CCNA ASSIGNMENT 3

Q.1 Explain Cisco Wireless Technology.

ANS. Cisco helps enterprises connect and monitor devices, secure and automate operations, and compute and manage data. Explore Cisco IoT.

Q.2 List of IEEE standard.

ANS.

IEEE P80	Guide for Safety in AC Substation Grounding
IEEE 255	Standard Letter Symbols for Semiconductor Devices, IEEE-255-1963
IEEE 260	Standard Letter Symbols for Units of Measurement, IEEE-260-1978 (now 260.1-2004)
IEEE 488	Standard Digital Interface for Programmable Instrumentation, IEEE-488-1978 (now 488.1)
IEEE 519	Recommended Practice and Requirements for Harmonic Control in Electric Power Systems
IEEE 603	Standard Criteria for Safety Systems for Nuclear Power Generating Stations
IEEE 610	Standard Glossary of Software Engineering Terminology
IEEE 754	Floating point arithmetic specifications
IEEE 802	LAN/MAN

IEEE 802.1	Standards for LAN/MAN bridging and management and remote media access control (MAC) bridging
IEEE 802.2	Standards for Logical Link Control (LLC) standards for connectivity
IEEE 802.3	Ethernet Standards for Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
IEEE 802.4	Standards for token passing bus access
IEEE 802.5	Standards for token ring access and for communications between LANs and MANs
IEEE 802.6	Standards for information exchange between systems
IEEE 802.7	Standards for broadband LAN cable
IEEE 802.8	Fiber-optic connection
IEEE 802.9	Standards for integrated services, like voice.
IEEE 802.10	Standards for LAN/MAN security implementations
IEEE 802.11	Wireless Networking – "WiFi"
IEEE 802.12	Standards for demand priority access method
IEEE 802.14	Standards for cable television broadband communications
IEEE 802.15.2	Bluetooth and Wi-Fi coexistence mechanism
IEEE 802.15.4	Wireless Sensor/Control Networks "Zigbee"

IEEE 802.15.6	Wireless Body Area Network[17] (BAN)
IEEE 802.16	Wireless Networking – "WiMAX"
IEEE 802.24	Standards for Logical Link Control (LLC) standards for connectivity
IEEE 828	Configuration Management in Systems and Software Engineering
IEEE 829	Software Test Documentation
IEEE 830	Software Requirements Specifications
IEEE 854	Standard for Radix-Independent Floating-Point Arithmetic, IEEE-854-1987 (replaced by IEEE-754-2008 and newer)
IEEE 896	Futurebus
IEEE P1003.1	Portable Operating System Interface – – POSIX
IEEE 1016	Software Design Description
IEEE 1028	Standard for Software Reviews and Audits
IEEE 1044.1	Standard Classification for Software Anomalies
IEEE 1059	Software Verification And Validation Plan
IEEE 1073	Point of Care Medical Device Communication Standards
IEEE 1074	Software Development Life Cycle
IEEE 1076	VHDL – VHSIC Hardware Description Language

IEEE 1149.1	JTAG
IEEE 1149.6	AC-JTAG
IEEE 1180	Discrete cosine transform accuracy
IEEE 1233	System Requirements Specification
IEEE 1275	Open Firmware
IEEE 1284	Parallel port
IEEE P1363	Public key cryptography
IEEE 1364	Verilog
IEEE 1394	Serial bus – "FireWire", "i.Link"
IEEE 1471	software architecture / system architecture
IEEE 1541	Prefixes for Binary Multiples
IEEE 1547	Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces
IEEE 1584	Guide for Performing Arc Flash Hazard Calculations
IEEE 1588	Precision Time Protocol
IEEE 1609	Wireless Access in Vehicular Environments (WAVE)
IEEE P1619	Security in Storage Working Group (SISWG)

