TCP/IP e Internet

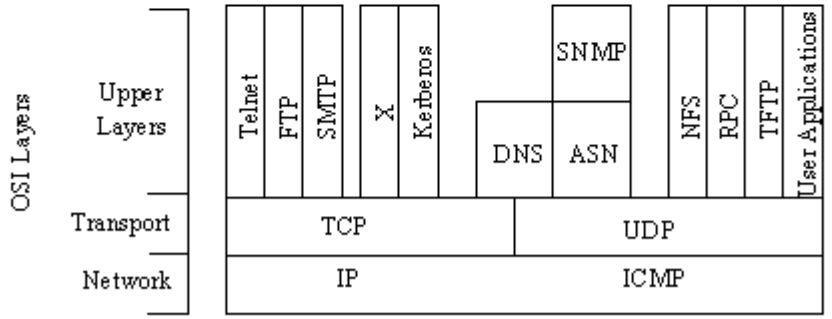
TCP/IP è un protocollo software di comunicazione usato nel networking. Sebbene il nome TCP/IP implichi che l’intero panorama del prodotto sia una combinazione di due protocolli – Transmission Control Protocol e Internet Protocol – il termine TCP/IP si riferisce non ad una singola entità che combina due protocolli, ma ad un

più ampio set di programmi software che forniscono servizi di rete come il login remoto, il trasferimento di file remoto, e la posta elettronica. TCP/IP fornisce un metodo per trasferire informazioni da una macchina all'altra. UN protocollo di comunicazione dovrebbe trattare errori di trasmissione, governare l'instradamento e la consegna dei dati, e controllare la trasmissione mediante l'uso di determinati segnali di stato. TCP/IP fa tutto questo.

IL modello di riferimento OSI si compone di sette strati. Anche il protocollo TCP/IP è stato concepito a strati, sebbene non ci sia una corrispondenza uno ad uno con il modello OSI. Possiamo sovrapporre i programmi TCP/IP su questo modello per avere una idea grossolana sulla posizione in cui risiedono gli strati TCP/IP. Prima di questo però diamo un rapido sguardo ai protocolli TCP/IP e a come essi si relazionano l'uno all'altro, e mostriamo una grossolana mappatura rispetto al modello OSI. La figura seguente mostra che alcuni dei protocolli di livello superiore, come Telnet e FTP, dipendono da TCP, mentre altri , come TFTP e RPC dipendono da UDP. La gran parte dei protocolli di livello superiore TCP/IP usa soltanto uno dei protocolli di trasporto (TCP o UDP), mentre pochi, come DNS (Domain Name System) possono usare entrambi.

Telnet - RemoteLogin
FTP - File Transfer Protocol
SMTP - Simple Mail Transfer Protocol
X - X Windows System
Kerberos - Security
DNS - Domain Name System
ASN - Abstract Syntax Notation
SNMP - Simple Network Management Protocol

NFS - Network File Server
RPC - Remote Procedure Calls
TFTP - Trivial File Transfer Protocol
TCP - Transmission Control Protocol
User Datagram Protocol
IP - Internet Protocol
ICMP - Internet Control Message Protocol



Una nota precauzionale circa TCP/IP: nonostante il fatto che TCP/IP sia un protocollo aperto, molte compagnie lo hanno modificato per i propri sistemi di networking. Ci possono essere incompatibilità a causa di queste modifiche, che, sebbene aderiscano agli standard ufficiali, possono avere altri aspetti che causano problemi.

TCP/IP è fondato sul concetto client e server. IL termine client/server ha un semplice significato nel protocollo TCP/IP : ogni apparecchio che inizia la comunicazione è il client, il dispositivo che risponde è il server. Il server sta rispondendo (sta servendo) alla richiesta del client.

Una rapida carrellata dei componenti di TCP/IP

Per comprendere il ruolo dei molti componenti della famiglia di protocolli TCP/IP è utile capire cosa si può fare in una rete TCP/IP.

Una volta che vengono comprese le applicazioni, i protocolli che rendono ciò possibile sono più facili da comprendere.

Telnet

Il programma Telnet fornisce una capacità di login remoto. Ciò permette ad un utente di collegarsi ad un'altra macchina ed agire come se egli fosse di fronte all'altro computer. La connessione può avvenire in un network locale o in un altro network in un punto qualsiasi nel mondo, se naturalmente l'utente ha il permesso di collegarsi con il sistema remoto. Questa possibilità non è realizzata con frequenza eccettuato un contesto LAN o WAN, ma alcuni sistemi accessibili in Internet consentono sessioni Telnet per permettere agli utenti di familiarizzare con nuove applicazioni o sistemi operativi.

File Transfer Protocol

L'FTP permette di copiare un file risiedente su un sistema in un altro sistema. L'utente in realtà non si collega come un utente completamente padrone della macchina a cui vuole accedere come nelle sessioni Telnet, ma invece usa il programma FTP per abilitarsi l'accesso. Ancora una volta sono necessari opportuni permessi per avere accesso ai file. Una volta che la connessione alla macchina remota sia stata stabilita, FTP ci permette di copiare uno o più file sulla nostra macchina (il termine transfer implica che il file è spostato da un sistema all'altro ma l'originale non è modificato, i file vengono copiati).

Simple Mail Transfer Protocol

Simple Mail Transfer Protocol (SMTP) è utilizzato per trasferire messaggi di posta elettronica. Esso è completamente trasparente all'utente. Dietro la scena, SMTP si connette alla macchina remota e trasferisce i messaggi di posta elettronica un po' cometa FTP per i file.

Kerberos

Kerberos è un protocollo ampliamente supportato per la sicurezza. Kerberos usa una particolare applicazione nota come authentication server per convalidare password e schemi di crittografia. Kerberos è uno dei più sicuri sistemi di crittografia ed è molto comune in UNIX.

Domain Name System

Domain Name System (DNS) abilita un computer che abbia un nome comune ad esser trasformato in uno speciale indirizzo di rete. Per esempio, un computer chiamato Pippo non può ricevere accessi da altri computer dello stesso network o di altri network collegati a meno ché non sia disponibile qualche metodo che controlli il nome del computer e lo rimpiazzi con l'indirizzo hardware della macchina. DNS fornisce la conversione fra il nome comune locale è l'8indirizzo fisico univoco della connessione di rete del computer.

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) fornisce messaggi di stato e report su eventuali problemi nella rete all'amministratore. SNMP usa UDP (User Datagram

Protocol) come meccanismo di trasporto. SNMP usa termini leggermente diversi da TCP/IP, poiché invece di lavorare con client e server, lavora con manager e agent(anche se significano la stessa cosa). Un agente fornisce informazioni circa un apparecchio mentre un manager comunica con agenti lungo la rete.

