

Virtual Private Networks: References

- [White Papers](#)
- [Vendor Specific Information](#)
- [News Items](#)
- [VPN Vendors](#)
- [Books on VPNs](#)
- [IETF Working Groups](#)
- [USEnet Newsgroups](#)
- [IETF RFC's](#)
- Internet Drafts
 - [L2TP](#)
 - [IPSec](#)
 - [RADIUS](#)
 - [DIAMETER](#)
 - [Other](#)
- For related topics see also:
 - Quality of Service over IP References, http://www.cis.ohio-state.edu/~jain/refs/ipqs_ref.htm
 - MPOA and IP Switching References, http://www.cis.ohio-state.edu/~jain/refs/ipsw_ref.htm

Note: A periodically updated version of this list is kept on-line at

http://www.cis.ohio-state.edu/~jain/refs/ref_vpn.htm

Back to [Hot Topics in Networking References](#)

Back to [Raj Jain's Home Page](#)

White Papers

- Microsoft, "Virtual Private Networking: An Overview," <http://www.microsoft.com/workshop/server/feature/vpnovw.asp>
- P. Ferguson and G. Huston, "What is a VPN?," <http://www.employees.org/~ferguson/vpn.pdf>
- Checkpoint - Virtual Private Networks Security Components, <http://www.checkpoint.com/vpn/vpnwp.html>
- Aventail, VPN FAQs, <http://www.aventail.com/index.phtml/solutions/faqs.phtml>
- Ascend - **Virtual Private Networks Resource Guide**, <http://www.ascend.com/2174.html>
- Request For Proposal: VPNs Across Multiple Sites - Vendors present proposals that push the network backbone out to the Internet, Network Computing, July 1, 1998, pp. 38-68, <http://www.techweb.com/se/directlink.cgi?NWC19980701S0020>
- Socks Version 5: The Unfirewall, Network Computing, March 15, 1998, <http://www.techweb.com/se/directlink.cgi?NWC19980315S0022>
- Cisco - Solutions for Virtual Private Dialup Networks, http://www.cisco.com/warp/public/728/General/vpdn_wp.htm
- Cisco - Service Provider: VPN Services, <http://www.cisco.com/warp/public/779/servpro/solutions/vpn/>
- Building Access Virtual Private Networks, http://www.cisco.com/warp/public/779/servpro/solutions/vpn/vpntd_wp.htm
- Cisco - Access VPN: Business Level Service Description, http://www.cisco.com/warp/public/779/servpro/solutions/vpn/avpn_rg.htm
- Network Management Solutions for IP-VPN Services,

- http://www.cisco.com/warp/public/779/servpro/solutions/csm/vpn_wp.htm
- Cisco - VPN Services: Quick Links to All VPN Information, <http://www.cisco.com/warp/public/779/servpro/solutions/vpn/quicklink.htm>
- Cisco - The New World of Virtual Private Networking Services, http://www.cisco.com/warp/public/779/servpro/solutions/vpn/nwvpn_pl.htm
- Cisco - Access VPN, http://www.cisco.com/warp/public/779/servpro/solutions/vpn/avpn_bc.htm
- Cisco - Layer 2 Tunneling Protocol (L2TP), http://www.cisco.com/warp/public/732/l2tp/l2tun_ds.htm
- Summit Online - Making Sense of Virtual Private Networks, <http://www.summitonline.com/netmanage/papers/aventail2.html>
- Building VPNs: The 10-point Plan, Data Communications Magazine, June 1998, pp. 123-132.
- VPNs: Security With an Uncommon Touch, Data Communications Magazine, Sept 21, 1997, http://www.data.com/lab_tests/vpn.html
- Bulletproof IP, Data Communications Magazine, November 1997, <http://www.data.com/tutorials/bullet.html>
- Dial-in Virtual Private Networks Using Layer 3 Tunneling, <http://www.baynetworks.com/products/Remote/vpn/dialing.html>
- S. Sanghi, "Virtual Private Networks," <http://www.indialine.com/net.columns/column42.html>
- Aventail - Directed VPNs, <http://www.aventail.com/index.phtml/solutions/directedvpn.phtml>
- Tom Dunigan's Virtual Private Networks page, <http://www.epm.ornl.gov/~dunigan/vpn.html>
- SSL 3.0 Specification, <http://home.netscape.com/eng/ssl3/draft302.txt>
- BYTE Magazine - July 1997 / Features / A Virtual Private Affair, <http://www.byte.com/art/9707/sec6/art3.htm>
- BYTE Magazine - November 1997 / BYTE Software Lab Report / Extend Your Net with VPNs, <http://www.byte.com/art/9711/sec10/art1.htm>
- BayNetworks - White Paper: Remote Access, <http://www.baynetworks.com/products/Papers/2746.html>
- All about S/WAN, <http://www.rsa.com/rsa/SWAN/home.html>
- VPNs: Security With an Uncommon Touch, http://www.data.com/lab_tests/vpn.html
- Ssh (Secure Shell) Home Page, <http://www.cs.hut.fi/ssh/>
- Point to Point Tunneling Protocol (PPTP) Technical Specifications, <http://infodeli.3com.com/infodeli/tools/remote/general/pptp/pptp.htm>
- IPsec Implementation Survey, <http://web.mit.edu/tytso/www/ipsec/results9710.html>
- IPsec-Compliant VPN Solutions: Virtualizing Your Network, <http://www.networkcomputing.com/914/914r1.html>
- Counterpane Systems: PPTP Crack, <http://www.counterpane.com/pptp.html>
- CIPE, <http://sites.inka.de/sites/bigred/devel/cipe.html>
- Virtual Private Network, <http://comet.ctr.columbia.edu/research/architectures/VPN.html>

