

# *Reti di Calcolatori*

---

## *Terzo Modulo*

### *Protocolli complementari ad IP, NATting, PPP*

*vers.1.0*

Claudio Covelli

[claudio.covelli@gmail.com](mailto:claudio.covelli@gmail.com)

Trento, 7 dicembre 2007



# Agenda



---

## Protocolli complementari ad IP, Natting, PPP

- ARP
- ICMP
- Tecniche di natting
- PPP



# Arp

## Protocollo ARP (Address Resolution Protocol)

- Il secondo livello dello stack ISO/OSI (data link) corrisponde al livello Network Interface dello stack TCP/IP
- In questo livello sono situate molte delle tecnologie LAN/WAN viste nel corso (es. FrameRelay, ATM, Ethernet)
- Il terzo livello (IP) effettua invece l'instradamento dei pacchetti fra le varie LAN (internetworking) e **consente l'interconnessione fra più LAN diverse e di tecnologia differente (Internet)**



# Arp

## Protocollo ARP (Ethernet Address Resolution Protocol)

- IP usa indirizzi logici usati per l'internetworking; il livello 2 indirizzi fisici (es. MAC Address per Ethernet) utilizzati per la consegna fisica all'interno della singola LAN
- Esiste quindi la necessità di un protocollo che consenta la trasformazione degli indirizzi logici in indirizzi fisici
- Tale protocollo viene denominato ARP (Address Resolution Protocol)
- Impraticabilità del direct mapping (cfr. [www.tcpipguide.com](http://www.tcpipguide.com))



# Arp

---

## Protocollo ARP (Ethernet Address Resolution Protocol)

- Si tratta quindi di un protocollo complementare ad IP , di **raccordo fra i livelli 3 e 2** (alcuni autori lo considerano di livello 3; altri di livello 2)



# Arp

## Protocollo ARP (Ethernet Address Resolution Protocol)

- Una transazione ARP nasce quando il layer IP deve inviare un pacchetto al **destinatario sulla stessa sottorete** oppure, in alternativa, al **router**
- In entrambi i casi, IP conosce l'indirizzo IP del destinatario (proviene dal livello applicativo oppure, nel caso del gateway, dalla configurazione della scheda di rete ) ma **NON** il suo indirizzo fisico
- IP **delega ad ARP** l'ottenimento di questa informazione



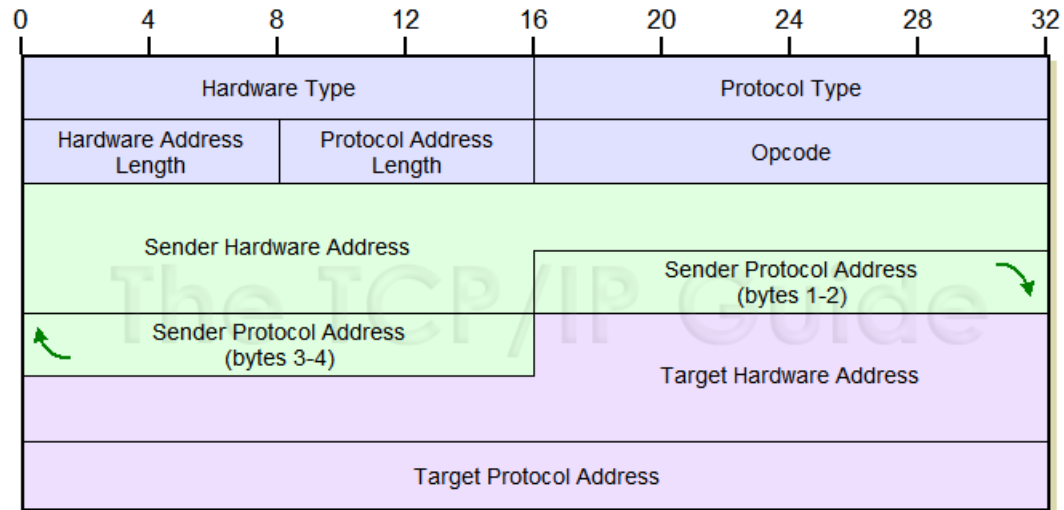
# Arp

---

## Protocollo ARP

- ARP chiede ad Ethenet di inviare sulla rete un **particolare frame (Arp request)** contenente la richiesta dell'indirizzo MAC
- Tale frame ha come MAC source quello della scheda di rete del mittente e come MAC destinatario, un valore corrispondente a tutti 1 (**FF:FF:FF:FF:FF:FF**) in modo **che sia letta da tutte le schede di rete della LAN (broadcasting di livello 2)**
- Nella richiesta sono inoltre riportati l'indirizzo IP mittente e destinatario

# Arp



Frame ARP



# Arp

## Protocollo ARP

---

- Tutte le schede di rete leggono il frame in quanto esso è di broadcasting
- Solo la scheda di rete avente indirizzo IP corrispondente a quello del destinatario, risponde, inviando al richiedente un frame (**ARP reply**) riportante il suo MAC
- ARP mittente archivia il MAC destinatario in una **tabella di cache**



# Arp

## Protocollo ARP

---

- Anche il destinatario aggiorna la sua tabella di cache; per tale motivo nel frame di richiesta è presente anche l'indirizzo IP del mittente (**cross-resolution**)
- La tabella di cache consente di evitare continui broadcasting che possono portare a collisioni e rallentamenti nella rete
- La tabella viene aggiornata ad intervalli regolari per eliminare la presenza di informazioni obsolete



