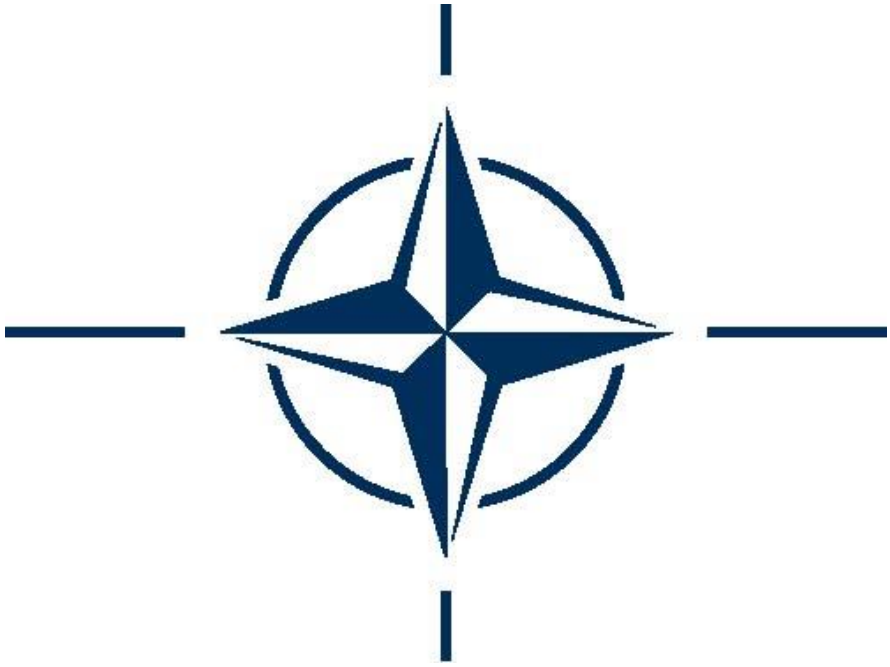
NATO STANDARD

AComP-4711

INTEROPERABILITY POINT QUALITY OF SERVICE (IP QoS)

Edition A Version 1

JANUARY 2018



NORTH ATLANTIC TREATY ORGANIZATION

ALLIED COMMUNICATIONS PUBLICATION

Published by the

NATO STANDARDIZATION OFFICE (NSO)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

25 January 2018

1. The enclosed Allied Communications Publication AComP-4711, Edition A, Version 1 – INTEROPERABILITY POINT QUALITY OF SERVICE (IP QoS), which has been approved by the nations in the Consultation, Command, and Control Board (C3B), is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 4711.

2. AComP-4711, Edition A, Version 1, is effective upon receipt.

3. No part of this publication may be reproduced, stored in a retrieval system, used commercially, adapted, or transmitted in any form or by any means, electronic, mechanical, photo-copying, recording or otherwise, without the prior permission of the publisher. With the exception of commercial sales, this does not apply to member or partner nations, or NATO commands and bodies.

4. This publication shall be handled in accordance with C-M(2002)60.

Dieter Schmaglowski
Deputy Director NSO
Branch Head P&C

Edvardas MAŽEIKIS
Major General, LTUAF
Director, NATO Standardization Office

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

RECORD OF RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS

Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.

INTENTIONALLY BLANK

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

INTENTIONALLY BLANK

TABLE OF CONTENTS

CHAPTER 1 : INTRODUCTION

1.1. INTRODUCTION

1.1.1. Federation of Networks (FoN), which is envisioned as the future within the NATO Network Enabled Capability (NNEC), requires standardization of the Interoperability Point (IOP) which connects two different networks having their individual internal structures. This interoperability definition has to take all layers of the communication stack into account and also different technologies used and service architectures that may be employed over the networks. In parallel with these, mechanisms and processes for security and Service Level Management (SLM) also need to be defined.

1.1.2. Service Level Management in Federation of Networks (FoN) requires common principles for continuity management. This continuity management contains all mechanisms and definitions that are required to make sure that important services operate over the FoN even in cases of severe degradations of network service. A part of this are mechanisms that commonly are called Quality of Service (QoS). QoS mechanisms build support for continuity management as well as service differentiation based on agreed communications policy.

1.1.3. In a federation of technology independent network, end-to-end Quality of Experience (QoE) requires that all interconnected networks share a common Military QoS policy at the interconnection. Additionally, interconnected networks must perform individually and together to meet Service Level Targets (SLT) set for them.

1.2. AIM

The purpose of the IOP Quality of Service (QoS) standard is:

- Achieve a common understanding about Service Level Management on Federation of Military Networks
- Define common Service Level Targets and how individual networks are to be abstracted to represent their Key Performance Indicators (KPI)
- Define abstractions of functions that are required at each side of the IOP
- Define the signalling schemes used to deliver Service Class and importance information over the IOP from one network to another

1.3. SCOPE

1.3.1. The scope of this Standard is end-to-end Service Level Management on NATO Federation of Networks concept; and especially how this Service Level Management relates to the network interconnection points (Interoperability Point – IOP) on military

networks.

1.3.2. The internals of individual networks are out of scope of this Standard. Only their domain wide representation of service between ingress and egress IOP is incorporated in this standard. Honouring of common communication policy and the signalled service attributes is expected from individual networks

1.4. APPLICABILITY

This STANAG is applicable to all interconnections between network domains in NATO Federation of Networks environment

1.5. IMPLEMENTATION OF THE AGREEMENT

This STANAG is considered implemented by a nation when that nation has placed in service one or more Interoperability Points (IOP) for interconnection with other national and/or NATO networks complying with the standards defined in this document.

RELATED DOCUMENTS:

A. Technical Note 1417 - IP QoS Standardization for the NII
B. Reference Document 2933 RC8 – IP QoS Standardization for the NII

CHAPTER 2 : TECHNOLOGY AGNOSTIC QoS MODEL (INFORMATIONAL – FOR CLARIFICATION OF NORMATIVE PARTS)

2.1. MOTIVATION

This Chapter presents a framework and a QoS model used in the normative Chapters. It aims to build an understanding on how protocol dependent actions should be implemented in different networking scenarios. Numerical KPI values for framework scenarios are provided as examples on how metrics are to be used, while it should be understood that real network (mission network) scenarios may deviate from these guidelines considerably, due to topologies and technologies applied.

2.2. AIM

This standard aims to define operation on and between IOPs in a way that it is technologically agnostic within the IOP and within individual networks. However, this standard also provides a group of annexes that define the operation of IOPs from the perspective of individual implementation technologies. The common part of the standard is providing technology agnostic heuristics for the operation of IOP and FoN at large in relation to business oriented Service Level Management process and common network operation process. Common operation over the IOP is defined by negotiation of quality, forwarding and resource reservation primitives in a way that end-to-end user traffic flow is receiving service from the network that it requires to execute information exchange it was tasked for.

2.3. NEED FOR QUALITY OF SERVICE

QoS is needed to maintain service continuity and to control different types of traffic in times of congestion in an effective way, without requiring over-capacity, so that important traffic is transmitted ahead of less important traffic and that real-time traffic can be supported over the converged network supporting also other communication services like high speed data and messaging. This allows a single network to support different service needs, with different quality constraints and different availability requirements. Congestion and/or capacity limitations which call for these actions may be due to limitations on transmission capacity, damaged or degraded network or underestimation of service demand.

2.4. NEED FOR SERVICE LEVEL MANAGEMENT

Service Level Management (SLM) is needed to maintain Federation of Network (FoN) services on a level that they support operational demand and mission. Service Level

Management is a process which takes into account all stakeholders in FoN. Operations personnel provide input for the business level objectives which are then translated into network level requirements that need to be put in place to support the operation. In an ideal world this would mean end-to-end multilateral SLAs which are, however, impossible to maintain and to support in process, not to mention at network layer. Prevalent solution is to provide only network based SLAs (Figure 1) which state requirements only for individual network hops (ingress IOP – egress IOP). Therefore, situation with SLM is such that end-to-end service is not under guarantee but it should still have continuity control through common QoS policy.

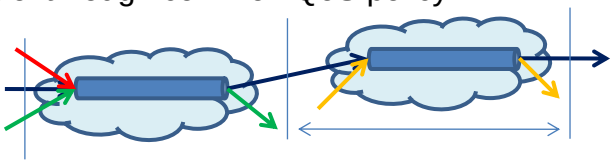


Figure 1: Network based SLA framework

It is assumed that Service Level Management procedures will evolve over time and that multilateral SLAs will become a reality as and when two key elements for the overall architecture evolve, namely interdomain QoS routing procedures and multilateral SLM framework (Figure 2).

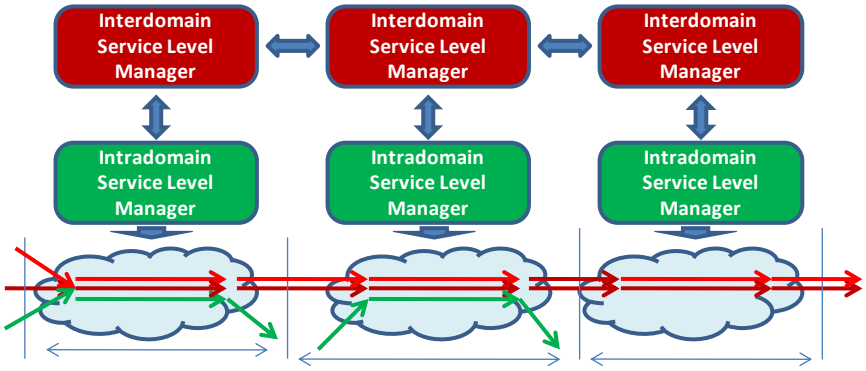


Figure 2: Multilateral SLM framework

2.5. NETWORK ARCHITECTURE FRAMEWORK

The foundation of this standard is to define a technology agnostic model for implementing QoS in interoperability points (IOP) connecting different network domains. This is based on general terms on behaviour that can be observed over an IOP and over the connecting network domain.

The basis for the model is a reference architecture presented in Figure 3. This reference model is illustrative and should not be considered as guideline for selecting technologies to implement interconnections at any level.

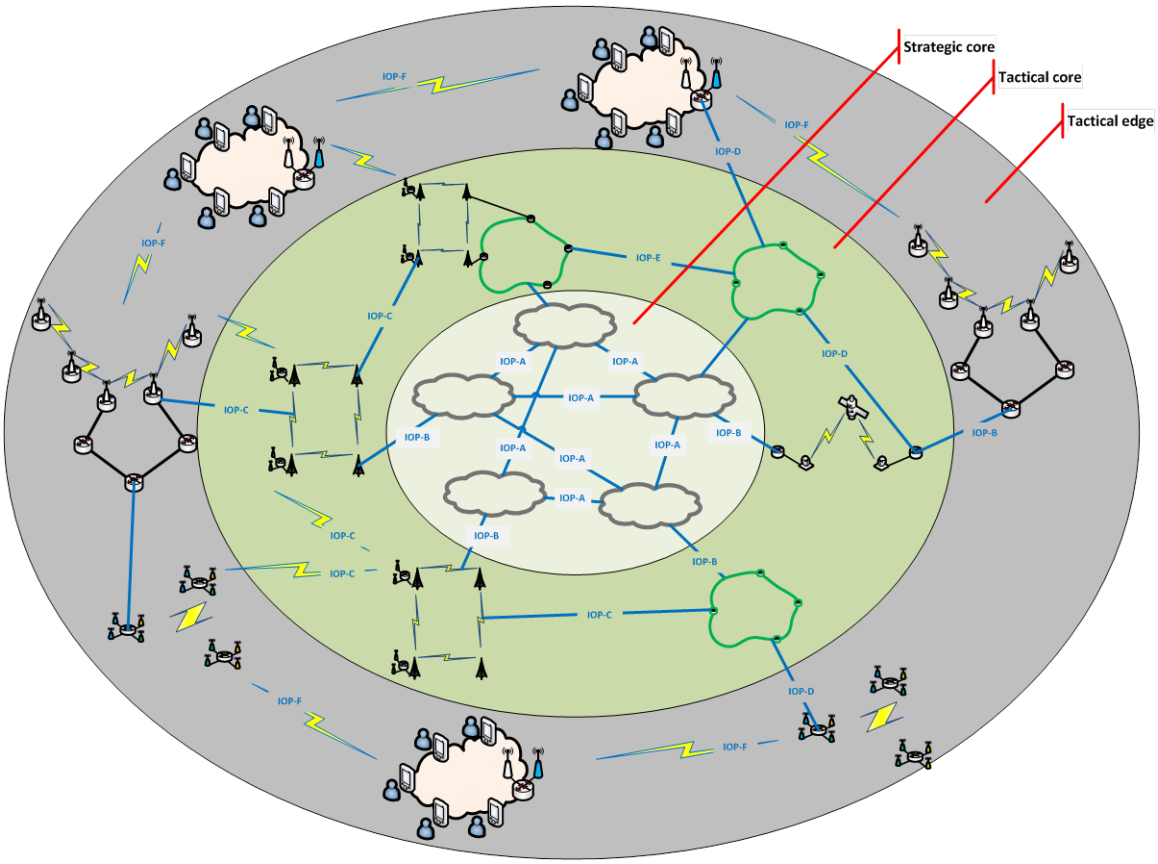


Figure 3: Network model

The framework is based on military network structures where there are

(a) Strategic core networks operated by individual nations as their core infrastructure, and networks of coalition organizations like NATO

(b) Tactical core networks operated by individual nations and/or coalition

(c) Tactical edge networks operated by field units from individual nations

In addition to these networks there are different levels of interconnections between networks and nations. This standard uses a convention of IOP-{Letter} to define the IOP type and typical usage of a particular IOP.

