Interconnessioni IP

Rappresenta il problema di collegare i router di più sedi di un'azienda. La problematica è quella di stabilire una topologia di rete che sia efficiente e flessibile in quanto le necessità degli utenti possono cambiare nel tempo. Vi sono diverse tecnologie d'accesso che si possono utilizzare.

SONET/SDH: (tecnologia sincrona)
- framing di livello fisico
- framing di livello 2: PPP
- il formato delle trame è STS-1: 810 ottetti ogni 125 microsecondi, per raggiungere banda da 51.84 Mbs
- PRO:
  - infrastruttura di gestione standard
  - connessioni virtuali
- CONTRO:
  - una interfaccia per ogni collegamento
  - nessuna multiplazione statistica
  - limitata flessibilità di riconfigurazione

ATM: (tecnologia asincrona)
- la commutazione di cella permette di avere flessibilità nella multiplazione
- connessioni virtuali semi-permanenti e commutate
- protocollo di livello 2
- PRO:
  - connessioni virtuali
  - più connessioni per ogni interfaccia
  - completa flessibilità di riconfigurazione
  - flessibilità nella multiplazione
- CONTRO:
  - elevato overhead del protocollo

FRAME RELAY:
- la commutazione di trama (frame) consente flessibilità nella multiplazione
- connessioni virtuali semi-permanenti
- protocollo di livello 2
- PRO:
  - connessioni virtuali
  - più connessioni per interfaccia
  - larga base di installato
- CONTRO:
  - nessuna garanzia nella qualità del servizio (QoS)

IP:
- soluzione naturale per trasportare i pacchetti IP
- VPN
- diverse tecnologie di accesso, DSL, SDH/PDH, ATM, Frame Relay ed Ethernet
- PRO:
  - unica tecnologia
  - nessun overhead aggiuntivo (di trasmissione e controllo)
- CONTRO:
  - possibili conflitti di indirizzamento privato
  - poco controllo sul traffico:
    - difficile dimensionare
    - dato che è difficile controllare non si può fare traffic engineering

MPLS (Multi Protocol Label Switching):

Pacchetti IP (normalmente)
Connessioni virtuali LSP (Label Switched Path)
varie tecnologie per l'accesso (DSL, SDH/PDH, ATM, Frame Relay, Ethernet)
PRO:
- unica tecnologia
- velocità di commutazione ed efficienza
- orientamento alla connessione (billing e separazione)
- controllo sul traffico:
  - più semplice dimensionare
  - più semplice controllare:
    - è possibile effettuare traffic engineering

Dark Fiber (IP su fotoni):
i router sono collegati da fibre ottiche, il segnale ottico è trasmesso da un router e ricevuto da quello all'altro capo
framing di livello 2:
- trasmissione sincrona e PPP
- IEEE 802.3

PRO:
- no overhead

CONTRO:
- collegamenti a livello fisico, nessuna riconfigurazione dinamica della topologia
- una interfaccia per collegamento
- no infrastruttura di gestione standard
- no multiplazione statistica

DWDM (Dense Wavelength Division Multiplexing):
varie trasmissioni contemporanee sulla stessa fibra a frequenza (colori) diverse
si moltiplica la capacità della fibra
commutatori ottici con routing ottico
framing di livello 2: PPP
PRO:
- elevatissima capacità
- connessioni virtuali grazie al routing ottico

CONTRO:
- non c'è una infrastruttura di gestione standard
- no multiplazione statica

Panoramica sulle tecnologie disponibili

Saranno presentate le tecnologie per il trasferimento delle informazioni in ambito

geografico (WAN). Ciò che caratterizza queste tecnologie sono le tipologie di circuito analogiche o digitali, la modalità trasmissiva, sincrona, asincrona o plesiocrona, modalità di commutazione, a circuito, pacchetto, trama, cella.

ISDN

Caratterizzato da:

- dati + fonia + videotelefonia + fax
- il terminale utente diventa digitale
- tipologie:
  - 2B + D o accesso base
  - 30B + D o accesso primario
- estensione del numero telefonico attuale
  - sottoindirizzo per identificare i dispositivi

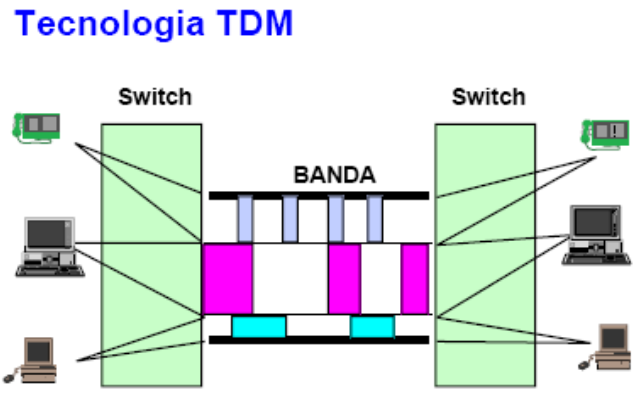
Canali diretti

Possono essere di tipo analogico oppure digitale. Quelli analogici sono ormai obsoleti, quelli digitali presentano queste caratteristiche:

- rete molto capillare sul territorio nazionale
- nodi che realizzano una commutazione di circuito (ripartitori elettronici digitali)
- circuiti PDH: 64 Kbps * N, 2 Mbps, 34 Mbps

Reti private basate su TDM

Il Time Division Multiplexing divide la banda in sottobande, sono basati sui canali E1/T1. L'aspetto fondamentale è che ***ogni servizio vede la propria sottobanda come un canale sincrono a velocità fissa***. I router ed i bridge li vedono come CDN. La parte di banda dedicata ad un servizio e non utilizzata in un determinato momento viene persa e non può essere utilizzata da altri servizi.

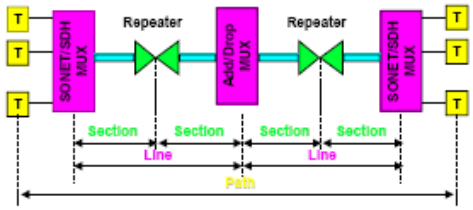


PDH e SDH

L'architettura fisica è composta da 3 componenti:

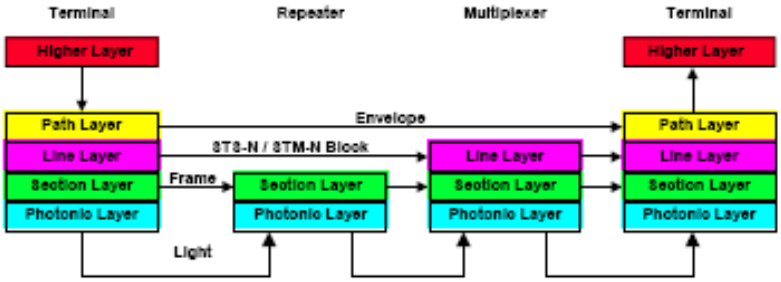
- **Section**: collegamento in fibra ottica tra tranceiver
- **Line**: sequenza di sezioni che tra dispositivi che lavorano a livello trama

Path: circuito diretto numerico end-to-end



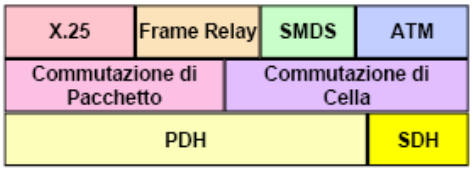
L'architettura protocollare è composta da 4 elementi:

Photonic Layer: fibra, laser
Section Layer: trame, OAM (Operation Administration and Management)
Line Layer: sincronizzazione, multiplazione, commutazione, OAM
Path Layer: trasferimento dati (bytes) end-to-end



Il formato delle trame è di 810 ottetti (1 ottetto è 1 byte) ogni 125 microsecondi, ovvero 51.84 Mbps

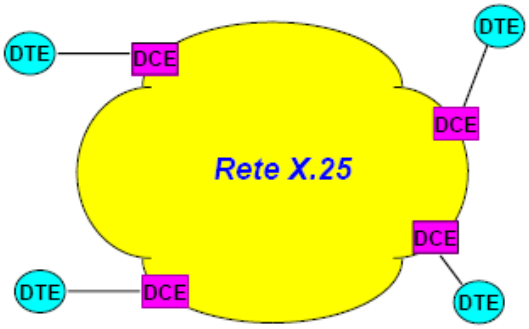
Livelli delle tecnologie



La commutazione di pacchetto prevede che:

L'informazione venga divisa in pacchetti di lunghezza variabile
L'instradamento avvenga a livello 3 OSI
Lo standard è X.25
Servizio pubblico in Italia è ITAPAC

Rete X.25

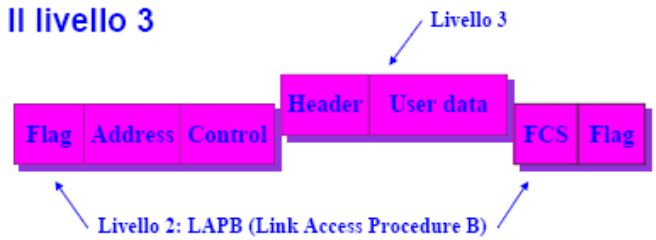


Il ***livello 2*** si occupa:

Sincronizzazione della trasmissione

Rilevazione e conseguente recupero degli errori
LAPB di derivazione HDLC/SDLC

Il ***livello 3*** si occupa:
Instaurazione circuiti virtuali:
Gruppo di canale logico (GCL)
Numero di canale logico (NCL)
Queste informazioni sono presenti nell'intestazione dei pacchetti



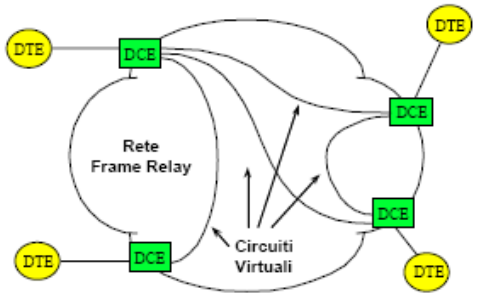
Le ***tipologie di connessione*** sono 2:
PVC (circuito virtuale permanente):
Connessione logica tra 2 DTE
Adatto a chi si connette frequentemente e per lunghi periodi con un corrispondente fisso
SVC (circuito virtuale commutato):
Connessione logica temporanea tra due DTE
Adatta a chi deve comunicare con diversi corrispondenti
Il campo Call User Data (CUD) specifica il protocollo di livello superiore che transiterà sulla connessione

Le ***modalità di internetworking*** di X.25 sono:
Si possono collegare bridge mediante X.25
Grazie al campo CUD si possono collegare router multiprotocollo:
Un circuito virtuale per ogni protocollo
Due buste di livello 3
Corrispondenza tra indirizzi di livello rete e X.121:
Normalmente mediante configurazione

I ***vantaggi e svantaggi*** di X.25 sono:
Ogni pacchetto viene completamente verificato in ogni nodo intermedio della rete:
A livello 2 si usa LAPB
Adatto a linee lente con errori
Alto tempo di attraversamento della rete
Rete adatta solo a trasmissione dati:
Nessun video o voce
Interconnessione di LAN

Lo standard Frame Relay

È uno standard d'interfaccia tra DTE e DCE che permette di far convivere diversi circuiti virtuali sulla stessa linea, simile ad X.25
È uno standard puramente di livello 2 (X.25 ha anche il livello 3)
Approccio Core-Edge alla correzione degli errori
X.25 corregge gli errori su ogni tratta
È pensato per linee veloci ed affidabili



Le ***applicazioni di Frame Relay*** sono:

Standard per interfacciare apparecchiature di rete locale (router, bridge, gateway) a reti per trasmissione dati

Permette di richiedere la banda necessaria

Disponibile su reti a commutazione di frame e di cella e sulle MAN

LAPF:

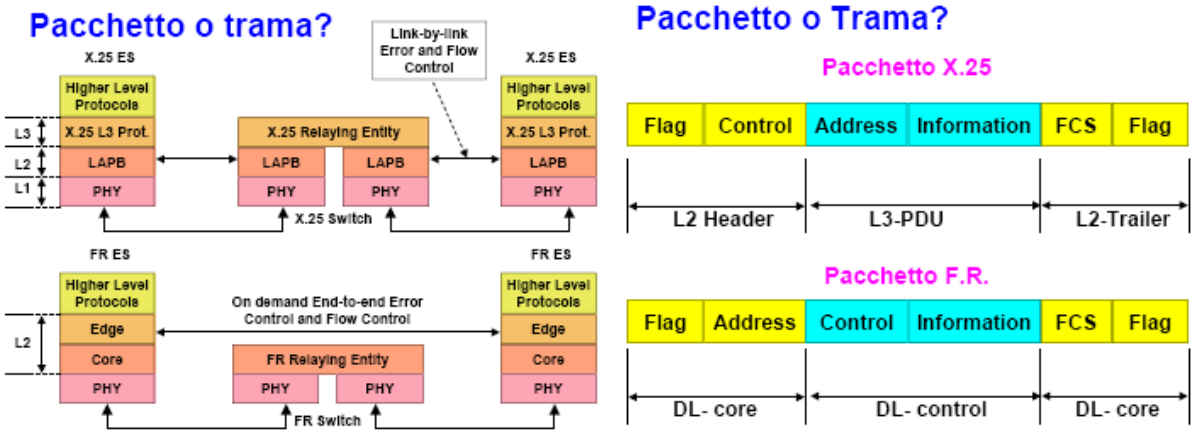
Link Access Procedure to Frame mode Bearer Services

Protocollo derivato da HDLC

Il LAPF è diviso in 2 parti:

DL-Core (Data Link Core Protocol), definito dalla raccomandazione I.233

DL-Control (Data Link Control Protocol)



Commutazione di trama:

Trame di lunghezza variabile: simile alle reti a pacchetto

Le trame vengono commutate a livello 2: nelle reti a pacchetto la commutazione avviene a livello 3

Correzione degli errori: approccio Core-Edge:

Gli errori si correggono solo mediante ritrasmissione ai bordi (edge) della rete e non nei nodi intermedi (core)

Necessità di di linee trasmissive di elevata capacità: da 64Kbps a 2Mbps

CIR (Committed Information Rate):

Bc: committed burst size: massima burstiness

Tc = Bc / CIR:

Intervallo in cui CIR è verificato

Si possono trasmettere fino a Bc bit alla velocità del collegamento fisico in ogni intervallo di durata Tc

Vantaggi e Svantaggi di Frame Relay:

Prestazioni migliori:
- Mezzi trasmessivi affidabili
- Approccio core-edge

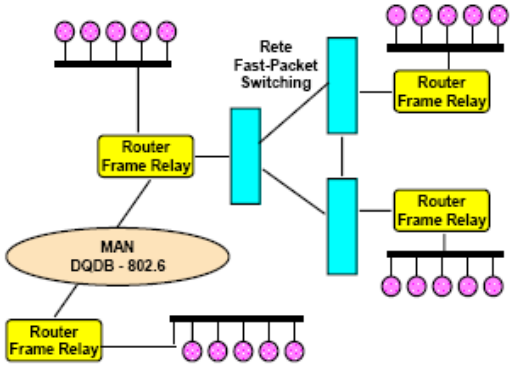
Ritardo introdotto minore:
- 2 ms per nodo frame relay
- da 5 a 20 ms per nodo X.25
- ritardi comunque variabili (non è idoneo alla trasmissione della voce)

il servizio Frame Relay è uno standard per collegare su base geografica apparati di internetworking di LAN (router, bridge, gateway)

disponibilità immediata di prodotti

disponibile su reti FastPacket e X.25 e molte altre MAN

Esempio di rete Frame Relay



B-ISDN

La grande sfida è il Broadband ISDN, ovvero fornire servizi ISDN su banda larga, il B-ISDN si basa su:

trasmissione principalmente su fibra ottica

trasmissione sincrona SONET/SDH

ATM

Il Broadband è un servizio o un sistema che richiede una velocità trasmissiva superiore a quella dell'accesso primario ISDN. Il B-ISDN è utilizzato per enfatizzare la caratteristica Broadband dell'ISDN, esisterà un solo ISDN comprensivo di servizi BroadBand e Narrowband. ATM è la tecnologia di trasporto per la realizzazione di B-ISDN.

