SENG 460

Practice of Information Security and Privacy

Telecommunications and Network Security

Overview

- Telecommunication & Network Basics
- Network Models
- Remote Connection Security
- Wireless Security
- Network Attacks & Countermeasures

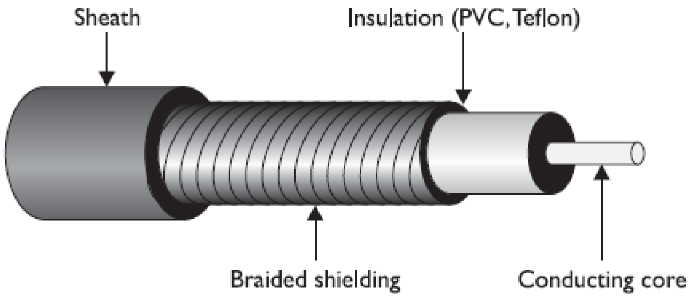
Telecommunication & Network Basics
- Some Concepts & Terminologies

- **Telecommunication:** the electrical transmission of data among systems through analog, digital, or wireless transmission types.
- **Network Protocol:** a standard set of rules that determines how systems will communicate across networks.
- **Bandwidth:** the maximum amount of *bits* that can be transmitted over a link within a time unit.
- **Data Throughput:** the actual amount of *data* that can be transmitted over a link within a time unit.
- **Baseband:** data is sent as digital signals through the media as a single channel that uses the entire bandwidth of the media.
- **Broadband:** data is sent in the form of an analog signal through the media . Each transmission is assigned to a portion of the bandwidth, hence multiple transmissions are possible at the same time.

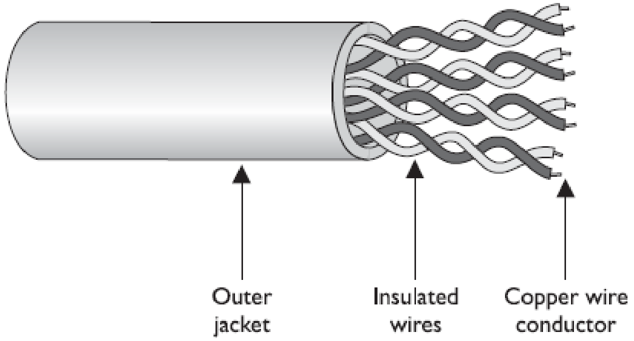
Telecommunication & Network Basics

- Data Transmission Media (Cabling)

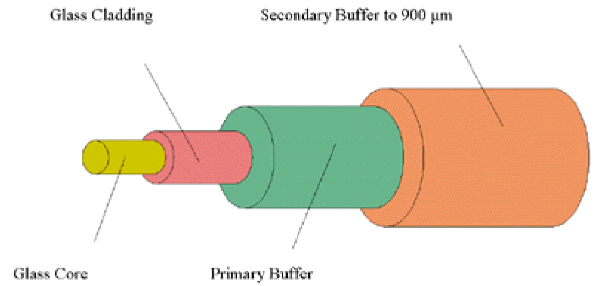
- Coaxial Cables



- Twisted-Pair Cable



- Fiber-Optic Cable



A fibre optic cable

Telecommunication & Network Basics
- Cabling Problems

- **Noise:** *Electromagnetic Interference (EMI)* generated by other devices in the environment can combine with the data being transmitted over the cable and distort the original signal

- **Attenuation:** signal strength can be lost as it travels. The longer a cable, the more signal loss occurs, which causes the signal carrying the data to deteriorate

- **Crosstalk:** a phenomenon that occurs when electrical signals of one wire spill over to the signals of another wire. When the different electrical signals mix, their integrity degrades and data corruption can occur.

- **Fire hazard:** Some cables produce hazardous gases when on fire that would spread throughout the building quickly.

Telecommunication & Network Basics
- Cable Media Comparation

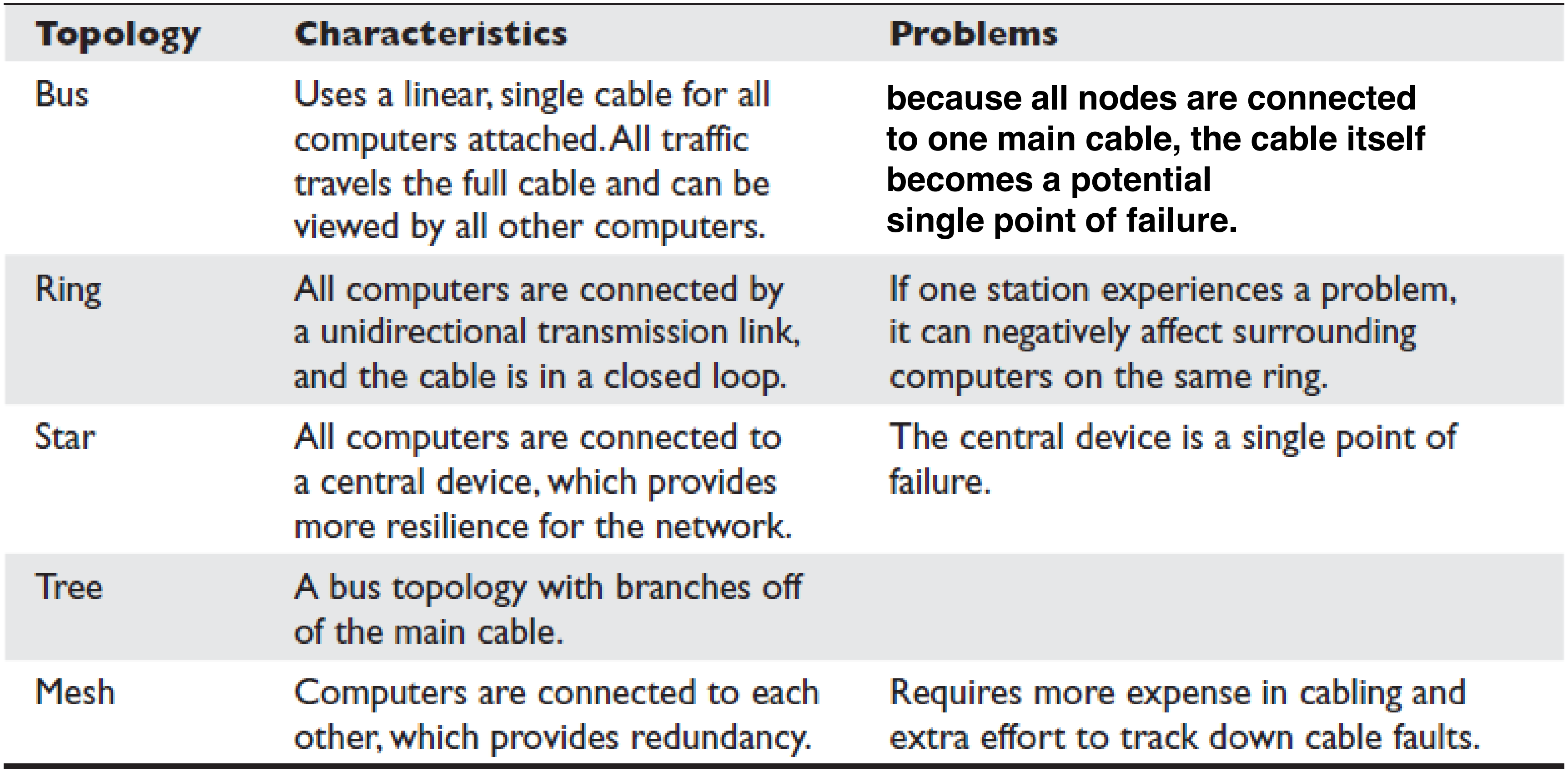
- **Coaxial Cables**
  - more resistant to electromagnetic interference (EMI) than Twisted-Pair Cable
  - provides a higher bandwidth than Twisted-Pair Cable
  - supports the use of longer cable lengths than Twisted-Pair Cable

- **Twisted-Pair Cable**
  - Cheaper
  - Easier to work with

- **Fiber-Optic Cable**
  - highest transmission speeds
  - not so affected by *Attenuation* and *EMI*
  - more secure

Telecommunication & Network Basics
- Network Topology

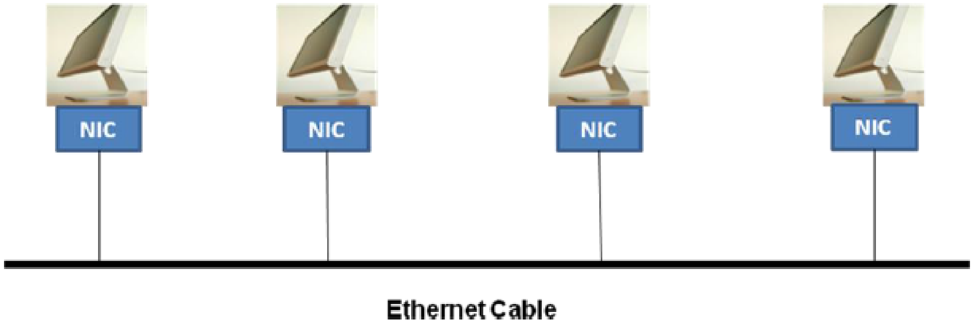
The physical arrangement of computers and devices is called a ***network topology***.

