EXCENTIS

excellence
in telecom
and ict
services

testing
consulting
training
products

Study on the Network Termination Point of Internet access and Telephony over Cable Networks (HFC)

Version: 1.0, January 29, 2015

Table of contents

List of Abbreviations

ANSI	American National Standards Institute
CATV	Cable Television
CM	Cable Modem
CMCI	Cable Modem to Customer Premises Equipment Interface
CMTS	Cable Modem Termination System
CPE	Customer Premises Equipment
DOCSIS	Data-over-Cable Service Interface Specification
DS	Downstream (Forward Path)
DVB-C	Digital Video Broadcasting-Cable
EN	European Norm
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
HFC	Hybrid Fiber Coax
MULPI	Mac-and Upper Layer Protocols Interface Specification
NAT	Network Address Translation
NTP	Network Termination Point
ON	Optical Node
PAL	Phase Alternate Line
PKI	Public Key Infrastructure
RF	Radio Frequency
SCTE	Society of Cable Telecommunications Experts
TDM	Time Division Multiplexing
UL	Underwriters Laboratories
US	Upstream (Return path)
VOD	Video On Demand
WDM	Wavelength Division Multiplexing

Executive Summary

This document is the result of a study by Excentis on the Network Termination Point (NTP) for Internet Access and Telephony over cable networks (Hybrid Fibre Coax infrastructure (HFC)).

For telephony services it turned out that the NTP is the analogue twisted pair connection point, where customers can plug in their own phone. Cable operators provide such analogue twisted pair interface for telephony services on their cable modems by typically an RJ11-connector. This interface follows the same specifications as the Deutsche Telekom Telephony Network Termination Point as defined in 1TR110[1]. Consumers can use their existing telephony sets (analogue phones, DECT systems, etc.) to the provided interface.

For Internet Access, based on the analysis, it is concluded that the NTP in cable networks should be the well-known and consumer familiar Ethernet interface. This interface is defined in the DOCSIS standard (in the CMCI interface specification[2]). As the most important criterion this view puts the responsibility regarding the proper operation of the delivered service (esp. the internet speed) on the cable operator. This is because only in this case the cable operator remains fully responsible (and in control) of the complex interaction between cable modem (CM) and cable modem termination system (CMTS). The customer on the other hand still has full flexibility to connect any device (router, computer, etc.) to the Ethernet interface on the cable modem. This solution refrains from restrictions regarding end-user devices while clearly making the cable operator responsible for the technology that provides the service (internet access) to the house. It also protects the consumer from investing in devices that cannot be used on the network.

The analysis also shows that the Radio Frequency (RF)-interface should not be defined as the NTP. This is due to many reasons:

- In a cable network there is the possibility that one bad modem interferes with the internet and telephony service of a large group of customers.
- Allowing customers to use or install their own software on cable modems is a very big security risk to cable networks and has to remain impossible at all means, since it can introduce problems both related to network operations (interfering with the services of many other users), and as well problems related to security and authentication.
- Modems might have specific interoperability issues with the network and/or equipment of the operator. A Cable Modem purchased by the consumer might not be compatible with the network or become incompatible during the network's evolution. Such equipment would have to be replaced by the consumer.
- Retail Modems might not be ready for new services that the operator wants to offer.
- Consumers have no easy way to check the speed offered at the RF-interface; on the other hand, the speed offered to the CMCI interface can easily be verified.

[1] 1 TR 110 "Technische Beschreibung der Analogen Wählanschlüsse am T-Net/ISDN der T-Com

[2] Data-Over-Cable Service Interface Specifications, Cable Television Laboratories, Inc. 2008-2014, CM-SP-CMCIv3.0 Interface between cable modem and CPE (Customer Premises Equipment) (normative reference in ETSI EN 302 878-4)

1 Introduction

Excentis was commissioned by ANGA to make an independent study on the Network Termination Point (NTP) in the context of Internet access and telephony over a cable network.

The European directives leave the definition of the Network Termination Point up to the network operator under recital 24 of the R&TTE Directive.

The document provides an overview of cable networks in section 2, including a short comparison to xDSL networks, which is followed by an overview of the operation of Internet Access over cable networks in section 3. In Section 4 the analysis for the definition of the NTP is conducted and a conclusion is drawn. The Key Points are highlighted in boxes.

2 Technical overview of cable networks

2.1 Structure of a cable network

The architecture of an HFC network is shown in Figure 1. A digital backbone is used to bring the different signals to the headends (HE in the figure). From each headend fibers are used to connect to the different optical nodes (ON on the figure) in the field. The part between headend and optical node is shown in more detail in Figure 2.

