NETWORKING BASICS

prepared by Dusko Jagodic (dusko.jagodic@zg.tel.hr)

Contents

OVERVIEW

This section will give you some overview of computer networking. It will teach you to create a small computer network and share its resources. After connecting computers you will be able to access files on other computers, print on printers connected to them and share CD-ROMs, CD recorders, Zip drives or any other device installed on any of the computers in the network. At the end you will be able to access Internet with your whole network using modem installed in one of the computers and Internet connectivity server software like Wingate.

CREATING A SMALL COMPUTER NETWORK

Steps to create a computer network:
- Installing network adapters
- Connecting computers with cables
- Installing network protocols
- Sharing network resources

Installing network adapters

Network adapter cards function as the link between the wiring of your network and your computer. These adapter cards give you connection points to which your network cables connect. Depending on the speed of your card you can build 10 or 100Mbps network. There are two major connection methods and accordingly network card can have two types of connectors or both of them: BNC or coaxial connection and UTP connection. Using BNC connection you are creating so called Bus Network or Star Network using UTP connection.

Assuming that your network adapter card is already installed inside of your computer, in order to make card be recognized by your operating system you must do the following:

1. Open the Start menu and choose Settings, Control Panel
2. Double-click the Add New Hardware icon
3. Choose Next in the Add New Hardware dialog box to continue
4. Choose No when prompted to let Windows detect your hardware. Choose Next
5. Select network adapter and then choose Next to proceed to the Network Adapter choices
6. Select the card manufacturer in the list on the left side of the dialog box, and then choose the card model on the right side. Click OK.

   If your Windows 95/98 driver for this card is not included with Windows 95/98 but came on a disk from the manufacturer, choose Have Disk and provide the drive letter or path of the driver
7. Windows displays the hardware settings for this card that will work with your computer
8. Configure the card to use these settings.
9. Click Next
10. Insert Windows 95/98 installation CD-ROM as prompted.
11. Click Finish.
12. When prompted to restart computer, select Continue.

If your card is Plug and Play and you have Plug and Play BIOS, Windows will recognize new hardware at the startup and try to install the driver. The procedure is very similar to the one described above.

Connecting computers with cables

Depending on a type of your network card and the network you want to create, you will be using two types of network cables: BNC coaxial cable or UTP cable.

BNC coaxial cable is used for Bus Networks where all computers are connected to a main wire of the network and have equal access to the wire at any point in time. Main disadvantage is that if network is cut at any point, the entire network is out of service.
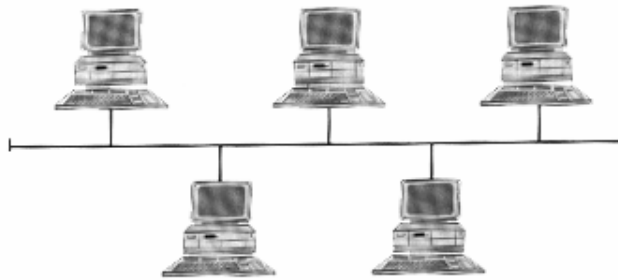
Bus Network

UTP cable is used to connect computers through the central hub in the Star network. The central hub distributes the signals to all the connecting computers. The main advantage of using the star configuration is that each cable is separate connection to central hub and if it brakes or disconnects the rest of the network will still work.
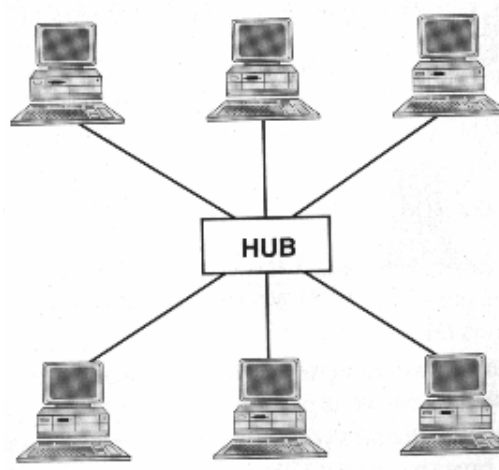
Star network

Installing network protocols

Installing the Microsoft Network Client
Install the Client software so you can use the shared resources on the network.
1. Open the Start menu and choose Settings, Control Panel.
2. Double-click the Network icon in the control Panel. The Network dialog box appears.
3. In the Configuration tab, choose Add. The Select Network Component Type dialog box appears.
4. In the Component list, select Client and then choose Add. The select Network client dialog box appears.
5. In the Manufacturers select Microsoft and then select Client for Microsoft Networks from the Client list on the right.
6. Click OK to install the client.
7. When installation is complete Windows returns to the Network Dialog box.
8. Restart the computer.