Vendor Specific Information

- Microsoft, "Understanding PPTP," <http://www.microsoft.com/windows/downloads/bin/communications/understand.exe>
- Secure Virtual Private Networks - 1747, <http://www.intel.com/network/doc/1747/>
- Solutions For IP Virtual Private Dialup Networks, <http://www.telematics.com/whatsnew/white/virtual.htm>
- Download Library, <http://www.signal9.com/about/download/download.html>
- Virtual Private Networks, <http://www.objs.com/survey/vpn.htm>
- Case Study: Internet Service Providers, <http://www.baynetworks.com/Solutions/isp/concentric/>

- BayDVS Executive Summary, <http://www.baynetworks.com/products/Remote/vpn/baydvs.html>
- All About S/WAN, <http://www.rsa.com/rsa/SWAN/home.html>
- Redefining the Virtual Private Network (VPN), <http://www.checkpoint.com/vpn/vpndef.html>
- Concentric Network - Virtual Private Networks, <http://www.onlineacc.net/business/vpns/vpns.html>
- Brivida, Inc. - Technology for Virtual Private Networks "VPN", <http://www.brivida.com/>
- AltaVista Software Tunnel, <http://altavista.software.digital.com/tunnel/index.asp>
- IBM security home page: SecureWay offerings...cryptography, AntiVirus, firewalls and more, <http://www.ibm.com/Security/>
- Xerox Ethernet Tunnel Technical Product Description, <http://www.xerox.com/xeu/xettpd.html>
- ICQ Inc. - Virtual Private Online Network, <http://www.icq.com/create-network.html>

News Items

- RADIUS Servers: Funk And Shiva Go Head-To-Head, Network Computing, July 1, 1998, <http://www.techweb.com/se/directlink.cgi?NWC19980701S0022>
- VPNs: Safety First, But What About Speed? -- Don't worry about security: VPN devices prove their strength. But performance proves a problem, Data Communications, July 1998, <http://www.techweb.com/se/directlink.cgi?DAT19980701S0027>
- Data Fellows Brings Strong Encryption to Virtual Private Networks, <http://www.datafellows.com/news/articles/datafels.htm>
- VPNs Use Tunneling To Build Private Business Links (Datamation June 1, 1996), <http://www.datamation.com/PlugIn/issues/1996/june1/06ainet3.html>
- BYTE Magazine - December 1996 / State Of The Art / Internet Armor, <http://www.byte.com/art/9612/sec7/art4.htm>
- BYTE Magazine - October 1997 / International Features / VPNs Proliferate, <http://www.byte.com/art/9710/sec17/art1.htm>
- Cryptography: The Study of Encryption, <http://world.std.com/~frank/crypto/>
- Unlocking Virtual Private Networks, <http://www.networkcomputing.com/820/820f1.html>
- PC WEEK: Using the Net for virtual private networking, <http://www.zdnet.com/pcweek/sr/0428/02virt.html>
- PC WEEK: 'Virtual' privacy is not enough, <http://www.zdnet.com/pcweek/reviews/0810/10vpn.html>
- PC WEEK: Hidden VPN security costs are worth the price, <http://www.zdnet.com/pcweek/opinion/0720/20week.html>
- PC WEEK: VPNs: Many markets, many standards, <http://www.zdnet.com/pcweek/reviews/0427/27vpn.html>

VPN Vendors

- Ascend Communications, <http://www.ascend.com>
- Assured Digital, Inc., <http://www.assured-digital.com>
- Aventail Corp., <http://www.aventail.com>
- Bay Networks, <http://www.baynetworks.com>
- Cisco, <http://www.cisco.com>
- PSINet, <http://www.psi.com>
- RedCreek Communications, <http://www.redcreek.com>
- Shiva Corp, <http://www.shiva.com>
- 3Com Corp., <http://www.3com.com>

- TimeStep Corp., <http://www.timestep.com>
- VPNet Technologies, <http://www.vpnet.com>
- Compaq, <http://www.altavista.software.digital.com>
- Borderware, <http://www.securecomputing.com>
- Check Point Software Technologies, <http://www.checkpoint.com>
- Raptor Systems, <http://www.raptor.com>
- Data Fellows, <http://www.datafellows.com>
- Trusted Information Systems, <http://www.tis.com>
- Microsoft, <http://www.microsoft.com>
- FTP Software, <http://www.ftp.com>
- Sun Microsystems, <http://www.sun.com>

