

Funzione di Bridging su Windows XP

(le problematiche di convivenza con lo Spanning Tree)

La funzione di Bridging dei sistema operativi Windows XP e 2003 permette di implementare due tipi di funzioni:

1. Funzione di “Bridging puro” adottabile in una piccola rete di tipo Home-Office realizza una funzione di bridging tra due o più Interfacce di rete, di seguito denominate NIC (Network Interface Card). Si veda la figura 1.
2. Funzione “Link Fault-Tolerant” permette di realizzare una connessione ridondata di un PC verso la rete Switched attraverso la funzione di Bridging con STP tra due NIC (si veda la figura 1). La porta di una delle NIC viene selezionata come Root o Designated port, la porta dell’altra NIC viene selezionata come Blocking. Questa funzione è teoricamente alternativa a quella delle interfacce Fault-Tolerant (esempio Intel e 3COM) che svolgono tale funzione in modo indubbiamente più sicuro ed efficace (si veda la figura 2). Queste interfacce di tipo fault tolerant dispongono di elettronica doppia e di un meccanismo che invia un pacchetto in broadcast quando attiva la porta secondaria per forzare l'aggiornamento delle tabelle di inoltro di tutti gli switch della rete.

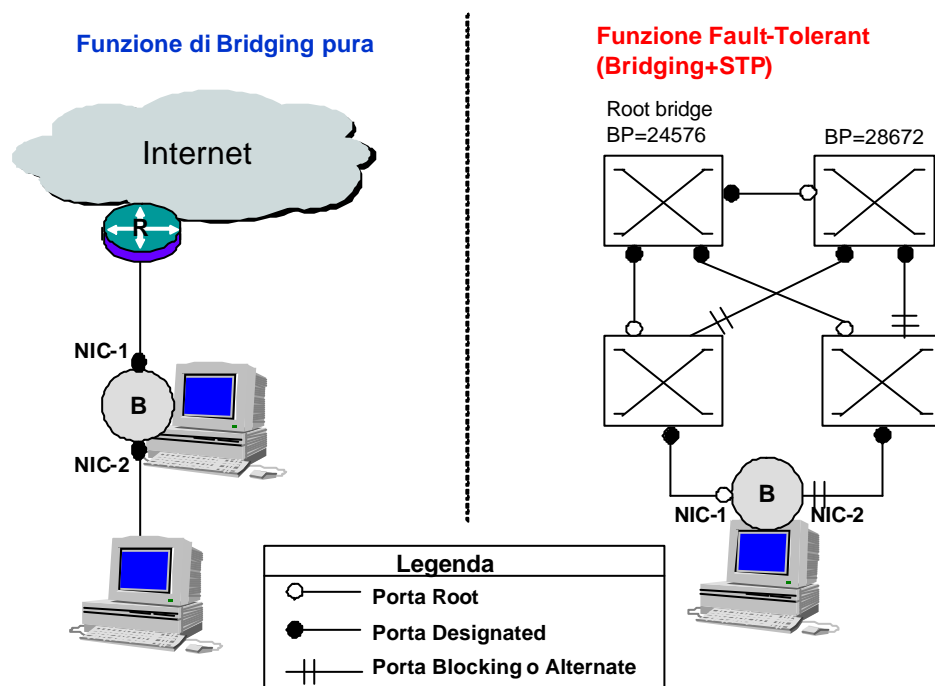
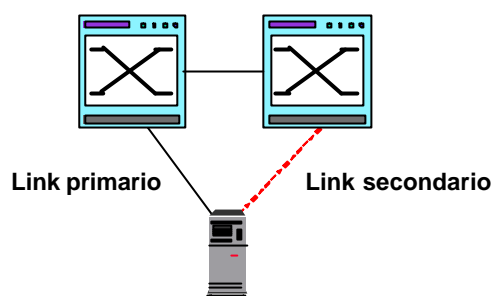


