

5. přednáška

**H.323 – deštník
pro celou škálu
protokolů**

Co si ověřuje CUCM?

```
Internet Protocol Version 4, Src: 192.168.1.254 (192.168.1.254), Dst: 192.168.1.1 (192.168.1.1)
Transmission Control Protocol, Src Port: cisco-sccp (2000), Dst Port: 50752 (50752), Seq: 1, Ack: 273
Skinny Client Control Protocol
  Data length: 24
  Header version: Basic (0x00000000)
  Message ID: RegisterAckMessage (0x00000081)
  Keep-alive interval: 30
  Date template: M/D/YA
  Secondary keep-alive interval: 60
```

O čem informuje telefon CUCM?

```
Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.254 (192.168.1.254)
Transmission Control Protocol, Src Port: 50202 (50202), Dst Port: cisco-sccp (2000), Seq: 13, A
Skinny Client Control Protocol
```

```
Data length: 12
Header version: Basic (0x00000000)
Message ID: OffHookMessage (0x00000006)
Line instance: 0
Call identifier: 0
```

```
Internet Protocol Version 4, Src: 192.168.1.254 (192.168.1.254), Dst: 192.168.1.1 (192.168.1.1)
Transmission Control Protocol, Src Port: cisco-sccp (2000), Dst Port: 50202 (50202), Seq: 13, A
Skinny Client Control Protocol
```

```
Data length: 28
Header version: Basic (0x00000000)
Message ID: CallStateMessage (0x00000111)
Call state: OffHook (1)
Line instance: 1
Call identifier: 13
```

O čem informuje CUCM volanou stanicí?

```
Internet Protocol Version 4, Src: 192.168.1.254 (192.168.1.254), Dst: 192.168.1.3 (192.168.1.3)  
Transmission Control Protocol, Src Port: cisco-sccp (2000), Dst Port: 51052 (51052), Seq: 13, A  
Skinny Client Control Protocol
```

```
Data length: 28  
Header version: Basic (0x00000000)  
Message ID: CallStateMessage (0x00000111)  
Call state: RingIn (4)  
Line instance: 1  
Call identifier: 14
```

```
Internet Protocol Version 4, Src: 192.168.1.254 (192.168.1.254), Dst: 192.168.1.3 (192.168.1.3)  
Transmission Control Protocol, Src Port: cisco-sccp (2000), Dst Port: 51052 (51052), Seq: 49, A  
Skinny Client Control Protocol
```

```
Data length: 48  
Header version: Basic (0x00000000)  
Message ID: DisplayPromptStatusMessage (0x00000112)  
Message time-out: 0  
Display message: \200\027: 4755001  
Line instance: 1  
Call identifier: 14
```

Co musíme otevřít, aby mohl proběhnout telefonní hovor?

```
Internet Protocol Version 4, Src: 192.168.1.254 (192.168.1.254), Dst: 192.168.1.3 (192.168.1.3)
Transmission Control Protocol, Src Port: cisco-sccp (2000), Dst Port: 51052 (51052), Seq: 885,
Skinny Client Control Protocol
  Data length: 72
  Header version: Basic (0x00000000)
  Message ID: OpenReceiveChannel (0x00000105)
  Conference ID: 4
  Pass-thru party ID: 0
  MS/packet: 20
  Payload capability: G.711 u-law 64k (4)
  Echo-cancel type: Media_EchoCancellation_On (1)
  G723 bitrate: Media_G723BRate_6_4 (2)
```

```
Internet Protocol Version 4, Src: 192.168.1.3 (192.168.1.3), Dst: 192.168.1.254 (192.168.1.254)
Transmission Control Protocol, Src Port: 51052 (51052), Dst Port: cisco-sccp (2000), Seq: 105,
Skinny Client Control Protocol
  Data length: 24
  Header version: Basic (0x00000000)
  Message ID: OpenReceiveChannelAck (0x00000022)
  Opened receive-channel status: orcOk (0)
  IP address: 192.168.1.3 (192.168.1.3)
  Port number: 27368
  Pass-thru party ID: 0
```

K čemu slouží tento paket?

```
Internet Protocol Version 4, Src: 192.168.1.254 (192.168.1.254), Dst: 192.168.1.3 (192.168.1.3)
Transmission Control Protocol, Src Port: cisco-sccp (2000), Dst Port: 51052 (51052), Seq: 985,
Skinny Client Control Protocol
  Data length: 88
  Header version: Basic (0x00000000)
  Message ID: StartMediaTransmission (0x0000008a)
  Conference ID: 4
  Pass-thru party ID: 0
  Remote IP address: 192.168.1.1 (192.168.1.1)
  Remote port: 25438
  MS/packet: 20
  Payload capability: G.711 u-law 64k (4)
  Precedence: 0
  Silence suppression: Media_SilenceSuppression_Off (0x00000000)
  Max frames per packet: 0
  G723 bitrate: Media_G723BRate_6_4 (2)
```

Obsah

1. Základní informace
2. Protokol RAS
3. Protokol H.225
4. Protokol H.245
5. Evoluce H.323
6. Příklad konfigurace na Cisco

1. Základní informace

K popisu H.323 je použita ASN.1

- Notace ASN.1 zavádí jednoznačnou klasifikaci jednotlivých objektů a metody pro definice jejich vlastností v textové i číselné formě. Tento jazyk je definován v doporučení ITU X.208 a návazných X.680 a X.683. Je určen pro zápisy dobře čitelné pro člověka.
- Jazyk ASN.1 definuje typy, což jsou pojmenované množiny hodnot. Jako příklad lze uvést typ BOOLEAN s množinou hodnot TRUE a FALSE. Identifikátor typu má syntax podobnou Fortranu či jazyku C a pořadí zápisu jako COBOL či PL/I. Jako příklad lze uvést deklaraci proměnné INTEGER.

Příklad popisu objektu v ASN.1

```
OSOBA ::= SEQUENCE {  
    prijmeni    Prijmeni,  
    jmeno       Jmeno,  
    pohlavi     Pohlavi }
```

```
Prijmeni ::= IAString,  
Jmeno     ::= IAString,  
Pohlavi   ::= BOOLEAN }
```

Příklad zápisu ASN.1 pro prvky H.323

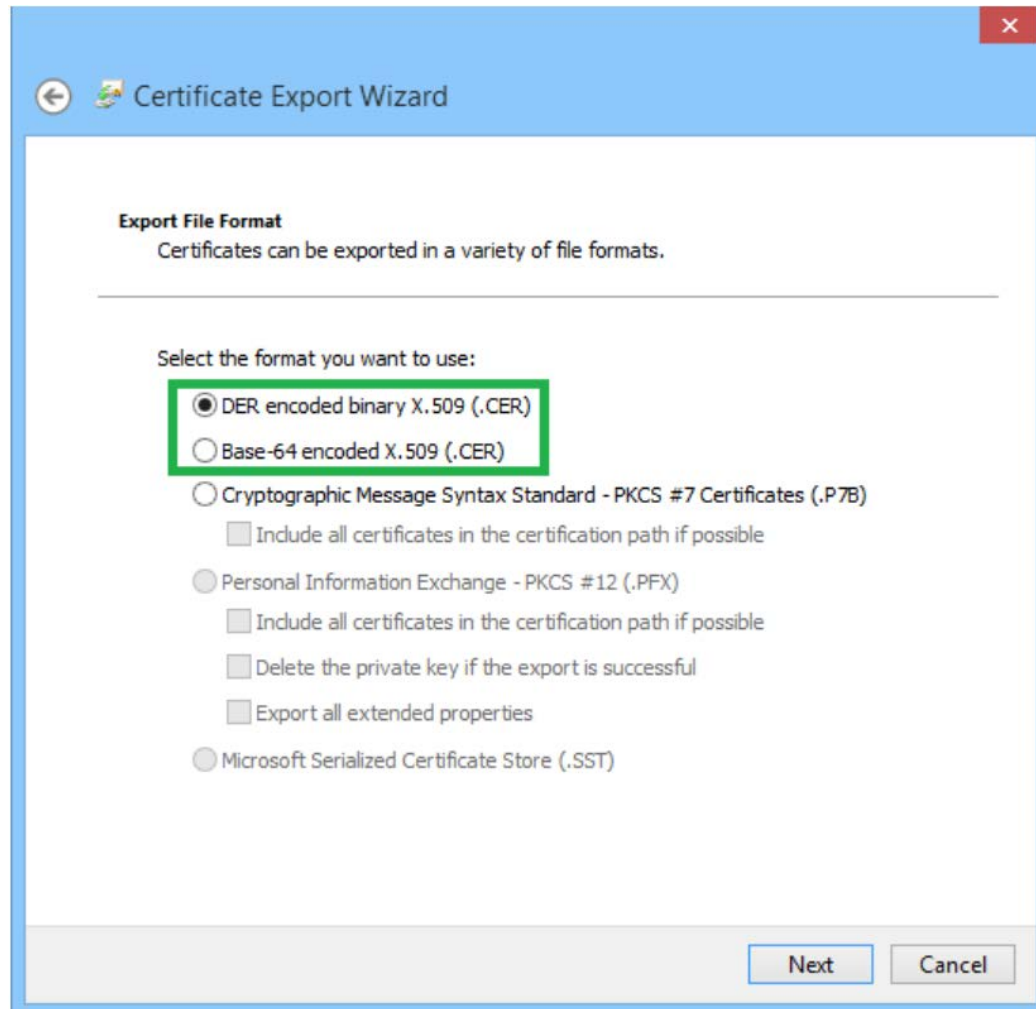
(blíže <http://www.itu.int/ITU-T/formal-language/itu-t/h/h225-0/2009/H323-MESSAGES.html>)

```
H323-UU-PDU ::= SEQUENCE {
  h323-message-body
    CHOICE {setup          Setup-UUIE,
             callProceeding CallProceeding-UUIE,
             connect       Connect-UUIE,
             alerting      Alerting-UUIE,
             information    Information-UUIE,
             releaseComplete ReleaseComplete-UUIE,
             facility       Facility-UUIE,
             ...,
             progress      Progress-UUIE,
             empty         NULL, -- used when a Facility message is sent,--
             -- but the Facility-UUIE is not to be invoked
             -- (possible when transporting supplementary
             -- services messages in versions prior to
             -- H.225.0 version 4). Also used as specified
             -- in H.323 to send messages that are not
             -- call related.
             status        Status-UUIE,
             statusInquiry StatusInquiry-UUIE,
             setupAcknowledge SetupAcknowledge-UUIE,
             notify        Notify-UUIE},
  nonStandardData          NonStandardParameter OPTIONAL,
  ...,
  ...
}
```

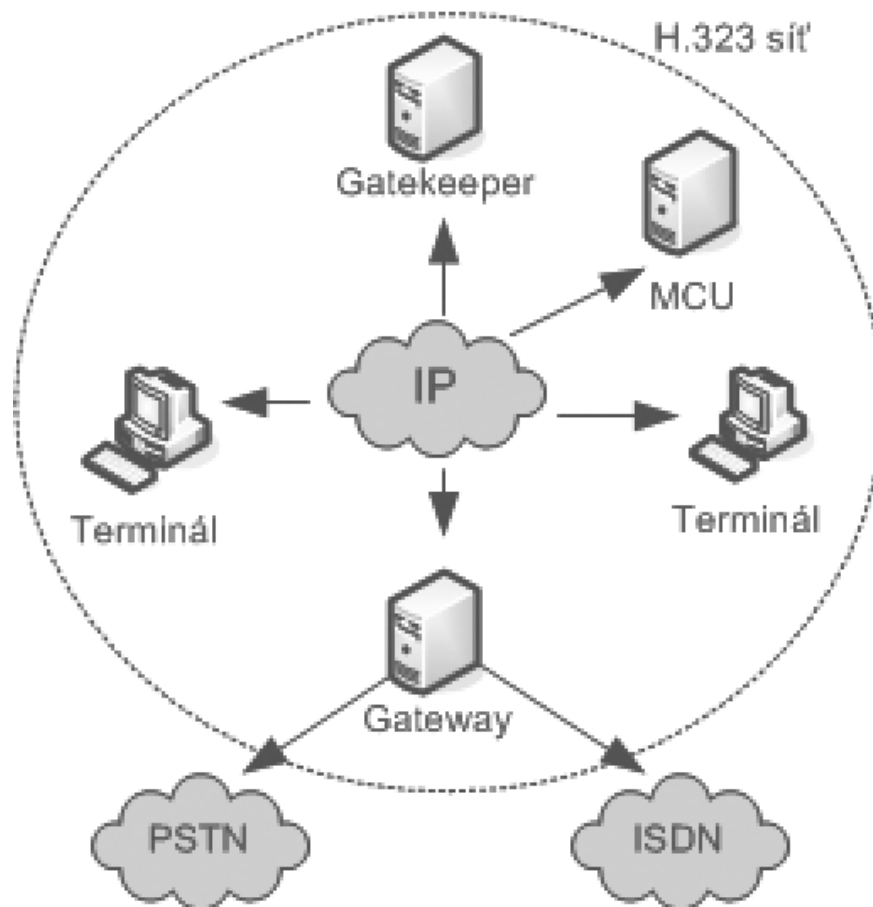
Pro zakódování je použita specifikace PER (Packed Encoding Rules), daná doporučením ITU-T Recommendation X.691. Jméno specifikace bylo vybráno pro rozlišení od jednodušší specifikace BER (Basic Encoding Rules).

S DER jste se už purčitě potkali.
Kde?

DER



Struktura sítě podle H.323

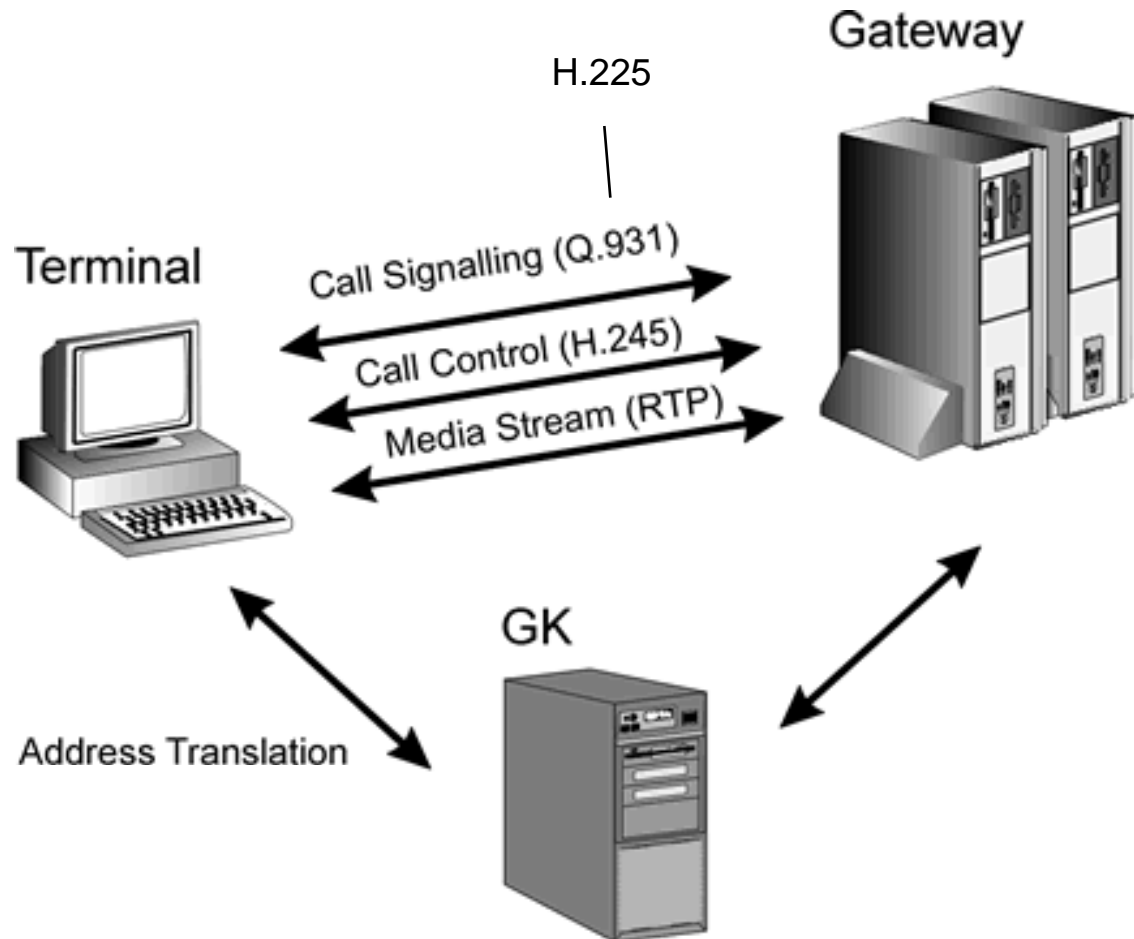


Žargon H.323

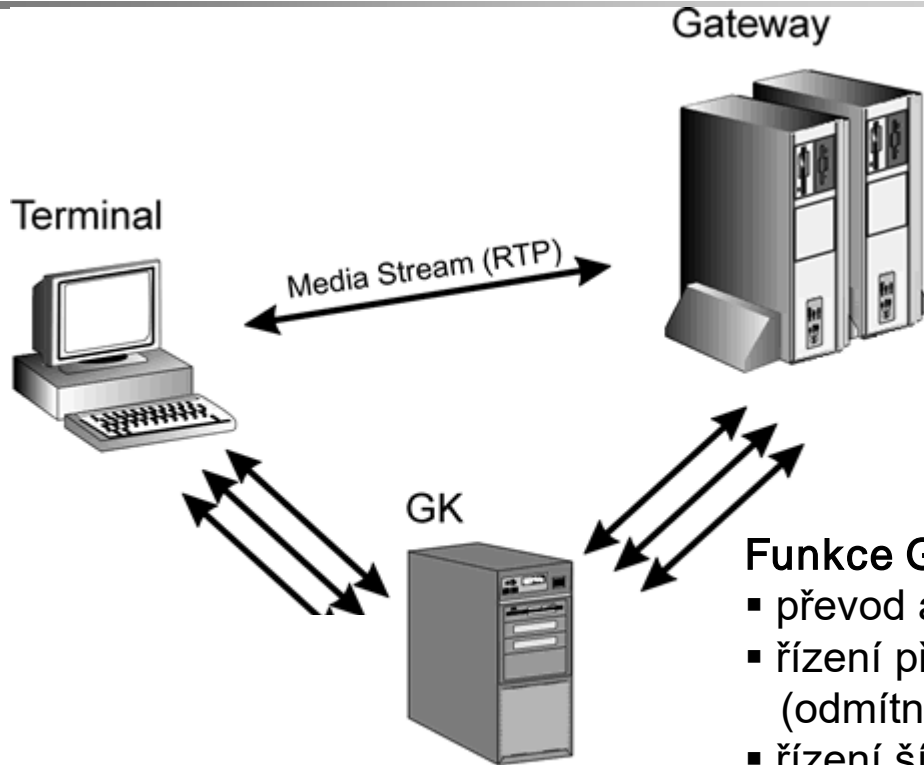
(základní komponenty sítě)

- **terminál** je základní a jedinou povinnou komponentou H.323 sítě. Používá se pro obousměrnou komunikaci v reálné čase. Terminál představuje např. PC, VoIP/videotelefon, hlasový odpovídač, voicemail;
 - **brána** (gateway) zabezpečuje spojení s jinou sítí (např. ISDN). Slouží jako případný překladač protokolů mezi různými sítěmi;
 - **gatekeeper** (volitelný, ale užitečný prvek) umožňující ve specifikované zóně směrování a centrální management koncových bodů sítě, čímž mohou chránit svoji zónu před zahlcením, lze je použít i pro autentizaci, autorizaci, převod jmen a telefonních čísel na IP adresy. V analogii s PSTN se jedná o inteligentní ústřednu;
 - **MCU** (Multipoint Control Unit) je zařízení, které zajišťuje komunikaci mezi třemi a více terminály. Směšuje datové toky a rozesílá je všem účastníkům ve skupině; umožňuje tedy pořádání konferenčních hovorů.
- Doména působení protokolu H.323 může obsahovat libovolné množství terminálů, bran nebo MCU jednotek, vždy však pouze jednoho gatekeepera. Mluvíme pak o tzv. H.323 zóně. Signalizace může probíhat přímo mezi koncovými uzly (terminály, bránami) nebo pomocí gatekeeperu.

Signalizace terminálu



Funkce Gatekeeperu



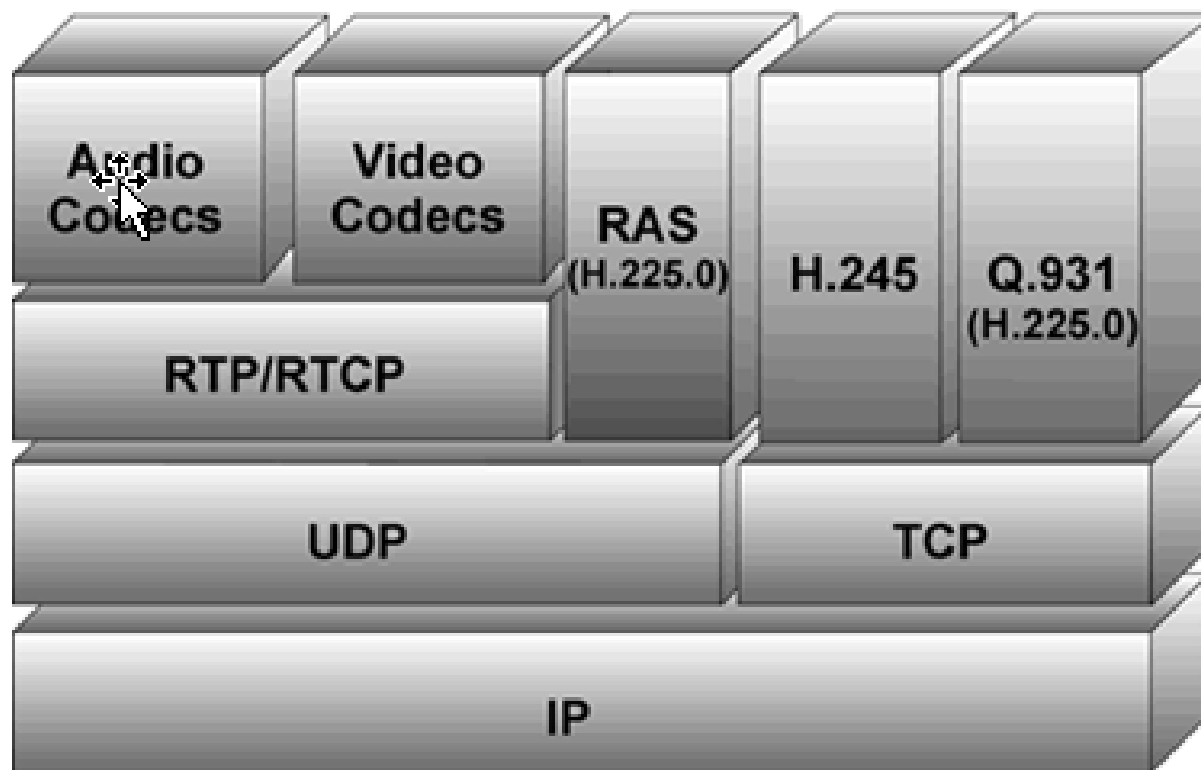
Funkce GK:

- převod adres E.164 na IP adresy
- řízení přístupu
(odmítnutí zpřístupnění zprávou ARJ – Admission Reject)
- řízení šířky pásma (RAS)
- správa zón
- případně
 - správa hovorů (je obsazeno?)
 - opravňování (např. od 8 do 16 hod.)
 - správa šířky pásma
(např. pokud není k dispozici, není hovor povolen)

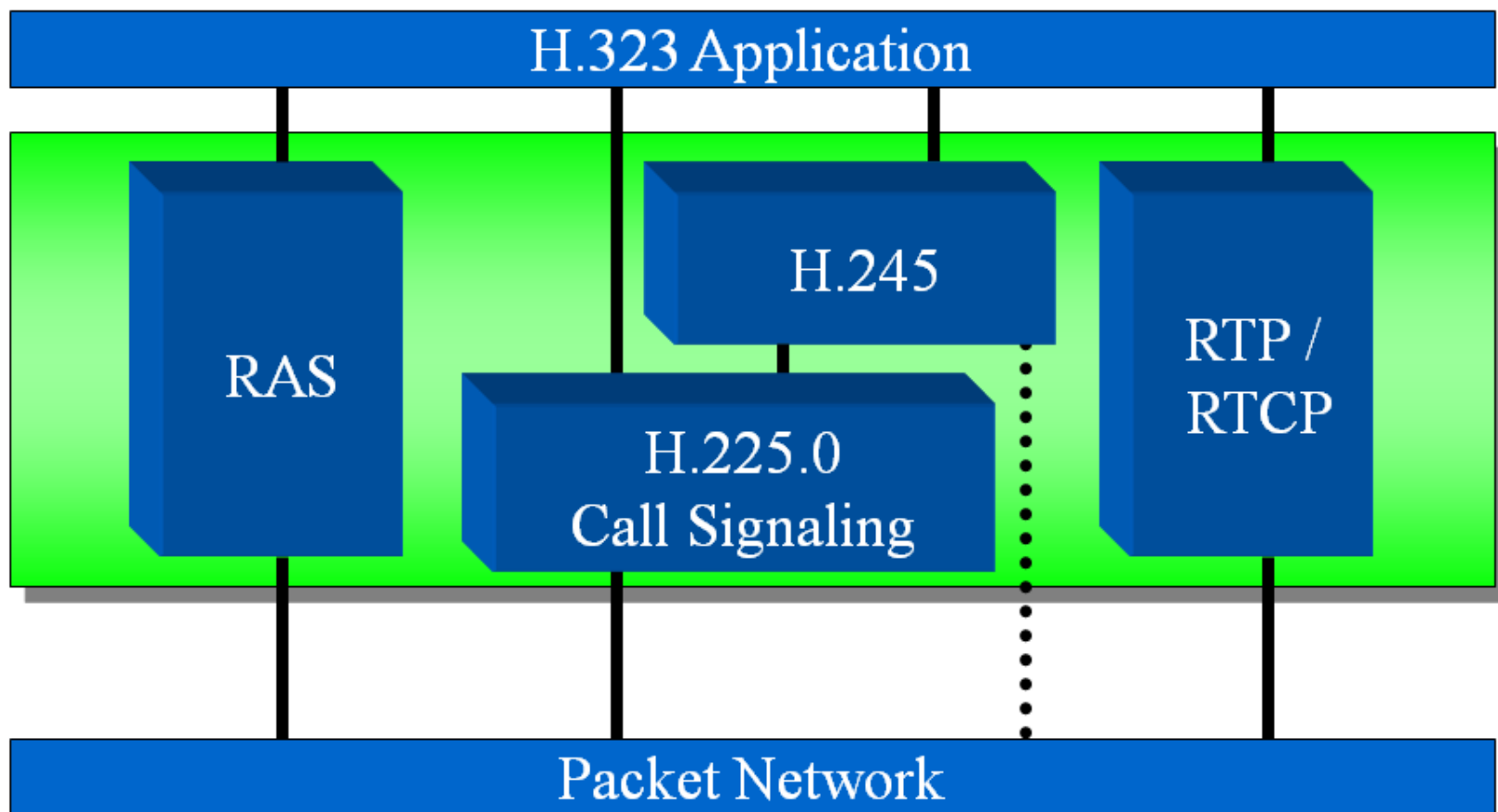
Vícebodová kontrolní jednotka (Multipoint Control Unit – MCU)

- Zodpovídají za řízení vícebodové konference.
- Skládají se ze dvou logických entit a sice vícebodového řadiče (MC) a vícebodového procesoru (MP).
- Z praktického hlediska je MCU konferenční most odlišný od těch běžně používaných ve veřejných komutovaných telefonních sítích. Hlavním rozdílem je to, že H.323 MCU je schopný směřovat a přepínat **nejen audio, ale i video** na rozdíl od běžného směšování audia běžnými konferenčními mosty.
- Některé MCU umožňují spolupráci dat z více bodů. Což pro koncového uživatele znamená to, že díky přenosu videa prostřednictvím H.323 MCU je uživatel schopen vidět všechny ostatní účastníky konference a ne jen pouze slyšet jejich hlasy.

