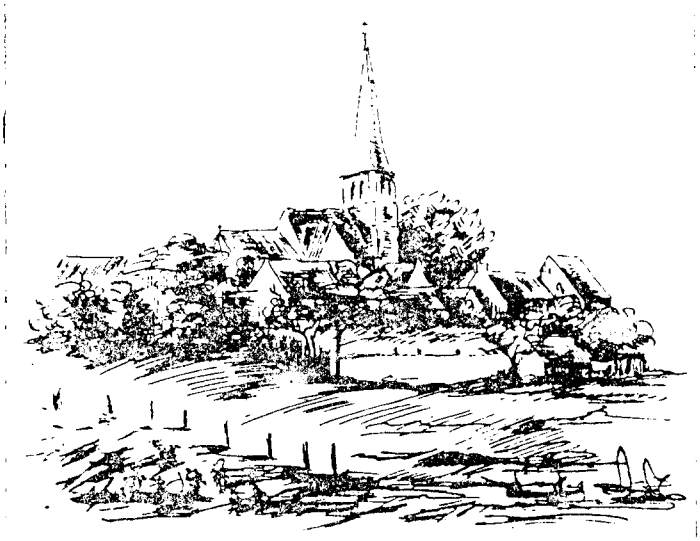
Maandelijks Infoblad van de :
TECHNOLOGY INTEREST GROUP HEIST-OP-DEN-BERG
Jaargang 3, Nummers 7,8,9, Juli, Augustus en September 1993

WetensWaard

Aan:

ONL8969
Luyten Joost
Werfsesteenweg, 44
2220 HEIST-OP-DEN-BERG



Verantwoordelijke Uitgever:
ONHAJO
NYS Jozef, Kerkhofstraat, 25
2220 Heist-op-den-Berg

Tel: 015/25.14.35

Postkantoor van afgifte:
2220 HEIST-OP-DEN-BERG 2

WETENSWAARD

Het maandelijks infoblad van de

TECHNOLOGY INTEREST GROUP

Heist-op-den-Berg

Samenstelling U.B.A. en V.V.R.A

U.B.A

Voorzitter
LE GUEN Pierre , ON5IE
Klein Bollostraat 42
3120 TREMELO

QSL-Manager
CLAUW Guido, ON1BGC
Stationssteenweg, 15
2560 KESSEL

V.V.R.A.

Voorzitter

SPRUYT Paul , ON1APS
Processieweg, 13
2260 WESTERLO-Heultje

Verantwoordelijke
Uitgever
en
Redaktie

ON4AJO
NYS, Jozef
Kerkhofstraat 25
2220 HEIST O/D BERG
Tel: 015 / 25 14 35

KALENDER 1993 T.I.G. - H.O.B.

08 Januari:	ATV- Voordracht door ON5IE, Kathode Modulatie van een 2C39
12 Februari:	Vrij
12 Maart:	Vrij
09 April:	Vrij
14 Mei:	Vrij
11 Juni:	Vrij
09 Juli:	Vakantievergadering
13 Augustus:	Vakantievergadering
10 September:	Vrij
08 Oktober:	Vrij
12 November:	Vrij
10 December:	Vrij

WE FELICITEREN.

Wij feliciteren onze jarigen:
Van der Auwera Ria op 2 Juli; Vercammen Jean Paul op 7 Jul; ON1ABH, Carl op 11 Juli;ON1BGC, Guido op 17 Juli; ON7CQ ,Ronald op 19 Juli; ON1BBU, Wilfried op 26 Augustus ; ON1AIN, Luc op 14 Augustus;ON1BIO, Thierry op 3 September en tot slot ONL 7761, Stefan op 26 September. Aan allen proficiat en nog vele jaren.

INHOUDSOPGAVE:

Medewerkers gezocht

Graag had ik enkele medewerkers gevonden die bereid zijn af en toe een artikel te schrijven over hun bezigheden in de radio-amateur wereld. Er zijn onder onze leden diverse specialisten in diverse modes en die moeten toch af en toe enkele tips kunnen geven.
Verder zoek ik ook personen die me maandelijks info toesturen voor een rubriek *" Voor U gelezen "* die ik zou willen opstarten. Niet wat betreft radio-amateurtijdschriften, die vinden we in CQ-QSO maar wel andere Elektronika tijdschriften en van de diverse Computertijdschriften. Andere Wetenschappelijke publicaties worden ook gelezen en alle artikels zijn welkom, zolang ze passen in ons ruim kader van de Technology Interest Group. Bij voorbaat dank voor Uw spontane reakties.
Publicaties in mijn bezit, die nog niet verschenen zijn, komen later aan bod. Aan de auteurs dus " dont't panic"

RADIO VLAANDEREN INTERNATIONAAL (RVI)

Radio Vlaanderen Internationaal is te bereiken :

- per brief : Postbus 26
B-1000 BRUSSEL

- per telefoon : 02-741.38.02 (dienst Public Relations)

buiten de kantooruren:
02-741.38.08 (Regie)

- per fax : 02-732.62.95 (nieuw nummer!!)

- per computer en modem : 03-825.36.13 (via DXA-BBS, waar u ook een bericht kunt achterlaten voor RVI)

De Wereldomroep op teletekst :

pag. 467 programma's
pag. 468 toelichtingen bij de programma's
pag. 469 de Wereldomroep in Belgie, Europa en de rest van de wereld
pag. 470 frequentiewijzigingen
pag. 471 mededelingen
pag. 472 frequenties zomerschema
pag. 473 adres
pag. 474 kortegolf-tips

pag. 333 wereldklok
pag. 380 ligging zeeschepen

Info door Armand, ON9BBS

REDAKTIONEEL

De vakantiemaanden zijn achter de rug en stilaan herneemt zich het dagelijkse leven zoals we het ervaren. Een sleur zou ik het niet durven noemen alhoewel. Enkele gelukkigen onder ons verblijven nog op een vakantiebestemming en zien met lede ogen ook het einde van hun vakantie naderen.

De aktiviteiten in het radio-amateurisme zullen zich dra ook herstellen en wie in de winterperiode wat aktief wil zijn en/of eventueel aan een kontest wenst deel te nemen adviseren we nu nog vlug zijn antennepark na te kijken. De zomer bracht niet veel goed weer met zich en de septemberdagen zijn al even erg, dus profiteer van elke goede dag om de klus te klaren.

Het wordt ook stilaan tijd dat de schrijvers van artikels zich aan het werk zetten, de voorraad hier op de redactie is uitgeput. Met uitzondering van enkele korte artikels die Luc, ON1AIN schreef blijft er niets aktueel over. Herman, ON4AVI, is bezig aan een SPIDER - QUAD en in de mate van het mogelijke verschijnt hierover een technisch artikel in ons volgend nummer. Tevens ontving ik van Herman een PC programma VHFLOG geschreven door ON7FH. Ik heb dit vlug bekeken en kan U mededelen dat het een prachtig programma is dat weinig uitlegt vergt en waarmee de contesters onder ons wel een degelijk log zullen kunnen samenstellen. Ik hoop ook dat Andre, ON1AIG, waarvan U de voorlaatste aflevering van zijn artikel over VIRUSSEN hier kunt lezen, weer wat van zich laat horen, mogelijks met TRACK-LOG Andre. ?.....

