

Preface

As the pace of economic globalization picks up, more and more enterprises have set up branch offices beyond the geographical boundaries. Traditionally, private leased lines are used to connect the headquarters with its branch offices. The cost of private lease lines, however, is very high that it has become a huge financial burden to enterprises with large number of branch offices all over the world. VPN (Virtual Private Network) technology was then developed as the solution to this problem.

This white paper explains in details one of Xtera's newly-developed VPN related technologies called Tunnel Routing. This unique technology addresses the problem of VPN load balancing in a network with dynamic IP addresses. It also frees the risk of VPN downtime and supports the bi-directional VPN load balancing.

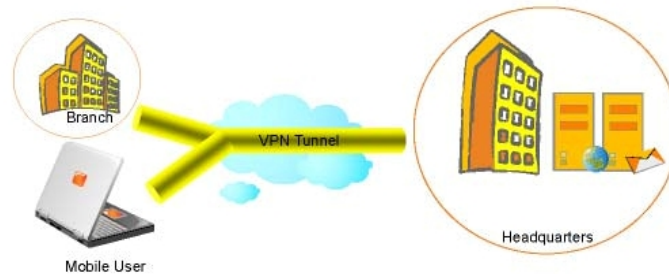
Challenge

To better manage corporate internal information and provide better services to clients, enterprises usually implement some sorts of information management system, such as ERP, OA, BI, and SCM, etc. These C/S (Client/Server) and B/S (Browser/Server) service models, however, are only available from the LAN of the headquarters, which means that branch offices cannot access such information resource inside the headquarters from the outside. The challenge then is to enable branch offices to access the information resources from the headquarters as if inside the LAN of headquarters and bring LAN-like access from the WAN side.

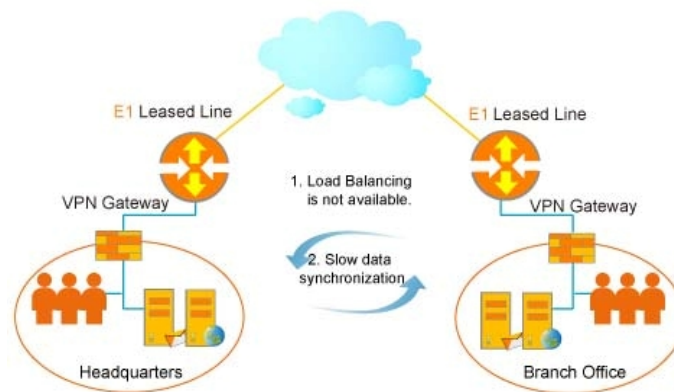


VPN technology is to employ IPsec or MPLS network to establish VPN Tunnels among the networks of headquarters and branch offices, so that the different LANs could access to one another across the WAN, and 'LAN-like' file or print services can be delivered to different branch offices across the WAN links. Mobile users and users from branch offices could conveniently access the corp. headquarters resources as if from the inside of the local network.

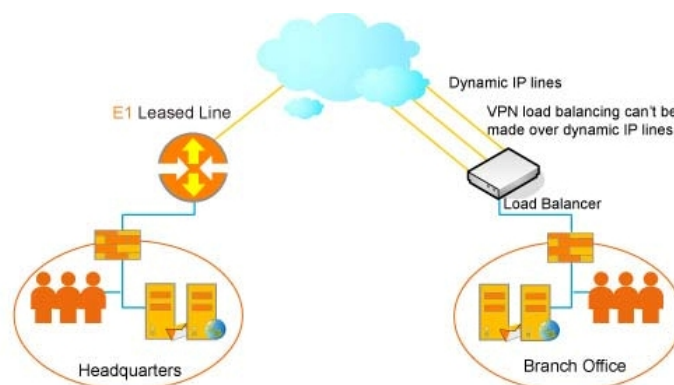
The following picture illustrates the deployment scenario of VPN:



The leased line such as DDN is expensive, although it is of high stability and reliability. More and more enterprises prefer VPN over public Internet, also known as IPSec VPN, to reduce the operating costs. Despite the relative inexpensive costs, IPSec VPN however has the issue of reliability as well as insufficient bandwidth: VPN can only be connected via a single link, and it is not possible to load balance VPN across multiple lines. As a result, the stability of key applications running on top of the VPN connection cannot be guaranteed.



For enterprises with multiple branch offices, IPSec VPN is used to connect between the headquarters and branch offices for VoIP, Video Conferencing, or critical corporate applications such as ERP or CRM. Broadband WAN connection such as ADSL often times is used for smaller branch office connectivity for cost consideration. The issues of running IPSec VPN on a single WAN link, particularly on ADSL, are for both reliability and insufficient bandwidth.