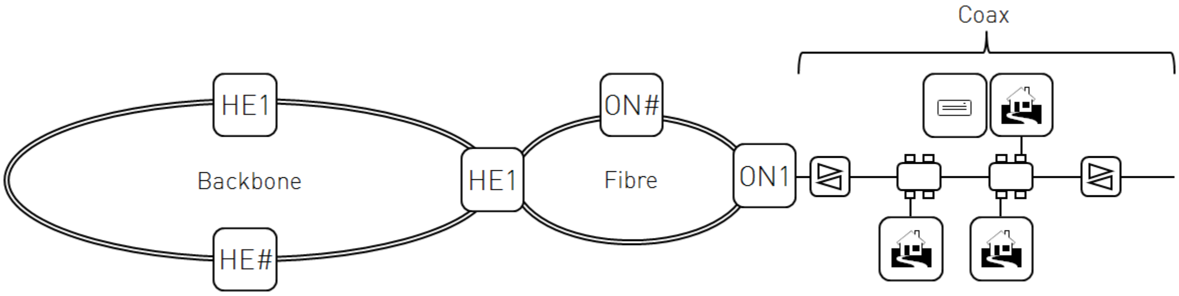

Figure 1: Architecture of cable network

Logically, two fibers are used between each node and the headend. One for the downstream (forward) signal and one for the upstream (return) signal. It is possible to also carry multiple signals over a single fiber using techniques like WDM.

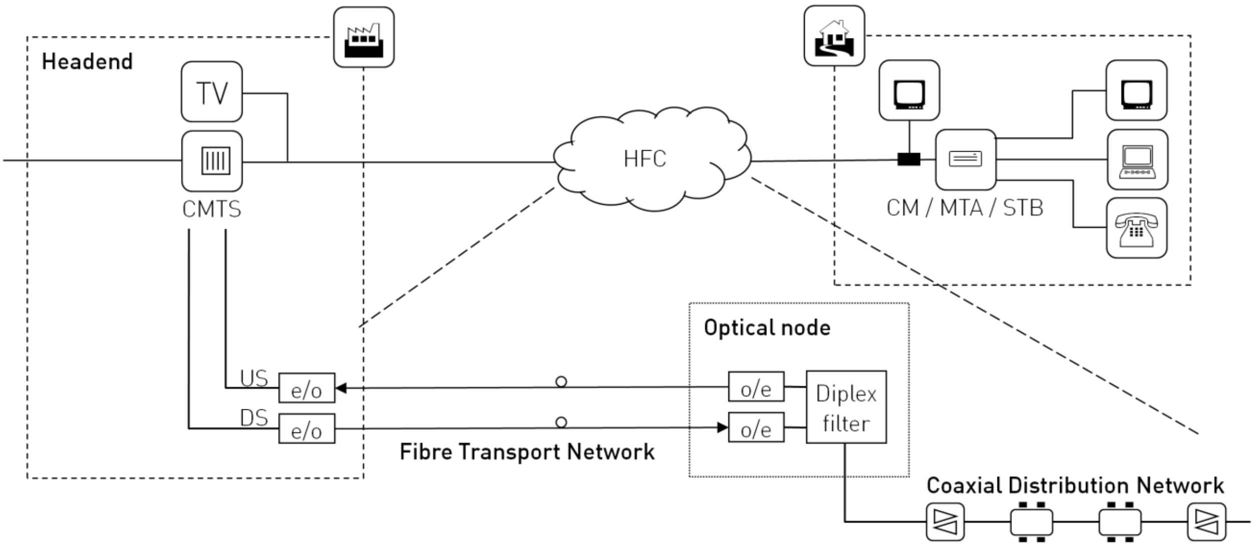

Figure 2: HFC-part of cable network

On the coaxial part of the network, both the upstream and downstream signals are present. By using a different frequency band, it is possible to use bidirectional electrical amplifiers in the coaxial part of the network. In the coaxial part, taps are used to bring the signal to each individual household. The upstream spectrum that is used in Europe goes from 5 to 65 MHz. In the downstream the frequencies between 87.5 MHz up to 1002 MHz are used. Coaxial cables used in CATV networks have a characteristic impedance of 75 Ohm.

Figure 1 and Figure 2 show that many households are connected to a single coaxial cable (shared medium) on which all the different services are present.

2.2 Radio Frequency (RF) spectrum usage

The spectrum in the downstream is used for the delivery of different services to the households:

- Analogue Television and FM radio
- Digital Television (including VOD)
- Internet (IP)
- Telephony (runs over IP)

In CATV networks signals for analogue TV, digital TV and EuroDOCSIS (IP) are placed in the cable frequency spectrum one next to the other without causing interference to each other. Due to the broadcast nature of a cable network the full spectrum is typically occupied.

An example of a possible spectrum allocation is shown in Figure 3.