# Arp

---

## Protocollo ARP

- Laboratorio: analisi del protocollo ARP tramite Ethereal
- Arp poisoning  
(<http://www.oxid.it/downloads/apr-intro.swf>)

# ICMP

## ICMP (Internet Control Message Protocol)

- IP è stato progettato come protocollo “leggero”, con l'esclusivo compito di trasmettere i pacchetti fra le LAN ([internetworking](#))
- Esso opera negli host mittente e destinatario ma [soprattutto nei vari router, interposti fra tali host](#), prendendosi carico del corretto instradamento di tutti i pacchetti trasmessi
- IP è [connectionless, unreliable and unacknowledged](#) nel senso che si limita ad instradare tali pacchetti, demandando a TCP lato destinatario tutti gli aspetti riguardanti la loro corretta ricezione, la notifica al mittente (acknowledgment) e l'eventuale richiesta di ritrasmissione

# ICMP

## ICMP (Internet Control Message Protocol)

- Possono però verificarsi **errori in uno dei vari router** che compongono il percorso di instradamento dei pacchetti fra il mittente ed il destinatario (**errori di livello 3**)
- Ad esempio potrebbe accadere che un router sia configurato in modo errato e quindi non riesca ad inoltrare i pacchetti alla rete di destinazione (perchè manca banalmente la entry nella relativa tabella di routing oppure è errato il gateway impostato per una certa destinazione etc)
- Può anche succedere che un certo router tutto ad un tratto non sia più disponibile (blocco o sovraccarico) e quindi alcuni pacchetti vadano persi

# ICMP

## ICMP (Internet Control Message Protocol)

- In tutti i casi nei quali si verificano questi errori, è importante notificare IP lato mittente del problema verificatosi, in modo che possano essere adottate le necessarie contromisure
- E' infatti da notare che **TCP lato destinatario**, in casi come questi, **o non riceverebbe alcun pacchetto** (es. errore di configurazione) **oppure li riceverebbe in modo incompleto** (blocco o sovraccarico), limitandosi a chiederne la ritrasmissione, **senza poter notificare il mittente circa i motivi della perdita**



# ICMP

---

## ICMP (Internet Control Message Protocol)

- Si deduce quindi che esiste la necessità di informare IP lato mittente che esistono problemi in fase di instradamento dei pacchetti in modo che siano date indicazioni precise sul tipo di errore verificatosi

# ICMP

## ICMP (Internet Control Message Protocol)

- Ip delega ad uno specifico protocollo (ICMP) la notifica ad IP mittente di tutti i problemi riscontrati in fase di instradamento, usando messaggi opportunamente codificati
- Si può quindi considerare ICMP un protocollo corollario ad IP, nel senso che è parte integrante di quest'ultimo
- I messaggi ICMP sono inglobati, come se fossero dati, in pacchetti IP