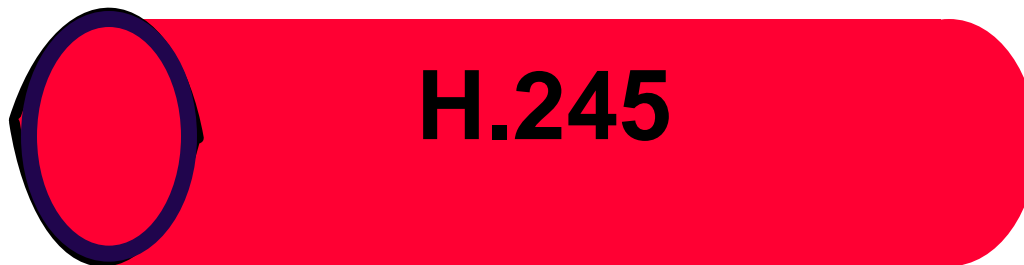
Protokolový zásobník



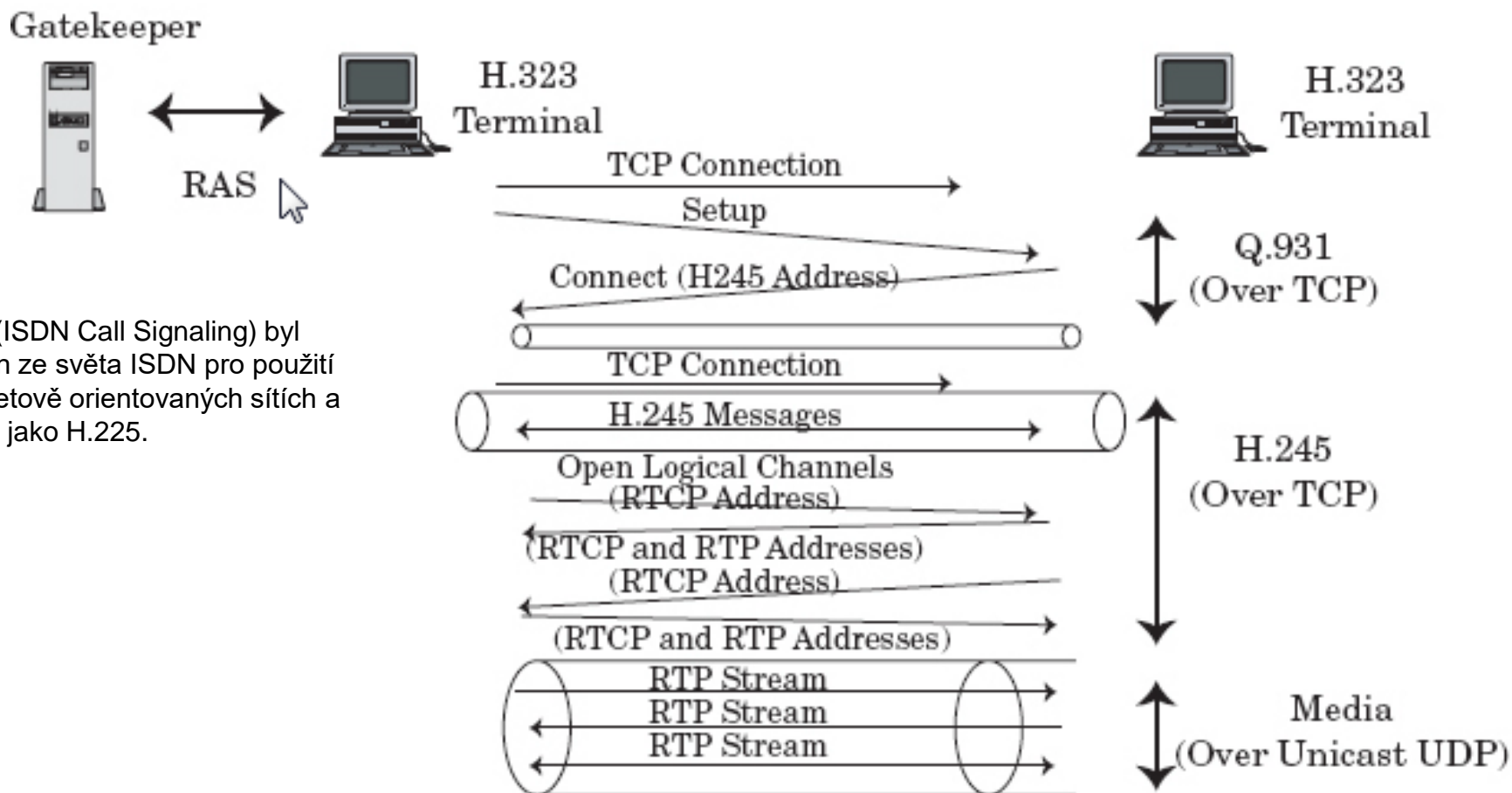
Klíčové protokoly této sady



Protokolové roury



Návaznosti jednotlivých protokolů



Q.931 (ISDN Call Signaling) byl upraven ze světa ISDN pro použití na paketově orientovaných sítích a nazván jako H.225.

2. Protokol RAS

(Registration, Admission, Status)

Zprávy RAS jsou zabaleny do UDP a používají port 1719

Internet Protocol Version 4, Src: 192.168.16.23 (192.168.16.23), Dst: 192.168.16.1
User Datagram Protocol, Src Port: 49301 (49301), Dst Port: h323gatestat (1719)

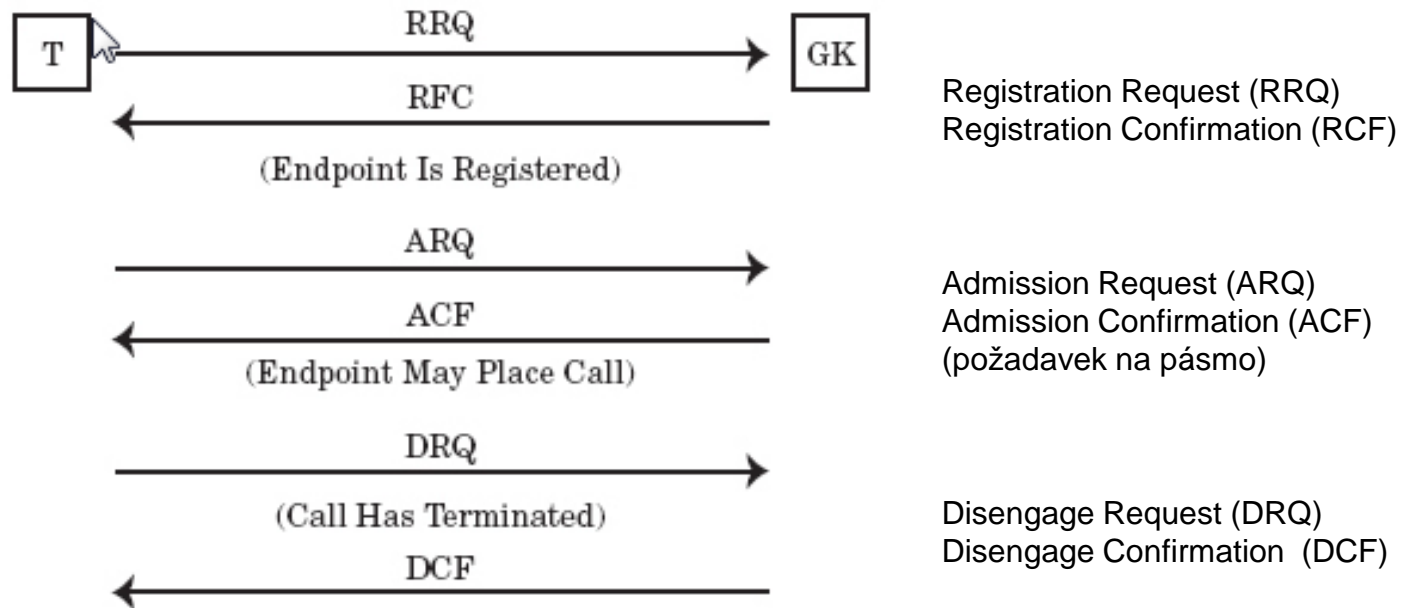
H.225.0 RAS

- ▣ RasMessage: gatekeeperRequest (0)
 - ▣ gatekeeperRequest
 - requestSeqNum: 2
 - protocolIdentifier: 0.0.8.2250.0.5 (Version 5)
 - ▣ nonStandardData
 - ⊕ nonStandardIdentifier: object (0)
 - data: 3 octets
 - ▣ Data (3 bytes)
 - Data: 850140
 - [Length: 3]
 - ▣ rasAddress: ipAddress (0)
 - ▣ ipAddress

000	00	04	0d	e3	e3	d5	00	09	6e	05	cb	11	08	00	45	88	n.....E.
010	01	52	01	4a	00	00	40	11	d6	60	c0	a8	10	17	c0	a8	.R.J..@.
020	10	01	c0	95	06	b7	01	3e	85	6c	03	20	00	01	06	00>..]
030	08	91	4a	00	05	00	0a	60	86	48	01	86	f8	72	04	02	..J.....	.H...r..
040	01	03	85	01	40	00	c0	a8	10	17	c0	95	02	00	01	03@...
050	00	44	44	44	41	2b	10	80	b1	01	90	00	0a	60	86	48	.DDDA+..H
060	01	86	fc	0b	01	06	02	00	04	00	c5	34	64	5e	f9	4a4d^..J
070	da	22	a0	bc	c4	4a	e9	1e	0c	3a	0d	1e	2c	a8	4a	7c	.."....J..,..J
080	55	40	8a	34	81	8e	4b	5d	f9	86	44	07	82	00	a8	04	U@.4..K]	..D.....
090	be	7c	d9	37	3f	d0	34	34	65	f4	ed	d0	3f	2d	40	2c	.. .7?.44	e...?-@,

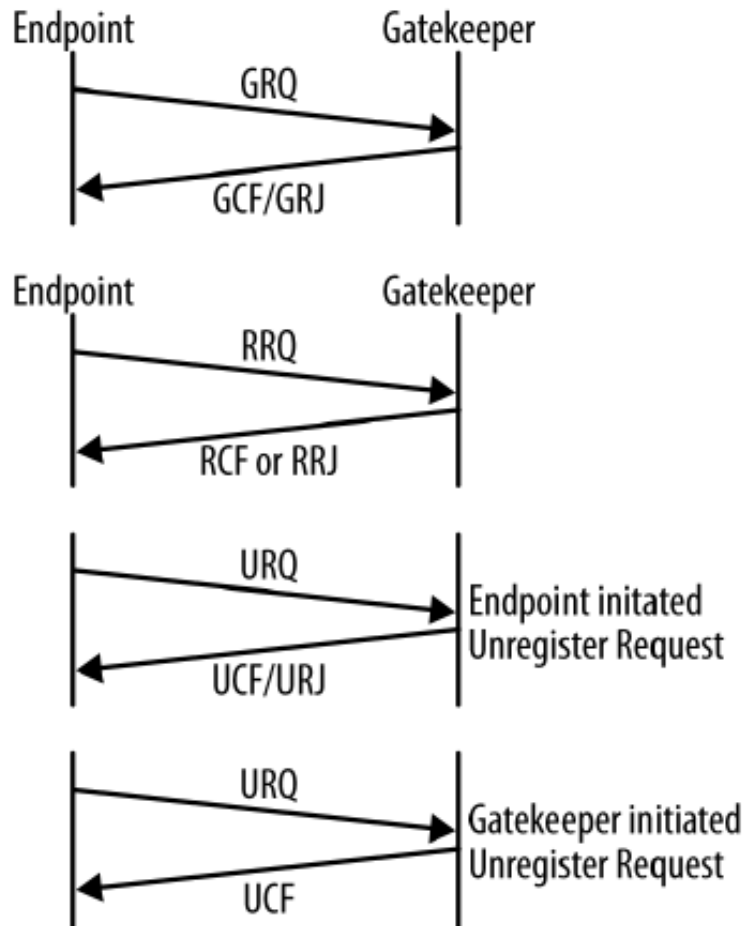
RAS

Protokol RAS (Registration, Admission, Status) je protokol, jehož zprávy jsou umístěny do zpráv protokolu H.225 a slouží pouze při registraci a rušení hovoru. Používá se pro komunikaci gatekeeper – endpoint a naopak. Zde máme požadavek na registraci, který je potvrzen či odmítnut.



Pro unicast je určen UDP port 1719 a pro multicast UDP port 1718 25

Telefon si najde GK, pak se registruje a odregistruje



Pole CryptoToken ve zprávě RRQ

cryptoTokens: 2 items

Item 0

Item: cryptoEPPwdHash (0)

cryptoEPPwdHash

alias: h323-ID (1)

h323-ID: 950012315 ————— **ochrana proti přehrávání**

timeStamp: Feb 26, 2006 15:36:41.000000000

token

algorithmOID: 1.2.840.113549.2.5 (md5)

paramS

hash: 8BB5DFAE1F23EA0AA5C7E73C23B18639

V poli CryptoToken jsou informace potřebné pro autentizaci
Druhá možnost použití tohoto pole je zpráva H.225.0 Q.931

Některé zprávy gatekeeperu

	Doba čekání na odpověď [s]	Počet pokusů
GRQ	5	2
RRQ	3	2
URQ	3	1
ARQ	5	2
BRQ	3	2
IRQ	3	1
IRR	5	2
DRQ	3	2
LRQ	5	2
RAI	3	2
SCI	3	2

Gatekeeper Request – GRQ (port 1718)
Hledání gatekeeperu

Gatekeeper Registration – RRQ
Registrace na dobu TTL

Unregister Request – URQ
Zrušení registrace

Admission Request – ARQ
Indikace požadavku na pásmo

Bandwidth Request – BRQ
Vyžádání si změny šířky pásma

Information Request – IRQ
Vyžádání detailních informací o voláních

Disengage Request – DRQ
Vyžádání informací potřebných pro účtování

Location Request – LRQ
Např. pošli IP adresu tohoto čísla.

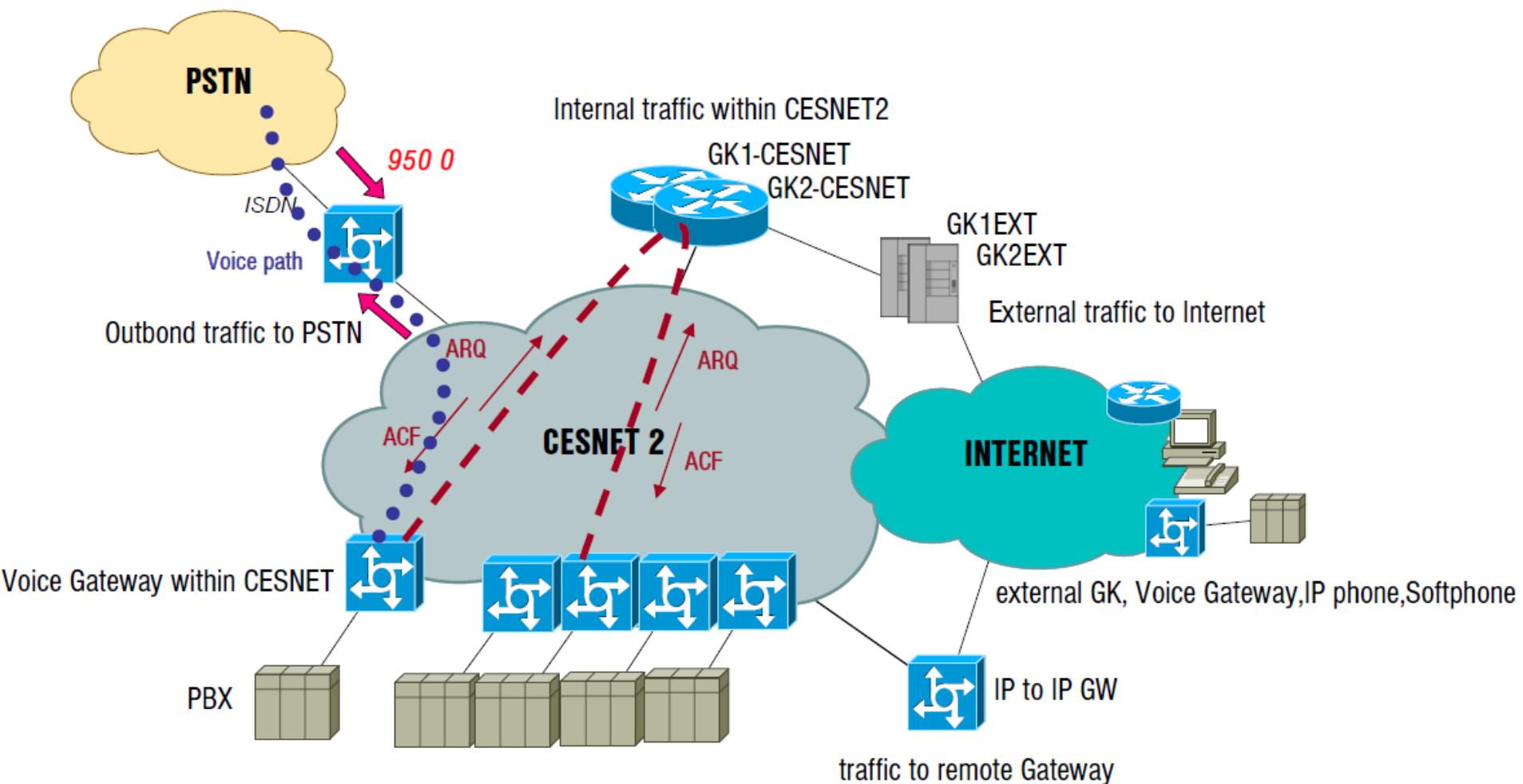
Resource Availability – RAI
Jsme blízko limitu zdrojů?

Service Control Indication – SCI
Vyžádání si některého typu služby

Popis příkazu ARQ v ASN.1

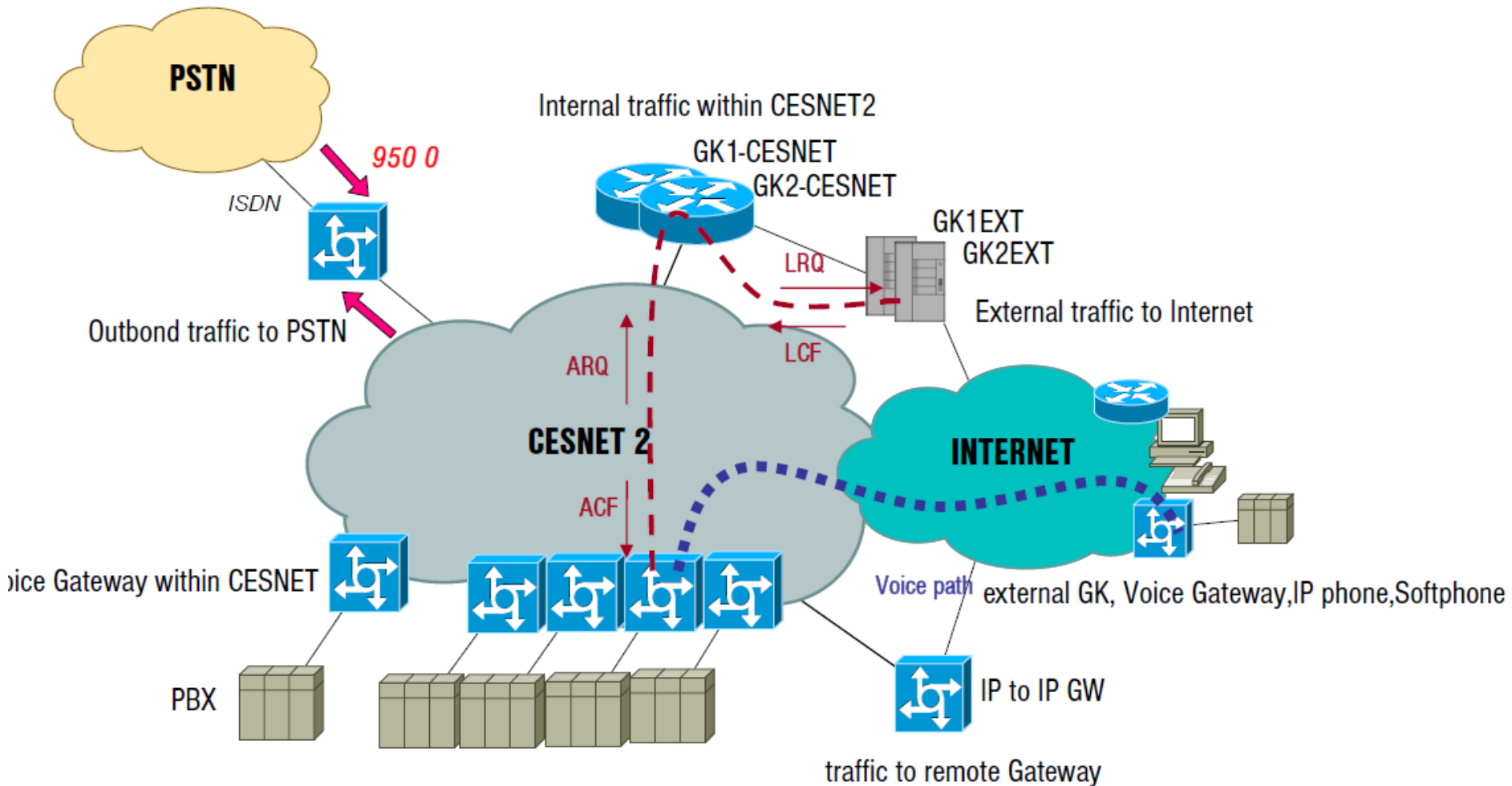
```
AdmissionRequest ::= SEQUENCE --(ARQ)
{
    requestSeqNum          RequestSeqNum,
    callType               CallType,
    callModel              CallModel OPTIONAL,
    endpointIdentifier     EndpointIdentifier,
    destinationInfo       SEQUENCE OF AliasAddress OPTIONAL,
    destCallSignalAddress TransportAddress OPTIONAL,
    destExtraCallInfo     SEQUENCE OF AliasAddress OPTIONAL,
    srcInfo                SEQUENCE OF AliasAddress,
    srcCallSignalAddress  TransportAddress OPTIONAL,
    bandwidth              BandWidth,
    callReferenceValue    CallReferenceValue,
    nonStandardData       NonStandardParameter OPTIONAL,
    callServices           QseriesOptions OPTIONAL,
    conferenceID          ConferenceIdentifier,
    activeMC              BOOLEAN,
    answerCall            BOOLEAN, -- answering a call
    ...,
    canMapAlias           BOOLEAN, -- can handle alias address
    callIdentifier        CallIdentifier,
    srcAlternatives       SEQUENCE OF Endpoint OPTIONAL,
    destAlternatives      SEQUENCE OF Endpoint OPTIONAL,
    gatekeeperIdentifier  GatekeeperIdentifier OPTIONAL,
    tokens                SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens          SEQUENCE OF CryptoH323Token OPTIONAL,
    integrityCheckValue   ICV OPTIONAL,
    transportQOS          TransportQOS OPTIONAL,
    willSupplyUUIEs      BOOLEAN,
    callLinkage           CallLinkage OPTIONAL,
    gatewayDataRate      DataRate OPTIONAL,
    capacity              CallCapacity OPTIONAL,
    circuitInfo          CircuitInfo OPTIONAL,
    desiredProtocols     SEQUENCE OF SupportedProtocols OPTIONAL,
    ...
}
```

Příklad použití ARQ a ACF



Příklad použití LRQ a LCF

(externí spojení přes hraniční GW)



Časové omezení registrace a její prodlužování – příklad: CESNET

- Registrace EP (Endpoint - H.323 telefon nebo H323 brána) je na GK časově omezená. GK vrací při registraci každému EP dobu platnosti registrace ve zprávě RFC (Registration Confirm), která je zapsána v poli *TTL*. Po vypršení této doby je registrace zrušena.
- Každý EP by měl svou registraci periodicky obnovovat zasíláním **RRQ** (Registration Request).
- Je povoleno obnovování TTL pomocí **lightweight RRQ**, tzn. pomocí bitu *keepAlive*, to probíhá tak, že před uplynutím platnosti registrace na GK zašle EP zprávu RRQ s *keepAlive*, čímž resetuje čítač TTL a registrace je prodloužena.
- EP může požadovat i menší čas *timeToLive* ve zprávě RRQ, než má GK jako default. Aby nedošlo k zahlcení RRQ zprávami, tak GK vrací jako nejmenší limitní čas pro registraci *60 sekund*, i kdyby EP požadoval nižší.

Nastavení TTL na Gatekeeperu

```
[Gatekeeper::Main]
```

```
Fourtytwo=42
```

```
Name=gk1ext
```

```
Home=195.113.222.2
```

```
TimeToLive=300
```

```
StatusTraceLevel=3
```

```
EndpointIDSuffix=_gk1ext
```

A co když doba registrace vyprší?

- Po expiraci registrace na GK zašle GK dvě zprávy **IRQ** (Information Request), kterými zjistí, zda je EP komunikativní.
- Pokud nedostane odpověď zprávou **IRR** (Information Response), kterou může být registrace prodloužena, tak posílá na endpoint **URQ** (Unregistration Request) s odůvodněním *ttlExpired*.
- V této chvíli je vymazán z databáze aktivních EP na GK a EP musí provést opětovnou registraci pomocí **RRQ**.
- GK má na zrušení registrace EP nastaveno *300 sec*.

Příklad

(zdroj: http://homel.vsb.cz/~voz29/files/voz_54.pdf)

EP obnovuje registraci zprávou RRQ a dostává potvrzení RCF

3749.159777 195.113.113.136 -> 195.113.222.2 H.225.0 RAS: registrationRequest

3749.163724 195.113.222.2 -> 195.113.113.136 H.225.0 RAS: registrationConfirm

EP byl nekorektně odpojen od sítě a neposlal URQ, čili se neodregistroval, GK posílá dvakrát IRQ a nedostává odpověď, ruší tedy registraci URQ a odstraňuje záznam o EP z aktivní databáze registrovaných EP na GK

3915.925904 195.113.222.2 -> 195.113.113.136 H.225.0 RAS: infoRequest

3976.525900 195.113.222.2 -> 195.113.113.136 H.225.0 RAS: infoRequest

4037.126022 195.113.222.2 -> 195.113.113.136 H.225.0 RAS: unregistrationRequest

Po půl hodině dojde k připojení EP a ten posílá RRQ, dostává zpět RCF a znovu je zaregistrován na GK

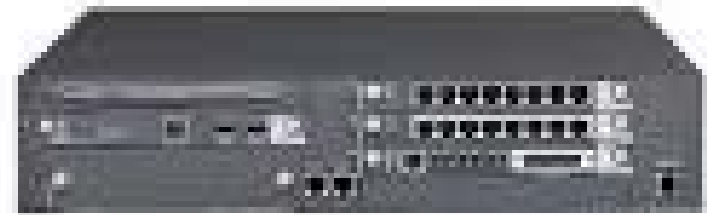
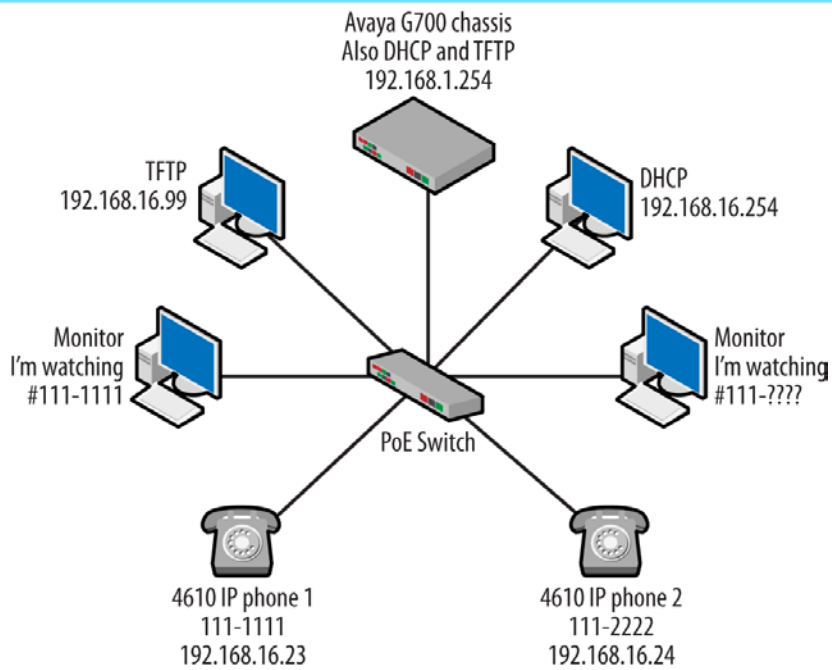
5606.461970 195.113.113.136 -> 195.113.222.2 H.225.0 RAS: registrationRequest

5606.466969 195.113.222.2 -> 195.113.113.136 H.225.0 RAS: registrationConfirm

Příklad menší sítě:

Registrace probíhá na obou terminálech

No.	Source	Destination	Protocol	Info
568	192.168.16.23	192.168.16.1	H.225.0	RAS: gatekeeperRequest
569	192.168.16.1	192.168.16.23	H.225.0	RAS: gatekeeperConfirm
570	192.168.16.23	192.168.16.1	H.225.0	RAS: registrationRequest
571	192.168.16.1	192.168.16.23	H.225.0	RAS: registrationConfirm



G700

589	192.168.16.24	192.168.16.1	H.225.0	RAS: gatekeeperRequest
591	192.168.16.1	192.168.16.24	H.225.0	RAS: gatekeeperConfirm
592	192.168.16.24	192.168.16.1	H.225.0	RAS: registrationRequest
593	192.168.16.1	192.168.16.24	H.225.0	RAS: registrationConfirm