I servizi sono di due tipologie:

Interattivi:
- Conversazione
- Messaggeria
- Retrieval

Distribuzione:
- Senza controllo dell'utente
- Con controllo dell'utente

ATM, caratteristiche generali

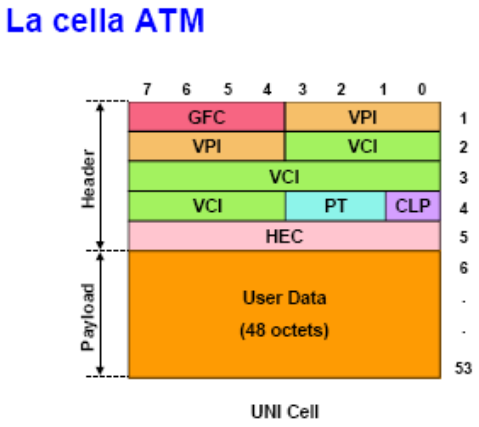
Commutazione di cella di lunghezza fissa 53 bytes

Mezzi trasmissivi veloci con basso tasso di errore (> 150 Mbps)

Bassi ritardi: idoneo per dati, voce, immagini video

Tecnica di trasferimento adatta a realizzare WAN e LAN
Tecnica scelta per B-ISDN
Segnalazione sofisticata:
    Gestione di connessioni multypart e punto-multipunto
Meccanismi sofisticati per il controllo di flusso (i tradizionali meccanismi a finestra non sono efficienti)
Allocazione di banda dinamica
Granulosità fine nell'assegnazione della banda
Supporto anche per il traffico di tipo "bursty"
Adattabilità sia per le applicazioni sensibili al ritardo che per quelle sensibili alla perdita di celle
Canali virtuali
Multiplazione statistica

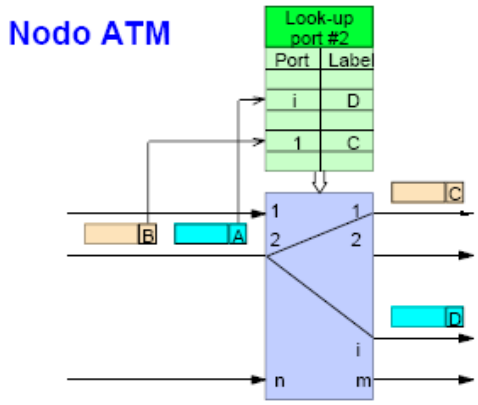
Cella ATM



GFC: General Flow Control
VPI: Virtual Path Identifier
VCI: Virtual Channel Identifier
PT: Payload Type
CLP: Congestion Loss Priority
HEC: Header Error Control

Trasmissione

Le celle sono trasmesse una dopo l'altra inserendo eventualmente celle vuote
Ogni cella è marcata con un identificatore di connessione VCI, VPI
Correzione degli errori con approccio core-edge
Controllo di flusso sofisticato perché è necessario considerare:
    Diversi tipi di traffico
    L'effetto memoria del canale



VCI/VPI varia ogni volta che si attraversa un multiplex ATM

Protocolli principio del core-edge

Nei nodi sono eseguite solo le funzioni essenziali (commutazione e multiplazione) a livello ATM (1-2 pila OSI)

Le funzionalità residue per i diversi tipi di servizi sono eseguite agli estremi

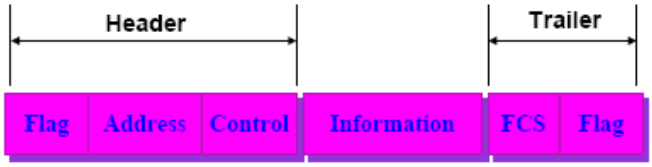
Protocolli di linea

HDLC

High level Data Link Control

Standard ISO
Altri protocolli della stessa famiglia:
- LAPB
- LAPF
- LAPD
- LLC

Pacchetto HDLC



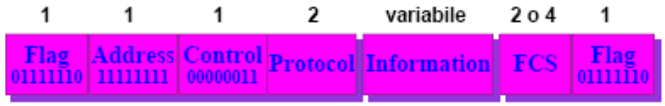
Flag: marcatore di inizio/fine
Address: usato unicamente per la gestione delle linee multipunto e non identifica il protocollo di livello 3
Control: usato per disporre di tre tipi di pacchetto: information, supervisor, unnumbered. Consentono di usare HDLC come protocollo connesso e non connesso. Su rete geografica si utilizza la modalità connessa che usa tutti e tre le tipologie di pacchetto.

Information: modalità connessa, acknowledge
Supervisor: acknowledge
Unnumbered: modalità non connessa, iniziare e terminare connessioni

HDLC è idoneo a collegare attraverso un CDN due router monoprotocollo o due brige. Non fornisce supporto multiprotocollo nativo e quindi non può collegare brouter o router multi protocollo di costruttori diversi.

PPP (Point to Point Protocol)

Metodo d'imbustamento dei pacchetti su link seriali: è un'estensione di HDLC con supporto di multiprotocollo
LCP (Link Control Protocol): permette l'instaurazione, la configurazione ed il controllo delle connessioni
NCP (Network Control Protocol): famiglia di protocolli per configurare diversi protocolli di rete



La comunicazione su link seriali avviene con questa modalità:
invio pacchetti LCP per configurare e collaudare il collegamento a livello data link
negoziazione dei parametri opzionali del livello data link
invio di pacchetti NCP per scegliere e configurare uno o più protocolli a livello rete
invio dei pacchetti di livello rete

Il link rimane operativo finchè non viene chiuso esplicitamente mediante un pacchetto LCP o NCP.

IP Control Protocol

NCP per IP
Negoziazione del protocollo di compressione
Negoziazione dell'indirizzo IP locale
Negoziazione dell'indirizzo IP remoto

Autenticazione CHAP (Challange Handshake Authentication Protocol)

Il router locale manda un pacchetto CHAP contenente una sfida:
- Nome del router locale o nome dell'utente sul router remoto
- Numero casuale

Il router remoto è sfidato a rispondere con:
- Il numero casuale crittografato usando la password
- Il proprio nome

Il router locale cerca la password corrispondente al nome ed effettua la stessa operazione di cifratura ***quindi la pwd non è mai trasmessa***.

Questa richiesta avviene solo in fase di apertura della connessione e durante la trasmissione dati non vengono lanciate sfide.

Autenticazione PAP (Password Authentication Protocol)

Il router che richiede il collegamento invia nome utente e password
Il router locale conferma la connessione
Viene inviata la password sul canale!

Controllo della qualità

- I pacchetti LQR (Link Quality Report) sono inviati periodicamente
  - Ad un LQR viene risposto con un altro LQR
- La qualità del collegamento è controllata:
  - Qualità in uscita: rapporto tra traffico ricevuto dall'altro estremo e quello generato localmente
  - Qualità in ingresso: rapporto tra il traffico ricevuto e quello generato dall'altro estremo
- Se la qualità scende al di sotto di una certa soglia predefinita, la connessione viene abbattuta

Reti ottiche

WDM (Wavelength Division Multiplexing)

Trasmissione di diverse lunghezze d'onda sulla stessa fibra:
DWDM (Dense WDM): sofisticato e costoso
CWDM (Coarse WDM): poche lunghezze d'onda e più economico

Sviluppo di WDM

Incrementare la capacità trasmissiva della fibra: configurazioni punto-punto
Add/drop multiplexing: topologie ad anello con add/drop multiplexing
- Inserire lunghezze d'onda nell'anello
- Togliere lunghezze d'onda dall'anello

Reti commutate a lunghezza d'onda: tipologie mesh arbitrarie con le lunghezze d'onda
- Wavelength router, lambda router, lamda switches
- Oggi esistono praticamente solo connettori cross di lunghezze d'onda

Switching ottico

Fiber cross-connect:
- Il segnale proveniente da una fibra di input viene commutato su una fibra di output
- Micro-electro-Mechanical-System MEMS

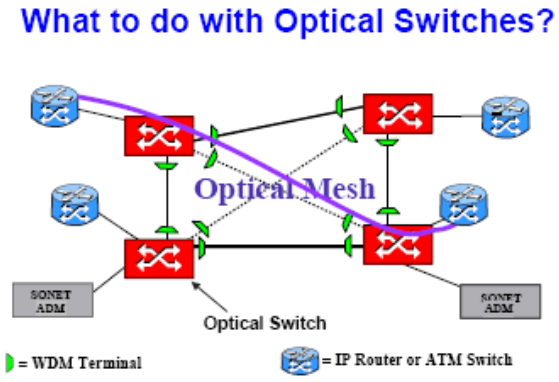
Wavelength cross-connect senza conversione di lunghezza d'onda:
- Una o più lunghezze d'onda su fibre in ingresso verso una fibra di uscita
- WDM de-multiplexer + MEMS
- Amplificazione prima o dopo la commutazione
  - OEO: conversione con rigenerazione elettronica
  - Amplificazione ottica

Wavelength cross-connect con conversione di lunghezza d'onda:
- Una o più lunghezze d'onda su fibre in ingresso verso una o più fibre in uscita
- OEO conversione con commutazione elettronica
- Semplice monitoring del segnale
- Forward Error Correction può ridurre Bit Error Ratio

Switching ottico dinamico

Commutazione di lunghezza d'onda senza conversione (di lunghezza d'onda):
- La configurazione dello switch varia dinamicamente
- WDM de-multiplexer + MEMS

Commutazione di lunghezza d'onda con conversione (di lunghezza d'onda):
- OEO conversione con commutazione elettronica
- Commutazione a circuito (SONET/SDH)



Conversione di lunghezza d'onda

Complesso:

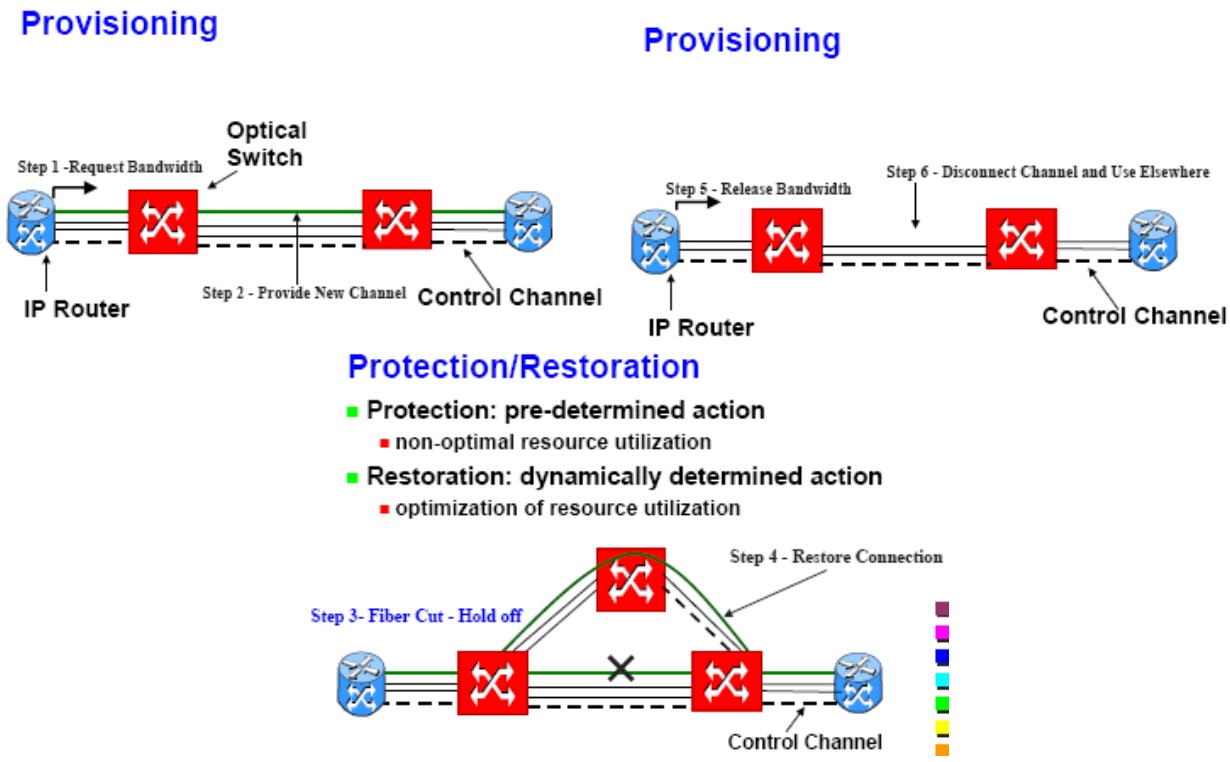
Conversione OEO: costoso, non trasparente ai dati e quindi non scalabile

Non è richiesta la stessa lunghezza d'onda ent-to-end

Non ci devono essere problemi nell'assegnazione delle lunghezze d'onda: non è semplice dato che c'è il problema N^2

Caratteristiche necessarie nelle reti ottiche

- Provisioning e protection dei lightpaths ent-to-end
- Client equipment per i layer ottici
- Costi effettivi dello sviluppo per reti flessibili



Protection & Restoration

- Livelli multipli di protezione:
  - Layer 1 optical: SONET
  - Layer 2 data link
  - Layer 2.5: protected MPLS
  - Layer 3: routing
- Utilizzo di diversi livelli di ripristino:
  - Ognuno ha diverse tempistiche per la determinazione e per il ripristino
- Bisogna evitare:
  - Traffic shifting, pacchetti persi, riordinamento
  - Pathological feedback: stabilizzazione non automatica

Segnalazione: cosa serve negli switch

- Resource discovery:

- Topologia, punti d'accesso ed identificazione, utilizzazione delle risorse
- Connection management:
  - Lightpath setup, abbattimento, modifica
- Mesh/ring protection and recovery:
  - Routing distribuito
- Istaurazione di classi di servizio protette

Segnalazione: necessità degli utenti

Resource discovery:

Gli indirizzi degli utenti devono essere raggiungibili attraverso la rete ottica

Gestione dei lightpaths:

Lightpath setup, abbattimento, modifica

Negoziazione dei servizi a classi protette:

Classi protette, non protette, servizi best-effort

Segnalazione: come realizzarla

Come controllare il layer ottico?

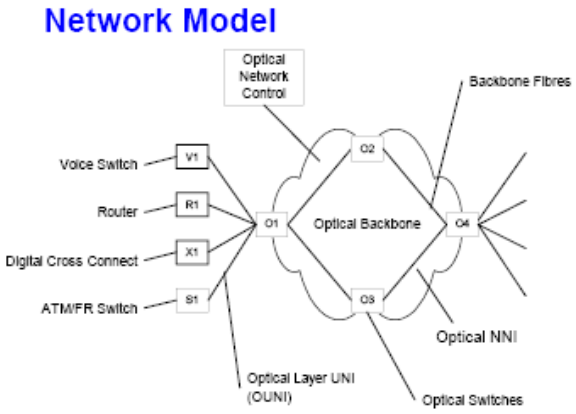
A livello 3?

MPLS?

OSPF, BGP4?

Nuovi protocolli di segnalazione?

Out of Band oppure in-band?



Routing

Nella rete Internet ottica, gli utenti sono i router.

Modello Overlay:

La rete ottica provvede alla connettività tra i routers

I router vedono la rete ottica come una scatola nera, è trasparente ai routers

I router devono essere provvisti di qualche informazione di raggiungibilità

Modello Peer:

I router e gli switch partecipano con gli stessi protocolli di routing

I router conoscono la topologia della rete ottica

I router possono scegliere il percorso dei lightpath

Trasporto dati

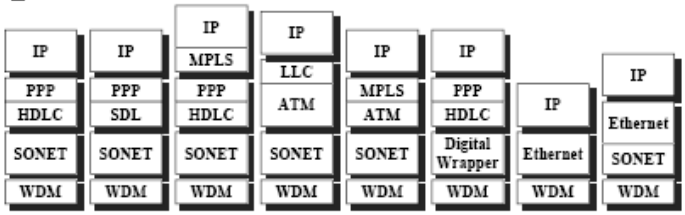
Livello fisico:
- SONET
- Ethernet
- Digital Wrapper

Livello Data link:
- PPP
- Ethernet
- ATM

MPLS?

Livello Network: IP

Alcune configurazioni sviluppate:



Digital Wrapper

- Improve Bit Error Ratio (BER)
- Provide transparent transport

OCh - Optical Channel
OH - Overhead
FEC - Forward Error Correction

Considerazioni

- Ligthpath (lamba) è una pipe larga, 2.5 – 40 Gb/s
- Individualmente, gli utenti non generano un ampio volume di traffico
  - È necessaria una commutazione fine
    - Problema N^2
    - Problematica nel frazionare le lunghezze d'onda
    - Le lunghezze d'onda devono essere governate

Packet Based Fractional Wavelength Switching and Grooming (Terabit oruters)

Costoso processamento dell'intestazione
- Complesso e lento

Servizio probabilistico
- Non si può garantire elevata QoS

Tempi di ripristino elevati per i router

ATTUALMENTE SONET RAPPRESENTA LA SOLUZIONE PER FRAZIONARE E GOVERNARE LE LUNGHEZZE D'ONDA

Problematiche della QoS

Applicazioni multimediali nelle reti a pacchetto

La multimedialità è l'utilizzo contemporaneo di vari media: audio, video, immagini, testo.

Codifica dei media: campionamento, quantizzazione e codifica

Compressione: eliminazione delle ridondanze: spaziale, temporale, si può eventualmente avere perdita di informazione e quindi degrado della qualità

Lo standard di codifica da scegliere dipende da:

- Capacità elaborative dei terminali
- Disponibilità di risorse della rete
- Tipo di applicazione:
  - Live, real-time
  - Store & retrive

Le applicazioni multimediali in rete sono diverse: WWW, distribuzione video, video on demand, telefonia, radio, jukebox, teleconferenza, giochi distribuiti interattivi, realtà virtuale. Le applicazioni multimediali hanno caratteristiche diverse dalle applicazioni tradizionali, quindi anche l'utilizzo di un solo media può essere critico, questo perché sono applicazioni in tempo reale, devono avere tempi di risposta brevi, il ritardo è fondamentale! Le caratteristiche più rilevanti sono quindi banda larga e comunicazione molti a molti.

