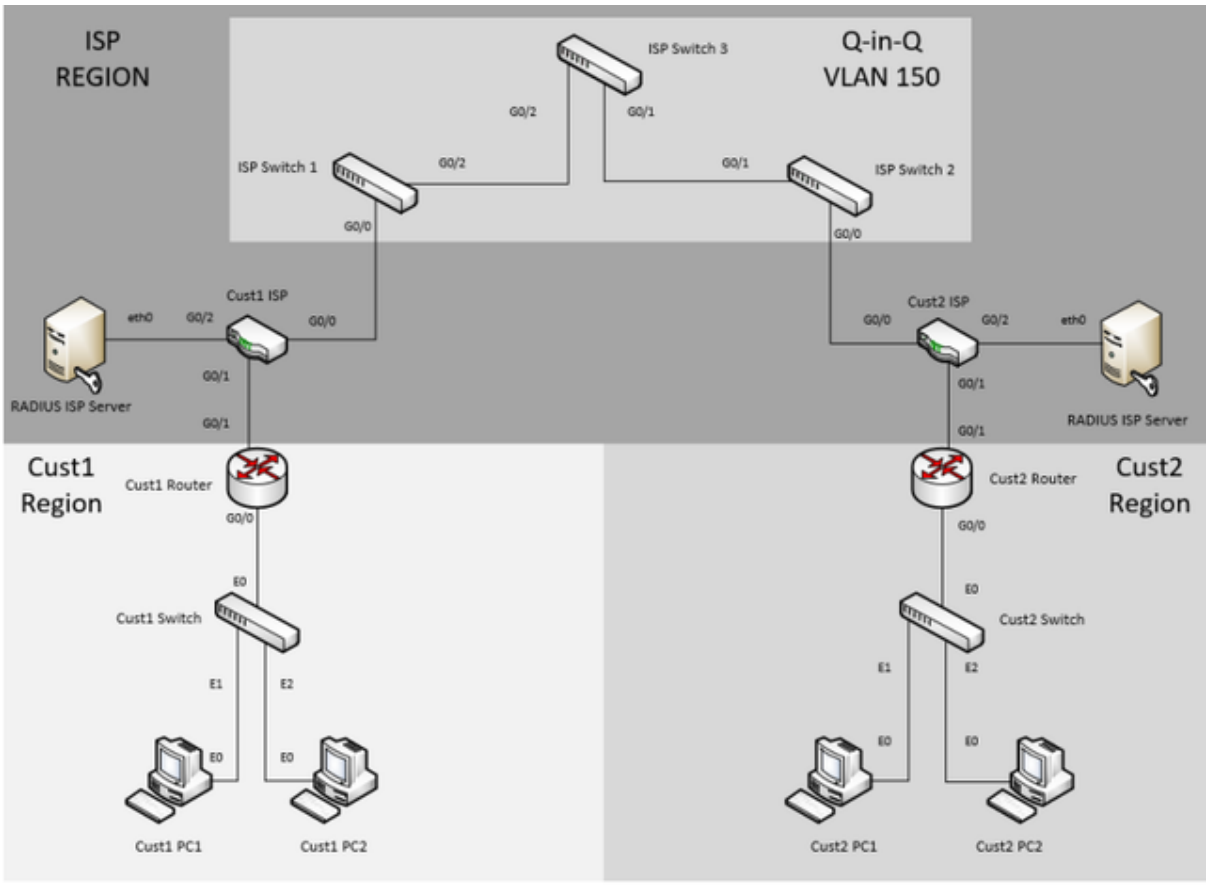


RADIUS PPPoE & Q-in-Q Tunneling

Ethan Linton

Table of Contents

Proposal – Outcomes

This section aims to outline the outcomes resulting from the completion of this project. A video demonstration showing the entire process is introduced later, along with proof-of-concept. Wireshark captures are presented via Cloudshark to avoid proprietary formats.

