Jan 2008

Laboratory Handbook

Network Troubleshooting

Network Solution for Monitoring and Maintenance Your Networking.

Vol. **1** Rev. **1**

Author:
Heru Sukoco

Improving MIS Capacity - IMHERE PROGRAM
Information System Development Office (KPSI)
Bogor Agricultural University (IPB)
Bogor – West Java - Indonesia

"Let's use Open Source Software"
"Bring your better future with Linux"

Brief Bibliography

DOC/10-25.10.2007

Heru Sukoco, lahir di Jakarta, 13 Juli 1975, merupakan anak pertama dari tiga bersaudara. Saat ini penulis bekerja sebagai staf pengajar tetap di Departemen Ilmu Komputer FMIPA IPB Bagian Net-Centric Computing sejak tahun 1999.

Alamat Kantor:
1) Departemen Ilmu Komputer FMIPA IPB
Jl. Raya Pajajaran Baranangsiang III 16144
Telp./Fax. +62-251-356653
Gedung Departemen Ilmu Komputer Lt. 5 – 6
Jl. Raya Darmaga Kampus IPB Darmaga 16680
Telp./Fax. +62-251-625584

2) Kantor Pengembangan Sistem Informasi (KPSI) IPB
Jl. Raya Darmaga Gedung Rektorat Lt. 2 Kampus IPB Darmaga
Bogor – Jawa Barat 16680
Telp./Fax. +62-251-623936L
Email: hsrkom@ipb.ac.id, hsrkom@ilkom.fmipa.ipb.ac.id,
hsrkom@yahoo.com
Website: http://web.ipb.ac.id/~hsrkom

EDUCATION

1994 – 1999	S1, Sarjana Komputer, Departemen Ilmu Komputer FMIPA IPB
2002 – 2005	S2, Magister Sistem Informasi Telekomunikasi, Departemen Teknik Elektro, ITB

EXPERIENCE

1999–sekarang	Staf Dosen Departemen Ilmu Komputer FMIPA IPB
2006–sekarang	Kepala Bagian Net-centric Computing
2003–sekarang	Kepala Bidang Infrastruktur & Jaringan Komputer KPSI IPB
1998 – 2002	Ketua Kelompok Pengguna Linux Indonesia (KPLI) Regional Bogor

Selain sebagai pengajar, penulis juga aktif menulis buku-buku Teknologi Informasi (TI) untuk Siswa Sekolah Dasar dan konsultan TI di berbagai instansi pendidikan, pemerintah dan swasta.

SKILLS

Bidang penelitian dan pengajaran yang diminati penulis saat ini adalah komputasi di bidang Net-centric, seperti *network design, network and database programming, network analysis and performance, network simulation, high-speed computing, wireless and mobile technology.*

بِسْمِ اللهِ الرَّحْمنِ الرَّحِيْمِ

Dengan menyebut nama الله Yang Maha Pengasih lagi Maha Penyayang

Revisi: 1.0, Edisi ke-1 (November 2007 – Januari 2008)

Lisensi Dokumen:

Semua informasi yang Anda temukan pada buku ini telah dikompilasi dengan perhatian yang sungguh-sungguh namun penulis tidak menjamin kelengkapan isi dan akurasi lengkapnya.

Preamble/Mukadimah

Dokumen ini ditulis dalam rangka peningkatan kapasitas kompetensi sumber daya manusia di bidang jaringan komputer pada program I-MHERE IPB tahun 2007. Panduan ini berisikan tips dan trik untuk troubleshooting seputar jaringan komputer khususnya yang sering terjadi di Jaringan Backbone/Core maupun Distribusi IPBNet. Namun demikian, mudah-mudahan ini juga dapat digunakan untuk troubleshooting jaringan secara umum yang berbasiskan TCP/IP. Tool-tools yang digunakan pada dokumen ini berbasiskan sistem operasi open source (Linux) dan propriatery (Microsoft Windows) dan disajikan secara langkah demi langkah dengan menyertakan penjelasan singkat untuk memudahkan pengguna memahami tool dan hasilnya.

Melalui tulisan ini diharapkan para pembaca, baik umum maupun pembaca awam TI sekalipun, dapat mengimplementasikan dan memahami penggunaan alat-alat troubleshooting serta hasilnya di lingkungan jaringan Anda masing-masing. Selain itu, tulisan dan dokumentasi ini bertujuan untuk menjadi buku pegangan bagi para penanggung jawab teknis dan jaringan di lingkungan Institut Pertanian Bogor. Mudah-mudahan panduan dan dokumen ini dapat memberikan manfaat bagi para pembacanya.

Feedback/Umpan-balik

Kesempurnaan hanyalah datang dari **Allah SWT** dan sebagai manusia yang tidak pernah luput dari kesalahan/kekhilafan, penulis sangat berharap saran, masukan dan kritik membangun dari para pembaca demi perbaikan dokumen ini. Saran, masukan dan kritik membangun dapat dikirimkan melalui **email** ke alamat: hsrkom@ipb.ac.id (**CC**: hsrkom@yahoo.com).

Acknowledgments/Penghargaan

Dengan penuh keikhlasan dan keridhaan hati, penulis mengucapkan rasa syukur kehadirat ***Illahi Rabbi*** atas kesehatan, kesempatan, dan rahmat yang telah diberikan-Nya. Selain itu, penghargaan yang tinggi juga penulis ucapkan kepada semua pihak atas komitmennya membantu dalam penulisan dokumen ini, baik secara langsung maupun tidak langsung, terutama untuk Istriku “Sri Retno Martuti” sebagai editor, anak-anakku “Anisa Fatimah Azzahra” dan Muhammad Naufal Afif” sebagai penghiburku di saat jenuh, I-MHERE IPB sebagai sponsor kegiatan “Improving MIS Capacity”, dan POSS IPB sebagai tempat repository aplikasi dan dokumen *open source.*

Dokumen ini tidaklah mungkin dapat ditulis dan diterbitkan tanpa dukungan semua pihak dan melalui tulisan ini penulis berharap setidaknya ada sedikit pengetahuan yang dapat disumbangkan kepada para pembaca.

Semoga bermanfaat dan berkah. Amin.

Bogor, Januari 2008
Penulis,

Heru Sukoco

Email: hsrkom@ipb.ac.id
Website: http://web.ipb.ac.id/~hsrkom
Yahoo! ID: hsrkom@yahoo.com
Friendster: hsrkom@yahoo.com

DAFTAR ISI

DAFTAR GAMBAR

Network Troubleshooting

Sebelum kita melakukan troubleshooting pada jaringan dan menggunakan beberapa toolnya (alat software/hardware), ada baiknya kita memahami apa itu Network Troubleshooting. Network troubleshooting dapat diartikan sebagai cara atau teknik mengenal (*recognizing*) dan mendiagnosa (*diagnosing*) masalah-masalah jaringan dengan tujuan untuk menjaga agar jaringan kita tetap berjalan dengan normal. Sebagai seorang administrator jaringan, teknisi jaringan, dan spesialis jaringan, perhatian utama kita adalah memelihara konektivitas dari semua perangkat jaringan (dalam sebuah proses biasanya kita sebut *fault management*). Kita juga secara rutin dan berkelanjutan haruslah mengevaluasi dan meningkatkan kinerja jaringan. Karena terkadang masalah-masalah jaringan yang serius dapat mengindikasikan masalah kinerja dari sebuah jaringan sehingga dengan perhatian yang lebih serius dapat membantu kita mengetahuinya lebih dini sebelum menjadi masalah yang lebih serius.

Network troubleshooting yang akan kita lakukan adalah berbasiskan pada layanan-layanan di TCP/IP atau Internet. Beberapa alat troubleshooting untuk software yang digunakan berbasiskan pada platform sistem operasi (OS) Linux dan Windows. Hal-hal yang sering terjadi dalam jaringan di antaranya adalah:

1. Masalah Konektivitas

Masalah konekvitas terjadi ketika suatu *end stations* (seperti komputer, hub/switch, router) tidak dapat berkomunikasi satu sama lain baik di lingkungan jaringan LAN *(local area network)* maupun WAN (*wide area network*). Menggunakan alat-alat manajemen berupa software maupun hardware, kita sering dapat mengatasinya bahkan sebelum pengguna lainnya mendapat peringatan. Masalah konektivitas meliputi:

a. Kehilangan Konektivitas (*Loss of connectivity*) - Ketika para pengguna tidak dapat mengakses jaringan kita maka keefektifan organisasi Anda adalah lemah sehingga Anda harus dengan segera memperbaikinya.

b. Konektivitas terputus-putus atau tidak stabil (*Intermittent connectivity*) – Kendati para pengguna memiliki akses ke sumber daya jaringan beberapa kali tetapi mereka kadangkala masih menghadapi koneksi jaringan yang 'mati' (*periods of downtime*). Masalah konektivitas yang terputus-putus dapat mengindikasikan bahwa jaringan kita berada pada ambang kerusakan yang lebih parah. Jika konektivitas tidak menentu (aneh) segeralah kita melakukan pengamatan dan penyelidikan pada masalah tersebut.

c. Masalah Timeout - Timeouts menyebabkan kehilangan konektivitas (*loss of connectivity*) tetapi lebih sering dihubungkan dengan kinerja jaringan yang buruk.

