

The Must-Have Reference for Multilayer Switching

This reference provides the information you need to understand the terminology associated with multilayer switching products and 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 rise of the multilayer switch. New higher-density ASICs (Application-Specific Integrated Circuits) allow real-time switching and forwarding at 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

Multilayer switching is new, and there is no industry standard yet on nomenclature. 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 seems to be the best and most 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 technology. 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, 3Com, and Bay Networks — is one of the newest multilayer switching techniques and is also the most promising. 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 based on the contents of OSI layer 4 (the Transport Layer) where the end-station 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.

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 problems of its own. 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 Multilayer Switching

Overview of Terms by Topic

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

ATM Terms that are related to ATM networking:

- FANP (Flow Attribute Notification Protocol)
- GSMP (General Switch Management Protocol)
- IFMP (Ipsilon Flow Management Protocol)
- I-PNNI (Integrated PNNI)
- MARS (Multicast Address Resolution Server)
- MPLS (Multi-Protocol Label Switching)
- MPOA (Multiprotocol over ATM)
- PNNI (Private Network-to-Network Interface)
- VTOA (Voice and Telephony over ATM)

Gigabit Ethernet Terms that are related to Gigabit (1000 Mbps) Ethernet:

- 802.3ab (Gigabit Ethernet on Copper Twisted Pair)
- 802.3z (Gigabit Ethernet on Fiber and Shielded Copper)

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 IPv6.

Management Terms that are associated with network management, policy management, and network directory systems:

- CIM (Common Information Model)
- DEN (Directory Enabled Networking)
- HMMP (Hypermedia Management Protocol)
- LDAP (Lightweight Directory Access Protocol)
- PEPCI (Protocol for Exchange of Policy Information)
- RMON and RMON2 (Remote Monitoring)
- SNMP (Simple Network Management Protocol)
- WBEM (Web-Based Enterprise Management)

Multicast IP multicast requires several protocols to operate. End stations use IGMP (Internet Group Management Protocol) to specify their participation in a particular multicast group. Routers must run IGMP and 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)
- PGM (Pretty Good Multicast)
- RMTP (Reliable Multicast Transport Protocol)

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)
- ISSLL (Integrated Services over Specific Link Layers)
- MPLS (Multi-Protocol Label Switching)
- OOPS (Open Outsourcing Policy Services)
- RSVP (Resource Reservation Protocol)
- SBM (Subnet Bandwidth Manager)

Routing Protocols Dynamic routing protocols include OSPF (Open Shortest Path First), which is popular in large internetworks, and RIP (Routing Information Protocol), which is often used in small networks. 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), and IDRP (Interdomain Routing Protocol).

Novell NetWare networks use IPX (Internet Packet Exchange).

AppleTalk networks use RTMP (Routing Table Management Protocol).

Other terms that are associated with dynamic route determination methods:

- I-PNNI (Integrated PNNI)
- IS-IS (Intermediate System to Intermediate System)
- PNNI (Private Network-to-Network Interface)

Security Terms that are associated with network security:

- IPSec (IP Security)
- S-HTTP (Secure Hypertext Transfer Protocol)
- SSH (Secure Shell)
- SSL (Secure Socket Layer)

VLANs Terms that are related to Virtual LANs:

- 802.1p (Priority and VLAN Topology)
- 802.1Q (VLAN Tagging)
- 802.3ac (VLAN Tagging for Ethernet)
- GARP (Generic Attributes Registration Protocol)
- GVRP (GARP VLAN Registration Protocol)

Voice Terms that are associated with voice transmission over LANs:

- VoIP (Voice Over IP)
- VTOA (Voice and Telephony over ATM)

VPNs Terms that are associated with Virtual Private Networks:

- L2TP (Layer 2 Tunneling Protocol)
- NAT (Network Address Translation)
- PPTP (Point to Point Tunneling Protocol)

Also see VPN (Virtual Private Network).

Alphabetic List of Terms and Abbreviations

802.1p Priority and VLAN Topology

A 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. 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.

802.1Q VLAN Tagging

Defines changes to Ethernet frames that will 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. 802.1Q is planned for release in the first half of 1998.

802.3ab Gigabit Ethernet on Copper Twisted Pair

IEEE working group defining the 1000BASE-TX standard for Gigabit Ethernet operation on 100m of 4-pair Category 5 twisted pair copper cabling. This effort is approximately 1 to 2 years behind 802.3z for Gigabit operation on fiber. The target for a draft standard is 12/98.

