

Instradamento

- All'accensione una macchina sa:
 - il suo indirizzo MAC
 - il suo indirizzo IP (e la rete locale a cui appartiene)
 - il suo indirizzo alfanumerico
- NON sa:
 - chi ha attorno (macchine "visibili" direttamente)
 - qual'è il modo per raggiungere l'esterno (indirizzo dei gateways)

Instradamento

- Un cammino attraversato da un *datagramma* IP è composto da sotto-reti interconnesse da router
- Un datagramma è interpretato da una sotto-rete come un'unità di dati di servizio (SDU)
- Una sotto-rete consegna la SDU al router successivo o alla destinazione (se la destinazione è all'interno della sottorete) utilizzando i propri meccanismi protocollari
- Due tipi di instradamento
 - diretto
 - indiretto

Instradamento diretto

- si applica quando il pacchetto deve essere rilanciato nella sotto-rete di destinazione
- l'host di destinazione è connesso alla stessa sotto-rete dell'host sorgente o del router che emette il *datagramma*
- Il trasferimento dei *datagrammi* IP non coinvolge router intermedi
- E' necessaria la traduzione dell'indirizzo IP dell'host di destinazione nel suo indirizzo fisico (es. indirizzo MAC)
- Il *datagramma* IP viene incapsulato nell'unità dati della sotto-rete che viene inviata direttamente all'host di destinazione
- L'instradamento all'interno della sotto-rete utilizza i meccanismi specifici della sotto-rete

Instradamento indiretto

- si applica quando il pacchetto deve essere instradato in sotto-reti diverse da quella di destinazione
- quando l'host di destinazione è connesso ad una sotto-rete diversa da quella dell'host sorgente o del router che emette il datagramma
- L'host mittente identifica il router a cui inviare il datagramma IP ed individua il suo indirizzo fisico
- Il router esamina il datagramma IP ricevuto e decide il router successivo verso cui instradarlo
 - l'instradamento attraverso la sotto-rete che connette i due router avviene secondo i meccanismi della sottorete
- Il processo si ripete di router in router sino alla sotto-rete di destinazione
 - nella sotto-rete di destinazione è utilizzato l'instradamento diretto

Routing Table

- La scelta del router verso cui inviare il datagramma avviene utilizzando la Tabella di Instradamento (Routing Table - RT) contenuta in ogni host e router
- Ogni elemento di una RT contiene
 - Indirizzo IP di destinazione (host address o network address)
 - Indirizzo del router successivo (next hop router) sul cammino verso la rete di destinazione
 - Indicazione dell'interfaccia fisica di uscita
- Un router non conosce il cammino completo verso la destinazione

Routing Table

- Un router esegue i seguenti passi:
 - ricerca nella RT un elemento che corrisponda completamente all'indirizzo di destinazione contenuto nel datagramma
 - ricerca di un elemento che corrisponda all'indirizzo di rete
 - ricerca di un elemento secondo la tecnica "longest prefix matching"
 - ricerca l'indirizzo del "router di default"
- Se nessuno dei passi precedenti ha esito positivo, il *datagramma* è classificato come "undeliverable" ed è scartato

Routing Table

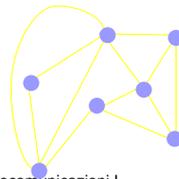
- La tabella di instradamento di un router è riempita mediante le informazioni ricevute dal Router stesso mediante i Protocolli di Instradamento (Routing Protocol)
- La scelta del percorso e quindi del router successivo dipende da un fissato criterio di ottimalità (es. costo minimo)
- E' necessario che un Router conosca lo stato della rete:
 - la topologia
 - il costo di attraversamento dei singoli rami
- Ad ogni ramo della rete è associato un costo che può essere
 - inversamente proporzionale alla banda del ramo
 - proporzionale al carico istantaneo sul ramo
 - proporzionale al costo d'uso del ramo
 - qualsiasi combinazione tra i precedenti criteri