2. Masalah Kinerja Jaringan

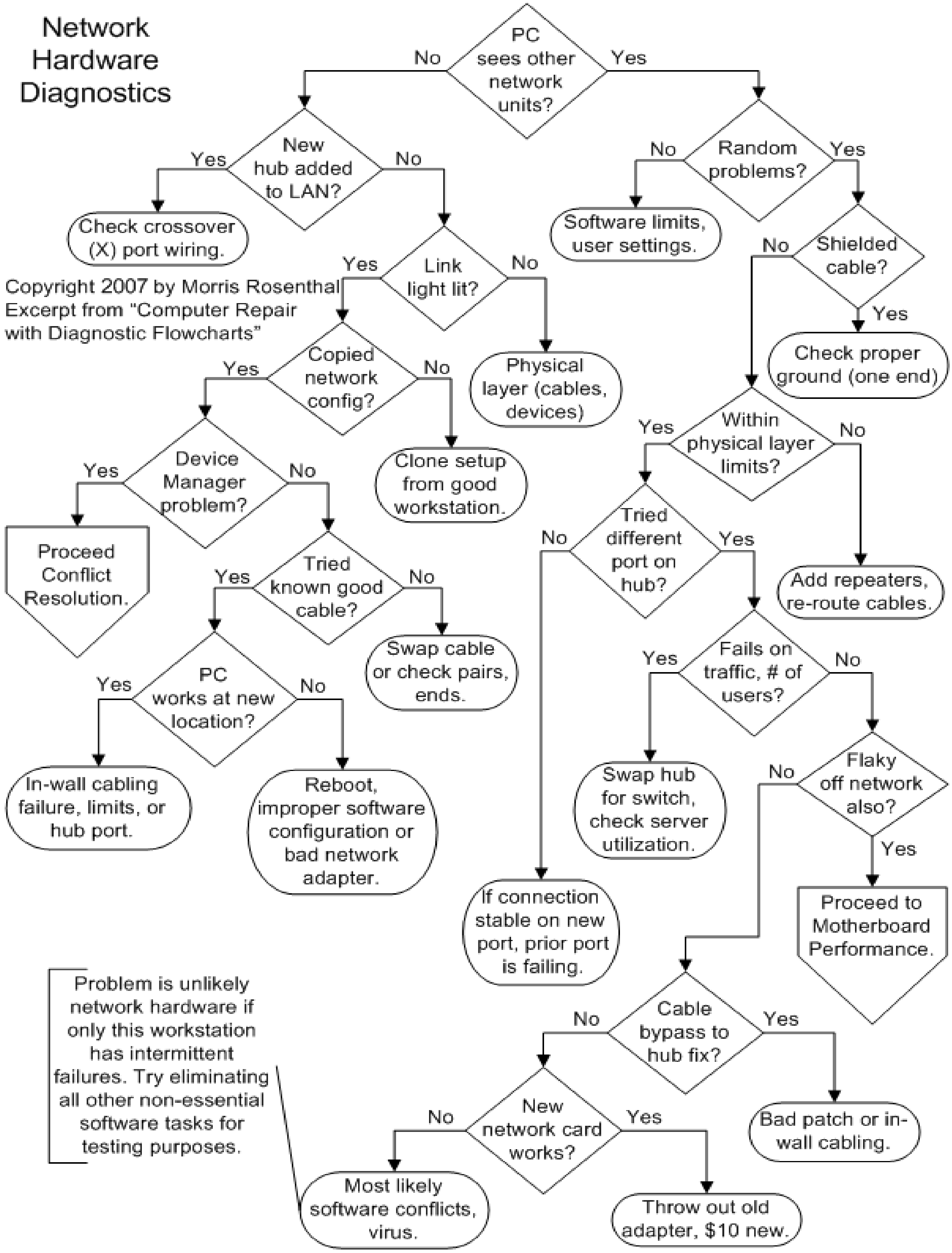
Jaringan kita memiliki masalah kinerja ketika ia tidak dapat beroperasi secara efektif. Sebagai contoh, waktu respon jaringan yang lambat, jaringan tidak stabil seperti biasanya, dan para pengguna banyak yang mengeluh bahwa jaringan melayani pekerjaan mereka lebih lama. Beberapa masalah kinerja yang bersifat sewaktu-waktu muncul seperti duplikasi alamat dan laju utilisasi jaringan yang selalu konsisten tinggi dapat saja terjadi.

Jika Anda secara teratur dapat memeriksa jaringan untuk masalah kinerja, Anda dapat memperpanjang fungsi konfigurasi jaringan yang ada dan merencanakan peningkatan kualitas jaringan dibandingkan harus menunggu akibat atau dampak dari masalah tersebut terhadap produktivitas pengguna.

"If all procedures documented on this website have been followed, the network should work, but sometimes, it does NOT! In such cases, I have the tendency first to yell that the computers:

Gambar 1. "my friends tell me, that this picture is a 'close' match to reality" (www.wown.com, 2002)

1 Diagram Alir Network Troubleshooting



Gambar 2. Network Troubleshooting Flowchart

2 Jaringan Berjalan Lambat

Ketika telah berhasil menginstall jaringan baru atau memperluas konfigurasi jaringan yang ada, Anda pasti menginginkan dan berharap komunikasi yang terjadi berlangsung cepat, berlari seperi cheetah:

Tetapi, ternyata apa yang telah Anda lakukan terjadi tidak seperti yang Anda bayangkan. Komunikasi dalam jaringan berlangsung sangat lambat bahkan seolah-olah mati perlahan mirip seperti jalannya seekor ulat atau sebuah traktor :)

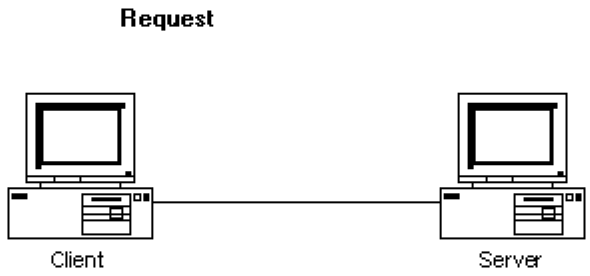
Tips:

Jika jaringan Anda berbasis TCP/IP dan berjalan cepat di satu arah sementara lambat di arah yang lain, kemungkinan masalahnya terletak pada Registry komputer.

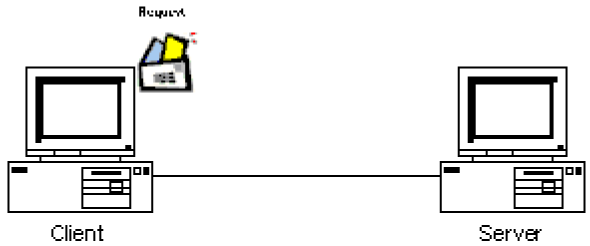
Jaringan yang sehat seharusnya bekerja seperti larinya seekor cheetah dan hanya memerlukan waktu yang cukup singkat untuk merespon dan menjalankannya seperti terlihat pada Gambar di bawah ini:

Gambar di atas adalah dalam format animasi GIF sehingga pada dokumen tercetak tidak akan terlihat. Untuk itu, lihat paparan gambar-gambar statik di bawah ini yang menggambarkan proses komunikasi gambar animasi GIF di atas:

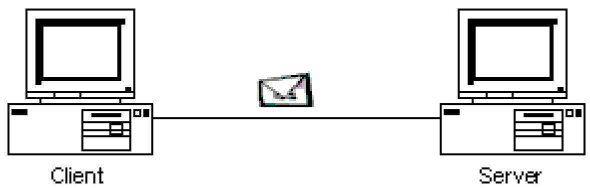
Kasus SUKSES: Kondisi Jaringan Baik/Normal



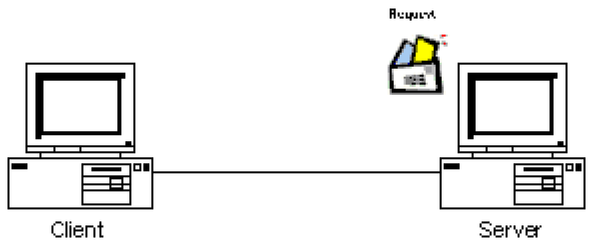
Klien mengirimkan sebuah REQUEST (misalnya: meminta daftar direktori, membuka file, membaca/menulis file, mencetak dokumen))



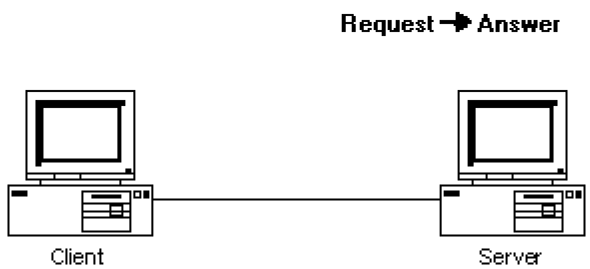
REQUEST tersebut diletakkan pada sebuah “Amplop” di jaringan. Amplop di sebuah jaringan biasanya diistilahkan dengan paket.



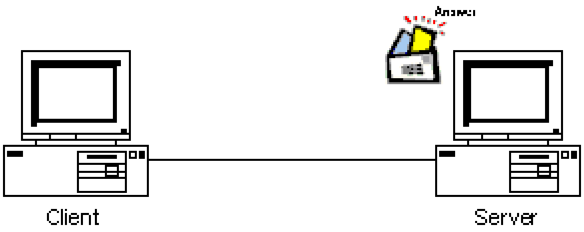
Amplop tersebut kemudian dikirim dalam bentuk sinyal elektrik melalui kabel Ethernet ke sistem Server.



