

(43) International Publication Date
23 December 2009 (23.12.2009)(10) International Publication Number
WO 2009/155191 A1(51) International Patent Classification:
H04N 7/173 (2006.01)(21) International Application Number:
PCT/US2009/046965(22) International Filing Date:
11 June 2009 (11.06.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
12/140,843 17 June 2008 (17.06.2008) US(71) Applicant (for all designated States except US): **GENERAL INSTRUMENT CORPORATION** [US/US];
101 Tournament Drive, Horsham, PA 19044 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **JOYCE, Gerald, R.** [US/US]; 121 Parmenter Road, Newton, MA 02465 (US). **BAO, Qi** [CN/US]; 3208 Windsor Ridge, Westborough, MA 01581 (US). **FLANAGAN, David** [US/US]; 110 Lockland Avenue, Framingham, MA 01701 (US). **PATRICK, Michael, W.** [US/US]; 9 Elizabeth Drive, Assonet, MA 02702 (US). **ULM, John** [US/US]; 16 Lakin Street, Pepperell, MA 01463 (US).(74) Agents: **CULLEN, Lawrence, T.** et al.; 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: APPARATUS, METHOD AND SYSTEM FOR MANAGING BYPASS ENCAPSULATION OF INTERNET CONTENT WITHIN A BYPASS ARCHITECTURE

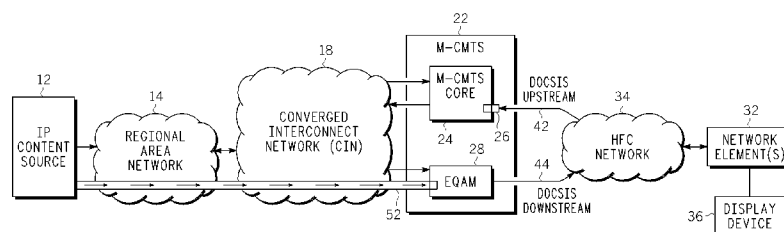


FIG. 2

(57) Abstract: An apparatus, method and system for delivering Internet content within a system that includes a bypass architecture, such as a bypass architecture that transmits content from the Internet or an Internet content source to a downstream modulator, such as an Edge Quadrature Amplitude Modulation (EQAM) modulator, in a manner that bypasses the system's Cable Modem Termination System (CMTS). Content from the Internet or an Internet source is transmitted to a last-hop router, which is configured to identify content for bypass encapsulation. The last-hop router also can be configured to perform at least a portion of the necessary bypass encapsulation for proper bypass flows of the identified content. Alternatively, the EQAM is configured to perform the bypass encapsulation, and the last-hop router transmits the identified content to the EQAM, which performs at least a portion of the necessary bypass encapsulation on the identified content.

APPARATUS, METHOD AND SYSTEM FOR MANAGING
BYPASS ENCAPSULATION OF INTERNET CONTENT
WITHIN A BYPASS ARCHITECTURE

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The invention relates to the delivery of Internet Protocol (IP) content over cable systems using a standard protocol Data Over Cable System Interface Specification (DOCSIS). More particularly, the invention relates to transmitting IP content within systems involving Cable Modem Termination System (CMTS) architecture and processing.

Description of the Related Art

[0002] Most cable systems currently provide video (and data) content delivery services via digital broadcast. The video image is first digitized, and then compressed, e.g., via one of several digital algorithms or compression standards, such as the MPEG2 (Moving Pictures Expert Group) algorithm or the MPEG4 part 10 algorithm, where the latter also is known as the International Telecommunications Union (ITU) H.264 standard. These compression standards allow the same video content to be represented with fewer data bits. Using MPEG2, standard definition television currently can be transmitted at a rate of approximately 4 Megabits per second (Mbps). Using MPEG 4 Part 10, the same video content can be transmitted at a rate of approximately 2 Mbps.

The digital video content typically is transmitted from a source at a cable provider's headend to one or more network elements, such as an end user's set-top box (or other suitable video processing device), via a digitally modulated radio frequency (RF) carrier, with the video content organized into an MPEG2 Transport Stream (MPEG2-TS) format.

[0003] Cable system operators are considering Internet Protocol (IP) -based methods for delivery of content, such as IP-video and IP Television (IPTV), to supplement their current digital video delivery methods. The internet protocol is not required for MPEG2 Transport Streams. However, IP-based video delivery allows the possibility of new video sources, such as the Internet, and new video destinations, such as end user IPTV playback devices. If cable systems do include IP-based content delivery, it is quite possible and likely that relatively large amounts of bandwidth will be needed to deliver IPTV content to end users. Moreover, as end users continue to shift their viewing desires toward on-demand applications, a relatively large percentage of such on-demand content likely will be IPTV content.

[0004] The cable industry developed the Data Over Cable System Interface Specification (DOCSIS[®]) standard or protocol to enable the delivery of IP data packets over cable systems. Later, in anticipation of IP video traffic, the DOCSIS 3.0 standard was developed. In general, DOCSIS defines interface requirements for cable modems involved in high-speed data distribution over cable television system networks. The cable industry also developed the Cable Modem Termination System (CMTS) architecture and the Modular CMTS (M-CMTS[™]) architecture for this purpose. In general, a CMTS is a component, typically located at the headend or local office of a

cable television company, that exchanges digital signals with cable modems on a cable network.

[0005] In general, an EdgeQAM (EQAM) or EQAM modulator is a headend or hub device that receives packets of digital content, such as video or data, re-packetizes the digital content into an MPEG transport stream, and digitally modulates the digital transport stream onto a downstream RF carrier using Quadrature Amplitude Modulation (QAM). EdgeQAMs are used for both digital broadcast, and DOCSIS downstream transmission. In a conventional IPTV network system arrangement using M-CMTS architecture, the EdgeQAMs are downstream DOCSIS modulators, and are separated from a core portion of the M-CMTS core. An IPTV server or other suitable IP content provider is coupled to a regional area or backbone network. This backbone network, in turn, is connected to a converged interconnect network (CIN) which also links the M-CMTS core and the EdgeQAMs. The CIN performs as one or more access routers or switches, i.e., devices configured for routing data in an IP network. There is a Layer Two Tunneling Protocol version 3 (L2TPv3) tunnel from the M-CMTS core to the EdgeQAMs, with this tunnel being identified as a Downstream External Physical Interface (DEPI). The IPTV content is carried on the downstream DOCSIS RF carrier from the EdgeQAM to one or more end user network elements, such as a DOCSIS set-top box or an Internet Protocol set-top box (IP-STB). An IP set-top box is a set-top box or other multimedia content processing device that can use a broadband data network to connect to television channels, video streams and other multimedia content. An upstream DOCSIS receiver is coupled to and receives data from a cable modem via the DOCSIS

protocol. Some of the data is simply DOCSIS Media Access Control (MAC) Management packets originating at the cable modem (CM) and used for the functioning of the DOCSIS protocol. Other data are upstream IP packets from devices connected to the CM, such as on-demand commands, from the end user multimedia content processing device, and are forwarded to other devices via the CIN. Upstream DOCSIS receivers are combined with or contained within a core portion of the M-CMTS component.

[0006] In general, for conventional M-CMTS architecture, all packets traveling upstream or downstream typically travel through the M-CMTS core for appropriate forwarding to the correct network interface or DOCSIS carrier. However, since the downstream DOCSIS modulators (i.e., the EQAMs) are separate from the M-CMTS core, the downstream packets travel from the M-CMTS core, through the CIN, and to the EQAMs on special “tunnel” or “pseudo-wire” connections. These tunnels, which are defined by the Layer Two Tunneling Protocol (L2TP) version 3 (i.e., L2TPv3), are known within the DOCSIS 3.0 standard as Downstream External Physical Interface (DEPI) tunnels, and typically are carried over gigabit Ethernet links.

[0007] One of the features of the DOCSIS 3.0 specification intended to facilitate the use of IPTV content delivery is that the number of downstream EQAMs can be increased independently of the number of upstream DOCSIS data channels. Hence, the downstream DOCSIS capacity can be arbitrarily increased to whatever bandwidth is needed. However, as discussed, downstream IPTV content or data packet flow from the IPTV server to the end user DOCSIS network elements conventionally is required to travel through the CIN to the M-CMTS core, then from the M-CMTS core, on a DEPI

tunnel, back through the CIN again, and on to the EQAM. Such “hairpin” forwarding of downstream data packets back through the CIN requires a disproportionate amount of switching bandwidth and other resources compared to other portions of the system.

[0008] Accordingly, there has been a need to provide a bypass architecture that overcomes or avoids the issues involved with data packet flow from the CIN into and through the M-CMTS core, and then back from the M-CMTS core through the CIN and on to the EQAM. One application for such a bypass architecture might involve or include direct tunneling of video content from servers controlled by a multiple systems operator (MSO) to a downstream modulator, such as a low-cost downstream EQAM, in a manner that bypasses the CMTS, including the M-CMTS core. In such case the MSO has some latitude in carrying out the DOCSIS M-CMTS core bypass. The necessary encapsulation could be done at the server itself, or at the EQAM, or elsewhere.

However, another application is to provide a bypass to the M-CMTS core for video content that the MSO does not control. This content would not originate from an MSO controlled server, but rather, directly from the Internet. Such content is referred to as over-the-top content, because the IP content bypasses the conventional distribution services of an MSO (or other broadband provider) and goes directly to the end user via an end user network, such as a Hybrid Fiber Coaxial (HFC) network. Over-the-top IP content is expected to comprises a relatively significant portion of all DOCSIS IP content traffic in the future. Accordingly, there is a need for a content distribution system bypass architecture that includes the management of the bypass content flows of over-the-top content.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] FIG. 1 is a block diagram of a conventional Internet Protocol (IP) content delivery system, including a conventional modular Cable Modem Termination System (M-CMTS) network;

[0010] FIG. 2 is a block diagram of an IP content delivery system, including a DOCSIS IP-video Bypass Architecture (DIBA), in which the IP content bypasses the M-CMTS core;

[0011] FIG. 3 is a block diagram of an IP content delivery system with an integrated CMTS network, and also including a DOCSIS IP-video Bypass Architecture (DIBA), in which the IP content bypasses the integrated CMTS;

[0012] FIG. 4 is a block diagram of an IP content delivery system according to the PacketCable Multimedia (PCMM) architecture specifications, and including a bypass architecture for over-the-top content;

[0013] FIG. 5 is a block diagram of a bypass encapsulation apparatus for use in an IP content delivery system having a bypass architecture;

[0014] FIG. 6 is a block diagram of an IP content delivery system according to the PacketCable Multimedia (PCMM) architecture specifications, and including an alternative bypass architecture for over-the-top content;

[0015] FIG. 7 is a block diagram of data encapsulations at various stages in the IP content delivery system of FIG. 4, in which the EQAM performs the bypass encapsulation of the IP content; and

[0016] FIG. 8 is a flow chart that schematically illustrates a method for delivering IP content within a system that includes a bypass architecture for over-the-top content.