Network File System

NFS è un set di protocolli sviluppati da Sun Microsystem per permettere a più macchine di accedere alle directory di ciascuna in modo trasparente. Essi fanno questo usando uno schema di file system distribuito. Sistemi NFS sono comuni in ampi ambienti aziendali che usano workstation Unix.

Remote Procedure Call

Il protocollo RPC è un set di funzioni che abilita un'applicazione a comunicare con un'altra macchina (il server). Esso fornisce funzioni di programmazione, codici, e variabili predefinite per supportare il calcolo distribuito.

Trivial File Transfer Protocol

TFTP è un protocollo di trasferimento file molto semplice e che manca di sicurezza. Esso usa UDP come meccanismo di trasporto

Transmission Control Protocol

TCP è un protocollo di comunicazione che fornisce un affidabile trasferimento di dati. E' responsabile dell'assemblaggio in pacchetti standard dei dati passatigli da applicazioni dei livelli superiori e assicura che i dati siano trasferiti correttamente.

User Datagram Protocol

UDP è un protocollo senza connessione, il che significa che esso non provvede a ritrasmettere i datagrammi in caso di errore (a differenza di TCP che è orientato alla connessione). UDP non è affidabile ma ha scopi specializzati. Se le applicazioni che usano UDP posseggono controlli di affidabilità, le deficienze del protocollo UDP vengono superate.

Internet Protocol

IP è responsabile della movimentazione dei pacchetti di dati assemblati da TCP o UDP lungo la rete. Esso usa un set di indirizzi univoci per ogni apparecchiatura della rete per determinare l'instradamento e la destinazione.

Internet Control Message Protocol

ICMP è responsabile del controllo e della generazione di messaggi di stato dei dispositivi presenti sulla rete. Esso può essere utilizzato per informare altri dispositivi dell'avaria di una particolare macchina. Generalmente ICMP e IP lavorano insieme.

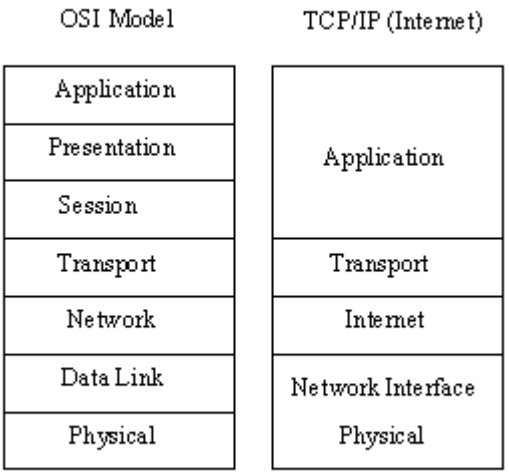
Modello OSI e TCP/IP

L'adozione del TCP/IP non è entrata in conflitto con gli standard OSI perché i due si sono sviluppati in parallelo. In qualche modo TCP/IP ha contribuito al modello OSI e viceversa. Esistono varie importanti differenze, però, che sorgono dalle specifiche di base di TCP/IP che sono:

- Un set di applicazioni comune
- Instradamento dinamico

- Protocolli non orientati alla connessione ai livelli di rete
- Connettività universale
- Commutazione di pacchetto

Le differenze fra l'architettura Osi e TCP/IP risiedono negli strati superiori a quello di trasporto e quelli a livello di rete. Il modello Osi ha sia il livello di sessione che il livello di presentazione, mentre TCP/IP li combina entrambi in un livello di applicazione. La richiesta di un protocollo non orientato alla connessione richiede inoltre che TCP/IP combini lo strato fisico e data link del modello OSI in un unico strato di rete. La figura seguente mostra un confronto fra l'organizzazione in strati del modello TCP/IP e del modello OSI.



La combinazione dei due ultimi strati in un singolo livello non costituiva uno scandalo visto che la maggior parte delle realizzazioni concrete del modello OSI combinavano i livelli fisico e di linea in un controller intelligente (come le schede di rete). Un pregio ancora più grande del livello unico consiste nel fatto che lo sviluppo

di una sottorete era indipendente da qualsiasi protocollo di rete poiché TCP/IP era indifferente ai dettagli di implementazione. Ciò permetteva a reti chiuse, proprietarie di implementare i protocolli TCP/IP per comunicare con l'ambiente esterno.

L'approccio a livelli diede origine al nome TCP/IP. Lo strato di trasporto usa in protocolli TCP o UDP (ve ne sono altri ma questi sono i più comuni) mentre vi è un unico protocollo di rete costituito da IP. Ciò è quello che assicura la connettività universale, uno degli obiettivi primari.

TCP/IP e Ethernet

Per molte persone i termini TCP/IP e Ethernet vanno a braccetto quasi automaticamente, principalmente per ragioni storiche e anche per la ragione che vi sono più reti TCP/IP basate su Ethernet che di qualunque altro tipo.

Ethernet è un sistema hardware che fornisce i primi due livelli del modello OSI .

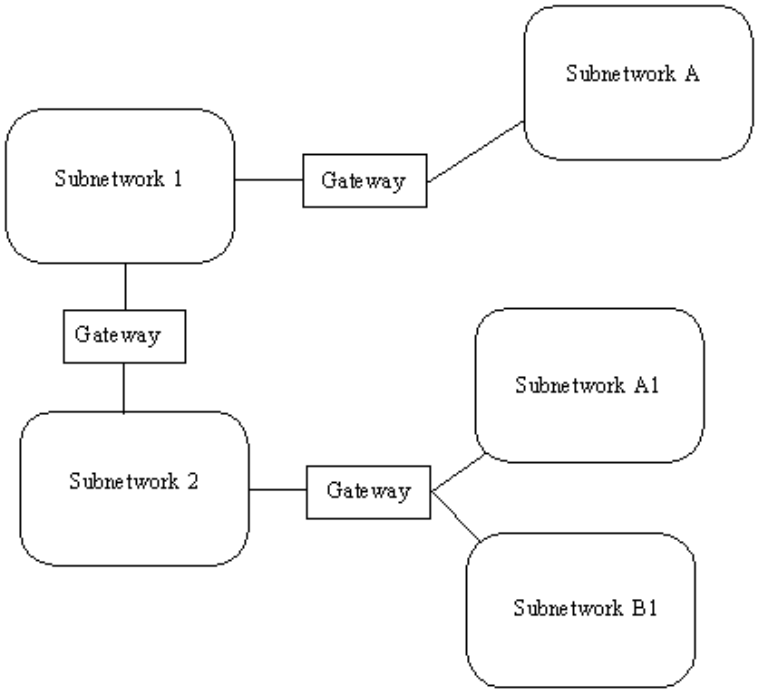
Ethernet e TCP/IP lavorano bene insieme, con Ethernet che fornisce la connessione fisica (livelli uno e due) e TCP/IP che fornisce il protocollo di comunicazione (Livelli tre e quattro). I due hanno i propri procedimenti per impacchettare le informazioni: TCP/IP usa indirizzi a 32 bit mentre Ethernet usa uno schema a 48 bit. I due sistemi lavorano bene insieme grazie a un componente di TCP/IP chiamato Address Resolution Protocol (ARP), che effettua una conversione fra i due schemi.