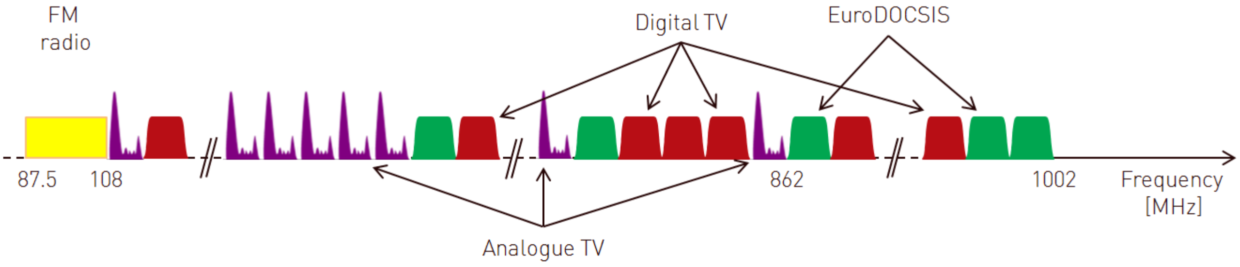

Figure 3: Example spectrum usage

As a consequence of the structure of CATV networks all signals present on the coaxial cable reach all households (shared medium) within that optical node (group of houses). By using different frequencies the different services (e.g. analogue TV, digital TV, Internet (EuroDOCSIS) do not interfere with each other.

2.3 Shared Medium

Unlike many other technologies for fixed telecommunications services cable networks are a shared medium in the access network. This means that a group of houses (all houses connected to a node) are connected through taps to the same physical coaxial cable. These houses share the electrical signal that is transmitted by the headend towards the customers (so called downstream signal). This means that the electrical signal that carries information for one customer is also physically present at the coaxial cables that enter the houses of all other customers connected on the same fiber node.

In the direction from the customer houses towards the operator (so called upstream) the different connected devices (cable modems) also share the same spectrum. This means that a very advanced control mechanism needs to be used to make sure that the transmissions from the different devices do not interfere with each other. If one modem transmits with a wrong timing, wrong frequency or wrong power level it causes disturbance to the services received by all other modems on that fiber node.

An example of communication over such a shared medium within a single frequency band is shown in Figure 4. Note that this figure only illustrates communication over a shared medium in a single frequency band. In reality different frequency bands are used at the same time as well.

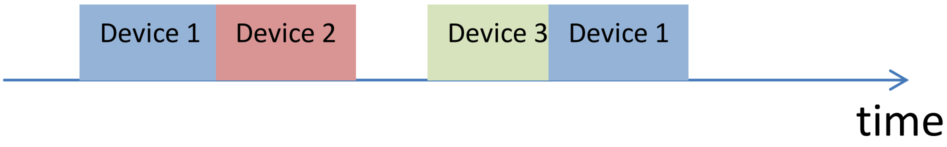

Figure 4: Example of communication over a shared medium

As can be seen in Figure 4 in a shared medium it is essential that each device only transmits at the time interval that has been allocated to the device (Time Division Multiplexing). For this type of communication advanced scheduling and synchronization is therefore required.

As a cable network is a shared medium, advanced synchronization and scheduling is needed and all devices that are connected to the network must respect the rules of transmission as otherwise communication for all devices on the node (group of houses) is disturbed.

Due to the nature of a shared medium it is not possible to detect where (in which house) a certain device is located. As a consequence strong authentication is needed on the device itself to identify the device. Since the medium is shared all communication has to be encrypted as otherwise it would be easy to wiretap on the communication.

Key Points

In cable networks the electrical signal that carries information for one customer in the downstream is also physically present at the coaxial cables that enter the houses of all other customers connected on the same fiber node. In the upstream, all signals from all modems are combined at the headend. If one modem transmits with a wrong timing, wrong frequency or wrong power level it causes disturbance to the services received by all other modems on that fiber node. Consequently, advanced synchronization and scheduling is needed and all devices that are connected to the network must respect the rules of transmission. This requires strong authentication on the device itself to identify the device.

2.4 Comparison to xDSL networks

The structure of an xDSL network is shown in Figure 5. The main characteristic is that there is a dedicated twisted pair from each house to the central office of the operator. Since there is a dedicated point-to-point link in the access network, each xDSL modem is identified by the line (wire) on which it is connected. As a consequence, there is no need for strong authentication. Further, the impact from a defective device is limited to the individual user and any security issues are also limited to the individual user.

