

The Must-Have Reference for IP and Next Generation Networking

This reference provides the information you need to understand the terminology associated with IP and next generation network switching, routing, and testing products. It enables you to make informed decisions about the products.

Understanding the Layers

Internetworking devices such as bridges, routers, and switches have traditionally been categorized by the OSI layer they operate at and the role they play in the topology of a network:

- Bridges and switches operate at Layer 2: they extend network capabilities by forwarding traffic among LANs and LAN segments with high throughput.
- Routers operate at Layer 3: they perform route calculations based on Layer 3 addresses and provide multi-protocol support and WAN access, but typically at the cost of higher latency and much more complex administration requirements.

Layer 2 refers to the layer in the communications protocol that contains the physical address of a client or server station. It is also called the data link layer or MAC layer. Layer 2 contains the address that is inspected by a bridge, switch, or PC NIC. The Layer 2 address of every network device is unique, fixed in hardware by its manufacturer and usually never changed. Traditionally, products that were called switches operated by forwarding all traffic based on its Layer 2 addresses.

Layer 3 refers to the layer in the communications protocol that contains the logical address of a client or server station. It is also called the network layer. Layer 3 contains the address (such as IP or IPX) that is inspected by a router that forwards the traffic through the network. The Layer 3 address of a network device is a software setting established by the user network administrator that can and does change from time to time; only devices that need to be addressed by Layer 3 protocols such as IP have Layer 3 addresses. Traditionally, routers operated solely on Layer 3 addresses.

What is Multilayer Switching?

Multilayer switching is simply the combination of traditional Layer 2 switching with Layer 3 protocol routing in a single product, usually through a fast hardware implementation. In fact, it is this hardware that has enabled the recent development and success of the multilayer switch. New higher-density ASICs (Application-Specific Integrated Circuits) allow real-time switching and forwarding with wirespeed performance, and at lower cost than traditional software-based routers built around general-purpose CPUs.

Three factors combined over the last two years to fuel the evolution of multilayer switching:

- Users need to get beyond the performance bottleneck of collapsed backbone routers and avoid the high cost of expanding them.
- IP traffic from intranet and Internet applications has increased dramatically.
- ASIC densities increased enough to allow economic implementation of complex routing functions directly in high-speed hardware instead of using the slow software techniques of traditional routers.

Multilayer Switch Names

Vendors, analysts, and editors don't agree about the specific meaning of terms such as multilayer switch, Layer 3 switch, IP switch, routing switch, switching router, and wirespeed router. Typically these different terms don't reflect differences in product architecture as much as differing editorial and marketing policies.

Nevertheless, the term multilayer switch is a widely used description of this class of product that performs both Layer 3 routing and Layer 2 switching functions.

Basic Multilayer Switch Architectures

Many new switching products are being introduced and their various naming schemes are confusing. To deal with all of this it is helpful to sort products into one of four groups according to what multilayer switching technique they use: generic cut-through routing, ATM-based cut-through routing, Layer 3 learning bridging, and wirespeed routing. These are described here, with some guidelines to help you recognize which is which.

Generic Cut-Through Routing In this architecture Layer 3 routing calculations are performed only on the first packet in a data flow, either by a router or by a separate route server. Following packets that are identified as belonging to the same flow are switched at Layer 2 along the same route. The two key functions of a traditional router – route calculation and frame forwarding – are thus handled very differently in this architecture.

After the initial route calculation has been completed, the following frames benefit from the low latency and high throughput of Layer 2 switching, but are not truly “routed”. Different vendors implement the cut-through scheme using a variety of proprietary technologies. As a result, cut-through routing products from different vendors can rarely interoperate to exchange routing information or continue forwarding the data at Layer 2. These devices can often be recognized by the proprietary names of their routing schemes, such as “FastIP”, “SecureFast”, or “DirectIP”.

ATM-Based Cut-Through Routing This variation of generic cut-through routing is based on ATM cells rather than frames, and products referred to as IP switches and tag switches generally fall into this category. ATM-based cut-through routing offers several advantages over generic cut-through techniques, including improved support of LAN emulation and multi-vendor support in the form of the Multiprotocol Over ATM (MPOA) standard. However, ATM networking requires a significant initial investment as well as extra training to allow IS managers to support its higher complexity. Accordingly, this option makes sense only if an ATM structure in the network is dictated by other concerns.

Layer 3 Learning Bridging Layer 3 learning bridging differs from the other architectures in that it performs no routing whatsoever. Instead, it uses IP “snooping” techniques to learn the MAC/IP address relationships of endstations from true routers that must exist elsewhere in the network. Then it redirects traffic away from the routers and switches it based on its Layer 2 addresses. The easiest way to recognize these devices is by their lack of support for any dynamic routing protocols such as RIP or OSPF. These devices offer short-term relief for overloaded routers, but are only a temporary tactical solution due to their limited functionality and proprietary nature.

Wirespeed Routing Wirespeed routing -- from vendors such as Anritsu Company, Extreme Networks, and Foundry Networks -- is one of the newest multilayer switching techniques and also represents the future of this technology. Unlike cut-through and learning bridging, this architecture routes every packet individually. It is

often referred to as packet-by-packet Layer 3 switching. Using advanced ASICs to perform Layer 3 routing in hardware, it implements dynamic routing protocols such as OSPF and RIP. This type of product often goes beyond basic IP routing to support IP multicast routing, VLAN segregation, and multiple priority levels to assist in quality of service.

Unlike the cut-through techniques, wirespeed routing does not introduce proprietary technology into the network, so it offers full interoperability and avoids excessive administrative overhead. In effect, these devices are true routers capable of operating at speeds formerly associated only with Layer 2 switches.

What About Layer 4 Switching?

Recently the term “Layer 4 switching” has emerged in the multilayer switch market, adding to the confusion of people who are still trying to get comfortable with Layer 3 switching. This is mostly a marketing term rather than a precise technical description. Layer 4 switching refers to a product’s ability to make various traffic handling decisions such as prioritization or filtering based on the contents of OSI layer 4 (the Transport Layer) where the endstation application is identified. Layer 4 switching almost always refers to capabilities that augment the Layer 2 and 3 functions of a multilayer switch rather than to some new type of switching. Products with Layer 4 capabilities frequently use those parameters to control which server a data packet is sent to.

Why Aren’t Multilayer Switches Called Routers?

If multilayer switches perform both parts of the router’s traditional function—route calculation and traffic forwarding based on Layer 3 protocols—then why aren’t they called routers? There are a variety of technical and market-based reasons.

The technical reasons that multilayer switches aren’t called “routers” are:

- Multilayer switches are much faster and less expensive than routers.
- Some multilayer switches are really small stackable workgroup switches and lack the modularity, flexibility, and port density usually associated with routers.
- Many are more limited than routers in the variety of traffic and routing protocols they support, although some multilayer switches designed for ATM-based networks are protocol-independent. Most currently support only traffic based on IP. Several support IPX and a few other traffic types as well. For example,

Anritsu multilayer switches handle IP, IPX, and AppleTalk traffic.

- Multilayer switches generally don't support all the WAN interfaces handled by traditional routers. But this is changing and innovative vendors such as Anritsu will focus on that area in the future.

In addition to these technical differences, there are marketing-oriented reasons why most vendors avoid referring to multilayer switches as routers. Because of their dramatically lower price, device vendors introducing multilayer switches as a new high-performance class of router risk cutting into the sales of their established router product lines. And some vendors want to avoid associating the new devices in customers' minds with the much slower, higher-cost routers they are designed to replace.

The Evolution of Routers and Switches

Routers When first introduced, routers played a central role in the development of the modern hierarchical network. By calculating routes and forwarding traffic among subnetworks based on Layer 3 address protocols, they enabled managers to extend the area that an enterprise network could cover. In addition, the segmentation of networks into subnets reduced the number of users per LAN, and lessened the volume of broadcast traffic within each LAN. However, as computing technology advanced, the delays caused by the router's software-based processing became a problem.

With faster PC speeds and new types of user network access generating unprecedented levels of traffic, the relatively low throughput of software-based routers created performance bottlenecks within enterprise networks. Routers would always be essential in allowing LANs and WANs based on different protocols to communicate, calculating efficient routes, and performing vital filtering and security functions. But now, intranet applications have created the need for multilayer switching by demanding higher-throughput, lower-cost devices without requiring all the features of a traditional router.

Switches Switches were introduced as an alternative to routers for use within a LAN. These simple devices operate at Layer 2, directing traffic by MAC address rather than routing by the network address at Layer 3. By handling intra-subnet traffic quickly and efficiently, and interconnecting LANs through multiple ports, switches reduced the amount of traffic passed on to routers. Routers, in turn, were pushed to the WAN interface at the edge of the network. Priced affordably, switches let network managers increase bandwidth without adding complexity or latency to the network.

But Layer 2 switching has its own problems. Unlike hierarchical router-based structures, flat switched networks can allow routine status updates to generate bandwidth-choking broadcast storms. Virtual LANs, in which endstations are grouped into broadcast domains, offer some relief. However, some VLANs are single-vendor solutions, introducing the limitations of proprietary technology into the network. Furthermore, the routers used to interconnect VLANs introduce new bottlenecks.

The spanning tree protocol, implemented in many Layer 2 switches, prevents forwarding loops in switched networks. But this works by shutting down redundant connections and never using them. In contrast, routers are able to keep redundant connections active and make use of this built-in redundancy to increase network reliability and performance.

Most significantly, the rise of the Internet and the increasing role of Web-based intranets and applications have shifted enterprise traffic dramatically. Whereas in the past most traffic was local in nature, the majority of packets are now directed outside the host's subnet, and often outside the enterprise network. High-volume IP traffic, such as videoconferencing and distributed workflow applications, has driven the demand for high-performance, wide bandwidth networks. While Layer 2 switches play an important role in increasing performance within an enterprise, their inability to perform Layer 3 routing leaves them ineffective in meeting this new challenge.

With Layer 2 switching reaching the limits of its potential, the multilayer switch represents the next stage in the evolution of internetworking devices.

Terms Used in Conjunction with IP and Next Generation Networking

In the descriptions of terms that follow, underlined words signify hyperlinks that are present in the online version of this document at www.us.anritsu.com/musthave. While online, clicking on a hyperlink will take you to a place on the Web where substantial additional information about that term is available. The online version of this document is updated frequently, and may contain new terms or new information about one of the terms below.

Overview of Terms by Topic

The terms referenced in this overview are described in detail in the alphabetic list of terms and abbreviations that follows.

ATM Terms that are related to ATM networking:

- ARA (Address Resolution Advertisement)
- BUS (Broadcast and Unknown Server): see LANE
- CIP (Classical IP Over ATM): see IP Over ATM
- FANP (Flow Attribute Notification Protocol)
- GSMP (General Switch Management Protocol)
- IFMP (Ipsilon Flow Management Protocol)
- IMA (Inverse Multiplexing over ATM)
- I-PNNI (Integrated PNNI)
- IPOA, IP Over ATM
- LANE (ATM LAN Emulation)
- LECS (LAN Emulation Configuration Server): see LANE
- LES (LAN Emulation Server): see LANE
- MARS (Multicast Address Resolution Server)
- MPLS (Multi-Protocol Label Switching)
- MPOA (Multiprotocol over ATM)
- Multiprotocol Encapsulation Over ATM AAL5
- PNNI (Private Network-to-Network Interface)
- VTOA (Voice and Telephony over ATM)

Ethernet Over SONET/SDH Terms that are related to transporting Ethernet efficiently over SONET and SDH:

- BCP (Bridging Control Protocol)
- EoS (Ethernet Over SONET/SDH)
- EoS-VC (Ethernet Over SONET Virtual Concatenation)
- GFP (Generic Framing Protocol)
- LAPF (Link Access Procedure-Frame Mode)
- LAPS or X.86 (Link Access Procedure-SDH)
- LCAS (Link Capacity Adjustment Scheme)
- LEX (LAN Extension Protocol)

Gigabit Ethernet Terms that are related to Gigabit and 10 Gigabit Ethernet:

- 802.3ae (10 Gigabit Ethernet)
- 802.3ab (Gigabit Ethernet on Copper Twisted Pair)
- 802.3z (Gigabit Ethernet on Fiber and Shielded Copper)
- 1000BASE-XX (Gigabit Ethernet)
- CJPAT (Continuous Jitter Tolerance Test Pattern)
- CRPAT (Continuous Random Test Pattern)
- Ethernet Data Rates
- XAUI (10 Gb Ethernet Transceiver Interface)
- X2, XENPAK, XFP, and XPAK (10 Gbps interface multi-source agreements)

IP Switching The IP switching approach for IP over ATM was developed by Ipsilon. Its protocols are now in the public domain as informational RFCs to encourage acceptance and usage:

- GSMP (General Switch Management Protocol)
- IFMP (Ipsilon Flow Management Protocol)

IPv6 Terms that are associated with the new Internet Protocol version 6 or that contain references to it:

- DHCP (Dynamic Host Configuration Protocol)
- ICMP (Internet Control Message Protocol)
- NDP (Neighbor Discovery Protocol)
- OSPF (Open Shortest Path First)

Also see the term IPv6.

Link Aggregation Terms that are associated with link aggregation or trunking:

- 802.3ad (Link Aggregation)
- EtherChannel
- ISL (InterSwitch Link)
- LACP (Link Aggregation Control Protocol)
- MPLA (Multi-Point Link Aggregation)
- PNNI (Private Network-to-Network Interface)

Management Terms that are associated with network management:

- HMMP (Hypermedia Management Protocol)
 - RMON and RMON2 (Remote Monitoring)
 - SMON (Switch Monitoring)
 - SNMP (Simple Network Management Protocol)
 - WBEM (Web-Based Enterprise Management)
- Also see Policy-Based Network Management (below).

MPLS Terms that are associated with Multi-Protocol Label Switching:

- CR-LDP (Constraint-Based Routed Label Distribution Protocol)
- Fast Reroute
- GMPLS (Generalized Multi-Protocol Label Switching)
- LDP (Label Distribution Protocol)
- MPLS (Multi-Protocol Label Switching)
- MPλS (Multi-Protocol Lambda Switching)
- RSVP-TE (RSVP With Traffic Engineering Extensions)
- VPN (Virtual Private Network)

Multicast IP multicast requires several protocols to operate:

- IGMP: End stations use IGMP (Internet Group Management Protocol) to specify their participation in a particular multicast group. Routers that support multicast must run IGMP.
- DVMRP, MOSPF, PIM: Routers must also run one of several IP Multicast routing protocols such as DVMRP (Distance Vector Multicast Routing Protocol), MOSPF (Multicast Open Shortest Path First), or PIM (Protocol-Independent Multicast). The routers use these protocols to tell their neighboring routers whether they need to receive the multicast traffic for a particular multicast group.

Other terms that are associated with multicast:

- BGMP (Border Gateway Multicast Protocol)
- CBT (Core Based Trees)
- CGMP (Cisco Group Multicast Protocol)
- MALLOC (Multicast Address Allocation)
- MARS (Multicast Address Resolution Server)
- MBGP (Multicast Border Gateway Protocol)
- MDHCP (Multicast DHCP)
- MFTP (Multicast File Transport Protocol)
- MSDP (Multicast Source Distribution Protocol)
- PGM (Pragmatic General Multicast)
- RMTP (Reliable Multicast Transport Protocol)

Optical Networking Although many terms can apply to optical networking, these terms are particularly relevant:

- DS (Digital Signal)
- G.709 Digital Wrapper
- OTN (Optical Transport Network) – see G.709
- SONET (Synchronous Optical Network)
- WDM (Wavelength Division Multiplexing)

Policy-Based Management Terms that are associated with network management based on overall policies that can be established by network managers:

- CIM (Common Information Model)
- COPS (Common Open Policy Service)

- DEN (Directory Enabled Networking)
- LDAP (Lightweight Directory Access Protocol)
- PBNM (Policy-Based Network Management)
- RSVP (Resource Reservation Protocol)

Also see Management (above).

Quality of Service (QoS) Terms that are associated with traffic priority, class of service, or quality of service:

- 802.1p (Priority and VLAN Topology)
- COPS (Common Open Policy Service)
- DiffServ (Differentiated Services)
- DSCP (Differentiated Services Codepoint) -- see DiffServ
- IntServ (Integrated Services)
- ISSLL (Integrated Services over Specific Link Layers)
- MPLS (Multi-Protocol Label Switching)
- QoS (Quality of Service)
- QoS SR (Quality of Service Routing)
- RSVP (Resource Reservation Protocol)
- SBM (Subnet Bandwidth Manager)
- TOS (Type of Service)

Routing Protocols Dynamic routing protocols include:

- OSPF (Open Shortest Path First), which is popular in large internetworks.
- RIP (Routing Information Protocol), which is often used in small networks.
- IGRP, EIGRP: Cisco offers proprietary protocols IGRP (Interior Gateway Routing Protocol) and EIGRP (Enhanced IGRP) in its network products.

Exterior gateway protocols share only pre-specified information among selected routers. These include:

- BGP (Border Gateway Protocol)
- EGP (Exterior Gateway Protocol)
- IDRP (Interdomain Routing Protocol)

Novell NetWare networks use:

- IPX (Internet Packet Exchange)
- NLSP (NetWare Link Services Protocol)

RTMP: AppleTalk networks use RTMP (Routing Table Management Protocol).

RTP: Banyan VINES servers use RTP (VINES Routing Table Protocol).