Requisiti sulla rete

- Streaming:
  - Perdite limitate: molte applicazioni sono relativamente tolleranti alle perdite
  - Ritardi costanti
- Interattività:
  - Dialogo sotto 100, 150 ms, one way
- Larga banda trasmissiva (elevata disponibilità di risorse):
  - Capacità trasmissiva
  - Memoria nei nodi (buffer)
  - Potenza elaborativi (routing)
  - Commutazione
- Comunicazioni di gruppo:
  - Servizi di trasmissione multicast
    - IP multicasting
    - MBone
  - Server con funzionalità di reflector o multiconference unit
- RITARDO

La problematica del ritardo

Le applicazioni multimediali sono dette anche real-time. ***Il problema del ritardo è che***

varia a seconda del carico istantaneo sui nodi.
Contromisure nelle stazioni per compensare le variazioni del ritardo:
Replay buffer
Dimensione fissa per applicazioni non interattive
Adattativi per applicazioni interattive
Adattamento alle condizioni della rete:
Diminuire il traffico generato quando la qualità della sessione diminuisce

L'unico modo per compensare le variazioni è conformare tutti a chi ha subito ritardo massimo, questo provoca un aumento del ritardo end-to-end. Quindi questo diventa critico per l'interattività, la telefonia, la conferenza, i giochi e la realtà virtuale.

Strumenti

Comunicazione:
- Informazioni temporali:
  - RTP Real-time Transport Protocol: contiene un timestamp
- Stato della comunicazione:
  - RTCP RTP Control Protocol

Codifica a livelli (layered encoding):
- Layer base:
  - Trasmesso a più alta priorità
  - Eventualmente risorse riservate
- Layer aggiuntivi che aumentano la qualità:
  - Trasmessi a bassa priorità
  - Eventualmente best-effort

Codifica adattativa:
Granularità di quantizzazione
Parametri della compressione
Feedback, per es. RTCP

Soluzioni nella rete:
Classificazione del traffico
Sofisticati algoritmi di accoramento
Micro-controllo del traffico in ingresso alla rete (pacchetto)
Shaping/policing

Contromisure nella rete:
Macro-controllo del traffico in ingresso alla rete (chiamata)
Segnalazione con prenotazione di risorse
RSVP: Resource reSerVation Protocol (IP)
UNI: User Network Interface (ATM)
Macro-controllo a priori:
Network engineering:
Dimensionamento della rete rispetto al traffico previsto
Limite sul numero di utenti
Traffic engineering:
Distribuzione controllata del traffico

Problemi collaterali:

UDP a livello trasporto:
I requisiti real-time sono spesso incompatibili con i tempi di ri-trasmissione del TCP
Applicazioni non altruiste: TCP si adatta alle condizioni di traffico, UDP le ignora
Le applicazioni multimediali possono penalizzare le altre
Vengono penalizzate soprattutto quelle che usano TCP che è cortese
Segregazione delle applicazioni e policing (bandwidth shaper) per limitare la banda della applicazioni real-time

Tecniche per il supporto della qualità di servizio – Accodamento

Sono necessarie code multiple e scheduling. Per far ciò è necessario classificare i pacchetti, ovvero identificare i pacchetti a cui garantire qualità.
Algoritmi di scheduling:

- Priorità queuing
- Round Robin
  - Weighted Round Robin
- Class Base Queuing
- Weighted Fair Queuing
- Deadline queuing

Classificazione: basata su varie informazioni nell'intestazione IP
Indirizzo IP sorgente
Indirizzo IP destinazione
Protocollo di trasporto
Porta mittente
Porte destinazione

La classificazione prevede algoritmi complicati che debbono spesso essere realizzati in hardware mediante ASIC e CAM.

Capacità di commutazione:

- La commutazione immediata richiede sempre speed-up
  - La switching fabric opera a velocità maggiore degli ingressi
- Particolarmente problematico ad alta velocità

Accoramento e commutazione:

- Le code in uscita sono la soluzione più semplice
- Tuttavia bisogna considerare che la capacità di commutazione è una risorsa limitata e quindi non è detto che i pacchetti possano essere commutati appena arrivano
  - Si inseriscono code in ingresso
  - Si inseriscono code distribuite mediante Virtual output queuing (controllo distribuito). Le code sono nella matrice di commutazione

Tecniche per il supporto della qualità di servizio – Controllo dell'accesso

Controllo sull'accettazione di chiamate: Call Admission Control CAC

- Segnalazione:
  - Descrizione del traffico generato
  - Descrizione servizio voluto
  - Es. RSVP e UNI ATM

- Prenotazione delle risorse

QoS routing:

- Trovare un percorso con le risorse necessarie
- Protocolli di routing distribuiscono informazioni sull'occupazione delle risorse in tempo reale: informazioni molto dinamiche che variano molto nel tempo!
- La decisione di routine è basata su informazioni di occupazione: non solo sulla tipologia
- Instabilità con trasferimento dati non connesso
- Es. PNNI (Private Network Node Interface) in ATM

Network Engineering & Traffic Engineering: Azioni preventive

Continuo controllo dello stato della rete
Eventuale cambiamento del dimensionamento e direttrici di traffico
Dimensionamento della rete per il caso peggiore: statistiche sugli utenti
Determinazione delle direttrici di traffico: distribuzione del traffico
Bassa efficienza nell'uso delle risorse 20%-30%
Semplicità e scalabilità

Policing & Shaping: assicurarsi che il traffico in ingresso alla rete sia come ci si aspetta, Leaky Bucket. I pacchetti non conformi sono ritardati, scartati o mandati a bassa priorità.

Policy (Politica): stabilisce aspetti generali di funzionamento di una rete, determina gli aspetti specifici del funzionamento di un apparato:

Tipo di accoramento
Regole per l'accettazione di chiamate
Parametri Leaky Bucket

Flessibilità: policy management

- Una policy può dipendere dal tipo di traffico e/o dall'ora del giorno
- Evitare di dover configurare ogni apparato di rete e cambiare la configurazione
- Il problema si risolve con COPS (Common Open Policy Service): permette la distribuzione automatica di policy:
    - Gli apparati prelevano le policy dal server
    - Il server invia le policy agli apparati

Servizi Integrati – Architettura Integrated Services

L'architettura IntServ è una soluzione ambiziosa ma forse inutile che prevede:

- Prenotazione di risorse per flussi attraverso RSVP
- Garanzie sulla qualità del servizio mediante accoramento per flusso nei router
- Elevata complessità
- Bassa scalabilità

Lo standard è stato completato nel 1994, realizzato dai costruttori di router che hanno implementato la gestione dei messaggi RSVP e gli algoritmi di accoramento (è da verificare quali e come). In sostanza questa architettura è inutilizzabile su larga scala, ovvero non è adeguato a fornire i servizi pubblici. Si hanno 2 modalità: GQoS e CLS.

Modalità Guaranteed Qualità of Service

- Si garantiscono le caratteristiche del servizio ottenuto in termini di PERDITE, RITARDO e BANDA
- Controllo sull'accesso e accoramento per flusso

Controlled Load Service

- Si fornisce il servizio che darebbe la rete in condizioni di basso carico
- Non ci sono garanzie
- Controllo sull'accesso

Ci si pone il problema se serva o meno prenotare le risorse, considerando che:

- in futuro la banda sarà quasi infinita, ma se ne userà ancora di più e la connettività è abbastanza costosa
- una singola priorità potrebbe essere sufficiente, tuttavia ogni applicazione richiede un servizio specifico
- le applicazioni possono adattarsi comunque con dei limiti

L'architettura IntServ è caratterizzata da una specifica di flusso Flow Descriptor:

- Filterspec (+ destinazione): indica i pacchetti del flusso ed è essenziale per classificarli
- Flowspec: indica il profilo del traffico generato ed il servizio richiesto

Inoltre l'architettura IntServ prevede:

Controllo dei flussi:
- Classificatore dei pacchetti
- Schedulatore dei pacchetti
- Gestione dei buffer

Controllo di ammissione
Prenotazione delle risorse
Instradamento

Servizi integrati su Internet – la prenotazione di risorse mediante RSVP

RSVP: Resource Reservation Protocol

- Si appoggia su IP
- Trasporta i Flow Descriptor: filterspec e flowspec
- Approccio soft-state: è necessario rinnovare periodicamente le prenotazioni
- Permette flussi eterogenei
- La prenotazione è a carico del ricevitore: approccio receiver oriented
- Organizza i dati in flussi simplex

Obiettivi del progetto:

- Ricevitori eterogenei
- Gruppi multicast dinamici
- Aggregazione dei flussi
- Adattamento all'instradamento
- Limitazione dell'overhead

- Modularità

Tutto ciò genera un'elevata complessità non semplice da gestire e non scalabile.

FlowSpec: che servizio si vuole (Service Class)

Esistono 2 tipi di servizio, garantito e non garantito: Guaranteed Quality e Controlled Load.

RSPEC: Reserve, qualità -> ritardo

- Rate: si assume fluid model con deviazione pubblicata dai router
- Slack: tolleranza rispetto alla richiesta

TSPEC: Traffic, descrizione del flusso di dati generato

- Parametri di un Leaky Bucket:
  - Rate medio
  - Rate di picco
  - Burstiness

RSPEC e TSPEC sono insiemi di parametri numerici

Reservation model

- Grant or refuse: come la telefonia tradizionale
  1. l'utente formula una richiesta
  2. se la rete non può garantire la QoS, l'utente è bloccato

- Two pass reservation: richiede due passi: esplorazione&risposta, richiesta
  1. la rete comunica il livello di QoS che può garantire
  2. la richiesta è formulata di conseguenza

- One pass: utilizzabile con RSVP
  1. l'utente formula una richiesta
  2. se non può garantire la QoS richiesta, la rete fornisce un servizio senza garanzie, ovvero best-effort

- One pass with advertisement: versione potenziata di one pass, utilizzabile con RSVP
  1. da mittente a destinazione si raccolgono informazioni sulla QoS che la rete è in grado di fornire
  2. la destinazione richiede una QoS minore o uguale a quella comunicata

Prenotazione delle risorse

Messaggio PATH:

- indirizzo del Previous Hop per guidare l'inoltro dei messaggi RESV
- Sender Tspec:
  - Descrive il traffico generato dalla sorgente
- ADSPEC
  - QoS che la rete è in grado di fornire
  - La funzione di controllo di accesso di ogni nodo aggiorna il campo prima di

inoltrare il messaggio PATH

Messaggio RESV:

- Reservation request: consiste di un flow descriptor
  - Flowspec + FilterSpec
- FlowSpec: QoS desiderata
  - Programma lo scheduler
- FilterSpec: descrizione dei pacchetti che devono ricevere la QoS
  - Programma il classifier
  - Aggiorna il traffic control database
- FlowSpec:
  - Service class
  - Receiver Tspec: descrizione del traffico interessato
  - Receiver Rspec: richiesta di QoS
- Merging dei FlowSpec

E' progettato per comunicazioni molti a molti

Reservation Policy

- Accesso preferenziale alle risorse per alcuni utenti
- Identificazione affidabile del richiedente
- Policy Control oltre che Admission Control
- Policy Data vanno forniti ai router: per esempio COPS

RSVP e instradamento

Usa la routine table per inoltrare i messaggi PATH
Reagire ai cambiamenti nell'instradamento per recuperare i guasti: utilizzo di percorsi alternativi
Route pinning: ignorare i cambiamenti per usare la prenotazione

Servizi differenziati – L'architettura Differentiated Services

Questa architettura si differenzia notevolmente come scopo rispetto a quella dei servizi integrati, infatti non garantisce nessuna QoS. La premessa fondamentale è:

IL TRAFFICO DIFFERENZIATO RAPPRESENTA UNA PICCOLA PERCENTUALE DELLA CAPACITA' DELLA RETE

Niente garanzie sulla qualità
Niente prenotazione delle risorse
Niente stato per flusso
Servizio differenziato per tipi di traffico diversi:
DS field (campo DiffServ)

Trattamento per classe
Dimensionamento della rete:
Network engineering
Traffic engineering
Controllo di accesso ai confini
Policing and Shaping
Traffic conditioning

Caratteristiche generali:
bassa efficienza
semplicità e scalabilità
sempre più utilizzato, per esempio IP telephony

Architettura di DiffServ

Vendita dei servizi

I servizi sull'architettura DiffServ si vendono utilizzando due tipologie di contratti caratterizzati da alcune informazioni che descrivono il servizio offerto.

- Service Level Agreement SLA:
  - Tra il cliente e service provider
  - Tra internet service provider
- Service Level Specification (SLS):
  - Traffic Conditioning Specification (TCS)
  - Parametri Leaky Bucket

DS Field

- Ex campo ToS
- 6 bit per il codepoint
- 2 bit per ECN (Explicit Congestion Notification): attualmente non usato
- DS codepoint compatibili con i vecchi valori di ToS (usava 3 bit)

Per Hop Behavior (PHB)

Riguarda il trattamento dei pacchetti nel singolo router

- Si crea una corrispondenza tra DS codepoint e PHB:
  - Standard
  - Specifica per un DS domain:
    - Tramite configurazione
    - Re-marking
- La realizzazione dipende: dal costruttore e dal gestore della rete (configurazione dei router)
- Il servizio end-to-end risulta dalla concatenazione di PHB

PHB Standard:

- Expedite Forwarding: rate di servizio maggiore o uguale a valore specificato
- Assured Forwarding:
  - Gruppo di PHB (4 classi)
  - Diversa priorità di scarto

Expedite Forwarding:

- Realizzazioni d'esempio:
  - Simple priorità queuing
  - Weighted Round Robin
  - Class Based Queuing
- Esempio di applicazioni: Virtual Leased Lines
- I pacchetti subiscono basso ritardo e bitter
- Attenzione, questa è stata giudicata impossibile da realizzare, si è pubblicata un'altra rfc con una definizione rivista

La RFC dichiarava: "Il rate di partenza dei pacchetti aggregati da ogni nodo DiffServ deve essere maggiore o uguale al rate configurato. Il traffico EF DOVREBBE ricevere questo rate indipendentemente dall'intensità di ogni altro traffico che sta transitando nel nodo."

Assured Forwarding:

- PHB group:
  - Varie AF classes indipendenti
  - In ogni classe ci sono vari levels of drop precedence
- Realizzazione di esempio:
  - Random Early Detection
- Servizi d'esempio:
  - Olympic Service

La RFC dichiara: "i pacchetti in una classe AF DEVONO essere inoltrati indipendentemente dai pacchetti inoltrati appartenenti ad un'altra classe. Ogni classe DOVREBBE essere servita in modo da raggiungere il rate configurato. Una implementazione di AF DEVE determinare e rispondere a congestioni di lungo tempo entro ogni classe, eliminando i pacchetti. AF richiede un algoritmo di gestione della coda. Il condizionamento del traffico (traffic conditioning) potrebbe includere il traffic shaping, lo scarto di alcuni pacchetti, e il riassegnamento dei pacchetti ad un'altra classe."

Per Domain Behavior (PDB)

- Concetto aggiunto a posteriori
- Insieme di pacchetti trattati nello stesso modo da un DS domain e l'associata descrizione del servizio ricevuto
- CLASSIFIER + CONDITIONERS + CONCATENAZIONE DI PHB
  - I classificatori segnano i pacchetti appartenenti al PDB
  - I conditioner realizzano policing alla periferia del DS domain
  - Il servizio end-to-end ricevuto dai pacchetti risulta dalla concatenazione dei PHB previsti

Accesso alle reti IP – Internet Access

Essere connessi alla rete Internet

Si è connessi alla rete IP se si ha un collegamento diretto (livello 2) ad un router che è parte di Internet.

Punto di vista fisico

Host

- Dial-up connection
- High speed connection
- Wireless
- LAN

Network -> router

- Leased Line
- DSL/cable modem
- MAN/WAN
  - Frame relay
  - ATM
  - Ethernet
- LAN

Punto di vista del protocollo

Host

- IP Address
- Line protocol
  - PPP
  - SLIP
  - Ethernet

Network

- IP Address pool
- Routine protocol
- Line protocol
  - PPP
  - HDLC
  - Frame Relay
  - ATM
  - Ethernet

Accesso Dial-up

Caratterizzato da:

- Line protocol (protocollo di linea):
  - PPP
  - SLIP
- Address negotiation (negoziazione dell'indirizzo):
  - PPP -> IPCP
  - SLIP -> non standard, text based

Accesso DSL/cable modem

Accesso alle reti IP – Unbundling

Local Loop Unbundling

Il local loop unbundling consiste nell'utilizzo di componenti e o servizi della rete da parte di un altro operatore. Unbundling significa disaggregazione.

- Il regolamento lo impone all'operatore dominante
- Per esempio, obbligo di fornitura presso le centrali di spazi per la collocazione di apparati di operatori alternativi
- Escluso qualsiasi obbligo d'investimento in nuove infrastrutture

Unbundling: disaggregazione

- Mezzo fisico: affitto del portante trasmissivo
  - Doppini in rame
  - Fibra nuda
- Accesso al canale trasmissivo:
  - Canali numerici: bitstream access

Altri servizi correlati:

- Co-locazione (fisica o virtuale)
- Condivisione di infrastrutture civili
- Prolungamento di accesso nel caso di stadi di linea remotizzati

Le opzioni per i nuovi operatori

- Posa di infrastruttura trasmissiva
- Affitto della infrastruttura trasmissiva fino al cliente – Copper Rental
- Affitto di un canale trasmissivo – Bit Stream Access
- Raccolta indiretta – Carrier Selection
- Rivendita di traffico – Reselling

xDSL e cable modem

Queste due soluzioni sono state preferite rispetto ad altre perché possono sfruttare l'infrastruttura già esistente. In particolare queste tecnologie permettono l'accesso a banda larga in modo capillare.

