NCS TECHNICAL INFORMATION BULLETIN 04-2

INTERNET TECHNOLOGIES
IN A CONVERGED NETWORK ENVIRONMENT

December 2004

PROJECT OFFICER:	APPROVED FOR PUBLICATION:
David Nolan Computer Engineer Technology and Programs Division	PETER M. FONASH, Ph.D. Chief, Technology and Programs Division

FOREWORD

Future national security and emergency preparedness (NS/EP) telecommunications services will encompass various multi-media communications allowing users to exchange data, voice and video information. Market conditions are pushing many service providers to transition their networks and services to Internet Protocol (IP) technology by converging voice and data communications on the same physical network infrastructure. Anticipating this convergence, the NCS is looking for ways to provide assured communications for all applications using IP technologies. In November 2003, the NCS posted a Request for Information (RFI) on current industry IP capabilities and plans for future IP capabilities that might be used to support an Internet Priority Service (IPS) program for NS/EP users. This document provides synopsized descriptions of technologies mentioned in vendor responses, in addition to synopses of technologies discovered through independent research by the NCS. It has been prepared to inform interested Federal and industry activities. Any comments, inputs or statements of requirements which could assist in the advancement of this work are welcome and should be addressed to:

National Communications System
Attn: N2
P. O. Box 4502
Arlington, VA 22204-4502

ACKNOWLEDGEMENTS

Significant technical contributions were made by the following:

Wayne Austad, Idaho National Engineering and Environmental Laboratories

Dr. Edward Jacques, The Mitre Corporation

Steven Karty, National Communications System

Paul Martinez, Idaho National Engineering and Environmental Laboratories

Amy Nguyen, National Communications System

David J. Nolan, National Communications System

Bev Novak, Idaho National Engineering and Environmental Laboratories

Jeff Smith, National Aeronautics and Space Administration

Steve Williams, Idaho National Engineering and Environmental Laboratories

Technical editor: Valerie Liles, National Communications System

Table of Contents

Internet Technologies
In a Converged Network Environment

1 Introduction

In November 2003, the NCS posted a request for information [*RFI: Internet Priority Service (IPS) Capability Design/Development*] on current contractor/vendor Internet Protocol (IP) capabilities and plans for future IP capabilities that might be used to support an IPS program for NS/EP users. The NCS assembled a team of subject matter experts from various technical and programmatic areas to assess and compile the forty-seven (47) responses to the IPS RFI. The results of this effort, completed in June 2004, are published the *Internet Priority Service (IPS) Request for Information (RFI) Assessment Report.*

This TIB describes the non-proprietary concepts and protocols that were components of the responses, in addition to information obtained from sources such as standard bodies, technology forums, technology magazines, and professional organizations (e.g. IEEE, ITU, IETF, etc.). The technologies documented in this report are those that the NCS deems most likely to be used to meet the next generation networks (NGN) NS/EP functional requirements for IPS.

1.1 Background

The NCS, as directed by Executive Order 12472—*Assignment of national security and emergency preparedness telecommunications functions*, is responsible for the development of a national telecommunications infrastructure responsive to the national security and emergency preparedness (NS/EP) telecommunications needs of the President and federal departments and agencies.

The NCS defines and administers programs, such as the Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS), which provide priority access for critical users of the wire line and wireless resources of the Public Switched Telephone Network (PSTN) (for detailed information on these programs, go to www.ncs.gov). Although the emphasis of these services is on voice communications and voice band data transmission, NS/EP communications are expanding to encompass various multi-media communications to allow critical users to exchange and retrieve data and video information as well as voice. This use prompted the development of a priority service capability, via the Internet, for critical government and first responder use.

1.2 Convergence

Telecommunications market conditions are pushing many PSTN service providers to converge voice and data communications on the same physical network infrastructure, transitioning their networks and services from circuit-switched to packed-based (IP) technology. With the carriers' ongoing initiatives to migrate voice services, the NCS must ensure that GETS and WPS features will be enabled in the IP services domain.

To ensure reliability, security and Quality of Service (QoS), mission critical applications are normally deployed within an enterprise's private or managed IP network (e.g., dedicated circuits and/or services with no shared resources). The challenge the NCS faces is deploying an NS/EP IP service to customers that do not have a dedicated IP network infrastructure. These customers could use shared commodity IP services or Virtual Private Network (VPN) resources on their intranet as well as on inter-connectivity with other agency's networks; however, these connectivity solutions do not have QoS guarantees and constitute unrealistic approaches in that all agencies would need to deploy private networks and dedicated connections between agencies in support of NS/EP.

An IPS solution that fits within the NCS business model requires that QoS and priority are end-to-end among network providers. No carriers are currently providing a service within a public network environment where QoS and priority markings are recognized and acted upon throughout the entire network; however, there is a great deal of emphasis being placed on this general problem due to the increasing importance of data applications and the migration of voice services to the Internet.

1.2.1 Internet/Industry Business Model

Telecommunications carriers wish to migrate current voice and data services onto a single networking technology in order to save on life cycle costs associated with maintaining two separate networks. Adopting a single network technology for all services simplifies operations and mitigates high costs of maintaining many diverse technologies providing the same services. IP technology appears to be the preferred migration path for current voice services, as well as for evolving data and video services. Voice, data, and video services need to be ubiquitous through the high-speed optical backbone, fixed and mobile wireless, and other broadband networks. Today, the telecommunications industry recognizes that all of the capabilities in the circuit-switched world are not available using the current IP technologies.

Moderate congestion on inter-carrier peering links and even on intra-carrier links occurs daily on the Internet, and can result in packet loss, higher latency and jitter. Deploying QoS-sensitive applications, such as voice, in this environment requires additional priority and QoS guarantees—a large impediment to deploying IPS. The government must continue working closely with industry to develop a strong business case that serves both the industry and the government while upgrading the telecommunications infrastructure to support IPS communications. Within the NCS business model, IPS deployment requires Internet and IP-managed services to support priority services ubiquitously, and the effective control of priority traffic as it is transported among carriers.

1.2.2 Current Collaboration Efforts

Telecommunications and Internet service providers, government (NIST, DISA, DoS, DHS/NCS), and equipment manufacturers are participating in many forums supporting development of standards for advanced IP features and capabilities. Standards organizations supporting IP priority and Emergency Telecommunication Services (ETS) include the Internet Engineering Task Force (IETF), International Telecommunications Union (ITU), and Alliance for Telecommunications Industry Solutions (ATIS). The IETF is addressing inter-carrier traffic engineering requirements, and there are industry bodies and consortia, such as the "Infranet Initiative", addressing business impetus for deploying priority services in the Internet and exploring how standards can be deployed that are more sensitive to the quality concerns of the Internet users.

One area to be addressed by the ITU in its effort to develop global standards for NGNs is the concept of "nomadicity", which will give fixed line and mobile users completely seamless communications, so the underlying technology will be invisible to the user regardless of a multi-service, multi-protocol, multi-vendor environment. An ITU-T Focus Group plans to build on existing fixed/mobile convergence architecture (e.g., 3GPP/3GPP2 IP multimedia subsystem (IMS)) to provide transparency between fixed and mobile networks.

1.2.3 IPS Convergent Network Architecture

Figure 1-1 illustrates the concept of a converged telecommunications architecture that is Internet centric. In this concept, IP is the common network layer addressing scheme that provides applications and network control layer services between end-systems and the underlying telecommunications infrastructure. There is emerging consensus that IP will be the common network layer protocol across all services due to its robustness, scalability, and large deployed base. Major efforts are underway at both the control and service layers to develop protocols that bind the four layers in this model. An integrated architecture in which the application layer is able to control the lower layers of the network must be developed to meet service requirements. The current Internet architecture adequately provides connectivity between end-systems, but is unable to meet the reliability, security and QoS requirements of more advanced services such as emergency telecommunications, voice or video services.

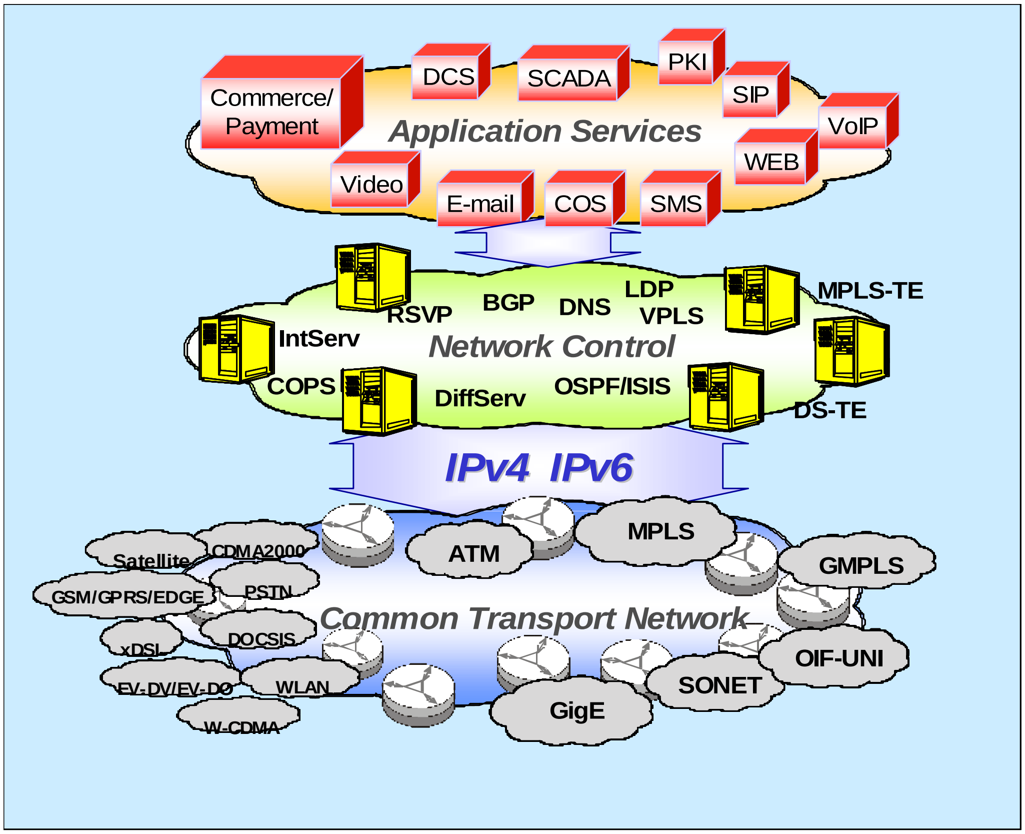

Figure 1-1. Converged Network Architecture

1.3 NGN Functional Requirements

The White House Communications Managers Working Group has developed a set of high-level functional requirements for NS/EP priority communications. From this set of requirements, the IPS must conform to the following functional requirements:

- Service Assurance – NS/EP national leadership must be assured constant availability of NS/EP user-to-user telecommunications services (wire line and wireless), without service degradation in stressed and hostile environments, with highest restoration priority in the event of loss or damage to facilities.

