

1. Servizi Multimediali e  
Qualità del Servizio (QoS) su IP  
1.7 Architettura H.323

Prof. Raffaele Bolla



## H.323

- Definito dall'ITU-T.
- Rappresenta una sorta di “ombrello” sotto il quale sono raccolti una serie di standard relativi a servizi di conferenza multimediale (H.225.0, H.245, ecc.) su reti a pacchetto
  - IP, ATM, ...
  - sono ottimizzati per l'architettura TCP/IP.
- Il target sono i servizi interattivi in tempo reale.

## H.323

---

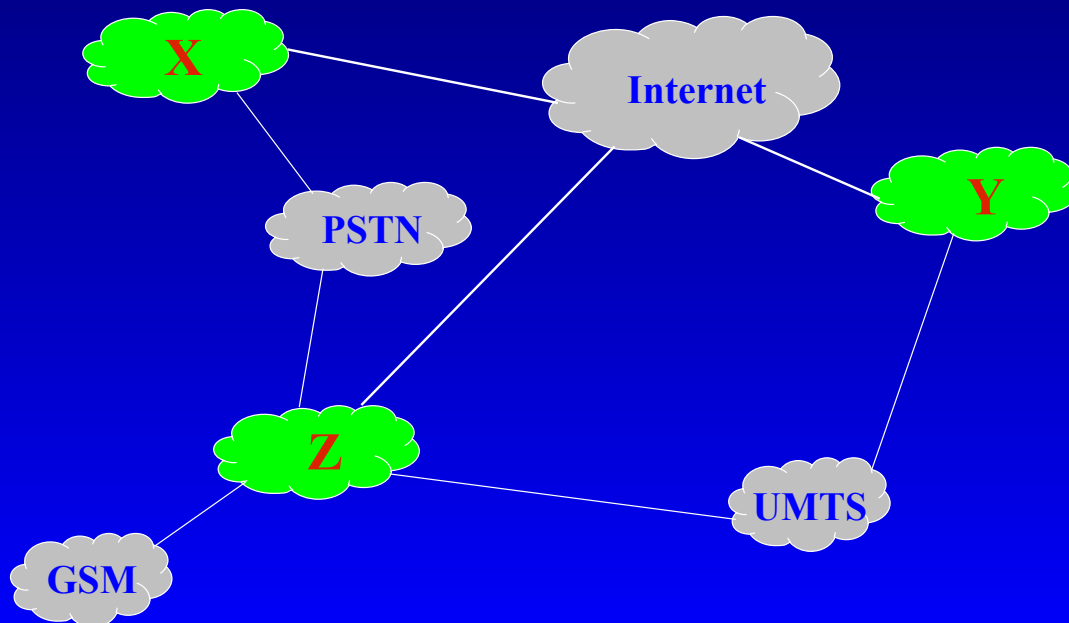
- Le specifiche includono:
  - Come i nodi terminali fanno e ricevono le chiamate.
  - Come negoziano le codifiche.
  - Come i flussi vengono incapsulati.
  - Come avviene la sincronizzazione.
  - Come i terminali colloquiano con elementi di coordinamento (*Gatekeeper*).
  - Come i terminali possono interagire con la rete telefonica tradizionale.

## H.323 - Architettura

---

- La rete H.323 è composta da diversi *domini amministrativi*
  - un dominio amministrativo è un insieme di entità funzionali H.323 poste sotto il controllo di una unica autorità amministrativa;
  - la struttura interna di ogni dominio amministrativo non deve essere nota agli altri;
  - i domini amministrativi interagiscono con le reti telefoniche classiche e tra di loro attraverso la rete IP.

## H.323 - Architettura



Lezione 1.7, v. 1.0

6.5

## H.323 - Architettura

- Internet e la rete PSTN presentano diverse filosofie architettureali
  - in Internet l'intelligenza risiede nei sistemi terminali
    - » la rete agisce puramente come sistema di trasporto,
    - » l'intelligenza della rete è limitata alla gestione dell'instradamento;
  - nella rete PSTN, al contrario, l'intelligenza risiede all'interno della rete stessa
    - » i sistemi terminali si limitano essenzialmente a fornire "stimoli" alla rete (sgancio ricevitore, riaggancio, numerazione).

Lezione 1.7, v. 1.0

6.6

## H.323 - Architettura

---

- H.323 permette entrambi i modelli
  - l'inclinazione è comunque verso l'approccio telefonico classico.
  - ad es. alcuni servizi possono essere realizzati in modalità
    - » distribuita, se i sistemi terminali interagiscono direttamente tra di loro,
    - » centralizzata, se l'esecuzione viene coordinata da un server e i terminali si limitano a fornire stimoli.

## H.323 - Servizi

---

- Servizi di base
  - comunicazioni multimediali (voce, video, dati, fax).
- Servizi supplementari
  - inoltro di chiamata;
  - trasferimento di chiamata;
  - trattenimento di chiamata;
  - gestione di chiamate multiple.
- Servizi telefonici tradizionali
  - appoggiandosi ad un PBX.

## H.323 - Elementi

---

- **Endpoint**, terminano la segnalazione ed il media:
  - **terminali**: terminano la segnalazione ed il flusso di dati all'utente
    - » telefoni, videotelefoni, *soft phone*, PC multimediali, telefoni GSM, ecc.;
  - **MCUs (Multipoint Control Units)**: gestiscono conferenze tra 3 o più terminali mescolando i diversi flussi in arrivo
    - » l'MCU contiene un *Multipoint Controller* (MC) che gestisce la segnalazione e opzionalmente uno o più *Multipoint Processor* (MP) per gestire il media (mixing, switching, ecc)
      - spesso selezionano la sorgente con maggiore energia.

## H.323 - Elementi

---

- **gateway**: interconnettono la rete a pacchetto H.323 con le reti a commutazione di circuito e convertono i formati della segnalazione e del flusso dei media
  - » H.225.0/H.245 - SS7 Inband per PSTN o ISUP per ISDN,
  - » RTP - PCM per PSTN.
  - » sono composti da una parte di controllo (MGC, *Media Gateway Controller*) e una parte di gestione dei media (MG, *Media Gateway*);
  - » PSTN/voice gateway, PSTN/fax gateway, PSTN/H.324 gateway, GSM gateway, PBX gateway.

## H.323 - Elementi

---

- *Gatekeeper*

- è un elemento opzionale del sistema;
- fornisce servizi agli *endpoint* ed instrada le chiamate H.323
  - » risoluzione degli indirizzi (come un DNS, ossia tradurre il nome di una persona (numero E.164) nel corrispondente indirizzo IP)
  - » *Authentication, Authorization and Accounting (AAA)*;
  - » gestione della banda (attraverso un controllo d'accesso);
- tipicamente si appoggia ad appositi server per fornire i diversi servizi

Lezione 1.7, v. 1.0 » agisce come un *proxy*;

6.11

## H.323 - Elementi

---

- esiste un unico *gatekeeper* per ogni "zona":
  - » quando attivata, una applicazione H.323 si deve registrare presso il *gatekeeper* (se esiste), usando il RAS,
  - » nel momento in cui deve fare una chiamata l'applicazione chiede il permesso al *gatekeeper*,
  - » se gli viene accordato il permesso invia un indirizzo email, un nome, un numero telefonico e il *gatekeeper* lo traduce (interagendo eventualmente con altri *gatekeeper*) in un indirizzo IP e lo rimanda all'applicazione.
- *Feature server*: fornisce servizi supplementari (per es. le chiamate in attesa)
  - gli *endpoint* possono comunicare direttamente o tramite il *gatekeeper*.

Lezione 1.7, v. 1.0

6.12

## H.323 - Elementi

---

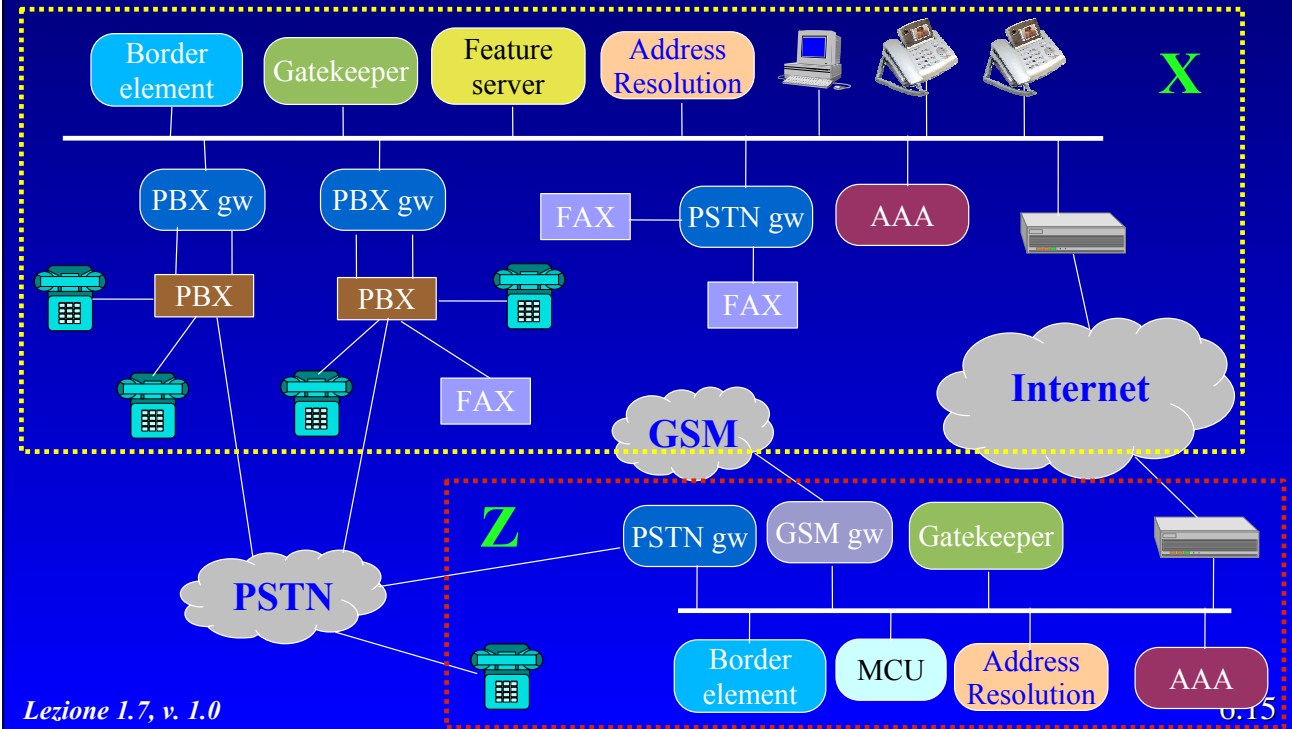
- *Border element*: fornisce un accesso pubblico al dominio per effettuare la risoluzione degli indirizzi, il controllo d'accesso e un resoconto dell'utilizzo delle risorse
  - può aggregare informazioni sugli indirizzi, in modo da limitare il traffico nella rete.

## H.323 - Elementi

---

- Gli elementi identificati da H.323 sono funzionalità logiche
  - esse possono essere raggruppate all'interno di singole entità fisiche
    - » varie combinazioni sono possibili
  - per esempio si possono combinare in un unico apparato
    - » il gatekeeper ed il border element,
    - » il gatekeeper , un gateway ed il border element.