DETAILED DESCRIPTION

[0017] In the following description, like reference numerals indicate like components to enhance the understanding of the bypass architecture and corresponding data encapsulation and transmission devices and methods through the description of the drawings. Also, although specific features, configurations and arrangements are discussed herein below, it should be understood that such specificity is for illustrative purposes only. A person skilled in the relevant art will recognize that other steps, configurations and arrangements are useful without departing from the spirit and scope of the invention.

[0018] The apparatus, methods and systems described herein involve using a last-hop router as part of a bypass architecture within an IP content distribution system. The last-hop router transmits over-the-top content received from an IP content source directly to the system EQAM, bypassing the system CMTS. The last-hop router is configured to identify the IP content that is to be bypass encapsulated, to allow for proper bypass flow of the IP content to the EQAM. One or both of the last-hop router and the EQAM are configured to perform the necessary bypass encapsulation of the IP content identified for bypass flow from the last-hop router to the EQAM. The bypass encapsulated content is transmitted from the EQAM to the end user network elements as a DOCSIS flow.

[0019] Referring now to FIG. 1, shown is a block diagram of a conventional Internet Protocol (IP) content delivery system 100 including a conventional modular Cable Modem Termination System (M-CMTS) network arrangement. The system 100 includes one or more sources of IP content, e.g., one or more video on demand (VOD) servers 102, IPTV broadcast video servers 104, Internet video sources 106, or other suitable sources for providing IP content. The IP content sources are connected to a regional area or backbone network 114. The regional area network 114 can be any communication network or network server arrangement suitable for transmitting IP content. For example, the regional area network 114 can be or include the Internet or an IP-based network, a computer network, a web-based network or other suitable wired or wireless network or network system.

[0020] Coupled to the regional area network 114 is a converged interconnect network (CIN) 118, which includes the routing and switching capability for connecting the regional area network 114 to a Cable Modem Termination System (CMTS), such as a modular CMTS (M-CMTS) 122. In general, as discussed hereinabove, the CIN typically performs as an access router for routing data in an IP network. The CIN typically has gigabit Ethernet interfaces and can perform layer 2/3/4 forwarding, i.e., routing of data in layers 2, 3 and 4 as defined according to the seven-layer Open Systems Interconnection (OSI) network protocol. In general, a CMTS or an M-CMTS is a component that exchanges digital signals with network elements (such as network elements including cable modems, set-top boxes and other content processing devices, and media terminal adapters) on a cable network. The CMTS or M-CMTS typically is located at the local

office of a cable television company. In a typical arrangement, the CMTS and the cable modem are the endpoints of the DOCSIS protocol, with the hybrid fiber coax (HFC) cable plant therebetween. DOCSIS enables IP packets to pass between devices on either side of the link between the CMTS and the cable modem.

[0021] The M-CMTS 122 includes an M-CMTS core 124, which typically includes or contains one or more upstream receivers 126, such as an upstream DOCSIS receiver. The M-CMTS 122 also includes one or more downstream DOCSIS modulators, such as one or more EdgeQAMs (EQAMs) 128, which are external to and not part of the M-CMTS core 124. The M-CMTS 122 typically is connected to one or more network elements 132, such as an end user cable modem, a set-top box, a media terminal adapter (MTA) or other suitable end user or customer premises equipment (CPE). Note that there should be a cable modem attached to the HFC network. It is possible for a set-top box or MTA to include a cable modem by which that device attaches to the HFC network. The network elements 132 may include an associated display device 136 coupled thereto. The M-CMTS 122 typically is connected to the network elements 132 via an end user network, which typically is a Hybrid Fiber Coaxial (HFC) cable network 134 and/or other suitable end user network or network system.

[0022] The upstream receiver 126 is configured to receive upstream IP/DOCSIS transmissions, such as on-demand commands from an end user set-top box. The upstream data is transmitted to the upstream receiver 126 via the network 134 and an upstream data channel 142 coupled between the network 134 and the upstream receiver 126. The M-CMTS core 124, which includes the upstream receiver 126, removes the

upstream DOCSIS encapsulation and Ethernet link header. The remaining Internet Protocol (IP) packets, are then re-encapsulated with Ethernet and sent to an IP router, or other suitable device or component, for transmission across the CIN 118 and the regional area network 114. For downstream data, the M-CMTS core 124 completes the Ethernet encapsulation and a portion of the DOCSIS encapsulation, and sends that payload over a DEPI tunnel to one or more EQAMs 128 or other suitable downstream modulators. These EQAMs then complete the encapsulation of the IP packet data within a DOCSIS formatted transport stream or other suitable digital transport stream and modulate the digital transport stream onto a downstream RF carrier using Quadrature Amplitude Modulation (QAM) to the network elements 132. The downstream data is transmitted from the EQAM 128 to the network elements 132 via the network 134 and a downstream data channel 144 coupled between the EQAM 128 and the network 134.

[0023] One or more of the components within the M-CMTS 122, including one or more of the M-CMTS core 124, the upstream receiver 126 and the EQAM 128 can be comprised partially or completely of any suitable structure or arrangement, e.g., one or more integrated circuits. Also, it should be understood that the M-CMTS 122 includes other components, hardware and software (not shown) that are used for the operation of other features and functions of the M-CMTS 122 not specifically described herein. Also, the M-CMTS 122 can be partially or completely configured in the form of hardware circuitry and/or other hardware components within a larger device or group of components. Alternatively, the M-CMTS 122 can be partially or completely configured in the form of software, e.g., as processing instructions and/or one or more sets of logic

or computer code. In such configuration, the logic or processing instructions typically are stored in a data storage device (not shown). The data storage device typically is coupled to a processor or controller (not shown). The processor accesses the necessary instructions from the data storage device and executes the instructions or transfers the instructions to the appropriate location within the M-CMTS 122.

[0024] A DOCSIS 3.0 cable modem and other network elements are able to receive multiple downstream channels 144. According to the DOCSIS 3.0 standard, there may be “primary” and “non-primary” downstream channels. Of these, one and only one downstream channel will be the “primary” downstream channel of the network elements. The network elements will only receive synchronization time-stamps, which are necessary for upstream operation and which are known as SYNC messages, on its primary downstream channel. Thus, the “primary” channel is also a “synchronized” channel. The network elements also rely on the “primary” channel for the delivery of Mac Domain Descriptor (MDD) messages, which enable the network elements to perform operations including plant topology resolution and initial upstream channel selection. During initialization, the network elements are only required to receive Upstream Bandwidth Allocation Maps (MAPs) and Upstream Channel Descriptors (UCDs) on its “primary” downstream channel.

[0025] In systems using M-CMTS architecture, the IP data packets traveling upstream or downstream typically travel through the M-CMTS core 124 for appropriate processing and subsequent forwarding to the correct network interface or data carrier, such as a DOCSIS RF carrier. Since the upstream receiver 126 is combined with the M-

CMTS core 124 and its processing, upstream data received by the upstream receiver 126 can be transmitted directly from the upstream receiver 126 to the M-CMTS core 124 and then forwarded appropriately. However, since the downstream modulator (EQAM 128) is not part of the M-CMTS core 124, downstream data received by the M-CMTS 122 from the CIN 118 travels first through the M-CMTS core 124 for appropriate processing and then is directed to the EQAM 128 for appropriate conversion and modulation.

Downstream data packets from the M-CMTS core 124 conventionally must travel back through the CIN 118 and then to the EQAM 128 using special “tunnel” or “pseudo-wire” connections, such as downstream or DOCSIS Downstream External Physical Interface (DEPI) tunnels. As discussed hereinabove, such “hairpin” forwarding from the M-CMTS core 124 back through the CIN 118 to the EQAM 128 will require a disproportionate amount of switching bandwidth for the M-CMTS core 124 and the CIN 118.

[0026] Referring now to FIG. 2, shown is a block diagram of an IP content delivery system 50 including M-CMTS bypass architecture. In the system 50, downstream content or traffic travels directly from one or more IP content sources 12 to an EQAM 28, e.g., via a regional area network 14 and a CIN 18, thus bypassing the M-CMTS core 24. The downstream content travels directly to the EQAM 28 using one or more suitable connections (shown generally as a connection 52). For example, the connection 52 can be one or more “tunnel” or “pseudo-wire” connections, such as a DEPI tunnel. As will be discussed in greater detail hereinbelow, content that is tunneled or otherwise transmitted directly from the IP content source 52 to the EQAM 28 emerges from the EQAM 28 with partial or full DOCSIS framing, suitable for forwarding through to

DOCSIS-compatible end user network elements, such as an end user cable modem that is DOCSIS-compatible. In general, the system 50 accomplishes the functionality of an M-CMTS without the associated cost of the M-CMTS core. Conventionally, the M-CMTS does allow the addition of corresponding EQAMs to the system without having to increase the number of upstream data channels, providing some system flexibility. However, the bypass architecture, e.g., as shown in FIG. 2, provides the additional advantage of allowing additional EQAMs, without having to add additional processing capacity to the M-CMTS core 24, or the CIN 18, which would be relatively expensive.

[0027] Also, alternatively, an M-CMTS bypass architecture can be used in systems that include an integrated CMTS, rather than a more expensive M-CMTS. In this manner, the bypass architecture makes it possible to deploy an integrated CMTS with additional external EQAMs. The integrated CMTS includes a “synchronized” or “primary” downstream DOCSIS data channel from the integrated CMTS to the end user network elements, in addition to the downstream DOCSIS data channels from the EQAM to the end user network elements, which may be “synchronized” or “non-synchronized.” Referring now to FIG. 3, shown is a block diagram of an IP content delivery system 60 including an integrated CMTS network, and including a bypass architecture in which the IP content bypasses the integrated CMTS. The system 60 includes an integrated CMTS 62, which differs from an M-CMTS in that it also includes a downstream DOCSIS data channel 64 coupled to end user network elements 32, e.g., via an HFC network 34. Network elements 32 can include one or more end user network elements, such as a cable modem, a set-top box, a media terminal adapter (MTA) or other suitable end user or

customer premises equipment (CPE). The downstream DOCSIS data channel 64 is fully functional, containing synchronization timestamps, and thus is considered to be “primary” or “synchronized.” By comparison, the downstream DOCSIS data channel 44 from the EQAM 28 to the network elements 32 (via the HFC network 34), which carries IP content, can be configured to operate without synchronization timestamps, and thus may, in that case, be considered to be “non-synchronized.”

[0028] Because IP content can be delivered to DOCSIS cable modems and other network elements 32 using non-synchronized downstream data channels, the EQAM 28 can be used to deliver IP content even when the EQAM 28 is not synchronized to the DOCSIS master clock with the DOCSIS Timing Interface (DTI) (not shown), which is part of the integrated CMTS 62. DOCSIS modems require DOCSIS master clock synchronization on only one synchronized data channel, i.e., the so-called “primary” downstream data channel. Therefore, such synchronization can be supplied by the integrated CMTS 62, via the “synchronized” downstream DOCSIS data channel 64. Alternatively, such synchronization can be supplied by a single M-CMTS EQAM that is synchronized to the DOCSIS master clock with the DOCSIS DTI.