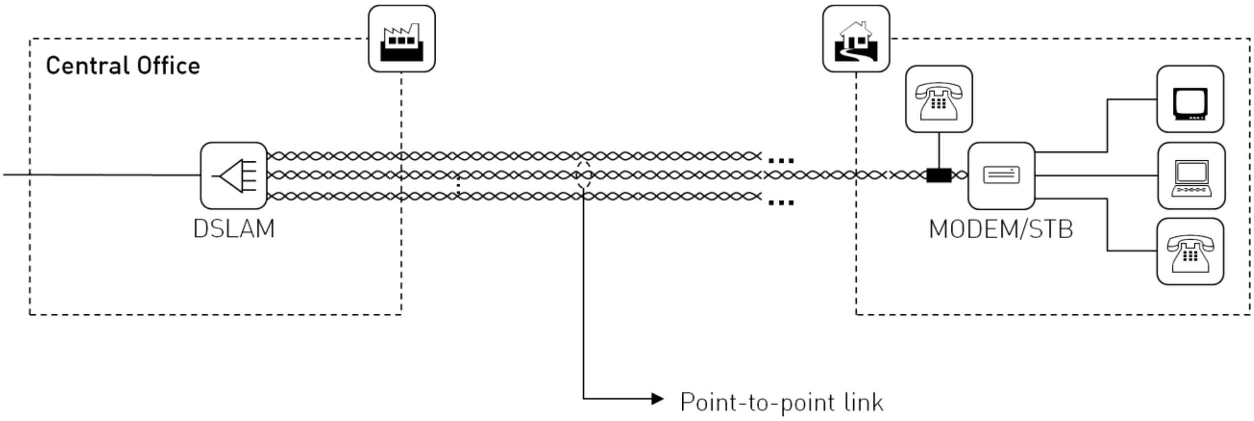

Figure 5: Structure of an xDSL network

3 Internet Access over Cable Networks

Internet access in a cable network is provided over DOCSIS technology. Currently deployed DOCSIS uses the same modulation techniques as digital television (i.e. DVB-C with 64QAM or 256QAM). The cable modem termination system (CMTS) is the device located in the headend that generates the downstream signals and receives the upstream signals. In EuroDOCSIS one or more downstream channels (each 8 MHz) are used to transport data and signaling packets to the cable modems. Cable modems share the bandwidth of these channels. Up to EuroDOCSIS 2.0 a cable modem is only demodulating a single downstream channel of 8 MHz (which is still shared with other modems). With EuroDOCSIS 3.0 channel bonding is used. With this technology a single modem can use multiple (currently typically 4 to 16) downstream channels at the same time, which are of course still shared with other modems. The downstream channels are placed in the same spectrum as digital television and can be allocated anywhere in the RF spectrum from 108 MHz up to 862 MHz. EuroDOCSIS 3.0 defines the frequency band above 862 MHz and up to 1002 MHz as an option.

For the return path, currently, EuroDOCSIS uses the frequency spectrum between 5 and 65 MHz. Modems are assigned upstream channels to use by the CMTS. A single upstream channel is shared in a TDM-way by different modems, the CMTS acts as the master and controls which modem is allowed to transmit at what time.

The next generation of the DOCSIS standard (called 3.1) is already defined (at the day of writing no products are available yet).

Key Point

Internet access in a cable network is provided over DOCSIS technology. Cable Modems share the channels used for both, down- and upstream.

3.1 DOCSIS defined interfaces

EuroDOCSIS has a set of specifications that define the minimum requirements that Cable Modems and Cable Modem Termination Systems have to fulfill to be considered EuroDOCSIS compliant.

The set of specifications for the 3rd generation of the standard is given in table 1.

Table 1: Specification overview

Specification	Abbreviation of interface	Summary
CM-SP-CMCIv3.0	DOCSIS Cable Modem to CPE Interface specification	Interface between cable modem and CPE (Customer Premises Equipment) (c.f. section 3.1.1 below)
CM-SP-MULPIv3.0	DOCSIS 3.0 MAC and Upper Layer Protocols Interface Specification	Defines the full MAC-protocol and all functionality above (IP-layer, etc.)

CM-SP-OSSIv3.0	DOCSIS 3.0 Operations Support System Interface Specification	Specifies management protocols and variables for the CM and CMTS
CM-SP-PHYv3.0	DOCSIS 3.0 Physical Layer Specification	Defines the physical layer (RF) requirements
CM-SP-SECv3.0	DOCSIS 3.0 Security Specification	Defines the authentication and encryption and additional security requirements for CM and CMTS
CM-SP-DRFI	Downstream RF Interface Specification	Defines the requirements for the downstream signal of the CMTS

The relation between ETSI, CableLabs and ANSI/SCTE specifications is given in table 2.

Note that the CMCI specification is a normative reference in ETSI EN 302 878-4. So it is a well defined interface in the ETSI specifications for DOCSIS.

