

CCNA_1 (Versione 3.1) Networking basics

Cap. 9 Protocollo TCP/IP & Indirizzamento IP

ithum

Marco Ciampi
m.ciampi@ithum.it



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Ithum Learning License

Licenza d'uso del materiale didattico

Questo documento e tutto il materiale prodotto da Ithum S.r.l. e dai suoi collaboratori in qualità di autori originari costituisce una “opera” intellettuale protetta dal diritto d'autore e/o dalle altre leggi applicabili.

Tale opera (si veda anche l'appendice *Materiale allegato*) è messa a disposizione sulla base dei termini della presente *Ithum Learning License* ovvero della *Licenza concessa da Ithum Srl per l'utilizzo del materiale prodotto*.

È proibita ogni utilizzazione dell'opera che non sia autorizzata ai sensi della presente licenza o del diritto d'autore.

Ithum Srl e gli autori originari, in qualità di licenzianti, concedono l'utilizzo dell'opera con i diritti ed i doveri di seguito elencati.

Con il semplice esercizio sull'opera di uno qualunque dei diritti di seguito elencati, si accetta e ci si impegna a rispettare integralmente ed a far rispettare a terzi i termini e le condizioni della presente licenza.

L'opera può essere riutilizzata così come è oppure riadattata alle proprie esigenze come specificato da quanto segue.

Ithum S.r.l. e gli autori originari concedono:

- L'utilizzo dell'opera per fini educativi ed informativi personali;
- La riproduzione, distribuzione, comunicazione e/o esposizione in pubblico, rappresentazione, esecuzione o recitazione dell'opera;
- La creazione di opere derivate;

Alle seguenti imprescindibili condizioni:

1. riconoscere sempre e comunque il contributo di Ithum S.r.l. e dell'autore originario, dandone sempre evidenza scritta o comunque documentabile;
2. tener traccia sempre e comunque dei soggetti cui l'opera viene distribuita e comunicarla tempestivamente ad Ithum ed all'autore originario;
3. chiarire e far sottoscrivere agli altri sempre e comunque, in occasione di ogni atto di utilizzo o distribuzione, i termini della presente licenza;
4. contattare preventivamente sempre Ithum S.r.l. e l'autore originario per negoziarne coinvolgimento e compensi in caso di utilizzo ai fini commerciali;
5. Se si ottiene il permesso documentato dal titolare del diritto d'autore (Ithum S.r.l. e l'autore originario) è possibile rinunciare ad alcune o tutte le precedenti condizioni.

Le utilizzazioni libere e gli altri diritti non sono in nessun modo limitate da quanto sopra.

Per qualsiasi informazione è possibile scrivere a formazione@ithum.it.



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Contenuti

- **Introduction to TCP/IP**
 1. History and future of TCP/IP
 2. Application layer
 3. Transport layer
 4. Internet layer
 5. Network access layer
 6. Comparing the OSI model and the TCP/IP model
 7. Internet architecture
- **Internet Addresses**
 1. IP addressing
 2. Decimal and binary conversion
 3. IPv4 addressing
 4. Class A, B, C, D, and E IP addresses
 5. Reserved IP addresses
 6. Public and private IP addresses
 7. Introduction to subnetting
 8. IPv4 versus IPv6
- **Obtaining an IP Address**
 1. Obtaining an Internet address
 2. Static assignment of an IP address
 3. RARP IP address assignment
 4. BOOTP IP address assignment
 5. DHCP IP address management
 6. Problems in address resolution
 7. Address Resolution Protocol (ARP)



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Obiettivi

- Sviluppo di Internet e del protocollo TCP/IP
- I 4 strati del modello TCP/IP e le loro funzioni
- Confronto tra modello OSI e TCP/IP
- Funzionamento e struttura dell'indirizzamento IP
- Necessità del Subnetting
- Differenze tra indirizzamento pubblico e privato
- Funzioni degli indirizzi IP riservati
- Assegnazione statica degli indirizzi
- Assegnazione dinamica degli indirizzi con RARP, BootP e DHCP
- Utilizzo di ARP per ottenere gli Indirizzi MAC

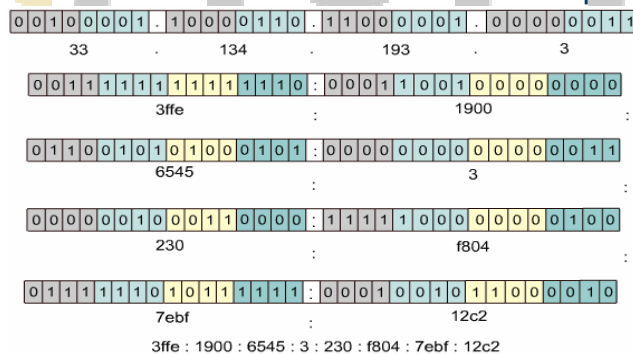


Cap. 9 Protocollo TCP/IP & Indirizzamento IP

TCP/IP

Lo stack protocollare TCP/IP:

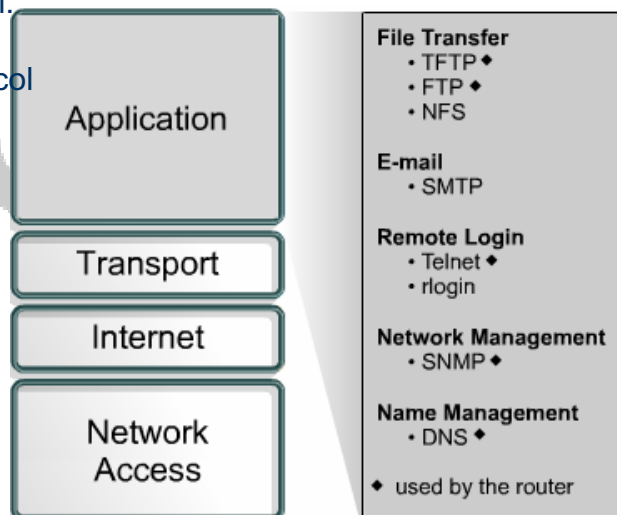
- Nasce per richiesta del DoD che intendeva poter creare una rete in grado di funzionare in qualsiasi tipo di situazione
- È divenuto lo standard di riferimento per Internet
- Non confondere i Layer del modello TCP/IP con quelli del modello OSI, anche se hanno la medesima nomenclatura
- Standard internazionale dal 1981
- Gli indirizzi IP nella versione 4 sono di 32 bit, scritti nella versione dotted decimal; nella versione 6 sono di 128 bit, e sono scritti in esadecimale e i blocchi da 16 bit sono separati da i due punti



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

L'Application Layer

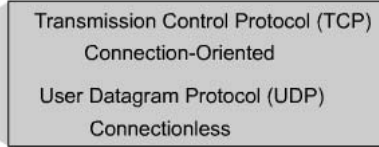
- L'application layer del modello TCP/IP gestisce protocolli di alto livello
- Verifica che i dati siano impacchettati nella maniera corretta prima di passarli ad un altro strato
- Include specifiche per supportare trasferimento di file, e-mail, accesso (e login) da remoto ed altre applicazioni:
 - FTP: file transfer protocol
 - TFTP: trivial file transfer protocol
 - NFS: network file system
 - SMTP:
 - Telnet
 - SNMP:
 - DNS:



Il Transport Layer



- Fornisce il servizio di trasporto dall'host sorgente a quello di destinazione
- E' la connessione logica tra 2 utenti finali della rete
- I protocolli di trasporto segmentano e riassemblano le applicazioni degli strati più alti in un flusso di dati che fornisce servizi di trasporto end-to-end
- Quando si usa TCP, il compito primario del layer di trasporto è il controllo end-to-end mediante le Sliding Windows, gli Acknowledgment e l'affidabilità dei numeri di sequenza (SN)