Routing Table

- Le Routing Table sono dinamiche
 - ogni router ed ogni host aggiornano nel tempo le informazioni di instradamento in loro possesso
- L'aggiornamento dinamico è necessario perché:
 - Internet non può essere considerata stabile
 - in caso di guasti alcuni cammini non sono utilizzabili
 - È consigliabile scegliere il cammino in base allo stato di occupazione delle risorse di rete
- Le RT devono essere aggiornate continuamente (anche ad intervalli di pochi secondi)
- L'aggiornamento delle RT è attuato mediante protocolli di colloquio tra i router (Routing Protocol)

Grafi

- Una qualsiasi rete a pacchetto può essere modellata come un grafo orientato pesato
 - i nodi sono i router
 - i rami sono le linee trasmissive o le sotto-reti
- L'instradamento (routing) di un pacchetto equivale alla ricerca di un cammino nel grafo associato della rete
- Ricerca del cammino a minima distanza (numero minimo di hop)
 - grafo non pesato
- Ricerca del cammino a minima lunghezza (costo minimo)
 - grafo pesato (pesi corrispondenti a costo, congestione, capacità, ecc.)



6 novembre 2004

Corso di Reti di Telecomunicazioni I

36

I protocolli di instradamento

- Routing Information Protocol (RIP) appartiene alla categoria degli Distance Vector Routing Protocols
 - E' richiesto che ogni nodo scambi informazioni (costi dei rami e le minime distanze verso le altre reti) con i nodi adiacenti, ad intervalli regolari o quando la routing table cambia.
 - due nodi sono adiacenti se sono direttamente connessi mediante la stessa rete
 - RIP è utilizzato in reti di piccole dimensioni
 - E' molto semplice, tuttavia
 - la convergenza è lenta
 - lo stato di equilibrio può essere un sub-ottimo

6 novembre 2004

Corso di Reti di Telecomunicazioni I

37

I protocolli di instradamento

- Open Shortest Path First (OSPF)
 - L'OSPF è un protocollo "Link State" che sostituisce il protocollo RIP in reti di grandi dimensioni
 - Principi base:
 - i router hanno la responsabilità di contattare i router adiacenti e di acquisire la loro identità (pacchetti Hello)
 - i router
 - formano i Link State Advertisement (LSA) che contengono una lista delle reti adiacenti con i relativi costi di raggiungimento
 - gli LSA sono trasmessi a tutti gli altri router
 - tutti i router della rete hanno lo stesso insieme di dati e quindi possono costruire lo stesso grafo pesato della rete
 - il grafo di rete è utilizzato per determinare i cammini ottimi e quindi l'instradamento

I protocolli di instradamento

- Open Shortest Path First (OSPF)
 - Gli LSA sono emessi
 - quando un router contatta un nuovo router vicino
 - quando un ramo si guasta
 - quando il costo di un ramo varia
 - periodicamente ogni fissato intervallo di tempo
 - La rete trasporta gli LSA mediante la tecnica di flooding
 - un LSA è rilanciato da un router su tutte le sue interfacce tranne quella da cui è stato ricevuto
 - gli LSA trasportano dei riferimenti temporali (time stamp) o numeri di sequenza per
 - evitare il rilancio di pacchetti già rilanciati
 - consentire un corretto riscontro dal ricevente

I protocolli di instradamento

■ Open Shortest Path First (OSPF)

- La tecnica flooding ha i seguenti vantaggi
 - esplora tutti i possibili cammini tra origine e destinazione
 - è estremamente affidabile e robusta
- Il traffico generato dipende dalle dimensioni della rete e può essere molto
- I pacchetti OSPF sono incapsulati in datagrammi IP