Other terms that are associated with dynamic route determination methods:

- ARA (Address Resolution Advertisement)
- ECMP (Equal-Cost Multipath Routing)
- I-PNNI (Integrated PNNI)
- IS-IS (Intermediate System to Intermediate System)
- OMP (Optimized Multipath forwarding)

- PNNI (Private Network-to-Network Interface)
- Traffic Engineering

Security Terms that are associated with network security:

- 802.1x (Port-Based Network Access Control)
- IKE (Internet Key Exchange)
- IPsec (IP Security)
- MD5 (Message Digest 5)
- PKI (Public Key Infrastructure)
- RADIUS (Remote Access Dial-In User Service)
- SHA-1 (Secure Hash Algorithm-1)
- S-HTTP (Secure Hypertext Transfer Protocol)
- SSH (Secure Shell)
- SSL (Secure Socket Layer)
- SOCKS
- TACACS (Terminal Access Controller Access Control System)

SANs and Storage Networking Terms that are associated with Storage Area Networking:

- ESCON (Enterprise System Connection)
- FICON (Fiber Connection)
- iFCP (Internet Fibre Channel Protocol)
- IPFC (IP Over Fibre Channel)
- iSCSI (Internet Small Computer Systems Interface)
- iSNS (Internet Storage Name Service)
- FCIP (Fibre Channel Over TCP/IP)
- mFCP (Metro Fibre Channel Protocol)

Testing Terms that are associated with IP and network testing:

- CJPAT (Continuous Jitter Tolerance Test Pattern)
- CRPAT (Continuous Random Test Pattern)
- IMIX (Internet Mix)
- PRBS (Pseudo-Random Bit Sequence)
- QRSS (Quasi-Random Signal Source)
- RFC1242 (Benchmarking Terminology for Network Interconnection Devices)
- RFC2285 (Benchmarking Terminology for LAN Switching Devices)
- RFC2544 (Benchmarking Methodology for Network Interconnect Devices)
- RFC2889 (Benchmarking Methodology for LAN Switching Devices)
- Tcl (Tool Command Language)

VLANS Terms that are related to Virtual LANs:

- 802.1p (Priority and VLAN Topology)
- 802.1Q (VLAN Tagging)
- 802.1s (Multiple Spanning Trees for VLANs)
- 802.1v (VLAN Classification by Protocol and Port)
- 802.3ac (VLAN Tagging for Ethernet)
- GARP (Generic Attributes Registration Protocol)
- GVRP (GARP VLAN Registration Protocol)
- ISL (InterSwitch Link)
- MST (Multiple Spanning Trees for VLANs)
- PVST (Per-VLAN Spanning Tree)

Voice and Video Terms that are associated with voice or video transmission over LANs:

- H.323 (Real-time transmission of voice, video, and data)
- MGCP (Media Gateway Control Protocol)
- Real-Time Transport Protocol (RTP)
- Real-Time Streaming Protocol (RTSP)
- SIP (Session Initiation Protocol)
- VoIP (Voice Over IP)
- VTOA (Voice and Telephony over ATM)

VPNs Terms that are associated with Virtual Private Networks:

- GRE (Generic Route Encapsulation)
- IPsec (IP Security)
- L2TP (Layer 2 Tunneling Protocol)
- Martini
- NAT (Network Address Translation)
- MPLS (Multi-Protocol Label Switching)
- PPTP (Point to Point Tunneling Protocol)
- VPLS (Virtual Private LAN Service)

Also see the term VPN (Virtual Private Network).

Wireless LANs Terms that are associated with Wireless LANs:

- 802.1x (Port-Based Network Access Control)
- 802.11 Wireless LANs
- LEAP (Lightweight Extensible Authentication Protocol)
- TKIP (Temporal Key Integrity Protocol)
- WAP (Wireless Application Protocol)
- WEP (Wired Equivalent Privacy)
- Wi-Fi (Wireless Fidelity – see 802.11B)

Alphabetic List of Terms and Abbreviations

100BASE-SX

A standard (SP-4360) proposed by over 25 companies in the [Fiber Optics LAN Section](#) of TIA that provides for 100 Mbps Fast Ethernet full duplex operation over 300 meters of FDDI-grade 62.5/125 micron multimode fiber. 100BASE-SX uses 850 nm optics that are compatible with 10 Mbps 10BASE-FL, enabling 10/100 Mbps speed negotiation and upgrades from the installed base of 10 Mbps fiber users. 100BASE-FX, the primary Fast Ethernet fiber standard, operates with 1300 nm optics and can not be compatible with 10BASE-FL.

802.1d Spanning Tree Protocol

See STP (Spanning Tree Protocol). 802.1d now also includes the priority and VLAN standards formerly designated 802.1p and 802.1Q. See 802.1p and 802.1Q.

802.1p Priority and VLAN Topology

A Layer 2 method for signaling network priority on a per-frame basis. There are two components:

- A prioritization component allows network managers to assign priorities to specific packets. It provides for 8 different priorities for Level-2 traffic based on a 3-bit “User Priority” field defined by 802.1Q – see 802.1Q.
- GARP (Group Address Registration Protocol) lets switches and end-stations exchange VLAN topology information.

Although most LANs don't have continual congestion, bursts of traffic may introduce latency that is unacceptable in real-time networks intended to support voice and video. 802.1p specifies a method for reordering packets based on priority to allow for timely delivery of delay-sensitive traffic. There is no specified model in 802.1p for deciding which packet to send next, once they are mapped into multiple queues; this decision is made by each vendor. 802.1p supplements the RSVP protocol – see RSVP.

In addition to defining priority, 802.1p introduces a new protocol: the Generic Attributes Registration Protocol (GARP). Two specific implementations of this protocol have been defined. The first of these is the GARP Multicast Registration Protocol (GMRP), which lets workstations request membership in a multicast domain. The second protocol is the GARP VLAN Registration Protocol (GVRP). GVRP is similar to GMRP, but instead of requesting admission to a multicast domain, the workstation requests admission to a particular VLAN. This protocol links 802.1p and 802.1Q. See GARP, GMRP, and GVRP. NOTE: 802.1p is technically a historical document because this work has been merged into 802.1d.

Issues 802.1p prioritization can be important for assuring timely traffic delivery to the edge of a network or to a PC/application, but there is much more industry support for using Layer 3 Differentiated Services (see DiffServ) to handle traffic classification throughout a network.

802.1Q VLAN Tagging

Defines changes to Ethernet frames that enable them to carry VLAN information. It allows switches to assign end-stations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks. Four bytes have been added to the Ethernet frame for this purpose, causing the maximum Ethernet frame length to increase from 1518 to 1522 bytes. In these 4 bytes, 3 bits allow for up to eight priority levels and 12 bits identify one of 4,094 different VLANs. 802.3ac will define the specifics of these changes for Ethernet frames. 802.1p specifies a method for indicating frame priority based on the new fields -- see 802.1p.

The missions of 802.1p and 802.1Q are to provide a uniform method for conveying frame priority and VLAN trunking information across the network. NOTE: 802.1Q is technically a historical document because this work has been merged into 802.1d.

802.1s Multiple Spanning Trees for VLANs

IEEE standard 802.1Q specifies the operation of virtual local area network (VLAN) bridges, which support VLAN operation within an IEEE 802 bridged LAN. This [802.1s](#) supplement to 802.1Q adds the facility for VLAN bridges to use multiple spanning trees (“MST”), allowing traffic belonging to different VLANs to flow over different paths within the virtual bridged LAN. If a link fails on one spanning tree, the VLANs using that spanning tree can shift to a different spanning tree for failure recovery. See STP (Spanning Tree Protocol) and PVST (Per-VLAN Spanning Tree).

802.1v VLAN Classification by Protocol and Port

IEEE working group [802.1v](#) is developing this standard for defining the structure of a VLAN based on the protocol(s) that it carries and/or the device port(s) that it connects to.

802.1w Rapid Reconfiguration for STP Networks

IEEE working group [802.1w](#) is developing a protocol for much faster reconfiguration of Spanning Tree Protocol (STP)

networks, or “Rapid Spanning Tree Protocol” (RSTP), with a goal of 100 msec. Standard STP requires many seconds to automatically change configuration. See STP.

802.1x Port-Based Network Access Control

The [802.1x supplement](#) to IEEE 802.1d (Spanning Tree Protocol) provides user authentication for IEEE 802-based LANs. It defines the changes necessary to the operation of a MAC Bridge in order to provide port-based network access control capability and a standard way for logging onto networks. Port-based access control, such as a password, can determine whether a user is permitted to access a network and define what network services are made available to the user. Cisco and Microsoft partnered to implement 802.1x on wireless LANs (see 802.11), and work is underway at the IEEE to incorporate 802.1X services into the 802.11 specifications.

802.11 Wireless LANs

802.11 defines standards for wireless LANs and was approved in Jul'97. IEEE 802.11a and 802.11b (standardized in Sept'99) and 802.11g (still in development) define different physical layer standards for wireless LANs, and the 802.11 standard offers no provisions for interoperability between these physical layers. Microsoft certification applies to both 802.11a and 802.11b. The [IEEE 802.11 Working Group](#) page has helpful information.

802.11a

802.11a operates at 5 GHz and provides data rates up to 54 Mbps using OFDM (Orthogonal Frequency Division Multiplexing) modulation, like European digital TV. Compared to 802.11b, 802.11a offers higher (2X-5X) throughput, more available frequencies, avoiding multipath echoes, but shorter range (perhaps 60 feet). Actual throughput is often only 1-2 Mbps. 802.11a products did not become available from most U.S. vendors until early 2002.

802.11b (Wi-Fi)

802.11b operates at 2.4 GHz (along with cordless phones and microwave ovens) and provides data rates up to 11 Mbps over links of 150-300 feet using Direct Sequence Spread Spectrum (DSMM) modulation. Actual throughput is often only 8-10 Mbps. The Wi-Fi Alliance (www.wi-fi.com), previously known as WECA, is involved with certifying interoperability and promoting the standard. 802.11 Planet has a helpful paper comparing [802.11a vs. 802.11b](#). 802.11b-compatible products were the first ones to become available in the U.S.

802.11g

802.11g is an extension to 802.11b to provide data rates up to 54 Mbps while operating at 2.4 GHz like 802.11b but using OFDM modulation like 802.11a. The IEEE has approved a draft standard, and products from vendors are expected by mid-2003 and are expected to have RF interference problems similar to 802.11b. 802.11 Planet has a helpful [tutorial](#) comparing 802.11a with 802.11g.

802.3ab Gigabit Ethernet on Copper Twisted Pair

IEEE standard approved June '99 defining the 802.3 1000BASE-T specification for Gigabit Ethernet operation on up to 100m of 4-pair Category 5 (CAT-5) copper wiring. In addition, it defines operation, testing, and usage requirements for the installed base of CAT-5 copper wiring. 1000BASE-T is important because most of the installed building cabling is CAT-5 UTP, because it will allow much less expensive connections than fiber-based Gigabit Ethernet, and because it allows for auto-negotiation between 100 and 1000 Mbps to make migration easier. Beginning in late 2000 and early 2001, PC servers began shipping with 1000BASE-T NICs (Network Interface Cards) for network connections.

802.3ac VLAN Tagging for Ethernet

Applies the VLAN tagging defined by 802.1Q to Ethernet frames – see 802.1Q.

802.3ad Link Aggregation

IEEE standard to allow users to create a single high-speed logical link that combines several lower-speed physical links: for example, a 200 Mbps logical link that is comprised of 2 separate 100 Mbps Fast Ethernet connections between the same end points. Also see LACP (Link Aggregation Control Protocol) and MPLA (Multi-Point Link Aggregation).

802.3ae 10 Gigabit Ethernet

The IEEE standard was approved in June'02. Operation is full duplex only. Two families of interfaces are defined because LAN and WAN applications for 10 Gigabit Ethernet have different requirements for line speed, coding, and management. The WAN interfaces operate at 9.58 Gbps (the payload rate of SONET OC-192c) for compatibility with the SONET/SDH transport infrastructure, which will allow 10 Gigabit Ethernet links to operate over the installed based of WAN equipment and facilitate transmission over Metropolitan Area Networks (MANs). The LAN interfaces are optimized for the cabling and equipment infrastructure typical in enterprise networks and operate at 10.00 Gbps. This will be the first time that LAN and SONET data rates are closely matched, so this offers an important opportunity to converge LAN, MAN, and WAN traffic. Also see XAUI and XENPAK.

The nomenclature for the physical interface is “10GBASE-mc”, where:

“m” signifies the medium: S=short wavelength (850 nm); L=long wavelength (1300 nm); E=extra long wavelength (1550 nm).

“c” signifies the coding: R=64bit/66bit LAN coding; W=64bit/66bit WAN coding + STS-192 encapsulation; X4=8B/10B LAN coding with 4 wavelengths over WWDM.

The physical media alternatives for 10 Gigabit Ethernet are:

Type	Capacity	Line Rate	Name	Reach	Fiber	Optical Transceiver
LAN	10.0 Gbps	10.3 Gbps	10GBASE-SR	300 m	MMF	850 nm serial
			10GBASE-LR	10 km	SMF	1310 nm serial
			10GBASE-ER	40 km	SMF	1550 nm serial
		4 x 3.125 Gbps	10BASEG-LX4	300 m	MMF	1310 nm WWDM
				10 km	SMF	1310 nm WWDM
WAN	9.29 Gbps	9.953 Gbps	10GBASE-SW	300 m	MMF	850 nm serial
			10GBASE-LW	10 km	SMF	1310 nm serial
			10GBASE-EW	40 km	SMF	1550 nm serial

Vendors stated in a Miercom survey that 10GBASE-LR will be most important in the market, followed by 10GBASE-ER, 10GBASE-SR, 10GBASE-LX4, 10GBASE-LW, 10GBASE-EW, and 10GBASE-SW. The 10 Gigabit Ethernet Alliance is involved with promoting this technology and has some useful information on their web site at www.10gea.org. Technical Essence Webs (www.10gigabit-ethernet.com) has helpful information about the technology, the market, and vendors.

802.3af DTE (Data Terminal Equipment) Power via MDI (Media Dependent Interface)

The IEEE [802.3af](#) task force has the objective of economically providing power through an RJ-45 connector to a single Ethernet device over a twisted-pair link segment. 10BASE-T and 100BASE-TX devices are the primary target; 1000BASE-T (Gigabit Ethernet) is being considered.

802.3ah Ethernet in the First Mile

An IEEE task force formed in Sept'01 to draft a standard for Ethernet in the first mile, after a year-long technical investigation supported by more than 80 companies. Nine vendors (Alloptic, Cisco, Elastic Networks, Ericsson Telecom, Extreme Networks, Finisar, Intel, NTT, and World Wide Packets) announced formation of the Ethernet in the First Mile Alliance ([EFMA](#)), and its first meeting in February '02. The objective of the standard is to transmit Ethernet traffic over existing copper phone lines at up to 10 Mbps and up to 750 m. With fiber links, the goal is 1 Gbps at 10 km. The task force is also working on operations, administration, and maintenance issues. A first draft specification is planned for Sept'02 that will include physical layer specifications for copper, fiber point-to-point, and fiber point-to-multipoint.

802.3x Full Duplex Flow Control

Defines Ethernet frames with start/stop requests and timers. This provides for primitive flow control and takes the place of collisions that don't exist on full-duplex links.

802.3z Gigabit Ethernet on Fiber and Shielded Copper

Defines the 1000BASE-xx standards for Gigabit Ethernet on fiber and shielded copper cabling. The 1000BASE-T standard for operation on 100m of 4-pair Category 5 twisted pair copper cabling is defined by 802.3ab – see 802.3ab.

1000BASE-SX defines operation with short (850nm) wavelength lasers using a dual SC connector – this is the most common Gigabit interface to date:

- MMF 50u:
 - 400 MHz*km modal bandwidth – 500m maximum length
 - 500 MHz*km modal bandwidth – 550m maximum length
- MMF 62.5u (most commonly installed fiber):
 - 160 MHz*km modal bandwidth (old FDDI-grade fiber; TIA 568 spec) – 220m maximum length
 - 200 MHz*km modal bandwidth (ISO/IEC spec) – 275m maximum length

1000BASE-LX defines operation with long (1300nm) wavelength lasers using a dual SC connector:

- MMF 50u (400 and 500 MHz*km modal bandwidth) – 550m maximum length
- MMF 62.5u (500 MHz*km modal bandwidth) – 550m maximum length
- SMF 9u – 5km maximum length

1000BASE -CX defines operation with 150-Ohm shielded balanced copper cables up to 25m (jumper cables). It also supports twin-axial cable used by the majority of pre-standard products.

802.17 Resilient Packet Ring (RPR)

An IEEE standards development project (IEEE802.org/17) begun with 34 companies in December 2000 to define a Resilient Packet Ring Access Protocol for use in Local, Metropolitan, and Wide Area Networks for transfer of data packets at rates scalable to many gigabits per second. Key features include:

- dynamic bandwidth allocation without pre-provisioning;
- higher bandwidth in dual-ring configurations by utilizing both fiber rings for active traffic in normal situations;
- resiliency to respond to node failures in less than 50 msec.;
- simplified provisioning without the need to create connection-oriented circuits; and
- QoS designated in a 3-bit RPR frame header field.

The protocol can use existing physical layer standards such as Gigabit Ethernet, OC-48, and OC-192. It seeks to provide many of the benefits of SONET for high-speed data transfer. RPR has little similarity with SONET except that RPR switches are connected in a ring and restoration can occur within 50 msec. RPR is based in part on Cisco Dynamic Packet Transport (DPT) and Spatial Reuse Protocol (SRP, RFC2892), Luminous Resilient Packet Transport (RPT), and Nortel IPT technologies. The [RPR Alliance](#) was founded in January 2001 to promote the standardization of the technology. The expectation for IEEE standardization is March 2003. Cisco, Dynarc, Luminous, and Nortel are among vendors who say they are shipping products with RPR-like features now.

1000BASE-XX Gigabit Ethernet

For 1000BASE-SX, 1000BASE-LX, and 1000BASE-CX, see 802.3z. For 1000BASE-T, see 802.3ab. 1000BASE-LH is the informal name given to new technology that several vendors are trying to standardize for operating Gigabit Ethernet over fiber at distances up to 80 km or more for MAN applications.