- IOP-A: IOP typically between two nations on a Strategic core network level with high bandwidth (fixed transmission / fibre optic environment). This may also apply to a connection between a nation and NATO.

- IOP-B: IOP typically between Strategic core network and Tactical core network. This can be created with long backhaul connections from the

theatre area to the national home front. These links are operated commonly by SATCOM (military and/or commercial) or Radio Relay when it is possible.

- IOP-C: IOP typically between two nations on a Tactical core networks at high bandwidth area (fixed transmission / fibre optic environment). Tacoms phase II standards can be used for this area.

- IOP-D: IOP typically between two Tactical core networks at low bandwidth area (radio link level environment).

- IOP-E: IOP typically between the Tactical core networks operated by nations and Post Command (fixed transmission / fibre optical environment). Tacoms phase I+ or Tacoms phase II standards can be used in this area.

- IOP-F IOP typically between two radio networks at Tactical edge network area. Emerging Stanag 5633 (Narrowband Waveform Network) could be used in the future as one potential solution for IOP at Tactical edge networks.

It should be noted that many of these IOP solutions are also applicable to connect tactical core and edge networks both within national domain but also within coalition between two or more nations.

2.6. SERVICE LEVEL MANAGEMENT FRAMEWORK

Following framework (Figure 4) is used within this Standard to describe the pair-wise connectivity between Service Level Management process and Network Operation process. Service Level Management framework defines the interaction between Service Level Management process and Network Operations process. It should be noted that this shows only the generic interaction while this standard aims to formalize certain aspects of this interaction to a network technology independent format.

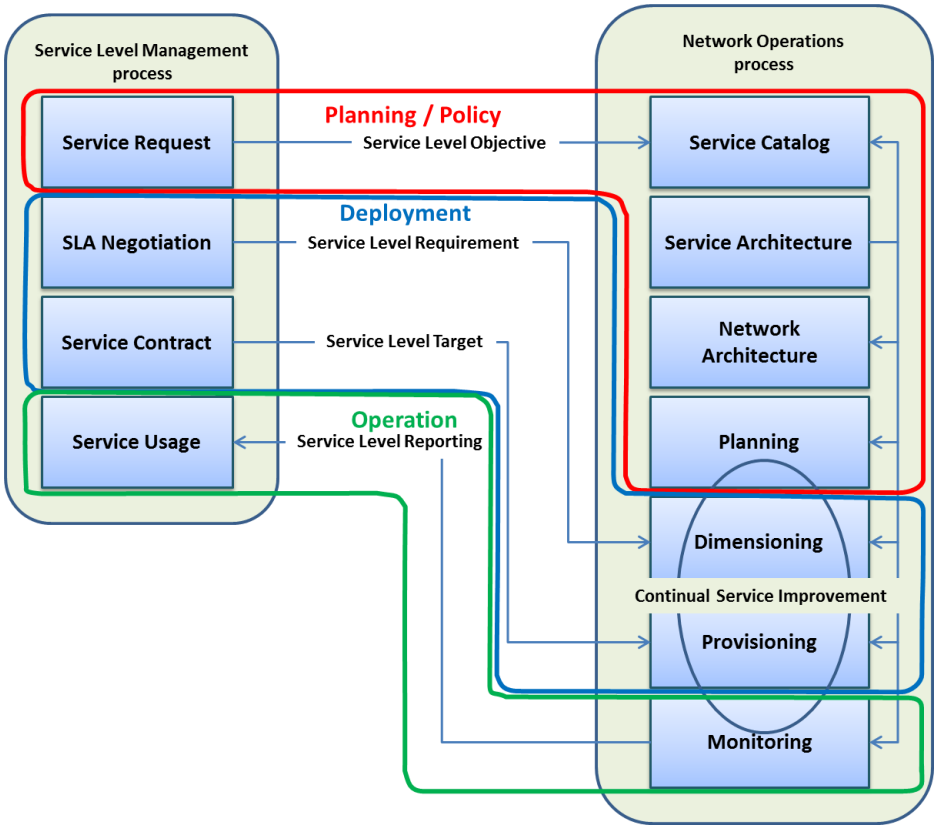


Figure 4: Service Level Management Framework

Service Level Management (SLM) is a process of negotiating Service Level Agreements (SLA), and ensuring that these are met. In this process, business driven qualitative objectives are defined for the services (Service Level Objective – SLO). These qualitative objective form the basis for understanding how the IT service influences the business process (how operation of networks affects the operation of C2 systems and ultimately the outcome of the operation/mission). Definition of SLOs is the ultimate lever from the operation planning – SLOs set the constraints for the Service Catalogues (services that are provided over and between IOPs by individual networks). Service Level Objectives form the foundation for more specific metrics namely Service Level Targets (SLT). SLTs are used to set performance targets for individual network services over individual networks (in a black box approach these are the performance metrics of individual networks for different Service Classes) and for the service as a whole over the Federation of Networks. It should be noted that there are no technical means to assess whether the overall FoN is able to provide the SLTs as the structure of the FoN changes with movement of troops and is also dependent on the routing employed at the networks level. It is assumed that for the sake of the communication continuity SLTs are abandoned when the network is either under extreme stress (degraded) or the topology is overly suboptimal for realistic service delivery. For both of these cases, service differentiation based on operational policy provides levers that can be used to control outcome of the network usage.

Network operational process includes whole network and service design and operation process. It contains definitions that come out from the operational policy as means of what and how service differentiation needs to be implemented and signalled over the IOP but also how it should be carried out by individual network domains (black box transfer function – Per Domain Behaviour heuristics). Network operational process also contains limitations that rise from the actual network technology and architecture that individual network is based on. This is the white-box model of the network and as such only visible to the operator of the particular network. The most visible limitations that may arise are based on technological differences at the military network level. While IOPs in this standard are based on several technologies and capabilities (connectionless IP technology is expected to be the most used IOP technology on interim purposes), individual networks themselves may, however, be based on any available technology that is able to provide the performance and services defined at the IOPs boundaries.

2.7. SERVICE LEVEL AGREEMENT

Service Level Agreement (SLA) is a contract between customer and service provider in which commodity/good, that is sold to the customer, is defined in an exact way along with the price that is paid for the commodity/good. It also contains means and methods to assess whether or not commodity is provided as described in the agreement to the customer, and how deviations from the agreed delivery process are escalated and compensated. SLA always contains applicability statement which limits the validity of contract to normal conditions and excludes all events that are not foreseeable and not controllable by provider.

From this perspective SLA is driven by business process optimization / business risk management of provider and customer. This kind of approach is natural on stable consumer and business-to-business market, where providers differentiate themselves by providing visibility to their services by offering SLA driven services. In real-world, SLA has very little merit as an QoS driver. It only provides means to market service providers technical goals as the compensations from the SLA deviations are on the order of one day compensation from monthly service fee.

Federation of Networks (FoN) is analogous to a small Internet. Therefore, the closest match for business processes can be inherited from the Internet community. In the Internet community, there exists no real SLA process other than direct neighbour SLA (network SLA) model. This is due to the fact that business model for cost/revenue transfer across service provider boundaries is non-existing. This is largely due to the unstructured network peerings where the only incentive is to provide reachability. The other problem behind multilateral SLAs is the lack of QoS routing protocols which would propagate KPIs across domains and thus allow selection of suitable forwarding paths per service. Models behind Telco peering ecosystem are based on static

infrastructure and automated cost transfer across network boundaries. These models do not lend themselves to more dynamic and chaotic IP peering ecosystem which is based on upstream revenue propagation.
Current military network ecosystem is closer to Telco ecosystem due to the fact that large portion of operation infrastructure is based on loose correlation to the orbat command structure (units at lower level tend to connect to units at higher level due to heavy correlation to the placement on the battle-field). FoN ecosystem is more orthogonal between command structure and connectivity (network infrastructure is supporting whatever command structure due to 'Internet' type of visibility across networks.

Therefore, SLA can be used on direct peering relationship to express service that is delivered for neighbour in normal situations. SLA cannot be used to express service which is delivered under exceptional conditions and/or end-to-end.

In parallel with SLA model a process oriented service policy is employed. This process policy is a realization of rules and methods that are employed for command and control during the operation. It is based on generic notion of common goal (which was also behind original ARPANET) for operation and thus common incentives to use network and especially Military Precedence trustworthy. This process model in principle states how to use Military Precedence in scheduling important traffic ahead of less important traffic with same nature. It also states how traffic of similar nature is aggregated to Service Classes and what is the relation between these classes. With this respect SLA agreements should be made with external service providers to provide services which are bound to be accessible only under normal conditions and based on the business process of provider. SLA can also be used for strategic networks which are more national asset than asset of common operation. On tactical and deployed networks, relationships between coalition partners are bound to be more driven by common goal.

2.8. QOS-MODELS

Three different models of QoS service offerings can be distinguished, as shown in Figure 5. The first one (A in Figure 5) is the single domain where a provider delivers QoS services inside the boundaries of its own network (this can be considered a model where there is single network for which all nations are users of network services). This reflects AMN type of network structure. The second one (B in Figure 5) is multiple domains where a small set of providers, with mutual business interests, co-operate to deliver QoS services inside the boundaries of their network aggregate (this can be thought as a model where few nations or NATO and few nations form a core for the network to which rest of the nations attach as users of services). This resembles typical network structure operated on Combined Endeavour exercises and which is the basis of Federated Mission Network. The third one (C in Figure 5) is the Federation of Networks (like the Internet) where QoS services can be delivered from almost any source to any destination and network interconnections are deployed where seen necessary, and which are operated autonomously by individual nations. In this model

there is no visible difference between core and user domains.

