element.

When the preceding side receives a CONNECT message that contains a Policy constraint information element with valid content (as defined in Section 10), and either:

- the SETUP message did not contain any report request, or
- the SETUP message contained a valid report request, it was not forwarded using a policy with a “require” policy operator, and this interface is not tagged with any Ne-NSCs,

then the preceding side shall include the received information element unchanged in the connect indication forwarded to Call Control.

7.2.3.2 Procedures at the Succeeding Side

If the succeeding side receives a SETUP message containing a Policy constraint information element with content error (as defined in Section 10), the pass along request field (bit 4 of octet 2) set to “no pass along request” and the action indicator (bits 1-3 of octet 2) set to “clear call”, then the succeeding side shall crankback the connection with cause #100, "invalid information element contents", a diagnostic field set to the Policy constraint information element identifier and a crankback cause set to cause #192 "unrecognized policy constraint".

If a SETUP message received by the succeeding side contains a Policy constraint information element with valid content (as defined in Section 10) and the connection is progressed, the succeeding side shall include this Policy constraint information element unchanged in the setup indication forwarded to Call Control.

Whenever path, local link and resource selection occur for a received SETUP message that contains a policy constraint, the policy constraint shall be taken into account as specified in Sections 6.2, 6.3 and 6.4.

When the succeeding side receives the connect request, if the SETUP message contained a report request and either:

- that report request was not recognized, or
- a policy with a "require" policy operator was used to select resources at this interface, or
- this interface is tagged with at least one Ne-NSC,

then:

- If the received connect request contains a Policy constraint information element with invalid content (as defined in Section 10), then the succeeding side shall:
  - discard the received Policy constraint information element, and
  - replace it with one containing a Report octet group with a report gap, and
  - the remaining procedures of this section shall not apply.
- If the received connect request contains a Policy constraint information element with valid content (as defined in Section 10) and more than one recognized Report octet group, then the following procedures shall only apply on the first recognized occurrence of the Report octet group.
- If a received Policy constraint information element is recognized and the connect request is progressed, any unrecognized octet group it might contain shall be included in the forwarded Policy constraint information element, in the same position (with regards to other received octet groups) it was received in.
- If the received connect request does not contain a Policy constraint information element, the succeeding side shall insert one containing a report in the CONNECT message sent to the preceding side.
- If the received connect request contains a Policy constraint information element that does not contain a report, the succeeding side shall insert a Report octet group in that Policy constraint information element.
- If the SETUP message contained an unrecognized report request, then:
  - the succeeding side shall add a report gap in the connect indication, if one is not already present, and
  - the remaining procedures of this section shall not apply.
- If
  - the "require" policy operator used when selecting resources at this interface contained a Rp-NSC list, and
  - the SETUP message contained a report request set to either "Report all required NSCs" or "Report required Rp-NSCs", or "Report all Ne-NSCs and required Rp-NSCs", and
  - the received connect request does not contain a Rp-NSC report list,

  then such a list shall be included in the report contained in the CONNECT message.
- If
  - the "require" policy operator used when selecting resources at this interface contained a Ne-NSC list, and
  - the SETUP message contained a report request set to either "Report all required NSCs" or "Report required Ne-NSCs", and
  - the received connect request does not contain a Ne-NSC report list,

  then such a list shall be included in the report contained in the CONNECT message.

- If
  - this interface is tagged with at least one Ne-NSC, and
  - the SETUP message contained a report request set to either "Report all Ne-NSCs" or "Report all Ne-NSCs and required Rp-NSCs", and
  - the received connect request does not contain a Ne-NSC report list,

  then such a list shall be included in the report contained in the CONNECT message.
- If present in the CONNECT message, the Rp-NSC report list shall contain all the Rp-NSCs that were contained in the received connect request, if any. In addition, the Rp-NSC report list shall contain all the Rp-NSCs that were listed in the policy used when selecting resources at this interface and which tag the resource partition into which the connection was established by this node. If the connection was established on a network entity with its "tagged by all Rp-NSCs" flag set to one, the Rp-NSC report list shall contain all the Rp-NSCs that were listed in the policy used when selecting resources at this interface. A given Rp-NSC may only appear once in the Rp-NSC report list included in the CONNECT message. Note that if the connection was established in bare resources and Rp-NSC_Bare was contained in the policy used to select resources at this interface, then Rp-NSC_Bare must be included in the forwarded Rp-NSC report list.
- If present in the CONNECT message, the Ne-NSC report list shall contain all the Ne-NSCs that were contained in the received connect request, if any. In addition:
  - If the SETUP message contained a report request set to "Report required Ne-NSCs" or "Report all required NSCs", then the Ne-NSC report list shall contain the Ne-NSCs that were listed within the "require" Policy Operator octet group of the policy used when selecting resources at this interface and which tag the network entity over which the connection was established by this node.
  - If the SETUP message contained a report request set to "Report all Ne-NSCs" or "Report all Ne-NSCs and required Rp-NSCs", then the Ne-NSC report list shall contain all the Ne-NSCs that tag this interface.

  A given Ne-NSC may only appear once in the Ne-NSC report list included in the CONNECT message.
- If, as a result of the procedures above, the length of the Policy constraint information element to be included in the CONNECT message would exceed the information element maximum length minus two octets, then the succeeding side shall include a report gap if one is not already present. The succeeding side may also include as much of the information from the steps above as can fit in the information element.

When the succeeding side receives a connect request that contains a Policy constraint information element with valid content (as defined in Section 10), and either:

- the SETUP message did not contain any report request, or
- the SETUP message contained a valid report request, the resources at this interface were not selected using a policy with a "require" policy operator, and this interface is not tagged with any Ne-NSCs,

then the succeeding side shall include the received information element unchanged in the CONNECT message sent to the preceding side.

7.2.4 Signalling Procedures for Point to Multipoint Connections

The procedures for basic point to multipoint call/connection control as specified in [PNNI 1.1] shall apply. This section contains additional procedures that apply when Policy Routing is supported.

7.2.4.1 Procedures at a Branching Point

A branching point is a node where a received ADD PARTY message is forwarded to an interface where the connection does not exist and as a result gets translated into a SETUP message. At a branching point, Call Control translates a received add party indication into a setup request towards the leaf.

When an add party indication that contains a Policy constraint information element is translated into a setup request, the setup request shall contain the received Policy constraint information element unchanged.

When a connect indication that contains a Policy constraint information element is translated into an add party acknowledge request, the add party acknowledge request shall contain the received Policy constraint information element unchanged.

Because of possible race conditions during the establishment of subsequent parties, the report contained in a CONNECT message for a given party may contain information that was gathered during the setup phase of a previous party. At any given interface, the information added in a CONNECT message reports the NSCs used to establish the original connection at that interface, regardless of the specific party this message is associated with.

Procedures specific to the handling of ADD PARTY and ADD PARTY ACKNOWLEDGE messages are specified in the following sections.

7.2.4.2 Procedures at the Preceding Side

If an add party request received by the preceding side contains a Policy constraint information element, the preceding side shall include this Policy constraint information element unchanged in the ADD PARTY message sent to the succeeding side.

When a received ADD PARTY ACKNOWLEDGE message contains a Policy constraint information element, the preceding side shall include the received Policy constraint information element unchanged in the add party acknowledge indication forwarded to Call Control.

7.2.4.3 Procedures at the Succeeding Side

If the succeeding side receives an ADD PARTY message containing a Policy constraint information element with content error (as defined in Section 10), the pass along request field (bit 4 of octet 2) set to “no pass along request” and the action indicator (bits 1-3 of octet 2) set to “clear call”, then the succeeding side shall crankback the party by sending an ADD PARTY REJECT message with cause #100, "invalid information element contents", with a diagnostic field set to the Policy constraint information element identifier and a crankback cause set to cause #192 "unrecognized policy constraint".

If the ADD PARTY message received by the succeeding side contains a Policy constraint information element and the party is progressed, the succeeding side shall include this Policy constraint information element unchanged in the add party indication forwarded to Call Control.

Whenever path selection occurs for a received ADD PARTY message that contains a policy constraint, the following applies:

- If the point-to-multipoint connection already exists between two given nodes, a parallel branch between these two nodes shall not be established, even if the resources supporting the connection do not match any of the policies of the policy constraint associated with the ADD PARTY message. During path selection, this equates to considering that resources supporting the existing connection tree match all policies.
- From the branching point on to the called party, the policy constraint contained in the ADD PARTY message shall be taken into account as specified in Sections 6.2 and 6.3.

If the add party acknowledge request received by the succeeding side contains a Policy constraint information element, the succeeding side shall include this Policy constraint information element unchanged in the ADD PARTY ACKNOWLEDGE message sent to the preceding side.

7.2.5 Compatibility with nodes not supporting Policy Routing

Upon receiving a message containing a Policy constraint information element, nodes that do not support this feature will treat the Policy constraint information element as an unrecognized information element.

The setting of the IE instruction field in the Policy constraint information element will vary with the signalled policy constraint. As such, it shall be set on a connection by connection basis.

Nodes supporting Policy Routing shall set the IE instruction field in the Policy constraint information element contained in a SETUP or ADD PARTY message as follows:

- If a node originates an instance of the Policy constraint information element that allows routing on untagged resources, or the Policy constraint information element was received in a setup or add party request from a UNI interface:
    - The IE instruction field flag (bit 5 of octet 2) shall be set to “follow explicit instructions”,
    - The action indicator (bits 1-3 of octet 2) shall be set to “discard information element and proceed” or “discard information element, proceed, and report status”, and
    - The pass along request field (bit 4 of octet 2) shall be set to “pass along request”.
- If a node originates an instance of the Policy constraint information element that does not allow routing on untagged resources, or the Policy constraint information element was received from a UNI interface:
    - The IE instruction field flag (bit 5 of octet 2) shall be set to “follow explicit instructions”,
    - The action indicator (bits 1-3 of octet 2) shall be set to “clear call”, and
    - The pass along request field (bit 4 of octet 2) shall be set to “no pass along request”.

Nodes supporting Policy Routing and receiving a setup or add party request containing a Policy constraint information element from a PNNI or AINI interface shall not change the received IE instruction field.

Nodes supporting Policy Routing shall set the IE instruction field in the Policy constraint information element contained in a CONNECT or ADD PARTY ACKNOWLEDGE message as follows:

- The IE instruction field flag (bit 5 of octet 2) shall be set to “follow explicit instructions”,
- The action indicator (bits 1-3 of octet 2) shall be set to “discard information element and proceed” or “discard information element, proceed, and report status”, and
- The pass along request field (bit 4 of octet 2) shall be set to “pass along request”.

When the Policy constraint information element allows routing on untagged resources, these settings allow connections with a Policy constraint information element to be routed through nodes that do not support Policy Routing and be progressed by these nodes.

For further guidelines related to backwards compatibility, see Section 4.3.

8 AINI Support of Policy Routing

[Normative]

An AINI Signalling implementation that complies with Policy Routing Version 1.0 shall be capable of:

- Supporting and processing up to six policies per Policy constraint information element,
- Supporting and processing all types of report requests defined in this specification,
- Signalling and processing all policies defined in this specification.

8.1 Additions to AINI Signalling Messages

Section 7.2.1 shall apply.

8.2 Signalling Procedures for Point to Point Connections

The procedures for basic call/connection control as specified in [AINI 1.1] shall apply. This section contains additional procedures that apply when Policy Routing is supported.

8.2.1.1 Procedures at the Preceding Side

The following procedures shall apply in the specified order.

Whenever local resource selection occurs for a setup request that contains a policy constraint, the received policy constraint shall be taken into account as specified in Section 6.4.

If the preceding side receives a setup request which does not contain a Policy constraint information element, based on local configuration, the preceding side may include a Policy constraint information element in the SETUP message forwarded to the succeeding side. Note that the Policy constraint information element included in the SETUP message is considered as a service request to the next network, and has no bearing on local resource selection.

If the preceding side receives a setup request containing a Policy constraint information element, based on local configuration, the preceding side may:

- Include the received Policy constraint information element unchanged in the SETUP message forwarded to the succeeding side.
- Discard the received Policy constraint information element and replace it with another one in the SETUP message forwarded to the succeeding side. Note that the Policy constraint information element included in the SETUP message is considered as a service request to the next network, and has no bearing on local resource selection.
- Discard the received Policy constraint information element and forward the SETUP message to the succeeding side without any policy constraint.

If the received setup request did not contain a Policy constraint information element (whether valid or being passed along), then the preceding side shall discard any Policy constraint information element that may be contained in the received CONNECT message, and the remaining procedures of this section shall not apply.

If the received setup request contained a Policy constraint information element that was discarded by the preceding side then the remaining procedures of this section shall apply as if the received CONNECT message did not contain any Policy constraint information element.

If the received setup request contained a Policy constraint information element that was replaced by the preceding side then the remaining procedures of this section may either:

- be applied as if the received CONNECT message did not contain any Policy constraint information element, or
- be applied using the received Policy constraint information element.

When the preceding side receives a CONNECT message that contains a Policy constraint information element and either:

- the preceding side sent a SETUP message without a valid Policy constraint information element, or
- the preceding side sent a SETUP message with a valid Policy constraint information element, without a report request.

then the preceding side shall either:

- ignore the received Policy constraint information element if the preceding side would otherwise reject a pass along request for a Policy constraint information element.
- include the received Policy constraint information element unchanged in the connect indication forwarded to Call Control, if the preceding side would otherwise grant a pass along request for a Policy constraint information element.

When the preceding side receives the CONNECT message, if the setup request contained a report request and either:

- that report request was not recognized, or
- a policy with a "require" policy operator was used to select the link and resources at this interface, or
- this interface is tagged with at least one Ne-NSC,

then:

- If the preceding side would otherwise grant a pass along request for a Policy constraint information element and the received CONNECT message contains a Policy constraint information element with invalid content (as defined in Section 10), then the preceding side shall:
  - discard the received Policy constraint information element, and
  - replace it with one containing a Report octet group with a report gap, and
  - the remaining procedures of this section shall not apply.
- If the preceding side would otherwise grant a pass along request for a Policy constraint information element and the received CONNECT message contains a Policy constraint information element with valid content (as defined in Section 10) and more than one recognized Report octet group, then the following procedures shall only apply on the first recognized occurrence of the Report octet group.
- If the preceding side would otherwise reject a pass along request for a Policy constraint information element and the received CONNECT message contains a Policy constraint information element with an unrecognized octet group (as defined in Section 10), or without a Report octet group, or with more than one Report octet group, then the preceding side shall:
  - discard the received Policy constraint information element, and
  - replace it with one containing a Report octet group with a report gap, and
  - the remaining procedures of this section shall not apply.
- If a received Policy constraint information element is recognized and the message is progressed, any unrecognized octet group it might contain shall be included in the forwarded Policy constraint information element, in the same position (with regards to other received octet groups) it was received in.
- If the received CONNECT message (after applying the steps above) does not contain a Policy constraint information element, the preceding side shall insert one containing a report in the connect indication forwarded to Call Control.
- If the received CONNECT message (after applying the steps above) contains a Policy constraint information element that does not contain a report, the preceding side shall insert a Report octet group in that Policy constraint information element.

- If the setup request contained an unrecognized report request, then:
  - the preceding side shall add a report gap in the connect indication, if one is not already present, and
  - the remaining procedures of this section shall not apply.
- If
  - the "require" policy operator used when forwarding the SETUP message contained a Rp-NSC list, and
  - the setup request contained a report request set to either "Report all required NSCs" or "Report required Rp-NSCs", or "Report all Ne-NSCs and required Rp-NSCs", and
  - the received CONNECT message does not contain a Rp-NSC report list,

  then such a list shall be included in the report contained in the forwarded connect indication.
- If
  - the "require" policy operator used when forwarding the SETUP message contained a Ne-NSC list, and
  - the setup request contained a report request set to either "Report all required NSCs" or "Report required Ne-NSCs", and
  - the received CONNECT message does not contain a Ne-NSC report list,

  then such a list shall be included in the report contained in the forwarded connect indication.
- If
  - this interface is tagged with at least one Ne-NSC, and
  - the setup request contained a report request set to either "Report all Ne-NSCs" or "Report all Ne-NSCs and required Rp-NSCs", and
  - the received CONNECT message does not contain a Ne-NSC report list,

  then such a list shall be included in the report contained in the forwarded connect indication.
- If present in the forwarded connect indication, the Rp-NSC report list shall contain all the Rp-NSCs that were contained in the received CONNECT message, if any. In addition, the Rp-NSC report list shall contain all the Rp-NSCs that were listed in the policy used when forwarding the SETUP message and which tag the resource partition into which the connection was established by this node. If the connection was established on a network entity with its "tagged by all Rp-NSCs" flag set to one, the Rp-NSC report list shall contain all the Rp-NSCs that were listed in the policy used when forwarding the SETUP. A given Rp-NSC may only appear once in the Rp-NSC report list forwarded in the connect indication. Note that if the connection was established in bare resources and Rp-NSC_Bare was contained in the policy used to forward the SETUP message, then Rp-NSC_Bare must be included in the forwarded Rp-NSC report list.
- If present in the forwarded connect indication, the Ne-NSC report list shall contain all the Ne-NSCs that were contained in the received CONNECT message, if any. In addition:
  - If the SETUP message contained a report request set to "Report required Ne-NSCs" or "Report all required NSCs", then the Ne-NSC report list shall contain the Ne-NSCs that were listed within the "require" Policy Operator octet group of the policy used when forwarding the SETUP message and which tag the network entity over which the connection was established by this node.
  - If the SETUP message contained a report request set to "Report all Ne-NSCs" or "Report all Ne-NSCs and required Rp-NSCs", then the Ne-NSC report list shall contain all the Ne-NSCs that tag this interface.

  A given Ne-NSC may only appear once in the Ne-NSC report list forwarded in the connect indication.

- If, as a result of the procedures above, the length of the Policy constraint information element to be included in the connect indication would exceed the information element maximum length minus two octets, then the preceding side shall include a report gap if one is not already present. The preceding side may also include as much of the information from the steps above as can fit in the information element.

When the preceding side receives a CONNECT message that contains a Policy constraint information element with valid content, the SETUP message contained a valid report request, the SETUP message was not forwarded using a policy with a “require” policy operator, and this interface is not tagged with any Ne-NSCs, then the preceding side shall include the received information element unchanged in the connect indication forwarded to Call Control.

8.2.1.2 Procedures at the Succeeding Side

The following procedures shall apply in the specified order.

If the succeeding side would otherwise grant a pass along request for a Policy constraint information element and it receives a SETUP message containing a Policy constraint information element with content error (as defined in Section 10), the pass along request field (bit 4 of octet 2) set to “no pass along request” and the action indicator (bits 1-3 of octet 2) set to “clear call”, then the succeeding side shall crankback the connection with cause #100, "invalid information element contents", a diagnostic field set to the Policy constraint information element identifier and a crankback cause set to cause #192 "unrecognized policy constraint".

If the succeeding side would otherwise reject a pass along request for a Policy constraint information element and it receives a SETUP message containing a Policy constraint information element with an unrecognized policy or an unrecognized octet group (as defined in Section 10), then the succeeding side shall reject the connection with Cause #100 “invalid information element contents”, with a diagnostic field set to the Policy constraint information element identifier.

If the succeeding side receives a SETUP message which does not contain a Policy constraint information element and the connection is progressed, based on local configuration, the succeeding side may include a Policy constraint information element in the setup indication forwarded to Call Control.

If the succeeding side receives a SETUP message containing a Policy constraint information element and the connection is progressed, based on local configuration, the succeeding side may:

- Include the received Policy constraint information element unchanged in the setup indication forwarded to Call Control.
- Discard the received Policy constraint information element and replace it with another one in the setup indication forwarded to Call Control. Note that the Policy constraint information element included in the setup indication may contain a new set of policies and a new report request.
- Discard the received Policy constraint information element and forward the setup indication to Call Control without any policy constraint.

Path and local link selection for a setup indication that contains a policy constraint shall be performed as specified in Sections 6.2, 6.3 and 6.4. Whenever local resource selection occurs for a setup indication that contains a policy constraint in a Policy constraint information element that was not added or replaced by the succeeding side, the policy constraint shall be taken into account as specified in Section 6.4. When local resource selection occurs for a setup indication that contains a policy constraint in a Policy constraint information element that was added or replaced by the succeeding side, the policy constraint may be taken into account as specified in Section 6.4.

If the setup indication that was forwarded to Call Control contained a Policy constraint information element that was added by the succeeding side, the CONNECT message sent to the preceding side shall not contain a Policy constraint information element.

If the setup indication that was forwarded to Call Control contained a Policy constraint information element that was replaced by the succeeding side, either the CONNECT message sent to the preceding side shall not contain a Policy constraint information element, or the succeeding side shall follow the remaining procedures in this section.

When the succeeding side receives a connect request that contains a Policy constraint information element and either:

- the succeeding side forwarded a setup indication without a valid Policy constraint information element, or
- the succeeding side forwarded a setup indication with a valid Policy constraint information element, without a report request.

then the succeeding side shall either:

- ignore the received Policy constraint information element if the succeeding side would otherwise reject a pass along request for a Policy constraint information element.
- include the received Policy constraint information element unchanged in the CONNECT message sent to the preceding side, if the succeeding side would otherwise grant a pass along request for a Policy constraint information element.