The DOCSIS specification is available in three different standardization bodies:

- ETSI: European Telecommunications Standards Institute
- CableLabs; Membership organization of cable operators
- ANSI/SCTE: American National Standards Institute/Society of Cable Telecommunications Engineers

Table 2: Overview ETSI, CableLabs and ANSI/SCTE DOCSIS specifications

ETSI Standards number	Based on CableLabs	ANSI/SCTE standards number	Summary
EN 302 878-1 (V1.1.1)	None	None	Defines the relationship between the different parts
EN 302 878-2 [1] (V1.1.1)	CM-SP-PHYv3.0-I09-101008	ANSI/SCTE 135-1	Defines the physical layer (RF) requirements
EN 302 878-3 [2] (V1.1.1)	CM-SP-DRFI-I10-100611	ANSI/SCTE 133	Defines the requirements for the downstream signal of the CMTS
EN 302 878-4 [3] (V1.1.1)	CM-SP-MULPIv3.0-I14-101008	ANSI/SCTE 135-2	Defines the full MAC-protocol and all functionality above (IP-layer, etc.)
EN 302 878-5 [4] (V1.1.1)	CM-SP-SECv3.0-I13-100611	ANSI/SCTE 135-3	Defines the authentication and encryption and additional security requirements for CM and CMTS

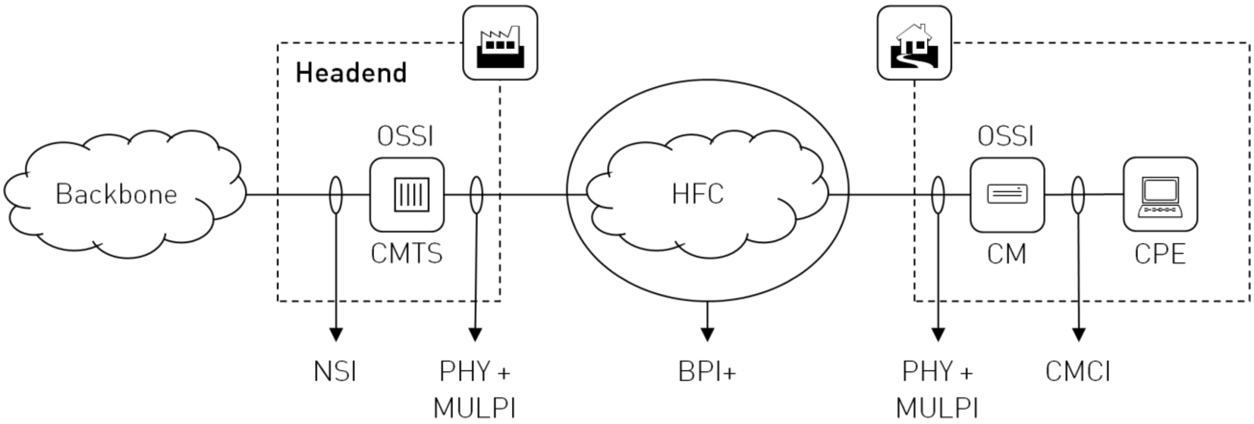

Figure 6: DOCSIS reference network

Figure 6 shows where the specifications are applicable in a graphical format.

Key Points

The EuroDOCSIS standard defines several requirements for CM and CMTS. One of them is the CMCI-interface (Cable Modem to Customer Premises Equipment Interface) specification. The CMCI is the interface between the CM and the customer equipment. It is a normative reference in an ETSI standard (European Norm (EN)).

3.1.1 The CMCI-interface

The interface between the cable modem and the end-user equipment is described in the CMCI (Cable Modem to Customer Premises Equipment Interface) specification. Historically, cable modems were operator serviceable equipment connected on the outside of the house. This is why the modem has never been considered as CPE-equipment, i.e. the equipment attached to the cable modem is the CPE-equipment. This interface corresponds to an Ethernet interface (100 MBit/s or 1 GBit/s).

The new DOCSIS 3.1 standard makes significant changes to many of the interfaces. However, it does not change the CMCI interface.

Key Point

According to the specifications of the DOCSIS standard, customer premises equipment (CPE) is the equipment attached to the cable modem over the CMCI interface.

3.2 Introduction to DOCSIS operation

3.2.1 Downstream capacity allocation in a cable network

The current technology used by cable operators is EuroDOCSIS 3.0, so this study will focus on this technology. To be able to offer the bandwidth to its customers a cable operator uses a mix of technologies and techniques.

