1

INTRODUCTION AND OVERVIEW

Mehmet Toy

1.1 INTRODUCTION

Cable companies (multiple system operators or MSOs) have been offering phone and TV services over copper medium as the basic residential services for a long time. With the proliferation of broadband, fiber, and wireless technologies, fiber is deployed to provide TV, voice, and Internet services (i.e., triple play) while serving rates over cable are increased with new techniques in supporting triple-play services.

MSOs have been providing residential services over coaxial cable using the Data Over Cable Service Interface Specification (DOCSIS) protocol that permits the addition of high-speed data transfer to an existing cable TV (CATV) system in Mbps currently and aims at supporting capacities of at least 10 Gbps downstream and 1 Gbit/s upstream.

Toward the end of 1990s, MSOs initiated PacketCable project to deliver real-time communication services, namely Voice over Internet Protocol (VoIP). Later, content distribution network (CDN) is created to deliver content to deliver video distribution over IP. IP television (IPTV) system delivered television using IP over a packet-switched network such as a LAN or the Internet. For delivering IP multimedia services, IP Multimedia Subsystem (IMS) architectural framework was introduced by 3rd Generation Partnership Project (3GPP). MSOs provide both residential and commercial services over IMS platform today.

Cable Networks, Services, and Management, First Edition. Edited by Mehmet Toy.

In recent years, in order to centralize data and video applications on a single platform to reduce overall system cost, MSOs introduced Converged Cable Access Platform (CCAP).

In addition to residential services, MSOs have been offering services to small- and medium-sized enterprises (SMEs), and large businesses. Metro Ethernet services in the form of private line, virtual private line, and multipoint-to-multipoint services are among them. In order to optimize MSO networks and improve quality and rates of service offerings, DOCSIS 3.1, DOCSIS provisioning of EPON (DPoE), EPON protocol over coax (EPoC), and Wi-Fi systems have been introduced. CCAP will support business services as well.

Chapter 2 describes architecture and services for DOCSIS 3.0/3.1, CCAP, CDN, IP TV, and PacketCable and Wi-Fi for residential services.

Chapter 3 describes operational systems and management architectures, service orders, provisioning, fault management, performance management, billing systems and formats, and security for residential services.

Chapter 4 describes architecture and services for Carrier Ethernet, DPoE, EPoC, CCAP, IMS for business services.

Chapter 5 describes operational systems and management architectures, service orders, provisioning, fault management, performance management, billing systems and formats, and security for business services.

Finally, Chapter 6 explains the future directions for cable networks by describing cloud services, virtualization, SDN, and the author's proposed self-managed network concepts with their applications.

1.2 RESIDENTIAL NETWORK ARCHITECTURES AND SERVICES

MSOs provide residential services over coaxial cable using the Data Over Cable Service Interface Specification (DOCSIS) protocol. PacketCable project was initiated to deliver real-time communications services, namely VoIP. Later, Content Distribution Networks (CDN) is created to deliver content to deliver video distribution over IP. The goal is to serve content to end-users with high availability and high performance. In order to deliver television using IP over a packet-switched network such as a LAN or the Internet, Internet Protocol television (IPTV) system was introduced. Many advanced communications services to users are delivered by IP Multimedia Subsystem (IMS).

In order to reduce cost by centralizing data and video applications on a single platform, MSOs introduced Converged Cable Access Platform (CCAP). CCAP is expected to dramatically increase system capacity and density to enable the MSOs the ability to protect and maximize existing infrastructure investment, and provide orderly migration of existing video services to IP video.

The DOCSIS system allows transparent bi-directional transfer of Internet Protocol (IP) traffic, which is called High Speed Data (HSD) Internet or Broadband service, between the cable system head-end and customer location, over an all-coaxial or hybrid-fiber/coax (HFC) cable network. The service is supported by a Cable Modem Termination

System (CMTS) or a CCAP at the head-end, and a Cable Modem (CM) at customer location. It is also possible to support this service with a PON system at head-end and Optical Networking Unit (ONU) at customer location.

The CMTS and CCAP head-end devices reside within the MSO's core network and are generally considered secure. The CM provides the demarcation point between the subscriber and the MSO's network. It is considered unsecure and untrusted. Due to the different nature of each of these devices as well as differing business and technical requirements, they are managed differently from the MSO's back office.

DOCSIS 3.0 protocol is the currently deployed within MSO networks today. DOCSIS 3.0 and DOCSIS 3.1 systems were designed to support high capacities with predictable Quality of Service (QoS). The DOCSIS 3.0 protocol supports 240 Mbps in the upstream and 1.3 Gbps in the downstream, while the DOCSIS 3.1 protocol increases the upstream and downstream capacities significantly promising 2 Gbps and 10 Gbps on the upstream and downstream respectively.

