

Università di Genova
Facoltà di Ingegneria

Livello di Applicazione in Internet
**9. Intranet ed interconnessione
con Internet**

Prof. Raffaele Bolla



Intranet

- Il nome **Intranet** indica semplicemente una rete “aziendale” (quindi privata) che utilizza la tecnologia di Internet (TCP/IP).
- Una Intranet può essere o meno collegata ad Internet.
- Collegare ad internet una intranet implica affrontare un certo insieme di problemi che sono principalmente legati:
 - all’indirizzamento;
 - al tipo di interconnessione fra l’intranet e l’ISP (*Internet Service Provider*).
- Anche nel caso in cui non sia immediatamente necessario collegare la rete ad internet è comunque opportuno tener conto nella progettazione di un possibile futura interconnessione.

Indirizzamento

- Gli indirizzi su Internet devono essere univoci, questo implica che, in teoria, se collego una intranet ad Internet, tutti gli indirizzi usati sulla rete devono essere assegnati univocamente dalla IANA (Internet Assigned Numbers Authority) all'azienda proprietaria della rete.
- Questa operazione ha un costo, gli indirizzi disponibili non sono molti, ed in genere non è strettamente necessario (anzi talvolta non sarebbe neppure opportuno) che ciascun utente abbia un indirizzo diretto (pubblico) su Internet.

Complementi di Reti e Sistemi R. Bolla

9.3

Indirizzi Privati

- La IANA ha definito uno spazio di indirizzamento ad uso privato, ossia un insieme di reti i cui indirizzi non vengono propagati dai router di Internet:
 - Una classe A: 10.0.0.0/8
 - 16 Classi B: dalla 172.16.0.0/16 alla 172.31.0.0/16
 - 256 classi C: dalla 192.168.0.0/24 alla 192.168.255.0/24
- L'idea di fondo è quella che l'intranet utilizzi al suo interno questi indirizzi, l'azienda si faccia assegnare un numero di indirizzi "pubblici" minore del numero di interfacce presenti sulla propria rete e si applichi nel punto di interconnessione con internet un meccanismo di "traduzione" (NAT).

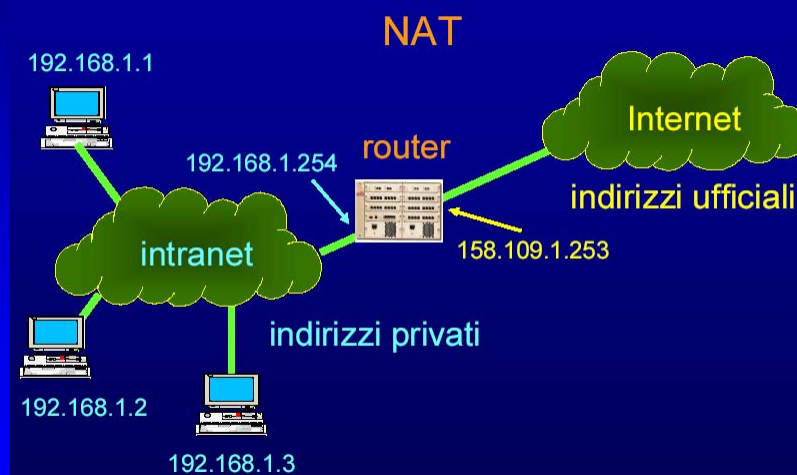
Complementi di Reti e Sistemi R. Bolla

9.4

NAT

- **Network Address Translation**
- Riduce il numero di indirizzi IP pubblici necessari per collegare una LAN a Internet.
- Mantiene inalterati la configurazione di rete e il funzionamento dei protocolli e delle applicazioni (nel caso in cui si attivi l'interconnessione in un tempo successivo o si cambi piano di indirizzamento esterno e si stia già utilizzando gli indirizzi privati)
- Porta un maggiore sicurezza per i calcolatori della rete privata