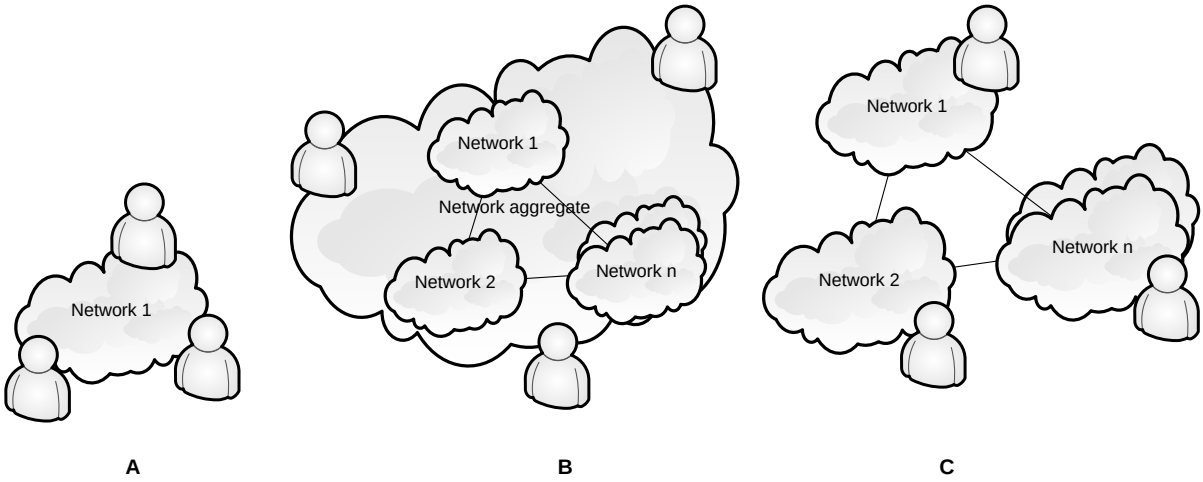


Figure 5: Different models for service offerings

For the sake of scalability, providers don't need to be concerned with what occurs more than one domain away from their own network domain when they negotiate inter-domain QoS agreements. They should base their agreements on nothing but their local QoS capabilities and those of their direct neighbours. This is due to the fact that multilateral SLAs need to provide real hard bounded end-to-end QoS services which are not possible to accomplish with management tools and protocols available today or in the near future.

2.9. ABSTRACTION OF NETWORK DOMAINS

The service over individual network domains is characterised as performance metrics (Capacity, Delay, Jitter and Loss) that they provide from the particular ingress IOP to the particular egress IOP (Figure 6).

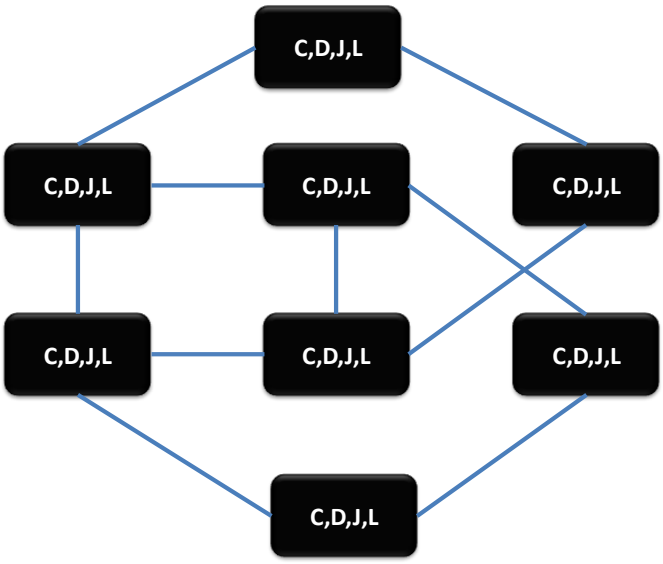


Figure 6: Black-box view on a interconnected network

The actual end-to-end service is a spatial composition of individual domain KPIs via path the communication is taking place. However, there are significant uncertainties in end-to-end KPIs which depend on technologies used to implement IOPs and domains themselves. These uncertainties are results from the loose coupling of routing and service requirements in several technologies used today.

2.10. SERVICE MAPPING

From the Quality of Service standpoint, an IOP provides a capability to map two different domains internal service structures in an uniform way. This is done in individual network domain IOPs by having a policy that matches local services with meta services defined in operations QoS policy (IOP services) bases on best-fit of KPIs. Two domains that implement this kind of local policy are able to exchange and transit traffic with best possible end-to-end semantics as mapping is done with best-fit policy on each of the domains (Figure 7).

This may also be done on a bilateral basis by negotiating QoS based bindings between individual network services in each of the domains (this is the case when a provider network is used as a backhaul of operations network).

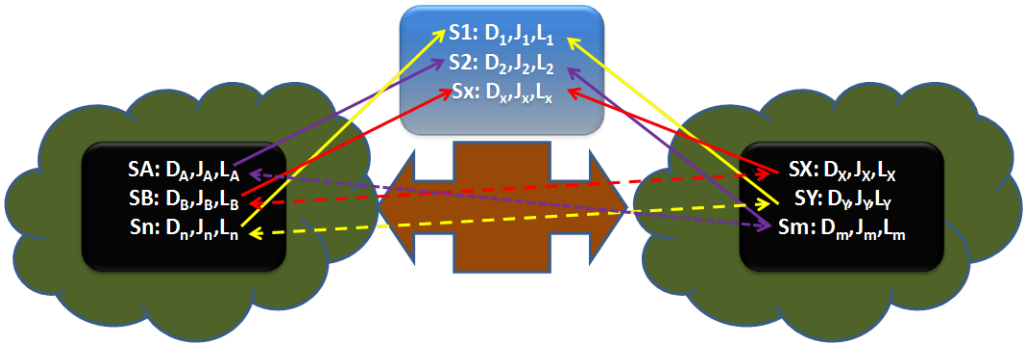


Figure 7: Interoperability Point service mapping

As an example, interoperability function in an connectionless IP IOP would contain meta services categorised KPIs and expressed as DSCP-values. These meta services are dependent on a service policy which is based on joint agreement or by coalition orders. However, each nation has their own internal service structures which are mapped locally to the IOP meta services. This mapping is done based on best-fit – meaning that IOP level meta services are implemented in national domains as they are best served based on their quality/performance constraints (KPIs). On a transmission path, packets may be remapped from a value to another or they may be locally encapsulated a separate forwarding header to encompass tunnelling between IOPs, however packet should have same meta service mapping throughout the FoN.
Eventually FoN can be abstracted into network graph (Figure 8) that represents individual nations as links having their internal performance metrics (KPIs), and IOPs as a nodes that interconnect individual nation to a number of other nations. These nodes execute single hop function (PHB) that maps services from one domain to another. This functionality, however, is not existing today – as there are no real solutions for inter-domain QoS routing which would be needed to route information through FoN in a manner that best suites its requirements.

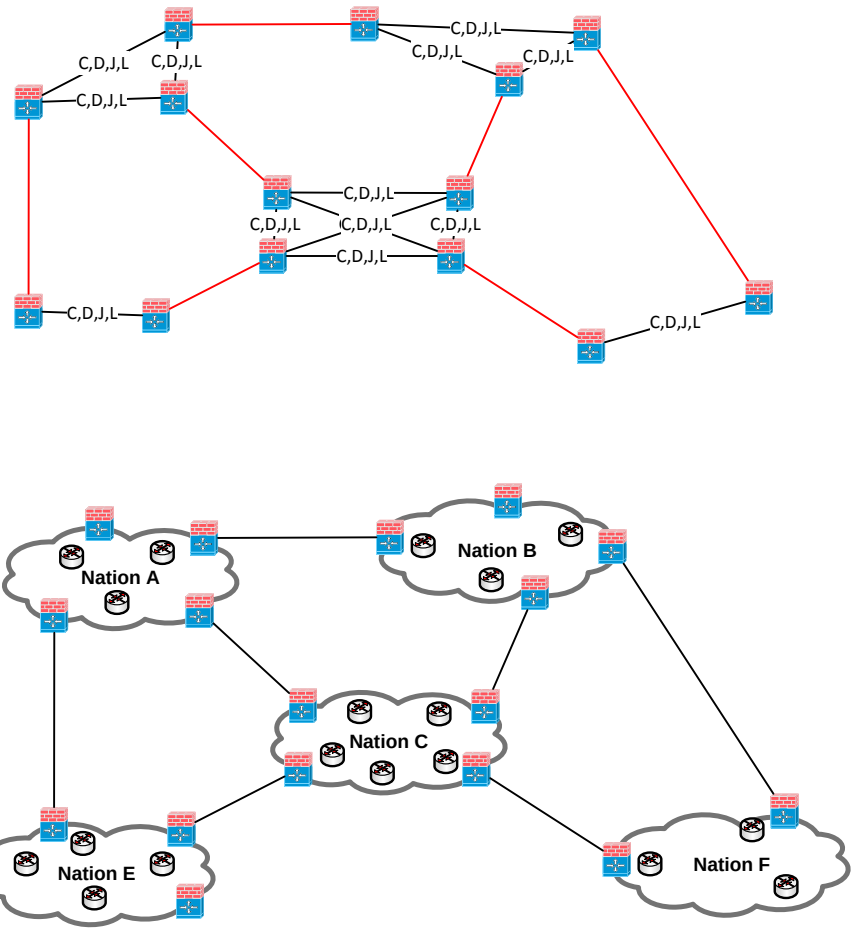


Figure 8: Abstraction of national network structure to KPI's and IOP-network

There are several other functionalities and/or capabilities that can be used over the network boundary. These capabilities provide levers for controlling the outcome of the usage of network services. These levers are used to control network resource consumption in contrast of communications policy that is enforced locally by individual nations in their network domains and by joint agreement over the IOPs.

2.11. QOS LEVERS

There are several time/network scales of Service Level Management which are all bound to different QoS mechanisms (Figure 9) and provide levers which can be used to control outcome of the network service.

From the bottom up these levers and mechanisms are

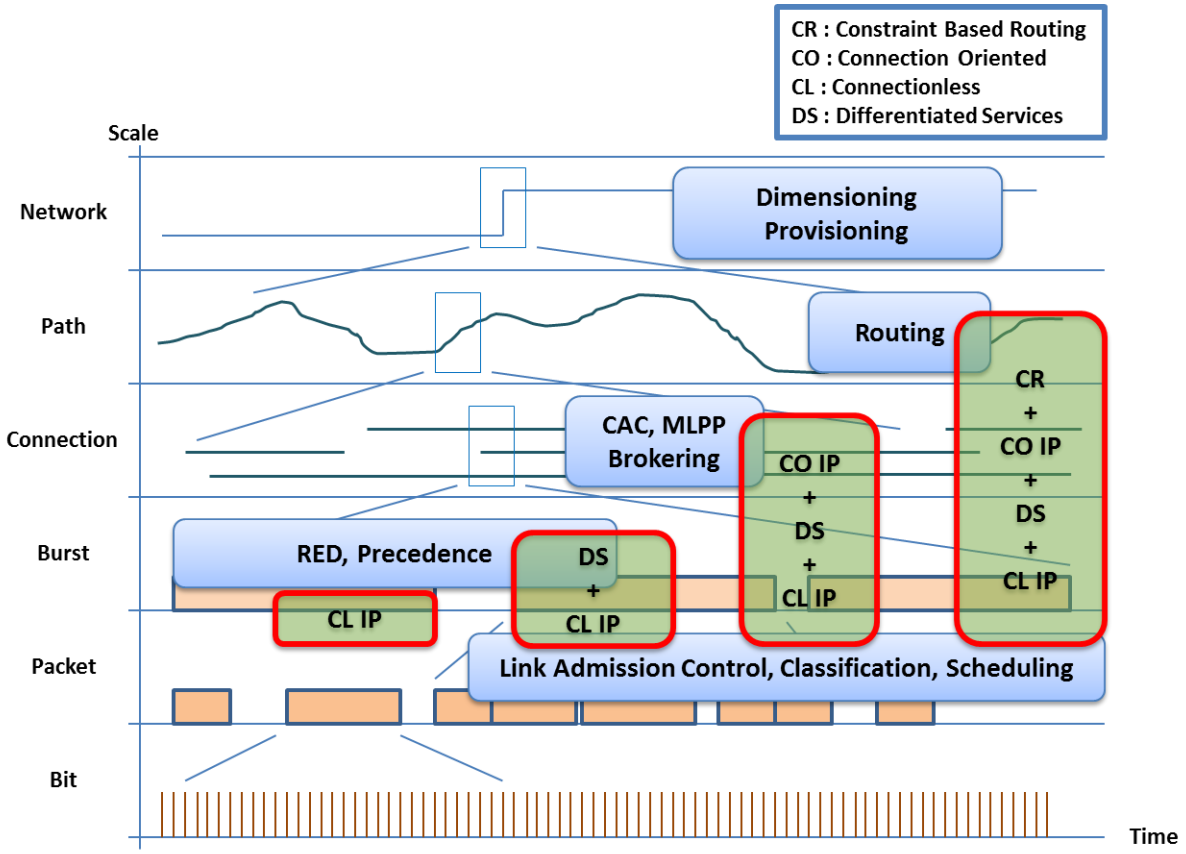


Figure 9: Levers on different layers (note: references to IP technology are provided for the sake of understanding how different functionalities stack up)

- Packet level:
    - Link Admission Control e.g. policing of the traffic at the ingress of the network. This function is used to secure network resources from intentional or unintentional surges of the traffic. Policing can be used to steer network resource usage by limiting certain military traffic classes across network boundaries.
    - Classification of the traffic to the military Service Classes that are targeted to offer some level of service to particular military traffic class. Changing the classification list allows targeting network Service Classes to some defined usage.
    - Scheduling is used to build Service Class and precedence based differentiation. As a lever scheduling can be used to control the effect of military precedence and relation between different military Service Classes (e.g. values of KPIs).

