COMPREHENSIVE PERFORMANCE ANALYSIS AND SPECIAL ISSUES OF VIRTUAL PRIVATE NETWORK STRATEGIES IN THE COMPUTER COMMUNICATION:

A NOVEL STUDY

[1]Dr.S.S.Riaz Ahamed [2] P.Rajamohan

[1]Principal, Sathak Institute of Technology, Ramanathapuram, Tamilnadu, India.
[2] Lecturer, Department of Information Technology, HELP University College, Malaysia
Email:globalresearch@india.com, parthasarathy_rajamohan@yahoo.com

ABSTRACT

An Internet-based virtual private network uses the open, distributed infrastructure of the Internet to transmit data between corporate sites. VPNs using the Internet have the potential to solve many of the business networking problems. Virtual Private Networks provide an economical yet secure way to connect sites together and to provide network access to remote users. Virtual Private Networks provide attractive solution. A VPN uses the Internet infrastructure to interconnect sites and provide connectivity for remote dial-up users. The nearly universal coverage of the Internet eliminates the need for private leased lines and modem pools, and it eliminates long distance telephone charges remote, dial-up users. VPNs are less costly than conventional wide area networks. A VPN operates by passing data over the Internet or corporate intranet through “tunnels” which are secure, encrypted virtual connections that use the Internet (or corporate intranet) as the connection medium. The VPN establishes tunnels between servers in a site-to-site VPN, and between clients and servers in a client-to site VPN. The VPN encrypts and encapsulates each IP (or IPX) packet before passing it through a tunnel. The encapsulated packet includes authentication information to ensure the authenticity of the data and its source. The VPN also uses the authentication information to check that the original data has not been corrupted during transmission, ensuring the integrity of the data.

Keywords: Virtual Private Dial-Up Network (VPDN), Internet Protocol Security (IPS), Security Parameters Index (SPI).

1. INTRODUCTION

Virtual Private Network is defined as a network that uses a public network such as the Internet as a backbone to connect two or more private networks. VPNs can also be implemented on corporate intranet infrastructures. In this way, companies can implement private networks within their intranets to enable members of particular department or group to share sensitive information securely. A company, example, can enable a geographically dispersed engineering staff working on new secret products to collaborate and share sensitive information over the intranet without jeopardizing the security of the information. A VPN operates by passing data over the Internet or corporate intranet through “tunnels” which are secure, encrypted virtual connections that use the Internet (or corporate intranet) as the connection medium[2][5][11]-[19]. The VPN encrypts and encapsulates each IP (or IPX) packet before passing it through a tunnel. The encapsulated packet includes authentication information to ensure the authenticity of the data and its source. The VPN also uses the authentication information to check that the original data has not been corrupted during transmission, ensuring the integrity of the data [7][14][21]-[27].

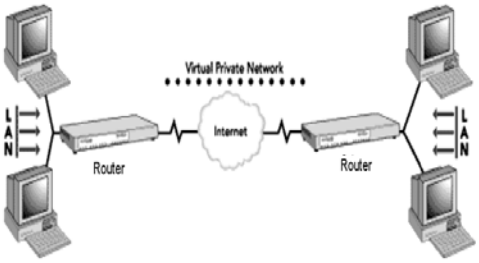

Figure 1.Virtual Private Network

2. MAJOR ISSUES

The construction & successful execution of VPN involves certain issues that have got to be remembered throughout the process. These stand as pillars to make the VPN. They include.

2.1 DATA INTEGRITY

- The condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.
- The condition in which data are identically maintained during any operation, such as transfer, storage, and retrieval**.**
- Relative to specified operations, the a priori expectation of data quality.

Data Integrity refers to the feature of precision of the data being sent from the client to the server. In other words, the data sent from the client to the server or vice-versa should not get corrupted during transmission. This can be implemented by what we call #functions. This is implemented in programming routers [9][14][17]-[26].