Figura 1: Le funzioni Bridging di Windows XP



Fault-tolerance d'interfaccia

- ✎ Esistono delle interfacce duali 10/100 con doppio RJ45 e singolo MAC che possono essere connesse ad hub o switch differenti
- ✎ sono in genere interfacce da server



09-LANPRJ - 30

Copyright ©2002 - M. Baldi - P. Nicoletti: see page 2

Figura 2: Interfaccia Fault-Tolerant

Sulle interfacce di tipo fault tolerant ci sono due diversi approcci dei produttori:

- Le interfacce Intel dispongono di elettronica e porte doppie nel medesimo modulo.
- La 3COM adotta due interfacce di tipo fault tolerant che occupano rispettivamente due diversi alloggiamenti PCI sul computer; il driver software dell'interfaccia si occupa degli aspetti di ridondanza automatica.

Le interfacce fault tolerant dispongono di un unico indirizzo MAC, quando viene attivata la connessione secondaria questa assume lo stesso indirizzo MAC e IP di quella primaria.

1. La funzione Bridging di Windows XP

Windows sceglie l'indirizzo MAC della NIC sulla quale è stata abilitata la funzione di bridging come una sorta d'indirizzo virtuale, opportunamente modificato, per identificare l'insieme necessario a connettere in rete il PC che funge anche da Bridge. Se c'era una NIC precedentemente configurata per la connessione alla rete questa perde la sua configurazione originaria e viene inglobata nell'insieme della funzione di Bridging che compare sulle risorse di rete con un'icona che richiama il ponte (bridge). Nelle risorse di rete compaiono quindi le icone delle due NIC più il Bridge. Cliccando sulle proprietà del Bridge è possibile assegnare a quest'insieme le proprietà classiche di un'interfaccia di rete (IP address, default gateway, DNS). Si veda la figura 3.

