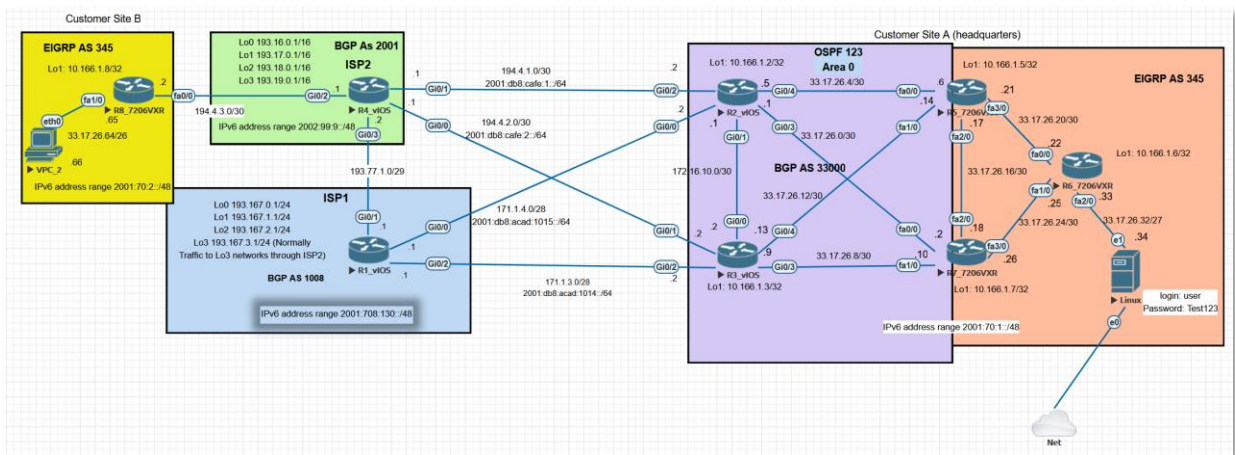


Advanced Routing in Enterprise Networks

Topology



Encrypting all passwords in customer routers in the most secure way supported by your IOS image.

```
username Cisco privilege 15 secret 9 $9$qqDDy/TWa70wYAP$HgGLVM9asW.CpcNN4Fb4Kd6AW
zPKX9TiXPCPewDk/OM
username Student secret 9 $9$mhR0oZT61nGjkt$ae4jd.EimTIDb099j1cxHJ/Fb3Bce.8swv5V
M3KWPGw
```

Disabling telnet and enabling SSH connection on all customer network devices.

```
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
transport input ssh
line vty 5 15
transport input ssh
```

Use Linux server as Radius server (use FreeRadius) with fallback to device's local password database. Configure user username with password P@55w0rd3000 in radius server. Limiting management of customer devices to be allowed only from Customer Site A addresses

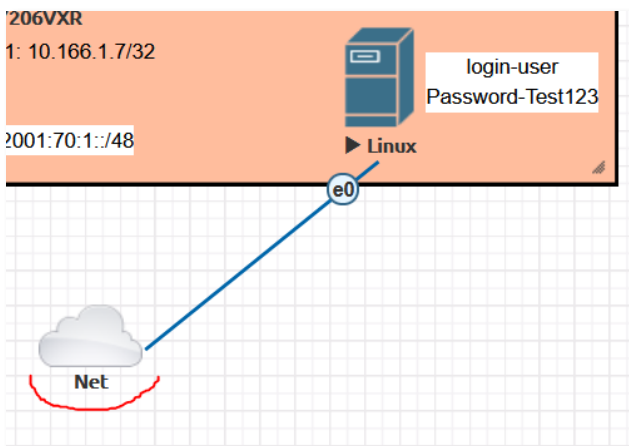
```
R8(config)#ip access-list extended vty-in
R8(config-ext-nacl)#permit ip 33.17.26.32 0.0.0.31 any
R8(config-ext-nacl)#exit
R8(config)#line vty 0 15
R8(config-line)#access-class vty-in in
R8(config-line)#
```

The ssh connection is allowed for the 33.17.26.32/27 network.