In 1990s, MSOs began looking for value-added services such as VoIP that could ride on top of their newly deployed DOCSIS technology. The PacketCable project was initiated for the delivery of real-time communications services over the two-way cable plant. PacketCable 1.5 was designed to provide traditional voice telephone service, and subsequently PacketCable 2.0 was designed to provide advanced multi-media services beyond basic voice.

In order to reach a large population of leased or consumer-owned devices, enable linear and on-demand video to non-technical subscribers, and provide a viewing experience similar to traditional TV, MSOs developed IPTV service delivery architecture. The video services comprise local linear video, national linear video, video-on-demand (VOD), and pay-per-view (PPV).

National VOD programming is typically delivered to MSOs over satellite as well, where the video asset and its associated metadata are placed on a satellite by the content programmers, beamed by the satellite to all of the MSOs who are authorized to distribute that content, received by the MSOs, and placed onto the appropriate VOD distribution servers and represented in a navigational client so that customers can find the video content.

Content Distribution Networks (CDN) are created to deliver content, whether video or web pages as quickly as possible, with the least latency, at the lowest cost, to the widest quantity of consumers who are spread over a disparate geographic area. A CDN is an interconnected network of servers used to deliver web assets to consuming devices in an efficient manner, taking advantage of caching of content to reduce or eliminate the retransmission of a single asset to multiple consumers. This chapter describes deploying a CDN for video distribution over IP, the architecture of a CDN, services supplied by a CDN and areas for future CDN research.

CCAP will dramatically increase system capacity and density to enable MSOs the ability to protect and maximize existing critical infrastructure investment, by delivering various access technologies from the same chassis. It will play a vital role in completing a smooth transition to IP video transport and an "all IP" service offering more generally, in lock-step with the ongoing evolution of the HFC plant and every increasing capacity needs per user.

Wi-Fi is becoming a network of choice for both service providers (SPs) and consumers alike. This chapter reviews some of the recent technological advances in the Wi-Fi domain and describes residential network architecture and services over DOCSIS, CDN, Packet Cable, IMS and CCAP.

1.3 OAMPT (OPERATIONS, ADMINISTRATION, MAINTENANCE, PROVISIONING, TROUBLESHOOTING) FOR RESIDENTIAL SERVICES

OAMPT capabilities are necessary to order and maintain the residential services described in Chapter II. In addition to OAMPT, services need to be billed to subscribers.

Service order process begins with sales. Once the service order is in, the provisioning process installs equipment at customer premises, sets-up equipment at customer premises and central offices, sets-up user accounts, and creates new circuits. The provisioning processes will also include checklists that need to be strictly adhered to and signed off, and integration and commissioning processes which will involve sign-off to other parts of the business life cycle.

Operations encompass automatic monitoring of the environment, detecting and determining faults and alerting network administration. Network administration collects performance statistics, accounts data for the purpose of billing, plans capacity based on usage data, maintains system reliability, administers network security, and maintains the service database for periodic billing.

Maintenance involves routine equipment checks, upgrading software and hardware, fixes, new feature enablement, backup and restore, standard network equipment configuration changes as a result of policy or design, and monitoring facilities. When there is a failure, failed components are identified by diagnostic tools and troubleshooting.

OAMPT for residential services are challenging mainly due to the involvement of a very large number of Customer Premises Equipment (CPE), facilities and connections (i.e., in the order of millions). As a result, automation for each OAMPT function is crucial for MSOs. Autoprovisioning of CPE and connections, administration of network security via DOCSIS protocol and back office systems are developed to resolve these scalability issues.

The DOCSIS service and device management approach uses FCAPS (Fault, Configuration, Accounting, Performance, and Security) model, to organize the requirements for the configuration and management of the CMTS/CCAP and CM devices.

Fault management is a proactive and on-demand network management function that allows abnormal operation on the network to be detected, diagnosed, and corrected. When an abnormal condition is detected, an autonomous event (often referred to as an alarm notification) is sent to the network operations center (NOC) to alert the MSO of a possible fault condition in the network affecting a customer's service. Once the MSO receives the event notification, further troubleshooting and diagnostics can be performed by the MSO to correct the fault condition and restore the service to proper operation.