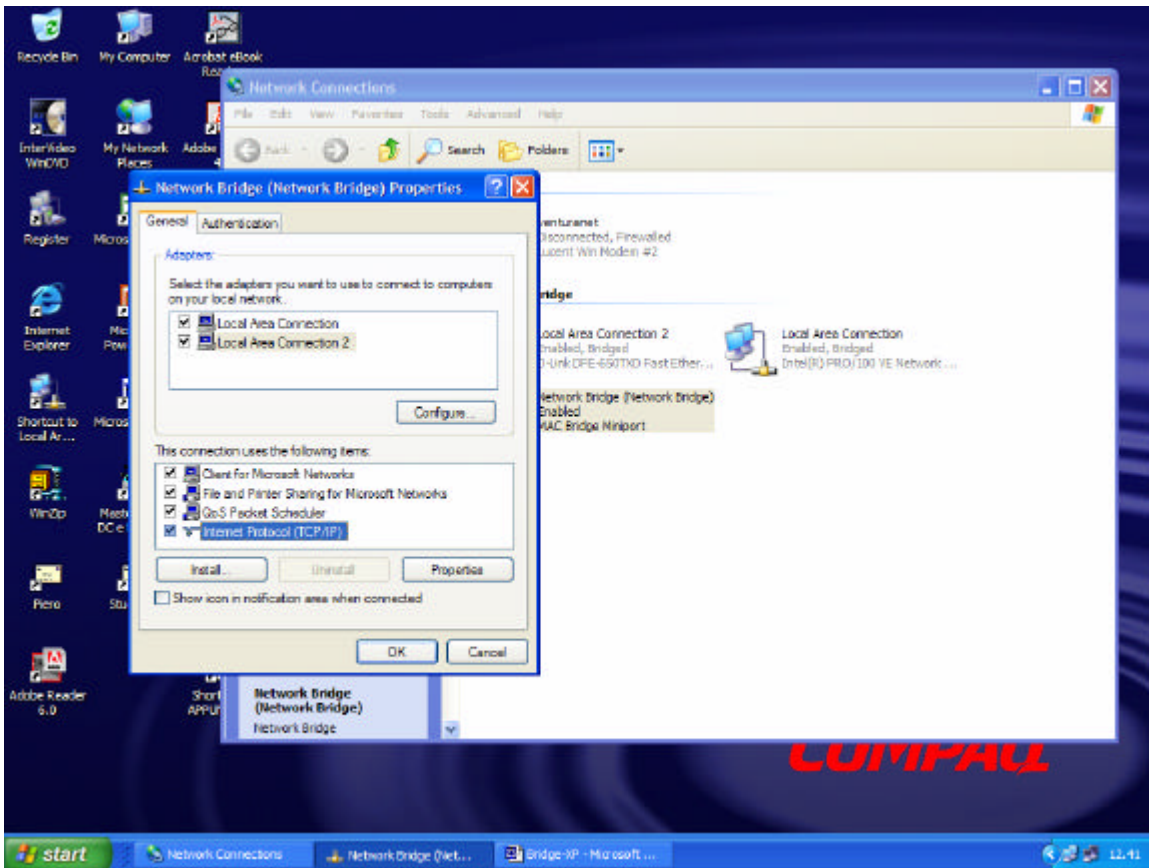


Figura 3: Configurazione proprietà del Bridge XP

L'insieme Bridge assumerà un unico indirizzo MAC che equivale a quello dell'interfaccia di rete da cui si è partiti per la configurazione della funzione di bridging con l'aggiunta del secondo bit meno significativo del primo Byte che viene impostato a 1 e fa diventare l'indirizzo MAC di tipo locale.

Nell'esempio è stata configurata la funzione di bridging partendo da un'interfaccia Dlink che aveva l'indirizzo MAC 0050BA7D29F5 e dopo la configurazione di bridging l'insieme ha assunto l'indirizzo MAC 0250BA7D29F5.

A seguito della configurazione della funzione Bridging il PC userà l'indirizzo MAC modificato di tipo locale sia per i pacchetti destinati ad altre stazioni, sia come indirizzo MAC per identificare il bridge nelle BPDU (Bridge Protocol Data Unit) utilizzate dal protocollo di SpanningTree.

Cattura di pacchetto di ICMP Echo Reply dove si può notare l'indirizzo MAC modificato

```
SUMMARY Delta T Destination Source Summary
2 0.0014 [192.168.54.9] [192.168.54.1] DLC Ethertype=0800, size=74
bytes
IP D=[192.168.54.9]
S=[192.168.54.1] LEN=40 ID=7424
ICMP Echo reply

DLC: ----- DLC Header -----
DLC:
DLC: Frame 2 arrived at 11:08:39.4786; frame size is 74 (004A hex) bytes.
DLC: Destination = Station 0250BA7D29F5
DLC: Source = Station 000427FD6CEE
```

```

DLC:  Ethertype = 0800 (IP)
DLC:
IP:   ----- IP Header -----
IP:
IP:   Version = 4, header length = 20 bytes
IP:   Type of service = 00
IP:       000. .... = routine
IP:       ...0 .... = normal delay
IP:       .... 0... = normal throughput
IP:       .... .0.. = normal reliability
IP:   Total length = 60 bytes
IP:   Identification = 7424
IP:   Flags = 0X
IP:       .0.. .... = may fragment
IP:       ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live = 255 seconds/hops
IP:   Protocol = 1 (ICMP)
IP:   Header checksum = B165 (correct)
IP:   Source address = [192.168.54.1]
IP:   Destination address = [192.168.54.9]
IP:   No options
IP:
ICMP: ----- ICMP header -----
ICMP:
ICMP: Type = 0 (Echo reply)
ICMP: Code = 0
ICMP: Checksum = 325C (correct)
ICMP: Identifier = 512
ICMP: Sequence number = 8448
ICMP: [32 bytes of data]
ICMP:
ICMP: [Normal end of "ICMP header".]
ICMP:

```

2. Funzione “Link Fault Tolerant” tramite Bridging con STP

Lo Spanning Tree è automaticamente abilitato quando viene configurata la funzione di Bridging, ma esso opera la potatura del link alternativo solo se esiste una richiusura o maglia.