Servizi offerti:

TCP e UDP:

- Segmentazione dei dati provenienti dalle applicazioni di strati superiori
- Spedizione dei segmenti da un device all'altro

SOLO TCP:

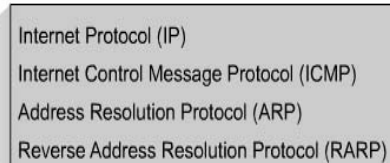
- Stabilire operazioni end-to-end
- Flow-control grazie alle sliding window
- Affidabilità mediante Ack ed SN



Internet Layer



- Ha lo scopo di individuare il miglior percorso attraverso la rete su cui far viaggiare i pacchetti e di fare **Packet Switching**
- Il protocollo più noto è IP



IP fornisce un servizio **Connectionless, Best Effort** di recapito dei pacchetti: definisce il pacchetto e lo schema di indirizzamento, trasferisce i dati tra Internet Layer e Network Access, instrada i pacchetti verso gli host remoti)

- **ICMP** (Internet Control Message Protocol): controllo ed aggiornamento tramite messaging
- IP è un protocollo inaffidabile nel senso che non compie correzioni e controllo di errori, lasciandoli ai protocolli di strato superiori; (non perché non recapiti correttamente i dati)



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Il Network Access Layer



- Detto anche host-to-network layer
- Si preoccupa di tutto ciò che serve ad un pacchetto IP per poter passare attraverso un link fisico sul mezzo della rete
- Definisce le procedure per interfacciarsi con l'hardware della rete e per accedere al mezzo di trasmissione
- SLIP (Serial Line Internet Protocol) e il Point-to-Point Protocol sono i protocolli che consentono accesso tramite la connessione via modem

- Ethernet
- Fast Ethernet
- SLIP & PPP
- FDDI
- ATM, Frame Relay & SMDS
- ARP
- Proxy ARP
- RARP

- Include funzioni di mappatura degli IP Address con gli indirizzi fisici (MAC) e di incapsulamento dei pacchetti IP in frame
- ARP: determina gli indirizzi MAC una volta noti quelli IP
- RARP: determina gli indirizzi IP una volta noti quelli MAC



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

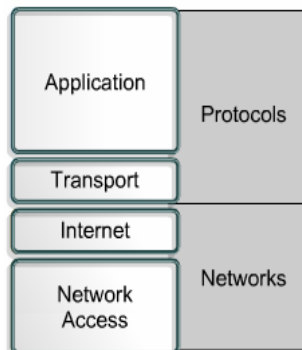
Paragone tra il modello OSI e la pila protocollare TCP/IP

Compariamo i modelli OSI e TCP/IP, individuando le differenze e le similitudini:

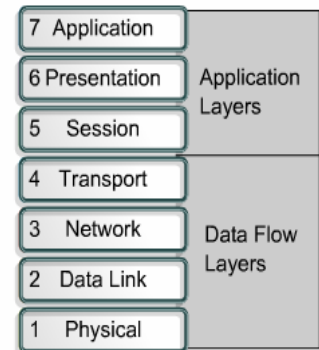
Similitudini

- Hanno una struttura a layer
- Hanno l'Application Layer, pur implementando servizi differenti
- Hanno Layer di Trasporto e di Network paragonabili
- Si assume l'uso di tecnologie packet-switched
- I professionisti delle reti devono conoscerli entrambi

TCP/IP Model



OSI Model



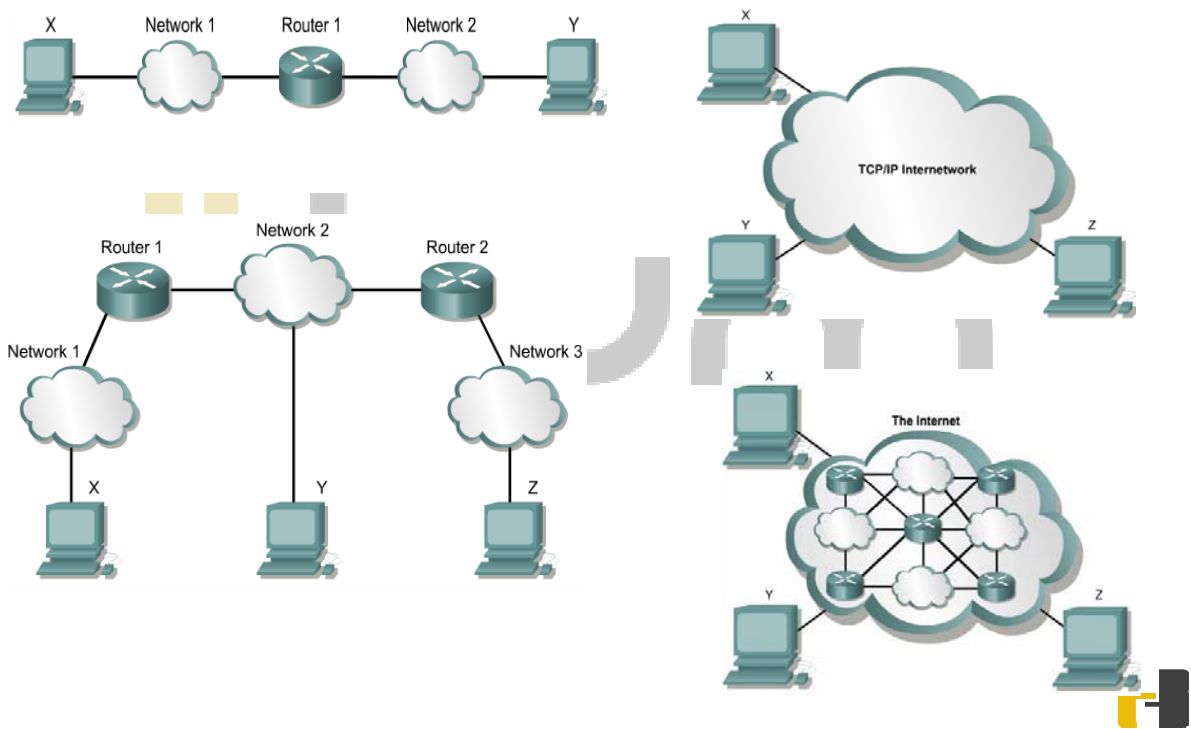
Differenze

- Il TCP/IP riunisce in alcuni layer, più layer del modello OSI
- Più semplice perché con meno layer
- TCP/IP ha credibilità grazie ai suoi protocolli



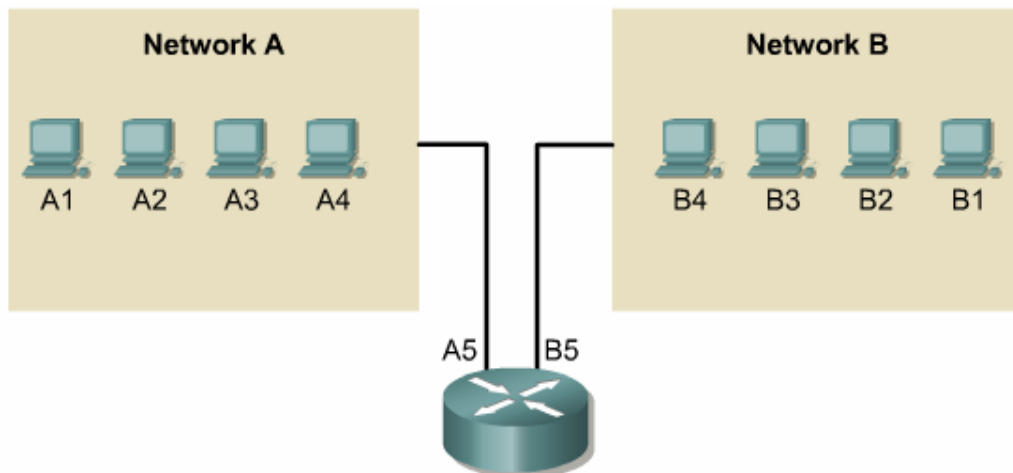
Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Architettura di Internet