De voorzitters van zowel U.B.A. als V.V.R.A. hebben de laatste maanden ook niet veel bijgedragen aan WetensWaard, ik hoop dat ook zij wat meer gaan informeren via ons clubblad.

Blijven nog de schrijvers van de technische artikels over, ik hoop dat zij tussendoor ook nog wat tijd vinden om ons een interressant bouwproject of een nieuwigheid toe te lichten.

Tijdens de vakantiemaanden Juli en Augustus is er geen WetensWaard verschenen. Allerlei factoren hebben hierin een rol gespeeld en ikzelf heb dan (noodgedwongen) ook maar wat op mijn lauweren gerust. Pientere lezers hebben dit al gemerkt wanneer ze op de voorpagina gelezen hebben dat dit nummer voor 3 maanden geschreven is.

Rest er mij nog U veel sterkte toe te wensen in Uw werk en/of studies en veel leesgenot met dit nummer, tot in het volgende nummer.

73, Jef, ON4AJO

Notulen Vergadering T.I.G. - H.O.B.
Juli - Augustus.

Vakantie !!!!!!!
Gesloten wegens Jaarlijks Verlof

Het is niet mogelijk op deze kleine oppervlakte de notulen, zoals gewoonlijk gepubliceerd , neer te schrijven. Er waren duidelijk vele clubleden die toch behoefte hadden om naar de vergadering te komen , dit merkten we aan het aantal bezoekers zowel in Juli als in Augustus.

Het deed ons zelfs veel plezier op deze vakantievergadering mensen te mogen begroeten die belangstelling hebben voor onze hobby en zich willen wagen aan de RTT of moet ik nu schrijven BIPT examens om os te vergezellen in onze hobby. Dus weeral nieuw leven kortelings in onze kontreien. Dat hoop ik althans.

Diegenen die afwezig waren werden verondersteld op verlof te zijn. Dit is slechts een vermoeden want geen enkel lid deelde plaats, tijd of andere info mede om eventueel QSO's te draaien.

Weeral om allerlei diverse factoren heb ik de lokalen wel geopend tijdens de vakantie doch ben zelf niet kunnen blijven. De sleutels werden me later terug bezorgd en uit hetgeen ik vernam hebben de aanwezigen het tamelijk laat vergaderd.

Langs deze weg wil ik toch een oproep richten aan personen die op een of andere manier kunnen bijdragen om op onze vergaderingen een spreker te krijgen, die ons over een of andere tak van de hobby komt onderhouden, dit jaar is het op dit vlak vrij rustig geweest.

Ronald, ON7CQ is de laatste die een voordracht gaf over de examens bij de ARRL, de uitgeschreven teksten vindt U in dit nummer.

Verder valt er weinig te vertellen over deze vakantievergaderingen, de opkomst was vrij hoog en de sfeer was duidelijk ontspannen, dit stimuleert de vriendschapsbanden onderling

De aanwezigheden werden wel genoteerd en diegenen die echt wensen te weten wie er al dan niet aanwezig was op de vergadering kan dit navragen bij Pierre, ON5IE CM HOB.

Ondertussen heb ik, U waarschijnlijk ook, een uitnodiging gekregen van de diensten B.I.P.T om de jaarlijkse taksen te betalen. Vergeet dit vooral niet. Anders is U in overtreding.

Zo, volgende maand zal ik weer trachten in deze rubriek U een overzicht te geven van de vergadering in September. Met alle aan- en afwezigen, besproken onderwerpen en alle nuttige nieuwtjes, tot zolang.

73, Jef, ON4AJO

Info

OSCAR OSCAR PREFIX BELGIUM

DEAR YL, OM,
BELGIAN AUTHORITIES HAVE GRANTED PERMISSION FOR BELGIAN RADIO AMATEURS TO USE THE PREFIX "OO" (OSCAR OSCAR) INSTEAD OF THE REGULAR "ON" PREFIX. THIS TO COMMERMORATE THE CROWNING OF KING ALBERT II. THIS PREFIX MAY BE USED BETWEEN 10 AUG 93 00:00 AND 30 SEP 93 24:00. **SIGNED OO7CI,** PRESIDENT FLEMISH RADIO AMATEUR SOCIETY.

UBA @ON7RC de:ON6JG 06.08.93 14:17 61 1457 Bytes OO Prefix *** Bulletin-ID: 068306ON7RC ***
de ON6JG @ ON7RC.BT.BEL.EU to UBA @ ON7RC.BT.BEL.EU

TROONSBESTIJGING VAN ZIJNE MAJESTEIT KONING ALBERT II

Ter gelegenheid van de troonsbestijging van Zijne Majesteit Koning Albert II, verleent de Minister van Verkeerswezen en Overheidsbedrijven aan de Belgische radioamateurs de toelating, in hun roepnaam het voorzetsel "OO" te gebruiken in de plaats van het voorzetsel "ON". Deze toelating geldt van dinsdag 10 Augustus 1993 om nul uur, tot 30 September 1993 om 24 uur, plaatselijke tijd. **(Medegedeeld door ON4WF**, Voorzitter van de U.B.A.).

ACCESSION AU TRONE DE SA MAJESTE LE ROI ALBERT II

A l'occasion de l'avenement de Sa Majeste le Roi Albert II, le Ministre des Communications et des Entreprises publiques autorise les radioamateurs Belges a utiliser leur indicatif avec le prefixe "OO" en lieu et place du prefixe "ON". Cette autorisation est valable du mardi 10 aout a 0 heure jusqu'au 30 septembre 1993 a 24 heures, temps local. (Communique par ON4WF, President de l'U.B.A.).

THE CORONATION OF HIS MAJESTY KING ALBERT II

To celebrate the inauguration of His Majesty King ALBERT II, Belgian radio amateurs may replace their "ON" prefix by using "OO" (Oscar, Oscar) from August 10 1993 until September 30 1993. (Communicated by ON4WF, President of U.B.A.)

Voordracht

Op 24 September 1993 te 19.30 uur is er in het lokaal van de radio-amateurs te **DIEST** een voordracht door **ON4PW**, POPPE Arthur uit Kalken een voordracht over:
Windbelasting op antennes en antennemasten en bijhorende sterkteberekeningen.

tevens richt de sektie **DIEST** een **ONL-cursus** in
Plaats: Cafe SYRK
Turnhoutsebaan, 7
3290 DIEST

INFO ON4AYP Neveistreen Francois
014/ 30 16 24

Alle verdere informatie op telefoon 013/32.18.24 of op de clubfrequentie 144.725 MHz.

Gezocht

Onze vriend, Armand, ON9BBS, zoekt een beugel om zijn mobiele tranceiver een YAESU FT 227R te monteren in zijn voertuig. Telefoon 03/411.06.27.

HET WETEN WAARD ...

Iedereen van ons kent een modem. Het klink in deze tijd vanzelfsprekend dat men zulk een kleinood gebruikt om datacommunicatie te plegen met andere modemgebruikers of ook de zogenoemde BBS-en. Bits, pariteit stopbit en nog ander fraais ... wat heeft dat toch allemaal te betekenen ? Een verklarend woordje uitleg .

