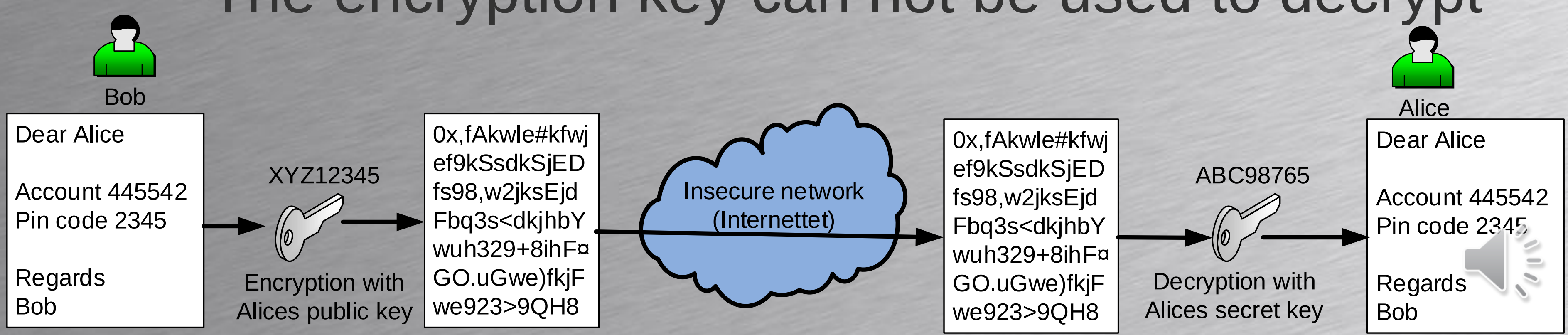
Encryption keys

- 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



MPLS VPN

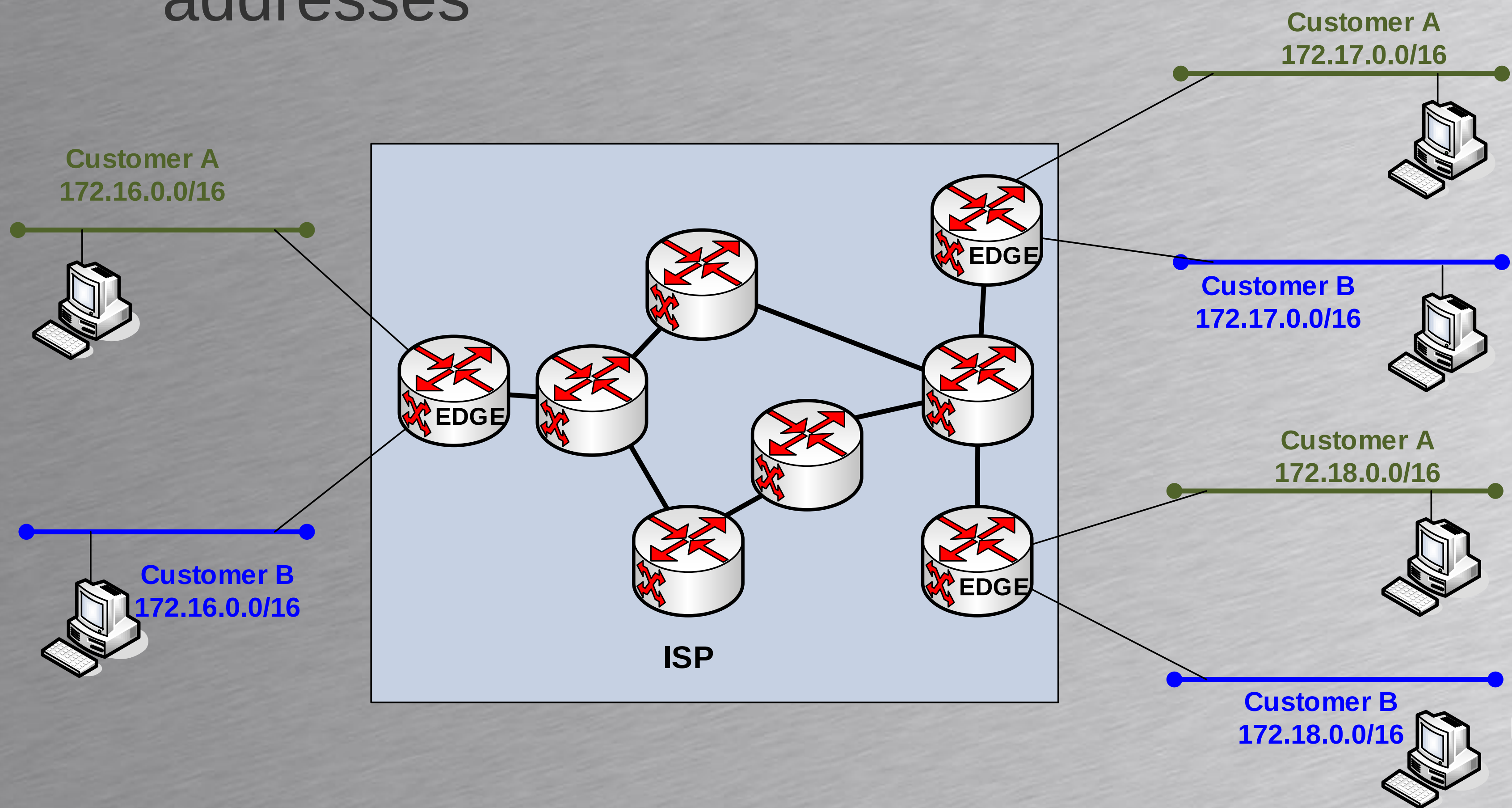
Multi Protocol Label Switching

- 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

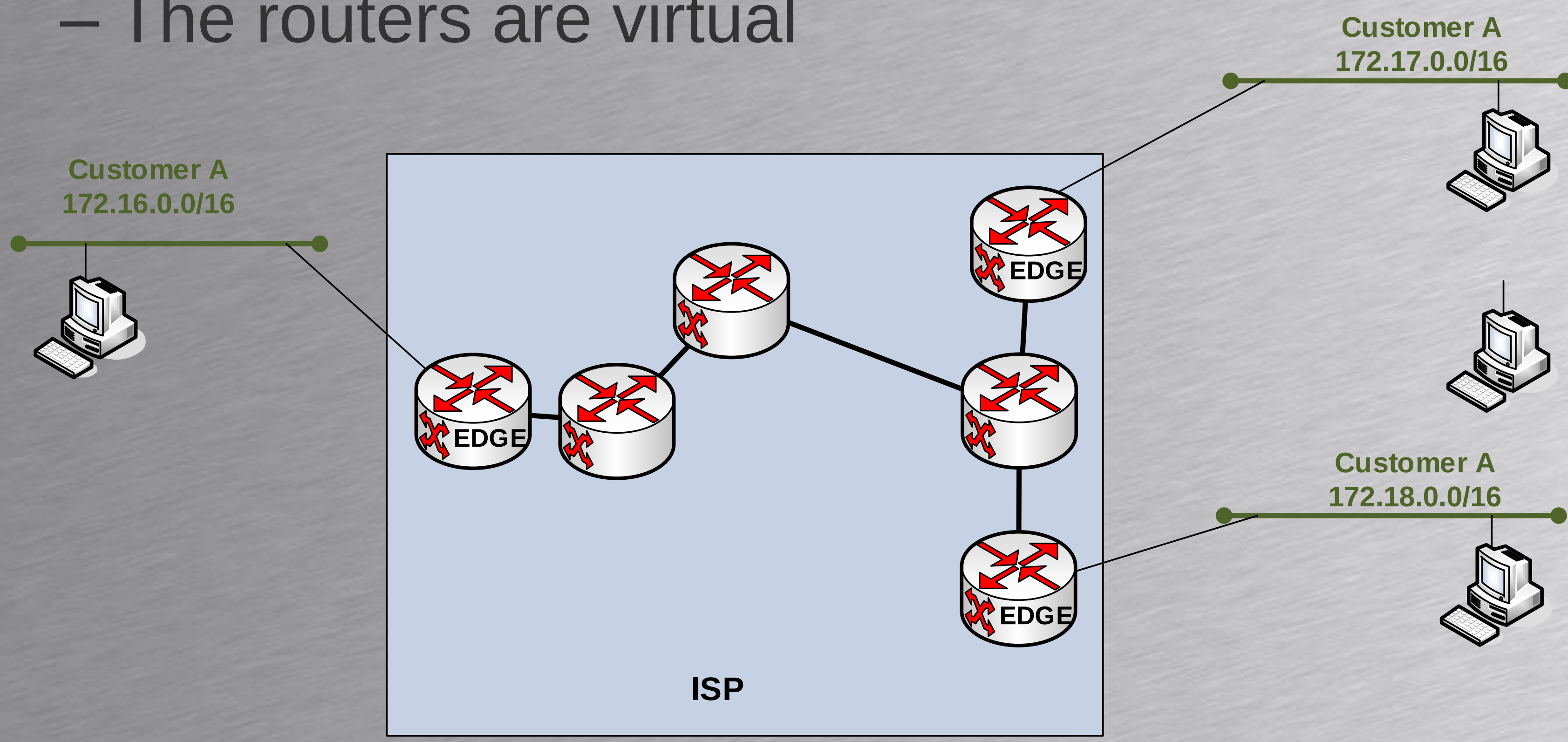
- Physical network as seen from the ISP
  - Both customers “accidently” uses same IP addresses