- Doppino telefonico -> xDSL
  - Digital Subscriber Loop
- Cavo coassiale della TV -> cable modem

Trasmissione

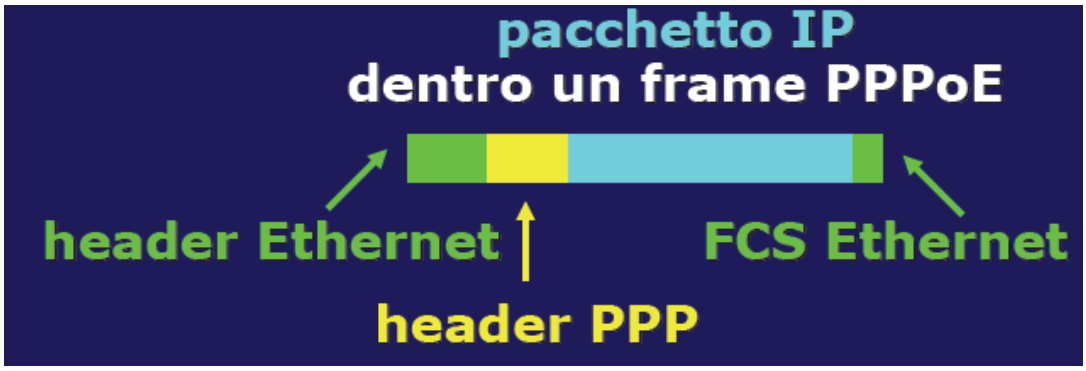
La trasmissione avviene sfruttando:

- Codifiche di linea molto sofisticate
  - Complesse modulazioni di ampiezza e di fase
- Velocità di trasmissione adattativi
  - In caso di interferenze si ha la diminuzione della velocità
  - La velocità è solo nominale

Unbundling logico e fisico

Architettura protocollare

PPPoE è utilizzato sulla tratta dal router o modem ADSL dell'utente e il DSLAM della centrale telefonica. Normalmente i frame ethernet sono modificati.



ADSL (Asymmetrical Digital Subscriber Line)

Le caratteristiche generali dell'ADSL sono:

Velocità elevata in ricezione fino a 8Mb/s
Velocità più bassa in trasmissione fino a 1Mb/s
Ideale per navigare in Internet
NON ADATTO A CONNESSIONI DIRETTE
Per esempio tra due sedi
Usa una coppia di doppini
Coesiste con la telefonia tradizionale

HDSL (High bit rate DSL)

Le caratteristiche generali dell'HDSL sono:

- Usa due coppie di doppini
- Non è compatibile con la telefonia tradizionale
- 2Mb/s bidirezionale

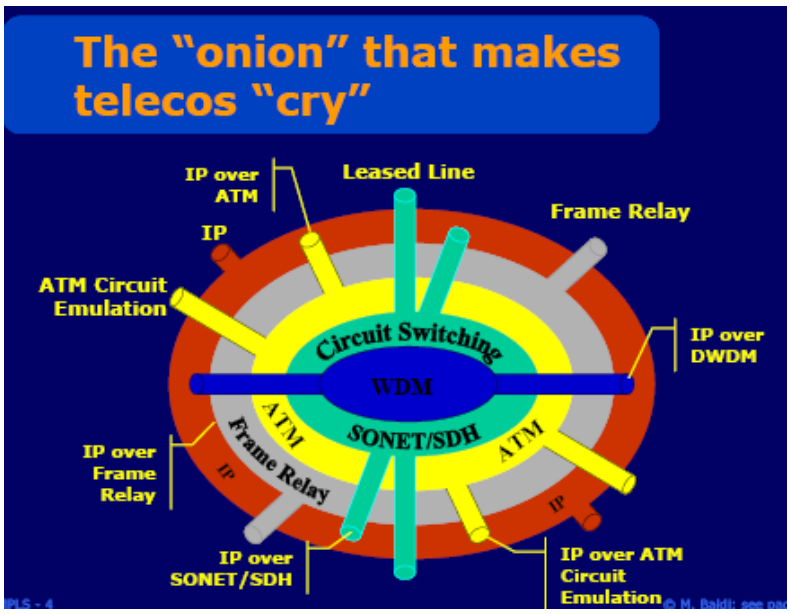
SHDSL (Symmetric DSL)

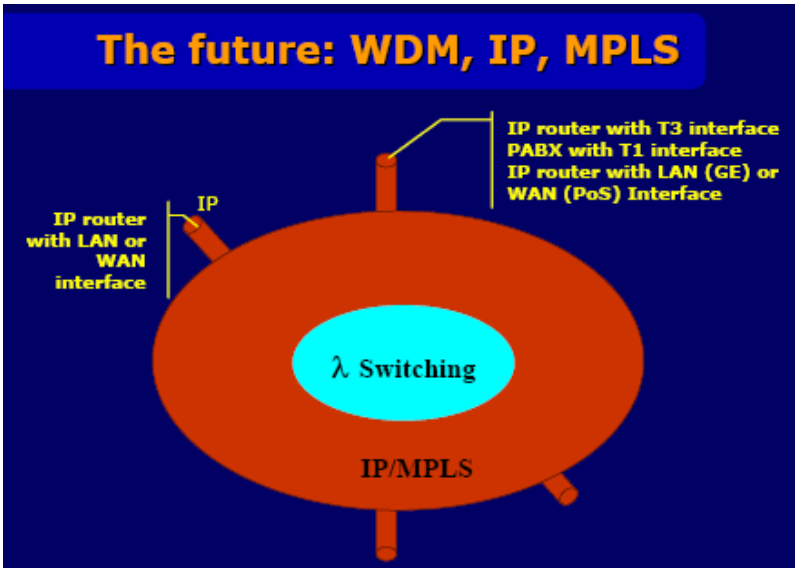
L'SHDSL è una soluzione derivata da HDSL, le sue caratteristiche sono:

- velocità comprese tra 256Kb/s e 2Mb/s
- la simmetria si presta
  - alle connessioni dirette
  - all'accesso ad Internet

MPLS (Multi-Protocol Label Switching)

MPLS è probabilmente la tecnologia abilitante per la nuova rete pubblica broadband (IP). MPLS introduce il paradigma connection-oriented nelle reti IP.





L'idea alla base di MPLS

inserire un'etichetta davanti al pacchetto ip
instradare i dati utilizzando l'etichetta e non l'indirizzo IP

questo permette di:

- ottenere un lookup più veloce, l'etichetta può essere usata come indice
- Traffic engineering: questa è la caratteristica migliore
- Grazie a questa idea, MPLS introduce il paradigma connection-oriented nelle reti IP

Architettura della rete

E' formata da due tipi di apparati:

- Label Switch Router LSR

- Label edge router ingress/egress LSR

Evoluzione di MPLS

- Tag switching
- IP on ATM
  - Nessun problema nella risoluzione degli indirizzi
  - Segnalazione semplice
  - Un solo piano di controllo
- ATM con IP
  - Riutilizzo degli switch ATM
- MPλS (Multi Protocol Lambda Switching)
- G-MPLS (Generalized MPLS)
  - Commutazione di pacchetto
  - Commutazione di cella
  - Commutazione di circuito (SONET/SDH)
  - Lambda switching
  - Anything switching
  - Piano di controllo unificato

Elementi chiave di MPLS

- MPLS header: contiene l'etichetta
- Upgrade dei protocolli di routing: scelta dei percorsi sottoposti a vincoli
- Protocolli per la distribuzione delle etichette: segnalazione

ATM e Frame Relay

- Protocolli di livello 2 connessi
- Etichette MPLS nell'intestazione di livello 2
  - VCI/VPI in ATM
  - DLCI in Frame Relay

Forwarding Equivalence Class (FEC)

I pacchetti che seguono lo stesso percorso nella rete MPLS o vengono trattati allo stesso modo da ogni LSR ricevono la stessa etichetta.

Label Binding

Lo switch a valle di un collegamento associa le etichette usate dallo switch a monte a:
Porta di uscita
Nuove etichette

Creazione degli LSP

Label Binding Statico

- Attraverso management
- Equivalente a PVC ATM
- NON SCALABILE

- No interoperabilità tra sistemi di gestione
- IMPOSSIBILE AVERE LSP TRA GESTORI DIVERSI

Label Binding Dinamico

- Protocol (IP) driver
  - La creazione di LSP è legata alla scoperta di route verso le destinazioni
- Creazione automatica di LSP
  - Segnalazione esplicita
  - Iniziato dai label EDGE router

Protocolli di distribuzione delle etichette

Tre alternative incompatibili:

- Routing Protocol: BGP, solo protocol driver
- Label Distribution Protcol: LDP, progettato per lo scopo
- RSVP: allocazione nelle reti Integrated Services

Protocolli di routing

Sono utilizzati per determinare l'instradamento degli LSP, guidano le procedure Label Binding ed in modo indiretto determinano l'instradamento dei pacchetti. I protocolli esistenti sono OSPF, IS-IS e BGP-4 e trasportano le informazioni sulla topologia, nel contesto MPLS devono essere potenziati per PORTARE INFORMAZIONI SUI VINCOLI DEL ROUTING, in particolare:

- Capacità dei collegamenti
- Utilizzazione dei collegamenti
- Dipendenze tra i collegamenti (utilizzato per il recupero dai guasti)

Extensive Routing Protocol

Il ROUTING CON VINCOLI (Contraint based routing) è fondamentale per il supporto del TRAFFIC ENGINEERING: OSPF-TE, IS-IS-TE

Hop by Hop routing

Con questa modalità di routine ogni switch decide il prossimo passo dell'LSP. Questa modalità è simile al routing per i pacchetti IP

- Gli switch si accordano sulle corrispondenze tra:
  - Etichetti di ingresso e uscita
  - Etichette e FEC

Explicit Contraint based routing

In questa modalità un singolo switch può scegliere l'intero percorso dell'LSP. La scelta può essere fatta da Ingress LSR o Explicit routing. La scelta è BASATA SU VINCOLI.

Distribuzione delle etichette

La distribuzione delle etichette deve essere modificata:

- CR-LDP: Contraint based Routing LDP
- RSVP-TE: RSVP for Traffic Engineering
- Sono abbinati a OSPF-TE e IS-IS-TE

Nuove possibilità offerte

- Traffic engineering: permette la distribuzione del traffico sui vari collegamenti in base ai vincoli:
  - Nessuna congestione
  - Utilizzo uniforme
- Qualità del servizio: non realizzata
- Classi di servizio differenziate
- Scalabilità
- Supporto delle VPN IP
- Recupero dei guasti veloce: in meno di 50 ms

Piano di controllo e piano dati

Traffic Engineering

Gli obiettivi principali del traffic engineering sono:

Mappare il traffico in modo efficiente sulle risorse disponibili

Controllare l'utilizzo delle risorse

Ridistribuire il traffico in modo rapido ed efficace in risposta ai cambiamenti di topologie della rete

Agire in modo complementare al network engineering, disponendo della capacità della rete in corrispondenza del traffico

Traffic engineering senza MPLS

- ATM è stata utilizzata per molto tempo per il traffic engineering sulle reti IP
- 2 piani di controllo perché i router sono ATM-unaware
- elevato numero di adiacenze: scalabilità limitata

Traffic enginnering con MPLS

- MPLS è IP-aware!
- 1 solo piano di controllo opera sulla topologia fisica
  - semplice
  - elevata scalabilità

Estensioni di MPLS

- MPλS (Multi-Protocol Lambda Switching):
  - Piano di controllo MPLS nelle reti ottiche
  - Efficace nel traffic engineering
- GMPLS (Generalized MPLS):
  - Piano di controllo MPLS in ogni rete: a pacchetto, circuito, ottico

Class of Service e Quality Of Service

Le risorse e le modalità dei servizi possono essere associati alla FEC all'inizializzazione dell'LSP. E' necessario un supporto esplicito nel data plan e nel control plan dell'LSR

Class of Service CoS

- Priorità relativa fra differenti FECs

- Offre garanzie
- Supporto del modello DiffServ:
  - Per Hop Behavior
  - Per EF e AF
- Traffic engineering per le classi: DS-aware traffic engineering

Quality of Service QoS
Specifiche garanzie per banda, ritardo e dimensione dei burst.

Vantaggi della QoS in MPLS
SLOGAN: Rete unificata che sostiene tutti i tipi di servizio

- Supporto per QoS e servizi real-time su IP non ancora pronto
- Molte delle reti multi servizio (multi-service networks) ora hanno il paradigma ships-in-the-night:
  - I protocolli ATM sono tipici servizi ATM
  - Piano di controllo MPLS per servizi IP

MPLS e scalabilità

- Le etichette di MPLS introducono gerarchia: è necessario un certo numero di livelli gerarchici per permettere la scalabilità
- Le tabelle di routine dei router di transito non dovrebbero essere complete: LSP tra border router
- Semplice e veloce ricerca delle etichette rispetto al long-prefix match

VPN Virtual Private Network in MPLS

Servizio simile ad una rete privata in cui i dati sono trasportati su infrastruttura pubblica (IP):

- overlapped piano di indirizzamento: no indirizzi univoci (vale per ind. Privati, quindi i privati possono usare gli stessi indirizzi)
- CoS & QoS
- L'etichetta nasconde gli indirizzi IP degli utenti sulla rete pubblica
- MPLS permette una soluzione scalabile per i servizi VPN:
  - Numero di VPN
  - Numero di membri per VPN
  - Altri approcci devono essere impostati manualmente attraverso tunnel tra website
- Flessibilità del servizio grazie alla FEC
- Standardizzazione attraverso IETF e MPLS Forum

VPN Virtual Private Network

Definizione

Connettività personalizzata distribuita su una infrastruttura di rete pubblica che grazie ad alcune politiche permette di utilizzare un servizio come se ci fosse un collegamento diretto.

Le tipologie di infrastruttura pubblica possono essere la rete IP, Frame Relay, ATM. Le politiche possono riguardare la sicurezza, la tolleranza ai guasti, la QoS. Le VPN permettono di tagliare i costi rispetto ad un collegamento diretto o dedicato.

Le VPN permettono di ottenere un accesso flessibile e selettivo alla rete corporate:

- Servizi limitati sono disponibili a utenti esterni: sicurezza, pochi servizi sono permessi attraverso il firewall
- Tutte le funzionalità di intranet sono permesse agli utenti corporate che accedono da internet

Caratteristiche

- Access VPN o Remote VPN o virtual dial in
  - Connessione dei terminali alla rete remota
  - Virtualizzare la connessione d'accesso (dial-up): ISDN, PSTN, DSL
  - PPTP, L2TP
- Site-to-site VPN
  - Connette reti remote
  - Virtualizza le linee dedicate
  - IPsec, GRE, MPLS

Scenari di VPN

- Intranet VPN: interconnessione di sedi corporate, uffici remoti
- Extranet VPN: interconnessione per i clienti, fornitori, partners, comunità
- Remote user access: telelavoro, clienti, partner, impiegati di viaggio

Intranet VPN e Extranet VPN

Site-to-site VPN
Shared infrastructure: rete di un service provider, due o più reti di service provider, internet
Accesso all'infrastruttura condivisa: DSL, leased line, fibra, ethernet
Tecnologie: IPsec, GRE, MPLS

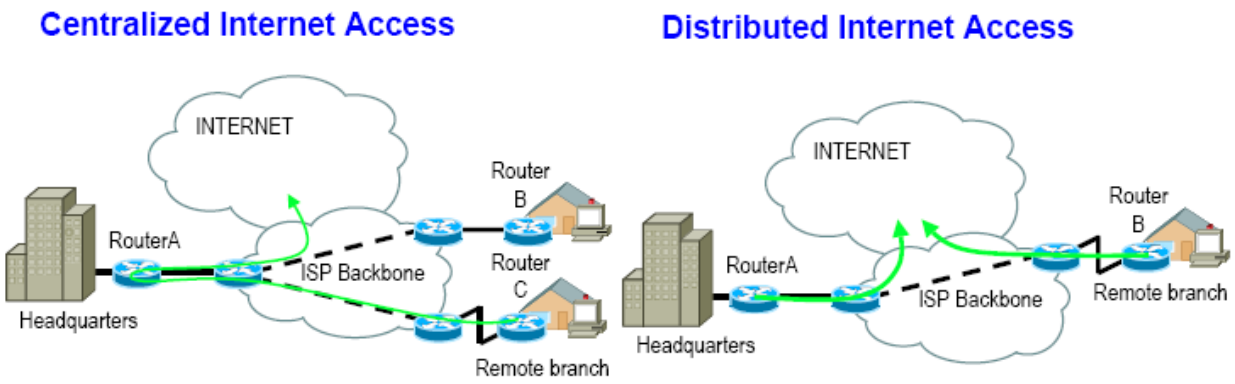
In più, per le reti Extranet è previsto:

- Accesso ristretto alla rete per le reti connesse: firewall sulla VPN
- Address clash: NAT

Remote user access

- Shared infrastructure: rete di un service provider, internet
- Accesso all'infrastruttura condivisa mediante ISDN, PSTN, DSL, WLAN
- Tecnologie: PPTP, L2TP, IPsec (implementato dal device utente)