Books on VPN

See http://www.cis.ohio-state.edu/~jain/refs/vpn_book.htm

IETF Working Groups

- Domain Name System Security (dnssec), <http://www.ietf.org/html.charters/dnssec-charter.html>
- IP Security Protocol (ipsec), <http://www.ietf.org/html.charters/ipsec-charter.html>
- S/MIME Mail Security (smime), <http://www.ietf.org/html.charters/smime-charter.html>
- Transport Layer Security (tls), <http://www.ietf.org/html.charters/tls-charter.html>
- Web Transaction Security (wts), <http://www.ietf.org/html.charters/wts-charter.html>
- Site Security Handbook (ssh), <http://www.ietf.org/html.charters/ssh-charter.html>
- Remote Authentication Dial-In User Service (radius), <http://www.ietf.org/html.charters/radius-charter.html>
- Authenticated Firewall Traversal (aft), <http://www.ietf.org/html.charters/aft-charter.html>
- Common Authentication Technology (cat), <http://www.ietf.org/html.charters/cat-charter.html>
- One Time Password Authentication (otp), <http://www.ietf.org/html.charters/otp-charter.html>
- An Open Specification for Pretty Good Privacy (openpgp), <http://www.ietf.org/html.charters/openpgp-charter.html>
- Remote Authentication Dial-In User Service (radius), <http://www.ietf.org/html.charters/radius-charter.html>
- Authenticated Firewall Traversal (aft), <http://www.ietf.org/html.charters/aft-charter.html>
- Common Authentication Technology (cat), <http://www.ietf.org/html.charters/cat-charter.html>
- One Time Password Authentication (otp), <http://www.ietf.org/html.charters/otp-charter.html>
- Secure Shell (secsh), <http://www.ietf.org/html.charters/secsh-charter.html>
- Simple Public Key Infrastructure (spki), <http://www.ietf.org/html.charters/spki-charter.html>
- G and R for Security Incident Processing (grip), <http://www.ietf.org/html.charters/grip-charter.html>
- Multiprotocol Label Switching (mpls), <http://www.ietf.org/html.charters/mpls-charter.html>
- QoS Routing (qosr), <http://www.ietf.org/html.charters/qosr-charter.html>
- Differentiated Services (diffserv), <http://www.ietf.org/html.charters/diffserv-charter.html>
- Integrated Services (intserv), <http://www.ietf.org/html.charters/intserv-charter.html>
- RSVP Admission Policy (rap), <http://www.ietf.org/html.charters/rap-charter.html>
- Resource Reservation Setup Protocol (rsvp), <http://www.ietf.org/html.charters/rsvp-charter.html>

Usenet Newsgroups

- [Comp.dcom.sys.cisco](#)
- [comp.security.firewalls](#)
- [comp.os.ms-windows.networking.ras](#)
- [microsoft.public.windowsnt.protocol.ras](#)
- [microsoft.public.windowsnt.steelhead](#)
- [comp.protocols.tcp-ip](#)

IETF RFC's

- RFC 2367, "PF_KEY Key Management API, Version 2", 07/10/1998, 68 pp.,
<ftp://ftp.isi.edu/in-notes/rfc2367.txt>
- RFC 2350, "Expectations for Computer Security Incident Response", 06/04/1998, 38 pp.,
<ftp://ftp.isi.edu/in-notes/rfc2350.txt>
- RFC 2341, "Cisco Layer Two Forwarding (Protocol) 'L2F'", 05/06/1998, 29 pp., RFC Index
<ftp://ftp.isi.edu/in-notes/rfc2341.txt>
- RFC 2316, "Report of the IAB Security Architecture Workshop", 04/13/1998, 9 pp.,
<ftp://ftp.isi.edu/in-notes/rfc2316.txt>
- RFC 2313, "PKCS #1: RSA Encryption Version 1.5", 03/24/1998, 19 pp.,
<ftp://ftp.isi.edu/in-notes/rfc2313.txt>
- RFC 2284, "PPP Extensible Authentication Protocol (EAP)", 03/04/1998, 15 pp., RFC Index
<ftp://ftp.isi.edu/in-notes/rfc2284.txt>
- RFC 2274, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", 01/26/1998, 76 pp., <ftp://ftp.isi.edu/in-notes/rfc2274.txt>
- RFC 2268, "A Description of the RC2(r) Encryption Algorithm", 03/04/1998, 11 pp.,
<ftp://ftp.isi.edu/in-notes/rfc2268.txt>
- RFC 2228, "FTP Security Extensions", 10/28/1997, 27 pp., (Updates RFC959) RFC Index
<ftp://ftp.isi.edu/in-notes/rfc2228.txt>
- RFC 2222, "Simple Authentication and Security Layer (SASL)", 10/29/1997, 16 pp.,
<ftp://ftp.isi.edu/in-notes/rfc2222.txt>
- RFC 2207, "RSVP Extensions for IPSEC Data Flows", 10/01/1997, 14 pp.,
<ftp://ftp.isi.edu/in-notes/rfc2207.txt>
- RFC 2196, "Site Security Handbook", 09/15/1997, 75 pp., (FYI 8)
<ftp://ftp.isi.edu/in-notes/rfc2196.txt>
- RFC 2179, "Network Security For Trade Shows", 07/22/1997, 10 pp.,
<ftp://ftp.isi.edu/in-notes/rfc2179.txt>
- RFC 2166, "APPN Implementer's Workshop Closed Pages Document DLSw v2.0 Enhancements",
06/19/1997, 34 pp., <ftp://ftp.isi.edu/in-notes/rfc2166.txt>
- RFC 2144, "The CAST-128 Encryption Algorithm", 05/21/1997, 15 pp.,
<ftp://ftp.isi.edu/in-notes/rfc2144.txt>
- RFC 2139, "RADIUS Accounting", 04/18/1997, 25 pp., <ftp://ftp.isi.edu/in-notes/rfc2139.txt>
- RFC 2138, "Remote Authentication Dial In User Service (RADIUS)", 04/18/1997, 65 pp.,
<ftp://ftp.isi.edu/in-notes/rfc2138.txt>
- RFC 2107, "Ascend Tunnel Management Protocol - ATMP", 02/06/1997, 21 pp.,
<ftp://ftp.isi.edu/in-notes/rfc2107.txt>
- RFC 2104, "HMAC: Keyed-Hashing for Message Authentication", 02/05/1997, 11 pp.,
<ftp://ftp.isi.edu/in-notes/rfc2104.txt>