# ICMP



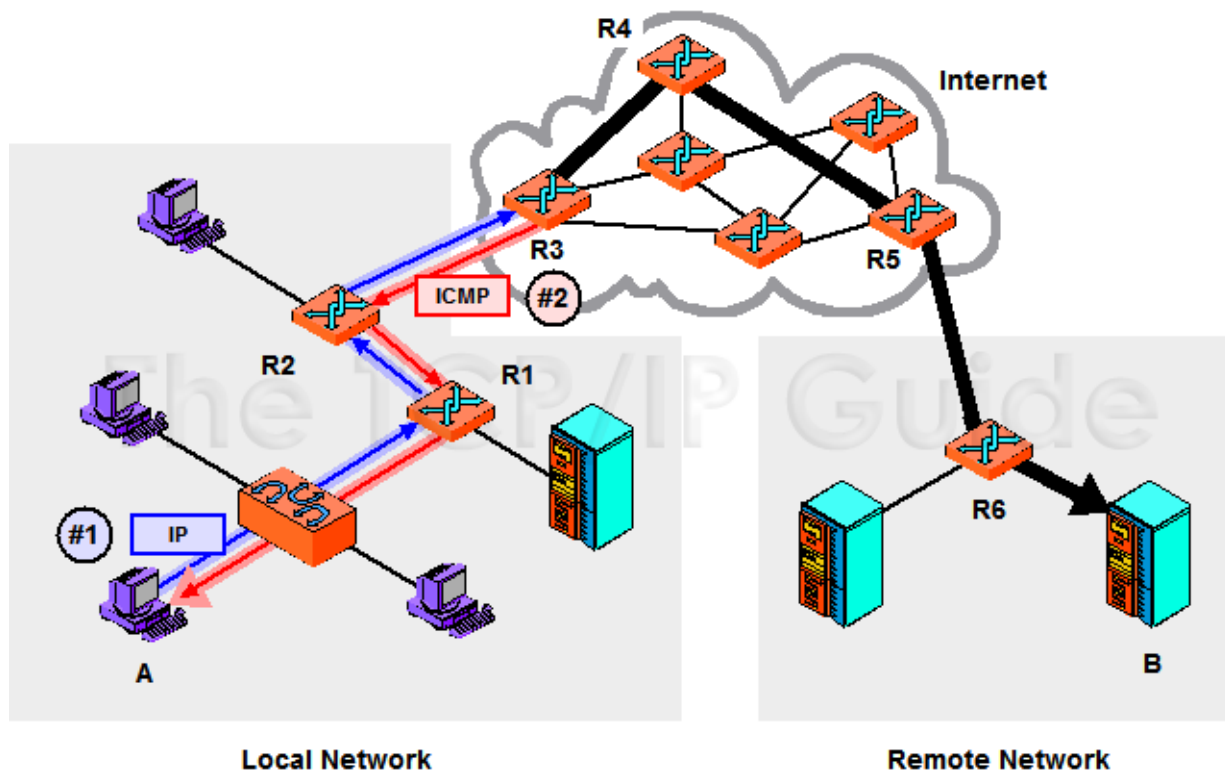
---

## ICMP

- ICMP è stato progettato per notificare non solo errori (**error messages**) ma anche informazioni di vario tipo (**informational messages**)
- I messaggi ICMP di tipo error sono trasmessi dal **layer IP del router che riscontra problemi nell'instradamento del pacchetto**, anche nei casi nei quali questi dipendano da uno dei router precedentemente attraversati
- Questo comporta evidentemente dei limiti nella tracciabilità dell'errore ma semplifica sensibilmente la progettazione e gestione del protocollo

# ICMP

ICMP



# ICMP



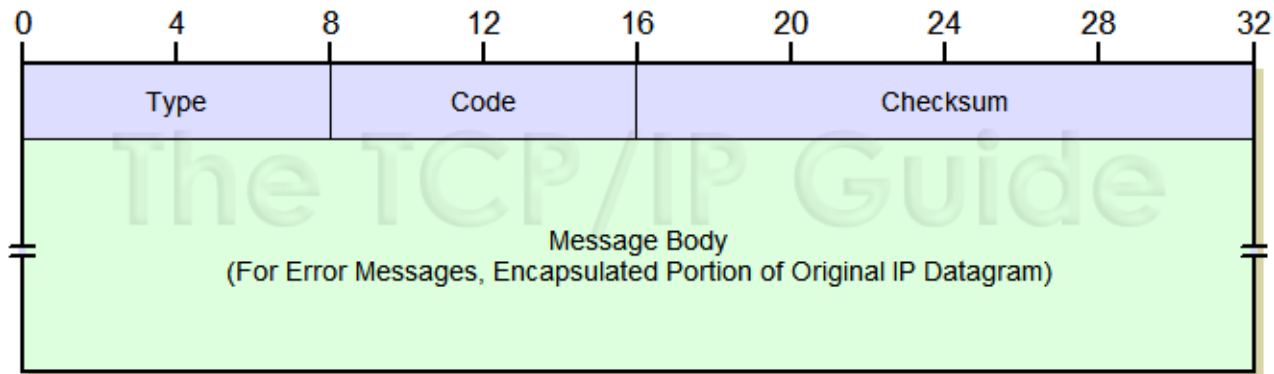
---

## Protocollo ICMP

- Laboratorio: verifica del messaggio Destination Network Unreacheable ottenuto pingando un indirizzo Internet inesistente (193.207.9.253)

# ICMP

## ICMP (dati inviati tramite pacchetti IP)



- Type (da 1 a 127 error messages; da 128 a 255 informational messages)
- Code (ulteriore specificazione di type)
- Checksum
- Dati (valore funzione del type)

# ICMP



---

## ICMP

- Due tipi di informational messages frequentemente utilizzati :
  - ◆ **Echo request** (inviato dal mittente)
  - ◆ **Echo reply** (inviato in risposta dal destinatario)
- Questi messaggi sono importanti per capire il motivo di errori di connettività e vengono utilizzati dal comando ping
- Un altro comando che usa ICMP è **traceroute**

# ICMP



---

## Protocollo ICMP

- Laboratorio: analisi informational messages di ICMP tramite Ethereal (ping)

# Natting



---

## Nat (Network Address Translation)

- Indirizzi privati (**non utilizzabili su Internet**) usati nelle LAN
  - da 10.0.0.0 a 10.255.255.255
  - da 172.16.0.0 a 172.31.255.255
  - da 192.168.0.0 a 192.168.255.255
- Una LAN con indirizzi privati si può collegare ad Internet tramite un router che effettui il **natting** ossia sostituisca l'indirizzo IP **mittente** privato con uno pubblico (**Basic Nat**)
- Alla ricezione della risposta sulla scheda di rete ogni indirizzo IP destinatario viene rimappato in quello privato originario, basandosi sul numero di porta mittente
- **PAT**: il mapping interessa sia gli indirizzi IP che le porte