Internet Access



VPN Service Provision

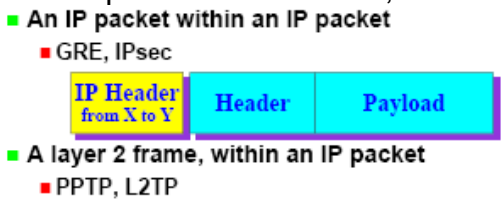
- Modello Overlay: i router della rete non sono a conoscenza dell'esistenza della VPN
  - Basato su IPsec
  - Realizzazione mediante tunneling
  - Ogni VPN gateway deve conoscere ogni altro VPN gateway
- Modello Peer: tutti i router della rete conoscono e gestiscono la VPN
  - MPLS network
  - Ogni VPN gateway conosce solo il suo router peer pubblico:
    - Scambio delle informazioni di routine
    - La rete del service provider diffonde le informazioni di routine
  - I router pubblici instradano il traffico tra gateways della stessa VPN

Tassonomia

Tunneling

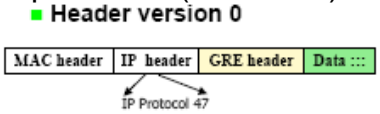
Un pacchetto o una trama è trasportato attraverso una rete IP dentro un pacchetto IP, tipologie:

- Pacchetto IP dentro pacchetto IP: GRE, IPsec
- Trama di livello 2 dentro un pacchetto IP: PPTP, L2TP



GRE Generic Routing Encapsulation

Incapsulazione (tunneling) di ogni protocollo (incluso IP) dentro IP



IPv4 Encapsulation and Routing Information

- IP address List: source routing information, lista dei router da attraversare
- SRE offset: byte dell'indirizzo IP del next hop, aggiornato ad ogni source route hop

- SRE Length: lunghezza totale della lista di indirizzi

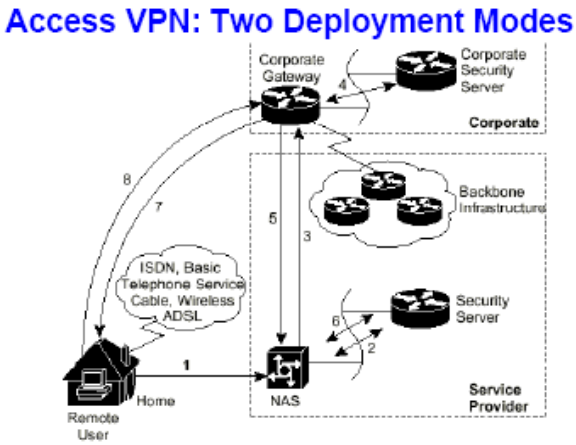
Enhanced GRE (versione 1)

- Schierato da PPTP
- Acknowledgment Number: la consegna dei pacchetti ent-point può essere comunicata

(Virtual) VPN Topologies

- Hub e spoke:
  - Ogni ramo comunica direttamente con la sede centrale
  - Adatto al flusso dati di molte aziende
  - L'ottimizzazione del routing è secondaria
  - Limitato numero di tunnel: difficile da configurare manualmente
  - L'hub può diventare un collo di bottiglia
- Mesh:
  - Elevato numero di tunnel: facile da configurare manualmente
  - Routing ottimizzato

Access VPN: Due modalità di schieramento



Provider Provisioned Deployment Mode

1. L'utente remoto inizia una connessione PPP con il NAS
2. il NAS identifica l'utente
3. il NAS inizializza un tunnel L2TP o PPTP verso il corporate gateway
4. il corporate gateway autentica l'utente in accordo con le politiche di sicurezza
5. il corporate gateway conferma l'accettazione del tunnel
6. il NAS crea un log e registra eventualmente anche il traffico
7. il corporate gateway costituisce una negoziazione PPP con l'utente remoto
8. tunnel end-to-end tra l'utente ed il corporate gateway

Virtual Dial-UP, punti salienti

autenticazione e sicurezza: eseguita dal gateway VPN, politiche della rete corporate
autorizzazione: eseguita dal gateway VPN
allocazione dell'indirizzo: gli indirizzi corporate sono allocati dinamicamente, stesso accesso come quando si è direttamente connessi

Access VPN: Due protocolli

- L2TP: Layer 2 Tunneling Protocol
  - Non molto implementato nei terminali
  - Indipendente dal protocollo di livello 2
  - Sicurezza attraverso IPsec, forte ma complicata
- PPTP: Point to Point Tunneling Protocol
  - Multiprotocollo
  - Debole crittografia e autenticazioni
  - Gestione della chiave proprietaria

Layer 2 Tunneling Protocol

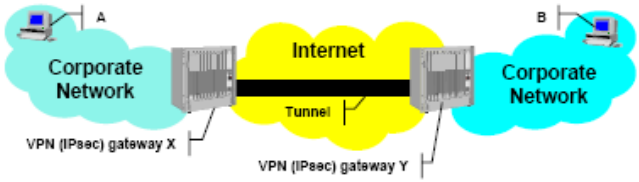
- Tunneling tra punto d'accesso pubblico e corporate network, anche tra service provider diversi
- L2TP Access Concentrator LAC: device d'accesso che supporta L2TP, NAS (Network Access Server)
- L2TP Network Server LNS: corporate VPN gateway
- CPE include le funzionalità di LAC
- L2TP Header: control message e data message

Point to Point Tunneling Protocol

- Adottato da IETF
- Microsoft encryption: MPPE
- Microsoft Authentication: MS CHAP
- PPTP Network Server PNS: corporate VPN gateway
- PPTP Access Concentrator PAC: per il provider provisioning deployment mode
- PPTP Data Tunneling:
  - Data transport
  - PPP tunneling
  - GRE
- Control connection:
  - Tunnel data session setup, gestione e abbattimento
  - Incapsulazione TCP

IPsec VPNs

Instaurazione di un tunnel tra due VPN gateway, con crittografia, autenticazione ed incapsulazione.



VPN Gateway e Firewall

- Interno: nessuna ispezione del traffico VPN, il gateway VPN è protetto dal firewall
- Parallelo: potenzialmente accesso incontrollato
- Esterno: il VPN gateway è protetto da un router
- Integrato: massima flessibilità

VPN gateway e NAT

Authentication Header:

Gli indirizzi IP sono parte del checksum dell'AH (Authentication Header), i pacchetti saranno scartati

Transport mode:

Se gli indirizzi IP del tunnel IPsec non sono come ci si aspetta, i pacchetti saranno scartati

No PAT (Protocol Address Translation)

Tunnel mode:

Gli indirizzi IP dentro i pacchetti crittografati possono essere cambiati prima di entrare nel gateway, per esempio stesso indirizzo in 2 VPN sites

Molto spesso il NAT non è necessario per i pacchetti esterni

IP-based peer VPNs

Dedicated router: il service provider costituisce una rete di router dedicati per il cliente, solo per i clienti più grossi

Shared/virtual router: il service provider crea un'istanza di router dedicato dentro i suoi router

ASIC

Scambio di pacchetti attraverso IPsec o tunnel GRE

MPLS-based Layer 2 VPNs: PWE3

- Pseudo Wire Emulation End-to-End
- Molti servizi sulla stessa rete: ip, linee dedicate, frame relay, ATM, ethernet
- Customer Edge (CE) dispongono in modo nativo delle caratteristiche necessarie
- Il traffico è trasportato attraverso LSP tra Ces
- 2 etichette:
  - esterna: per routing all'interno della rete, identifica il punto d'accesso della rete
  - interna: multiplazione di diversi usenti/servizi sullo stesso punto d'accesso
- dovrebbe esserci dei dispositivi di aggregazione all'interno della rete
- principalmente configurazione manuale degli LSP

MPLS-based Layer 3 VPNs

- soluzione provider provisioned: le politiche sono implementate dall'ISP, il cliente non deve fare nulla
- scalabilità

- due soluzioni alternative:
  - BGP
  - Virtual router

MPLS/BGP VPN components

- VRF (VPN Routine Forwarding) table:
  - Associato ad una o più porte
  - Le informazioni d'inoltro sono usate per il traffico ricevuto attraverso la porta
- PE routers:
  - Scambiano le informazioni di routine
  - Sono ingress e egress LSR per il backbone

MPLS VPN components

- CE router creano adiacenze con i PE router:
  - informano delle loro destinazioni
  - ricevono informazioni sulle destinazioni delle VPN
  - routine statico o IGP
  - E-BGP
  - PE router non hanno informazioni su tutti i router di tutte le VPNs

Control plane

- Scambio di informazioni di routine alla periferia basato su MP-BGP
- Route filtering: i PE router determinano quali router installare in VRF
- Supporto per l'overlapping (sovrapposizione) degli spazi di indirizzamento
- Instaurazione di LSPs attraverso il backbone

Packet Routing

Benefici

- Nessun vincolo sul piano d'indirizzamento: indirizzi univoci solo all'interno di ogni VPN
- CE router non scambiano informazioni
- I clienti non devono preoccuparsi di gestire i backbone
- I provider non devono avere un backbone virtuale per cliente
- Le VPN possono estendersi attraverso diversi provider
- Sicurezza equivalente a frame relay o ATM: traffico isolato, non c'è crittografia
- QoS supportato attraverso gli experimental bits nell'MPLS header

MPLS/Virtual Router VPNs

- I router PE eseguono un'istanza virtuale per ogni VPN
- Ogni istanza virtuale di routing (VR) ha strutture dati separate
- Le VRs della stessa VPN comunicano attraverso LSP

Multi-Protocol Support

Access VPN:
    Trasparente: L2TP, PPTP
Overlay (IPsec based): GRE, trasporta ogni protocollo di livello 3 all'interno del pacchetto IP
Peer (MPLS based)

IPsec - Internet Protocol security

Descrizione

- Application layer security: security email, DNS, SSH
- Trasnport layer security: SSL
- Network layer security: IPsec:
    - Protezione delle intestazioni IP, TCP e UDP
    - Autenticazione di IP, TCP e UDP

IPsec

- Struttura per rispondere a problemi di sicurezza standard e flessibile
- Basato sulla crittografia
- Può essere usato il tunnel
- Trasparente alle applicazioni e agli utenti

IPsec e crittografia

Un paio di chiavi di sessione condivise per le direzioni di comunicazione:
    Una per la crittografia dei dati
    Una per l'autenticazione
Le chiavi condivise devono essere accettate
Le chiavi di sessione sono cambiate regolarmente per incrementare la robustezza
Scambio della chiave:
    Manuale
    Dinamico, automatico: IKE

IKE Internet Key Exchange

Autenticazione delle parti comunicanti, es tunnel endpoint
Certificato digitale per valicare le chiavi pubbliche
Scambio delle chiavi:
    Diffide-Hellman
    Public key cryptography per firmare lo scambio di chiavi
    DES
Serve per accordarsi su:
    Protocolli
    Algoritmi di crittografia e autenticazione
    Chiavi: shared secret e digital certificates

SA Security Association

- Accordo che abilita lo scambio dei dati
- Per autenticazione e segretezza è richiesto un SA per ognuno
- Un SA include:
  - Session keys
  - IP address degli endpoint (può essere un prefisso di una subnet)
  - IP address per gli IPsec gateway
  - Scadenza della chiave di sessione: quando la chiave è scaduta bisonga rifare la SA

Implementazione

- Sul client
- Sul gateway: software o hardware
- Indipendente dall'algoritmo

SSL – Secure Socket Layer

Sostituisce l'interfaccia dei socket tradizionali, fornendo sicurezza nella trasmissione dei dati. Supporta qualsiasi applicazione come http, FTP … Garantisce riservatezza, autenticazione ed integrità. Si basa su:

- SSL handshake protocol
- SSL record protocol

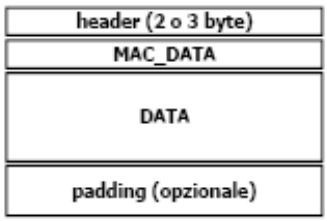
SSL Handshake protocol

Per aprire una sessione tra server e client è necessario:

- Autenticare gli endpoint tramite certificato o chiave condivisa
- Concordare gli algoritmi di cifratura, autenticazione ed integrità
- Concordare le chiavi

SSL Record protocol

- Consente di incapsulare dati e informazioni di autenticazione
- I messaggi SSL sono accorpati in record lunghi fino a 32K



SSL VPN

L'SSL è il meccanismo centrale su cui si basa l'accesso sicuro

- Site to site VPN
- Remote access VPN

- Secure Service Access
- Tunneling basato su TCP o UDP

IPsec vs SSL

IPsec VPN

- IPsec è troppo difficile o troppo costoso da usare in modo sicuro: troppe opzioni da configurare e amministrare
- Opera nello spazio del kernel:
  - I guasti potenzialmente possono essere catastrofici
  - Installazione difficile e rischiosa

SSL VPN

- Bassa complessità di installazione, configurazione e gestione
- Non interferisce con il kernel
- Ampiamente usata -> sicurezza più elevata
- IPsec VPN connette le reti, oppure host a reti
- SSL VPN connette:
  - Utenti ai servizi
  - Application client to application server
- Nessun codice aggiuntivo da installare
- Applicazioni disponibili tramite web browser
- Non è una soluzione generale di sicurezza

In sostanza:

- SSL VPN hanno buone chance di lavorare su ogni scenario di rete
- Possono realizzare tunnel TCP o UDP
- Possono attraversare NAT, firewall e router
- Le SSL VPN possono ABILITARE CLIENT UNIVERSALI COME IL WEB BROWSER

Rispetto ad IPsec:

- Nessun problema con il NAT traversal:
  - Non c'è AH
- Pacchetti scartati ad alto livello: può essere critico con attacchi DoS

Rispetto a PPTP:

- Inizialmente proprietario
- Inizialmente sicurezza debole
- Scarsa interoperabilità
- GRE tunneling: possono essere bloccati dai router

Caratteristiche delle SSL VPN

Pseudo VPN:

- Web proxing
- Application translation
- Port forwarding
- SSL'ed protocols
- Application proxing

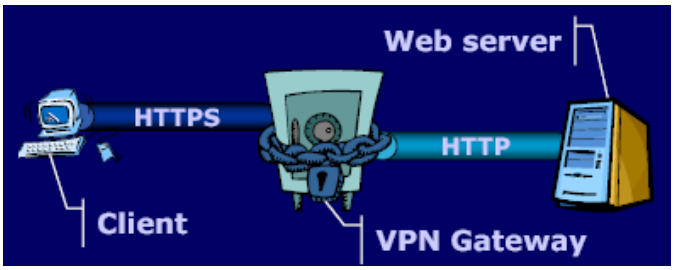
VPN:

Network extension: site-to-site connectivity

Proxing

VPN gateway scarica le pagine attraverso HTTP

Le trasporta verso il client attraverso HTTPS

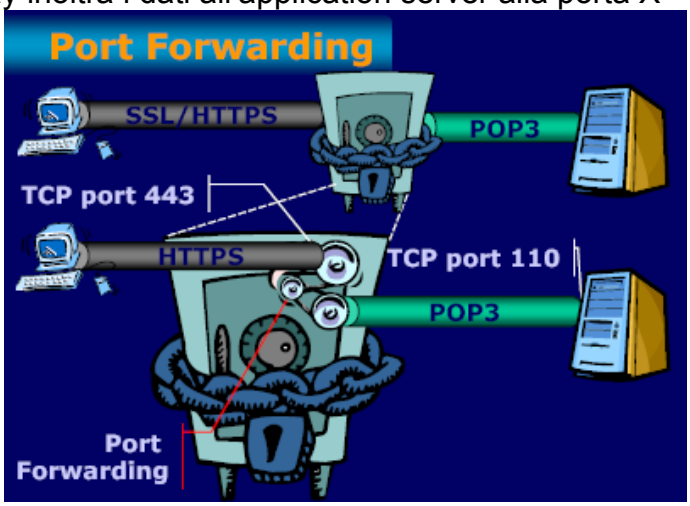


Application Translation

- Protocolli nativi tra il gateway VPN e gli application server, per es. POP, FTP …
- L'applicazione usa l'interfaccia come una pagina web
- HTTPS tra VPN server e client
- Non è adeguato per tutte le applicazioni

Port Forwarding

- Port forwarder sul client: necessita di software aggiuntivo, dipendente dalla piattaforma, Java o Active X
- L'applicazione punta a localhost alla porta X (solita porta dell'applicazione)
- Il port forwarder spedisce i dati attraverso SSL al VPN gateway alla porta Y (spesso HTTPS 443)
- Il VPN gateway inoltra i dati all'application server alla porta X



Funziona solo con protocolli che utilizzano una porta fissa

Problemi con indirizzi e porte nei protocolli di livello applicazione:

SSL-VPN gateway deve conoscere il protocollo di applicazione da tradurre

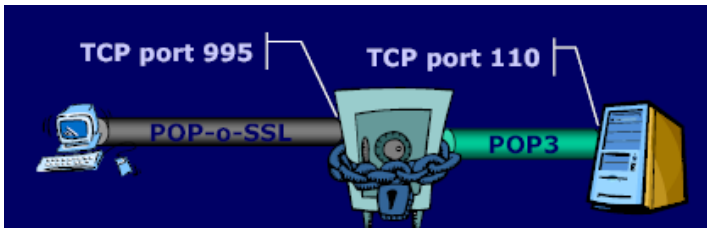
Application layer gateway ALG

SSL'ed Protocols

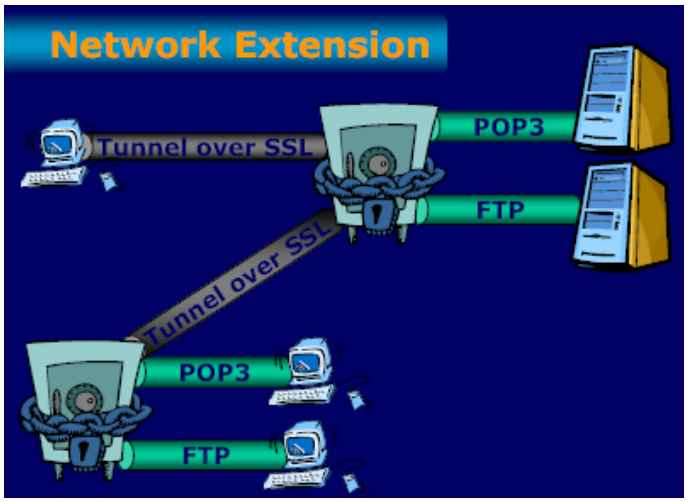
Secure application protocols
Protocollo sopra SSL, per es. POPS
È necessario il supporto sia sul server che sul client

