How To | Configure Allied Telesis and Cisco routers to interoperate over L2TP

Introduction

This document covers a range of examples on how to configure Allied Telesis and Cisco routers to interoperate over Layer 2 Tunnelling Protocol (L2TP). The two main components that make up L2TP are the L2TP Access Concentrator (LAC), which is the device that physically terminates a call and the L2TP Network Server (LNS), which is the device that terminates and potentially authenticates the PPP stream.

What information will you find in this document?

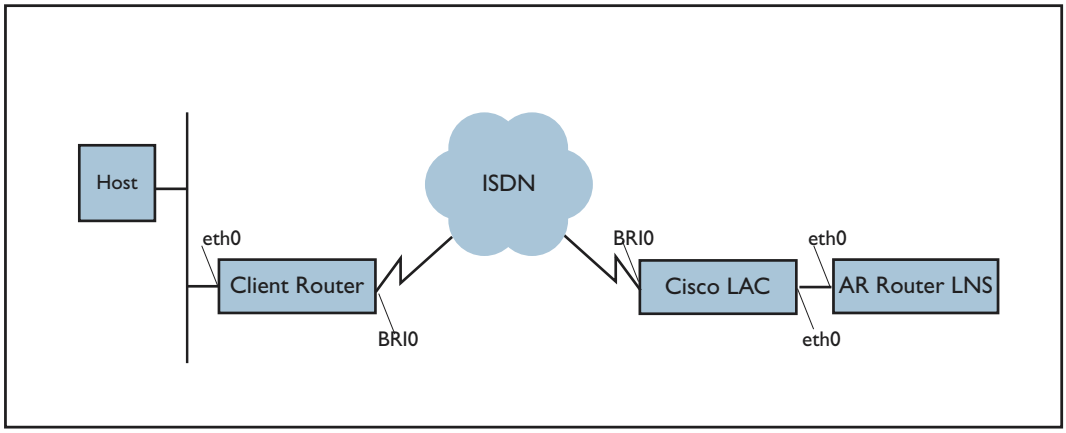
This document contains the following sections:

Which products and software versions does this information apply to?

- Products:
  Rapier, AT-8800, AT-8900, AT-9900, AT-9800 and SwitchBlade series switches
  AR400 and AR700 series routers
- Software versions: 2.7.1 and later

Example 1 - Cisco as LAC, Allied Telesis router as LNS, no RADIUS

In this example the LAC is configured with a Virtual Private Dial-up Network (VPDN) group, which specifies the IP address of the LNS and the L2TP username, and is associated with a matching entry in the user database containing the password to send to the LNS for L2TP authentication.



Some points to note:

a On the Client router:

In this particular setup it is not really necessary to configure a username with a domain suffix as it is being authenticated locally by the LNS rather than by RADIUS.

b On the LAC:

Under "vpdn-group 1" the local name "lac" is what the router will send to the LNS as its L2TP username. If no local name is configured the router's hostname will be used instead.

c On the LNS:

Allied Telesis routers do not have an equivalent to Cisco's "local name" command. The system name of the Allied Telesis router is always used as the L2TP username

```
Client Router Configuration
set system name="user"

add isdn call=l2tp number=12345 precedence=out

create ppp=0 idle=60 over=isdn-l2tp
set ppp=0 iprequest=on username="username@domain.com" password="password"

enable ip
enable ip remote
add ip int=ppp0 ip=0.0.0.0
add ip int=eth0 ip=192.168.1.1
```

LAC Configuration on Cisco Router:

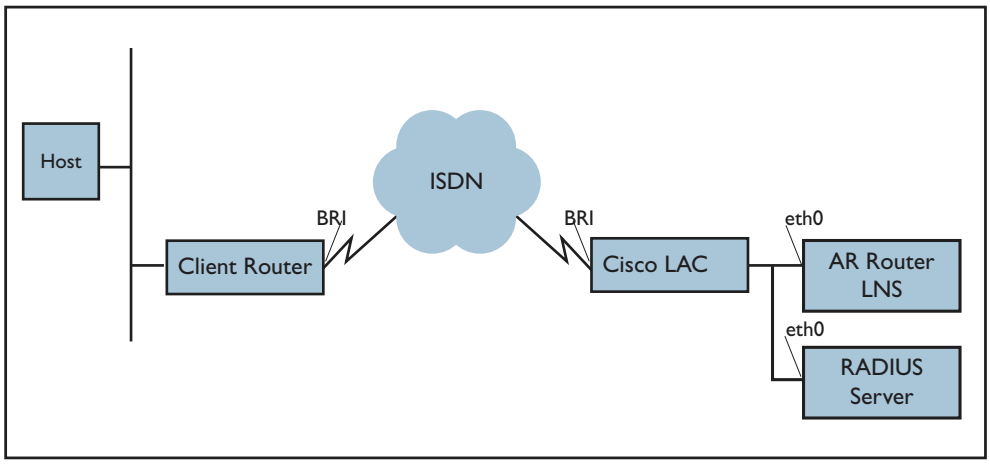
```
hostname lac

username lac password 0 lns
username lns password 0 lns

ip subnet-zero

vpdn enable
vpdn search-order domain

vpdn-group 1
 request-dialin
 protocol l2tp
 domain domain.com
 initiate-to ip 200.1.1.1
 local name lac

isdn switch-type basic-net3

interface Ethernet0
 ip address 200.1.1.2 255.255.255.0

interface BRI0
 no ip address
 encapsulation ppp
 dialer idle-timeout 60
 isdn switch-type basic-net3
 no fair-queue
 ppp authentication chap

ip classless
ip route 0.0.0.0 0.0.0.0 BRI0
ip http server
```

LNS configuration on Allied Telesis Router:

```
set system name="lns"

add user=username@domain.com pass=password lo=no priv=user

create ppp template=1
set ppp template=1 bap=off ippool="pool1" authentication=chap mtu=1450
set ppp template=1 lqr=off echo=30

enable l2tp
enable l2tp server=lns
add l2tp password="lns"
add l2tp ip=0.0.0.0-255.255.255.255 ppptemplate=1

enable ip
add ip int=eth0 ip=200.1.1.1
add ip rou=0.0.0.0 mask=0.0.0.0 int=eth0 next=200.1.1.2
create ip pool="pool1" ip=200.1.1.50-200.1.1.100

create firewall policy="l2tp"
enable firewall policy="l2tp" icmp_f=all
create firewall policy="l2tp" dy=dynamic
add firewall policy="l2tp" dy=dynamic us=any
add firewall policy="l2tp" int=dyn-dynamic type=private
add firewall policy="l2tp" int=eth0 type=public
```

Example 2 - Cisco as LAC, Allied Telesis router as LNS, using RADIUS to pass L2TP parameters to the LAC

In this example there is no VPDN group configuration on the LAC. Instead, the L2TP process will send the client's domain-name to a RADIUS server, and will ask that server for the IP address of the LNS, and the username and password to send to the LNS for L2TP authentication.



Some points to note:

a On the Client Router:

Note the password of "cisco" that is configured on PPP0. This is the L2TP password that the Cisco LAC uses by default.

b On the LAC:

Note that in this example there is a "global" RADIUS password configured with the command:

```
radius-server key hotlinkstest
```

There is also a "radius host" RADIUS password that is configured with the command:

```
radius-server host 217.14.129.3 auth-port 1812 acct-port 1813 key hotlinks
```

This command overrides the "global" RADIUS password when configured.

Client Router Configuration:

```
set system name="steel"

add isdn call=l2tp num=12345 prec=out direction=out

create ppp=0 idle=60 over=isdn-l2tp
set ppp=0 iprequest=on username="username@domain.com" password="cisco"

enable ip
enable ip remote
add ip int=ppp0 ip=0.0.0.0
add ip int=eth0 ip=192.168.1.1
add ip rou=0.0.0.0 mask=0.0.0.0 int=ppp0 next=0.0.0.0
```

LAC Configuration on Cisco Router:

```
hostname lac

boot-start-marker
boot-end-marker

aaa new-model

aaa authentication ppp isdn local
aaa authorization network default local group radius
aaa session-id common
ip subnet-zero

vpdn enable
vpdn search-order domain

isdn switch-type basic-net3
interface Ethernet0
 ip address 202.49.72.16 255.255.255.224

interface BRI0
 ip unnumbered Ethernet0
 encapsulation ppp
 dialer idle-timeout 60
 isdn switch-type basic-net3
 isdn point-to-point-setup
 no fair-queue
 ppp authentication chap isdn

ip http server
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet0 202.49.72.30
ip route 192.168.1.0 255.255.255.0 BRI0 192.168.1.1

no radius-server attribute nas-port
radius-server host 217.14.129.3 auth-port 1812 acct-port 1646 key hotlinks
radius-server key hotlinkstest
radius-server vsa send authentication
```