AES Advanced Encryption Standard

The U.S. Government recently selected AES to replace its traditional Data Encryption Standard (see DES) because AES is more secure and much faster to compute. AES is based on a key size of 128, 192, or 256 bits. In February 2001, Cisco stated its intention to support AES. It won't be widely used until the IETF specifies how to use AES within the IP Security (IPsec) and Secure Sockets Layer (SSL) protocols; see IPsec and SSL. Widespread implementation is expected by 2004.

ARA Address Resolution Advertisement

A new OSPF routing service being defined by the IETF (www.ietf.org/html.charters/ospf-charter.html). It propagates IP/ATM address mappings to OSPF ATM-attached routers and allows a shortcut SVC to be set up immediately between distant ATM routers. This avoids the query time and potential packet loss associated with using NHRP. It interoperates with NHRP and MPOA.

ARP Address Resolution Protocol

Based on standard RFC826: a TCP/IP protocol used to obtain the physical address of a node when only its logical IP address is known. An ARP request with a desired IP (Layer 3) address is broadcast onto the network, and the node having that address responds by sending back its hardware (Layer 2) address so that packets can be sent to it.

Reverse ARP (RARP) does the opposite, finding the Layer 3 address that corresponds to a Layer 2 address – see RARP and BootP.

BCP Bridging Control Protocol

Background: The Point-to-Point Protocol (PPP, RFC1661) provides a standard method for transporting multi-protocol data over remote bridges on point-to-point links between two peers such as switches or routers. Using PPP is a common way to transmit Ethernet over SONET (also see EoS).

BCP, defined by RFC2878, is responsible for configuring, enabling, and disabling the bridge protocol modules on both ends of a PPP link.

BGMP Border Gateway Multicast Protocol

See MBGP (Multicast Border Gateway Protocol).

BGP Border Gateway Protocol

Based on IETF RFC1771: a TCP/IP routing protocol for interdomain routing in large networks. It is used in the Internet and enables policy-based routing between ISPs. It could be applicable to corporate intranets that attach to the public Internet at more than one point. It is an alternative to EGP (Exterior Gateway Protocol). The current version is BGP-4. The 1996 web page <http://joe.lindsay.net/bgp.html> contains links to related RFCs, links to tutorial pages, and tips for configuring BGP routing.

Internal BGP is used within one Autonomous System (AS). External BGP is used between two border routers that are in different Autonomous Systems. See MBGP (Multicast Border Gateway Protocol). See GUM.

BITS Building Integrated Timing Supply

The primary timing source in a carrier facility or data center. BITS is usually distributed to equipment using alternate mark inversion (AMI) or binary 8-zero substitution (B8ZS) T1 (1.544 Mbps) circuits. T1s used for synchronization may be special timing circuits from a clock distribution device, or traffic bearing circuits from a trusted network element such as a digital cross-connect system (DCS) or SONET ADM with GPS input.

BootP Bootstrap Protocol

Based on IETF [RFC951](#): a low-level TCP/IP protocol used by a diskless workstation or a network computer to boot itself from the network. BootP enables the station to determine its own logical IP (Layer 3) address upon startup. It uses the UDP transport mechanism and is an alternative to the RARP protocol – see RARP.

DHCP (Dynamic Host Configuration Protocol) includes all the BootP functions, so a DHCP server can respond to BootP requests. See DHCP. A BootP Relay Agent in a router is a function that relays BootP requests from a workstation on one subnet to a BootP or DHCP server on a different subnet. BootP requests are broadcast requests, so without this function the requests will not cross subnet boundaries.

BUS Broadcast and Unknown Server

An ATM LAN Emulation service: see LANE (LAN Emulation).

CBT Core Based Trees

An IETF [draft](#) defining an IP multicast protocol based on shared trees. It uses the existing unicast routing table plus Join/Prune/Graft schemes to build a multicast distribution tree. Related RFC documents include: [RFC2189](#) on Core Based Trees (CBT version 2) Multicast Routing; [RFC2201](#) on Core Based Trees (CBT) Multicast Routing Architecture.

CGMP Cisco Group Multicast Protocol

A Cisco-proprietary form of IGMP (Internet Group Multicast Protocol) snooping. It lets a switch selectively send IP multicast traffic to those ports on a VLAN that want to participate in the multicast.

CIDR Classless Inter-Domain Routing

Based on IETF [RFC1817](#): a method for allocating a contiguous block of Class-C addresses to one organization because sufficient Class-B IP addresses are not available. It uses the existing 32-bit Internet Address Space more efficiently and reduces the burden on routing tables in the Internet. It allows Internet service providers to provide a subnetwork by combining a number of Class C IP addresses into one. This is a notation rather than a protocol. It is used by BGP and OSPF routing protocols (see BGP, OSPF).

CIM Common Information Model

A standard format for storing management information and providing common definitions for managed objects in an enterprise networking environment. The development of the standard was turned over to the DMTF (Desktop Management Task Force). A CIM tutorial is at www.dmtf.org/spec/cim_tutorial. CIM is comprised of a Specification (which defines how it integrates with other management models such as SNMP MIBs) and a Schema (which describes data models). CIM is a key element of Directory Enabled Networking (see DEN).

CIM v2.3 (March 2000) completed the interface between CIM and LDAP, the protocol for accessing DEN-based directories (see LDAP). CIM v2.5 (February 2001) added the Event Model (for alerting management systems about network element failures) and the IPsec Model (defining protocols for secure communications).

SNMP is an alternative management scheme that is well established for networking devices. CIM proponents say that a key strength compared to SNMP is CIM's management object files that define the associations between components and allow users to track the relationships between managed objects.

CIP Classical IP Over ATM

See IP Over ATM.

CJPAT Continuous Jitter Tolerance Test Pattern

CJPAT and CRPAT (Continuous Random Test Pattern) are test patterns specified in the 802.3ae 10 Gigabit Ethernet draft standard for evaluating PMD receiver and transmitter jitter compliance in a system environment.

CLI Command Line Interface

For routers and switches, this is a type of user interface for entering line-by-line commands for control and configuration, typically from a terminal that is either physically attached locally or attached remotely via a telnet network connection.

CMIP Common Management Information Protocol

An ITU-T standard protocol designed for exchanging network monitoring and control information on OSI networks. CMOT (CMIP Over TCP/IP) is a version that runs on TCP/IP networks. [RFC1189](#) describes CMIP and CMOT. Compared to SNMP, CMIP has some additional features, is more complex, and is less popular than SNMP in North America. Carnegie Mellon has a technology description at www.sei.cmu.edu/str/descriptions/cmip_body.html. Also see SNMP and TL1.

COPS Common Open Policy Service

A simple query-and-response protocol defined by IETF [RFC2748](#) for exchanging information over TCP/IP between a policy server (a PDP-Policy Decision Point) and its clients, which are policy enforcing network devices (PEPs - Policy Enforcement Points) such as a multilayer switch. It defines a way for network devices to exchange information about a network's policies – typically related to QoS and security -- with a policy server. For example, Cisco's COPS QoS Policy Manager (QPM-COPS) claims to share policy information with other directory-enabled applications via the COPS protocol and publish information in enterprise directories based on the DEN schema -- see Directory Enabled Networking (DEN) and Lightweight Directory Access Protocol (LDAP).

CR-LDP Constraint-Based Routed Label Distribution Protocol

CR-LDP and RSVP-TE are protocols for distributing labels among MPLS routers for constraint-based routing. See MPLS. [RFC3213](#) explains the applicability of CR-LDP.

CRPAT Continuous Random Test Pattern

See CJPAT (Continuous Jitter Tolerance Test Pattern).

CSV Comma-Separated Values

A Windows-compatible format for data elements separated by commas, such as produced by networking or test equipment.

Data Rates for Ethernet

See Ethernet Data Rates.

DDNS Dynamic Domain Name System

This is an extension to the Domain Name System (DNS) that enables DNS servers to dynamically update the DNS database when a facility such as DHCP assigns an IP address to a network device.

DEN Directory Enabled Networking

A scheme that allows entire networks to be managed by setting enterprise-wide policies instead of by configuring individual network devices such as switches and routers. Such policy-based networking links specific network users or groups to sets of information (policies) that define the network services or priorities they are entitled to. A major part of the DEN effort involves defining the directory structures used to store this information and the protocols by which network applications will access and use the directory information.

There is widespread vendor support for using LDAP as the primary directory access protocol to access directories based on DEN – see LDAP. In March 1998 Cisco and Microsoft, who were leading the DEN effort, gave the CIM working group the responsibility for further DEN development. In September 1998 the DMTF (Desktop Management Task Force – www.dmtf.org/) took over responsibility for defining DEN. DEN is based on the DMTF Common Information Model (see CIM), which is used to represent the devices, services, and users that DEN controls.

Microsoft's Active Directory in Windows 2000 supports DEN, a major step in enabling widespread DEN implementation. Novell supports DEN through NDS eDirectory 8.5, released in October 2000. Sun and Netscape created a joint venture called iPlanet to provide DEN-compatible directories for ecommerce. Cisco Networking Services (CNS) products are based on DEN standards. Various hardware vendors are referencing DEN in connection with their products, but it is not clear that any of these products interoperate.

DES Data Encryption Standard

DES is the U.S. Government-approved encryption standard from the 1970s that has proven to be breakable because of its relatively small 56-bit key size. Most people wanting high security uses the Triple-DES version, based on a key size of 112 or 168 bits. [FIPS standard 46-3](#) designates DES and Triple-DES. DES requires too much computing resources for high speed throughput, so the U.S. Government has recently chosen the Advanced Encryption Standard to replace DES (see AES). Also see IPsec.

DHCP **Dynamic Host Configuration Protocol**

Based on IETF [RFC2131](#): a protocol for dynamic IP address assignment and automatic TCP/IP configuration that provides both static and dynamic address allocation. Extensions are being added to support PC boot from the network: Network PC v1.0 Reference Design specifies using DHCP for network boot, and DHCP is likely to replace RPL. NetWare 5.0 will include support for DHCP. IBM's LAN Client Control Manager v2 uses DHCP, replacing RPL that was used in v1.

DHCP includes all the BootP (Bootstrap Protocol) functions, so a DHCP server can respond to BootP requests. See BootP. DHCPv6 is the version under development for IPv6 – see IPv6. See MDHCP (multicast version of DHCP) and DNS (static address allocation).

Background Manually assigning static addresses to each network device has long been a problem. In the past, workstations used RARP and BootP to obtain IP addresses from the network. But these protocols support only static allocation, and BootP requires workstation information such as the IP host address to be set up manually in a server database. Dynamic address assignment using DHCP provides for easier initial configuration and changes, allowing plug and play network operation for workstations and PCs.

How it works When a DHCP client workstation boots, it broadcasts a DHCP request asking for IP address and configuration parameters from any DHCP server on the network. An authorized DHCP server for this client will suggest an IP address by sending a reply to the client. The client may accept the first IP address or wait for additional offers from other servers on the network. Eventually the client selects the offer made by a particular server sends a request to accept it. That server sends an acknowledgment confirming the client's IP address and providing any other configuration parameters that the client asked for.

The client's DHCP-issued IP address has an associated lease time that defines how long the IP address is valid. The client can repeatedly ask the server for renewal. If the client does not request renewal or if the client machine is shut down, the lease will eventually expire. Then that IP address can be reused by giving it to another machine. DHCP servers can also assign static network addresses to clients. This is handled by giving addresses an infinite lease.

A DHCP Relay Agent in a router is a function that relays DHCP requests from a workstation on one subnet to a DHCP server on a different subnet. DHCP requests are broadcast requests, so without this function the requests will not cross subnet boundaries.

Issues Since DHCP dynamically allocates IP addresses it is possible that one computer that is booted several times may be assigned more than one address on any given day. Furthermore, a computer is not likely to always be assigned the same IP address. To prevent the same IP address from being issued to more than one user on the network, DHCP servers commonly verify addresses by the simplistic approach of issuing a ping to ensure that an IP address isn't already in use. If there's a computer using that address on the network and that computer is running, it sends back a reply. A group of vendors including Cisco, Microsoft, and Novell is submitting a proposal to store configuration data in an LDAP directory where different servers can access it to prevent address duplication (see LDAP).

DiffServ **Differentiated Services**

The result of an IETF working group that is defining a new bandwidth-management scheme for IP networks. The plan redefines part of the existing Type-of-Service (ToS) byte in every IP packet header to mark the priority or service level that packet requires – see TOS; this byte is renamed the DS byte. DiffServ will work well with security protocols because the TOS byte is in the IP header and is therefore not encrypted. The Diff Serv charter is defined at <http://www.ietf.org/html.charters/diffserv-charter.html>. Links to additional information are at www4.ncsu.edu/~kwu/diffserv/qosref.html. Information about proposed standards is contained in [RFC2474](#) and [RFC2475](#). DiffServ has extremely widespread support among equipment vendors and service providers. It is expected to be a key element of Voice Over IP service (see VOIP).

Traffic service requirements are marked in the DS byte in the IP packet header. A 6-bit field called the Differentiated Services Codepoint (DSCP) defines the per-hop behavior (PHB) that the packet will receive; 2 bits are currently unused. The DS byte determines how a multilayer switch or router will handle the packet. Setting the bits in the DS byte will typically be performed only at the network boundary.

The scheme is expected to scale well because the work of making these assignments, which involves examining Layer 3 or higher layers of each packet, is limited to edge routers. LDAP is the likely protocol that these routers will use for handling policies regarding how to mark each packet (see LDAP). Routers in the core of the network simply examine Layer 2 and give the same service to all packets that are marked the same way. ISPs, or potentially ISP customers, may be able to mark the packets based on service level agreements.

Other references: See Integrated Services (IntServ) for an alternate approach that preceded DiffServ. Multi-Protocol Label Switching (see MPLS) is an entirely different approach that maps Layer 3 traffic to connection-oriented Layer 2 transports such as ATM.

Digital Wrapper

See G.709.

DNS Domain Name System

Based on IETF [RFC1033](#) DNS is a distributed database system for translating names of Internet host computers into IP addresses. A DNS server computer maintains a database for resolving host names into IP addresses so that client computer users can address a remote computer by its host name (such as [www.anritsu.com](#)) rather than its complicated numerical IP address. The [DNS Resources Directory](#) provides extensive online technical information and news about DNS. Also see DDNS.

DNS also allows a host computer that is not directly on the Internet to have the same style of registered name. DNS normally only works with static IP addresses. DHCP allows dynamically assigned IP addresses to be tracked by DNS servers – see DHCP.

DS Digital Signal

A system of classifying digital circuits according to the rate and format of the signal (DS) and the equipment providing the signals (T). DS and T designations have come to be used synonymously so that DS1 implies T1, and DS3 implies T3. In SONET, STS is used for electrical formats and OC is used for optical formats.

Voice Channels in North America, Japan, Korea:

<u>Service</u>	<u>Channels</u>	<u>Speed</u>
DS0	1	64 Kbps
DS1	24	1.544 Mbps (T1)
DS1C	48	3.152 Mbps (T1C)
DS2	96	6.312 Mbps (T2)
DS3	672	44.736 Mbps (T3)
DS4	4032	274.176 Mbps (T4)

Voice Channels in Europe and the ITU:

<u>Service</u>	<u>Channels</u>	<u>Speed</u>
E1	30	2.048 Mbps
E2	120	8.448 Mbps
E3	480	34.368 Mbps
E4	1920	139.264 Mbps
E5	7680	565.148 Mbps

SONET and SDH Circuits:

<u>U.S. SONET Level</u>	<u>ITU SDH Level</u>	<u>Speed</u>	<u>Usable Payload Capacity in Concatenated Format (c)</u>
STS/OC-1		51.84 Mbps (28 DS1 or 1 DS3)	
STS/OC-3	STM-1	155.52 Mbps (3 STS-1)	149.76 Mbps
STS/OC-12	STM-4	622.08 Mbps (12 STS-1)	599.04 Mbps
STS/OC-48	STM-16	2.4883 Gbps (48 STS-1)	2.39616 Gbps
STS/OC-192	STM-64	9.9533 Gbps (192 STS-1)	9.58464 Gbps
STS/OC-768	STM-256	39.813 Gbps (768 STS-1)	
STS/OC-1536	STM-512	79.626 Gbps (1536 STS-1)	

A “c” suffix on STS and OC rates (such as OC-12c) signifies a concatenated format where the payloads from a number of STS-1 equivalent frames are combined to create one higher-capacity channel with less SONET overhead.

DSCP Differentiated Services Codepoint

See DiffServ (Differentiated Services).

DVMRP Distance Vector Multicast Routing Protocol

A routing protocol for IP multicast based on IETF experimental standard [RFC1075](#). DVMRP is the protocol currently used on the MBONE (Multicast Backbone), a global experimental network of routers that support IP multicasting. DVMRP maintains its own routing tables that are distinct from unicast routing tables. DVMRP is considered a “dense mode” protocol -- it relies on flooding to propagate information to all routers on the network.

Issues Because DVMRP uses its own routing tables, there can be differences between the multicast and unicast routing tables so that multicast and unicast traffic may not follow the same routes. Some people have the opinion that DVMRP behaves poorly in large networks because its overhead consumes too much bandwidth and multicast packets are sent to people who don't want them.

DWDM Dense Wavelength Division Multiplexing

See WDM (Wavelength Division Multiplexing)

E1

For E1 through E5, see DS (Digital Signal).

ECMP Equal-Cost Multipath Routing

A routing protocol variation that allows multiple paths between routing points that each have the same assigned cost. Traditional routing schemes assigned all traffic to a single path, even if other paths were available. With ECMP, routed traffic can be distributed across all multiple paths so that both load balancing and redundancy are achieved. ECMP for OSPF v2 is described in [RFC2328](#).

EGP Exterior Gateway Protocol

A generic term for protocols that broadcast TCP/IP addresses to the gateway in another network, and the name of a specific such protocol that has been replaced in the Internet by BGP (Border Gateway Protocol) -- see BGP.