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Indirizzamento IP



Binary : 11000000.10101000.00000001.00001000 and 11000000.10101000.00000001.00001001
Decimal : 192.168.1.8 and 192.168.1.9



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Conversione da Decimale a Binario – Primo metodo

128	207
	128
64	79
	64
8	15
	8
4	7
	4
2	3
	2
1	1

Position	8	7	6	5	4	3	2	1
Value	128	64	32	16	8	4	2	1

Position	8	7	6	5	4	3	2	1
Value	128	64	32	16	8	4	2	1
	1	1	0	0	1	1	1	1
	128	64			8	4	2	1

= 207



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Conversione da Decimale a Binario – Secondo metodo

1. Si prende il numero decimale
2. Si divide per 2 e si considera il resto di tale divisione, finché non rimane 0 oppure 1, e questa sarà l'ultima cifra binaria del numero in base 2 considerato
3. Si considera questo numero in base 2 leggendolo "al contrario"



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Conversione da Binario a Decimale

1. Si prende il numero binario
2. Si sommano i valori delle potenze di due che sono presenti, ovvero quelle che effettivamente sono moltiplicati per la cifra binaria 1 (ovviamente fosse uno zero....)

ithum



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

La rappresentazione dotted decimal

Attualmente gli indirizzi assegnati ai computer su Internet sono dei numeri binari da 32 bit.

Per rendere più facile lavorare con questi indirizzi, vengono proposti serie di numeri in base 10

Si prendono le 32 cifre binarie e si dividono in 4 gruppi da 8, si converte in decimale ciascun gruppo ed ecco la cosiddetta rappresentazione Dotted Decimal

Esempio:
10000000 01011101 00001111 10101010
200 114 6 51



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Indirizzamento IPv4

- Un router inoltra i pacchetti dalla rete sorgente a quella di destinazione usando il protocollo IP
- I pacchetti includono un identificativo per ciascuna rete. Il sistema di indirizzamento di IPv4 funziona come lo smistamento postale.
- Se la rete cui si deve recapitare è collegata al router, si analizza la parte di IP Address che identifica l'host.
- Se la rete non è collegata direttamente al router, instraderà i pacchetti spedendoli "all'ufficio postale di zona".
- Gli indirizzi sono disposti in modo gerarchico

IP Address Class	High Order Bits	First Octet Address Range	Number of Bits in the Network Address
Class A	0	0 - 127 *	8
Class B	10	128 - 191	16
Class C	110	192 - 223	24
Class D	1110	224 - 239	28

Address Class	Number of Networks	Number of Host per Network
A	126 *	16,777,216
B	16,384	65,535
C	2,097,152	254
D (Multicast)	N/A	N/A

* The 127.x.x.x address range is reserved as a loopback address, used for testing and diagnostic purposes.

- La classe D è stata creata per il Multicasting; un indirizzo multicast è un Network Address unico che direziona i pacchetti con tale indirizzo a un gruppo predefinito di indirizzi IP



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

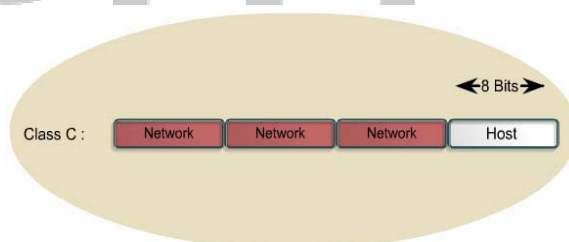
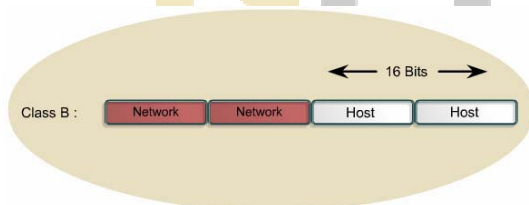
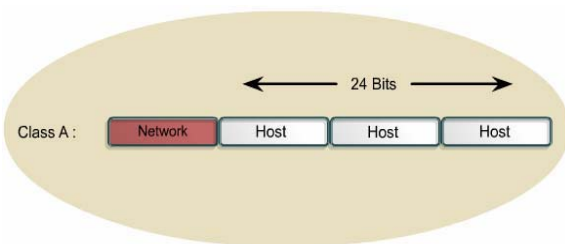
Gli indirizzi di tipo "classico"

Class A	Network	Host		
Octet	1	2	3	4

Class B	Network		Host	
Octet	1	2	3	4

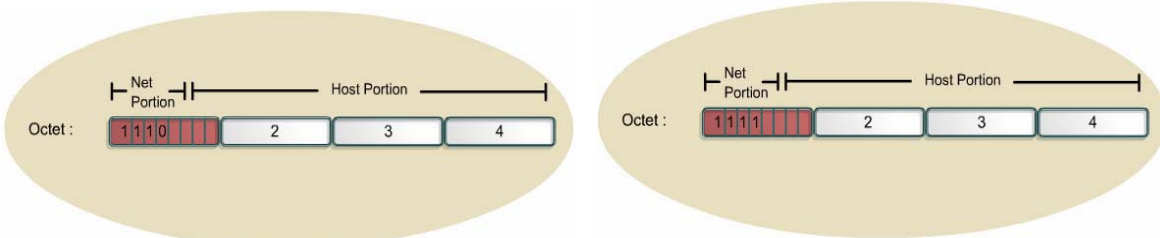
Class C	Network			Host
Octet	1	2	3	4

Class D	Host			
Octet	1	2	3	4



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Classe D e classe E



- Esistono anche queste classi di indirizzi.
- Della classe D abbiamo già detto (Multicasting)
- La classe E è un insieme di indirizzi che l' Internet Engineering Task Force (IETF) riserva per le proprie ricerche.