- RFC 2094, "Group Key Management Protocol (GKMP) Architecture", 07/02/1997, 22 pp., <ftp://ftp.isi.edu/in-notes/rfc2094.txt>
- RFC 2093, "Group Key Management Protocol (GKMP) Specification", 07/02/1997, 23 pp., RFC Index <ftp://ftp.isi.edu/in-notes/rfc2093.txt>
- RFC 2085, "HMAC-MD5 IP Authentication with Replay Prevention", 02/05/1997, 6 pp., <ftp://ftp.isi.edu/in-notes/rfc2085.txt>
- RFC 2084, "Considerations for Web Transaction Security", 01/22/1997, 6 pp., <ftp://ftp.isi.edu/in-notes/rfc2084.txt>
- RFC 2082, "RIP-2 MD5 Authentication", 01/10/1997, 12 pp., <ftp://ftp.isi.edu/in-notes/rfc2082.txt>
- RFC 2078, "Generic Security Service Application Program Interface, Version 2", 01/10/1997, 85 pp., <ftp://ftp.isi.edu/in-notes/rfc2078.txt>
- RFC 2069, "An Extension to HTTP: Digest Access Authentication", 01/03/1997, 18 pp., <ftp://ftp.isi.edu/in-notes/rfc2069.txt>
- RFC 2065, "Domain Name System Security Extensions", 01/03/1997, 41 pp., (Updates RFC1035) <ftp://ftp.isi.edu/in-notes/rfc2065.txt>
- RFC 2015, "MIME Security with Pretty Good Privacy (PGP)", 10/14/1996, 8 pp., <ftp://ftp.isi.edu/in-notes/rfc2015.txt>
- RFC 2015, "MIME Security with Pretty Good Privacy (PGP)", 10/14/1996, 8 pp., <ftp://ftp.isi.edu/in-notes/rfc2015.txt>
- RFC 1994, "PPP Challenge Handshake Authentication Protocol (CHAP)", 08/30/1996, 12 pp., <ftp://ftp.isi.edu/in-notes/rfc1994.txt>
- RFC 1969, "The PPP DES Encryption Protocol (DESE)", 06/19/1996, 10 pp., <ftp://ftp.isi.edu/in-notes/rfc1969.txt>
- RFC 1968, "The PPP Encryption Control Protocol (ECP)", 06/19/1996, 11 pp., <ftp://ftp.isi.edu/in-notes/rfc1968.txt>
- RFC 1961, "GSS-API Authentication Method for SOCKS Version 5", 06/19/1996, 9 pp., <ftp://ftp.isi.edu/in-notes/rfc1961.txt>
- RFC 1949, "Scalable Multicast Key Distribution", 05/17/1996, 18 pp., <ftp://ftp.isi.edu/in-notes/rfc1949.txt>
- RFC 1929, "Username/Password Authentication for SOCKS V5", 04/03/1996, 2 pp., <ftp://ftp.isi.edu/in-notes/rfc1929.txt>
- RFC 1915, "Variance for The PPP Connection Control Protocol and The PPP Encryption Control Protocol", 02/28/1996, 7 pp., <ftp://ftp.isi.edu/in-notes/rfc1915.txt>
- RFC 1910, "User-based Security Model for SNMPv2", 02/28/1996, 44 pp., <ftp://ftp.isi.edu/in-notes/rfc1910.txt>
- RFC 1858, "Security Considerations for IP Fragment Filtering", 10/25/1995, 10 pp., <ftp://ftp.isi.edu/in-notes/rfc1858.txt>
- RFC 1852, "IP Authentication using Keyed SHA", 10/02/1995, 6 pp., <ftp://ftp.isi.edu/in-notes/rfc1852.txt>
- RFC 1848, "MIME Object Security Services", 10/03/1995, 48 pp., <ftp://ftp.isi.edu/in-notes/rfc1848.txt>
- RFC 1847, "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted", 10/03/1995, 11 pp., <ftp://ftp.isi.edu/in-notes/rfc1847.txt>
- RFC 1847, "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted", 10/03/1995, 11 pp., <ftp://ftp.isi.edu/in-notes/rfc1847.txt>
- RFC 1828, "IP Authentication using Keyed MD5", 08/09/1995, 5 pp., <ftp://ftp.isi.edu/in-notes/rfc1828.txt>
- RFC 1827, "IP Encapsulating Security Payload (ESP)", 08/09/1995, 12 pp., <ftp://ftp.isi.edu/in-notes/rfc1827.txt>