MPLS

Multi Protocol Label Switching

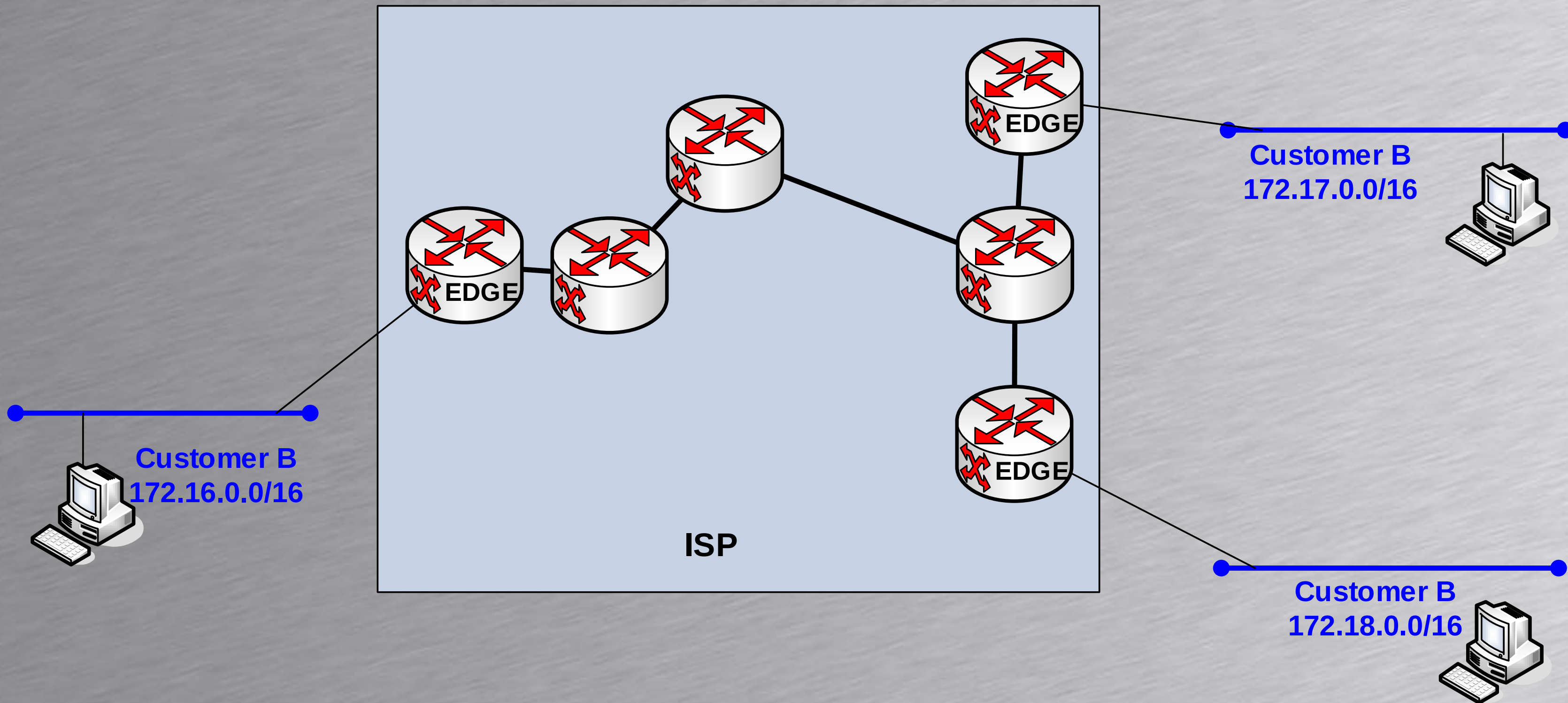
- Physical network as seen from Customer A
  - Customer A sees “his own network”
  - The routers are virtual



MPLS VPN

Multi Protocol Label Switching

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



VPLS

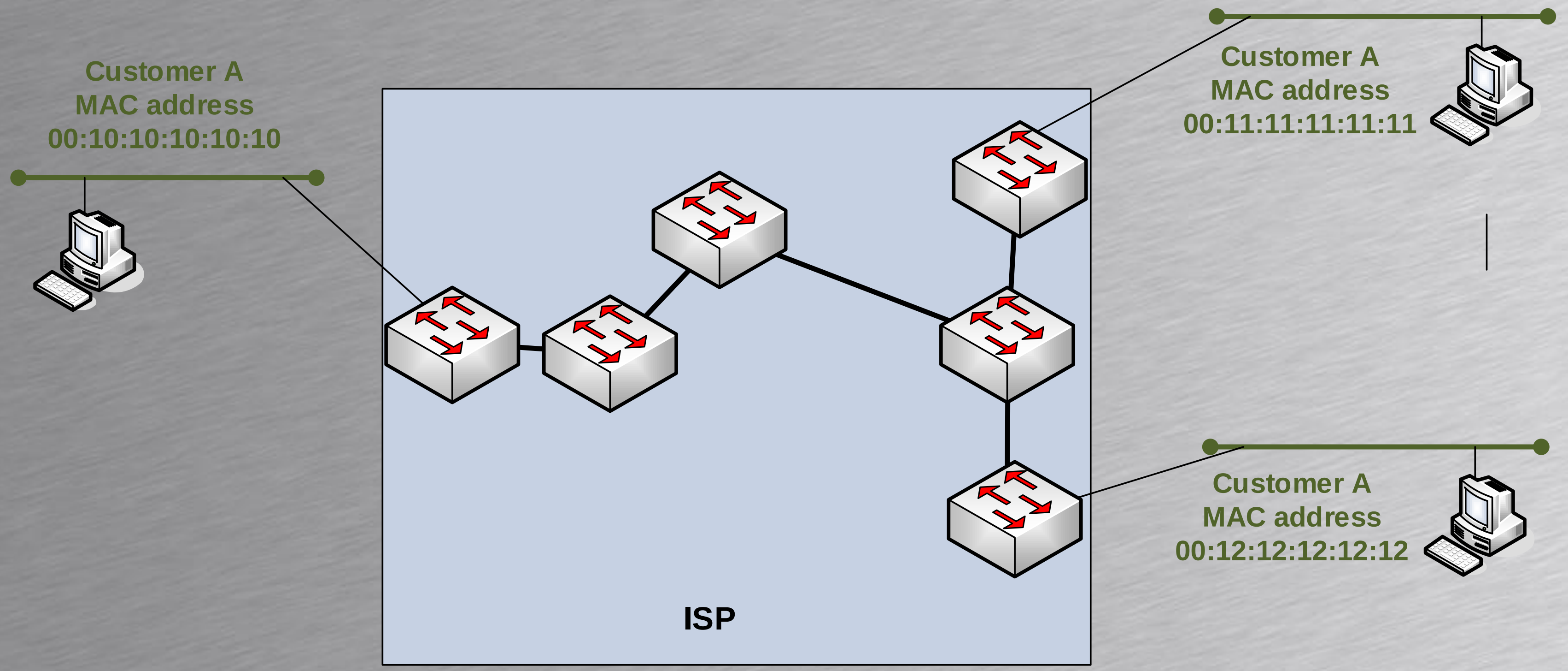
Virtual Private Lan Service

- 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 Customer A
  - Switching between remote sites



ascom

HOUSE OF TECHNOLOGY

– en del af mercantec

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)
Assured Forwardi… Low Drop Precedenc…								
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

be allocated to differe… …ences

00_2 = 0 = lowest drop preference

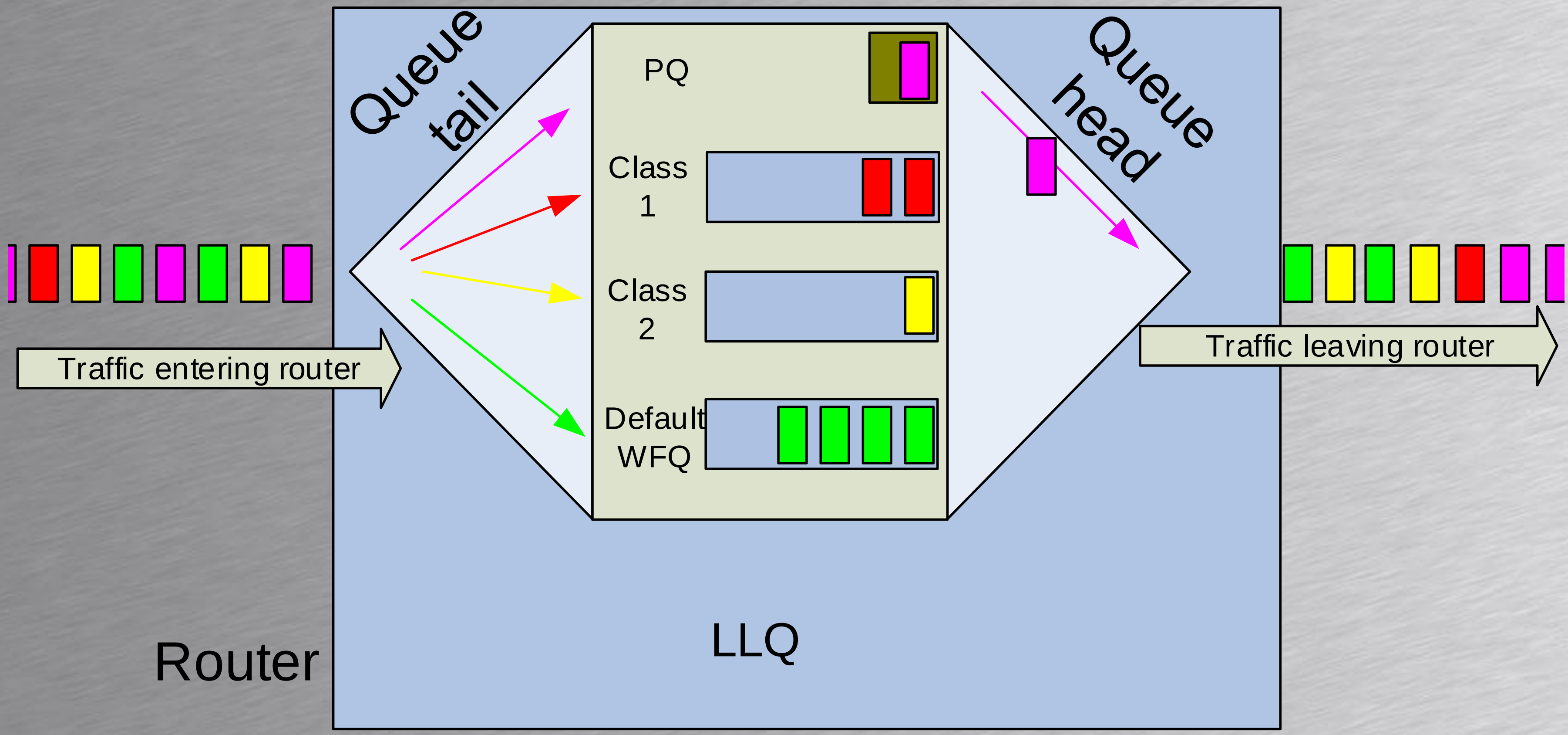
…

11_2 = 3 = highest drop preference

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



VoIP SECURITY

Encryption of voice and signaling

SIP Security

- SIP Register authentication vulnerability
  - A SIP phone registers with its proxy using username and password
  - If the username and password are transmitted in clear text, identity theft is possible
- SIP register authentication security
  - The server sends a ‘nonce’ to the client
    - A nonce is a random number
  - The client adds the nonce to the password and calculate a hash value returned to the server

