La rete di esempio[1]

Disegniamo ora una rete TCP/IP dedicata per mostrare i passi che occorrono per settarla[2], configurarla[3], e testare[4] l'implementazione TCP/IP. Il network di esempio si basa su diversi server, sebbene molte reti ne abbiano soltanto uno. Inoltre usiamo qui diversi tipi di server per mostrare come possono essere configurati. Tutte le macchine sono connesse su una rete Ethernet. In tutto questo esempio di rete ha quattro server e tre client.

Ciascuna delle sette macchine ha il suo proprio nome ed indirizzo IP. Per questa rete di esempio la maschera di indirizzo è stata scelta a caso come 147.120. La configurazione è mostrata nella figura seguente.

---

[1] sample

[2] set up

[3] configure

[4] test

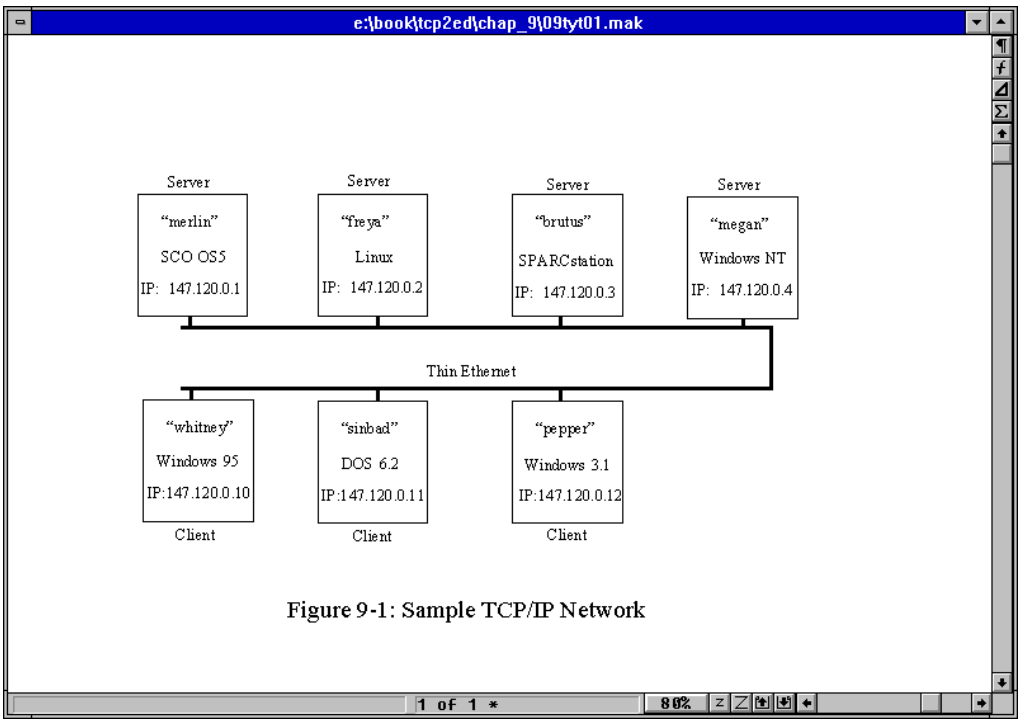


Figure 9-1: Sample TCP/IP Network

Viene affrontato prima il setup fisico[5] della rete. Ciò coinvolge l'installazione di una scheda di interfaccia di rete in ogni macchina eccetto la SPARCstation[6] [7] [8] [9]che la scheda di rete come parte della scheda madre[10]. Su ogni sistema si deve assicurare che tutti i jumper[11] [12] per i vettori di interruzione[13] [14] [15]e indirizzi di memoria[16] [17] e

---

[5] physical setup

[6] SPARC station

[7] SPARC station

[8] SPARC

[9] station

[10] motherboard

[11] jumper

[12] jumpers

[13] interrupt vectors

[14] vectors vector

[15] interrupt

IO[18] [19] [20] [21]non vadano in conflitto con le altre schede su ogni sistema. (alcune delle schede sono programmabili via software , altre sono settate da jumper o DIP switch[22]). Tutte le schede in questo sistema sono di differenti costruttori[23] per mostrare la natura indipendente delle reti TCP/IP.

I cavi devono essere disposti tra tutte le macchine, collegando le schede di rete. Nel caso Ethernet i cavi devono essere terminati in maniera appropriata. L'esempio sua la thin[24] Ethernet. I connettori Thin Ethernet BNC[25] assomigliano a delle T, con i cavi collegati agli estremi della T e lo stelo collegato alla scheda di rete. Due delle macchine formano al fine del cavo e richiedono un resistore terminatore[26] come parte della loro T. La SPARCstation usa normalmente un connettore RJ45[27].

Per testare la rete fisica, è più facile attendere finché una coppia di macchine abbia avuto una completa configurazione software. Non è necessario che siano attive tutte

---

[16] memory

[17] memory Addresses

[18] Memory IO addresses

[19] IO addresses

[20] addresses

[21] address

[22] DIP switches DIP switch DIP switch switches

[23] manufacturers manufacturer

[24] thin

[25] BNC Thin Ethernet connector Ethernet connector Thin Ethernet connector BNC BNC connector connector

[26] terminating resistor resistor

[27] RJ45

le macchine in rete, se il cavo di rete[28] è contiguo da un capo all'altro ed ogni connettore BNC è collegato ad una scheda di rete per fornire terminazione elettrica[29]. Alcuni sistemi di monitoraggio della rete[30] possono fornire informazioni di integrità[31] prima di installare la rete, ma questi sistemi non sono usualmente disponibili per amministratori di sistema che stanno giusto iniziando l'installazione, o hanno un piccolo numero di macchine da gestire (in particolare poiché i tester di rete[32] tendono ad essere costosi).

Configurare il software TCP/IP

Passiamo ora alla configurazione del software TCP/IP. La discussione si applica in maniera identica a macchine Unix, DOS, Windows(come ad altre macchine come Macintosh[33]). I filename possono cambiare con differenti sistemi operativi, ma l'approccio generale rimane valido.

La maggior parte dei sistemi operativi e packaged software TCP/IP forniscono diverse utilità, inclusi script[34] a menu[35] che aiutano ad automatizzare il processo di

---

[28] network cable

[29] electrical termination electrical termination

[30] network monitoring devices network monitoring device monitoring device monitoring device

[31] integrity information integrity information

[32] network testers network tester tester testers

[33] Macintosh

[34] scripts script

[35] menu-driven menu

installazione[36] delle applicazioni TCP/IP. Alcuni sistemi operativi (principalmente i sistemi Unix più vecchi) richiedono ancora una configurazione manuale di diversi file usando un text editor[37]. Per configurare in maniera appropriata il software TCP/IP occorre conoscere diverse informazioni prima di partire. Le informazioni necessarie sono:

- Domain name: il nome che userà l'intera rete
- System Name:il nome univoco di ogni macchina locale
- Indirizzo IP
- Driver type:ogni interfaccia alla rete deve esser associata con un driver di apparecchiatura , che istruisce il sistema operativo su come parlare all'apparecchiatura
- Broadcast address
- Network mask che identifica in maniera univoca la rete locale
- Informazioni di configurazione della scheda di rete il vettore delle interruzioni e indirizzo di memoria della scheda di rete

Il nome di dominio del sistema risulta necessario se la rete va collegata ad altre macchine fuori della rete locale. I nomi di domino possono essere inventati dall'amministratore. Se, comunque, la rete deve essere interfacciata con Internet o uno dei suoi provider, il nome di dominio dovrebbe essere approvato da Internet

[36] installation process installation

[37] text editor editor text

Network Information Center[38] (InterNIC[39]). La rete di esempio usa il domain name tcpi.com.

Come visto già precedentemente, il nome della macchina è usato per la denominazione simbolica[40] invece di costringere a specificare l'indirizzo IP. Il nome di sistema deve essere unico sulla rete locale. Altre reti possono avere macchine con lo steso nome, ma le loro maschere di rete sono diverse, così non vi è confusione nell'instradamento dei pacchetti. Nella maggior parte dei casi i nomi di sistema sono composti di otto caratteri e sono usualmente tutti caratteri minuscoli (per la tradizione Unix). Il nome del sistema può esser un mix di caratteri e cifre. Organizzazioni più ampie tendono a numerare le proprie macchine e piccole aziende danno alle proprie macchine nomi più familiari.

Il device driver istruisce il sistema operativo su come comunicare con l'interfaccia di rete (usualmente una scheda di rete o una porta seriale). Ogni interfaccia ha il suo driver specifico. La maggior parte dei sistemi operativi hanno driver inclusi nel loro software di distribuzione, sebbene alcuni richiedano software fornito con la scheda di rete. Driver generici sono disponibili per la maggior parte delle schede di rete su bulletin board system[41].

---

[38] Internet Network Information center

[39] InterNIC

[40] symbolic naming naming symbolic

[41] bulletin board system BBS

Con la maggior parte dei sistemi operativi vi è un limite sul numero massimo di device simili che sono supportati. SCO Unix per esempio, abilita fino a quattro schede Ethernet, due adattatori Token Ring[42], quattro linee Serial Line Internet Protocol[43] (SLIP) e quattro linee Point to Point Protocol[44] (PPP).

La configurazione della scheda di rete deve essere conosciuta per installare il device driver in maniera appropriata. Le schede di rete usualmente hanno diversi settaggi di configurazione[45], in dipendenza del sistema per cui sono stati sviluppati. Per le macchine basate su PC nella rete di esempio , ogni scheda deve avere un vettore di interruzione unico (chiamato IRQ[46]) ed un indirizzo di memoria e IO univoco. I settaggi di IRQ ed indirizzo su molte delle schede[47] di rete più recenti sono configurabili via software[48] , rendendo installazione e configurazione più semplice.

