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 IP-enabled security devices onto local area networks and the Internet.

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.

While the ESNT can be considered a Stand-Alone Certification, the technicians seeking the ESNT Certified Electronics Technician specialty are required to also have a basic education in fundamental electronics. That basic knowledge is assessed in the Associate CET examination. The Associate CET exam, plus the ESNT specialty examination together will form a complete journeyman CET certification.

1.0 GENERAL NETWORKING

- 1.1 Describe the meaning of “network”
  - 1.1.1 Describe the basic types of network configurations - LAN and WAN
  - 1.1.2 Demonstrate knowledge of common network terms
- 1.2 Demonstrate knowledge of IEEE 802.3 Ethernet standards
- 1.3 Identify common Ethernet data transmission bandwidths
- 1.4 Identify the layers of the OSI and TCP/IP stacks including:
  - 1.4.1 common network components
  - 1.4.2 common protocols at each layer
  - 1.4.3 the functions at each layer
- 1.5 Describe techniques to avoid data collision in Ethernet networks
- 1.6 Explain broadcast and collision domains
- 1.7 Describe the function of VLANs (virtual networks) and contrast with subnets
- 1.8 Demonstrate knowledge of the differences between TCP and UDP transmissions

2.0 NETWORK ADDRESSING

- 2.1 Demonstrate knowledge of MAC addresses - function and purpose
- 2.2 Explain common IP addressing on LANs
- 2.3 Identify IPV4 and IPV6 addresses
- 2.4 Explain the purposes and uses of TCP/IP software ports
- 2.5 Demonstrate 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 Demonstrate 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 Demonstrate knowledge of end-to-end transmission in a multi-hop network

3.0 NETWORK CABLING

- 3.1 Demonstrate 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 Demonstrate knowledge of the Ethernet cabling distances and bandwidth (if different) for:
  - 3.3.1 Cat5 cable
  - 3.3.2 Cat5e cable

- 3.3.3 Cat6 cable
- 3.3.4 $Cat6_A$ cable
- 3.3.5 multimode fiber
- 3.3.6 single-mode fiber

3.4 Explain the functional differences between multimode and single-mode fiber
3.5 Demonstrate knowledge of fiber optic technician safety issues
3.6 Demonstrate knowledge of proper 568-A and 568-B UTP connector terminations
3.7 Demonstrate knowledge of the maximum pull strength (tension) 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 Demonstrate knowledge of the pairs required for Ethernet communications over UTP
3.10 Demonstrate knowledge of the different types of terminations used for Ethernet UTP cabling and pin connections
3.11 Demonstrate knowledge of the use of alternative cabling media for network transmissions
3.12 Demonstrate knowledge of the proper testing of coaxial copper cables for Ethernet and Power over Ethernet transmission.

4.0 NETWORK DEVICES

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

4.2 Demonstrate knowledge of-network topology hierarchies
4.3 Explain the concepts of measuring and building availability into networks
- 4.3.1 Discuss network design and common network protocols that are used to provide high availability

4.4 Demonstrate knowledge of IEEE 802.11x Wi-Fi functions, programming, standards, ranges
4.5 Describe the details of Wi-Fi installation and connection
4.6 Explain the basic details of the installation of Wi-Fi based mesh networks
4.7 Describe the coverage patterns of omnidirectional and Yagi radio antennas
4.8 Describe common RAID configurations
4.9 Explain the concepts of data backup and fault tolerance

5.0 INTERNET CONNECTIONS

5.1 Explain the concept of "broadband" Internet connections
5.2 Demonstrate 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 DSL
- 5.2.5 T1

5.3 Explain the difference between symmetric and asymmetric bandwidth capabilities
5.4 Describe the function of an Internet Service Provider
5.5 Demonstrate 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 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 Domain Name Servers
5.10 Demonstrate knowledge of common Internet browser software as relates to physical security devices
5.11 Explain the uses of Java and Active X 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
5.14 Explain the use of the "WHOIS" Internet search