When the succeeding side receives the connect request, if the setup indication forwarded to Call Control contained a report request and either:

- that report request was not recognized, or
- a policy with a “require” policy operator was used to select resources at this interface, or
- this interface is tagged with at least one Ne-NSC,

then:

- If the succeeding side would otherwise grant a pass along request for a Policy constraint information element and the received connect request contains a Policy constraint information element with invalid content (as defined in Section 10), then the succeeding side shall:
  - discard the received Policy constraint information element, and
  - replace it with one containing a Report octet group with a report gap, and
  - the remaining procedures of this section shall not apply.
- If the succeeding side would otherwise grant a pass along request for a Policy constraint information element and the received connect request contains a Policy constraint information element with valid content (as defined in Section 10) and more than one recognized Report octet group, then the following procedures shall only apply on the first recognized occurrence of the Report octet group.
- If the succeeding side would otherwise reject a pass along request for a Policy constraint information element and the received connect request contains a Policy constraint information element with an unrecognized octet group (as defined in Section 10), or without a Report octet group, or with more than one Report octet group, then the succeeding side shall:
  - discard the received Policy constraint information element, and
  - replace it with one containing a Report octet group with a report gap, and
  - the remaining procedures of this section shall not apply.
- If a received Policy constraint information element is recognized and the connect request is progressed, any unrecognized octet group it might contain shall be included in the forwarded Policy constraint information element, in the same position (with regards to other received octet groups) it was received in.
- If the received connect request (after applying the steps above) does not contain a Policy constraint information element, the succeeding side shall insert one containing a report in the CONNECT message sent to the preceding side.

- If the received connect request (after applying the steps above) contains a Policy constraint information element that does not contain a report, the succeeding side shall insert a Report octet group in that Policy constraint information element.
- If the setup indication contained an unrecognized report request, then:
  - the succeeding side shall add a report gap in the CONNECT message, if one is not already present, and
  - the remaining procedures of this section shall not apply.
- If
  - the "require" policy operator used when selecting resources at this interface contained a Rp-NSC list, and
  - the setup indication contained a report request set to either "Report all required NSCs", or "Report required Rp-NSCs", or "Report all Ne-NSCs and required Rp-NSCs", and
  - the received connect request does not contain a Rp-NSC report list,

  then such a list shall be included in the report contained in the CONNECT message.
- If
  - the "require" policy operator used when selecting resources at this interface contained a Ne-NSC list, and
  - the setup indication contained a report request set to either "Report all required NSCs", or "Report required Ne-NSCs", and
  - the received connect request does not contain a Ne-NSC report list,

  then such a list shall be included in the report contained in the CONNECT message.
- If
  - this interface is tagged with at least one Ne-NSC, and
  - the setup indication contained a report request set to either "Report all Ne-NSCs" or "Report all Ne-NSCs and required Rp-NSCs", and
  - the received connect request does not contain a Ne-NSC report list,

  then such a list shall be included in the report contained in the CONNECT message.
- If present in the CONNECT message, the Rp-NSC report list shall contain all the Rp-NSCs that were contained in the received connect request, if any. In addition, the Rp-NSC report list shall contain all the Rp-NSCs that were listed in the policy used when selecting resources at this interface and which tag the resource partition into which the connection was established by this node. If the connection was established on a network entity with its "tagged by all Rp-NSCs" flag set to one, the Rp-NSC report list shall contain all the Rp-NSCs that were listed in the policy used when selecting resources at this interface. A given Rp-NSC may only appear once in the Rp-NSC report list included in the CONNECT message. Note that if the connection was established in bare resources and Rp-NSC_Bare was contained in the policy used to select resources at this interface, then Rp-NSC_Bare must be included in the forwarded Rp-NSC report list.

- If present in the CONNECT message, the Ne-NSC report list shall contain all the Ne-NSCs that were contained in the received connect request, if any. In addition:
  - If the setup indication contained a report request set to "Report required Ne-NSCs" or "Report all required NSCs", then the Ne-NSC report list shall contain the Ne-NSCs that were listed within the "require" Policy Operator octet group of the policy used when selecting resources at this interface and which tag the network entity over which the connection was established by this node.
  - If the setup indication contained a report request set to "Report all Ne-NSCs" or "Report all Ne-NSCs and required Rp-NSCs", then the Ne-NSC report list shall contain all the Ne-NSCs that tag this interface.

  A given Ne-NSC may only appear once in the Ne-NSC report list included in the CONNECT message.
- If, as a result of the procedures above, the length of the Policy constraint information element to be included in the CONNECT message would exceed the information element maximum length minus two octets, then the succeeding side shall include a report gap if one is not already present. The succeeding side may also include as much of the information from the steps above as can fit in the information element.

When the succeeding side receives a connect request that contains a Policy constraint information element with valid content, the setup indication contained a valid report request, the resources at this interface were not selected using a policy with a "require" policy operator, and this interface is not tagged with any Ne-NSCs, then the succeeding side shall include the received information element unchanged in the CONNECT message sent to the preceding side.

8.3 Signalling Procedures for Point to Multipoint Connections

The procedures for basic point to multipoint call/connection control as specified in [AINI 1.1] shall apply. This section contains additional procedures that apply when Policy Routing is supported.

8.3.1 Procedures at a Branching Point

See Section 7.2.4.1.

8.3.2 Procedures at the Preceding Side

If the preceding side receives an add party request which does not contain a Policy constraint information element and the SETUP message forwarded for that connection contained a Policy constraint information element then, based on local configuration, the preceding side may include a Policy constraint information element in the ADD PARTY message forwarded to the succeeding side.

If the preceding side receives an add party request containing a Policy constraint information element, based on local configuration, the preceding side may:

- Include the received Policy constraint information element unchanged in the ADD PARTY message forwarded to the succeeding side.
- Discard the received Policy constraint information element and replace it with another one in the ADD PARTY message forwarded to the succeeding side.
- Discard the received Policy constraint information element and forward the ADD PARTY message to the succeeding side without any policy constraint.

If the preceding side discarded a received Policy constraint information element and forwarded the SETUP message without one, it is recommended that subsequent ADD PARTY messages also not contain any Policy constraint information element. Similarly, if the preceding side added or replaced the Policy constraint in the SETUP message, it is recommended that subsequent ADD PARTY messages contain the same Policy constraint information element.

When a received ADD PARTY ACKNOWLEDGE message contains a Policy constraint information element and either:

- the received add party request did not contain a Policy constraint information element (whether valid or being passed along), or
- the received add party request contained a Policy constraint information element that was discarded by the preceding side,

then the preceding side shall discard the received Policy constraint information element from the add party acknowledge indication forwarded to Call Control.

When a received ADD PARTY ACKNOWLEDGE message contains a Policy constraint information element and the received add party request contained a Policy constraint information element that was replaced by the preceding side, then the preceding side may discard the received Policy constraint information element from the add party acknowledge indication forwarded to Call Control.

When a received ADD PARTY ACKNOWLEGE message contains a Policy constraint information element which the preceding side does not discard, then the preceding side shall include the received Policy constraint information element unchanged in the add party acknowledge indication forwarded to Call Control.

8.3.3 Procedures at the Succeeding Side

The following procedures shall apply in the specified order.

If the succeeding side would otherwise grant a pass along request for a Policy constraint information element and it receives an ADD PARTY message containing a Policy constraint information element with content error (as defined in Section 10) the pass along request field (bit 4 of octet 2) set to “no pass along request” and the action indicator (bits 1-3 of octet 2) set to “clear call”, then the succeeding side shall crankback the party by sending an ADD PARTY REJECT message with cause #100, "invalid information element contents", with a diagnostic field set to the Policy constraint information element identifier and a crankback cause set to cause #192 "unrecognized policy constraint".

If the succeeding side would otherwise reject a pass along request for a Policy constraint information element and it receives an ADD PARTY message containing a Policy constraint information element with an unrecognized policy or an unrecognized octet group (as defined in Section 10), then the succeeding side shall reject the party with Cause #100 “invalid information element contents”, with a diagnostic field set to the Policy constraint information element identifier.

If the succeeding side receives an ADD PARTY message which does not contain a Policy constraint information element and the party is progressed , based on local configuration, the succeeding side may include a Policy constraint information element in the add party indication forwarded to Call Control.

If the succeeding side receives an ADD PARTY message containing a Policy constraint information element and the party is progressed, based on local configuration, the succeeding side may:

- Include the received Policy constraint information element unchanged in the add party indication forwarded to Call Control.
- Discard the received Policy constraint information element and replace it with another one in the add party indication forwarded to Call Control.
- Discard the received Policy constraint information element and forward the add party indication to Call Control without any policy constraint.

If the succeeding side discarded a received Policy constraint information element and forwarded the setup indication without one, it is recommended that subsequent add party indications also not contain any Policy constraint information element. Similarly, if the succeeding side added or replaced the Policy constraint in the setup indication, it is recommended that subsequent add party indications contain the same Policy constraint information element.

Whenever path selection occurs for an add party indication that contains a policy constraint, the following applies:

- If the point-to-multipoint connection already exists between two given nodes, a parallel branch between these two nodes shall not be established, even if the resources supporting the connection do not match any of the policies of the policy constraint associated with the add party indication. During path selection, this equates to considering that resources supporting the existing connection tree match all policies.
- From the branching point on to the called party, the policy constraint contained in the add party indication shall be taken into account as specified in Sections 6.2 and 6.3.

If the add party indication that was forwarded to Call Control did not contain a Policy constraint information element, or it contained a Policy constraint information element that was added by the succeeding side, the ADD PARTY ACKNOWLEDGE message sent to the preceding side shall not contain a Policy constraint information element.

If the add party indication contained a Policy constraint information element that was replaced by the succeeding side, then the succeeding side may discard any Policy constraint information element that may be contained in the received add party acknowledge request.

If the succeeding side receives an add party acknowledge request that contains a Policy constraint information element which the succeeding side does not discard, then the succeeding side shall include the received Policy constraint information element unchanged in the ADD PARTY ACKNOWLEDGE message sent to the preceding side.

8.4 Compatibility with Nodes not Supporting Policy Routing

Section 7.2.5 shall apply, with the exception of the following paragraph:

> Nodes supporting Policy Routing and receiving a setup or add party request containing a Policy constraint information element from a PNNI or AINI interface shall not change the received IE instruction field.

8.5 Interworking between AINI and PNNI

The procedures of Section 4.2 of [AINI 1.1] apply (i.e. information elements and messages are mapped to their equivalent counterparts).

9 UNI Support of Policy Routing

[Normative]

A UNI terminal equipment that complies with Policy Routing Version 1.0 shall be capable of:

- Signalling one policy as defined in this specification.

  The minimum set of required procedures amounts to considering that a UNI terminal equipment always "adds" a Policy constraint information element when it originates a connection with a policy constraint, and always "discards" the Policy constraint information element when it terminates a connection with a policy constraint.

A UNI Signalling network side that complies with Policy Routing Version 1.0 shall be capable of:

- Supporting and processing up to six policies per Policy constraint information element,
- Supporting and processing all types of report requests defined in this specification,
- Signalling and processing all policies defined in this specification.

9.1 Additions to UNI Signalling Messages

9.1.1 Basic Point to Point Call

The following is added to Section 2/SIG 4.1 Basic Point-to-Point Call:

3.1.3/Q.2931 CONNECT:
Add the following to Table 3-4/Q.2931:

Information Element	Reference	Direction	Type	Length
Policy constraint	5.1	Both	O (1)	6-253 (2)

Note 1 - May be included in the CONNECT message if the SETUP message contained a Report Request.

Note 2 - The maximum length of the Policy constraint information element was computed to allow signalling of:

- a policy constraint containing 6 policies, each consisting of a "require" policy operator followed by a list of 4 Ne-NSCs and a list of 4 Rp-NSCs, and a "must avoid" policy operator followed by a list of 4 Ne-NSCs. And,
- a report request

3.1.7/Q.2931 SETUP:
Add the following to Table 3-8/Q.2931:

Information Element	Reference	Direction	Type	Length
Policy constraint	5.1	Both	O	7-253 (1)

Note 1 - The maximum length of the Policy constraint information element was computed to allow signalling of:

- a policy constraint containing 6 policies, each consisting of a "require" policy operator followed by a list of 4 Ne-NSCs and a list of 4 Rp-NSCs, and a "must avoid" policy operator followed by a list of 4 Ne-NSCs. And,
- a report request

4.5.1/Q.2931 Coding Rules
Add the following row to Table 4-3/Q.2931:

Table 9-1: Additional Information Element used in UNI Signalling 4.1

Bits 8 7 6 5	Bits 4 3 2 1	Information Element	Max Length	Min Length	Max no. of Occurrences
1 1 1 1	1 0 0 0	Policy constraint	253 (1)	6 (2)	1

Note 1 - The maximum length of the Policy constraint information element was computed to allow signalling of:

- a policy constraint containing 6 policies, each consisting of a "require" policy operator followed by a list of 4 Ne-NSCs and a list of 4 Rp-NSCs, and a "must avoid" policy operator followed by a list of 4 Ne-NSCs. And,
- a report request

Note 2 - The minimum length of the Policy constraint information element in the SETUP and ADD PARTY messages is 7.

9.1.2 Point-to-Multipoint Calls

The following is added to Section 5/SIG 4.1 Point-to-Multipoint Calls:

8.1.2.1/Q.2971 ADD PARTY:
Add the following to Table 8-10/Q.2971:

Information Element	Reference	Direction	Type	Length
Policy constraint	5.1	Both	O	7-253 (1)

Note 1 - The maximum length of the Policy constraint information element was computed to allow signalling of:

- a policy constraint containing 6 policies, each consisting of a "require" policy operator followed by a list of 4 Ne-NSCs and a list of 4 Rp-NSCs, and a "must avoid" policy operator followed by a list of 4 Ne-NSCs. And,
- a report request

8.1.2.2/Q.2971 ADD PARTY ACKNOWLEDGE:
Add the following to Table 8-11/Q.2971:

Information Element	Reference	Direction	Type	Length
Policy constraint	5.1	Both	O(1)	6-253 (2)

Note 1 - May be included in the ADD PARTY ACKNOWLEDGE message if the ADD PARTY message contained a report request.

Note 2 - The maximum length of the Policy constraint information element was computed to allow signalling of:

- a policy constraint containing 6 policies, each consisting of a "require" policy operator followed by a list of 4 Ne-NSCs and a list of 4 Rp-NSCs, and a "must avoid" policy operator followed by a list of 4 Ne-NSCs. And,
- a report request

9.2 Signalling Procedures for Point to Point Connections

The procedures for basic call/connection control as specified in [SIG 4.1] shall apply. This section contains additional procedures that apply when Policy Routing is supported.

9.2.1 Procedures at the Originating Interface

9.2.1.1 Procedures at the User Side

The procedures of Section 8.2.1.1 shall apply with the following modifications:

- The terms "preceding side" and "succeeding side" shall respectively be replaced by "user side" and "network side".
- The terms "next network" shall be replaced by "network".
- In the fifth paragraph, delete the parenthesis "(whether valid or being passed along)".
- When the procedures make a distinction between an interface that would grant, and an interface that would reject a pass along request for a Policy constraint information element, the user shall always be considered as an interface that would reject such a pass along request, and the corresponding procedures shall apply.

9.2.1.2 Procedures at the Network Side

The procedures of Section 8.2.1.2 shall apply with the following modifications:

- The terms "preceding side" and "succeeding side" shall respectively be replaced by "user side" and "network side".
- Add the following text as a new second paragraph, immediately following the "The following procedures shall apply in the specified order" statement:

  If the network side receives a SETUP message containing a Policy constraint information element, it shall check that the user has subscribed to the services associated with the contained policy or policies. If the user has not subscribed to the services associated with the signalled policy or policies, the network side shall reject the connection with Cause # 50 "*requested facility not subscribed*" and a diagnostic field set to the Policy constraint information element identifier.
- When the procedures make a distinction between an interface that would grant, and an interface that would reject a pass along request for a Policy constraint information element, the network side shall always be considered as an interface that would reject such a pass along request, and the corresponding procedures shall apply.

9.2.2 Procedures at the Destination Interface

9.2.2.1 Procedures at the Network Side

The procedures of Section 8.2.1.1 shall apply with the following modifications:

- The terms "preceding side" and "succeeding side" shall respectively be replaced by "network side" and "user side".
- Replace the second sentence of the second bullet of the fourth paragraph with the following text:

  Note that the Policy constraint information element included in the SETUP message has no bearing on local resource selection.
- In the fifth paragraph, delete the parenthesis "(whether valid or being passed along)".
- When the procedures make a distinction between an interface that would grant, and an interface that would reject a pass along request for a Policy constraint information element, the network side shall always be considered as an interface that would reject such a pass along request, and the corresponding procedures shall apply.

9.2.2.2 Procedures at the User Side

The procedures of Section 8.2.1.2 shall apply with the following modifications:

- The terms “preceding side” and “succeeding side” shall respectively be replaced by “network side” and “user side”.
- Delete the second paragraph.
- Replace the third paragraph with the following text:

  If the user side receives a SETUP message containing a Policy constraint information element with an unrecognized policy or an unrecognized octet group (as defined in Section 10), then:

  - If the user side is the called party, the received Policy constraint information element shall be ignored.
  - If the user side is not the called party and the connection would need to be progressed further, the user side shall reject the connection with Cause #100 “invalid information element contents”, with a diagnostic field set to the Policy constraint information element identifier.
- When the remaining procedures make a distinction between an interface that would grant, and an interface that would reject a pass along request for a Policy constraint information element, the user side shall always be considered as an interface that would reject such a pass along request, and the corresponding procedures shall apply.

9.3 Signalling Procedures for Point to Multipoint Connections

The procedures for point to multipoint call/connection control as specified in [SIG 4.1] shall apply. This section contains additional procedures that apply when Policy Routing is supported.

9.3.1 Adding a Party at the Originating Interface

9.3.1.1 Procedures at the User Side

The procedures of Section 8.3.2 shall apply with the following modifications:

- The terms “preceding side” and “succeeding side” shall respectively be replaced by “user side” and “network side”.
- In the fourth paragraph, add the following text as a new first bullet:
  - the received Policy constraint information element does not contain a Report octet group, or contains an unrecognized octet group (as defined in Section 10), or contains more than one Report octet group; or
- In the (now) second bullet of the fourth paragraph, delete the parenthesis “(whether valid of being passed along)”.

9.3.1.2 Procedures at the Network Side

The procedures of Section 8.3.3 shall apply with the following modifications:

- The terms "preceding side" and "succeeding side" shall respectively be replaced by "user side" and "network side".
- Add the following text as a new second paragraph, immediately following the "The following procedures shall apply in the specified order" statement:

  If the network side receives an ADD PARTY message containing a Policy constraint information element, it shall check that the user has subscribed to the services associated with the contained policy or policies. If the user has not subscribed to the services associated with the signalled policy or policies, the network side shall reject the party with Cause # 50 "*requested facility not subscribed*" and a diagnostic field set to the Policy constraint information element.
- When the procedures make a distinction between an interface that would grant, and an interface that would reject a pass along request for a Policy constraint information element, the network side shall always be considered as an interface that would reject such a pass along request, and the corresponding procedures shall apply.

9.3.2 Add Party Establishment at the Destination Interface

9.3.2.1 Procedures at the Network Side

9.3.2.1.1 Procedures at the S_B and Coincident S_B/T_B Reference Points

The procedures of Clause 9.2/Q.2971 with the additional procedures of Section 9.2.2.1 shall apply.

9.3.2.1.2 Procedures at T_B Reference Points

The procedures of Section 8.3.2 shall apply with the following modifications:

- The terms "preceding side" and "succeeding side" shall respectively be replaced by "network side" and "user side".
- In the fourth paragraph, add the following text as a new first bullet:
  - the received Policy constraint information element does not contain a Report octet group, or contains an unrecognized octet group (as defined in Section 10), or contains more than one Report octet group; or
- In the (now) second bullet of the fourth paragraph, delete the parenthesis "(whether valid of being passed along)".

9.3.2.2 Procedures at the User Side

9.3.2.2.1 Procedures at the S_B and Coincident S_B/T_B Reference Points

The procedures of Clause 9.2/Q.2971 with the additional procedures of Section 9.2.2.2 shall apply.

9.3.2.2.2 Procedures at T_B Reference Points

The procedures of Section 8.3.3 shall apply with the following modifications:

- The terms "preceding side" and "succeeding side" shall respectively be replaced by "network side" and "user side".
- Delete the second paragraph.

- Replace the third paragraph with the following text:

  If the user side receives an ADD PARTY message containing a Policy constraint information element with an unrecognized policy or an unrecognized octet group (as defined in Section 10), then:

  - If the user side is the called party, the received Policy constraint information element shall be ignored.
  - If the user side is not the called party and the party would need to be progressed further, the user side shall reject the party with Cause #100 “invalid information element contents”, with a diagnostic field set to the Policy constraint information element identifier.
- When the procedures make a distinction between an interface that would grant, and an interface that would reject a pass along request for a Policy constraint information element, the user side shall always be considered as an interface that would reject such a pass along request, and the corresponding procedures shall apply.

9.4 Compatibility with UNIs not Supporting Policy Routing

Upon receiving a message containing a Policy constraint information element, nodes that do not support this feature will treat the Policy constraint information element as an unrecognized information element.