hash

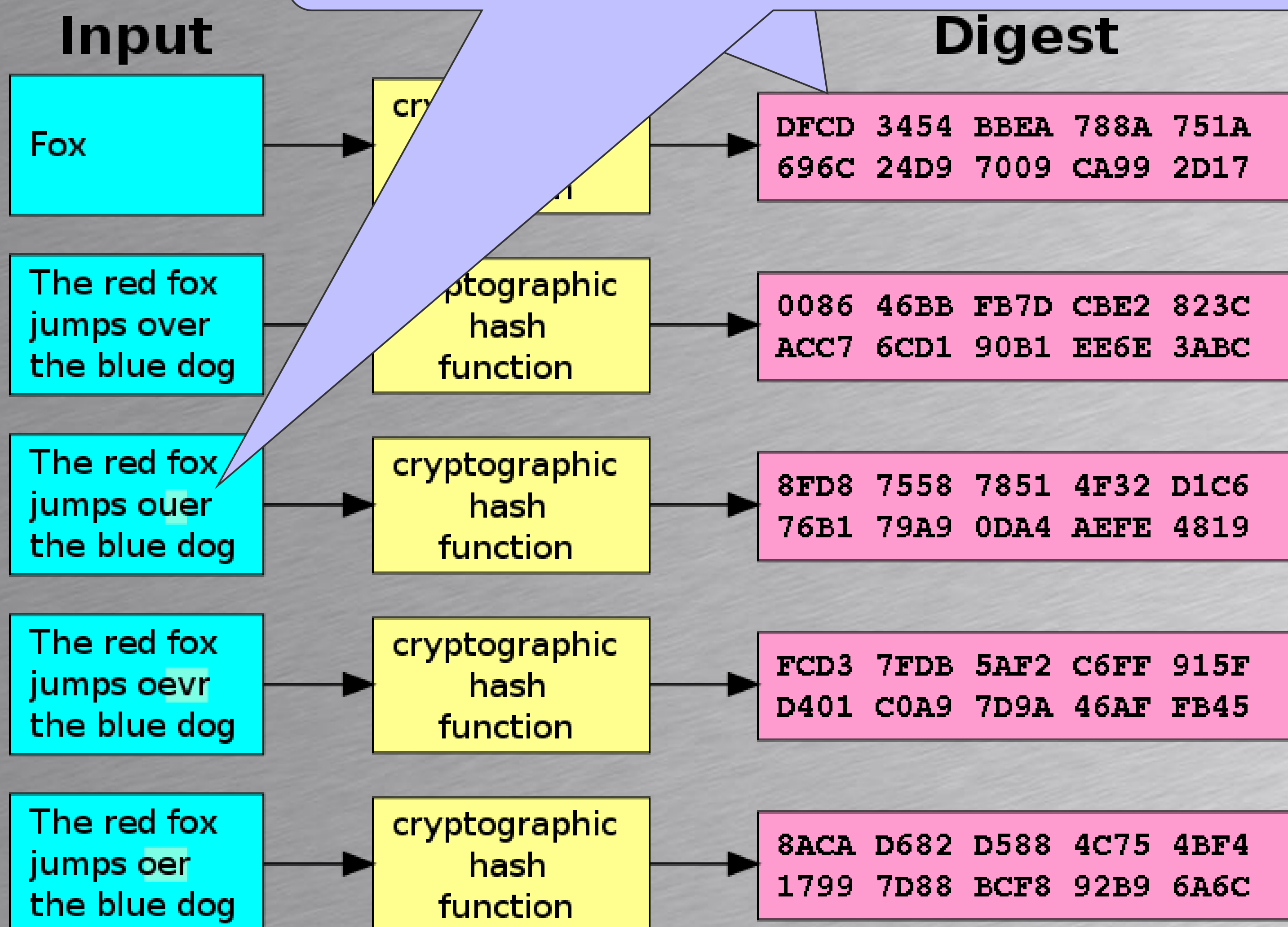
- A hash is a mathematical function
- Maps variable length data to fixed length data
- Used to protect passwords
- MD5 is presently the most used hash function
  - MD5 hash is considered compromised
  - Other hashes such as SHA-1, SHA-2 and SHA-3 are more secure. SHA-3 the most secure.
  - We will properly see them in SIP soon

HOUSE OF TECHNOLOGY

– en del af mercantec⁺

Note the output of the hash function all have the same length – regard
The hash value is ca

A small change in the input value yields a totally different digest



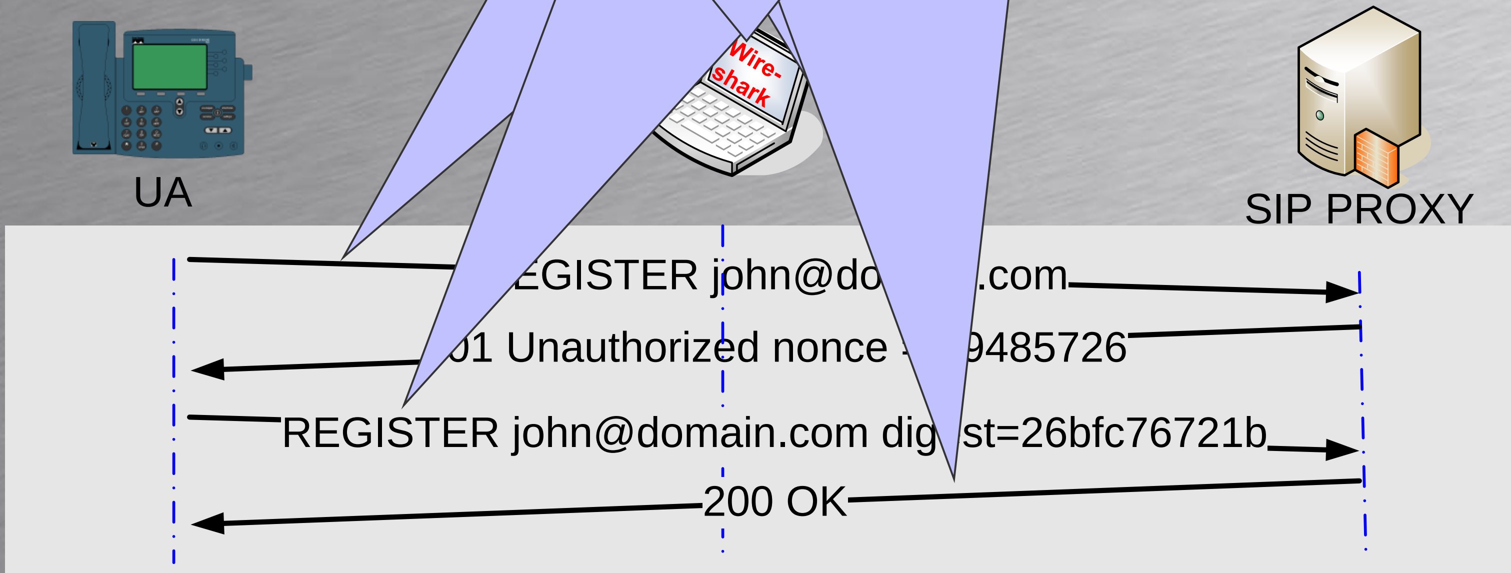
Basic principle

- The pas[...] d to
  the serv[...] e
  - The "ha[...] ord

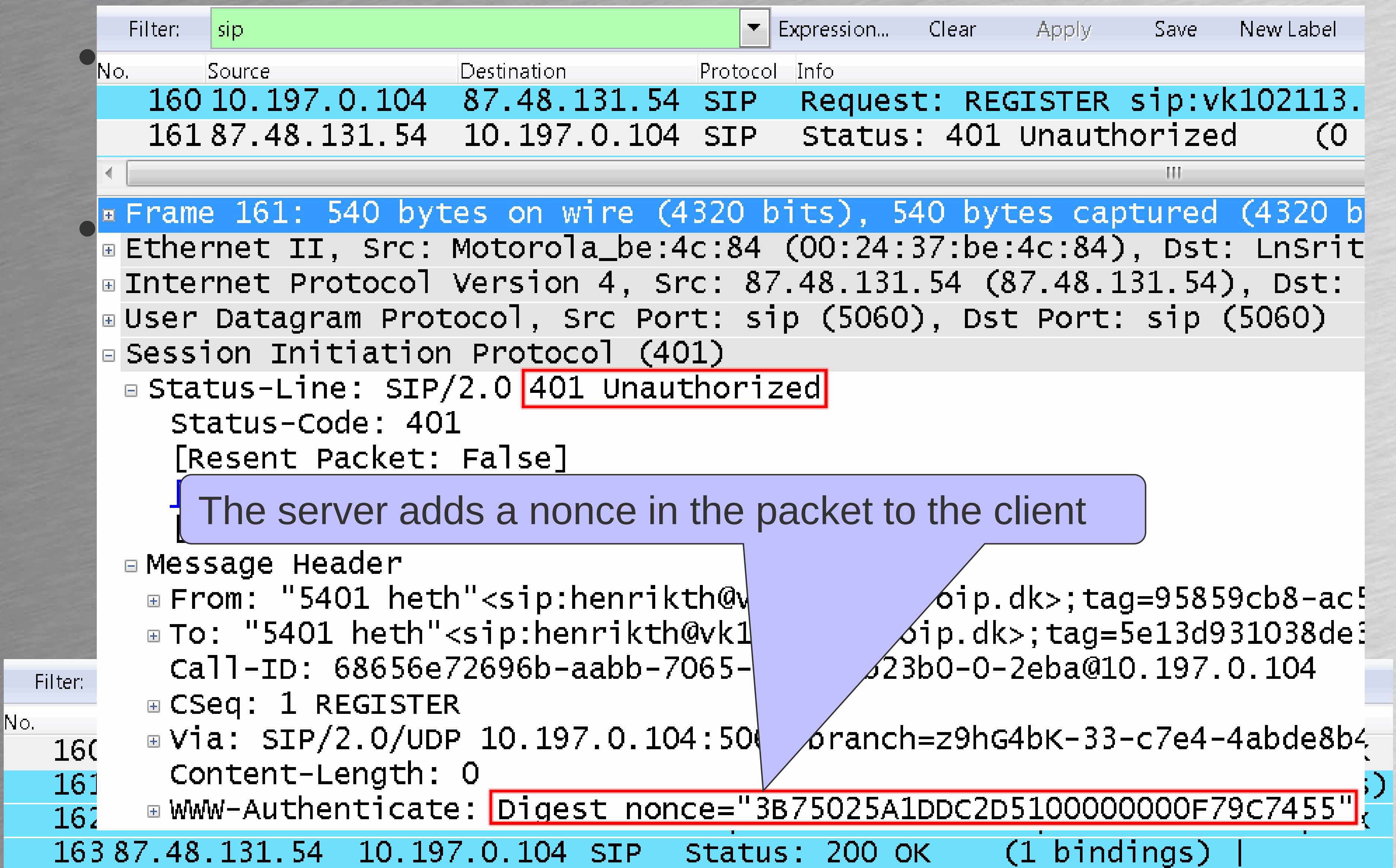
The hacker has learned
The username – the public URI
The nonce
The hash'ed password+nonce
Next time the server will choice a new random nonce