La maggior parte delle schede arriva con setting di default[49] che potrebbero entrare in conflitto[50] con altre schede di sistema. Gli utenti devono controllare attentamente per

---

[42] Token Ring adapters Token Ring adapter Token Ring Token

[43] Serial Line Internet Protocol Internet Protocol Serial Line Serial Line SLIP

[44] Point-to-point Protocol PPP

[45] configuration settings configuration setting configuration setting settings

[46] IRQ

[47] boards board

[48] software-configurable

[49] default settings default setting default

i conflitti, usando un sistema di diagnostica[51] se disponibile. Gli utenti Unix hanno a disposizione diverse utilità, in dipendenza del sistema operativo. SCO Unix e la maggior parte dei sistemi operativi System V Release 4 hanno l'utilità hwconfig[52], che mostra la configurazione hardware corrente. Il seguente esempio mostra il risultato di hwconfig e il risultato con l'opzione –h che da la formattazione lunga con headers[53] (rendendolo più semplice da leggere).

```
$ hwconfig

name=fpu vec=13 dma=- type=80387

name=serial base=0x3F8 offset=0x7 vec=4 dma=- unit=0 type=Standard nports=1

name=serial base=0x2F8 offset=0x7 vec=3 dma=- unit=1 type=Standard nports=1

name=floppy base=0x3F2 offset=0x5 vec=6 dma=2 unit=0 type=96ds15

name=floppy vec=- dma=- unit=1 type=135ds18

name=console vec=- dma=- unit=vga type=0 12 screens=68k

name=adapter base=0x2C00 offset=0xFF vec=11 dma=- type=arad ha=0 id=7 fts=st

name=nat base=0x300 offset=0x20 vec=7 dma=- type=NE2000 addr=00:00:6e:24:1e:3e

name=tape vec=- dma=- type=S ha=0 id=4 lun=0 ht=arad

name=disk vec=- dma=- type=S ha=0 id=0 lun=0 ht=arad fts=stdb
```

---

[50] conflict conflicts

[51] diagnostic program

[52] hwconfig

[53] headers header

```
name=Sdsk vec=- dma=- cyls=1002 hds=64 secs=32

$

$ hwconfig -h

device          address    vec  dma  comment

======        ========   ===  ===  ========

fpu             -       13   -   type=80387

serial       0x3f8-0x3ff    4   -   unit=0 type=Standard nports=1

serial       0x2f8-0x2ff    3   -   unit=1 type=Standard nports=1

floppy       0x3f2-0x3f7    6   2   unit=0 type=96ds15

floppy          -        -   -   unit=1 type=135ds18

console         -        -   -   unit=vga type=0 12 screens=68k

adapter      0x2c00-0x2cff  11   -   type=arad ha=0 id=7 fts=st

nat          0x300-0x320    7   -   type=NE2000 addr=00:00:6e:24:1e:3e

tape            -        -   -   type=S ha=0 id=4 lun=0 ht=arad

disk            -        -   -   type=S ha=0 id=0 lun=0 ht=arad fts=stdb

Sdsk            -        -   -   cyls=1002 hds=64 secs=32
```

Questo output proviene dal server SCO Unix settato per la rete di esempio. Esso ha la scheda di rete Ethernet già configurata come device[54] nat, che usa la IRQ 7 (mostrata sotto la colonna vec o interrupt vector). La linea nat mostra inoltre l'indirizzo di

[54] device devices

memoria come 300-320 (esadecimale) e il driver di device come NE2000[55] (un driver compatibile Novell NetWare). Le colonne address e vec non mostrano conflitti tra i settaggi usati per la scheda di rete ed altri device nel sistema.(la voce per l'adattatore è una scheda ad alta velocità SCSI-2[56], che controlla sia il nastro[57] sia il Sdsk[58], il hard drive primario SCSI[59]).

Gli utenti DOS possono usare la utilità diagnostica microsoft[60] MSD.EXE[61], o uno dei diversi tool di terza parte[62] come Central Point PC Tool[63] o The Norton Utilities[64] per visualizzare i vettori IRQ e gli indirizzi di memoria in uso sul sistema. Alcuni software mostrano perfino quali vettori o indirizzi sono disponibili.

L'indirizzo IP è un numero a 32 bit che deve essere univoco per ogni macchina. Se la rete deve essere connessa ad Internet l'indirizzo IP deve esser assegnato dal NIC (e viene dato usualmente quando si registra il nome di dominio).

---

[55] NE2000

[56] SCSI-2 SCSI

[57] tape tape device

[58] Sdsk device sdsk

[59] primary SCSI hard drive SCSI hard drive hard drive primary drive

[60] Microsoft Diagnostic utility Microsoft Diagnostic Diagnostic utility

[61] MSD.EXE

[62] third-party

[63] Central Point PC Tools PC Tools Central Point

[64] The Norton Utilities Norton

Il NIC ha quattro classi di indirizzi IP in uso in dipendenza dell'ampiezza della rete. La maggior parte degli indirizzi sono di classe B, sebbene alcune grandi aziende chiedono indirizzi di tipo A.

Class	Network Mask Bytes	Number of Hosts per Network	Valid Addresses
A	1	16,777,216	1.0.0.1 to 126.255.255.254
B	2	65,534	128.0.0.1 to 191.255.255.254
C	3	254	224.0.0.0 to 255.255.255.254
D	reserved		

La maschera di rete è l'indirizzo IP a cui sono tolti gli identificatori di rete , lasciando solo l'indirizzo della macchina locale. Per un indirizzo di classe A[65], questo elimina un byte, mentre per una rete di classe B[66] vengono eliminati due byte. Le piccole reti di classe C[67] eliminano tre byte , lasciando un byte per identificare la macchina locale. La rete di esempio è configurata come una macchina di classe B con una maschera di rete per gli indirizzi IP scelta in modo causale come 147.120.

L'indirizzo broadcast identifica pacchetti che devono essere inviati a tutte le macchine della rete locale. Poiché la scheda di rete usualmente ignora ogni pacchetto che non contenga al suo interno il suo specifico indirizzo IP, uno speciale indirizzo broadcast può essere settato per permettere scheda di intercettare il pacchetto che lo

[65] Class A network Class A

[66] Class B network Class B

[67] Class C network Class C

contenga. L'indirizzo broadcast[68] ha la porzione relativa al host settata a tutti 1 o tutti 0, in dipendenza delle convenzioni seguite.

Gli indirizzi broadcast possono sembrare semplici poiché vi sono soltanto due settaggi possibili. Tali indirizzi, comunque, causano problemi poiché sono usati settaggi conflittuali su una rete. BSD Unix[69] usava la convezione di tutti 0 per le versioni 4.1 e 4.2, mentre 4.3BSD[70] e SVR4[71] mossero alla convenzione di tutti 1. Lo standard Internet specifica la convenzione di tutti 1 per gli indirizzi broadcast. La rete di esempio usa la convenzione di tutti 1.

I passi da seguire per configurare TCP/IP sono i seguenti:

- Link dei driver: TCP/IP deve essere linkato al kernel del sistema operativo o caricato nella fase di boot.
- Aggiunta di informazioni sul host: fornire una lista di tutte le macchine (host) nella rete.
- Stabilire le tabelle di instradamento: fornire le informazioni per instradare in maniera corretta i pacchetti se non è sufficiente la risoluzione dei nomi.
- Settare l'accesso dell'utente: configurare il sistema per abilitare l'accesso alla rete, così come stabilire i permessi.

---

[68] broadcast address broadcast

[69] BSD Unix

[70] 4.3BSD

[71] SVR4

- Accesso ai device remoti: configurare il sistema per accedere a stampanti remote, scanner[72], CD-ROM[73] ed altri device condivisi.
- Configurare il server di dominio del nome[74]: se si usa un sistema distribuito di indirizzamento lookup[75] come Berkeley Internet Domain Server[76] (BIND) o NIS , occorre completare i file del server di nome.
- Sincronizzare i sistemi per le prestazioni: poiché un sistema su cui gira TCP/IP ha prestazioni diverse da un sistema senza TCP/IP , usualmente è richiesto qualche metodo di sincronizzazione.
- Configurazione di NFS: se si deve usare Network File System[77] (NFS[78]) occorre configurare entrambi i file system e l'accesso di utente.
- FTP anonimo[79]: se il sistema deve abilitare il FTP anonimo , occorre configurare il sistema e le cartelle pubbliche.

Configurazione di TCP/IP per Unix

La maggio parte dei sistemi operativi TCP/IP Unix si basano su diversi file di configurazione. Essi sono riassunti nella tabella seguente. I nomi dei file possono

---

[72] scanner

[73] CD-ROM

[74] name domain server domain server name name domain

[75] distributed address lookup system address lookup system lookup system lookup distributed

[76] Berkeley Internet Name Domain Server BIND

[77] Network File System

[78] NFS

[79] anonymous FTP

cambiare con differenti implementazioni del sistema Unix, ma le informazioni di configurazione sono consistenti.

File	Description
/etc/hosts	Host names
/etc/networks	Network names
/etc/services	List of known services
/etc/protocols	Supported protocols
/etc/hosts.equiv	List of trusted hosts
/etc/ftpusers	List of unwelcome FTP users
/etc/inetd.conf	List of servers started by inetd

La configurazione di SCO Unix

SCO Unix e SCO OpenServer 5[80] includono diverse utilità di configurazione per aiutare a fornire informazioni per TCP/IP e collegare il driver nel kernel correttamente. Questo non elimina la necessità di editare manualmente i molti file di configurazione e fornire informazioni circa le altre macchine sulla rete.

La maggior parte delle reti basate su Unix hanno un server principale che inizia i processi di rete. Questa macchina è qualche volta chiamata super server[81], poiché ogni macchina che fa girare processi di rete e accetta richieste da altre macchine è un server. UNIX usa il processo inetd come il server master[82] per tutti i processi di rete

---

[80] SCO OpenServer 5 OPenServer

[81] super server

[82] master server master

che devono essere attivati (usualmente contenuti nel file chiamato inetd.conf). la configurazione hardware richiede informazioni di collegamento circa la scheda di rete e il protocollo al kernel del sistema operativo. La configurazione è talvolta chiamata chain. Il processo è usualmente automatizzato da un file di script, richiedendo agli utenti di fornire il numero del vettore di interruzione, l'indirizzo di memoria IO e il tipo di scheda. Il device driver per quella scheda di rete è poi ricostruito all'interno del kernel così il driver è attivo quando il sistema parte.