Installing the network protocol

The Protocol is the language, or set of rules, the computer uses to communicate with other computers over the network. Protocols govern format, timing, sequencing and error control. All of the computers on the network must use the same protocol to communicate with each other.

After correctly installing the network adapter, you must install the correct protocol for the network. To do so, follow these steps:

1. Open the Start menu, and choose Settings, Control Panel.
2. Double-click the Network icon in the Control Panel. The Network dialog box appears.
3. In the Configuration page, choose Add without choosing a component from the list. The Select Network Component Type dialog box appears.
4. In the Component list, select Protocol and then choose Add. The Select Network Protocol dialog box appears.
5. Select Microsoft from the Manufacturers list. A list of Network Protocols appears in the list on the right.
6. Select a protocol from the Network Protocols list and click OK.

Possible choices for network protocols are NetBEUI, IPX/SPX and TSP/IP. We will not go here into the details explaining each protocol. Since we will be using our network to access the Internet we will choose TCP/IP (Transmission Control Protocol/Internet Protocol) as our main network protocol. TCP/IP is the one being used as a protocol for the Internet.

The installation and configuration of TCP/IP is explained in the section about WinGate.

Sharing network resources

After establishing a computer network you might want to share some files with your co-workers. These files will be accessible to all computers in the network. Also you might want to share a printer(s) that are connected to any of the networked computers.

When working on a such network, you can choose to share or stop sharing the files and printer on each computer.

To set file and print sharing, follow these steps:

1. Open the Start menu and choose Settings, Control Panel.
2. Double-click the Network icon in the Control Panel. The Network dialog box appears.
3. In the Configuration page, select Client for Microsoft Networks from the list of installed network components.
4. Choose the File and Print Sharing button. The File and Print Sharing dialog box appears.
5. If you want to give other users on the network access to your files, select the option I Want to Be Able to Give Others Access to My Files. If you want to enable other users to use your printer, select the option I Want to Be Able to Allow Others to Print to My Printer(s) A check in the box means the option is on; no check mark signifies the option is turned off.
6. Choose OK to close the dialog box and Windows returns to the Net-work dialog box.
7. Choose OK to close the Network dialog box; alternatively, you can modify any of the other settings in the dialog box.

This procedure doesn't set up any of your devices (drives, printers, and so on) for sharing. To share your devices, you select each individually and set up the security options for them to determine which users can access the devices. That can be done by choosing device's Properties.

WINGATE

What is WinGate?

WinGate is an Internet connectivity server and firewall. These types of products are traditionally the exclusive domains of network specialists, and there are a number of concepts that may seem new to you. Keep reading if you don't understand some of the terms used, as this manual is packed with explanations in understandable language.

WinGate provides Internet access to a whole Local Area Network (LAN) via a single machine on the LAN. This machine can be connected to the Internet using any type of interface that is supported by the operating system. WinGate can save you money by eliminating the need for separate dial-up accounts, telephone lines and modems for each user that wants access to the Internet. With WinGate, they can all use the same link, at the same time.

WinGate was designed to facilitate Internet access. It can be used in any network environment that uses the TCP/IP network protocol. WinGate controls access to Internet services such as email and the World Wide Web. WinGate can be used on Intranets or company WANs that have no Internet connection. Throughout this manual, Internet connections are normally assumed. In reality this could be any connection (e.g. remote office dial-up link, etc), via LAN, WAN or Internet.

WinGate 3 has two server components and a client applet. The WinGate engine is a service that runs on the machine that is directly connected to the Internet. This engine provides the actual connectivity but is not visible to the user. GateKeeper is the control and configuration interface for the WinGate engine. The WinGate Internet Client (WGIC) runs on client machines and provides access to Winsock redirection capabilities.

As GateKeeper uses a TCP/IP connection to the engine, it can be run on any machine that can connect to WinGate. This means you can securely administer WinGate from the WinGate machine, and if you have a Pro license, from any machine on your network, or even on the Internet!

Once WinGate is installed and your workstations are configured, you are ready to surf the Internet.

Setting up the WinGate machine

Before you can install WinGate, you must insure that the WinGate machine is prepared.

This involves:
- Installing the TCP/IP protocol
- Configuring the TCP/IP protocol

Once these steps are complete, WinGate installation can proceed.