# Natting

## Nat

### Vantaggi

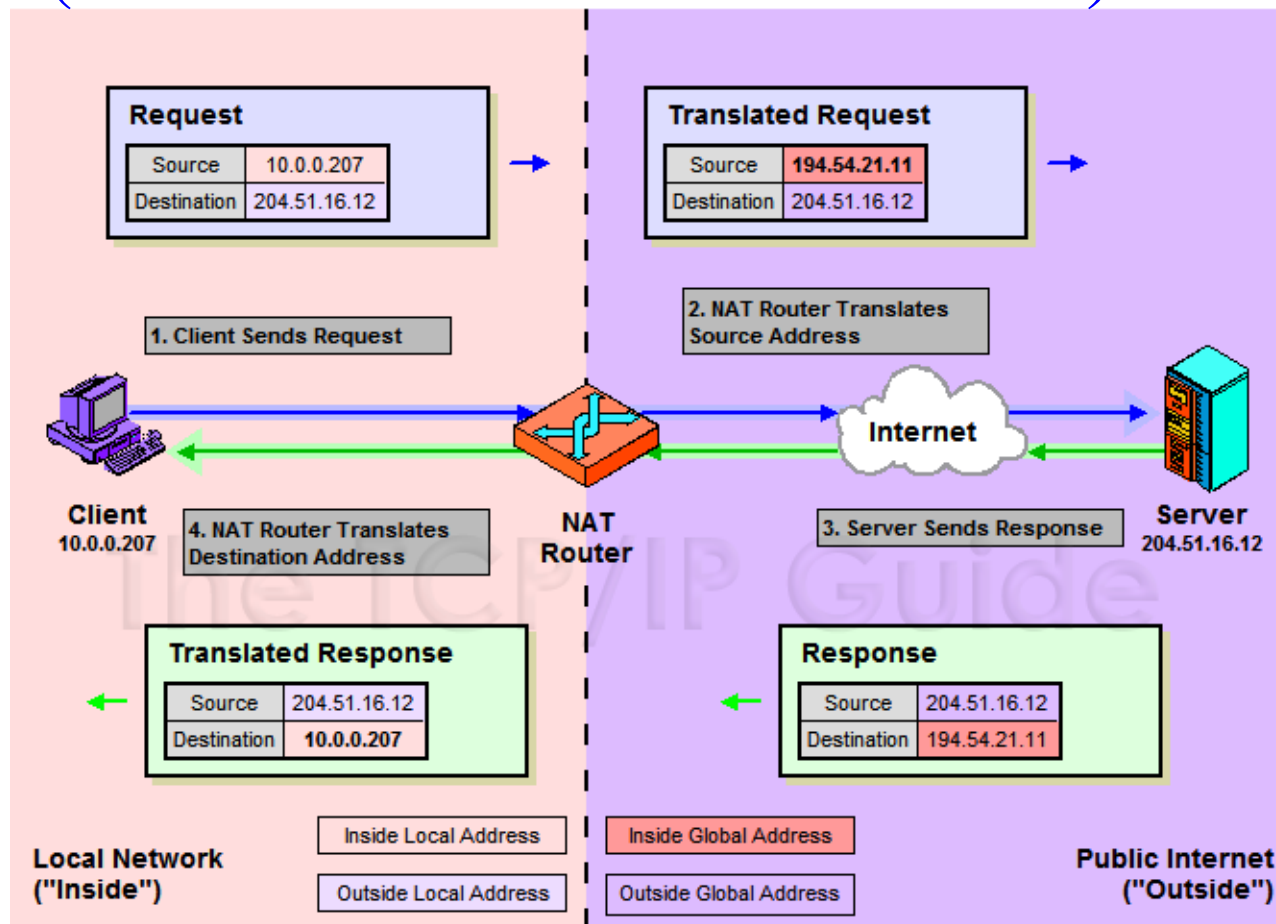
- Riduzione del numero di indirizzi pubblici utilizzati
- Maggior facilità nel cambio di ISP
- Maggior sicurezza (Indirizzi privati non visibili su Internet)

### Svantaggi

- Potenziali problemi di funzionamento con alcuni protocolli (es. IPSEC)
- Maggior complessità di gestione
- Performance

