Quality of Service Challenges in IP Networks

Andrzej Jajszczyk
Department of Telecommunications
Hangzhou, China, August 25, 2008

Outline

• Introduction
• QoS Assurance
• Major Challenges
• Conclusion
Introduction

• Introduction
  – Basic Definitions
  – Overview of Standardization

• QoS Assurance

• Major Challenges

• Conclusion

Some Definitions

• Quality
  – ISO 8402: The totality of characteristics of an entity that bear on its ability to satisfy stated and implied needs
  – ISO 9000: Degree to which a set of inherent characteristics fulfills requirements

• Service
  – ITU-T Rec. X.790 Amd. 1 (96): This term represents telecommunication capabilities that the customer buys or leases from a service provider

• Quality of Service (QoS)
  – ITU-T Rec. E.800: The collective effect of service performances which determine the degree of satisfaction of a user of the service
Quality of Experience (QoE)  
ITU-T Rec. P.10/G.100 Amd. 1

• The overall acceptability of an application or service, as perceived subjectively by the end-user
  – Quality of Experience includes the complete end-to-end system effects (client, terminal, network, services infrastructure, etc.)
  – Overall acceptability may be influenced by user expectations and context

• QoE is a measure of the overall level of customer satisfaction with a vendor. QoE is related to but differs from QoS, which embodies the notion that hardware and software characteristics can be measured, improved and perhaps guaranteed. In contrast, QoE expresses user satisfaction both objectively and subjectively.
Overview of Standards
ITU-T E-Series

- **E.800 (08.1994)**
  Terms and definitions related to quality of service and network performance including dependability

- **E.801 (10.1996)**
  Framework for Service Quality Agreement

- **E.802 (02.2007)**
  Framework and methodologies for the determination and application of QoS parameters
Overview of Standards
ITU-T G-Series

• G.1000 (11/2001)  
  Communications quality of service:  
  A framework and definitions

• G.1010 (11/2001)  
  End-user multimedia QoS categories

• G.1020 (07/2006)  
  Performance parameter definitions for quality of speech  
  and other voiceband applications utilizing IP networks

• G.1030 (11/2005)  
  Estimating end-to-end performance in IP networks  
  for data applications

Overview of Standards
ITU-T Y-Series

• Y.1291 (05/2004)  
  An architectural framework for support of Quality of Service in packet networks

• Y.1540 (11/2007; Pre-published)  
  Internet protocol data communication service – IP packet transfer and availability performance parameters

• Y.1541 (02/2006)  
  Network performance objectives for IP-based services

• Y.1542 (07/2006)  
  Framework for achieving end-to-end IP performance objectives

• Y.1543 (11/2007; Pre-published)  
  Measurements in IP networks for inter-domain performance assessment
Some Performance Metrics (ITU-T Y.1540)

- IP Packet Transfer Delay (IPTD): upper bound on the mean end-to-end delay (UNI-to-UNI)
- IP Packet Delay Variation (IPDV): upper bound on the 1–10⁻³ quantile on the IPTD minus the minimum IPTD
- IP Packet Loss Ratio (IPLR): upper bound on the packet loss probability
- IP Packet Errored Ratio (IPER): upper bound on the number of errored packets per total packets sent
## IP Network QoS Classes (Y.1541)

<table>
<thead>
<tr>
<th>Network Performance Parameter</th>
<th>Network Performance Objective</th>
<th>Class 0</th>
<th>Class 1</th>
<th>Class 2</th>
<th>Class 3</th>
<th>Class 4</th>
<th>Class 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPTD</td>
<td>Upper bound on the mean IPTD</td>
<td>100 ms</td>
<td>400 ms</td>
<td>100 ms</td>
<td>400 ms</td>
<td>1 s</td>
<td>U</td>
</tr>
<tr>
<td>IPDV</td>
<td>Upper bound on the $1 - 10^{-3}$ quantile of IPTD minus the minimum IPTD</td>
<td>50 ms</td>
<td>50 ms</td>
<td>U</td>
<td>U</td>
<td>U</td>
<td>U</td>
</tr>
<tr>
<td>IPLR</td>
<td>Upper bound on the packet loss probability</td>
<td>$1 \times 10^{-3}$</td>
<td>$1 \times 10^{-3}$</td>
<td>$1 \times 10^{-3}$</td>
<td>$1 \times 10^{-3}$</td>
<td>$1 \times 10^{-3}$</td>
<td>U</td>
</tr>
<tr>
<td>IPER</td>
<td>Upper bound</td>
<td>$1 \times 10^{-4}$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>U</td>
</tr>
</tbody>
</table>

