STADIA
HELSINGIN AMMATTIKORKEAKOULU

FACULTY OF TECHNOLOGY

Information Technology

Telecommunications

GRADUATE STUDY

TRANSFER OF MPEG-2 TRANSPORT STREAM OVER MPLS

Author: Mikko Kiuru
Supervisor: Jouko Kurki
Instructors: Jukka Rakkola,
Henri Viljasjärvi

Approved: __. __. 2006

Jouko Kurki
Principal Lecturer

ABSTRACT

Name: Mikko Kiuru

Title: Transfer of MPEG-2 Transport Stream Over MPLS

Date: 14th November 2006 Number of pages: 52

Department: Information Technology

Study Programme: Telecommunications

Instructors: Jukka Rakkola, M.Sc., System Specialist, Digita Oy
Henri Viljasjärvi, Head of System Management, Digita Oy

Supervisor: Jouko Kurki, Dr. Tech., Principal Lecturer, Helsinki Polytechnic

This study examines how MPEG-2 Transport Stream, used in DVB-T video transmission, can be reliably and efficiently transferred to remote locations over an MPLS network. All the relevant technologies used in this scenario are also discussed in the study. This study was done for Digita Oy, which is a major radio and television content distributor in Finland.

The theoretical part of the study begins with the introduction to MPLS technology and continues with explanation of IP Multicast and its components. The fourth section discusses MPEG-2 and the formation and content of MPEG-2 Transport Stream. These technologies were studied in relevant literature and RFC documentation. After the theoretical part of the study, the test setup and the test cases are presented.

The results of the test cases, and the conclusions that can be drawn based on them, are discussed in the last section of the study. The tests showed that it is possible to transfer digital video quite reliably over an MPLS network using IP Multicast. By configuring the equipment correctly, the recovery time of the network in case of a failure can be shortened remarkably. Also, the unwanted effect of other traffic on the critical video traffic can be eliminated by defining the Quality of Service parameters correctly. There are, however, some issues that need to be tested further before this setup can be used in broadcast networks. Reliable operation of IP Multicast and proper error correction are the main subjects for future testing.

Keywords: MPLS, IP, Multicast, MPEG-2, Transport Stream

STADIA
HELSINGIN AMMATTIKORKEAKOULU

INSINÖÖRITYÖN TIIVISTELMÄ

Tekijä: Mikko Kiuru

Työn nimi: MPEG-2 Transport Streamin siirto MPLS-verkon yli

Päivämäärä: 14.11.2006 Sivumäärä: 52

Koulutusohjelma: Tietotekniikka Suuntautumisvaihtoehto: Tietoliikennetekniikka

Työn valvoja: tekn.toht. Jouko Kurki, yliopettaja, Helsingin ammattikorkeakoulu

Työn ohjaajat: dipl.ins. Jukka Rakkola, järjestelmäasiantuntija, Digita Oy
Henri Viljasjärvi, järjestelmänhallinnan ryhmäpäällikkö, Digita Oy

Tässä insinöörityössä on tutkittu, miten MPEG-2 Transport Stream, jota käytetään digitaalisen televisiosignaalin siirtoon, voidaan tehokkaasti ja luotettavasti välittää lähetysasemille MPLS-verkon yli. Kaikki oleelliset teknologiat, joita tällaisen järjestelmän toteuttamiseen tarvitaan, on myös käsitelty tässä työssä. Insinöörityö on tehty Digita Oy:lle, joka on Suomen huomattavin radio- ja televisiopalvelujen jakelija maanpäällisissä verkoissa.

Insinöörityön teoreettisessa osuudessa on aluksi esitelty MPLS-teknologiaa. Seuraavaksi on selvitetty IP Multicastin ja siinä käytettävien komponenttien toimintaa. Työssä on myös tutustuttu MPEG-2-standardiin ja MPEG-2 Transport Streamin sisältöön ja muodostumiseen. Työn teoreettiset osiot perustuvat aiheisiin liittyvän kirjallisuuden ja RFC-dokumenttien tutkimiseen. Teoriaosuuden jälkeen on kerrottu testiverkon rakenteesta ja suoritetuista testeistä.

Testit osoittivat että digitaalista televisiosignaalia pystyy siirtämään melko luotettavasti MPLS-verkon yli käyttäen IP Multicastia. Konfiguroimalla verkon laitteet oikein, voitiin verkon toipumisaikaa vikatilanteen sattuessa lyhentää huomattavasti. Muun verkkoliikenteen haittavaikutukset kriittiseen videoliikenteeseen voitiin myös eliminoida määrittelemällä verkon palvelunlaatuparametrit oikealla tavalla. Tässä ratkaisussa todettiin kuitenkin olevan vielä asioita, jotka tarvitsevat lisää testausta ennen järjestelmän käyttämistä valtakunnallisessa televisioverkossa. IP Multicastin luotettava toiminta ja järjestelmän virheenkorjaus olivat aiheita, joiden todettiin tarvitsevan myöhempää testausta.

Avainsanat: MPLS, IP, Multicast, MPEG-2, Transport Stream

TABLE OF CONTENTS

ABSTRACT

TIIVISTELMÄ

ACRONYMS

1 INTRODUCTION 1

2 INTRODUCTION TO MPLS 4

2.1 Operation of MPLS 4

2.2 MPLS Traffic Engineering and Fast ReRoute 9

3 DATA TRANSFER USING IP MULTICAST 15

3.1 Multicast Distribution Trees 15

3.2 Internet Group Management Protocol 17

3.3 Reverse Path Forwarding 18

3.4 Protocol Independent Multicast 19

3.5 Pragmatic General Multicast 20

4 TRANSMISSION OF DIGITAL VIDEO SIGNAL 22

4.1 MPEG-2 Standard 22

4.2 MPEG-2 Compression 23

4.3 MPEG-2 Transport Stream 24

4.4 MPEG TS to IP Encapsulation and Pro-MPEG FEC 27

5 TESTING DIGITAL VIDEO TRANSFER OVER MPLS NETWORK 32

5.1 Equipment 34

5.2 Setting up the MPLS and Multicast Network 36

5.3 Initial Testing of the Network 38

5.4 Testing Quality of Service for the Video Stream 40

5.5 Optimizing Network Recovery 44

5.6 Monitoring of MPEG-2 Transport Stream Components 45

6 CONCLUSIONS 48

REFERENCES 51

ACRONYMS

Acronym	Description
BGP	*Border Gateway Protocol.* An exterior gateway routing protocol
CB-LSP	*Constraint-based Label Switched Path.*
CBR	*Constraint Based Routing.*
DVB-T	*Digital Video Broadcasting – Terrestrial.*
ES	*Elementary Stream.*
FEC	*Forwarding Equivalence Class.* Packet flow in MPLS network
FEC	*Forward Error Correction.*
IETF	*Internet Engineering Task Force.*
IGMP	*Internet Group Management Protocol.*
IGP	*Interior Gateway Protocol.*
IOS	*Internetwork Operating System.* Cisco proprietary operating system
IP	*Internet Protocol.*
LDP	*Label Distribution Protocol.* Protocol to establish label switched paths
LFIB	*Label Forwarding Information Base.*
LSR	*Label Switched Router.* A network node capable of MPLS
LSP	*Label Switched Path.* A route through the MPLS domain
MDT	*Multicast Distribution Tree.*
MPEG	*Moving Pictures Experts Group.*
MPLS	*Multiprotocol Label Switching.*
MTU	*Maximum Transmission Unit.*
OSPF	*Open Shortest Path. First* Link-state routing protocol in IP networks
PAT	*Program Association Table.*
PCR	*Program Clock Reference.*
PES	*Packetised Elementary Stream.*
PGM	*Pragmatic General Multicast.* Reliable multicast transport protocol
PID	*Packet ID.*
PIM	*Protocol Independent Multicast.*
PIM-DM	*Protocol Independent Multicast – Dense Mode.*
PIM-SM	*Protocol Independent Multicast – Sparse Mode.*
PMT	*Program Map Table.*
QoS	*Quality of Service.* Guaranteed throughput level of data
RP	*Rendezvous Point.*
RPF	*Reverse Path Forwarding.*
RR	*Route Reflector.* Used for reflect BGP routes inside autonomous system
RSVP	*Resource Reservation Protocol.* Protocol for reserving network resources
RTP	*Real-time Transfer Protocol.*
SDH	*Synchronous Digital Hierarchy.* European (ITU) version of SONET
SPT	*Shortest Path Tree.*
TCP	*Transport Control Protocol.*
TDP	*Tag Distribution Protocol.*
TE	*Traffic Engineering.*
TS	*Transport Stream.*
UDP	*User Datagram Protocol.*
VPN	*Virtual Private Network.* Private network over public wires
WAN	*Wide Area Network.* Network connecting remote sites

1 INTRODUCTION

The current trend in telecommunications networks is that almost all the traffic is moving from circuit switched or cell-based networks to packet switched, IP-based networks. This sets new demands for packet switched networks. IP-based networks were not originally created for real-time applications such as voice or video. If you want to transfer real-time voice or video through a TCP/IP-network with good quality, with no missing video frames or syllables, special adjustments to the network are needed. There always has to be guaranteed bandwidth, low latency and no jitter for these kinds of applications. Today, most of these needs can be fulfilled.

The purpose of this project is to examine whether or not it is currently possible to transfer digital video signal, such as DVB-T's MPEG-2 Transport Stream, through an MPLS network efficiently and reliably. This kind of vision would allow distributors to provide different services over one and same network infrastructure. This would also simplify operation and maintenance and allow easier launching of new services. At the moment, at least in Finland, the digital video signal is transferred to the transmitters around the country over an SDH (Synchronous Digital Hierarchy) network. SDH is a fairly reliable, low latency and jitter free transfer technology but at the same time it is not very flexible or efficient. Every service has a dedicated bandwidth whether it is entirely used or not. In packet switched networks, such as MPLS, all the services share the same media and bandwidth and therefore the usage is more efficient. Reliability and robustness of an IP network can also be increased with different software features. For example Quality of Service for varying types of services is something that is properly supported only in IP based MPLS networks. However, MPLS is not yet widely employed as the transfer technology for broadcasting networks. This means that there are still unresolved issues that could compromise the quality of, for example, digital video signal.

The scope of the tests that were performed in this study was to create some possible conditions that could have an effect on the video quality that is transferred over an MPLS network. These conditions were for example network congestion and physical network failures. If a packet switched network is used and several services are transported over the same media, there is a chance that some service could eat the bandwidth from the video and therefore cause degradation in the video quality. To avoid this kind of situation, Quality of Service was taken in use and tested. When a physical link on the transport path breaks, the network needs to converge and forward the traffic to an alternate path. This was tested through building a redundant network and breaking an active link. The result was immediately seen as a pause in the video that was monitored. The goal was to make the pause in the video as short as possible by optimizing the MPLS network.

The main technologies used in this graduate study are explained and studied in their own sections. Section 2 examines the operation of Multiprotocol Label Switching (MPLS), which is the most crucial part of the study. Also, ways to improve the robustness and reliability of an MPLS network are covered in the second section. Section 3 explains the behavior of IP Multicast, which is the only reasonable technique to be used for transferring high bandwidth data streams to several locations at the same time. The fourth and the last theoretical section takes a look at the MPEG-2 Transport Stream which is the form in which the DVB-T video signal is transferred. The last section also describes how the Transport Stream is encapsulated into IP packets and what kind of error correcting scheme can be used to ensure reliable transfer.

After all the used technologies are studied in their own sections, Section 5 presents information about the tests that were performed. The used equipment is described in the first subsection and the network setup in the following. After the components and the topology of the network are clear, different test cases are covered in their own subsections.

Section 6 gathers the information from the theoretical chapters and the results of the testing. In this section it is decided what conclusions are drawn based on the available information.

2 INTRODUCTION TO MPLS

Multiprotocol label switching (MPLS) was designed to solve several well-known limitations of traditional IP routing, ranging from scalability issues to poor support of Quality of Service (QoS) and complex integration with Layer 2 backbones. An American company called Ipsilon, later purchased by Nokia, first came up with the idea of combining fast ATM switching with IP routing in 1996. At the time the technique was called IP Switching. Cisco introduced their MPLS technique called tag-switching in 1998. Internet Engineering Task Force (IETF) published first official MPLS standard in 2001 after four years of development. MPLS has rapidly become popular in multivendor and -protocol core networks in service provider environment as well as in large-scale corporate networks.

MPLS was created to combine the benefits of connectionless Layer 3 (IP) routing and forwarding with connection-oriented Layer 2 (e.g. ATM) forwarding. MPLS was developed to be compatible with multiple existing protocols. It can support pure IP-based network, pure ATM network, pure Frame Relay network or a combination of all of these. The universal nature of MPLS is appealing to operators who currently have mixed network technologies and seek ways to optimize resources and expand QoS support.

2.1 Operation of MPLS

MPLS network consists of a set of nodes, Label Switched Routers (LSR), that are capable of switching and routing packets on the basis of a label which has been appended to each packet. Labels define a flow of packets between two endpoints or, in the case of multicast, between a source endpoint and a multicast group of destination endpoints. Labels specify the path through the network of LSRs for each distinct packet flow. Each packet flow is called Forwarding Equivalence Class (FEC). Quality of Service parameters can be defined for each packet flow individually. Much greater performance is achieved because packets are switched based on simple tag information without the need for IP header look-up. There is no need to check packet headers in each LSR inside the domain of MPLS-enabled routers. [1, p.4.]

Per-Hop Behaviour (PHB) can be defined in each LSR. Because of this, each Forwarding Equivalence Class can be treated as needed. Packets can be queued or dropped based on the PHB information. Packets between same endpoints can belong to different FECs. As a result of this, packets are labelled differently and switched along a different path within MPLS domain. FEC can be configured based on the following information:

- Source or destination IP addresses or network addresses
- Source or destination ports
- IP protocol ID
- Differential services codepoint
- Ipv6 flow label

The basic operation of MPLS is illustrated in Figure 1.

