Advice on Choosing the best Range of IP Addresses to use on your LAN

How Network Address Translation saved the Internet

In order for a computer to connect to the Internet it must have an IP address.

There are around 4 billion possible IP addresses ranging between:-

0.0.0.0 and **255.255.255.255**

and, excluding a few ranges set aside for special purposes, most are valid for use on the Internet.

Even 25 years ago it looked as though this large amount of IP addresses would soon be used up - then **Network Address Translation** (NAT) came to the rescue.

This allows hundreds of computers to connect to the Internet, at the same time, through a ***single*** computer, or router, which needs only ***one*** of the precious Internet IP addresses.

A NAT Router forwards requests from an internal computer onto the Internet using its single Internet IP address as the source address. When the reply comes back from the Internet site, the NAT Router remembers which internal PC issued the original request and routes the reply back to this originating computer.

By using different source TCP ports, a NAT Router can handle simultaneous requests to the same Internet destination from multiple internal computers.

All these internal computers still need to have IP addresses, so several IP address ranges have been withdrawn from use on the Internet itself and reserved for use on internal networks, operating from behind a NAT Router.

These reserved IP addresses can be used, over and over again, on tens of thousands of LANs throughout the world.

The reserved IP address ranges are shown in the table below:-

Start Address	**End Address**	**Number of Individual IP Addresses**
192.168.0.0	**192.168.255.255**	**65,536**
172.16.0.0	**172.31.255.255**	**1,048,576**
10.0.0.0	**10.255.255.255**	**16,777,216**

There is another range of IP addresses that don't appear on the Internet and are reserved for private networks:-

169.254.0.0 to **169.254.255.255**

In theory, 64,000 PCs can operate behind one NAT router.

NAT is sometimes and perhaps more accurately, called Port Address Translation (PAT) but NAT is what it's commonly known as.

Internet IP addresses are sometimes called **Public IP addresses** while Internal LAN IP addresses are sometimes called **Private IP addresses**.

This is called the **APIPA** range (*Ah-peep-ah*) - Automatic Private IP Addressing.
Microsoft has incorporated this into all versions of Windows.
The theory is that if a workstation has been set to get its IP address from DHCP, but no DHCP server responds to the workstation's broadcast, then, using the principle that ***any*** IP address is better than none, the workstation picks an IP address for itself, at random, from the APIPA range.
The workstation may then be able to communicate with other workstations in a similar situation but it almost certainly won't be able to access any server resources or the Internet.
In my experience the APIPA system gives ***nothing but trouble!***
I would much prefer that a DHCP-enabled computer that can't contact a DHCP server throws up a warning message on the screen rather than silently deciding to take an APIPA address and pretend everything's OK.
You can disable APIPA or even set static IP parameters to use, should no answer be forthcoming from a DHCP server, but APIPA is enabled by default.

Don't purposely choose to use any of the APIPA IP addresses on your internal network unless your express aim is to cause confusion.

Loopback IP Addresses

For completeness I'll also mention another range of IP addresses not found on either the Internet or on private LANs:-

127.0.0.0 to **127.255.255.255**

This range is called the Loopback Address Range.
Every PC running TCP/IP has a virtual network adaptor (one that is implemented in software but not connected to any real hardware) and ***all*** the IP addresses in the Loopback range, except the first and last, are assigned to this adaptor, although we normally only refer to address 127.0.0.1 which has the DNS name "localhost".
Loopback IP addresses are only used for testing and to allow processes running on a single computer to talk to each other, as any data sent out on this interface is immediately received back on it again (it's looped back).
As far as this discussion is concerned, Loopback Addresses are not suitable for use on ***any*** network and are just another 16 million addresses lost from the available pool.

Which range of IP addresses should I choose for my LAN?

The choice is so big that it's hard to know which range you should choose for your own network.
Does it matter which one you choose?
Generally no, they'll all probably work in most situations but there are some factors to consider when making your decision, particularly as you don't want to make the wrong choice now and then have to change them all again in 6 months' time.

My recommendations are:-

- Don't use addresses in the **172.16/172.31** range simply because I've never come across any network that uses them. Choosing this range is therefore only likely to cause confusion. It's also a ***middle-sized*** range that's not really required: small networks use the **192.168** range and larger networks use the **10.0.0.0** range.

- If your network will never, ever have more than 200 computers on it, choose a range of 256 x IP addresses from the **192.168** values.

- If your network has ***any*** chance of growing beyond 200 computers, may need multiple separate networks, perhaps at different locations, or requires anything at all complicated then choose a suitable range of IP addresses from the **10.0.0.0** range.

