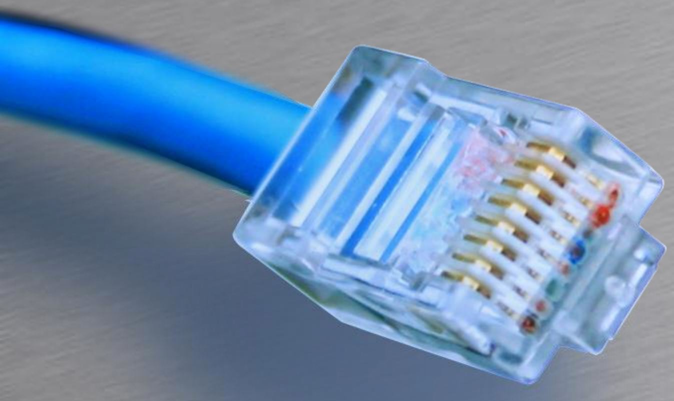
IP Telephony



HOUSE OF TECHNOLOGY

– en del af mercantec+

IPT

WAN Technology / QoS

Subjects

- WAN technologies
  - MPLS/VPLS/Dedicated fiber
- Call Admission Control (CAC).
- QoS principle – Trust boundary.
- DIFFSERV (DSCP) Priority Queuing.
- 802.1Q/p (P-tagging) Switch Queues.
- Layer2/3 QoS marking and remarking.

WAN technologies

Wide Area Networks

WAN technologies

- VPN
  - Virtual Private Network
- MPLS VPN
  - Multi Protocol Label Switching
- VPLS
  - Virtual Private LAN Service
- MAN
  - Metropolitan Area Network
- Dedicated fiber

Type of netwoks

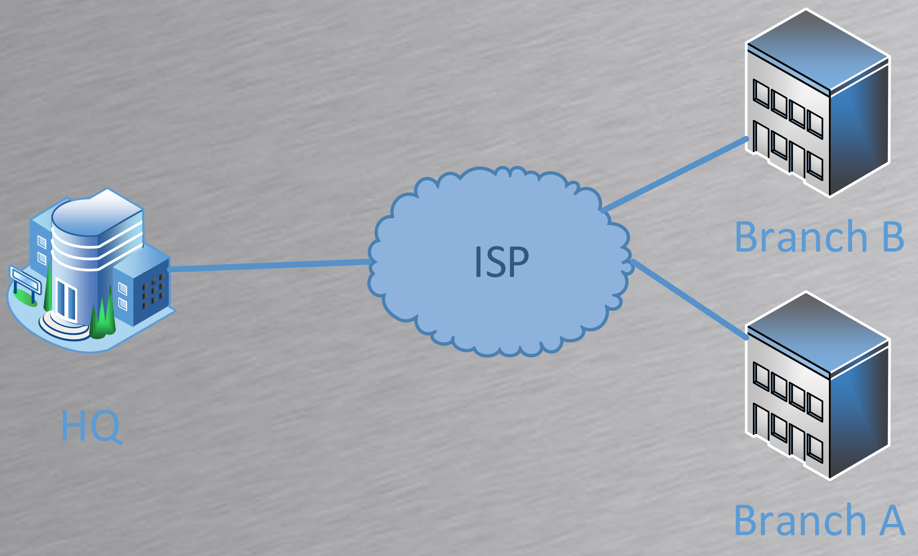
- Network geographically extent

Abbr	Meaning	Typical coverage	Typical use
PAN	Personal Area Network	< 10 meters	Bluetooth, IrDA
LAN	Local Area Network	< 1 Km	Ethernet
MAN	Metropolitan Area Network	< 10 Km	Metro Ethernet
WAN	Wide Area Network	> 10 Km	MPLS, VPLS

VPN

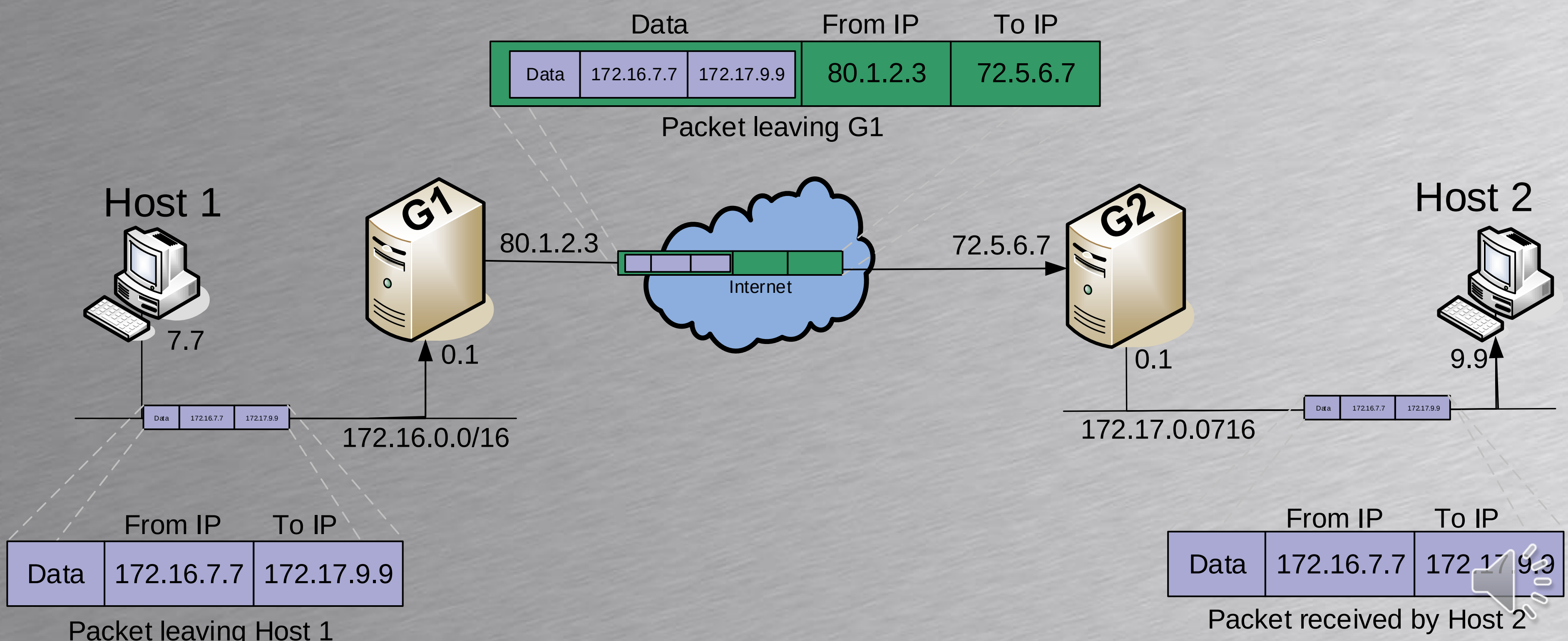
Virtual Private Network

- A private network is a network owned by an organization
- A virtual private network is a leased connection between two or more end-points. Typically leased from an ISP



Tunneling protocol

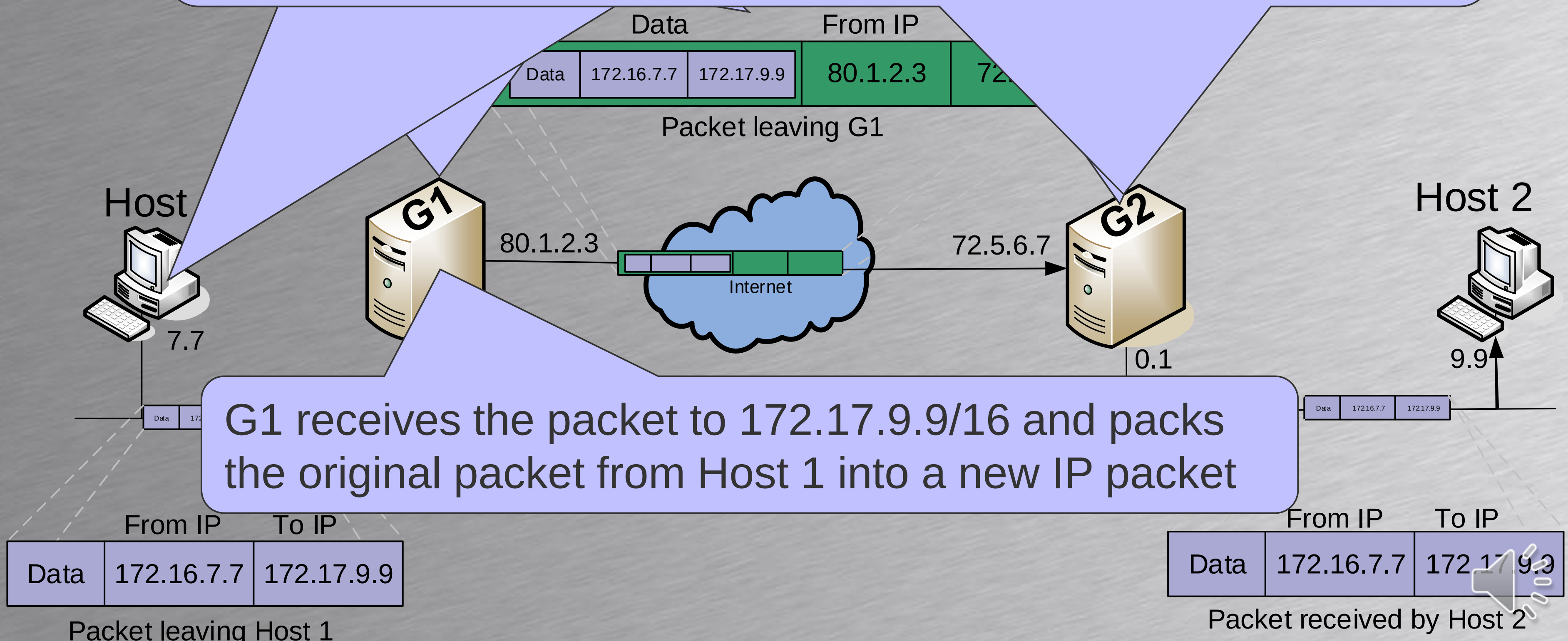
- A tunneling protocol is a logical path between two gateways where traffic is transmitted
- An IP packet within an IP packet



Tunneling protocol

G1 transmits the new packet to its Peer G2 using public IP addresses
The packet is transmitted between 80.1.2.3 and 72.5.6.7
NOT
Also
its de

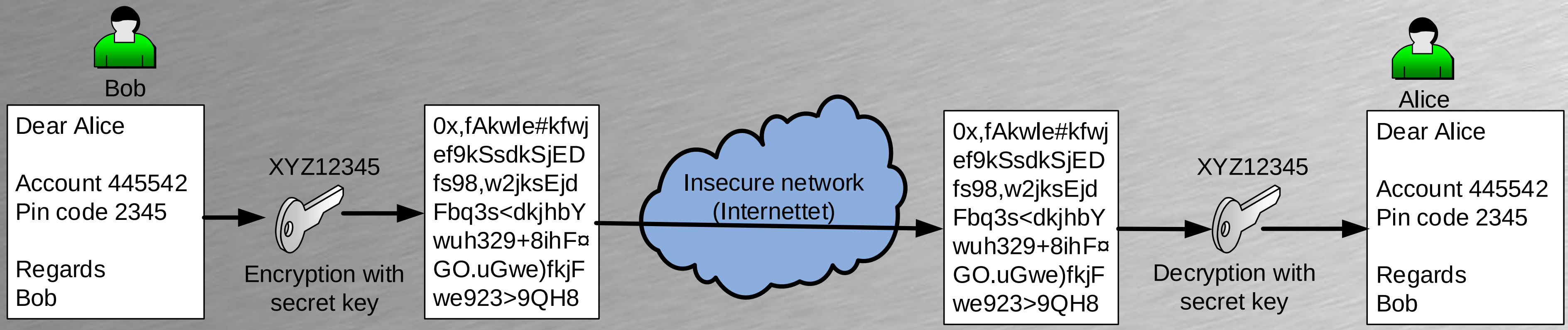
When G2 receives the packet from G1 it removes the outer packet and transmits the inner packet on the inside network interface to host 2



G1 receives the packet to 172.17.9.9/16 and packs the original packet from Host 1 into a new IP packet

Encryption

- encryption is the process of encoding messages in such a way that eavesdroppers or hackers cannot read it if intercepted.
- Authorized parties can decrypt and read it

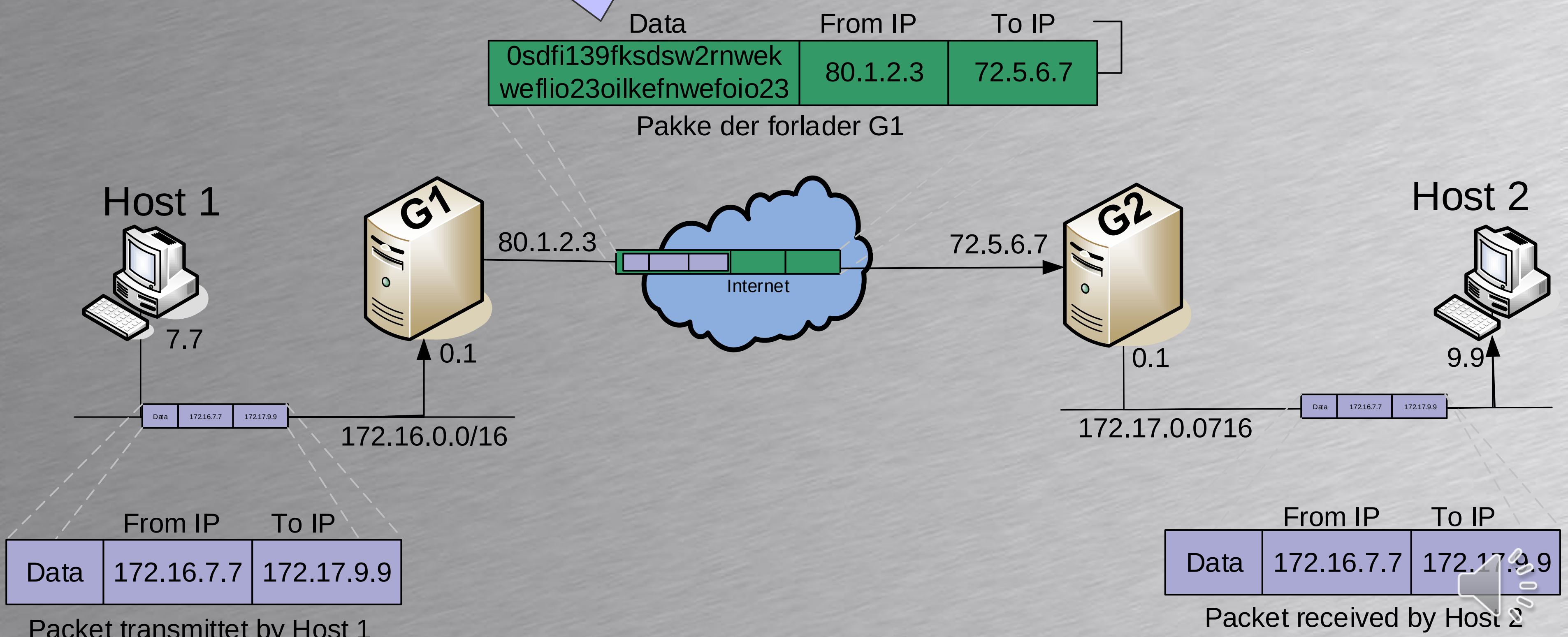


Encryption and tunneling

The inner packet is encrypted hiding
1. The identity of the transmitter
2. The identity of the receiver
3. The contents of the packet