IEEE 1625	Standard for Rechargeable Batteries for Multi-Cell Mobile Computing Devices
IEEE 1666	IEEE Standard for Standard SystemC Language Reference Manual
IEEE 1667	Standard Protocol for Authentication in Host Attachments of Transient Storage Devices
IEEE 1701	Optical Port Communication Protocol to Complement the Utility Industry End Device Data Tables
IEEE 1800	SystemVerilog
IEEE 1801	Unified Power Format
IEEE 1849	IEEE Standard for eXtensible Event Stream (XES) for Achieving Interoperability in Event Logs and Event Streams
IEEE 1855	IEEE Standard for Fuzzy Markup Language
IEEE 1901	Broadband over Power Line Networks
IEEE 1906.1	Recommended Practice for Nanoscale and Molecular Communication Framework
IEEE 1914	Next Generation Fronthaul Interface Working Group
IEEE 1914.1	Standard for Packet-based Fronthaul Transport Networks
IEEE 1914.3	Standard for Radio Over Ethernet Encapsulations and Mappings
IEEE 2030	Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads

IEEE 2030.5	Standard for Smart Energy Profile Application Protocol	
IEEE 2050	RTOS for embedded systems standard	
IEEE 2143.1	Standard for General Process of Cryptocurrency Payment	
IEEE 2413	Standard for an Architectural Framework for the Internet of Things (IoT)	
IEEE 2418.2	Approved Draft Standard Data Format for Blockchain Systems	
IEEE 2600	Hardcopy Device and System Security (and related ISO/IEC 15408 Protection Profiles)	
IEEE 3001.4	Recommended Practice for Estimating the Costs of Industrial and Commercial Power Systems	
IEEE 7010	Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being	
IEEE 12207	Information Technology – Software life-cycle processes	
IEEE C37.2040	Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems	
IEEE Switchgear Committee	C37 series of standards for Low and High voltage equipment	
IEEE Transformers Committee	C57 series of standards for the design, testing, repair, installation and operation and maintenance of transformers	

Q.3 Explain Wireless Topologies.

ANS. The topology of a wireless network is simply the way network components are arranged. It describes both the physical layout of devices, routers, and gateways, and the paths that data follows between them.

Q.4 Explain Wireless security protocol and Encryption method type.

ANS. Wi-Fi security protocols use encryption technology to secure networks and protect the data of their clients. Wireless networks are often less secure than wired ones, so wireless security protocols are crucial for keeping you safe online. The most common Wi-Fi security protocols today are WEP, WPA, and WPA2.

There are two types of encryption in widespread use today: symmetric and asymmetric encryption. The name derives from whether or not the same key is used for encryption and decryption.

1.In symmetric encryption the same key is used for encryption and decryption. It is therefore critical that a secure method is considered to transfer the key between sender and recipient.

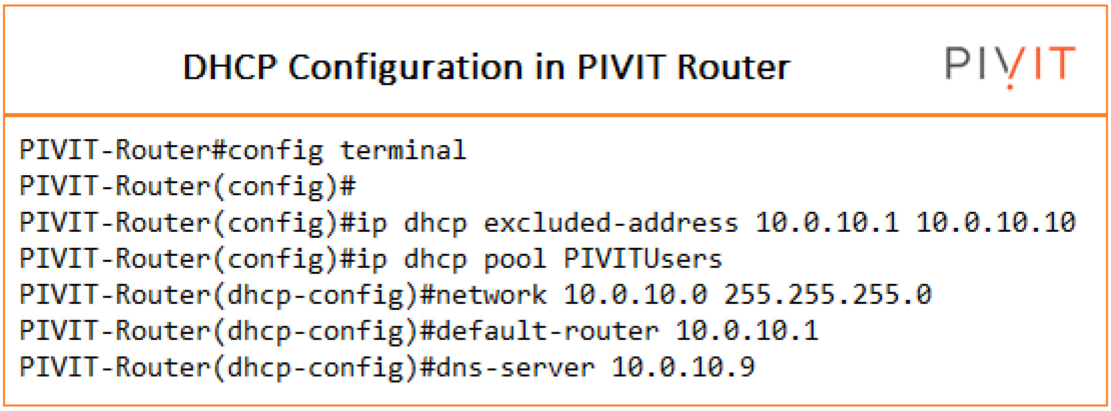
2.Asymmetric encryption uses the notion of a key pair: a different key is used for the encryption and decryption process. One of the keys is typically known as the private key and the other is known as the public key.

