RTCP Extensions for SSM Sessions with Unicast Feedback

Julian Chesterfield

Eve Schooler

Jörg Ott

AVT WG - 20 November 2002

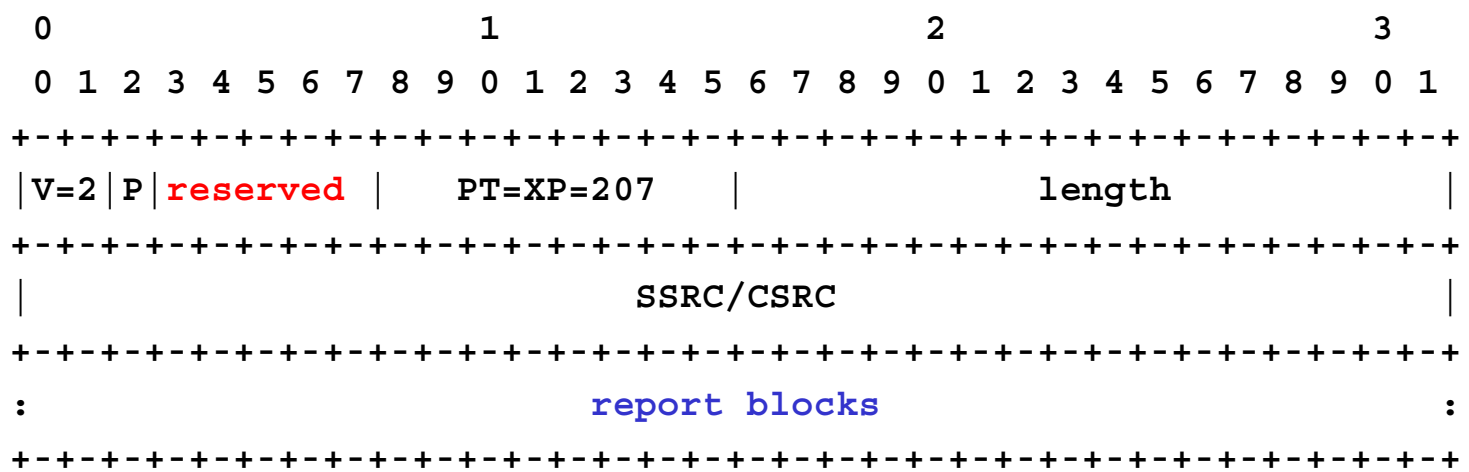
Changes

Really “work in progress”…

1. **Security considerations**
2. **Removed SSRC distribtion**
3. **Included cumulative value in distribution**
4. **Added Backwards-compatibility section**
5. **Specify IANA considerations more clearly**
6. **Use XR packet formats**
7. **SDP text modification**
8. **Signal feedback address in packet and specify rules of use**
9. **Examples as ASCII**

Packet Format

- **Alignment with XR packet format**
  - **PT = 207 (205, 206 taken by RTCP Feedback)**
- **New format to be developed**
  - **too many levels of indirection**
- **Align XR draft?**
  - **Smaller length field?**
  - **1 byte: 256*32 bits = 1024 bytes should suffice**


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
V=2
P
reserved
PT=XP=207
length
SSRC/CSRC
report blocks
0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
BT=24
subtype = 0
length
Timestamp
Group size
Receiver RTCP Bandwidth

Security Considerations

- **Significantly reworked**

Assumptions

- **Maintain low overhead on RTP entities**
- **Distribution of session parameters (SIP, SAP, HTTP, Mail, ...) beyond scope**
  - **Secure distribution assumed (authenticated!, possibly encrypted)**
- **Address transport layer and above**
  - **Problems inherent to SSM distribution need to be taken into account**

Threats

- **Denial-of-service**
  - **Particularly attacking or using the distribution source**
- **Packet forgery**
  - **RTCP packet contents influences session**
- **Session replay**
  - **May trigger feedback sent to distribution source**
- **Eavesdropping**
  - **May provide information to launch other attacks**

Source-to-Receiver

- **Source issues packets that control the operation of the entire session**
  - **Report bandwidth, group size, ...**
  - **RTCP target address**
- **Threats**
  - **DoS, packet forgery, session replay, eavesdropping**

- **Remedies:**
  - **Source authentication**
  - **Integrity protection**
  - **Confidentiality OPTIONAL**

Receiver-to-Source

- **Receiver input is reflected back**
  - **Indirectly in summary packets**
  - **Directly in simple forwarding mode**
- **Both impact processing at the source**
  - **False statistics information**
  - **Spoofed / false SSRC information**
    - Generate collisions
  - **Spoofed BYE packets**
  - **Also: replay**
- **Receivers may become DoS source**
- **Remedies:**
  - **Data integrity and authentication**
  - **Optional confidentiality**

Trust Models

- **Group authentication**
  - **shared key model**
  - **Assumes OOB key distribution mechanism**
  - **More efficient**
  - **Expensive to manage in large, dynamic groups**
  - **Group members may misbehave**
- **Source authentication**
  - **Easier for source-to-receiver path**
  - **Potential scalability problem**

Relations to other I-Ds

- **Report Extensions I-D**
  - **IANA Registry required**
  - **Publication times need to be aligned**
- **SSM Considerations for other I-Ds?**
  - **We have dealt with baseline RTCP messages right now.**
  - **What about newly defined ones?**

Open “Issues” / Next Steps

- **Add consideration for BYE packets**
- **Revise Message Format**
  - **Reorder description according to importance**
  - **Make receiver RTCP bandwidth optional**
  - **Align with other RTCP Extensions**
- **Add discussion section on general relation to other RTP/RTCP extensions**
- **Complete IANA registration section**
  - **SDP, XR packet formats, RSI registry**
- **Editorial cleanup**

- **Submit a revised draft in December**