We weten dat de ASCII-code letters en andere tekens kan opslaan in de zogenoemde acht-bits-code, met in het totaal 256 mogelijkheden. De oorspronkelijke **ASCII-code** omvatte slechts 7 bits,wat slechts een combinatie toeliet van 128 tekens, veruit niet genoeg voor de veel gebruikte bijkomende symbooltekens die de meeste talen in zich hebben (denk maar eens aan de accenten...).

De huidige modems houden nog steeds rekening met de mogelijkheid om over te schakelen van 8 naar 7 bits en omgekeerd. Dus de eerste instelling die bij een modem dient te gebeuren zal de keuze tussen de beide mogelijkheden moeten zijn.

Toch wordt er 8 bits doorgestuurd, omdat de eventuele 8 ste bit kan gebruikt worden als controle-bit. Hoe gaat dat in zijn werk... Veronderstel dat wij de letter "C" willen doorsturen. Binair is dat 1000011. We ontdekken in deze binaire code drie bits met de waarde "1". Voegen we daar als controle nog een "1" aan toe dan is het aantal énen paar. Is in een andere code het aantal énen reeds paar, dan voegen we een "nul" toe en we houden het dus zo. In een engelse term wordt dit **PARITY EVEN** genoemd. Omgekeerd zou uiteraard ook kunnen en dan spreken wij van **PARITY ODD** of oneven pariteit. **NO PARITY** kan uiteraard ook.

Zulke instelling moet je natuurlijk zomaar niet kiezen. Alles hangt af van de instelling van je correspondentiepartner. Wanneer we naar de specificatie van een BBS kijken dan vinden we steeds deze gegevens terug, en als laatste element vinden we de stopbit.

Nu kunnen we deze 8-bitsinformatie parallel (over acht draadjes) of serieel gaan doorsturen. Voor de gegevens naar een printer te sturen kunnen we dat best inderdaad parallel doen. Bij het gebruik van de telefoon hebben wij uiteraard zulke middelen niet ter beschikking.

Het alternatief, is dus de seriële communicatie. Daartoe moeten al deze tekens in rijen worden opgesplitst die achter elkaar doorgestuurd worden. Als nu de ontvangende bron elke acht bit die binnenkomt, zou kunnen onderscheiden dan is er helemaal geen probleem, want eens een eerste bit gedetecteerd loopt alles volgens plan. De klok van de ontvanger wordt immers verplicht in gelijke pas te lopen met deze van de zender. Dit noemen we **SYNCHRONE** transmissie.

In het andere geval is dat niet zo, want heel wat BBS-en werken **ASYNCHROON**. Dat maakt dat na elk rijtje van 8 bits, laat ons zeggen, een opening moet voorkomen die de herkenning van elk achttal mogelijk maakt.

Eigenlijk zit het zo dat ieder teken wordt ingeleid door een startbit met een waarde" 1", en eindigt met een stopbit met waarde "0". Het startbit zet telkenmale de identificatie van het teken in zodat enig verschil in kloktijd geen probleem meer vormt.

De Fransman Baudot gaf zijn naam aan de eenheid van transmissiesnelheid. Een snelheid van 300 baud = aan 300 bits per seconde...Dat komt overeen met ongeveer 30 lettertekens, absoluut niet snel .

Nu zijn de moderne modems heel wat sneller. Het probleem van snelheid zit hem meestal in de kwaliteit van de telefoonlijn. Als de kwaliteit uitstekend is, kan je rustig je modem op 9600 baud zetten. Is de kwaliteit niet denderend, dan ga je merken dat de snelheid van uw modem automatisch terugvalt tot meestal 2400 baud. De test van die telefoonlijn mag je rustig overlaten aan je modem, hij klaart die karwei wel zelf.

Bij **DUPLEX-verkeer** is de communicatie in beide richtingen mogelijk. **SIMPLEX** is dus daar het omgekeerde van. Een voorbeeld van SIMPLEX verkeer is de teletekst op je TV. **HALF DUPLEX** wil zeggen dat de richting kan omgekeerd worden door het omschakelen aan het einde van het bericht, net zoals wij amateus zeggen: "....over". Bij DUPLEX gebruiken we nog de termen **ORIGINATE** en **ANSWER**. Dit is belangrijk opdat wij de zender en de ontvanger van elkaar moeten kunnen onderscheiden door signalen te gebruiken.

Er betaat ook nog de zogenamde **SPLIT-baudrate**. Dan tref je bijvoorbeeld 1200/75 baud aan...Dan wil dat zeggen dat de 'zendsnelheid' in de ene richting 1200 baud is en in de andere richting slechts 75 baud is. Wel erg traag zou ik denken...

Je hebt wel begrepen dat een zo hoog mogelijke snelheid tengoede komt aan je telefoonrekening. Maar nogmaals alles hangt af van de kwaliteit van de lijn.

Als deze kwaliteit echter uitstekend is zoals bij specifieke DATA-lijnen, dan kunt ge hoge snelheden halen. Maar dan moet ge weer diep in je zak tasten voor de huur van zulk een datalijn...

73's from Luc , ON1AIN

USA EXAMENKOORTS

— door ON7CQ —

USA amateur radio licence

Een Amerikaanse licentie bestaat uit 2 delen, namelijk een *station-license* die je het recht geeft om een vast station op te stellen op een bepaald adres en een *operator-license* die je bepaalde operator-privileges geeft op het vlak van frequentiebanden, modes en vermogens. De licentie is 10 jaar geldig en wordt verleend door de *FCC - Federal Communications Commission* welke met onze BIPT/NCS te vergelijken is. Als de looptijd bijna verstreken is kan je deze verlengen met opnieuw 10 jaar door middel van de *610-Form*, een formulier dat gebruikt wordt voor alle administratie aangaande radio-amateur licenties (bvb. initiële licentie-aanvraag, adreswijziging, enz...) Je dient steeds minstens een kopie van je licentie op zak te hebben wanneer je radio-amateurisme bedrijft in de USA en in de basis-shack moet eveneens minstens een kopie aanwezig zijn. Het origineel mag veilig ergens weggeborgen zijn.

De enige 2 vereisten om een licentie te verkrijgen is dat je geslaagd bent in een examen en dat je bereikbaar bent via de *U.S. Mail Service* – je moet met andere woorden een adres in de USA hebben waarop je alle post die van de *FCC* komt, kan ontvangen. Dit kan een Amerikaans familielid of kennis zijn die bereid is alle post door te sturen naar het adres waar je werkelijk woont (indien dat buiten de USA is).