Su sistemi SCO Unix viene usata una utilità chiamata netconfig, richiedendo all'utente i tre pezzi di informazione (IRQ, indirizzo e tipo di scheda) e poi ricostruisce il kernel. Sotto OpenServer 5 si possono svolgere gli stessi compiti mediante una utility GUI-driven. Quando parte, il programma netconfig di SCO Unix si presenta con questa schermata

```
$ netconfig

Currently configured chains:

 1. nfs->sco_tcp

    nfs       SCO NFS Runtime System for SCO Unix

    sco_tcp   SCO TCP/IP for UNIX

 2. sco_tcp->lo0

    sco_tcp   SCO TCP/IP for UNIX

    lo0       SCO TCP/IP Loopback driver

Available options:
```

1. Add a chain

2. Remove a chain

3. Reconfigure an element in a chain

q. Quit

Select option: Please enter a value between 1 and 3 ('q' to quit):

Poiché va aggiunto un device driver TCP/IP deve essere selezionata l'opzione 1 (Add a chain) . alcuni utenti confondono la prima chain configurata nella lista con un driver tCP per la rete e tentano di riconfigurarlo. Il primo driver elencato nel precedente output è un valore di default per NFS e dovrebbe essere lasciato stare. Non ha nulla a che fare con l'aggiunta di una scheda TCP/IP. La seconda chain elencata e il driver di loopback, che dovrebbe essere creato automaticamente per tutti i sistemi SCO quando viene installato il software del sistema operativo.

Dopo che si è indicato che deve essere aggiunta una nuova chain , il sistema chiede il tipo della chain

Num Name Description

1. lmxc SCO LAN Manager Client

2. nfs SCO NFS Runtime System for SCO UNIX

3. sco_ipx SCO IPX/SPX for UNIX

4. sco_tcp SCO TCP/IP for UNIX

Select top level of chain to Add or 'q' to quit:

Viene scelta l'opzione 4poichè si sta installando TCP/IP. Sono usati LAN Manager e IPX/SPX per l'integrazione con reti basate su DOS. Il Runtime System NFS[83] è aggiunto più tardi se NFS deve essere usato nella rete.

L'utilità netconfig presenta poi una lista di diverse schede di rete per le quali il sistema ha valori di default. Se viene mostrata la scheda installata nel sistema , deve essere scelta la voce corrispondente. Se la scheda non è sulla lista , deve essere trovata una voce compatibile[84]. Ciò richiede talvolta di scavare nella documentazione[85] della scheda alla ricerca di emulatori[86] e valori compatibili.

Il sistema richiede[87] poi il valore di IRQ della scheda, seguito dall'indirizzo di memoria. Dopo che sono stati inseriti questi valori, il sistema operativo crea le voci necessarie nel suo file di configurazione interno. Come passo finale il sistema chiede se l'utente vuole ricostruire e reimpostare i collegamenti del kernel. Questo deve esser fatto per rendere efficace l'introduzione dei nuovi driver. Dopo che il sistema si riavvia i driver diventano attivi e possono essere testati con il ping.

Possiamo effettuare il ping del localhost per prima cosa, seguito dall'indirizzo IP della macchina SCO. Ciò non testa la connessione di rete, poiché il sistema operativo non si interessa di usare la scheda di rete quando fa il pinging di se stessa. Il test,

---

[83] NFS Runtime System Runtime System Runtime

[84] compatible

[85] documentation

[86] emulation

[87] prompt

comunque, verifica che l'indirizzo IP sia settato in maniera appropriata e che il software TCP/IP sia incastonato nel kernel del sistema operativo. Un esempio di questo tipo di test è il seguente

```
# ping -c5 localhost

PING localhost (127.0.0.1): 56 data bytes

64 bytes from localhost (127.0.0.1): icmp_seq=0 ttl=64 time=10 ms

64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0 ms

64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0 ms

64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0 ms

64 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0 ms

--- localhost ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 0/2/10 ms

# ping -c5 147.120.0.1

PING 147.120.0.1 (147.120.0.1): 56 data bytes

64 bytes from merlin (147.120.0.1): icmp_seq=0 ttl=64 time=0 ms

64 bytes from merlin (147.120.0.1): icmp_seq=1 ttl=64 time=0 ms

64 bytes from merlin (147.120.0.1): icmp_seq=2 ttl=64 time=0 ms

64 bytes from merlin (147.120.0.1): icmp_seq=3 ttl=64 time=0 ms

64 bytes from merlin (147.120.0.1): icmp_seq=4 ttl=64 time=0 ms
```

```
--- 147.120.0.1 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 0/0/0 ms
```

Il software di rete TCP/IP per Unix si affida a diversi file di configurazione. Diamo un ‘occhiata a questi file per la rete di esempio.

Il file /etc/hosts contiene il nome delle altre macchine in rete ed il loro indirizzo di rete. Il file ha un aspetto del genere

```
#      @(#)hosts    1.2 Lachman System V STREAMS TCP  source

#      SCCS IDENTIFICATION

127.0.0.1          localhost tpci

147.120.0.1        merlin merlin.tpci.com

147.120.0.2        freya freya.tpci.com

147.120.0.3        brutus brutus.tpci.com

147.120.0.4        megan megan.tpci.com_

147.120.0.10       whitney whitney.tpci.com

147.120.0.11       sinbad sinbad.tpci.com

147.120.0.12       pepper pepper.tpci.com
```

IL file /etc/networks contiene una lista di nomi di reti e i loro indirizzi. Questo è un file opzionale. L’esempio seguente mostra alcune delle macchine SCO e due reti cui si collegano frequentemente le macchine locali.

```
#      @(#)networks 1.2 Lachman System V STREAMS TCP  source
```

```
#       SCCS IDENTIFICATION

loopback        127

sco             132.147

sco-hq          132.147.128

sco-mfg         132.147.64

sco-engr        132.147.192

sco-slip        132.147.32

sco-tcplab      132.147.160

sco-odtlab      132.147.1

maclean_net     147.50.1

bnr.ca          47
```

Il file /etc/services include informazioni su tutti i servizi TCP/IP supportati dal sistema. Per la rete di esempio e la maggior parte delle piccole reti, i valori di default sono accettabili. Queste voci sono cambiate soltanto se un servizio viene rimosso da TCP/IP , ad esempio per impedire accessi Telnet. Il file ha il seguente aspetto

```
#       @(#)services 5.1 Lachman System V STREAMS TCP  source

#

#    System V STREAMS TCP - Release 4.0

# Network services, Internet style

#
```

```
echo            7/tcp

echo            7/udp

discard         9/tcp         sink null

discard         9/udp         sink null

systat          11/tcp        users

daytime         13/tcp

daytime         13/udp

netstat         15/tcp

qotd            17/tcp        quote

chargen         19/tcp        ttytst source

chargen         19/udp        ttytst source

ftp             21/tcp

telnet          23/tcp

smtp            25/tcp        mail

time            37/tcp        timserver

time            37/udp        timserver

rlp             39/udp        resource      # resource location

nameserver      42/tcp        name          # IEN 116

whois           43/tcp        nicname

domain          53/tcp        nameserver    # name-domain server
```

```
domain          53/udp        nameserver

mtp             57/tcp                    # deprecated

bootps          67/udp        bootps        # bootp server

bootpc          68/udp        bootpc        # bootp client

tftp            69/udp

rje             77/tcp        netrjs

finger          79/tcp

link            87/tcp        ttylink

supdup          95/tcp

hostnames       101/tcp       hostname      # usually from sri-nic

tsap            102/tcp       osi-tp0 tp0

#csnet-cs       105/?

pop             109/tcp       postoffice

sunrpc          111/tcp

sunrpc          111/udp

auth            113/tcp       authentication

sftp            115/tcp

uucp-path       117/tcp

nntp            119/tcp       readnews untp   # USENET News Transfer Protocol

ntp             123/tcp
```

```
ntp             123/udp

nb-ns           137/udp         nbns netbios-nameservice

nb-ns           137/tcp         nbns netbios-nameservice

nb-dgm          138/udp         nbdgm netbios-datagram

nb-dgm          138/tcp         nbdgm netbios-datagram

nb-ssn          139/tcp         nbssn netbios-session

snmp            161/udp

snmp-trap       162/udp

bgp             179/tcp

#

# UNIX specific services

#

exec            512/tcp

biff            512/udp         comsat

login           513/tcp

who             513/udp         whod

shell           514/tcp         cmd             # no passwords used

syslog          514/udp

printer         515/tcp         spooler         # line printer spooler

talk            517/udp
```

```
ntalk          518/udp

efs            520/tcp                 # for LucasFilm

route          520/udp        router routed   # 521 also

timed          525/udp        timeserver

tempo          526/tcp        newdate

courier        530/tcp        rpc

conference     531/tcp        chat

netnews        532/tcp        readnews

netwall        533/udp                 # -for emergency broadcasts

uucp           540/tcp        uucpd          # uucp daemon

remotefs       556/tcp        rfs_server rfs  # Brunhoff remote filesystem

pppmsg         911/tcp                 # PPP daemon

listen         1025/tcp       listener RFS remote_file_sharing

nterm          1026/tcp       remote_login network_terminal

ingreslock     1524/tcp
```

il file /etc/hosts.equiv controlla l'accesso da altre macchine , il file /etc/ftpusers previene login non autorizzati con specifici username.

Il file /etc/inetd.conf controlla i processi iniziati dal daemon inetd quando il sistema parte. Il file appare come segue

```
#      @(#)inetd.conf    5.2 Lachman System V STREAMS TCP  source
```

```
#
#    System V STREAMS TCP - Release 4.0
#
#      SCCS IDENTIFICATION
ftp       stream    tcp  nowait    NOLUID    /etc/ftpd      ftpd
telnet    stream    tcp  nowait    NOLUID    /etc/telnetd   telnetd
shell     stream    tcp  nowait    NOLUID    /etc/rshd      rshd
login     stream    tcp  nowait    NOLUID    /etc/rlogind   rlogind
exec      stream    tcp  nowait    NOLUID    /etc/rexecd    rexecd
finger    stream    tcp  nowait    nouser    /etc/fingerd   fingerd
#uucp     stream    tcp  nowait    NOLUID    /etc/uucpd     uucpd
# Enabling this allows public read files to be accessed via TFTP.
#tftp     dgram     udp  wait      nouser    /etc/tftpd     tftpd
comsat    dgram     udp  wait      root      /etc/comsat    comsat
ntalk     dgram     udp  wait      root      /etc/talkd     talkd
#bootps   dgram     udp  wait      root      /etc/bootpd    bootpd
echo      stream    tcp  nowait    root      internal
discard   stream    tcp  nowait    root      internal
chargen   stream    tcp  nowait    root      internal
daytime   stream    tcp  nowait    root      internal
```

```
time      stream    tcp  nowait    root      internal

echo      dgram     udp  wait      root      internal

discard   dgram     udp  wait      root      internal

chargen   dgram     udp  wait      root      internal

daytime   dgram     udp  wait      root      internal

time      dgram     udp  wait      root      internal

smtp      stream    tcp  nowait    mmdf      /usr/mmdf/chans/smtpd smtpd /usr/mmdf/chans/smtpsrvr smtp
```

La maggior parte dei sistemi richiede un reboot[88] dopo che vi sono stati cambiamenti al kernel o a qualche file di configurazione , così modifiche ai file TCP/IP dovrebbero essere seguite dal reset[89] del sistema.