- Burst level:
    - Precedence can be used also to control military precedence. Burst level priority is based on algorithms that control buffer space occupancy.
    - Active Queue Management algorithms (RED, WRED) are algorithms that control the outcome of buffer level priority. As a lever there are several parameters that can be used to balance operation of controlled load services like TCP based services. Also relation of different priority delivery levels can be controlled.
- Connection
    - Connection Admission Control is used to control resources when there are connection oriented network service or service overlay. CAC algorithms (or equivalent) with routing mechanism and their “safety margin” can be used as a lever to control how conservative resource reservation policy.
    - Military Precedence and Pre-emption (or MLPP) can be used to pre-empt lower priority connections from the network in favour of higher priority connections. MPP is a lever that can be used through communications policy – when and how precedences are allowed to be used.
    - Brokering is a method which can be used for resource reservation in cases when network element is not able to perform mechanisms required to establish connection-oriented connection (connection signalling and CAC algorithm for resource allocation).
- Path
    - Routing can be used to control forwarding paths that are used for delivering traffic. Currently there are intra-domain routing protocols that are capable to provide constraints based routing through traffic engineering extensions. These extensions and algorithms used for calculating optimal forwarding path against pursued policy are the lever that can be used to control traffic distribution on net. However, inter-domain proactive routing based on BGP is currently having poor traffic engineering as it does not provide capabilities to transfer network status. Also there are no means to calculate differing paths as protocol conveys only the best possible path for all existing routes. Inter-domain QoS routing is needed before real end-to-end SLA is achieved. International research community has advanced in this area to develop multipath BGP and also capabilities to signal QoS Service Classes across the network

boundaries.

- Network

  - Provisioning is the ultimate lever for controlling which traffic and Service Class has premium capacity allocation (capacity is allocated over the assumed traffic volume). Provisioning is also a tool to build Service Level Management across network domains as there needs to be several network based SLAs that are co-ordinated to form reasonable end-to-end QoS.

  - Dimensioning is a lever that can also be used when network deployments are planned.

2.12. PERFORMANCE TARGETS

2.12.1. Reference transmission path

The reference transmission path is defined in Figure 10.

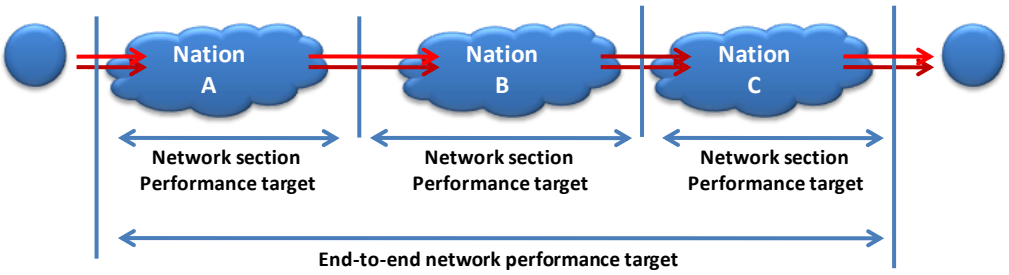


Figure 10 End-to-End Reference Path for QoS Objectives

The user-to-user performance target consists of the user installation(s) and all (NATO and national) networks in between. The user installation (end system) is outside the scope of this QoS Standard. The performance targets, given in this section, refer to the network end-to-end performance, which constitute the end system to end system connection, across one or more military networks excluding user service and user terminal processing.

2.12.2. Accumulated performance

Each of the networks and network devices contribute to the delay and error budget. The performance target specifies the upper bounds for the accumulated metrics. The SLAs for each of the networks must reflect the respective delay and error budgets based on the targets. Failing of one of the target metrics implies failure of the end-to-end QoS guarantee.

It should be noted that only true multilateral end-to-end SLAs makes possible to distribute Service Level Targets per domain in a manner that takes into account individual domain properties. Per domain SLAs, as presumed in this document, categorize domains into three main classes:

(i) Tactical networks comprising networks and technologies that are used by military networks suitable for operations. These system are continuously moving on manoeuvre area and thus have high variability on their capabilities, topology and performance. These devices are commonly based on low to moderate bit-rate technologies (kbps-Mbps) with a special hardware and software solutions. Span of these networks is usually rather small (intra theatre) while the amount of transmission hops may be relatively high (1-10). Tactical edge networks have highly varying topological and also technological solutions. At the one extreme there are non line of sight radios which cover the theatre with only a single hop, while at the other extreme there are mesh networks which cover only a small area of responsibility with several hops.

(ii) Tactical core networks comprising networks and technologies that are used in backbone structures to cover the theatre area. Requirements of tactical core networks are in respect to operation requirements. These devices are commonly based on moderate to medium bit-rate technologies (Mbps). These devices are typically based on MOTS, but also COTS can be used in certain scenarios (depending on operation requirements). Span of these networks is usually also small (intra theatre but with some backhaul to national or NATO strategic networks).

(iii) Strategic networks comprising networks and technologies that are used inside national military backbone structures between theatres and in national cores. These devices are typically based on medium-high bit-rate technologies (Mbps-Gbps) COTS technology. However, MOTS/mixed solutions are also valid examples for this area. Span of these networks is usually large. Outside of the scope are networks/sections that are provided by commercial service providers (due to the fact that they do not share common incentives).

Due to the different nature of these networks they will have very different levels on their performance metric - Key Performance Indicators (KPI). Table 1, Table 2 and Table 3 provide numerical indicators for KPIs on different network domains. It should be noted that these are targets based on performance of existing commercial core networks and derivate from those numbers to more volatile tactical environment. Based on the feasibility, performance targets set to different network sections may deviate from

these targets considerably.

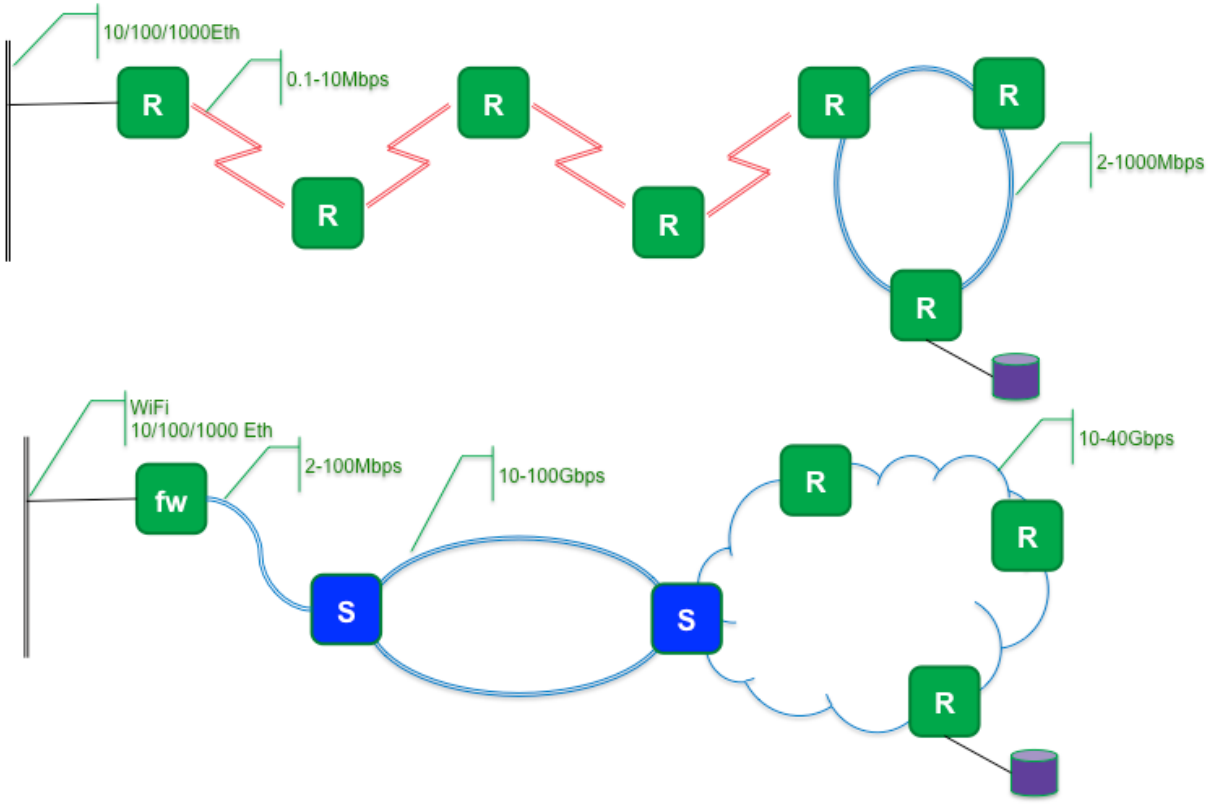


Figure 11: Difference between commercial and military network reference models

It should also be noted, that military networks and commercial networks do not share the same optimization goal. While commercial networks are designed to increase business through meeting increasing capacity demand of user community with as low marginal cost per bit as possible, military networks on the other hand assure the communications and to withstand surges and sudden degradations on network itself. Therefore, commercial network are designed as flat and direct as possible leading to high-speed aggregation and routing of information in the core. While for military networks coverage and capability to local operation is crucial. This added security and reliability does not come without a cost and/or penalty in transmission capacity. Therefore, military networks are some orders of magnitude lower in their capacity and have higher delays and delay variations than their commercial counterparts. This is due to higher number of network elements, especially radio-relays and security devices which cause number of additional processing cycles for packets on their way from one user to another. Also when looking at the larger level commercial networks have been streamlined over the years to a level that any user is connected to any other user with as few hops as possible. Today this means on the average four providers and two to three hops per provider. While in military networks Internet type of FoNs are only emerging and their structure is largely unknown, however several nations are expected to be passed and nationally the structure contains several hops if legacy systems are used to build up FoN transport. The consequence will be that the user community

needs to be aware that they cannot expect same performance level as is provided by commercial networks. Also applications that are designed and brought into military networks, need to be implemented with procedures that withstand fluctuations of network KPIs.

2.13. PERFORMANCE TARGETS

2.13.1. Guidance for performance target usage

The initial use of these performance targets is for network design and planning, and also to lay foundation for common understanding of different network sections quality constraints. It is plausible that nations and network owners report data on network performance to the NATO network health service, in order to create trustworthy and reliable statistics for the future references. Normalization of the performance measurement and reporting procedures and mechanisms are outside the scope of this Standard. Distribution of the performance targets, like the delay budget, over various networking components or segments (like LAN and WAN links) is a nation/domain internal concern and is beyond the scope of this Standard.