LNS configuration on Allied Telesis Router:

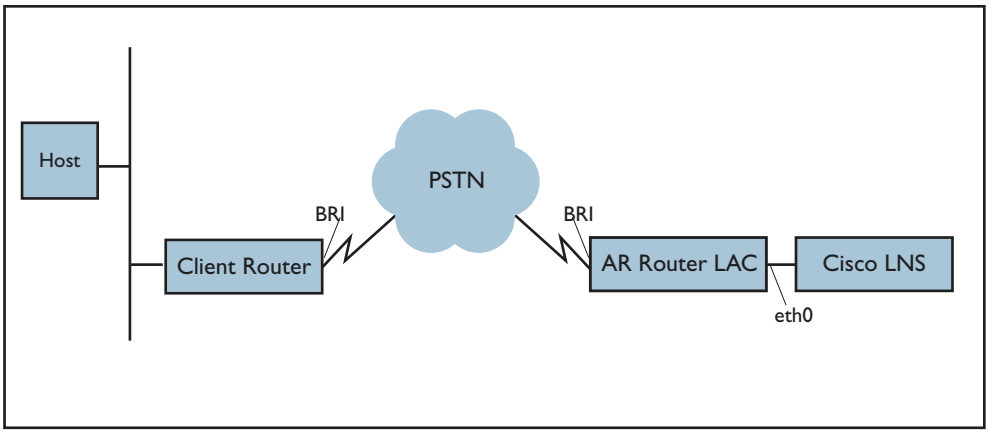
```
set system name="steel"

add user=username@domain.com password=cisco lo=no privilege=user

create ppp template=1
set ppp template=1 bap=off ippool="ippool1" authentication=chap mtu=1450
set ppp template=1 lqr=off echo=30

enable l2tp
enable l2tp server=lns
add l2tp password="steel"
add l2tp ip=0.0.0.0-255.255.255.255 ppptemplate=1

enable ip
add ip int=eth0 ip=217.14.130.34 mask=255.255.255.252
add ip rou=0.0.0.0 mask=0.0.0.0 int=eth0 next=217.14.130.33
create ip pool="ippool1" ip=217.14.131.66-217.14.131.254

create firewall policy="l2tp"
create firewall policy="l2tp" dy=dynamic
add firewall policy="l2tp" dy=dynamic us=any
add firewall policy="l2tp" int=dyn-dynamic type=private
add firewall policy="l2tp" int=eth0 type=public
```

RADIUS profile

```
username@domain.com  Auth-Type = Local, Password = "cisco"
        Service-Type = Framed-User,
        Tunnel-Medium-Type = IP,
        Tunnel-Type = L2TP,
        Tunnel-Server-Endpoint = 217.14.130.34,
        Tunnel-Password = steel,
        Tunnel-Client-Auth-Id = steel,
        Tunnel-Server-Auth-Id = steel
```

Example 3 - Cisco as LNS, Allied Telesis router as LAC

This is an example where the connection from the client to the LAC is by Async.



Client Router Configuration:

```
set sys name=Router_A
set asyn=1 speed=9600 cdc=connect flow=hard

add acc call=call1 asyn=1 encap=ppp dscript=dial.mds dir=originate  authen=none

create ppp=1 over=acc-call1 idle=on bap=off iprequest=on user=Router_A
set ppp=1 over=acc-call1 lqr=off echo=30 pass=password2

ena ip
ena ip remote
add ip int=ppp1 ip=0.0.0.0
add ip int=eth0 ip=192.168.45.1
```

LAC Configuration on Allied Telesis Router:

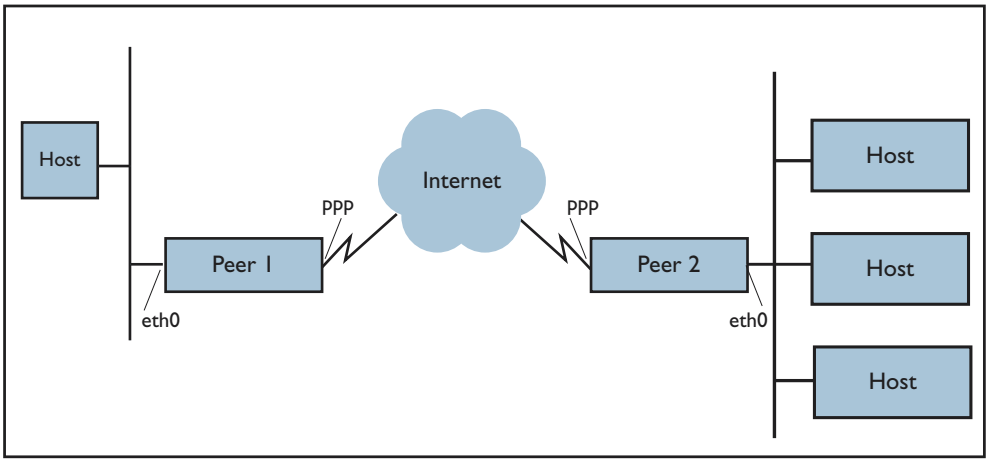
```
set sys name=lac
set asyn=1 speed=9600 cdc=connect flow=hard

enable ip
add ip int=eth0 ip=10.17.39.210 mask=255.255.255.0
add ip int=vlan1 ip=10.34.2.33 mask=255.255.255.248

ena l2tp
ena l2tp server=lac
set l2tp password=password
add l2tp user=Router_A action=database ip=10.17.39.211

create ppp template=1 bap=off authen=pap
add acc call=call1 asyn=1 encap=ppp ppptempl=1 dir=answer authen=none
```

LNS Configuration on Cisco Router:

```
hostname lns

username lac password password
username Router_A password password2
username lns password password
ip subnet-zero

vpdn enable

vpdn-group 1
 accept-dialin
  protocol any
  virtual-template 1
 terminate-from hostname lac
 local name lns

interface Loopback1
 ip address 20.20.20.2 255.255.255.0

interface Ethernet0
 ip address 10.17.39.211 255.255.255.0
 no ip redirects
 no keepalive

interface Virtual-Template1
 ip unnumbered Loopback1
 no ip route-cache
 peer default ip address pool mypool

ip local pool mypool 20.20.20.1
ip classless
ip http server

dialer-list 1 protocol ip permit
no cdp run
```

Example 4 - Cisco and Allied Telesis router as peers over virtual tunnel

All the previous examples involve a client calling an LAC, and being tunnelled through to an LNS. But in this example, L2TP is simply being used to tunnel data across the Internet between two peer routers.



Configuration on Allied Telesis Router peer:

```
enable l2tp
enable l2tp server=both
add l2tp call="remote" rem="tunnel" ip=211.132.221.233 ty=virtual prec=out

create ppp=0 idle=240 over=tnl-remote
set ppp=0 iprequest=on username="username" password="password"

enable ip
enable ip remote
add ip int=eth0 ip=192.168.1.10
add ip int=eth1 ip=10.34.1.1 mask=255.255.255.0
add ip int=ppp0 ip=0.0.0.0 mask=0.0.0.0
add ip rou=0.0.0.0 mask=0.0.0.0 int=ppp0 next=0.0.0.0
add ip rou=211.132.221.0 mask=255.255.255.0 int=eth0 next=192.168.1.5
```

Configuration on Cisco Router peer:

```
username username password 0 password

vpdn enable
vpdn-group vpns
 Default L2TP VPDN group
 Default PPTP VPDN group
 accept-dialin
  protocol any
  virtual-template 1
 local name remote
 no l2tp tunnel authentication
 l2tp tunnel timeout no-session 30

interface FastEthernet0/0
 ip address 211.132.221.233 255.255.255.0
 duplex auto
 speed auto

interface Virtual-Template1
 ip address 172.20.1.100 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip mroute-cache
 peer default ip address pool default
 ppp authentication chap

ip local pool default 172.20.1.1 172.20.1.50
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0 211.132.221.1
```

USA Headquarters | 19800 North Creek Parkway | Suite 200 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesis.com

C613-16070-00 REV B

Connecting The IP World

Allied Telesis