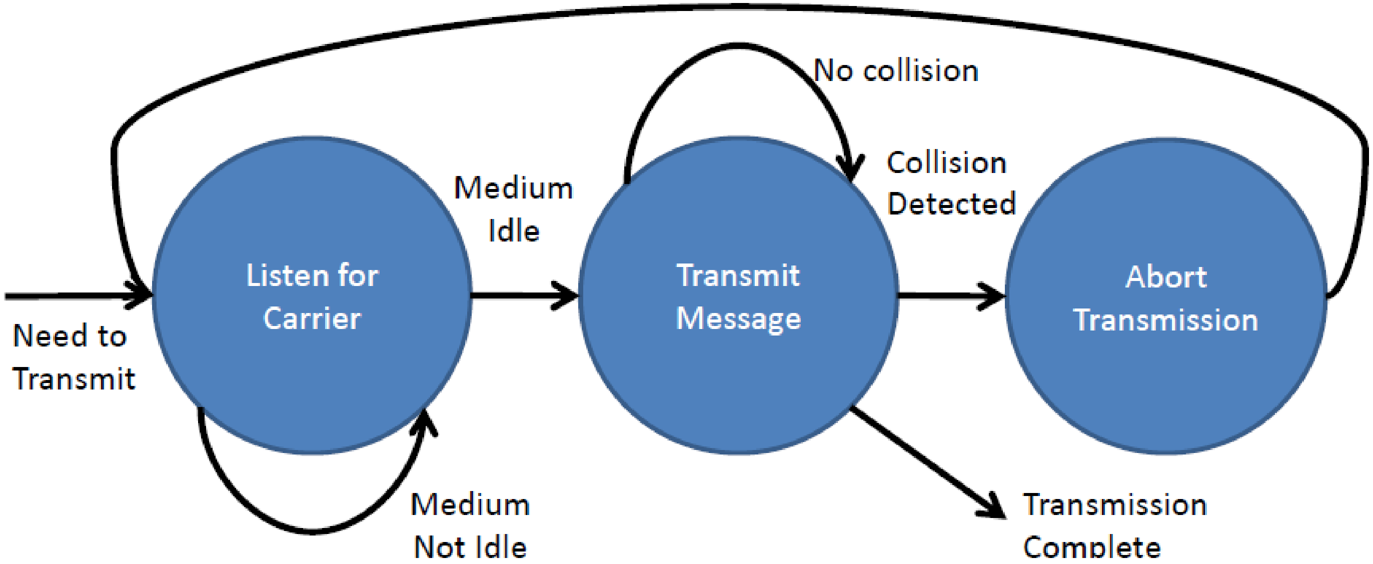


Topology	Characteristics	Problems
Bus	Uses a linear, single cable for all computers attached. All traffic travels the full cable and can be viewed by all other computers.	**because all nodes are connected to one main cable, the cable itself becomes a potential single point of failure.**
Ring	All computers are connected by a unidirectional transmission link, and the cable is in a closed loop.	If one station experiences a problem, it can negatively affect surrounding computers on the same ring.
Star	All computers are connected to a central device, which provides more resilience for the network.	The central device is a single point of failure.
Tree	A bus topology with branches off of the main cable.	
Mesh	Computers are connected to each other, which provides redundancy.	Requires more expense in cabling and extra effort to track down cable faults.

Telecommunication & Network Basics
- Network Media Access Technologies - Ethernet

Ethernet

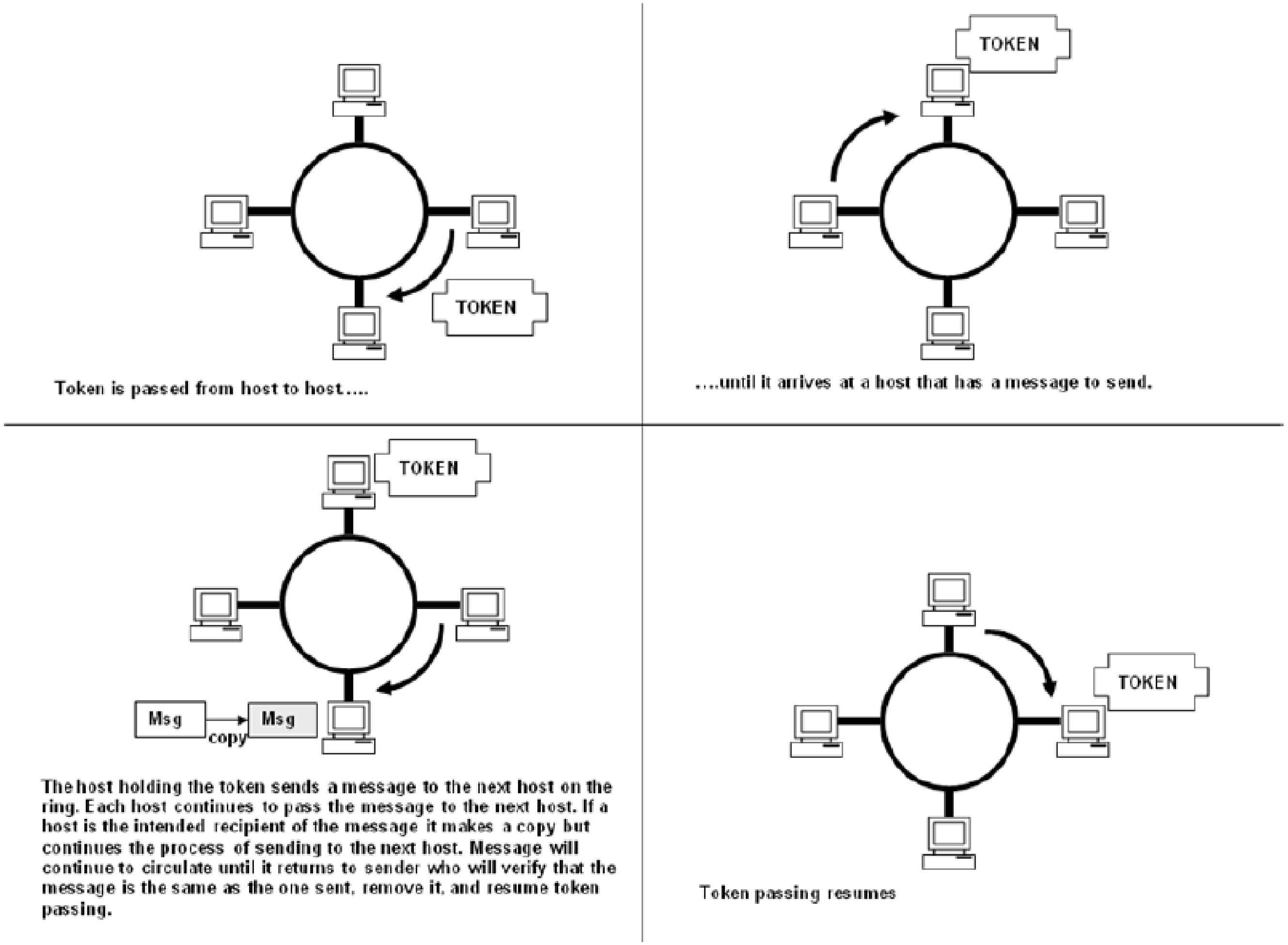




Telecommunication & Network Basics

- Network Media Access Technologies – Token Ring

Token Ring



Token is passed from host to host….

….until it arrives at a host that has a message to send.

The host holding the token sends a message to the next host on the ring. Each host continues to pass the message to the next host. If a host is the intended recipient of the message it makes a copy but continues the process of sending to the next host. Message will continue to circulate until it returns to sender who will verify that the message is the same as the one sent, remove it, and resume token passing.

Token passing resumes

Telecommunication & Network Basics

- Networking Devices

- **Repeaters:** a devices which only repeats electrical signals between cable segments, which enables it to extend a network. (A ***HUB*** is a multiport repeater)
- **Bridges:** a device used to connect LAN segments. It works with MAC addresses. A bridge amplifies the electrical signal, also enable the administrator to filter frames based on MAC addresses.
- **Switches:** a multiport bridging device, and each port provides dedicated bandwidth to the device attached to it.
- **Routers:** a device that has two or more interfaces to connect similar or different networks. It works with IP addresses, and It knows how to get packets to their destinations based on a local routing table.

Telecommunication & Network Basics
- Network Services

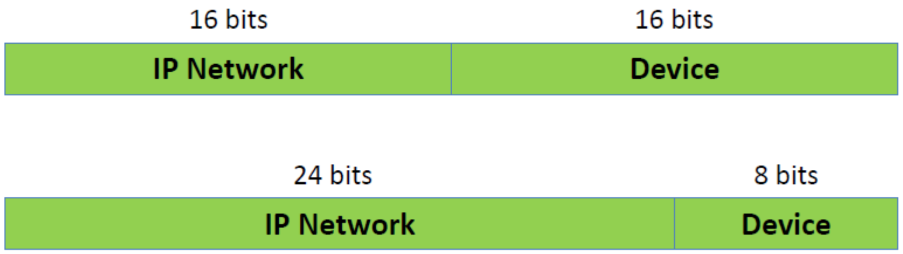
- **Domain Name Service:** used to resolve hostnames to IP addresses so names can be used instead of IP addresses within networked environments.
- **Address Resolution Protocol:** Used to assign hardware addresses, it maps the hardware address (MAC address) and associated IP address and stores this mapping in its table for a predefined amount of time.
- **Dynamic Host Configuration Protocol:** Used to assign IP addresses to network clients in real time.
- **Internet Control Message Protocol:** used to test connectivity and troubleshoot problems on IP networks.
- **Simple Network Management Protocol:** with the growing demand of managing network IP devices. SNMP was developed to view the status of their network, traffic flows, and the hosts within the network.