Ethernet si appoggia su un protocollo chiamato Carrier Sense Multiple Access with Collision Detect (CSMA/CD). Un dispositivo controlla il cavo di rete per

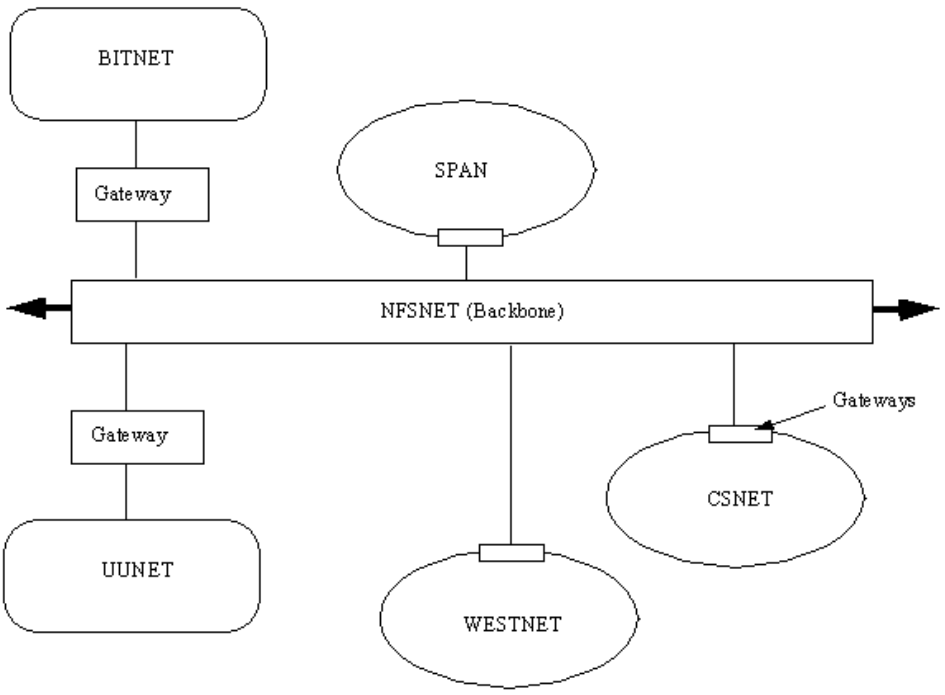
verificare se qualcosa viene trasmesso. Se la via è libera l'apparecchio invia i suoi dati. Se il cavo è occupato (rilievo della portante), l'apparecchio attende che esso sia libero. Se due apparecchi trasmettono contemporaneamente (si ha cioè collisione), essi lo scoprono poiché confrontano costantemente il traffico sul cavo con i dati conservati nel loro buffer di uscita. Se si ha collisione i due computer attendono un tempo casuale per riprovare a trasmettere.

La struttura di Internet

Internet non è una singola rete ma una collezione di sottoreti che comunicano l'una con l'altra mediante gateway. Possiamo definire un gateway (a volte chiamato router) come un sistema che svolge funzioni di interconnessione tra reti, come mostra la figura seguente



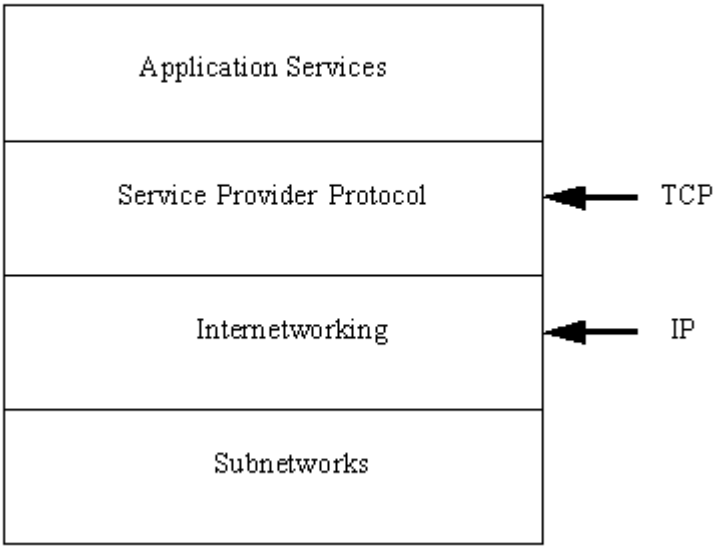
Con TCP/IP tutte le interconnessioni tra reti fisiche avvengono mediante gateway. Un punto importante da ricordare per il seguito è che i gateway instradano i pacchetti di dati in base al nome della loro sottorete di destinazione e non della macchina di destinazione. Si presuppone che i gateway siano completamente trasparenti all'utente il che li solleva dal trattare applicazioni di utente (a meno che la macchina che funziona da gateway non sia anche la macchina di lavoro di qualcuno o il server di un network locale). Posta la questione in maniera semplice, il solo scopo di un gateway è di ricevere una PDU (Protocol Data Unit) dalla rete di interconnessione o dalla rete locale e di instradarla al prossimo gateway o alla rete locale perché venga inviata all'utente destinatario. I gateway lavorano con ogni tipo di hardware o sistema operativo, l'importante è che usino TCP/IP.



Gli strati di Internet

La maggior parte delle reti di interconnessione, incluso Internet, può essere pensata come un'architettura a strati per semplificarne la comprensione. Il concetto di strato aiuta nel compito di sviluppare applicazioni per l'internetworking. La stratificazione mostra inoltre come i vari componenti di TCP/IP lavorano insieme. Bisogna stare attenti però a capire che questi strati sono solo concettuali, non sono strati hardware o software come gli strati del modello Osi o di TCP/IP.