- Interoperability – NS/EP national leadership must be assured seamless systems and services interoperate with current and emerging government and public services systems and networks.

- Priority Treatment – In the event of crisis, NS/EP national leadership must receive end-to-end priority treatment over other users.

- Ubiquitous Coverage – NS/EP national leadership must be assured seamless connectivity to government and public services and systems regardless of location.

- Access and Identity – NS/EP national leadership must be provided the highest level of security against technological vulnerabilities. Features must include user anonymity, non-traceability, and protected access.

- Bandwidth Services – NS/EP national leadership requires assured access to government and public telecommunications services offering integrated high quality voice, scalable data and a full-range of video services for NS/EP telecommunications.

- Quality of Service – NS/EP traffic must be identified with its own class of service – beyond “best effort”.

2 Converged Network Technologies

2.1 Transport Layer

The transport layer encompasses the physical and link layers of the TCP/IP protocol model. This section discusses the major technologies associated with the transport layer having the greatest impact on IPS. Many protocols make up the transport layer, as shown in Figure 1.1. Many of the transport technologies have sub-components that reside in other layers of the protocol model. For example, MPLS is a layer 2.5 technology that binds the IP layer to lower physical layers. It also has significant related component protocols operating at the control layer in the protocol model. These sub-component parts are discussed appropriately in the network, control, or service layer sub-sections of this document.

2.1.1 Multi-Protocol Label Switching (MPLS)

MPLS defines a mechanism for packet forwarding in network routers. Originally developed to provide faster packet forwarding than traditional IP routing, the flexibility of MPLS has led to it become the default way for modern networks to achieve QoS, next generation VPN services, and optical signaling.

Traditional IP networks are connectionless. When a packet is received, the router determines the next hop using the destination IP address on the packet along with information from its own forwarding table. The router's forwarding tables contain information on the network topology. They use an IP routing protocol, such as OSPF, IS-IS, BGP, RIP or static configuration, to keep their information synchronized with changes in the network.

MPLS uses IP addresses, either v4 or v6, to identify end points and intermediate switches and routers. This makes MPLS networks IP-compatible and easily integrated with traditional IP networks. However, unlike traditional IP, MPLS flows are connection-oriented and packets are routed along pre-configured Label Switched Paths (LSPs).

Many carriers have deployed MPLS into their networks, making it an important technology for IPS. MPLS networks are able to achieve QoS through the underlying layer capabilities such as ATM Class of Service (CoS) or Ethernet 802.1P, as well as through Differentiated Services and traffic engineering extensions for Differentiated services (DS-TE). Increased reliability is obtained through MPLS via such things as MPLS fast-reroute and MPLS traffic engineering extensions. MPLS VPNs are able to meet security requirements of certain users by limiting outside connectivity to designated entry points within a network. LDP, RSVP-TE, and MPLS-TE are signaling components of the overall MPLS framework.

2.1.2 Gigabit Ethernet

Gigabit Ethernet (GigE) is an extension of the original IEEE 802.3 Ethernet specification and allows Ethernet to operate at 1 Gbps speeds. It is widely deployed in Internet exchange points, metro fiber networks and campus networks due to its simple architecture and the wide availability of low-cost GigE layer 3 switches. Additional specifications have extended the speed to 10Gbps. GigE switches are also interoperable with 10 and 100Mbps Ethernet formats. One of the features is its ability to provide CoS using the 802.1Q VLAN tag header, which provides marking for eight levels of priority. Currently, standards and implementations are not well developed to translate IP CoS (DiffServ) markings to Ethernet priority markings, although there are some means to manage policy through hardware vendor specific proprietary management applications. GigE is less vulnerable to security concerns as it is not implemented in a shared media configuration. There were no significant findings for this technology presented in any of the RFI responses.

2.1.3 Asynchronous Transfer Mode (ATM)

ATM is currently implemented to provide high bandwidth service for public carriers. ATM is normally deployed in conjunction with a Layer 1 SONET infrastructure. ATM is feature rich and offers many different services, but it’s slowly being replaced by other technologies that can offer more cost effective capacity and simplified management to integrate voice, video. One of the key aspects is its wide support by ANSI and ITU for carrying a complete range of user traffic for voice, video and data for any type of physical media. ATM scalability is limited due to the high cost of chip sets and limited number of implementations that can exceed OC-192 speeds, as IP device requirements are for operation at speeds up to OC-768.

ATM contains QoS capabilities for delivery of real-time traffic and other delay sensitive traffic. QoS is achieved through assignment of traffic to Constant Bit Rate (CBR), Variable Bit Rate (VBR) and Unspecified Bit Rate (UBR) CoS. For example, ATM CBR allows specification of a CoS to achieve controlled latency, jitter and throughput for real-time applications such as voice or video traffic.

The IETF has defined a suite of protocols for carrying IP traffic over ATM, and these standards not only address delivery of best effort traffic, but also standardize the use of RSVP to signal IP application requirements to the ATM infrastructure to allocate QoS resources. Since ATM is still deployed at the edges of many networks, ATM CoS will continue to be used as a means to deliver real-time traffic for the foreseeable future. However, the emergence of new technologies such as Dense Wavelength Division Multiplexing (DWDM), MPLS and GigE will more tightly integrate network management and provide higher performance for lower cost than ATM.

2.1.4 Synchronous Optical Networks (SONET)

SONET is a family of fiber optic transmission rates from 51.84 Mbps (OC-1) to 39.812 Gbps (OC-768) created to provide the flexibility needed to transport many digital signals with different capacities. Moreover, SONET is an optical interface standard that allows inter-working of transmission products from multiple vendors. SONET is widely deployed by carriers in a physical ring topology with fast switching between rings (50 milliseconds), with multiple fibers providing transport redundancy. SONET has been widely implemented within carrier domains and has only recently been challenged by DWDM, which, although it lacks robust network management standards, offers higher aggregate speeds and is far less expensive. SONET traditionally has been used to carry TDM traffic, which is considered inappropriate for IP traffic; other criticisms of SONET include bandwidth limitations, high overhead, and high costs of provisioning. The strongest argument for its continued use in the transport network arena is its strong network management capabilities, a strong set of standards, and the large embedded base of equipment used in carriers' networks.

SONET, in spite of its limitations, has a key role in the next generation telecommunications infrastructure. Carriers have considerable investment in their SONET networks and cannot see enough revenues coming from new services to justify building overlay networks. As a result, SONET will likely not be replaced by an all-optic network or by a native Ethernet transport network within the next ten years. SONET equipment manufactures are evolving their equipment offerings to conform to the carriers' requirements demanding affordable, standards-based platforms that are highly scalable and deliver packet and TDM services bot` seamlessly and without manual configuration. To achieve these goals, vendors are developing their products to span from the customer core, using advances in multi-protocol traffic adaptation, and developing their products for end-to-end operations management. Industry pundits predict that multi-service SONET platforms will be as fundamental to telecommunications networks in the coming decade as routers were to the Internet of the 1990s.

2.1.5 Optical Networking (GMPLS, OIF, VPLS)

Lambda Networking, also known as Wave Division Multiplexing (WDM), permits multiple communication channels over a single fiber by using different frequencies of light for each channel. In the past a single fiber could only transport a single "carrier", such as Synchronous Digital Hierarchy (SDH) or SONET. With WDM's ability to transport multiple SDH/SONET carriers over one fiber, the capacity of the existing fiber infrastructure is increased by orders of magnitude.

Lambda networking is provided as a commodity service by many telecommunication companies, most notably Qwest and Level3. WDM is also being used extensively throughout the High Performance Research and Education Networks like the National LambdaRail (NLR), and for connectivity with the Netherland's SURFnet and Canada's Canarie network.

While WDM is not an Internet technology in the IP world (i.e., it doesn't go up the protocol stack into the Layer3 area), it could be a promising transport layer technology for use in the IPS environment. WDM could be used to 1) provide another layer of security and 2) provide traffic segregation between voice, video and data. There may or may not be a business case for telecommunication companies to build out another transport layer infrastructure to support different service types, with MPLS VPN with QoS providing the features.

Lambda Switching is the next step in Lambda networking. To transition from one fiber to another, less expensive WDM devices convert the optical signal to an electrical signal, and then back into an optical signal (called "o-e-o"). Higher end WDM devices with the ability to receive, switch, and transmit optical signals without conversion are called "o-o".

Lambda uses three switching methods, as follows:

Manual Switching. Each optical trail is set up, hop-by-hop, by the operator's network management system (NMS), giving carriers the ultimate control over their network resources. It requires considerable configuration and monitoring, as backup paths have to be pre-configured at each stage to cope with failures. Typically, an offline routing package is used to calculate and re-optimize paths periodically, but it is always a human operator (using a network management system) who makes the actual changes.

Dynamic Switching. Industry is working towards a much more dynamic form of lambda switching, called Generalized MPLS (GMPLS), where MPLS control protocols are extended and generalized to operate with TDM and LSC interfaces. In a GMPLS network, electronic devices connect into the optical core over an Optical User Network Interface (O-UNI). In-band control information is assumed able to pass over the O-UNI.

Automatic Switching. Typically built as a 1x2 unit, protection switches are used to protect individual fibers against catastrophic failures such as a break or connector failure. They may be controlled by an external monitoring system, but may also have built-in detection for loss of signal on the primary fiber. In general, protection switches are relatively simple devices.