The setting of the IE instruction field in the Policy constraint information element will vary with the signalled policy constraint. As such, it shall be settable on a connection by connection basis.

It is recommended that users originating a connection and supporting Policy Routing set the IE instruction field in the Policy constraint information element contained in a SETUP or ADD PARTY message as follows:

- If the Policy constraint information element allows routing on untagged resources, then:
  - The IE instruction flag field (bit 5 of octet 2) shall be set to “follow explicit instructions”,
  - The action indicator (bits 1-3 of octet 2) shall be set to “discard information element and proceed” or “discard information element, proceed, and report status”, and
- If the Policy constraint information element does not allow routing on untagged resources, then:
  - The IE instruction flag field (bit 5 of octet 2) set to “follow explicit instructions”,
  - The action indicator (bits 1-3 of octet 2) set to “clear call”

It is recommended that users supporting Policy Routing set the IE instruction field in the Policy constraint information element contained in a CONNECT or ADD PARTY ACKNOWLEDGE message as follows:

- The IE instruction flag field (bit 5 of octet 2) shall be set to “follow explicit instructions”,
- The action indicator (bits 1-3 of octet 2) shall be set to “discard information element and proceed” or “discard information element, proceed, and report status”.

10 Policy Constraint Information Element Content Validation

[Normative]

This section introduces the notions of "recognized" and "unrecognized" octet groups within a Policy constraint information element. It then defines the minimum conditions that a Policy constraint information element must meet in order for it to be considered valid at a PNNI and at an AINI that grants pass along requests to Policy constraint information elements.

An unrecognized octet group is defined as:

- an octet group for which the identifier is unrecognized, or
- an octet group with a recognized identifier but with content error, or
- an octet group containing an unrecognized octet group (as defined by the two previous bullets).

Conversely, the term "recognized octet group" is defined as an octet group which has a recognized identifier, and valid contents.

During content validation of a Policy constraint information element, any unrecognized octet group shall be treated as a TLV with a one octet identifier followed by a one octet length field. Note that a length of zero is allowed, meaning that the TLV has no value octets.

Within a SETUP or ADD PARTY message at a PNNI or an AINI that grants pass along requests to Policy constraint information elements, a Policy constraint information element with valid contents is defined as an information element that, at a minimum:

- complies with the supported maximum information element length, and
- contains at least one octet group, and
- does not contain more than 6 Policy octet groups, and
- if it contains any Policy octet groups, at least one is recognized (any contained recognized Policy octet groups shall be processed as defined in Section 6, in the order that they appear in the information element), and
- does not contain any top level unrecognized octet groups other than Policy or Report Request octet groups.

Note - In the case of a node supporting Policy Routing Version 1.0, a recognized Policy octet group is one where, at a minimum, the node recognizes all contained policy operators (octet group 5.2), Ne-NSC list logical operators (octet 5.2.3.2) and Rp-NSC list logical operator (octet 5.2.4.2). Any received Ne-NSC Identifier (octets 5.2.3.3 and 5.2.3.4) other than zero, and any Rp-NSC Identifier (octets 5.2.4.3 and 5.2.4.4) values shall always be considered recognized.

Within a CONNECT or ADD PARTY ACKNOWLEDGE message at a PNNI or an AINI that grants pass along requests to Policy constraint information elements, a Policy constraint information element with valid contents is defined as an information element that, at a minimum:

- complies with the supported maximum information element length, and
- does not contain a Policy octet group.

A received Policy constraint information element with content error shall be treated as a non mandatory information element with content error.

11 Feature Interaction

[Normative]

11.1 Policy Routing and Domain-based rerouting

A rerouting node may add, replace or discard a policy constraint in the SETUP message for the rerouting connection, regardless of the policy constraint that was used to establish the initial connection. Alternatively, the rerouting connection may have the same policy constraint as the initial connection.

12 Appendix I - Example Application of Policy Routing: Inter-LATA Carrier Selection for Data Services

[Informative]

12.1 Introduction

In the past, the telecommunications regulations in the United States would not allow a ILEC (incumbent local exchange carrier) to provide inter-LATA (long-distance) voice and data services. However, due to recent regulatory changes, the ILECs are beginning to get long-distance relief on a state by state basis. As ILECs get long-distance authority, they must provide those services through a separate subsidiary and the remaining local carrier subsidiaries cannot provide any services to the affiliated long-distance entity that they do not make available to other carriers.

Currently, the most common method of interconnecting a LEC to an IXC (inter-exchange carrier) is through NNIs (network to network interface) between switches in the LEC's network and switches in the IXC's network. However, a different scheme would be to allow the IXC to provide only private line inter-LATA facilities to inter-connect the local subsidiary's networks in various LATAs, with the local-carrier providing all switching with automatic end-to-end routing and rerouting. This scheme is likely to be attractive to the IXC affiliates of ILECs as well as small "reseller" carriers. Regulatory issues require the local carrier to be able to allow multiple IXCs to provide their own sets of inter-LATA facilities for the exclusive use of their customers. In providing end-to-end routing and rerouting across LATA boundaries for these various IXCs, the ILEC must insure that each IXC's connections only utilize their inter-LATA facilities, but a common set of ILEC intra-LATA facilities can be used for all of the IXCs as well as the ILEC's intra-LATA connections.

Consider an ILEC with intra-LATA networks 1 and 2 in Figure 12-1 that are interconnected with several private line facilities from IXC's 1, 2 and 3. The intra-LATA network switches and transport facilities constitute the ILEC's network and are shared resources for all customers. The IXC's transport facilities are for exclusive use of their customers to inter-connect their sites that span multiple LATAs.

A potential application for policy routing is to tag the trunking facilities belonging to each carrier and for each connection to use a policy to allow that connection to only use facilities belonging to the proper IXC or the ILEC.

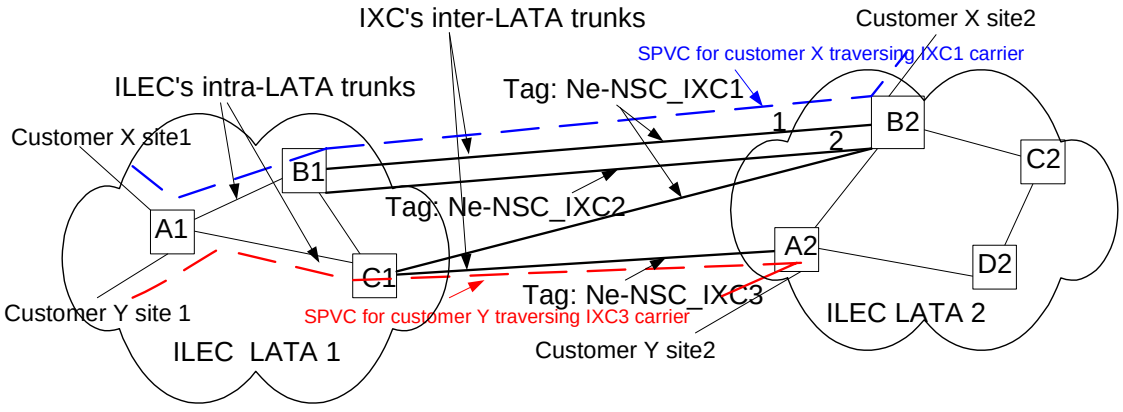


Figure 12-1: ILEC LATA / POPs Connected by IXC Facilities

12.2 Assumptions

- The intra-LATA ILEC ATM network is running PNNI.
- The inter-LATA physical facilities that connect ATM switches in different ILEC LATAs are provided by IXCs.
- Each intra-LATA ILEC ATM network belongs to a single PNNI Peer group, multiple intra-LATA networks may belong to the same or different peer groups. The IXC facilities connecting these networks could represent inside or outside links.

12.3 Inter-LATA Carrier Selection for Data Services Using Policy Routing

- Policy based routing allows an ILEC to force connections (SPVCs/SVCs) to be exclusively routed on specific inter-LATA facilities in a PNNI domain network.
- These policy constraints specify which resources a node shall consider when it computes a path or establishes a connection with that policy constraint associated with it.
- An ILEC would require that connections that cross LATA boundaries use a particular IXC's dedicated inter-LATA facilities and use the shared ILEC's facilities for the intra-LATA portion. Policy routing would allow the service provider to tag the inter-LATA dedicated facilities with a Ne-NSC tag to differentiate them from each other as well as the ILEC's facilities.

12.3.1 Resource Advertisements

- Refer to Figure 12-1, all of the ILEC's facilities within the LATA 1 and LATA 2 networks are tagged with network entity tags Ne-NSC = Ne-NSC_LEC. The intra-LATA network links are assigned to a particular resource partition Rp-NSC_LEC_1 as show in Figure 12-2.
- It is required that path selection for a connection that originates and terminates within a LATA network use only the ILEC's intra-LATA network entities and resources. For example, in case of a link failure within LATA 1, if there was not enough bandwidth on intra-LATA facilities to carry all provisioned connections between B1 and C1, it is not acceptable to go to LATA 2 and back to re-establish these connections.

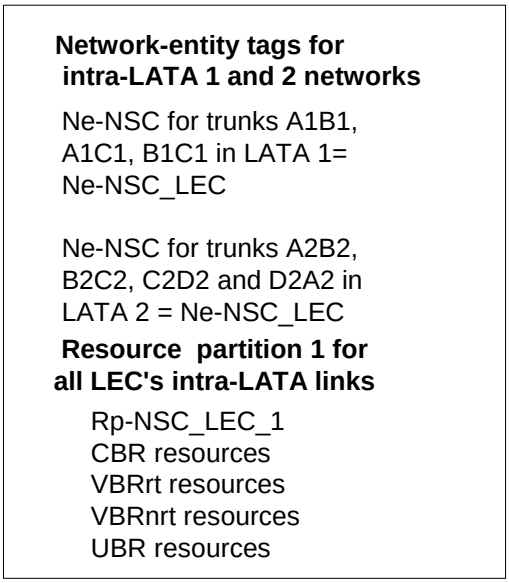


Figure 12-2: Advertising Ne-NSCs and Rp-NSCs on a Given LEC's Network Entity

The two intra-LATA ILEC networks are inter-connected with three inter-exchange carrier's (IXC1, IXC2 and IXC3) physical facilities. IXC1 has two physical facilities interconnecting switches B1 to B2 and C1 to B2. Consider that each of the IXC's physical facilities are tagged with network entity tags, Ne-NSC tags = IXC1, IXC2 and IXC3 respectively.

IXC1's physical facilities have two resource partitions Rp-NSC_IXC1_1 and Rp-NSC_IXC1_2, wherein resource partition Rp-NSC_IXC1_1 is used for initial call setup and Rp-NSC_IXC1_2 is reserved for re-route bandwidth in case of a trunk failure. IXC2 and IXC3 facilities support only 1 resource partition, that is, Rp-NSC_IXC2_1 and Rp-NSC_IXC3_1 respectively, and have no redundant bandwidth in case of trunk failure. Figure 12-3 shows advertising Ne-NSCs and Rp-NSCs on a given network entity for inter-exchange carrier's facilities.

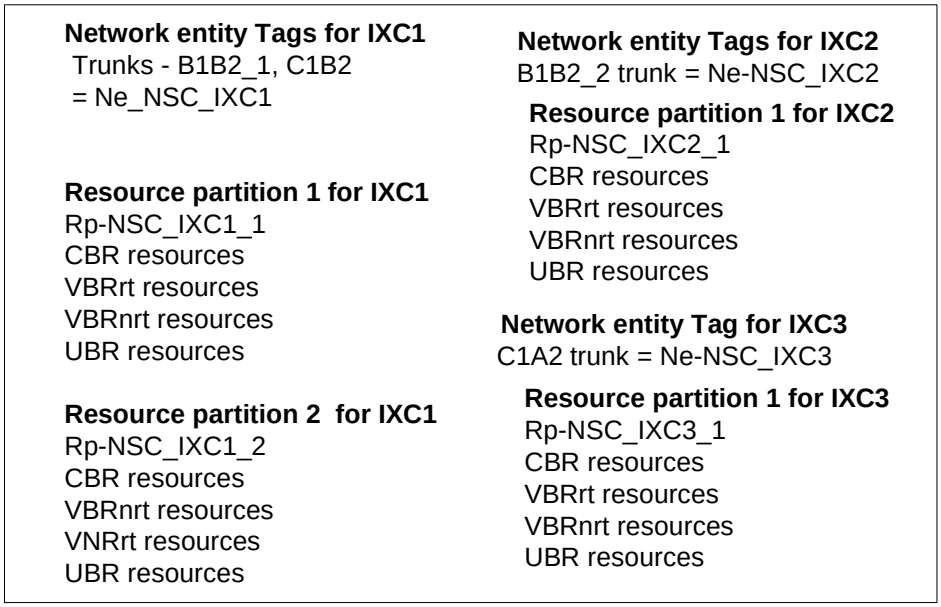


Figure 12-3: Advertising Ne-NSCs and Rp-NSCs on a Given IXC's Network Entity

The intra-LATA network entity tags (Ne-NSC_LEC), their resource partition tags (Rp-NSC_LEC_1) and inter-LATA network entity tags (Ne-NSC = IXC1, IXC2, IXC3) and their resource partitions tags (Rp-NSC_IXC1_1, Rp-NSC_IXC1_2, Rp-NSC_IXC2_1, Rp-NSC_IXC3_1) are advertised with in a PNNI routing domain. These policy constraints specify which resources a node shall consider when it computes a path or establishes a connection with that policy constraint associated with it.

12.3.2 Policy constraint for LEC's networks

The following policy constraint could be used for intra-LATA connections to insure that they only use the ILEC's intra-LATA facilities:

Policy_LEC ::= require (logical AND {Ne-NSC_LEC; Rp-NSC_LEC_1})

12.3.3 Policy constraint for IXC1's network

Consider that a customer requires that the connections be exclusively routed over IXC1's Inter-LATA facilities. In addition, IXC1 has a policy to only utilize 50% of the bandwidth on each facility for initial call setup (Rp-NSC_IXC_1) and reserve the remaining 50% for use in rerouting around failures (Rp-NSC_IXC1_2). Note that with the current PNNI standards there is no way to enforce this policy in the network. With policy based routing, the policy for path selection for a connection to be routed over IXC1's facilities between LATAs 1 and 2 at initial call setup could be:

> Policy_IXC1_option1 ::= require (logical OR {Ne-NSC_LEC; Ne-NSC_IXC1}; logical OR {Rp-NSC_LEC_1; Rp-NSC_IXC1_1)

When reestablishing connections after having a call cleared due to a failure situation there could be second option for a policy for using the reserved bandwidth. Note, this capability would require vendor specific feature development to allow different policies to be specified on initial call setup and reroutes after a failure has been detected.

> Policy_IXC1_option2 ::= require (logical OR {Ne-NSC_LEC; Ne-NSC_IXC1}; logical OR {Rp-NSC_LEC_1; Rp-NSC_IXC1_2)

The policy routing specification allows an alternate approach to address the above drawback of PNNI routing. If a switch vendor does not support defining two policies for a connection setup as described above, the service provider can use the "Report List feature" in policy routing specification to determine when a connection setup request went into the "reserved" reroute bandwidth resource partition. This notification would be used by the carrier to initiate network augments as required. The "Report Identifier list" would include the Rp-NSCs and/or Ne-NSCs that were listed in the policy used when forwarding the SETUP message and which tag the resource and/or network entity partition into which the connection was established. This feature would require the ability of a network management system to provide such reports on a scheduled interval determined by the operator.

12.3.4 Policy constraint for IXC2's network

The policy for path selection for routing calls over IXC2's facilities is defined as below:

> Policy_IXC2 ::= require (logical OR {Ne-NSC_LEC; Ne-NSC_IXC2}; logical OR {Rp-NSC_LEC_1; Rp-NSC_IXC2_1)

12.3.5 Policy constraint for IXC3's network

The policy for path selection for routing calls over IXC3 facilities, is defined as below:

> Policy_IXC3 ::= require (logical OR {Ne-NSC_LEC; Ne-NSC_IXC3}; logical OR {Rp-NSC_LEC_1; Rp-NSC_IXC3_1)

Annex A PNNI 1.1 Protocol Implementation Conformance Statement (PICS) for Policy Routing Version 1.0

A.1 Introduction

To evaluate conformance of a particular implementation, it is necessary to have a statement of which capabilities and options have been implemented. Such a statement is called a Protocol Implementation Conformance Statement (PICS).

A.1.1 Scope

This document provides the PNNI 1.1 PICS proforma for Policy Routing Version 1.0, defined in [1], in compliance with the relevant requirements, and in accordance with the relevant guidelines, given in ISO/IEC 9646-7. In most cases, statements contained in notes in the specification, which were intended as information, are not included in the PICS.

A.1.2 Normative References

[1] af-cs-0195.000, Policy Routing Version 1.0, April 2003

[2] ISO/IEC 9646-1: 1994, Information technology – Open systems interconnection – Conformance testing methodology and framework – Part 1: General Concepts (See also ITU Recommendation X.290 (1995)).

[3] ISO/IEC 9646-7: 1995, Information technology – Open systems interconnection – Conformance testing methodology and framework – Part 7: Implementation Conformance Statements (See also ITU Recommendation X.296 (1995)).

[4] ISO/IEC 9646-3:1998, Information technology – Open systems interconnection – Conformance testing methodology and interconnection – Part 3: The Tree and Tabular Combined Notation (TTCN) (See also ITU telecommunication X.292 (1998)).

[5] af-pnni-0055.002, Private Network-Network Interface Specification Version 1.1 (PNNI 1.1) – April 2002

A.1.3 Definitions

Terms defined in [1] and [5]

Terms defined in ISO/IEC 9646-1 and in ISO/IEC 9646-7

In particular, the following terms defined in ISO/IEC 9646-1 apply:

Protocol Implementation Conformance Statement (PICS): A statement made by the supplier of an implementation or system, stating which capabilities have been implemented for a given protocol.

PICS proforma: A document, in the form of a questionnaire, designed by the protocol specifier or conformance test suite specifier, which when completed for an implementation or system becomes the PICS.

A.1.4 Acronyms

ASN.1 Abstract Syntax Notation One
ATS Abstract Test Suite
IUT Implementation Under Test
PICS Protocol Implementation Conformance Statement
SUT System Under Test

A.1.5 Conformance

The PICS does not modify any of the requirements detailed in Policy Routing Version 1.0. In case of apparent conflict between the statements in the base specification and in the annotations of "M" (mandatory) and "O" (optional) in the PICS, the text of the base specification takes precedence.

The supplier of a protocol implementation, which is claimed to conform to the PNNI component of the ATM Forum Policy Routing Version 1.0, is required to complete a copy of the PICS proforma provided in this document and is required to provide the information necessary to identify both the supplier and the implementation.

A.2 Identification of the Implementation

Identification of the Implementation Under Test (IUT) and system in which it resides (the System Under Test (SUT)) should be filled in so as to provide as much detail as possible regarding version numbers and configuration options.

The product supplier information and client information should both be filled in if they are different.

A person who can answer queries regarding information supplied in the PICS should be named as the contact person.

A.2.1 Date of Statement

_____

A.2.2 Implementation Under Test (IUT) Identification

IUT Name: _____

_____

_____

IUT Version: _____

A.2.3 System Under Test (SUT) Identification

SUT Name: _____

_____

Hardware Configuration: _____

_____

_____

Operating System: _____

A.2.4 Product Supplier

Name: _____

Address: _____

_____

_____

Telephone Number: _____

Facsimile Number: _____

Email Address:_____

Additional Information: _____

_____

_____

A.2.5 Client

Name: _____

Address: _____

_____

_____

Telephone Number: _____

Facsimile Number: _____

Email Address:_____

Additional Information: _____

_____

_____

A.2.6 PICS Contact Person

(A person to contact if there are any queries concerning the content of the PICS)

Name: _____

Telephone Number: _____

Facsimile Number: _____

Email Address:_____

Additional Information: _____

Identification of the Protocol Specification

This PICS proforma applies to the following specification:

[1] af-cs-0195.000, Policy Routing Version 1.0, April 2003

A.3 PICS Proforma

A.3.1 Global statement of conformance

The implementation described in this PICS meets all of the mandatory requirements of the reference protocol.

[ ] YES
[ ] NO

Note: Answering "No" indicates non-conformance to the specified protocol. Non-supported mandatory capabilities are to be identified in the following tables, with an explanation by the implementor explaining why the implementation is non-conforming.

A.3.2 Instructions for Completing the PICS Proforma

The PICS Proforma is a fixed-format questionnaire. Answers to the questionnaire should be provided in the rightmost columns, either by simply indicating a restricted choice (such as Yes or No), or by entering a value or a set of range of values.

The following notations, defined in ISO/IEC 9647-7, are used for the support column:
Yes supported by the implementation
No not supported by the implementation

The following notations, defined in ISO/IEC 9647-7, are used for the status column:
M mandatory – the capability is required to be supported.
O optional – the capability may be supported or not.
O.i qualified optional – for mutually exclusive or selectable options from a set. “i” is an integer which identifies a unique group of related optional items and the logic of their selection is defined immediately following the table.

