

The use of Service Level Agreements in Tactical Military Coalition Force Networks

Ingvild Sorteberg,
Baseline Communications as, Havegt. 2, 2010 Strømmen, Norway
ingvild.sorteberg@baseline.no

Øivind Kure,
Q2S, NTNU, O.S. Bragstads plass 2E, N-7491 Trondheim, Norway
okure@q2s.ntnu.no

1 Abstract

Tactical military coalition force IP networks will have to offer Quality of Service (QoS). Service Level Agreements (SLA) and Service Level Specifications (SLS) are important elements of the QoS architecture in civilian networks. However, SLA/SLS in military coalition networks should not be applied in the same fashion as in a commercial network. Our contribution is to identify the useful role SLA/SLS can play in network engineering and QoS management of tactical coalition force networks. The SLS definition need to be more detailed than commercial SLS and its monitoring need to be performed on a finer timescale than in comparable commercial networks. The security architecture of military coalition networks may also restrict the monitoring and SLA management. Finally we sketch a measurement based approach showing how the SLS can be used in tactical coalition networks to support both call admission control and network engineering. Parts of this analysis include a discussion of SLS and the proposed NATO standards for tactical communications network.

2 Introduction

Service Level Agreements (SLA) can be used in Quality of Service (QoS) enabled Internet Protocol (IP) based networks to define the network service between consumers and producers of network services. In commercial networks the SLA and the Service Level Specification (SLS) define the network service, how it is measured, and possible penalties if the SLS is not met. SLAs are also used to regulate the interconnection between network providers.

Tactical military coalition force IP networks will to some extent mimic the consumer and supplier roles found in civilian networks. However the SLA and SLS will have different usages. This article discusses these differences and the implications SLA/SLS will have on such networks.

A tactical coalition network will have users and network elements from different nations. Although a coalition force will have common objectives, the network elements will also be used to ensure national political control over the individual elements of the force. In addition, some nations may have additional national objectives requiring communication resources. A tactical coalition network will therefore have a strong need to define and regulate the network service interfaces between the network elements constituting the coalition network.

Tactical coalition force networks are set up and reconfigured to meet operational demands. The links may have very limited bandwidth compared to commercial networks. They are also susceptible to wear and tear, due to accidents or hostile action, at a substantially shorter timescale compared to civilian networks. We also believe fluctuations in load will be higher; the traffic will vary with the operations combined with a higher frequency of link break and reconfigurations.

There are different security architectures being deployed in coalition networks. One approach is to have different trust levels for signaling and user traffic [5]. All signaling traffic is within the same common trust level allowing hop-by-hop signaling. Another approach is to have networks at different trust levels. In this case communication between networks at the same trust level is supported using encrypted tunnels. This does not permit hop-by-hop signaling.

In a coalition network we can not assume that all networks have the same level of trusted. The use of SLAs addresses the problems encountered when signaling between networks of different trust levels. In a situation where all networks and all network elements are at the same trust level other solutions may be more applicable.

A tactical coalition IP network may consist of number of local area networks (LAN) interconnected using military and commercial networks. The information is typically secured through the use of secure IP (IPsec) tunnels across the wide area network infrastructure, see **Error! Reference source not found.**

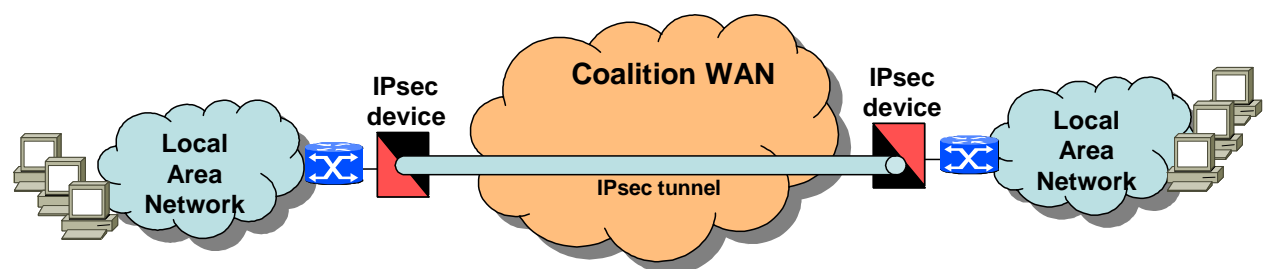


Figure 1: Secure military IP network architecture

Examples of this type of architecture can be found in the proposed NATO standards from the TACOMS Post 2000 project [10], experimental projects like the Interoperable Networks for Secure Communication (INSC) project conducted by several NATO countries as well as in operational military networks.