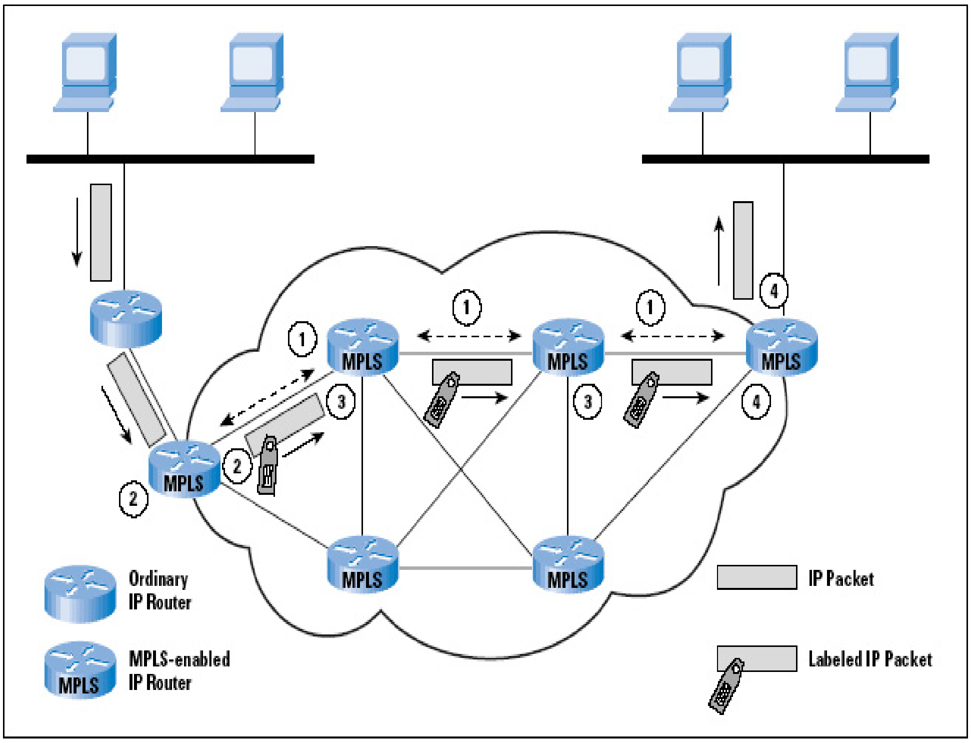


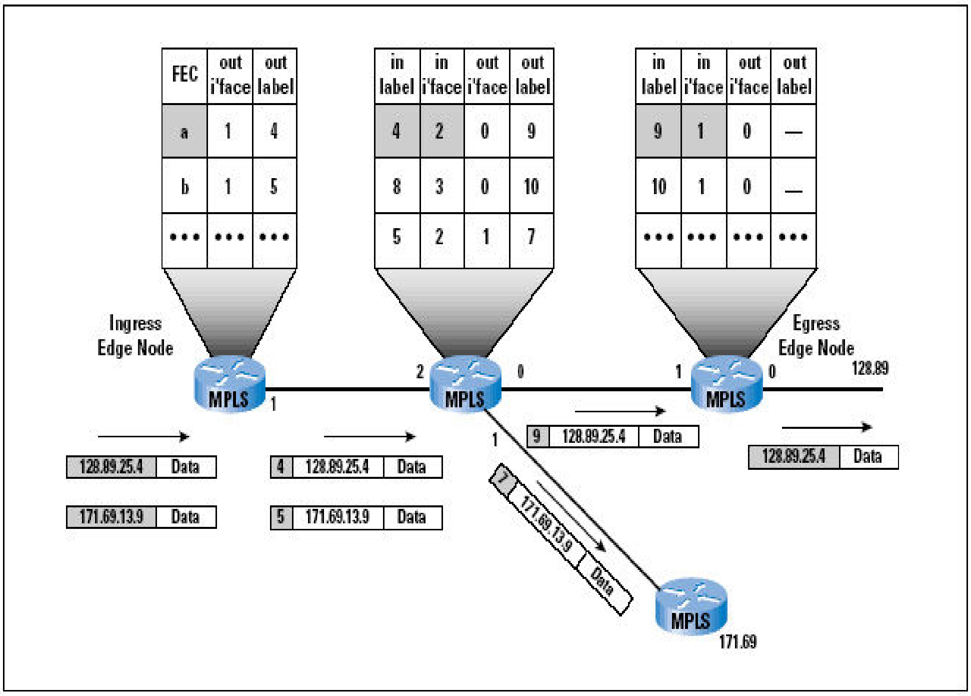
Figure 1. *MPLS operation [1]*

The following are the key points of the MPLS operation [1, p. 5-6]:

1. Before any packets can be transported through the network, the route, known as Label Switched Path (LSP), has to be discovered. QoS parameters also have to be defined along the LSP. Connections between LSRs can be established by using a dynamic routing protocol such as IS-IS or OSPF. Two protocols can be used to build an LSP through the network: Label Distribution Protocol (LDP) or Resource Reservation Protocol (RSVP). LSPs have only local significance within each MPLS domain. Static routes can be manually assigned by the network administrator if needed.
2. When the packet arrives from ordinary IP router to border of the MPLS domain, the ingress router checks the QoS parameters for the packet. Label Switched Router assigns packet to particular FEC, appends the label for the packet and forwards the packet to Label Switched Path. If no LSP exists for this FEC, the edge LSR must cooperate with the other LSRs in defining a new LSP.

3. Next LSR checks the incoming packet's label, removes it and appends a new one based on the router's forwarding table. After that, the packet is forwarded to next LSR in the path.
4. Egress router strips the label, examines the IP header information and routes packet to destination.

Switching within an MPLS domain is done based on a predefined table called Label Forwarding Information Base (LFIB) that maps the label values to next hop addresses. There is no need to examine the IP packet's header information for the routing decisions. Figure 2 shows the label handling and label forwarding operations in more detail.



FEC	out i'face	out label
a	1	4
b	1	5
•••	•••	•••

in label	in i'face	out i'face	out label
4	2	0	9
8	3	0	10
5	2	1	7

in label	in i'face	out i'face	out label
9	1	0	—
10	1	0	—
•••	•••	•••	•••

Figure 2. *MPLS Labelling and switching [1]*

Each Label Switched Router maintains a forwarding table for each passing LSP. When the packet arrives, the LSR checks the incoming label value, examines the table for outgoing interface and then appends the new label for the next LSR. This is much like the mechanism in an ATM switch where a

Virtual Path Identifier (VPI) – Virtual Circuit Identifier (VCI) pair is swapped to another when exiting an ATM switch. Before any label switching can occur, the connections between LSRs must be established using dynamic routing protocols such as OSPF or static routes. Ingress router must be aware of the neighbouring routers. For scalability reasons labels have local significance only. In Figure 2 there is a good example of a switching decision: packets with label 4 arriving to interface 2 of the LSR in the middle are being forwarded from interface 0 with label 9. Packets arriving to the same interface with label 5 are forwarded from interface 1 with label 7.

The label itself is 32-bit field tag (Figure 3) attached to normal header information of the used protocol.

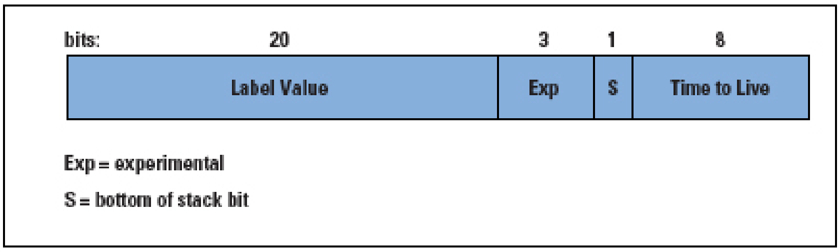


Figure 3. *MPLS label format [1]*

The label consists of the following fields:

- 20-bit Label Value is used to carry information about source and the destination as well as label ID.
- 3-bit Exp field is currently being used for delivering QoS parameters in the label.
- 1-bit Stack field is used to point the oldest entry on stack.
- 8-bit TTL is used to measure the hop count or time to live before the packet is discarded inside MPLS domain.

Label stacking is one of the most important features of MPLS. Simple unicast routing does not use the label stack, but other MPLS applications such as MPLS Virtual Private Networks (MPLS VPNs) or MPLS Traffic Engineering (MPLS TE) rely heavily on it. A labelled packet can carry many labels organized in last-in-first-out stack. Packet processing is always done for the label on top of the stack. Stack field indicates the last label in stack with value one. All other stack bit values are turned to zero. Label stacking allows multiple Label Switched Paths to be aggregated into one LSP. For example a service provider can group multiple LSPs together in the border of their own MPLS domain when accessing some other MPLS domain. Grouped LSPs mean smaller state tables and faster switching. [1, p. 9.]

2.2 MPLS Traffic Engineering and Fast ReRoute

Transmission capacity is usually expensive which means that service providers and network operators want high use of it. MPLS Traffic Engineering (MPLS TE) makes traditional Layer 2 traffic engineering features available for Layer 3. With MPLS TE there is no need for multi-tier networks any longer. MPLS TE provides the solution for efficient use of backbone resources as well as for fast recovery from link or node failures. IP routing is also optimized according to constraints imposed by backbone capacity and topology. Also more variables can be given for normal shortest path first (SPF) calculations. [2, p. 3.]

When MPLS TE is enabled in a network, administrators can set different requirements for different Label Switched Paths. Examples of these requirements could be for example needed bandwidth or preferred media type. LSP is then established according to the network resources. This is called constraint-based routing (CBR). The path for the traffic flow is the shortest path that meets the requirements. Traditional Interior Gateway Protocols (IGPs) without the enhancements of MPLS TE only find the shortest path to the destination. [2, p. 15.]

Figure 4 illustrates an example of a possible network topology.

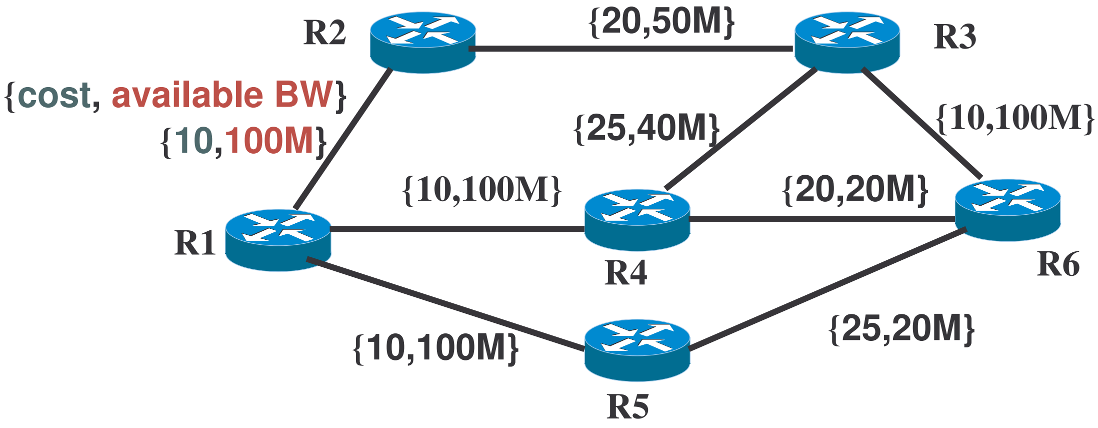


Figure 4. *Network topology example*

There are six LSRs which are partially meshed. Cost and bandwidth have been marked on each link. In this case, which is the best path from R1 to R6 with bandwidth of 30Mbps? If traditional IGP routing was used, such as IS-IS or OSPF, the path would go through R4 because of the lowest cost. But in the case of MPLS TE the best path is in fact through R2 and R3 because that path meets the bandwidth requirement and is of lower cost than path via R4 and R3.

When the best path has been found, an MPLS Traffic Engineering Tunnel is created over the Label Switched Path between the endpoints, the ingress and the egress Label Switched Router. These tunnels can also be referred to as Traffic Trunks (TTs). MPLS TE Tunnels and attributes need to be manually configured on the LSRs. Paths for the tunnels can be configured to be established dynamically according to the requirements or statically through defining each hop on the path. The Label Switched Path MPLS TE Tunnels use is called Constraint-based LSP (CB-LSP). CB-LSP differs from a normal LSP because it needs to meet the defined requirements. A signalling protocol called Resource Reservation Protocol (RSVP) establishes and maintains the LSPs for MPLS TE Tunnels along explicit paths and reserves resources across a network. Link-state Interior Gateway Protocol with MPLS TE enhancements then floods the available resources across the network. [3.]

Label assignment and switching in the case of an MPLS TE Tunnel is shown in Figure 5.

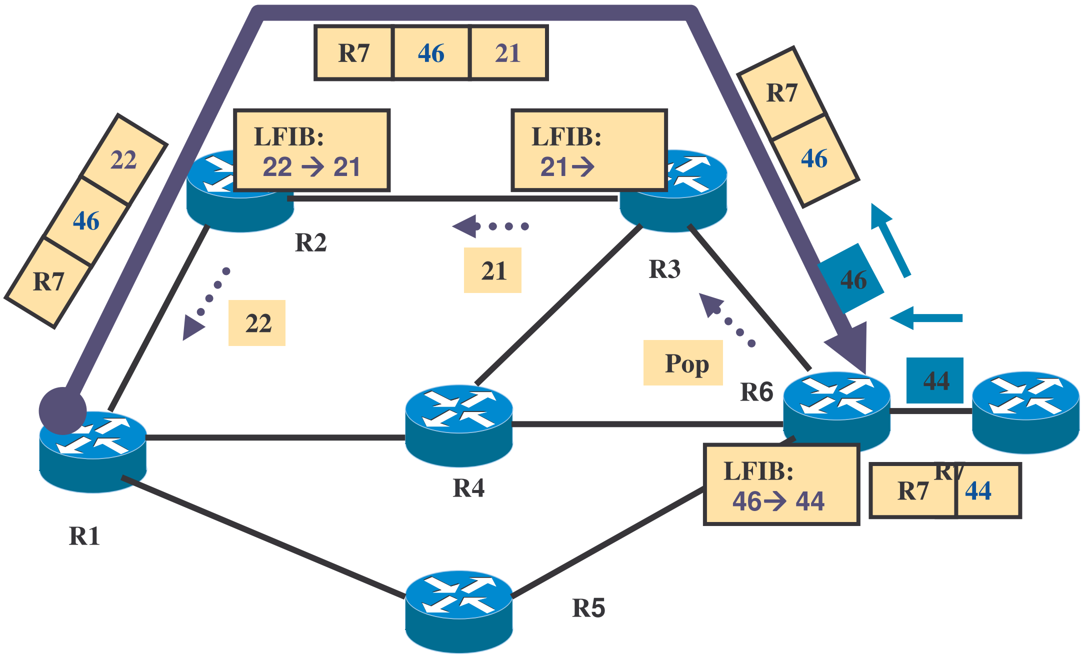


Figure 5. *Label Switching in the case of an MPLS TE Tunnel*

Resource Reservation Protocol first allocates labels for the precompiled tunnel path, labels 21 and 22. Label Switched Routers R6 and R7 use normal LDP/TDP messaging to assign labels 44 and 46. MPLS packet at R1 destined to R7 carries a stack of labels. R1 knows that R6, label 46, is the next hop behind the tunnel. There has to be labels also for the tunnel path so labels are stacked. The first label is for the tunnel endpoint and second for the tunnel route. When arriving at R6, the last route label is popped and normal label switching, 46 to 44, is done to reach the destination LSR R7.