2.2 DATA CONFIDENTIALITY

Confidentiality prevents the disclosure of the plain text content of a message to any party other than the intended recipient(s). It is provided on a per-message basis using an asymmetric or symmetric encryption technique. The encrypted content is unintelligible to any MTA handling the message. If the originator chooses an asymmetric algorithm, the recipient's public key is used to encrypt the message content. The recipient uses its private key to decrypt the content. If an asymmetric encryption algorithm is used, the message can only be addressed to a single recipient (i.e., the recipient whose private key is paired with the public key used to perform the encryption). If the originator chooses a symmetric algorithm, delivery to multiple recipients is possible. The originator encrypts the content using a symmetric encryption key. This key may be distributed to each message recipient by placing the key in the encrypted-data of the message token for that recipient. The key may also be distributed by some other means. The message originator can encrypt the content using any symmetric or asymmetric algorithm understood by both the originator and the recipient. All information relevant to the algorithm, such as the algorithm's object identifier and any input parameters, can be conveyed in the message envelope or the signed-data of the message token. Data Confidentiality is the topmost level of all these features which helps is the data being transferred between two ends in the most secured way that even if the data are hacked during transmission they prove to be of no use to the hacker. These are accomplished by encrypting the data at the sending end & decrypting the same at the other end so as to retrieve the original message [1]-[9][13]-[20].

2.3 DATA AUTHENTICATION

Data Authentication can be a process used to verify data integrity, e.g., verification that data received are identical to data sent. Data Authentication allows VPN clients and servers to correctly establish the identity of people on the network. It checks for the identification of the source from where the data is received & only if it matches with the original coded identity of the network users will it allow the data to reach the required destination. This can be incorporated using software[5]-[11].

3. TECHNOLOGICAL ISSUES

Several network protocols have become popular as a result of VPN developments:

- PPTP
- L2TP
- IPsec
- SOCKS

These protocols emphasize authentication and encryption in VPNs. Authentication allows VPN clients and servers to correctly establish the identity of people on the network. Encryption allows potentially sensitive data to be hidden from the general public. Many vendors have developed VPN hardware and/or software products. Unfortunately, immature VPN standards mean that some of these products remain incompatible with each other[3]-[17].

4. VPN HARDWARE

Routers

Perle's high performance Routers provide complete routing and integrated security functionality without the premium pricing associated with competitive products. The Perle access router family delivers full-featured IP/IPX routing solutions to satisfy the developing needs of midmarket and small office networks. In today's market, end-users want reliable, secure, easy to configure and standards-based equipment that are competitively-priced.

P800

Small footprint Routers for Small Offices and Telecommuters

P841 to P844 routers provide ISDN connectivity

Perle P851 to P853 support synchronous serial connections for Frame Relay and Point-to-Point Protocol (PPP)

Virtual Private Network (VPN) capabilities for secure, low cost networking

P1700

High Performance Router with Dual LAN/WAN capability for Branch Office Networking

support up to two WAN and LAN interface cards

ISDN spoofing, auto-configuration PPP interoperability and QoS

VPN capabilities with 3DES encryption

Connectivity Options

The Perle P841 to P844 routers provide ISDN connectivity for small offices around the world. High data throughput and line management is maintained through data compression and bandwidth protocols to ensure the optimal and economic utilisation of BRI connections. The Perle P841 to P844 routers include a low-cost entry-level model where up to 10 LAN users can access the Internet. These routers can be expanded with a software upgrade as the office needs grow. The Perle P851 to P853 support synchronous serial connections for Frame Relay and Point-to-Point Protocol (PPP). At all speeds, the P850 routers optimize data transfer by monitoring for Frame Relay congestion. If necessary, the routers will scale back transmission to improve actual data throughput[15][18]-[29].

Security

Perle routers ensure data privacy with secure user authentication, firewalls, monitoring, configurable PPP security levels and other features. Optional VPN software ensures secured data gets to its intended audience and to no-one else.

Management

The Perle P800 Series routers support administrator management from a range of platforms and applications. By utilizing the Perle router configuration tools, such as the easy-to-use system and the automatic self configuration of the Frame Relay and leased line interfaces, administrators can very quickly set up the routers at local and remote sites for immediate productivity.

5. MERITS AND APPLICATIONS

- Permanent or dial up ISDN BRI connections
- Integrated security to protect LANs from unauthorized network access
- P850 uses auto-configuration to detect Frame Relay parameters for trouble-free connectivity
- Compatibility with other vendors' products via industry standard protocols
- Stac LZS data compression increases data throughput up to 600%
- POTS version saves phone line rental
- Point-to-Point Protocol over Ethernet for access to DSL or cable modem broadband networks
- Multiple variants to suit specific user requirements
- RoHS and WEEE Compliant
- Lifetime warranty for security and peace of mind

Applications

- Remote office access to control office
- Home office access to ISP and central office
- Small office with single ISDN link
- Internet Access