NAT

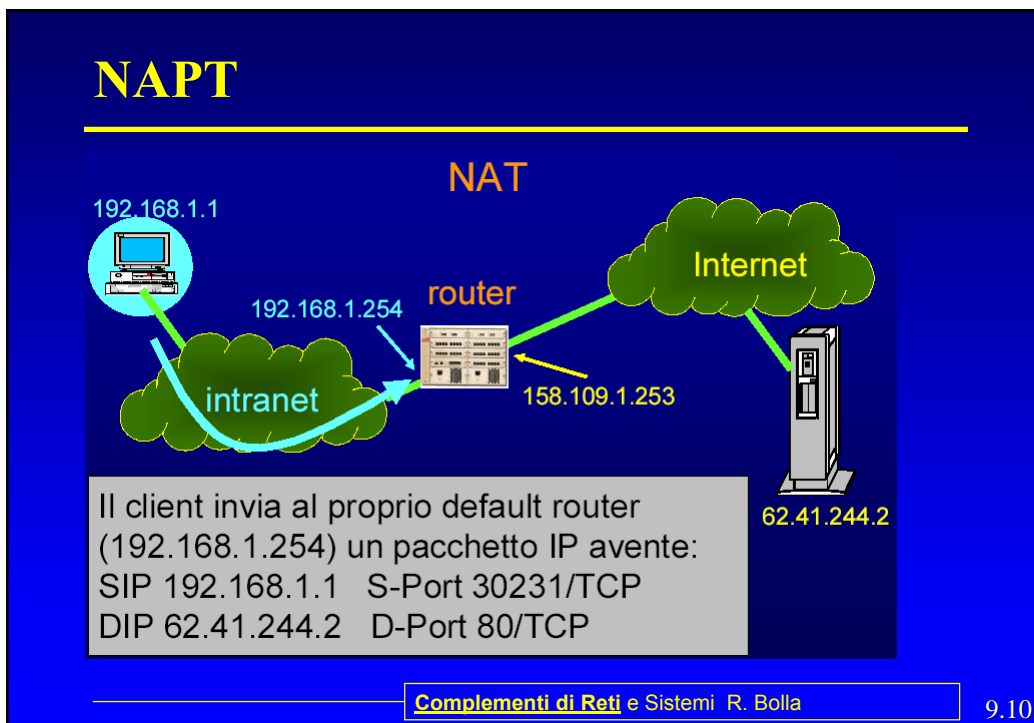
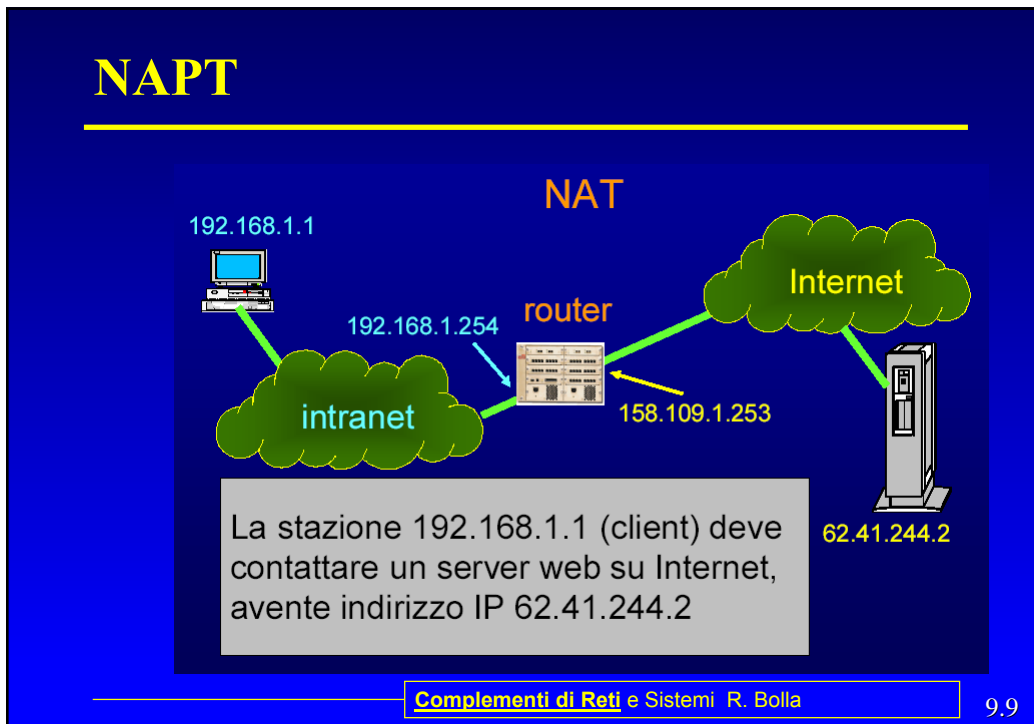


NAT

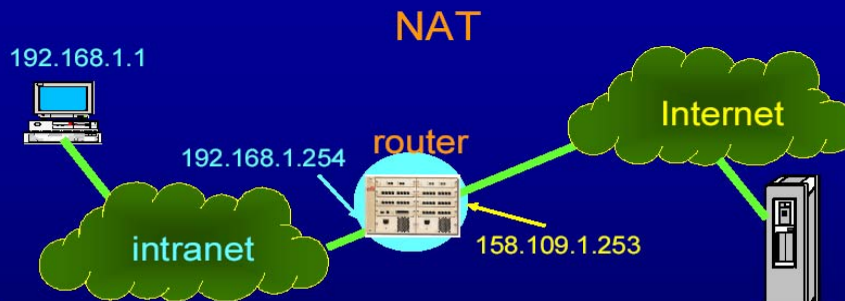
- La traduzione di indirizzi può avvenire in diversi modi:
 - Univoco, ossia ad un indirizzo privato viene fatto corrispondere un indirizzo fisico, e questa tecnica può portare a due ulteriori distinzioni:
 - » Statico (usato in genere per i server)
 - » Dinamico
 - Non univoco, ossia fatto sulla base della coppia Indirizzo-Porta, si ha quindi un NAPT (Network Address Port Translation) o un IP Masquerading o un NAT-PAT

Caso tipico: NAPT o IP masquerading dinamico

- Permette di condividere una singola connessione a Internet per più calcolatori di una intranet (rete IP privata).
- Tecnica frequentemente utilizzata nel caso degli accessi xDSL o ISDN per piccole/medie reti aziendali.