If there is a failure on the path of the tunnel, for example between R2 and R3, the headend LSR, in this case R1, is able to quickly calculate a new path for the tunnel with the help of the underlying protocols. This way the service is not interrupted at the IP level since the tunnel interface stays up. Traffic just flows via different LSP. There are a lot of different attributes that can be defined for an MPLS TE Tunnel to control its operation: bandwidth-related, priority-related and behaviour under fault conditions just to name a few. These attributes will not be discussed here any further.

Sometimes with critical traffic flows even a small delay, caused by messaging in the case of a link failure along a MPLS TE tunnel, is not acceptable. For that purpose MPLS Fast ReRoute (MPLS FRR) was introduced. FRR enables very fast switching to a preconfigured backup path in case of a link or node failure. Traffic is redirected into backup tunnel within 50 milliseconds. When using Fast ReRoute, the reroute decision is completely controlled by the local LSR interfacing the failed link. Local router that has the backup tunnel configured prevents any further packet loss caused by the failed link. Local router starts forwarding the traffic via the backup path immediately when a fault occurs. This gives the headend Label Switched Router time to establish the tunnel along another optimal path. If the headend router does not find a new path, the backup tunnel continues to be used. [4.]

Figure 6 shows the operation of MPLS Fast ReRoute.

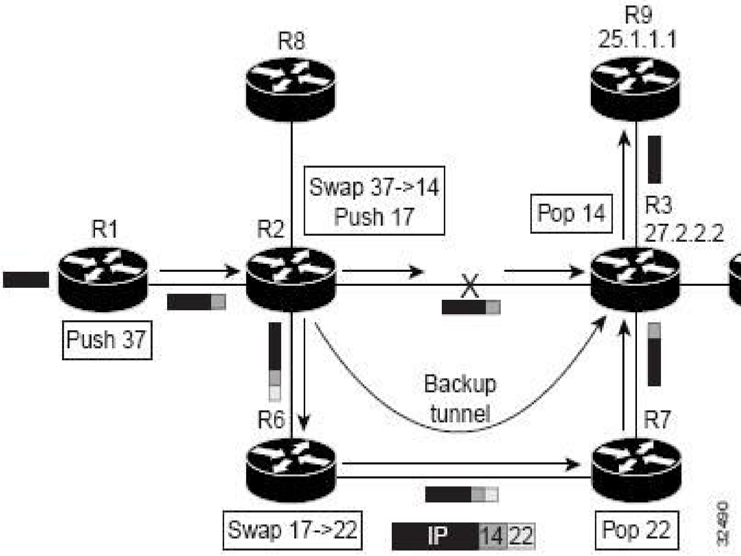


Figure 6. *Operation of MPLS Fast ReRoute. [5]*

There is an MPLS Traffic Engineering tunnel between R1 and R9 via R2 and R3. Link between R2 and R3 fails but there is a backup tunnel configured on R2 via R6 and R7. After the normal label swap, R2 pushes the label for R6 on the label stack. Label 14 for R3 remains in the label stack and is used when the traffic returns to the original path. [5.]

MPLS Traffic Engineering and Fast ReRoute are very recommendable features for networks that are used to transfer critical and sensitive data and therefore require high reliability. For example transferring real-time video is very demanding when it comes to network resources and fault recovery. Packet drops are all seen or heard in the end system since there is no retransmission in these kinds of applications. Real-time video also requires reasonably high bandwidth which needs to be guaranteed.

MPLS as a technique makes data transfer faster compared to traditional IP routing. MPLS Traffic Engineering and Fast ReRoute on the other hand enhance the Quality of Service and shorten the recovery time in case of a fault in a network. This is a very good starting point when designing a network that will be used for transfer of high bandwidth digital video. However, this setup allows only unicast point to multipoint connections, meaning that the same stream has to be sent separately to every destination device. This is not very efficient. For these kinds of situations, a technique called IP Multicast was developed. It allows multiple receivers to receive one single stream instead of individual streams per receiver. IP Multicast and its components are studied in the next chapter in more detail.

3 DATA TRANSFER USING IP MULTICAST

When multiple users across a network want to use the same high bandwidth application such as live video, it would conventionally cause a high load on the network. Each user would require a separate unicast traffic flow even if more than one user was viewing the same video. For this problem there is a solution called IP multicast. When using multicast, only a single video stream is sent from the server to the recipients. This way there is no extra burden on the source or on the network.

Multicast is based on the concept of a group. Multicast group is defined by a class D IP address which falls in the range of 224.0.0.0 to 239.255.255.255. Some of these addresses are reserved for special purposes, for example 224.0.0.5 and 6 for the OSPF routing protocol. Addresses from 239.0.0.0 to 239.255.255.255 are to be used inside an organization or domain and those are not routed over the internet or between different organizations. [6, p.1, 3.]

The following subsections describe how multicast traffic finds its way from the source to the receivers. There is some signalling needed by the routers and receiving hosts in order for the traffic to be forwarded to the correct parts of the network and eventually to the hosts that subscribe the stream.

3.1 Multicast Distribution Trees

Routers that are multicast enabled create Multicast Distribution Trees (MDT) to control the path that multicast traffic takes through a network from source to receivers. The simplest form of an MDT is a source tree, also referred to as a shortest path tree (SPT) because it takes the shortest path through the network. An SPT is marked with notation (S, G) where S is source unicast IP address and G is multicast group IP address where traffic is destined to. If there is another source sending traffic to the same multicast group, a separate shortest path tree is created. A simple MDT with one source, 192.1.1.1, and two group members is illustrated in Figure 7.

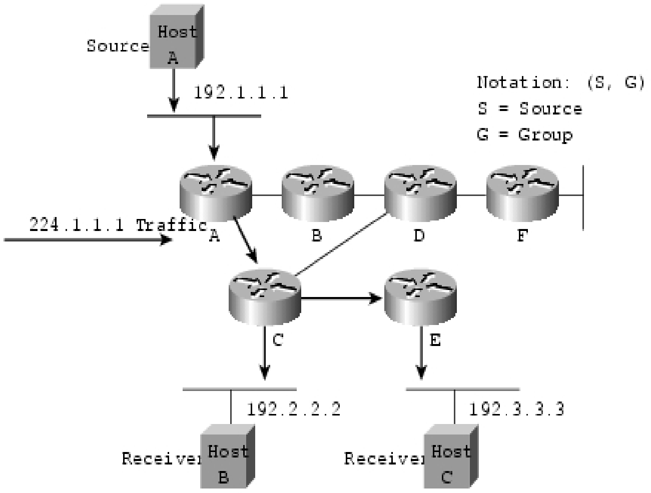


Figure 7. *Source tree MDT with one source and two receivers. [7]*

When there is more than one source sending multicast traffic, the MDT is called a shared tree (Figure 8).

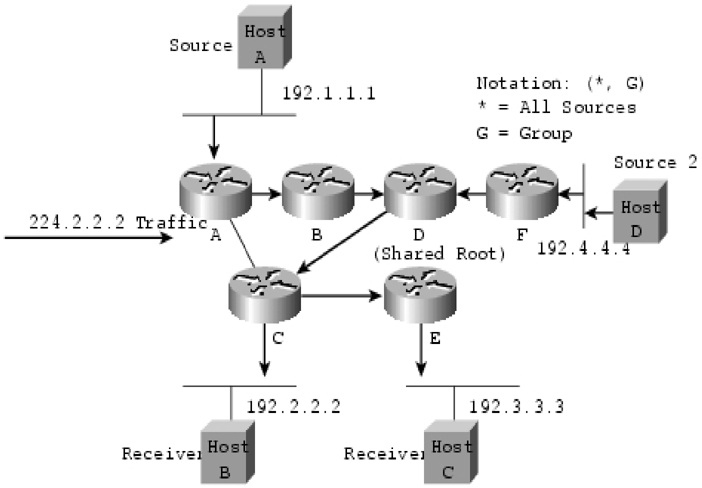


Figure 8. *Shared tree MDT with two sources and two receivers. [7]*

Unlike SPTs that have their root at the source, shared trees have a common root at some chosen router in the network. This router is called the rendezvous point (RP). In the case of a shared tree an MDT is marked (*, G) where * represents all the sources and G represents the multicast group IP address. All sources send their traffic to the RP before it is actually forwarded down the tree to the recipients. Shared tree topology consumes less router memory than source tree topology because the routers do not have to maintain the path information for each source individually. The downside of shared tree topology compared to source tree topology is that the route from source to destination might not be always optimal and may result in increased latency. [7.]

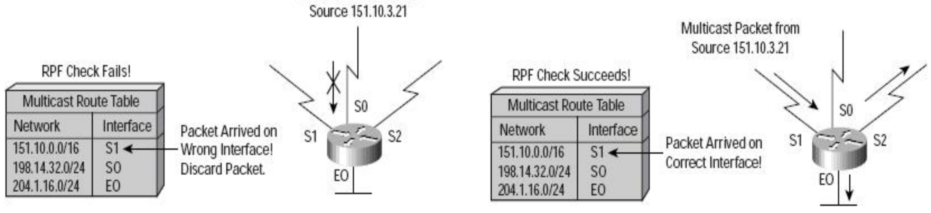
3.2 Internet Group Management Protocol

If a host wants to join a certain multicast group, it sends out an Internet Group Management Protocol (IGMP) message to the local multicast router. On the other hand, the router periodically sends out queries to local network to check that there is at least one host in the subnet that is interested in receiving the multicast traffic. When using IGMP Version 1 the router stops forwarding multicast traffic to a subnet after three unanswered queries. In

IGMP Version 2 there is a leave group message which a host sends to the router when it wants to leave the group. This allows unwanted traffic to be stopped sooner. [7.]

3.3 Reverse Path Forwarding

In traditional unicast routing a router forwards the traffic from the source to the destination based on its routing table. Unicast router does not really care about the source address, its only goal is to forward the traffic to the destination. Multicast router, on the other hand, has to make a decision which direction is upstream and which is downstream. If there are multiple downstream paths, it needs to replicate the packet and forward it down the appropriate paths. This method of forwarding traffic away from the source, rather than to the destination, is called reverse path forwarding (RPF). RPF is a very fundamental part of multicast routing process. It takes the information from the unicast routing table to determine the upstream and downstream neighbours and enables multicast router to only forward multicast traffic if it is received on an upstream interface. The operation of RPF check can be seen in Figure 9. [7.]


RPF Check Fails!
Packet Arrived on Wrong Interface! Discard Packet.
Multicast Packet from Source 151.10.3.21
S0
S1
S2
EO
RPF Check Succeeds!
Packet Arrived on Correct Interface!
Multicast Packet from Source 151.10.3.21
S0
S1
S2
EO

Multicast Route Table

Network	Interface
151.10.0.0/16	S1
198.14.32.0/24	SO
204.1.16.0/24	EO

Multicast Route Table

Network	Interface
151.10.0.0/16	S1
198.14.32.0/24	SO
204.1.16.0/24	EO

Figure 9. *Operation of RPF check. [7]*

The multicast router in Figure 9 uses its unicast routing table to determine if the multicast traffic, with source address of 151.10.3.21, arrives on the interface that is on the reverse path back to the source. On the left in Figure 9, the RPF check fails and the packet is dropped because the traffic is received on the wrong interface. On the right, packet arrives on the interface leading back to the source and RFP check succeeds.

3.4 Protocol Independent Multicast

Protocol Independent Multicast (PIM) is a multicast protocol that runs on any unicast IP routing protocol, for example OSPF, IS-IS or BGP. PIM uses the unicast routing table to perform Reverse Path Forwarding checks which will be discussed in the next chapter. Some other multicast routing protocols build their own independent tables instead, and therefore require more CPU resources on the routers or add overhead to the multicast operation.

There are two types of Protocol Independent Multicast: Dense-mode (PIM-DM) and Sparse-mode (PIM-SM). Both types of PIM form adjacencies with neighbouring PIM enabled routers through Hello-messages that are sent every 30 seconds. When PIM-DM is configured on the network and PIM router receives a multicast packet, an RPF check is first performed. If RPF check succeeds, the packet is copied and forwarded to all downstream PIM neighbours. This process is repeated in every PIM router until the multicast group traffic reaches the last hop routers. The MDT type for PIM-DM networks is always the shortest path tree, which was described earlier. Not all the links in a PIM-DM network are necessarily filled with multicast group traffic; PIM-DM routers can send *Prune*-messages to neighbouring routers to remove the link on which the message was received from the SPT. This happens when PIM router receives multicast traffic on more than one interface, meaning that the RPF check fails. PIM router can have multiple forwarding interfaces but it can only have one receiving interface. [8, p. 5.]