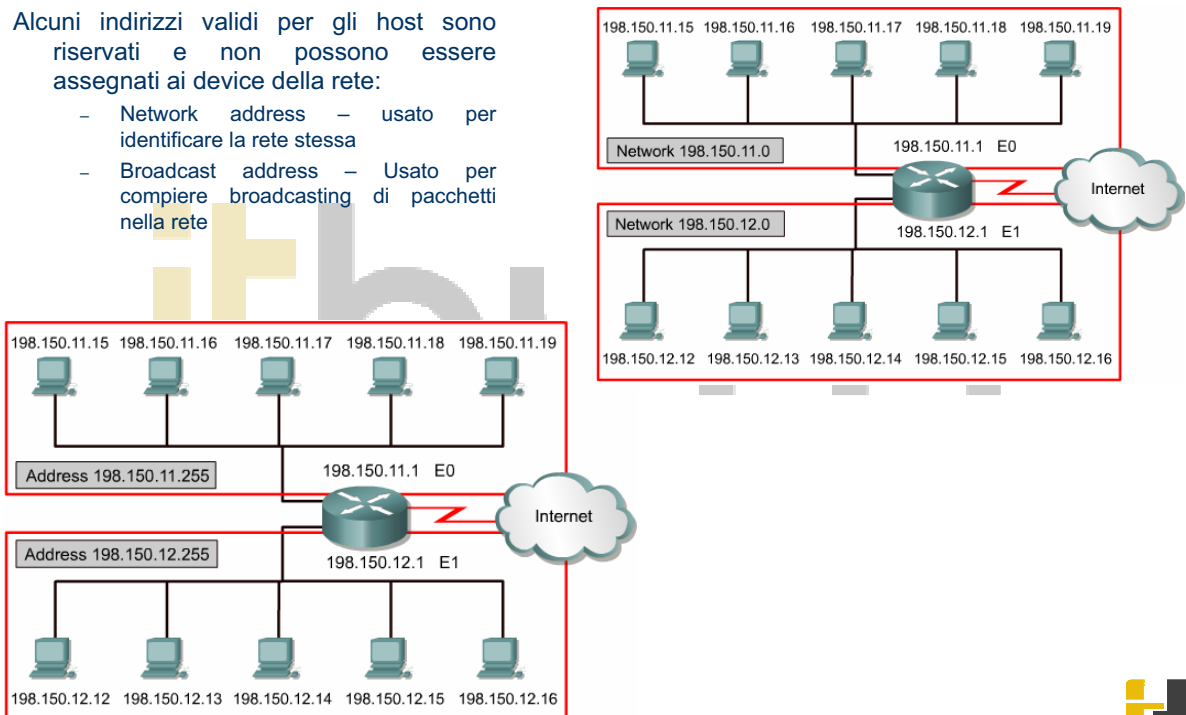
IP address class	IP address range (First Octet Decimal Value)
Class A	1-126 (00000001-01111110) *
Class B	128-191 (10000000-10111111)
Class C	192-223 (11000000-11011111)
Class D	224-239 (11100000-11101111)
Class E	240-255 (11110000-11111111)

Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Indirizzi IP riservati

Alcuni indirizzi validi per gli host sono riservati e non possono essere assegnati ai device della rete:

- Network address - usato per identificare la rete stessa
- Broadcast address - Usato per compiere broadcasting di pacchetti nella rete



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Indirizzi IP pubblici e privati

- La stabilità di Internet dipende direttamente dalla unicità degli indirizzi pubblici usati (problemi di vario tipo, primo fra tutti impossibilità di capire a chi recapitare)

Class	RFC 1918 internal address range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255

- Internet Network Information Center (InterNIC), soppiantata da Internet Assigned Numbers Authority (IANA), gestiva la procedura con cui si verificava l'unicità degli indirizzi pubblici in rete
- Un utente può ottenere indirizzi pubblici a sue spese o da un ISP
- Una soluzione alla penuria di indirizzi pubblici sono quelli privati, definiti nell'RFC1918, per la classe A, parte della B e della C. (reti aziendali non connesse)
- Gli indirizzi appartenenti a tali gruppi non sono instradati nelle backbone, i router li scartano subito



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Subnetting

- Subnetting è un metodo di gestire gli indirizzi IP, che ha prevenuto il completo esaurimento degli indirizzi IP
- Il subnetting è estremamente importante da capire per l'amministrazione di rete, poiché permette di dividere ed identificare reti separate all'interno della stessa LAN
- Subnetting una rete significa usare la subnet mask per dividere la rete e renderla ben più efficiente e gestibile
- E' importante sapere quante subnet o reti sono necessarie e quanti host saranno richiesti in ogni rete
- Col subnetting il network non è limitato alle classi di indirizzamento di default A, B e C, ed inoltre anche le network mask saranno non quelle standard
- Per subnetting si devono prendere in prestito dei bit dal campo degli host (minimo 2, al massimo tutti tranne 2)



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Subnet Mask

- Determina quale parte dell'indirizzo IP è il campo relativo alla rete e quale è la parte relativa all'host. Per determinare la subnet mask seguire i seguenti passi:
 - 1. Esprimere l'indirizzo IP in forma binaria.
 - 2. Rimpiazzare la porzione della rete (ed eventuale sottorete) con tutti 1.
 - 3. Rimpiazzare la porzione dell'host con tutti 0.
 - 4. Convertire l'espressione binaria di nuovo nella notazione dotted-decimal.



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Subnet Mask

11111111.11111111.11110000.00000000

Class B Network
16 bits for the Network
4 bits for the Subnetwork
12 bits for the Host

Subnet mask in decimal = 255.255.240.0

- ◆ 32 bits long
- ◆ Divided into four octets
- ◆ Network and subnet portions all 1's
- ◆ Host portion all 0's



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Schema riassuntivo del subnetting

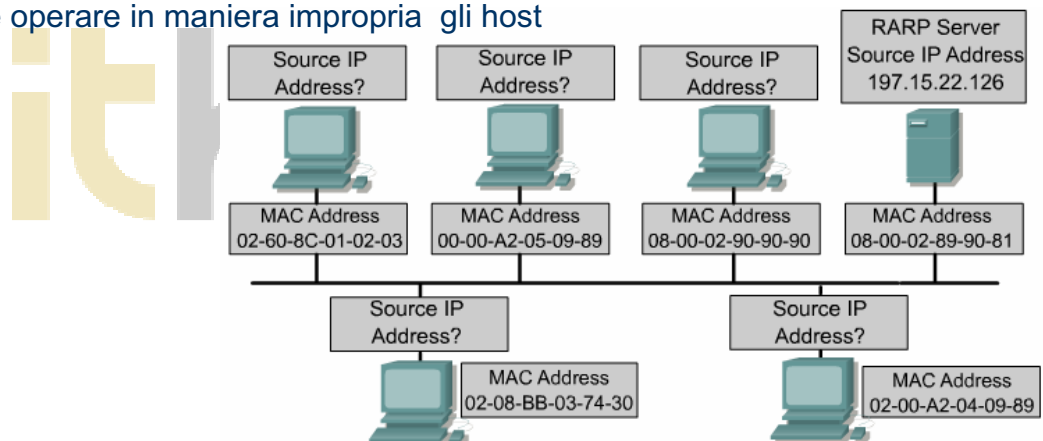
Decimal notation for first Host octet	Number of Subnets	Number of Class A Hosts per Subnet	Number of Class B Hosts per Subnet	Number of Class C Hosts per Subnet
.192	2	4,194,302	16,382	62
.224	6	2,097,150	8,190	30
.240	14	1,048,574	4,094	14
.248	30	524,286	2,046	6
.252	62	262,142	1,022	2
.254	126	131,070	510	-
.255	254	65,534	254	-



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Come si ottiene un indirizzo IP?

- L'assegnazione IP può avvenire in due modi: dinamica o statica.
- La versione dinamica ha tre varianti diverse
- A prescindere dallo schema di indirizzamento scelto non possono esserci due interfacce che abbiano lo stesso indirizzo IP; ciò porterebbe a dei conflitti e farebbe operare in maniera impropria gli host



The hosts have a physical address by having a network interface card that allows connection to the physical medium. IP addresses have to be assigned to the host in some method. The two methods of IP address assignment are static or dynamic.

Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Assegnazione statica

- Funziona bene in reti piccole e che cambiano poco frequentemente
- L'amministratore di rete assegna manualmente gli indirizzi IP per ogni computer, stampante, server dell'intranet
- È fondamentale mantenere dei record aggiornati e corretti per tracciare ed evitare errori (facile quando ci sono pochi device)
- Ai server è bene assegnare indirizzi IP in maniera statica in modo che le workstation e i vari device sappiano sempre dove andare per accedere ai servizi
- Oltre ai server è fondamentale dare indirizzi statici ai router, alle stampanti e ai vari server delle applicazioni



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Il protocollo ARP

- Serve per conoscere il MAC address, una volta noto l'indirizzo IP di destinazione
- Alcuni device mantengono delle tavole in cui si legano degli indirizzi IP ai rispettivi indirizzi MAC; sono dette ARP table (sono presenti nella RAM) e rarissimamente sono editate manualmente
- L'ARP table si può arricchire "sniffando" il traffico della rete e catturando le coppie di indirizzi che viaggiano nei pacchetti oppure facendo delle ARP request quando se ne ha bisogno (messaggio broadcast)
- Se il device con l'IP address in questione è sulla rete, risponde alla ARP request con una reply contenente IP-MAC; se non è sulla stessa rete non vi è risposta, e si riporta un errore



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Il protocollo ARP (2)

- Se la richiesta ARP è per un IP che appartiene ad una altra rete c'è un modo, ovvero il Proxy ARP
- Il router non instrada pacchetti broadcast, per cui (se la feature è presente ed attiva) risponde a chi ha fatto la richiesta con il MAC address dell'interfaccia cui è giunta la richiesta
- Un altro metodo è quello del gateway di default, ovvero una opzione nella configurazione di rete dell'host in cui si riporta l'indirizzo dell'interfaccia del router
- Se il default gateway non è attivato e non lo è neanche la caratteristica proxy ARP allora sul router il traffico dati non può lasciare la rete locale

Arp Table 198.150.11.36	
MAC	IP
FE:ED:F9:44:45:66	198.150.11.34
DD:EC:BC:00:04:AC	198.150.11.33
DD:EC:BC:00:94:D4	198.150.11.35
FE:ED:F9:23:44:EF	198.150.11.36



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

RARP (Reverse Address Resolution Protocol)

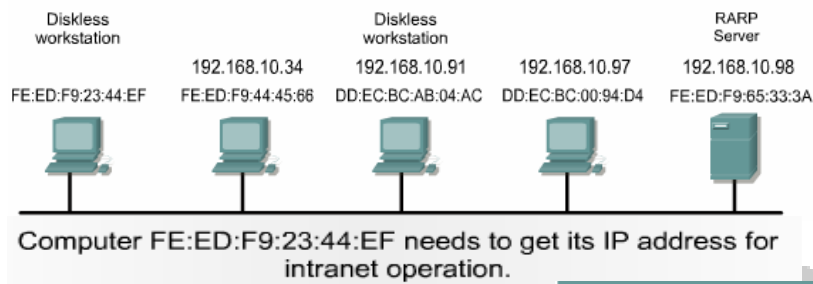
- Il RARP associa un indirizzo MAC ad un indirizzo IP, permettendo l'incapsulazione dei dati prima che siano spediti
- Una workstation diskless potrebbe conoscere il suo MAC address ma non l'IP; il RARP le permette di fare una richiesta per conoscere il suo IP
- Ci deve essere un server RARP nella rete per poter rispondere alla richiesta
- RARP usa lo stesso formato di pacchetto dell'ARP

0 - 15 bits		16 - 31 bits	
Hardware Type		Protocol Type	
HLen (1 byte)	PLen (1 byte)	Operation	
Sender HA (bytes 1 - 4)			
Sender HA (byte 5 - 6)		Sender PA (byte 1 - 2)	
Sender PA (byte 3 - 4)		Target HA (byte 1 - 2)	
Target HA (bytes 3 - 6)			
Target PA (bytes 1 - 4)			
RARP header structure			



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

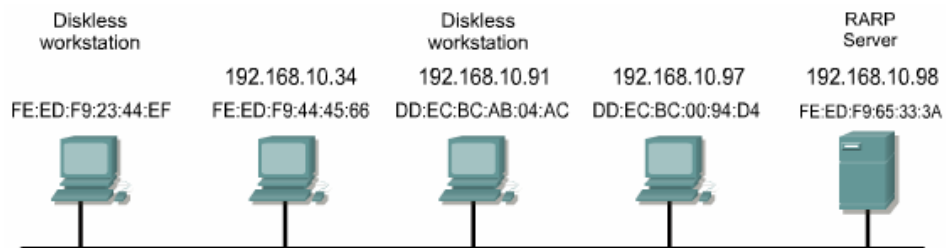
Il processo del RARP



Field	Description
Hardware Type	Specifies a hardware interface type for which the sender requires a response.
Protocol type	Specifies the type of high-level protocol address the sender has supplied.
HLen	Hardware address length.
PLen	Protocol address length.
Operation	The values are as follows: 1 ARP request. 2 ARP response. 3 RARP request. 4 RARP response. 5 Dynamic RARP request. 6 Dynamic RARP reply. 7 Dynamic RARP error. 8 InARP request. 9 InARP reply.

Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Il processo RARP (2)



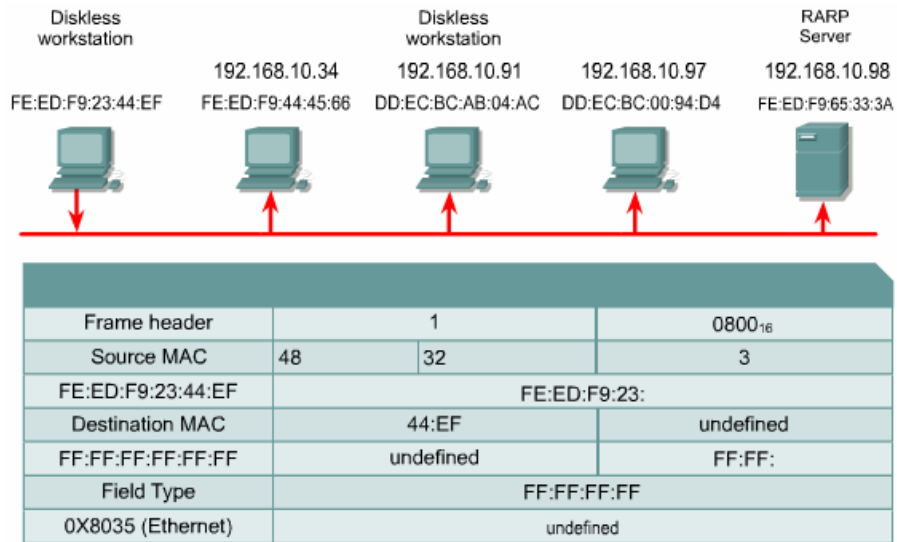
Frame header	1	0800 ₁₆
Source MAC	48	32
FE:ED:F9:23:44:EF	FE:ED:F9:23:	
Destination MAC	44:EF	undefined
FF:FF:FF:FF:FF:FF	undefined	FF:FF:
Field Type	FF:FF:FF:FF	
0X8035 (Ethernet)	undefined	

Computer FE:ED:F9:23:44:EF generates a RARP request.



