Research on Tunneling Techniques in Virtual Private Networks

Amankatiyar ,AnupamVishwakarma, Aditya soni , Hemantjain ,JayeshSurana

Student,Student,Student,Student,Faculty

Information Technology
SVITS,Indore,India

Abstract—Virtual Private Networks (VPNs) to be used for information exchange between enterprises, between branches of enterprises and between enterprises and their employees instead of traditional dial networks and leased lines. The tunneling technique is the key technique to implement VPN. In this paper, with the VPN implementation requirements in mind, we perform a comparative research on the existing tunneling protocols including GRE, L2TP, IPSec and IP/IP. We also propose an integrated scheme of tunneling mechanism that supports V PN under the current condition.

IndexTerms-VPN, tunneling protocol, GRE, L2TP ,IPSec, IP/IP

---

1 . INTRODUCTION

The collaborations between enterprises and the contacts between the enterprises and their customers become tighter day by day which develop and change dynamically. All the above relations need to be maintained and strengthened via the network .This work is supported by the National 863 High Technology Plan Project — Research on Extranet Key Technology (item number: 9846—005).These trends make traditional dial-up networks and leased lines unsuitable. Therefore, a novel technique, VPN (Virtual Private Network) [l] creates. VPN is defined as the private network that constructed on top of the public network infrastru cture, such as the Internet. Using VPN instead of the dial-up networks and leased lines at least has the following advantages: (l) saving large communication costs; (2) utilizing the ubiquity of the Internet; (3) convenience for dynamic building and maintenance. The rest of this paper is organized as follows. Section 2 introduces some basic conceptsincluding the VPN model we use, the implementation requirements of VPN and some proposed tunneling protocols. In section 3 we perform a comparative research on the existing tunneling protocols. We give our integrated tunneling scheme in section 4 and conclude this paper in section 5

2. Some Basic Concepts

2.1 VPN Models

There are various VPN models [2], such as the Virtual Leased Line (VLL) model which emulates a leased line between two endpoints, the Virtual Private Routed Network (VPRN) model which emulates a multi-site wide area routed network, the VirtualPrivate Dial Network (VPDN) model which allows for remote users to connect into remote sites and the Virtual Private LAN Segment (VPLS) model which emulates a LAN segment. Of these models the VLL model is the simplest one (see Figure l). Between the enterprise's Intranet and the public Internet there exists a V PN device which is used as the VPN agent for other devices in the Intranet. For simplicity reason and no loss of problem essences, we use the V LL model as the basic model for our tunneling research.

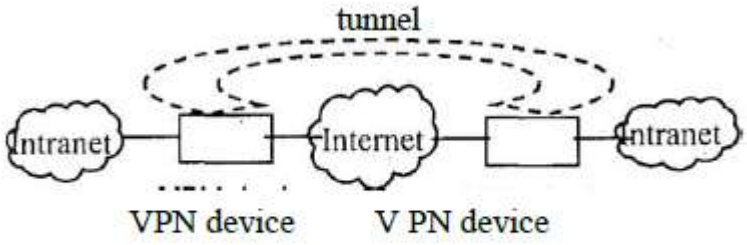

Figure l: VLL model of VPN

2.2 Implementation Requirements of VPN

As a "private" network, the V PN must satisfy the following requirements. Support for transparent packets transport: The packets carried on a V PN may have no relation with the packets on the public network. They may use different protocols and addressing mechanisms and if they use the same addressing mechanism, their address spaces may overlap. Especially, for a Internet based VPN, the non- unique private IP address may be used. In addition, one public network may support several VPNs simultaneously and they are also transparent to each other.Support for security functions: Public network is short of security protections, customers who use V PN require some security functions like user authentication against data spoofing, the data encryption against snooping and the integrity computation against unlawful tampering.Support for Quality of Service (QoS) guarantees: V PN should support various levels of QoS according to the customers' requirements, including the bandwidth and delay guarantees.

