ZCZC

---

QST de PI4GAZ, PI4GAZ, PI4GAZ
Afdelingsstation van de VERON in Gouda, R17, JO22IA
Uitgezonden door PA0POS vanuit Haastrecht, JO21JX
Om 11.45 uur op 145,475 MHz met RTTY (50 baud)
Om 12.30 uur op 3,580 MHz met PSK31
Aflevering no.: 555, 20 januari 2002

---

Onderwerpen: Afdelingsnieuws, Having a field day with he Moxon rectangle, Nieuwe virussen ontdekt, Beveiliging PC (deel 10)

Afdelingsnieuws:

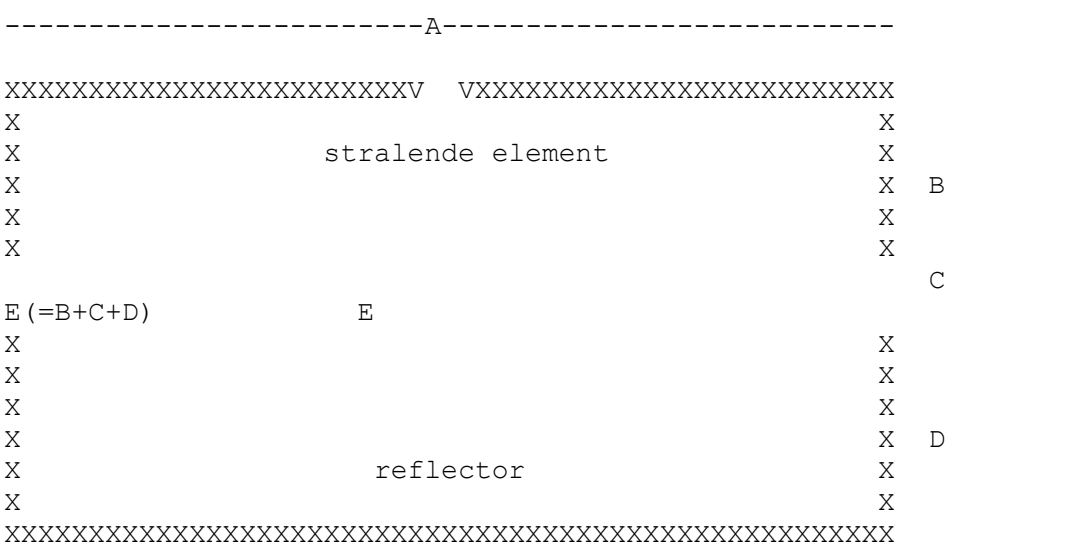
25 januari is de volgende bijeenkomst. Er staat dan een avond onderling QSO gepland. Heeft u iets bijzonders m.b.t. de hobby laat dan eens wat van u horen.

22 februari - Jaarvergadering

De afdelingsbijeenkomsten worden gehouden in de Zuivelboer derij, gelegen aan de Gouderakse Tiendweg 99 te Gouderak. U bent daar welkom om 20:00 uur.
Weet u nog mensen die geïnteresseerd zijn in onze prachtige radiohobby? U weet het: "Introducés zijn van harte welkom".

Having a field day with he Moxon rectangle:

In QST van juni 2000 staat op de blz. 38 t/m 42 een uitgebreid artikel over de Moxon rectangle antennes. Het gaat hier om draad antennes bestaande uit een stralende halve golf dipool en reflector. Beide "elementen" zijn voor een deel haaks gespannen, eventueel tussen palen opgehangen. Het voedingspunt V is 50 ohm. Het verdient aanbeveling om daar een "choke" in op te nemen of een 1:1 balun asymmetrisch naar symmetrisch. Hieronder volgt een tekeningetje voorzover dat gaat en daaronder een tabel waar de afmetingen zijn weergegeven.



A is de lengte van een deel van de dipool
B is de lengte van het haakse deel van de dipool evenzo is dat D voor het reflector deel
C is de opening tussen de einden van de dipool en de reflector
E is de totale lengte van B, C en D
Het gebruikte draad is 14 AWG hetgeen neerkomt op 1,63 mm