•

• Note the in… is totally encrypted

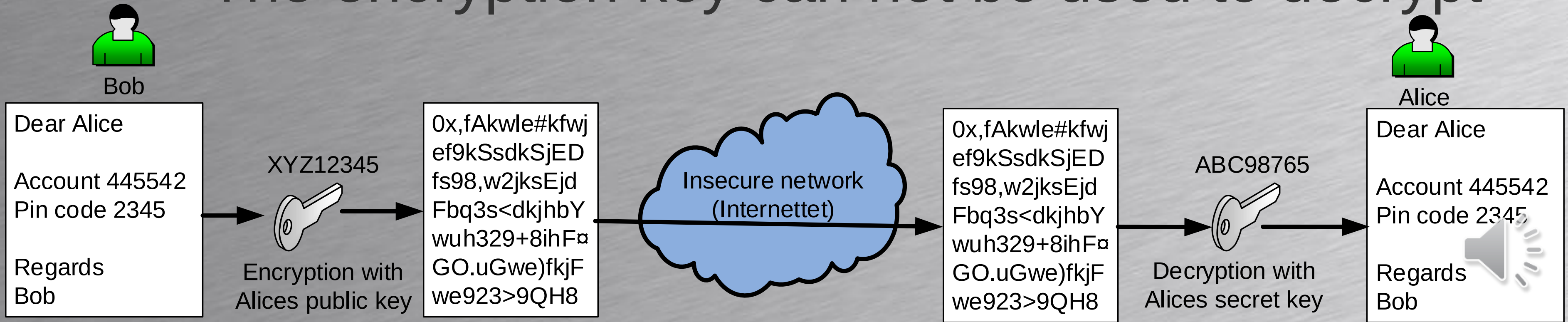


Encryption keys

- Symmetrical keys
  - Same key used for encryption and decryption
  - Exchange of symmetrical keys between parties difficult without risk of interception
- Asymmetrical keys
  - One key for encryption and another for decryption - called a key pair.
  - Encryption key can not be used to decrypt
  - Exchange of encryption key without risk

Asymetrical keys

- Alices computer generates a key pair
  - A public key: XYZ123345 (Used to encrypt)
  - A secret key: ABC98765 (Used to decrypt)
- Alice transmit her public key to Bob
- Bob uses Alices public key to encrypt
- If a hacker intercept the messages
  - The encryption key can not be used to decrypt



IPsec VPN

IP Security Architecture

- IPsec is end-to-end security system
  - Can be used between hosts and gateways
- IPsec offers
  - Confidentiality: Encryption
  - Authentication: Identity of parties
  - Integrity: Data not change in transit
  - Replay protection: Recorded packets can not be replayed
- IPsec can use tunneling

MPLS VPN

Multi Protocol Label Switching

MPLS VPN

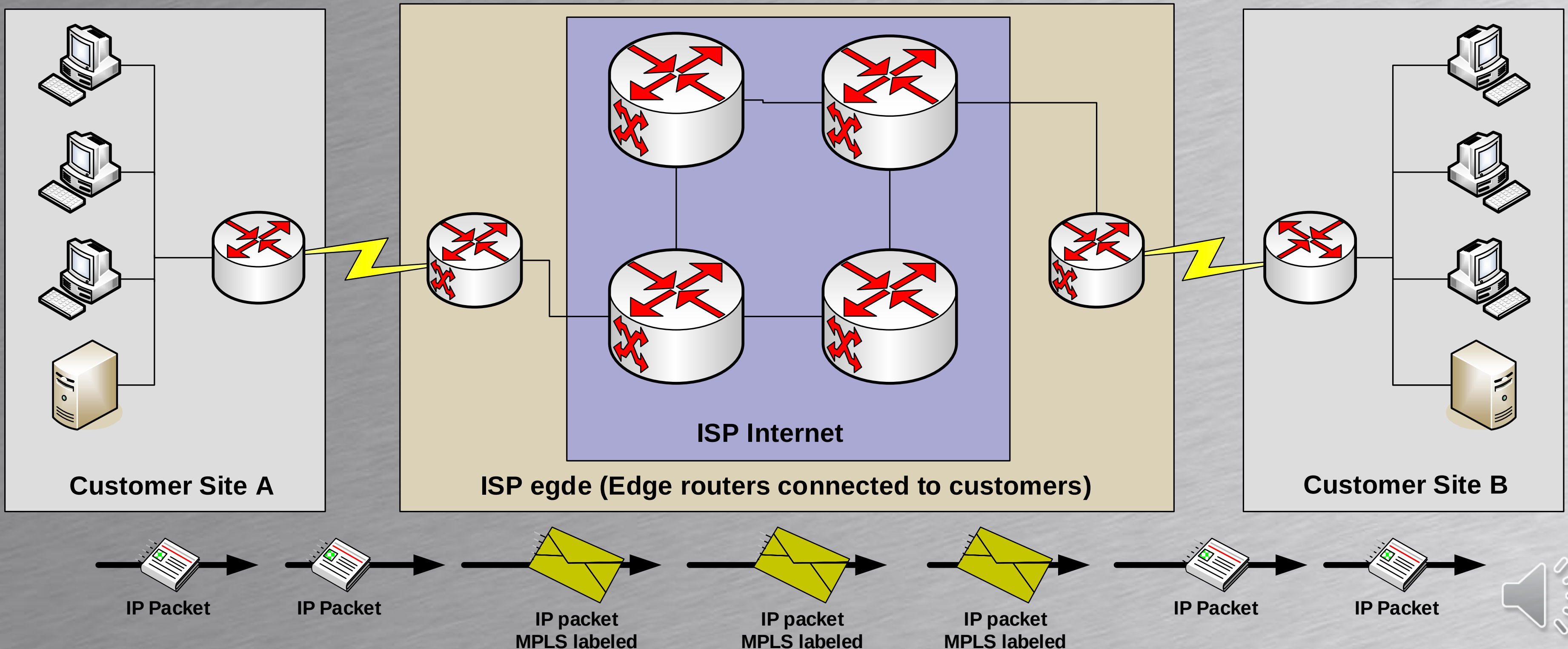
Multi Protocol Label Switching

- From a ISP's MPLS brochure
  - The customers locations are connected together in a closed private network
    - Transport via the Internet in a closed group
  - Internet access not possible through MPLS
  - Speeds from 512 Kbps to 1 Gbps
  - Existing customer IP address plan preserved
    - Normally private IP addresses are used by customers
      - 10.0.0.0/8
      - 172.16.0.0/12
      - 192.168.0.0/16

MPLS VPN

Multi Protocol Label Switching

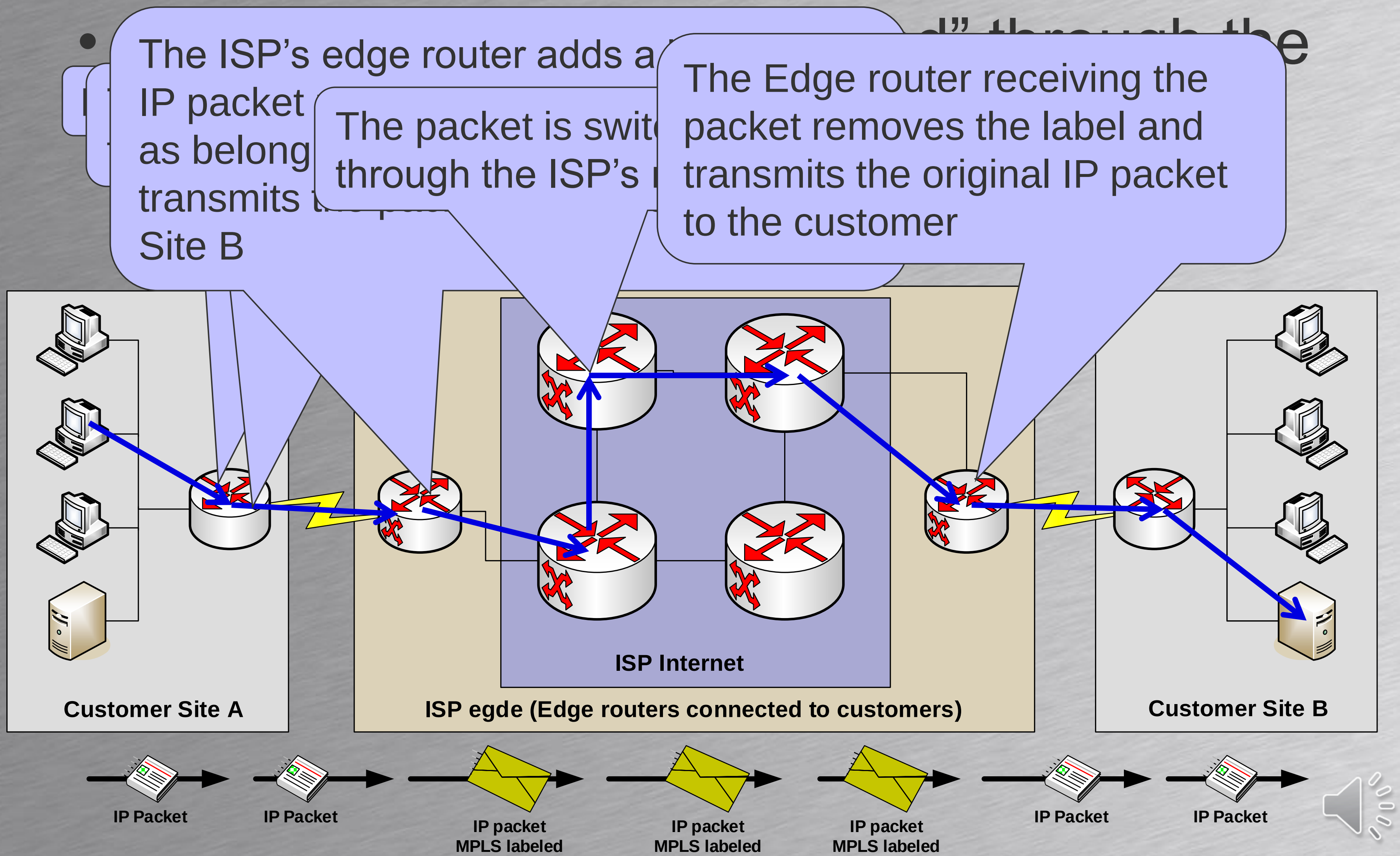
- When the ISP's routers transmit packets they use labels instead of IP addresses to forward packets inside the ISP's network



MPLS

Multi Protocol Label Switching

• d” through the



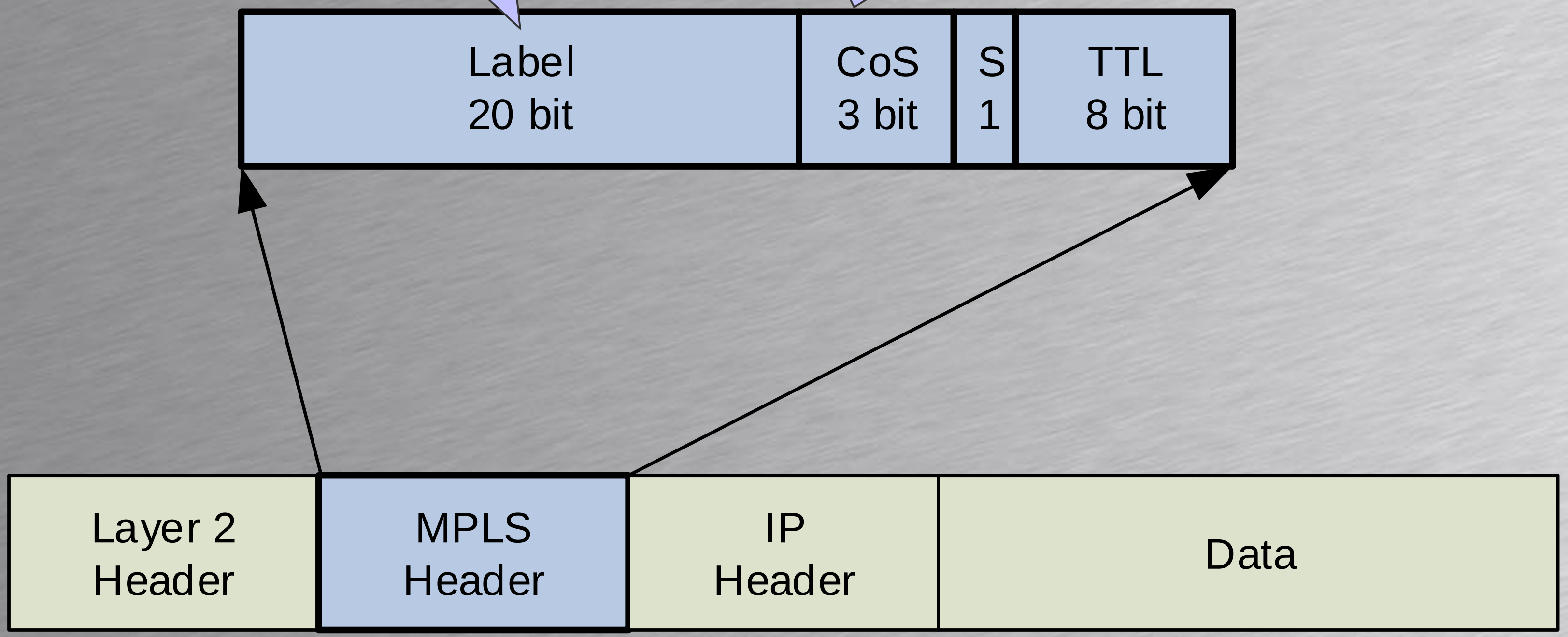
MPLS - Header

- Inde rnet ...)
- 4 and 3
  – Sc
- The label i entifies th estination

Ident
For e

CoS or Class of Service can be used for Quality of Service. Three bits giving eight levels of priorities.

0 = lowest priority
7 = highest priority



MPLS

Multi Protocol Label Switching

LSR1			
Label in	Port in	Port out	Label out
57	P1	P2	81

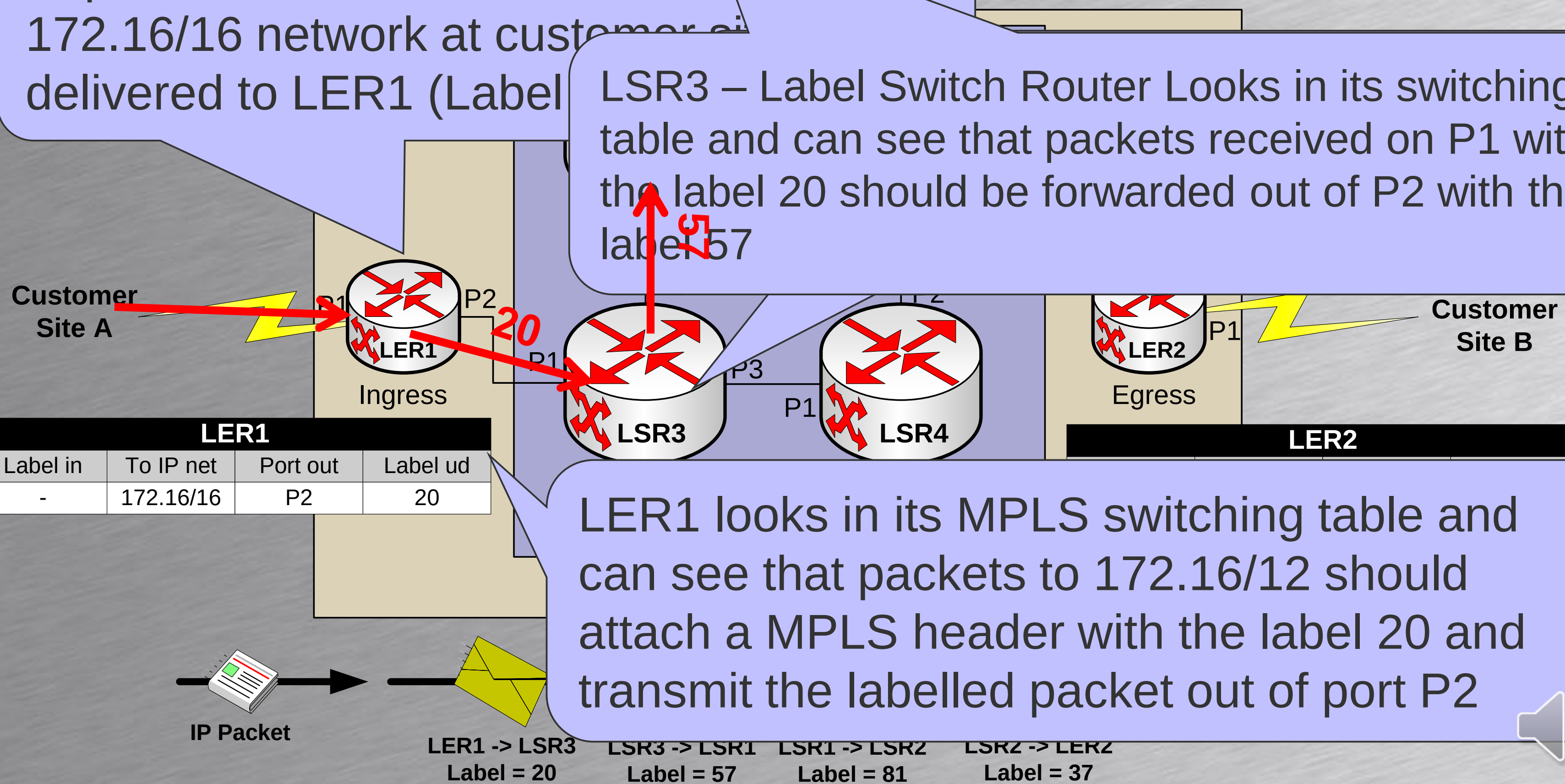
LSR2			
Label in	Port in	Port out	Label out
81	P1	P3	37