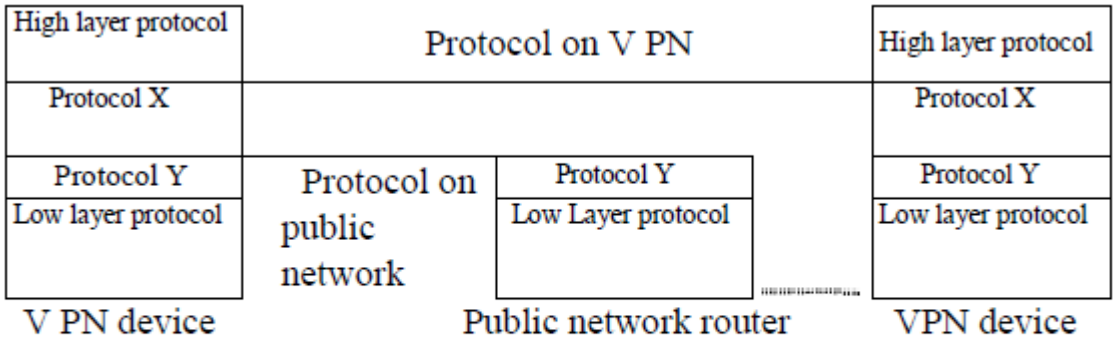

Figure 2: the protocol architecture of V PN

2.3 Tunneling Protocols

To satisfy the above requirements, V PN must be implemented through some form of tunneling mechanism. Tunneling is in fact a kind of encapsulation, i.e., a protocol (protocol X) is encapsulated within another protocol (protocol Y) when transporting, so the protocol X is transparent to the public network. The protocol architecture of VPN implemented via tunneling mechanism is illustrated in Figure 2. Here the protocol X is called encapsulated protocol while the protocol Y is called encapsulating protocol. In general, when encapsulating, specific tunneling protocol using IP as the encapsulating protocol is named IP tunneling protocol. Currently there already .proposed several IP tunneling protocols which are briefly introduced as follows. Generic Routing Encapsulation (GRE) protocol [3]: It is a general encapsulation protocol which was proposed aiming at -some specific ncapsulation schemes such as IPX encapsulated within IP, X .25 encapsulated within IP and so on. In this protocol, the encapsulating and encapsulated protocols both can be any network protocols. Layer 2 Tunnel Protocol (L2TP) [4]: We classify L2TP, Microsoft's Point to Point Tunnel Protocol (PPTP) and Cisco's Layer 2 Forwarding (L2F) as one type (In fact L2TP is the development result of PPTP and L2F). They are tunneling protocols supporting Internet-based remote access and work on the data link layer of the OSI/RM architecture. The encapsulation form of L2TP is (IP(UDP(L2TP(protocol X)))) IP Security (IPSec) protocol [5]: It includes a series of standards proposed by IETF which introduce security Inechanisms into TCP/IP network. The proposed
standards are made up of security protocols including Authentication Header (AH) [6] and Encapsulating Security Payload (ESP) [7], Security Associations (SAS), key management and security algorithms. The encapsulation form of IPSec working on tunnel mode is (IP(AH or ESP(IP))). [P Encapsulation within IP (IP/IP) protocol [9]: It was proposed by IETF mobile IP working group and used for communications between mobile hosts and their home agents in mobile IP. This group also proposed the tunnel establishment protocol (TEP) [1 0] to build tunnels. The encapsulation form of IP/IP is (IP(tunnel header(IP))). The above tunneling protocols were not specifically proposed for VPN, so they. may not satisfy all the VPÌV implementation requirements. In the next
section, with the VPN requirements in mind, we will elaborately compare the protocol mechanisms of various tunneling protocols.

3.Protocols Comparison

Difference of the Working Mode In the above tunneling protocols, GRE, IPSec and IP/IP all work on the peer-to-peer mode and the functions implemented on two VPN endpoints are symmetrical. Oppositely, L2TP works on the client/server mode. When it is used to implement VPN, the compulsory tunnel style must be used and one VPN device need to implement the L2TP Access Concentrator (LAC) function while another need to implement the L2TP Network Server (LNS) function. To make them symmetrical, both VPN devices need to implement LAC and LNS functions. Obviously it will increase the implementation overhead and the complexity of configuration and management operations.