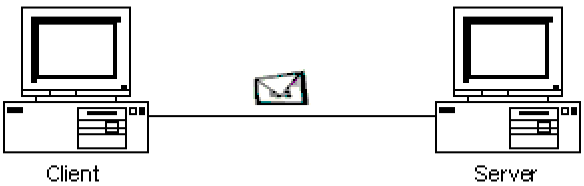
Server menerima “Amplop”



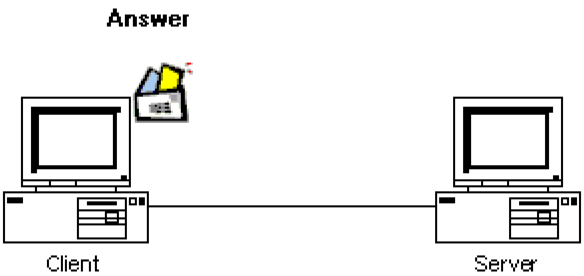
Server merespon REQUEST dan memberikan jawaban dengan mengirimkan Amplop yang akan ditujukan ke klien



Kemudian, jawabannya akan dimasukkan kembali ke "Amplop" balasan



Amplop yang berisikan jawaban dari server selanjutnya dikirimkan kembali ke klien.



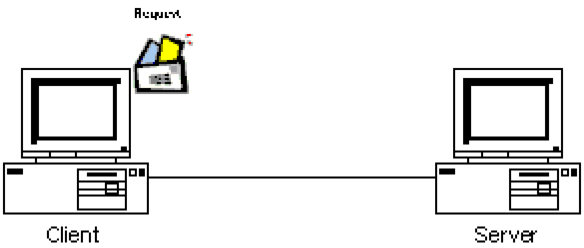
Klien menerima "Amplop" dan membukanya untuk dibaca hasil jawaban dari Server.

Kasus GAGAL: Kondisi Jaringan Bermasalah

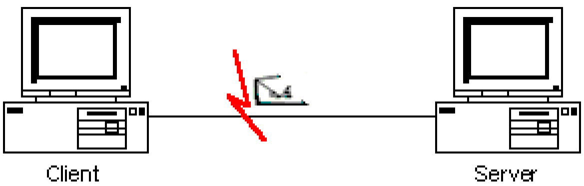
Pada kondisi jaringan yang bermasalah, kemungkinan Amplop yang dikirim akan mengalami kegagalan (tidak sampai atau rusak). Ilustrasi gambar di bawah masih menggunakan animasi GIF yang tidak akan terlihat pada dokumen tercetak.

Untuk itu, mari kita lihat masalah yang sering terjadi pada jaringan kabel dengan ilustrasi gambar-gambar statik di bawah ini:

Klien mengirimkan sebuah REQUEST (misalnya: meminta daftar direktori, membuka file, membaca/menulis file, mencetak dokumen)



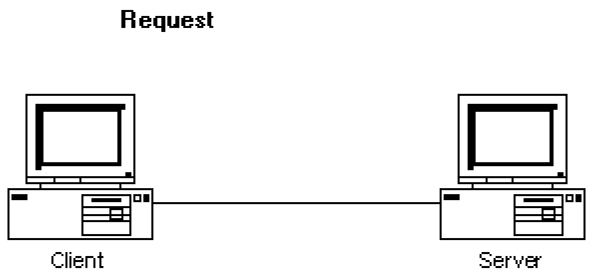
REQUEST tersebut diletakkan pada sebuah "Amplop" di jaringan. Amplop di sebuah jaringan biasanya diistilahkan dengan paket.



Amplop tersebut kemudian dikirim dalam bentuk sinyal elektrik melalui kabel Ethernet ke sistem Server tetapi mengalami kerusakan.

Server menerima "Amplop" tetapi dikarenakan kerusakan tersebut ia tidak dapat mengerti isi REQUEST dan untuk itu Server TIDAK membuat "JAWABAN".

Sejak server tidak mengerti "REQUEST" dari klien maka tidak ada jawaban yang dikirimkan kembali sehingga akhirnya setelah beberapa waktu klien berasumsi "Amplop telah hilang" atau Timeout.



Selanjutnya, klien akan kembali mengirimkan ulang sebuah “REQUEST".

Dikarenakan waktu tunggu (*waiting time*) hingga batas waktu "Time-out" pada klien dan klien kembali melakukan retransmisi (mengirim ulang) maka jaringan akan terlihat menjadi lebih lambat. Dan seandainya hal ini terjadi lebih sering dan jumlah REQUEST yang gagal sangat banyak maka akan menyebabkan kinerja jaringan turun drastis (mati total)

Troubleshooting atau Cara Penanganannya:

Untuk melihat kejadian ini, maka Anda dapat menggunakan aplikasi **NETSTAT** pada Windows untuk mengecek data statistik jaringan dengan perintah sebagai berikut:

NETSTAT

Fungsi:

- mengecek 'kesehatan' jaringan dengan menganalisa statistik jaringan.
- menampilkan koneksi TCP aktif, port-port mana saja yang digunakan, statistik ethernet, tabel rute IP, statistik IPv4 (untuk protokol IP, ICMP, TCP, dan UDP), dan IPv6 (untuk protokol IPv6, ICMPv6, TCP over IPv6, dan UDP over IPv6). Penggunaan tanpa parameter hanya akan menampilkan koneksi TCP yang aktif.

Paket Ethernet (“Amplop”) dapat rusak biasanya disebabkan karena perangkat keras (*hardware*) yang jelek seperti:

1. NIC (Network Interface card) yang jelek/rusak
2. rusaknya terminator atau port hub
3. kabel terlalu panjang melebihi kemampuan spesifikasi teknis kabel
4. konektor T yang jelek/rusak

Contoh: **netstat -se**

Hasil: WINDOWS

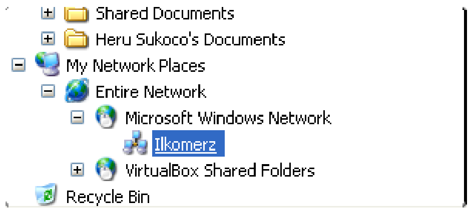
```
Interface Statistics
                           Received            Sent

Bytes                      27824843         1868952
Unicast packets               54898           45459
Non-unicast packets             100             115
Discards                          0               0
Errors                            0               0
Unknown protocols                 0

IPv4 Statistics

  Packets Received                          = 54982
  Received Header Errors                    = 0
  Received Address Errors                   = 15
  Datagrams Forwarded                       = 0
  Unknown Protocols Received                = 0
  Received Packets Discarded                = 12
  Received Packets Delivered                = 54970
  Output Requests                           = 45566
  Routing Discards                          = 0
  Discarded Output Packets                  = 2
  Output Packet No Route                    = 0
  Reassembly Required                       = 0
  Reassembly Successful                     = 0
  Reassembly Failures                       = 0
  Datagrams Successfully Fragmented         = 0
  Datagrams Failing Fragmentation           = 0
  Fragments Created                         = 0

IPv6 Statistics

  Packets Received                          = 2
  Received Header Errors                    = 0
  Received Address Errors                   = 0
  Datagrams Forwarded                       = 0
  Unknown Protocols Received                = 0
  Received Packets Discarded                = 0
  Received Packets Delivered                = 0
  Output Requests                           = 0
  Routing Discards                          = 0
  Discarded Output Packets                  = 0
  Output Packet No Route                    = 0
  Reassembly Required                       = 0
  Reassembly Successful                     = 0
  Reassembly Failures                       = 0
  Datagrams Successfully Fragmented         = 0
  Datagrams Failing Fragmentation           = 0
  Fragments Created                         = 0

ICMPv4 Statistics
                            Received    Sent
  Messages                  66          7
  Errors                    0           0
  Destination Unreachable   2           3
  Time Exceeded             64          0
  Parameter Problems        0           0
  Source Quenches           0           0
  Redirects                 0           0
  Echos                     0           4
  Echo Replies              0           0
  Timestamps                0           0
  Timestamp Replies         0           0
  Address Masks             0           0
  Address Mask Replies      0           0
```

```
ICMPv6 Statistics
                            Received    Sent
  Messages                  2           30
  Errors                    0           0
  MLD Reports               0           2
  Router Solicitations      0           27
  Router Advertisements     2           0
  Neighbor Solicitations    0           1

TCP Statistics for IPv4

  Active Opens                        = 19
  Passive Opens                       = 0
  Failed Connection Attempts          = 0
  Reset Connections                   = 18
  Current Connections                 = 1
  Segments Received                   = 19571
  Segments Sent                       = 10089
  Segments Retransmitted              = 0

TCP Statistics for IPv6

  Active Opens                        = 0
  Passive Opens                       = 0
  Failed Connection Attempts          = 0
  Reset Connections                   = 0
  Current Connections                 = 0
  Segments Received                   = 0
  Segments Sent                       = 0
  Segments Retransmitted              = 0

UDP Statistics for IPv4

  Datagrams Received    = 35393
  No Ports              = 9
  Receive Errors        = 0
  Datagrams Sent        = 35455

UDP Statistics for IPv6

  Datagrams Received    = 0
  No Ports              = 0
  Receive Errors        = 0
  Datagrams Sent        = 0
```