LSR3

LSR4			
	Port in	Port out	Label out

IP packet from customer site A to 172.16/16 network at customer si… delivered to LER1 (Label…

LSR3 – Label Switch Router Looks in its switching table and can see that packets received on P1 with the label 20 should be forwarded out of P2 with the label 57



LER1			
Label in	To IP net	Port out	Label ud
-	172.16/16	P2	20

LER2

LER1 looks in its MPLS switching table and can see that packets to 172.16/12 should attach a MPLS header with the label 20 and transmit the labelled packet out of port P2

MPLS

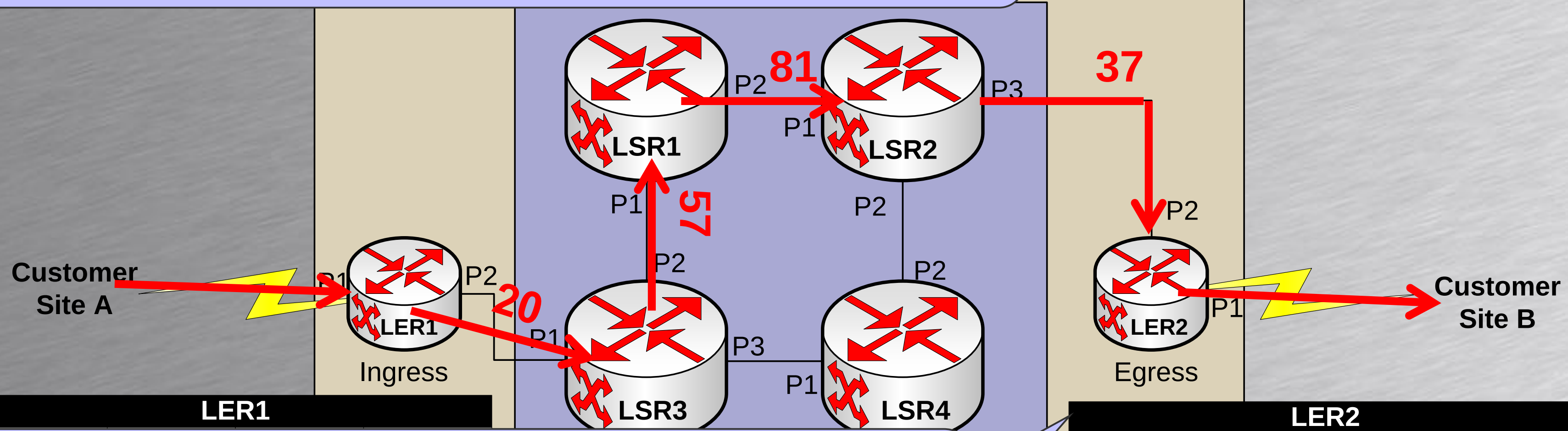
Multi Protocol Label Switching

LSR1			
Label in	Port in	Port out	Label out
57	P1	P2	81

LSR2			
Label in	Port in	Port out	Label out
81	P1	P3	37

label 57 on port P1 and
t of P2 with label 81

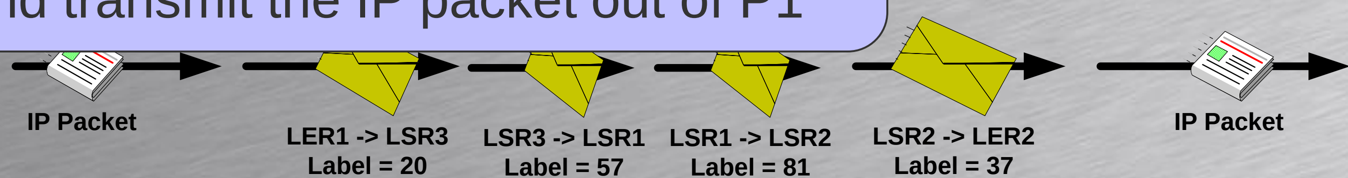
LSR2 receives label 81 on port P1 and forwards the packet out of P3 with label 37



LER1

LER2			
Label in	Port in	Port out	To IP net
37	P2	P1	172.16/16

LER2 receives label 37 on port P2 and can see in its switching table that it should remove the label and transmit the IP packet out of P1

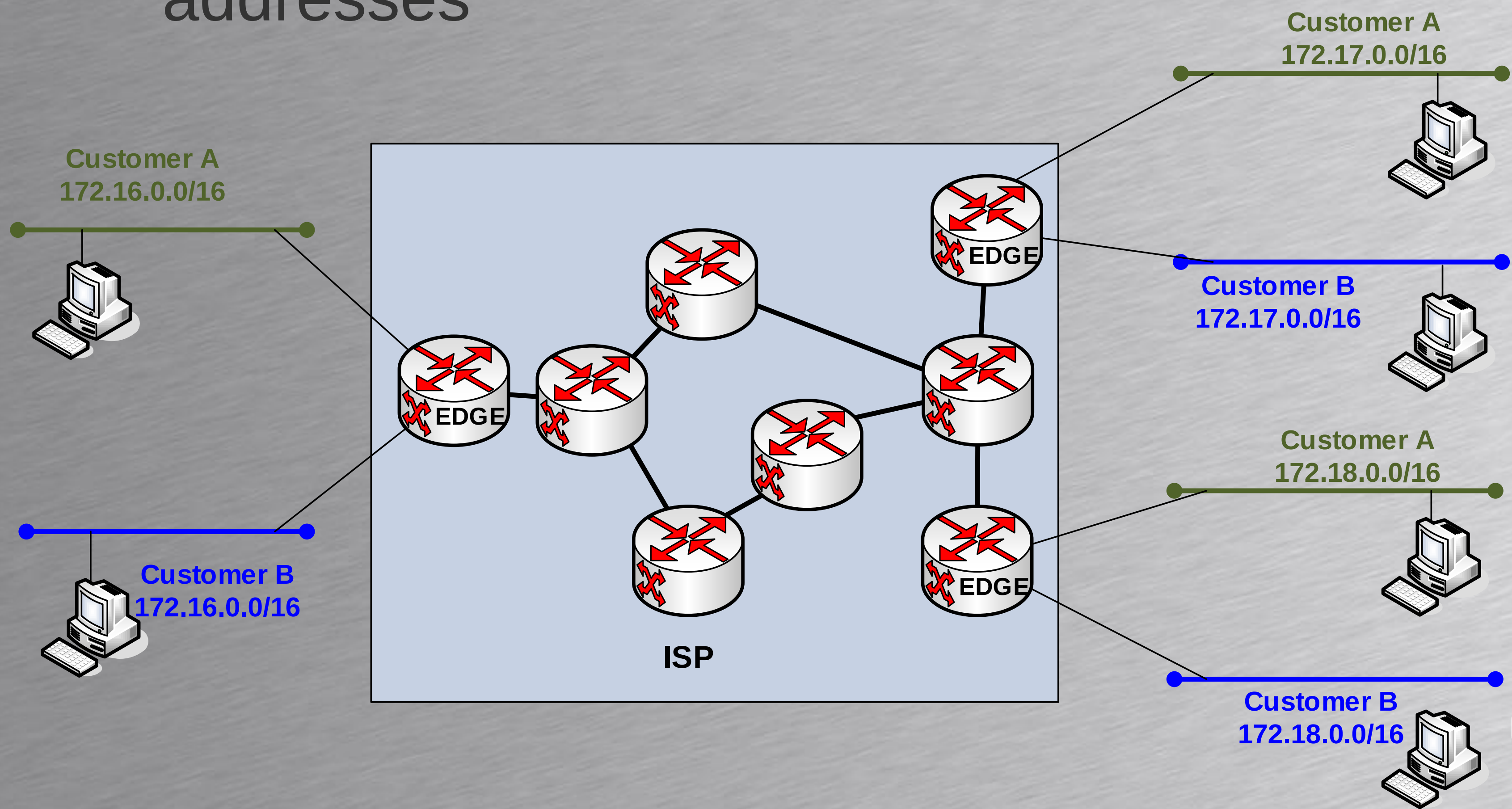


MPLS VPN

Multi Protocol Label Switching

HOUSE OF TECHNOLOGY
– en del af mercantec+

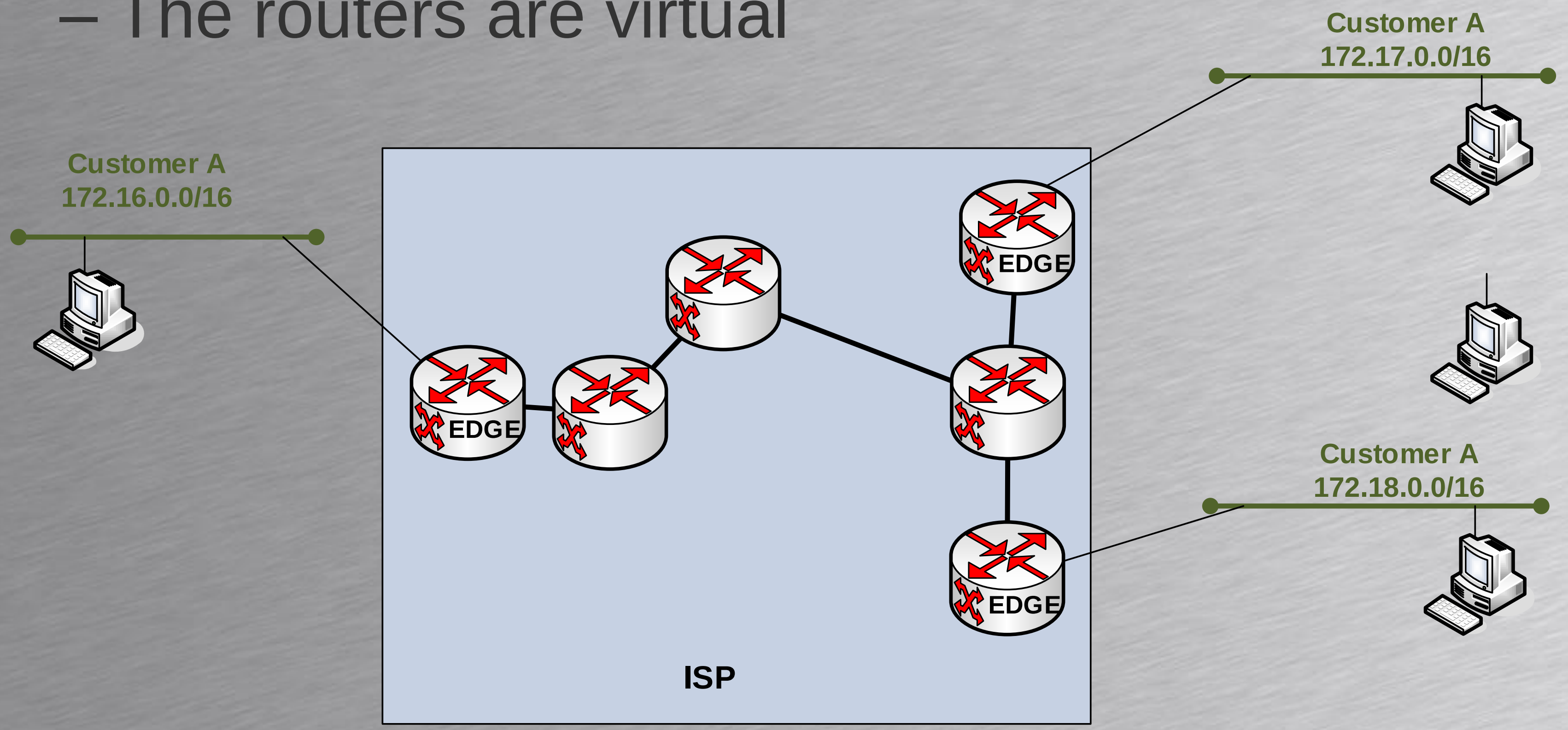
- Physical network as seen from the ISP
  - Both customers “accidently” uses same IP addresses



MPLS

Multi Protocol Label Switching

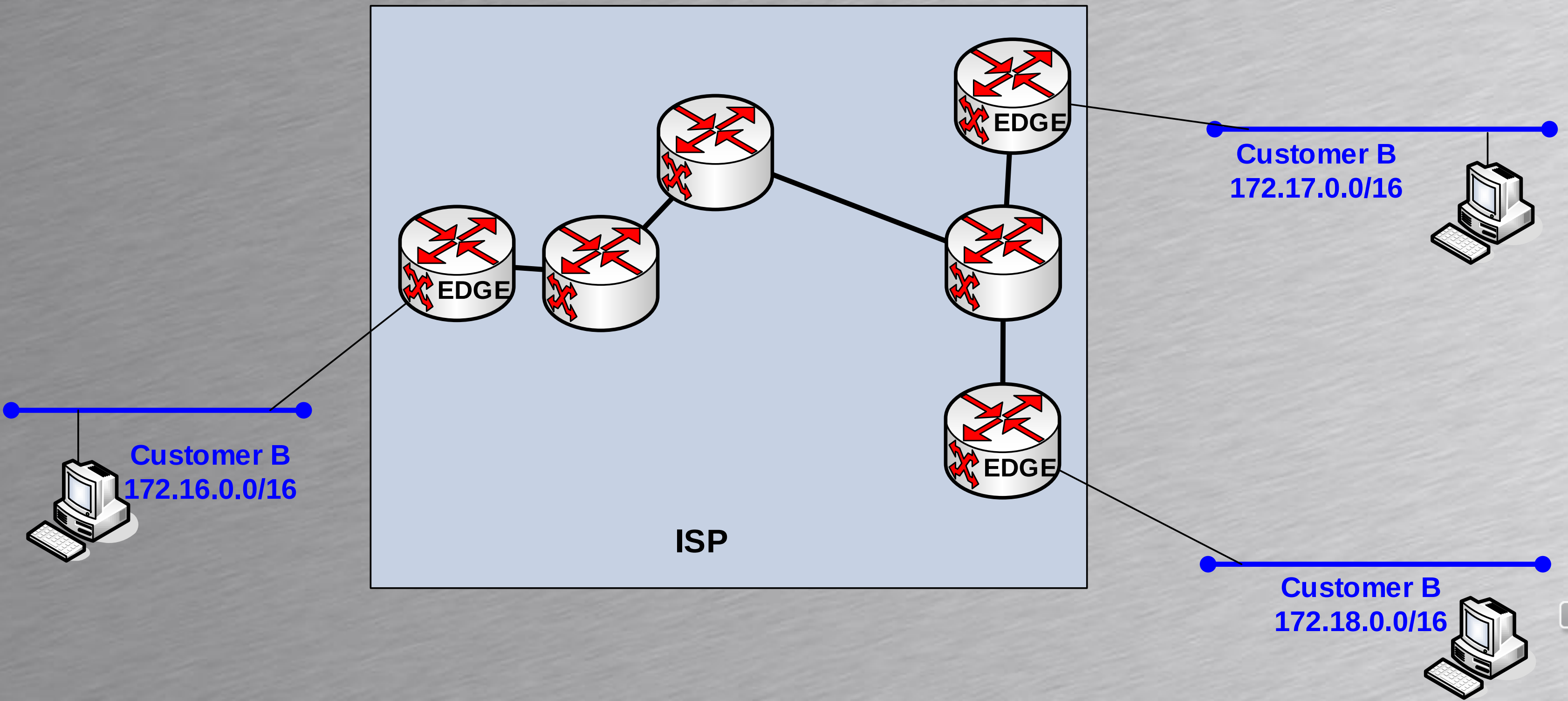
- Physical network as seen from Customer A
  - Customer A sees “his own network”
  - The routers are virtual



MPLS VPN

Multi Protocol Label Switching

- Physical network as seen from Customer B
  - Customer B sees "his own network"
  - The routers are virtual