RAS GRQ ID objektu, IP adresa, a port

Internet Protocol Version 4, Src: 192.168.16.23 (192.168.16.23), Dst: 192.168.16.1
User Datagram Protocol, Src Port: 49301 (49301), Dst Port: h323gatestat (1719)
H.225.0 RAS

[-] RasMessage: gatekeeperRequest (0)

[-] gatekeeperRequest

requestSeqNum: 2

protocolIdentifier: 0.0.8.2250.0.5 (Version 5)

Object ID v ASN.1

[-] nonStandardData

[-] nonStandardIdentifier: object (0)

object: 2.16.840.1.113778.4.2.1 (joint-iso-itu-t.16.840.1.113778.4.2.1)

data: 2 octets

[+] Data (3 bytes)

[-] rasAddress: ipAddress (0)

[-] ipAddress

ip: 192.168.16.23 (192.168.16.23)

port: 49301

[+] endpointType

[+] endpointAlias: 1 item

[+] tokens: 1 item

[+] authenticationCapability: 2 items

[+] algorithmOIDs: 2 items

[+] featureSet

Pole konfigurace EP

```
Internet Protocol Version 4, Src: 192.168.16.23 (192.168.16.23), Dst: 192.168.16.1
User Datagram Protocol, Src Port: 49301 (49301), Dst Port: h323gatestat (1719)
H.225.0 RAS
```

```
▣ RasMessage: gatekeeperRequest (0)
```

```
▣ gatekeeperRequest
```

```
requestSeqNum: 2
```

```
protocolIdentifier: 0.0.8.2250.0.5 (Version 5)
```

```
▣ nonStandardData
```

```
▣ rasAddress: ipAddress (0)
```

```
▣ endpointType
```

```
terminal
```

```
.0.. .... mc: False
```

```
..0. .... undefinedNode: False
```

```
▣ endpointAlias: 1 item
```

```
▣ Item 0
```

```
▣ AliasAddress: dialledDigits (0)
```

```
dialledDigits: 1111111
```

```
▣ tokens: 1 item
```

```
▣ authenticationCapability: 2 items
```

```
▣ algorithmOIDs: 2 items
```

```
▣ featureSet
```

[\[The response to this request is in frame 569\]](#)

mc – multipoint controller - nenastaven

```
000 00 04 0d e3 e7 d5 00 09 6e 05 cb 11 08 00 45 88 ..... n.....E.
010 01 52 01 4a 60 00 40 11 d6 60 c0 a8 10 17 c0 a8 .R.J..@. ....
020 10 01 c0 95 06 b7 01 3e 85 6c 03 20 00 01 06 00 ..J...> .l. ....
030 08 91 4a 06 05 00 0a 60 86 48 01 86 f8 72 04 02 ..J.... .H...r..
040 01 03 85 01 40 00 c0 a8 10 17 c0 95 02 00 01 03 .....@.... .H...
050 00 44 44 44 41 2b 10 80 b1 01 90 00 0a 60 86 48 .DDDA+.. .....H
060 01 86 fc 0b 01 06 02 00 04 00 c5 34 64 5e f9 4a ..... 4d^..J
070 da 22 a0 bc c4 4a e9 1e 0c 3a 0d 1e 2c a8 4a 7c .."....J... ..J|
```

RAS token pole žádosti

- ▣ tokens: 1 item
 - ▣ Item 0
 - ▣ ClearToken
 - tokenOID: 2.16.840.1.114187.1.6.2 (joint-iso-itu-t.16.840.1.114187.1.6.2)
 - ▣ dhkey
 - halfkey: c534645ef94ada22a0bcc44ae91e0c3a0d1e2ca84a7c5540... [bit length 1024]
 - ▣ profileInfo: 2 items
 - ▣ Item 0
 - ▣ ProfileElement
 - elementID: 2
 - ▣ element: octets (0)
 - octets: 0000489c
 - ▣ Item 1
 - ▣ ProfileElement
 - elementID: 1
 - ▣ element: octets (0)
 - octets: 6c89000010d2000008480000
 - ▣ authenticationCapability: 2 items
 - ▣ Item 0
 - ▣ AuthenticationMechanism: pwdSymEnc (1)
 - pwdSymEnc: NULL
 - ▣ Item 1
 - ▣ AuthenticationMechanism: keyExch (8)
 - keyExch: 2.16.840.1.114187.1.6.2 (joint-iso-itu-t.16.840.1.114187.1.6.2)
 - ▣ algorithmOIDs: 2 items
 - ▣ Item 0
 - algorithmOIDs item: 1.3.14.3.2.6 (desECB)
 - ▣ Item 1
 - algorithmOIDs item: 2.16.840.1.114187.1.3 (joint-iso-itu-t.16.840.1.114187.1.3)
 - ▣ featureSet

Začátek OID je specifický pro typ telefonu



autentizace



šifrování DES-ECB

Pole vlastností RAS žádosti

```
⊕ endpointAlias: 1 item
⊕ tokens: 1 item
⊕ authenticationCapability: 2 items
⊕ algorithmOIDs: 2 items
⊖ featureSet
  .... 0... replacementFeatureSet: False
  ⊖ supportedFeatures: 2 items
    ⊖ Item 0
      ⊖ FeatureDescriptor
        ⊖ id: oid (1)
        → oid: 2.16.840.1.114187.1.9 (joint-iso-itu-t.16.840.1.114187.1.9)
        ⊖ parameters: 1 item
          ⊖ Item 0
            ⊖ parameters item
              ⊖ id: standard (0)
                standard: 1
            ⊖ content: number8 (4)
                number8: 1
          ⊖ Item 1
            ⊖ FeatureDescriptor
              ⊖ id: oid (1)
              → oid: 2.16.840.1.114187.1.10 (joint-iso-itu-t.16.840.1.114187.1.10)
              ⊖ parameters: 6 items
                ⊖ Item 0
                  ⊖ parameters item
                    ⊖ id: standard (0)
                      standard: 1
                ⊕ Item 1
                ⊕ Item 2
                ⊕ Item 3
                ⊕ Item 4
                ⊕ Item 5
```


Potvrzení registrace (telefon teď může volat)

```
Internet Protocol Version 4, Src: 192.168.16.1 (192.168.16.1), Dst: 192.168.16.23
User Datagram Protocol, Src Port: h323gatestat (1719), Dst Port: 49301 (49301)
H.225.0 RAS
```

```
[-] RasMessage: registrationConfirm (4)
```

```
[-] registrationConfirm
```

```
requestSeqNum: 3
```

```
protocolIdentifier: 0.0.8.2250.0.5 (Version 5)
```

```
[+] nonStandardData
```

```
[-] callSignalAddress: 1 item
```

```
[-] Item 0
```

```
[-] TransportAddress: ipAddress (0)
```

```
[-] ipAddress
```

```
ip: 192.168.16.1 (192.168.16.1)
```

```
port: 1720
```

```
endpointIdentifier: .n
```

```
[+] alternateGatekeeper: 1 item
```

```
0... .... willRespondToIRR: False
```

```
[-] preGrantedARQ
```

```
.1... .... makeCall: True může hned volat
```

```
..1. .... useGKCallSignalAddressToMakeCall: True
```

```
...1 .... answerCall: True
```

```
.... 1... useGKCallSignalAddressToAnswer: True
```

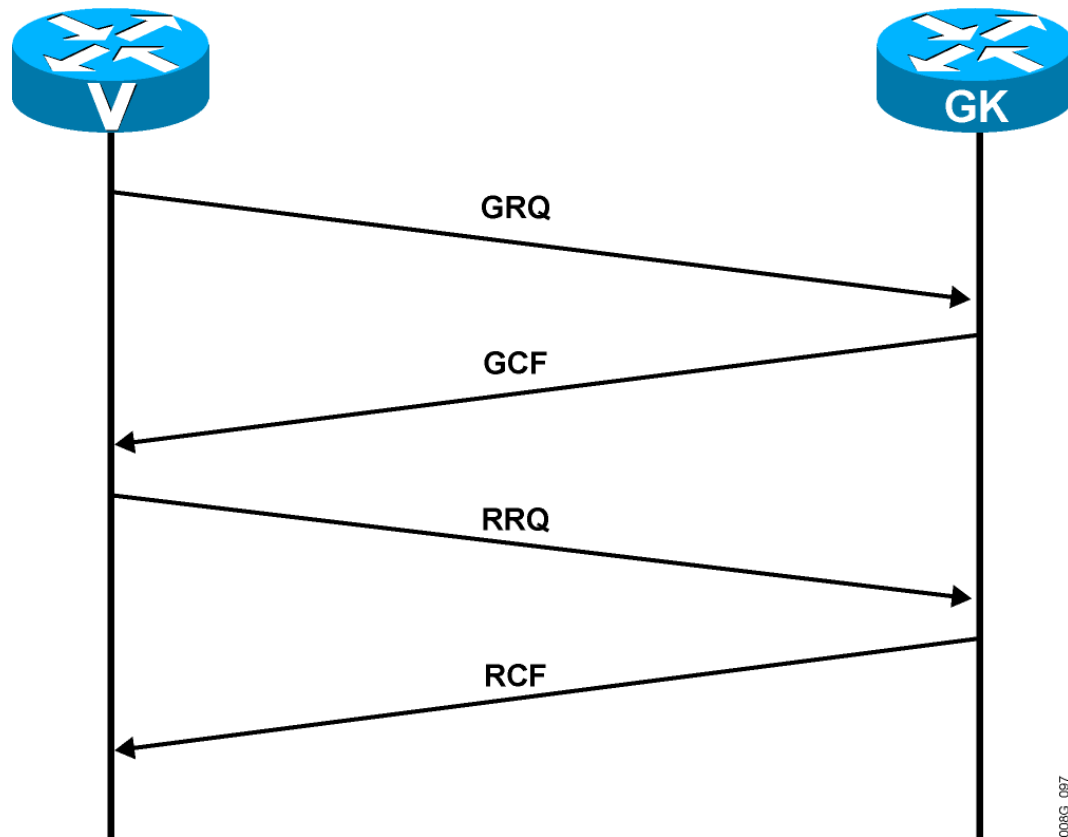
```
1... .... maintainConnection: True
```



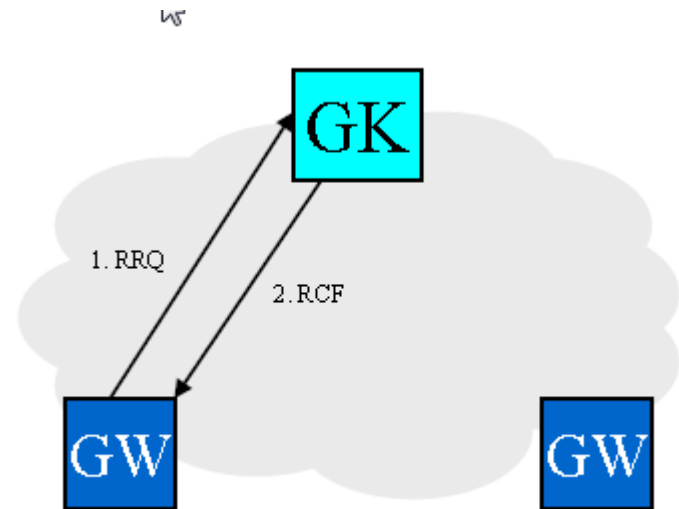
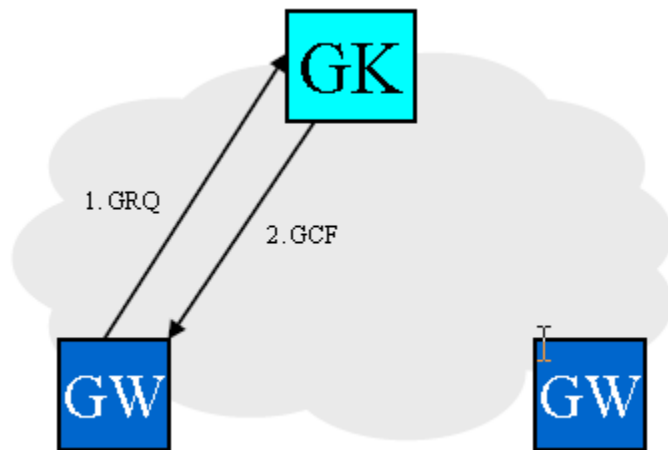
IP adresa, port



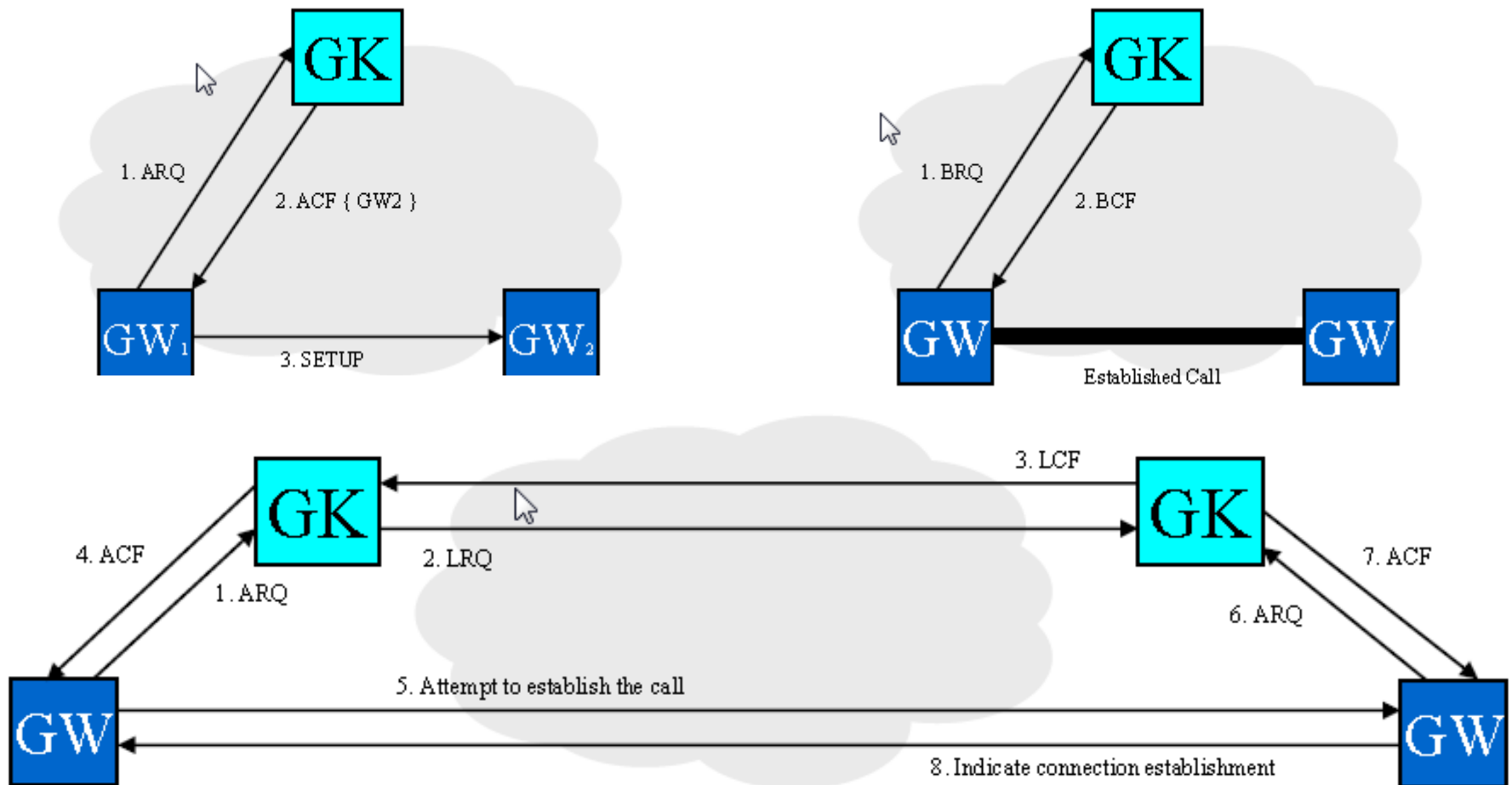
Nalezení GK a registrace telefonu



Reakce na zprávy GRQ a RRQ



Reakce na zprávy ARQ, BRQ a LRQ



Výpis výkonnostních statistik

```
Router# show gatekeeper performance stats

-----Gatekeeper Performance Statistics-----

Performance statistics captured since: 00:17:00 UTC
Mon Mar 14 2011

Gatekeeper level Admission Statistics:
  ARQs received: 1
  ARQs received from originating endpoints: 0
  ACFs sent: 1
  ACFs sent to the originating endpoint: 0
  ARJs sent: 0
  ARJs sent to the originating endpoint: 0
  ARJs sent due to overload: 0
  Number of concurrent calls: 0
  Number of concurrent originating calls: 0
Gatekeeper level Location Statistics:
  LRQs received: 1
  LRQs sent: 0
  LCFs received: 0
  LCFs sent: 1
  LRJs received: 0
  LRJs sent: 0
  LRJs sent due to overload: 0
Gatekeeper level Registration Statistics:
  RRJ due to overload: 0
  Total Registered Endpoints: 1
Gatekeeper level Disengage Statistics:
  DRQs received: 1
  DRQs sent: 0
  DCFs received: 0
```

3. Protokol H.225

<http://www.itu.int/rec/T-REC-H.225.0-200912-I/en>



International Telecommunication Union

ITU-T
TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.225.0
(12/2009)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS
Infrastructure of audiovisual services – Transmission
multiplexing and synchronization

**Call signalling protocols and media stream
packetization for packet-based multimedia
communication systems**

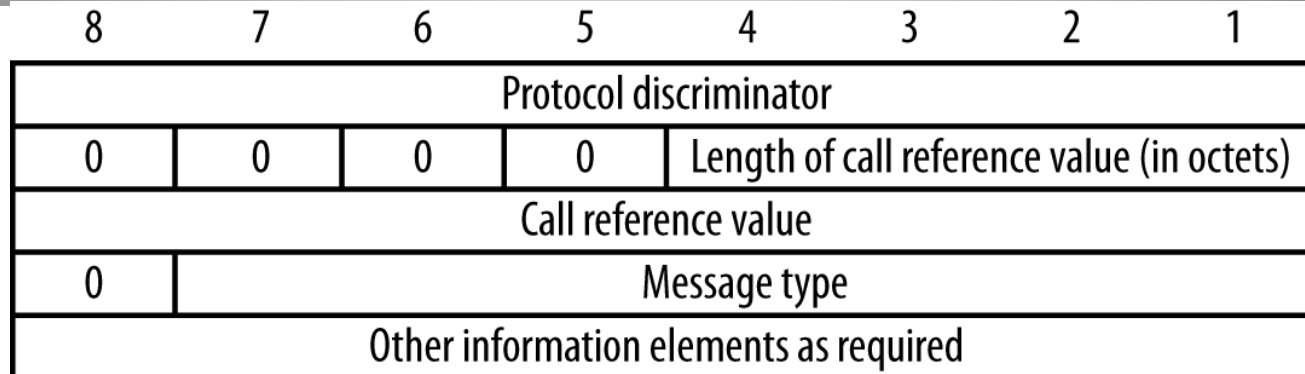
Recommendation ITU-T H.225.0



Protokol H.225

- Slouží pro sestavení spojení mezi dvěma koncovými body. Sestavení hovoru probíhá buď
 - přímo mezi koncovými zařízeními nebo
 - mezi koncovým zařízením a gatekeeperem
- Je odvozen od Q.931 (ISDN Call Signaling), ale byl upraven pro použití na paketově orientovaných sítích.
- Pro přenos na 4. vrstvě OSI se používá transportní protokol TCP

Formát záhlaví protokolu H.225



```
Internet Protocol Version 4, Src: 10.210.200.112 (10.210.200.112), Dst: 10.210.200.111 (10.210.200.111)
Transmission Control Protocol, Src Port: mdtp (3232), Dst Port: h323hostcall (1720), Seq: 509, Ack: 1,
TPKT, Version: 3, Length: 648
```

Q.931

```
Protocol discriminator: Q.931
Call reference value length: 2
Call reference flag: Message sent from originating side
Call reference value: 689f
Message type: SETUP (0x05)
```

- ⊕ Bearer capability
- ⊕ Display 'Administrator'
- ⊕ User-user

H.225.0 CS

```
Internet Protocol Version 4, Src: 10.210.200.111 (10.210.200.111), Dst: 10.210.200.112 (10.210.200.112)
Transmission Control Protocol, Src Port: h323hostcall (1720), Dst Port: mdtp (3232), Seq: 1, Ack: 649,
TPKT, Version: 3, Length: 103
```

Q.931

```
Protocol discriminator: Q.931
Call reference value length: 2
Call reference flag: Message sent to originating side
Call reference value: 0a9f
Message type: ALERTING (0x01)
```

- ⊕ User-user

H.225.0 CS

Ne všechny zprávy H.225 jsou povinné

	Transmit	Receive and Act Upon
Call Establishment Messages		
Alerting	mandatory	mandatory
Call Proceeding	optional	conditional mandatory
Connect	mandatory	mandatory
Progress	optional	conditional mandatory
Setup	mandatory	mandatory
Setup Acknowledge	optional	optional

Část Q.931 sahá ve výpisu od 08 po 95

```
Internet Protocol Version 4, Src: 10.210.200.111 (10.210.200.111), Dst: 10.210.200.112  
Transmission Control Protocol, Src Port: h323hostcall (1720), Dst Port: mdtp (3232), Seq  
TPKT, Version: 3, Length: 103
```

Q.931

```
Protocol discriminator: Q.931  
Call reference value length: 2  
Call reference flag: Message sent to originating side  
Call reference value: 689f  
Message type: ALERTING (0x01)
```

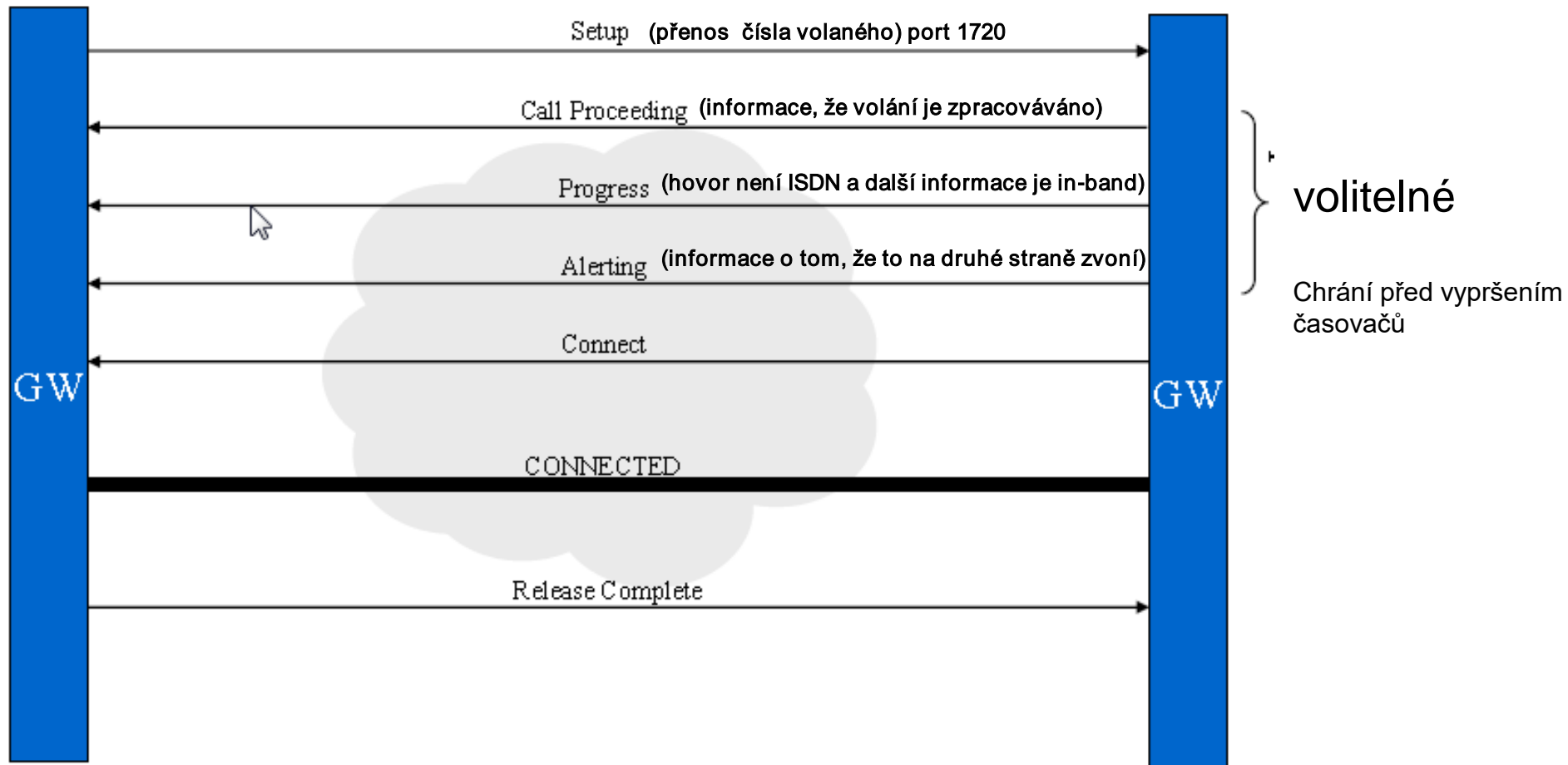
▣ User-user

```
Information element: User-user  
Length: 91  
Protocol discriminator: X.208 and X.209 coded user information
```

H.225.0 CS

```
00 05 5d ce 90 78 00 50 ba c4 2e 04 08 00 45 00 ..]..x.P .....E.  
00 8f f2 52 40 00 80 06 61 92 0a d2 c8 6f 0a d2 ...R@... a....o..  
c8 70 06 b8 0c a0 ec 90 9e 4e 47 4f f4 01 50 18 .p..... .NGO..P.  
fd 77 02 b6 00 00 03 00 00 67 08 02 e8 9f 01 7e .w.... .g.....~  
00 5b 05 23 80 06 00 08 91 4a 00 04 22 c0 b5 00 .[#.... .J..."..  
23 31 0f 50 6f 6c 79 63 6f 6d 20 56 69 61 56 69 #1.Polyc om ViaVi  
64 65 6f 16 52 65 6c 65 61 73 65 20 38 2e 30 3a deo.Rele ase 8.0:  
20 38 2e 30 2e 30 2e 30 35 32 32 01 b0 d8 00 11 8.0.0.0 522.....  
00 02 28 5a 75 30 0d 90 10 11 14 e3 e0 99 5e 3f ..(Zu0.. .....^?  
0d 01 00 01 80 01 00 01 40 10 80 01 00 ..... @....
```

Základní signalizace protokolu H.225



Zpráva SETUP

```
⊕ Internet Protocol Version 4, Src: 192.168.16.23 (192.168.16.23), Dst: 192.168.16.1
⊕ Transmission Control Protocol, Src Port: 4296 (4296), Dst Port: h323hostcall (1720)
⊕ TPKT, Version: 3, Length: 1367
⊕ Q.931
  Protocol discriminator: Q.931
  Call reference value length: 2
  Call reference flag: Message sent from originating side
  Call reference value: 0001
  Message type: SETUP (0x05)
⊕ Bearer capability
  Information element: Bearer capability
  Length: 3
  1... .. = Extension indicator: last octet
  .00. .... = Coding standard: ITU-T standardized coding (0x00)
  ...0 0000 = Information transfer capability: Speech (0x00)
  1... .... = Extension indicator: last octet
  .00. .... = Transfer mode: Circuit mode (0x00)
  ..1 0000 = Information transfer rate: 64 kbit/s (0x10)
  1... .... = Extension indicator: last octet
  .01. .... = Layer identification: Layer 1 identifier (0x01)
  ...0 0010 = User information layer 1 protocol: Recommendation G.711 u-law (0x02)
⊕ User-user
⊕ H.225.0 CS
```

Call Proceeding, Connect, ...

