NIOC MARYLAND ADVANCED COMPUTER NETWORK OPERATIONS COURSE

Coordinated by
Title

- Content
WHY ARE WE TEACHING THIS?

- **5 Pillars of IO:**
  - OPSEC
  - MILDEC
  - MISO
  - EW
  - CNO

- **The next major conflict will start in cyberspace**
  - Whether we recognize the signs is another matter
  - Recent conflicts have already shown the importance of CNO (Russia/Georgia)
  - Think China will make a move on Taiwan without bringing down their communications networks?

- **As IW officers (or IDC) – we are expected to know and understand CNO and communicate with decision makers**

- **Recently announced plans from Command in Chief and Pentagon officials emphasize cyber space operations**

- **Basic 1810/IDC quals are a good foundation, but CO/XO want you to know more about CNO**
**Course Overview**

**Wednesday, April 11th**  
Location: OPS2B  
2B4118-1

<table>
<thead>
<tr>
<th>Time</th>
<th>Topic</th>
<th>Briefer</th>
</tr>
</thead>
<tbody>
<tr>
<td>0730-0900</td>
<td>CNO Intro/ TAO Overview</td>
<td>LT [redacted] / CTN1 [redacted]</td>
</tr>
<tr>
<td>0900-1000</td>
<td>Analysis</td>
<td>CTN1 [redacted] / CTN2 [redacted]</td>
</tr>
<tr>
<td>1000-1100</td>
<td>EAO</td>
<td></td>
</tr>
<tr>
<td>1100-1200</td>
<td>Lunch</td>
<td></td>
</tr>
<tr>
<td>1200-1300</td>
<td>IOD/Scanning</td>
<td>CTN1 [redacted] / CTN1 [redacted]</td>
</tr>
<tr>
<td>1300-1400</td>
<td>DNT</td>
<td>ENS [redacted]</td>
</tr>
<tr>
<td>1430-1500</td>
<td>TAO Brief/Tour</td>
<td>ENS [redacted]</td>
</tr>
</tbody>
</table>
## Course Overview

**Thursday, April 12th**

**Location:** OPS2B 2B4118-3

<table>
<thead>
<tr>
<th>Time</th>
<th>Topic</th>
<th>Briefer</th>
</tr>
</thead>
<tbody>
<tr>
<td>0800-0900</td>
<td>CND Intro/Threat Brief</td>
<td>LTJG Brown / LTJG Brown (S: U:</td>
</tr>
<tr>
<td>0900-1000</td>
<td>Red Team Brief</td>
<td>CTN2 Brown/ CTN2 Brown (S: U:</td>
</tr>
<tr>
<td>1000-1030</td>
<td>Blue Team Brief</td>
<td>LCDR Brown / LCDR Brown (S: U:</td>
</tr>
<tr>
<td>1030-1100</td>
<td>JCMA Brief</td>
<td>CTR1 Brown / CTR1 Brown (S: U:</td>
</tr>
<tr>
<td>1100-1130</td>
<td>Hunt Brief</td>
<td>CTN2 Brown / CTN2 Brown (S: U:</td>
</tr>
<tr>
<td>1130-1300</td>
<td>Lunch</td>
<td>CTN2 Brown / CTN2 Brown (S: U:</td>
</tr>
<tr>
<td>1400-1530</td>
<td>NIOC Brief/ Walkthrough</td>
<td>TED Center of Excellence</td>
</tr>
</tbody>
</table>

POC: LCDR Brown
**Course Overview**

**Friday, April 13th**  
**Location:** OPS2B  
**2B4118-3**

<table>
<thead>
<tr>
<th>Time</th>
<th>Topic</th>
<th>Briefer</th>
</tr>
</thead>
<tbody>
<tr>
<td>0800-0900</td>
<td>POD</td>
<td>CTN2I MAJ</td>
</tr>
<tr>
<td>0900-1000</td>
<td>OCO</td>
<td>LTJG LT MAJ</td>
</tr>
<tr>
<td>1000-1100</td>
<td>Legal Authorities</td>
<td>LT</td>
</tr>
<tr>
<td>1100-1200</td>
<td>Lunch</td>
<td></td>
</tr>
<tr>
<td>1200-1400</td>
<td>PKC/PKI (Asymmetric Encryption)</td>
<td>LT</td>
</tr>
<tr>
<td>1400-1430</td>
<td>Debrief/Discussion</td>
<td>LT</td>
</tr>
</tbody>
</table>
Class I
- Automated