The private key is kept secret by the owner and the public key is either shared amongst authorised recipients or made available to the public at large.

Data encrypted with the recipient’s public key can only be decrypted with the corresponding private key. Data can therefore be transferred without the risk of unauthorised or unlawful access to the data.

Q.5 Example of DHCP configuration.

ANS.



DHCP Configuration in PIVIT Router

```
PIVIT-Router#config terminal
PIVIT-Router(config)#
PIVIT-Router(config)#ip dhcp excluded-address 10.0.10.1 10.0.10.10
PIVIT-Router(config)#ip dhcp pool PIVITUsers
PIVIT-Router(dhcp-config)#network 10.0.10.0 255.255.255.0
PIVIT-Router(dhcp-config)#default-router 10.0.10.1
PIVIT-Router(dhcp-config)#dns-server 10.0.10.9
```

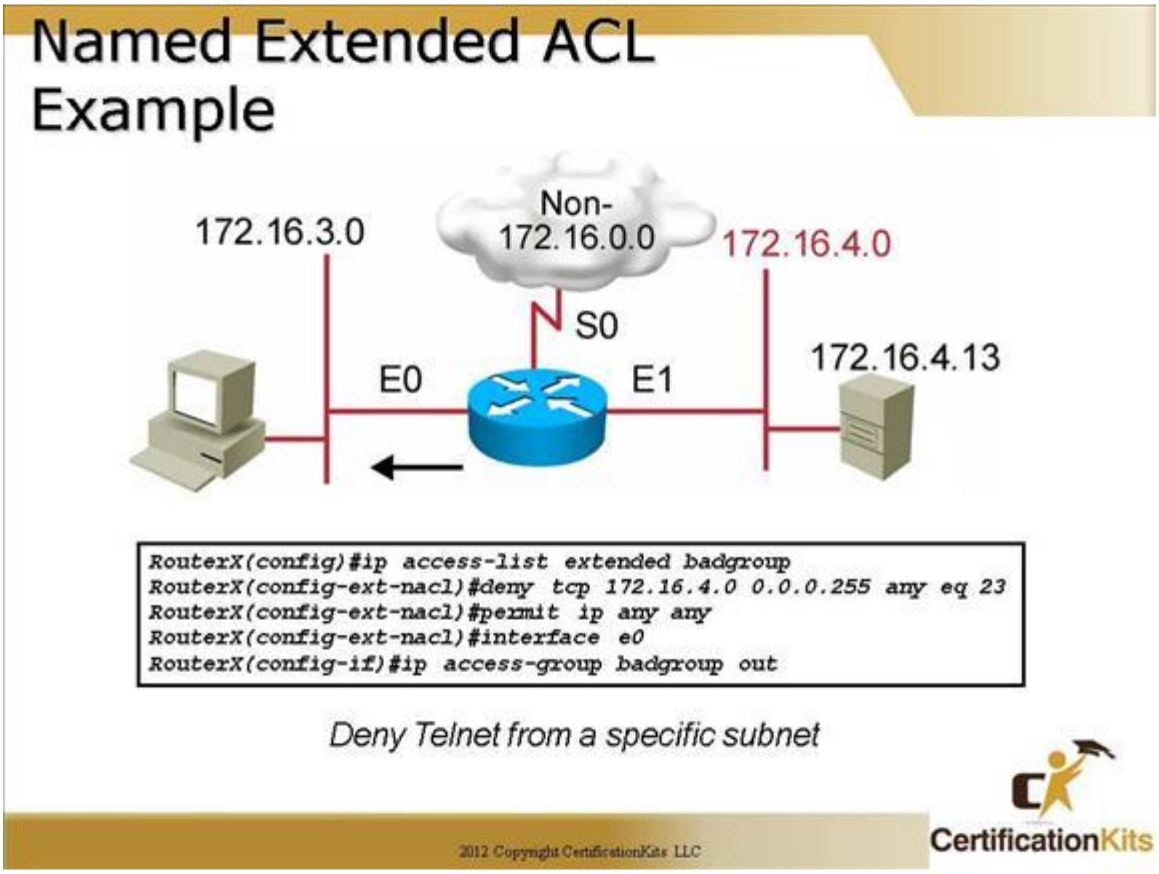
Q.6 What is ACL? Types of ACL and Example of Extended ACL.