EIGRP Enhanced Interior Gateway Routing Protocol

Cisco's newest version of its proprietary routing algorithm IGRP. It provides better convergence properties and operating efficiency than IGRP, and claims to combine the advantages of link state protocols (such as OSPF) with the advantages of distance vector protocols (such as RIP).

EoS Ethernet Over SONET/SDH

EoS is not a single standard; there are various processes for transporting Ethernet over SONET or SDH. See BCP (Bridging Control Protocol), EoS-VC (Ethernet Over SONET Virtual Concatenation), GFP (Generic Framing Protocol), LAPF (Link Access Procedure-Frame Mode), LAPS (Link Access Procedure-SDH), and LEX (LAN Extension Protocol). [CommsDesign](#) provides a helpful tutorial on EoS.

EoS-VC Ethernet Over SONET/SDH Virtual Concatenation

Until recently, the primary way to transport Ethernet frames across a SONET/SDH network was by mapping them into fixed sized SONET Synchronous Payload Envelopes (SPE) or SDH Virtual Containers (VC). Because of the bandwidth mismatch between Ethernet and SONET/SDH, this is inefficient, inflexible, and expensive compared to native Ethernet Layer 2 switching or ATM. EoS-VC, defined by the G.7041 Generic Framing Procedure (see GFP) of the [ANSI T1X1.5](#) subcommittee, combines a number of noncontiguous, fixed-size SPEs or VCs into a single virtual payload of a higher combined capacity known as an EoS-VC group. Also see LCAS (Link Capacity Adjustment Scheme).

- STS-m-nv designates high-order SONET virtual concatenation rates, where "nv" indicates the multiple n of the "STS-m" base rate. Example: STS-3c-7v designates 7 x STS-3c rate, which is around 1 Gbps and appropriate for transporting Gigabit Ethernet.
- VC-m-nv is similar for SDH, where "nv" indicates the multiple n of the "VC-m" base rate. Example: VC-4-7v designates 7 x VC-4 rate, which is equivalent to STS-3c-7v above.
- VT-m-nv designates low-order virtual concatenation rates, based on multiples of the VT-1.5 or VT-2 virtual tributary rates. Example: VT-1.5-7v designates 7 x VT-1.5 rate.

ESCON Enterprise System Connection (IBM)

An IBM storage networking legacy protocol for disk storage that preceded Fibre Channel. ESCON is a 200 Mbps unidirectional serial transmission protocol used to dynamically connect mainframes with their various control units, with connections limited to around 9 km for best performance. Also see FICON.

EtherChannel

A proprietary scheme for link aggregation (trunking) developed by Cisco. See 802.3ad (standard Link Aggregation).

Ethernet Data Rates

Ethernet packets (or "frames") traditionally have a minimum length of 64 Bytes and a maximum length of 1518 Bytes. Optional VLAN tagging, developed a few years ago, adds 4 Bytes to every packet so that VLAN tagged packets are 68-1522 Bytes long – see 802.1Q. There are four standard Ethernet data rates, resulting in these bit, byte, and gap timings:

	<u>10 Mbps</u>	<u>100 Mbps</u>	<u>1 Gbps</u>	<u>10 Gbps</u>
Bit time	0.1µs	0.01µs/10ns	0.001µs/1ns	0.1ns
Byte time	0.8µs	0.08µs/80ns	0.008µs/8ns	0.8ns
64 Byte time	51.2µs	5.12µs	0.512µs	512ns
1518 Byte time	1.21ms	121µs	12.1µs	1.21µs

Minimum inter-packet gap time (96 bits)	9.6µs	0.96µs	0.096µs/96ns	9.6ns
---	-------	--------	--------------	-------

There is a minimum "inter-packet" gap time between Ethernet packets that corresponds to 96 bits (12 Bytes) plus an 8 Byte preamble to each packet; these are not counted in the 64-1518 Byte packet length. Based on this gap and preamble overhead and the above timings, the maximum packet per second (pps) data rates for various lengths of Ethernet packets are:

	10 Mbps	100 Mbps	1 Gbps	10 Gbps
64 Byte packets	14,880 pps	148.8 Kpps	1.488 Mpps	14.88 Mpps
512 Byte packets	2,347 pps	23.47 Kpps	234.7 Kpps	2.347 Mpps
1518 Byte packets	812.7 pps	8.127 Kpps	81.27 Kpps	812.7 Kpps

You can compute the maximum bit throughput by multiplying pps x (packet length in Bytes) x (8 bits/Byte). For 64 Byte packets and 1 Gigabit Ethernet, the maximum throughput is 1.488 Mpps x 64 Bytes/packet x 8 bits/Byte = 761 Mbits/sec., or 76% of the theoretical bandwidth; the other 24% is lost to the gap and preamble overhead. The percentage lost to overhead for the longest 1518 Byte packets is much less (13%) because the overhead remains constant at 20 Bytes.

FANP Flow Attribute Notification Protocol

Based on standard [RFC2129](#) first published in 4/97: cell-switched routers use the FANP protocol proposed by Toshiba as well as native ATM signaling to establish the virtual path/virtual channel (VP/VC) links between nodes. Default-VC is a general-purpose virtual circuit between neighboring nodes used for conventional hop-by-hop forwarded traffic, including routing messages, RSVP messages and Flow Attribute Notification Protocol (FANP) messages. For similar functionality MPOA (Multi-Protocol Over ATM) uses Q.931 and IP switching uses IFMP.

Fast Reroute (MPLS)

An IETF draft related to MPLS that allows for creating traffic backup paths, providing carriers with a cost-effective failure recovery mechanism and increased reliability in order to meet the needs of real-time applications such as VoIP, where it is desirable to be able to re-direct traffic onto backup paths in 10s of milliseconds. Fast Reroute uses RSVP and RSVP-TE to establish explicitly-routed backup paths to repair primary explicitly-routed paths that fail. The backup paths are to be as close to the failure point as possible to avoid significant delay from reporting failure between nodes. [Isocore](#) is organizing the first public demonstration of MPLS Fast Reroute interoperability in October '02.

FCIP Fibre Channel Over TCP/IP

An IETF [draft](#) protocol that links Fibre Channel (FC) storage area networks over TCP/IP networks and enables existing FC mechanisms and infrastructure to be leveraged for IP storage networking. FCIP uses existing FC switches and end devices, tunneling the entire FC stack over TCP. Scalability is thus limited by FC technology, with not more than 8-10 FC switches in each joined fabric. iFCP is an alternate proposal for a similar process (see iFCP).

FICON Fiber Connection (IBM)

The next generation of the IBM storage networking legacy protocol ESCON for connecting mainframes with storage control units. FICON is a bidirectional channel protocol that runs over Fibre Channel at 1.062 Gbps, supports a switch topology, and operates up to 100 km. There has been relatively little deployment of FICON, however. See ESCON.

FTP File Transfer Protocol

An application protocol that is used for transferring files between network nodes. FTP is part of the TCP/IP protocol stack and is defined by standard [RFC959](#). See TCP/IP and TFTP.

G.709 Digital Wrapper

Provides a flexible and protocol-independent "container" for efficiently transporting virtually any type of data across DWDM optical links in an Optical Transport Network (OTN). The objective of an OTN is to combine the benefits of SONET/SDH technology with the bandwidth expansion provided by DWDM to enable the multi-service transport of both packet based and legacy traffic. G.709 defines a structure in which forward error correction (which is essential to counteract the effects of optical channel errors at high data rates) as well as optical channel overhead functions are specified separately from the data payload, overcoming limitations of SONET and SDH. The ITU-T approved G.709 (Network Node Interface for the Optical Transport Network-OTN) in February 2001. It is expected to enable important interoperability and management technologies for DWDM optical networks. G.709 requires new hardware that will be a challenge for some capital-constrained service providers with large SONET investments. The 10.709 Gbps and 43.125 Gbps G.709 interfaces will probably be most popular; these rates are 7% higher than their respective SONET rates because of FEC. A good [tutorial](#) and helpful [article](#) by AMC about G.709 are available. Acterna has a good [white paper](#) describing OTN.

GARP Generic Attributes Registration Protocol

Defined by 802.1p. There are two versions of this protocol. The first version is the GARP Multicast Registration Protocol

(GMRP), which lets workstations request membership in a multicast domain. This joining action is called a leaf-initiated join. GMRP provides a standard protocol for sending traffic to only those ports that have requested multicast traffic. It is compatible with 802.1Q because the protocol operates on a port basis.

The second version is the GARP VLAN Registration Protocol (GVRP). Under GVRP a workstation requests admission to a specific VLAN rather than to a multicast domain.

This protocol links 802.1p and 802.1Q -- see 802.1p and 802.1Q.

GBIC Gigabit Interface Converter

A small hardware module that handles the internal interface to a Gigabit Ethernet port connection. Some vendors use this technology in Gigabit Ethernet products to provide flexibility so that one interface module can handle different kinds of fiber or copper physical interfaces depending on which GBIC module is installed, but this approach usually increases the total cost of the interface.

GFP Generic Framing Procedure

A robust and efficient packet transport mechanism standard (G.7041) in [ANSI T1X1.5](#) that provides better performance than Packet Over SONET (see POS) and is directly applicable to DWDM. Its mapping is intended to operate only over point-to-point connections and is transparent to Layer 2 and higher layers. It is not limited to SONET/SDH nor tied to any specific physical layer. The GFP standard defines Ethernet over SONET Virtual Concatenation – see EoS-VC. In frame-based GFP, a single data frame (such as an Ethernet MAC frame or an IP packet) is mapped into a single GFP frame. Transparent GFP is a different process that maps a fixed number of data characters into a GFP frame of pre-determined length and transparently transports 8B/10B control characters. Transparent GFP ensures deterministic latency and is primarily targeted at storage area networking where latency is critical. Resilient Packet Ring (see 802.17) carried over SONET/SDH supports both GFP and POS framing.

GMPLS Generalized Multi-Protocol Label Switching

Proposal to extend MPLS control plane concepts to general connection provisioning in multiple technology domains. MPLS concentrates on IP-over-optical applications, mapping intelligent packet flows onto optical wavelengths. GMPLS extends the idea of MPLS label-switched path techniques to controlling light paths (wavelengths) as well as TDM and SONET/SDH networks. (See MPLS and MPLS.)

GMRP GARP Multicast Registration Protocol

Allows workstations to request membership in a multicast domain in order to reduce multicast flooding a network. GMRP provides a standard protocol for sending traffic to only those ports on a switch that have end stations requesting multicast traffic. See GARP.

GPRS General Packet Radio Service

GPRS functions as a data services upgrade to [GSM digital cellular networks](#), providing "always-on", higher capacity, Internet-based content and packet-based data services. This enables services such as color Internet browsing and e-mail on the move. GPRS uses a packet-mode technique to transfer bursty traffic in an efficient manner. GPRS supports four different quality of service levels. Deployment started in 1999.

GRE Generic Route Encapsulation

The Generic Routing Encapsulation (GRE) protocol provides a mechanism for encapsulating arbitrary packets within an arbitrary transport protocol. The payload is first encapsulated in a GRE packet, which possibly also includes a route. The resulting GRE packet is then encapsulated in some other protocol (the delivery protocol) and forwarded. GRE is used in conjunction with Point-to-Point Tunneling Protocol (see PPTP) to create virtual private networks (VPNs) between clients or between clients and servers. The data or payload that is going to pass through the tunnel is given a PPP header and then placed inside a GRE packet. After the GRE packet has arrived at the final destination (the endpoint of the tunnel), it is discarded and the encapsulated packet is then transmitted to its final destination. GRE is an IETF Standards Track protocol defined by [RFC2784](#) and extended by [RFC2890](#).

GRE is a very simple, low-overhead approach lacking real authentication or tunnel configuration parameter negotiation. For additional functionality, Layer 2 Tunneling Protocol (see L2TP) essentially implements PPP over a GRE tunnel. In certain cases it may be useful to carry MPLS packets through a GRE tunnel, and the [IETF Internet draft](#) "MPLS Label Stack Encapsulation in GRE" describes this.

GSMP General Switch Management Protocol

Based on standard [RFC2297](#): Ipsilon's proposal for connecting a router to an ATM switch by telling the switch where to direct each IP flow. Ipsilon called this "IP Switching". See IFMP also. No longer applicable.

GTP GPRS Tunneling Protocol
See GPRS (General Packet Radio Service).

GUM Grand Unified Multicast
An IETF [draft](#) protocol used in connection with MBGP (Multicast Border Gateway Protocol) -- see MBGP.

GVRP GARP VLAN Registration Protocol
To establish VLANs in an environment of multiple switches, GVRP provides a protocol mechanism that lets the switches dynamically establish and update their knowledge of the set of Virtual LANs that currently have active members. See GARP.

H.323
An ITU standard for videoconferencing over LANs, other packet-switched networks, and the Internet. It provides for sending any combination of real-time voice, video, and data. Various standards within H.323 define how calls are set up, what audio and video compression (codec) schemes are permitted, and how to participate in conferences. H.323 runs on TCP.

Issues H.323 was not specifically designed with the Internet in mind and thus has some problems with scalability related to network size, the amount of information that gateways must maintain about calls, and lack of support for routing loop detection. H.323-based conference calls cause some problems because they require a separate multicast distribution server. Furthermore, the call setup process is long and complex. Also see MGCP (Media Gateway Control Protocol) and SIP (Session Initiation Protocol) -- these are alternate VOIP protocols created by the IETF specifically for the Internet.

HMMP Hypermedia Management Protocol
A common access language that applications can use to access Web-based management data stored in a CIM (Common Information Model) database. Definition of HMMP is expected to start after the definition of CIM v2.0 is complete. See CIM.

HSRP Hot Standby Router Protocol
A proprietary protocol by vendors including Cisco and Foundry to provide backup protection for routers. The comparable industry standard protocol is Virtual Router Redundancy Protocol (see VRRP).

HTTP Hypertext Transfer Protocol
An application-level protocol for distributed, collaborative systems that has been in use on the world-wide web since 1990. This is the protocol used by web clients such as browsers to access and retrieve information from web servers and link to other documents. Version 1.0 was defined by [RFC1945](#). Version 1.1 ([RFC2068](#)) adds cache control and various network efficiencies such as allowing a single TCP connection to retrieve multiple objects from a server without remaking the connection between each retrieval.

ICMP Internet Control Message Protocol
An IETF protocol based on [RFC792](#) that provides a number of diagnostic functions including sending error packets to hosts and sending PING messages. ICMP uses the basic support of IP and is an integral part of IP. [ICMP Redirect](#) is a process whereby a router informs a host computer that there is a better route from that host to a specific destination than via that host's default router (default gateway). ICMPv6 ([RFC1885](#)) is the new version that is integral to IPv6. It includes functions from IGMP and is required in every IPv6 node.

IDRP Inter-Domain Routing Protocol
An Exterior Gateway Protocol that exchanges only pre-specified information among selected routers. It has been replaced in the Internet by BGP (Border Gateway Protocol) -- see BGP.

iFCP Internet Fibre Channel Protocol
An IETF [draft](#) protocol that links Fibre Channel storage area devices over TCP/IP networks and enables existing Fibre Channel mechanisms and infrastructure to be leveraged for IP storage networking. iFCP uses existing Fibre Channel end devices, which are relatively expensive, but replaces Fibre Channel switches using the iSNS protocol to accomplish their fabric services (see iSNS). FCIP is an alternate protocol for a similar process.

IFMP Ipsilon Flow Management Protocol
Based on IETF [RFC1953](#): Ipsilon's proposed IP Switching protocol between two adjacent nodes. No longer applicable.

IGMP Internet Group Management Protocol
A protocol used by IP hosts to report their multicast group memberships to an adjacent multicast router.
v1—Provides a simple Group Join with fixed timeout. The router sends periodic queries to determine when users no longer exist on LAN segment. This version, defined by IETF [RFC1112](#), was widely deployed. It does not provide any way to explicitly

stop traffic or leave the group.

v2—"Leave Group Message" function added: Host indicates that it is leaving the group. The router can respond by sending a Group Query message to determine if other recipients remain in the subnet, which is quicker than the timeout scheme required in v1. This version is defined by [RFC2236](#) and is being implemented. Microsoft has a test version for Win95.

v3—Allows receivers to specify desired sources, and exclude unwanted sources. This is still experimental and not formally implemented yet, defined by IETF [draft](#).

IGMP Snooping is a scheme where a workgroup switch examines traffic from attached end stations to determine multicast group membership. It then automatically filters traffic to provide selective delivery of IP multicast traffic to appropriate group members only. See CGMP.

IGRP Interior Gateway Routing Protocol

A proprietary distance-vector routing protocol developed by Cisco for use in large, heterogeneous networks.

IKE Internet Key Exchange

A security key management protocol standard used in conjunction with security protocols such as IPsec (see IPsec).

IMA Inverse Multiplexing for ATM

An ATM Forum [specification](#) approved in July 1997 that defines a mechanism for dividing a single high-speed stream of ATM cells across multiple lower-speed links, and then recombining the cells into a single stream at the other end. This allows several low-speed links to be combined to achieve the performance and functionality of a single higher-speed link. For example, a single T-1 link is often too slow but T-3 or OC-3 speeds may be too expensive. IMA allows a second T-1 link to be added to achieve twice the bandwidth without incurring the cost of upgrading all the way to T-3. See 802.3ad regarding a similar scheme for combining frame-based links.

IMIX Internet MIX

The "Internet MIX" or IMIX is a well-known packet mix representative of Internet traffic that includes 40-byte IP datagrams (58 percent), 552-byte IP datagrams (33 percent), and 1500-byte IP datagrams (9 percent). Thus for every 12 packets, 7 have 40-byte IP payload (padded to 46-byte payload on Ethernet), 4 have 552-byte IP payload, and 1 has 1500-byte IP payload. Therefore, IMIX traffic is also referred to as traffic with 7:4:1 distribution. Cisco focuses on IMIX in the development of their routing and switching products. Automated test suites from Adtech, SmartBits, and Ixia enable IMIX test cases.