The output shows the rejected connection from R6 since it is not allowed network, and a successful connection from the Linux server, based on its IP address.

```
R8>exit
[Connection to 33.17.26.65 closed by foreign host]
R6#ssh 33.17.26.65
% Connection refused by remote host ✓
R6#
[ -Q query_option] [-R address] [-S ctl_path] [-W host:port]
[-w local_tun[:remote_tun]] destination [command]
[user@localhost ~]$ ssh -l test 33.17.26.65
ssh: connect to host 33.17.26.65 port 22: Connection refused
[user@localhost ~]$ ssh -l test 33.17.26.65
Password: ✓
R8>
```

The Linux Server powered by CentOS 8 was installed. To have access to the internet temporary connection was deployed in the workspace, the connection is provided by the built-in tool in EVE-NG which use the NAT connection through the VMWare virtual switch to the outside area, such as INTERNET and LAN.



The given task requires the FreeRadius server to be installed on the Linux server.

The first step is to update the CentOS system by command ***sudo yum update -y***.

```
libzstd-1.4.4-1.el8.x86_64
mozjs60-60.9.0-4.el8.x86_64
python3-ethtool-0.14-3.el8.x86_64
python3-inotify-0.9.6-13.el8.noarch
python3-nftables-1:0.9.3-16.el8.x86_64
python3-pip-wheel-9.0.3-18.el8.noarch
python3-setuptools-wheel-39.2.0-6.el8.noarch
python3-subscription-manager-rhsm-1.27.16-1.el8.x86_64
rhsm-icons-1.27.16-1.el8.noarch
subscription-manager-1.27.16-1.el8.x86_64
subscription-manager-rhsm-certificates-1.27.16-1.el8.x86_64

Complete!
[user@localhost ~]$
```

The next step is to install the FreeRadius server itself.

The FreeRadius server also requires FreeRadius-utils, FreeRadius-MySQL and FreeRadius-Perl packages. All the packages will be installed in one command as ***sudo yum install freeradius freeradius-utils freeradius-mysql freeradius-perl -y***.

```

Verifying if make-1:4.2.1-10.el8.x86_64
Installed products updated.

Installed:
  freeradius-3.0.20-3.module_el8.3.0+476+0982bc20.x86_64
  freeradius-perl-3.0.20-3.module_el8.3.0+476+0982bc20.x86_64
  freeradius-utils-3.0.20-3.module_el8.3.0+476+0982bc20.x86_64
  make-1:4.2.1-10.el8.x86_64
  perl-Time-HiRes-1.9758-1.el8.x86_64

Complete!
[user@localhost ~]$

```

After installation of freeradius packages, check the radiusd service, the service must be in an inactive state. This service will not start by default, it requires to be manually started by command `service radiusd start`. And then check again that the service is in a running state.

```

Complete!
[user@localhost ~]$ service radiusd status
Redirecting to /bin/systemctl status radiusd.service
● radiusd.service - FreeRADIUS high performance RADIUS server.
   Loaded: loaded (/usr/lib/systemd/system/radiusd.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
[user@localhost ~]$ service radiusd start
Redirecting to /bin/systemctl start radiusd.service
[user@localhost ~]$ service radiusd status
Redirecting to /bin/systemctl status radiusd.service
● radiusd.service - FreeRADIUS high performance RADIUS server.
   Loaded: loaded (/usr/lib/systemd/system/radiusd.service; disabled; vendor preset: disabled)
   Active: active (running) since Fri 2021-05-07 20:58:20 EDT; 56s ago
     Process: 38447 ExecStart=/usr/sbin/radiusd -d /etc/raddb (code=exited, status=0/SUCCESS)
     Process: 38443 ExecStartPre=/usr/sbin/radiusd -C (code=exited, status=0/SUCCESS)
     Process: 38404 ExecStartPre=/bin/sh /etc/raddb/certs/bootstrap (code=exited, status=0/SUCCESS)
     Process: 38401 ExecStartPre=/bin/chown -R radiusd.radiusd /var/run/radiusd (code=exited, status=0/SUCCESS)
    Main PID: 38449 (radiusd)
     Tasks: 6 (limit: 24013)

```

Adding devices and users to the Radius service

gedit /etc/raddb/clients.conf

Client.conf file

```

client 33.17.26.33 {
    secret = cisco
    nastype = cisco
    shortname = R6
}

```

Users file

gedit /etc/raddb/users

Restarting the service

```
osition not supported
[user@localhost ~]$ sudo service radiusd restart
```