This project aims to successfully implement particular ISP elements within a GNS3 virtual environment using Cisco IOSvL2 switches, and Cisco IOSv routers. The implemented ISP elements within this project are as follows:

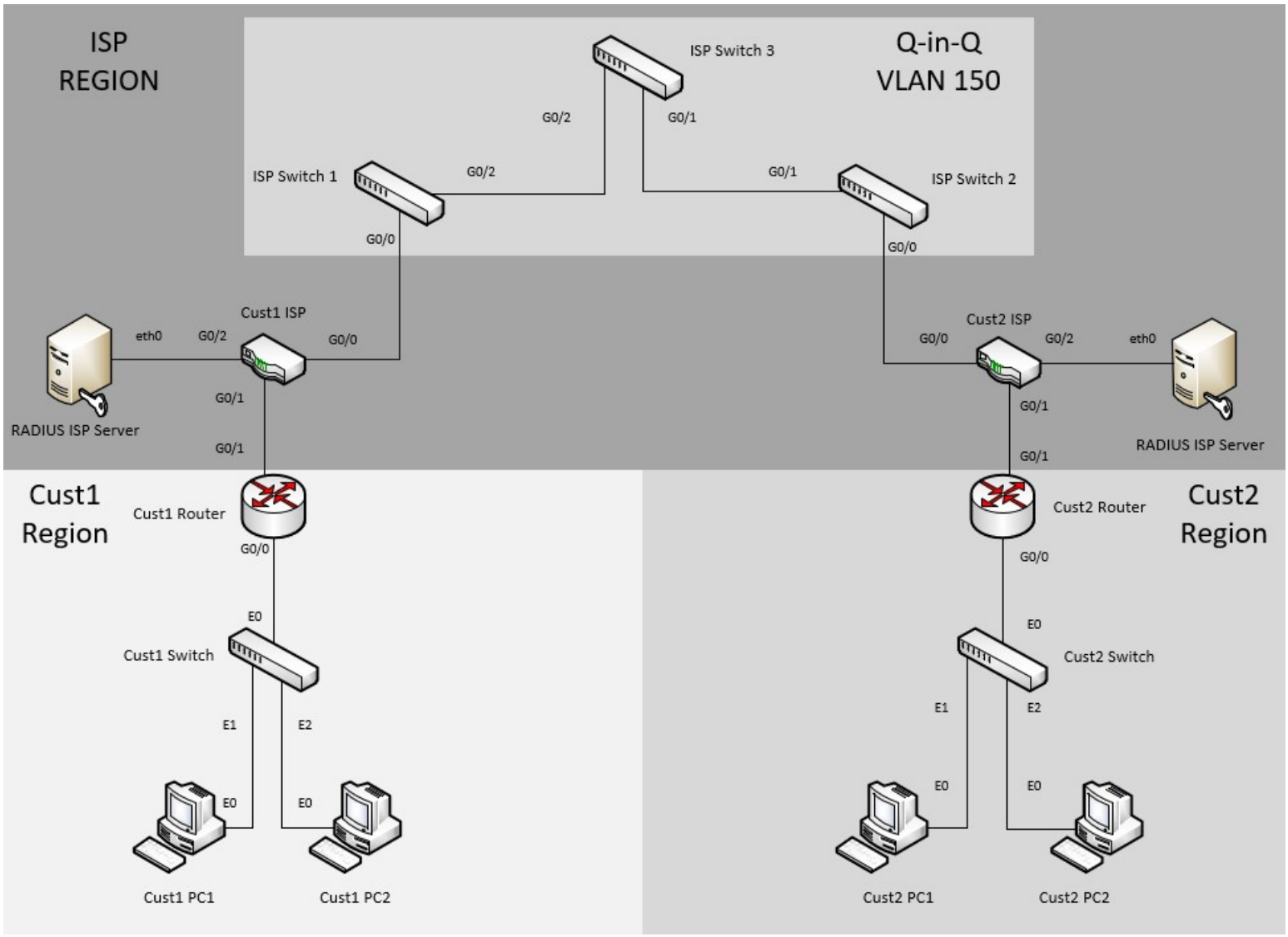
- RADIUS Authentication through PPPoE - Q-in-Q Tunneling.