AscenLink Solution

An ideal solution to the IPSec VPN issues mentioned above, is to be able to enjoy the cheaper broadband infrastructure while maintaining high reliability as well as high throughput by running a virtual network on top of multiple ADSL connections. Xtera develops the Tunnel Routing technology and integrates this unique technology in the flagship product, AscenLink. Running a virtual tunnel network across multiple WAN links is nothing special. With our Tunnel Routing mechanism, however, VPN load balancing can be performed even in the network with dynamic IP addresses. By integrating multiple links, AscenLink could perform link backup and establish tunnel routing on a group of ADSL lines with dynamic IP addresses so as to bring LAN-like Intranet access to the branch offices via WAN links.

Working Mechanism of Tunnel Routing:

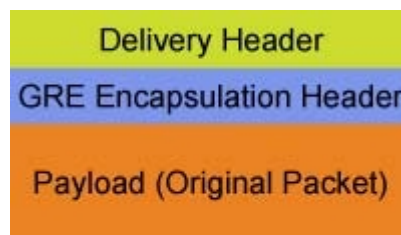
Tunnel is the foundation of the VPN technology, which is to establish a Point-to-point, encrypted pipe on Internet. All packets through the VPN tunnel will be encrypted and could only be transferred via this tunnel. AscenLink sets up a proprietary tunnel which we called "Tunnel Routing" between source and destination sites with GRE (Generic Routing Encapsulation) protocol to make the VPN can be load balanced.

GRE (Generic Routing Encapsulation) Protocol packs the Payload (Original Packet) with Delivery Header and GRE Encapsulation Header. Then the packet is routed to the destination IP address.

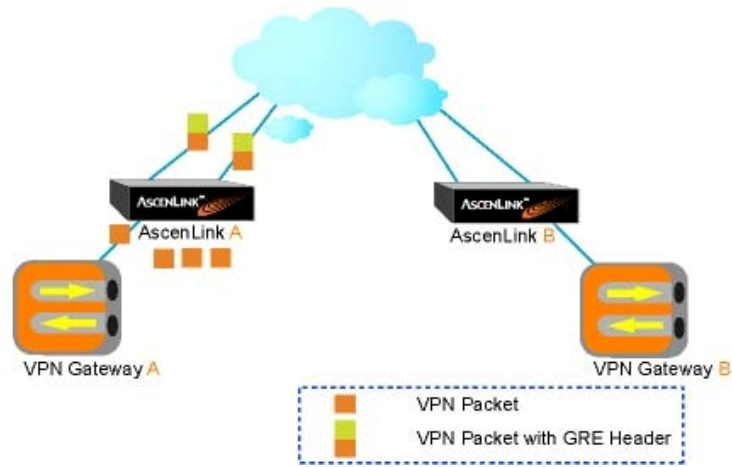
The feature of AscenLink's Tunnel Routing is that with proper policy setting it can do the routing between a single point and multiple points as well as between multiple points and multiple points. When packet arrives at the destination IP, the remote AscenLink on destination will decapsulate the packet to regain the source and destination IP address and forward the packet to the target host, so the LANs in different locations can do communications with AscenLink directly.

Being packed with GRE header and given the new source and destination IP address, the original packet could be transferred via multiple links according to the defined Tunnel Routing rules. Furthermore, should WAN link break down, AscenLink's WLHD function would reroute the packet to the healthy WAN link so that the network connection and the data transfer reliability are guaranteed. Even the traffic of the most severe appliance as VPN connection can be guaranteed by Tunnel Routing, what else Tunnel Routing can not do.

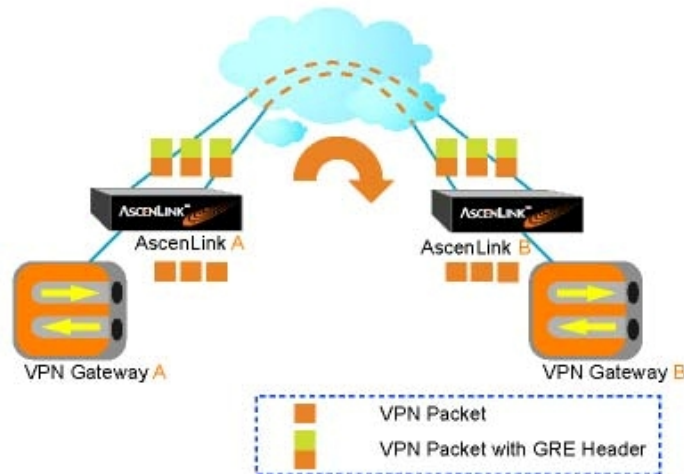
The following four pictures illustrate the work mechanism of Tunnel Routing and how packet is transferred from VPN Gateway A to Gateway B:



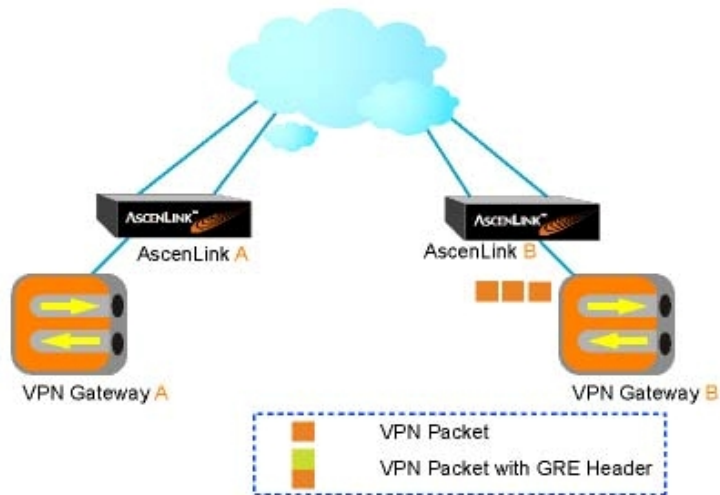
Packet Structure



AscenLink A gives VPN packets a VPN Delivery Header



VPN packets are transferred to AscenLink B via Tunnel Routing on multiple links



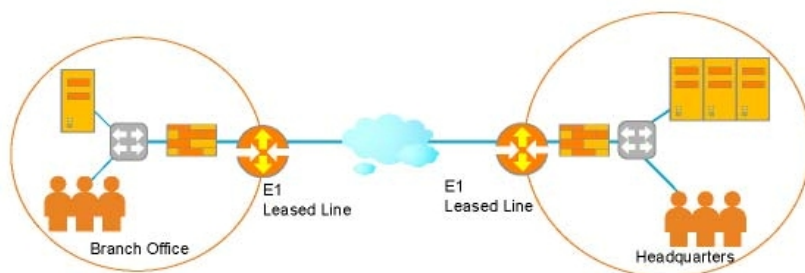
AscenLink B unpacks the packet and then resends the packet to VPN Gateway B

Example

■ VPN load balancing on multiple links

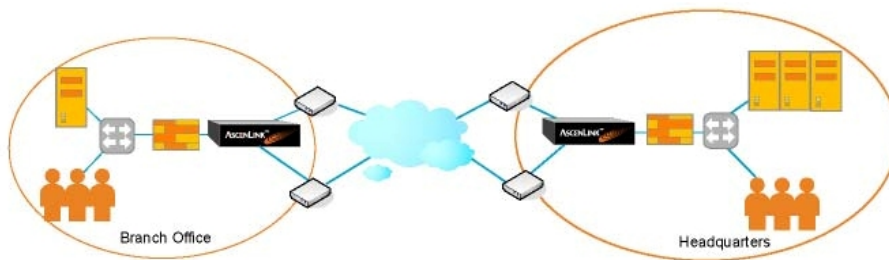
The headquarters of an enterprise with branch offices all over the world uses VPN to communicate with one another. In this example, the leased line E1 is used to establish VPN. Since the leased line E1 is a single link, the downtime often occurs in busy hours, so the key application cannot be guaranteed. In addition, the leased line E1 is of quite high cost.

The following picture illustrates the network topology without AscenLink.



To address the problems above, AscenLink is chosen as the solution. AscenLinks are installed in headquarters and branch offices and the leased line E1 is replaced by ADSL. AscenLink integrates multiple links and performs VPN load balancing with its Tunnel Routing. With AscenLink, the total bandwidth is expanded and the cost is cut down.

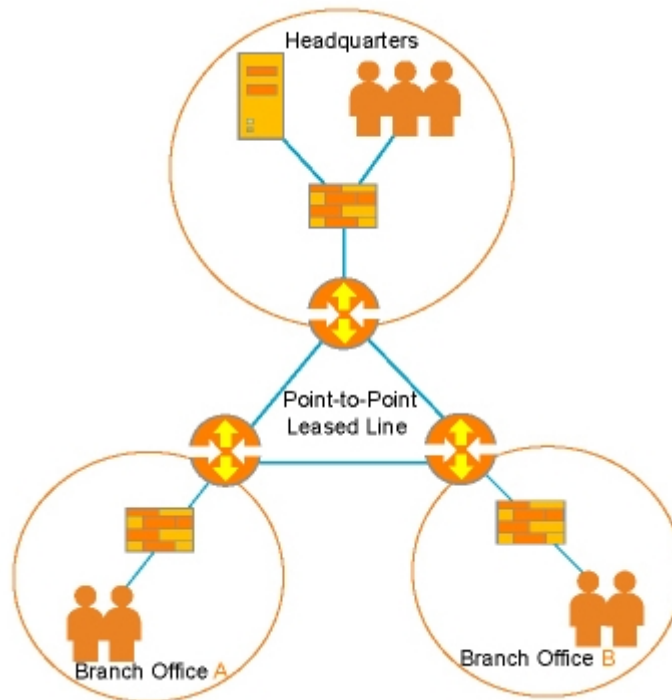
The following picture illustrates the network topology with AscenLink:



■ **Bring LAN-like file delivery to WAN and facilitate the information resource share**

An enterprise's headquarters is in Washington and two branch offices are respectively in San Jose and New York. Three leased lines are required to establish VPN so as to connect each point and share the company resources.