- ▣ Q.931
 - Protocol discriminator: Q.931
 - Call reference value length: 2
 - Call reference flag: Message sent to originating side
 - Call reference value: 0001
 - Message type: CALL PROCEEDING (0x02)
 - ⊕ User-user
- ⊕ H.225.0 CS
- ▣ Q.931
 - Protocol discriminator: Q.931
 - Call reference value length: 2
 - Call reference flag: Message sent to originating side
 - Call reference value: 0001
 - Message type: CONNECT (0x07)
 - ⊕ User-user
- ⊕ H.225.0 CS
- ▣ Q.931
 - Protocol discriminator: Q.931
 - Call reference value length: 2
 - Call reference flag: Message sent to originating side
 - Call reference value: 0001
 - Message type: FACILITY (0x62)
 - ⊕ User-user
- ⊕ H.225.0 CS

Facility – doplňkové služby

631	192.168.16.1	192.168.16.23	H.225.0	CS: facility OpenLogicalChannel
-----	--------------	---------------	---------	---------------------------------

Frame 631: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits)

- reverseLogicalChannelParameters
 - dataType: audioData (3)
 - audioData: g711Ulaw64k (3) ←
 - g711Ulaw64k: 20
 - multiplexParameters: h2250LogicalChannelParameters (2)
 - h2250LogicalChannelParameters
 - sessionID: 1
 - mediaChannel: unicastAddress (0)
 - unicastAddress: ipAddress (0)
 - ipAddress
 - network: 192.168.16.4 (192.168.16.4)
 - tsapIdentifier: 2052 ←
 - mediaControlChannel: unicastAddress (0)
 - 0... .. silenceSuppression: False

Internet Protocol Version 4, Src: 192.168.16.4 (192.168.16.4), Dst: 192.168.16.23 ←


User Datagram Protocol, Src Port: clearvisn (2052), Dst Port: tsb2 (2742) ←

Real-Time Transport Protocol

Zpráva H.225 SETUP

(rozšířené pole Bearer caacity)

```
Internet Protocol Version 4, Src: 192.168.16.23 (192.168.16.23), Dst: 192.168.16.1
Transmission Control Protocol, Src Port: 4296 (4296), Dst Port: h323hostcall (1720)
TPKT, Version: 3, Length: 1367
Q.931
  Protocol discriminator: Q.931
  Call reference value length: 2
  Call reference flag: Message sent from originating side
  Call reference value: 0001
  Message type: SETUP (0x05)
  Bearer capability
    Information element: Bearer capability
    Length: 3
    1... .... = Extension indicator: last octet
    .00. .... = Coding standard: ITU-T standardized coding (0x00)
    ...0 0000 = Information transfer capability: Speech (0x00)
    1... .... = Extension indicator: last octet
    .00. .... = Transfer mode: Circuit mode (0x00)
    ...1 0000 = Information transfer rate: 64 kbit/s (0x10)
    1... .... = Extension indicator: last octet
    .01. .... = Layer identification: Layer 1 identifier (0x01)
    ...0 0010 = User information layer 1 protocol: Recommendation G.711 u-law (0x02)
  User-user
H.225.0 CS
```



Byly snahy o H.323/RSVP synchronizaci (Co je RSVP?)

Caller (EP A)

Callee (EP B)

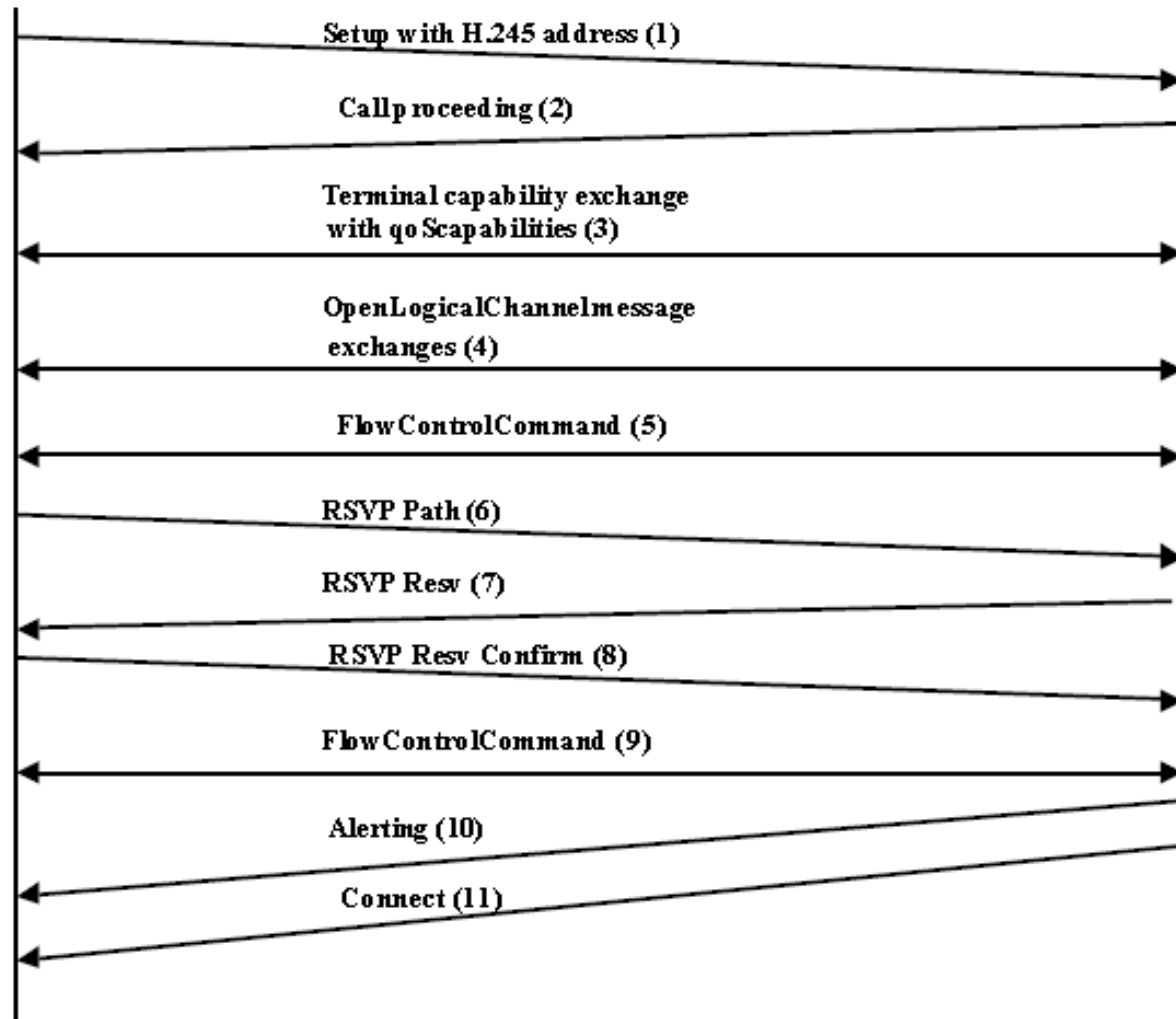


H.323/RSVP Synchronization for Video over IP

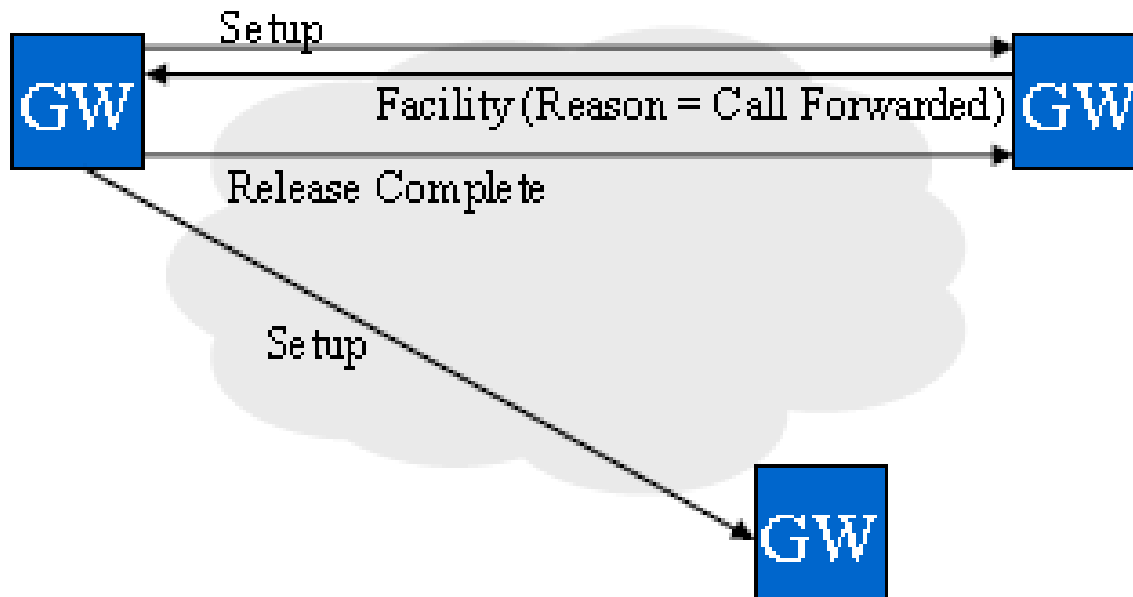
Engineering White Paper

Subha Dhesikan
Cisco Systems
December 5, 2002

ENG-177305
Version 1.0



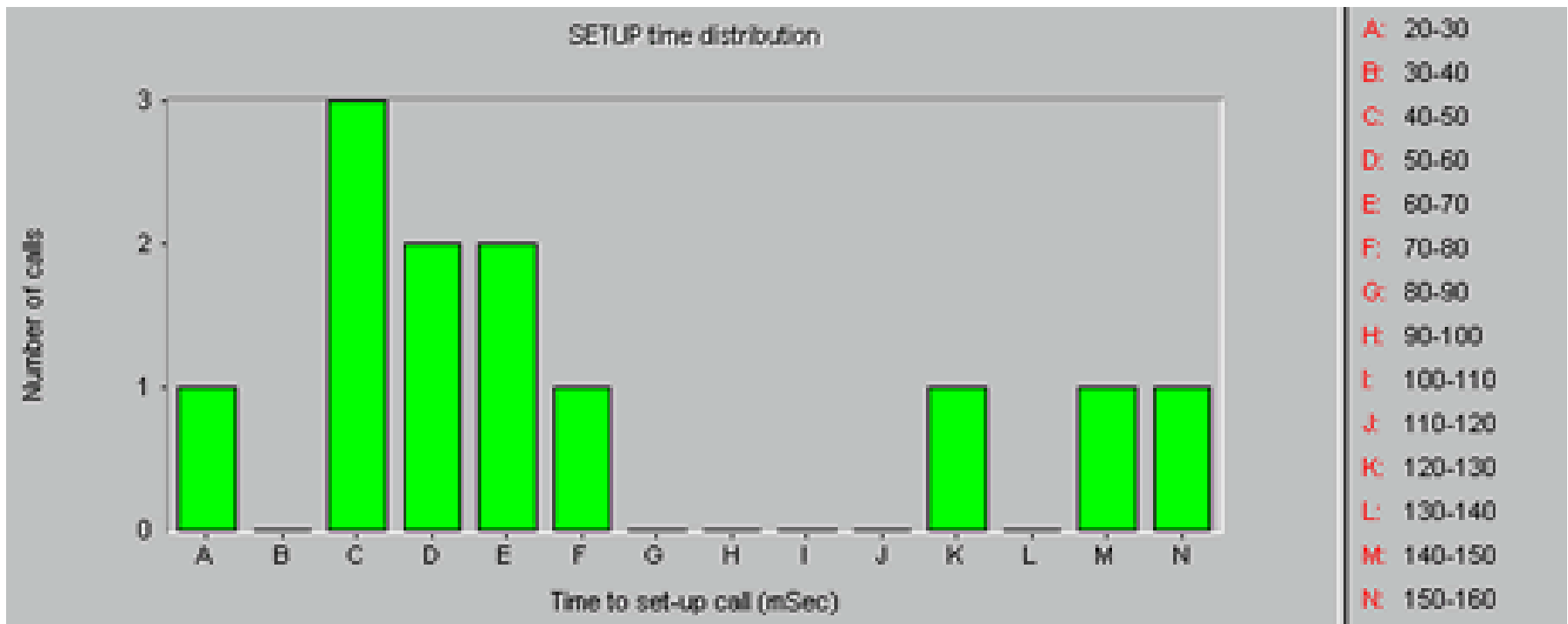
Call Forwarding



Výměna zpráv mezi terminály

Terminal 1	Terminal 2
Setup	Alerting
	Connect
termCapSet	termCapAck
	termCapSet
termCapAck	
masterSlvDet	
	masterSlvDetAck
masterSlvDetConfirm	
openReq	
	openAck
openAck	openReq
endSession	
	endSession
Release	

Ukázka měření doby Setupu



<http://www.itu.int/rec/T-REC-H.245-200912-I/en>

4. Protokol H.245

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.245

(12/2009)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS
Infrastructure of audiovisual services – Communication
procedures

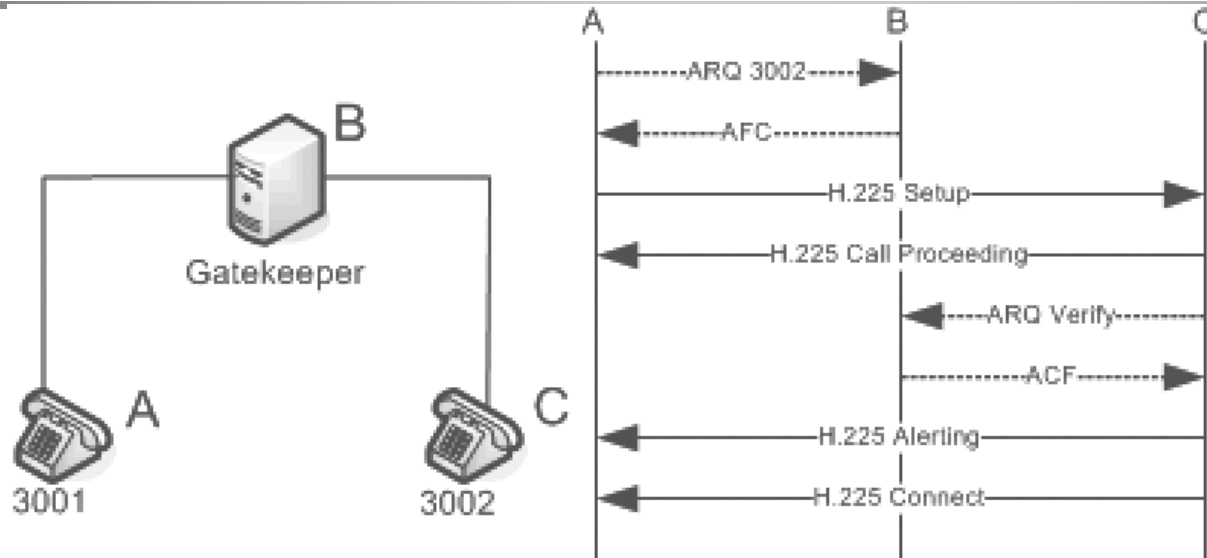
Control protocol for multimedia communication

Recommendation ITU-T H.245

ITU-T



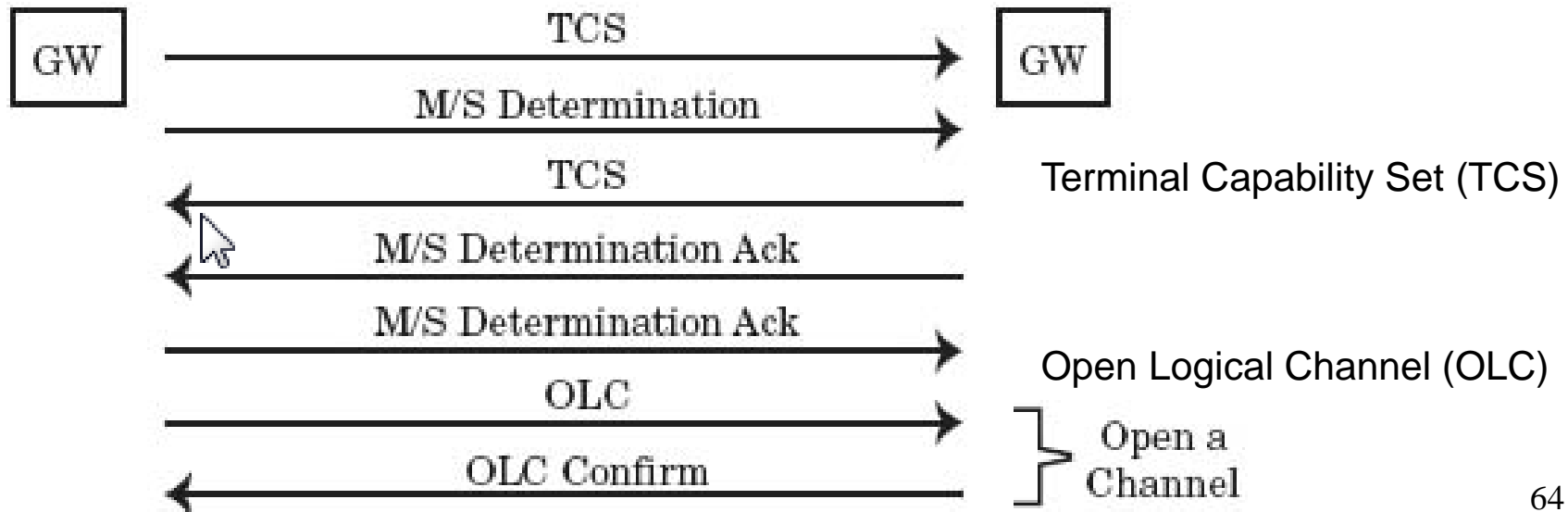
Sestavení hovoru přes gatekeeper



1. Volající pošle zprávu ARQ (Admissions Request) na gatekeeper (předloží svoji identifikaci a číslo volaného), tato zpráva je součástí RAS protokolu.
2. Gatekeeper odpoví potvrzením ACF (Admissions Confirm) nebo odmítnutém ARJ (Admissions Reject).
V případě potvrzení volajícímu tak gatekeeper odpoví, že požadované session je v pořádku (opět protokolem RAS).
3. Volající odešle volanému zprávu H.225 Setup.
4. Volaný odešle volajícímu provizorní zprávu Call Proceeding. Provizorní je proto, protože volaný musí nejprve ověřit autenticitu volajícího předtím, než vytvoří trvalé spojení.
5. Volaný odešle na gatekeeper zprávu ARQ s dotazem, zda je volání legitimní. V tento moment by měl mít gatekeeper uložen záznam o původním ARQ od volajícího k porovnání s ARQ od volaného.
6. Pokud má gatekeeper odpovídající ARQ záznam, pošle volanému potvrzující zprávu ACF.
7. Jakmile je zpráva ACF přijata volaným, pošle H.225 volajícímu zprávu Alerting. Volaný pak pošle H.225 zprávu Connect volající straně. **Ta uvolní cestu pro H.245.**

Protokol H.245

- Slouží pro řízení multimediálního přenosu, nastavení parametrů přenosu, otevření a zavření logických kanálů pro přenos, volby zvukového kodeku atd.
- Vyjednávání parametrů přenosu začíná po sestavení hovoru.
- Pro přenos paketů se používá protokol TCP.



Tři kola komunikace H.245

10	10.210.200.112	10.210.200.111	H.225.0	CS: setup
12	10.210.200.111	10.210.200.112	H.225.0	CS: alerting
18	10.210.200.111	10.210.200.112	H.225.0	CS: connect
25	10.210.200.112	10.210.200.111	H.245	terminalCapabilitySet
27	10.210.200.112	10.210.200.111	H.245	masterSlaveDetermination
31	10.210.200.111	10.210.200.112	H.245	terminalCapabilitySet
33	10.210.200.111	10.210.200.112	H.245	masterSlaveDetermination
38	10.210.200.112	10.210.200.111	H.245	terminalCapabilitySetAck
39	10.210.200.112	10.210.200.111	H.245	masterSlaveDeterminationAck
41	10.210.200.111	10.210.200.112	H.245	terminalCapabilitySetAck
42	10.210.200.111	10.210.200.112	H.245	masterSlaveDeterminationAck
44	10.210.200.112	10.210.200.111	H.245	openLogicalChannel (generic)
46	10.210.200.112	10.210.200.111	H.245	openLogicalChannel (genericVideoCapability)



Zprávy H.245

25	10.210.200.112	10.210.200.111	H.245	terminalCapabilitySet
27	10.210.200.112	10.210.200.111	H.245	masterSlaveDetermination
31	10.210.200.111	10.210.200.112	H.245	terminalCapabilitySet
33	10.210.200.111	10.210.200.112	H.245	masterSlaveDetermination
38	10.210.200.112	10.210.200.111	H.245	terminalCapabilitySetAck
39	10.210.200.112	10.210.200.111	H.245	masterSlaveDeterminationAck
41	10.210.200.111	10.210.200.112	H.245	terminalCapabilitySetAck
42	10.210.200.111	10.210.200.112	H.245	masterSlaveDeterminationAck
44	10.210.200.112	10.210.200.111	H.245	openLogicalChannel (generic)
46	10.210.200.112	10.210.200.111	H.245	openLogicalChannel (genericVideoCapability)
48	10.210.200.111	10.210.200.112	H.245	openLogicalChannel (generic)
51	10.210.200.112	10.210.200.111	H.245	openLogicalChannelAck

Otevření více kanálů

Time	10.210.200.112 10.210.200.111	Comment
5.709857	→ setup (1720)	H225 From: To: TunnH245:off FS:off
5.882944	← alerting (1720)	H225 TunnH245:off FS:off
10.702663	→ connect (1720)	H225 TunnH245:off FS:off
10.991370	→ TCS (3231)	H245 terminalCapabilitySet
10.991521	→ MSD (3231)	H245 masterSlaveDetermination
11.310257	← TCS (3231)	H245 terminalCapabilitySet
11.310394	← MSD (3231)	H245 masterSlaveDetermination
12.140347	→ TCSAck (3231)	H245 terminalCapabilitySetAck
12.140352	→ MSDAck (3231)	H245 masterSlaveDeterminationAck
12.196862	← TCSAck (3231)	H245 terminalCapabilitySetAck
12.196866	← MSDAck (3231)	H245 masterSlaveDeterminationAck
12.824751	→ OLC (generic) (3231)	H245 openLogicalChannel
13.567298	→ OLC (genericVideoCapability) (3231)	H245 openLogicalChannel
13.762027	← OLC (generic) (3231)	H245 openLogicalChannel
14.070986	→ OLCAck (3231)	H245 openLogicalChannelAck
14.103243	→ OLC (genericVideoCapability) (3231)	H245 openLogicalChannel
14.247915	→ OLC (genericVideoCapability) (3231)	H245 openLogicalChannel
14.382810	→ OLC (genericDataCapability) (3231)	H245 openLogicalChannel
14.664064	← OLCAck (3231)	H245 openLogicalChannelAck
14.856877	← OLCAck (3231)	H245 openLogicalChannelAck
14.932047	→ FCC (3231)	H245 flowControlCommand
14.991657	→ MC (3231)	H245 miscellaneousCommand
15.215888	→ OLC (genericVideoCapability) (3231)	H245 openLogicalChannel
15.355210	← OLCAck (3231)	H245 openLogicalChannelAck
15.393647	← FCC (3231)	H245 flowControlCommand
15.437293	← MC (3231)	H245 miscellaneousCommand
15.466774	← OLCAck (3231)	H245 openLogicalChannelAck
15.546179	← MC (3231)	H245 miscellaneousCommand
15.656911	→ RTP (RTPType-127) (3230)	RTP Num packets:1187 Duration:47.382s SSRC:0xCF3B3801
15.669859	← MI (3231)	H245 miscellaneousIndication
15.866618	← FCIndication (3231)	H245 flowControlIndication

TCS

Zpráva protokolu H.245 TCS (Terminal Capacity Set)

```
Transmission Control Protocol, Src Port: whisker (3233), Dst Port: vidigo
TPKT, Version: 3, Length: 1086
H.245
  PDU Type: request (0)
    request: terminalCapabilitySet (2)
      terminalCapabilitySet
        sequenceNumber: 1
        protocolIdentifier: 0.0.8.245.0.7 (h245 version 7)
        multiplexCapability: h2250Capability (4)
        capabilityTable: 45 items
        capabilityDescriptors: 1 item
```

! 45 položek! Tolik!

Určení, kdo je Master a kdo Slave u EP

```
Internet Protocol Version 4, Src: 10.210.200.112 (10.210.200.112), Dst: 10.210.200.111
Transmission Control Protocol, Src Port: whisker (3233), Dst Port: vidigo (3231), Seq:
TPKT, Version: 3, Length: 11
H.245
```

▣ PDU Type: request (0)

▣ request: masterSlaveDetermination (1) — typ terminálu (ten s větším číslem je master)

▣ masterSlaveDetermination

terminalType: 50

statusDeterminationNumber: 1151465

— při rovnosti rozhoduje toto číslo

```
Internet Protocol Version 4, Src: 10.210.200.111 (10.210.200.111), Dst: 10.210.200.112
Transmission Control Protocol, Src Port: vidigo (3231), Dst Port: whisker (3233), Seq:
TPKT, Version: 3, Length: 11
H.245
```

▣ PDU Type: request (0)

▣ request: masterSlaveDetermination (1)


▣ masterSlaveDetermination

terminalType: 50


statusDeterminationNumber: 10199967

a Master se stává koncový bod s adresou 10.210.200.112

```
Internet Protocol Version 4, Src: 10.210.200.112 (10.210.200.112), Dst: 10.210.200.111  
Transmission Control Protocol, Src Port: whisker (3233), Dst Port: vidigo (3231), Seq:  
TPKT, Version: 3, Length: 6  
H.245
```

- ▣ PDU Type: response (1)
 - ▣ response: masterSlaveDeterminationAck (1)
 - ▣ masterSlaveDeterminationAck
 - ▣ decision: master (0) 
 - master: NULL

```
Internet Protocol Version 4, Src: 10.210.200.111 (10.210.200.111), Dst: 10.210.200.112  
Transmission Control Protocol, Src Port: vidigo (3231), Dst Port: whisker (3233), Seq:  
TPKT, Version: 3, Length: 6  
H.245
```

- ▣ PDU Type: response (1)
 - ▣ response: masterSlaveDeterminationAck (1)
 - ▣ masterSlaveDeterminationAck
 - ▣ decision: slave (1) 
 - slave: NULL

A následuje otevření logického kanálu

```
Internet Protocol Version 4, Src: 10.210.200.112 (10.210.200.112), Dst: 10.210.200.111  
Transmission Control Protocol, Src Port: whisker (3233), Dst Port: vidigo (3231), Seq:  
TPKT, Version: 3, Length: 62  
H.245
```

- ▣ PDU Type: request (0)
 - ▣ request: openLogicalChannel (3)
 - ▣ openLogicalChannel
 - forwardLogicalChannelNumber: 2
 - ▣ forwardLogicalChannelParameters
 - ⊕ dataType: h235Media (7)
 - ▣ multiplexParameters: h2250LogicalChannelParameters (3)
 - ▣ h2250LogicalChannelParameters
 - sessionID: 1
 - ▣ mediaControlChannel: unicastAddress (0)
 - ▣ unicastAddress: ipAddress (0)
 - ▣ ipAddress
 - network: 10.210.200.112 (10.210.200.112)
 - tsapIdentifier: 3231
 - dynamicRTPPayloadType: 127



Fast Start (Fast Connect)

V rámci standardního vyjednávání H.245 koncové body potřebují tři kola komunikace, než se dohodnou na parametrech audio či video kanálů

1. dohoda, kdo je Master a kdo Slave,
2. výměna informací o kapacitách terminálů
3. otevření logických kanálů



V určitých situacích a to zejména na linkách s vysokým zpožděním to může trvat příliš dlouho.

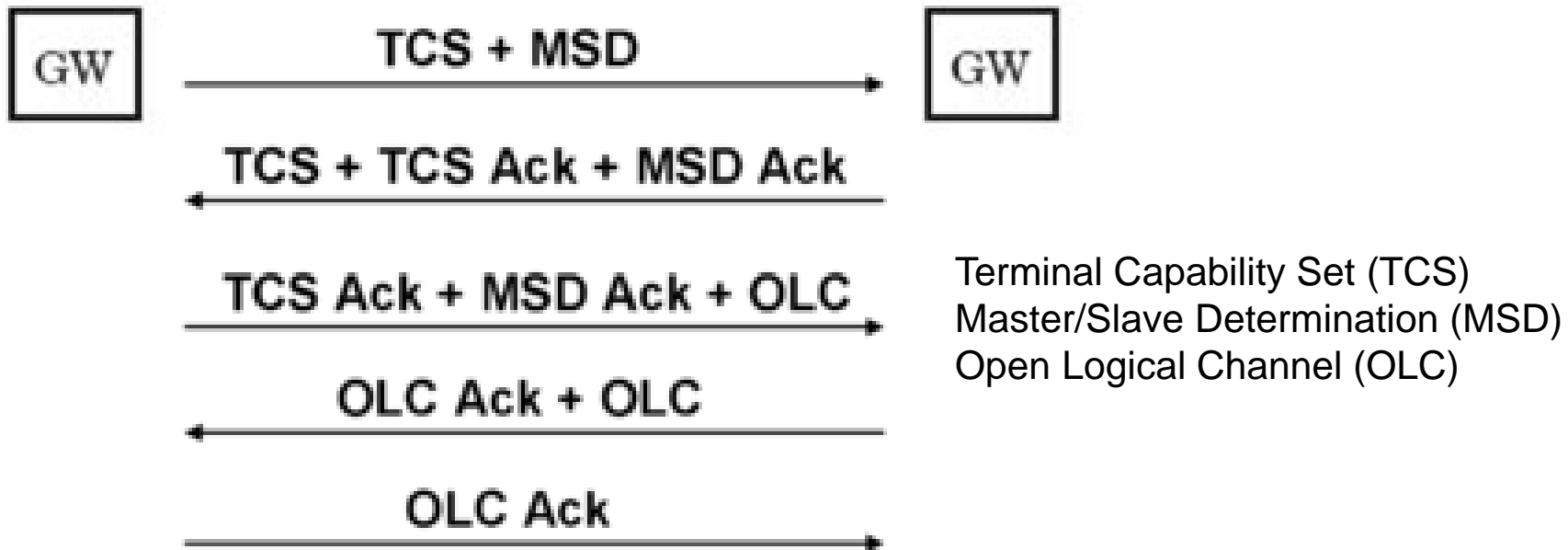
Fast Connect

- Zpoždění lze eliminovat metodou Fast Connect (Fast Start). Koncový bod jednoduše **připraví několik variant žádosti o otevření logického kanálu** v závislosti na tom, kolik kodeků podporuje. Poté je zakóduje do binární formy a výsledek vloží do H.225.0/Q.931 zprávy (obvykle zpráva Setup).
- Volaný účastník vybere jednu z variant a potvrdí ji v příští H.225.0/Q.931 zprávě a přiloží vlastní seznam variant logických kanálů. Zbylá část komunikace proběhne standardním způsobem.
- Pomocí Fast Connect jsou parametry logických kanálů (kodeky, IP adresy a porty) sesouhlaseny v rané fázi výměny zpráv, tj. předtím, než volaný uživatel přijme hovor a tudíž se **doba této výměny nepočítá do ceny spojení**.
- Fast Connect a H.245 tunelování mohou být použity současně.