Installing TCP on the WinGate machine

For Windows 95/98
1.   Press the start button
2.   Select Settings - Control Panel
3.   Double-click the Network icon
4.   To install TCP/IP, hit the Add... button
5.   Double-click Protocol, then select Microsoft
6.   Select TCP/IP and hit OK

Setting up TCP/IP on the WinGate machine

Because of the way WinGate works, you'll need to assign a special (known as static) IP address to the WinGate machine LAN card. We strongly recommend 192.168.0.1 and we will refer to that number from here on. If you are not using this number, or any of the defined private addresses allocated by the InterNIC (the governing body that allocates all Internet addresses) then you may run into conflict problems. This should be relatively rare however.

For Windows 95/98
1.   Press the Start button, select Settings..., then Control Panel
2.   Double-click the Network icon. You'll see a dialog box
3.   Select the TCP/IP properties that are assigned to your physical network adapter, NOT your dial-up adapter
4.   Press the Properties... button. You should get the TCP/IP Properties box

Configuration Instructions

IP Address	Select the Specify an IP address option. Then type in 192.168.0.1 as the IP address. This is a private address that won't exist anywhere on the Internet, so you can let the WinGate machine use it for the internal LAN only. Next, fill in the Subnet Mask text area with 255.255.255.0
WINS Configuration	Leave this as is.
Gateway	Leave this entry blank.
Bindings	By default, the Client for Microsoft Networks option is checked. Leave it alone.

Advanced	No changes are needed from the default.
DNS Configuration	Select the Enable DNS option. Enter your user name in the Host box. In the Domain, put in the name of your ISP, like abc.com or partyon.com or whatever. In the DNS Server Search Order section, put in the IP address of your provider's name server and press the Add button .It should already be there, so don't add it again if it is. To find this number if you have a shell account on your ISP's server, you can log into your provider with a terminal program (telnet) and type nslookup. Your provider's server will return the DNS address. If that doesn't work, you can use 131.107.1.7 and/or 204.95.111.254 (those belong to Microsoft). In the Domain Suffix Search Order section, type in the domain suffix (usually the same as the domain) and press the Add button.

When you're all done setting these options, press the OK button. Then press the OK button in the Network dialog box. Windows will ask you to reboot. Press 'Yes' and wait for your machine to restart.

Testing TCP/IP

When you have installed TCP/IP on all the machines, they should all be able ping the WinGate machine. We will explain this shortly. Ping is a useful utility that comes with TCP/IP. Pinging a computers IP address sends out a message to that IP address saying "Are you there". The pinged machine sends a reply.

Ping the WinGate machine
At the command line type:
```
ping 192.168.0.1
```
The response should be
```
Pinging [192.168.0.1] with 32 bytes of data

Reply from 192.168.0.1: bytes=32 time<=10ms TTL=32
Reply from 192.168.0.1: bytes=32 time<=10ms TTL=32
Reply from 192.168.0.1: bytes=32 time<=10ms TTL=32
Reply from 192.168.0.1: bytes=32 time<=10ms TTL=32
```

That is the sign that TCP/IP is working. This result should be the same from any machine on the network. If this is the case move on to the next step.

Installing WinGate

To Install WinGate:

Run the *wingate* install file.
This will install WinGate, GateKeeper and various other files.

WinGate, GateKeeper, and Help files will be installed by default into the directory
C:\Program Files\WinGate\
this is configurable in the installer.

When the Install has finished, the WinGate engine will be started. Icons are added in the
WinGate group for Stopping and Starting the service. Ensure the WinGate engine is running
before starting to configure the client machines.

Client or Server

The installer can detect if you have WinGate 3 server installed on a machine on your network. If
this is the case, it will default to "Configure this machine as a WinGate Internet Client". If the
installer does not detect a WinGate server on your network, it will default to the server install
option.

Log on to GateKeeper

GateKeeper is the user interface for WinGate. It is used for all operations on WinGate, all
administration tasks, and any configuration you may do. GateKeeper has been designed to be
easy to understand and use. You will find that some parts of GateKeeper are very similar to that
of the NT user manager. It uses the same ideas including 'Users' and 'Groups' (Not in Home).

Logging on to GateKeeper:
1.   Run GateKeeper. You can find the Shortcut in the Start menu
2.   Click Log on
3.   You will be presented with a dialog box
4.   The options as you see there are correct for the first log on
5.   Click OK
6.   You will be asked to change your password
7.   Save the changes with the Button on the tool bar

If you have a Pro license and you want to use GateKeeper on machines other than the WinGate
machine:

1.   Ensure you are looking at the advanced view by selecting the Control panel option from
        the Options menu
2.   Double click Remote control service in the System services section
3.   Select the interfaces tab, check the Bind to all interfaces option
4.   Click OK

The first time you log on with GateKeeper, use the user name *Administrator*. You will be asked to change your password. Use the *Change password* option in the file menu. User names and passwords are case sensitive.