Class II
- Interactive
  - Proximal Access
  - Physical Interdiction
  - Multi-Staged

Human-enabled

Who: TAO
Where: ROC

Who: CYBERCOM
Where: ROC

Defensive Cyber Operations (DCO)
- NTOC: TUTELAGE (mil)
- NCDOC: HAWKEYE (navy mil)
- DHS: EINSTEIN (gov)
- Response-Action Timely & Proportional

Offensive Cyber Operations (OCO)
- Conducted by US Military Personnel or DoD Civilians with UCMD Waivers
- Information Assurance (IA)

DoD Global Information GIG Operations (DGIO)
- Proactive Network Operations (PNO)
DoD Global Information Grid Operations (DGO)

DGO operations consist of aspects of NetOps directing operation of the GIG.

Goal: support efforts to build, configure, secure, operate, maintain and sustain DoD networks.

Desired end-state: enable pillars of Information Assurance.

Achieved via Proactive Network Operations (PNO).

DISA operates the GIG, but USCYBERCOM ensures operation and availability.

Pillars of Information Assurance:
- Confidentiality
- Integrity
- Availability
- Non-Repudiation
- Authentication

Responsible Organizations:
- USCYBERCOM
- NSANet: IAD & NTOC
- JWICS: DIA
- navy.mil
- Navy Cyber Defense Operations Command (CTF 1020)
- NAVNETWARCOM (CTF 1010)

FLTCYBERCOM / C10F
U.S. FLEET CYBER COMMAND / U.S. TENTH FLEET
Defensive Cyberspace Operations (DCO)

- Direct and synchronize actions to detect, analyze, counter and mitigate cyber threats and vulnerabilities
- Protect critical missions, enable freedom of action in cyberspace
- Flexible response, incorporating Title 10 and Title 50 authorities, to defend the GIG

Responsible Organizations:
- USCYBERCOM: .mil
- NCDOC: navy.mil
- DHS: .gov

NTOC uses SIGINT
- Hawkeye
- Einstein

FLT CYBERCOM / C10F

---

U.S. FLEET CYBER COMMAND / U.S. TENTH FLEET

---
Offensive Cyberspace Operations (OCO)

- Enabling and attack effects in cyberspace
- Support national and CCDRs’ objectives via cyber actions
- Remote Operations Center, civilians and military personnel
- Enables active defense against cyber actors/adversaries

ROC Relationships:

Remote Operations Center

USCYBERCOM tasks

NSA/CSS controls

Navy’s Role: Force Provider
Computer Network Operations
• **TAO Overview**
  – Mission Aligned Cells (MAC)

• **Manning / Placement**

• **Department Operations**
  – Summary
  – Examples: Russia & Lebanon
  – Joint Cyber Attack Team
  – NCAT Vision
  – Afloat CNO

• **Discussion Topics**
Mission-Aligned Cells (MACs)

Concept:

- TAO recently completed a major effort to align resources from R&T, ROC, DNT and MIT into mission focused teams.
- **Mission Aligned Cells**
  - Teams composed of operators, analysts and developers working together to focus on a specific target set.
- Allows TAO to efficiently resources on high-priority projects and targets.

Current MAC’s:

- China/North Korea (NSAW, NSAH)
- Iran (NSAW, NSAG)
- Russia (NSAW, NSAH)
- Cyber Counterintelligence (CCI) (NSAW, NSAG, NSAT, NSAH)
- Counterterrorism (CT) (NSAW, NSAG)
- Target Service Provider (TSP) (NSAW, NSAT)
- Regional Targets (RT) (NSAW, NSAT)
Leadership Positions:

RDML
- Deputy Chief, TAO

CAPT
- TAO Cyber Operations Integrated Lead (COIL)
- Principle advisor to TAO leadership for operational cyber issues

S32:
Staff (2/2/0)
Leadership Positions:

**LC DR**
- D/Chief, CT & Afghanistan

**LC DR**
- In training – slated for Hard Targets Division, DPRK Branch

**LT**
- CNO Coordinator – China/DPRK Branch

S327:

R&T Influence (8/6/0)

Endpoint Exploitation (57/35/0)