Implementation of both ISP elements has been successful. The outcome of this implementation is as follows:

- PPPoE successfully authenticates Customer routers through the use of a FreeRadius server running within the ISP.
- When successfully authenticated, the interface Dialer1 of the Customer Router is granted an IP address. The Dialer1 interface is linked to the outgoing G0/1 interface of the Customer router. The result of being allocated this IP address is that hosts behind the Customer Router can now interact with the ISP network, simulating a real-life instance of a router connecting to an ISP.
- If a customer router becomes unauthenticated, the IP address is stripped, and the unauthenticated customer region can not interact with the ISP region.
- The result of being successfully authenticated against PPPoE, and with the Customer router now being allocated an IP address, the hosts of one Customer region can now ping the other hosts within another authenticated Customer region. All Customer regions are on VLAN 12, while the service-provider Q-in-Q tunneling region is allocated VLAN 150. This setup shows correct implementation of Q-in-Q tunneling as packets are double-tagged.
- Static routes have been set within each Customer region, allowing for successful pings across regions to provide proof-of-concept for the Q-in-Q tunneling implementation, taking note that static routes have been used instead of dynamic routing methods due to the size of the network (External/Internal BGP).
- DHCP has also been implemented on the Customer Router interface G0/0 of both regions. This is to provide IP addresses to clients automatically.

Ethan Linton

Logical Topology



Devices

- All Routers (Customer & ISP Routers)
    - Cisco IOSv Version 15.6(2)T 2016
- ISP Switches
    - Cisco vIOSl2 15.2 2017
- RADIUS ISP Servers
    - Ubuntu 16.04 LTS – FreeRadius Server running
- Customer Switches
    - Standard GNS3 Switches
- End Clients
    - GNS3 Virtual PCs.

Design considerations

During the design planning for this network, I had to take into consideration the needed elements that each device had to be capable of for completing this project. Due to Cisco virtual IOS images not including everything that the physical Cisco IOS counterpart contains, I had to ensure that elements such as Q-in-Q Tunneling, and PPPoE were possible on the images.

The choice of switches determined if the image was capable of configuring Q-in-Q tunneling. Luckily, as of recently, Cisco had updated their images to include the capability of configuring Q-in-Q tunneling on their vIOSl2 images.

The use of the standard GNS3 Switches and GNS3 Virtual PC's were made final as no configuration on the end-user switches was needed, along with only needing end-users as test clients for connectivity.

IP Addresses Allocated

Cust1 PC1	192.168.3.0 (DHCP)
Cust1 PC2	192.168.3.0 (DHCP)
Cust1 Switch	NULL
Cust1 Router G0/0 Dialer1	 192.168.3.1 192.168.2.0 (DHCP – PPPoE Interface)
Cust1 ISP G0/0.12 G0/2 Virtual-Template1	 192.168.4.1 (Sub-Interface) 192.168.1.10 192.168.2.9
RADIUS ISP Server	192.168.1.1
Cust2 PC1	192.168.12.0 (DHCP)
Cust2 PC2	192.168.12.0 (DHCP)
Cust2 Switch	NULL
Cust2 Router G0/0 Dialer1	 192.168.12.1 192.168.11.0 (DHCP – PPPoE Interface)
Cust2 ISP G0/0.12 G0/2 Virtual-Template1	 192.168.4.2 (Sub-Interface) 192.168.10.10 192.168.11.9
RADIUS ISP Server	192.168.10.1
ISP Switch 1/2/3	NULL

Proof-of-Concept

Q-in-Q Tunneling & PPPoE Video

The following linked video illustrates the use of PPPoE and Q-in-Q tunneling. Within this video, the Cust1_Router is running with incorrect credentials configured for PPPoE. This video shows that an IP address is not allocated, and pings fail if PPPoE is not authenticated. Also shown is authenticated PPPoE and a successful ping from Cust1_PC1, and Cust2_PC2, along with a Wireshark capture showing the execution of the Q-in-Q Tunnel.