Telecommunication & Network Basics
- Network Addressing

- Public IP Address
  - A public IP address is assigned to every computer that connects to the Internet where each IP is unique
  - A public IP address can be either **static** or **dynamic**.
- Private IP Address
  - An IP address is considered private if the IP number falls within one of the IP address ranges reserved for private networks

10.0.0.0 – 10.255.255.255 (Total Addresses: 16,777,216)
172.16.0.0 – 172.31.255.255 (Total Addresses: 1,048,576)
192.168.0.0 – 192.168.255.255 (Total Addresses: 65,536)

- Devices with private IP addresses cannot connect directly to the Internet

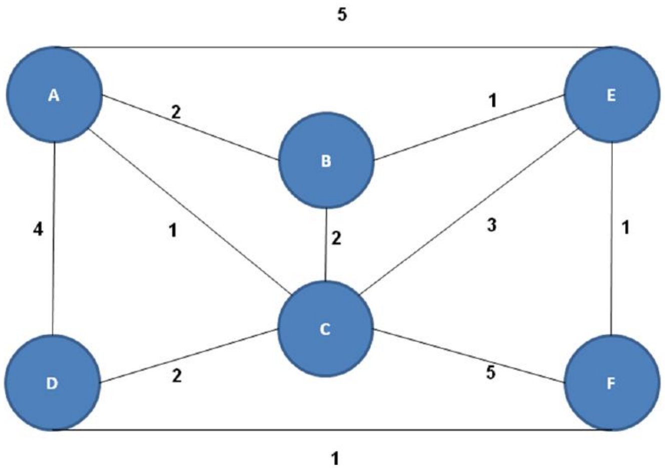


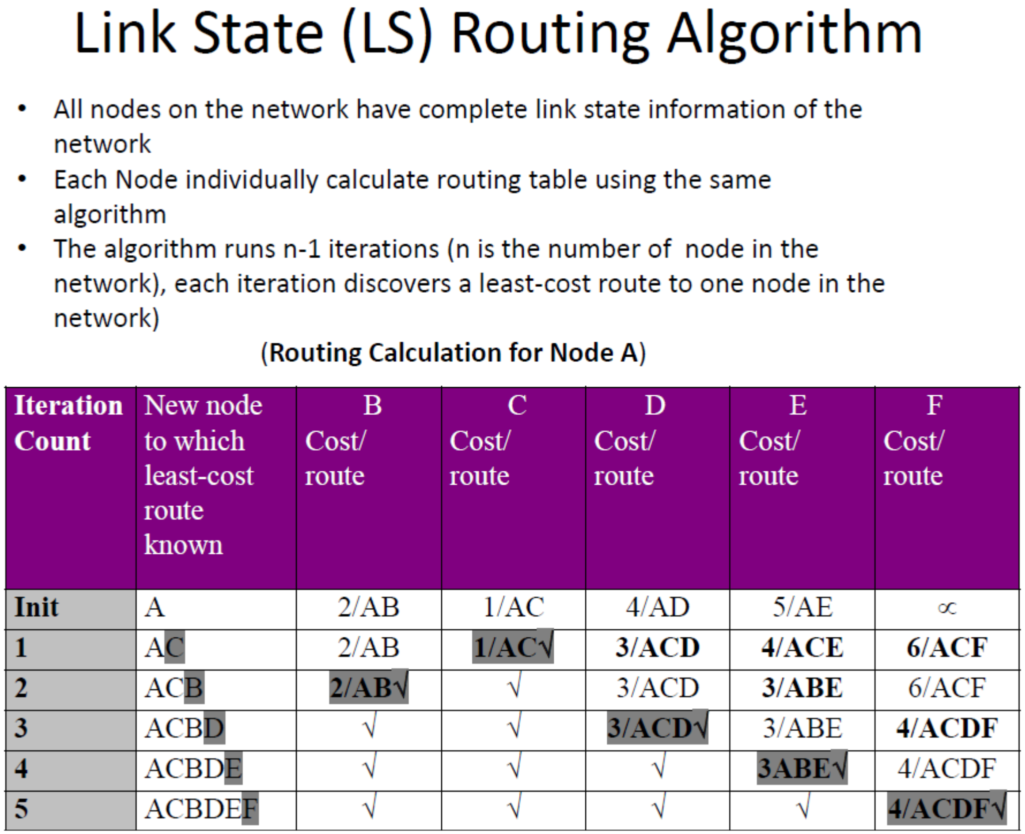
16 bits
IP Network
16 bits
Device

24 bits
IP Network
8 bits
Device

Denote an IP network with the notation: ***x.y.z.0/n***

Telecommunication & Network Basics
- Network Routing Algorithms





Link State (LS) Routing Algorithm

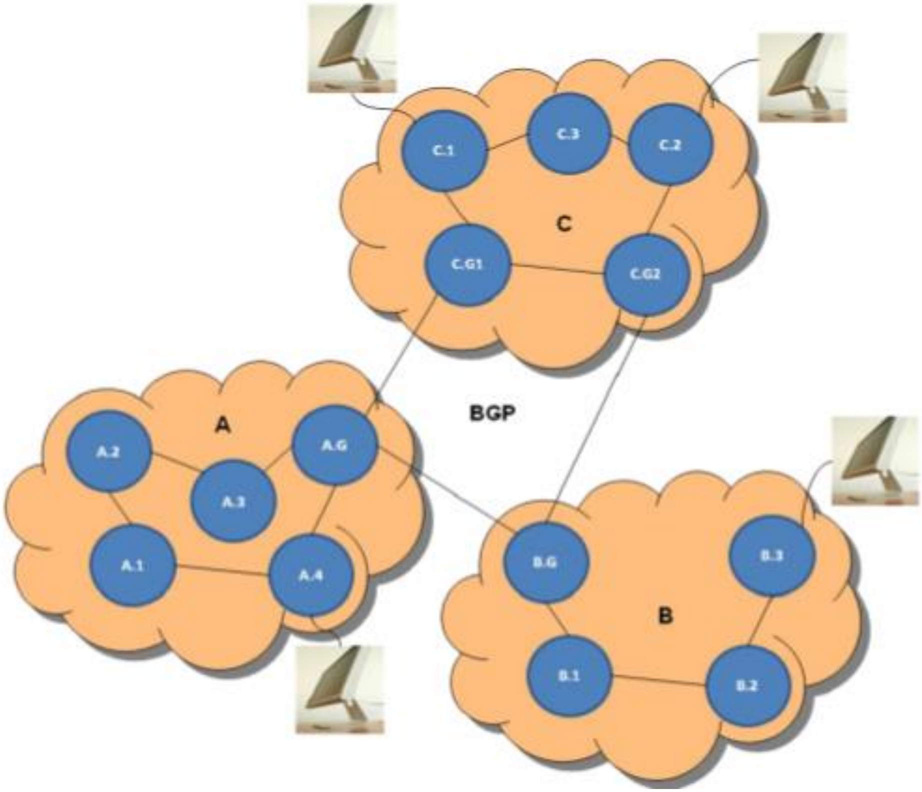
- All nodes on the network have complete link state information of the network
- Each Node individually calculate routing table using the same algorithm
- The algorithm runs n-1 iterations (n is the number of node in the network), each iteration discovers a least-cost route to one node in the network)

(Routing Calculation for Node A)

Iteration Count	New node to which least-cost route known	B Cost/ route	C Cost/ route	D Cost/ route	E Cost/ route	F Cost/ route
Init	A	2/AB	1/AC	4/AD	5/AE	∝
1	AC	2/AB	**1/AC√**	**3/ACD**	**4/ACE**	**6/ACF**
2	ACB	**2/AB√**	√	3/ACD	**3/ABE**	6/ACF
3	ACBD	√	√	**3/ACD√**	3/ABE	**4/ACDF**
4	ACBDE	√	√	√	**3ABE√**	4/ACDF
5	ACBDEF	√	√	√	√	**4/ACDF√**

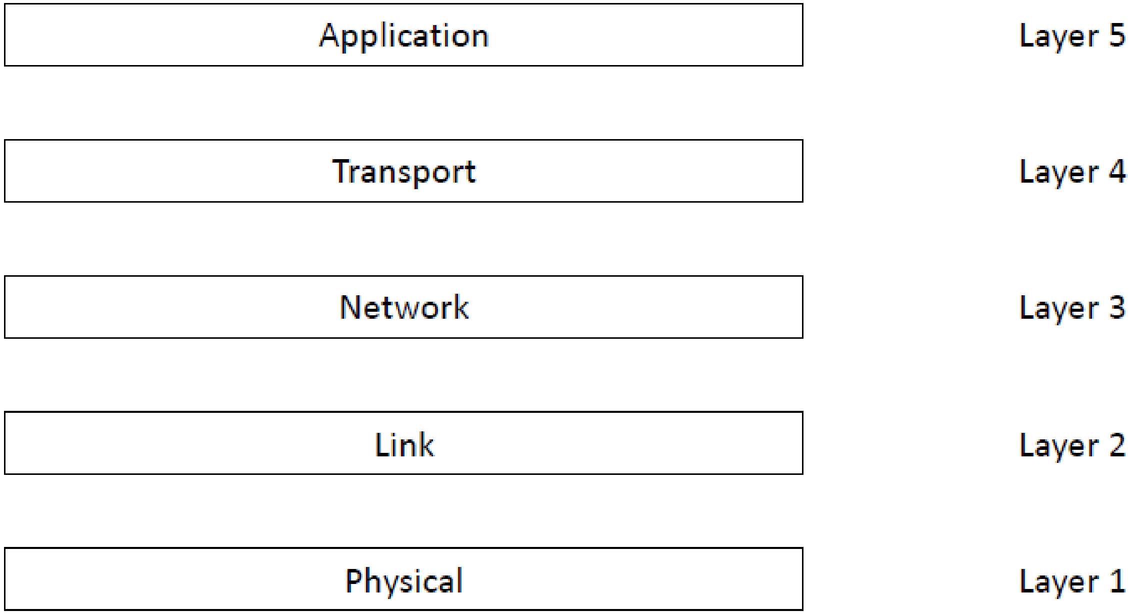
Telecommunication & Network Basics
- Network Hierarchical Routing