802.3ac VLAN Tagging for Ethernet

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

802.3ad Trunking

IEEE working group to define network link aggregation and trunking standards.

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-TX standard for operation on 100m of 4-pair Category 5 twisted pair copper cabling is being defined by 802.3ab – see 802.3ab.

100BASE-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 bandwidth – 500m maximum length
 - 500 MHz*km bandwidth – 550m maximum length
- MMF 62.5u (most commonly installed fiber):
 - 160 MHz*km bandwidth (old FDDI-grade fiber; TIA 568 spec) – 220m maximum length
 - 200 MHz*km 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 bandwidth) – 550m maximum length
- MMF 62.5u (500 MHz*km 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.

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.

BGMP Border Gateway Multicast Protocol

Draft standard (draft-ietf-idmr-gum-01.txt) that contains extensions to BGP (Border Gateway Protocol) for IP multicast. It is in the early stage of definition and research.

See MBGP.

- BGP** Border Gateway Protocol
- Based on standard RFC1163: a TCP/IP routing protocol for interdomain routing in large networks. It is used in the Internet and is an alternative to EGP (Exterior Gateway Protocol). The current version is BGP v4.
- See BGMP, MBGP. See GUM.
- BOOTP** Bootstrap Protocol
- Based on standard 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.
- CBT** Core Based Trees
- Draft standard (draft-ietf-idmr-cbt-br-spec-01.txt) 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 that are available from online RFC libraries: RFC 2189 on Core Based Trees (CBT version 2) Multicast Routing; RFC 2201 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 standard 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.
- CIM** Common Information Model
- A standard format for storing management information and providing common definitions for managed objects that will use Web-based network management. CIM was originally called HMMS (Hypermedia Management Schema), a portion of of the WBEM (Web-Based Enterprise Management) initiative that around 70 vendors including Cisco, Compaq, Microsoft, and Intel began in July 1996. The development of the standard was turned over to the DMTF (Desktop Management Task Force), which renamed it CIM.
- CIM v1.0 was completed by the DMTF in April 1997 but is only a rough outline. v2.0 is more complete and is scheduled for publishing in the first half of 1998. Products based on CIM are expected to reach the market in summer 1998, with many available by the end of 1998. Microsoft has included CIM support in Beta copies of Windows 98, Windows NT 5.0, and SMS 2.0.
- CIM explains how information is stored, but does not define its common access language HMMP. The DMTF is expected to start working on HMMP after CIM 2.0 is completed, However, there are differing agendas for Web-based management from Microsoft and Sun. See HMMP.
- CLMP**
- A routed packet type.

COPS Common Open Policy Service

A simple query-and-response protocol for exchanging information over TCP/IP between policy servers and clients (such as routers). It lets RSVP-based routers know how to handle RSVP data flows. It also defines a way for routers and other devices to exchange information with centralized servers that store a network's QoS policies. A draft standard was released by IETF in February 1998.

See OOPS, a specification for managing QoS policy servers.

Data Rates

Key timing for Ethernet packets:

	<u>10Mbps</u>	<u>100Mbps</u>	<u>1Gbps</u>
Bit time	0.1us	0.01us/10ns	0.001us/1ns
Byte time	0.8us	0.08us/80ns	0.008us/8ns
64 Byte time	51.2us	5.12us	0.51us
1518 Byte time	1.21ms	121us	12.1us
Interframe gap	9.6us	0.96us	0.096us/96ns

Maximum packet (frame) rates for Ethernet:

64 Byte packets	14,879pps	148.8Kpps	1.48Mpps
512 Byte packets	2,347pps	23.5Kpps	235Kpps
1518 Byte packets	811pps	8.11Kpps	81.1Kpps

DEN Directory Enabled Networking

A scheme to create a common framework for storing management information about various network devices and their relationships and to define a common set of attributes for all directories. Cisco and Microsoft are leading this effort. Directories that support the DEN framework can be used to set management policies to govern network devices.

The first draft of the specification was planned for release in early 1998, and is scheduled to be turned over to IETF by mid-1998 for ratification. Microsoft says that network managers will be able to take advantage of the DEN initiative when Windows NT Server 5.0 ships in early 1999.

LDAP is a directory scheme with a simpler goal of letting directories talk with one another – see LDAP.

DHCP Dynamic Host Configuration Protocol

Based on standard 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.

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.

Issues Since DHCP dynamically allocates IP addresses it is possible that one computer that is boot-ed 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 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. This is a simplistic approach that seems to work.

DNS Domain Naming System

Based on standard RFC1033: 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.