3.1 Security

Security is one of the basic requirements of VPN and the Internet almost does not provide any security guarantees, so the tunneling protocol should offer some security mechanisms. Of the above several tunneling protocols, only IPSec provides the complete bu ild-in security mechanisms. Two security protocols were defined in Il) Sec: one is the IP authentication header (AH) protocol which is used to provide data origin authentication, data integrity and anti-replay protection; the other is IP Encapsulating Security Payload (ESP) which provides data confidentiality, limited traffic flow confidentiality and optional data origin authentication, data integrity and anti-replay protection. According to the security requirements, they can be used in separate or combined ways. According to the customer's demands, the IPSec- based VPN can provide multi-level security services. The other tunneling protocols do not provide any security mechanisms or only provide very weak security mechanisms. For example, L2TP inherits the authentication and encryption of PPP, but it cannot p•rovide packet-level protection to L2TP control and data messages. Another example is that GRE provides an optional four-byte Key field that can be used for origin authentication. IP/IP provides no security mechanisms. In order to provide more strong security in these protocols, usually the "tunneling protocol A + IPSec" scheme is adopted. In this scheme, the security is added outside and the protocol overhead will increase.

3.1 Tunnel Configuration and Establishment

Before establishing a tunnel, some parameters need to be configured§ such as the IP address of another tunnel endpoint, the needed security service and security level and some tunnel characteristics. In general, these tunnel parameters are configured via networkmanagement operations. For example we can define SNMP Management Information Base (MIB) to accomplish the configurations. In addition to this, IPSec also provides an alternative method, i.e., onfiguring the parameters via IKE proto col.

Comparing with network management, this method at least has the following advantages: (l) taking full advantage of the security mechanisms provided by IKE; (2) making VPN transparent to the ISP when no ISP participates in VPN construction; (3) greatlyreducing the network management load, especially when VPN spanning multiple administrative domains reducing the coordination between domains; (4) more flexible when the mobile hosts want to establish tunnels on demand.Tunnel establishmen t is a dynamic process. There are two types of tunnel establishing processes. One has the explicit tunnel establishing procedure, such as the control messages interchange in L2TP and the registration procedure when IP/IP or GRE being used in mobile IP. Another has not theexplicit tunnel establishing procedure, such as IPSec. The two processes both have their respective advantages and disadvantages. The advantages of explicit tunnel establishing process are: (l) being able to authenticate to tunnel establish ment easily; (2) beingable to dynamic negotiate some paran-leters; (3) being able to reserve resource at the tunnel granularity; (4) being beneficial to long-duration applications such as file transferring. The advantages of implicit tunnel establishing process are: (l) simple, saving bandwidth and reducing delay; (2) being consistent with connectionless IP service model; (3) being beneficial to short-duration applications such as transaction processing.

3.1 Tunnel Management and Maintenance

In the above tunneling protocols, L2TP defines some tunnel management and maintenance operations, such as sending Hello messages periodically to judge the connectivity of the tunnel and using the Next Sent (NS) and Next Received (Nr) fields provided by the protocol to implement flow control and congestion control of the tunnel. In addition, IP/IP provides a more general tunnel management mechanism. It takes advantage of the ICMP messages in the IP network and no additional bandwidth overhead is needed. The principle of this mechanism is as follows. In the tunnel endpoints some soft states are maintained including the Maximum Transmission Unit (MTU) of the tunnel, the Time To Live (TTL) of the tunnel, the reachability of the tunnel destination and so on. These soft states will be changed according to the received ICMP messages to reflect the current state of the tunnel. The packets that are to be sent will be dealt with according to the soft states. The soft state mechanism can solve the MTU, time out and congestion problems in the tunnel. Finally, IPSec and GRE do not consider the tunnel management an d maintenance problems.