- Internet is divide into regions called Autonomous Systems (AS)
- Gateway nodes use Border Gateway Protocol (BGP)
- Nodes within AS use routing algorithms like LS



Network Models
- TCP/IP Model

Divide the Processing of Networking into different layers



Application	Layer 5
Transport	Layer 4
Network	Layer 3
Link	Layer 2
Physical	Layer 1

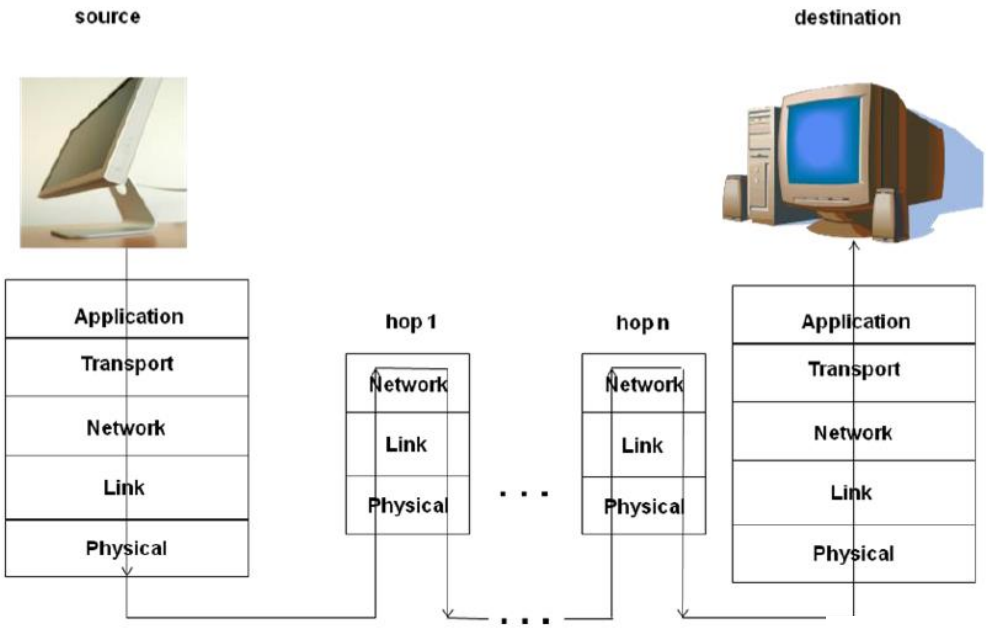
(TCP/IP Model)

Network Models
- Responsibilities of TCP/IP Model Layers

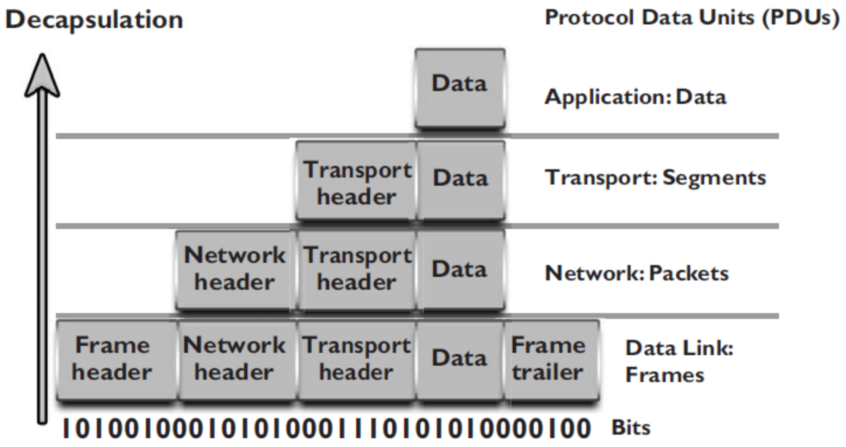
- Application Layer : Responsible for Application – specific message Handling (e.g. HTTP, SMTP, FTP)
- Transport layer: Breaks application message into packets, handles some packet delivery issues such as out of order packet delivery, packet missing, etc. (e.g. TCP)
- Network layer: Responsible for packet routing (e.g. IP)
- Link layer: Responsible for point-to-point communications (e.g. Ethernet, Token Ring)
- Physical layer: Responsible for physical medium setup (e.g. Cable, Copper wires)

Network Models

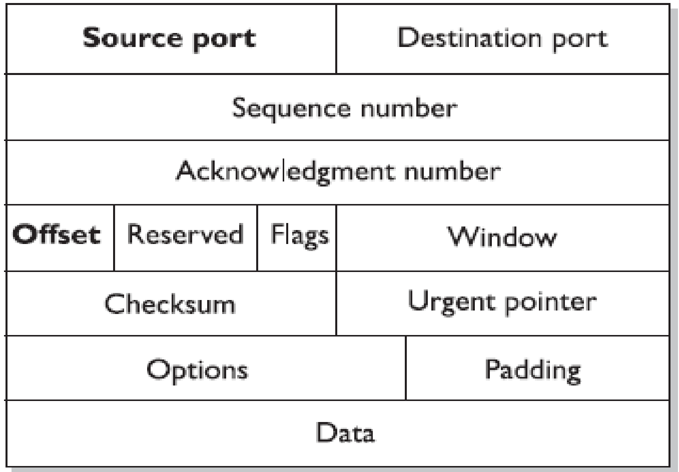
- Network Process with TCP/IP Model



Data Encapsulation: A common procedure to process data for data transmission, which involves adding header and trailer information to the original data.



Network Models
- Network Data Format



Source port | Destination port

Sequence number

Acknowledgment number

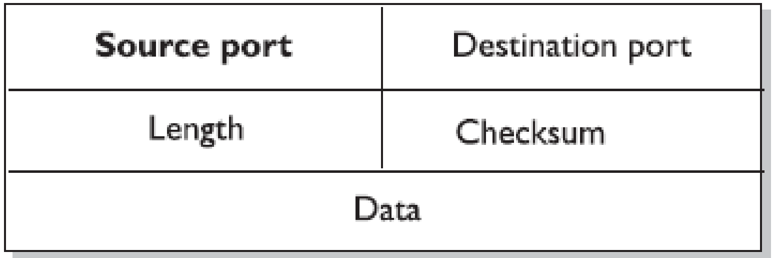
Offset | Reserved | Flags | Window

Checksum | Urgent pointer

Options | Padding

Data

TCP Segment Format

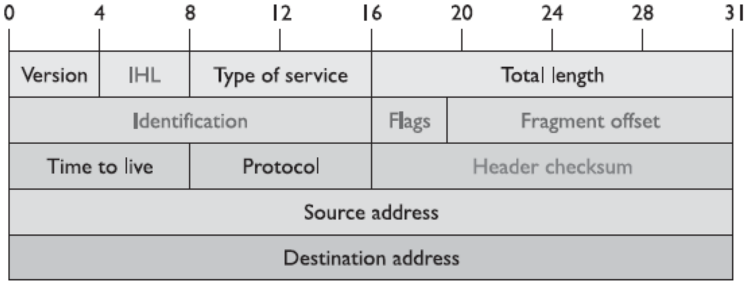


Source port | Destination port

Length | Checksum

Data

UDP Segment Format



Version | IHL | Type of service | Total length

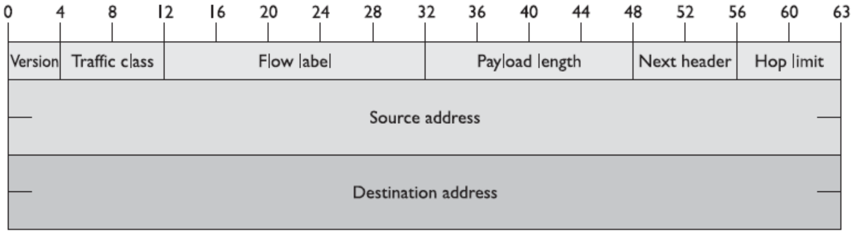
Identification | Flags | Fragment offset