Afmetingen van de draad Moxon rectangle antenne van 80 - 10 meter:
In de kolommen A, B, C, D en E zijn de afmetingen in meters weergegeven

| Band | QRG in MHz | A | B | C | D | E |
|---|---|---|---|---|---|---|
| 80 | 3,6 | 30,394 | 4,703 | 0,657 | 5,573 | 11,236 |
| 75 | 3,9 | 28,053 | 4,341 | 0,608 | 5,144 | 10,093 |
| 40 | 7,09 | 15,410 | 2,377 | 0,350 | 2,842 | 5,569 |
| 20 | 14,175 | 7,691 | 1,176 | 0,188 | 1,429 | 2,794 |
| 15 | 21,225 | 5,132 | 0,778 | 0,134 | 0,955 | 1,867 |
| 10 | 28,3 | 3,846 | 0,578 | 0,106 | 0,717 | 1,401 |

voor de Engels georiënteerden onder ons de afmetingen in feet:

| Band | QRG in MHz | A | B | C | D | E |
|---|---|---|---|---|---|---|
| 80 | 3,6 | 99,98 | 15,45 | 2,16 | 18,33 | 36,96 |
| 75 | 3,9 | 92,28 | 14,28 | 2,00 | 16,92 | 33,20 |
| 40 | 7,09 | 50,69 | 7,82 | 1,15 | 9,35 | 18,32 |
| 20 | 14,175 | 25,30 | 3,876 | 0,62 | 4,70 | 9,19 |
| 15 | 21,225 | 16,88 | 2,56 | 0,44 | 3,14 | 6,14 |
| 10 | 28,3 | 12,65 | 1,90 | 0,35 | 2,36 | 4,61 |

In het artikel is voor de 10 meter 2 elements draad beam in de vrije ruimte, de volgende versterking en F/B verhouding opgegeven:
28 MHz;6,2 dB F/B 18dB, 28,2MHz;6dB F/B 30dB, 28,4MHz;5,7 dB F/B 24dB, 28,6MHz;5,5dB F/B 18dB, 28,8MHz;5,2 dB F/B 13dB, 29 MHz;5dB F/B 12dB.

Het is een uitgebreid artikel dewelke ook ingaat op meerdere constructies, de opstelling en antenne hoogte en de hoek waaronder het signaal afstraalt. Een interessant artikel om eens te lezen.

Nieuwe virussen ontdekt:

Hierbij een waarschuwing die ik (Piet PA0POS) via e-mail d.d. 18-1-2002 binnen kreeg.
Wees zo verstandig om dit even goed te lezen en door te sturen.

Er is pas een nieuw virus ontdekt, dat Microsoft en McAfee als het tot nu toe gevaarlijkste virus beschouwen. Dit virus werd pas vrijdagnamiddag door McAfee vastgesteld en wordt nog niet door virusscanners herkend. Het vernietigt de nul-sector van de harde schijf waarin belangrijke gegevens voor de functie van de harde schijf opgeslagen zijn.
Het virus werkt als volgt: het hecht zich automatisch vast aan

alle contactadressen uit het e-mail adressenboek en geeft als referentie tekst; "A Virtual Card for You" aan. Zodra deze zogenaamde virtuele postkaart geopend wordt, blijft de computer hangen zodat de gebruiker opnieuw moet starten. Wordt nu de combinatie [Ctr]+[Alt]+[Del] of de Reset-knop ingedrukt, dan wist het virus de nul-sector van de harde schijf, waardoor deze laatste definitief onbruikbaar wordt. Als U dus een bericht met de aanduiding; "A Virtual Card for You" ontvangt, open dan deze mail IN GEEN GEVAL, maar wis het bericht onmiddellijk.
Vrijdag jl. (11-1-2002), heeft dit virus binnen enkele uren een ware paniek onder de EDV gebruikers in New York veroorzaakt, zoals CNN heeft medegedeeld. Deze waarschuwing is afkomstig van een Microsoft medewerker.

Intel meldt eveneens een nieuw en zeer gevaarlijk virus, dat zich met de aanduiding; "An Internet Flower For You" verspreidt. Indien U zulk een email ontvangt, open deze niet, maar wis hem meteen. Dit virus wist alle DLL-gegevens van uw computer, zodat hij daarna niet meer kan opgestart worden.

Ook kwam heden vanuit het Medien- und Eventagentur Suttner in Duitsland het volgende bericht met het verzoek het onmiddellijk door te zenden: Er zijn opnieuw 3 nieuwe, enorm gevaarlijke virussen ontdekt. Ze komen per e-mail met de titels: "PSYCHOSPIEL, SCREENSAVER, BABY FUN of Emanuel.exe! Ze zijn blijkbaar nog gevaarlijker dan het; "I LOVE YOU" virus, daar de complete harde schijf gewist wordt. Er bestaat nog geen bescherming tegen!

DUS A.U.B. NIETS OPENEN DAT (EEN VAN) DEZE TITELS DRAAGT! Nog niet veel mensen zijn ervan op de hoogte, dus KOPIEER BOVENSTAANDE BERICHTEN EN STUUR HET ZO SNEL MOGELIJK DOOR. De virussen zijn pas 7 dagen in omloop.