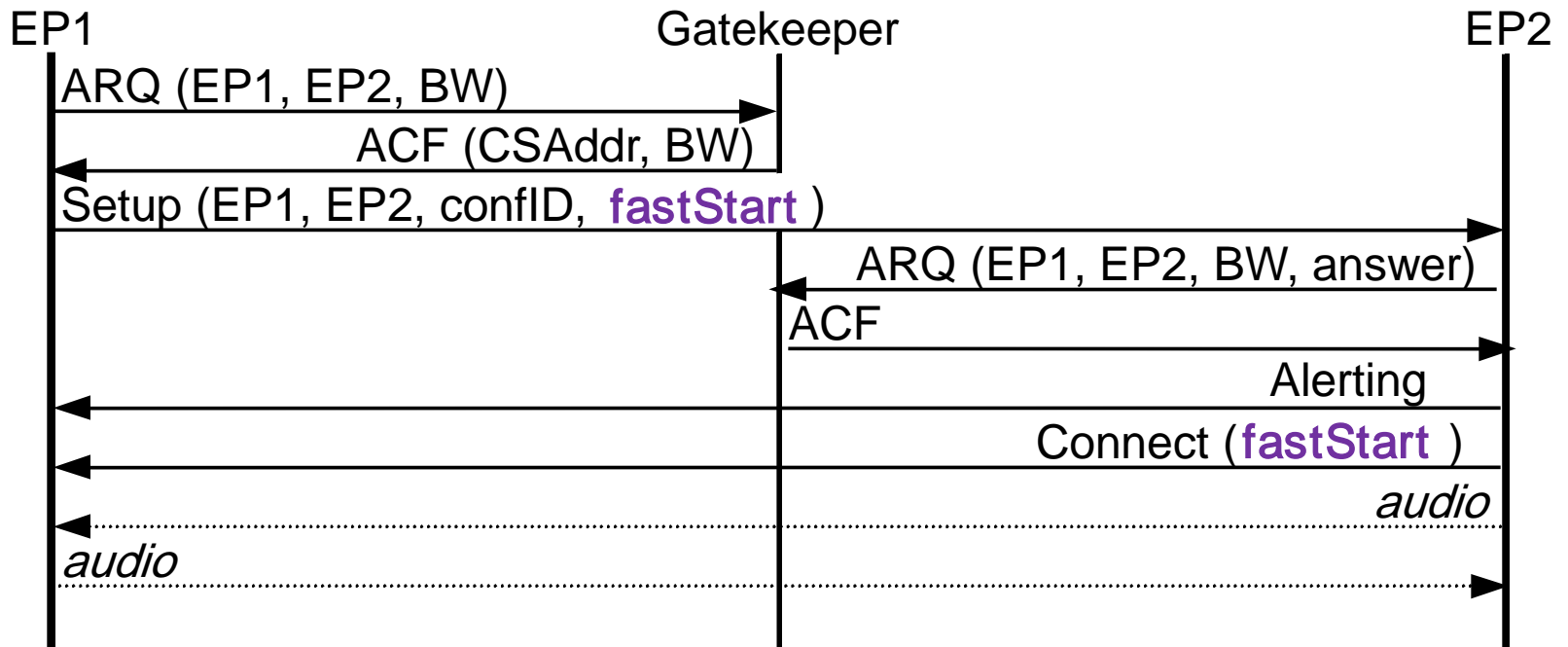
fastStart

```
Internet Protocol Version 4, Src: 192.168.16.23 (192.168.16.23), Dst: 192.168.16.1
Transmission Control Protocol, Src Port: 4296 (4296), Dst Port: h323hostcall (1720)
TPKT, Version: 3, Length: 1367
Q.931
H.225.0 CS
  H323-UserInformation
    h323-uu-pdu
      h323-message-body: setup (0)
        setup
          protocolIdentifier: 0.0.8.2250.0.5 (Version 5)
          sourceInfo
            ...0 .... activeMC: False
            conferenceID: 00000000-0000-1000-0000-0000c0a81017
          conferenceGoal: callIndependentSupplementaryService (4)
          callType: pointToPoint (0)
          callIdentifier
          fastStart: 36 items
            1... .... mediaWaitForConnect: True
            1... .... canOverlapSend: True
            0... .... h245Tunnelling: False
```

Signalizace volby Fast Connect



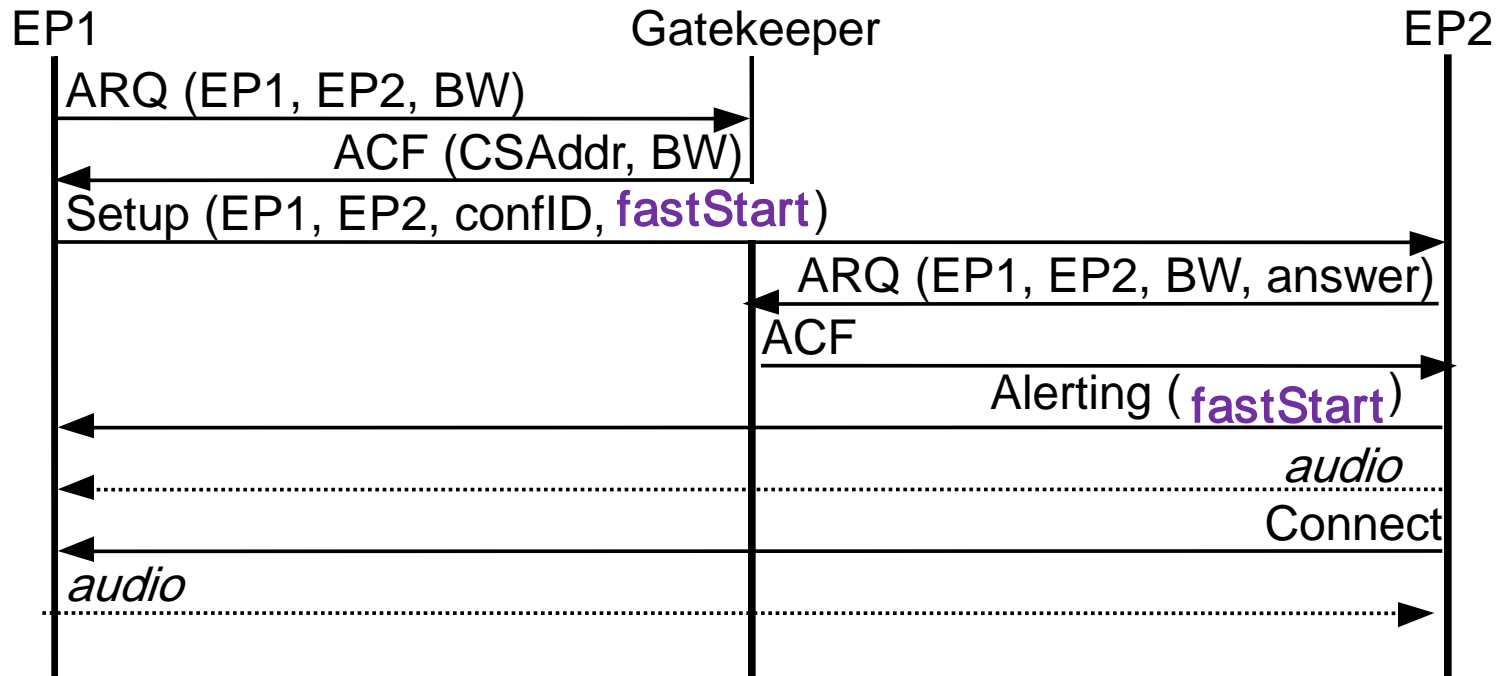
Fast Start



Pole *fastStart* obsahuje seznam struktur `OpenLogicalChannel`

Audio je po `Connect`

Fast Start s vlastností Early Audio



Audio je před Connect

Příklad nároků na porty pro koncové body videa Polycomu

| Port | Required/Opt | Port Type | Usage | direction |
|--------|--------------|------------|---|-----------------|
| 389 | For ILS | Static TCP | ILS Registration (LDAP) | (Bidirectional) |
| 1718 | Required | Static UDP | Gatekeeper Discovery | (Bidirectional) |
| 1719 | Required | Static UDP | Gatekeeper RAS | (Bidirectional) |
| 1720 | Required | Static TCP | H.323 Call Setup | (Bidirectional) |
| 1731 | Required | Static TCP | Audio Call Control | (Bidirectional) |
| 3230-5 | Required | TCP/UDP | Signaling and control
audio, volání, video, data | (Bidirectional) |
| 3603 | Optional | Static TCP | Web Interface | (Bidirectional) |

Konfigurace FXO pro GnuGK

```
usr/config$ h323 -print
```

```
H.323 stack relate information
```

```
  RAS mode                : GK mode
  Registration mode       : Gateway
  Gatekeeper IP address   : 10.55.10.51
  Gatekeeper ID          : GK
  Registered e164         : 0
  Registered H323 ID      : gw3
  Gatekeeper Discovery    : On
  Q931 port               : 1720
  RAS port                : 16640
  RTP port                : 16384
  RAS TTL time           : 60
  Gatekeeper discovery port: 1718
  Gatekeeper RAS port     : 1719
  Allocated port range   :
    start port           : 1024
    end port             : 65535
  Response timeOut       : 5
  Connect timeOut        : 200
```

```
usr/config$
```

Příklad: Faststart

```
Internet Protocol Version 4, Src: 192.168.16.23 (192.168.16.23), Dst: 192.168.16.1
Transmission Control Protocol, Src Port: 4296 (4296), Dst Port: h323hostcall (1720)
TPKT, Version: 3, Length: 1367
Q.931
H.225.0 CS
  H323-UserInformation
    h323-uu-pdu
      h323-message-body: setup (0)
        setup
          protocolIdentifier: 0.0.8.2250.0.5 (Version 5)
          sourceInfo
            ...0 .... activeMC: False
            conferenceID: 00000000-0000-1000-0000-0000c0a81017
          conferenceGoal: callIndependentSupplementaryService (4)
          callType: pointToPoint (0)
          callIdentifier
          fastStart: 36 items
            1... .... mediaWaitForConnect: True
            1... .... canOverlapSend: True
            0... .... h245Tunnelling: False
```

Stejné ID pro všechny zprávy spojené se stejným voláním

36 položek

tunel H.245 je vypnut

Položka 25 otevírá logický kanál (obdobně má svoji položku security protokol H.235)

```
Item 23
Item 24
Item 25
  FastStart item: 30 octets
  OpenLogicalChannel
    forwardLogicalChannelNumber: 26
    forwardLogicalChannelParameters
      dataType: nullData (1)
      multiplexParameters: none (4)
    reverseLogicalChannelParameters
      dataType: audioData (3)
      audioData: g711Ulaw64k (3)
        g711Ulaw64k: 60
      multiplexParameters: h2250LogicalChannelParameters (2)
        h2250LogicalChannelParameters
          sessionID: 1
          mediaChannel: unicastAddress (0)
            unicastAddress: ipAddress (0)
              ipAddress
                network: 192.168.16.23 (192.168.16.23)
                tsapIdentifier: 2742
          0... .... mediaGuaranteedDelivery: False
          mediaControlChannel: unicastAddress (0)
            unicastAddress: ipAddress (0)
              ipAddress
                network: 192.168.16.23 (192.168.16.23)
                tsapIdentifier: 2743
          0... .... mediaControlGuaranteedDelivery: False
          .1.. .... silenceSuppression: True
  Item 26
```

```
Ethernet II, Src: GiantEle_05:cb:11 (00:09:6e:05:cb:11), Dst: Avaya_ef:48:f8 (00:04
Internet Protocol Version 4, Src: 192.168.16.23 (192.168.16.23), Dst: 192.168.16.4
User Datagram Protocol, Src Port: tsb2 (2742) Dst Port: clearvisn (2052)
Real-Time Transport Protocol
```

IP adresa
a číslo portu

Faststart zde pro rychlost vypouští služby H.245.

Co jsou zde ale ty „empty“ pakety?

| | | | |
|---------------|---------------|---------|---------------------------------------|
| 192.168.16.23 | 192.168.16.1 | H.225.0 | RAS: registrationRequest |
| 192.168.16.1 | 192.168.16.23 | H.225.0 | RAS: registrationConfirm |
| 192.168.16.23 | 192.168.16.1 | H.225.0 | CS: setup OpenLogicalChannel |
| 192.168.16.1 | 192.168.16.23 | H.225.0 | CS: callProceeding |
| 192.168.16.1 | 192.168.16.23 | H.225.0 | CS: connect OpenLogicalChannel |
| 192.168.16.1 | 192.168.16.23 | H.225.0 | CS: empty |
| 192.168.16.1 | 192.168.16.23 | H.225.0 | CS: empty |
| 192.168.16.1 | 192.168.16.23 | H.225.0 | CS: empty |
| 192.168.16.1 | 192.168.16.23 | H.225.0 | CS: empty CS: empty CS: empty |
| 192.168.16.1 | 192.168.16.23 | H.225.0 | CS: empty |
| 192.168.16.23 | 192.168.16.1 | H.225.0 | CS: empty |
| 192.168.16.1 | 192.168.16.23 | H.225.0 | CS: empty |
| 192.168.16.23 | 192.168.16.1 | H.225.0 | CS: empty |
| 192.168.16.1 | 192.168.16.23 | H.225.0 | CS: empty |
| 192.168.16.1 | 192.168.16.23 | H.225.0 | CS: empty |
| 192.168.16.1 | 192.168.16.23 | H.225.0 | CS: empty |
| 192.168.16.1 | 192.168.16.23 | H.225.0 | CS: facility OpenLogicalChannel |
| 192.168.16.4 | 192.168.16.23 | RTP | PT=ITU-T G.711 PCMU, SSRC=0xF5952C7C, |
| 192.168.16.4 | 192.168.16.23 | RTP | PT=ITU-T G.711 PCMU, SSRC=0xF5952C7C, |

Jsou to INFORMATION pakety

(přenos specifických údajů pro telefony Avaya)

```
Internet Protocol Version 4, Src: 192.168.16.1 (192.168.16.1), Dst: 192.168.16.23 (192.168.16.23)
Transmission Control Protocol, Src Port: h323hostcall (1720), Dst Port: 4296 (4296), Seq: 269, Ac
TPKT, Version: 3, Length: 56
```

Q.931

```
Protocol discriminator: Q.931
Call reference value length: 2
Call reference flag: Message sent to originating side
Call reference value: 0001
Message type: INFORMATION (0x7b)
```

⊞ User-user

H.225.0 CS

⊞ H323-UserInformation

⊞ h323-uu-pdu

```
⊞ h323-message-body: empty (8)
  empty: NULL
```

```
0... .... h245Tunnelling: False
```

⊞ nonStandardControl: 1 item

⊞ Item 0

⊞ NonStandardParameter

⊞ nonStandardIdentifier: object (0)

```
  object: 2.16.840.1.113778.4.2.10 (joint-iso-itu-t.16.840.1.113778.4.2.10)
```

```
  data: 20 octets
```

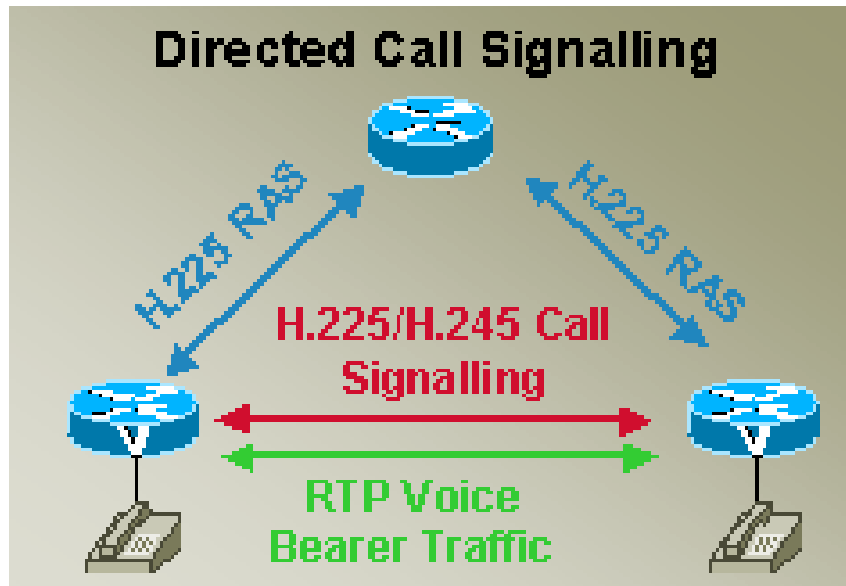
⊞ Data (20 bytes)

```
  Data: 14381120abe31b5b003b00481b5b024ba3830442
```

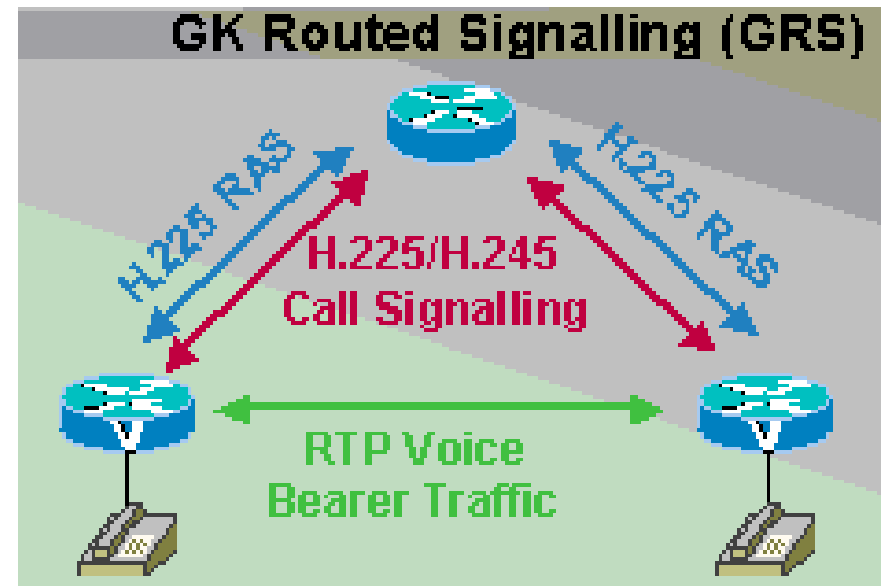
```
  [Length: 20]
```



Dva modely volání



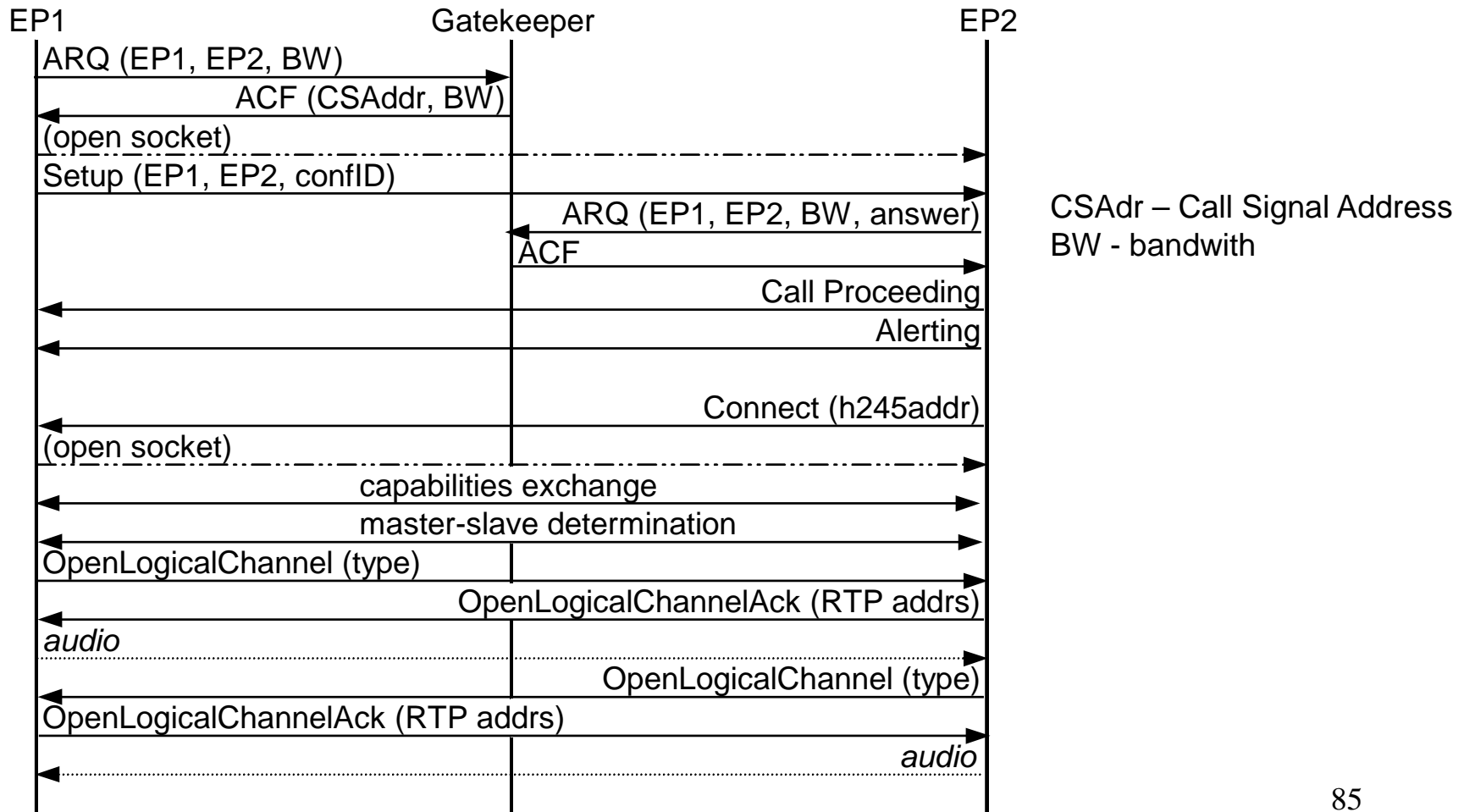
- rychlejší setup
- vlastnosti poskytují EP
- nahrazuje trunk



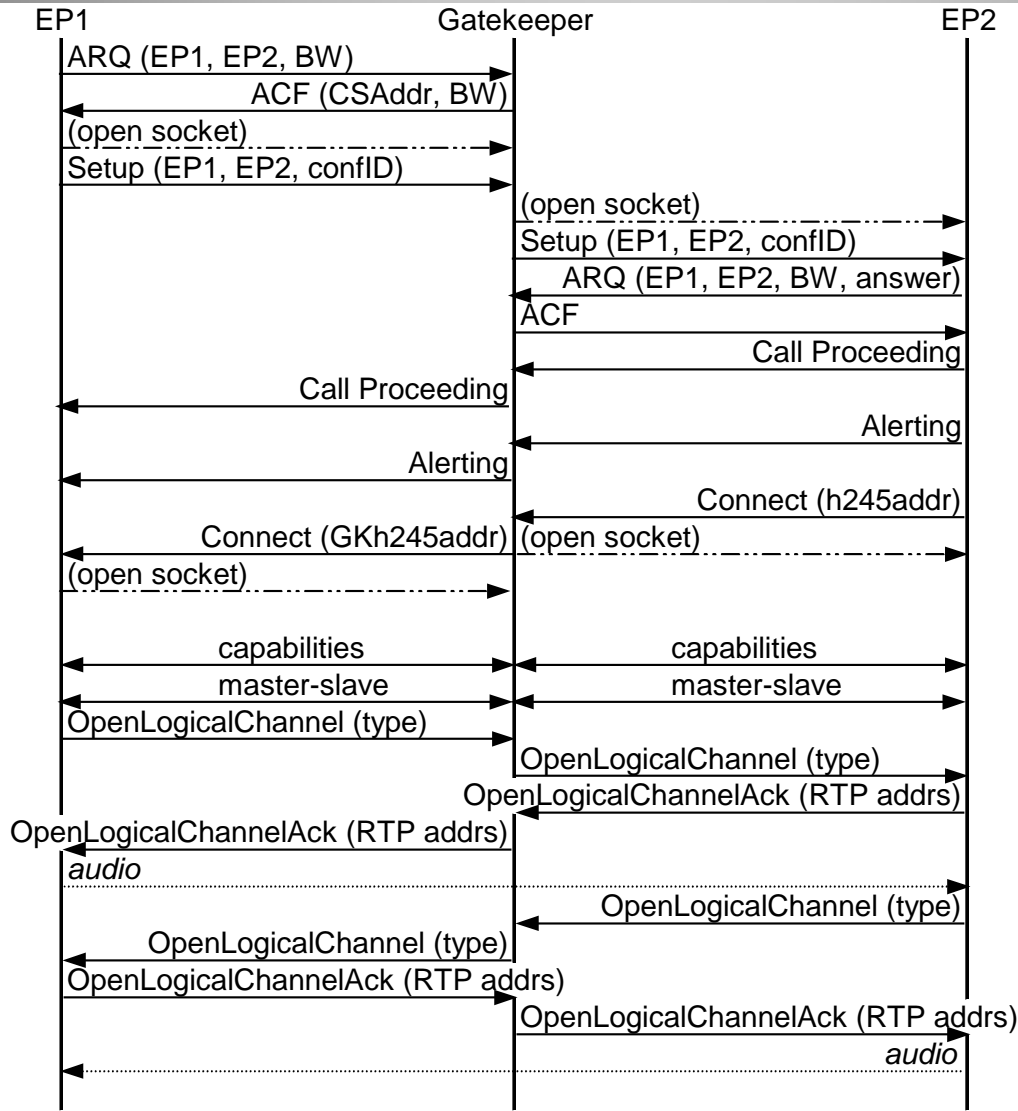
- gatekeeper může fungovat jako „server vlastností“
- např. pro audiokonference