Hasil: LINUX

```
Ip:
    166843 total packets received
    4 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    166839 incoming packets delivered
    143956 requests sent out
    202 dropped because of missing route
Icmp:
    65 ICMP messages received
    0 input ICMP message failed.
    ICMP input histogram:
        destination unreachable: 60
        echo requests: 2
        echo replies: 3
    86 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 84
        echo replies: 2
Tcp:
    1692 active connections openings
    22 passive connection openings
    8 failed connection attempts
    119 connection resets received
    1 connections established
    155576 segments received
    132694 segments send out
    200 segments retransmited
    0 bad segments received.
    598 resets sent
Udp:
    11153 packets received
    41 packets to unknown port received.
    0 packet receive errors
    11016 packets sent
UdpLite:
TcpExt:
    7 packets pruned from receive queue because of socket buffer overrun
    377 TCP sockets finished time wait in fast timer
    1 time wait sockets recycled by time stamp
    2626 delayed acks sent
    3 delayed acks further delayed because of locked socket
    Quick ack mode was activated 209 times
    70 packets directly queued to recvmsg prequeue.
    70572 of bytes directly received from prequeue
    83536 packet headers predicted
    57 packets header predicted and directly queued to user
    5168 acknowledgments not containing data received
    7914 predicted acknowledgments
    53 congestion windows recovered after partial ack
    0 TCP data loss events
    1 timeouts in loss state
    31 retransmits in slow start
    83 other TCP timeouts
    206 packets collapsed in receive queue due to low socket buffer
    205 DSACKs sent for old packets
    24 DSACKs received
    117 connections reset due to unexpected data
    32 connections reset due to early user close
    12 connections aborted due to timeout
IpExt:
    InMcastPkts: 92
    OutMcastPkts: 109
    InBcastPkts: 1272
    OutBcastPkts: 537
```

3 Komputer tidak muncul di Network Neighborhood atau My Network Places

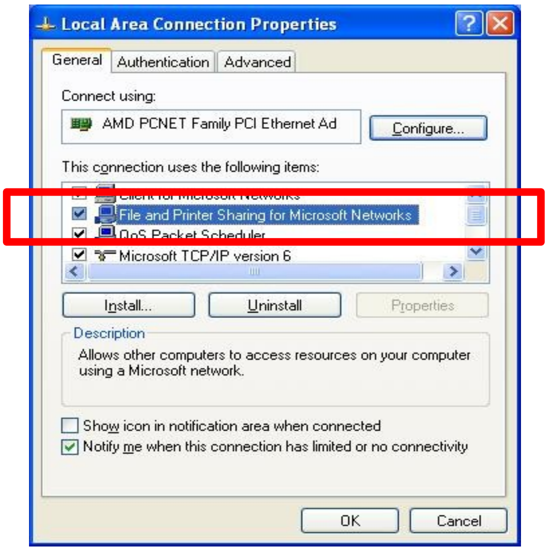


Gambar 3. Komputer tidak muncul di Windows Explorer -> My Network Places

Troubleshooting atau Cara Penanganannya:

Jika Anda tidak dapat memunculkan daftar komputer pada My Network Places (Windows Me/XP/Vista) atau Network Neighborhood (Windows 95/98) melalui Windows Explorer, maka silahkan cek salah satu penyebab atau cara di bawah ini:

1. Apakah fitur “Microsoft File and Printer Sharing” telah terinstall? Cek fitur ini melalui Control Panel -> Network Connections -> Local Area Connection, seperti terlihat pada gambar di bawah ini



2. Apakah Anda telah melakukan *sharing* pada file, folder, atau printer? File, folder atau printer yang di-*sharing* ini seharusnya akan muncul pada My Network Places atau Network

Neighborhood di Windows Explorer. Pergunakanlah aplikasi **PING** untuk mendeteksi apakah komputer Anda terhubung ke komputer-komputer pada jaringan.

3. Apakah protokol-protokol jaringan seperti Microsoft NetBEUI, IPX (Novell Netware), atau TCP/IP (Internet) telah terinstall?

   Microsoft File and Printer Sharing akan berfungsi sangat baik jika protokol Microsoft NetBEUI telah terinstall.

4. Apakah sistem Anda (komputer) berada pada Workgroup atau Domain yang sama dan memiliki nama komputer yang UNIK?

Pergunakanlah perintah:

- **PING** untuk mengecek apakah komputer kita terhubung ke komputer lain dalam jaringan atau tidak.

```
hsrkom@hsrkom-linux:~$ ping google.com
PING google.com (64.233.167.99) 56(84) bytes of data.
64 bytes from google.com (64.233.167.99): icmp_seq=2 ttl=234 time=309 ms
64 bytes from google.com (64.233.167.99): icmp_seq=3 ttl=234 time=320 ms
64 bytes from google.com (64.233.167.99): icmp_seq=4 ttl=234 time=319 ms
64 bytes from google.com (64.233.167.99): icmp_seq=5 ttl=234 time=311 ms
64 bytes from google.com (64.233.167.99): icmp_seq=6 ttl=234 time=311 ms
--- google.com ping statistics ---
6 packets transmitted, 5 received, 16% packet loss, time 5010ms
rtt min/avg/max/mdev = 309.340/314.687/320.715/4.712 ms
```

- **NET VIEW** untuk melihat daftar komputer dan sumber daya yang di-*sharing* pada sebuah workgroup atau domain.

  Mari kita coba perintah-perintah NET VIEW berikut dan perhatikan hasilnya!

  NET VIEW /domain:nama-domain [masukkan nama domain/workgroup]

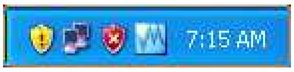
  NET VIEW \\nama-komputer [masukkan nama komputer yang diinginkan]

4 Berapa Alamat IP komputer saya?

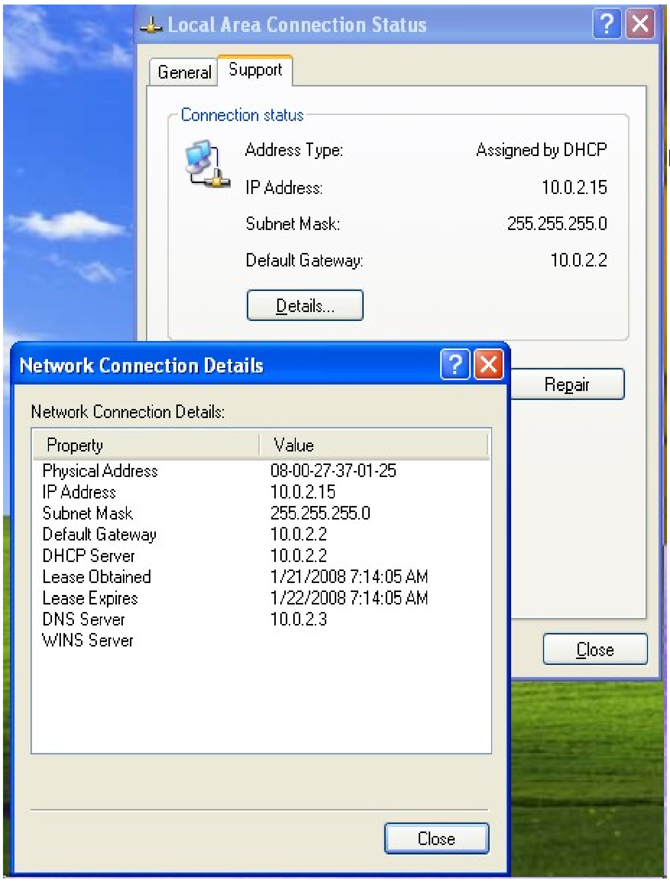
Ketika ditanya oleh rekan Anda mengenai alamat IP komputer sering Anda merasa bingung bagaimana memperoleh atau mengetahuinya? Bagaimana cara mengetahuinya, terutama jika sistem jaringan Anda memperoleh IP dinamis dari server DHCP (*Dynamic Host Configuration Protocol*)? Pada lingkungan OS Windows maupun OS Linux, ada beberapa cara mengetahui alamat IP, yaitu:

Pada Windows:

Cara I: Lihat ikon komputer pada bagian kanan-bawah di taskbar Windowx XP. Klik kanan dan pilih STATUS untuk melihat alamat IP komputer Anda seperti terlihat pada ilustrasi di bawah ini:



Ikon komputer sebagai indikator koneksi jaringan

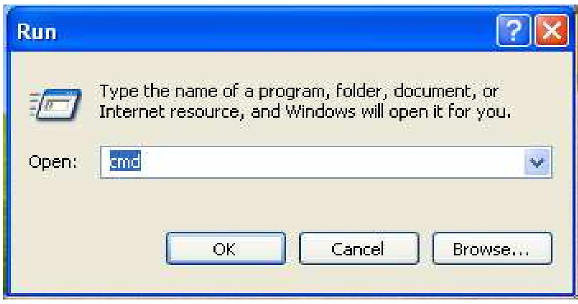


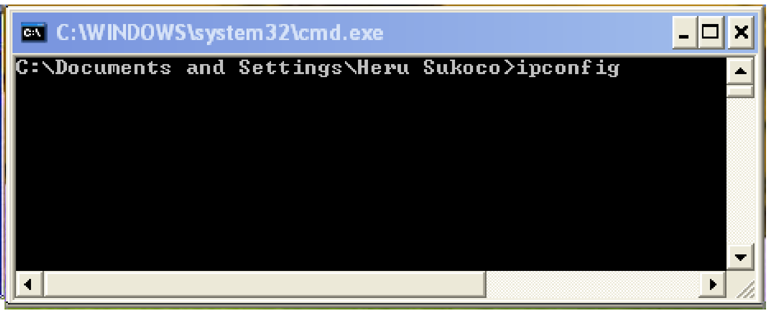
Alamat IP dapat diketahui setelah Anda memilih tab SUPPORT dan klik DETAILS.