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Il processo RARP (3)

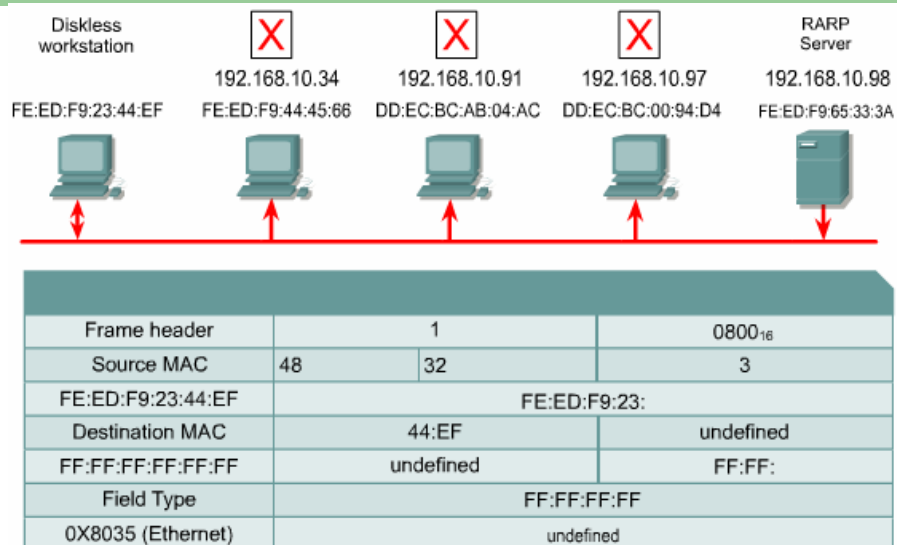


Il computer FE:ED:F9:23:44:EF trasmette la richiesta RARP



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Il processo RARP (4)

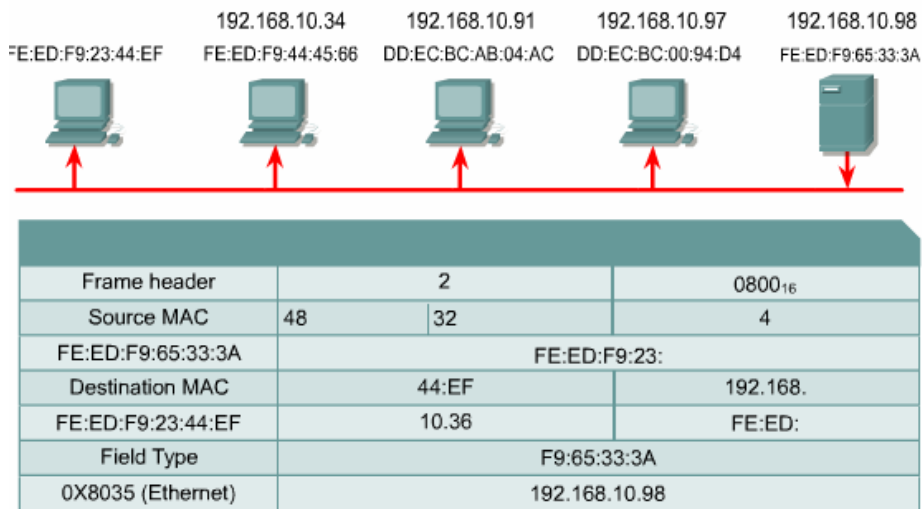


Tutti i computer prendono scartano il pacchetto tranne il RARP server, che riconosce il campo richiesta RARP.



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Il processo RARP (5)

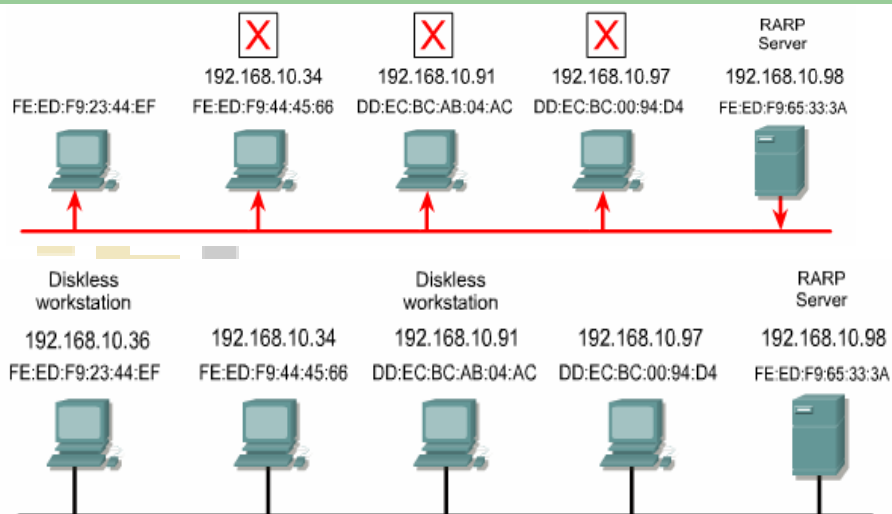


Il server RARP crea un pacchetto di risposta (RARP reply) e lo invia. Tutti i computer lo prendono e lo processano. Lo terrà solamente quello interessato, ovvero che ha il MAC address uguale al MAC di destinazione.



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Il processo RARP (6)



Il computer FE:ED:F9:23:44:EF immagazzina l'IP address ricevuto nella RARP reply in modo che lo possa usare in seguito.



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Il protocollo ARP

- Serve per conoscere il MAC address, una volta noto l'indirizzo IP di destinazione
- Alcuni device mantengono delle tavole in cui si legano degli indirizzi IP ai rispettivi indirizzi MAC; sono dette ARP table (sono presenti nella RAM) e rarissimamente sono editate manualmente
- L'ARP table si può arricchire "sniffando" il traffico della rete e carpendo le paia di indirizzi che necessariamente viaggiano nei pacchetti oppure facendo delle ARP request quando se ne ha bisogno (messaggio broadcast)
- Se il device con l'IP address in questione è sulla rete, risponde alla ARP request con una reply contenente IP-MAC; se non è sulla stessa rete non vi è risposta, e si riporta un errore



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Il protocollo ARP (2)

- Se la richiesta ARP è per un IP che appartiene ad una altra rete c'è un modo, ovvero il Proxy ARP
- Il router non instrada pacchetti broadcast, per cui (se la feature è presente ed attiva) risponde a chi ha fatto la richiesta con il MAC address dell'interfaccia cui è giunta la richiesta
- Un altro metodo è quello del gateway di default, ovvero una opzione nella configurazione di rete dell'host in cui si riporta l'indirizzo dell'interfaccia del router
- Se il default gateway non è attivato e non lo è neanche la caratteristica proxy ARP allora sul router il traffico dati non può lasciare la rete locale



Arp Table 198.150.11.36

MAC	IP
FE:ED:F9:44:45:66	198.150.11.34
DD:EC:BC:00:04:AC	198.150.11.33
DD:EC:BC:00:94:D4	198.150.11.35
FE:ED:F9:23:44:EF	198.150.11.36

Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Il BOOTP (Bootstrap protocol)

- Opera in ambienti client-server e richiede lo scambio di un solo pacchetto per avere delle informazioni IP
- Diversamente dal RARP il BOOTP ha un pacchetto che include l'indirizzo IP, l'indirizzo del router, di un server e informazioni specifiche sul fornitore
- Non è pensato per l'assegnazione dinamica degli indirizzi
- Con BOOTP l'amministratore deve creare dei file di configurazione che specifichino i parametri di ogni device, per cui se si aggiungono host, deve mantenere un database molto accurato
- Anche se l'assegnazione è "dinamica" c'è un rapporto uno a uno tra gli indirizzi ed il numero degli host
- Ci deve essere un BOOTP profile per ogni host con dentro un IP address assegnato
- BOOTP usa UDP per consegnare i messaggi
- La richiesta e la risposta BOOTP si mandano in broadcast