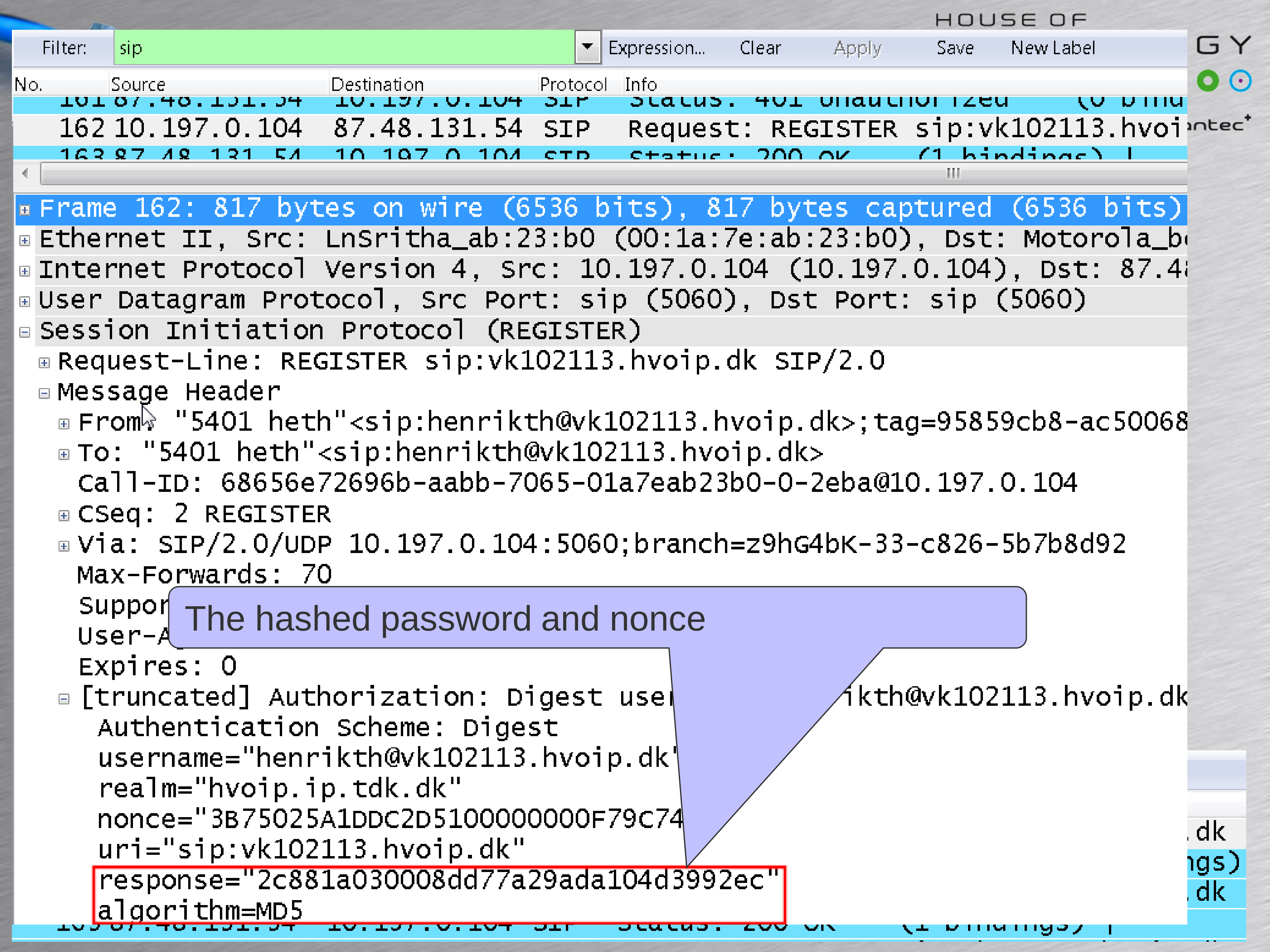
Username: john@domain.com
Password: ABC123

Username: john@domain.com
Password: ABC123



Wireshark capture




HOUSE OF
Filter: sip
Expression... Clear Apply Save New Label
No. Source Destination Protocol Info
162 10.197.0.104 87.48.131.54 SIP Request: REGISTER sip:vk102113.hvoi
Frame 162: 817 bytes on wire (6536 bits), 817 bytes captured (6536 bits)
Ethernet II, Src: LnSritha_ab:23:b0 (00:1a:7e:ab:23:b0), Dst: Motorola_b
Internet Protocol Version 4, Src: 10.197.0.104 (10.197.0.104), Dst: 87.4
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
Session Initiation Protocol (REGISTER)
Request-Line: REGISTER sip:vk102113.hvoip.dk SIP/2.0
Message Header
From: "5401 heth"<sip:henrikth@vk102113.hvoip.dk>;tag=95859cb8-ac50068
To: "5401 heth"<sip:henrikth@vk102113.hvoip.dk>
Call-ID: 68656e72696b-aabb-7065-01a7eab23b0-0-2eba@10.197.0.104
CSeq: 2 REGISTER
Via: SIP/2.0/UDP 10.197.0.104:5060;branch=z9hG4bK-33-c826-5b7b8d92
Max-Forwards: 70
Expires: 0
[truncated] Authorization: Digest user
Authentication Scheme: Digest
username="henrikth@vk102113.hvoip.dk"
realm="hvoip.ip.tdk.dk"
nonce="3B75025A1DDC2D5100000000F79C74
uri="sip:vk102113.hvoip.dk"
response="2c881a030008dd77a29ada104d3992ec"
algorithm=MD5
The hashed password and nonce

ascom

HOUSE OF TECHNOLOGY

– en del af mercantec+

Wireshark capture

- Packet 160 – Client register request
  - No password attached
- Packet 161 – Register rejected
- Packet 162 – Client register request
  - Hash digest included
- Packet 163 – Server registers client
  - The client is online

Filter: sip   Expression... Clear Apply Save New Label

No.	Source	Destination	Protocol	Info
160	10.197.0.104	87.48.131.54	SIP	Request: REGISTER sip:vk102113.hvoip.dk
161	87.48.131.54	10.197.0.104	SIP	Status: 401 Unauthorized (0 bindings)
162	10.197.0.104	87.48.131.54	SIP	Request: REGISTER sip:vk102113.hvoip.dk
163	87.48.131.54	10.197.0.104	SIP	Status: 200 OK (1 bindings) |

SRTP

Secure Real Time Transport Protocol

- SRTP provides
  - Confidentiality: Encryption of voice
  - Authentication: Identity of parties
  - Integrity: Data not changed in transit
  - Replay protection: Packets cant be replayed
- SRTP can be used with unicast and multicast
- SRTP is described in RFC 3711

SRTP

Secure Real Time Transport Protocol

- RFC 3711 does not cover key exchange between end-points
- A master key must be exchanged securely between end-points
- The master key is used to generate the all the necessary session keys
- Key exchange implemented using public or proprietary methods
  - Different vendors different method ☹

SRTP

Secure Real Time Transport Protocol

- Keys could be exchanged using
  - MIKEY: Public RFC 3830
    - Multimedia Internet Keying
  - ZRTP: Public RFC 6189
    - Zimmermann RTP
  - KEYMGT: Public RFC 4567
    - Key Management Extensions
  - SDMS
    - Session Description Protocol Security Descriptions for Media Streams

SRTP with ZRTP

Secure Real Time Transport Protocol

- ZRTP is a cryptographic key-agreement protocol to negotiate keys for encryption
- Uses Diffie-Hellman key exchange
- Uses same UDP ports as SRTP
  - No extra UDP or TCP ports necessary
- ZRTP can be used with SIP and H.323

Diffie and Hellman

- Dr. Whitfield Diffie
- Bachelor of science mathmatics
- Retired but studying security in grid computing