The following picture illustrates the network topology without AscenLink.



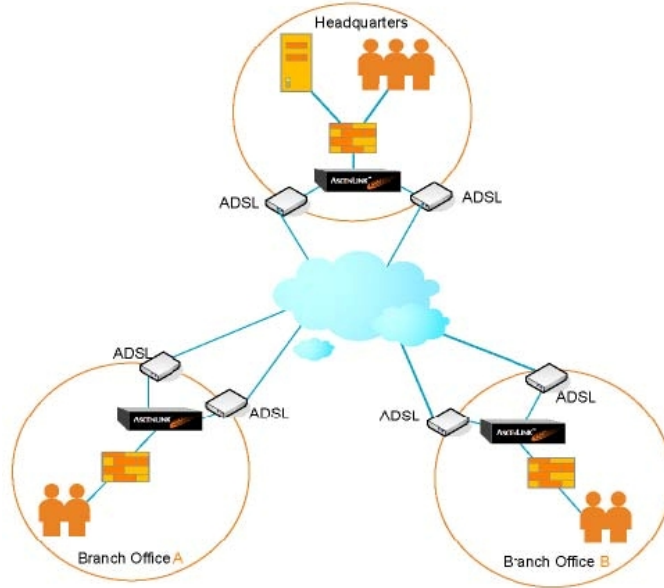
Since traditional VPN technology allows only one link to access, VPN load balancing is not available. As a result, should the single link failure occurs, the VPN connection would break down.

To make the file delivery in WAN as smooth as in LAN, the P2P connection must be established in a VPN network. That is to say if there are N devices in the network, $N \times (N-1) / 2$ connections need to be established. If so, the network architecture would be too complex to manage. Besides, should the configuration of even one of the device changed, the others need to be readjusted correspondingly, which greatly increase the complexity and cost of network management; also, the low VPN download speed has always been a serious problem bothering the users.

To address the above problem, AscenLink's Tunnel Routing is developed to establish a high performance VPN tunnel at a cost. The built-in forwarding technology makes it available for headquarters and branch offices to communicate.

Tunnel Routing also supports various types of WAN links such as T1, Fiber, ADSL, etc. With AscenLink, users could integrate the multiple links together by proper policy setting, so that both the VPN bandwidth and reliability are improved. Together with the QoS/Bandwidth management function, users can well plan and improve the bandwidth usage, bringing the LAN-like file delivery to WAN.

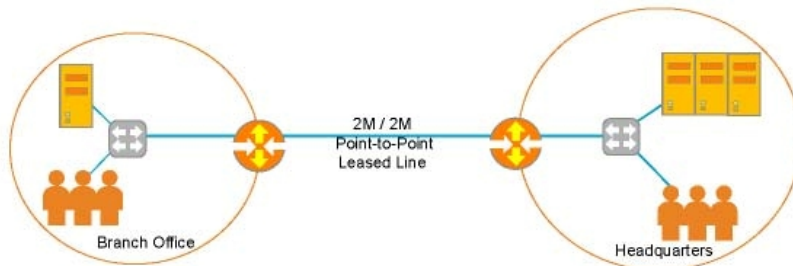
The following picture illustrates the network topology with AscenLink:



■ VPN packets transfer in the network with dynamic IP Address

Usually it is necessary to know the IP address of remote device to establish VPN tunnels. Should even one of the remote IP addresses changed, the configuration of other devices need to be adjusted accordingly, which greatly increases the complexity and the network management cost.

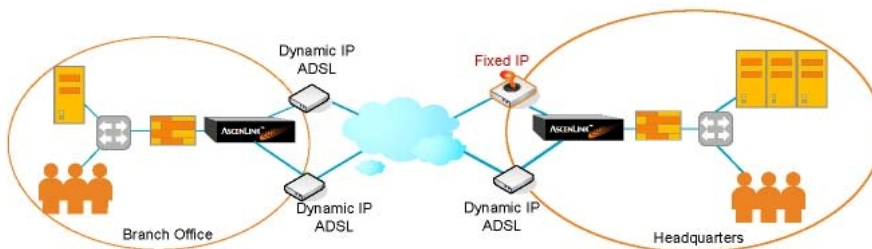
The following picture illustrates the network topology without AscenLink.