6. CLASSIFICATION AND VIRTUAL ROUTERS

VPN can be broadly classified into two types. They are: Site-to-site VPN and Remote access VPN

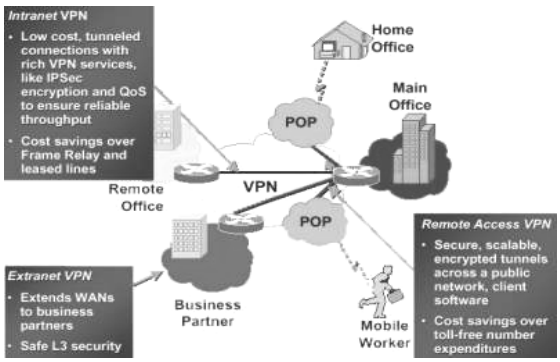

Figure 2 Classification

Site-to-site VPN

Site to site VPN can be further classified into two types. They are

- Intranet-based VPN

- Extranet-based VPN

Intranet-Based VPN

If a Company has more remote locations that it wishes to join in a single private network, it can create an Intranet VPN to connect LAN to LAN.

Extranet-Based VPN

When a Company has close relationship with another company, it can build an Extranet VPN that connects LAN to LAN and allows all of the various companies to work in a shared environment. Remote access VPN can be also called as virtual private dial-up network (VPDN). This Remote access VPN establishes the User-to-LAN connection. Here Telecommuters dial up to reach the Server and use their VPN client software to access the corporate network. Thus an authenticated User can logon to the VPN tunnel from anywhere using a laptop.

Virtual Routers

draft-ietf-l3vpn-as-vr	Applicability Statement for Virtual Router-based Layer 3 PPVPN approaches
draft-ietf-l3vpn-vpn-vr	Network based IP VPN Architecture using Virtual Routers
draft-ietf-l3vpn-vr-mib	Virtual Router Management Information Base Using SMIv2

Table 1-Virtual Routers

7 VPN SOLUTIONS AND KEY FEATURES

A VPN supplies network connectivity over a possibly long physical distance. In this respect, a VPN is a form of Wide Area Network (WAN). VPNs enable file sharing, video conferencing and similar network services. Virtual private networks generally don't provide any new functionality that isn't already offered through alternative mechanisms, but a VPN implements those services more efficiently / cheaply in most cases. A key feature of a VPN is its ability to work over both private networks as well as public networks like the Internet. Using a method called tunneling, a VPN use the same hardware infrastructure as existing Internet or intranet links. VPN technologies includes various security mechanisms to protect the virtual, private connections. Specifically, a VPN supports at least three different modes of use:

- Internet remote access client connections
- LAN-to-LAN internetworking
- Controlled access within an intranet

A VPN can be set up to support remote, protected access to the corporate home offices over the Internet. An Internet VPN solution uses a client/server design works as follows:

1. A remote host (client) wanting to log into the company network first connects to any public Internet Service Provider (ISP).

2. Next, the host initiates a VPN connection to the company VPN server.
3. Once the connection has been established, the remote client can communicate with the internal company systems over the Internet just as if it were a local host.

Before VPNs, remote workers accessed company networks over private leased lines or through dialup remote access servers. While VPN clients and servers careful require installation of hardware and software, an Internet VPN is a superior solution in many situations[3][6]-[19].

7.1 Internetworking

Besides using virtual private networks for remote access, a VPN can also bridge two networks together. In this mode of operation, an entire remote network (rather than just a single remote client) can join to a different company network to form an extended intranet. This solution uses a VPN server to VPN server connection[4].

7.2 Intranet / Local Network

Internal networks may also utilize VPN technology to implement controlled access to individual subnets within a private network. In this mode of operation, VPN clients connect to a VPN server that acts as the network gateway.

This type of VPN use does not involve an Internet Service Provider (ISP) or public network cabling. However, it allows the security benefits of VPN to be deployed inside an organization. This approach has become especially popular as a way for businesses to protect their WiFi local networks.

