pennsylvania
DEPARTMENT OF EDUCATION

High School Graduation Years 2013, 2014 and 2015

Computer System Networking and Telecommunications
CIP 11.0901
Task Grid

Unit/Standard Number	Secondary Competency Task List
100	**DEMONSTRATE KNOWLEDGE OF PERSONAL AND ENVIRONMENTAL SAFETY**
101	List common causes of accidents and injuries in a computer facility .
102	Wear personal protective equipment.
103	List and identify safety hazard symbols.
104	Review Material Safety Data Sheets (MSDS) and explain their requirements in handling hazardous materials.
105	Describe types of fire extinguishers and explain which types to use for extinguishing various fires.
106	Demonstrate safe procedures to follow when lifting and carrying heavy objects.
107	Describe the importance of safety as it relates to environmental issues.
108	Identify potential hazards when working with power supplies.
109	Identify proper disposal procedures for batteries and display devices.
110	Identify proper disposal procedures for chemical solvents and pressurized cans.
111	Identify and prevent Electro Static Discharge conditions.
112	Describe the meaning and importance of the Energy Star Rating System.
113	Configure a computer's power management settings to maximize energy efficiency.
114	Maintaining a safe work area to avoid common accidents and injuries.
200	**DEMONSTRATE KNOWLEDGE OF COMPUTER HARDWARE**
201	Categorize storage devices and backup media.
202	Categorize the different types of computer cases.
203	Explain motherboard components, types and features.
204	Categorize power supplies types and characteristics.
205	Explain the purpose and characteristics of CPUs and their features.
206	Explain cooling methods and devices.
207	Compare and contrast memory types, characteristics and their purpose.
208	Distinguish between the different display devices and their characteristics.
209	Summarize the function and types of adapter cards.
210	Install and configure peripherals and input devices.
211	Install, configure and optimize laptop components and features.
212	Install and configure printers.

Unit/Standard Number	pennsylvania DEPARTMENT OF EDUCATION — High School Graduation Years 2013, 2014 and 2015 **Computer System Networking and Telecommunications** **CIP 11.0901** **Task Grid**
213	Given a scenario, install, configure and maintain personal computer components.
214	Given a scenario, detect problems, troubleshoot, and repair/replace desk top and laptop computer components.
215	Given a scenario, diagnose and repair common printer issues.
300	**DEMONSTRATE KNOWLEDGE OF TROUBLESHOOTING, REPAIR AND MAINTENANCE**
301	Describe and explain the troubleshooting theory.
302	Describe and explain and interpret common hardware and operating system symptoms and their causes.
303	Describe and determine the troubleshooting methods and tools for printers.
304	Describe and interpret common laptop issues and determine the appropriate basic troubleshooting method.
305	Given a scenario, integrate common preventative maintenance techniques.
306	Compare and contrast network troubleshooting with hardware/software troubleshooting.
400	**DEMONSTRATE KNOWLEDGE OF OPERATING SYSTEMS AND SOFTWARE**
401	Compare and contrast the different Operating Systems and their features.
402	Given a scenario, demonstrate proper use of user interfaces.
403	Explain the process and steps to install and configure an operating system.
404	Explain the basics of boot sequences, methods and startup utilities.
405	Select the appropriate commands and options to troubleshoot and resolve problems.
406	Differentiate between various operating system directory structures.
407	Identify and use system utilities/tools and evaluate the results.
408	Evaluate and resolve common OS and software issues.
409	Explain the administration of local users, groups and institute local security policy.
410	Compare and contrast a network operating system (NOS) with a workstation operating system (OS)
500	**DEMONSTRATE KNOWLEDGE OF NETWORK TECHNOLOGIES**
501	Explain the function of common networking protocols, such as FTP, TCP/IP suite, DHCP, DNS, etc.
502	Identify commonly used TCP and UDP default ports, including TCP ports: FTP – 20, 21, SSH – 22, TELNET – 23, HTTP – 80, etc.
503	Identify the following address formats, including IPv6, IPv4, MAC addressing.
504	Given a scenario, evaluate the proper use of addressing technologies and addressing schemes, including: Subnetting: Classful vs. classless, NAT, PAT, SNAT, Public vs. private, DHCP, Addressing schemes: Unicast, Multicast, Broadcast., etc.
505	Identify common IPv4 and IPv6 routing protocols, including Link state, Distance Vector, and Hybrid protocols.

