



MINNESOTA MARSGRAM



Information for Minnesota Navy-Marine Corps. MARS Members

November, 2004

Volume 8, Number 11

NNN0ALL Minnesota

by NNN0GAZ Tim

Each and every one of us has the opportunity to participate in a process that is proudly an American obligation, electing a president to serve for the next four years. Regardless of your party affiliations I am hopeful that each and every one of you will exercise your right to vote.

As Election Day draws closer, experts will continue to

warn us that the risk of terrorist actions attempting to influence the outcome of our elections will increase. My hope is that no influences other than events of our own choosing and/or the candidates and their campaigns have influenced the outcome of our elections.

After a faulty start with our message handling exercise in October, we hope to do better this month. Elsewhere in this issue we have included a description of November's message handling drill. Hopefully we have anticipated and answered any questions that may arise. These exercises are necessary to keep us in practice handling traffic via



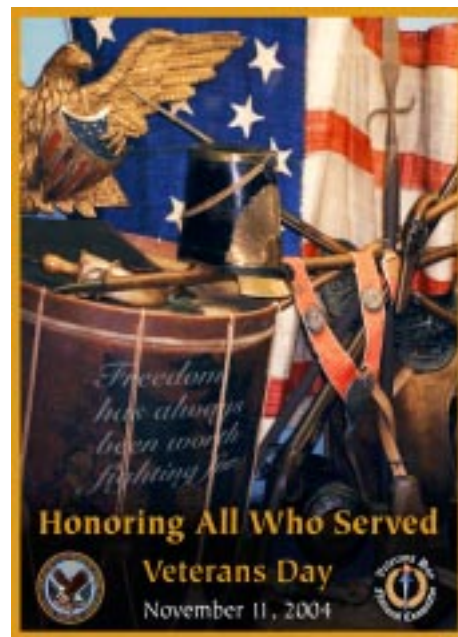
voice. Have fun with the exercise; it is meant to be a learning experience. If you have ideas for an exercise, send your idea and outline to NNN0GAZ.

Speaking of exercises, as the year draws to a close I anticipate that we will have at least one more emergency communications exercise – either on our own or in cooperation with another state in Region

Five. This is your heads up notice – please don't stay off the air, don't avoid the net, don't avoid the exercise. While I realize that this theme has repeated itself again this month, I believe that it is important and so do others. As MARS members participating in one exercise a quarter seems to be a small price to pay. Lets look at what we enjoy as members: the use of interference free frequencies, not available to other amateur services, for both our voice and digital traffic; training programs not available to

other amateurs, and the list goes on. This time lets have a good showing.

Enjoy this issue of the Minnesota MARSGRAM. *BT OVER*



The MINNESOTA MARSGRAM is published for the benefit of Amateur Radio Operators in Minnesota and other interested individuals. The contents DO NOT reflect official Navy positions.

EDITOR: Bob Reid NNN0XYA / NNN0GAZ3

Snail Mail: 13600 Princeton Circle
Savage, MN. 55378-2625

E-Mail: n0bhc@aol.com
Minnesota State Coordinator:

Tim Isom NNN0XEE / NNN0GAZ

Content Contributions Welcomed and Encouraged

MINNESOTA TRAFFIC NETS

Designator	Frequency	Local Times
5G1B	Pri. NCE Sec. NBG Ter. NAR	18:30 Daily

MINNESOTA ADMIN. NET

5G4A	Pri. NCE	19:00 2nd Sunday
------	----------	---------------------

MARS DATA SYSTEM

	Frequency
NN0DVD	NCO AFSK/USB
Intranet site	http://www.communityzero.com/mnmars

November Message Handling Exercise

Exercise Message Example

```
R 012340Z NOV 04
FM NNN0XEE
TO NNN0XYA
BT
UNCLAS
SUBJ: NOVEMBER MESSAGE HANDLING EXERCISE
1. THIS IS A MESSAGE HANDLING EXERCISE MESSAGE
2. PLEASE PASS THIS MSG TO THE NAVY-MARINE
CORPS MARS STATION OF YOUR CHOISE DURING
A 5G1B VOICE NET.
3. MY FAVORITE OPERATING MODE IS CW.
4. STATIONS YET TO HANDLE THIS MESSAGE ARE:
NNN0AAT, NNN0ACY, NNN0AFU, NNN0AMU,
NNN0APD, NNN0APLT, NNN0AQK, NNN0BJJ,
NNN0BQH, NNN0EMO, NNN0JAY, NNN0KZC,
NNN0OCF, NNN0PLH, NNN0SXU, NNN0XEE,
NNN0XYA, NNN0YWH
```

Paragraph 2

Directions for how the message can reach the next station. The message is to be passed during a voice net.