7.3 Cost Savings

Organizations historically needed to rent network capacity such as T1 lines to achieve full, secured connectivity between their office locations. With a VPN, you use public network infrastructure including the Internet to make these connections and tap into that virtual network through much cheaper local leased lines or even just broadband connections to a nearby Internet Service Provider (ISP). A VPN also can replace remote access servers and long-distance dialup network connections commonly used in the past by business travelers needing to access to their company intranet. With VPNs, the cost of maintaining servers tends to be less than other approaches because organizations can outsource the needed support from professional third-party service providers. These provides enjoy a much lower cost structure through economy of scale by servicing many business clients[11]-[23]. The cost to an organization of building a dedicated private network may be reasonable at first but increases exponentially as the organization grows. A company with two branch offices, for example, can deploy just one dedicated line to connect the two locations, but 4 branch offices require 6 lines to directly connect them to each other, 6 branch offices need 15 lines, and so on. Internet based VPNs avoid this scalability problem by simply tapping into the the public lines and network capability readily available. Particularly for remote and international locations, an Internet VPN offers superior reach and quality of service.

7.4 Limitations

Organizations should consider issues like the below when deploying and using virtual private networks in their operations:

1. VPNs require detailed understanding of network security issues and careful installation / configuration to ensure sufficient protection on a public network .

2. The reliability and performance of an Internet-based VPN is not under an organization's direct control. Instead, the solution relies on an ISP and their quality of service.

3. Historically, VPN products and solutions from different vendors have not always been compatible due to issues with VPN technology standards. Attempting to mix and match equipment may cause technical problems, and using equipment from one provider may not give as great a cost savings[11]-[19][23][29]-[30].

8. TUNNELING

Virtual private network technology is based on the idea of tunneling. VPN tunneling involves establishing and maintaining a logical network connection (that may contain intermediate hops). On this connection, packets constructed in a specific VPN protocol format are encapsulated within some other base or carrier protocol, then transmitted between VPN client and server, and finally de-encapsulated on the receiving side. For Internet-based VPNs, packets in one of several VPN protocols are encapsulated within Internet Protocol (IP) packets. VPN protocols also support authentication and encryption to keep the tunnels secure.

9. ENCRYPTION

9.1 Data Encryption

The Data Encryption Standard is something of an edict from the government that suggests the use of a certain mathematical algorithm in the encrypting and decrypting of binary information. The system consists of an algorithm and a key. The key has a length of sixty four bits, of which fifty six are used as the key in the classical sense. The remaining eight bits are parity bits used in checking for errors. Even with just fifty six bits there are over seventy quadrillion possible keys. The digits in the key must be independently determined to take full advantage of seventy quadrillion possible keys. The mechanics of DES are deceptively simple. DES enciphers data in blocks of sixty four bits of binary data. Given a message that needs to be encrypted one must

first pick a sixty four bit key and then convert the plaintext into binary form. It takes a string of only five bits to describe our alphabet, since 2^5=32 and the alphabet is 26 letters long. This is relatively easy to do. Now within the blocks or strings of sixty four bits order is important. The leftmost bit is known as the first bit or is in the first position. The rightmost bit is the sixty fourth bit. The first step in the DES procedure is to change the order within each block. For example, the fifty eighth bit in the original string Becomes the first bit in this new block. Bit fifty becomes bit two and so forth, as specified by a table. This step is called the initial permutation. Permutation is used in the strict mathematical sense that only order is changed. (Not unlike the permutation matrix in linear algebra.) The results of this initial permutation are broken down into two halves. The first thirty two bits become L0. The last thirty two bits are called R0. Data is subjected to the following transformation sixteen times:

Ln = Rn-1 where R0 occurs at n=1
Rn = Ln-1 (((Rn-1, Kn) where L0 occurs at n=1 After one iteration
Ln+1 = Rn in essence Ln+1 = Ln-1 (((Rn, K0)
Rn+1 = Ln (((Rn, K0) in essence Rn+1 = Rn-1 (((Rn, K0)

DES algorithm seems to be feedback mechanism with the addition of a disturbance term. This is the essence of DES. The key and the message become interwoven and inseparable. This makes it difficult to break the apart the cipher text into its constituent parts. This procedure is performed sixteen times. The expression Rn = Ln-1 (((Rn+1, Kn) is simply saying add L, bit by bit in modulo two, from one iteration ago to the term ((Rn-1, Kn). This function is determined by R one iteration ago and Kn, which is based on the key. Kn is, in turn, given by another formula, Kn= KS(n, KEY). Since this algorithm goes through sixteen iterations, Kn will be of length forty eight. The calculation of Kn is another operation where one looks in the table provided by the government. The calculation of the function ((Rn+1,Kn) is likewise simple. First, however, notice that R is of thirty two bit length and K is forty eight bits long. R is expanded to forty eight bits using another table. The resulting R(is added to K (using bit by bit addition in mod base 2). The result of this addition is broken into eight six bit strings. One enters into another table that gives the primitive function Sn. There is one S function for each six bit block. The result of entering into these S functions is a thirty two bit string. After sixteen iterations we should have L16 and R16. These two strings are united where R forms the first thirty two bits and L forms the last thirty two. The sixty four bit result is entered into the inverse of the initial permutation function. The result of this last step is cipher text. Decoding is accomplished by simply running the process backwards[2]-[11][29][33]-[37].