IntServ Integrated Services

An IP traffic classification scheme being developed by the IETF that will provide per-flow classification and guaranteed delays to support real-time traffic. It must be implemented by each router in the network. RSVP is the signaling protocol that is used to communicate to the routers. (See RSVP.) The IntServ charter is explained at www.ietf.org/html.charters/diffserv-charter.html. The IntServ Guaranteed Service definition incorporates Weighted Fair Queuing (see WFQ) with Random Early Detection (see RED) and the RSVP protocol. The IntServ Controlled Load Service omits WFQ and the RSVP protocol.

Issues This is an elaborate scheme requiring substantial equipment changes and much more definition. Many vendors feel that Differentiated Services provides an adequate solution, and is clearly much more feasible to implement (see DiffServ).

IP Internet Protocol

Based on IETF [RFC791](#): the TCP/IP standard protocol that defines the IP datagram. It is used in gateways to connect networks at Layer 3. See TCP/IP. IPv4 (version 4) is standard today. See IPv6.

IP Address

The Layer 3 address of a host (computer) attached to a TCP/IP network. Every host must have a unique IP address. IP addresses are 32-bit values written as four sets of decimal numbers separated by periods; for example, 125.6.65.7. Each decimal number (0-255) represents 8 bits of the complete 32-bit value.

The TCP/IP packet uses 32 bits to contain the IP address, which consists of a network address (netid) and a host address (hostid). The 32 bits are divided in different ways according to the class of the address, which determines the number of hosts that can be attached to the network. If more bits are used for the host addresses (such as in Class A), fewer bits are available for the network address. The three address classes support the following numbers of network and host addresses:

<u>IP Address Class</u>	<u>Number of Network Addresses</u>	<u>Number of Host Addresses</u>
A	128	16M
B	16K	65K
C	16M	256

Network addresses are supplied to organizations by the InterNIC Registration Service. See CIDR.

IPCP Internet Protocol Control Protocol

An IETF standard documented by [RFC1332](#) that defines the network control protocol for establishing and configuring IP over PPP (Point-to-Point Protocol) links.

IPFC IP Over Fibre Channel

An IETF effort to standardize the process of sending IP and ARP commands over Fibre Channel networks. This work is partly defined by the standards-track document [RFC2625](#).

IP Multi-Netting

A network architecture where two or more IP subnets exist on the same Ethernet segment. This capability was often important for traditional routers that had few Ethernet ports. The total bandwidth of the segment is shared among the subnets, and IP traffic between any two of the subnets must go out to a router and come back over the same port.

IPng IP Next Generation

IPng refers to the development effort for the next-generation IP protocol. The resulting protocol is named IPv6. See IPv6.

I-PNNI Integrated PNNI

An extension of the PNNI (Private Network-to-Network) protocol that ATM switches use to inform each other of their network topology so they can make appropriate forwarding decisions. I-PNNI is implemented in edge devices and legacy routers, which can share information with the ATM switches. See PNNI.

IPOA IP Over ATM

See "IP Over ATM" below.

IPOS IP Over SONET

See POS (Packet Over SONET).

IP Over ATM

Based on [RFC2225](#) (which obsoletes RFC1577): a scheme for sending classical IP and ARP (Address Resolution Protocol) traffic over ATM Adaptation Layer 5 (AAL5). This is also known as Classical IP Over ATM (CIP) and IPoA. Also see LANE (ATM LAN Emulation) and MPOA (Multiprotocol Over ATM).

IPSec IP Security

A suite of protocols that handles encryption, authentication, and secure transport of IP packets such as for VPNs. It is described in [RFCs 2401-2412](#) produced by the IETF IPsec working group (www.ietf.org/html.charters/ipsec-charter.html). The IPsec Developers Forum web site (www.ip-sec.com/) provides technical information and allows vendors to schedule interoperability testing. Microsoft provides IPsec clients for VPNs in Windows XP and Windows 2000. IPsec provides network-layer security for IPv4 and IPv6. The VPN Consortium (www.vpnc.org) has established an inexpensive test for conformance with basic IPsec protocols.

IPSec works at Layer 3 to transport data transparently to network applications. It is intended to provide more lower-level security than SSL (Secure Socket Layer). IPSec adds a header to packets being sent over a VPN to identify that those packets that have been secured. It supports several types of encryption including the Data Encryption Standard (DES) and triple DES (3DES), supports several types of authentication including Message Digest 5 (MD5, [RFC2403](#)) and SHA-1 ([RFC2404](#)), and several key management schemes that allow parties to agree upon parameters for the session. Current implementations mostly use manual key distribution, Public Key Infrastructure (PKI) key exchange, or the IKE (Internet Key Exchange) protocol, which requires each pair of nodes to be linked via a unique key and thus creates a need for a huge number of keys when there are many nodes. Support for the Advanced Encryption Standard still needs to be added (see AES).

Proposals call for adding additional security features. IPSec also provides for data compression, which partially compensates for the poor compression that modems are able to perform on encrypted data. IPSec does not provide support for NAT (Network Address Translation). IPsec requires every user to have a defined public IP address, so if IP addresses are shared using NAT the security privileges are also shared.

SSL works differently by operating at Layer 4 and focusing on the upper layers of the OSI model – see SSL. Also see PPTP.

IPv6 Internet Protocol Version 6

Based on standard [RFC1883](#) and [RFC1752](#): a new version of the IP protocol (see IP) that was designed to provide a solution

to the address space limitations of the current version IPv4. The 6BONE is a worldwide network begun around 1996 that runs IPv6 on an experimental basis: see www.6bone.net. The IPv6 Forum (www.ipv6forum.com) is a consortium dedicated to promoting IPv6. IPv6 was formerly known as IPng (IP Next Generation). IPv6-enabled devices will still forward IPv4 traffic, and there is a standard for encapsulating IPv4 information within a virtual tunnel between IPv6 devices.

IPv6 provides:

- 128-bit address space (increased from 32 bits)
- Automatic address configuration capability based on DHCPv6 that allows a host to discover automatically the information it needs to connect to the Internet or to a private TCP/IP network.
- A simplified packet header structure, with many fields optional
- Support for source-selected routes (like Token Ring's source routing)
- Scalable routing architectures
- Network-layer security
- Quality-of-service (QoS) levels
- Mobile computing capabilities
- Multicasting features.

Issues Additions to IPv4, such as Dynamic Host Configuration Protocol (see DHCP), and the development of address translators (see NAT-Network Address Translation) have given IPv4 a longer life than originally expected. IPv6 will be difficult to implement, but provides many new capabilities. Some say that its support for diverse network devices is not relevant to end users or that IPv6 does not offer enough security or quality of service improvements to warrant immediate adoption. Since IPv4 and NAT are already widely deployed, the IETF has issued documents that define a transitional edge router: DNS extensions to Network Address Translators (RFC2694); Stateless IP/ICMP Translation (RFC2765); NAT Protocol Translation (RFC2766); and Connection of IPv6 Domains via IPv4 Clouds (RFC3056).

Status Prospects for large-scale conversion from IPv4 to IPv6 improved in March 2000 when Microsoft and Cisco announced plans for IPv6 support. Cisco is shipping IPv6 support in its IOS software since June 2001, and promises hardware support in ASIC-based routers within the following 12 months. The next-generation European wireless initiative (3GPP) mandated IPv6 support in May 2000, but is only interested in the addressing features. Microsoft has released IPv6 tools for developers, and with USC/ISI-East is creating an IPv6 implementation for research purposes – see research.microsoft.com/msripv6. Microsoft support for IPv6 support is built into Windows XP. In March 2000 NTT became the first commercial ISP to announce IPv6 support. Sun bundles IPv6 support in Solaris 8; Linux and BSD Unix support IPv6. Compaq plans 2H'01 support in some of its server and e-mail clients, and IBM is developing IPv6 support for its S/390 Enterprise Server systems. Nortel plans native hardware IPv6 support in next-generation routing products, and Nokia is shipping IPv6 in IPSO 3.3.

IPX Internet Packet Exchange

Based on standard IPX Router Specification v1.2: a Novell NetWare communications protocol used to route messages from one node to another. Because IPX packets can get lost, IPX does not guarantee delivery of a message. Either the application or NetWare's SPX protocol has to provide the control to ensure that the entire message was received.

IPX-RIP and IPX-SAP

Based on standard IPX Router Specification v1.2: IPX dynamic routing protocols. See IPX.

IRDP ICMP Router Discovery Protocol

An extension of ICMP described in RFC1256 by which routers announce themselves to network hosts. Hosts can listen to IRDP broadcasts and learn IP addresses of neighboring routers through which they can send information to destinations outside their own subnet. See ICMP.

iSCSI Internet SCSI

The Small Computer Systems Interface (SCSI) is a popular family of protocols for communicating with computer I/O devices, especially storage devices. iSCSI is an IETF [draft](#) protocol for running SCSI over TCP/IP as a way to interconnect SANs (Storage Area Networks) over the Internet, and especially to connect servers to remote storage devices, completely replacing Fibre Channel switches. Version 1 of the standard is expected by January 2002. iSCSI is widely supported, and approximately 250 companies are developing related products.

IS-IS Intermediate System to Intermediate System

A hierarchical routing protocol that uses intermediate systems (routers) to exchange routing information based on a single metric to determine network topology. IS-IS is based on DECnet Phase V routing. IS-IS is a link state routing protocol like OSPF: all routers maintain identical databases so that they can compute the shortest path to any destination. Integrated IS-IS (formerly Dual IS-IS) is a routing protocol based on the OSI routing protocol IS-IS (see RFC1142). Support for IP is defined in RFC1195. Integrated IS-IS implementations send only one set of routing updates, regardless of protocol type, making it more

efficient than two separate implementations. The IETF IS-IS working group is at ietf.org/html.charters/isis-charter.html.

ISL InterSwitch Link

A Cisco proprietary protocol for VLAN trunking over link aggregated connections. Today, the industry standard 802.3ad (Link Aggregation) and 802.1Q (VLAN Tagging) protocols accomplish this without need for proprietary communications.

iSNS Internet Storage Name Service

An IETF [draft](#) protocol that provides the generic framework and naming service for storage entity management in an IP-based storage network. It incorporates existing Fibre Channel and DNS mechanisms and relies on standards-based, distributed directory databases such as the Lightweight Directory Access Protocol (LDAP). iSNS is used within the iSCSI and iFCP protocols (see iSCSI, iFCP).

ISSLL Integrated Services over Specific Link Layers

IETF [draft](#) protocol intended to add QoS (Quality of Service) capabilities to Layer 2 devices such as Ethernet and Token Ring switches. It includes a number of recommended service classes based on how much latency a packet can withstand. An application layer protocol like Resource Reservation Protocol (see RSVP) can be mapped on top of these service classes to create a complete system for controlling priority. The result is intended to be a network where an application can request QoS services from both Layer 3 and Layer 2 devices using RSVP.

Issues 802.1p is an unrelated standard by the IEEE that defines the details of Layer 2 traffic priorities (see 802.1p). Differentiated Services is an alternative standard being developed by the IETF that will operate at Layer 3 and has much broader industry support than ISSLL (see DiffServ).

ITU-T International Telecommunication Union – Telecommunication Standardization Sector

[ITU-T](#) is one of three sectors of the International Telecommunication Union (ITU). It was created in 1993 to replace the former International Telegraph and Telephone Consultative Committee (CCITT), whose origins go back to 1865. ITU-T's mission is to ensure production of high quality standards covering all fields of telecommunications.

Jumbo Frames

Ethernet frames that are extended beyond the standard maximum length of 1.5 KB to 9 KB in order to reduce server CPU overhead by reducing the number of different packets and interrupts that must be processed for a given number of bytes of data. Server overhead is a concern for Gigabit Ethernet because the packet (and thus interrupt) rates are very high, but there is considerable disagreement over whether jumbo frames are an appropriate solution.

Kompella Draft

See VPN (MPLS Layer 2 VPNs).

L2F Layer 2 Forwarding

A Cisco proprietary Layer 2 tunneling protocol – see L2TP.

L2TP Layer 2 Tunneling Protocol

The first proposed IETF protocol for tunneling Point-to-Point Protocol (PPP) across a private or public network. L2TP is defined by [RFC2661](#), and is the result of a merger of Microsoft PPTP, Cisco Layer 2 Forwarding (L2F), and IPsec. It provides point-to-point or point-to-multipoint links between customer locations. L2TP support for VPNs was first planned for Windows NT 5.0 (Windows 2000). L2TP is expected to receive broad industry acceptance in VPNs as a replacement to current proprietary protocols that do not allow equipment from multiple vendors to interoperate – see VPN. It enables support for multiple protocols and unregistered IP addresses, allowing existing non-IP protocol applications such as SNA to be used. In 8/98 Cisco announced support for L2TP in the Cisco IOS software. L2TP is a data-link layer protocol that creates one or more “tunnels” through an IP network between an L2TP Access Concentrator (LAC) and an L2TP Network Server (LNS). The tunnels carry traffic sessions over Point-to-Point Protocol (PPP) links. An authentication protocol (PAP or CHAP) and an optional encryption protocol (such as PPP Triple-DES) provide security.

L2TPv3 is in IETF [draft](#) status. It extends L2TP, which was focused on narrow-band dial-up links, by reducing overhead for better operation on high-speed routers, and increasing the number of supported tunnels from 65,000 to over 4 billion. Its objective is to allow traffic such as Frame Relay or ATM to travel across an IP or MPLS backbone.

LACP Link Aggregation Control Protocol

LACP is a protocol that operates at a new link aggregation sublayer to Layer 2 of the traditional Ethernet protocol stack. LACP is part of the 802.3ad Link Aggregation standard and handles automatically assigning ports to a Link Aggregation Group when all the ports at both ends of a physical link have the same characteristics. It also monitors existing groups and deletes ports whose characteristics have changed. See 802.3ad.

LANE ATM LAN Emulation

An ATM Forum [specification](#) defining services and protocols that allow Ethernet and Token Ring network traffic to be transported over an ATM backbone without modifying the Ethernet or Token Ring end stations. LANE includes these software services:

- LES (LAN Emulation Server), which handles the translation between classical Ethernet/Token Ring MAC addresses and ATM addresses;
- LECS (LAN Emulation Configuration Server), which assigns clients to emulated LANs; and
- BUS (Broadcast and Unknown Server), which handles multicast and broadcast traffic.

LANE operates at Layer 2 (Link Layer), and requires a router for sending traffic between subnets. LANE has been the de facto standard for transporting classical LAN services over an ATM network, but has significant limitations in fault tolerance and scalability. LANE 1.0 was the original version and was widely implemented. LANE 2.0 was adopted by the ATM Forum in July 1997 and adds QoS and multicast features, but has less vendor support.

MPOA (Multiprotocol Over ATM) is a newer standard built on top of LANE 2.0 that operates at Layer 3 (Network Layer) and incorporates ATM's PNNI routing. See MPOA.

LAPF Link Access Procedure-Framed Mode

ITU-T Q.922 protocol for Ethernet frame encapsulation and decapsulation over SONET/SDH. Also see GFP, LAPS.

LAPS Link Access Procedure-SDH

ITU-T X.86/X.85 protocol for Ethernet frame encapsulation and decapsulation over SDH. This provides a simple technique to connect Ethernet LANs and provide Ethernet LAN extension over a private and/or public SDH-based WAN. Also see GFP, LAPF.

LCAS Link Capacity Adjustment Scheme

A companion protocol to Ethernet over SONET virtual concatenation (see EoS-VC) that dynamically increases or decreases the number of SONET/SDH channels and thus control the guaranteed bandwidth being allocated. LCAS also provides fault tolerance by a process for detecting and removing faulty channels but allowing the link to continue to operate at reduced bandwidth. The ITU-T defined LCAS for use on either SONET/SDH or a G.709 Optical Transport Network (OTN -- see G.709).

LDAP Lightweight Directory Access Protocol

A protocol defined in IETF [RFC1777](#) that is used to access a directory listing in order to make multiple directories in an enterprise interoperable and manageable from a single point for policy-based network management. Based on current models an LDAP client (a PDP-Policy Decision Point) accesses a policy repository (a Directory) using the LDAP protocol, interprets the policy, and conveys it to an enforcer (a PEP-Policy Enforcement Point) such as a multilayer switch using the Common Open Policy Services protocol (see COPS). An LDAP client could be included within a multilayer switch or reside in a separate server. The current version is LDAP v3.0, defined by [RFC2251-2256](#) and 2829-2831.

There is widespread industry support for LDAP and for Directory Enabled Networking (see DEN) as the standard defining the structure of the directory it accesses. LDAP in switches can provide an alternative to DHCP. DHCP allows users to log on from any PC but it can be more difficult to implement policy services based on DHCP-issued IP addresses since multiple people reuse them. There are extensive Web resources describing LDAP: www.umich.edu/~dirsvcs/ldap/doc lists frequently-asked questions and LDAP documentation, and www.kingsmountain.com/ldapRoadmap.shtml contains a tutorial and guide to LDAP resources on the Internet.

LDP Label Distribution Protocol

An MPLS protocol that defines procedures and messages by which one LSR (Label Switched Router) informs another of the label bindings it has made. See MPLS. Also see CR-LDP and RSVP-TE.

LEAP Lightweight Extensible Authentication Protocol

A proprietary protocol somewhat like IEEE 802.1x created by Cisco to provide user authentication for its Aironet wireless LAN products. See 802.1x and 802.11.

LECS LAN Emulation Configuration Server

An ATM LAN Emulation service: see LANE (LAN Emulation).

LES LAN Emulation Server

An ATM LAN Emulation service: see LANE (LAN Emulation).

LEX LAN Extension Protocol for PPP

A LAN extension interface unit is a hardware device installed at a remote site that connects a LAN across a WAN serial link to a router at a central site. Based on informational [RFC1841](#) by Cisco, LEX is a protocol for transferring Ethernet MAC frames across this serial link, and few if any vendors other than Cisco implement it. This type of interface always depends on a host router, and cannot operate standalone like a bridge. LEX is a PPP (Point-to-Point Protocol) Network Control Protocol. Also see EoS (Ethernet over SONET).