As ADSL is getting popular for its low cost, more and more enterprises prefer xDSL and Ethernet. Both xDSL and Ethernet, however, are of dynamic IP address; therefore, how to do VPN load balancing in the network with dynamic IP address becomes a problem for traditional VPN solution.

AscenLink’s Tunnel Routing technology supports VPN load balancing and the network with dynamic IP address. Administrators only need to specify Local Host ID and Remote Host ID, and then AscenLink can automatically exchange IP information. AscenLink helps the enterprise to establish a high-speed, convenient and reliable VPN environment at a much lower cost.

The following picture illustrates the network topology with AscenLink:

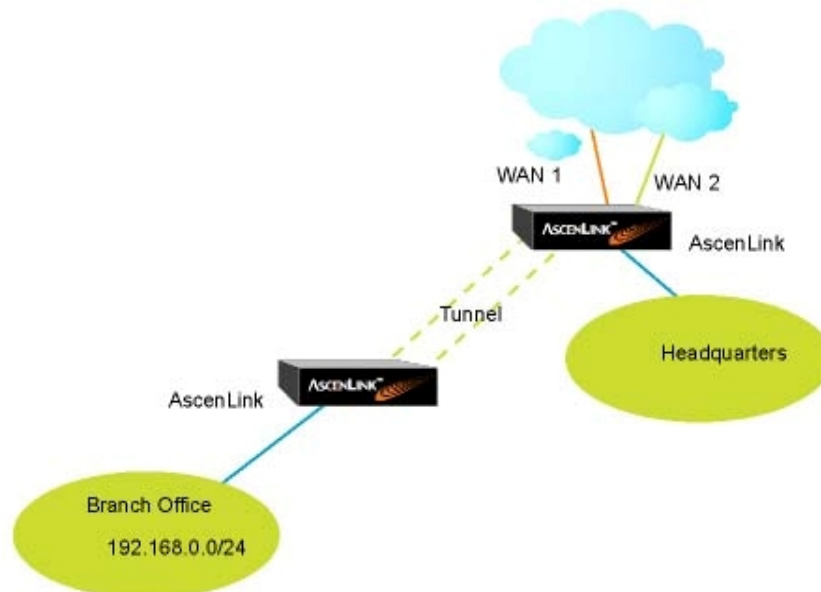


Note: please refer to next section “Establish Tunnel Routing in the network with dynamic IP address” for the more detailed information.

Central Routing

Central Routing is to establish a tunnel with two AscenLinks, through which the LAN of branch offices can access to the Internet via the Tunnel established between the AscenLinks in branch offices and the headquarters.

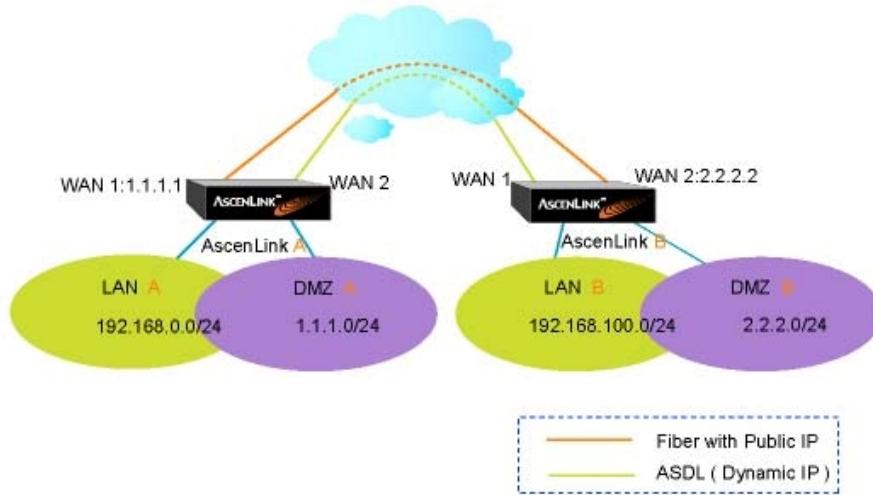
The topology of Central Routing:



■ WAN link backup

AscenLink's Tunnel Routing could perform multiple links backup. AscenLink's WLHD (WAN Link Health Detection) constantly monitors the status of WAN links. Should a WAN link break down, AscenLink would detect the situation and redirect traffic away from failed links. Users can create 2 Tunnel groups and backup with each other. Furthermore, Auto Routing and Tunnel Routing can also be the backup with each other. When Tunnel routing is down, packets will be routed by Auto Routing and when Auto routing is down, packets also can be routed by Tunnel Routing.