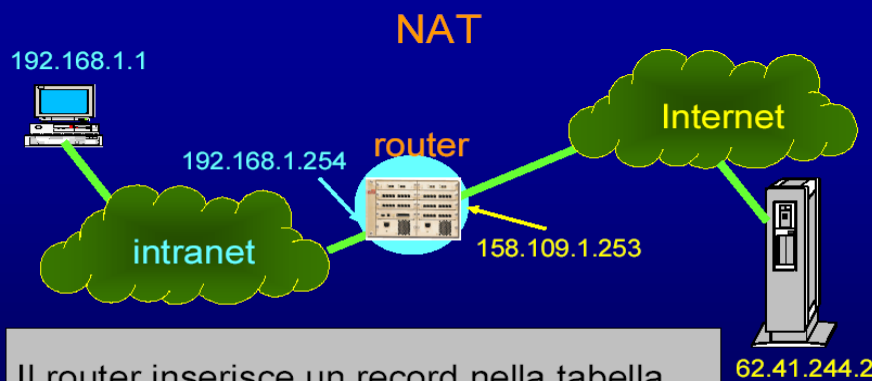
NAPT



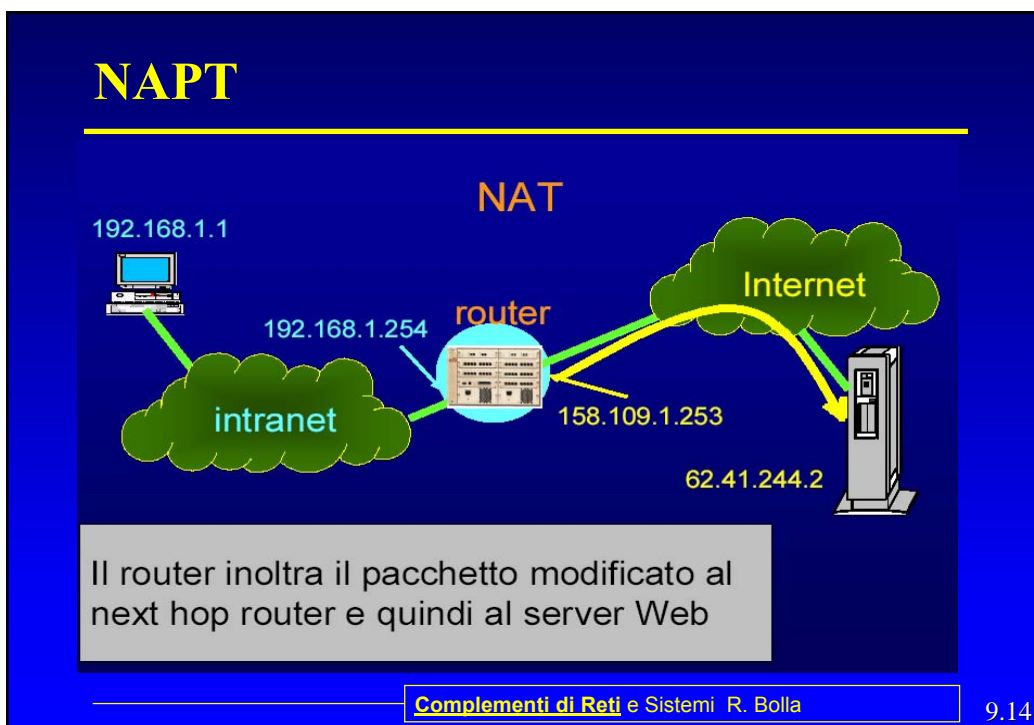
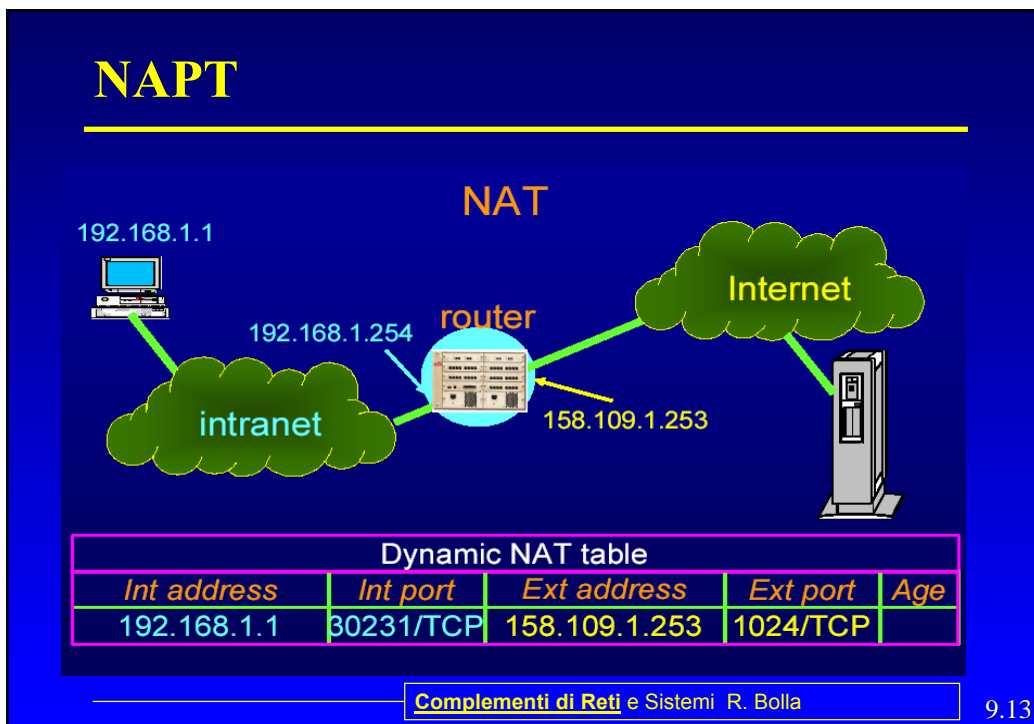
Il router riceve il pacchetto e, prima di inoltrarlo, ne modifica:

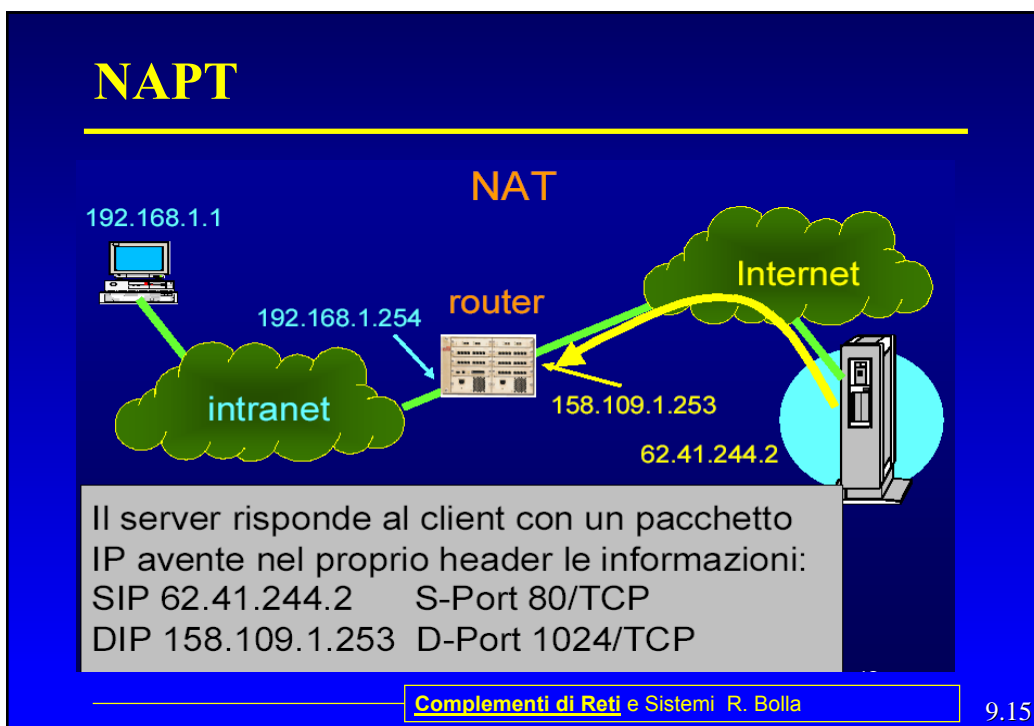
- l'indirizzo sorgente: 192.168.1.1 \Rightarrow 158.109.1.253
- la porta sorgente: 30231/TCP \Rightarrow 1024/TCP

NAPT



Il router inserisce un record nella tabella delle corrispondenze (Dynamic NAT table) per tenere traccia del flusso di dati uscente





NAPT

NAT

192.168.1.1

192.168.1.254

158.109.1.253

intranet router Internet

Dynamic NAT table				
<i>Int address</i>	<i>Int port</i>	<i>Ext address</i>	<i>Ext port</i>	<i>Age</i>
192.168.1.1	30231/TCP	158.109.1.253	1024/TCP	

Complementi di Reti e Sistemi R. Bolla 9.17

NAPT

NAT

192.168.1.1

192.168.1.254

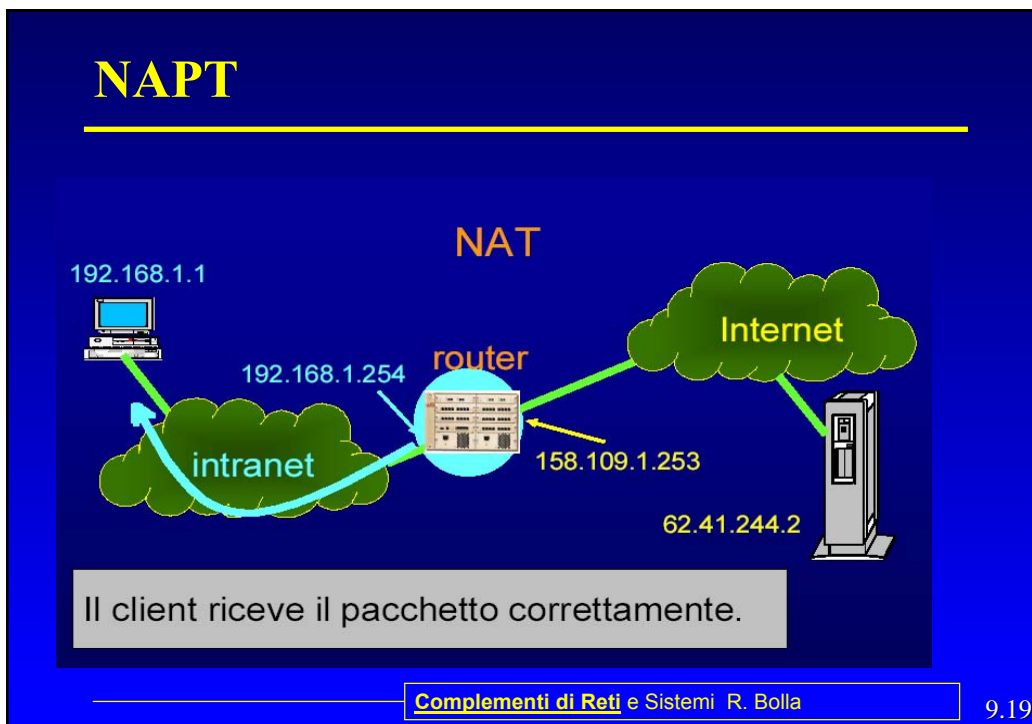
158.109.1.253

intranet router Internet

Il router prima di inoltrare il pacchetto al client ne modifica:

- l'indirizzo destinazione: 158.109.1.253 ⇒ 192.168.1.1
- la porta destinazione: 1024/TCP ⇒ 30231/TCP

Complementi di Reti e Sistemi R. Bolla 9.18



- ## NAPT
- Ogni client dialoga con qualunque server esterno senza accorgersi della traduzione di indirizzo (NAT) e di porta (PAT) effettuati dal default router
 - Ulteriori flussi uscenti genereranno nuove entry nella tabella dinamica.
 - Porte usate dal router per la PAT: 1024 - 4999.
 - Per rendere raggiungibili eventuali server interni occorre forzare la traduzione inserendo delle entry statiche nella tabella del router.
 - Ci sono dei problemi nella realizzazione pratica di questi meccanismi che talvolta generano malfunzionamenti e che rendono il processo di traduzione reale significativamente più complesso di quello qui delineato.
- Complementi di Reti e Sistemi R. Bolla 9.20