[0029] By using the CMTS bypass architecture, the system 60 avoids the expense of the CMTS (or the M-CMTS) having to establish or generate both synchronized and non-synchronized downstream data channels for delivery of IP content. A single synchronized data channel from the integrated CMTS 62 or its core can provide the synchronization timestamps, and also provide other DOCSIS Media Access Control (MAC) functions, including instructing the network elements 32 when to transmit

upstream and delivering other MAC layer messages for various network element functions, such as registration and maintenance. One or more non-synchronized DOCSIS data channels can be established or generated for one or more EQAMs 28. A non-synchronized DOCSIS data channel generated for an EQAM is less expensive than generating a synchronized DOCSIS data channel for an integrated CMTS or an M-CMTS. Also, with an integrated CMTS and no timestamps in the non-synchronized data channel, the DTI (which is required in the M-CMTS architecture) is not necessary in systems using CMTS bypass architecture.

[0030] Depending on the content source 12, the regional area network 14 and the CIN 18, as well as the type of EQAM 28, IP content delivery systems using CMTS bypass architecture can use many different tunneling techniques and therefore have many suitable bypass data encapsulations. Data encapsulation generally is the process of taking a packet of a particular format that contains data as its payload, and enveloping or encapsulating that entire packet as the payload of a new packet. The new packet is generally formed by adding additional header fields, of a different format, to the old packet, which becomes the payload. The outermost header must be compatible with the device receiving the data. If the EQAM 28 is an M-CMTS DEPI EQAM (DEPI EQAM), data encapsulation can occur using at least two DEPI tunneling techniques. Using either tunneling technique, the content source 12 generates or originates an L2TPv3 (DEPI) tunnel to the DEPI EQAM. In the first DEPI tunneling technique, known as the DOCSIS Packet Stream Protocol (PSP), IP content is encapsulated into DOCSIS MAC frames or data packets, i.e., DOCSIS frames are transported in the L2TPv3 tunnel payload (data).

In general, the PSP allows DOCSIS frames to be appended together in a queue, using either concatenation (to increase network performance) or fragmentation (if tunneled packets are too large). The PSP DEPI tunneling technique allows the EQAM 28 to mix both IP content originated from the IP content sources 12 with non-IP content, such as VOIP (Voice over Internet Protocol) data originated from the M-CMTS core 24, on the same DOCSIS downstream data carrier.

[0031] In the second DEPI tunneling technique, known as DOCSIS MPEG Transport (D-MPT), multiple 188-byte MPEG2 Transport Stream (MPEG-TS) packets are transported in the L2TPv3 tunnel payload. In D-MPT, IP content is encapsulated into DOCSIS MAC frames and the DOCSIS MAC frames are encapsulated into MPEG-TS packets. All DOCSIS frames, including packet-based frames and any necessary MAC management-based frames, are included within the one D-MPT data flow. The EQAM receiving the D-MPT data flow searches the D-MPT payload for any DOCSIS SYNC messages and performs SYNC corrections. The EQAM then forwards the D-MPT packet to the RF interface, for transmission on the RF data carrier. Using the D-MPT tunneling technique, MPEG packets can be received by the EQAM and forwarded directly to the RF interface without having to terminate and regenerate the MPEG framing. The only manipulation of the D-MPT payload is the SYNC correction.

[0032] Alternatively, the EQAM 28 can be a standard MPEG2 Transport Stream (MPEG2-TS) EQAM. If the EQAM 28 is an MPEG2-TS EQAM, the IP content source 12 can transmit IP content in PSP formatted data packets. In such case, a PSP/MPT converter is used to convert the data format into an MPEG2-TS format, which an

MPEG2-TS EQAM can process. The PSP/MPT converter can be attached to or embedded within the CIN 18 or one or more networking devices within the CIN 18. Alternatively, the IP content source 12 can directly generate and transmit IP content in MPT formatted data packets, which the MPEG2-TS EQAM can process.

[0033] As discussed hereinabove, there has been a need to provide a bypass architecture that overcomes or avoids the issues involved with data packet flow from the M-CMTS core back through the CIN and then on to the EQAM. Such a bypass architecture might involve or include direct tunneling of video content from a video server controlled by a multiple systems operator (MSO) to a downstream modulator, such as a low-cost downstream EQAM, in a manner that bypasses the CMTS, including the M-CMTS core. The use of a CMTS bypass or other bypass architecture within an IP content delivery system requires various encapsulation for proper IP content bypass flows. For example, to achieve proper bypass, the IP content servers need to have DOCSIS encapsulation information, as well as selected EQAM information, e.g., tunneling information of the EQAM. In such a bypass architecture, the MSO-controlled server might be modified to perform the DOCSIS encapsulation that conventionally would be done by a CMTS. The MSO-controlled server then would transmit the resulting content with DOCSIS encapsulation to a conventional DOCSIS EQAM via a Downstream External Physical Interface (DEPI) tunnel. The EQAM then transmits the content as a standard downstream DOCSIS RF signal to the end user network and network elements.

[0034] However, such systems and methods typically would not apply to over-the-top content, i.e., IP content that originates directly from the Internet, rather than from an MSO-controlled server. As discussed hereinabove, over-the-top content bypasses the conventional distribution services of the MSO-controlled server (or other broadband provider) and goes directly to the end user network and network elements. The apparatus, methods and systems describe herein provide appropriate identification and encapsulation of over-the-top content for such bypass flows within a content distribution system having a bypass architecture.

[0035] A last-hop router apparatus is configured to identify the over-the-top content to be given the necessary bypass encapsulation for bypass flow within a content distribution system having a bypass architecture. The last-hop router also is configured to provide a bypass tunnel directly to the EQAM, thus bypassing the CMTS. Bypass encapsulation of the IP content identified for bypass data flow is performed in a suitable manner by an appropriate system bypass encapsulation device or component. For example, the last-hop router that is configured to identify the over-the-top content to be bypass encapsulated also can be configured to perform the bypass encapsulation of the over-the-top content identified for bypass flow. Alternatively, the last-hop router can transmit the content identified for bypass flow to an EQAM that is configured to perform bypass encapsulation, and the EQAM performs the bypass encapsulation of the identified over-the-top content. In this manner, over-the-top content from an IP content source is transmitted to the last-hop router, which identifies the content for bypass data flow and passes the content directly to the EQAM, bypassing the CMTS. The necessary bypass

encapsulation is performed by the last-hop router and/or the EQAM. The bypass encapsulated content is transmitted from the EQAM to the end user network elements as a DOCSIS flow.

[0036] Referring now to FIG. 4, shown is a block diagram of an IP content delivery system 70 according to the PacketCable Multimedia (PCMM) architecture specifications, and including a bypass architecture for over-the-top content. The PCMM specifications define a framework for providing Quality of Service (QoS), security and resource allocation and management for any type of service within a DOCSIS network.

[0037] The IP content delivery system 70 includes one or more IP content sources 72 of over-the-top content or IP content. The system 70 also includes one or more last-hop routers 74 coupled between the IP content source 72 and the EQAM 28. The last-hop router 74 is coupled to the IP content source 72 in any suitable manner, e.g., via one or more networks 76, such as a regional area network or a local network. As will be discussed in greater detail hereinbelow, the last-hop router 74 is coupled to the EQAM 28 using one or more suitable connections 52, such as one or more “tunnel” or “pseudo-wire” (DEPI) connections. The display device 36 and/or the network element 32 are able to communicate with and select content from various IP content sources 72. These communications are carried out via IP packets traveling between the network element 32 and the IP content sources 72, over the usual path of the cable modem portion of the network element 32, the HFC network 34, the upstream DOCSIS data channel 42 and the downstream DOCSIS data channel 64, the CMTS 62, the last hop router 74, and the network 76.

[0038] The PCMM framework includes a Proxy Call Session Control Function (P-CSCF) 82. In general, the P-CSCF 82 is responsible for reserving, committing and releasing Quality of Service (QoS) resources for a given IP content flow session over the CMTS 62 and the EQAMs 28. Messages between the P-CSCF 82 and the last-hop router 74 are exchanged using an appropriate protocol, e.g., the session initiation protocol (SIP), and using an appropriate interface therebetween, such as a Gm interface.

[0039] The PCMM framework also includes a Policy and Charging Rules Function (PCRF) 84 coupled between the P-CSCF 82 and the CMTS 62. The PCRF 84 includes a PacketCable Application Manager (PAM) 86 coupled to the P-CSCF 82 and a Policy Server 88 coupled between the PAM 86 and the CMTS 62. The PAM 86 is a specialized application manager primarily responsible for determining the QoS resources needed for a session, based on the received session descriptors from the P-CSCF 82, and managing the QoS resources allocated for the session. The Policy Server 88 generally is a system that primarily acts as an intermediary between the PAM 86 and the CMTS 62. The Policy Server 88 applies network policies to requests by the PAM 86 and proxies messages between the PAM 86 and the CMTS 62.

[0040] The session-based policy set-up information exchanged between the P-CSCF 82 and the PAM 86 occurs using an appropriate protocol, e.g., the Diameter protocol, and using an appropriate interface therebetween, such as an Rx interface. The requests, messages and other information exchanged between the PAM 86 and the Policy Server 88 occurs using an appropriate protocol, e.g., the Common Open Policy Service (COPS)

protocol. Also, the messages and information exchanged between the Policy Server 88 and the CMTS 62 occurs using an appropriate protocol, such as the COPS protocol.

[0041] An edge resource manager (ERM) 89 is shown coupled between the CMTS 62 and the EQAM 28. In general, the ERM 89 allocates and manages the resources of the edge devices, e.g., the EQAM 28. The ERM 89 also communicates with and receives instructions from a session manager (not shown), which may be located in the CMTS 62 or, alternatively, may be located in the PAM 86. The information exchanged between the ERM 89 and the EQAM 28 occurs according to the DOCSIS specification, e.g., using the Real Time Streaming Protocol (RTSP).

[0042] Some of the components in the system 70 typically are located within the same local network and therefore can be configured to pass control messages, for purposes of configuration and control, or otherwise communicate with one another over a control plane across the particular local network. For example, the last-hop router 74, the EQAM 28 and the CMTS 62 typically are located within the same local network and therefore can communicate with one another over the local network, such as by passing configuration and control messages therebetween.

[0043] Referring now to FIG. 5, with continuing reference to FIG. 4, shown is a block diagram of a bypass encapsulation apparatus 90 for use in the IP content delivery system 70. The bypass encapsulation apparatus 90 can be any suitable standalone component or apparatus within an existing system component that performs appropriate bypass encapsulation or DOCSIS bypass encapsulation of IP content identified by the last-hop router 74 or other appropriate system component. As discussed hereinabove,

and as will be discussed in greater detail hereinbelow, the last-hop router 74 can be configured as a bypass encapsulation apparatus 90 or include a bypass encapsulation apparatus 90 therein. Alternatively, the EQAM 28 can be configured as a bypass encapsulation apparatus 90 or include a bypass encapsulation apparatus 90 therein. For example, the MSO may want to use less modified last-hop routers, and therefore the EQAM 28 can be configured as or include the bypass encapsulation apparatus 90.