As a first point a cable operator deploys a number of downstream channels (each 8 MHz wide) on a fiber node. Depending on the modulation each channel provides a bandwidth of 42 or 56 MBit/s. The number of provided channels defines the total shared downstream capacity for that specific node. EuroDOCSIS 3.0 defines that a cable modem must be able to use at least 4 downstream channels at the same time, but more is allowed and is currently typically used. The maximum bandwidth (irrespective of the service offering) that can be used by a single customer is defined by the type of cable modem deployed. If the cable modem is still an old 2.0 cable modem it will be only about 40 MBit/s, if the EuroDOCSIS 3.0 modem only supports 4 channels, it will be about 160 MBit/s.

3.2.2 Upstream transmission management in a cable network

In the upstream (transmission from the cable modem towards the CMTS) a very advanced mechanism is used. It is essential to understand that different (up to 100's) cable modems share the same upstream spectrum. The sharing of this upstream spectrum is both in frequency division multiplexing (the channel being used for a transmission) and time division multiplexing (at what moment and for how long a transmission is allowed). In order to prevent disturbances it has to be ensured that no single cable modem transmits anything at the wrong time, power level or frequency. Otherwise, interferences with the valid transmission of another cable modem (or even multiple modems) might occur, effectively causing disturbances to all other users on that HFC node, thereby potentially making the cable network unusable. Consequently, cable operators pay a lot of attention on testing the interoperability of cable modems with their networks to ensure that the used devices fully comply with the requirements regarding upstream transmission. In the worst error cases, cable modems have to refrain from transmitting unless they are 100% confident that the transmission is allowed.

Key Points

Cable modems connected to the same node share the used spectrum for data transmission. In order to prevent disturbances it has to be ensured that no cable modem transmits anything at the wrong time, power level or frequency. Consequently, cable operators pay a lot of attention on testing the interoperability of cable modems with their networks to ensure that the used devices fully comply with the requirements regarding transmission.

3.2.3 Capacity management in a cable network

Cable operators manage the capacity in the network by the following mechanisms:

- Limit the total number of users on a single HFC node; if this number becomes too high, a node split has to be performed
- Add downstream channels on the fiber node (for more downstream capacity)

- Add upstream channels on the fiber node (for more upstream capacity)

The maximum capacity that can be reached by a single cable modem depends on the type of cable modem (e.g. some modems that only support reception of 4 downstream channels at the same time can never reach a speed higher than about 160 MBit/s).

For capacity reasons a cable operator can e.g. have 16 downstream channels in a fiber node, but each modem supports reception of only 8 downstream channels at the same time. Advanced techniques are used between CM and CMTS to load-balance the whole group of cable modems across these 16 downstream channels. This load-balancing is done dynamically which means that the CMTS can decide at any moment in time to move a modem to a different set of downstream or upstream channels. This operation is critical for the proper operation of the cable network. Perfect interoperability between cable modem and cable modem termination system – and the exercise of control over the cable modem's operational behavior – is therefore of utmost importance.

Key Point

Cable network operators balance the capacity load dynamically via a number of down- and upload channels. This requires control over the communication between CM and CMTS und thus over the operation of the CM.

3.2.4 Security and authentication in a cable network

As explained above, a cable network is a shared medium. That means that the same electrical signal arrives at each single house in a fiber node. In order to ensure privacy it is essential that encryption is used to protect customers from eavesdropping[3] attacks. The encryption is established by the exchange of a public key from the cable modem to the CMTS. The CMTS uses this public key to send an encrypted, dynamically generated random key to the cable modem. As the cable network is a shared medium, a cable operator has no physical wire to identify the connection of a specific customer. In a cable environment customer identification is therefore done based on a unique identifier for each individual cable modem. This is the MAC-address of the cable modem.

Since it is quite easy to fake a MAC-address, the MAC-address that the cable modem uses to identify itself is protected using a digital certificate using a Public Key Infrastructure (PKI). Every single cable modem has a unique private-public key pair that needs to be installed in the cable modem at manufacturing time. To protect customers from eavesdropping or other hacking attacks this private key has to be kept private; it can therefore only be accessed by the legitimate software running on the cable modem. If a hacker has access to the private key due to insecure software on the modem, the hacker could easily deny or steal service to/from an existing customer. Furthermore, he could easily perform illegal actions (downloading/uploading illegal content, etc.), while it is very difficult (due to the cable network being a shared medium) to identify the physical location and as a consequence the individual who is doing this illegal activity. Consequently, operators have to require firm security on these cable modems and cannot allow customers to install their own software on the cable modems. New software for cable modems can

[3] Eavesdropping is secretly listening to the private conversation of others without their consent.

only be installed by cable operators over the RF network, but is also digitally signed by the manufacturer of the cable modem. A cable operator will only install the new software if he is sure the new software does not damage anything related to the proper operation of the cable modems on the network and does not create any security related risk.