Cara II: Menggunakan perintah IPCONFIG melalui prompt Windows XP dengan perintah sebagai berikut:

klik START -> pilih RUN -> ketik CMD -> selanjutnya akan muncul prompt Windows

ketikkan perintah: **C:\> ipconfig [ENTER] maka akan muncul alamat IP komputer seperti terlihat pada ilustrasi gambar berikut ini:**





Hasilnya:

```
Windows IP Configuration
Ethernet adapter Local Area Connection:
        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.0.2.15
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : fe80::a00:27ff:fe37:125%5
        Default Gateway . . . . . . . . . : 10.0.2.2
Tunnel adapter Teredo Tunneling Pseudo-Interface:
        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : fe80::5445:5245:444f%4
        Default Gateway . . . . . . . . . :
Tunnel adapter Automatic Tunneling Pseudo-Interface:
        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : fe80::5efe:10.0.2.15%2
        Default Gateway . . . . . . . . . :
```

Pada Linux:

Ketikkan perintah **ifconfig atau /sbin/ifconfig** pada prompt Linux sebagai berikut:

hsrkom@hsrkom-linux:~$ /sbin/ifconfig

```
eth0      Link encap:Ethernet  HWaddr 00:16:36:4B:08:B7
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:17

eth1      Link encap:Ethernet  HWaddr 00:13:02:2F:8B:CF
          inet addr:192.168.1.3  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::213:2ff:fe2f:8bcf/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:75315 errors:17 dropped:147 overruns:0 frame:0
          TX packets:48583 errors:0 dropped:23 overruns:0 carrier:96
          collisions:0 txqueuelen:1000
          RX bytes:167286901 (159.5 MB)  TX bytes:14289022 (13.6 MB)
          Interrupt:16 Base address:0xe000 Memory:54000000-54000fff
```

```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:6783 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6783 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2476464 (2.3 MB)  TX bytes:2476464 (2.3 MB)
```

5 Menguji koneksi TCP/IP ke komputer di jaringan

Jalankan kembali prompt Windows dan ketikkan salah satu komputer lain di jaringan, misalnya:

C:\> *ping 192.168.10.2*

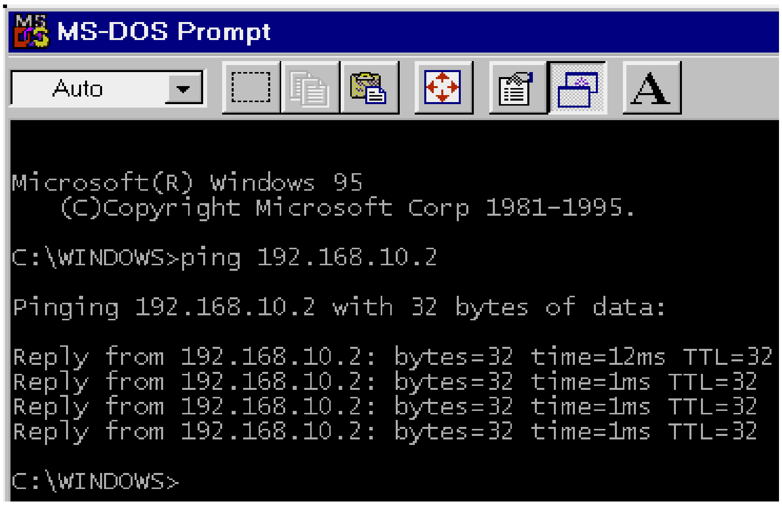
Ada beberapa kemungkinan yang sering muncul dari hasil perintah di atas, di antaranya adalah:

- Reply from...
- Request timed out
- Destination host unreachable

Untuk melengkapi keterangan di atas, perhatikan pengujian/troubleshooting berikut:

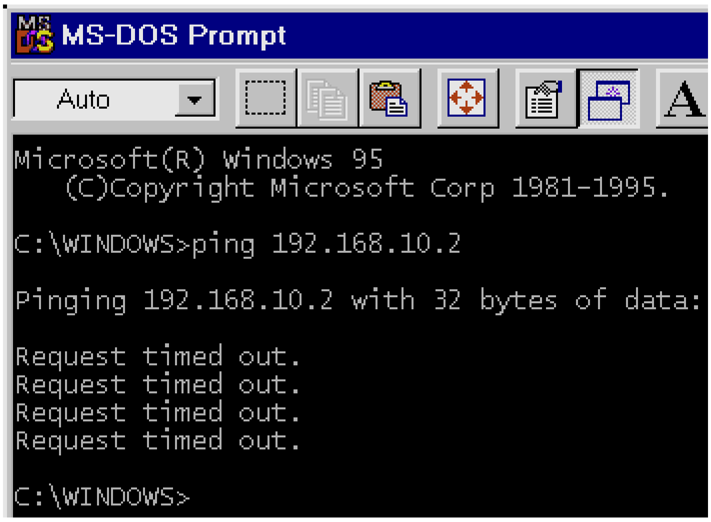
Hasil 1: Akan muncul "**Reply from...**" (balasan dari) dari alamat IP 192.168.10.2:

```
Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time.......
```



Jika "**Reply from...**" yang dihasilkan berarti konfigurasi LAN Card, alamat IP, perangkat hub/switch dan kabel Anda tidak bermasalah.

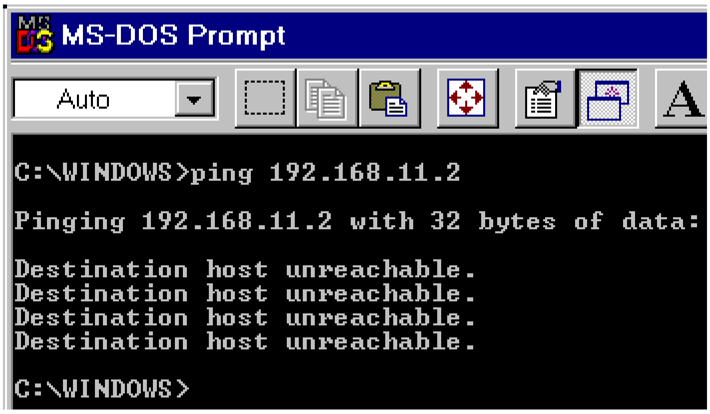
Hasil II: Akan muncul pesan **dari jaringan berupa pesan ICMP "Request timed out..."**



Jika "**Request timed out...**" **yang dihasilkan berarti ada beberapa kemungkinan yang terjadi, di antaranya:**

- **Kedua jaringan tidak saling terhubung satu sama lain**
- **Jarak kedua komputer terlalu jauh atau panjang kabel melebihi batas spesifikasi**
- **Salah satu komputer mengaktifkan firewall yang tidak mengizinkan paket PING (ICMP)**
- Komputer yang dituju mungkin down atau 'mati'.
- Konfigurasi pada salah satu komputer belum benar atau berfungsi

Hasil III: Akan muncul pesan **dari jaringan berupa pesan ICMP "Destination host unreachable..."**



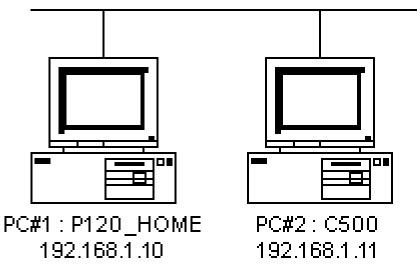
Jika "Destination host unreachable..." yang terjadi, hal ini disebabkan karena Anda sedang berusaha mencapai atau menghubungi sebuah komputer yang tidak berada pada jaringan atau sub-jaringan yang berbeda. Untuk menghubungi komputer pada sub-jaringan yang berbeda maka Anda memerlukan sebuah Gateway atau Router.

6 PING hanya bekerja pada SATU arah saja

Kadangkala, kita menemukan kasus bahwa komputer kita dapat melakukan pengecekan koneksi ke komputer lain menggunakan perintah PING. Namun anehnya, komputer lain tidak dapat melakukan pengecekan koneksi dengan perintah yang sama. Apa yang kiranya menjadi penyebab hal ini?

Perhatikan contoh kasus berikut ini! Kita memiliki 2 unit komputer yang terhubung satu sama lain pada jaringan sederhana dan menggunakan protokol TCP/IP. Konfigurasi yang digunakan adalah sebagai berikut:

- Nama komputer dan alamat IP diberikan pada kedua komputer, yaitu P120_HOME (IP: 192.168.1.10) dan C500 (IP: 192.168.1.11).
- Nama workgroup yang sama diberikan untuk kedua komputer.
- Fitur File and Printer Sharing telah terinstall dan sudah ada file/folder/printer yang juga telah di share.



Namun, ketika kita melakukan browsing dengan Windows Explorer untuk melihat yang telah di-*share* dan PING untuk mengecek konektivitas, masing-masing hanya berfungsi SATU arah seperti terlihat pada ilustrasi berikut:

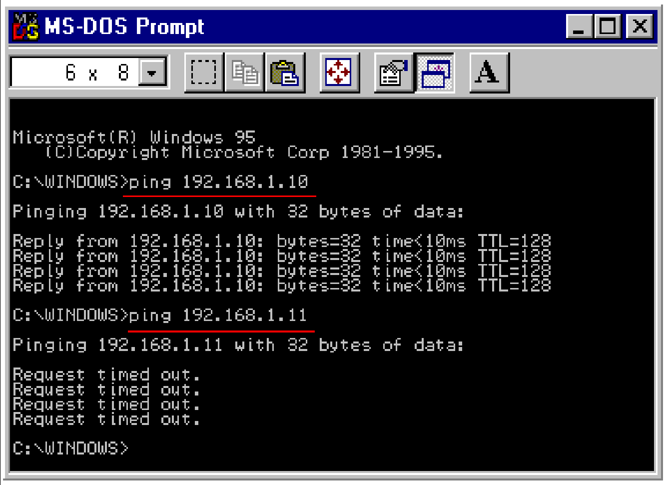
Pada kedua sistem, masing-masing hanya menampilkan dirinya sendiri, sementara komputer lain tidak dapat ditampilkan pada Network Neighborhood atau My Network Places.