Configuration Management provides a set of network management functions that enables system configuration building and instantiating, installation and system turn up,

network and device provisioning, auto-discovery, backup and restore, software download, status, and control (e.g., checking or changing the service state of an interface). DOCSIS Configuration Management is typically performed at the network layer (e.g., device provisioning at the CMTS/CCAP and CM).

Accounting Management is a network management function that allows MSOs to measure the use of network services by subscribers for the purposes of cost estimation and subscriber billing. Subscriber Accounting Management Interface Specification (SAMIS), as defined in DOCSIS, is an example of an implemented Accounting Management function.

Performance Management is a proactive and on-demand network management function which is gathering and analyzing "statistical data for the purpose of monitoring and correcting the behavior and effectiveness of the network, network elements (NEs), or other equipment and to aid in planning, provisioning, maintenance and the measurement of quality." A Performance Management network layer and service-level use case might include the NOC performing periodic (15 min, for example) collections of Quality of Service (QoS) measurements from network elements to perform monitoring and identification of any potential performance issues that may be occurring with the service being monitored.

Security Management provides for the management of network and operator security, as well as providing an umbrella of security for the telecommunications management network functions including authentication, access control, data confidentiality, data integrity, event detection, and reporting.

The CM and CMTS reside within the Network Layer where services are provided to end subscribers and various metrics are collected about network and service performance, among other things. Various management servers reside in the Network Management Layer within the MSO back office to provision, monitor and administer the CM within the Network Layer.

The major service and network management features introduced in the DOCSIS 3.1 protocol specification include configuration, monitoring and reporting on the feature set DOCSIS Light Sleep Mode (DLS), Backup Primary Channels, Active Queue Management (AQM) and Proactive Network Maintenance (PNM). The DOCSIS service and device management approach used for the DOCSIS 3.1 network remains the same as the DOCSIS 3.0 network for the CM management model. With respect to DOCSIS 3.1 management of the CMTS, the management model is aligned with the CCAP management approach, where configuration management using XML-based configuration files is used.

Provisioning of CM is primarily performed using the configuration file download process. Binary configuration files are constructed using the TLV definitions from the DOCSIS specifications.

Fault management is a proactive and on-demand network management function including Alarm Surveillance, Fault Localization, Fault Correction, and Testing. When service-impacting abnormalities of an NE is detected, an autonomous event (often referred to as an alarm notification) is sent to the network operations center (NOC) to alert the MSO of a possible fault condition in the network affecting a customer service. Once the NOC receives the event notification, further troubleshooting and diagnostic testing can be performed on-demand by the NOC to correct the fault condition and restore the service to proper operation.

Performance Management is a proactive and on-demand network management function which is gathering and analyzing "statistical data for the purpose of monitoring and correcting the behavior and effectiveness of the network, NEs, or other equipment and to aid in planning, provisioning, maintenance and the measurement of quality. NOC periodically (15 min, for example) collects Quality of Service (QoS) measurements from network elements to perform monitoring and identification of any potential performance issues that may be occurring with the service being monitored. With the historical data that has been collected, trending analysis can be performed to identify issues that may be related to certain times of day or other corollary events.

For the DOCSIS 3.0 and 3.1 networks, identified performance metric data sets implemented in the CMTS and CCAP, both Simple Network Management Protocol (SNMP) and IP Detail Record/Streaming Protocol (IPDR/SP) protocols are available for bulk data collection of the data sets. MSO business policies and back office application architectures dictate which protocol is utilized for collecting the various performance metrics.

The core function of the "Billing" system is to generate an accurate bill. The name "billing" is a misnomer because it indicates just one of the many functions have been built into these software applications. Some of the biller functions are Product Catalogue, the CPE Inventory, the Order Entry system, the Service Order Manager, the Taxation Engine, the Biller as well as the Workforce Manager (determining the number of availability of installation technicians), and the Serviceable Homes Database of the operator (which premises are serviceable for what services).

When providing content and services over a network to subscribers it is important to apply proper security. There are many threats that exist that can negatively impact a subscriber's experience and service provider's business. These threats include spoofing, tampering and information disclosure.

DOCSIS 3.0/3.1 security features focus on preventing theft of service and loss of privacy. The main features are device authentication and traffic encryption, secure software download, and secure provisioning. A DOCSIS CM is provisioned by sending its configuration file to the CM which it then forwards to the CMTS. Since the CM is untrusted, it is important that security controls are in place to verify service settings.

This chapter further describes OAMPT including security and billing for residential services.

1.4 BUSINESS NETWORK ARCHITECTURES AND SERVICES

MSOs offer services to small and medium size enterprises (SMEs) and large businesses. Carrier Ethernet services in the form of private line, virtual private line and multipoint-to-multipoint services are among them.