MPLS VPN

Multi Protocol Label Switching

- MPLS VPN Conclusion
  - Existing IP network used for closed networks
    - Cheap in investment
  - MPLS VPN offers no encryption
    - Encryption/decryption in CPE equipment
      - Customer Placed Equipment
  - MPLS is a layer 3 (routed) private network
  - MPLS is easy to expand
  - QoS is an additional service offered by ISP’s
  - Many ISP’s work together offering MPLS network in large geographically areas (world)

VPLS

Virtual Private Lan Service

- VPLS is another VPN type using MPLS technology
- MPLS VPN is a routed VPN (OSI layer 3)
  - Each customer site having different IP networks
  - Virtual Routers
- VPLS VPN is switched VPN (OSI layer 2)
  - Each customer site have different MAC addresses

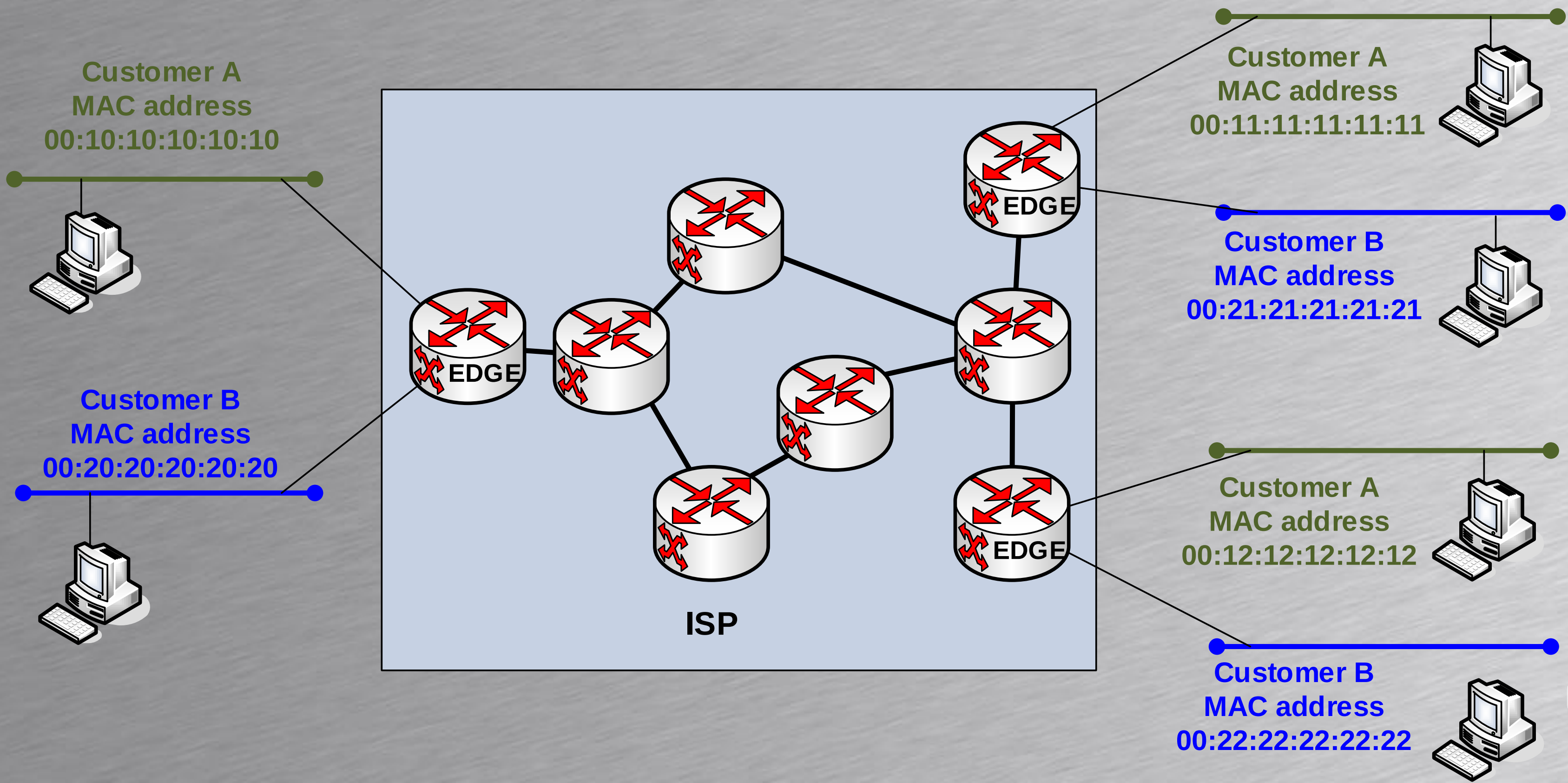
VPLS

Virtual Private Lan Service

- VPLS is another VPN type using MPLS technology
- MPLS VPN is a routed VPN (OSI layer 3)
  - Each customer site having different IP networks
  - Virtual Routers
- VPLS VPN is switched VPN (OSI layer 2)
  - Each customer site have different MAC addresses

VPLS
Virtual Private Lan Service

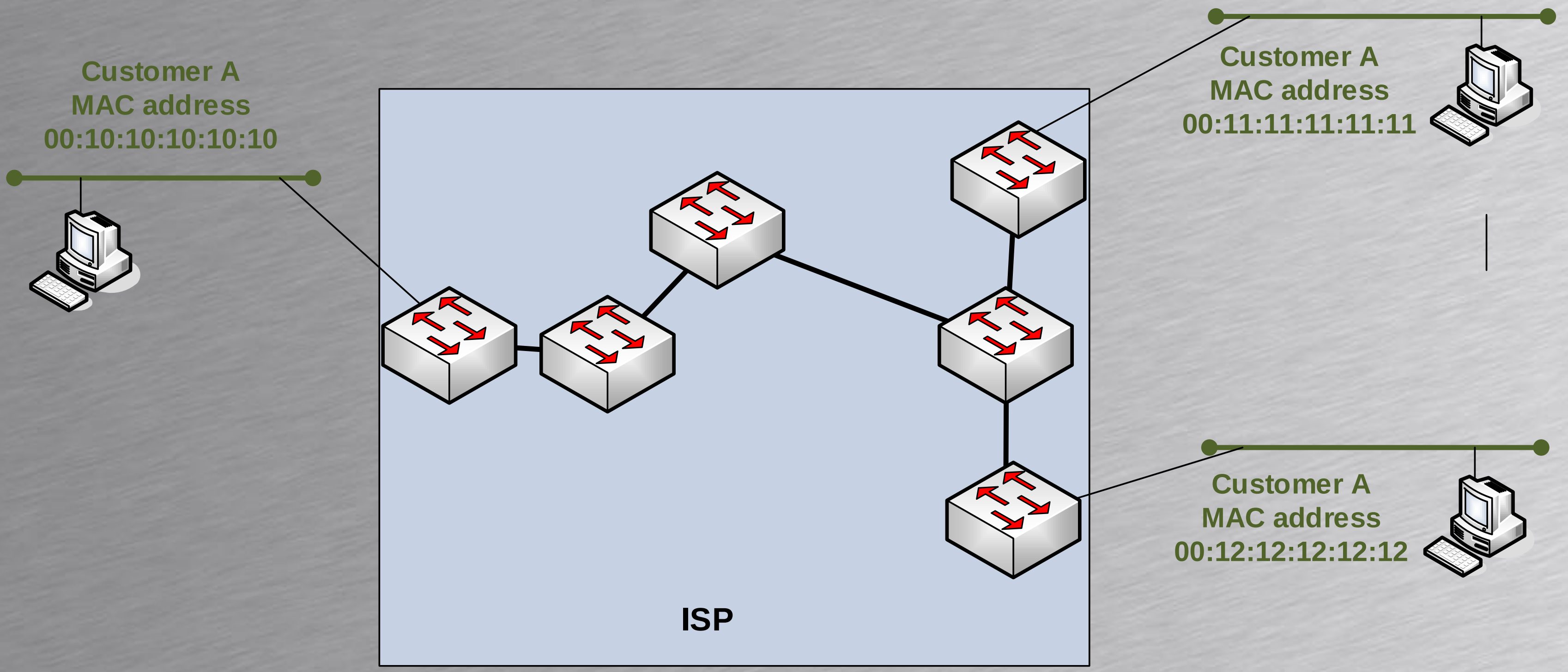
- Physical network as seen from the ISP



VPLS

Virtual Private Lan Service

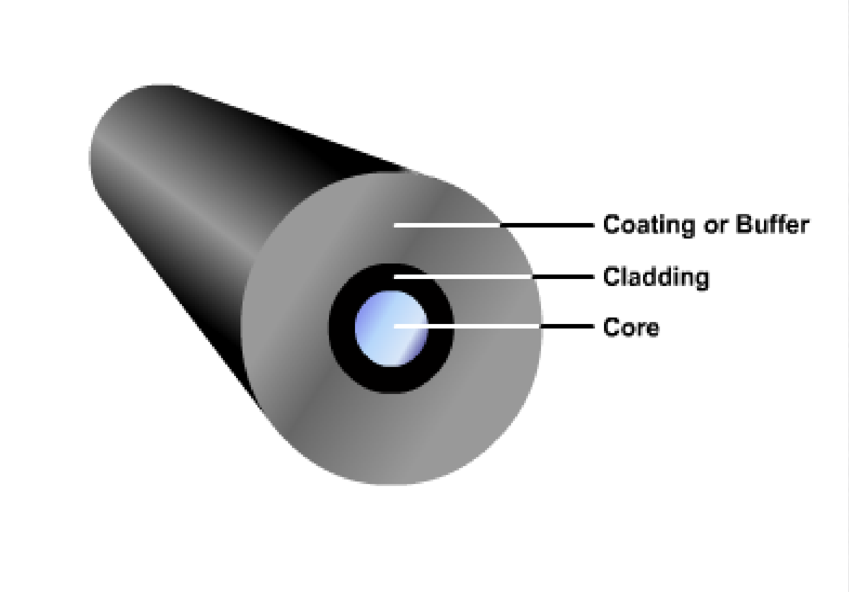
- Physical network as seen from Customer A
  - Switching between remote sites



OPTICAL MEDIAS

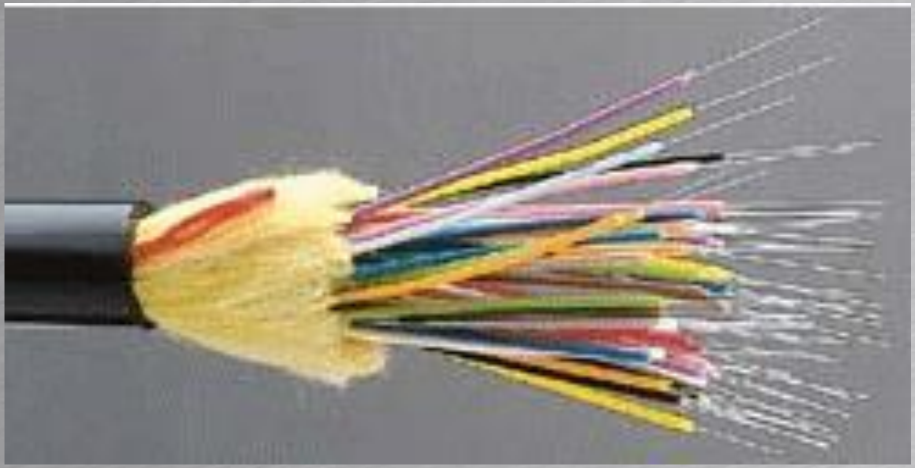
Fiber optical cable

- Consists of a inner core of glass or plastic
- The core is surrounded by another layer of glass called cladding
- Protected by one or more layers of coating



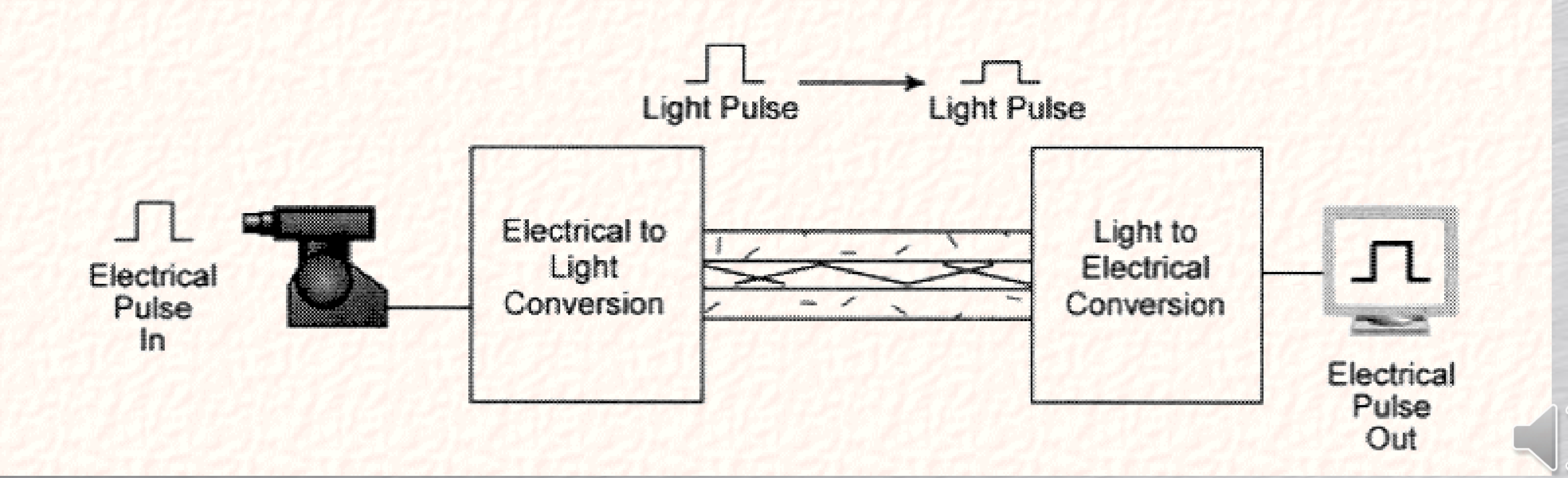
Fiber optical cable

- A fiber optical cable typically consists of multiple separate fibers
  - 2,4,8,12,24,48 eller 96 separate fibre.
- It is expensive to install fibers between buildings and cities
- Unused fibers are called “dark fiber” and can be leased/used later



Transmissions principle

- A laser is used to produce light pulses send through the fiber
- A photo diode is used to convert the light pulses to electrical pulses at the receiver

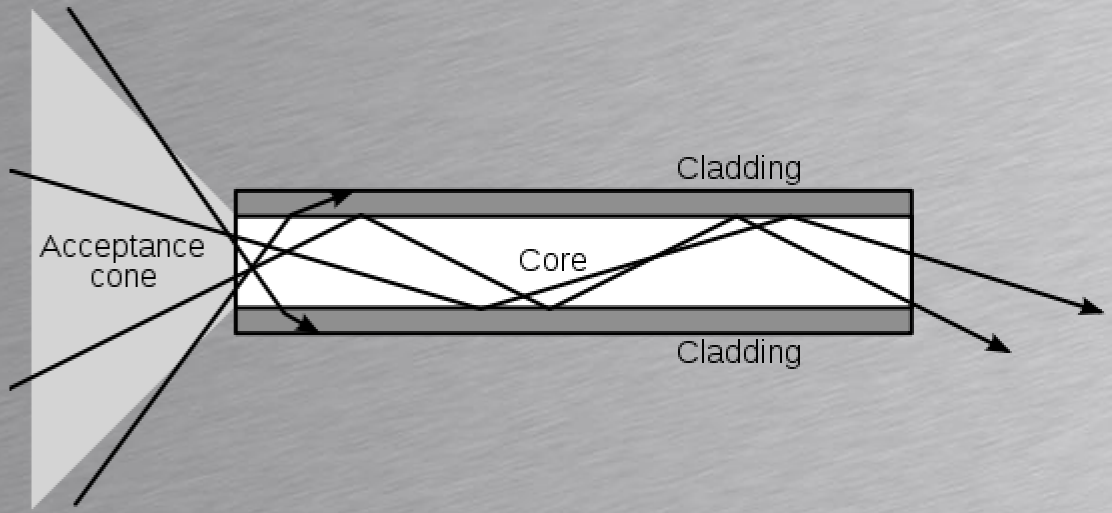


Laser energy

- High energy lasers are used in long distance fibers…
- At long distances ~> 80 Km repeaters are installed