MALLOC Multicast Address Allocation

An IETF [draft](#) protocol for dynamic multicast address allocation that includes MASC (Multicast Address Set Claim) and AAP (Address Allocation Protocol).

MAPOS Multiple Access Protocol over SONET/SDH

A proprietary connectionless POS protocol for sending IP traffic over SONET or SDH networks at speeds such as 155 or 622 Mbps without the overhead of ATM. Developed by NTT (Tokyo) and proposed to IETF in [RFC2171](#) through [RFC2176](#). A MAPOS Alliance and current status is described at www.mapos.org. Has no provisions for prioritizing traffic. See IPOS (IP Over SONET).

MARS Multicast Address Resolution Server

Based on IETF [RFC2022](#): a component of Multiprotocol Over ATM (MPOA) to efficiently support multiple network protocols over ATM. See MPOA. IETF [RFC2149](#) describes Multicast Server Architectures for MARS-based ATM multicasting.

Martini Draft

See VPN (MPLS Layer 2 VPNs).

MBGP Multicast Border Gateway Protocol

[IETF draft](#) protocol that contains extensions to BGP (Border Gateway Protocol) for IP multicast. This is a key to making IP multicast services on the Internet feasible. The North American Network Operator's Group completed interoperability testing of MBGP in late 1998. Also see MSDP (Multicast Source Distribution Protocol).

MD5 Message Digest 5

A security protocol for message authentication (for verifying data integrity) – see IPsec. SHA-1 is another popular authentication protocol.

MDHCP Multicast DHCP

Multicast version of DHCP (Dynamic Host Configuration Protocol) that is being widely implemented to allow users to request dynamic assignment of a multicast address. It is similar to DHCP, but directed to a different server. It uses regular DHCP to obtain the address of its MAAS server. See DHCP.

mFCP Metro Fibre Channel Protocol

An IETF [draft](#) protocol that transports the Fibre Channel Protocol for SCSI (FCP) over metro- and local-scale IP networks in order to achieve latency, reliability, and performance at levels comparable to those of a Fibre Channel network.

MFTP Multicast File Transport Protocol

A protocol for reliable data transport over IP multicast developed by StarBurst Communications and used in their StarBurst Multicast product. This protocol is designed specifically for file transfer rather than real-time applications such as videoconferencing. Typical applications of StarBurst Multicast are for software distribution, transferring business-critical information such as inventory, parts, pricing, and account information, and preventing degradation in multimedia files.

MGCP Media Gateway Control Protocol

The major VOIP protocol that will govern future interfaces between IP-based networks and traditional voice telephone networks (PSTN). MGCP is a combination of the Internet Protocol Device Control (IPDC) specification developed by a hardware/software vendor consortium formed by Level 3 Communications and the Simple Gateway Control Protocol (SGCP) that was developed by Bellcore and Cisco Systems. Draft specifications have been submitted to the IETF and the European Telecommunications Standards Institute. By mid-1999, at least 20 telco switching and internetworking hardware vendors had announced support for MGCP. Its companion VOIP protocol is Session Initiation Protocol -- see SIP.

The alternative H.323 protocol will apparently continue to play a role in enterprise videoconferencing and call setup (see H.323).

MLPPP Multilink PPP Protocol

A PPP (point-to-point) link protocol defined by [RFC1990](#) that provides a method for splitting, recombining, and sequencing datagrams sent across multiple logical data links when more bandwidth is needed than one link can supply. This was originally developed by creating multiple bearer (B) channels in ISDN, but is equally applicable to any situation in which multiple PPP links connect two systems.

MP Multilink PPP Protocol

See MLPPP.

MOSPF Multicast Open Shortest Path First

Based on IETF [RFC1584](#): a multicast routing protocol that embeds multicast routing information in OSPF link-state advertisements to determine distribution routes for each multicast source. As link states and group membership change, the routes are recalculated. MOSPF is thought to be more efficient than DVMRP, but it works only in OSPF networks.

MPLA Mutli-Point Link Aggregation

Link aggregation creates a single high-speed logical link (or trunk) that combines several lower-speed physical links. MPLA goes beyond this to allow trunks to span multiple switches and traverse divergent network paths, allowing a network to recover from the complete failure of a switch by redirecting traffic to an entirely different path.

MPLA originally consisted of proprietary extensions to the IEEE 802.3ad Link Aggregation standard proposed by 3Com and implemented in several 3Com products. There are indications that vendors such as Cabletron, Cisco, and Nortel are joining in support of MPLA technology and a standardization effort. See 802.3ad.

MPLS Multi-Protocol Label Switching

MPLS is designed to speed operation of routers performing IP switching in the core of the Internet and replace similar proprietary approaches such as Tag Switching (Cisco), IP Navigator (Ascend), ARIS (IBM), IP Switching (Ipsilon), and Cell Switch Routing (Toshiba). Its key concept is separating routing, performed only at Label Edge Routers (LERs) at the network edge, from forwarding that is performed by Label Switch Routers (LSRs) throughout the network core. A major initial justification for MPLS was the need to handle large-scale IP networks over the ATM core that will continue to exist within service providers' networks, since providing a full mesh of ATM virtual circuits between all nodes in a large ISP network is not practical. MPLS was intended to provide end-to-end IP services that can scale gracefully to large ATM networks, although it is not limited to either IP or ATM networks. Providers are not expected to deliver MPLS directly to end users, so most enterprise routers will not have to support MPLS directly. See GMPLS and MP λ S also.

Standard development is underway within IETF, and the MPLS charter is explained at www.ietf.org/html.charters/mpls-charter.html. In March 2000 16 companies formed the [MPLS Forum](#) to accelerate interoperability testing and deployment of MPLS. UUNET announced that it will start replacing its existing ATM core backbone with one based on MPLS in Q3'99.

The MPLS edge router (LER) determines the routing and assigns the traffic to a Forwarding Equivalence Class (FEC) based on traffic requirements such as VPN or QoS. MPLS uses the same routing protocols as IP, such as OSPF and IS-IS. The LER attaches a label to each packet identifying its path through the network and its attributes such as QoS, and uses the Label Distribution Protocol (LDP) to associate labels with paths through the switching nodes (LSRs). Each MPLS LSR uses the packet's label to look up the correct output port and priority in its Label Information Base (LIB), and thus can theoretically be much simpler and faster than a full-function IP router. Security is dealt with separately: packets underneath the label can be encrypted with existing methods.

The key capabilities of MPLS that have become important recently include:

- Explicit routing (traffic engineering), the ability to force traffic along paths other than the shortest ones selected by current IP routing algorithms. Either the RSVP-TE or CR-LDP signaling protocol can be used to automate this process. Cisco chose to implement RSVP-TE first, but the protocols are very similar and most vendors will implement both.
- Virtual private networks (VPNs) using labels to hide potentially-conflicting overlapping IP addresses, and leveraging the QoS capability of MPLS. MPLS should allow network service providers to reduce the costs associated with providing VPNs. MPLS also allows ISPs to concatenate traffic onto a single router from various enterprises that may have the same IP addresses in their respective backbones. MPLS provides for both Layer 2 and Layer 3 VPNs – see VPN.

MP λ S Multi-Protocol Lambda Switching

An effort within IETF to investigate how the MPLS control plane can be extended to optical switching. See MPLS and GMPLS.

MPOA Multiprotocol over ATM

An ATM Forum [specification](#) that provides routing of legacy protocols such as IP and IPX over ATM networks. The MPOA specification consists of three components:

- Route Servers perform the routing function between the Hosts and Edge Devices on an MPOA-enabled network. A server is typically either a stand-alone workstation or is integrated into another ATM device.
- Edge Devices connect traditional networks, such as Ethernet and Token-Ring, to ATM networks.
- ATM Hosts are MPOA-enhanced LAN Emulation hosts that are directly attached to MPOA networks.

The route server learns the Layer 3 addresses that can be reached through various ATM addresses and makes all the routing decisions in an MPOA network, leveraging ATM's PNNI routing capabilities (see PNNI). Initially, the server routes packets itself. If the server detects a large amount of traffic for a particular session, it can divert the data flow to a direct virtual circuit, allowing the two stations to bypass the server and communicate directly with each other. This is known as cut-through routing.

MPOA addresses the loss of performance caused by the increased number of router hops that packets make as traditional routed networks become more complex. Although the traffic in an MPOA network may go through several hops in the virtual circuit, traditional routing information does not have to be considered at each hop so performance is expected to improve. MPOA uses NHRP (Next Hop Routing Protocol) to enable Layer 3 protocols to run over ATM networks – see NHRP. MPOA v1.1 was scheduled for final ballot on 4/99. MPOA is built on top of LANE 2.0; see LANE (ATM LAN Emulation). Also see Multiprotocol Encapsulation Over ATM AAL5.

MSDP Multicast Source Distribution Protocol

A IETF [draft](#) protocol that is one of the keys to making IP multicast services on the Internet feasible. MSDP allows one domain to advertise its interest in multicast addresses to another domain. MSDP works in conjunction with MBGP (Multicast Border Gateway Protocol).

MST Multiple Spanning Trees for VLANs

“MST” is a term used in the developing IEEE 802.1s standard to refer to multiple spanning trees; see 802.1s. However, Cisco uses “MST” in the documentation on their proprietary PVST (Per-VLAN Spanning Tree) protocol to mean “Mono Spanning Tree”.

MTU Maximum Transmission Unit

The longest physical packet size that can be sent over a specific network. The MTU of most Ethernet networks is 1500 bytes; the MTU of X.25 networks is 576 bytes. Path MTU Discovery is a process defined by [RFC1191](#) for dynamically discovering the smallest MTU of any link between two arbitrary network hosts.

Multihoming

When applied to network interface cards (NICs) and servers, multihoming has two meanings:

- Multihoming is used to bind multiple IP addresses to a single NIC. This allows Web servers to use a single server host for multiple virtual Web sites.
- Multihoming also applies to the installation of two or more network adapters (NICs) in a server where each is attached to a separate network segment. When the multiple NICs are attached to the same network segment you can have a different IP address/host name bound to each NIC. Both these multiple-NIC schemes provide some load-balancing and fault tolerance.

Multihoming also refers to enterprises that have multiple Internet connections, often through different service providers. This provides greater fault tolerance, reduces concerns about service provider financial failures, and allows new route control and smart routing products (see www.nanog.org/mtg0206/smart.html) to offer improved performance and lower costs.

Multiprotocol Encapsulation Over ATM AAL5

Based on IETF [RFC2684](#) (which replaces and obsoletes RFC1483), this specifies two encapsulation methods for carrying network interconnect traffic over ATM using ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual connection, and the second method assumes that each protocol is carried over a separate ATM virtual connection. Also, refer to these other earlier specifications developed by the IETF or ATM Forum that addressed various aspects of bridged or routed protocols over ATM: IP Over ATM; LANE (ATM LAN Emulation); and MPOA (Multiprotocol Over ATM).

Multiservice Networking

A single converged product for carriers and service providers that supports a variety of services and networks that traditionally required separate devices such as ATM and frame relay switches, TDM and SONET muxes, IP routers, DWDM muxes, and voice circuit switches. The [Multiservice Switching Forum](#), originally founded by Cisco, WorldCom, and Telcordia in 1998, is developing intra-switch protocols and interface standards. However, unique internal architectures and product differentiation may make vendors unwilling to cooperate sufficiently.

NAT Network Address Translation

Based on IETF [RFC1631](#): Converts the internal private IP addresses of an enterprise back and forth from a single public IP

address that is valid on the Internet. This allows the enterprise to be represented externally by a single public address while using different internal IP addresses that do not conform to global standards. NAT helps extend the limited public IP address space, provides important security by masking host addresses that are inside the enterprise, and simplifying organizational changes that result in overlapping IP addresses.

NAT provides VPN functions by translating private IP addresses to global IP addresses in order to traverse a global network. Two address ranges are set up: one for the internal (private) network and one for the external (global) network. A firewall maintains a table that maps the internal to external numbers.

Issues NAT makes end-to-end authentication using IPsec unfeasible because NAT changes the packet addressing (see IPsec).

NDP Neighbor Discovery Protocol

An IPv6 protocol used to discover the Data Link Layer addresses of neighbors on attached links. It incorporates the functions of IPv4, ARP, ICMP Router Discovery messages, and ICMP Redirect messages. It replaces ARP, which doesn't exist in IPv6. See IPv6.

NEBS Network Equipment Buildings Standard

Defines a rigid and extensive set of performance, quality, environmental, and safety requirements for network equipment housed in carrier facilities. NEBS was developed by Telcordia (formerly Bellcore), the R&D and standards organization once owned by the Regional Bell Operating Companies (RBOCs).

NFS Network File System

A client/server protocol for accessing a network file system and standardized by the IETF in RFC1094 (NFSv2), RFC1813 (NFSv3), and RFC3010 (NFSv4). NFS is designed to allow any OS to access files.

NHRP Next Hop Routing Protocol

Defined by IETF [RFC2332](#): specifies how an end station finds out the IP address of either a destination node or the next router on the way to the target destination. MPOA uses NHRP to enable Layer 3 protocols to run over ATM networks – see MPOA. ARA (Address Resolution Advertisement) is an alternative scheme: see ARA.

NLSP NetWare Link Services Protocol

A link state routing protocol developed by Novell to improve handling of IPX traffic in large networks by reducing wasted bandwidth that is associated with the IPX-RIP routing protocol. Link state protocols, such as NLSP and OSPF, exchange routing table updates with neighboring routers only when there are changes to the tables. Distance vector protocols, such as RIP and IPX-RIP, exchange updates periodically whether changes occurred or not and thus consume more bandwidth in large networks with many routers and clients. NLSP was available for NetWare v3.11 and was first bundled in NetWare v3.2.

NTP Network Time Protocol

A TCP/IP-based protocol that allows any device to keep an accurate local time by referencing any time server on the Internet that has a very accurate radio or atomic clock. The local device measures the round-trip transit time from itself to the time server and uses that to adjust the time that the server reports. SNTP (Simple Network Time Protocol) is a simplified version of NTP that is described by [RFC1769](#).

OC-1

For OC-1 through OC-768, see DS (Digital Signal).

OMP Optimized Multipath

A new OSPF routing service to use loading information to distribute traffic across multiple links that have equal cost. This is currently an IETF [draft](#) protocol.

OTN Optical Transport Network

See G.709 Digital Wrapper.

OSPF Open Shortest Path First

Based on IETF [RFC2328](#) (which obsoletes RFC2178), OSPF is a link state routing protocol that determines the best path for routing IP traffic over a TCP/IP network. It was developed to create less route-calculation traffic between routers than the RIP protocol. Features include least-cost routing, multipath routing, and load balancing. The IETF OSPF working group is at [ietf.org/html.charters/ospf-charter.html](#). Also see MOSPF (Multicast OSPF). OSPFv3 is an updated version with minor changes that accommodate IPv6 – see IPv6.

PBNM Policy-Based Network Management

A generic term referring to an initiative to address methods of network management based on policies such as service-level agreements and quality of service (QoS) from a multivendor perspective. PBNM is intended to allow management of the conditions under which a user or application may have access to resources such as bandwidth, VLANs, and multicasting. PBNM complies with the standards for LDAP, RSVP, and COPS. HP, Intel, Cisco, and others began work on PBNM around mid-1998. See LDAP, RSVP, and COPS.

PGM Pragmatic General Multicast

A reliable transport protocol for IP Multicast developed by Cisco with contributions from Tibco Software Inc., submitted to IETF as a [draft](#) protocol. Also known as “Pretty Good Multicast”. Cisco and [Tibco Software](#) Inc. are supporting it.

PKI Public Key Infrastructure

A security key management protocol standard used in conjunction with security protocols such as IPsec (see IPsec).

PIM Protocol-Independent Multicast

A multicast routing architecture defined by the IETF that enables IP multicast routing on existing IP networks. Its key point is its independence from any underlying unicast protocol such as OSPF or BGP. Two versions are defined: v1 and v2. Many router vendors either already support PIM or plan to soon. A few ISPs are beginning to deploy PIM in their backbones: GTE Internetworking has already switched to PIM. See netweb.usc.edu/pim for an overview of PIM and links to related web sites.

The Protocol-Independent Multicast Dense-Mode protocol is known as PIM-DM and is an IETF [draft](#) protocol. Dense Mode is similar to DVMRP and best suited to stable multicast groups containing few senders and many receivers. For sparser networks with widely scattered groups and frequently changing memberships, a sparse version called PIM-SM (defined by [RFC2362](#)) can be used.

PNNI Private Network-to-Network Interface

A routing protocol for ATM that provides automatic load balancing, implicit capability for redundant links, and trunking capability. It is used between ATM switches in an ATM network that lets the switches inform each other about network topology so they can make appropriate forwarding decisions. PNNI-1 allows dynamic routing decisions to handle failed links or switches; PNNI-0 was an earlier interim specification that provided only static routing. See I-PNNI.

POS Packet Over SONET/SDH

A protocol defined by [RFC2615](#) for carrying IP traffic directly over SONET/SDH and avoiding the “cell tax” overhead of ATM. IP Over SONET (IPOS) refers to the same thing. With POS, IP runs over PPP (Point-to-Point Protocol – see PPP) and then over SONET/SDH without incurring ATM’s overhead from fixed-length cells that normally increase the data transferred by 10 percent. Usually the Data Link layer is null. If the Data Link layer contains an Ethernet MAC function, the format is called Ethernet Over SONET (see EoS-VC). Sprint launched the first OC-12 packet-over-SONET (POS) Internet network in late 1997. Cisco provides a good [tutorial](#) about POS. Also see MAPOS (Multiple Access Protocol over SONET/SDH).