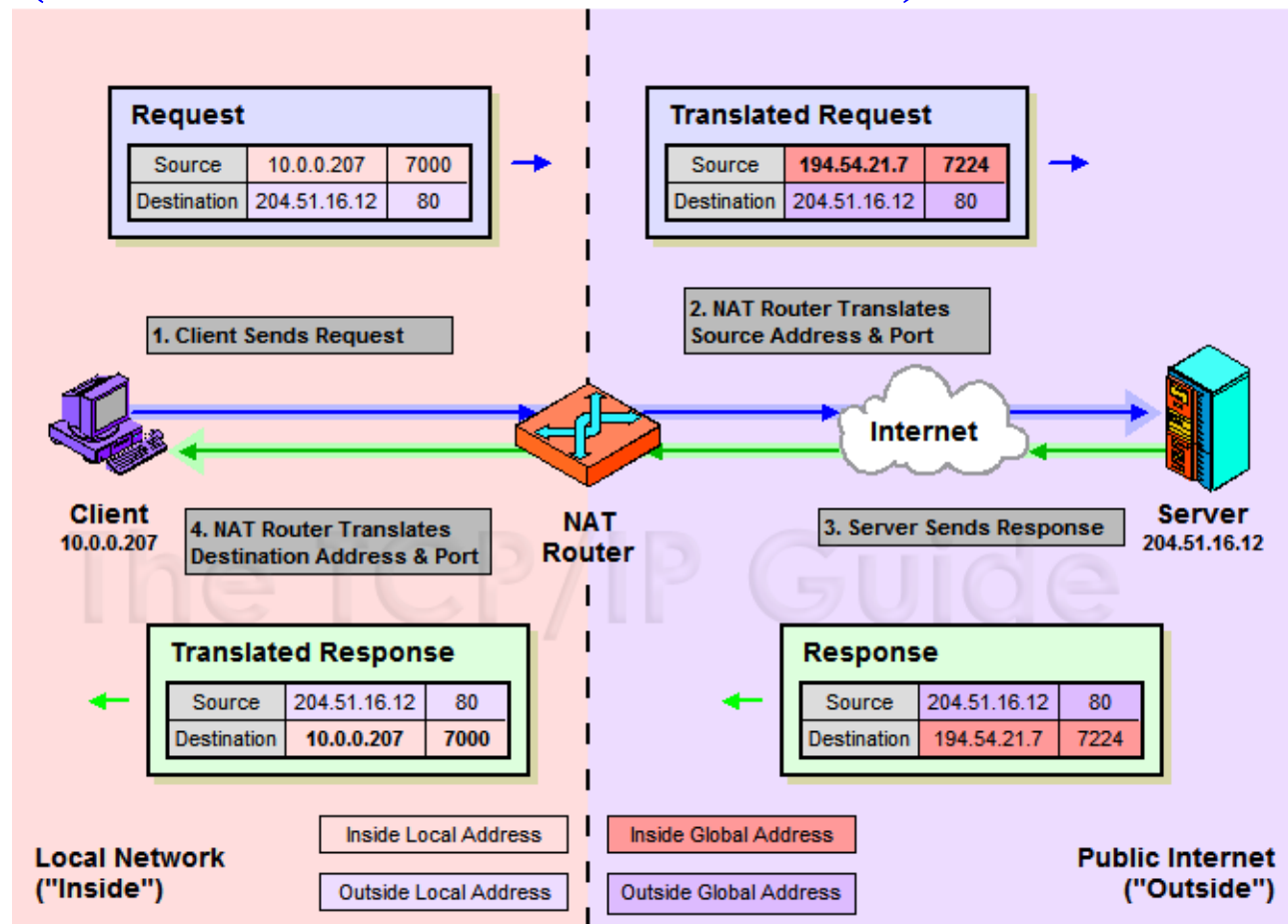
# Natting

## Nat (Network Address Translation)



# Natting

## PAT (Port Address Translation)



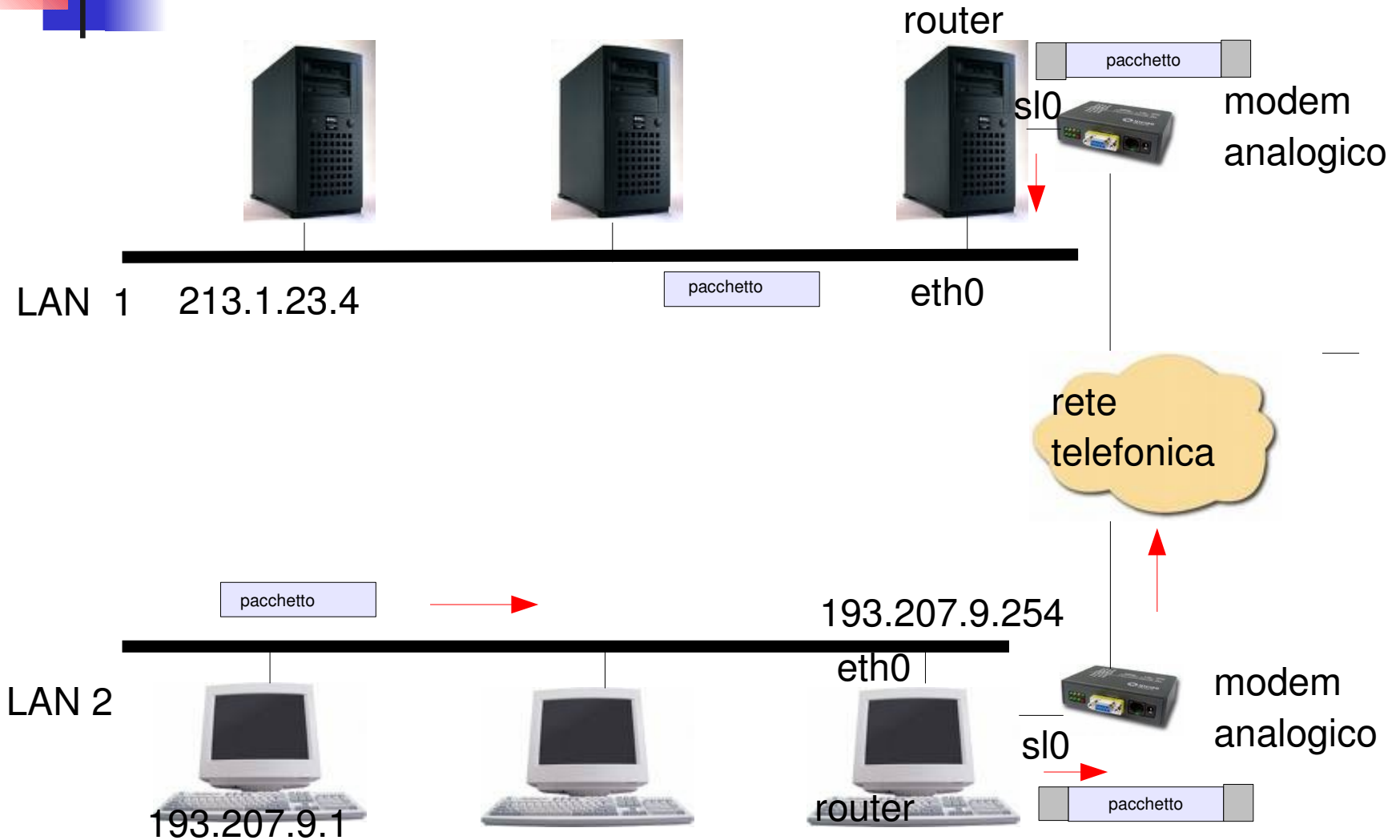


# Slip

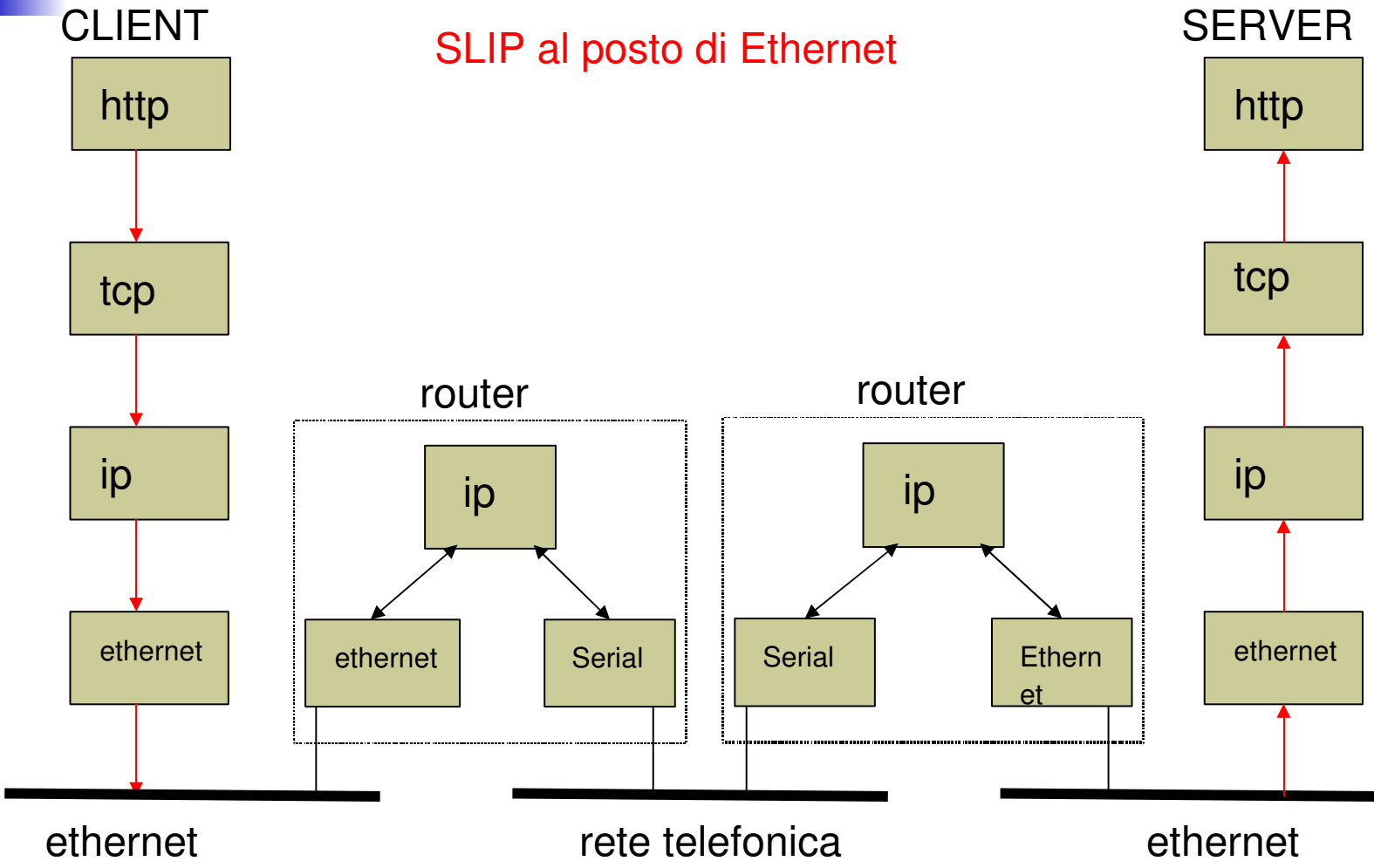
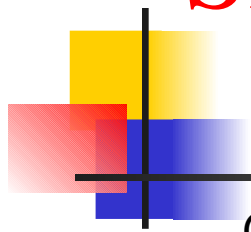
---

- Protocollo originariamente (1984) utilizzato per la connessione ad ISP su linea seriale (doppino telefonico) quando non era ancora disponibile PPP