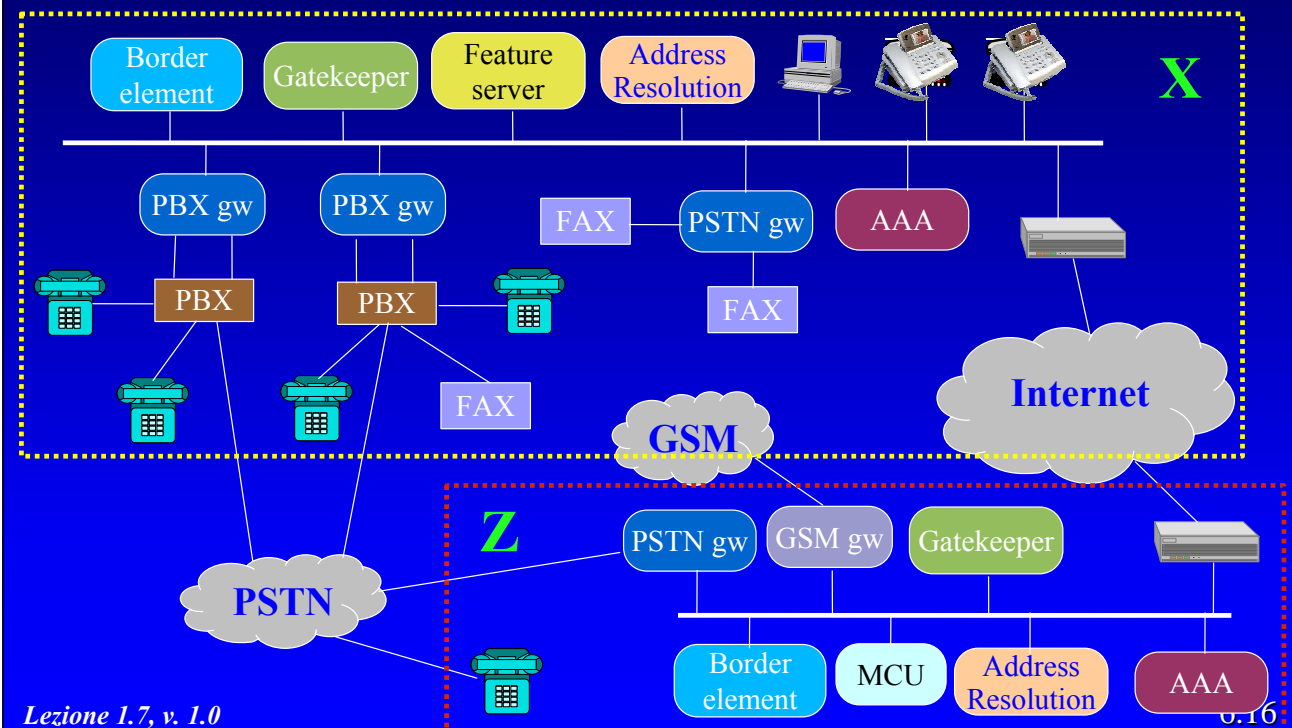
# H.323 - Elementi



Lezione 1.7, v. 1.0

6.15

# H.323 Chiamata Intradominio



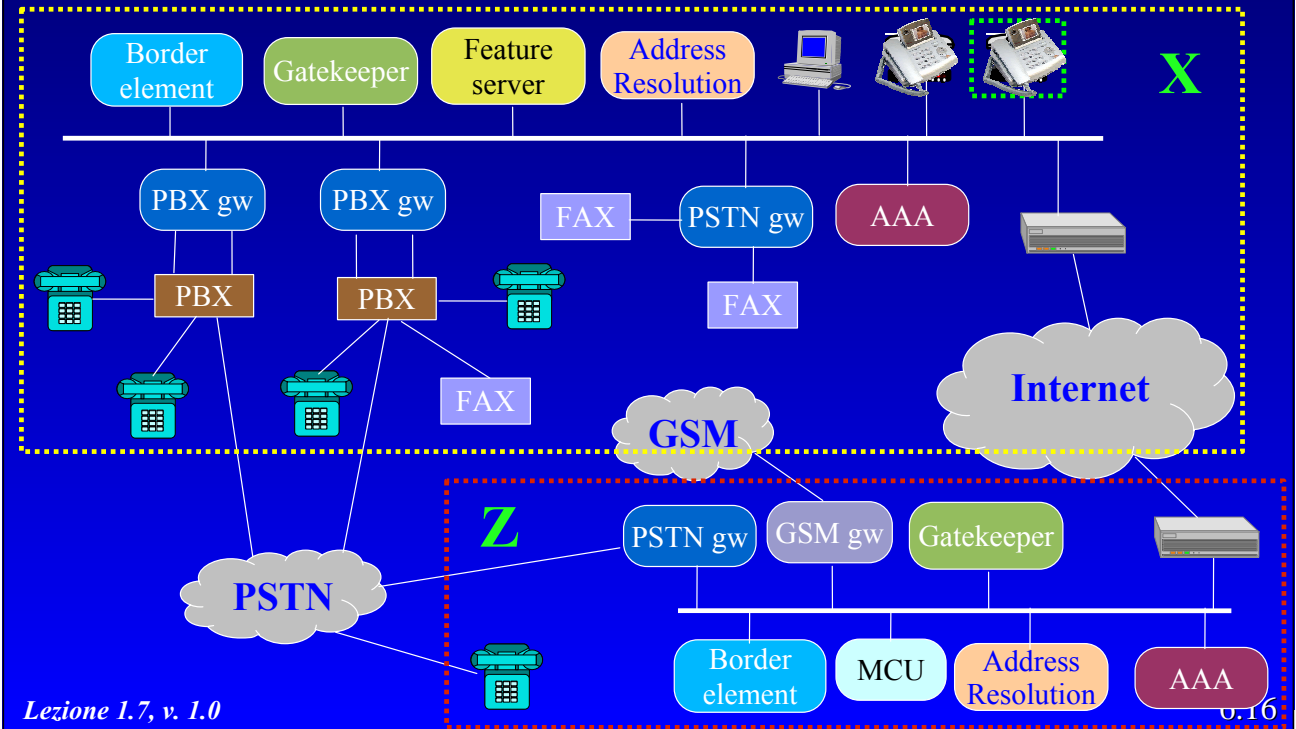
Lezione 1.7, v. 1.0

6.16



### H.323

## Chiamata Intradominio

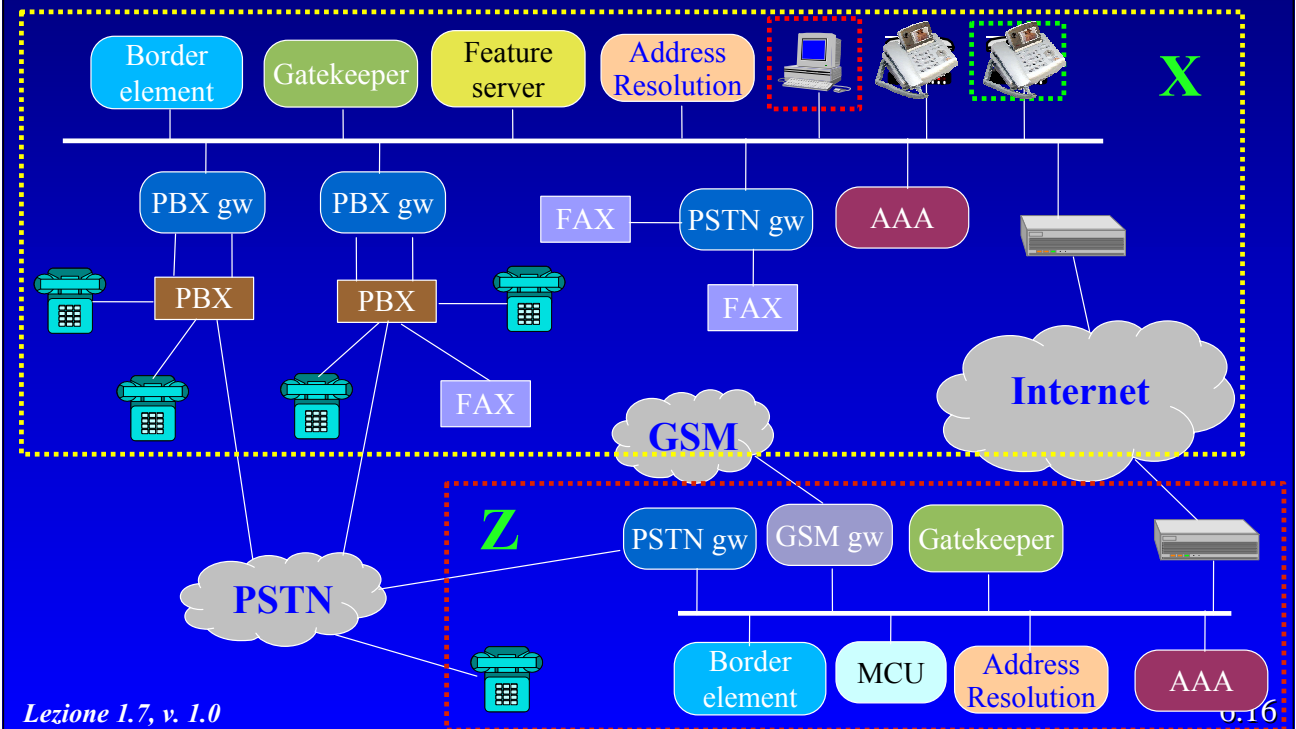


Lezione 1.7, v. 1.0

6.16

### H.323

## Chiamata Intradominio

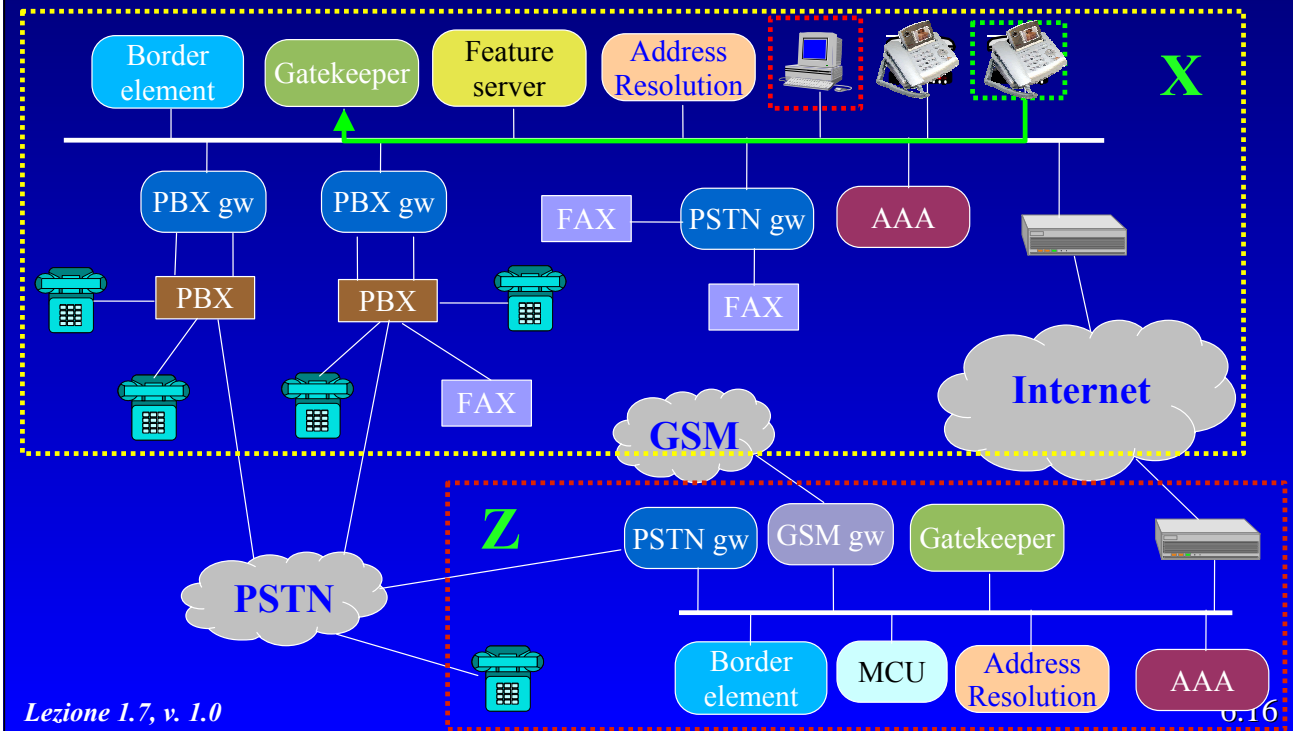


Lezione 1.7, v. 1.0

6.16

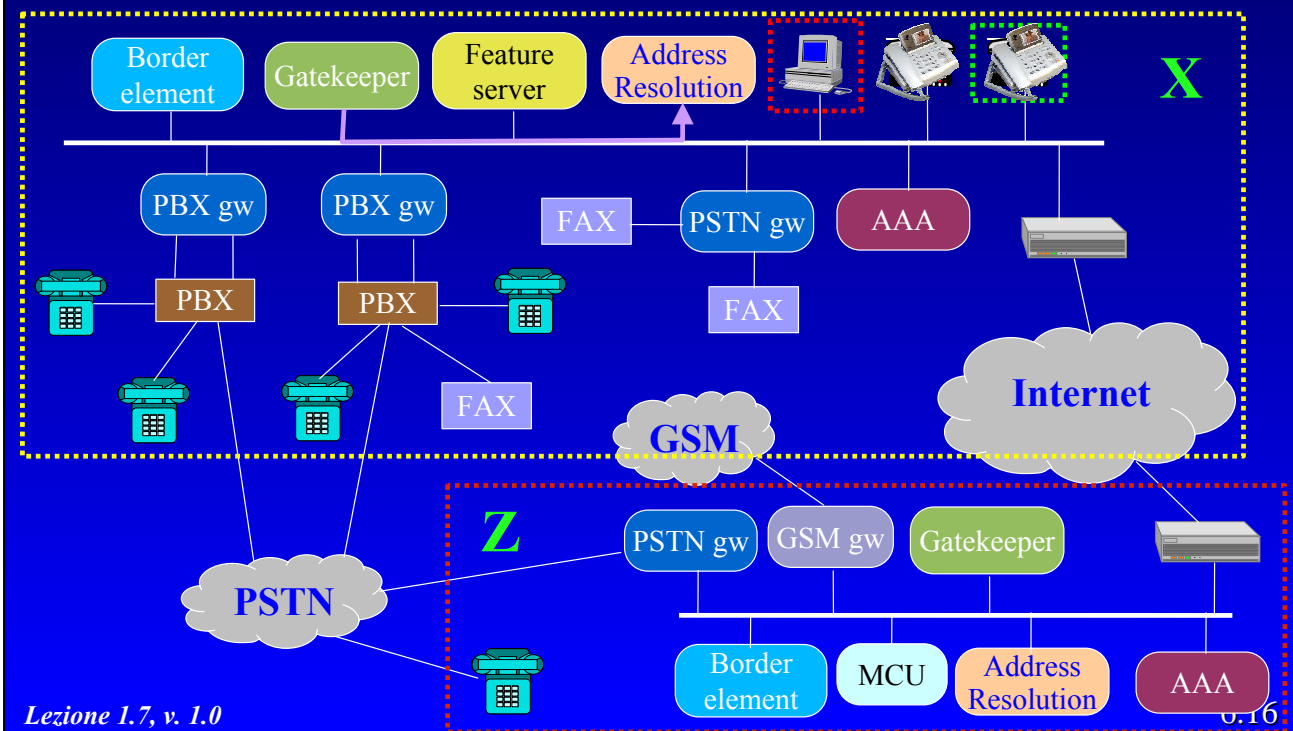
### H.323

## Chiamata Intradominio



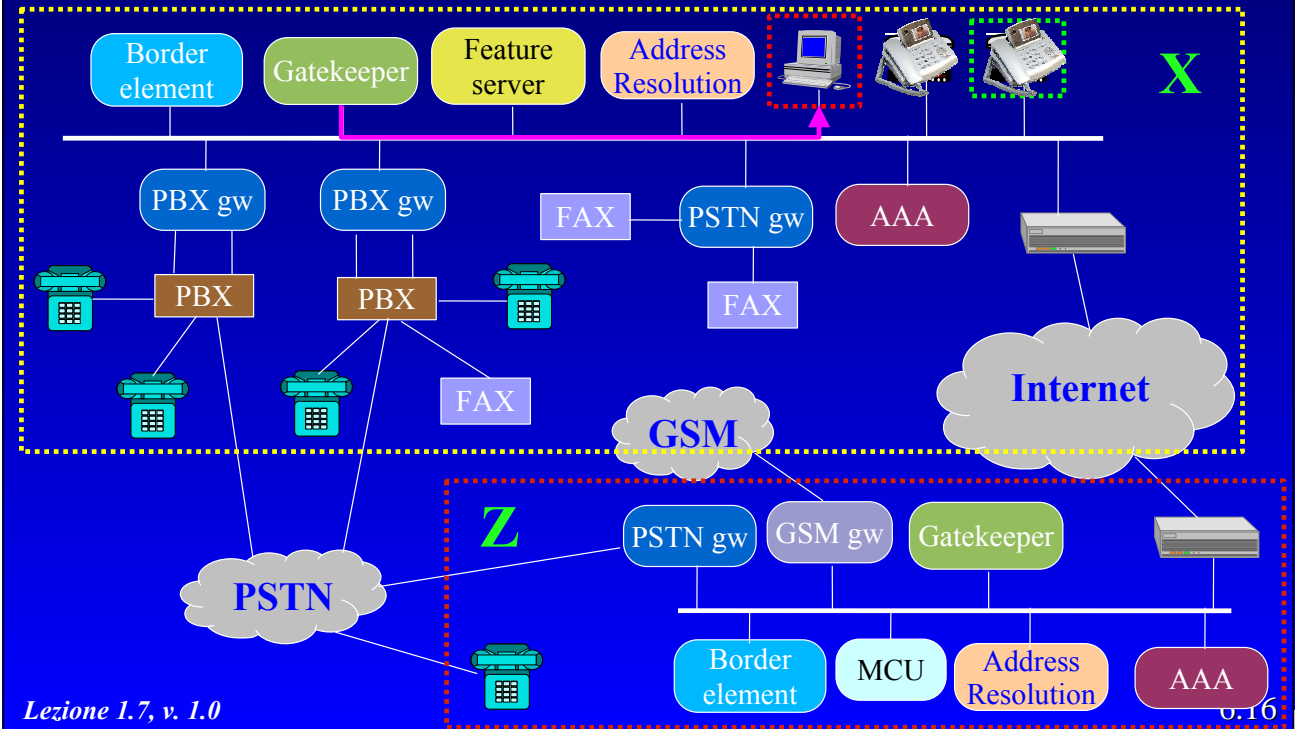
### H.323

## Chiamata Intradominio



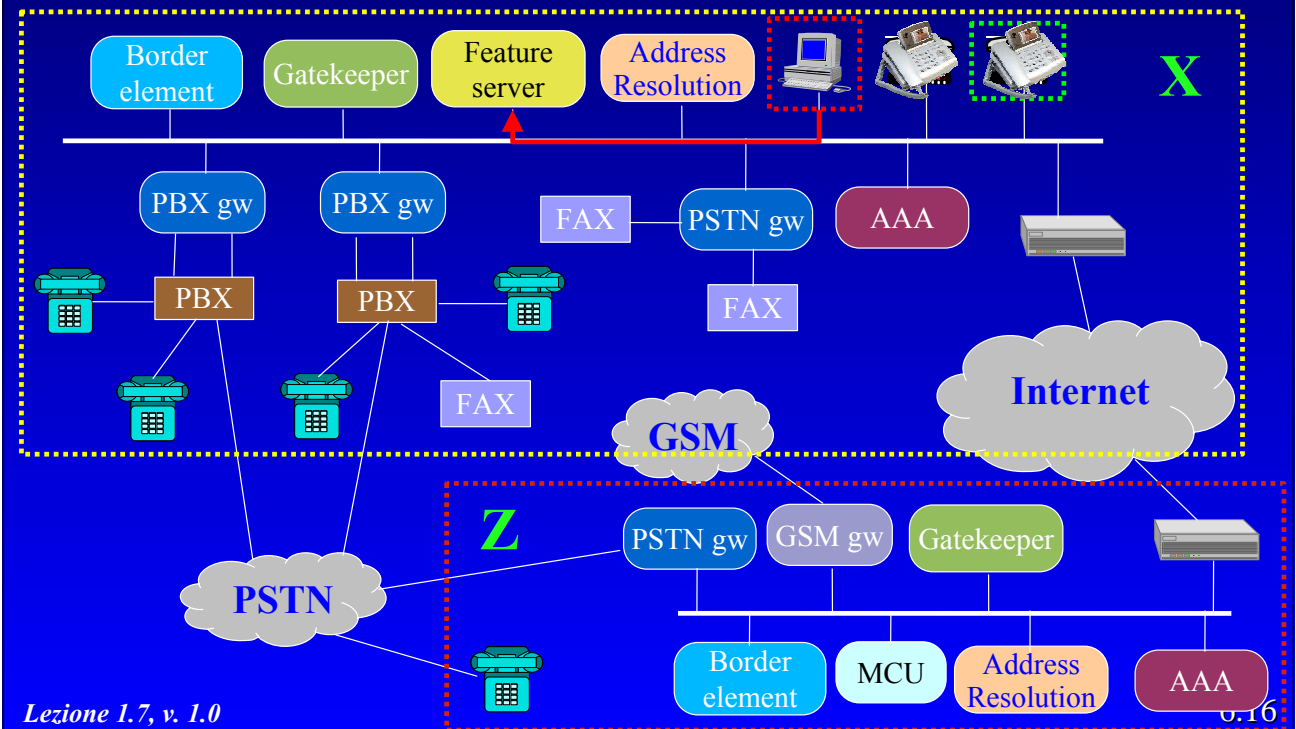
### H.323

## Chiamata Intradominio



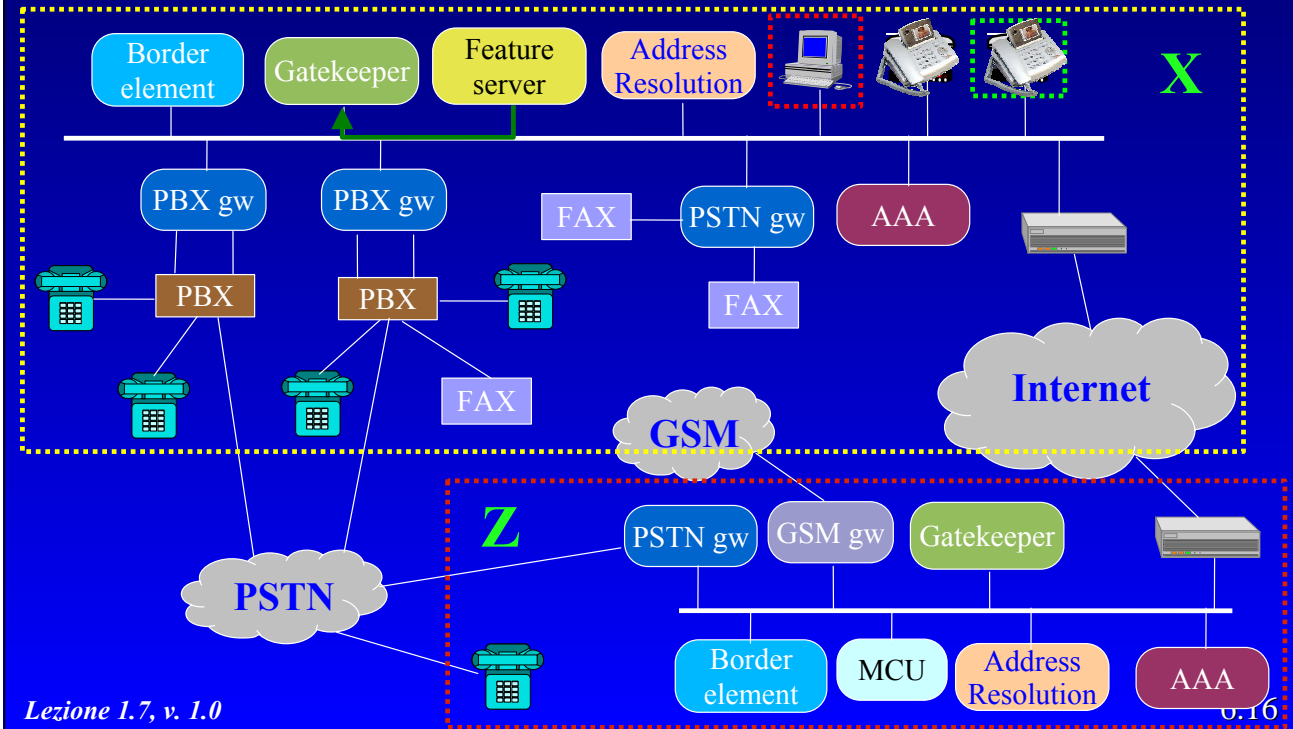
### H.323

## Chiamata Intradominio



### H.323

## Chiamata Intradominio

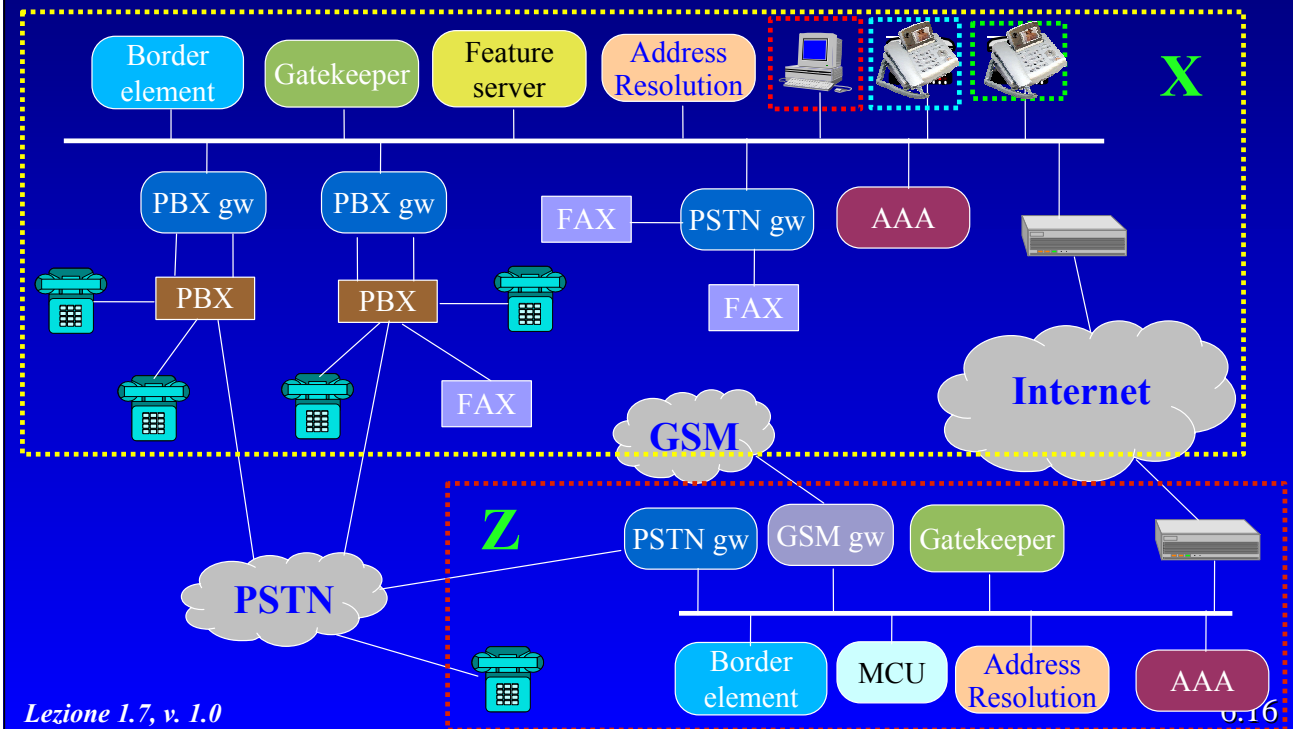


Lezione 1.7, v. 1.0

6.16

### H.323

## Chiamata Intradominio

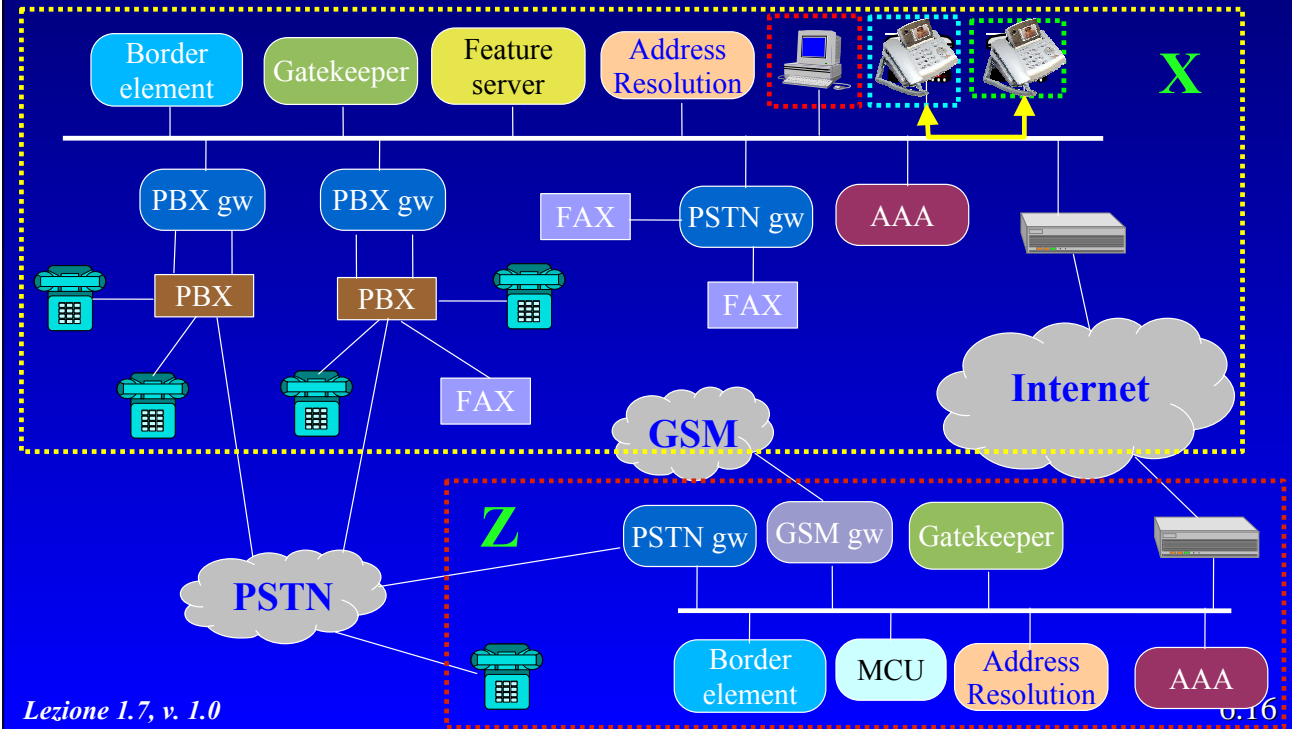


Lezione 1.7, v. 1.0

6.16

### H.323

## Chiamata Intradominio

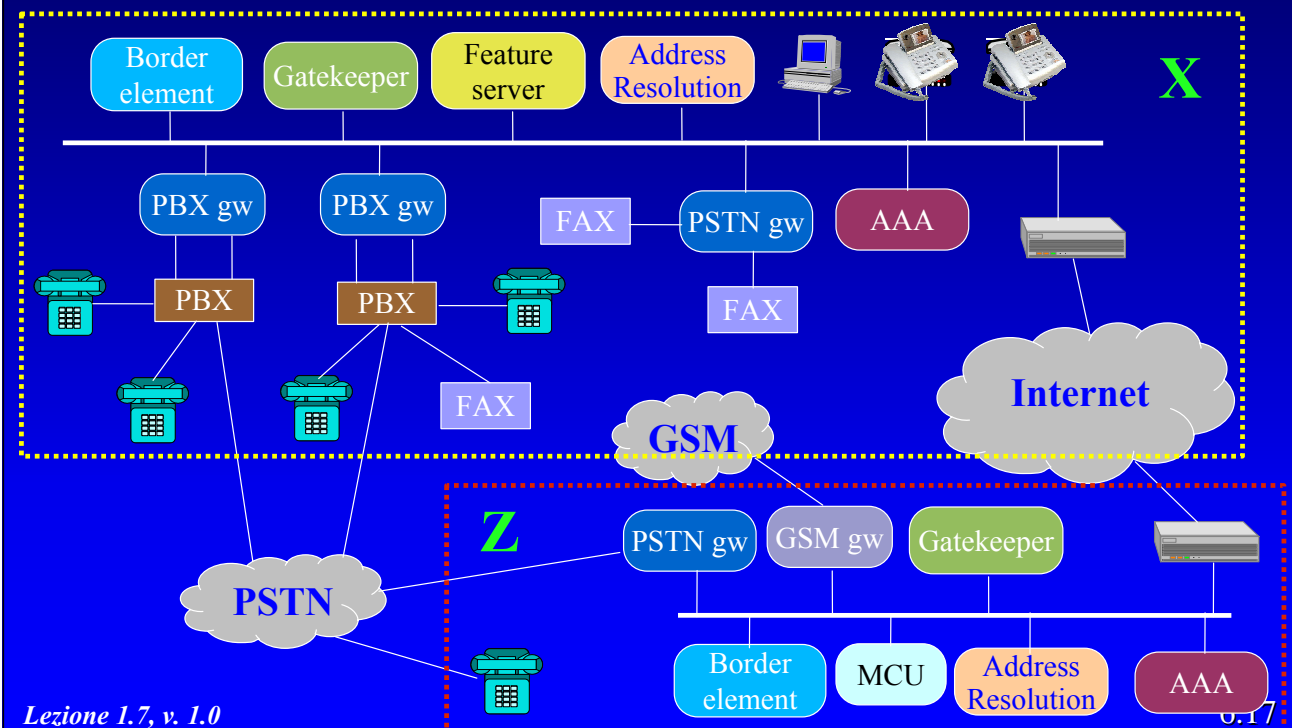


Lezione 1.7, v. 1.0

6.16

### H.323

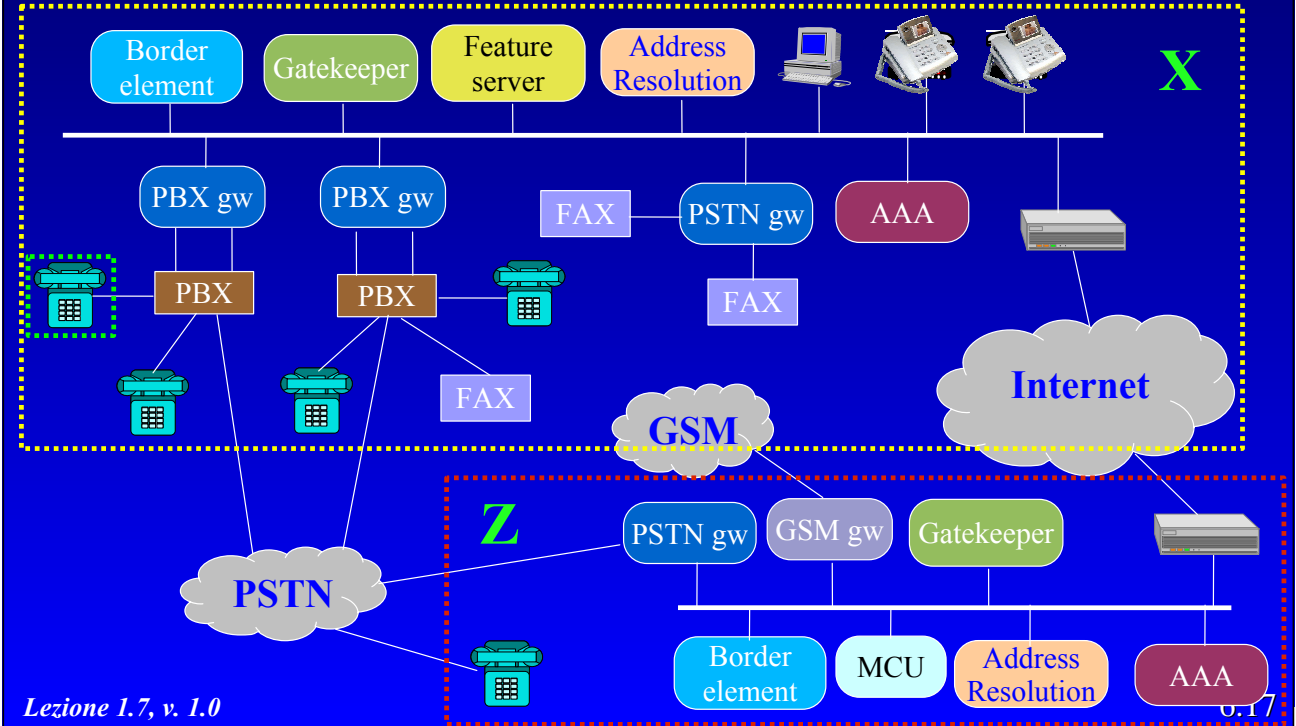
## Trunking



Lezione 1.7, v. 1.0

6.17

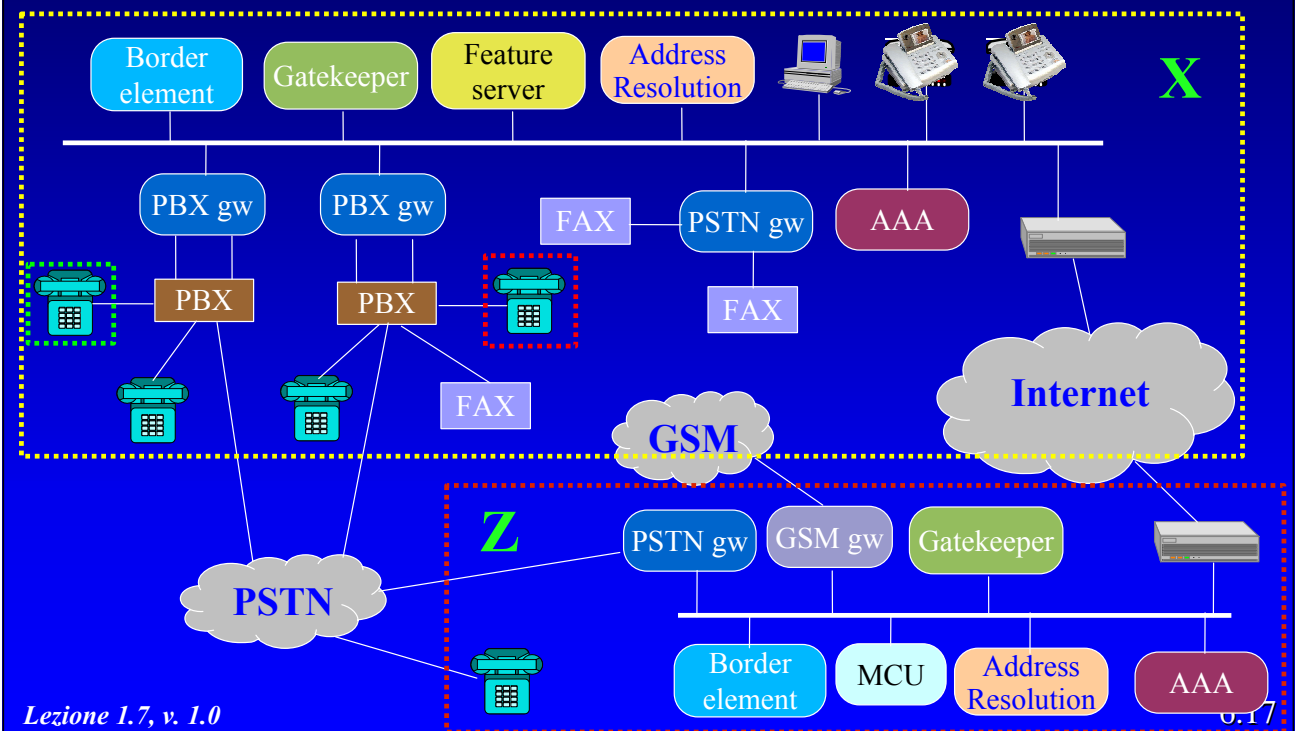
# H.323 Trunking



Lezione 1.7, v. 1.0

6.17

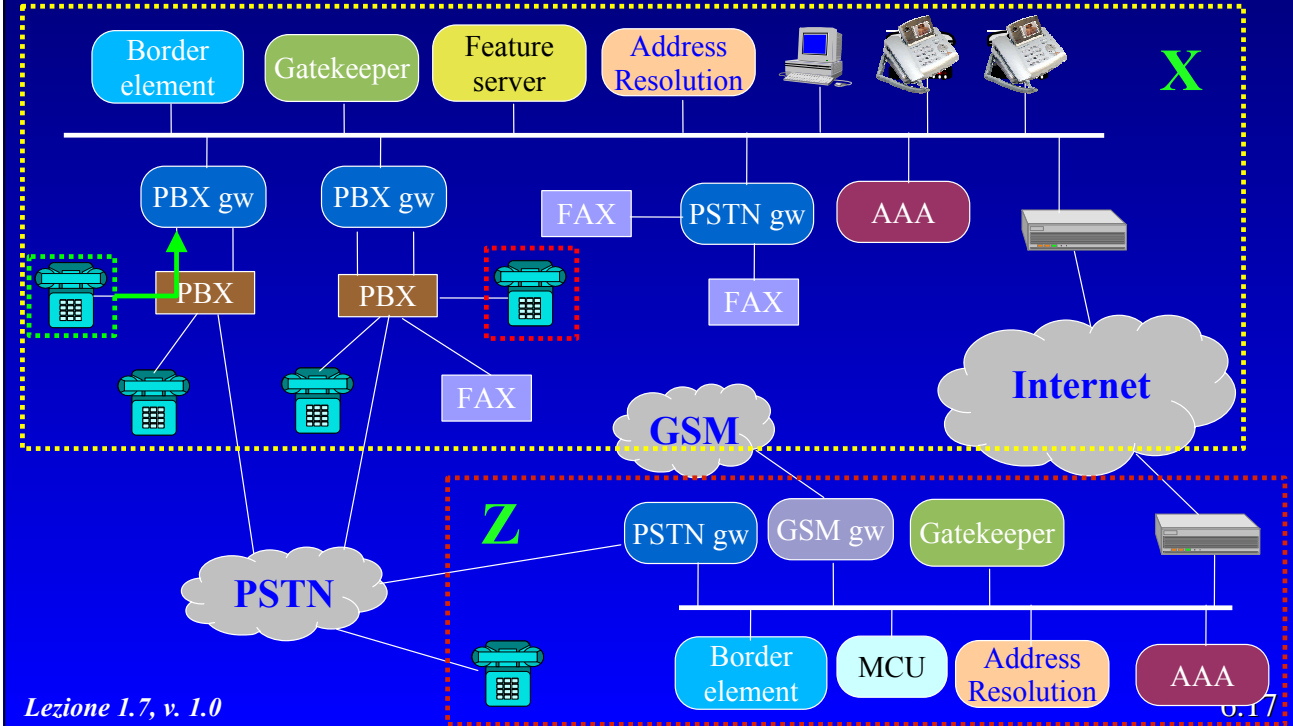
# H.323 Trunking



Lezione 1.7, v. 1.0

6.17

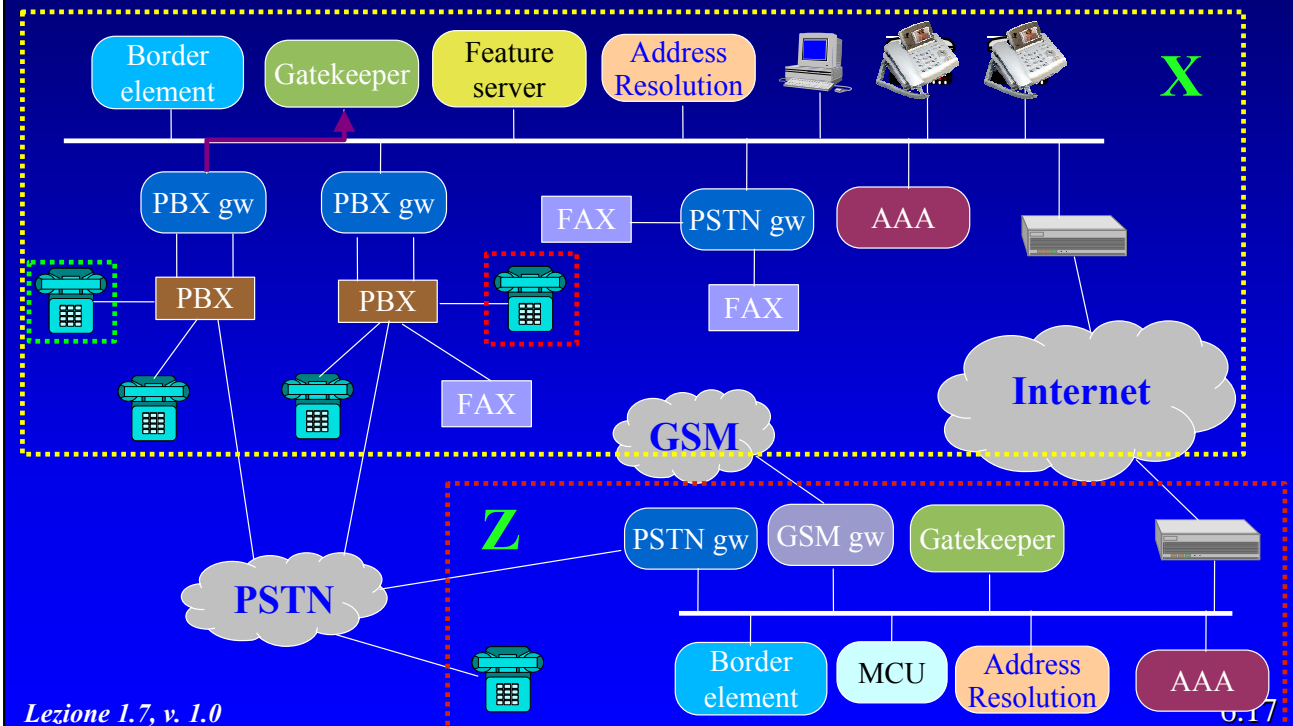
# H.323 Trunking



Lezione 1.7, v. 1.0

6.17

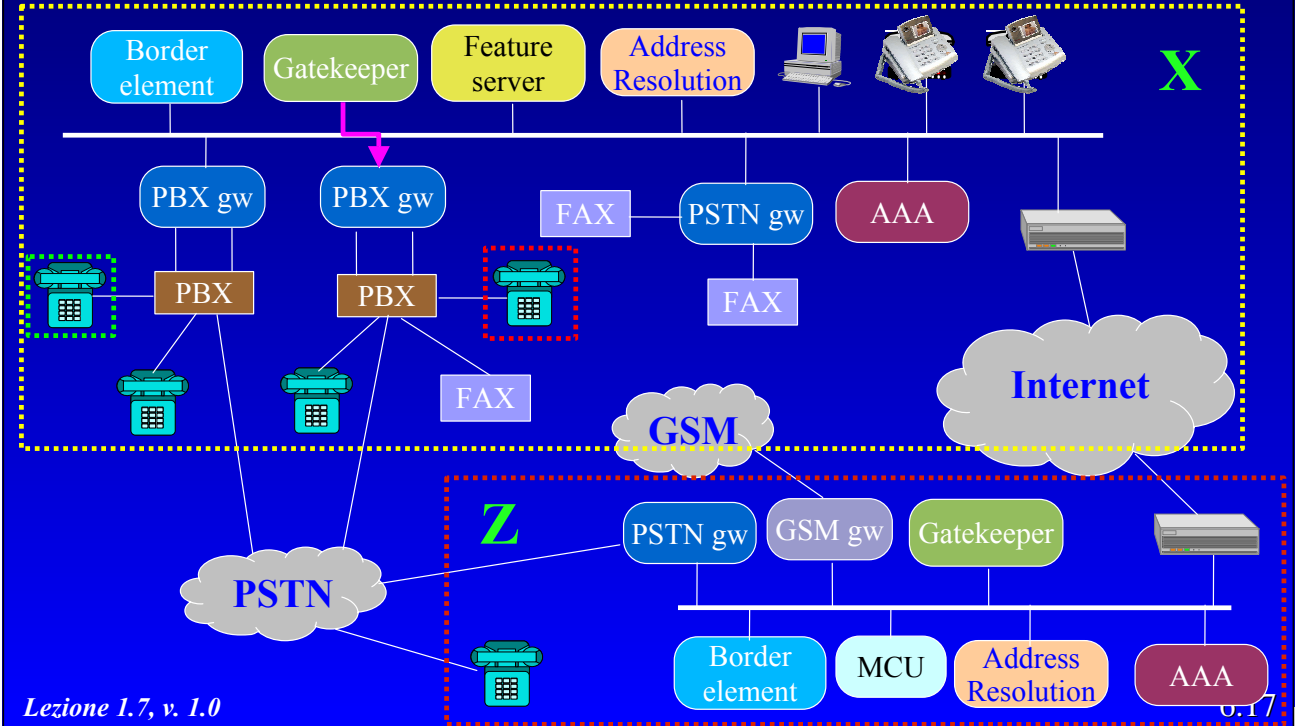
# H.323 Trunking



Lezione 1.7, v. 1.0

6.17

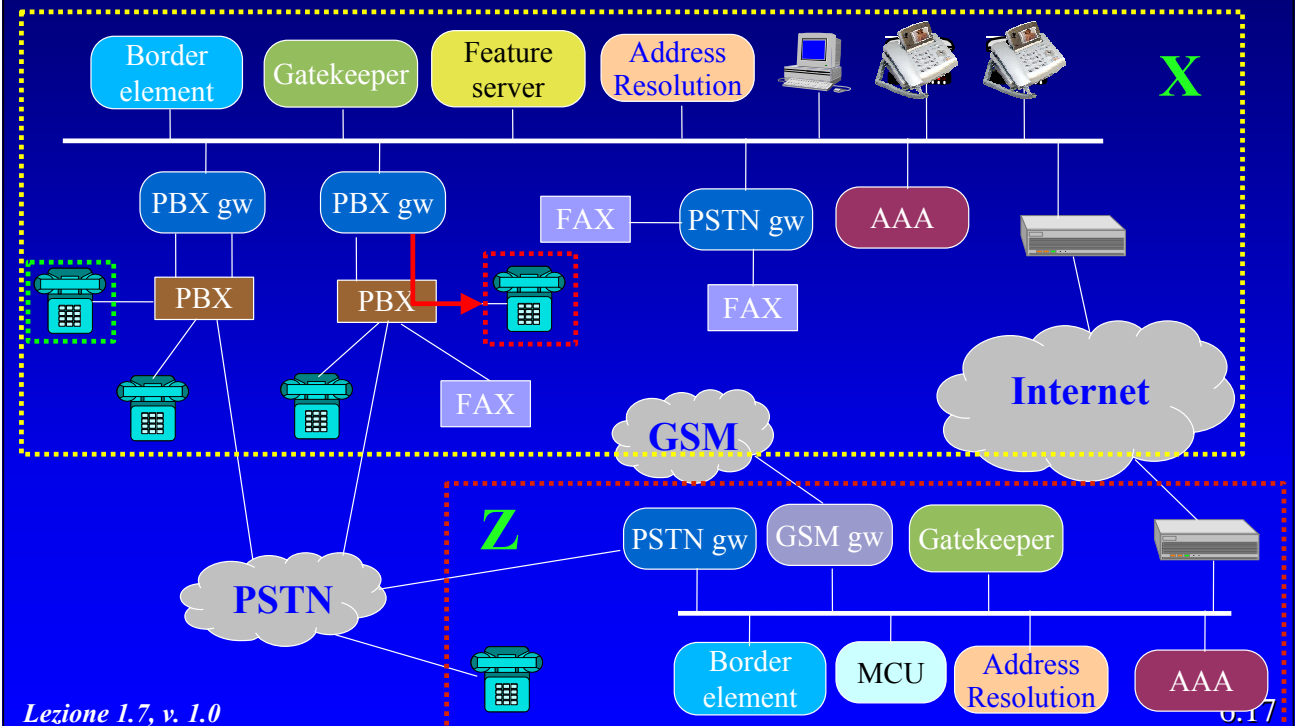
# H.323 Trunking



Lezione 1.7, v. 1.0

6.17

# H.323 Trunking

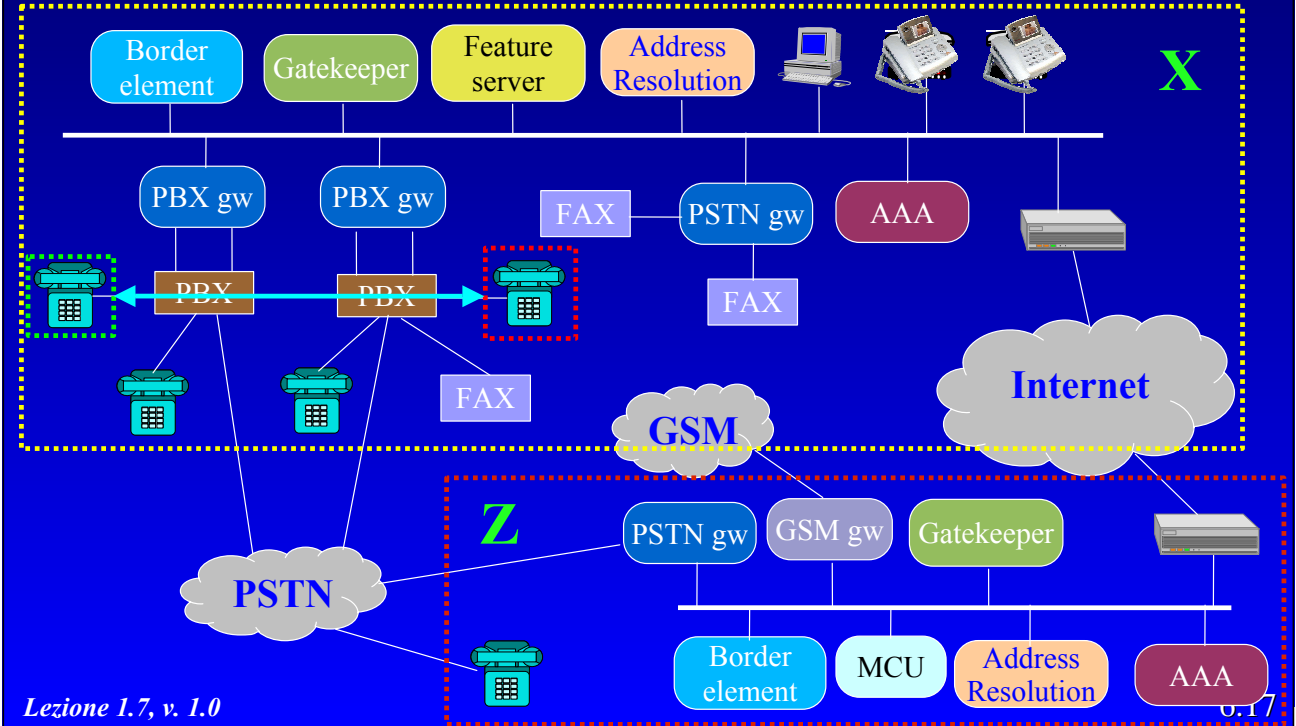


Lezione 1.7, v. 1.0

6.17



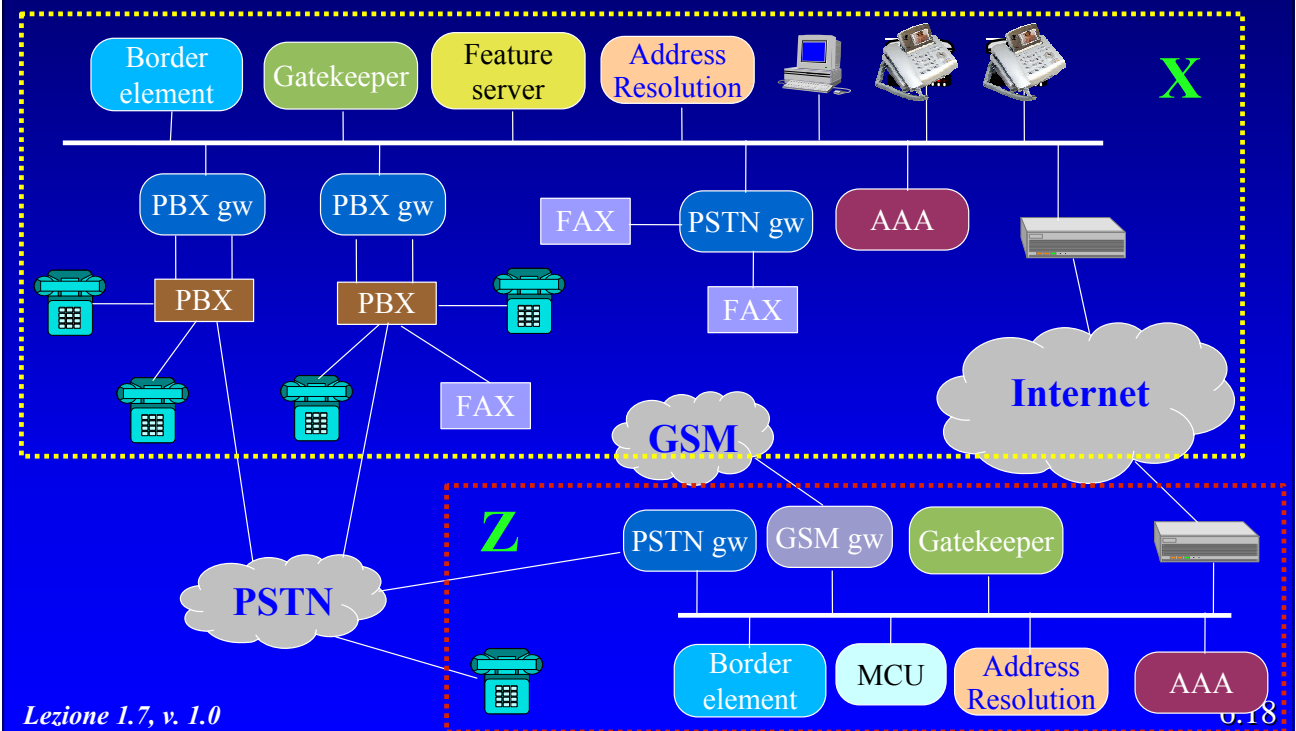
# H.323 Trunking



Lezione 1.7, v. 1.0

6.17

# H.323 Chiamata Interdominio

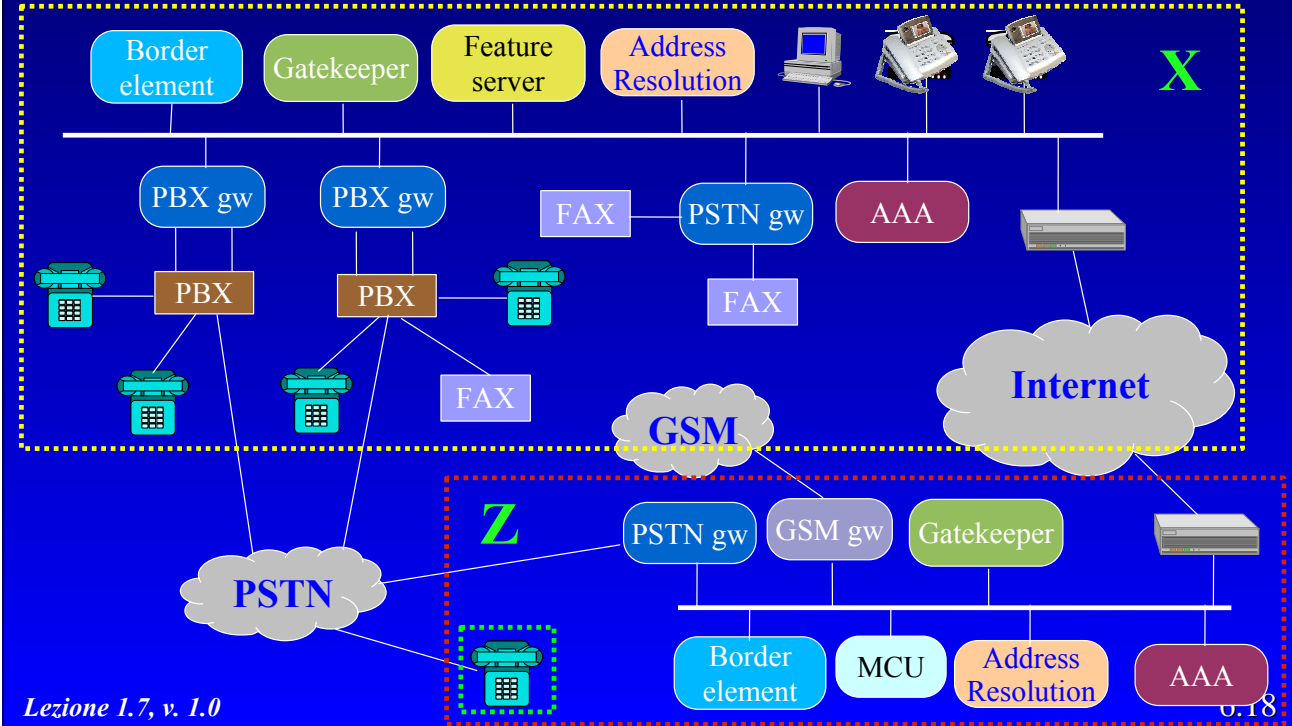


Lezione 1.7, v. 1.0

6.18

### H.323

## Chiamata Interdominio

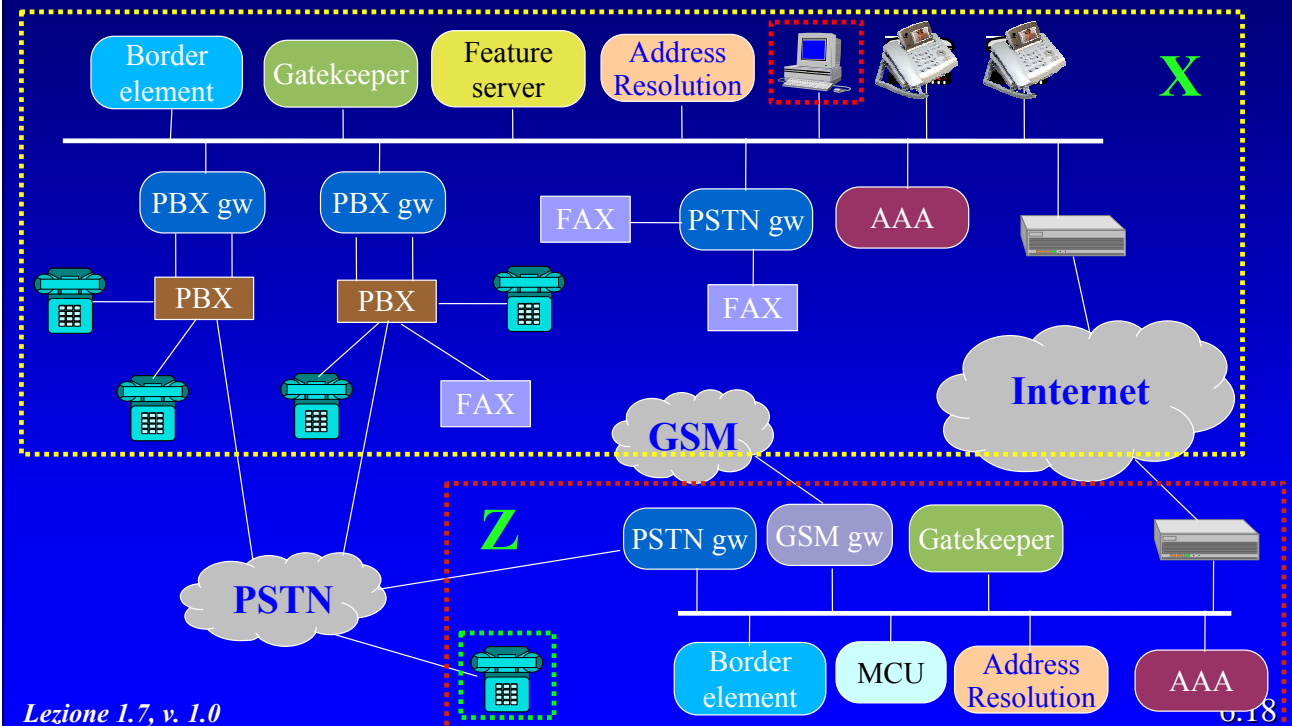


Lezione 1.7, v. 1.0

6.18

### H.323

## Chiamata Interdominio

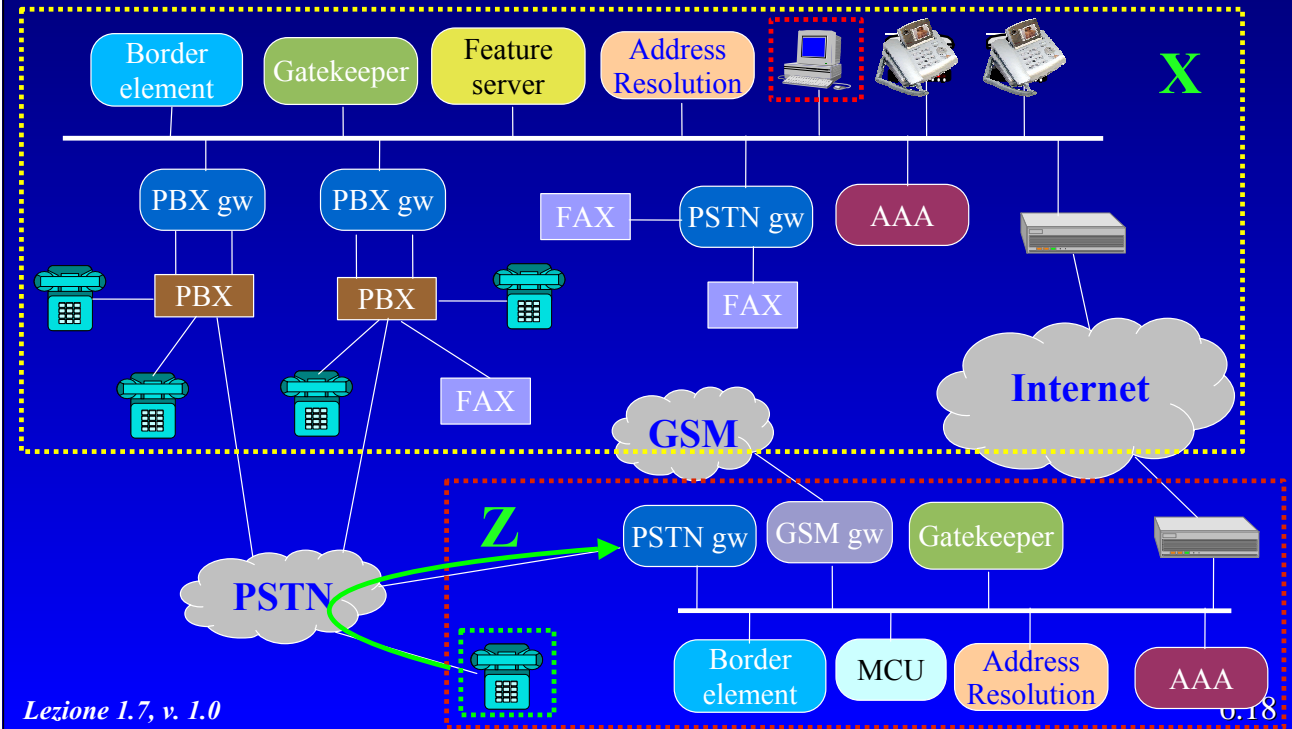


Lezione 1.7, v. 1.0

6.18

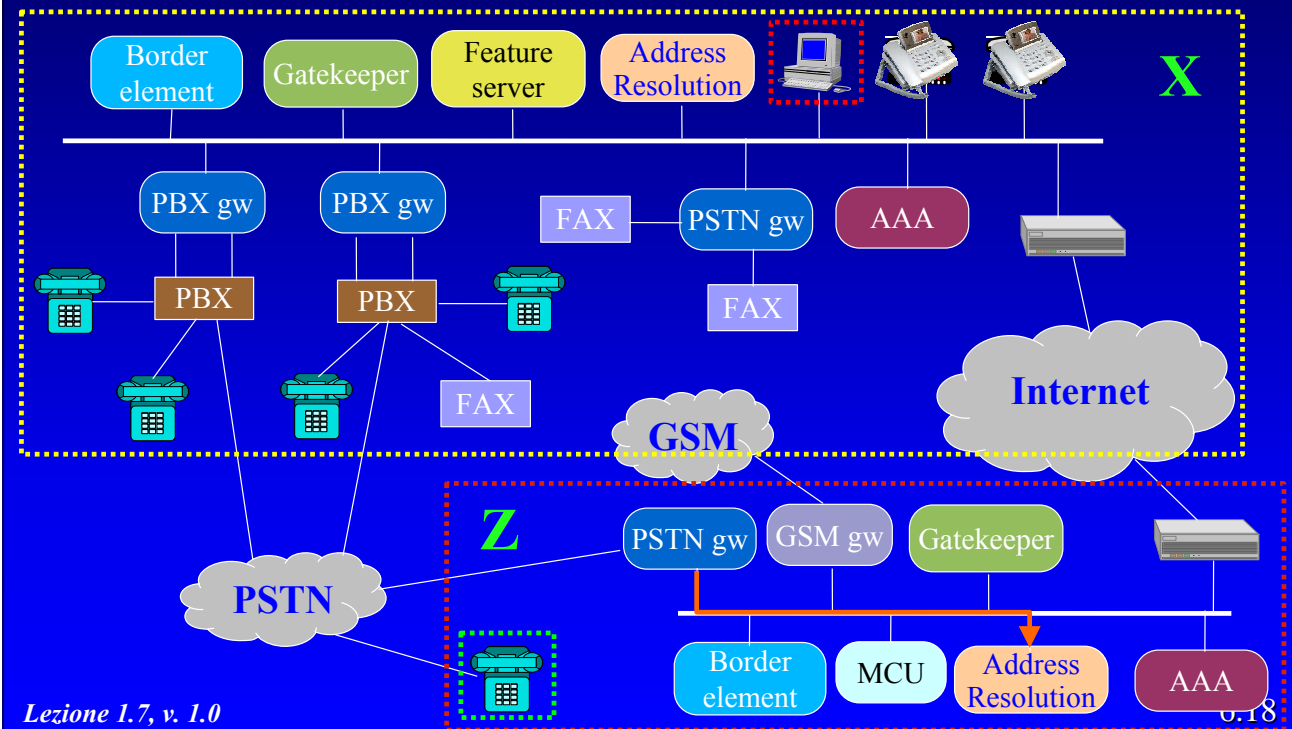
### H.323

## Chiamata Interdominio



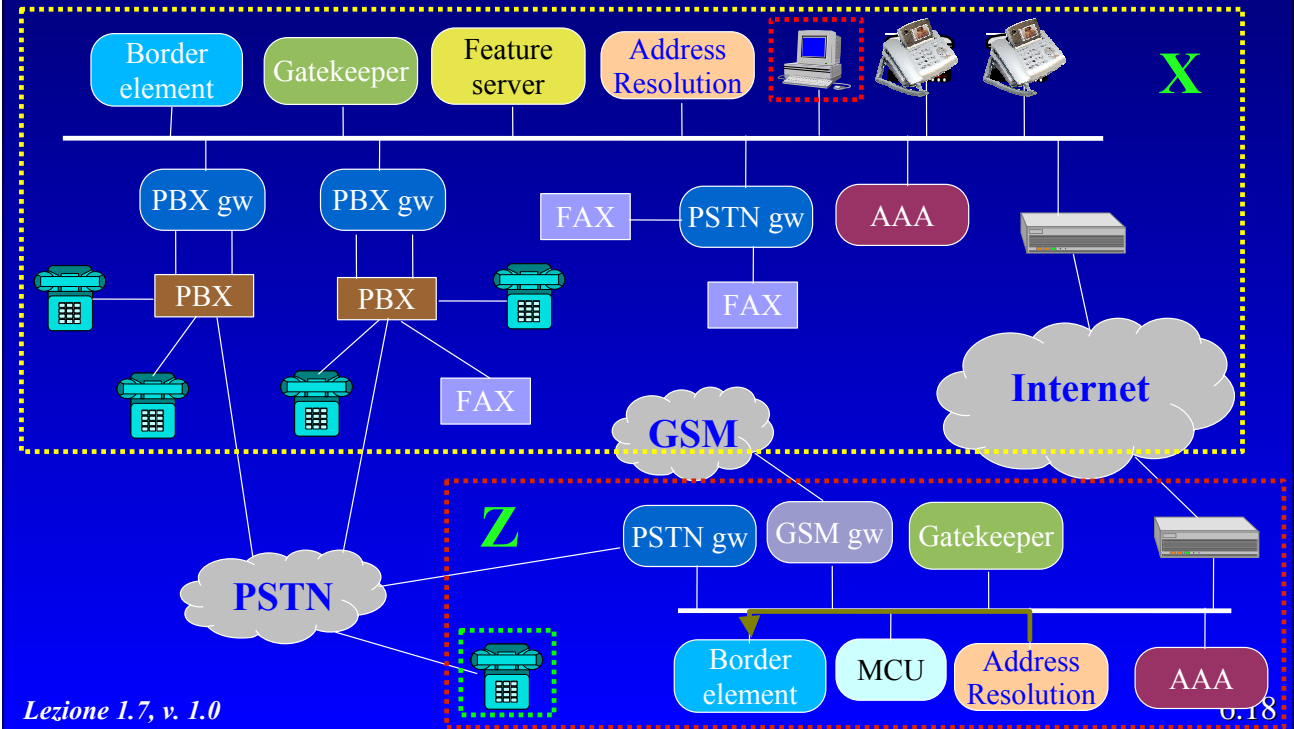
### H.323

## Chiamata Interdominio



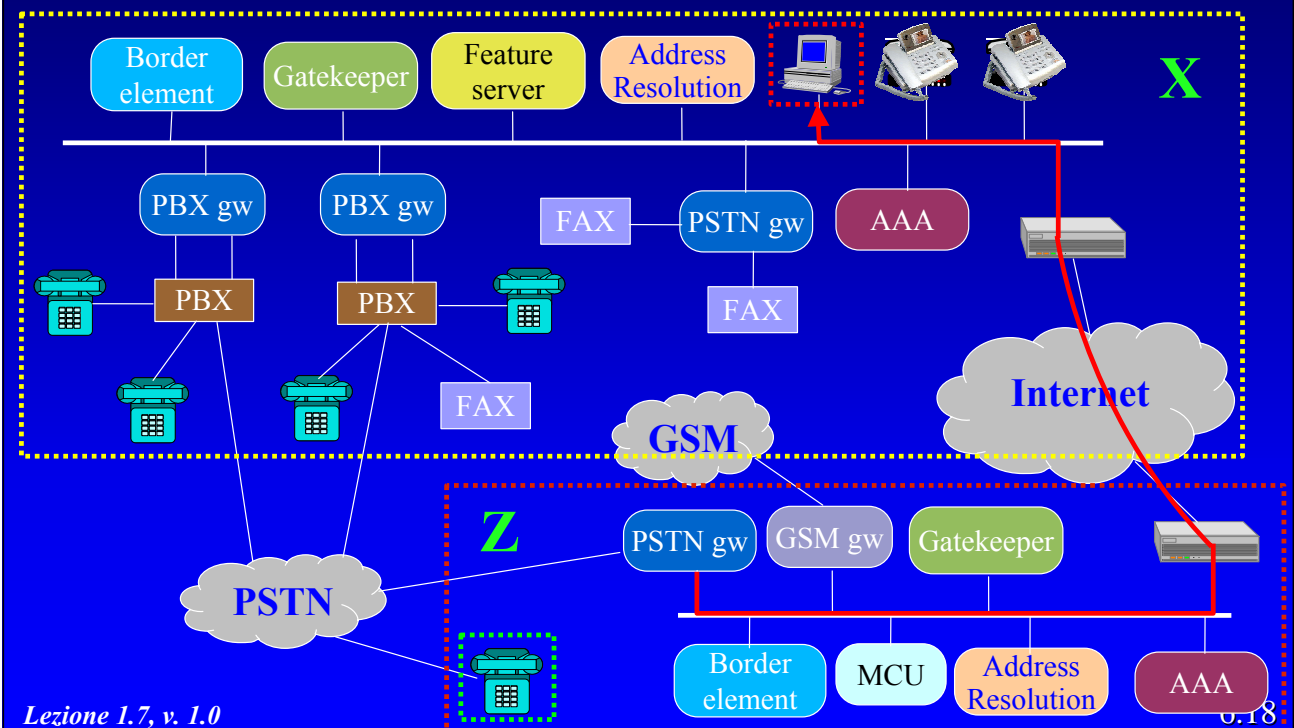
### H.323

## Chiamata Interdominio



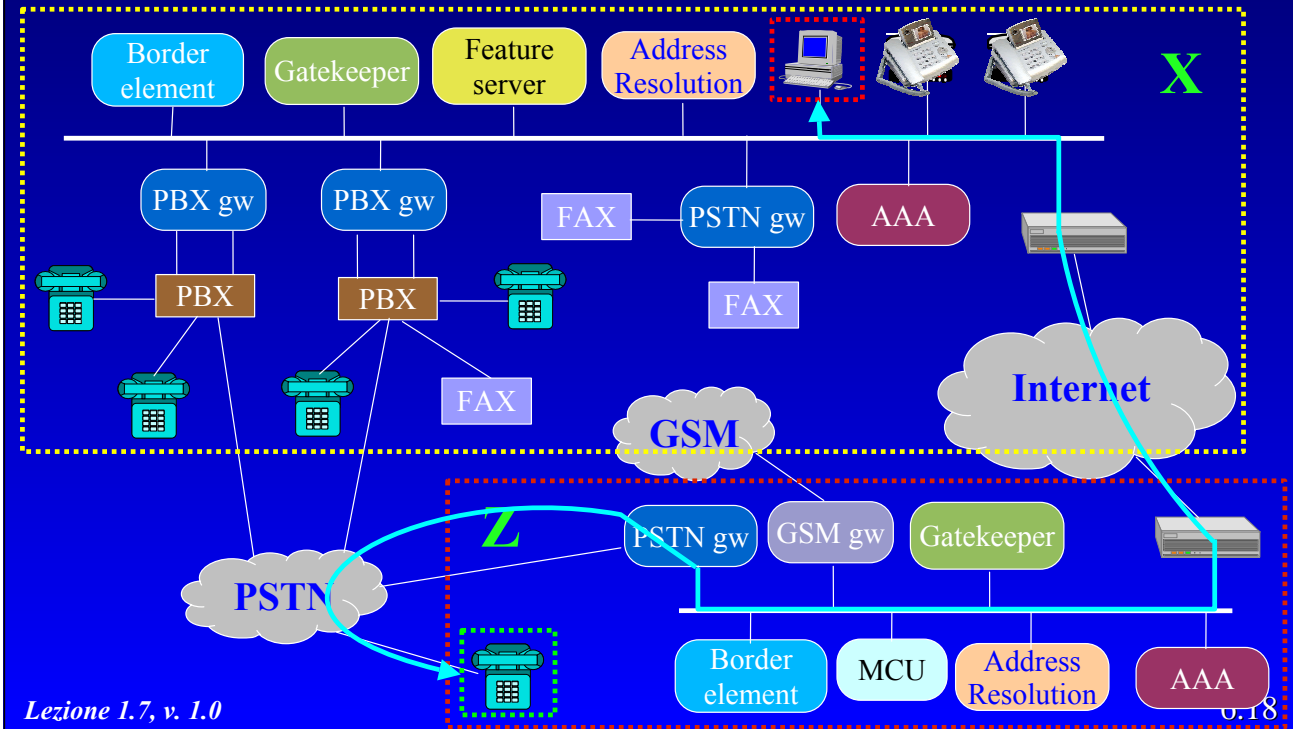
### H.323

## Chiamata Interdominio



### H.323

## Chiamata Interdominio

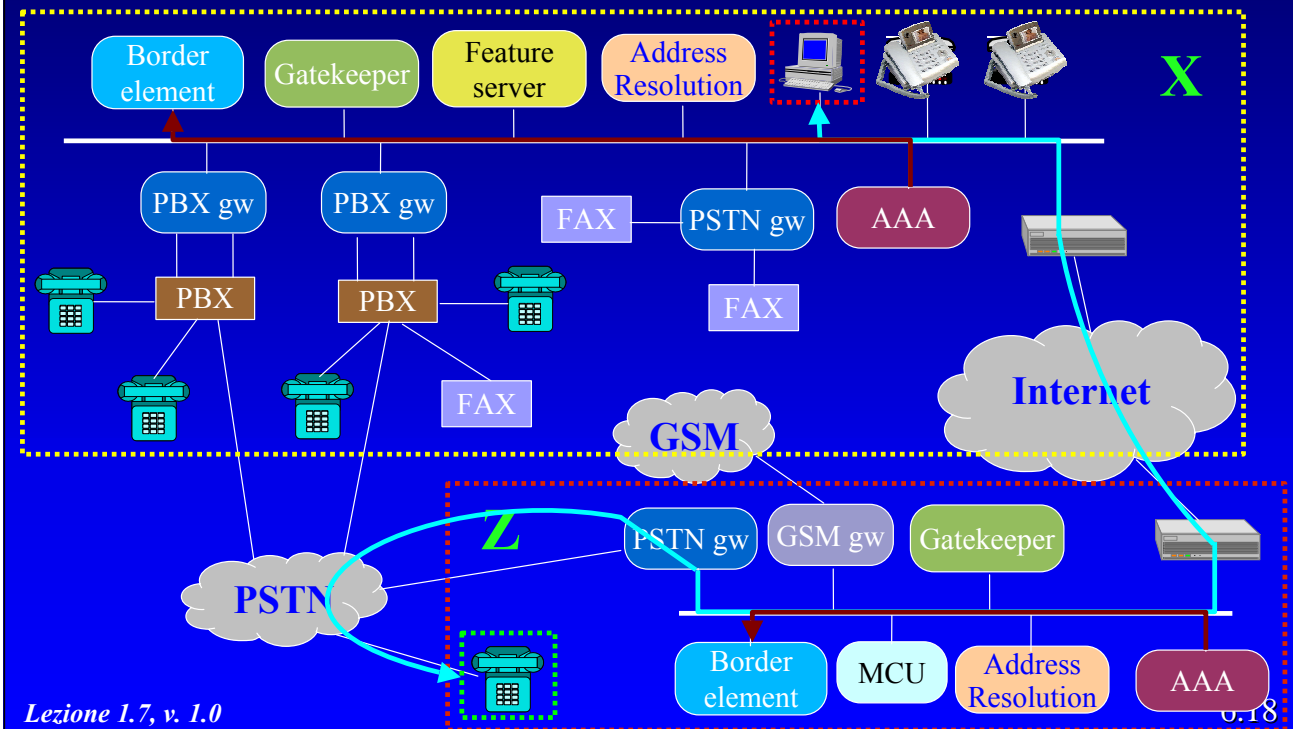


Lezione 1.7, v. 1.0

6.18

### H.323

## Chiamata Interdominio

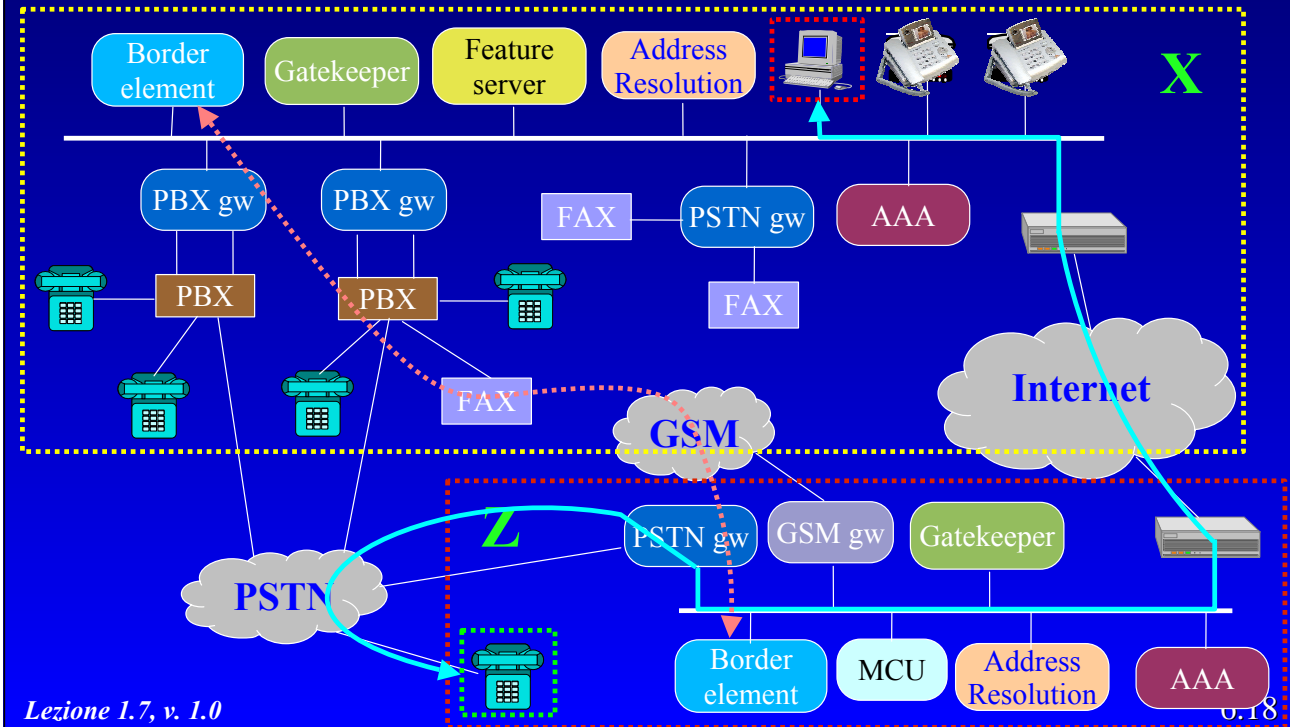


Lezione 1.7, v. 1.0

6.18

## H.323

## Chiamata Interdominio



## H.323 - Protocolli

- H.225.0-Q.931 Call Signaling

- definisce le procedure e la segnalazione necessarie per creare e terminare le chiamate tra due terminali;
- derivata da Q.931 (segnalazione ISDN) e adattata per reti a pacchetto
  - » rende l'integrazione con la rete ISDN più semplice,
  - » introduce gli "User-to-User" Information Element;
- utilizza la notazione ASN.1;
- permette di instaurare i canali di controllo H.245.

## H.323 - Protocolli

---

- H.245

- viene utilizzata tra gli *endpoint* per lo scambio di informazioni e per il controllo dei media
  - » capacità dei terminali (codifiche supportate);
  - » determinazione master/slave;
  - » apertura chiusura canali logici (per instaurazione sessioni RTP/RTCP).
- in sostanza H.245 ha, per la sessione di conferenza multimediale, la stessa funzione che RTCP ha per lo *stream* del singolo media.

## H.323 - Protocolli

---

- H.225.0-RAS (*Registration, Admission, Status*):

- usato tra i dispositivi terminali e il *gatekeeper* allo scopo di
  - » permettere al *gatekeeper* di gestire i terminali;
  - » permettere ai terminali di richiedere l'autorizzazione alle chiamate (AAA);
  - » permettere al *gatekeeper* di offrire il servizio di risoluzione dei nomi ai terminali
    - il protocollo tra *gatekeeper* e AAA o risolutore dei nomi non è standardizzato da H.323.
- deve essere utilizzato quando è presente un *gatekeeper*.

## H.323 - Protocolli

---

- RTP/RTCP, per la trasmissione dei media.
- H.450
  - definisce il dialogo tra due entità H.323 per la realizzazione di servizi supplementari;
  - si appoggia su H.225.0-Q.931;
  - le due entità possono essere
    - » due *endpoint*,
    - » un *endpoint* ed un *feature server*.
- H.323 Annex K
  - definisce l'utilizzo di HTTP tra due entità H.323 per l'esecuzione di servizi supplementari.

## H.323 - Protocolli

---

- H.323 Annex L
  - definisce il dialogo tra una entità H.323 non intelligente (es. telefono) e un *feature server*;
  - il terminale non intelligente è in grado di fornire solo "stimoli".
- H.225.0 Annex G
  - definisce il dialogo tra due *border elements*;
  - i *border element* sono utilizzati da:
    - » risolutori dei nomi,
    - » server AAA.



## H.323 - Protocolli

---

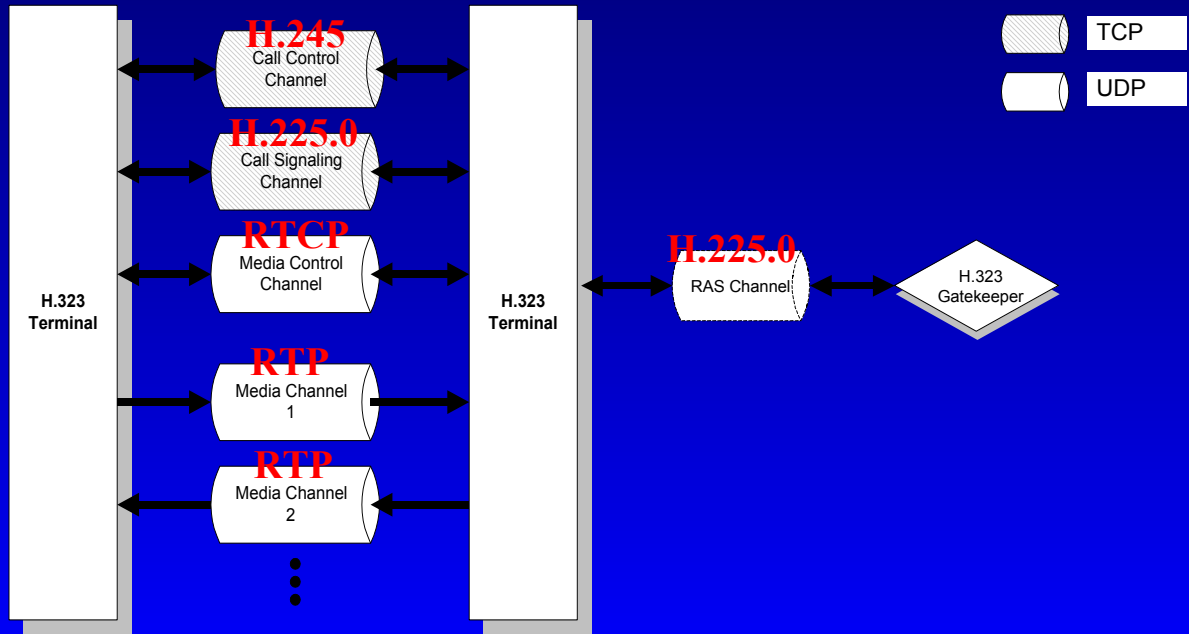
- H.460
  - diverse estensioni a H.323.
- H.501
  - gestione della mobilità per comunicazioni inter/intra dominio.
- H.510
  - *user, terminal, and service mobility.*
- H.530
  - Specifiche di sicurezza per H.510.

## H.323 - Protocolli

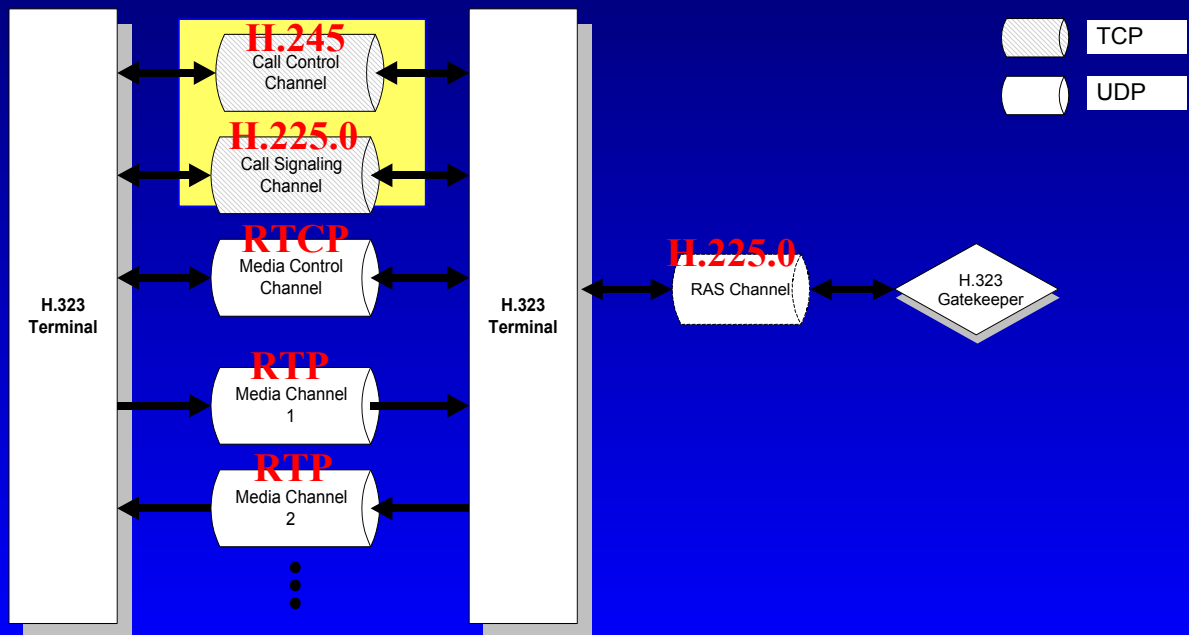
---

- H.235
  - definisce la struttura di sicurezza necessaria per garantire
    - » autenticazione,
    - » non ripudiabilità,
    - » segretezza,
    - » integrità;
  - l'informazione di sicurezza è trasportata all'interno dei messaggi H.225.0-Q.931, H.225.0-RAS, H.245, H.225.0 Annex G e RTP.

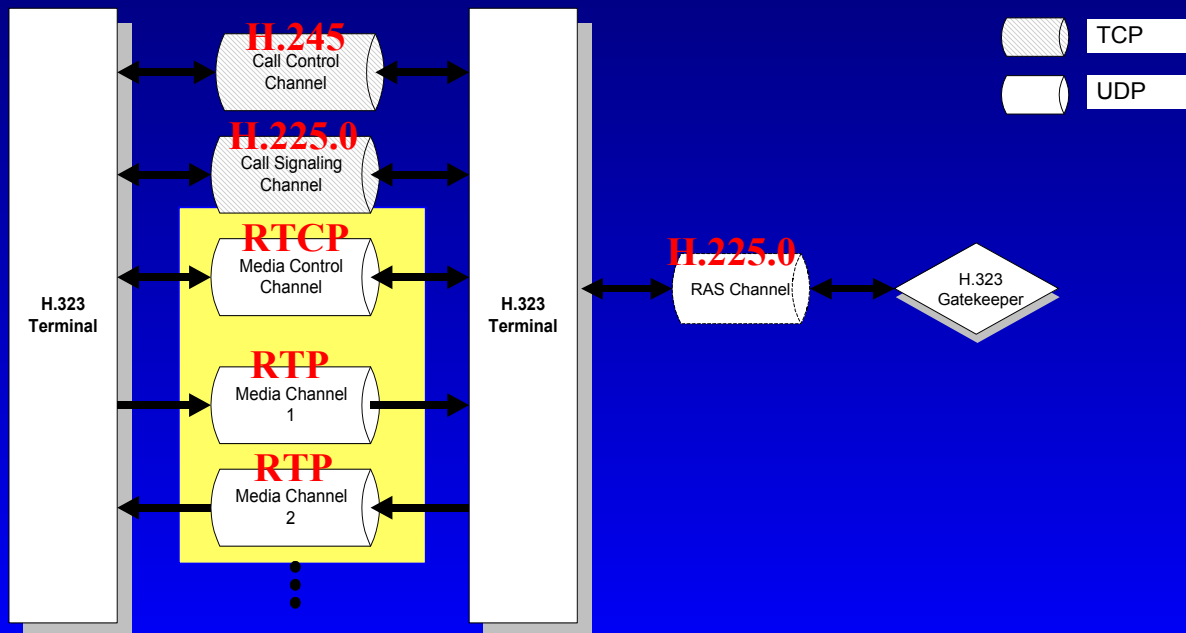
# H.323 I flussi di informazione



# H.323 I flussi di informazione



## H.323 I flussi di informazione



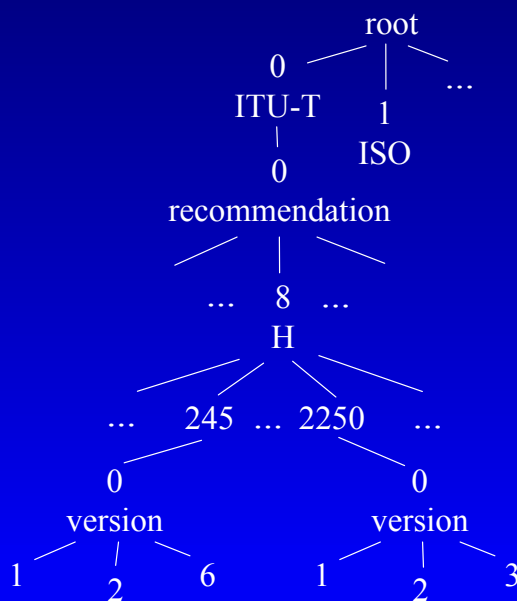
## Abstract Syntax Notation One (ASN.1)

- Definita nelle raccomandazioni ITU-T X.680 – X.683.
- Definisce diverse regole di codifica
  - Packed Encoding, XML.
- Separa la sintassi del protocollo dalla codifica utilizzata per la trasmissione.
- Permette agli sviluppatori di concentrarsi sulla logica del programma, piuttosto di perdere tempo con regole di *parsing*.

## Abstract Syntax Notation One (ASN.1)

- Utilizzato per identificare in modo univoco un database di elementi (*Object Identifier*)
  - ogni elemento è individuato da una sequenza di numeri interi, separati da un punto decimale.
- La struttura è ad albero
  - la radice non ha nome;
  - i nodi principali sono assegnati alle diverse organizzazioni;
    - » ogni organizzazione è responsabile di mantenere aggiornato il proprio ramo.

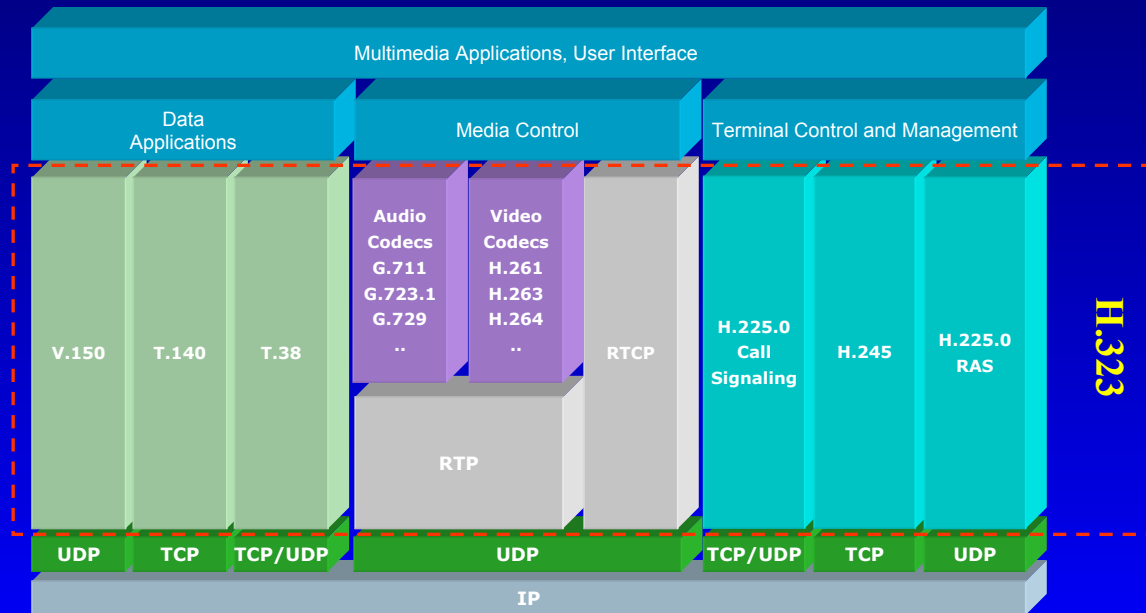
## Abstract Syntax Notation One (ASN.1)



Per. es. la versione 6 di H.245 è identificata da:  
0.0.8.245.0.6

H.225.0-RAS e  
H.225.0-Q.931 hanno  
lo stesso  
identificativo:  
0.0.8.2250.0.3

## H.323: Architettura protocollare tipica



Lezione 1.7, v. 1.0

6.30

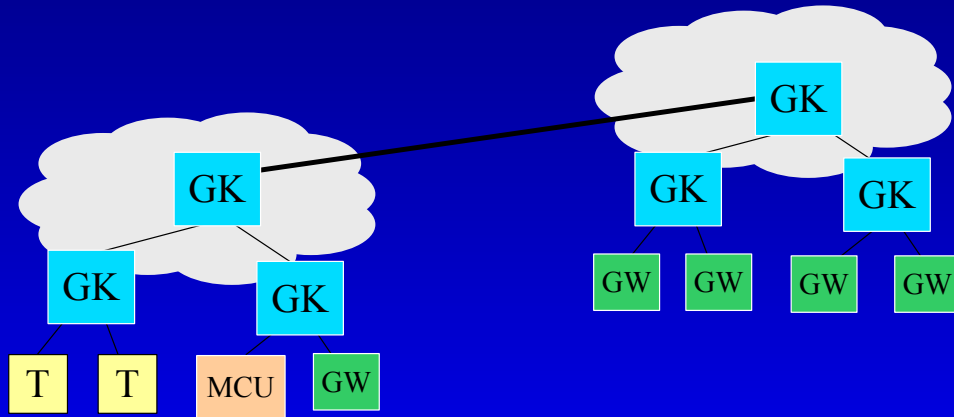
## Comunicazione tra domini amministrativi

- I Service Provider possono utilizzare due diverse architetture per la comunicazione Interdominio
  - RAS
    - » crea una struttura gerarchica di Gatekeeper;
  - H.225.0 Annex G
    - » utilizza i Border Element (BE).

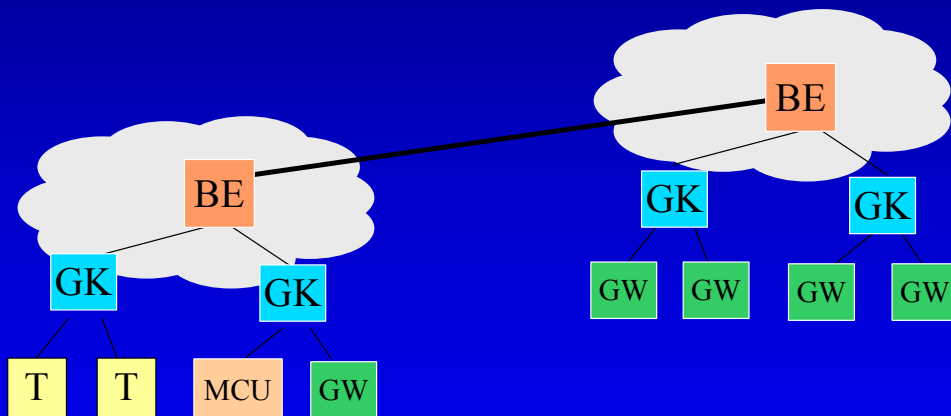
Lezione 1.7, v. 1.0

6.31

## Comunicazione tra domini amministrativi Topologia con RAS



## Comunicazione tra domini amministrativi Topologia con H.225 Annex G



## Chiamate Punto-Punto

---

- Identificazione degli *endpoint*
  - risoluzione degli indirizzi
- Instaurazione delle chiamate
  - segnalazione: H.225.0 Call Signalling
  - controllo: H.245
  - RAS
  - Modelli di chiamate

## Chiamate Punto-Punto

---

- Identificazione degli *endpoint*
  - risoluzione degli indirizzi
- Instaurazione delle chiamate
  - segnalazione: H.225.0 Call Signalling
  - controllo: H.245
  - RAS
  - Modelli di chiamate

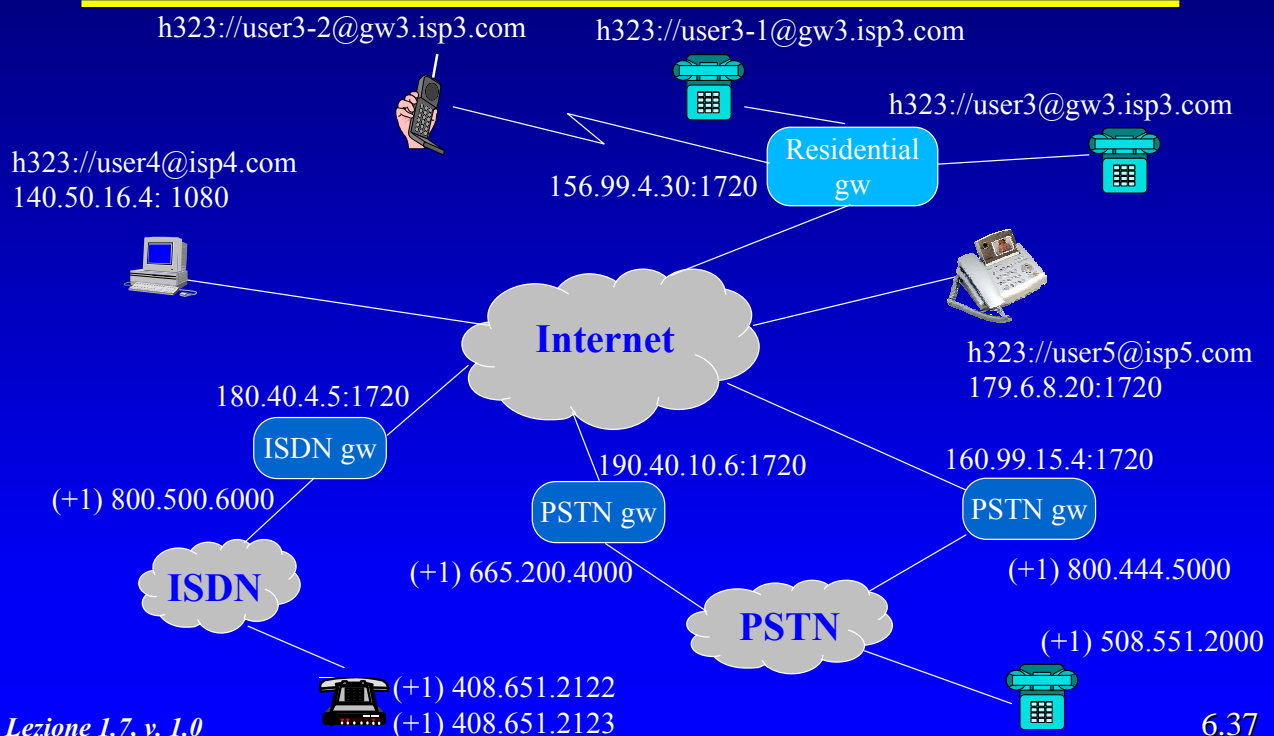
## Chiamate Punto-Punto

# Identificazione degli endpoint

- Gli utenti H.323 possono essere identificati attraverso:
  - un numero E.164
    - » (+1) 408.651.2122, (+1) 408.651.2123;
  - un indirizzo IP e una porta TCP
    - » 179.6.8.20:1720
  - un URL H.323
    - » h323://user@domain, h323://domain/user
    - » la parte "domain" deve poter essere tradotta in un indirizzo IP + una porta TCP (DNS, LDAP),
    - » la parte "user" identifica lo specifico utente in sistemi potenzialmente multiutente.

## Chiamate Punto-Punto

# Identificazione degli endpoint





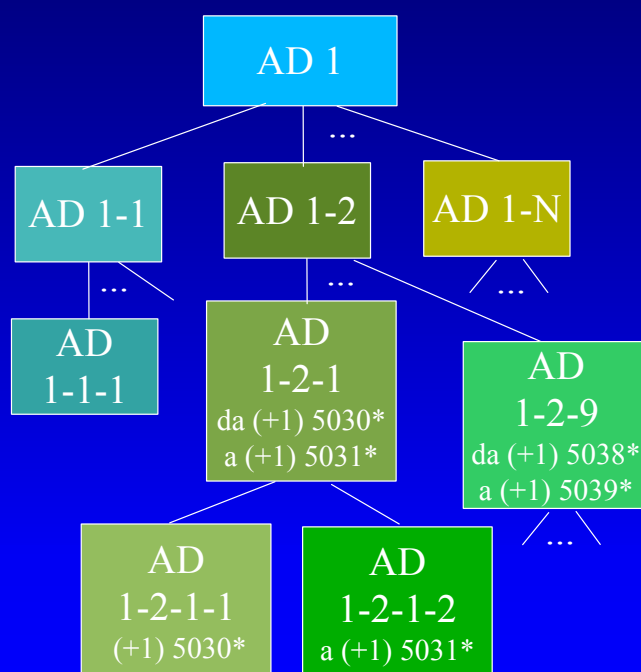
## Chiamate Punto-Punto

### Identificazione degli endpoint

- Nessun Service Provider può fornire un servizio globale
  - la presenza di diversi Service Provider rende necessaria la cooperazione per far comunicare due qualsiasi utenti;
  - parte di questa cooperazione consiste nello scambio di informazioni per l'instradamento delle comunicazioni;
  - H.225.0 Annex G è il protocollo in H.323 che i Border Element utilizzano per comunicare tra loro.

## Chiamate Punto-Punto

### Strutture per risolvere gli alias



### Struttura gerarchica

Funziona in maniera analoga ad un DNS.

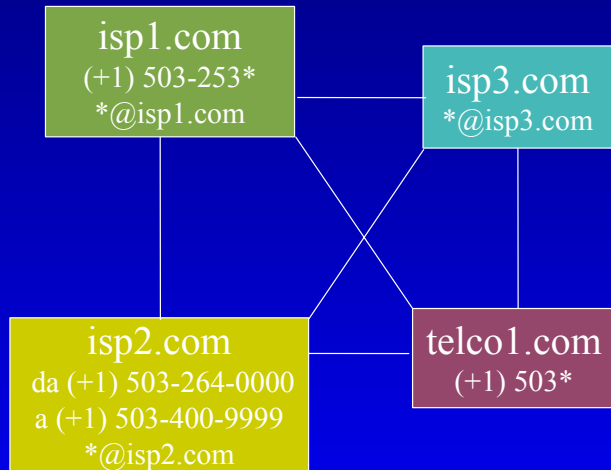
AD = Administrative Domain

## Chiamate Punto-Punto

# Strutture per risolvere gli alias

## Struttura distribuita

Ogni dominio possiede la lista degli altri domini e degli indirizzi che risolvono.



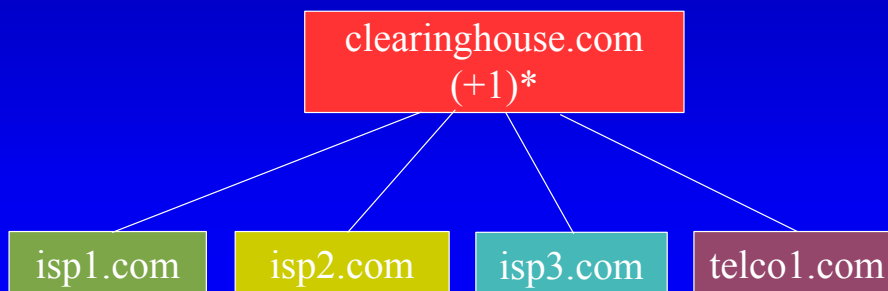
## Chiamate Punto-Punto

# Strutture per risolvere gli alias

## Organizzazione Clearinghouse

Una unica organizzazione mantiene accordi bilaterali con tutti i domini.

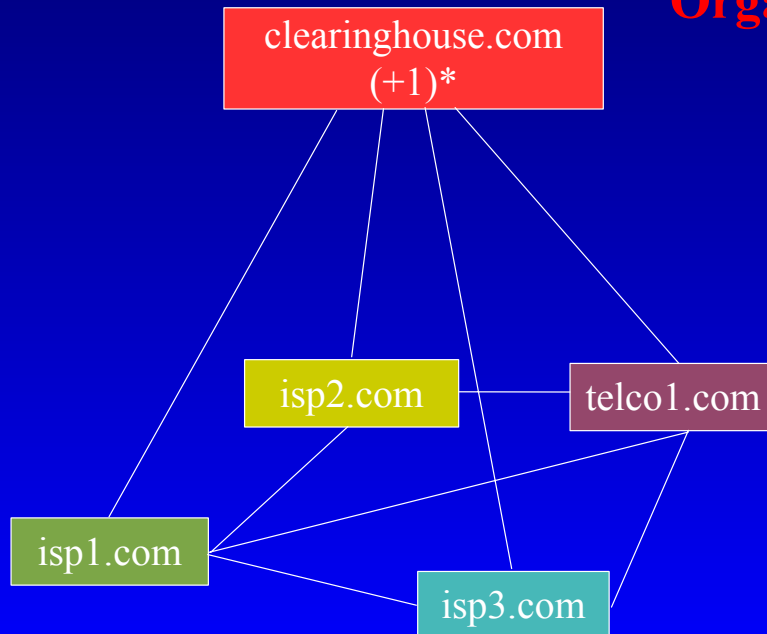
La clearinghouse agisce come intermediario nel processo di instaurazione di ogni chiamata interdominio.



## Chiamate Punto-Punto

# Strutture per risolvere gli alias

## Organizzazione Ibrida



Ogni dominio mantiene accordi bilaterali con gli altri e con la clearinghouse.

## Chiamate Punto-Punto

# Strutture per risolvere gli alias

- I BE all'interno dei domini possono essere identificati con:
  - indirizzi e-mail
    - » be-ID@be-admin-domain;
  - URL specifiche:
    - » h2250-annex-g://be-ID@be-admin-domain,
    - » h2250-annex-g://be-admin-domain/be-ID,
    - » es. h2250-annex-g://be1@be.isp3.com, h2250-annex-g://503@be.telco1.com.

**Chiamate Punto-Punto****H.225.0 Annex G**

---

- H.225.0 Annex G può essere usato sia su TCP che su UDP.
- Prevede un funzionamento di tipo client-server tra i BE.
- Funzioni
  - traduzione degli indirizzi;
  - propagazione di informazioni di instradamento;
  - *usage reporting*;
  - *access authorization*.

