Research on the Problem of Big Datagram Outburst Transmission

To cite this article: Xiang Wang and Haixiao Chen 2018 IOP Conf. Ser.: Mater. Sci. Eng. 452 042078

View the article online for updates and enhancements.
Research on the Problem of Big Datagram Outburst Transmission

Xiang Wang*, Haixiao Chen*
China Satellite Maritime Measurement and Control Department, Jiangyin, China

*Corresponding author e-mail: wangxiang8606@163.com, *328165758@qq.com

Abstract. This paper analyses the transmission character of the high priority big data-gram in some network architecture adopting tunnel technology. Describe the second separation mechanism in the transmission progress. Design experiments to test the performance of router. Through the data analysis and experiments validation, get the reasons of packet loss in the outburst transmission, introduces how the high priority queue influence the lower. Some solutions have been proposed.

1. Introduction
With the development of the Internet, the scale and technology of the network are constantly expanding and developing. Various network services are emerging one after another. Users are not satisfied with the simple data transmission, but require more kinds of information transmission and information sharing services. As a result, network traffic continues to increase, and network behavior becomes more and more complex [1]. The advantage of IP networks is the integrated transmission of multimedia services such as data, voice, images and video. The IP bearer network serves as an integrated service network transmission and exchange platform. A highly stable and available network can ensure reliable operation of the business. It can guarantee to provide good quality of service to users, so that the delay, delay jitters and packet loss of the service on the network are controllable and predictable.

All kinds of real-time services generally use UDP transmission, and the video service has a large amount of information, and there are many single-frame data. As the traffic increases, the possibility of network congestion increases gradually [2]. In order to avoid congestion and ensure high-speed, high-reliability transmission of important data, the network edge router can classify the data stream according to different QoS (Quality of Service) requirements, and specify the corresponding DSCP (Differentiated Services Code Point Priority). The service priority flag is a value that aggregates the DSCP value and the flow to the same stream [3].

2. Question raised
In some networks, because the devices connected to the router's egress support insufficient multicast capability, such as MSS (Multi-Service Switch), or to improve the security of data transmission, tunnel technology will be adopted in the WAN router [4], as shown in Figure 1. AS1 and AS2 are Huawei Layer 3 switches, and R1 and R2 are Huawei NE20 series routers. The transmitted large packet application layer length is 6692 bytes. The access rate of the data transmitted by the PC1 is 2304 kbit/s, and the priority is set to EF (Expedited Forwarding) queue. The R1 of the router is limited
to 2560 kbit/s. The routers use GRE (Generic Routing Encapsulation) tunnel agreement. The data sent by PC1 has a constant rate of 2176 kbit/s on the order of seconds. When some burst traffic occurs, the data received by PC2 will be lost.

![Figure 1. Data transmission diagram](image)

3. Data Transmission Research

3.1. One split
According to the Ethernet protocol, the MTU (Maximum Transfer Unit) value of the Ethernet frame is 1518, that is, the transmitted data frame must not be larger than 1518 bytes (including the 14-byte header and the 4-byte end). The maximum length of the IP packet data field is 1480 bytes [5]. The length of the big data packet is 6692 bytes. When PC1 sends it, it will be divided into 5 pieces. The IP packet data field of the first 4 pieces (chips A, B, C, and D) is 1480 bytes long, and the last piece (chip E) The IP packet data field length is 780 bytes, where slice A contains the transport layer protocol UDP header and data, and the remaining four IP headers are encapsulated as pure data. The one-position big data packet in Figure 1 is split once, as shown in Figure 2.

![Figure 2. Schematic diagram of one split](image)

3.2. Secondary split
After the five-frame data split by the big data packet is sent to the NE20 router, the GRE tunneling protocol is adopted because the router exit uses the tunnel technology, and all the data forwarded on this interface needs to be GRE encapsulated. The GRE encapsulation needs to add a new IP header (the source destination address is the tunnel address of both ends) and the GRE header before the IP header of the original packet, and the size is 20 bytes and 4 bytes respectively, so that the length of 4 frames is long. For a data frame of 1518 bytes, its encapsulated length is 1542 bytes, which exceeds the maximum transmission frame length of the Ethernet link. Therefore, the router will perform GRE encapsulation on 5 pieces of data and then 4 the big data frame is split for the second time. A complete big data packet is split into 9 pieces in the 2 position of Figure 1 (slices A1, A2, B1, B2, C1, C2, D1, D2 and E’), as shown in Figures 3 to 5.
3.3. Packet Loss

Through the mirror port, Wireshark software is used to analyze the packet capture of the incoming and outgoing routers [6]. It is found that the transmission order of the router exit fragments is out of order, and the order between the slices of slices A to D is unchanged, and the slice E the transmission is sent randomly, as shown in Figure 6. When a packet loss occurs, the router does not completely discard all the fragments of the frame. Instead, it discards two of the nine fragments, one random is the number 1 fragment, and one random is the number 2 fragment. As a result, the frame cannot be reorganized.
4. Analysis of packet loss mechanism
In order to verify whether the packet loss is caused by insufficient router processing capability, relevant test verification is performed. Under the condition that the interval of sending packets is constant and the rate limit of the router is slightly larger than the traffic of large packets, all data can be transmitted normally without packet loss. As shown in Table 1, the processing capability of the NE20 router meets the requirements.