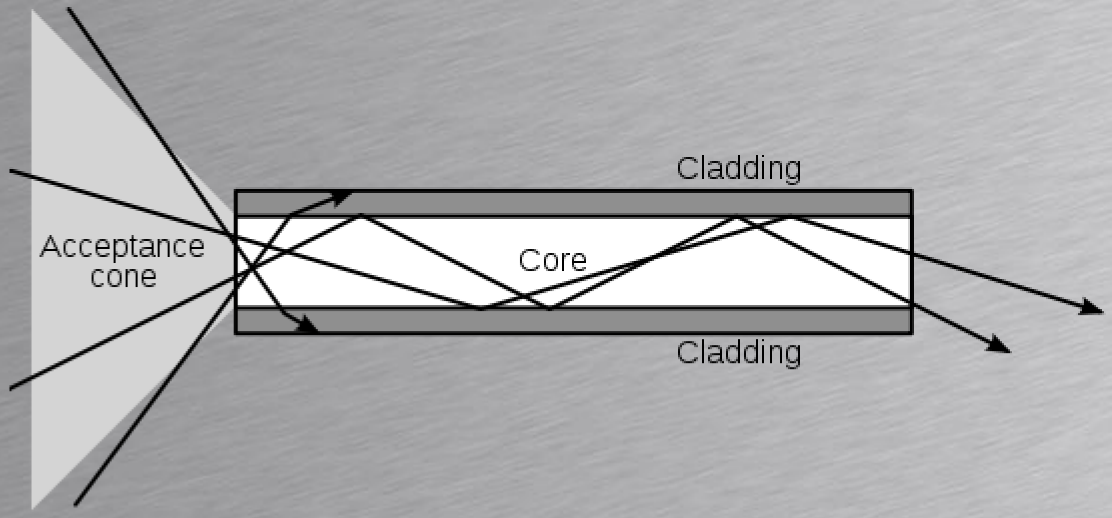
Multimode fiber

- In a multimode fiber the light beam is reflected throgh the cable.
  - The layer between the core and cladding acting as a mirror
- High loss of energy – used for short hauls



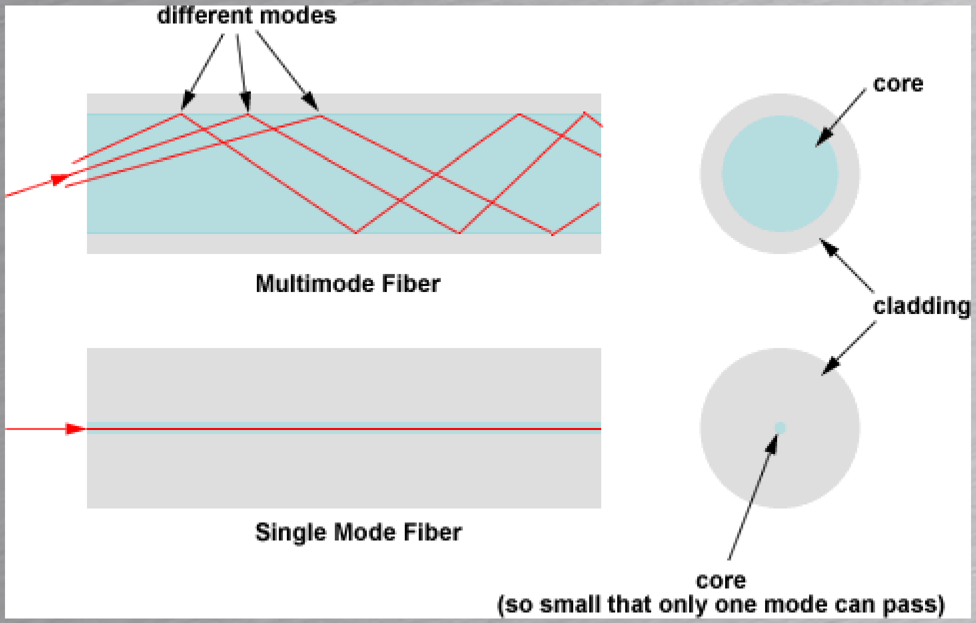
Multimode fiber

- High loss of energy – used for short hauls
- Cheap and easy to use
- Often used inside buildings
  - Up to 1 Km



Singlemode fiber

- In a singlemode fiber the light beam is directed throgh the cable.
- Low loss of energy – used for long hauls
  - Used between buildings, cities and countries




Greenland
USA
Reykjavik
Thorshavn
Tromsoe
Trondheim
Østersund
Umeå
Uleåborg
Jyväskylä
Bergen
Tammerfors
Russia
Oslo
Örebro
Helsinki
Tallinn
China
Stockholm
Kristiansand
Gothenburg
Riga
Copenhagen
Malmö
Vilnius
Hamborg
Amsterdam
London
Bruxelles
Frankfurt
Paris

MAN

Metropolitan Area Network

ascom

MAN

Metropolitan Area Networks

HOUSE OF TECHNOLOGY

– en del af mercantec+

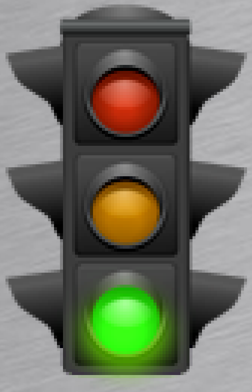
- MAN's are used in highly populated areas
  - – Typically cities and campus areas
- Privately or ISP owned
  - – Privately – big companies, universities…
  - – ISP – Lease bandwidth to local organizations

ascom

HOUSE OF TECHNOLOGY

– en del af mercantec+

QoS INTRODUCTION



Quality of Service

IP standard service

- IP designed for best-effort services
  - No delay or bandwidth guaranty
- IP designed for
  - Complex endpoints for example TCP
    - Realigns packets out of sequence
    - Retransmits lost packets
  - Simple network routing
    - No bandwidth guaranty
    - No delay guaranty

Traffic classes

- Different kind of traffic gets same service using IP best-effort
  – Ordinary data (Transaction oriented)
    - WWW, FTP, database transactions ….
  – IP Telephony (VoIP)
    - RTP, SIP, H.323 …..
  – On-line based (Character oriented)
    - Telnet, SSH, Citrix (Terminal services) …

Traffic classes

	VoIP	Video	Transaction	Character
Typical bandwidth	40-90 Kbps	90-300 Kbps	0 - maximum Greedy	5-25 Kbps
Data flow	Constant	Variable	Very Variable	Variable
Delay demand	Very little < 150 ms	Very little < 150 ms	Not sensitive < 1 sec	Little < 200-300 ms
Jitter	Very sensitive < 30 ms	Very sensitive < 30 ms	Not sensitive	A little sensitive
Packet loss	Sensitive UDP	Sensitive UDP	Not sensitive TCP	A little sensitive TCP

QoS approaches

- Problems with Quality of service?

- Approach 1:
  - Add more bandwidth

- Problems with the – add more bandwidth
  - Expensive – and still best-effort
  - No bandwidth or delay guaranty when network or devices are congested

What is QoS

- Split the traffic in traffic-classes
  - VoIP, WWW, mail …
  - Treat each class of traffic based on a agreed QoS policy
- The purpose of QoS
  - Guaranty a minimum bandwidth for a class
  - Guaranty a maximum delay for a class
- QoS do not dreate more bandwidth – but
  - Controls the bandwidth using it efficient

QoS

- Some traffic classes get a higher priority than other

You could say:

- **– QoS is planned unfairness for some classes**

ascom

HOUSE OF TECHNOLOGY

- en del af mercantec

Where are the problems

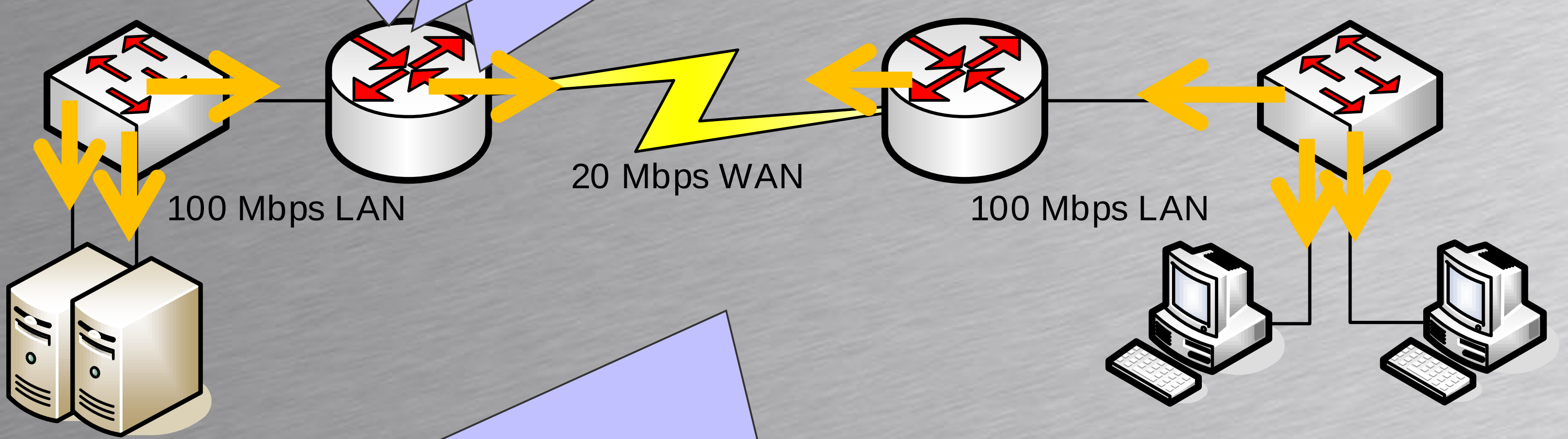
- When designing/configuring QoS you look

The router can receive up to 100 Mbps on its LAN interface, but can only tr

The route

outgoing d evice

The router needs to be configured to classify the packets and select which packets must the transmitted and drop the less interesting packets



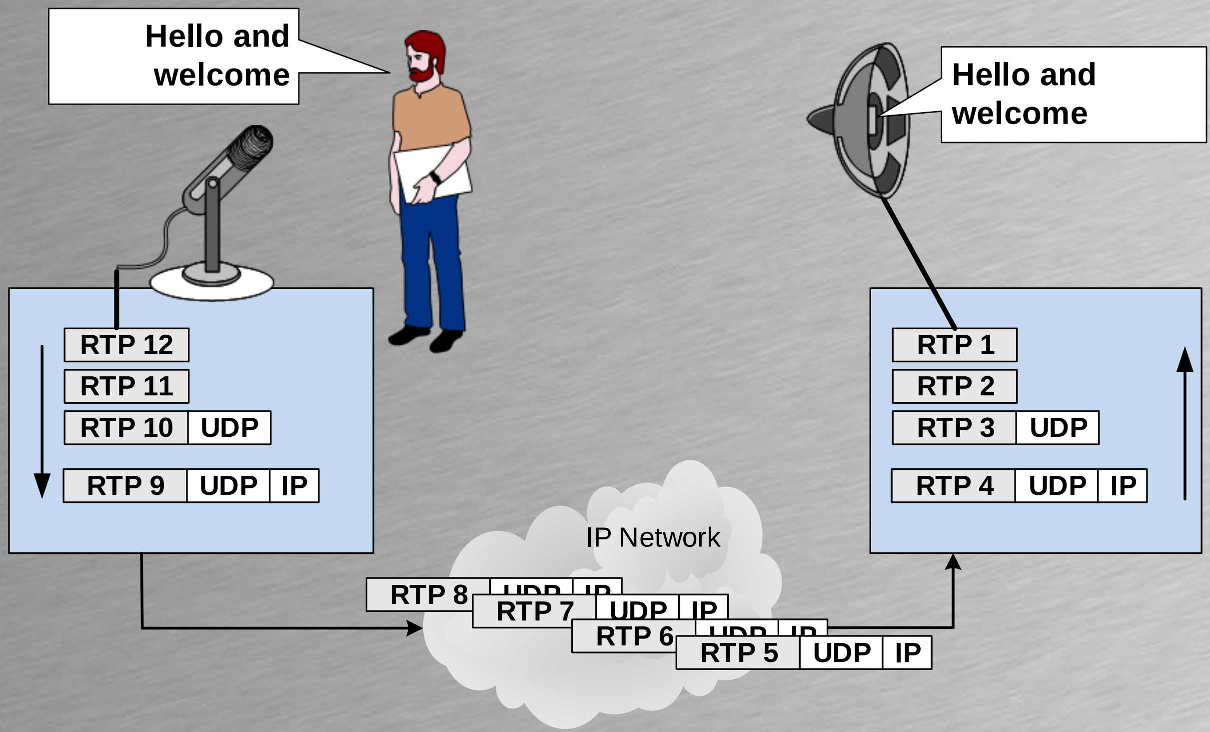
Possible congestion points in this network are?

QoS definition

- QoS is a given networks ability to deliver
  - A given quality of delivery of packets
    - A maximum packet loss
    - A maximum delay
    - Maximum jitter
  - High availability
    - For example 99,995 % (< 26 minuttes a year)

VoIP Delay/latency

- VoIP defines delay as
  - The time spent from the voice leaves the mouth of the talker – until it reaches the ear of the listener



VoIP delay/latency

- **Packetization delay**
  - The time it takes to assemble the packet in the phone. Including sampling and encoding
- **Serialization delay**
  - The time it takes to send the packet bit-by-bit
  - Each device between the phones add delay
- **Propagation delay**
  - The time it takes for the information to travel through the media. (Electrical/optical)
- **Switching/queing delays**
  - The time routers and switches use to queue and process the packets in transit

Types of QoS

- DiffServ (Differentiated Services)
  - Split the traffic into classes according to a policy
  - Each router/switch must be configured to obey policy
  - Does not guaranty real QoS, but demands administrative control of traffic flows and classes
- IntServ (Integrated Services)
  - Devices reserve bandwidth and delay guaranty from all devices between end-devices
  - Uses the reservation protocol RSVP
  - Not used much – and not a part of this course

ascom

HOUSE OF TECHNOLOGY

– en del af mercantec+

CAC

Call Admission Control

CAC

Call Admission Control

- A G.711 A-law with 50 packets pr. Second – or PPS – use a bandwidth of 80 Kbps without OSI layer 2 heading
  - Rule of thumb: 100 Kbps in each direction for each active call
- 10 calls = 1 Mbps and 20 calls = 2 Mbps
  - To ensure good voice quality a QoS policy guarantying 2 Mbps of RTP traffic would give good voice quality for up to 20 simultaneous calls

CAC

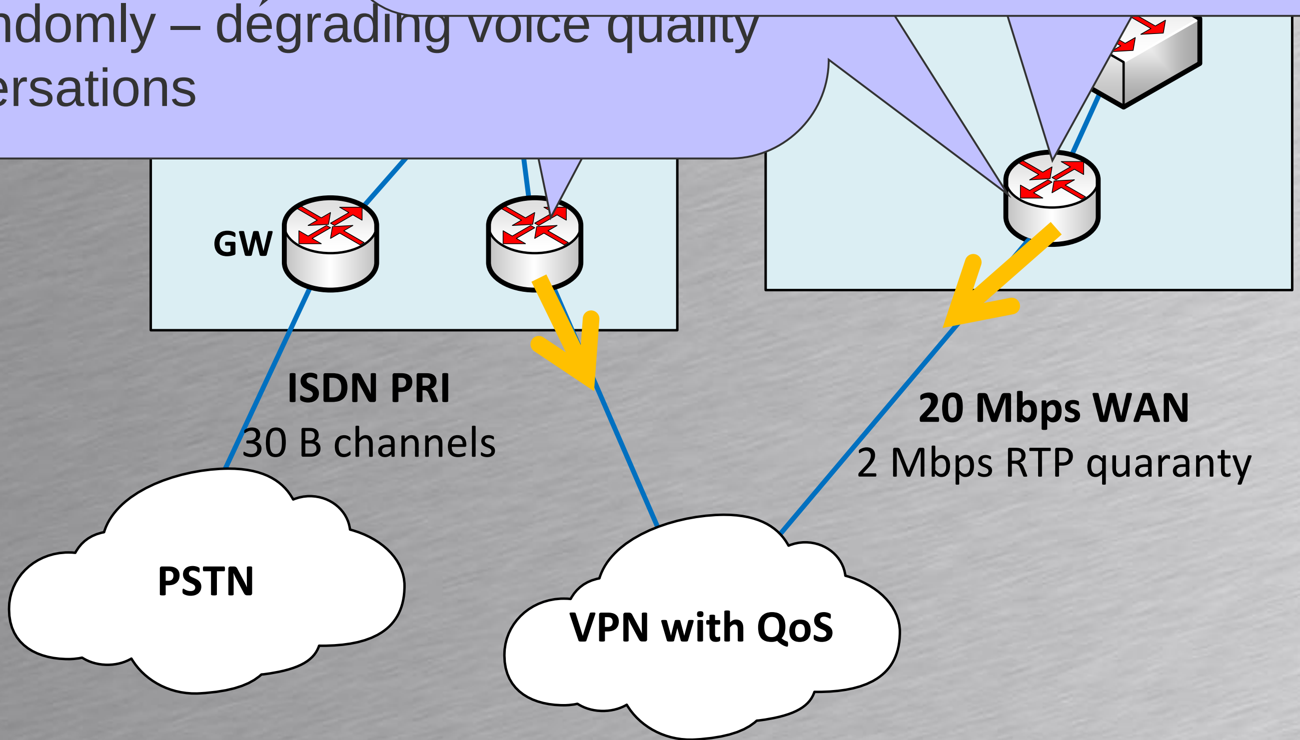
Call Admission Control

If more than 20 users calls
all traffic exceeding 2 Mbp
downgraded to “normal” tr
guaranty

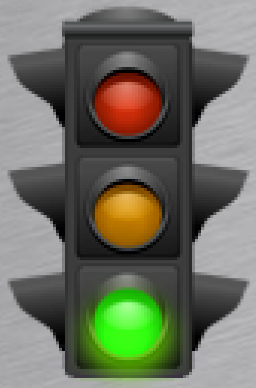
RTP packets exceeding 2
dropped randomly – degrading voice quality
off all conversations

IP-PBX must be configured to accept call requests from up to 20 phones from Branch A. Rejecting further requests. This is called CAC.