Performance targets, in this Standard, are based on a network performance that is achievable with terrestrial wire-line and terrestrial line-of-sight radio. Values, for strategic networks, in this document are combination of ITU recommendations values and what are the KPI levels of current Tier-1 service provider core networks (which are for networks with high transmission capabilities ~10Gbps); they are rigorous and not likely to be achieved in other locations than within Europe and US. It should be noted that in order to achieve these values considerable over provisioning of resources for individual services is expected (average load level ~ 25%). Therefore, in case of commercial backhaul it is expected that these values may not be met if connection is provided using asynchronous transmission techniques. Values for tactical core networks are based on modern transmission systems utilizing fibre optic connections and having capacities several orders of magnitude lower than strategic networks (2Mbps~100Mbps). If and when radio relays are used to form these links some additional constraints need to be taken account. Tactical networks should be taken from the perspective that network capacities are several orders of magnitude lower than in tactical core networks (10kbps~2Mbps) and that the main technology used to implement these networks is based on radio relays. It should also be noted that these networks usually contain several hops which cumulate the values of KPIs rapidly.

Performance metrics shown in following tables take into account common network security mechanisms like firewalls, encryption, and traffic management functions like shaping. Shaping is considered to be done in all egress interfaces of IOP per Treatment Aggregate or Service Class (depending on QoS policy in force). With shaping, only a moderate shaping is assumed – delay added by shapers is in relation to the transmission capacities over the IOPs). Parameter <P> that is expressed in each of the delay measures takes account great circle distance between ingress and egress

point with a nominal speed of light at fibre optic transmission system and necessary regeneration of signal at proper distances (approx 1ms per 100km).
Values within the table represent performance target for individual network from an ingress IOP to the egress IOP. End-to-end performance is cumulated across all networks that information must flow through on a way from the sender to the receiver. To have understanding of end-to-end metrics, it is assumed that it is a rare case that traffic flows across more than four networks. From individual metrics delays and losses are considered additive while delay variations are considered to be bounded by maximal value of individual network that is used for realising the connection.

Treatment Aggregate	Service Class	QoS Target
Real-Time	Telephony Equivalent Circuit	Delay (D) < (20 + P)ms Jitter (J) < 10ms Loss (L) < 0.1% MOS ≥ 3.9
Near-Real-Time	Signalling Video	Delay (D) < (28 + P)ms Jitter (J) < 10ms Loss (L) < 0.25%
Assured Elastic	Low-Latency Data	Delay (D) < (28 + P)ms Loss (L) < 0.25%
Elastic	High-Throughput Data Low-Priority Data	Loss (L) < 0.5%

Table 1 Performance targets applicable for strategic networks

Treatment Aggregate	Service Class	QoS Target
Real-Time (1)	Circuit Equivalent	Delay (D) < 20ms Jitter (J) < 5ms Loss (L) < 0.1% MOS ≥ 3.9
Real-Time (2)	Telephony Equivalent	Delay (D) < (28 + P)ms Jitter (J) < 20ms Loss (L) < 0.5% MOS ≥ 3.9
Near-Real-Time	Signalling Video	Delay (D) < (60 + P)ms Jitter (J) < 30ms Loss (L) < 1%
Assured Elastic	Low-Latency Data	Delay (D) < (60 + P)ms Loss (L) < 1%
Elastic	High-Throughput Data Low-Priority Data	Loss (L) < 1%

Table 2 Performance targets applicable for tactical core networks

Treatment Aggregate	Service Class	QoS Target
Real-Time (1)	Circuit Equivalent	Delay (D) <20 ms Jitter (J) < 5ms Loss (L) < 0.1% MOS ≥ 3.9
Real-Time (2)	Telephony Equivalent	Delay (D) < 40ms Jitter (J) < 15ms Loss (L) < 0.1% MOS ≥ 3.0
Near-Real-Time	Signalling Video	Delay (D) <150 ms Jitter (J) < 50ms Loss (L) < 1%
Assured Elastic	Low-Latency Data	Delay (D) < (150 + P)ms Loss (L) < 1%
Elastic	High-Throughput Data Low-Priority Data	Loss (L) < 2%

Table 3 Performance targets applicable for tactical networks

CHAPTER 3 : TECHNICAL STANDARDS FOR CONNECTIONLESS IP QOS (NORMATIVE)

3.1. MOTIVATION

Internet Protocol (IP) is the predominant technology for NATO and NATO nations' communication networks. Where today NATO and many NATO nations still operate a parallel circuit switched network for voice telephony and other real-time services, migration to a full IP network (full IP network should be interpreted as a network that uses IP as service delivery platform and not necessarily as forwarding technology) is ongoing. This migration process towards a single IP service delivery platform for many of military communication services is often referred to as IP convergence.
It is expected that this migration will happen through stages where the first stage will be dominated by the connectionless IP service with Best Effort and Differentiated Services service models. At later stages more and more connection-oriented functionalities will be introduced through connection-oriented service architecture like Integrated Services, and traffic engineering solutions like Multiprotocol Label Switching or equivalent.

3.2. DESCRIPTION

The following subchapters will describe the functionality needed to realize connectionless IP QoS.

3.2.1. Traffic Marking

The marking of IP packets shall be done in the Differentiated Services Code Point Field of the IP header (DSCP) as described in RFC 2474, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers" [IETF RFC 2474, 1998]

Each network domain SHALL mark their packets when exiting the national domain according definitions stated in this document and values defined in the operations policy.

The content of DSCP field is formulated to have two, three bit locators in the old IPv4 ToS field octet. For IPv6 the TrafficClass-octet contains the same bits, with only the six most significant bits having significance. The last two bits are unused.

DSCP in IPv4 Header:

Ver	IHL	ToS	TotLen	Id	Flags	FragOffset	TTL	Proto	Chksum	Source Addr	Dest Addr	Options (optional)

DSCP in IPv6 Header:

Ver	TrafficClass	FlowLabel	PayloadLen	NextH	HopLim	Source Address	Dest Address

ToS and TrafficClass-octet, as used in this STANAG:

DSCP bit 1(MSB)	DSCP bit 2	DSCP bit 3	DSCP bit 4	DSCP bit 5	DSCP bit 6	ECN bit 1	ECN bit 2
ServiceClass SC0-SC7			Precedence (4 levels)		0: CL	Not used	Not used
					1: CO		

The bit structure is defined in this STANAG as:

(i) The three most significant bits (bits 1-3) define the Service Class; and are used by routers to define QoS queues to where to place the traffic. Values are based on IETF Class Selector (CS) code-points: SC0 = CS0 … SC7 = CS7. Several Service Classes may share a common queue. Class Selector values are used both in the CL and CO IP QoS action to reflect service type.

(ii) Bits 4-5 define the expedited forwarding treatment, i.e. how each specific traffic packet should be handled within its queue. There are four precedencies that can be signalled with this capability (00 = Routine, 01 = Flash, 10 = Immediate, 11 = Priority). The rest of the precedence classes defined in RFC 4542 – “Implementing an Emergency Telecommunications Service” and references therein are not considered in this Standard as their usage is limited to high level officials and not to field operations.

(iii) Least significant bit (bit 6) indicates whether traffic is to be handled and delivered according connectionless or connection-oriented traffic handling functionalities. The coding of the bit indicates connectionless operation when valued as 0 (also meaning IANA/IETF standards action and thus providing easy co-operation with commercial providers), when valued as 1 meaning connection-oriented operation (also meaning

IANA/IETF experimental / local usage).

Commercial networks acting as individual network in FoN may interpret latter three bits (bits 4-6) as normal Assured Forwarding queue precedence bits. This means that they offer several classes of drop priorities to implement differentiated forwarding treatment within individual Service Class. This is also an option for networks which have network devices that do not support hierarchical queuing systems. In both of these cases network devices should be engineered in a way that packet dropping functions are cascaded to provide packet dropping on the order of precedence (lowest precedence packets are discarded completely before second lowest precedence packets are started to be discarded). It should be noted that in some cases network devices are not able to use bit 6 which leads to situation that CL domain serving CO connections is not capable of differentiate state full connection-oriented traffic from stateless connectionless traffic and thus will use same precedence dropping order for both CL and CO packets.

The receiving network element (adjacent domain in the FoN or delivering entity in the domain) MAY remark transit traffic within the national network to match the local marking scheme. If remarking takes place within domain, domain shall present the traffic at the egress IOP with the same marking that it had when received from the ingress IOP.

3.2.2. Service Classes

Applications and their traffic are bound to Service Classes (SC) which are based on RFC 4594 - Guidelines for DiffServ Service Classes and RFC 5127 – “Aggregation of DiffServ Service Classes”. These definitions are modified to be better in line with military requirements.

Table 4 show Service Classes (SC) which are used in this document with indicative tolerance to Key Performance Indicator (KPI)

Service Class	Tolerance to		
	Loss	Delay	Jitter
Circuit Emulation (TDMoIP) (SC7)	Very Low	Very Low	Very Low
Signaling, OAM, Network MGMT (SC6)	Low	Low	Medium
Voice (SC5)	Low	Low	Medium
Video (SC4)	Low - Medium	Low	Low
Transaction messaging (SC3)	Low – Medium	Medium	Medium
Low-Latency Data (SC2)	Low	Low - Medium	High
High-Throughput Data (SC1)	Low	Medium – High	High
Low-Priority Data (SC0)	High	High	High

Table 4 Service Classes and their quality constraints

3.2.3. Treatment Aggregates

The following (Table 5) four Treatment Aggregates (TA) based on RFC 5127 – “Aggregation of Diffserv Service Classes” are used in this document. Treatment aggregates can be used for mapping services to fewer than eight forwarding queues within network. Other formations of treatment aggregates are possible and are based on national interest / constraints.

Treatment Aggregate	Tolerance to		
	Loss	Delay	Jitter

Real-Time	Very Low	Very Low	Low
Near Real-Time	Low	Low – Medium	Medium
Assured Elastic	Low	Medium	High
Elastic	Medium	Medium – High	High

Table 5 Treatment Aggregates and their quality constraints

3.2.4. Military Precedence handling

Military Precedence is handled as a transmission priorities on IP layer – thus complying to the original operational ideology behind Military Precedence (seizing transmission resources for more important traffic on times when there are contention of resources).

IP Military Precedence Level (IP MPL) is a mapping of Military Precedence to the IP level (originally ToS packet precedence and nowadays to the Differentiated Services code point based on local agreement).

Precedence-level	**IPMPL-DSCP**
CL-Flash	xxx 010
CL-Immediate	xxx 100
CL-Priority	xxx 110
CL-Routine	xxx 000
CO-Flash	xxx 011
CO-Immediate	xxx 101
CO-Priority	xxx 111
CO-Routine	xxx 001

Table 6 Mapping between Military Precedence Level and DSCP-coding

By having two schemas for marking, a differentiation can be made between connection oriented and connectionless traffic within packet level. This is important for the cases where there is a connectionless domain interconnecting two connection oriented domains. IPMPL-values selected for the Flash, Immediate, Priority and Routine are based on the values used in Differentiated Services Assured Forwarding PHB (RFC 2597) and thus are supported with devices that implement regular DiffServ functionality through differentiated loss priorities in queue level. Value for the Routine is based on default Class Selector class value (00) and should be considered “best effort” within Service Class. All other precedence values within the Service Class are considered to provide better service than default class selector value (00). In this respect value for

the Priority is derived from the AFx3 (11) - the highest drop precedence value in AF drop precedence system, value for Immediate is derived from the AFx2 (10) – the middle drop precedence value in AF drop precedence system, and value for the Flash is derived from the AFx1 (01) – the lowest drop precedence value in AF drop precedence system.

When a connectionless domain is serving also connection oriented traffic, ordering of IPMPLs shall be based on notion that CO precedence overrides CL precedence ie. CO-Flash → CL-Flash → CO-Immediate → CL-Immediate → CO-Priority → CL-Priority → CO-Routine → CL-Routine.