Time to live | Protocol | Header checksum

Source address

Destination address

IP V4 Packet Header Format



Version | Traffic class | Flow label | Payload length | Next header | Hop limit

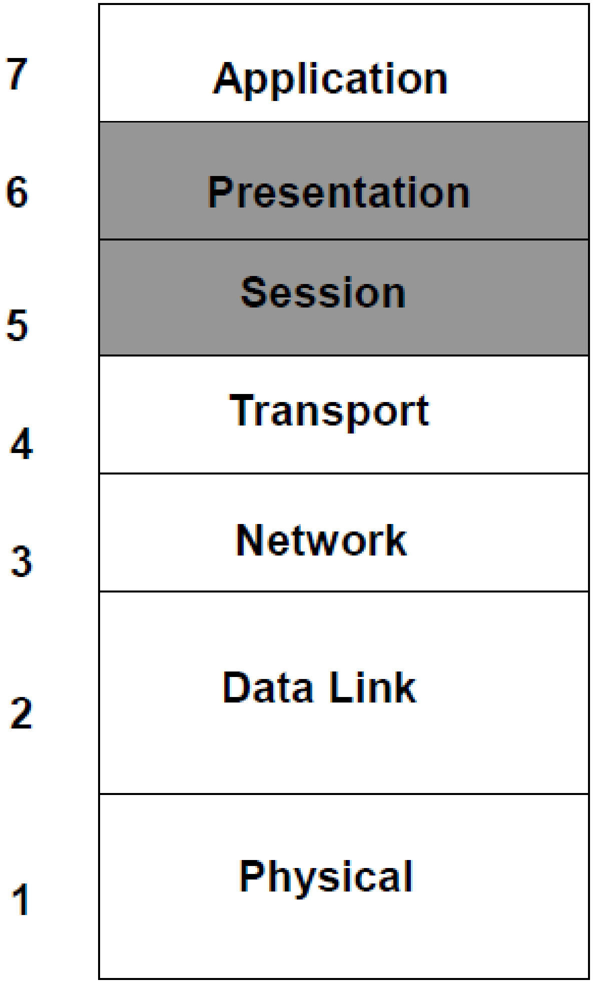
Source address

Destination address

IP V6 Packet Header Format

Network Models

- Open Systems Interconnection Reference Model



7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

1 Physical

- Presentation layer subsumes user directed input/output functionalities that are common across different applications.
- Session layer maintains process-to-process communication details and provides a higher-level abstraction between an application and the transport layer (e.g. Unix socket).

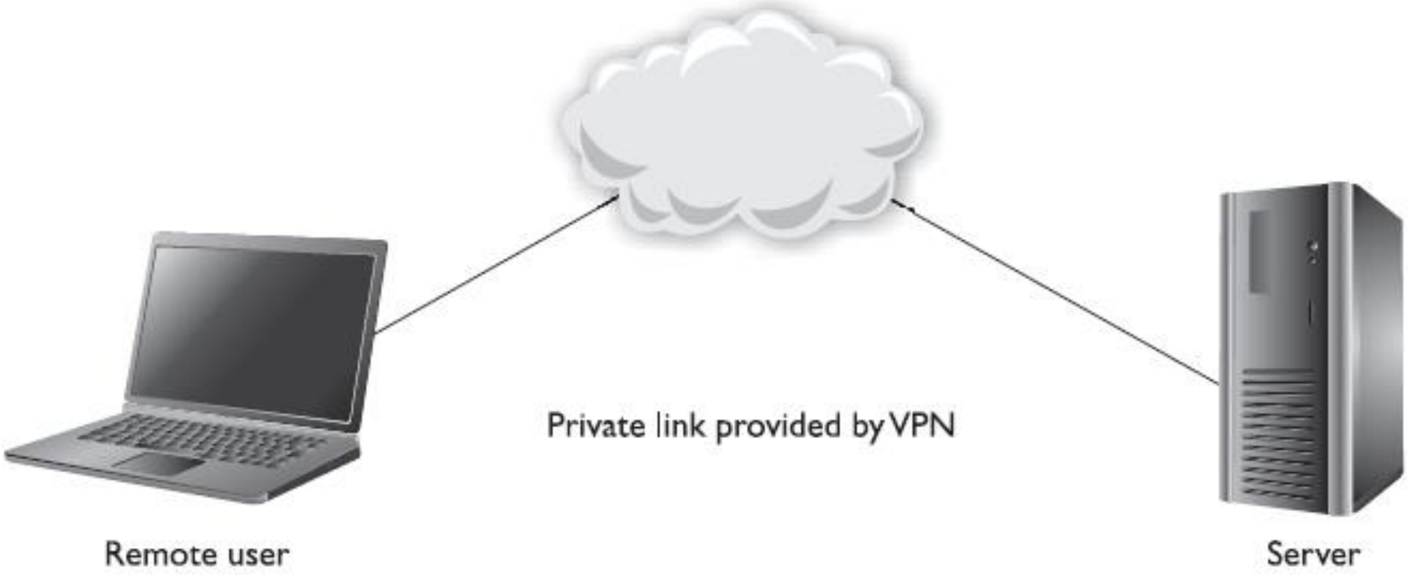
Remote Connection Security

Remote connectivity covers several technologies that enable remote and home users to connect to networks that will grant them access to network resources that help them perform their tasks. Most of the time, these users must first gain access to the Internet through an ISP, which sets up a connection to the destination network.

- **Virtual Private Network (VPN):** a secure, private connection through an untrusted network.
- **Authentication Protocols:** protocols used by remote users to authenticate themselves over remote connections.

Remote Connection Security
- Virtual Private Network (VPN)

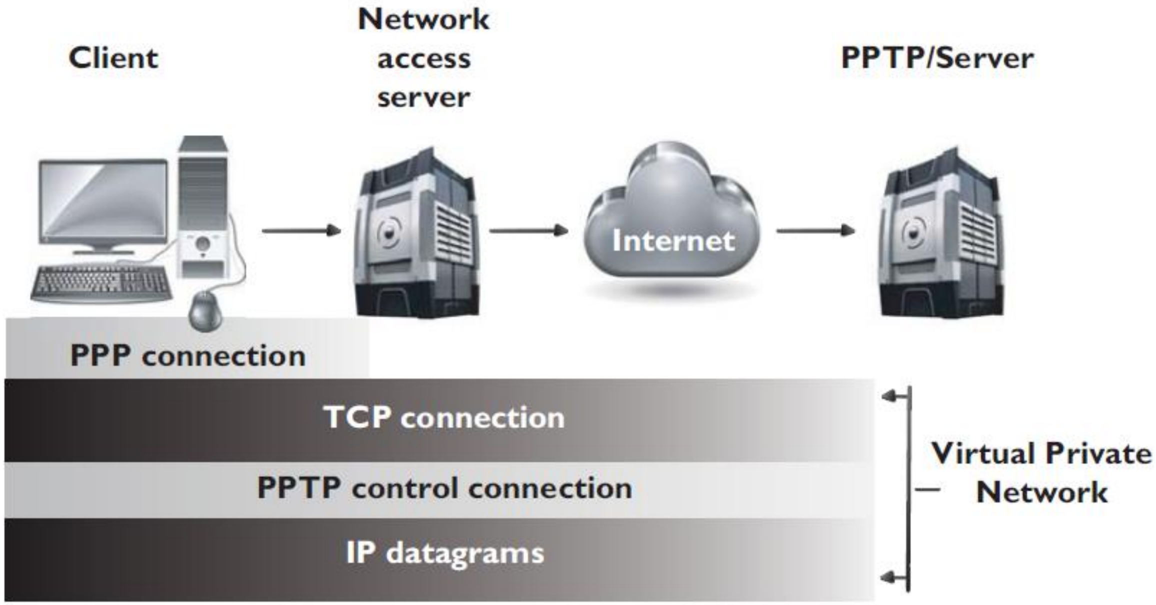
VPN technology requires a end-to-end connection to work and it assumes encryption on this connection. ***Point-to-point protocol (PPP)*** is a protocol commonly used for point-to-point connections.



*In computer networks, a **tunneling protocol** allows a network user to access or provide a network service that the underlying network does not support or provide directly.*

Remote Connection Security
- VPN Solutions – Network Layer

1) Point-To-Point Tunneling Protocol (PPTP) + IPSec: PPTP encapsulate **PPP** packets and extend a **PPP** connection through an IP network.
2) Layer 2 Tunneling Protocol (L2TP) + IPSec: L2TP tunnels PPP traffic over various network types (IP, ATM, X.25, etc.); thus, it is not just restricted to IP networks



Remote Connection Security
- PPTP vs. L2TP

1. If the Internet is an IP-based network, why do we even need PPP?
Answer: *The point-to-point telecommunication line devices that connect individual systems to the Internet do not understand IP, so the traffic that travels over these links has to be encapsulated in PPP.*

2. If PPTP and L2TP do not actually secure data themselves, then why do they exist?
Answer: *They extend PPP connections by providing a tunnel through networks that do not understand PPP.*