Quando il sistema parte i daemons TCP/IP elencati nel messaggio di startup mostrato sulla console. Ogni errore nello startup dei daemon viene mostrato sul display o inviato via posta all'amministratore di sistema. Usualmente questi messaggi sono criptici ma almeno indicano la presenza di un errore.

Configurare Linux[90]

Linux è una versione di pubblico dominio di Unix divenuta veramente popolare. In questa sezione configuriamo la versione SlakWare[91] di Linux sulla rete di esempio.

---

[88] reboot

[89] reset

[90] configuring linux

La maggior parte dei file di configurazione per TCP/IP è identica a quelli di SCO Unix e Solaris[92].

La maggior parte delle versioni di reti di Linux si appoggiano sul filesystem /proc[93] che deve esser creato prima che la rete possa essere configurata e testata. La maggior parte delle versioni Linux crea automaticamente il file quando viene installato il sistema operativo. Questo filesystem è essenzialmente un rapido punto di interfaccia per il kernel per ottenere informazioni sulla rete, così come per mantenere tabelle importanti tenute usualmente nella sottodirectory /proc/net, creata dalla routine di installazione.

Se il filesystem /proc non viene creato dal kernel Linux , occorre ricostruire il kernel e selezionare l'opzione /proc. Occorre andare alla directory sorgente (come /usr/src/Linux) e lanciare la routine di configurazione con il comando

make config

Occorre rispondere si quando viene chiesto se si vuole il supporto procfs[94]. Se non si riceve la richiesta sul supporto proc e non viene creata la directory /proc occorre eseguire l'upgrade[95] del kernel per supportare il networking.

---

[91] SlackWare

[92] Solaris

[93] /proc filesystem

[94] procfs

[95] upgrade

Ci si può assicurare che il filesystem /proc venga montato automaticamente sul sistema Linux esaminando il codice di startup del kernel. Per forzare il montaggio automatico del filesystem occorre modificare il file /etc/fstab[96] e aggiungere il comando mount[97]. Occorre verificare il file fstab per controllare se vi è una riga come la seguente

none /proc proc defaults

Se non esiste una riga del genere occorrerebbe aggiungerla la file.

Un altro passo è settare l'hostname con il comando

hostname *name*

Il passo successivo è di rendere la scheda di rete accessibile. Questo è realizzato con il comando ifconfig. Questo comando, quando viene lanciato fa lavorare lo strato di rete del kernel con l'interfaccia di rete assegnandole un indirizzo IP.

Il formato generale del comando è il seguente

ifconfig *interface_type IP_Address*

Una volta che l'interfaccia è attiva si può usare il comando route per aggiungere o rimuovere percorsi nella tabella di instradamento del kernel. Questo è necessario per abilitare la macchina locale a trovare altre macchine. Il formato generale del comando è il seguente

route add|del *IP_Address*

---

[96] /etc/fstab

[97] mount command mount

Si può visualizzare il contenuto corrente della tabella di instradamento del kernel ad ogni momento digitando il comando route da solo come nell'esempio seguente

```
$ route

Kernel Routing Table

Destination    Gateway   Genmask   Flags  MSS  Window  Use Iface

loopback       *      255.0.0.0   U    1936  0      16  lo
```

Le colonne importanti sono il destination name che mostra il nome del target configurato 8nel nostro caso loopback), la maschera da usare (Genmask) e l'interfaccia (Iface). Si può forzare il comando a mostrare gli indirizzi IP invece dei nomi simbolici con l'opzione –n.

```
$ route -n

Kernel Routing Table

Destination    Gateway   Genmask   Flags  MSS  Window  Use Iface

127.0.0.1      *      255.0.0.0   U    1936  0      16  lo
```

Una tipica configurazione di rete Linux usualmente comprende due interfacce. L'interfaccia loopback dovrebbe essere presente su tutte le macchine. Una volta che il driver loopback sia stato configurato si può aggiungere il driver Ethernet sulla rete.

L'interfaccia di loopback ha sempre l'indirizzo IP 127.0.0.1 così il file /etc/hosts dovrebbe avere una voce per questa interfaccia. Il drive di loopback potrebbe essere stato creato dal kernel durante l'installazione software , così dobbiamo controllare il file /etc/hosts per una riga del genere

localhost 127.0.0.1

Se la riga esiste il driver di loopback è a posto. Si può anche usare il comando ifconfig per sapere tutte le informazioni che esso possiede sul driver di loopback con un comando del genere

ifconfig lo

se si ottiene un messaggio di errore non esiste il drive di loopback.

Se il drive non è presente nel file /etc/hosts occorre crearlo con il comando ifconfig. Il comando

ifconfig lo 127.0.0.1

crea la riga necessari in /etc/hosts.

Poi occorre aggiungere il driver di loopback alle tabelle di instradamento del kernel con uno dei seguenti comandi

route add 127.0.0.1

or

route add localhost

Per controllare rapidamente se tutto è a posto con il driver loopback si può usare il comando ping. Se si inserisce uno dei seguenti comandi

ping localhost

or

ping 127.0.0.1

si dovrebbe avere un risultato come il seguente

```
PING localhost: 56 data bytes

64 bytes from 127.0.0.1: icmp_seq=0.  ttl=255 time=1 ms

64 bytes from 127.0.0.1: icmp_seq=1.  ttl=255 time=1 ms

64 bytes from 127.0.0.1: icmp_seq=2.  ttl=255 time=1 ms

64 bytes from 127.0.0.1: icmp_seq=3.  ttl=255 time=1 ms

64 bytes from 127.0.0.1: icmp_seq=4.  ttl=255 time=1 ms

64 bytes from 127.0.0.1: icmp_seq=5.  ttl=255 time=1 ms

64 bytes from 127.0.0.1: icmp_seq=6.  ttl=255 time=1 ms

64 bytes from 127.0.0.1: icmp_seq=7.  ttl=255 time=1 ms

^C

--- localhost PING Statistics ---

7 packets transmitted, 7 packets received, 0% packet loss

round-trip (ms) min/avg/max = 1/1/1
```

Se non si hanno risposte dal commando ping vuol dire che non è stato riconosciuto l'indirizzo IP 127.0.0.1 o il nome localhost e occorrerebbe controllare i file di configurazione e le voci di route di nuovo.

Se i file di configurazione sembrano corretti e il comando route viene accettato in maniera corretta, ma il comando ping non produce risultati si ha un problema più serio. In alcuni casi il kernel di rete non è configurato correttamente e l'intero processo deve esser condotto di nuovo.

Occorre poi aggiungere i driver Ethernet al kernel. Si può effettuare lo stesso processo di configurazione con il driver Ethernet. Per iniziare, si setta l'interfaccia Ethernet usando ifconfig. Per rendere l'interfaccia attiva , si usa il comando ifconfig con il nome del device Ethernet e l'indirizzo IP locale . per esempio usando il comando

ifconfig eth0 147.120.0.2

per settare la macchina locale con l'indirizzo 147.120.0.2. l'interfaccia è il device Ethernet /dev/eth0. non si deve specificare la maschera di rete con il comando ifconfig poiché esso deduce il valore appropriato dall'indirizzo IP inserito. Se si vuole inserire esplicitamente il valore della maschera con il comando config si può aggiungere con la keyword[98] netmask[99]:

ifconfig eth0 147.120.0.2 netmask 255.255.255.0

si può poi controllare l'interfaccia con il comando ifconfig usando il nome dell'interfaccia

```
$ ifconfig eth0

eth0        Link encap 10Mps: Ethernet Hwaddr

        inet addr 147.123.20.1 Bcast 147.123.1.255 Mask 255.255.255.0

        UP BROADCAST RUNNING  MTU 1500 Metric 1

        X packets:0 errors:0 dropped:0 overruns:0
```

[98] keyword

[99] netmask

```
TX packets:0 errors:0 dropped:0 overruns:0
```

L’ampiezza della Message Transfer Unit 8MTU) è usualmente settata al valore massimo di 1500 supportato dalle reti Ethernet.

Ora occorre inserire una voce per le tabelle di instradamento del kernel che consente al kernel di conoscere l’indirizzo di rete della macchina locale. Ciò gli permette di mandare dati ad altre macchine sulla stessa rete. L’indirizzo IP usato con il comando route per fare ciò non è l’indirizzo IP della macchina locale, ma quello della rete come una totalità senza l’identificatore locale. Per settare l’intera rete locale in un sol colpo si usa l’opzione –net del comando route. Nell’esempio precedente il comando sarebbe

```
route add -net 147.120.0
```

Ciò aggiunge tutte le macchine della rete identificata dall’indirizzo di rete 147.120.0 alla lista del kernel delle macchine accessibili. Se non si fa in questo modo si deve inserire manualmente l'indirizzo IP di ogni macchina nella rete. Un metodo alternativo è quello di usare il file /etc/networks, che può contenere una lista di nomi di rete e dei loro indirizzi IP: se si avesse una voce nel file /etc/networks per una rete chiamata maclean_net , si potrebbe aggiungere l’intera rete alla tabella di instradamento con il seguente comando

```
route add maclean_net
```

Ora possiamo configurare I file usati da TCP/IP come già fatto per il sistema SCO Unix.