- Martin Hellman
- Professor Emeritus from Stanford University
- Retired

Diffie-Hellman key exchange

- Uses mathematical one-way functions
- Security based on huge prime numbers

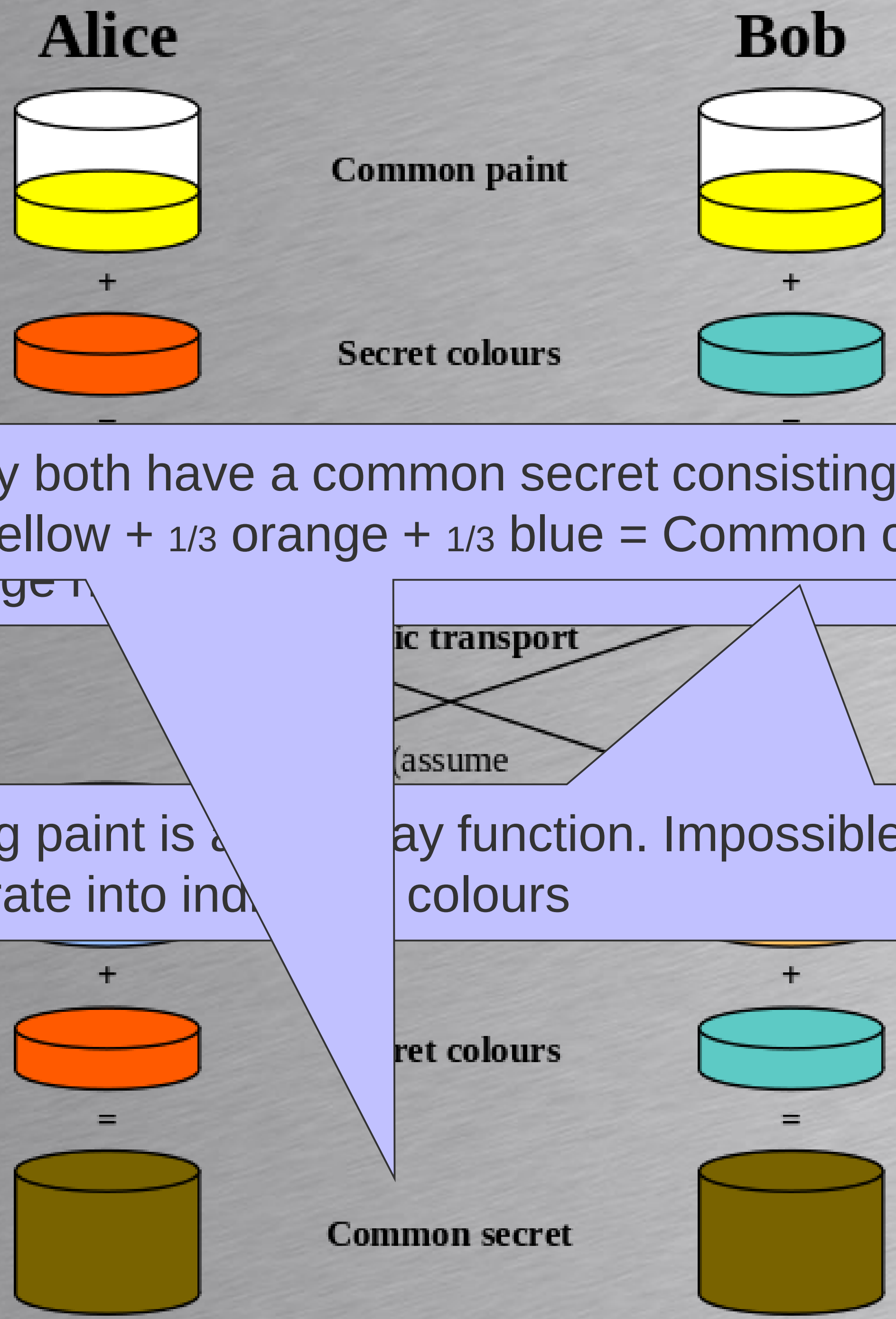
<u>A 1024 bit prime:</u>

1797693134862315907708391567937874531978602960487560
1170644442368419718021615851936894783379586492554150
2180565485980503646440548199239100050792877003355816
6392295531362390765087357599148225748625750074253020
7744771258955095793777842444242661733472762929938766
870920560605027081084290769293201912819446762 7007

– DH Group 2 = 1024 bit

– DH Group 5 = 1536 bit

- Higher group numbers are more secure

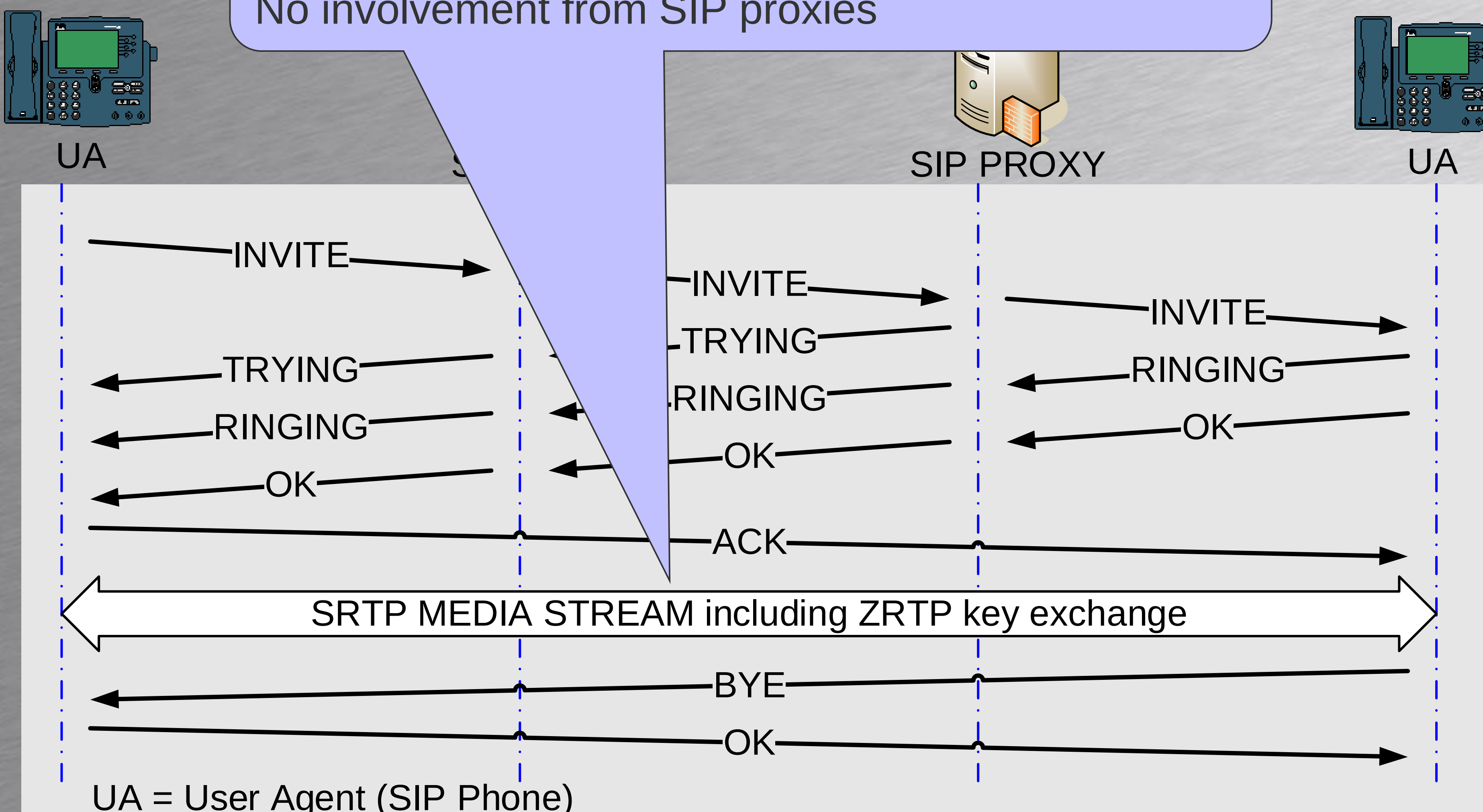


They both have a common secret consisting of
1/3 yellow + 1/3 orange + 1/3 blue = Common colour

Mixing paint is a one-way function. Impossible to separate into individual colours

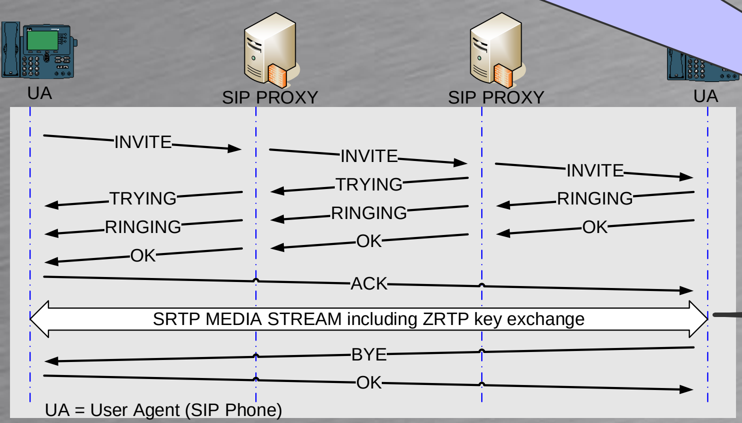
SIP and ZRTP flow

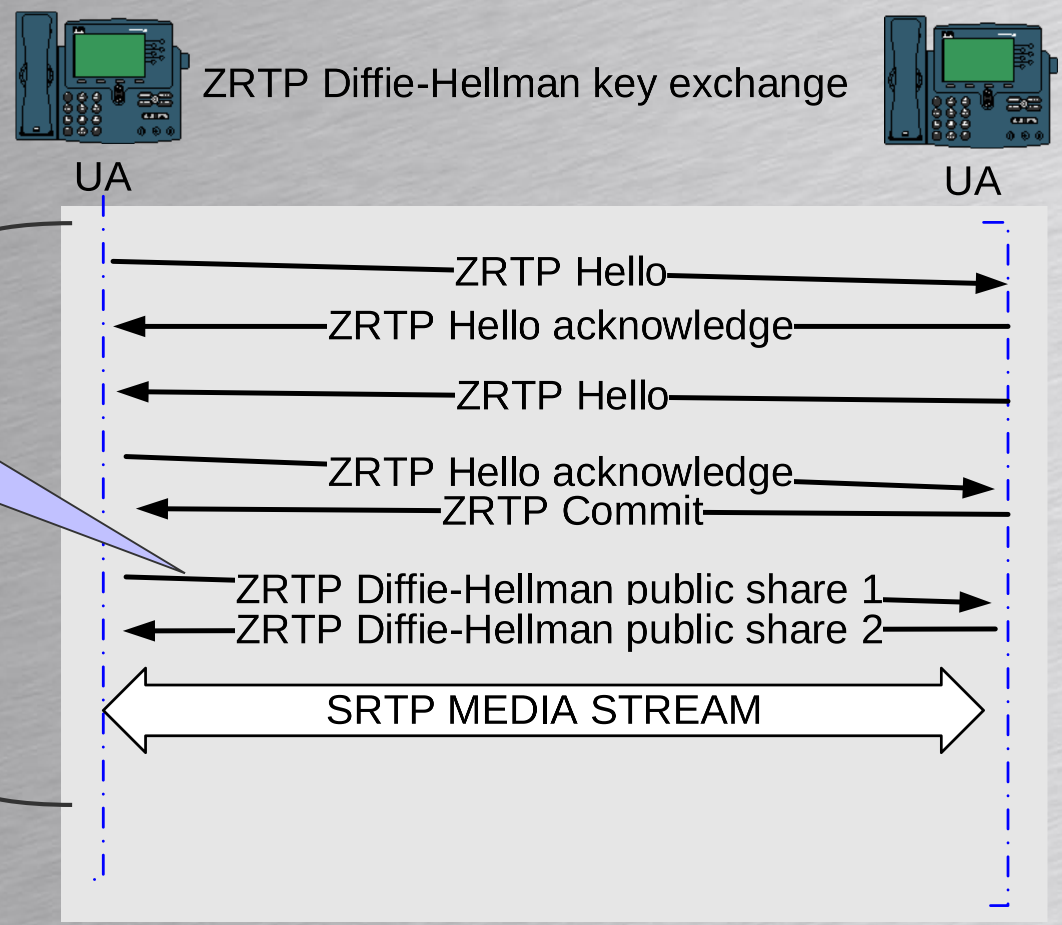
Encrypted SRTP media stream. Keys exchanged with diffie-hellman directly between the endpoints. No involvement from SIP proxies