Questo tipo di connessione può essere molto pericolosa se inserita in una rete switched che non è opportunamente configurata in quanto potrebbe causare loop di rete con le disastrose conseguenze di tempeste di broadcast per effetto della duplicazione di questo tipo di pacchetti sui percorsi circolari.

I problemi legati alla configurazione del Bridging di Windows XP:

1. Il parametro di Bridge Priority è impostato al valore di default di 32768 (8000 esadecimale), quindi se non è stato forzato un particolare Switch della rete a diventare Root Bridge, attraverso la riduzione del parametro Bridge Priority, può diventarlo un PC con funzione di bridging tra due NIC.
2. I timer dello Spanning Tree non sono quelli di default previsti dallo standard IEEE 802.1D, ma sono drammaticamente più bassi. Il parametro Max Age invece di essere impostato a 20 s è impostato a 8 s, il parametro Forward Delay invece di essere impostato a 15 s è impostato a 5 s, l'Hello Time è impostato al valore di default previsto dallo standard che è pari a 2 s. Con tali parametri si può avere una rete magliata costituita da un solo bridge in quanto il parametro Maximum Bridge Diameter scende da 7 a 1.

Nella cattura della BPDU, di seguito mostrata, generata da un PC che è diventato Root Bridge si possono notare i valori dei parametri sopra indicati.

C:\ENCAP\XPBR1.ENC, Page 4

LLC C D=42 S=42 UI
BPDU S: Pri=8000 Port=8000

Root: Pri=8000 Addr=0250BA7D29F5 Cost=0

```
DLC: ----- DLC Header -----
DLC:
DLC: Frame 4 arrived at 11:01:52.6027; frame size is 60 (003C hex) bytes.
DLC: Destination = Multicast 0180C2000000, Bridge_Group_Addr
DLC: Source      = Station 0050BA7D29F5
DLC: 802.3 length = 38
DLC:
LLC: ----- LLC Header -----
LLC:
LLC: DSAP Address = 42, DSAP IG Bit = 00 (Individual Address)
LLC: SSAP Address = 42, SSAP CR Bit = 00 (Command)
LLC: Unnumbered frame: UI
LLC:
BPDU: ----- Bridge Protocol Data Unit Header -----
BPDU:
BPDU: Protocol Identifier = 0000
BPDU: Protocol Version   = 00
BPDU:
BPDU: BPDU Type = 00 (Configuration)
BPDU:
BPDU: BPDU Flags = 00
BPDU:  0... .... = Not Topology Change Acknowledgment
BPDU:  .... ...0 = Not Topology Change
BPDU:  .000 000. = Unused
BPDU:
BPDU: Root Identifier   = 8000.0250BA7D29F5
BPDU:   Priority        = 8000
BPDU:   MAC Address     = 0250BA7D29F5
BPDU:
BPDU: Root Path Cost    = 0
BPDU:
BPDU: Sending Bridge Id  = 8000.0250BA7D29F5.8000
BPDU:   Priority          = 8000
BPDU:   MAC Address       = 0250BA7D29F5
BPDU:   Port              = 8000
BPDU: Message Age        = 0.000 seconds
BPDU: Information Lifetime = 8.000 seconds
BPDU: Root Hello Time     = 2.000 seconds
BPDU: Forward Delay       = 5.000 seconds
BPDU:
DLC: Frame padding= 8 bytes
```

2.1 Problemi non completamente risolti con Root Bridge predefinito

Qualora la funzione di “Link Fault Tolerant” tramite Bridging con STP sia abilitata su PC in una rete dove è stato configurato uno switch adeguato a diventare Root Bridge il problema diventa meno critico, ma non è completamente risolto se la rete è grande, magari di campus, e coinvolge parecchi switch. La presenza di due o più PC con la funzione di Fault Tolerance tramite STP abilitata può incrementare di due il Maximum Bridge Diameter della rete che potrebbe quindi superare il default pari a 7 con possibilità che inneschino dei loop. In questo caso i timer per tutta la rete diventano quelli dello switch che è diventato Root Bridge.