https://www.youtube.com/watch?v=CkH91LFca30&feature=youtu.be

PPPoE Authentication

ISP routers were configured as PPPoE servers. The ISP routers authenticated against a FreeRadius server running on Ubuntu within the ISP region. The settings configured within the FreeRadius server are as follows:

Customer1 RADIUS ISP Server Users File –

```
Cust@ISPfirst   Auth-Type := CHAP, Cleartext-Password := "password1"
                    Framed-Protocol = PPP,
                    Framed-IP-Address = 255.255.255.254
```

Customer1 RADIUS ISP Server Clients.conf File –

```
client 192.168.1.10/32 {
    secret          = passw0rd
    shortname       = C1
    nastype         = cisco
}
```

Customer2 RADIUS ISP Server Users File –

```
Cust2@ISPsecond         Auth-Type:= CHAP, Cleartext-Password := "password2"
                            Framed-Protocol = PPP,
                            Framed-IP-Address = 255.255.255.254
```

Customer2 RADIUS ISP Server Clients.conf File –

```
client 192.168.10.10/32 {
    secret          = passw0rd2
    shortname       = C2
    nastype         = cisco
}
```

These configurations are taken from the FreeRadius server for both customer regions. As shown within the user file for the Customer 1 FreeRadius server, a user has been defined with the following parameters:

Username – Cust@ISPfirst

Password – password1

These details are what is needed for the customer router in the Customer 1 region to be authenticated against PPPoE.

Shown within the Customer 1 FreeRadius clients.conf file is the defined PPPoE server which is the ISP router. The IP address defined within this client parameter is the interface G0/2 (interface connected to the FreeRadius server) IP address of the ISP router for Customer 1. The secret defined for this client being “passw0rd” is needed to authenticate the ISP router as the PPPoE server.

PPPoE Customer router authentication

The following proof-of-concept was conducted via restarting the Dialer1 interface to force reauthentication for PPPoE on the Customer 1 Router. Figure 1 shows us that the Dialer 1 interface, after being restarted, attempts reauthentication with PPPoE, using the hostname and password configured shown in Figure 2. The response of reauthentication is a success, and the Dialer 1 interface is now allocated an IP address through IPCP.

For continue proof-of-concept, a successful ping from Cust1 PC1 (PC-1), to Cust2 PC1 (PC-4) captured within the Q-in-Q tunnel is shown in Figure 3, and the Wireshark file attached.

The following is a proof-of-concept showing the Customer router not having the correct credentials for PPPoE. Shown in Figure 4 the username has been changed to “wrong@username”. This resulted in a failure in authentication, and no IP address was allocated to the Dialer 1 interface. In result of this, the Customer 1 region can not reach the ISP network. Shown in Figure 5, when Cust1 PC1 attempts to ping Cust2 PC1 again, the pings timeout/fail. This is due to failed authentication of PPPoE on the Customer 1 router, resulting in no outgoing Customer 1 router IP address for the dialer 1 interface.

Q-in-Q Tunneling

All traffic going to and from each Customer region goes through a Q-in-Q tunnel located within the ISP region.

```
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 150
    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = DEI: Ineligible
    .... 0000 1001 0110 = ID: 150
    Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 12
    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = DEI: Ineligible
    .... 0000 0000 1100 = ID: 12
    Type: IPv4 (0x0800)
```

(Screenshot is taken from attached PPPoE Customer Router Authentication capture mentioned previously)

These packets were captured between ISP Switch 1 G0/0, and ISP Switch 3 G0/2, for a ping from Customer 1 PC and Customer 2 PC. As depicted from the screenshot above, while the packet transverses the Q-in-Q tunnel, a VLAN tag of 150 is added to the packet.

