ELECTRONIC SECURITY NETWORKING TECHNICIAN - ESNT

COMPETENCY REQUIREMENTS

The following is a listing of each topic considered necessary to be included in a course of study directed towards the education of technicians needed to properly cable, connect, install, program and troubleshoot Internet Protocol (IP)-enabled security devices onto local area networks (LAN), wide area networks (WAN) and the Internet. Prior basic security information is important and prior Information Technology (IT) knowledge will be essential to comprehending the following competencies.

While the **ESNT** can be considered a Stand-Alone Certification, the technicians seeking the **ESNT Certified Electronics Technician (C.E.T.)** specialty are required to also have a basic education in fundamental electronics. That basic knowledge is assessed in the **Associate CET (CETa)** examination. The **CETa** exam, plus the **ESNT** specialty examination together will form a complete journeyman **CET** certification. For a more complete Cyber Security certification it is recommended that a technician also complete the **ITS** cyber certification found https://www.etai.org/information_technology.html.

There are nine (9) general categories of knowledge. This COMPETENCY listing is the syllabus, or identification of each individual subject, in which the technician must be knowledgeable and skilled. The **ESNT** certification examination is based upon these competencies and assumes a working fundamental knowledge of network and security terminologies.

1.0 GENERAL NETWORKING

- 1.1 Describe the meaning of “Network”
  - 1.1.1 Describe the basic types of network configurations - LAN and WAN
    - 1.1.1.1 Explain design concepts of measuring and building availability into networks
  - 1.1.2 Summarize knowledge of common network terms
- 1.2 Summarize knowledge of IEEE 802.3 Ethernet communication standards
  - 1.2.1 Identify standards for new interfaces with media access control data rates of 40 Gb/s and 100 Gb/s
- 1.3 Summarize knowledge of IEEE 802.11x Wi-Fi™ functions, programming, standards, ranges
- 1.4 Describe the details of Wi-Fi™ installation and connection
- 1.5 Describe the coverage patterns of omnidirectional and Yagi radio antennas
- 1.6 Identify the layers of the OSI (Open Systems Interconnect) and TCP/IP (Transmission Control Protocol/Internet Protocol) stacks including:
  - 1.6.1 common network components
  - 1.6.2 common protocols at each layer
  - 1.6.3 the functions at each layer
- 1.7 Explain broadcast domain
- 1.8 Differentiate between TCP and UDP (User Datagram Protocol) transmissions knowledge

2.0 NETWORK ADDRESSING

- 2.1 Summarize knowledge of MAC (Media Access Control) addresses - function and purpose
  - 2.1.1 Understand Organizational Unique Identifier MAC section
  - 2.1.2 Understand the basics of hexadecimal coding
- 2.2 Explain common IP addressing on LANs
  - 2.2.1 Understand dotted decimal notation
- 2.3 Identify IPV4 and IPV6 addresses
- 2.4 Explain the purposes and uses of TCP/IP software ports
- 2.5 Summarize knowledge of subnet mask addresses and their uses distinguishing between:
  - 2.5.1 Broadcast address
  - 2.5.2 Network address
  - 2.5.3 Host address
- 2.6 Explain the uses of static and dynamic IP addresses on LANs
- 2.7 Summarize knowledge of IP address classes and private IP address ranges
- 2.8 Explain the use of broadcast IP addresses

2.9 Explain placement and use of source and destination addresses in the TCP/IP protocol stack Layers 2, 3 and 4
2.10 Explain the concept of data encapsulation
2.11 Explain how ARP (Address Resolution Protocol) works to reconcile Layer 2 and Layer 3 addressing
2.12 Describe the function of VLANs (virtual networks) and contrast with subnets