Setting up dialing

If you wish to use a modem on the WinGate machine for access to the Internet, you need to configure a phonebook entry using dial-up networking . WinGate uses the Windows phonebook entries to dial and log in to your service provider with no user intervention required.

So, once you have set this up in dial-up networking, and tested it and it is working, you should connect to WinGate with GateKeeper with Administrator privileges, double click on the dialer icon, and you will be presented with the WinGate Dialer Properties dialog. This will list your dialer profiles.

Double click to edit.

* In the dialog that is presented, enter appropriate values. Name and Password are needed even if you have them in the DUN phone book entry.

The Auto Connect to option gives a list of your existing phone book entries. Select the one you wish to use.

APLICATION SETUP

Internet Explorer

1. From the MSIE menu bar, under the "Tools" menu, choose 'Internet Options…' to bring up the "Internet Options" dialog box.
2. Select the "Connection" tab and 'LAN Settings', enable the 'Use a proxy server' option under Proxy server area. Click on the 'Advanced…' button to bring up the "Proxy Settings" dialog box.
3. In the 'Servers' area, disable the 'Use the same proxy server for all protocols' option.
4. Under 'Proxy address to use' for the HTTP FTP and Secure address types, enter 'wingate', or whatever label you gave in your hosts file to the machine running WinGate. Enter the port number that the WWW proxy in WinGate is configured to accept connections on for HTTP FTP and Secure. This is usually 80.
5. For the Socks address proxy enter 'wingate'. In the "Port:" entry adjacent to this entry, enter the port number that the SOCKS proxy in WinGate is configured to accept connections on.

6. Do not make any other proxy entries as MSIE will then use the SOCKS proxy for the remaining services.
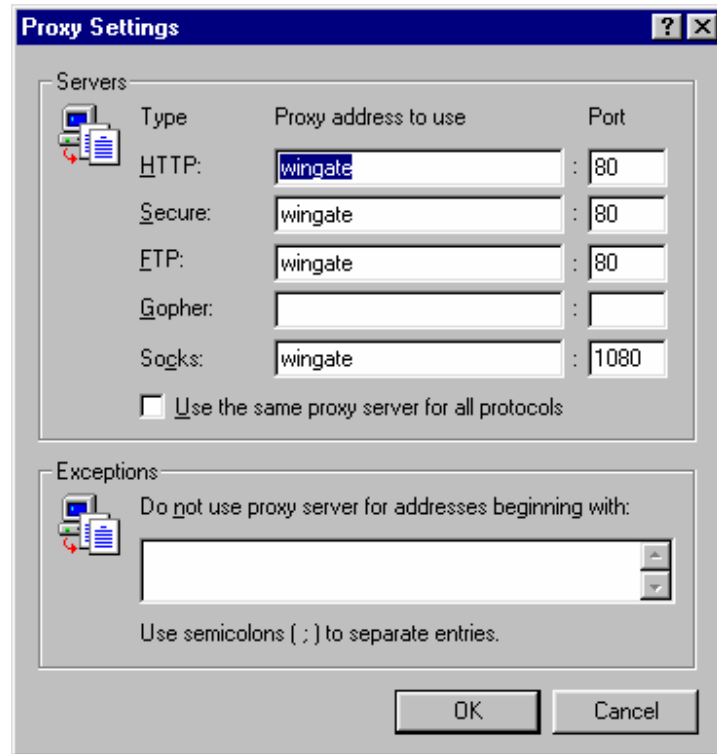

Netscape Navigator

1. From the Navigator 3 Menu bar, choose the Options menu, and select Network Preferences to bring up the Preferences dialog box. Or, in Navigator 4, select Edit - Preferences - Network.
2. Select the Proxies tab. Enable the Manual Proxy Configuration option and hit the View button. This brings up the Manual Proxy Configuration dialog box.
3. Under HTTP Proxy, FTP Proxy and Secure Proxy: enter wingate. Under Port: enter the port number the WWW proxy in WinGate is configured to accept connections on. This is usually 80.
4. Under SOCKS Host: enter wingate. Under Port: enter the port number the SOCKS proxy in WinGate is configured to accept connections on.
5. Do not make any other proxy entries. Netscape uses the SOCKS proxy only if there is no specific proxy given for a particular protocol. If you put an entry in for any of these other protocols, then Netscape will not work for those protocols.

