Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 4, 2013
S. Shah
P. Thubert
Cisco Systems
July 3, 2012

Differentiated Service Class Recommendations for LLN Traffic
draft-svshah-lln-diffserv-recommendations-00

Abstract

Differentiated services architecture is widely deployed in traditional networks. There exist well defined recommendations for the use of appropriate differentiated service classes for different types of traffic (eg. audio, video) in these networks. Per-Hop Behaviors are typically defined based on this recommendations. With emerging Low-power and Lossy Networks (LLNs), traffic originated in a LLN, such as metering, command and control, may transit over a converged campus IP network, or even a Wide Area Network, and will share resources with traditional classes of traffic such as voice, video and data. It is important to have defined differentiated services recommendations for LLN traffic to co-exist with traditional class of traffic.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

With emerged LLNs, it is anticipated that more and more such networks will be connected to existing Campus, WANs, Provider core networks. As deployments of LLNs grow, traffic out of such Networks will also grow which is to co-exist with traditional types of traffic. Per-Hop Behaviors (PHB) and Inter-domain Service Level Agreements (SLAs), not only at the LLN Border but also in the managed IP networks, will have to be defined considering all types of traffic.

We will first categorize different types of LLN traffic into service classes and then provide recommendations for Differentiated Service Code-Point(DSCP) for those service classes. Mechanisms to be used, like Traffic Conditioning and Active Queue Management, for differentiated services is well defined in RFC4594. This document does not focus to re-call them again here but the document will call out any specific mechanism that requires particular consideration. Though nodes inside LLNs MAY use code-points recommended here.

This document focuses on Diffserv recommendations for LLN class of traffic in managed IP networks outside of LLNs that is for the traffic from LLN to the Campus, WAN, Provider Core as well as for the traffic in the reverse direction. It does not focus on Diffserv architecture or any other QoS recommendations within the LLNs. Given constraints of LLNs and their unique requirements, it is expected of a focus within a separate efforts.

In Section 3 we categorize different types of traffic from Different LLNs. Section 4 recommends differentiated services, including DSCPs and QoS mechanics, for categorized classes of traffic. Section 5 evaluates one of the deployment scenario.

1.1. Definitions

DSCP: Differentiated Service Code Point. It is a 6-bits value in the TOS and Traffic Class field of the IPv4 and IPv6 header respectively. This 6-bits numerical value defines standard set of behavior to be performed by Differentiated Services capable hops.

Diffserv
Class: Diffser Class in this document is used to refer to DSCP code-point(s) and associated Per-hop Behaviors for it.

LLN: Low-power and lossy Network. Network constructed with sensors, actuators, routers that are low-power and with higher loss/ success transmission ratio, due to transmission medium and nature of dynamics of changing topology, compare to wired and other traditional networks.

SLA: Service Level Agreement. It is a collection of Traffic classification rules and set of services associated with each Traffic Class. Traffic classification may be defined based on just DSCP code-points or additionally (or otherwise) based on some other packet attributes.

WAN: Wide Area Network. Broader area of network that connects multiple LANs, LLNs to each other including LAN, LLN networks from different sites across regions.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119.

3. Application Types and Traffic Patterns

Different types of traffic can be collapsed into following network service classes.

- Alert signals
- Critical control signals
- Monitoring data
  - Video data
  - Query-based response data
  - Periodic reporting/logging, Software downloads

3.1. Alert signals

Alerts/alarms reporting fall in this category where such signal is triggered in a rare un-usual circumstances. An alert may be triggered for an example when environmental hazard level goes beyond certain threshold. Such alerts require to be reported with in the human tolerable time. Note that certain critical alert reporting in certain automation systems may be reported via very closely and tightly managed method that is not implemented within LLNs, due to the nature of transmission media of LLNs and due to the stringent latency requirement for those alerts. Such types of signals are not considered here since they are not within the scope of LLN or any other IP networks.

Examples :

- Environmental hazard level goes beyond certain threshold
- Measured blood pressure exceeds the threshold or a person falls to the ground
- Instructional triggers like start/stop traffic lights during certain critical event

Traffic Pattern:

Typically size of such packets is very small. any specific device of LLN is expected to trigger only handful of packets (may be only 1 packet). That too only during an event which is not a common occurrence.

In an affected vicinity, only a designated device or each affected devices may send alerts. In certain type of sensor networks, it is predictable and expected to have only a designated device to trigger such an alert while in certain other types scale number of alert flows may be expected.

Latency required for such traffic is not stringent but is to be within human tolerable time bound.

3.2. Control signals

Besides alerts, LLNs also trigger and/or receive different types of control signals, to/from control applications outside of LLNs. These control signals are important enough for the operation of sensors, actuators and underneath network. Administrator controlling applications, outside of LLN network, may trigger a control signal in response to alerts/data received from LLN (in some cases control signal trigger may be automated without explicit human interaction in the loop) or administrator may trigger an explicit control signal for a specific function.