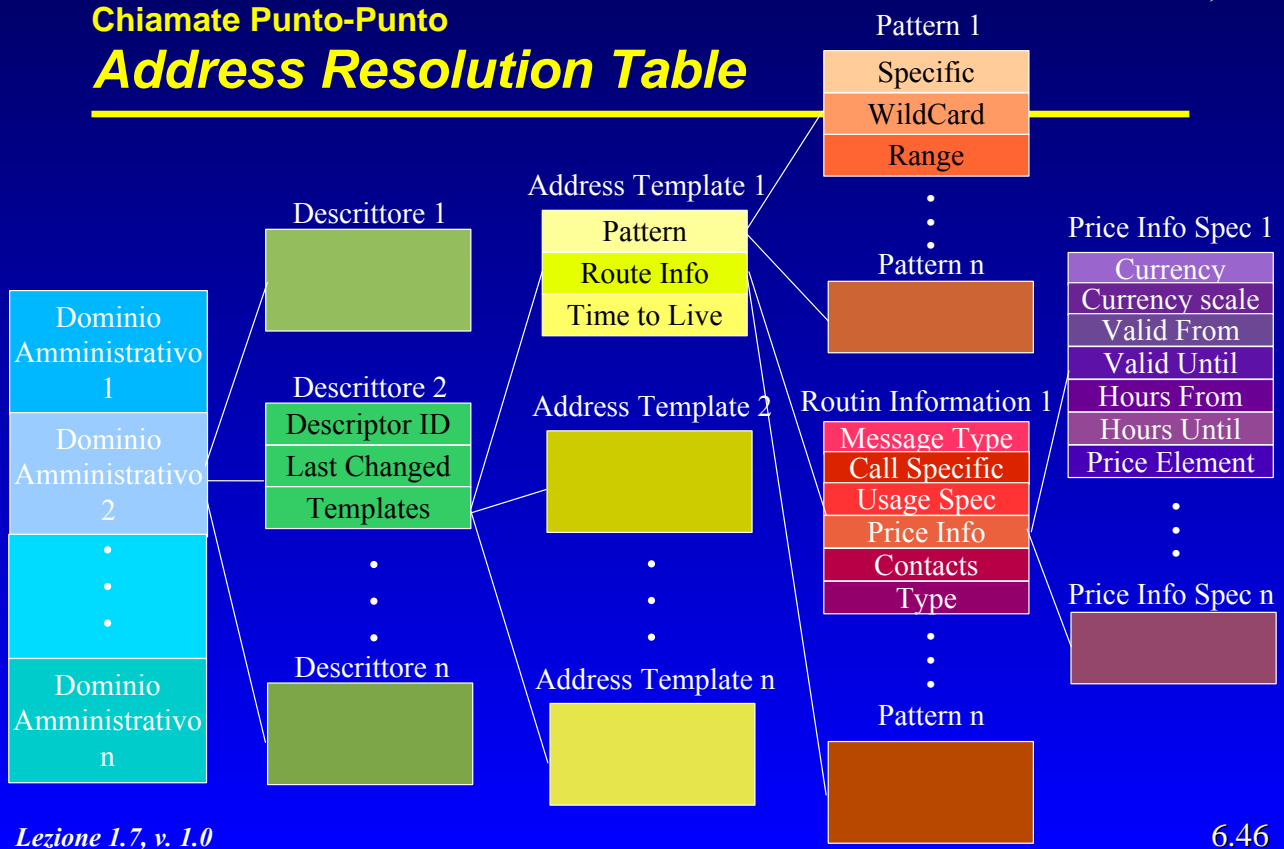
**Chiamate Punto-Punto****La risoluzione degli alias**

---

- Per tradurre gli alias in indirizzi IP i BE utilizzano una *Address Resolution Table* (ART).
  - consiste in una lista di domini amministrativi in grado di terminare le chiamate;
  - è organizzata in descrittori, *template* e *pattern*;
  - le informazioni contenute riguardano il dominio, gli alias che possono essere terminati, informazioni di instradamento, i costi del servizio.

## Chiamate Punto-Punto

# Address Resolution Table



Lezione 1.7, v. 1.0

6.46

## Chiamate Punto-Punto

# Address Resolution Table

- La costruzione di una ART richiede
  - di conoscere i domini amministrativi e i relativi BE
    - » accordi bilaterali tra i domini amministrativi,
      - si configura il nome DNS del BE;
      - non è prevista nessuna procedura automatica;
    - » a partire dal nome DNS, si risale all'indirizzo attraverso i record SRV o TXT;
  - di stabilire delle relazioni di servizio con questi BE;
  - di collezionare i descrittori dai domini amministrativi.

Lezione 1.7, v. 1.0

6.47

## Chiamate Punto-Punto

### Record SRV

---

- I record SRV permettono di localizzare i servizi all'interno di un dominio:
  - `srv.prot.name ttl class pri weight port target`
  - es.:
    - » `_http._tcp IN SRV 0 5 80 www.example.com`
    - » `_h2250_annex_g._udp IN SRV 0 5 2099 server.example.com;`
  - l'utilizzo dei record SRV non è attualmente molto diffuso.
- La risposta ad una richiesta di record TXT consiste in un record di tipo A relativo al nome del dominio.

## Chiamate Punto-Punto

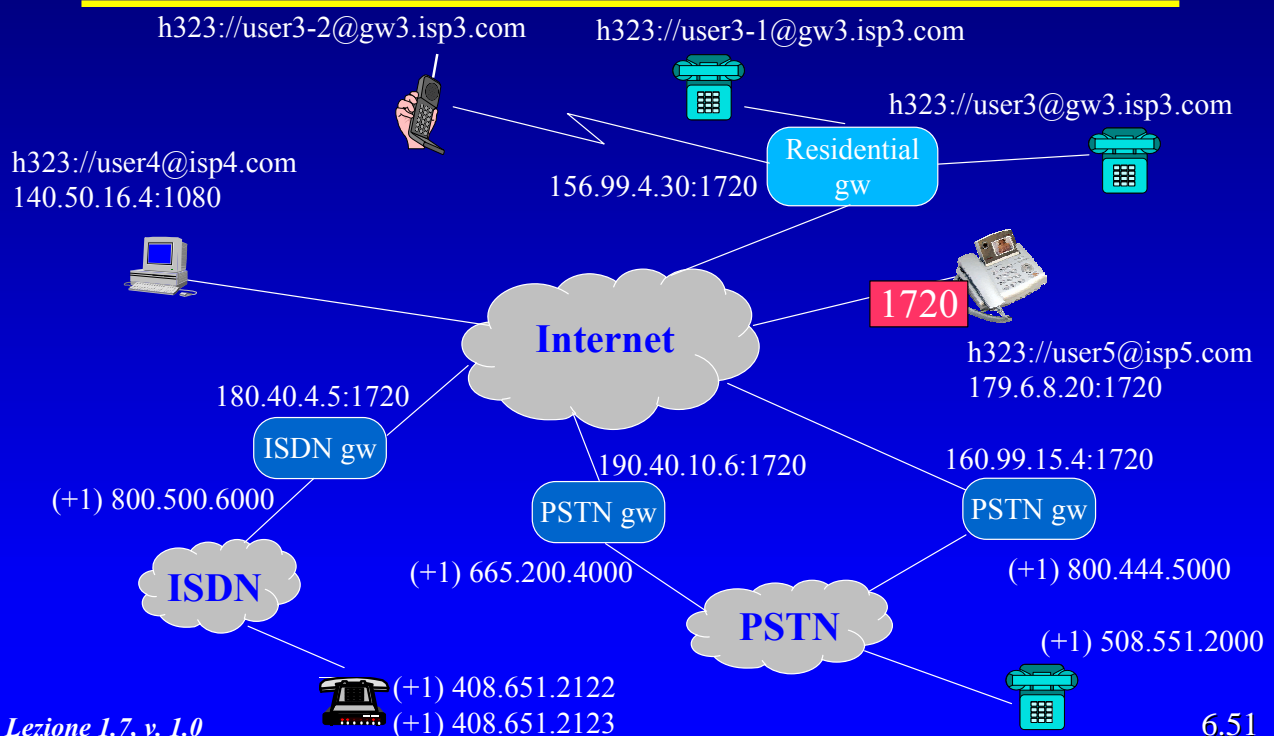
---

- Identificazione degli *endpoint*
  - risoluzione degli indirizzi
- Instaurazione delle chiamate
  - segnalazione: H.225.0 Call Signalling
  - controllo: H.245
  - RAS
  - Modelli di chiamate

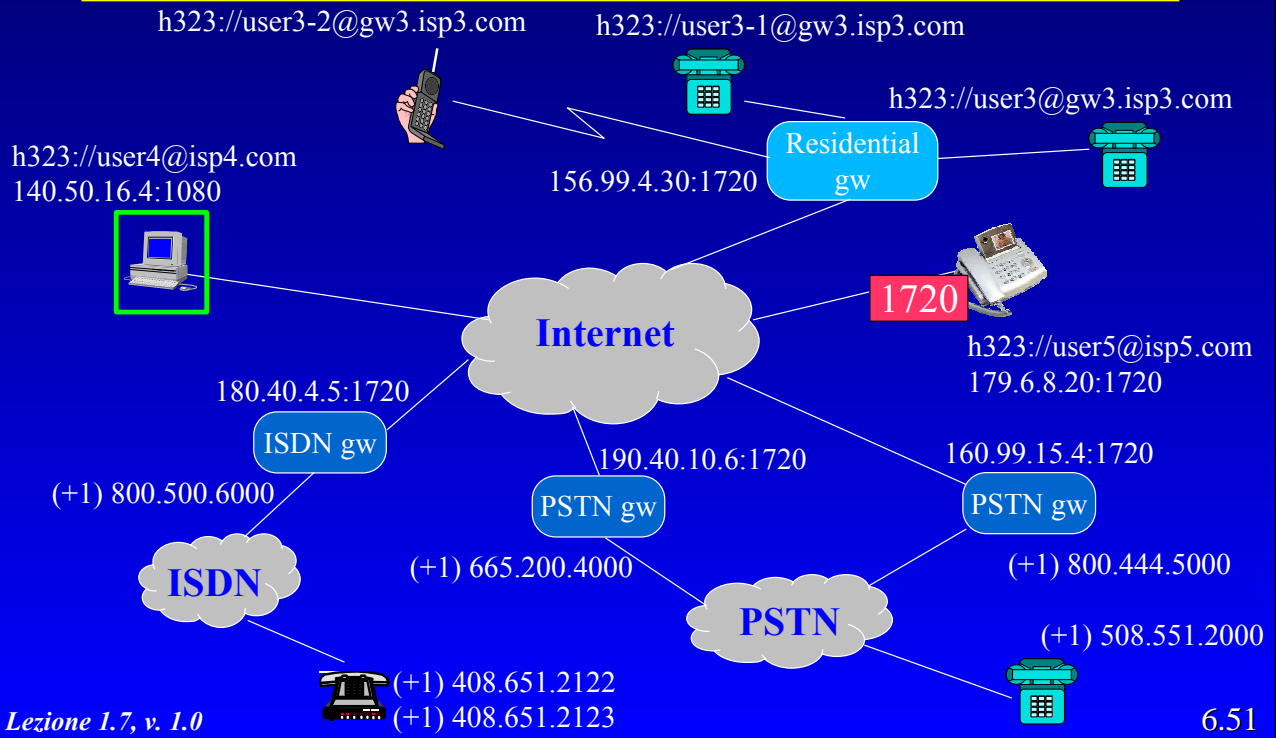
## Chiamate Punto-Punto H.225.0 Call Signaling

- L'utente 4 (terminale 4) vuole effettuare una chiamata verso l'utente 5.
- I meccanismi per ottenere l'indirizzo dell'utente 5 sono già stati descritti.
- L'utente 4 inizia quindi una connessione verso l'host 179.6.8.20, porta 1720  
- 1720 è una porta di *default* per H.323.

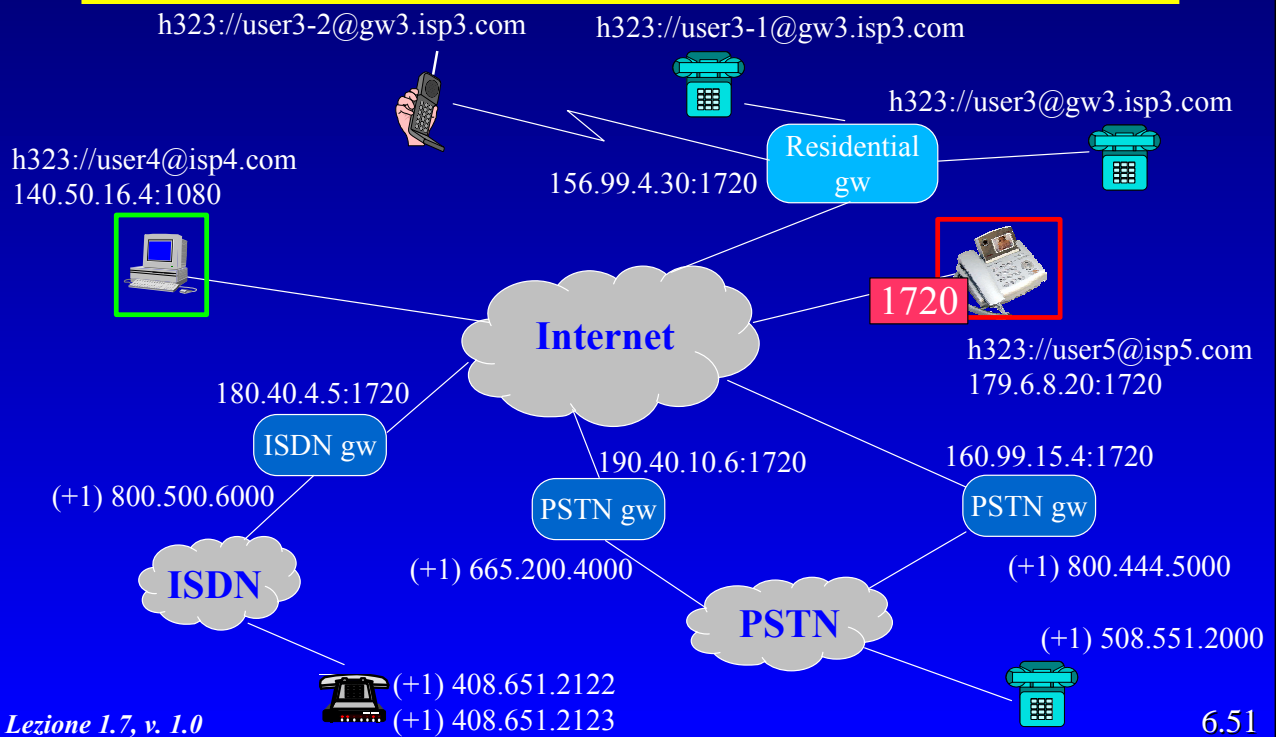
## Chiamate Punto-Punto H.225.0 Call Signaling



# Chiamate Punto-Punto H.225.0 Call Signaling

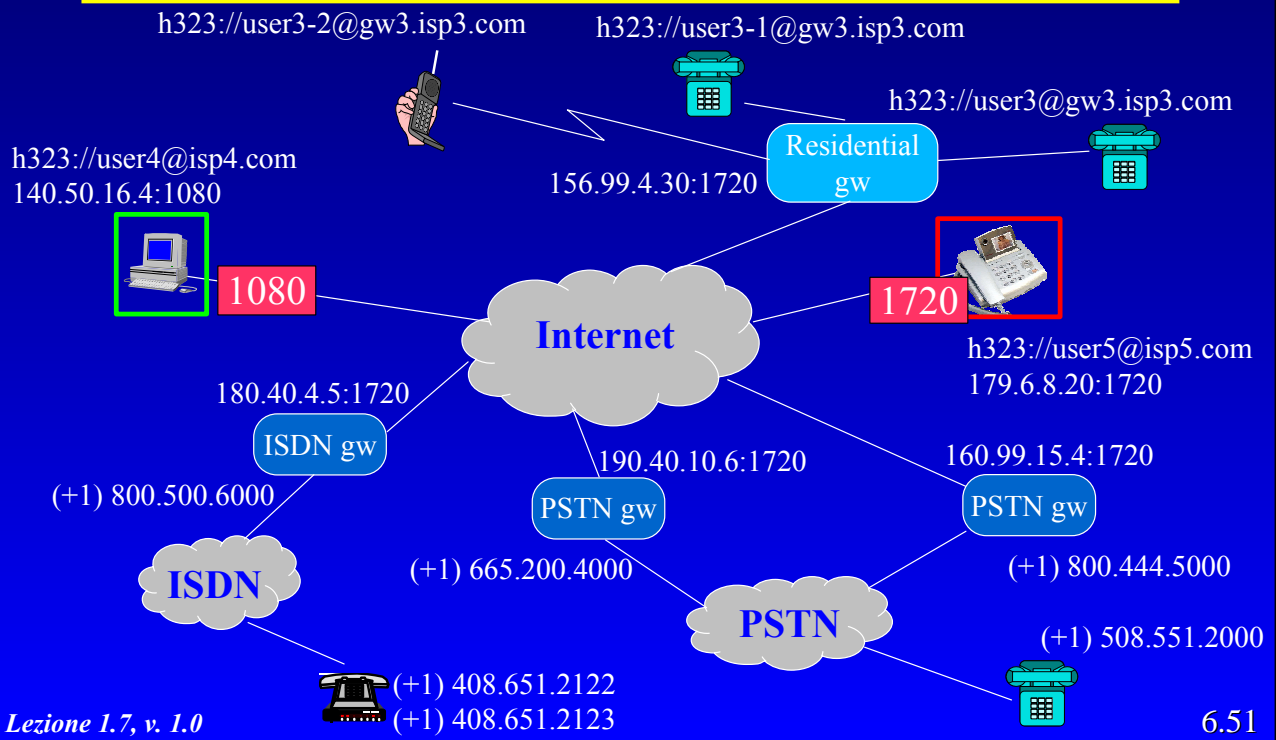


# Chiamate Punto-Punto H.225.0 Call Signaling

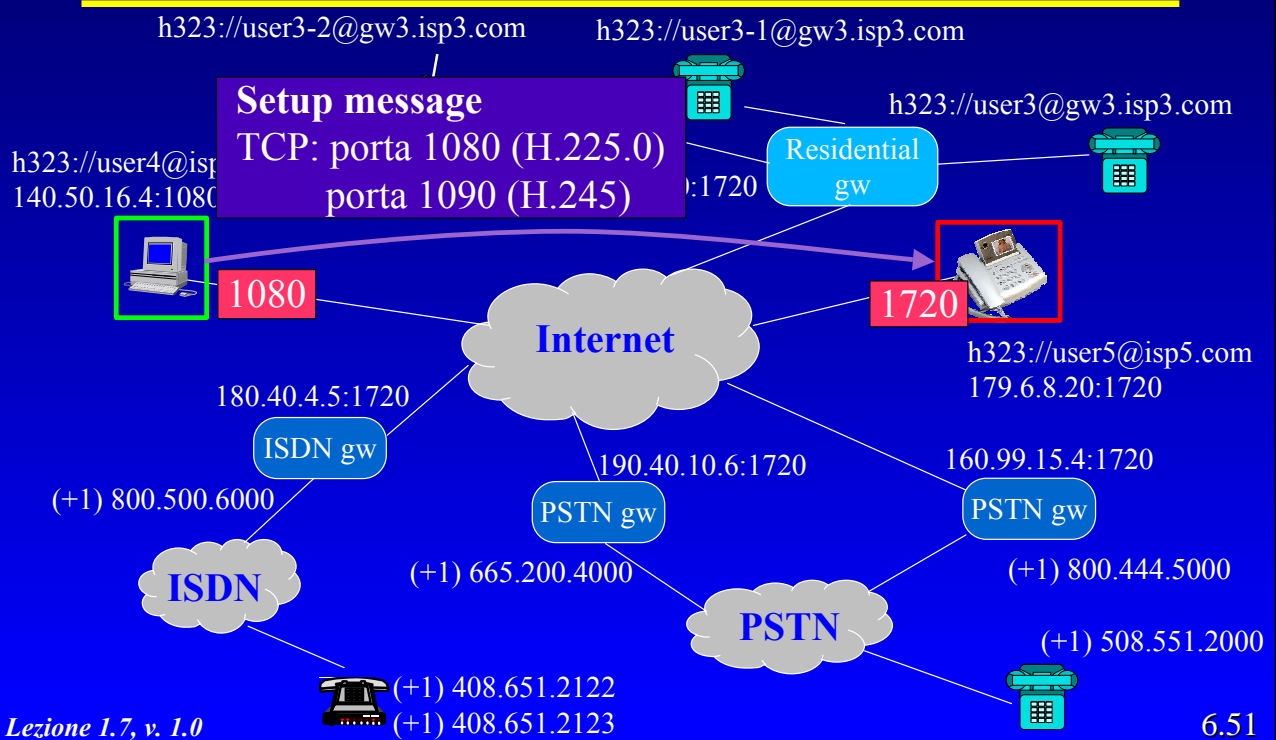




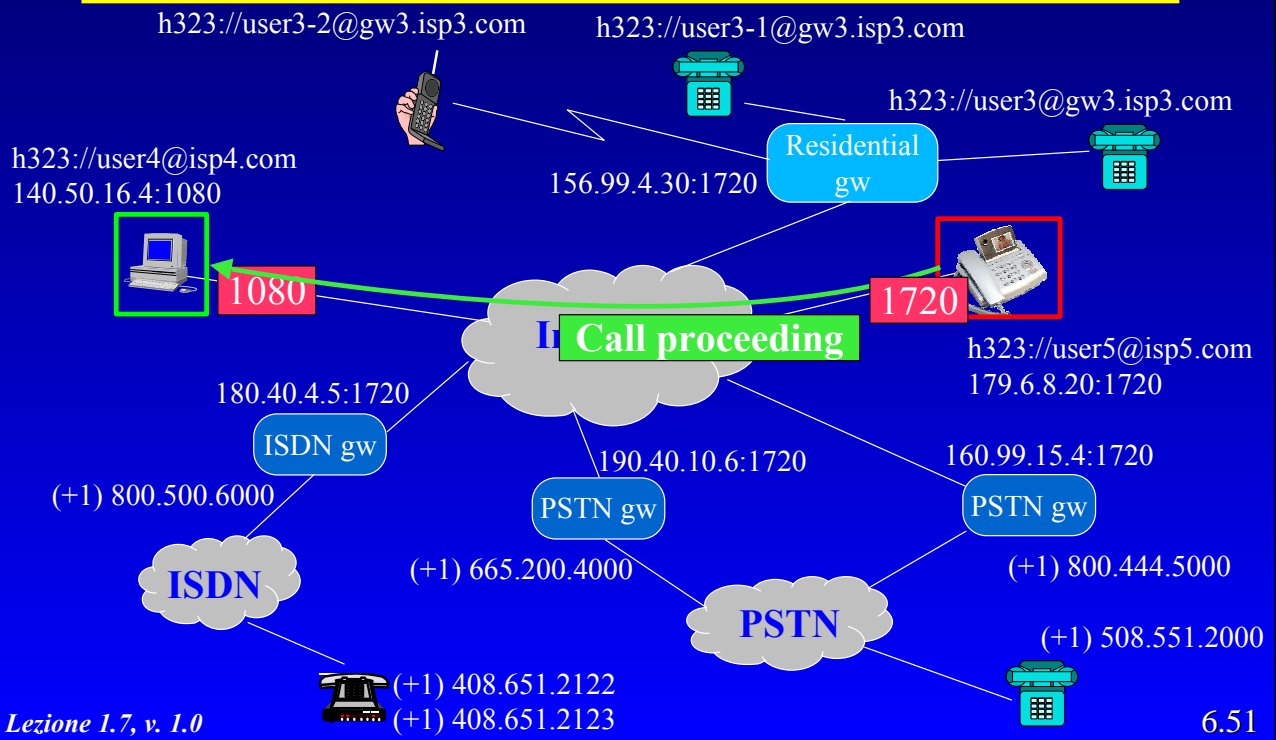
# Chiamate Punto-Punto H.225.0 Call Signaling



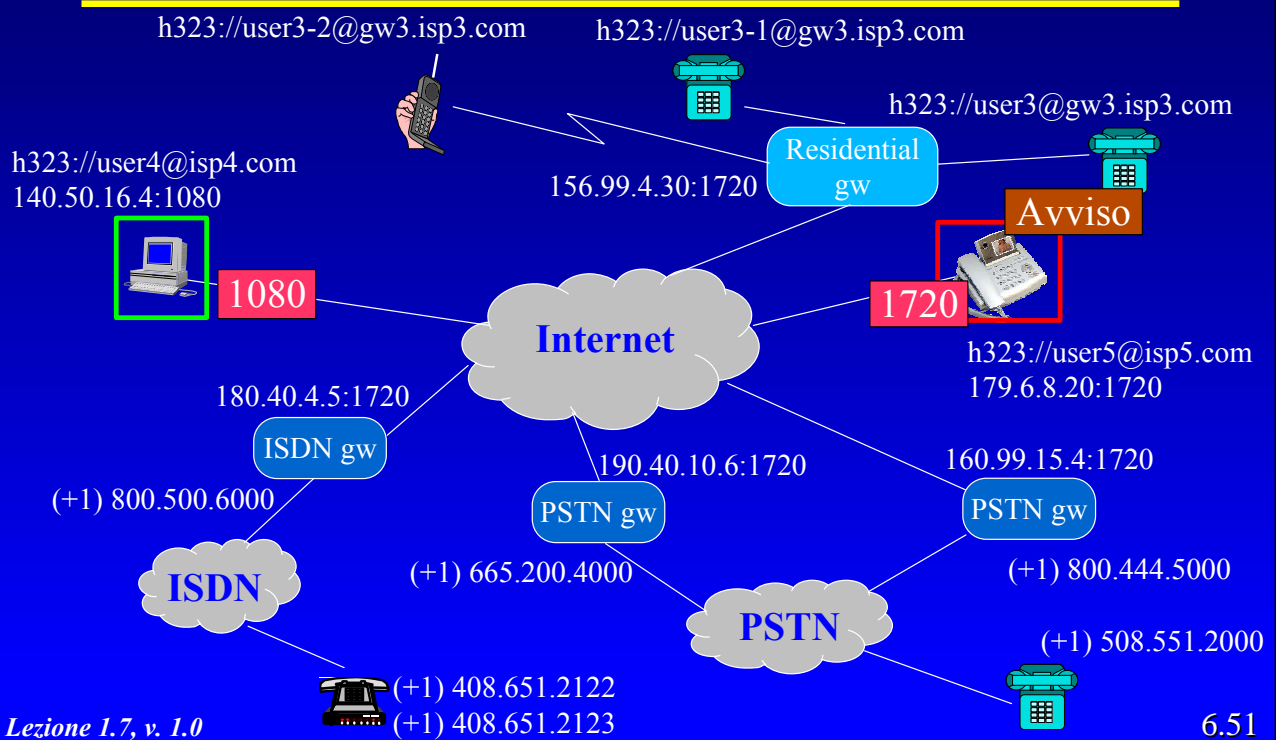
# Chiamate Punto-Punto H.225.0 Call Signaling



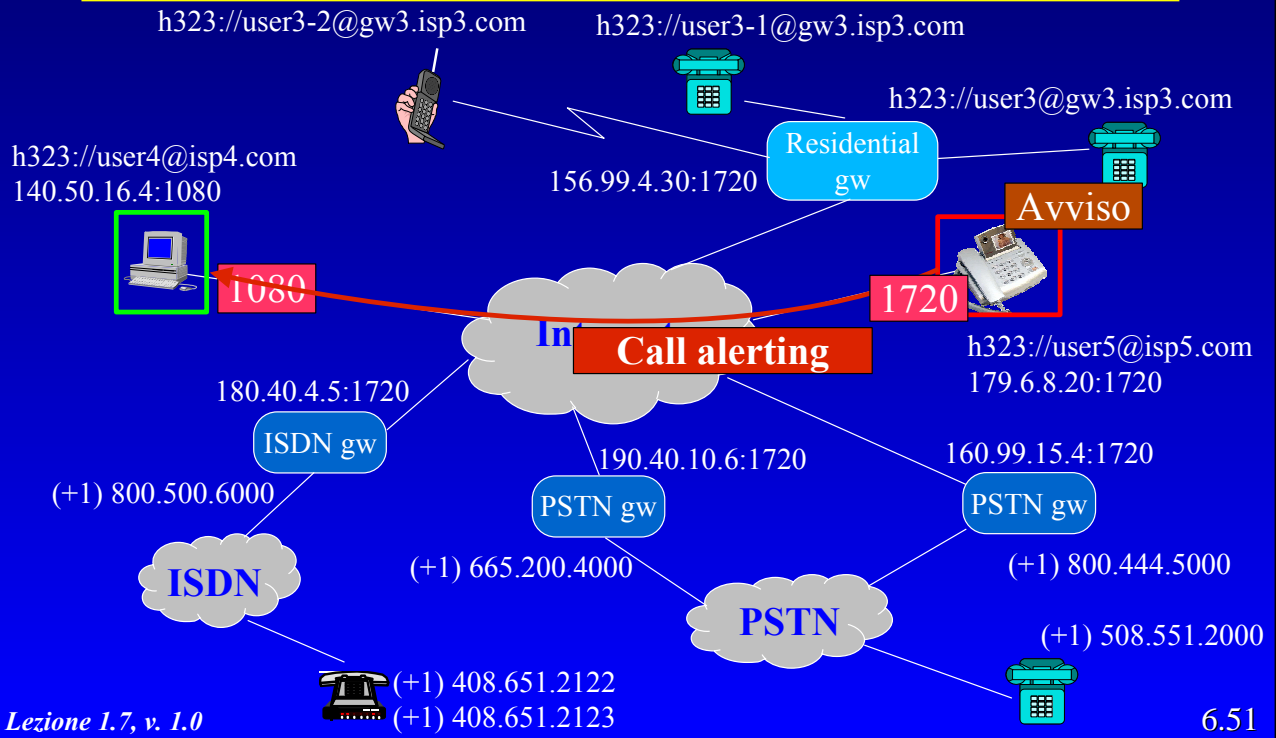
# Chiamate Punto-Punto H.225.0 Call Signaling



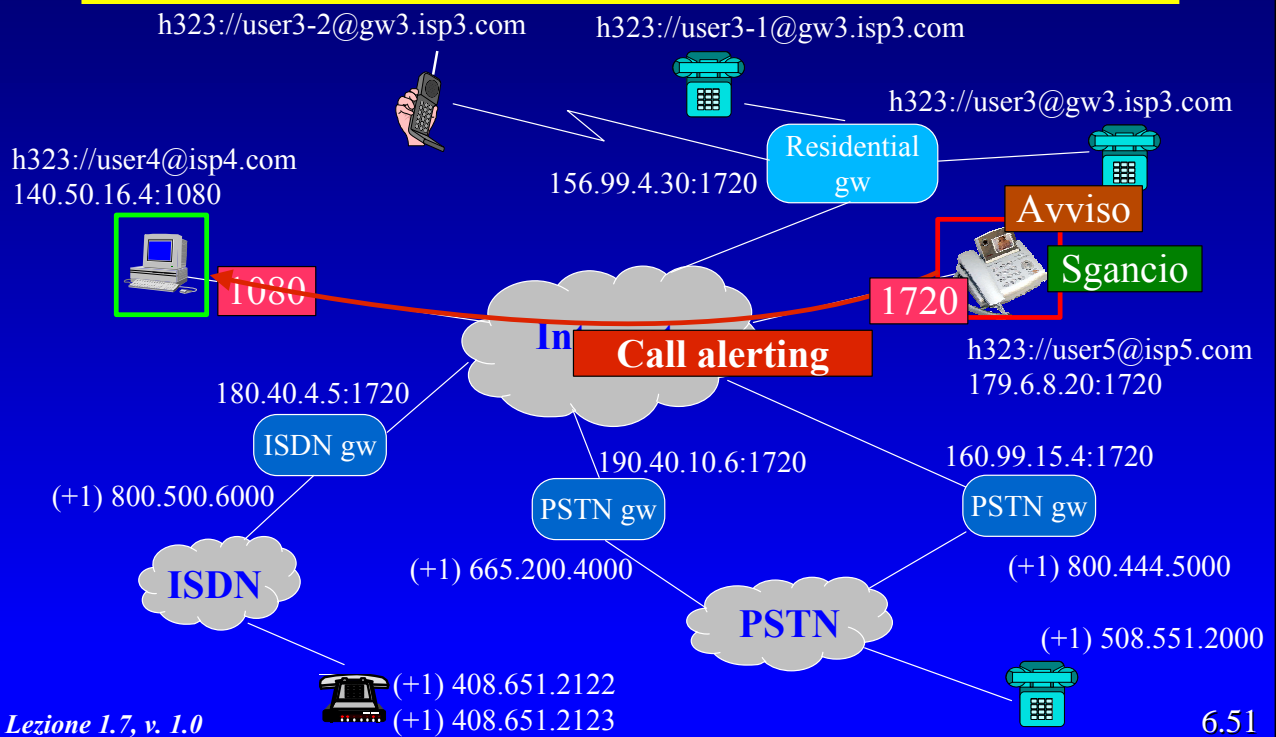
# Chiamate Punto-Punto H.225.0 Call Signaling



# Chiamate Punto-Punto H.225.0 Call Signaling



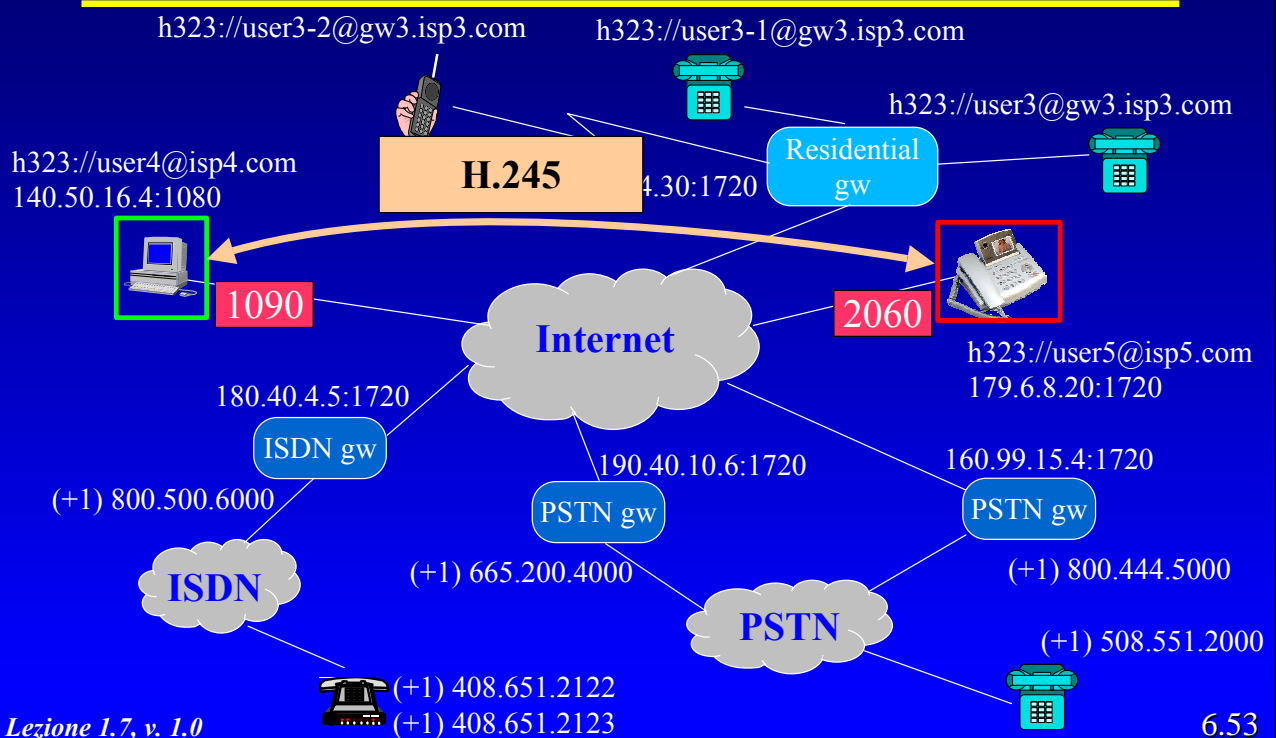
# Chiamate Punto-Punto H.225.0 Call Signaling



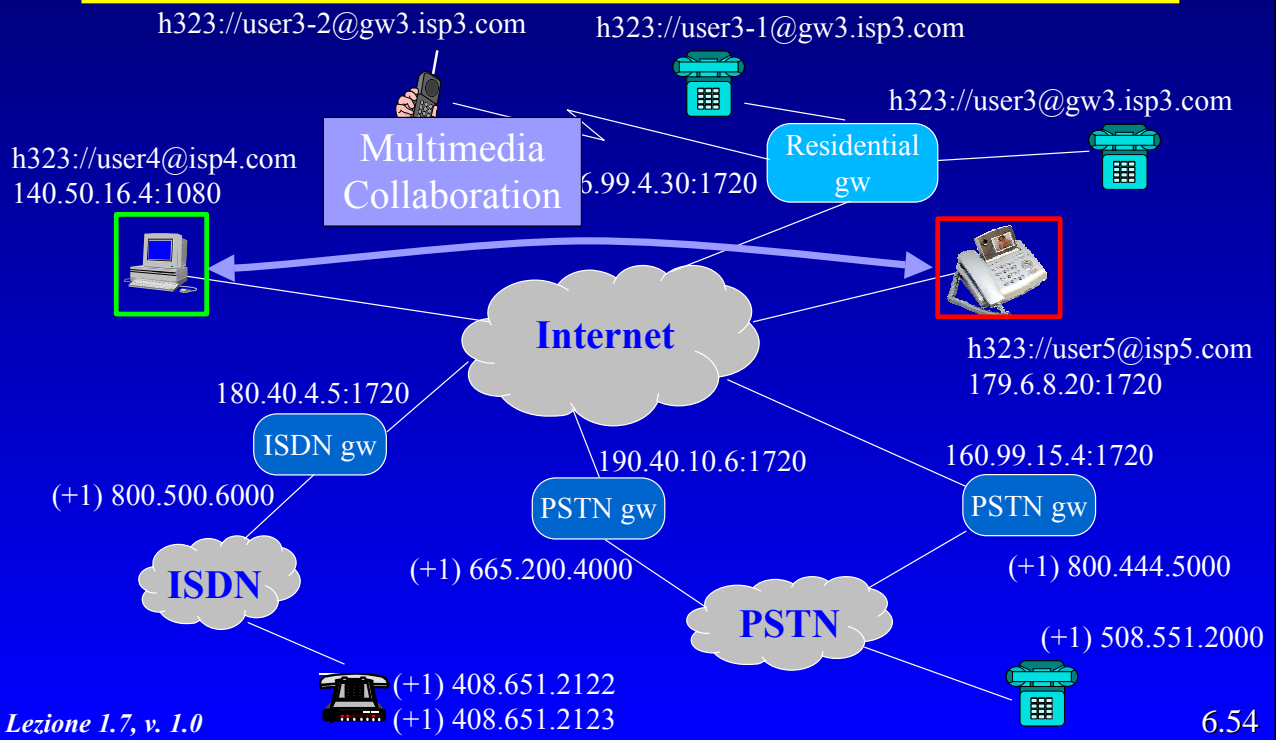
# Chiamate Punto-Punto H.225.0 Call Signaling



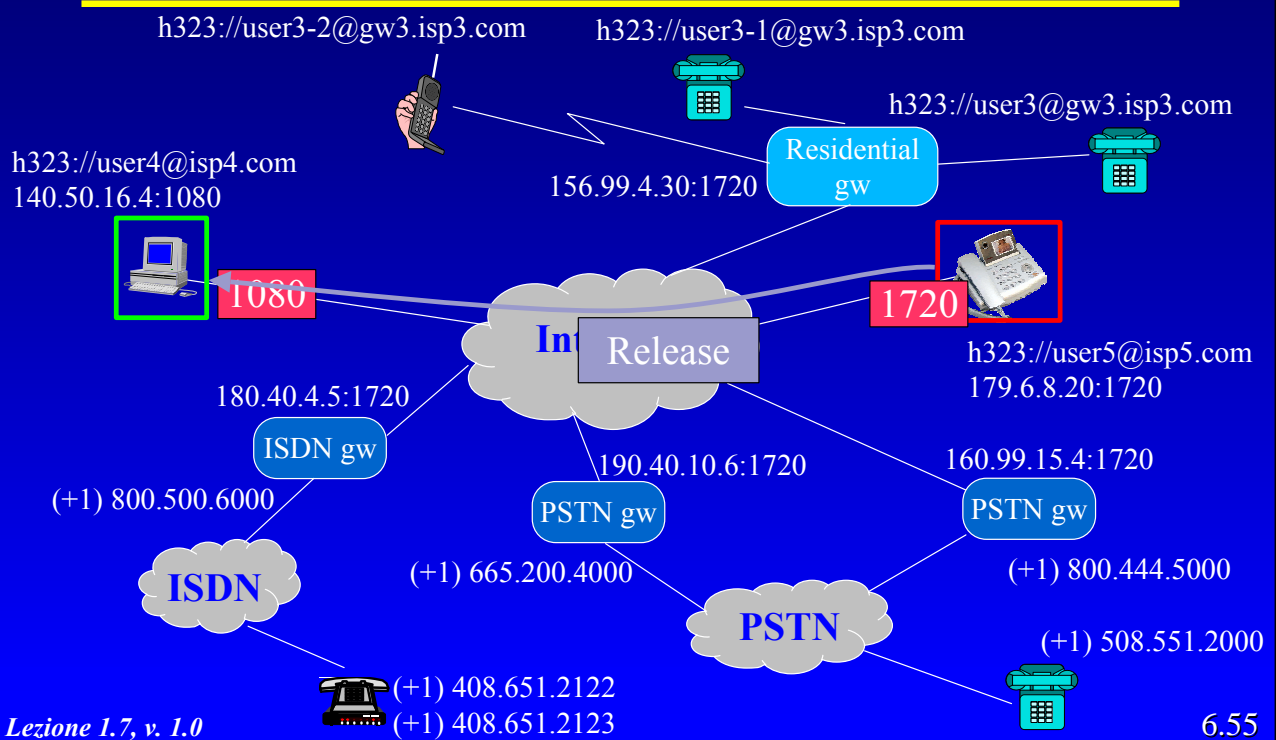
# Chiamate Punto-Punto H.225.0 Call Signaling



# Chiamate Punto-Punto H.225.0 Call Signaling



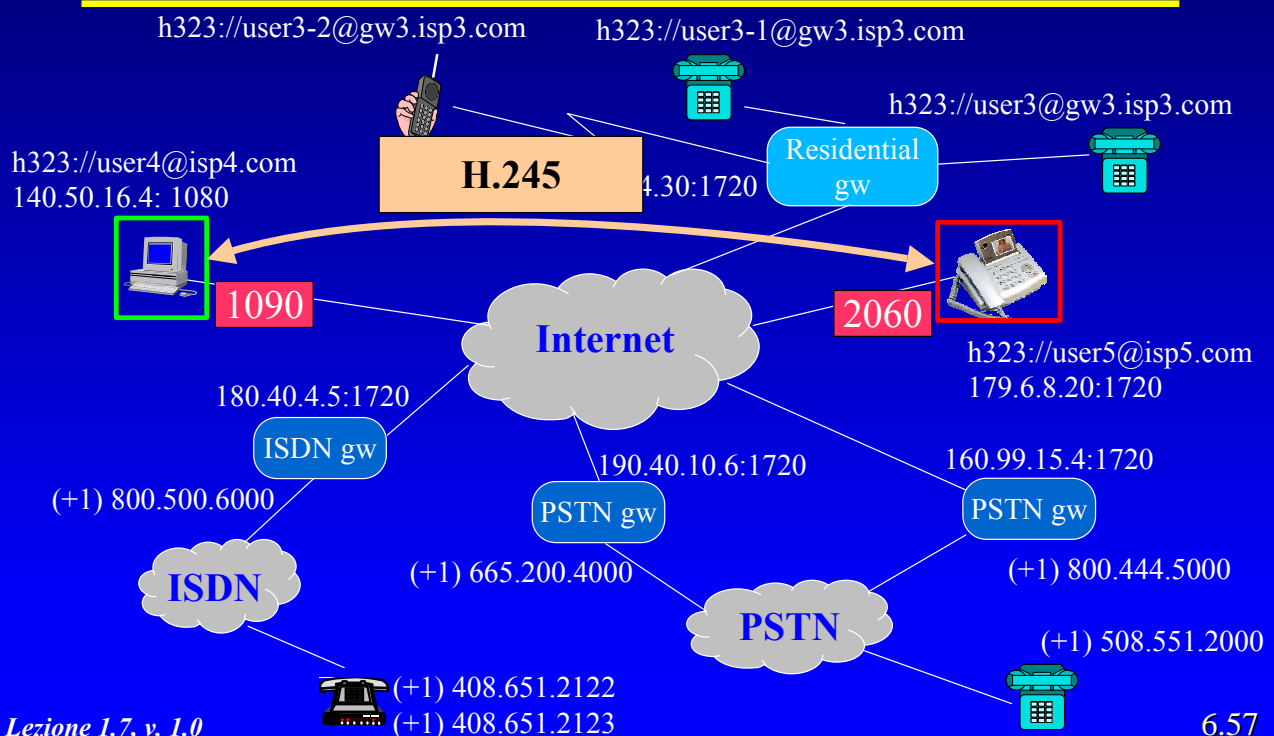
# Chiamate Punto-Punto H.225.0 Call Signaling



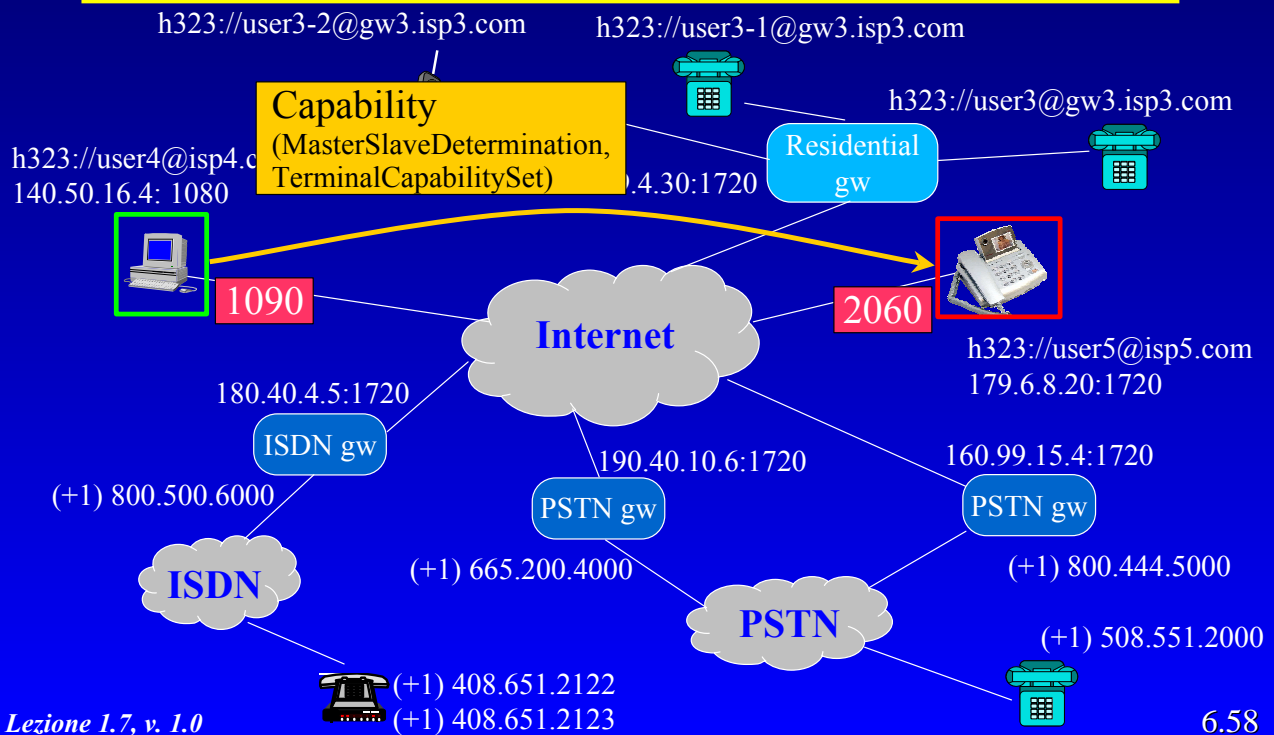
## Chiamate Punto-Punto

- Identificazione degli *endpoint*
  - risoluzione degli indirizzi
- **Instaurazione delle chiamate**
  - segnalazione: H.225.0 *Call Signalling*
  - **controllo: H.245**
  - RAS
  - Modelli di chiamate

## Chiamate Punto-Punto H.245



## Chiamate Punto-Punto H.245 - Capability



## Chiamate Punto-Punto H.245 - Capability

- MasterSlaveDetermination
  - determina quale endpoint agisce come master e quale come slave,
  - i due endpoint potrebbero richiedere contemporaneamente la stessa risorsa
    - il master risolve il conflitto;
- TerminalCapabilitySet
  - molte funzionalità H.323 sono opzionali
    - » ogni endpoint deve conoscere le funzionalità supportate dall'altro,
  - Audio/VideoCapability, elenco dei code supportati e di proprietà associate (risoluzione dei vari formati CIF, meccanismi di recupero di errore di H.263),
  - DataApplicationCapability, t140 e t38fax,
  - UserInputCapability, interfaccia utente,
  - multiplexCapability, pacchettizzazione, ridondanza e trasporto (QoS) dei media.

## TerminalCapabilitySet Media trasportati

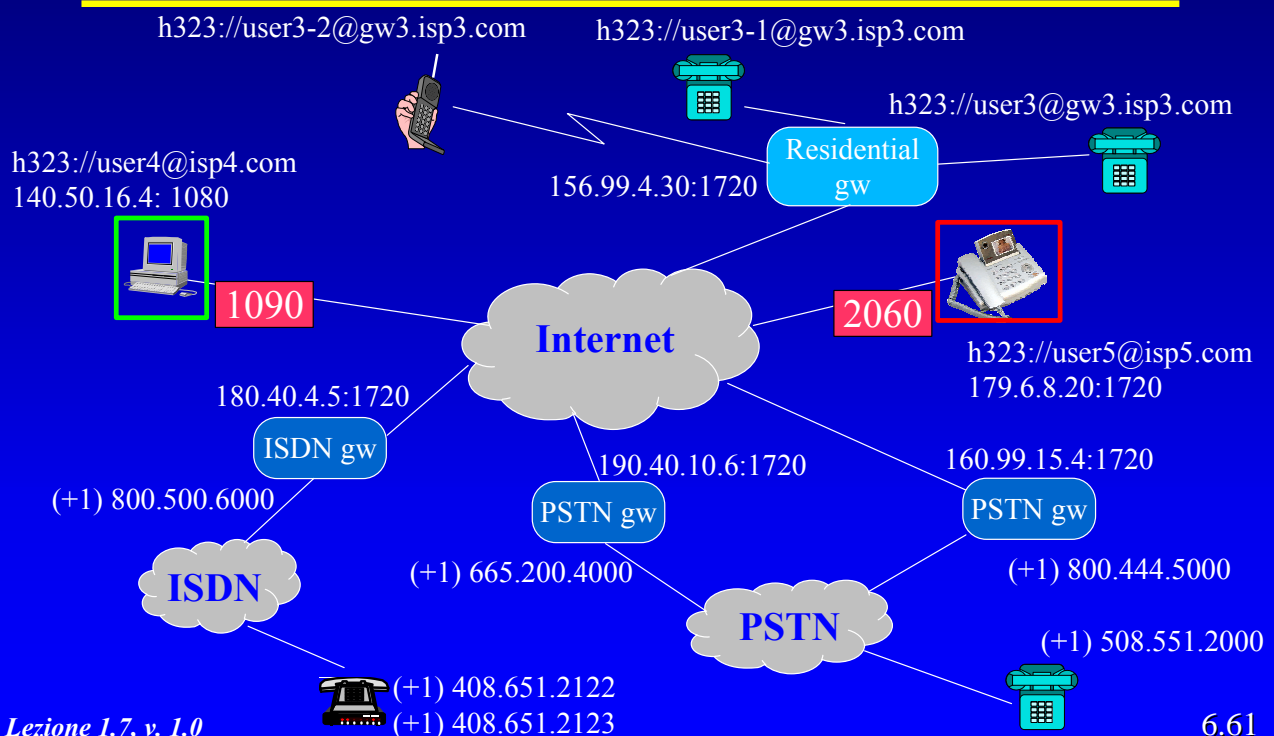
### Audio

- I terminali devono supportare lo standard di compressione voce G.711 a 56-64 Kbps.
- Consigliato il supporto del G.723.1 che opera a 5,3 - 6,3 Kbps.
- Opzionalmente si possono usare G722, G728 e G729.

### Video

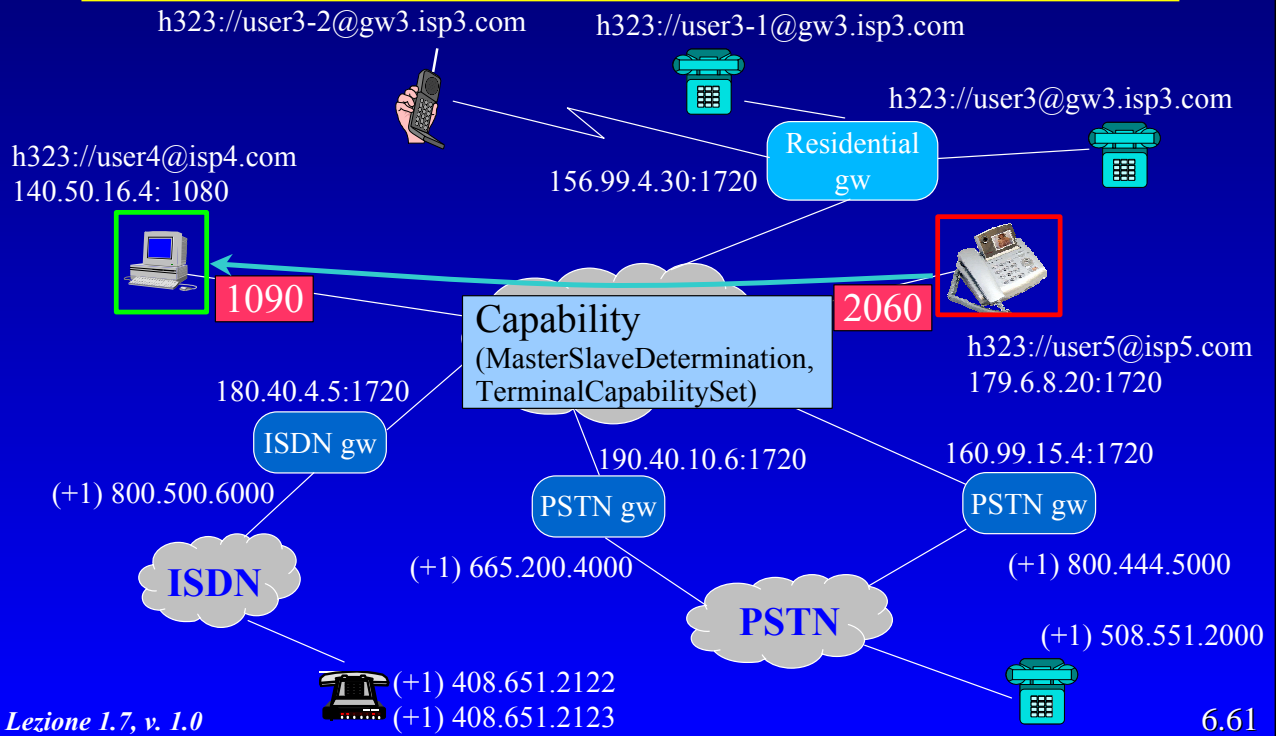
- Le capacità video sono opzionali.
- Se capace di trattare video, un terminale deve supportare formati QCIF H.261 (176 x 144 pixel).
- Opzionalmente può supportare H.263 e dimensioni CIF (352 x 288), 4CIF (704 x 576) e 16CIF (1408 x 1152).

## Chiamate Punto-Punto H.245 - ChannelManagement

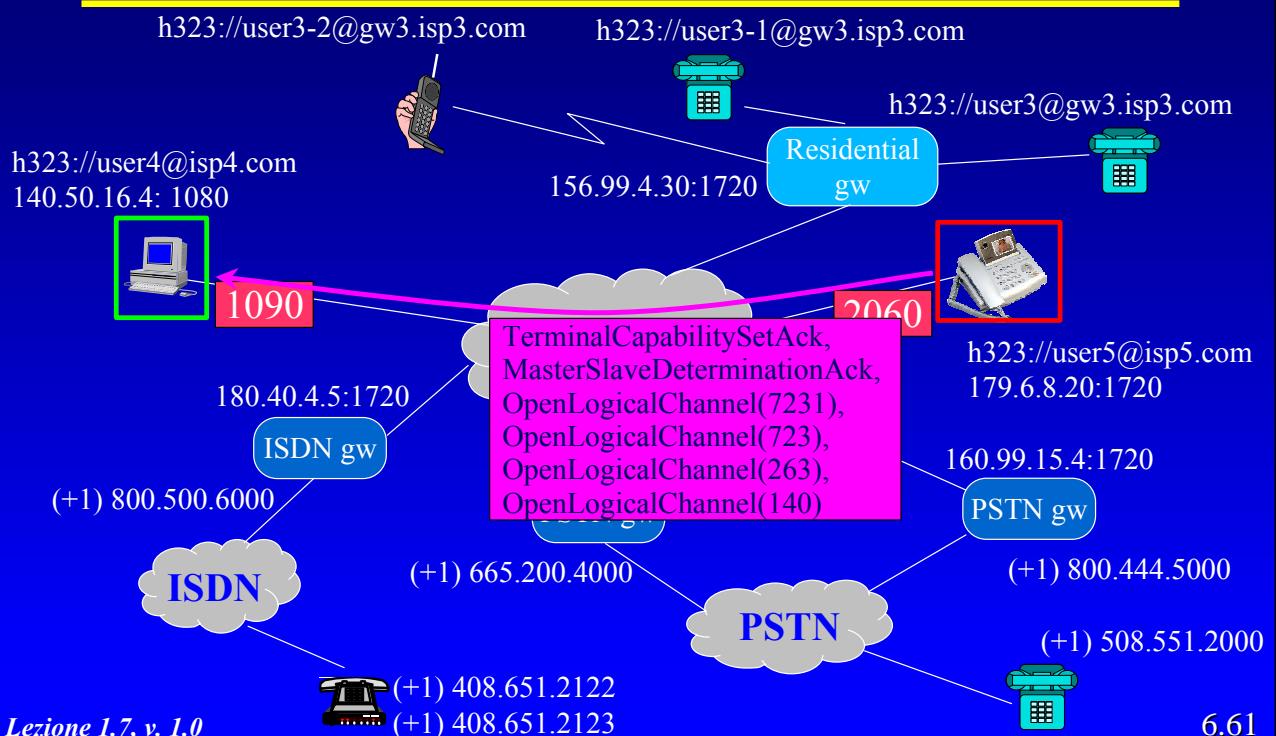




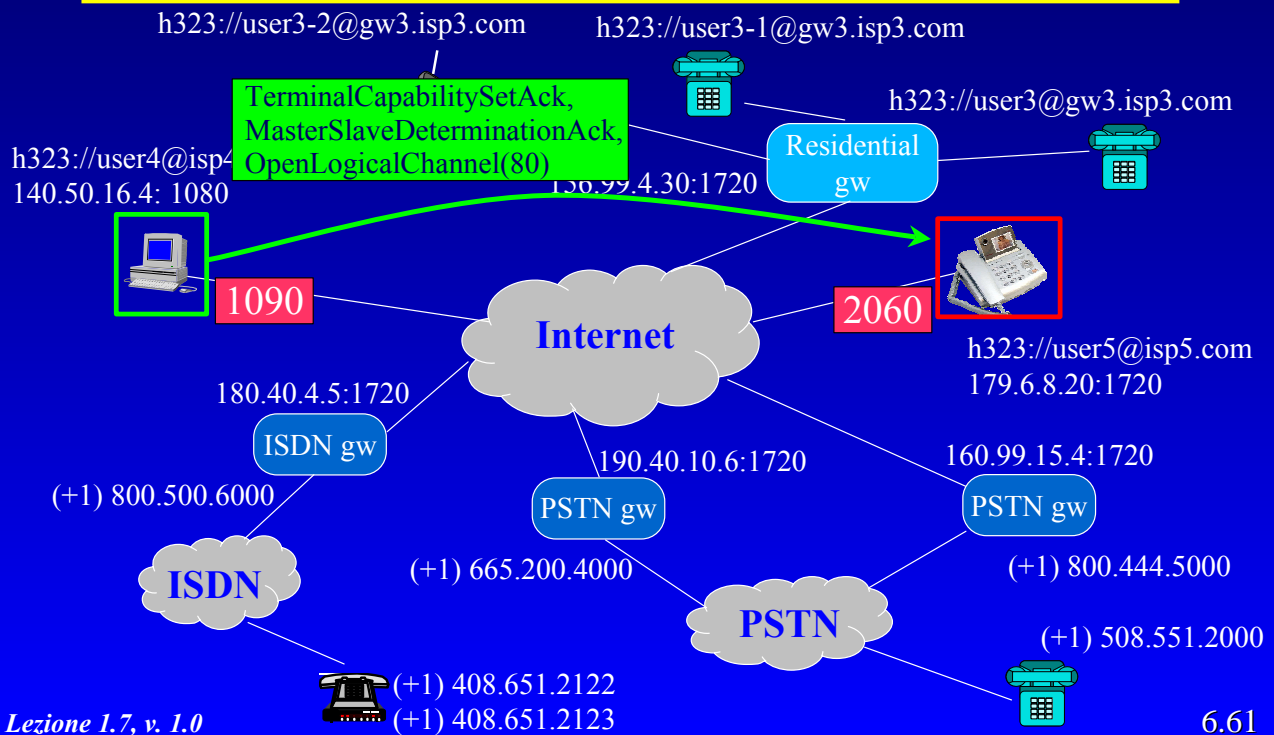
# Chiamate Punto-Punto H.245 - ChannelManagement



# Chiamate Punto-Punto H.245 - ChannelManagement



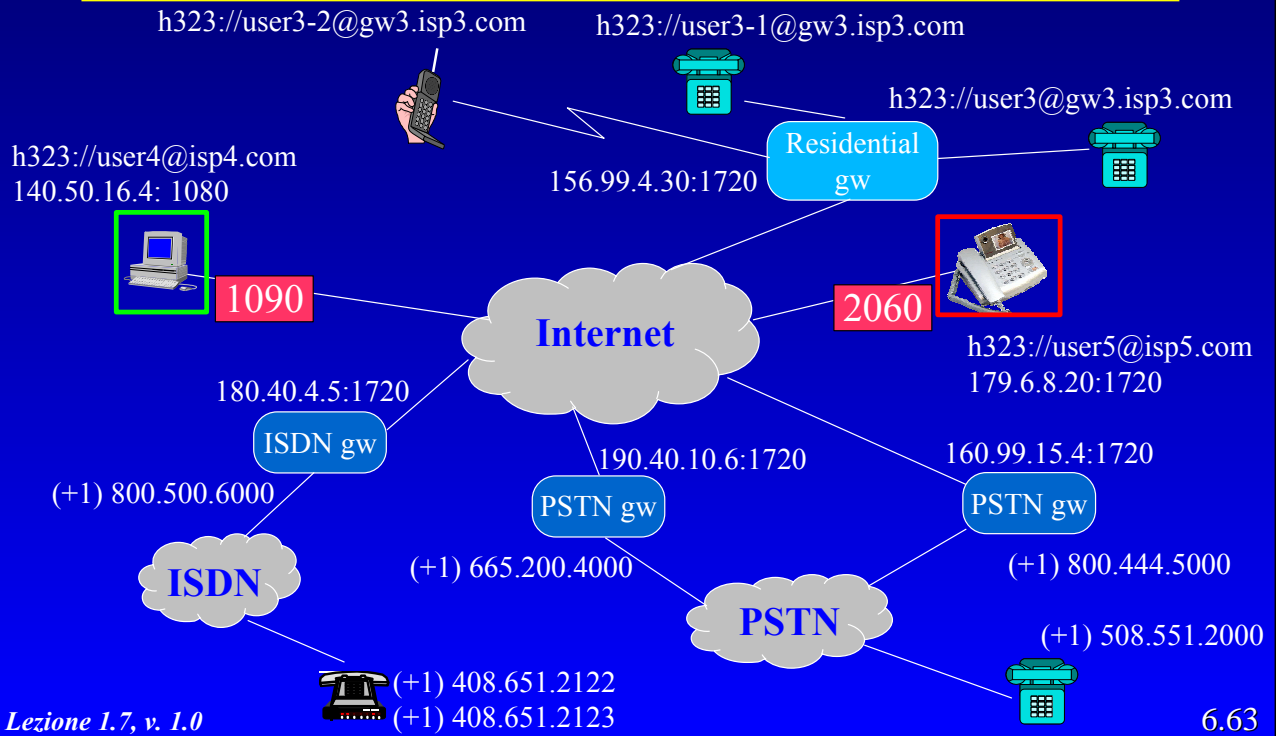
## Chiamate Punto-Punto H.245 - ChannelManagement



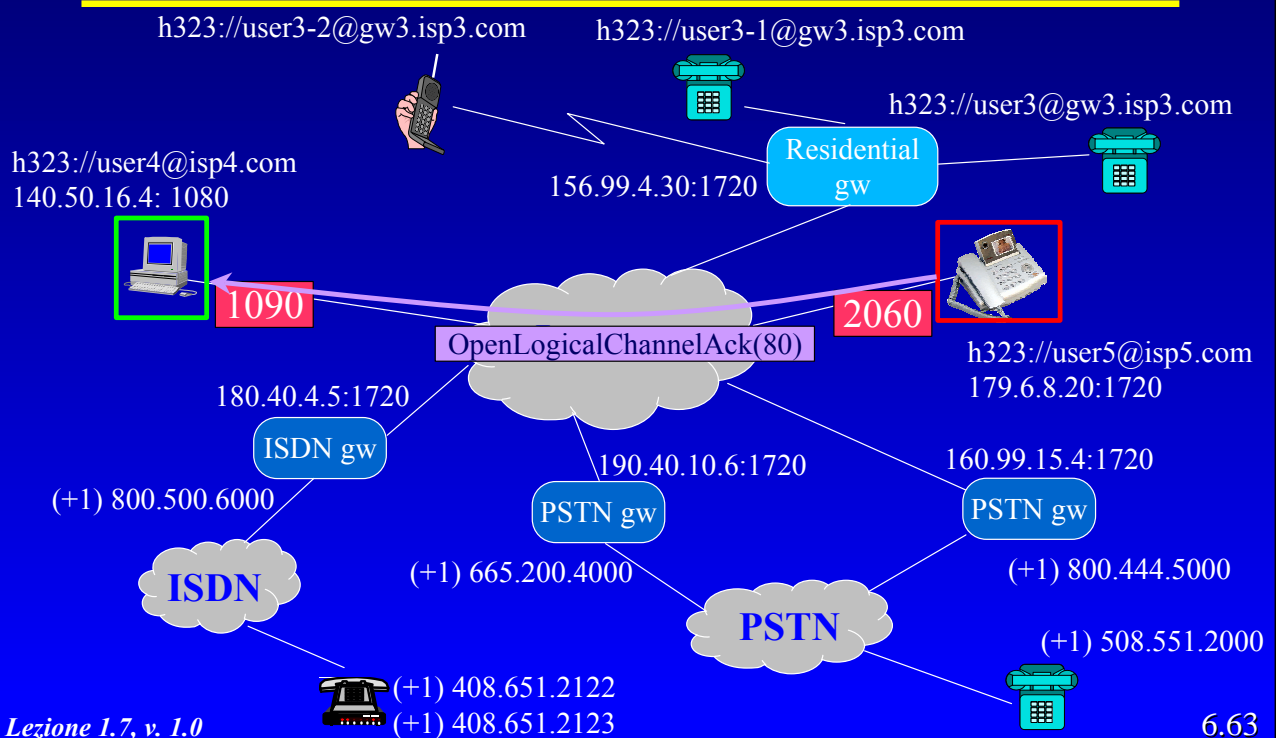
## Chiamate Punto-Punto H.245 - ChannelManagement

- OpenLogicaChannel, il trasmettitore specifica le caratteristiche del media
  - devono essere conformi alle capacità annunciate in precedenza,
- OpenLogicalChannelAck, il ricevitore informa il trasmettitore di essere pronto a ricevere il media,
- CloseLogicalChannel, per chiudere il canale aperto
  - in genere la trasmissione del media viene interrotta in precedenza,
- CloseLogicalChannelAck, indica che il canale può essere chiuso
  - il ricevitore rilascia le risorse prima di spedire questo messaggio,
  - il trasmettitore le rilascia alla ricezione di questo messaggio.