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.

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 Circuits:

<u>Service</u>		<u>Speed</u>
STS-1	OC1	51.84 Mbps (28 DS1s or 1 DS3)
STS-3	OC3	155.52 (3 STS-1s)
STS-3c	OC3c	155.52 (concatenated)
STS-12	OC12	622.08 (12 STS-1s, 4 STS-3s)
STS-12c	OC12c	622.08 (12 STS-1s, 4 STS-3c's)
STS-48	OC48	2488.32 (48 STS-1s, 16 STS-3s)

DVMRP Distance Vector Multicast Routing Protocol

An IP multicast protocol described by IETF draft standard (draft-ietf-idmr-dvmrp-v3-05.txt). 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.

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.

E1

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

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.

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.

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 are using this technology in Gigabit Ethernet products shipped before 802.3z is approved so that if a change in the standard is made, users can swap out the GBICs for new, standards-compliant converters.
GMRP	GARP Multicast Registration Protocol
	Allows workstations to request membership in a multicast domain. GMRP provides a standard protocol for sending traffic to only those ports that have requested multicast traffic. See GARP.
GUM	Grand Unified Multicast
	Draft standard (draft-ietf-idmr-gum-01.txt) used in connection with BGMP (Border Gateway Multicast Protocol) — see BGMP.
GSMP	General Switch Management Protocol
	Based on standard RFC1987: 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.
GVRP	GARP VLAN Registration Protocol
	Allows workstations to request admission to a particular VLAN for multicast purposes. See GARP.
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
	An initiative by vendors including Cisco and Foundry to provide backup protection for routers.
ICMP	Internet Control Message Protocol
	Based on standard IETF STD1 and RFC792: 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.
	ICMPv6 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.
IFMP	Ipsilon Flow Management Protocol
	Based on standard RFC1953: Ipsilon’s proposed IP Switching protocol between two adjacent nodes. See GSMP.
IGMP	Internet Group Management Protocol
	Based on standard RFC2236: 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 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 starting to be deployed, and Microsoft has a test version for Win95.

v3—Allows receivers to specify desired sources, and exclude unwanted sources. As of early 1998, it is still being discussed and not on the standards track yet.

“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.

IP Internet Protocol

Based on standard IETF STD1: 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 computer (host) 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 addresses support the following number of networks and hosts:

<u>IP Address Class</u>	<u>Number of Networks</u>	<u>Number of Hosts (PCs)</u>
A	128	16M
B	16K	65K
C	16M	256

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

IPng IP Next Generation

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

IPOS IP Over SONET

Refers to sending IP Packets directly over a SONET (POS) transport when the Data Link layer is null. If the Data Link layer contains an Ethernet MAC function, the format is called Ethernet Over SONET. See POS.

IPSec IP Security

A suite of protocols that handles encryption, authentication, and secure transport of IP packets. It currently consists of almost 20 Internet Drafts and five RFCs (“IPSec RFCs”). IPsec support for VPNs is planned in Windows NT 5.0 Beta 2. IPSec will be incorporated into IPv6 – see IPv6.

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 Message Digest 5 (MD5). It supports two kinds of key management schemes that allow parties to agree upon parameters for the session.

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

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 GBONE is a worldwide network begun around 1996 that runs IPv6 on an experimental basis.

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 (DHCP), and the development of address translators have given IPv4 a longer life than originally expected. It 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. ATM will not replace IPv6 but is synergistic with it. Some say that IPv6 does not offer enough security or quality of service improvements to warrant immediate adoption.

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.

