WAN Transmission Acceleration

Technology White Paper

Ruijie

Copyright Statement

Ruijie Networks©2000-2017

Ruijie Networks reserves all copyrights of this document. Any reproduction, excerption, backup, modification, transmission, translation or commercial use of this document or any portion of this document, in any form or by any means, without the prior written consent of Ruijie Networks is prohibited.

Exemption Statement

This document is provided “as is”. The contents of this document are subject to change without any notice. Please obtain the latest information through the Ruijie Networks website. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Obtaining Technical Assistance

- Ruijie Networks Website: http://www.ruijienetworks.com/
- Service Email: service_rj@ruijienetworks.com
- Technical Support: http://www.ruijienetworks.com/service.aspx
- Technical Support Hotline: +86-4008-111-000

Documentation Conventions

The symbols used in this document are defined as follows:

This symbol brings your attention to some helpful suggestions and references.

This symbol means that you must be extremely careful not to do some things that may damage the switch or cause data loss.

Contents

Overview **4**
Basics **4**
Large Initial Window 4
Selective Acknowledgment and Expansion 5
Congestion Control 6
Technical Principle **6**
References **7**
Configuration **8**
Default Configuration 8
Configuration Guide 8
Globally Enabling WAN-TA 8
Creating a WAN-TA Policy 9
Enabling a WAN-TA Policy on an Interface 10
Displaying WAN-TA Configuration 11
Configuration Example **11**
WAN-TA Configuration Example 11

Overview

With the furthering of information network construction, longitudinal networks in industries such as government, finance, and education gradually extend to remote terminal branches. For the majority of remote areas, it is not feasible to use private line access because the cost would be rather high and therefore currently WAN links, such as 3G or VPN, are applied to access. Compared with wired lines, 3G or VPN links are characterized by a long delay, a high bit error rate (BER), and asymmetric and low bandwidths. These characteristics result in poor transmission quality of 3G or VPN links and difficulty in guaranteeing the quality of service (QoS) on 3G or VPAN links.

Launched initially as an RFC draft (RFC 793) in 1981, the Transmission Control Protocol (TCP) provides a mechanism that enables application processes to reliably exchange data on a network. Although TCP indeed provides a reliable connection-oriented transmission environment, networks on which applications are deployed have greatly changed in the past two decades. In many cases, TCP becomes a bottleneck that restricts the application performance of a wide area network (WAN). In particular, plenty of TCP-based applications exist in finance and government industries where Ruijie routers are mostly used, and TCP brings about low transmission efficiency on 3G, VPN and ADSL networks. Furthermore, as applications based on WAN are rapidly growing, customers tend to use plenty of 3G, VPN or ADSL links as backup links for conventional wired lines or use them as master links, bringing an urgent need for promoting the transmission efficiency of TCP on these links.

Currently, there are numerous enhanced versions to improve the transmission performance of TCP. Some of the enhancements can effectively improve the performance of TCP connections, but the TCP protocol stack at two ends of a service does not necessarily include such new features for the time being. To enhance the transmission efficiency of TCP in the application environments of Ruijie routers, Ruijie introduced some new TCP features to its routers through WAN transmission acceleration (WAN-TA), a generic term for a series of technologies for improving the efficiency of TCP on WAN links such as 3G, ADSL and VPN links. WAN-TA enables Ruijie routers to apply new TCP features to forwarded data flows, thereby improving the transmission performance of TCP on WAN links. WAN-TA can eliminate almost all TCP performance obstacles, without requiring any change for client, server, or network features.

Basics

WAN-TA is a generic term for technologies for improving the efficiency of TCP on WAN links. It splits a TCP connection of a Ruijie router into two connections, so that the Ruijie router participates in a TCP session as a terminal device. In Ruijie routers, TCP data flows are controlled by WAN-TA policies. WAN-TA has ushered in the following technologies:

Large Initial Window

TCP has raised a series of mechanisms to avoid network congestion. Initially, V. Jacobson put forward a TCP congestion control mechanism composed of slow start and congestion avoidance in his paper in 1988. In the initial TCP version, after a connection is successfully established on a network, plenty of data packets are sent to the network. This, however, may easily cause the cache space of routers on the network to be exhausted,