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

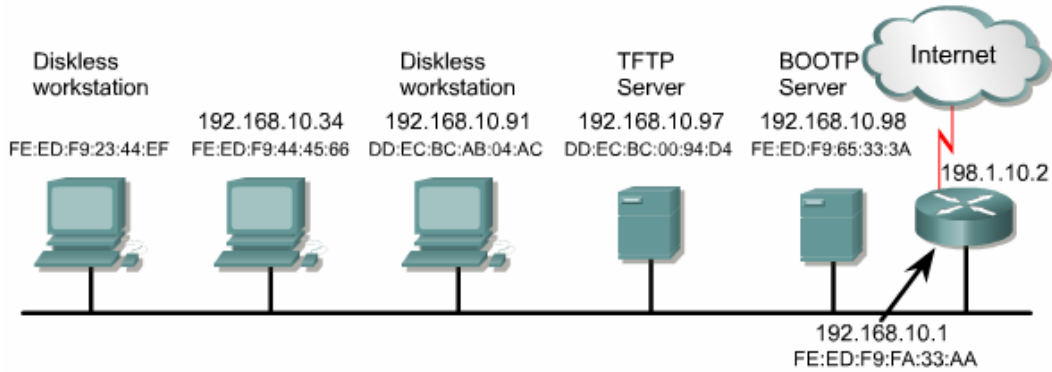
Struttura del messaggio BOOTP

0 - 7 bits	8 - 15 bits	16 - 23 bits	24 - 31 bits
Op (1)	Htype (1)	HLen (1)	Hops (1)
Xid (4bytes)			
Seconds (2 bytes)		Unused	
Ciaddr (4 bytes)			
Yiaddr (4 bytes)			
Siaddr (4 bytes)			
Giaddr (4bytes)			
Chaddr (16 bytes)			
Server Host Name (32 bytes)			
Boot File Name (64 bytes)			
Vendor Specific Area (32 bytes)			
BOOTP message structure			

Field	Description
Op	Message operation code. Messages can be either BOOTREQUEST or BOOTREPLY
Htype	Hardware address type
HLen	Hardware address length
Hops	Client places zero, this field is used by BOOTP server to send request to another network
Xid	Transaction ID
Secs	Seconds elapsed since the client began the address acquisition or renewal process
Ciaddr	Client IP address
Yiaddr	"Your" (client) IP address
Siaddr	IP address of the next server to use in bootstrap
Giaddr	Relay agent IP address used in booting via a relay agent
Chaddr	Client hardware address
Server Host Name	Specifies particular server to get BOOTP information from
Boot File Name	Allows for multiple boot files to be used allowing hosts to run different operating systems
Vendor Specific Area	Contains optional vendor specific information that can be passed to the host

Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Il processo BOOTP

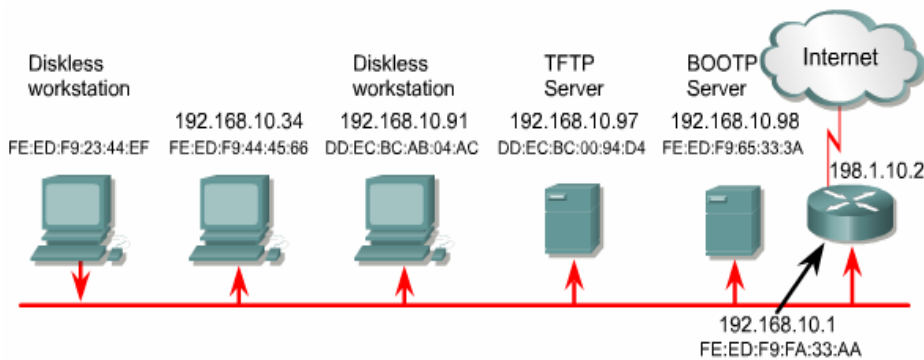


Computer FE:ED:F9:23:44:EF needs to obtain its IP address for Internet and intranet operation.



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Il processo BOOTP (2)

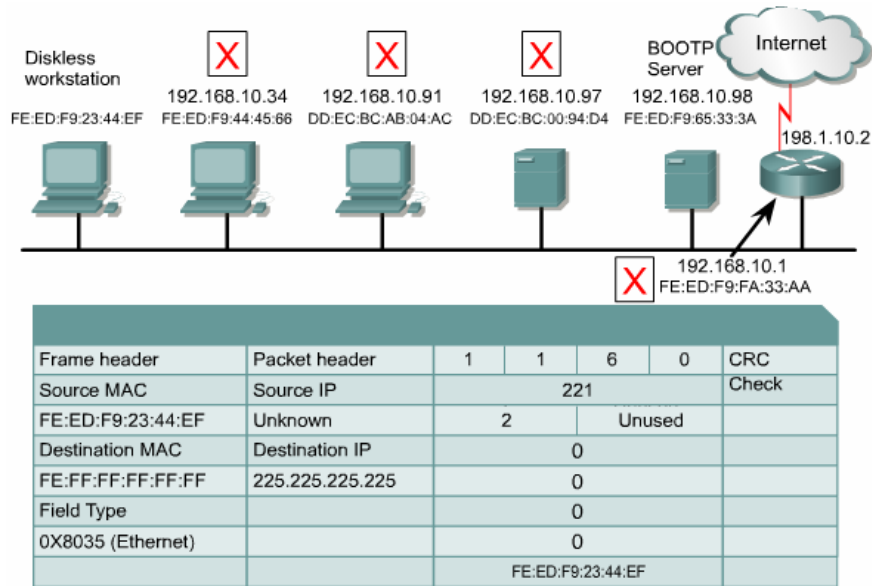


Frame header	Packet header	1	1	6	0	CRC
Source MAC	Source IP	221				Check
FE:ED:F9:23:44:EF	Unknown	2	Unused			
Destination MAC	Destination IP	0				
FE:FF:FF:FF:FF:FF	225.225.225.225	0				
Field Type		0				
0X8035 (Ethernet)		0				
		FE:ED:F9:23:44:EF				



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Il processo BOOTP (3)

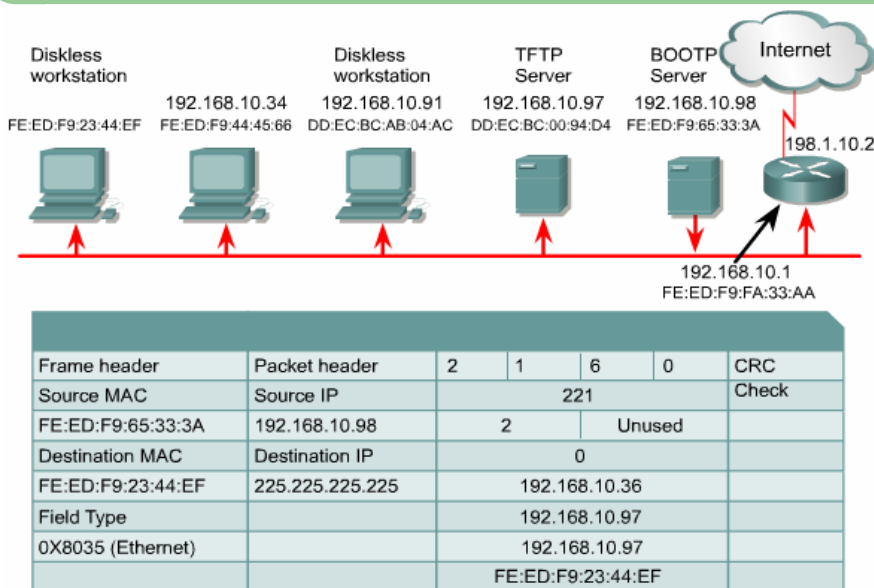


I vari computer scartano il pacchetto dopo avere tolto gli header di layer 2 e di layer 3 (erano dei broadcast) perché vedono la BOOTP request



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Il processo BOOTP (4)



Il BOOTP server risponde con una BOOTP reply e include, nel messaggio che manderà in broadcast, anche indirizzi IP di alcuni server.