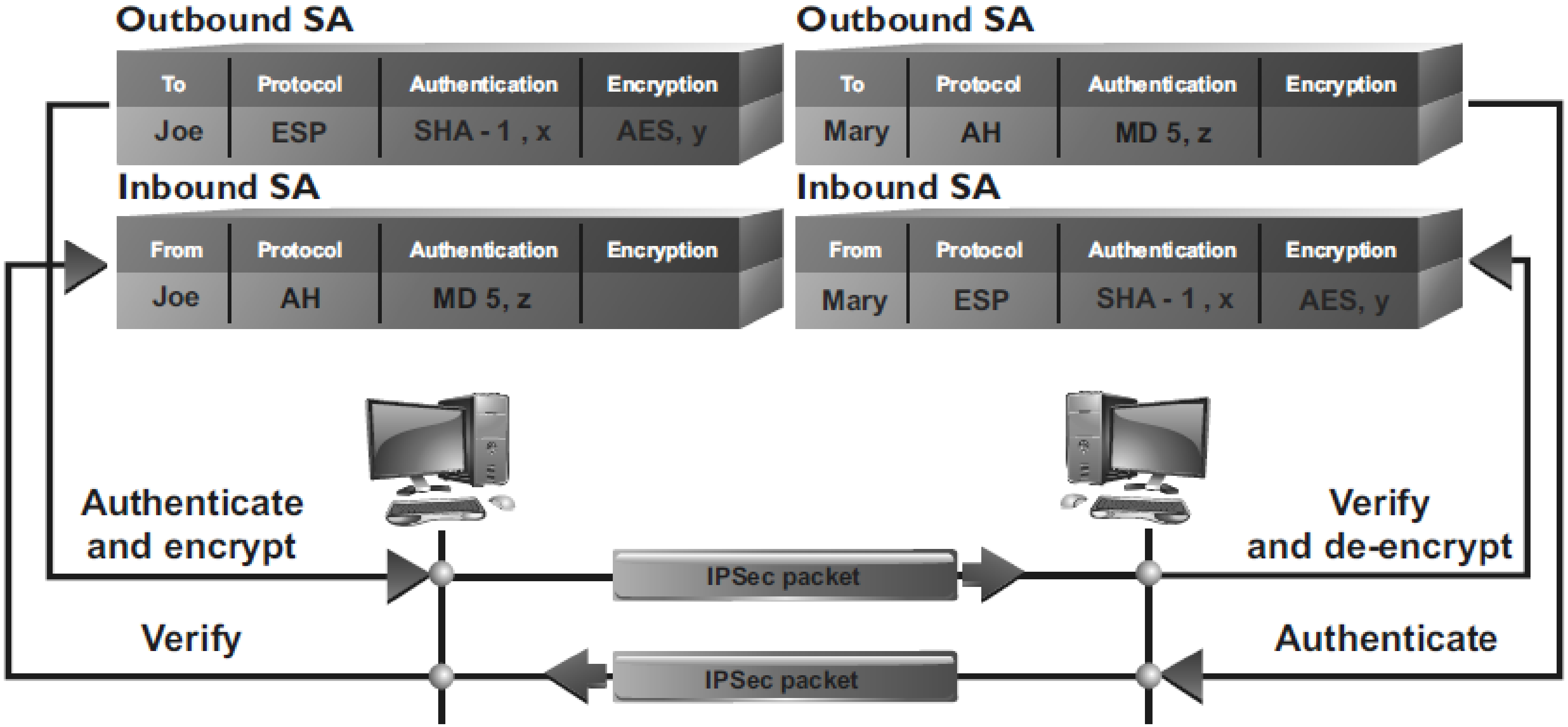
3. If PPTP and L2TP basically do the same thing, why choose L2TP over PPTP?
Answer: *PPTP only works over IP-based networks. L2TP works over IP-based and WAN-based (ATM, frame relay) connections. If a PPP connection needs to be extended over a WAN-based connection, L2TP must be used.*

4. If a connection is using IP, PPP, and L2TP, where does IPSec come into play?
Answer: *IPSec provides the encryption, data integrity, and system-based authentication.*

Remote Connection Security

- IPSec

IPSec is a suite of protocols that was developed to specifically protect IP traffic. IPv4 does not have any integrated security, so IPSec was developed to “bolt onto” IP and secure the data the protocol transmits. Where PPTP and L2TP work at the data link layer, IPSec works at the network layer of the OSI model.



Outbound SA

To	Protocol	Authentication	Encryption
Joe	ESP	SHA - 1 , x	AES, y

Inbound SA

From	Protocol	Authentication	Encryption
Joe	AH	MD 5, z	

Outbound SA

To	Protocol	Authentication	Encryption
Mary	AH	MD 5, z	

Inbound SA

From	Protocol	Authentication	Encryption
Mary	ESP	SHA - 1 , x	AES, y

Remote Connection Security
- VPN Solutions – Application Layer

3) Secure Sockets Layer (SSL): SSL works at the transport and session layers of the network stack and is used mainly to protect HTTP traffic.

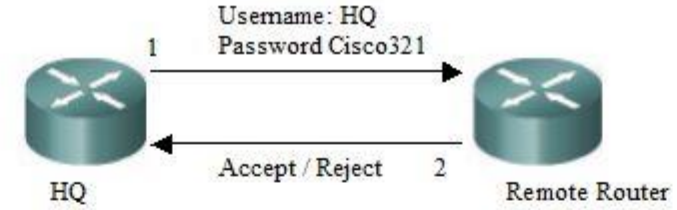
SSL Portal VPNs: An individual uses a single standard SSL connection to a web site to securely access multiple network services. The web site accessed is typically called a portal because it is a single location that provides access to other resources. The remote user accesses the SSL VPN gateway using a web browser, is authenticated, and is then presented with a web page that acts as the portal to the other services.

SSL Tunnel VPNs: An individual uses a web browser to securely access multiple network services, including applications and protocols that are not web-based, through an SSL tunnel. This commonly requires custom programming to allow the services to be accessible through a web-based connection.

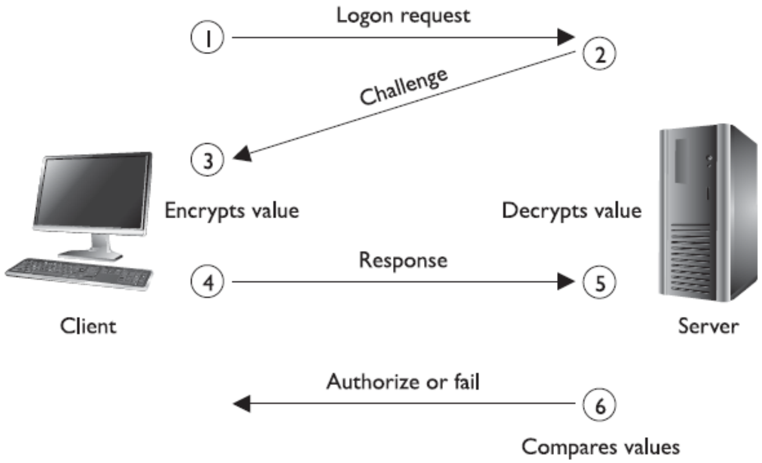
Remote Connection Security
- Remote Authentication Protocols

Password Authentication Protocol (PAP)

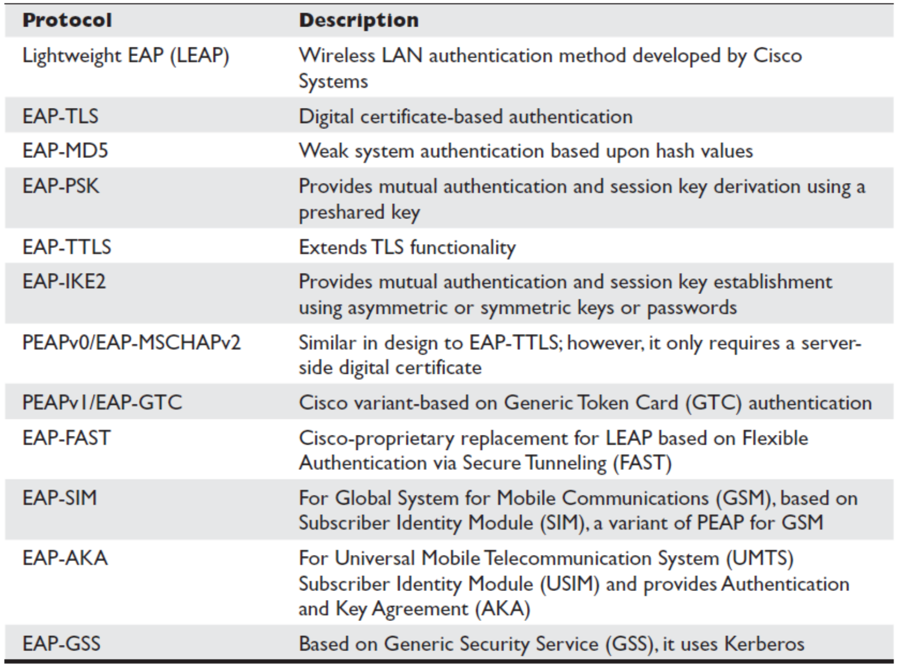
PAP 2-way handshake



Challenge Handshake Authentication Protocol (CHAP)