When you've chosen between the **192.168** and **10** ranges of IP addresses, which ***exact*** one should you choose?

Don't choose **192.168.0.0** to **192.168.0.255** as this is the most common range that is used.

Don't choose **192.168.1.0** to **192.168.1.255** as this is the second most common range that is used.

In some people's minds an address range starting

Choosing these common IP ranges has 2 problems:-

If you use the Windows Internet Connection Sha

1 - If knowing the internal IP range that is used on your LAN can help a hacker break into your network, they will surely try these 2 ranges.

2 - If you need to connect to another private network via a VPN which happens to be using the same internal range on their LAN as you are on yours, the VPN will connect but no traffic

will flow between the 2 LANs.
This is because when you try to connect to a device on the remote LAN, the IP routing part of Windows on your PC will assume the device is located on the local LAN.

Similarly **10.0.0.0** to **10.0.0.255** is another common range to avoid.

Choose an unusual, easy to remember range such as:-

10.20.30.0 to **10.20.30.255**
or
192.168.240.0 to **192.168.240.255**

Network range shorthand

To specify the range of IP addresses used on a network you usually write the first IP address in the range followed by the **subnet mask** such as:-

192.168.0.0   255.255.255.0

You may come across a shorthand way of writing this:-

192.168.0.0/24

Why does 255.255.255.0 equal 24?
24 is the number of ones, counting from the left, of the subnet mask when it's represented as a binary number.
The network **10.20.30.0** subnet mask **255.255.248.0**
can also be represented as:-**10.20.30.0/21**

What to do if your LAN is larger or more complicated than normal

When you use an IP range with a subnet mask of **255.255.255.0** you get 256 different IP addresses.
The very lowest one in the range is not normally assigned to a device but is used for the network name.
The very highest one in the range is also not normally used for a device and is called the **Broadcast Address** - every device on the LAN listens to IP packets sent to the broadcast address.
On the **192.168.0.0** network with subnet mask **255.255.255.0** then **192.168.0.0** is the network name and **192.168.0.255** is the network Broadcast Address which leaves 254 other IP addresses that can be assigned to devices.

"Device" is a term denoting a piece of equipmen

This includes servers, workstations, printers, rou

You may see subnet masks where the 4th digit is something other than zero. This reduces the amount of IP addresses available on a network. If you ask for a block of 8 Public IP addresses from your ISP they will be allocated on a small network with a subnet mask of **255.255.255.248**

Internet IP addresses are precious and can't be wasted while internal IP addresses don't need be conserved. There is therefore no good reason to ever limit an internal IP address range to less than 256 addresses and so the 4th digit of the subnet mask should always be zero.

If you need ***more*** than 254 devices on your internal network you have 2 choices:-

1 - Have 2 internal networks**, *both*** with subnet masks of **255.255.255.0** connected by a router.

2 - Reduce the 3rd digit of the subnet mask to allow more IP addresses to be available for devices on your network.

The problem with **Option 1** is that you now need to purchase, configure and maintain another router.
The problem with **Option 2** is that too many devices on the same network can reduce performance.

My advice is that with modern network switches you can have as many as 1022 devices on the same network.
If you have a network bigger than this then you probably also have a big enough IT department that a router or 2 won't be a problem.

The subnet mask **255.255.252.0** allows 1022 IP addresses for devices.
An example of such a network range is:-
10.20.30.0 to **10.20.34.255**

(Although **192.168.30.0** to **192.168.34.0** would also work, it's not traditional and so can only cause confusion.)

My recommendations are:-
If you need a network with more than 254 devices then use a network range beginning with **10** and the subnet mask of **255.255.248.0** and be prepared for the differences from the **255.255.255.0** networks you are familiar with.

In a network with a subnet mask where the 3rd digit smaller than 255, the "IP maths" can be confusing and look odd.
In the previous example, both of the following IP addresses are valid to use for devices:-
10.20.30.255
10.20.32.0

Don't forget to actually install a WINS server.

Detailed recommendations of how to assign the internal IP addresses on a typical LAN

Let's assume that you've chosen **192.168.25.0** to **192.168.25.255** as your internal IP address range.
You still need to assign IP addresses within this range to the different types of network devices.