Application Proxing

- Compatibilità con i vecchi server
- Il client punta a SSL VPN gateway



Network Extension



Prodotti disponibili

Vi sono diversi prodotti e produttori disponibili, alcuni opensource, altri no. Tuttavia le maggiori problematiche risiedono:

- Interoperabilità
- Specifiche caratteristiche dei prodotti
- Possibili implementazioni deboli
- Disponibilità di client per una specifica piattaforma

Gestione e monitoring di rete

Il network monitoring consiste nell'osservazione e all'analisi dello stato e del comportamento dei dispositivi di rete, degli end system, dei collegamenti, del traffico di rete e delle applicazioni di rete. E' necessario eseguire network monitoring per i seguenti aspetti:

- Statistiche di rete: per ottimizzazione, planning, hardening
- Network mapping ed inventario: per conoscere i dispositivi in rete
- Sicurezza: identificare i servizi o server non ufficiali che possano provocare problemi alla sicurezza della rete o del sistema. Detenzione delle violazioni della sicurezza attraverso IDS
- Trobleshooting: identificazione dell'hardware difettoso, mancanza di connettività, risorse e servizi disponibili
- Accounting: mantenere le registrazioni (log) di ciò che fanno gli utenti della rete

Elementi da monitorare

- Traffico: forse il più importante
  - Misure: quando si sa esattamente cosa monitorare
  - Generic monitors: quando non si sa esattamente cosa monitorare
  - Caratterizzazione del traffico: quando si vuole costruire un modello del traffico generato
  - Sonde: quando si vuole sondare la rete
- Disponibilità dei collegamenti, risorse e servizi
- Eventi e Alert

Lo strumento ntop

Ntop è uno strumento per misurare il traffico che supporta diverse attività di gestione tra cui: ottimizzazione della rete, planning, individuazione di violazioni di sicurezza.
Caratteristiche funzionali di ntop:

- Misure sul traffico
- Caratterizzazione del traffico e monitoring
- Ottimizzazione e planning di rete
- Rilevazione di anomalie attraverso alcuni parametri comuni di traffico
- TCP/IP stack verification: per es. rilevazione di portscan, DOS, IDS
- Intrusion detection: trojan, spoofing

Approcci al network monitoring

Vi sono due tipi di approcci al network monitoring:

- Attivo: il sistema che deve essere monitorato è periodicamente sondato da segnali esterni
- Passivo: una sonda colleziona silenziosamente dati e trae alcune proprietà da questi

Network monitoring attivo

Spesso è basato su traffico specifico/racket patterns, generato specificatamente per scopi di monitoring: per es. pacchetti ICMP. E' utilizzato per misure di ritardo. Alcuni esempi sono RIPE, pingER, nmap.

Network monitoring passivo

E' l'approccio più usato, è preferito perché non è intrusivo. E' utilizzato per misure di traffico, caratterizzazione e monitoring. Le tecnologie disponibili sono: racket sniffing, SNMP, RMON, netflow, sFlow, IPFIX.

Network monitoring passivo: packet based approach

Lo sniffing è l'attività che permette di catturare esattamente tutto il traffico che è trasferito su un cavo o su uno specifico segmento di rete. E' caratterizzato da:

Visione dei pacchetti molto dettagliata
Le problematiche dei link-layer sono difficili da identificare (es. ethernet collision)
Sono processati molti dati
Problematiche sulla privacy

Sniffing nei dispositivi di rete

- E' difficile ottenere esattamente la traccia dei pacchetti voluti:
  - SNMP non permette la cattura del traffico
  - RMON permette la cattura del traffico solo utilizzando maschere predefinite
  - Cisco Netflow non permette la cattura del traffico
  - sFlow permette la cattura ma è poco personalizzabile
  - la nuova intestazione che contiene il pacchetto, a volte alcune informazioni chiave sono mancanti, per es. le interfacce d'origine
- IETF PSAMP dovrebbe essere utile
- Richiede hardware ad-hoc, altrimenti le risorse sono rubate dai router

Problematiche legali dello sniffing

- Bisogna accertarsi che sia legale nel paese dove ci si trova
- E' consentito fare sniffing per: sicurezza nazionale, prevenire o individuare un crimine, per prevenire o individuare utilizzi non autorizzati, per accertarsi delle operazioni del sistema
- E' necessario accertarsi che l'identità di chi spedisce o riceve i dati non possa essere inferita dai dati catturati: si utilizza address masquerating e dati aggregati

NM passivo: approccio SNMP

- Permette di ottenete statistiche generiche, stato della rete: non molto usato per la configurazione della rete
- Definisce meccanismi per la gestione remota dei dispositivi di rete
- Principio fondamentale: TUTTA LA GESTIONE DEL DISPOSITIVO E' ESEGUITA DALLA SEMPLICE MANIPOLAZIONE DI VARIABILE
- Approccio:
  - Standard per specificare le quantità riconosciute dai dispositivi
  - Protocollo per richiesta e risposta, notifica dei valori cambiati

Architettura

i componenti sono:

- Protocollo per scambiare informazioni tra Agent e Management Entity: SNMP
- Definizione degli oggetti che possono essere letti/modificati: MIB
- Sintassi usata per specificare la Management Information Base: SMIv2

Struttura della MIB

- SMIv2 definisce le regole per creare le MIB ed è basato su variabili di tipo: basato su ASN.1
- Caratterizzazione delle variabili definite da SMI:
  - Datatype
  - Non implementano complesse strutture dati e operazioni sulle variabili
  - Le variabili sono scalari o colonne in una tabella a 2 dimensioni
- Organizzata secondo una gerarchia

ASN.1 identificazione di oggetti

- Le variabili sono identificate globalmente da una stringa unica di cifre
- I nomi di variabili sono alias per le stringhe di cifre (dentro MIB)

SNMP Message Encoding

- Codifica del messaggio come stream di byte usando ASN.1
- Quantità codificate come Type, Length, Value triples

SNMP Encapsulation

- UDP, agent port: 161, management entity port : 162
- La consegna delle informazioni di management è particolarmente importante durante congestioni o operazioni improprie sulla rete
- TCP non è adatto, anche se supportato

SNMPv3

- SNMP sempre più usato per il controllo, funzionalità in più rispetto al monitor, operazioni di write
- Aggiunge sicurezza: poco implementato, molti hanno problemi di implementazione

Network monitoring con SNMP

- Possibile catturare e creare valori verso obiettivi stabiliti: le informazioni raccolte da SNMP possono essere usate per NM: per es. arrivi dei pacchetti, partenze degli stessi, carico del dispositivo
- Alcuni tools sono MRTG e HP OpenView

Alcune problematiche di SNMP

- Spesso i dati possono essere esportati solo attraverso MIB proprietarie: è difficile gestire reti multivendor
- Non si può aggiungere una nuova MIB dentro un agente:
  - Non è possibile personalizzare le variabili necessarie a monitorare il traffico
  - Aggiungere una nuova MIB nella Management Station è semplice

Passive NM: RMON

- Definisce un metodo di monitorare in remoto le MIB: in aggiunta al set base di SNMP
- Con RMON e MIBII, il network manager può ottenere informazioni che sono locali individualmente per ogni dispositivo. Si ha il concetto di collision domain
- Caratteristiche:
  - Utilizzato per monitoring passivo per i dati trasmessi sui segmenti delle LAN
  - Fornisce interoperabilità tra SNMP-based management console e i monitor remoti
- Punti focali, goals:
  - Off-line implementation: RMON MIB permette ad una sonda configurata di eseguire la diagnostica quando si ha assenza di comunicazione con la stazione gestita
  - Proactive monitoring: il monitor può continuare ad eseguire log e diagnostica sulle performance della rete, in caso di guasto il monitor può fornire questa informazione alla management station
  - Problem detecntion and reporting: il monitor può essere configurato per riconoscere condizioni di errore ed eventualmente notificarle alla management station
  - Value added data: il remote monitoring device può registrare gli host che hanno generato più errori di traffico
  - Multiple managers: un'organizzazione può avere più stazioni di gestione, allora il monitor può essere configurato per dialogare con più di una stazione di management in modo concorrente

RMONv1 vs RMONv2

RMONv1 è stato progettato per i protocolli di basso livello, sotto IP

RMONv2 è stato progettato per monitorare i protocolli di alto livello, estende quindi la versione 1 aggiungendo 9 gruppi

RMONv2 Time Filter

- Tabella che contiene elevato numero di valori: traffico per ogni host verso altri della rete
- Richiamare i dati di tutta la tabella può essere costoso
- Il Time Filter permette di ottenere solo i valori che sono cambiati dopo un certo tempo T specificato

Problematiche di RMON

L'implementazione degli agenti RMON e delle stazioni di gestione è molto complesso: normalmente RMON è inserito in hardware

Personalizzazione: non si possono aggiungere nuove funzionalità alle MIB esistenti, è quindi necessario comprare nuovo hardware

Non molto usato

Passive NM: Flow-based

Approccio

- Vantaggi:
  - Ricuce la quantità di informazioni da processare (le informazioni di flusso sono ridotto rispetto a quelle dei singoli pacchetti)
  - Più scalabile

- Problemi:
  - Non è possibile dialogare con alcuni aspetti relativi al livello pacchetto
- Tecnologie più importanti:
  - Cisco NetFlow
  - IETF IPFIX
  - sFlow

Cisco NetFlow

- standard aperto per la misurazione del traffico di rete definito da Cisco, tecnologia più usata
- poca interazione tra collector e exporter:
  - SNMP può essere utilizzato per sondare e occasionalmente per acquisire dati
  - I dati sono esportati su pacchetti UDP
- Campionatura dei pacchetti per diminuire il il costo del processamento
- I flussi sono esportati al collezionatore quando:
  - Il flusso termina
  - Il flusso è inattivo per un certo periodo
  - Il flusso è attivo ma ha raggiunto il time out
  - Vincoli interni della sonda, poca memoria, il flusso è interrotto prematuramente
- Problemi:
  - Metodi differenti per esportare il flusso: rende il processamento difficoltoso
  - Perdita di alcuni record in certe condizioni particolari
  - Utilizzabile solo per reti TCP/IP
  - Non è possibile aggiungere nuove informazioni nei record da esportare
  - Campionamento dei pacchetti: alcuni pacchetti sono persi!

IETF IPFIX

- IP Flow Information Export: prodotto praticamente identico a NetFlow
- Differenze limitate:
  - Protocollo di trasporto SCTP, opzionalmente TCP o UDP
  - Limitata personalizzazione dei campi da esportare

Realtime Traffic Flow Measurement

- Gruppo IETF
- La proposta è più avanzata di NetFlow
- Simple Ruleset Language:
  - Si può personalizzare
- I flussi sono bidirezionali: è facile verificare le due direzioni della connessione
- Interazione tra sonda e collezionatore è eseguita tramite query SNMP
- Non è supportato nei dispositivi commerciali

sFlow

Campionamento dei pacchetti come nel NetFlow
Si possono esportare:
Pacchetti campionati
Informazioni di flusso
Tecnologia eccellente ma non supportata da Cisco

VoIP Voice over IP

Processo di creazione di un flusso VoIP

1. campionamento
2. codifica
3. pacchettizzazione
4. accodamento
5. trasmissione
6. propagazione
7. de-jitter
8. riordinamento
9. decodifica

Pacchettizzazione

- prima operazione peculiare di una rete a pacchetto
- caratteristiche:
    - necessaria per abbassare gli overhead degli headers (non possono spedire un pacchetto per campione! Altrimenti uso una banda enorme! DEVO INSERIRE PIU' CAMPIONI NELLO STESSO PACCHETTO)
    - introduce molto ritardo
    - trade off tra ritardo ed efficienza (valori di ritardo di pacchettizzazione tra 20 e 40 ms)

Problematiche di accoramento

- presenti quando il traffico in ingresso supera la capacità del canale di uscita
    - il nodo deve memorizzare il traffico in eccesso (buffering)
    - AUMENTO DEL RITARDO
- Possibile soluzione: ACCODAMENTO A PRIORITA'

Problematiche di trasmissione

- Un pacchetto ha dimensioni finite:
    - È necessario aspettare la fine della trasmissione del pacchetto precedente prima di poter trasmettere quello successivo
- Tempo di trasmissione di un pacchetto nel caso di priorità queuing:
    - Si suppone che non ci siano altri pacchetti ad alta priorità in coda
    - Tempo di trasmissione del pacchetto in esame più quello del pacchetto attualmente in trasmissione

De-jitter

- Problema:
    - La rete inserisce dei ritardi variabili da pacchetto a pacchetto
    - I campioni vocali nei pacchetti devono essere riprodotti con lo stesso ritmo con cui sono stati generati
- Soluzione:
    - Blocco de-jitter
    - Polmone (buffer) che estrae i dati ad un ritmo costante
    - Dimensionamento: massimo jitter introdotto dalla rete, oppure massimo ritardo ammesso dal blocco: i pacchetti che arrivano troppo in ritardo, fuori da questa soglia sono considerati persi

Riordinamento dei pacchetti

- Serve per riordinare i pacchetti
- La soluzione è la stessa del jitter, spesso le due operazioni vengono fatte insieme

Tecniche di correzione dell'errore

- Sono basate sul concetto di ridondanza
  - L'informazione relativa ad N campioni viene messa:
    - Nel pacchetto corrente ad alto bit rate
    - Nel pacchetto successivo a basso bit rate
  - Codifiche gerarchiche
- Poco usata in pratica: si preferisce sfruttare la capacità di recupero dell'orecchio umano

Parametri di una sessione vocale

RITARDO: il più importante in assoluto
Banda
Perdite

Ritardo

- È il parametro fondamentale per una corretta interazione
- Ritardo end-to-end (l'ITU ha definito delle soglie):
  - 0-150ms: accettabile
  - 150-400ms: solo per collegamenti intercontinentali
  - >400ms: non accettabile in quanto il talking overlap diventa troppo fastidioso
- Ritardo effettivo round trip delay (ritardo di andata e ritorno)

Banda

- Traffico vocale è ANAELASTICO:
  - Il flusso di pacchetti non può essere ritardato neppure per brevi periodi
  - È inutile implementare meccanismi di bufferizzazione all'interno della rete: nei meccanismi priorità queiuing le code dei pacchetti vocali sono molto corte
- Traffico dati è ELASTICO

Perdite

- Massima percentuale tollerata: 5%:
  - L'orecchio umano è in grado di tollerare un certo numero di pacchetti mancanti
- Qualità della comunicazione:
  - Il round trip delay è più importante dell'integrità della comunicazione
  - I blocchi di riordinamento e de-jitter sono normalmente configurati con BUDGET DI RITARDO MOLTO RIDOTTI

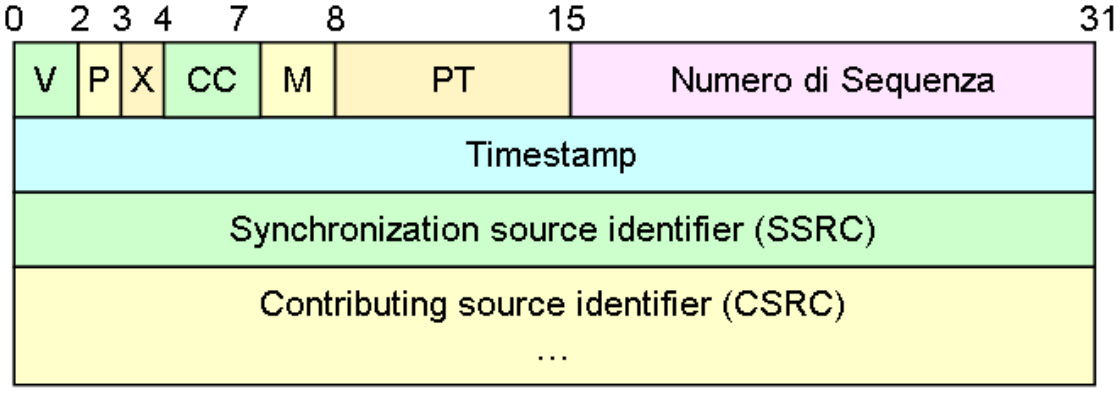
Protocollo RTP (Real-Time Protocol)

RTP è un protocollo di trasporto che garantisce il recapito dei pacchetti e la ricostruzione della corretta sequenza temporale, funzionalità richiesta da qualunque meccanismo di tipo real-time.