As shown within the Wireshark capture, it does note 802.1Q being used. Although, the output includes a drop eligibility indicator field (DEI). 802.1Q was superseded with 802.1ad, and in result of this 802.1ad replaced the previous canonical format identifier (CFI) with DEI. Due to this, we are technically seeing that the output is actually 802.1ad. [1]

In terms of the ethertype 0x8100 being used, this is the default setting for Cisco devices when configuring Q-in-Q tunneling. Cisco sees Q-in-Q as 802.1Q with frames tagged as 0x8100, while the IEEE sees Q-in-Q as 802.1ad with frames tagged as 0x88a8, although a standard implementation of 802.1ad Q-in-Q tunneling seems to use the ethertype of 0x8100 or 0x88a8. [2] The switches used within this project did not have the ability to change the ethertype. As of right now, only Cisco Nexus Switches have the ability to change the ethertype. With Cisco forcing 0x8100 ethertypes on many of their devices, this can cause interoperability issues within a multi-vendor setup, unless a Cisco Nexus switch is being used, or the other vendor provides 0x8100 tagged frames.

Pings & Wireshark captures

All pings for the Wireshark were captured between ISP_Switch 1 G0/2 and ISP_Switch 3 G0/2.

The following are the current associated IP addresses allocated to each end client through DHCP.

Cust1_PC1:

```
NAME        : PC-1[1]
IP/MASK     : 192.168.3.4/24
GATEWAY     : 192.168.3.1
DNS         :
DHCP SERVER : 192.168.3.1
DHCP LEASE  : 71009, 86400/43200/75600
MAC         : 00:50:79:66:68:00
LPORT       : 10028
RHOST:PORT  : 127.0.0.1:10029
MTU:        : 1500
```

Cust1_PC2:

```
NAME        : PC-2[1]
IP/MASK     : 192.168.3.5/24
GATEWAY     : 192.168.3.1
DNS         :
DHCP SERVER : 192.168.3.1
DHCP LEASE  : 84130, 86400/43200/75600
MAC         : 00:50:79:66:68:01
LPORT       : 10026
RHOST:PORT  : 127.0.0.1:10027
MTU:        : 1500
```

Cust2_PC1:

```
NAME        : PC-4[1]
IP/MASK     : 192.168.12.2/24
GATEWAY     : 192.168.12.1
DNS         :
DHCP SERVER : 192.168.12.1
DHCP LEASE  : 61332, 86400/43200/75600
MAC         : 00:50:79:66:68:03
LPORT       : 10052
RHOST:PORT  : 127.0.0.1:10053
MTU:        : 1500
```

Cust2_PC2:

```
NAME        : PC-3[1]
IP/MASK     : 192.168.12.3/24
GATEWAY     : 192.168.12.1
DNS         :
DHCP SERVER : 192.168.12.1
DHCP LEASE  : 61360, 86400/43200/75600
MAC         : 00:50:79:66:68:02
LPORT       : 10054
RHOST:PORT  : 127.0.0.1:10055
MTU:        : 1500
```

The following are clickable links to a capture file-sharing website named CloudShark (to avoid proprietary formats).

Cust1_PC1 to Cust2_PC1

Cust1_PC1 to Cust2_PC2

Cust1_PC2 to Cust2_PC1

Cust1_PC2 to Cust2_PC2

Cust2_PC1 to Cust1_PC1

Cust2_PC1 to Cust1_PC2

Cust2_PC2 to Cust1_PC1

Cust2_PC2 to Cust1_PC2

As shown, all pings are successful between each host on each customer region along with the Q-in-Q tunnel double tagging successfully working.

Configuration annotation

Full configurations are attached to the submission, but this section covers critical sections within the configuration of each device that play a vital part in the implementation of PPPoE, and Q-in-Q.

Cust1_ISP (Same as Cust2_ISP):

```
interface GigabitEthernet0/0.12
 encapsulation dot1Q 12
 ip address 192.168.4.1 255.255.255.0
!
```

This is the configuration for the subinterface of G0/0, being G0/0.12. *Encapsulation dot1Q 12* sets the encapsulation type as dot1q (IEEE 802.1Q Virtual LAN) with an allocated VLAN ID being 12. It instructs the router that when using the G0/0.12 sub interface, it tags all frames with VLAN 12 so that in this case the ISP_Switch_1 trunk port configured on the switch port at the other end can figure out that it belongs to VLAN 12.