RTP,ZRTP and SRTP

ZRTP exchanges Diffie-Hellman keys using the RTP protocol and SRTP uses the keys for encryption





Secure SIP

- As known from web surfing
  - HTTP is unencrypted transport on TCP port 80
  - HTTPS is encrypted transport on TCP port 443
  - HTTPS uses SSL/TLS for security
- SIPS signaling or SIP over SSL/TLS gives
  - SIP is unencrypted transport on TCP port 5060
  - SIPS is encrypted transport on TCP port 5061
  - SIPS uses SSL/TLS for security

SSL/TLS

- SSL – Secure Sockets Layer
  - Older but still used
- TLS – Transport Layer Security
  - New version of SSL giving better security
- SSL and TLS can use different security protocols and key sizes
  - Client and server agree on which security settings to use. Also called Cipher setting

SSL/TLS

- When a client initiates a SSL or TLS connection to a server it list the possible Cipher settings it supports
- The server responds with the cipher setting it prefers
- A cipher setting typically include
  - Exchange of public keys (Asymmetric keys)
  - An encryption standard and key size
  - An HASH algorithm to use

ascom

SSL/TLS

HOUSE OF TECHNOLOGY

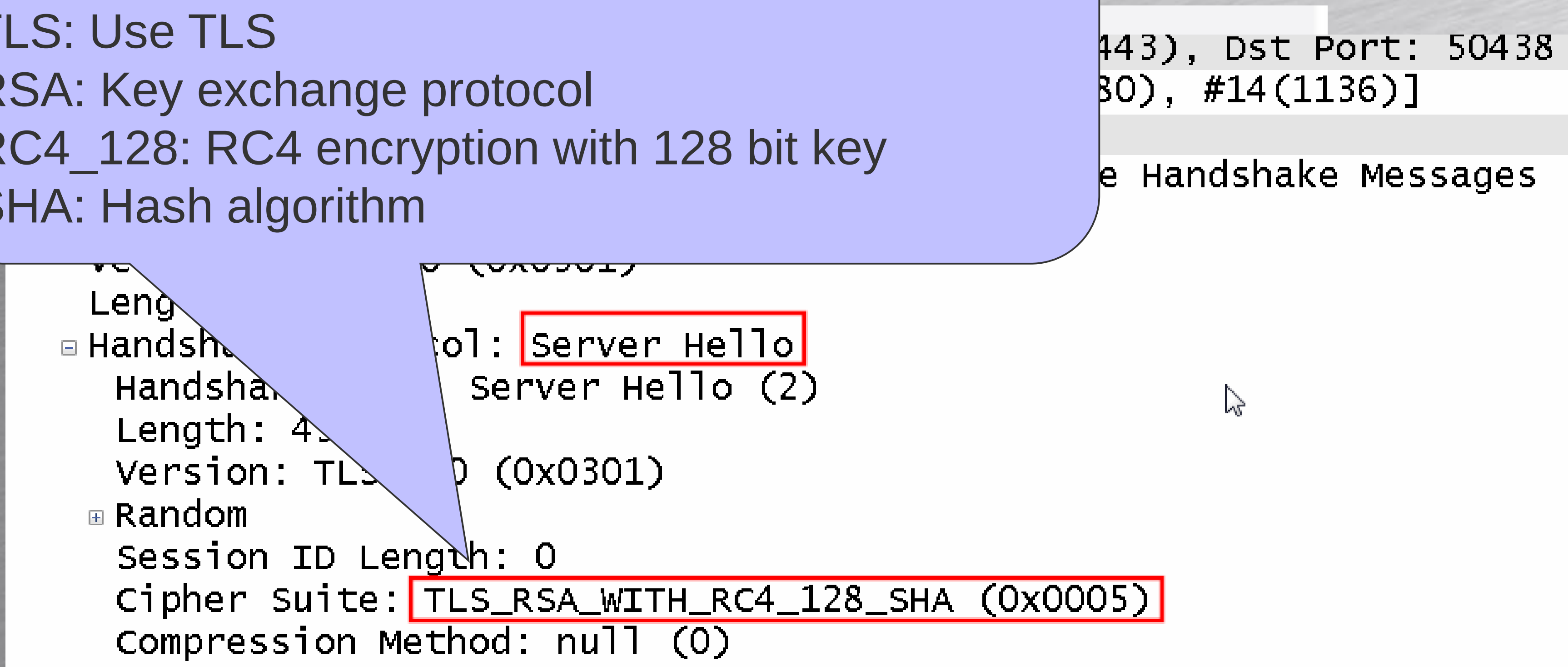
- en del af mercantec

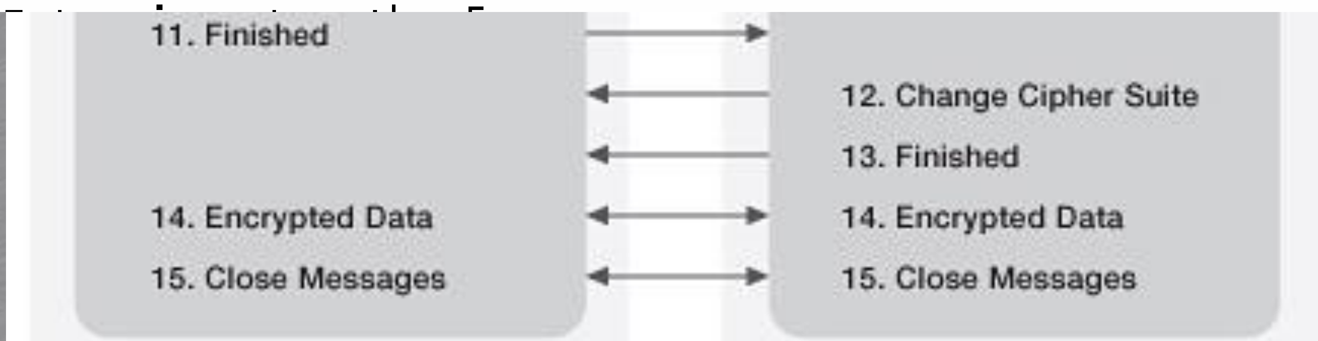
```
⊞ Transmission Control Protocol, Src Port: 50438 (50438), Dst Port:
⊟ Secure Sockets Layer
  ⊟ TLSv1 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x030
      Length: 191
    ⊟ Handshake Protocol: Cli
        Handshake Type: Client
        Length: 187
        Version: TLS 1.1 (0x0302)
      ⊞ Random
        Session ID Length: 0
        Cipher Suites Length: 72
      ⊟ Cipher Suites (36 suites)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
          Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
          Cipher Suite: TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0088)
          Cipher Suite: TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA (0x0087)
          Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
          Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
          Cipher Suite: TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
          Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)
          Cipher Suite: TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0084)
```

In this example the client lists 36 different Cipher settings/suites the server can choice from

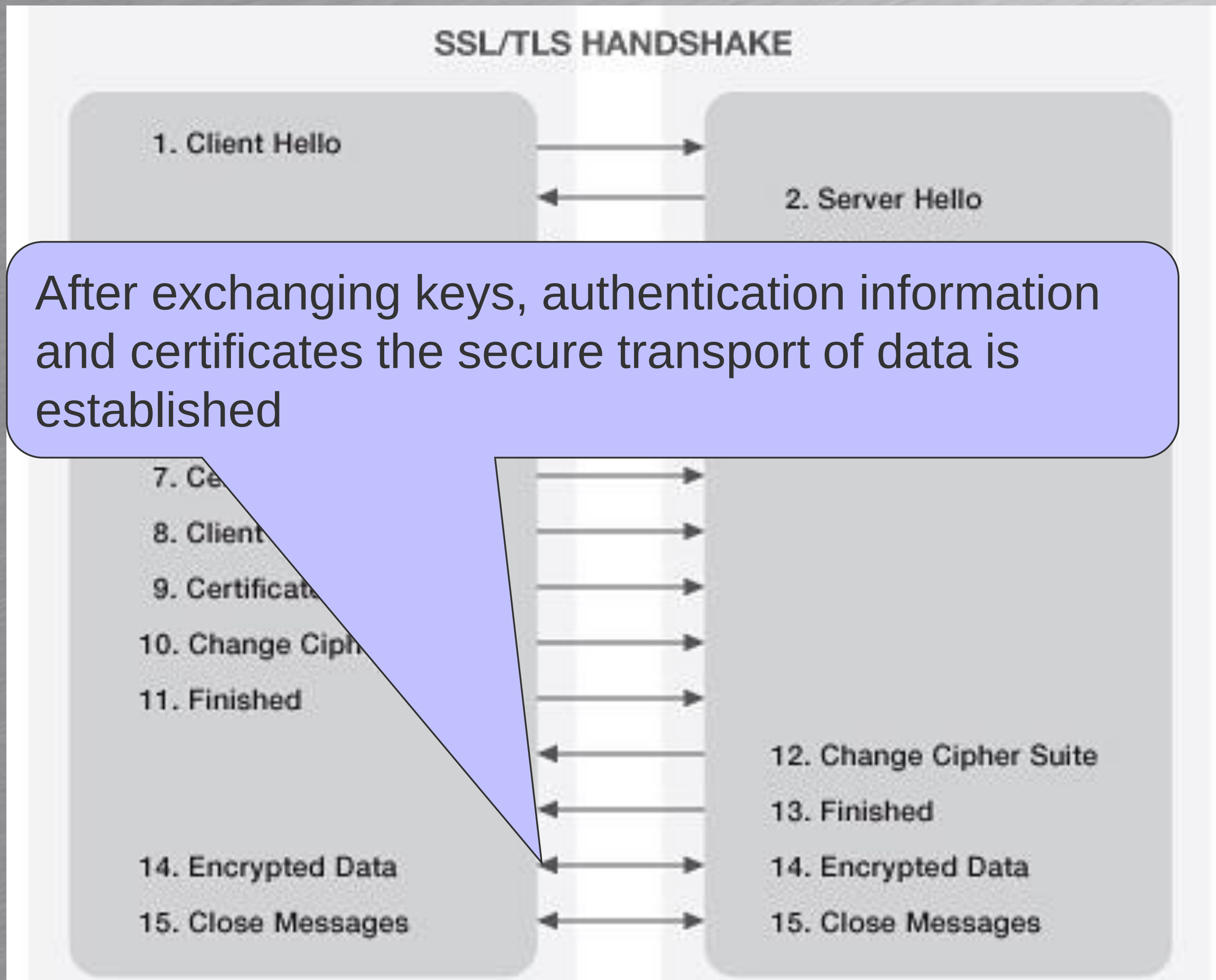
SSL/TLS

In this example the server have chosen the Cipher setting
TLS: Use TLS
RSA: Key exchange protocol
RC4_128: RC4 encryption with 128 bit key
SHA: Hash algorithm