- RFC 1826, "IP Authentication Header", 08/09/1995, 13 pp., <ftp://ftp.isi.edu/in-notes/rfc1826.txt>
- RFC 1825, "Security Architecture for the Internet Protocol", 08/09/1995, 22 pp., <ftp://ftp.isi.edu/in-notes/rfc1825.txt>
- RFC 1824, "The Exponential Security System TESS: An Identity-Based Cryptographic Protocol for Authenticated Key-Exchange (E.I.S.S.-Report 1995/4)", 08/11/1995, 21 pp., <ftp://ftp.isi.edu/in-notes/rfc1824.txt>
- RFC 1824, "The Exponential Security System TESS: An Identity-Based Cryptographic Protocol for Authenticated Key-Exchange (E.I.S.S.-Report 1995/4)", 08/11/1995, 21 pp., <ftp://ftp.isi.edu/in-notes/rfc1824.txt>
- RFC 1795, "Data Link Switching: Switch-to-Switch Protocol AIW DLSw RIG: DLSw Closed Pages, DLSw Standard Version 1.0", 04/25/1995, 91 pp., <ftp://ftp.isi.edu/in-notes/rfc1795.txt>
- RFC 1750, "Randomness Recommendations for Security", 12/29/1994, 25 pp., <ftp://ftp.isi.edu/in-notes/rfc1750.txt>
- RFC 1734, "POP3 AUTHentication command", 12/20/1994, 5 pp., <ftp://ftp.isi.edu/in-notes/rfc1734.txt>
- RFC 1731, "IMAP4 Authentication mechanisms", 12/20/1994, 6 pp., <ftp://ftp.isi.edu/in-notes/rfc1731.txt>
- RFC 1704, "On Internet Authentication", 10/26/1994, 17 pp., <ftp://ftp.isi.edu/in-notes/rfc1704.txt>
- RFC 1675, "Security Concerns for IPng", 08/08/1994, 4 pp., <ftp://ftp.isi.edu/in-notes/rfc1675.txt>
- RFC 1636, "Report of IAB Workshop on Security in the Internet Architecture - February 8-10, 1994", 06/09/1994, 52 pp., <ftp://ftp.isi.edu/in-notes/rfc1636.txt>
- RFC 1535, "A Security Problem and Proposed Correction With Widely Deployed DNS Software", 10/06/1993, 5 pp., <ftp://ftp.isi.edu/in-notes/rfc1535.txt>
- RFC 1511, "Common Authentication Technology Overview", 09/10/1993, 2 pp., <ftp://ftp.isi.edu/in-notes/rfc1511.txt>
- RFC 1510, "The Kerberos Network Authentication Service (V5)", 09/10/1993, 112 pp., <ftp://ftp.isi.edu/in-notes/rfc1510.txt>
- RFC 1509, "Generic Security Service API : C-bindings", 09/10/1993, 48 pp., <ftp://ftp.isi.edu/in-notes/rfc1509.txt>
- RFC 1507, "DASS - Distributed Authentication Security Service", 09/10/1993, 119 pp., <ftp://ftp.isi.edu/in-notes/rfc1507.txt>
- RFC 1492, "An Access Control Protocol, Sometimes Called TACACS", 07/23/1993, 21 pp., <ftp://ftp.isi.edu/in-notes/rfc1492.txt>
- RFC 1472, "The Definitions of Managed Objects for the Security Protocols of the Point-to-Point Protocol", 06/08/1993, 11 pp., <ftp://ftp.isi.edu/in-notes/rfc1472.txt>
- RFC 1457, "Security Label Framework for the Internet", 05/26/1993, 14 pp., <ftp://ftp.isi.edu/in-notes/rfc1457.txt>
- RFC 1455, "Physical Link Security Type of Service", 05/26/1993, 6 pp., <ftp://ftp.isi.edu/in-notes/rfc1455.txt>
- RFC 1446, "Security Protocols for version 2 of the Simple Network Management Protocol (SNMPv2)", 05/03/1993, 51 pp., <ftp://ftp.isi.edu/in-notes/rfc1446.txt>
- RFC 1424, "Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services", 02/10/1993, 9 pp., <ftp://ftp.isi.edu/in-notes/rfc1424.txt>
- RFC 1423, "Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers", 02/10/1993, 14 pp., <ftp://ftp.isi.edu/in-notes/rfc1423.txt>
- RFC 1422, "Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management", 02/10/1993, 32 pp., <ftp://ftp.isi.edu/in-notes/rfc1422.txt>
- RFC 1421, "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures", 02/10/1993, 42 pp., RFC Index <ftp://ftp.isi.edu/in-notes/rfc1421.txt>

- RFC 1416, "Telnet Authentication Option", 02/01/1993, 7 pp., <ftp://ftp.isi.edu/in-notes/rfc1416.txt>
- RFC 1412, "Telnet Authentication : SPX", 01/27/1993, 4 pp., <ftp://ftp.isi.edu/in-notes/rfc1412.txt>
- RFC 1411, "Telnet Authentication: Kerberos Version 4", 01/26/1993, 4 pp., <ftp://ftp.isi.edu/in-notes/rfc1411.txt>
- RFC 1355, "Privacy and Accuracy Issues in Network Information Center Databases", 08/04/1992, 4 pp., (FYI 15) <ftp://ftp.isi.edu/in-notes/rfc1355.txt>
- RFC 1352, "SNMP Security Protocols", 07/06/1992, 41 pp., <ftp://ftp.isi.edu/in-notes/rfc1352.txt>
- RFC 1170, "Public Key Standards and Licenses", 01/11/1991, 2 pp., <ftp://ftp.isi.edu/in-notes/rfc1170.txt>
- RFC 1108, "U.S. Department of Defense Security Options for the Internet Protocol", 11/27/1991, 17 pp., <ftp://ftp.isi.edu/in-notes/rfc1108.txt>
- RFC 1004, "Distributed-protocol authentication scheme", 04/01/1987, 8 pp., <ftp://ftp.isi.edu/in-notes/rfc1004.txt>
- RFC 927, "TACACS user identification Telnet option", 12/01/1984, 4 pp., <ftp://ftp.isi.edu/in-notes/rfc927.txt>
- RFC 644, "On the problem of signature authentication for network mail", 07/22/1974, 6 pp., <ftp://ftp.isi.edu/in-notes/rfc644.txt>