Interconnessione all'ISP

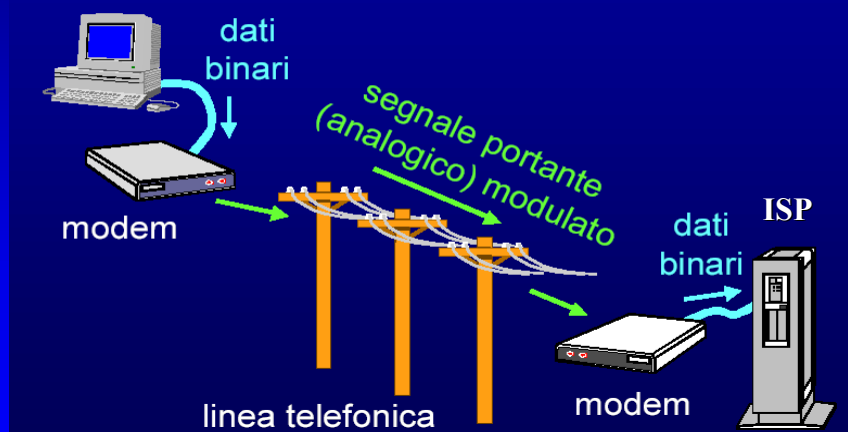
- In generale il problema è usufruire di un collegamento fra l'utente e l'ISP.
- In genere la soluzione più frequente sfrutta la rete pubblica pre-esistente dei gestori di telefonia (in doppino): si tenta quindi di utilizzare al meglio l' "ultimo miglio".
- Due tipologie di interconnessione:
 - Commutata, fra cui
 - » Modem su linea telefonica analogica (V.90)
 - » N-ISDN
 - Fissa, fra cui
 - » ADSL, xDSL
 - » CDN (Circuito Dedicato Numerico)
 - » ATM

Complementi di Reti e Sistemi R. Bolla

9.21

Modem Telefonico

Impiego dei modem (in teoria)



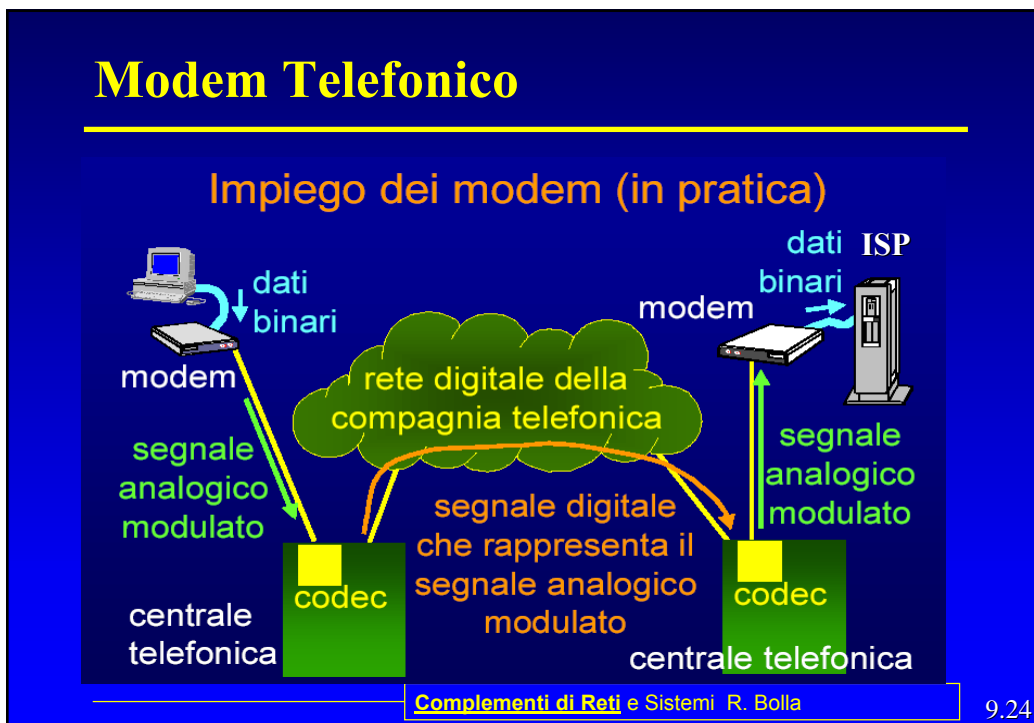
Complementi di Reti e Sistemi R. Bolla

9.22

Modem Telefonico

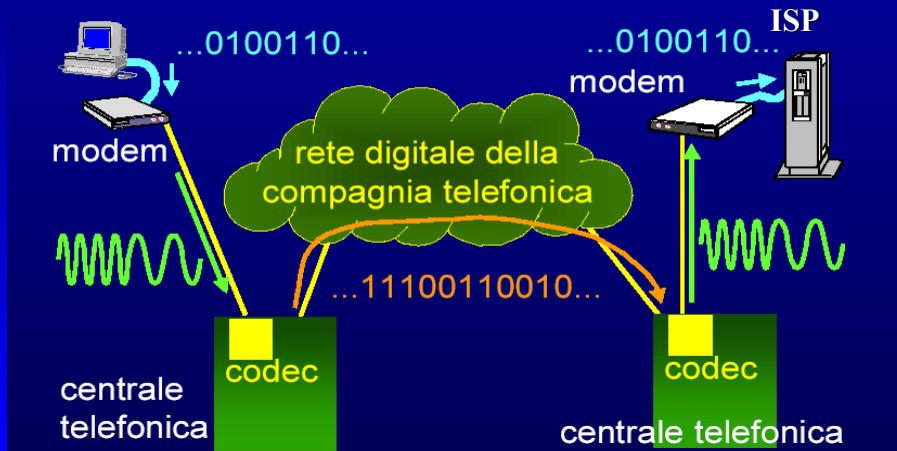


Modem Telefonico



Modem Telefonico

Impiego dei modem (in pratica)