Il file /etc/hosts è usato per contenere gli indirizzi di rete e i nomi simbolici, così com il driver di loopback. L'indirizzo di connessione di loopback è usualmente elencato come il nome di macchina del loopback o localhost. IL file /etc/hosts consiste dell'indirizzo di rete in una colonna e del nome simbolico nell'altra. Sebbene gli indirizzi di rete possono essere specificati in formato decimale, ottale o esadecimale, il decimale è la forma più comunemente usata. Si può specificare più di un nome simbolico su una riga separando i nomi con caratteri bianchi (spazi o tab). Il file /etc/hosts del server Linux della rete di esempio ha l'aspetto seguente

```
# network host addresses

127.0.0.1          localhost tpci

147.120.0.2        freya freya.tpci.com

147.120.0.1        merlin merlin.tpci.com

147.120.0.3        brutus brutus.tpci.com

147.120.0.4        megan megan.tpci.com_

147.120.0.10       whitney whitney.tpci.com

147.120.0.11       sinbad sinbad.tpci.com

147.120.0.12       pepper pepper.tpci.com
```

Il file /etc/protocols identifica tutti i protocolli di trasporto disponibili sul server Linux e da i loro rispettivi numeri di protocollo. Esso non è usualmente modificato dall'amministratore ma dal software di networking ed aggiornato automaticamente come parte del processo di installazione. Il file contiene il nome del protocollo, il suo

numero e ogni alias che può essere usato per quel protocollo. Il file per il server Linux è mostrato di seguito

```
# protocols

ip      0    IP   # internet protocol, pseudo protocol number

icmp    1    ICMP # internet control message protocol

igmp    2    IGMP # internet group multicast protocol

ggp     3    GGP  # gateway-gateway protocol

tcp     6    TCP  # transmission control protocol

pup     12    PUP  # PARC universal packet protocol

udp     17    UDP  # user datagram protocol

idp     22    IDP  # WhatsThis?

raw     255    RAW  # RAW IP interface
```

L'ultimo file è /etc/services per identificare i servizi di rete esistenti. Come con il file precedente esso non viene modificato dall'amministratore ma dai processi di installazione dei programmi. Il file è in formato ASCII e consiste del nome del servizio , un numero di porta, e il tipo di protocollo. Il numero di porta e il protocollo sono separati da una slash. Segue ogni alias possibile per il servizio. Un esempio è il seguente

```
# network services

echo    7/tcp

echo    7/udp
```

```
discard  9/tcp   sink  null

discard  9/udp   sink  null

ftp      21/tcp

telnet   23/tcp

smtp     25/tcp   mail mailx

tftp     69/udp

# specific services

login    513/tcp

who      513/udp   whod
```

Configurare Solaris[100]

Il Solaris SunSoft[101] è una versione di Unix così la sua configurazione è molto simile a quella vista per il sistema SCO Unix. L'interfaccia Ethernet e il driver vengono collegate al kernel quando viene caricato il sistema operativo, così nessuna delle configurazioni di device dovrebbe essere modificata. Quando il sistema operativo Solaris viene caricato, parte della procedura di configurazione chiede il nome del server e l'indirizzo IP . Questi settaggi sono poi posti nel file /etc/hosts . Si può usare

[100] Solaris

[101] SunSoft Sun Sun MIcrosystems

un editor ASCII per inserire il resto delle macchine sulla rete di esempio per completare il file come mostrato qui:

```
#
# Internet Host Table
#
127.0.0.1          localhost
147.120.0.3        brutus brutus.tpci.com loghost
147.120.0.1        merlin merlin.tpci.com
147.120.0.2        freya freya.tpci.com
147.120.0.4        megan megan.tpci.com_
147.120.0.10       whitney whitney.tpci.com
147.120.0.11       sinbad sinbad.tpci.com
147.120.0.12       pepper pepper.tpci.com
```

Il file /etc/networks è simile a quello della stazione SCO Unix

```
loopback       127
sco            132.147
sco-hq         132.147.128
sco-mfg        132.147.64
sco-engr       132.147.192
sco-slip       132.147.32
```

sco-tcplab 132.147.160

sco-odtlab 132.147.1

maclean_net 147.50.1

bnr.ca 47

Configurazione di Windows NT Server

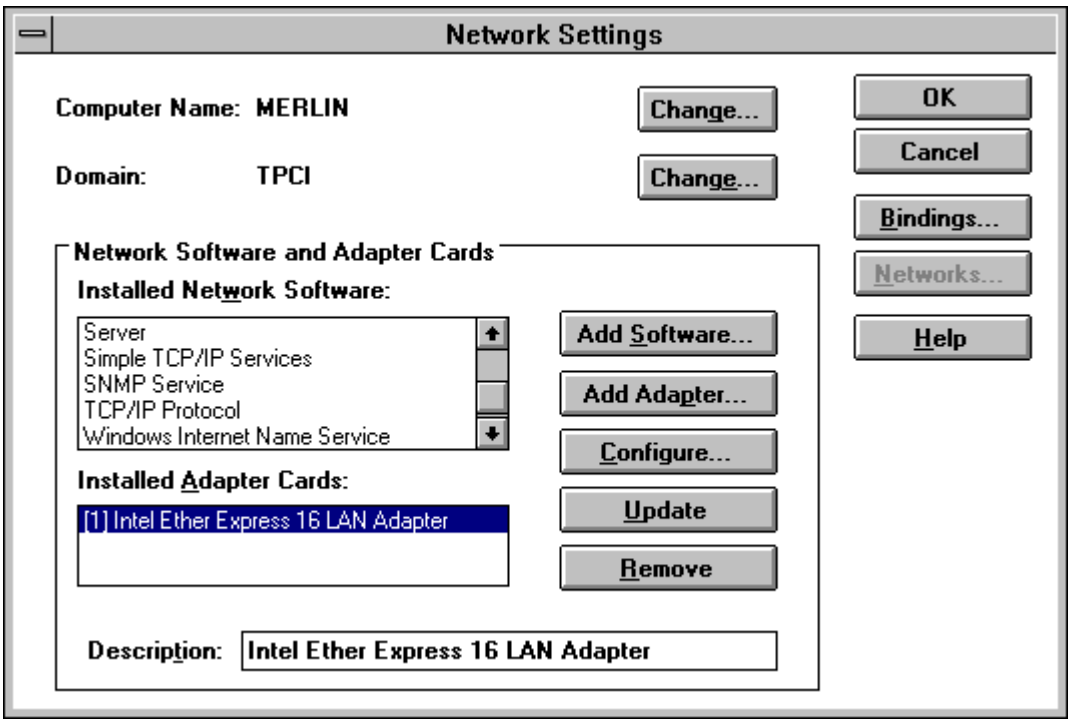
Windows[102] NT è disponibile sia nella versione server che workstation[103]. Sebbene TCP/IP sia fornito con Windows NT non viene installato come il protocollo di rete di default. Sono invece installati come protocolli di default IPX/SPX e NetBEUI. Si può controllare la presenza del software TCP/IP aprendo la finestra Network Settings [104]nel Pannello di controllo[105]. La finestra è mostrata nella figura seguente

[102] Windows Windows NT NT Windows NT server Version server version server version

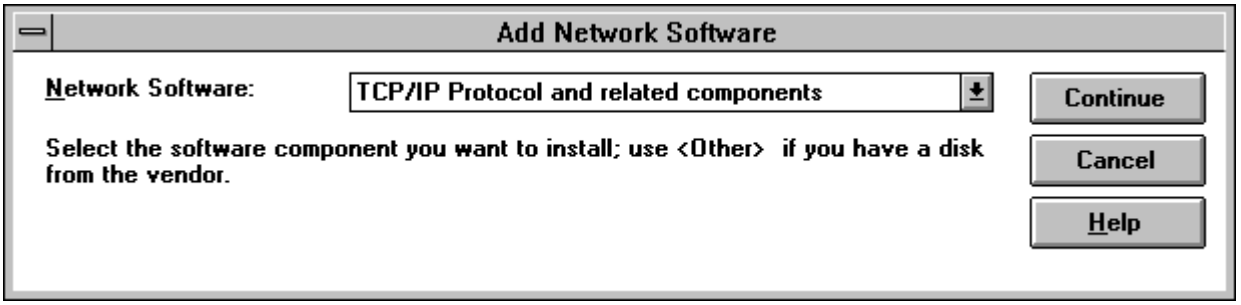
[103] Windows NT workstation version workstation version workstation

[104] Network setting Network setting window

[105] Control Panel Pannello di controllo

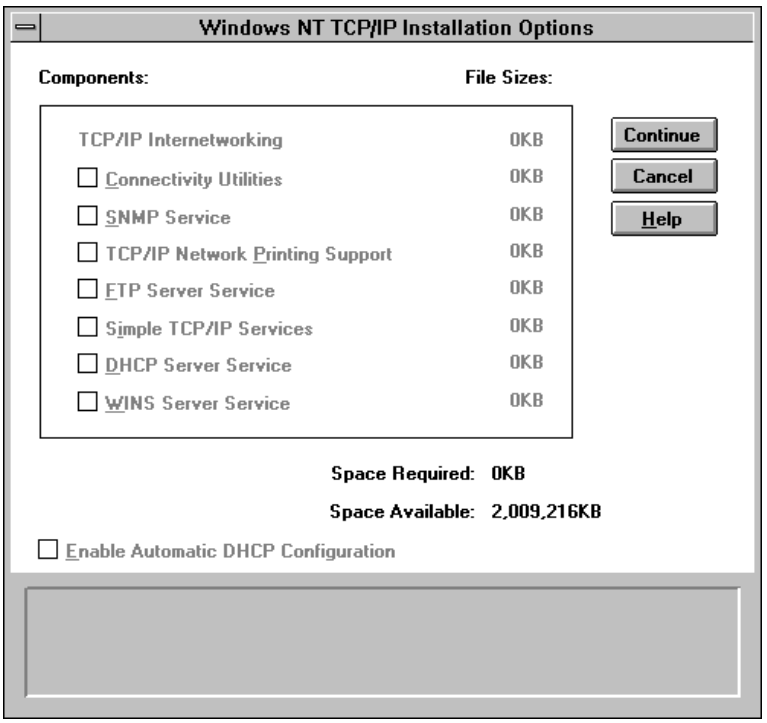


Quando si seleziona Add software il sistema controlla tutti i componenti installati e disponibili poi mostra la finestra seguente



Dopo aver selezionato TCP/IP per l'installazione, sui possono selezionare i componenti specifici Tcp/IP e altri servizi[106] che si voglia installare.