Internet Drafts on L2TP

- "Layer Two Tunneling Protocol : ATM access extensions.", 08/10/1998, <ftp://www.ietf.org/internet-drafts/draft-tjoens-pppext-l2tp-atmext-00.txt>
- "Layer Two Tunneling Protocol 'L2TP'", 05/22/1998, <ftp://www.ietf.org/internet-drafts/draft-ietf-pppext-l2tp-11.txt>
- "Layer Two Tunneling Protocol 'L2TP' Security Extensions for Non-IP networks", 07/29/1998, <ftp://www.ietf.org/internet-drafts/draft-ietf-pppext-l2tp-sec-04.txt>
- "Layer Two Tunneling Protocol 'L2TP' Management Information Base", 08/06/1998, <ftp://www.ietf.org/internet-drafts/draft-ietf-pppext-l2tp-mib-02.txt>
- "L2TP Header Compression ('L2TPHC')", 12/22/1997, <ftp://www.ietf.org/internet-drafts/draft-ietf-pppext-l2tp-hc-01.txt>
- "Securing L2TP using IPSEC", 05/22/1998, <ftp://www.ietf.org/internet-drafts/draft-ietf-pppext-l2tp-security-02.txt>
- "L2TP-over-IP Path MTU Discovery ('L2TPMTU')", 01/05/1998, <ftp://www.ietf.org/internet-drafts/draft-ietf-pppext-l2tpmtu-00.txt>
- "L2TP Alternate Data Channel ('L2TPADC')", 01/13/1998, <ftp://www.ietf.org/internet-drafts/draft-ietf-pppext-l2tpadc-00.txt>
- "Layer Two Tunneling Protocol 'L2TP' IP Differential Services Extension", 07/29/1998, <ftp://www.ietf.org/internet-drafts/draft-ietf-pppext-l2tp-ds-02.txt>
- "Layer Two Tunneling Protocol 'L2TP' Multi-Protocol Label Switching Extension", 07/29/1998, <ftp://www.ietf.org/internet-drafts/draft-ietf-pppext-l2tp-mpls-01.txt>
- "L2TP Dynamic Data Window Adjustment", 06/26/1998, <ftp://www.ietf.org/internet-drafts/draft-ietf-pppext-l2tpdwin-00.txt>
- "Layer Two Tunneling Protocol (L2TP) over Frame Relay", 07/15/1998, <ftp://www.ietf.org/internet-drafts/draft-ietf-pppext-l2tp-fr-00.txt>
- "L2TP Over AAL5 and FUNI", 08/06/1998, <ftp://www.ietf.org/internet-drafts/draft-ietf-pppext-l2tp-atm-00.txt>
- "Implementation of PPTP/L2TP Compulsory Tunneling via RADIUS", 05/21/1998, <ftp://www.ietf.org/internet-drafts/draft-ietf-radius-tunnel-imp-03.txt>
- "Layer Two Tunneling Protocol : ATM access extensions.", 08/10/1998,

- <ftp://www.ietf.org/internet-drafts/draft-tjoens-pppext-l2tp-atmext-00.txt>
- "Layer Two Tunneling Protocol 'L2TP'", 05/22/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-pppext-l2tp-11.txt>
- "Layer Two Tunneling Protocol 'L2TP' Security Extensions for Non-IP networks", 07/29/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-pppext-l2tp-sec-04.txt>
- "Layer Two Tunneling Protocol 'L2TP' Management Information Base", 08/06/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-pppext-l2tp-mib-02.txt>
- "L2TP Header Compression ('L2TPHC')", 12/22/1997,
<ftp://www.ietf.org/internet-drafts/draft-ietf-pppext-l2tp-hc-01.txt>
- "Securing L2TP using IPSEC", 05/22/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-pppext-l2tp-security-02.txt>
- "L2TP-over-IP Path MTU Discovery ('L2TPMTU')", 01/05/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-pppext-l2tpmtu-00.txt>
- "L2TP Alternate Data Channel ('L2TPADC')", 01/13/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-pppext-l2tpadc-00.txt>
- "Layer Two Tunneling Protocol 'L2TP' IP Differential Services Extension", 07/29/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-pppext-l2tp-ds-02.txt>
- "Layer Two Tunneling Protocol 'L2TP' Multi-Protocol Label Switching Extension", 07/29/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-pppext-l2tp-mpls-01.txt>
- "L2TP Dynamic Data Window Adjustment", 06/26/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-pppext-l2tpdwin-00.txt>
- "Layer Two Tunneling Protocol (L2TP) over Frame Relay", 07/15/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-pppext-l2tp-fr-00.txt>
- "L2TP Over AAL5 and FUNI", 08/06/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-pppext-l2tp-atm-00.txt>
- "Implementation of PPTP/L2TP Compulsory Tunneling via RADIUS", 05/21/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-radius-tunnel-imp-03.txt>