Eudora

1. From the Eudora Menu bar, under the "Tools" menu, select "Options…". This will bring up the "Options" dialog box.

2. In the "Category" menu, choose the "Getting Started" icon.
3. In the "Pop account:" field enter the user name given to you by your POP server, your POP server's host name and the wingate machine name. Use this form: 'username' # 'host name' @ 'name of wingate machine'. For example: billg#microsoft.com@wingate
4. The delimiter character '#' should be that specified in the set-up of the POP3 proxy.
5. Still under the "Getting Started" icon, in the "Connection Method:" options, enable "Winsock".
6. In the "Category" menu, choose the "Personal Information" icon. Enter the same "POP account:" as above. The "Return address:" field should be in the 'user'@'host' format.
7. In the "Category" menu, choose the "Hosts" icon. Once again enter the same "POP account:" details. In the "SMTP:" field, enter 'wingate' or any other name you gave to your WinGate server.
8. In the "Category" menu, choose the "Checking Mail" icon. Enter the "POP account:" details yet again.
9. In the "Category" menu, choose the "Sending Mail" icon. Enter the "Return Address:" as above. In the "SMTP server:" field enter 'wingate' or any other name you gave to your WinGate server.
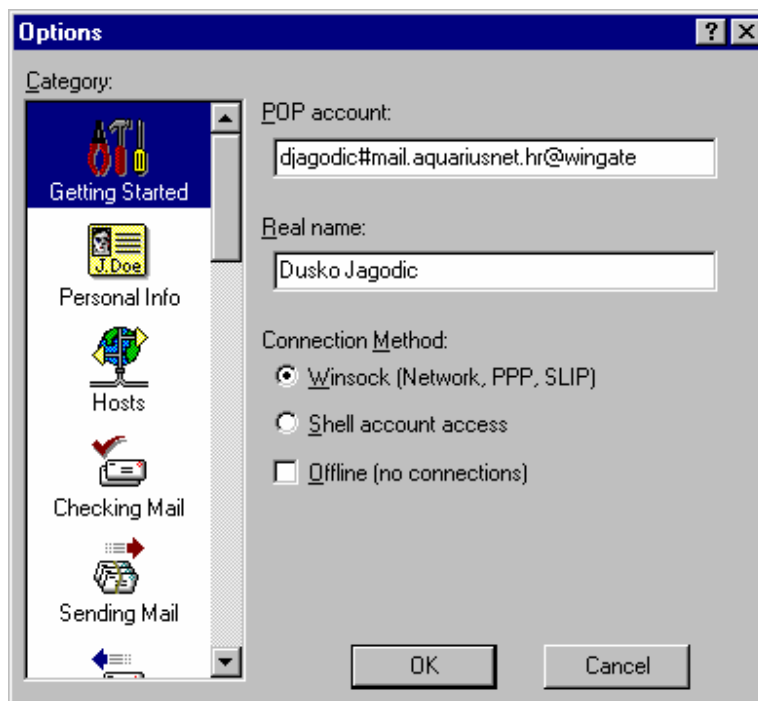
Microsoft Outlook Express

1. From the menu bar, under the "Tools" menu, select 'Accounts…' to bring up the "Internet Accounts" dialog box.
2. Select your account out of the list in the 'Mail' tab and click 'Properties'