Lambda Networking is quickly becoming the transport mechanism of choice by the WAN telecommunications carriers as well as government agencies and academia. Many telecommunications companies offer WDM connectivity between their PoPs; however, gaining access to this transport technology is dependent on each customer's end locations. Obtaining Lambda connectivity end-to-end mostly depends on the fiber build out by the LECs—unless the LEC has adequate fiber resources to the customer's site, Lambda service will mostly like be cost prohibitive. This issue should not be a problem for large telecommunication carriers.

Lambda Networking has the ability to create separate data, video and voice networks over the same fiber infrastructure, thus significantly reducing the impact of congestion resulting from a national disaster.

2.1.6 Optical Internetworking Forum User Network Interface (OIF UNI) 1.0

The OIF UNI 1.0 enables clients to establish optical connections dynamically using signaling procedures compatible with GMPLS signaling. This, along with intelligence within the optical network, will allow provisioning to occur within seconds rather than days or weeks. In addition to signaling, the UNI specification includes two discovery mechanisms to simplify management of complex networks.

Neighbor discovery mechanisms permit equipment on both ends of a fiber link to identify each other and allow management systems to build interconnection maps automatically, reducing the cost of manually building such databases and minimizing errors in manual databases. Service discovery mechanisms enable clients to determine services available from the optical network and allow clients to automatically discover and take advantage of new optical network services as they are introduced over time.

The OIF approved the UNI 1.0 specification in December 2001. An interoperability demonstration of 25 different vendors illustrating a significant subset of the UNI 1.0 capabilities was shown in June 2001 at SUPERCOMM. The OIF is presently considering enhancements to UNI 1.0 ("UNI 2.0").

The impact of UNI 1.0 on IPS will depend on how the carriers proceed with converging networks. Carriers are trying to reduce recurring costs of their transport infrastructure. The UNI 1.0 control protocol could be used in conjunction with Lambda Networking to create separate data, video and voice networks over the same fiber infrastructure, thus significantly reducing the impact of congestion resulting from a national disaster. However, if the carriers' goals are to reduce infrastructure costs by eliminating duplicate transport infrastructure by combining voice, video and data, UNI 1.0 will have little or no benefit to IPS.

2.1.7 Access Technologies

2.1.7.1 Cable Modem

A cable modem is a modem designed to operate over a cable TV service facility. Because the coaxial cable used by cable operators provides much greater bandwidth than telephone voice-grade lines, a cable modem achieves extremely fast access to the World Wide Web. This, combined with the fact that millions of homes are already wired for cable TV, has made the cable modem something of an attractive 'need' for Internet and cable TV companies.

Theft of service is becoming more common on DOCSIS networks as the details of vulnerabilities are distributed by the press and on websites dedicated to helping subscribers understand how to steal service. The possibility of subscriber data theft or other violations of data integrity is increasingly problematic. Denial-of-service attacks such as Code Red and NIMDA have crippled CMTS devices and cable IP networks throughout the world.

However, the cable IP network can be made at least as secure as other common access media. The DOCSIS specifications, along with advanced features available on some CMTS platforms, enable cable operators to effectively combat security risks through simple means. Cable operators are accelerating deployment of security features such as DOCSIS shared secrets, BPI+, and other cable IP network features to mitigate all but the most aggressive attacks.

Because of the cable distribution architecture, some subscribers may see what sites other subscribers are visiting on the Internet. Current technology creates a sort of local area network allowing others on the same segment visibility of each other's data traversing the cable. Most ISPs have not yet addressed this problem.

For added security, some business customers have installed a router between their cable modem and LAN. Cisco Systems Inc. has developed the first integrated cable modem router product line. The Cisco uBR904 includes a standards-based DOCSIS cable modem, router with firewall capabilities, and four-port Ethernet hub in a compact design. Cisco's uBR924 adds two RJ-11 ports to support IP telephone and fax services. While this device is attractive for business users, it can only be used in markets where cable companies are offering cable modem services with standards-based DOCSIS equipment.

2.1.7.2 Data over Cable Service Interface Specification (DOCSIS) 1.1

Two international standards have emerged for cable modem products: DOCSIS, which is the standard in North America and other International markets, and EuroDOCSIS, which is the dominant standard in Europe.

The IEEE 802.14 Cable TV Media Access Control (MAC) and Physical (PHY) Protocol Working Group developed the DOCSIS Standard. This working group's goal was to develop an international cable modem standard by December 1995, but missed that target by more than two years. Tired of waiting, cable operators combined their purchasing power to jumpstart the standards process. In January 1996, MSOs Comcast, Cox, TCI (now AT&T), and Time Warner formed a limited partnership called Multimedia Cable Network System Partners Ltd. (MCNS) to research and publish their own cable modem system specifications. MediaOne Group, Rogers Cablesystems and Cable Television Laboratories Inc. also signed on to the initiative.

MCNS released its draft standard, called the Data over Cable Service Interface Specification (DOCSIS 1.0), to the manufacturing community in March 1997. Vendors immediately began building prototype products and the first public interoperability demonstration of DOCSIS equipment was held in December 1997. In early 1998, CableLabs began a formal certification program for DOCSIS equipment to ensure products built by different manufacturers are indeed compatible. In March 1998, the ITU accepted DOCSIS as a cable modem standard, called ITU J.112.

To deliver DOCSIS data services over a cable television network, one 6 MHz radio frequency (RF) channel in the 50 - 750 MHz spectrum range is typically allocated for downstream traffic to homes and another channel in the 5 - 42 MHz band is used to carry upstream signals. A head end cable modem termination system (CMTS) communicates through these channels with cable modems located at the customer premise. Most cable modems are external devices that connect to a personal computer through a standard 10Base-T Ethernet card or Universal Serial Bus (USB) interface, although internal PCI modem cards are also available.

CableLabs manages a certification process to ensure DOCSIS cable modems manufactured by different vendors comply with the standard and are interoperable. Those products that pass the tests earn the right to affix a seal marked "CableLabs Certified" to their DOCSIS cable modem packaging, informing buyers that the product is guaranteed to interoperate with other certified products.

In April 1999 CableLabs issued a second-generation specification called DOCSIS 1.1, which adds key enhancements to the original standard, such as improved QoS and hardware-based packet-fragmentation capabilities, to support IP telephony and other constant-bit-rate services. In short, DOCSIS 1.1 provides the bandwidth and latency guarantees required to offer toll-quality voice, dedicated business-class data services and multimedia applications across a shared cable modem access network. The next-generation standard is designed to be backward compatible, enabling DOCSIS 1.0 and 1.1 modems to operate in the same spectrum on the same network.

In addition to 1.1, CableLabs developed DOCSIS 2.0, a third-generation standard that adds an advanced PHY to the core specifications to increase upstream transmission capacity and reliability. DOCSIS 2.0 mandates the use of both frequency-agile time division multiple access (FA-TDMA) and synchronous code division multiple access (S-CDMA) technology.

EuroDOCSIS through ComLabs in Belgium, cable operators are certifying modems for compliance with a European version of the DOCSIS standard called EuroDOCSIS.

2.1.8 All types of Digital Subscriber Lines (xDSL)

xDSL designates generic Digital Subscriber Line (DSL) equipment and services such as provided by Asymmetrical Digital Subscriber Line (ADSL) and Synchronous Digital Subscriber Line (SDSL) services offered by LECs. xDSL technologies provide high bandwidth over twisted pair runs from the PSTN central office to residential customers or small business offices. SDSL lines provide the same bandwidth speed in both directions while ADSL creates three information channels — a high speed downstream channel, a medium speed duplex channel, depending on the implementation of the ADSL architecture, and a POTS (Plain Old Telephone Service) or an ISDN channel. Local phone companies have installed many xDSL loops to provide faster access to the Internet.

To compete with the success of the cable TV industry, xDSL equipment vendors have teamed up within the DSL Forum to outline a new framework for QoS-enabled IP services over DSL. A new proposed DSL architecture will support user-controlled, on-demand service provider and service level selection at the session and application level.

The DSL Forum's goal of standardizing the delivery of both existing best-effort and tiered QoS-enabled services over DSL promises to benefit the service provider community and equipment vendors. LECs hope that DSL deployment based on the DSL forum's architecture framework will provide an open mechanism for application service providers to augment overlay service offerings to end-users and generate new revenues from standard DSL connections. The biggest challenge faced by DSL service providers will be to make the new DSL architecture economically viable while still providing delivery of dynamic tiered bandwidth services and meeting IP QoS expectations.

DSL is still unavailable in many concentrated suburban areas with subscribers who are too far from the Telco Central Office. Fortunately, many of these areas are well served by cable modems.

2.1.9 Mobile Wireless

2.1.9.1 CDMA (Code-Division Multiple Access)

CDMA is a spread spectrum technology that allows many users to occupy the same time and frequency allocations in a given band/space by assigning unique codes to each communication. In a world of finite spectrum resources, this enables more people to share the airwaves at the same time. CDMA, the fastest growing wireless technology, was first used during World War II by the English allies to foil the German attempts to jam transmissions. Qualcomm was first to commercialize CDMA technology by creating communication chips; many cellular phone vendors, such as Lucent and Ericsson, now support CDMA.

2.1.9.2 CDMA 2000

CDMA2000, an evolution of an existing wireless standard, is a 3rd Generation (3G) solution based on IS-95 and supports 3G services defined by the International Telecommunications Union (ITU) for IMT-2000. Taking advantage of mobility and new market dynamics created by the Internet, it is designed to mitigate risks, significantly boost performance and protect investments. CDMA2000 also offers improvements in voice quality and capacity. The first phase of CDMA2000 (CDMA2000 1x) will deliver data at an average rate of 144 Kbps. The next phase (CDMA2000 1xEV) will deliver data at rates grater than 2 Mbps.

2.1.9.3 One-channel Radio Transmission Technology (1xRTT)

1xRTT (Single Carrier (1x) radio transmission technology): 1xrtt is a 3g wireless technology that is based on the CDMA platform. Part of the CDMA2000 specification, it can provide 40 to 60 kbps sustained rates, bursting up to 144 kbps for data applications.