[106] TCP/IP services



La versione server di Windows NT offre diverse opzioni di configurazioni TCP/IP e servizi extra . essi includono:

- TCP/IP internetworking[107]: deve essere installato per far funzionare TCP/IP. Include driver per tCP, IP UDP e ARP, così come altri protocolli come ICMP. Sono forniti anche PPP e SLIP:
- Utilità di connettività[108]: utilità come finger[109], ping, telnet e molte altre.
- Servizio SNMP[110]: i driver SNMP sono usati per permettere l'amministrazione remota del server o workstation. Questa opzione dovrebbe essere usata se la

[107] TCP/IP INternetworking INternetworking

[108] Connectivity utilities Connectivity utility Connectivity connettività

[109] finger

[110] SNMP Service SNMP

macchina Windows NT deve essere gestita in maniera remota[111] da una workstation Unix. Il servizio SNMP è inoltre richiesto quando si voglia lanciare il Performance Monitor[112] ed avere statistiche sul comportamento di TCP/IP.

- TCP/IP Network Printing[113]: abilita le stampanti di rete[114] (quelle collegate direttamente al cavo di rete invece che ai PC). Questa opzione può esser usata anche quando si voglia inviare richieste di stampa[115] ad un'alta macchina come il Unix print server[116].
- FTP Server Service[117]
- Simple TCP/IP Services[118]: offre specialità come Daytime, Echo, Quote che sono usate da alcune applicazioni.
- DHCP Server Service[119]: installa il software server DHCP.
- Wins Server[120].

Se è stato installato un adattatore di rete quando è stato caricato Windows NT , la schede dovrebbe apparire nella lista di componenti installati nella finestra Network

---

[111] administered remotely administered remotely

[112] Performance Monitor Performance Monitor

[113] TCP/IP Network Printing Network Printing Printing

[114] network printers network printer

[115] print requestes print request

[116] Unix print server print server print

[117] FTP Server Service FTP Server

[118] Simple TCP/IP Services

[119] DHCP Server Service DHCP

[120] Wins Server Wins

settings. Se occorre aggiungere una nuova scheda al sistema, anch'esso può esser aggiunto attraverso la finestra Network settings. Il pulsante[121] Add adapter fa partire la routine di installazione[122], che richiede il tipo di scheda e poi i settaggi per l'IRQ e l'indirizzo di memoria. Dopo che la scheda è stata configurata i driver sono caricati e al reboot del sistema la scheda è disponibile.

La finestra Network settings permette di configurare ogni componente di TCP/Ip installato. Si può cambiare il nome della macchina e il nome del dominio cliccando il pulsante Change. Solo l'amministratore[123] può cambiare i nomi di macchina e di dominio.

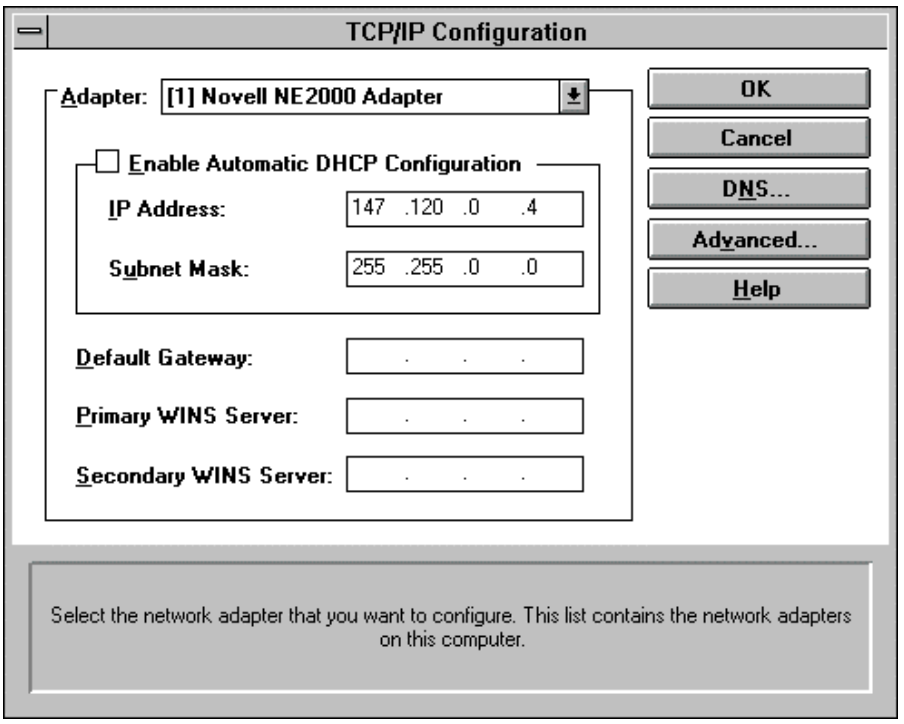
Se si seleziona la voce TCP/IP Protocol nella finestra Network Settings e poi si clicca sul pulsante Configure , appare la finestra TCP/IP Configuration mostrata nella figura seguente. Questo consente di fornire l'indirizzo IP della macchina locale (assumendo che non sia stato assegnato attraverso l'uso di un servizio come DHCP o Wins). Se si sta usando un server DHCP o Wins (diversi dalla macchina che si sta configurando) l'indirizzo IP di quel server dovrebbe essere inserito attraverso questa schermata.

---

[121] button

[122] installation routine

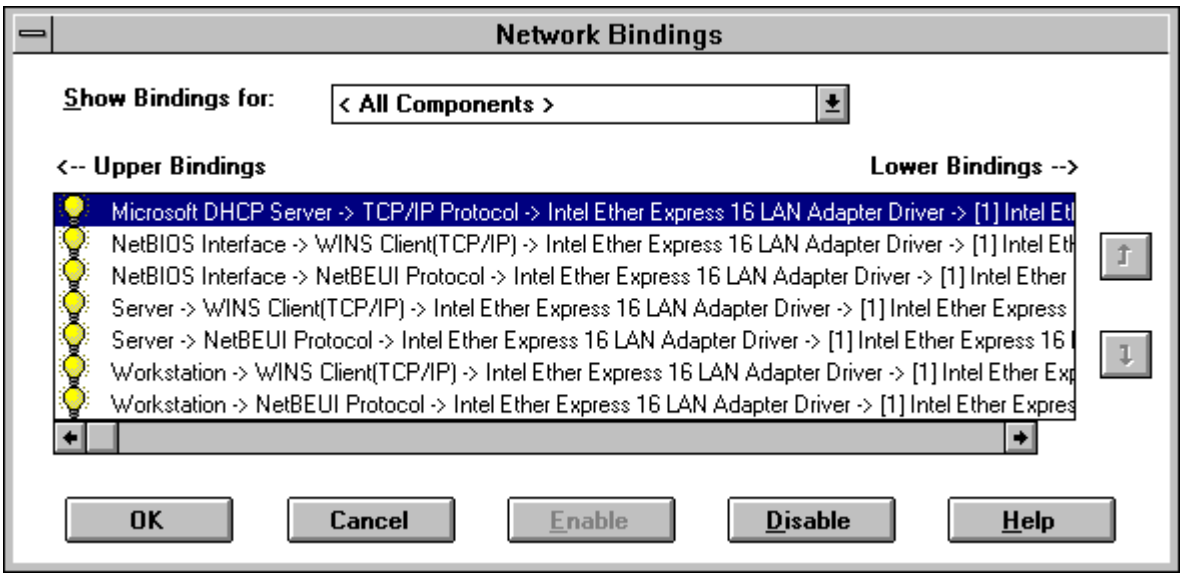
[123] administrator



Se si sta utilizzando DNS sulla rete , occorre selezionare il pulsante DNS dalla finestra di configurazione TCP/IP. Appare la finestra di configurazione DNS. Questa finestra consente di specificare l'hostname e il nome di dominio del server DNS così come ogni specifica sull'ordine di ricerca del server DNS. Infine il pulsante Advanced consente di selezionare subnet mask e indirizzi IP di gateway.

Dalla finestra Network settings si dovrebbe controllare i binding di rete per essere sicuri che tCP/IP sia usato per comunicazioni nella rete locale. Selezioniamo il pulsante Bindings per selezionare la finestra Network Bindings[124], mostrata nella figura seguente

[124] bindings network bindings



se TCP/IP è appropriatamente configurato vediamo il protocollo TCP/IP collegato all'adattatore della scheda di rete. Il collegamento dovrebbe essere attivato come mostrato da una lampadina gialla a sinistra del nome di binding. Se non è abilitato cliccare sul pulsante enable[125] in basso nella finestra.

Se altri protocolli sono abilitati e collegati alla stessa scheda e non sono necessari andrebbero disabilitati.

Testare le configurazioni del server

Il test della configurazione TCP/IP delle quattro configurazioni viste prima è diretto. Si inizia usando il comando ping su ogni macchina per assicurare che il software sta dialogando con l'hardware di rete. Sfortunatamente un ping con successo sulla macchina locale non significa sempre che si sta accedendo in maniera adeguata ala rete. Semplicemente significa che il software di rete sta elaborando la richiesta. Per

[125] enable

testare l’interfaccia di rete si deve fare il ping di tutte le altre macchine di rete. Segue l’esempio

```
$ ping merlin

PING localhost (147.120.0.1): 56 data bytes

64 bytes from localhost (147.120.0.1): icmp_seq=0 ttl=255 time=0 ms

64 bytes from localhost (147.120.0.1): icmp_seq=1 ttl=255 time=0 ms

64 bytes from localhost (147.120.0.1): icmp_seq=2 ttl=255 time=0 ms

64 bytes from localhost (147.120.0.1): icmp_seq=3 ttl=255 time=0 ms

64 bytes from localhost (147.120.0.1): icmp_seq=4 ttl=255 time=0 ms

--- localhost ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 0/0/0 ms

$ ping sinbad

PING sinbad (147.120.0.11): 56 data bytes

64 bytes from localhost (147.120.0.1): icmp_seq=0 ttl=255 time=20 ms

64 bytes from localhost (147.120.0.1): icmp_seq=1 ttl=255 time=20 ms

64 bytes from localhost (147.120.0.1): icmp_seq=2 ttl=255 time=50 ms

64 bytes from localhost (147.120.0.1): icmp_seq=3 ttl=255 time=30 ms

64 bytes from localhost (147.120.0.1): icmp_seq=4 ttl=255 time=40 ms

--- pepper ping statistics ---
```

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 20/32/50 ms

Il primo test mostra che il software è configurato in maniera appropriata . dopo la verifica della macchina locale si testa la macchina remota .il round trip[126] con successo dei pacchetti indica che la macchina remota sta funzionando in maniera corretta .