---

3. Select the "Servers" tab. Within the "Servers" area are two server fields; "Outgoing Mail (SMTP):" and "Incoming Mail(POP3)". For both fields enter 'wingate', or whatever label you gave in your hosts file to the machine running WinGate.
4. Still within the "Servers" area, in the "Incoming Mail Server" field, enter the user name given to you by your POP server and your POP server's host name, in the following fashion: 'user name' # 'host name'. For example: billg#microsoft.com.
5. The delimiter character '#' should be that specified in the set-up of POP3 proxy.
6. Select the "Advanced" tab to bring up the "Server Port Numbers". Enter the port number of your SMTP mapped link in the "Outgoing Mail (SMTP) " field and enter the port number of your POP3 proxy in the "Incoming Mail(POP3)" field.
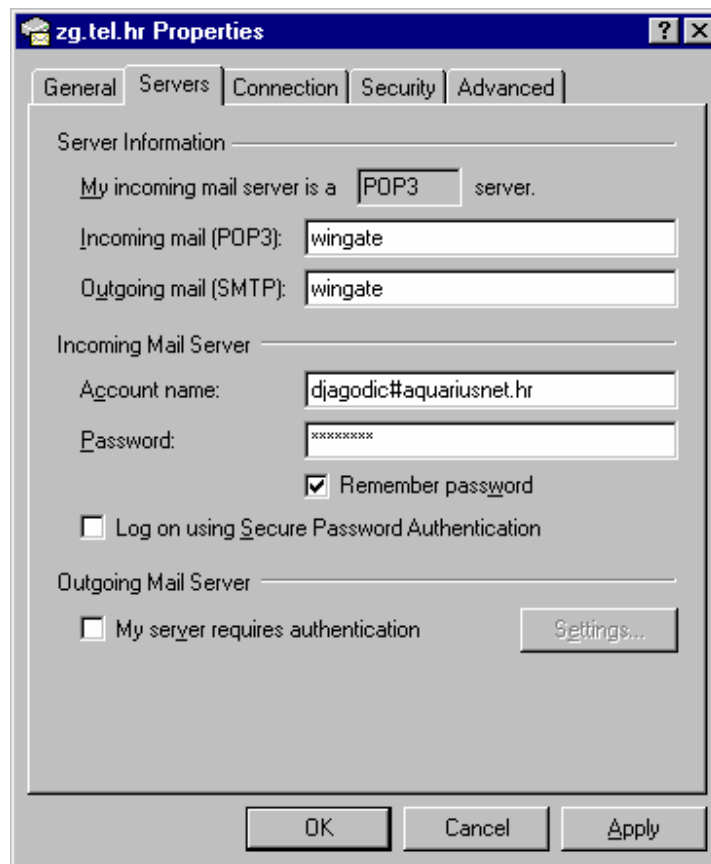
GLOSSARY

A

Active Service
An active service is a service that is running ie listening for TCP/IP requests.

B

Binding
A binding is a 'requirement to use'. In the case of a service (or protocol) to interface binding, it is a requirement for the service to use the specified interface. Binding a service to an interface causes the service to listen on the specified interface. WinGate services bind to all interfaces by default. Services only listen to interfaces for which they have a binding. WinGate eliminates the chance of binding to non-existent interfaces by listing only the interfaces actually on the WinGate machine.

C

Caching
The WinGate 3 WWW Proxy performs HTTP caching. Caching is the process of storing recently accessed graphics, HTML documents or other files from the Internet on the WinGate machine, to allow faster retrieval. The cache in WinGate checks documents daily to ensure they are up-to-date, and will get a new copy of the file if 'Reloaded' from a browser. The cache will not store URLs that have a '?' symbol, ie CGI dependent documents.

Client
A client is a recipient of a service. With computers, client machines are PC's on networks that are generally used by a single person. That computer can access a Server if it requires data or a service that is not part of the client system. For example, when a client computer wants Internet access, it will ask the server for a connection. Client software is a program that makes use of Server software to obtain the required data or service.

Connection
A connection can mean several things. At a physical level it means a joining of two devices, by cable, plug or similar. With Modems, a connection made on a successful dialing of another modem. At a Internet software level it commonly means a channel of communication between the client and server has been established.

D

DHCP
Dynamic Host Configuration Protocol. This is a service that automatically configures the TCP/IP settings for the client machines on your network.

Dialer
The dialer is software that tells the modem who and when to dial. WinGate has a built in dialer.

Dun
This stands for Dial-Up-Networking, a Microsoft term for the part of the operating system used to get modems to talk to each other in Windows.

F

Firewall
A firewall is a barrier between your network and the Internet, through which only authorized traffic can pass. As traffic passes between your network and the Internet it's examined by the firewall which follows the strict guideline of "whatever is not expressly permitted is denied."

To create the rules by which your firewall allows and disallows traffic, simply select the different Internet services, IP addresses and hosts you wish to permit or deny.

Most firewalls screen traffic between a company's internal network and the Internet, however firewalls can also secure one part of a network from another. For instance securing your corporate accounting department or your network from your subsidiary's network.

FTP

FTP stands for File-Transfer-Protocol. This is a method by which files are up/down loaded from the internet. Many client applications exist to make the process easy.

H

HTTP
HTTP is the Protocol used for World Wide Web browsing, but many other programs are starting to use HTTP. The WinGate WWW proxy allows HTTP access to LAN users so they can view World Wide Web sites.

HTTPS
This is secure http. Netscape and other browsers have built in encryption, to make data exchange more secure. This is commonly used for Online purchasing, especially where Credit cards are involved. Sometimes called SHTTP.

I

Interface
An interface is a 'network connection'. That may be a network card, an online Dialer profile, or your localhost loopback.