Paragraph 3

The contents of this paragraph are left to the discretion of the transmitting station. It can be the year you were licensed as a ham, the year you started in MARS, what you had for breakfast, etc. The purpose of this sentence is to add some variety so that the receiver has to listen and copy the contents of the paragraph.

Paragraph 4

As stations receive the message and transmit it to the next station, they remove their callsign from the list in paragraph 4. The last station on this list transmits two service messages – one to the one to the station from whom he received the message to let the sender know the disposition of the message, a second service message to

Notes and Instructions for the exercise

- 1) The contents of paragraph one and two are not to be changed or be corrected. If there are misspelled words or abbreviations, just as in third party or administrative messages we handle over a net the misspellings and abbreviations are left intact.
- 2) The contents of paragraph three are at the discretion of the transmitting stations. To prevent this from becoming a “copy and pass” exercise, the transmitting station can change the contents of paragraph three – example – you may choose to have paragraph three be the year you became a ham or joined MARS, it could be the date of your wedding anniversary, etc.. Having this paragraph change from station to station will mean the receiving station has to listen, copy and be prepared to ask for fills.
- 3) The list of stations in paragraph four will become shorter as the message moves through the membership. Here is how paragraph four works, since NNN0XEE transmitted the message, the callsign NNN0XEE is crossed off the list in paragraph four, meaning it would not be transmitted to the receiving station (NNN0XYA). The message does **not** have to be transmitted according to the order of the callsigns in paragraph four. Once there is only one station left in paragraph four to transmit to, the message is passed to the final station and the final station sends a service message to the transmitting station and to NNN0GAZ.
- 4) The Message Handling Exercise message must be transmitted over a voice net by voice, no other MARS recognized communication mode is allowed for the exercise message.
- 5) In addition to the exercise message, each receiving station – once it passes the exercise message to another station will send a service message to the originating station of their exercise message. Information regarding the service message portion of the drill can be found in the *Exercise Service Message Example* (see pg. 3).

This is an exercise, no one is going to get everything right and no one is going to get everything wrong. We practice so we can find out where we need to spend our training time.

November Message Handling Exercise

Exercise Service Message Example

R 102345Z OCT 04
 FM NNN0XYA
 TO NNN0XEE
 BT
 UNCLASS SVC
 ZEU R 012340Z NOV 04 FM NNN0XEE ZDF3 AT 022345Z
 NOV 04 NNN0XYA
 BT

Everything above the BT looks very familiar, a message precedence, date-time group, an originator (FM) and an addree (TO).

In a service message, following the UNCLASS is the abbreviation noting that this is a service (SVC) message.

The heart of the service message

ZEU – Exercise (drill) message, followed by the DTG of the original (or in our case the message that started this drill), the originating station (FM NNN0XEE) ZDF3 Message was delivered to addressee by broadcast at DTG the message was passed to the station NNN0XYA passed the message to and this service message is signed by NNN0XYA.

Where do I find this information...

Information necessary to format a service message can be found in NTP8C, Chapter 6 section 611.

Operating signals can be found in Annex C of NTP8C

Notes and Instructions for the service message portion of the exercise

1) In addition to the exercise message, each receiving station - once it passes the exercise message to another station will send a service message to the originating station of the exercise message they received. This service message is to use the appropriate operating signals to describe the disposition of the message.

In the sample above, NNN0XYA is sending a service message to NNN0XEE after NNN0XYA passed the message to the next station. The service message may be passed by any MARS recognized mode - voice, PSK, PACTOR (via the switch or direct), MT63, etc. Email is not an acceptable means of transmission and is not to be used for this exercise. Traffic reps need to be prepared to list the service message traffic on the 5G1B net to alert the station to traffic on the switch or relay the message during the 5G1B session.

2) There is a possibility, especially if you are the next to last to receive the message, that you may not be able to pass the traffic to the remaining station on the list. In that case, do not hesitate to format and send a service message that indicates the message is not deliverable. Perhaps the station remaining after you has not been on the air or has submitted a SITREP indicating their station equipment is down.