## QoS Assurance

- **Introduction**
- **QoS Assurance**
  - Available Mechanisms
  - Overprovisioning
  - IntServ
  - DiffServ
  - Others
- **Major Challenges**
- **Conclusion**
Available Mechanisms (Y.1291)

**Control Plane**
- Admission Control
- QoS Routing
- Resource Reservation

**Data Plane**
- Traffic Classification
- Congestion Avoidance
- Buffer Management
- Packet Marking
- Traffic Shaping
- Traffic Policing
- Queuing & Scheduling

Guidance for IP QoS Classes (Y.1541)

<table>
<thead>
<tr>
<th>QoS class</th>
<th>Applications (examples)</th>
<th>Node mechanisms</th>
<th>Network techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Real-time, jitter sensitive, high interaction (VoIP, VTC)</td>
<td>Separate queue with preferential servicing, traffic grooming</td>
<td>Constrained routing and distance</td>
</tr>
<tr>
<td>1</td>
<td>Real-time, jitter sensitive, interactive (VoIP, VTC)</td>
<td>Separate queue, drop priority</td>
<td>Less constrained routing and distances</td>
</tr>
<tr>
<td>2</td>
<td>Transaction data, highly interactive (signaling)</td>
<td>Separate queue, drop priority</td>
<td>Constrained routing and distance</td>
</tr>
<tr>
<td>3</td>
<td>Transaction data, interactive</td>
<td></td>
<td>Less constrained routing and distances</td>
</tr>
<tr>
<td>4</td>
<td>Low loss only (short transactions, bulk data, video streaming)</td>
<td>Long queue, drop priority</td>
<td>Any route/path</td>
</tr>
<tr>
<td>5</td>
<td>Traditional applications of default IP networks</td>
<td>Separate queue (lowest priority)</td>
<td>Any route/path</td>
</tr>
</tbody>
</table>
Best Effort Approach

• Three principles*
  – No traffic is denied admission to the network
  – All traffic is treated in the same manner
  – Traffic is transmitted in the best possible way given the available resources

• The default service offering in IP networks

• In case of congestion
  – Non-controlled delays
  – Non-controlled losses


Overprovisioning

• The approach is based on providing sufficient network capacity so that congestion will rarely occur

• Overprovisioning can work, provided availability of cheap resources

• Two properties:
  – Relying mainly on capacity for providing QoS
  – Using other traffic control mechanisms with discretion and not relying on resource reservation or admission control

Integrated Services (IntServ)

• Observation: A flow that experiences a service rate slightly higher than the flow’s data rate has a bounded delay (A. Parekh and R. Gallager)

• Components of the IntServ architecture include
  – A set of predefined service classes
  – A ReSerVation Protocol (RSVP) for setting up specific service parameters for a flow

• Problems
  – Limited scalability due to the fact that the amount of state information increases proportionally with the number of flows
  – Large overhead
  – Ubiquitous deployment is required for guaranteed service
  – High requirements on routers
  – Overkill for short-lived flows
  – Difficult charging

Differentiated Services (DiffServ)

• The basic assumption: scalability in the core

• Traffic entering a network is classified and conditioned at the boundaries of the network only, and assigned to different behavior aggregates

• Aggregated packet processing by a network node is called per hop behavior (PHB)

• Problems*
  – No performance guarantee
  – Only effective when there is traffic congestion and the amount of high priority traffic is small
  – The end user may not perceive the difference between DiffServ and Best Effort treatment

## IntServ and DiffServ Comparison

<table>
<thead>
<tr>
<th>Feature</th>
<th>IntServ</th>
<th>DiffServ</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS assurance</td>
<td>Per flow</td>
<td>Per aggregate</td>
</tr>
<tr>
<td>QoS assurance range</td>
<td>End-to-end (application-to-application)</td>
<td>Domain (edge-to-edge) or DiffServ region</td>
</tr>
<tr>
<td>Resource reservation</td>
<td>Controlled by application</td>
<td>Configured at edge nodes based on SLA</td>
</tr>
<tr>
<td>Resource management</td>
<td>Distributed</td>
<td>Centralized within DiffServ domain</td>
</tr>
<tr>
<td>Signaling</td>
<td>Dedicated protocol (RSVP)</td>
<td>Based on DSCP carried in IP packet header</td>
</tr>
<tr>
<td>Scalability</td>
<td>Not recommended for core networks</td>
<td>Scalable in all parts of network</td>
</tr>
<tr>
<td>Class of Service</td>
<td>GS, CL, BE</td>
<td>BE and a set of mechanisms for CoS design (EF and AF PHBs)</td>
</tr>
</tbody>
</table>


## Major Challenges

- **Introduction**
- **QoS Assurance**
  - **Major Challenges**
    - Network Neutrality
    - Quality of Recovery
    - End-to-End Interoperability
- **Conclusion**
Challenge 1: Network Neutrality

- The idea of Network Neutrality is that a user traffic is not discriminated at all in relation to traffic generated by other network users.
- Network Neutrality means no discrimination.
- Network Neutrality prevents Internet providers from speeding up or slowing down Web content based on its source, ownership or destination.
- Network Neutrality is the guiding principle that preserves the free and open Internet.