Adding the rule to the firewall and reloading the firewall itself

```
[user@localhost ~]$ sudo firewall-cmd --add-service=radius --permanent
success
[user@localhost ~]$ sudo firewall-cmd --reload
success
[user@localhost ~]$
```

The configuration on the routers:

```
aaa new-model
aaa authentication login default group radius local
radius-server host 33.17.26.34 auth-port 1812 acct-port 1813 key cisco
For R2 and R3*
(radius server Linux
address ipv4 33.17.26.34 auth-port 1812 acct-port 1813
key cisco)
line vty 0 15
login authentication default
exit
line console 0
login authentication default
exit
```

Synchronizing all clocks in active devices by using NTP (Linux Server) and configuring correct time zones (EET) and summertime transition rules (EEST

```
clock timezone EET 2
clock summer-time EEST recurring
ntp server 33.17.26.34
```

Installing NTP server on Linux Server

```
dnf install chrony
systemctl enable chronyd
```

```
[user@localhost ~]$ sudo dnf install chrony
[sudo] password for user:
Last metadata expiration check: 0:22:39 ago on Fri 07 May 2021 08:54:19 PM EDT.
Package chrony-3.5-1.el8.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[user@localhost ~]$ systemctl enable chronyd
[user@localhost ~]$
```

Adding Chrony to act as an NTP server for a local network.

/etc/chrony.conf

Allow 0.0.0.0/0

systemctl restart chronyd

```
# Increase the minimum number of selectable sources required to adjust
# the system clock.
#minsources 2

# Allow NTP client access from local network.
allow 0.0.0.0/0
```

```
[user@localhost ~]$ sudo systemctl restart chronyd
[user@localhost ~]$ sudo firewall-cmd --permanent --add-service=ntp
success
[user@localhost ~]$ sudo firewall-cmd --reload
success
[user@localhost ~]$
```

Configuring the network devices to synchronize the time with the Linux NTP server.

NTP server 33.17.26.34

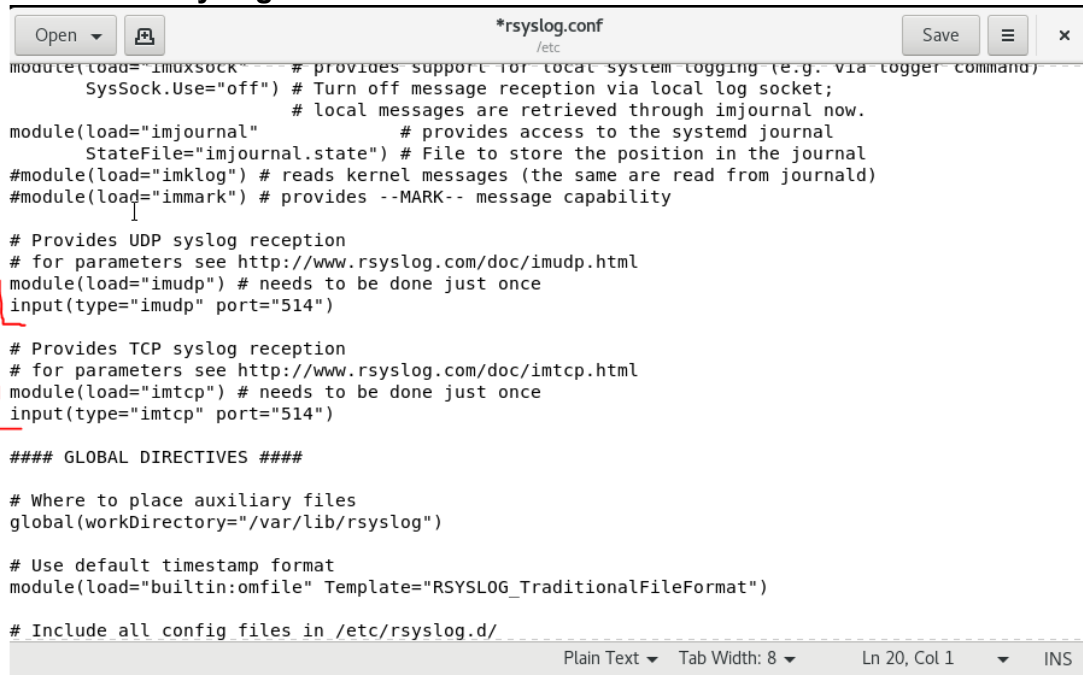
Checking the NTP status on R6

```
R6(config)#do sh ntp status
Clock is synchronized, stratum 4, reference is 33.17.26.34
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**19
ntp uptime is 593700 (1/100 of seconds), resolution is 4000
reference time is E443834F.E2DD877A (13:02:55.886 EEST Mon May 10 2021)
clock offset is 0.2284 msec, root delay is 39.37 msec
root dispersion is 58.59 msec, peer dispersion is 3.23 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000006 s/s
system poll interval is 256, last update was 2399 sec ago.
R6(config)#
```