[Billet Description *(BA/COB/Deployed)*]
**Remote Operations Center (S321)**

*Leadership Positions:*

**CAPT**
- Deputy Chief, ROC

**LCDR**
- D-Chief, STO
- Chief, Iran MAC (IMAC)

**CTNCS**
- ROC SER

**LCDR**
- Chief, Cyber Operations Branch

**LTJG**
- Tech Lead, Cyber Operations Branch

---

**S321:**
- ROC Influence (9/9/0)
- Lead (3/3/0)
- Interactive Operator (49/26/0)
- Production Operator (25/14/0)

[Billet Description (BA/COB/Deployed)]
**Leadership Positions:**

**LT**
- Chief, Cyber Technologies Branch

**LT**
- Chief, Engineering Services Division

**S323:**
- Development (Officer) (2/2/0)
- Development (Enlisted) (16/6/0)

[Billet Description (BA/COB/Deployed)]
Leadership Positions:

LT
- Chief, Operations Branch

LT
- D-Chief, EAO

S328:
ATO (Officer) (4/4/0)
ATO (Enlisted) (23/15/1)

[Billet Description (BA/COB/Deployed)]
S325 - Mission Infrastructure Technologies:

Infrastructure (Enlisted) (7/1/0)

S352 - Global Access Operations:

Global Access (Officer) (0/1/0)
Global Access (Enlisted) (1/1/1)

10 Dept Summary:

Officers**

- 28 BA / 26 COB = 93%

Enlisted

- 182 BA / 101 COB = 55%

**2/9 CS P-coded officer billets filled; need M.S. Computer Science personnel
**Weekly Interactive CNE operations**

<table>
<thead>
<tr>
<th></th>
<th>Operators</th>
<th>Ops Conducted</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ALL</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>All</td>
<td>208</td>
<td>2588</td>
</tr>
<tr>
<td>CIV</td>
<td>70</td>
<td>1059</td>
</tr>
<tr>
<td>NAVY</td>
<td>52</td>
<td>674</td>
</tr>
<tr>
<td>AF</td>
<td>44</td>
<td>343</td>
</tr>
<tr>
<td>ARMY</td>
<td>29</td>
<td>376</td>
</tr>
<tr>
<td>USMC</td>
<td>11</td>
<td>108</td>
</tr>
<tr>
<td>USCG</td>
<td>2</td>
<td>28</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Operators</th>
<th>Ops Conducted</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NAVY</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAVY</td>
<td>52</td>
<td>674</td>
</tr>
<tr>
<td>NIOC-M</td>
<td>28</td>
<td>292</td>
</tr>
<tr>
<td>NIOC-T</td>
<td>10</td>
<td>133</td>
</tr>
<tr>
<td>NIOC-G</td>
<td>8</td>
<td>107</td>
</tr>
<tr>
<td>NIOC-H</td>
<td>6</td>
<td>142</td>
</tr>
</tbody>
</table>

**Target Sets - R&T Analysts**

- China
- Russia
- Iran
- Afghanistan
- Pakistan
- India
- Iraq
- Counterterrorism
- Cyber
- Counterintelligence (CCI)

**Supporting Roles**

- ROC Senior Watch Officers
- Development
**Target Example:**

**Team**

- **MAC:** Mission Aligned Cell – puts analysts and operators together to increase target familiarity and efficiency of operations
- Joint military and civilian entity
• **Current TAO Targets**
  
  - **Political**
    - [Masked] leadership to include Ministry of Interior, Parliament Members, and Presidential Palace
  
  - **Military**
    - Former Commander of [Masked] Common Border Force
    - Col. [Masked] IT Directorate
    - Gen. [Masked] Medical Command
    - Gen. [Masked] (affiliation unknown)
    - Col. [Masked] Instructor, Army Staff and Command College

• **Recent Reporting**

  - [Masked] Armed Forces Reviewed
    Personnel Issues Regarding Retirement, Communications, and Health Care
FLEET FOCUS

Framework and support for Navy requirements

Provides structure to develop holistic Navy capability

CTE Manning

Unix and Windows Operators:
- Exploiter Qualified (Minimum Requirement)
Router and Firewall Operators:
- May shift between CTE’s depending on operator specialty and mission requirement

CTE Support five (5) Combined Task Elements

CTU CDR
- CDE [0-6]

D/COR
- [04-5]