ANS. An access control list (ACL) contains rules that grant or deny access to certain digital environments. There are two types of ACLs: Filesystem ACLs━filter access to files and/or directories. Filesystem ACLs tell operating systems which users can access the system, and what privileges the users are allowed.

TYPES OF ACL

Standard ACL

Extended ACL



Named Extended ACL Example

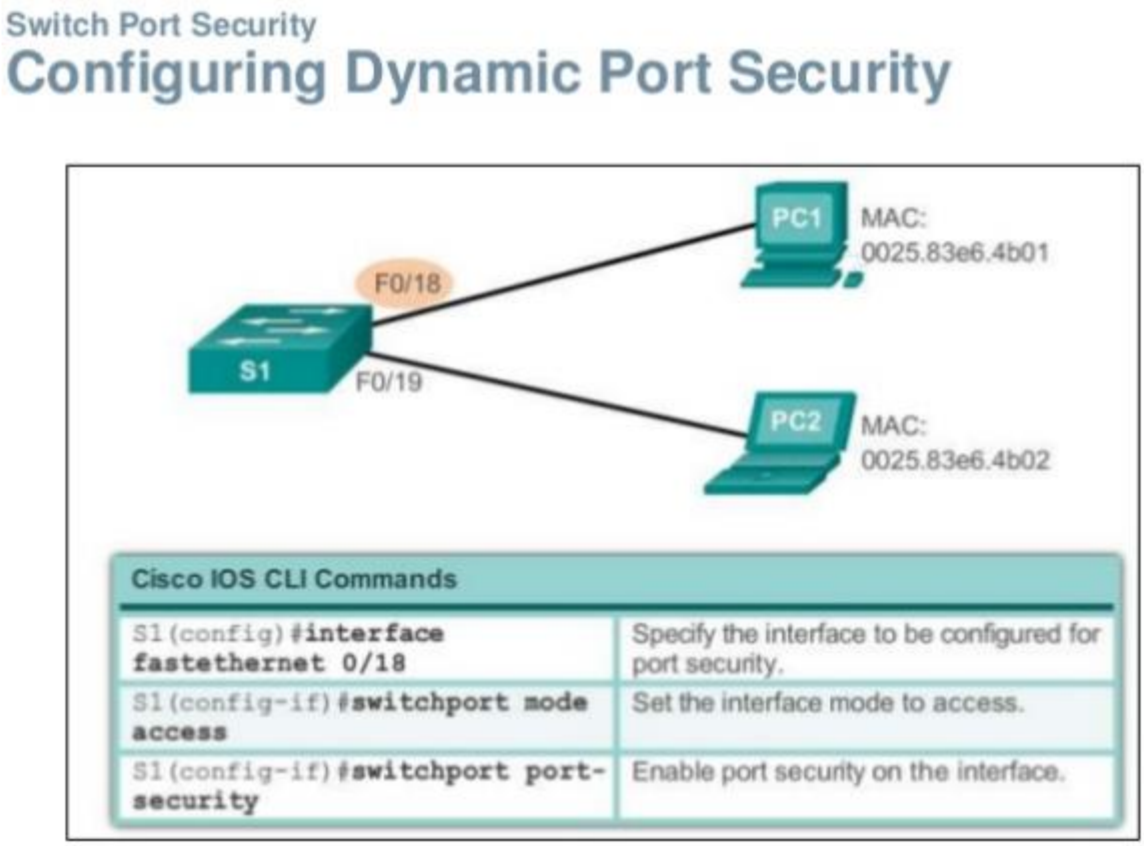
```
RouterX(config)#ip access-list extended badgroup
RouterX(config-ext-nacl)#deny tcp 172.16.4.0 0.0.0.255 any eq 23
RouterX(config-ext-nacl)#permit ip any any
RouterX(config-ext-nacl)#interface e0
RouterX(config-if)#ip access-group badgroup out
```