6.0 NETWORK SERVICES

- 6.1 Explain the function of ARP (Address Resolution Protocol)
- 6.2 Explain the use of a DDNS (Dynamic Domain Name System) service
- 6.3 Demonstrate 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 Demonstrate knowledge of 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 Demonstrate knowledge of the basic IP programming necessary to connect a physical security device to a LAN
- 7.2 Demonstrate knowledge of the "commonly used" TCP/IP ports
- 7.3 Explain the difference between Unicast, Broadcast and Multicast messaging
  - 7.3.1 Provide examples where each type of communication is / should frequently be used with security devices
- 7.4 Explain the concept of multicasting of video and audio signals through a network
- 7.5 Demonstrate knowledge of compression video compression formats including:
  - 7.5.1 M-JPEG
  - 7.5.2 H-264
- 7.6 Explain the differences between TCP and UDP transmission of video images
- 7.7 Demonstrate knowledge of the IEEE standards for PoE (Power over Ethernet) and High PoE
- 7.8 Demonstrate knowledge of default IP addresses in devices and vendor device discovery software
- 7.9 Explain the common options for increasing or decreasing the bandwidth requirements for security video transmissions over networks
- 7.10 Demonstrate knowledge of megapixel IP cameras, their uses and bandwidth requirements
- 7.11 Demonstrate knowledge of panoramic cameras and the role of dewarping software
- 7.12 Demonstrate knowledge of the capabilities and limitations of “cloud” recording and Video Management System usage over LANs, WANs and the Internet
- 7.13 Demonstrate knowledge of the HD video format in terms of resolution, frames per second, and aspect ratio
- 7.14 Demonstrate knowledge of proper pixel calculations based on a field of view, to determine the proper MP resolution needed

8.0 NETWORK SECURITY

- 8.1 Explain the common uses and types of network firewalls
- 8.2 Demonstrate knowledge of IEEE 802.1x protocol
- 8.3 Demonstrate knowledge of "strong" passwords
- 8.4 Explain the uses of network device auditing
- 8.5 Demonstrate knowledge of methods used to secure Wi-Fi communications
- 8.6 Identify the common types of hacker attacks on networks and devices
- 8.7 Demonstrate knowledge of the means and effects of a malware infection
- 8.8 Demonstrate knowledge of common problems with Operating System software including:
  - 8.8.1 OS software patching needs
- 8.9 Explain the concept of "phishing" and “spear phishing” email attacks
- 8.10 Describe the problems associated with Ethernet packet manipulation
- 8.11 Explain the use of network scanning software tools
- 8.12 Demonstrate knowledge of the "deny all" security concept
- 8.13 Explain what ACLs are and what network devices frequently use them
- 8.14 Explain the uses of Network Intrusion Detection systems

9.0 COMMON NETWORK TESTING AND TROUBLESHOOTING

- 9.1 Demonstrate knowledge of common LED 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 Demonstrate 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 Demonstrate 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 Demonstrate knowledge of the methods by which to test network communications for:
- 9.7.1 packet loss
- 9.7.2 latency
- 9.7.3 bandwidth

9.8 Demonstrate 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

ESNT Additional 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}

Review **fiberopticsinstitute.com** and **securityspecifiers.azurewebsites.net** and **adiglobal.us** websites;

ESNT Subject Matter Advisory Board:

Agard, CET, FOI, PVI; Rich	(SEPTA); PA	regard@aol.com
Coulombe, ESNT, CDT; Ray	(Gilwell Technology Services); RI	ray@gilwelltechnology.com
Elsenbroek, Eric	(ADI Systems); KY	Eric_Elsenbroek@Adi-dist.com
Engebretson, ESNT; Dave	(Slayton Solutions); IL	slaytonsolutions@sbcglobal.net
Groves, FOT, ESNT, etal; J.B.	(Wharton Co. J.C., FT. Bend Tech. Ctr.); TX	jbgroves@wcjc.edu
Gulczynski, Paul	(E. Norman Security); IL	pgulczy@comcast.net
Hayes, Joseph	(All County Security); NY	hayescpp@optonline.net
McLaughlin, Jim	(American Fibertek); NJ	jmclaughlin@americanfibertek.com

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