2.1.9.4 Evolution Data Optimized (EV-DO)

ED-VO by Verizon Wireless provides wireless connections for laptops. It can provide longer, wider range coverage than Wi-Fi technology at speeds up to 300-500 Kbps sustained and burst rates to 2 Mbps. It does have drawbacks, however, in that it does not work in “dead spots” where a regular cell phone signal is weak. Users may also experience slower rates where Verizon depends on roaming agreements with other carriers. Verizon will be offering ED-VO for personal-digital assistance and cell phones.

2.1.9.5 3G Data Capabilities Variants

Wideband CDMA (W-CDMA) uses a chip that allows a rate of 4.096 Mbps, but because W-CDMA is not backward compatible to 2G systems, it will cost about $10 billion dollars to implement. W-CDMA is backed by mostly European and Japanese manufactures of cell phones. The current 2G providers would need to purchase new licenses for the 3G products.

2.1.9.6 CDPD (Cellular Digital Packet Data)

CDPD, supporting wireless access to the Internet and other public packet-switched networks, is an open specification that adheres to the layered structure of the Open Systems Interconnection (OSI) model. CDPD supports both the IP and the ISO Connectionless Network Protocol (CLNP), and IP multicast service which allows a company to send the same message to multiple people wirelessly. Because CDPD supports packet switching, a persistent link is not needed.

Many companies use CDPD technology, including the following service providers: Verizon Wireless, Earthlink Wireless, AT&T Wireless Services, Globicom Wireless, Telus Mobility, Alltel, and Arilink. Modem devices using CDPD technology include: Merlin PC Card CDPD Special Edition Win CE, Sierra Wireless MP 200 external serial RS232, Novatel Wireless Merlin PC Card, and AirCard 350 Network Adapter PC Card.

2.1.9.7 EMSS (Enhanced Mobile Satellite Services)

EMSS is an emerging technology that can support voice and data services from lightweight Iridium satellite phones. This service and the phones are commercially provided, but can be modified for unique U.S. government features – one being end-to-end encryption. The DISA has established an EMSS system for government and authorized non-DoD users such as customers in Australia, United Kingdom, Canada and New Zealand. A removable NSA-approved Type-1 Communication Security (COMSEC) sleeve can be placed over the phone for transferring classified data. General Dynamics Advance Information provides the service and the phones for the EMSS; they are working with Veridian Information Solutions, Inc.

2.1.9.8 GPRS (General Packet Radio Service)

GPRS is a non-voice value added service that supplements today’s Circuit Switched Data (CSD) and Short Message Service (SMS) and allows information to be sent and received across the wireless telephone network. Reaching speeds of 171.2 Kbps, GPRS is about three times faster than CSD, fully enabling Internet applications and, subject to radio coverage, allowing instant connections.

GPRS overlays a packet based air interface on the existing circuit switched GSM network. The information is split into separate but related packets and is reassembled at the receiving end, allowing the resources to be used only when the users are actually sending or receiving data. GPRS does affect the networks cell capacity. Nokia offers a GPRS phone; Cisco offers GPRS in their Gateway GPRS Support Node (GGSN) network; and Motorola offers a GPRS/ Edge product.

2.1.9.9 Layer 2 VPN

Layer 2 VPN is mainly based on an overlay model where the PE maps incoming Layer 2 traffic onto the appropriate point-to-point tunnel. Simple point-to-point tunnels are established on a provider's network to handle various forms of Layer 2 traffic (Ethernet, frame relay, ATM, TDM, and PPP/HDLC). From the peering aspect, CE routers peer with the CE router; but the PE router is not a peer to the CE router and does not maintain separate routing tables. No L3 processing of the customer packet takes place in the PE router. This is an advantage where direct interoperability with existing Layer 2 VPN deployments is important. The layer 2's MPLS "overlay" model is more attractive for carriers with existing Layer 2 VPN deployments. The disadvantages include a scaling problem. Layer 2 networks lack the scope of routed networks, limiting a Layer 2 implementation to the confines of the transport medium.

2.1.9.10 Layer 3 VPN

Layer 3 VPN is based on Peer-to-peer Model. Layer 3 MPLS VPN is implemented by using a two-level label stack. The ingress PE router pushes both a Next-Hop BGP header (for the private network) and a Next-Hop Interior Gateway Protocol (IGP) header (for the shared infrastructure) onto the packet. After reaching the egress PE router via one or more MPLS Label Switched Paths (LSPs), the PE pops the MPLS headers and delivers a normal IP packet to the customer. In this case, CE routers peer with PE routers. The advantages of a Layer 3 VPN are the ubiquity of Layer 3 IP networks over multiple transport networks. Multiple customers with IP running over different data link layers can form a Layer 3 VPN. Dynamic VPNs are also supported through strong automatic route discovery. Layer 3 VPNs are economical for ISPs using BGP extensively, with high-end IP/MPLS routing equipment at the edge; a disadvantage is its complexity and expense over traditional non-VPN connectivity.

2.2 Network (IP) Layer

IP is a network-layer (Layer 3) protocol in the OSI model that contains addressing information and some control information to enable packet routing in networks. IP is the primary network-layer protocol in the TCP/IP protocol suite and, together with TCP, represents the heart of Internet protocols. IP is equally well suited for both LAN and WAN communications.

2.2.1 IPv4

IPv4, the current version of the IP deployed worldwide, has proven remarkably robust, easy to implement, and interoperable with a wide range of protocols and applications. Though substantially unchanged since it was first specified in the early 1980s, IPv4 has supported the scaling of the Internet to its current global proportions and is used in most IP-based networks today; however, the success of IPv4 has actually emphasized its limitations. The most obvious limitation of IPv4 is its 32-bit address field, which, with approximately 4 billion addresses, is nearly exhausted. With the proliferation of networked devices including PCs, cell phones, wireless devices, etc., unique IP addresses are becoming scarce, and were it not for network address translation, the world could theoretically run out of IP addresses.

2.2.2 IPv6

IPv6, also called next generation IP or IPng, increases the IP address size from 32 bits to 128 bits, to support more levels of addressing hierarchy, a much greater number of addressable nodes and simpler auto-configuration of addresses. Scalability of multicast addresses is introduced and a new type of address, called an anycast address, will send a packet to any one of a group of nodes. Additional improvements over IPv4 include:

- Improved efficiency in routing and packet handling
- Support for auto configuration and plug and play
- Support for embedded IPSec-IPSec for end-to-end security
- Enhanced support for Mobile IP and mobile computing devices
- Elimination of the need for network address translation (NAT)
- Support for widely deployed routing protocols

In addition to addressing other limitations of IPv4, the IPv6 protocol promises to solve the address shortage completely with its 128-bit address. IPv6 packets have been simplified to speed up router processing and are labeled to provide QoS for priority applications such as real-time video and voice. IPv6 also natively offers improved security features with support for authentication and privacy. Designed as an evolution of IPv4, many IPv4 features remain in the new protocol and the two can coexist during the transition to a complete IPv6 internetworking environment.

IPv6 can be installed as a normal software upgrade in Internet devices. Its deployment strategy is designed for no ‘flag days’ or other dependencies. IPv6 is designed to run well on high performance networks (e.g. Gigabit Ethernet, OC-12, ATM, etc.) and still be efficient for low bandwidth networks (e.g. wireless). In addition, it provides a platform for new Internet functionality that will be required in the near future.

IPv6 includes a transition mechanism designed to allow users to adopt and deploy it in a highly diffuse fashion and to provide direct interoperability between IPv4 and IPv6 hosts. The IPv6 transition allows users to upgrade their hosts to IPv6, and the network operators to deploy IPv6 in routers, with very little coordination between the two.

2.2.3 Upgrading from IPv4 to IPv6

Some considerations for upgrading from IPv4 to IPv6 include:

- Individual IPv4 hosts and routers may be upgraded to IPv6 individually, without requiring any other hosts or routers to be upgraded at the same time. New IPv6 hosts and routers can be added one by one.

- The only prerequisite to upgrading hosts to IPv6 is that the DNS server must first be upgraded to handle IPv6 address records; there is no prerequisite to upgrading routers.

- When existing IPv4 hosts or routers are upgraded to IPv6, they may continue to use their existing address; new addresses and new addressing plans are not required.

- Little or no preparation work is needed to upgrade existing IPv4 systems to IPv6, or to deploy new IPv6 systems

IPv6 can improve user productivity by enabling network connectivity via a wider range of media and delivery mechanisms. While several end user environments and applications (e.g., Windows XP, Linux, sendmail) support IPv6 today, more applications are needed to enhance IPv6's overall acceptance.

Initial IPv6 development focuses primarily on the software level, to prove functionality. As the technology matures to mainstream deployment, implementation will move to the hardware level for ultimate performance. The new IPv6 routing protocols (e.g., OSPFv3, RIPng, ISISv6 and MBGP+) will need to process larger addresses and routes to achieve scalability similar to that of existing IPv4 networks. Service providers and network operators must properly characterize scalability in order to understand the impact of the new IPv6 design and to prevent bottlenecks. Tunneling will be a key technology to interconnect IPv6 islands during the early stage of IPv6 deployment. Since the scalability and performance of a tunneling mechanism depends on the number of tunnels a device can handle, this metric must be monitored and measured.

2.2.4 Mobile IP Defined

The mobile workforce must communicate with customers, partners, and fellow workers anywhere, anytime, and have access to relevant business applications and tools to conduct business effectively. Enterprise mobility provides ubiquitous connectivity to the mobile user independent of the devices and access technologies. Mobile IP, an IETF standard (RFC 2002), allows a host device to be identified by a single IP address even though the device may move its physical point of attachment from one network to another. Regardless of movement between networks, connectivity at different points is achieved seamlessly, without user intervention. Roaming from a wired network to a wireless or wide-area network is also done with ease. Mobile IP is part of both IPv4 and IPv6 standards.

Mobile IP routes packets from a source endpoint to a destination device through normal IP routing processes, with the cooperation of three separable mechanisms: discovering the care-of address, registering the care-of address and tunneling to the care-of address. To maintain existing transport-layer connections as the mobile node moves from place to place, it must keep its IP address the same. In TCP, a quadruplet that contains the IP addresses and port numbers of both endpoints indexes connections; changing any of these four numbers will cause the connection to be disrupted and lost. Mobile IP has been designed to solve this problem by allowing the mobile node to use both home and care-of IP addresses.