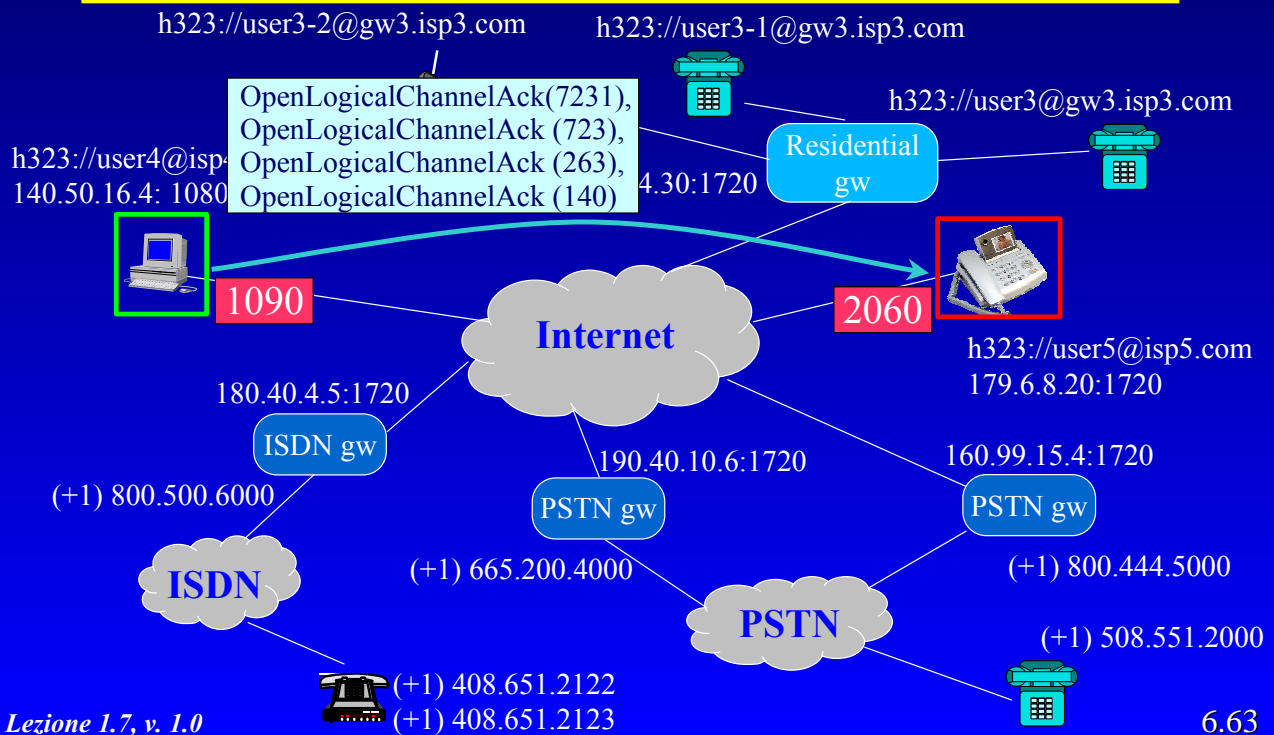
# Chiamate Punto-Punto H.245 - ChannelManagement



# Chiamate Punto-Punto H.245 - ChannelManagement



## Chiamate Punto-Punto H.245 - ChannelManagement



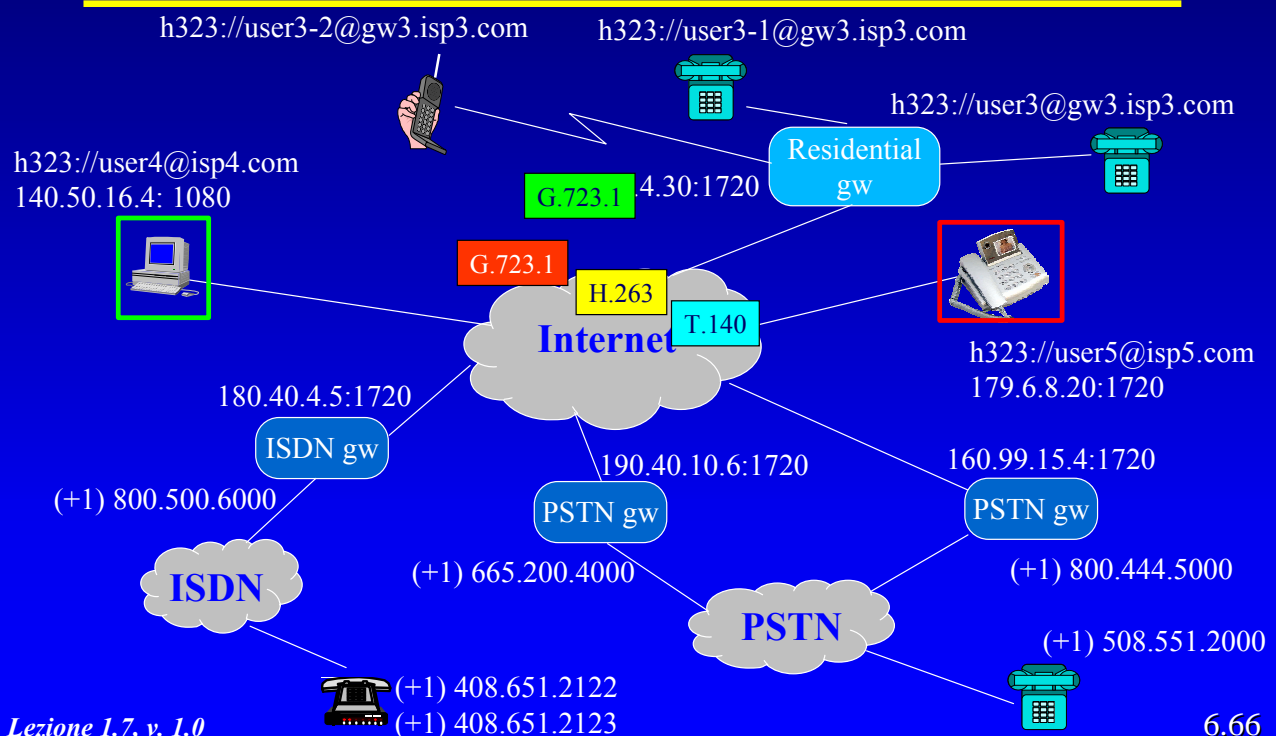
## Chiamate Punto-Punto H.245 - ChannelManagement

- Canale logico n. 80
  - G.723.1, Session ID 1
  - RTP: 140.50.16.4:1080 ⇒ 179.6.8.20:2060
  - RTCP: 140.50.16.4:1081 ⇒ 179.6.8.20:2061
- Canale logico n. 7231
  - G.723.1, Session ID 1
  - RTP: 179.6.8.20:2060 ⇒ 140.50.16.4:1080
  - RTCP: 179.6.8.20:2061 ⇒ 140.50.16.4:1081
- Canale logico n. 723
  - G.723.1, codifica ridondante, Session ID 1
  - RTP: 179.6.8.20:2060 ⇒ 140.50.16.4:1080
  - RTCP: 179.6.8.20:2061 ⇒ 140.50.16.4:1081

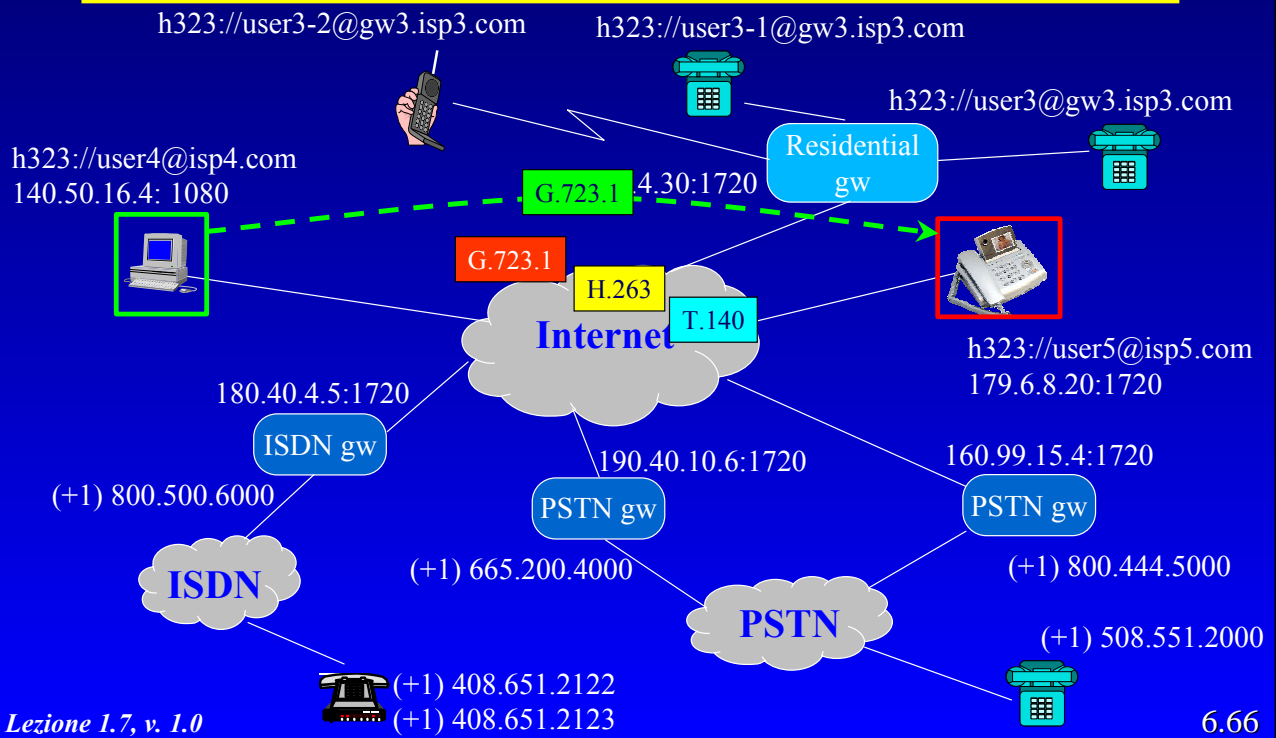
## Chiamate Punto-Punto H.245 - ChannelManagement

- Canale logico n. 263
  - H.263, Session ID 2
  - RTP: 179.6.8.20:4010 ⇒ 140.50.16.4:1044
  - RTCP: 179.6.8.20:4011 ⇒ 140.50.16.4:1045
- Canale logico n. 140
  - T.140, Session ID 3
  - RTP: 179.6.8.20:4020 ⇒ 140.50.16.4:4010
  - RTCP: 179.6.8.20:4021 ⇒ 140.50.16.4:4011

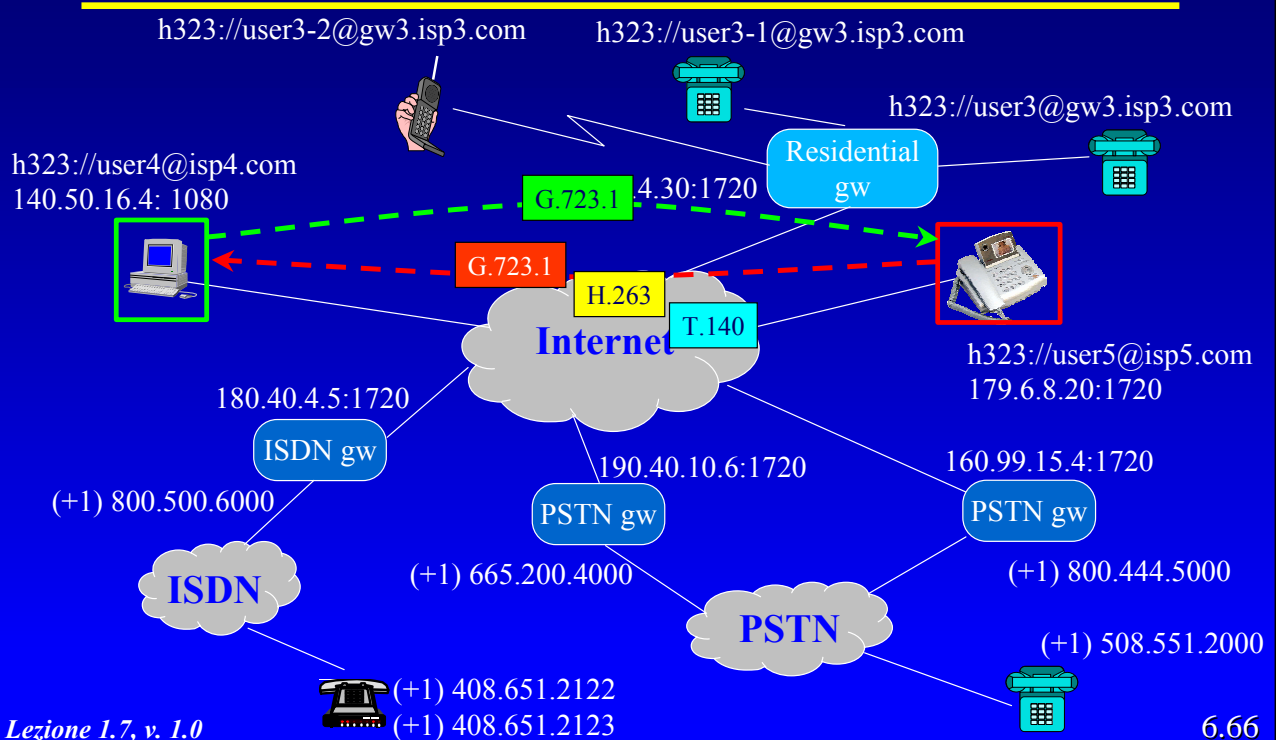
## Chiamate Punto-Punto H.245 - ChannelManagement



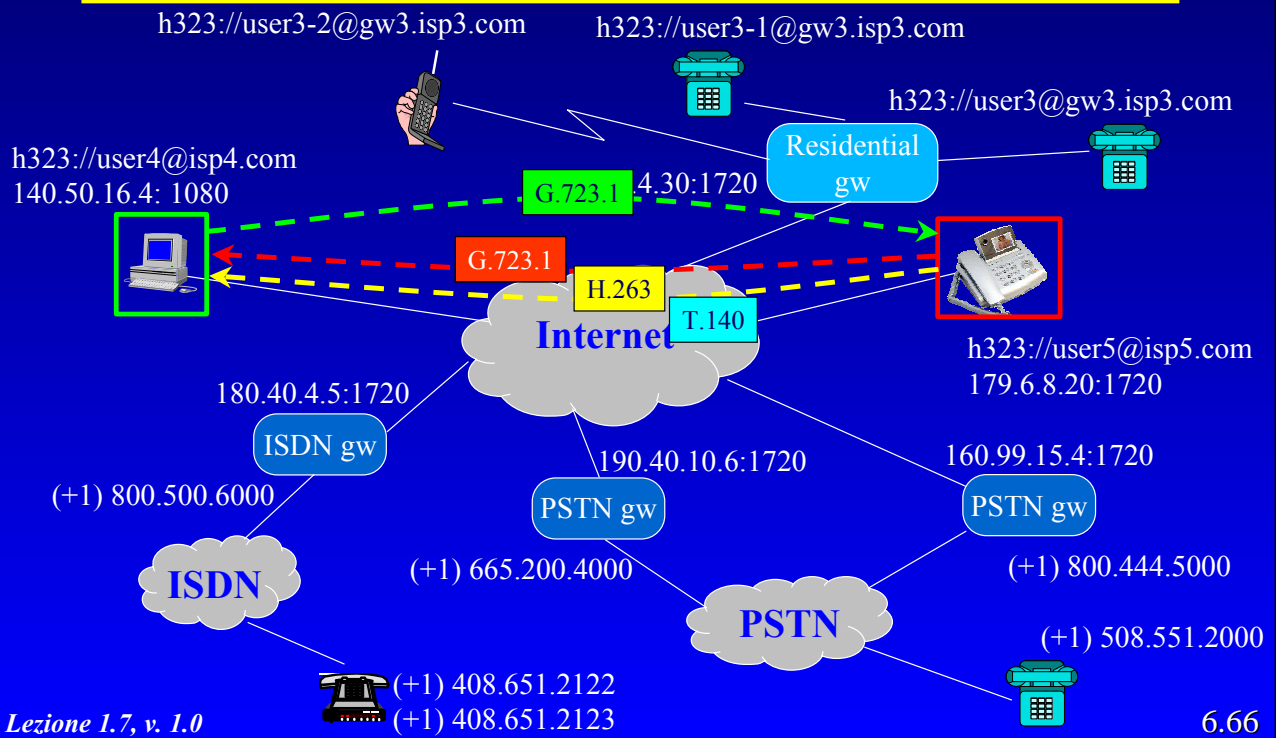
# Chiamate Punto-Punto H.245 - ChannelManagement



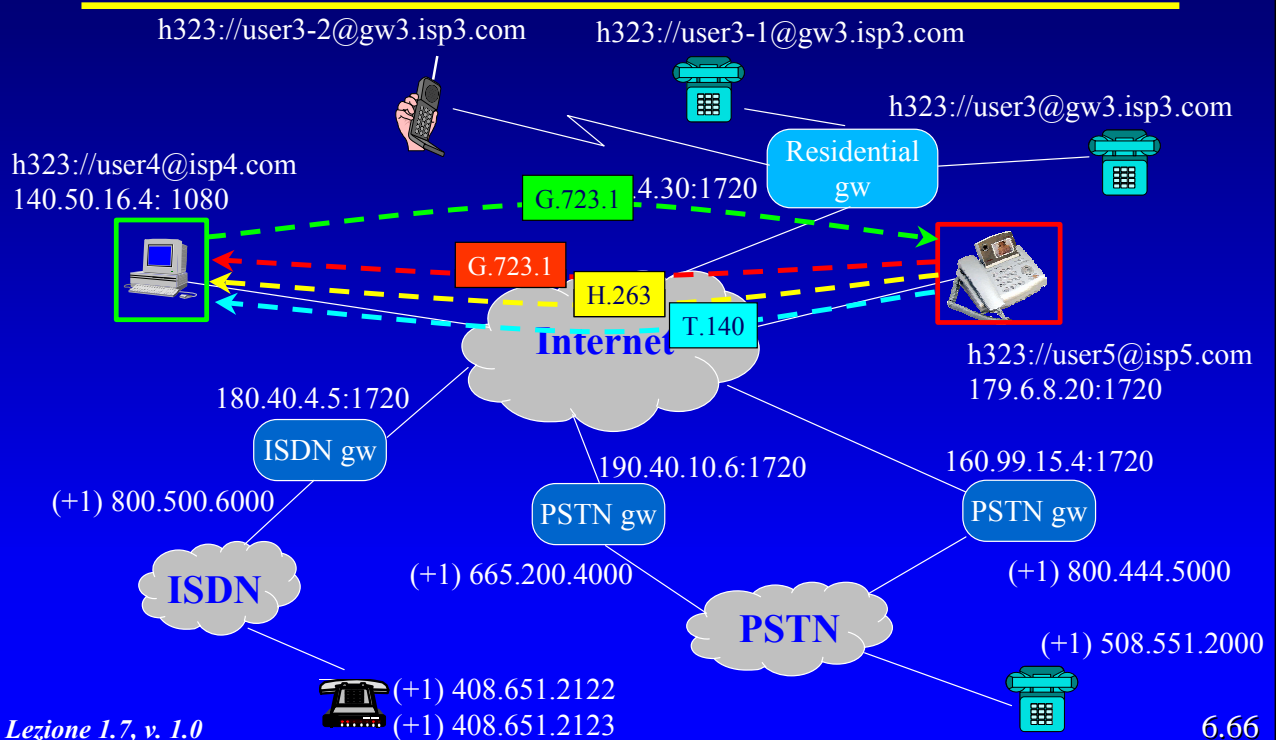
# Chiamate Punto-Punto H.245 - ChannelManagement



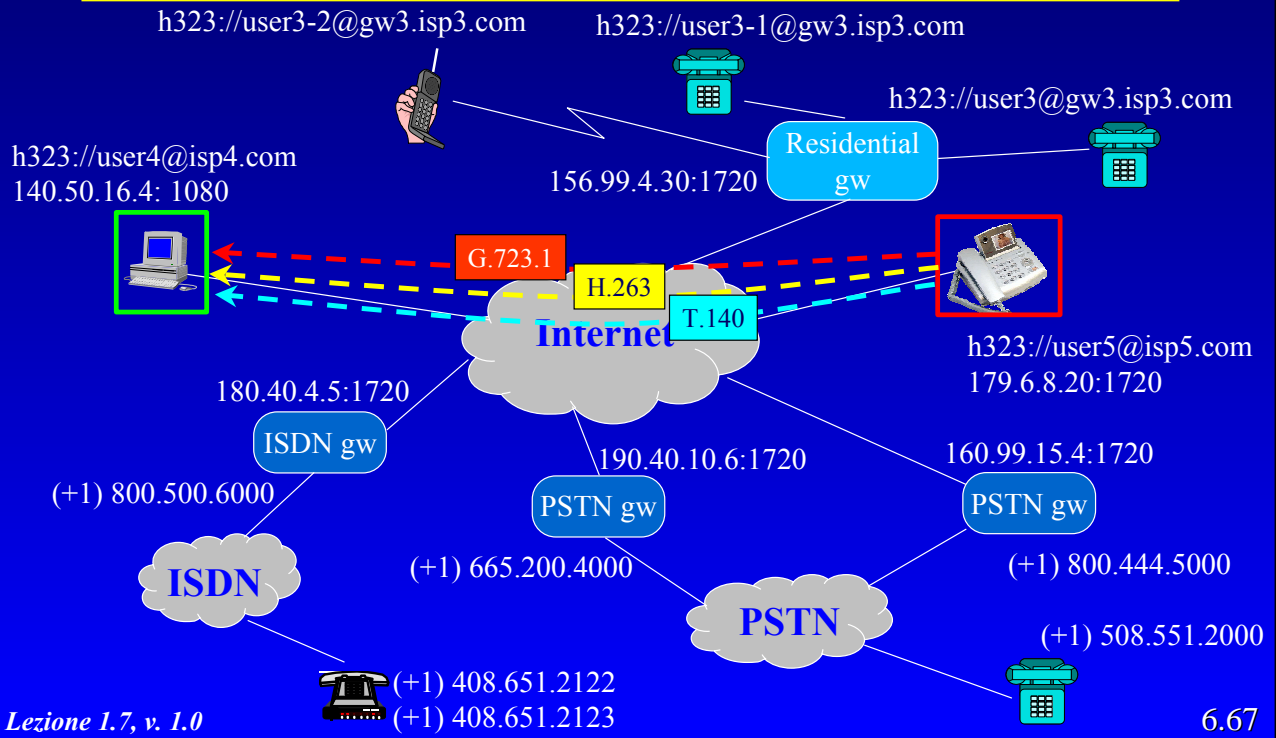
# Chiamate Punto-Punto H.245 - ChannelManagement



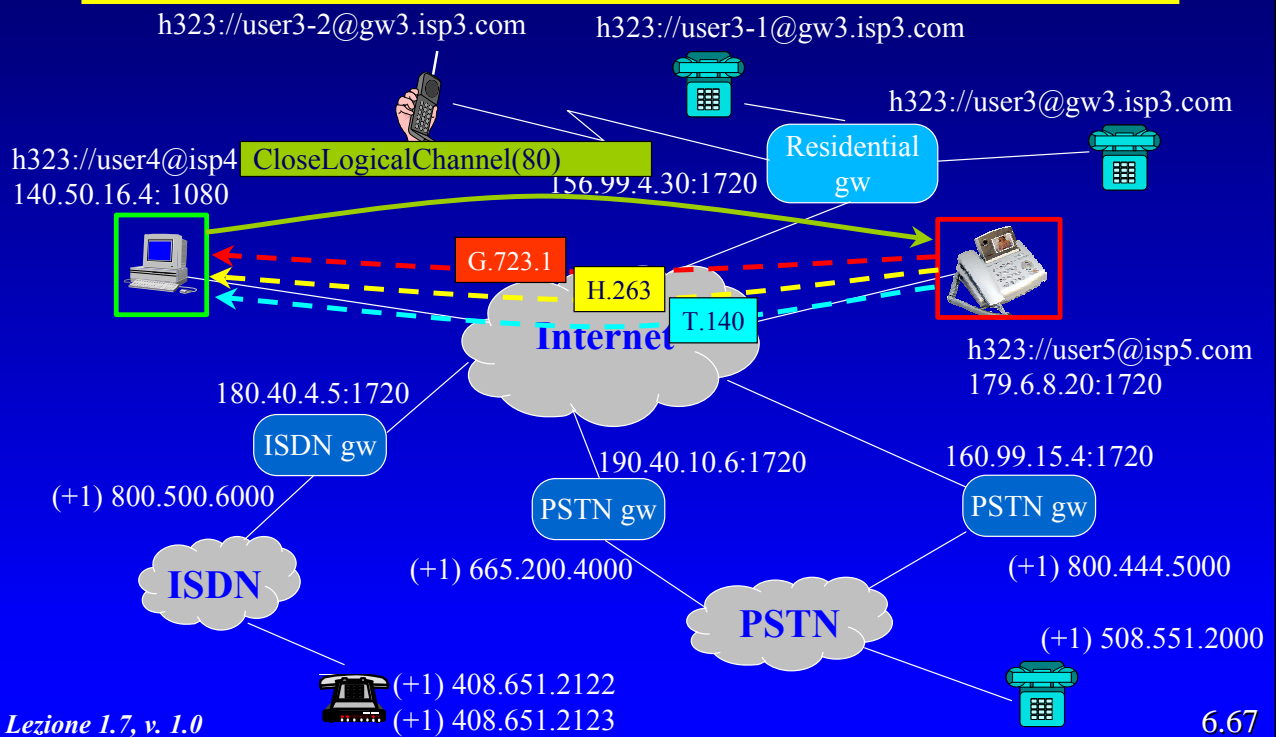
# Chiamate Punto-Punto H.245 - ChannelManagement



# Chiamate Punto-Punto H.245 - ChannelManagement

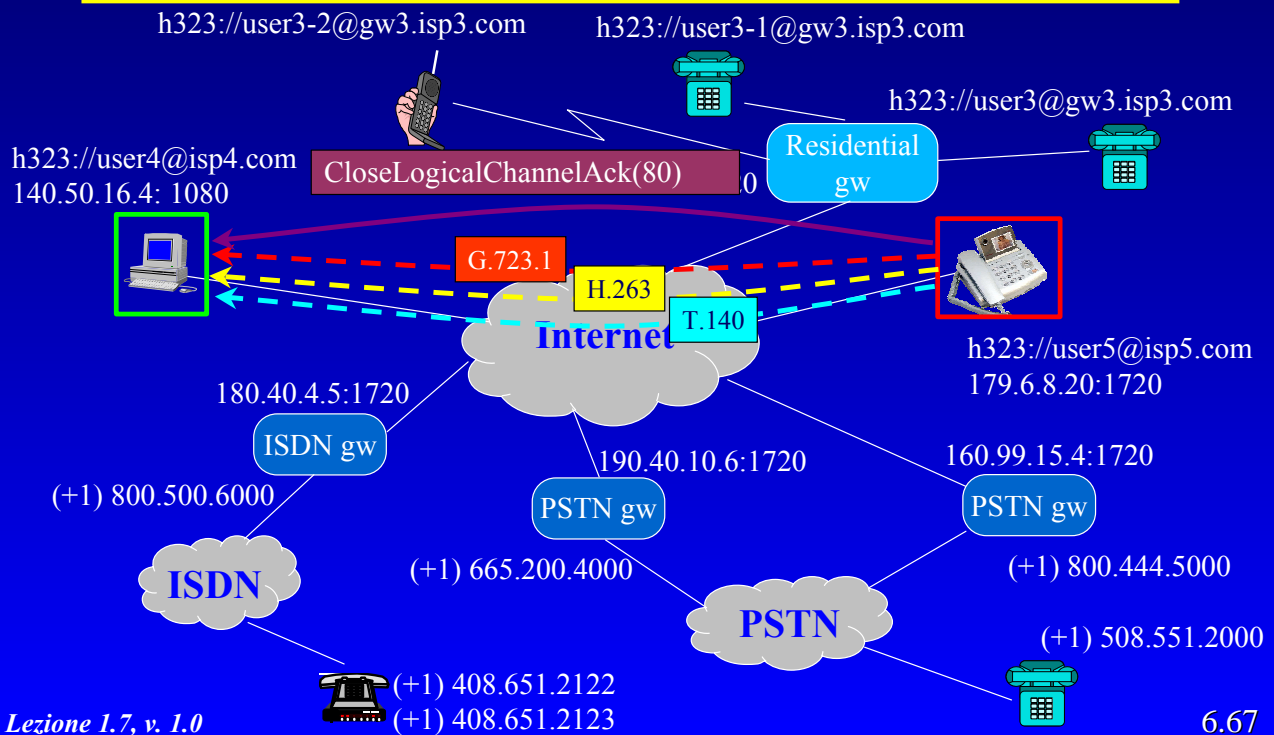


# Chiamate Punto-Punto H.245 - ChannelManagement





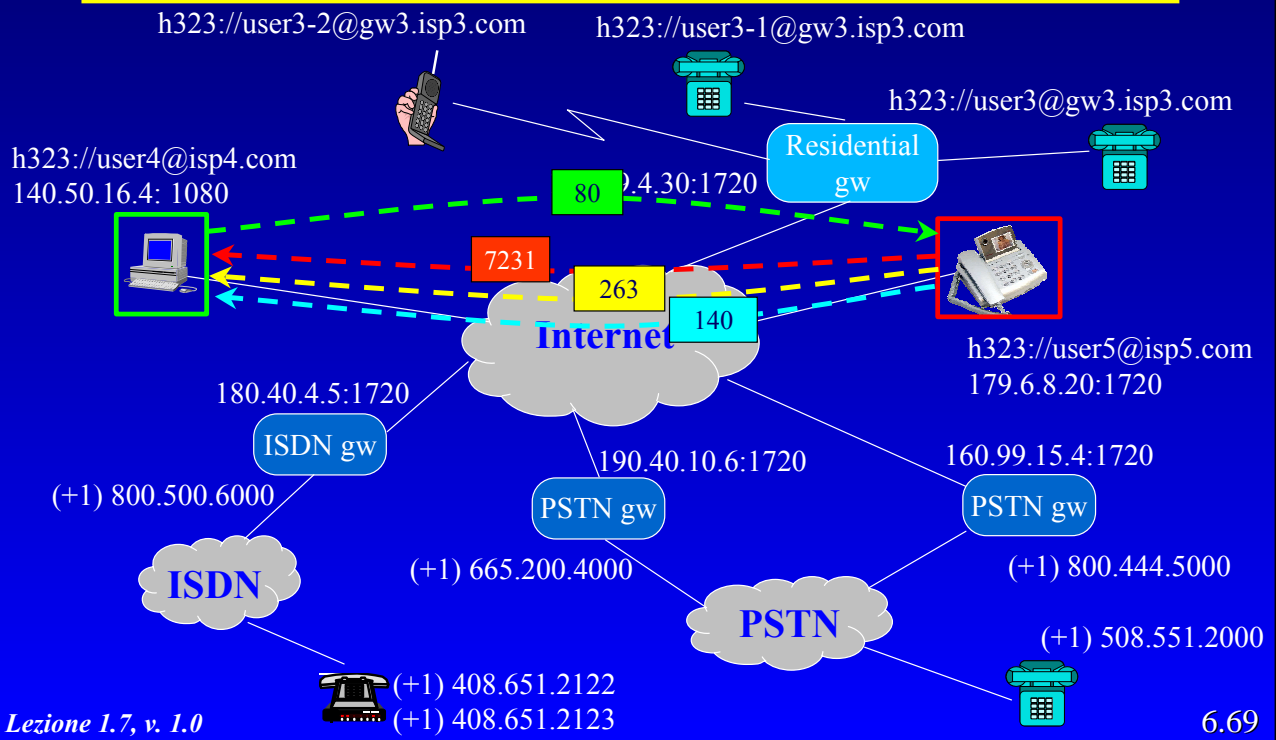
## Chiamate Punto-Punto H.245 - ChannelManagement



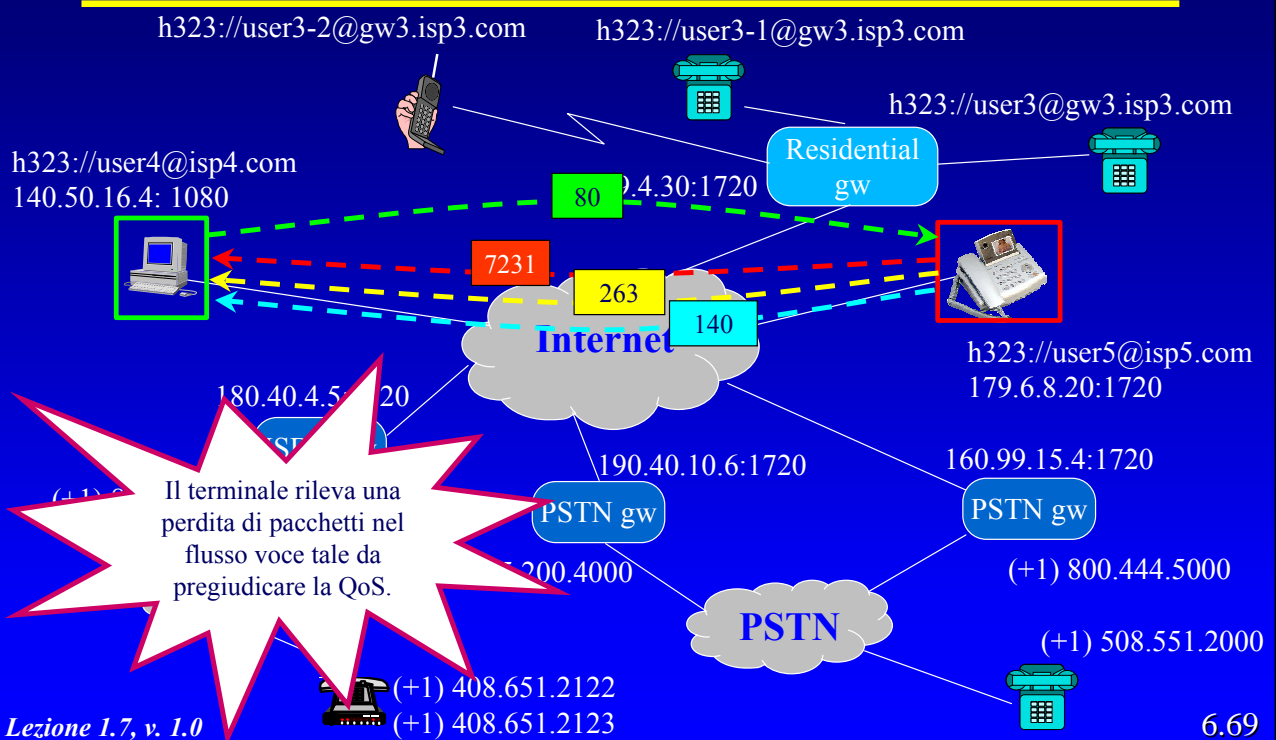
## Chiamate Punto-Punto H.245 - ChannelOperation

- **FlowControlCommand**, per modificare il tasso trasmissivo del media
  - utile per adattare la QoS alle diverse condizioni della rete
    - » le condizioni della rete possono essere misurate dal *tasso di perdita dei pacchetti*, dal *jitter*, dal *ritardo*.
- **UserInputIndication**, trasmette l'input generato dall'utente attraverso una qualche interfaccia
  - alfanumerica, per es. la tastiera,
  - segnale, come un tastierino numerico DTMF;
- **MiscellaneousCommand**, consiste in una ampia varietà di messaggi
  - ad es. per controllare un flusso video.

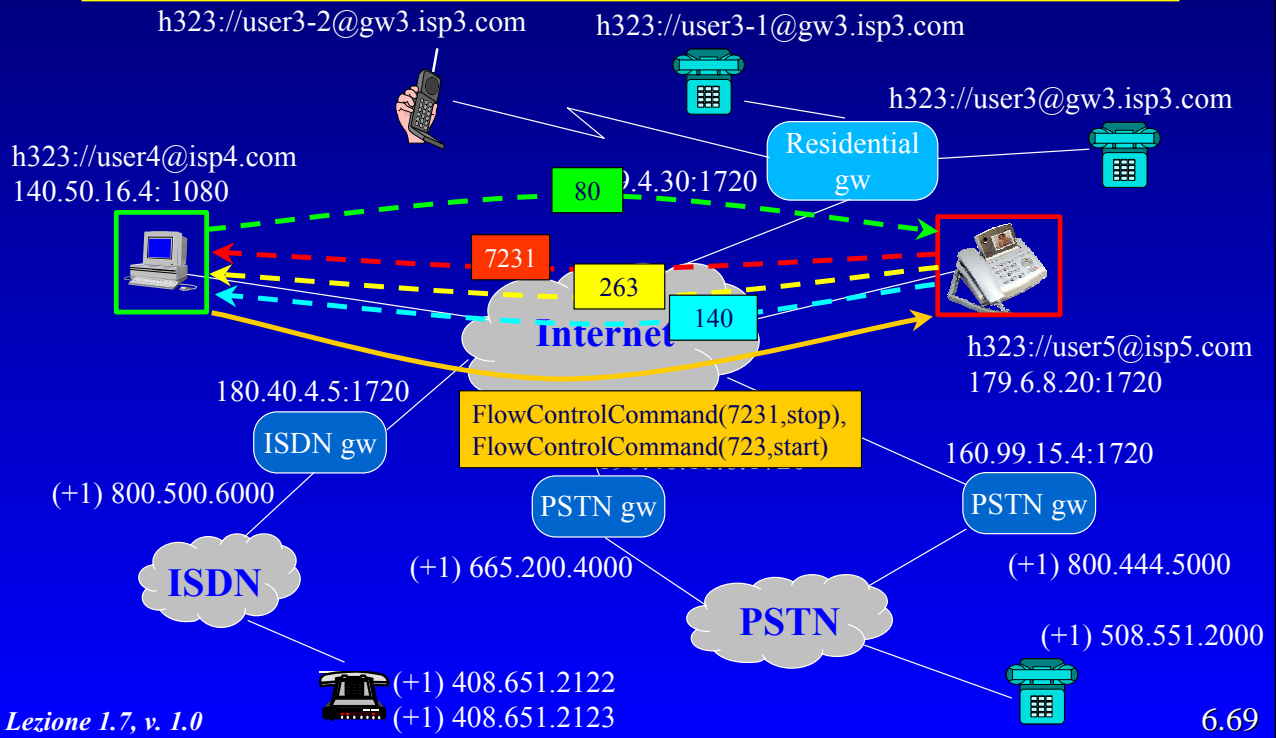
# Chiamate Punto-Punto H.245 - ChannelOperation



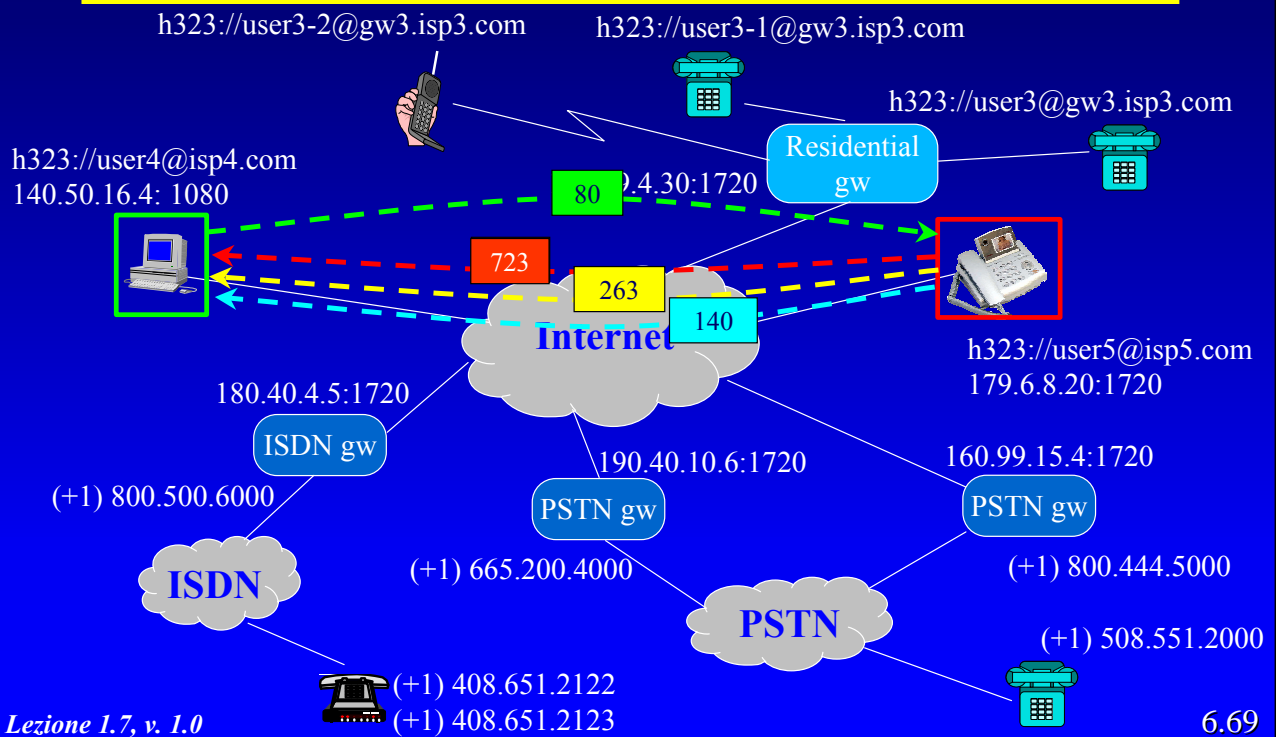
# Chiamate Punto-Punto H.245 - ChannelOperation



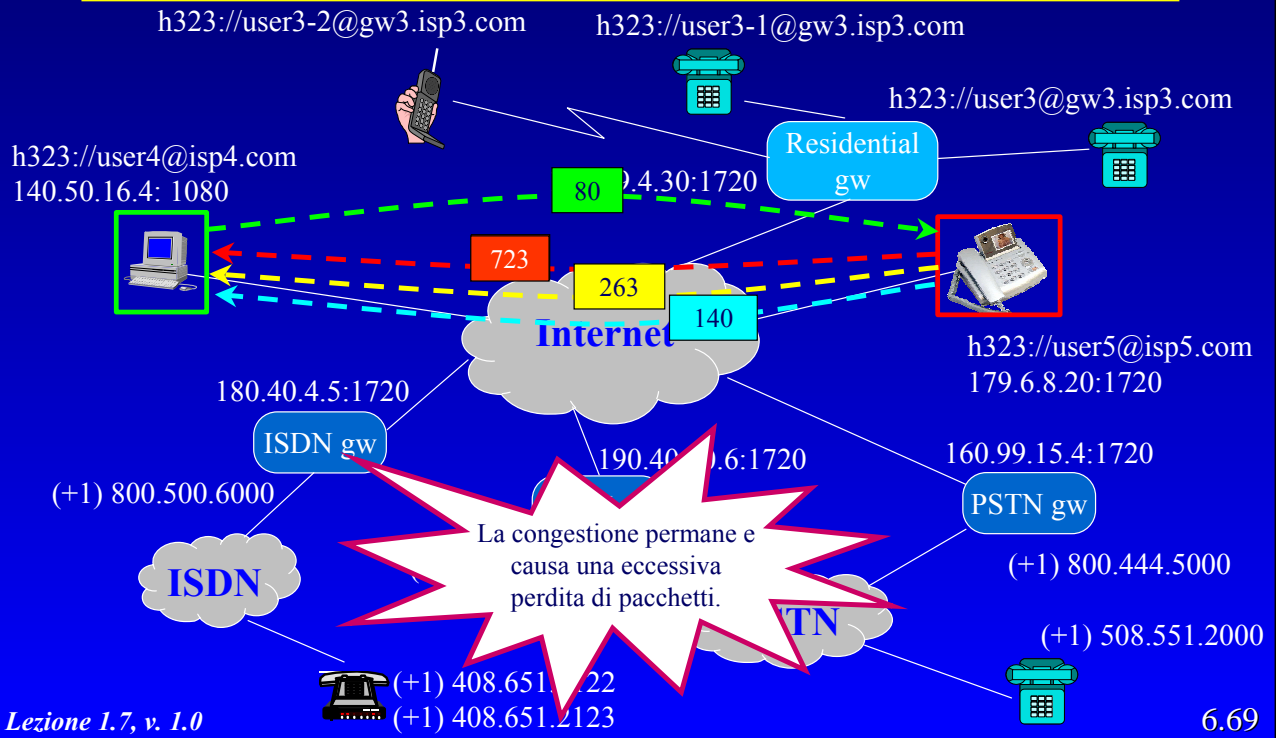
# Chiamate Punto-Punto H.245 - ChannelOperation



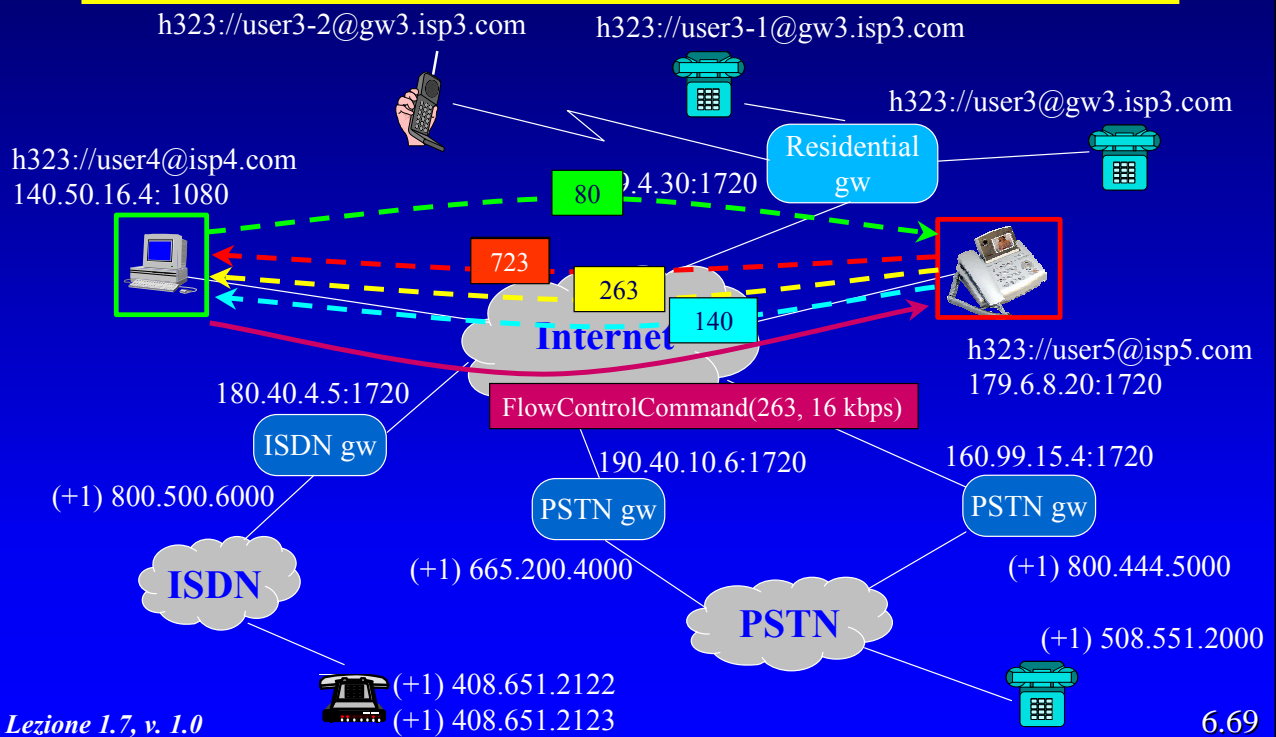
# Chiamate Punto-Punto H.245 - ChannelOperation



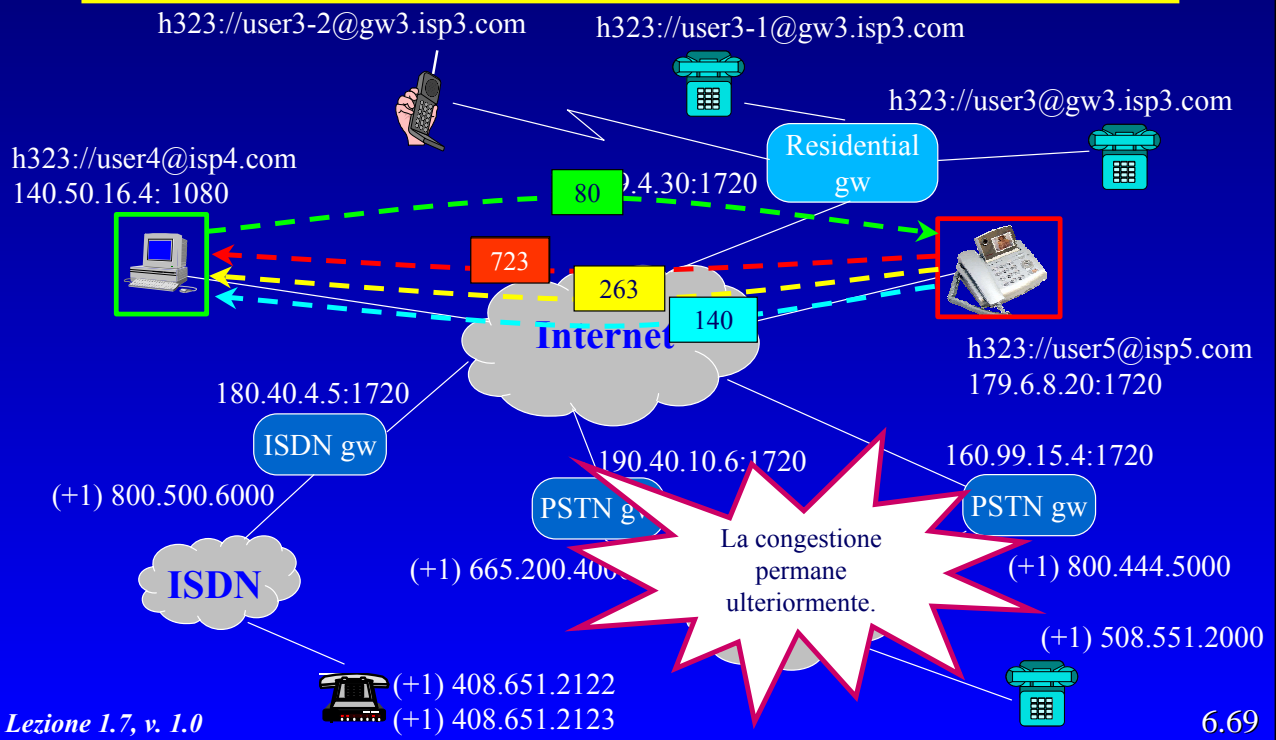
# Chiamate Punto-Punto H.245 - ChannelOperation



# Chiamate Punto-Punto H.245 - ChannelOperation

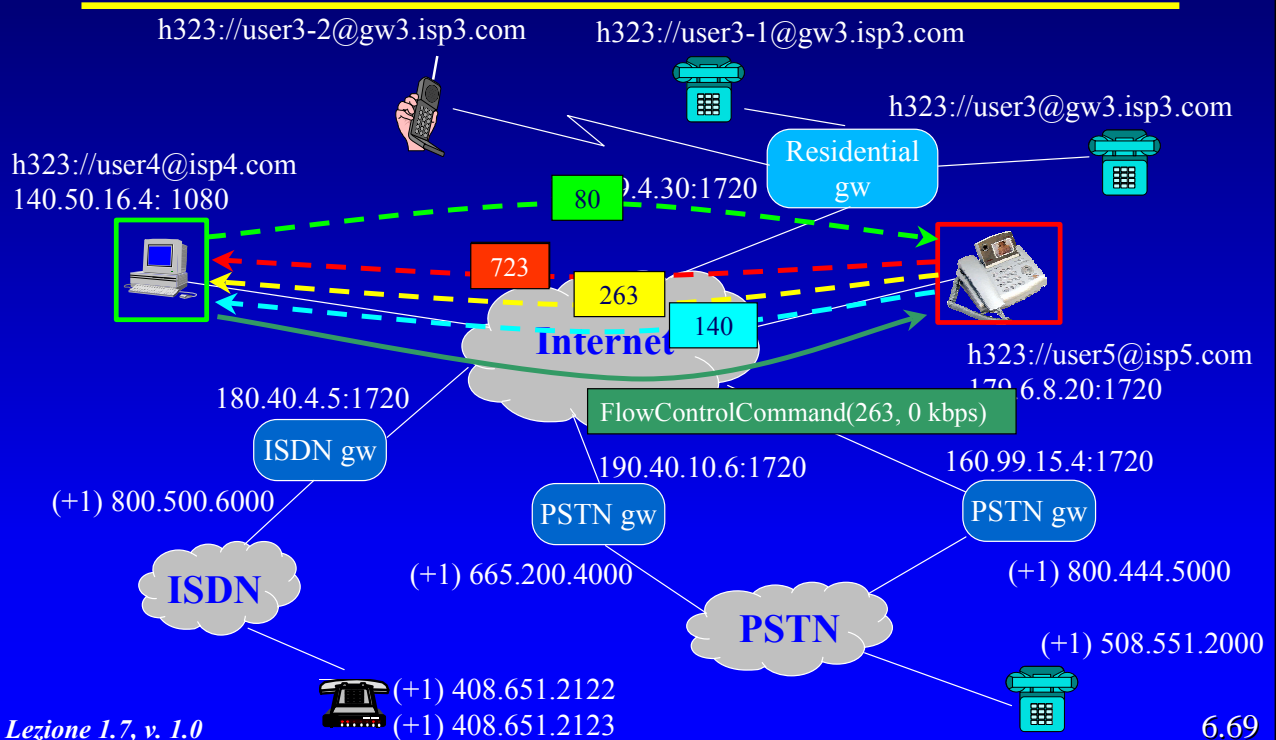


# Chiamate Punto-Punto H.245 - ChannelOperation



Lezione 1.7, v. 1.0

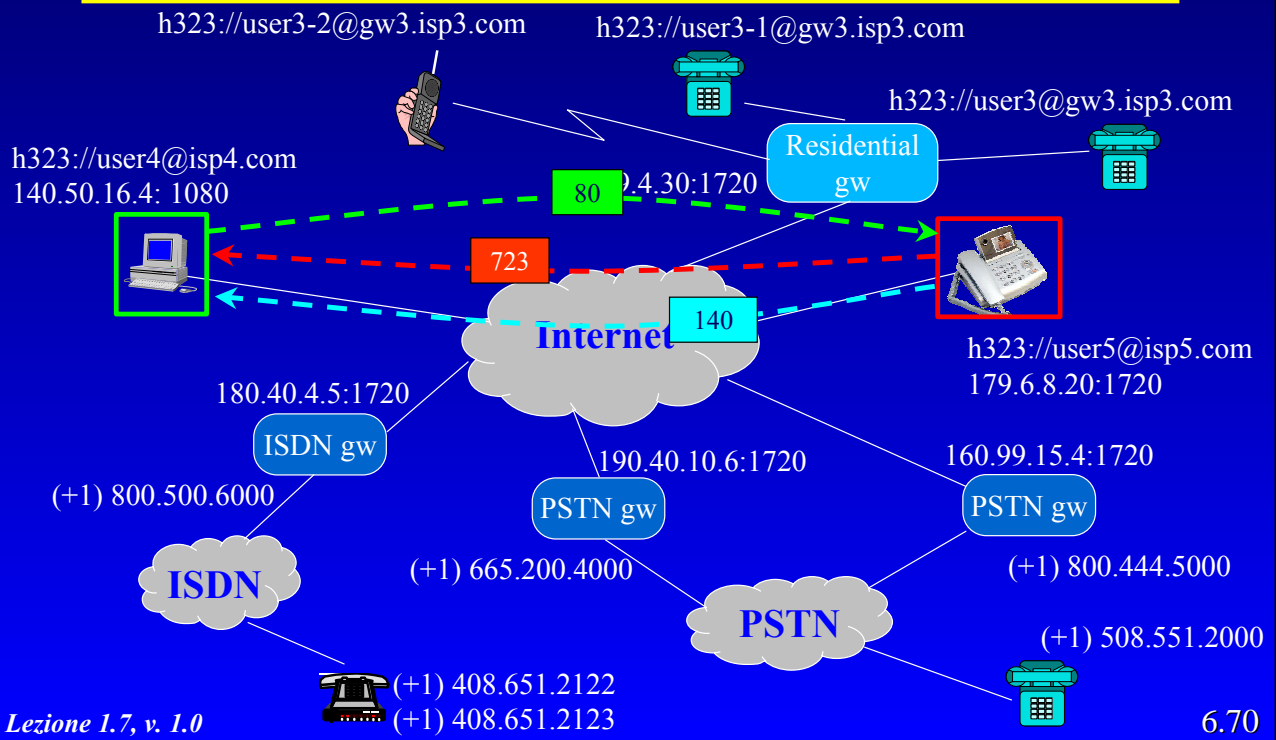
# Chiamate Punto-Punto H.245 - ChannelOperation



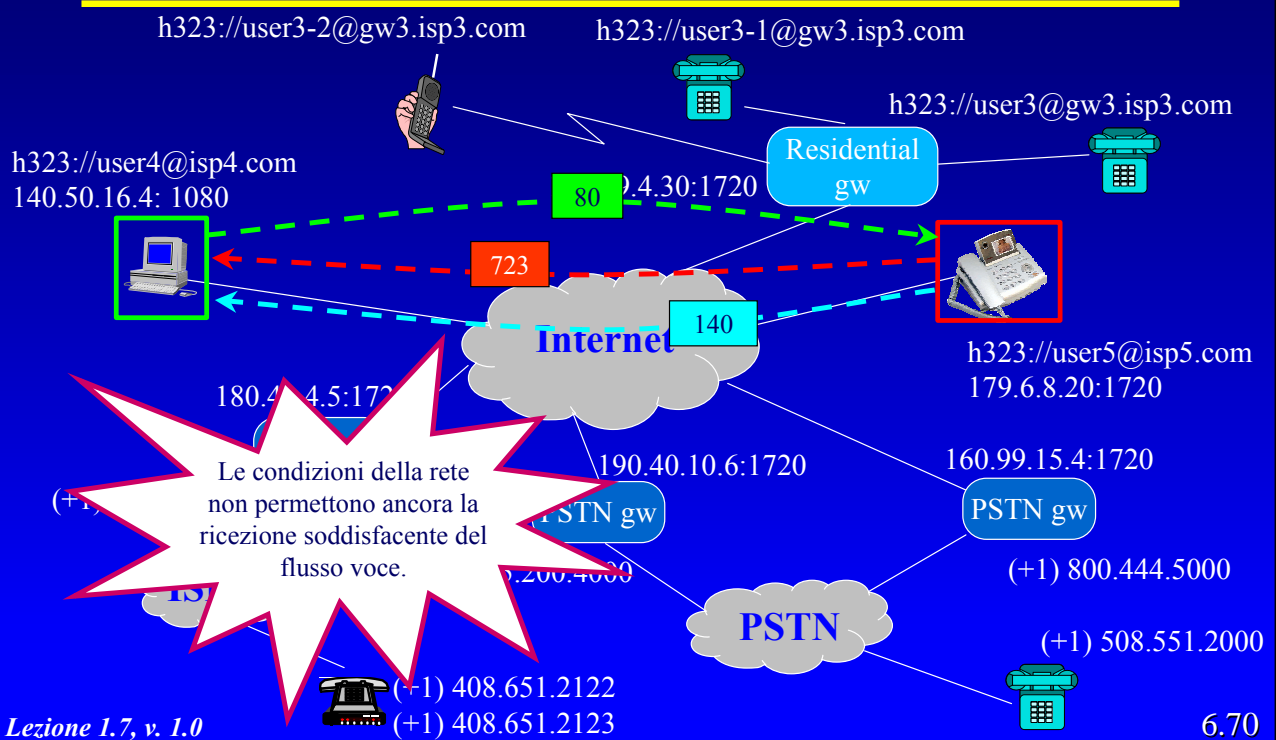
Lezione 1.7, v. 1.0

6.69

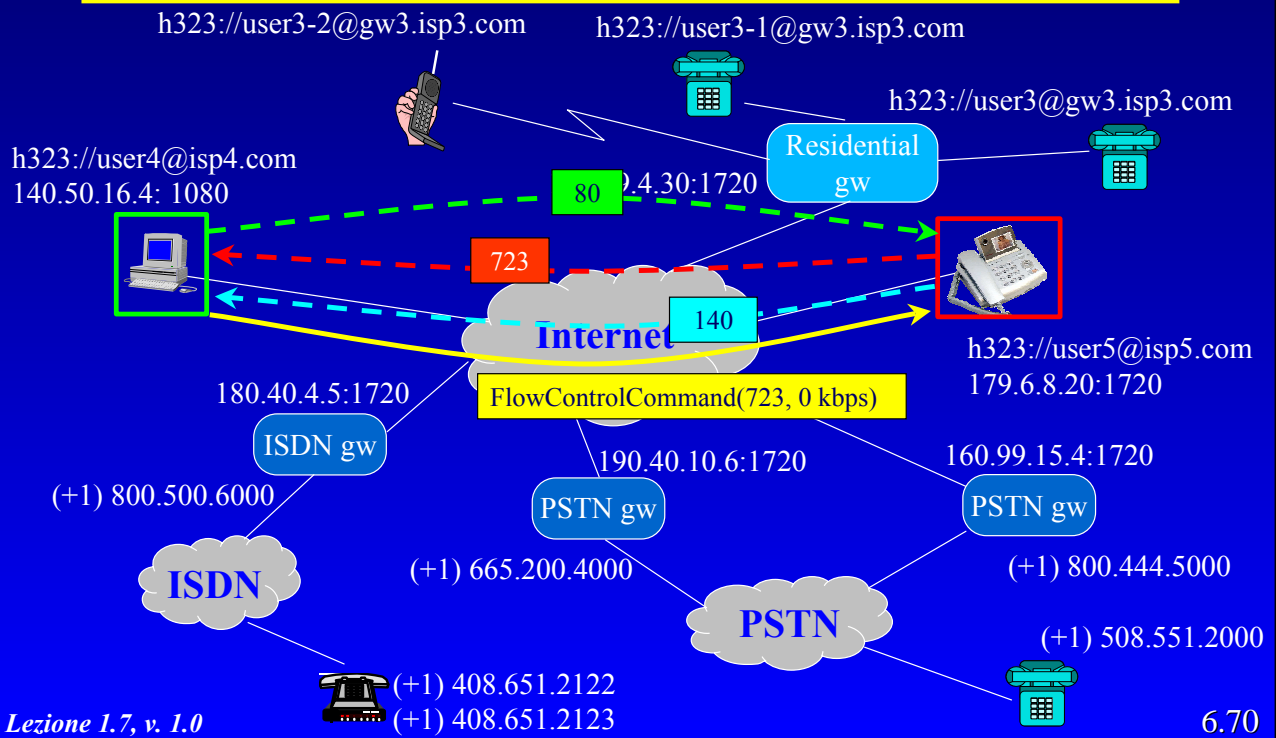
# Chiamate Punto-Punto H.245 - ChannelOperation



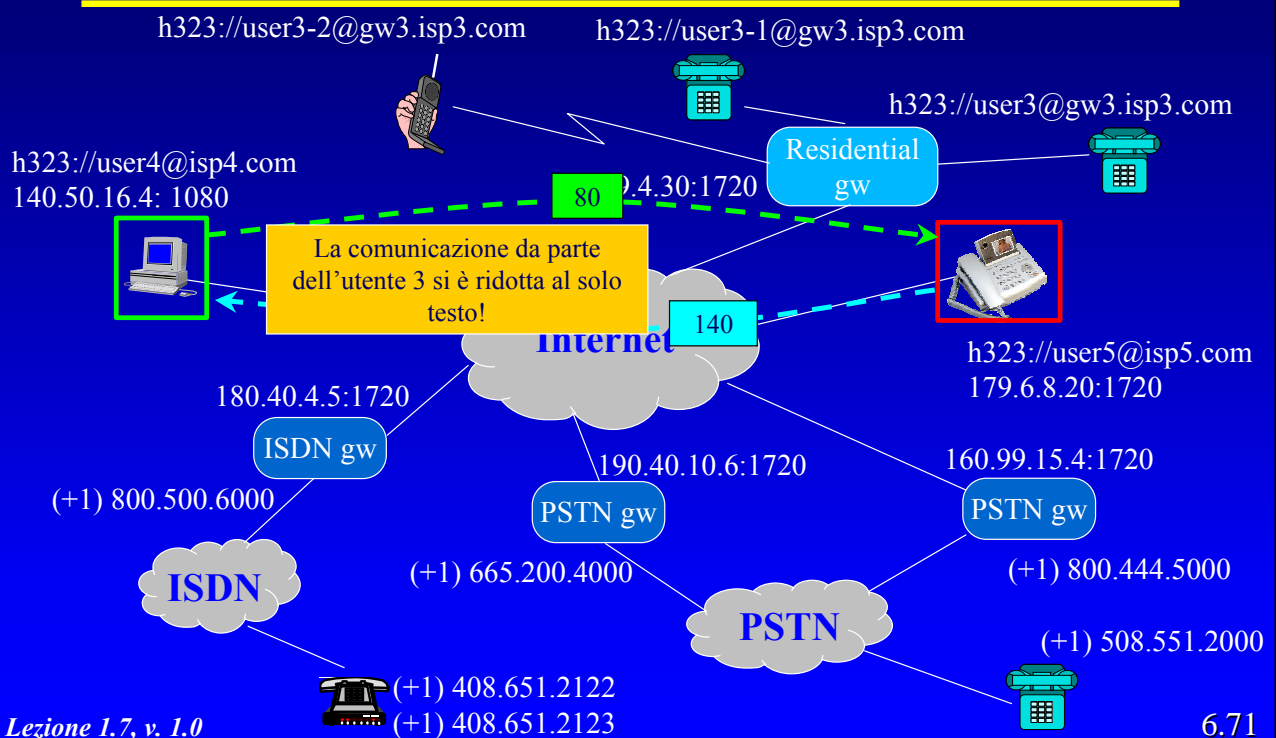
# Chiamate Punto-Punto H.245 - ChannelOperation



# Chiamate Punto-Punto H.245 - ChannelOperation



# Chiamate Punto-Punto H.245 - ChannelOperation



## Chiamate Punto-Punto

### H.245v2

---

- La segnalazione illustrata è tipica di H.323v1.
  - La versione 2 introduce ulteriori elementi
    - H.245 Tunneling
      - » la versione 1 richiede 2 porte TCP,
      - » la versione 2 prevede la possibilità di incapsulare H.245 dentro i messaggi H.225.0, in modo da richiedere una sola porta TCP
        - aumenta la scalabilità,
        - è necessario de-multiplexare i due flussi;
    - Fast Connect
      - » i canali logici possono essere aperti prima del completamento della fase di connessione H.225.0,
      - » i messaggi H.245 sono incapsulati nei messaggi H.225.0 *Setup* e *Alerting*
- l'instaurazione della connessione avviene più rapidamente.