Tactical coalition networks represent a challenge for QoS provisioning, since the solutions will have to extend over different domains, where the security architecture may imply isolation of domains. The SLS at these boundaries are therefore important. Each domain can compare the offered or received traffic against a specification (SLS) and there is no need for call admission control or congestion notifications information to cross the boundary.

This article focuses on how the use of SLAs can support the planning and operation of military coalition networks. It looks at the technical aspects related to the support of SLA/SLS monitoring. It does not cover the organizational aspects of SLS setup and negotiation nor the management processes for traffic engineering. These are clearly military operational procedures and therefore outside the scope of any technical discussions. However, as we point out, such processes are more important than any technical mechanisms in order to have well functioning tactical coalition networks.

In the article we first present the state-of-art before discussing how the security and QoS architectures impact the use of SLS in military coalition networks. We describe in detail how the SLS can be used in both network engineering and call admission control to improve network responsiveness and the end-to-end service quality. Finally we present a measurement architecture to support SLS management in tactical coalition force networks.

3 Service Level Agreements (SLA)

A commercial SLA normally consists of three main parts. The contractual part includes information about the parties bound by the agreement, SLA contact information, review procedures, etc. The second part contains a description of the technical aspects including the product and service definitions, the user connections and the SLS which details the quality of the delivered services and any limitations imposed upon the user traffic (e.g. shaping and policing). The third part details administrative issues like fault and problem reporting procedures, prices, billing, and compensations.

3.1 Service Level Specification (SLS)

A network SLA identifies the IP performance levels that a network service provider guarantees. The technical specification of the connectivity service is given in the Service Level Specification (SLS). A definition of the term SLS is given in RFC3260 [1]: “A *Service Level Specification (SLS)* is a set of parameters and their values which together define the service offered to a traffic stream by a *Differentiated Service (DiffServ) domain*”.

The SLS needs to contain a description of the context and the actual parameters. The context includes the scope, the traffic classes, and the characteristics of the traffic it is valid for, for example burst and average rates. Potentially, the SLS can also contain a specification of the treatment of the traffic that is outside the agreed characteristics, for example whether it should be remarked or dropped. Once the context of the SLS is defined, the actual parameters for delay, loss, jitter and availability can be defined. The throughput is normally part of the context. If the bandwidth offered is not sufficient to meet the agreed service level, it will appear as a combination of excessive loss, delay and jitter.

An SLA may contain clauses stipulating compensation if the SLS is not met. This implies clear definitions of how the parameters in the SLS should be measured and monitored. The accuracy of the SLS may be considered a part of the SLS itself. Accurate measurements and monitoring require more resources, in terms of manpower, equipment, processing and bandwidth. It can therefore be an additional charged service.

3.2 Dynamic SLS

One challenging aspect is the granularity and the dynamics of the SLS invocation. The changing nature of tactical military networks demands dynamic SLS to ensure efficient utilization of resources and a predictable end-to-end QoS. As the network and traffic loads change, the SLS may have to be renegotiated.

While a broad static SLS is commonly used in the civilian market, dynamic service negotiation and invocation at the flow level have been the target of recent research projects funded by the European Union as part of their Information Society

Technologies (IST) program. Several proposed architectures [2], [3], [6], [8], [9] for dynamic SLS negotiation have been proposed. The different proposals do share some common elements, e.g. resource control and monitoring mechanisms and functions to control and dynamically distribute resources. However, the architectures represent different trade-offs between trust, granularity of the changes to the SLS, both in terms of timescale and delta in parameter value, and scalability.

The set of SLS that will have to be managed and negotiated may for some domains be the union of all SLS used in all domains. To provide a better ability to scale, it may be preferable to limit the SLS to a small set of SLS classes agreed by all domains [7].