Configuring all devices to log in debug level all messages to local 64000 bytes circular buffer (logging buffered 64000) and to Linux server where I have a log-server enabled.

dnf install -y rsyslog

Edit the /etc/rsyslog.conf file.

A screenshot of a text editor window titled '*rsyslog.conf /etc'. The window contains the configuration for the rsyslog service. The file is in 'Plain Text' mode with a tab width of 8. The cursor is at line 20, column 1. The configuration includes modules for local logging, systemd journal, kernel messages, and UDP/TCP reception. The UDP and TCP input modules are highlighted with red boxes. The global directives section is also visible.

```
module(load="imuxsock" # provides support for local system logging (e.g. via logger command)
        SysSock.Use="off") # Turn off message reception via local log socket;
                           # local messages are retrieved through imjournal now.
module(load="imjournal" # provides access to the systemd journal
        StateFile="imjournal.state") # File to store the position in the journal
#module(load="imklog") # reads kernel messages (the same are read from journald)
#module(load="immark") # provides --MARK-- message capability

# Provides UDP syslog reception
# for parameters see http://www.rsyslog.com/doc/imudp.html
input(type="imudp" port="514")

# Provides TCP syslog reception
# for parameters see http://www.rsyslog.com/doc/imtcp.html
input(type="imtcp" port="514")

#### GLOBAL DIRECTIVES ####

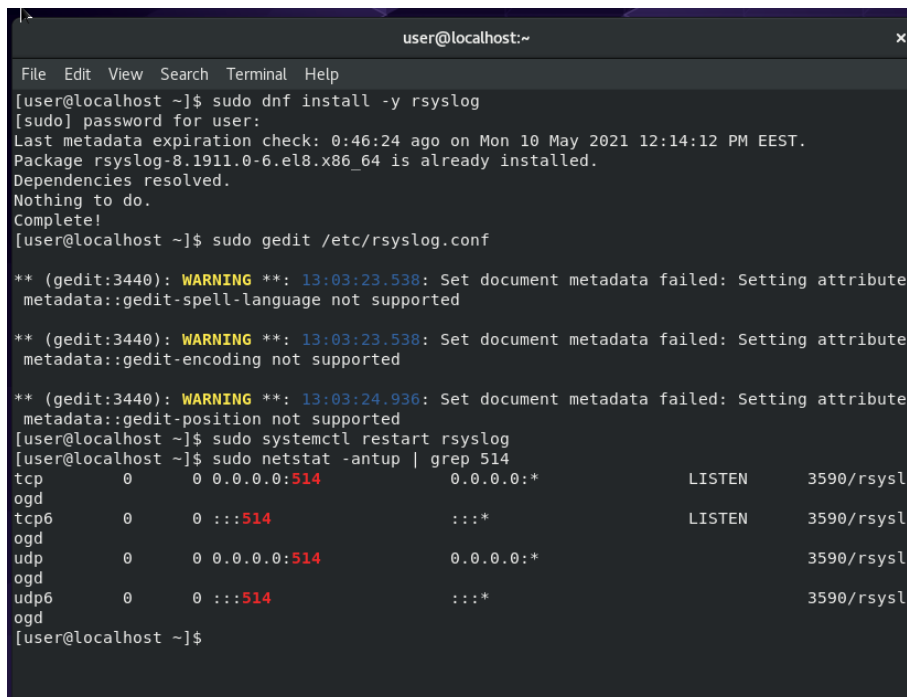
# Where to place auxiliary files
global(workDirectory="/var/lib/rsyslog")

# Use default timestamp format
module(load="builtin:omfile" Template="RSYSLOG_TraditionalFileFormat")

# Include all config files in /etc/rsyslog.d/
```

Restarting the Syslog service

Verify the Syslog server listening on port 514.