Signalizace modelu

Directed Call Signaling

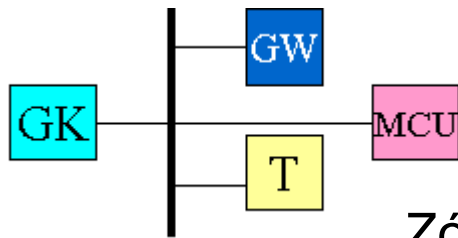


Signalizace modelu Gatekeeper Routed

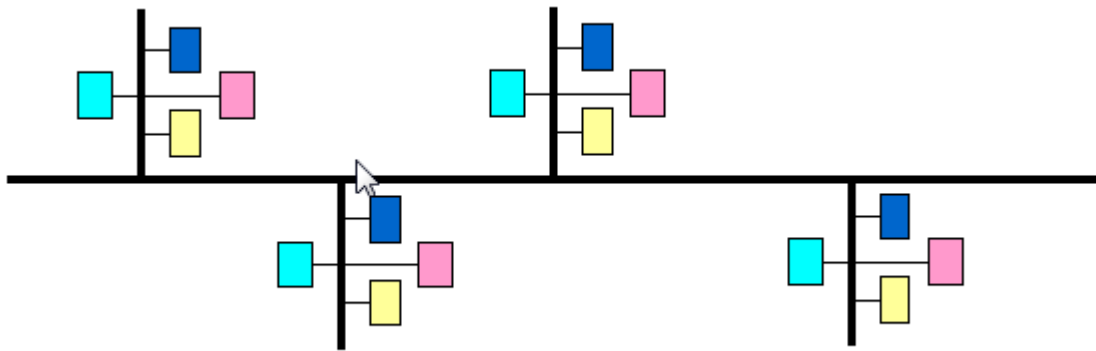


CSAdr – Call Signal Address
 BW - bandwidth

Zóna a administrativní doména



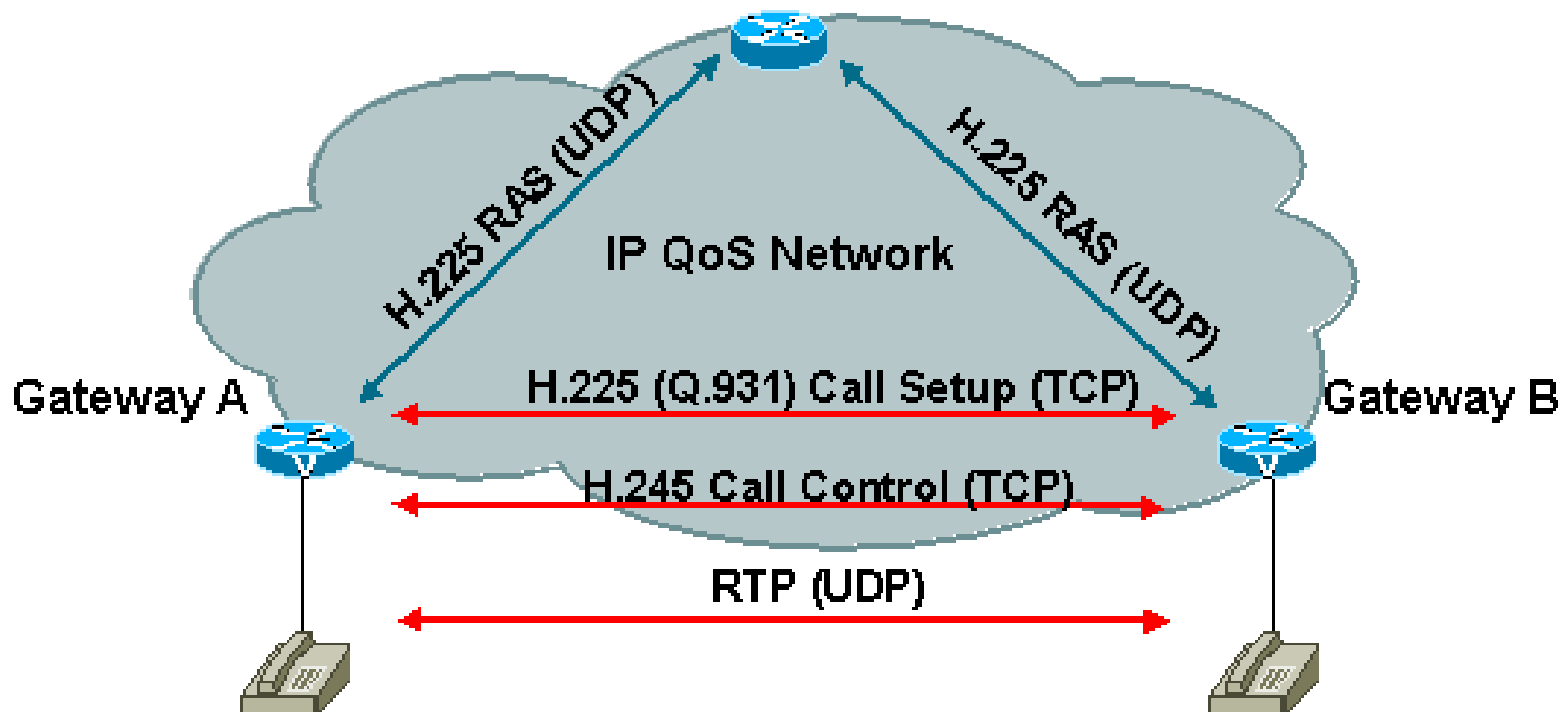
Zóna je řízena jedním či více gatekeeperů
Administrativní doména je řízena ISP či správcem sítě



Gatekeeper mezi branami

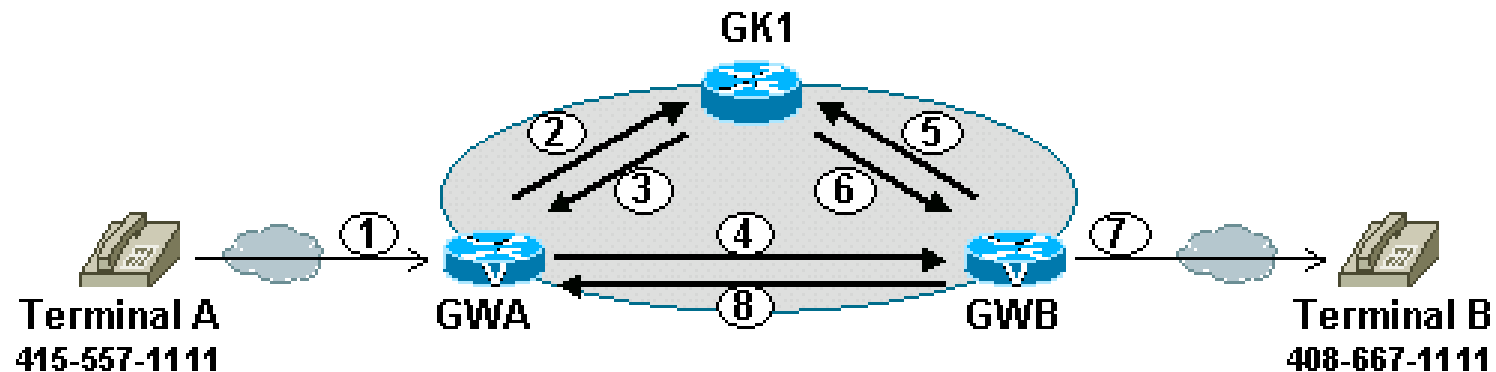
Gatekeeper

Address Translation: Every GW needs to know only about the GK, not about all other GWs



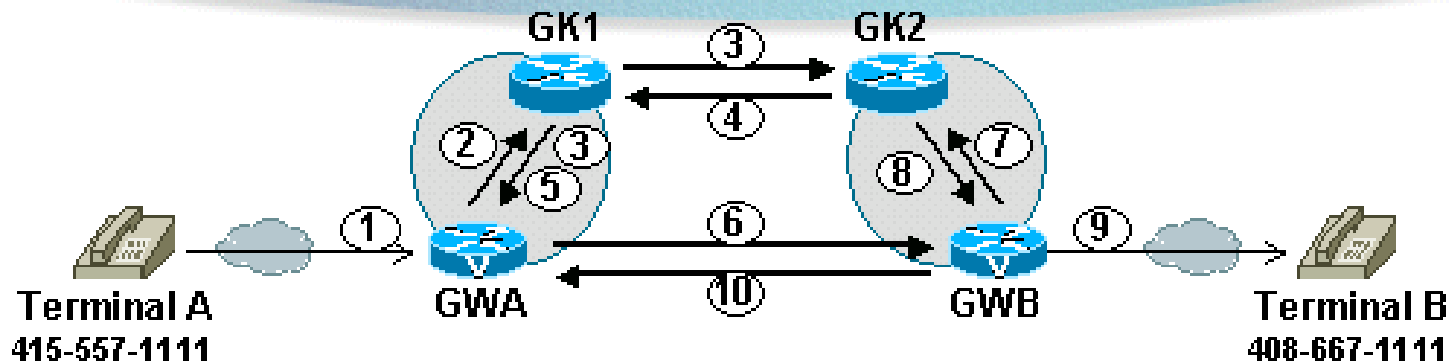
Intra-Zone Call Setup

http://www.cisco.com/warp/public/788/voip/2zone_gw_gk.pdf



- 1) Terminal A **dials** the phone number 408-667-1111 for Terminal B
- 2) GWA sends GK1 an **ARQ**, asking permission to call Terminal B
- 3) GK1 does a look-up and finds Terminal B registered; returns an **ACF** with the IP address of GWB
- 4) GWA sends a **Q.931 Call-Setup** to GWB with Terminal B's phone number
- 5) GWB sends GK1 an **ARQ**, asking permission to answer GWA's call
- 6) GK1 returns an **ACF** with the IP address of GWA
- 7) GWB sets up a **POTS call** to Terminal B at 408-667-1111
- 8) When Terminal B answers, GWB sends **Q.931 Connect** to GWA
- 9) GWs send **IRR** to GK after call is setup

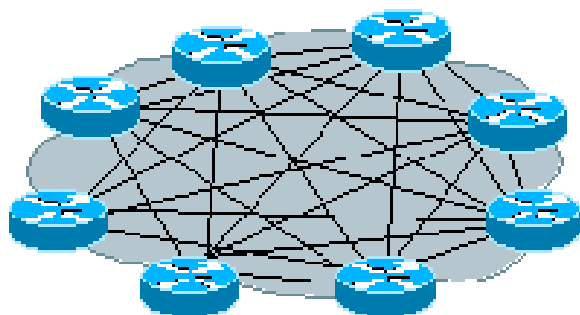
Inter-Zone Call Setup



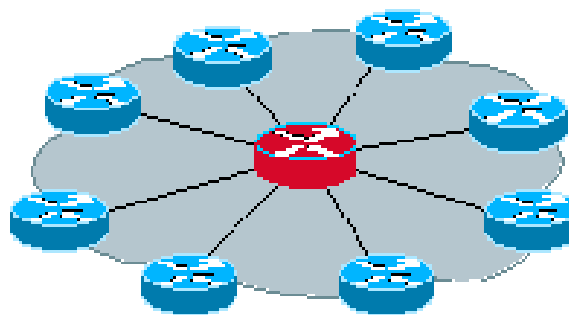
- 1) Terminal A **dials** the phone number 408-667-1111 for Terminal B
- 2) GWA sends GK1 an **ARQ**, asking permission to call Terminal B
- 3) GK1 does a look-up and does **NOT** find Terminal B registered; GK1 does a prefix look-up and finds a match with GK2; GK1 sends an **LRQ** to GK2, and **RIP** (Request In Progress) to GWA
- 4) GK2 does a look-up and finds Terminal B registered; returns an **LCF** with the IP address of GWB
- 5) GK1 returns an **ACF** with the IP address of GWB
- 6) GWA sends a **Q.931 Call-Setup** to GWB with Terminal B's phone number
- 7) GWB sends GK2 an **ARQ**, asking permission to answer GWA's call
- 8) GK2 returns an **ACF** with the IP address of GWA
- 9) GWB sets up a **POTS call** to Terminal B at 408-667-1111
- 10) When Terminal B answers, GWB sends **Q.931 Connect** to GWA

Škálování sítí s gatekeeperem

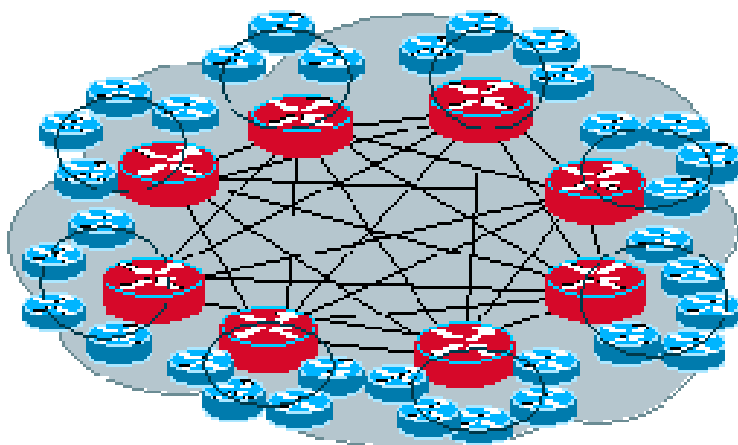
Small Network - Gateways only



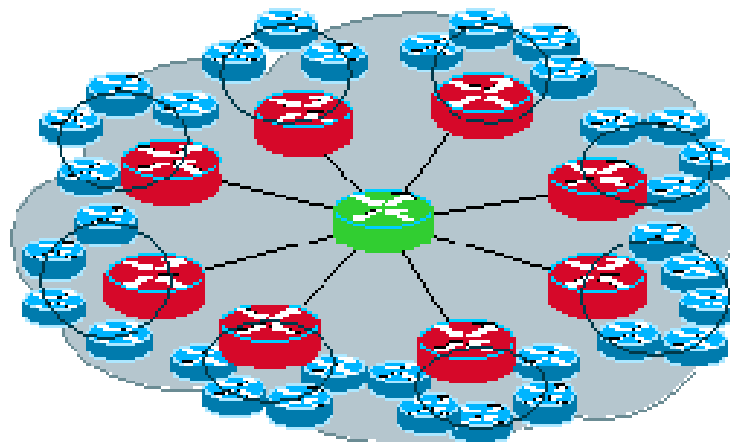
Small Network - simplified with a Gatekeeper



Medium Network - Multiple Gatekeepers



Medium-Large Network - Multiple Gatekeepers and a Directory Gatekeeper



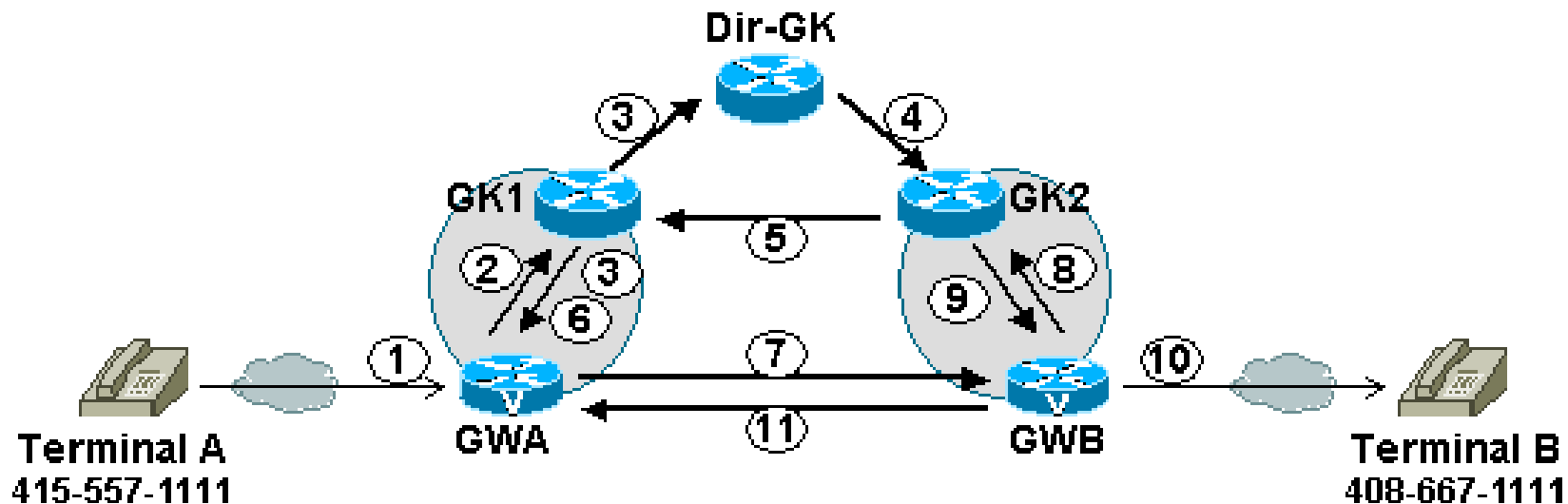
Gateway

Gatekeeper

Directory Gatekeeper

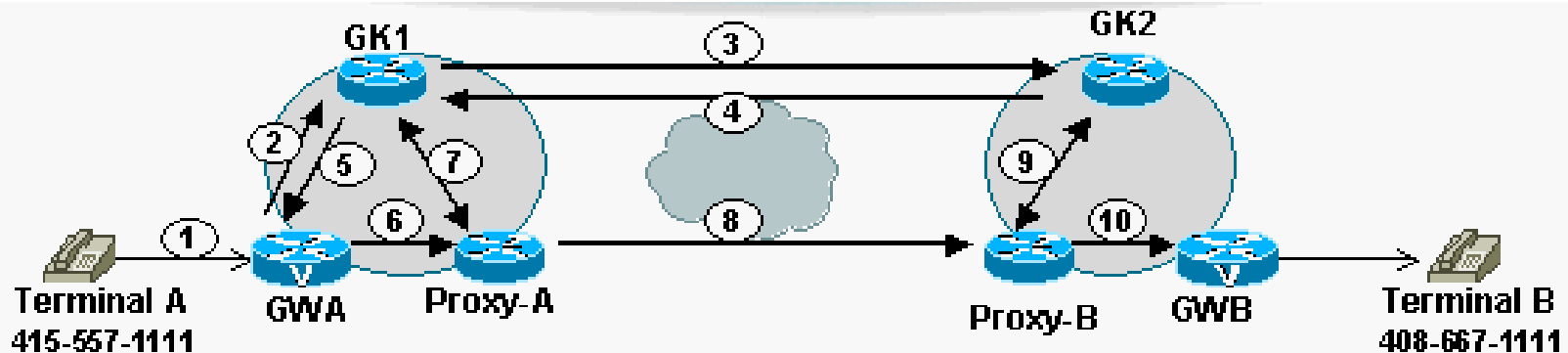


Inter-Zone Call Setup a Directory Gatekeeper



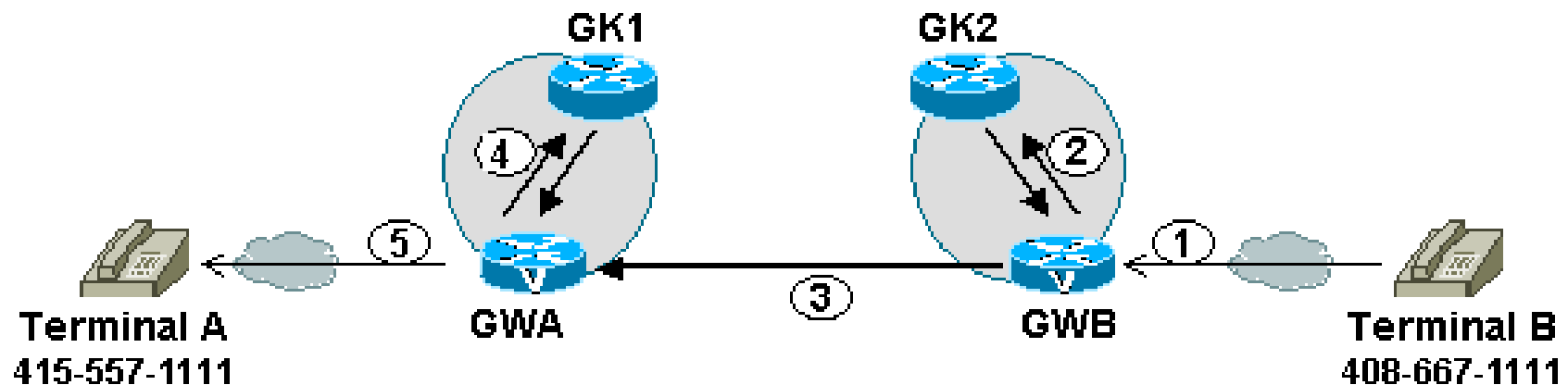
- 1) Terminal A **dials** the phone number 408-667-1111 for Terminal B
- 2) GWA sends GK1 an **ARQ**, asking permission to call Terminal B
- 3) GK1 does a look-up and does NOT find Terminal B registered; GK1 does a prefix look-up and finds a wildcard match with Dir-GK; GK1 sends **LRQ** to Dir-GK, and **RIP** to GWA (RIP – Request In Progress, informuje GW o zpracovávaném volání)
- 4) Dir-GK does a prefix look-up and finds GK2; Forwards the **LRQ** to GK2
- 5-11) Same as steps 4-10 in previous scenario

Proxy-Assisted Call Setup



- 1) Terminal A dials Terminal B
 - 2) GWA sends ARQ to GK1
 - 3) GK1 sends LRQ to GK2
 - 4) GK2 returns Proxy-B's address, hiding GWB's identity
 - 5) GK1 knows to get to Proxy-B, it must go through Proxy-A, so GK1 returns Proxy-A's address to GWA
 - 6) GWA calls Proxy-A
 - 7) Proxy-A consults GK1 to find the true destination, GK1 tells it to call Proxy-B
 - 8) Proxy-A calls Proxy-B
 - 9) Proxy-B consults GK2 for the true destination, which is GWB; GK2 gives GWB's address to Proxy-B
 - 10) Proxy-B completes the call to GWB
- From here the call proceeds as before...*

Call Disconnect

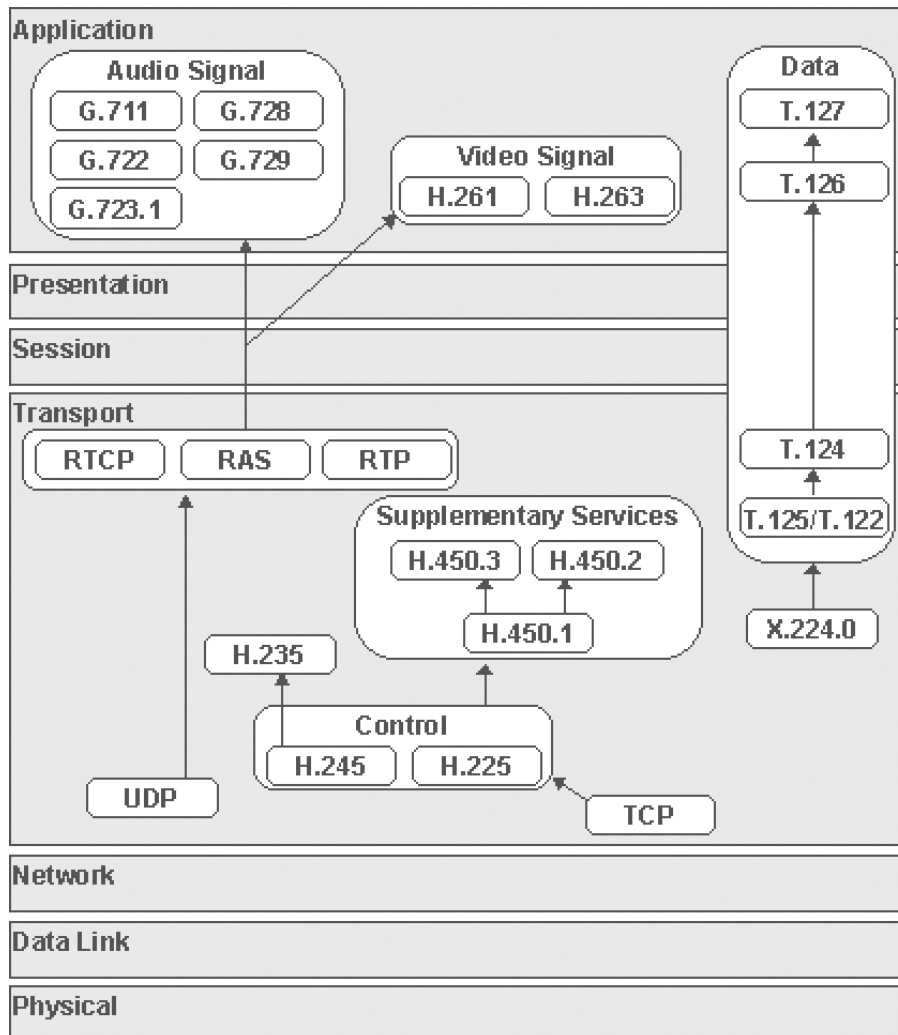


Terminals A and B are in active conversation...

- 1) Terminal B hangs up
- 2) GWB sends **DRQ** to GK2, disconnecting the call between Terminals A and B. A DCF is received some time later.
- 3) GWB sends a **Q.931 Release Complete** to GWA
- 4) GWA sends **DRQ** to GK1, disconnecting the call between Terminals A and B. A DCF is received some time later.
- 5) GWA signals a **call disconnect** to the voice network (the mechanism differs depending on the trunk used on GWA. If it is a phone set (FXS), then there is no mechanism to signal the disconnect.

5. Evolve H.323

Detailnější struktura protokolů H.323



Základní protokoly

- *H.225* pro signalizaci volání
- *RAS* pro registraci
- *H.235*, který definuje zabezpečení v H.323 systému
- *H.245* pro řízení signalizace a řízení toku dat

Aktuální stav standardu

H.323 Document Status and History

The following tables shows the current documents that are under consideration by [ITU-T SG16](#) Working Party 2 that are related to H.323, as well as a historical list of previously approved documents. This list does not represent an official list of publications from the [ITU](#). To see a list of current standards in force, visit the [H.323 standards](#) page.

Current H.323 Series Documents in Progress

| Document | Most Recent Document | Expected Approval |
|---|----------------------|-------------------|
| H.323 Annex I (Communication over Error-Prone Channels) | TD-334/WP2 (07/2010) | 12/2011 |
| H.450.1 | TD-335/WP2 (07/2010) | 03/2011 |
| H.450.2 | TD-336/WP2 (07/2010) | 03/2011 |
| H.460.23 Amendment 1 | C.390 (07/2010) | 03/2011 |
| H.460.24 Amendment 1 | C.389 (07/2010) | 03/2011 |

Decided/Approved Documents

| Document | Most Recent Document | Determination Decision | |
|--|-------------------------------------|------------------------|---------|
| H-Series Supplement 4 Release 1 (List of GEF Identifiers) | TD-74/PL (05/2003) | n/a | 05/2003 |
| H-Series Supplement 4 Release 2 (List of GEF Identifiers) | TD-79/PL (01/2004) | n/a | 01/2004 |
| H-Series Supplement 4 Release 3 (List of GEF Identifiers) | TD-61/PL (11/2004) | n/a | 11/2004 |
| H-Series Supplement 4 Release 4 (List of GEF Identifiers) | TD-111R1/WP (08/2005) | n/a | 08/2005 |
| H-Series Supplement 4 Release 5 (List of GEF Identifiers) | TD-259/PL (04/2006) | n/a | 04/2006 |
| H-Series Supplement 4 Release 6 (List of GEF Identifiers) | TD-419/PL (07/2007) | n/a | 07/2007 |
| H-Series Supplement 4 Release 7 (List of GEF Identifiers) | TD-217/PL (2010/07) | n/a | 07/2010 |
| H.225.0v3 | COM16-96 + TD-7/PL + TD-8/PL (9/99) | 05/1999 | 09/1999 |
| H.225.0v4 | COM16-134 + TD-91/PL (11/2000) | 02/2000 | 11/2000 |
| H.225.0v5 | TD-60R1/PL (05/2003) | AAP | 05/2003 |
| H.225.0v6 | TD-275/PL (04/2006) | AAP | 04/2006 |
| H.225.0v7 | TD-181/PL (10/2009) | AAP | 10/2009 |
| H.225.0v6 Amendment 1 | TD-315 (11/2006) | AAP | 11/2006 |
| H.225.0 Annex Gv1 (Communication Between Administrative Domains) | TD-32/PL + TD-53/PL (5/99) | 09/1998 | 05/1999 |
| H.225.0 Annex Gv2 (Communication Within and Between | TD-76/PL (10/2002) | AAP | 10/2002 |

H.323 Forum



- [Why H.323?](#)
- [H.323 Global Network](#)
- [H.323 Service Providers](#)
- [H.323 Products and Services](#)
- [Papers & Presentations](#)
- [H.323 Standards](#)
- [Open Specifications](#)
- [H.323 Developer Zone](#)
- [FAQs](#)
- [H.323 Forum Mailing Lists](#)
- [More Links](#)

Sponsored by:



Where it all comes together[™]

H.323 Forum™ Welcome

The H.323 Forum was formed in 2002 to bring more market awareness to the H.323 protocol, to provide a forum for technical discussions, and to serve as a launching board for new ideas that will lead us forward in the real-time multimedia application space.

After its initial launch, the H.323 Forum attracted thousands of people to its mailing lists and web site, held a number of successful events, and successfully brought the needed attention, not just to H.323, but to the entire VoIP and videoconferencing spaces.

While the marketing activities of the H.323 Forum have concluded, work is continuing in the form of technical specifications and white papers referred to as "Open Community Specifications," some of which are educational and some of which define new functionality for H.323. Discussion of these documents and other topics takes place on the H.323 Forum [mailing list](#).

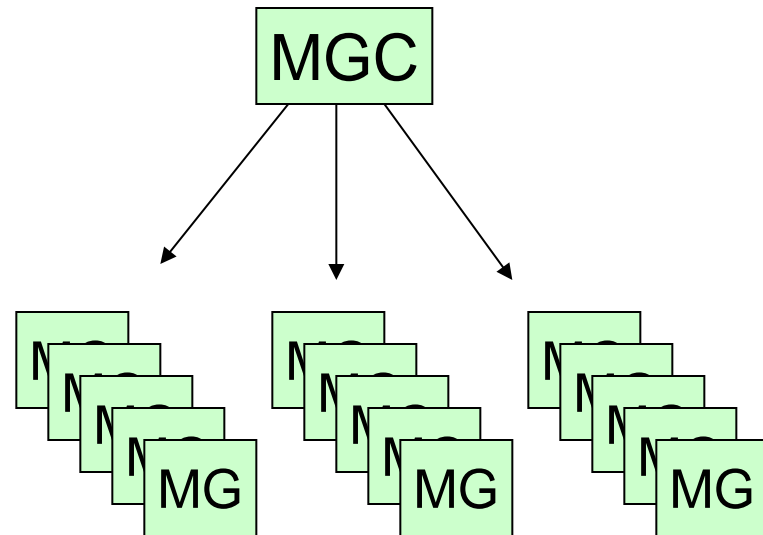
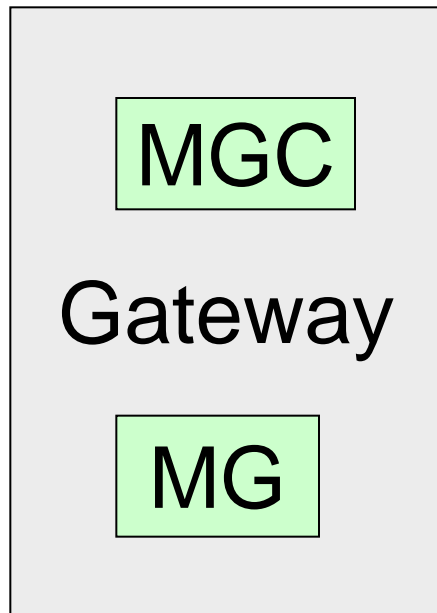
Equally important, the H.323 Forum, in partnership with the [IMTC](#) and [Packetizer](#), continues to serve as a place for people to learn more about H.323, to share ideas, and to develop new technologies related to multimedia communication.