Chief of Operations
- [0-3]

Technical Director [Civilian]

CTE Mission Commander
- 2 Windows Operators
- 2 Basic Operators
- 2 Unit Operators
- 1 Infrastructure Operator
- 14 R&T Analyst

JOINT FOCUS

Navy support to joint priorities

Structure supports Manning requirements levied on Navy

Mission Alignment

NCAT
Service-led JCAT
JCAT Support
Service CNE Support

SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
JCAT Concept of Operations:

- Assembled for Title 10 execution support
- Mission Commanders and Operators provide full-time support to CNE operations outside of JCAT

Requirements:

- CAUI Support
  - 1 Mission Commander
  - 2 CNA Operators

- TASKORD 11-0335
  - 3 Mission Commanders
  - 10 CNA Operators

Current Navy Participation:

- Mission Commanders:
  - LTJG [REDACTED]
  - Qualification based on JQS administered by the Cyber Operations Branch
  - Five (5) additional officers in training

- Operators:
  - Working to certify all qualified Interactive Operators for JCAT
  - Requires LOAC/ROE Briefing and Tool Training
AUTEC testing with USS Annapolis. 18 NOV 2011

**Interactive Operations**
- Connection via: NEPTUNETHUNDER, BLINDDATE/HAPPYHOUR
- Successful exploits at 4, 6, and 8 NM with 4 watt Access Point (AP).
- Predict max connection distance to standard 100 mw AP to be 4 NM.

**Man On the Side Operations**
- Inject using: BLINDDATE/NİTESTAND
- Successful inject at 4 NM to 100 mw client computer.
Network Operations - Overview

Overall classification of this brief is:
Networking Fundamentals

• Describe the following network component/terms:

  – Proxy Server:
    • An intermediary computer that completes application network requests on behalf of a host.

  – Router
    • A layer 3 device used to route traffic between networks

  – File Server
    • A server dedicated to the hosting and sharing of files.

  – Perimeter Network
    • The network segment located between LAN and Internet, used to place Internet facing services like Web and Mail Servers.

  – Internet
    • The aggregate of publicly connected networks implementing the IP addresses
Networking Fundamentals

- **Describe the following network component/terms:**
  - **Intranet**
    - A private network not normally accessible through the internet.
  - **Firewall**
    - A mechanism to filter network traffic using rules based on attributes like source, destination, packet type, port, and session status.
  - **IDS (Intrusion Detection System):**
    - Network traffic analyzer that uses patterns to detect malicious activity.
  - **TACACS (Terminal Access Controller Access Control System).**
    - Provides authentication, authorization, and accounting control to network devices via central server.
  - **RADIUS (Remote Authentication Dial In User Service)**
    - Authentication protocol for remote users to access network resources via network access methods like Dial-in, VPN, DSL, and WAP.
Networking Fundamentals

- Define the following cross domain solutions:
  
  - High Assurance Guards
    - Connects networks operating within different security domains. Filters traffic like a firewall but operates on all levels of the TCP/IP stack.
  
  - SABI (Secret and Below Interoperability)
  
  - TSABI (Top Secret and Below Interoperability)
    - Connection of Top Secret Security Domain to domains of lesser classification levels.
  
  - Bastion Host
    - A host on an internal network that is also publicly exposed to the Internet or another public network. Usually used for service hosting (web, email, etc) or as part of a firewall solution.
Networking Fundamentals

- Describe the location of the following components in a simple networked environment:
  a. Proxy Server
  b. Router
  c. Firewall
  d. Workstation
  e. DMZ
  f. Switch
Wireless Networking

- Define wireless networking to include the following aspects:
  - Wireless Access Point
    - Wired to Wireless bridging.
  - 802.11 Protocols
    - The set of layer 1 & 2 protocols defining the RF, physical layer and media access control.
      - **STANDARD** | **Frequency Range** | **Modulation Method** | **Bit Rate**
      - 802.11a       | 5.0 GHz          | OFDM                | 54 Mbps
      - 802.11b       | 2.4 GHz          | DSSS                | 11 Mbps
      - 802.11g       | 2.4 GHz          | OFDM                | 54 Mbps
      - 802.11n       | 2.4 or 5 GHz     | SDM                 | 600 Mbps
    - Other wireless technologies in the 2.4 GHz range include Bluetooth (802.15), cordless phones, microwaves, baby monitors, etc...
  - MAC Filtering
    - Only defined hardware addresses can connect to network
Networking Fundamentals