A supplier may also provide additional information, categorised as exceptional or supplementary information. These additional information should be provided as items labeled X.<i> for exceptional information, or S.<i> for supplemental information, respectively, for cross reference purposes, where <i> is any unambiguous identification for the item. The exception and supplementary information are not mandatory and the PICS is complete without such information. The presence of optional supplementary or exception information should not affect test execution, and will in no way affect interoperability verification. The column labeled ‘Reference’ gives a pointer to sections of the protocol specification for which the PICS Proforma is being written.

A.4 PICS for the support of Policy Routing at the PNNI interface

A.4.1 Major Capability at PNNI (MCP)

Item Number	Item Description	Status	Condition for status	Reference	Support
MCP1	Does the IUT support Policy Routing at the PNNI interface?	M			Yes__ No__
MCP2	Does the IUT support advertising its supported Policy Version?	M		7.1	Yes__ No__
MCP3	Does the IUT support advertising at least 2 resource partitions per network element, each tagged by at least two Rp-NSCs?	M		7.1	Yes__ No__
MCP4	Does the IUT support advertising network elements tagged by at least 2 Ne-NSCs?	M		7.1	Yes__ No__
MCP5	Does the IUT support the "Tagged by all Rp-NSCs" information group flag, as defined in Section 7.1.3?	M		7.1	Yes__ No__
MCP6	Does the IUT support Policy Routing for a switched virtual channel connection (SVCC) ?	M		1.1	Yes__ No__
MCP7	Does the IUT support Policy Routing for a switched virtual path connection (SVPC) ?	M		1.1	Yes__ No__
MCP8	Does the IUT support Policy Routing for a soft PVCC?	M	OPT_7/[5]	1.1	Yes__ No__
MCP9	Does the IUT support Policy Routing for a soft PVPC?	M	OPT_7/[5]	1.1	Yes__ No__
MCP10	Does the IUT support the origination of a soft PVCC with a policy constraint?	M	OPT_7/[5]	1.1	Yes__ No__
MCP11	Does the IUT support the origination of a soft PVPC with a policy constraint?	M	OPT_7/[5]	1.1	Yes__ No__
MCP12	Does the IUT support processing up to 6 Policies received in a Policy constraint information element?	M		7.2	Yes__ No__
MCP13	Does the IUT support the "must avoid" policy operator?	M		7.2	Yes__ No__
MCP14	Does the IUT support the "require" policy operator?	M		7.2	Yes__ No__
MCP15	Does the IUT support Ne-NSC identifiers in policies?	M		7.2	Yes__ No__
MCP16	Does the IUT support Rp-NSC identifiers in policies?	M		7.2	Yes__ No__
MCP17	Does the IUT support the policy information report capability?	M		7.2	Yes__ No__
Comments:					

A.4.2 Subsidiary Capabilities at PNNI (SCP)

Item Number	Item Description	Status	Condition for status	Reference	Support
SCP1	Does the IUT support policy routing for the establishment of point-to-point connections?	M		7.2.3	Yes__ No__
SCP2	Does the IUT support policy routing for the establishment of point-to-multipoint connections?	M		7.2.4	Yes__ No__
Comments:					

A.4.3 Routing Procedures at the PNNI (RPP)

Item Number	Item Description	Status	Condition for status	Reference	Support
RPP1	Does the IUT support the advertisement of the Policy Version information group within the Nodal information group?	M		7.1	Yes__No__
RPP2	Does the IUT support the advertisement of the Ne-NSC Identifiers information group within the Uplink information attribute IG?	M N/A	SS_B/[5] NOT SS_B/[5]	7.1.1.1	Yes__No__
RPP3	Does the IUT support the advertisement of the Ne-NSC Identifiers information group within the Nodal State parameters IG?	M N/A	SS_P/[5] NOT SS_P/[5]	7.1.1.1	Yes__No__
RPP4	Does the IUT support the advertisement of the Ne-NSC Identifiers information group within the Internal reachable ATM addresses IG?	M		7.1.1.1	Yes__No__
RPP5	Does the IUT support the advertisement of the Ne-NSC Identifiers information group within the Exterior reachable ATM addresses IG?	M		7.1.1.1	Yes__No__
RPP6	Does the IUT support the advertisement of the Ne-NSC Identifiers information group within the Horizontal links IG?	M		7.1.1.1	Yes__No__
RPP7	Does the IUT support the advertisement of the Ne-NSC Identifiers information group within the Uplinks IG?	M N/A	SS_B/[5] NOT SS_B/[5]	7.1.1.1	Yes__No__
RPP8	Does the IUT support the advertisement of Resource Partition information groups within the Uplink information attribute IG?	M N/A	SS_B/[5] NOT SS_B/[5]	7.1.1.1	Yes__No__
RPP9	Does the IUT support the advertisement of Resource Partition information groups within the Nodal State parameters IG?	M N/A	SS_P/[5] NOT SS_P/[5]	7.1.1.1	Yes__No__

Item Number	Item Description	Status	Condition for status	Reference	Support
RPP10	Does the IUT support the advertisement of Resource Partition information groups within the Internal reachable ATM addresses IG?	M		7.1.1.1	Yes__No__
RPP11	Does the IUT support the advertisement of Resource Partition information groups within the Exterior reachable ATM addresses IG?	M		7.1.1.1	Yes__No__
RPP12	Does the IUT support the advertisement of Resource Partition information groups within the Horizontal links IG?	M		7.1.1.1	Yes__No__
RPP13	Does the IUT support the advertisement of Resource Partition information groups within the Uplinks IG?	M N/A	SS_B/[5] NOT SS_B/[5]	7.1.1.1	Yes__No__
RPP14	Does the IUT support the advertisement of Outgoing resource availability IGs within a Resource Partition information group?	M		7.1.1.1	Yes__No__
RPP15	Does the IUT support the advertisement of Incoming resource availability IGs within a Resource Partition information group?	M		7.1.1.1	Yes__No__
RPP16	Does the IUT ignore a Ne-NSC Identifiers IG advertised by a node that is not advertising a Policy Version IG in its Nodal IG?	M		7.1.2.1	Yes__No__
RPP17	Is the IUT capable of advertising multiple Ne-NSC identifiers within a Ne-NSC Identifiers IG?	M		7.1.2.1	Yes__No__
RPP18	Does the IUT set the information group tags of all Ne-NSC Identifiers IG it advertises to all zeroes?	M		7.1.2.1	Yes__No__
RPP19	Does the IUT never advertise a Ne-NSC Identifier equal to 0 ?	M		7.1.2.1	Yes__No__
RPP20	Is the IUT capable of advertising multiple Rp-NSC identifiers within a Resource Partition IG?	M		7.1.2.2	Yes__No__
RPP21	Does the IUT never advertise a Rp-NSC Identifier equal to 0 ?	M		7.1.2.2	Yes__No__
RPP22	Does the IUT follow the PNNI 1.1 rules governing how RAIGs are included in reachable ATM addresses, horizontal link, uplink, nodal state parameters, or ULIA IGs, for RAIGs within a given Resource Partition IG?	M		7.1.2.2	Yes__No__
RPP23	During state significant computations and path computations, does the IUT ignore a Resource Partition IG advertised by a node that is not advertising a Policy Version IG in its Nodal IG?	M		7.1.2.2	Yes__No__

Item Number	Item Description	Status	Condition for status	Reference	Support
RPP24	Does the IUT set the information group tags of all Resource Partition IG it advertises to all zeroes?	M		7.1.2.2	Yes__No__
RPP25	Does the IUT, at the lowest level, advertise the highest supported policy version in its Policy Version IG?	M		7.1.2.3	Yes__No__
RPP26	Is the policy version advertised by the IUT, as a logical group node, configurable?	M N/A	SS_P/[5] NOT SS_P/[5]	7.1.2.3	Yes__No__
RPP27	By default, is the policy version advertised by the IUT, as a logical group node, the lowest of the policy versions advertised within its child peer group?	M N/A	SS_P/[5] NOT SS_P/[5]	7.1.2.3	Yes__No__
RPP28	By default, does the IUT, as a logical group node, advertise a Policy Version IG only if all nodes within its child peer group each advertise a Policy Version IG?	M N/A	SS_P/[5] NOT SS_P/[5]	7.1.2.3	Yes__No__
RPP29	When not advertising a Policy Version IG, does the IUT not advertise any Ne-NSC Identifiers IGs nor Resource Partition IGs?	M		7.1.2.3	Yes__No__
RPP30	When not advertising a Policy Version IG, does the IUT not set the “Tagged by all Rp-NSCs” flag in any information group it advertises?	M		7.1.2.3	Yes__No__
RPP31	When receiving a Nodal IG containing multiple Policy Version IGs, does the IUT only consider the first occurrence?	M		7.1.2.3	Yes__No__
RPP32	Does the IUT set the information group tags of a Policy Version IG it advertises to all zeroes?	M		7.1.2.3	Yes__No__
RPP33	When receiving an advertisement with its “Tagged by all Rp-NSCs” flag set to one, does the IUT consider the resources that are associated with that advertisement and are not contained in a specific resource partition both as bare resources and as resources tagged by all Rp-NSCs?	M		7.1.3	Yes__No__
RPP34	When receiving an IG that contains a Resource Partition IG and has its “Tagged by all Rp-NSCs” flag set to one, does the IUT consider the resources advertised within the resource partition to only be tagged by the Rp-NSCs explicitly listed in that Resource Partition IG, while other resources are considered as both bare and tagged by all Rp-NSCs?	M		7.1.3	Yes__No__

Item Number	Item Description	Status	Condition for status	Reference	Support
RPP35	Does the IUT ignore the setting of the "Tagged by all Rp-NSCs" flag in information groups advertised by a node that is not advertising a Policy Version IG?	M		7.1.3	Yes__No__
RPP36	Does the IUT treat as a significant change to the containing IG a change: • of a contained Policy Version IG, or • of the setting of the "Tagged by all Rp-NSCs" flag, or • of a contained Ne-NSC Identifiers IG, or • of a contained Resource Partition IG	M		7.1.4	Yes__No__
RPP37	Does the IUT perform Policy information aggregation when advertising one of the following : • Outside links and uplinks that are to be aggregated by a border node that supports Policy Routing • Links between logical group nodes that are to be aggregated by a logical group node advertising support for Policy Routing • The radius or an exception for a logical group node advertising support for Policy Routing • Reachability information that results of address summarization	M N/A	SS_P/[5] NOT SS_P/[5]	7.1.5.2	Yes__ No__
Comments:					

A.4.4 Path Selection with Policy Routing (PSPR)

Item Number	Item Description	Status	Condition for status	Reference	Support
PSPR1	When performing path selection for a connection with no policy constraint, does the IUT consider only bare resources?	M		6.1	Yes__ No__
PSPR2	For a connection with no policy constraint, when no acceptable path exists, does the IUT crankback the connection?	O		6.1	Yes__ No__
PSPR3	When performing path selection for a connection with a policy constraint containing a single policy, does the IUT prune its topological map of the PNNI routing domain, leaving only the network entities and resources that match the policy?	M		6.2	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
PSPR4	When performing path selection using a given policy, does the IUT ensure that nodes along the path of the connection understand (or can safely ignore) that policy?	M		6.2	Yes__ No__
PSPR5	When performing path selection using a policy that uses a syntax of policy version "x", does the IUT ensure that nodes along the path of the connection all advertise a supported policy version of "x" or higher in their Policy Version IG?	M		6.2	Yes__ No__
PSPR6	Does the IUT always consider resources associated with a reachable ATM addresses advertisements (either internal or exterior) that: • has it "tagged by all Rp-NSCs" flag set to zero, and • does not contain a Ne-NSC Identifiers IG, and • does not contain a Resource Partition IG, regardless of the policy used to select a path?	M		6.2	Yes__ No__
PSPR7	For a connection with a policy constraint containing a single policy, when no acceptable path that satisfies the policy exists, does the IUT crankback the call?	O		6.2	Yes__ No__
PSPR8	Does the IUT consider only resources tagged at least by NSC_1 when performing path selection for a connection with the policy "require (single {NSC_1})"?	M		6.2.1.1	Yes__ No__
PSPR9	Does the IUT consider only bare resources of network entities that are not tagged by Ne-NSC_1, when performing path selection for a connection with the policy "must avoid (single {Ne-NSC_1})"?	M		6.2.1.2	Yes__ No__
PSPR10	When performing path selection for a connection with a policy "require (logical OR {list of Ne-NSCs})", does the IUT consider only the bare resources of network entities that are tagged at least by any one or any combination of the listed Ne-NSCs, ?	M		6.2.2.1	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
PSPR11	When performing path selection for a connection with a policy "require (logical OR {list of Rp-NSCs})", does the IUT consider only the resources in resource partitions that are tagged at least by any one or any combination of the listed Rp-NSCs ?	M		6.2.2.2	Yes__ No__
PSPR12	When performing path selection for a connection with a policy "require (logical OR {list of Rp-NSCs})" where Rp-NSC_Bare is part of the list of Rp-NSCs, does the IUT also consider bare resources?	M		6.2.2.2	Yes__ No__
PSPR13	When performing path selection for a connection with a policy "require (logical AND {list of Ne-NSCs})", does the IUT only consider bare resources of network entities that are tagged by at least all the listed Ne-NSCs?	M		6.2.2.3	Yes__ No__
PSPR14	When performing path selection for a connection with a policy "require (logical AND {list of Rp-NSCs})", does the IUT only consider the resources in resource partitions that are tagged by at least all the listed Rp-NSCs?	M		6.2.2.4	Yes__ No__
PSPR15	If Rp-NSC_Bare is included in the list of Rp-NSCs of a policy "require (logical AND {list of Rp-NSCs})", does the IUT treat the policy as an unrecognized Policy octet group, as defined in Section 10?	M		6.2.2.4	Yes__ No__
PSPR16	When performing path selection for a connection with a "require" policy containing a list of Rp-NSCs and a list of Ne-NSCs, does the IUT only consider the resources of resource partitions that match the "require" policy on the list of Rp-NSCs, within network entities that match the "require" policy on the list of Ne-NSCs?	M		6.2.2.5	Yes__ No__
PSPR17	When performing path selection for a connection with a policy "must avoid (logical OR {list of Ne-NSCs})", does the IUT consider only the bare resources of network entities that are not tagged by any one of the listed Ne-NSCs?	M		6.2.3.1	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
PSPR18	When performing path selection for a connection with a policy "must avoid (logical AND {list of Ne-NSCs})", does the IUT consider only the bare resources of network entities that are not tagged by all the listed Ne-NSCs?	M		6.2.3.2	Yes__ No__
PSPR19	When performing path selection for a connection with a policy containing both "require" and "must avoid" operators, does the IUT consider only resources that satisfy both policy operators at the same time?	M		6.2.4	Yes__ No__
PSPR20	Does the IUT consider a policy constraint containing multiple policies as an ordered list of policies, the policy appearing first is the most desirable, while the policy appearing last is the least desirable?	M		6.3	Yes__ No__
PSPR21	When performing path selection for a connection with a policy constraint containing multiple policies, does the IUT first attempt to find a path using the first recognized policy, and if no such path exists, does it attempt to find a path using the next recognized policy in the list, and keeps trying with the next policy until it either finds an acceptable path of reaches the end of the list?	M		6.3	Yes__ No__
PSPR22	When performing path selection for a connection with a policy constraint containing multiple policies, if no acceptable path matching any one of the listed policies is found, does the IUT crankback the connection?	O		6.3	Yes__ No__
PSPR23	Does the IUT select the local link over which to forward a connection according to the procedures of Sections 6.2 and 6.3?	M		6.4	Yes__ No__
PSPR24	During actual CAC, does the IUT select the resource partition in which to establish a connection with a policy constraint according to the procedures related to Rp-NSCs in Sections 6.2 and 6.3?	M		6.4	Yes__ No__
PSPR25	When performing alternate path selection for a crankbacked connection with a policy constraint, does the IUT follow the procedures of Sections 6.2 and 6.3?	M		6.5	Yes__ No__
Comments:					

A.4.5 Encoding at the PNNI (EP)

Item Number	Item Description	Status	Condition for status	Reference	Support
EP1	Does the IUT support the Policy constraint information element as defined in Section 5.1?	M		5.1	Yes__ No__
EP2	Does the IUT support the maximum length of Policy constraint information element of 253 octets?	M		7.2.1	Yes__ No__
EP3	Does the IUT support the Policy constraint information element in the CONNECT message?	M		7.2.1.1	Yes__ No__
EP4	Does the IUT support the Policy constraint information element in the SETUP message?	M		7.2.1.2	Yes__ No__
EP5	Does the IUT support the Policy constraint information element in the ADD PARTY message?	M		7.2.1.3	Yes__ No__
EP6	Does the IUT support the Policy constraint information element in the ADD PARTY ACKNOWLEDGE message?	M		7.2.1.4	Yes__ No__
EP7	Does the IUT consider “valid” a Policy constraint information element that meets the conditions defined in Section 10?	M		5.1	Yes__ No__
EP8	Does the IUT support the new crankback cause # 192 “unrecognized policy constraint”?	M		7.2.2	Yes__ No__
Comments:					

A.4.6 Signalling Procedures for Point to Point Connections at the PNNI (SPP)

Item Number	Item Description	Status	Condition for status	Reference	Support
SPP1	When at the preceding side, for a setup request that contains a policy constraint, does the IUT perform resource selection over the interface as specified in Section 6.4?	M		7.2.3.1	Yes__ No__
SPP2	When progressing a connection, does the IUT include the Policy constraint received from a previous PNNI interface unchanged in the SETUP message sent to the succeeding side?	M		7.2.3.1	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SPP3	When at the preceding side, if the IUT receives a CONNECT message that contains a Policy constraint information element with valid content, and the SETUP message it forwarded did not contain any report request, does the IUT forward the received Policy constraint information element unchanged to call control?	M		7.2.3.1	Yes__ No__
SPP4	When at the preceding side, if the IUT receives a CONNECT message that contains a Policy constraint information element with valid content, and: • the SETUP message it forwarded contained a valid report request, • the SETUP message was not forwarded using a policy with a "require" policy operator, and • this interface is not tagged with any Ne-NSCs, then does the IUT forward the received Policy constraint information element unchanged to call control?	M		7.2.3.1	Yes__ No__
SPP5	If the SETUP message forwarded by the IUT contained an unrecognized report request, does the IUT include a report gap, if one is not already present, in the Policy constraint information element contained in the connect indication sent to call control?	M		7.2.3.1	Yes__ No__
SPP6	If the IUT receives a CONNECT message containing a Policy constraint information element with invalid content (as defined in Section 10), does the IUT replace the Policy constraint information element with one containing a Report octet group with a report gap, as specified in Section 7.2.3.1?	M		7.2.3.1	Yes__ No__
SPP7	If the IUT forwarded a SETUP message using a "require" policy operator containing a Rp-NSC list, and the SETUP message contained a report request set to either "Report all required NSCs", "Report required Rp-NSCs", or "Report all Ne-NSCs and required Rp-NSCs", does the IUT make sure that the connect indication sent to call control contains a Rp-NSC report list?	M		7.2.3.1	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SPP8	If the IUT forwarded a SETUP message using a "require" policy operator containing a Ne-NSC list, and the SETUP message contained a report request set to either "Report all required NSCs" or "Report required Ne-NSCs", does the IUT make sure that the connect indication sent to call control contains a Ne-NSC report list?	M		7.2.3.1	Yes__ No__
SPP9	If this interface is tagged with at least one Ne-NSC, and the SETUP message contained a report request set to either "Report all Ne-NSCs" or "Report all Ne-NSCs and required Rp-NSCs", does the IUT make sure that the connect indication sent to call control contains a Ne-NSC report list?	M		7.2.3.1	Yes__ No__
SPP10	When a Rp-NSC report list is present in a connect indication, does the IUT update its contents as specified in Section 7.2.3.1?	M		7.2.3.1	Yes__ No__
SPP11	When a Ne-NSC report list is present in a connect indication, does the IUT update its contents as specified in Section 7.2.3.1?	M		7.2.3.1	Yes__ No__
SPP12	When processing a Rp-NSC report list in a connect indication, does the IUT make sure that the Rp-NSC report list does not contain multiple instances of the same Rp-NSC identifier?	M		7.2.3.1	Yes__ No__
SPP13	When processing a Ne-NSC report list in a connect indication, does the IUT make sure that the Ne-NSC report list does not contain multiple instances of the same Ne-NSC identifier?	M		7.2.3.1	Yes__ No__
SPP14	If the IUT forwarded the SETUP message using bare resources and the connect indication contains a Rp-NSC report list, does the IUT make sure that the Rp-NSC report list contains Rp-NSC_Bare?	M		7.2.3.1	Yes__ No__
SPP15	If, as a result of compiling a report, the length of the Policy constraint information element included in the connect indication would exceed this information element's maximum length minus two octets, does the IUT include a report gap if one is not already present?	M		7.2.3.1	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SPP16	When at the succeeding side, if a received SETUP message contains a Policy constraint information element with content error (as defined in Section 10), the pass along request field set to "no pass along request and the action indicator set to "clear call", does the IUT crankback the connection with cause #100 "invalid information element contents", a diagnostic field set to the Policy constraint information element identifier and a crankback cause #192 "unrecognized policy constraint"?	M		7.2.3.2	Yes__ No__
SPP17	When at the succeeding side, if the received SETUP message contains a valid Policy constraint information element (as defined in Section 10) and the connection is progressed, does the IUT forward the Policy constraint information element unchanged?	M		7.2.3.2	Yes__ No__
SPP18	Whenever path, local link and resource selection occur for a received SETUP message that contains a policy constraint, does the IUT take the policy constraint into account as specified in Sections 6.2, 6.3, 6.4?	M		7.2.3.2	Yes__ No__
SPP19	When at the succeeding side, if the IUT receives a connect request that contains a Policy constraint information element with valid content, and the SETUP message it received did no contain any report request; does the IUT forward the received Policy constraint information element unchanged in the CONNECT message sent to the preceding side?	M		7.2.3.2	Yes__ No__
SPP20	When at the succeeding side, if the IUT receives a connect request that contains a Policy constraint information element with valid content, and: • the SETUP message it received contained a valid report request, • the resources at this interface were not selected using a "require" policy, and • this interface is not tagged with any Ne-NSCs, then does the IUT forward the received Policy constraint information element unchanged in the CONNECT message sent to the preceding side?	M		7.2.3.2	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SPP21	If the SETUP message received by the IUT contained an unrecognized report request, does the IUT include a report gap, if one is not already present, in the Policy constraint information element contained in the CONNECT message sent to the preceding side?	M		7.2.3.2	Yes__ No__
SPP22	When at the succeeding side, if the IUT receives a connect request containing a Policy constraint information element with invalid content (as defined in Section 10), does the IUT replace the Policy constraint information element with one containing a Report octet group with a report gap?	M		7.2.3.2	Yes__ No__
SPP23	If the IUT established the connection at this interface using a "require" policy operator containing a Rp-NSC list, and the received SETUP message contained a report request set to either "Report all required NSCs", "Report required Rp-NSCs", or "Report all Ne-NSCs and required Rp-NSCs", does the IUT make sure that the CONNECT message sent to the preceding side contains a Rp-NSC report list?	M		7.2.3.2	Yes__ No__
SPP24	If the IUT established the connection at this interface using a "require" policy operator containing a Ne-NSC list, and the received SETUP message contained a report request set to either "Report all required NSCs" or "Report required Ne-NSCs", does the IUT make sure that the CONNECT message sent to the preceding side contains a Ne-NSC report list?	M		7.2.3.2	Yes__ No__
SPP25	If this interface is tagged with at least one Ne-NSC, and the received SETUP message contained a report request set to either "Report all Ne-NSCs" or "Report all Ne-NSCs and required Rp-NSCs", does the IUT make sure that the CONNECT message sent to the preceding side contains a Ne-NSC report list?	M		7.2.3.2	Yes__ No__
SPP26	When a Rp-NSC report list is present in a CONNECT message, does the IUT update its contents as specified in Section 7.2.3.2?	M		7.2.3.2	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SPP27	When a Ne-NSC report list is present in a CONNECT message, does the IUT update its contents as specified in Section 7.2.3.2?	M		7.2.3.2	Yes__ No__
SPP28	When processing a Rp-NSC report list in a CONNECT message to be sent to the preceding side, does the IUT make sure that the Rp-NSC report list does not contain multiple instances of the same Rp-NSC identifier?	M		7.2.3.2	Yes__ No__
SPP29	When processing a Ne-NSC report list in a CONNECT message to be sent to the preceding side, does the IUT make sure that the Ne-NSC report list does not contain multiple instances of the same Ne-NSC identifier?	M		7.2.3.2	Yes__ No__
SPP30	If the IUT established the connection in bare resources at this interface and the CONNECT message to be sent to the preceding side contains a Rp-NSC report list, does the IUT make sure that the Rp-NSC report list contains Rp-NSC_Bare?	M		7.2.3.2	Yes__ No__
SPP31	If, as a result of compiling a report, the length of the Policy constraint information element included in the CONNECT message would exceed the maximum length minus two octets, does the IUT include a report gap if one is not already present?	M		7.2.3.2	Yes__ No__
Comments:					