- Incapsula in uno specifico frame gli IP datagram che vengono trasmessi sequenzialmente sulla linea seriale
- Ogni frame è formato aggiungendo il carattere Ascii END (0xc0) in testa ad ogni IP datagram

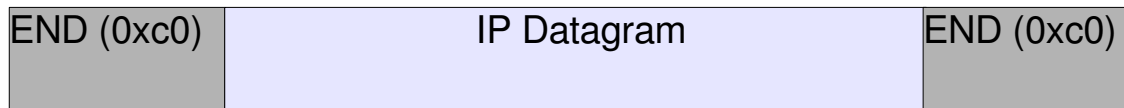
# Slip



# Slip

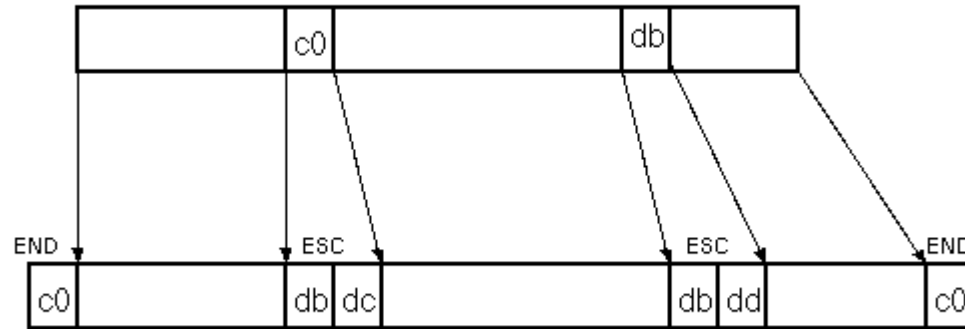


# Slip



Frame Slip: ogni IP datagram è preceduto da un carattere separatore

# Slip



Se un byte interno del datagramma e' `0xc0`, e' sostituito dalla coppia di bytes `0xdb 0xdc`. Il carattere `0xdb` viene chiamato ESC.