3.2 Support for Multiplexing

In the V LL model, VPN device is used as the VPN agent of the enterprise Intranet and each tunnel endpoint may support multiple customers at the same time. In this case, separate tunnel can be established for each pair of customers, but the processing overheadand delay of tunnel establishment will increase. So the better way is sharing one tunnel amongst all customers (multiplexing). In order to differentiate which packets belong to which customers (the goal to differentiate them is that different customers may have

different transport requirements such as quality requirements), a multiplexing field is needed in the tunneling protocol. Of the above tunneling protocols, L2TP (via the tunnel-id and callid fields) and IPSec (via the Security Parameter Index, or SPI field) have amultiplexing mechanism. Strictly speaking GRE does not have a multiplexing field. However the key field, which was intended to be used for packet origin authentication, has sometimes been used as a multiplexing field. IP/IP does not support multiplexing.

Support for Multi-protocol Transport

In many application environments, the protocol running on VPN is not the IP protocol, so the tunnel protocols should support various protocols such as IP, PX, Aþpletalk and so on. In the above tunneling protocols, L2TP inherits from PPP, so it can support multi-protocol. GRE was defined as general encapsulation and it can support multi-protocol. IP/IP cannot support multi-protocol. Originally, IPSec was designed to transport IP packets, so it cannot support multi-protocol. But we can extend it and make itsuitable for multi-protocol environment. An extending method is encapsulating the non-IP protocol (protocol X) in the IP protocol using another tunneling protocol which supports multi-protocol such as GRE before IPSec encapsulation. Then IPSec encapsulation is adopted. In this way the encapsulation form becomes (IP(IPSec(IP(GRE(protocol X))))) we can see that it will increase the processing and transferring overhead. 3.3 Support for Packets Sequence In the physical leased lines, the packets transferringsequence is guaranteed. The packets sent firstly will arrive at the destination firstly. However, the IP protocol is connectionless and cannot guarantee the packets sequence, so the tunneling protocol should record the sequence information so that the packetssequence can be reconstructed at the destination end. In the above tunneling protocols, the NS and Nr fields of L2TP can store the packets sequence information. IPSec has a sequence number field, but currently it is only used by a receiver to perform ananti-replay check, not to guarantee in-order delivery of packets. The other tunneling protocols do not support packets sequence.

Support for Quality of Service Support for Quality of Service (QoS) is a basic requirement of VPN. The packets sequence described above can be seen as a kind of QoS, but generally QoS has wider contents, such as the bandwidth and delay guarantees, different service levels and so on. But unfortunately, in the above tunneling protocols, none can provide support for QoS.

How to provide QoS guarantee in the current IP network is an active research area. The research work covers resource reservation, admission control, QoS routing, packet scheduling, link sharing and so on.

3.5 Scalability Problem

Before discussing this problem, we extend the V LL V PN model from two enterprises to several (assume the number to be N) enterprises (therefore it becomes the VPRN model mentioned in section 2. l). According to the original method, in order to build the full- connective relationship between these . VPN devices, the number of tunnels is N*(N-l)/2. Each V PN device needs to maintain (N-l) tunnels with other V PN devices. With N increasing, the overhead of the tunnel configuration and maintenance operations becomes a serious problem. When the VPN relation changes, the tunnels must be reconfigured. The factors which cause the scalability problem are the full-connective network architecture (a tunnel is established between every two VPN devices) and the static routing (the tunnel configuration can be seen as a kind of static routing). To solve the scalability problem, we must focus on the above two aspects. Especially a dynamic routing protocol needs to be designed which can run on any topological VPNs.When designing this routing protocol, the problems which should be considered include the expression of V PN membership, the transport of reachability information, the relation with the current routing protocols running on the Internet and so on. All of theseneed to be study further. Table I summarizes the differences of protocol mechanisms between various tunneling protocols.