A.4.7 Signalling Procedures for Point to Multipoint Connections at the PNNI (SPMP)

Item Number	Item Description	Status	Condition for status	Reference	Support
SPMP1	When the IUT translates a received ADD PARTY message into an outgoing SETUP message, does it include the Policy constraint information element from the ADD PARTY message unchanged in the SETUP message?	M		7.2.4.1	Yes__ No__
SPMP2	When the IUT translates a received connect indication into an add party acknowledge request for the previous interface, does it include the Policy constraint information element from the connect indication unchanged in the add party acknowledge request?	M		7.2.4.1	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SPMP3	When at the succeeding side, if the IUT receives an ADD PARTY message containing a Policy constraint information element with content error (as defined in Section 10), the pass along request field set to “no pass along request” and the action indicator set to “clear call”, does the IUT crankback the party by sending an ADD PARTY REJECT message with cause #100, "invalid information element contents", with a diagnostic field set to the Policy constraint information element identifier and a crankback cause set to cause #192 "unrecognized policy constraint"?	M		7.2.4.3	Yes__ No__
SPMP4	When at the succeeding side, whenever path selection occurs for an ADD PARTY message that contains a policy constraint, does the IUT consider that resources supporting the existing connection tree match all policies?	M		7.2.4.3	Yes__ No__
SPMP5	When at the succeeding side, whenever path selection occurs for an ADD PARTY message that contains a policy constraint, does the IUT take the policy constraint into account as specified in Section 6.2 and 6.3 to select a path from the branching point to the called party?	M		7.2.4.3	Yes__ No__
Comments:					

A.4.8 Compatibility with nodes not supporting Policy Routing at the PNNI (COMPP)

Item Number	Item Description	Status	Condition for status	Reference	Support
COMPP1	Does the IUT support setting the Policy constraint information element IE instruction field on a connection by connection basis?	M		7.2.5	Yes__ No__
COMPP2	If the IUT originates a Policy constraint information element within a SETUP or ADD PARTY message that allows routing on untagged resources, does the IUT: • set the IE instruction field flag to "follow explicit instructions", • set the action indicator to "discard information element and proceed" or "discard information element, proceed, and report status", and • set the pass along request field set to "pass along request"?	M		7.2.5	Yes__ No__
COMPP3	If a Policy constraint information element within a SETUP or ADD PARTY message that allows routing on untagged resources is received from a UNI, does the IUT: • set the IE instruction field flag to "follow explicit instructions", • set the action indicator to "discard information element and proceed" or "discard information element, proceed, and report status" and • set the pass along request field set to "pass along request"?	M		7.2.5	Yes__ No__
COMPP4	If the IUT originates a Policy constraint information element within a SETUP or ADD PARTY message that does not allow routing on untagged resources, does the IUT: • set the IE instruction field flag to "follow explicit instructions", • set the action indicator to "clear call", and • set the pass along request field set to "no pass along request"?	M		7.2.5	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
COMPP5	If a Policy constraint information element within a SETUP or ADD PARTY message that does not allow routing on untagged resources is received from a UNI, does the IUT: • set the IE instruction field flag to "follow explicit instructions", • set the action indicator to "clear call", and • set the pass along request field set to "no pass along request"?	M		7.2.5	Yes__ No__
COMPP6	When receiving a Policy constraint information element from a PNNI or an AINI, does the IUT not change the IE instruction field?	M		7.2.5	Yes__ No__
COMPP7	When a Policy constraint information element is contained in a CONNECT or ADD PARTY ACKNOWLEDGE message, does the IUT: • set the IE instruction field flag to "follow explicit instructions", • set the action indicator to "discard information element and proceed" or "discard information element, proceed, and report status", and • set the pass along request field set to "pass along request"?	M		7.2.5	Yes__ No__
Comments:					

Annex B AINI 1.1 Protocol Implementation Conformance Statement (PICS) for Policy Routing Version 1.0

B.1 Introduction

To evaluate conformance of a particular implementation, it is necessary to have a statement of which capabilities and options have been implemented. Such a statement is called a Protocol Implementation Conformance Statement (PICS).

B.1.1 Scope

This document provides the AINI 1.1 PICS proforma for Policy Routing Version 1.0, defined in [1], in compliance with the relevant requirements, and in accordance with the relevant guidelines, given in ISO/IEC 9646-7. In most cases, statements contained in notes in the specification, which were intended as information, are not included in the PICS.

B.1.2 Normative References

[1] af-cs-0195.000, Policy Routing Version 1.0, April 2003

[2] ISO/IEC 9646-1: 1994, Information technology – Open systems interconnection – Conformance testing methodology and framework – Part 1: General Concepts (See also ITU Recommendation X.290 (1995)).

[3] ISO/IEC 9646-7: 1995, Information technology – Open systems interconnection – Conformance testing methodology and framework – Part 7: Implementation Conformance Statements (See also ITU Recommendation X.296 (1995)).

[4] ISO/IEC 9646-3:1998, Information technology – Open systems interconnection – Conformance testing methodology and interconnection – Part 3: The Tree and Tabular Combined Notation (TTCN) (See also ITU telecommunication X.292 (1998)).

B.1.3 Definitions

Terms defined in [1]

Terms defined in ISO/IEC 9646-1 and in ISO/IEC 9646-7

In particular, the following terms defined in ISO/IEC 9646-1 apply:

Protocol Implementation Conformance Statement (PICS): A statement made by the supplier of an implementation or system, stating which capabilities have been implemented for a given protocol.

PICS proforma: A document, in the form of a questionnaire, designed by the protocol specifier or conformance test suite specifier, which when completed for an implementation or system becomes the PICS.

B.1.4 Acronyms

ASN.1 Abstract Syntax Notation One
ATS Abstract Test Suite
IUT Implementation Under Test
PICS Protocol Implementation Conformance Statement
SUT System Under Test

B.1.5 Conformance

The PICS does not modify any of the requirements detailed in the Policy Routing Version 1.0. In case of apparent conflict between the statements in the base specification and in the annotations of "M" (mandatory) and "O" (optional) in the PICS, the text of the base specification takes precedence.

The supplier of a protocol implementation, which is claimed to conform to the AINI component of the ATM Forum Policy Routing Version 1.0, is required to complete a copy of the PICS proforma provided in this document and is required to provide the information necessary to identify both the supplier and the implementation.

B.2 Identification of the Implementation

Identification of the Implementation Under Test (IUT) and system in which it resides (the System Under Test (SUT)) should be filled in so as to provide as much detail as possible regarding version numbers and configuration options.

The product supplier information and client information should both be filled in if they are different.

A person who can answer queries regarding information supplied in the PICS should be named as the contact person.

B.2.1 Date of Statement

_____

B.2.2 Implementation Under Test (IUT) Identification

IUT Name: _____

_____

_____

IUT Version: _____

B.2.3 System Under Test (SUT) Identification

SUT Name: _____

_____

Hardware Configuration: _____

_____

_____

Operating System: _____

B.2.4 Product Supplier

Name: _____

Address: _____

_____

_____

Telephone Number: _____

Facsimile Number: _____

Email Address:_____

Additional Information: _____

_____

_____

B.2.5 Client

Name: _____

Address: _____

_____

_____

Telephone Number: _____

Facsimile Number: _____

Email Address:_____

Additional Information: _____

_____

_____

B.2.6 PICS Contact Person

(A person to contact if there are any queries concerning the content of the PICS)

Name: _____

Telephone Number: _____

Facsimile Number: _____

Email Address:_____

Additional Information: _____

Identification of the Protocol Specification

This PICS proforma applies to the following specification:

[1] af-cs-0195.000, Policy Routing Version 1.0, April 2003

B.3 PICS Proforma

B.3.1 Global statement of conformance

The implementation described in this PICS meets all of the mandatory requirements of the reference protocol.

[ ] YES
[ ] NO

Note: Answering "No" indicates non-conformance to the specified protocol. Non-supported mandatory capabilities are to be identified in the following tables, with an explanation by the implementor explaining why the implementation is non-conforming.

B.3.2 Instructions for Completing the PICS Proforma

The PICS Proforma is a fixed-format questionnaire. Answers to the questionnaire should be provided in the rightmost columns, either by simply indicating a restricted choice (such as Yes or No), or by entering a value or a set of range of values.

The following notations, defined in ISO/IEC 9647-7, are used for the support column:
Yes supported by the implementation
No not supported by the implementation

The following notations, defined in ISO/IEC 9647-7, are used for the status column:
M mandatory – the capability is required to be supported.
O optional – the capability may be supported or not.
O.i qualified optional – for mutually exclusive or selectable options from a set. “i” is an integer which identifies a unique group of related optional items and the logic of their selection is defined immediately following the table.

A supplier may also provide additional information, categorised as exceptional or supplementary information. These additional information should be provided as items labeled X.<i> for exceptional information, or S.<i> for supplemental information, respectively, for cross reference purposes, where <i> is any unambiguous identification for the item. The exception and supplementary information are not mandatory and the PICS is complete without such information. The presence of optional supplementary or exception information should not affect test execution, and will in no way affect interoperability verification. The column labeled ‘Reference’ gives a pointer to sections of the protocol specification for which the PICS Proforma is being written.

B.4 PICS for the support of Policy routing at the AINI interface

B.4.1 Major Capability at the AINI interface (MCA)

Item Number	Item Description	Status	Condition for status	Reference	Support
MCA1	Does the IUT support Policy Routing at the AINI interface?	M			Yes__ No__
MCA2	Does the IUT support the Policy Routing procedures for point to multipoint connections?	M	Note 1	1.1	Yes__ No__
MCA3	Does the IUT support Policy Routing for a switched virtual channel connection (SVCC) ?	M		1.1	Yes__ No__
MCA4	Does the IUT support Policy Routing for a switched virtual path connection (SVPC) ?	M		1.1	Yes__ No__
MCA5	Does the IUT support Policy Routing for a soft PVCC?	M	Note 2	1.1	Yes__ No__
MCA6	Does the IUT support Policy Routing for a soft PVPC?	M	Note 2	1.1	Yes__ No__
MCA7	Does the IUT support origination of a soft PVCC with a policy constraint?	M	Note 2	1.1	Yes__ No__
MCA8	Does the IUT support origination of a soft PVPC with a policy constraint?	M	Note 2	1.1	Yes__ No__
MCA9	Does the IUT support processing up to 6 Policies received in a Policy constraint information element?	M		8	Yes__ No__
MCA10	Does the IUT support the “must avoid” policy operator?	M		8	Yes__ No__
MCA11	Does the IUT support the “require” policy operator?	M		8	Yes__ No__
MCA12	Does the IUT support Ne-NSC identifiers in policies?	M		8	Yes__ No__
MCA13	Does the IUT support Rp-NSC identifiers in policies?	M		8	Yes__ No__
MCA14	Does the IUT support the policy information report capability?	M		8	Yes__ No__
MCA15	Does the IUT support adding a policy constraint to a connection?	O		8	Yes__ No__
MCA16	Does the IUT support replacing a received policy constraint with another for a connection?	O		8	Yes__ No__
MCA17	Does the IUT support discarding a policy constraint for a connection?	O		8	Yes__ No__
Comments: Note 1: if point to multipoint is supported. Note 2: if soft PVCCs/PVPCs are supported.					

B.4.2 Encoding at AINI (EA)

Item Number	Item Description	Status	Condition for status	Reference	Support
EA1	Does the IUT support the Policy constraint information element as defined in Section 5.1?	M		5.1	Yes__ No__
EA2	Does the IUT support the maximum length of Policy constraint information element of 253 octets?	M		8.1	Yes__ No__
EA3	Does the IUT support the Policy constraint information element in the CONNECT message?	M		8.1	Yes__ No__
EA4	Does the IUT support the Policy constraint information element in the SETUP message?	M		8.1	Yes__ No__
EA5	Does the IUT support the Policy constraint information element in the ADD PARTY message?	M	MCA2	8.1	Yes__ No__
EA6	Does the IUT support the Policy constraint information element in the ADD PARTY ACKNOWLEDGE message?	M	MCA2	8.1	Yes__ No__
EA7	If the IUT would otherwise grant a pass along request to a Policy constraint information element, does the IUT consider “valid” a Policy constraint information element that meets the conditions defined in Section 10?	M		5.1	Yes__ No__
EA8	If the IUT would otherwise reject a pass along request to a Policy constraint information element, does the IUT follow normal information element content validation rules for the Policy constraint information element?	M		5.1	Yes__ No__
EA9	Does the IUT support the new crankback cause # 192 “unrecognized policy constraint”?	M		8.1	Yes__ No__
Comments:					

B.4.3 Signalling Procedures at the AINI Preceding side for Point to Point Connections (SAPPP)

Item Number	Item Description	Status	Condition for status	Reference	Support
SAPPP1	When at the preceding side, for a setup request that contains a policy constraint, does the IUT perform resource selection over the interface using the received policy constraint as specified in Section 6.4?	M		8.2.1.1	Yes__ No__
SAPPP2	If the preceding side receives a setup request which does not contain a Policy constraint information element, is the IUT capable of including a Policy constraint information element in the SETUP message forwarded to the succeeding side, based on local configuration?	M	MCA15	8.2.1.1	Yes__ No__
SAPPP3	If the preceding side receives a setup request containing a Policy constraint information element, based on local configuration, is the IUT capable of including the received Policy constraint information element unchanged in the SETUP message forwarded to the succeeding side?	M		8.2.1.1	Yes__ No__
SAPPP4	If the preceding side receives a setup request containing a Policy constraint information element, based on local configuration, is the IUT capable of discarding the received Policy constraint information element and replacing it by another one in the SETUP message forwarded to the succeeding side?	M	MCA16	8.2.1.1	Yes__ No__
SAPPP5	If the preceding side receives a setup request containing a Policy constraint information element, based on local configuration, is the IUT capable of discarding the received Policy constraint information element and forwarding the SETUP message to the succeeding side without any policy constraint?	M	MCA17	8.2.1.1	Yes__ No__
SAPPP6	When at the preceding side, the IUT has either added or replaced the Policy constraint information element contained in the SETUP message sent to the succeeding side, does it not use that policy constraint for local resource selection?	M	SAPPP2 OR SAPPP4	8.2.1.1	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SAPPP7	If the setup request received at the preceding side did not contain any Policy constraint information element (either valid or not), does the IUT discard any Policy constraint information element that is contained in the CONNECT message?	M		8.2.1.1	Yes__ No__
SAPPP8	If the IUT replaced the Policy constraint information element in the SETUP message sent to the succeeding side, does the IUT ignore any report list that may be contained in the CONNECT message?	O	SAPPP4	8.2.1.1	Yes__ No__
SAPPP9	If the IUT receives a CONNECT message that contains a Policy constraint information element and it had sent a SETUP message without a valid Policy constraint information element, does the IUT: • ignore the received Policy constraint information element if it would otherwise reject a pass along request for a Policy constraint information element, or • include the received Policy constraint information element unchanged in the connect indication forwarded to Call Control, if it would otherwise grant a pass along request for a Policy constraint information element?	M		8.2.1.1	Yes__ No__
SAPPP10	If the IUT receives a CONNECT message that contains a Policy constraint information element and it had sent a SETUP message with a valid Policy constraint information element without a report request, does the IUT: • ignore the received Policy constraint information element if it would otherwise reject a pass along request for a Policy constraint information element, or • include the received Policy constraint information element unchanged in the connect indication forwarded to Call Control, if it would otherwise grant a pass along request for a Policy constraint information element?	M		8.2.1.1	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SAPPP11	When the IUT receives a CONNECT message that contains a Policy constraint information element with valid content, the SETUP message it forwarded contained a Policy constraint information element with a valid report request that was not added, the connection was not forwarded using a "require" policy, and this interface is not tagged with any Ne-NSCs; does the IUT forward the received Policy constraint information element unchanged to call control?	M		8.2.1.1	Yes__No__
SAPPP12	If the setup request received from call control contained an unrecognized report request, does the IUT include a report gap, if one is not already present, in the Policy constraint information element contained in the connect indication sent to call control?	M		8.2.1.1	Yes__No__
SAPPP13	If the IUT would otherwise grant a pass along request for a Policy constraint information element, and the IUT receives a CONNECT message containing a Policy constraint information element with invalid content (as defined in Section 10), does the IUT replace the Policy constraint information element with one containing a Report octet group with a report gap?	M		8.2.1.1	Yes__No__
SAPPP14	If the IUT would otherwise reject a pass along request for a Policy constraint information element, and the IUT receives a CONNECT message containing a Policy constraint information element with an unrecognized octet group (as defined in Section 10), or without a Report octet group, or with more than one Report octet group; does the IUT replace the Policy constraint information element with one containing a Report octet group with a report gap?	M		8.2.1.1	Yes__No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SAPPP15	If the IUT would otherwise grant a pass along request for a Policy constraint information element, and the IUT receives a CONNECT message containing a Policy constraint information element with valid content (as defined in Section 10) and more than one recognized Report octet group, does the IUT update (if applicable) the first recognized occurrence?	M		8.2.1.1	Yes__No__
SAPPP16	If the IUT forwarded a SETUP message using a "require" policy operator containing a Rp-NSC list, and the corresponding setup request contained a report request set to either "Report all required NSCs", "Report required Rp-NSCs", or "Report all Ne-NSCs and required Rp-NSCs", does the IUT make sure that the connect indication sent to call control contains a Rp-NSC report list?	M		8.2.1.1	Yes__No__
SAPPP17	If the IUT forwarded a SETUP message using a "require" policy operator containing a Ne-NSC list, and the corresponding setup request contained a report request set to either "Report all required NSCs" or "Report required Ne-NSCs", does the IUT make sure that the connect indication sent to call control contains a Ne-NSC report list?	M		8.2.1.1	Yes__No__
SAPPP18	If this interface is tagged with at least one Ne-NSC, and the setup request contained a report request set to either "Report all Ne-NSCs" or "Report all Ne-NSCs and required Rp-NSCs", does the IUT make sure that the connect indication sent to call control contains a Ne-NSC report list?	M		8.2.1.1	Yes__No__
SAPPP19	When a Rp-NSC report list is present in a connect indication, does the IUT update its contents as specified in Section 8.2.1.1?	M		8.2.1.1	Yes__No__
SAPPP20	When a Ne-NSC report list is present in a connect indication, does the IUT update its contents as specified in Section 8.2.1.1?	M		8.2.1.1	Yes__No__
SAPPP21	When processing a Rp-NSC report list in a connect indication, does the IUT make sure that the Rp-NSC report list does not contain multiple instances of the same Rp-NSC identifier?	M		8.2.1.1	Yes__No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SAPPP22	When processing a Ne-NSC report list in a connect indication, does the IUT make sure that the Ne-NSC report list does not contain multiple instances of the same Ne-NSC identifier?	M		8.2.1.1	Yes__No__
SAPPP23	If the IUT forwarded the SETUP message using bare resources and the connect indication contains a Rp-NSC report list, does the IUT make sure that the Rp-NSC report list contains Rp-NSC_Bare?	M		8.2.1.1	Yes__No__
SAPPP24	If, as a result of compiling a report, the length of the Policy constraint information element would exceed the maximum length minus two octets, does the IUT include a report gap if one is not already present?	M		8.2.1.1	Yes__No__
Comments:					