As stated previously, this is an exercise, no one is going to get everything right and no one is going to get everything wrong. We practice so we can find out where we need to spend our training time.

The message diagrams and examples offered here are meant to act as guides for creating your message. While they look complicated, the diagrams and this exercise are not meant to be complicated or a source of frustration.

The message handling drill will begin any time and by any staff member station after the distribution of the November MARSGRAM. Please move the message quickly through the membership. Further message handling drills can be expected in the coming months.

You Need a (Properly Configured) Firewall

by Sheryl Canter is a contributing editor to PC Magazine.
Her Web site is www.SherylCanter.com

Nearly everyone understands the need for antivirus software, but it may not be clear why a firewall is also needed. The two reinforce each other and back each other up. Firewalls use safe computing rules to protect your computer from intrusion, while antivirus software scans your file system for known malware that has slipped through the firewall, then removes it when found.

Antivirus software is easy to set up and use. The default settings won't hinder your computer's operation; you just need to update the virus definitions regularly. With firewalls, though, the settings must be customized. Improperly configured firewalls either provide inadequate protection or hamper legitimate activities.

Firewalls can be either hardware- or software-based. Many PC security packages—such as Norman Internet Control, Norton Internet Security, McAfee Internet Security Suite, and ZoneAlarm Security Suite—include both antivirus software and a firewall. A firewall's wizards are helpful but can't make every decision. A wrong choice can create a false sense of security.

This article explains how attackers try to gain access to your computer and how antivirus software and firewalls block these attacks. It also lists general principles in configuring a software firewall. (For more on firewalls, see PC Magazine August 3 issue).

Your computer is vulnerable to attack in two areas: the file system and the network stack (the set of protocols that defines network communication). Antivirus software guards the file system, scanning e-mail attachments and file downloads as well as inspecting files before loading, saving, or executing them. Scanned files are compared with a database of known virus definitions, or signatures. False positives are rare with signature monitoring.

Some antivirus programs offer heuristic scanning, which tries to identify viruses not in the database by looking for suspicious patterns. Such behavior monitoring gives more false positives and is usually turned off by default. In firewalls, it's the reverse.

Your computer can become infected whenever you're connected to the Internet—even if your e-mail program and browser are closed—through attacks against the network stack. Every computer connected to the Internet has a unique address (the IP, or Internet Protocol, address) so communication can be directed to it. With dial-up, your IP address changes each time you log in. From a security standpoint this is good, as it makes your computer a

moving target for human hackers (though some automated worms can check the whole range of IP addresses in less than 15 minutes). With broadband, your IP address is always the same, so hackers can probe your computer at leisure. Firewalls protect your computer's network ports, or endpoints of communication (as opposed to the USB and other ports used to connect devices to the computer). Common Internet services use specific ports; HTTP is usually on port 80; FTP, on port 21. An open port can give hackers a way in, so firewalls close and hide ("stealth") all unused ports. Use of other ports is governed by sets of rules. A firewall, for example, may allow outgoing FTP requests but not incoming (so you can download files from the Internet, but others can't pull files from your hard disk).

The MS-Blaster worm provides a good example of how firewalls can protect you where antivirus software can't. The worm entered computers through port 135. A Windows remote execution service (for starting programs at the request of other computers) automatically launched the worm. Usually programs launched remotely have limited access to the host system, but MS-Blaster got around this with a buffer overflow—sending more data to an input buffer (an area in memory allocated by a program for user input) than it can hold. This overwrites adjacent areas of memory, letting attackers alter settings or add instructions.

Once MS-Blaster appeared, antivirus programs updated their signature files to recognize it, but only after numerous computers had been infected. A firewall could have prevented infection by blocking access to the port.

If you had to leave port 135 open for a valid service, an Intrusion Detection System (IDS), which provides signature-based monitoring, would help. If a buffer overflow attack was seen to send 4,875 bytes to port 135, this would go into the IDS signature database, and similar attacks would be caught, even if port 135 were open. Sygate Personal Firewall Pro and Norton Personal Firewall are examples of software firewalls with an IDS. (ZoneAlarm doesn't use one.)

Firewalls are of two basic types, proxy servers and packet filters. Proxy firewalls, used by large business networks, use dedicated servers to break the connection between client and server. This applies to both incoming and outgoing traffic, so the client could be an employee or an external hacker. The server could be an external Web server or the company's internal server. Packet filters evaluate packets—the units in which data travels the Internet—to decide whether or not to forward them.