Internet Drafts on IPsec

- "Internet Security Association and Key Management Protocol (ISAKMP)", 07/10/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-ipsec-isakmp-10.txt> or
<ftp://www.ietf.org/internet-drafts/draft-ietf-ipsec-isakmp-10.ps>
- "The OAKLEY Key Determination Protocol", 07/25/1997,
<ftp://www.ietf.org/internet-drafts/draft-ietf-ipsec-oakley-02.txt>
- "The ESP Triple DES Transform", 07/03/1997,
<ftp://www.ietf.org/internet-drafts/draft-ietf-ipsec-ciph-des3-00.txt>
- "IP Authentication Header", 07/06/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-ipsec-auth-header-07.txt>
- "Security Architecture for the Internet Protocol", 08/05/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-ipsec-arch-sec-07.txt>
- "The Internet Key Exchange (IKE)", 06/10/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-ipsec-isakmp-oakley-08.txt>
- "The Internet IP Security Domain of Interpretation for ISAKMP", 07/07/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-ipsec-ipsec-doi-10.txt>
- "Implementation of Virtual Private Network (VPNs) with IP Security", 03/14/1997,
<ftp://www.ietf.org/internet-drafts/draft-ietf-ipsec-vpn-00.txt>
- "The Use of HMAC-MD5-96 within ESP and AH", 02/18/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-ipsec-auth-hmac-md5-96-03.txt>

- "The ESP DES-CBC Cipher Algorithm With Explicit IV", 02/13/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-ipsec-ciph-des-expiv-02.txt>
- "IP Security Document Roadmap", 12/04/1997,
<ftp://www.ietf.org/internet-drafts/draft-ietf-ipsec-doc-roadmap-02.txt>
- "The Use of HMAC-SHA-1-96 within ESP and AH", 02/18/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-ipsec-auth-hmac-sha196-03.txt>
- "IP Encapsulating Security Payload (ESP)", 07/06/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-ipsec-esp-v2-06.txt>
- "ESP with Cipher Block Check Sums (CBCS)", 07/24/1997,
<ftp://www.ietf.org/internet-drafts/draft-simpson-ipsec-cbc3-01.txt>
- "The ESP CBC-Mode Cipher Algorithms", 09/08/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-ipsec-ciph-cbc-03.txt>
- "The ISAKMP Configuration Method", 05/21/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-ipsec-isakmp-mode-cfg-04.txt>
- "The Use of HMAC-RIPEMD-160-96 within ESP and AH", 07/24/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-ipsec-auth-hmac-ripemd-160-96-02.txt>
- "A GSS-API Authentication Mode for ISAKMP/Oakley", 12/23/1997,
<ftp://www.ietf.org/internet-drafts/draft-ietf-ipsec-isakmp-gss-auth-01.txt>
- "Dynamic remote host configuration over IPSEC using DHCP", 12/04/1997,
<ftp://www.ietf.org/internet-drafts/draft-ietf-ipsec-dhcp-00.txt>
- "Revised SA negotiation mode for ISAKMP/Oakley", 12/04/1997,
<ftp://www.ietf.org/internet-drafts/draft-ietf-ipsec-isakmp-SA-revised-00.txt>
- "Extended Authentication Within ISAKMP/Oakley", 05/21/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-ipsec-isakmp-xauth-02.txt>
- "IPSec Policy Data Model", 02/25/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-ipsec-policy-model-00.txt>
- "The Pre-Shared Key for the Internet Protocol", 04/06/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-ipsec-internet-key-00.txt>
- "A DH-less encryption mode for IKE", 07/06/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-ipsec-dhless-enc-mode-00.txt>
- "A Framework for Group Key Management for Multicast Security", 08/05/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-ipsec-gkmframework-00.txt>
- "PKI Requirements for IP Security", 09/15/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-ipsec-pki-req-01.txt>
- "Use of IPSec in Mobile IP", 01/08/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-mobileip-ipsec-use-00.txt>
- "ICMP Security Failures Messages", 04/30/1996,
<ftp://www.ietf.org/internet-drafts/draft-simpson-icmp-ipsec-fail-02.txt>
- "Internet Security Transform Enhancements", 04/30/1997,
<ftp://www.ietf.org/internet-drafts/draft-simpson-ipsec-enhancement-01.txt>
- "Path MTU discovery in the presence of security gateways", 09/04/1998,
<ftp://www.ietf.org/internet-drafts/draft-richardson-ipsec-pmtu-discov-02.txt>
-
- "Configuration of Tunnel Mode Isec Endpoint Parameters", 11/26/1997,
<ftp://www.ietf.org/internet-drafts/draft-ohara-ipsecparam-00.txt>
- "Definition of a Common Management Interface Format", 12/30/1997,
<ftp://www.ietf.org/internet-drafts/draft-liu-ipsec-vpn-management-00.txt>
- "Network Address Translation issues with IPsec", 02/12/1998,
<ftp://www.ietf.org/internet-drafts/draft-moskowitz-net66-vpn-00.txt>
- "DIAMETER IP Security Policy Extensions", 03/05/1998,

- <ftp://www.ietf.org/internet-drafts/draft-calhoun-diameter-ipsec-policy-00.txt>
- "Secure, Remote Access over the Internet using IPSec", 06/17/1998,
<ftp://www.ietf.org/internet-drafts/draft-gupta-ipsec-remote-access-00.txt>
- "A Hybrid Authentication Mode for IKE", 06/26/1998,
<ftp://www.ietf.org/internet-drafts/draft-litvin-ipsec-isakmp-hybrid-auth-00.txt>
- "ISAKMP Certificate Key Exchange Type Specification", 07/31/1998,
<ftp://www.ietf.org/internet-drafts/draft-shima-ipsec-isakmp-cke-type-00.txt>
- "RADIUS IP Security Extensions", 11/10/1997,
<ftp://www.ietf.org/internet-drafts/draft-ietf-radius-ipsec-00.txt>

