

Summary of ITN Modules 1 & 2

Module 1: Networking Today This module introduces the role of networks in our daily lives, their components, and the different types of networks. Key points include: - Networks connect people, organizations, and devices globally. - Core components: end devices, intermediary devices (switches, routers, firewalls), and transmission media. - Network representations use physical and logical topologies. - Types of networks: LAN, WAN, Internet, intranets, extranets. - Internet connection methods: DSL, cable, fiber, wireless, and business-class services. - Converged networks combine data, voice, and video. - Reliable network characteristics: fault tolerance, scalability, QoS, and security. - Trends: BYOD, collaboration, video communication, cloud computing, smart homes, wireless broadband. - Network security threats (external and internal) and solutions (antivirus, firewalls, VPNs, ACLs, IPS). - IT professionals benefit from CCNA certification for networking careers.

Module 2: Basic Switch and End Device Configuration This module covers basic switch configuration, IOS navigation, and IP addressing. Key points include: - Cisco IOS provides CLI access with User EXEC, Privileged EXEC, and Global Configuration modes. - Access methods: Console, SSH (secure), Telnet (insecure). - Command structure includes keywords and arguments; syntax must be followed. - Help features: context-sensitive help and syntax checking. - Basic device configuration includes setting hostnames, securing passwords, encrypting passwords, and configuring banner messages. - Saving configurations: running-config (RAM) vs startup-config (NVRAM). Commands: ``copy running-config startup-config``. - Ports and addressing: IPv4, IPv6, subnet masks, default gateways, and network media types. - Manual and automatic IP address configuration (DHCP). - Switch Virtual Interface (SVI) configuration with IP and ``no shutdown`` command. - Connectivity verification using ping and Packet Tracer labs. - Module emphasizes initial switch setup, securing access, and verifying end-to-end connectivity.