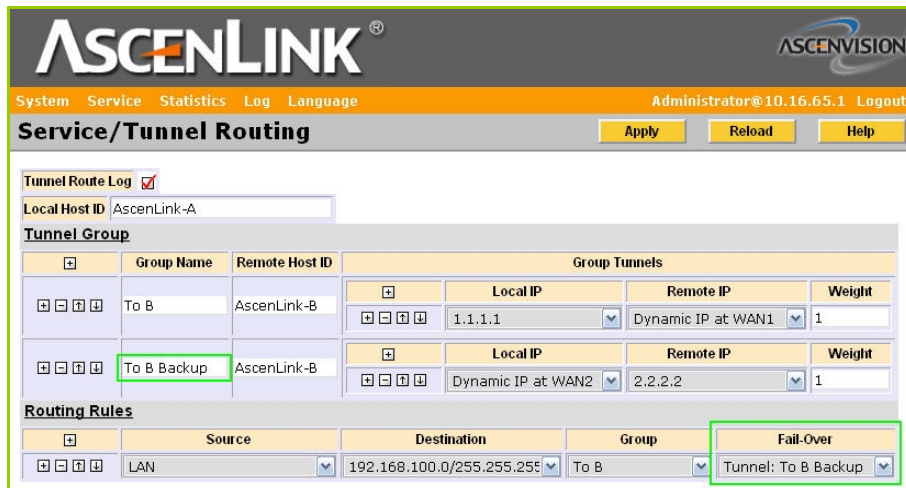
The following picture illustrates the network topology of an example with AscenLink:



Requirement 1:

- Tunnel: (A) WAN 1 <-> (B) WAN 1
- Backup Tunnel: (A) WAN 2 <-> (B) WAN 2
- LAN A <-> LAN B can communicate directly.

The configuration of AscenLink is as follows:



First of all, set up a "Tunnel Group" as the default Tunnel and name it "To B". The IP address of each end is respectively the IP address of AscenLink's WAN 1. And then, set up another "Tunnel Group" as the backup Tunnel and name it "To B Backup". The IP address of each end is respectively the IP address of AscenLink's WAN 2. Should the default tunnel break down on WAN 1, packets will be routed to backup tunnel on WAN 2, so that Tunnel will not break down.

Above "Backup" policy include both "Tunnel Routing Backup" and "Auto Routing Backup".

Requirement 2:

Tunnel: (A) WAN 1 <-> (B) WAN 2

DMZ on each end can communicate directly.

Should Tunnel breaks down, Auto Routing would perform as the backup.

The configuration of AscenLink is as following example:



In above example, Auto Routing is the backup of Tunnel "To B". Should WAN 1, whose IP is 1.1.1.1, break down, Tunnel would break down either. Then all DMZ packets destined to IP range 2.2.2.0/255.255.255.0 will be forwarded to Auto Routing.

Note: To make Auto Routing the backup for Tunnel Routing, it is necessary that the IP addresses of both terminals are public IP addresses. In this example, even though Tunnel breaks down, Auto Routing can still help each DMZ with public IP communicate with each other via WAN. Should the communication between LAN A and LAN B break down, it would not be available for Auto Routing to route the traffic with private IP address.

Establish Tunnel Routing in the network with dynamic IP address

1. Set an ID

While setting Tunnel with a dynamic IP address, the proper configuration is necessary. The configuration of AscenLink is as follows:



The screenshot shows the AscenLink web interface for 'Service/Tunnel Routing'. The 'Local Host ID' is 'AscenLink01' and the 'Remote Host ID' is 'AscenLink02'. The 'Group Tunnels' table is as follows:

Group Name	Remote Host ID	Local IP	Remote IP	Weight
NewGroup	AscenLink02	1.1.1.1	2.2.2.2	1

The 'Routing Rules' table is as follows:

Source	Destination	Group	Fail-Over
Any Address	WAN	NewGroup	NO-ACTION

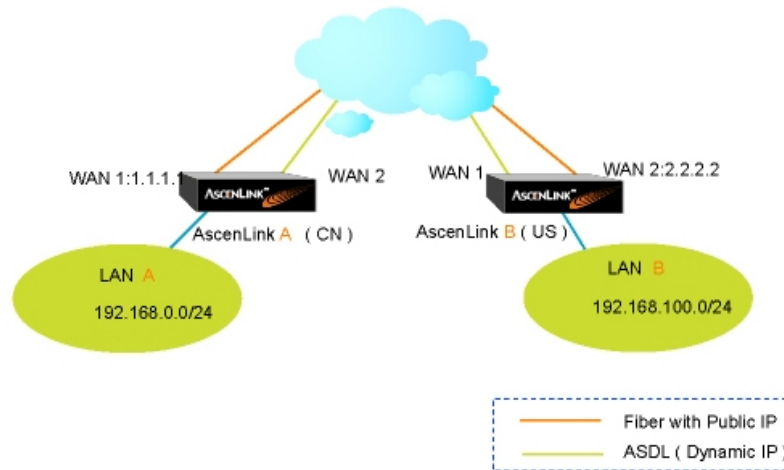
In “Local Host ID”, specify the ID of local AscenLink with “0-9”, “a-z”, “A-Z”, “_”, etc. Administrator can use this ID to communicate with the remote AscenLink.