In Mobile IP, the home address is static, whereas the care-of address changes at each new point of attachment and indicates the network number—thus identifying the mobile node's point of attachment. The home address makes it appear that the mobile node is continually able to receive data on its home network. Whenever the mobile node is not attached to its home network, the home agent still gets all the packets destined for the mobile node and arranges to deliver them to the mobile node's current point of attachment. [This is a routing inefficiency currently being pursued in the IETF Mobile IP working group.]

When the mobile node moves, it registers its new care-of address with its home agent, and the home agent then moves a packet from the home network to the care-of address by constructing a new IP header containing the mobile node's care-of address as the destination IP address. The new header then shields or encapsulates the original packet, causing the mobile node's home address to have no effect on the encapsulated packet's routing until it arrives at the care-of address. Such encapsulation is also called tunneling, which suggests that the packet burrows through the Internet, bypassing the usual effects of IP routing. When the packet arrives at the care-of address, the reverse transformation is applied so that the packet once again appears to have the mobile node's home address as the destination IP address.

The Mobile IP method supports transparency above the IP layer, including the maintenance of active TCP connections and UDP port bindings. Where this level of transparency is not required, solutions such as DHCP and dynamic DNS updates may be adequate and techniques such as Mobile IP not needed.

2.3 Control Layer

Connectivity is the concept of any two IP end systems being able to communicate; DNS and BGP/IGP routing provide end-to-end connectivity within the global Internet. Systems resolve hostnames to IP addresses through DNS and intermediate systems (routers) forward packets to the correct network based on their destination IP address and the IP network address information distributed by BGP and IGPs.

Much of the Internet’s reliability is provided through fault tolerant designs within the control and transport layers. In the control layer, limited outages and non-availability of components does not adversely affect connectivity; for example, DNS maintains duplicate servers at the root and top-level domain so single/multiple outages cannot disable address lookup. BGP maintains knowledge of network topology and selects the best available path to forward packets along. Nonetheless, the Internet, being a best effort network, does not have the same reliability standards as the PSTN. Within every layer are numerous vulnerabilities that can be exploited by a range of factors, including malicious hacking, operator error and physical outages. Generally, performance or QoS suffers because of the congestion brought about by increased traffic generated by worms or viruses, or by alternate routing of traffic due to an outage.

As more mission critical applications use the Internet, QoS becomes more of a requirement. There are a range of requirements that different types of applications have for the Internet, nominally defined by packet loss, delay, throughput, and jitter. Degradation of these parameters affects each application differently. For example, packetized voice is an interactive real time streaming application requiring low jitter and low delay in order to maintain good voice quality. Interactive Web applications require low packet loss and delay to maintain good performance. File transfer requires high throughput to speed transactions. In general, all of these differing QoS requirements are competing for network resources. Non-streaming data applications such as Web and file transfer are bursty, and use large packets. When data competes with Voice, which uses small packets at a steady rate, the result is an increase in Jitter (decrease in quality) in the voice transmissions, since voice packets must wait in queue for data packets up to 24 times larger to be transmitted.

QoS is a major requirement for migrating TDM voice to VoIP; priority access for NS/EP traffic to available network resources is an additional requirement that control layer technologies must meet. The ability to reliably transition applications services from a normal operating environment to a degraded environment with loss of network resources should be contained within the control layer. Three IETF standards were proposed for providing QoS and reliability for an IPS: MPLS, Differentiated Services and Integrated Services.

2.3.1 Label Distribution Protocol (LDP)

LDP is often used to establish MPLS LSPs that follow the existing IP routing when traffic engineering is not required. LDP can operate in many modes to suit different requirements; however, the most common usage is unsolicited mode, which sets up a full mesh of tunnels between routers.

In solicited mode, the ingress router sends an LDP label request to the next hop router, as determined from its IP routing table, which is then forwarded on through the network by each router. Once the request reaches the egress router, a return message is generated confirming the LSP and telling each router the label mapping to use on each link for that LSP.

In unsolicited mode, the egress routers broadcast label mappings for each external link to all of their neighbors, fanning across every link throughout the network until they reach the ingress routers. Across each hop, they inform the upstream router of the label mapping to use for each external link, and by flooding the network, they establish LSPs between all of the external links. LDP is most often used in unsolicited mode due to the ease in setting up a full mesh of LSPs within a group of routers.

2.3.2 Multi-Protocol Label Switching-Traffic Engineering (MPLS-TE)

MPLS-TE (RFC 2702) is mainly used to provide QoS and load balancing across the network core, and includes the ability to control all-optical networks. Traffic engineering is the process of distributing load among elements of the network to reduce congestion and more evenly utilize network resources. Traffic can normally be identified and placed onto a separate LSP by Forwarding Equivalence Class (FEC), usually limited to a destination IP block from the BGP routing table. Extensions to BGP will also provide FECs that are more granular for QoS type and application type.

RSVP-TE (RFC 3209) is the signaling component of MPLS-TE that allows the use of source routing where the ingress router determines the complete path through the network. The ingress router can use a Constrained Shortest Path First (CSPF) calculator to determine a path to the destination, ensuring that any QoS and Shared Risk Link Group (SRLG) requirements are met. The resulting path is then used to establish the LSP.

2.3.3 Resource Reservation Setup Protocol (RSVP)

RSVP Aggregation (RFC 3175) uses a single RSVP reservation to aggregate other RSVP reservations across a transit routing region, in a manner conceptually similar to the use of Virtual Paths in an ATM. It proposes a way to dynamically create the aggregate reservation, classify the traffic for which the aggregate reservation applies, determine how much bandwidth is needed to achieve the requirement, and recover the bandwidth when the sub-reservations are no longer required

2.3.4 Multi-Protocol Label Switching (MPLS) Fast Re-route

MPLS fast re-route allows provisioning a redundant data path should a network interface or link fail. MPLS fast re-route is a Traffic Engineering technique intended to offer SONET-like failover times for IP traffic, on the order of 10s of milliseconds. Backup or detour LSPs can be established at each node and traffic can be switched immediately to this LSP, once a failure has been detected downstream of the backup LSP. A bypass tunnel can be used to merge a large number of LSPs onto a single backup path to reduce the number of alternate paths that must be maintained.

2.3.5 MPLS-VPN

MPLS-VPN traffic is isolated by the use of tags, much in the same way ATM and Frame Relay PVCs are kept isolated in a public ATM/Frame Relay network. This implies that security of MPLS-VPNs is equivalent to that of Frame Relay or ATM public network services. Interception of any of these three types of traffic would require access to the service provider network. MPLS-VPNs do not prohibit security; if security is an issue, traffic can be encrypted before it is encapsulated into MPLS by using a protocol such as IPSec or SSL.

2.3.6 Differentiated Services (DiffServ)

DiffServ enables a number of network node functional elements to provide different levels of service for different customers and types of traffic. The protocol includes a small set of per-hop forwarding behaviors, packet classification functions, and traffic conditioning functions including metering, marking, shaping, and policing. DiffServ defines a set of codepoints for marking traffic with class selector information for routers to rapidly identify traffic destined for priority handling. Prioritization is handled on a hop-by-hop basis; two sets of per-hop forwarding behaviors (PHB) have been defined. Expedited Forwarding (EF) (RFC 3246) consists of a single codepoint marking and is used to build a low loss, low latency, low jitter, assured bandwidth, end-to-end service through DiffServ domains. Often referred to as Premium service, it appears to the endpoints like a point-to-point connection or a "virtual leased line" and is normally used to deliver real-time traffic such as VoIP or Video—where packet loss and jitter control are crucial. Assured Forwarding (AF) (RFC 2597) enables a provider DiffServ domain to offer different levels of forwarding assurances. Each of four AF classes is allocated a certain amount of forwarding resources (buffer space and bandwidth); the customer or provider DiffServ domain assigns IP packets appropriate for the AF PHB group into one or more of these AF classes according to the services the customer has subscribed to. Normally, the AF PHB is used for providing service differentiation for data applications.

High priority and delay sensitive applications like interactive web or mission critical applications are assigned to the higher priority traffic class.

2.3.7 DiffServ Support for MPLS

DiffServ support for MPLS (RFC 3270) allows the MPLS network administrator to select how DiffServ Behavior Aggregates (BAs) are mapped onto LSPs to best match the Diff-Serv, Traffic Engineering and protection objectives within the network. For instance, this solution allows the network administrator to decide whether different sets of BAs are to be mapped onto the same LSP or mapped onto separate LSPs.

2.3.8 Differentiated Services Aware Traffic Engineering (DS-TE)

DS-TE is able to enforce different bandwidth constraints for different sets of Traffic Trunks. By mapping the traffic from a given DiffServ class of service on a separate LSP, it allows this traffic to use resources available to the given class on both shortest paths and non-shortest paths, and follow paths that meet engineering constraints (cost, performance and reliability) specific to the given class. DiffServ-aware Traffic Engineering (DS-TE) benefits networks with scarce bandwidth, significant amounts of delay sensitive traffic, or non-uniform proportions of traffic across the supported classes of service.

DS-TE (RFC 3564) proposes several models to provide bandwidth management/resource allocation for MPLS tunnels. One method is the Maximum Allocation Model (MAM) in which the maximum allowable bandwidth usage of each Class Type (CT) is explicitly specified. In the Russian Doll Model (RDM), the maximum allowable bandwidth usage is done cumulatively by grouping successive CTs according to priority classes. Under the Maximum Allocation Resource (MAR) model, a maximum bandwidth allocation is given to each CT. Through bandwidth reservation and protection mechanisms, CTs are allowed to exceed their bandwidth allocations under conditions of no congestion, but must revert to their allocated bandwidths when overload and congestion occurs.