[0044] The bypass encapsulation apparatus 90 includes a first interface 94, a second interface 95, a controller 96 coupled between the first and second interfaces 94, 95, and a data storage element 98 coupled to the controller 96. The controller 96 generally processes IP content and other information received by the bypass encapsulation apparatus 90. The controller 96 also manages the movement of IP content and other information, such as bypass encapsulation information, to and from the data storage element 98. In addition to the content storage element 98, the bypass encapsulation apparatus 90 can include at least one type of memory or memory unit (not shown) within the controller 96 and/or a storage unit or data storage unit coupled to the controller 96 for storing processing instructions and/or information received and/or created by the bypass encapsulation apparatus 90.

[0045] The first interface 94 is configured to receive IP content from other components within the system 70, e.g., the IP content source 72 or the last-hop router 74. The second interface 95 is configured to transmit bypass encapsulated IP content to other components within the system 70, e.g., the EQAM 28 or the CMTS 62 and/or end user network elements 32. It should be understood that the interfaces 94, 95 can be a single

input/output interface coupled to the controller 96. Also, it should be understood that one or more of the interfaces 94, 95 can be an interface configured to support more than one connection from more than one system component or device. The input and/or output interfaces 94, 95 are configured to provide any protocol interworking between the other components within the bypass encapsulation apparatus 90 and the other components within the system 70 that are external to the bypass encapsulation apparatus 90. Because all content distribution systems are not the same, the interfaces 94, 95 are configured to support the protocols of the particular system that is providing the content. Such protocol support functionality includes the identification of the content streams and corresponding protocol support required by the distribution system. Each distribution system typically will use a defined set of protocols.

[0046] One or more of the controller 96, the storage element 98 and the interfaces 94, 95 can be comprised partially or completely of any suitable structure or arrangement, e.g., one or more integrated circuits. Also, it should be understood that the bypass encapsulation apparatus 90 includes other components, hardware and software (not shown) that are used for the operation of other features and functions of the bypass encapsulation apparatus 90 not specifically described herein. Moreover, the bypass encapsulation apparatus 90 can be partially or completely configured in the form of hardware circuitry and/or other hardware components within a larger device or group of components. Alternatively, the bypass encapsulation apparatus 90 can be partially or completely configured in the form of software, e.g., as processing instructions and/or one or more sets of logic or computer code. In such configuration, the logic or processing

instructions typically are stored in a data storage device, e.g., the content storage element 98 or other suitable data storage device. The data storage device typically is coupled to a processor or controller, e.g., the controller 96. The controller accesses the necessary instructions from the data storage element and executes the instructions or transfers the instructions to the appropriate location within the bypass encapsulation apparatus 90.

[0047] As discussed hereinabove, the last-hop router 74 can be configured to be or include as a portion thereof the bypass encapsulation apparatus 90. In such arrangement or embodiment, the last-hop router 74, e.g., via its controller, is configured to identify the IP packets or other IP content for bypass encapsulation. The last-hop router 74 also is configured to apply or perform the appropriate bypass encapsulation, and to transmit the bypass encapsulated IP content directly to the EQAM 28, bypassing the CMTS 62. The IP content emerges from the EQAM 28 as a DOCSIS flow, e.g., a downstream DOCSIS RF signal from the point of view of the network elements 32. In such arrangement, the last-hop router 74 is configured to signal to appropriate components within the system 70, e.g., the CMTS 62, the packet cable multimedia QoS mechanism (e.g., the Proxy CSCF 82) and other elements of the DOCSIS bypass control plane, e.g., one or more elements containing bypass encapsulation information.

[0048] In this manner, the last-hop router 74 can be signaled when to apply the bypass encapsulation and when to bypass to a new IP content flow. Then, the last-hop router 74 can access and obtain appropriate bypass encapsulation information from a database or otherwise made available by an appropriate component within the system 70 that contains the appropriate bypass encapsulation information. Such information can

include the 5-tuple with which to identify the packets of that new video flow, such as the Source and Destination IP addresses, the Source and Destination Layer 4 port numbers, and the IP protocol type. The last-hop router 74 also can obtain other bypass encapsulation fields for the new data flow, such as the hardware address for the network element 32 to which the IP content video is destined, and the IP address of the EQAM 28 to which to send the bypass encapsulated IP content. With such bypass encapsulation information, the last-hop router 74 is able to perform the bypass encapsulation and then transmit the encapsulated IP content directly to the appropriate EQAM 28, e.g., via an appropriate tunnel, such as a DEPI tunnel.

[0049] Also, as discussed hereinabove, alternatively, the EQAM 28 can be configured to be or include as a portion thereof the bypass encapsulation apparatus 90. In such arrangement or embodiment, the EQAM 28, e.g., via its controller, is configured to apply or perform bypass encapsulation on the IP content identified by the last-hop router 74 for bypass encapsulation. The last-hop router 74 identifies the IP content for bypass encapsulation by accessing or obtaining the appropriate bypass encapsulation information, e.g., from one or more databases or other components within the system 70. The last hop router 74 also sets up a tunnel to the appropriate EQAM 28, and transmits the IP content for a given bypass flow to the EQAM 28 via this tunnel. In this case, the tunnel is an IP over IP type tunnel, such as a Generic Routing Encapsulation (GRE) tunnel.

[0050] The EQAM 28 then applies or performs the actual bypass encapsulation. For example, the EQAM 28 accesses or obtains bypass encapsulation fields and other bypass

encapsulation information from an appropriate database or other component within the system, e.g., the same components used by the last-hop router 74 to access or obtain bypass encapsulation information. For example, the EQAM 28 downloads the DOCSIS MAC Header field, the DOCSIS MAC Extended Header field and other appropriate fields for performing the bypass encapsulation. The EQAM 28 also downloads the necessary QoS fields for the given DOCSIS data flow. Such QoS information can be access or obtained from the ERM 89 or other appropriate component within the system 70. With the appropriate bypass encapsulation information, the EQAM 28 is able to perform the bypass encapsulation and provide the correct QoS levels for that flow. The EQAM 28 then transmits the bypass encapsulated IP content as a DOCSIS flow, e.g., a downstream DOCSIS RF signal, to the network elements 32.

[0051] Various routers within an IP content delivery system, e.g., the IP content delivery system 70, are able to initiate tunnels, such as L2TP (DEPI) tunnels and GRE tunnels. However, such routers typically are not equipped to apply or perform bypass encapsulation. Therefore, it may be more convenient to modify or configure the EQAM 28 to perform bypass encapsulation rather than the last hop router 74. In this manner, the bypass encapsulation process can be divided between the last hop router 74 and the EQAM 28. That is, the last hop router 74 identifies the IP content that is to be carried via the bypass encapsulation and sends the IP content to the appropriate EQAM 28, which performs the bypass encapsulation on the IP content identified for bypass encapsulation. DOCSIS EQAMs generally are able to terminate L2TP (DEPI) tunnels, therefore, using such a tunnel typically does not require any modification to either the last-hop router 74

or the EQAM 28. However, adding the ability to terminate a GRE tunnel likely will require a modification of an EQAM 28.

[0052] Using this arrangement, an MSO can automatically provide DIBA encapsulation, delivery and Quality of Service to over-the-top content or other IP content from the Internet. The MSO can use relatively standard last hop routers and modified EQAMs. Because EQAMs intrinsically are cable devices, their configurations lend themselves to modification for bypass encapsulation.

[0053] According to an alternative arrangement, bypass encapsulation is performed by a separate component or group of components coupled between the last-hop router 74 and the EQAM 28. Referring to Fig. 6, shown is a block diagram of an IP content delivery system that includes a stand-alone bypass encapsulation apparatus 90. In this arrangement, the last-hop router 74 identifies IP content for bypass encapsulation, e.g., as discussed hereinabove, and transmits the IP content for a given bypass flow to the bypass encapsulation apparatus 90. The bypass encapsulation apparatus 90 performs bypass encapsulation and transmits the encapsulated IP content to the EQAM 28 for transmission to the network elements 32, as discussed hereinabove.

[0054] The specific data flows associated with the IP content bypass encapsulation as described hereinabove now will be described. Initially, the data flows are described for an IP content delivery system in which last-hop router both identifies the IP content for bypass encapsulation and performs the bypass encapsulation, i.e., the bypass encapsulation apparatus is included as a portion of the last-hop router.

[0055] First, the end user client or IP content client, which is assumed to be or include an SIP-enabled browser provided by the MSO, selects desired IP content from a web site, e.g., by “clicking” or otherwise obtaining the Uniform Resource Locator (URL) of the IP content. In response, the browser sends an SIP INVITE command to the P-CSCF 82 to set up a new bypass flow. The SIP INVITE command includes various information about the IP content and the desired end user transaction, including the URL of the selected IP content and the IP address and Layer 3 port of the destination end user (customer) premises equipment (CPE). At this stage, typically, it is not yet known if there is a QoS agreement between the IP content provider and the MSO.

[0056] The P-CSCF 82 searches for the URL in a database or other appropriate location to see if there is a QoS agreement between the MSO and the provider of the selected IP content. If there is an QoS agreement, the P-CSCF 82 locates the associated QoS settings. The P-CSCF 82 also locates the IP address of the IP content provider associated with the URL of the selected IP content. Such IP address could be made available from the Internet. Alternatively, if the IP address is cached locally, the P-CSCF 82 can access the IP address information locally. Also, alternatively, it is possible that the content web site and the IP content client (within the network element 32) are modified to communicate the necessary QoS for the IP content to the IP content client. In this manner, the IP content client is able to signal directly to the P-CSCF 82 the necessary QoS for this IP content.

[0057] The P-CSCF 82 activates the QoS mechanism using the PAM 86. Then, using the Policy Server 88, the PCMM communicates with the CMTS 62 (via COPs) to set up

the gate for the IP content data flow. In response, the CMTS 62 requests DOCSIS bandwidth via the ERM 89 and an EQAM 28. The CMTS 62 obtains the necessary bandwidth on an available EQAM 28. The CMTS 62 then sets up a DOCSIS DEPI tunnel from the CMTS 62 to the particular EQAM 28. In the case where the last hop router 74 is generating a DOCSIS Packet Streaming Protocol (PSP) flow to the EQAM 28, this tunnel is needed to pass certain DOCSIS MAC management information to the EQAM 28, such as Mac Domain Descriptors (MDDs). MDDs are needed for the downstream DOCSIS channel 44 from the EQAM 28 to the cable modem portion of the network element 32, and are generally generated by the CMTS 62.