A sub-interface was used because you cannot set encapsulation settings on 'normal' router interfaces.

```
interface GigabitEthernet0/1
 description Connection to Customers
 no ip address
 duplex auto
 speed auto
 media-type rj45
 pppoe enable group global
!
```

This is the configuration for the connection between Cust1_ISP, and Cust1_Router. As shown, the *pppoe enable group global* command enables PPPoE on the interface and attaches the BBA group 'Global' to the interface.

```
bba-group pppoe global
 virtual-template 1
```

The bba-group was created with the shown command, and a virtual-template interface was attached to the BBA group 'Global.'

```
interface Virtual-Template1
 ip address 192.168.2.9 255.255.255.0
 peer default ip address pool localpool
 ppp authentication chap
!
```

The virtual interface is responsible for dealing with the DHCP requests for Dialer1 when the Customer router has authenticated with PPPoE. The *peer default ip address pool localpool* command enables a set DHCP pool of addresses to be allocated in this case to the Dialer 1 interface on the Customer 1 router.

```
ip local pool localpool 192.168.2.1 192.168.2.30
ip dhcp excluded-address 192.168.2.9
```

Shown here is the configuration pool of IP addresses. As shown previously, the Dialer1 interface acquires an IP address between 192.168.2.1 – 192.168.2.30 when the Customer 1 router has been authenticated with PPPoE.

```
radius server rad_isp
 address ipv4 192.168.1.1 auth-port 1812 acct-port 1813
 key passw0rd
```

This is the configuration for the FreeRadius server. This is how the ISP routers communicate with their allocated FreeRadius server. A name being 'rad_isp' was defined for the ISP 1 FreeRadius server. The server IP address of the FreeRadius server was then entered being

'192.168.1.1', along with the authentication and accounting ports, and the secret key which was defined on the FreeRadius server.

```
aaa new-model
!
!
aaa authentication ppp default group radius
```

Aaa new-model enables newer access control commands and functions, being the next shown command *aaa authentication ppp default group radius*, which sets an AAA authentication PPP list for all Radius hosts.

Cust1_Router (Same as Cust2_Router):

```
interface GigabitEthernet0/0
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
!
```

Interface G0/0 configuration for connection to end clients. Default-router on end clients is set to the defined IP within the G0/0 interface being 192.168.3.1.

```
interface Dialer1
 mtu 1492
 ip address negotiated
 encapsulation ppp
 dialer pool 1
 ppp authentication chap callin
 ppp chap hostname Cust@ISPfirst
 ppp chap password 0 password1
!
```

Dialer1 interface configuration in which is attached to the outgoing G0/1 interface towards the ISP router. Dialer pool to be used is specified as '1'. Encapsulation has been set to PPP. PPP Link authentication method has been set using the command *ppp authentication chap callin* with the Challenge Handshake Authentication Protocol (RADIUS-CHAP) enabled, and with authentication remote on incoming call only (*callin*). *PPP chap hostname/password* parameters are defined to authenticate with PPPoE. These credentials are set on the FreeRadius server. If these credentials are incorrect then PPPoE will fail to authenticate.

```
interface GigabitEthernet0/1
 description Connection to ISP router
 no ip address
 ip access-group ICMP out
 duplex auto
 speed auto
 media-type rj45
 pppoe enable group global
 pppoe-client dial-pool-number 1
!
```

Interface G0/1 configuration in which is the outgoing port connected to the ISP router. PPPoE has been enabled on this port, with the bba-group 'Global' attached. This interface is assigned with the PPPoE dial group being the interface Dialer1 (*pppoe-client dialpool-number 1*).

```
ip dhcp excluded-address 192.168.3.1
!
ip dhcp pool home-POOL
 network 192.168.3.0 255.255.255.0
 default-router 192.168.3.1
!
```

This DHCP pool was created for assigning IP addresses to the end clients behind the Cust1_router with an exclusion set for 192.168.3.1 since that is the defaultrouter IP address.