## Chiamate Punto-Punto

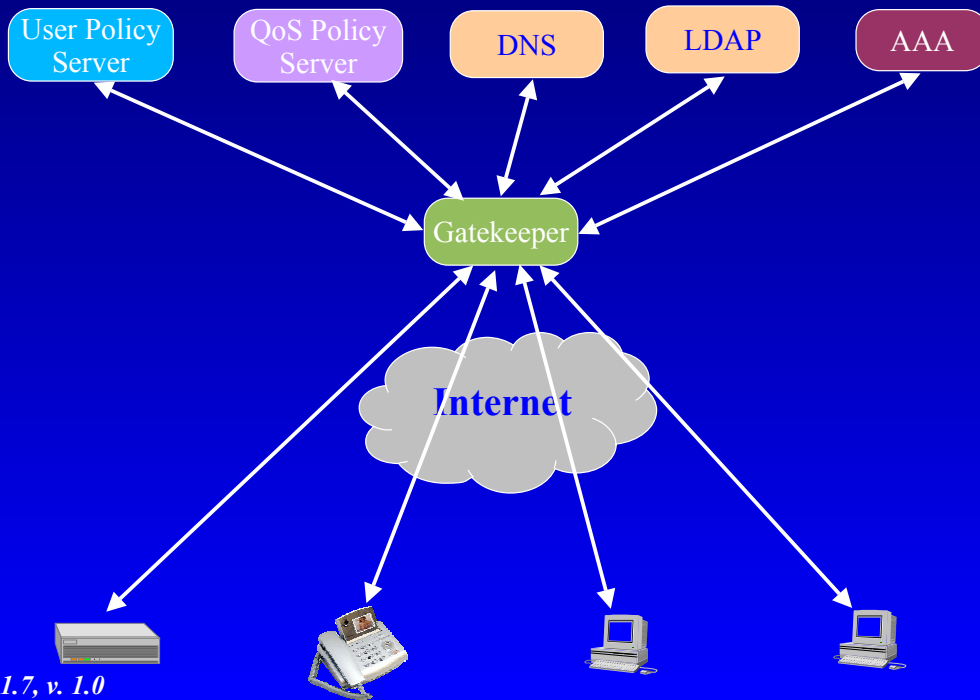
### H.225.0-RAS

---

- **H.225.0-RAS** fornisce un protocollo unificato in modo da offrire all'*endpoint* un'interfaccia comune per ottenere diversi servizi:
  - risoluzione dei nomi;
  - controllo di accesso
    - » autenticazione,
    - » QoS;
  - tariffazione.
- H.225.0-RAS è utilizzato tra gli *endpoint* ed il *gatekeeper*
  - RAS server (*Registration, Admission and Status*).



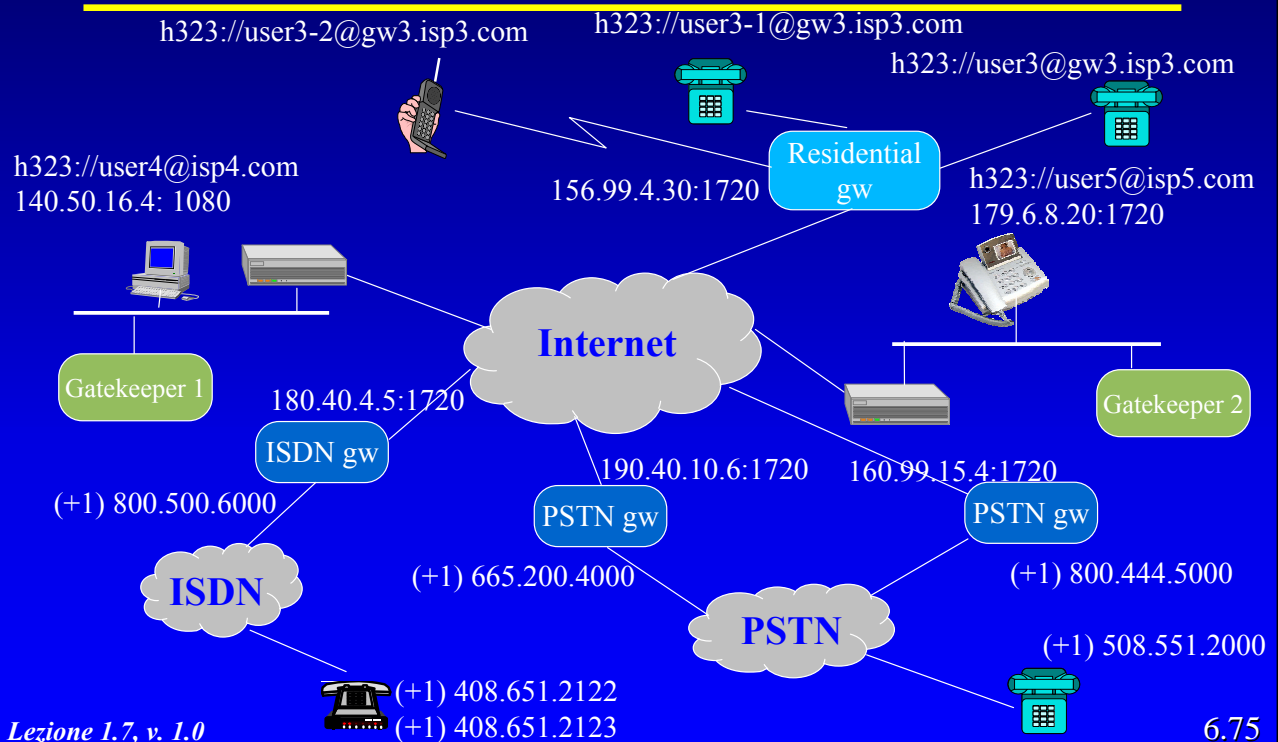
# Chiamate Punto-Punto H.225.0-RAS



Lezione 1.7, v. 1.0

6.74

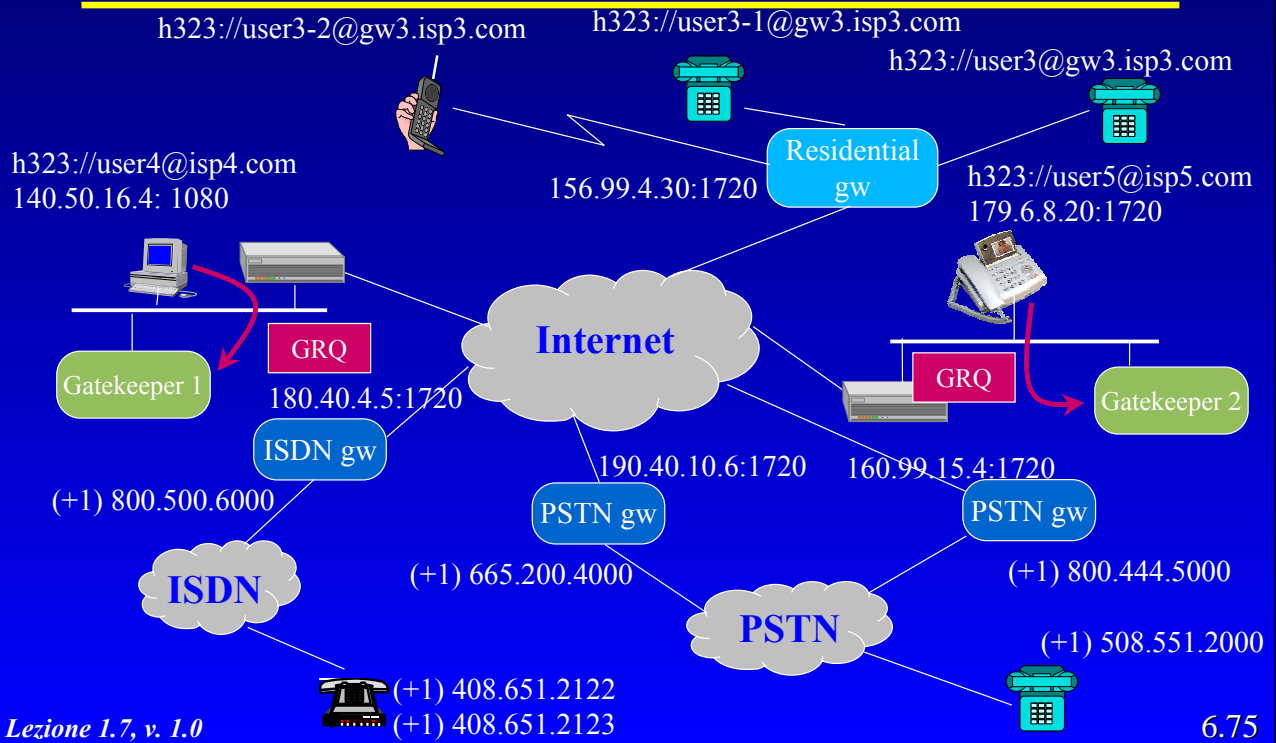
# Chiamate Punto-Punto H.225.0 – Ricerca del Gk



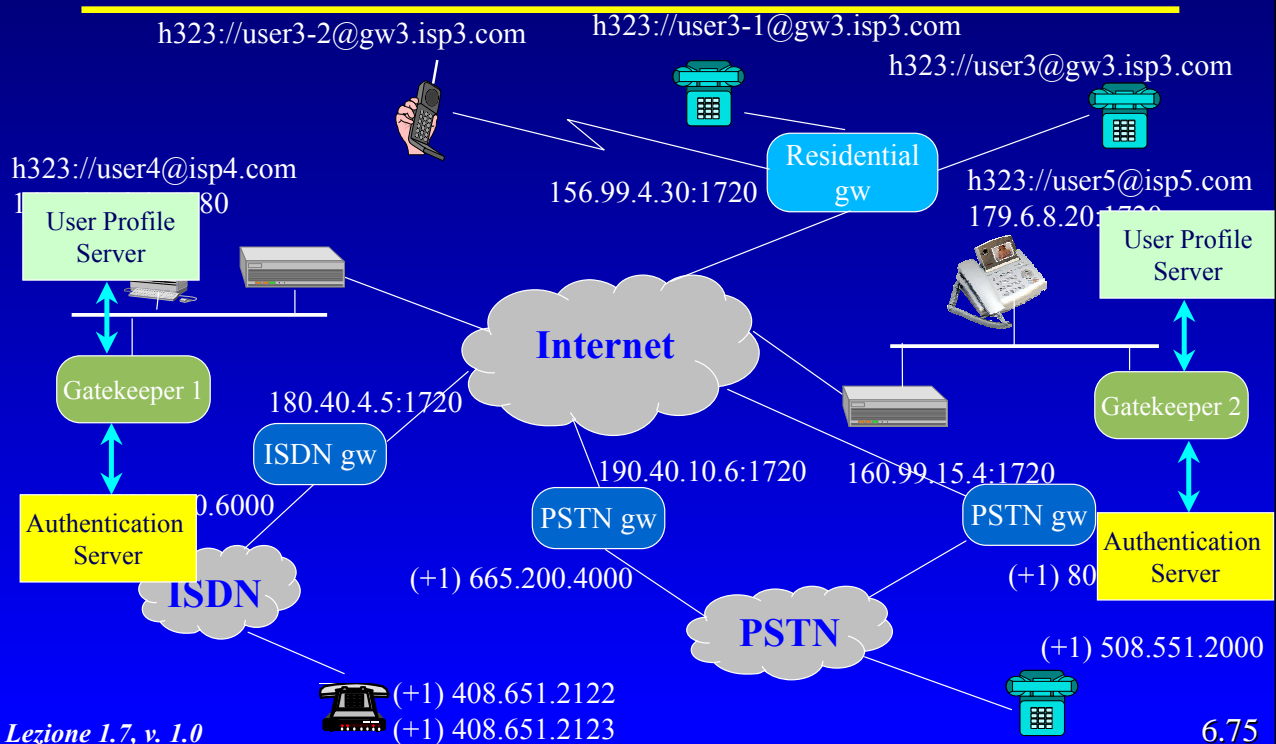
Lezione 1.7, v. 1.0

6.75

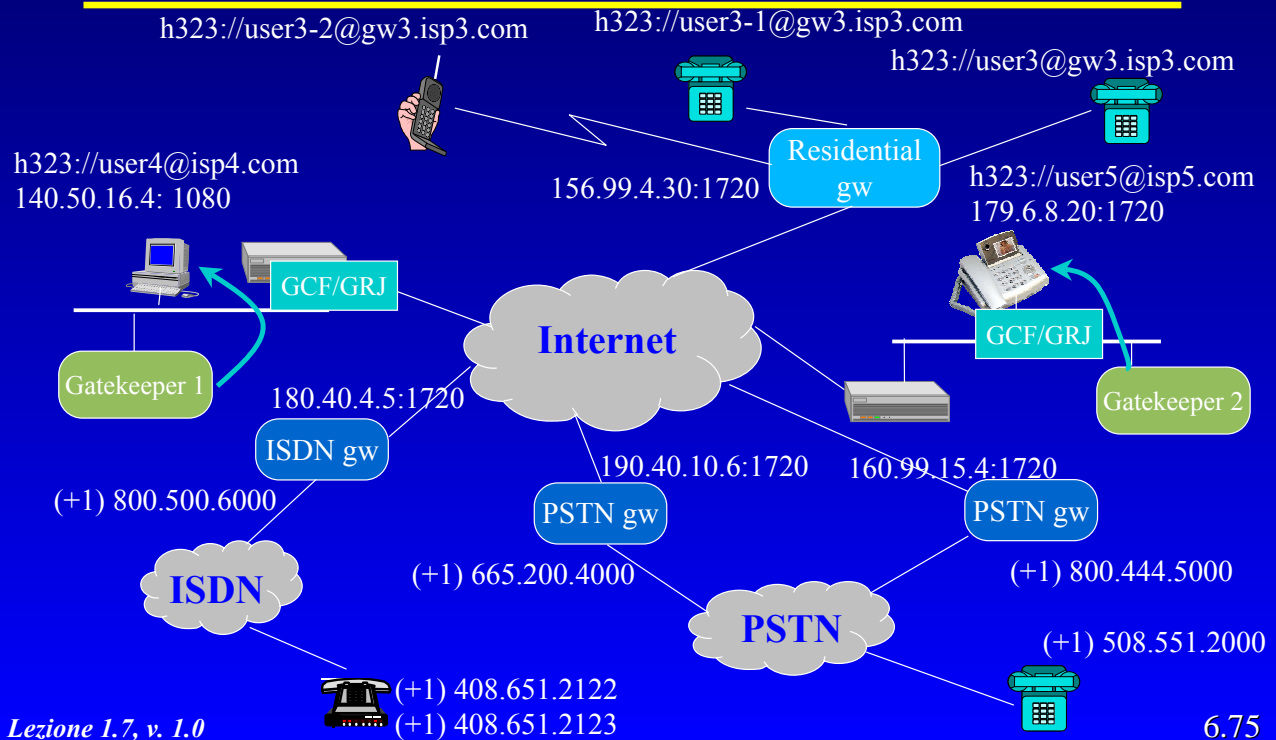
# Chiamate Punto-Punto H.225.0 – Ricerca del Gk



# Chiamate Punto-Punto H.225.0 – Ricerca del Gk



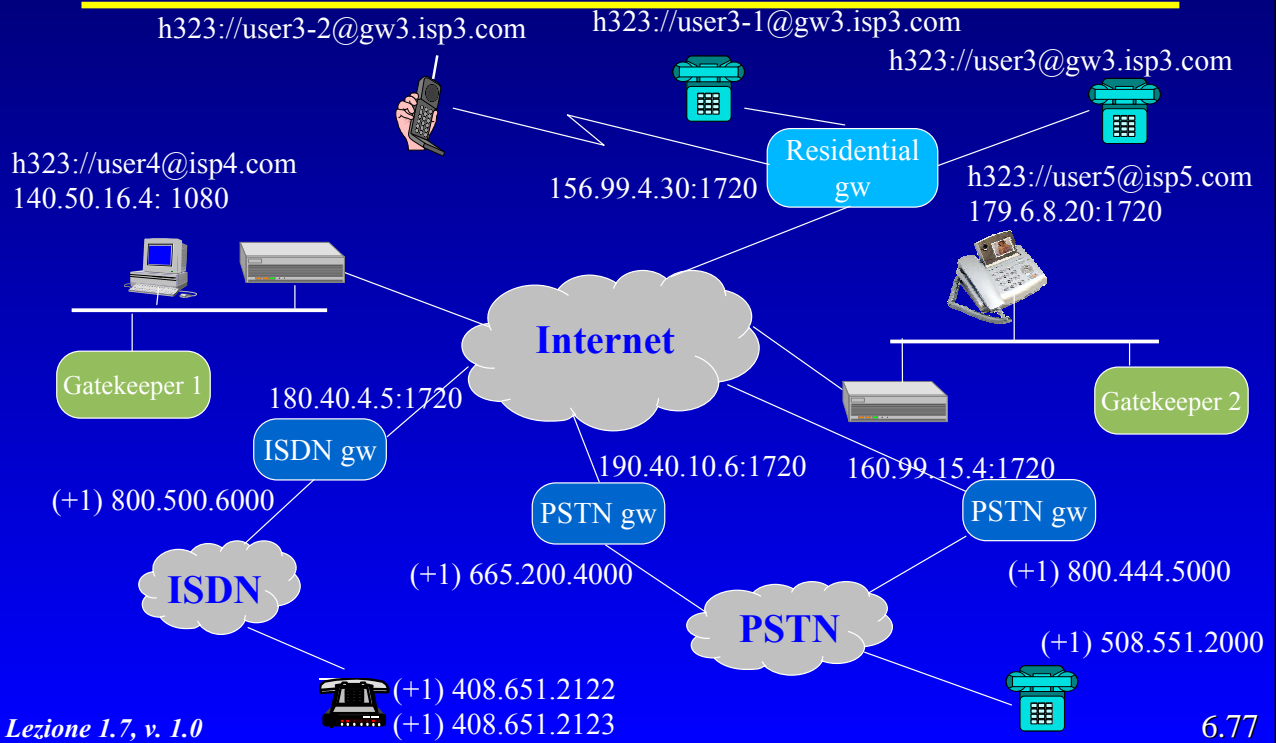
## Chiamate Punto-Punto H.225.0 – Ricerca del Gk



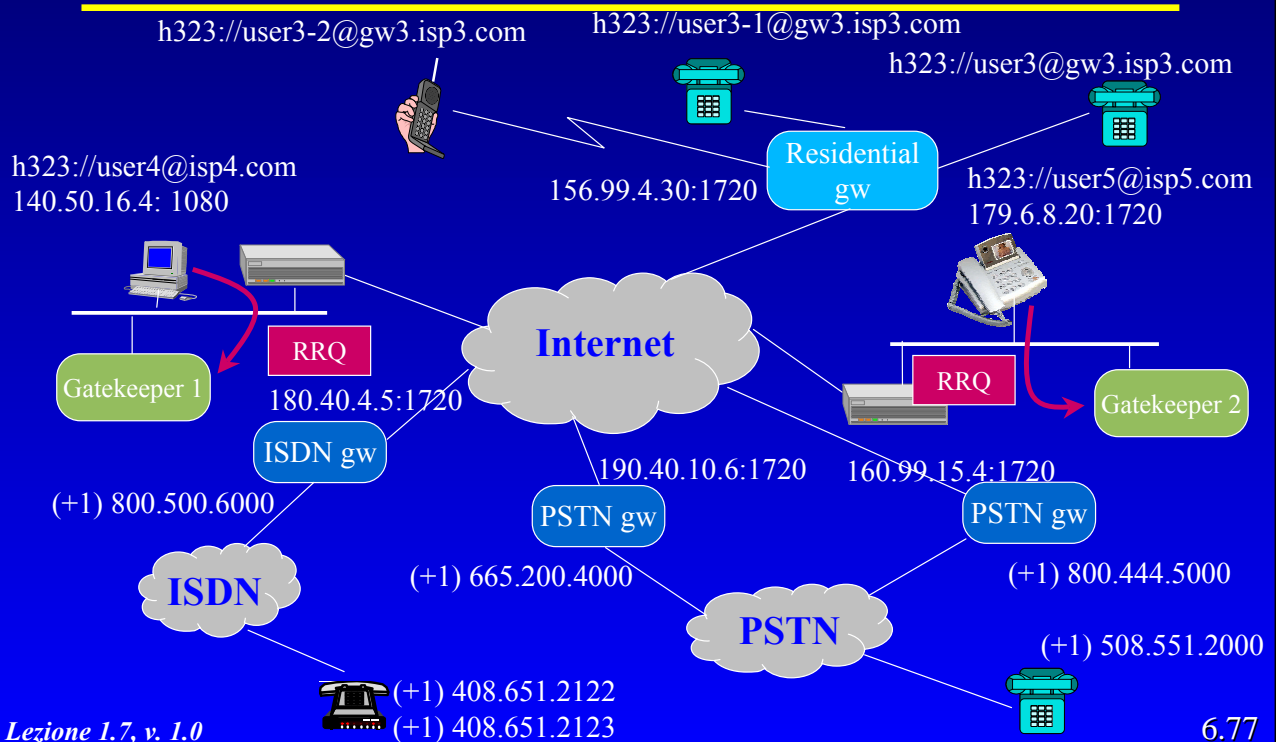
## Chiamate Punto-Punto H.225.0 – Ricerca del Gk

- La ricerca del Gk può avvenire con due modalità
  - manuale, impostando l'indirizzo del Gk
  - automatica
    - » multicast, all'indirizzo 224.0.1.41, porta 1718,
    - » DNS, a partire dal nome del Gk
      - gk-id@domain, ras://gk-id@domain, ras://domain/gk-id,
      - la risoluzione avviene tramite ricerca di record SRV o TXT relativi al nome del dominio (la porta di default è la 1719).

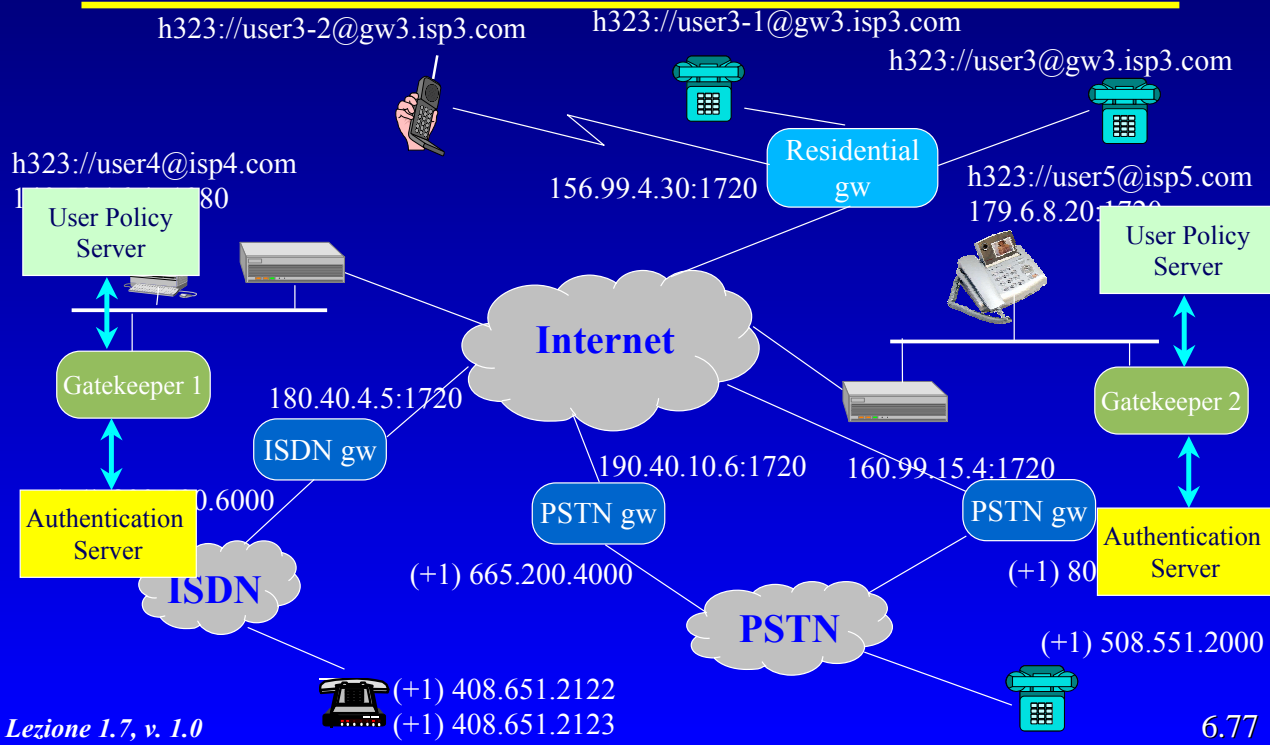
# Chiamate Punto-Punto H.225.0 – Registrazione



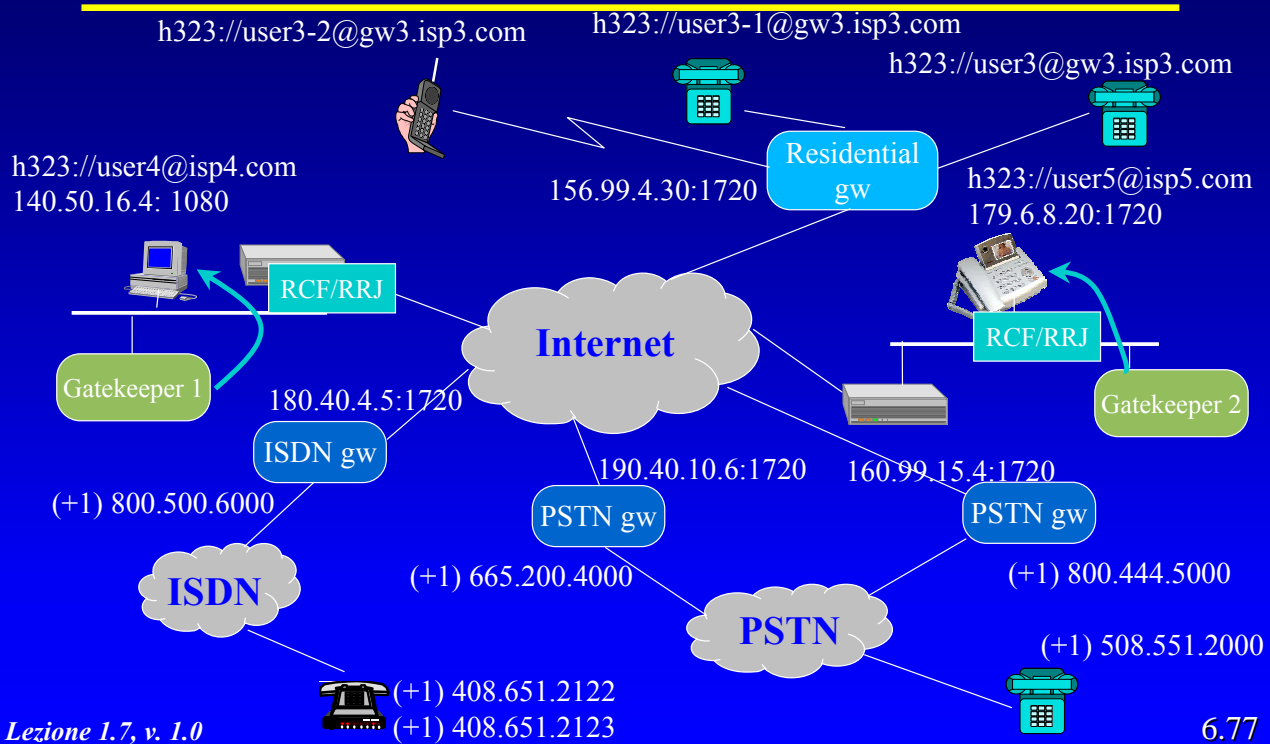
# Chiamate Punto-Punto H.225.0 – Registrazione



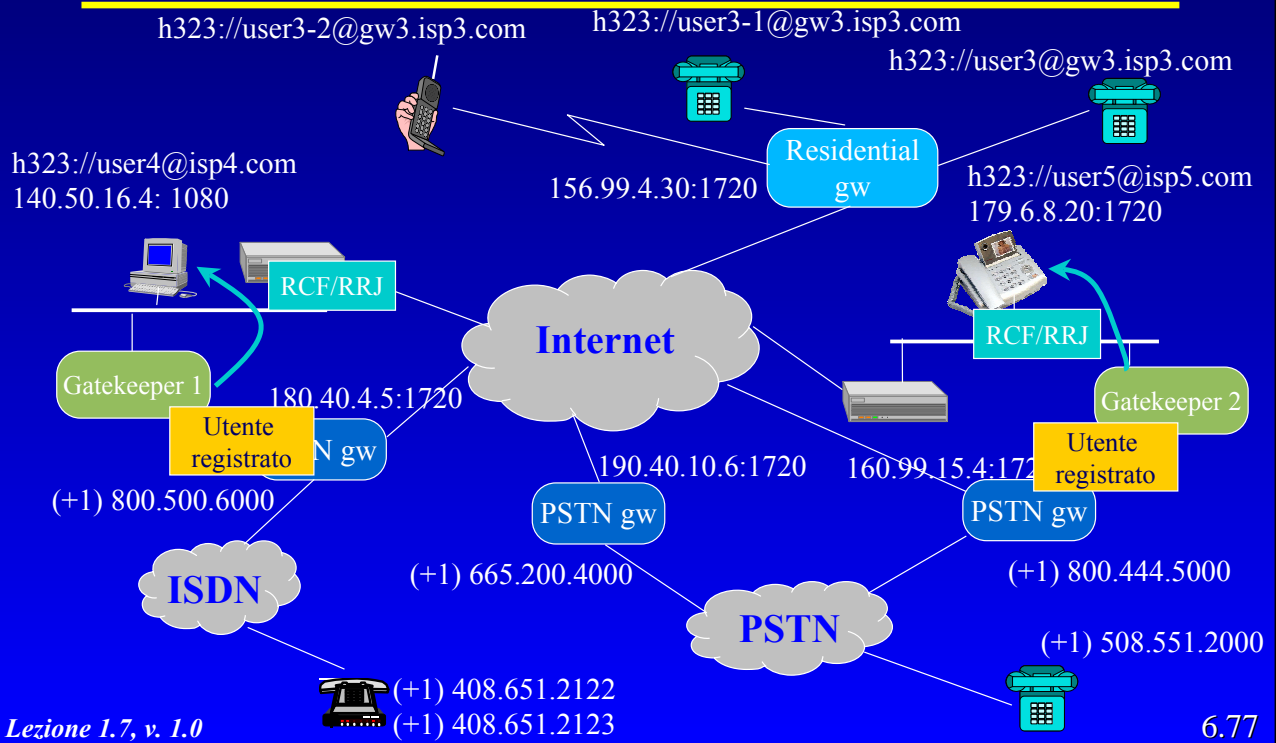
# Chiamate Punto-Punto H.225.0 – Registrazione



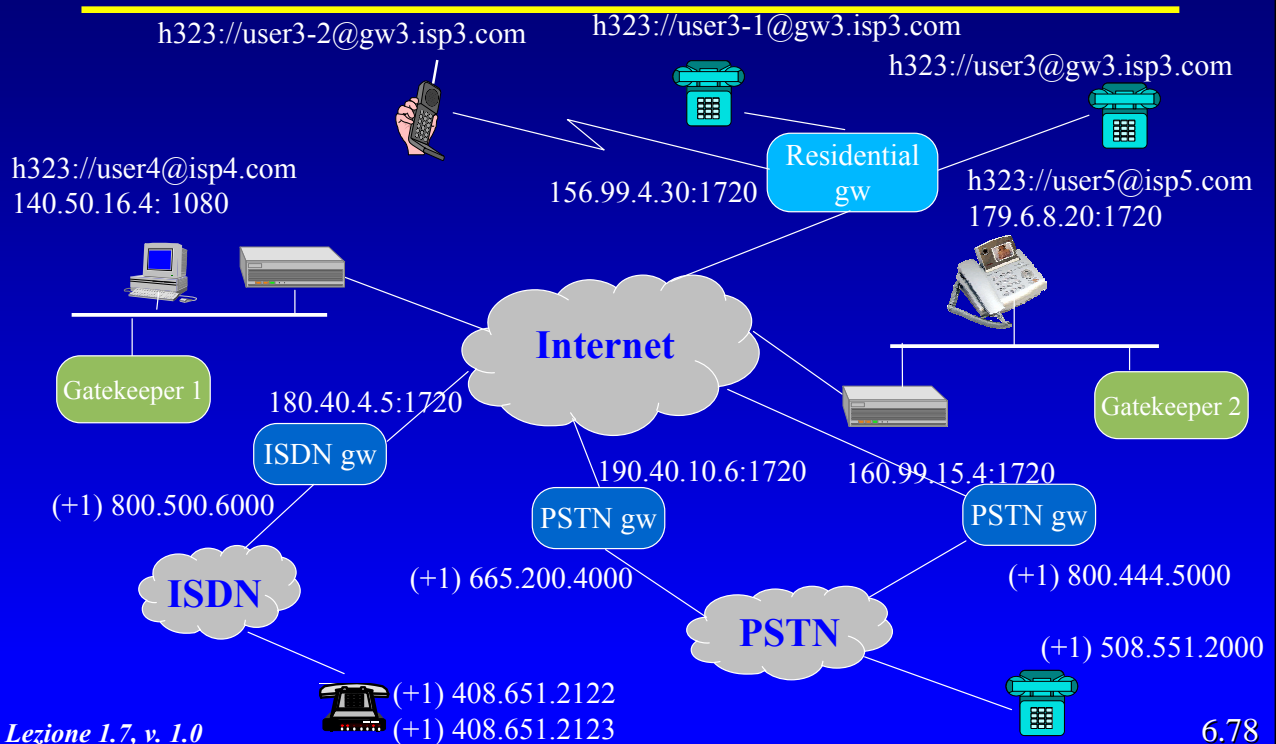
# Chiamate Punto-Punto H.225.0 – Registrazione



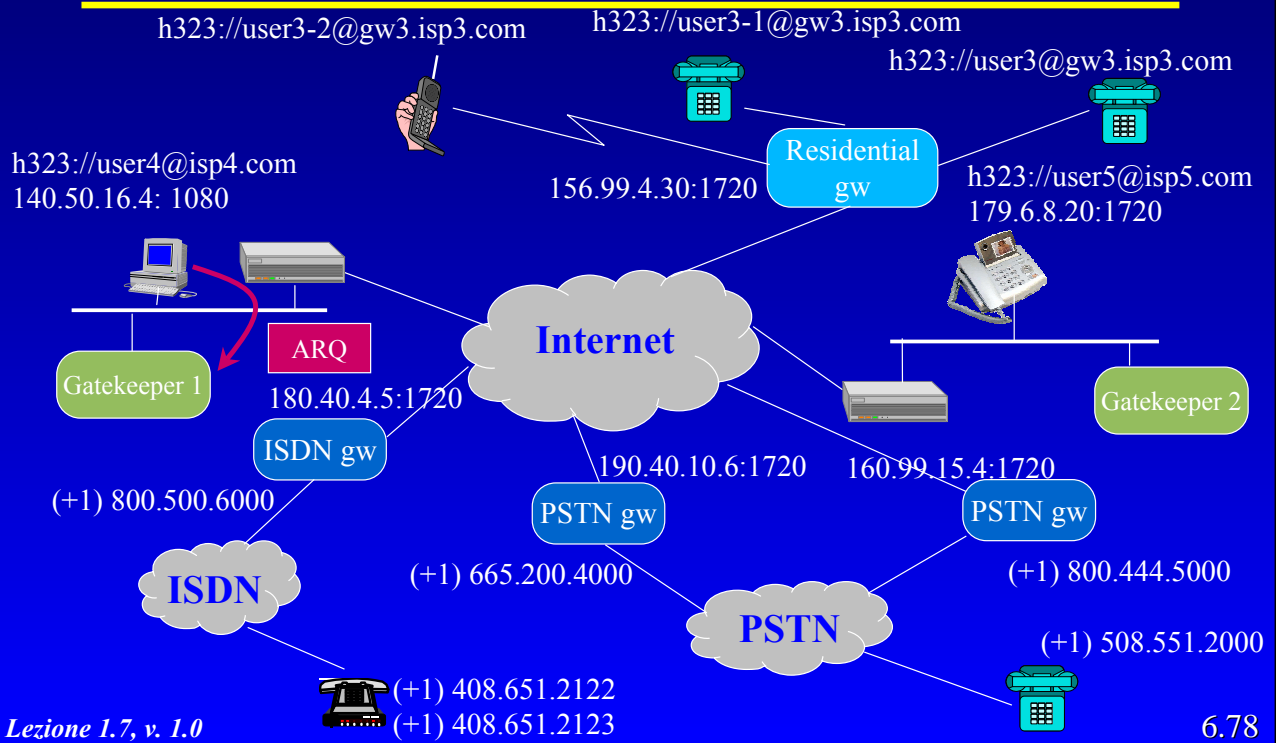
# Chiamate Punto-Punto H.225.0 – Registrazione



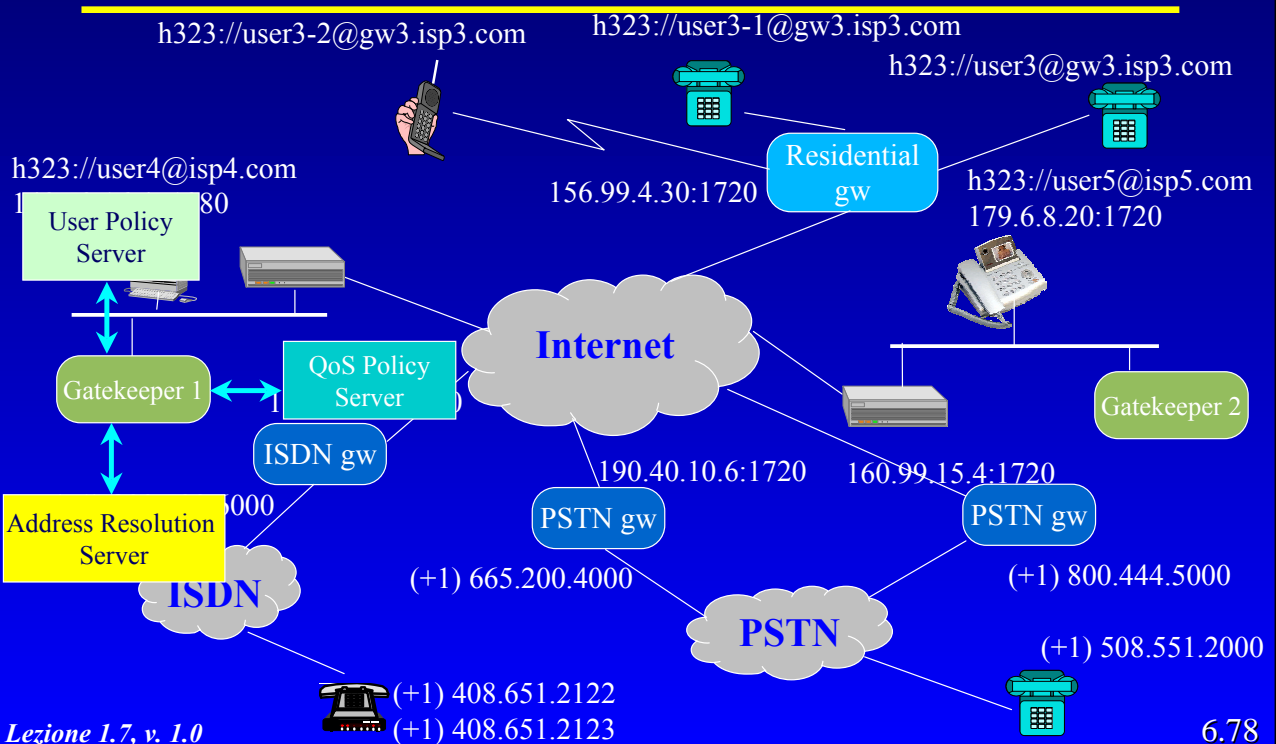
# Chiamate Punto-Punto H.225.0 – Instaurazione della chiamata



# Chiamate Punto-Punto H.225.0 – Instaurazione della chiamata

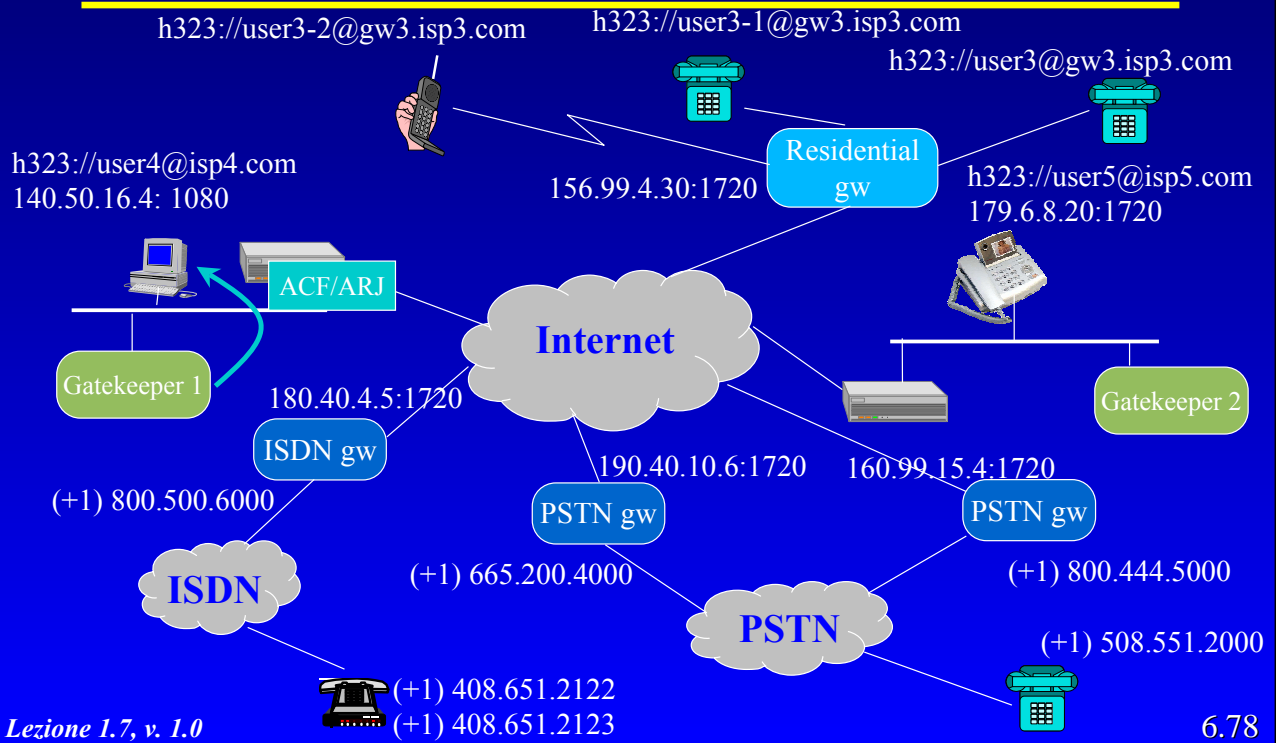


# Chiamate Punto-Punto H.225.0 – Instaurazione della chiamata



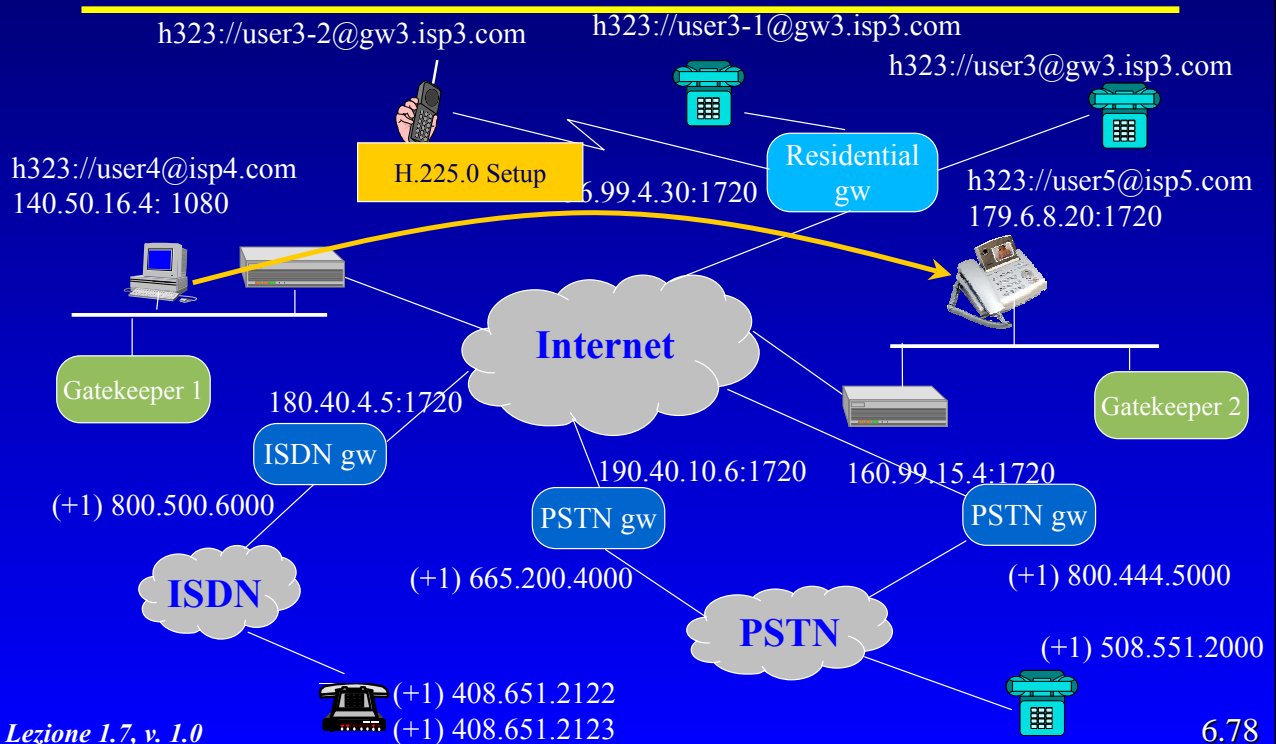
### Chiamate Punto-Punto

# H.225.0 – Instaurazione della chiamata



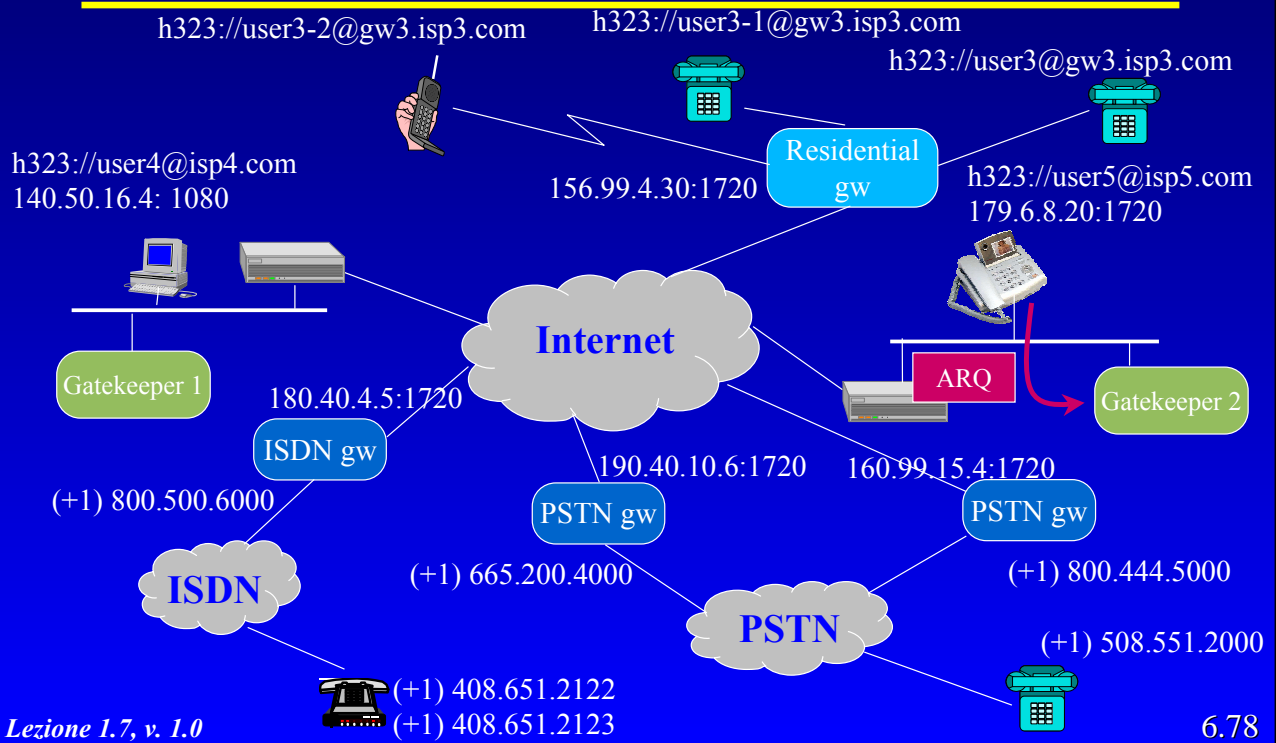
### Chiamate Punto-Punto

# H.225.0 – Instaurazione della chiamata

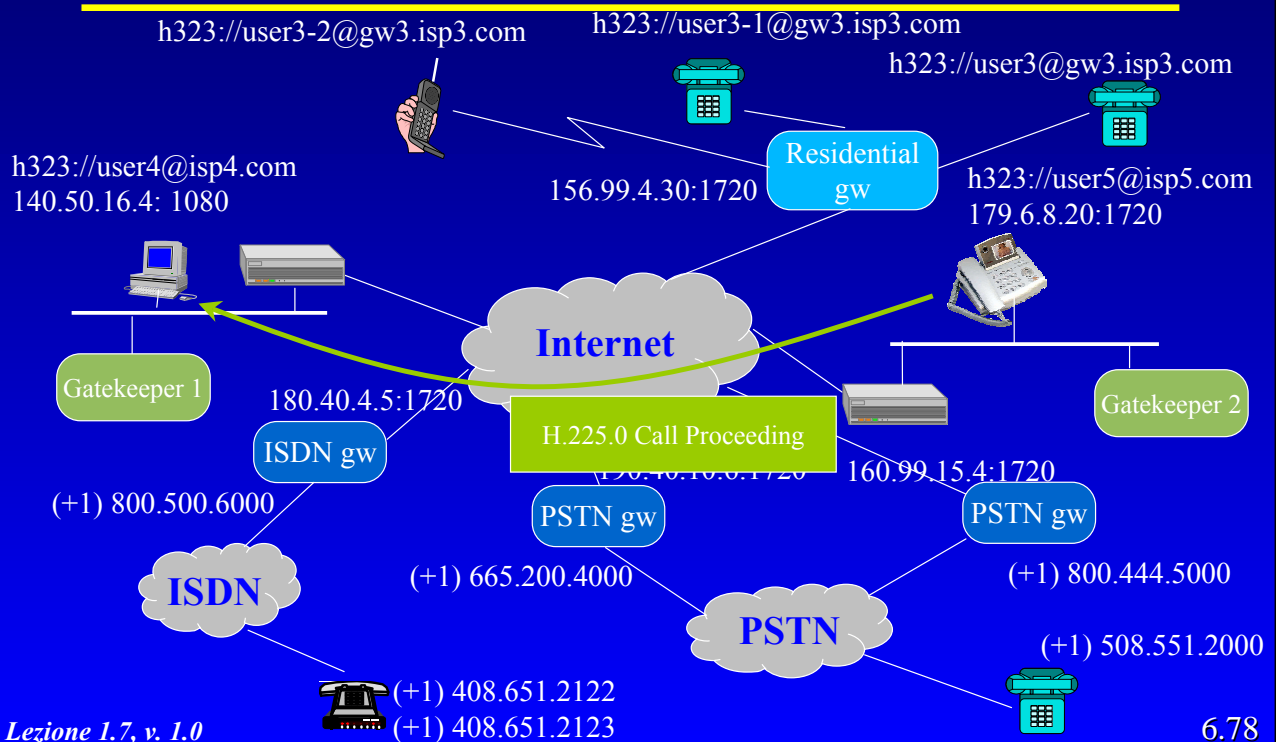




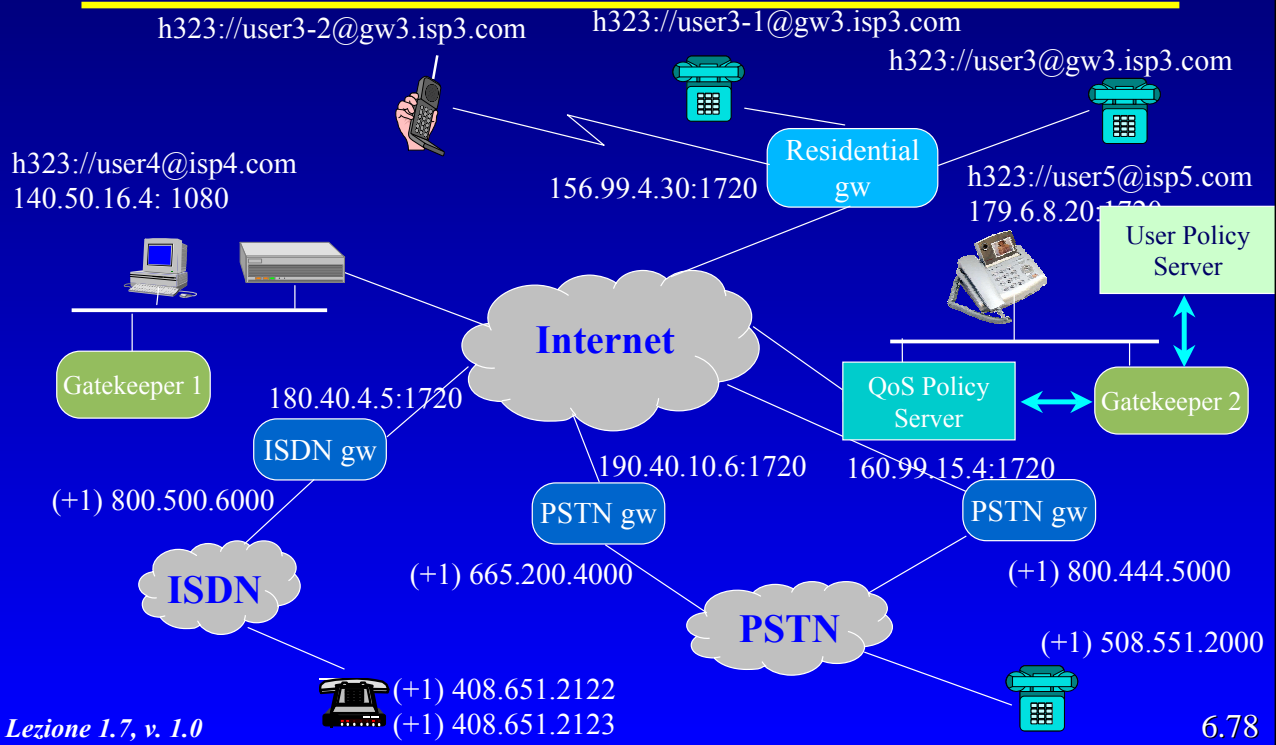
# Chiamate Punto-Punto H.225.0 – Instaurazione della chiamata