Pada komputer #1: P120_HOME: 192.168.1.10

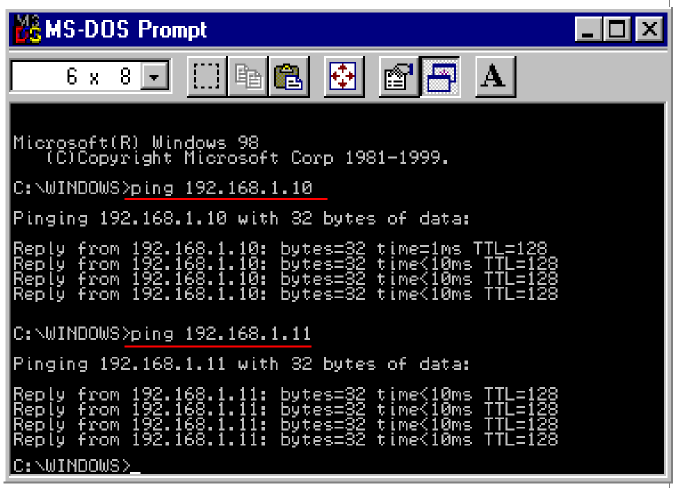
Pada komputer #2 : C500: 192.168.1.11

Kasus yang sama juga terjadi ketika kita melakukan PING pada kedua komputer tersebut.

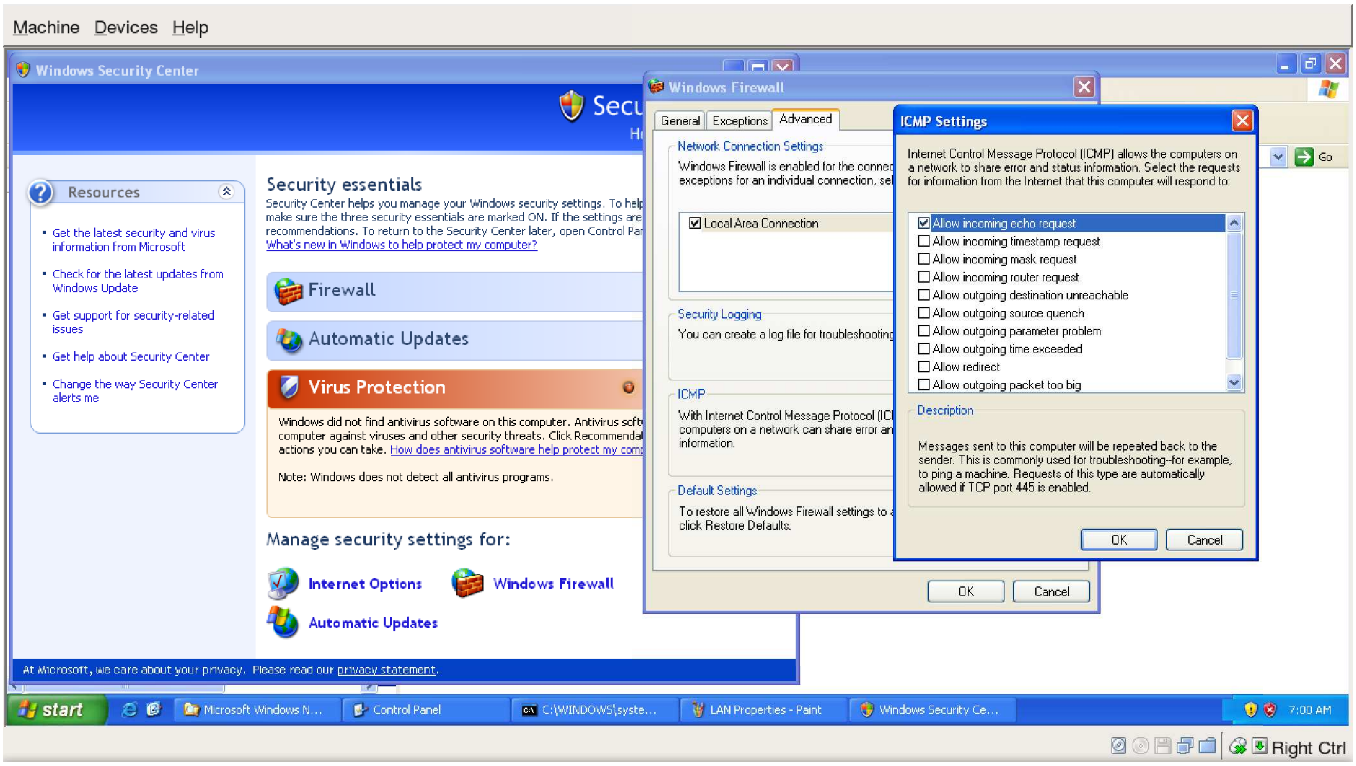
Komputer #1 (192.168.1.10) melakukan PING ke komputer #2 at 192.168.1.11 tetapi GAGAL, tidak ada REPLY.



Komputer #2 (192.168.1.11) melakukan PING ke dirinya sendiri dan komputer #1 at 192.168.1.10, keduanya BERHASIL dengan sukses.



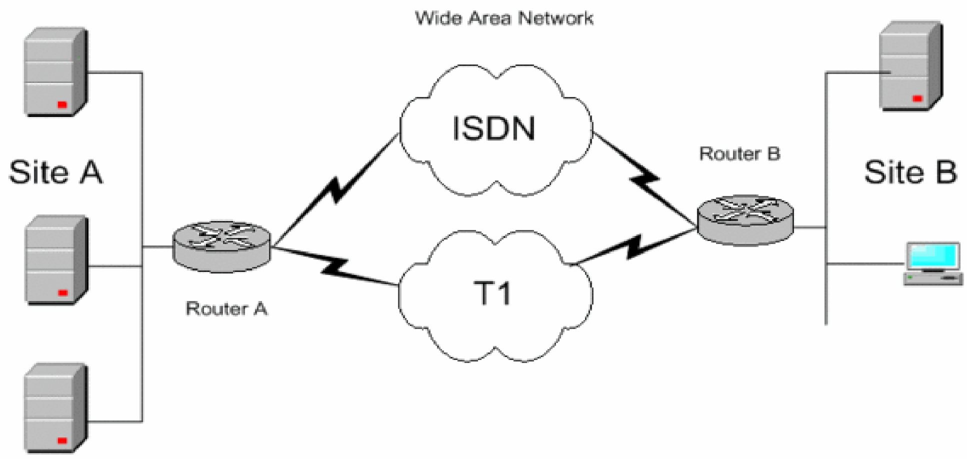
Aneh bukan? Sebenarnya tidak aneh. Hal ini biasanya terjadi karena salah satu komputer (dalam hal ini komputer #1) mengaktifkan firewall untuk memblokir paket PING (protokol ICMP). Untuk itu, lakukan konfigurasi firewall pada sistem operasi Windows XP Anda sesuai dengan kebutuhan seperti terlihat pada ilustrasi gambar di berikut ini:



7 Penggunaan PATHPING

Salah satu peralatan uji jaringan di lingkungan OS Windows yang cukup favorit adalah PATHPING. Pathping adalah perintah teks berbasiskan Windows yang dapat digunakan untuk menyediakan informasi mengenai jalur (path) data yang digunakan atau ditempuh ke tujuan, latency (delay) jaringan dan informasi hilangnya paket pada setiap hop di jalur perangkat intermediate antara komputer asal (pengirim) hingga ke komputer tujuan (penerima). Melalui alat ini, kita akan melihat bagaimana menggunakan pathping sebagai alat troubleshooting jaringan untuk mengatasi masalah-masalah sebenarnya di jaringan.

Pathping merupakan sebuah utiliti atau tool dengan command-line berbasiskan TCP/IP yang menyediakan informasi bermanfaat mengenai statistik jaringan, seperti delay/latency dan hilangnya paket selama proses penelusuran dari pengirim ke tujuan untuk setiap hop-nya. Pathping melakukan ini dengan cara mengirimkan permintaan (request) ECHO melalui protokol ICMP (*Internet Control Message Protocol*) dan menganalisa hasilnya. ICMP mendukung paket yang berisikan pesan kesalahan, kontrol dan informasi lainnya. Pathping akan mengirimkan beberapa pesan permintaan ECHO (*multiple echo request messages*) ke setiap router/gateway di antara komputer yang sedang dituju (tujuan) hingga alamat pengirim (sumber). Jika komputer tujuan Anda melalui link WAN maka sudah pasti bahwa Anda akan menggunakan beberapa router, setidaknya 2, yang berarti bahwa Anda dapat menguji PATHPING melalui jaringan 2-hop – hop 2-router. Contoh diagram jaringan sederhana dapat dilihat pada ilustrasi gambar di bawah ini.



Gambar 4. Typical WAN

Gambar 4, merupakan konfigurasi jaringan WAN standar (khas) di mana terdiri dari 2 site (segmen/sub-jaringan) yang satu sama lain dihubungkan melalui sebuah koneksi link T1 dan ISDN (*Integrated Services Digital Network*). T1 (atau T-1) merupakan sebuah istilah pada komunikasi digital untuk mengirimkan sinyal digital (DS-1) pada laju 1.544 Mbps. T1 memiliki 24 channel terpisah yang menggunakan sinyal PCM (*Pulse Code Modulation*) dan mekanisme multiplexing TDM (*Time Division Multiplexing*). T1 memerlukan perangkat koneksi digital (CSU/DSU - *Customer Switching Unit/Digital Switching Unit*) untuk menghubungkan ke kawat-4 (4-wires, biasa dipakai di kabel telepon PSTN, *Public Switched Telephone Network*) yang digunakan untuk membawa informasi.