Network Neutrality Variations

- **Strict Network Neutrality**
  - no QoS allowed whatsoever

- **Reasonable Network Neutrality**
  - QoS is allowed, but the differentiation cannot be based on source, destination or the property of traffic.
  - For example, we can prioritize all VoIP traffic, but not VoIP coming from a certain application or source/destination.

- **No Network Neutrality policies/law**
  - just as today
Four Nightmares of Network Neutrality

- Inequity nightmare
  - “Advanced Internet” available to a small part of society
- Corporate bureaucracy nightmare
  - Web sites availability (a higher charge to some web sites)
- Bad incentive nightmare
  - ISPs promote only their own services and discriminate the competition
- Less innovative content nightmare
  - Business becomes more difficult for young, experimental ventures


QoS and Network Neutrality

- QoS is possible with Network Neutrality
- The differentiation must not be specific to a certain application
- IntServ cannot be used under Network Neutrality policies
- Using DiffServ is possible, however, brings opportunities to abuse
- Flow Aware Networking (or similar) would be suitable and risk-free
QoS-Aware Network Neutrality

- The concept based on Flow-Aware Networks (FAN)
- FAN: A proposal for realizing the data transfer with a guaranteed quality (S. Oueslati and J. Roberts)*
- Traffic is sent as flows:
  - Streaming (with priority)
  - Elastic
- A flow is a sequence of packets with a common “characteristic”
- The characteristic can be based on any field of the packets
- A flow usually exist for some period of time
- Implicit traffic classification


FAN Architecture

- Two main elements:
  - Admission control block
  - Scheduler block

![Diagram of FAN Architecture]
FAN Architecture, cont.

- **Scheduler block**
  - Packets are served in a proper way according to the scheduling algorithm
  - Two parameters are estimated:
    - fair_rate, i.e., the rate currently realized by elastic flows
    - priority_load, i.e., the measured quotient of the sum of the packet lengths (with a high priority) in a given time period to the length of this period

- **Admission control block**
  - Decides of accepting or rejecting the flows
  - Each packet is accepted in a congestionless state
  - Only packets of flows, which identifiers are written to the PFL (Protected Flow List) are accepted in the congestion state

---

Operation on PFL in FAN

- The identifier of each flow is added to PFL in congestionless state

---

```
New ID →

ID_3 elastic
ID_2 elastic
ID_1 streaming
ID_1 elastic

PFL
```

---

```
AC  Sch
congestionless
```

---
Operation on PFL in FAN

- No new identifiers can be added to PFL in congestion

FAN: Congestion Notification

- `min_fair_rate`: minimum allowed value of the `fair_rate` parameter
- `max_priority_load`: maximum allowed value of the `priority_load` parameter

\[
\text{if } \text{fair\_rate} < \text{min\_fair\_rate} \quad \text{or} \quad \text{priority\_load} > \text{max\_priority\_load} \\
\text{then} \\
\text{CONGESTION IS NOTIFIED}
\]
Admission Control in FAN

New flow

\[ fr > fr_{\text{min}} \]
\[ pl < pl_{\text{max}} \]

Yes \rightarrow Admit

No \rightarrow Block

\[ fr \] fair rate

\[ pl \] priority load

Flow Rates Under Congestion: Classic FIFO

[Graph showing flow rates over time]

Flow rate [Mbit/s]

Time [s]
Flow Rates Under Congestion: FAN

DiffServ vs. FAN

DiffServ
- Explicit classifier
- Admission control
- Class N
- Accept
- PHB₁
- PHBₙ
- Dropper

FAN
- Implicit classifier
- On PFL?
- Yes
- MBAC
- Add to PFL
- PFQ
- Reject
- Dropper