My recommendations are:-

192.168.25.1	Your Router or whatever you set as your gateway to the Internet
192.168.25.5	Your main server. If this is also your router to the Internet then keep it as **5**
192.168.25.6	A second server, if you have one
192.168.25.15	Your network switch. Not all switches can have (or need) an IP address assigned to them
192.168.25.20 to 192.168.25.30	Other special devices that require a static IP address
192.168.25.50 to 192.168.25.149	Your DHCP address pool for workstations
192.168.25.225	A Network Attached Storage (NAS) Drive
192.168.25.240	A network-attached printer
192.168.25.241	A second printer

This scheme allows room for the various categories of devices to expand as required.
For larger **255.255.248.0** networks, keep the same categories, in the same order but increase the ***amount*** of IP addresses in each category, as necessary.
One very large pool of DHCP addresses is OK.

Tips on configuring a DHCP server on your network

- Definitely have one. It's not hard to set up and it makes managing your network's IP addresses easier.

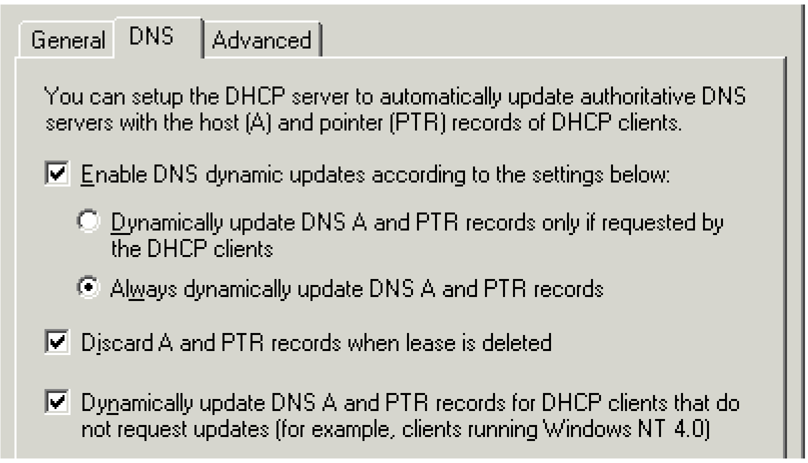
- Have ***only*** one. Router's and other devices often come with a built-in DHCP server.
  If you have a Windows network then make the Windows Server your DHCP server and disable all other DHCP servers on your network.

- If you have multiple servers and want a second DHCP server for redundancy then use another Windows Server as the second DCHP server and make sure that the range of IP addresses available to clients is different on each server.
  As an alternative, set up a second DHCP server with identical settings to the first but keep it disabled and only enable it if the first one fails.

- In the **Scope Options** set values for the following options:-

Option	*Value*
003	Default Gateway. This is your Internet router.
006	The main DNS server plus a second one if your network has one. Use Windows Servers running the DNS service in preference to any other DNS server, such as those at your ISP. It's usual for the Windows DNS server to use the router or the DNS servers at your ISP as **Forwarders** to resolve addresses not on your network.
015	Your local network's DNS name e.g. **mycompany.local**
044	Your network's WINS server. Most networks still use this service and it should be provided by a Windows server.
046	Set it as **0x8**

- On Windows Server 2003 also set these options:-



You can setup the DHCP server to automatically update authoritative DNS servers with the host (A) and pointer (PTR) records of DHCP clients.

☑ Enable DNS dynamic updates according to the settings below:

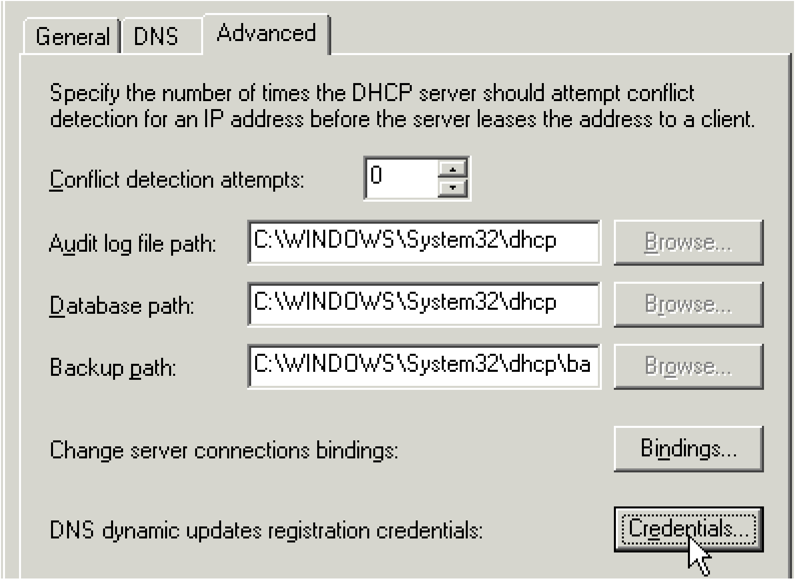
○ Dynamically update DNS A and PTR records only if requested by the DHCP clients

● Always dynamically update DNS A and PTR records

☑ Discard A and PTR records when lease is deleted

☑ Dynamically update DNS A and PTR records for DHCP clients that do not request updates (for example, clients running Windows NT 4.0)

On the **Advanced** tab set administrator level credentials:-



Specify the number of times the DHCP server should attempt conflict detection for an IP address before the server leases the address to a client.