Modeling results show that MAR improves performance over methods lacking bandwidth reservation and allowing more bandwidth sharing under congestion, such as MAM and RDM. MAR achieves service differentiation for high-priority, normal-priority and best-effort priority services. Bandwidth reservation supports greater efficiency in bandwidth sharing while providing bandwidth isolation and protection against QoS degradation, and is critical to stable and efficient network performance. [www.ietf.org/internet-drafts/draft-ietf-tewg-diff-te-mar-04]

2.3.9 Inter-AS MPLS-TE

While there are other means of traffic engineering, including IGP metrics based (for use within an AS) and BGP attribute based (for use across ASs), these means offer coarser control of traffic paths and do not readily offer bandwidth guarantees or fast restoration. In Inter-AS MPLS-TE, either the head-end LSR (label switched router) and tail-end LSR do not reside within the same AS, or both head-end LSR and tail-end LSR are in the same AS but the TE LSP transiting path is across different ASs. Inter-AS bandwidth guarantees regarding a set of QoS policies are required, which can be expressed in terms of maximum one-way transit delay, inter-packet delay variation, loss rate, etc. Many service providers have partial or full deployment of DiffServ implementations in their networks today, either across the entire network or at least on the edge of the network, across CE-PE links. In situations where strict QoS bounds are required, admission control inside the backbone of a network is sometimes required in addition to current DiffServ mechanisms. Other requirements for Inter-AS TE are being pursued in the IETF Traffic Engineering working group and include more granular mechanisms than the current BGP based TE and fast recovery mechanisms across ASs. These requirements are a large step towards ubiquitous QoS and priority based Internet necessary to meet IPS requirements; however, this work is in its early stages, as protocols are not yet defined.

2.3.10 Integrated Services (IntServ)

The IntServ framework provides the ability for applications to choose among multiple controlled levels of delivery service for their data packets. The focus is on long-lived Unicast and multicast flows to guarantee QoS requirements through the complete path, from the sender to the receiver. To support this capability, two things are required:

- Individual network elements (subnets and IP routers) along the path followed by an application's data packets must support mechanisms to control the quality of service delivered to those packets.

- Find a way to communicate the application's requirements to network elements along the path and to convey QoS management information between network elements and the application.

In the integrated services framework the first function is provided by QoS control services such as Controlled-Load [RFC 2211] and Guaranteed [RFC 2212]. The second function may be provided in a number of ways, but is frequently implemented by a resource reservation setup protocol such as RSVP [RFC 2205]. RSVP uses objects to convey the senders traffic specification (SENDER-TSPEC), the data path properties (ADSPEC), and the receivers reservation request (FLOWSPEC).

The IntServ model permits nodes in the path to support or not support RSVP. If a node does not support RSVP, the setup message will pass through transparently; only nodes supporting RSVP will reserve resources. IntServ are implemented in the current generation of Internet routers and hosts, but have significant limitations to an IPS. These limitations are with respect to the number of flows classified, the number of queues that can be serviced or scheduled, and the number of messages that are processed. In the IPS architecture, RSVP capable routers will likely occur only at the edge of the network where interface speeds are DS1 or lower and the number of RSVP messages is limited. Scaling of IntServ to an Internet wide configuration supported on every router hop is unlikely due to the sheer number of individual flows that would have to be signaled and processed in queues in the core of the network. Nevertheless, the model supports a hybrid approach where only certain nodes in key congested locations deploy IntServ in support of Internet telephony. DiffServ will also be used in core routers where large numbers of flows do not permit the deployment of IntServ.

2.3.11 RSVP

RSVP is designed to be used with a variety of QoS control services, and because the QoS control services are designed to be used with a variety of setup mechanisms, a logical separation exists between the two specifications. The RSVP specification does not define the internal format of those RSVP protocol fields or objects related to invoking QoS control services; rather, RSVP treats these objects as opaque. The objects can carry different information to meet different application and QoS control service requirements. Similarly, interfaces to the QoS control services are defined in a general format, so the services can be used with a variety of setup mechanisms. RSVP is primarily used for setting up MPLS traffic engineered flows and for setting up Integrated Services (RFC 2205) per session microflows.   RSVP also has optical extensions to include the ability to signal optical wavelengths and shared risk link groups, as well as bandwidth, latency and other link characteristics.

2.3.12 Common Open Policy Service Protocol (COPS)

COPS is a query response protocol used to exchange policy information between a network policy server and a set of clients, supporting policy control over QoS signaling protocols. COPS is being developed within the RSVP Admission Policy Working Group (RAP WG) of the IETF, primarily for use as a mechanism for providing policy-based admission control over requests for network resources. A client/server model where the PEP sends requests, updates, and deletes to the remote PDP and the PDP returns decisions back to the PEP. The state of various transactions is held by the PDP and affects future requests.

2.3.13 IPv6 Flow Label

A new capability within IPv6 involves labeling packets belonging to particular traffic "flows" for which the sender requests special handling, such as non-default QoS or "real-time" service (RFC 2460 – IPv6 Specifications).

The 24-bit Flow Label field in the IPv6 header may be used by a source to label those packets for which it requests special handling by the IPv6 routers, such as non-default quality of service or "real-time" service. This aspect of IPv6 is still somewhat experimental and subject to change as the requirements for flow support in the Internet become clearer. Hosts or routers that do not support the functions of the Flow Label field are required to set the field to zero when originating a packet, pass the field on unchanged when forwarding a packet, and ignore the field when receiving a packet.

A flow is a sequence of packets sent from a particular source to a particular (unicast or multicast) destination for which the source desires special handling by the intervening routers. The nature of that special handling might be conveyed to the routers by a control protocol, such as a resource reservation protocol, or by information within the flow's packets themselves, e.g., in a hop-by-hop option.

2.4 Applications Service Layer

2.4.1 Session Initiation Protocol (SIP)

SIP is an emerging standard for setting up telephone calls, multimedia conferencing, instant messaging, and other types of real-time communications on the Internet. SIP is at the application layer and is advertised as being much faster, more scalable, and easier to implement than H.323. There is an array of network equipment such as IP phones, IP PBXs, servers, media gateways, and softswitches implementing the SIP protocol. The SIP protocol is used for the establishment, modification, and termination of conferencing and telephony sessions over an IP-based network. SIP uses text-based messages much like HTTP, was developed by the IETF, and is defined in RFC 2543. SIP addressing is built around either a telephone number or a Web name. SIP can negotiate the session's features and capabilities at the time a session is established. As an example, a caller might establish a call using G.711 audio and H.261 video. The advanced negotiation process using the session description protocol (SDP) is claimed to greatly reduce the call set-up required for H.323 sessions. One particular feature of the SIP is the ability to modify the session's capabilities during the course of a session (call).

Microsoft has chosen to use SIP in its servers and several iPBX vendors (e.g. Cisco) are developing SIP products as well. A recent SIP published report indicated that over 47 companies with over 78 products have already been developed or are in development. Moreover, dozens of vendors are now offering SIP-based or SIP-supported platforms, although few are carrier grade. Softswitch makers, such as Lucent and Nortel, have added SIP support to their softswitches although most of them are positioned primarily as replacement for public network switches. Full SIP implementations are not expected to be available from carrier-grade network equipment vendors until a full transition is made to an IP-based architecture.

2.4.2 Instant Messaging (IM)

IM is an Internet application that provides users the ability to see whether chosen friends and co-workers are connected to the Internet. Instant messaging differs from ordinary e-mail in the immediacy of the message exchange, and makes a continued exchange simpler than sending e-mail back and forth. IM exchanges are mostly text and sometimes voice messaging and file sharing.

The current problem with IM is interoperability; that is, none of the IM applications can inter-work with one another because each application is based on different sets of protocols. For example, AOL's own proprietary IM application cannot interconnect with other IM applications. Even though an Instant Messaging and Presence Protocol (IMPP) standard interface is available from the IETF, IM vendors are reluctant to implement it for business competition reasons.

2.4.3 Electronic Mail (E-Mail)

Electronic Mail (E-mail) is the exchange of computer-stored messages by telecommunications and is based on the Simple Message Transfer Protocol (SMTP) to transport mail across networks. E-mail messages are usually encoded in ASCII text; however, you can also send non-text files, such as graphic images and sound files, in binary stream attachments. E-mail can be distributed to lists of people as well as to individuals.

Although RFC 2821 describes how to implement SMTP, there is no consistent SMTP standard implementation for message priority across email applications. An option for users is to create rules using the X-Priority field within the email header to specify the priority. In most cases, the value for X-Priority ranges from 1-5, and most email applications use an X-Priority value of 3 for messages with "normal" priority, and 1 for urgent messages. Email software vendors currently implement SMTP programs without preferential treatment because email spammers can take advantage of this priority feature to flood a user's mailbox.

The NCS could use one of the values in the X-Priority field to flag emergency email, and will work with standards organizations and software vendors to implement SMTP programs to recognize and process an X-Priority value for NS/EP users. In times of congestion in email queues, a unique value would enable an SMTP program to selectively process email messages for NS/EP users first and provide appropriate authentication and encryption accordingly. Once the X-priority value is supported by standards organizations and implemented by vendors, NS/EP users can securely set the X-Priority value to send emergency email.

2.4.4 World Wide Web (WWW)

World Wide Web (WWW) is based on the Hypertext Transfer Protocol (HTTP), which is an application protocol using a set of rules for transferring files such as text, graphic images, sound, video, and other multimedia files. HTTP uses client/server technology; a web browser is on a client side and a web server is on a server side. As soon as a Web user opens their Web browser and enters a Uniform Resource Locator (URL) in it, the user is indirectly making use of HTTP to send requests to server machines. A Web server machine contains a HTTP daemon (a web server program), which is designed to wait for HTTP requests and handle them when they arrive.

2.4.5 Border Gateway Protocol (BGP)

Border Gateway Protocol (BGP) is a protocol for exchanging routing information between gateways of a network of autonomous systems (ASs). An AS is a unit of router policy and is either a single network or a group of networks that is controlled by a common network administrator. BGP is often the protocol used between gateway routers on the Internet. The routing table contains a list of known routers, the addresses they can reach, and a cost metric associated with the path to each router so that the best available route is chosen. Gateway routers use BGP protocol (which runs on top of TCP) to send updated router table information only when one host has detected a change (only the affected part of the routing table is sent). BGP enables ASs to be interconnected.