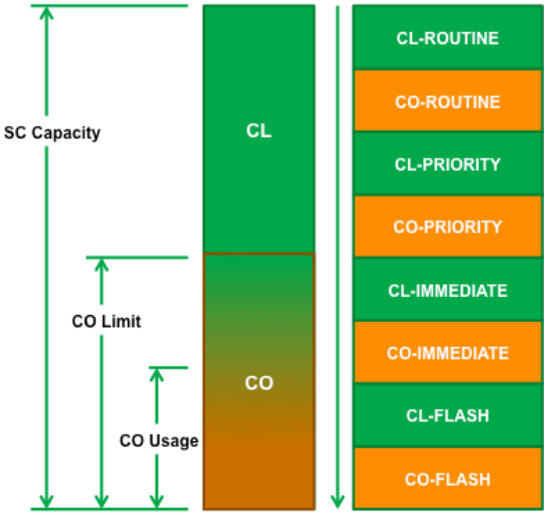


Figure 12 IP Military Precedence Level dropping order

Spirit of this standard is that implementation of service based on Service Class and IP MPL can be based on any possible combination of mechanisms as long as black box operation resembles following definition:

“Traffic signalling higher IP MPL should receive service before traffic signalling lower IP MPL taking into account rate allocations between Service Classes.”

This can be seen in the right hand side of the Figure 12, where dropping order of the packets from an individual Service Class is shown. The example shows the case when there are both CO- and CL-packets in a queue. Left hand side of the Figure 12 shows the principle of dividing link resources for one Service Class. Looking at these both sides of resource control, shows that under normal conditions CO has certain upper limit for usage in a Service Class, but when congested IP MPL dictates the order on which resources are granted to traffic. This is also important when CL-domain serves CO-domain, like in cases where true CO-functionality is not existing or when CL acts as a transit between two CO-domains. On those occasion true pre-emption is not available for CO-traffic and thus only local priority handling is given to the traffic.

This can be interpreted either by;

1. having link resources being shared by rate based scheduling between Service Classes and priority (based on IP MPL) based scheduling within Service Class, or

2. it may be based on link resource sharing by IP MPL with individual Service Class allocations across the priorities (token bucket rate controlled priority queues).

If the implementation does not support hierarchical scheduling, implementation may be based on link resource sharing using normal rate based queuing having weighted random early detection based precedence system within queues.

In both cases, operation of IP MPL is invisible when there are no congestion on the resources. Operation of MPL will become visible when link resources are congested and operative decision to use higher precedence for important traffic exists. In those occasions important traffic has priority to service or priority to queue space. Service Classes reveals itself during normal contention when packets are buffered and served based on the relative order of services. Relation of SCs is based on operation policy / QoS policy.

Implementation of this QoS Standard assumes hierarchical scheduling or at minimum novel differentiated services based system. At the time of writing this document, these features are existing on software based routers and some commercial platforms implementing rate based scheduling algorithms with priorities.

It is the intention of this IP QoS Standard to provide the best possible service to IP MPL Routine under normal network conditions with available resources. However, it is the intention of IP MPL to fully sacrifice packets signalling a lower MPL, in favour of packets signalling a higher IP MPL.

3.2.5. Traffic Classification

Traffic classification within individual network domain is a matter of individual network operator but traffic that is delivered over the IOP shall be classified by common interoperability schema. There are two options to build traffic classification:
Application/service driven approach where classification and marking of packets is based on application/service that generated the packet. This is used to deliver information across a network domain for the sake of processing at intervening network elements like firewalls.
Quality driven approach where traffic is classified based on their requirements from the network level QoS forwarding. This approach aims to optimize end-to-end QoS related existing domain based services.

Each source network shall mark all traffic which it presents at the IOP. In case traffic is not marked it should receive service of Low-Priority Data with Routine forwarding precedence (CS0:Routine).

The classification shall be according to the QoS policy of the operation.

3.2.6. QoS aware packet forwarding

QoS aware packet forwarding means that QoS information is used in conjunction with selecting the best path (if multi-topology routing is employed) and selecting the per domain/hop behaviour that best suits for particular Traffic Aggregate. QoS aware packet forwarding is domain dependent issue and is therefore not defined in this standard. However, packet forwarding at IOP level is defined at this standard.

Current technology standard for connectionless IP based IOPs is Differentiated Services as defined by RFC2475 – “An Architecture for Differentiated Services” and using interoperability service mapping as defined in this standard. There is an alternative approach to build interdomain QoS by extending the RFC2475 framework with capability of PDB selection negotiation (RFC 5160 “Considerations of Provider-to-Provider Agreements for Internet-Scale Quality of Service (QoS)”) but this framework has not yet received wide support.

This standard proposes an extension to RFC2475 framework by employing two dimensional time-based service differentiation for individual network domain. RFC2475 builds upon time-based differentiation provided by different Per Hop Behaviours (PHB) and queue space differentiation provided by adaptive queue management mechanisms within individual PHBs. This standard extends this model to provide two dimensions of time-based differentiation: one between PHBs (Service Classes) and one within PHB (Service Classes). This is done in order to cater military priorities with the option to have better control over the resource usage than by having adaptive queue management to decide the outcome of the military priority. Also time based differentiation within individual PHB enables the provision of a true Flash service.

Algorithms and processes implementing router functions on forwarding- and control plane are beyond the scope of this standard (it is assumed that where applicable standard procedures like “RFC 1812 - Requirements for IP Version 4 Routers” are followed).

3.2.7. QoS aware routing

QoS aware routing is a process which builds several forwarding trees over same network topology. These forwarding trees may be pre-processed for aggregate traffic elements like Treatment Aggregates or they may be processed on-demand by

resource management elements. Latter being the approach that several connection-oriented technologies use. Both of these approaches are built on the assumption that network status and capabilities can be inferred and distributed across network domain and in future across network domains. This distribution is often seen as a duty of routing protocol – especially in cases of link-state routing which naturally distributes link and nodal information. However, interdomain routing is policy oriented and thus not quality nor status oriented and in general distributes only the best outcome and thus does not provide opportunity to select multiple paths over the same network topology. This is however, active research topic at IETF and about to change in the future. It has been argued that this functionality would probably melt interdomain routing in global scale, as the potential amount of routing information would explode. For closed environments like military networks this will not be a problem.

QoS routing in intradomain is a matter of individual networks and is not therefore standardised in this document. QoS routing in interdomain belongs to the area of this standard, but as there is not yet consensus on the industry on how to do it, it is currently not defined in this standard.

3.3. ENGINEERING THE QOS

Engineering the quality in FoN is dependent of the following constraints:

(a) Are all users/networks operating based on common QoS policy

If an individual domain is not operating with the same principles, then usage of two dimensional forwarding control will not produce desired outcome as users will experience asymmetric performance, and would mean that in an operation, there would be a coalition partner not co-operating.

(b) Are all network ingresses regulated at the packet level

Regulation of traffic at the ingress is only a mean to secure network resources. Therefore, boundary agreement (SLA) between domains must exist. This boundary agreement reflects capabilities (SLS) of serving domain and operational demand (SLO and SLT) from the generating domain. The combination of SLS and SLT uniformly express what is the state-space that can be applied over the interconnection. It does not state global guarantee, only local capabilities. Traffic entering domain must be regulated at the ingress to prevent resource monopolization and starvation in serving domain based on transit and sourcing traffic from the generating domain.

(c) Are resources of the network uniformly communicated through routing metrics

Resources (mainly link capacities) should be communicated to the neighbouring domains by using resource metrics. It is advisable to use common reference bandwidth to express distance as a function of network resources. These metrics need to be mapped across routing protocols in a uniform way. Calculation of best routes should be based on optimality on resources and not on optimality on hop count. With the BGP Accumulated IGP Metric (AIGP) Attribute real cost of internal network domains can be signalled across the network. However, AIGP is not yet standardized and thus not available in commercial solutions. Also BGP MED can be used to signal internal costs across the domain, however path length usually overrides the MED values. Thus, in interim, coding of domain resources to the PATH length may be advisable.

(d) Are traffic within different classes shaped to the egress IOP

One aspect of quality control is the nature of forwarded traffic. Bursty data traffic uses network resources more aggressively than smooth voice traffic. This is due to temporal contention caused by multiplexed high speed bursts at the IOP. This multiplexing also causes unnecessary packet loss on the ingress policing of serving domain. Therefore, individual Service Classes or Treatment Aggregates need to be shaped to conform to boundary agreement (SLA) between generating and serving domains. Shaping is a process of virtual buffering where, packets are queued and served by non-work conserving scheduling thus leading to potential idling of network resources. This extra buffering increases delay over the IOP which, if not controlled carefully, can cause hundreds of milliseconds additional delay for E2E communication path. Correct parameterization of shaping buffers is necessary based on serving link speed and agreed service rate for shaped traffic aggregate.

Common QoS policy guides implementation and usage of levers that exist in the network for fine-tuning the network services to better match operational requirements. The most important lever is the IP Military Precedence Level which allows prioritizing mission critical traffic ahead of other traffic. This prioritizing is not pre-emption of communication services at the connection level, rather it provides packet level priority on scheduling services. Within an individual IP MPL, packets are transmitted based on resource policy between different Service Classes. It is assumed that current devices are not capable of handling large number of Service Classes and therefore Treatment Aggregates are defined. Treatment Aggregates are consolidated Service Classes serving multiple Service Classes with aggregated manner.

3.4. NPICS

NPICS stands for NATO Protocol Implementation Conformance Statement. NPICS collects statements of mandatory and optional items from this Annex into compact form - thus just reviewing content of NPICS, quick overview on major principles can be drawn. Fine-grained details and justifications are, however, within the Chapter itself.

QoS-1	Are all users/networks operating on a common QoS policy	00 on page 9	M	Yes [ ]
POLI-1	Are all network ingresses regulated at the packet level – policing	00 on page 9	M	Yes [ ]
SHAP-1	Are traffic within different service classes or treatment aggregates shaped at the network egress	00 on page 10	M	Yes [ ]
MARK-1	Marking of IP packets is done in the Differentiated Services Code Point Field of the IP header (DSCP) as described in RFC 2474.	0 on page 1	M	Yes [ ]
MARK-2	The source network SHALL mark all traffic which it presents at the IOP.	0 on page 3	M	Yes [ ]
MARK-3	The receiving network element MAY remark transit traffic within the national network to match the local scheme. If remarking takes place within domain, domain shall present the traffic at the remote IOP with the same marking that it had when received.	0 on page 3	M	Yes [ ]
MARK-4	Is the marking of IP Military Precedence Level (IP MPL) done according to the reference	00 on page 2 and 3.2.4 on page 5	MPL-1:M	Yes [ ]
MPL-1	Is the domain sourcing packets with IP MPL		O	Yes [ ] No [ ]

CLAS-1	Does the implementation support classification based on IP Military Precedence Level, at the IOP	0 on page 7	M	Yes [ ]
CLAS-2	Traffic marked with an unrecognized marking SHALL be given the service of standard traffic (CS0:Routine).	0 on page 7	M	Yes [ ]
SCHED-1	Does the implementation provide packet dropping according to signalled precedence (IP MPL)	3.2.4 on page 5	M	Yes [ ]
SCHED-2	Does a higher IP MPL receive service before a lower IP MPL, taking into account rate allocations between Service Classes	3.2.4 on page 5	M	Yes [ ]

3.5. SOME EXAMPLES ON MARKING DIFFERENT TYPES OF TRAFFIC..VOIP, EMAIL..NETW-CONTROL, MGMT, ETC.

These examples aim to demonstrate that more than one approach can be taken for the service based mapping based on either national aspiration or based on mission policy and operation type.