ISP_Switch_1 (Same as ISP_Switch_2):

```
interface GigabitEthernet0/0
 switchport access vlan 150
 switchport mode dot1q-tunnel
 media-type rj45
 negotiation auto
!
```

This is the configuration for port G0/0, facing the Customer 1 ISP router. This port has *switchport access* enabled, with a VLAN ID of 150 assigned. *Switchport mode dot1q-tunnel* sets the trunking mode for the interface to tunnel unconditionally.

```
interface GigabitEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
!
```

This is the configuration for port G0/2 connected to ISP_Switch_3. *Switchport trunk encapsulation dot1q* sets the trunking characteristics of the interface to only use 802.1q trunking encapsulation when trunking.

ISP_Switch_3:

```
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
!
interface GigabitEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
!
```

Shown in this figure are the configurations for the interfaces G0/2, and G0/1. Both of these interfaces face ISP_Switch_1, and ISP_Switch_2 respectively. Both interfaces only allow the use of 802.1Q trunking encapsulation when trunking.

The command *VLAN 150* in global configuration mode was also used to make the router aware of such VLAN being used.

Figures

Figure 1 – PPPoE Authentication and IP address allocation (Cust1_Router)

```
HomeRouter#debug ppp authentication
PPP authentication debugging is on
HomeRouter#
HomeRouter#clear dialer
HomeRouter#clear dialer sessions
HomeRouter#
HomeRouter#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HomeRouter(config)#int dialer 1
HomeRouter(config-if)#shut
HomeRouter(config-if)#
*Sep  1 02:53:11.158: %DIALER-6-UNBIND: Interface Vi2 unbound from profile Di1
*Sep  1 02:53:11.172: Di1 DDR: dialer shutdown complete
*Sep  1 02:53:11.217: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2, changed state to downn
HomeRouter(config-if)#no shut
*Sep  1 02:53:11.221: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to down
HomeRouter(config-if)#no shut
HomeRouter(config-if)#e
*Sep  1 02:53:13.178: %LINK-5-CHANGED: Interface Dialer1, changed state to administratively down
HomeRouter(config-if)#
*Sep  1 02:53:16.119: %LINK-3-UPDOWN: Interface Dialer1, changed state to up
HomeRouter(config-if)#
HomeRouter(config-if)#exit
HomeRouter(config)#exit
HomeRouter#
HomeRouter#
*Sep  1 02:53:33.137: %SYS-5-CONFIG_I: Configured from console by console
*Sep  1 02:53:33.331: %DIALER-6-BIND: Interface Vi2 bound to profile Di1
*Sep  1 02:53:33.333: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to up
*Sep  1 02:53:33.352: Vi2 PPP: Using dialer call direction
*Sep  1 02:53:33.353: Vi2 PPP: Treating connection as a callout
*Sep  1 02:53:33.353: Vi2 PPP: Session handle[CC000004] Session id[4]
*Sep  1 02:53:33.386: Vi2 PPP: No authorization without authentication
*Sep  1 02:53:33.387: Vi2 CHAP: I CHALLENGE id 1 len 24 from "ISP"
*Sep  1 02:53:33.388: Vi2 PPP: Sent CHAP SENDAUTH Request
*Sep  1 02:53:33.391: Vi2 PPP: Received SENDAUTH Response FAIL
*Sep  1 02:53:33.392: Vi2 CHAP: Using hostname from interface CHAP
*Sep  1 02:53:33.392: Vi2 CHAP: Using password from interface CHAP
*Sep  1 02:53:33.392: Vi2 CHAP: O RESPONSE id 1 len 34 from "Cust@ISPfirst"
*Sep  1 02:53:33.467: Vi2 CHAP: I SUCCESS id 1 len 4
HomeRouter#
*Sep  1 02:53:33.485: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2, changed state to up
HomeRouter#
HomeRouter#
HomeRouter#sh ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         192.168.3.1     YES manual up                    up
GigabitEthernet0/1         unassigned      YES NVRAM  up                    up
GigabitEthernet0/2         unassigned      YES NVRAM  up                    up
GigabitEthernet0/3         unassigned      YES NVRAM  administratively down down
Dialer1                    192.168.2.6     YES IPCP   up                    up
Virtual-Access1            unassigned      YES unset  up                    up
Virtual-Access2            unassigned      YES unset  up                    up
HomeRouter#
```