2.4.6 Domain Name System (DNS)

Domain Name System (DNS) is the way that the Internet domain names (e.g., www.ncs.gov, etc.) are located and translated into Internet addresses (e.g., 162.117.148., etc.). A domain name is a meaningful mnemonic that translates to an Internet address. To keep one central list of domain names and their corresponding IP addresses is impractical and prone to denial-of-service attacks.

The lists of domain names and IP addresses are distributed throughout the Internet in a hierarchy of authority. A DNS server within close geographic proximity to a user's access provider usually maps the domain names in his Internet requests or forwards them to other servers in the Internet.

Because DNS is a critical service and one of the fundamental building blocks of the Internet, DNS Security Extension (DNS-SEC) was introduced to provide end-to-end authentication and integrity, and is designed to protect the Internet from certain attacks. All answers in DNS-SEC are digitally signed. By checking the signature, a resolver is able to check if the information is identical (correct and complete) to the information on the authoritative server.

2.4.7 Short Message Service (SMS)

Short Message Service (SMS) is a service for sending messages of up to 160 characters to mobile phones—similar to paging but without requiring the mobile phone to be active and within range (messages are held for a number of days until the phone is active and within range). SMS messages are transmitted within the same cell or to anyone with roaming service capability. They can also be sent to digital phones from a Web site equipped with PC Link or from one digital phone to another.

2.4.8 Session Initiation Protocol (SIP)

Session Initiation Protocol (SIP) is an IETF standard protocol for initiating an interactive user session that involves multimedia elements such as video, voice, chat, gaming, and virtual reality. SIP can establish, modify, or terminate multimedia sessions or Internet telephony calls, and can invite participants to unicast and multicast sessions that do not necessarily involve the initiator. Because SIP supports name mapping and redirection services, it makes it possible for users to initiate and receive communications and services from any location, and for networks to identify the users wherever they are.

Videoconference: A videoconference is a live connection in the Internet between people in separate locations for the purpose of communication, usually involving audio and often text as well as video. At its simplest, videoconferencing provides transmission of static images and text between two locations; at its most sophisticated, it provides transmission of full-motion video images and high-quality audio between multiple locations.

Voice over Internet Protocol (VoIP): VoIP is a way to deliver voice over the Internet. In general, this means sending voice information in digital form in IP packets rather than in the traditional circuit-committed protocols of the public switched telephone network. There are three flavors of VoIP: H.323, SIP and Media Control Gateway Protocol (MCGP). These three use the Real Time Protocol (RTP) to help ensure that packets get delivered in a timely way. It is difficult to guarantee any QoS for VoIP using public networks. Better service is possible with private networks managed by an enterprise or by an Internet telephony service provider.

3 Security Technologies

The primary drivers for IPS security can be categorized into three areas: confidentiality, integrity, and availability. IPS confidentially addresses a hacker's ability to eavesdrop on data streams, determine the origin or destination of user traffic, and the ability to learn about the overall network infrastructure. Integrity of information addresses concerns about caller identity, authentication of devices to prevent rogue devices impersonating applications and altering traffic. Availability deals with the ability to resist attempts to degrade the ability to provide service to the users.

Confidentiality:

- Can hackers eavesdrop on data streams?
- Can call traffic be analyzed to determine the caller and called-party and the origin and destination of the traffic?

- Can components of the network system be attacked to learn about the overall infrastructure such as call managers and gatekeepers in order to plan additional attacks?
- Can the IPS be attacked in such a way to call an IP or soft phone and eavesdrop on office conversations?

Integrity:

- Is the caller who he says he is?
- Are devices authenticated by the IPS to prevent attachment of rogue devices that can steal service and impersonate applications (or persons)?
- Is the IPS vulnerable to man-in-the-middle attacks?
- Can the stream traffic be altered in transit?
- Are administrative support interfaces secured to require authentication before allowing access to or modification of equipment?

Availability:

- Can call managers, gatekeepers, and proxies resist malicious traffic designed to cause resets or failures?
- Can equipment be reconfigured trough remote or local interfaces or can the configuration server instruct devices to hang-up, automatically resulting in denial of service?

3.1 BGP Filtering and Secure BGP (S-BGP)

BGP Filtering is a way to get BGP updates from neighboring routers. Access lists are created to define and apply the updates to or from a neighboring router, setting up a trusted group from which a router can be updated. BGP Filtering allows the router to determine the fastest route to get the data to the destination.

S-BGP secures Internet routing from false routing updates and DOS type of attacks. It will run only at the edge of a service provider network to secure control traffic that crosses between autonomous systems (ASs). The protocol uses IPSEC, digital signatures, PKI, and a hierarchy of registry servers that accompanies the protocol software running on routers. S-BGP allows individual ISPs to register their network attributes and other ISPs to validate the control traffic they receive. It permits other routers not running S-BGP to remain in the network, permits changing routes in real time (without registration), and does not change the route selection process. Adding new networks involves a registration time lag, however.

S-BGP protects three pieces of the routing system, and when combined with various protections afforded at the transport layer and the addition of some simple policies, is able to eliminate most (if not all) of the attacks a single network operator could make against another network operator, or against the network. Each AS creates and advertises PKI certificates that contain the following four types of information: the AS and its public key; what the AS is authorized to advertise (such as routes, adjacencies, and other information); other AS connections; and policy concerning advertised routes that other AS connections should follow. Essentially, these four items convey an AS's authority to advertise a given block of IP addresses, confirm that the path from the device advertising a given destination can reach that destination, and verify the policies of the "originating AS" with respect to a particular block of IP addresses.

3.2 Distributed Denial of Service (DDOS)

This type of attack is produced when a multitude of compromised systems attack a single target. When the system is flooded by the incoming messages, it is forced to shutdown. This exploit is accomplished by gaining control of several vulnerable computer systems and causing a flood attack on a single target system. Once the intruder has control of the systems, he sends one command to instruct the controlled systems to launch on of many flood attacks against the target system. Many of the IPS RFI proposals can defend against these attacks by making the system secure so hackers cannot break in to them.

3.3 Encryption

Encryption helps to secure data being sent across the network. Various encryption methods include:

3.3.1 Data Encryption Standard (DES)

IBM developed DES, originally called Lucifer, in 1974. This algorithm encrypts and decrypts blocks of 64-bits with a 64-bit key. In 1977, DES was the first encryption algorithm adopted by NIST. DES runs the main algorithm 16 times to produce the cipher text; using both permutations and substitutions. DES is both a product cipher and a block cipher.

DES algorithm has been broken by brute force attacks. It has gotten easier to discover the 64-bit key as computers increased in speed and computing power. In 1997, NIST abandoned their official endorsement of DES and began work on AES;; however, many financial services and other industries still use DES as their encryption algorithm.

3.3.2 Triple Data Encryption Standard (3DES)

3DES is a modification of the DES algorithm, fixing many of its shortcomings. Although three times slower, 3DES is much more secure, using three 64-bit keys to make an overall key of 192 bits. The entire 192-bit key is typed in and the algorithm breaks it up in to the 64-bit keys, padded if necessary. If the three keys are identical then it is just like running the original DES algorithm. 3DES was endorsed by NIST as a temporary standard until AES was completed.

3.3.3 Advanced Encryption Standard (AES)

In 2001, NIST adopted the Rijndeal algorithm as the official AES algorithm. Rijdael is a block cipher algorithm designed by Joan Daemen and Vincent Rijmen, and uses a variable block and key lengths. These lengths can be 128, 192 or 256 bits. All nine combinations of the three-block length and three-key lengths are possible in this algorithm.

3.3.4 IP Security Virtual Private Network (IPSEC VPN)

Offered by many different companies, this tool is used to build a secure tunnel for computers to communicate with each other. IPSec provides a mutual authentication between the user’s computer and the VPN server. It also provides a strong encryption of the data being exchanged between the client and server.

Virtual Private Network (VPN) RFC 2547 bis: The Standard RFC 2547-bis defines the interaction between BGP- Multi-protocol Label Switching (MPLS) and VPN.

3.3.5 Public Key Infrastructure (PKI)

PKI integrates digital signatures, Public Key Cryptography (PKC), and Certificate Authority (CA) into a security system. Digital signatures, created by PKC and CA tools, put a time stamp on the object being signed; many states have adopted the digital signature as a valid signature. PKC, invented in 1976, is sometimes called *Diffie-Hellman encryption* or *asymmetric encryption* because not all parties hold the same information. The CA assigns the keys; the public key is kept in a database type system and the private key is placed on a device that the user carries around (like a smart card or badge). The CA validates the two keys to allow the user access to the system. .

3.3.6 RADIUS/Authentication, Authorization and Accounting (AAA)

Radius is a server that provides AAA. This is one of the more popular systems used today to authenticate users before allowing them on to a system, and many companies supply Radius software. This is one way to make sure only authorized people access a system.

3.3.7 RSA SecureID®

RSA Security developed the RSA SecureID® software to be used for authentication. This product is a two-part authentication based on something the user knows, like a password or PIN, and something the user has (an authenticator). This provides a more reliable level of user authentication then a reusable password.

3.3.8 Secure Socket Layer (SSL)

SSL is the most widely deployed system used for security on the Internet. It provides three important security capabilities: server authentication to the client, confidentiality of the transmitted data, and client authentication, like a password, to the server. The authentication uses a digital certificate that is installed on the server. This certificate has a domain contained in it that must match the actual domain of the server. Confidentiality is provided by the activation of the SSL protocol. SSL protocol is built into all common Web and application servers. It does an initial secret key exchange and cryptographic protocol negotiation, that is used to encrypt all the data being transmitted between the client and server. It also optionally supports mutual or two-way authentication. The server requires a certificate from the client to verify the identity of the client before the data is transmitted. Digital certificates used by SSL can be acquired quickly from various public Certificate Authorities (CAs), such as VeriSign, Entrust and GeoTrust.

3.3.9 Extensible Messaging and Presence Protocol (XMPP)

XMPP is an open, XML-based protocol for near real-time extensible messaging and presence. The Internet Engineering Steering Group (IESG) has approved XMPP Core specification as an IETF Proposed Standard. XMPP is used mainly to build instant messaging and presence applications that meet the requirements of RFC 2779 Instant Messaging/ Presence Protocol Requirements. Instant messaging allows user to communicate with each other via an application common on each machine.