- Solo il computer interessato prenderà il pacchetto e ne trarrà le informazioni utili; questo perché il MAC address di destinazione è proprio il suo



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

II DHCP – Dynamic Host Configuration Protocol

- E' il successore del BOOTP
- Permette di ottenere dinamicamente l'IP address senza che l'amministratore di rete metta su un profilo per ogni device della rete
- Si richiede di definire un range di IP address sul server DHCP
- L'intera configurazione del computer si può ottenere tramite un messaggio, quindi si hanno le stesse informazioni dei messaggi BOOTP più l'indirizzo IP e la subnet mask
- Permette agli utenti di essere mobili



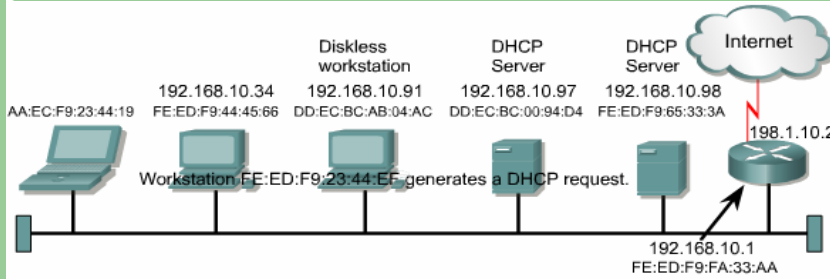
Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Pacchetto DHCP e campi del pacchetto

0 - 7 bits	8 - 15 bits	16 - 23 bits	24 - 31 bits
Op (1)	Htype (1)	HLen (1)	Hops (1)
Xid (4bytes)			
Seconds (2 bytes)		Flags(2 bytes)	
Ciaddr (4 bytes)			
Yiaddr (4 bytes)			
Siaddr (4 bytes)			
Giaddr (4bytes)			
Chaddr (16 bytes)			
Server Host Name (32 bytes)			
Boot File Name (64 bytes)			
Vendor Specific Area (variable)			
DHCP message structure			
Op	Message operation code Messages can be either BOOTREQUEST or BOOTREPLY.		
Htype	Hardware address type		
Hlen	Hardware address length		
Hops	Client places zero, this field is used by BOOTP server to send request to another network		
Xid	Transaction ID		
Secs	Seconds elapsed since the client began the address acquisition or renewal process		
Flags	Flags		
Ciaddr	Client IP address		
Yiaddr	"Your" (client) IP address		
Siaddr	IP address of the next server to use in bootstrap		
Giaddr	Relay agent IP address used in booting via a relay agent		
Chaddr	Client hardware address		
Server Host Name	Specifies particular server to get BOOTP information from		
Boot File Name	Allows for multiple boot files to be used allowing hosts to run different operating systems		
Vendor Specific Area	Contains optional vendor specific information that can be passed to the host		

Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Il processo DHCP – creazione della richiesta

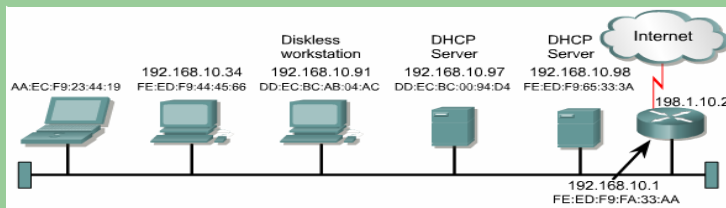


Frame header	Packet header	1	1	6	0	CRC Check
Source MAC	Source IP	221				
AA:EC:F9:23:44:19	Unknown	2	Flags			
Destination MAC	Destination IP	0				
FF:FF:FF:FF:FF:FF	225.225.225.225	0				
Field Type		0				
		AA:EC:F9:23:44:19				
0X8035 (Ethernet)		53	1	1		

All devices pick up a copy of the frame, detect a broadcast MAC destination, strip off the frame header, and pass the packet up to the Network layer. The devices detect that the IP destination is a broadcast IP address, strip off the packet header, and pass the reply data to the Transport layer. All of the devices detect the DHCP request field as being a DHCP request. All devices except for the DHCP servers discard the request.

Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Il processo DHCP – creazione della “offerta”



Frame header	Packet header	2	1	6	0	CRC Check
Source MAC	Source IP	12				
FE:ED:F9:65:33:3A	192.168.10.98	2	Flags			
Destination MAC	Destination IP	192.168.10.35				
AA:EC:F9:23:44:19	225.225.225.225	0				
Field Type		192.168.10.1				
		AA:EC:F9:23:44:19				
0X8035 (Ethernet)		53	1	2		

The server prepares a DHCP offer to send back to the requesting device. This includes Client IP address, DHCP server address, and Default Gateway address. In the Frame header, Source and Destination addresses are reversed. In the Packet header, the DHCP server places its IP address in the source field and a broadcast address in the destination field. This is done to get the DHCP response packet back up to the Transport layer to be processed. Only a broadcast will be passed since the client still does not know its IP address.

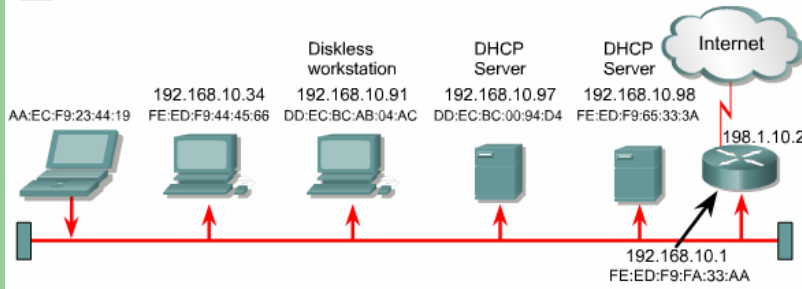
The DHCP server sends the DHCP reply frame back to the requesting device. All devices pick up the packet and examine it.

The destination MAC address is not theirs and not a broadcast, so they discard the packet. The MAC address is matched on the requesting client device and so the Source IP and MAC address of the DHCP server are stored in the ARP table of the laptop. The frame header is stripped off and discarded.



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Il processo DHCP – generazione della richiesta



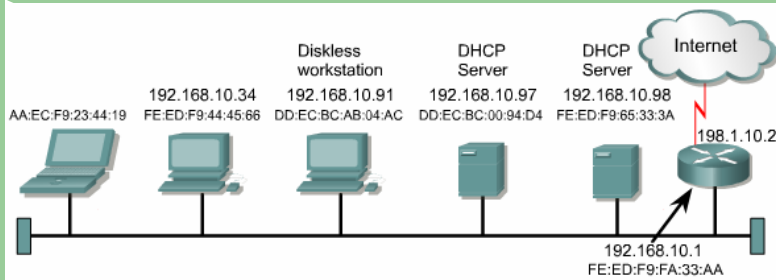
Frame header	Packet header	1	1	6	0	CRC Check
Source MAC	Source IP	12				
AA:EC:F9:23:44:19	Unknown	2	Flags			
Destination MAC	Destination IP	0				
FA:ED:F9:65:33:3A	192.168.10.98	192.168.10.35				
Field Type		0				
		192.168.10.1				
		AA:EC:F9:23:44:19				
0X8035 (Ethernet)		53	1	3		

The laptop computer now sends a DHCPREQUEST addressed to the specific DHCP server that sent the accepted offer.



Cap. 9 Protocollo TCP/IP & Indirizzamento IP

Il processo DHCP – creazione del DHCPACK



Frame header	Packet header	2	1	6	0	CRC Check
Source MAC	Source IP	12				
FE:ED:F9:65:33:3A	192.168.10.98	2	Flags			
Destination MAC	Destination IP	0				
AA:EC:F9:23:44:19	225.225.225.225	192.168.10.35				
Field Type		0				
		192.168.10.1				
		AA:EC:F9:23:44:19				
0X8035 (Ethernet)		53	1	5		

The DHCP server sends the DHCPACK frame back to the requesting device. All devices pick up the packet and examine it.

a questo punto il pc che riceve il DHCPACK, adotta l'IP assegnato dal server DHCP.