A screenshot of a terminal window titled 'user@localhost:~'. The terminal shows the command 'dnf install -y rsyslog' being executed, which reports that the package is already installed. Then, 'sudo gedit /etc/rsyslog.conf' is run, showing several warnings about metadata. Finally, 'sudo systemctl restart rsyslog' is executed, and 'netstat -antup | grep 514' is used to verify that the service is listening on port 514 for both UDP and TCP.

```
user@localhost:~
File Edit View Search Terminal Help
[user@localhost ~]$ sudo dnf install -y rsyslog
[sudo] password for user:
Last metadata expiration check: 0:46:24 ago on Mon 10 May 2021 12:14:12 PM EEST.
Package rsyslog-8.1911.0-6.el8.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[user@localhost ~]$ sudo gedit /etc/rsyslog.conf

** (gedit:3440): WARNING **: 13:03:23.538: Set document metadata failed: Setting attribute
metadata::gedit-spell-language not supported

** (gedit:3440): WARNING **: 13:03:23.538: Set document metadata failed: Setting attribute
metadata::gedit-encoding not supported

** (gedit:3440): WARNING **: 13:03:24.936: Set document metadata failed: Setting attribute
metadata::gedit-position not supported
[user@localhost ~]$ sudo systemctl restart rsyslog
[user@localhost ~]$ sudo netstat -antup | grep 514
tcp        0      0 0.0.0.0:514          0.0.0.0:*            LISTEN     3590/rsysl
ogd
tcp6       0      0 :::514              :::*                  LISTEN     3590/rsysl
ogd
udp        0      0 0.0.0.0:514          0.0.0.0:*            3590/rsysl
ogd
udp6       0      0 :::514              :::*                  3590/rsysl
ogd
[user@localhost ~]$
```

Firewall

```
firewall-cmd --permanent --add-port=514/udp  
firewall-cmd --reload  
firewall-cmd --permanent --add-port=514/tcp  
firewall-cmd --reload
```

```
[user@localhost ~]$ sudo firewall-cmd --permanent --add-port=514/udp  
success  
[user@localhost ~]$ sudo firewall-cmd --reload  
success  
[user@localhost ~]$ sudo firewall-cmd --permanent --add-port=514/udp  
Warning: ALREADY_ENABLED: 514:udp  
success  
[user@localhost ~]$ sudo firewall-cmd --permanent --add-port=514/tcp  
success  
[user@localhost ~]$ sudo firewall-cmd --reload  
success  
[user@localhost ~]$
```

Validation

```
tail -f /var/log/messages
```

and checking the logs after the interface f0/0 of R6 was switched off and on.

```
user@localhost:~  
File Edit View Search Terminal Help  
May 10 13:50:07 localhost NetworkManager[894]: <info> [1620643807.4917] dhcp4 (ens3): state changed extended -> extended  
May 10 13:50:07 localhost dbus-daemon[803]: [system] Activating via systemd: service name='org.freedesktop.nm_dispatcher' unit='dbus-org.freedesktop.nm-dispatcher.service' requested by ':1.14' (uid=0 pid=894 comm="/usr/sbin/NetworkManager --no-daemon " label="system_u:system_r:NetworkManager_t:s0")  
May 10 13:50:07 localhost systemd[1]: Starting Network Manager Script Dispatcher Service..  
May 10 13:50:07 localhost dbus-daemon[803]: [system] Successfully activated service 'org.freedesktop.nm_dispatcher'  
May 10 13:50:07 localhost systemd[1]: Started Network Manager Script Dispatcher Service.  
May 10 13:50:12 _gateway 35: May 10 10:50:11.126: %DUAL-5-NBRCHANGE: EIGRP-IPv4 345: Neighbor 33.17.26.21 (FastEthernet0/0) is down: interface down  
May 10 13:50:12 _gateway 36: May 10 10:50:11.158: %DUAL-5-NBRCHANGE: EIGRP-IPv4 200: Neighbor 33.17.26.21 (FastEthernet0/0) is down: interface down  
May 10 13:50:14 _gateway 37: May 10 10:50:13.074: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down  
May 10 13:50:14 _gateway 38: May 10 10:50:14.074: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down  
May 10 13:50:17 localhost systemd[1]: NetworkManager-dispatcher.service: Succeeded.  
May 10 13:50:51 localhost NetworkManager[894]: <info> [1620643851.2927] agent-manager: agent[05156f853cf4fc61,:1.223/org.gnome.Shell.NetworkAgent/1000]: agent registered  
May 10 13:52:14 _gateway 39: May 10 10:52:13.926: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up  
May 10 13:52:14 _gateway 40: May 10 10:52:14.926: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up  
May 10 13:52:16 _gateway 41: May 10 10:52:15.486: %DUAL-5-NBRCHANGE: EIGRP-IPv4 200: Neighbor 33.17.26.21 (FastEthernet0/0) is up: new adjacency  
May 10 13:52:17 _gateway 42: May 10 10:52:16.666: %DUAL-5-NBRCHANGE: EIGRP-IPv4 345: Neighbor 33.17.26.21 (FastEthernet0/0) is up: new adjacency
```