USA amateur radio principles

De *FCC* heeft 5 doelstellingen gedefinieerd waarop de *amateur radio service* gefundeerd is:

1. Het verlenen van een vrijwillige niet-commerciële communicatie-service aan het publiek, meer specifiek de erkenning van de communicatie in nood-omstandigheden,
2. De vooruitgang van de radio - kunst,
3. Verbetering van de communicatie (operator) bekwaamheid en technische bekwaamheid,
4. Het verhogen van het aantal getrainde radio-operatoren en electronica specialisten,
5. De verhoging van de internationale *GOODWILL*

Deze *5 principles* zijn de rode draad die in de USA door heel de reglementering van het radio-amateurisme loopt. Wie er tegen zondigt loopt risico geschorst te worden of zijn licentie volledig te verliezen. Wat erg lovenswaardig is, is dat de voorrangs-positie van *emergency communications* (punt 1), het belang van vooruitgang op technisch vlak (bvb. het testen van nieuwe modes, punt 2) en het aan de dag leggen van de nodige *Hamspirit* (punt 5) benadrukt worden.

Do's and don't's

De Amerikaanse radio-amateur mag heel wat, maar er zijn enkele dingen die niet kunnen. Zo is het uit den boze om *Business Communications* te voeren op de frequenties. Bvb. een pizza bestellen mag dus niet, evenmin als reclame maken voor een bepaald merk van toestellen of een distributeur van apparatuur. Eveneens dien je je handen af te houden van uitspraken die onzedelijk zijn, iemands overtuiging kunnen schaden of die staatsondermijnend zijn. Je transmissies mogen niet geheim gecodeerd

noch misleidend noch ongeïdentificeerd zijn, noch een kriminele aktiviteit steunen, noch muziek bevatten, noch betaald worden, noch bedoeld zijn om nieuws te vergaren. Sommige van de bovenstaande zaken zijn wel onder zeer uitzonderlijke en gedefinieerde omstandigheden toch toegelaten. Bvb. nieuwsvergaring wanneer normale communicatiekanalen niet meer toegankelijk zijn in een bepaald gebied.

Verder is er niet veel wat niet mag in de USA. Noodomstandigheden verbreden meestal wat toegelaten is. Noodomstandigheden heeft men nauwkeurig gedefinieerd als elke toestand waarbij menselijk leven of eigendom in onmiddellijk gevaar verkeren. Dus via frequentie doorgeven dat een inbraak gaat gebeuren in pizzeria X mag wel en is in die context geen *Business Communication* maar een beveiliging van een eigendom. Ook mag men in noodomstandigheden gebruik maken van eender welke radio-middelen men tot zijn beschikking heeft!

Amateurs mogen in de USA ook *third-party traffic* doorgeven, dit zijn berichten van persoonlijke aard die belangeloos worden doorgegeven tussen radio-amateurs tot ze hun doel bereikt hebben. In dit verband bestaan er zelfs speciale *third-party traffic-nets* die op afgesproken periodes dergelijke berichten doorgeven. Ook mag zelfs een niet-gelicentieerde (is ook een *third-party*) onder permanent toezicht van een wel-gelicentieerd radio-amateur het station gebruiken! De gelicentieerde dient konstant het toezicht te houden en blijft verantwoordelijk voor het gebruik van het station.

Repeaters mogen in de states met elkaar verbonden zijn in *repeater-nets*, dit zijn een aantal stations die met elkaar verbonden zijn en op die manier een link vormen over ettelijke honderden kilometers. Dit maakt het mogelijk om bvb. op VHF portabele stations met elkaar over dergelijke afstanden te laten communiceren. Ook mogen repeaters een verbinding vormen met het telefoonnet, mits men zich houdt aan de algemene beperkingen wat betreft de inhoud van de communicatie die men voert.

Radio-afstandsbesturing is toegelaten aan gelicentieerde radio-amateurs. Men dient hier wel volgens bepaalde voorschriften tewerk te gaan (bvb. het adres en het roepteken van de radio-amateur moeten duidelijk aangebracht zijn op de gebruikte apparatuur). De kodering van de stuursignalen wordt hier niet als geheim gezien.

Naast al deze mogelijkheden die de Amerikaanse radio-amateur kan benutten dient hij wel de nodige hoffelijkheid oftewel *Hamspirit* aan de dag te leggen. Zo heeft de *FCC* wettelijk vastgelegd dat elke *Ham* het MINIMAAL vereiste vermogen dient toe te passen nodig om de communicatie betrouwbaar tot stand te brengen. Met andere woorden: 1500 Watt mag, maar ENKEL als het werkelijk nodig is... Zo dient men ook lokale communicatie te houden op banden die daarvoor geschikt zijn en niet op een frequentieband die openstaat voor veraf gelegen stations... Men dient ook de communicatie te voeren op voldoende frequentie-afstand van andere aan de gang zijnde verbindingen zodat deze niet gestoord worden... Mobiele stations moeten tijdens verkeers-piekuren voorrang krijgen voor het gebruik van repeaters... Het testen van zenders dient te gebeuren met een *dummy load* en niet op frequentie... Dit zijn allemaal hoffelijkheids-regels waaraan men verondersteld wordt te voldoen, wil men in de USA als volwaardig radio-amateur door het leven gaan. Elk radio-amateur draagt op die manier bij aan de *self-disciplined* en *self-policing service* met de gekende hoge standaard.

USA amateur radio privileges

In de USA zijn er 5 verschillende licentie-niveaus in gebruik, namelijk *Novice, Technician, General, Advanced,* en *Extra. Novice* komt qua privileges zowat overeen met onze ON2-licentie, *Technician* met ON1 en *General* met ON4+. Om deze niveaus te halen dien je een examen af te leggen dat bestaat uit een schriftelijk gedeelte betreffende techniek en wetgeving en een praktisch morse gedeelte. Voor *Technician* dien je geen morse-kunst te bewijzen. Om op te klimmen in de privilege-ladder moet je achtereenvolgens verschillende examen *elements* af te leggen. Deze zijn als volgt:

LICENCE	MORSE	TECHN./REGUL.	EQUIVALENT
Extra	1C (20 WPM)	2 + 3A + 3B + 4A + 4B	
Advanced	1B (13 WPM)	2 + 3A + 3B + 4A	
General	1B (13 WPM)	2 + 3A + 3B	ON4+
Technician	-	2 + 3A	ON1
Novice	1A (5 WPM)	2	ON2

Hoe moet je deze tabel nu lezen? Enkele voorbeelden zullen dit verduidelijken. Om *General* te bereiken dien je examen *elements 1B, 2, 3A* en *3B* met succes af te leggen. Hierin is 1B een morse decodeer-test aan 13 woorden per minuut (meting volgens de PARIS-methode, d.w.z. 13 keer het woord PARIS geseind binnen 1 minuut). 2, 3A en 3B zijn elk elementen die handelen over techniek en wetgeving (*Regulations*). Om nu een *upgrade* te bereiken naar het *Advanced* niveau dien je enkel *element 4A* af te leggen, dit kan op een latere datum zijn (bvb. na enkele jaren als *General* de hobby bedreven te hebben). De *Technician* licentie is een beetje speciaal: je moet er geen morse test voor af leggen. Dit is dus de enige licentie waarvoor je niet alle testen van de niveaus daaronder moet afgelegd hebben. Doe je echter toch *element 1A*, dan heb je een licentie van *Technician with HF-privileges.*