3.0 NETWORK CABLING

3.1 Summarize knowledge of TIA 568- cabling standards as they apply to common IP-enabled physical security devices
3.2 Identify the common components of a standardized structured cabling system
3.3 Summarize knowledge of the Ethernet cabling distances and bandwidth (if different) for:
- 3.3.1 Cat5e cable
- 3.3.2 Cat6 cable
- 3.3.3 $Cat6_A$ cable
- 3.3.4 multimode fiber
- 3.3.5 single-mode fiber

3.4 Explain the functional differences between multimode and single-mode fiber
3.5 Summarize knowledge of fiber optic technician safety issues
3.6 Summarize knowledge of proper 568-A and 568-B UTP (unshielded twisted pair) connector terminations
3.7 Summarize knowledge of the maximum pull strength (tensile) ratings for common UTP and fiber optic cables
3.8 Explain common problems associated with UTP and fiber cabling installation including:
- 3.8.1 proper correction resolutions

3.9 Summarize knowledge of the pairs required for Ethernet communications over UTP
3.10 Differentiate the types of terminations used for Ethernet UTP cabling and pin connections
3.11 Summarize knowledge of the use of alternative cabling media for network transmissions
3.12 Describe the knowledge of proper testing of coaxial copper cables for Ethernet and Power over Ethernet transmission
3.13 PoE (Power Over Ethernet):
- 3.13.1 Summarize knowledge of the 802.3 PoE standards - (IEEE 802.3bt, especially)
- 3.13.2 Differentiate between copper UTP cable and copper clad aluminum (cca) UTP cable
- 3.13.3 Differentiate between Power Sourcing Equipment (PSE) and Powered Device (PD), and why there is dissimilarity in the power levels specified for these
- 3.13.4 Explain why a PoE “Midspan” is economical
  - 3.13.4.1 Explain why power over fiber (PoF) is not economical, yet

4.0 NETWORK DEVICES

4.1 Explain the basic functions of network devices knowledge:
- 4.1.1 routers
- 4.1.2 switches
- 4.1.3 end devices

4.2 Describe common “Redundant Array of Independent Disks” (RAID) configurations
4.3 Explain the concepts of data backup and fault tolerance

5.0 INTERNET CONNECTIONS

5.1 Explain the concept of "broadband" Internet connections
5.2 Summarize knowledge of common broadband Internet connections in terms of their potential use for physical security video transmissions:
- 5.2.1 satellite
- 5.2.2 fiber
- 5.2.3 cable modem
- 5.2.4 digital subscriber line (DSL)

5.3 Differentiate between symmetric and asymmetric bandwidth capabilities
5.4 Describe the function of an Internet Service Provider (ISP)
5.5 Summarize knowledge of public and private IP addresses
5.6 Explain the uses of static and dynamic public IP addresses

5.7 Describe the functions of NAT (Network Address Translation) as relates to the communications of IP-enabled security devices over the Internet
5.8 Explain the programming necessary to allow communications of devices through common Internet firewalls
5.9 Describe the function of DNS (Domain Name Servers)
5.10 Summarize common Internet browser software knowledge relating to physical security devices
5.11 Explain the uses of Java™ and ActiveX software programs as related to IP video communications
5.12 Identify the common software ports used for Internet communications
5.13 Identify the entity which assigns public IP addresses

6.0 NETWORK SERVICES

6.1 Explain the function of ARP in the network
6.2 Explain the use of a DDNS (Dynamic Domain Name System) service
6.3 Summarize knowledge of SNMP (Simple Network Management Protocol) for device monitoring on a network
6.4 Describe the use of NTP (Network Time Protocol) servers as relates to IP-enabled security devices
6.5 Summarize the common uses and deployment of DHCP (Dynamic Host Configuration Protocol) services
6.6 Explain the uses of the FTP (File Transfer Protocol)
6.7 Identify secure versus non-secure data transmission protocols