PIM Sparse-mode has completely different approach than PIM-DM for delivering multicast traffic to receivers. When PIM-SM is configured on the network, no multicast group traffic is forwarded until some host specifically asks for it. Downstream routers need to send *Join*-messages continually upstream in order to receive multicast traffic. If upstream router does not receive *Join*-message in time, it marks the link pruned and no longer forwards traffic on the link. PIM-SM operation requires a shared-tree MDT, which means that there needs to be a rendezvous point (RP) in the network. There are two steps when it comes to forwarding traffic towards hosts; first the traffic is sent from the source to the RP and after that the RP sends the traffic to routers that have joined the group. All routers that want to forward multicast traffic to a group need to be registered with the RP. Although shared-tree topology is required in PIM-SM when setting up the multicast traffic path from source to receiver, PIM-SM also supports the shortest path trees. When the steps that are needed to start the multicast traffic to flow are performed, the last hop router can switch to a shortest path tree. This operation can be controlled with a bandwidth threshold, which is configurable in the last hop router. [9, p. 2.]

3.5 Pragmatic General Multicast

Normal multicast traffic does not have any features that would increase its reliability. Multicast uses UDP protocol and because of that, the source does not have any knowledge of whether the traffic was received or not. “Pragmatic General Multicast (PGM) is a reliable multicast transport protocol for applications that require ordered, duplicate-free, multicast data delivery from multiple sources to multiple receivers. PGM guarantees that a receiver in a multicast group either receives all data packets from transmissions and retransmissions or can detect unrecoverable data packet loss.” [10, p. 1.]

PGM is network-layer independent protocol but it is mostly used over IP. PGM needs to be enabled in sources, receivers and network elements (routers) for it to work. Operation of PGM is basically based on negative acknowledgements (NAKs) and NAK confirmations (NCFs). If the receiver notices that a data packet is missing from the expected sequence in the multicast stream which the source is transmitting, the receiver sends out a unicast NAK message to the nearest upstream PGM router. All PGM routers along the distribution tree perform the same operation, they forward the unicast NAK message upstream towards the source and multicast an NFC on the interface the NAK was received. The path that the NAK message takes from the receiver to the source is reverse to the original distribution tree. Finally the source receives the NAK message, sends out an NCF to the group and re-sends the missing or erroneous packet to the subnet from where the original request came from. [10, p. 4.]

Unfortunately there are not many applications available that support Pragmatic General Multicast. Reliability remains as the major challenge of IP Multicast, retransmission and error correction of an UDP stream based on receiver's request naturally sets higher demands on the network and devices participating in the system. That is why the behaviour of IP Multicast in case of network faults is worth testing and studying. However, error correction schemes for multicast have been developed. One of them, Pro-MPEG Forum's Pro-MPEG FEC, is described in one of the subsections of the next chapter. The next chapter focuses in the compression of video in case of a DVB system and the content and formation of the MPEG-2 Transport Stream. There needs to be a way to transfer non-IP Transport Stream over an IP based network so the encapsulation of MPEG-2 Transport Stream into IP packets is also covered in the following section.

4 TRANSMISSION OF DIGITAL VIDEO SIGNAL

Digital Video Broadcasting – Terrestrial (DVB-T) is the standard chosen for digital television in Finland and many other European countries. The main advantages of digital television compared to analogue television are for example higher quality of video and audio, good spectral efficiency and error correction. The main elements in the DVB-T system from the distributor's point of view are encoders, decoders, multiplexers and transmitters. In this study the main focus is on the encoded and compressed digital video signal and how it can be transported to remote DVB-T decoders and transmitters.

The following subsections will introduce the video compression standard used in DVB system, MPEG-2. The main interest from the tests' point of view is on the MPEG-2 Transport Stream and the critical components it consists of. The interface between DVB system and IP networks is studied in the last subsection of the chapter. It is also mentioned, that it is possible to use error correction when streaming IP encapsulated MPEG-2 Transport Stream even though IP Multicast is being used.

4.1 MPEG-2 Standard

The Moving Pictures Expert Group (MPEG), set up in the late 1980's, first created MPEG-1 standard for moving picture digital compression. This was originally used for compressing moving images to be replayed from CD-ROM with data rate around 1,5 Mbit/s. Later, a new standard optimized for broadcast video compression was needed and the MPEG-2 standard was defined. Enhancements added to MPEG-1 to form MPEG-2 were for example higher sampling resolution and different aspect ratios. The MPEG-2 standard is very scalable and it can be decoded to different picture resolutions. [11, p. 1.2.]

4.2 MPEG-2 Compression

The general structure of an MPEG encoder is shown in Figure 10.

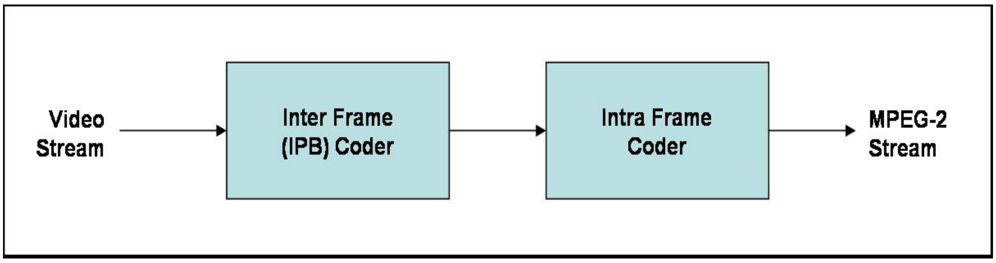


Figure 10. *General structure of an MPEG encoder. [11, p. 3.1]*

In the inter frame coder, or the IPB coder, the compression is based on predicting the next video frame either from an earlier frame (*P* frames), or previous and following frame (*B* frames). Also *I* frames, that are not predicted from other frames, are compressed as stand alone units. The use of *P* and *B* frames greatly improves the efficiency of the picture compression, because the content usually changes very little between neighbouring frames. Only the difference between the predicted frame and actual video frame needs to be transmitted, which reduces significantly the amount of data. Normal video frames entering the encoder are referred to as Presentation Units. When the frames exit the inter frame coder as *I*, *P* and *B* frames, they are called Access Units. [11, p. 2.1.]

After the inter frame coder, the Access Units enter the intra frame coder which can also be seen in Figure 10. In the intra frame coder the compression is done with different bit rate reduction (BRR) processes. The main goal of the intra frame coder is to reduce the amount of bits that represent the video stream. [11, p. 2.1] The stream of concatenated *I*, *P* and *B* frames that exits the inter and intra compression processes, is called the MPEG-2 Elementary Stream (ES). Figure 11 below shows the high level MPEG-2 processes and structure. The Elementary Stream is broken into packets to form the Packetised Elementary Stream (PES) which will be discussed further in the next chapter.

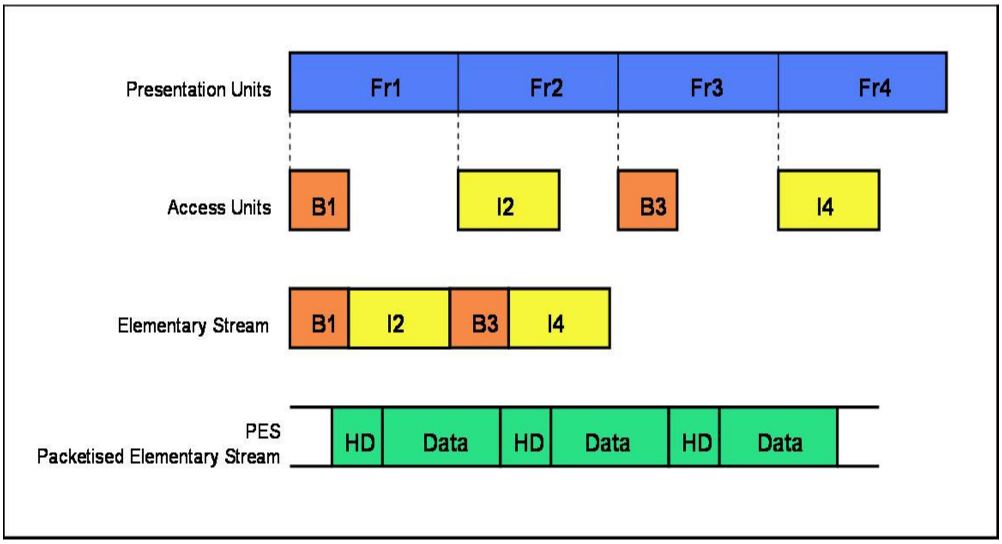


Figure 11. *High Level MPEG System Layer Structure. [11, p. 5.1]*

4.3 MPEG-2 Transport Stream

Once the original video stream has been processed by the MPEG-2 compression layer, the data stream must be assembled for transmission. After the encoding process, Elementary Streams enter a packetiser which forms Packetised Elementary Streams (PES's). Packetised Elementary Streams are streams of packets that are 64 kilobytes or less in size, with the exception of video packets which are not constrained. All packets have a header and data section and the data can be for example audio, video or control. [11, p. 5.2.]

In Figure 12 it can be seen that the Transport Stream is generated from different Packetised Elementary Streams.

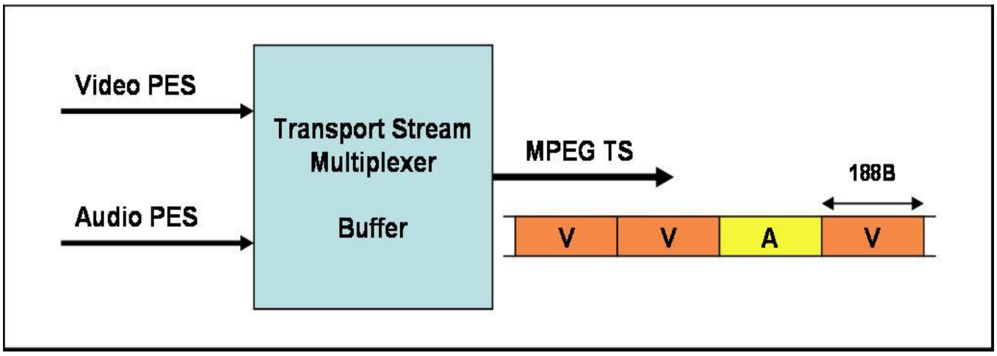


Figure 12. *Transport Stream generation. [11, p. 5.5]*

Every PES is broken into 184 byte blocks, which are then multiplexed to form a stream of 188 byte Transport Stream packs (Figure 13).

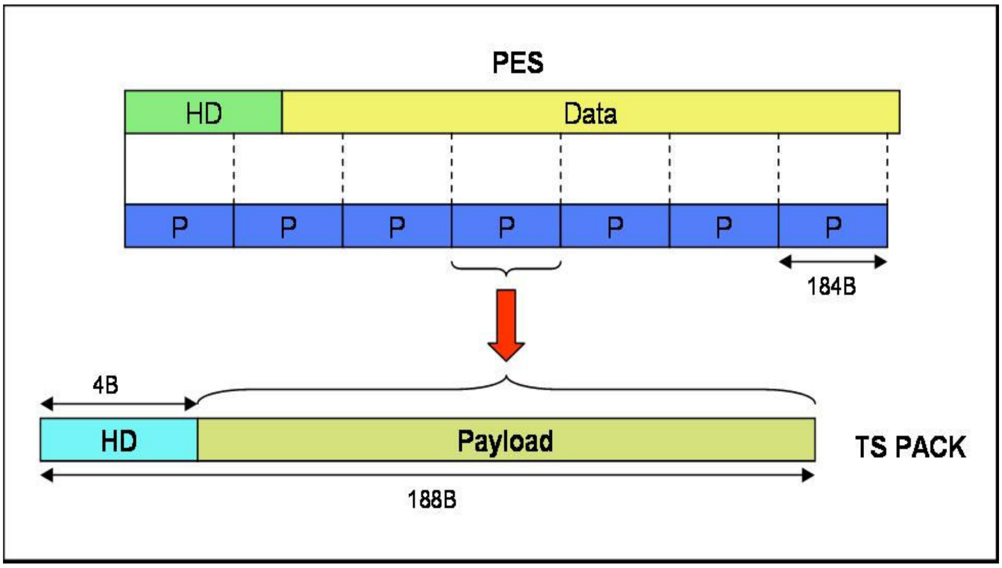


Figure 13. *Transport Stream packet structure. [11, p. 5.5]*

The stream is also buffered in order to achieve constant rate output. TS packs include 4 byte header section and 184 byte payload (data) section. Because the data section of the pack needs to be 184 bytes and it is unlikely that a PES packet is a multiple of that, padding data can be added to adaptation fields in place of the payload. [11, p. 5.4.]

The Transport Stream packet header carries 32 bits of information. The most important fields in the header are Sync (8 bits), Continuity Counter (4 bits) and packet ID, PID (13 bits). The Sync and the Continuity Counter (CC) increase the reliability of the stream. The Sync information is carried in every packet, which enables the stream to recover quickly from temporary packet loss. The CC is a simple error checking mechanism which increments for every TS packet of a particular PID value, so that packet loss is noticed. The PID information is very important because it indicates for example to which Packetised Elementary Stream the payload belongs to. As it was mentioned earlier, different PES streams are multiplexed to a single TS stream so there needs to be a way to point out which TS packets are related. Also with PID, it is decided which different PES streams, for example audio, video and teletext, form an entire program or in analogue terms, a channel. PID value 0 is reserved for the Program Association Table (PAT) which contains PIDs for different Program Map Tables (PMTs). PMTs with individual PIDs then contain the PID information of the program components, such as video and audio. The logic of PID relations is shown below in Figure 14. For example, when a viewer selects Program 1, the Program Map Table with PID 0256 would tell the decoder which packet IDs it needs to pull out from the Transport Stream. [11, p. 5.6 – 5.8.]