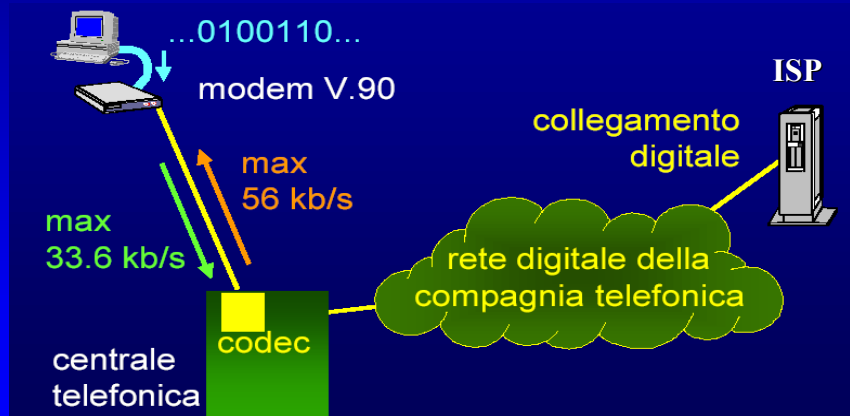


Complementi di Reti e Sistemi R. Bolla

9.25

Standard V.90

- Supera il limite del rumore di quantizzazione dovuta alla codifica A/D
- Richiede un collegamento digitale alla centrale telefonica su cui è attestato l'utente



Complementi di Reti e Sistemi R. Bolla

9.26

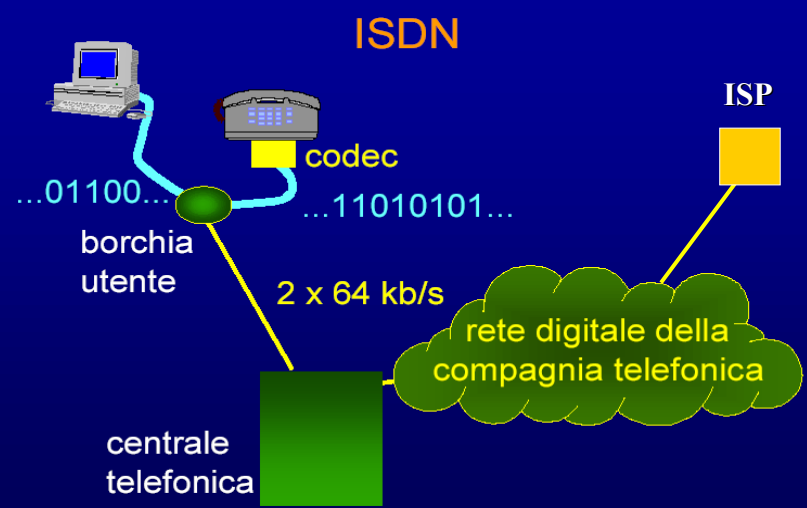
N-ISDN

- **Narrowband - Integrated Services Digital Network**
- Rappresenta l'evoluzione della telefonia analogica.
- Sostituisce la linea telefonica analogica commutata con una linea digitale commutata da 64/128 Kbps.
- Come la linea telefonica è tariffata a tempo.

Complementi di Reti e Sistemi R. Bolla

9.27

N-ISDN



Complementi di Reti e Sistemi R. Bolla

9.28

ADSL, HDSL

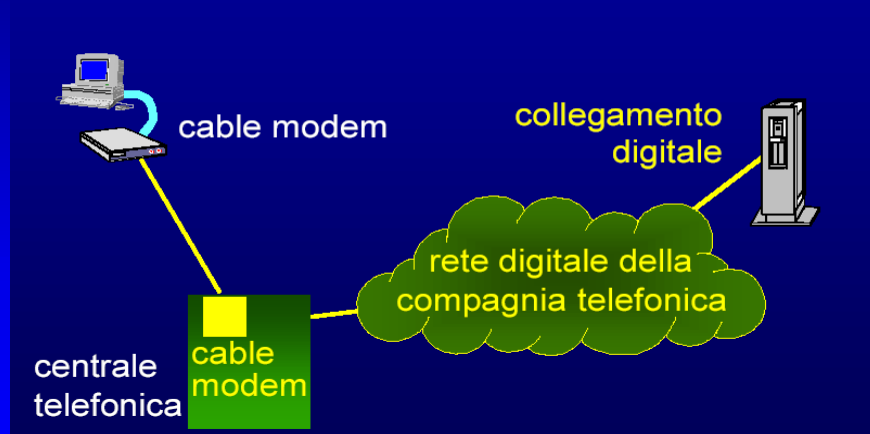
- **ADSL**: Asymmetric Digital Subscriber Line
- **HDSL**: High-Bit-Rate Digital Subscriber Line
- In generale: xDSL
- Eliminano completamente le apparecchiature in banda fonica per utilizzare al meglio il doppino telefonico
- Richiede l'installazione delle apparecchiature nella centrale telefonica e non sfruttano la rete telefonica

Complementi di Reti e Sistemi R. Bolla

9.29

ADSL, HDSL

ADSL, HDSL, ecc.



Complementi di Reti e Sistemi R. Bolla

9.30

CDN - ATM

- Sono circuiti numerici punto-punto dedicati a velocità che vanno da 64Kbps a 2Mbps.
- Sono realizzati dalla Telecom attraverso una rete detta “rete flessibile” che si appoggia sulla rete SDH (o PDH)
- Velocità superiori (da 34 Mbps in su) sono forniti utilizzando direttamente la rete SDH
- In alternativa si usano collegamenti ABR, VBR e CBR su ATM.