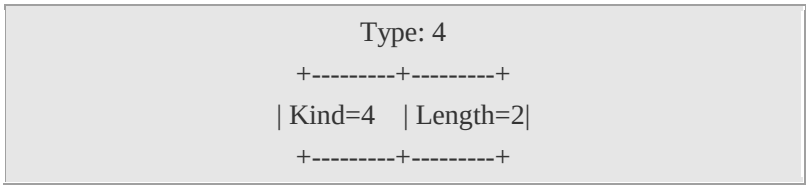
thereby causing congestion. For this reason, plenty of data packets should not be sent immediately after the connection is established. Instead, the amount of data to be sent each time should increase gradually according to the network status, so as to avoid the congestion. Specifically, when a connection is established, the value of cwnd is initially one maximum segment size (MSS) and the sender starts to send data according to the congestion window size. The value of cwnd is incremented by one MSS each time one packet segment is acknowledged. In this way, the value of cwnd exponentially grows along with the round trip time (RTT) of the network. In fact, slow start is not slow at all, except that its starting point is relatively low. On a high-delay and high-bandwidth WAN link, however, it takes a rather long time to wait for the acknowledgement of each packet. Using a large initial window can help TCP quickly exit the slow start process and make full use of bandwidth resources.

Selective Acknowledgment and Expansion

During TCP communications, if a certain data packet is lost in the transmit sequence, TCP will retransmit the packets that follow the last acknowledged packet. For this reason, packets already correctly transmitted may be sent again, resulting in a sharp decrease in TCP performance. The selective acknowledgment (SACK) technology enables TCP to transmit only the lost packets instead of retransmitting all the subsequent packets, and provides a mechanism that enables the recipient to inform the sender of various information, such as the lost data, the retransmitted data, and the data received ahead of time. In particular, SACK improves the transmission performance of TCP in a high-BER environment.

SACK information is provided by the options field in the TCP header and classified into two types. One indicates whether SACK is supported, and is sent during a TCP handshake. The other is specific SACK information.

SACK-Permitted Option

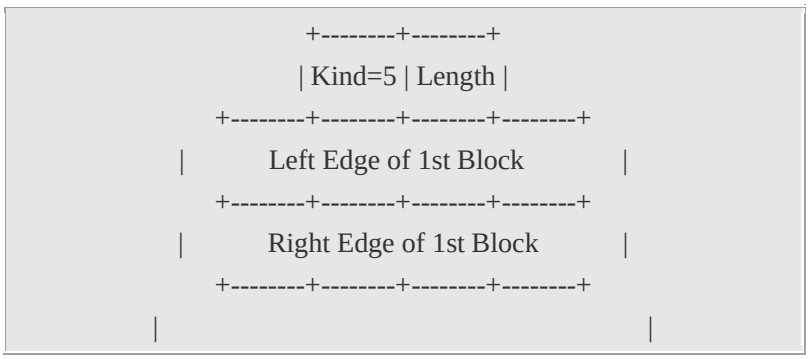


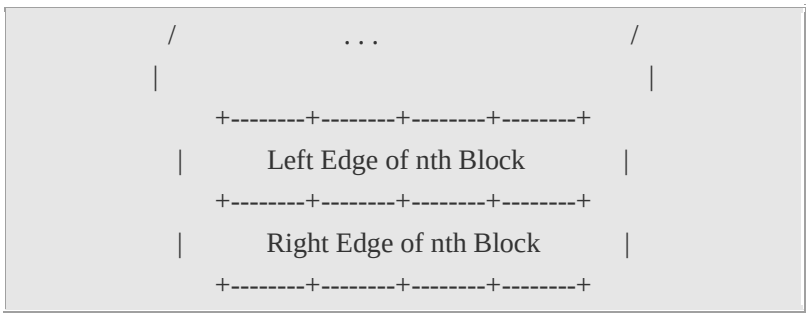
This option is only allowed in a TCP packet with a SYN flag. That is, this option exists in the first two packets during a TCP handshake, and indicates whether SACK is supported.

SACK Option

Type of the option: 5

Length of the option: The length is variable but the length of all TCP options cannot exceed 40 bytes. Actually there cannot be more than four groups of Edge values.





The parameters of this option are used to inform the sender of the discontinuous data blocks already received and cached, so that the sender can check which data block is lost according to the information and then sends the corresponding data block.

* Left Edge of Block

This parameter indicates the sequence number of the first data block among the discontinuous blocks.