Se un byte interno del datagramma e' `0xdb`, e' sostituito dalla coppia di byte `0xdb 0xdd`.



# Slip

---

- Può essere utilizzato solo per incapsulare IP datagram
- E' necessario conoscere a priori l'indirizzo IP del destinatario (no ARP)
- No checksum
- I frame vengono spediti immediatamente senza alcun protocollo di negoziazione di parametri
- Semplice, di facile implementazione ma ora in disuso
- Esiste anche una versione compressa (CSLIP)



# PPP

---

- Consente, analogamente a Slip, la trasmissione di IP datagram su linea seriale ma in modo più flessibile
- Consente di spedire anche pacchetti di protocolli diversi da quelli Ip
- La connessione PPP avviene in diversi step
- Come primo step si attiva la connessione a livello fisico inviando al modem collegato gli opportuni **comandi AT** (es ATZ, ATDT0461944444)
- Effettuata la connessione a livello fisico, PPP attiva uno specifico protocollo (**Link Control Protocol**) che consente la **negoiazione** di vari parametri di connessione (es. MTU)



# PPP

---

- Due ulteriori protocolli, denominati **Network Control Protocol** ed **IP Control Protocol**, consentono a PPP la negoziazione di parametri specifici per IP (es. indirizzi IP)
- In funzione di ulteriori parametri richiesti per la connessione, PPP attiva ulteriori protocolli come ad esempio
  - **CCP** (Compression Control Protocol) per negoziare i parametri di compressione
  - **PAP** (Password Authentication Protocol) per eseguire l'autenticazione dell'utente
  - In alternativa a PAP si può usare **CHAP** (Challenge Authentication Protocol) che evita l'invio della password (si basa sulla verifica di eguaglianza di un valore di hash)



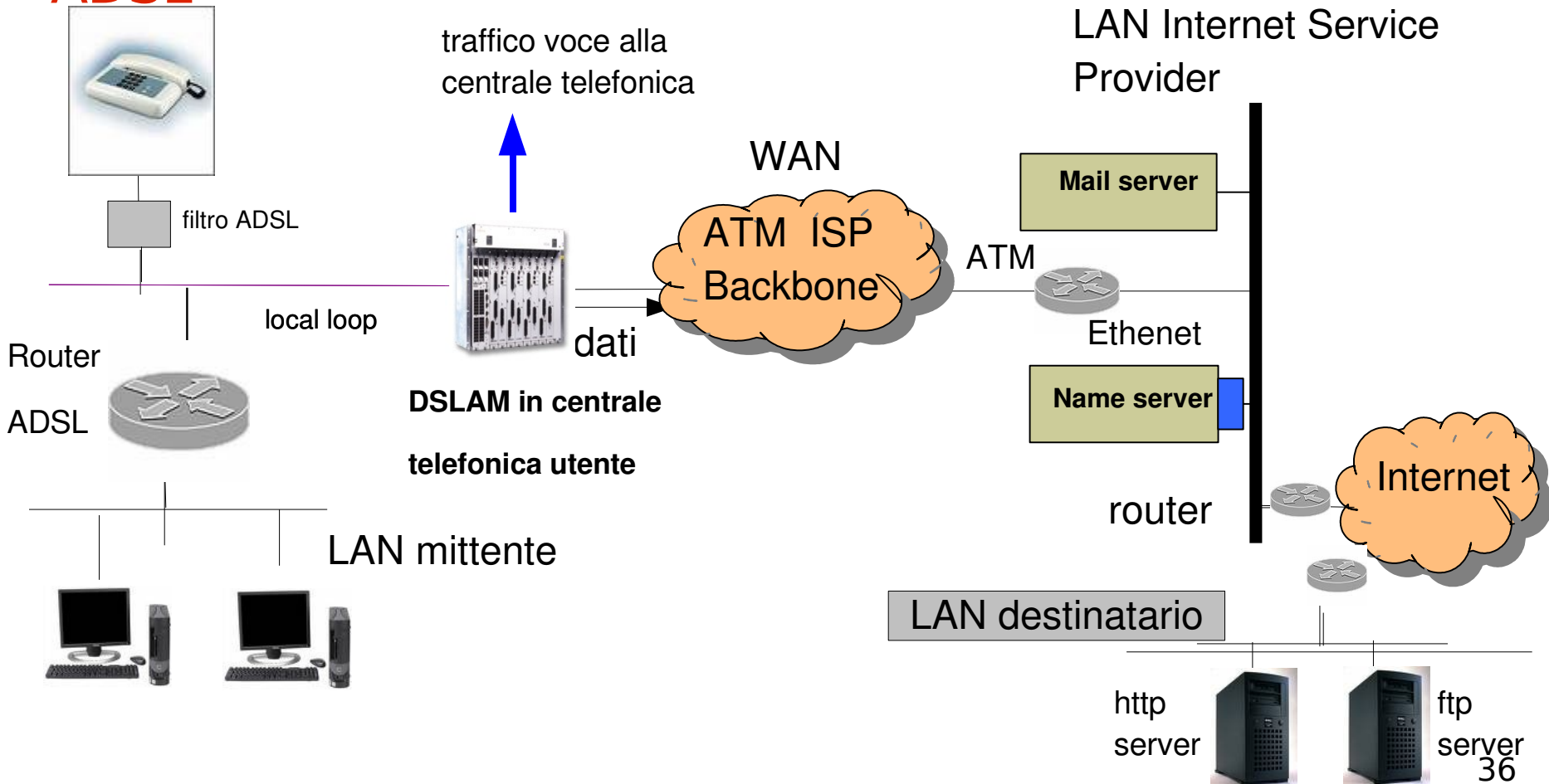
# PPP

---

- Protocollo molto usato nelle due varianti PPPOA (PPP over ATM) e PPPOE (PPP over Ethernet) per la connessione via ADSL ad ISP, a seconda che quest'ultimo raccolta i pacchetti da DSLAM attraverso una rete ATM od Ethernet
- PPP consente ad ISP di implementare importanti funzioni quali l'autenticazione (via PAP o CHAP) e l'assegnazione automatica di indirizzi IP