10. TUNNELING ISSUES

Most VPNs rely on tunneling to create a private network that reaches across the Internet. Essentially, tunneling is the process of placing an entire packet within another packet and sending it over a network. The protocol of the outer packet is understood by the network and both points, called tunnel interfaces, where the packet enters and exits the network. Tunneling has amazing implications for VPNs. For example, you can place a packet that uses a protocol not supported on the Internet (such as NetBeui) inside an IP packet and send it safely over the Internet. Or you could put a packet that uses a private (non-routable) IP address inside a packet that uses a globally unique IP address to extend a private network over the Internet. In a site-to-site VPN, GRE (generic routing encapsulation) is normally the encapsulating protocol that provides the framework for how to package the passenger protocol for transport over the carrier protocol, which is typically IP-based. This includes information on what type of packet you are encapsulating and information about the connection between the client and server. Instead of GRE, IPSec in tunnel mode is sometimes used as the encapsulating protocol. IPSec works well on both remote-access and site-to-site VPNs. IPSec must be supported at both tunnel interfaces to use[1][4][6]-[16][21]-[31]. In a remote-access VPN, tunneling normally takes place using PPP. Part of the TCP/IP stack, PPP is the carrier for other IP protocols when communicating over the network between the host computer and a remote system. Remote-access VPN tunneling relies on PPP.

Each of the protocols listed below were built using the basic structure of PPP and are used by remote-access VPNs.

L2F (Layer 2 Forwarding) - Developed by Cisco, L2F will use any authentication scheme supported by PPP.

PPTP (Point-to-Point Tunneling Protocol) - PPTP was created by the PPTP Forum, a consortium which includes US Robotics, Microsoft, 3COM, Ascend and ECI Telematics. PPTP supports 40-bit and 128-bit encryption and will use any authentication scheme supported by PPP.

L2TP (Layer 2 Tunneling Protocol) - L2TP is the product of a partnership between the members of the PPTP Forum, Cisco and the IETF (Internet Engineering Task Force). Combining features of both PPTP and L2F, L2TP also fully supports IPSec.

10.1 Tunneling Protocols

L2TP can be used as a tunneling protocol for site-to-site VPNs as well as remote-access VPNs. In fact, L2TP can create a tunnel between Client and router,NAS and router & Router and router. The long-term direction for secure networking, IPSec is a suite of cryptography-based protection services and security protocols. Because it requires no changes to applications or protocols, you can easily deploy IPSec for existing networks. IPSec provides machine-level authentication, as well as data encryption, for VPN connections that use the L2TP protocol. IPSec negotiates between your computer and its remote tunnel server before an L2TP connection is established, which secures both passwords and data. L2TP uses standard PPP-based authentication protocols, such as EAP , MS-CHAP, SPAP, and PAP with IPSec. Encryption is determined by the IPSec Security Association, or SA. A security association is a combination of a destination address, a security protocol, and a unique identification value, called a Security Parameters Index (SPI).

11. MOBILE ENVIRONMENT

Mobile VPNs have been widely used in public safety, where they give law enforcement officers access to mission-critical applications, such as computer-assisted dispatch and criminal databases, as they travel between different subnets of a mobile network. They are also used in field service management and by healthcare organizations, among other industries.
Increasingly, mobile VPNs are being adopted by mobile professionals and white-collar workers who need reliable connections. They allow users to roam seamlessly across networks and in and out of wireless-coverage areas without losing application sessions or dropping the secure VPN session. A conventional VPN cannot survive such events because the network tunnel is disrupted, causing applications to disconnect, time out, or fail, or even cause the computing device itself to crash.
Instead of logically tying the end point of the network tunnel to the physical IP address, each tunnel is bound to a permanently associated IP address at the device. The mobile VPN software handles the necessary network authentication and maintains the network sessions in a manner transparent to the application and the user. The Host Identity Protocol (HIP), under study by the Internet Engineering Task Force, is designed to support mobility of hosts by separating the role of IP addresses for host identification from their locator functionality in an IP network. With HIP a mobile host maintains its logical connections established via the host identity identifier while associating with different IP addresses when roaming between access networks[9]-[14][17][19]-[25].