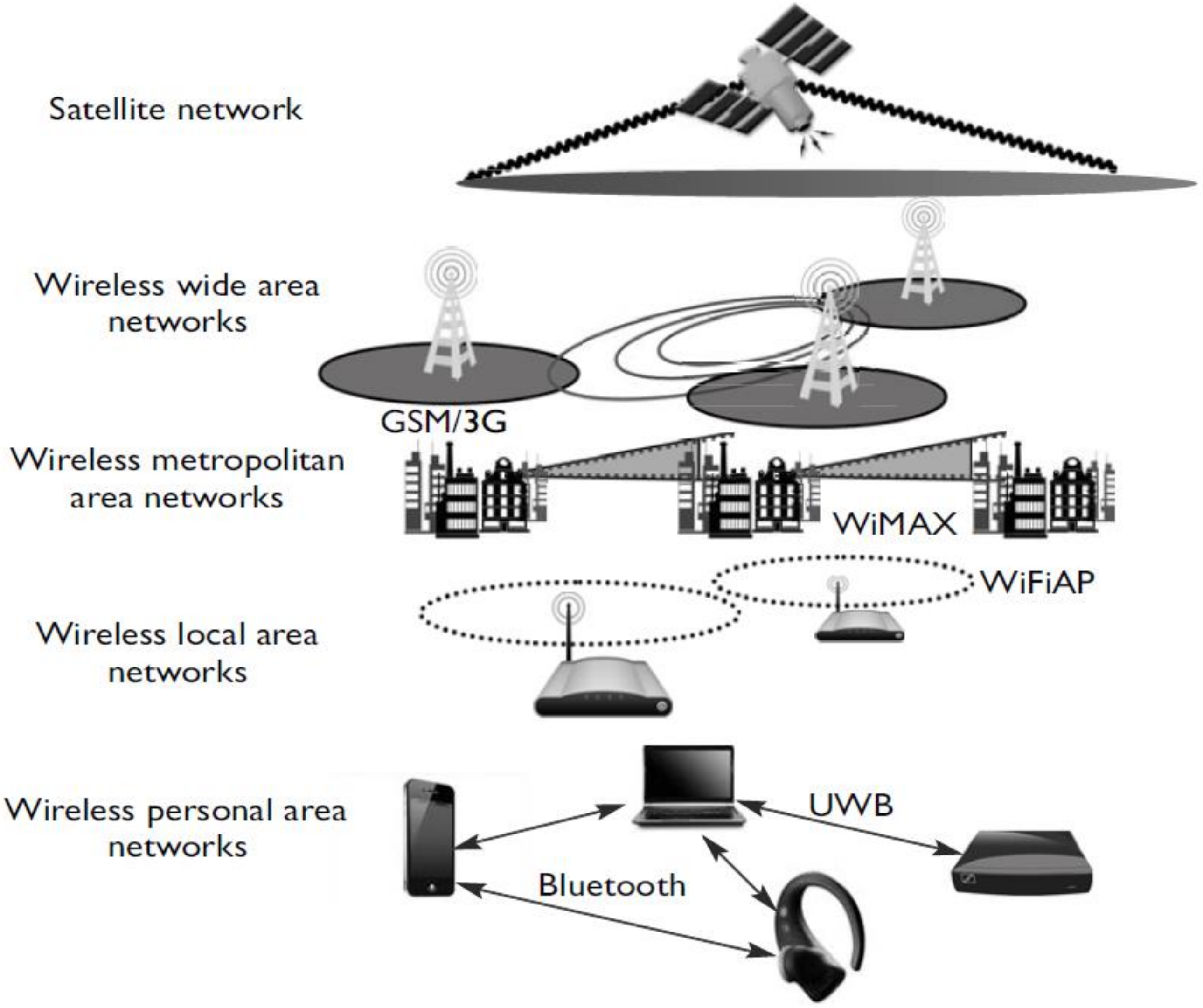


Extensible Authentication Protocol (EAP)



Protocol	Description
Lightweight EAP (LEAP)	Wireless LAN authentication method developed by Cisco Systems
EAP-TLS	Digital certificate-based authentication
EAP-MD5	Weak system authentication based upon hash values
EAP-PSK	Provides mutual authentication and session key derivation using a preshared key
EAP-TTLS	Extends TLS functionality
EAP-IKE2	Provides mutual authentication and session key establishment using asymmetric or symmetric keys or passwords
PEAPv0/EAP-MSCHAPv2	Similar in design to EAP-TTLS; however, it only requires a server-side digital certificate
PEAPv1/EAP-GTC	Cisco variant-based on Generic Token Card (GTC) authentication
EAP-FAST	Cisco-proprietary replacement for LEAP based on Flexible Authentication via Secure Tunneling (FAST)
EAP-SIM	For Global System for Mobile Communications (GSM), based on Subscriber Identity Module (SIM), a variant of PEAP for GSM
EAP-AKA	For Universal Mobile Telecommunication System (UMTS) Subscriber Identity Module (USIM) and provides Authentication and Key Agreement (AKA)
EAP-GSS	Based on Generic Security Service (GSS), it uses Kerberos

Wireless Security
- Wireless Transmission Types


Satellite network
Wireless wide area networks
GSM/3G
Wireless metropolitan area networks
WiMAX
WiFiAP
Wireless local area networks
Wireless personal area networks
UWB
Bluetooth

Wireless Security
- WLAN Elements

- **Access Point (AP):** a transceiver which connects to an wired network.
- ***Service Set ID (SSID)***: AP’s identification information.
- **Wireless Devices:** devices that communicates with AP.
- **Channel:** a certain frequency within a given frequency band. The AP is configured to transmit over a specific channel, and the wireless device will “tune” itself to be able to communicate over this same frequency.

Wireless Security
- WLAN Security

- **Wired Equivalent Privacy (WEP):**
  - CHAP for authentication
  - RC4 Cipher with pre-shared key + IV for encryption
  - No data integrity protection

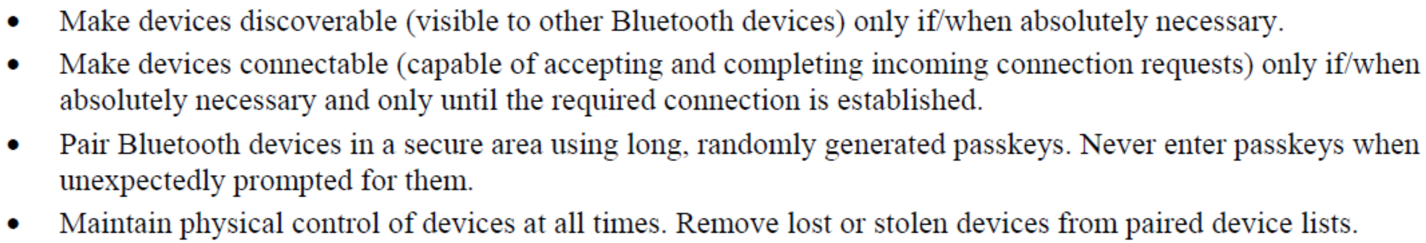
- **Wi-Fi Protected Access (WPA):**
  - EPA for authentication
  - Temporal Key Integrity Protocol (TKIP) for encryption (rotate encryption keys for each data frame)
  - Use message authentication code (MAC) for data integrity

- **Wi-Fi Protected Access II (WPA2):**
  - EPA for authentication
  - CCMP for encryption (an AES-based encryption mode)
  - CCMP for data integrity

Wireless Security
- Bluetooth Security

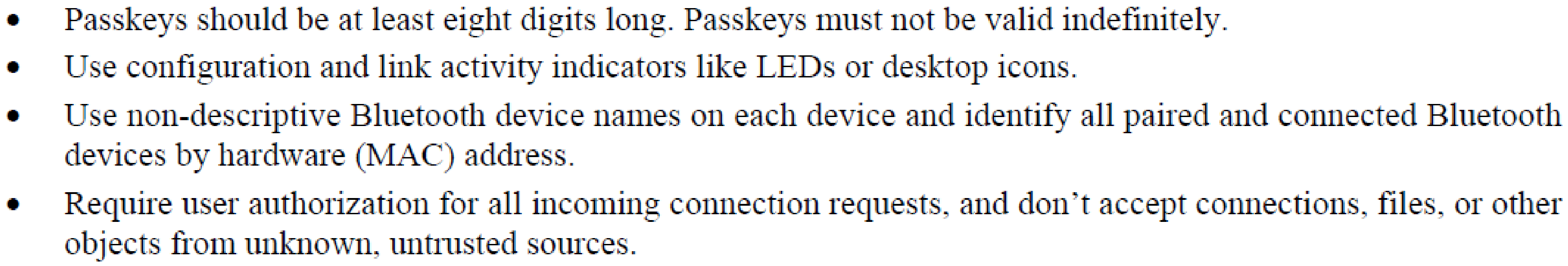
Both users and Bluetooth application developers have responsibilities and opportunities to minimize the risk of compromise via Bluetooth.

User Recommendations



- Make devices discoverable (visible to other Bluetooth devices) only if/when absolutely necessary.
- Make devices connectable (capable of accepting and completing incoming connection requests) only if/when absolutely necessary and only until the required connection is established.
- Pair Bluetooth devices in a secure area using long, randomly generated passkeys. Never enter passkeys when unexpectedly prompted for them.
- Maintain physical control of devices at all times. Remove lost or stolen devices from paired device lists.

Developer Recommendations

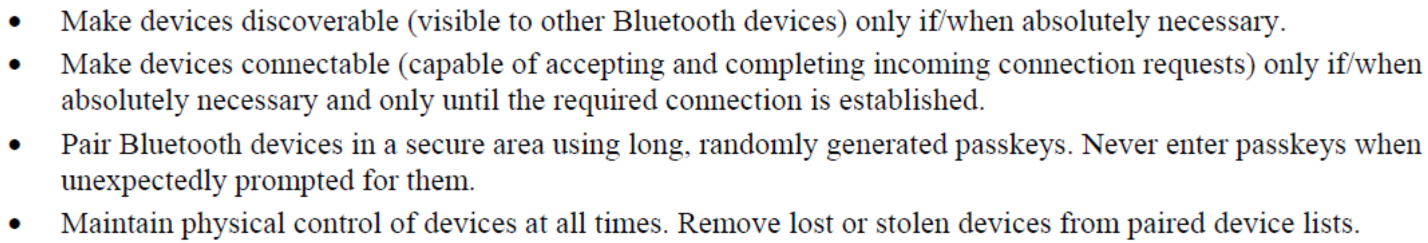


- Passkeys should be at least eight digits long. Passkeys must not be valid indefinitely.
- Use configuration and link activity indicators like LEDs or desktop icons.
- Use non-descriptive Bluetooth device names on each device and identify all paired and connected Bluetooth devices by hardware (MAC) address.
- Require user authorization for all incoming connection requests, and don't accept connections, files, or other objects from unknown, untrusted sources.