[0058] The CMTS 62 then sets up the IP content data flow to the network elements 32 (e.g., a cable modem) of the end user client who selected the particular IP content. As part of this data flow setup, various information is exchanged between the CMTS 62 and the end user network elements 32, such as a Service Flow ID and QoS settings and the downstream DOCSIS carrier frequency. Also, the CMTS 62 issues requests for a Dynamic Service Addition and for a Downstream Bonding Channel.

[0059] The CMTS 62 makes available necessary DOCSIS bypass headers and other bypass information for use by other components, such as the last-hop router 74, later in the process. For example, the CMTS 62 can enter certain data fields into a database or other data repository that is accessible by the last-hop router 74 or other component that will perform bypass encapsulation. Such information can include the Source Port, the IP Destination Port, the CPE MAC address, the PSP Flow ID, the PSP Initial Sequence

Number, the EQAM IP address and the EQAM port number. The CMTS 62 then signals back to the P-CSCF 82, via the PCMM, of a successful QoS setup.

[0060] Upon successful QoS setup, the last hop router 74 obtains the necessary bypass encapsulation header information provided by the CMTS 62, e.g., from a database or other data repository accessible to both the CMTS 62 and the last-hop router 74. For example, the P-CSCF 82 can issue an SIP invite command to the last hop router 74. Once the last-hop router 74 has obtained the bypass packet inspection information and encapsulation information, the last-hop router 74 issues an SIP OK message back to the P-CSCF 82. In response, the P-CSCF 82 issues an SIP OK message to the IP content client. The IP content client then can initiate data flow of the selected IP content (e.g., using an HTTP GET command) from the IP content source (or from a local cache if the IP content previously was stored locally). In this manner, the IP content data flow begins from the IP content source to the last-hop router 74.

[0061] Upon receiving the IP content from the IP content source, the last-hop router 74 (e.g., the bypass encapsulation apparatus 90 portion of the last-hop router 74) performs bypass encapsulation on the received IP content. The last-hop router 74 then transmits the bypass encapsulated IP content directly (via DEPI tunnel) to the EQAM 28, bypassing the CMTS 62. The IP content flow transmitted to the EQAM 28 then is transmitted over the non-primary downstream DOCSIS channel 44 to the network elements 32 and the IP content client, e.g., in a conventional manner.

[0062] The specific data flows associated with the IP content bypass encapsulation now will be described for an IP content delivery system in which last-hop router

identifies the IP content for bypass encapsulation and the EQAM performs the bypass encapsulation, i.e., the bypass encapsulation apparatus is included as a portion of the EQAM. Many of the data flows are similar to or the same as the data flows for the IP content delivery system in which the last-hop router performs the bypass encapsulation. For example, in response to an end user client or IP content client selecting desired IP content from a web site, the browser sends an SIP INVITE command to the P-CSCF 82 to set up a new bypass flow.

[0063] The P-CSCF 82 searches for the URL of the selected IP content to see if there is a QoS agreement between the MSO and the IP content provider. If there is an QoS agreement, the P-CSCF 82 locates the associated QoS settings. The P-CSCF 82 also locates the IP address of the IP content provider associated with the URL of the selected IP content, either from the Internet or from local cache. Alternatively, it is possible that the content web site and the IP content client (within the network element 32) are modified to communicate the necessary QoS for the IP content to the IP content client. In this manner, the IP content client is able to signal directly to the P-CSCF 82 the necessary QoS for this IP content.

[0064] The P-CSCF 82 then activates the PCMM QoS mechanism, and the PCMM communicates with the CMTS 62 (via COPS) to set up the gate for the IP content data flow. In response, the CMTS 62 requests DOCSIS bandwidth via the ERM 89 and an EQAM 28, and obtains the necessary bandwidth on an available EQAM 28. The CMTS 62 then sets up a DOCSIS DEPI tunnel from the CMTS 62 to the EQAM 28, and sets up the IP content data flow to the appropriate end user network elements 32.

[0065] Like the example previously described herein, a PSP session for IP content data flow can be established. The CMTS 62 uses the PSP/DEPI tunnel to transmit DOCSIS management packets to the EQAM 28. As in the previous data flow description, the CMTS 62 makes available necessary DOCSIS bypass headers and other bypass information for use by other components, such as the last-hop router 74 and the EQAM 28, later in the process. Such information, which can be entered into a database or other data repository accessible by the last-hop router 74 and the EQAM 28, can include the Source Port, the IP Destination Port, the CPE MAC address, the PSP Flow ID, the PSP Initial Sequence Number, the EQAM IP address and the EQAM port number.

[0066] The last-hop router 74 then accesses or retrieves the bypass packet identification information, such as the source and destination IP addresses, the source and destination port numbers, and the IP payload type, provided by the CMTS 62, e.g., from the database or data repository. It is also possible that the PAM 86 or the general PCRF 84 uses a control interface to the last hop-router 74 to set the forwarding policy in that router. This policy would include the packet identification information given hereinabove, and the specific layer 3 tunnel in which to forward these IP video packets to the appropriate EQAM 28. The last-hop router 74 is informed to which EQAM 28 the new IP content flow is to be sent. The last-hop router 74 then sets up a GRE or other layer 3 tunnel to that EQAM 28. The last-hop router 74 also uses the information about the EQAM 28 to identify the IP content packets and route them directly to the EQAM 28, instead of to the CMTS 62 (as in conventional system arrangements).

[0067] The EQAM 28 also accesses or retrieves the bypass encapsulation header information from the database or data repository. The EQAM 28 also can allow a DEPI tunnel to be set up from the last-hop router 74 for bypass data flow, although such allowance is optional. The EQAM 28 also sets up the appropriate internal queuing for the bypass data flow. The database then signals back to the CMTS 62 that the encapsulation information has been retrieved by the last-hop router 74 and the EQAM 28.

[0068] The CMTS 62 then signals back to the P-CSCF 82, via the PCMM, of a successful QoS setup. In response, the P-CSCF 82 issues an SIP OK message to the IP content client. The IP content client then can initiate data flow of the selected IP content (e.g., using an HTTP GET command) from the IP content source (or from a local cache if the IP content previously was stored locally). In this manner, the IP content data flow begins from the IP content source to the last-hop router 74.

[0069] Upon receiving the IP content from the IP content source 72, the last-hop router 74 identifies the packets for the selected IP content and transmits them, via a tunnel, directly to the EQAM 28. The EQAM 28 (e.g., the bypass encapsulation apparatus 90 portion of the EQAM 28) performs bypass encapsulation on the received IP content. Once the EQAM 28 has performed the bypass encapsulation, the EQAM 28 sends the encapsulated IP content over the non-primary downstream DOCSIS channel 44 to the network elements 32 and the IP content client. Also, a PSP link from the CMTS 62 to the EQAM 28 is used to carry DOCSIS management packets to the EQAM 28 and the network elements 32.

[0070] FIG. 7 shows the data encapsulations at various stages in the IP content delivery system of FIG. 4, in which the EQAM performs the bypass encapsulation of the IP content.

[0071] Referring now to FIG. 8, with continuing reference to FIGs. 4-6, shown is a flow chart that schematically illustrates a method 200 for delivering IP content within a system that includes a bypass architecture for over-the-top content. The method 200 includes a step 202 of transmitting IP content from the IP content source 72 to the last-hop router 74, e.g., via the network 76. The IP content can be transmitted from an Internet source or from a locally-cached IP content source. Also, the method 200 includes a step 204 of the last-hop router 74 identifying IP content for bypass encapsulation.

[0072] As discussed hereinabove, the IP content delivery system 70 can include a last-hop router 74 that is configured to identify IP content for encapsulation and to perform bypass encapsulation on the identified IP content. Accordingly, once the last-hop router has identified the IP content for encapsulation (step 204), the method 200 can include perform a step 206 of the last-hop router 74 performing bypass encapsulation. In such system, the last-hop router 74 includes the bypass encapsulation apparatus 90. IP content received by the last-hop router 74 (and the bypass encapsulation apparatus 90) is bypass encapsulated by the last-hop router 74. The last-hop router 74 then transmits the bypass encapsulated IP content directly to the EQAM 28, bypassing the CMTS 62. In such arrangement, the method 200 includes a step 208 of the last-hop router 74 transmitting bypass encapsulated IP content to the EQAM 28.

[0073] Alternatively, the IP content delivery system 70 can include a last-hop router 74 that is configured to identify IP content for encapsulation, and an EQAM 28 that is configured to perform bypass encapsulation on the IP content identified by the last-hop router 74. In such arrangement, the EQAM 28 includes the bypass encapsulation apparatus 90. Accordingly, once the last-hop router has identified the IP content for encapsulation (step 204), the method 200 can include perform a step 210 of the last-hop router 74 transmitting the IP content identified for bypass encapsulation to the appropriate EQAM 28. In such arrangement, the method 200 can include a step 212 of the EQAM 28 performing bypass encapsulation. IP content received directly from the last-hop router 74 by the EQAM 28 (bypassing the CMTS 62) is bypass encapsulated by the EQAM 28. For example, the bypass encapsulation is performed by a bypass encapsulation apparatus 90 within the EQAM 28.

[0074] Alternatively, the IP content delivery system 70 can include a last-hop router 74 that is configured to identify IP content for encapsulation, and a separate bypass encapsulation apparatus 90 configured to perform bypass encapsulation on the IP content identified by the last-hop router 74. In this arrangement, once the last-hop router has identified the IP content for encapsulation (step 204), the method 200 can include perform a step 214 of the last-hop router 74 transmitting the IP content identified for bypass encapsulation to the bypass encapsulation apparatus appropriate EQAM 28. In such arrangement, the method 200 can include a step 216 of the bypass encapsulation apparatus 90 performing bypass encapsulation of the IP content received directly from the last-hop router 74 by the bypass encapsulation apparatus 90 (bypassing the CMTS

62). The method 200 also can include a step 218 of the bypass encapsulation apparatus 90 transmitting the bypass encapsulated IP content to the EQAM 28.

[0075] The method 200 also includes a step 220 of the EQAM 28 transmitting bypass encapsulated IP content to the network elements 32 of the end user IP client. The EQAM 28 is configured to send the bypass encapsulated IP content to the network elements 32 via the downstream DOCSIS channel 44.

[0076] The method shown in FIG. 8 may be implemented in a general, multi-purpose or single purpose processor. Such a processor will execute instructions, either at the assembly, compiled or machine-level, to perform that process. Those instructions can be written by one of ordinary skill in the art following the description of FIG. 7 and stored or transmitted on a computer readable medium. The instructions may also be created using source code or any other known computer-aided design tool. A computer readable medium may be any medium capable of carrying those instructions and includes random access memory (RAM), dynamic RAM (DRAM), flash memory, read-only memory (ROM), compact disk ROM (CD-ROM), digital video disks (DVDs), magnetic disks or tapes, optical disks or other disks, silicon memory (e.g., removable, non-removable, volatile or non-volatile), packetized or non-packetized wireline or wireless transmission signals.