Se il ping del localhost fallisce il software era stato configurato in maniera non corretta o non vi è stato un accesso corretto al software .

Il comando netstat network status[127] è utile per monitorizzare la performance della rete e scoprire problemi.

Un problema comune è la mancanza di buffer STREAM[128] che causano la chiusura di un processo o di una connessione senza apparente ragione. L'ampiezza del buffer STREAM e il suo stato corrente possono essere controllate con il comando netstat –m:

$ netstat -m

streams allocation:

	config	alloc	free	total	max	fail
streams	292	78	214	145	79	0

[126] round-trip

[127] netstat network status command netstat

[128] STREAMS buffer buffers buffer STREAMS STREAM

```
queues                1424     360    1064     327     364       0
mblks                 5077     197    4880    3189     206       0
dblks                 4062     197    3865    3167     205       0
class 0,    4 bytes    652      51     601     357      53       0
class 1,   16 bytes    652       1     651     284       3       0
class 2,   64 bytes    768       8     760    2158      15       0
class 3,  128 bytes    872     104     768     237     106       0
class 4,  256 bytes    548      21     527      90      22       0
class 5,  512 bytes    324      12     312      13      13       0
class 6, 1024 bytes    107       0     107       1       1       0
class 7, 2048 bytes     98       0      98       1       1       0
class 8, 4096 bytes     41       0      41      26       1       0
total configured streams memory: 1183.09KB
streams memory in use: 44.66KB
maximum streams memory used: 58.28KB_
```

Il numero nella colonna fail dovrebbe essere sempre 0 altrimenti vi è un problema nella quantità di buffer allocata. Per cambiare il numero di buffer allocati devono essere cambiate le variabili di kernel e il kernel relinkato.

Pseudo tty

La maggior parte dei sistemi Unix supporta il pseudo tty (terminale falso) per abilitare macchine esterne ad usare Telnet e rlogin per l'accesso alla macchina locale. Senza uno pseudo tty la macchina remota non può stabilire una connessione.

Il sistema SCO Unix per esempio configura 32 pseudo tty per default, aggiunta o eliminazione di pseudo tty può essere realizzata attraverso una utilità di configurazione o, nel caso di SCO Unix, con il comando mkdev ptty.

User Equivalence

La user equivalence[129] consente ad un utente il rlogin ad un'altra macchina con qualche informazione di account[130] senza inserire una password[131] . questo è utile quando un utente deve accedere ad un'altra macchina frequentemente .

Per consentire l'equivalenza degli utenti UNIX richiede che l'utente esista su entrambe le macchine e che le voci in due file di configurazione corrispondano. Il file /etc/passwd che controlla l'accesso complessivo alla macchina deve avere una voce per il login name dell'utente su entrambe le macchine. Uno dei due file di configurazione deve avere informazioni circa l'utente.

---

[129] User equivalence User

[130] account

[131] password

Se viene usato il file .rhosts la user equivalence è stabilita soltanto per account specificatamente nominati nel file. Il file .rhosts usualmente risiede nella root directory . Un file .rhosts ha un aspetto del genere

```
# .rhosts file for brutus.com

merlin tparker

merlin ychow

merlin bsmallwood

pepper etreijs

pepper tparker
```

freya rmaclean

se viene usato il file hosts.equiv (che usualmente risiede nella directory /etc) la user equivalence è valida per ogni account su entrambe la macchine eccetto la root. Se il file contiene soltanto un nome di macchina sarebbe garantita user equivalence ad ogni valido utente di quella macchina eccetto la root[132]. La macchina è detta trusted host.

Sfortunatamente questo tipo di accesso pone molti problemi di sicurezza . un problema notevole è che un utente potrebbe effettuare il login come ogni altro valido utente sul sistema remoto senza usare la password. Un esempio di file hosts.equiv è il seguente

```
# hosts.equiv for brutus.com
```

[132] root

merlin tparker

pepper

freya rmaclean

IN questo esempio ogni utente del sistema remoto (pepper) potrebbe effettuare il login sulla macchina locale senza usare password. Soltanto l'utente tparker sulla macchina remota di nome merlin potrebbe effettuare il login come utente valido sulla macchina locale.

Facciamo ora un esempio ulteriore. Assumiamo che l'utente ychow , sulla macchina pepper voglia accedere ala macchina merlin sia come ychow sia come shortie sulla macchina merlin senza usare password (in altre parole ychow sulla macchina pepper è equivalente a ychow e shortie su merlin). Vi sono diversi metodi per configurare il sistema e fare questo. L'amministratore di sistema può creare un file .rhosts nella root che ha le seguenti registrazioni

pepper ychow

pepper shortie

questo permette soltanto a ychow sulla macchina pepper di effettuare il login come ychow con nessun accesso come shortie a meno che shortie sia loggiato anch'esso su pepper. Questo non è quanto richiesto. Una registrazione nel file hosts.equiv come la seguente

pepper ychow

non risolve il problema poiché ychow può ora effettuare il login come ogni altro valido utente su merlin. La soluzione richiede che ogni utente che voglia permettere a ychow di accedere alle proprie directory deve piazzare un file .rhosts nella propria home directory.

Usare ychow può ora effettuare il login in merlin usando uno dei seguenti comandi

```
rlogin merlin
```

or

```
rlogin merlin -l shortie
```

l'ultimo comando fa loggare ychow come l'utente equivalente shortie . notiamo che il file .rhosts risiede nella home directory degli utenti che vogliono permettere accesso all'utente remoto.

FTP anonimo

Il FTP anonimo abilità gli utenti da altre locazioni ad accedere un sistema senza effettuare il login. Essi ottengono il prompt FTP come usuale ma inseriscono anonymous come user name. Nella maggior parte dei sistemi la password può essere qualsiasi cosa sebbene le convenzioni richiedano che venga fornita il login name dell'utente per scopi di tracking[133]. Non vi è alcun controllo del nome naturalmente. Una volta ottenuto l'accesso l'utente può visionare le directory pubbliche e prendere

[133] tracking

file che risiedono li. Oil FTP anonimo è ecce3llente per mettere a disposizione informazioni al pubblico. Ma l'accesso aperto pone problemi di sicurezza.

Quando un utente accede con il ftp anonimo UNIX invoca un processo chiamato chroot[134] che impedisce all'utente di uscire dalla home directory . la dipendenza da chroot richiede che qualche file di configurazione del sistema risieda nella directory del ftp anonimo.

Configurare un sistema Unix per il ftp anonimo comporta lo stabilire un sistema di directory pubbliche e il cambiamento dei permessi dei file per prevenire accessi non desiderati ad altre parti del file system. Inoltre un account anonimo viene creato usando il user name ftp. Il FTP anonimo usualmente usa la home directory del ftp di utente creata quando l'utente viene generato.

Per settare un accesso ftp anonimo occorre creare un utente chiamato ftp. Con Unix questo viene fatto generalmente con uno script chiamato mkuser o un'utilità di sistema. Alternativamente l'utente può essere aggiunto con il file /etc/passwd. Un gruppo chiamato ftp dovrebbe esistere o essere creato. Una volta che esiste la home directory per l'utente ftp, occorre cambiare il suo utente e le sue identità di gruppo ad ftp (usando i comandi chown e chgrp).

Assumendo che il user ID ftp è stato creato e la home directory è /usr/ftp i passi da seguire sono mostrati qui.

```
$ cd /usr/ftp   # change to the home directory
```

---

[134] chroot

```
$ chmod 555 .   # set file permissions to r-x

$ chown ftp .   # change the owner to ftp

$ chgrp ftp .   # change the group to ftp

$ mkdir pub     # create public directory (see below)

$ chmod 777 pub # set pub dir permissions as rwx

$ mkdir bin     # create bin dir for executables

$ cd bin

$ chmod 555 bin # set bin dir to r-x

$ cp /bin/sh /bin/ls .

$ cd ..

$ mkdir etc     # create etc dir for passwd file

$ chmod 555 etc # set etc dir to r-x

$ cd etc

$ cp /etc/passwd /etc/group .

$ chmod 444 passwd group
```

$ cd ..

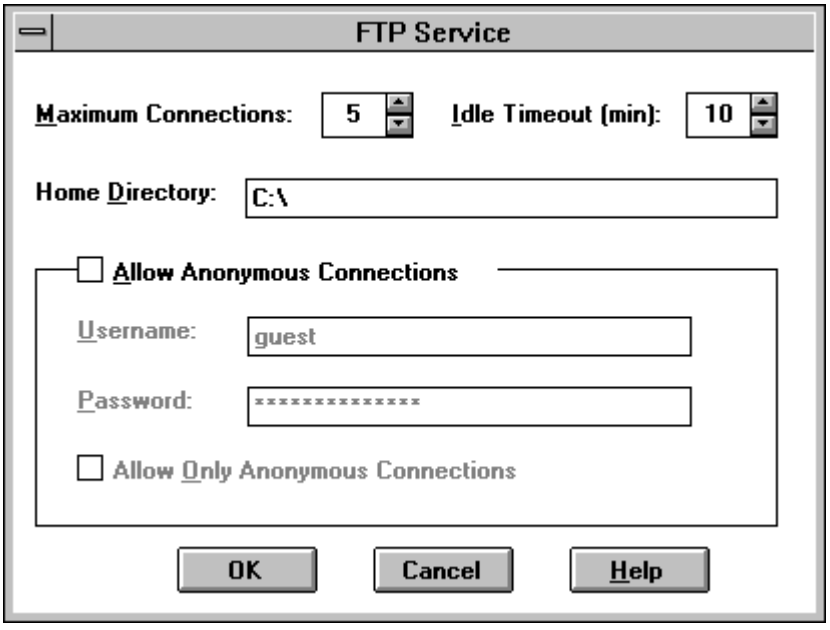
Se si vogliono creare sottodirectory all'interno della home directory per l'accesso dell'utente anonimo , occorre assicurare che essi abbiano una corretta proprietà. È pratica comune creare una directory chiamata ftp/pub per l'upload di file nel sistema. Nel precedente esempio tutte le directory eccetto pub sono settate per la lettura ed esecuzione soltanto.