In “Remote Host ID”, specify the ID of the remote AscenLink with “0-9”, “a-z”, “A-Z”, “_”, etc. While the local AscenLink is establishing the connection with the remote AscenLink, each AscenLink would inform the other one the ID of “AscenLink01” and “AscenLink02”. Tunnel is established with authentication.

Note: If both “Local IP” and “Remote IP” are fixed, “ID” can be left blank. If “Local IP” is dynamic and “Remote IP” is fixed, “Local Host ID” is necessary and “Remote Host ID” can be left blank. If “Local IP” is fixed and “Remote IP” is dynamic, “Remote Host ID” is necessary and “Local Host ID” can be left blank.

2. Set Tunnel Group to support dynamic IP address

ADSL is of low cost and can be used as backup link, so more and more users prefer ADSL to the leased line. AscenLink V5.1 and higher version support Tunnel Routing in the ADSL network with dynamic IP address.



Tunnel Routing in the network with dynamic IP address

Above picture illustrates the topology of Tunnel Routing in the network with dynamic IP address.

Model:

WAN1 of AscenLink A is fiber; WAN 2 is the backup of WAN 1 and it can be used for bandwidth expansion; ADSL is of dynamic IP address; AscenLink B is the same as AscenLink A.

WAN IP Address:

IP addresses of WAN1 on each end are separately 1.1.1.1 and 2.2.2.2; WAN2 is of dynamic IP Address.

LAN IP Range:

LAN A is 192.168.0.0/24;
LAN B is 192.168.100.0/24.

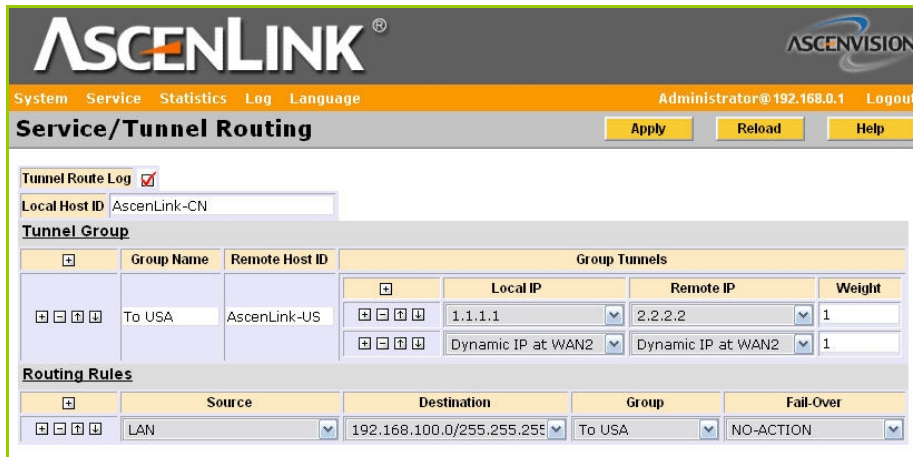
Location:

AscenLink A is in China;
AscenLink B is in USA.

Tunnel:

(A) WAN 1 <-> (B) WAN 1
(A) WAN 2 <-> (B) WAN 2

The Configuration of AscenLink A:



The screenshot shows the AscenLink configuration interface for AscenLink A. The page title is "Service/Tunnel Routing". The "Local Host ID" is set to "AscenLink-CN". Under "Tunnel Group", there is one group named "To USA" with a "Remote Host ID" of "AscenLink-US". This group contains two tunnels: one with "Local IP" 1.1.1.1 and "Remote IP" 2.2.2.2, and another with "Dynamic IP at WAN2" for both local and remote IP addresses. Both tunnels have a "Weight" of 1. Under "Routing Rules", there is one rule with "Source" set to "LAN", "Destination" set to "192.168.100.0/255.255.255.0", "Group" set to "To USA", and "Fail-Over" set to "NO-ACTION".