Call Admission Control prevents oversubscription



QoS MARKING



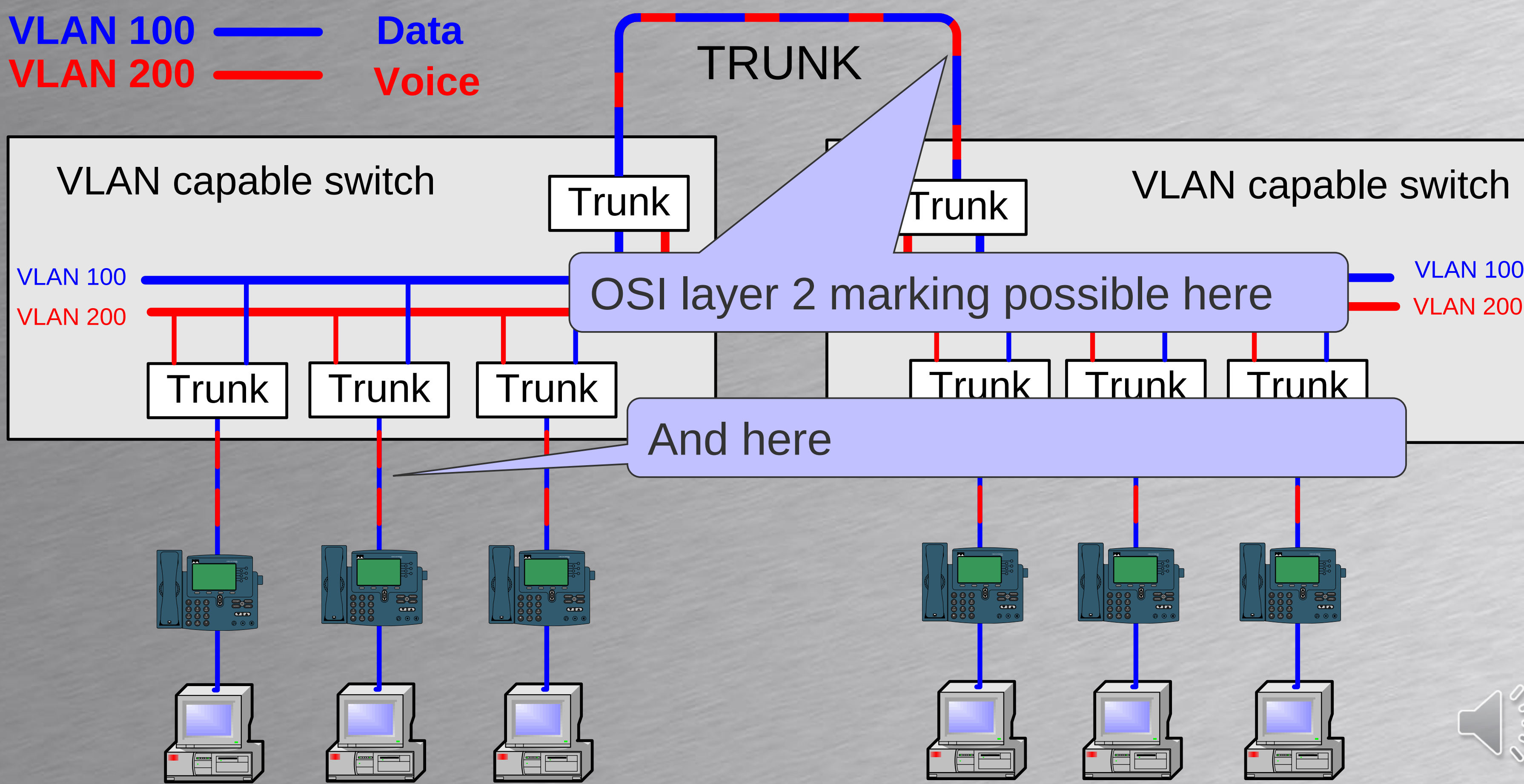
OSI layer 2 and layer 3 marking

QoS marking

- Each packet will have its own QoS marking notifying routers and switches of its importance or lack of importance
- Packet can be marked in
  - OSI layer 2 – the Data Link layer
    - When Ethernet is used marking are done in VLAN trunks (IEEE 802.1Q/p)
  - OSI layer 3 – The Network layer
    - The IP protocol have a specific field for QoS

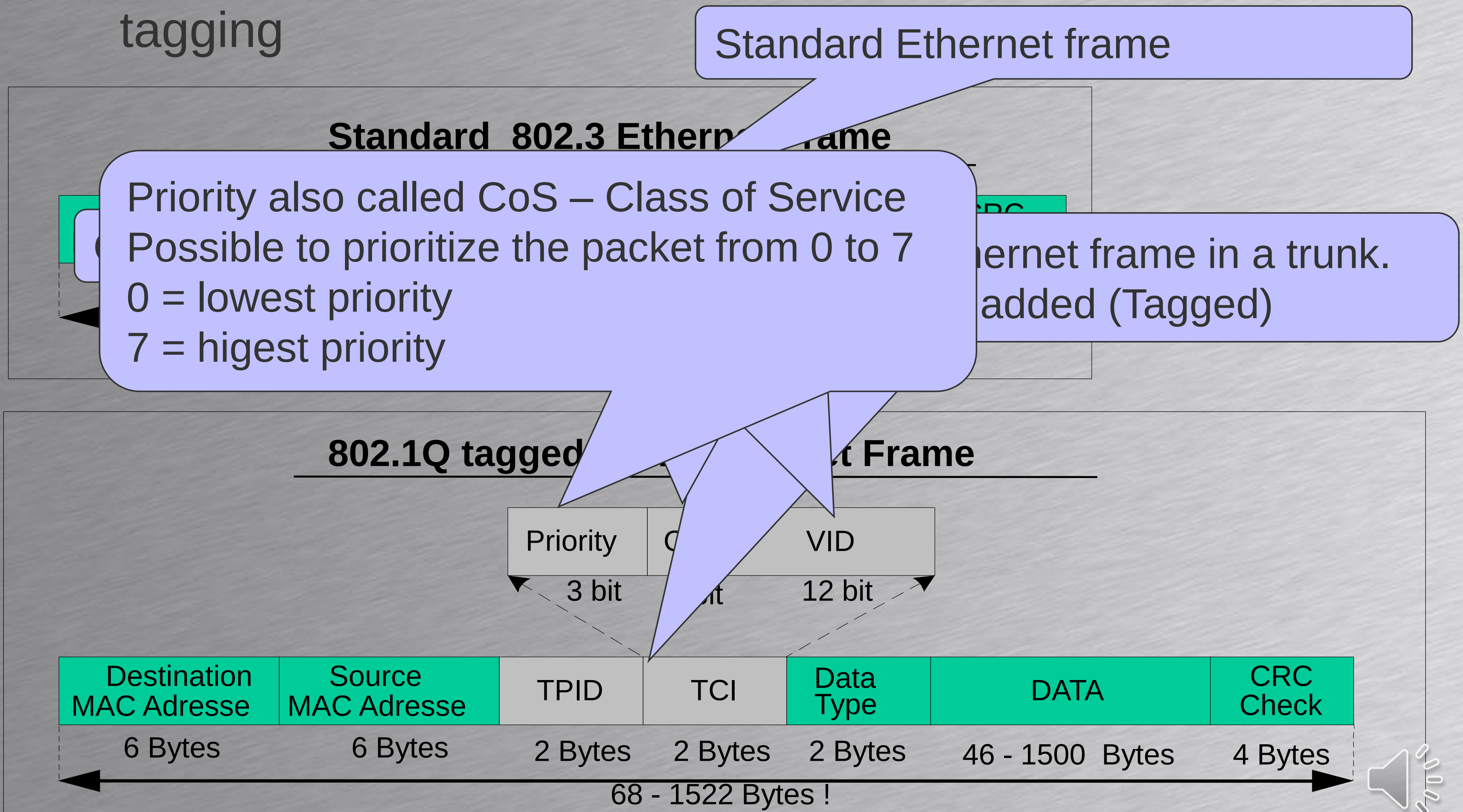
OSI layer 2 marking

- Marking in trunks between switches and between phone and switches when Voice VLAN deployed



OSI layer 2 marking

- In trunks Ethernet frames are tagged using 802.1Q tagging



OSI layer 2 marking

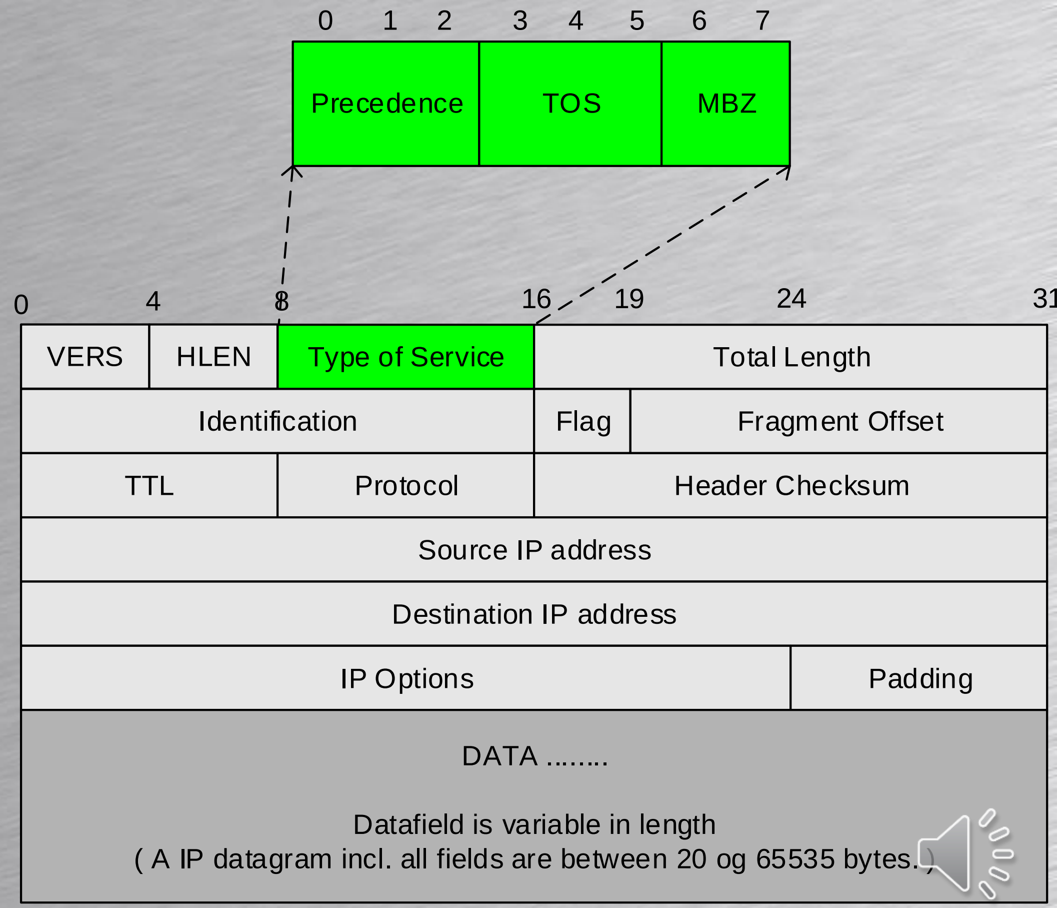
- Typical use of Class of Service – CoS

Layer 2 Class of Service	Typical trafic class
CoS 0 (000 binary)	Background
CoS 1 (001 binary)	Best effort
CoS 2 (010 binary)	Fri
CoS 3 (011 binary)	Business critical / VoIP signaling
CoS 4 (100 binary)	Streaming multimedia
CoS 5 (101 binary)	Voice (RTP)
CoS 6 (110 binary)	Internetwork control
CoS 7 (111 binary)	Network control

Layer 3 marking

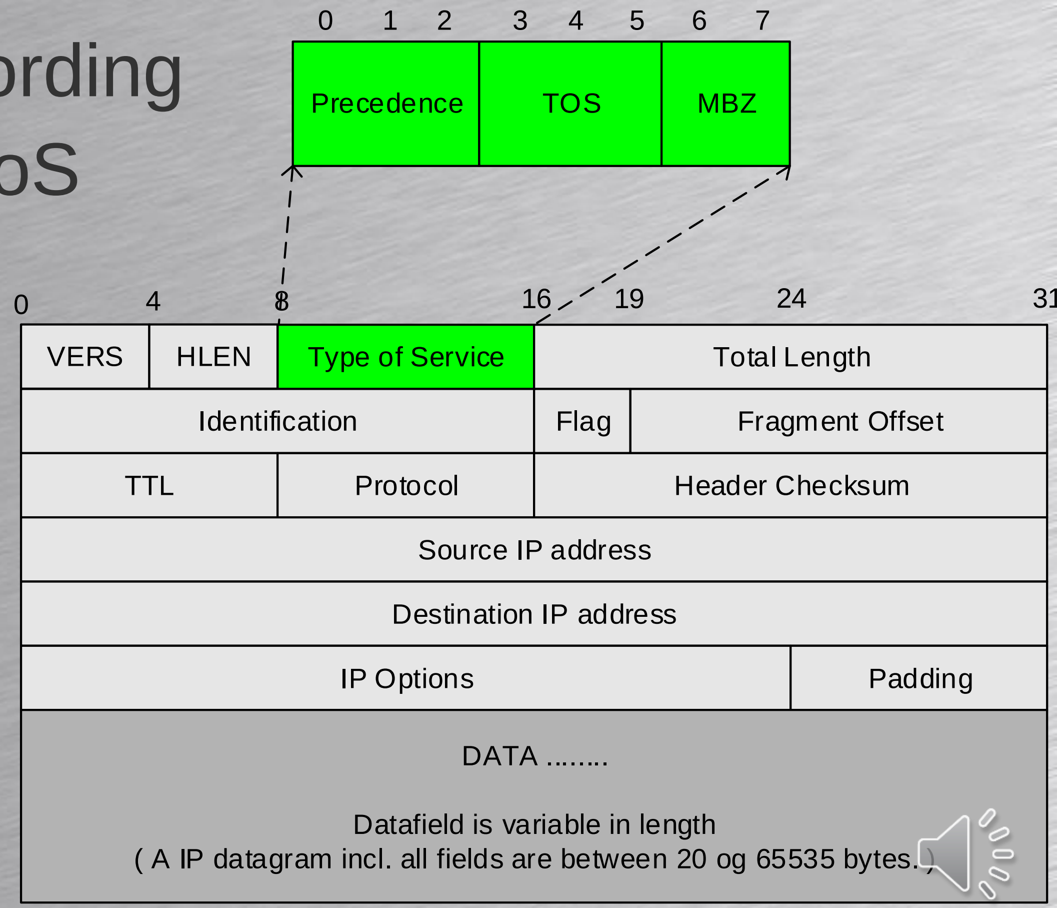
IPv4 packet

- Type of service contains three subfields
  - Precedence
    - 3 Bits describing the packets priority in the network.
    - 0 = low ; 7 = high
  - TOS: Type Of Service
    - **000: Normal service**
    - **100: Minimum delay**
    - **010: High throughoutput**
    - **001: High reliability**
    - **Can be combined**
  - MBZ: Not used
    - Must Be Zero



IPv4 packet

- Each packet will have its QoS profile marked in these bits.
- Routers and switches must treat each packet according to its marking when QoS is configured



IP ToS and DiffServ

- The original IP ToS field was described in RFC 791 in 1981 by Jon Postel
- The IPv4 packet unchanged since !
- Except the ToS field was revised in 1998 in RFC 2474 to align with QoS in IPv6
  - Now the field is called
    - Differentiated Services Field - DS

      Or

    - Differentiated Services Code Point - DSCP

IP ToS to IP DiffServ

- Backward compability from ToS to DiffServ
  - Just annoying we need to learn both ☺

ToS

Precedens (3 bit)			Type of Service (3 bit)			Not used (2 bit)
			D	T	R	

↓ ↓ ↓

DiffServ

Class Selector Codepoint (3 bit)			Drop Preference (3 bit)			Not used (2 bit)

IP ToS to IP DiffServ

	Class 0	Class 1	Class 2	Class 3	Class 4	Class 5	Class 6	Class 7
Class Selector	**000000**	**001000**	**010000**	**011000**	**100000**	**101000**	**110000**	**111000** (CS7) **…ork …ag**
Assured Forwardi… Low Drop Precede…								
Assured Forwardi… Medium Drop Precedence								
Assured Forwarding High Drop Precedence								
Expedited Forwarding						(EF) **IP voice**		

If a router or switch experience congestion it will start to drop packets in configured classes.