IS-IS	<p>Intermediate System to Intermediate System</p> <p>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.</p> <p>Integrated IS-IS (formerly Dual IS-IS) is a routing protocol based on the OSI routing protocol IS-IS, but with support for IP or other networks. Integrated IS-IS implementations send only one set of routing updates, regardless of protocol type, making it more efficient than two separate implementations.</p>
ISSLL	<p>Integrated Services over Specific Link Layers</p> <p>Draft standard (draft-ietf-issll-802-01.txt): 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 (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. 802.1p is defining the details of Layer 2 priorities in the switches.</p>
L2TP	<p>Layer 2 Tunneling Protocol</p> <p>The first proposed IETF protocol for tunneling Point-to-Point Protocol (PPP) across a private or public network. L2TP support for VPNs is planned in Windows NT 5.0 Beta 2. 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. It enables support for multiple protocols and unregistered IP addresses, allowing existing non-IP protocol applications such as SNA to be used.</p> <p>For organizations needing to provide remote network access, L2TP support enables local – rather than long distance – dial access through the Internet. It allows carriers and Internet service providers to offer new services to their customers.</p>
LDAP	<p>Lightweight Directory Access Protocol</p> <p>A protocol used to access a directory listing that makes multiple directories in an enterprise interoperable and manageable from a single point. LDAP support is being implemented in Web browsers and e-mail programs to allow them to query an LDAP-compliant directory. LDAP is expected to provide a common method for searching e-mail addresses on the Internet.</p> <p>LDAP in switches provides 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.</p> <p>LDAP v3 lacks fault tolerance and protection for reliable directory interoperability.</p>
MALLOC	<p>Multicast Address Allocation</p> <p>A dynamic multicast address allocation protocol that includes MASC (Multicast Address Set Claim) and AAP (Address Allocation Protocol).</p>
MARS	<p>Multicast Address Resolution Server</p> <p>Based on standard RFC2022: a component of Multiprotocol Over ATM (MPOA) to efficiently support multiple network protocols over ATM. See MPOA.</p> <p>Standard RFC2149 describes Multicast Server Architectures for MARS-based ATM multicasting.</p>
MBGP	<p>Multicast Border Gateway Protocol</p> <p>IP Multicast extensions to BGP (Border Gateway Protocol). See BGMP.</p>

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.

MFTP Multicast File Transport Protocol

A protocol for reliable data transport over IP multicast developed by StarBurst 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.

MOSPF Multicast Open Shortest Path First

Based on standard 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.

MPLS Multi-Protocol Label Switching

Designed to speed operation of cut-through routers performing IP switching over ATM and replace similar proprietary approaches such as Tag Switching (Cisco), IP Navigator (Ascend), ARIS (IBM), IP Switching (Ipsilon), and Cell Switch Routing (Toshiba). A major justification for MPLS is 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 is intended to provide end-to-end IP services that can scale gracefully to large ATM networks.

A standard development is underway within IETF, with ratification expected in Fall 1998. MPLS attaches a label to a packet with various attributes such as QoS. Security is dealt with separately: packets underneath the label can be encrypted with existing methods. Initial plans for MPLS are limited to handling IP only.

MPLS is expected to allow network service providers to reduce the costs associated with providing VPNs. MPLS will be directed toward large enterprise communications over high-speed ATM and frame relay backbones.. 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.

MPOA Multiprotocol over ATM

An ATM Forum standard 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 host and edge device on an MPOA-enabled network. The routing processing is separated from the traffic forwarding: the route server determines the routes and sends its results to the ATM switches and edge devices that forward the packets.
- Edge Devices connect traditional networks, such as Ethernet and Token-Ring, to ATM networks.
- ATM hosts are MPOA-enhanced LAN Emulation hosts directly attached to MPOA.

MPOA addresses the loss of performance caused by the increased number of router hops that packets make as networks become more complex. MPOA routers use IP routing tables to route IP packets between the source and the destination router by creating a virtual circuit between the source and destination. Although the traffic may go through several hops in the virtual circuit, additional routing information from the hop routers is not required 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.

Multihoming

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.

NAT Network Address Translation

Based on standard RFC1631: 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.

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.

NHRP Next Hop Routing Protocol

Defines 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.

OOPS Open Outsourcing Policy Services

IETF specification for managing QoS policy servers that use the COPS protocol. See COPS.

OSPF Open Shortest Path First

A router 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. Also see MOSPF (Multicast OSPF).

OSPF v3 is an updated version with minor changes that accommodate IPv6 – see IPv6.

PEPCI Protocol for Exchange of Policy Information

Draft IETF specification: a protocol to exchange policy information among a policy server and its clients.

PGM Pretty Good Multicast

A reliable transport protocol for IP Multicast developed by Cisco with contributions from Tibco Software Inc., submitted to IETF as a proposed standard. Multicast software developers GlobalCast Communications Inc. and Tibco Software Inc. are supporting it.

PIM Protocol-Independent Multicast

A multicast routing architecture that enables IP multicast routing on existing IP networks. 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: BBN Planet has already switched to PIM.

The Protocol-Independent Multicast Dense-Mode protocol is known as PIM-DM. 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 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. See I-PNNI.

POS Packet Over SONET

A protocol for carrying IP traffic over SONET and avoiding the “cell tax” overhead of ATM: the fixed-length cells of ATM add approximately 10 percent overhead. POS maps variable-length packets into SONET without incurring ATM’s overhead.