3.3 Use of SLA/SLS in existing military networks

SLA/SLS are already used in military networks, primarily due to the increasing use of commercial service providers. In these cases, the SLAs are standard business agreements between military forces and commercial service providers. The main purposes are to ensure service delivery and if there are problems invoke measures to correct this.

However, the use of SLAs is also investigated with respect to tactical coalition networks and to manage the offering of services within national military networks. This differs from commercial SLAs both in terms of the goals and the usage. One initiative has come from the Tactical Communications (TACOMS) Post 2000 project which is a lead by NATO and where an industry consortium has developed a set of NATO Standardization Agreements (STANAG) [10] for the next generation Tactical Communications Networks.

TACOMS Post 2000 has defined a multi-technology network architecture and proposed standards for the functionality over the interface interconnecting different national tactical networks. One part of this is a set of SLS used to support the network engineering and planning processes [10].

The TACOMS Post 2000 project has defined two traffic handling classes, connection oriented and connectionless. The traffic handling classes are separated into different logical channels by the use of Multi-Protocol Label Switching (MPLS) at the interconnection point between two national networks. Within the two traffic handling classes, five classes of service are defined. SLS1 is always mapped to the connection oriented traffic handling class and SLS5 is always mapped to the connectionless traffic handling class. SLS2, SLS3 and SLS4 can be mapped to either traffic handling class and the choice of mapping is a deployment issue. The TACOMS Post 2000 SLS definitions are shown in Table 1.

The connection oriented traffic handling classes is used to support applications with stringent QoS requirements. It use a modified version of the H.323 signaling protocol to establish connections, request a SLS class for the particular flow and reserve resources. The connection oriented traffic is secured by the use of application encryption.

The connectionless interface is a standard IP based interface with DiffServ and will be used for all data traffic not requiring hard QoS guarantees. The connectionless traffic handling classes are mapped to an SLS classes using the DiffServ Code Point (DSCP). The connectionless traffic handling classes are secured through the use of IPsec tunnels.

SLS name	SLS name (mnemonic)	Characteristics	Use
SLS1	LR-LD-ML Low rate – Low Delay – Medium Loss	Stringent requirements concerning: delay and jitter	Suited for low bandwidth constant bit rate applications and applications that generate low bandwidth CBR flows (e.g. telephony).
SLS2	LR-LD-LL Low rate – Low Delay - Low Loss	Stringent requirements concerning loss probability	Suited for applications that require a very reliable delivery: Real-time data transfer, critical C4I messages, SMCS alarms
SLS3	MR-MD Med. Rate – Med. Delay – Med. Loss	Medium to high bandwidth requirements, and requirements concerning delay and jitter	Well suited for applications that generate medium bandwidth VBR flows (e.g. videoconference)
SLS4	HR-HD High Rate – High Delay – Med Loss	High bandwidth requirements	Streaming video
SLS5	NGD-PL Not Guaranteed Delay – Med Loss	Non-guaranteed delay and packet loss.	Similar to the “Best Effort” traffic in IP-based networks (the applications are assumed to implement some congestion control mechanism).

Table 1: The TACOMS Post 2000 SLS class definition [10].

The SLS defines the requirements towards the networks' performance characteristics. The requirements define the minimum and recommended number of interconnection points supported and the performance is defined by the maximum delay, jitter, packets loss and bandwidth requirements.

To verify the quality of the network services, TACOMS Post 2000 has defined a measurement architecture. Both end-to-end and per network monitoring is used to ensure that the networks comply with the target values defined in the SLS. Active measurements are used to monitor end-to-end or network element delay, jitter and packet loss. Passive measurements are used to determine network mean and peak load. Service quality measurements for the connection oriented traffic handling classes are done using synthetic flow generation. This means that the measurement probes must support the call signaling for the connection oriented traffic handling classes. The connectionless traffic handling classes are measured using active probing and correlating network statistics.

4 Future use of SLA/SLS in military networks

As already stated, we believe that SLA/SLSs are needed in military tactical coalition networks. However, they will have a different role compared to commercial networks, since they are operating on a different timescale, and breach of contract reflects a true degeneration of the network's available capacity.