- Define the following application protocols/services and identify their port numbers:
  
  - Telnet: TCP 23
  - NTP (Network Time Protocol): TCP/UDP 123
  - NetBEUI (NetBIOS Extended User Interface): Non routable transport protocol used in pre-WinXP LAN’s.
  - Net BIOS (Network Basic Input/Output System): TCP/UDP 139
  - FTP (File Transfer Protocol): TCP 21
  - POP3 (Post Office Protocol 3): TCP 110
  - RPC (Remote Procedure Call):
    - SUN/UNIX: TCP 111, 32771
    - WIN: TCP/UDP 135
  - HTTP (Hypertext Transfer Protocol): TCP 80
Define the following application protocols/services and identify their port numbers (continued...):

- **SMTP (Simple Mail Transfer Protocol):** TCP 25
- **DNS (Domain Name System):** TCP/UDP 53
- **SNMP (Simple Network Management Protocol):** UDP 161
- **SSL (Secure Socket Layer):** Presentation Layer protocol for use by applications to secure communications
- **SSH (Secure Shell):** TCP 22
- **TFTP (Trivial FTP):** UDP 69
- **HTTPS (HTTP Secure):** TCP 443
- **FTPS (Secure FTP):**
- **DHCP (Dynamic Host Configuration Protocol):** UDP 67
Network Layer Protocols

- Define the following network layer protocols to include their relationship to TCP/IP:
  - **IP**
    - Layer 3 (Network) used for network addressing and routing
  - **TCP**
    - Layer 4 (Transport) used for application session and reliable delivery
  - **UDP**
    - Layer 4 (Transport) used for application communication.
  - **ARP**
    - Layer 2 (Link) used for Mapping IP addresses to MAC Addresses
  - **RARP**
    - Layer 2 (Link) used for Mapping MAC addresses to IP Addresses
  - **ICMP**
    - Layer 3 (Network) used for Network Diagnostics
List and describe the 7 layers of the OSI Model:
List and describe the 4 layers of the TCP/IP Model to include how they relate to the OSI Model:

- The TCP/IP model combines the Session and Presentation layers with the Application layer. It is assumed if a program has need of layer 5 or 6 functionality, then the program will have to provide it.
TCP 3-Way Handshake

- Define and illustrate the TCP 3-Way Handshake

The 3-Way handshake is the method that all TCP sessions use to initialize connections and session parameters. It follows the sequence SYN, SYN-ACK, ACK. Application data can begin sending with the final ACK packet.
TCP Flags

Define and briefly describe the use of the following TCP flags:

- **SYN**: Used to initialize the TCP by setting the packet sequence number.
- **ACK**: Used to acknowledge receipt of all package sequences up to the number indicated.
- **PSH**: Indicates that all data already received should be given to the application as soon as possible. Flushes the buffer.
- **URG**: Urgent Data. Commonly used for interrupts.
- **FIN**: Indicates there is no more data to send from that end of the connection. Session closes after both ends acknowledge FINs.
- **RST**: Immediate termination of connection. Commonly used to indicate unavailable service.
Define and describe the structure of the following protocol headers:

- **IP**

```
<table>
<thead>
<tr>
<th>Field</th>
<th>Bit Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>0-3</td>
<td>4-bit version</td>
</tr>
<tr>
<td>Header Length</td>
<td>4-11</td>
<td>8-bit total length (in bytes)</td>
</tr>
<tr>
<td>Type of Service</td>
<td>12-15</td>
<td>8-bit type of service (TOS)</td>
</tr>
<tr>
<td>Identification</td>
<td>16-31</td>
<td>16-bit identification</td>
</tr>
<tr>
<td>Flags</td>
<td>16-23</td>
<td>3-bit flags</td>
</tr>
<tr>
<td>Fragment Offset</td>
<td>24-31</td>
<td>13-bit fragment offset</td>
</tr>
<tr>
<td>TTL</td>
<td>32-39</td>
<td>8-bit time to live (TTL)</td>
</tr>
<tr>
<td>Protocol</td>
<td>40-47</td>
<td>8-bit protocol</td>
</tr>
<tr>
<td>Header Checksum</td>
<td>48-55</td>
<td>16-bit header checksum</td>
</tr>
<tr>
<td>Source IP</td>
<td>56-71</td>
<td>32-bit source IP address</td>
</tr>
<tr>
<td>Destination IP</td>
<td>72-87</td>
<td>32-bit destination IP address</td>
</tr>
<tr>
<td>Options</td>
<td>88-103</td>
<td>options (if any)</td>
</tr>
<tr>
<td>Data</td>
<td>104-208</td>
<td>data</td>
</tr>
</tbody>
</table>
```