Conflict detection attempts: 0

Audit log file path: C:\WINDOWS\System32\dhcp

Database path: C:\WINDOWS\System32\dhcp

Backup path: C:\WINDOWS\System32\dhcp\ba

Change server connections bindings:

DNS dynamic updates registration credentials:

- If you are using a Windows 2003 Active Directory controller as your DHCP server, make the server a member of the built-in DNS Proxy group.

- If the number of workstations requiring DHCP addresses exceed 75% of the available address pool then increase the address pool and/or reduce the lease time from the default value of 8 days to 4 days or less.

- If you have server, printers etc. that have static IP addresses then also set these up as reservations in the DHCP server. This has the advantages that:-

1 - If the devices loses its settings and reverts to DHCP it will still get the correct IP settings.

2 The DHCP management console has a complete record of

- all the IP and MAC addresses used on your network.

- Make sure that any firewall running on the DHCP server computer isn't blocking incoming DHCP requests to the broadcast address 255.255.255.255 on UDP ports 67 and 68.

How many static IP addresses should I get from my ISP?

To allow remote access to your network, or the operation of an in-house mail-server, you need a static Public Internet IP address from your ISP.

A static IP address is one whose value never changes as opposed to a dynamic IP address where a different address is assigned every time your Internet service connects.

A static IP address usually costs between £2 and £5 extra per month.

If you want to send emails directly you should also have a DNS name assigned to your static IP address

Most ISPs offer businesses a choice of a single IP address or a group of 8.

So how many do you need?

Because Internet IP addresses are precious, a whole range of techniques have evolved to allow you to perform a multitude of different functions from behind a ***single*** IP address.

The only good reasons I can think of for having more than one Public IP address are:-

To check if a DNS name is assigned to your IP a
nslookup <your IP address>

This DNS name should be entered as your mail-s

(Arrowmail needs 30 public IP addresses to run a

- You want completely separate various in-house system such as your computer netwero and your IP Phone system.

- You need to have 2 or more of the same type of server, using the same TCP port, accessible from the Internet - such as 2 Terminal Servers.

I've seen several companies that opted for a block of 8 Internet addresses but only ever use one and so, for simplicity and cheapness, go for a single IP address unless you are sure that you need more.

With a single Public IP address you can use a standard ADSL/Cable router while with a block of 8 you need a special router or 2 standard routers back-to-back.

What about using IPv6 addresses?

Everything on this webpage, besides this section, talks about Internet Protocol version 4 (IPv4). However, a new system called Internet Protocol version 6 (IPv6) has was designed over 20 years

ago, trialled, universally agreed on and built into the latest versions of operating systems.
There are routers and switches available that work with IPv6 which also perform any necessary IPv4-to-IPv6 conversions.
IPv6 was designed to overcome the limitations of IPv4, most notably the number of IP addresses available. Here's a comparison:-

Number of Available IP addresses

IPv4	4,294,967,296
IPv6	340,282,366,920,938,463,463,374,607,431,768,211,456

A typical IPv6 address looks like this:-

805B:D9D:DC28::FC57:200:D4C8:1FFF

It's 8 blocks of 4-digit hexadecimal numbers with leading zeroes omitted, and any block that is all zeroes is also omitted - hence the "double colon".

However, right now, IPv6 isn't used on the Internet and very few ISPs will assign you an IPv6 address.
IPv6 ***was*** the solution to the ongoing expansion of the Internet, (newer better schemes have since been proposed), but it doesn’t seem that any progress is being made to replace IPv4 on the Internet. If you have all the public IPv4 addresses you need then why change?

What does this mean for your company's LAN IP address scheme?

At the moment nothing.
You could if you wished use IPv6 addresses on your LAN and buy IPv6 enabled switches and routers, but you would need to go through an IPv6-to-IPv4 convertor to access the Internet.
In the vast majority of cases this would be madness.

When some alternative to IPv4 does eventually go live on the Internet your ISP will probably do the conversion for you to start with, and later you'd have your own compatible Router and IPv4 convertor.
Finally, when the Internet has completely changed over to a new system, who knows if private LANs will continue to use IPv4 addresses or if the information and recommendations on this page will then be irrelevant.