Within each class it will drop packets according to drop preference.

High drop preference = high probability the packet is dropped

Cl…

…

Cl…

be allocated to differe… …ences

$00_2 = 0$ = lowest drop preference

…

$11_2 = 3$ = highest drop preference

DiffServ and VoIP

	Class 0	Class 1	Class 2	Class 3	Class 4	Class 5	Class 6	Class 7
Class Selector	**000000** (CS0) **Best Effort**	**001000** (CS1)	**010000** (CS2)	**011000** (CS3)	**100000** (CS4) **Stream video**	**101000** (CS5)	**110000** (CS6) **IP routing**	**111000** (CS7) **network Manag**
Expedited Forwarding						**101110** (EF) **IP voice**		

101110 or EF – Expedited forwarding – is de facto standard for RTP packets. (Voice packets)

These packets needs guarantied bandwidth, minimum delay and jitter.

Routers and switches must act accordingly

selector 3 drop preference 1

IP ToS to IP DiffServ

	Class 0	Class 1	Class 2	Class 3	Class 4	Class 5	Class 6	Class 7
Class Selector	000000 (CS0) **Best Effort Data**	001000 (CS1)	010000 (CS2)	011000 (CS3)	100000 (CS4) **Stream video**	101000 (CS5)	110000 (CS6) **IP routing**	111000 (CS7) **network Manag**
Assured Forwarding Low Drop Precedence		001010 (AF11)	010010 (AF21)	011010 (AF31) **VoIP signaling**	100010 (AF41) **Video**			
Assured Forwarding Medium Drop Preced		001100 (AF12)	010100 (AF22)	011100 (AF32)	100100 (AF42)			
Assure Forwar High Drop Precedence								
Expedited Forwarding						101110 (EF) **IP voice**		

Class selector 3 and drop preference 1 often used for VoIP signalling (SIP, H.323) also called

Cisco QoS baseline

Traffic class	PHB	DSCP	TOS
IP Routing	CS6	48 – (110000)	192
Voice	**EF**	**46 – (101110)**	**184**
Interac		)	136
Strea		)	128
Miss			104
Call			
Tran			
Netw			
Bulk			40
Scav			32
Best			0

EXAMPLE:

TOS 184 = DSCP 46

TOS looks at all eight bits in the TOS byte
10111000 = 184

DSCP only looks at six bits in the DSCP field
101110 = 46

tos 184

switches should
marking

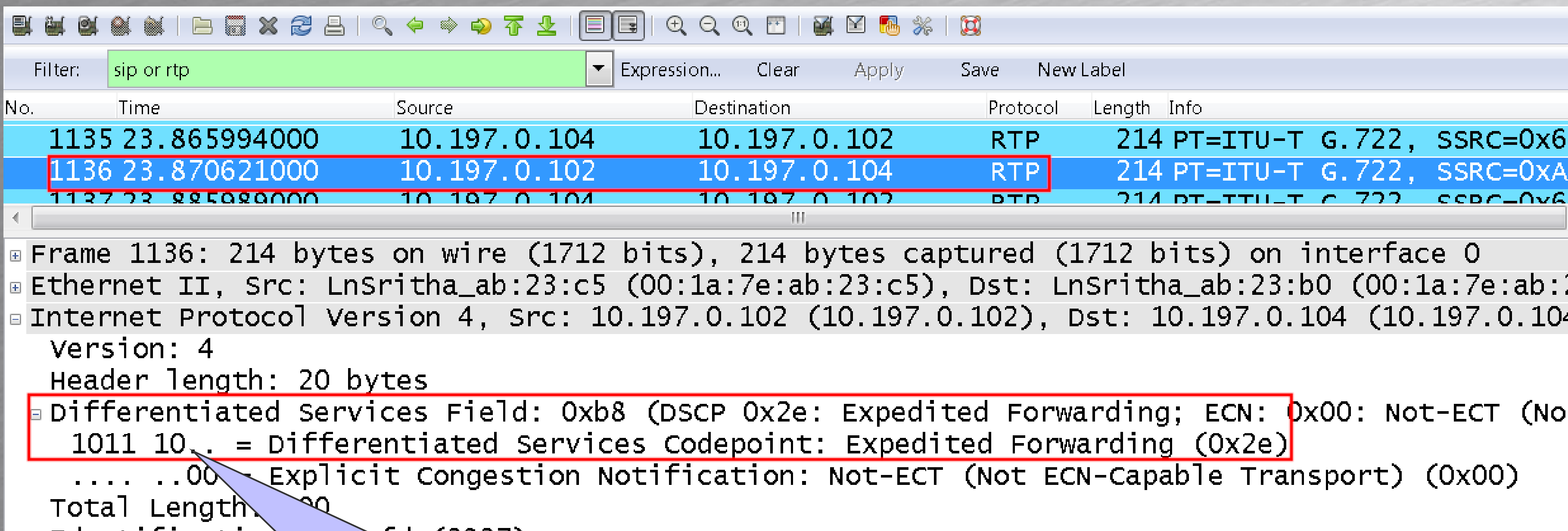
ascom

HOUSE OF TECHNOLOGY

– en del af mercantec+

Marking of packets

- The DiffServ, DSCP or ToS field can be marked by



SIP packe… by LG/Nortel IP8815 IP phone

RTP packet marked by LG/Nortel IP8815 IP phone

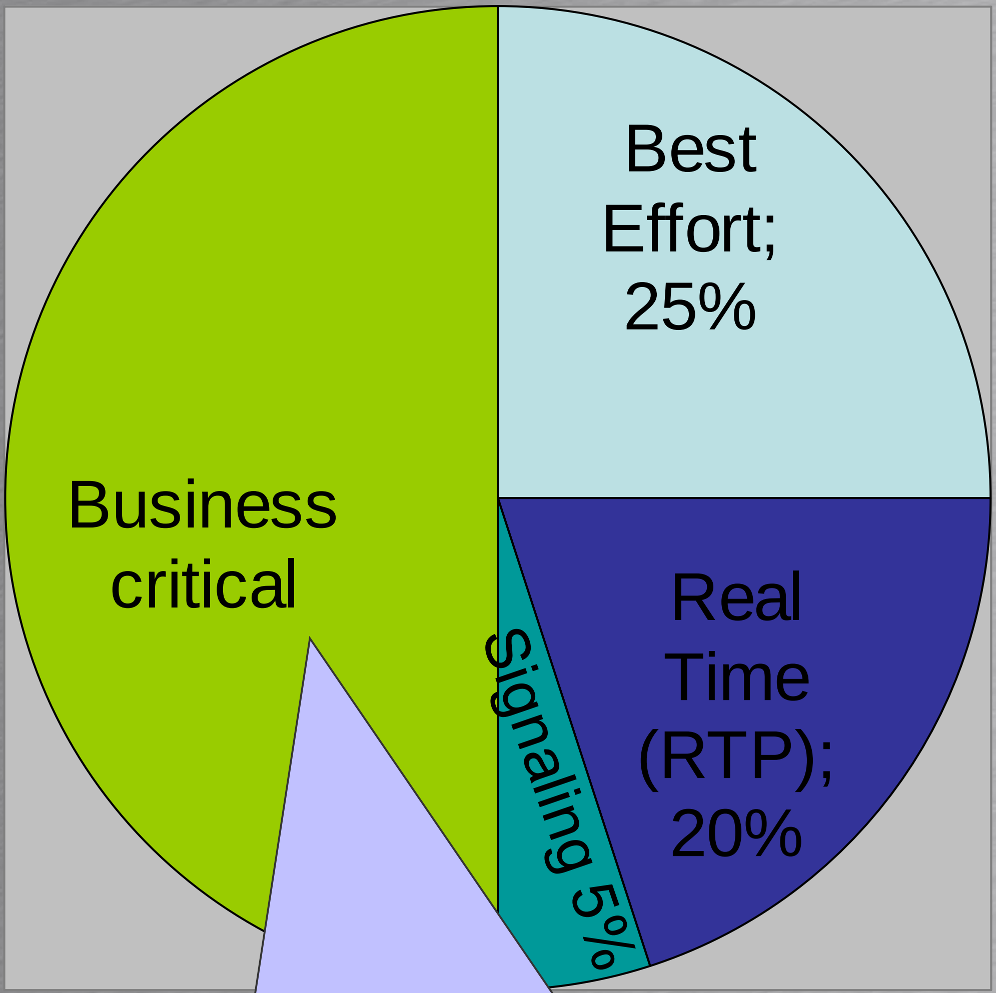
Classification and marking

- Classification
  - Identifying which traffic class a packet belong to
  - For example RTP traffic
- Marking
  - When the packet is classified it can be marked in the DSCP field
  - For example RTP traffic – DSCP = EF
    - Expedite Forwarding = 46 = 101110_2

Policing and markdown

- Policing
  - Set a bandwidth limit for a class and drop excessive traffic in that class
  - For example police RTP to 2 Mbps and drop RTP traffic that exceeds 2 Mbps for a given time period
- Markdown
  - Instead of dropping excessive traffic in a given class it can be marked down to a higher drop preference

Bandwidth allocation

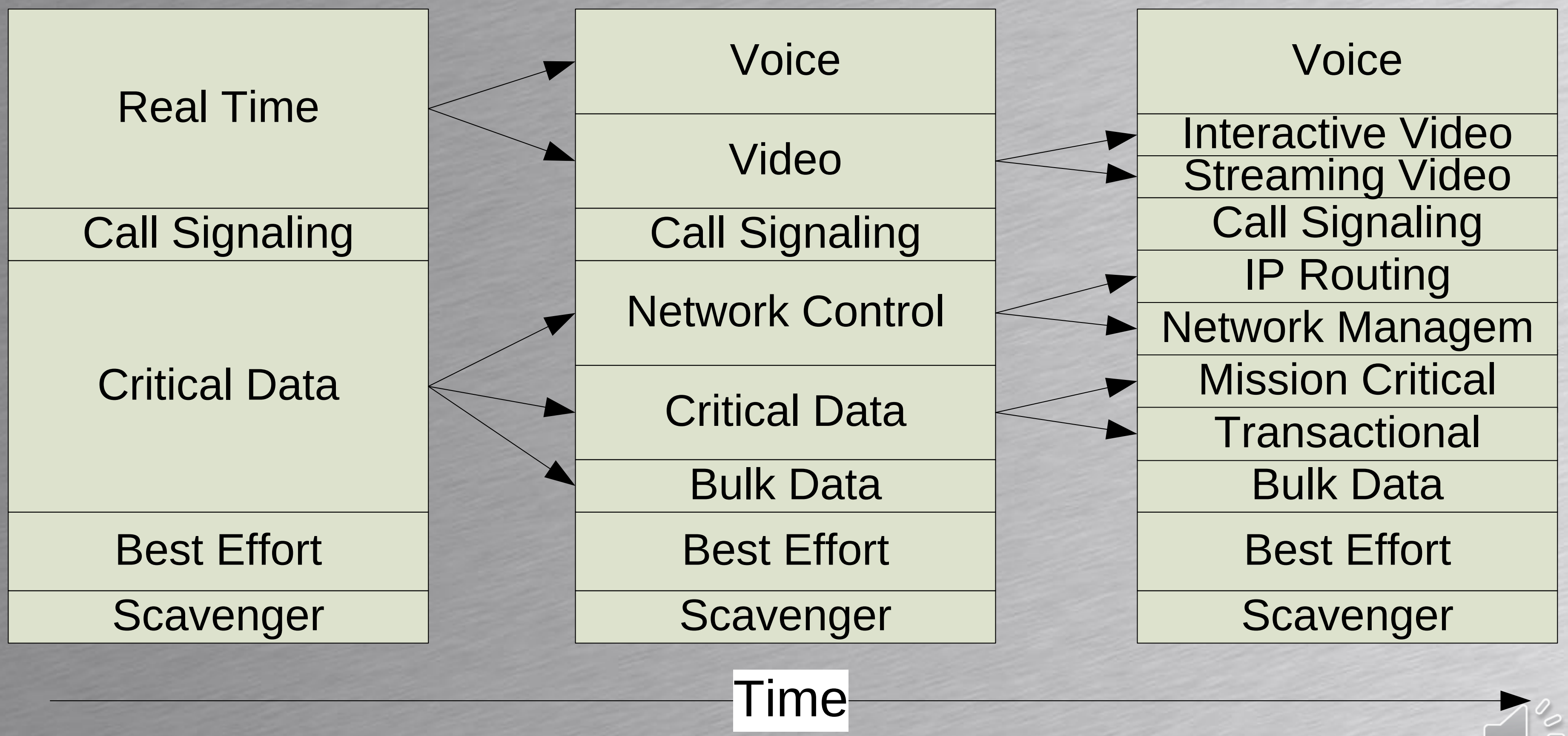


Unused traffic in one class, can be used when available by other classes that exceed their share

- In WAN environments for example MPLS a guarantied bandwidth is typically allocated
- For example in a 10 Mbps MPLS connection shown left
  - 2,5 Mbps best effort
  - 2 Mbps real time
  - 500 Kbps signaling
  - 5 Mbps critical

Traffic Classes

4/5 Class model | 8 Class model | QoS Baseline model



Configuration Example

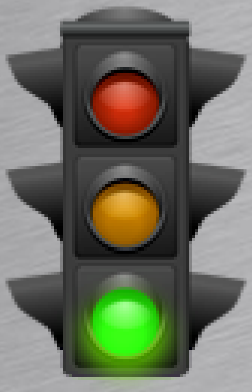
- LLQ

```
class-map MISSION-CRITICAL
  match dscp af41
class-map match-all VoIP
  match dscp ef
class-map SIGNALING
  match dscp af31
!
policy-map WAN-VIBORG
  class MISSION-CRITICAL
    bandwidth 25000000
  class VoIP
    priority 10000000
  class SIGNALING
    bandwidth 100000
  class class-default
    fair-queue
!
interface fastethernet0/0
 service-policy output WAN-VIBORG
```

OR

```
policy-map WAN-VIBORG
  class VoIP
    priority percent 33
  class MISSION-CRITICAL
    bandwidth remaining percent 50
  class class-default
    bandwidth remaining percent 50
```