Deny Telnet from a specific subnet

CertificationKits

Q.7 Example of Port security in Switch.

ANS.



Switch Port Security

Configuring Dynamic Port Security

Cisco IOS CLI Commands	
`S1(config)#interface fastethernet 0/18`	Specify the interface to be configured for port security.
`S1(config-if)#switchport mode access`	Set the interface mode to access.
`S1(config-if)#switchport port-security`	Enable port security on the interface.

Q.8 List Of WAN connection with protocol.

ANS. Automatic IP

Static IP

PPPoE

PPTP

L2TP

PROTCOLS

HDLC

PPP

LCP

NCP

FRAME RELAY

ISDN

Q.9 Explain Frame-Relay and PPP.

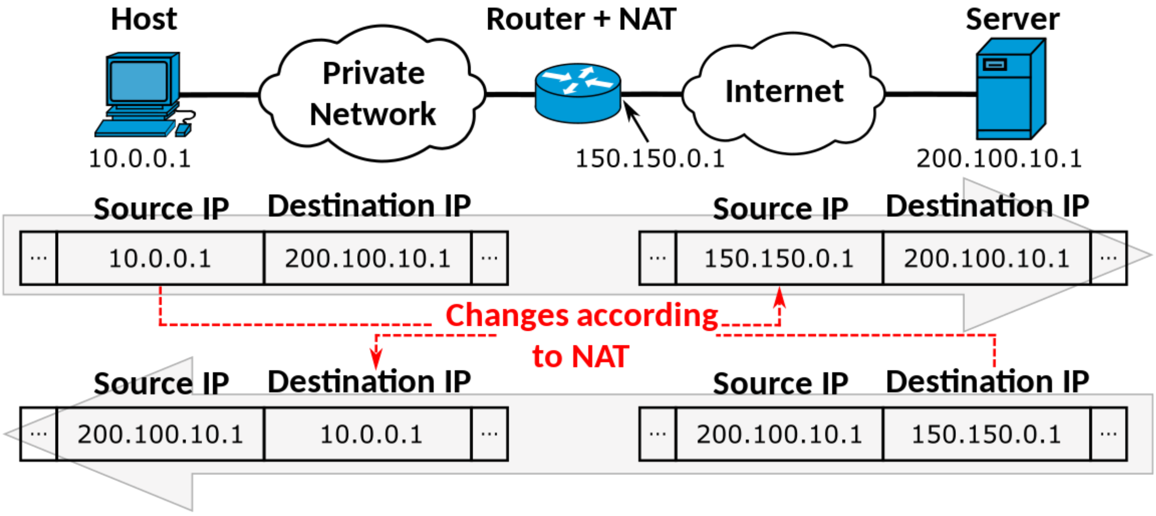
ANS. Frame relay is a packet-switching telecommunications service designed for cost-efficient data transmission for intermittent traffic between local area networks (LANs) and between endpoints in wide area networks (WANs).

