CGTF Looking Glass Platform

1. Introduction

A Looking Glass is a piece of software running on a web server server which allows users to get a look at routing and network behavior as it originates from the remote network. A looking glass accesses a remote router and performs a host, ping, trace, or one of several show commands allowing a view of the IP and BGP route tables. Looking Glasses are most commonly used for verifying routing between the providers, and for verifying that routes are propagating correctly across the Internet.

Looking Glass allows us to view the Internet from different locations. It can help network operators quickly locate network faults and also provide network researchers with very meaningful data.

2. Web-based Looking Glass

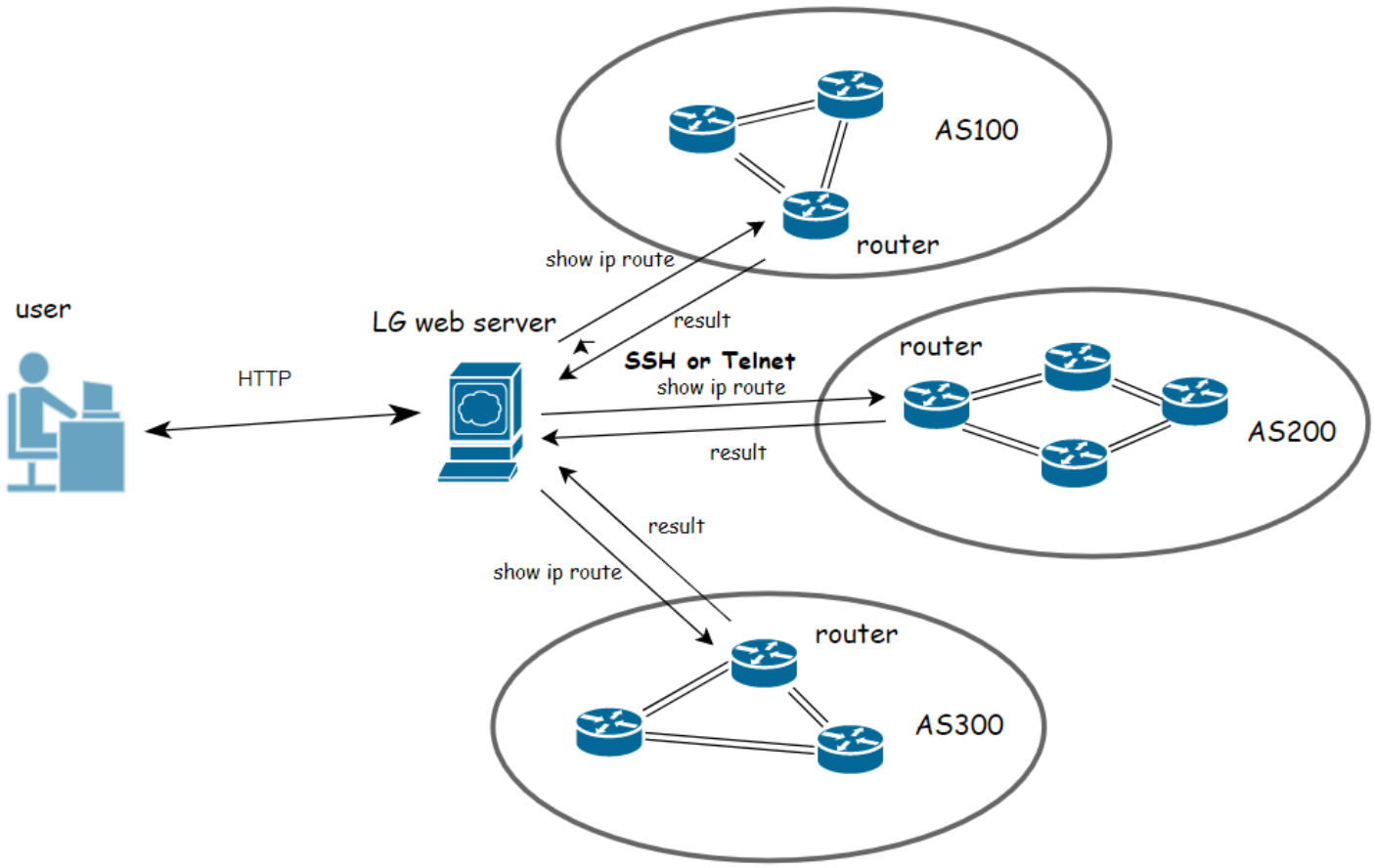

Figure 1 Architecture of web-based LG

Figure 1 shows the architecture of the web-based LG. In this architecture, LG is actually a web application running on the LG web server. We can regard it as a command agent that forwards the

user's commands to the router, and then returns the router's execution results to the user.

The following is a complete LG command execution process. First, the user visits the LG web server through a browser to get the LG page. Then, the user makes a command execution request to the LG web server by selecting commands, selecting routers, entering query parameters, and other operations on the page. After receiving the request, the server connects to the corresponding router through SSH or Telnet based on the parameters selected by the user. Afterwards, the router executes the command and returns the command execution result to the LG web server. Finally, the LG web server sends the results to the user.

3. CGTF Looking Glass

we have deployed a LG at https://lg.cgtf.net.

The open source LG software that we use is gmazoyer/looking-glass: Easy to deploy Looking Glass (github.com). We modified the open source and made some changes to the front-end pages of the LG.

Command Supported

RFC8522 categorizes LG commands into four groups: diagnostic commands, informational commands, organizational commands, and extensible commands. LG is an effective tool for network administrators to diagnose their networks, however, the ability of LG is entirely determined by the commands it supports. Based on the RFC documentation recommendations and our survey of existing LGs, we decided to implement the following commands.

```
ping <ip>
traceroute <ip>
show ip route <ASN>
show ip route <ip>
show ip route <as-path-regex>
```

Secure on Web Server

Malicious users may use scripts to send a large number of query commands to LG in a short period of time, increasing the burden on the router, which may cause DoS attacks. To prevent malicious users from using LG to attack the router, we implemented Query Rate Limiting on the WEB server.

- Query Rate Limiting
  Implement a query rate limiting mechanism on the web server to prevent excessive query commands from burdening the router。

4. Router Configuration

The partners need to provide us with an account and password of their routers. We recommend that each organization creates an account only for LG and then configure firewall filtering rules on the routers.

Router Login Security

Every time a user submits a query request, the web server needs to log in to the router and then the router executes the command. We know that logging into the router is an operation that requires great caution. So we need do something to secure the router login. Following are some solutions:

- Create an router account only for LG, and this account only has privileges of executing the above command.
- Use IP filtering mechanism. Add the web server IP to the whitelist.
- Generate SSH key, disable password login. Only login via SSH key to ensure the security of router account and password.

Router Configuration Example

We have currently tested it on the Jnuiper router. Here is our configuration for LG router account permissions and SSH key login：

```
Juniper JUNOS:
    Define the login class with permissions:
        set system login class lookinglass permissions network
        set system login class lookinglass permissions routing
        set system login class lookinglass permissions view

    Define the login user:
        set system login user lookinglass class lookinglass
        set system login user lookinglass authentication encrypted-password "encrypted-text"
        set system login user lookinglass authentication ssh-rsa "ssh-rsa rsa-pub-key-text"
```

When configuring the LG account, please ensure that it has the privileges to execute the commands given above.

If you have any question or advice , please contact sec@cgtf.net .