E' conveniente immaginare che Internet sia organizzata su quattro strati. Questa organizzazione a strati è mostrata nella figura seguente



Questi strati non dovrebbero essere confusi con l'architettura di ogni singola macchina, come descritta nel modello a sette strati OSI . Essi sono invece un metodo per capire come la rete di interconnessione, le varie reti, TCP/IP e le varie macchine

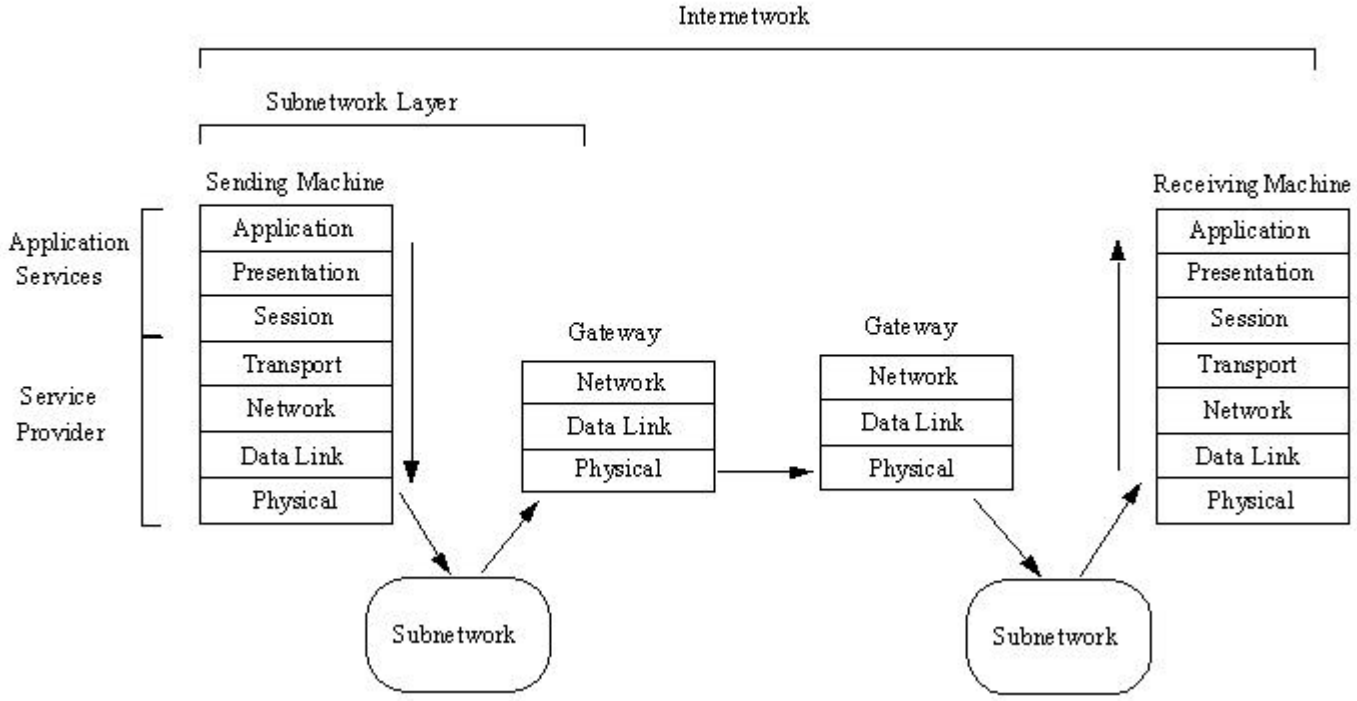
lavorano insieme. Le macchine indipendenti risiedono in uno strato di sottorete al livello più basso dell'architettura.

Al di sopra dello strato di sottorete vi è lo strato di interconnessione che fornisce le funzionalità di interconnessione delle sottoreti mediante gateway. Lo strato internetwork è lo strato dove i dati vengono trasferiti da gateway a gateway finché essi raggiungono la loro destinazione e passano allo strato subnetwork. Lo strato Internetwork usa il protocollo IP.

Lo strato service provider protocol è responsabile della comunicazione end-to-end della rete. Questo è lo strato che usa il protocollo TCP ed altri. Esso governa il flusso dei dati e garantisce l'affidabilità del trasferimento di messaggi.

LO strato in cima alla stratificazione è lo strato application services che fornisce l'interfacciamento con le applicazioni degli utenti. Questo strato si interfaccia con la posta elettronica, il trasferimento remoto dei file, e l'accesso remoto. Diversi protocolli sono utilizzati in questo strato.

Per capire come lavora questo modello dell'architettura di Internet è utile un semplice esempio. Assumiamo che un'applicazione su una macchina voglia trasferire un datagramma ad un'applicazione su un'altra macchina in un'altra sottorete. Senza tutti i segnali fra i vari strati e semplificando un po' l'architettura il processo è mostrato nella figura seguente



il dato è inviato giù lungo tutti gli strati della macchina che invia , assemblando il datagramma con tutte le informazioni di controllo dei protocolli (PCI Protocol Control Information) via via che il dato attraversa i vari strati . dallo strato fisico il datagramma, che spesso è definito frame dopo che lo strato di data link vi ha aggiunto un header e informazioni di tracciamento, viene inviato alla rete locale. La LAN instrada l'informazione verso il gateway . durante questo processo la LAN non si preoccupa del contenuto del datagramma . alcune reti, comunque, alterano l'header per mostrare attraverso quali macchine è passato il datagramma .

il datagramma passa da gateway a gateway finché giunge alla sottorete di destinazione. Ad ogni passo il gateway esamina l'header per verificare se il datagramma è destinato alla sottorete che quel gateway guida. Se la risposta è negativa esso lo instrada di nuovo verso la rete di interconnessione. Questa analisi è

realizzata nello strato fisico evitando in tal modo di far andare il pacchetto su e giù per i vari strati della macchina. L'header può essere modificato da ogni gateway per riflettere il suo percorso di instradamento. Quando il datagramma è finalmente ricevuto dal gateway della sottorete di destinazione, il gateway riconosce che il datagramma è giunto alla sottorete corretta e lo instrada alla rete locale ed infine alla macchina di destinazione. L'instrada,mento è realizzato leggendo le informazioni contenute nell'header. Quando il datagramma giunge alla macchina di destinazione, risale i vari strati , mentre ogni strato elimina il suo header con le sue informazioni PCI . in cima lo strato di applicazione esamina l'header finale e passa il datagramma all'applicazione corretta.

Problemi di interconnessione

Non tutto va liscio quando si trasferiscono dati da una sottorete all'altra. Accadono tutti i tipi di problemi , nonostante il fatto che tutti usino lo stesso protocollo. Un tipico problema è la limitazione dell'ampiezza del singolo datagramma. La rete di partenza potrebbe supportare datagrammi da 1024 byte ma il network ricevitore potrebbe usare solo datagrammi da 512 byte (a casa del differente protocollo hardware ad esempio). Qui diviene importante il processo di segmentazione, separazione, riassemblaggio e concatenazione (spiegato alla fine).