Table 1. Equal-interval data transmission and reception test results

| Packet rate (packet/second) | Packet interval (ms) | Routing rate limit (bit/s) | Access service rate limit (bit/s) | Actual rate (bit/s) | Number of transmissions | Number of lost packets |
|-----------------------------|----------------------|---------------------------|----------------------------------|--------------------|------------------------|-----------------------|
| 32                          | 25                   | 2560k                     | 2304k                            | 1.8M               | 31,236                 | 0                     |
| 66                          | 15                   | 5.4M                      |                                  | 3.6M               | 20,678                 | 0                     |
| 200                         | 5                    | 15M                       |                                  | 11M                | 20,128                 | 0                     |
| 500                         | 2                    | 30M                       | Cancel the speed limit, retain the priority label | 27M                | 59,969                 | 0                     |

In order to obtain the different priority queue lengths of the NE20 routers, the corresponding bearer capabilities of the BE (Best Effort) priority queue and the EF priority queue are tested under different rate limiting bandwidths. The results are shown in Table 2.

Table 2. NE20 router bearer burst capability test

| Speed limit bandwidth | Frame length | BE priority queue | EF priority queue |
|-----------------------|--------------|-------------------|-------------------|
| 256kbit/s             | 1518Byte     | 11                | 65                |
| 2048kbit/s            | 1518Byte     | 11                | 67                |
| 6912kbit/s            | 1518Byte     | 11                | 70                |
| 14912kbit/s           | 1518Byte     | 13                | 76                |
| 25000kbit/s           | 1518Byte     | 13                | 86                |

Remarks: The length of the BE queue and EF queue in the table is a multiple of 1500 Byte. For example, 11 represents 11×1500 Byte.

In order to test the performance of the forwarding burst data of the NE20 router, the data sent on the PC1 has a constant rate of 2176 kbit/s in the order of seconds, and the burst amount is continuously increased in the order of milliseconds, and the results are shown in Table 3.
Table 3. Burst flow test

| The way | Outsourcing characteristics | Number of transmissions | Number of lost packets | Packet loss rate |
|---------|----------------------------|-------------------------|-----------------------|-----------------|
| Uniform | 25ms one pack evenly       | 20000                   | 0                     | 0%              |
|         | 1ms, 49ms loop            | 20000                   | 0                     | 0%              |
| Burst   | 2 consecutive 1ms, 73ms loop | 20000                   | 0                     | 0%              |
|         | 13 consecutive 1ms, 337ms loop | 20000                   | 0                     | 0%              |
|         | 14 consecutive 1ms, 361ms loop | 20000                   | 4                     | 0.02%           |
|         | 15 consecutive 1ms, 385ms loop | 3233                    | 206                   | 6.4%            |

A dual-flow test is performed under the condition that a single-stream burst test does not cause packet loss to verify the impact of the EF queue on other priority queues. PC1 sends a large packet with priority EF, and the rate is constant at 2176 kbit/s in the order of milliseconds, increasing the burst amount on the order of milliseconds. At the same time, a normal service data stream is sent, the priority is BE, and PC2 performs data reception. The test results are shown in Table 4.

Table 4. EF queue impact test results of BE queue

| The way | priority | Outsourcing characteristics | Number of transmissions | Number of lost packets | Packet loss rate |
|---------|----------|----------------------------|-------------------------|-----------------------|-----------------|
| Uniform | EF       | 25ms a pack                | 12000                   | 0                     | 0%              |
|         | BE       | 10ms a pack                | 30000                   | 0                     | 0%              |
| Burst 1 | EF       | 1ms, 49ms cycle            | 12000                   | 0                     | 0%              |
|         | BE       | 10ms a pack                | 30000                   | 0                     | 0%              |
| Burst 2 | EF       | 2 consecutive 1ms, 73ms cycle | 12000                   | 0                     | 0%              |
|         | BE       | 10ms a pack                | 30000                   | 3998                  | 13.3%           |
| Burst 3 | EF       | 13 consecutive 1ms, 337ms cycle | 12000                   | 0                     | 0%              |
|         | BE       | 10ms a pack                | 30000                   | 15050                 | 51.3%           |

Set the priority of the normal service data flow to AF31 (Assured Forwarding). The test results are shown in Table 5. The AF31 queue of the NE20 router is more powerful than the BE queue against the EF queue burst traffic. The cache test of the AF31 queue data transmission of the NE20 router alone is about 63KByte (more than 15KByte of the BE queue cache).