Livello Trasporto

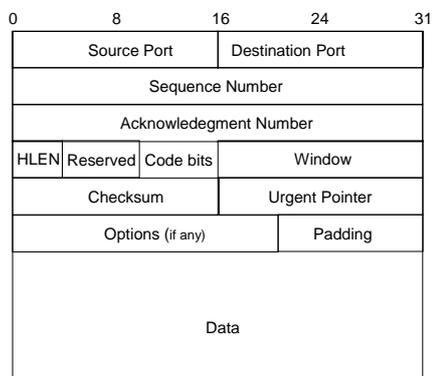
- Lo strato di trasporto fornisce un servizio di trasferimento allo strato applicativo conforme ai requisiti di qualità richiesti dall'applicazione
- Il protocollo TCP
 - offre un servizio di trasferimento orientato alla connessione
 - trasferisce un flusso informativo continuo e bidirezionale
 - ha i mezzi per recuperare eventi di perdita, duplicazione e consegna fuori sequenza dei dati
 - esegue le funzioni di controllo di flusso per adeguare il volume dei dati trasferito alle capacità di ricezione e di emissione
 - è utilizzato per applicazioni che generano flussi informativi di una certa complessità che richiedono funzioni di controllo d'errore e di flusso
- Il protocollo UDP
 - offre un servizio solo poco più raffinato dell'IP. In pratica offre in più solo il multiplexing di porta
 - è utilizzato quando l'applicazione non richiede funzioni di controllo di flusso e controllo d'errore

Transmission Control Protocol (TCP)

- Gestisce un flusso informativo bi-direzionale tra due host
- E' un protocollo con connessione
- Funzioni eseguite
 - indirizzamento di una specifica applicazione all'interno di un host
 - ri-ordinamento delle unità informative
 - controllo e recupero di errore
 - controllo di flusso
 - controllo di congestione

Unità dati TCP

- Source Port (16 bit) e Destination Port (16 bit)
 - identificano i processi sorgente e destinazione
- Sequence Number (32 bit)
 - numero di sequenza in trasmissione
 - contiene il numero di sequenza del primo byte di dati contenuti nel segmento a partire dall'inizio della sessione TCP
- Acknowledgement Number (32 bit)
 - numero di sequenza in ricezione
 - se ACK=1, contiene il numero di sequenza del prossimo byte che il trasmettitore del segmento si aspetta di ricevere
 - è possibile la modalità piggybacking di riscontro (ovvero il riscontro attraverso un segmento dati nell'altro verso di trasmissione)



Unità dati TCP

- HLEN (4 bit)
 - contiene il numero di parole di 32 bit contenute nell'intestazione TCP
 - l'intestazione TCP non supera i 60 byte ed è sempre un multiplo di 32
- Reserved (6 bit)
 - riservato per usi futuri, per ora contiene degli zeri
- Window (16 bit)
 - larghezza della finestra in byte (controllo di flusso è orientato al byte)
 - è il numero di byte che, ad iniziare dal valore del campo Ack
 - Number, l'host che trasmette il segmento è in grado di ricevere
- Checksum (16 bit)
 - protegge l'intero segmento più alcuni campi dell'header IP (es. indirizzi)

Unità dati TCP

- Urgent Pointer (16 bit)
 - contiene il numero di sequenza dell'ultimo byte dei dati che devono essere consegnati urgentemente al processo ricevente
 - tipicamente sono messaggi di controllo (out-of-band traffic)
- Options (di lunghezza variabile)
 - sono presenti solo raramente
 - Esempio: Maximum Segment Size (MSS)
- Padding (di lunghezza variabile)
 - impone che l'intestazione abbia una lunghezza multipla di 32 bit

User Datagram Protocol (UDP)

- E' un protocollo senza connessione
- Non supporta meccanismi di riscontro e di controllo d'errore
- E' utilizzato per il supporto di transazioni semplici tra applicativi
 - interrogazioni di database
 - risoluzione di indirizzi
 - messaggi di management

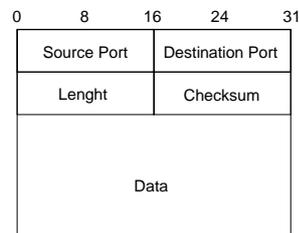
6 novembre 2004

Corso di Reti di Telecomunicazioni I

46

User Datagram Protocol (UDP)