12. CONCLUSION

VPNs allow network managers to connect remote branch offices and project teams to the main corporate network economically and provide remote access to employees while reducing the in-house requirements for equipment and support. VPNs using the Internet have the potential to solve many of these business networking problems. In addition, VPNs are not limited to corporate sites and branch offices. As an added advantage, a VPN can provide secure connectivity for mobile workers. These workers can connect to their company's VPN by dialing into the POP of a local ISP, which reduces the need for long-distance charges and outlays for installing and maintaining large banks of modems at corporate sites. The military networks may themselves be implemented as VPNs on common transmission equipment, but with separate encryption and perhaps routers.

13. REFERENCES

[1] Building and Managing Virtual Private Networks, Dave Kosiur, Wiley & Sons; ISBN: 0471295264, Pp 35-110.
[2] Firewalls and Internet Security: Repelling the Wily Hacker, William R. Cheswick and Steven M. Bellovin, Addison-Wesley; ISBN: 0201633574,Pp 50-140.
[3] VPNs A Beginners Guide, John Mains, McGraw Hill; ISBN: 0072191813,Pp 28-72.
[4] "Layer 2 VPN Architectures" by Wei Luo, Carlos Pignataro, Dmitry Bokotey, Anthony Chan (Cisco Press 2005), Pp73-122.
[5] "Computer Networks" by Andrew S. Tanenbaum (Pearson Education, Fourth Edition 2003),Pp 65-140.
[6] A. A. Abouzeid et al., "Comprehensive Performance Analysis of a TCP Session Over a Wireless Fading Link With Queueing," IEEE Trans. on Wireless Comm., Vol. 2, pp. 344-356 (March 2003).
[7] Y.-M. Chuang, et al., "Trading CDPD availability and voice blocking probability in cellular networks," IEEE Network, March-April 1998, pp. 48-52.
[8] M. H. Habaebi and B. M. Ali, "The FPBA Algorithm with Controlled Capture," Proc. IEEE ICC 2001, pp. 1416-1420.
[9] V. M. Jovanovic and J. Gazzola, "Capacity of Present Narrowband Cellular Systems: Interference-Limited or Blocking Limited?" IEEE Personal Communications, December 1997, pp. 42-51.
[10] L. Kleinrock, "On Queueing Problems in Random-Access Communications," IEEE Trans. on Information Theory, vol. IT-31, pp. 166-175 (March 1985).