* Right Edge of Block

This parameter indicates the sequence number of the data block that follows the last data block among the discontinuous blocks. It indicates that the data with the sequence numbers (Left Edge – 1) and (Right Edge) are not yet received.

Congestion Control

The default congestion algorithm of TCP is designed mainly based on real congestion of wired lines. On a WAN link especially a 3G, VPN or ADSL link, conventional congestion algorithm is no longer helpful in identifying congestions. In the wired TCP, when packet loss occurs as represented by three repetitive ACKs or when the retry timer expires, it indicates that congestion occurs on the sender side of the network. After the sender discovers the congestion, the slow start process continues again or the congestion window is reduced by half depending on the specific congestion algorithm. In the 3G, VPN or ADSL application environment, however, packet loss may not only be caused by congestion. When bit errors occur on a link, packets will be discarded and the available bandwidth of the link decreases. Therefore, if the packet loss is identified as congestion and the send window is reduced, the performance greatly degrades. In particular, the TCP performance is rather poor when the BER is high. In the 3G, VPN, or ADSL application environment, the delay of a packet is also indeterminate, a sudden delay will cause the TCP retry timer to expire, and the send window is reduced according to the conventional congestion algorithm in the case of TCP retry timer expiry. In this case, the expiry of the retry timer is not caused by congestion either. Reducing the send window leads to degraded TCP performance. The conventional congestion algorithm cannot well deal with the preceding problem. In view of this, WAN-TA has ushered in numerous congestion algorithms based on 3G application scenarios, including default, high-delay, high-lost, and low-bandwidth-delay.

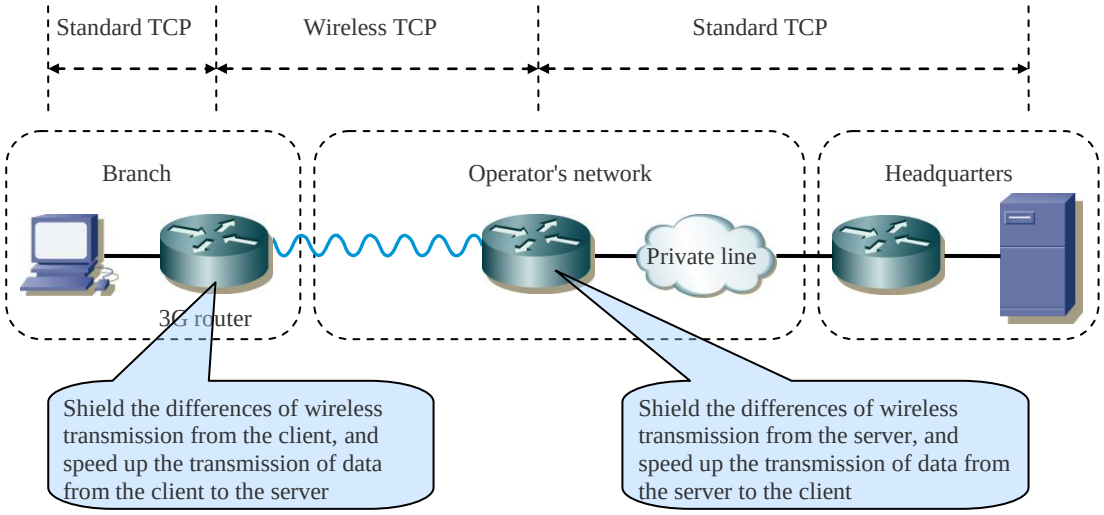
Technical Principle

A 3G network is a typical heterogeneous network on which both wired and wireless network nodes exist. Considering an obvious difference of transmission quality between wireless links and wired lines, the WAN-TA feature targeted at 3G wireless links should be preferably deployed and enabled on a gateway device at the boundary between the wireless links and the wired lines. In this case, the gateway device identifies the

difference between networks on the two sides, performs transmission adaptation and conversion, and shields the processing from the two ends of a transmission session.

For example, in a typical scenario shown in Figure 1-1, WAN-TA may be deployed on the 3G access router of the branch, the router of the operator's network, or the convergence router in the headquarters (However, the acceleration effect is not so ideal as that when WAN-TA is deployed on the router of the operator's network).