Key Points

The shared medium structure in cable networks causes security and privacy issues. In order to protect the customers' privacy and the security of their communication as well as the network, strong encryption and authentication mechanisms are implemented. Furthermore, only network operator software is allowed on CMs. In order to correctly identify CMs their MAC address, secured by a PKI, is used. If the strength of the encryption is weakened, hackers could use this to perform illegal activities for which it is hard to identify the criminal.

3.2.5 Cable modem optional and additional features

Although EuroDOCSIS 3.0 defines a minimum set of requirements, an operator still has to determine which options the modems have to support taking into account current and future services and network requirements.

The most important ones are:

- Number of supported downstream channels
- Number of supported upstream channels
- Frequency range supported in the downstream
- Frequency range supported in the upstream
- Support of extended upstream transmit power
- Several other features: number of service flows, filters, classifiers, etc.

Improper or limited support for these optional features limits the flexibility that an operator has to deploy current and future services.

Beyond the minimum set of DOCSIS requirements in the above list cable operators ensure that the cable modem is fully interoperable with their network and system configuration. (See section 3.3 below on modem acceptance testing)

Apart from this general interoperability testing an operator might also specify (i.a.):

- Immunity to lightning (cable networks are regularly hit by lightning caused by thunderstorms)
- Quality of materials used (especially on the RF-part, to limit problems related to interference, noise, etc.)
- LED-requirements to assist during customer problems

Key Points

The DOCSIS standard defines a minimum set of requirements. To ensure proper operation of cable modems in a network the operator has to determine which features and which additional requirements the modems have to support.

3.3 Cable modem acceptance testing

All cable networks differ from each other. This has to do with the type and configuration of the CMTS-equipment, the different historical aspects of the rollout of the cable network and the differences of equipment used in the network itself (amplifiers, etc.).

Before deploying a new cable modem or new software on existing cable modems, a cable operator needs to ensure that the cable modems operate properly on the network and do not create a security threat. Therefore cable operators require new modems at least to be DOCSIS certified by CableLabs as this ensures the basic compliance with the specifications. Additionally, cable operators always need to execute an extensive set of additional testing to ensure the hardware/software combination meets all their requirements from a security and interoperability point of view. The interoperability testing is related to the different versions of CMTSs, different ways of provisioning, etc. that are deployed by the operator and the different service setup (number of channels, exact channel configuration, etc.). Furthermore cable operators typically roll out models that are future-proof or meet network requirements for at least some time in the future. E.g., a cable operator could but wouldn't deploy modems that only support 4 downstream channels for customers that order a 10 MBit/s service. While such modem would perfectly support 10 MBit/s from a specification point of view, the operator would have to replace that modem by a new model if the customer decides to upgrade to another service. Furthermore having modems that only support 4 downstream channels complicate the load balancing on the CMTS, so operators will not do this based on their technical roadmap.

The acceptance of new software/hardware by a cable operator typically takes several weeks (or even months) of testing.

For any change in the network (e.g. CMTS software update, configuration change, linecard change, increase in capacity, etc.) the proper operation of all modems has to be ensured again by performing an extensive set of interoperability testing. Typically this happens several times a year as operators continually invest in improving their networks.

Key Points

Cable modems go through an extensive testing process before operators deploy the modems on their networks. The interoperability testing is related to the different versions of CMTSs, different ways of provisioning, etc. that are deployed by the operator and the different service setup (number of channels, exact channel configuration, etc.). For any change in the network (e.g. CMTS software update, configuration change, linecard change, increase in capacity, etc.) the proper operation of all modems has to be ensured again by performing an extensive set of interoperability testing. Typically this happens several times a year as operators continually invest in improving their networks.

4 Analysis of the NTP

4.1 NTP for telephony services

For telephony services the NTP is the analogue twisted pair connection point, where a customer can plug in their own phone. Cable operators provide such analogue twisted pair interface for telephony services on their cable modems by typically an RJ11-connector. This interface follows the same specifications as the Deutsche Telekom telephony NTP as defined in 1TR110.

4.2 NTP for internet access

4.2.1 CMCI as NTP

For internet access the logical NTP is the Cable Modem to Customer Premises Equipment Interface as defined in the CMCI specification (Ethernet). Using this interface as the NTP has several advantages:

- It is both logically and physically at the same level as the NTP for telephony services, i.e. at the outlet of the cable modem.
- It is a well understood, well defined and equipment interoperable interface.
- Using Ethernet (1 Gigabit/s that can autonegotiate to 100 MBit/s) as the NTP provides the consumer with a well-understood connection point, where consumers also have a large choice of cables without endangering any services.
- By using the CMCI-interface the responsibility of the service as experienced by the customer fully remains with the cable operators. If a cable operator offers 200 MBit/s services, it needs to correspond to a 200 MBit/s service at the Ethernet interface of the cable modem. If the 200 MBit/s service would be defined at any other interface, customers will have no mechanisms at all to verify if a bad service is due to the provided service or to their equipment.