	GRE	L2TP	IPSec	IP/IP
Working mode	Peer to peer	Client/Server	Peer to peer	Peer to peer
Security mechanisms	Authentication	Authentication and encr tion	Complete build-in securit mechanisms	None
Tunnel configuration and establishment	Network mana ement, ex licit	Same as GRE	IKE interchange, im licit	Same as GRE
Tunnel management and maintenance	None	Hello message, etc	None	Soft state mechanism
Support for multi lexin	Support (usin Ke field)	Support	Support	Not support
Support for multi-rotocol	Support	Support	Not support	Not support
Support for packets se uence	Not support	Support	Support, but not use	Not support
Support for QoS	All not support, need for further study			
Scalability problem	Still not solved			

Table I : The comparison of the protocol mechanisms between various tunneling protocols

Integrated Tunneling Scheme

Through above comparison of various tunneling protocols, we can see that the implementation of V PN introduces more requirements to tunneling protocol. None of the proposed tunneling protocols can solve all the problems in V P N. In the current condition, we propose an extended IPSec/IKE tunneling scheme, which has been implemented in our VPN. Through testing it can satisfy the VPN requirements. We introduce it as follows. We use the tunnel mode IPSec as the basic encapsulation mechanism and the security guarantee of the tunnel, make use of the Internet Key Exchange protocol as the signaling protocol for tunnel configuration and refer to the soft state mechanism in IP/IP as the means for tunnel maintenance and management. For QoS support, we propose a simple method. It can provide the limited userbased different level service and no change is needed to the current IP service model. The principle of this method is as follows. Some service levels are defined in ' advance. When configuring the tunnel they are configured in the SA according to the users' requirements and identities. And when establishing the tunnel to encapsulate the packets, the service level recorded in the SA is mapped to the Type of Service (TOS) field of the IP header so that the relay routers can perform corresponding actions.If multi-protocol support is needed, in addition to the "twice encapsulation" scheme described in section 3.6, we propose a Inore direct method. In this method, the nonIP protocol is direc tly encapsulated within IPSec. But the encapsulated protocol type item is needed to add to the SA which is designated when configuring the tunnel. IPSec is extended to support multi-protocol.

5. Conclusion

It is important to point out that in order to guarantee the compatibility and interoperability between various V PN implementations, the standardization of tunneling protocols supporting V PN is necessary. When standardizing the problems listed above should be considered and the results already gaining should be referred to.

As it is designated above, how to let tunneling protocols support QoS, and how to run dynamic routing protocols in the V PRN model need for further study. All of these are our next research emphases. GRE L2TP IPSec IP/IP Working mode Peer to peer Client/Server Peer to peer Peer to peer Security mechanisms Authentication Authentication and encrtion Complete build-in securit mechanisms None Tunnel configuration and establishment Network manaement, ex licit Same as GRE IKE interchange, im licit Same as GRE Tunnel management and maintenance None Hello message, etc None Soft state mechanism Support for

multi lexinSupport (usinKe field) Support Support Not support Support for multi- rotocol Support Support Not support Not support Support for packets se uence Not support SupportSupport, but not use Not support Support for QoS All not support, ne ed for further study Scalability problem Still not solved

References

1. Hanks, S., Li, T, Farinacci, D. , and P. Traina, "Generic Routing Encapsulation", RFC 1701, October 1994.
2. Townsley, W. et al, "Layer Two Tunneling Protocol 'L2TP"', RFC2661, August 1999.
3. Kent, S. and Atkinson, R., "IP Authentication Header", RFC2402, November 1998.
4. D. Harkins & D. Carrel, "The Internet Key Exchange (IKE)'t , RFC2409, November 1998.
5. Perkins, C. , "IP Encapsulation within IP", RFC2003 October 1996.
6. Calhoun, P. et al., "Tunnel Establishment Protocol Internet Draft, March 1998.
7. Baohong He, Tianhui. Technology of IPSecVPN [M], Beijing: Posts and Telecom Press 2008.
8. Huaking Mao, "A comparative research on SSL VPN AndIPSec VPN, September 2012.
9. D. Frarinacci, "Generic Routing Encapsulation", Mar 2000.
10. PushpaYadav and RohitSinghal, "Effective tunneling of Trafficand Data in Network with L2TP Based on L2F, February 2014"