Firewall - *cont'd from pg. 4*

Personal firewalls, as well as many business firewalls, use packet filtering. The simplest packet filters use rules based only on the source and destination IP addresses, source and destination ports, and protocol. Firewalls that view this data for each packet in isolation are called static packet filters. They can control what Internet services a computer can use or provide, but as software they are vulnerable to IP spoofing. More often these filters are built into routers, where a process called Network Address Translation (NAT) hides the IP addresses of computers on a local network, exposing just the router to the Internet.

Most worms attack Windows or Windows-based applications. Since routers don't use Windows, they're fairly immune to these attacks. Even if you have just one computer, it helps to use a NAT router along with a software firewall to bolster security.

Dynamic packet filtering (or stateful packet inspection) looks at IP packets in context. This method can tell whether a given IP packet continues an existing connection or starts a new one. To prevent IP spoofing, communication not initiated by the firewall owner is blocked. The method's weakness is that outgoing traffic is always permitted, letting Trojan horses spread themselves or pilfer private data.

ZoneAlarm was the first program to monitor outgoing traffic as well as to filter communication on an application level; this is now the standard in personal firewalls. With outbound monitoring, you can allow requests from your browser while denying requests from a Trojan, even for the same port. Most personal firewalls use application information along with port, protocol, and flow data to provide multilevel stateful inspection. Norman's firewall does this especially well (www.norman.com). When an unknown program tries to access the Internet, a wizard lets you control how much access to grant it.

With the Windows XP firewall (SP1 and SP2), you can give applications permission to listen for incoming requests but not to talk, so this firewall doesn't help against Trojans. Microsoft says the XP SP2 firewall is not designed to replace third-party firewalls but to give all users a minimal level of protection from worms like MS-Blaster.

The most common decision a personal firewall asks you to make is whether to let a particular program access the Internet. You'll get such prompts most often when you first install the firewall. The question can be confusing because you may not recognize the name of your e-mail client's executable, or the Windows system components that access the Internet. It's good to start with as clean a system as possible. Update your virus definitions and perform a full system scan before you install the firewall; this should catch any Trojans on your system. Then you can safely answer Yes

to the access requests you get the first time you go online.

For access requests after that, look at the program's information. If you don't recognize it, think about what you were doing before getting the prompt. If you just installed software or selected a command that might trigger communication, the request is probably valid. If you're unsure, tell the firewall to block it but to prompt you if the program again requests access. If saying No blocks something you want to do, say Yes the next time you're prompted.

When your firewall won't let you do something, resist the temptation to punch a hole in the wall rather than trying to define a pinhole that will keep your computer safe. If you want to access your work computer from home, it's easier to give full access to the file-sharing ports or turn off your firewall than to figure out how to give file-sharing access only to your home computer's IP address. But it's worth taking the time to do the job right, or else your computer will be left open to attack.

Several Web-based vulnerability tests can tell you how well protected you are:

Shields Up (www.grc.com/x/ne.dll?bh0bkyd2)

PC Flank (<http://www.pcflank.com/about.htm>)

Sygate Tests (<http://scan.sygate.com>)

Run one of these and you'll see why you need to insert a firewall between yourself and the Internet. - BT OVER



North Arabian Gulf - (Oct. 20, 2004) - The U.S. Coast Guard cutter Monomoy (WPB 1326) patrols the waters surrounding the Al Basrah Oil Terminal (ABOT) as a super tanker takes-on crude oil. Monomoy is among several U.S. Navy, Coast Guard and coalition ships that share the responsibilities of patrolling and safeguarding the waters near the Khawr AL Amaya Oil Terminal (KAAOT) and the Al Basrah Oil Terminal (ABOT) in the Arabian Gulf. Monomoy is one of two Coast Guard cutters stationed at the Kuwait Naval Base. U.S. Navy photo by Photographer's Mate 1st Class David C. Lloyd