Commands issued on the routers:

```
logging buffered 64000
```

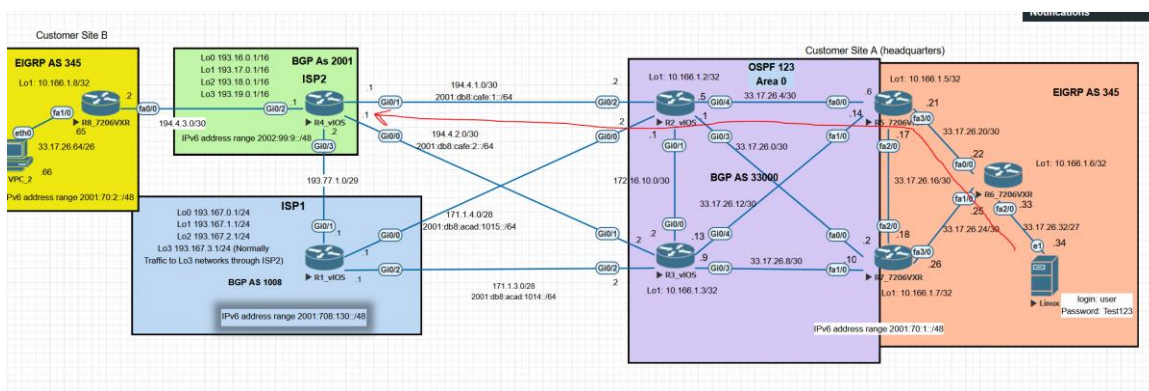
```
logging host 33.17.26.34 (*the IP address of the Linux server).
```


Configure BGP routing in this Network so that all networks originating from ISP2 are normally accessed from R2 to R4 router. If connections from both R2 and R3 to R4 are not working, then traffic should use a backup route through ISP1.

Traffic to ISP1's network should normally go through R3 to R1, but for network 193.167.3.0/24 they should prefer a route through ISP2

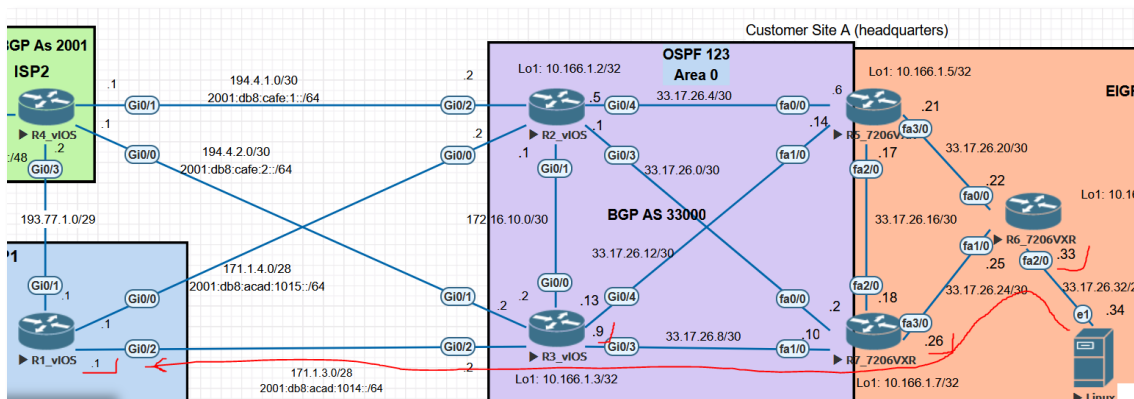
Traceroute to the 193.16.0.0 network

```
traceroute to 193.16.0.1 (193.16.0.1), 30 hops max, 60 byte packets
 1 _gateway (33.17.26.33) 9.431 ms 9.330 ms 9.195 ms
 2 33.17.26.21 (33.17.26.21) 25.977 ms 25.859 ms 25.712 ms
 3 33.17.26.5 (33.17.26.5) 31.088 ms 39.323 ms 49.810 ms
 4 194.4.1.1 (194.4.1.1) 39.042 ms * *
[user@localhost ~]$
```