Figure 0-1 WAN-TA Deployment Modes



WAN-TA directly accelerates outbound traffic, and the acceleration effect is obvious. However, WAN-TA has a limited acceleration effect since it indirectly accelerates the inbound traffic. Therefore, WAN-TA should be preferably deployed on both sides of a wireless link. In Figure 1-1, if WAN-TA is deployed on the 3G access router of the branch, the original TCP link between the client and the server is split into two segments: a wired line between the client and the 3G access router, using the standard TCP; and a wireless link between the 3G access router and the server, using the wireless TCP. The 3G router shields the client from differences of transmission features in wireless environment, receives and caches the traffic sent by the client, and sends data at a highest possible rate to the server depending on the quality of the air interface, thereby making full use of the transmission bandwidth on the air interface and accelerating the traffic (in the outbound direction) from the client to the server. The wireless TCP optimization feature of the 3G access router indirectly affects the behaviors of TCP on the server, accelerating the traffic (in the inbound direction) from the server to the client to some extent. The situation is similar if WAN-TA is deployed on the operator's router or the convergence router in the headquarters.

References

RFC protocols related to TCP are specified as follows:

RFC793: Transmission Control Protocol (TCP)

RFC1323: TCP Extensions for High Performance

RFC2018: TCP Selective Acknowledgment Options

RFC2581: TCP Congestion Control

Configuration

Default Configuration

Feature	Default Settings
Globally enabling WAN-TA	WAN-TA is disabled by default.
Configuring a WAN-TA policy	No WAN-TA policy is configured.
Configuring the congestion control algorithm of the WAN-TA policy	No congestion control algorithm is configured.
Configuring the WAN-TA policy to support SACK	The SACK option of the WAN-TA policy is enabled.
Configuring the initial window of the WAN-TA policy	The initial window size is not configured by default.
Configuring the MSS of the WAN-TA policy	MSS is not configured by default.
Applying the WAN-TA policy to an interface	WAN-TA is disabled on an interface.

Configuration Guide

- The inbound interface and the outbound interface of data flows to which WAN-TA is applied must be express-forwarding interfaces.
- All TCP data flows optimized by WAN-TA are forwarded by the device running WAN-TA.

Globally Enabling WAN-TA

Command	Function
Ruijie(config)# **wan-ta enable**	Globally enables the WAN-TA function. The WAN-TA function takes effect on an interface only when the WAN-TA function is globally enabled and a WAN-TA policy is applied to the interface.

To disable the WAN-TA function, use the no wan-ta enable command in global configuration mode.

Configuration example:

The following example enables the global WAN-TA function:

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# wan-ta enable
```

After the WAN-TA function is enabled, it takes effect for only new flows instead of existing flows. If you hope that the WAN-TA function takes effect for an existing connection, you need to disconnect and then re-create the connection after enabling the WAN-TA function.

After the global WAN-TA function is disabled, the existing TCP sessions to which WAN-TA is applied will continue to be effective.

Creating a WAN-TA Policy

Command	Function
Ruijie(config)# **wan-ta policy** { **video** | *policy-name* } [**cong-algorithm** *cong-value* | **init-cwnd** *cwnd-value* | **sack** { **enable** | **disable**} | **mss** *mss-value* | **keepalive interval** *interval-value* retry *retry-count*]	Creates a WAN-TA policy and specifies the parameters of the WAN-TA policy. This command can be configured in the following two ways: Directly specify parameters behind the command. Then the command does not enter the following WAN-TA policy configuration mode. Do not specify any parameter behind the command. Then the command enters the following WAN-TA policy configuration mode, and you can specify the parameters of the WAN-TA policy one by one.
Ruijie(config-wan-ta-policy)#**cong-algorithm { default | high-delay-1 | high-delay-2 | high-lost | low-bandwidth-delay** }	Configures the congestion algorithm of the WAN-TA policy. This command has the same function as the cong-algorithm *cong-value* parameter of the wan-ta policy command.
Ruijie(config-wan-ta-policy)# **sack { enable | disable }**	Enables or disables the SACK function of the WAN-TA policy. This command has the same function as the sack parameter of the wan-ta policy command.
Ruijie(config-wan-ta-policy)# **init-cwnd** *cwnd-value*	Configures the initial window size of the WAN-TA policy. The value range is 2 to 10. This command has the same function as the init-cwnd *cwnd-value* parameter of the wan-ta policy command.
Ruijie(config-wan-ta-policy)#**mss** *mss-value*	Configures the MSS of the WAN-TA policy. The value range is 68 to 1460. This command has the same function as the mss *mss-value* parameter of the wan-ta policy command.

To delete the configured WAN-TA policy, use the no wan-ta policy video command in global configuration mode.

Configuration example 1:

The following example creates a system-defined WAN-TA policy named "video":