The larger carriers have invested heavily in an infrastructure based on ATM backbones so telco-centric users will have an affinity for ATM. ISPs are more likely to gravitate toward POS, though it is a newer technology and lacks the same breadth of infrastructure. Sprint launched the first OC-12 packet-over-SONET (POS) Internet network in late 1997.

PMC-Sierra is among the first SONET-chip vendors to provide POS support. Its PM5342 Spectra-155 integrated SONET framer IC maps T1/T3, ATM and frame relay, and IP using POS into 155 Mbps SONET pipes.

PPTP Point to Point Tunneling Protocol

A protocol that enables virtual private networking by encapsulating other protocols such as NetWare IPX for transmission over an IP network. PPTP is also used to create a private network (VPN) within the public Internet by taking advantage of its RSA encryption. Remote users can access their corporate networks via any ISP that supports PPTP on its servers.

The protocol 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 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.

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. See 802.1p and RSVP.

RARP Reverse ARP

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.

RIP Routing Information Protocol

Based on standards RFC1058, RFC1721, RFC1722, and RFC1723: 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 (RIP version 2) works the same way but adds support for subnet zero, classless IP, and some basic authentication. RIPv2 is the designation for a new version of RIP that handles the larger addresses associated with IPv6.

RMON Remote Monitoring

Standard RFC1757: 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.

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.
RSVP	Resource Reservation Protocol
	Based on standard RFC2205: a resource reservation setup protocol for IP networks that is being implemented by 802.1p and ATM. See 802.1p and ISSLL.
RTMP	Routing Table Management Protocol
	An AppleTalk routing protocol.
SAP	Service Advertising Protocol
	Protocol used in NetWare IPX networks to handle server name-to-network address resolution.
SBM	Subnet Bandwidth Manager
	Draft IETF specification for a 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.
S-HTTP	Secure Hypertext Transfer Protocol
	An extension of 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.
SLP	Service Location Protocol
	New IETF 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.
SNMP	Simple Network Management Protocol
	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).
	See RMON.
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
	<p>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.</p> <p>SSL is a leading security protocol on the Internet, and support for it is built into most browsers now. Also see S-HTTP.</p>
STS-1	For STS-1 through STS-48, see DS (Digital Signal).
T1	For T1 through T4, see DS (Digital Signal).
TCP/IP	Transmission Control Protocol-Internet Protocol
	<p>Based on standard IETF STD1: 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. For Ethernet networks, the maximum packet size is 1518 Bytes. Also see IP, UDP.</p> <p>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.</p>
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.
UDP	User Datagram Protocol
	A connectionless mode protocol that is part of the TCP/IP family. UDP allows an application to send a message to one of several other applications running on a remote or local machine. Data sent via the UDP protocol is not acknowledged and is considered unreliable. It can also be out of sequence and potentially duplicated.
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
	<p>An extension of ITU-T standards to provide recommendations for supporting voice communications over IP networks such as the Internet with compatibility between products from different manufacturers. Some incompatibilities exist now between various implementations due to the unfinished state of H.323 standards. VoIP is used mostly over private IP WANs so QoS can be assured.</p> <p>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.</p>

VPN	<p>Virtual Private Network</p> <p>A tunneled connection using PPTP over the public network that provides secure communications from a remote site. VPNs are also used for private communications over public networks using IPSec and MPLS, which are generally safer and more scalable than tunneling – see IPSec and MPLS.</p>
VRRP	<p>Virtual Router Redundancy Protocol</p> <p>An IETF initiative 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.</p>
VTOA	<p>Voice and Telephony over ATM</p> <p>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 proposal is being developed by the VTOA Working Group of the ATM Forum. VTOA requires implementation of one of two previous ATM Forum standards: UNI (User-Network Interface) 4.0 or PNNI (Private Network-Network Interface) 1.0.</p>
WBEM	<p>Web-Based Enterprise Management</p> <p>A system for unified administration of network, systems and software resources proposed by Microsoft, Intel, Compaq, Cisco, BMC Software, and others. It incorporates three new protocols to allow users to manage distributed systems using any Web browser:</p> <ul style="list-style-type: none"> • CIM (Common Information Model) defines the objects to be managed • Hypermedia Management Protocol (HMMP) handles information transport • Object Manager (OM) collects management data and acts as an interface to supporting applications. <p>As of early 1998, CIM v2.0 is being finalized by the DMTF (Desktop Management Task Force) organization, HMMP standardization is in limbo, and OS vendors are handling OM. Microsoft offers only a Beta version, and there have been many changes of direction.</p>

Notes