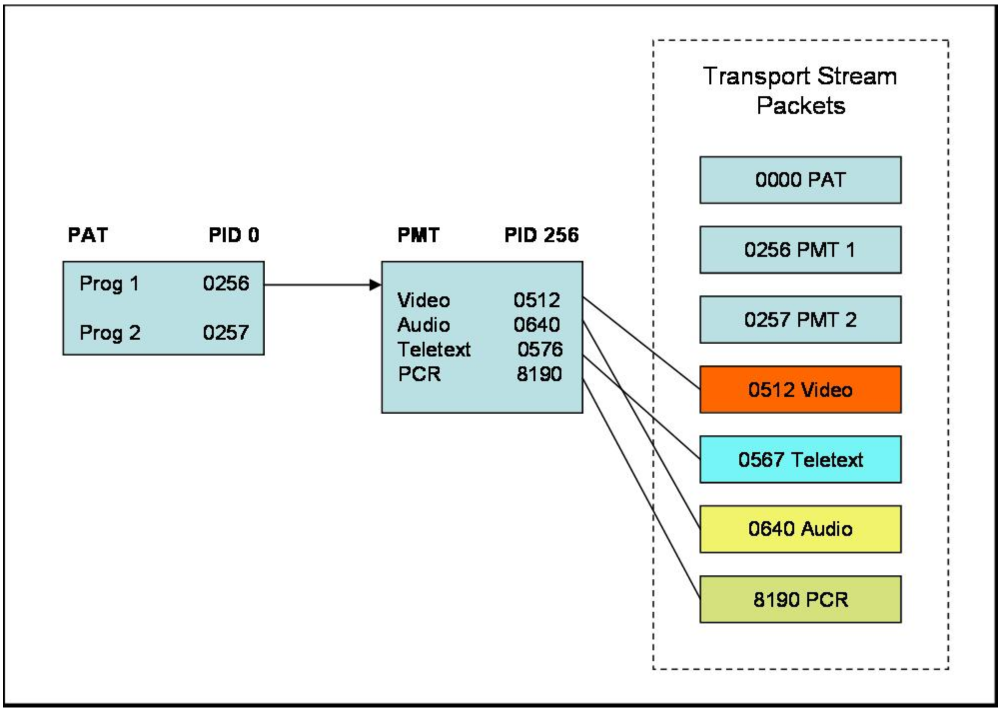


Figure 14. *PID relations. [11, p. 5.7]*

Another important feature in the MPEG-2 Transport Stream is the Program Clock Reference (PCR). The PCR is taken from the encoder's system clock and then incorporated into the Transport Stream (Figure 14) every 40 milliseconds. In order for the program to be presented correctly, all the elements in the system need to be synchronized. PCR is used to synchronize the decoder's clock, but there are also timestamps in the program material which define when the material should be presented to the decoder and when it should be presented to the viewer. It is obvious that the Program Clock Reference is very sensitive to different kind of transmission problems such as jitter and packet loss, so it is necessary to guarantee a low latency and high priority transmission for the Transport Stream. [11, p. 5.8 – 5.11.]

4.4 MPEG TS to IP Encapsulation and Pro-MPEG FEC

As mentioned in the Multicast section of this study, the reliability and error correction is very difficult when using UDP protocol for streaming for example IP encapsulated high bandwidth video over a packet switched network. On the other hand, UDP or RTP are the only reasonable protocols to use with these kinds of applications. Pro-MPEG forum's Code-of-Practice #3 defines a scheme for Forward Error Correction (FEC) when using UDP for streaming IP encapsulated MPEG Transport Stream.

On its way from source to destination, a stream will most likely pass an Ethernet section at some point of the network. The maximum transmission unit (MTU) of an Ethernet network is usually 1500 bytes in size and because in this case fragmentation is not allowed, the IP frame can contain maximum of seven 188 byte MPEG TS packets (Figure 15). [12]

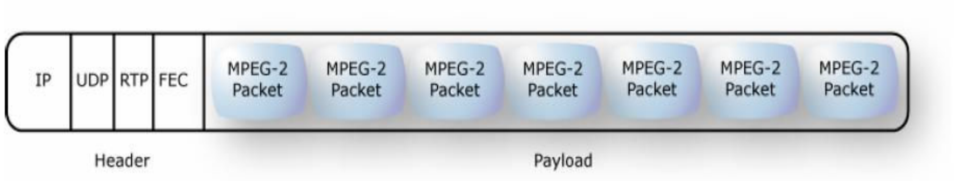


Figure 15. *Seven MPEG-2 TS packets in an RTP packet. [12]*

The number of TS packets in an IP frame can usually be defined in the encapsulation process. 7 TS packets in an IP frame is the most efficient encapsulation from the network's point of view, but packet loss on the other hand causes the most damage to the video stream. Less than 7 TS packets per IP frame reduces data loss in case of a packet drop but increases transmission overhead. [12.]

In the Pro-MPEG FEC scheme the FEC packets, that contain the information for recovering missing packets, are generated from periodically selected media packets. The media packets are first placed in a matrix whose size can be pre-defined. Matrixes are expressed as (L,D) notation, where L is the length (number or columns) and D is the depth (number of rows) of the matrix. There are two types of FEC packets; column FEC and row FEC packets.

The column FEC packets are generated by performing an XOR operation for media packets in the same column. Packets in the same column are not consecutive, so column FEC is effective against burst errors and is able to recover lost packets for as many consecutive packets as there are columns. The row FEC packets are generated by performing the same operation for consecutive media packets in the same row. The row FEC is effective against random packet loss where only one packet is lost. A combination of column and row FEC results in robust error correction scheme that is able to correct both burst and random media packet loss. [13, p. 6] The operation of Pro-MPEG FEC with column and row FEC packets is shown in Figure 16.

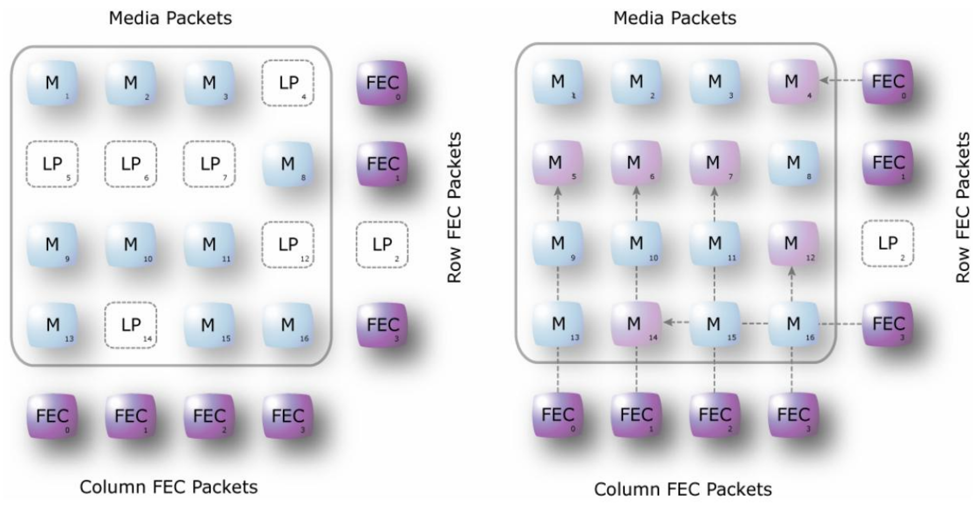


Figure 16. *Operation of Pro-MPEG FEC. [12]*

Column FEC packets are able to recover the missing consecutive media packets 5, 6 and 7. Row FEC packets recover the missing random packets 4 and 14. Because one of the row FEC packets is also missing, column FEC can step in since it is always able to correct one media packet per column.

According to the standard, the FEC packets are transmitted alongside the media as separate streams on different UDP ports. While the data is using UDP port number *n*, the column FEC uses port number *n+2* and row FEC port number *n+4*. This allows also the receivers that do not have FEC enabled to receive the media stream. Receivers that do not support Pro-MPEG FEC simply ignore the FEC streams. [12.]

The cost of using Forward Error Correction in this manner is, of course, increased transmission overhead. The size of the media packet matrix has an effect on the required overhead. As stated before, the size of the matrix can be selected and therefore it can be optimized for networks with different behavior. In networks where packet loss is expected to appear mostly in bursts, a matrix with more columns and fewer rows should be used. In networks where random packet loss is expected, the matrix size should be chosen vice versa. [12] Table 1 shows how the matrix size affects on transmission overhead, implied latency with different bit rates and how many IP packets are recoverable.

Table 1. *Influence of the FEC matrix size on transmission overhead, network latency and recovery capabilities. [13, p. 8]*

XOR (L,D)	Overhead	Latency			Recovery (IP Packets)	Buffer size
		3Mbit/s	30Mbit/s	100Mbit/s		
XOR (5,10)	10%	175,5 ms	17,5 ms	5,3 ms	5	66400B
XOR (10,10)	10%	350,9 ms	35,1 ms	10,5 ms	10	132800B
XOR (20,5)	20%	350,9 ms	35,1 ms	10,5 ms	20	132800B
XOR (8,8)	12,5%	224,6 ms	22,5 ms	6,7 ms	8	84992B
XOR (10,5)	20%	175,5 ms	17,5 ms	5,3 ms	10	66400B
XOR (8,5)	20%	140,4 ms	14,0 ms	4,2 ms	8	53120B
XOR (5,5)	20%	87,7 ms	8,8 ms	2,7 ms	5	33200B
XOR (4,6)	16,7%	84,2 ms	8,4 ms	2,5 ms	4	31872B
XOR (6,4)	25%	84,2 ms	8,4 ms	2,5 ms	6	31872B

All of the major techniques and their properties involved in this study have now been explained to some extent. At least these subjects have to be understood before any testing can take place. Unfortunately not all of the techniques covered in this study could be used in the tests because of equipment restrictions. The following section will explain how the test environment was set up and present all the tests that were made and the results that were gained.

5 TESTING DIGITAL VIDEO TRANSFER OVER MPLS NETWORK

The testing took place in a telecommunications laboratory at Digita Oy. The goal was to perform tests that would be somewhat realistic and that would give some idea about the requirements what such a critical application as video sets for an MPLS network.

Because the idea of packet switched networks is that there can be multiple services sharing the same network, a lot of thought had to be given for Quality of Service in the test setup. In order to see if the Quality of Service definitions really worked for the video stream in the MPLS core network, a lot of background traffic had to be generated to create congestion. The lack of decent IP traffic generators forced to configure the MPLS core links as 100Mbit/s even though the equipment would have been capable of 1000Mbit/s on every link. The video stream used Real-time Transfer Protocol (RTP) and it was distributed throughout the network by using IP Multicast. The operation of multicast in the network also had to be verified and monitored.

The other aspect of the tests performed was to monitor how quickly the network recovers from a failure. There are a few ways to shorten the recovery time caused by a topology change or link failure, one of them is MPLS Traffic Engineering which was discussed earlier in the study. Other ways to make network convergence faster is to modify the timers of Interior Gateway Protocol, in this case OSPF. Unfortunately MPLS Fast-ReRoute feature is only supported on Packet-over-Sonet (POS) interfaces on the routers that were used and those POS interface cards were not available at the time of the testing. Detailed IP layer monitoring and analyzing was done with an IP analyzer at the edge of the MPLS network.

Besides testing the MPLS network and how the traffic behaves in it, the video and MPEG2-TS were also closely monitored. Video quality degradation was in most of the cases immediately seen visually. Lost IP frames and following errors in RTP sequence numbers appeared as malformed pixels and pauses in the video. Also a measuring device, designed for DVB technology and especially for MPEG2 Transport Stream, was used in the test setup to monitor the critical components in the TS.

The layout of the test network can be seen in Figure 17.

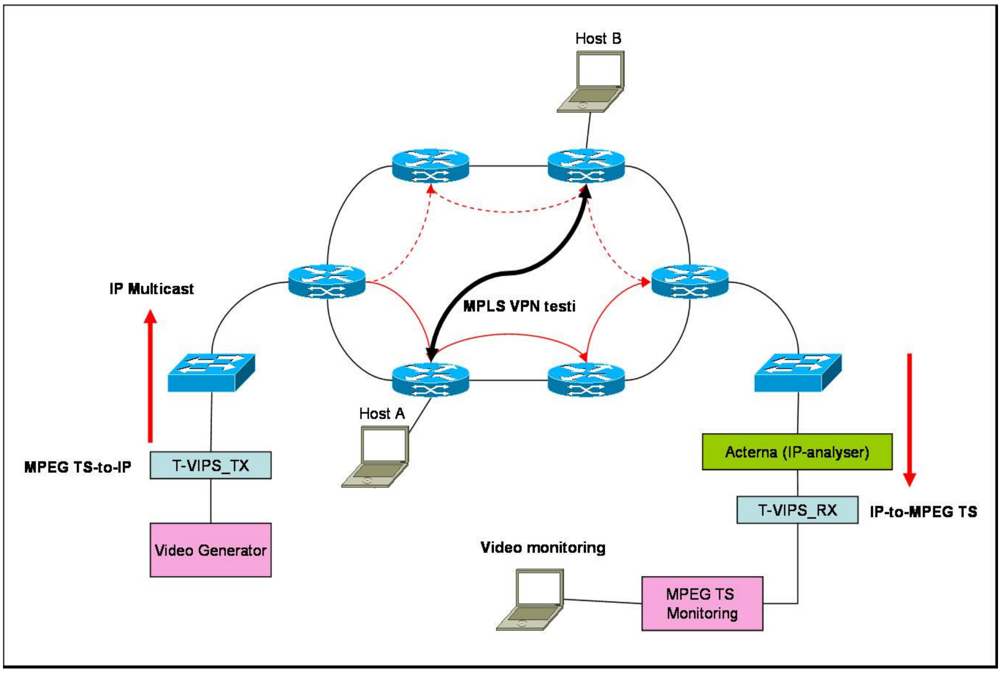


Figure 17. *Test network setup*

The network consists of six MPLS routers, two switches, a video generator and a pair of MPEG2-to-IP video gateways of which the other transmits and the other receives. In addition, there is equipment for analysis and for creating background traffic. All the devices used in the test network are described in the following sub-section.