4.1 Interdomain QoS and SLS

Interdomain QoS is the closest civilian equivalent to QoS management in coalition force networks. A common understanding of the most suitable architecture seems to be lacking and there are yet no Internet Engineering Task Force (IETF) groups chartered within this area. The Border Gateway Reservation Protocol (BGRP) [9] is an example of a proposed interdomain QoS solution that has not been implemented. BGRP supports QoS signaling and can be deployed in DiffServ based networks. It offers aggregation of resource reservations along the sink trees generated by the Border Gateway Protocol (BGP). The approach offers a simple solution to

interdomain QoS within one trust level, but one weakness is the convergence problems of BGP in dynamic non-hierarchical networks may result in difficulties to deploy this in a tactical coalition network, [11], [13]. Another problem with signaling based QoS regimes is the need for signaling proxy devices to support end-to-end signaling services. Therefore, the solution does not appear as a likely approach for tactical coalition networks.

Using dynamic SLS between the domains in a coalition force is an available method to ensure a common view of the network capabilities and service qualities supported by the networks.

4.2 SLA management

Commercial SLA/SLS are normally fairly static and are only renegotiated at predefined intervals, for example every 6-12 months. The changes negotiated or the establishment of new SLAs does not necessarily require changes to the provider's network topology since the networks are normally largely over-provisioned. However in tactical networks the SLA/SLS are less static due to frequent changes in topology, mobile networks and users. Also tactical networks operate at a higher utilization and they must be expected to be influenced by hostile actions and accidents. Therefore even minor changes to the SLA and the traffic load might trigger alterations to the core network topology, for example the need to establish additional links or change the network routing. Dynamic SLS negotiation can not be used if signaling from a low to a high security domain is not allowed, To support a very limited form of signaling, simple information guards are in some cases supported to allow predefined messages to pass between security domains.

In coalition networks, the main goals of the SLA/SLS are to define clear areas of responsibility between the different network managers, to support the network and traffic engineering and to ensure a predictable end-to-end service for the users by offering a traffic description that can be used as the basis for the QoS management and call admission control mechanisms. This usage is likely to result in that military SLA/SLS will differ from commercial SLA/SLS since the granularity and the dynamics of the information used to perform call admission control will be different from information used to support billing and accounting.

There are two main solutions for managing SLA/SLS, an end-to-end [3] approach and a cascaded approach [6]. In the end-to-end approach the SLA is negotiated directly with every network provider involved in constructing the end-to-end service. This requires that the path between the source and destination network is known in advance and in highly dynamic networks routes may change frequently requiring renegotiation and unnecessary service quality degradation. In the cascaded approach, the providers only negotiate with their immediate neighbors, see Figure 2. It offers a scalable and robust solution, and it is easier to adapt to a military environments where the networks experiences frequent rerouting.



Figure 2: Cascading SLA solution

The cascaded approach defined in [6] can not be applied directly across different security domains since it assumes that the SLS neighbors are the same as the BGP peers. In a network architecture using IPsec tunnels to protect traffic, the secure (red) networks do not have knowledge of their BGP peers only the destination networks and IPsec tunnel endpoints. The router on the black side has no knowledge of which neighbors are needed to support the IPsec tunnels so to make this work either an SLS needs to be negotiated with all neighbors or the black router needs to know about the active IPsec tunnel endpoints. Also, to our knowledge it has not been shown that the cascaded approach presented in [6] will converge in dynamic environments.

4.3 The role of SLS in network planning and engineering

The main difference in the use of SLS in military and civilian networks is in our opinion due to the dissimilarity in why the network becomes overloaded. In a civilian network, except for failure situations, network overload is most likely to occur if the operator overestimates the potential for multiplexing. Therefore the breach of contract clauses acts as a marginal cost of additional sale of multiplexing more traffic onto the existing network.

In a tactical network congestion is normal because bandwidth is usually very limited. Congestion can also be caused by accident, hostile actions, or a change in military objectives and therefore also priorities. The role of the SLS changes from a definition of a service guarantee to a definition of a mutual service quality target. Therefore the SLS will be important in the planning and engineering of military networks.

The operational network requirements for the coalition mission are detailed in the SLS and used in the network engineering activities. The engineering activities include designing the underlying network transport infrastructure, establishing routes and security tunnels and configuring QoS parameters. The SLS must offer information to support this level of network planning.