Unit/Standard Number	pennsylvania DEPARTMENT OF EDUCATION — High School Graduation Years 2013, 2014 and 2015 **Computer System Networking and Telecommunications** **CIP 11.0901** **Task Grid**
506	Explain the purpose and properties of routing, including IGP vs. EGP, Static vs. dynamic, Next hop, interpret routing tables and how they pertain to path selection, Explain convergence (steady state).
507	Compare the characteristics of wireless communication standards, including 802.11 standards: Speeds, Distance, Channels, Frequency, Authentication and encryption.
600	**DEMONSTRATE KNOWLEDGE OF NETWORK MEDIA AND TOPOLOGIES**
601	Categorize standard cable types and their properties including: UTP, STP, Coaxial, Fiber; Plenum vs. Non-plenum Properties: Transmission speeds, Distance, Duplex, Noise immunity, Frequency.
602	Identify common connector types, including UTP, STP, Coaxial, and Fiber
603	Identify common physical network topologies.
604	Given a scenario, differentiate and implement appropriate wiring standards, including 568A, 568B, and Loopback.
605	Categorize common WAN technology types and properties.
606	Categorize common LAN technology types and Ethernet properties: CSMA/CD, Broadcast, Collision, Bonding, Speed, Distance.
607	Explain common logical network topologies and their characteristics, including Peer to peer and Client/server.
608	Install components of wiring distribution, including Vertical and horizontal cross connects, Verify installation and termination.
700	**DEMONSTRATE KNOWLEDGE OF NETWORK DEVICES**
701	Install, configure and differentiate between common network connectivity devices.
702	Identify the functions of specialized network devices such as, Multilayer switch, Content switch, IDS/IPS, Load balancer, Multifunction network devices, DNS server, Bandwidth shaper, Proxy server, CSU/DSU.
703	Explain the advanced features of a switch such as, PoE, Spanning tree, VLAN, Trunking, Port mirroring, Port authentication, etc.
704	Implement a basic wireless network, including Client configuration, Access point placement and Installation.
705	Configure appropriate encryption, Configure channels and frequencies, Set ESSID and beacon, verify installation.
800	**DEMONSTRATE KNOWLEDGE OF NETWORK MANAGEMENT**
801	Explain, compare and contrast the layers of the TCP/IP and OSI models.
802	Identify types of configuration management documentation such as, Wiring schematics, Physical and logical network diagrams, Baselines, Policies, procedures and configurations, Regulations.
803	Given a scenario, evaluate the network based on configuration management documentation such as, Compare wiring schematics, physical and logical network diagrams, baselines, policies and procedures and configurations to network devices and infrastructure, Update wiring schematics, physical and logical network diagrams, configurations and job logs as needed.
804	Conduct network monitoring to identify performance and connectivity issues such as, packet sniffers, connectivity software, load testing, throughput testers, System logs, history logs, event logs.
805	Explain different methods and rationales for network performance optimization.
900	**DEMONSTRATE KNOWLEDGE OF NETWORK TOOLS AND TROUBLESHOOTING**

Unit/Standard Number	pennsylvania DEPARTMENT OF EDUCATION — High School Graduation Years 2013, 2014 and 2015 **Computer System Networking and Telecommunications** **CIP 11.0901** **Task Grid**
901	Given a scenario, select the appropriate command line / graphical tools and interpret the output to verify functionality such as, Traceroute, Ipconfig, Ifconfig, Ping, Arp ping, Arp, Nslookup, Hostname, Dig, Mtr, Route, Nbtstat, Netstat.
902	Explain the purpose of network scanners such as, Packet sniffers, Intrusion detection software, Intrusion prevention software, Port scanners.
903	Given a scenario, select the appropriate hardware tools such as, Cable testers, Protocol analyzer, Certifiers, TDR, OTDR, Multimeter, Toner probe, Butt set, Punch down tool, Cable stripper, Snips, Voltage event recorder, Temperature monitor.
904	Given a scenario, implement network troubleshooting methodologies, including Information gathering – identify symptoms and problems, Identify the affected areas of the network.
905	Describe and create an action plan and solution identifying potential effects, Implement and test the solution, Identify the results and effects of the solution, Document the solution and the entire process.
906	Given a scenario, troubleshoot common wired and wireless connectivity issues and select an appropriate solution to include Physical and Logical issues.
1000	**SECURITY FUNDAMENTALS**
1001	Explain, compare, and contrast the function of hardware and software security devices such as, Network based firewall, Host based firewall, DMZ, IDS, IPS, VPN concentrator.
1002	Explain common features of a firewall such as, Application layer vs. network layer, Stateful vs. stateless, Scanning services, Content filtering, Signature identification, Zones.
1003	Explain the methods of network access security such as, ACL: MAC filtering, IP filtering Tunneling and encryption: SSL VPN, VPN, L2TP, PPTP and related others.
1004	Explain methods of user authentication such as, PKI, Kerberos, AAA: RADIUS, TACACS+, Network access control: 802.1x, CHAP, MS-CHAP, EAP.
1005	Explain issues that affect device security such as, Physical security, Restricting local and remote access, Secure methods vs. unsecure methods: SSH, HTTPS, SNMPv3, SFTP, SCP; TELNET, HTTP, FTP, RSH, RCP, SNMPv1/2.
1006	Identify common security threats and mitigation techniques.
1007	Identify security features including BIOS Security, Password management, Locking workstations, and Biometrics.