Table 5. EF queue impact test results on AF31 queue

| The way | priority | Outsourcing characteristics | Number of transmissions | Number of lost packets | Packet loss rate |
|---------|----------|----------------------------|-------------------------|-----------------------|-----------------|
| Uniform | EF       | 25ms a pack                | 12000                   | 0                     | 0%              |
|         | AF31     | 10ms a pack                | 30000                   | 0                     | 0%              |
| Burst 1 | EF       | 8 consecutive 1ms, 193ms cycle | 12000                   | 0                     | 0%              |
|         | AF31     | 10ms a pack                | 30000                   | 0                     | 0%              |
| Burst 2 | EF       | 9 consecutive 1ms, 73ms cycle | 12000                   | 0                     | 0%              |
|         | AF31     | 10ms a pack                | 30000                   | 147                   | 0.49%           |
| Burst 3 | EF       | 13 consecutive 1ms, 337ms cycle | 12000                   | 18                    | 0.15%           |
|         | AF31     | 10ms a pack                | 30000                   | 5384                  | 17.9%           |

In the large data packet transmission process of Figure 1, the PQ (Priority Queening) scheduling mechanism of the physical port HQoS of the NE20 router does not function for the GRE tunnel encapsulation packets generated in the device. The GRE encapsulated packets are directly exported. The BE queue cannot be scheduled for PQ according to the DSCP value of the packet. All IP packets
are forwarded to the routers BE priority queue. Even if the IP packets are set to the EF priority, they can only enter the exit BE priority queue. When the burst traffic is large, packet loss occurs. The EF queue affects the queues of other priorities. The lower the priority, the greater the impact.

5. Solutions
In the case that the data transmission mode cannot be adjusted, the following three methods for avoiding packet loss can be used in a specific network with large data packet burst transmission:

1) Adjust the speed limit method. The access switch is added to the back end of the router to remove the rate limit policy of the router. The rate limit is adopted by the physical rate limit on the access switch. After the actual environment is verified, the method can effectively achieve the rate limit. However, this method adds a link in the link to reduce the reliability of the link.

2) Increase the speed limit rate. If the rate limit is adjusted to 15 Mbit/s, packet loss can be avoided. However, increasing the rate limit rate cannot overcome the impact of sudden abnormal traffic in the network. After the rate limit policy is adjusted to 15 Mbit/s, the packet loss phenomenon disappears. This indicates that the increase of the rate limit in the HQoS policy of the router can reduce or even avoid the impact on the cache queue size of the high priority packet storage and the speed limit. It also directly increases the sending rate of the egress, which is more conducive to the timely clearing of the store-and-forward cache queue, and avoids packet loss caused by the buffer queue overflow.

3) Remove the router speed limit. Practice has proved that removing the router speed limit can avoid packet loss. The network access switch sets a fixed transmission rate for the traffic flow rate limit or the access terminal, and the average traffic of the WAN data transmitted by the router in real time is lower than the available bandwidth.

6. Conclusion
In the process of network construction, it is necessary to conduct necessary analysis on the characteristics of the transmitted data, and conduct adequate research and preparation for possible abnormal situations. The transmission of key data should be avoided as much as possible, and the smooth way can improve reliability and reduce the possibility of packet loss. The transmission of large data packets should avoid multiple splits as much as possible, and reduce the uncertainties caused by the quality of service settings. In order to prevent problems before they occur, the critical network needs to establish a scientific network service data specification mechanism, analyze the impact domains of all network running business systems, and limit the important parameters of each system transmission data to ensure data transmission security and stability, reducing the risk of various abnormal conditions.

References
[1] FAN Fei, ZHAO Hui, YAN Xu, CHEN Lue. Information Traffic Monitoring and Control Technology and Its Application. Journal of Spacecraft TT&C Technology, Vol.8 (2011) No.4, p.30.
[2] LI Jian-ying, ZHAO Zong-yin. Study on Design of End-to-End Guaranteed QoS for a Private IP network. Journal of Spacecraft TT&C Technology, Vol.2 (2010) No.1, p.29.
[3] GE Lian-sheng, JIANG Lin, QIN Feng-lin. A survey of QoS multicast routing algorithms. Journal of Shangdong University(Natural Science, Vol.1(2010) No.45, p.56-57.
[4] LV Hui, HE Yan-xiang, TU Hang. Multicast Joining Algorithm with QoS Constraints. Journal of Wuhan University of Technology, Vol.10 (2010) No.32, p.201-202.
[5] GAO Lei, ZHANG Deyun, ZHAO Dongping, ZHENG Weibin. Research on Big Datagram Problem of Hop Integrity. Computer Engineer, Vol.6 (2005) No.12, p.31.
[6] TANG Miao, WANG Chen-chen, ZHOU Yang-hui. Policy of reliability and analysis of questions in the communication IP network. Electronic Design Engineering,Vol.9 (2011) No.18, p.19.