Figure 3 illustrates the relationship between the SLA/SLS and the network engineering process. The network engineering and SLS definition processes are iterative processes. The service level definitions and requirements for the operation are defined and together with the traffic forecasts used as input in the planning of the coalition network. If all the service requirements can not be met by the network, the SLS has to be altered. Ideally, these tasks and their interaction should be automated. In the next generation of QoS enabled tactical coalition IP networks this is not likely to be the case and a great deal of manual work is required to ensure that the service quality guarantees are supported and network changes implemented.

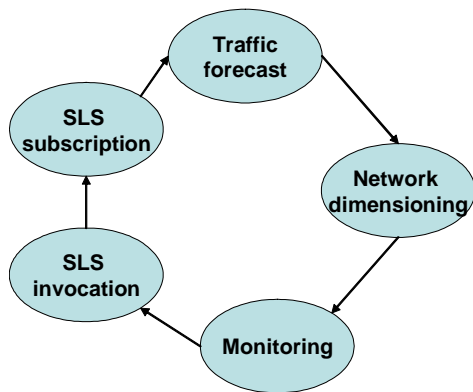


Figure 3: Integration of SLS management and network engineering and planning

Commercial SLS normally provides the traffic description on a per access basis since the core network is over-provisioned. In tactical networks, the core network will in many cases be the bottleneck. To engineer the core network topology, the SLS needs to define the traffic matrix at a finer granularity, most likely traffic loads need to be forecasted per tunnel and per class of service.

As the network becomes operational, traffic monitoring and fault detection tools will identify deterioration of the service quality. The network engineering process must be able to adapt the network infrastructure to support changes in the traffic characteristics and to handle network topology changes due to mobility or degradation.

The TACOMS Post 2000 SLS has been designed to mainly support the procurement and planning process, it does not include information about the traffic characteristics or procedures for handling excess traffic. The SLS can therefore not easily be used in the real-time network engineering process.

Careful network engineering is one approach to ensure the service quality and the goal is not to respond to fluctuations in the quality, but if the network has been overloaded over a period of time, the network engineering process will initiate actions to improve network conditions. Since these actions might require the establishment of additional radio trunks or satellite connections, the response times are in the orders of hours and days.

4.4 The role of SLS and call admission control

When the network quality deteriorates, the network engineering activities have a response time of hours and days and in some cases it will not be possible to continue to ensure the end-to-end quality unless traffic load into the network is reduced. The SLS is an important part of the traffic and QoS management in tactical coalition networks since it defines limits for the traffic load allowed into the network.

The solution offering the highest service guarantees is the use of hop-by-hop resource reservation before admitting any new flows. An example of this is the use of the Resource reSerVation Protocol (RSVP) to negotiate and reserve resources per network hop. The use of H.323 for the connection oriented traffic handling classes in TACOMS Post 2000 networks offers a similar functionality. The problem with hop-by-hop signaling is that it is difficult to support in military networks where signaling traffic can not go from less trusted to more trusted networks, for example in the use of IPsec. RSVP may also have limited ability to scale.

Therefore DiffServ seems to be the preferred QoS architecture. Strict priority schemes can be implemented with careful setting of the drop probabilities for the various DiffServ classes [12]. Within one DiffServ class, the packet loss will be evenly distributed. With limited congestion, the packet loss rate will still result in acceptable application performance, and no explicit limitation of new flows will be needed. However, there exists a load level where the packet loss rate impairs the applications. At such a level, a call admission control mechanism must be used to ensure that already initiated flows are allowed to terminate before new ones are added.

The goal of the call admission control is to prevent the access network from admitting more than acceptable amounts of traffic into a DiffServ class. Several alternative solutions can be used to support call admission control.

An alternative is the use of Bandwidth Brokers to negotiate changes to the SLS. The Bandwidth Broker holds an updated picture of the network status and the traffic load and based on this it determines if additional traffic flows are admitted into the network. This approach has been prototyped and tested in several research projects. However, one underlying assumption of these projects was the availability of additional capacity in the core network. Exceeding the SLS limits was used as a capacity buying indication to the core network provider. This is not necessarily the case for tactical military networks; also this approach does rely on signaling traffic traversing security domains.

A variation of this alternative is to use for example H.323/SIP gatekeepers which can be configured to only allow a certain number of simultaneously voice and video calls. The gatekeeper is then consulted before new calls are established. The main problem is that only applications using H.323 or SIP can be supported.