I reali metodi di indirizzamento usati dai diversi network possono causare conflitti quando si instradano i datagrammi . poiché le sottoreti comunicanti potrebbero non usare lo steso software di controllo , le informazioni degli header basate sulla

sottorete potrebbero differire , nonostante il fatto che i metodi di comunicazione siano basati su TCP/IP. Un problema associato si ha quando si tratta con le differenze fra i nomi logici e gli indirizzi fisici delle varie macchine. Nella stessa maniera una sottorete che prescrive la cifratura invece del datagramma in chiaro potrebbe interferire con la decodifica delle informazioni contenute nell'header. differenze nella politica di sicurezza implementata dalle varie reti potrebbero influenzare il traffico dei datagrammi. Tutte queste differenze possono essere risolte via sofware , ma i problemi associati con i metodi di indirizzamento possono diventare considerevoli.

Un altro problema comune è la differente tolleranza dei vari network ai problemi di tempificazione. Valori di time out o di retry possono differire cosi quando due sottoreti tentano di stabilire una connessione una potrebbe aver rinunciato ed essere passata ad un altro compito mentre la seconda sta ancora attendendo pazientemente un segnale di acknowledgment . inoltre se due reti stanno comunicando in maniera appropriata ed un di esse diventa occupata e ha la necessità di effettuare una pausa breve nel processo di comunicazione , l'ammontare di tempo che l'altro network interpreta come una disconnessione diventa un problema primario. Coordinare le temporizzazione in tutta la rete di interconnessione può diventare complicato.

I metodi di instradamento e la velocità delle varie macchine possono anch'essi influenzare l'efficacia della interconnessione. Se un gateway è implementato da una macchina veramente lenta , il traffico che arriva attraverso quel gateway può tornare indietro, causando ritardi e trasmissioni incomplete in tutta la rete. Sviluppare una

interconnessione capace di ricaricare e reindirizzare i datagrammi quando si ha un collo di bottiglia diventa veramente importante.

Indirizzi Internet

Indirizzi di rete sono analoghi ad indirizzi di posta in quanto essi dicono al sistema dove consegnare un datagramma. Tre termini comunemente utilizzati in Internet sono relazionati con l'indirizzamento: nome, indirizzo e percorso.

Un nome è una specifica identificazione di una macchina, di un utente, di un'applicazione. Esso è usualmente unico e fornisce un obiettivo assoluto per il datagramma. Un indirizzo tipicamente identifica dove è localizzato il target, usualmente la sua collocazione fisica e logica nella rete. Un percorso indica al sistema come far giungere il datagramma a destinazione.

Noi utilizziamo spesso il nome del ricevente, specificando il nome utente o il nome della macchina, e la macchina fa la stessa cosa in modo trasparente a noi. Dal nome, un software chiamato name server tenta di risolvere il nome ed il percorso, rendendo quest'aspetto non importante. Quando inviamo un messaggio di posta elettronica, indichiamo semplicemente il destinatario, facendo affidamento sul fatto che il name server trovi il modo di consegnare il messaggio al destinatario.

Usare un name server ha un'altro vantaggio importante oltre a rendere l'indirizzamento e il routing non importante per l'utente finale. Esso da al sistema o all'amministratore di rete molta libertà per effettuare modifiche alla rete, senza aver bisogno di informare ogni singola macchina della rete sulle modifiche effettuate.

Finché un’applicazione può accedere al name server , ogni cambiamento nell’instradamento può essere ignorato dall’applicazione e dall’utente.

Le convenzioni per l’attribuzione di nomi variano al variare della piattaforma, della rete, della versione del software.

Subnetwork addressing

In una singola rete, diverse parti dell’informazione sono necessarie per garantire la corretta consegna dei dati. I componenti principali sono l’indirizzo fisico e l’indirizzo di data link.

L’indirizzo fisico

Ogni dispositivo in una rete che dialoga con altri dispositivi ha un indirizzo fisico unico, chiamato talvolta indirizzo hardware. Su ogni dato network, vi è una sola occorrenza di ogni indirizzo; altrimenti, il name server non ha alcuna possibilità il dispositivo target in maniera non ambigua. Per l’hardware, gli indirizzi sono usualmente codificati in una scheda di interfaccia di rete, e sono settati mediante switch o via software. Facendo riferimento al modello OSI, l’indirizzo fisico è localizzato al livello fisico.

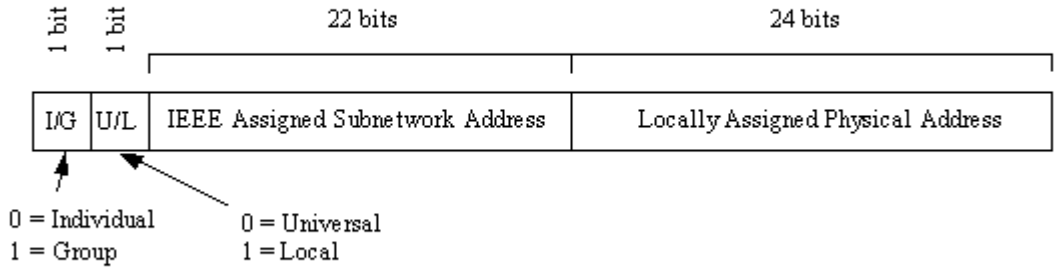
Nel livello fisico è realizzata l’analisi di ogni singolo datagramma in arrivo. Se l’indirizzo del destinatario combacia con l’indirizzo fisico del dispositivo, il datagramma può essere passato agli strati superiori. Se gli indirizzi non corrispondono, il datagramma viene ignorato. Mantenere quest’analisi al livello più

basso del modello Osi previene inutili ritardi, perché altrimenti il datagramma dovrebbe essere passato ai livelli superiori per effettuare l'analisi degli indirizzi.

La lunghezza dell'indirizzo fisico varia in dipendenza del tipo di rete, ma Ethernet ed altri sistemi utilizzando indirizzi a 48 bit.per le comunicazioni occorrono due indirizzi: uno per il mittente ed uno per il destinatario.

La IEEE ha assunto ora il compito di assegnare indirizzi universali ad ogni sottorete. Per ogni sottorete IEEE un unico identificatore di organizzazione (Organization Unique Indetifier OUI) lungo 24 bit,abilitando l'organizzazione ad assegnare gli altri 24 bit come desidera. (in realtà 2 dei 24 bit assegnati all'OUI sono bit di controllo per cui rimangono a disposizione 22 bit per l'indirizzo il che rende disponibili 2^{22} combinazioni possibili , per cui già è prevedibile la possibilità che si possano esaurire gli OUI se l'attuale ritmo di crescita della rete prosegue.