4 Acronyms

1XRTT	SINGLE CARRIER RADIO TRANSMISSION TECHNOLOGY

2G	2ND GENERATION
3DES	TRIPLE DATA ENCRYPTION STANDARD
3G	3RD GENERATION
3GPP	THIRD GENERATION PARTNERSHIP PROJECT
3GPP2	THIRD GENERATION PARTNERSHIP PROJECT TWO
AAA	AUTHENTICATION, AUTHORIZATION AND ACCOUNTING
ADSL	ASYMMETRICAL DIGITAL SUBSCRIBER LINE
AES	ADVANCED ENCRYPTION STANDARD
AF	ASSURED FORWARDING
ANSI	AMERICAN NATIONAL STANDARDS INSTITUTE
AS	AUTONOMOUS SYSTEM
ATIS	ALLIANCE FOR TELECOMMUNICATIONS INDUSTRY SOLUTIONS
ATM	ASYNCHRONOUS TRANSFER MODE
BGP	BORDER GATEWAY PROTOCOL
BPI+	BASELINE PRIVACY INTERFACE
CA	CERTIFICATE AUTHORITY
CBR	CONSTANT BIT RATE
CDMA	CODE DIVISION MULTIPLE ACCESS
CDPD	CELLULAR DIGITAL PACKET DATA
CE	CUSTOMER EDGE
CLNP	CONNECTIONLESS NETWORK PROTOCOL
CMTS	CABLE MODEM TERMINATION SYSTEM
COMSEC	COMMUNICATIONS SECURITY
COPS	COMMON OPEN POLICY SERVICE
COS	CLASS OF SERVICE

CSD	CIRCUIT SWITCHED DATA
CSPF	CONSTRAINED SHORTEST PATH FIRST
CT	CLASS TYPE
DES	DATA ENCRYPTION STANDARD
DHCP	DYNAMIC HOST CONFIGURATION PROFILE
DHS	DEPARTMENT OF HOMELAND SECURITY
DIFFSERV	DIFFERENTIATED SERVICES
DISA	DEFENSE INFORMATION SYSTEMS AGENCY
DNS	DOMAIN NAME SYSTEM
DNS-SEC	DNS SECURITY EXTENSION
DOCSIS	DATA OVER CABLE SERVICE INTERFACE SPECIFICATION
DOD	DEPARTMENT OF DEFENSE
DOS	DEPARTMENT OF STATE
DS-TE	DIFFERENTIATED SERVICES - TRAFFIC ENGINEERING
DWDM	DENSE WAVELENGTH DIVISION MULTIPLEXING
EF	EXPEDITED FORWARDING
EMSS	ENHANCED MOBILE SATELLITE SERVICES
ETS	EMERGENCY TELECOMMUNICATION SERVICES
FA-TDMA	FREQUENCY-AGILE TIME DIVISION MULTIPLE ACCESS
FEC	FORWARDING EQUIVALENCE CLASS
GBPS	GIGABITS PER SECOND
GETS	GOVERNMENT EMERGENCY TELECOMMUNICATIONS SERVICE
GGSN	GATEWAY GPRS SUPPORT NODE
GIGE	GIGABIT ETHERNET
GMPLS	GENERALIZED MULTI-PROTOCOL LABEL SWITCHING

GPRS	GENERAL PACKET RADIO SERVICE
HTTP	HYPERTEXT TRANSFER PROTOCOL
IEEE	INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS
IESG	INTERNET ENGINEERING STEERING GROUP
IETF	INTERNET ENGINEERING TASK FORCE
IGP	INTERIOR GATEWAY PROTOCOL
IMPP	INSTANT MESSAGE AND PRESENCE PROTOCOL
IMS	IP MULTIMEDIA SUBSYSTEM
IMT	INTERNATIONAL MOBILE TELECOMMUNICATIONS
INTSERV	INTEGRATED SERVICES
IP	INTERNET PROTOCOL
IPS	INTERNET PRIORITY SERVICE
IPSEC	INTERNET PROTOCOL SECURITY
IS-IS	INTERMEDIATE SYSTEM - INTERMEDIATE SYSTEM
ITU	INTERNATIONAL TELECOMMUNICATIONS UNION
ITU-T	ITU TELECOMMUNICATIONS STANDARDIZATION SECTOR
L3	LAYER 3
LDP	LABEL DISTRIBUTION PROTOCOL
LEC	LOCAL EXCHANGE CARRIER
LSC	LAMBDA SWITCH CAPABLE
LSP	LABEL SWITCHED PATH
LSR	LABEL SWITCHED ROUTER
MAC	MEDIA ACCESS CONTROL
MAM	MAXIMUM ALLOCATION MODEL
MAR	MAXIMUM ALLOCATION RESOURCE

MCNS	MULTIMEDIA CABLE NETWORK SYSTEM PARTNERS LTD.
MGBP+	MULTIPROTOCOL BORDER GATEWAY PROTOCOL
MPLS	MULTI-PROTOCOL LABEL SWITCHING
MPLS-TE	MULTI-PROTOCOL LABEL SWITCHING-TRAFFIC ENGINEERING
NAT	NETWORK ADDRESS TRANSLATION
NCS	NATIONAL COMMUNICATIONS SYSTEM
NGN	NEXT GENERATION NETWORK
NIST	NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
NLR	NATIONAL LAMBDARAIL
NMS	NETWORK MANAGEMENT SYSTEM
NS/EP	NATIONAL SECURITY AND EMERGENCY PREPAREDNESS
NSA	NATIONAL SECURITY AGENCY
OIF	OPTICAL INTERNET FORUM
OIF UNI	OPTICAL INTERNETWORKING FORUM USER NETWORK INTERFACE
OSI	OPEN SYSTEMS INTERCONNECTION
OSPF	OPEN SHORTEST PATH FIRST
O-UNI	OPTICAL USER NETWORK INTERFACE
PBX	PRIVATE BRANCH EXCHANGE
PDP	POLICY DECISION POINT
PE	PROVIDER EDGE
PEP	POLICY ENFORCEMENT POINT
PHB	PER-HOP [FORWARDING] BEHAVIOR
PKC	PUBLIC KEY CRYPTOGRAPHY
PKI	PUBLIC KEY INFRASTRUCTURE
PPP/HDLC	POINT TO POINT PROTOCOL/HIGHLEVEL DATA LINK CONTROL

PSN	PUBLIC SWITCHED NETWORK
PSTN	PUBLIC SWITCHED TELEPHONE NETWORK
PVC	PERMANENT VIRTUAL CIRCUIT
QOS	QUALITY OF SERVICE
RAP WG	RSVP ADMISSION POLICY WORKING GROUP
RDM	RUSSIAN DOLL MODEL
RFC	REQUEST FOR COMMENTS
RFI	REQUEST FOR INFORMATION
RIP	ROUTING INFORMATION PROTOCOL
RSVP	RESOURCE RESERVATION PROTOCOL
RSVP-TE	RESOURCE RESERVATION PROTOCOL-TRAFFIC ENGINEERING
S-BGP	SECURE BGP
S-CDMA	SYNCHRONOUS CODE DIVISION MULTIPLE ACCESS
SDH	SYNCHRONOUS DIGITAL HIERARCHY
SDP	SESSION DESCRIPTION PROTOCOL
SDSL	SYNCHRONOUS DIGITAL SUBSCRIBER LINE
SIP	SESSION INITIATION PROTOCOL
SMS	SHORT MESSAGE SERVICE
SMTP	SIMPLE MESSAGE TRANSFER PROTOCOL
SONET	SYNCHRONOUS OPTICAL NETWORK
SRLG	SHARED RISK LINK GROUP
SSL	SECURE SOCKET LAYER
TCP	TRANSMISSION CONTROL PROTOCOL
TCP/IP	TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL
TDM	TIME DIVISION MULTIPLEXING

UBR	UNSPECIFIED BIT RATE
UDP	USER DATAGRAM PROTOCOL
URL	UNIFORM RESOURCE LOCATOR
USB	UNIVERSAL SERIAL BUS
VBR	VARIABLE BIT RATE
VLAN	VIRTUAL LOCAL AREA NETWORK
VPLS	VIRTUAL PRIVATE LOCAL AREA NETWORK SERVICE
VPN	VIRTUAL PRIVATE NETWORK
WAN	WIDE AREA NETWORK
W-CDMA	WIDEBAND CODE DIVISION MULTIPLE ACCESS
WDM	WAVE DIVISION MULTIPLEXING
WPS	WIRELESS PRIORITY SERVICE
WWW	WORLD WIDE WEB
XDSL	GENERIC DIGITAL SUBSCRIBER LINE
XML	HIGH LEVEL MARKUP LANGUAGE
XMPP	EXTENSIBLE MESSAGING AND PRESENCE PROTOCOL

5 References

This document is a compilation of publicly available information regarding the operation of Next Generation Networks and converged Internet technologies. Specific references are not cited in the document directly, but instead are implied through the mention of an open standard or standards group. Additionally, information was gleaned from numerous websites and trade magazines, as well as the Industry RFI responses and product literature. The following is a short list of standards organizations and commercial entities active in developing these specifications. Many of the appropriate background documents are publicly available through their websites.

- National Institute of Standards (NIST) www.nist.gov
- Internet Engineering Task Force www.ietf.org
- Institute of Electrical and Electronic Engineers (IEEE) www.ieee.org

- International Telecommunications Union (ITU) www.itu.org
- American National Standards Institute (ANSI) www.ansi.org
- European Telecommunications Standards Institute (ETSI) www.etsi.org
- ATM Forum www.atmforum.org
- Optical Internet Forum www.oifforum.org
- Third Generation Partnership Program (3GPP) www.3gpp.org
- Third Generation Partnership Program Two (3GPP2) www.3gpp2.org
- CableLabs www.cablelabs.com
- Alliance for Telecommunications Solutions (ATIS) www.atis.org
- Frame Relay/MPLS Forum Alliance www.mplsforum.org
- Network Interconnection/Interoperability Forum www.atis.org/niif/index.asp
- LightReading www.lightreading.com
- Cisco Systems www.cisco.com
- Juniper Networks www.juniper.net