Table 7: An example of mapping applications to Service Classes and MPLs

Application Type	Protocol	Description	Service Class	MPL	BitCode
File Transfer	FTP,SCP	Bulk file transfer	SC0	Routine-Flash	000xx0
ExtraNet	HTTP	Webservice	SC0	Routine-Flash	000xx0
Email	SMTP	Email delivery	SC1	Routine-Flash	001xx0
SMS	SIP, IM	Short message transactions	SC2	Routine-Flash	010xx0
ERP	HTTP	SAP	SC2	Routine-Flash	010xx0
BMS	MIP	Battlefield management system	SC3	Routine-Flash	011xx0
BFT	NFFI	Blue force tracking	SC3	Routine-Flash	011xx0
BD	LDAP	Battlefield Directory Service	SC3	Routine-Flash	011xx0
Domain Name Service	DNS	Name service query - response	SC3	Routine-Flash	011xx0
Video	RTP	Video stream delivery	SC4	Routine-Flash	100xx0
Voice	RTP	Voice media stream	SC5	Routine-Flash	101xx0
Routing	BGP,MSDP	Interdomain routing	SC6	Flash	110010

Media routing-support	BGP	STANAG 4705 prefix exchange	SC6	Immediate	110100
Signaling	H.323	Session signaling	SC6	Immediate	110100
Signaling	SIP	Session signaling	SC6	Immediate	110100
Domain Name Service	DNS	Name service Zone Transfer	SC6	Immediate	110100
Security	IKE	Key negotiation	SC6	Priority	110110
Security	DPD	Liveness detection IPSEC	SC6	Priority	110110
OAM	BFD	Liveness detection for routing	SC6	Priority	110110
SNMP	SNMP	Network monitoring	SC6	Routine	110000
Synchronous Data	RTP,UDP	Streaming sensor data	SC7	Routine-Flash	111xx0
E1 over IP	TDMoIP	E1 circuit emulation	SC7	Routine-Flash	111xx0

Table 8: An example of mapping derived from French national QoS scheme. It should be noted that French national scheme is mainly based on previous ST4711/TN1417 works

Application Type	**Protocol**	**Description**	**BitCode**	**Derived Service Class**	**Derived MPL**
Others		Non categorized usage	000000	SC0	Routine
File Transfer	FTP,SCP	Bulk file transfer	001xx0	SC1	Priority-Flash
Email	SMTP	Email delivery	001xx0	SC1	Priority-Flash
Domain Name Service	DNS	Name service –Zone Transfer	001xx0	SC1	Priority-Flash
SMS	SIP, IM	Short message transactions	010xx0	SC2	Priority-Flash
ExtraNet	HTTP	Webservice	010xx0	SC2	Priority-Flash
ERP	HTTP	SAP	010xx0	SC2	Priority-Flash
OAM	SNMP, Syslog, COPS	Network management	010000	SC2	Routine
Authentication	Radius	AAA	010000	SC2	Routine
Administration	SSH	Remote Shell	010000	SC2	Routine
Directory Services	LDAP	LDAP query/response	010000	SC2	Routine
Common Services	DNS, NTP, DHCP	Common support services	010xx0	SC2	Priority-Flash
Multimedia Streaming		Broadcast, CCTV	011xx0	SC3	Priority-Flash
Tactical data links		Radar signals, data links	100000	SC4	Routine
Video	RTP	Video stream delivery	100xx0	SC4	Priority-Flash
Video	H.323	Video signalling	100xx0	SC4	Priority-Flash
Video	SIP	Video signalling	100xx0	SC4	Priority-Flash
Voice	RTP	Voice stream delivery	101xx0	SC5	Priority-Flash

Table 8: An example of mapping derived from French national QoS scheme. It should be noted that French national scheme is mainly based on previous ST4711/TN1417 works

Application Type	Protocol	Description	BitCode	Derived Service Class	Derived MPL
Voice	SIP	Voice signalling	101xx0	SC5	Priority-Flash
Voice	H.323	Voice signalling	101xx0	SC5	Priority-Flash
Network Control	BGP	Inter-domain routing	110000	SC6	Routine
Network Control	PIM	Multicast routing	110000	SC6	Routine
Network Control	RSVP	Network Signaling	110000	SC6	Routine
Network Control	SNMP	Alarms	110000	SC6	Routine
Network Control	ICMP	Error Messages	110000	SC6	Routine

INTENTIONALLY BLANK

CHAPTER 4 : TECHNICAL STANDARDS FOR CONNECTION-ORIENTED IP QOS

(INFORMATIVE)

4.1. INTRODUCTION

This Chapter is provided to build an understanding on how connection-oriented IP QoS can be provided. This Chapter is under development and shall be not be considered as mandatory. Also it should be noted that this Chapter will evolve and have normative structure in the future, when proper research and standardization work will finish. However, ground rules and foundations given in this Chapter are general and applicable to any solution at the end.

4.2. MOTIVATION

Internet Protocol (IP) is the predominant technology for NATO and NATO nations' communication networks. Where today NATO and many NATO nations still operate a parallel circuit switched network for voice telephony and other real-time services, migration to a full IP network (full IP network should be interpreted as a network that uses IP as service delivery platform and not necessarily as forwarding technology) is on going. This migration process towards a single IP service delivery platform for many of military communication services is often referred to as IP convergence.
It is expected that this migration will happen through stages where the first stage will be dominated by the connectionless IP service with Best Effort and Differentiated Services service models. At later stages more and more connection-oriented functionalities will be introduced through connection-oriented service architecture like Integrated Services, and traffic engineering solutions like Multiprotocol Label Switching or equivalent.

4.3. DESCRIPTION

The following subchapters will describe the functionality needed to realize connection-oriented QoS in IP layer. It builds upon the Connectionless IP QoS by introducing signalling and connection routing for hard reservations of capacity also forwarding plane functionalities that secure communication resources for stateful flows are expected to be in place. Other functions are similar to those in connectionless IP QoS and are not repeated here.

4.3.1. Connection oriented network architecture

Connection-oriented network architecture means a network which uses connection/session setup and teardown processes to select the best possible route and/or capacity reservation for every new connection attempt. This requires network level processing either at every router or management system capability to control all connection attempts. Both of these approaches require that network is capable to

interact with the user terminal and that network has to have certain level of distributed intelligence to make proper decisions whether or not accept new connections.

4.3.2. Signalling

Signalling is a process in which end user terminal requests network a connection to a selected destination for transmitting data with certain profile. This profile consists three distinct parts

1. Definition of filter that defines the packet flow that connection carries. This filter is usually so called five-tuple [srcIP, dstIP, protocol, srcPort, dstPort]

2. Definition of temporal traffic profile [Traffic Specification]. Usually this is a token bucket representation for the rate of a traffic stream. Token bucket parameters contain options to define peak rate, average rate and maximum burst size at peak rate when operating in on/off mode.

3. Definition for QoS level that network should deliver [Resource/Quality Specification]. This is usually expressed with following KPIs: delay, delay variation and loss rate. There can also be additional constraints for the service – like Service Class.

For IP networks there are two IP layer signalling protocols that are used and/or proposed:

1. Resource Reservation protocol (RSVP) that has long history and is adapted for usage in many networking scenarios. However, being relatively old protocol is has shown some difficulties in adaption to new services. RSVP was originally developed for Integrated Services (IntServ) architecture which was intended to be the QoS architecture for IP networks. However, IntServ showed some scaling issues due to large amount of state reservations within core of the network. One particular problem was simple reservation mode that RSVP supports (receiver oriented simplex reservations). However, RSVP is the most commonly used signalling protocol while it has large footprint on traffic engineering solutions based on MPLS technology.

2. Next Generation Signalling Systems (NSIS) is an attempt to redesign signalling protocol from the perspective of more versatile usage. It supports variety of signalling modes (receiver/sender orientation, simplex-duplex reservation). NSIS is also using SIP based approach is construction of signalling flow – packets are textually constructed which allows flexible parsing of information (however, it takes more computing power to realize same task as it takes with RSVP). NSIS has however, more generic structure which should give flexibility to use it for variety signalling purposes like SS#7 was used in PSTN.

4.3.3. Resource Reservation

Resource reservation is a part of Quality and Resource Management (QRM) process in which signalled connection attempt is either parsed locally hop by hop or sent to the processing in centralized resource management system. In both of these cases connection admission control is executed, where

1. For each connection request a path via which reservation must follow is calculated. This path may contain all IP level network hops or it may only contain some intermediate steps that reservation must follow. The execution of this step is dependent on whether task is executed locally within system or path was determined externally by path computation element. Distinct path or at the minimum next-hop is required before advancing next step of the process.

2. Resources in each step of the path are checked against existing resource consumption and requirements of a new connection. This process takes account reservation limit for the Service Class and also the precedence of the request with respect existing connections. If resources are available for a new connection a reservation is granted. If resources are not available precedence of the new connection is compared to the existing connections via route to the next-hop. If lower precedence connections contain requested amount of resources a conditional granting of resources is done (final granting is conditional to success of the reservation procedure on a full end-to-end path). If resources are not available on lower precedences, connection is revoked and proper signalling message is generated.

3. Connection is instantiated to the network devices by forming a state which binds traffic filter and connection resources. Instantiation is either done by

    a. source routing signalling messages via the path that was calculated from the ingress to the egress of network domain

    b. forming state via management action using protocols like COPS or ForCes to realize device level state

    Only at this stage seizure of resources from the lower precedence connections is executed and signalling message of the event is generated to the communicating parties whose connection was terminated.

Resource reservation MAY be done either at microflow level (for individual service requests) or at macroflow level (for individual Service Classes). Aggregating individual service requests to Service Class level implies that the isolation between microflows within Service Classes is lost but the complexity of resource management is diminished when planning and dimensioning of the network. This also helps in situations when

both connectionless and connection-oriented services are provided within the network and/or Service Classes are considered to be equally important from the mission perspective.

4.3.4. QoS Routing

QoS Routing is routing process which takes account different aspects of connection-oriented networking. Biggest challenge for the QoS routing is the distribution of topology and network status information across the whole network. There are working solutions for intra-domain topology and resource distribution like ISIS-TE and OSPF-TE where traffic engineering extensions to the link-state routing protocol facilitate building up a separate database called Traffic Engineering Database (TED). For inter-domain routing there is no counterpart which would distribute network status and all topological realisations. All existing protocols are based on distribution of ‘best’ path which is selected based on combination of optimality and local policy. Therefore, to facilitate real resilient QoS aware inter-domain routing, new functionalities need to be added to inter-domain routing architecture. There is work in progress proposals in IETF that overcome some of these limitations. However, their acceptance and time-frame is still unkown.

Roughly QoS routing can be divided into two different categories based on their

- Search algorithm

    1. Constraint based routing where network topology is pruned with links and nodes that are not able to serve request at hand. This incapability to serve may be due to lack of networking resources or lack for the support of functionalities. Constraint based routing in principle does not provide optimal route rather it provides first search result that fulfils the demand.

    2. Optimal QoS routing where network topology is pruned with links and nodes that are not able to serve request at hand and after which optimal routing decision is made based on combined KPIs that where provided to search algorithm. This leads to long computation time as search must go through all possible combinations of service path.

- Dynamicity

    1. Pre-calculated routes, where for each destination a pre-calculated route is cached to make decision process faster. Pre-calculation is usually executed based on some default KPI criterion (per Service Class or based on usual demand).

    2. On-demand calculation, where path is calculated when request arrives based on KPI criterion provided by the request. This is slower process

but search results path that is selected for that particular request.

Combining these approaches builds up the real solution for connection-oriented network service.

From the IOP perspective connection oriented service is divided into two distinct problems

1. Selection of proper egress point if that is not already given by the arriving request (if the request contains already chain of IOPs that it is commenced to travel, egress point selection is done by the source of the information)

2. Selection of proper forwarding path across the network domain between ingress and egress IOPs

4.3.5. Military Precedence and Pre-emption handling

Military Precedence is handled both at the connection layer and IP-layer as a transmission priority – thus complying to the original operational ideology behind Military Precedence (seizing transmission resources for more important traffic on times when there are contention of resources).
Military Pre-emption service seizes system facilities which are being used to serve lower precedence communications to meet the needs of communications of higher precedence. This seizure is implemented as signalling messages to both directions of connection to tear-down resources and to notify end-points about blockage.