Caratteristiche generali:

- Gestione multicast nativo
- Non richiede un tipo di rete specifico (anche se attualmente è usato solo con IP e IPv6)
- Non gestisce frammentazione e riassemblaggio dei pacchetti: deve essere gestito dalla rete sottostante
- Non gestisce errori di trasmissione (checksum): se necessario devono essere definiti dalla rete sottostante
- RTP Mixer:
  - Presenza di client unicast / multicast nella stessa sessione: viene usato il campo CSRC
  - Elaborazione del segnale (per esempio soppressione dei canali dei soggetti non attualmente attivi)
- Non specifica il formato dei dati real-time:
  - Sono specificati in documenti appositi (Audio Video profiles)
  - Non è legato a codec
  - Gestisce il protocollo con il “payload type”
- Trasporto dai real-time:
  - Gestione della sequenza dei pacchetti
  - Gestione temporale (timestamp)
  - Gestione di un solo flusso per sessione
  - Nessuna gestione di sincronismo:
    - È possibile mediante una entità esterna ed il timestamp
    - Non è possibile collegare un flusso video ad un cambio di schermata nel flusso dati
- Real-time Control Protocol RTPC
  - Monitoraggio e controllo della connessione
  - Porta UDP successiva a quello di RTP
- Difficile da individuare
  - Non usa porte standard
  - Molte implementazioni richiedono l’utilizzo statico di certi range di porte

Formato del pacchetto RTP



Modello di una rete per VoIP

Gateway tra la rete telefonica e la rete IP:

- Media gateway
- Signaling gateway
- Gateway controller

Gateway in reti omogenee

Le architetture di rete:

Rete IP come backbone
Rete mista
Rete IP
Rete totalmente IP

Media gateway

- Traduzione della codifica audio: per es. tra rete IP e rete telefonica
- Nel caso di terminali intelligenti è incluso nel terminale

Signaling gateway

- Interfacciamento dal punto di vista della segnalazione:
  - Composizione del numero telefonico
  - Tono di libero o occupato
  - Gancio, sgancio della cornetta
  - Segnalazione interna alla rete: per l'instaurazione della chiamata al giusto endpoint
  - Segnalazione di rete intelligente: richiamata su occupato, identificativo chiamante, conversazione a tre
- Spesso non vi è una chiara separazione tra Media e Signaling gateway:
  - Generazione di tono libero e occupato: sono normali pacchetti audio inviati al telefono

Controller gateway

- Supervisione e monitoraggio dell'intero gateway:
  - Controllo della qualità del traffico: spesso si ammette una certa quantità di traffico telefonico, pena la degradazione della qualità
  - Controllare le autorizzazioni: utente autorizzato a fare o ricevere chiamate
  - Autenticazione: per esempio per fatturazione

Gateway in reti omogenee

- Alcune funzioni non possono essere integrate nel terminale utente:
  - Funzioni complicate come l'instradamento della chiamata
  - Funzioni riservate come l'autenticazione del chiamante
- Il gateway è ancora presente nelle reti omogenee:
  - Le funzionalità sono ridotte: per es. il media gateway è normalmente integrato nel terminale utente

Rete Telefonica, backbone IP

- La raccolta del traffico è in modalità tradizionale
- Il backbone è in tecnologia IP
- Utile nel processo di migrazione: economicità perché vi sono pochi punti da aggiornare
- La classica telefonata attraversa normalmente 2 gateway, nessuno se è locale

Rete mista

- I casi di impiego più frequenti sono:
  - Nuovo gestore telefonico che non dispone di una infrastruttura preesistente
  - Azienda con nuova sede: rete voce + dati. (al suo interno l'azienda comunica sulla rete IP, verso l'esterno avrà un gateway)
- Interfacciamento tra rete aziendale e rete esterna

- Caratteristiche:
  - Normalmente telefono VoIP distinto dal PC
  - Esempio di utilizzo del gateway all'interno della rete IP

Rete IP

- Vi sono due step:
  - Servizi di rete intelligente ancora con interfaccia di tipo telefonico (in particolare per la segnalazione)
  - Rete totalmente IP

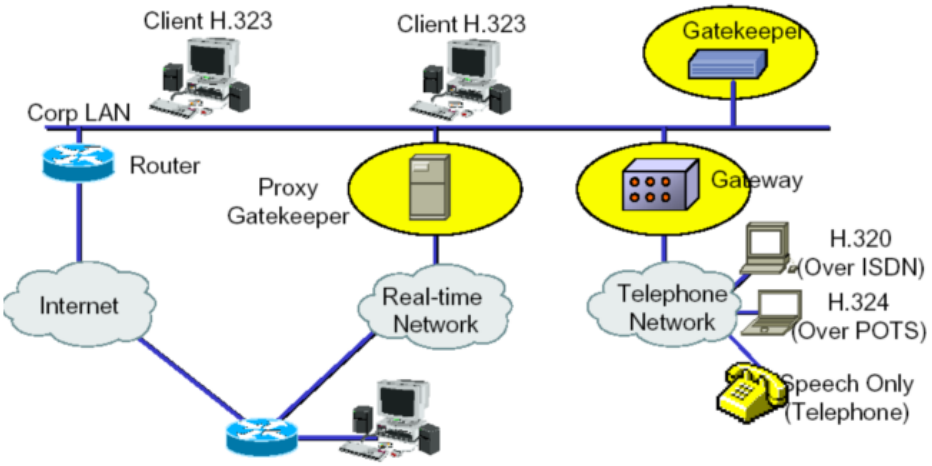
Protocolli di segnalazione

- Scopi:
  - Indirizzamento
  - Trasporto dei dati
  - Sicurezza della comunicazione
  - Supporto ai servizi di rete intelligente
  - Semplicità e trasparenza
- Standard principali:
  - H.323, ITU:
    - Soluzione di cui esistono più implementazioni
    - Molto complessa
  - SIP, IETF:
    - Soluzione a cui si stanno orientando tutti

H.323

- Caratteristiche fondamentali:
  - Standard per comunicazioni su LAN: reti a pacchetto senza garanzie di qualità del servizio
  - Esteso per operare su WAN
- Supporto di audio (obbligatorio), video, dati (lavagna condivisa)

Componenti della specifica H.323



Multipoint Control Unit MCU

Composta da 2 componenti:
- Multipoint Controller (obbligatorio): permette di negoziare le minime capabilities comuni
- Multipoint Processor (facoltativo): mixing / switching di flussi, adattamento di banda

Utilizzato in caso di:
- Conferenza tra tre o più terminali in modalità unicast
- Conferenza tra tre o più terminali in modalità mista unicast e multicast
- Non ha senso come entità distinta in multicast puro

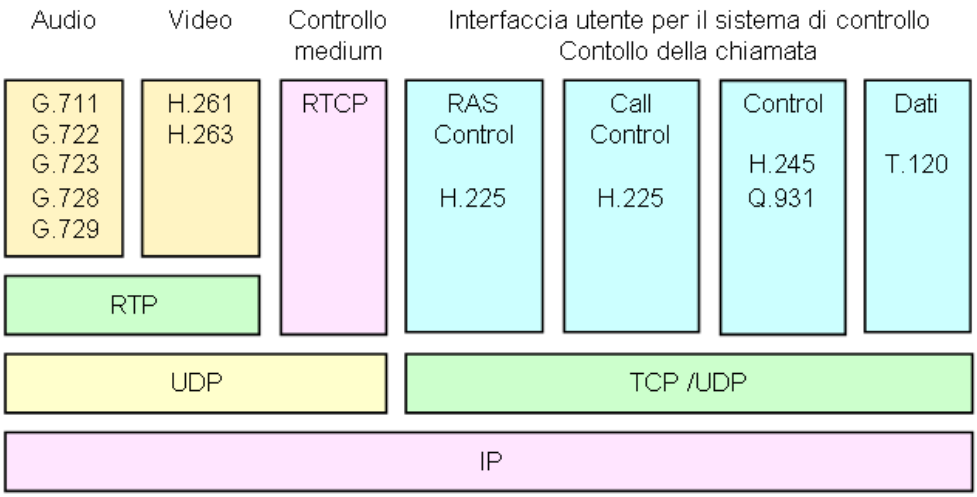
Zona

Insieme di elementi H.323 gestiti da un solo gatekeeper:
- Richiede almeno un terminale
- Non deve contenere più di un gatekeeper: nessun meccanismo di fault tolerance
- Non fa alcuna assunzione sulla tipologia di rete sottostante

Formato dei messaggi

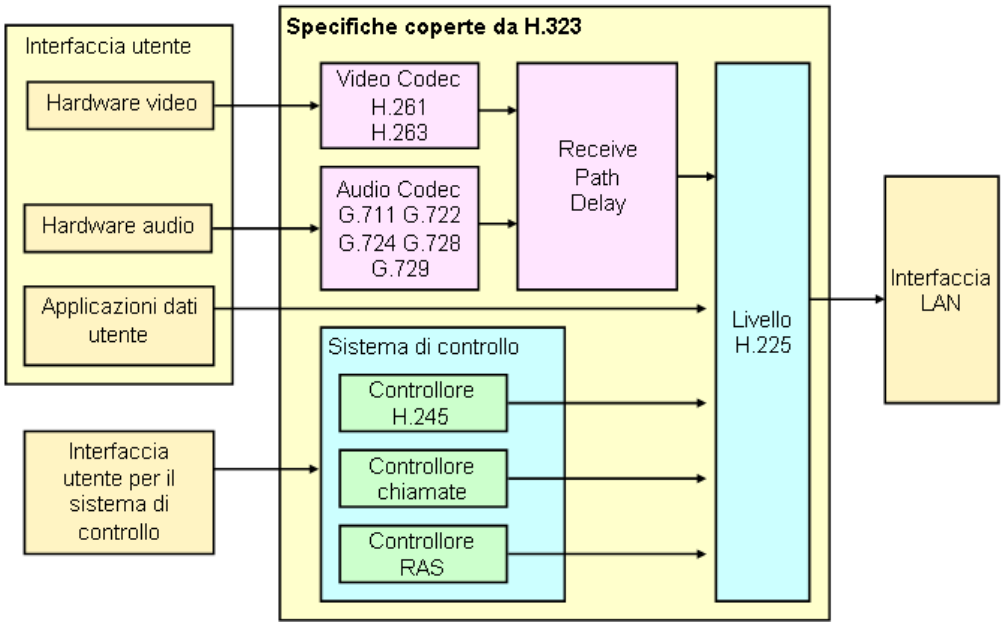
Messaggi codificati in ASN.1
- Include funzionalità avanzate come byte ordering
- Molto complesso
- Codifica difficoltosa e soprattutto il debugging
- Una delle critiche maggiori a H.323

Architettura protocollare



RAS: Registration, Admission and Status

Schema di un terminale H.323



H.225 compiti principali

Creazione e formattazione dei canali logici: trasmissione e ricezione dei pacchetti
Numerazione di sequenza
Assegnazione numero di canale logico (0-65525)
Rilevazione e correzione errori

Controllore RAS

- Utilizza messaggi H.225
  - Registrazione del terminale
  - Ammissione del terminale
  - Cambiamenti della larghezza di banda (anche durante una chiamata)
  - Controlli di status
  - Procedure di sgancio tra endpoint e gatekeeper
- Canali RAS
  - Aperto all'interno di H.225
  - Indipendenti dai canali di segnalazione chiamate e controlli H.245
  - Aperto prima di ogni altro canale
- Attivo solo se presente un gatekeeper

Controllore chiamate

Utilizza la segnalazione H.225
Stabilisce una connessione tra 2 endpoint
Attivato dopo il canale RAS

Controllore H.245

- Canale logico di controllo end-to-end
- Scopi:
  - Capacità dei terminali
  - Richiesta di modi operativi
  - Comandi ed indicazioni generali
- Stabilito normalmente tra endpoint e gatekeeper (che agisce come proxy)
- Un canale per ogni chiamata: un gatekeeper può avere molti canali aperti
- Realizzazione fisica:

  - Canale distinto
  - Canale 0 all'interno di H.225

Gateway

- Appare come terminale H.323 sulla rete IP e come terminale telefonico sulla rete PSTN
- Traduce:
  - Canali dati (es. G.729 / RTP in campionamento telefonico)
  - Canale di controllo (es. H.225 in H.221)
  - Procedure di segnalazione (es. H.245 a H.242)
- Impiego:
  - Interfaccia tra tecnologie differenti
  - Dispositivo di "adattamento" su reti omogenee (es. compressione)
  - Backup della rete IP sulla rete telefonica

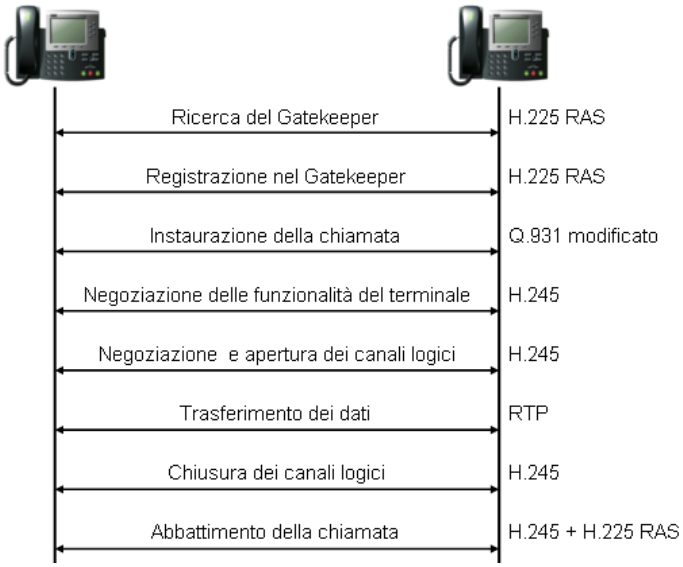
Gatekeeper

- Responsabile di una zona:
  - Traduzione degli indirizzi da indirizzo alias H.323 a indirizzo a livello trasporto
  - Controllo d'ammissione alla rete, attraverso l'uso di messaggi RAS
  - Gestione delle zone H.323
- Funzioni opzionali:
  - Autorizzazione delle chiamate
  - Gestione della banda:
    - Per esempio limitando in numero di terminali sulla rete
  - Gestione chiamate
    - Tenendo traccia dei terminali attualmente occupati in una comunicazione

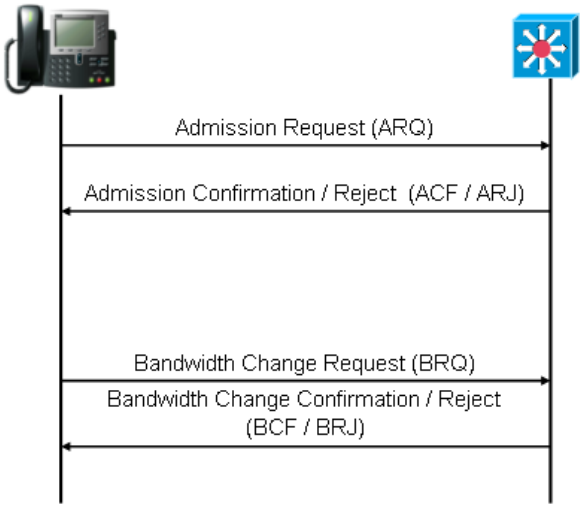
Indirizzamento

- Indirizzo di rete: IP
- Identificatore TSAP: Transport Layer Access Point
  - Corrisponde alla porta TCP/UDP
  - Well known: canale di segnalazione della chiamata, canale RAS
  - Decisi a runtime: canali dati
- Indirizzi alias:
  - nome@dominio.com, numero telefonico, ecc.
  - disponibili SOLO SE ESISTE UN gatekeeper