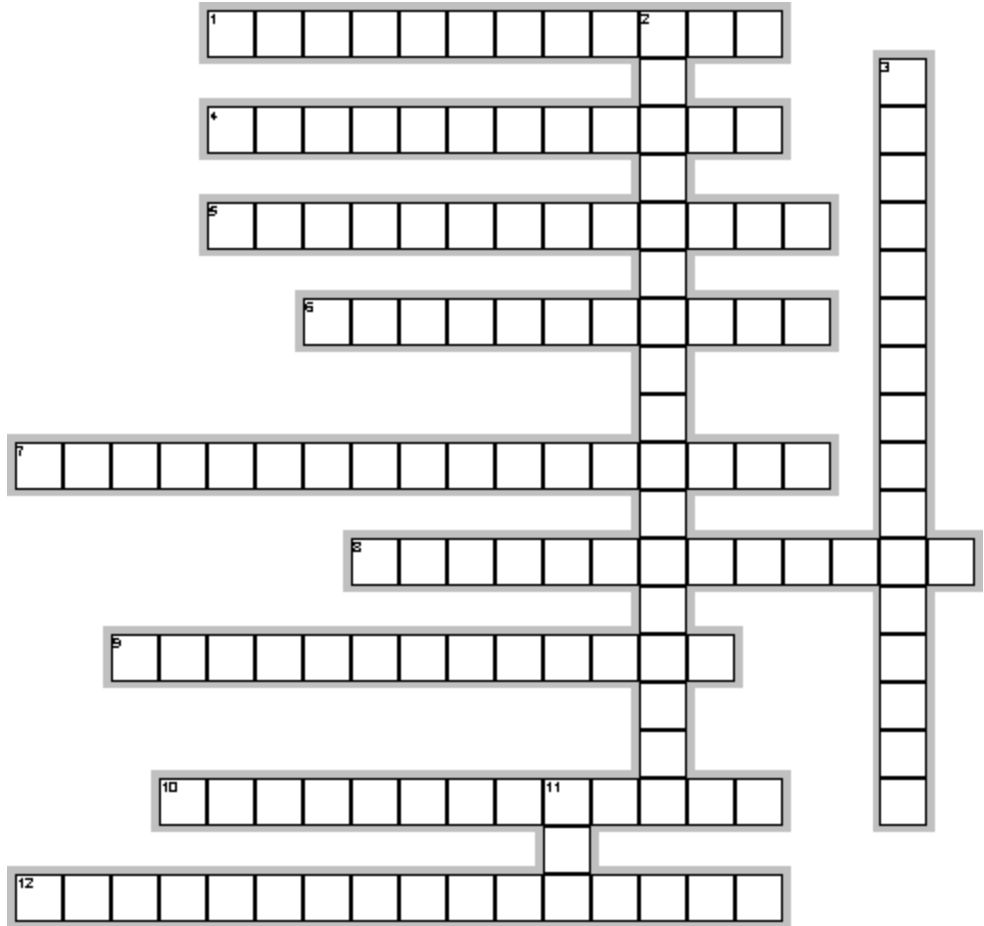
Presidential Trivia

Across

- 1. Shortest President
- 4. Youngest elected president
- 5. President who lived with a bullet in his chest most of his life
- 6. First President to be born in a hospital
- 7. This President became Chief Justice after his presidency?
- 8. Lives in the Admiral's House
- 9. Only president to date buried in Washington, D.C.?
- 10. This President could write Greek with one hand and Latin with the other
- 12. First President to have electric lights in the White House