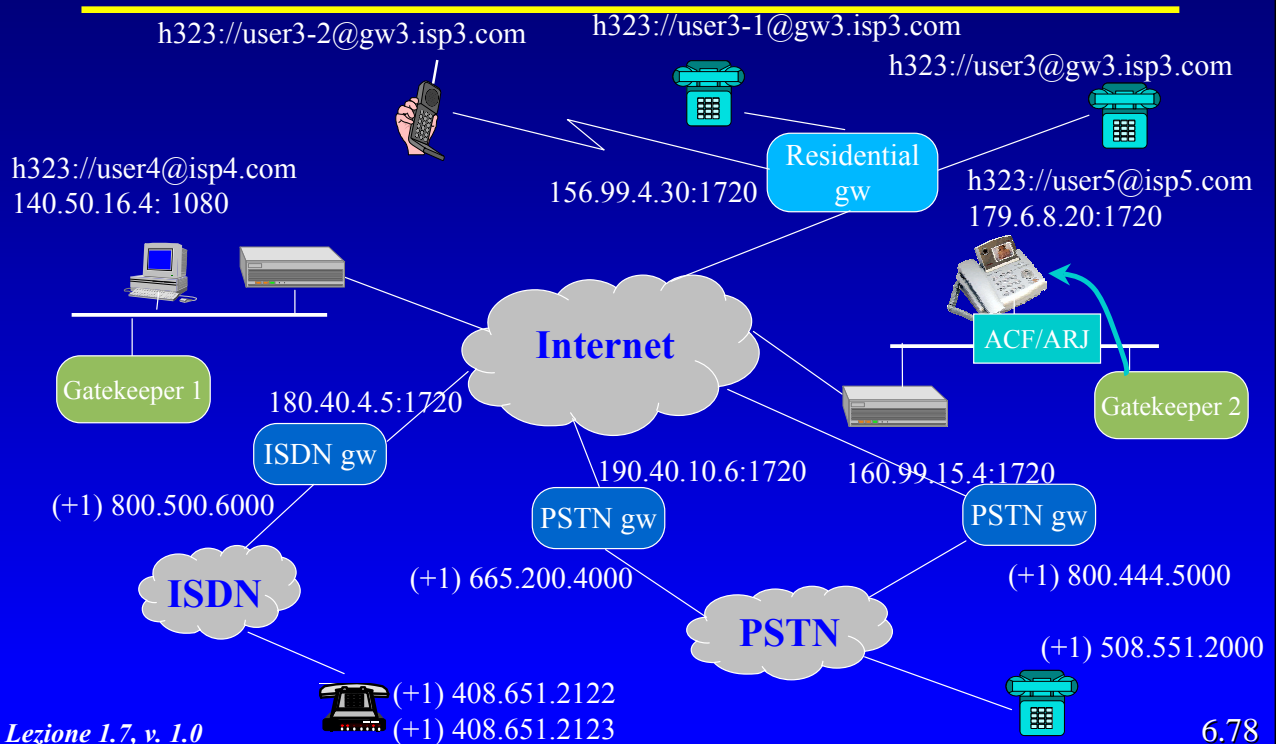
# Chiamate Punto-Punto H.225.0 – Instaurazione della chiamata



# Chiamate Punto-Punto H.225.0 – Instaurazione della chiamata

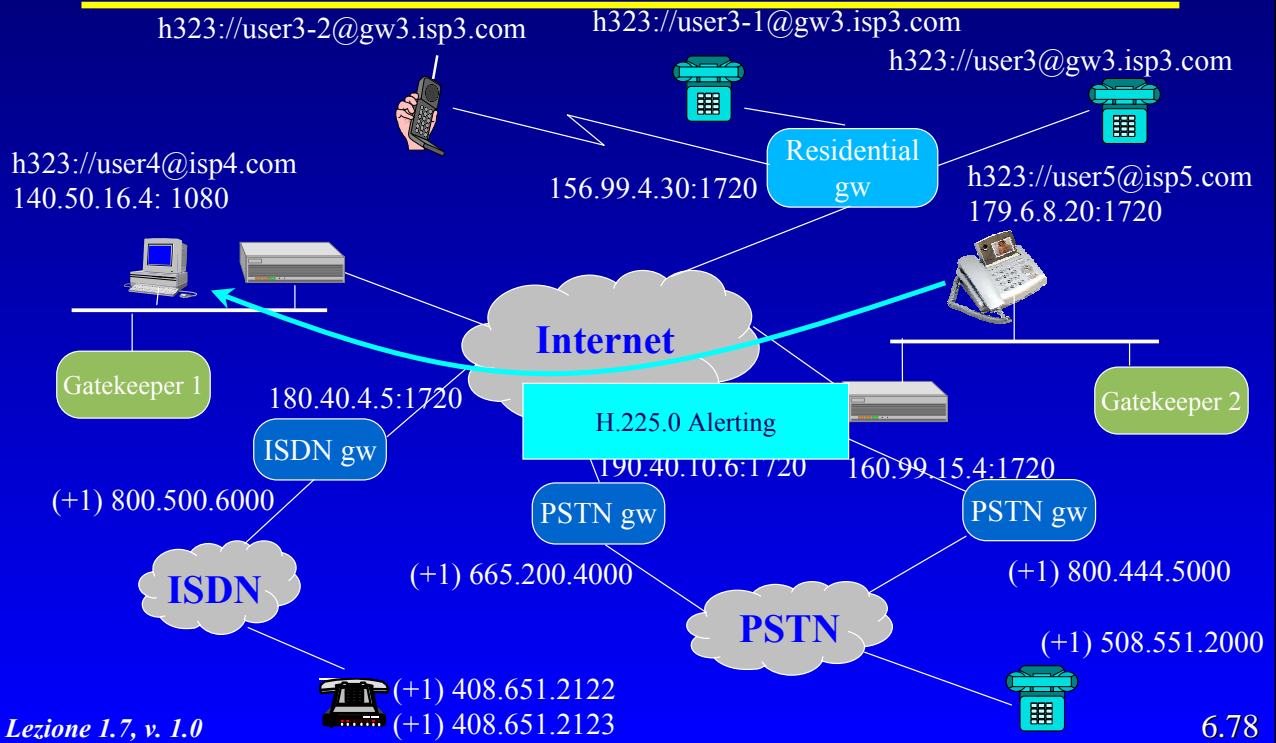


# Chiamate Punto-Punto H.225.0 – Instaurazione della chiamata



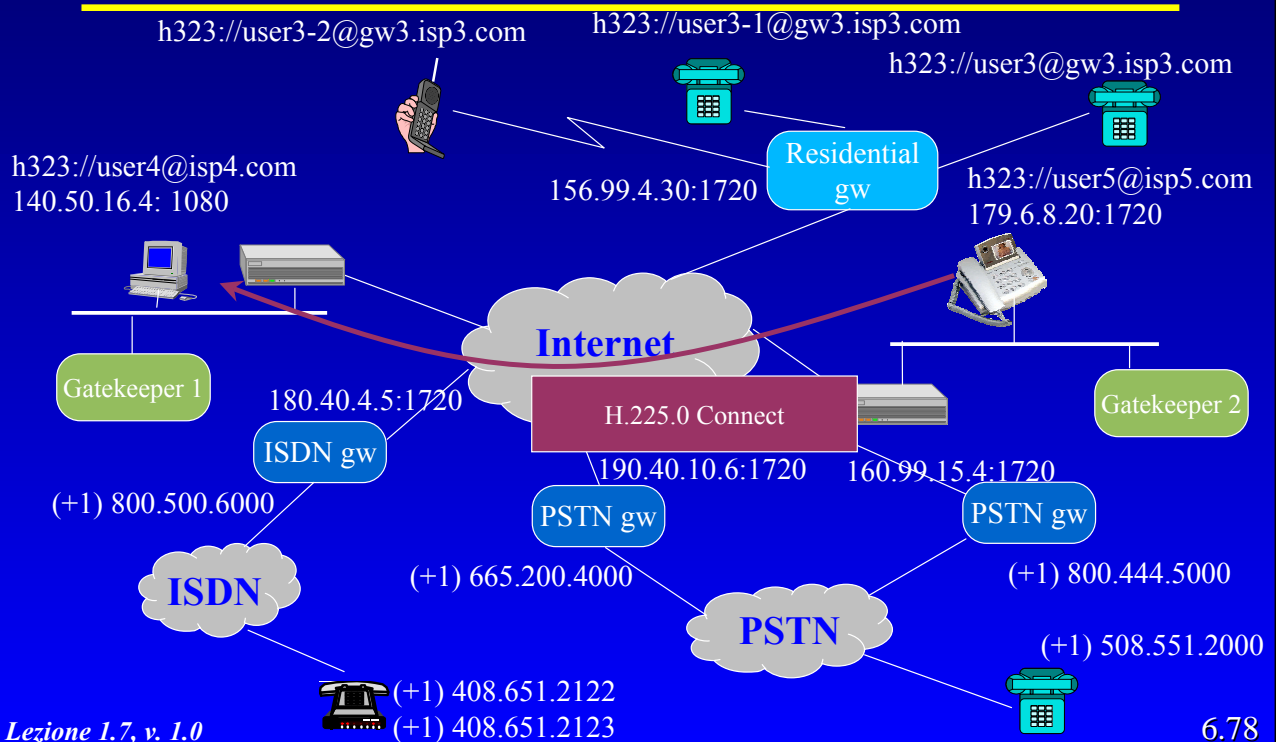
### Chiamate Punto-Punto

## H.225.0 – Instaurazione della chiamata

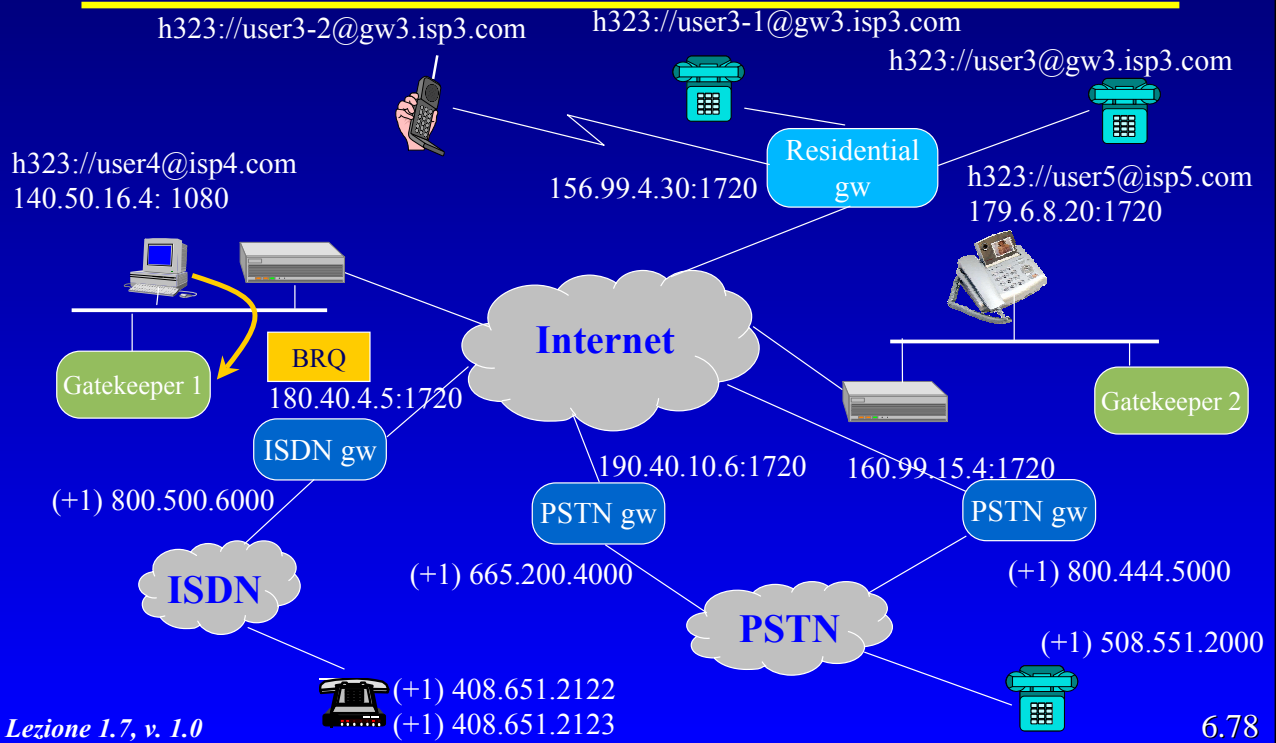


### Chiamate Punto-Punto

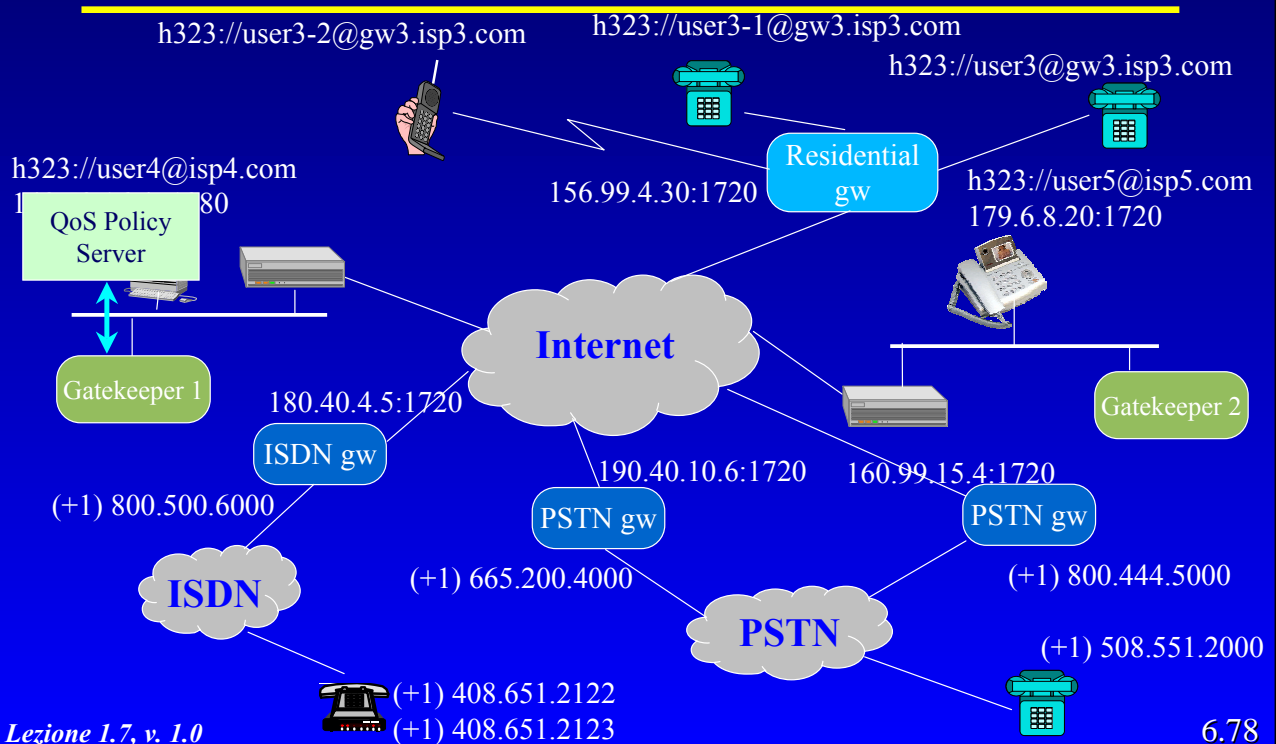
## H.225.0 – Instaurazione della chiamata



# Chiamate Punto-Punto H.225.0 – Instaurazione della chiamata

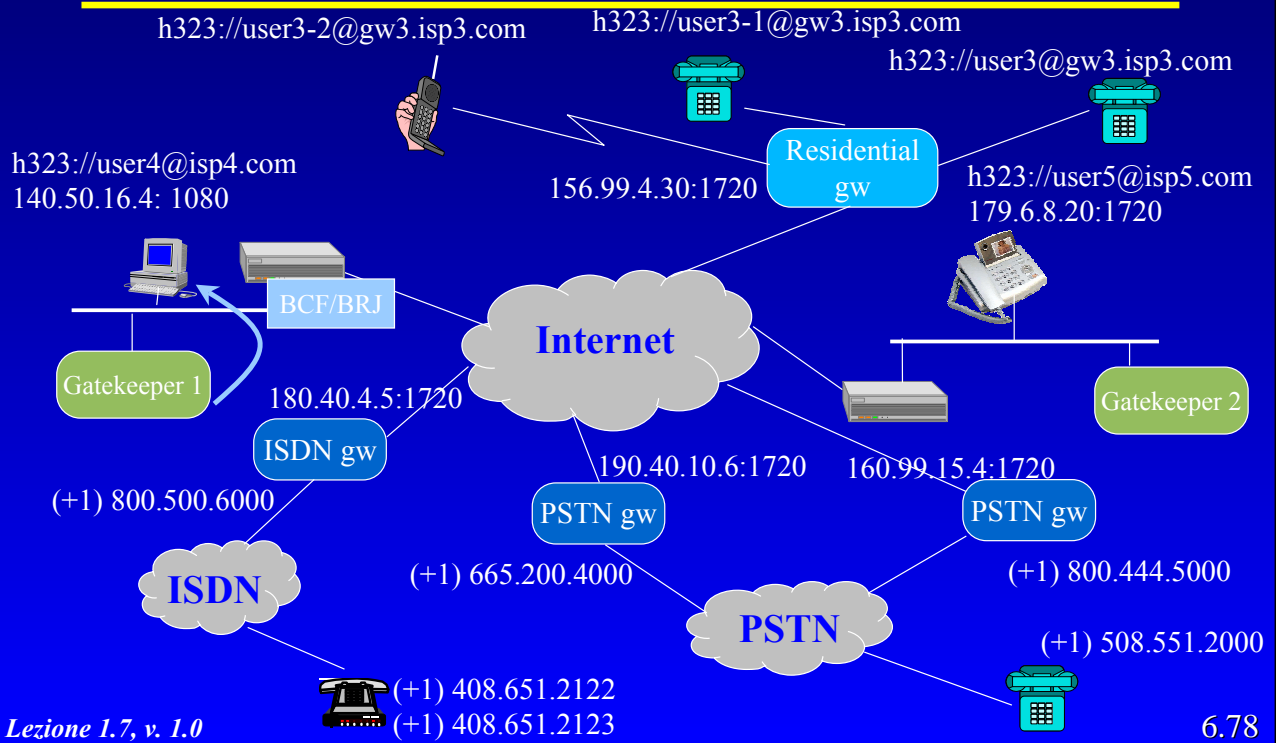


# Chiamate Punto-Punto H.225.0 – Instaurazione della chiamata



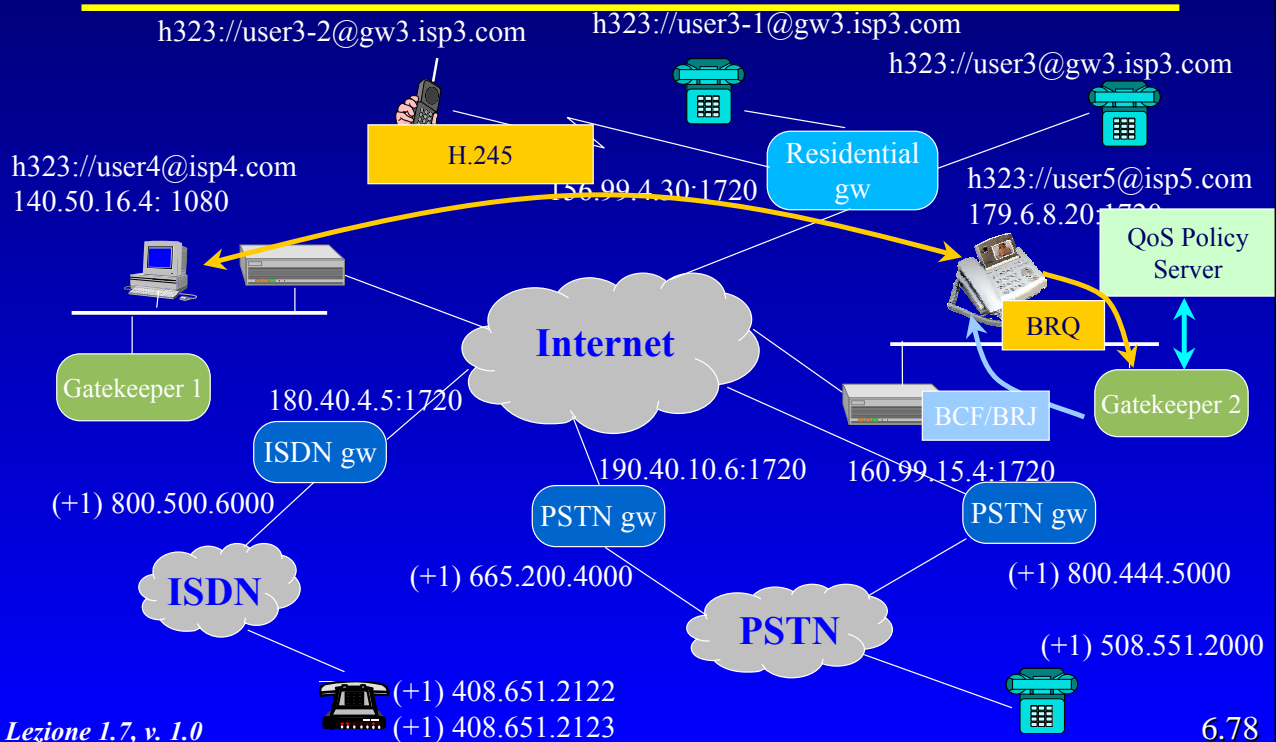
### Chiamate Punto-Punto

## H.225.0 – Instaurazione della chiamata



### Chiamate Punto-Punto

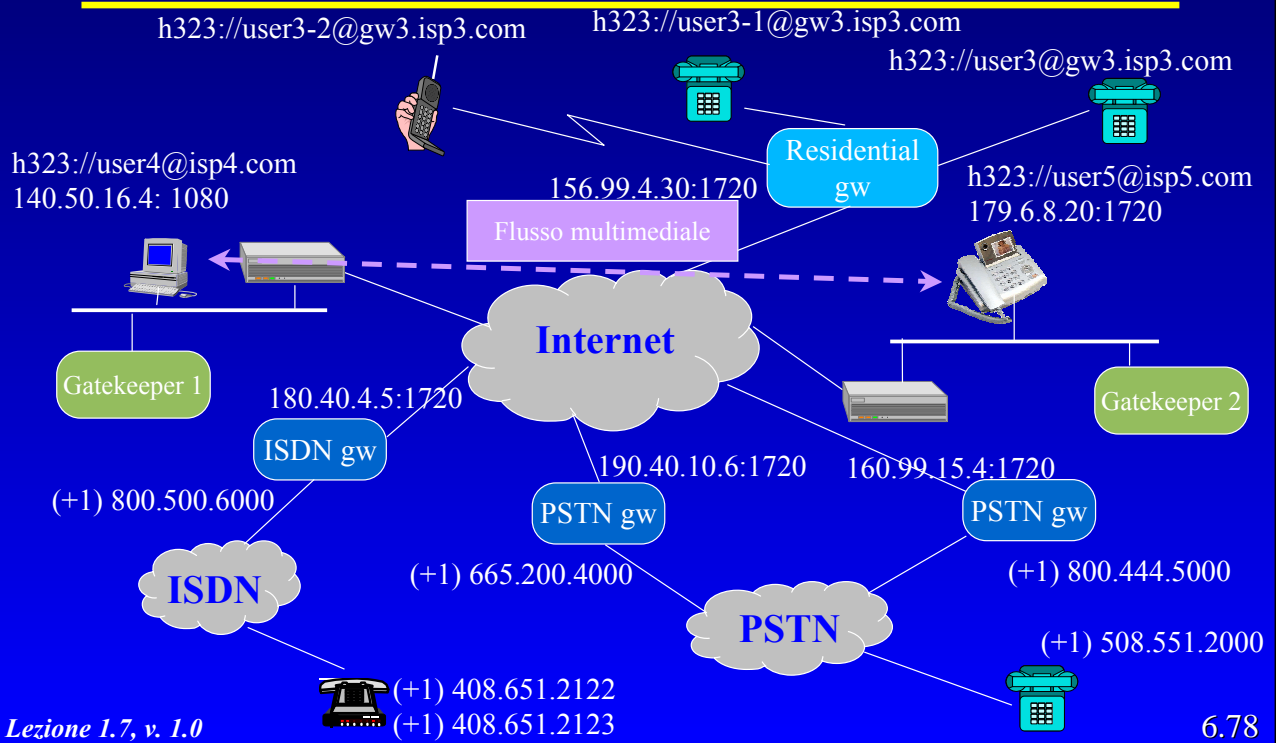
## H.225.0 – Instaurazione della chiamata





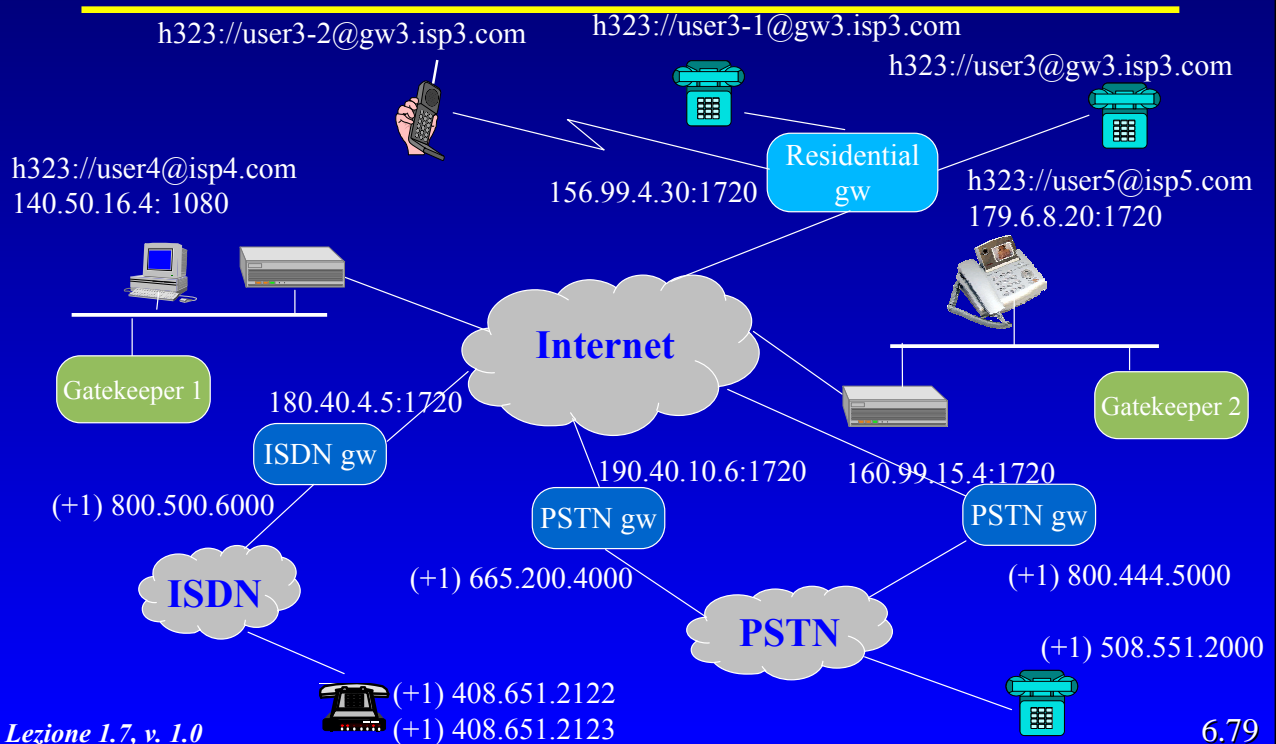
### Chiamate Punto-Punto

# H.225.0 – Instaurazione della chiamata



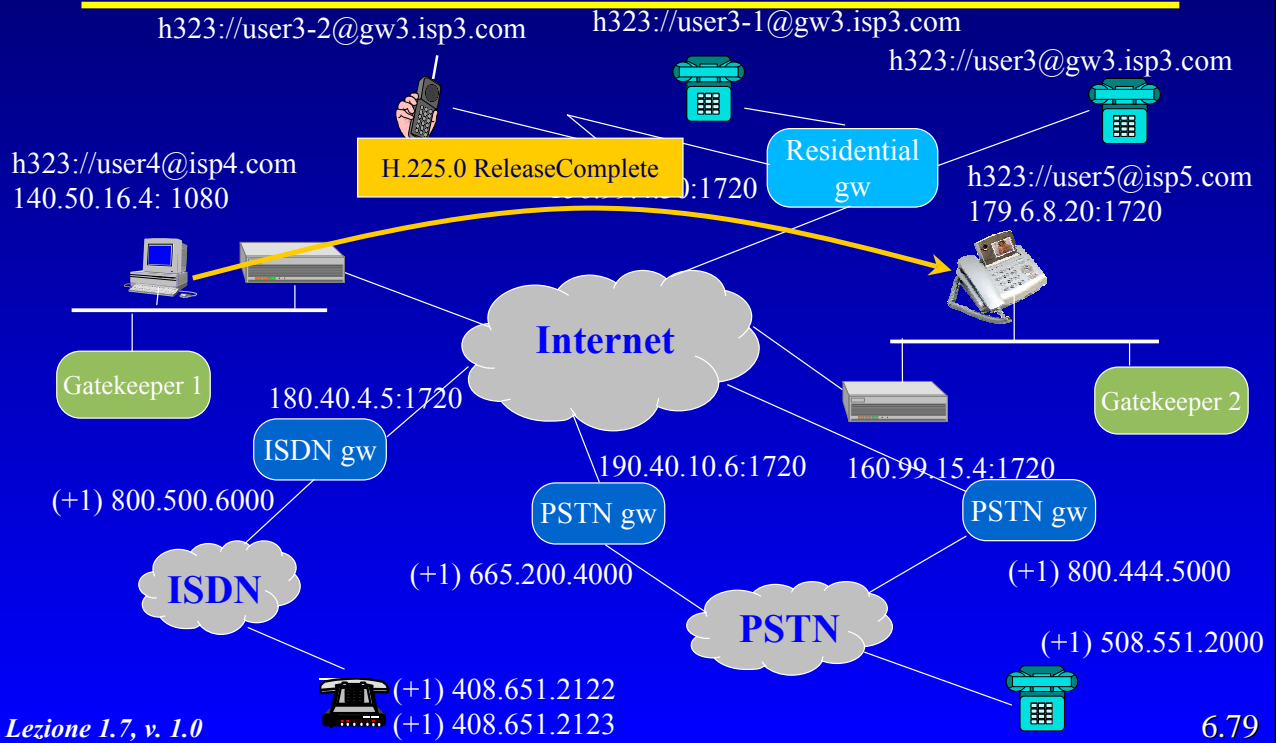
### Chiamate Punto-Punto

# H.225.0 – Instaurazione della chiamata



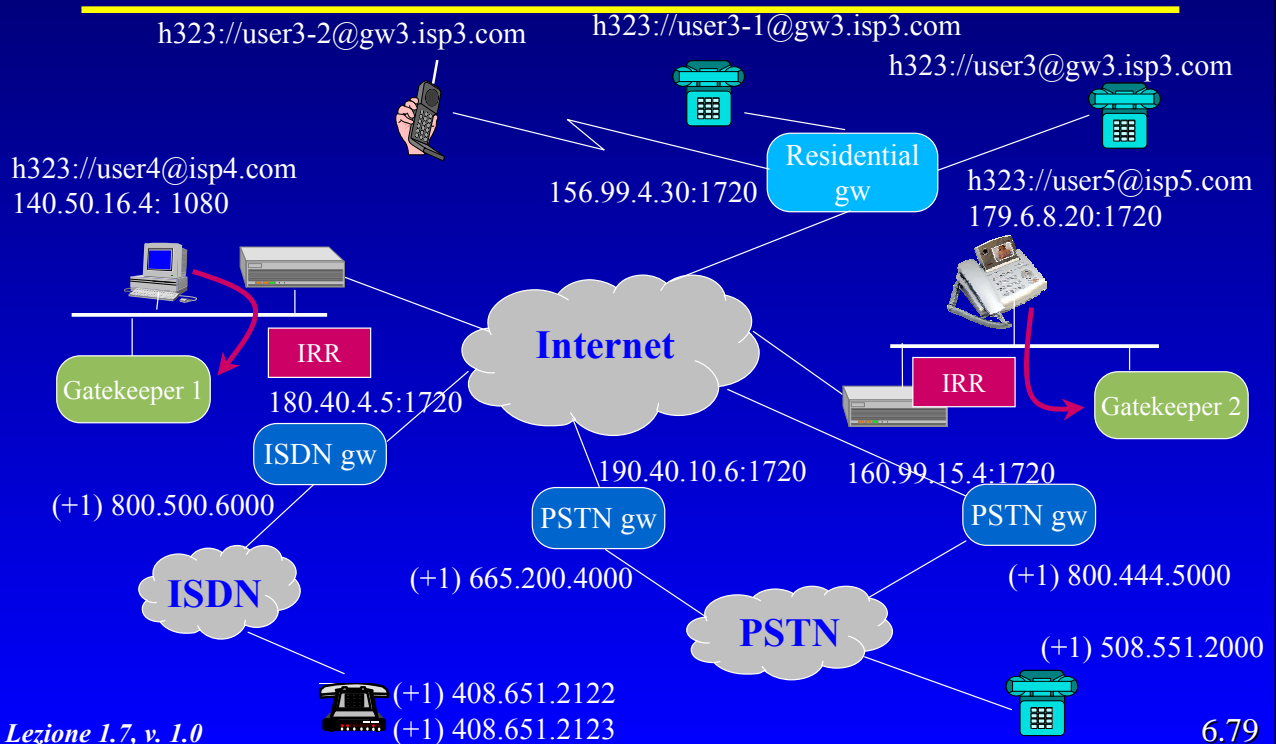
### Chiamate Punto-Punto

## H.225.0 – Instaurazione della chiamata



### Chiamate Punto-Punto

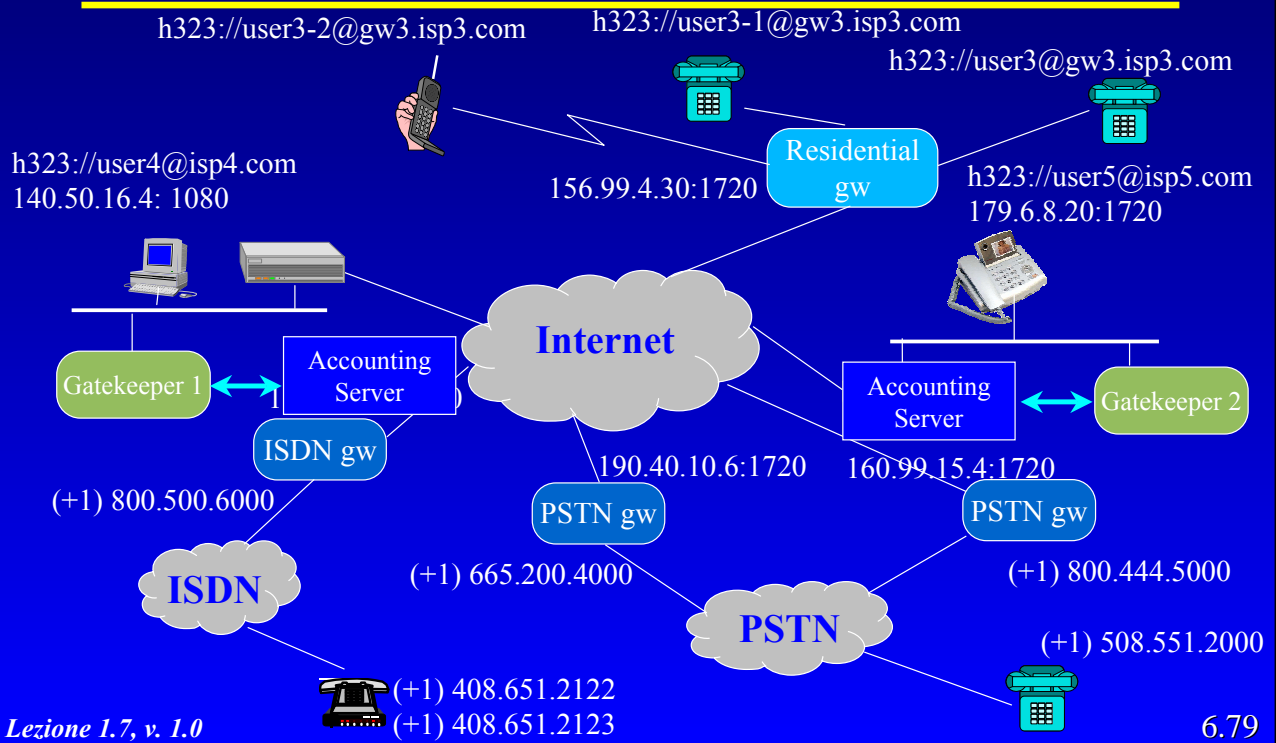
## H.225.0 – Instaurazione della chiamata





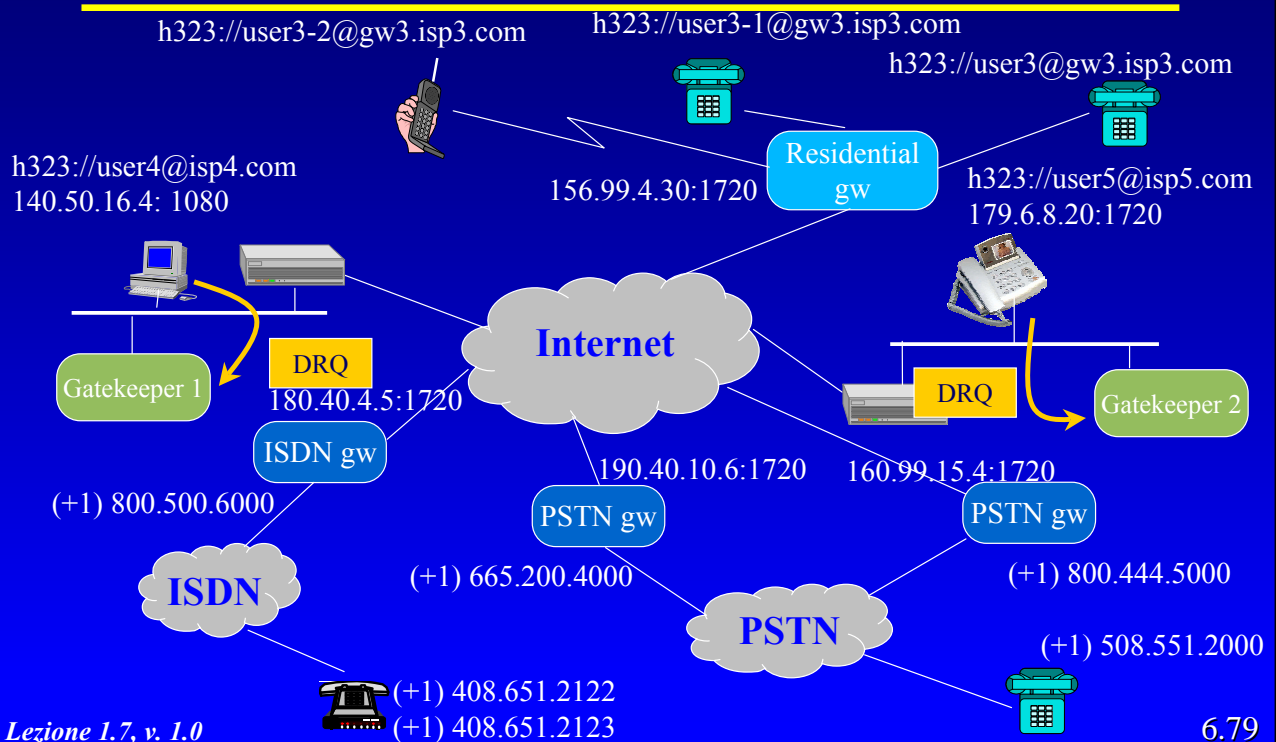
### Chiamate Punto-Punto

## H.225.0 – Instaurazione della chiamata

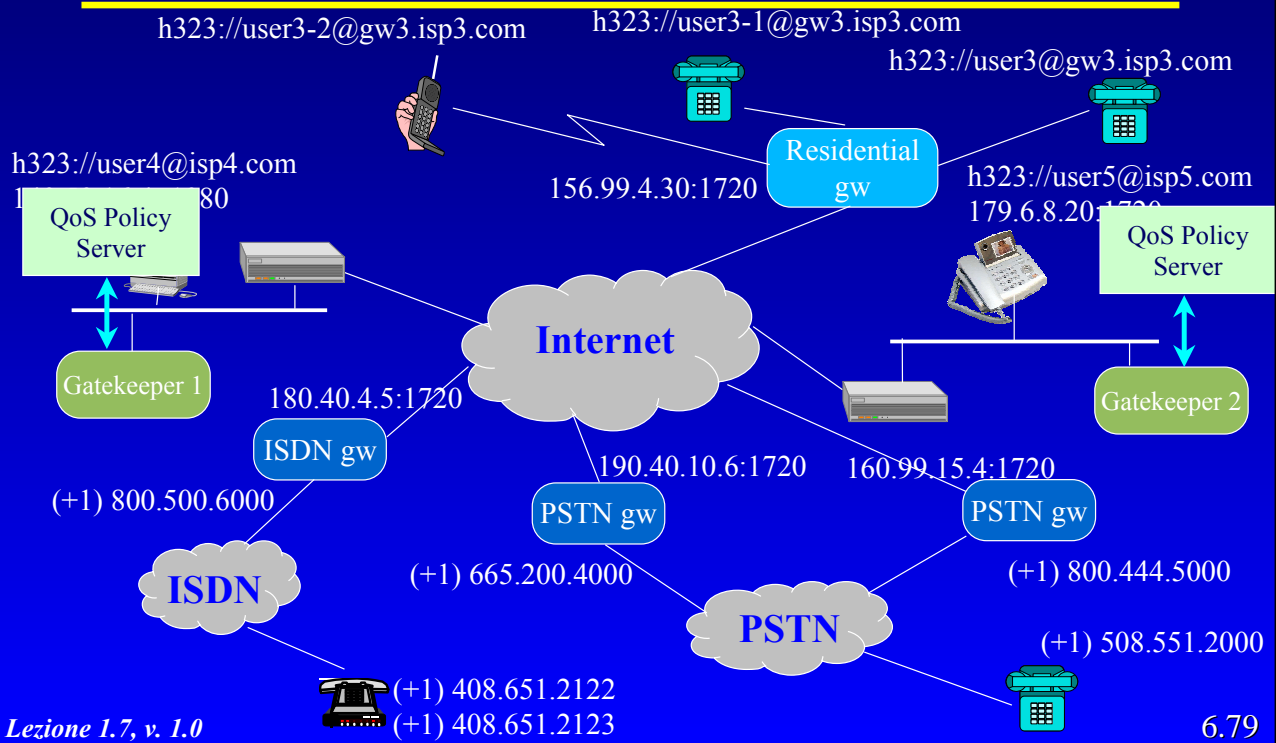


### Chiamate Punto-Punto

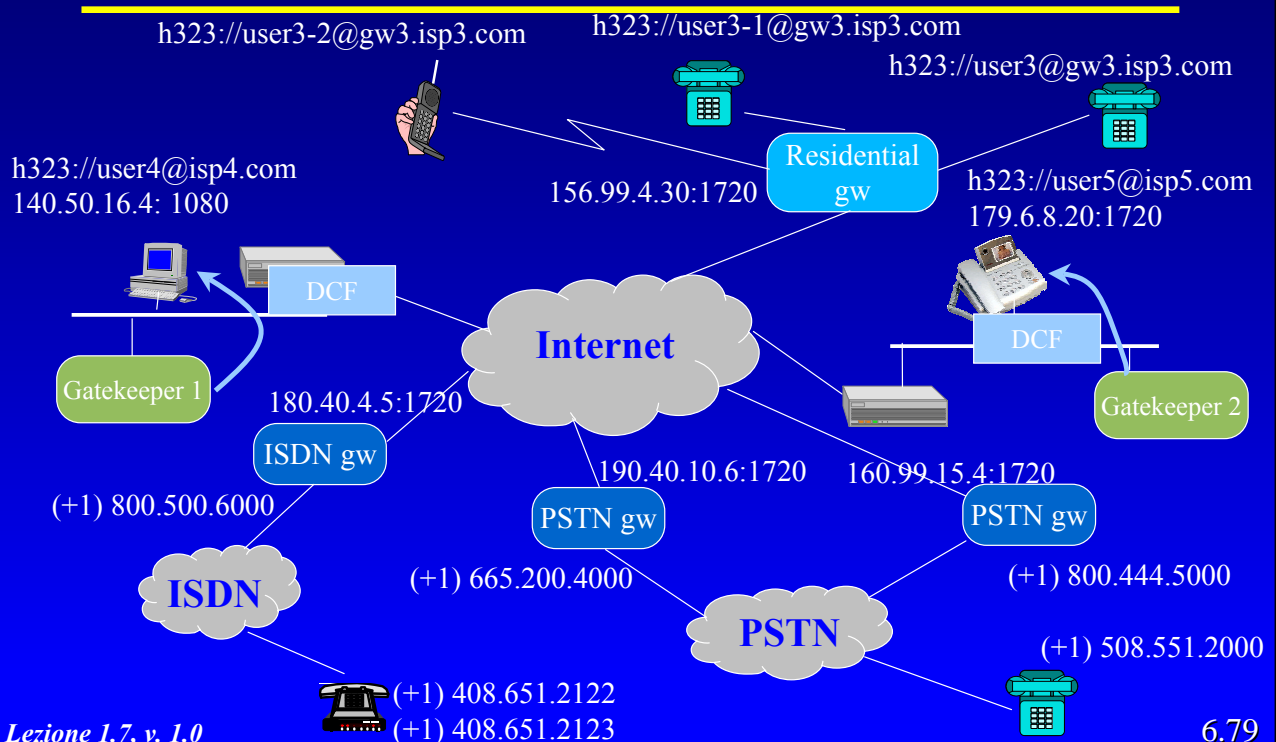
## H.225.0 – Instaurazione della chiamata



# Chiamate Punto-Punto H.225.0 – Instaurazione della chiamata

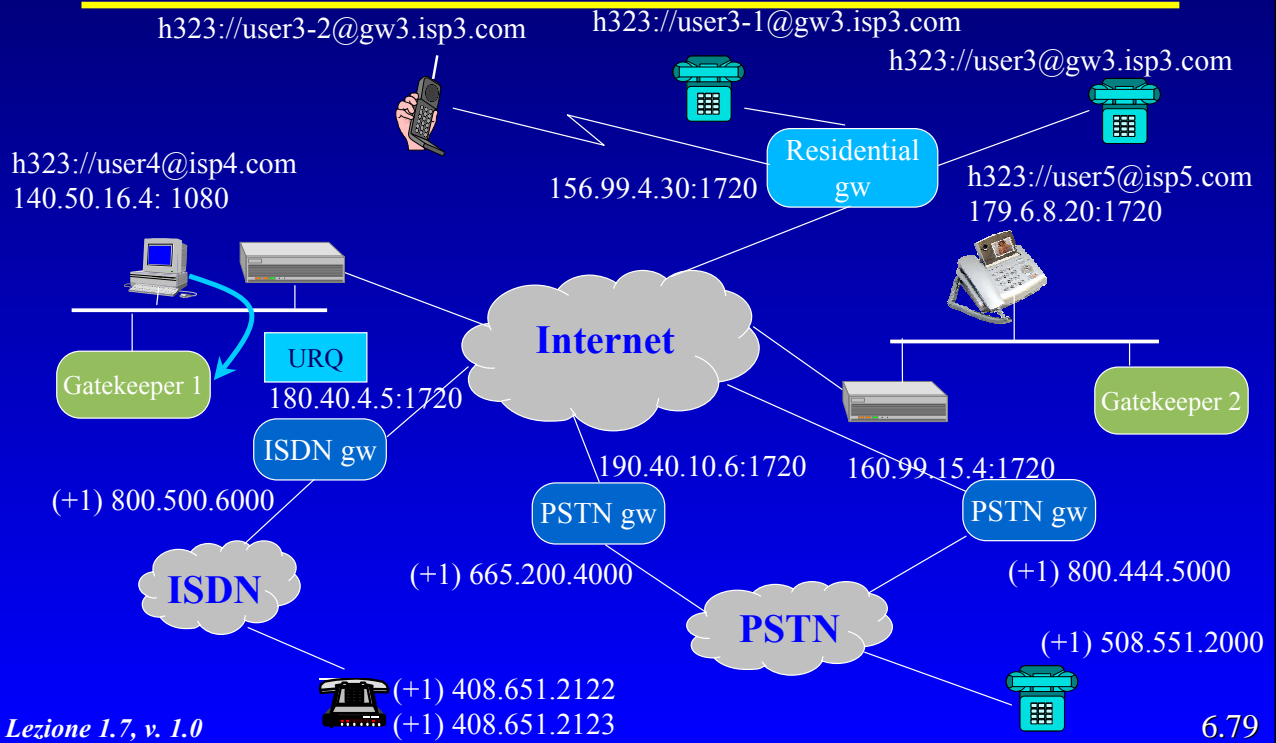


# Chiamate Punto-Punto H.225.0 – Instaurazione della chiamata



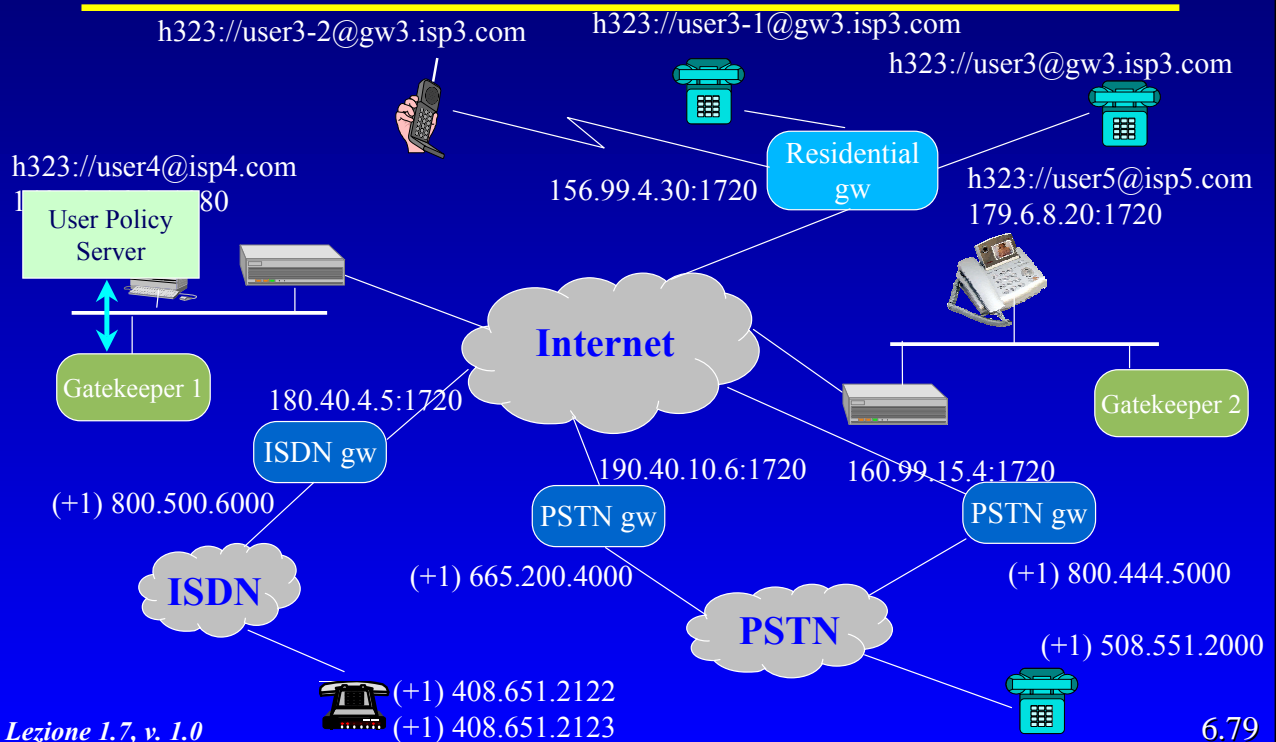
### Chiamate Punto-Punto

# H.225.0 – Instaurazione della chiamata



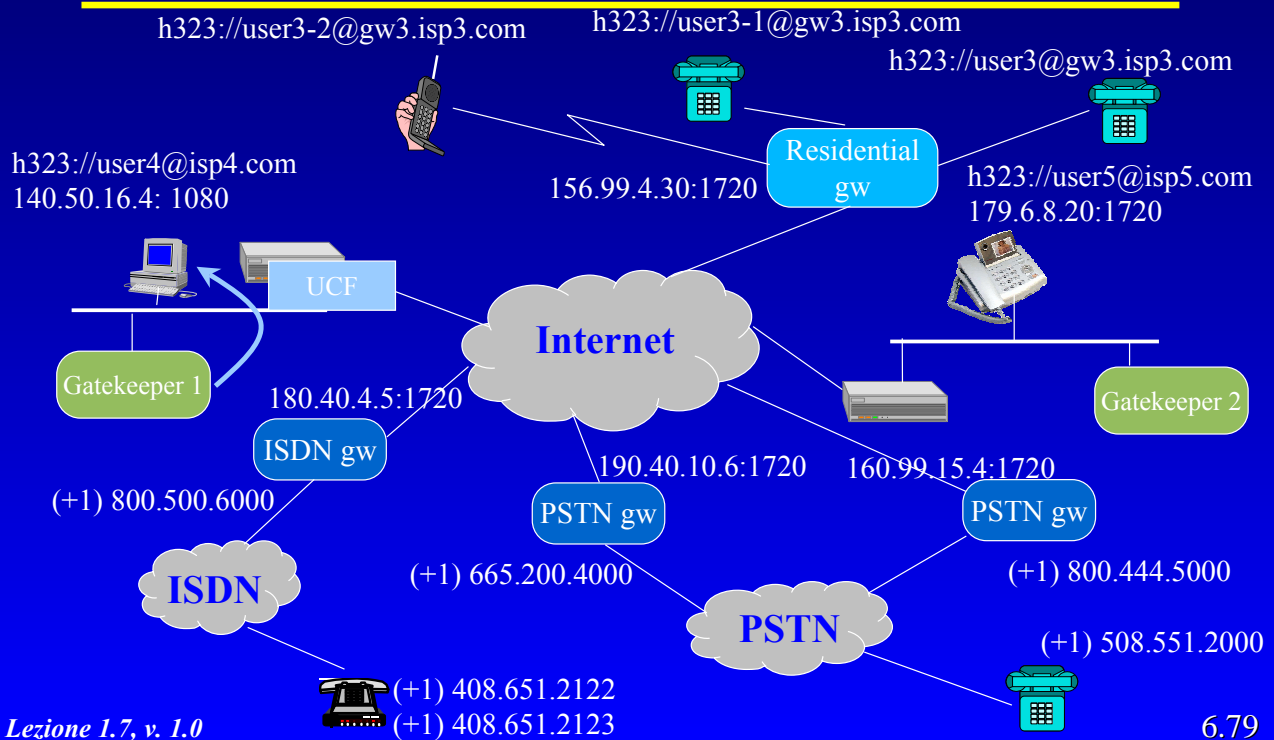
### Chiamate Punto-Punto

# H.225.0 – Instaurazione della chiamata



## Chiamate Punto-Punto

# H.225.0 – Instaurazione della chiamata



## Chiamate Punto-Punto

# Modelli di chiamata

- Segnalazione diretta senza Gatekeeper
  - non esiste una comunicazione RAS con il Gatekeeper;
  - la risoluzione degli indirizzi avviene tramite H.225.0-annex-g o impostazioni manuali.
- Segnalazione diretta
  - il Gatekeeper si limita a risolvere gli indirizzi ed effettuare un controllo di accesso;
  - tutta la segnalazione H.225.0 e H.245 viene scambiata tra gli endpoint.
- Segnalazione Gatekeeper-routed
  - la segnalazione H.225.0 attraversa il Gatekeeper;
  - il Gatekeeper inserisce il proprio IP al posto di quello dell'end-point in fase di risoluzione del nome.

## Segnalazione Gatekeeper-routed

---

- Vantaggi
  - i *Gatekeeper* sono elementi in genere più affidabili degli *endpoint*;
  - utilizzare le informazioni provenienti dagli *endpoint* per la tariffazione non è gradito.
- Svantaggi
  - la scalabilità del *gatekeeper* è limitata, così come il numero di utenti che possono essere serviti.
- La segnalazione H.245
  - può essere scambiata direttamente tra gli *endpoint*;
  - può essere instradata dal *Gatekeeper*
    - » quest'ultima soluzione è la preferita,
    - » riduce ulteriormente la scalabilità del *Gatekeeper*
      - per questa ragione spesso è utilizzata nella modalità tunnel in H.225.0.

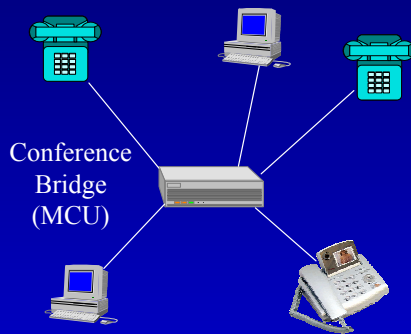
## Conferenze multimediali

---

- Le conferenze multimediali sono caratterizzate:
  - dal tipo di conferenza
    - » meet-me,
    - » ad hoc,
    - » interactive-broadcast;
  - dalla configurazione di rete
    - » multi-unicast,
    - » multicast,
    - » master-slave.

## Conferenze multimediali

# Tipi di conferenze

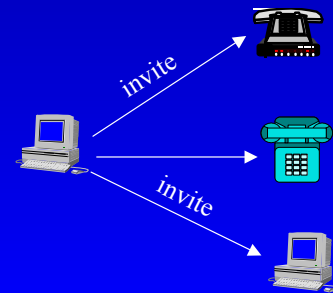


### Meet-me

- I partecipanti conoscono l'indirizzo del bridge e i tempi della conferenza.
- Il bridge mescola le voci delle diverse sorgente e le invia a tutti i partecipanti.
- Il bridge può anche invitare i partecipanti a partecipare alla sessione.

### Ad hoc

- La conferenza parte come una chiamata punto-punto.
- I partecipanti possono invitare altre persone.
- Non è necessario che questo tipo di conferenza sia programmato in anticipo.
- Nella rete PSTN esiste un meccanismo simile a 3 partecipanti che prevede di mettere in attesa la parte attualmente attiva.

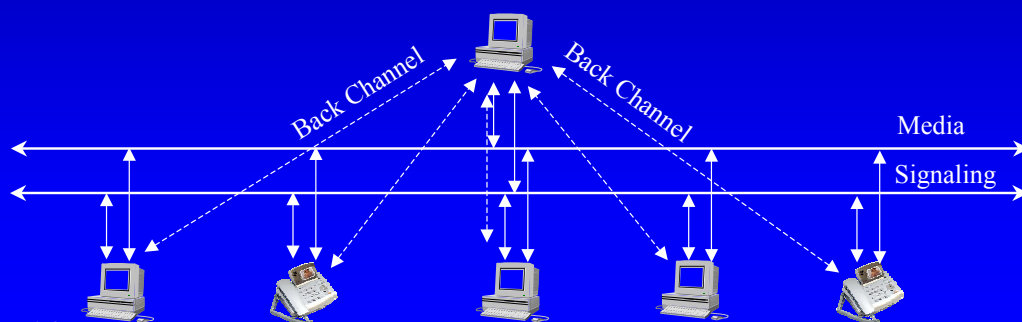


## Conferenze multimediali

# Tipi di conferenze

### Interactive-broadcast

- Una entità invia in broadcast i media e la segnalazione agli altri terminali.
- I terminali hanno un canale di feedback (Back Channel) verso il trasmettitore.
- Questo tipo di conferenza permette la partecipazione di centinaia di partecipanti.



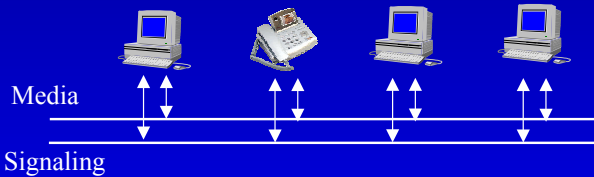
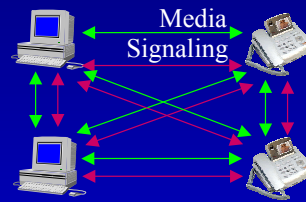
## Conferenze multimediali

# Configurazioni di rete



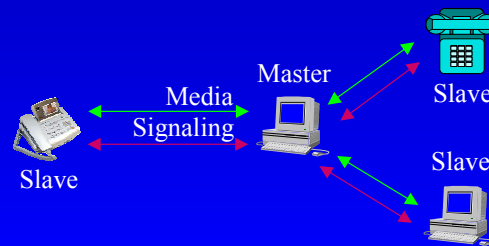
**Point-to-Point**

**Multi-unicast**



**Multicast**

**Master-Slave**



## Conferenze multimediali

# Configurazioni di rete

- Le diverse configurazioni possono essere confrontate sulla base di alcune caratteristiche:
  - semplicità, di implementazione dei terminali,
    - » le stazioni master sono più complesse delle slave;
  - scalabilità;
  - utilizzo della rete;
  - punti critici
    - » il mancato funzionamento di alcuni terminali pregiudica l'intera conferenza;
  - ritardo
  - utilizzabilità con diversi tipi di conferenza
    - » master-slave per meet-me e ad hoc,
    - » multi-unicast per ad hoc,
    - » multicast per interactive-broadcast.

## Conferenze multimediali in H.323

---

- Configurazione di rete
  - la configurazione è diversa per media e segnalazione
    - » per la segnalazione è sempre centralizzata con la configurazione master-slave
      - le funzionalità sono concentrate nel MC (che si può trovare in un terminale, MCU, Gw o Gk);
      - la configurazione multi-unicast non può essere usata perché in H.323 lo stato della conferenza è centralizzato
        - tutte le informazioni concernenti la sessione e i suoi partecipanti risiedono nel MC;

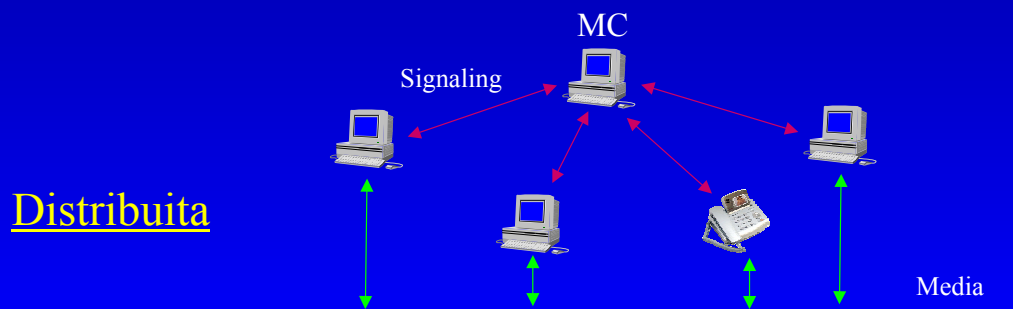
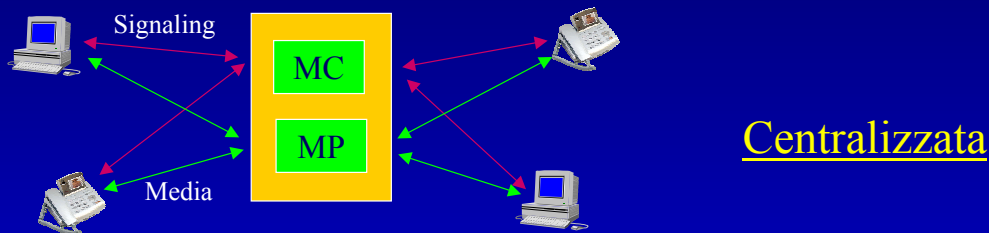
## Conferenze multimediali in H.323

---

- » per i media può essere
  - centralizzata, con la configurazione master-slave,
    - l'entità centrale è rappresentata dal MP (che si può trovare in un MCU, Gw o Gk),
    - l'MP aggrega i flussi provenienti da diverse sorgenti;
  - distribuita, con la configurazione multicast,
    - la distribuzione del media avviene attraverso un indirizzo multicast,
    - ogni terminale aggrega i flussi provenienti dagli altri;
  - ibrida, per es. con l'invio multi-unicast verso il MP e la distribuzione multicast da parte di quest'ultimo elemento.



## Conferenze multimediali in H.323



Lezione 1.7, v. 1.0

6.89

## Conferenze multimediali in H.323

- H.323 prevede conferenze di tipo
  - ad hoc
    - » conferenze su piccola scala (ca 5 partecipanti);
  - meet-me
    - » conferenze su media scala (ca 100 endpoint);
  - a causa della struttura centralizzata per la segnalazione la scalabilità del sistema è limitata dal numero massimo di connessione di segnalazioni supportabile dal MC.
- L'instaurazione di una conferenza H.323 prevede una serie di messaggi lievemente differenti da quelli visti per le comunicazioni punto-punto
  - è necessario comunicare con un MC ed eventualmente un MP.

