



Electronics Technicians Association, International
COMPETENCY REQUIREMENTS
ELECTRONIC SECURITY NETWORKING TECHNICIAN - ESNT

2008

The following is a listing of each topic considered necessary to be included in a course of study directed towards the education of workers 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 training. This COMPETENCY listing is the syllabus, or identification of each individual subject, in which the technician must be knowledgeable and skilled.

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 go together to form the complete journeyman CET exam.

ESNT COMPETENCIES

1.0 General Networking

- 1.1 Describe the basic types of modern network configurations - LAN and WAN
- 1.2 Demonstrate knowledge of IEEE Ethernet standards
- 1.3 Identify common Ethernet data transmission bandwidths
- 1.4 Demonstrate knowledge of common network terms
- 1.5 Identify the layers of the OSI protocol stack as related to NICs, hubs, switches and routers
- 1.6 Describe Ethernet and Wi-Fi data collision functions
- 1.7 Describe the function of VLANs
- 1.8 Explain broadcast and collision domains
- 1.9 Demonstrate knowledge of the functions of the TCP and UDP protocols

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
- 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

3.0 Network Cabling

- 3.1 Demonstrate knowledge of EIA/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 Category 5, 5E, 6 cables and multimode and single fiber.
- 3.4 Explain the functional differences between multimode and singlemode 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 ratings for common UTP and fiber optic cables
- 3.8 Explain common problems associated with UTP and fiber cabling installation, and proper corrections

- 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.

4.0 Network Devices

- 4.1 Describe common RAID configurations
- 4.2 Explain the concepts of data backup and fault tolerance as they pertain to servers.
- 4.3 Demonstrate knowledge of the basic functions and programming of network routers, switches, and hubs
- 4.4 Demonstrate knowledge of the 2- and 3-tier network topology hierarchies and discuss the merits of each, including where each is generally appropriate.
- 4.5 Explain the concepts of measuring and building availability into networks. Discuss network design and common network protocols that are used to provide high availability.
- 4.6 Demonstrate knowledge of 802.11x Wi-Fi functions, programming, standards, ranges
- 4.7 Describe the details of Wi-Fi installation and connection
- 4.8 Explain the basic details of the installation of Wi-Fi based mesh networks
- 4.9 Describe the coverage patterns of omnidirectional and Yagi radio antennas

5.0 Internet Connections

- 5.1 Explain the concept of "broadband" Internet connections
- 5.2 Demonstrate knowledge of common broadband Internet connections (satellite, cable modem, DSL, T-1) in terms of their potential use for physical security video transmissions
- 5.3 Describe the function of an Internet Service Provider
- 5.4 Demonstrate knowledge of public and private IP addresses
- 5.5 Explain the uses of static and dynamic public IP addresses
- 5.6 Describe the functions of Network Address Translation as relates to the communications of IP-enabled security devices over the Internet
- 5.7 Explain the programming necessary to allow communications of devices through common Internet firewalls
- 5.8 Describe the function of Domain Name Servers
- 5.9 Demonstrate knowledge of common Internet browser software as relates to physical security devices
- 5.10 Explain the uses of Java and Active X software programs as related to IP video communications
- 5.11 Identify the common software ports used for Internet communications
- 5.12 Identify the entity which assigns public IP addresses
- 5.13 Explain the use of the "WHOIS" Internet search

6.0 Network Services

- 6.1 Explain the use of a DDNS service
- 6.2 Demonstrate knowledge of SNMP for device monitoring on a network
- 6.3 Describe the use of NTP servers as relates to IP-enabled security devices
- 6.4 Demonstrate knowledge of the common uses and deployment of DHCP services
- 6.5 Explain the uses of the File Transfer Protocol

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. 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 MPEG, JPEG and H-264 video compression formats
- 7.6 Explain the differences between UDP and TCP transmission of video images
- 7.7 Demonstrate knowledge of the IEEE standards for Power over Ethernet
- 7.8 Demonstrate knowledge of default IP addresses in devices, and "MAC search" vendor 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

8.0 Network Security

- 8.1 Explain the common uses and types of network firewalls
- 8.2 Demonstrate knowledge of "strong" passwords
- 8.3 Explain the uses of network device auditing
- 8.4 Demonstrate knowledge of methods used to secure Wi-Fi communications
- 8.5 Identify the common types of hacker attacks on networks and devices
- 8.6 Demonstrate knowledge of common problems with Operating System software
- 8.7 Explain the concept of "phishing" email attacks
- 8.8 Describe the problems associated with Ethernet packet manipulation
- 8.9 Explain the use of network scanning software tools
- 8.10 Demonstrate knowledge of the "deny all" security concept
- 8.11 Explain what are ACLs and what network devices frequently use them.
- 8.12 Explain the need for Operating System software patching
- 8.13 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 - cabling testers, OTDRs, optical loss meter sets, tone generators
- 9.3 Demonstrate knowledge of the uses of Windows "command line" options: Ping, arp, tracert, 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 packet loss, latency, and bandwidth
- 9.8 Demonstrate knowledge of the logical sequences used to solve common network problems

ESNT Study Textbooks Reference List

ESNT ETA approved text:

Guide to Networking for Physical Security Systems, David Engebretson, Thomson Delmar.

Below are books that can be used by candidates as supplemental student materials for study for the ETA's ESNT examination.

1. *Exam Prep 2 Network +, Second Edition*, Bird et al. Que Publications.
2. *CCNA: Cisco Certified Network Associate, Deluxe Edition*, Todd Lammle. Sybex Publications.