Complementi di Reti e Sistemi R. Bolla

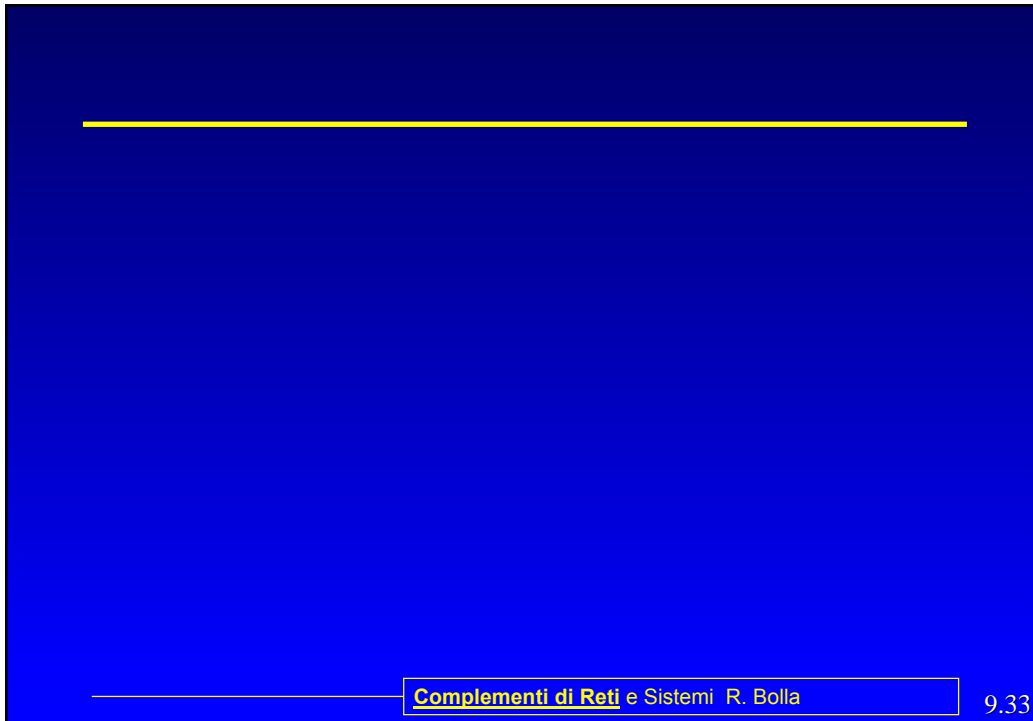
9.31

PPP

- Il *Point-to-Point Protocol (PPP)* nasce, in origine, per il trasporto su collegamenti punto - punto di pacchetti IP.
- E' diventati poi uno standard per
 - l'assegnamento e la gestione di indirizzi IP
 - incapsulamento sincrono (bit-stuffing) ed asincrono (character stuffing),
 - il multiplexing di protocolli di rete,
 - la configurazione la verifica della qualità della linea,
 - la rivelazione d'errore
 - la negoziazione di parametri e di compressione di intestazioni e dati a livello di rete
 - L'autenticazione dell'accesso

Complementi di Reti e Sistemi R. Bolla

9.32



Point-to-Point Protocol (PPP)

- Il *Point-to-Point Protocol (PPP)* nasce, in origine, per il trasporto di pacchetti IP (ossia per fornire un livello di linea semplice all'IP) su collegamenti dedicati punto - punto.
- Le sue funzioni si sono estese nel tempo fino a coprire:
 - l'assegnamento e la gestione di indirizzi IP;
 - l'incapsulamento sincrono (bit-stuffing) ed asincrono (character stuffing);
 - il multiplexing di protocolli di rete;
 - la configurazione e la verifica della qualità della linea,
 - la rivelazione d'errore;
 - la negoziazione di parametri e della compressione dell'intestazioni e dei dati del livello di rete;
 - L'autenticazione dell'accesso.

PPP

- E' descritto negli RFC 1661, 1662 e 1663
- Si compone di più parti, le principali sono:
 - Una parte comune che opera la suddivisione non ambigua delle trame (inizio e fine) o frame e permette la rilevazione degli errori;
 - Un *Link Control Protocol* (LCP) che attiva la linea fisica, ne verifica il funzionamento e negozia parametri quali, ad esempio, la dimensione del pacchetto e il tipo di autenticazione;
 - Un *Network Control Protocol* (NCP) che gestisce le informazioni sui protocolli di livello più alto (livello 3). Ciascun protocollo di livello tre ha un proprio specifico tipo di NCO (per esempio: IPCP per IP).
 - Un protocollo per l'autenticazione (*Password Authentication Protocol* -PAP, *Challenge Handshake Authentication Protocol* CHAP o *Remote Authentication Dial-In User Service* - RADIUS)

Complementi di Reti e Sistemi R. Bolla

9.35

Sequenza di funzionamento

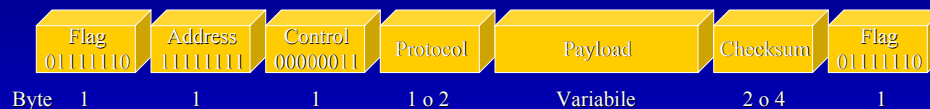
- Scenario di esempio: PC che si vuole connettere a Internet.
 - Il PC si connette a livello fisico con il router del fornitore (ad esempio tramite un modem e una linea telefonica);
 - Attivato il collegamento fisico, il PC manda una serie di pacchetti LCP nel campo *Payload* di una o più trame PPP: in base alle risposte si scelgono i parametri da utilizzare sulla linea;
 - Una volta raggiunto un "accordo" vengono inviati una serie di pacchetti NCP per configurare il livello rete (ad esempio l'indirizzo IP dinamico);
 - Al termine del collegamento viene utilizzato NCP per rilasciare l'indirizzo.