Op welke frequentiebanden geven deze niveaus nu recht? Als *Novice* mag je werken op beperkte bandgedeeltes van 23 cm (max. 5 Watt PEP all mode), 1.25 m (max. 25 Watt PEP all mode) en op een hele reeks HF banden enkel in CW met een 'beperkt vermogen' van maximaal 200 Watt PEP nl. op 10, 15, 40 en 80 meter. Als *Technician* mag je globaal gezien werken in all mode met een maximum van 1500 Watt PEP op de banden 13 cm, 23 cm, 33 cm, 70 cm, 1.25 m, 2 m en 6 m. Als je een licentie *Technician with HF-privileges* hebt dan kan je de banden van het *Novice*-niveau er ook nog bij gebruiken. Als *General* mag je natuurlijk op alle banden van Novice en Technician werken, maar daar komt bij dat je in alle modes mag gaan op HF en met een hoger vermogen van maximaal 1500 Watt PEP. Ook zijn de HF-bandsegmenten die je mag gebruiken breder dan voor *Novices.* De niveaus *Advanced* en *Extra* betekenen niet zoveel meer, enkel een paar kleine bandsegmenten (waar bvb. high speed CW wordt beoefend) krijg je er nog bij. Deze niveaus hebben echter wel meer betekenis in verband met de inrichting van de *amateur radio exams,* zoals je verder zal lezen.

USA amateur radio exams

Tot een 10-tal jaar geleden werden examens in de USA afgenomen door de *FCC* zelf. Door kostenbesparende maatregelen en het vertrouwen dat de verenigingen hadden kunnen opbouwen bij de *FCC* is men echter overgestapt naar een systeem waarbij de examens door de radio-amateurs zelf worden ingericht. Dit systeem werkt met *VECs (Voluntary Examiner Coordinators)* en *VE-teams (Voluntary Examiner teams).* Een *VEC* is meestal een radio-amateurclub (bvb. de *ARRL - American Radio Relay League)* welke onder toezicht van de FCC de coördinatie van verschillende *VE-teams* waarneemt. Een dergelijk team bestaat dan uit minstens 3 gelicentieerden (van een minimum niveau) welke de examensessies inrichten. Afhankelijk van het niveau van de testen die de *VEs* willen afnemen, moeten zij ook zelf een hoger niveau hebben. Het *Novice*-examen kan bvb. afgenomen worden door *General VEs,* voor de hogere nieveaus heeft men *Advanced* en *Extra VEs* nodig. De leden van een *VE-team* staan onder een strikt toezicht van de *VEC,* en bij de minste onregelmatigheden kan men zijn erkenning als *VE* of

zelfs zijn licentie kwijtspelen of geschorst worden. De *VEC* coördineert alles en maakt bvb. ook de testmaterialen aan welke door de teams gebruikt worden om de examens af te nemen. Voor gehandicapte personen past men de testen aan of stelt men ze vrij. De teams die examens inrichten moeten dit vooraf aankondigen (bvb. in packet radio) bij zoveel mogelijk geïnteresseerde partijen.

Preparing for the examination

Jezelf voorbereiden op de examens is helemaal niet moeilijk. De *ARRL-VEC* bvb. geeft publikaties uit welke het volledige studiemateriaal bevatten voor elk van de licentie-niveaus. Deze boekjes bevatten ook de *Question Pools* met alle multiple choice vragen waaruit de examens samengesteld worden. Deze vragen worden op het examen op exact dezelfde manier gesteld zoals ze vermeld zijn in deze gidsen. Je kan dus nooit van een verrassing spreken op het examen, want de vragen en hun antwoorden waren van voor het examen al bekend! Uiteraard zijn de vragenlijsten zo uitgebreid dat kennis van de vragen zo goed als gelijk staat met de volledige kennis van het studiemateriaal. De meeste vragen zijn steeds zo opgevat dat ze zonder problemen kunnen opgelost worden door een radio-amateur die zijn kennis heeft vergaard door het opdoen van ervaring tijdens het beoefenen van de hobby. Dit principe *Learn by Experience* trekt zich ook door in de moeilijkheidsgraad van de examens. Het *Novice* niveau ligt namelijk niet erg hoog, zodat iedereen met een minimum aan inspanning kan kennis maken met het radio-amateurisme en kan verder leren door ervaring op te doen 'via de band'. Elk hoger niveau kan in principe op dezelfde manier door ervaring 'aangekweekt' worden. Het enige wat men voor het *Novice* niveau goed moet onder de knie krijgen zijn de eerste elementaire *Regulations* en *Operating Practices*, welke in de studiegidsen uitstekend uitgelegd worden. Informatie over deze studiegidsen vind je in het maandblad *QST* van de *ARRL*. De volgende titels zijn ter beschikking:

- *Now You're Talking: All You Need To Get Your First Ham License.* (Behandelt het technisch en wetgevings studiemateriaal + *Question Pools* van het *Novice* en *Technician* niveau. Bevat ook een interessante introduktie tot de hobby en erg boeiende delen over *Operating Practice*, veiligheid en hoe je een station kan opbouwen, enz...)

- *The ARRL General Class License Manual*
- *The ARRL Advanced Class License Manual*
- *The ARRL Extra Class License Manual*

Daarnaast geeft de *ARRL* nog een hele reeks interessante boekwerken uit die vrijwel elk aspect van het radio-amateurisme op een praktische wijze belichten. Om morse aan te leren stelt men apart studiemateriaal ter beschikking bestaande uit een gids en oefen-cassettes.

USA amateur radio exam session

Hoe gaat het er op een dergelijke examensessie nu aan toe? Ik had het geluk er zelf recent een mee te maken op de *BITBURG AIRBASE* in Bitburg, Duitsland. Hier worden ongeveer 3 tot 4 keer per jaar examensessies gehouden door een lokale organisatie van Amerikaanse radio-amateurs. Een lokatie waar een *Test Session* wordt gehouden noemt men de *Test Site*. De lokatie kan eender welke plaats zijn waar de leden van het *VE-team* hun keus hebben op laten vallen om de examensessie te houden (mits toelating van de eigenaars natuurlijk). De meeste *test sites* bevinden zich natuurlijk in de USA, maar er zijn er ook een aantal in het buitenland, zoals in Duitsland te Wiesbaden en Bitburg. Sommige teams vereisen dat je vooraf registreert dat je zal meedoen, maar in Bitburg werkt men volgens het *Walk-In* principe. Dit wil zeggen, je loopt het lokaal binnen en geeft jezelf op dat je wil meedoen aan de examens. Men registreert je deelname en je dient dan de *test-fee* van iets minder dan 6 US$ te betalen. Als je enkel de *Novice exam elements* (dus 1A en 2) wil meedoen, dan is je deelname gratis! Je dient een *Form 610* in te vullen, waarop je je identificatie aangeeft en ook het *US Mail serviced address* waar de *FCC* de licentie uiteindelijk naartoe mag sturen. Je moet jezelf kunnen identificeren aan de hand van 2 documenten (bvb. identiteitskaart en rijbewijs).