MBAC: Measurement Based Admission Control
Congestion Control in FAN

- It is impossible to begin, e.g., a VoIP call in the congestion state

- Solution: a congestion control mechanism*
  - Basic Flushing Mechanism (BFM): identifiers of all flows are removed from the PFL
  - Enhanced Flushing Mechanism (EFM): only identifiers of elastic flows are removed from the PFL
  - Remove Active Elastic Flows (RAEF)
  - Remove and Block Active Elastic Flows (RBAEF)


Enhanced Flushing Mechanism

- Identifiers of elastic flows are removed from the PFL in congestion
Enhanced Flushing Mechanism Example

Waiting Times for VoIP
Admission Control Routine in FAN with Differentiated Blocking

\[ fr > fr_{\text{min}} \quad pl < pl_{\text{max}} \]

New flow

Class selector

Standard class

Premium class

Yes

Admit

No

Block

Admit


Challenge 2: Quality of Recovery

• In Y.1540, availability is the sole network reliability parameter. A network portion is defined to be available over an observation period if the observed loss ratio is less than a specified threshold of 0.75

• Some other criteria used in other standards

• Need for a broader approach allowing carriers to guarantee an required level of resilience

• The answer: The Quality of Recovery (QoR) approach*

QoR: Main Assumptions

- Methodology is related to connection-oriented technology (especially MPLS and its derivatives)
- QoR is calculated for particular LSPs
- Parameters used as components
  - Probability that LSP fails → Availability of a connection, $A$
  - Transmission quality degradation after failure → Quality of the recovery path, $Q$
  - Inconvenience related to the recovery switching → Recovery time, $T$
  - Cost of the recovery → Bandwidth redundancy, $R$
  - Imperfections connected with recovery → Affected traffic, $L$

Quality of Recovery (QoR): Methodology

- Abstraction
  - Calculation of values describing parameters of a real network
  - Result: Vector of real parameters $\mathbf{v}_R = (A, B, T, R, L)$
- Normalization
  - Modification of parameter values after which they are placed in the $[0,1]$ interval
  - Result: Vector of unified parameters $\mathbf{v}_Q = (Q_A, Q_B, Q_T, Q_R, Q_L)$
- Applications
  - Study of interdependencies of selected parameters
  - Unified measure for evaluation of recovery procedures
  - SLA formulation and supervision
QoR: Availability Component

- **Abstraction**
  - Input: data measurement (MTBF, MTTR; e.g., cable cut assessment)
  - LSP’s availability calculation: based on complex reliability structures
  - For instance, 1+1 path protection: parallel-serial structure
  - Output: probability value \( A_{LSP} \in (0, 1) \)

- **Normalization**
  - Input: availability value
  - Input: operator’s policy
  - Input: client’s expectations
  - Output: normalized parameter

\[ Q_A = g(A), Q_A \in (0, 1) \]

---

QoR: Example of the Availability Component

**Normalization**

\[ Q_A = A^{13.5} \]
QoR in the Broader Sense: Example

\[ QoR = \frac{\sum_{i \in \{A,B,T,R,L\}} (\alpha_i \times Q_i)}{\sum_{i \in \{A,B,T,R,L\}} \alpha_i} \]

\[ \alpha_i = 1, \ i \in \{A,B,T,R,L\} \]

\[ \alpha_R = 4; \ \alpha_i = 1, \ i \in \{A,B,T,L\} \]

Challenge 3: End-to-End Interoperability

- Migration from multiservice network to multinetwork service
- Customer expectations have to be satisfied for End-to-End QoS
- **End-to-End** has a different meaning in various ITU-T recommendations
  - In voice quality recommendations, end-to-end means, for example, from mouth to ear.
  - Within the context of Y.1541, end-to-end is to be understood as from UNI-to-UNI
- Problem: Interworking of networks based on different standards
QoS Class Mapping – Y.1541/UMTS Example

Proposed Mapping:
- Y.1541 Class 0  UMTS “Conversational” Class
- Y.1541 Class 1  UMTS “Streaming” Class
- Y.1541 Classes 2-4  UMTS “Interactive” (Sub) Classes
- Y.1541 Class 5  UMTS “Background” Class

Observations:
- UMTS QoS Classes do not limit jitter
- Delay statistics differ (Y.1541 Mean vs. UMTS Maximum)
- UMTS “Interactive” priorities do not offer quantitative delay limits

Conclusion

- A high level challenge:
  - Assuring QoS without loosing the key advantage of IP networks, i.e., their simplicity and robustness

- Other important challenges:
  - Assuring QoS without discrimination of some users (Network Neutrality)
  - Assuring multidimensional QoS (multiplicity of QoS parameters)
  - Interoperability of networks using different QoS architectural frameworks

- QoS issues will determine further evolution of the Internet
Thank you for your attention!