(20 bytes)
Protocol Headers

- Define and describe the structure of the following protocol headers:

  - TCP

```
    0                             15 16                             31
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>16-bit source port number</td>
<td>16-bit destination port number</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>32-bit sequence number</td>
<td>32-bit acknowledgment number</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>4-bit header length</td>
<td>reserved</td>
</tr>
<tr>
<td>U R C G</td>
<td>A F S T</td>
</tr>
<tr>
<td>S S Y F</td>
<td>16-bit window size</td>
</tr>
<tr>
<td>16-bit TCP checksum</td>
<td>16-bit urgent pointer</td>
</tr>
<tr>
<td>options (if any)</td>
<td>data (if any)</td>
</tr>
</tbody>
</table>
```

20 bytes
Protocol Headers

- Define and describe the structure of the following protocol headers:
  - UDP

![UDP Protocol Header Diagram]
MAC Addressing

- Discuss the following as it pertains to MAC Addressing:
  - LENGTH OF MAC ADDRESS IN BITS: 48
  - DISPLAY OF MAC ADDRESS: Hexadecimal Format 00:8e:f0:59:31:ae
  - LOCATION OF MAC ADDRESS: First 48 bits in message
  - MANUFACTURER SPECIFIC BITS: First 3 Octets
  - HOST SPECIFIC BITS: Last 3 Octets

![MAC Address Diagram]
ARP

• Discuss the following as it pertains to ARP:
  
  – ADDRESS RESOLUTION:

  • ARP (Address Resolution Protocol) facilitates the mapping between hardware addresses (MAC Address) and logical network addresses (IP Addresses). This mapping can be stored in a file or can determined through ARP broadcast requests on a local network.
ICMP

Discuss the following as it pertains to ICMP:

- ICMP is a protocol that defines a collection of message types commonly used for network diagnostics.

  - Layer of the OSI model: ICMP (usually) consists of Layer 3 (Network) messages transported by IP.
  - Ping: Message Type 8 (request) and 0 (reply). Used to determine if a device is active on the network.
  - Traceroute: Uses a combination of the IP time-to-live (TTL) field and the ICMP messages 11 (time exceeded) and 3.3 (port unreachable) to determine the route a packet takes through the network.
Discuss the routing table as it pertains to the router:

- The Routing Table Stores what networks are reachable through each interface along with metadata about that route.
IP Addressing

- Discuss the following as it pertains to ranges of IP addressing:
  
  - Classful networks were the original method of distributing address groups to organizations.
  
  - Class A: First 8 bits for Network ID and the last 24 bits for Host ID.
    - 126 Networks : 16,277,214 Hosts/net
  
  - Class B: First 16 bits for Network ID and the last 16 bits for Host ID.
    - 16,384 Networks : 65,534 Hosts/net
  
  - Class C: First 24 bits for Network ID and the last 8 bits for the Host ID.
    - 2,097,152 Networks : 254 Hosts/net
TCP/IP

- Discuss the following as it pertains to TCP/IP:
  - Number of bits in an IP address: 32
  - Number of octets contained in an IP address: 4

- IPv6 has 128 bits, roughly a 300 trillion 300 trillion more
  - 90,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000 times the space of IPv4
Networking Fundamentals

• Discuss the following as it pertains to the following protocols:
  
  – TCP
  – UDP
IP Subnets

Discuss the following as it pertains to IP Subnets:

- Number of bits used in a subnet mask.
- How the subnet mask identifies the network portion of the IP address.
- Borrowing bits from the host portion of the address.
- Benefits of subnetting.
• Discuss the following as it pertains to TELNET:
  – Use: Create a Network Virtual Terminal session on a remote system.
  – Type of connection: TELNET uses TCP as the transport protocol.
  – Default port number: 23
References


6. Intelipedia Articles.

7. NSA Wiki Articles.
Questions

- Questions?