PPP Point-To-Point Protocol

An IETF standard defined by [RFC1661](#) for sending IP packets over asynchronous and synchronous serial lines. The Bonn Institute of Computer Science provides a good [PPP Reference](#). Related protocols include The PPP Multilink Protocol-MP ([RFC1990](#)), PPP Vendor Extensions ([RFC2153](#)), and PPP in HDLC-Like Framing ([RFC1662](#)).

PPPoE Point-to-Point Protocol Over Ethernet

Defined by [RFC2516](#), PPPoE is a way to provide connections from multiple remote hosts to a central site over an Ethernet link. Each connection uses PPP (Point-to-Point Protocol – see PPP) and is therefore able to carry traffic that is not Ethernet compatible. PPPoE is in some ways the opposite of BCP (Bridging Control Protocol), which transports Ethernet frames over PPP links – see BCP.

PPTP Point to Point Tunneling Protocol

A Layer 2 protocol that enables virtual private networking by encapsulating other protocols such as NetWare IPX for transmission over an IP network. PPTP is used as a VPN tunneling protocol; other such protocols are IPsec and L2TP. See IPsec, L2TP.

PPTP is also used to create a private network (VPN) within the public Internet by taking advantage of its RSA encryption or its Microsoft Point-to-Point Encryption (MPPE). Remote users can access their corporate networks via any ISP that supports PPTP on its servers. The protocol was developed by the PPTP Forum, which included Ascend, Microsoft, 3Com, and U.S. Robotics. It was first demonstrated in Spring 1996 by U.S. Robotics and Microsoft. U.S. Robotics developed the Windows NT PPTP driver, for integration into Microsoft’s Windows NT Server 4.0. PPTP support is built into Windows 95 and 98.

PPTP allows NT network clients to take advantage of the services provided by Microsoft's RAS (Remote Access Service). For remote access, over analog or ISDN lines, PPTP creates a tunnel directly to the appropriate network NT Server. By terminating the remote user's PPP connection at the NT server, rather than at the remote access hardware, PPTP allows network administrators to standardize security using the existing services and capabilities built into the Windows NT security domain.

PRBS Pseudo-Random Bit Sequence

Data test patterns utilized in bit error rate testing of SONET links.

PVST Per-VLAN Spanning Tree

A Cisco-proprietary enhancement of Spanning Tree Protocol (STP) that allows switches to use multiple spanning trees, allowing traffic belonging to different VLANs to flow over different paths within the virtual bridged LAN. PVST+ adds support for VLAN (802.1Q) trunks to map multiple spanning trees to a single spanning tree. IEEE 802.1s is the industry standard protocol under development for Multiple Spanning Trees for VLANs; see STP and 802.1s.

QoS Quality of Service

Network device capabilities that provide some guarantee of performance such as traffic delivery priority, speed, latency, or latency variation. Delivery of good-quality audio or video streams typically requires QoS capabilities. The www.employees.org/~ferguson/QoS.html page on "Delivering QoS on the Internet and in Corporate Networks" contains an extensive bibliography, tutorial information, and links to QoS-related draft standards. The QoS Forum (www.qosforum.com) is devoted to educating the market and accelerating the adoption of standards-based QoS technologies but is not a standards-setting group. Also see 802.1p and RSVP.

QoSR Quality of Service Routing

Procedures being studied by the IETF ([RFC2386](http://www.ietf.org/rfc/rfc2386.html)) to select routing paths based on network resource availability and the quality requirements of the traffic flow. Current routing protocols (such as RIP, OSPF, and BGP4) do not consider the link capacity when making route assignments.

QRSS Quasi-Random Signal Source

A test pattern used in SONET testing to find timing or data errors. QRS generates every combination of 20-bit words, repeats every 1,048,575 bits, and contains high density sequences, low density sequences, and sequences that change between low density and high density.

RADIUS Remote Access Dial-In User Service

A common security feature in routers that authenticates a user logging onto the network using a challenge/response method. A RADIUS client contacts a RADIUS server to authenticate access to the network. A typical RADIUS server can handle remote-access authentication, controlling user access rights, and gathering accounting information, a group of functions commonly known as "AAA." RADIUS was developed by Livingston Enterprises for their own routers. It was submitted to the IETF and is described in [RFC2138](http://www.ietf.org/rfc/rfc2138.html). Novell Directory Services (NDS) provides an alternative kind of centralized authentication. Also see TACACS (Terminal Access Controller Access Control System).

RARP Reverse ARP

A standard defined by IETF [RFC903](http://www.ietf.org/rfc/rfc903.html) that performs the opposite of ARP, finding a Layer 3 address that corresponds to a Layer 2 address. It is used by diskless workstations that need to obtain unique IP addresses upon startup. A RARP server responds to a RARP broadcast from the workstation and sends back the IP address. See ARP and BOOTP.

RED Random Early Detection

A congestion control technique for TCP/IP in which a router randomly drops packets from all sources when the traffic gets heavy prior to periods of high congestion. While this causes some retransmissions, it is an improvement over conventional schemes that simply drop packets from the end of a queue when the router's buffers become full, and tend to cause huge waves of retransmissions in large networks. RED is accomplished by dropping packets in a statistically random fashion when the router buffers exceed a certain threshold of fullness. Cisco lab experiments showed that voice traffic can tolerate a loss of approximately 1 out of every 10 packets. For an overview of references on RED see www.aciri.org/floyd/red.html. Also see WRED (Weighted Random Early Detection.)

RFC1242 Benchmarking Terminology for Network Interconnection Devices

[RFC1242](http://www.ietf.org/rfc/rfc1242.html) defines terms that are used in describing RFC2544 performance benchmarking tests and their results. See RFC2544.

RFC2285 Benchmarking Terminology for LAN Switching Devices

[RFC2285](#) defines terms that are used in describing RFC2889 performance benchmarking tests and their results. See RFC2889.

RFC2544 Benchmarking Methodology for Network Interconnect Devices

[RFC2544](#) defines tests that may be used to describe the performance characteristics of a network interconnecting device and describes specific formats for reporting the results. Appendix A lists the tests and conditions to be included for specific cases and gives additional information about testing practices. Appendix B lists maximum frame rates to be used with specific frame sizes on various media. Appendix C gives some examples of frame formats to be used in testing. See RFC2889.

RFC2889 Benchmarking Methodology for LAN Switching Devices

The [RFC2889](#) IETF document provides methodology for benchmarking LAN switching devices: forwarding performance, congestion control, latency, address handling, and filtering. It is an extension to [RFC2544](#), which discusses benchmarking for network interconnecting devices. In addition to defining the tests, this document also describes specific formats for reporting the results of the tests. See RFC2285 and RFC2544.

RIP Routing Information Protocol

Based on IETF [RFC1058](#), a router protocol that determines the best path for routing traffic over a network by analyzing hop counts. RIP is based on distance-vector algorithms that measure the shortest path between two points on a network based on the number of router hops between those points. RIP protocols consume a lot of network bandwidth by continuously announcing themselves on the network. AppleTalk, DECnet, TCP/IP, NetWare and VINES all use incompatible versions of RIP.

RIP is inefficient on large networks because it was never designed to support situations in which there are hundreds of possible destinations from a specific source. In large networks it can often take longer than the 30-second interval between broadcasts for the protocol to converge and recalculate routing after a topology change. That means that routers may broadcast outdated information because changes haven't reached them yet and confuse routers that have already received the updated information, causing routing loops or dead routes.

RIP2 or RIPv2 (RIP version 2, [RFC1723](#)) works the same way but adds support for subnet zero, classless IP, and some basic authentication. It can use IP Multicast to send updates to other routers. RIPv6 is the designation for a new version of RIP that handles the larger addresses associated with IPv6. See IPv6.

RMON Remote Monitoring

Defined by [RFC1757](#), RMON provides extensions to the Simple Network Management Protocol (SNMP) that provide comprehensive network monitoring capabilities. Standard SNMP is designed so that the device being monitored has to be queried to obtain information. RMON is proactive so it eliminates the polling required in standard SNMP: it can set alarms on a variety of traffic conditions, including specific types of errors. See RMON2 and SMON (Switch Monitoring)

The full RMON capabilities are very extensive so routers and other network devices generally only implement portions of it. The complete set of RMON groups are:

- 1-Statistics (traffic and errors)
- 2-History (periodic samples of the Statistics counters)
- 3-Alarms (setting thresholds and sampling intervals to generate alarms on any RMON variable)
- 4-Hosts (traffic and error statistics for each host)
- 5-Hosts Top N (extends Hosts by providing sorted host statistics)
- 6-Matrix (traffic and errors between pairs of devices)
- 7-Filter (instructions to capture packets that match a specific criterion)
- 8-Capture (capture buffers for uploading and analysis)
- 9-Events (create log entries or send SNMP traps based on crossing a defined threshold of any RMON variable).

RMON2

Extensions to RMON that include:

- Protocol directory (identifies packets used by many of the new groups in the standard)
- Protocol distribution (counts of traffic per protocol)
- Address mapping (MAC addresses)
- Network layer host (tracks amount of traffic between network addresses)
- Network layer matrix (determines top conversations between network addresses)
- Application layer host (tracks amount of traffic by application protocol)
- Application layer matrix (information on top conversations based on application protocols).

RMON2 has better traffic analysis capabilities than RMON, but not all network devices implement the standard and it requires much more processor bandwidth than RMON.

RMTP Reliable Multicast Transport Protocol

A protocol for reliable data transport over IP multicast developed by Bell Labs. It is used by Lucent Technologies in its [e-cast](#) product to handle file transfer, real-time applications, and near-real-time applications. Lucent's e-cast is based on a single sender, an optional hierarchy of "designated receivers," and multiple ordinary receivers.

RPR Resilient Packet Ring

See 802.17.

RSTP Rapid Spanning Tree Protocol

See 802.1w.

RSVP Resource Reservation Protocol

Based on IETF [RFC2205](#): a resource reservation setup protocol for IP networks. Routers can use RSVP-based signaling exchanges to reserve or set aside resources such as bandwidth that may be needed to handle designated traffic flows. CR-LDP and RSVP-TE are protocols for distributing labels among MPLS routers for constraint-based routing – see MPLS. Until March '99 USC maintained a web page devoted to RSVP information and status at www.isi.edu/rsvp. Also see 802.1p and ISSLL.

RSVP+ is a name given to various extensions to RSVP by Microsoft and Cisco described in an [IETF draft](#) working document. With RSVP+ applications prioritize themselves with respect to each other by announcing their requirements to the network. It assumes that a switch/router uses RSVP as a COPS client in communicating with a policy server -- see COPS.

Microsoft is a strong supporter and has incorporated RSVP support in Windows 2000, believing that it should be used to signal for any important, consistent application. A WinSock API extension allows applications to request RSVP signaling.

Issues There is considerable criticism of RSVP for large public Internet applications where it won't be feasible for routers to keep track of a huge number of different traffic flows and their respective attributes, so RSVP is no longer expected to be used to control end-to-end signaling. Enterprise networks typically have much smaller and simpler bandwidth reservation needs, and won't have this problem. There is broader industry support for Differentiated Services (see DiffServ) as a much simpler and more feasible method of traffic classification. Industry support is growing for using RSVP at the network edge to negotiate bandwidth provisioning, and using DiffServ or MPLS to control the network resources.

RSVP-TE RSVP With Traffic Engineering Extensions

CR-LDP and RSVP-TE are protocols for distributing labels among MPLS routers for constraint-based routing. See MPLS.

RTMP Routing Table Management Protocol

An AppleTalk routing protocol.

RTP Real-Time Transport Protocol

RTP provides end-to-end network transport functions suitable for applications transmitting real-time data such as audio or video over multicast or unicast network services. It is an IETF standard defined by [RFC1889](#) and [RFC1890](#). It does not establish connections or provide any guarantees of delivery or network availability. It includes the Real-Time Control Protocol (RTCP) for use in multicasting. RTP runs over UDP and IP, and is important for transporting Voice Over IP (see VOIP). See <http://www.cs.columbia.edu/~hgs/rtp/> for an overview of RTP and related topics.

RTP (VINES) Routing Table Protocol

A routing protocol for Banyan VINES that is based on the RIP protocol (see RIP). It uses delay as a routing metric.

RTSP Real-Time Streaming Protocol

RTSP, published as proposed standard [RFC2326](#) in April '98, is a client-server protocol for controlled, on-demand delivery of real-time data such as audio and video over IP networks where large-scale broadcasts and audio/video-on-demand streaming are important. RTSP provides "VCR-style" capabilities such as pause, fast forward, reverse, and absolute positioning. Both H.323 and RTSP use RTP as their standard means of actually delivering the multimedia data (see H.323 and RTP). The [RTSP.org](#) web site has a helpful overview and FAQ section.

RU Rack Unit

The standard method of specifying the height of data communication equipment or servers mounted in racks. 1 RU equals

1.75 inches. 42 RU (73.5 inches) is the most common height for racks in enterprise data centers, although 44 RU racks are now being used also. Telephone company central offices usually specify rack height in feet rather than RU because they go from floor to ceiling; 7 feet tall is the most common telco rack height.

SAP Service Advertising Protocol

Protocol used in NetWare IPX networks to handle server name-to-network address resolution.

SBM Subnet Bandwidth Manager

An IETF [draft](#) signaling scheme used to convey 802.1p priorities between Layer 2 switches. It will communicate class of service information between RSVP clients and RSVP-enabled networks.

SDH Synchronous Digital Hierarchy

See SONET.

SHA-1 Secure Hash Algorithm-1

A security protocol for message authentication (for verifying data integrity) – see IPsec. MD5 is another popular authentication protocol.

S-HTTP Secure Hypertext Transfer Protocol

An extension of HTTP (see HTTP) that provides authentication and data encryption between a Web server and a Web browser to enable secure transactions over the World Wide Web. It is endorsed by NCSA and a variety of organizations and is widely used but is only a draft standard. v1.3 was released in March 1997. Also see SSL (Secure Socket Layer).

SIP Session Initiation Protocol

A proposed IETF standard ([RFC2543](#)) for signaling Voice Over IP and other multimedia calls over the Internet using TCP or UDP. The [IETF SIP](#) working group has been handling this since September 1999. SIP is widely expected to be the future standard for handling VoIP. Windows XP supports SIP for making telephone calls, attaching voice and sound clips to e-mails, and for instant messaging. Cisco shipped its SIP Proxy Server in March '02. AOL is adopting SIP for instant messaging and for interoperability with other services. SIP is a partial alternative to the ITU's complex H.323 standard -- see H.323. One of the primary advantages of SIP is its simplicity. Columbia University is hosting SIP interoperability testing for various vendors. Media Gateway Control Protocol is a companion VOIP protocol whose development is also being managed by the IETF -- see MGCP.

Issues There is currently no universally compatible SIP phone number directory system, so VoIP calls between different SIP services are sometimes impossible. Even within a single SIP service, traversing enterprise NAT and firewall servers is currently a big technical obstacle because these systems were not designed to handle the 2 TCP ports plus 2-4 UDP ports needed for each SIP call.

SLA Service-Level Agreement

An agreement between an Internet service provider and its customer (or between two service providers) regarding the types of networking services, including service-level guarantees, that it will provide for stated prices. It will be important for future multilayer switches and other network devices to provide tools for enforcing compliance with these service levels and means for measuring compliance with them.

SLB Server Load Balancing

A process for directing an IP packet to the most appropriate server based on the content of the packet in order to balance the load across a group of servers or to ensure that certain types of transactions are handled by appropriate servers.

SLP Service Location Protocol

IETF [draft](#) protocol used by new Novell operating systems to handle server name-to-network address resolution. SLP is a version of SAP (used in IPX networks) that is modified for IP traffic but with less bandwidth waste than SAP. SLP can be used to locate resources on an IP network without entering the IP address.

SMON Switch Monitoring

An IETF proposed standard ([RFC2613](#), "Remote Network Monitoring MIB Extensions for Switched Networks") proposed in February '99 based on technology developed by LANNET and acquired by Lucent Technologies. SMON allows simultaneous monitoring of real-time network traffic across multiple switches in a network and across all ports in a single switch. This capability was first announced in Lucent products in late 1998. Also see RMON (Remote Monitoring).

SNMP Simple Network Management Protocol

IETF protocol widely used in conjunction with TCP/IP for network management and monitoring network devices. It allows network management applications to query a management agent that uses a standard data storage structure called a MIB (Management Information Base). The [SNMP Research](#) web site has helpful material explaining SNMP and its various versions. Also see RMON, CMIP, and TL1.

SNMPv1 became a TCP/IP standard protocol in 1990, and is described by [RFC1157](#) in conjunction with [RFC1155](#) and [RFC1212](#). SNMPv2, which was described by [RFC1902](#)-1908 in early 1996, is a major revision that corrects performance concerns about the original version while providing more data types and better error handling. However, major goals regarding added security and security management were not met. SNMPv3 is described in [RFC2271](#)-2275 and adds security (authentication, privacy, access control) and related administration features. In April 2002 SNMPv3 became a full standard and v1/v2 were moved to historical status.

SOCKS

A security protocol sponsored by NEC Systems Laboratory (see www.socks.nec.com), who says that the protocol interoperates with and adds value to IPsec and PPTP. Its stated benefits include the ability to implement UDP-based applications – such as streaming audio and video -- securely across firewalls, use a variety of encryption and authentication schemes, and provide secure communications using differing addressing schemes. SOCKS has not been nearly as popular as IPsec and PPTP, but NEC is promoting it heavily and several vendors plan to submit an updated version to the IETF. See IPsec and PPTP.

SONET Synchronous Optical Network

An intelligent system for transmitting high-speed digital signals on fiberoptic networks that has self-healing and network management capabilities. The SONET standard applies in North America and Japan; the comparable European standard is SDH (Synchronous Digital Hierarchy). The SONET standard includes a physical interface, a frame format with timing and network management provisions, and optical data rates (OC-1, OC-3, etc.). The OC rates correspond to the equivalent STS (Synchronous Transport Signal) rates where STS-1 is 51.84 Mbps and higher values are multiples of that. The SDH standard uses STM rates instead of STS rates. See Digital Signal (DS).