7.0 IP-ENABLED PHYSICAL SECURITY DEVICES

7.1 Explain the basic IP programming necessary to connect a physical security device to a LAN
7.2 Summarize knowledge of the "commonly used" TCP/IP ports
7.3 Identify components used in video security installations:
- 7.3.1 Explain video camera terms
  - 7.3.1.1 PTZ (Pan, Tilt, Zoom)
  - 7.3.1.2 Panoramic
  - 7.3.1.3 Multi-sensor
- 7.3.2 Differentiate between a DVR (Digital Video Recorder) and an NVR (Network Video Recorder)
  - 7.3.2.1 Identify the advantages of IP cameras
  - 7.3.2.2 Identify advantages of PoE use
- 7.3.3 Explain the use of VMS (Video Management Software)
  - 7.3.3.1 Explain how video analytics software works
  - 7.3.3.2 Explain the purpose of the ONVIF (Open Network Video Interface Forum)
- 7.3.4 Summarize knowledge of proper pixel calculations based on a field of view, to determine the proper MP (megapixel) resolution needed:
  - 7.3.4.1 High Definition (HD) video formats
- 7.3.5 Explain the common options for increasing or decreasing the bandwidth requirements for security video transmissions over networks:
  - 7.3.5.1 Uplink bit rate
  - 7.3.5.2 Downlink bit rate
- 7.3.6 Summarize knowledge of high-quality video compression formats including:
  - 7.3.6.1 MJPEG
  - 7.3.6.2 H.264 {MPEG-4 Part 10, AVC (Advanced Video Coding)}
  - 7.3.6.3 H.265 {High Efficiency Video Coding}

7.4 Explain the differences between TCP and UDP transmission of video images
7.5 Describe the PoE power requirements for security devices
7.6 Summarize knowledge of default IP addresses in devices and vendor device discovery software
7.7 Explain cloud services for security networks knowledge
7.8 Summarize the concept of IoT (Internet of Things) knowledge
7.9 Compare knowledge of the wireless communications options for IoT devices, including Wi-Fi™, Z-Wave®, Zigbee, Low-Rate WPAN (IEEE 802.15.4), Bluetooth® (802.15.1) short range wireless and Universal Powerline Bus (UPB) technologies

8.0 CYBER SECURITY FOR ELECTRONIC SECURITY DEVICES

- 8.1 Summarize Cyber Security threats
  - 8.1.1 Describe the most common cyber threats to a physical security deployment
  - 8.1.2 Describe the potential threats posed by IoT device deployment
  - 8.1.3 Explain “insider threat”
- 8.2 Summarize Device Security
  - 8.2.1 Explain how to do secure firmware update procedures and their importance
  - 8.2.2 Explain how to do provisioning of device access levels
- 8.3 Summarize Network Security
  - 8.3.1 Explain the importance of VLAN’s in network security
  - 8.3.2 Describe how to apply "strong" passwords and password security provisions
  - 8.3.3 Explain the common uses and types of network firewalls
- 8.4 Summarize “Wi-Fi™ Security”
  - 8.4.1 Identify commonly used wireless services in security
  - 8.4.2 Describe common threats to Wi-Fi™ services
  - 8.4.3 Explain how to apply methods used to secure wireless communications
- 8.5 Summarize IT Infrastructure Security
  - 8.5.1 Identify physical security approaches to safeguard IT infrastructure
- 8.6 Operations
  - 8.6.1 Explain the importance of maintaining a complete inventory of IP physical devices
  - 8.6.2 Describe vulnerability and penetration testing
  - 8.6.3 Explain the use of network scanning software tools