B.4.4 Signalling Procedures at the AINI Succeeding side for Point to Point Connections (SASPP)

Item Number	Item Description	Status	Condition for status	Reference	Support
SASPP1	When at the succeeding side, if: • a received SETUP message contains a Policy constraint information element with content error (as defined in Section 10), the pass along request field set to "no pass along request" and the action indicator set to "clear call", and • the IUT would otherwise grant a pass along request for a Policy constraint information element then does the IUT crankback the connection with cause #100 "invalid information element contents", a diagnostic field set to the Policy constraint information element identifier and a crankback cause #192 "unrecognized policy constraint"?	M		8.2.1.2	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SASPP2	When at the succeeding side, if: • a received SETUP message contains a Policy constraint information element with an unrecognized policy or an unrecognized octet group (as defined in Section 10), and • the IUT would otherwise reject a pass along request for a Policy constraint information element then does the IUT reject the connection with cause #100 "invalid information element contents", and a diagnostic field set to the Policy constraint information element identifier?	M		8.2.1.2	Yes__ No__
SASPP3	If it receives a SETUP message which does not contain a Policy constraint information element, is the IUT capable of including a Policy constraint information element in the setup indication forwarded to call control, based on local configuration?	M	MCA15	8.2.1.2	Yes__ No__
SASPP4	If the IUT receives a SETUP message containing a Policy constraint information element, based on local configuration, is the IUT capable of including the received Policy constraint information element unchanged in the setup indication forwarded to call control?	M		8.2.1.2	Yes__ No__
SASPP5	If the IUT receives a SETUP message containing a Policy constraint information element, based on local configuration, is the IUT capable of discarding the received Policy constraint information element and replacing it by another one in the setup indication forwarded to call control?	M	MCA16	8.2.1.2	Yes__ No__
SASPP6	If the IUT receives a SETUP message containing a Policy constraint information element, based on local configuration, is the IUT capable of discarding the received Policy constraint information element and forwarding the setup indication to call control without any policy constraint?	M	MCA17	8.2.1.2	Yes__ No__
SASPP7	Does the IUT perform path and local link selection for a setup indication that contains a policy constraint as specified in Sections 6.2, 6.3 and 6.4?	M		8.2.1.2	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SASPP8	When the IUT has neither added nor replaced a Policy constraint information element with a policy constraint contained in a received SETUP message, does it use the policy constraint for local resource selection, as specified in Section 6.4?	M		8.2.1.2	Yes__ No__
SASPP9	When the IUT has either added or replaced a Policy constraint information element with a policy constraint contained in a received SETUP message, does it use that policy constraint for local resource selection, as specified in Section 6.4?	O	SASPP3 OR SASPP5	8.2.1.2	Yes__ No__
SASPP10	If the setup indication forwarded to call control contained a Policy constraint information element that was added, does the IUT not include any Policy constraint information element in the CONNECT message sent to the preceding side?	M	SASPP3	8.2.1.2	Yes__No__
SASPP11	If the setup indication forwarded to call control contained a Policy constraint information element that was replaced, does the IUT include an updated Policy constraint information element in the CONNECT message sent to the preceding side?	O	SASPP5	8.2.1.2	Yes__No__
SASPP12	When at the succeeding side, the IUT receives a connect request that contains a Policy constraint information element and it had forwarded a setup indication that did not contain a valid Policy constraint information element, does the IUT: • ignore the received Policy constraint information element if it would otherwise reject a pass along request for a Policy constraint information element, or • include the received Policy constraint information element unchanged in the CONNECT message sent to the preceding side, if it would otherwise grant a pass along request for a Policy constraint information element?	M		8.2.1.2	Yes__No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SASPP13	When at the succeeding side, the IUT receives a connect request that contains a Policy constraint information element and it had sent a setup indication with a valid Policy constraint information element without a report request, does the IUT: • ignore the received Policy constraint information element if it would otherwise reject a pass along request for a Policy constraint information element, or • include the received Policy constraint information element unchanged in the CONNECT message sent to the preceding side, if it would otherwise grant a pass along request for a Policy constraint information element?	M		8.2.1.2	Yes__No__
SASPP14	When at the succeeding side, the IUT receives a connect request that contains a Policy constraint information element with valid content, the setup indication that was forwarded contained a Policy constraint information element with a valid report request that was not added, the connection was established at this interface without using a "require" policy, and this interface is not tagged with any Ne-NSCs; does the IUT forward the received Policy constraint information element unchanged in the CONNECT message sent to the preceding side?	M		8.2.1.2	Yes__No__
SASPP15	If the setup indication forwarded to call control contained an unrecognized report request, does the IUT include a report gap, if one is not already present, in the Policy constraint information element contained in the CONNECT message sent to the preceding side?	M		8.2.1.2	Yes__No__
SASPP16	If the IUT would otherwise grant a pass along request for a Policy constraint information element, and the IUT receives a connect request containing a Policy constraint information element with invalid content (as defined in Section 10); does the IUT replace the Policy constraint information element with one containing a Report octet group with a report gap?	M		8.2.1.2	Yes__No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SASPP17	If the IUT would otherwise reject a pass along request for a Policy constraint information element, and the IUT receives a connect request containing a Policy constraint information element with an unrecognized octet group (as defined in Section 10), or without a Report octet group, or with more than one Report octet group, does the IUT replace the Policy constraint information element with one containing a Report octet group with a report gap?	M		8.2.1.2	Yes__No__
SASPP18	If the IUT would otherwise grant a pass along request for a Policy constraint information element, and the IUT receives a connect request containing a Policy constraint information element with valid content (as defined in Section 10) and more than one recognized Report octet group, does the IUT update (if applicable) the first recognized occurrence?	M		8.2.1.2	Yes__No__
SASPP19	If the IUT established the connection at this interface using a “require” policy operator containing a Rp-NSC list, and the forwarded setup indication contained a report request set to either “Report all required NSCs”, “Report required Rp-NSCs”, or “Report all Ne-NSCs and required Rp-NSCs”, does the IUT make sure that the CONNECT message sent to the preceding side contains a Rp-NSC report list?	M		8.2.1.2	Yes__No__
SASPP20	If the IUT established the connection at this interface using a “require” policy operator containing a Ne-NSC list, and the forwarded setup indication contained a report request set to either “Report all required NSCs” or “Report required Ne-NSCs”, does the IUT make sure that the CONNECT message sent to the preceding side contains a Ne-NSC report list?	M		8.2.1.2	Yes__No__
SASPP21	If this interface is tagged with at least one Ne-NSC, and the setup indication contained a report request set to either “Report all Ne-NSCs” or “Report all Ne-NSCs and required Rp-NSCs”, does the IUT make sure that the CONNECT message sent to the preceding side contains a Ne-NSC report list?	M		8.2.1.2	Yes__No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SASPP22	When a Rp-NSC report list is present in a CONNECT message, does the IUT update its contents as specified in Section 8.2.1.2?	M		8.2.1.2	Yes__No__
SASPP23	When a Ne-NSC report list is present in a CONNECT message, does the IUT update its contents as specified in Section 8.2.1.2?	M		8.2.1.2	Yes__No__
SASPP24	When processing a Rp-NSC report list in a CONNECT message to be sent to the preceding side, does the IUT make sure that the Rp-NSC report list does not contain multiple instances of the same Rp-NSC identifier?	M		8.2.1.2	Yes__No__
SASPP25	When processing a Ne-NSC report list in a CONNECT message to be sent to the preceding side, does the IUT make sure that the Ne-NSC report list does not contain multiple instances of the same Ne-NSC identifier?	M		8.2.1.2	Yes__No__
SASPP26	If the IUT established the connection in bare resources at this interface and the CONNECT message to be sent to the preceding side contains a Rp-NSC report list, does the IUT make sure that the Rp-NSC report list contains Rp-NSC_Bare?	M		8.2.1.2	Yes__No__
SASPP27	If, as a result of compiling a report, the length of the Policy constraint information element would exceed the maximum length minus two octets, does the IUT include a report gap if one is not already present?	M		8.2.1.2	Yes__No__
Comments:					

B.4.5 Signalling Procedures at the AINI Preceding Side for Point to Multipoint Connections (SAPMP)

Item Number	Item Description	Status	Condition for status	Reference	Support
SAPMP1	When the IUT translates a received connect indication into an add party acknowledge request for the previous interface, does it include the Policy constraint information element from the connect indication unchanged in the add party acknowledge request?	M	MCA2	8.3.1	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SAPMP2	If the preceding side receives an add party request which does not contain a Policy constraint information element, is the IUT capable of including a Policy constraint information element in the ADD PARTY message forwarded to the succeeding side, based on local configuration?	M	MCA2 AND MCA15	8.3.2	Yes__ No__
SAPMP3	If the preceding side receives an add party request containing a Policy constraint information element, based on local configuration, is the IUT capable of including the received Policy constraint information element unchanged in the ADD PARTY message forwarded to the succeeding side?	M	MCA2	8.3.2	Yes__ No__
SAPMP4	If the preceding side receives an add party request containing a Policy constraint information element, based on local configuration, is the IUT capable of discarding the received Policy constraint information element and replacing it by another one in the ADD PARTY message forwarded to the succeeding side?	M	MCA2 AND MCA16	8.3.2	Yes__ No__
SAPMP5	If the preceding side receives an add party request containing a Policy constraint information element, based on local configuration, is the IUT capable of discarding the received Policy constraint information element and forwarding the ADD PARTY message to the succeeding side without any policy constraint?	M	MCA2 AND MCA17	8.3.2	Yes__ No__
SAPMP6	When a received ADD PARTY ACKNOWLEDGE message contains a Policy constraint information element, and the received add party request did not contain a Policy constraint information element (whether valid or being passed along), does the IUT discard the received Policy constraint information element?	M	MCA2	8.3.2	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SAPMP7	When a received ADD PARTY ACKNOWLEDGE message contains a Policy constraint information element, and the received add party request contained a Policy constraint information element that was discarded by the preceding side, does the IUT discard the received Policy constraint information element?	M	MCA2 AND SAPMP4	8.3.2	Yes__ No__
SAPMP8	When a received ADD PARTY ACKNOWLEDGE message contains a Policy constraint information element, and the received add party request contained a Policy constraint information element that was replaced by the preceding side, does the IUT discard the received Policy constraint information element?	O	MCA2 AND SAPMP5	8.3.2	Yes__ No__
SAPMP9	When a received ADD PARTY ACKNOWLEDGE contains a Policy constraint information element which the IUT does not discard, does the IUT forward the received Policy constraint information element unchanged?	M	MCA2	8.3.2	Yes__ No__
Comments:					

B.4.6 Signalling Procedures at the AINI Succeeding Side for Point to Multipoint Connections (SASMP)

Item Number	Item Description	Status	Condition for status	Reference	Support
SASMP1	When the IUT translates a received ADD PARTY message into an outgoing SETUP message, does it include the Policy constraint information element from the ADD PARTY message unchanged in the SETUP message?	M	MCA2	8.3.1	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SASMP2	When at the succeeding side, if: • a received ADD PARTY message contains a Policy constraint information element with content error (as defined in Section 10), the pass along request field set to "no pass along request and the action indicator set to "clear call", and • the IUT would otherwise grant a pass along request for a Policy constraint information element then does the IUT crankback the party with an ADD PARTY REJECT message with cause #100 "invalid information element contents", a diagnostic field set to the Policy constraint information element identifier and a crankback cause #192 "unrecognized policy constraint"?	M	MCA2	8.3.3	Yes__ No__
SASMP3	When at the succeeding side, if: • a received ADD PARTY message contains a Policy constraint information element with an unrecognized policy or an unrecognized octet group (as defined in Section 10), and • the IUT would otherwise reject a pass along request for a Policy constraint information element then does the IUT reject the party with cause #100 "invalid information element contents", and a diagnostic field set to the Policy constraint information element identifier?	M	MCA2	8.3.3	Yes__ No__
SASMP4	If it receives an ADD PARTY message which does not contain a Policy constraint information element, is the IUT capable of including a Policy constraint information element in the add party indication forwarded to call control, based on local configuration?	M	MCA2 AND MCA15	8.3.3	Yes__ No__
SASMP5	If the IUT receives an ADD PARTY message containing a Policy constraint information element, based on local configuration, is the IUT capable of including the received Policy constraint information element unchanged in the add party indication forwarded to call control?	M	MCA2	8.3.3	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SASMP6	If the IUT receives an ADD PARTY message containing a Policy constraint information element, based on local configuration, is the IUT capable of discarding the received Policy constraint information element and replacing it by another one in the add party indication forwarded to call control?	M	MCA2 AND MCA16	8.3.3	Yes__ No__
SASMP7	If the IUT receives an ADD PARTY message containing a Policy constraint information element, based on local configuration, is the IUT capable of discarding the received Policy constraint information element and forwarding the add party indication to call control without any policy constraint?	M	MCA2 AND MCA17	8.3.3	Yes__ No__
SASMP8	When at the succeeding side, whenever path selection occurs for an ADD PARTY message that contains a policy constraint, does the IUT consider that resources supporting the existing connection tree match all policies?	M	MCA2	8.3.3	Yes__ No__
SASMP9	When at the succeeding side, whenever path selection occurs for an ADD PARTY message that contains a policy constraint, does the IUT take the policy constraint into account as specified in Section 6.2 and 6.3 to select a path from the branching point to the called party?	M	MCA2	8.3.3	Yes__ No__
SASMP10	If the add party indication forwarded to call control did not contain a Policy constraint information element, does the IUT not include a Policy constraint information element in the ADD PARTY ACKNOWLEDGE message sent to the preceding side?	M	MCA2	8.3.3	Yes__No__
SASMP11	If the add party indication forwarded to call control contained a Policy constraint information element that was added by the succeeding side, does the IUT not include a Policy constraint information element in the ADD PARTY ACKNOWLEDGE message sent to the preceding side?	M	MCA2 AND SASMP4	8.3.3	Yes__No__
SASMP12	If the add party indication forwarded to call control contained a Policy constraint information element that was replaced by the succeeding side, does the IUT not include a Policy constraint information element in the ADD PARTY ACKNOWLEDGE message sent to the preceding side?	O	MCA2 AND SASMP6	8.3.3	Yes__No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SASMP13	When a received add party acknowledge request contains a Policy constraint information element which the IUT does not discard, does the IUT include the received Policy constraint information element unchanged in the ADD PARTY ACKNOWLEDGE message sent to the preceding side?	M	MCA2	8.3.3	Yes__No__
Comments:					

B.4.7 Compatibility with nodes not supporting Policy Routing at the AINI (COMPA)

Item Number	Item Description	Status	Condition for status	Reference	Support
COMPA1	Does the IUT support setting the Policy constraint information element IE instruction field on a connection by connection basis?	M		8.4	Yes__ No__
COMPA2	If the IUT originates a Policy constraint information element within a SETUP or ADD PARTY message that allows routing on untagged resources, does the IUT: • set the IE instruction field flag to "follow explicit instructions", • set the action indicator to "discard information element and proceed" or "discard information element, proceed, and report status", and • set the pass along request field set to "pass along request"?	M		8.4	Yes__ No__
COMPA3	If a Policy constraint information element within a SETUP or ADD PARTY message that allows routing on untagged resources is received from a UNI, does the IUT: • set the IE instruction field flag to "follow explicit instructions", • set the action indicator to "discard information element and proceed" or "discard information element, proceed, and report status" and • set the pass along request field set to "pass along request"?	M		8.4	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
COMPA4	If the IUT originates a Policy constraint information element within a SETUP or ADD PARTY message that does not allow routing on untagged resources, does the IUT: • set the IE instruction field flag to "follow explicit instructions", • set the action indicator to "clear call", and • set the pass along request field set to "no pass along request"?	M		8.4	Yes__ No__
COMPA5	If a Policy constraint information element within a SETUP or ADD PARTY message that does not allow routing on untagged resources is received from a UNI, does the IUT: • set the IE instruction field flag to "follow explicit instructions", • set the action indicator to "clear call", and • set the pass along request field set to "no pass along request"?	M		8.4	Yes__ No__
COMPA6	When a Policy constraint information element is contained in a CONNECT or ADD PARTY ACKNOWLEDGE message, does the IUT: • set the IE instruction field flag to "follow explicit instructions", • set the action indicator to "discard information element and proceed" or "discard information element, proceed, and report status", and • set the pass along request field set to "pass along request"?	M		8.4	Yes__ No__
Comments:					

Annex C UNI Signalling 4.1 Protocol Implementation Conformance Statement (PICS) for Policy Routing Version 1.0

C.1 Introduction

To evaluate conformance of a particular implementation, it is necessary to have a statement of which capabilities and options have been implemented. Such a statement is called a Protocol Implementation Conformance Statement (PICS).

C.1.1 Scope

This document provides the UNI Signalling 4.1 PICS proforma for Policy Routing Version 1.0, defined in [1], in compliance with the relevant requirements, and in accordance with the relevant guidelines, given in ISO/IEC 9646-7. In most cases, statements contained in notes in the specification, which were intended as information, are not included in the PICS.

C.1.2 Normative References

[1] af-cs-0195.000, Policy Routing Version 1.0, April 2003

[2] ISO/IEC 9646-1: 1994, Information technology – Open systems interconnection – Conformance testing methodology and framework – Part 1: General Concepts (See also ITU Recommendation X.290 (1995)).

[3] ISO/IEC 9646-7: 1995, Information technology – Open systems interconnection – Conformance testing methodology and framework – Part 7: Implementation Conformance Statements (See also ITU Recommendation X.296 (1995)).

[4] ISO/IEC 9646-3:1998, Information technology – Open systems interconnection – Conformance testing methodology and interconnection – Part 3: The Tree and Tabular Combined Notation (TTCN) (See also ITU telecommunication X.292 (1998)).

C.1.3 Definitions

Terms defined in [1]

Terms defined in ISO/IEC 9646-1 and in ISO/IEC 9646-7

In particular, the following terms defined in ISO/IEC 9646-1 apply:

Protocol Implementation Conformance Statement (PICS): A statement made by the supplier of an implementation or system, stating which capabilities have been implemented for a given protocol.

PICS proforma: A document, in the form of a questionnaire, designed by the protocol specifier or conformance test suite specifier, which when completed for an implementation or system becomes the PICS.

C.1.4 Acronyms

ASN.1 Abstract Syntax Notation One
ATS Abstract Test Suite
IUT Implementation Under Test
PICS Protocol Implementation Conformance Statement
SUT System Under Test

C.1.5 Conformance

The PICS does not modify any of the requirements detailed in the Policy Routing Version 1.0. In case of apparent conflict between the statements in the base specification and in the annotations of "M" (mandatory) and "O" (optional) in the PICS, the text of the base specification takes precedence.

The supplier of a protocol implementation, which is claimed to conform to the UNI Signalling component of the ATM Forum Policy Routing Version 1.0, is required to complete a copy of the PICS proforma provided in this document and is required to provide the information necessary to identify both the supplier and the implementation.

C.2 Identification of the Implementation

Identification of the Implementation Under Test (IUT) and system in which it resides (the System Under Test (SUT)) should be filled in so as to provide as much detail as possible regarding version numbers and configuration options.

The product supplier information and client information should both be filled in if they are different.

A person who can answer queries regarding information supplied in the PICS should be named as the contact person.