Traceroute to the 193.167.0.0 network

```
traceroute to 193.167.0.1 (193.167.0.1), 30 hops max, 60 byte packets
 1 _gateway (33.17.26.33) 13.869 ms 11.741 ms 10.999 ms
 2 33.17.26.26 (33.17.26.26) 19.837 ms 17.914 ms 17.738 ms
 3 33.17.26.9 (33.17.26.9) 26.725 ms 26.596 ms 26.377 ms
 4 171.1.3.1 (171.1.3.1) 25.997 ms * *
[user@localhost ~]$
```

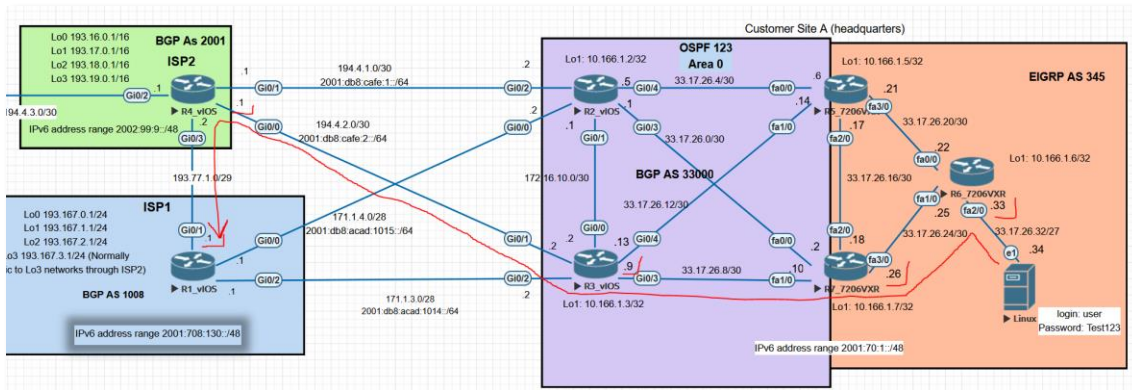


Traceroute to the 193.167.3.0 network


```

traceroute to 193.167.3.1 (193.167.3.1), 30 hops max, 60 byte packets
 1 _gateway (33.17.26.33) 4.012 ms 3.888 ms 3.695 ms
 2 33.17.26.26 (33.17.26.26) 43.593 ms 43.531 ms 43.450 ms
 3 33.17.26.9 (33.17.26.9) 43.355 ms 61.914 ms 61.891 ms
 4 194.4.2.1 (194.4.2.1) 46.141 ms 46.012 ms 61.529 ms
 5 193.77.1.1 (193.77.1.1) 42.744 ms * *
[user@localhost ~]$

```



Configure BGP to use the most secure way of authentication supported by your devices.

address-family ipv6

neighbor 2001:70:1:1000::13 password cisco

neighbor 2001:70:1:3000::1 password cisco

exit-address-family

Configure access lists on R2, R3 and R8 routers to secure Customer Site A and B. Access lists should only allow normal user traffic (HTTP, HTTPS, SSH, and DNS, ping traceroute and ICMP error messages BGP to neighbour routers) out and the site is not providing any services to the internet.

Example of R8

Ip access-list extended 110

permit tcp any any eq 80

permit tcp any any eq 443

permit tcp any any eq 22

permit udp any any eq 53

permit udp any any eq 179

permit icmp any any echo-reply

permit tcp any any eq bgp

R8

int fa0/0

ip access-group 110 out

Configure devices to support IPv6 (example of R8)

```
ip domain name test.com
ip cef
ipv6 unicast-routing
ipv6 cef
!
```

```
interface Loopback1
 ip address 10.166.1.8 255.255.255.255
 ipv6 address FE80::8:10 link-local
 ipv6 address 2001:70:2:1000::8/52
 ipv6 enable
!
```