A third alternative is the use of measurement based call admission control, where the results of network and traffic measurements are used to determine if new flows can be admitted into the network. In a tactical coalition network using IPsec tunneling, this is an attractive solution since it does not require signaling information to flow between security domains. The problem is the cost of performing accurate measurements.

Combinations of the above schemes can also be used to offer different degrees of service guarantees. Except from hop-by-hop signaling solutions, resource control devices (e.g. H.323/SIP gatekeepers and Bandwidth Brokers) need to derive information about the traffic limits to impose from the SLS.

5 Monitoring and SLS management

We believe that SLS will become an important element in the network planning and engineering process and as input to the call admission control of IP based tactical coalition networks. DiffServ networks use packet drop and packet scheduling to ensure that the applications' QoS requirements are met. Such mechanisms need to be augmented with call admission control, to ensure that the capacity is used for something that is meaningful from an application and operational viewpoint.

We propose a measurement based solution integrated with SLS management, Figure 4. The monitoring devices support a distributed service quality measurement scheme and the SLS managers control that the end-to-end service qualities comply with the SLS descriptions.

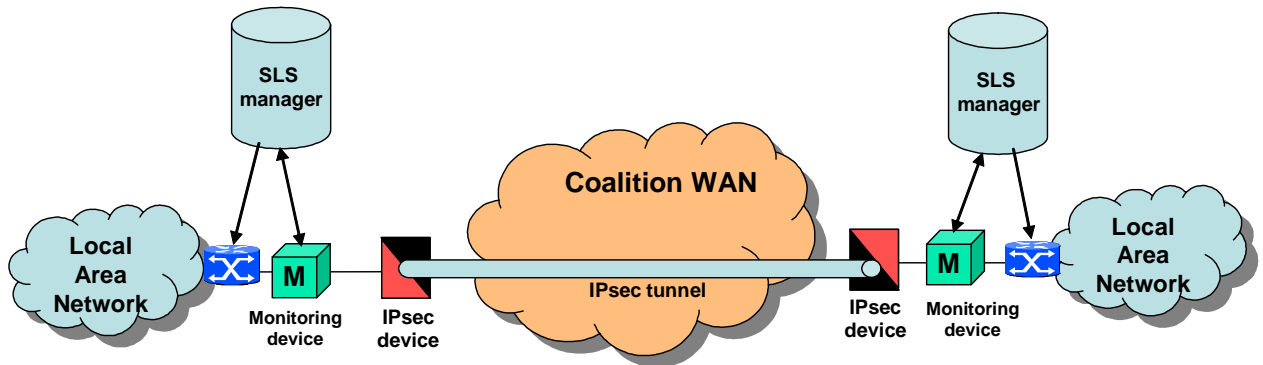


Figure 4: Architecture for measurement based call admission control integrated SLS management

The SLS definition must provide a description of the service quality per tunnel and per class of service since this is the granularity of the path selection. An example of a SLS template is shown in Table 2. The traffic parameters translate into QoS parameters to be configured in the edge router.

Corresponding LAN	Packet/flow identification	Total capacity	Classes of service supported and capacity per class	
LAN A	Tunnel end-points [src IP addr] [dest IPaddr] [DiffServ Code Point (DSCP)]	[kbps]	Voice	[No. of voice calls]
			Video	[kbps]
			High priority data	[kbps]
			Best effort	[kbps]
LAN B	Tunnel end-points [src IP addr] [dest IPaddr] [DiffServ Code Point (DSCP)]	[kbps]	Voice	[No. of voice calls]
			Video	[kbps]
			High priority data	[kbps]
			Best effort	[kbps]
LAN C	Tunnel end-points [src IP addr] [dest IPaddr] [DiffServ Code Point (DSCP)]	[kbps]	Voice	[No. of voice calls]
			Video	[kbps]
			High priority data	[kbps]
			Best effort	[kbps]

Table 2: SLS description template for IPsec tunnels originating from the same LAN

5.1 Monitoring

In a commercial setting, monitoring is used to ensure that the requirements being paid for are met. There is a large span of suitable measurement methods and in the granularity of the monitoring. For example with a trusted supplier, the monitoring may be infrequent or simply based on exception reporting.