Examples:

- auto [demand] response (e.g. manage peak load, service disconnect, start/stop street lights)
- manual remote service disconnect, remote demand reset

- open-loop regulatory control
- non-critical close-loop regulatory control
- trigger to start Video surveillance

Traffic Pattern:

Variable size packets but typically size of such packets is small. Certain control signals may be regular and so with number of devices in a particular LLN, it is predictable on average, how many such signals to expect. However, certain other control signals are irregular or on-demand.

Typically most of the open-loop, that requires manual interaction, signals are tolerant to latency above 1 second. Certain close-loop control signals require low jitter and low latency, latency in the order of 100s of ms.

Some of the tightly coupled closed loop control signals are very sensitive to latency and jitter. However they today, just like critical alerts, are implemented via other management methods outside of LLN.

3.3. Monitoring data

Reaction to control signals may initiate flow of data-traffic in either direction. Sensors/Actuators in LLNs may also trigger periodic data (eg. monitoring, reporting data). All different types of data may be categorized in following classes.

3.3.1. Video data

A very common example of this type of monitoring data is Video surveillance or Video feed, triggered thru control signals. This Video feed is typically from LLN towards an application outside of LLN.

Traffic Pattern:

Video frame size is expected to be big with a flow of variable rate.

3.3.2. Query based data

Application at the controller, outside the LLN, or user explicitly may launch query for the data. For example, query for an urban environmental data, query for health report etc. Since this data is query based data, it is important to report data with reasonable latency though not stringent. In addition, some periodic logging data also may require timely reporting and so may expect same type of service (eg. at-home health reporting).

Traffic Pattern:

Size of packets can vary from small to big. While rate may be predictable in some cases, in most of the cases traffic rate for such data is variable. The traffic is bursty in the nature.

3.3.3. Periodic reporting/logging, Software downloads

Many sensors/actuator in different LLNs report data periodically. With some exceptions, as mentioned above for healthcare monitoring logs, most of such data do not have any latency requirement and can be forwarded either thru lower priority assured forwarding or with service of store and forward or even best effort.

Sensors/actuators may require software/firmware upgrades where software/ firmware may be downloaded on demand bases. These upgrades and so downloads do not have stringent requirement of timely delivery to the accuracy of seconds. This data also can be forwarded thru lower priority assured forwarding.

Traffic Pattern:

Periodic reporting/logging typically can be predicated as constant rate. Data may be bursty in the nature. Software download data also may be bursty in nature. Such traffic is tolerant to jitter and latency.

3.4. Traffic Class Characteristics Table

Traffic Class Name	Traffic Characteristics	Tolerance to Loss	Tolerance to Delay	Tolerance to Jitter
Alerts/ alarms	Packet size = small Rate = typically 1-few packets Short lived flow Burst = not bursty	Low	Low	N/A
Control Signals	Packet size = variable, typically small Rate = few packets Short lived flow Burst = none to some-what	Yes	Low	Yes
Very low latency close-loop Control Signals	Packet size = variable, typically small Rate = few packets Short lived flow Burst = none to some-what	Low	Very Low	Low
Video Monitoring/feed	Packet size = big Rate = variable Long lived flow Burst = non-bursty	Low	Low - Medium	Low
Query-based Data	Packet size = variable Rate = variable Short lived elastic flow Burst = bursty	Low	Medium	Yes
Periodic Reporting/log, Software downloads	variable packet size, rate bursty	Yes	Medium - High	Yes

4. Differentiated Service recommendations for LLN traffic

4.1. Alert signals

Alerts/alarms signaling service requires transmission of few packets with low delay, tolerable to human. This requirement is very similar to signaling traffic in the traditional networks. Alert signals MAY use Diffserv code-point CS5.

4.2. Control signals

As described in earlier section, control signals over IP are divided in two categories. Control signals that require very low latency, service inline with EF PHB, and control signals that require low delay but do not mandate lowest latency. Service requirement for later class of control signals is very similar to service for signaling traffic in the traditional networks. Recommendation for this class of control signals is to use Diffserv code-point CS5.

Control signals, like some of the closed-loop signals, that require lower delay and jitter compare to CS5 class of control signals, are recommended to use EF Diffserv class. These control signals are expected to be of the small packet size and short-lived flows. Specifically while sharing EF class with voice traffic, any big control packets can cause additional latency to voice packets and so care MUST be taken either to use a different Diffserv class for them or compress such packets to smaller size.

4.3. Monitoring Data

4.3.1. Video Data

RFC4594 has well documented recommendations for different types of Video traffic. If there is any Video traffic from/to LLNs to/from outside of LLNs, they should use same recommended dscp from RFC4594. For example, surveillance video feed is recommended to use dscp CS3.

4.3.2. Query based data

Low latency data, like query based report and non-critical signals, is recommended to use AF2 assured forwarding service. Also, certain periodic reporting/logging data that are critical to be reported with regular interval with relatively low jitter is recommended to use AF2x service.

4.3.3. Periodic reporting/logging, Software downloads

Non-critical periodic reporting/logging and rest all other data MAY use AF1x or BE service class.