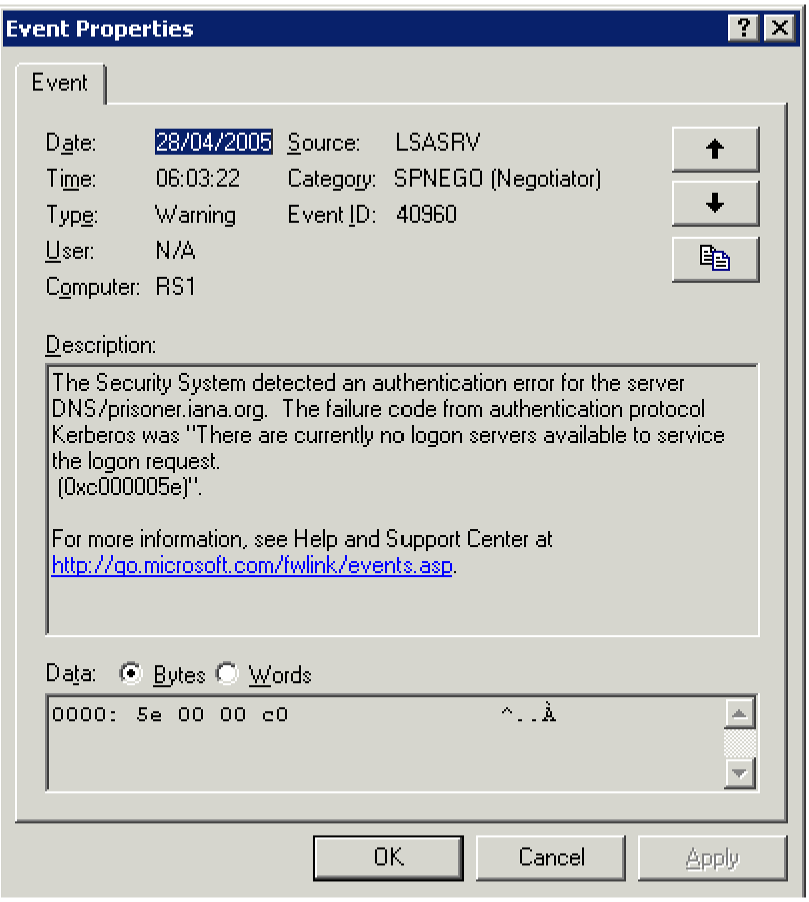
The Prisoner on the Internet

So you've chosen the IP range for your LAN, set up the static IP address devices, configured a DHCP scope and established a DNS server on your LAN to resolve local DNS names.
Is there anything else you've forgotten to do?
Many people forget to set up a reverse DNS zone on the local DNS server.
A reverse DNS zone allows your LAN's DNS server to answer questions such as:-
"What is the name of the computer with IP address 192.168.1.123?"
The answer might be something like:-
workstation28.companyname.local

With no reverse DNS zone, your DNS server does what it does with all questions it doesn't know the answer to: it asks its big brother on the Internet who then passes the query around other DNS servers until, after a minute or so, the answer comes back "Don't know".
Because there are 10s of 1000s of computers around the world with the IP address 192.168.1.123, each with a different name, it's not a question that Internet DNS servers can ever answer.
There are so many request for DNS names of private IP addresses sent out to the Internet that a special DNS server has been set up to answer them all.
It has the striking DNS name of **prisoner.iana.org** and it relieves other DNS servers from the burden of answering these requests.
What answer does **prisoner.iana.org** give in reply to requests for the DNS name of a private IP address?

- It blows a raspberry.
- It gives the Buddhist answer "mu" - un-ask the question.
- 42
- It shouts "stop wasting my time with stupid questions."

A more technically accurate explanation is that it tells the requesting server that it's failed to authenticate when trying to register its DNS record.
This shows up as in the Event Viewer system log which an administrator might eventually spot, work out and then rectify the problem:-



Event Properties

Event

Date: 28/04/2005 Source: LSASRV
Time: 06:03:22 Category: SPNEGO (Negotiator)
Type: Warning Event ID: 40960
User: N/A
Computer: RS1

Description:

The Security System detected an authentication error for the server DNS/prisoner.iana.org. The failure code from authentication protocol Kerberos was "There are currently no logon servers available to service the logon request.
(0xc000005e)".

For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.

Data: ● Bytes ○ Words

```
0000: 5e 00 00 c0                 ^..À
```