- Source Port (16 bit) e Destination Port (16 bit)
 - identificano i processi sorgente e destinazione dei dati
- Datagram Length (16 bit)
 - è la lunghezza totale (espressa in byte) del datagramma, compreso l'header UDP
- Checksum (16 bit)
 - protegge il datagramma UDP e i campi indirizzo, protocol e datagram length dell'header IP



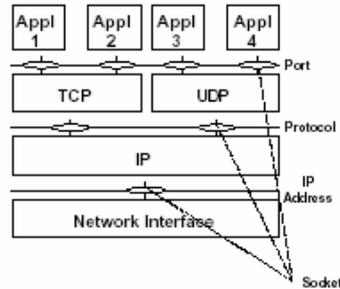
6 novembre 2004

Corso di Reti di Telecomunicazioni I

47

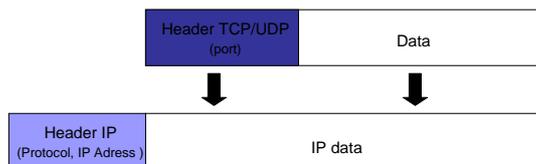
Indirizzamento

- Distingue tra i programmi applicativi (processi) che sono utenti dello stesso servizio di trasporto
- Port
 - identifica un utente dello strato di trasporto
 - è rappresentato da un intero (16 bit)
- Socket
 - identifica l'interfaccia tra l'applicazione ed i protocolli di comunicazione
 - è rappresentata dalla tripletta (port; protocol; IP_Address)



Indirizzamento

- La componente "Port" è contenuta nell'intestazione dell'unità dati di TCP/UDP
- Le componenti "Protocol" e "IP_Address" sono contenute nell'intestazione dell'unità dati di IP
- Lo strato Ip esegue la moltiplicazione di una molteplicità di flussi di trasporto



Indirizzamento

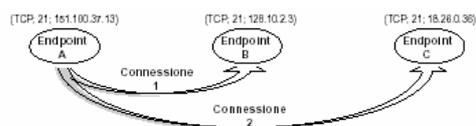
- Il numero di porta può essere
 - statico
 - sono identificativi staticamente associati ad applicazioni largamente utilizzate
 - sono utilizzati identificativi inferiori a 256

Numero	Applicazione
21	FTP (File Transfer Protocol)
23	Telnet
25	SMTP (Simple Mail Transport Protocol)

- dinamico
 - sono identificativi assegnati direttamente dal sistema operativo al momento dell'apertura della connessione
 - si utilizzano valori maggiori di 1023

La connessione TCP

- Il protocollo TCP è un protocollo orientato alla connessione
- Nella fase di instaurazione della connessione, le due entità TCP remote si sincronizzano scambiandosi i propri numeri di sequenza iniziale
- Il numero di sequenza iniziale rappresenta il numero a partire dal quale tutti i byte trasmessi saranno numerati in sequenza
- Una connessione TCP è identificata dalla coppia di socket associati agli endpoint tra cui vengono scambiate informazioni
- Un endpoint può essere impegnato allo stesso tempo in più connessioni TCP



Controllo d'errore in TCP

- Il TCP prevede esclusivamente riscontri positivi (ACK)
- La ritrasmissione dei segmenti è innescata dalla mancata ricezione degli ACK entro un fissato tempo limite (Retransmission Timeout - RTO)
- Il dimensionamento dell'RTO è critico
 - se il suo valore è troppo piccolo, alcuni segmenti in ritardo a causa di congestione, potrebbero essere considerati persi e quindi ri-trasmessi inutilmente
 - se il suo valore è troppo grande, la risposta ad un evento di perdita sarebbe troppo lenta

Controllo d'errore in TCP

- Il Retransmission TimeOut (RTO) è determinato con uno schema adattativo
- Il TCP misura dinamicamente il Round Trip Time (RTT)
 - RTT = ritardo tra l'invio di un segmento e la ricezione del relativo ACK
- Il valore di RTO è scelto maggiore del valore medio di RTT
- La misura del RTT è affetta da errori
 - l'emissione degli ACK del ricevente può essere non immediata
 - in caso di ritrasmissioni è impossibile distinguere se l'ACK si riferisce al segmento iniziale o al segmento ritrasmesso
 - lo stato di congestione della rete può cambiare rapidamente