4.4. NPICS

NPICS stands for NATO Protocol Implementation Conformance Statement. NPICS collects statements of mandatory and optional items from this Annex into compact form - thus just reviewing content of NPICS, quick overview on major principles can be drawn. Fine-grained details and justifications are, however, within the Chapter itself.

QoS-1	Are all users/networks operating on a common QoS policy		O	Yes [ ]
POLI-1	Are all network ingresses regulated at the packet level – policing		O	Yes [ ]
SHAP-1	Are traffic within different classes shaped at the network egress		O	Yes [ ]
MARK-1	Marking of IP packets is done in the Differentiated Services Code Point Field of the IP header (DSCP) as described in RFC 2474.		O	Yes [ ]
MARK-2	The source network SHALL mark all traffic which it presents at the IOP.		O	Yes [ ]
MARK-3	The receiving network element MAY remark transit traffic within the national network to match the local scheme. If remarking takes place within domain, domain shall present the traffic at the remote IOP with the same marking that it had when received.		O	Yes [ ]
MARK-4	Is the marking of IP Military Precedence Level (IP MPL) done according to the reference		MPL-1:O	Yes [ ]
MPL-1	Is the domain sourcing packets with IP MPL		O	Yes [ ] No [ ]

CLAS-1	Does the implementation support classification based on IP Military Precedence Level, at the IOP		O	Yes [ ]
CLAS-2	Traffic marked with an unrecognized marking SHALL be given the service of standard traffic (CS0:Routine).		O	Yes [ ]
SIG-1a	Does implementation support signalling over the IOP : RSVP		O	Yes [ ]
SIG-1b	Does implementation support signalling over the IOP : NSIS		O	Yes [ ]
QRM-2a	Does implementation provide Quality Resource Management by having reserved resources per microflow through the domain		O	Yes [ ]
QRM-2b	Does implementation provide Quality Resource Management by having reserved resources per Service Class through the domain		O	Yes [ ]
QRM-3	Does implementation provide Quality Resource Management by having military precedences on signaling		O	Yes [ ]
QRM-4	Does implementation provide Quality Resource Management by having support for resource pre-emption based on military precedences		O	Yes [ ]

INTENTIONALLY BLANK

CHAPTER 5 : TRAFFIC FLOW CONFIDENTIALITY (INFORMATIVE)

When data is transmitted over a network, protocols with specific headers are added. On Ethernet, information is transferred in frames of variable sizes and intervals. Even though using IPSec, a statistical analysis of sizes and intervals of packets can be performed revealing important information of the communication.

There are some mechanisms that can make it more difficult for doing such an analysis, thus providing TFC. By using encryption at lower layers, address and service hiding can be achieved.

Hiding sizes and intervals – volume confidentiality – by padding and/or fragmentation, are other means.

In the past, bits in the DSCP-field have been foreseen as a good place for signalling TFC. Though its need for standardization is recognized, it doesn't belong in a QoS-standard and should hence be described elsewhere.

Signalling of TFC should not be done utilizing the DSCP-field, instead other headers and fields like the security option in IP Options (see RFC-791 for IPv4 and RFC-5570 for IPv6) or utilising special signalling mechanisms like NSIS NAT/Firewall signalling layer protocol (see RFC-5973) are suggested.

INTENTIONALLY BLANK

ANNEX A: TERMS AND DEFINITIONS

- **Service Level Management (SLM):** Process that takes into account whole life cycle for a service between ‘customer’ and ‘provider’. Service being at this occasion transmission service between two IOPs of an individual networks.

- **Service Level Objective (SLO):** Qualitative metrics that define what kind of network service is required for executing the business driven goals. This is the foundation for communications policy derived from the operational policy and mission statement.

- **Service Level Target (SLT):** Quantitative metrics that define how service should be provisioned within individual networks and how they should perform as whole. SLTs form a foundation for network dimensioning and provisioning in the Network Operations process.

- **Service Level Agreement (SLA):** Contractual agreement between network stakeholders to provide services based on SLOs and SLTs. As well as processes that relate to reporting and support in case of degradations of service. SLAs are usually used as means to form legally binding contract between customer and provider. Customer uses SLA as a tool to manage their business related risks from network services by contracting services that meet the performance requirements of business, and by escalating violations in a process of pursuing litigations during service degradations. The provider uses SLAs as a mean to control risks which relate to the customers and to the business as whole. With proper processes SLA contacts provide means to steer network dimensioning and also steer new investments to the infrastructure. Properly executed SLA and service provisioning minimises litigations during service degradations (degraded network service is targeted to the customers that have lowest service availability at their SLA or that have lowest penalty). SLAs are always formed as daisy chains where one network is provider to another and customer to another. How this daisy chain scales is dependent on the type of SLA that is pursued.

- **Service Class (SC):** Grouping of user services based on the operational policy (usually with similar characteristics). User services grouped in a SC should have similar requirements with respect to transmission delay (D); delay variation (DV) = jitter (J); and loss rate (L). Several SCs may share a single Treatment Aggregate (TA) and thus have similar performance targets (SLTs), but are conditioned independently at the ingress of the network (e.g. admission control; policing) following the Service Level Agreement.

- **Treatment Aggregate (TA):** A grouping of one or several Service Classes to one network level service. TA aggregates SCs that share similar Service Level Targets

to a common forwarding behaviour within network. TAs are a matter for individual networks and as such out of the scope for this standard. However, they are used in this document to explain how individual networks may implement Service Level Management with different Network Operations processes and still fully comply with this standard.

- **Quality of Service (QoS):** The capability of a network to provide a certain level of service guarantee (dynamic, reactive, proactive, differentiated, statistic or absolute) to selected subsets of traffic utilizing shared transmission resources of finite capacity. Main difference between ordinary/civilian and military networks is the distribution of resources during congestion. During congestion each user in civilian network receives their fair share of network resources. This fair share is on the average equal on the core network but regulated to the SLA level at the entrance to the network. User perceived quality is also heavily dependent on the operation of end-system congestion control mechanisms (like TCP). While in military networks resources are granted first to the prioritized usage at the point of resource contention. This point of resource contention may be a pool of available connections, transmission capacity of an individual link or buffer space of a network device. Due to more transactional messaging nature of military applications, user perceived quality is less controlled by end-system congestion control mechanisms than in civilian networks. This document refers to QoS in military networks and thus assumes presence of prioritized traffic.

- **QoS aware forwarding:** Packets are forwarded by a router (or other forwarding device) using differentiated queuing and potentially differentiated dropping based on the delivery requirements of the packet.

- **QoS aware routing**: The path that information takes is dependent on the capability and / or performance of the transmission path with respect to delay, loss and/or throughput (Paths that cannot support the QoS requirement for a TA are not used for forwarding that particular TA). This process may involve policy-based routing; multi-topology routing; traffic engineering; and resource reservation mechanisms. QoS aware routing is a mandatory function for end-to-end SLAs and for end-to-end connection-oriented networking. However, it should be noted that at the moment there are no standardized solutions for inter-domain QoS routing.

- **Signalling**: Signalling implies indication of Service and/or Service Class either by explicit message exchange using a specific protocol based on technologies (i.e. RSVP, NSIS, H323, SIP, etc.) and/or by implicit indication using commonly agreed header values in data packets (i.e. IP DSCP header, ATM CLP header, MPLS EXP header). Protocol based signalling is mandatory for connection-oriented networks and service overlays while for connectionless networks they may be used together with bandwidth brokers to facilitate finer granularity of service control.

- **Guaranteed Service**: Service and/or Service Class that has absolute service guarantee and is engineered with resources allocated per cumulated peak bit rate of connections in the traffic class, or that traffic class is given strict priority over other traffic classes. In both cases strict policing needs to be applied at the boundary of the network in order to avoid traffic in this class to starve resources from other classes and to prevent surges between connections sharing the resources.

- **Assured Service**: Service and/or Service Class that has statistical service guarantee and is engineered in a way that allocated resources for this class are based on statistical analysis on cumulative rate of traffic in the traffic class. Statistical analysis is based on calculation of effective bandwidth e.g. average rate with certain level of acceptable packet loss (tail of the cumulative probability function for instantaneous rate is less than acceptable packet loss). This service also needs strict policing at the edge of the network to prevent surges between connections sharing the resources.

- **Differentiated Service (Relative Service):** Service that has relational service guarantee in contrast to other services within same category, and is engineered in a way that allocated resource for this class matches the expected amount of traffic and relative share of resources among other Service Classes using Differentiated Services. This ordering of Service Classes is based on resource sharing policy which implements the network QoS policy.

- **Military Precedence and Pre-emption service** (in commercial standard MLPP Multi-Level Precedence and Pre-emption) is the “core” of Military QoS – it aims to guarantee service to a user or service that must be able to communicate in all (also “critical”) situations. This service has two parts – precedence and pre-emption. Precedence involves assigning a priority level to a communication (i.e. traffic flow, message delivery, signalling path, etc.). Pre-emption involves the seizing of system facilities which are being used to serve lower precedence communications to meet the needs of communications of higher precedence. The Military Precedence and Pre-emption is applicable in all kinds of network services: connection oriented services (data and voice), message handling, connectionless packet based, etc.

- **Traffic Precedence** is the forwarding layer mechanism associated to a single link or queue to accomplish priority based forwarding of information (packet, frame, cell). Traffic Precedence implements MLPP Precedence functionality on a forwarding path as an independent entity and thus aims to support MLPP on devices and links that do not support it on a control plane. Typically precedence information is coded in header fields of delivered information: DSCP/ ToS precedence (type of traffic) for IP, Cell Loss priority for best effort ATM traffic class, MPLS traffic class (and payload type), etc.

- **Real-time service**: A service that has strict delay constraints. Typically the transmission must be guaranteed within a constant time limit (with a little or no delay variation). Often loss of information is preferred over variation of delay (very little or no buffering).

- **Near real-time service**: Near real-time service is a service that has implications of real-time service but with a relaxed manner. Near real-time service can be for example streaming of media or data over the network with certain level of delay and jitter compensation employed. It can also be signalling or other control plane action that has events across network that need to be processed in a timely manner but their execution is not synchronized.

- **Non real-time service**: A non real-time service has more relaxed delay constraints than a real-time service but usually has more stringent loss constraints. Typically delaying transmission of packets for a short period in time is preferred in favour of dropping the information.

- **Elastic**: An elastic service and traffic source is able to adjust its generated traffic volume based on the available capacity in the transmission path. This requires either co-operation from the network (explicit congestion notification) or inferring the status of the network by examining flow of the packets at the receiver and sender via return channel (TCP rate control and multilayer video systems).

- **Inelastic**: An inelastic service is a traffic source that cannot adjust its generated traffic volume and will generate a sustained load regardless of the available capacity. Inelastic traffic source is not capable of dynamically adjusting its bandwidth usage based on feedback from the network. A typical example is an UDP based service, such as voice over IP telephony or sensor systems like radars.

- **End-to-end: End-to-end (E2E)** is defined in this context as FoN network ingress to FoN network egress and therefore, does not take into account end-system internal processing.

- **Per Domain Behaviour (PDB)**: PDB is a black-box transfer function of a service that is going to be delivered over an individual network from ingress IOP to egress IOP. This PDB is a heuristic representation of service and mechanisms that are used to implement the service. PDB associated KPIs form a foundation to end-to-end service level metrics and also in future allow intelligent service level based routing decisions on a FoN scale.

- **Per Hop Behaviour (PHB)**: PHB is a black-box transfer function of services over a single hop in a network. In this case this hop is IOP which is a special case of the

network providing mapping between two independent PDBs operated by two entities. This document describes a Interoperability PHB which should be used to map two possibly different PDB structures on a border (IOP) in a common way and thus when used over the chain of network interconnections, allow coherent QoS throughout the network.

AComP-4711(A)(1)