In a tactical setting for coalition forces, the SLS still defines the requirements for a particular network connection. However, if the SLS is not met, this is an indication of a problem, and not a means for commercial compensation or litigation. Instead the implications are to reengineer the network and/or possibly change the call admission control parameters. This has implications on the monitoring methods and the required granularity.

The challenge when using a measurement based call admission control scheme is to ensure that the measurements quickly detect changes, but without loading the network with large amounts of measurement traffic. If the SLS cannot be met, the call admission control mechanism must adapt the load to the available resources. Otherwise the network will become congested and the service quality deteriorates for

all types of traffic. This will require measurements to be performed more or less continuously. The measurements also need to be fairly detailed since the call admission control needs to be performed per tunnel and per class of service.

We believe these requirements are best met with passive monitoring. Active monitoring of SLS is more of a value when the time average behavior is of interest, as it is in a commercial environment. In the tactical coalition force network, we argue that whether the SLS is met or not is of interest only when there is traffic, and therefore the traffic itself can be used as basis for monitoring.

It is an open issue whether all parameters of a SLS need to be monitored. If the network is correctly configured, loss and delay will increase only when the offered load exceeds the load agreed in the SLS or the network capacity has been reduced. With a focus on traffic engineering and call admission control, monitoring available capacity should be sufficient. In addition, if the admission target is reduced based on measurements, there has to be a symmetric process where the target is increased when resources become available. The monitoring must therefore detect significant changes in available resources. This requires active measurements, where the issues are overhead versus precision. This is discussed in more detail in the next section.

5.2 SLS manager

The SLS manager uses the measurement results to manage the call admission control mechanism. Deteriorating quality can easily be detected by observing the packet loss or by measuring an increase in the end-to-end delay. If the underlying network is not able to meet the requirements in the SLS, the call admission control mechanism loses its function. Instead, it is better to set the call admission control level to one that is commensurable with the available resources by letting the SLS manager switch to a different SLS and a different QoS configuration. For example depending on the scheduling algorithms used in the routers, it can be meaningful to shift offered load from one class to another. In a tactical network with DiffServ, it is therefore reasonable to assume sequences of defined SLS, one being the fallback of the previous. However, the effect will be limited unless all the affected networks respond to changes in the SLS.

If one allows for SLS to be downgraded, there need to be a symmetric process of upgrading SLS to take advantage of new resources. However, it is a more difficult to detect when additional resources become available. Active measurement methods to detect available capacity typically send packet trains with dynamically changing inter-packet spacing. Based on the perturbation of the inter-packet gap the available capacity can be estimated. One of the more effective methods is pathChirp [4]. It requires that the probing rate exceeds the available capacity for a short duration of time. Depending on the time between probes, the average probe traffic can be reduced to the desired level. In the reported results, the average probe traffic has been in the order of 1% to 5% to reach coefficient of variation in the order of 0.1.

These techniques are not well suited for DiffServ. They are based on temporarily offering a load larger than the available capacity. Such load runs the risk of being dropped or remarked, since the QoS configuration at the edge will limit the traffic flow into the core network not to exceed the SLS. Additional capacity can then not be detected. Instead, the QoS configuration will need to support a solution where the measurement traffic is not limited at the edge, but allowed to enter the core network and only dropped in the core if resources are not available. This is not an ideal

solution since it can cause congestion problems in the core network. An alternative solution with similar drawbacks could be to periodically upgrade downgraded SLS and measure whether the SLS is met. This may lead to unnecessary congestion or long lead times to discover available resources.

Another possibility is to implement an approach where the network manager in the coalition core network signals to the red LAN network whenever changes occur in the black network or which SLS to implement. This information can be sent from the black to the red network through a simple information guard. An information guard allows predefined information elements to be passed from the black to the red network, no information is allowed to flow in the opposite direction. The use of information guards are commonly used and normally allowed within the current security policies.

6 Conclusions

The use of SLA/SLS in military networks has been promoted by several military projects lately, the TACOMS Post 2000 project and the Interoperable Networks for Secure Communication (INSC) project being two examples.

The main difference between our proposal and the TACOMS Post 2000 proposal is that we advocate use of SLS information not only in the network planning and engineering process, but also integrate SLS management into the call admission control.