Complementi di Reti e Sistemi R. Bolla

9.36

Formato della trama

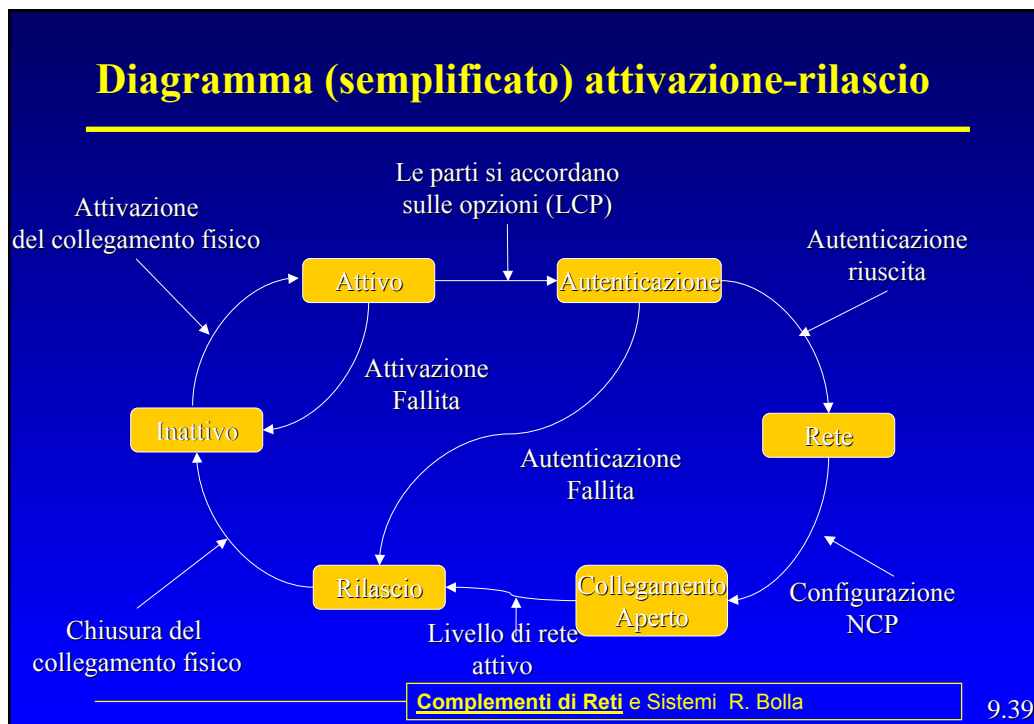
- PPP simile all'HDLC ma orientato al carattere



- *Flag*: come in HDLC (bit stuffing nel *Payload*)
- *Address*: sempre 11111111; “diretto a tutte le stazioni”
- *Control*: sempre 00000011: ovvero trame non numerate
 - LCP permette di negoziare l’eliminazione dei campi *Address* e *Control* che sono sempre uguali

Formato Pacchetto

- *Protocol*: indica il tipo di pacchetto contenuto nel campo *Payload*:
 - Inizia con 0 per i protocolli di rete come IP, IPX, OSI, CLNP e XNS;
 - Inizia con 1 per i protocolli usati per negoziare altri protocolli come LCP e NCP, diversi per ogni protocollo di rete supportato;
- *Payload*: ha dimensione variabile che arriva fino ad un massimo negoziato in fase iniziale, se non negoziato altrimenti la lunghezza è fissata a 1500 byte (si utilizza un riempimento).



- ### LCP
- È un meccanismo di negoziazione più che definire le opzioni;
 - È un metodo per permettere la processo che inizia di fare una proposta e al processo che risponde di accettare o rifiutare in parte o totalmente;
 - Permette di testare la linea (se è abbastanza buona per stabilire la connessione)
 - Permette di rilasciare le linee quando non più necessarie
- Complementi di Reti e Sistemi R. Bolla 9.40

LCP

- 11 tipi di pacchetti

Nome	Direzione	Descrizione
Configure-request	I \Rightarrow R	Lista delle opzioni e dei valori proposti
Configure-ack	I \Leftarrow R	Tutte le opzioni sono accettate
Configure-nak	I \Leftarrow R	Alcune opzioni non sono accettate
Configure-reject	I \Leftarrow R	Alcune opzioni non sono negoziabili
Terminate-request	I \Rightarrow R	Richiesta di chiusura della linea
Terminate-ack	I \Leftarrow R	OK, linea chiusa
Code-reject	I \Leftarrow R	Ricevuta richiesta sconosciuta
Protocol-reject	I \Leftarrow R	Protocollo richiesto sconosciuto
Echo-request	I \Rightarrow R	Rispedire indietro il frame
Echo-reply	I \Leftarrow R	Questo è il frame rispedito indietro
Discard-request	I \Rightarrow R	Scartare questo frame (per test)

Complementi di Reti e Sistemi R. Bolla

9.41

PPP over ATM

- PPP over ATM si basa su Adaptation Layer 5 di ATM (AAL5) (RFC 2364) quindi utilizza per il formato dei frame lo standard AAL5 che è in grado di realizzare sia PVC sia SVC.
- PPPoA è stato studiato principalmente come supporto per ADSL.
- It relies on RFC1483, operating in
- either Logical Link Control-Subnetwork Access Protocol (LLC-SNAP) or VC-Mux mode. A customer
- premises equipment (CPE) device encapsulates the PPP session based on this RFC for transport across the
- ADSL loop and the digital subscriber line access multiplexer (DSLAM).

Complementi di Reti e Sistemi R. Bolla

9.42

ADSL Access

QuickTime™ and a TIFF (Uncompressed) decompressor are needed to see this picture.

Complementi di Reti e Sistemi R. Bolla

9.43

PPPoA

QuickTime™ and a TIFF (Uncompressed) decompressor are needed to see this picture.

PPPoA

Complementi di Reti e Sistemi R. Bolla

9.44