The CMCI-interface either requires a "naked" cable modem (cable modem with only bridging functionality) or an integrated device that has the option of setting the cable modem in bridge mode.

4.2.1.1 Bridging versus routing mode

Today, most operators deploy advanced gateways which combine the cable modem functionality with additional features like router and Wi-Fi functionality. Operators do this for the benefit of their customers as:

- It is an easy way to connect multiple devices to the Internet.
- It provides basic security.
- It eliminates the need to buy additional equipment for Wi-Fi functionality.

All cable modems can however be configured in bridging mode where additional functionalities like routing and Wi-Fi are disabled[4]. For consumers who want to deploy their own routers and Wi-Fi equipment operators can offer a bridged interface. Consumers do have to take care of their own basic internet security in those situations, since the basic level of security (NAT-functionality) is not provided by the cable operator in that case.

4.2.2 RF-interface

Besides the Ethernet interface (CMCI) the only other interface present on a cable modem is the RF-connector. This is the only other interface that can be examined.

The RF-interface should not be defined as the NTP due to the following reasons:

- If the RF-interface is used, all aspects of the complex DOCSIS protocol need to be defined explicitly. Even though the DOCSIS specifications and certifications exist today, there is no explicit definition of each and every parameter – which in the past has led to the development of differing DOCSIS implementations in the relevant network elements. Therefore even defining sufficient standards would not be enough to ensure proper operation without changing relevant hardware/software-parts of existing cable networks.
- The exact details of the requirements for this RF-interface differ between different operators (each operator currently deploying their own selected cable(s) modem taking into account their own technical requirements and interoperability with their network) due to requirements going beyond DOCSIS.
- In case of problems, it is hard to determine the root cause of the issue: is it due to the customer-owned modem or not; if it is the customer-owned modem, the operators cannot be responsible for support, since they do not own or supply the device.
- Operators regularly make changes to the network or system configuration to increase capacity, implement new features, etc. If these changes cause problems with the customer-owned modem it is unclear who is responsible for fixing the problems.
- Consumers might be stuck with old devices, whereby as a consequence if they want to sign up for new (higher-speed) services they have to replace their modem. If the operator supplies the device the operator is responsible for this aspect and will supply the new modem. The operators need to make sure the service works on the modem supplied by them.
- If the consumer has a bad device that interferes with the network (causing service degradation or even network outage) it is not clear who is responsible for this. It has to be stressed again that one bad device can interfere with the service for all users on that node.
- Connecting customer owned devices opens the door for hacking attacks on the whole network, endangering privacy and security of other consumers.

The RF-interface should therefore not be defined as the NTP.

[4] The provided software by the manufacturer must support enabling this mode.

Key Points

The NTP for Telephony over cable networks is the analogue twisted pair connection point.
For Internet access the CMCI interface is most suitable as the NTP. It puts the responsibility for service quality, interoperability and security on the network operator who provides the CM. Defining the RF-interface as NTP for Internet services over cable networks would on the other hand cause risks to the integrity of the network and the privacy and security of the customers. The subsequent liability and responsibility issues are unsolved.

4.3 Situation in the US market

In the US, cable network operators, e.g. Comcast, allow customers to purchase their modem in the retail shop. The following restrictions apply:

- The device must have passed CableLabs certification, UL (Underwriters Laboratories) certification, FCC (Federal Communications Commission) certification, and Comcast DOCSIS certification
- Comcast has different tiers of devices, one star, two stars and three stars. The testing fee for one star testing by ComCast is 25000 US$, for other levels, additional costs will apply. Payment gives no guarantee that the device is approved.
- Comcast is entitled to make any changes to the device (software).
- Comcast does not take any liability with respect to damage to the device during any work (including firmware upgrades).

Details on the Comcast policy can be found at:

- http://networkmanagement.comcast.net/images/pdf/docsis-testing.pdf
- http://networkmanagement.comcast.net/index.php/8-network-management-news/4-rules-regarding-the-attachment-of-devices-to-the-network
- http://www.comcast.com/Corporate/Customers/Policies/SubscriberAgreement.html

This situation is not applied in any European country.

4.4 Conclusion

Based on the analysis it is concluded that the CMCI-interface (Ethernet) is by far the most suitable interface to use for the NTP. It defines a well known and customer-understood interface that allows customers to use any device behind the cable modem. It keeps the cable operator responsible for the provided service over the HFC network. This also means that customers are protected from investing in devices that cannot deliver the offered services. It also ensures that a bad (in the meaning of harmful to the network) customer owned cable modem disturbs the services provided by the cable operator.