De morsetesten gebeuren volgens het 'moeilijkste eerst' principe. Dit wil zeggen men begint met 20 WPM, daarna komen onmiddellijk 13 WPM en 5 WPM testen aan de beurt. Je krijgt op een cassetterecorder een doorgang te horen van een station dat bezig is aan een QSO en daarin bepaalde informatie geeft zoals zijn naam, de lokatie, het weer, de gebruikte *rig* en *antenna*, hoeveel staten en landen hij/zij al gewerkt heeft, enz... Nadat je deze doorgang hebt opgenomen, krijg je een vragenlijst met 10 vragen en multiple choice antwoorden waarop je minstens 7 korrekt dient te beantwoorden om te slagen. De vragen gaan over de inhoud van het QSO, bvb. 'Wat was het roepteken van het seinende station', of 'Met welk land heeft het station regelmatig een sked?' Men test dus niet specifiek je letter - per - letter vertaalvermogen van de Morse-tekens maar wel je begrip van de inhoud van het QSO. Als je de 7 vragen niet haalt, kijkt men nog na of je eventueel minstens 1 minuut van volledig korrekt gedecodeerde Morse hebt genoteerd. In voorkomend geval ben je alsnog geslaagd. Ben je geslaagd in een bepaald Morse-niveau (bvb. in 13 WPM) dan hoef je de lagere test (5 WPM) niet meer mee te doen.

De schriftelijke testen aangaande de *Technical/Regulations* gedeelten volgen elkaar op in omgekeerde volgorde, dus van laag naar hoog, dit omdat je om een bepaald niveau te bereiken, je toch moet slagen in de examens van alle niveaus daaronder. Uiteraard moet je niveaus waarin je vroeger al geslaagd was, niet meer opnieuw doen. Elke test bestaat uit enkele 10-tallen multiple choice vragen waarvan je je antwoorden moet aanbrengen op een apart *answer-sheet*.

Zowel bij de Morse- als de schriftelijke testen controleert men je resultaat onmiddellijk en stelt men je direkt op de hoogte dat je al dan niet geslaagd bent voor het betreffende element. Ben je inderdaad geslaagd, dan kan je onmiddellijk verder doen met de test van het volgende hogere niveau. Ben je niet geslaagd, dan kan je (mits opnieuw-betaling van de *test-fee*) dezelfde test opnieuw proberen, uiteraard zijn het dan andere vragen (maar wel uit dezelfde *Question Pool* van het betreffende niveau). Voor de Morse testen mag je eveneens meer dan 1 keer opnieuw proberen.

Je bent niet verplicht om zowel het Morse-gedeelte als het schriftelijk gedeelte van een bepaald niveau op een en dezelfde *exam-session* met succes te bereiken. Je kan dus zonder meer je eerst concentreren op bvb. het schriftelijke gedeelte en daarin slagen, en pas op een latere sessie de vereiste Morse-testen afleggen voor het niveau dat je schriftelijk al bereikt hebt. Je moet een bepaald niveau echter wel binnen het jaar volledig opgebouwd hebben, want anders vervallen je vrijstellingen en zal je de betreffende *exam elements* opnieuw moeten afleggen. Dit jaar geeft echter in elk geval wel voldoende ruimte om je licentie aan je eigen ritme op te bouwen, en zonder al te veel stress aan de examens deel te nemen.

De manier van testen is er duidelijk op gericht om de testkandidaten zich zo gemakkelijk mogelijk te laten voelen. Examen-stress is er helemaal niet bij omdat je niet binnen een bepaalde tijd dient af te geven en als het niet van de eerste keer lukt, mag je altijd opnieuw proberen. Op de testsessie in Bitburg hing ook een rustige en joviale sfeer van radio-amateurs onder elkaar, natuurlijk werd er wel volgens de regels van de *FCC* de examens afgenomen. De examinatoren probeerden ook echt iedereen verder te motiveren om wanneer men niet slaagt, het toch opnieuw te proberen. Aan het eind van de examensessie vult men een *CSCE - Certificate of Successful Completion of Examination* in, dit is een documentje dat bewijst dat je geslaagd bent in bepaalde examen *elements*. Als je voor het examen al een licentie had (bvb. je had een *Novice*) en je haalt een hoger niveau (bvb. *General*) dan mag je onmiddellijk na het examen je verhoogde privileges in de praktijk toepassen, je moet dan wel een extensie achter je roepteken gebruiken die aangeeft welk privilege je hebt bijgewonnen (dus bvb. *KB5SGH/AG* waarin *AG* staat voor *Acquired General*). Had je voordien nog geen licentie (en dus ook geen roepteken) dan moet je wachten tot de *FCC* je licentie heeft doorgestuurd. Aangezien de *ARRL-VEC* hier ook nog een tussenschakel in het papierwerk vormt mag je rekenen op een wachttijd van makkelijk 6 weken. Als je weet dat er maandelijks tot meer dan 5000 nieuwe licenties en *Upgrades* worden verwerkt dan valt deze wachttijd nog wel mee.

Conversion to Belgian license

Volgens art. 16 van het Ministerieel besluit van 19 december 1986 betreffende het aanleggen en doen werken van radio-elektrische stations door radioamateurs worden Belgen die in het buitenland geslaagd zijn voor een examen dat hun het recht verleent er een amateurstation aan te leggen en er te doen werken, met de ingezetenen van dat land gelijkgesteld. Art. 15 van hetzelfde besluit maakt onderscheid tussen vreemde radioamateurs die langer of korter dan 1 jaar in België verblijven. Op basis van de vreemde radioamateurvergunning kan men op eenvoudige aanvraag van de titularis een Belgische vergunning verkrijgen welke vervalt op 31 december van het eerste volledige jaar dat volgt op de datum van de aanvraag. Het in het buitenland afgelegde examen moet wel van een niveau zijn dat minstens gelijkwaardig of hoger is dan de Belgische A-, B- of C-examens. In elk geval kan men minstens een vergunning voor een station van de sectie A op deze manier verkrijgen.

Dat deze conversie werkt, is reeds bewezen geweest door iemand binnen onze HOB-TIG. En niet alleen voor het laagste *Novice* niveau. Het station in kwestie wist op deze manier al een licentie in de wacht te slepen voor een vergunning van de sectie B (dus het ON1-equivalent). En het sectie-C equivalent gaat nog volgen vermoed ik. De stations die volgens dit systeem een vergunning hebben gekregen zijn de ON9-stations. ON9A.. komt overeen met een ON2... (sectie A), ON9B.. met ON1... (sectie B) en ON9C.. met ON4+... (sectie C).

Nog een voordeel van het hebben van een Amerikaanse licentie, is dat je nooit meer een tijdelijke *Reciprocal License* moet aanvragen bij de *FCC* als je op reis gaat naar de states en er de hobby portabel en/of mobiel wil bedrijven. Een dergelijke tijdelijke vergunning kan je in de USA altijd verkrijgen op basis van je Belgische, maar je zit dan ook weer met de wachttijd van (meer dan) 6 weken. Als je wat pech hebt en de betreffende licentie blijft wat lang weg, dan kan je het wel vergeten met *amateur radio* op je reis. Met een eigen Amerikaanse vergunning heb je dit risico niet en stap je als radio-amateur binnen en buiten de USA wanneer je wilt (wel geen toeristen-visum vergeten!).