Lezione 1.7, v. 1.0

6.90

## Servizi supplementari

---

- Le reti telefoniche tradizionali forniscono tutta una serie di servizi accessori
  - trasferimento di chiamata, conferenza, chiamata in attesa;
  - segreteria telefonica, recupero e ascolto dei messaggi e spedizione di fax.
- La telefonia IP
  - deve fornire gli stessi servizi, già noti e richiesti dagli utenti,
  - deve avere la possibilità di fornire nuovi e più avanzati servizi, sfruttando le potenzialità della rete a pacchetto.

## Servizi supplementari

---

- L'adozione dei servizi tradizionali
  - permette una creazione ed una implementazione rapida grazie all'esperienza maturata in passato,
  - richiede di comprendere al meglio le differenze che sorgono nel passare da una rete a commutazione di circuito ad una a pacchetto
    - » la rete IP offre un'interfaccia unificata per lo sviluppo di applicazioni, indipendente dalla rete di trasporto vera e propria,
    - » molte applicazioni possono essere installate in modo molto semplice anche dagli utenti;
  - le differenze rendono la creazione e lo sviluppo di servizi basati su IP molto più veloce e semplice.

## Servizi supplementari in H.323

# Architettura di Segnalazione

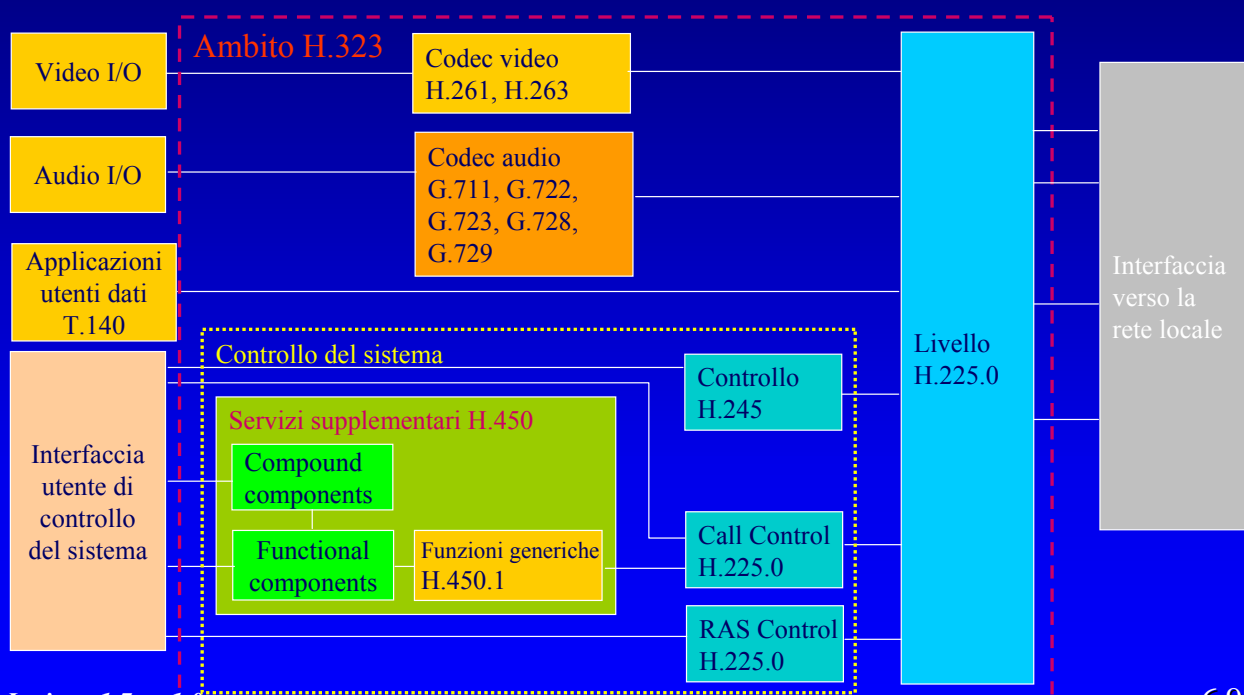
- Le applicazioni di controllo delle chiamate e i servizi supplementari possono essere:
  - *centralizzate*, per es. nel Gk o nel Feature Server
    - » è necessario un protocollo *stimulus* (H.323 Annex L o H.248);
    - » i terminali sono molto semplici e non devono essere aggiornati (es. telefono PSTN);
  - *localizzate in qualsiasi punto della rete* e accessibili tramite un controllo basato su HTTP
    - » questo canale di controllo può essere utilizzato anche per fornire una interfaccia utente per H.450, l'aggiornamento del software, l'invio di messaggi pubblicitari;
  - *distribuite* sugli endpoint ed i server
    - » interagiscono tra di loro attraverso protocolli peer-to-peer (H.323/H.450);
    - » è necessario prevedere meccanismi in grado di gestire le richieste quando il terminale interessato non sia attivo.

Lezione 1.7, v. 1.0

6.93

## Servizi supplementari in H.323

# Architettura di Segnalazione H.450



Lezione 1.7, v. 1.0

6.94

## Sicurezza in H.323

---

- Sicurezza dei messaggi di segnalazione
  - autenticazione degli utenti;
  - generazione di chiavi segrete;
  - cifratura dei canali di comunicazione tramite IPSec/TLS;
  - scambio di opzioni di sicurezza tra gli endpoint;
  - anonimato, quando l'indirizzo fisico del peer non è noto.
- Sicurezza dei flussi dei media
  - apertura di canali confidenziali per i media;
  - generazione, distribuzione e rinnovo delle chiavi per la cifratura;
  - tecniche di segretezza: cifratura a livello RTP, IPSec, ...

## Sicurezza in H.323

### Generazione di una chiave segreta

---

- I meccanismi a chiave segreta sono preferiti per la cifratura di grosse quantità di dati.
- Per la generazione di una chiave segreta comune si può utilizzare una:
  - una password
    - » ci sono diversi meccanismi,
    - » H.323 utilizza ISO 9798-2;
  - il meccanismo Diffie-Hellman
    - » richiede un meccanismo di autenticazione, un canale sicuro o una preliminare autenticazione a chiave pubblica.

**Sicurezza in H.323****Autenticazione**

- L'identità della parti coinvolte nell'autenticazione deve essere verificata:
  - meccanismi a chiave condivisa/segreta
    - » cifratura di campi noti ad entrambe le parti,
    - » generazione di un hash a partire da messaggi che contengano la chiave;
    - » l'autenticazione può avvenire tramite messaggi RAS, H.225.0 o H.245;
    - » non fornisce la non-repudiabilità!
  - meccanismi a chiave pubblica.
- L'autenticazione spesso è desiderabile anche per i messaggi di controllo RAS/H.225.0/H.245
  - genera un codice di autenticazione (MAC)
    - » utilizza gli stessi meccanismi dell'autenticazione utente, di solito ha valore end-to-end.

**Sicurezza in H.323****Segretezza dei canali logici**

- Sicurezza del canale H.225.0
  - TLS/IPSec,
  - necessitano della negoziazione di TLS o IPSec
    - » i canali H.225.0 con TLS utilizzano la porta 1300;
- Sicurezza del canale H.245
  - i messaggi H.225.0 possono essere utilizzati per negoziare i meccanismi di sicurezza per H.245,
  - TLS/IPSec/meccanismi non standard;
- Sicurezza del flusso dei media
  - cifratura a livello RTP/IPSec,
  - distribuzione della chiave a tutti i partecipanti.

## Segretezza del canale di trasporto

---

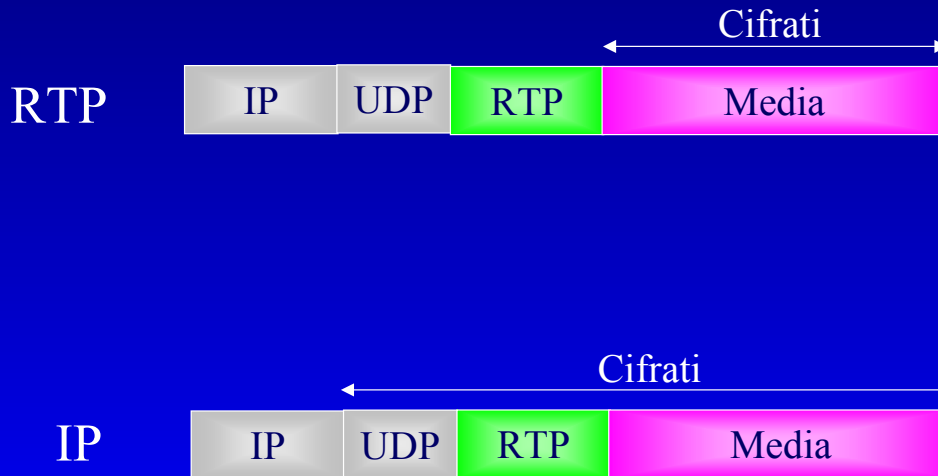
- Distribuzione della chiave
  - la generazione della chiave è compito del master;
  - la distribuzione deve avvenire in modo sicuro:
    - » un canale H.245 cifrato,
    - » la cifratura tramite una chiave condivisa fra i partecipanti,
    - » la cifratura tramite la chiave pubblica dello slave;
  - la distribuzione può avvenire anche a flusso già attivo
    - » inizio cifratura, refresh della chiave.

## Segretezza del canale di trasporto

---

- Cifratura a livello RTP
  - gli header non sono cifrati;
  - ogni pacchetto è cifrato in modo indipendente
    - » tolleranza delle perdite;
  - cifratura a blocchi
    - » ECB, CBC, OFB, CFB possono essere utilizzati,
    - » l'IV viene calcolato come una funzione del Sequence Number e del Timestamp;
    - » *stealing* o *padding* per l'ultimo blocco
      - *stealing*, se l'uscita dell'ultima cifratura non ha la stessa dimensione del blocco di cifratura,
      - *padding*, richiede di settare il relativo bit a 1 nell'intestazione RTP.

## Sicurezza in H.323

**Segretezza del canale di trasporto**

## Sicurezza in H.323

**Profili di sicurezza**

- H.235 prevede diversi servizi di sicurezza
  - esistono diversi meccanismi per realizzare lo stesso obiettivo,
  - esistono diversi algoritmi che possono essere utilizzati.
- La flessibilità nella scelta di meccanismi ed algoritmi può risultare in un scarsa interoperabilità degli apparati.
- H.235 definisce quindi dei profili di sicurezza:
  - *Baseline Security Profile*,
  - *Signature Security Profile*.

**Sicurezza in H.323****Profili di sicurezza**

---

**● Baseline Security Profile**

- autenticazione ed integrità per RAS, H.225.0 e H.245
  - » meccanismo di hash basato su chiave segreta derivata da password,
  - » meccanismo di chiamate Gatekeeper routed,
  - » l'algoritmo utilizzato è HMAC-SHA1-96 (96 bit);
- segretezza per i flussi dei media (opzionale)
  - » la chiave di sessione viene distribuita dopo essere stata cifrata mediante un valore segreto generato da uno scambio Diffie-Hellman non autenticato,
  - » gli algoritmi utilizzati per la cifratura sono RC2, DES (56 bit) o triplo DES (168 bit).

**● Signature Security Profile**

- autenticazione, integrità e non repudiabilità per RAS, H.225.0 e H.245
  - » meccanismi a chiave pubblica: RSA-SHA1 o RSA-MD5;
- segretezza dei flussi dei media (opzionale).

*Lezione 1.7, v. 1.0*

6.103

**Sicurezza in H.323****H.323 e firewall**

---

- La presenza di firewall non è trasparente ai sistemi H.323
  - solo la porta H.225.0 è statica (1720),
  - molti canali logici utilizzano UDP.
- La presenza di porte dinamiche rende necessario l'utilizzo di firewall in grado di analizzare ed interpretare il traffico H.323
  - *Application Level Gateway (AGL)* o proxy H.323.

*Lezione 1.7, v. 1.0*

6.104



## Sicurezza in H.323

# Tipi di firewall

### ● *Packet filter*

#### – statici

- » hanno una configurazione statica,
- » le regole si basano sui campi dell'intestazione IP/TCP (indirizzi IP, porte TCP, flag),
- » non permettono l'accesso al traffico UDP
  - non è possibile identificare una connessione;
- » non sono adatti per essere utilizzati con H.323
  - il traffico UDP non può attraversarli (RAS, flussi multimediali),
  - i canali H.245 utilizzano porte dinamiche,
  - le connessioni TCP dei canali H.245 non possono essere avviate dall'esterno.

## Sicurezza in H.323

# Tipi di firewall

a.b.\*.\* rappresenta la rete "interna"

Source IP	Destination IP	Source port	Destination Port	Transport protocol	Flags	Action
a.b.c.1	*	*	25	TCP		Deny
a.b.*.*	*	*	25	TCP		Allow
*	a.b.*.*	25	*	TCP	ACK	Allow
a.b.c.1	*	*	1720	TCP/UDP		Deny
a.b.*.*	*	*	1720	TCP /UDP		Allow
*	a.b.*.*	1720	*	TCP	ACK	Allow
x.y.z.*	a.b.*.*	*	25	TCP		Allow
x.y.z.*	a.b.*.*	*	1720	TCP /UDP		Allow
*.*.*.*	*.*.*.*	*	*	TCP		Deny

## Tipi di firewall

---

- Stateful packet filter
  - » le informazioni sono aggiornate dinamicamente sulla base delle informazioni provenienti dal flusso,
  - » viene mantenuto uno stato relativo alle connessioni TCP/UDP
    - in genere il termine di una connessione UDP è identificata da un timeout,
  - » il traffico UDP è quindi gestito in maniera più efficiente,
  - » rimangono alcune problematiche in H.323
    - le connessioni H.245 utilizzano porte dinamiche,
    - le connessioni TCP/UDP inizializzate da host esterni.

## Tipi di firewall

---

- *Circuit gateway*
  - prevedono la creazione di circuiti logici (connessioni TCP) tra gli host,
    - » il traffico sui circuiti logici può attraversare il firewall;
  - il più diffuso è il server SOCKS
    - » il client effettua una connessione sulla porta 1080 del server,
    - » il server esegue una autenticazione/autorizzazione del client,
    - » il client specifica l'host remoto ed il server assegna un indirizzo/porta a cui inviare i pacchetti
      - il server SOCKS agisce come intermediario fra i due host;
  - per quanto riguarda H.323, anche questi firewall presentano l'inconveniente di non essere in grado di esaminare il contenuto delle comunicazioni H.225.0 e H.245.

## Tipi di firewall

---

- **Application Level Gateway o Proxy**
  - funzionano a livello di applicazione;
  - interpretano i messaggi H.323
    - » sono in grado di capire quali porte devono essere aperte dinamicamente,
    - » possono effettuare un controllo sul traffico trasmesso;
  - vantaggi:
    - » sono più sicuri dei firewall a ispezione di pacchetti,
    - » sono l'unico meccanismo funzionante in presenza di NAT;
  - svantaggi:
    - » gestiscono le singole connessioni (scalabilità),
    - » sono lenti in confronto ai firewall a ispezione di pacchetti,
    - » sono inefficaci in presenza di una cifratura end-to-end del traffico.

## H.323 e NAT

---

- **Esistono diverse tipologie di NAT**
  - NAT di base: traduzione 1 a 1 degli indirizzi;
  - NATPT: gli indirizzi privati vengono tradotti in un unico indirizzo pubblico;
  - NAT bidirezionale: gli host nella rete privata possono essere accessibili dall'esterno
    - » l'individuazione degli host deve essere globalmente unica (si possono usare delle URI);
  - Twice NAT: utilizzo di indirizzi pubblici non annunciati al di fuori della rete privata;
  - Multi-homed NAT: presenza di più server NAT per ridondanza.

## Sicurezza in H.323

# H.323 e NAT

---

- In presenza di NAT, è necessario modificare gli indirizzi privati contenuti all'interno
  - l'utilizzo di un proxy o ALG permette di risolvere questo problema.
- In alternativa è possibile utilizzare *Realm Specific IP (RSIP)*
  - un server RSIP assegna su richiesta un numero limitato di indirizzi pubblici ai client.

## La mobilità in H.323

---

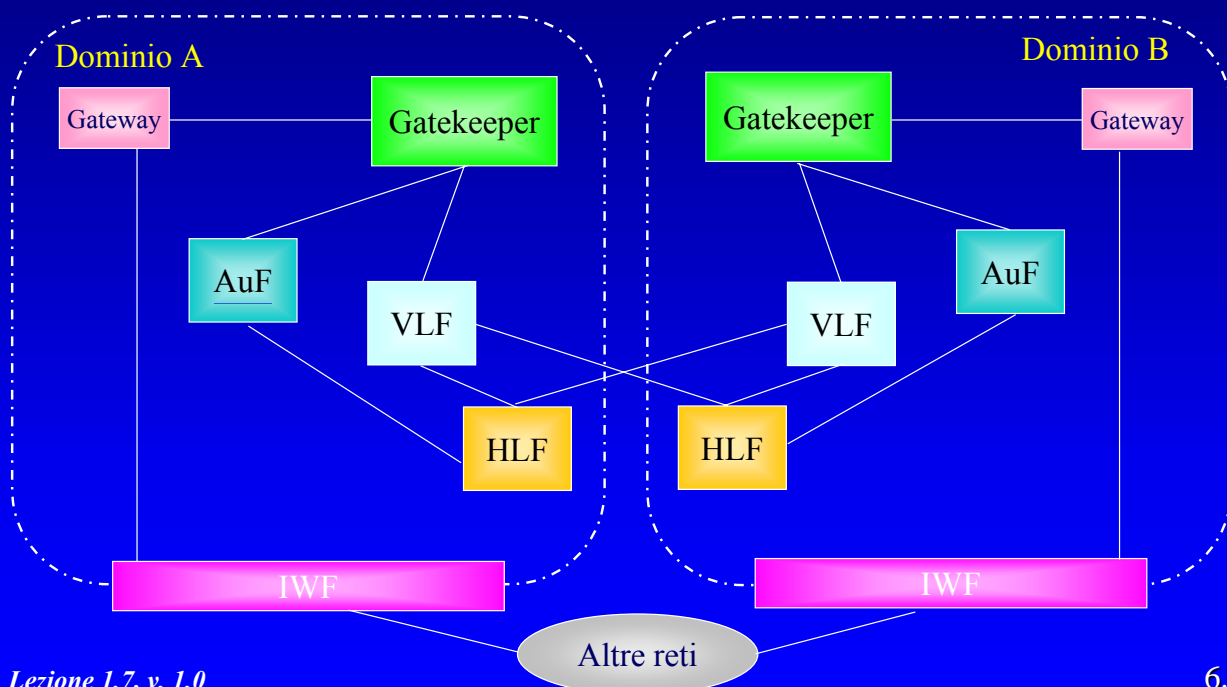
- La mobilità può essere intesa come:
  - *mobilità degli utenti*
    - » gli utenti hanno la possibilità di utilizzare diversi tipi di terminale, connessi a reti differenti;
    - » accesso a servizi fonici tramite PC, telefono GSM;
  - *mobilità dei terminali*
    - » la possibilità di mantenere la sessione attiva su un terminale durante uno spostamento geografico;
    - » *mobilità continua o discreta*;
  - *mobilità dei servizi*
    - » la possibilità di ottenere gli stessi servizi, indipendentemente dalla mobilità dell'utente o dei terminali;
    - » consiste in un profilo utente ed un'interfaccia sempre accessibile agli utenti.

## La mobilità in H.323

**Architettura di rete**

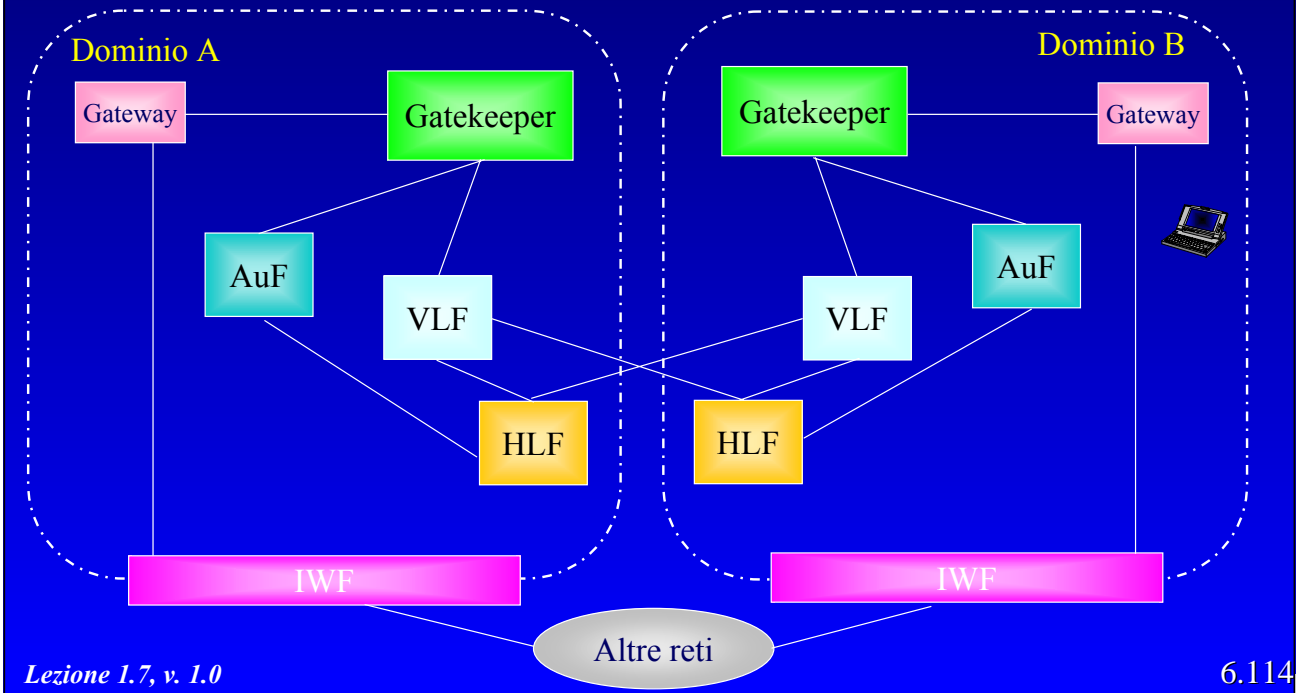
- La mobilità richiede l'introduzione di alcune entità funzionali:
  - *Home Location Function (HLF)*,
    - » permette di risalire alla posizione attuale dell'utente;
  - *Visitor Location Function (VLF)*,
    - » tiene traccia degli utenti ospiti all'interno del dominio;
  - *Authentication Function (AuF)*,
    - » associata ad un HLF,
    - » verifica l'autenticità di un utente,
    - » genera una chiave di sessione per comunicazioni sicure;
  - *Interworking Function (IWF)*,
    - » effettua la conversione di protocollo tra H.323 e il protocollo utilizzato in un'altro tipo di rete.

## La mobilità in H.323

**Aggiornamento della posizione**

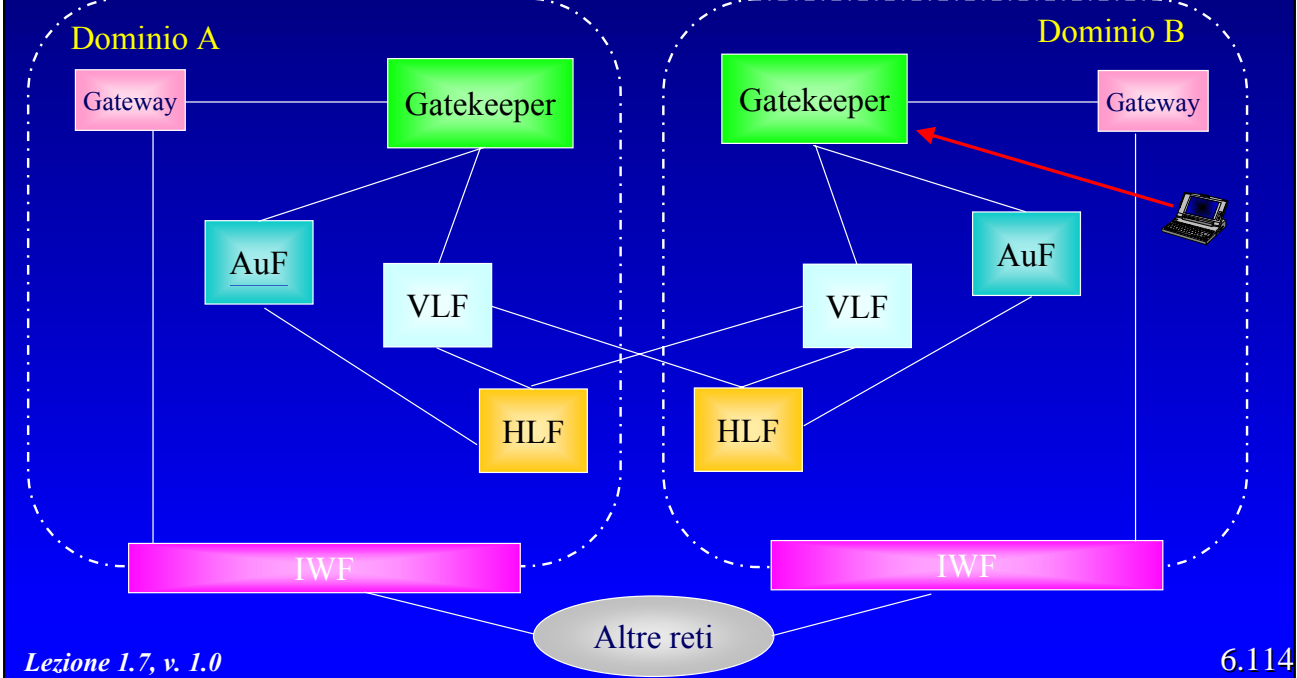
### La mobilità in H.323

## Aggiornamento della posizione



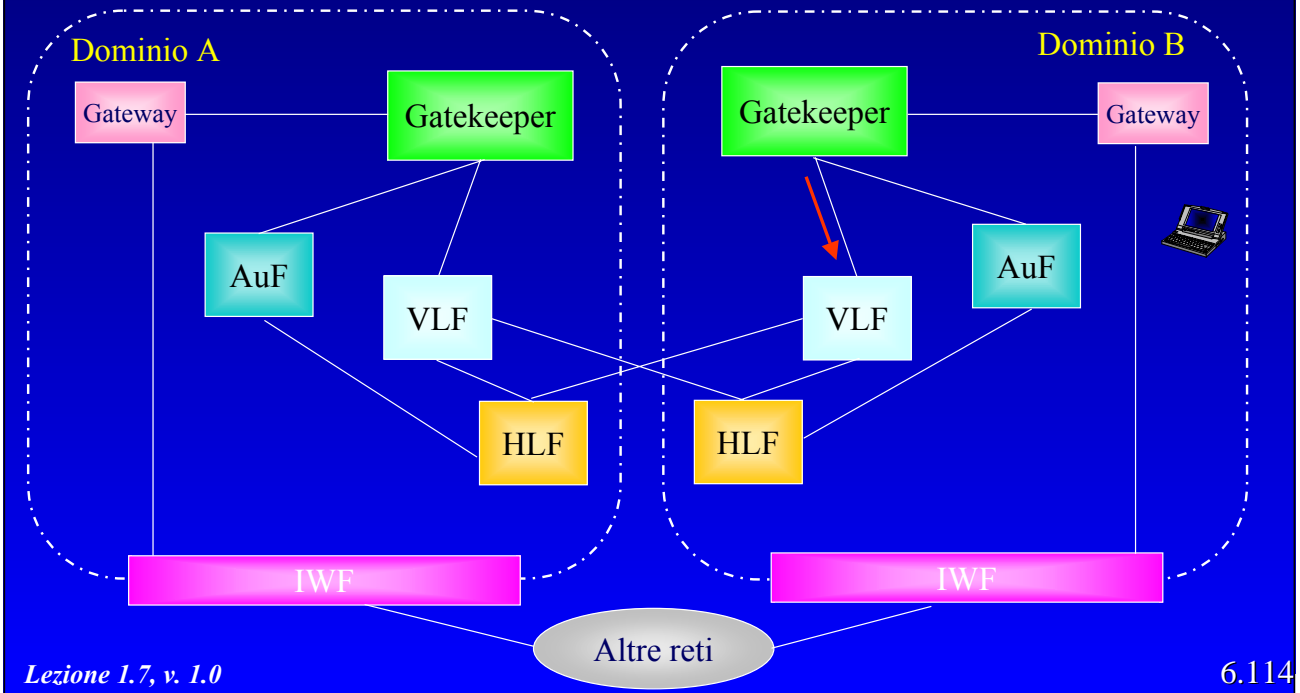
### La mobilità in H.323

## Aggiornamento della posizione



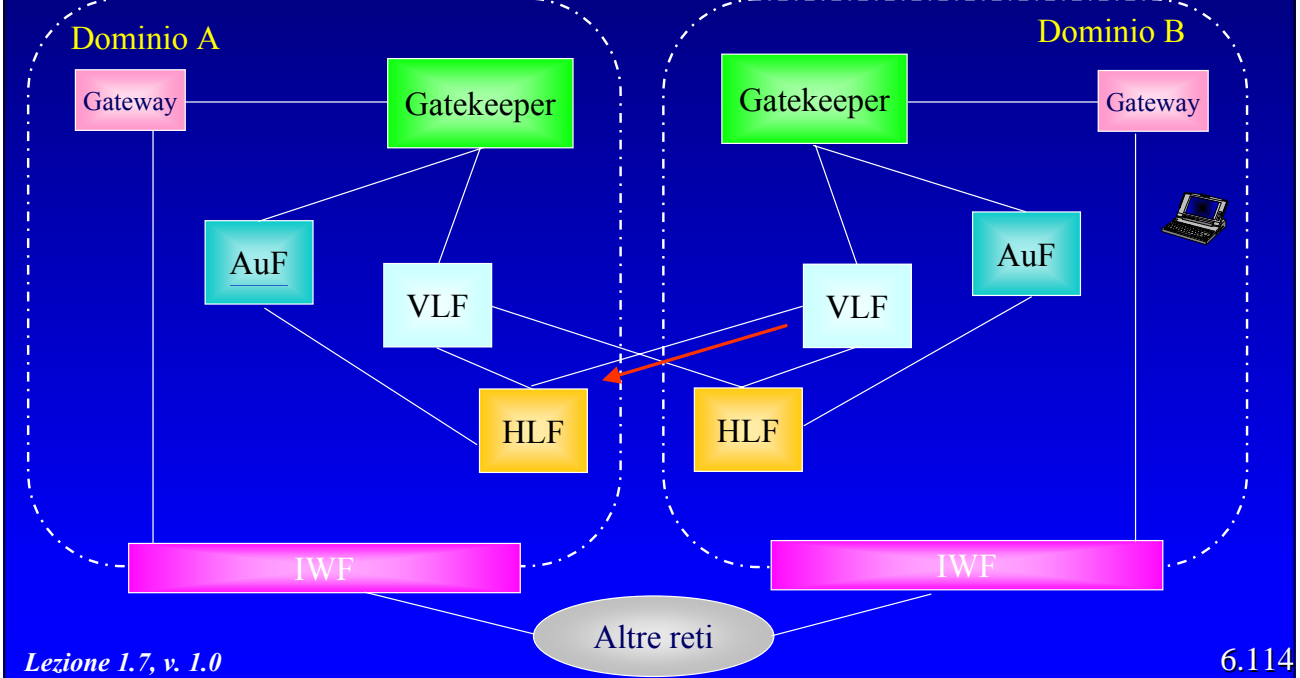
### La mobilità in H.323

## Aggiornamento della posizione



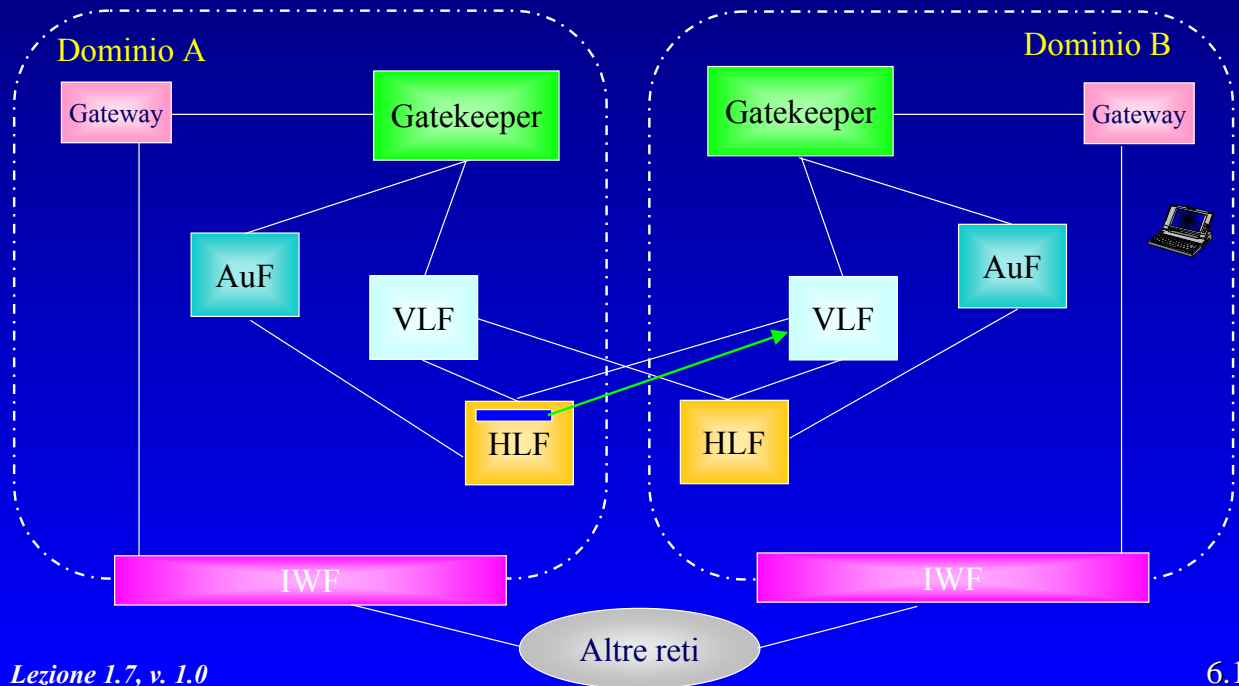
### La mobilità in H.323

## Aggiornamento della posizione



### La mobilità in H.323

## Aggiornamento della posizione



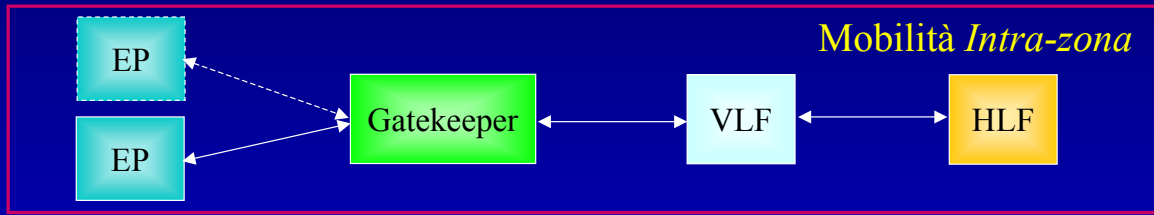
### La mobilità in H.323

## Aggiornamento della posizione



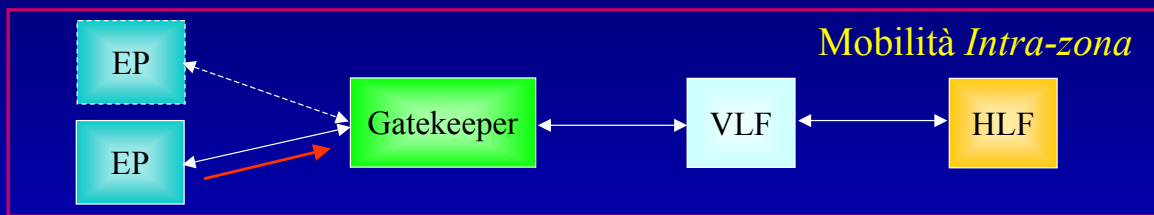
### La mobilità in H.323

## Aggiornamento della posizione



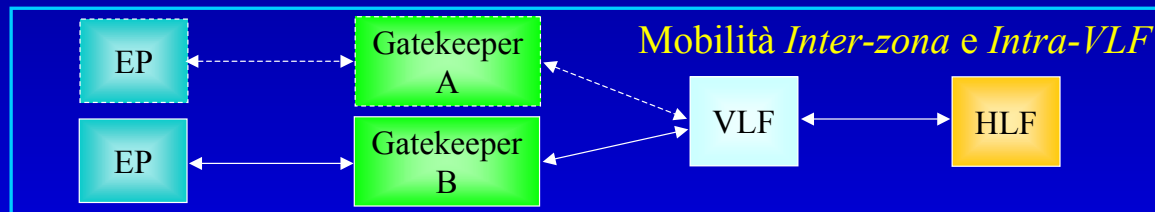
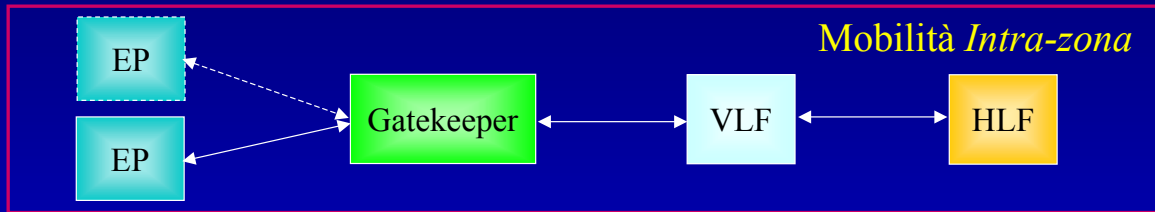
### La mobilità in H.323

## Aggiornamento della posizione



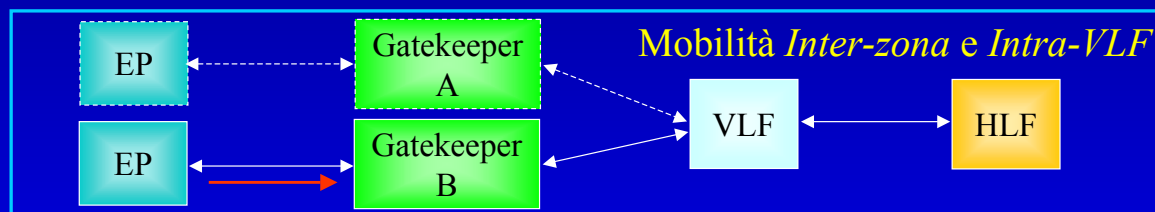
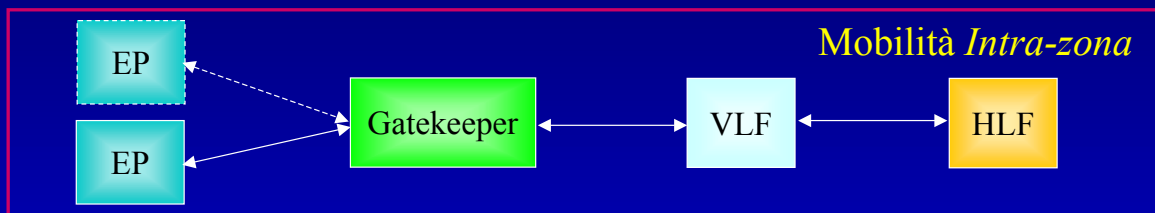
### La mobilità in H.323

## Aggiornamento della posizione



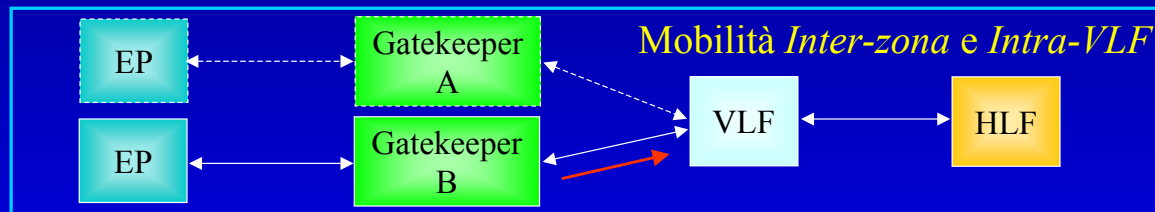
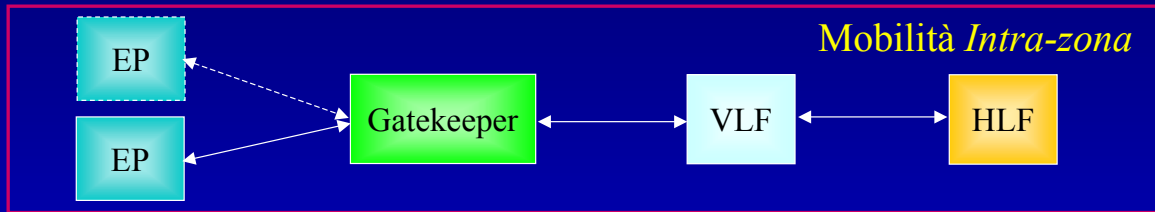
### La mobilità in H.323

## Aggiornamento della posizione



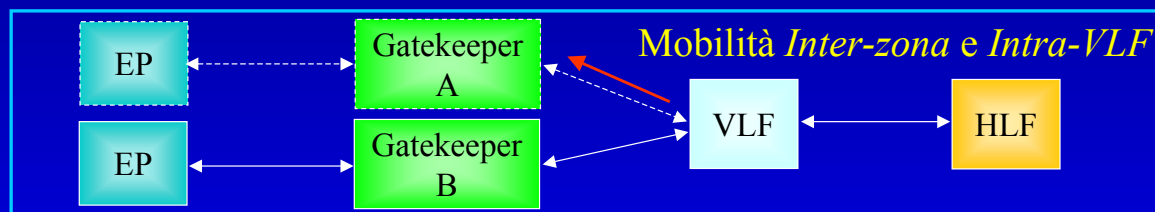
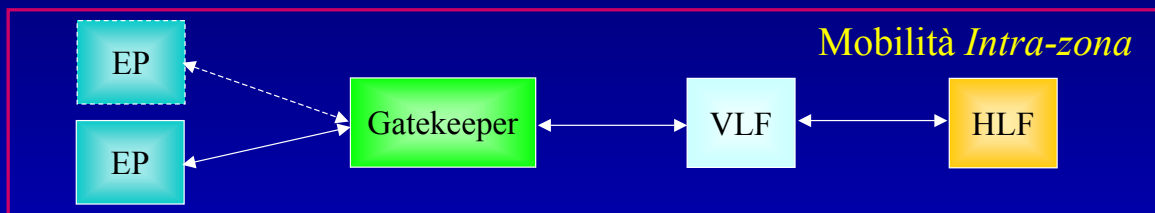
### La mobilità in H.323

## Aggiornamento della posizione



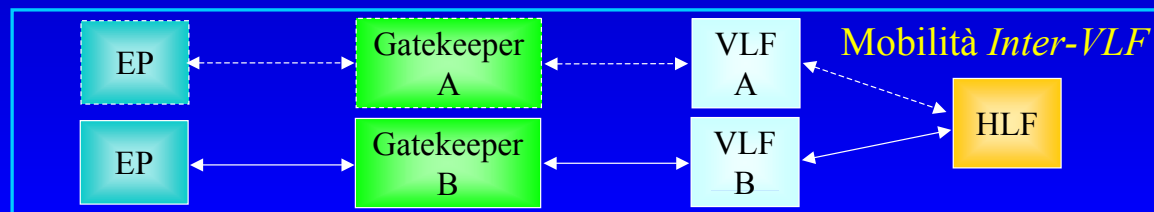
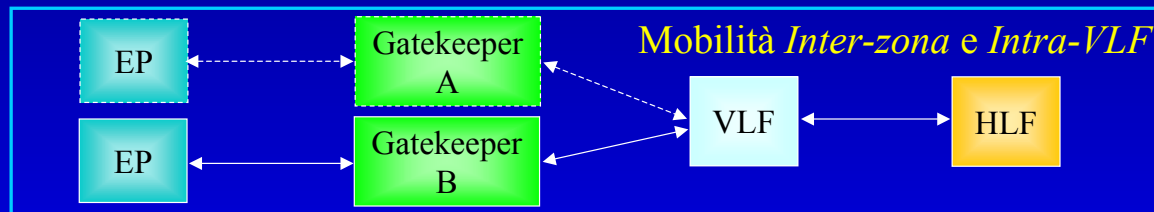
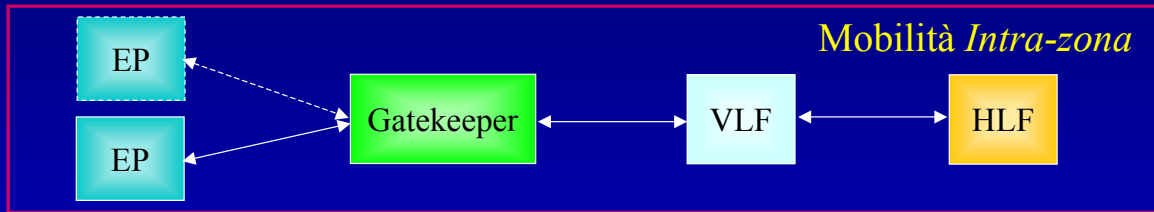
### La mobilità in H.323

## Aggiornamento della posizione



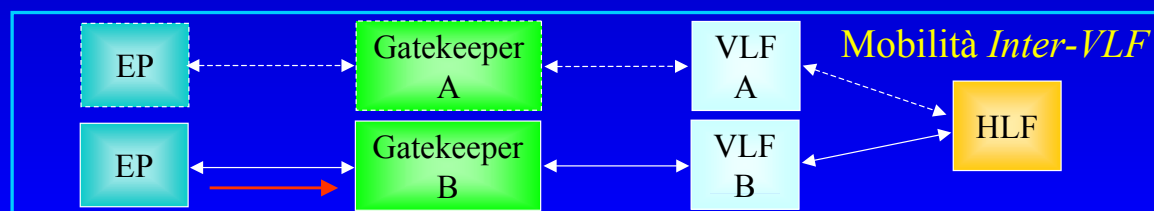
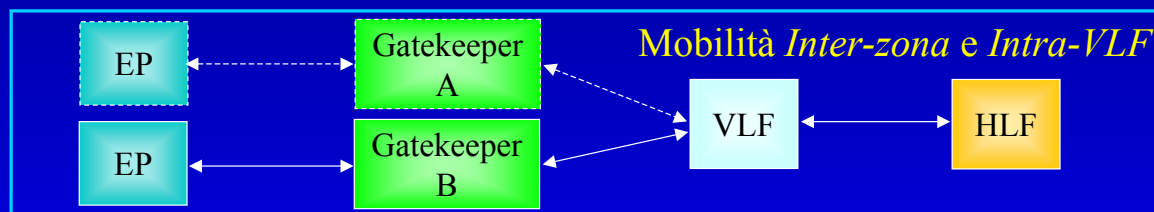
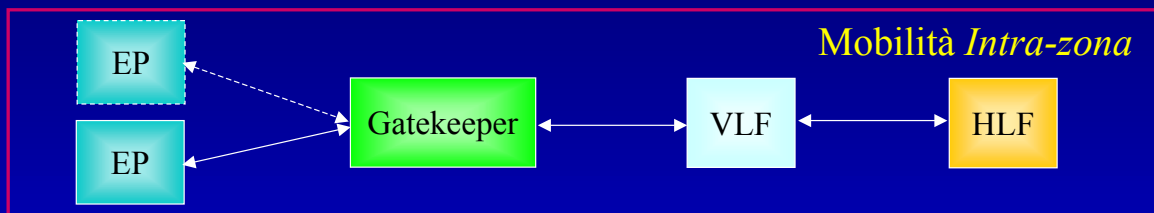
### La mobilità in H.323

## Aggiornamento della posizione



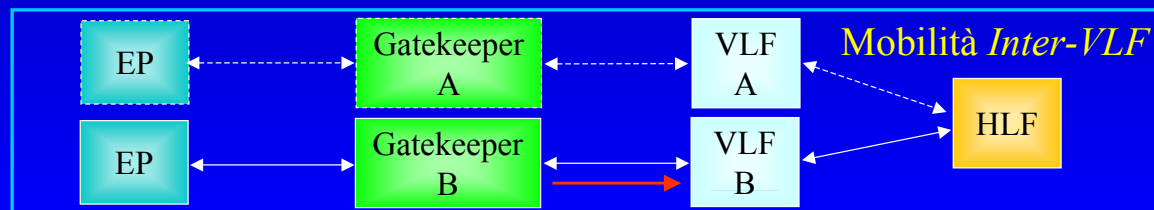
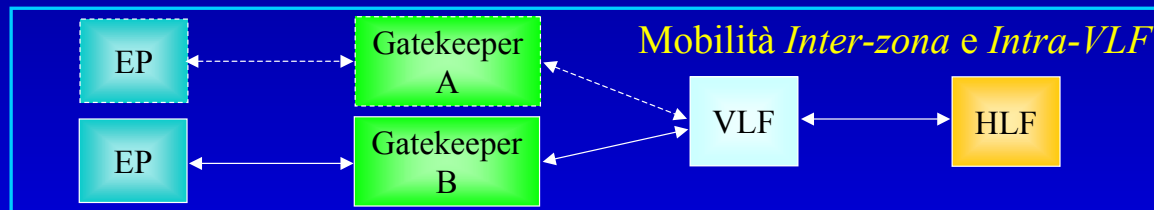
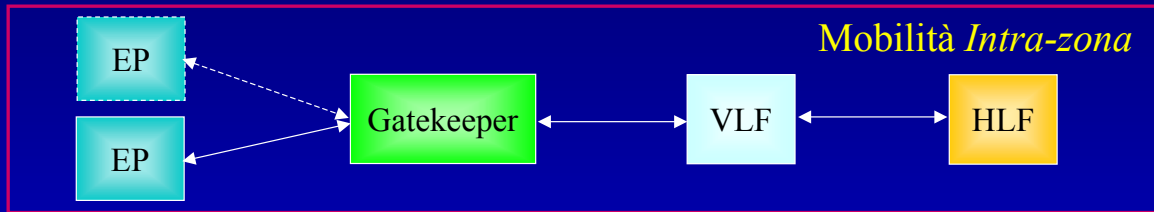
### La mobilità in H.323

## Aggiornamento della posizione



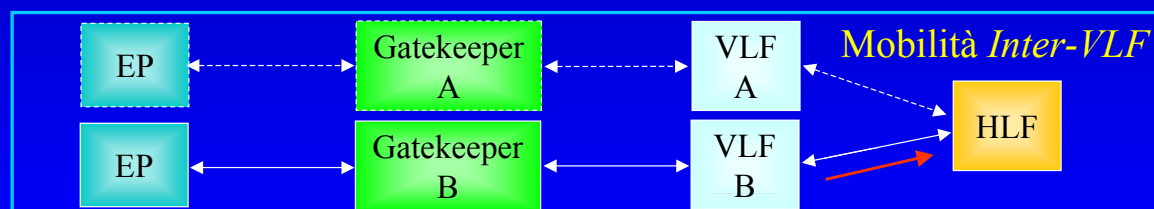
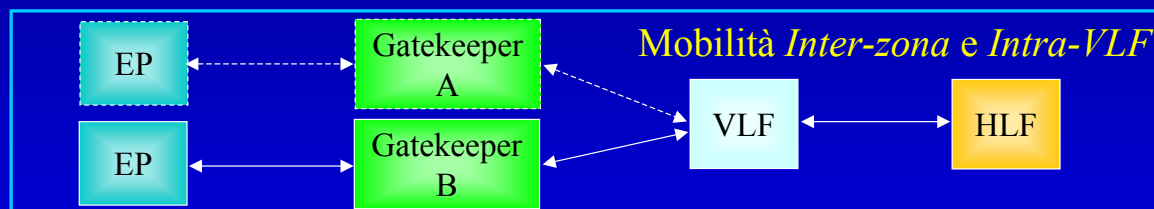
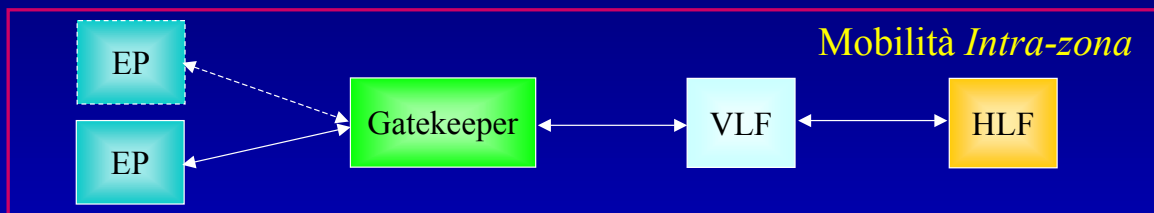
### La mobilità in H.323

## Aggiornamento della posizione



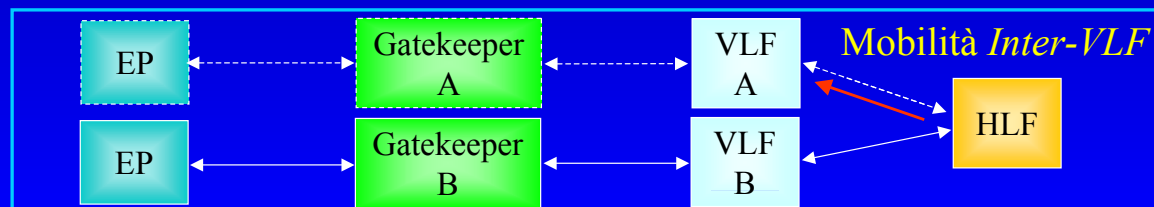
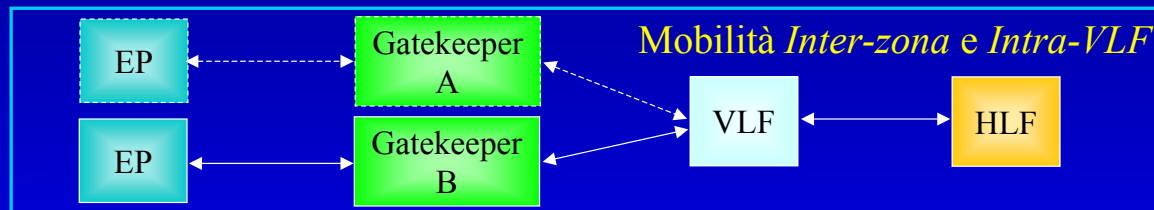
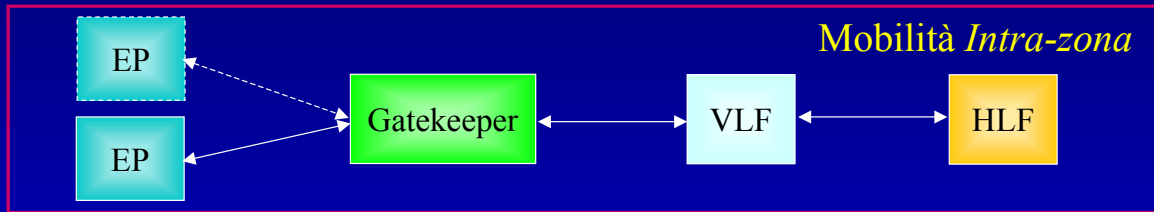
### La mobilità in H.323

## Aggiornamento della posizione



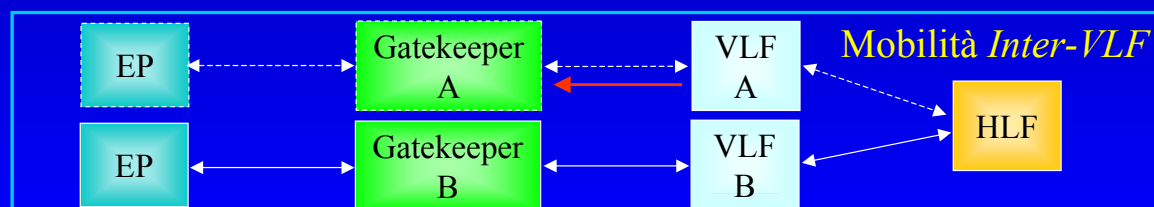
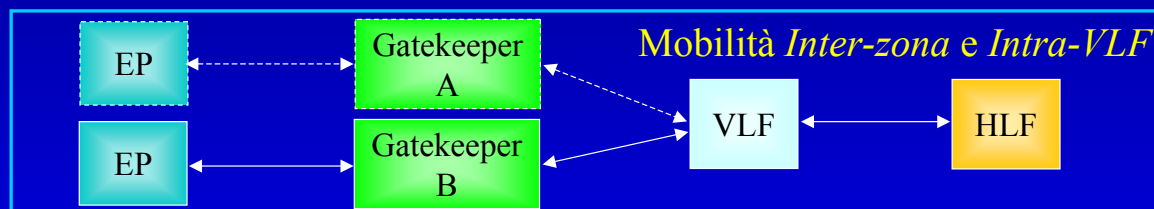
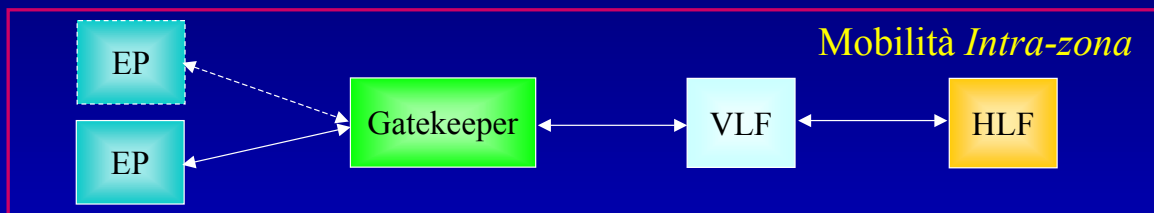
### La mobilità in H.323