5.1 Equipment

The MPLS core network was built using six Cisco 7206VXR routers with NPE-G1 processor cards. Routers were interconnected so that they formed a redundant ring topology. The NPE-G1 processor card, used in the routers, comes with three 10/100/1000Mbit/s Ethernet interfaces. As mentioned earlier, the 100Mbit/s configuration was used. The processor card is capable of processing 1 million packets per second. This can be considered high performance, especially in such a small network as this one. Each router has six slots for additional interface cards, such as POS cards that enable router to be interconnected to SDH (Synchronous Digital Hierarchy) networks. Cisco 7200VXR series routers are considered to be the best choice for Provider Edge (PE) routers, which are placed commonly between smaller network segments and a high bandwidth core network. These routers can be also used alone to build a moderately wide, for example nationwide, network where the use of separate core network is not necessarily efficient. In this test setup the routers acted as PE routers.

Access to the network was built with two Cisco Catalyst 3750 Metro switches. Even though these switches have routing functionalities, they acted only as switches in this setup. The switch has 24 10/100/1000Mbit/s Ethernet ports and for fibre optics two 1000Mbit/s interface pairs, which need SFP modules in order to function. Again, the uplink bandwidth was constrained to 100Mbit/s.

In addition to the MPLS core network, the video gateways which performed the encapsulation of MPEG TS into IP played an important role in the whole testing environment. These devices are manufactured by T-VIPS and the precise model is TVG420. TVG420 can be configured to be either a transmitter, which encapsulates MPEG TS into IP and streams it to the network, or a receiver, which receives the IP stream, de-encapsulates it and sends the data from the ASI interface. One device can handle up to 8 video streams (8 DVB ASI interfaces) and transmit or receive multicast and unicast traffic on the IP side using 10/100/1000Mbit/s Ethernet interface. The maximum Transport Stream bit rate on the TVG420 is 216Mbit/s. The device also has support for Pro-MPEG FEC which was discussed earlier.

The video stream was generated using Rohde-Schwartz Video Generator. The generator had Standard Definition (SD) video files in its hard drive which were played repeatedly. The SD video bit rate is normally 5-7Mbit/s but in order to test the network's capabilities properly, the stream was stuffed with zero bits so that the bit rate seen by the network was actually 38-50Mbit/s.

The MPEG2 Transport Stream was monitored after the MPLS core network with Tektronix' MTM400 Transport Stream Monitor. The main focus was on the PCR component of the TS. MTM400 was able to present real-time graphical statistics of for example PCR jitter and accuracy.

In order to capture and analyze the video stream encapsulated in IP and RTP, a network analyzer was placed in front of the receiving TVG420. Even though TVG420 itself has counters for lost IP frames and RTP sequence errors, a separate analyzer was considered to be more reliable. Acterna DA-3400 was used to capture traffic during network faults, such as congestion and re-routing. The captured traffic was further analyzed with Ethereal Network Protocol Analyzer software, which was able to decode and analyze the RTP streams.

Standard laptops with software for IP traffic generation were used for network congestion tests as well as for monitoring the streamed video. All of the devices in the test setup have been or will be present in a production environment. This test setup was also an opportunity to monitor the behaviour of the devices that have not been used in live networks yet.

5.2 Setting up the MPLS and Multicast Network

The first step of setting up the test environment was to configure an operational MPLS core network. IP addresses for routers and router interfaces had to be allocated first. Once the addresses had been configured, the IGP routing was established using OSPF. All the routers belonged to the same OSPF area to avoid unnecessary complexity. After the tag-switching was configured on the interfaces, the MPLS core was up and running. The IP addressing of the links and routers can be seen in Figure 18.

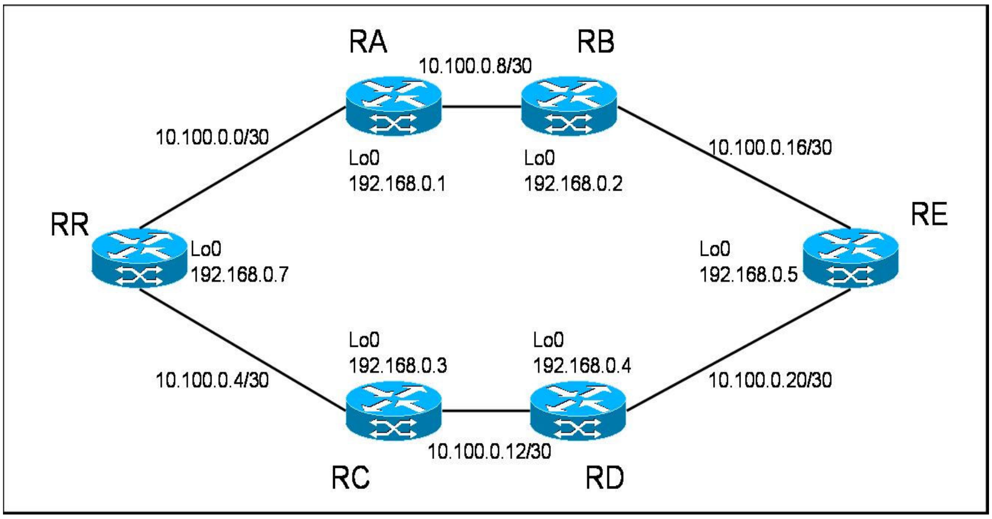


Figure 18. *IP addressing of the MPLS core network*

In order to transfer IP encapsulated MPEG TS over the network, multicast features needed to be configured also. All the router interfaces were configured to act in PIM Sparse Mode and one of the routers, RR, was chosen as the rendezvous point.

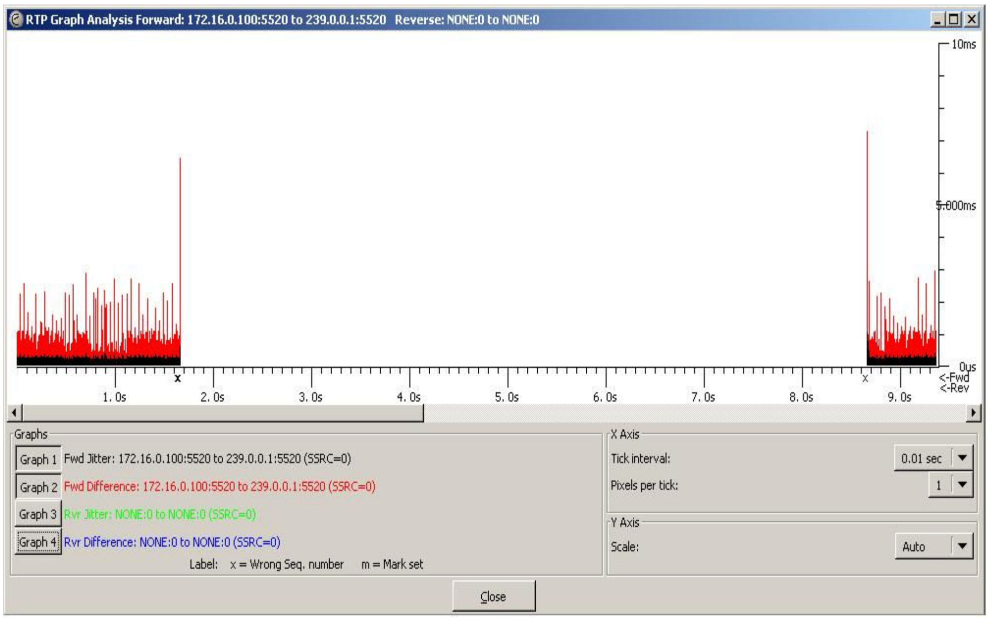
An MPLS Virtual Private Network called “testi” was also configured in the network to make the test setup more like a production network and separate traffic at a logical level. MPLS VPN required the use of Multiprotocol Border Gateway Protocol (MBGP) in the network. Border Gateway Protocol peering was implemented by using a Route Reflector (RR). Router RR acted as the Route Reflector for the network. The basic idea of a Route Reflector is that it distributes information that it gets from one BGP peer to other peers. Peers are configured as Route Reflector Clients in the Route Reflector and every peer has BGP neighbour relationship with the RR. This method decreases the traffic caused by routing information exchange and the sizes of state tables in the peering routers. In addition to the MBGP configuration, a Virtual Routing and Forwarding (VRF) instance, which is the actual MPLS Virtual Private Network, was configured on the routers. In this setup routers RC and RB had one sub-interface associated with the VRF “testi”. MPLS VPN can be thought as a network inside a network. Traffic that flows inside a Virtual Private Network has no knowledge about any other traffic in the same physical network and vice versa, although it uses the same network resources.

After it was tested that normal unicast traffic was flowing through the network and the VPN, the multicast features were configured. As stated before all the router interfaces, except the ones that belong to the VPN, were configured to act in Protocol Independent Multicast Sparse-mode (PIM-SM). The transmitting TVG420 MPEG Transport Stream to IP encapsulator was configured to stream its output to multicast group address 239.0.0.1 and the receiving TVG420 was configured to join that group. As it can be seen in Figure 17 on page 25, the transmitting TVG420, referred to as T-VIPS_TX in the figure, was connected to router RR through a Cisco 3750 Metro switch. The receiving TVG420, referred to as T-VIPS_RX, was connected to router RE also through a similar switch. Because router RR was located nearest to the multicast source and the network used redundant ring topology, router RR was the logical choice to be configured as the rendezvous point (RP) of the shared tree. When the T-VIPS_TX started streaming the encapsulated video and the T-VIPS_RX joined the multicast group, the Multicast Distribution Tree (MDT) was formed. The multicast traffic started flowing from router RR to router RE through routers RC and RD.

5.3 Initial Testing of the Network

The first thing that was tested was how quickly the MPLS core network would recover from a link failure and how the failure would affect the monitored video. The video stream bit rate was raised with the video generator up to 50Mbit/s to create load on the network. The effective bit rate of the video stream was approximately 4,5Mbit/s which is roughly the bit rate of one channel in the DVB-T system. The remaining 45,5Mbit/s was just zero bits.

The link failure was created on the link between routers RC and RD. That link was chosen because the Multicast Distribution Tree was formed through those routers, hence the multicast video traffic was flowing through them. Through unplugging the cable between routers RC and RD, it was tested how quickly the Interior Gateway Protocol OSPF (Open Shortest Path First) distributed the information across the network and how quickly a new MDT was formed. The results of this generated fault were monitored visually at the receiving end and also the traffic during the fault was captured. The captured traffic was further analyzed with Ethereal Network Protocol Analyzer. As it can be seen in Figure 19, there was roughly a 7 second break in the RTP stream caused by the unplugged link between routers RC and RD. In other words, it took altogether 7 seconds for OSPF to find another path and PIM to build a new Multicast Distribution Tree from source to destination.


RTP Graph Analysis Forward: 172.16.0.100:5520 to 239.0.0.1:5520 Reverse: NONE:0 to NONE:0

Graphs

Graph 1 Fwd Jitter: 172.16.0.100:5520 to 239.0.0.1:5520 (SSRC=0)

Graph 2 Fwd Difference: 172.16.0.100:5520 to 239.0.0.1:5520 (SSRC=0)

Graph 3 Rvr Jitter: NONE:0 to NONE:0 (SSRC=0)

Graph 4 Rvr Difference: NONE:0 to NONE:0 (SSRC=0)

Label: x = Wrong Seq. number m = Mark set

X Axis

Tick interval: 0.01 sec

Pixels per tick: 1

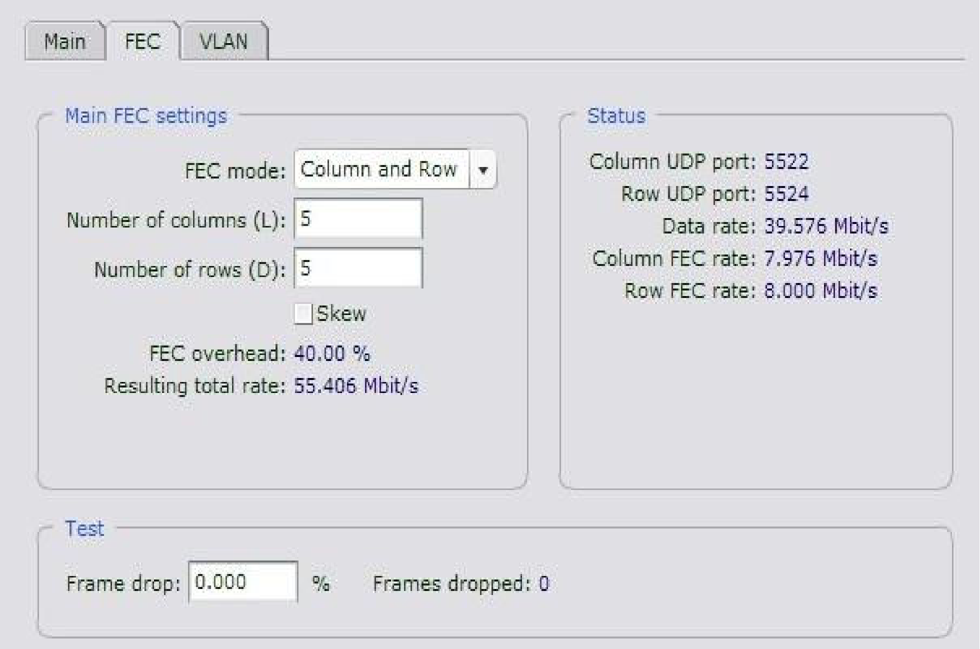
Y Axis

Scale: Auto

Figure 19. *Received RTP stream during link failure between routers RC and RD*

In the monitored video this disruption appeared as frozen picture. The video started playing at the receiving end as soon as the network recovered from the fault. With the bit rate that the video was streamed, more than 25000 RTP packets were dropped during the failure. It was also measured if there was a disruption when the unplugged link was plugged back in, and the traffic returned on the original path. Only 18 RTP packets were lost during the path change and its effect on the video was only some mosaic figure in the picture.

Because the TVG420's had support for Pro-MPEG Forum's Forward Error Correction, it was also tested if FEC had any effect on the received video. The matrix size for the media packets was defined to be 5 columns and 5 rows. Video bit rate had to be dropped to 39Mbit/s because of the overhead the FEC generated. The total bit rate with 5 by 5 FEC was 55Mbit/s which means that the overhead was 40% of the original bit rate. The FEC configuration and bit rates in the transmitting TVG420 can be seen in Figure 20.