As in residential services, business services can be voice, data and video services. The nature of services can differ depending on the size of the business. For example voice services for small and medium size enterprises (SMEs) might involve interfacing Private Branch Exchanges (PBXs) at customer premises and managing voice mailboxes while voice services for a large corporation might involve providing a private network

serving many locations. Furthermore, services for large corporations require better availability, better performance and multiple classes of services.

MSOs offer various Carrier Ethernet commercial services. They use service OAM capabilities of Metro Ethernet extensively. Automation of Metro Ethernet equipment and service provisioning is underway.

Carrier Ethernet is connection-oriented by disabling unpredictable functions such as MAC learning, Spanning Tree Protocol and "broadcast of unknown." It is scalable from 10 Mbps to 100 Gbps with finer granularity as low as 56 Kbps and 1 Mbps. With QoS and synchronization capabilities, applications with strict performance requirements such as Mobile Backhaul are being supported. Port and connection level fault monitoring, detection and isolation, performance monitoring and statistics and protection failover are available.

Some service providers are concerned of the scalability of Carrier Ethernet. There is an effort by Cloud Ethernet Forum (CEF) to increase scalability of Carrier Ethernet by using Provider Backbone Bridge (PBB) and Provide Backbone Transport (PBT).

Carrier Ethernet services are delivered to users at fiber, copper and coax user interfaces. The services over fiber interfaces can employ point-to-point and point-to-multipoint architectures such as Passive Optical Network (PON) which is characterized by having a shared optical fiber network which supports a single downstream transmitter and multiple simultaneous upstream transmitters. The downstream transmitter, an Optical Line Terminal (OLT), is typically located in the head end or hub of a service provider's network. Optical Network Units (ONUs) located on the customer premise terminate the PON. A passive optical splitter/combiner enables the fiber to be divided to reach multiple customer locations. The OLT schedules each ONU for upstream transmission and guarantees the frames do not overlap.

Business Real-Time Communications Services include both legacy business voice-calling services such as hunt groups and paging, and advanced communications services such as video conferencing and desktop-sharing. In Hosted IP-Centrex service, the service provider owns and manages the service and the service delivery equipment. The business customer has no equipment to buy, and simply pays a monthly subscription fee for the service. With SIP Trunking service, the business customer owns and operates the service delivery equipment, while the service provider simply provides the SIP Trunk that connects the SIP-PBX to the global telecom network.

This chapter covers architecture and services for business customers over DOCSIS, IMS, Metro Ethernet, DPoE, and EPoC technologies.

1.5 OAMPT FOR BUSINESS SERVICES

In Chapter 3, we described OAMPT for residential services. OAMPT is also crucial for business services. In fact, the OAMPT requirements for business services are tighter than those for residential services. This is due the fact that degraded or lost services can have larger financial impact.

In order to process service orders, keep inventory, configure equipment, provision services, collect measurement and accounting data, secure network access, report service

degradation and failures, troubleshoot the failures and fix them, and bill customers, MSOs have operations systems dedicated for business services.

Equipment manufacturers usually have their own Element Management System (EMS) to manage a Network Element (NE) such as a router and their own Network Management System (NMS) to manage a subnetwork of NEs. It is possible to combine these management systems with operators' operation systems to perform the OAMPT functions. In some cases, operators may choose to use only their operations systems to manage their network consisting of multiple vendor equipment.

Service providers have a need to tie together ordering, payment, and operation of systems. For example, when a typical enterprise service is provisioned, it would typically operate it at its maximum capacity. In contrast, a service provider selling a similar or even the same service to an enterprise may sell a fixed bandwidth service, a burstable service, or a billable service that must measure and count traffic.

The scale of service provider networks also dictates more automation. Service providers need to build processes to accept changes from business customers such as a move in location, additions of new locations or services at an existing location, or other changes such as capacity upgrades or downgrades.

Unlike most enterprise networks, service providers need to have means to control the traffic in their networks so as to avoid conflicts between the performance, quality, and reliability for both different services running on the same network and for different customers running on the same network.

In this chapter, operations systems, service order provisioning, fault management, performance management and security for business services over DOCSIS, CCAP, IMS, Metro Ethernet, DPoE, and EPoC have been described.

1.6 FUTURE DIRECTIONS IN CABLE NETWORKS, SERVICES AND MANAGEMENT

The previous chapters describe highly complex MSO residential and commercial networks and services, and their management. These networks and management systems have proven to be scalable and allow MSOs to create and offer new competitive services to their customers.