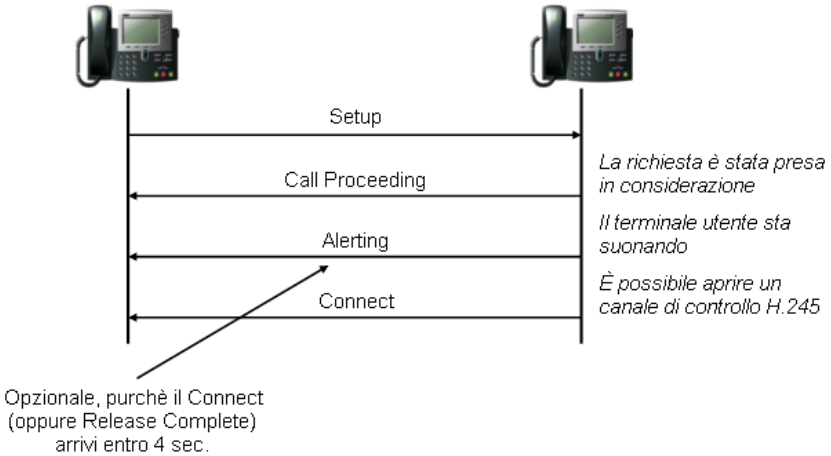
Le principali fasi di H.323

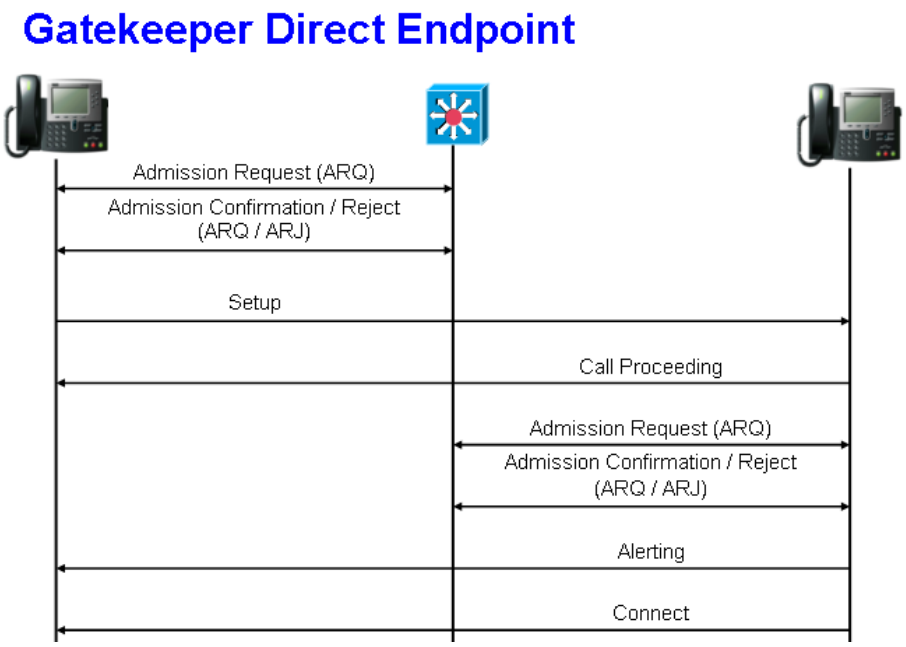


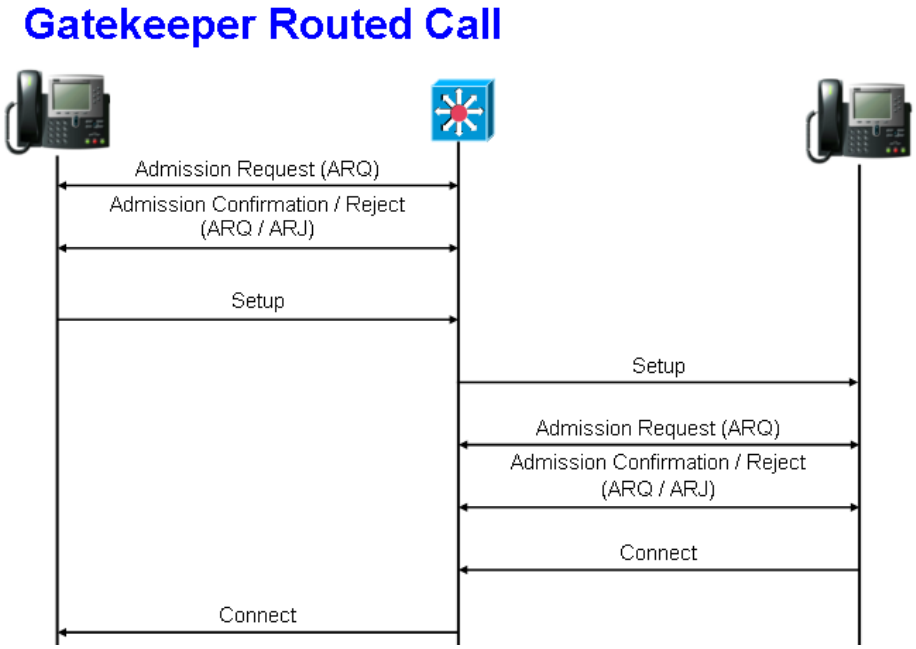
Ammissione e cambiamento di banda



Chiamata diretta senza Gatekeeper

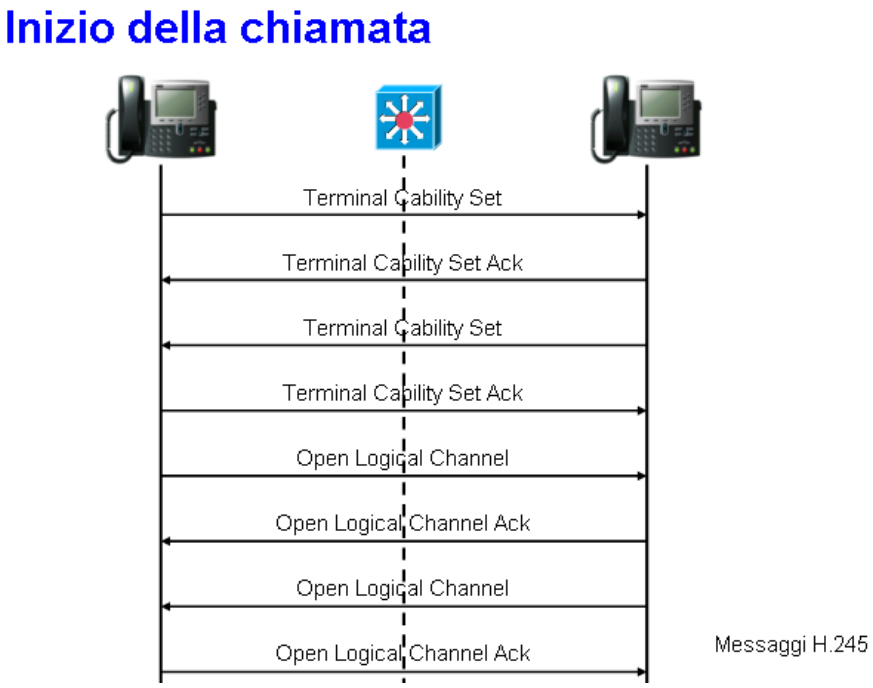






Instradamento messaggi di controllo

- Due possibilità:
  - Canale diretto tra endpoint
    - Usato nel caso della chiamata diretta
    - Sperimentale nel caso di chiamata tramite gatekeeper
  - Canale verso gatekeeper



SIP Session Initiation Protocol

- Protocollo ex-novo, non vi è un adattamento agli standard precedenti: sfrutta meglio le caratteristiche della rete IP
- Scopi limitati:
  - Protocollo di controllo: non specifica la trasmissione audio e dati
  - Maggiore semplicità e leggerezza
  - Non riserva risorse sulla rete:
    - Invia all'utente informazioni che permettono di farlo
    - SDP, RSVP
- Supporto:
  - Name mapping (indirizzo mail …)
  - Personal mobility: chiamata ad un terminale telefonico, voice mail, email

Caratteristiche del protocollo

- Interazione di tipo client-server
- Formato messaggi http-like (messaggi testuali)
- TCP e UDP a seconda degli scopi:
  - TCP è utile nei firewall
  - Definisce meccanismi per garantire l'affidabilità su UDP, three way handshake
  - TCP: una connessione può essere utilizzata per più request/response
- No frammentazione:
  - Tutto il messaggio deve essere contenuto in un pacchetto
  - MTU della rete, oppure 1500 bytes

SIP e sicurezza

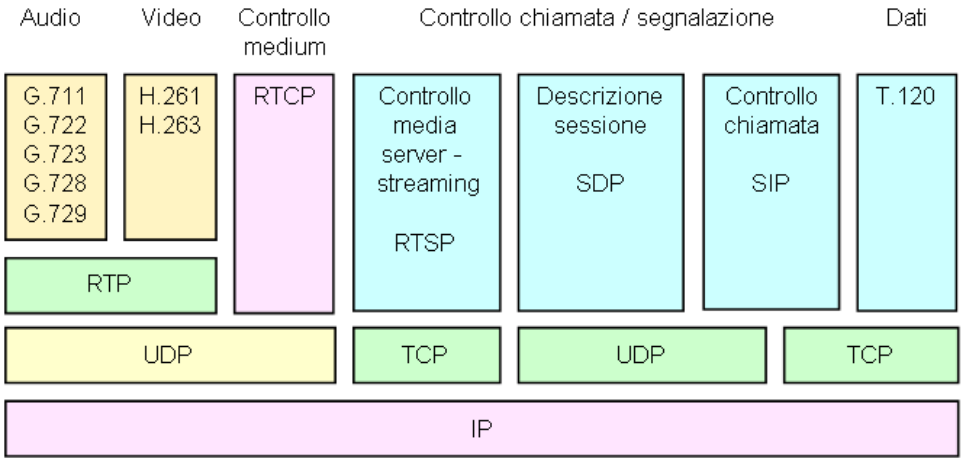
- Autenticazione dell'utente
- Meccanismi contro Denial of Service
- Meccanismi contro lo spam

- Criptatura opzionale di:
  - Corpo del messaggio
  - Indicazione dei nodi intermedi in cui è transitato il messaggio:
    - Potenzialmente può portare al loop del messaggio anche se esistono strategie per impedirlo

Servizi principali

- Localizzazione dell'utente: determina quale sia il terminale da usare per la comunicazione
- Capacità dell'utente: determina i mezzi ed i parametri da usare
- Disponibilità dell'utente: determina la volontà del chiamato di comunicare
- Setup della chiamata: stabilisce i parametri della chiamata
- Gestione della chiamata: servizi supplementari, trasferimento e gestione delle chiamate

La pila protocollare SIP



SDP Session Description Protocol

- Utilizzato per descrivere le sessioni multimediali:
  - Numero dei flussi media e tipo di codificatore
  - Banda
  - Indirizzi e porte
  - Tempo di inizio e fine del flusso
  - Sorgente
- Formato testuale
- Incluso nel corpo del messaggio SIP

RTSP Real-Time Streaming Protocol

- Controllo dei flussi in un media server:
  - Video on demand
  - Segreteria telefonica
- Comandi per gestire una registrazione:
  - DESCRIBE Request
  - SETUP Request

  - ISSUE Media Request: play, stop, record
  - TEARDOWN Request

Componenti principali

- User agent: include obbligatoriamente
  - User Agent Client
  - User Agent Server
- Proxy server:
  - Utilizzato per avere terminali più semplici (leggeri)
  - Agisce da server verso il chiamante e da client verso il chiamato
- Redirect server:
  - Ha un solo componente di tipi UAS User Agent Server
  - È un redirezionatore di chiamate
  - Utile per implementare politiche intelligenti: telefono ufficio in orario di lavoro, email altrimenti ecc..
- Media server: servizi a valore aggiunto
  - Segreteria telefonica
  - Musica intrattenimento nel caso il chiamato sia impegnato
- Location server: DNS, LDAP, risoluzione degli indirizzi
- Server AAA (Authentication, Autorization and Accounting): solitamente è un server RADIUS
- MCU: analoga a quella di H.323

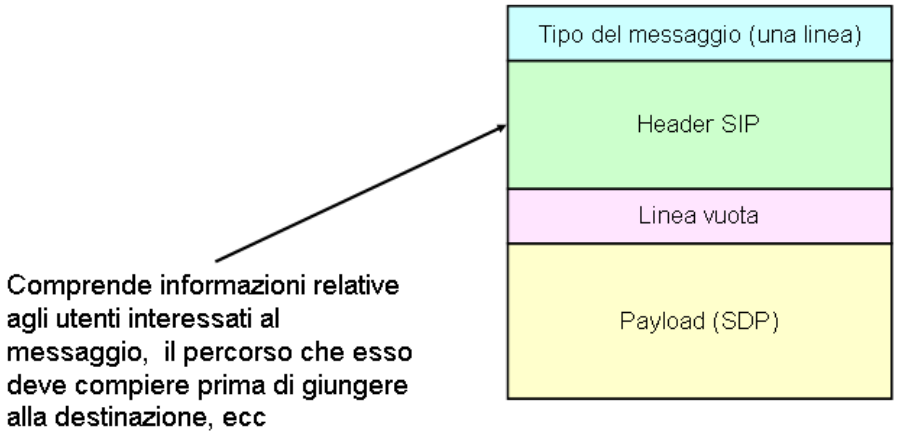
Indirizzamento

- Indirizza un utente e non un terminale
- Segue la filosofia degli standard Internet:
  - nomeutente@dominio.com: spesso coincide con l'email, il dominio può essere un qualunque terminatore di chiamata, server di dominio, nome macchina, indirizzo IP
  - num_telefono@gateway: in questo caso deve essere presente il campo user=phone per indicare che è una chiamata telefonica
- Privacy:
  - Realizzata inserendo alcuni filtri sui terminali utente o sui server
  - L'uso delle password è sconsigliato in quanto viaggiano in chiaro

Parametri di indirizzamento

- Permettono di personalizzare la chiamata:
  - Protocollo di trasporto
  - Indirizzo di multicast
  - Time to Live

Struttura dei messaggi SIP



Tipologie di messaggi

- INVITE:
  - Richiesta per iniziare una comunicazione: messaggio verso un server (proxy, redirect, terminale)
  - Include una descrizione SDP nel messaggio
  - Può essere inviato anche durante una comunicazione
- ACK:
  - Indica una conclusione positiva alla chiamata
  - Non è un messaggio di risposta
  - Può contenere una descrizione SDP dei parametri richiesti
- BYE:
  - Indica che la chiamata deve avere termine
  - Può essere inviata sia durante la fase di connessione che a sessione attivata
  - Il ricevente deve cessare immediatamente il flusso dati
- CANCEL:
  - Cancella una richiesta di connessione ancora pendente
  - Utilizzato dai server che hanno duplicato la chiamata per comunicare che è già stato ricevuto un ACK
- OPTIONS:
  - Utilizzato per scoprire le capacità del server
  - Utile per conoscere la capacità di un terminale attualmente impegnato in una comunicazione
- REGISTER:
  - Utilizzato per registrare un indirizzo SIP all'interno di un server
  - Può essere fatto in multicast (all SIP servers, 224.0.1.75)

Principali campi dell'header

- FROM:
  - Indica l'iniziatore della chiamata SIP
  - Viene mantenuto anche nel messaggio di ritorno: from e to non vengono cambiati nei messaggi
- TO:
  - Indica il terminatore della richiesta SIP
- VIA:

  - Permette di tenere traccia del percorso del messaggio
  - È necessario quando la richiesta SIP è gestita da più server proxy in cascata
  - Informazione aggiunta man mano che si va verso la destinazione e quando il messaggio torna indietro
- Call-ID: identifica univocamente
  - Un invito (se la procedura è un invite)
  - Tutte le registrazioni di un utente (se la procedura è register)
- Cseq:
  - Command sequenze
  - Indica il metodo richiesto, per es. invite
  - Non cambia tra richiesta e risposta
- Subject: oggetto della chiamata
- Content-Type: tipologia del payload contenuto nel pacchetto SIP
- Content-Length: lunghezza del payload
- Content-Encoding: indica eventuali altre elaborazioni fatte al payload, per es. codifica del messaggio

Codici di errore

Codice	Messaggio	Significato
1xx	Informational	Richiesta ricevuta, continua l'iter
2xx	Success	Richiesta ricevuta, capita, accettata
3xx	Redirection	Bisogna fare altro per completare la richiesta
4xx	Client Error	Errore sintassi o richiesta non eseguibile
5xx	Server Error	Server non può soddisfare richiesta corretta
6xx	Global Failure	Nessun server può soddisfare richiesta

Principali operazioni di SIP

- Transazione SIP: mantiene invariati i seguenti campi
  - From, To, Call-ID, CSeq
- Risoluzione dei nomi:
  - Attraverso DNS o LDAP, nel caso di DNS vengono tentate nell'ordine
    - Risoluzione DNS tramite SRV: si cerca l'esistenza del record SRV per quel dominio per il dominio di posta elettronica
    - Risoluzione DNS tramite CNAME: alias
    - Risoluzione DNS tramite record A: prende l'indirizzo IP

Chiamata con Proxy Server

1. il server proxy accetta l'INVITE request
2. contatta il server delle locazioni e ottiene l'indirizzo preciso della posizione attuale

del chiamato
3. invia un SIP INVITE request all'indirizzo ritornato dal loc. server
4. lo user agent server allerta l'utente
5. ritorna il success indicator al proxy server che avvisa il chiamante
6. la ricezione del messaggio è confermata dal chiamante attraverso un ACK che viene inoltrata al chiamato attraverso un proxy server o direttamente

Chiamata con Redirect Server

E' utilizzato per informare il chiamante dell'effettiva localizzazione del chiamato, in questo modo la chiamata potrà essere diretta tra le due controparti senza necessità di un proxy server. L'aspetto importante è che quanto il chiamante riceve dal server redirect l'indirizzo della locazione da chiamare, deve rispondere con un ACK. A questo punto il chiamante può procedere a chiamare direttamente il chiamato.

Interlavoro con la rete telefonica MeGaCo

Il Media Gateway Control Protocol, è attività di ricerca all'interno del Megaco Working Group dell'IETF.

Componenti

- Media gateway control protocol racchiude in se le funzionalità del gateway H.323:
  - Segnalazione H.323 RAS
  - Segnalazione H.323 (H.225 e H.242 opzionale)
  - Segnalazione SS7 opzionale
- Inoltre il Media gateway control protocol termina connessioni di tipo RTP e circuiti SCN:
  - Termina l'interfaccia IP e il trunk SCN

Modelli di connessioni

- Terminazioni: sono entità logiche che possono rappresentare link analogici, timeslots di canali TDM, stream RTP ed altri
- Contesti: rappresentano un numero variabile di terminazioni associate allo stesso media stream. La configurazione del contesto rappresenta l'associazione logica tra le terminazioni che appartengono al contesto

Comandi

H.GCP fornisce dei comandi per manipolare terminazioni e contesti, ad esempio è possibile: aggiungere o modificare una terminazione ad un contesto, eliminare una concessione da un contesto, modificare le proprietà associate ad una terminazione o ad un contesto.

Transazioni

Comandi dal Media Gateway Control verso il Media Gateway sono raggruppate un transazioni identificate da un Transaction ID. Tale Transaction ID è composto da Azioni, cioè da insiemi di comandi che possono operare all'interno di un unico contesto