[11] Y.-B. Lin, "Performance Modeling for Mobile Telephone Networks," IEEE Network, November/December 1997, pp. 63-68.
[12] D. Saha and S. E. Kay, "Cellular digital packet data network," IEEE Trans. on Vehic. Tech., Vol. 46, pp. 697-706.
[13] C. C. Wang and G. J. Pottie, "Variable Bit Allocation for FH-CDMA Wireless Communication Systems," IEEE Trans. on Communications, Vol. 50, pp. 1637-1644 (October 2002)
[14] Chris Metz. The Latest in Virtual Private Networks: Part I. IEEE Internet Computing, pp 87–91, 2003.
[15] Chris Metz. The Latest in Virtual Private Networks: Part II. IEEE Internet Computing,pp 60–65, 2004.
[16] Chris Metz. Multiprotocol Label Switching and IP, Part II: Multicast virtual private net-works. IEEE Internet Computing, pp 76–81, 2006.
[17] Floyd, S., and Fall, K., Promoting the Use of End-to-End Congestion Control in the Internet. IEEE/ACM Transactions on Networking, August 1999.
[18] L. E. Miller, "Models for MSE Traffic and Blocking Under Stress," JSLAI Report JC-2092-2-FF under contract DAAL02-89-C-0040 (Army Survivability Management Office), July 1992. (AD-B166477) Extract: Derivation of blocking probabilities used in telephone traffic theory (Erlang B, Erlang C, Bernoulli, etc.). Calculator for blocking probabilities.
[19] AbdelNasir Alshamsi and Takamichi Saito. A Technical Comparison of IPSec and SSL.
[20] Mun Choon Chan, Aurel A. Lazar and Rolf Stadler, " Customer Management and Control of Broadband VPN services" , IFIP/IEEE International Symposium on Integrated Network Management (IM '97), (San Diego, California), May 1997.
[21] IP Based Virtual Private Networks,RFC 2764, B. Gleeson et al.,February2000
[22] Generic Requirements for Provider Provisioned Virtual Private Networks (PPVPN),RFC3809, A. Nagarajan,June 2004
[23] Provider Provisioned Virtual Private Network (VPN) Terminology,RFC4026, L. Andersson and T. Madsen,March 2005
[24] BGP/MPLS VPNs,RFC 2547, E. Rosen & Y. Rekhter,March 1999
[25] Address Allocation for Private Internets,RFC 1918, Y. Rekhter et al.,February 1996
[26] A Core MPLS IP VPN Architecture,RFC 2918, K. Muthukrishnan& A. Malis,September 2000
[27] IP Based Virtual Private Networks,RFC 2341, A. Valencia et al.,May 1998
[28] M.C. Chan, H. Hadama and R. Stadler, "An architecture for broadband virtual networks under customer control", IEEE Network Operations and Management Symposium, (Kyoto, Japan), April 1996.
[29] A. Conti et al., "Bluetooth and IEEE 802.11b Coexistence: Analytical Performance Evaluation in Fading Channels," IEEE J. on Sel. Areas in Comm., Vol 21, pp. 259-269 (February 2003)
[30] J. del Prado and S. H. Choi, "Experimental Study on Co-existence of 802.11b with Alien Devices," Proc. IEEE VTC 2001 (Fall), pp. 977-981.
[31] M. Dukic and M. Babovic, "Interference analysis in fixed service microwave links due to overlay of broadband SSDS-CDMA wireless local loop system," Wireless Networks, Vol. 6, pp. 109-119.
[32] E. Green, "TGh [spectrum management] Functional Requirements," IEEE 802.11 document 01/071, 16 January 2001.
[33] N. Golmie et al., "Interference Evaluation of Bluetooth and IEEE 802.11b Systems," Wireless Networks, Vol. 9, pp. 201-211, 2003.
[34] I. Howitt, "WLAN and WPAN Coexistence in UL Band," IEEE Trans. on Vehicular Tech., Vol. 50, pp. 1114-1124 (July 2001).
[35] I. Howitt, "Bluetooth Performance in the Presence of 802.11b WLAN," IEEE Trans. on Vehicular Tech., Vol 51, pp. 1640-1651 (November 2002).
[36] J. Lansford, "Working Towards the Peaceful Coexistence of Wireless PANs, LANs, and WANs," Communications Design Conference, San Jose,CA, .Sept. 2002.
[37] J. Lansford et al., "Wi-Fi (802.11b) and Bluetooth: Enabling Coexistence," IEEE Network Magazine, Sept./Oct. 2001, pp. 20-27.
[38] J. M. Peha, "Wireless Communications and Coexistence for Smart Environments," IEEE Personal Comm., October 2000, pp. 6-8.
[39] Kurose, J. and Ross, K. 2005. Computer Networking: A Top-Down Approach Featuring the Internet. Addison Wesley: New Jersy.
[40] Odinma, A.C. 2006. “Next Generation Networks: Whence, Where and Thence”. Pacific Journal of Science and Technology. 7(1):10-16.
[41] Odinma, A.C. 2004. “The Convergence of Telecom Networks and Migration Strategies for Operators”. NSE, Electr. Div., National Conference. 6 – 7 October 2004.
[42] Fong, B., Ansari, N., Fong, A., Hong, G., and Rapajai, C. 2003. “On Scalability of Fixed Broadband Wireless Access Network Deployment”. IEEE Radio Communications
[43] Olexa, R. 2004. “Implementing 802.11, 802.16, and 802.20 Wireless Networks: Planning, Troubleshooting, and Operations”. Communications Engineering. Newnes: London.
[44] Pereira, M. 2000. "Fourth Generation: Now, It Is Personal". Proceedings of the 11th IEEE Intern. Symp. on Personal, Indoor and Mobile Radio Communications. London, UK, Sept. 2000.
[45] D. Wong and T. J. Lim, "Soft Handoffs in CDMA Mobile Systems," IEEE Personal Communications, December 1997, pp. 9-17.
[46] Arthur D. Little, Inc. 2006. “HSPA will Account for Most Mobile Broadband Deployment”. Arthur D. Little: New York.
[47] Junipa Research Report. 2007. “Mobile Entertainment: Revenue Opportunities”. February 2007.