[0077] It will be apparent to those skilled in the art that many changes and substitutions can be made to the bypass architecture devices, methods and systems herein described without departing from the spirit and scope of the invention as defined by the appended claims and their full scope of equivalents.

CLAIMS

1. A bypass encapsulation apparatus for use in a system for transmitting internet protocol (IP) content from at least one IP content source to at least one end user network element, wherein the system includes a cable modem termination system (CMTS) coupled between the at least one IP content source and the at least one end user network element, and wherein the system includes a downstream modulator coupled to the cable modem termination system and coupled between the at least one IP content source and the at least one end user network element, the bypass encapsulation apparatus comprising:

a first interface for receiving IP content transmitted from the at least one IP content source;

a controller coupled to the first interface and configured to perform bypass encapsulation on at least a portion of the IP content received by the bypass encapsulation apparatus; and

a second interface coupled to the controller and configured for transmitting bypass encapsulated IP content from the bypass encapsulation apparatus,

wherein the controller performs bypass encapsulation on the IP content received by the bypass encapsulation apparatus in such a way that the bypass encapsulated IP content can be transmitted from the bypass encapsulation apparatus to the at least one end user network element via the downstream modulator in such a way that the bypass encapsulated IP content bypasses the cable modem termination system.

2. The apparatus as recited in claim 1, wherein the bypass encapsulation apparatus is at least a portion of a last-hop router coupled between the at least one IP content source and the downstream modulator.

3. The apparatus as recited in claim 2, wherein the last-hop router provides a bypass communication channel between the last-hop router and the downstream modulator for transmission of the bypass encapsulated IP content from the last-hop router to the downstream modulator.

4. The apparatus as recited in claim 1, wherein the bypass encapsulation apparatus is at least a portion of the downstream modulator, and wherein the bypass encapsulation apparatus performs bypass encapsulation on IP content identified by and transmitted from a last-hop router coupled between the at least one IP content source and the downstream modulator.

5. The apparatus as recited in claim 4, wherein at least a portion of the bypass encapsulation apparatus is coupled between the last-hop router and the downstream modulator.

6. The apparatus as recited in claim 1, wherein the bypass encapsulation apparatus is configured to access bypass encapsulation information made available by the cable modem termination system, wherein the bypass encapsulation apparatus uses the

bypass encapsulation information to perform bypass encapsulation on the IP content received by the bypass encapsulation apparatus.

7. The apparatus as recited in claim 1, wherein the downstream modulator further comprises an Edge Quadrature Amplitude Modulation (EQAM) modulator.

8. The apparatus as recited in claim 1, wherein at least one IP content source includes at least one of a video on demand (VOD) server, an IPTV broadcast video server, and an Internet video source.

9. A method for transmitting internet protocol (IP) content from at least one IP content source to a downstream modulator within an IP content delivery system having a bypass architecture, wherein the IP content delivery system includes a cable modem termination system (CMTS) coupled between the at least one IP content source and the at least one end user network element, and wherein the IP content delivery system includes a downstream modulator coupled to the cable modem termination system and coupled between the at least one IP content source and the at least one end user network element, the method comprising the steps of:

receiving IP content transmitted from the at least one IP content source;

performing bypass encapsulation on at least a portion of the received IP content;

and

transmitting bypass encapsulated IP content to the at least one end user network element,

wherein bypass encapsulation is performed on the received IP content in such a way that the bypass encapsulated IP content can be transmitted to the at least one end user network element via the downstream modulator in such a way that the bypass encapsulated IP content bypasses the cable modem termination system.

10. The method as recited in claim 9, wherein at least a portion of the bypass encapsulation is performed by a last-hop router coupled between the at least one IP content source and the downstream modulator.

11. The method as recited in claim 10, wherein the last-hop router provides a bypass communication channel between the last-hop router and the downstream modulator for transmission of the bypass encapsulated IP content from the last-hop router to the downstream modulator.

12. The method as recited in claim 9, wherein at least a portion of the bypass encapsulation is performed by the downstream modulator.

13. The method as recited in claim 9, wherein at least a portion of the bypass encapsulation is performed by a bypass encapsulation apparatus coupled between the last-hop router the downstream modulator.

14. The method as recited in claim 9, further comprising the step of identifying IP content for bypass encapsulation from among the received IP content transmitted from

the at least one IP content source, wherein the identifying step is performed by a last-hop router having access to bypass encapsulation information, wherein the last-hop router is coupled between the at least one IP content source and the downstream modulator.

15. The method as recited in claim 9, further comprising the step of accessing bypass encapsulation information made available by the cable modem termination system, wherein the bypass encapsulation performing step uses the bypass encapsulation information to perform bypass encapsulation on the IP content.

16. A computer readable medium storing instructions that, when executed on a programmed processor, carry out a method for transmitting internet protocol (IP) content from at least one IP content source to a downstream modulator within an IP content delivery system having a bypass architecture, wherein the IP content delivery system includes a cable modem termination system (CMTS) coupled between the at least one IP content source and the at least one end user network element, and wherein the IP content delivery system includes a downstream modulator coupled to the cable modem termination system and coupled between the at least one IP content source and the at least one end user network element, the computer readable medium comprising:

instructions for receiving IP content transmitted from the at least one IP content source;

instructions for performing bypass encapsulation on at least a portion of the received IP content; and

instructions for transmitting bypass encapsulated IP content to the at least one end user network element,

wherein bypass encapsulation is performed on the received IP content in such a way that the bypass encapsulated IP content can be transmitted to the at least one end user network element via the downstream modulator in such a way that the bypass encapsulated IP content bypasses the cable modem termination system.

17. The computer readable medium as recited in claim 16, wherein at least a portion of the bypass encapsulation is performed by a last-hop router coupled between the at least one IP content source and the downstream modulator.

18. The computer readable medium as recited in claim 16, wherein at least a portion of the bypass encapsulation is performed by the downstream modulator.

19. The computer readable medium as recited in claim 16, further comprising instructions for identifying IP content for bypass encapsulation from among the received IP content transmitted from the at least one IP content source, wherein the identifying step is performed by a last-hop router coupled between the at least one IP content source and the downstream modulator.

20. The computer readable medium as recited in claim 16, further comprising instructions for accessing bypass encapsulation information, wherein the bypass

encapsulation is used by the bypass encapsulation performing instructions for performing bypass encapsulation on the IP content.

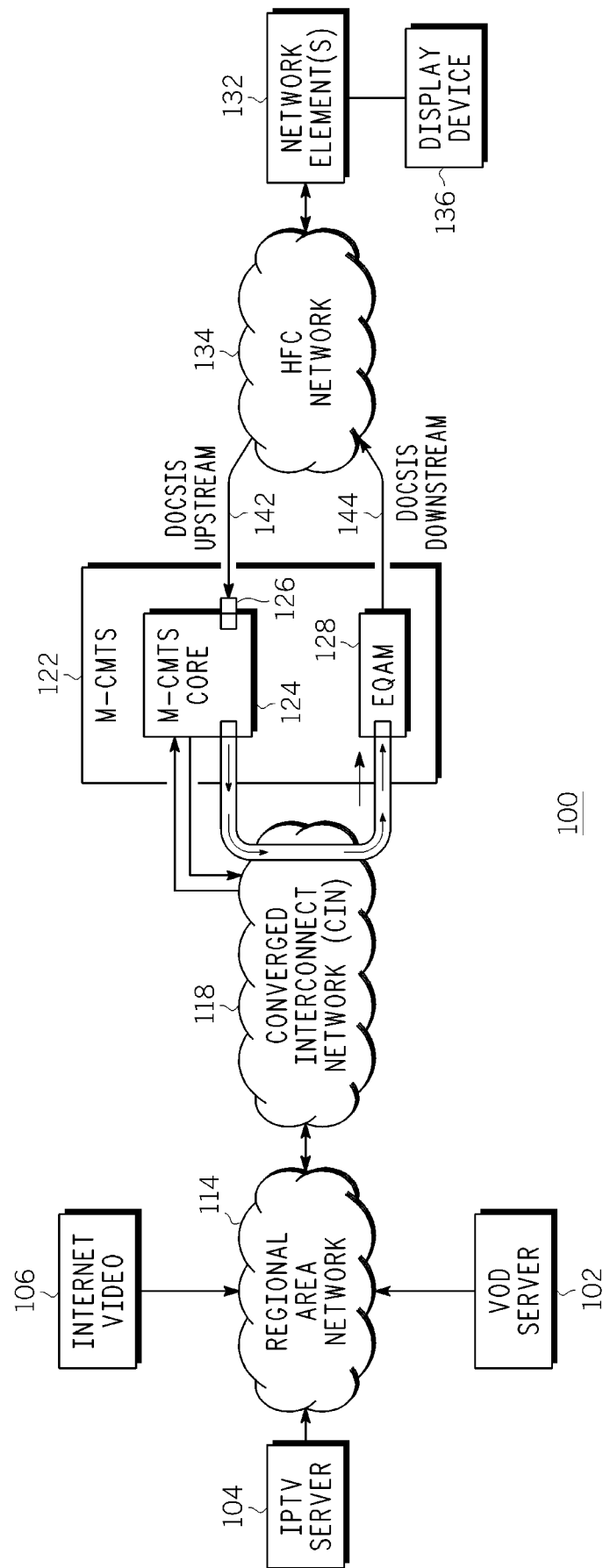
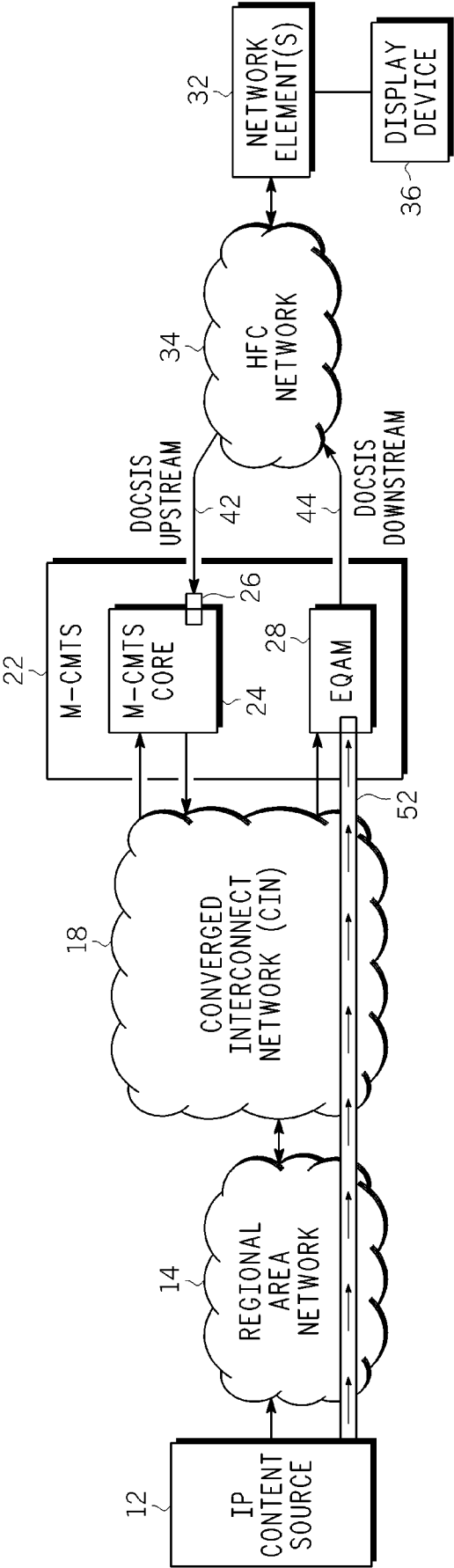
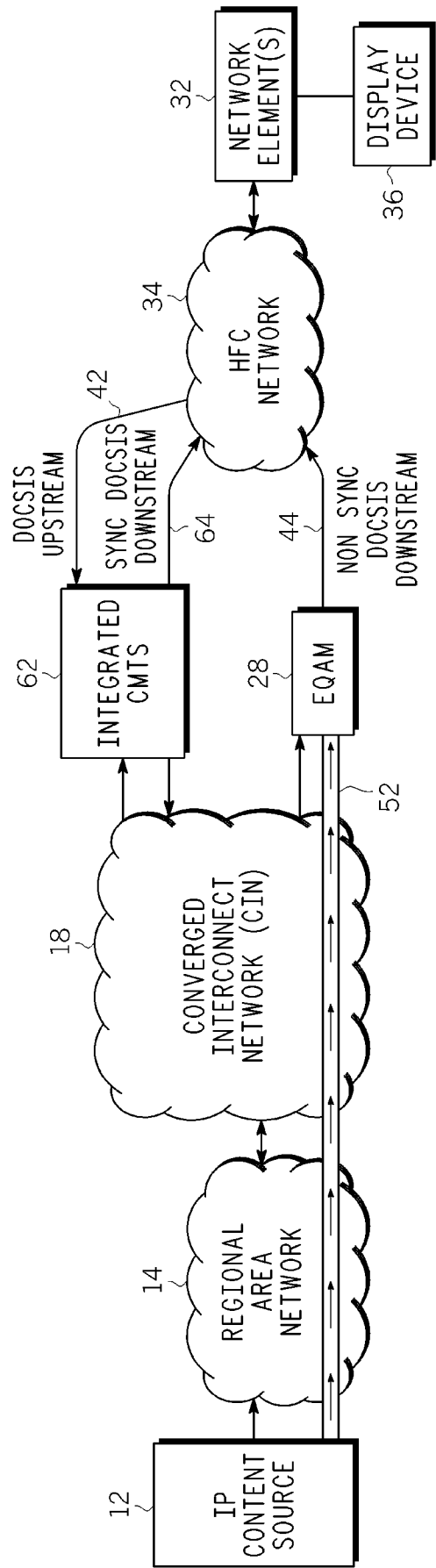