Počáteční evoluce protokolu H.323

H.323 je binární protokol využívající syntaxe ASN.1 (PER). Jedná se o otevřený standard, který má blízkou návaznost na technologie používané v ISDN. Doporučené zvukové kodeky G.711, G.723, G.729, videokodeky H.261, H.263.

- H.323v1 (1996) byl původně určen jen pro sítě LAN, firmy ho ale hned s dobrým výsledkem vyzkoušely pro sítě WAN a Internet.
- H.323v2 (1998) přináší: bezpečnost, Fast Connect (též FastStart), doplňkové(supplementary) služby, lepší zajištění DTMF, škálovatelnost, TTL (Time to Live), předběžná potvrzení (Pre-granted ARQ) , URL, integrace s T.120 (videokonference).
- H.323v3 (1999) přináší lepší integraci s PSTN, UDP (Annex E), jednoduché koncové body (Annex F), komunikace mezi administrativními doménami – řeší Annex G (Border Element) či RAS zprávou „Location Request“ (LRQ).
- H.323v4 (2000) – dekomponované brány, alternativní gatekeepery, hlášení kapacity koncových bodů, nové služby, „must have“ vlastnosti , Generic Extensibility Framework (GEF) – blíže viz další slajdy.

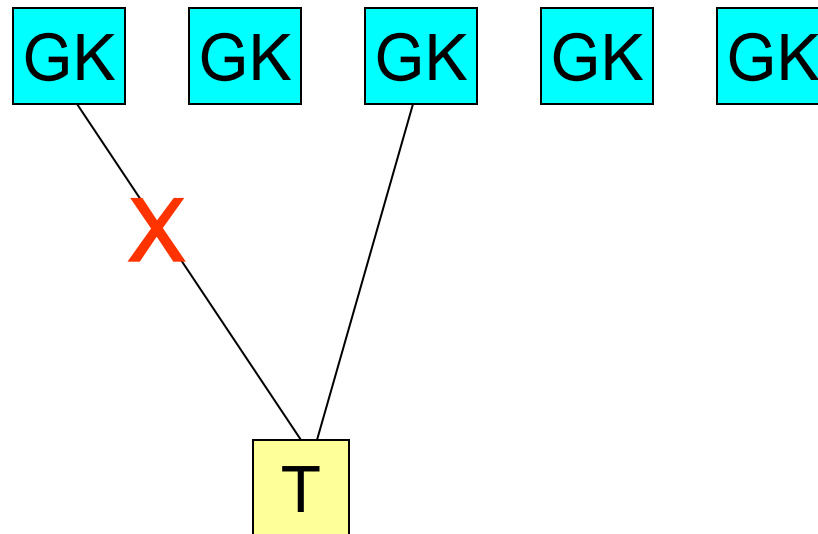
Dekomponované brány



Media Gateway Controller (MGC) – zajišťuje řízení
Media Gateway (MG) – převádí mediální tok

Odděluje funkce MGC od funkcí MG – s více MG lze lépe škálovat kapacitu toku
Komunikaci mezi MGC a MG zajišťuje protokol H.248.

Alternativní gatekeepery



Nové služby

Annex K – Services via HTTP

Annex L – Stimulus Control

H.450.8 – Name identification

H.450.9 – Call Completion

H.450.10 – Call Offer

H.450.11 – Call Intrusion

„Must have“ vlastnosti

- Hlášení použití
- Identifikace volajícího
- Mapování aliasů
- lepší management pásma pro multicast
- použití pro fax
- tunelování jiných protokolů (Annex M.x)
- H.323 specifická URL
- Výpočet kreditů
- Přenos DTMF přes RTP (RFC 2833)

Generic Extensibility Framework

- Stanovení způsobu, jak lze doplňovat volitelné vlastnosti beze změny platné syntaxe ASN.1
- Odolnost proti výpadkům (Annex E pro UDP transport)
- Jsou zde procedury zajišťující robustnost adres (Annex R)
- Přenosnost lokálních čísel (Annex H)

H.323v5 (2003)

- Annex M.3 – tunelování DSS1 (Digital Subscriber Signalling System No. 1, (Euro-ISDN či E-DSS1) signalizace uvnitř H.323 systémů
- Annex O – definuje, jak použít H.323 URL a další DNS služby
- Annex P – přenos přes modemy (jak použít protokol V.150.1)
- Annex Q – řízení vzdálených kamer pro videokonference
- Annex R – řeší fault tolerant systémy – volání není přerušeno v případě výpadku mezilehlé signalizační entity jako je softswitch (GEF)

- H.460.1 – úvod do GEF a „author's guide“
- H.460.2 – portabilita čísel (GEF)
- H.460.3 – mapa stavu obvodů (GEF), využití je pro přenos do PSTN
- H.460.4 – řešení priorit volání (GEF)
- H.460.5 – přenos duplicitních částí IE zpráv protokolu Q.931 (GEF)
- H.460.6 – rozšíření Fast Connectu z verze 2 (GEF)
- H.460.7 – digitální mapování v koncových bodech spojení (GEF)
- H.460.8 – fronty a alternativní směry (GEF)
- H.460.9 – monitorování a hlášení QoS (GEF)

Verze 5

User Datagram Protocol, Src Port: 49301 (49301), Dst Port: h323gatestat (1719)
H.225.0 RAS

- ▣ RasMessage: gatekeeperRequest (0)
 - ▣ gatekeeperRequest
 - requestSeqNum: 2
 - protocolIdentifier: 0.0.8.2250.0.5 (Version 5)
 - ▣ nonStandardData
 - ▣ rasAddress: ipAddress (0)
 - ▣ endpointType
 - ▣ endpointAlias: 1 item
 - ▣ tokens: 1 item
 - ▣ authenticationCapability: 2 items
 - ▣ algorithmOIDs: 2 items
 - ▣ featureSet



Transmission Control Protocol, Src Port: 4296 (4296), Dst Port: h323hostcall (1720)
TPKT, Version: 3, Length: 1367
Q.931

H.225.0 CS

- ▣ H323-UserInformation
 - ▣ h323-uu-pdu
 - ▣ h323-message-body: setup (0)
 - ▣ setup
 - protocolIdentifier: 0.0.8.2250.0.5 (Version 5)
 - ▣ sourceInfo
 - ...0 activeMC: False
 - conferenceID: 00000000-0000-1000-0000-0000c0a81017
 - ▣ conferenceGoal: callIndependentSupplementaryService (4)
 - ▣ callType: pointToPoint (0)
 - ▣ callIdentifier
 - ▣ fastStart: 36 items
 - 1... mediaWaitForConnect: True
 - 1... canOverlapSend: True
 - 0... h245Tunnelling: False



Protokol H.235

- Stanovuje **bezpečnostní profily**. To je nezbytné, protože H.323 nemá implementovány žádné jiné bezpečnostní mechanismy.
- Definované profily zavádějí různé stupně ochrany a zahrnují množinu bezpečnostních mechanismů.

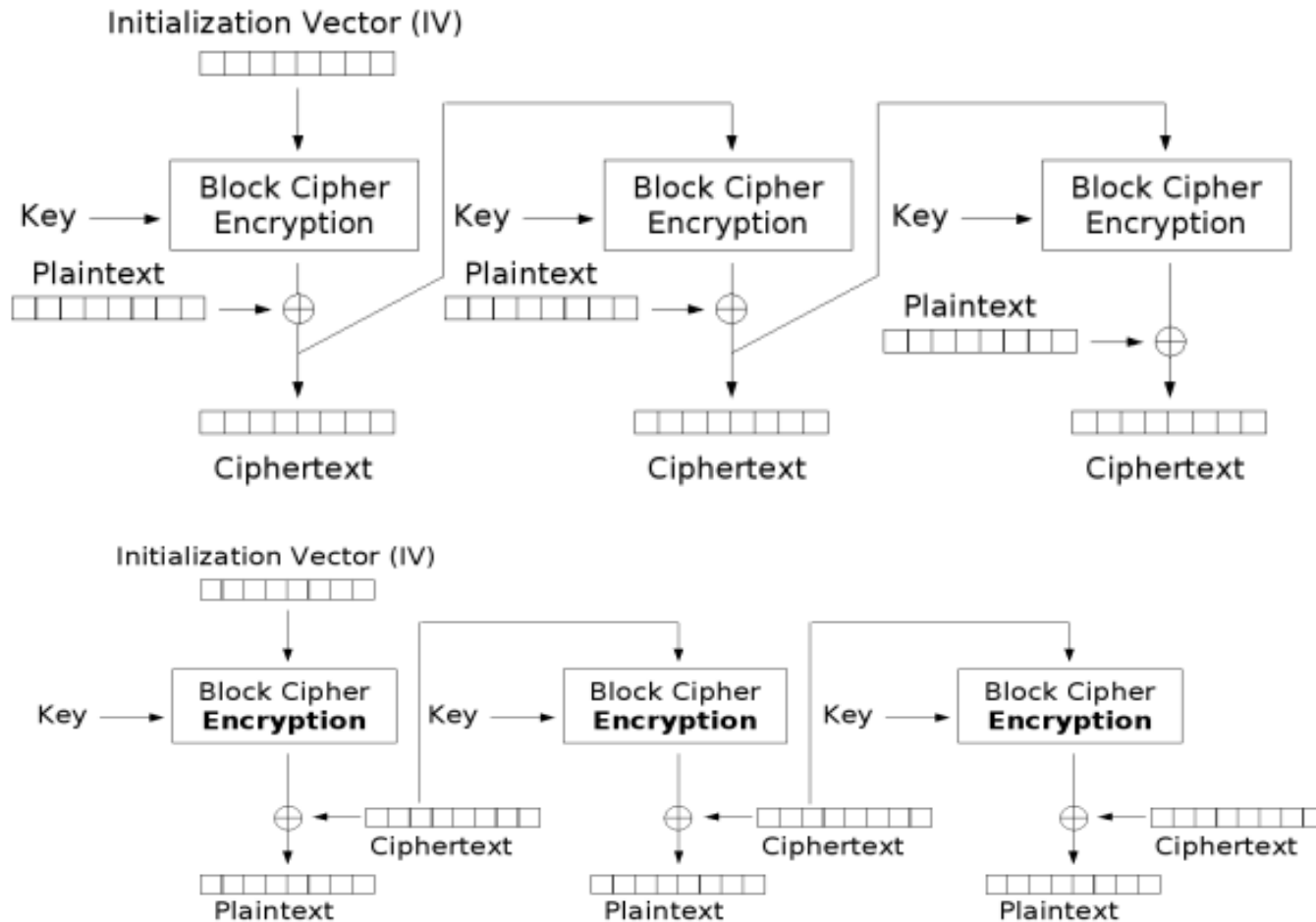
Bezpečnostní profily v dodatcích protokolu H.235

První verze protokolu H.235 vydalo ITU v roce 1998, po ní následovala v roce 2000 významná verze 2, která standardizovala podporu šifrovacímu standardu AES (Advanced Encryption Standard) a kryptografii eliptických křivek.

Pro interoperabilitu definovala některé bezpečnostní profily v dodatcích:

- Annex D – Shared secrets and keyed hashes
- Annex E – Digital signatures on every message
- Annex F – Digital signatures and shared secret establishment on first handshake, afterwards keyed hash usage
- Annex G – SRTP & MIKEY usage

Co je to za mód?



Verze protokolu H.235 a jeho dodatky

- *Annex D – Shared secrets and keyed hashes*, v němž byl pro výměnu klíčů v rámci protokolů H.225 a H.245 standardizován algoritmus **Diffie-Hellmana** a pro šifrování a kontrolu integrity algoritmus HMAC-SHA1-96, pro šifrování v rámci RTP DES, Triple-DES a AES;
- *Annex E – Digital signatures on every message*, v němž byly pro autentizaci a kontrolu integrity standardizovány algoritmy SHA1 a MD5;
- *Annex F – Digital signatures and shared secret establishment on first handshake, afterwards keyed hash usage*, v němž bylo doplněno šifrování pro H.225 a H.245 na bázi RSA. H.235 ve verzi 3 z roku 2003 doplňuje verzi 2 o procedury pro šifrování signálů DTMF (touch tone), identifikaci objektů pro šifrování zátěže algoritmem AES a speciální mód EOFB (Enhanced Outer FeedBack) pro šifrování proudů hlasových paketů. Během dalších dvou let vyšly další dodatky verze 2 protokolu H.235, z nichž je zvláště významný dodatek G:
- *Annex G – SRTP & MIKEY usage*, který byl zpracován pro podporu protokolu SRTP.

Jak dlouhý klíč dnes volíme pro D-H algoritmus?

$$Y = q^x \text{ mod } p$$

Annex D

Shared secrets and keyed hashes, v němž byl pro výměnu klíčů v rámci protokolů H.225 a H.245 standardizován algoritmus Diffieho-Hellmana a pro šifrování a kontrolu integrity algoritmus HMAC-SHA1-96, pro šifrování v rámci RTP: DES, Triple-DES a AES

$$Y = q^x \text{ mod } p$$

Velikost p 1024 nebo 3072

Velikost q 160 nebo 256

Řešení klíčového managementu: MIKEY

(Multimedia Internet Keying)

- Protokol SRTP sám o sobě nedefinuje klíčový management, nýbrž pracuje se sadami parametrů, z nichž odvozuje klíče relací pro šifrování, autentizaci a kontrolu integrity.
- Preferovaným řešením klíčového managementu je MIKEY, které bylo navrženo v rámci pracovní skupiny MSEC IETF a které bylo publikováno v RFC 3830.
- *Řešení MIKEY* má široké použití – jak pro RTSP tak pro SIP, tok řídicích i multimedialních paketů, pro unicast i multicast přenosy atd.

Volby MIKEY

pro autentizaci a vyjednávání

Definovány jsou **tři volby pro autentizaci a vyjednávání** tzv. master key, všechny jsou přitom založeny na dvoucestném handshakingu. Tyto volby jsou:

- distribuce symetrických klíčů – předsdílené klíče, kontrola integrity pomocí MAC (message authentication code);
- distribuce asymetrických klíčů;
- dohoda o klíči na bázi algoritmu Diffie-Hellmana chráněná digitálními podpisy před útokem MitM (Man-in-the-Middle).

V H.235v3 je uvažována ještě čtvrtá možnost, ta však není součástí specifikací MIKEY; předpokládá se zde výměna Diffieho-Hellmanových klíčů pomocí předsdílených symetrických šifrovacích algoritmů.

Pro přenos klíčů je povinně určen algoritmus AES v módu CTR resp. Counter.

MIKEY používá 160bitový autentizační tag generovaný pomocí HMAC s SHA-1, tak jak je to popsáno v RFC 2104. Při použití asymetrických mechanismů je další povinnou záležitostí **použití certifikátů** podle standardu X.509v3 pro šifrování veřejným klíčem a digitální podpisy.

Firewally jako problém pro H.323

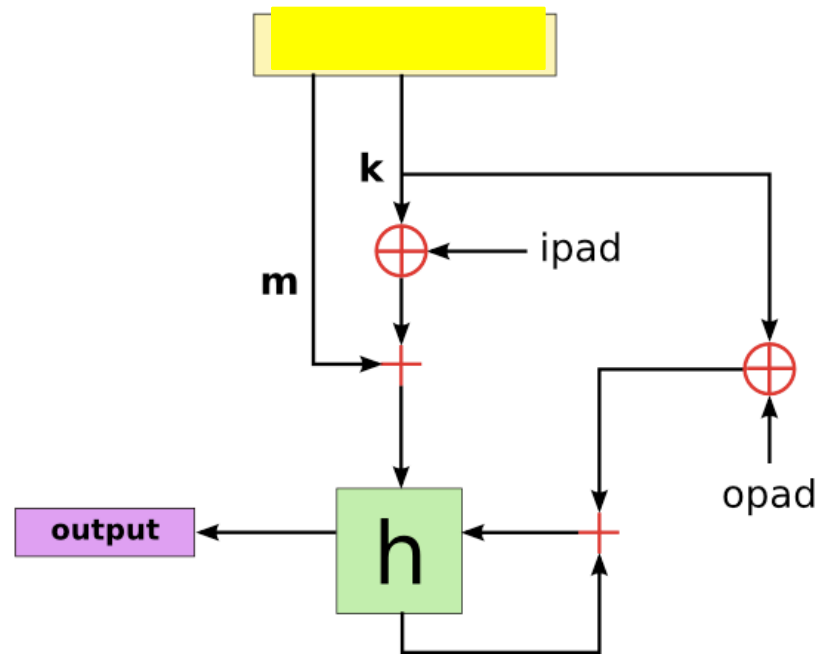
- Jde o **zvlášť nepříjemný problém**. S výjimkou „Q.931.like“ protokolu H.225 je všechny H.323 provoz je směrován přes dynamické porty. Pro Fast Start protokolu H.323 je obvykle využít port 1720. Pokud přidáme komunikaci RAS protokolu H.225 přes gatekeeper (UDP), je použit port 1719. **Každý další kanál znamená přiřazení dalšího portu**. Bylo by třeba mít dlouhodobě otevřeny desetitisíce UDP portů.
- Zprávy H.323 je schopen zpracovávat pouze stavový firewall. Ani pro tyto firewally není provoz protokolu H.323 triviální záležitost. Zprávy protokolu H.323 jsou kódovány v binárním formátu založeném na ASN.1. ASN.1 nepracuje s pevným umístěním adresní informace (offset) v paketu a **takový provoz je obtížné dekódovat**, neporadí si s ním nejen paketové filtry, ale i jednodušší stavové firewally. Prohledávání obsahu paketů zakódovaných pomocí ASN.1 zanáší **další zpoždění** do citlivých zařízení zajišťujících přenos hlasu.

NAT jako problém pro H.323

NAT je dalším problémem pro systémy na bázi VoIP používající pro navázání spojení protokol H.323. Pro tyto potřeby musí být speciálně uzpůsoben, aby mezi konci spojení správně protékaly dvojice IP adresa/port.

Opakování: Co je to za algoritmus?

$$H[(k \oplus \text{opad}) || H[k \oplus \text{ipad} || m]]$$



Šifrování a HMAC jako problém pro H.323

- Šifrování není pro hlasové služby výkonnostní problém, protože u proudové šifry jde jen o jednobitové zpoždění.
- Naopak operace algoritmu HMAC potřebují pro své zpracování celý blok dat, a to na straně vysílání i příjmu. To může vést ke **zpožděním**, která způsobují velké zkreslení hlasu.
- Někteří návrháři se domnívají, že autentizace při navazování spojení stačí a použití HMAC v průběhu vlastní konverzace omezují.

Shrnutí problémů H.323

- firewally – desetitisíce UDP portů
- NAT – speciálně uzpůsoben
- šifrování – malé zpoždění
- HMAC – velké zpoždění

Security Framework a.k.a. H.235v4

- Od roku 2005 lze na webu nalézt návrhy nového bezpečnostního rámce (Security Framework – a.k.a. H.235v4) pro protokol H.323 zpracované ITU-T Study Group 16. Otázkou je další dostupnost norem, které nejsou u ITU tradičně bezplatně dostupné. Mód je rovněž znám pod názvy Integer Counter Mode (ICM) a Segmented Integer Counter (SIC).
- Od roku 2005 nebyl protokol H.235 dále rozvíjen, pouze v roce 2008 byl bezpečnostní rámec doplněn o Amendment 1 (ITU-T Rec. H.235.6 Amendment 1 „H.323 security: Voice encryption profile with native H.235/H.245 key management: Support for 192 and 256 bits AES“), který je odezvou na potřebu použití AES s delším klíčem.

Jednotlivé složky rámce Security Framework a.k.a. H.235v4

| | |
|---------|---|
| H.235.0 | Security framework for H-series (H.323 and other H.245-based) multimedia systems (a.k.a, H.235v4) |
| H.235.1 | Baseline Security Profile |
| H.235.2 | Signature Security Profile |
| H.235.3 | Hybrid Security Profile |
| H.235.4 | Direct and Selective Routed Call Security |
| H.235.5 | Framework for secure authentication in RAS using weak shared secrets |
| H.235.6 | Voice encryption profile with native H.235/H.245 key management (See also Amendment 1) |
| H.235.7 | Usage of the MIKEY Key Management Protocol for SRTP |
| H.235.8 | Key Exchange for SRTP using secure Signalling Channels |
| H.235.9 | Security Gateway Support for H.323 |

H.323v6 (2006)

- Primární změnou je **koncept „Assigned Gatekeeper“** (k nim jsou koncové body registrované, např. z důvodu geografické vzdálenosti). Rozdíl oproti alternativním gatekeeperů je v tom, že si po přepnutí na alternativní gatekeeper stav přidělených gatekeeperů neustále monitoruje a po eliminaci důvodu přepnutí se vše vrací do původního stavu. Takovýto postup umožňuje efektivní hospodaření se zdroji.
- Pro podporu doporučení ITU-T V.151 byly k Annex G zpracovány dodatky pro podporu ToIP (Text over IP) prolínaného s audiem.
- Dále byly doplněny nové kodeky GSM, iLBC, a H.264.
- V oblasti bezpečnosti byl dokument H.235 rozčleněn na H.235.0 až H.235.9 atd. a byla přidána podpora pro SRTP.
- Řada nových funkcí byla doplněna inkrementálně, byly vytvořeny i další nové dokumenty.

Nové dokumenty H.323v6

- H.239 – management rolí (živé video, prezentace atd.)
- H.241 – rozšíření procedur videa (např. o podporu H.264 – AVC)
- H.249 – rozšíření User Input Indications o událostí typu klik či pohyb kurzoru
- H.361 – End-to-End QoS a signalizace priorit služeb
- H.460.10 – transport pole ISUP „Call Party Category“
- H.460.11 – nastavení zpožděného volání např. při průchodu firewallem
- H.460.12 – mechanismus řešení kolize při výběru stejného obvodu GK
- H.460.13 – dohled nad speciálními voláními (pohotovost atd.)
- H.460.14 – Podpora MLPP (Multi-Level Precedence and Pre-emption)
- H.460.15 – možnost shodit a přesměrovat volání
- H.460.16 – zajištění handshakingu pro doručení zprávy Release Complete (obrana před vyhazováním zpráv TCP po uzavření soketu)
- H.460.17 – tunelování RAS přes H.225.0 (část NAT/FW řešení)
- H.460.18 – přenosy signalizace přes NAT a firewally
- H.460.19 – přenosy média přes NAT a firewally jako proxy
- H.460.20 – transport „location number“ (obdobně ISUP – ISDN User Part)
- H.460.21 – rozhlašování zpráv

H.323v7 (2009)

Změny základních specifikací (H.225.0, a H.245) byly omezeny na minimum. Nicméně byla doplněna řada nových důležitých vlastností, což se opět řešilo pomocí GEF:

- “single transmitter multicast”, což je užitečné např. pro MoH (Music on Hold) šířené ze známé IP adresy a známého portu.
- Vlastnost umožňující H.323 síťovému prvku (např. MCU) kontaktovat H.323 terminály (např. videokonferenční či teleprezentační systém) a doručit jim kontaktní informace a na terminálu pak stačí pro připojení do konference jen stlačit tlačítko.
- Schopnost přenášet v rámci H.225.0 **informaci o volání ve více jazycích**. Je to užitečné např. u mezinárodních poboček, kdy si může volaný zobrazit identifikaci volajícího v preferovaném jazyku.
- Přenos varovných a poplašných zpráv protokolu CAP (Common Alerting Protocol, viz doporučení ITU-T Recommendation X.1303) systémem H.323.

Nové specifikace H.323v7

- H.460.22 – zajišťuje před vlastním voláním sesouhlasení bezpečnostních procedur mezi koncovými body. To například umožňuje před zahájením volání zjistit, zda volaný podporuje daný bezpečnostní signalizační mechanismu (např. IPSec či TLS).
- H.460.23 – umožňuje pro H.323 zařízení za NAT/FW v koordinaci s gatekeeperem a STUN serverem zjistit typ NAT/FW, což se využívá v rámci H.460.24.
- H.460.24 – definuje, jak zajistit komunikaci mezi koncovými body oddělenými NAT/FW zařízeními. Pokud dané zařízení nemá podporu protokolu pro přímé toky, je použito proxy v souladu s H.460.19.

Strategie použití H.460.23 a H.460.24 vychází z použití těchto protokolů před zahájením volání, neboli většinou nezatěžují ALG (Application Layer Gateway), media proxy či jiné zařízení.