C.2.1 Date of Statement

_____

C.2.2 Implementation Under Test (IUT) Identification

IUT Name: _____

_____

_____

IUT Version: _____

C.2.3 System Under Test (SUT) Identification

SUT Name: _____

_____

Hardware Configuration: _____

_____

_____

Operating System: _____

C.2.4 Product Supplier

Name: _____

Address: _____

_____

_____

Telephone Number: _____

Facsimile Number: _____

Email Address:_____

Additional Information: _____

_____

_____

C.2.5 Client

Name: _____

Address: _____

_____

_____

Telephone Number: _____

Facsimile Number: _____

Email Address:_____

Additional Information: _____

_____

_____

C.2.6 PICS Contact Person

(A person to contact if there are any queries concerning the content of the PICS)

Name: _____

Telephone Number: _____

Facsimile Number: _____

Email Address:_____

Additional Information: _____

Identification of the Protocol Specification

This PICS proforma applies to the following specification:

[1] af-cs-0195.000, Policy Routing Version 1.0, April 2003

C.3 PICS Proforma

C.3.1 Global statement of conformance

The implementation described in this PICS meets all of the mandatory requirements of the reference protocol.

[ ] YES
[ ] NO

Note: Answering "No" indicates non-conformance to the specified protocol. Non-supported mandatory capabilities are to be identified in the following tables, with an explanation by the implementor explaining why the implementation is non-conforming.

C.3.2 Instructions for Completing the PICS Proforma

The PICS Proforma is a fixed-format questionnaire. Answers to the questionnaire should be provided in the rightmost columns, either by simply indicating a restricted choice (such as Yes or No), or by entering a value or a set of range of values.

The following notations, defined in ISO/IEC 9647-7, are used for the support column:
Yes supported by the implementation
No not supported by the implementation

The following notations, defined in ISO/IEC 9647-7, are used for the status column:
M mandatory – the capability is required to be supported.
O optional – the capability may be supported or not.
O.i qualified optional – for mutually exclusive or selectable options from a set. “i” is an integer which identifies a unique group of related optional items and the logic of their selection is defined immediately following the table.

A supplier may also provide additional information, categorised as exceptional or supplementary information. These additional information should be provided as items labeled X.<i> for exceptional information, or S.<i> for supplemental information, respectively, for cross reference purposes, where <i> is any unambiguous identification for the item. The exception and supplementary information are not mandatory and the PICS is complete without such information. The presence of optional supplementary or exception information should not affect test execution, and will in no way affect interoperability verification. The column labeled ‘Reference’ gives a pointer to sections of the protocol specification for which the PICS Proforma is being written.

C.4 PICS for the support of Policy Routing at the UNI 4.1 interface

C.4.1 Major Capability at the UNI (MCU)

Item Number	Item Description	Status	Condition for status	Reference	Support
MCU1	Does the IUT support the Policy Routing UNI user side procedures?	O.1		9.2.1.1 9.2.2.2	Yes__ No__
MCU1.1	Does the IUT support the Policy Routing UNI user side procedures for point to multipoint connections?	M	MCU1 AND Note 1	9.3.1.1 9.3.2.2	Yes__ No__
MCU1.2	Does the IUT support Policy Routing at the user side of the S_B or coincident S_B/T_B reference points?	O.2	MCU1	9.3.2.1 9.3.2.2	Yes__ No__
MCU1.3	Does the IUT support Policy Routing at the user side of the T_B reference point?	O.2	MCU1	9.3.2.1 9.3.2.2	Yes__ No__
MCU2	Does the IUT support the Policy Routing UNI network side procedures?	O.1		9.2.1.2 9.2.2.1	Yes__No__
MCU3	Does the IUT support the Policy Routing UNI network side procedures for point to multipoint connections?	M	MCU2 AND Note 1	1.1	Yes__ No__
MCU4	Does the IUT support Policy Routing for a switched virtual channel connection (SVCC)?	M		1.1	Yes__ No__
MCU5	Does the IUT support Policy Routing for a switched virtual path connection (SVPC)?	M	Note 2	1.1	Yes__ No__
MCU6	Does the IUT support Policy Routing for a soft PVCC?	M	Note 3	1.1	Yes__ No__
MCU7	Does the IUT support Policy Routing for a soft PVPC?	M	Note 2 AND Note 3	1.1	Yes__ No__
MCU8	Does the IUT support originating a soft PVCC with a policy constraint?	M	Note 3	1.1	Yes__ No__
MCU9	Does the IUT support originating a soft PVPC with a policy constraint?	M	Note 2 AND Note 3	1.1	Yes__ No__
MCU10	Does the IUT support processing up to 6 Policies received in a Policy constraint information element?	M O	MCU2 MCU1	9	Yes__ No__
MCU11	Does the IUT support the “must avoid” policy operator?	M O.3	MCU2 MCU1	9	Yes__ No__
MCU12	Does the IUT support the “require” policy operator?	M O.3	MCU2 MCU1	9	Yes__ No__
MCU13	Does the IUT support Ne-NSC identifiers in policies?	M		9	Yes__ No__
MCU14	Does the IUT support Rp-NSC identifiers in policies?	M		9	Yes__ No__
MCU15	Does the IUT support the policy information report capability?	M		9	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
MCU16	Does the IUT support adding a policy constraint to a connection?	O		9	Yes__ No__
MCU17	Does the IUT support replacing a received policy constraint with another for a connection?	O		9	Yes__ No__
MCU18	Does the IUT support discarding a policy constraint for a connection?	O		9	Yes__ No__
Comments: O.1: At least one of MCU1 or MCU2 must be supported. O.2: At least one of MCU1.2 or MCU1.3 must be supported. O.3: At least one of MCU11 or MCU12 must be supported. Note 1: if point to multipoint procedures are supported. Note 2: if VPCs are supported Note 3: if soft PVCCs/PVPCs are supported.					

C.4.2 Encoding at UNI (EU)

Item Number	Item Description	Status	Condition for status	Reference	Support
EU1	Does the IUT support the Policy constraint information element as defined in Section 5.1?	M		5.1	Yes__ No__
EU2	Does the IUT support the maximum length of Policy constraint information element of 253 octets?	M		9.1.1, 9.1.2	Yes__ No__
EU3	Does the IUT support the Policy constraint information element in the CONNECT message?	M		9.1.1	Yes__ No__
EU4	Does the IUT support the Policy constraint information element in the SETUP message?	M		9.1.1	Yes__ No__
EU5	Does the IUT support the Policy constraint information element in the ADD PARTY message?	M	MCU1.1 OR MCU3	9.1.2	Yes__ No__
EU6	Does the IUT support the Policy constraint information element in the ADD PARTY ACKNOWLEDGE message?	M	MCU1.1 OR MCU3	9.1.2	Yes__ No__
Comments:					

C.4.3 Signalling Procedures for Point to Point Connections at the Originating Interface (SPPOI)

C.4.3.1 Procedures at the User Side

Item Number	Item Description	Status	Condition for status	Reference	Support
SPPOI1	When at the user side, for a setup request that contains a policy constraint, does the IUT perform resource selection over the interface using the received policy constraint as specified in Section 6.4?	M		9.2.1.1	Yes__ No__
SPPOI2	If the user side receives a setup request which does not contain a Policy constraint information element, is the IUT capable of including a Policy constraint information element in the SETUP message forwarded to the network side, based on local configuration?	M	MCU16	9.2.1.1	Yes__ No__
SPPOI3	If the user side receives a setup request containing a Policy constraint information element, based on local configuration, is the IUT capable of including the received Policy constraint information element unchanged in the SETUP message forwarded to the network side?	M		9.2.1.1	Yes__ No__
SPPOI4	If the user side receives a setup request containing a Policy constraint information element, based on local configuration, is the IUT capable of discarding the received Policy constraint information element and replacing it by another one in the SETUP message forwarded to the network side?	M	MCU17	9.2.1.1	Yes__ No__
SPPOI5	If the user side receives a setup request containing a Policy constraint information element, based on local configuration, is the IUT capable of discarding the received Policy constraint information element and forwarding the SETUP message to the network side without any policy constraint?	M	MCU18	9.2.1.1	Yes__ No__
SPPOI6	When at the user side, the IUT has either added or replaced the Policy constraint information element contained in the SETUP message sent to the network side, does it not use that policy constraint for local resource selection?	M	SPPOI2 OR SPPOI4	9.2.1.1	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SPPOI7	If the setup request received at the user side did not contain any Policy constraint information element, does the IUT discard any Policy constraint information element that is contained in the CONNECT message?	M		9.2.1.1	Yes__ No__
SPPOI8	If the IUT replaced the Policy constraint information element in the SETUP message sent to the network side, does the IUT ignore any report list that may be contained in the CONNECT message?	O	SPPOI4	9.2.1.1	Yes__ No__
SPPOI9	If the IUT receives a CONNECT message that contains a Policy constraint information element and it had sent a SETUP message without a valid Policy constraint information element, does the IUT ignore the received Policy constraint information element?	M		9.2.1.1	Yes__ No__
SPPOI10	If the IUT receives a CONNECT message that contains a Policy constraint information element and it had sent a SETUP message with a valid Policy constraint information element without a report request, does the IUT ignore the received Policy constraint information element?	M		9.2.1.1	Yes__ No__
SPPOI11	When the IUT receives a CONNECT message that contains a Policy constraint information element with valid content, the SETUP message it forwarded contained a Policy constraint information element with a valid report request that was not added, the connection was not forwarded using a “require” policy; and this interface is not tagged with any Ne-NSCs, does the IUT forward the received Policy constraint information element unchanged to call control?	M		9.2.1.1	Yes__No__
SPPOI12	If the setup request received from call control contained an unrecognized report request, does the IUT include a report gap, if one is not already present, in the Policy constraint information element contained in the connect indication sent to call control?	M		9.2.1.1	Yes__No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SPPOI13	If the IUT receives a CONNECT message containing a Policy constraint information element with an unrecognized octet group (as defined in Section 10), or without a Report octet group, or with more than one Report octet group; does the IUT replace the Policy constraint information element with one containing a Report octet group with a report gap?	M		9.2.1.1	Yes__No__
SPPOI14	If the IUT forwarded a SETUP message using a "require" policy operator containing a Rp-NSC list, and the corresponding setup request contained a report request set to either "Report all required NSCs", "Report required Rp-NSCs", or "Report all Ne-NSCs and required Rp-NSCs", does the IUT make sure that the connect indication sent to call control contains a Rp-NSC report list?	M		9.2.1.1	Yes__No__
SPPOI15	If the IUT forwarded a SETUP message using a "require" policy operator containing a Ne-NSC list, and the corresponding setup request contained a report request set to either "Report all required NSCs" or "Report required Ne-NSCs", does the IUT make sure that the connect indication sent to call control contains a Ne-NSC report list?	M		9.2.1.1	Yes__No__
SPPOI16	If this interface is tagged with at least one Ne-NSC, and the setup request contained a report request set to either "Report all Ne-NSCs" or "Report all Ne-NSCs and required Rp-NSCs", does the IUT make sure that the connect indication sent to call control contains a Ne-NSC report list?	M		9.2.1.1	Yes__No__
SPPOI17	When a Rp-NSC report list is present in a connect indication, does the IUT update its contents as specified in Section 9.2.1.1?	M		9.2.1.1	Yes__No__
SPPOI18	When a Ne-NSC report list is present in a connect indication, does the IUT update its contents as specified in Section 9.2.1.1?	M		9.2.1.1	Yes__No__
SPPOI19	When processing a Rp-NSC report list in a connect indication, does the IUT make sure that the Rp-NSC report list does not contain multiple instances of the same Rp-NSC identifier?	M		9.2.1.1	Yes__No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SPPOI20	When processing a Ne-NSC report list in a connect indication, does the IUT make sure that the Ne-NSC report list does not contain multiple instances of the same Ne-NSC identifier?	M		9.2.1.1	Yes__No__
SPPOI21	If the IUT forwarded the SETUP message using bare resources and the connect indication contains a Rp-NSC report list, does the IUT make sure that the Rp-NSC report list contains Rp-NSC_Bare?	M		9.2.1.1	Yes__No__
SPPOI22	If, as a result of compiling a report, the length of the Policy constraint information element would exceed the maximum length minus two octets, does the IUT include a report gap if one is not already present?	M		9.2.1.1	Yes__No__
Comments:					

C.4.3.2 Procedures at the Network Side

Item Number	Item Description	Status	Condition for status	Reference	Support
SPPOI23	When at the network side, if a received SETUP message contains a Policy constraint information element with a policy or policies associated with a service for which the user has not subscribed, does the IUT reject the connection with Cause # 50 “requested facility not subscribed” and a diagnostic field set to the Policy constraint information element identifier ?	M		9.2.1.2	Yes__ No__
SPPOI24	When at the network side, if a received SETUP message contains a Policy constraint information element with an unrecognized policy or an unrecognized octet group (as defined in Section 10), does the IUT reject the connection with cause #100 “invalid information element contents”, and a diagnostic field set to the Policy constraint information element identifier?	M		9.2.1.2	Yes__ No__
SPPOI25	If it receives a SETUP message which does not contain a Policy constraint information element, is the IUT capable of including a Policy constraint information element in the setup indication forwarded to call control, based on local configuration?	M	MCU16	9.2.1.2	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SPPOI26	If the IUT receives a SETUP message containing a Policy constraint information element, based on local configuration, is the IUT capable of including the received Policy constraint information element unchanged in the setup indication forwarded to call control?	M		9.2.1.2	Yes__ No__
SPPOI27	If the IUT receives a SETUP message containing a Policy constraint information element, based on local configuration, is the IUT capable of discarding the received Policy constraint information element and replacing it by another one in the setup indication forwarded to call control?	M	MCU17	9.2.1.2	Yes__ No__
SPPOI28	If the IUT receives a SETUP message containing a Policy constraint information element, based on local configuration, is the IUT capable of discarding the received Policy constraint information element and forwarding the setup indication to call control without any policy constraint?	M	MCU18	9.2.1.2	Yes__ No__
SPPOI29	Does the IUT perform path and local link selection for a setup indication that contains a policy constraint as specified in Sections 6.2, 6.3 and 6.4?	M		9.2.1.2	Yes__ No__
SPPOI30	When the IUT has neither added nor replaced a Policy constraint information element with a policy constraint contained in a received SETUP message, does it use the policy constraint for local resource selection, as specified in Section 6.4?	M		9.2.1.2	Yes__ No__
SPPOI31	When the IUT has either added or replaced a Policy constraint information element with a policy constraint contained in a received SETUP message, does it use that policy constraint for local resource selection, as specified in Section 6.4?	O	SPPOI25 OR SPPOI27	9.2.1.2	Yes__ No__
SPPOI32	If the setup indication forwarded to call control contained a Policy constraint information element that was added, does the IUT not include any Policy constraint information element in the CONNECT message sent to the user side?	M	SPPOI25	9.2.1.2	Yes__No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SPPOI33	If the setup indication forwarded to call control contained a Policy constraint information element that was replaced, does the IUT include an updated Policy constraint information element in the CONNECT message sent to the user side?	O	SPPOI27	9.2.1.2	Yes__No__
SPPOI34	When at the network side, the IUT receives a connect request that contains a Policy constraint information element and it had forwarded a setup indication that did not contain a valid Policy constraint information element, does the IUT ignore the received Policy constraint information element?	M		9.2.1.2	Yes__No__
SPPOI35	When at the network side, the IUT receives a connect request that contains a Policy constraint information element and it had sent a setup indication with a valid Policy constraint information element without a report request, does the IUT ignore the received Policy constraint information element?	M		9.2.1.2	Yes__No__
SPPOI36	When at the network side, the IUT receives a connect request that contains a Policy constraint information element with valid content, the setup indication that was forwarded contained a Policy constraint information element with a valid report request that was not added, the connection was established at this interface without using a “require” policy, and this interface is not tagged with any Ne-NSCs; does the IUT forward the received Policy constraint information element unchanged in the CONNECT message sent to the user side?	M		9.2.1.2	Yes__No__
SPPOI37	If the IUT receives a connect request containing a Policy constraint information element with an unrecognized octet group (as defined in Section 10), or without a Report octet group, or with more than one Report octet group, does the IUT replace the Policy constraint information element with one containing a Report octet group with a report gap?	M		9.2.1.2	Yes__No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SPPOI38	If the IUT established the connection at this interface using a "require" policy operator containing a Rp-NSC list, and the forwarded setup indication contained a report request set to either "Report all required NSCs", "Report required Rp-NSCs", or "Report all Ne-NSCs and required Rp-NSCs", does the IUT make sure that the CONNECT message sent to the user side contains a Rp-NSC report list?	M		9.2.1.2	Yes__No__
SPPOI39	If the IUT established the connection at this interface using a "require" policy operator containing a Ne-NSC list, and the forwarded setup indication contained a report request set to either "Report all required NSCs" or "Report required Ne-NSCs", does the IUT make sure that the CONNECT message sent to the user side contains a Ne-NSC report list?	M		9.2.1.2	Yes__No__
SPPOI40	If this interface is tagged with at least one Ne-NSC, and the setup indication contained a report request set to either "Report all Ne-NSCs" or "Report all Ne-NSCs and required Rp-NSCs", does the IUT make sure that the CONNECT message sent to the user side contains a Ne-NSC report list?	M		9.2.1.2	Yes__No__
SPPOI41	When a Rp-NSC report list is present in a CONNECT message, does the IUT update its contents as specified in Section 9.2.1.2?	M		9.2.1.2	Yes__No__
SPPOI42	When a Ne-NSC report list is present in a CONNECT message, does the IUT update its contents as specified in Section 9.2.1.2?	M		9.2.1.2	Yes__No__
SPPOI43	When processing a Rp-NSC report list in a CONNECT message to be sent to the user side, does the IUT make sure that the Rp-NSC report list does not contain multiple instances of the same Rp-NSC identifier?	M		9.2.1.2	Yes__No__
SPPOI44	When processing a Ne-NSC report list in a CONNECT message to be sent to the user side, does the IUT make sure that the Ne-NSC report list does not contain multiple instances of the same Ne-NSC identifier?	M		9.2.1.2	Yes__No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SPPOI45	If the IUT established the connection in bare resources at this interface and the CONNECT message to be sent to the user side contains a Rp-NSC report list, does the IUT make sure that the Rp-NSC report list contains Rp-NSC_Bare?	M		9.2.1.2	Yes__No__
SPPOI46	If, as a result of compiling a report, the length of the Policy constraint information element would exceed the maximum length minus two octets, does the IUT include a report gap if one is not already present?	M		9.2.1.2	Yes__No__
Comments:					

C.4.4 Signalling Procedures for Point to Point Connections at the Destination Interface (SPPDI)

C.4.4.1 Procedures at the Network Side

Item Number	Item Description	Status	Condition for status	Reference	Support
SPPDI1	When at the network side, for a setup request that contains a policy constraint, does the IUT perform resource selection over the interface using the received policy constraint as specified in Section 6.4?	M		9.2.2.1	Yes__ No__
SPPDI2	If the network side receives a setup request which does not contain a Policy constraint information element, is the IUT capable of including a Policy constraint information element in the SETUP message forwarded to the user side, based on local configuration?	M	MCU16	9.2.2.1	Yes__ No__
SPPDI3	If the network side receives a setup request containing a Policy constraint information element, based on local configuration, is the IUT capable of including the received Policy constraint information element unchanged in the SETUP message forwarded to the user side?	M		9.2.2.1	Yes__ No__
SPPDI4	If the network side receives a setup request containing a Policy constraint information element, based on local configuration, is the IUT capable of discarding the received Policy constraint information element and replacing it by another one in the SETUP message forwarded to the user side?	M	MCU17	9.2.2.1	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SPPDI5	If the network side receives a setup request containing a Policy constraint information element, based on local configuration, is the IUT capable of discarding the received Policy constraint information element and forwarding the SETUP message to the user side without any policy constraint?	M	MCU18	9.2.2.1	Yes__ No__
SPPDI6	When at the network side, the IUT has either added or replaced the Policy constraint information element contained in the SETUP message sent to the user side, does it not use that policy constraint for local resource selection?	M	SPPDI2 OR SPPDI4	9.2.2.1	Yes__ No__
SPPDI7	If the setup request received at the network side did not contain any Policy constraint information element, does the IUT discard any Policy constraint information element that is contained in the CONNECT message?	M		9.2.2.1	Yes__ No__
SPPDI8	If the IUT replaced the Policy constraint information element in the SETUP message sent to the user side, does the IUT ignore any report list that may be contained in the CONNECT message?	O	SPPDI4	9.2.2.1	Yes__ No__
SPPDI9	If the IUT receives a CONNECT message that contains a Policy constraint information element and it had sent a SETUP message without a valid Policy constraint information element, does the IUT ignore the received Policy constraint information element?	M		9.2.2.1	Yes__ No__
SPPDI10	If the IUT receives a CONNECT message that contains a Policy constraint information element and it had sent a SETUP message with a valid Policy constraint information element without a report request, does the IUT ignore the received Policy constraint information element?	M		9.2.2.1	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SPPDI11	When the IUT receives a CONNECT message that contains a Policy constraint information element with valid content, the SETUP message it forwarded contained a Policy constraint information element with a valid report request that was not added, the connection was not forwarded using a "require" policy, and this interface is not tagged with any Ne-NSCs; does the IUT forward the received Policy constraint information element unchanged to call control?	M		9.2.2.1	Yes__No__
SPPDI12	If the setup request received from call control contained an unrecognized report request, does the IUT include a report gap, if one is not already present, in the Policy constraint information element contained in the connect indication sent to call control?	M		9.2.2.1	Yes__No__
SPPDI13	If the IUT receives a CONNECT message containing a Policy constraint information element with an unrecognized octet group (as defined in Section 10), or without a Report octet group, or with more than one Report octet group; does the IUT replace the Policy constraint information element with one containing a Report octet group with a report gap?	M		9.2.2.1	Yes__No__
SPPDI14	If the IUT forwarded a SETUP message using a "require" policy operator containing a Rp-NSC list, and the corresponding setup request contained a report request set to either "Report all required NSCs", "Report required Rp-NSCs", or "Report all Ne-NSCs and required Rp-NSCs", does the IUT make sure that the connect indication sent to call control contains a Rp-NSC report list?	M		9.2.2.1	Yes__No__
SPPDI15	If the IUT forwarded a SETUP message using a "require" policy operator containing a Ne-NSC list, and the corresponding setup request contained a report request set to either "Report all required NSCs" or "Report required Ne-NSCs", does the IUT make sure that the connect indication sent to call control contains a Ne-NSC report list?	M		9.2.2.1	Yes__No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SPPDI16	If this interface is tagged with at least one Ne-NSC, and the setup request contained a report request set to either "Report all Ne-NSCs" or "Report all Ne-NSCs and required Rp-NSCs", does the IUT make sure that the connect indication sent to call control contains a Ne-NSC report list?	M		9.2.2.1	Yes__No__
SPPDI17	When a Rp-NSC report list is present in a connect indication, does the IUT update its contents as specified in Section 9.2.2.1?	M		9.2.2.1	Yes__No__
SPPDI18	When a Ne-NSC report list is present in a connect indication, does the IUT update its contents as specified in Section 9.2.2.1?	M		9.2.2.1	Yes__No__
SPPDI19	When processing a Rp-NSC report list in a connect indication, does the IUT make sure that the Rp-NSC report list does not contain multiple instances of the same Rp-NSC identifier?	M		9.2.2.1	Yes__No__
SPPDI20	When processing a Ne-NSC report list in a connect indication, does the IUT make sure that the Ne-NSC report list does not contain multiple instances of the same Ne-NSC identifier?	M		9.2.2.1	Yes__No__
SPPDI21	If the IUT forwarded the SETUP message using bare resources and the connect indication contains a Rp-NSC report list, does the IUT make sure that the Rp-NSC report list contains Rp-NSC_Bare?	M		9.2.2.1	Yes__No__
SPPDI22	If, as a result of compiling a report, the length of the Policy constraint information element would exceed the maximum length minus two octets, does the IUT include a report gap if one is not already present?	M		9.2.2.1	Yes__No__
Comments:					