IP
IP stands for Internet Protocol. This is the method used on the internet (and on many LANs) to communicate. IP is a system of datagram packets. IP is not usually dealt with directly, this is the job of TCP. IP gets datagrams from point A to point B. TCP sends IP a datagram, and a destination. It assembles and sends a packet with information from the source (eg TCP) and a checksum that indicates the integrity of the packet. IP doesn't care about what is in the datagram. In fact it does not care if the packet it sends even gets there, and when IP receives a packet, if it has be garbled, IP throws it away! It is up to the protocol using IP to arrange for the packet to be resent if required.

IP Number / IP address
An IP address is the way IP distinguishes computers (or more specifically Interfaces) that exist on the same network. On the Internet you simply can not have two computers sharing an IP, as this creates havoc when trying to send data to the correct location. All computers that are 'on' the Internet (or LAN) need discrete IPs. There are different types of IP.
You have probably seen addresses in the form 128.211.23.45. This is a 32-bit number separated in to 4 8 bit parts. The four parts are similar to a mailing address, except the detail is the other way round. The first number of the IP is the most general, the last is the most specific. Since each computer on the Internet needs a different IP, there has to be some way of dishing out the IPs so that large companies and organizations have one for all their machines, while smaller organizations have some to go around as well. Since there are a small number of Large organizations and a large number of small organizations, ranges of IPs can be allocated accordingly.

In an IP address there are 2 parts, the network and the host identifiers. There are three ways the IPs can be split in to 2 parts.
Class A nnn.hhh.hhh.hhh
Class B nnn.nnn.hhh.hhh
Class C nnn.nnn.nnn.hhh
where n's=network identifier, h's=host identifier

A huge company with very complex internal networks may be allocated a class A address range such as 105.*.*.* . Only the range 1.*.*.* to 126.*.*.* are available for A class addresses. There are very few A class addresses, and no more are to be allocated, mainly because no-one has 16 million computers on their network!

B class addresses however are common for Large companies, allowing a range of around 65000 IPs. Microsoft and IBM probably have several each. When an B class IP address is allocated, (say 165.103.*.*), the first two numbers identify that companies network. The company can decide what to do with the next two (*'s in this case mean any number), and give any IP in that range to any computer on their network. B class networks addresses have 128 - 191 as the first number in the IP.

Class C addresses, giving 254 possible addresses (0 and 255 are reserved) are the third type. Here, the first 3 8 bit fields are specified, and the remaining field is allocated by the owner of the address. C class licences are in the range 192.*.*.* to 223.*.*.*

Networks that are directly connected to the internet are connected to an ISP via some fulltime connection (such as a cable or leased line) and the ISP will inform the network administrator of which IP's can be used on the network. A router is used to 'tell computers how to get to a particular IP'. (You may wish to read about Routing)

ISP's typically have 1-2 C class licences, providing 250 to 500 IP's. When you dial up an ISP with a modem, you are Dynamically allocated an IP address. This will be in the range of the C class licence that they own.

Private IPs
Private IP addresses are ranges of IP addresses that are 'Known not to exist' on the Internet. What this means is that no computer on the Internet will be assigned these addresses. These can

safely be used in internal LANs, as they have no direct connection to the Internet. One example of a Private IP range is the 192.168.0.* range that this manual commonly refers to.

The private IP ranges that will not be allocated on the Internet are:

10.0.0.0to   10.255.255.255 Class A
172.16.0.0   to   172.31.255.255 Class B
192.168.0.0   to   192.168.255.255   Class C
Do not choose an IP range that is not on this list. Also note that 0 and 255 are reserved in any class.

ISP
This stands for Internet Service Provider. ISPs are companies that have a connection to the internet and provide dial-up or direct connections to customers. Typically ISPs have many modems that customers can dial up with a PPP account. Dialing up an ISP usually gives you direct access to the internet. Many ISPs also offer ISDN T1, or other connections for improved speed.

L

Leased line
A Leased line is a full-time network connection to the internet where you are given an IP address (or a range of IP addresses) for your LAN. There are different methods of connection including ISDN, modem and Ethernet. Basically they give you guaranteed access to the internet. Full-time connections are often called 24/7, meaning 24 hours, 7 days a week.

Localhost
localhost is a special term in TCP/IP. 127.0.0.0 is the localhost (loopback interface) this is a software only interface internal to the stack itself, and is not accessible over any interface.

P

Packet
A data packet is a like a 'mail parcel'. Think of a package that gets sent in the post. There are a few things that you have to have, requirements. There has to be a name and address for the recipient, a return address, there have to be stamps, and of course the envelope or wrapping paper. But, what you put in the parcel is up to you. You can send (with in reason) anything that will be accepted by the port office. A data packet is very similar to this. You have to supply certain 'Wrappers' like to and from fields, but what is sent as the payload is up to you.