Main FEC settings

FEC mode: Column and Row
Number of columns (L): 5
Number of rows (D): 5
□ Skew
FEC overhead: 40.00 %
Resulting total rate: 55.406 Mbit/s

Status

Column UDP port: 5522
Row UDP port: 5524
Data rate: 39.576 Mbit/s
Column FEC rate: 7.976 Mbit/s
Row FEC rate: 8.000 Mbit/s

Test

Frame drop: 0.000 %
Frames dropped: 0

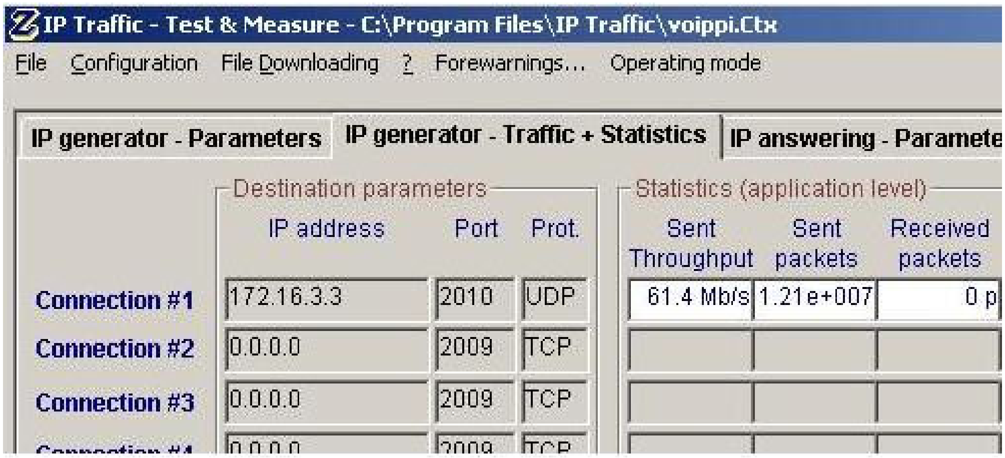
Figure 20. *FEC configuration in the transmitting TVG420*

Because of the number of lost RTP packets, FEC did not have any effect on the received video. With the matrix size used it is only possible to recover 5 consecutive RTP packets. In addition, also FEC packets were lost during the fault because all network traffic was stopped.

5.4 Testing Quality of Service for the Video Stream

The second test that was done was to see what happens to the video stream when the MPLS core links are congested. As mentioned before, the core links were configured as 100Mbit/s each. The video stream bit rate was 50Mbit/s so in order to congest the links, at least another 50Mbit/s of traffic had to be generated. To make it more interesting, the additional load was generated inside the MPLS Virtual Private Network that was configured on the network. This way the video stream and the bulk traffic were separated logically although they used the same physical network.

As it can be seen in the picture of the test network setup (Figure 17, page 25), laptops were connected to routers RC and RB. Those laptops were connected to router interfaces which belonged to the MPLS VPN “testi”. The laptop attached to router RC, Host A, had IP traffic generator software installed. Because there was only one license for the software, Host B acted merely as an endpoint for the traffic. In other words, UDP protocol had to be used. The parameters of the IP traffic generator software can be seen in Figure 21. Host A sent UDP traffic at bit rate of roughly 60Mbit/s to Host B, whose IP address was 172.16.3.3.

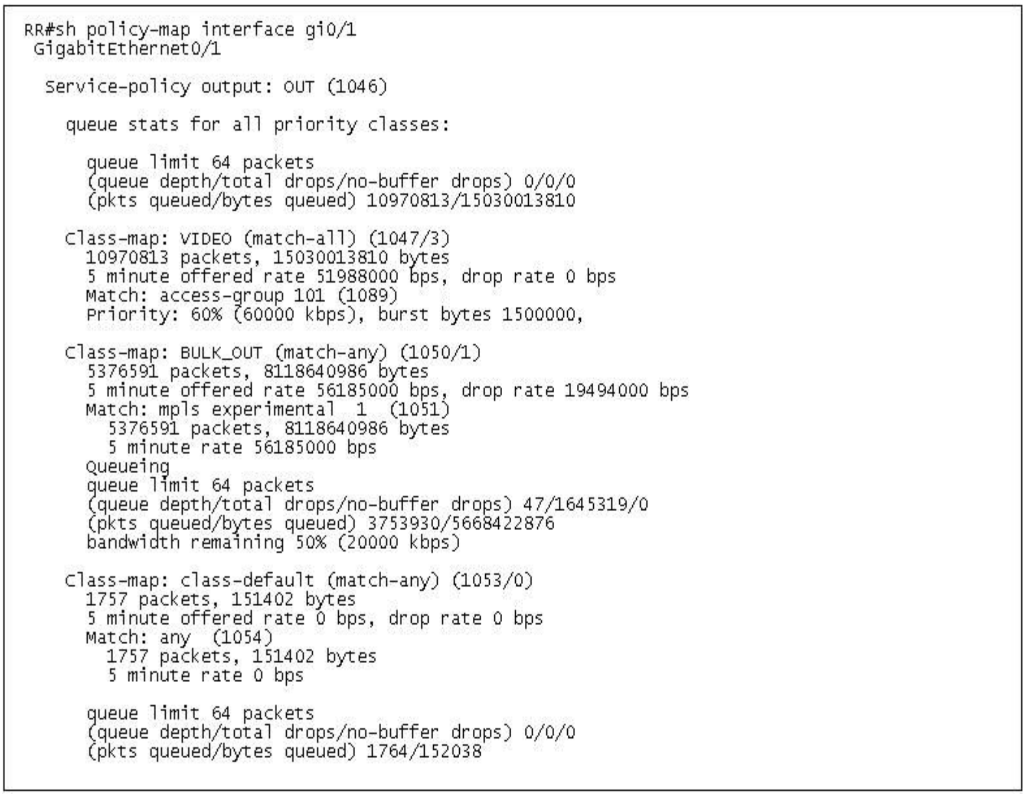

IP Traffic - Test & Measure - C:\Program Files\IP Traffic\voippi.Ctx
File
Configuration
File Downloading
?
Forewarnings...
Operating mode
IP generator - Parameters
IP generator - Traffic + Statistics
IP answering - Paramete
Destination parameters
Statistics (application level)

	IP address	Port	Prot.	Sent Throughput	Sent packets	Received packets
Connection #1	172.16.3.3	2010	UDP	61.4 Mb/s	1.21e+007	0 p
Connection #2	0.0.0.0	2009	TCP			
Connection #3	0.0.0.0	2009	TCP			
Connection #4	0.0.0.0	2009	TCP			

Figure 21. *IP traffic generator software in laptop Host A*

Because there were no Quality of Service parameters configured on the MPLS core routers, the video quality decreased significantly. The monitored video was practically a blur. Not a single clean video frame came through because of the excessive packet loss. Forward Error Correction did not really have an effect on the viewed video. The video remained a blur.

The goal of the Quality of Service definitions was to guarantee a reliable delivery of the video stream from source to destination even at the expense of other traffic. The IP addresses of both the video source and the bulk traffic source were known, therefore the classification of the traffic was done based on them. Access-lists which recognized the sources were placed on the routers where the sources were connected to. The video source T-VIPS_TX was connected to router RR and Host A which was sending the bulk traffic was connected to router RC (Figure 16). After the routers recognized the traffic, they were configured to mark the video traffic with Expedited Forwarding (EF) bits and bulk traffic with low priority MPLS Experimental bit 1. In addition, traffic policing was done on each link interface in the core. 60 percent of the link bandwidth across the whole MPLS core network was reserved for the video traffic. 50 percent of the remaining bandwidth was guaranteed for the bulk traffic but it did not really make any difference because there was not any more additional traffic in the network. In this experiment the multicast traffic for the video was flowing from router RR to router RE via routers RA and RB. The bulk traffic was flowing inside the MPLS Virtual Private Network from router RC to router RB through routers RR and RA (Figure 16). According to this traffic flow the first congested link was the link between routers RR and RA. The actions of Quality of Service policing for the congested link from router RR's point of view can be seen in Figure 22.



```
RR#sh policy-map interface gi0/1
 GigabitEthernet0/1

  Service-policy output: OUT (1046)

    queue stats for all priority classes:

      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts queued/bytes queued) 10970813/15030013810

    Class-map: VIDEO (match-all) (1047/3)
      10970813 packets, 15030013810 bytes
      5 minute offered rate 51988000 bps, drop rate 0 bps
      Match: access-group 101 (1089)
      Priority: 60% (60000 kbps), burst bytes 1500000,

    Class-map: BULK_OUT (match-any) (1050/1)
      5376591 packets, 8118640986 bytes
      5 minute offered rate 56185000 bps, drop rate 19494000 bps
      Match: mpls experimental  1  (1051)
        5376591 packets, 8118640986 bytes
        5 minute rate 56185000 bps
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 47/1645319/0
      (pkts queued/bytes queued) 3753930/5668422876
      bandwidth remaining 50% (20000 kbps)

    Class-map: class-default (match-any) (1053/0)
      1757 packets, 151402 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any  (1054)
        1757 packets, 151402 bytes
        5 minute rate 0 bps

      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts queued/bytes queued) 1764/152038
```

Figure 22. *Output of the command "show policy-map interface GigabitEthernet0/1" in router RR shows the reserved bandwidths and how the bulk traffic is dropped*

In the command output in Figure 22 it can be seen that the Service-policy which was attached to the outgoing link interface GigabitEthernet0/1 contained two Class-maps: one for video and one for bulk traffic. The Class-map for video shows that the video traffic was matched to access-list 101 and then assigned a priority of 60% of the link bandwidth, which in this case was 60Mbit/s. Output also shows the data rate and the drop rate for the traffic flows. At the time, the offered bit rate for the video traffic was almost 52Mbit/s and for bulk traffic over 56Mbit/s. This resulted in congestion and Service-policy needed to take actions. As can be seen in the section for the bulk traffic, the drop rate was almost 20Mbit/s. Not a single video packet was dropped due to congestion after the Quality of Service was configured on the routers. The basic logic of classification, marking and policing of traffic can be seen in Figure 23.

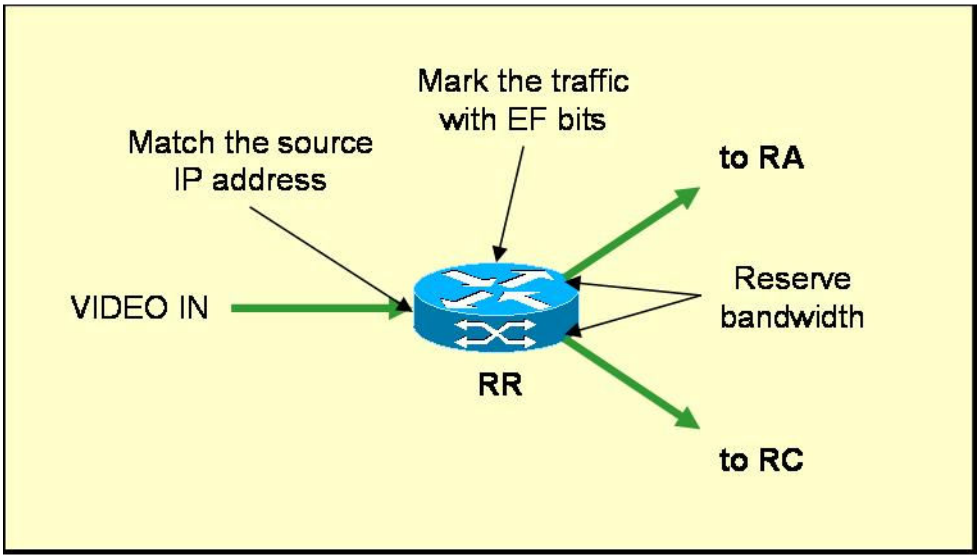


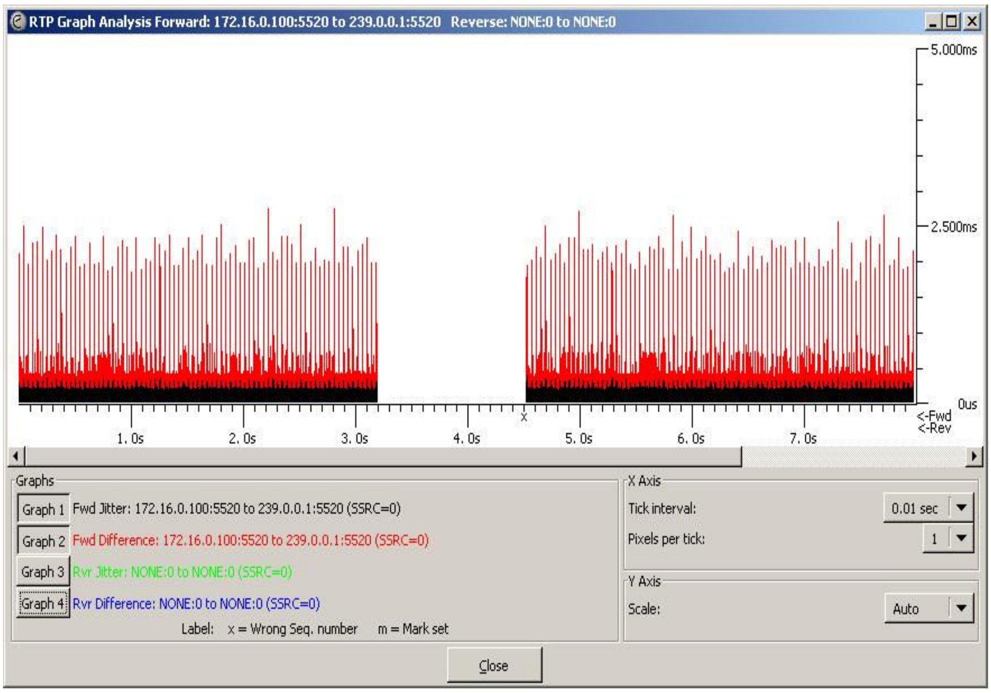
Figure 23. *The logic of Quality of Service actions in router RR*

Figure 23 shows roughly the phases of QoS operation in the router RR. First, the video traffic is recognized by matching the known IP address of the video source to an access-list. Then, the traffic that was matched is marked with high priority EF bits and 60 percent of available bandwidth is reserved for it.