Il formato dell'OUI è mostrato nella figura seguente



il bit meno significativo dell'indirizzo è il bit che indica se si tratta di un indirizzo individuale o di gruppo. Se il bit è posto a zero, si tratta di un indirizzo individuale, se è ad uno indica che il resto dell'indirizzo costituisce l'indirizzo di gruppo che

necessita di una ulteriore analisi. Se tutti i bit dell'OUI sono posti ad 1, l'indirizzo assume lo speciale significato che tutte le stazioni della rete sono destinatarie del messaggio. Il secondo bit è il bit locale o universale. Se è posto a zero, esso è stato impostato dall'organismo di amministrazione universale. Questo è cioè il settaggio per identificare OUI assegnati direttamente da IEEE. Se ha il valore ad uno vuol dire che l'OUI è stato assegnato localmente e potrebbe causare problemi di indirizzamento se utilizzato come indirizzo IEEE. I rimanenti 22 bit realizzano l'indirizzo fisico della sottorete , così come assegnato dalla IEEE. Il secondo set di 24 bit identifica indirizzi locali di rete ed è amministrato localmente. Se un'organizzazione esaurisce indirizzi fisici (ci sono circa 16 milioni di indirizzi fisici possibili con 24 bit), la IEEE può assegnare all'organizzazione un secondo indirizzo di sottorete.

La combinazione dei 24 bit dell'OUI e dei 24 bit assegnati localmente è chiamato indirizzo di accesso al mezzo (Media Access Control Address) . quando un pacchetto è assemblato per essere trasferito in una rete di interconnessione, ci sono due set di indirizzi MAC: uno della macchina mittente ed uno della macchina ricevente.

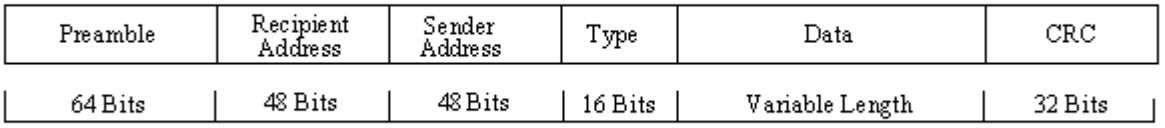
Indirizzo data-link

Gli standard IEEE Ethernet utilizzano un'altro indirizzo chiamato indirizzo del livello di linea (abbreviato come LSAP: Link Service Access Point). Il LSAP identifica il tipo di protocollo utilizzato nel livello di linea . come nel caso dell'indirizzo fisico, un datagramma porta sia il LSAP del trasmettitore che del ricevitore.

Frame Ethernet

L'organizzazione delle informazioni in ogni pacchetto di dati trasmesso differisce in dipendenza del protocollo,, ma è utile esaminarne uno per vedere come gli indirizzi e le relative informazioni sono legati ai dati. Usiamo Ethernet come un esempio a causa del suo uso diffuso con TCP/IP

Un tipico frame Ethernet è mostrato nella figura seguente



Il preambolo è un set di bit utilizzati principalmente per sincronizzare il processo di comunicazione e tener conto di ogni rumore aleatorio nei primi bit che vengono inviati. Alla fine del preambolo vi è una sequenza di bit detta Start Frame Delimiter (SFD) che indica che subito dopo inizia il pacchetto.

Gli indirizzi del mittente e del destinatario seguono il formato a 48 bit IEEE, seguito da un indicatore di tipo a 16 bit che viene utilizzato per identificare il protocollo. I dati seguono l'identificatore di tipo. Il campo dati ha una lunghezza compresa fra 46 e 1500 byte. Se i dati da inviare sono lunghi meno di 46 byte, essi sono riempiti di bit nulli fino a raggiungere la dimensione di 46 byte. Queste aggiunte non sono calcolate nella determinazione della dimensione del campo dati, che è utilizzata in una parte dell'header IP.

Alla fine del frame vi è il contatore CRC (Cyclic Redundancy Check), utilizzato per oscurare che i contenuto del frame non sono stati modificati durante il processo di trasmissione. Ciascun gateway lungo il percorso di instradamento calcola il valore di CRC del frame e lo confronta con il valore che trova alla fine del frame. Se i due valori corrispondono il frame può proseguire nel suo percorso. Se essi differiscono deve essere avvenuta una modifica nel frame ed esso viene scartato (per essere ritrasmesso dal trasmettitore quando scade un timer).

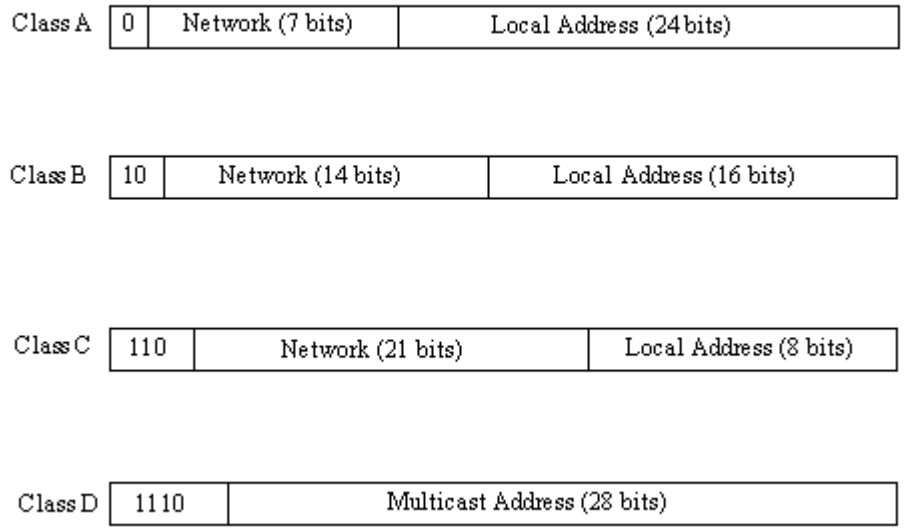
In alcuni protocolli come l'IEEE802.3 l'organizzazione generale del frame è la stessa con alcune piccole differenze nel contenuto. Nel 802.3 i 16 bit usati da Ethernet per identificare il tipo di protocollo sono rimpiazzate con un valore a 16 bit che da la lunghezza del blocco di dati.

Indirizzi IP

TCP/IP utilizza un indirizzo a 32 bit per identificare una macchina in una rete e la rete cui essa è collegata. Gli indirizzi IP identificano la connessione di una macchina alla rete non la macchina stessa, un'importante differenza. Quando viene modificata la localizzazione della macchina nella rete, anche l'indirizzo IP deve cambiare.