Wireless Security
- Bluetooth Security

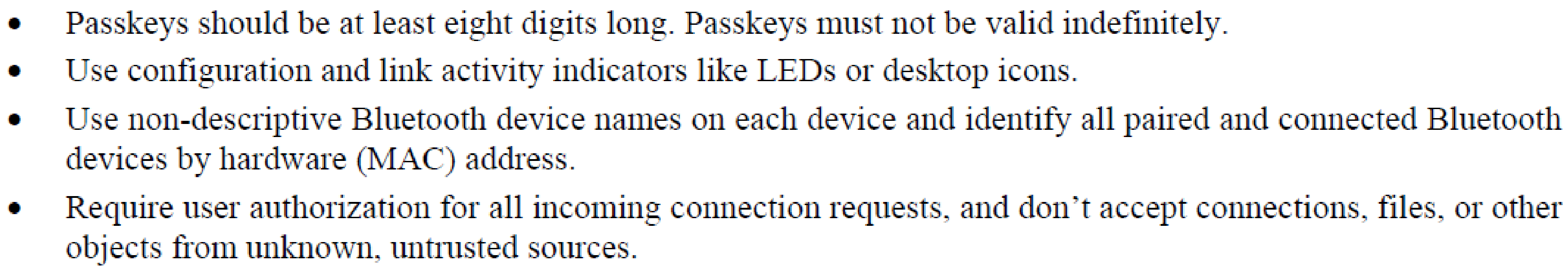
Both users and Bluetooth application developers have responsibilities and opportunities to minimize the risk of compromise via Bluetooth.

Recommendations to Users



- Make devices discoverable (visible to other Bluetooth devices) only if/when absolutely necessary.
- Make devices connectable (capable of accepting and completing incoming connection requests) only if/when absolutely necessary and only until the required connection is established.
- Pair Bluetooth devices in a secure area using long, randomly generated passkeys. Never enter passkeys when unexpectedly prompted for them.
- Maintain physical control of devices at all times. Remove lost or stolen devices from paired device lists.

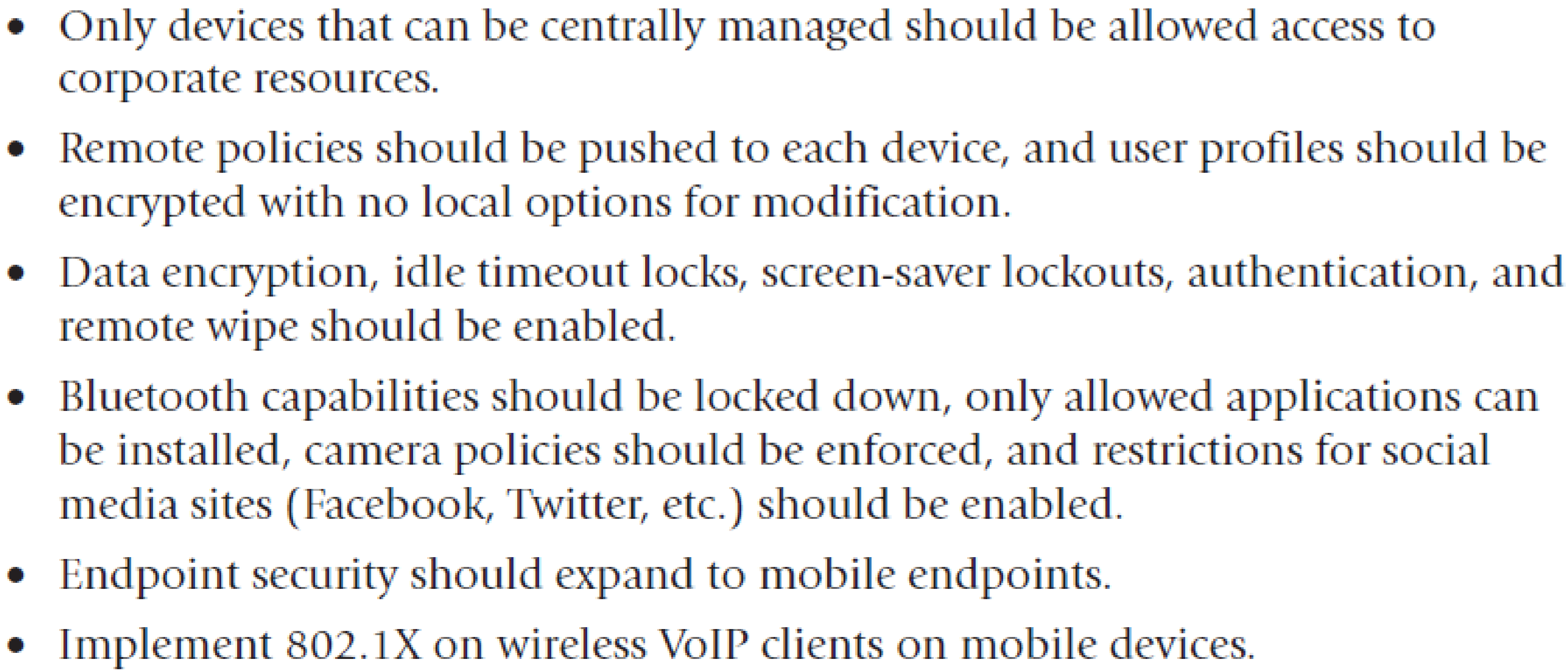
Recommendations to Developers



- Passkeys should be at least eight digits long. Passkeys must not be valid indefinitely.
- Use configuration and link activity indicators like LEDs or desktop icons.
- Use non-descriptive Bluetooth device names on each device and identify all paired and connected Bluetooth devices by hardware (MAC) address.
- Require user authorization for all incoming connection requests, and don’t accept connections, files, or other objects from unknown, untrusted sources.

Wireless Security
- Mobile Device Security

Mobile devices, if not properly managed, can compromise security in enterprise environment. The following is a short list of items that should be put into place for enterprise mobile device security:



- Only devices that can be centrally managed should be allowed access to corporate resources.
- Remote policies should be pushed to each device, and user profiles should be encrypted with no local options for modification.
- Data encryption, idle timeout locks, screen-saver lockouts, authentication, and remote wipe should be enabled.
- Bluetooth capabilities should be locked down, only allowed applications can be installed, camera policies should be enforced, and restrictions for social media sites (Facebook, Twitter, etc.) should be enabled.
- Endpoint security should expand to mobile endpoints.
- Implement 802.1X on wireless VoIP clients on mobile devices.

Network Threats & Countermeasures
- ICMP Attacks

- **Ping of Death:** a type of DoS attack in which oversized ICMP packets are sent to the victim, which may freeze or reboot the vulnerable machines.
- **Smurf:** the attacker sends an ICMP ECHO REQUEST packet with a spoofed source address to a victim's network broadcast address. This means that each system on the victim's subnet receives an ICMP ECHO REQUEST packet. Each system then replies to that request with an ICMP ECHO REPLY packet to the spoof address provided in the packets—which is the victim's address.
- **Port Scanning:** ICMP can be used to scan the network for open ports

The countermeasures to these types of attacks are to use firewall rules that only allow the necessary ICMP packets into the network and the use of IDS or IPS to watch for suspicious activities. Host-based protection (host firewalls and host IDS) can also be installed and configured to identify this type of suspicious behavior.

Network Threats & Countermeasures
- Email Related Attacks

- **E-mail Spoofing:** sending an email that appears to come from one source when it really comes from another.
- **Spear Phishing:** A phishing attack but targets on a specific person rather than a random set of people.
- **Spam:** Sending massive emails for profit.

The countermeasures to these types of attacks includes enabling SMTP authentication on the sending server, Implementing Sender Policy Framework (which validates emails data against pre-defined policy before delivering the email), enabling anti-spam services, and regulating with laws, etc.

Network Threats & Countermeasures
- Other Attacks

- **Eavesdropping:** sniffing data as it passes over a network. (***passive attacks)***
  - Encryption
- **Distributed Denial-of-service (DDoS) attack** An attacker is able to trigger large amounts of service requests to the victim's computer from a set of zombie machines.
  - Smart firewalls
- **Wardialing:** a brute force attack in which an attacker has a program that systematically dials a large bank of phone numbers with the goal of finding ones that belong to modems instead of telephones. These modems can provide easy access into an environment.
  - The countermeasures are to not publicize these telephone numbers and to implement tight access control for modems and modem pools.

Network Threats & Countermeasures
- Other Attacks

- **DNS Cache Poisoning:** provide a DNS server with incorrect information, which would point the victim to a malicious web site.
  - Limit the updates on DNS entries
- **URL Hiding:** Divert traffic to a fake website using embedded URLs.
  - Be cautious!
- **Session Hijacking:** Hijack a connection session to impersonate victims.
  - Protect session token!