SSL/TLS



After exchanging keys, authentication information and certificates the secure transport of data is established

VoIP AVAILABILITY

When things go wrong

Things that might fail

- IP PBX fails
  - All phones registered fail
- Power outage
  - All devices without battery backup fail
- Network device failure
  - All devices dependent on that device fail
- PSTN/ISDN connection fails
  - No incoming or outgoing calls possible
- VPN connection between sites fail
  - No calls between sites

Redundancy and failover

- Redundancy
  - When the primary device fails a redundant secondary device takes over the load and ensures connectivity
  - Important an alert is transmitted if the primary or secondary device fails
    - No impact on normal service

Redundant power supply for server

Types of redundancy

- Hot standby
  - Secondary device ready to offload primary
  - Heartbeats transmitted between secondary and primary
    - If primary device don’t answer heartbeats for a given time period secondary device takes over
      - Alarm transmitted to alert IT-Staff
    - If primary device don’t receive heartbeats from secondary device for a given time period
      - Alarm transmitted to alert IT-Staff

Types of redundancy

- Load balancing
  - Workload distributed between two or more redundant devices
  - Heartbeats transmitted between devices
    - If one device don’t answer heartbeats for a given time period the workload are distributed to the remaining
      - Alarm transmitted to alert IT-Staff

RAID: Redundant Array of Independent Disks

Virtual IP address

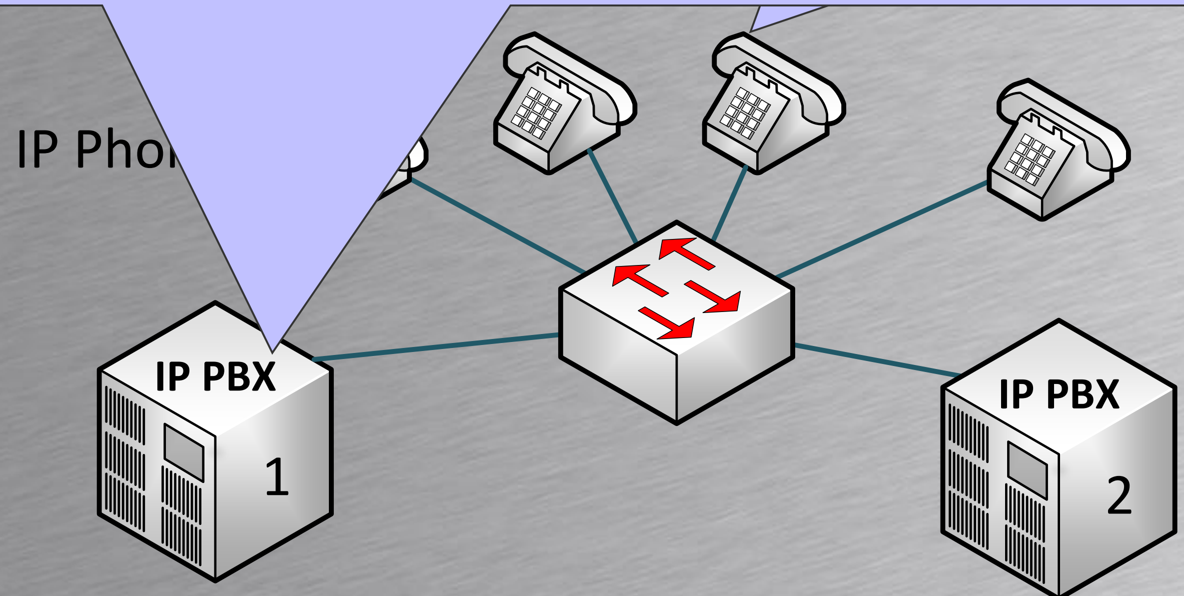
- A virtual IP address is a IP address shared between two or more devices
  - A virtual IP address uses a virtual MAC address
- Only one device will normally use the IP address
  - Called the Active device
- The active device does all the workload
- If the active device fails the standby device becomes active and takes over the virtual IP address and the virtual MAC address

Virtual IP address

Example

The phones register to 192.168.1.2

IP PBX 1 transmits all information included registered phones on-going calls and other information to IP PBX2 on 192.168.1.11




```
IP PBX 1 configuration

IP Address        : 192.168.1.10
State             : Active
Virtual IP addr.  : 192.168.1.2
Virtual MAC addr.: 00-10-20-30-40-50
```

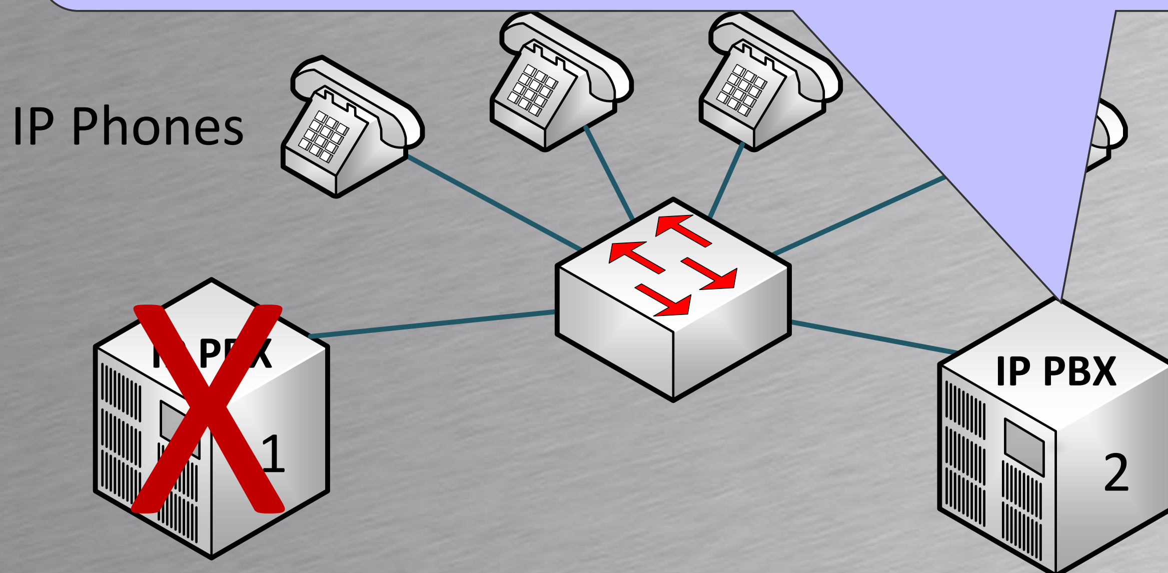
```
IP PBX 2 configuration

IP Address        : 192.168.1.11
State             : Standby
Virtual IP addr.  : -
Virtual MAC addr.: -
```

Virtual IP address

Example

IP PBX 2 takes over as active when no replies from heartbeats received. The state off all phones known and on-going calls still in progress



IP PBX 1 configuration

```
IP Address       : 192.168.1.10
State            : PBX service down
Virtual IP addr. : -
Virtual MAC addr.: -
```

IP PBX 2 configuration

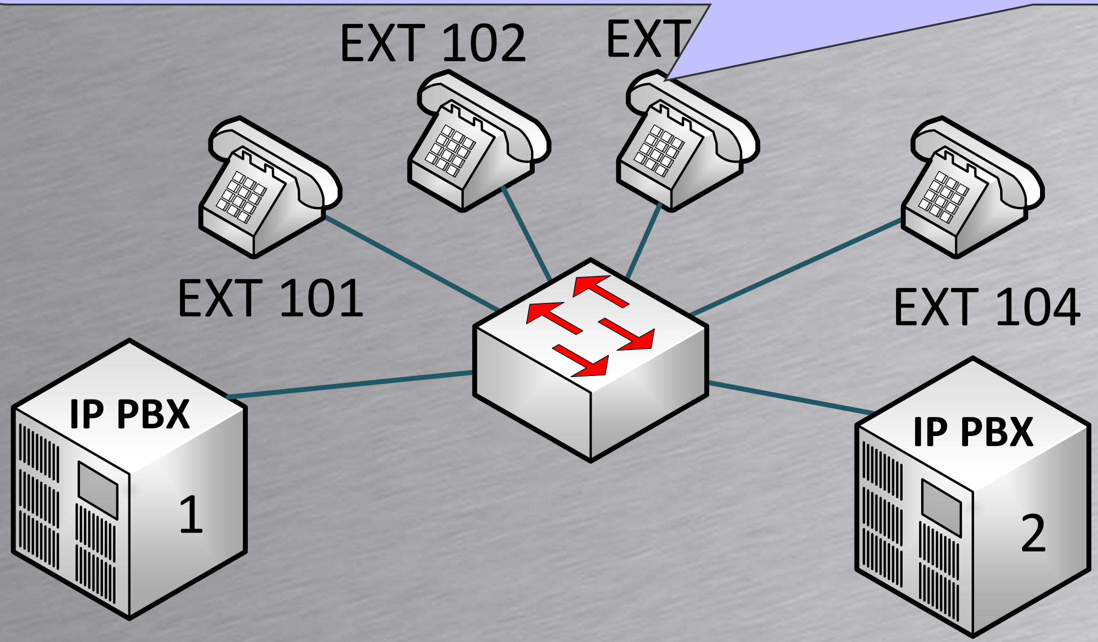
```
IP Address       : 192.168.1.11
State            : Active
Virtual IP addr. : 192.168.1.2
Virtual MAC addr.: 00-10-20-30-40-50
```