Gli indirizzi IP sono assentai dal Network Information Center (NIC) sebbene se una rete non è collegata ad internet essa può determinare la sua propria numerazione. Per tutti gli accessi Internet, l'indirizzo IP deve essere registrato presso il NIC.

Ci sono quattro formati diversi per l'indirizzo IP, ciascuno dei quali viene impiegato in dipendenza della ampiezza della rete. Essi sono denominati da Classe A a Classe D e sono mostrati nella figura seguente.



La classe è identificata dai primi bit della sequenza. La classe A è riservata per reti grandi con molte macchine. I 24 bit per l'indirizzo locale (spesso denominato indirizzo host) sono necessari in questo caso. L'indirizzo del network è limitato a 7 bit il che riduce il numero di reti che possono essere indirizzate. Gli indirizzi di classe B sono utilizzati per reti intermedie , con indirizzi host su 16 bit e indirizzi di rete su 14 bit. Gli indirizzi di classe C hanno solo 8 bit per gli indirizzi locali o host, limitando il numero di apparecchiature a 256. vi sono in compenso 21 bit per l'indirizzo della rete. Infine gli indirizzi di classe D sono utilizzati per il multicasting.

gli indirizzi IP sono 4 set di 8 bit, per un totale di 32 bit. Spesso questi bit sono rappresentati separati da un punto. Inoltre sono usualmente scritti mediante il loro equivalente decimale.

Dall'indirizzo IP, una rete può determ9inare se un frame deve uscire dalla sottorete tramite un gateway. I gateway che ricevono dati che vanno trasmessi ad un'altra sottorete devono determinare l'instradamento dall'indirizzo IP contenuto nei dati e da una tabella interna che contiene informazioni per l'instradamento.

Come menzionato, se un indirizzo contiene tutti bit ad 1, l'indirizzo si applica a tutti gli indirizzi della rete. La stessa regola si applica agli indirizzi IP, cosicché un indirizzo IP con 32 bit ad 1 è considerato un messaggio broadcast a tutte le apparecchiature e a tutte le reti. E' possibile mandare un messaggio in broadcast a tutte le macchine di una rete ponendo ad 1 tutti i bit dell'indirizzo host, cosicché ad esempio l'indirizzo 147.10.255.255 per un network di classe B (con indirizzo di rete 147.10) verrebbe ricevuto da tutti i computer di quella rete, ma i dati non lascerebbero quella rete.

E' possibile per un'apparecchiatura avere più di un indirizzo IP se essa è connessa a più di una rete, come nel caso dei gateway. Si dice che queste apparecchiature sono multihomed, poiché esse hanno un indirizzo univo per ogni rete cui sono collegate.

Due network possono avere lo stesso indirizzo di rete se sono collegati da un gateway. Questo può causare problemi di indirizzamento perché il gateway deve essere capace di individuare su quale rete si trova l'indirizzo fisico che sta trattando.

Protocollo di risoluzione dell'indirizzo

La determinazione degli indirizzi può essere difficoltosa perché ogni macchina della rete potrebbe non avere una lista di tutti gli indirizzi delle altre macchine. Mandare un

dato da una macchina all'altra, se non si conosce l'indirizzo del destinatario può provocare problemi se non vi è un meccanismo di risoluzione dell'indirizzo. Dover aggiornare costantemente una tavola di indirizzi su ogni macchina sarebbe un incubo per l'amministratore di rete. Il problema non è ristretto a piccole reti, perché se non è noto l'indirizzo di rete della rete di destinazione, si possono avere problemi di instradamento e consegna dei dati. Il protocollo ARP (Address Resolution Protocol) aiuta a risolvere questi problemi. Il lavoro dell'ARP è di convertire indirizzi IP in indirizzi fisici e, nel fare questo, eliminare la necessità per le applicazioni di conoscere gli indirizzi fisici. Essenzialmente ARP è un tavola con una lista di indirizzi IP e dei loro corrispondenti indirizzi fisici. La tavola è chiamata cache ARP. La struttura di una cache ARP è mostrata nella figura seguente

	IF INDEX	PHYSICAL ADDRESS	IP ADDRESS	TYPE
Entry 1				
Entry 2				
Entry 3				
Entry n				

Ogni riga corrisponde ad una apparecchiatura, con quattro pezzi di informazione per ogni apparecchiatura:

- Indice IF: la porta fisica (interfaccia)

- Indirizzo fisico:l’indirizzo fisico della macchina
- Indirizzo IP:l’indirizzo IP corrispondente all’indirizzo fisco
- Tipo: tipo della voce nella tabella

Tipi di mapping

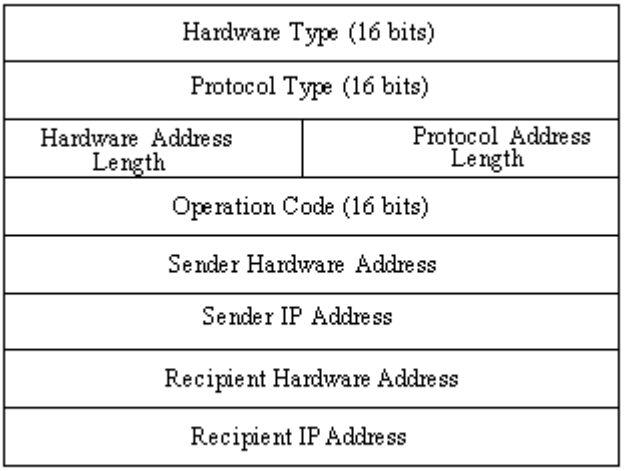
Il tipo di mapping è uno di quattro possibili valori che indicano lo stato della voce nella tabella. Un valore di 2 indica che quella voce non è valida; un valore di 3 indica che quella voce è dinamica e può essere cambiata; un valore 4 indica che la voce è statica (non può essere cambiata).

Quando l’ARP riceve l’indirizzo del destinatario, cerca nella tabella una corrispondenza. Se la trova, restituisce l’indirizzo fisico. Se non trova una corrispondenza nella tabella, esso manda un messaggio lungo la rete, detto ARP request, messaggio broadcast ricevuto da tutti i computer della rete locale: la ARP request contiene l’indirizzo IP del destinatario che si stava cercando: se un’apparecchiatura riconosce che quell’indirizzo IP le appartiene, manda un messaggio di replica contenente il suo indirizzo fisico alla macchina che ha generato la richiesta, tale informazione è posta nella cache per usi futuri. In tal modo la ARP può ricavare l’indirizzo fisico di ogni macchina basato sul suo indirizzo IP.