Controllo di flusso in TCP

- Il controllo di flusso ha lo scopo di limitare il tasso di generazione dei dati da parte di un host
- Il controllo di flusso è indispensabile in Internet dove sono presenti host di potenzialità molto diverse
- TCP utilizza un controllo di flusso a finestra basato su
 - una finestra scorrevole di ampiezza variabile
 - uno schema di allocazione di crediti
- Il controllo di flusso opera a livello di ottetti (byte) numerati in sequenza a partire dal numero scelto durante il 3-way handshaking
- Un riscontro (ACK Number= X e Window= W) significa che
 - sono riscontrati tutti gli ottetti ricevuti fino a quello numerato con $X-1$
 - il trasmittente è autorizzato a trasmettere fino a ulteriori w ottetti, ovvero
 - fino all'ottetto numerato con $X+W-1$

Controllo di congestione in TCP

- Ha lo scopo di recuperare situazioni di sovraccarico nella rete limitando il traffico offerto alla rete
- Difficoltà:
 - il protocollo IP (protocollo di rete) non possiede alcun meccanismo per rivelare e controllare la congestione
 - il TCP è un protocollo end-to-end e può rivelare e controllare la congestione solo in modo indiretto
 - la rete non coopera con gli host per il controllo della congestione
 - la conoscenza dello stato della rete da parte delle entità TCP è imperfetta a causa dei ritardi di rete
 - le entità TCP che usano la rete non cooperano tra loro, anzi competono per l'uso delle risorse distribuite

Controllo di Congestione a Finestra

- In caso di congestione, il controllo di flusso a finestra protegge implicitamente, oltre al destinatario, anche la rete
 - se la rete è congestionata arriveranno meno riscontri e quindi saranno emessi un numero minore di segmenti
 - il meccanismo adattativo di timeout evita ritrasmissioni che porterebbero ad un aumento della congestione invece che ad una sua diminuzione
- Il controllo di flusso end-to-end riesce ad adattare il rate di emissione della sorgente a quello corrispondente al bottleneck della rete (proprietà di self-clocking)

QOS in internet

- La Internet attuale è di tipo “Best Effort”
- Non esistono modi per garantire la Qualità del Servizio ricevuto su Internet
- Tutti i flussi sono trattati allo stesso modo
- La pila protocollare TCP/IP è stata sviluppata con l’idea di far accedere tutti allo stesso modo e con le stesse priorità
- La maggior parte dei nodi di rete (Router) ha delle code interne di tipo FIFO; se arrivano più pacchetti di quelli gestibili, vengono scartati

Politiche di QoS

- QoS nei nodi di rete (sostanzialmente a livello IP)
 - shaping del traffico,
 - schedulazione dei pacchetti
- QoS end-to-end (può coinvolgere anche livelli protocollari superiori)
 - meccanismi di segnalazione end-to-end
 - architetture di rete per la QoS

Politiche di QoS nei nodi di rete

- Edge
 - Classifier, osserva i pacchetti IP entranti nel nodo e li classifica in base al loro ind IP, Port Number e al tipo di protocollo superiore
 - Marker, provvede a "marchiare" i pacchetti a seconda di come sono stati classificati
 - Traffic Policer, fa condizionamento del traffico, osserva il rate possibile e agisce di conseguenza
 - Traffic Shaper, modella il flusso sulla porta di uscita in modo da ottimizzare il throughput
- Core
 - Scheduler, genera più code all'interno del nodo di rete, e usa algoritmi di schedulazione delle code, evitando o gestendo le congestioni di rete.