SSH Secure Shell

A protocol that provides authenticated and encrypted secure connections to a Web server using military-grade encryption. SSH protocol is based on public-key cryptography using a key pair. The sender encrypts with a public key, and the recipient decrypts with a different key that is secret. RSA cryptography is used for authentication and to promote the secure exchange of the session key. The SSH protocol was created around 1995 and has become widely used for encrypted remote logins over the Internet. It was originally developed as a replacement for the Berkeley UNIX *r** commands (rlogin, rsh and rcp).

SSL Secure Socket Layer

A transport level technology developed by Netscape that provides point-to-point authentication and data encryption between a Web server and a Web browser (client). SSL sends data over a "socket," a secure channel at the connection layer that exists in most TCP/IP applications. SSL is a leading security protocol on the Internet, and support for it is built into most browsers now. Also see S-HTTP and encryption standards DES and AES.

STP Spanning Tree Protocol

Defined by standard IEEE 802.1d, a scheme used by Layer 2 switches to automatically inactivate certain network links so that traffic will have only one path between a specific source and destination, and will not travel endlessly in loops. Spanning Tree is a self-learning protocol that automatically reconfigures itself if any network link fails to send traffic over another path if possible, although this reconfiguration time can be relatively slow in light of today's networking speeds.

Some switches provide STP-type functionality on a per-VLAN basis, meaning that separate network topology tables are maintained for every VLAN: See 802.1s (Multiple Spanning Trees for VLANs) and PVST (Per-VLAN Spanning Tree).

STS-1

For STS-1 through STS-48, see DS (Digital Signal).

T1

For T1 through T4, see DS (Digital Signal).

TACACS Terminal Access Controller Access Control System

A common security feature in routers that authenticates a user logging onto the network. A typical TACACS server can handle remote-access authentication, controlling user access rights, and gathering accounting information, a group of functions commonly known as "AAA." TACACS is described in [RFC1492](#) based on development work by Cisco. TACACS was a simple

username/password system and Extended TACACS (XTACACS) added more intelligence in the server. TACACS+ is the typical implementation today, which includes encryption and a challenge/response option. Also see RADIUS (Remote Access Dial-In User Service).

Tcl Tool Command Language

Pronounced “tickle”, Tcl is both a language and a library. It is a textual language that is simple and programmable, intended for issuing commands to interactive programs such as testers, debuggers, and shells. Tcl users can thus write command procedures to create more powerful functions than those built into the original unit. Tcl is also a library package with parser and procedures that can be embedded in application programs. Tk is an extension to Tcl that provides a programming interface to the X11 windowing system. www.neosoft.com/tcl/whatistcl.html has more explanations and references for Tcl and Tk.

TCP/IP Transmission Control Protocol-Internet Protocol

Based on IETF standard [RFC793](http://www.ietf.org/rfc/rfc793.txt): TCP is a reliable, connection-oriented protocol that first establishes a connection between the two systems that will exchange data. When an application sends a message to TCP for transmission, TCP breaks the message into packets, sized appropriately for the network. TCP provides flow control (to prevent overrunning the receiver) and congestion control (to prevent overrunning the capacity of the network.) For Ethernet networks, the maximum packet size is 1518 Bytes. Also see IP, UDP. TCP uses the IP protocol to address and send the packets. The IP protocol uses three key parameters: the IP address, subnet mask, and default gateway.

TKIP Temporal Key Integrity Protocol

A collection of enhancements being planned for the 802.11 wireless LAN standard to correct security deficiencies in the Wired Equivalent Privacy (WEP) standard. See 802.11 and WEP.

TL1 Transaction Language 1

A widely used protocol in telecommunications management that can be used to manage most telecom network elements in North America today. Unlike its alternatives CMIP and SNMP, TL1 is a man-machine interface that contains strings that humans can read and understand. TL1 was originally specified by Bellcore in 1986. www.tl1.com contains a helpful overview and history. Also see CMIP and SNMP.

TTL Time to Live

A field in an IP packet header that is decremented at each router that the packet passes through. It allows a router to determine when to discard a packet due to an apparent router loop. The TTL field is also used to limit the distance that IP Multicast packets propagate.

TOS Type of Service

A byte located in every IP packet header that contains 6 bits intended to identify the packet's priority and throughput handling requirements but rarely used. The IETF DiffServ working group is defining a new scheme for using this byte – see DiffServ.

Traffic Engineering

Traffic engineering means setting up explicit routes through a network that are not necessarily technically optimum according to the routing protocols that are in use. This capability allows network managers to override dynamic routing protocols in order to manually control certain traffic flows. See MPLS.

TFTP Trivial File Transfer Protocol

A simplified version of FTP that transfers files without password protection or directory capabilities. Network devices can use TFTP to download new versions of operating firmware. See FTP.

UDP User Datagram Protocol

A connectionless mode protocol that is part of the TCP/IP family, defined by IETF [RFC768](http://www.ietf.org/rfc/rfc768.txt). UDP allows an application to send a message to one of several other applications running on a remote or local machine. UDP operates much faster than TCP because it has much less overhead. Consequently, UDP is extremely important for many real-time video, audio, and storage networking applications where high speed and low latency are important. Wire-speed UDP processing is an important feature for switches or routers that must handle this type of real-time traffic reliably.

Data sent via the UDP protocol is not acknowledged and is thus less reliable than data sent via TCP/IP. Data can also be out of sequence and potentially duplicated.

Virtual Concatenation

See EoS-VC (Ethernet Over SONET Virtual Concatenation).

VLAN Virtual LAN

A group of independent devices that communicate as if they are on the same physical LAN segment but can actually be located anywhere on the network. VLANs typically allow each connected device to be placed into a logical group according to its physical point of connection (switch port), MAC address, or network protocol type. 802.1Q defines a numbering scheme that allows up to 4094 distinct VLANs on a network -- see 802.1Q.

VoIP Voice Over IP

An extension of ITU-T standards to support voice communications over IP networks such as the Internet with compatibility between products from different manufacturers. Typical scenarios are PC to PC, PC to phone, and phone to phone. Some incompatibilities exist now between various implementations due to the unfinished states of H.323 and SIP standards. VoIP is currently used mostly over private IP WANs so traffic priority can be assured. In the future, Differentiated Services (see DiffServ) may be crucial for providing appropriate priority so that VoIP can be implemented effectively on public networks.

VoIP typically uses the SIP or H.323 protocol to signal call setup. The audio stream is then sent over the Real-Time Transport Protocol (see RTP) using an encoding/compression protocol such as G.711 or G.729 in minimum-size packets with small payloads of 20 bytes.

The Voice over IP Forum was formed in 1996 by Cisco Systems, VocalTec, Dialogic, 3Com, Netspeak and others as a working group of the International Multimedia Teleconferencing Consortium (IMTC), which promotes the implementation of the ITU-T H.323 standard (see www.imtc.org). The Protocols.com web site maintains links to many VOIP references and standards (www.protocols.com/voip.htm).

VPLS Virtual Private LAN Service

VPLS is described by an [Internet Draft](#) within the IETF PPVPN Working Group and explains the requirements related to emulating a virtual private LAN segment over an IP or MPLS network. See VPN (MPLS Layer 2 VPNs).

VPN Virtual Private Network

A private connection over the public Internet that enables secure communications from a remote site. The two major classes of VPNs are remote access (accessing an enterprise network remotely via a dial-up call to a local Internet service provider) and site-to-site (linking two or more portions of an enterprise's intranet or extranet over the public Internet). The most common protocols for IP-based VPNs are MPLS (see MPLS and description below), Layer 2 Tunneling Protocol (see L2TP), and the collection of IP Security protocols known as IPsec (see IPsec). When high security is required, the security features of IPsec are more appropriate than those of L2TP. Some VPNs employ connections using PPTP, a popular VPN tunneling protocol developed by Microsoft -- see PPTP.

There are two types of MPLS VPNs (see MPLS):

- Layer 2 VPNs emulate Layer 2 networking services such as Ethernet, ATM, or Frame Relay and are referred to as Virtual Private LAN Service (VPLS). They forward data based on its Layer 2 header information and are typically invisible to the end user. Popular and widely adopted IETF draft standards referred to as Martini and Kompella describe these mechanisms. The Layer 2 Tunneling Protocol v3 (L2TPv3) is also being developed to transport native Layer 2 services across MPLS; see L2TPv3.
- Layer 3 VPNs are based on RFC2547bis and rely on IP routing mechanisms. They separate each VPN customer by creating a separate instance of a virtual router for each customer, implementing that user's unique routing space. They can create a huge demand for memory in service provider's edge routers, however, because of the need to support every user's routing tables.

VRRP Virtual Router Redundancy Protocol

An IETF protocol ([RFC2338](#)) to supply packet forwarding fail-over in case a primary router fails. The protocol is based on the concept of a virtual router comprised of an existing network router that backs up the main router. The virtual router acts as first hop router if the main router become unavailable. The proposed protocol handles ARP (Address Resolution Protocol) requests in a nonstandard way. Proprietary alternatives for providing router redundancy protection include HSRP from Cisco and FSRP from Foundry Networks.

VSR Very Short Reach

VSR optics are being developed to provide much lower cost OC-192 interfaces within service provider facilities where short links between networking products are sufficient. The [Optical Internetworking Forum](#) (OIF) is helping coordinate the standardization effort and provides a helpful white paper. Four VSR solutions are intended to cover the range of requirements and applications that service providers have:

VSR-1 12 fibers operating at 1.25 Gbps each (GbE speed) using 850nm VCSEL lasers. 2 MMF ribbon cables provide operation up to 300m.

VSR-2 1 fiber operating at 10 Gbps using 1310nm edge-emitting FP lasers (and eventually VCSEL lasers). 2 SMF fiber cables provide operation to 600m.

- VSR-3 4 fibers operating at 2.5 Gbps using 850nm VCSEL lasers. 4 MMF fiber cables provide operation to 300m.
VSR-4 1 fiber operating at 10 Gbps using an 850nm VCSEL laser. 1 MMF fiber cable provides operation to 300m.

VTOA Voice and Telephony over ATM

Provides for the integration of switched-voice services with broadband ATM terminals to allow users to save money by combining their voice and data networks while avoiding the interoperability issues that have been associated with the integration of ATM and telephony in the past. This ATM Forum [specification](#) is being developed by its VTOA Working Group. VTOA requires implementation of one of two previous ATM Forum [specifications](#): UNI (User-Network Interface) 4.0 or PNNI (Private Network-Network Interface) 1.0.

WAP Wireless Application Protocol

The WAP protocol provides for information services on wireless terminals such as digital mobile phones and pagers. All major operating systems support WAP, and WAP supports most wireless networks. WAP supports HTML and XML, but WML (Wireless Markup Language, an XML application) is designed to create pages to be displayed in a WAP browser on a small screen. The [Open Mobile Alliance](#), which combined the WAP Forum and the Open Mobile Architecture Initiative, is working to grow the mobile industry market and ensure application interoperability. The IEC provides a useful [WAP Tutorial](#).

WBEM Web-Based Enterprise Management

A system for unified administration of network, systems and software resources proposed by Microsoft, Intel, Compaq, Cisco, BMC Software, and others. It allows users to manage distributed systems using any Web browser. In June, 1998, WBEM was turned over to the DMTF (Desktop Management Task Force) standards body (see www.dmtf.org).

It incorporates a new Common Information Model protocol (see CIM) that defines the objects to be managed. CIM v2.0 is the current version. WBEM originally specified a new Hypermedia Management Protocol (HMMP) for transporting management information, but now XML (eXtensible Markup Language) will be used instead. Original plans to standardize an Object Manager (OM) that collects management data and acts as an interface to supporting applications have been dropped; vendors must now define this component themselves. HTTP is the access mechanism for WBEM. Compaq, HP, and Dell are planning to support WBEM. Tivoli supports WBEM in its NetView 5.1 product that runs on Windows NT and Unix. Cisco supports WBEM in its CiscoWorks 2000 product. Microsoft will support WBEM in Windows 98 and Windows 2000.

WDM Wavelength Division Multiplexing

Two or more colors of light sent over one optical fiber simultaneously, where each color carries one signal. Current technology can support 64 to 96 (or more) colors per fiber with each color carrying a Gigabit Ethernet, OC-48, or OC-192 signal. The Greek symbol lambda (λ) is often used to refer to a specific optical wavelength (or color). In practice, WDM refers to any such system. However, WDM can be used to describe systems with few colors per fiber (such as 8 or fewer), and DWDM (Dense Wavelength Division Multiplexing) can refer to larger numbers of colors per fiber.

WEP Wired Equivalent Privacy

A security protocol for wireless LANs that is part of the 802.11 Wireless LAN standard – see 802.11. WEP has been criticized for its relatively weak RC4-type encryption and lack of user authentication. The [“Security of the WEP algorithm”](#) paper by UC Berkeley addresses some of the security concerns with WEP. Other current alternatives include 802.1x, TKIP, and VPN technology (see 802.1x, TKIP, and VPN).

WFQ Weighted Fair Queuing

A system of scheduling packets that are waiting for transmission that separates the packets into classes of different priorities and guarantees that each class receives some portion of the available bandwidth. This ensures that both heavy and light network users receive consistent response times. WFQ dynamically adjusts bandwidth allocations based on the traffic parameters and the relative amounts of traffic, reducing jitter and producing more predictable round-trip delays.

Wi-Fi Wireless Fidelity

Refers to the 802.11b wireless LAN standard – see 802.11b.

WRED Weighted Random Early Detection

A version of the Random Early Detection collision control scheme (see RED) that drops packets selectively. Packets with a higher IP precedence are less likely to be dropped than those having a lower precedence, so higher priority traffic is delivered with a higher probability than lower priority traffic.

X2 10 Gbps Interface MSA

Electrically compatible with XENPAK, X2 is a multi-source agreement (MSA) that defines a smaller form-factor 10 Gbps pluggable fiber optic transceiver optimized for 802.3ae 10 Gb Ethernet, OC-192/STM-64 SONET/SDH interfaces, ITUT G.709, OIF OC-192 VSR, INCITS/ANSI 10GFC (10 Gb Fibre Channel), and other 10 Gbps applications. X2 is thermally and

mechanically similar to XPAK and is initially focused on optical links limited to 10 km where a "half size" XENPAK optical transceiver is desired. Announced in August '02 and led by Agilent, other X2 supporters include Agere Systems, JDS Uniphase, Mitsubishi Electric, NEC, OpNext, Optillion, and Tyco Electronics.. X2MSA.org explains the X2 MSA. See XENPAK, XPAK.

XAUI 10 Gb Ethernet Transceiver Interface

Defined by the 802.3ae 10 Gb Ethernet standard, XAUI (pronounced "zowie") is an internal electronics interface extender between the MAC (media access control) electronics and an optical network transceiver. XAUI is a low pin count self-clocked serial bus with four 3.125 Gbps differential data interfaces ("lanes") using the same 8B/10B transmission code as 1 Gb Ethernet. Maximum length is 0.5m. Also see 802.3ae, XENPAK, and XPAK. The "[10 Gigabit Ethernet and XAUI Interface](#)" paper by Agilent is very helpful to explain both the XAUI and XENPAK interfaces.

XENPAK 10 Gbps Interface MSA

A multi-source agreement (MSA) for a 10 Gbps hot-pluggable module that converts the 802.3ae 10 Gb Ethernet XAUI internal parallel electrical signals to an external SC duplex fiber network interface (121mm x 51.3mm). The [XENPAK MSA group](#), initiated in March '01 by Agilent Technologies and Agere Systems but now with a large number of members, is creating the specification and promoting it. XENPAK devices are in production now. XFP and XPAK are important competitive alternatives. XENPAK devices are larger, accommodating only 8 transceivers on typical line cards, and are intended to support all the 10 Gb Ethernet optical interface types. See XAUI.

X.86 Link Access Procedure-SDH

See LAPS (Link Access Procedure-SDH).

XFP 10 Gbps Interface MSA

A multi-source agreement (MSA) for a 10 Gbps hot-pluggable module that converts internal serial electrical signals to an external serial network interface that is typically optical, but could also be electrical (78mm x 18.35mm x 8.5mm). The [XFP MSA group](#), founded in March '02, is creating the specification and promoting it; Broadcom is a key leader. Production devices are not expected before 2003. XFP seeks to support OC-192/STM-64, 10 Gb Fibre Channel, 10 Gb Ethernet, and G.709. XENPAK and XPAK are important competitive alternatives. XFP claims to provide lower cost, lower power, and higher density (up to 16 transceivers on a typical 19 inch rack with 23mm pitch density). External functions (including SERDES) are needed for 10 Gb Ethernet support.

XPAK 10 Gbps Interface MSA

A multi-source agreement (MSA) for a 10 Gbps hot-pluggable module that converts internal parallel electrical signals to external serial, parallel, or CWDM network interfaces for distances up to 10 km (50.8mm x 38.1mm x 12.7mm). The agreement supports an electrically XENPAK-compatible parallel interface for both XAUI and SF14-P2 (protocol independent) and is intended for 10 Gb Ethernet, 10 Gb Fibre Channel, and SONET applications. The [XPAK MSA group](#), founded in March '02 by Infineon, Intel and Picolight, is creating the specification and promoting it. First samples were expected around Q4'02. XENPAK and XFP are important competitive alternatives. XPAK is the same width as XENPAK but half the length and height, claiming a less expensive interface for enterprise and SAN applications where long-haul optics are not needed, and supporting much higher density with up to 20 transceivers on a 17 inch circuit board.

ANRITSU COMPANY

North American Region Headquarters
1155 East Collins Boulevard
Richardson, TX 75081

Tel. 1-800-ANRITSU (267-4878)
E-mail: moreinfo@anritsu.com
www.us.anritsu.com

October 23, 2002