In questo modo si possono gestire cambiamenti negli indirizzi fisici nuove aggiunte alla rete, senza la cache, tutte le richieste ARP e le relative repliche genererebbero molto traffico, il che potrebbe avere un serio impatto sulle prestazioni della rete. Alcuni schemi più semplici abbandonano la cache e semplicemente utilizzano

messaggi broadcast ogni volta. Ciò è fattibile soltanto quando il numero delle apparecchiature è abbastanza piccolo da evitare problemi di traffico.

L'organizzazione di una ARP request è mostrata dalla figura seguente



Quando viene inviata una ARP request, sono utilizzati tutti i campi nella struttura eccetto il Recipient Hardware Address (indirizzo fisico del destinatario) che la richiesta sta tentando di identificare. In una replica sono invece utilizzati tutti i campi. Questo layout che è combinati con i protocolli della rete in una PDU (protocol Data Unit), ha vari campi:

- Hardware Type: il tipo di interfaccia hardware
- Protocol Type. Il tipo di protocollo utilizzato dalla macchina mittente
- Hardware Address Length: la lunghezza di ogni indirizzo hardware nel datagramma, data in byte
- Protocol Address Lenght: la lunghezza dell'indirizzo di protocollo nel datagramma, n byte

- Operation Code. Indica se si tratta di una request o di una risposta. Se si tratta di un datagramma richiesta esso è ad 1 altrimenti è a 2.
- Sender Hardware Address: indirizzo fisico della macchina che invia il messaggio
- Sender IP Address: indirizzo IP della macchina che ha inviato il messaggio
- Recipient IP Address: indirizzo IP della macchina ricevente
- Recipient Hardware Address:indirizzo fisico della macchina ricevente

Hardware type field

Esso identifica il tipo di interfaccia hardware. Valori ammessi sono i seguenti

Type	*Description*
1	Ethernet
2	Experimental Ethernet
3	X.25
4	Proteon ProNET (Token Ring)
5	Chaos
6	IEEE 802.X
7	ARCnet

Protocol Type Field

Tale campo identifica il tipo di protocollo che la macchina mittente utilizza . In genere con TCP/IP sono protocolli di tipo Ethernet per cui i valori consentiti sono i seguenti

Decimal	Description
512	XEROX PUP
513	PUP Address Translation
1536	XEROX NS IDP
2048	Internet Protocol (IP)
2049	X.75
2050	NBS
2051	ECMA
2052	Chaosnet
2053	X.25 Level 3
2054	Address Resolution Protocol (ARP)
2055	XNS
4096	Berkeley Trailer
21000	BBN Simnet
24577	DEC MOP Dump/Load
24578	DEC MOP Remote Console
24579	DEC DECnet Phase IV
24580	DEC LAT
24582	DEC
24583	DEC
32773	HP Probe
32784	Excelan
32821	Reverse ARP
32824	DEC LANBridge
32823	AppleTalk

Se non si tratta di protocolli ethernet sono possibili altri valori.

ARP e gli indirizzi IP

Due o più reti connesse tramite un gateway possono avere lo stesso indirizzo di rete. Il gateway deve a questo punto riuscire a capire a quale rete appartiene l'indirizzo IP o l'indirizzo fisico che sta trattando.il gateway può fare ciò mediante un ARP modificato, detto Proxy ARP (a volte chiamato ARP promiscuo). Un Proxy ARP crea una cache ARP che contiene voci da entrambe le reti . il gateway deve gestire le richieste e le repliche che attraversano i due network.

Un ovvio difetto del sistema ARP è che se un apparecchio non conosce il suo proprio indirizzo IP, non vi è alcun modo per generare richieste e repliche. Questo può accadere quando una nuova apparecchiatura è aggiunta alla rete. Il solo indirizzo di cui il dispositivo è a conoscenza è l'indirizzo fisico settato mediante switch o mediante sofware. Una semplice soluzione è il protocollo RARP (Reverse Address Resolution Protocol), che lavora in modo opposto al protocollo ARP, inviando un indirizzo fisico e aspettando in cambio il corrispondente indirizzo IP. La replica contenente l'indirizzo IP è inviata da un server RARP, una macchina che può fornire l'informazione. Sebbene l'apparecchiatura di origine mandi il messaggio in broadcast, le regole RARP prevedono che soltanto il server RARP possa replicare.

Domain Name System

Invece di usare l'indirizzo completo a 32 bit IP, molti sistemi utilizzano nomi più significativi per i loro apparecchi e reti. I nomi delle reti normalmente riflettono il

nome dell'organizzazione. I nomi di singoli apparecchi all'interno della rete possono variare da nomi descrittivi su piccole reti a più complesse convenzioni di denominazione in reti più grandi. La traduzione fra questi nomi e gli indirizzi IP sarebbe praticamente impossibile su scala Internet.

Per risolvere il problema dei nomi di rete, il Network Information Center (NIC) mantiene una lista di nomi di reti e dei corrispondenti indirizzi di gateway. Questo sistema crebbe da una semplice lista ad un più complicato sistema denominato Domain Name System.

Il DNS usa un'architettura gerarchica. Il primo livello di naming suddivide le reti in categorie di sottoreti, come com per le reti commerciali, mil per le militari edu per le istituzioni educative, e così via. Al di sotto di questa vi è un'altra suddivisione che identifica i singoli network, usualmente uno per ogni organizzazione. Questo è il nome di dominio (domain name) ed è univoco. Il manager del sistema dell'organizzazione può ulteriormente suddividere la rete dell'organizzazione come desidera, dove ogni sottorete è denominata sottodominio.

Il NIC ha stabilito sette nomi di dominio di primo livello. Essi sono i seguenti

.arpa	***An ARPANET-Internet identification***
.com	Commercial company
.edu	Educational institution
.gov	Any governmental body
.mil	Military
.net	Networks used by Internet Service Providers
.org	Anything that doesn't fall into one of the other categories

IL NIC permette che sia utilizzato come suffisso anche un identificatore di nazione, come .it per Italia, ecc.

DNS utilizza due sistemi per stabilire e tracciare nomi di dominio. Un name revolver su ogni rete esamina le informazioni in un nome di dominio. Se esso non può trovare un completo indirizzo IP, esso interroga un name server, che ha l'intera informazione. Il name revolver tenta di ottenere l'intero indirizzo utilizzando il proprio database, che aggiorna in maniera simile al sistema ARP quando deve interrogare un name server. Se il name server interrogato non è in grado di risolvere l'indirizzo, si può interrogare un altro name server, e così via lungo l'intera rete.