Se nella rete il diametro massimo è già prossimo o pari a 7 si può decidere di modificare opportunamente i timer sullo Switch che è Root Bridge. Per esempio si può impostare il Max Age al valore di 24 s, il Forward Delay al valore di 18 s e lasciare l’Hello Time a 2 s, ottenendo un Maximum Bridge Diameter pari a 9 bridge/switch.

Nella BPDU catturata e di seguito mostrata si può notare che:

- è stata trasmessa dalla funzione di Bridging del PC;
- il Root Bridge della rete è diventato uno Switch al quale è stata impostata la Bridge Priority al valore 24576 (6000 esadecimale) ed i timer sono stati modificati: il Max Age al valore di 24 s, il Forward Delay al valore di 18 s e l’Hello Time al valore di 2 s.

```
SUMMARY Delta T Destination Source Summary
M 1 Bridge_Group... 0050BA7D29F5 DLC 802.3 size=38 bytes
LLC C D=42 S=42 UI
BPDU S: Pri=8000 Port=8000
```

```
Root: Pri=6000 Addr=00E01EEC3C84 Cost=100
```

```
DLC: ----- DLC Header -----
DLC:
DLC: Frame 1 arrived at 16:59:50.4616; frame size is 60 (003C hex) bytes.
DLC: Destination = Multicast 0180C2000000, Bridge_Group_Addr
DLC: Source = Station 0050BA7D29F5
DLC: 802.3 length = 38
DLC:
LLC: ----- LLC Header -----
LLC:
LLC: DSAP Address = 42, DSAP IG Bit = 00 (Individual Address)
LLC: SSAP Address = 42, SSAP CR Bit = 00 (Command)
LLC: Unnumbered frame: UI
LLC:
BPDU: ----- Bridge Protocol Data Unit Header -----
BPDU:
BPDU: Protocol Identifier = 0000
BPDU: Protocol Version = 00
BPDU:
BPDU: BPDU Type = 00 (Configuration)
BPDU:
BPDU: BPDU Flags = 00
BPDU: 0... .. = Not Topology Change Acknowledgment
BPDU: .... ..0 = Not Topology Change
BPDU: .000 000. = Unused
```

```
BPDU:
BPDU: Root Identifier      = 6000.00E01EEC3C84
BPDU:   Priority            = 6000
BPDU:   MAC Address        = 00E01EEC3C84
BPDU:
BPDU: Root Path Cost       = 100
BPDU:
BPDU: Sending Bridge Id    = 8000.0250BA7D29F5.8000
BPDU:   Priority            = 8000
BPDU:   MAC Address        = 0250BA7D29F5
BPDU:   Port                = 8000
BPDU: Message Age          = 0.003 seconds
BPDU: Information Lifetime = 24.000 seconds
BPDU: Root Hello Time     = 2.000 seconds
BPDU: Forward Delay       = 18.000 seconds
BPDU:
DLC:  Frame padding= 8 bytes
```

2.2 Un approccio di massima prudenza da parte del gestore di rete

Il gestore di rete potrebbe cautelarsi impedendo agli utenti di abilitare la funzione di Bridging sui PC. Su switch come quelli della Cisco è disponibile una funzione particolare denominata “BPDU GUARD” che se configurata su una porta dello Switch causa lo stato di “Error Disable” alla ricezione della prima BPDU. Per riabilitare la porta bisogna dapprima metterla in stato di Shutdown e successivamente No-Shutdown. Nel caso in cui un utente configurasse la funzione di Bridging sul PC alla prima Bridge PDU che questo invia per proporsi come Root Bridge le porte degli Switch a cui questo è connesso vanno in stato di “Error Disable”.

Questo approccio potrebbe sembrare esageratamente prudente, ma non va dimenticato che quand’anche la configurazione dei parametri di Spanning Tree sugli Switch sia ottimale è sufficiente che ci sia una condizione di hang sul processo di spanning tree del PC il quale, essendo partecipe insieme a tutti gli Switch della rete all’algoritmo di STP, potrebbe causare il loop di tutta rete.