Coba kita perhatikan! Pada gambar terlihat ada beberapa jalur (*multiple paths*) di sepanjang jaringan yang dilalui kedua site, yaitu sambungan (link) T1 dan ISDN, yang terhubung satu sama lain. Link T1 berkecepatan 1.544 Mbps dijadikan sebagai sambungan utama dan link ISDN merupakan sambungan backup yang akan menggantikan link T1 jika mengalami kegagalan. Karena ISDN merupakan sebuah teknologi yang mengizinkan Anda membayar hanya berdasarkan penggunaan saja, maka teknologi ini merupakan solusi yang tepat untuk menempatkan perangkat backup yang hanya digunakan pada saat dibutuhkan (*to lay dormant untill needed*) walaupun kecepatannya tidaklah besar, sekitar 64 kbps. Namun perlu diingat bahwa link ISDN hanya digunakan sebagai alternatif pada kasus darurat saja dan penulis merasa hal ini sudah cukup baik untuk layanan yang bersifat darurat/kritis.

Penurunan bandwidth ini tentunya akan menambah waktu untuk sebuah paket melewati jaringan dan menambah latency atau delay suatu trafik. **Latency** merupakan sebuah pengukuran mengenai seberapa lama suatu paket data memerlukan waktu untuk berpindah dari sebuah node ke node lainnya. Node di sini dapat berupa komputer, hub, switch, router atau perangkat aktif lainnya. Pathping merupakan alat pengujian yang cukup baik untuk kasus kita ini.

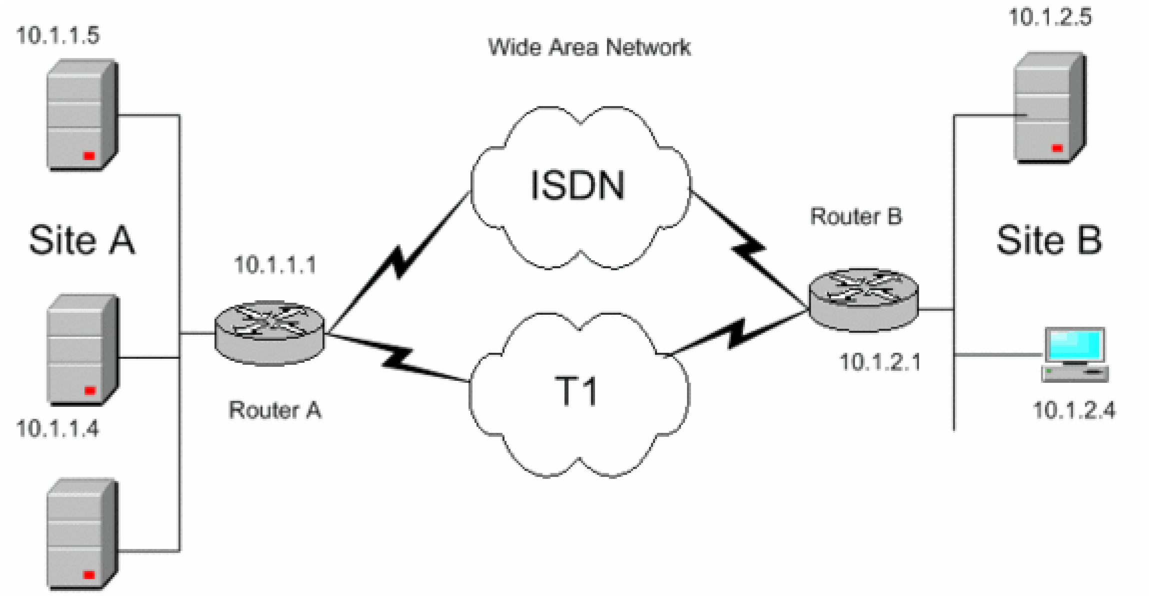
Cara Kerja dan Menghitung Latency:

- Sender (pengirim) mengirim sebuah paket test ke Receiver (penerima)
- Receiver menerima paket request dan mengirimkannya kembali ke Sender
- Pada Sender akan terlihat waktu perioda paket (biasanya diistilah dengan round-trip time, RTT). Inilah yang dipertimbangkan sebagai nilai Latency (periode waktu yang diperlukan sebuah paket untuk 'pulang-pergi')

Tips:

- Pathping merupakan sebuah tools yang tidak hanya dapat melihat sebuah paket melalui jaringan tetapi juga dapa melihat apakah paket tersebut melalui jalur yang benar dan disukai (dalam kasus ini adalah T1, bukan ISDN) atau melewati jalur alternatif (ISDN) jika jaringan kita mengalami bottleneck, untuk melihat isu-isu seputar latency/delay. Ketidakcukupan bandwdith dan latency/delay akan menyebabkan terjadinya *time out* pada proses pengiriman data.
- Dengan menggunakan tool PATHPING, Anda dapat mengirimkan beberapa paket pesan request ECHO ke setiap router di antara komputer Anda dan komputer tujuan yang diinginkan. Dan beberapa saat setelah waktu pengiriman berlangsung, PATHPING akan menghitung hasil dari hasil informasi yang diterimanya dari setiap router yang dilalui oleh paket dan selanjutnya menampilkan hasilnya.

Mari kita rinci lagi Gambar 4 dengan menambahkan alamat IP pada setiap jaringan dan node-nya, seperti terlihat pada Gambar 5.



Gambar 5. Typical WAN dengan pemberian alamat IP

Sekarang kita perhatikan komputer di site B dengan alamat IP 10.1.2.4 yang akan melakukan pengujian terhadap server di site B dengan alamat IP 10.1.15 dengan menggunakan PATHPING. Sebelum melakukan pengujian, mari kita lihat parameter-parameter apa saja yang dapat digunakan pada PATHPING, seperti terlihat pada Gambar 6.

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>pathping

Usage: pathping [-g host-list] [-h maximum_hops] [-i address] [-n]
                [-p period] [-q num_queries] [-w timeout] [-P] [-R] [-T]
                [-4] [-6] target_name

Options:
    -g host-list     Loose source route along host-list.
    -h maximum_hops  Maximum number of hops to search for target.
    -i address       Use the specified source address.
    -n               Do not resolve addresses to hostnames.
    -p period        Wait period milliseconds between pings.
    -q num_queries   Number of queries per hop.
    -w timeout       Wait timeout milliseconds for each reply.
    -P               Test for RSVP PATH connectivity.
    -R               Test if each hop is RSVP aware.
    -T               Test connectivity to each hop with Layer-2 priority tags.
    -4               Force using IPv4.
    -6               Force using IPv6.

C:\>
```

Gambar 6. Typical WAN dengan pemberian alamat IP

Penjelasan setiap parameter (yang paling banyak digunakan) di atas dapat dilihat pada Tabel 1. Penjelasan parameter-parameter pada Tabel 1 sengaja tidak penulis terjemahkan ke dalam bahasa Indonesia agar tidak menghilangkan makna yang sebenarnya.

TABEL 1. PENJELASAN PARAMETER-PARAMETER PATHPING (DALAM ENGLISH)

-n	Prevents pathping from attempting to resolve the IP addresses of intermediate routers to their names. You may want to consider doing this if you think you have a name resolution issue, or if DNS for example is not configured on your system … the time spent trying to contact a name server can be avoided using this switch.
-h	Specifies the maximum number of hops in the path to search for the target (destination). The default is 30 hops.
-p	Specifies the number of milliseconds to wait between consecutive pings. The default is 250 milliseconds (1/4 second).
-q	Specifies the number of Echo Request messages sent to each router in the path. The default is 100 queries.
-w	Specifies the number of milliseconds to wait for each reply. The default is 3000 milliseconds (3 seconds).
/?	Displays help at the command prompt

Berikut ini merupakan contoh (Kasus I) penelusuran dan pengujian komputer sumber (IP: 10.1.2.4) di site B ke komputer tujuan (IP: 10.1.15) di site A.

```
D:\>pathping -n server-1

Tracing route to server-1 [10.1.1.5]
over a maximum of 30 hops:
  0  10.1.2.1
  1  10.1.1.1
  2  10.1.1.5

Computing statistics for 50 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           10.1.2.1
                                0/ 100 =  0%   |
  1   35ms     0/ 100 =  0%     0/ 100 =  0%  10.1.1.1
                               13/ 100 = 13%   |
  2   28ms    16/ 100 = 16%     3/ 100 =  3%  10.1.1.5
                                0/ 100 =  0%   |

Trace complete.