Beveiliging PC:
(Deel 10, vervolg van aflevering 554, d.d. 13-01-2002)

Packet Sniffers

Voor de liefhebbers noem ik volledigheidshalve het bestaan van zogenaamde 'Packet Sniffers'. Deze programma's zijn ideaal voor het opsporen van 'malicious codes and strings' op een LAN of een back-bone van een netwerk of domweg op de internet- ingang van onze computer. De filters kunnen naar behoefte ingesteld worden. Helaas kunnen de filters ook ingesteld worden om bepaalde e-mails en/of paswoorden uit de data-brei te vissen... E-mail capturing, zoals dat fraai heet, op een LAN of back-bone is uiteraard een verwerpelijke zaak. Uiteraard zijn deze Packet Sniffers zeer geschikt om ook SPAM en Spyware en dergelijke zaken op te sporen.

De beste Packet Sniffer is momenteel naar verluidt 'The Spynet Sniffer' en is te downloaden van URL:
http://www.eye.com/html/Products/Iris/overview.html
Het slechte nieuws is dat dit een duur programma is (1745.- US dollar en een jaarlijkse 'maintenance fee' van 550.- US dollar). Het goede nieuws is dat er 30 dagen gratis mee

gestoeid kan worden.

Een andere programma, eenvoudiger maar stukken voordelige (99,- US dollar voor een single home user), is het programma Commview dat is te downloaden van URL:
http://www.tamos.com/products/commview
Ook hier is het na 30 dagen weer gedaan met de pret. Het is echter de moeite waard om eens de vele mogelijkheden van dit programma aan de tand te voelen.

Intrusion Detection Systems

Firewalls zijn tot op zekere hoogte nuttig, maar er zijn duidelijk grenzen aan de mogelijkheden omdat zo'n programma door ons geprogrammeerd wordt om een beperkt aantal zaken tegen te houden. Via de HTTP-(internet)poort 80 die door de Firewall bewaakt wordt, kunnen zaken die het programma niet kent naar binnen glippen. IDS is meer een passieve dan actieve vorm van netwerkbewaking. Data die spoort met een set van IDS-patronen wordt opgemerkt en gelogd. Een aanslag op de integriteit of de beschikbaarheid van een computer of netwerk wordt feilloos geconstateerd. Een IDS grijpt niet in, dat moet op een andere, handmatige wijze gebeuren.
Het is te vergelijken met SOSUS (Sound Surveillance System), ten tijde van de Koude Oorlog, dat als een soort Intrusion Detection System diende. Een netwerk van op de oceaanbodem bijna geheel ingegraven arrays van sensoren, de behuizing zo groot als olietanks op een raffinaderij en verbonden met elkaar via ingegraven (waarschijnlijk glasfiber kabels) om zo passief en dus onopgemerkt onderzeeboot geluiden op te vangen. En om deze vervolgens te 'fingerprinten', zeg maar het type/klasse van de onderzeeboot vast te stellen en koers en snelheid te bepalen. Op deze wijze hoopte men een mogelijke bedreiging van een onverwachte nucleaire onderzeeboot aanval te kunnen onderkennen en vervolgens het hoofd te bieden.

Terug naar 'onze' IDS. Een groot nadeel is dat het versleutelde informatie niet kan analyseren. Er zijn zowel software als hardware uitvoeringen van een IDS. Hackers proberen een IDS lam te leggen door deze te verzadigen (flooding of spoofing) of programma's te schrijven die een IDS van slag brengen. Het 'over de schouder meekijken' is een dure hobby. Een evaluatie programma 'NFR Intrusion Detection System' is te downloaden van http://www.nfr.net. Zelf gebruik ik al enige tijd 'BackOfficer Friendly' van NFR dat Freeware is. Ga naar URL:
http://www.nfr.net/products/bof/index.html BOF.exe is een ZIP-file van slechts 76kb. Het kan een aantal zaken emuleren zoals FTP en SMTP. Het kan ook onbekommerd 'praten' met hackers (Faking Replies). Ik heb het al vele maanden draaien, helaas is tot nu toe geen enkele hacker geïnteresseerd gebleken! Een ander programma is Dragon 4 en nu ook 5. Het kost echter voor ons eenvoudige amateurs een klein vermogen, bijna 5000 Euro's. Meer informatie is te vinden op URL:
http://www.anterasys.com/idsl Een evaluatie programma is ook niet zomaar te krijgen.
(wordt vervolgd)

Bron: Ferry, PA0EEU
(met hartelijke dank voor deze bijdrage, Piet PA0POS)

Tenslotte:

Kopij kan worden gestuurd naar P.C. van der Post, Spechtstraat 18, 2851 VL Haastrecht. Ook kan men via e-mail een bericht sturen naar pa0pos(at)amsat.org
PI4GAZ bulletin op Internet: www.veron.nl/afdeling/gouda

QSL-kaarten van luisteramateurs worden zeer op prijs gesteld en uiteraard beantwoord met een PI4GAZ QSL kaart.

Alle zend- en luisteramateurs een prettige zondag gewenst, en veel plezier met de hobby.

nnnn