FIG. 1
-PRIOR ART-



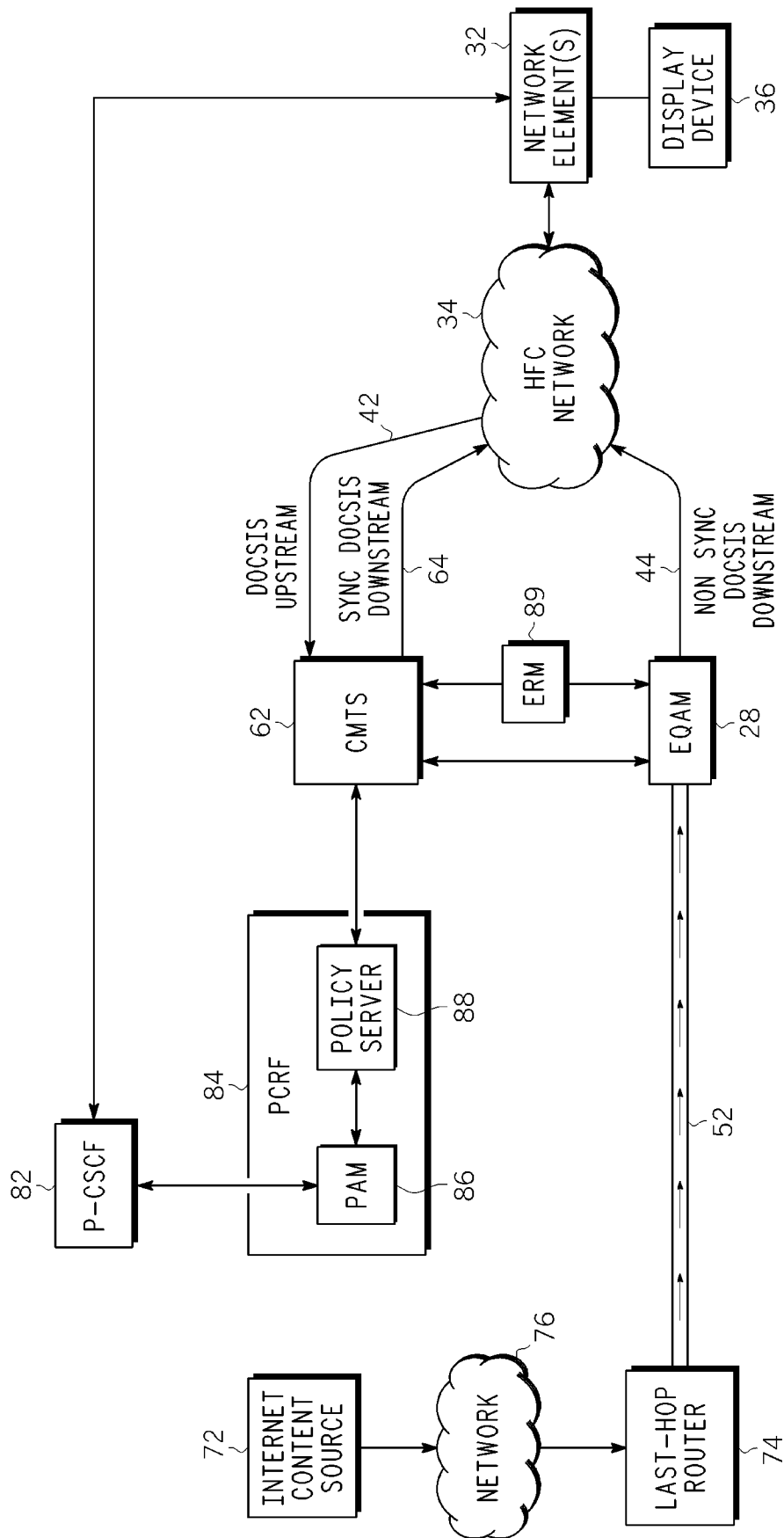
50

FIG. 2



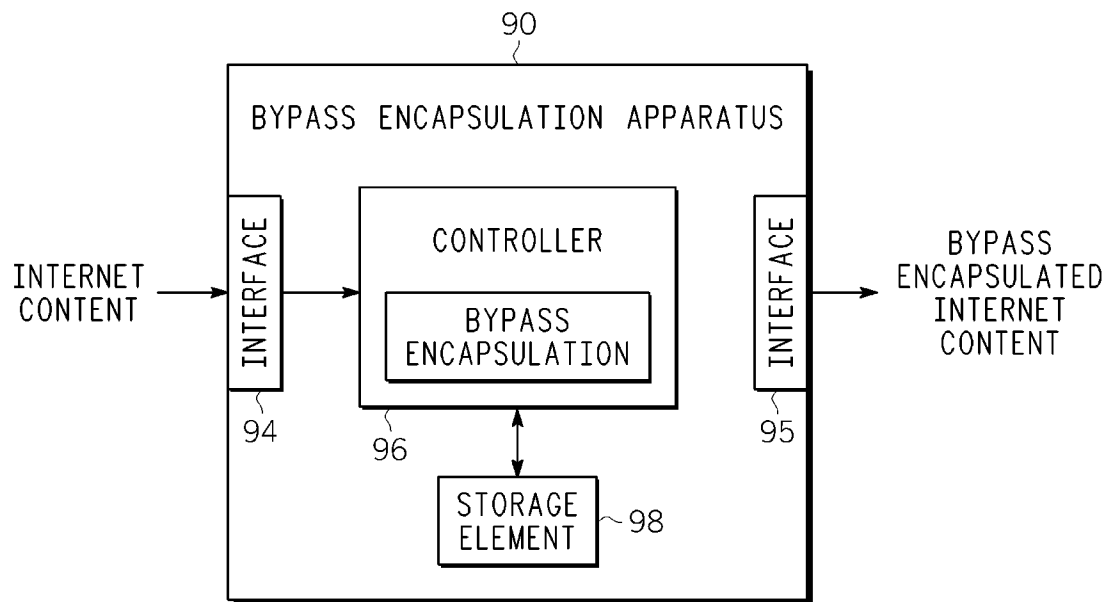
60

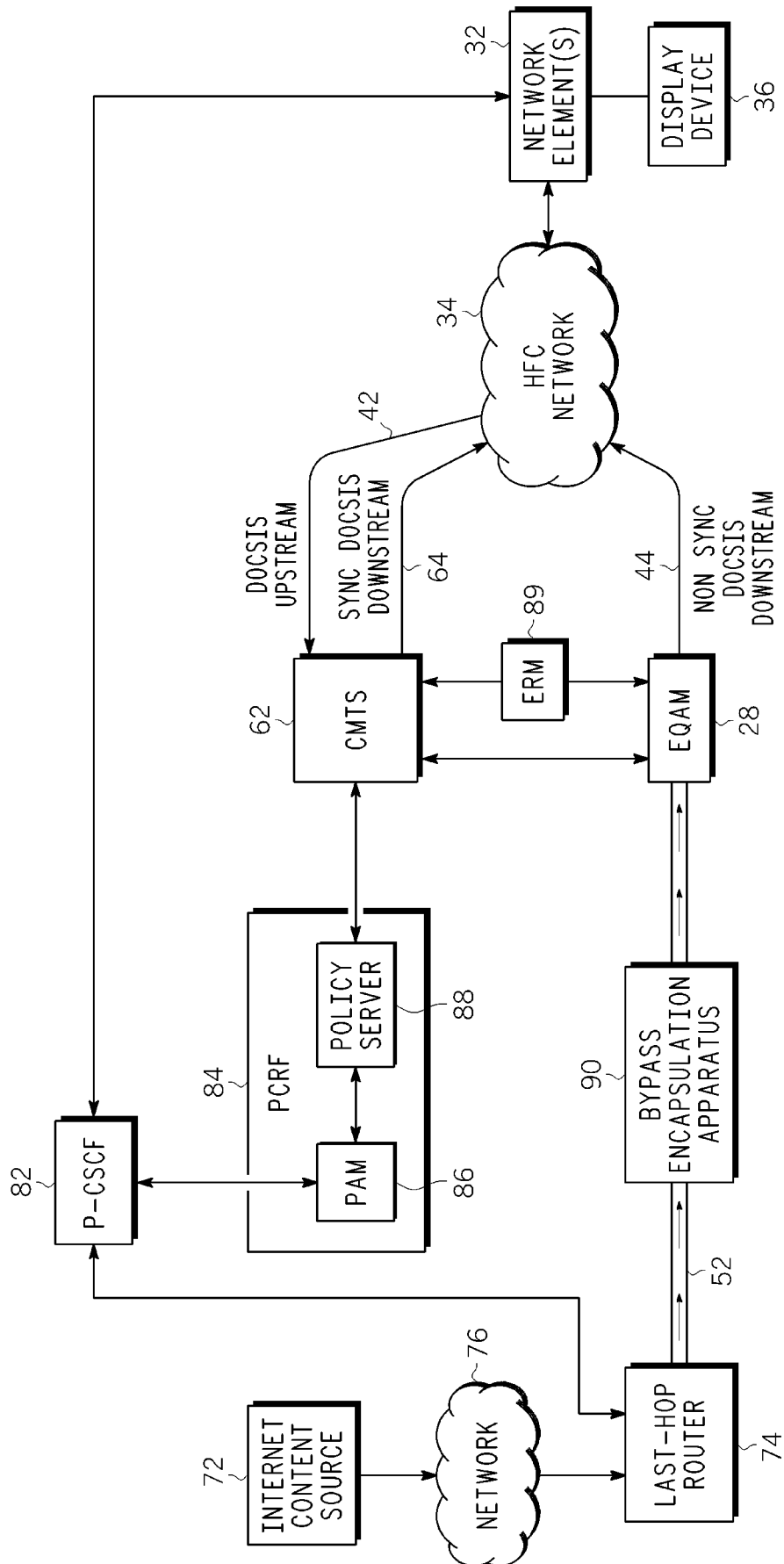
FIG. 3



70

FIG. 4

**FIG. 5**



70

FIG. 6

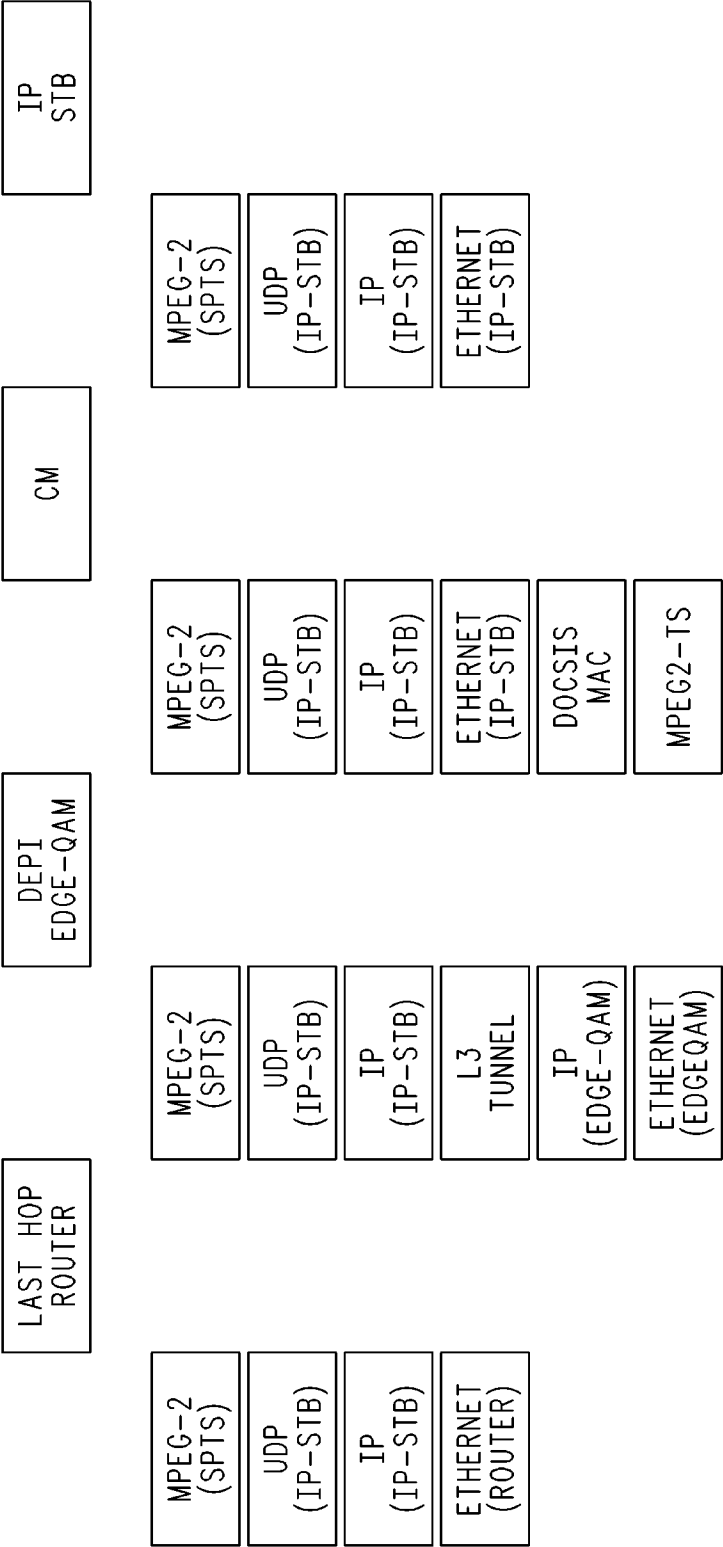
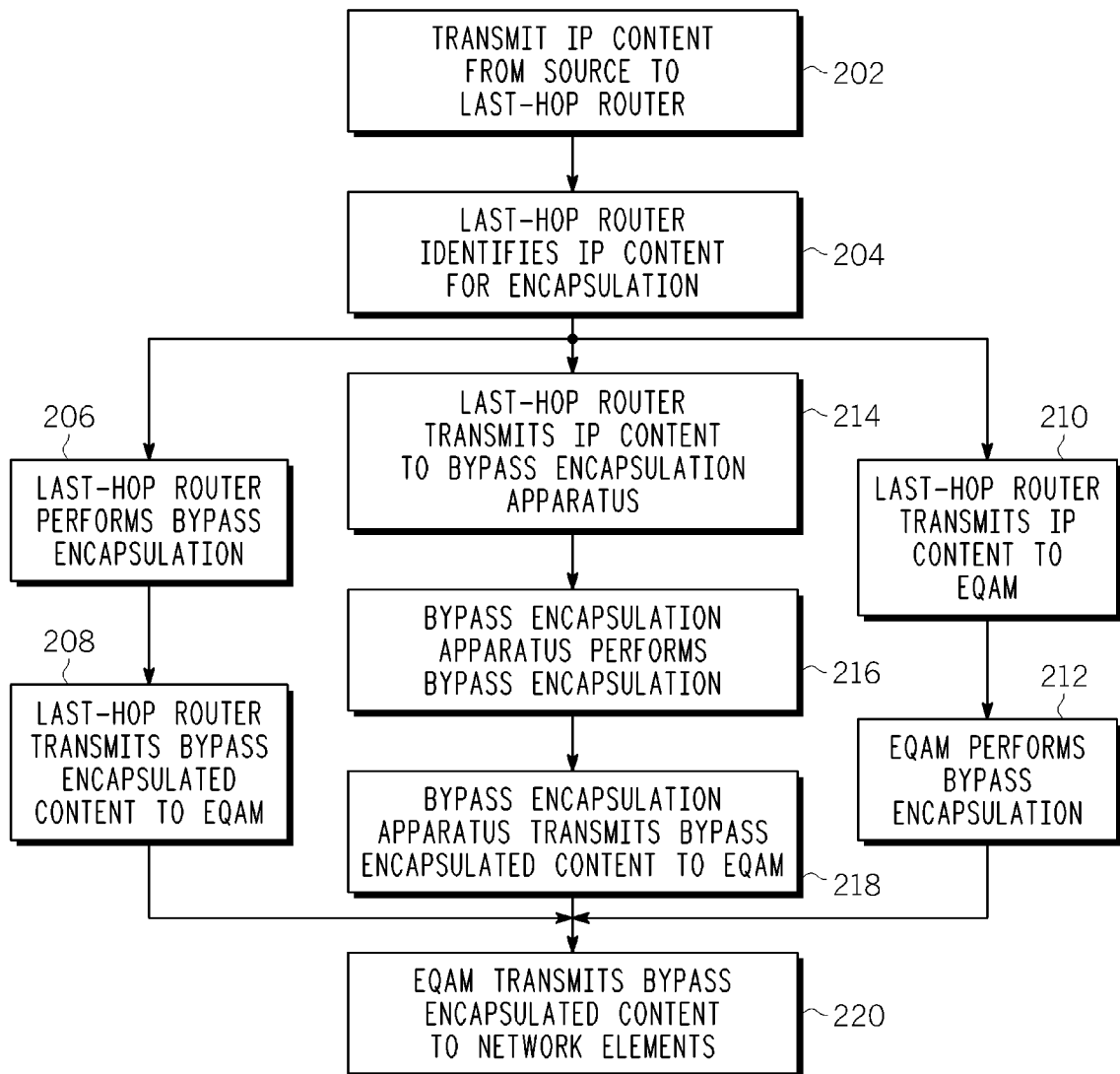


FIG. 7



200

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US2009/046965

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - H04N 7/173 (2009.01)

USPC - 725/111

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC(8) - H04N 7/173 (2009.01)

USPC - 725/111, 109, 131, 119, 138, 139; 370/527, 467, 395.52, 395.62

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

USPTO WEST System (US, USPG-PUB, EPO), Google Patent., Google scholar, PateBase, IEEE Xplore

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Patrick, Michael, Joyce, Gerald. Delivering Economical IP Video over DOCSIS by Bypassing the M-CMTS with DIBA, SCTE, 23-25 Jan. 2007 [Retrieved on 22 July 2009]. Retrieved from the internet: <URL: http://broadband.motorola.com/BCNewsletter/0507_docs/MOTOROLA%20DIBA%20SCTE%20ET%20Paper%202007-final.pdf > entire document	1-20
A, P	US 7,539,216 B2 (JOHNS et al) 26 May 2009 (26.05.2009) entire document	1-20
A	US 2006/0225118 A1 (ROLLS et al) 05 October 2006 (05.10.2006), entire document	1-20

☐ Further documents are listed in the continuation of Box C.


* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

23 July 2009

Date of mailing of the international search report

04 AUG 2009

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents

P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-3201

Authorized officer:

Blaine R. Copenheaver

PCT Helpdesk: 571-272-4300

PCT OSP: 571-272-7774