# PPP

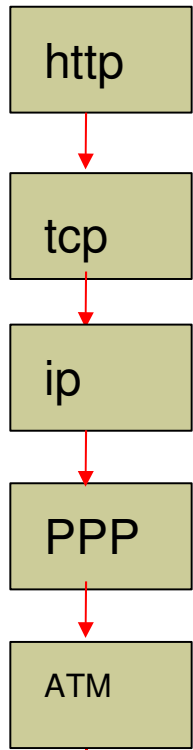
## ADSL



# PPP

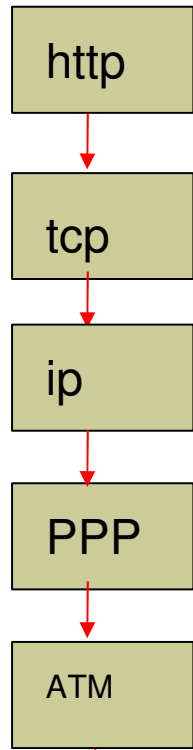
## PPP over ATM

CLIENT



} Layer 1,2

SERVER

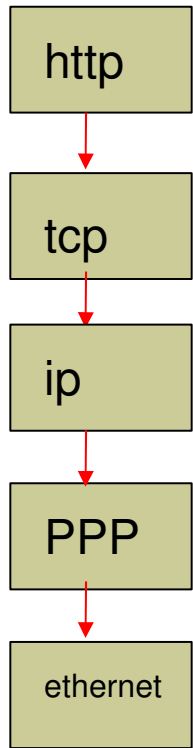


Backbone ATM

# PPP

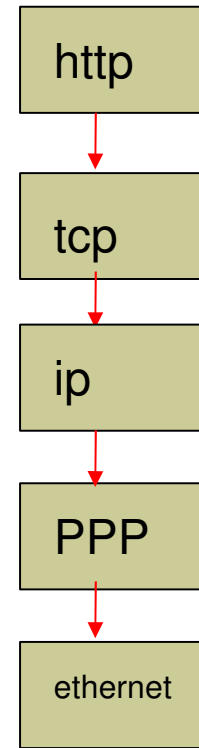
## PPP over Ethernet

CLIENT



Layer 1,2

SERVER



Backbone ETHERNET

# PPP



Frame PPP che incapsula un IP datagram



Frame PPP usato da LCP



Frame PPP usato da NCP

# PPP

## PPP

no modem

nessuna  
autorizzazione

```
pppd /dev/ttyS0 115200 local noauth debug  
192.168.92.1:192.168.92.2 nodetach
```

using channel 4

Using interface ppp0

Connect: ppp0 <-> /dev/ttyS0

rcvd [LCP ConfReq id=0x1 <asynctest 0x0> <magic 0x5cb47b57> <pcomp> <accomp>]

sent [LCP ConfReq id=0x1 <mru 1524> <asynctest 0x0> <magic 0x954e795e> <pcomp> <accomp>]

sent [LCP ConfAck id=0x1 <asynctest 0x0> <magic 0x5cb47b57> <pcomp> <accomp>]

rcvd [LCP ConfAck id=0x1 <mru 1524> <asynctest 0x0> <magic 0x954e795e> <pcomp> <accomp>]

sent [LCP EchoReq id=0x0 magic=0x954e795e]

sent [CCP ConfReq id=0x1 <deflate 15> <deflate(old#) 15> <bsd v1 15>]

sent [IPCP ConfReq id=0x1 <compress VJ 0f 01> <addr 192.168.92.1>]

rcvd [LCP EchoReq id=0x0 magic=0x5cb47b57]

sent [LCP EchoRep id=0x0 magic=0x954e795e]

rcvd [CCP ConfReq id=0x1 <deflate 15> <deflate(old#) 15> <bsd v1 15>]

sent [CCP ConfAck id=0x1 <deflate 15> <deflate(old#) 15> <bsd v1 15>]

rcvd [IPCP ConfReq id=0x1 <compress VJ 0f 01> <addr 192.168.92.2>]



# PPP

---

## PPP

sent [IPCP ConfAck id=0x1 <compress VJ 0f 01> <addr 192.168.92.2>]

rcvd [LCP EchoRep id=0x0 magic=0x5cb47b57]

rcvd [CCP ConfAck id=0x1 <deflate 15> <deflate(old#) 15> <bsd v1 15>]

Deflate (15) compression enabled

rcvd [IPCP ConfAck id=0x1 <compress VJ 0f 01> <addr 192.168.92.1>]

Cannot determine ethernet address for proxy ARP

local IP address 192.168.92.1

remote IP address 192.168.92.2

Script /etc/ppp/ip-up started (pid 9217)

Script /etc/ppp/ip-up finished (pid 9217), status = 0x0