## Aggiornamento della posizione

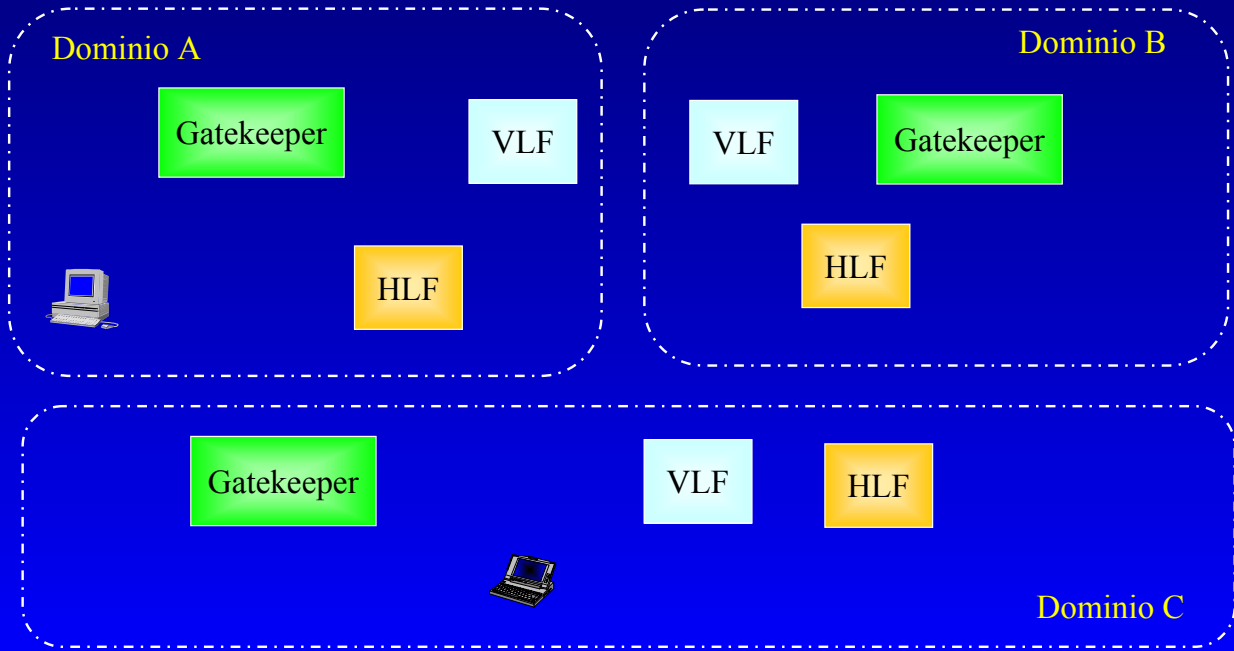


### La mobilità in H.323

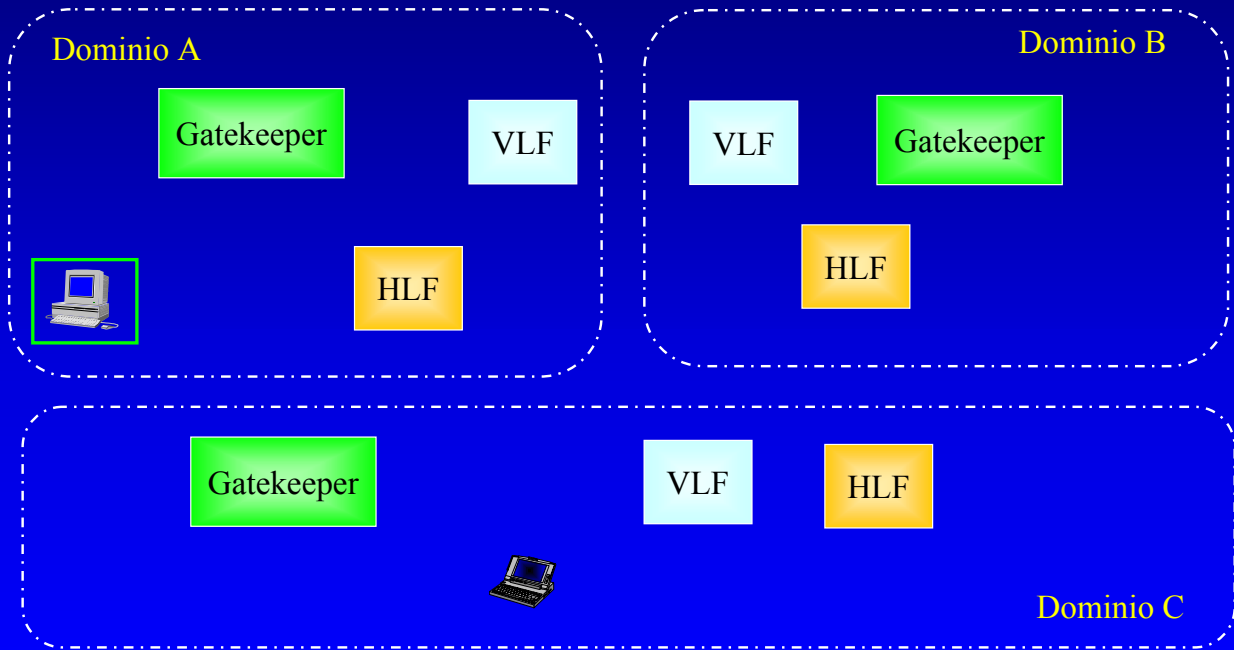
## Aggiornamento della posizione



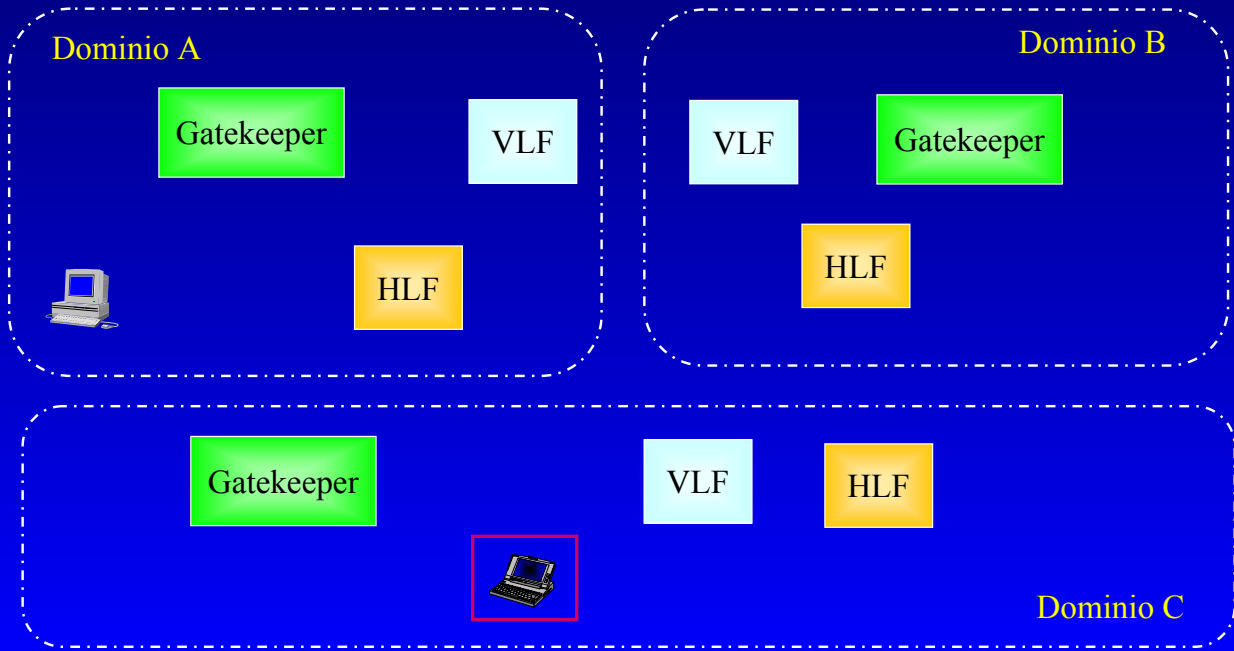
# La mobilità in H.323 Chiamate



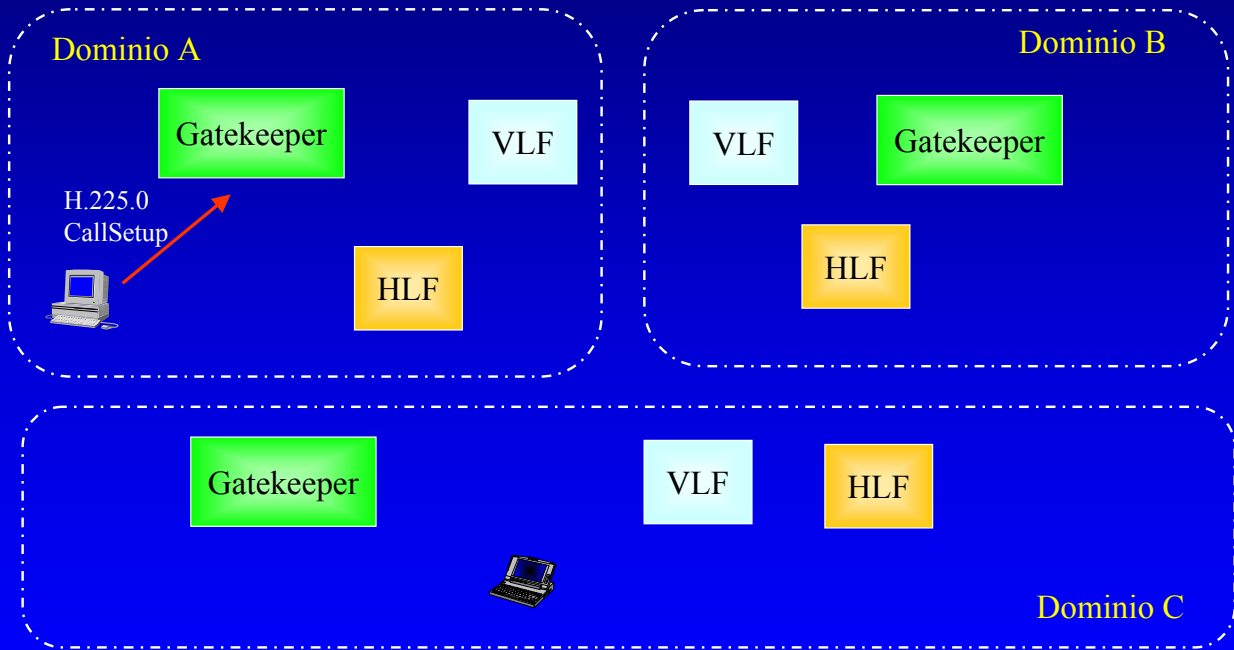
# La mobilità in H.323 Chiamate



# La mobilità in H.323 Chiamate

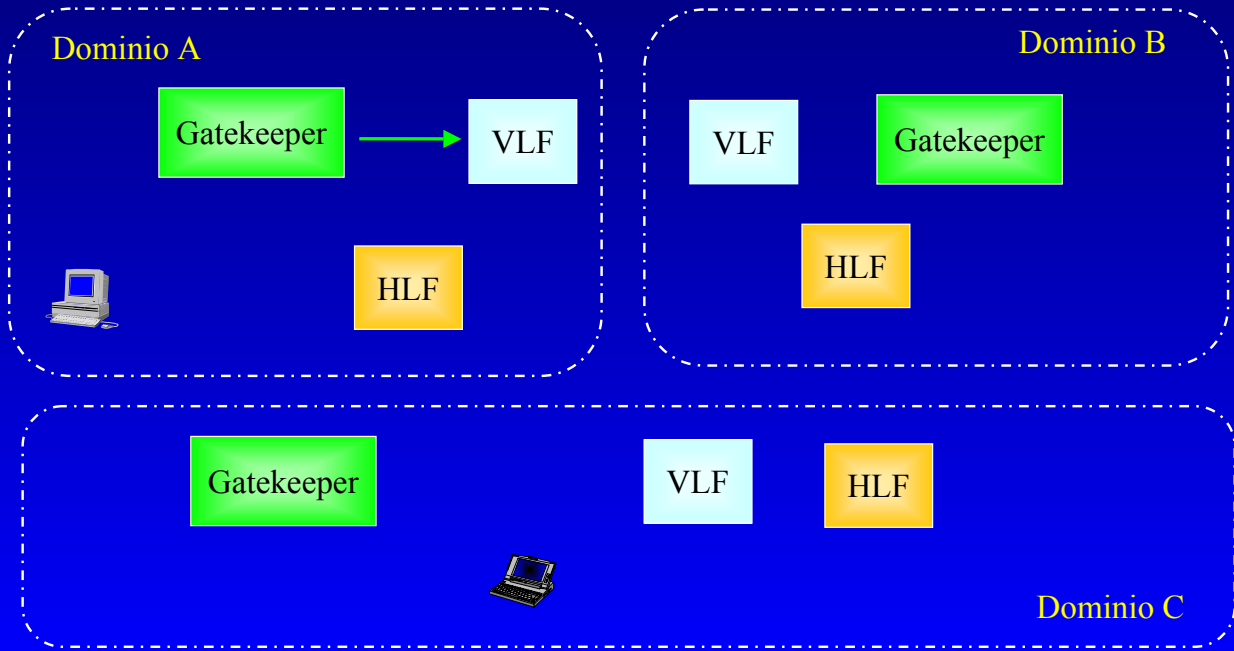


# La mobilità in H.323 Chiamate

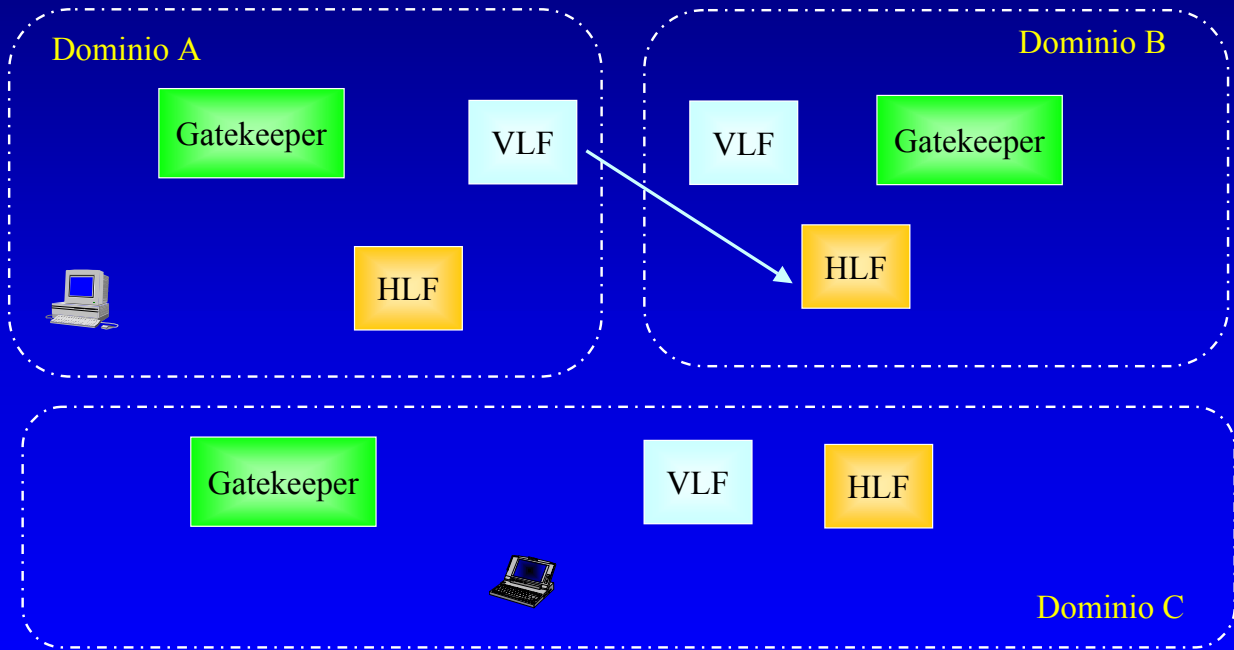




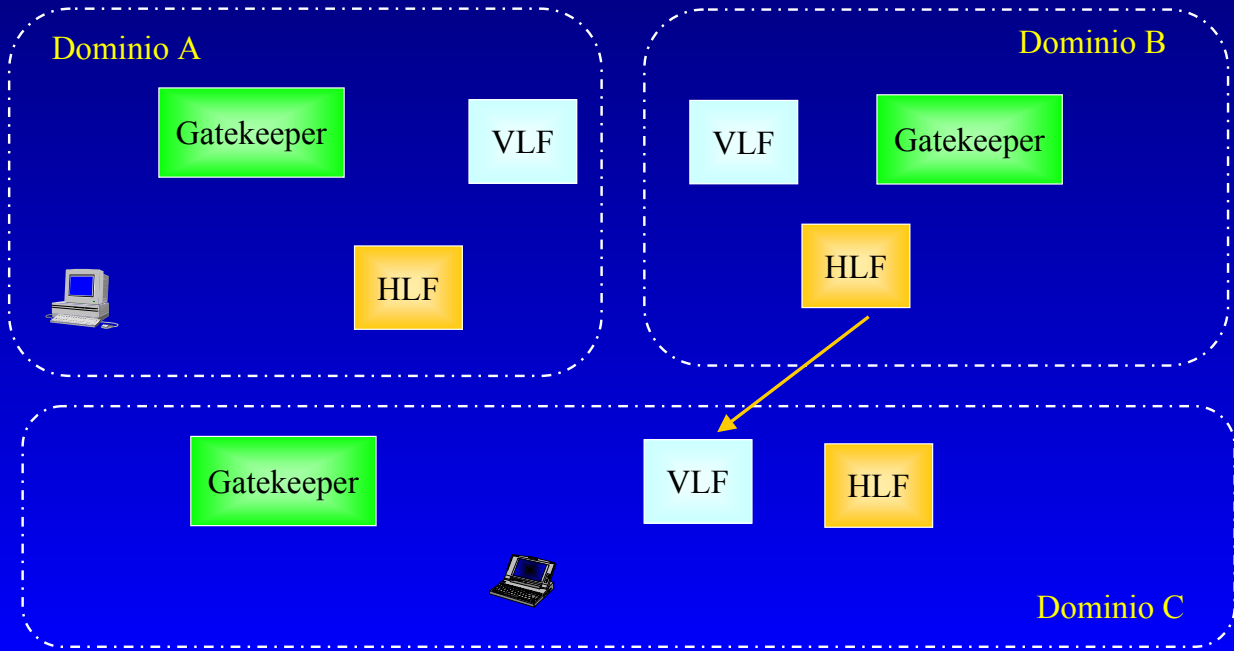
# La mobilità in H.323 Chiamate



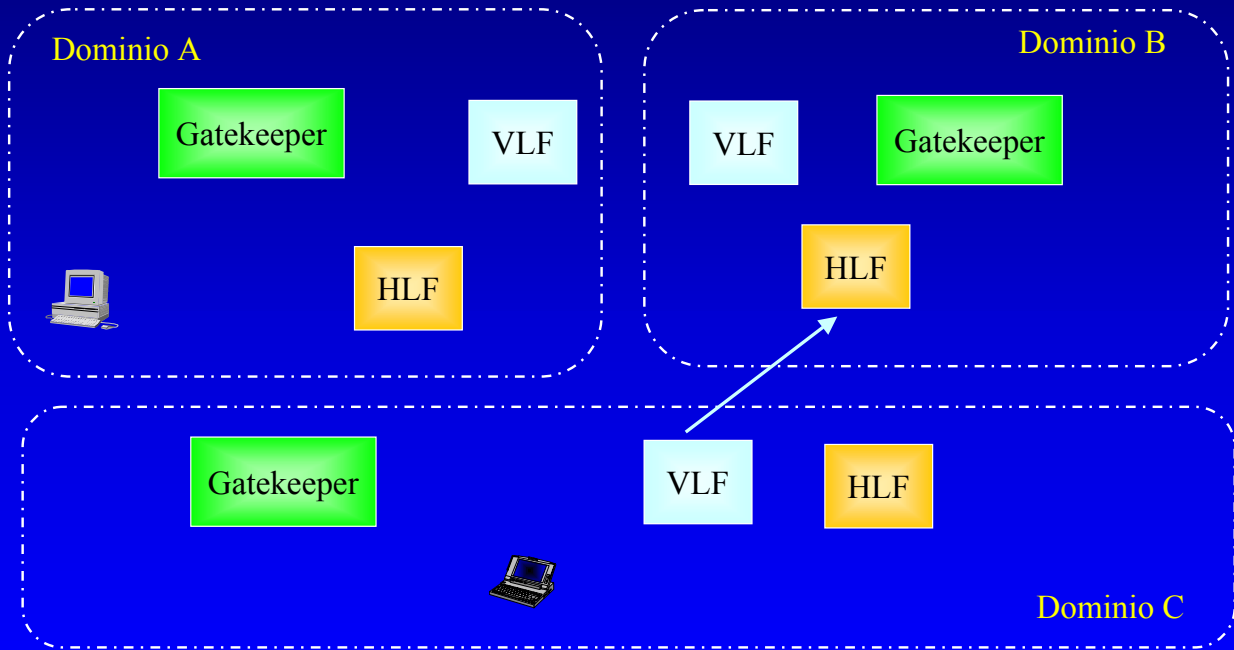
# La mobilità in H.323 Chiamate



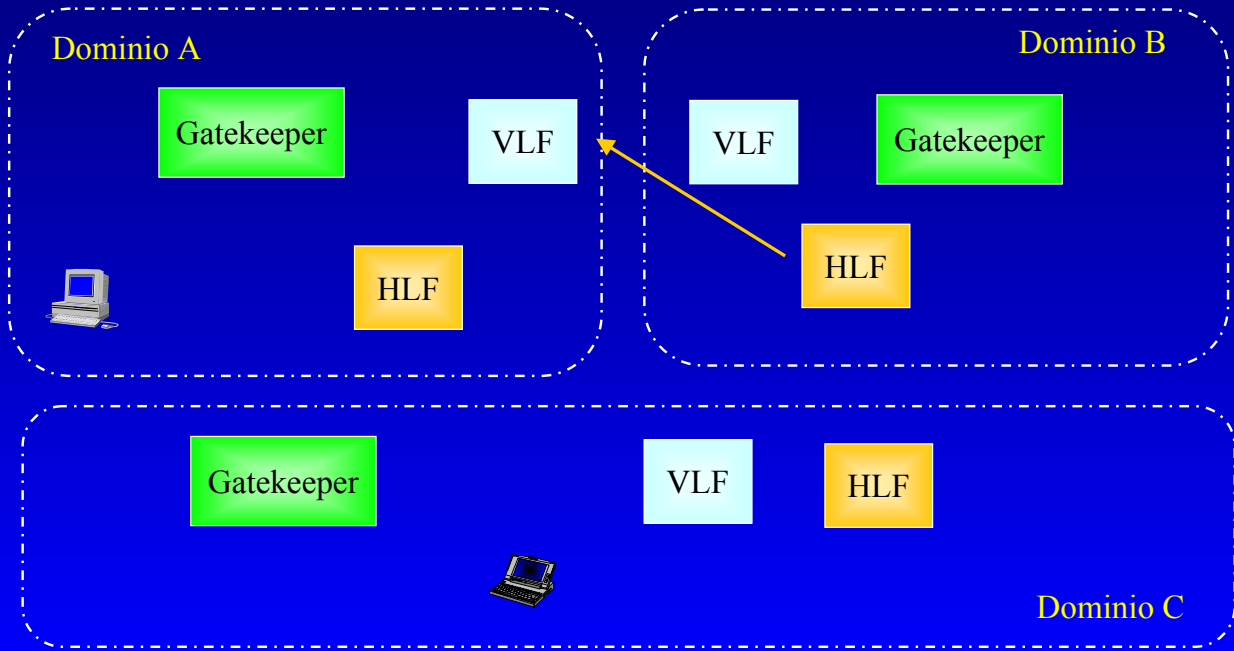
# La mobilità in H.323 Chiamate



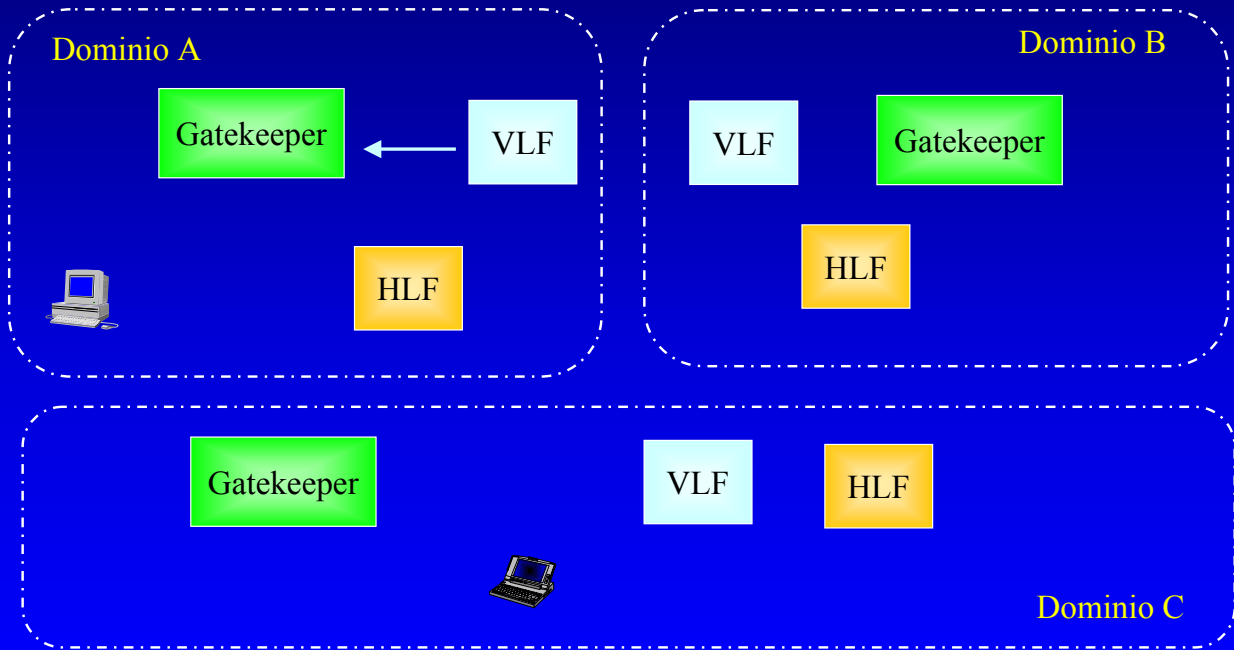
# La mobilità in H.323 Chiamate



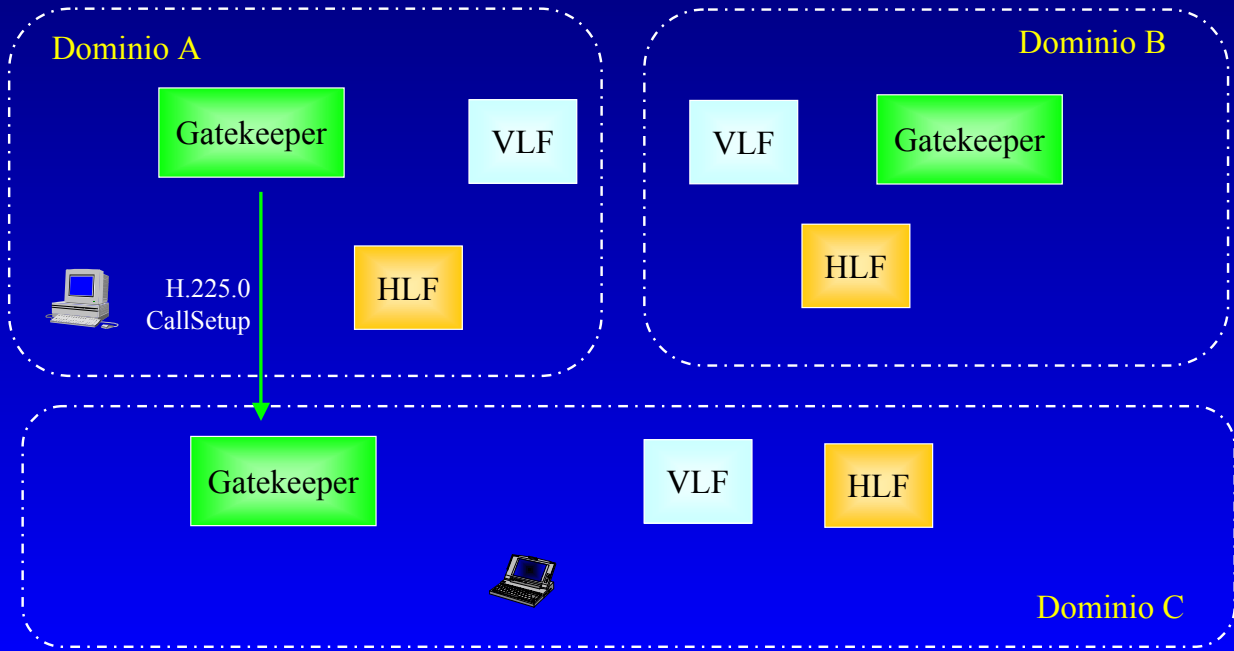
# La mobilità in H.323 Chiamate



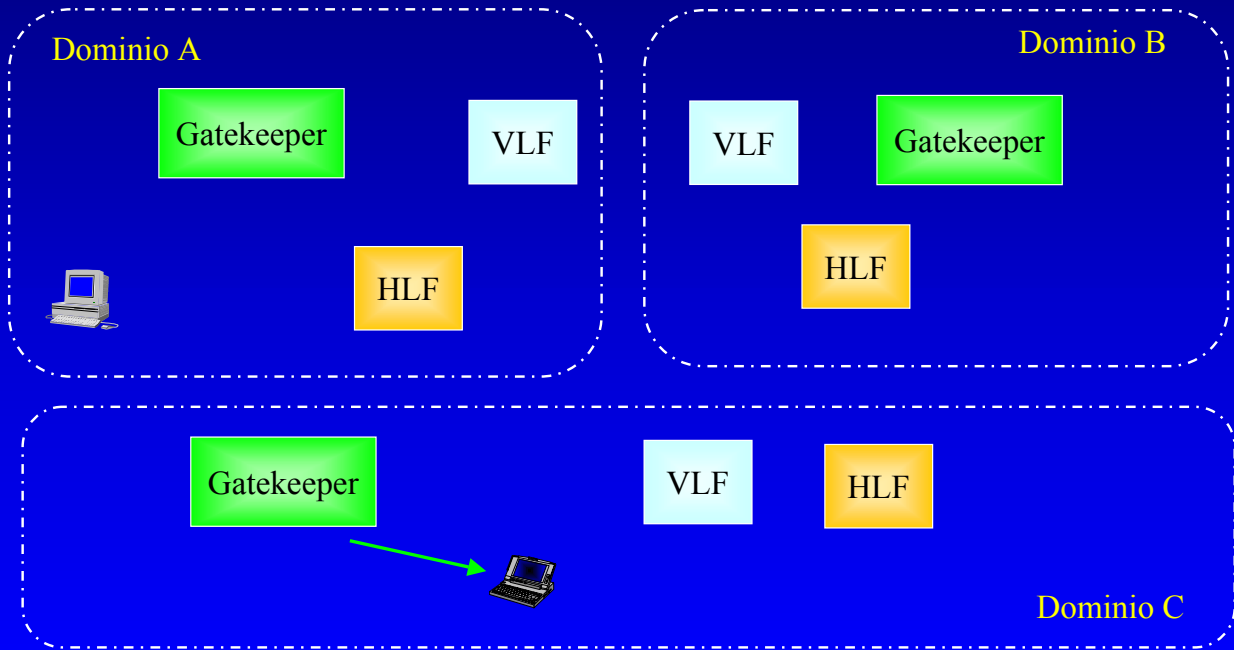
# La mobilità in H.323 Chiamate



# La mobilità in H.323 Chiamate



# La mobilità in H.323 Chiamate

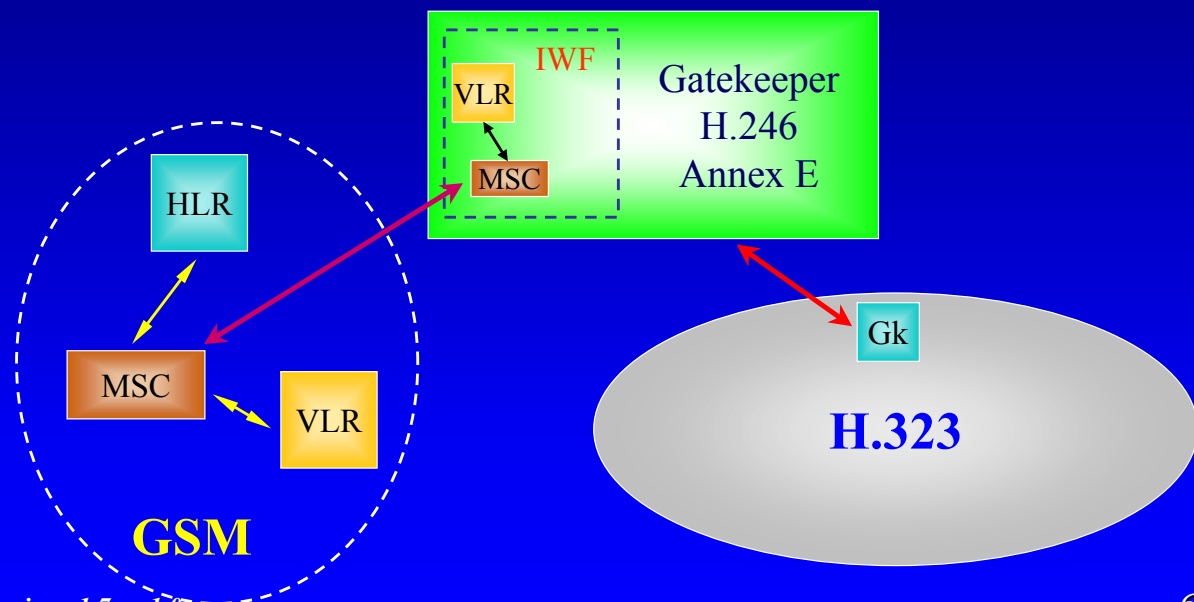


## La mobilità in H.323

**Interoperabilità con PLMN**

- Le *Public Land Mobile Networks* (PLMN) utilizzano un unico identificatore per individuare gli utenti
  - IMSI per le reti GSM.
- H.323 utilizza degli alias
  - all'interno di questa struttura dati è previsto un campo per gli identificatori IMSI delle PLMN più diffuse.
- L'esistenza di un identificatore unico per l'utente permette l'interazione tra le reti H.323 e le reti PLMN.

## La mobilità in H.323

**Interoperabilità con PLMN**

# H.323/PLMN Registrazione

---

HLR



Gk Annex E



# H.323/PLMN Registrazione

---

HLR



Gk Annex E



← GRQ(UIM)



# H.323/PLMN Registrazione

---



# H.323/PLMN Registrazione

---



# H.323/PLMN Registrazione

---



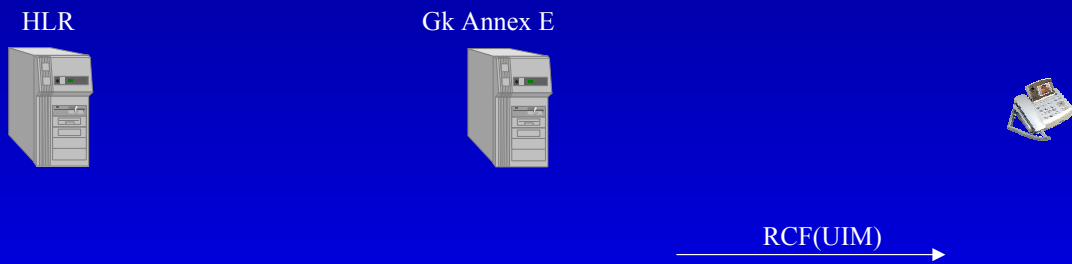
# H.323/PLMN Registrazione

---

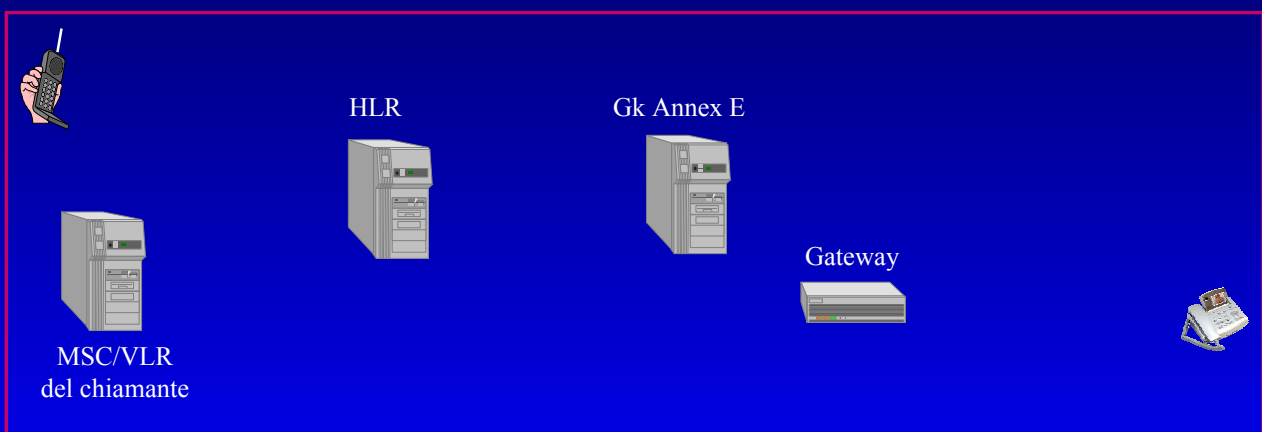




# H.323/PLMN Registrazione

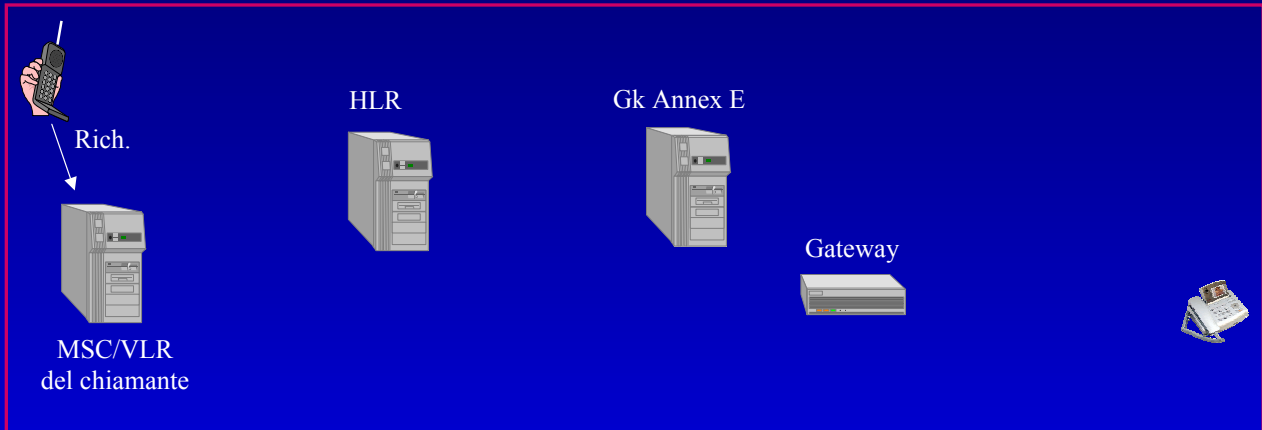


# H.323/PLMN Ricevimento di chiamate



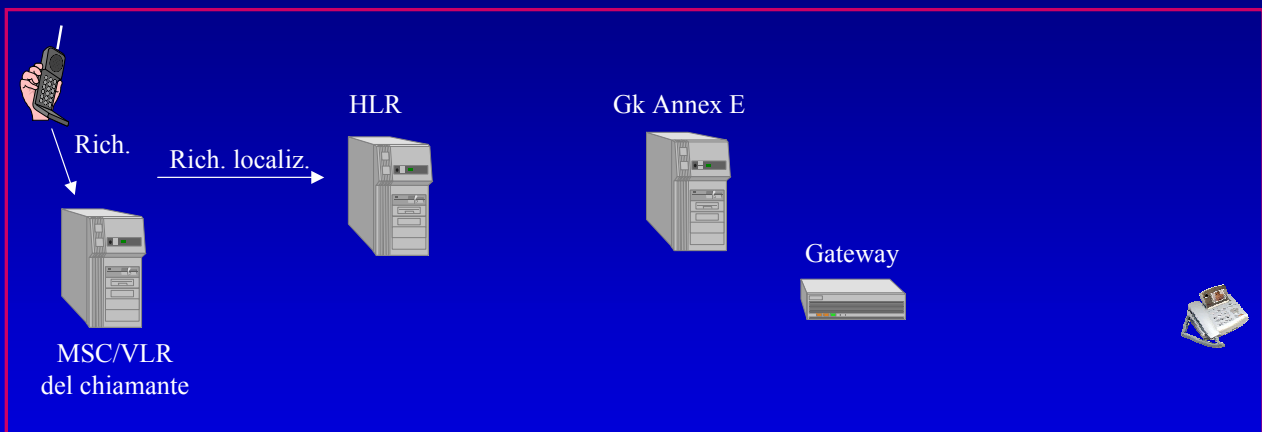
## H.323/PLMN

# Ricevimento di chiamate



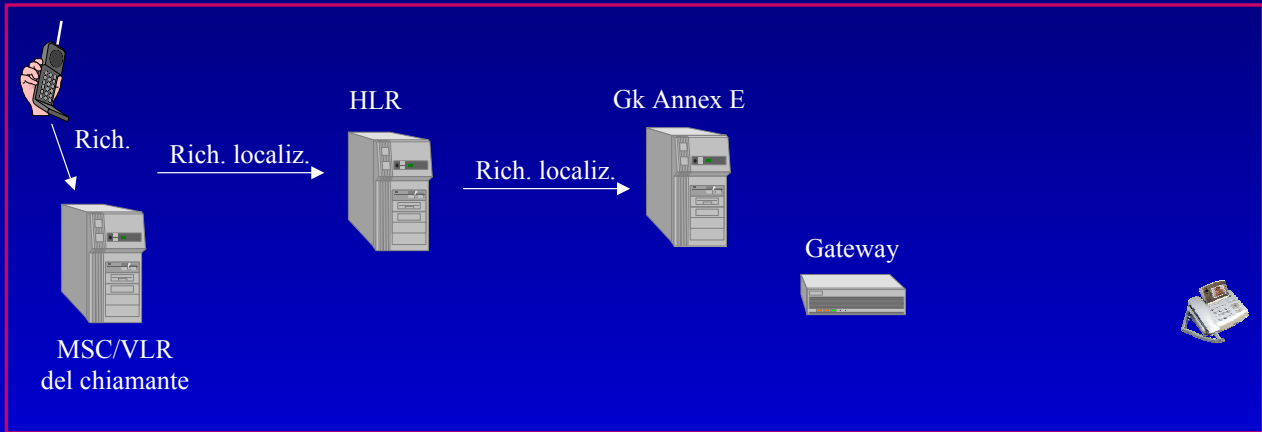
## H.323/PLMN

# Ricevimento di chiamate



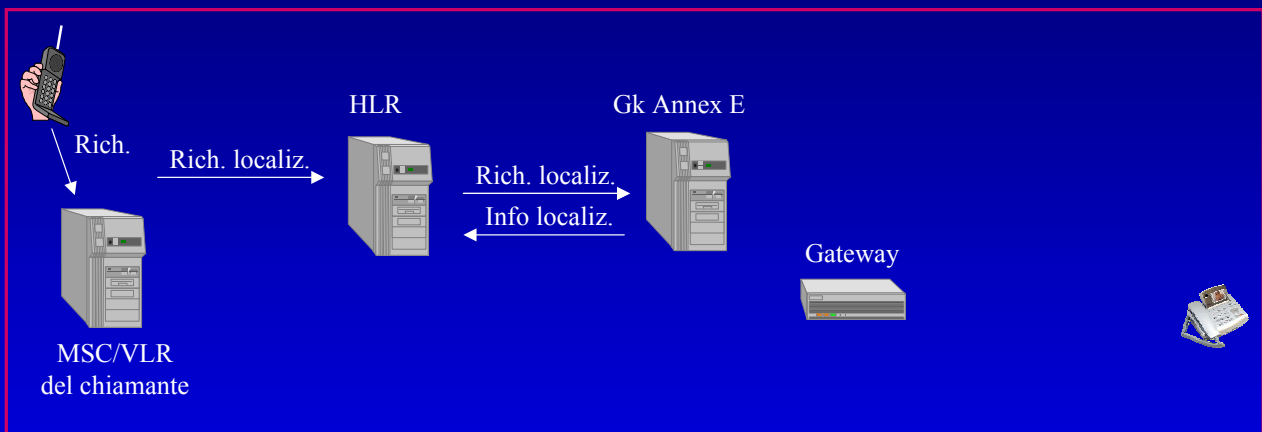
## H.323/PLMN

# Ricevimento di chiamate



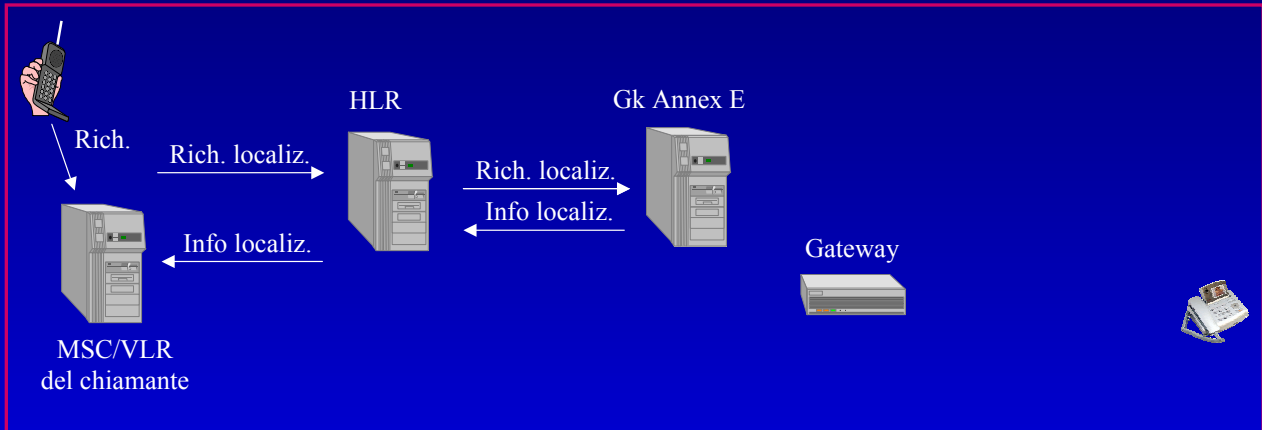
## H.323/PLMN

# Ricevimento di chiamate



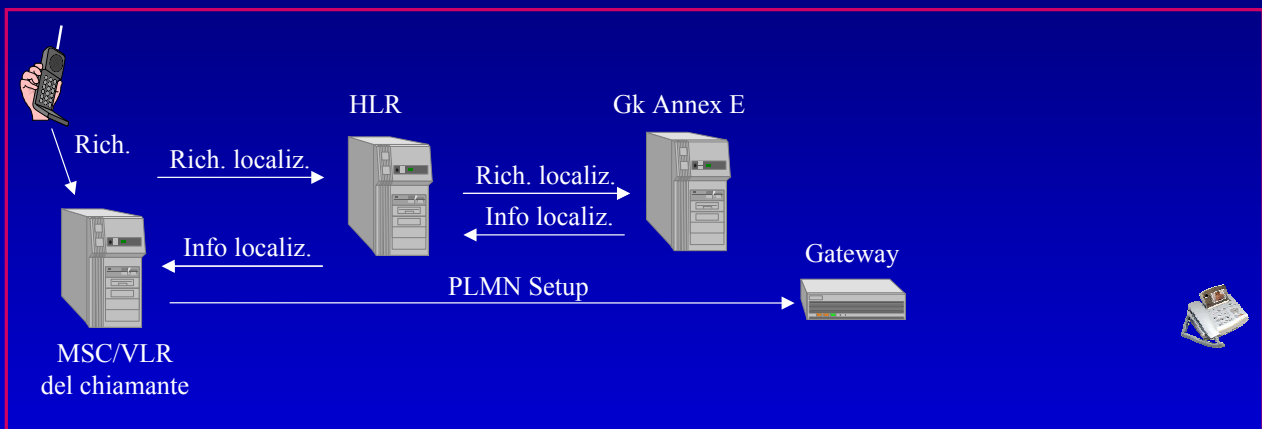
### H.323/PLMN

## Ricevimento di chiamate

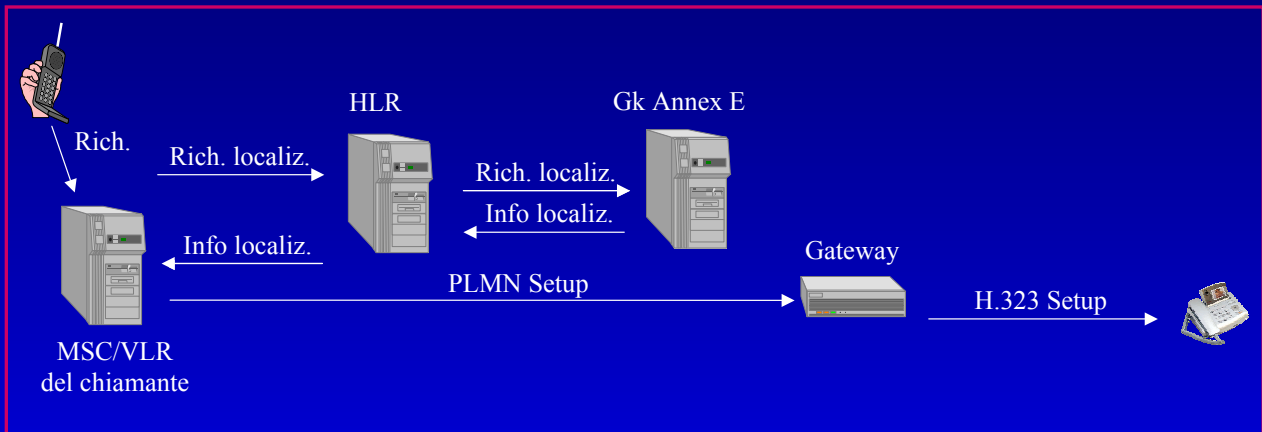


### H.323/PLMN

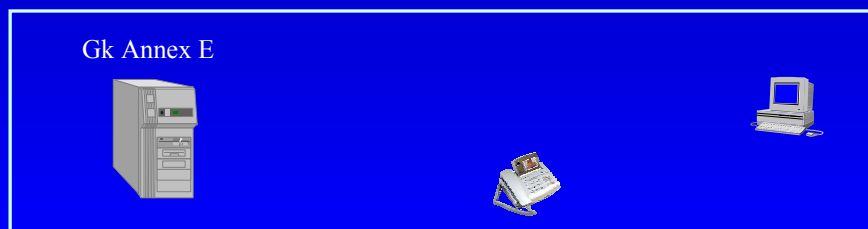
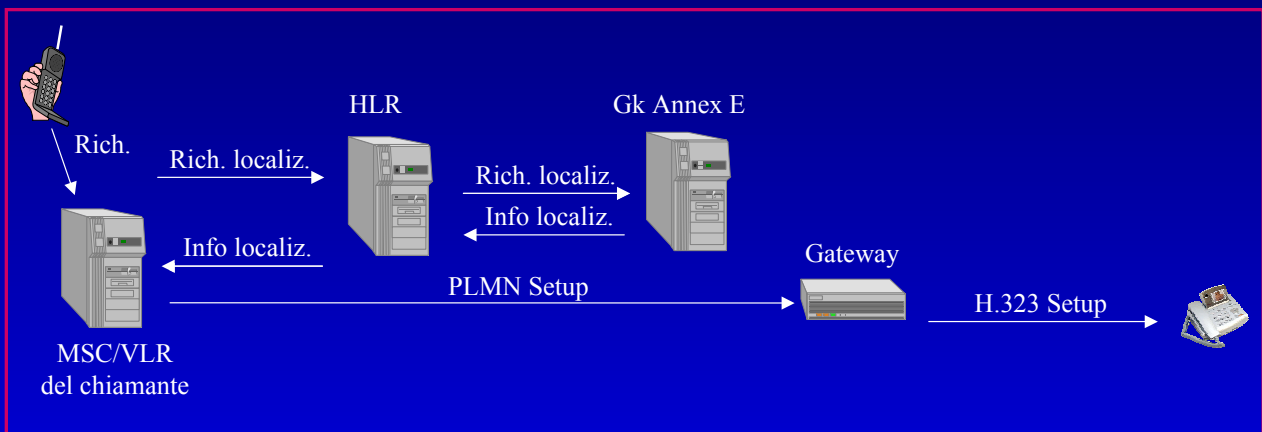
## Ricevimento di chiamate



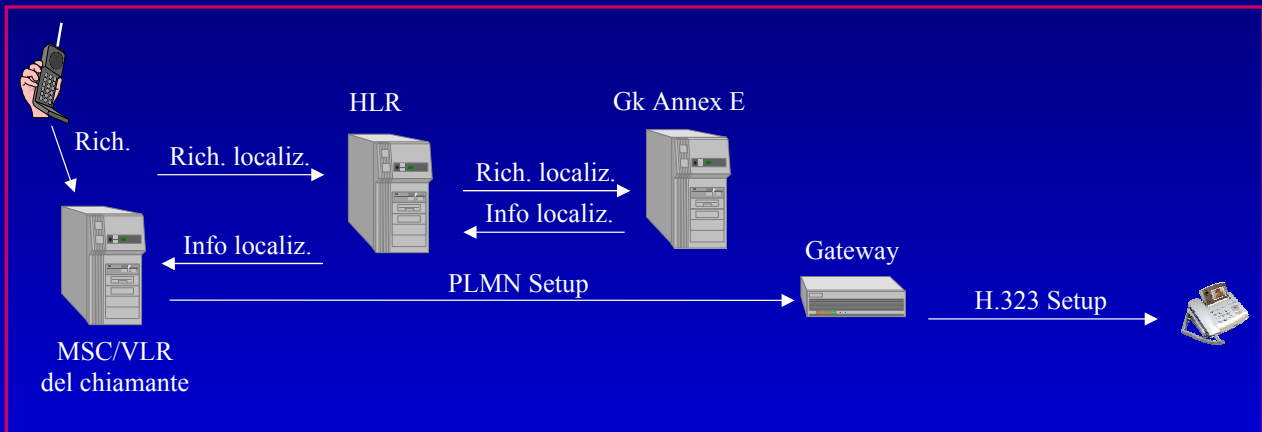
# H.323/PLMN Ricevimento di chiamate



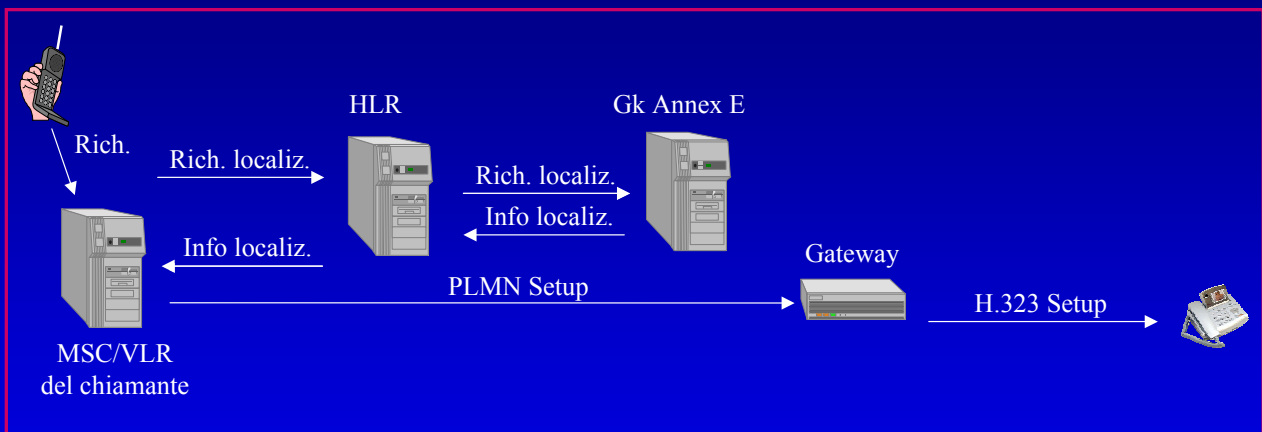
# H.323/PLMN Ricevimento di chiamate



# H.323/PLMN Ricevimento di chiamate

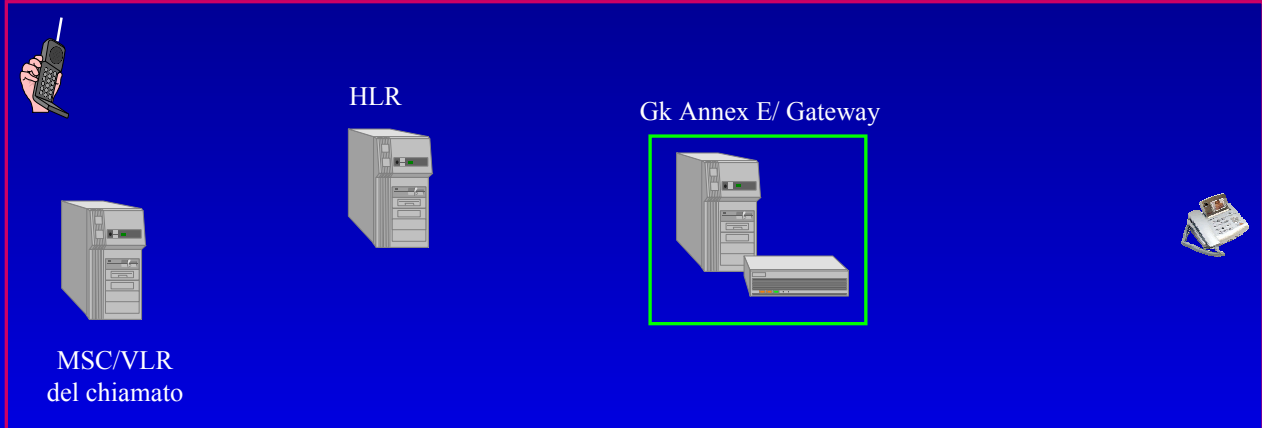


# H.323/PLMN Ricevimento di chiamate



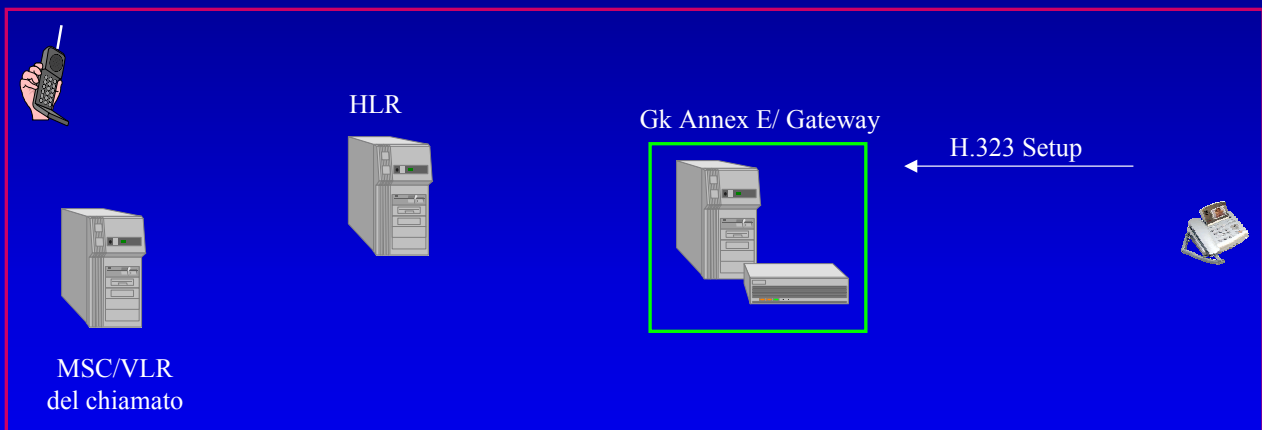
## H.323/PLMN

# Instaurazione di chiamate



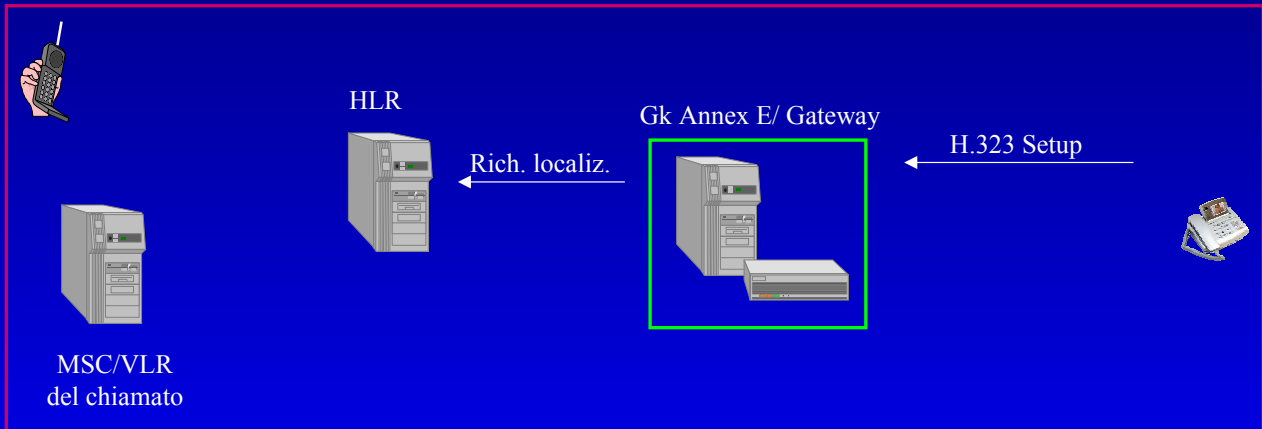
## H.323/PLMN

# Instaurazione di chiamate



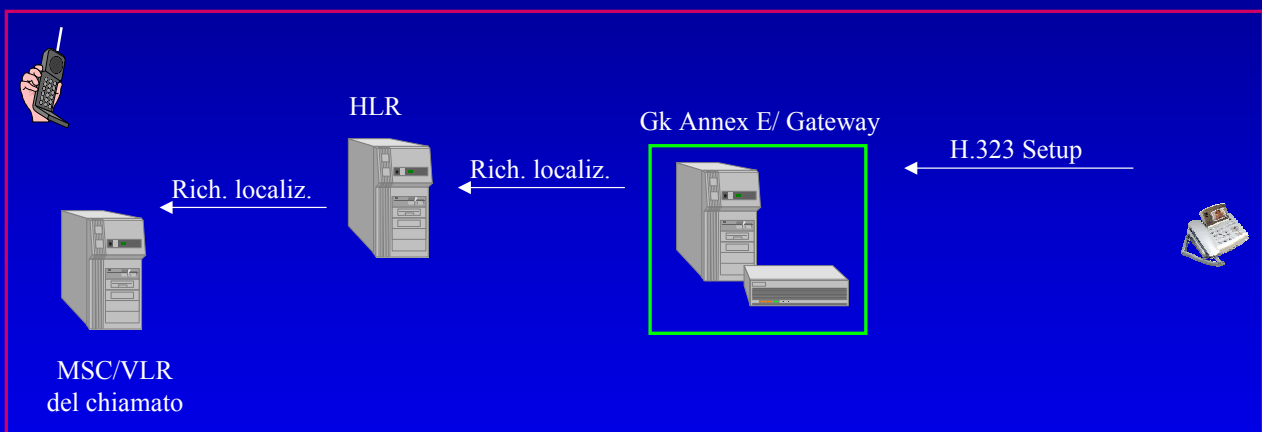
## H.323/PLMN

# Instaurazione di chiamate



## H.323/PLMN

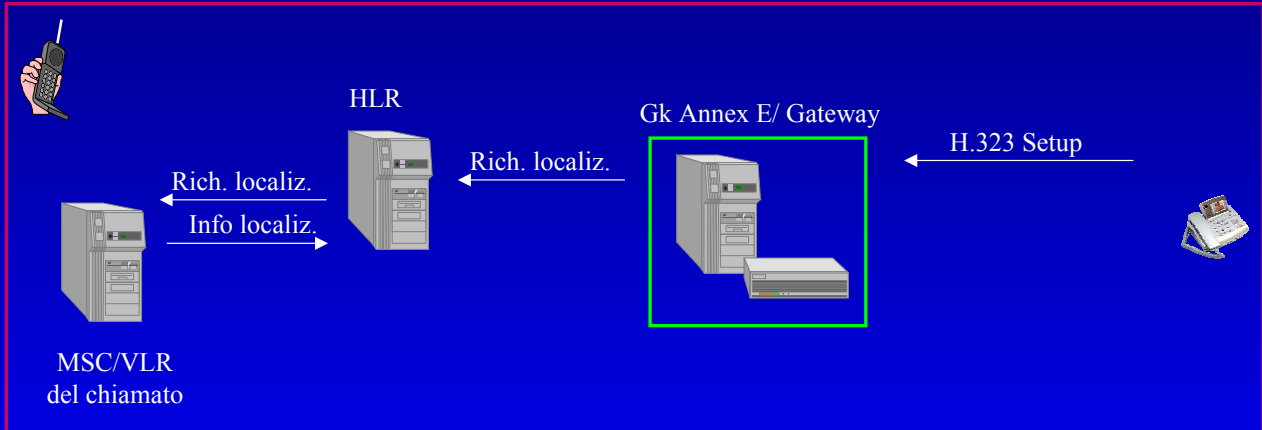
# Instaurazione di chiamate





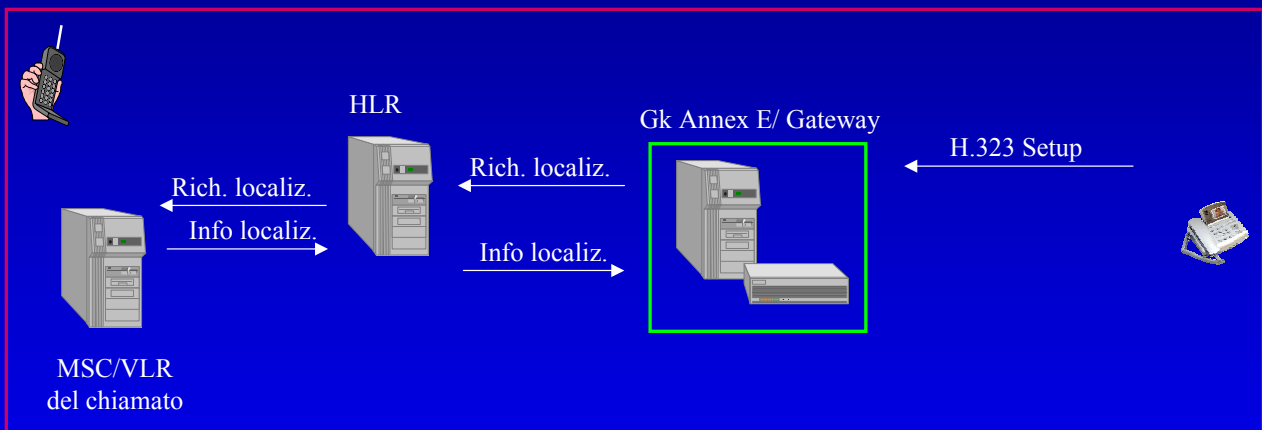
## H.323/PLMN

# Instaurazione di chiamate



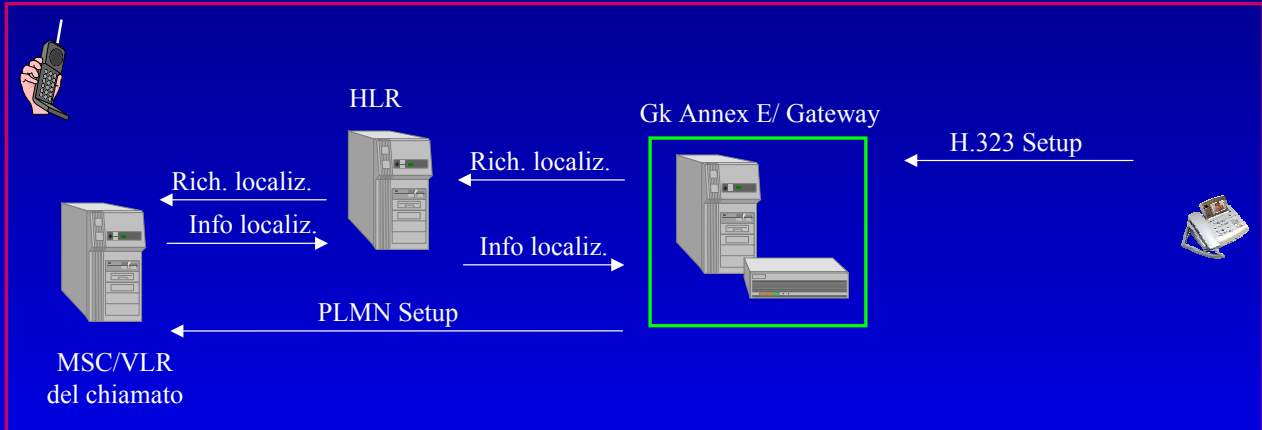
## H.323/PLMN

# Instaurazione di chiamate



## H.323/PLMN

# Instaurazione di chiamate



## H.323/PLMN

# Instaurazione di chiamate

