draft-ietf-syslog-transport-udp

Internet Draft 00

Anton Okmianski
aokmians@cisco.com

Overview

- Standards Track Internet Draft
- Replaces informational RFC3164
- Defines UDP transport for syslog-protocol Internet Draft
- Syslog clients and servers MUST support UDP transport
- Defines UDP server port as 514

Transport

- One datagram per syslog message
- One datagram per syslog message part for multi-part syslog messages
- UDP checksums RECOMMENDED
- IP fragmentation SHOULD be avoided
- Recommends syslog payload of no more than 548 bytes to avoid fragmentation

Reliability Considerations

- Lost datagrams
- Corrupted datagrams
- No congestion control
- No sequenced delivery
- IP fragmentation increase risk of datagram loss

Security Considerations

- No message authenticity
- No strong authentication
- Message forgery possible
- Message observation possible
- Replay attacks possible
- Issues due to lack of reliability
- No prioritization
- Denial of service possible
- Covert channels possible