```
Ruijie(config)#wan-ta policy video
```

Configuration example 2:

The following example creates a user-defined WAN-TA policy named "ftp" and specifies parameters behind the command:

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# wan-ta policy ftp init-cwnd 10 cong-algorithm low-bandwidth-delay
```

Configuration example 3:

The following example creates a user-defined WAN-TA policy named "ftp" and enters the policy mode to specify parameters:

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#wan-ta policy ftp
Ruijie(config-wan-ta-policy)#init-cwnd 10
Ruijie(config-wan-ta-policy)#cong-algorithm low-bandwidth-delay
```

- It is not recommended that you specify parameters when creating a system-defined policy, such as the policy in configuration example 1. The system automatically generates the parameters. It is not recommended that you modify the settings of the parameters.
- When creating a user-defined policy, you can directly use the **wan-ta policy** command with parameters or enter the WAN-TA policy configuration mode to specify parameters one by one. For details, see configuration examples 2 and 3.
- Before deleting a WAN-TA policy, you need to remove the WAN-TA policy from interfaces on which the WAN-TA policy has been applied. If you modify the configuration after a policy is applied on an interface, the changes do not take effect for the existing connections to which WAN-TA is applied.
- The system supports a maximum of eight WAN-TA policies. One policy named "video" is reserved, and at most seven user-defined policies can be configured.
- The name of a user-defined policy cannot be the prefix of a system policy name, such as "v", "vi", "vid", "vide", or "video". Otherwise, you automatically enter the system policy.

Enabling a WAN-TA Policy on an Interface

Command	Function
Ruijie(config-if-gigaethernet0/0)# **wan-ta-policy {** *policy-name* **| video} list** { *acl-id* | *acl-name*}	Applies a WAN-TA policy to an interface. The acl-id or acl-name parameter specifies the ACL that matches the flow to be optimized.

To delete the configured WAN-TA policy from an interface, use the no wan-ta-policy { policy-name | video } command in interface configuration mode.

Configuration example:

The following example applies a WAN-TA policy named "video" to an interface, so that all flows matching ACL 101 will be accelerated according to the WAN-TA policy named "video":

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#interface gigaethernet0/0
```

```
Ruijie(config-if-gigaethernet0/0)# wan-ta-policy video  list 101
```

⚠ Multiple WAN-TA policies can be applied to an interface. The optimization is based on the first matching policy. The matching sequence is as follows: First perform matching according to the policy configuration sequence on the inbound interface of a packet, and then perform matching according to the policy configuration sequence on the outbound interface of the packet.

⚠ When there is a TCP connection to which a WAN-TA policy is applied on an interface, the WAN-TA function still takes effect on the interface even after the WAN-TA policy is deleted from the interface.

Displaying WAN-TA Configuration

Command	Function
Ruijie# **show wan-ta policy session**	Displays summary information about TCP sessions to which WAN-TA has been applied.
Ruijie# **show wan-ta policy session** *session_id*	Displays statistics about the session with the specified session ID.
Ruijie# **show wan-ta policy** { *policy-name* | **video**}	Displays configuration information about a WAN-TA policy.

Configuration Example

WAN-TA Configuration Example

Network Requirements

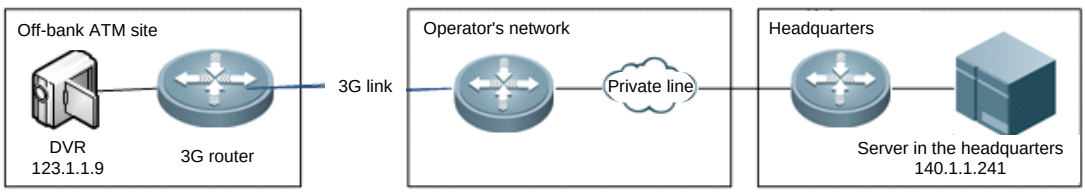
1) An off-bank ATM uses a Ruijie router as the access router, which is connected to an upstream server in the headquarters through 3G links.