4.4. Summary of Differentiated Code-points and QoS Mechanics for them

- Alert Signals CS5

- Control Signaling CS5

- Lower latency control-signals EF

- Video broadcast/feed CS3

- Query-based data AF2x

- Assured monitoring data high throughput AF1x

- Best Effort monitoring data BE
  Reporting (periodic reporting.certain types of periodic monitoring MAY require assured forwarding)

Service Class	DSCP	Conditioning at DS Edge	PHB Used	Queuing	AQM
lower latency control signals	EF	Police using sr+bs Police using sr+bs	RFC3246	Priority	No
Alert signals/ Control signals	CS5	Police using sr+bs	RFC2474	Rate	No
Video feed	CS3	Police using sr+bs	RFC2474	Rate	No
Query- based Data	AF21 AF22 AF23	Using single-rate, three-color marker (such as RFC 2697)	RFC2597	Rate	Yes per DSCP
Periodic Reporting/ logging	AF11 AF12 AF13	Using two-rate, three-color marker (such as RFC 2698)	RFC2597	Rate	Yes per DSCP

* "sr+bs" represents a policing mechanism that provides single rate with burst size control [RFC4594]

5. Deployment Scenario

Industrial Automation, as described in [RFC5673] and [ISA100.11a], classifies different types of traffic in following six classes ranging in complexity from Class 5 to Class 0 where Class 0 is the most time sensitive class.

- o Safety
  - * Class 0: Emergency action - Always a critical function
- o Control
  - * Class 1: Closed-loop regulatory control - Often a critical function
  - * Class 2: Closed-loop supervisory control - Usually a non-critical function
  - * Class 3: Open-loop control - Operator takes action and controls the actuator (human in the loop)
- o Monitoring
  - * Class 4: Alerting - Short-term operational effect (for example, event-based maintenance)
  - * Class 5: Logging and downloading / uploading - No immediate operational consequence (e.g., history collection, sequence-of-events, preventive maintenance)

It might not be appropriate to transport Class 0 traffic over a wireless network or a multihop network, unless tight mechanisms are put in place such as TDM and frequency hopping. Today this class of traffic is expected to use other tightly managed method outside of IP networks. Excluding class 0 traffic, following table maps Class 1 thru Class 5 service classes to Diffserv code-point.

Service Class	DSCP
Class 1*	EF
Class 2	CS5
Class 3	CS5
Class 4	AF2x
class 5	AF1x/BE

* Any Class 1 traffic that requires very tight control over latency and jitter falls in the same category as Class 0 traffic.

6. Security Considerations

A typical trust model, as much is applicable in traditional networks, is applicable with LLN traffic as well. At the border of the LLN, a trust model needs to be established for any traffic coming out of LLN. Without appropriate trust model to accept/mark dscp code-point for LLN traffic, misbehaving flow may attack a specific Diffserv class disrupting expected service for other traffic from the same Diffserv class. Trust models are typically established at the border router by employing rate-limiting and even marking down dscp code-point to Best Effort for non-trusted flows or dropping them as required.

7. Acknowledgements

Thanks to Fred Baker for his valuable comments and suggestions.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4594] Babiarz, J., Chan, K., and F. Baker, "Configuration Guidelines for DiffServ Service Classes", RFC 4594, August 2006.

[RFC5127] Chan, K., Babiarz, J., and F. Baker, "Aggregation of Diffserv Service Classes", RFC 5127, February 2008.

[RFC5548] Dohler, M., Watteyne, T., Winter, T., and D. Barthel, "Routing Requirements for Urban Low-Power and Lossy Networks", RFC 5548, May 2009.

[RFC5673] Pister, K., Thubert, P., Dwars, S., and T. Phinney, "Industrial Routing Requirements in Low-Power and Lossy Networks", RFC 5673, October 2009.

[RFC5826] Brandt, A., Buron, J., and G. Porcu, "Home Automation Routing Requirements in Low-Power and Lossy Networks", RFC 5826, April 2010.

[RFC5867] Martocci, J., De Mil, P., Riou, N., and W. Vermeylen, "Building Automation Routing Requirements in Low-Power and Lossy Networks", RFC 5867, June 2010.

8.2. Informative References

[ISA100.11a]
ISA, "ISA-100.11a-2011 - Wireless systems for industrial automation: Process control and related applications", May 2011.

[RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, December 1998.

[RFC2475] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and W. Weiss, "An Architecture for Differentiated Services", RFC 2475, December 1998.

[RFC6272] Baker, F. and D. Meyer, "Internet Protocols for the Smart Grid", RFC 6272, June 2011.

Authors' Addresses

Shitanshu Shah
Cisco Systems
170 W. Tasman Drive
San Jose, CA 95134
US

Email: svshah@cisco.com

Pascal Thubert
Cisco Systems
Village d'Entreprises Green Side
400, Avenue de Roumanille
Batiment T3
Biot - Sophia Antipolis 06410
FRANCE

Email: pthubert@cisco.com