Internet Drafts on RADIUS

- "Lightweight Directory Access Protocol (v3): Dynamic Attributes for the Remote Access Dialin User Service (RADIUS)", 11/21/1997,
<ftp://www.ietf.org/internet-drafts/draft-aboba-dynradius-01.txt>
- "Lightweight Directory Access Protocol (v3): Schema for the Remote Access Dialin User Service (RADIUS)", 02/05/1998, <ftp://www.ietf.org/internet-drafts/draft-aboba-radius-02.txt>
- "RADIUS Extension for Multicast Router Authentication", 03/18/1998,
<ftp://www.ietf.org/internet-drafts/draft-yamanouchi-radius-ext-00.txt>
- "ACC's Vendor Specific Attributes", 05/22/1998,
<ftp://www.ietf.org/internet-drafts/draft-ilgun-radius-accvsa-00.txt>
- "RADIUS Attributes for Tunnel Protocol Support", 04/08/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-radius-tunnel-auth-05.txt>
- "Extensible Authentication Protocol Support in RADIUS", 05/13/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-radius-eap-05.txt>
- "RADIUS Accounting Interim Accounting Record Extension", 01/27/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-radius-acct-interim-01.txt>
- "RADIUS Accounting Server MIB", 02/16/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-radius-acc-servmib-01.txt>
- "RADIUS Authentication Server MIB", 02/16/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-radius-auth-servmib-01.txt>
- "RADIUS Authentication Client MIB", 02/16/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-radius-auth-clientmib-01.txt>
- "RADIUS Accounting Client MIB", 02/16/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-radius-acc-clientmib-01.txt>
- "RADIUS Attributes for MS-CHAP Support", 11/06/1997,
<ftp://www.ietf.org/internet-drafts/draft-rfcd-info-zorn-01.txt>
- "RADIUS Attributes for MS-CHAP Support", 11/18/1997,
<ftp://www.ietf.org/internet-drafts/draft-ietf-radius-mschap-attr-01.txt>
- "RADIUS Accounting Modifications for Tunnel Protocol Support", 09/08/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-radius-tunnel-acct-02.txt>
- "Salt-Encryption of RADIUS Attributes", 12/04/1997,
<ftp://www.ietf.org/internet-drafts/draft-ietf-radius-saltencrypt-00.txt>
- "RADIUS Attributes for Multilink PPP Bandwidth Allocation Control", 02/16/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-radius-bap-01.txt>
- "RADIUS Attributes for Multilink PPP Bandwidth Allocation Control", 02/25/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-radius-ms-ba-attr-01.txt>
- "Support for Mobile IP in RADIUS", 04/20/1998,
<ftp://www.ietf.org/internet-drafts/draft-ietf-radius-mobileip-00.txt>

- "Secure Radius Server Operation Guidelines for Dial Roaming ", 10/21/1997,
<ftp://www.ietf.org/internet-drafts/draft-ietf-roamops-sec-00.txt>

Internet Drafts on DIAMETER

- "DIAMETER User Authentication Extensions", 07/28/1998,
<ftp://www.ietf.org/internet-drafts/draft-calhoun-diameter-authent-04.txt>
- "DIAMETER Base Protocol", 09/14/1998,
<ftp://www.ietf.org/internet-drafts/draft-calhoun-diameter-05.txt>
- "DIAMETER Extensible Authentication Protocol Extensions", 03/05/1998,
<ftp://www.ietf.org/internet-drafts/draft-calhoun-diameter-eap-01.txt>
- "DIAMETER Resource Management Extensions", 07/28/1998,
<ftp://www.ietf.org/internet-drafts/draft-calhoun-diameter-res-mgmt-02.txt>
- "DIAMETER Framework Document", 07/31/1998,
<ftp://www.ietf.org/internet-drafts/draft-calhoun-diameter-framework-01.txt>
- "DIAMETER QOS Extension", 05/28/1998,
<ftp://www.ietf.org/internet-drafts/draft-calhoun-diameter-qos-00.txt>
- "Bi-Directional Session Setup Extension to Diameter", 07/23/1998,
<ftp://www.ietf.org/internet-drafts/draft-greene-diameter-ss7-session-00.txt>
- "DIAMETER: Policy and Accounting Extension for SIP", 07/31/1998,
<ftp://www.ietf.org/internet-drafts/draft-pan-diameter-sip-00.txt>
- "DIAMETER Mobile IP Extensions", 08/03/1998,
<ftp://www.ietf.org/internet-drafts/draft-calhoun-diameter-mobileip-00.txt>
- "DIAMETER Proxy Server Extensions", 09/14/1998,
<ftp://www.ietf.org/internet-drafts/draft-calhoun-diameter-proxy-00.txt>
- "DIAMETER Device Configuration Extensions", 09/14/1998,
<ftp://www.ietf.org/internet-drafts/draft-greene-diameter-devconf-00.txt>

Other Internet Drafts

- "The TACACS+ Protocol Version 1.78", 01/06/1998,
<ftp://www.ietf.org/internet-drafts/draft-grant-tacacs-02.txt>