I file /etc/passwd e /etc/group devono essere copiati in una directory chiamata etc (sotto la home directory user ftp dell'utente) per permettere a chroot di funzionare in maniera appropriata.

Per aiutare a prevenire accessi non desiderati può essere creato il file etc/ftpusers per contenere i nomi degli utenti che danno luogo ad una disconnessione immediata.

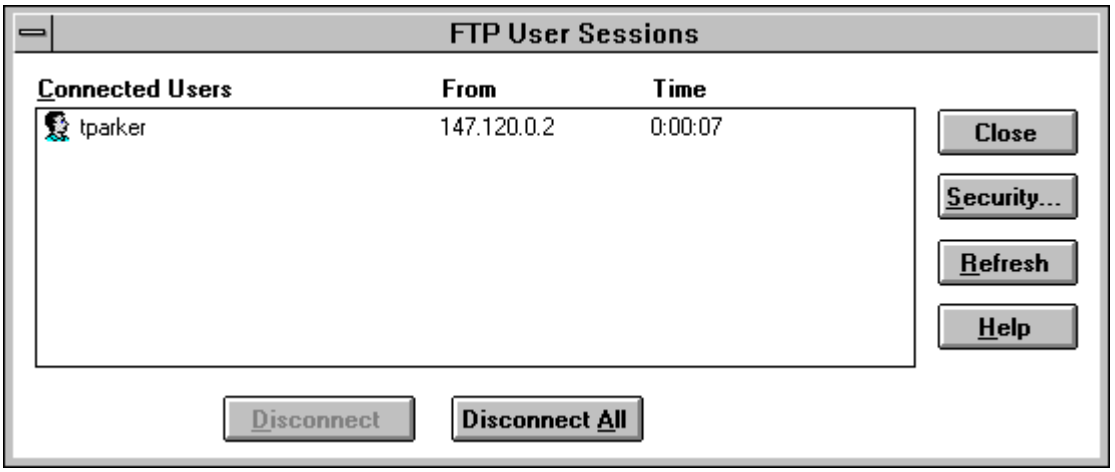
Windows NT Server abilita il ftp anonimo attraverso un meccanismo differente . occorre abilitare il server FTP. Il software per il server dovrebbe già essere stato installato.

Per configurare il software per il server FTP, si seleziona il server ftp dalla finestra Network setting e poi si clicca sul pulsante Configure. Ciò mostra la finestra di ftp service mostrata nella figura seguente.

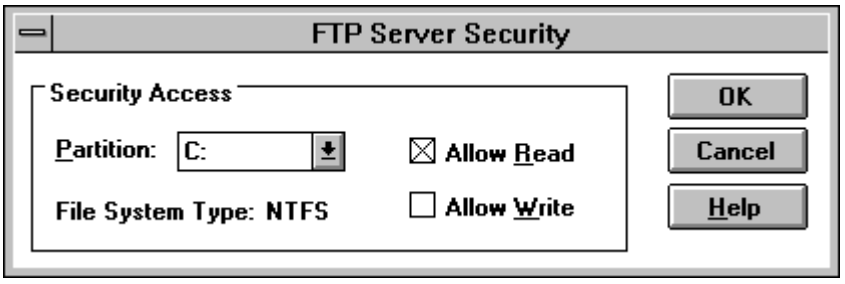


la parte finale dello schermo permette di abilitare connessioni anonime.

Si può monitorare il comportamento del ftp server attraverso l'icona FTP Server nel pannello di controllo. Esso mostra una finestra come quella della figura seguente che elenca tutti gli utenti attivi.



Alcuni setting di sicurezza possono essere controllati attraverso la finestra FTP Server cliccando sul pulsante Security. Appare la finestra seguente



Le opzioni read e write abilitano a controllare l'accesso a dischi interi.

Configurare SLIP e PPP

SLIP e PPP operano su linee seriali e richiedono alcune informazioni addizionali. Poiché le connessioni SLIP e PPP sono fra due macchine sono necessari gli indirizzi IP di sorgente e destinazione. Inoltre è necessario l'identificatore della porta incluso il vettore di interruzione usato. Le linee seriali devono essere configurate in maniera

appropriata con il loro baud rate[135]. Questo è usualmente settato in un altro file del sistema. SLIP chiede inoltre una netmask non richiesta per PPP.

PPP è più versatile di SLIP. SLIP supporta soltanto la comunicazione asincrona mentre PPP supporta sia la comunicazione sincrona che asincrona. SLIP deve avere linee dedicate mentre PP può condividere la linea con altri programmi. SLIP manca di ogni mezzo di controllo degli errori mentre PPP lo implementa.

Stampa remota

La stampa remota è un'utile caratteristica che abilita un utente su una macchina a inviare una stampa[136] ad altre macchine che hanno una stampante[137] collegata. Il sistema è chiamato Remote Line Printing[138] (RLP) ed è comunemente usato per condividere stampanti in un workgroup[139]. È utile inoltre per permettere l'accesso a stampanti speciali come laser a colori[140] e plotter[141]. RLP non supporta le printer classes[142] e alcuni sistemi operativi impongono restrizioni sulle opzioni di stampa in command line supportate.

---

[135] baud rate baud

[136] print jobs print print job

[137] printers printer

[138] Remote Line Printing Printing Remote Line RLP

[139] workgroup

[140] color lasers color laser

[141] plotter

[142] printer classes printer class

RLP funziona in maniera diversa rispetto alla normale stampa Unix . quando viene inoltrata una richiesta di stampa il sistema consulta il file di configurazione della stampante (usualmente /etc/printcap) per determinare se la stampante è locale o remota. Se la richiesta di stampa è locale si applica il processo normale. Se la richiesta è per una stampante remota il sistema locale mette in spool la richiesta ed invoca il daemon lpd, che impacchetta la richiesta di stampa e la invia alla macchina remota.

Assumendo che RLP sia disponibile nel sistema operativo (alcune versioni di Unix non supportano questa funzionalità), essa è usualmente installata e attivata con uno script o programma di utilità. Con SCO Unix un comando mkdev rlp iniziliazza lo script di installazione. Altri sistemi usano una utilità simile. Durante il processo di installazione , viene creato un certo numero di directory per lo spooling e sono fatte modifiche al file di configurazione delle stampanti. I vecchi comandi di stampa sono archiviati in una directory e nuove versioni che supportano RLP sono copiate al loro posto.

La stampa remota richiede una voce speciale nel file di configurazione ella stampante. Un esempio potrebbe essere

hplaser::lp=:rm=main_hplaser:rp=hplaser:sd=/usr/spool/lpd/hplaser

il primo campo è il nome usato dalla macchina locale per far riferimento alla stampante. Il secondo campo è usualmente vuoto. Esso definisce il nome di un file di log di errore ma non è usato sulla maggior parte dei sistemi. Il terzo campo è il nome di device per una stampante locale. Il quarto campo è il nome di rete della stampante .

esso può essere lo stesso del nome locale. Il quinto campo è il nome che il server di stampa usa per la stampante . infine il sesto campo è il nome della directory di spool. Windows NT Server ha capacità di stampa remota TCP/IP come parte della suite TCP/IP.

Configurazione di SNMP

La maggior parte delle reti usa il protocollo SNMP per monitorare la rete per problemi. Esso abilita un sistema ad esaminare ed alterare informazioni di rete gestite da altre macchine nella rete.

Molti sistemi Unix usano un daemon per far girare SNMP: quando il sistema è attivo, SNMP resta in ascolto sulle sue porte dedicate per richieste in arrivo. Usualmente sono coinvolti tre file di configurazione.

Il file /etc/snmpd.conf contiene informazioni di base richieste da SNMP. Il file contiene identificatori per i tipi di software SNMP e TCP/IP, così come il nome di contatto dell'amministratore di sistema e la locazione del sistema. Un esempio potrebbe essere il seguente

```
# snmpd.conf configuration file for tpci.com

# the first two fields are default value

descr=SNMPD Version 4.0 for SCO UNIX

objid=SCO.1.0

contact=Tim Parker x53153

location=Network Room
```

Se SNMP è settato per mandare messaggi trap[143] (messaggi di evento asincroni[144]) , esso manda pacchetti introduttivi (chiamati cold-start traps) ad altri sistemi informandoli che esso sta funzionando. Esso legge i nomi dei sistemi dal file /etc/snmp.trap, che elenca nomi , indirizzi IP e numeri di porta

```
# sample snmpd.trap file for tpci.com

# lists symbolic name, IP address, and port

test1   128.212.64.99   162

merlin   147.120.0.2    162
```

Il file /etc/snmpd.comm è una lista di comunità e coppie di indirizzi IP che specificano da chi l'agente può accettare query. Ogni linea ha il nome della community (talvolta chiamata sessione). L'indirizzo Ip del sito (un valore 0.0.0.0 abilita ogni indirizzo a comunicare), e il privilegio concesso a quel sito. Se il privilegio è settato a READ sono permesse soltanto operazioni di lettura, WRITE abilita operazioni sia di letture che di scrittura e NONE vieta ogni accesso.

```
# Copyrighted as an unpublished work.

#  Copyright 1989 INTERACTIVE Systems Corporation

# All rights reserved.

#      @(#)snmpd.comm    3.1 INTERACTIVE SNMP  source

test1 128.212.64.99 READ
```

---

[143] trap messages trap message

[144] asynchronous event messages

test2 128.212.64.15 WRITE

test3 128.212.64.15 READ

public 0.0.0.0 read

beast 0.0.0.0 read

excaliber 0.0.0.0 read

La configurazione di SNMP avviene usualmente attraverso uno script a shell interattiva. Durante l'esecuzione dello script all'utente vengono richieste tutte le informazioni necessarie per i tre file di configurazione. SCO Unix usa il comando mkdev snmp per installare il sistema.