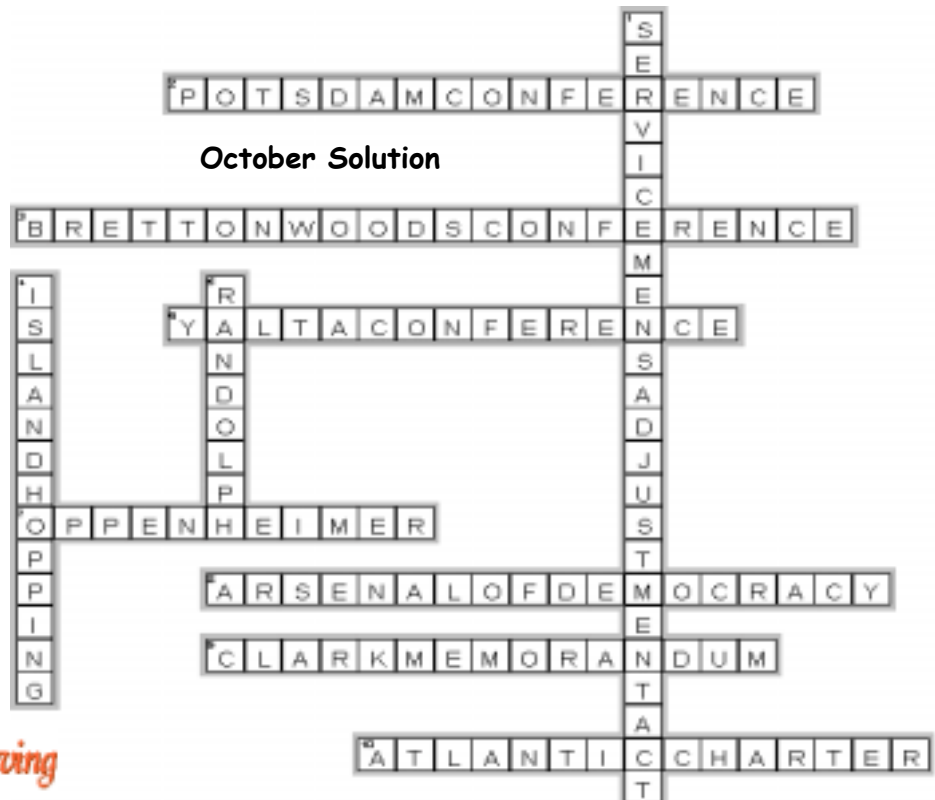
Down

- 2. Who (position) is the first in the line of succession to become president if the president and the vice-president both died?
- 3. First president to get a pilots license
- 11. First president, while in office, to fly in an airplane (initials)



Created with EclipseCrossword — www.eclipsecrossword.com

October Solution



Created with EclipseCrossword — www.eclipsecrossword.com



www.eclipsecrossword.com

Happy Thanksgiving

5G1B Net Schedule

6:30PM 4007 kHz USB

Day	NECOS	Tfc Rep
Sun.	XYA	XEE
Mon.	KZC	KZC
Tue.	XEE	XEE
Wed.	BQH	BQH
Thu.	SXU	SXU
Fri.	ACY	OCF
Sat.	Rotating Duty (see right)	

Don't be bashful, if the net has not been called by the net control station within 2 minutes, jump in and start things rolling.



NNN0AMU Fred Sauer 11/10
United States Marine Corps 11/10

Service Recognition

NNN0BQH	Bruce Meyer	18 yrs
NNN0OCI	Roger Wise	14 yrs
NNN0JAY	Cal Fuhrman	8 yrs
NNN0OCE	Joel Jensen	8 yrs

Don't forget your paperwork!

Saturday NECOS / TREP Schedule

	NECOS	TREP
Nov 6	XEE	XEE
Nov 13	BQH	BQH
Nov 20	SXU	SXU
Nov 27	ACY	OCF
Dec 4	XYA	XEE
Dec 11	KZC	KZC



Happy Birthday USMC

“Marines, as we celebrate with friends and families the founding of our beloved corps, you should take pride in our

long history of distinguished service to this great nation and its citizens. I ask you to remember especially the sacrifices of our fallen and wounded comrades. Finally, rededicate yourselves to taking care of one another and ensuring we remain the finest warfighting organization in the world.

Happy birthday marines, semper fidelis, and keep attacking!”

M.W.Hagee, General, U.S. Marine Corps,
 Commandant of the Marine Corps.



San Francisco Bay, Calif. (Oct. 9, 2004) - From right, the guided missile destroyers USS John Paul Jones (DDG 53) and USS Momsen (DDG 92), and the guided missile frigate USS Jarrett (FFG 33) sail into San Francisco Bay, Calif., at the start of Fleet Week 2004. San Francisco Fleet Week is a unique opportunity to share with the American public what today's sea services are all about. More than 2,000 Sailors, Marines and Coast Guardsmen visit San Francisco during the annual four-day event. U.S. Navy photo by Photographer's Mate 1st Class Marvin Harris

Test Your Analytical Skills

Can you solve this problem?

John D., Los Angeles, CA.

Courtesy of the Pantagraph, Parade Magazine.

Divide a sheet of paper into eight parts. Number them on one side as in the diagram. The problem is to fold the paper (along the lines) to form a packet (like a folded map) with No. 1 face-up on top, followed by the other numbers in order.

7	4	3	2
6	5	8	1

October Test Solution

Nine dots are placed in three rows of each three dots, as shown in the picture. These nine dots must be connected by four straight, connected lines (i.e. without 'lifting up the pen' in between).