H.323v8 zatím není

Current H.323 Series Documents in Progress

| Document | Most Recent Document | Expected Approval |
|---------------------------------|-------------------------|-------------------|
| H.323v8 | TD 357/WP1 (2016-05) | 01/2016 |
| H.225.0v8 | TD 365/WP1 (2016-05) | 01/2016 |
| H.245v17 | TD 352R1/WP1 (2016-05) | 01/2016 |
| H.235.10 (DTLS) | TD 346R1/WP1 (2016-05) | 01/2016 |
| H.EMQ | TD 259/WP1 (2015-02) | 2018 |
| H.TPS-AV | TD 359R1/WP1 (2016-06) | 01/2016 |
| H.TPS-SIG | TD 354 R1/WP1 (2016-06) | 01/2016 |

Závěr: Výhody H.323

- Výborná integrace s PSTN
- Použití pro hlas, obraz i data
- Vhodný jak pro audiokonference, tak pro videokonference
- Standard přijatý výrobci i organizacemi jako je ETSI
- Rychlé přidávání nových služeb

Závěr: Kritika H.323

- Přílišná komplexnost – není ale nezbytné realizovat každou komponentu
- Kodeky jsou podle ITU – není problém doplnit libovolný kodek
- Gatekeepery jako prvek zesložitující řešení
 - mohou zabezpečovat rozklad adres
 - komunikace mezi jednoduchými telefony a složitými zařízeními
 - platforma pro doplňování nových služeb
 - a nakonec – nejde o povinný prvek

6. Příklady konfigurace na Cisco

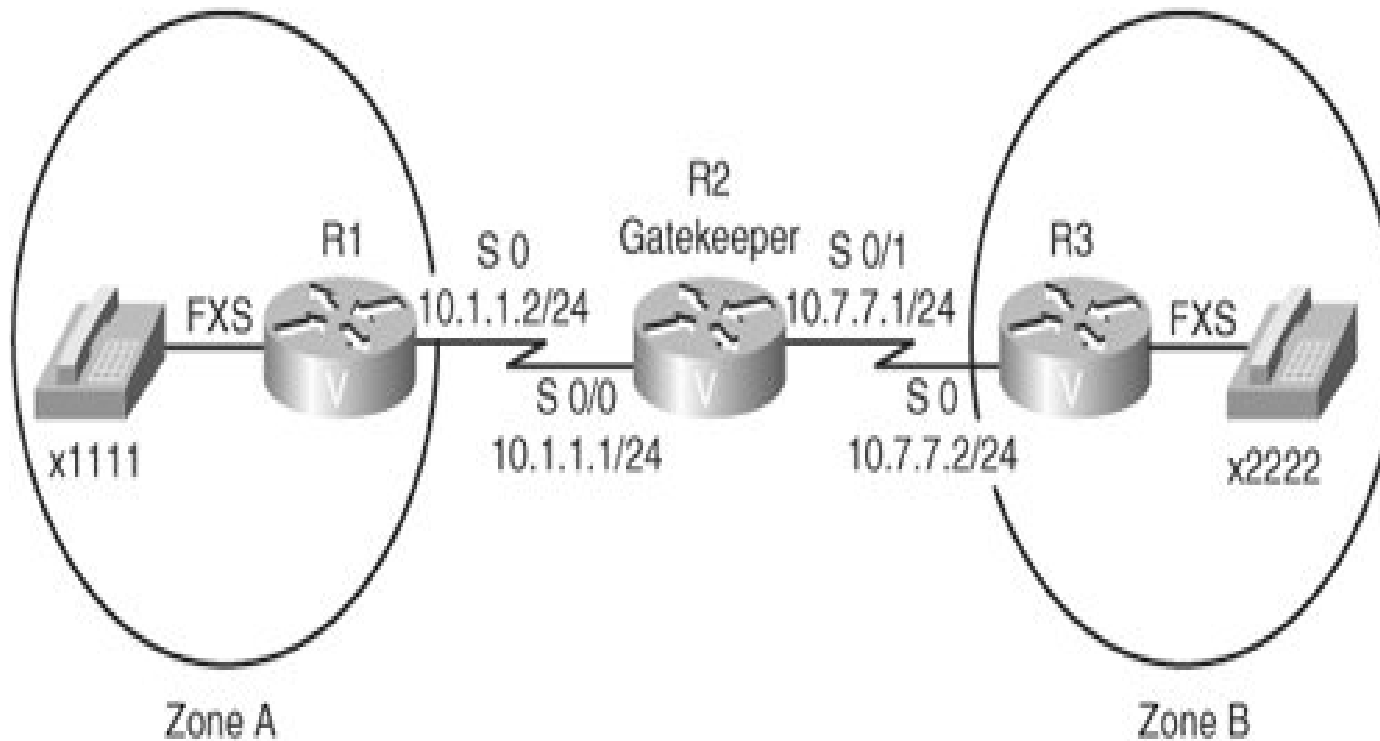
1. konfigurace

konfigurace brány H.323

```
Router(config)#voice service voip
Router(conf-voi-serv)#h323
Router(conf-voi-serv)#no shutdown
Router(config)#interface loopback 0
Router(config-if)#ip address 10.10.1.1 255.255.255.0
Router(config-if)#h323-gateway voip interface
Router(config-if)#h323-gateway voip h323-id gw1
Router(config-if)#h323-gateway voip bind srcaddr 10.10.1.1
Router(config)#voice class codec 100
Router(config-class)#codec preference 1 g711alaw
Router(config-class)#codec preference 2 g729br8
Router(config)#dial-peer voice 500 voip
Router(config-dial-peer)#codec g711alaw
Router(config)#voice class h323 600
Router(config-class)#h225 timeout tcp establish 10 (impl. 15)
Router(config-class)#h225 timeout setup 10
Router(config)#dial-peer voice 500 voip
Router(config-dial-peer)#voice-class h323 600
Router(config)#voice service voip
Router(conf-voi-serv)#h323
Router(conf-serv-h323)#h225 timeout tcp call-idle never
```

2. Konfigurace

(konfigurace gatekeeperu mezi dvěmi branami)



Konfigurace směrovače R2 (gatekeeper)

```
gatekeeper
```

```
zone local ZoneA acme.com 10.7.7.1
```

```
zone local ZoneB acme.com
```

```
zone prefix ZoneA 1...
```

```
zone prefix ZoneB 2...
```

```
gw-type-prefix 1#* default-technology
```

```
arq reject-unknown-prefix
```

```
bandwidth interzone default 64
```

```
bandwidth session default 16
```

```
no shutdown
```

Konfigurace směrovače R1 (brána)

```
interface Serial0
  bandwidth 128
  ip address 10.1.1.2 255.255.255.0
  encapsulation ppp
  h323-gateway voip interface
  h323-gateway voip id ZoneA ipaddr 10.7.7.1
1719
  h323-gateway voip h323-id R1
  h323-gateway voip tech-prefix 1#
  !
  gateway
  !
dial-peer voice 2222 voip
  destination-pattern 2222
  session target ras
```

Konfigurace směrovače R3 (brána)

```
interface Serial0
  bandwidth 2000
  ip address 10.7.7.2 255.255.255.0
  encapsulation ppp
  clock rate 2000000
  h323-gateway voip interface
  h323-gateway voip id ZoneB ipaddr 10.7.7.1
  1719
  h323-gateway voip h323-id R3
interface Serial0
  h323-gateway voip tech-prefix 1#
!
gateway
!
dial-peer voice 1111 voip
  destination-pattern 1111
  session target ras
```

Kontrola na R1

```
R1#show gateway
```

```
H.323 ITU-T Version: 4.0    H323 Stack Version:  
0.1
```

```
H.323 service is up
```

```
Gateway R1 is registered to Gatekeeper ZoneA
```

```
Alias list (CLI configured)
```

```
E164-ID 1111
```

```
H323-ID R1
```

```
Alias list (last RCF)
```

```
E164-ID 1111
```

```
H323-ID R1
```

```
H323 resource thresholding is Disabled
```


Kontrola na R3

```
R3#show gateway
```

```
H.323 ITU-T Version: 4.0    H323 Stack Version: 0.1
```

```
  H.323 service is up
```

```
  Gateway R3 is registered to Gatekeeper ZoneB
```

```
Alias list (CLI configured)
```

```
  E164-ID 2222
```

```
  H323-ID R3
```

```
Alias list (last RCF)
```

```
  E164-ID 2222
```

```
  H323-ID R3
```

```
  H323 resource thresholding is Disabled
```

Kontrola na R2

```
R2#show gatekeeper endpoints
```

```
GATEKEEPER ENDPOINT REGISTRATION
```

```
=====
```

| CallSignalAddr | Port | RASignalAddr | Port | Zone Name | Type | Flags |
|--|-------|--------------|-------|-----------|---------|-------|
| ----- | ----- | ----- | ----- | ----- | ----- | ----- |
| 10.1.1.2 | 1720 | 10.1.1.2 | 52605 | ZoneA | VOIP-GW | |
| E164-ID: 1111 | | | | | | |
| H323-ID: R1 | | | | | | |
| Voice Capacity Max.= Avail.= Current.= 1 | | | | | | |
| 10.7.7.2 | 1720 | 10.7.7.2 | 52354 | ZoneB | VOIP-GW | |
| E164-ID: 2222 | | | | | | |
| H323-ID: R3 | | | | | | |
| Voice Capacity Max.= Avail.= Current.= 1 | | | | | | |

```
Total number of active registrations = 2
```

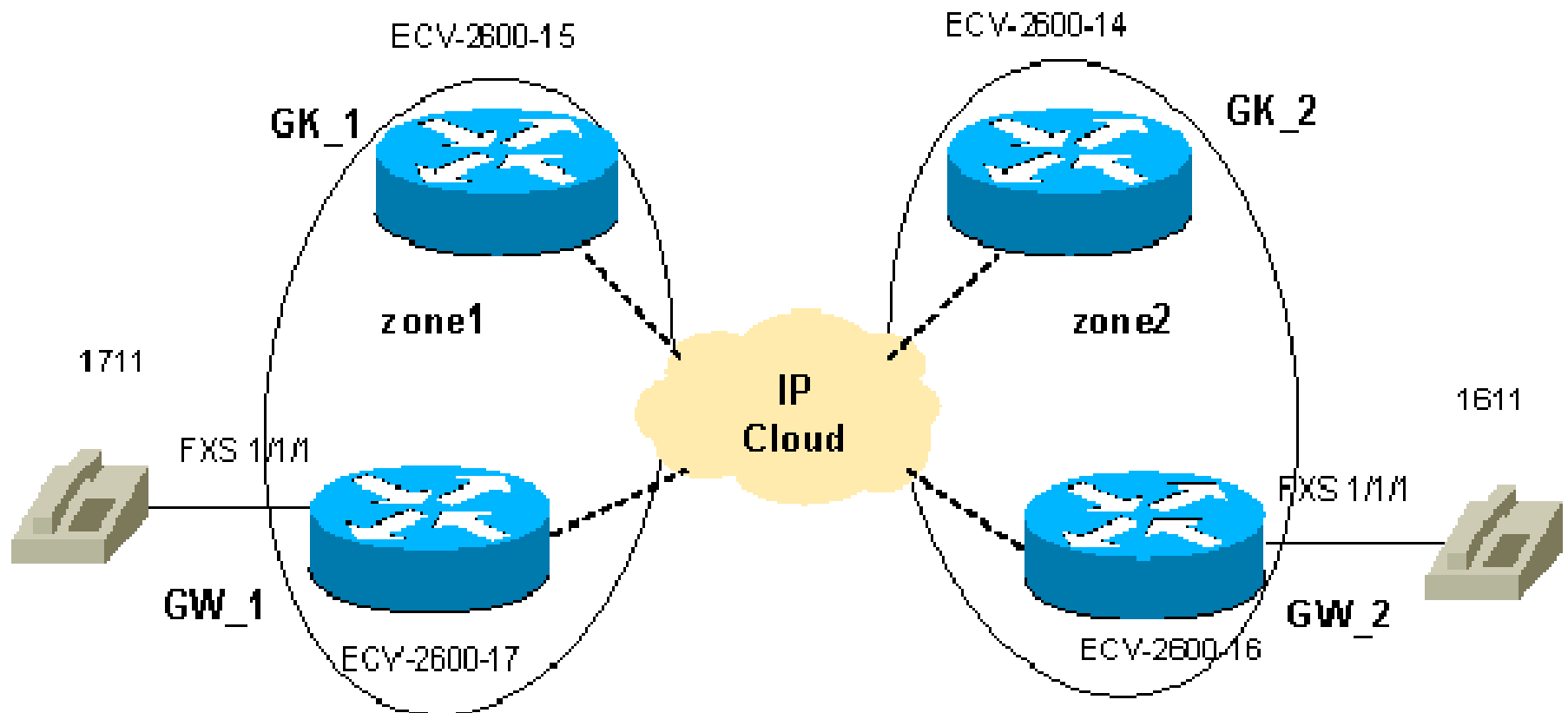
Aktivita RAS na směrovači R1 (konec příkladu)

```
R1#show h323 gateway ras
```

```
RAS STATISTICS AT 00:25:56
```

| RAS MESSAGE | REQUESTS SENT | CONFIRMS RCVD | REJECTS RCVD |
|-----------------|---------------|---------------|--------------|
| GK Discovery | grq 5 | gcf 1 | grj 0 |
| Registration | rrq 34 | rcf 34 | rrj 0 |
| Admission | arq 1 | acf 1 | arj 0 |
| Bandwidth | brq 0 | bcf 0 | brj 0 |
| Disengage | drq 0 | dcf 0 | drj 0 |
| Unregister | urq 0 | ucf 0 | urj 0 |
| Resource Avail | rai 0 | rac 0 | |
| Req In Progress | rip 0 | | |

3. konfigurace



GW_1 – ECV-2600-17 – část 1

```
hostname ECV-2610-17
!
interface Ethernet0/0
ip address 10.52.218.49 255.255.255.0
h323-gateway voip interface
!---- This command enables VoIP GW functions on the interface.
h323-gateway voip id gk-zone1.test.com ipaddr 10.52.218.47 1718
!---- This command defines the GK this GW works with.
h323-gateway voip h323-id gw_1
!---- This command defines the GW alias for the GK.
h323-gateway voip tech-prefix 1#
!---- It is desirable to have tech prefix on the GW for
!---- reliable registration and call routing.
h323-gateway voip bind srcaddr 10.52.218.49
!---- This command is not necessary in this simple topology,
!---- but for complex networks, it is recommended to use it.
```

GW_1 – ECV–2600–17 – část 2

```
voice-port 1/1/1
!
dial-peer voice 1 voip
destination-pattern 16..
session target ras
!!---- All IP addresses for the destination pattern 16.. should
!!---- be resolved through the requests to the GK.
!
dial-peer voice 2 pots
destination-pattern 1711
port 1/1/1
no register e164
!!---- This command prevents registration of this number with
!!---- the GK. The GW is registered with the GK with this alias only.
!
gateway
!
end
```

GW_2 – ECV-2600-16

```
hostname ECV-2610-16
!
interface Ethernet0/0
ip address 10.52.218.48 255.255.255.0
h323-gateway voip interface
h323-gateway voip id gk-zone2.test.com ipaddr 10.52.218.46 1718
h323-gateway voip h323-id gw_2
h323-gateway voip tech-prefix 1#
h323-gateway voip bind srcaddr 10.52.218.48
voice-port 1/1/1
!
dial-peer voice 1 voip
destination-pattern 17..
session target ras
!
dial-peer voice 2 pots
destination-pattern 1611
port 1/1/1
no register e164
```

GK_1 ECV-2600-15

```
hostname ECV-2610-15
!
interface Ethernet0/0
ip address 10.52.218.47 255.255.255.0
!
gatekeeper
zone local gk-zone1.test.com test.com 10.52.218.47
!---- This command defines the local zone. The GK name and
!---- zone name have the same meaning.
zone remote gk-zone2.test.com test.com 10.52.218.46 1719
!---- This command defines the name of the remote GK (zone).
zone prefix gk-zone2.test.com 16..
!---- This command explicitly defines the number length with
!---- the number of dots.
zone prefix gk-zone1.test.com 17.. gw-priority 10 gw_1
!---- This command explicitly defines which GW handles
!---- calls for 17.. numbers that could be done for the
!---- local zones only.
gw-type-prefix 1#* default-technology
!---- This command defines the default technology prefix
!---- that is necessary for routing decisions.
no shutdown
```


GK_2 ECV-2600-14

```
hostname ECV-2610-14
!
interface Ethernet0/0
ip address 10.52.218.46 255.255.255.0
!
gatekeeper zone local gk-zone2.test.com test.com 10.52.218.46
zone remote gk-zone1.test.com test.com 10.52.218.47 1719
zone prefix gk-zone2.test.com 16.. gw-priority 10 gw_2
zone prefix gk-zone1.test.com 17..
gw-type-prefix 1#* default-technology
no shutdown
!
end
```

Informační zdroje

- Packetizer <http://www.packetizer.com/>
- H.323 Forum <http://www.h323forum.org/>
- H.323 Plus <http://www.h323plus.org/>
- Doporučuji
http://www.yamahaproaudio.com/global/en/training_support/selftraining/dante_guide/chapter2/05_multicast/

Opakování protokolů použitých v H.323

- H.225.0 Registrace, signalizace
- H.245 Sestavování a řízení komunikačního kanálu
- RTP Přenos multimediálního streamu
- H.235 Zajištění bezpečnosti (jak signalizace, tak dat)
- H.239 Rozšíření pro podporu videokonferencí
- H.450, H.460 Doplnkové služby a rozšíření

Otázky pro test

- Kterých dvou podprotokolů H.323 se dnešní téma nejvíce týká?
- Který typ H.225 zprávy je použit při prvním volání na call server?
- Které dva porty používá H.225?
- Které doporučení je použito pro signalizaci H.225?
- Co je hlavním cílem H.245?
- Pravda nebo lež: všechny H.323 topologie využívají H.225 a H.245.
- Jaké slovo nejlépe vystihuje účel H.235?
- Která H.245 zpráva může být převedena na H.225 pole a je také používán pro výběr parametrů relace?
- Pravda nebo lež: Sada H.323 nepoužívá RTP nebo RTCP.

Otázky pro test

- Kterých dvou podprotokolů H.323 se dnešní téma nejvíce týká?
- Který typ H.225 zprávy je použit při prvním volání na call server?
- Které dva porty používá H.225?
- Které doporučení je použito pro signalizaci H.225?
- Co je hlavním cílem H.245?
- Pravda nebo lež: všechny H.323 topologie využívají H.225 a H.245.
- Jaké slovo nejlépe vystihuje účel H.235?
- Která H.245 zpráva může být převedena na H.225 pole a je také používán pro výběr parametrů relace?
- Pravda nebo lež: Sada H.323 nepoužívá RTP nebo RTCP.

Odpovědi

- Kterých dvou podprotokolů H.323 se dnešní téma týká?
- Který typ H.225 zprávy je použit při prvním volání na call server?
RAS
- Které dva porty používá H.225?
- Které doporučení je použito pro signalizaci H.225?
- Co je hlavním cílem H.245? “
- Právda nebo lež: všechny H.323 topologie využívají H.225 a H.245.
- Jaké slovo nejlépe vystihuje účel H.235?
- Která H.245 zpráva může být převedena na H.225 pole a je také používán pro výběr parametrů relace?
- Právda nebo lež: Sada H.323 nepoužívá RTP nebo RTCP.

-
- Kterých dvou podprotokolů H.323 se dnešní téma týká?
 - Který typ H.225 zprávy je použit při prvním volání na call server?
RAS
 - Které dva porty používá H.225? **1719 a 1720**
 - Které doporučení je použito pro signalizaci H.225?
 - Co je hlavním cílem H245?
 - Pravda nebo lež: všechny H.323 topologie využívají H.225 a H.245.
 - Jaké slovo nejlépe vystihuje účel H.235?
 - Která H.245 zpráva může být převedena na H.225 pole a je také používán pro výběr parametrů relace?
 - Pravda nebo lež: Sada H.323 nepoužívá RTP nebo RTCP.

-
- Kterých dvou podprotokolů H.323 se dnešní téma týká?
 - Který typ H.225 zprávy je použit při prvním volání na call server?
RAS
 - Které dva porty používá H.225? **1719 a 1720**
 - Které doporučení je použito pro signalizaci H.225? **Q.931**
 - Co je hlavním cílem H245? “
 - Pravda nebo lež: všechny H.323 topologie využívají H.225 a H.245.
 - Jaké slovo nejlépe vystihuje účel H.235?
 - Která H.245 zpráva může být převedena na H.225 pole a je také používán pro výběr parametrů relace?
 - Pravda nebo lež: Sada H.323 nepoužívá RTP nebo RTCP.

-
- Kterých dvou podprotokolů H.323 se dnešní téma týká?
 - Který typ H.225 zprávy je použit při prvním volání na call server?
RAS
 - Které dva porty používá H.225? **1719 a 1720**
 - Které doporučení je použito pro signalizaci H.225? **Q.931**
 - Co je hlavním cílem H245? “**Control protocol for multimedia communications**”
 - Pravda nebo lež: všechny H.323 topologie využívají H.225 a H.245.
 - Jaké slovo nejlépe vystihuje účel H.235?
 - Která H.245 zpráva může být převedena na H.225 pole a je také používán pro výběr parametrů relace?
 - Pravda nebo lež: Sada H.323 nepoužívá RTP nebo RTCP.

-
- Kterých dvou podprotokolů H.323 se dnešní téma týká?
 - Který typ H.225 zprávy je použit při prvním volání na call server?
RAS
 - Které dva porty používá H.225? **1719 a 1720**
 - Které doporučení je použito pro signalizaci H.225? **Q.931**
 - Co je hlavním cílem H245? “**Control protocol for multimedia communications**”
 - Pravda nebo lež: všechny H.323 topologie využívají H.225 a H.245. **F**
 - Jaké slovo nejlépe vystihuje účel H.235?
 - Která H.245 zpráva může být převedena na H.225 pole a je také používán pro výběr parametrů relace?
 - Pravda nebo lež: Sada H.323 nepoužívá RTP nebo RTCP.

-
- Kterých dvou podprotokolů H.323 se dnešní téma týká?
 - Který typ H.225 zprávy je použit při prvním volání na call server?
RAS
 - Které dva porty používá H.225? **1719 a 1720**
 - Které doporučení je použito pro signalizaci H.225? **Q.931**
 - Co je hlavním cílem H245? “**Control protocol for multimedia communications**”
 - Pravda nebo lež: všechny H.323 topologie využívají H.225 a H.245. **F**
 - Jaké slovo nejlépe vystihuje účel H.235? **Bezpečnost**
 - Která H.245 zpráva může být převedena na H.225 pole a je také používán pro výběr parametrů relace?
 - Pravda nebo lež: Sada H.323 nepoužívá RTP nebo RTCP.

-
- Kterých dvou podprotokolů H.323 se dnešní téma týká?
 - Který typ H.225 zprávy je použit při prvním volání na call server?
RAS
 - Které dva porty používá H.225? **1719 a 1720**
 - Které doporučení je použito pro signalizaci H.225? **Q.931**
 - Co je hlavním cílem H245? “**Control protocol for multimedia communications**”
 - Pravda nebo lež: všechny H.323 topologie využívají H.225 a H.245. **F**
 - Jaké slovo nejlépe vystihuje účel H.235? **Bezpečnost**
 - Která H.245 zpráva může být převedena na H.225 pole a je také používán pro výběr parametrů relace? **Open Logical Channel**
 - Pravda nebo lež: Sada H.323 nepoužívá RTP nebo RTCP.

-
- Kterých dvou podprotokolů H.323 se dnešní téma týká?
 - Který typ H.225 zprávy je použit při prvním volání na call server?
RAS
 - Které dva porty používá H.225? **1719 a 1720**
 - Které doporučení je použito pro signalizaci H.225? **Q.931**
 - Co je hlavním cílem H245? “**Control protocol for multimedia communications**”
 - Pravda nebo lež: všechny H.323 topologie využívají H.225 a H.245. **F**
 - Jaké slovo nejlépe vystihuje účel H.235? **Bezpečnost**
 - Která H.245 zpráva může být převedena na H.225 pole a je také používán pro výběr parametrů relace? **Open Logical Channel**
 - Pravda nebo lež: Sada H.323 nepoužívá RTP nebo RTCP. **F**
 - Na který protokol byste umístili signatury pro IDS?

Jakým způsobem byste u H.323
zajistili přenos tónů DTMF?

Přenos tónů DTMF u H.323

- v rámci paketů RTP (ale kódovány jinak, než datové vzorky)
- ve zprávách H.245 UII (User Input Identification) – tzv. alfanumerické metoda H.245
- ve zprávách H.245 se předávají údaje o délce tónu – metoda H.245 signal

Rozeberte posloupnost zachycených zpráv

| | | | | |
|----|----------------|----------------|---------|---|
| 10 | 10.210.200.112 | 10.210.200.111 | H.225.0 | CS: setup |
| 12 | 10.210.200.111 | 10.210.200.112 | H.225.0 | CS: alerting |
| 18 | 10.210.200.111 | 10.210.200.112 | H.225.0 | CS: connect |
| 25 | 10.210.200.112 | 10.210.200.111 | H.245 | terminalCapabilitySet |
| 27 | 10.210.200.112 | 10.210.200.111 | H.245 | masterSlaveDetermination |
| 31 | 10.210.200.111 | 10.210.200.112 | H.245 | terminalCapabilitySet |
| 33 | 10.210.200.111 | 10.210.200.112 | H.245 | masterSlaveDetermination |
| 38 | 10.210.200.112 | 10.210.200.111 | H.245 | terminalCapabilitySetAck |
| 39 | 10.210.200.112 | 10.210.200.111 | H.245 | masterSlaveDeterminationAck |
| 41 | 10.210.200.111 | 10.210.200.112 | H.245 | terminalCapabilitySetAck |
| 42 | 10.210.200.111 | 10.210.200.112 | H.245 | masterSlaveDeterminationAck |
| 44 | 10.210.200.112 | 10.210.200.111 | H.245 | openLogicalChannel (generic) |
| 46 | 10.210.200.112 | 10.210.200.111 | H.245 | openLogicalChannel (genericVideoCapability) |

Co je to dhkey a halfkey?

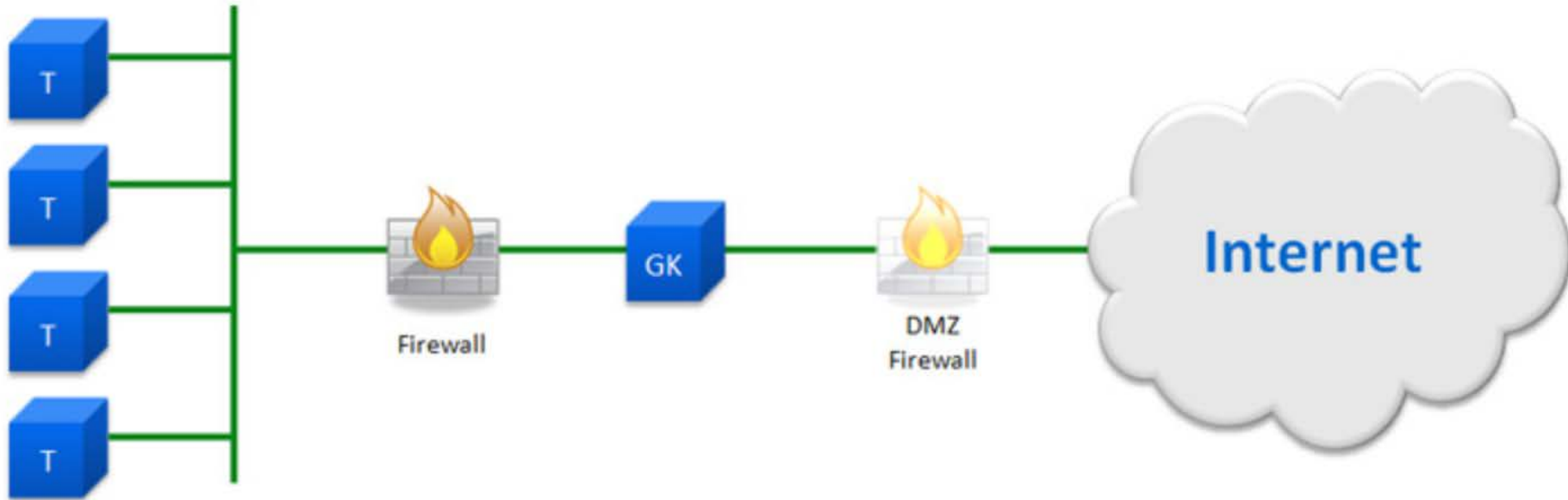
- ▣ tokens: 1 item
 - ▣ Item 0
 - ▣ ClearToken
 - tokenOID: 2.16.840.1.114187.1.6.2 (joint-iso-itu-t.16.840.1.114187.1.6.2)
 - ▣ dhkey
 - halfkey: c534645ef94ada22a0bcc44ae91e0c3a0d1e2ca84a7c5540... [bit length 1024]
 - ▣ profileInfo: 2 items
 - ▣ Item 0
 - ▣ ProfileElement
 - elementID: 2
 - ▣ element: octets (0)
 - octets: 0000489c
 - ▣ Item 1
 - ▣ ProfileElement
 - elementID: 1
 - ▣ element: octets (0)
 - octets: 6c89000010d2000008480000
 - ▣ authenticationCapability: 2 items
 - ▣ Item 0
 - ▣ AuthenticationMechanism: pwdSymEnc (1)
 - pwdSymEnc: NULL
 - ▣ Item 1
 - ▣ AuthenticationMechanism: keyExch (8)
 - keyExch: 2.16.840.1.114187.1.6.2 (joint-iso-itu-t.16.840.1.114187.1.6.2)
 - ▣ algorithmOIDs: 2 items
 - ▣ Item 0
 - algorithmOIDs item: 1.3.14.3.2.6 (desECB)
 - ▣ Item 1
 - algorithmOIDs item: 2.16.840.1.114187.1.3 (joint-iso-itu-t.16.840.1.114187.1.3)
 - ▣ featureSet

Analyzujte výpis

Filter: bootp || tftp.opcode==1 || h225 && eth.addr ==00:09:6e:05:cb:11 Expression... Clear Apply

| No. | Source | Destination | Protocol | Info |
|-----|---------------|-----------------|----------|--|
| 28 | 0.0.0.0 | 255.255.255.255 | DHCP | DHCP Discover - Transaction ID 0xc6e03148 |
| 33 | 0.0.0.0 | 255.255.255.255 | DHCP | DHCP Request - Transaction ID 0xc6e03148 |
| 46 | 192.168.16.23 | 192.168.16.99 | TFTP | Read Request, File: 46xxupgrade.scr, Trans |
| 76 | 192.168.16.23 | 192.168.16.99 | TFTP | Read Request, File: 46xxsettings.txt, Tran |
| 568 | 192.168.16.23 | 192.168.16.1 | H.225.0 | RAS: gatekeeperRequest |
| 569 | 192.168.16.1 | 192.168.16.23 | H.225.0 | RAS: gatekeeperConfirm |
| 570 | 192.168.16.23 | 192.168.16.1 | H.225.0 | RAS: registrationRequest |
| 571 | 192.168.16.1 | 192.168.16.23 | H.225.0 | RAS: registrationConfirm |
| 576 | 192.168.16.23 | 192.168.16.1 | H.225.0 | CS: setup OpenLogicalChannel |
| 578 | 192.168.16.1 | 192.168.16.23 | H.225.0 | CS: callProceeding |
| 579 | 192.168.16.1 | 192.168.16.23 | H.225.0 | CS: connect OpenLogicalChannel |

Kam s ním? Jaké jsou možnosti?



Co to je?

```
1.      30 23                ; SEQUENCE (23 Bytes)
2.      | | 31 0f                ; SET (f Bytes)
3.      | | | 30 0d                ; SEQUENCE (d Bytes)
4.      | | | 06 03                ; OBJECT_ID (3 Bytes)
5.      | | | | 55 04 03
6.      | | | |                ; 2.5.4.3 Common Name (CN)
7.      | | | 13 06                ; PRINTABLE_STRING (6 Bytes)
8.      | | | 54 65 73 74 43 4e                ; TestCN
9.      | | |                ; "TestCN"
10.     | | 31 10                ; SET (10 Bytes)
11.     | | 30 0e                ; SEQUENCE (e Bytes)
12.     | | 06 03                ; OBJECT_ID (3 Bytes)
13.     | | | 55 04 0a
14.     | | |                ; 2.5.4.10 Organization (0)
15.     | | 13 07                ; PRINTABLE_STRING (7 Bytes)
16.     | | 54 65 73 74 4f 72 67                ; TestOrg
17.     | |                ; "TestOrg"
```