MSOs can reduce CAPEX and OPEX, and amount of time to create new services. The concepts of Cloud Services, Virtualization, Software Defined Networks (SDN) and Self-Managed will help MSOs to achieve these goals. In fact, there are substantial efforts in MSOs to take advantage of these new technologies. Some MSOs do provide Cloud based services today.

Self-Managed networks will be an ultimate goal for the industry and requires substantial changes in how equipment and management systems are built and operated.

Substantial growth in high speed personal devices such as phones, laptops and IPAD, and IP video and IPTV applications are driving huge bandwidth demand in networks. Applications such as storage networking, video streaming, collaborative computing, and online gaming and video sharing are driving not only bandwidth demand in networks, but also resources of various data centers connected with these networks.

The concepts of cloud computing and cloud-based services are expected to help service providers to deal with these challenges.

Cloud Computing technologies are emerging as infrastructure services for provisioning computing and storage resources on-demand. Multi-provider and multi-domain resources, and integration with the legacy services and infrastructures are involved.

Cloud based virtualization allows for easy upgrade and/or migration of enterprise application, including also the whole IT infrastructure segments. This brings significant cost saving comparing to traditional infrastructure development and management that requires lot of manual work.

Cloud based applications operate as regular applications in particular using web services platforms for services and applications integration, however their composition and integration into distributed cloud based infrastructure will require a number of functionalities and services.

Virtual infrastructure provides a layer of abstraction between computing, storage and networking hardware, and the applications running on it. Virtual infrastructure gives administrators the advantage of managing pooled resources across the enterprise, allowing IT managers to be more responsive to dynamic organizational needs and to better leverage infrastructure investments.

Virtualization separates a resource or request for a service from the underlying physical delivery of that service. With virtual memory, for example, computer software gains access to more memory than is physically installed, via the background swapping of data to disk storage. Similarly, virtualization techniques can be applied to networks, storage, server hardware, operating systems, applications, and so on.

Virtualization can be Management Virtualization, Network Virtualization, Hardware Virtualization, Storage Virtualization, Operating System Virtualization, Application Server Virtualization, Application Virtualization, Service Virtualization that are described in details.

Software-Defined Networking (SDN) is defined by Open Networking Foundation (ONF) as an emerging architecture that decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services.

The switching plane can be heterogeneous, composed of network elements from multiple vendors, and it can provide distinct services with different characteristics, configurations, and control at the packet and/or optical layers. Abstracting the control plane from the network elements allows network-platform-specific characteristics and differences that do not affect services to be hidden. In addition, SDN is based on the principle that applications can request needed resources from the network via interfaces to the control plane. Through these interfaces, applications can dynamically request network resources or network information that may span disparate technologies.

As communication networks have grown in size and complexity, streamlining the architecture and implementation to reduce costs, simplify management, improve service provisioning time, and improve resource utilization has become increasingly important. Ideally, an application or service could be completely decoupled from the underlying network infrastructure, but this is not always realistic. Parameters that affect application performance, such as bandwidth, packet loss, and latency, are closely tied to the

underlying network. To meet application performance objectives, it becomes necessary for the underlying network to be aware of the application requirements and provides the necessary services.

There is a great deal of optimism that SDN will make networks more flexible, dynamic, and cost-efficient, while greatly simplifying operational complexity. Vendors has begun unveiling its open network environment, extending network capabilities and extracting greater intelligence from network traffic through programmatic interfaces.

Rise of cloud services and virtualization, and large-scale computing and storage in huge data-centers require on-demand availability of additional network capacity (i.e. scalability), rapid service creation and delivery. SDN is expected to automate service provisioning at least and help service providers to deliver services much quicker.

The infrastructure consists of both physical and virtual network devices such as switches and routers. These devices implement the OpenFlow protocol as a standards-based method of implementing traffic forwarding rules. The control layer consists of a centralized control plane for the entire network to provide a single centralized view of the entire network. The control layer utilizes OpenFlow to communicate with the infrastructure layer.

The application layer consists of network services, orchestration tools, and business applications that interact with the control layer. These applications leverage open interfaces to communicate with the control layer and the network state.

Virtualization, Cloud, and SDN concepts are mainly focused on operational efficiency and maximum utilization of network resources. Further operational efficiencies can be achieved with self-managed networks. Network resources and services should be automatically provisioned, and faulty components should be automatically identified and fixed by the network itself. The future networks are very likely to be self-managed.

This chapter describes Cloud, Virtualization, SDN, and Self-Managed concepts, and provides examples.