SIP proxy redundancy 1

- Client based failover
- SIP phones – UA – register with two SIP Proxies
  - NOTE: Not all SIP phones can register twice
  - A primary and a backup proxy
  - All phones in the SIP domain register with two proxies
  - If the primary fails the phones use the backup proxy

SIP proxy redundancy 1

Each SIP phone can initiate a call using IP PBX 1 or IP PBX 2.
If the first tried IP PBX is unavailable the SIP phone will try the other IP PBX



IP PBX 1 configuration
IP Address : 192.168.1.10

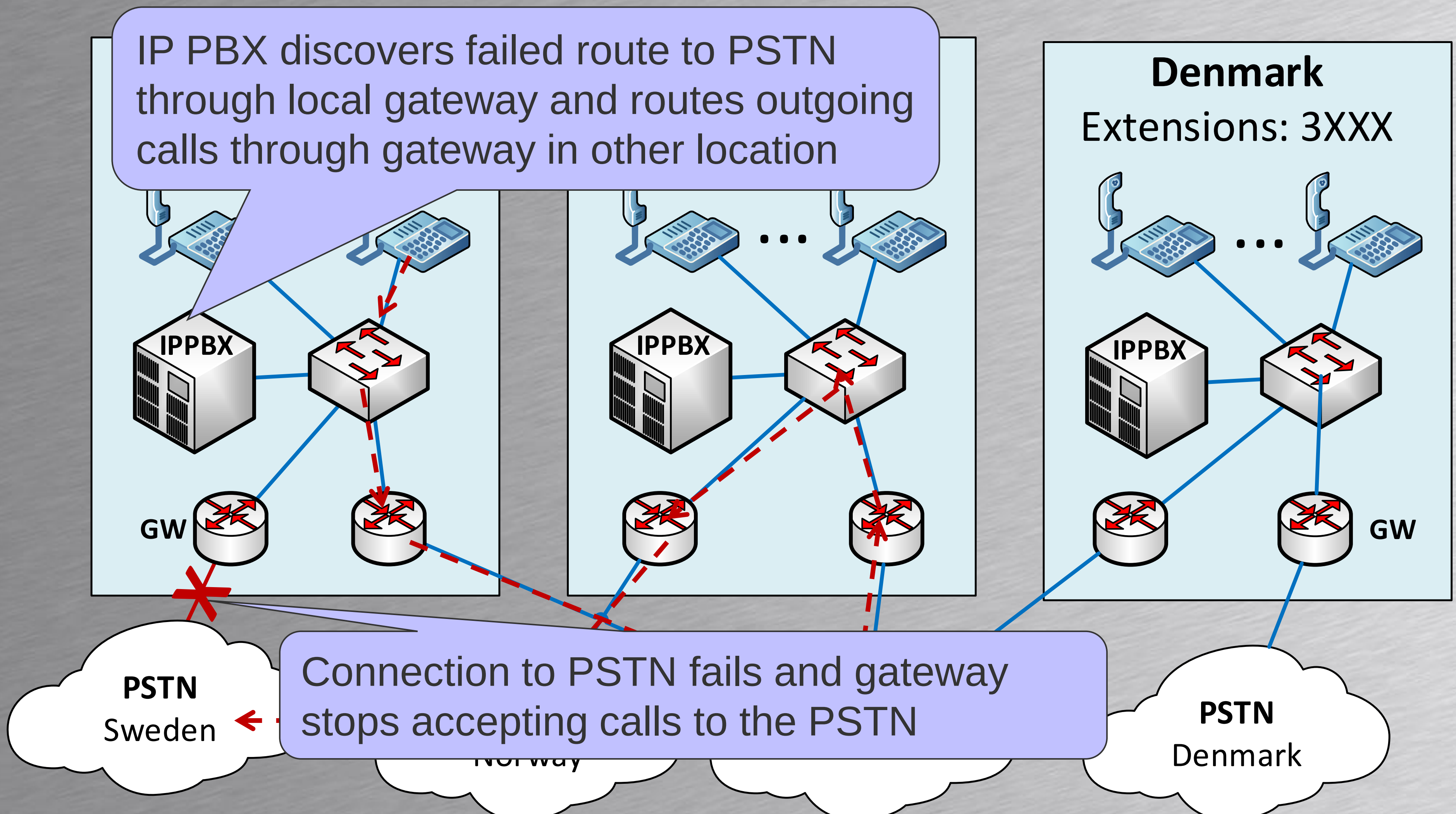
Registered phones
EXT: 101, 102, 103 and 104

IP PBX 2 configuration
IP Address : 192.168.1.11

Registered phones
EXT: 101, 102, 103 and 104

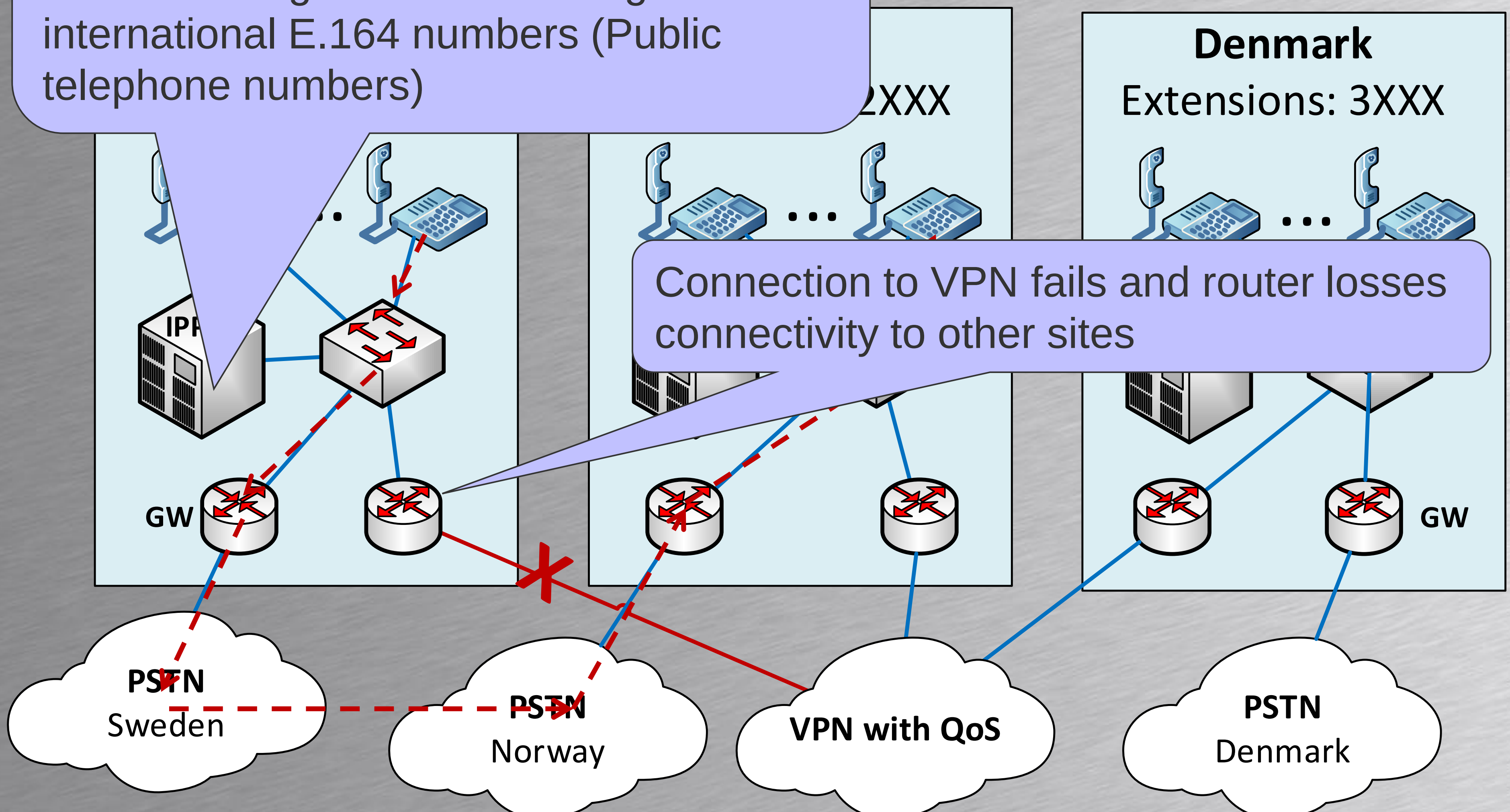
PSTN failover

- Rerouting calls to the PSTN



VPN failover

IP PBX discovers it cant reach IP PBX or IP phones in the other locations it routes the call through the PSTN using international E.164 numbers (Public telephone numbers)

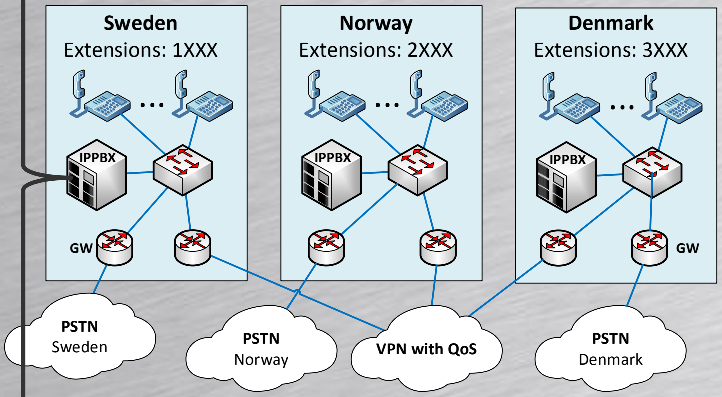


Connection to VPN fails and router losses connectivity to other sites

Route plans

- The individual IP PBX's are programmed with route plans
  - Example of Swedish route plan shown
    - Dialed 1xxx – x meaning any digit
    - Dialed 0. - . Meaning routed through
    - Pri = Priority. Lowest priority best. If unavailable try next

Dialed	Pri	Routed to
1xxx		Not routed processed locally
2xxx	1	The IP address of IP PBX in Norway
2xxx	2	The IP address of IP gateway in Sweden (Failover) Add 0047 for Norway + main-number + 2xxx (DiD)
3xxx	1	The IP address of IP PBX in Denmark
3xxx	2	The IP address of IP gateway in Sweden (Failover) Add 0045 for Denmark + main-number + 3xxx (DiD)
0.	1	The IP address of IP gateway in Sweden Line out – new dial tone from PSTN



VPN failover