PPP

Point-to-Point Protocol (PPP) is a TCP/IP protocol that is used to connect one computer system to another. Computers use PPP to communicate over the telephone network or the Internet. A PPP connection exists when two systems physically connect through a telephone line. You can use PPP to connect one system to another.

Q.10 What is NAT? explain with one example.

ANS. NAT stands for network address translation. It's a way to map multiple local private addresses to a public one before transferring the information. Organizations that want multiple devices to employ a single IP address use NAT, as do most home routers.



Q.11 What is HDLC? Which command using to show in software.

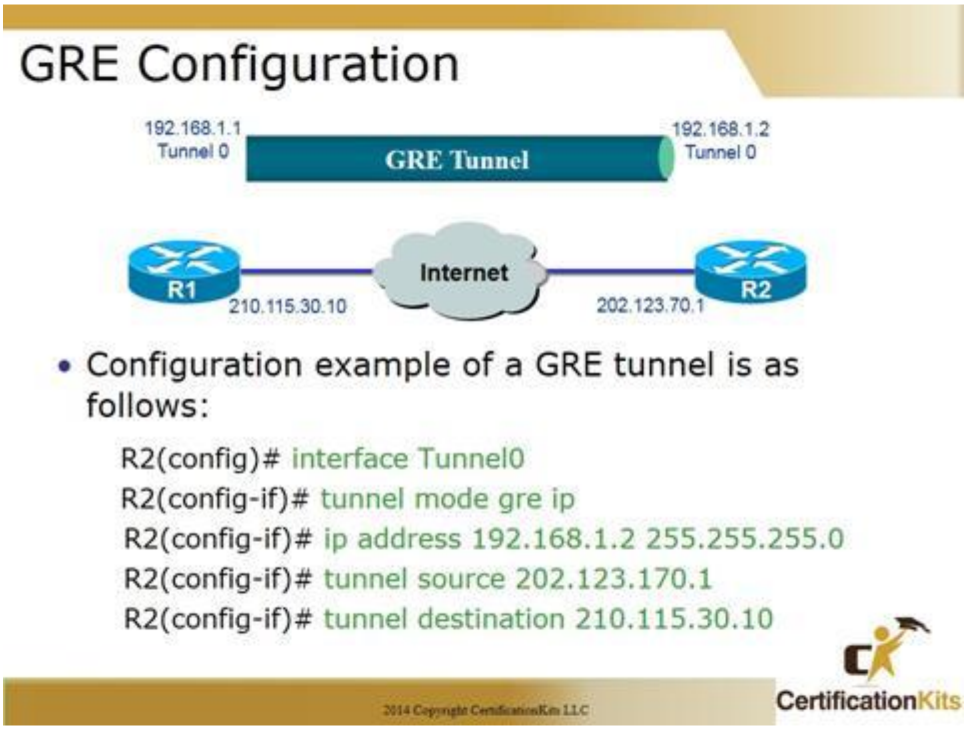
ANS. High-Level Data Link Control (HDLC) generally uses term “frame” to indicate and represent an entity of data or a protocol of data unit often transmitted or transferred from one station to another station. Each and every frame on link should begin and end with Flag Sequence Field (F).

```
Router# show interfaces serial 0/0
```

Q.12 What is Encapsulation? example of GRE Tunnel.

ANS. Encapsulation is the process of adding additional information when data is traveling in OSI or TCP/IP model. The additional information has been added on sender's side, starting from Application layer to Physical layer.

Tunneling is a concept where we put 'packets into packets' so that they can be transported over certain networks. We also call this encapsulation. A good example is when you have two sites with IPv6 addresses on their LAN but they are only connected to the Internet with IPv4 addresses.



GRE Configuration

- Configuration example of a GRE tunnel is as follows:

```
R2(config)# interface Tunnel0
R2(config-if)# tunnel mode gre ip
R2(config-if)# ip address 192.168.1.2 255.255.255.0
R2(config-if)# tunnel source 202.123.170.1
R2(config-if)# tunnel destination 210.115.30.10
```