5.5 Optimizing Network Recovery

After the Quality of Service for the video was working and the bulk traffic did no longer have any effect on the video, the last challenge was to shorten the network recovery time from 7 seconds to as short as possible. As stated before, OSPF is the protocol that mainly causes the network convergence to take such a long time. That is why the network optimization was done through tuning the timers that control OSPF Link-State Advertisements (LSAs). Special commands in the network's OSPF configuration enable OSPF to propagate changes in milliseconds. If these commands were not used, the LSAs would be rate-limited to 5 seconds.

When the OSPF configuration on each router had been optimized, the network was ready for the test. The test was carried out in the same manner as in the initial testing of the network. While traffic was flowing from source to destination via routers RR, RC, RD and RE (Figure 18), the link between routers RC and RD was unplugged. Figure 24 shows the received RTP stream during the generated fault.



RTP Graph Analysis Forward: 172.16.0.100:5520 to 239.0.0.1:5520 Reverse: NONE:0 to NONE:0

Graphs

Graph 1 Fwd Jitter: 172.16.0.100:5520 to 239.0.0.1:5520 (SSRC=0)

Graph 2 Fwd Difference: 172.16.0.100:5520 to 239.0.0.1:5520 (SSRC=0)

Graph 3 Rvr Jitter: NONE:0 to NONE:0 (SSRC=0)

Graph 4 Rvr Difference: NONE:0 to NONE:0 (SSRC=0)

Label: x = Wrong Seq. number m = Mark set

X Axis

Tick interval: 0.01 sec

Pixels per tick: 1

Y Axis

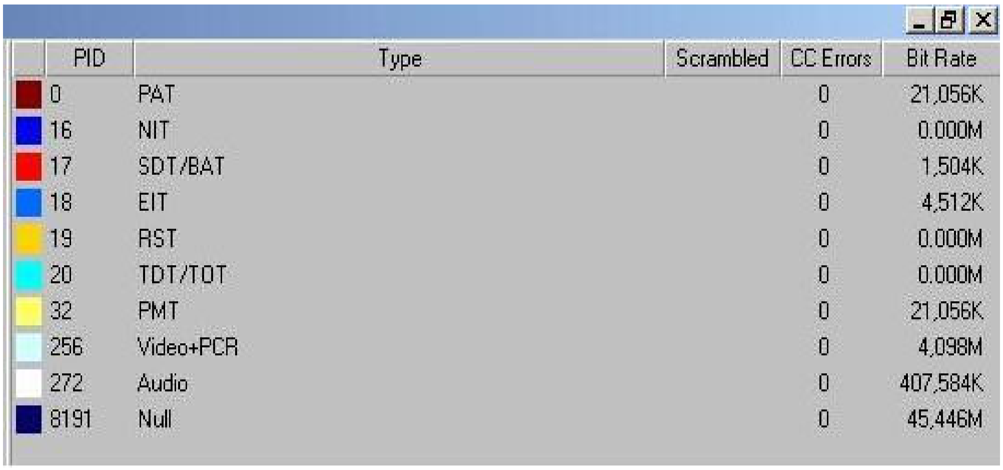
Scale: Auto

Figure 24. *Received RTP stream during link failure between routers RC and RD after OSPF optimization*

As it can be seen in the Figure 24, the time that the network needed to converge and redirect the traffic to alternate path was diminished remarkably. At the receiving end the video was paused roughly for only 1,3 seconds. When the link between RC and RD was re-established, the traffic returned to the original path only slightly faster than in the first test. For this part of the study, help was received from a Cisco consultant who was working on another network project at Digita simultaneously.

5.6 Monitoring of MPEG-2 Transport Stream Components

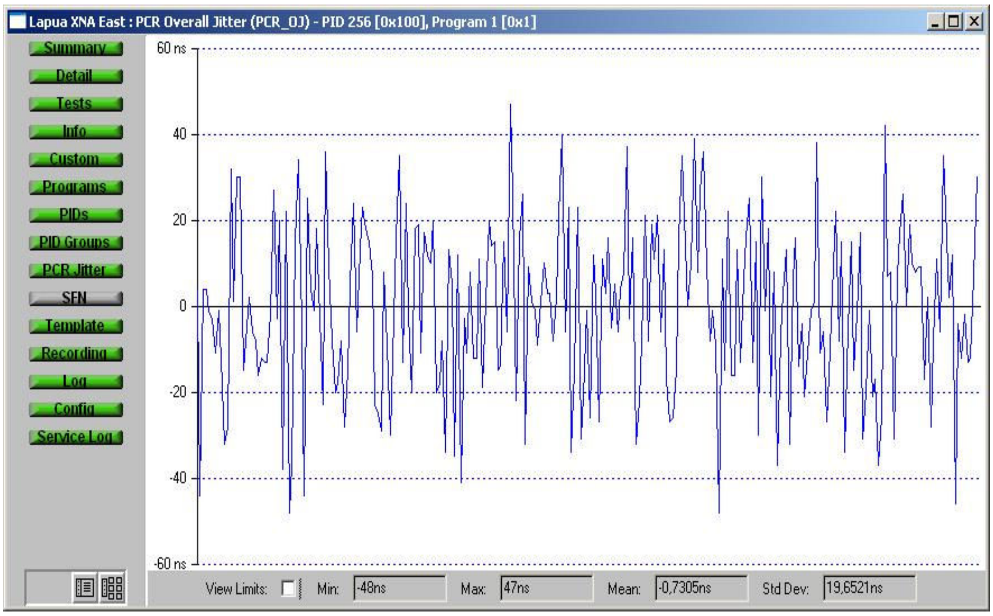
The MPEG-2 Transport Stream was monitored in the test network after the receiving TVG420 (Figure 17, page 25). The main focus was on the Program Clock Reference measurements. As mentioned in section 5, the device which handled the monitoring of the Transport Stream was Tektronix' MTM400 Transport Stream Monitor. Overall, there were no errors or jitter detected in the Transport Stream when the network was in its normal operational state. The different PIDs which the tested Transport Stream included can be seen in Figure 25, along with their bit rates.



	PID	Type	Scrambled	CC Errors	Bit Rate
🟥	0	PAT		0	21,056K
🟦	16	NIT		0	0.000M
🟥	17	SDT/BAT		0	1,504K
🟦	18	EIT		0	4,512K
🟧	19	RST		0	0.000M
🟦	20	TDT/TOT		0	0.000M
🟨	32	PMT		0	21,056K
⬜	256	Video+PCR		0	4,098M
⬜	272	Audio		0	407,584K
🟦	8191	Null		0	45,446M

Figure 25. *MPEG-2 Transport Stream PIDs and their bit rates in the test case*

The actual video and audio stream was, as mentioned before, only 4,5 Mbit/s. As can be seen in Figure 25, the Null PID 8191 made the stream total of 50 Mbit/s, which is what the IP network saw during the tests. Eventually, the only occasion when there were errors seen in the Transport Stream Monitor, was during network recovery tests. This was naturally expected because no data was coming to the receiver. The overall PCR jitter of the tested Transport Stream can be seen in Figure 26.



Lapua XNA East : PCR Overall Jitter (PCR_OJ) - PID 256 [0x100], Program 1 [0x1]

View Limits: □ Min: -48ns Max: 47ns Mean: -0,7305ns Std Dev: 19,6521ns

Figure 26. Overall PCR jitter of the tested MPEG-2 Transport Stream

The minimum and the maximum jitter stayed between +50ns and -50ns the whole time, which can be considered very stable. The limits according to the specifications are +/-500ns.

The next section summarizes the test results and discusses the conclusions that can be made based on the tests and the studies.

6 CONCLUSIONS

The goal of this study was to determine whether the idea of transferring digital video signal for DVB-T system over an MPLS network is currently realistic or not. The main challenges that were tackled were Quality of Service, fault tolerance and bandwidth efficiency.

The previous section of the study presented the test cases and the results that were gained. Building and configuring a fully functional MPLS network with IP Multicast support was alone a moderate challenge. The initial testing of the network simply proved that the network was working as expected and provided a starting point for optimizing the network. Setting up the test network revealed the fact that it requires a lot of work to get the network and all the features up and running. The test network consisted of only six routers and a couple of switches and encapsulators. A nationwide MPLS network could be several times larger, so cutover from an existing SDH system to MPLS based network would require a lot of time and effort. But, as mentioned in the first section of the study, adding new services to an already functional MPLS network does not necessarily need that much work. Quality of Service always needs to be kept in mind when adding new services, though.

The goal of the second actual test was to ensure that other, less critical, traffic would not have an effect on the streamed video. The extra challenge was that the bulk traffic was flowing inside an MPLS VPN and therefore logically in a different network than the video stream. There was a very clear difference between the network without any Quality of Service definitions and the network with priority on the video. After QoS was configured on the network, there was always a bandwidth reserved for the video. If there was congestion on some link in the network, the bulk traffic was dropped and video traffic was flowing without errors. Implementing proper Quality of Service in a vast MPLS network is a challenging task. In this study the configuration of

QoS was very simple because there were only two different services and only a few hosts. The traffic classification was done based on the source IP addresses, which might not be the optimal solution in a larger network. Also, different services need different kind of network resources. For example, voice over IP (VoIP) needs low latency but does not require a lot of bandwidth. Therefore, the QoS definitions need to be considered and designed individually for every service in a network. However, the big picture needs also to be kept in mind so that there are no overlapping definitions.

The third challenge was to tune the network and shorten the time it takes for the network to switch to an alternate path in case of a link failure. The trick was to adjust the timers of OSPF routing protocol. The idea is that by adjusting the interval at which Link-State Advertisements are sent, the routers in the network notice a change in the network sooner and propagate this information a lot faster than when using default timers. This sounds simple, but it is very important to realize all the implications the tuning can have. There is a danger that instead of making the network recover faster, the network might actually become very unstable. In this study, the tuning succeeded well. The time it took for the network to converge diminished by over 5 seconds after the timers were adjusted.

An important part of this study was, of course, the video. The video was monitored visually and with an analyzer. The most critical component of the MPEG-2 Transport Stream, Program Clock Reference, was monitored closely. The major observation that was made was that the MPLS network did not really have any significant effect on the stream's PCR. Packet loss, caused by a link failure, was the only reason there were noticeable errors in the Transport Stream and PCR. This was the goal and it was reached as expected. Unfortunately, it was not possible to create the kind of conditions in the test network that would cause random packet loss. The conclusion that can be made based on the tests is: when MPEG-2 Transport Stream is transferred over an MPLS network along with other services, the main attention should be placed on the reliability of the network and Quality of Service.

The results of the tests are encouraging. It is possible to multicast MPEG-2 Transport Stream over an MPLS network even though there are other services sharing the same network. The main challenges, which might still stand in the way for commercial use, are reliable operation of IP Multicast and stability of router software. Hence, a couple of bugs were found in the used version of Cisco IOS (Internetwork Operating System) during the tests. It is clear that IP Multicast has not been used widely in large networks yet. More testing on this issue should be done before these techniques can be used to provide a transport network for commercial DVB-T system.

REFERENCES

[1] Stallings, William. *The Internet Protocol Journal - MPLS* [Web publication]. Volume 4, Number 3, Sept. 2001 [Accessed May 18, 2006]. www.cisco.com/ipj.

[2] IETF - RFC 2702. *Requirements for Traffic Engineering Over MPLS* [Web document]. 1999 [Accessed May 18, 2006]. http://www.ietf.org/rfc/rfc2702.txt

[3] CCO – Cisco documentation. *MPLS Traffic Engineering and Enhancements* [Web document]. 2006. [Accessed May 23, 2006]. http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a008008029b.html

[4] CCO – Cisco documentation. *Traffic Engineering and Quality of Service in Cisco IP/MPLS Mobile Backbone* [Web document]. 2006. [Accessed May 23, 2006]. http://www.cisco.com/en/US/customer/netsol/ns341/ns396/ns177/ns443/networking_solutions_white_paper0900aecd8022e703.shtml

[5] CCO – Cisco documentation. *MPLS Traffic Engineering Fast Reroute – Link Protection* [Web document]. 2006. [Accessed June 10, 2006]. http://www.cisco.com/en/US/products/ps6550/products_white_paper09186a008008082d.shtml

[6] IETF - RFC 3171. *IANA Guidelines for IPv4 Multicast Address Assignments* [Web document]. 2001 [Accessed July 20, 2006]. http://www.ietf.org/rfc/rfc3171.txt

[7] CCO – Cisco documentation. *Internet Protocol IP Multicast Technology* [Web document]. 2000. [Accessed July 20, 2006]. http://www.cisco.com/en/US/tech/tk828/tech_brief09186a00800a4415.html

[8] IETF - RFC 3973. *Protocol Independent Multicast – Dense Mode (PIM-DM): Protocol Specification (Revised)* [Web document]. 2005 [Accessed July 28, 2006]. http://www.ietf.org/rfc/rfc3973.txt

[9] IETF - RFC 2362. *Protocol Independent Multicast – Sparse Mode (PIM-SM): Protocol Specification* [Web document]. 1998 [Accessed July 28, 2006]. http://www.ietf.org/rfc/rfc2362.txt

[10] IETF - RFC 3208. *PGM Reliable Transport Protocol Specification* [Web document]. 2001 [Accessed August 11, 2006]. http://www.ietf.org/rfc/rfc3208.txt

[11] Tozer E.P.J. and Anderson G.W. *A Guide to Digital Broadcast Technologies.* Version 204. Tandberg Technical Training

[12] Tandberg Television. *Inside Pro-MPEG FEC* [Web document]. [Accessed September 1, 2006]. http://www.tandbergtv.com/pdfs/Inside%20Pro-MPEG%20FEC.pdf

[13] Professional-MPEG Forum. *Pro-MPEG Code of Practice #3 release 2* [Web document]. 2004 [Accessed September 15, 2006]. http://www.pro-mpeg.org/publications/pdf/Vid-on-IP-CoP3-r2.pdf