QoS QUEUING

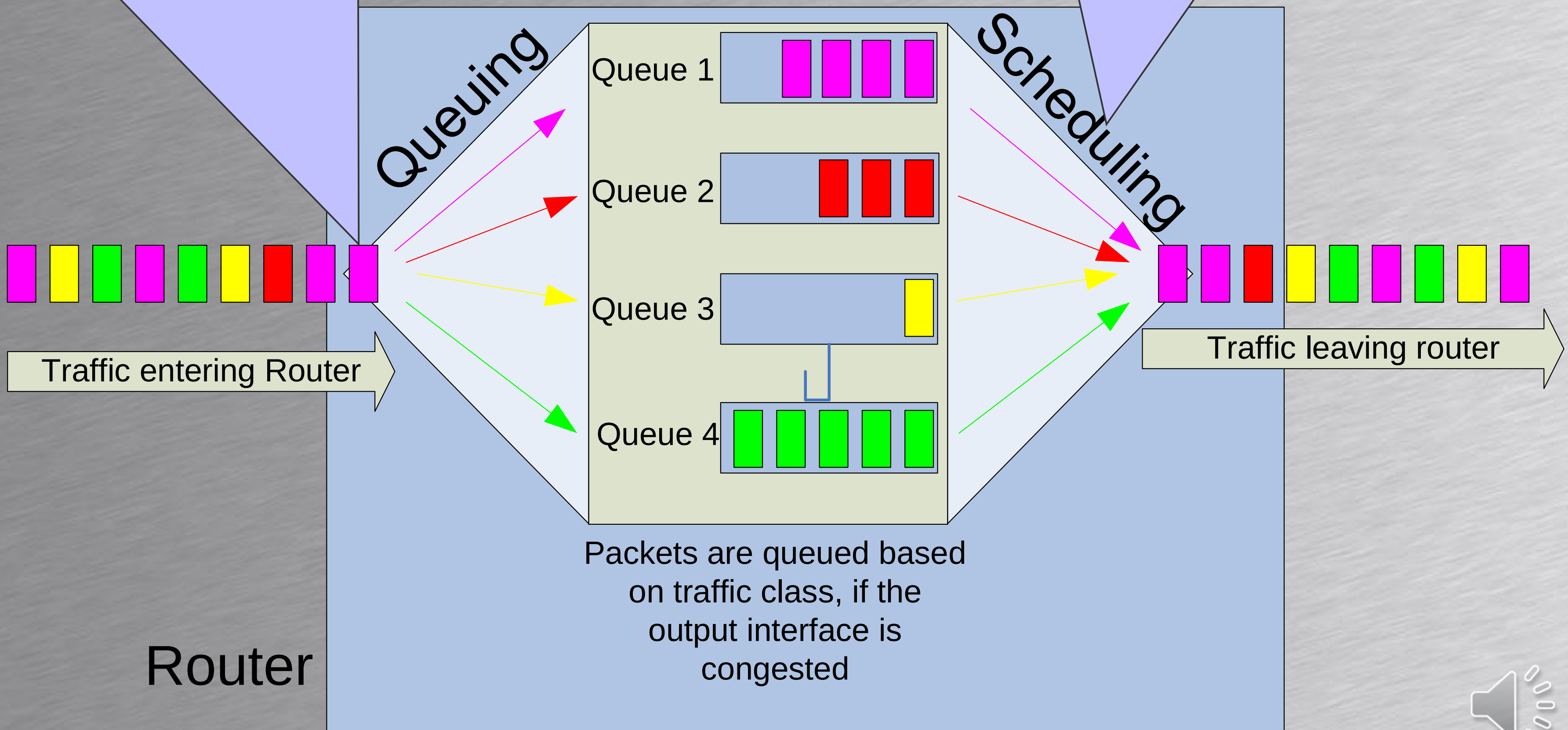


OSI layer 2 and layer 3 marking

Queuing principle

The scheduler empties the queues in a predetermined way based on the QoS policy

Packets are classified b
marking and queued in different queues based on the QoS policy. (Traffic class)



Queuing

- Putting the packets in one or more temporary buffers waiting for the scheduler to transmit the packet.
- Packets are only queued if the output interface is congested

Scheduling

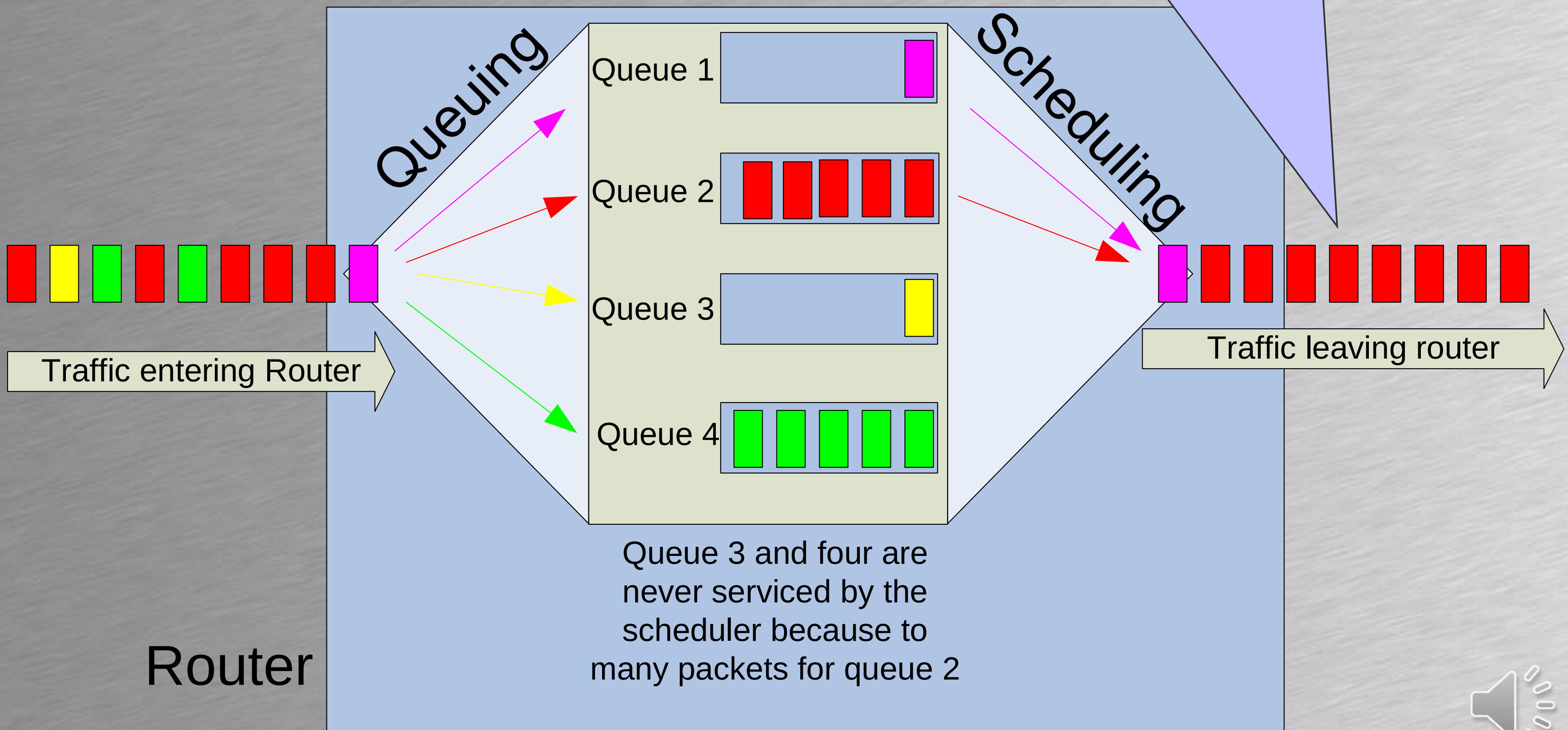
- The scheduler decides which packet to transmit next
- Scheduler policies
  - Strict priority
  - Round robin
  - Weighted fair
- Also called congestion management

Strict priority scheduling

- Queues have different priorities
  - Queue 1 have the highest priority
- Queue 1 must be empty before queue 2 is serviced
- Queue 2 must be empty before queue 3 is serviced
- …..
- Good for VoIP packets if they are in queue 1, but
  - Queues could go to a halt
- Example:
  - If there is to much traffic for queue 2 queues 3 and 4 would not be serviced by the scheduler

Strict priority scheduling

To many packets for queue number 2 causing congestion in queue 3 and 4



Round robin scheduling

- Each queue is serviced in turn
- No queues will halt because they are all serviced
- Delay variable for all queues
  - Not suitable for VoIP

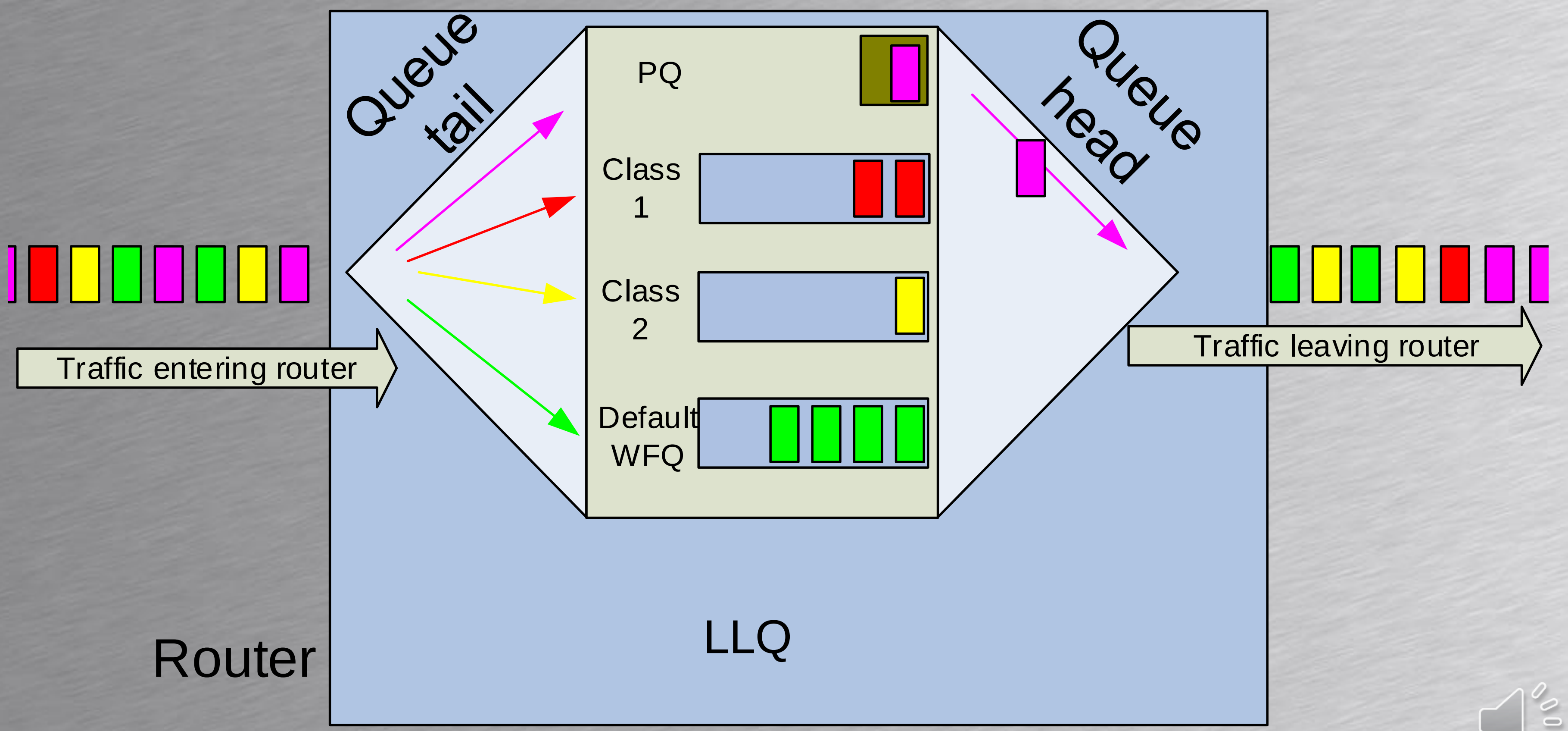
Weighted fair scheduling

- Controls each flow in the router based on IP addresses and port numbers
  - Gives a fair amount of bandwidth to each flow
- No bandwidth guaranty
  - Not suitable for VoIP

LLQ: Low Latency Queing

- LLQ takes the best from priority queuing, round robin and weighted fair queuing giving
  - 1 priority queue used for VoIP
  - Up to 256 round robin queues
  - Weighted fair queuing for traffic not classified

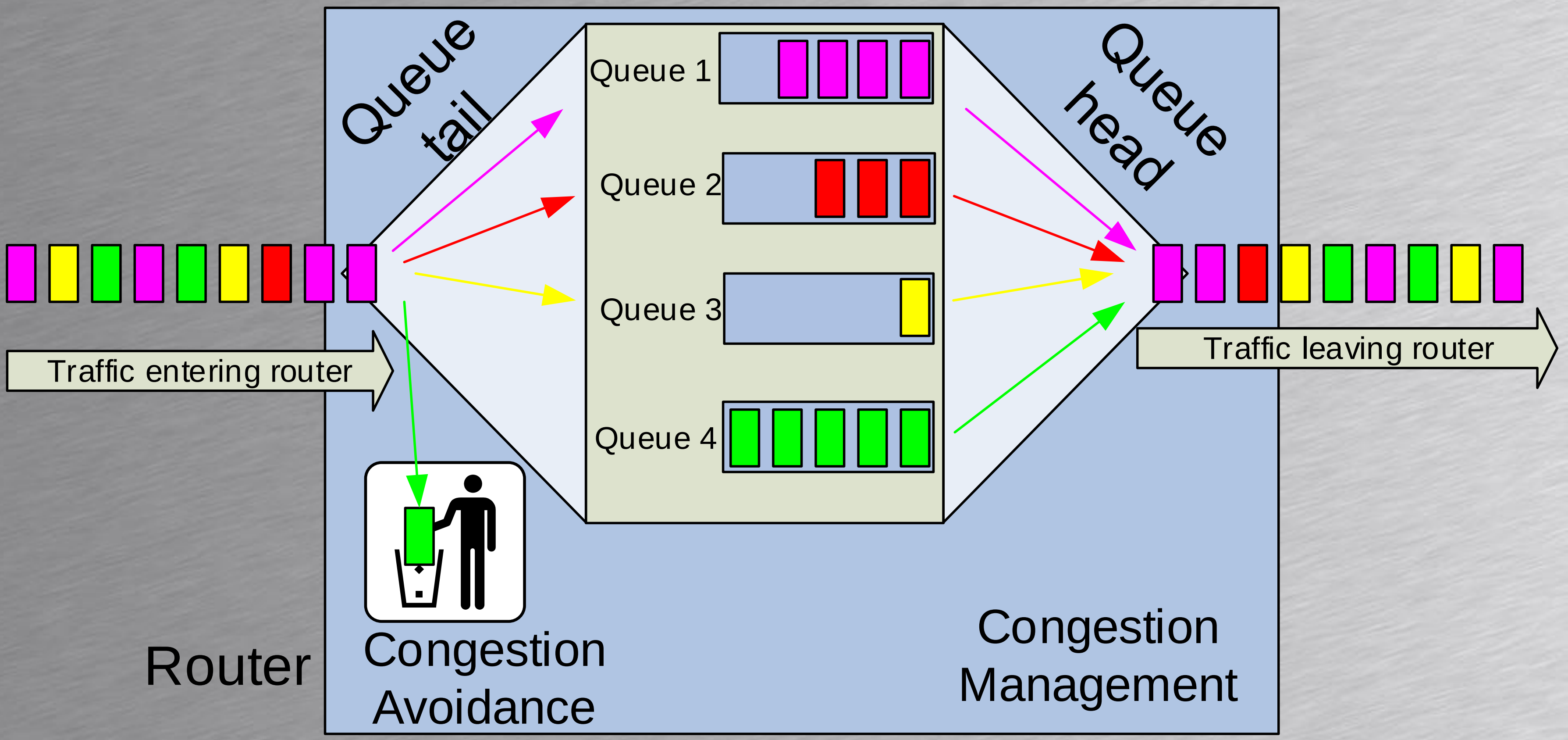
LLQ: Low latency queuing



Congestion avoidance

- When the queues are almost filled
- Selective dropping
  - Discard some of the received packets slowing down some of the packet streams
  - Works best dropping TCP packets

Congestion avoidance



Opgave

- Påvis i Wireshark at Telefonerne bliver markeret rigtigt.
- Find DSCP markeringerne for
  - Samtale trafik
  - Signalerings trafik
- Find CoS markeringen for
  - Samtale trafik
  - Signalerings trafik
- Lav et dokument der beskriver markeringen, og find nogle referencer til hvilke markeringer der skal bruges(cisco.com)