QoS e2e

■ Proposte IETF:

- Modello Servizi Integrati, RFC 1633, Giugno 1994;
- Modello Servizi Differenziati, RFC 2475, Dicembre 1998;
- Modello IntServ-DiffServ integra i precedenti (in via di definizione)

IntServ: Modello

- Flusso: sequenza di pacchetti con stesso indirizzo IP sorgente e destinazione, e stesso Port number
- Per avere QoS end-to-end ogni router della rete deve allocare banda a sufficienza per i diversi flussi
- Ciascun router della rete deve avere un per-flow state
- Poiché la memoria su ogni router è limitata, ciascun router dovrà controllare e decidere quali flussi allocare e quali rifiutare, adottando una modalità non più Best Effort.

IntServ: elementi funzionali

- Traffic Classes: classi di servizio ottenibili
- Traffic Controller: esegue controllo sul traffico che transita su ogni nodo di rete (ad esempio con WFQ)
- Setup Protocol: costituisce il sistema di segnalazione fra i nodi di rete per l'allocazione delle risorse di banda

DiffServ: Modello

- La complessità si sposta all'edge della rete, dove si classificano i singoli pacchetti, si marchiano ("colorazione") e si aggregano per poi inviarli nel core
- Flussi provenienti da diverse applicazioni possono essere aggregati insieme e trattati allo stesso modo (non è più l'applicazione che decide la QoS, come in IntServ): DiffServ opera su aggregati
- Nel core, il flusso aggregato riceve un trattamento relativo alla classe di servizio e al colore dei pacchetti che contiene (per-class state, non più per-flow)
- Non c'è più segnalazione (RSVP) né Admission Control e, dunque, si deve fare provisioning delle risorse a priori (si allocano più risorse del necessario), e controllare all'edge che il traffico immesso non sia eccessivo

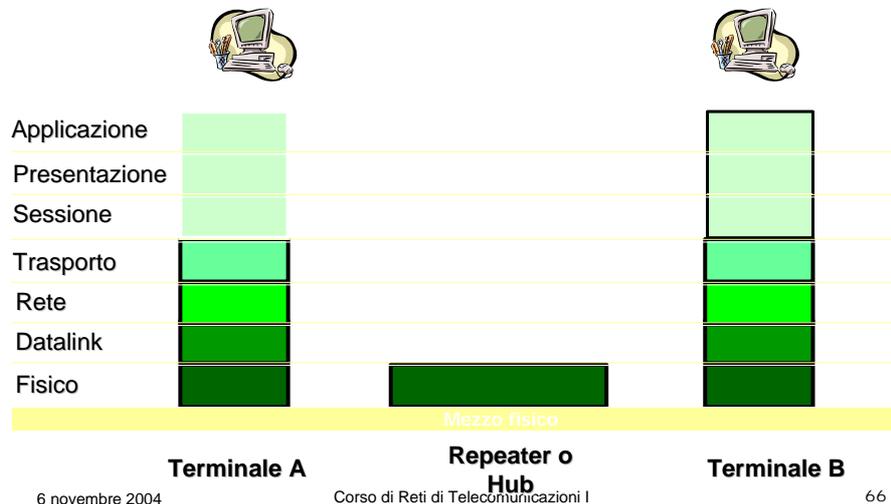
DiffServ: tipologie di PHB

- **Default:** Best Effort tradizionale
- **Expedited Forwarding** (EF-RFC 2598): supporta connessioni con basse perdite, basso ritardo e basso jitter; lo switching nel core deve essere rapido, e dunque il traffico è condizionato all'edge e il rate in ingresso è limitato. Usa un solo DSCP (101110, 46) per immettere il pacchetto nella coda a più alta priorità nei router di rete (con WFQ ad esempio)
- **Assured Forwarding** (AF- RFC 2597): definisce 4 classi di servizio relative, ciascuna con tre livelli di precedenza di scarto; usa, quindi, 12 distinte combinazioni di DSCP. Lo SLA dipende da:
 - classe AF (risorse allocate),
 - livello di traffico di quella classe,
 - drop precedence (in caso di congestione)