2) TCP connections are used for video surveillance between the branch and the server in the headquarters.

3) Before arriving at the router to which a WAN-TA policy is applied, data flows are not encrypted or encapsulated through other tunnels.

Networking Topology

Figure 0-1 Networking Topology of WAN-TA



Configuration Tips

1) Globally enable the WAN-TA function.

2) Identify the features of data flows to which the WAN-TA function will be applied.

3) Configure a WAN-TA policy.

4) Enable the WAN-TA policy on devices that data flows pass.

Configuration Steps

1) Configure the data of the services to be optimized.

Configure an ACL rule that matches the services to be optimized.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#ip access-list extended 101
Ruijie(config-ext-nacl)#10 permit tcp host 123.1.1.9 any
```

2) Enable WAN-TA.

Globally enable WAN-TA.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#wan-ta enable
```

3) Configure a WAN-TA policy.

Configure a WAN-TA policy named "video", which is used to optimize the connections for video surveillance between the branch and the server. Define an ACL rule "acl 101" to match the TCP data flows from the branch to the headquarters. Ensure that video data flows are uploaded from the off-bank ATM to the server in the headquarters, and the WAN-TA policy is deployed on the 3G router of the off-bank ATM.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# wan-ta policy video
```

4) Apply the WAN-TA policy to an interface.

Enable WAN-TA on the inbound interface gigaethernet0/1 of the off-bank ATM, or apply the WAN-TA policy to the outbound interface of data flows.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#int gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#wan-ta-policy video list 101
```

Verification

1) Check the configuration of the WAN-TA policy.

```
Ruijie#show wan-ta policy video
wan-ta policy: video
Congestion Control : low-bandwidth-delay
SACK Support: TRUE
Initial Congest Window: 10 MSS
Maxitum Segment Size: 1460
apply on interfaces:
```

```
interface name list
GigabitEthernet 0/0 101
GigabitEthernet 0/1 102
```

2) Check the current session.

```
Ruijie#sh wan-ta  policy session
session_id  pair        flow                          tcp_state           uptime
42          41    [140.1.1.241:3594->123.1.1.9:37777]     TCP_ESTABLISHED
0:00:03
41          42    [123.1.1.9:37777->140.1.1.241:3594]     TCP_ESTABLISHED
0:00:03
```

The session whose session_id is 42 undertakes LAN communications with the off-bank ATM, and the session whose session_id is 41 undertakes WAN communications with the headquarters. In this example, we focus on the WAN communications.

3) Check the running status of a certain session.

```
Ruijie#sh wan-ta policy session 41
[123.1.1.9:37777->140.1.1.241:3594]
1-10
timer notify 658. handle 658
signal handl 4594. while 3284
sock state: TCP_ESTABLISHED ref_cnt: 3
Congestion Control:
icsk_ca_state : open icsk_retransmits: 0
congestion : low-bandwidth-delay icsk_rto : 320ms, icsk_timeout:280ms
icsk_backoff : 0 icsk_probes_out : 0
TCP Options:
is_tstamp : no
is_sack : yes
is_wscale : no
Statistics:
unacked : 23 sacked : 0
lost : 0 retrans : 0
fackets : 0
in flight : 23
total retans : 8
Times:
last_data_sent: 40ms last_data_recv: 19340ms last_ack_recv: 40ms
Metrics:
srtt : 210ms bw : 0B/s
rcv_ssthresh : 10240 snd_ssthresh: 8
rtt : 210ms snd_cwnd : 23
rttvar : 50ms snd_wnd : 64831
rcv_rtt : 0ms advmss : 1024
mss_cache : 1420
in_pkt_num : 1 out_pkt_num : 1610
reordering : 3
Queue length: 0 write_queue_len: 200 ofo_queue_len: 0
```

The important parameters are explained as follows:

write_queue_len: send queue length. A packet can be sent on the link only when the value of this parameter is not null.

out_pkt_num: the number of sent packets.

snd_cwnd: send congestion window, indicating the number of packets that can be sent on the link. It is an important parameter related to congestion control.

total retans: the number of retransmitted packets.

srtt: the current delay of the link.

WAN Transmission Acceleration

Technology White Paper

www.ruijienetworks.com