(some output omitted)
```

Dari hasil statistik data jaringan di atas kita dapat memberikan kesimpulan berikut:

- Pada kasus di atas, terdapat sedikit Latency pada HOP yang kedua (10.1.1.1), melintasi link menuju HOP berikutnya, yaitu 10.1.1.5. Pada kondisi ini, kita melihat latency yang cukup kecil dan ini merupakan hal yang normal untuk link berukuran dan berkecepatan seperti ini. Namun jika laju milisecond-nya sangat besar, misalnya 500 ms, maka Anda mungkin harus mempertimbangkan bahwa Anda mulai memiliki masalah dengan bandwidth.

- Kalau kita perhatikan, PATHPING tidak hanya sekedar memeriksa konektivitas ke host tujuan tetapi juga menunjukkan kepada Anda bagaimana trafik Anda sampai di tujuan dan seberapa cepat trafik tersebut bergerak. Selain itu, PATHPING juga memberikan informasi mengenai seberapa besar ketahanannya dalam melewati sebuah WAN.

Perhatikan Contoh 2 dan 3 di bawah ini:

Kasus 2: Pemeriksaan konektivitas komputer LAN ke Web Server di Internet

```
C:\WINDOWS\SYSTEM32>pathping -n google.com

Tracing route to google.com [216.239.57.99]
over a maximum of 30 hops:
  0  10.8.53.218
  1  10.9.0.1
  2  167.206.32.34
  3  167.206.32.5
  4  65.19.104.209
  5  65.19.96.56
  6  65.19.97.226
  7     *        *        *
Computing statistics for 175 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           10.8.53.218
                                0/ 100 =  0%   |
  1   16ms     0/ 100 =  0%     0/ 100 =  0%  10.9.0.1
                                0/ 100 =  0%   |
  2   16ms     0/ 100 =  0%     0/ 100 =  0%  167.206.32.34
                              100/ 100 =100%   |
  3  ---     100/ 100 =100%     0/ 100 =  0%  167.206.32.5
                                0/ 100 =  0%   |
  4  ---     100/ 100 =100%     0/ 100 =  0%  65.19.104.209
                                0/ 100 =  0%   |
  5  ---     100/ 100 =100%     0/ 100 =  0%  65.19.96.56
                                0/ 100 =  0%   |
  6  ---     100/ 100 =100%     0/ 100 =  0%  65.19.97.226
                                0/ 100 =  0%   |
  7  ---     100/ 100 =100%     0/ 100 =  0%  0.0.0.0

Trace complete.
```

Apakah kesimpulan yang dapat Anda berikan:

Kesimpulan:

Kasus III: Pemeriksaan Komputer Server di KPSI (172.17.0.12) ke Server Web Departemen Ilmu Komputer FMIPA IPB (172.18.75.16)

Source: Server di KPSI IPB (172.17.0.12)

C:\Documents and Settings\Administrator>ipconfig

```
Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 172.17.0.12
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.17.0.1
```

Destination: Server di ILKOM FMIPA IPB (172.18.75.16)

C:\Documents and Settings\Administrator>pathping 172.18.75.16

```
Tracing route to 172.18.75.16 over a maximum of 30 hops

  0  KRS [172.17.0.12]
  1  172.17.0.1
  2  172.16.0.2
  3  172.16.0.26
  4  172.18.75.16

Computing statistics for 100 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           KRS [172.17.0.12]
                                0/ 100 =  0%   |
  1    0ms     0/ 100 =  0%     0/ 100 =  0%  172.17.0.1
                                0/ 100 =  0%   |
  2    0ms     0/ 100 =  0%     0/ 100 =  0%  172.16.0.2
                                0/ 100 =  0%   |
  3    0ms     0/ 100 =  0%     0/ 100 =  0%  172.16.0.26
                                0/ 100 =  0%   |
  4    0ms     0/ 100 =  0%     0/ 100 =  0%  172.18.75.16

Trace complete.
```

Apakah kesimpulan yang dapat Anda berikan:

Kesimpulan:

8 Penggunaan NSLOOKUP untuk Melihat DNS

Konsep penamaan domain atau lebih dikenal dengan istilah DNS (*Domain Name System*) merupakan sebuah protokol yang bertugas menggantikan penggunaan alamat IP. Manusia pada prinsipnya lebih mengenal NAMA dibandingkan harus menghafal alamat-alamat IP yang berupa ANGKA. Misalnya, kita lebih mudah menghafal nama HERU SUKOCO dibandingkan harus menghafal NIP: 132282666, atau lebih mudah menghafal www.google.com atau www.yahoo.com **dibandingkan alamat IP-nya 209.85.165.147 atau 209.85.165.99 (GOOGLE) dan 87.248.113.14 (YAHOO).**

Pemikiran inilah yang kemudian Internet menggunakan sistem DNS untuk menggantikan alamat IP. Bagaimana kita bisa mendapatkan alamat IP atau nama domain dari sebuah server di Internet? Jawabannya adalah NSLOOKUP. Tools ini menyediakan beberapa fitur untuk mendapatkan informasi berupa Nama Domain, Alamat IP, Alamat Email Server, dan sebagainya. Perintah NSLOOKUP dapat digunakan secara langsung atau melalui shell atau console-nya.

Kasus 1: Menggunakan NSLOOKUP secara Langsung

Windows:

```
C:\Documents and Settings\Administrator>nslookup www.google.com
*** Can't find server name for address 172.17.5.14: Non-existent domain
*** Can't find server name for address 172.17.5.21: Non-existent domain
*** Default servers are not available
Server:  UnKnown
Address:  172.17.5.14

Non-authoritative answer:
Name:    www.l.google.com
Addresses:  209.85.165.147, 209.85.165.99, 209.85.165.103, 209.85.165.104
Aliases:  www.google.com
```

Silahkan Anda coba dengan nama domain yang lain:

Linux:

```
hsrkom@hsrkom-linux:~$ nslookup www.google.com
Server:         172.17.5.14
Address:        172.17.5.14#53

Non-authoritative answer:
www.google.com  canonical name = www.l.google.com.
Name:   www.l.google.com
Address: 209.85.165.147
Name:   www.l.google.com
Address: 209.85.165.99
Name:   www.l.google.com
Address: 209.85.165.103
Name:   www.l.google.com
Address: 209.85.165.104
```

Silahkan Anda coba dengan nama domain yang lain:

Kasus 2: Menggunakan NSLOOKUP melalui SHELL/CONSOLE

Pada Windows:

```
C:\Documents and Settings\Administrator>nslookup
*** Can't find server name for address 172.17.5.14: Non-existent domain
*** Can't find server name for address 172.17.5.21: Non-existent domain
*** Default servers are not available
Default Server:  UnKnown
Address:  172.17.5.14

> www.ipb.ac.id
Server:  UnKnown
Address:  172.17.5.14

Name:    www.ipb.ac.id
Address:  222.124.11.124

> set type=any
> www.ipb.ac.id
Server:  UnKnown
Address:  172.17.5.14

www.ipb.ac.id   internet address = 222.124.11.124
ipb.ac.id       nameserver = ns1.mma.ipb.ac.id.ipb.ac.id
ipb.ac.id       nameserver = ns2.ipb.ac.id
ipb.ac.id       nameserver = nsjkt1.telkom.net.id
```

```
ipb.ac.id       nameserver = ns1.ipb.ac.id
ns1.ipb.ac.id   internet address = 222.124.11.104
ns2.ipb.ac.id   internet address = 222.124.11.107
> set type=mx
> www.ipb.ac.id
Server:  UnKnown
Address:  172.17.5.14

ipb.ac.id
        primary name server = ns1.ipb.ac.id
        responsible mail addr = hsrkom.ipb.ac.id
        serial  = 2008012007
        refresh = 10800 (3 hours)
        retry   = 3600 (1 hour)
        expire  = 3600000 (41 days 16 hours)
        default TTL = 86400 (1 day)
>
```

Pada Linux:

```
hsrkom@hsrkom-linux:~$ nslookup
> bima.ipb.ac.id
Server:         172.17.5.14
Address:        172.17.5.14#53

Name:   bima.ipb.ac.id
Address: 222.124.11.97
> set type=any
> bima.ipb.ac.id
Server:         172.17.5.14
Address:        172.17.5.14#53

Name:   bima.ipb.ac.id
Address: 222.124.11.97
> www.ipb.ac.id
Server:         172.17.5.14
Address:        172.17.5.14#53

Name:   www.ipb.ac.id
Address: 222.124.11.124
> set type=mx
> www.ipb.ac.id
Server:         172.17.5.14
Address:        172.17.5.14#53

*** Can't find www.ipb.ac.id: No answer
> smtp.ipb.ac.id
Server:         172.17.5.14
Address:        172.17.5.14#53

smtp.ipb.ac.id  canonical name = mail.ipb.ac.id.
>
```

9 Penggunaan TRACEROUTE/TRACERT

Tracert (Windows) atau dikenal juga sebagai traceroute (Linux) merupakan tools aplikasi berbasiskan protokol TCP/IP yang dapat berjalan pada berbagai platform OS, seperti Windows, Linux, FreeBSD, Mac, dan sebagainya. Aplikasi ini digunakan untuk membantu kita melakukan pengujian terhadap infrastruktur jaringan.

Perhatikan Gambar 4 dan 5 pada bagian sebelumnya. Kita akan melakukan pengujian jalur antara komputer klien di site B (10.1.2.4) ke komputer server di site A (10.1.1.6), baik melalui link utama (T1) maupun link backup (ISDN).

Kasus 1: Pengujian rute dari klien ke server melalui link utama T1

```
C:\>tracert 10.1.1.6
Tracing route to 10.1.1.6 over a maximum of 30 hops
   ---------------------------------------------------
   1       2 ms        3 ms        2 ms      10.1.2.1
   2      25 ms       83 ms       88 ms      192.168.11.1
   3      25 ms       79 ms       93 ms      10.1.1.6

   Trace complete.
```

Kasus 2: Pengujian rute dari klien ke server melalui link backup ISDN disebabkan karena link utama (T1) down.

Pada kasus ini, Anda dapat melihat bahwa jalur yang dilewati berbeda dan memerlukan waktu lebih lama dikarenakan kapasitas link yang jauh lebih kecil.

```
C:\>tracert 10.1.1.6
Tracing route to 10.1.1.6 over a maximum of 30 hops
   ---------------------------------------------------
   1       2 ms        3 ms        2 ms      10.1.2.1
   2      75 ms       83 ms       88 ms      192.168.10.1
   3      75 ms       79 ms       93 ms      10.1.1.6

   Trace complete.
```