C.4.4.2 Procedures at the User Side

Item Number	Item Description	Status	Condition for status	Reference	Support
SPPDI23	When at the user side, if a received SETUP message contains a Policy constraint information element with an unrecognized policy or an unrecognized octet group (as defined in Section 10), and the IUT is the called party, does the IUT ignore the received Policy constraint information element?	M		9.2.2.2	Yes__ No__
SPPDI24	When at the user side, if a received SETUP message contains a Policy constraint information element with an unrecognized policy or an unrecognized octet group (as defined in Section 10), the IUT is not the called party, and the connection would need to be progressed further, does the IUT reject the connection with cause #100 “invalid information element contents”, and a diagnostic field set to the Policy constraint information element identifier?	M		9.2.2.2	Yes__ No__
SPPDI25	If it receives a SETUP message which does not contain a Policy constraint information element, is the IUT capable of including a Policy constraint information element in the setup indication forwarded to call control, based on local configuration?	M	MCU16	9.2.2.2	Yes__ No__
SPPDI26	If the IUT receives a SETUP message containing a Policy constraint information element, based on local configuration, is the IUT capable of including the received Policy constraint information element unchanged in the setup indication forwarded to call control?	M		9.2.2.2	Yes__ No__
SPPDI27	If the IUT receives a SETUP message containing a Policy constraint information element, based on local configuration, is the IUT capable of discarding the received Policy constraint information element and replacing it by another one in the setup indication forwarded to call control?	M	MCU17	9.2.2.2	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SPPDI28	If the IUT receives a SETUP message containing a Policy constraint information element, based on local configuration, is the IUT capable of discarding the received Policy constraint information element and forwarding the setup indication to call control without any policy constraint?	M	MCU18	9.2.2.2	Yes__ No__
SPPDI29	Does the IUT perform path and local link selection for a setup indication that contains a policy constraint as specified in Sections 6.2, 6.3 and 6.4?	M	MCU1.3	9.2.2.2	Yes__ No__
SPPDI30	When the IUT has neither added nor replaced a Policy constraint information element with a policy constraint contained in a received SETUP message, does it use the policy constraint for local resource selection, as specified in Section 6.4?	M		9.2.2.2	Yes__ No__
SPPDI31	When the IUT has either added or replaced a Policy constraint information element with a policy constraint contained in a received SETUP message, does it use that policy constraint for local resource selection, as specified in Section 6.4?	O	SPPDI25 OR SPPDI27	9.2.2.2	Yes__ No__
SPPDI32	If the setup indication forwarded to call control contained a Policy constraint information element that was added, does the IUT not include any Policy constraint information element in the CONNECT message sent to the network side?	M	SPPDI25	9.2.2.2	Yes__No__
SPPDI33	If the setup indication forwarded to call control contained a Policy constraint information element that was replaced, does the IUT include an updated Policy constraint information element in the CONNECT message sent to the network side?	O	SPPDI27	9.2.2.2	Yes__No__
SPPDI34	When at the user side, the IUT receives a connect request that contains a Policy constraint information element and it had forwarded a setup indication that did not contain a valid Policy constraint information element, does the IUT ignore the received Policy constraint information element?	M		9.2.2.2	Yes__No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SPPDI35	When at the user side, the IUT receives a connect request that contains a Policy constraint information element and it had forwarded a setup indication with a valid Policy constraint information element without a report request, does the IUT ignore the received Policy constraint information element?	M		9.2.2.2	Yes__No__
SPPDI36	When at the user side, the IUT receives a connect request that contains a Policy constraint information element with valid content, the setup indication that was forwarded contained a Policy constraint information element with a valid report request that was not added , the connection was established at this interface without using a "require" policy, and this interface is not tagged with any Ne-NSCs; does the IUT forward the received Policy constraint information element unchanged in the CONNECT message sent to the network side?	M		9.2.2.2	Yes__No__
SPPDI37	If the setup indication forwarded to call control contained an unrecognized report request, does the IUT include a report gap, if one is not already present, in the Policy constraint information element contained in the CONNECT message sent to the network side?	M		9.2.2.2	Yes__No__
SPPDI38	If the IUT receives a connect request containing a Policy constraint information element with an unrecognized octet group (as defined in Section 10), or without a Report octet group, or with more than one Report octet group, does the IUT replace the Policy constraint information element with one containing a Report octet group with a report gap?	M		9.2.2.2	Yes__No__
SPPDI39	If the IUT established the connection at this interface using a "require" policy operator containing a Rp-NSC list, and the forwarded setup indication contained a report request set to either "Report all required NSCs", "Report required Rp-NSCs", or "Report all Ne-NSCs and required Rp-NSCs", does the IUT make sure that the CONNECT message sent to the network side contains a Rp-NSC report list?	M		9.2.2.2	Yes__No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SPPDI40	If the IUT established the connection at this interface using a "require" policy operator containing a Ne-NSC list, and the forwarded setup indication contained a report request set to either "Report all required NSCs" or "Report required Ne-NSCs", does the IUT make sure that the CONNECT message sent to the network side contains a Ne-NSC report list?	M		9.2.2.2	Yes__No__
SPPDI41	If this interface is tagged with at least one Ne-NSC, and the setup indication contained a report request set to either "Report all Ne-NSCs" or "Report all Ne-NSCs and required Rp-NSCs", does the IUT make sure that the CONNECT message sent to the network side contains a Ne-NSC report list?	M		9.2.2.2	Yes__No__
SPPDI42	When a Rp-NSC report list is present in a CONNECT message, does the IUT update its contents as specified in Section 9.2.2.2?	M		9.2.2.2	Yes__No__
SPPDI43	When a Ne-NSC report list is present in a CONNECT message, does the IUT update its contents as specified in Section 9.2.2.2?	M		9.2.2.2	Yes__No__
SPPDI44	When processing a Rp-NSC report list in a CONNECT message to be sent to the network side, does the IUT make sure that the Rp-NSC report list does not contain multiple instances of the same Rp-NSC identifier?	M		9.2.2.2	Yes__No__
SPPDI45	When processing a Ne-NSC report list in a CONNECT message to be sent to the network side, does the IUT make sure that the Ne-NSC report list does not contain multiple instances of the same Ne-NSC identifier?	M		9.2.2.2	Yes__No__
SPPDI46	If the IUT established the connection in bare resources at this interface and the CONNECT message to be sent to the network side contains a Rp-NSC report list, does the IUT make sure that the Rp-NSC report list contains Rp-NSC_Bare?	M		9.2.2.2	Yes__No__
SPPDI47	If, as a result of compiling a report, the length of the Policy constraint information element would exceed the maximum length minus two octets, does the IUT include a report gap if one is not already present?	M		9.2.2.2	Yes__No__
Comments:					

C.4.5 Signalling Procedures for Point to Multipoint Connections at the Originating Interface (SMPOI)

C.4.5.1 Procedures at the User Side

Item Number	Item Description	Status	Condition for status	Reference	Support
SMPOI1	If the user side receives an add party request which does not contain a Policy constraint information element, is the IUT capable of including a Policy constraint information element in the ADD PARTY message forwarded to the network side, based on local configuration?	M	MCU1.1 AND MCU16	9.3.1.1	Yes__ No__
SMPOI2	If the user side receives an add party request containing a Policy constraint information element, based on local configuration, is the IUT capable of including the received Policy constraint information element unchanged in the ADD PARTY message forwarded to the network side?	M	MCU1.1	9.3.1.1	Yes__ No__
SMPOI3	If the user side receives an add party request containing a Policy constraint information element, based on local configuration, is the IUT capable of discarding the received Policy constraint information element and replacing it by another one in the ADD PARTY message forwarded to the network side?	M	MCU1.1 AND MCU17	9.3.1.1	Yes__ No__
SMPOI4	If the user side receives an add party request containing a Policy constraint information element, based on local configuration, is the IUT capable of discarding the received Policy constraint information element and forwarding the ADD PARTY message to the network side without any policy constraint?	M	MCU1.1 AND MCU18	9.3.1.1	Yes__ No__
SMPOI5	When a received ADD PARTY ACKNOWLEDGE message contains a Policy constraint information element which does not contain a Report octet group, or contains an unrecognized octet group (as defined in Section 10), or contains more than one Report octet group, does the IUT discard the received Policy constraint information element?	M	MCU1.1	9.3.1.1	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SMPOI6	When a received ADD PARTY ACKNOWLEDGE message contains a Policy constraint information element, and the received add party request did not contain a Policy constraint information element, does the IUT discard the received Policy constraint information element?	M	MCU1.1	9.3.1.1	Yes__ No__
SMPOI7	When a received ADD PARTY ACKNOWLEDGE message contains a Policy constraint information element, and the received add party request contained a Policy constraint information element that was discarded by the user side, does the IUT discard the received Policy constraint information element?	M	MCU1.1 AND SMPOI4	9.3.1.1	Yes__ No__
SMPOI8	When a received ADD PARTY ACKNOWLEDGE message contains a Policy constraint information element, and the received add party request contained a Policy constraint information element that was replaced by the user side, does the IUT discard the received Policy constraint information element?	O	MCU1.1 AND SMPOI3	9.3.1.1	Yes__ No__
SMPOI9	When a received ADD PARTY ACKNOWLEDGE contains a Policy constraint information element which the IUT does not discard, does the IUT forward the received Policy constraint information element unchanged?	M	MCU1.1	9.3.1.1	Yes__ No__
Comments:					

C.4.5.2 Procedures at the Network Side

Item Number	Item Description	Status	Condition for status	Reference	Support
SMPOI10	When at the network side, if a received ADD PARTY message contains a Policy constraint information element with a policy or policies associated with a service for which the user has not subscribed, does the IUT reject the party with Cause # 50 “requested facility not subscribed” and a diagnostic field set to the Policy constraint information element identifier ?	M	MCU3	9.3.1.2	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SMPOI11	When at the network side, if a received ADD PARTY message contains a Policy constraint information element with an unrecognized policy or an unrecognized octet group (as defined in Section 10), does the IUT reject the party with cause #100 "invalid information element contents", and a diagnostic field set to the Policy constraint information element identifier?	M	MCU3	9.3.1.2	Yes__ No__
SMPOI12	If it receives an ADD PARTY message which does not contain a Policy constraint information element, is the IUT capable of including a Policy constraint information element in the add party indication forwarded to call control?	M	MCU3 AND MCU16	9.3.1.2	Yes__ No__
SMPOI13	If the IUT receives an ADD PARTY message containing a Policy constraint information element, based on local configuration, is the IUT capable of including the received Policy constraint information element unchanged in the add party indication forwarded to call control?	M	MCU3	9.3.1.2	Yes__ No__
SMPOI14	If the IUT receives an ADD PARTY message containing a Policy constraint information element, based on local configuration, is the IUT capable of discarding the received Policy constraint information element and replacing it by another one in the add party indication forwarded to call control?	M	MCU3 AND MCU17	9.3.1.2	Yes__ No__
SMPOI15	If the IUT receives an ADD PARTY message containing a Policy constraint information element, based on local configuration, is the IUT capable of discarding the received Policy constraint information element and forwarding the add party indication to call control without any policy constraint?	M	MCU3 AND MCU18	9.3.1.2	Yes__ No__
SMPOI16	When at the network side, whenever path selection occurs for an ADD PARTY message that contains a policy constraint, does the IUT consider that resources supporting the existing connection tree match all policies?	M	MCU3	9.3.1.2	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SMPOI17	When at the network side, whenever path selection occurs for an ADD PARTY message that contains a policy constraint, does the IUT take the policy constraint into account as specified in Section 6.2 and 6.3 to select a path from the branching point to the called party?	M	MCU3	9.3.1.2	Yes__ No__
SMPOI18	If the add party indication forwarded to call control did not contain a Policy constraint information element, does the IUT not include a Policy constraint information element in the ADD PARTY ACKNOWLEDGE message sent to the user side?	M	MCU3	9.3.1.2	Yes__No__
SMPOI19	If the add party indication forwarded to call control contained a Policy constraint information element that was added by the network side, does the IUT not include a Policy constraint information element in the ADD PARTY ACKNOWLEDGE message sent to the user side?	M	MCU3 AND SMPOI12	9.3.1.2	Yes__No__
SMPOI20	If the add party indication forwarded to call control contained a Policy constraint information element that was replaced by the network side, does the IUT not include a Policy constraint information element in the ADD PARTY ACKNOWLEDGE message sent to the user side?	O	MCU3 AND SMPOI14	9.3.1.2	Yes__No__
SMPOI21	When a received add party acknowledge request contains a Policy constraint information element which the IUT does not discard, does the IUT include the received Policy constraint information element unchanged in the ADD PARTY ACKNOWLEDGE message sent to the user side?	M	MCU3	9.3.1.2	Yes__No__
Comments:					

C.4.6 Signalling Procedures for Point to Multipoint Connections at the Destination Interface (SMPDI)

C.4.6.1 Procedures at the Network Side

Item Number	Item Description	Status	Condition for status	Reference	Support
SMPDI1	If the network side receives an add party request which does not contain a Policy constraint information element, is the IUT capable of including a Policy constraint information element in the ADD PARTY message forwarded to the user side, based on local configuration?	M	MCU3 AND MCU16	9.3.2.1.2	Yes__ No__
SMPDI2	If the network side receives an add party request containing a Policy constraint information element, based on local configuration, is the IUT capable of including the received Policy constraint information element unchanged in the ADD PARTY message forwarded to the user side?	M	MCU3	9.3.2.1.2	Yes__ No__
SMPDI3	If the network side receives an add party request containing a Policy constraint information element, based on local configuration, is the IUT capable of discarding the received Policy constraint information element and replacing it by another one in the ADD PARTY message forwarded to the user side?	M	MCU3 AND MCU17	9.3.2.1.2	Yes__ No__
SMPDI4	If the network side receives an add party request containing a Policy constraint information element, based on local configuration, is the IUT capable of discarding the received Policy constraint information element and forwarding the ADD PARTY message to the user side without any policy constraint?	M	MCU3 AND MCU18	9.3.2.1.2	Yes__ No__
SMPDI5	When a received ADD PARTY ACKNOWLEDGE message contains a Policy constraint information element which does not contain a Report octet group, or contains an unrecognized octet group (as defined in Section 10), or contains more than one Report octet group, does the IUT discard the received Policy constraint information element?	M	MCU3	9.3.2.1.2	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SMPDI6	When a received ADD PARTY ACKNOWLEDGE message contains a Policy constraint information element, and the received add party request did not contain a Policy constraint information element, does the IUT discard the received Policy constraint information element?	M	MCU3	9.3.2.1.2	Yes__ No__
SMPDI7	When a received ADD PARTY ACKNOWLEDGE message contains a Policy constraint information element, and the received add party request contained a Policy constraint information element that was discarded by the network side, does the IUT discard the received Policy constraint information element?	M	MCU3 AND SMPDI4	9.3.2.1.2	Yes__ No__
SMPDI8	When a received ADD PARTY ACKNOWLEDGE message contains a Policy constraint information element, and the received add party request contained a Policy constraint information element that was replaced by the network side, does the IUT discard the received Policy constraint information element?	O	MCU3 AND SMPDI3	9.3.2.1.2	Yes__ No__
SMPDI9	When a received ADD PARTY ACKNOWLEDGE contains a Policy constraint information element which the IUT does not discard, does the IUT forward the received Policy constraint information element unchanged?	M	MCU3	9.3.2.1.2	Yes__ No__
Comments:					

C.4.6.2 Procedures at the User Side

Item Number	Item Description	Status	Condition for status	Reference	Support
SMPDI10	When at the user side, if a received ADD PARTY message contains a Policy constraint information element with an unrecognized policy or an unrecognized octet group (as defined in Section 10) and the IUT is the called party, does the IUT ignore the received Policy constraint information element?	M	MCU1.3	9.3.2.2.2	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SMPDI11	When at the user side, if a received ADD PARTY message contains a Policy constraint information element with an unrecognized policy or an unrecognized octet group (as defined in Section 10), the IUT is not the called party, and the party would need to be progressed further, does the IUT reject the party with cause #100 "invalid information element contents", and a diagnostic field set to the Policy constraint information element identifier?	M	MCU1.3	9.3.2.2.2	Yes__ No__
SMPDI12	If it receives an ADD PARTY message which does not contain a Policy constraint information element, is the IUT capable of including a Policy constraint information element in the add party indication forwarded to call control, based on local configuration?	M	MCU1.3 AND MCU16	9.3.2.2.2	Yes__ No__
SMPDI13	If the IUT receives an ADD PARTY message containing a Policy constraint information element, based on local configuration, is the IUT capable of including the received Policy constraint information element unchanged in the add party indication forwarded to call control?	M	MCU1.3	9.3.2.2.2	Yes__ No__
SMPDI14	If the IUT receives an ADD PARTY message containing a Policy constraint information element, based on local configuration, is the IUT capable of discarding the received Policy constraint information element and replacing it by another one in the add party indication forwarded to call control?	M	MCU1.3 AND MCU17	9.3.2.2.2	Yes__ No__
SMPDI15	If the IUT receives an ADD PARTY message containing a Policy constraint information element, based on local configuration, is the IUT capable of discarding the received Policy constraint information element and forwarding the add party indication to call control without any policy constraint?	M	MCU1.3 AND MCU18	9.3.2.2.2	Yes__ No__
SMPDI16	When at the user side, whenever path selection occurs for an ADD PARTY message that contains a policy constraint, does the IUT consider that resources supporting the existing connection tree match all policies?	M	MCU1.3	9.3.2.2.2	Yes__ No__

Item Number	Item Description	Status	Condition for status	Reference	Support
SMPDI17	When at the user side, whenever path selection occurs for an ADD PARTY message that contains a policy constraint, does the IUT take the policy constraint into account as specified in Section 6.2 and 6.3 to select a path from the branching point to the called party?	M	MCU1.3	9.3.2.2.2	Yes__ No__
SMPDI18	If the add party indication forwarded to call control did not contain a Policy constraint information element, does the IUT not include a Policy constraint information element in the ADD PARTY ACKNOWLEDGE message sent to the network side?	M	MCU1.3	9.3.2.2.2	Yes__No__
SMPDI19	If the add party indication forwarded to call control contained a Policy constraint information element that was added by the user side, does the IUT not include a Policy constraint information element in the ADD PARTY ACKNOWLEDGE message sent to the network side?	M	MCU1.3 AND SMPDI12	9.3.2.2.2	Yes__No__
SMPDI20	If the add party indication forwarded to call control contained a Policy constraint information element that was replaced by the user side, does the IUT not include a Policy constraint information element in the ADD PARTY ACKNOWLEDGE message sent to the network side?	O	MCU1.3 AND SMPDI14	9.3.2.2.2	Yes__No__
SMPDI21	When a received add party acknowledge request contains a Policy constraint information element which the IUT does not discard, does the IUT include the received Policy constraint information element unchanged in the ADD PARTY ACKNOWLEDGE message sent to the network side?	M	MCU1.3	9.3.2.2.2	Yes__No__
Comments:					