The Configuration of AscenLink B:

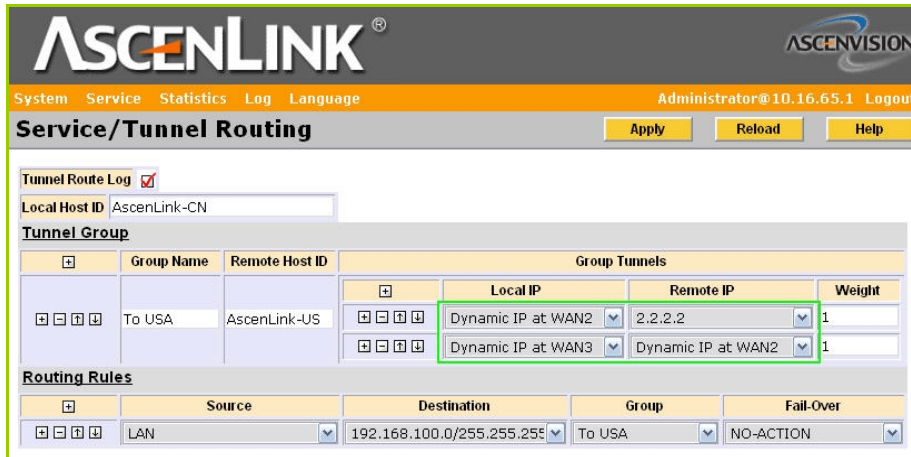


The screenshot shows the AscenLink configuration interface for AscenLink B. The page title is "Service/Tunnel Routing". The "Local Host ID" is set to "AscenLink-US". Under "Tunnel Group", there is one group named "To China" with a "Remote Host ID" of "AscenLink-CN". This group contains two tunnels: one with "Local IP" 2.2.2.2 and "Remote IP" 1.1.1.1, and another with "Dynamic IP at WAN2" for both local and remote IP addresses. Both tunnels have a "Weight" of 1. Under "Routing Rules", there is one rule with "Source" set to "LAN", "Destination" set to "192.168.0.0/255.255.255.0", "Group" set to "To China", and "Fail-Over" set to "NO-ACTION".

Note: While setting "Tunnel Group", Local IP Address and Remote IP Address should be corresponding with each other. In above example, "To USA" is corresponded to "To China".

- Each Group should have at least one fixed IP address

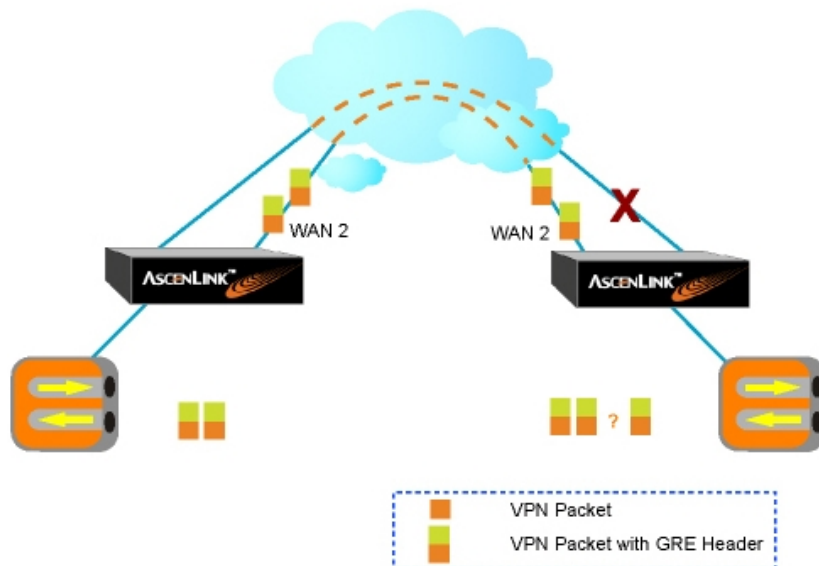
AscenLink still cannot support the network whose IP addresses are all of dynamic ones even when Tunnel is established. In other words, there should be at least one fixed IP address.



In this example, no matter “To USA” has how many dynamic IP addresses, a fixed IP address, such as “2.2.2.2”, will be necessary to establish Tunnel.

- Set Tunnel Rules to improve link usage

There are some tips in setting Tunnel to improve the efficiency of the link usage.



In above picture, if the Tunnel is established

- (A) WAN 1 <-> (B) WAN 1
- (A) WAN 2 <-> (B) WAN 2

If WAN1 of AscenLink B breaks down, WAN1 of AscenLink A will stop transfer packets via Tunnel. If so, even though the connection will not break down, the efficiency of the link usage is decreased.

Summary

This white paper explains in details that Xtera's newly-developed VPN load balancing technology--Tunnel Routing. The benefits of Tunnel Routing are:

- Bigger bandwidth at lower cost.
- High reliability and stability
- Link failure Bypass
- Load balancing in a dynamic IP network
- Data centralization
- The detailed report from LinkReport for trouble shooting