Apparati di Interconnessione

- **Obiettivi**
 - Aumentare estensione geografica rete
 - Aumentare numero di utenti collegabili ad una rete
 - Vincolo di non modificare protocolli (software e hardware utenti)
 - In generale, permette di ottenere prestazioni migliori
- **Apparati**
 - Repeater e Hub (livello 1)
 - servono per superare le limitazioni di alcuni mezzi trasmissivi
 - Bridge e Switch (livello 2)
 - hanno algoritmi di instradamento molto semplici
 - si utilizzano normalmente per interconnessioni locali
 - Router (livello 3)
 - hanno algoritmi di instradamento sofisticati
 - si utilizzano normalmente per interconnessioni geografiche
 - Gateway (livello 7)
 - si utilizzano per interconnettere architetture di rete diverse (es. SNA e Internet)

Apparati di Interconnessione



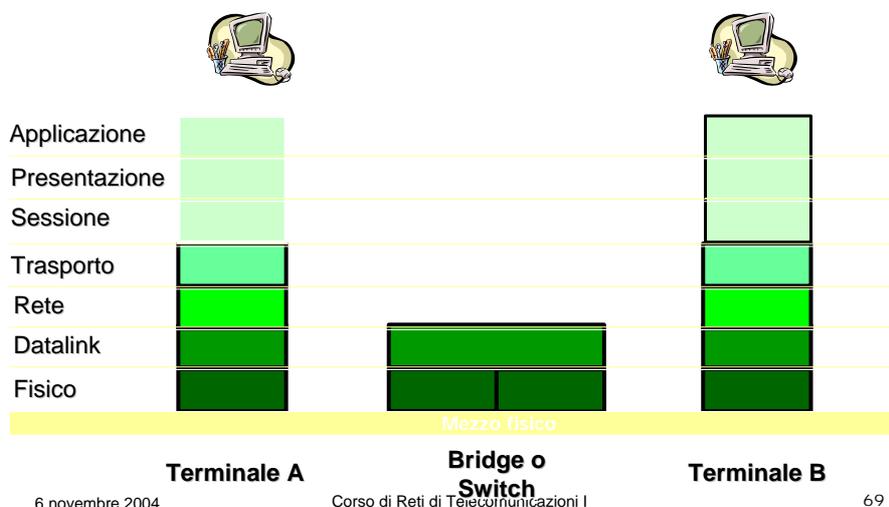
Repeater

- È un apparato di livello 1 (fisico), quindi interpreta solo i segnali elettrici e ha come unità trasmissiva il singolo bit
- Il repeater serve ad estendere la lunghezza del canale trasmissivo su LAN omogenee
- Porta a realizzare topologie ad albero
- Rigenera stringhe di bit ricevute su un canale e le ritrasmette sugli altri canali

Hub

- È un repeater multiporta
- È un concentratore di cablaggio (opera a livello fisico)
- Serve a collassare una topologia a bus o ad anello in un topologia a stella, semplificando (e rendendo più affidabili) le operazioni di cablaggio e manutenzione
- Ovviamente, non aumenta la capacità trasmissiva

Apparati di Interconnessione



Bridge

- Interconnettono LAN anche con livelli fisici e MAC diversi, ma con lo stesso LLC
- Se protocolli sono diversi, necessaria traduzione delle intestazioni (PCI)
- Funzionano in modalità store and forward
- Non intervengono sul contenuto dei pacchetti
- Intelligenza di instradamento limitata
- LAN interconnesse da bridge sono separate
- Tutte le stazioni credono di essere collegate alla stessa LAN (trasparenza). Le LAN interconnesse sono dette anche LAN estese.