Our ideas correspond well with the work performed in the INSC project. The INSC QoS architecture is a pure DiffServ architecture. The project plans to test and experiment with the use of SLA/SLS to control the traffic load in the network by integrating the SLS management and the call admission control. The project does not plan to experiment with the use of SLA/SLS in the network engineering, but acknowledges the usefulness of this use of the SLA. The INSC solution is based on a limited exchange of topology information between security domains, not monitoring information as we have promoted in this article.

Several research projects are looking into the use of SLA/SLS in commercial networks, addressing both the need for dynamic SLS negotiation and invocation. The results from these projects are of interest, but it is important to recognize that the differences in the security architectures may impact the use of SLS, particularly in the context of call admission control.

7 Acknowledgements

Our analysis has benefited strongly from discussions with researchers within the TACOMS Post 2000 project and the INSC project. However, the views expressed in this article represent only the authors' opinions. Thanks to the reviewers who provided very helpful recommendations on how to clearly express our ideas.

8 References

- [1] D. Grossman, New Terminology and Clarifications for DiffServ, RFC 3260, April 2002.
- [2] P. Trimintzios, I. Andrikopoulos, G. Pavlou, C.F. Cavalcanti, D. Goderis, Y. T'Joens, P. Georgatsos, L. Georgiadis, D. Griffin, C. Jacquenet, R. Egan, G. Memenios, *An Architectural Framework for Providing QoS in IP Differentiated*

- Services Networks*, 7th IFIP/IEEE International Symposium on Integrated Network Management (IM 2001).
- [3] Olivier Dugeon, Ada Diaconescu, *From SLA to SLS up to QoS Control: The CADENUS framework*, World Telecommunication Congress, September 2002.
 - [4] V.J. Ribeiro, R.H. Riedi, R.G. Baraniuk, J. Navratil, L. Cottrell, *pathChirp: Efficient Available Bandwidth Estimation for Network Paths*, PAM2003 - The Passive and Active Measurement Workshop, San Diego, April 2003.
 - [5] R. Cole Jr., D. Kallgren, R. Hale, J.R. Davis, *Multilevel Secure Mixed-Media Communication Networks*, Military Communications Conference, MILCOM '89, Conference Record.1989 IEEE 15-18 Oct. 1989 Page(s):117 - 121 vol.1.
 - [6] M.P. Howarth, P. Flegkas, G. Pavlou, N. Wang, P. Trimintzios, D. Griffin, J. Griem, M. Boucadair, P. Morand, H. Asgari and P. Georgatsos, *Provisioning for Inter-domain quality of service: the MESCAL approach*, IEEE Communications Magazine, June 2005.
 - [7] P. Levis, M. Boucadair, P. Morand, P. Trimintzios, *The Meta-QoS-Class concept: a step towards global QoS inter-domain services*, Proc. IEEE Int. Conference on Software, Telecommunications and Computer Networks (SoftCOM 2004), October 2004.
 - [8] T. Engel, H. Granzer, B.F. Koch, M. Winter, P. Sampatakos, I.S. Venieris, H. Hussmann, F. Ricciato, S. Salsano, *AQUILA: adaptive resource control for QoS using an IP-based layered architecture*, Communications Magazine, IEEE Volume 41, Issue 1, Jan. 2003 Page(s):46 – 53.
 - [9] P. Pan, E. Hahne, and H. Schulzrinne, *BGRP: Sink-Tree-Based Aggregation for Inter-domain Reservations*, KICS 2000.
 - [10] Tactical Communications Post 2000 (TACOMS), *STANAG 4637: TACOMS HEAD STANAG (Draft edition 1)*, NATO Standardisation Agency (NSA), 2005.
 - [11] I. Sorteberg, *BGP Convergence in Military Coalition Networks*, Military Communications Conference 2004, Milcom 2004, Monterey, USA, October 2004.
 - [12] Ø. Kure, I. Sorteberg, K. Øvsthus, *Architecture for TDM Circuit Emulation over IP in Tactical Networks*, Military Communications Conference 2003, Milcom 2003, Boston, USA, October 2003.
 - [13] Linix Gao, Jennifer Rexford, *Stable Internet Routing Without Global Coordination*, IEEE/ACM Transactions on Networking, Dec 2001, pp. 681-692.