Figure 2 – Hostname and Password configured for PPPoE

```
interface Dialer1
 mtu 1492
 ip address negotiated
 encapsulation ppp
 dialer pool 1
 ppp authentication chap callin
 ppp chap hostname Cust@ISPfirst
 ppp chap password 0 password1
```

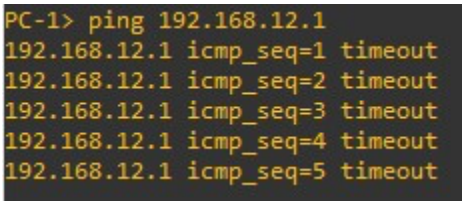
Figure 3 – Cust1_PC1 pings Cust2_PC1

```
PC-1> ping 192.168.12.1
84 bytes from 192.168.12.1 icmp_seq=1 ttl=252 time=11.461 ms
84 bytes from 192.168.12.1 icmp_seq=2 ttl=252 time=13.180 ms
84 bytes from 192.168.12.1 icmp_seq=3 ttl=252 time=14.355 ms
84 bytes from 192.168.12.1 icmp_seq=4 ttl=252 time=15.985 ms
84 bytes from 192.168.12.1 icmp_seq=5 ttl=252 time=12.441 ms
```

Figure 4 – Incorrect PPPoE Credentials

```
Cust1_Router(config)#
*Sep  1 03:12:40.688: Vi2 PPP: Using dialer call direction
*Sep  1 03:12:40.688: Vi2 PPP: Treating connection as a callout
*Sep  1 03:12:40.688: Vi2 PPP: Session handle[6F000005] Session id[5]
*Sep  1 03:12:40.714: Vi2 PPP: No authorization without authentication
*Sep  1 03:12:40.714: Vi2 CHAP: I CHALLENGE id 1 len 24 from "ISP"
*Sep  1 03:12:40.714: Vi2 PPP: Sent CHAP SENDAUTH Request
*Sep  1 03:12:40.716: Vi2 PPP: Received SENDAUTH Response FAIL
*Sep  1 03:12:40.716: Vi2 CHAP: Using hostname from interface CHAP
*Sep  1 03:12:40.716: Vi2 CHAP: Using password from interface CHAP
*Sep  1 03:12:40.716: Vi2 CHAP: O RESPONSE id 1 len 35 from "wrong@username"
*Sep  1 03:12:41.731: Vi2 CHAP: I FAILURE id 1 len 25 msg is "Authentication failed"
*Sep  1 03:12:41.739: %DIALER-6-UNBIND: Interface Vi2 unbound from profile Di1
Cust1_Router(config)#
*Sep  1 03:12:41.742: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to down
Cust1_Router(config)#
Cust1_Router(config)#
Cust1_Router(config)#do sh ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         192.168.3.1     YES manual up                    up
GigabitEthernet0/1         unassigned      YES NVRAM  up                    up
GigabitEthernet0/2         unassigned      YES NVRAM  up                    up
GigabitEthernet0/3         unassigned      YES NVRAM  administratively down down
Dialer1                    unassigned      YES IPCP   up                    up
Virtual-Access1            unassigned      YES unset  up                    up
Virtual-Access2            unassigned      YES unset  down                  down
```

Figure 5 – Failed pings resulted from failed PPPoE Authentication



References

[1] Wikipedia, "IEEE 802.1ad," 10 August 2019. [Online]. Available: https://en.wikipedia.org/wiki/IEEE_802.1ad.

[2] G. Shaw, "IEEE 802.1ad," 2018. [Online]. Available: http://www.microhowto.info/tags/802.1ad.html.