Bridge

- Migliorano
 - affidabilità
 - prestazioni (diversità spaziale, sfruttamento località del traffico)
- Permettono estensione geografica della rete
- Si può introdurre sicurezza (separazione del traffico)
- È necessario che ogni apparato abbia un indirizzo di livello 2 unico all'interno della LAN estesa
- Le procedure più comuni di instradamento su LAN estese sono:
 - spanning tree
 - source routing (legato a Token Ring)
- Ogni bridge ha un suo indirizzo (bridge_ID) e un identificativo per ogni porta (port_ID)

Switch

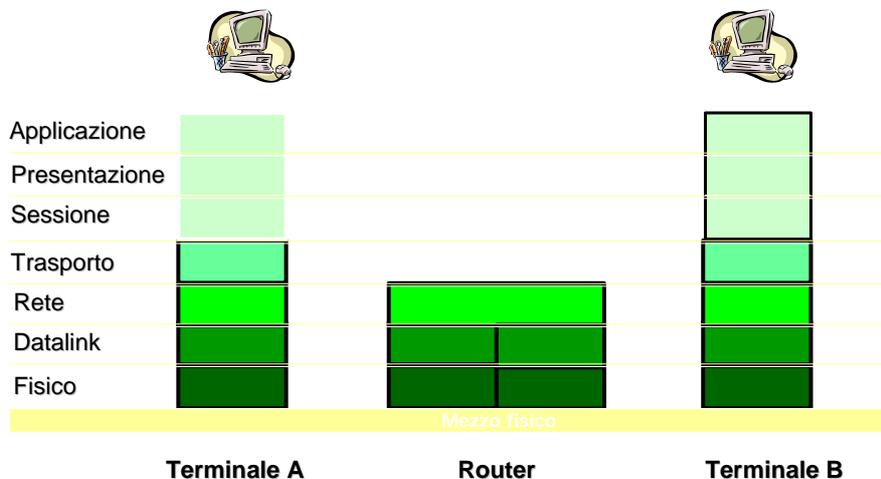
- È funzionalmente equivalente ad un bridge che opera su più di 2 porte
- Sono associati a topologie a stella o ad albero (cablaggio strutturato)
- Spesso ha una sola stazione per porta collegata
- Talvolta non supporta l'algoritmo spanning tree
- Supporta le LAN virtuali

6 novembre 2004

Corso di Reti di Telecomunicazioni I

72

Apparati di Interconnessione



6 novembre 2004

Corso di Reti di Telecomunicazioni I

73

Router

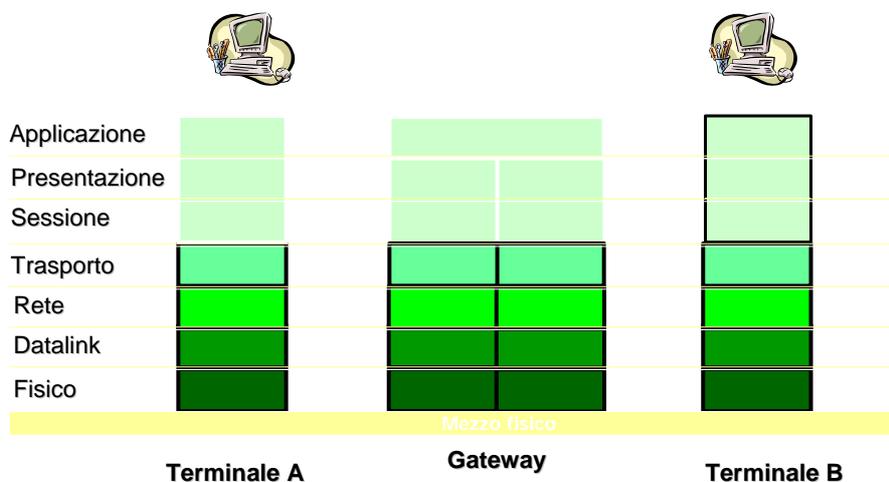
- Dispositivo di livello 3 (rete)
- Spesso multiprotocollo
- Implementano funzionalità di instradamento
- Nelle reti Internet lavorano a livello IP
 - Sono il dispositivo necessario a interconnettere LAN a Internet

6 novembre 2004

Corso di Reti di Telecomunicazioni I

74

Apparati di Interconnessione



6 novembre 2004

Corso di Reti di Telecomunicazioni I

75

Gateway

- Permettono di collegare sistemi appartenenti ad architetture di rete diverse
- Lavorando a livello applicativo si collocano a livello 7 OSI
- Esempio classico di gateway è quello per la posta elettronica