There are different types of packets used on the internet and other networks, but all of them use this idea of a parcel of data.

Ping
Ping is a command available on most TCP/IP capable systems including DOS. It is a command line program that tests a TCP connection between locations, and gives feedback on the speed of the link.

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS
        [-r count] [-s count] [[-j host-list] | [-k host-list]]

To test for a connection to ftp.microsoft.com, type at a command prompt:
```
ping ftp.microsoft.com <enter>
```

From a machine that is directly connected to the internet you will get a response such as

```
Pinging [198.105.232.1] with 32 bytes of data
Reply from [198.105.232.1] : Bytes=32  time 40ms
Reply from [198.105.232.1] : Bytes=32  time 20ms
Reply from [198.105.232.1] : Bytes=32  time 20ms
Reply from [198.105.232.1] : Bytes=32  time 30ms
```

You will notice that the name you typed is converted to an IP address. This is where DNS comes in. With out DNS you can only ping IP's.

From a workstation that is connected through WinGate you would get a result similar to

```
Pinging [198.105.232.1] with 32 bytes of data

Destination host unreachable
Destination host unreachable
Destination host unreachable
Destination host unreachable
```

(You may get 4 Request timed out message, they are basically the same thing)

This indicates that DNS is working. WinGate can't proxy ping packets, so you cant get the other data from the ping.

If you get a result like

```
Bad IP address ftp.microsoft.com
```

Then your DNS probably isn't working, so go back and check where you may have gone wrong.

Protocol
A Protocol is a method by which 2 or more parties can communicate or organize their communication. Network protocols are very strict. If an application does not follow the agreed style of communication, then they are unlikely to be understood. Protocol includes such things as greeting a server, logging on with a name and password, requesting and sending information, and saying 'good bye' when closing the connection. This is a similar idea as when one writes a letter. First one writes ones own details, then the recipients name and address, then you greet them with their correct title. Then the bulk of the letter is written. At the end, a suitable sign off such as 'Your sincerely' and then a signature close the communication. Proxy servers typically need one proxy per supported protocol. Examples of Protocols are POP3 Post office protocol and http hypertext transfer protocol.

Proxy
The normal meaning of the word proxy is someone who does something on behalf of someone else, e.g. voting by proxy. The Internet use of the word means basically the same thing, in relation to a software program. WinGate does things on behalf of other software programs. Specifically WinGate makes Internet requests on behalf of Internet clients to Internet servers.

R

Resource
A resource is a term used to mean any data item or hardware processing/storage. On a machine, resources are the memory, disk space, or processing time. An Internet resource is a Graphic, an HTML page, a downloadable file, live streaming video or any other available data. WinGate has internal resources, images, used to display the FTP listings in browsers.

S

Server
A machine and/or software that is set up to provide a service to assist you. Examples are FTP, Email, or Web servers.

Service
A service is something that helps or serves you. In WinGate, the proxies are services provided to help you connect to the internet.

SMTP
Simple Mail Transfer Protocol is the method used on the internet for sending mail. WinGate uses a Mapped link to facilitate SMTP.

SOCKS
SOCKS is a firewall negotiation protocol. WinGate has a SOCKS server built in.

Subnet
A subnet is a group of computers that are directly connected via coax or a hub. A computer with two network adapters will be on 2 subnets.

T

TCP/IP
TCP/IP is essential if you want to use the Internet. TCP/IP stands for 'Transmission Control Protocol / Internet Protocol'. TCP/IP (usually called TCP) is the standard method of sending data on the Internet. It is based on data packets that have a set format, including to and from addresses, similar to a letter. If you want to use the Internet or WinGate, it needs to be installed on every machine on your LAN.

Actually TCP and IP are different protocols, but they are so tied up that they are usually referred to in this way.

Telnet
Telnet is a command line program used to access remote computer and run programs on them. Telnet was the method by which the internet was first used. WinGate has a Telnet proxy.

Terminator
A small device used at each end of a coaxial cabled network. Terminators are essential.

U

UDP

User Datagram Protocol is a 'Connectionless' protocol. It uses IP to send datagrams in a similar way to TCP, except that like IP, and unlike TCP, UDP does not ensure the packets reach their destination.

URL

Uniform Resource Locator. URLs are a standard format for describing where a resource is on the Internet. Eg a Web URL reads as

http://www.aiha.com