Conclusion

Het Amerikaanse radio-amateur examensysteem is er op gericht om het radio-amateurisme zo democratisch mogelijk toegankelijk te maken. De onderste sport van de ladder is erg eenvoudig te bereiken en naarmate men meer ervaring krijgt en privileges wil, kan men opklimmen door de hogere examenniveaus met succes te doorlopen. Amerikaanse radio-amateurs genieten bij de *FCC* duidelijk meer vertrouwen dan wij bij onze kersverse BIPT/NCS. Dankzij dit vertrouwen en de ver doorgedreven *self-policing* en het verantwoordelijkheidsbesef van de USA-*hams* kunnen zij zelf de examens organiseren, waardoor deze zeer sterk ingesteld zijn op de behoeften van de amateurs zelf. Zoals gewoonlijk is de USA hier weer de kartrekker op wereldvlak. Spijtig genoeg kunnen we als Belgje hier slechts van proeven en testen of we in het Amerikaanse systeem 'aan de bak' zouden kunnen komen. Onze weg is nog lang...

De inhoud van dit artikel is gebaseerd op documentatie over het onderwerp en mijn persoonlijke impressie van een examensessie in de *Bitburg Airbase* die plaatsvond op 22 mei 1993. Uiteraard kan mijn documentatie al verouderd zijn, want de reglementering wordt regelmatig aangepast aan de veranderende behoeften van de Amerikaanse *hams* en de wetgeving van de *FCC*.

73 de Ronald - ON7CQ

PS: Als je graag nog meer informatie wil over al het bovenstaande of wil meedoen aan een dergelijke testsessie, kom je maar eens naar een vergadering van HOB-TIG. Ter vervollediging volgt hier ook nog het FAX-nr. en adres waar de *ARRL* te bereiken is:

ARRL, 225 Main Street, Newington, CT 06111 USA Fax. nr. 00-1-203 665 7531

C12) I have an infinite loop of sub-directories on my hard drive; am I infected?

Probably not. This happens now and then, when something sets the "cluster number" field of some subdirectory the same cluster as an upper-level (usually the root) directory. The /F parameter of CHKDSK, and any of various popular utility programs, should be able to fix this, usually by removing the offending directory. *Don't* erase any of the "replicated" files in the odd directory, since that will erase the "copy" in the root as well (it's really not a copy at all; just a second pointer to the same file).

Section D. Protection plans

D1) What is the best protection policy for my computer?

There is no "best" anti-virus policy. In particular, there is no program that can magically protect you against all viruses. But you can design an anti-virus protection strategy based on multiple layers of defense. There are three main kinds of anti-viral software, plus several other means of protection (such as hardware write-protect methods).

1) GENERIC MONITORING programs.
These try to prevent viral activity before it happens, such as attempts to write to another executable, reformat the disk, etc.
Examples: SECURE and FluShot+ (PC), and GateKeeper (Macintosh).

2) SCANNERS.
Most look for known virus strings (byte sequences which occur in known viruses, but hopefully not in legitimate software) or patterns, but a few use heuristic techniques to recognize viral code. A scanner may be designed to examine specified disks or files on demand, or it may be resident, examining each program which is about to be executed. Most scanners also include virus removers.
Examples: FindViru in Dr Solomon's Anti-Virus Toolkit, FRISK's F-Prot, McAfee's VIRUSCAN (all PC), Disinfectant (Macintosh). Resident scanners: McAfee's V-Shield, and VIRSTOP. Heuristic scanners: the Analyse module in FRISK's F-PROT package, and SCANBOOT.

3) INTEGRITY CHECKERS or MODIFICATION DETECTORS.
These compute a small "checksum" or "hash value" (usually CRC or cryptographic) for files when they are presumably uninfected, and later compare newly calculated values with the original ones to see if the files have been modified. This catches unknown viruses as well as known ones and thus provides *generic* detection. On the other hand, modifications can also be due to reasons other than viruses. Usually, it is up to the user to decide which modifications are intentional and which might be due to viruses, although a few products give the user help in making this decision. As in the case of scanners, integrity checkers may be called to checksum entire disks or specified files on demand, or they may be resident, checking each program which is about to be executed (the latter is sometimes called an INTEGRITY SHELL). A third implementation is as a SELF-TEST, i.e. the checksumming code is attached to each executable file so that it checks itself just before execution.
Examples: Fred Cohen's ASP Integrity Toolkit (commercial), and Integrity Master and VDS (shareware), all for the PC.

3a) A few modification detectors come with GENERIC DISINFECTION. I.e., sufficient information is saved for each file that it can be restored to its original state in the case of the great majority of viral infections, even if the virus is unknown.
Examples: V-Analyst 3 (BRM Technologies, Israel), marketed in the US as Untouchable (by Fifth Generation), and the VGUARD module of V-care.

Of course, only a few examples of each type have been given. All of them can find their place in the protection against computer viruses, but you should appreciate the limitations of each method, along with system-supplied security measures that may or may not be helpful in defeating viruses. Ideally, you would arrange a combination of methods that cover the loopholes between them.

A typical PC installation might include a protection system on the hard disk's MBR to protect against viruses at load time (ideally this would be hardware or in BIOS, but software methods such as DiskSecure and PanSoft's Immunise are pretty good). This would be followed by resident virus detectors loaded as part of the machine's startup (CONFIG.SYS or AUTOEXEC.BAT), such as FluShot+ and/or VirStop together with ScanBoot. A scanner such as F-Prot or McAfee's SCAN could be put into AUTOEXEC.BAT to look for viruses as you start up, but this may be a problem if you have a large disk to check (or don't reboot often enough). Most importantly, new files should be scanned as they arrive on the system. If your system has DR DOS installed, you should use the PASSWORD command to write-protect all system executables and utilities. If you have Stacker or SuperStore, you can get some improved security from these compressed drives, but also a risk that those viruses stupid enough to directly write to the disk could do much more damage than normal; using a software write-protect system (such as provided with Disk Manager or Norton Utilities) may help, but the best solution (if possible) is to put all executables on a disk of their own, protected by a hardware read-only system that sounds an alarm if a write is attempted.

If you do use a resident BSI detector or a scan-while-you-copy detector, it is important to trace back any infected diskette to its source; the reason why viruses survive so well is that usually you cannot do this, because the infection is found long after the infecting diskette has been forgotten with most people's lax scanning policies.

Organizations should devise and implement a careful policy, that may include a system of vetting new software brought into the building and free virus detectors for home machines of employees/students/ etc who take work home with them.

Other anti-viral techniques include:
(a) Creation of a special MBR to make the hard disk inaccessible whenbooting from a diskette (the latter is useful since booting from a diskette will normally bypass the protection in the CONFIG.SYS and AUTOEXEC.BAT files of the hard disk). Example: GUARD.
(b) Use of Artificial Intelligence to learn about new viruses and extract scan patterns for them. Examples: V-Care (CSA Interprint, Israel; distributed in the U.S. by Sela Consultants Corp.), Victor Charlie (Bangkok Security Associates, Thailand; distributed in the US by Computer Security Associates).
(c) Encryption of files (with decryption before execution).

D2) Is it possible to protect a computer system with only software?