9.0 COMMON NETWORK TESTING AND TROUBLESHOOTING

- 9.1 Summarize knowledge of common LED (light emitting diode) functions on network devices
- 9.2 Explain the uses of common network testing tools including:
  - 9.2.1 cabling testers
  - 9.2.2 OTDRs (optical time-domain reflectometer)
  - 9.2.3 OLTS (optical loss test/meter sets)
  - 9.2.4 tone generators
- 9.3 Summarize knowledge of the uses of Windows™ "command line" options:
  - 9.3.1 ping
  - 9.3.2 ARP
  - 9.3.3 tracert
  - 9.3.4 nslookup
- 9.4 Explain common power problems (surges, sags, outages) and their potential effects on network components
- 9.5 Summarize knowledge of available Internet tools for testing communications
- 9.6 Explain how to find a network's public IP address and the identity of the associated ISP
- 9.7 Explain how to apply the methods by which to test network communications for:
  - 9.7.1 packet loss
  - 9.7.2 latency
  - 9.7.3 bandwidth
- 9.8 Summarize knowledge of the logical sequences used to solve common network problems

End of Electronic Security Networking Competencies Listing
(with 9 knowledge categories)

Find An ETA Test Site: http://www.eta-i.org/test_sites.html

Suggested Additional ESNT Resource and Study Materials Reference List:

While the ESNT is a knowledge-based certification, there are additional courses and self-study material available. The certification examination is based upon the competencies.

Guide to Networking for Physical Security Systems; David Engebretson, ISBN# 978-1418073961; Delmar Cengage Learning; 2007; pp304.

Technician's Guide to Physical Security Networking: Enterprise Solutions; David Engebretson, ISBN# 978-1434399915; AuthorHouse; 2008; pp264.

EZ Guide to Installation and Programming of IP Cameras; David Engebretson. Order from ADI Distribution: 800-233-6261, part #3X-IPHOW2MAN. Illustrated instruction manual; 2016, pp55.

Technician's Guide to Termination, Testing and Usage of Alternative Cables for Ethernet and IP Adapter Applications; David Engebretson. Order from ADI distribution: 800-233-6261, part #3X-TECHGUIDE. Illustrated instruction manual; 2016, pp61.

ESNT Training Guide to Electronic Security Networking Technician certification; David Engebretson, part# 3X-ESNTDISC1; SlaytonSolutions,LTD; 2017; USB Media Video Flash Drive card. $80.00 http://www.fiberopticsinstitute.com/fiberopticsIPNet.html . {also available through ETA at 800-288-3824 or wwww.eta-i.org}

Computer Networking, A Top-Down Approach, 7E; James F. Kurose, Keith W. Ross; ISBN 978-0133594140; 2016; pp864

Cabling: The Complete Guide to Copper and Fiber-Optic Networking, 5E; Oliviero & Woodward; ISBN 978-1118807323; Sybex, Inc.; 2014; softcover; 1284 ppg**.** Available through ETA 800-288-3824, www.etai.org

Review Slayton Solutions Limited: www.fiberopticsinstitute.com and www.securityspecifiers.azurewebsites.net and www.adiglobal.us websites

ESNT Subject Matter Expert Advisory Board:

Rich Agard, RESIma	(SEPTA); PA	ragard@septa.org
Ray Coulombe, ITS, ESNT	(Security Specifiers); RI	ray@securityspecifiers.com
Paul Brinkmann, ESNT	(Somerset County Vo-Tech) NJ	pbrinkmann@scvts.net
Eric Elsenbroek,	(ADI Systems); KY	Eric_Elsenbroek@Adi-dist.com
Dave Engebretson, ESNT	(Slayton Solutions); IL	slaytonsolutions@sbcglobal.net
Michael Goshen, CST, ITS, NST	(Huntsville P.D.) AL	goshen@michaelgoshen.com
J.B. Groves, FOT, ESNT, etal	(Wharton Co. J.C.) TX	jbgroves@wcjc.edu
Paul Gulczynski,	(E. Norman Security); IL	pgulczy@comcast.net
Joseph Hayes,	(All County Security); NY	hayescpp@optonline.net
Steve MacMahon,	(Stanley Security) IN	Steve.MacMahon@sbdinc.com
Jim McLaughlin,	(American Fibertek); NJ	jmclaughlin@americanfibertek.com

ETA certification programs are accredited through ICAC, complying with the ISO/IEC 17024 standard.