Not perfectly; however, software defenses can significantly reduce your risk of being affected by viruses WHEN APPLIED APPROPRIATELY. All virus defense systems are tools - each with their own capabilities and limitations. Learn how your system works and be sure to work within its limitations.

From a software standpoint, a very high level of protection/detection can be achieved with only software, using a layered approach.

1) ROM BIOS - password (access control) and selection of boot disk.
(Some may consider this hardware.)

2) Boot sectors - integrity management and change detection.

3) OS programs - integrity management of existing programs, scanning of unknown programs. Requirement of authentication values for any new or transmitted software.

4) Locks that prevent writing to a fixed or floppy disk.

As each layer is added, invasion without detection becomes more difficult. However complete protection against any possible attack cannot be provided without dedicating the computer to pre-existing or unique tasks. The international standardization of the world on the IBM PC architecture is both its greatest asset and its greatest vulnerability.

D3) Is it possible to write-protect the hard disk with only software?

The answer is no. There are several programs which claim to do that, but *all* of them can be bypassed using only the currently known techniques that are used by some viruses. Therefore you should never rely on such programs *alone*, although they can be useful in combination with other anti-viral measures.

D4) What can be done with hardware protection?

Hardware protection can accomplish various things, including: write protection for hard disk drives, memory protection, monitoring and trapping unauthorized system calls, etc. Again, no tool is foolproof.

The popular idea of write-protection (see D3) may stop viruses spreading to the disk that is protected, but doesn't, in itself, prevent a virus from running.

Also, some of the existing hardware protections can be easily bypassed, fooled, or disconnected, if the virus writer knows them well and designs a virus which is aware of the particular defense.

D5) Will setting DOS file attributes to READ ONLY protect them from viruses?

No. While the Read Only attribute will protect your files from a few viruses, most simply override it, and infect normally. So, while setting executable files to Read Only is not a bad idea, it is certainly not a thorough protection against viruses!

D6) Will password/access control systems protect my files from viruses?

All password and other access control systems are designed to protect the user's data from other users and/or their programs. Remember, however, that when you execute an infected program the virus in it will gain your current rights/privileges. Therefore, if the access control system provides *you* the right to modify some files, it will provide it to the virus too. Note that this does not depend on the operating system used - DOS, Unix, or whatever. Therefore, an access control system will protect your files from viruses no better than it protects them from you.

Under DOS, there is no memory protection, so a virus could disable the access control system in memory, or even patch the operating system itself. On the more advanced operating systems (Unix) this is not possible, so at least the protection cannot be disabled by a virus. However it will still spread, due to the reasons noted above. In general, the access control systems (if implemented correctly) are able only to slow down the virus spread, not to eliminate viruses entirely.

Of course, it's better to have access control than not to have it at all. Just be sure not to develop a false sense of security and to rely *entirely* on the access control system to protect you.

D7) Will the protection systems in DR DOS work against viruses?

Partially. Neither the password file/directory protection available from DR DOS version 5 onwards, nor the secure disk partitions introduced in DR DOS 6 are intended to combat viruses, but they do to some extent. If you have DR DOS, it is very wise to password-protect your files (to stop accidental damage too), but don't depend on it as the only means of defense.

The use of the password command (e.g. PASSWORD/W:MINE *.EXE *.COM) will stop more viruses than the plain DOS attribute facility, but that isn't saying much! The combination of the password system plus a disk compression system may be more secure (because to bypass the password system they must access the disk directly, but under SuperStore or Stacker the physical disk is meaningless to the virus). There may be some viruses which, rather than invisibly infecting files on compressed disks in fact very visibly corrupt the disk.

The "secure disk partitions" system introduced with DR DOS 6 may be of some help against a few viruses that look for DOS partitions on a disk. The main use is in stopping people fiddling with (and infecting) your hard disk while you are away.

Furthermore, DR DOS is not very compatible with MS/PC-DOS, especially down to the low-level tricks that some viruses are using. For instance, some internal memory structures are "read-only" in the sense that they are constantly updated (for DOS compatibility) but not really used by DR DOS, so that even if a sophisticated virus modifies them, this does not have any effect.

In general, using a less compatible system diminishes the number of viruses that can infect it. For instance, the introduction of hard disks made the Brain virus almost disappear; the introduction of 80286 and DOS 4.x+ made the Yale and Ping Pong viruses extinct, and so on.

D8) Will a write-protect tab on a floppy disk stop viruses?

In general, yes. The write-protection on IBM PC (and compatible) and Macintosh floppy disk drives is implemented in hardware, not software, so viruses cannot infect a diskette when the write-protection mechanism is functioning properly.

But remember:

(a) A computer may have a faulty write-protect system (this happens!)
- you can test it by trying to copy a file to the diskette when it is presumably write-protected.

(b) Someone may have removed the tab for a while, allowing a virus on.

(c) The files may have been infected before the disk was protected.
Even some diskettes "straight from the factory" have been known to be infected in the pro duction processes.

So it is worthwhile scanning even write-protected disks for viruses.

D9) Do local area networks (LANs) help to stop viruses or do they facilitate their spread?

Both. A set of computers connected in a well managed LAN, with carefully established security settings, with minimal privileges for each user, and without a transitive path of information flow between the users (i.e., the objects writable by any of the users are not readable by any of the others) is more virus-resistant than the same set of computers if they are not interconnected. The reason is that when all computers have (read-only) access to a common pool of executable programs, there is usually less need for diskette swapping and software exchange between them, and therefore less ways through which a virus could spread.

However, if the LAN is not well managed, with lax security, it could help a virus to spread like wildfire. It might even be impossible to remove the infection without shutting down the entire LAN.

A network that supports login scripting is inherently more resistant to viruses than one that does not, if this is used to validate th client before allowing access to the network.

D10) What is the proper way to make backups?

Data and text files, and programs in source form, should be backed up each time they are modified. However, the only backups you should keep of COM, EXE and other *executable* files are the *original* versions, since if you back up an executable file on your hard disk over and over, it may have become infected meanwhile, so that you may no longer have an uninfected backup of that file.
Therefore:

1. If you've downloaded shareware, copy it (preferably as a ZIP or other original archive file) onto your backup medium and do not re-back it up later.
2. If you have purchased commercial software, it's best to create a ZIP (or other) archive from the original diskettes (assuming they're not copy protected) and transfer the archive onto that medium. Again, do not re-back up.
3. If you write your own programs, back up only the latest version of the *source* programs. Depend on recompilation to reproduce the executables.
4. If an executable has been replaced by a new version, then of course you will want to keep a backup of the new version. However, if it has been modified as a result of your having changed configuration information, it seems safer *not* to back up the modified file; you can always re-configure the backup copy later if you have to.
5. Theoretically, source programs could be infected, but until such a virus is discovered, it seems preferable to treat such files as non-executables and back them up whenever you modify them. The same advice is probably appropriate for batch files as well, despite the fact that a few batch file infectors have been discovered.

Section E. Facts and Fibs about computer viruses

E1) Can boot sector viruses infect non-bootable floppy disks?

Any diskette that has been properly formatted contains an executable program in the boot sector. If the diskette is not "bootable," all that boot sector does is print a message like "Non-system disk or disk error; replace and strike any key when ready", but it's still executable and still vulnerable to